ONTAP 9 문서

ONTAP 9

NetApp
February 14, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/ontap/index.html on February 14, 2026.
Always check docs.netapp.com for the latest.

목차

ONTAP 9 문서 1
릴리스 정보 2
ONTAP 9 릴리즈 주요 내용 2
ONTAP 9.18.1 주요 내용 2
ONTAP 9.17.1 주요 내용 3
ONTAP 9.16.1 하이라이트 4
ONTAP 9.15.1 하이라이트 5
ONTAP 9.14.1 주요 내용 6
ONTAP 9.13.1 주요 내용 6
ONTAP 9.12.1 주요 내용 7
ONTAP 9.11.1 하이라이트 8
ONTAP 9.10.1 하이라이트 9
ONTAP 9.9.1 주요 내용 10
ONTAP 9.18.1의 새로운 기능 10
데이터 보호 11
네트워킹 11
산 11
S3 오브젝트 스토리지 11
보안 12
스토리지 리소스 관리 기능 향상 12
ONTAP 9.17.1의 새로운 기능 13
데이터 보호 13
S3 오브젝트 스토리지 14
보안 14
스토리지 리소스 관리 기능 향상 15
ONTAP 9.16.1의 새로운 기능 15
데이터 보호 15
네트워킹 16
S3 오브젝트 스토리지 16
산 17
보안 17
스토리지 효율성 18
스토리지 리소스 관리 기능 향상 18
시스템 관리자 18
ONTAP 9.15.1의 새로운 기능 19
데이터 보호 19
보안 20
스토리지 효율성 21
스토리지 리소스 관리 기능 향상 21

시스템 관리자 21
업그레이드 21
ONTAP 9.14.1의 새로운 기능 22
데이터 보호 22
파일 액세스 프로토콜 23
S3 오브젝트 스토리지 23
산 23
보안 23
스토리지 효율성 24
스토리지 리소스 관리 기능 향상 25
SVM 관리 개선 사항 25
시스템 관리자 25
ONTAP 9.13.1의 새로운 기능 26
데이터 보호 26
파일 액세스 프로토콜 26
네트워킹 27
S3 오브젝트 스토리지 27
산 27
보안 27
스토리지 효율성 28
스토리지 리소스 관리 기능 향상 28
SVM 관리 개선 사항 28
시스템 관리자 29
ONTAP 9.12.1의 새로운 기능 29
데이터 보호 29
파일 액세스 프로토콜 30
네트워킹 31
S3 오브젝트 스토리지 31
산 31
보안 31
스토리지 효율성 32
스토리지 리소스 관리 기능 향상 32
SVM 관리 개선 사항 33
시스템 관리자 33
ONTAP 9.11.1의 새로운 기능 34
데이터 보호 34
파일 액세스 프로토콜 35
네트워킹 35
S3 오브젝트 스토리지 35
산 35
보안 36

스토리지 효율성 36
스토리지 리소스 관리 기능 향상 36
SVM 관리 개선 사항 36
시스템 관리자 37
ONTAP 9.10.1의 새로운 기능 38
데이터 보호 38
파일 액세스 프로토콜 38
네트워킹 39
S3 오브젝트 스토리지 39
산 39
보안 39
스토리지 효율성 40
스토리지 리소스 관리 기능 향상 40
SVM 관리 개선 사항 40
시스템 관리자 40
ONTAP 9.9.1의 새로운 기능 41
데이터 보호 42
파일 액세스 프로토콜 42
네트워킹 42
S3 오브젝트 스토리지 43
산 43
보안 43
스토리지 효율성 44
스토리지 리소스 관리 기능 향상 44
시스템 관리자 44
ONTAP 제한 및 기본값으로 변경합니다 45
ONTAP 기본값으로 변경합니다 45
ONTAP 제한 변경 사항 47
ONTAP 9 릴리스 지원 49
지원 수준 50
시작하십시오 51
ONTAP에 대해 알아보십시오 51
ONTAP 플랫폼 51
ONTAP 사용자 인터페이스 52
ONTAP System Manager를 NetApp 콘솔과 통합 53
클러스터 스토리지 55
고가용성 쌍 56
AutoSupport 및 디지털 자문업체 57
네트워크 아키텍처 58
클라이언트 프로토콜 61
디스크 및 로컬 계층 63

볼륨, Qtree, 파일 및 LUN 69
스토리지 가상화 70
경로 페일오버 74
ONTAP의 로드 밸런싱 76
복제 78
스토리지 효율성 86
보안 97
ONTAP 및 VMware vSphere 102
FabricPool 104
ONTAP를 위한 빠른 시작 105
ONTAP 클러스터 설정 106
ONTAP 클러스터 설정 워크플로 요약 106
ONTAP 클러스터 설정 정보를 수집합니다 107
ONTAP 클러스터를 생성하고 노드를 결합합니다 111
선택적으로 ONTAP 관리 LIF를 IPv4에서 IPv6로 변환합니다 115
Digital Advisor Config Advisor로 ONTAP 클러스터를 확인하십시오 116
ONTAP 클러스터 전체에서 시스템 시간을 동기화합니다 117
ONTAP 소프트웨어 및 펌웨어를 업그레이드하고 되돌립니다 121
ONTAP를 업그레이드합니다 121
ONTAP 업그레이드에 대해 알아봅니다 121
언제 ONTAP를 업그레이드해야 합니까? 121
계획된 업그레이드 전에 ONTAP 자동 업그레이드 사전 검사를 실행합니다 123
ONTAP 업그레이드를 준비합니다 135
업그레이드하기 전에 ONTAP 소프트웨어 이미지를 다운로드합니다 225
ONTAP 업그레이드 방법 226
ONTAP 업그레이드 후 수행할 작업 282
펌웨어, 시스템 및 보안 업데이트 297
ONTAP의 펌웨어, 시스템 및 보안 업데이트 개요 297
자동 업데이트 설치 예약 방법 299
자동 업데이트를 활성화합니다 300
자동 업데이트를 수정합니다 301
권장 자동 업데이트를 관리합니다 302
펌웨어를 수동으로 업데이트합니다 303
ONTAP를 되돌립니다 306
ONTAP 클러스터를 복구하려면 기술 지원이 필요합니까? 306
지원되는 ONTAP 되돌리기 경로 307
ONTAP 복원 문제 및 제한 사항 308
ONTAP 복원을 준비합니다 309
ONTAP 소프트웨어 이미지를 다운로드하고 설치합니다 328
ONTAP 클러스터를 되돌립니다 330
ONTAP 복원 후 수행할 작업 338

클러스터 관리 347
System Manager를 이용한 클러스터 관리 347
ONTAP System Manager를 사용한 클러스터 관리에 대해 알아보세요 347
시스템 관리자를 사용하여 ONTAP 클러스터에 액세스합니다. 348
ONTAP 클러스터에 프로토콜을 구성합니다 349
ONTAP System Manager를 사용하여 라이선스 키를 추가하여 새로운 기능을 활성화하세요. 350
ONTAP 시스템 관리자를 사용하여 클러스터 구성 다운로드 350
ONTAP 시스템 관리자를 사용하여 클러스터에 태그 지정 350
ONTAP System Manager를 사용하여 지원 사례 보기 및 제출 351
ONTAP System Manager에서 스토리지 VM의 최대 용량 한도를 관리합니다. 352
ONTAP System Manager에서 클러스터, 계층, SVM 용량 모니터링 353
ONTAP 시스템 관리자의 문제를 파악하기 위해 하드웨어 구성을 확인하세요. 356
ONTAP 시스템 관리자를 사용하여 노드 관리 362
라이센스 관리 364
ONTAP 라이센스 개요 364
NetApp Support 사이트에서 NetApp 라이센스 파일(NLF)을 다운로드합니다 367
ONTAP에서 NetApp 라이센스를 설치합니다 368
ONTAP 라이센스 관리 369
라이센스 유형 및 라이센스 방식 372
ONTAP에서 라이센스를 관리하는 명령입니다 373
CLI를 통한 클러스터 관리 374
ONTAP CLI를 사용한 클러스터 관리에 대해 자세히 알아보십시오 374
클러스터 및 SVM 관리자 374
CLI를 사용하여 클러스터에 액세스(클러스터 관리자만 해당) 376
ONTAP 명령줄 인터페이스를 사용합니다 389
ONTAP CLI 세션을 기록하고 녹화된 세션을 관리합니다 402
클러스터 관리(클러스터 관리자만 해당) 404
노드 관리 408
SP/BMC 네트워크를 구성합니다 432
SP/BMC를 사용하여 노드를 원격으로 관리합니다 438
ONTAP 클러스터 시간 관리(클러스터 관리자만 해당) 466
배너 및 MOTD 관리 468
ONTAP 작업 및 작업 일정 관리 478
클러스터 구성 백업 및 복원(클러스터 관리자만 해당) 481
ONTAP 클러스터의 노드 코어 덤프 관리(클러스터 관리자만 해당) 489
디스크 및 계층 관리 491
디스크 및 ONTAP 로컬 계층 491
로컬 계층 관리 492
디스크를 관리합니다 534
RAID 구성을 관리합니다 565
Flash Pool 로컬 계층 관리 571

FabricPool 계층 관리 586
ONTAP FabricPool를 통한 데이터 계층화에 대해 알아보십시오 586
ONTAP FabricPool 사용을 위한 요구 사항 587
ONTAP FabricPool 정책을 사용하여 데이터를 효율적으로 계층화 591
ONTAP FabricPool 구성 및 관리 작업에 대해 알아보세요. 595
FabricPool를 구성합니다 596
FabricPool 관리 613
FabricPool 미러를 관리합니다 635
FabricPool 리소스를 관리하기 위한 ONTAP 명령 643
SVM 데이터 이동성 645
ONTAP SVM 데이터 이동성에 대해 알아보세요 645
ONTAP SVM 마이그레이션 653
ONTAP 볼륨 마이그레이션 모니터링 656
ONTAP SVM 마이그레이션 일시 중지 및 재개 656
ONTAP SVM 마이그레이션 취소 657
ONTAP SVM 마이그레이션 후 클라이언트를 수동으로 컷오버합니다. 657
클라이언트 전환 후 소스 ONTAP SVM을 수동으로 제거합니다. 658
HA 쌍 관리 658
ONTAP 클러스터에서 HA 쌍 관리에 대해 알아보세요 658
ONTAP 클러스터에서 하드웨어 지원 인수에 대해 알아보세요 659
ONTAP 클러스터의 자동 인수 및 반환에 대해 알아보세요 660
ONTAP 자동 인수 명령 664
ONTAP 자동 포기 명령 664
ONTAP 수동 인수 명령 667
ONTAP 수동 포기 명령 669
ONTAP 클러스터에서 인수 및 반환 테스트 672
HA 쌍 모니터링을 위한 ONTAP 명령 674
스토리지 장애 조치를 활성화 및 비활성화하기 위한 ONTAP 명령 678
2노드 클러스터에서 인수를 시작하지 않고 ONTAP 노드를 중지하거나 재부팅합니다. 678
ONTAP HA 트래픽에 대한 암호화 구성 681
System Manager를 통한 REST API 관리 682
System Manager를 통한 REST API 관리 682
REST API 로그에 액세스 중입니다 683
볼륨 관리 686
System Manager를 사용하여 볼륨 및 LUN 관리 686
볼륨 관리 686
ONTAP 시스템 관리자를 사용하여 LUN 관리 692
ONTAP 시스템 관리자로 스토리지 확장 694
ONTAP System Manager를 사용하여 압축, 압축 및 중복 제거를 사용하여 저장 공간을 절약하세요. 696
ONTAP 시스템 관리자를 사용하여 LUN을 이동하여 부하를 균형 있게 조정합니다. 696
ONTAP 시스템 관리자를 사용하여 볼륨을 다른 계층으로 이동하여 부하를 균형 있게 조정합니다. 697

ONTAP 시스템 관리자를 사용하여 Ansible Playbook을 사용하여 볼륨이나 LUN을 추가하거나 편집합니다. 697
ONTAP System Manager를 사용하여 스토리지 효율성 정책을 관리하세요 699
ONTAP System Manager를 사용하여 할당량을 사용하여 리소스 관리 701
ONTAP 시스템 관리자를 사용하여 리소스 사용을 제한하기 위한 할당량 설정 701
ONTAP 시스템 관리자를 사용하여 테스트를 위해 볼륨 및 LUN 복제 702
ONTAP 시스템 관리자에서 정보 검색, 필터링 및 정렬 703
CLI를 통한 논리적 스토리지 관리 706
CLI를 통한 논리적 스토리지 관리 개요 706
볼륨 생성 및 관리 707
볼륨 이동 및 복사 725
FlexClone 볼륨을 사용하여 FlexVol 볼륨의 효율적인 복사본을 생성합니다 733
FlexClone 파일 및 FlexClone LUN을 사용하여 파일 및 LUN의 효율적인 복사본을 생성합니다 739
Qtree를 사용하여 FlexVol 볼륨을 분할합니다 747
볼륨에 대한 논리적 공간 보고 및 적용 752
할당량을 사용하여 리소스 사용을 제한하거나 추적합니다 759
중복제거, 데이터 압축, 데이터 컴팩션을 사용하여 스토리지 효율성을 높입니다 801
한 SVM에서 다른 SVM으로 볼륨을 다시 호스팅 829
권장되는 볼륨 및 파일 또는 LUN 구성 조합 836
파일 또는 디렉토리 용량 변경에 대한 주의 및 고려 사항 841
FlexClone 파일 및 FlexClone LUN에서 지원하는 기능입니다 843
FlexGroup 볼륨 관리 846
CLI를 사용한 ONTAP FlexGroup 볼륨 관리에 대해 자세히 알아보십시오 846
ONTAP FlexGroup 볼륨에 대해 알아보십시오 846
ONTAP FlexGroup 볼륨에 대해 지원되고 지원되지 않는 구성입니다 847
FlexGroup 볼륨 설정 852
FlexGroup 볼륨 관리 860
FlexGroup 볼륨에 대한 데이터 보호 896
FlexGroup 볼륨에 대한 데이터 보호 작업을 관리합니다 914
FlexVol 볼륨을 FlexGroup 볼륨으로 변환합니다 930
FlexCache 볼륨 관리 937
ONTAP FlexCache 볼륨에 대해 알아보십시오 937
ONTAP FlexCache 볼륨에 대해 지원되거나 지원되지 않는 기능 939
ONTAP FlexCache 볼륨 사이징 지침을 참조하십시오 944
ONTAP FlexCache 볼륨을 생성합니다 945
FlexCache 다시 쓰기 951
FlexCache 이중성 966
FlexCache 볼륨 관리 973
핫스팟 교정을 위한 FlexCache 980
네트워크 관리 993
시작하십시오 993
System Manager를 사용하여 ONTAP 네트워크를 시각화합니다 993

ONTAP 클러스터의 네트워킹 구성 요소에 대해 알아봅니다 994
ONTAP 네트워크 케이블 연결에 대한 모범 사례 996
ONTAP 네트워크에서 사용할 LIF 페일오버 정책을 결정합니다 998
NAS 경로 페일오버 워크플로우 1000
ONTAP 네트워크에서 NAS 경로 페일오버를 구성합니다 1000
ONTAP 네트워크에서 NAS 경로 페일오버를 위한 워크시트 1001
네트워크 포트 1007
ONTAP 네트워크 포트 구성에 대해 자세히 알아보십시오 1007
네트워크 포트를 구성합니다 1007
IPspace 1034
ONTAP IPspace 구성에 대해 자세히 알아보십시오 1034
ONTAP 네트워크용 IPspace를 생성합니다 1037
ONTAP 네트워크에서 IPspace를 확인합니다 1039
ONTAP 네트워크에서 IPspace를 삭제합니다 1039
브로드캐스트 도메인 1040
ONTAP 브로드캐스트 도메인에 대해 알아봅니다 1040
ONTAP 브로드캐스트 도메인을 생성합니다 1041
ONTAP 브로드캐스트 도메인에서 포트를 추가하거나 제거합니다 1044
ONTAP 포트 가용성을 복구합니다 1047
ONTAP 브로드캐스트 도메인을 IPspace로 이동합니다 1054
ONTAP 브로드캐스트 도메인을 분할합니다 1055
ONTAP 브로드캐스트 도메인을 병합합니다 1056
ONTAP 브로드캐스트 도메인의 포트에 대한 MTU 값을 변경합니다 1057
ONTAP 브로드캐스트 도메인을 봅니다 1059
ONTAP 브로드캐스트 도메인을 삭제합니다 1060
페일오버 그룹 및 정책 1061
ONTAP 네트워크에서의 LIF 페일오버에 대해 알아보십시오 1061
ONTAP 페일오버 그룹을 생성합니다 1062
LIF에 대한 ONTAP 페일오버 설정을 구성합니다 1063
ONTAP 명령으로 페일오버 그룹 및 정책을 관리할 수 있습니다 1064
서브넷(클러스터 관리자만 해당) 1065
ONTAP 네트워크의 서브넷에 대해 알아봅니다 1065
ONTAP 네트워크에 대한 서브넷을 생성합니다 1065
ONTAP 네트워크의 서브넷에서 IP 주소를 추가하거나 제거합니다 1068
ONTAP 네트워크의 서브넷 속성을 변경합니다 1070
ONTAP 네트워크의 서브넷을 봅니다 1072
ONTAP 네트워크에서 서브넷을 삭제합니다 1072
ONTAP 네트워크용 SVM을 생성합니다 1073
논리 인터페이스(LIF) 1080
LIF 개요 1080
LIF 관리 1089

ONTAP 가상 IP(VIP) LIF를 구성합니다 1107
네트워크 로드 밸런싱 1114
DNS 로드 밸런싱을 사용하여 ONTAP 네트워크 트래픽을 최적화합니다 1114
ONTAP 네트워크의 DNS 로드 밸런싱에 대해 알아봅니다 1114
ONTAP 네트워크에 대한 DNS 로드 밸런싱 존을 생성합니다 1115
로드 밸런싱 존에서 ONTAP LIF를 추가 또는 제거합니다 1116
ONTAP 네트워크에 대한 DNS 서비스를 구성합니다 1116
ONTAP 네트워크에 대한 동적 DNS 서비스를 구성합니다 1119
호스트 이름 확인 1120
ONTAP 네트워크의 호스트 이름 확인에 대해 알아봅니다 1120
ONTAP 네트워크의 호스트 이름 확인을 위해 DNS를 구성합니다 1120
ONTAP hosts 테이블을 관리하는 ONTAP 명령 1122
네트워크 보안 1123
모든 SSL 연결에 FIPS를 사용하여 ONTAP 네트워크 보안을 구성합니다 1123
IPsec 전송 중 암호화를 구성합니다 1126
ONTAP 백엔드 클러스터 네트워크 암호화 구성 1135
ONTAP 네트워크에서 LIF에 대한 방화벽 정책을 구성합니다 1136
방화벽 서비스 및 정책을 관리하는 ONTAP 명령 1142
QoS 표시(클러스터 관리자만 해당) 1142
ONTAP 네트워크 QoS(Quality of Service)에 대해 알아보기 1143
ONTAP 네트워크 QoS 표시 값을 수정합니다 1143
ONTAP 네트워크 QoS 표시 값을 확인합니다 1144
SNMP 관리(클러스터 관리자만 해당) 1144
ONTAP 네트워크의 SNMP에 대해 알아봅니다 1144
ONTAP 네트워크용 SNMP 커뮤니티를 생성합니다 1146
ONTAP 클러스터에서 SNMPv3 사용자를 구성합니다 1148
ONTAP 네트워크에서 SNMP용 traphosts를 구성합니다 1152
ONTAP 클러스터에서 SNMP 폴링을 확인합니다 1153
SNMP, 트랩 및 traphost를 관리하는 ONTAP 명령입니다 1154
SVM에서 라우팅 관리 1157
ONTAP 네트워크에서의 SVM 라우팅에 대해 알아보십시오 1157
ONTAP 네트워크에 대한 정적 라우트를 생성합니다 1157
ONTAP 네트워크에 대해 다중 경로 라우팅을 활성화합니다 1158
ONTAP 네트워크에서 정적 라우트를 삭제합니다 1158
ONTAP 라우팅 정보를 봅니다 1158
ONTAP 네트워크의 라우팅 테이블에서 동적 라우트를 제거합니다 1160
ONTAP 네트워크 정보 1161
ONTAP 네트워크 정보를 봅니다 1161
ONTAP 네트워크 포트 정보를 봅니다 1162
ONTAP VLAN 정보를 봅니다 1163
ONTAP 인터페이스 그룹 정보를 봅니다 1164

ONTAP LIF 정보 를 참조하십시오 1165
ONTAP 네트워크에 대한 라우팅 정보를 봅니다 1168
ONTAP DNS 호스트 테이블 항목을 봅니다 1170
ONTAP DNS 도메인 구성 정보를 봅니다 1170
ONTAP 페일오버 그룹 정보를 봅니다 1171
ONTAP LIF 페일오버 대상을 봅니다 1172
로드 밸런싱 존에서 ONTAP LIF를 확인하십시오 1174
ONTAP 클러스터 연결을 봅니다 1175
네트워크 문제를 진단하는 ONTAP 명령 1181
Neighbor Discovery Protocol을 통한 네트워크 접속 구성 보기 1182
NAS 스토리지 관리 1194
System Manager로 NAS 프로토콜을 관리합니다 1194
ONTAP System Manager를 사용한 NAS 관리에 대해 알아보세요 1194
ONTAP System Manager를 사용하여 VMware 데이터 저장소에 NFS 스토리지 프로비저닝 1194
ONTAP 시스템 관리자를 사용하여 홈 디렉토리에 대한 NAS 스토리지 제공 1195
ONTAP System Manager를 사용하여 NFS를 사용하여 Linux 서버용 NAS 스토리지 프로비저닝 1196
ONTAP System Manager를 사용하여 내보내기 정책을 사용하여 액세스 관리 1198
ONTAP 시스템 관리자를 사용하여 SMB를 사용하여 Windows 서버용 NAS 스토리지 프로비저닝 1198
ONTAP System Manager를 사용하여 NFS와 SMB를 모두 사용하여 Windows와 Linux 모두에 대한 NAS 스토리지를 프로비저닝합니다. 1201
ONTAP System Manager를 사용하여 Kerberos로 클라이언트 액세스 보안 1203
ONTAP 시스템 관리자를 사용하여 이름 서비스를 통해 클라이언트 액세스를 제공합니다. 1205
ONTAP System Manager를 사용하여 디렉토리 및 파일 관리 1205
ONTAP System Manager를 사용하여 호스트별 사용자 및 그룹 관리 1205
ONTAP 시스템 관리자를 사용하여 NFS 활성 클라이언트 모니터링 1209
NAS 스토리지를 설정합니다 1209
NFS 구성 1213
ONTAP CLI를 사용한 NFS 구성에 대해 알아보십시오 1213
ONTAP NFS 구성 워크플로에 대해 알아보세요 1214
준비 1215
SVM에 대한 NFS 액세스를 구성합니다 1227
NFS 지원 SVM에 스토리지 용량 추가 1261
추가 ONTAP NFS 정보를 찾을 수 있는 곳 1274
ONTAP 내보내기는 7-Mode 내보내기와는 어떻게 다릅니까 1276
NFS 관리 1279
NFS 프로토콜에 대한 ONTAP 파일 액세스에 대해 알아보세요 1279
NAS 파일 액세스 이해 1279
NAS 네임스페이스에서 데이터 볼륨을 생성하고 관리합니다 1287
보안 스타일을 구성합니다 1292
NFS를 사용하여 파일 액세스를 설정합니다 1297
NFS를 사용하여 파일 액세스를 관리합니다 1332

지원되는 NFS 버전 및 클라이언트 1382
병렬 NFS 1387
NFS 및 SMB 파일 및 디렉토리 명명 종속성 1410
NFS 트렁킹을 관리합니다 1415
ONTAP NFS 트렁킹에 대해 알아보십시오 1415
트렁킹을 위해 새 NFS 서버 및 내보내기를 구성합니다 1416
트렁킹을 위해 기존 NFS 내보내기 조정 1421
RDMA를 통해 NFS를 관리합니다 1426
ONTAP에서 RDMA를 통한 NFS에 대해 알아보십시오 1426
RDMA를 통해 NFS용 NIC를 구성합니다 1428
RDMA를 통해 NFS용 LIF를 구성합니다 1430
NFS 구성을 수정합니다 1433
CLI를 사용하여 SMB를 구성합니다 1433
ONTAP CLI를 사용한 SMB 구성에 대해 알아보십시오 1433
ONTAP SMB 구성 워크플로우 1434
준비 1435
SVM에 대한 SMB 액세스를 구성합니다 1445
공유 스토리지에 대한 SMB 클라이언트 액세스를 구성합니다 1465
CLI를 사용하여 SMB를 관리합니다 1474
ONTAP SMB에 대해 알아보십시오 1474
SMB 서버 지원 1474
SMB 서버를 관리합니다 1481
SMB를 사용하여 파일 액세스를 설정합니다 1571
SMB를 사용하여 파일 액세스를 관리합니다 1635
SMB 클라이언트 기반 서비스 구축 1722
SMB 서버 기반 서비스 구축 1735
NFS 및 SMB 파일 및 디렉토리 명명 종속성 1801
NAS 데이터에 S3 클라이언트 액세스 제공 1807
ONTAP S3 멀티프로토콜 지원에 대해 알아보세요 1807
ONTAP S3 클라이언트 액세스를 위한 NAS 데이터 요구 사항에 대해 알아보세요. 1810
ONTAP SVM에서 NAS 데이터에 대한 S3 프로토콜 액세스 활성화 1811
ONTAP S3 NAS 버킷 생성 1813
ONTAP S3 클라이언트 사용자 활성화 1815
Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성 1818
Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성 개요 1818
SMB 솔루션을 통해 Microsoft Hyper-V 및 SQL Server용 ONTAP를 구성합니다 1818
SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영 1819
원격 VSS와 공유 기반 백업 1823
SMB 공유를 통해 Hyper-V 및 SQL Server에서 ODX 복사 오프로드를 사용하는 방법 1827
구성 요구 사항 및 고려 사항 1828
SMB 구성을 통한 SQL Server 및 Hyper-V 권장 사항 1835

SMB를 통한 Hyper-V 또는 SQL Server 구성 계획 1835
SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영을 위한 ONTAP 구성 생성 1839
SMB 구성을 통해 Hyper-V 및 SQL Server 관리 1852
통계를 사용하여 SMB 작업을 통해 Hyper-V 및 SQL Server를 모니터링합니다 1857
구성이 무중단 운영이 가능한지 확인합니다 1860
SAN 스토리지 관리 1876
SAN 개념 1876
iSCSI를 사용한 SAN 프로비저닝 1876
iSCSI 서비스 관리 1877
FC를 통한 SAN 프로비저닝 1883
NVMe를 이용한 SAN 프로비저닝 1884
SAN 볼륨 1885
SAN 호스트측 공간 관리 1890
Igroup 정보 1890
igroup에 대해 이니시에이터 WWPN 및 iSCSI 노드 이름을 지정합니다 1892
가상화된 SAN 환경을 사용할 때의 이점 1892
ESX 호스트의 VMware VAAI 성능을 향상시킵니다 1892
SAN 복사 오프로드 1893
SAN 관리 1897
SAN 프로비저닝 1897
NVMe 프로비저닝 1907
LUN 관리 1919
Igroup 및 portset 관리 1931
iSCSI 프로토콜을 관리합니다 1937
FC 프로토콜을 관리합니다 1944
NVMe 프로토콜 관리 1946
FC 어댑터를 사용하여 시스템을 관리합니다 1956
모든 SAN 프로토콜에 대한 LIF 관리 1963
SAN 프로토콜에 ONTAP 공간 할당을 사용합니다 1970
권장되는 볼륨 및 파일 또는 LUN 구성 조합 1972
SAN 데이터 보호 1977
SAN 환경을 위한 ONTAP 데이터 보호 방법에 대해 알아보십시오 1977
ONTAP 스냅샷에서 단일 LUN을 복구합니다 1978
ONTAP 스냅샷에서 볼륨의 모든 LUN을 복구합니다 1980
ONTAP FlexClone LUN으로 데이터를 보호합니다 1981
SAN 환경에서 SnapVault 백업을 구성하고 사용합니다 1982
호스트 백업 시스템을 ONTAP에 연결하기 위한 권장 구성입니다 1990
호스트 백업 시스템을 사용하여 ONTAP 스토리지 시스템의 LUN을 보호합니다 1991
SAN 구성 참조 1993
ONTAP SAN 구성에 대해 자세히 알아보십시오 1993
iSCSI 구성 1993

FC 구성 1996
FCoE 구성 2003
FC 및 FCoE 조닝 2007
ONTAP 시스템 및 비 NetApp 시스템에 연결된 SAN 호스트의 요구 사항 2010
MetroCluster 환경의 SAN 구성입니다 2010
SAN 호스트 다중 경로에 대한 ONTAP 지원 2013
구성 제한 2014
S3 오브젝트 스토리지 관리 2030
ONTAP 9의 S3 지원에 대해 알아보십시오 2030
ONTAP S3 구성에 대해 자세히 알아보십시오 2030
FlexGroup 볼륨을 사용하는 ONTAP S3 아키텍처 2031
ONTAP S3 주요 사용 사례 2033
계획 2033
S3 오브젝트 스토리지를 위한 ONTAP 버전 및 플랫폼 지원 2033
ONTAP S3가 지원되는 작업 2034
ONTAP S3 상호 운용성 2044
ONTAP에서 S3를 사용한 검증된 타사 솔루션 2046
구성 2046
S3 구성 프로세스 정보 2047
SVM에 대한 S3 액세스를 구성합니다 2051
S3 지원 SVM에 스토리지 용량 추가 2067
액세스 정책 문을 만들거나 수정합니다 2083
S3 오브젝트 스토리지에 대한 클라이언트 액세스 지원 2098
ONTAP S3 스토리지 서비스 레벨 2101
ONTAP S3 버킷을 위한 CORS(Cross-Origin Resource Sharing)를 구성합니다 2102
SnapMirror S3로 버킷 보호 2107
ONTAP SnapMirror S3에 대해 알아보십시오 2107
원격 클러스터의 미러링 및 백업 보호 2110
로컬 클러스터의 미러링 및 백업 보호 2121
클라우드 타겟을 통한 백업 보호 2132
ONTAP SnapMirror S3 정책을 수정합니다 2141
스냅샷으로 S3 데이터를 보호합니다 2142
ONTAP S3 스냅샷에 대해 자세히 알아보십시오 2142
ONTAP S3 스냅샷을 생성합니다 2144
ONTAP S3 스냅샷을 보고 복원합니다 2146
ONTAP S3 스냅샷을 삭제합니다 2148
S3 이벤트를 감사합니다 2150
ONTAP S3 이벤트 감사에 대해 자세히 알아보십시오 2150
ONTAP S3 감사 구성 계획 2152
ONTAP S3 감사 구성을 생성하고 사용합니다 2155
ONTAP S3 감사를 위한 버킷 선택 2156

ONTAP S3 감사 구성을 수정합니다 2157
ONTAP S3 감사 구성을 표시합니다 2158
인증 및 액세스 제어 2161
인증 및 액세스 제어 개요 2161
클라이언트 인증 및 권한 부여 2161
관리자 인증 및 RBAC 2161
관리자 인증 및 RBAC 관리 2161
ONTAP의 관리자 인증 및 RBAC에 대해 알아봅니다 2161
ONTAP 관리자 인증 및 RBAC 워크플로 2162
ONTAP 관리자 인증 및 RBAC 설정을 위한 워크시트 2163
로그인 계정을 만듭니다 2176
액세스 제어 역할을 관리합니다 2191
관리자 계정을 관리합니다 2204
여러 관리자 검증 관리 2228
동적 권한 부여 관리 2261
OAuth 2.0을 사용한 인증 및 권한 부여 2270
ONTAP OAuth 2.0 구축 개요 2270
개념 2274
구성 및 배포 2288
원격 ONTAP 사용자에 대한 SAML 인증 구성 2295
SAML 인증을 활성화합니다 2295
SAML 인증을 비활성화합니다 2300
타사 IdP 구성 2301
SAML 구성 관련 문제를 해결합니다 2303
ONTAP 에서 OAuth 2.0 또는 SAML IdP 그룹 작업 2305
그룹을 식별하는 방법 2305
이름으로 그룹을 관리합니다 2306
UUID를 사용하여 그룹을 관리합니다 2307
WebAuthn MFA를 사용한 인증 및 권한 부여 2309
ONTAP System Manager 사용자를 위한 WebAuthn 다중 요소 인증에 대해 알아보세요. 2309
ONTAP 시스템 관리자 사용자 또는 그룹에 대해 WebAuthn MFA를 활성화합니다 2309
ONTAP 시스템 관리자 사용자를 위한 WebAuthn MFA를 비활성화합니다 2311
ONTAP WebAuthn MFA 설정을 보고 자격 증명을 관리합니다 2312
웹 서비스 관리 2314
웹 서비스 관리 개요 2314
ONTAP 웹 서비스에 대한 액세스 관리 2315
ONTAP에서 웹 프로토콜 엔진을 관리합니다 2317
웹 프로토콜 엔진을 관리하기 위한 ONTAP 명령 2318
ONTAP 웹 서비스에 대한 액세스 구성 2318
웹 서비스 관리를 위한 ONTAP 명령 2320
ONTAP 노드의 마운트 포인트를 관리하기 위한 명령 2320

ONTAP 에서 SSL 관리 2321
ONTAP 웹 서비스에 HSTS 사용 2321
ONTAP 웹 서비스 액세스 문제 해결 2323
인증서를 사용하여 원격 서버의 ID를 확인합니다 2326
ONTAP 에서 인증서를 사용하여 원격 서버의 신원을 확인하는 방법에 대해 알아보세요. 2326
ONTAP 에서 OCSP를 사용하여 디지털 인증서가 유효한지 확인합니다. 2326
ONTAP 에서 TLS 기반 애플리케이션의 기본 인증서 보기 2328
클러스터와 KMIP 서버를 상호 인증합니다 2329
ONTAP 클러스터와 KMIP 서버 개요 상호 인증 2329
ONTAP에서 클러스터에 대한 인증서 서명 요청을 생성합니다 2329
ONTAP 클러스터에 대한 CA 서명 서버 인증서 설치 2330
ONTAP 의 KMIP 서버에 대한 CA 서명 클라이언트 인증서 설치 2331
보안 및 데이터 암호화 2333
자율 랜섬웨어 보호 2333
ONTAP 자율적 랜섬웨어 방어에 대해 알아보십시오 2333
ONTAP 자율적 랜섬웨어 방어 사용 사례 및 고려사항 2340
ARP 활성화 2344
학습 기간 후에 ONTAP ARP에서 활성 모드로 전환합니다 2354
SAN 볼륨에 대한 ONTAP ARP 평가 기간에 대해 알아보세요. 2356
ONTAP 자율적 랜섬웨어 보호를 일시 중지하여 워크로드 이벤트를 분석에서 제외합니다 2359
ONTAP 자율적 랜섬웨어 방어 공격 감지 매개 변수를 관리합니다 2361
ONTAP ARP가 감지한 비정상적인 활동에 응답합니다 2365
랜섬웨어 공격 후 ONTAP ARP 스냅샷에서 데이터를 복원합니다 2371
자동 생성된 ARP 스냅샷에 대한 설정 조정 2375
AI(ARP/AI)로 ONTAP 자율적 랜섬웨어 방어 업데이트 2379
Vscan을 통한 바이러스 보호 2381
ONTAP Vscan을 사용한 바이러스 백신 구성에 대해 알아보세요 2381
NetApp 바이러스 백신 보호 정보 2381
Vscan 서버 설치 및 구성 2387
스캐너 풀을 구성합니다 2395
액세스 시 스캔을 구성합니다 2402
온디맨드 스캐닝 구성 2407
ONTAP Vscan에서 오프박스 바이러스 백신 기능을 구성하기 위한 모범 사례 2412
SVM ONTAP Vscan에서 바이러스 검사 활성화 2413
ONTAP Vscan 스캔 파일 상태 재설정 2414
ONTAP를 사용하여 Vscan 이벤트 로그 정보를 봅니다 2415
연결 문제를 모니터링하고 해결합니다 2415
SVM에서 NAS 이벤트를 감사합니다 2421
SMB 및 NFS 프로토콜 모두에 대해 ONTAP를 사용하여 파일 액세스를 감사하는 방법에 대해 알아보십시오 2421
감사 작동 방식 2422
ONTAP 감사를 위한 사전 요구 사항 2424

ONTAP 감사 레코드의 스테이징 파일 크기에 대한 제한 사항 2426
ONTAP 감사 이벤트 로그에 지원되는 형식에 대해 알아봅니다 2426
ONTAP 감사 이벤트 로그를 보고 처리합니다 2427
감사할 수 있는 SMB 이벤트입니다 2428
NFS 파일 및 디렉토리 액세스 이벤트에 대한 ONTAP 감사 에 대해 자세히 알아보십시오 2433
ONTAP SVM에 대한 감사 구성 계획 2434
SVM에 파일 및 디렉토리 감사 구성을 생성합니다 2440
파일 및 폴더 감사 정책을 구성합니다 2443
파일 및 디렉토리에 적용된 감사 정책에 대한 정보를 표시합니다 2447
감사할 수 있는 CLI 변경 이벤트입니다 2453
감사 구성을 관리합니다 2460
ONTAP 감사 및 스테이징 볼륨 공간 문제 해결 2464
SVM에서 파일 모니터링 및 관리를 위해 FPolicy를 사용합니다 2466
FPolicy 이해 2466
FPolicy 구성을 계획합니다 2474
FPolicy 구성을 생성합니다 2510
FPolicy 구성을 관리합니다 2517
보안 추적을 사용하여 액세스를 확인합니다 2526
ONTAP 보안 추적에 대해 알아보세요 2526
ONTAP SVM에서 보안 추적 모니터링을 위한 액세스 검사 유형 2527
ONTAP SVM에서 보안 추적을 생성할 때의 고려 사항 2527
보안 추적을 수행합니다 2528
ONTAP 보안 추적 결과 해석 2536
ONTAP SVM에 대한 추가 정보를 찾을 수 있는 곳 2537
System Manager로 암호화를 관리합니다 2538
소프트웨어 기반 암호화를 사용하여 ONTAP 클러스터에 저장된 데이터를 암호화합니다. 2538
자체 암호화 드라이브를 사용하여 ONTAP 클러스터에 저장된 데이터를 암호화합니다. 2538
CLI를 사용하여 암호화를 관리합니다 2539
ONTAP 저장 데이터 암호화에 대해 알아보세요 2539
NetApp 볼륨 및 집계 암호화 구성 2539
NetApp 하드웨어 기반 암호화를 구성합니다 2575
NetApp 암호화 관리 2598
데이터 보호 및 재해 복구 2634
클러스터 및 SVM 피어링 2634
ONTAP 클러스터 및 SVM 피어링에 대해 알아보십시오 2634
클러스터 및 SVM 피어링을 준비합니다 2634
인터클러스터 LIF를 구성합니다 2638
피어 관계를 구성합니다 2650
피어 관계에서 ONTAP 클러스터 피어링 암호화를 활성화합니다 2659
피어 관계에서 ONTAP 클러스터 피어링 암호화를 제거합니다 2660
로컬 스냅샷을 관리합니다 2661

로컬 ONTAP 스냅샷 관리에 대해 자세히 알아보십시오 2661
ONTAP 장기 보존 스냅샷에 대해 알아보세요 2661
사용자 지정 스냅샷 정책을 구성합니다 2662
스냅샷을 수동으로 관리합니다 2665
스냅숏 예비 공간을 관리합니다 2668
스냅샷에서 파일을 복원합니다 2672
SnapMirror 볼륨 복제 2678
SnapMirror 볼륨 복제에 대해 알아보십시오 2679
SnapMirror 볼륨 복제를 구성합니다 2706
SnapMirror 볼륨 복제를 관리합니다 2726
SnapMirror SVM 복제 관리 2756
ONTAP SnapMirror SVM 복제에 대해 알아보십시오 2756
SVM 구성 복제 2763
SnapMirror SVM DR 대상에서 데이터 제공 2775
SnapMirror 소스 SVM을 재활성화합니다 2779
ONTAP SnapMirror 볼륨 DR 관계를 SVM DR 관계로 변환합니다 2792
ONTAP SnapMirror SVM 복제 관계를 삭제합니다 2793
SnapMirror 루트 볼륨 복제를 관리합니다 2795
ONTAP SnapMirror 루트 볼륨 복제에 대해 알아보십시오 2795
ONTAP 로드 공유 미러 관계를 생성하고 초기화합니다 2795
ONTAP 로드 공유 미러 관계를 업데이트합니다 2797
ONTAP 로드 공유 미러를 상향 이동합니다 2797
클라우드에 백업 2799
ONTAP SnapMirror 클라우드 라이센스를 설치합니다 2799
ONTAP SnapMirror를 사용하여 클라우드에 데이터를 백업합니다 2800
NetApp Backup and Recovery를 사용하여 데이터 백업 2802
SnapLock 기술을 사용한 아카이브 및 규정 준수 2806
ONTAP SnapLock 에 대해 알아보세요 2806
SnapLock를 구성합니다 2811
WORM 파일 관리 2825
ONTAP SnapLock 볼륨 이동 2839
랜섬웨어 공격으로부터 보호하기 위해 ONTAP 스냅샷 잠금 2841
정합성 보장 그룹 2848
ONTAP 일관성 그룹에 대해 알아보세요 2848
ONTAP 일관성 그룹 제한에 대해 알아보세요 2853
단일 ONTAP 일관성 그룹 구성 2854
계층적 ONTAP 일관성 그룹 구성 2858
ONTAP 일관성 그룹 보호 2862
ONTAP 일관성 그룹의 멤버 볼륨 수정 2870
ONTAP 일관성 그룹 지오메트리 수정 2875
ONTAP 일관성 그룹 애플리케이션 및 구성 요소 태그 수정 2880

ONTAP 일관성 그룹 복제 2881
ONTAP 일관성 그룹 삭제 2883
SnapMirror 활성 동기화 2884
소개 2884
계획 2896
구성 2905
SnapMirror 활성 동기화를 관리하고 데이터를 보호합니다 2947
문제 해결 2964
MetroCluster 및 SnapMirror Active Sync를 위한 ONTAP Mediator 2974
ONTAP 중재자에 대해 자세히 알아보십시오 2974
ONTAP Mediator의 새로운 기능 2975
설치 또는 업그레이드 2981
ONTAP 중재자 관리 3025
ONTAP 중재자를 위한 호스트 OS를 유지 관리합니다 3055
ONTAP System Manager를 사용한 MetroCluster IP 사이트 관리에 대해 알아보세요 3059
테이프 백업을 사용한 데이터 보호 3060
ONTAP FlexVol 볼륨의 테이프 백업에 대해 알아보세요 3060
ONTAP 테이프 백업 및 복원 워크플로 3060
ONTAP SMTape 및 덤프 백업 엔진의 사용 사례 3061
테이프 드라이브 관리 3061
테이프 드라이브 정보 3067
스토리지 시스템 간 데이터 전송 3076
FlexVol 볼륨용 NDMP 3079
ONTAP FlexGroup 볼륨을 통한 NDMP 지원에 대해 알아보세요. 3099
ONTAP SnapLock 볼륨을 사용한 NDMP에 대해 알아보세요 3099
FlexVol 볼륨에 대한 노드 범위 NDMP 모드를 관리합니다 3099
FlexVol 볼륨에 대한 SVM 범위의 NDMP 모드를 관리합니다 3101
FlexVol 볼륨의 덤프 엔진 정보 3107
FlexVol 볼륨용 SMTape 엔진 정보 3118
FlexVol 볼륨에 대한 테이프 백업 및 복원 작업을 모니터링합니다 3122
FlexVol 볼륨의 테이프 백업 및 복원에 대한 오류 메시지입니다 3125
NDMP 구성 3146
ONTAP NDMP 구성에 대해 자세히 알아보십시오 3146
ONTAP NDMP 구성 워크플로에 대해 알아보세요 3146
ONTAP NDMP 구성 준비 3147
ONTAP NDMP 테이프 장치 연결 확인 3150
ONTAP NDMP 백업 작업에 대한 테이프 예약 활성화 3151
SVM 범위 NDMP를 구성합니다 3152
노드 범위 NDMP를 구성합니다 3161
ONTAP NDMP 구성을 위한 백업 애플리케이션 구성 3166
NetApp Element 소프트웨어와 ONTAP 간 복제 개요 3166

이벤트, 성능 및 상태 모니터링 3167
System Manager로 클러스터 성능을 모니터링합니다 3167
ONTAP 시스템 관리자를 사용하여 클러스터 성능 모니터링 3167
ONTAP System Manager 대시보드의 뷰 클러스터에 대해 알아보세요 3167
ONTAP 시스템 관리자에서 핫 볼륨 및 기타 객체 식별 3169
ONTAP 시스템 관리자에서 QoS 수정 3169
ONTAP 시스템 관리자에서 위험 모니터링 3169
ONTAP System Manager 통찰력으로 시스템을 최적화하세요 3171
ONTAP 시스템 관리자에서 기본 FPolicies 구성 3173
CLI를 사용하여 클러스터 성능을 모니터링하고 관리합니다 3174
ONTAP 성과 관리 워크플로 3174
기본 인프라 검사를 수행합니다 3175
워크로드 관리 3182
Unified Manager를 사용하여 클러스터 성능을 모니터링하고 관리하세요. 3201
ONTAP Unified Manager를 사용하여 클러스터 성능 모니터링 3201
ONTAP Active IQ Unified Manager 성능 모니터링 및 관리에 대해 알아보세요 3201
성능을 모니터링합니다 3202
ONTAP Active IQ Digital Advisor 사용하여 시스템 성능을 확인하세요. 3212
ONTAP Data Infrastructure Insights를 사용하여 클러스터 성능 모니터링 3212
모든 리소스를 모니터링, 문제 해결 및 최적화합니다 3213
로깅 감사 3213
ONTAP 감사 로깅 구현에 대해 자세히 알아보십시오 3213
ONTAP 감사 로깅의 변경 사항에 대해 알아봅니다 3214
ONTAP 감사 로그 내용을 표시합니다 3215
ONTAP 감사 가져오기 요청 설정을 관리합니다 3216
ONTAP 클러스터 간 감사 활성화 3216
ONTAP 감사 로그 대상을 관리합니다 3218
AutoSupport 3219
AutoSupport에 대해 자세히 알아보십시오 3220
계획 3232
구성 3239
AutoSupport를 사용하여 파일을 업로드합니다 3242
문제 해결 3244
상태 모니터링 3250
ONTAP 시스템 상태 모니터링에 대해 알아보십시오 3250
ONTAP 상태 모니터링 구성 요소에 대해 알아보십시오 3250
ONTAP 시스템 상태 경고 응답에 대해 알아보십시오 3251
ONTAP 시스템 상태 경고 사용자 지정에 대해 자세히 알아보십시오 3251
ONTAP AutoSupport 상태 경고 트리거에 대해 자세히 알아보십시오 3252
사용 가능한 ONTAP 클러스터 상태 모니터에 대해 자세히 알아보십시오 3252
ONTAP 시스템 상태 경고를 자동으로 수신합니다 3253

성능이 저하된 ONTAP 시스템 상태에 응답합니다 3254
성능이 저하된 ONTAP 시스템 상태에 대한 응답에 대해 자세히 알아보십시오 3255
ONTAP 시스템의 상태를 모니터링하는 명령입니다 3258
ONTAP 환경 정보 보기 3261
파일 시스템 분석 3261
ONTAP 파일 시스템 분석에 대해 알아보십시오 3261
ONTAP 파일 시스템 분석 활성화 3263
FSA를 사용하여 ONTAP 파일 시스템 활동 보기 3267
FSA를 사용하여 ONTAP 활동 추적 활성화 3268
FSA를 사용하여 ONTAP 사용 분석 활성화 3270
FSA에서 ONTAP 분석을 기반으로 시정 조치를 취하세요 3271
ONTAP 파일 시스템 분석을 통해 역할 기반 액세스 제어 3272
ONTAP 파일 시스템 분석을 위한 고려 사항 3274
EMS 구성 3276
ONTAP EMS 구성에 대해 자세히 알아보십시오 3276
System Manager를 사용하여 ONTAP EMS 이벤트 알림 및 필터를 구성합니다 3276
CLI로 EMS 이벤트 알림을 설정한다 3279
더 이상 사용되지 않는 EMS 이벤트 매핑을 업데이트합니다 3285
ONTAP 명령 참조입니다 3293
제한된 ONTAP 지원 버전에 대한 명령 참조(PDF만 해당) 3293
CLI 비교 툴 3293
법적 고지 3294
저작권 3294
상표 3294
특허 3294
개인 정보 보호 정책 3294
오픈 소스 3294
ONTAP 3294
MetroCluster IP 구성을 위한 ONTAP 중재자 3294

ONTAP 9 문서

릴리스 정보

ONTAP 9 릴리즈 주요 내용

ONTAP 9 데이터 관리 소프트웨어의 각 릴리즈는 ONTAP의 기능, 관리성, 성능 및 보안 기능을 강화하는 새롭고 향상된 기능을 제공합니다.

이러한 주요 기능 외에도 최신 ONTAP 릴리스에 도입된 새로운 기능 및 향상된 기능을 버전별로 포괄적으로 제공합니다.

- 에 대해 자세히 알아보십시오 "새롭고 향상된 ONTAP MetroCluster 기능".
- 에 대해 알아보세요 "NetApp AFX 스토리지 시스템을 위한 새롭고 향상된 ONTAP 소프트웨어 기능" .
- 에 대해 알아보세요 "NetApp ASA r2 스토리지 시스템을 위한 새롭고 향상된 ONTAP 소프트웨어 기능" .
- 에 대해 알아보세요 "AFF, ASA 및 FAS 시스템과 지원되는 스위치에 대한 새롭고 향상된 지원" .
- 의 업데이트에 대해 알아봅니다 "ONTAP REST API를 참조하십시오".

최신 ONTAP 9 릴리스에서 알려진 문제, 제한 사항 및 업그레이드 주의 사항에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 릴리즈 노트". 릴리스 정보에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

ONTAP의 최신 릴리즈로 업그레이드하려면 를 참조하십시오 ONTAP의 최신 버전으로 업그레이드하십시오 및 언제 ONTAP를 업그레이드해야 합니까?

ONTAP 9.18.1 주요 내용

ONTAP 9.18.1은 데이터 인프라 현대화를 지원하기 위해 보안, 확장성, 스토리지 관리 분야에서 새롭고 향상된 기능을 제공합니다. 이러한 개선 사항은 확장하고, 더 효율적으로 운영하고, 미래를 위해 데이터를 보호하는 데 도움이 됩니다. 새로운 기능 및 향상된 기능의 전체 목록을 보려면 다음을 참조하세요.ONTAP 9.18.1의 새로운 기능 .

- 백엔드 클러스터 HA 암호화

  백엔드 클러스터 네트워크를 암호화하기 위해 mTLS를 사용할 수 있는 기능입니다.

- 전송 중인 데이터에 대한 PQC 지원

  전송 중인 데이터에 포스트 양자 알고리즘을 사용할 수 있는 능력.

- HW 오프로드를 통한 IPv6 IPSec 지원

  IPv6 주소로 하드웨어 오프로드를 통한 IPSec 지원.

- ARP/AI 지원 FlexGroup 볼륨

  NetApp FlexGroup 볼륨은 ARP/AI를 지원하여 고급 머신 러닝 기반 랜섬웨어 탐지 및 보호 기능을 제공합니다.

- NVMe를 위한 복사 오프로드

  복사 작업을 스토리지에 직접 오프로드하여 대용량 데이터 전송을 가속화하고, 호스트 CPU와 네트워크 부하를 줄입니다.

- 저장소 기반 S3 버킷 스냅샷 복원

  S3 버킷에서 손상된 객체를 복원하거나 기존 버킷 위에 전체 버킷을 복원하는 기능을 제공합니다.

ONTAP 9.17.1 주요 내용

ONTAP 9.17.1은 SAN을 위한 AI 기반 자율 랜섬웨어 보호에 혁신을 제공하고 SnapMirror 액티브 동기화 및 일관성 그룹 계층 관리를 통해 NVMe 프런트엔드 호스트 지원을 추가합니다. 이러한 개선 사항을 통해 NetApp은 데이터 보안과 사이버 복원력 분야에서 리더십을 강화하고 ONTAP 성능, 확장성, 효율성 및 비즈니스 연속성을 개선합니다. 새로운 기능 및 향상된 기능의 전체 목록은 다음을 참조하세요. ONTAP 9.17.1의 새로운 기능 .

- 자율형 랜섬웨어 보호를 통한 SAN 지원

  ARP는 암호화 기반 이상 탐지 기능을 갖춘 SAN 볼륨을 지원하고, 상세한 엔트로피 통계를 위한 새로운 명령을 도입하며, 이전에 NAS에 집중되었던 System Manager의 랜섬웨어 보호 메시징 기능을 통합합니다. 구성 가능한 탐지 임계값과 더욱 확정적인 스냅샷 보존 기능은 다양한 워크로드에 대한 유연성을 높여줍니다.

- HTTP Strict Transport Security(HSTS) 지원

  ONTAP 9.17.1은 웹 서비스에 대한 HTTP Strict Transport Security를 지원하여 사용자 브라우저와 ONTAP 간의 안전한 HTTPS 통신을 시행할 수 있습니다.

- 링크 집계 그룹을 통한 IPsec 하드웨어 오프로드

  ONTAP 9.17.1은 링크 집계 그룹에 대한 IPsec 하드웨어 오프로드를 지원하여 ONTAP 9.16.1에 도입된 하드웨어 오프로드 지원을 확장합니다.

- IPsec 포스트퀀텀 사전 공유 키 지원

  ONTAP 미래의 양자 컴퓨터 공격으로부터 보호하기 위해 IPsec에 대한 포스트퀀텀 사전 공유 키를 지원합니다.

- OpenStack Barbican 키 관리자 지원

  ONTAP NetApp 볼륨 암호화(NVE) 키에 대한 OpenStack의 Barbican 키 관리자를 지원합니다.

- JIT(Just in Time) 권한 승격 지원

  ONTAP 역할 기반 액세스 제어(RBAC)를 위한 JIT 권한 승격을 지원합니다. 사용자는 구성된 역할에 대한 임시 권한 승격을 요청하여 필요에 따라 권한이 부여된 명령에 액세스할 수 있습니다. 클러스터 관리자는 JIT 권한 승격에 액세스할 수 있는 사용자, 액세스 허용 시점 및 기간을 설정할 수 있습니다.

- SAML 인증을 위한 Entra IdP 및 IdP 그룹 지원 지원

  ONTAP SAML ID 공급자로 Microsoft Entra를 지원합니다. 또한 IdP에서 제공하는 그룹 정보를 ONTAP 역할에 매핑할 수 있습니다.

- NVMe를 통한 호스트 액세스를 위한 SnapMirror 활성 동기화 지원

  SnapMirror Active Sync는 NVMe/TCP를 사용하는 VMware 워크로드에 대한 NVMe 액세스 지원과 2노드 ONTAP 클러스터에 대한 NVMe/FC 호스트 액세스를 추가합니다.

- SnapMirror Active Sync를 통한 ONTAP Cloud Mediator 지원

ONTAP Cloud Mediator는 ONTAP 9.17.1에 도입되었으며 SnapMirror 액티브 동기화 관계를 지원합니다. ONTAP Mediator와 마찬가지로 클라우드 기반 Mediator는 SnapMirror 액티브 동기화 관계에 대한 쿼럼 감시 역할을 하여 투명한 장애 조치를 보장하는 동시에 제3자 사이트 유지 관리의 운영 복잡성을 줄여줍니다.

ONTAP 9.16.1 하이라이트

ONTAP 9.16.1은 보안 관리, 데이터 보호, 네트워킹, SAN 관리 및 스토리지 관리 영역에서 새롭고 향상된 기능을 제공합니다. 새로운 기능 및 향상된 기능의 전체 목록은 를 참조하십시오ONTAP 9.16.1의 새로운 기능.

- MAV(Multi-admin Verification) 기능 향상

  ONTAP 9.16.1은 악의적인 내부자로부터 추가적인 보호를 위해 MAV 프레임워크에 더 많은 명령을 추가합니다. 이러한 향상된 기능에는 다수의 CG(Consistency Group), Vscan 및 ARP(Autonomous Ransomware Protection) 관리, NVMe 구성 명령이 포함됩니다.

- AI 개선(ARP/AI)을 통한 자율적 랜섬웨어 방어

  ARP는 새로운 AI 기능으로 업그레이드되어 99%의 정밀도와 리콜로 랜섬웨어 공격을 감지하고 이에 대응할 수 있습니다. AI는 포괄적인 데이터 세트에서 훈련되기 때문에 FlexVol 볼륨에서 실행되는 ARP에 대한 학습 기간이 더 이상 없으며 ARP/AI가 즉시 활성 모드에서 시작됩니다. ARP/AI는 또한 ONTAP 업그레이드와 독립적인 자동 업데이트 기능을 도입하여 최신 위협에 대한 지속적인 보호 및 복원력을 보장합니다.

- TLS를 통한 NVMe/TCP 1.3

  IPSec에 비해 간소화된 구성과 향상된 성능으로 프로토콜 계층에서 NVMe/TCP를 "유선"으로 보호합니다.

- 새 네트워크 카드에 대한 IPsec HW 오프로드 지원

  ONTAP 9.16.1은 최신 AFF A 시리즈 및 AFF-C 시리즈 시스템 플랫폼에 도입된 오프로드 카드에서 IPSec 하드웨어 오프로드 기능을 활용할 때 보다 높은 "유선" 암호화 성능을 제공합니다.

- NVMe 공간 할당 해제 지원

  이제 NVMe 네임스페이스에 대한 공간 할당 해제(홀 펀칭 및 언맵이라고도 함)가 지원됩니다. 공간 할당 해제는 호스트 애플리케이션에서 데이터를 삭제할 때 씬 프로비저닝된 볼륨과 NVMe 네임스페이스가 사용되지 않은 공간을 회수하는 데 도움이 됩니다. 이를 통해 전반적인 저장 효율성이 크게 향상되며, 특히 데이터 회전율이 높은 파일 시스템의 경우 더욱 그렇습니다.

- FlexGroup 볼륨을 위한 고급 용량 밸런싱

  NetApp FlexGroup 볼륨은 필요에 따라 여러 백 엔드 구성 볼륨에 걸쳐 단일 파일 내의 데이터를 스트라이핑하여 성능 병목 현상을 줄이고 백엔드 구성 볼륨 간에 용량 밸런싱의 일관성을 추가할 수 있습니다.

- MetroCluster 구성 마이그레이션에 대한 SVM 데이터 이동성 지원

  ONTAP은 다음 MetroCluster SVM 마이그레이션을 지원합니다.

  - 비 MetroCluster 구성과 MetroCluster IP 구성 간에 SVM 마이그레이션
  - 2개의 MetroCluster IP 구성 간에 SVM 마이그레이션
  - MetroCluster FC 구성과 MetroCluster IP 구성 간에 SVM 마이그레이션

ONTAP 9.15.1 하이라이트

ONTAP 9.15.1은 보안 관리, 데이터 보호 및 NAS 워크로드 지원 영역에서 새롭고 향상된 기능을 제공합니다. 새로운 기능 및 향상된 기능의 전체 목록은 를 참조하십시오 ONTAP 9.15.1의 새로운 기능.

- "새로운 AFF A-Series 시스템 및 AI용으로 구축된 스토리지 지원"

  ONTAP 9.15.1은 AI/ML 훈련 및 추론과 같은 차세대 비즈니스 워크로드를 위해 설계된 새로운 고성능 AFF A1K, AFF A90 및 AFF A70 시스템을 지원합니다. 이 새로운 시스템은 기존 AFF A 시리즈 제품보다 최대 2배 더 뛰어난 성능을 제공하고 성능 저하 없이 "상시" 향상된 스토리지 효율성을 제공합니다.

- Windows 백업 애플리케이션 및 서버의 Unix 스타일 심볼릭 링크

  ONTAP 9.15.1부터 symlink가 가리키는 데이터 대신 symlink 자체를 백업하는 옵션도 있습니다. 이를 통해 백업 애플리케이션의 향상된 성능을 비롯한 여러 가지 이점을 얻을 수 있습니다. ONTAP CLI 또는 REST API를 사용하여 이 기능을 사용하도록 설정할 수 있습니다.

- 동적 권한 부여

  ONTAP 9.15.1에는 관리자 계정에서 발급한 명령을 거부하거나 추가 인증을 요구하거나 진행할 수 있도록 허용할지 여부를 결정할 수 있는 보안 기능인 동적 권한 부여를 위한 초기 프레임워크가 도입되었습니다. 시간, 위치, IP 주소, 신뢰할 수 있는 장치 사용, 사용자의 인증 및 권한 부여 내역 등의 요소를 고려하여 사용자 계정의 신뢰 점수를 기준으로 결정됩니다.

- 다중 관리자 검증에 대한 영향 범위 확대

  ONTAP 9.15.1 RC1은 악의적인 내부자로부터 추가적인 보호를 위해 MAV 프레임워크에 100개 이상의 새로운 명령을 추가합니다.

- 클러스터 피어링 등을 위해 TLS 1.3 암호화 지원

  ONTAP 9.15.1에서는 S3 스토리지, FlexCache, SnapMirror 및 클러스터 피어링 암호화에 대한 TLS 1.3 암호화 지원을 소개합니다. FabricPool, Microsoft Azure 페이지 Blob 스토리지 및 SnapMirror Cloud와 같은 애플리케이션에서는 9.15.1 릴리즈에 TLS 1.2를 계속 사용합니다.

- TLS를 통한 SMTP 트래픽 지원

  TLS 지원 기능을 사용하여 이메일을 통해 AutoSupport 데이터를 안전하게 전송합니다.

- 대칭 액티브/액티브 구성을 위한 SnapMirror 액티브 동기식

  이 새로운 기능은 무중단 업무 운영 및 재해 복구를 위한 동기식 양방향 복제 기능을 제공합니다. 여러 장애가 발생한 도메인 전반에서 데이터에 대한 동시 읽기 및 쓰기 액세스를 통해 중요한 SAN 워크로드에 대한 데이터 액세스를 보호하여 무중단 운영을 지원하고 재해 또는 시스템 장애 발생 시 다운타임을 최소화합니다.

- FlexCache 다시 쓰기

  FlexCache write-back을 사용하면 클라이언트가 FlexCache 볼륨에 로컬로 쓸 수 있으므로, 원래 볼륨에 직접 쓸 때보다 지연 시간이 단축되고 성능이 향상됩니다. 새로 작성된 데이터는 원래 볼륨으로 비동기식으로 다시 복제됩니다.

- RDMA를 통한 NFSv3

NFSv3을 통한 RDMA 지원은 TCP를 통해 짧은 지연 시간과 높은 대역폭으로 액세스하여 고성능 요구사항을 해결하는 데 도움이 될 수 있습니다.

ONTAP 9.14.1 주요 내용

ONTAP 9.14.1은 FabricPool, 랜섬웨어 방지 보호, OAuth 등 영역에서 새롭고 향상된 기능을 제공합니다. 새로운 기능 및 향상된 기능의 전체 목록은 를 참조하십시오 ONTAP 9.14.1의 새로운 기능.

- WAFL 예약 감소

  ONTAP 9.14.1은 30TB 이상의 애그리게이트에서 WAFL 예비 공간을 줄임으로써 FAS 및 Cloud Volumes ONTAP 시스템에서 사용 가능한 공간이 5% 증가됩니다.

- FabricPool의 향상된 기능

  FabricPool 은 상승을 제안합니다 읽기 성능 또한 클라우드에 직접 쓸 수 있으므로 콜드 데이터를 더 저렴한 스토리지 계층으로 이동하여 공간 부족 위험을 줄이고 스토리지 비용을 절감할 수 있습니다.

- "OAuth 2.0 지원"

  ONTAP는 OAuth 2.0 프레임워크를 지원하며, System Manager를 사용하여 구성할 수 있습니다. OAuth 2.0을 사용하면 일반 텍스트 스크립트와 Runbook에 사용자 ID와 암호를 생성하거나 노출하지 않고도 자동화 프레임워크용 ONTAP에 안전하게 액세스할 수 있습니다.

- "ARP(자율 랜섬웨어 방어) 개선"

  ARP는 이벤트 보안에 대한 더 많은 제어 권한을 부여하여 경고를 생성하는 조건을 조정하고 오탐의 가능성을 줄일 수 있습니다.

- System Manager의 SnapMirror 재해 복구 예행 연습

  System Manager는 원격 위치에서 재해 복구를 쉽게 테스트하고 테스트 후 정리하는 단순한 워크플로우를 제공합니다. 이 기능을 사용하면 테스트를 더 쉽고 자주 수행할 수 있으며 복구 시간 목표에 대한 신뢰도가 높아집니다.

- S3 오브젝트 잠금 지원

  ONTAP S3는 오브젝트 잠금 API 명령을 지원하므로 S3로 ONTAP에 기록된 데이터가 삭제되지 않도록 보호할 수 있습니다
  표준 S3 API 명령을 사용하여 중요한 데이터를 적절한 시간 동안 보호합니다.

- 클러스터 및 볼륨 태그 지정

  온프레미스에서 클라우드로 이동하고 반대되는 데이터를 따르는 볼륨 및 클러스터에 메타데이터 태그를 추가합니다.

ONTAP 9.13.1 주요 내용

ONTAP 9.13.1은 랜섬웨어 방지, 일관성 그룹, 서비스 품질, 테넌트 용량 관리 등 영역에서 새롭고 향상된 기능을 제공합니다. 새로운 기능 및 향상된 기능의 전체 목록은 를 참조하십시오 ONTAP 9.13.1의 새로운 기능.

- ARP(자율 랜섬웨어 방어) 개선 사항:

- 자동 활성화

  ONTAP 9.13.1을 사용하면 ARP가 학습 데이터가 충분하면 교육에서 생산 모드로 자동 이동하므로 관리자가 30일 후 이를 활성화할 필요가 없습니다.

- 다중 관리자 인증 지원

  ARP disable 명령은 다중 관리자 검증에 의해 지원되기 때문에 단 한 명의 관리자가 ARP를 비활성화하여 데이터를 잠재적인 랜섬웨어 공격에 노출시킬 수 없습니다.

- FlexGroup 지원

  ARP는 ONTAP 9.13.1부터 FlexGroup 볼륨을 지원합니다. ARP는 클러스터의 여러 볼륨 및 노드에 걸쳐 있는 FlexGroup 볼륨을 모니터링하고 보호할 수 있으므로 가장 큰 데이터세트도 ARP로 보호할 수 있습니다.

- System Manager의 일관성 그룹에 대한 성능 및 용량 모니터링

  성능 및 용량 모니터링 기능이 각 일관성 그룹에 자세히 제공되므로 단순히 데이터 개체 수준이 아닌 애플리케이션 수준에서 잠재적 문제를 빠르게 식별하고 보고할 수 있습니다.

- 테넌트 용량 관리

  멀티 테넌트 고객 및 서비스 공급자는 각 SVM에 대한 용량 제한을 설정할 수 있으므로 클러스터에서 하나의 테넌트가 용량을 과도하게 사용하는 위험 없이 셀프 서비스 프로비저닝을 수행할 수 있습니다.

- 서비스 천장과 바닥의 품질

  ONTAP 9.13.1을 사용하면 볼륨, LUN 또는 파일과 같은 오브젝트를 그룹으로 그룹화하고 QoS 상한(최대 IOPS) 또는 바닥(최소 IOPS)을 할당하여 애플리케이션 성능에 대한 기대치를 개선할 수 있습니다.

ONTAP 9.12.1 주요 내용

ONTAP 9.12.1은 보안 강화, 보존, 성능 등의 영역에서 새롭고 향상된 기능을 제공합니다. 새로운 기능 및 향상된 기능의 전체 목록은 를 참조하십시오 ONTAP 9.12.1의 새로운 기능.

- 변조 방지 스냅샷

  SnapLock 기술을 사용하면 소스 또는 대상에서 스냅샷이 삭제되지 않도록 보호할 수 있습니다.

  랜섬웨어 공격자나 악성 관리자가 운영 스토리지와 2차 스토리지의 스냅샷을 삭제하지 못하도록 보호하여 더 많은 복구 지점을 유지합니다.

- ARP(자율 랜섬웨어 방어) 개선

  운영 스토리지에 대해 이미 완료된 선별 모델에 따라 보조 스토리지에서 지능형 자율적 랜섬웨어 보호를 즉시 지원합니다.

  페일오버 후 2차 스토리지에 대한 잠재적 랜섬웨어 공격을 즉시 파악합니다. 영향을 받기 시작한 데이터에 대한 스냅샷이 즉시 생성되며 관리자에게 알림이 전달되므로 공격을 중지하고 복구를 향상시킬 수 있습니다.

- FPolicy를 참조하십시오

ONTAP FPolicy를 한 번의 클릭으로 활성화하여 알려진 악성 파일을 자동으로 차단할 수 있습니다. 활성화 단순화 덕분에 알려진 일반적인 파일 확장명을 사용하는 일반적인 랜섬웨어 공격으로부터 보호할 수 있습니다.

- 보안 강화: 조작 방지 보존 로깅

  손상된 관리자 계정을 손상시키는 ONTAP의 무단 복제 방지 보존 로깅은 악의적인 작업을 숨길 수 없습니다. 시스템 정보 없이는 관리자 및 사용자 기록을 변경하거나 삭제할 수 없습니다.

  출처에 상관없이 모든 관리자 작업을 기록하고 감사하여 데이터에 영향을 미치는 모든 작업이 캡처됩니다. 알림은 관리자에게 변경 사항을 통지하는 과정에서 시스템 감사 로그가 무단으로 변경될 때마다 생성됩니다.

- 보안 강화: 확장된 다단계 인증

  SSH(Multifactor Authentication)를 위한 MFA(Multifactor Authentication)는 Yubikey 물리적 하드웨어 토큰 장치를 지원하므로 공격자가 훔친 자격 증명 또는 손상된 클라이언트 시스템을 사용하여 ONTAP 시스템에 액세스할 수 없습니다. Cisco Duo는 System Manager를 통해 MFA를 지원합니다.

- 파일 오브젝트 이중화(멀티 프로토콜 액세스)

  파일 오브젝트 이중화: 네이티브 S3 프로토콜 읽기 및 쓰기 액세스가 이미 NAS 프로토콜 액세스를 가지고 있는 동일한 데이터 소스에 대해 가능합니다. 동일한 데이터 소스의 파일로 또는 오브젝트로 스토리지를 동시에 액세스할 수 있으므로 오브젝트 데이터를 사용하는 분석과 같이 서로 다른 프로토콜(S3 또는 NAS)에서 사용할 데이터의 중복 복사본이 필요하지 않습니다.

- FlexGroup 재조정

  FlexGroup 구성요소의 균형이 무너지면 에서 운영 중단 없이 FlexGroup를 재조정하여 관리할 수 있습니다 CLI, REST API 및 System Manager와 같은 기능을 사용할 수 있습니다. 최적의 성능을 위해서는 FlexGroup 내의 구성 요소가 사용된 용량을 균등하게 분산해야 합니다.

- 향상된 스토리지 용량

  WAFL 공간 예약이 크게 줄어 애그리게이트당 최대 40TiB의 가용 용량을 제공합니다.

ONTAP 9.11.1 하이라이트

ONTAP 9.11.1은 보안, 보존, 성능 등의 영역에서 새롭고 향상된 기능을 제공합니다. 새로운 기능 및 향상된 기능의 전체 목록은 를 참조하십시오 ONTAP 9.11.1의 새로운 기능.

- 다중 관리 검증

  MAV(다중 관리자 검증)는 업계 최초의 네이티브 검증 방법이므로 스냅샷이나 볼륨 삭제와 같은 민감한 관리 작업에 대해 여러 번의 승인을 받아야 합니다. MAV 구현에 필요한 승인은 악의적인 공격과 실수로 데이터를 변경하는 것을 방지합니다.

- 자율적 랜섬웨어 방어의 개선 사항

  ARP(자율적 랜섬웨어 방어)는 머신 러닝을 사용하여 세분성이 높은 랜섬웨어 위협을 감지하므로, 보안 위협을 빠르게 식별하고 위반이 발생할 경우 복구를 가속화할 수 있습니다.

- FlexGroup 볼륨에 대한 SnapLock 규정 준수

  WORM 파일 잠금으로 데이터를 보호하여 전자 설계 자동화, 미디어 및 엔터테인먼트와 같은 워크로드를 위한 수

페타바이트에 달하는 데이터 세트를 변경 또는 삭제할 수 없도록 보호합니다.

- 비동기식 디렉토리 삭제

  ONTAP 9.11.1을 사용하면 ONTAP 시스템 백그라운드에서 파일 삭제가 수행되므로 대규모 디렉토리를 쉽게 삭제할 수 있을 뿐 아니라 호스트 입출력에 대한 성능 및 지연 시간 영향을 제거할 수 있습니다

- S3 개선

  버킷 수준의 추가 API 엔드포인트 및 오브젝트 버전 관리를 통해 ONTAP로 S3의 오브젝트 데이터 관리 기능을 간소화 및 확장하여 여러 버전의 오브젝트를 동일한 버킷에 저장할 수 있습니다.

- System Manager의 향상된 기능

  System Manager는 스토리지 리소스를 최적화하고 감사 관리를 개선하는 고급 기능을 지원합니다. 이러한 업데이트에는 스토리지 애그리게이트의 관리 및 구성 능력이 향상되고, 시스템 분석에 대한 가시성이 개선되며, FAS 시스템을 위한 하드웨어 시각화가 포함됩니다.

ONTAP 9.10.1 하이라이트

ONTAP 9.10.1은 보안 강화, 성능 분석, NVMe 프로토콜 지원 및 오브젝트 스토리지 백업 옵션 영역에서 새롭고 향상된 기능을 제공합니다. 새로운 기능 및 향상된 기능의 전체 목록은 를 참조하십시오 ONTAP 9.10.1의 새로운 기능.

- 자율 랜섬웨어 보호

  자율적 랜섬웨어 방어는 볼륨의 스냅샷을 자동으로 생성하고 비정상적인 활동이 감지되면 관리자에게 경고하여 랜섬웨어 공격을 신속하게 감지하고 더욱 신속하게 복구할 수 있도록 지원합니다.

- System Manager의 향상된 기능

  System Manager는 Active IQ Digital Advisor (Digital Advisor 라고도 함), NetApp Console 및 인증서 관리와의 새로운 통합을 제공하는 것 외에도 디스크, 셸프, 서비스 프로세서에 대한 펌웨어 업데이트를 자동으로 다운로드합니다. 이러한 개선을 통해 관리가 간소화되고 비즈니스 연속성이 유지됩니다.

- 파일 시스템 분석 기능 향상

  File System Analytics는 추가 원격 측정 기능을 제공하여 파일 공유에서 최상위 파일, 디렉토리 및 사용자를 식별함으로써 워크로드 성능 문제를 식별하여 리소스 계획 및 QoS 구현을 개선할 수 있도록 지원합니다.

- AFF 시스템에 대한 NVMe over TCP(NVMe/TCP) 지원

  기존 이더넷 네트워크에서 NVMe/TCP를 사용할 경우 AFF 시스템에서 엔터프라이즈 SAN과 최신 워크로드의 성능을 높이고 TCO를 절감할 수 있습니다.

- NetApp FAS 시스템에 대한 NVMe/FC(NVMe over Fibre Channel) 지원

  하이브리드 어레이에서 NVMe/FC 프로토콜을 사용하여 NVMe로 균일하게 마이그레이션할 수 있습니다.

- 오브젝트 스토리지용 네이티브 하이브리드 클라우드 백업

  원하는 오브젝트 스토리지 대상을 선택하여 ONTAP S3 데이터를 보호합니다. SnapMirror 복제를 사용하여 StorageGRID를 통해 사내 스토리지, Amazon S3를 지원하는 클라우드 또는 NetApp AFF 및 FAS 시스템의 다른

ONTAP S3 버킷에 백업할 수 있습니다.

- FlexCache을 사용한 글로벌 파일 잠금

  FlexCache를 사용한 글로벌 파일 잠금을 통해 오리진의 소스 파일을 업데이트하는 동안 캐시 위치에서 파일 일관성을 보장합니다. 향상된 기능을 통해 향상된 잠금이 필요한 워크로드에 대해 오리진-캐시 관계에서 파일 읽기 잠금을 독점적으로 사용할 수 있습니다.

ONTAP 9.9.1 주요 내용

ONTAP 9.91.1 은 스토리지 효율성, 다단계 인증, 재해 복구 등 영역에서 새롭고 향상된 기능을 제공합니다. 새로운 기능 및 향상된 기능의 전체 목록은 를 참조하십시오 ONTAP 9.1.1의 새로운 기능.

- CLI 원격 액세스 관리를 위한 보안 강화

  SHA512 및 SSH A512 암호 해싱이 지원되므로 시스템 액세스를 시도하는 악의적인 행위자로부터 관리자 계정 자격 증명을 보호할 수 있습니다.

- "MetroCluster IP 기능 향상: 8노드 클러스터 지원"

  새로운 제한은 이전 한도보다 2배 더 크므로 MetroCluster 구성을 지원하고 지속적인 데이터 가용성을 구현할 수 있습니다.

- SnapMirror 활성 동기화

  NAS 워크로드용 대규모 데이터 컨테이너의 백업 및 재해 복구를 위한 더 많은 복제 옵션을 제공합니다.

- SAN 성능 향상

  VMware 데이터 저장소와 같은 단일 LUN 애플리케이션에 대해 최대 4배 높은 SAN 성능을 제공하므로 SAN 환경에서 고성능을 달성할 수 있습니다.

- 하이브리드 클라우드를 위한 새로운 오브젝트 스토리지 옵션

  StorageGRID를 NetApp Cloud Backup Service의 대상으로 사용하여 온프레미스 ONTAP 데이터의 백업을 단순화하고 자동화할 수 있습니다.

다음 단계

- ONTAP의 최신 버전으로 업그레이드하십시오
- 언제 ONTAP를 업그레이드해야 합니까?

ONTAP 9.18.1의 새로운 기능

ONTAP 9.18.1에서 사용할 수 있는 새로운 기능에 대해 알아보세요.

최신 ONTAP 9 릴리스에서 알려진 문제, 제한 사항 및 업그레이드 주의 사항에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 릴리즈 노트". 릴리스 정보에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

- 새로운 기능 및 향상된 기능에 대해 알아봅니다 "ONTAP MetroCluster 기능".

- 에 대해 알아보세요 "NetApp AFX 스토리지 시스템을 위한 새롭고 향상된 ONTAP 소프트웨어 기능" .
- 에 대해 알아보세요 "NetApp ASA r2 스토리지 시스템을 위한 새롭고 향상된 ONTAP 소프트웨어 기능" .
- 에 대해 알아보세요 "AFF, ASA 및 FAS 시스템과 지원되는 스위치에 대한 새롭고 향상된 지원" .
- 의 업데이트에 대해 알아봅니다 "ONTAP REST API를 참조하십시오".

최신 버전의 ONTAP로 업그레이드하려면 를 참조하십시오"ONTAP 업그레이드를 준비합니다".

데이터 보호

업데이트	설명
MetroCluster FlexGroup 볼륨에 대한 SnapMirror 클라우드 지원	SnapMirror 클라우드는 MetroCluster 구성의 FlexGroup 볼륨에 대한 백업 및 복원 작업을 지원합니다.

네트워킹

업데이트	설명
IPsec 하드웨어 오프로드 IPv6 지원	IPsec 하드웨어 오프로드 지원이 IPv6로 확장되었습니다.
OpenSSL PQC 알고리즘	ONTAP SSL을 위한 포스트퀀텀 컴퓨팅 암호화 알고리즘을 지원합니다. 이러한 알고리즘은 미래의 양자 컴퓨팅 공격에 대한 추가적인 보호 기능을 제공하며, SSL FIPS 모드가 비활성화된 경우 사용할 수 있습니다.
ONTAP 백엔드 클러스터 네트워크 암호화	ONTAP 백엔드 클러스터 네트워크에서 전송 중인 데이터에 대해 TLS 암호화를 활성화할 수 있습니다.
ONTAP HA 트래픽 네트워크 암호화	고가용성(HA) 쌍의 노드 간 트래픽에 대한 암호화를 활성화할 수 있습니다.

산

업데이트	설명
NVMe 복사 오프로드	NVMe 복사 오프로드를 사용하면 NVMe 호스트가 CPU에서 ONTAP 스토리지 컨트롤러의 CPU로 복사 작업을 오프로드할 수 있습니다. 호스트는 애플리케이션 워크로드를 위해 CPU 리소스를 예약하는 동시에 한 NVMe 네임스페이스에서 다른 네임스페이스로 데이터를 복사할 수 있습니다.

S3 오브젝트 스토리지

업데이트	설명
특정 시점 S3 스냅샷 복원 지원	이제 ONTAP CLI를 통해 S3 스냅샷 버킷에 기본적으로 액세스할 수 있습니다. 또한 S3 클라이언트에서 S3 스냅샷으로부터 단일 객체, 객체 집합 또는 전체 버킷을 복원할 수 있습니다.
FlexCache 볼륨에 NAS 버킷 생성 지원	FlexCache 볼륨에 NAS 버킷을 생성할 수 있으며, 클러스터의 모든 노드가 ONTAP 9.18.1 이상을 사용하는 경우 애플리케이션은 S3 프로토콜을 사용하여 FlexCache 볼륨의 데이터에 액세스할 수 있습니다. NAS FlexCache 볼륨에 대한 S3 액세스 활성화에 대한 자세한 내용은 "NAS FlexCache 볼륨에 대한 S3 액세스를 활성화합니다"을 참조하십시오.

보안

업데이트	설명
ARP/AI에 대한 FlexGroup 볼륨 지원	NetApp FlexGroup 볼륨은 ARP/AI를 지원하여 고급 머신 러닝 기반 랜섬웨어 탐지 및 보호 기능을 제공합니다. ONTAP 9.17.1 및 이전 버전에서는 FlexGroup 볼륨에 대해 1세대 ARP만 사용할 수 있었습니다. ONTAP 9.18.1부터 FlexGroup 볼륨은 온프레미스 ONTAP 플랫폼(AFF 및 FAS)과 가상 ONTAP 배포(Cloud Volumes ONTAP 및 ONTAP Select 포함) 모두에서 FlexVol 볼륨과 동등성을 갖습니다. 결과적으로 ARP/AI는 FlexVol 및 FlexGroup 볼륨 모두에 대한 기본 ARP 기술이 됩니다.
지원되는 시스템에서는 새 볼륨에 대해 ARP/AI가 기본적으로 활성화됩니다.	새 클러스터를 생성하거나 클러스터를 9.18.1로 업그레이드하면 12시간의 유예 기간 후 AFF A 시리즈, AFF C 시리즈, ASA 및 "ASA r2" 시스템의 모든 새 볼륨에서 ARP/AI가 기본적으로 자동 활성화됩니다. 이 유예 기간 동안 기본 활성화를 해제할 수 있습니다.

스토리지 리소스 관리 기능 향상

업데이트	설명
SVM 및 볼륨에서 2단계 중첩 QoS 정책 그룹 지원	SVM과 SVM 아래의 볼륨에 동시에 QoS 정책을 할당할 수 있습니다.
SVM-DR 관계에서 원본 볼륨의 SVM FlexCache 볼륨을 생성합니다.	SVM-DR 관계의 일부인 원본 볼륨의 SVM FlexCache 볼륨을 생성할 수 있습니다.

업데이트	설명
공간 사용 정보를 표시하는 명령입니다	ONTAP 9.18.1 이상에서는 `storage aggregate show-space` 명령이 논리적 참조 용량 및 논리적 미참조 용량 보고 방식을 변경합니다. 논리적 참조 용량은 모든 객체의 참조된 블록과 조각화된 객체의 미참조 블록을 보고합니다. 논리적 미참조 용량은 충만도 임계값을 초과하고 객체 삭제 및 조각 모음 대상인 객체의 미참조 블록만 보고합니다. 예를 들어 ONTAP S3 및 StorageGRID에 대해 기본 애그리게이트 충만도 임계값 40%를 사용하는 경우 객체의 블록 중 60%가 참조되지 않아야 블록이 참조되지 않은 용량으로 보고됩니다. ONTAP 9.18.1 이전 릴리스에서는 논리적 참조 용량이 모든 객체(전체 객체 및 조각화된 객체 모두)의 참조된 블록을 보고합니다. 논리적 미참조 용량은 모든 객체의 미참조 블록을 보고합니다.

ONTAP 9.17.1의 새로운 기능

ONTAP 9.17.1에서 사용할 수 있는 새로운 기능에 대해 알아보세요.

최신 ONTAP 9 릴리스에서 알려진 문제, 제한 사항 및 업그레이드 주의 사항에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 릴리즈 노트". 릴리스 정보에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

- 새로운 기능 및 향상된 기능에 대해 알아봅니다 "ONTAP MetroCluster 기능".
- 에 대해 알아보세요 "NetApp AFX 스토리지 시스템을 위한 새롭고 향상된 ONTAP 소프트웨어 기능" .
- 에 대해 알아보세요 "NetApp ASA r2 스토리지 시스템을 위한 새롭고 향상된 ONTAP 소프트웨어 기능" .
- 에 대해 알아보세요 "AFF, ASA 및 FAS 시스템과 지원되는 스위치에 대한 새롭고 향상된 지원" .
- 의 업데이트에 대해 알아봅니다 "ONTAP REST API를 참조하십시오".

최신 버전의 ONTAP로 업그레이드하려면 를 참조하십시오"ONTAP 업그레이드를 준비합니다".

데이터 보호

업데이트	설명
NVMe를 통한 호스트 액세스를 위한 SnapMirror 활성 동기화 지원	SnapMirror Active Sync는 NVMe/TCP를 사용하는 VMware 워크로드에 대한 NVMe 액세스 지원과 2노드 ONTAP 클러스터에 대한 NVMe/FC 호스트 액세스를 추가합니다. VMware 워크로드의 NVMe/TCP 지원은 VMware 버그가 해결되어야 가능합니다.
SnapMirror Active Sync를 통한 ONTAP Cloud Mediator 지원	ONTAP Cloud Mediator는 ONTAP 9.17.1에 도입되었으며 SnapMirror 액티브 동기화 관계를 지원합니다. ONTAP Mediator와 마찬가지로 클라우드 기반 Mediator는 SnapMirror 액티브 동기화 관계에 대한 쿼럼 감시 역할을 하여 투명한 장애 조치를 보장하는 동시에 제3자 사이트 유지 관리의 운영 복잡성을 줄여줍니다.

S3 오브젝트 스토리지

업데이트	설명
ONTAP S3 NAS 버킷의 CopyObject 작업 지원	CopyObject 작업은 ONTAP S3 NAS 버킷 내에서 지원됩니다.
S3 NAS 버킷을 연결 경로에 연결하기 위한 지원	ONTAP CLI를 사용하여 S3 NAS 버킷을 생성할 때, 버킷을 연결 경로 대신 볼륨에 연결하도록 선택할 수 있습니다. 볼륨에 연결하면 볼륨이 마운트 해제되거나 마운트되는 등 경로가 변경되면 연결 경로가 자동으로 업데이트됩니다.
태그 지정 및 메타데이터를 위한 S3 다중 프로토콜 지원	태그 지정 및 사용자 메타데이터 키/값 쌍은 다중 프로토콜(S3 및 NAS) 환경에서 CreateMultipartUpload 작업에서 지원됩니다.

보안

업데이트	설명
자율형 랜섬웨어 보호 스냅샷 업데이트	ONTAP ARP 스냅샷에 대한 몇 가지 업데이트를 도입했습니다.
HTTP Strict Transport Security(HSTS) 지원	ONTAP 웹 서비스에 대해 HTTP Strict Transport Security를 지원하여 사용자 브라우저와 ONTAP 간의 안전한 HTTPS 통신을 시행할 수 있습니다.
링크 집계 그룹을 통한 IPsec 하드웨어 오프로드	ONTAP 9.16.1에서 도입된 하드웨어 오프로드 지원을 확장하여 링크 집계 그룹에 대한 IPsec 하드웨어 오프로드를 지원합니다.
IPsec 포스트퀀텀 사전 공유 키 지원	ONTAP 미래의 양자 컴퓨터 공격으로부터 보호하기 위해 IPsec에 대한 포스트퀀텀 사전 공유 키를 지원합니다.
OpenStack Barbican 키 관리자 지원	ONTAP NetApp 볼륨 암호화(NVE) 키에 대한 OpenStack의 Barbican 키 관리자를 지원합니다.
JIT(Just in Time) 권한 승격 지원	ONTAP 역할 기반 액세스 제어(RBAC)를 위한 JIT 권한 승격을 지원합니다. 사용자는 구성된 역할에 대한 임시 권한 승격을 요청하여 필요에 따라 권한이 부여된 명령에 액세스할 수 있습니다. 클러스터 관리자는 JIT 권한 승격에 액세스할 수 있는 사용자, 액세스 허용 시점 및 기간을 설정할 수 있습니다.
SAML 인증을 위한 Entra IdP 및 IdP 그룹 지원 지원	ONTAP SAML ID 공급자로 Microsoft Entra를 지원합니다. 또한 IdP에서 제공하는 그룹 정보를 ONTAP 역할에 매핑할 수 있습니다.
클러스터 간 요청 감사	시작 소스 클러스터와 대상(실행) 클러스터 모두에서 감사 작업을 구성하고 실행할 수 있습니다. 이전 릴리스에서는 클라이언트 요청을 수신하는 클러스터에서만 감사를 수행했습니다. 이 기능을 사용하면 클러스터 간 요청을 처리하는 피어링된 클러스터도 해당 활동을 로깅합니다. 이러한 감사 작업은 ONTAP 내에서 시작된 모든 SET 또는 GET 요청으로 활성화 및 확장될 수 있습니다.

업데이트	설명
자율형 랜섬웨어 보호를 통한 SAN 지원	ARP는 암호화 기반 이상 탐지 기능을 갖춘 SAN 볼륨을 지원하고, 상세한 엔트로피 통계를 위한 새로운 명령을 도입하며, 이전에 NAS에 집중되었던 System Manager의 랜섬웨어 보호 메시징 기능을 통합합니다. 구성 가능한 탐지 임계값과 더욱 확정적인 스냅샷 보존 기능은 다양한 워크로드에 대한 유연성을 높여줍니다.

스토리지 리소스 관리 기능 향상

업데이트	설명
새 볼륨에 대해 기본적으로 FSA가 활성화됨	NAS 프로토콜에 할당된 ONTAP 클러스터에서 새로 생성된 SVM에 생성된 볼륨에는 기본적으로 파일 시스템 분석(FSA)이 활성화되어 있습니다. FSA는 볼륨이 생성되는 즉시 자동으로 활성화되어 추가 구성 없이 즉각적인 분석 기능을 제공합니다.
FlexGroup 볼륨에서 직접 삭제 진행 상황을 보기 위한 향상된 지원	ONTAP CLI 명령 `volume file async-delete show` 클라이언트에서 실행된 비동기 삭제 작업을 포함하도록 향상되었습니다.

ONTAP 9.16.1의 새로운 기능

ONTAP 9.16.1에서 사용 가능한 새로운 기능에 대해 알아보십시오.

최신 ONTAP 9 릴리스에서 알려진 문제, 제한 사항 및 업그레이드 주의 사항에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 릴리즈 노트". 릴리스 정보에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

- 새로운 기능 및 향상된 기능에 대해 알아봅니다 "ONTAP MetroCluster 기능".
- 에 대해 알아보세요 "NetApp ASA r2 스토리지 시스템을 위한 새롭고 향상된 ONTAP 소프트웨어 기능" .
- 에 대해 알아보세요 "AFF, ASA 및 FAS 시스템과 지원되는 스위치에 대한 새롭고 향상된 지원" .
- 의 업데이트에 대해 알아봅니다 "ONTAP REST API를 참조하십시오".

최신 버전의 ONTAP로 업그레이드하려면 를 참조하십시오"ONTAP 업그레이드를 준비합니다".

데이터 보호

업데이트	설명
SnapMirror 액티브 동기화에 대한 다중 노드 지원	이전의 2노드 제한에서 확장된 SnapMirror 액티브 동기화는 4노드 클러스터를 지원하므로 대규모 워크로드를 위한 데이터 복제가 가능합니다.
팬아웃 관계를 구축하기 위한 SnapMirror 클라우드 지원	SnapMirror 클라우드는 동일한 소스 볼륨 또는 FlexGroup에서 두 개의 서로 다른 오브젝트 저장소로 팬아웃 관계를 지원합니다. 팬아웃은 두 개의 오브젝트 저장소와 오브젝트 저장소의 한 개 또는 두 개의 버킷으로 구성될 수 있습니다.

업데이트	설명
마이그레이션된 볼륨에서 SnapMirror 클라우드 백업 지원	SnapMirror 클라우드는 기존 ONTAP REST API를 사용하여 클라우드로 마이그레이션된 볼륨을 백업할 수 있습니다. 새로운 기능은 기준 변경 작업을 수행할 필요 없이 클라우드의 마이그레이션된 볼륨에서 동일한 대상 오브젝트 저장소 엔드포인트로 SnapMirror 클라우드 백업을 지원합니다. FlexVol 볼륨과 FlexGroup 볼륨이 모두 지원됩니다.

네트워킹

업데이트	설명
BGP 피어 그룹에 대한 MD5 인증 지원	ONTAP는 BGP 피어 그룹에서 MD5 인증을 지원하여 BGP 세션을 보호합니다. MD5를 사용하면 승인된 피어 사이에서만 BGP 세션을 설정 및 처리할 수 있으므로 공격자가 BGP 업데이트를 스푸핑하여 네트워크에 잘못된 라우팅 정보를 주입하려는 경로 하이재킹과 같은 공격을 방지할 수 있습니다.
IPsec 하드웨어 오프로드 지원	IP 보안(IPsec)은 클라이언트와 ONTAP 노드 간의 모든 IP 트래픽을 보호하는 데 사용할 수 있는 이동 중인 데이터 보안 옵션입니다. 이 프로토콜은 처음에 ONTAP 9 .8에서 사용할 수 있었으며 소프트웨어로만 구현되었습니다. ONTAP 9.16.1부터 암호화 및 무결성 검사와 같은 계산 집약적인 특정 작업을 스토리지 노드에 설치된 지원되는 NIC(Network Interface Controller) 카드로 오프로드할 수 있습니다. 이 하드웨어 오프로드 옵션을 사용하면 IPsec으로 보호되는 네트워크 트래픽의 성능과 처리량을 크게 향상시킬 수 있습니다.

S3 오브젝트 스토리지

업데이트	설명
S3 오브젝트 메타데이터 및 태깅을 위한 멀티프로토콜 S3 버킷 지원	ONTAP 9.16.1부터 S3 오브젝트 태깅은 비멀티프로토콜 ONTAP S3 버킷에서 NAS 및 S3 멀티프로토콜 ONTAP S3 버킷으로 확장됩니다. 태그는 S3 프로토콜에서만 표시됩니다. S3 클라이언트를 사용하여 S3 오브젝트에 적용함으로써 "태그 및 메타데이터" ONTAP에 오브젝트 또는 파일로 저장된 데이터에서 라이프사이클, 비용 청구, 데이터 범주 및 사용자 지정 워크플로우를 정의하는 데 도움이 됩니다. Bedrock 또는 Athena와 같은 AWS 데이터 서비스와 통합할 경우 태그 및 메타데이터가 이 서비스에서 제공하는 Data Processing의 핵심이 됩니다. 네이티브 S3 버킷에서 태그 및 사용자 정의 메타데이터에 대한 지원은 ONTAP 9.9.1부터 시작되었습니다.
멀티프로토콜 S3 버킷은 다중 부분 업로드를 지원합니다	멀티 파트 업로드는 처음부터 멀티프로토콜 ONTAP S3 버킷이 지원되던 핵심 S3 기능입니다. ONTAP 9.16.1부터 이 핵심 기능은 NAS 및 S3 멀티프로토콜 ONTAP S3 버킷으로 확장됩니다.

업데이트	설명
ONTAP S3 버킷에 대한 CORS(Cross-Origin Resource Sharing) 지원	CORS(Cross-Origin Resource Sharing)로 웹 애플리케이션의 잠재력을 최대한 활용하십시오. CORS를 사용하면 한 도메인의 클라이언트 응용 프로그램과 다른 도메인의 리소스 간에 원활한 상호 작용이 가능합니다. CORS 지원을 통합하면 리소스에 대한 선택적 교차 오리진 액세스를 통해 ONTAP S3 기반 웹 애플리케이션의 역량을 강화할 수 있습니다.
ONTAP는 ONTAP S3 버킷의 스냅샷 생성을 지원합니다	ONTAP S3 버킷의 읽기 전용 시점 스냅샷을 생성할 수 있습니다. S3 스냅샷 기능을 사용하면 스냅샷을 수동으로 생성하거나 스냅샷 정책을 통해 스냅샷을 자동으로 생성할 수 있습니다. 또한, S3 스냅샷을 확인, 탐색, 삭제하고, S3 클라이언트를 통해 스냅샷 콘텐츠를 복원할 수 있습니다.

산

업데이트	설명
NVMe 공간 할당 취소가 기본적으로 활성화되어 있습니다	NVMe 네임스페이스의 경우 공간 할당 해제("홀 펀칭" 및 "언맵"이라고도 함)가 기본적으로 활성화되어 있습니다. 공간 할당 해제를 통해 호스트는 네임스페이스에서 사용되지 않은 블록을 할당 해제하여 공간을 회수할 수 있습니다. 이를 통해 전반적인 저장 효율성이 크게 향상되며, 특히 데이터 회전율이 높은 파일 시스템의 경우 더욱 그렇습니다.

보안

업데이트	설명
다중 관리자 확인을 위해 확장된 규칙 보호 명령 집합입니다	관리자는 다중 관리자 검증 규칙을 생성하여 작업 생성, 삭제 및 수정, 일관성 그룹 스냅샷 생성 및 삭제, 기타 명령 등 일관성 그룹을 보호할 수 있습니다.
AI 개선(ARP/AI)을 통한 자율적 랜섬웨어 방어	ARP는 새로운 AI 기능으로 업그레이드되어 99%의 정밀도와 리콜로 랜섬웨어 공격을 감지하고 이에 대응할 수 있습니다. AI는 포괄적인 데이터 세트에서 훈련되기 때문에 FlexVol 볼륨에서 실행되는 ARP에 대한 학습 기간이 더 이상 없으며 ARP/AI가 즉시 활성 모드에서 시작됩니다. ARP/AI에는 최신 위협에 대한 지속적인 보호 및 복원력을 보장하는 자동 업데이트 기능도 포함되어 있습니다. ARP/AI 기능은 현재 NAS만 지원합니다. 자동 업데이트 기능은 System Manager에서 배포할 새 보안 파일의 가용성을 표시하지만 이러한 업데이트는 NAS 워크로드 보호에만 적용됩니다.
TLS를 통한 NVMe/TCP 1.3	IPSec에 비해 간소화된 구성과 향상된 성능으로 프로토콜 계층에서 NVMe/TCP를 "유선"으로 보호합니다.
FabricPool 개체 저장소 통신을 위한 TLS 1.3 지원	ONTAP는 FabricPool 개체 저장소 통신에 TLS 1.3을 지원합니다.

업데이트	설명
Microsoft Entra ID용 OAuth 2.0	ONTAP 9.14.1에서 처음 도입된 OAuth 2.0 지원은 Microsoft Entra ID 인증 서버(이전의 Azure AD)를 지원하는 데 있어 표준 OAuth 2.0 클레임이 추가되었습니다. 또한 UUID 스타일 값에 기반한 Entra ID 표준 그룹 클레임은 새로운 그룹 및 역할 매핑 기능을 통해 지원됩니다. Entra ID로 테스트되었지만 지원되는 인증 서버에서 사용할 수 있는 새로운 외부 역할 매핑 기능도 도입되었습니다.

스토리지 효율성

업데이트	설명
지연 시간 메트릭 및 기간별 통계를 포함하도록 qtree 성능 모니터링을 확장했습니다	이전 ONTAP 릴리즈에서는 초당 I/O 작업, 읽기/쓰기 등 다양한 범주에서 처리 성능을 비롯한 qtree 사용을 위한 강력한 실시간 메트릭을 제공합니다. ONTAP 9.16.1부터 실시간 지연 시간 통계에 액세스하고 보관된 기록 데이터를 볼 수도 있습니다. 이러한 새로운 기능을 통해 IT 스토리지 관리자는 시스템 성능에 대한 보다 정확한 통찰력을 얻고 장기간에 걸친 추세를 분석할 수 있습니다. 이를 통해 데이터 센터 및 클라우드 스토리지 리소스의 운영 및 계획과 관련하여 정보에 입각한 의사 결정을 내릴 수 있습니다.

스토리지 리소스 관리 기능 향상

업데이트	설명
스토리지 제한이 설정된 SVM에서 데이터 보호 볼륨 지원	스토리지 제한이 설정된 SVM은 데이터 보호 볼륨을 포함할 수 있습니다. 계단식 배열, 동기식 재해 복구 관계 및 복원 관계가 없는 비동기식 재해 복구 관계의 FlexVol 볼륨이 지원됩니다. ONTAP 9.15.1 및 이전 릴리즈에서는 데이터 보호 볼륨, SnapMirror 관계 볼륨 또는 MetroCluster 구성을 포함하는 모든 SVM에 대해 스토리지 한도를 구성할 수 없습니다.
FlexGroup 고급 용량 배포 지원	고급 용량 균형 조정을 사용하면 매우 큰 파일이 확장되어 구성원 볼륨 한 개에 있는 공간을 사용할 때 FlexGroup 구성원 볼륨 간에 파일 내의 데이터를 분산할 수 있습니다.
MetroCluster 구성 마이그레이션에 대한 SVM 데이터 이동성 지원	ONTAP은 다음 MetroCluster SVM 마이그레이션을 지원합니다. • 비 MetroCluster 구성과 MetroCluster IP 구성 간에 SVM 마이그레이션 • 2개의 MetroCluster IP 구성 간에 SVM 마이그레이션 • MetroCluster FC 구성에서 MetroCluster IP 구성으로 SVM 마이그레이션

시스템 관리자

업데이트	설명
System Manager에서 피싱 방지 WebAuthn 다중 요소 인증 지원	ONTAP 9.16.1은 WebAuthn MFA 로그인을 지원하므로 System Manager에 로그인할 때 하드웨어 보안 키를 두 번째 인증 방법으로 사용할 수 있습니다.

ONTAP 9.15.1의 새로운 기능

ONTAP 9.15.1에서 사용할 수 있는 새로운 기능에 대해 알아봅니다.

최신 ONTAP 9 릴리스에서 알려진 문제, 제한 사항 및 업그레이드 주의 사항에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 릴리즈 노트". 릴리스 정보에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

- 새로운 기능 및 향상된 기능에 대해 알아봅니다 "ONTAP MetroCluster 기능".
- 에 대해 알아보세요 "AFF, ASA 및 FAS 시스템과 지원되는 스위치에 대한 새롭고 향상된 지원" .
- 의 업데이트에 대해 알아봅니다 "ONTAP REST API를 참조하십시오".

최신 버전의 ONTAP로 업그레이드하려면 를 참조하십시오"ONTAP 업그레이드를 준비합니다".

데이터 보호

업데이트	설명
Windows 백업 애플리케이션 및 서버의 Unix 스타일 심볼릭 링크	Windows 백업 응용 프로그램에서 Unix 스타일의 심볼 링크(symlink)를 발견하면 링크가 따라가고 실제 데이터가 ONTAP에 의해 반환되고 백업됩니다. ONTAP 9.15.1부터 symlink가 가리키는 데이터 대신 symlink 자체를 백업하는 옵션도 있습니다. 이를 통해 백업 애플리케이션의 향상된 성능을 비롯한 여러 가지 이점을 얻을 수 있습니다. ONTAP CLI 또는 REST API를 사용하여 이 기능을 사용하도록 설정할 수 있습니다.
SnapMirror 액티브 동기화는 대칭 액티브/액티브 구축을 지원합니다	이제 SnapMirror Active Sync(이전의 SnapMirror Business Continuity)가 대칭 액티브/액티브 구축을 지원하므로 양방향 동기식 복제를 통해 보호된 LUN의 두 복사본에서 읽기 및 쓰기 I/O 작업을 수행할 수 있습니다.
SnapMirror 비동기식을 사용하는 일관성 그룹의 볼륨 제한이 증가했습니다	SnapMirror의 비동기식 보호를 사용하는 일관성 그룹이 이제 일관성 그룹에서 최대 80개의 볼륨을 지원합니다.
일관성 그룹을 통한 REST API 및 CLI 작업에 대한 관리자 권한 수준 지원	일관성 그룹을 위한 CLI 및 REST API 작업이 관리 권한 수준에서 지원됩니다.
Windows Server 페일오버 클러스터링을 사용하는 VMware 가상 볼륨에 대한 영구 예약	ONTAP은 현재 VMware 가상 볼륨(VVol)과 기존 LUN과의 영구 예약을 지원합니다. ONTAP 9.15.1부터 VVOL을 통해 영구 예약을 생성할 수도 있습니다. 이 기능에 대한 지원은 VMware vSphere 9용 ONTAP 툴에 구현되어 있습니다. 클러스터된 Windows 가상 머신 그룹인 WSFC(Windows Server Failover Cluster)에서만 지원됩니다.

보안

업데이트	설명
단순화된 FPolicy 영구 저장소 생성 및 구성	를 사용하여 FPolicy 영구 저장소를 생성하고 볼륨 생성 및 구성을 동시에 자동화할 수 있습니다 `persistent-store create` 명령. 향상됨 `persistent-store create` 또한 명령을 실행하면 자동 크기 조정 모드 매개 변수를 사용할 수 있으므로 사용된 공간의 양에 따라 볼륨이 증가 또는 축소됩니다.
RDMA에서 NFSv3 지원	이제 NFS over RDMA 구성이 NFSv3을 지원합니다.
FPolicy는 NFS 4.1 프로토콜을 지원합니다	FPolicy는 NFS 4.1 프로토콜을 지원합니다.
FPolicy에 대한 Protobuf 엔진 형식 지원	Protobuf는 구조화된 데이터를 serialize하는 Google의 언어 중립적 메커니즘입니다. XML에 비해 더 작고 빠르며 간단하여 FPolicy 성능을 개선하는 데 도움이 됩니다. protubuf 외부 엔진 형식을 사용할 수 있습니다. protobuf로 설정하면 Google Protobuf를 사용하여 알림 메시지가 바이너리 형태로 인코딩됩니다. 외부 엔진 형식을 protobuf로 설정하기 전에 FPolicy 서버가 prototbuf deserialization도 지원하는지 확인하십시오.
SSH 연결에 대한 동적 인증	ONTAP 9.15.1은 관리자 사용자에게 보안 신뢰 점수를 할당하고 의심스러운 활동이 있을 때 추가 인증 검사를 통해 ONTAP 시스템 관리를 위한 보안 강화 기능을 제공하는 동적 권한 부여에 대한 초기 프레임워크를 제공합니다. 동적 권한 부여를 데이터 중심의 제로 트러스트 보안 아키텍처의 일부로 활용할 수 있습니다.
S3 스토리지, FlexCache 및 클러스터 피어링 암호화를 위해 TLS 1.3 지원	TLS 1.3은 ONTAP 9.11.1 이후로 관리 액세스를 위해 지원되었지만, 현재 S3 스토리지, FlexCache 및 클러스터 피어링 암호화에 대해 ONTAP 9.15.1에서 지원됩니다. FabricPool, Microsoft Azure 페이지 Blob 스토리지 및 SnapMirror Cloud와 같은 일부 애플리케이션은 9.15.1 릴리즈에 TLS 1.2를 사용하는 것으로 계속 제한됩니다.
다중 관리자 확인을 위해 확장된 규칙 보호 명령 집합입니다	관리자는 다중 관리자 검증 규칙을 생성하여 클러스터 구성, LUN 삭제, 시스템 구성, IPsec 및 SAML을 위한 보안 구성, 볼륨 스냅샷 작업, SVM 구성 및 기타 명령을 보호할 수 있습니다.
TLS와 함께 SMTP를 사용하여 AutoSupport 메시지 배달	AutoSupport 메시지를 NetApp로 전송하는 것이 HTTPS이지만 암호화되지 않은 SMTP도 사용할 수 있습니다. ONTAP 9.15.1을 사용하는 고객은 이제 SMTP와 함께 TLS를 사용할 수 있습니다. SMTPS 프로토콜은 이메일 트래픽과 선택적 이메일 서버 자격 증명을 암호화하여 보안 전송 채널을 설정합니다. 명시적 TLS가 사용되므로 TCP 연결이 생성된 후 TLS가 활성화됩니다. 메시지의 복사본을 로컬 이메일 주소로 보내는 경우 동일한 구성이 사용됩니다.

스토리지 효율성

업데이트	설명
볼륨 공간 메트릭 보고에 대한 변경 사항	사용 중인 메타데이터만 표시하는 새로운 카운터가 두 개 도입되었습니다. 또한 메타데이터를 제거하고 사용자 데이터만 표시하도록 기존 카운터 중 일부를 조정했습니다. 이러한 변경 사항을 함께 사용하면 두 가지 유형의 데이터로 구분된 메트릭을 보다 명확하게 확인할 수 있습니다. 고객은 이러한 카운터를 사용하여 전체 메타데이터의 할인을 줄이고 실제 사용자 데이터만 고려하여 보다 정확한 차지백 모델을 구현할 수 있습니다.
CPU 또는 전용 오프로드 프로세서를 통한 스토리지 효율성	ONTAP은 AFF A70, AFF A90 및 AFF A1K 플랫폼을 기반으로 스토리지 효율성 및 데이터 컴팩션을 제공합니다. 플랫폼에 따라 주 CPU 또는 전용 오프로드 프로세서를 사용하여 압축이 수행됩니다. 스토리지 효율성이 자동으로 활성화되며 구성이 필요하지 않습니다.

스토리지 리소스 관리 기능 향상

업데이트	설명
FlexCache write-back 지원	캐시 볼륨에 쓰기 작업이 설정되어 있으면 쓰기 요청이 원본 볼륨이 아닌 로컬 캐시로 전송되어 에지 컴퓨팅 환경과 쓰기 작업이 많은 캐시가 더 나은 성능을 제공합니다.
파일 시스템 분석 성능 향상	ONTAP는 파일 시스템 분석을 활성화할 때 볼륨 용량의 5~8%를 가용 용량으로 유지해야 하므로 볼륨 및 파일 시스템 분석 시 잠재적인 성능 문제가 완화됩니다.
FlexClone 볼륨 암호화 키	FlexClone 볼륨에는 FlexVol 볼륨(호스트) 암호화 키와 무관한 전용 암호화 키가 할당됩니다.

시스템 관리자

업데이트	설명
SnapLock 볼트 관계 구성을 위한 System Manager 지원	원본과 대상 모두 ONTAP 9.15.1 이상을 실행 중인 경우 시스템 관리자를 사용하여 SnapLock 볼트 관계를 구성할 수 있습니다.
System Manager 대시보드 성능이 향상되었습니다	System Manager 대시보드의 상태, 용량, 네트워크, 성능 뷰에 대한 정보에는 지연 시간 또는 성능 문제를 식별하고 해결하는 데 도움이 되는 성능 메트릭에 대한 향상된 기능을 비롯하여 더 자세한 설명이 포함되어 있습니다.

업그레이드

업데이트	설명
자동화된 무중단 업그레이드 중에 LIF를 HA 파트너 노드로 마이그레이션할 수 있습니다	무중단 자동 업그레이드 중에 LIF가 다른 배치 그룹으로 마이그레이션되면 LIF는 같은 배치 그룹의 HA 파트너 노드로 마이그레이션됩니다.

ONTAP 9.14.1의 새로운 기능

ONTAP 9.14.1에서 사용할 수 있는 새로운 기능에 대해 알아보십시오.

최신 ONTAP 9 릴리스에서 알려진 문제, 제한 사항 및 업그레이드 주의 사항에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 릴리즈 노트". 릴리스 정보에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

- 새로운 기능 및 향상된 기능에 대해 알아봅니다 "ONTAP MetroCluster 기능".
- 에 대해 알아보세요 "AFF, ASA 및 FAS 시스템과 지원되는 스위치에 대한 새롭고 향상된 지원" .
- 의 업데이트에 대해 알아봅니다 "ONTAP REST API를 참조하십시오".

최신 버전의 ONTAP로 업그레이드하려면 를 참조하십시오ONTAP 업그레이드를 준비합니다.

데이터 보호

업데이트	설명
SVM 루트 볼륨에서 NVE 지원	NetApp 볼륨 암호화가 있는 고유 키를 사용하여 SVM 루트 볼륨을 암호화할 수 있습니다.
장기 보존 스냅샷에 대한 스냅샷 잠금을 설정할 수 있습니다 및 규정 준수 시계를 다시 초기화하려면	SnapLock 라이센스가 있는 클러스터에서 장기 보존이 가능한 스냅샷에 대한 무단 스냅샷 잠금을 SnapLock SnapMirror가 아닌 대상 볼륨에 생성된 스냅샷에 대해 설정할 수 있으며 SnapLock 볼륨이 없는 경우 규정 준수 클록을 초기화할 수 있습니다.
SnapMirror 활성 동기화는 SCIS3 영구 예약 및 Windows 페일오버 클러스터링을 지원합니다	SCSI3 영구 예약 및 Window Failover Clustering for SnapMirror Active Sync는 여러 노드를 장치에 액세스하는 동시에 다른 노드에 대한 액세스를 차단하므로 서로 다른 애플리케이션 환경에 대한 클러스터링이 일관적이고 안정적으로 유지됩니다.
볼륨 세분화 스냅샷을 일관성 그룹으로 복사합니다	정합성 보장 그룹을 활용하여 비동기식 SnapMirror 스냅샷 및 볼륨 세분화 스냅샷을 대상 정합성 보장 그룹에 복제하여 추가 재해 복구 계층을 수행할 수 있습니다.
SVM 재해 복구 관계 내 일관성 그룹을 위한 비동기식 데이터 보호 지원	SVM 재해 복구용으로 구성된 SVM은 SVM에 일관성 그룹이 포함된 경우 일관성 그룹 정보를 2차 사이트로 복제할 수 있습니다.
"20개의 팬아웃 타겟에 대한 SnapMirror 비동기 지원"	ONTAP 9.14.1을 사용할 경우 A700 이상 시스템에서 지원되는 SnapMirror 비동기식 팬아웃 타겟의 수가 16개에서 20개로 증가합니다.
암호화된 소스에서 암호화되지 않은 캐시 생성	ONTAP 9.14.0부터 FlexCache는 암호화된 소스에서 암호화되지 않은 FlexCache 볼륨 생성을 지원합니다. 이전 ONTAP 버전에서는 캐시 소스가 암호화되었을 때 FlexCache 생성이 실패했습니다.
일관성 그룹에 대한 CLI 지원	ONTAP CLI를 사용하여 일관성 그룹을 관리합니다.

파일 액세스 프로토콜

업데이트	설명
NFSv4.1 세션 트렁킹	세션 트렁킹은 내보낸 데이터 저장소에 대한 여러 경로를 허용합니다. 따라서 관리가 간소화되고 워크로드 확장에 따른 성능이 향상됩니다. 특히 VMware 워크로드가 있는 환경에서 적합합니다.

S3 오브젝트 스토리지

업데이트	설명
S3 FlexGroup 볼륨에서 자동 크기 조정을 사용하여 버킷이 생성되었을 때 과도한 용량 할당을 제거했습니다	신규 또는 기존 FlexGroup 볼륨에 버킷이 생성되거나 삭제되면 필요한 최소 크기로 볼륨 크기가 조정됩니다. 필요한 최소 크기는 FlexGroup 볼륨에 있는 모든 S3 버킷의 총 크기입니다.
미러링된 및 미러링되지 않은 애그리게이트에서 S3 오브젝트 스토리지 지원	MetroCluster IP 및 FC 구성의 경우, 미러링되거나 미러링되지 않은 애그리게이트의 SVM에서 S3 오브젝트 스토리지 서버를 사용하도록 설정할 수 있습니다.
사용자 역할 및 잠금 보존 기간을 기반으로 하는 개체 잠금	S3 버킷의 오브젝트를 덮어쓰지 않거나 삭제하지 못하도록 잠글 수 있습니다. 개체를 잠그는 기능은 특정 사용자 또는 시간을 기반으로 합니다.
외부 디렉토리 서비스를 지원하도록 LDAP 사용자 그룹에 대한 액세스를 구성하고 액세스 및 비밀 키에 대한 유효 기간을 추가합니다	ONTAP 관리자는 LDAP(Lightweight Directory Access Protocol) 또는 Active Directory 사용자 그룹에 대한 액세스를 ONTAP S3 오브젝트 스토리지에 구성할 수 있으며 LDAP 빠른 바인드 모드에서 인증을 활성화할 수 있습니다. 로컬 또는 도메인 그룹 또는 LDAP 그룹의 사용자는 S3 클라이언트에 대한 자체 액세스 및 보안 키를 생성할 수 있습니다. S3 사용자의 액세스 키 및 비밀 키에 대한 유효 기간을 정의할 수 있습니다. ONTAP는 과 같은 변수를 지원합니다 `$aws:username` 버킷 정책 및 그룹 정책에 사용됩니다.

산

업데이트	설명
NVMe/TCP 자동 호스트 검색	NVMe/TCP 프로토콜을 사용하여 컨트롤러에 대한 호스트 검색은 기본적으로 자동화되어 있습니다.
NVMe/FC 호스트 측 보고 및 문제 해결	기본적으로 ONTAP는 NVMe/FC 호스트의 기능을 지원하여 고유 식별자로 가상 머신을 식별하고 NVMe/FC 호스트에서 가상 머신 리소스 활용률을 모니터링할 수 있도록 합니다. 또한 호스트측 보고 및 문제 해결이 향상됩니다.
NVMe 호스트 우선순위 지정	특정 호스트에 대한 리소스 할당의 우선순위를 지정하도록 NVMe 서브시스템을 구성할 수 있습니다. 높은 우선 순위가 할당된 호스트는 더 큰 입출력 대기열 수와 더 큰 대기열 깊이를 할당합니다.

보안

업데이트	설명
SSH 사용자를 위한 Cisco Duo 다단계 인증 지원	SSH 사용자는 로그인 중에 Cisco Duo를 두 번째 인증 요소로 사용하여 인증할 수 있습니다.

업데이트	설명
"OAuth 2.0 지원 개선 사항"	ONTAP 9.14.1은 ONTAP 9.14.0에서 처음 제공되는 코어 토큰 기반 인증 및 OAuth 2.0 지원을 확장합니다. 그룹-역할 매핑과 함께 Active Directory 또는 LDAP를 사용하여 권한 부여를 구성할 수 있습니다. 보낸 사람 제한 액세스 토큰도 상호 TLS(MTL)를 기반으로 지원 및 보안됩니다. Auth0 및 Keycloak 외에도 Microsoft ADFS(Windows Active Directory Federation Service)는 ID 공급자(IDP)로 지원됩니다.
"OAuth 2.0 권한 부여 프레임워크"	OAuth 2.0(Open Authorization) 프레임워크가 추가되고 ONTAP REST API 클라이언트에 토큰 기반 인증을 제공합니다. 따라서 REST API 스크립트 또는 Ansible에서 제공하는 자동화 워크플로우를 사용하여 ONTAP 클러스터를 더욱 안전하게 관리하고 관리할 수 있습니다. 발급사, 대상, 로컬 검증, 원격 검사, 원격 사용자 클레임 및 프록시 지원 클라이언트 권한 부여는 자체 포함된 OAuth 2.0 범위를 사용하거나 로컬 ONTAP 사용자를 매핑하여 구성할 수 있습니다. 지원되는 ID 공급자(IDP)에는 여러 개의 동시 서버를 사용하는 Auth0 및 Keycloak이 포함됩니다.
자율적 랜섬웨어 방어에 대한 조정 가능한 경고	새 파일 확장명이 감지되거나 ARP 스냅샷이 생성될 때 알림을 수신하도록 Autonomous 랜섬웨어 방지 기능을 구성하여 가능한 랜섬웨어 이벤트에 대한 조기 경고를 수신합니다.
FPolicy는 영구 저장소를 지원하여 지연 시간을 줄여줍니다	FPolicy를 사용하면 SVM에서 의무 사항이 아닌 비동기 정책의 파일 액세스 이벤트를 캡처하는 영구 저장소를 설정할 수 있습니다. 영구 저장소는 클라이언트 I/O 처리를 FPolicy 알림 처리와 분리하여 클라이언트 지연 시간을 줄여 줍니다. 동기 및 비동기 필수 구성은 지원되지 않습니다.
FPolicy는 SMB에서 FlexCache 볼륨을 지원합니다	FPolicy는 NFS 또는 SMB에서 FlexCache 볼륨에 지원됩니다. 이전에는 SMB가 있는 FlexCache 볼륨에 대해 FPolicy가 지원되지 않았습니다.

스토리지 효율성

업데이트	설명
File System Analytics의 스캔 추적	진행 상황 및 임계치 조절에 대한 실시간 인사이트를 통해 File System Analytics 초기화 스캔을 추적합니다.
FAS 플랫폼에서 사용 가능한 애그리게이트 공간이 증가합니다	FAS 플랫폼의 경우, 크기가 30TB보다 큰 애그리게이트의 WAFL 예약 공간이 10%에서 5%로 감소하여 애그리게이트에서 가용 공간이 증가합니다.
TSSE 볼륨에서 실제 사용된 공간 보고 변경	TSSE(Temperature-Sensitive Storage Efficiency)가 활성화된 볼륨에서 볼륨에 사용된 공간의 양을 보고하기 위한 ONTAP CLI 메트릭에는 TSSE를 통해 실현된 공간 절약이 포함됩니다. 이 메트릭은 volume show-physical-used 및 volume show-space-physical used 명령에 반영됩니다. FabricPool의 경우, 의 값입니다 `-physical-used` 는 용량 계층과 성능 계층의 조합입니다. 자세한 내용은 https://docs.netapp.com/us-en/ontap-cli-9141/volume-show.html 링크를 참조하십시오[`volume show`https://docs.netapp.com/us-en/ontap-cli-9141/volume-show-space.html. (영어) 및 링크[`volume show space^].

스토리지 리소스 관리 기능 향상

업데이트	설명
사전 예방을 위한 FlexGroup 재조정	FlexGroup 볼륨은 디렉토리에서 증가하는 파일을 원격 구성요소로 자동 이동하여 로컬 구성요소에서 I/O 병목 현상을 줄일 수 있도록 지원합니다.
FlexGroup 볼륨의 스냅샷 태그 지정	에서 태그 및 레이블(주석)을 추가, 수정 및 삭제하여 스냅샷을 식별하고 FlexGroup 볼륨에서 실수로 스냅샷을 삭제하지 않도록 할 수 있습니다.
FabricPool 를 사용하여 클라우드에 직접 쓰십시오	FabricPool는 FabricPool의 볼륨에 데이터를 쓰는 기능을 추가하여 계층화 스캔을 기다리지 않고 클라우드로 직접 이동합니다.
FabricPool를 활용한 공격적 미리 읽기	FabricPool은 FabricPool이 지원하는 모든 플랫폼의 볼륨에 있는 파일에 대한 적극적인 미리 읽기 기능을 제공합니다.

SVM 관리 개선 사항

업데이트	설명
SVM 데이터 이동성 지원으로 사용자 및 그룹 할당량과 qtree가 포함된 SVM을 마이그레이션할 수 있습니다	SVM 데이터 이동성은 사용자 및 그룹 할당량, Qtree가 포함된 SVM 마이그레이션을 지원합니다.
SVM 데이터 이동성을 사용하여 SVM당 최대 400개의 볼륨, 최대 12개의 HA 쌍, NFS 4.1에서 pNFS 지원	SVM 데이터 이동성을 지원하는 SVM당 지원되는 볼륨의 최대 수는 400개로 증가하고 지원되는 HA 쌍 수가 12개로 증가합니다.

시스템 관리자

업데이트	설명
SnapMirror 테스트 페일오버 지원	System Manager를 사용하여 기존 SnapMirror 관계를 중단하지 않고 SnapMirror 테스트 페일오버 예행 연습을 수행할 수 있습니다.
브로드캐스트 도메인의 포트 관리	System Manager를 사용하여 브로드캐스트 도메인에 할당된 포트를 편집하거나 삭제할 수 있습니다.
중재자 지원 MAUSO(Automatic Unplanned Switchover) 지원	System Manager를 사용하여 IP MetroCluster 스위치오버 및 스위치백을 수행할 때 중재자 지원 MAUSO(Automatic Unplanned Switchover)를 사용하거나 사용하지 않도록 설정할 수 있습니다.
클러스터 및 볼륨 태그 지정	System Manager에서 태그를 사용하여 용도, 소유자 또는 환경별로 클러스터와 볼륨을 다양한 방법으로 분류할 수 있습니다. 이 기능은 같은 형식의 개체가 여러 개 있을 때 유용합니다. 사용자는 지정된 태그를 기반으로 특정 개체를 빠르게 식별할 수 있습니다.
일관성 그룹 모니터링 지원 기능이 향상되었습니다	System Manager에는 일관성 그룹 사용에 대한 기간별 데이터가 표시됩니다.
NVMe 대역 내 인증	System Manager를 사용하면 DH-HMAC-CHAP 인증 프로토콜을 사용하여 NVMe/TCP 및 NVMe/FC 프로토콜을 통해 NVMe 호스트와 컨트롤러 간에 안전하고 단방향 양방향 인증을 구성할 수 있습니다.

업데이트	설명
System Manager로 확장된 S3 버킷 라이프사이클 관리 지원	System Manager를 사용하여 버킷의 특정 오브젝트를 삭제하는 규칙을 정의하고 이 규칙을 통해 버킷 오브젝트를 만료시킬 수 있습니다.

ONTAP 9.13.1의 새로운 기능

ONTAP 9.13.1에서 사용 가능한 새로운 기능에 대해 알아보십시오.

최신 ONTAP 9 릴리스에서 알려진 문제, 제한 사항 및 업그레이드 주의 사항에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 릴리즈 노트". 릴리스 정보에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

- 새로운 기능 및 향상된 기능에 대해 알아봅니다 "ONTAP MetroCluster 기능".
- 에 대해 알아보세요 "AFF, ASA 및 FAS 시스템과 지원되는 스위치에 대한 새롭고 향상된 지원" .
- 의 업데이트에 대해 알아봅니다 "ONTAP REST API를 참조하십시오".

ONTAP를 업그레이드하려면 을 ONTAP 업그레이드를 준비합니다참조하십시오.

데이터 보호

업데이트	설명
"다중 관리 검증"	클러스터 관리자는 일부 SnapLock 작업이 실행되기 전에 쿼럼이 승인되도록 클러스터에서 다중 관리자 확인을 명시적으로 활성화할 수 있습니다.
"볼륨 이동 및 구조를 비롯한 일관성 그룹 관리 지원 개선"	일관성 그룹 간에 볼륨을 이동하고, 계층적 일관성 그룹의 구조를 수정하고, 일관성 그룹에 대한 용량 통찰력을 얻을 수 있습니다. System Manager는 새로운 NAS 볼륨 또는 NVMe 네임스페이스로 일관성 그룹을 생성할 수 있도록 지원합니다.
"SnapMirror Synchronous를 사용한 NDMP 복원"	NDMP 복원은 SnapMirror Synchronous에서 지원됩니다.
SnapMirror 액티브 동기화 개선 사항	• "활성 SnapMirror 활성 동기화 관계가 있는 일관성 그룹에 볼륨을 중단 없이 추가합니다." • "SnapMirror 활성 동기화로 NDMP 복구를 사용합니다"..
"단일 일관성 그룹에서 비동기식 SnapMirror 지원"	일관성 그룹이 비동기식 SnapMirror 구성을 지원하므로 단일 일관성 그룹에 대해 SnapMirror 백업을 저장할 수 있습니다.

파일 액세스 프로토콜

업데이트	설명
"NFSv4.x 스토리지 풀 지원"	일부 클라이언트에서는 NFSv4.x 스토리지 풀 리소스를 너무 많이 소비하므로 다른 NFSv4.x 클라이언트가 NFSv4.x 스토리지 풀 리소스를 사용할 수 없어 차단됩니다. 해당 환경에서 많은 NFSv4.x storepool 리소스를 사용하는 클라이언트를 거부 및 차단할 수 있습니다.

네트워킹

업데이트	설명
RDMA 클러스터 인터커넥트에 대한 하드웨어 지원 확대	ONTAP은 X91153A 클러스터 NIC를 사용하는 클러스터 인터커넥트 RDMA용 AFF A900, ASA A900 및 FAS9500 시스템을 지원하여 지연 시간을 단축하고, 페일오버 시간을 줄이며, 노드 간 통신 속도를 높이는 데 도움이 됩니다.
데이터 LIF 제한이 증가합니다	ONTAP는 HA Pair 및 클러스터 모두에 대해 데이터 LIF 확장 제한을 늘려 유연성을 강화합니다.
A800 및 FAS8700 플랫폼에서 클러스터 설정 중에 IPv6 지원	A800 및 FAS8700 플랫폼에서는 ONTAP CLI를 사용하여 IPv6 전용 네트워킹 환경에서 새 클러스터를 생성하고 구성할 수 있습니다.

S3 오브젝트 스토리지

업데이트	설명
S3 버킷 라이프사이클 관리	S3 오브젝트 만료 동작은 버킷의 오브젝트가 만료되는 시점을 정의합니다. 따라서 오브젝트 버전을 관리할 수 있으므로 보존 요구사항을 충족하고 전체 S3 오브젝트 스토리지를 효과적으로 관리할 수 있습니다.

산

업데이트	설명
AIX 호스트에서 NVMe/FC 지원	ONTAP는 AIX 호스트에서 NVMe/FC 프로토콜을 지원합니다. 를 참조하십시오 "NetApp 상호 운용성 툴" 지원되는 구성.

보안

피처	설명
자율 랜섬웨어 보호	• 여러 관리자가 자율적 랜섬웨어 방어 기능으로 기능을 확인합니다 • 학습에서 활성 모드로 자동 전환 • FlexGroup 지원FlexGroup 볼륨 확장, FlexVol에서 FlexGroup FlexGroup으로 전환, FlexGroup 재조정에 대한 분석 및 보고 기능이 포함되어 있습니다.
Active Directory를 사용한 SSH 공개 키 인증	Active Directory(AD) 사용자의 기본 인증 방법으로 SSH 공개 키를 사용하거나, AD 사용자 이후의 보조 인증 방법으로 SSH 공개 키를 사용할 수 있습니다.
SSH 공개 키가 있는 X.509 인증서	ONTAP를 사용하면 X.509 인증서를 계정의 SSH 공개 키와 연결하여 SSH 로그인 시 인증서 만료 및 해지 확인 보안을 강화할 수 있습니다.
FPolicy 파일 액세스 실패 알림	FPolicy는 액세스가 거부된 이벤트에 대한 알림을 지원합니다. 파일 작업에 대한 알림은 권한 부족으로 인해 실패함(예: NTFS 사용 권한 실패, Unix 모드 비트로 인한 실패, NFSv4 ACL로 인한 실패).
TOTP(시간 기반 1회 암호)를 통한 다단계 인증	TOTP(Time-Based One-Time Password)를 사용하여 다단계 인증으로 로컬 사용자 계정을 설정합니다. TOTP는 항상 두 번째 인증 방법으로 사용됩니다. SSH 공개 키 또는 사용자 암호를 기본 인증 방법으로 사용할 수 있습니다.

스토리지 효율성

업데이트	설명
System Manager의 기본 데이터 축소율에 대한 보고 변경	System Manager에 표시되는 운영 데이터 축소율에는 계산에 스냅샷 공간 절약이 더 이상 포함되지 않습니다. 사용된 논리적 공간과 사용된 물리적 공간 간의 비율만 나타냅니다. ONTAP의 이전 릴리즈에서는 기본 데이터 축소율이 스냅샷의 공간 절약 이점을 크게 나타냈습니다. 따라서 ONTAP 9.13.1로 업그레이드할 때 보고된 기본 비율이 현저히 낮습니다. **Capacity** Details(용량** 세부 정보) 보기에서는 스냅샷을 사용한 데이터 축소율을 계속 볼 수 있습니다.
온도에 민감한 스토리지 효율성	온도에 민감한 스토리지 효율성: 인접한 물리적 블록을 순차적으로 패킹하여 스토리지 효율성을 높입니다. 온도에 민감한 스토리지 효율성이 활성화된 볼륨은 시스템을 ONTAP 9.13.1로 업그레이드할 때 자동으로 순차적 패킹이 활성화됩니다.
논리적 공간 적용	논리적 공간 적용은 SnapMirror 대상에 지원됩니다.
스토리지 VM 용량은 지원을 제한합니다	스토리지 VM(SVM)에 용량 한도를 설정하고 SVM이 백분율 임계값에 가까워지면 경고를 설정할 수 있습니다.

스토리지 리소스 관리 기능 향상

업데이트	설명
최대 inode 수가 증가합니다	볼륨이 680GB보다 커지는 경우에도 ONTAP는 inode(32KB의 볼륨 공간당 1개의 inode 속도로) 계속해서 inode를 자동으로 추가합니다. ONTAP는 최대 2,040,109,451에 도달할 때까지 inode를 계속 추가합니다.
FlexClone 생성 중 SnapLock 유형을 지정할 수 있습니다	읽기/쓰기 볼륨의 FlexClone을 생성할 때 Compliance, Enterprise 또는 비 SnapLock의 세 가지 SnapLock 유형 중 하나를 지정할 수 있습니다.
기본적으로 파일 시스템 분석을 사용하도록 설정합니다	새 볼륨에 대해 File System Analytics를 기본적으로 사용하도록 설정합니다.
FlexGroup 볼륨과의 SVM 재해 복구 계획 관계	FlexGroup 볼륨에서 SVM DR의 팬 아웃 제한은 제거됩니다. FlexGroup를 지원하는 SVM DR에는 8개 사이트에 대한 SnapMirror 팬아웃 관계가 포함되어 있습니다.
단일 FlexGroup 재조정 작업	단일 FlexGroup 재조정 작업이 지정한 날짜와 시간에 시작되도록 예약할 수 있습니다.
FabricPool 읽기 성능	FabricPool는 클라우드에 상주하는 데이터 및 계층화 처리량을 위해 단일 및 멀티 스트림 워크로드에 향상된 순차적 읽기 성능을 제공합니다. 이러한 성능 향상을 통해 GET 및 PUT의 속도가 백엔드 객체 저장소로 보다 빠르게 전송될 수 있습니다. 온프레미스 오브젝트 저장소가 있는 경우 오브젝트 저장소 서비스의 성능 여유 공간을 고려하여 FabricPool 푸드를 제한해야 하는지 여부를 결정해야 합니다.
적응형 QoS 정책 템플릿	적응형 QoS 정책 템플릿을 사용하여 SVM 레벨에서 처리량 한도를 설정할 수 있습니다.

SVM 관리 개선 사항

업데이트	설명
SVM 데이터 이동성	최대 200개의 볼륨이 포함된 SVM 마이그레이션 지원 증가

시스템 관리자

ONTAP 9.12.1부터 System Manager가 NetApp Console과 통합되었습니다. 자세히 알아보세요 NetApp 콘솔과 시스템 관리자 통합 .

업데이트	설명
기본 데이터 축소율 보고 변경	System Manager에 표시되는 운영 데이터 축소율에는 계산에 스냅샷 공간 절약이 더 이상 포함되지 않습니다. 사용된 논리적 공간과 사용된 물리적 공간 간의 비율만 나타냅니다. ONTAP의 이전 릴리즈에서는 기본 데이터 축소율이 스냅샷의 공간 절약 이점을 크게 나타냈습니다. 따라서 ONTAP 9.13.1로 업그레이드할 때 보고된 기본 비율이 현저히 낮습니다. Capacity details(용량 세부 정보) 보기에서는 스냅샷의 데이터 축소율을 계속 볼 수 있습니다.
변조 방지 스냅샷 잠금	System Manager를 사용하여 SnapLock가 아닌 볼륨의 스냅샷을 잠가 랜섬웨어 공격으로부터 보호할 수 있습니다.
외부 키 관리자 지원	System Manager를 사용하여 외부 키 관리자를 관리할 수 있으며 인증 및 암호화 키를 저장하고 관리할 수 있습니다.
하드웨어 문제 해결	System Manager 사용자는 ASA 플랫폼 및 AFF C-Series 플랫폼을 포함한 "하드웨어" 페이지에서 추가 하드웨어 플랫폼을 시각적으로 볼 수 있습니다. AFF C-Series 플랫폼에 대한 지원은 ONTAP 9.12.1, ONTAP 9.11.1 및 ONTAP 9.10.1의 최신 패치 릴리스에도 포함되어 있습니다. 시각화는 플랫폼의 문제나 문제를 식별하여 사용자가 하드웨어 문제를 신속하게 해결할 수 있는 방법을 제공합니다.

ONTAP 9.12.1의 새로운 기능

ONTAP 9.12.1에서 사용할 수 있는 새로운 기능에 대해 알아봅니다.

최신 ONTAP 9 릴리스에서 알려진 문제, 제한 사항 및 업그레이드 주의 사항에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 릴리즈 노트". 릴리스 정보에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

- 새로운 기능 및 향상된 기능에 대해 알아봅니다 "ONTAP MetroCluster 기능".
- 에 대해 알아보세요 "AFF, ASA 및 FAS 시스템과 지원되는 스위치에 대한 새롭고 향상된 지원" .
- 의 업데이트에 대해 알아봅니다 "ONTAP REST API를 참조하십시오".

ONTAP를 업그레이드하려면 을 ONTAP 업그레이드를 준비합니다참조하십시오.

데이터 보호

업데이트	설명
SnapMirror Synchronous로 더 큰 FlexVol 볼륨 지원	SnapMirror Synchronous 구성에서 지원되는 최대 FlexVol 볼륨 크기가 100TB에서 300TB로 증가했습니다. 소스 클러스터와 대상 클러스터 모두 _ONTAP 9.12.1P2 또는 이후 _ 을(를) 실행해야 합니다.
SnapMirror Synchronous에서 더 큰 파일 및 LUN 크기 지원	SnapMirror Synchronous 구성에서 지원되는 최대 파일 및 LUN 크기가 16TB에서 128TB로 증가했습니다. 소스 클러스터와 대상 클러스터 모두 ONTAP 9.12.1 P2 이상을 실행해야 합니다.
일관성 그룹에 대한 지원이 향상되었습니다	• 정합성 보장 그룹에서 볼륨을 추가 및 제거하고 정합성 보장 그룹(스냅샷에서 포함)을 클론 복제할 수 있습니다. • 일관성 그룹은 애플리케이션 태그를 지원하여 데이터 보호 및 관리 프로세스를 간소화합니다. • ONTAP REST API에서는 NFS/SMB 볼륨 또는 NVMe 네임스페이스를 사용하여 일관성 그룹을 구성할 수 있습니다.
SnapMirror Synchronous NDO	SnapMirror Synchronous는 HA 테이크오버 및 반환, 볼륨 이동 및 기타 유지보수 관련 작업에 대한 무중단 운영(NDO)을 지원합니다. 이 기능은 AFF/ASA 플랫폼에서만 사용할 수 있습니다.
ONTAP mediator 1.5는 SnapMirror 비즈니스 연속성을 지원합니다	ONTAP mediator 1.5를 사용하여 SnapMirror 활성 동기화 관계를 모니터링할 수 있습니다.
SnapMirror 액티브 동기화 연속성 개선 사항	SnapMirror 활성 동기화는 스냅샷에서 부분 LUN 복원을 지원합니다. 또한 SnapMirror 활성 동기화는 QoS를 SnapMirror 관계에 없는 볼륨으로 확장합니다.
SnapMirror 비동기식에 대한 데이터 웨어하우스 리빌드 표시기	SnapMirror Asynchronous는 재해 복구 예행 연습 후 완료율을 표시하여 데이터 웨어하우스 재구축에 걸리는 시간을 보여 줍니다.
최소 보존 시간을 "지정되지 않은" 절대 보존 시간을 설정하는 SnapLock 옵션입니다	SnapLock에는 절대 보존 시간이 "지정되지 않음"으로 설정된 경우 최소 보존 시간을 설정하는 옵션이 포함되어 있습니다.
변조 방지 스냅샷	SnapLock가 아닌 볼륨에서 스냅샷을 잠가 랜섬웨어 공격으로부터 보호할 수 있습니다. 스냅샷을 잠그면 실수로 또는 악의적으로 삭제되지 않습니다.

파일 액세스 프로토콜

업데이트	설명
AES 암호화를 사용하여 Kerberos 기반 통신에 대한 보안 구성	새로운 SMB 보안 옵션을 사용하면 AD(Active Directory) KDC와의 Kerberos 기반 통신을 위해 AES(Advanced Encryption Standard) 암호화 유형에 따라 RC4 및 DES를 사용하지 않도록 설정할 수 있습니다.
S3 클라이언트에서 NAS 데이터에 액세스	S3 클라이언트는 다시 포맷하지 않고도 NFS 및 SMB 클라이언트와 동일한 NAS 데이터에 액세스할 수 있으므로 오브젝트 데이터가 필요한 S3 애플리케이션을 더욱 쉽게 제공할 수 있습니다.
NFS 확장 속성입니다	NFSv4.2에 설정된 NFS 서버는 xattr 인식 클라이언트에서 NFS 확장 속성(xattrs)을 저장하고 검색할 수 있습니다.
NFSv4.2 분할 파일 및 공간 예약 지원	NFSv4.2 클라이언트는 분할 파일에 대한 공간을 예약할 수 있습니다. 또한 파일에서 공간을 할당 해제하거나 예약 해제할 수 있습니다.

네트워킹

업데이트	설명
LIF 서비스	를 사용할 수 있습니다 `management-log-forwarding` 감사 로그를 원격 syslog 서비스에 전달하는 데 사용되는 LIF를 제어하는 서비스입니다

S3 오브젝트 스토리지

업데이트	설명
S3 작업에 대한 지원이 확장되었습니다	지원되는 Amazon S3 API 작업은 다음과 같습니다. • `CopyObject` • `UploadPartCopy` • `BucketPolicy` (가져오기, 넣기, 삭제)

산

업데이트	설명
AFF 및 FAS 플랫폼의 최대 LUN 크기가 증가합니다	ONTAP 9.12.1P2부터 AFF 및 FAS 플랫폼에서 지원되는 최대 LUN 크기가 16TB에서 128TB로 증가했습니다.
"증가된 NVMe 제한"	NVMe 프로토콜은 다음을 지원합니다. • 단일 스토리지 VM 및 단일 클러스터에서 8K 서브시스템을 지원합니다 • 12노드 클러스터 NVMe/FC는 포트당 256개의 컨트롤러를 지원하고 NVMe/TCP는 노드당 2K 컨트롤러를 지원합니다.
보안 인증을 위한 NVMe/TCP 지원	DHHMAC-CHAP 인증 프로토콜을 사용하여 NVMe/TCP를 통해 NVMe 호스트와 컨트롤러 간에 안전한 단방향 및 양방향 인증이 지원됩니다.
NVMe에 대한 MetroCluster IP 지원	NVMe/FC 프로토콜은 4노드 MetroCluster IP 구성에서 지원됩니다.

보안

2022년 10월, NetApp는 TLSv1.2 또는 보안 SMTP를 사용하여 HTTPS에서 전송되지 않는 AutoSupport 메시지 전송을 거부하기 위한 변경 사항을 구현했습니다. 자세한 내용은 을 참조하십시오 "SU484: NetApp는 전송 보안이 불충분하여 전송된 AutoSupport 메시지를 거부합니다".

피처	설명
자율적 랜섬웨어 방어 상호 운용성 개선	자율적 랜섬웨어 방어는 다음 구성에 사용할 수 있습니다. • SnapMirror로 보호되는 볼륨 • SnapMirror로 SVM 보호 • 마이그레이션을 위해 SVM 지원(SVM 데이터 이동성)
FIDO2 및 PIV(Yubikey에서 모두 사용)를 통한 SSH에 대한 다단계 인증(MFA) 지원	SSH MFA는 사용자 이름 및 암호로 하드웨어 지원 공용/개인 키 교환을 사용할 수 있습니다. Yubikey는 MFA 보안을 강화하기 위해 SSH 클라이언트에 연결된 물리적 토큰 디바이스입니다.
변조 방지 로깅	모든 ONTAP 내부 로그는 기본적으로 무단 변경이 방지되므로 손상된 관리자 계정이 악의적인 작업을 숨길 수 없습니다.
이벤트에 대한 TLS 전송	EMS 이벤트는 TLS 프로토콜을 사용하여 원격 syslog 서버로 전송될 수 있으므로 중앙 외부 감사 로깅을 위한 유선을 통한 보호가 강화됩니다.

스토리지 효율성

업데이트	설명
온도에 민감한 스토리지 효율성	새로운 AFF C250, AFF C400, AFF C800 플랫폼 및 볼륨에서 온도에 민감한 스토리지 효율성이 기본적으로 활성화됩니다. TSSE는 기존 볼륨에서 기본적으로 활성화되어 있지 않지만 ONTAP CLI를 사용하여 수동으로 활성화할 수 있습니다.
사용 가능한 애그리게이트 공간의 증가	AFF(All Flash FAS) 및 FAS500f 플랫폼의 경우 30TB를 초과하는 애그리게이트에 대한 WAFL 예약 공간이 10%에서 5%로 감소하므로 애그리게이트에서 가용 공간이 증가합니다.
파일 시스템 분석: 크기별 상위 디렉토리	이제 File System Analytics는 볼륨에서 가장 많은 공간을 소비하는 디렉토리를 식별합니다.

스토리지 리소스 관리 기능 향상

업데이트	설명
FlexGroup 재조정	무중단 FlexGroup 볼륨 재조정을 자동으로 수행하여 FlexGroup 구성요소 간에 파일을 재배포할 수 있습니다. FlexVol에서 FlexGroup로 변환한 후에는 자동 FlexGroup 재조정을 사용하지 않는 것이 좋습니다. 대신 명령을 입력하여 ONTAP 9.10.1 이상에서 사용할 수 있는 중단 소급 파일 이동 기능을 사용할 수 있습니다 `volume rebalance file-move`. 자세한 내용과 명령 구문은 다음을 참조하세요. "ONTAP 명령 참조" .
FlexGroup 볼륨을 지원하는 SnapVault용 SnapLock	FlexGroup 볼륨을 지원하는 SnapVault용 SnapLock

SVM 관리 개선 사항

업데이트	설명
SVM 데이터 이동성의 개선 사항	클러스터 관리자는 하이브리드 애그리게이트의 FAS AFF 플랫폼을 사용하여 운영 중단 없이 SVM을 소스 클러스터에서 타겟 클러스터로 재배치할 수 있습니다. Disruptive SMB 프로토콜과 Autonomous 랜섬웨어 Protection에 대한 지원이 추가되었습니다.

시스템 관리자

ONTAP 9.12.1부터 System Manager가 NetApp Console과 통합되었습니다. 콘솔을 사용하면 관리자는 익숙한 시스템 관리자 대시보드를 유지하면서 단일 제어 평면에서 하이브리드 멀티클라우드 인프라를 관리할 수 있습니다. System Manager에 로그인하면 관리자는 NetApp 콘솔에서 System Manager 인터페이스에 액세스하거나 System Manager에 직접 액세스하는 옵션이 제공됩니다. 자세히 알아보세요 NetApp 콘솔과 시스템 관리자 통합 .

업데이트	설명
SnapLock에 대한 System Manager 지원	규정 준수 클록 초기화, SnapLock 볼륨 생성 및 WORM 파일 미러링을 포함한 SnapLock 작업이 System Manager에서 지원됩니다.
케이블 연결의 하드웨어 시각화	System Manager 사용자는 클러스터에 있는 하드웨어 장치 간의 케이블 연결에 대한 연결 정보를 확인하여 연결 문제를 해결할 수 있습니다.
System Manager에 로그인할 때 Cisco Duo를 통해 다단계 인증을 지원합니다	Cisco Duo를 SAML ID 공급자(IDP)로 구성하여 사용자가 System Manager에 로그인할 때 Cisco Duo를 사용하여 인증할 수 있습니다.
System Manager 네트워킹 개선 사항	System Manager는 네트워크 인터페이스를 생성하는 동안 서브넷 및 홈 포트 선택에 대한 제어 기능을 제공합니다. System Manager는 RDMA 연결을 통한 NFS 구성도 지원합니다.
시스템 표시 테마	System Manager 사용자는 System Manager 인터페이스 표시에 사용할 밝은 또는 어두운 테마를 선택할 수 있습니다. 또한 운영 체제 또는 브라우저에 사용되는 테마를 기본값으로 선택할 수도 있습니다. 이 기능을 통해 사용자는 디스플레이를 보다 편안하게 읽을 수 있는 설정을 지정할 수 있습니다.
로컬 계층 용량 세부 정보 개선	System Manager 사용자는 특정 로컬 계층의 용량 세부 정보를 보고 공간이 과도하게 할당되었는지 확인할 수 있습니다. 즉, 로컬 계층에 공간이 부족하지 않도록 용량을 추가해야 할 수 있습니다.
향상된 검색 기능	System Manager의 향상된 검색 기능을 사용하면 사용자가 System Manager 인터페이스를 통해 NetApp Support 사이트에서 관련 및 문맥에 민감한 지원 정보 및 System Manager 제품 문서를 직접 검색하고 액세스할 수 있습니다. 이를 통해 사용자는 지원 사이트의 다양한 위치에서 검색할 필요 없이 적절한 조치를 취하는 데 필요한 정보를 얻을 수 있습니다.
볼륨 프로비저닝 개선	스토리지 관리자는 기본 정책을 사용하지 않고 System Manager를 사용하여 볼륨을 생성할 때 스냅샷 정책을 선택할 수 있습니다.
볼륨 크기를 늘립니다	스토리지 관리자는 System Manager를 사용하여 볼륨 크기를 조정할 때 데이터 공간과 스냅샷 예약에 미치는 영향을 볼 수 있습니다.
스토리지 풀 및 Flash Pool을 참조하십시오 관리	스토리지 관리자는 System Manager를 사용하여 SSD 스토리지 풀에 SSD를 추가하고, SSD 스토리지 풀 할당 유닛을 사용하여 Flash Pool 로컬 계층(애그리게이트)을 생성하고, 물리적 SSD를 사용하여 Flash Pool 로컬 계층을 생성할 수 있습니다.

업데이트	설명
System Manager에서 NFS over RDMA 지원	System Manager는 RDMA 기반 NFS에 대한 네트워크 인터페이스 구성을 지원하고 RoCE 지원 포트를 식별합니다.

ONTAP 9.11.1의 새로운 기능

ONTAP 9.11.1에서 사용할 수 있는 새로운 기능에 대해 알아봅니다.

최신 ONTAP 9 릴리스에서 알려진 문제, 제한 사항 및 업그레이드 주의 사항에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 릴리즈 노트". 릴리스 정보에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

- 새로운 기능 및 향상된 기능에 대해 알아봅니다 "ONTAP MetroCluster 기능".
- 에 대해 알아보세요 "AFF, ASA 및 FAS 시스템과 지원되는 스위치에 대한 새롭고 향상된 지원" .
- 의 업데이트에 대해 알아봅니다 "ONTAP REST API를 참조하십시오".

최신 버전의 ONTAP로 업그레이드하려면 를 참조하십시오ONTAP 업그레이드를 준비합니다.

데이터 보호

업데이트	설명
클러스터 외부 키 서버	클러스터 KMIP 서버 솔루션을 제공하는 NetApp 파트너를 위해 클러스터형 외부 키 관리 서버 지원이 추가되었습니다. 이를 통해 기본 및 보조 KMIP 서버를 추가하여 암호화 키 데이터의 중복을 방지할 수 있습니다. 지원되는 파트너는 을 참조하십시오 "상호 운용성 매트릭스 툴".
System Manager의 SnapMirror 비동기식 정책	System Manager를 사용하면 볼륨 및 스토리지 VM을 보호할 때 미리 생성된 사용자 정의 미러 및 소산 정책을 추가하고, 레거시 정책을 표시하고, 보호 정책에 정의된 전송 일정을 재정의할 수 있습니다. System Manager를 사용하여 볼륨 및 스토리지 VM 보호 관계를 편집할 수도 있습니다. ONTAP 9.8P12 이상 ONTAP 9.8 패치 릴리즈를 실행 중인 경우, System Manager를 사용하여 SnapMirror를 구성한 후 ONTAP 9.9.1 또는 ONTAP 9.10.1 릴리스로 업그레이드하려면 ONTAP 9.9.1P13 이상 및 ONTAP 9.10.1P10 이상 패치 릴리즈를 사용하십시오.
SnapMirror Cloud 단일 디렉토리 복원	admin 권한 수준의 클러스터 관리자가 클라우드 엔드포인트에서 단일 디렉토리 복원 작업을 수행할 수 있습니다. 복원 중인 백업 끝점을 식별하려면 소스 끝점 UUID를 제공해야 합니다. 여러 백업이 동일한 데이터를 사용할 수 있기 때문입니다 `cloud_endpoint_name` restore 명령에 대해 백업과 연결된 UUID를 대상으로 제공해야 합니다. 를 사용할 수 있습니다 `snapmirror show` 명령을 사용하여 를 가져옵니다 `source_endpoint_uuid`.
SnapMirror 액티브 동기화 지원이 향상되었습니다	• SnapMirror 액티브 동기화는 AIX를 호스트로서 지원합니다 • SnapMirror 액티브 동기화는 단일 파일 SnapRestore를 지원하므로 SnapMirror 액티브 동기화 구성에서 개별 LUN 또는 일반 파일을 복원할 수 있습니다.

업데이트	설명
SVM 데이터 복제 빠른 재동기화	SVM 데이터 복제 빠른 재동기화는 스토리지 관리자가 전체 데이터 웨어하우스 재구축을 우회하고 재해 복구 예행연습을 통해 보다 빠르게 복구할 수 있는 기능을 제공합니다.
MetroCluster를 통한 SVM 데이터 복제 지원	SVM-DR 소스는 MetroCluster 구성의 양쪽 모두에서 지원됩니다.
2단계 정합성 보장 그룹 스냅샷 생성	REST API에서 일관성 그룹은 2단계 스냅샷 절차를 지원하므로 스냅샷을 커밋하기 전에 사전 점검을 수행할 수 있습니다.

파일 액세스 프로토콜

업데이트	설명
TLSv1.3 지원	ONTAP는 HTTPS 및 REST API 관리 프로토콜에 TLS 1.3을 지원합니다. TLS 1.3은 SP/BMC 또는 클러스터 피어링 암호화와 함께 지원되지 않습니다.
LDAP Fast bind 지원	LDAP 서버에서 지원되는 경우 LDAP 빠른 바인딩을 사용하여 ONTAP 관리자 사용자를 빠르고 간단하게 인증할 수 있습니다.

네트워킹

업데이트	설명
LLDP(Link Layer Discovery Protocol)	클러스터 네트워크는 ONTAP가 CDP(Cisco Discovery Protocol)를 지원하지 않는 클러스터 스위치와 함께 작동하도록 LLDP를 지원합니다.
LIF 서비스	새로운 클라이언트 측 LIF 서비스는 아웃바운드 AD, DNS, LDAP 및 NIS 요청에 사용되는 LIF를 보다 효과적으로 제어합니다.

S3 오브젝트 스토리지

업데이트	설명
S3 오브젝트 작업에 대한 추가 지원	ONTAP API에서 지원되는 작업은 다음과 같습니다. `CreateBucket`, `DeleteBucket`, `DeleteObjects`. 또한 ONTAP S3는 와의 오브젝트 버전 관리 및 관련 작업을 지원합니다 `PutBucketVersioning`, `GetBucketVersioning`, `ListBucketVersions`.

산

업데이트	설명
iSCSI LIF 페일오버	새로운 iSCSI LIF 페일오버 기능은 SFO 파트너 페일오버 및 로컬 페일오버에서 iSCSI LIF의 자동 및 수동 마이그레이션을 지원합니다. iSCSI LIF 페일오버는 모든 SAN 어레이(ASA) 플랫폼에서 사용할 수 있습니다.
LUN에서 NVMe 네임스페이스로, NVMe 네임스페이스에서 LUN으로 중단 없이 마이그레이션	ONTAP CLI를 사용하여 데이터 이동 없이 를 변환합니다 기존 LUN을 NVMe 네임스페이스에 제공 또는 을 누릅니다 LUN에 대한 기존 NVMe 네임스페이스.

보안

업데이트	설명
ARP(자율 랜섬웨어 방어) 개선	ARP 탐지 알고리즘은 추가 맬웨어 위협을 감지하도록 개선되었습니다. 또한 자율적 랜섬웨어 방어를 활성화하는 데 새로운 라이센스 키가 사용됩니다. ONTAP 9.10.1에서 ONTAP 시스템을 업그레이드할 경우 이전 라이센스 키는 동일한 기능을 제공합니다.
다중 관리 검증	다중 관리자 확인이 활성화된 경우 볼륨 또는 스냅샷 삭제와 같은 특정 작업은 지정된 관리자의 승인 후에만 실행할 수 있습니다. 따라서 손상되거나 악의적이거나 경험이 부족한 관리자가 원치 않는 변경 또는 데이터 삭제를 방지할 수 있습니다.

스토리지 효율성

업데이트	설명
물리적인 설치 공간 절약 효과를 확인하십시오	볼륨에서 온도에 민감한 스토리지 효율성을 활성화한 경우 volume show-footprint 명령을 사용하여 물리적인 설치 공간 절약 효과를 표시할 수 있습니다.
FlexGroup 볼륨에 대한 SnapLock 지원	SnapLock는 FlexGroup 볼륨에 저장된 데이터를 지원합니다. FlexGroup 볼륨 지원은 SnapLock 규정 준수 및 SnapLock 엔터프라이즈 모드에서 사용할 수 있습니다.
SVM 데이터 이동성	지원되는 AFF 어레이의 수를 3개로 늘리고 소스 및 타겟에서 ONTAP 9.11.1 이상을 실행 중인 경우 SnapMirror 관계 지원을 추가합니다. 외부 키 관리(KMIP)도 도입되어 클라우드 및 사내 설치 모두에서 사용할 수 있습니다.

스토리지 리소스 관리 기능 향상

업데이트	설명
File System Analytics에서 SVM 레벨에서 활동 추적	활동 추적은 SVM 레벨에서 집계되어 읽기/쓰기 IOPS 및 처리량을 추적하여 데이터에 대한 즉각적이고 실행 가능한 통찰력을 제공합니다.
파일 액세스 시간 업데이트를 활성화합니다	활성화된 경우 현재 액세스 시간이 사용자가 지정한 기간을 초과하는 경우에만 FlexCache 원본 볼륨에서 액세스 시간이 업데이트됩니다.
비동기식 디렉토리 삭제	비동기 삭제는 스토리지 관리자가 볼륨에 대한 권한을 부여한 경우 NFS 및 SMB 클라이언트에서 사용할 수 있습니다. 비동기 삭제가 활성화된 경우 Linux 클라이언트는 mv 명령을 사용할 수 있고 Windows 클라이언트는 rename 명령을 사용하여 디렉토리를 삭제하고 숨겨진 디렉토리로 이동할 수 있습니다 `.ontaptrashbin` 디렉토리.
FlexGroup 볼륨에 대한 SnapLock 지원	SnapLock는 FlexGroup 볼륨에 저장된 데이터를 지원합니다. FlexGroup 볼륨 지원은 SnapLock 규정 준수 및 SnapLock 엔터프라이즈 모드에서 사용할 수 있습니다. SnapLock은 FlexGroup 볼륨에 대해 SnapLock for SnapVault, 이벤트 기반 보존 및 법적 보관과 같은 작업을 지원하지 않습니다.

SVM 관리 개선 사항

업데이트	설명
SVM 데이터 이동성	지원되는 AFF 어레이의 수를 3개로 늘리고 소스 및 타겟에서 ONTAP 9.11.1 이상을 실행 중인 경우 SnapMirror 관계 지원을 추가합니다. 외부 키 관리(KMIP)도 도입되어 클라우드와 사내 설치 모두에서 사용할 수 있습니다.

시스템 관리자

업데이트	설명
SnapMirror 비동기식 정책을 관리합니다	System Manager를 사용하여 사전 생성된 사용자 정의 미러 및 소산 정책을 추가하고, 레거시 정책을 표시하고, 볼륨 및 스토리지 VM을 보호할 때 보호 정책에 정의된 전송 일정을 재정의할 수 있습니다. System Manager를 사용하여 볼륨 및 스토리지 VM 보호 관계를 편집할 수도 있습니다. ONTAP 9.8P12 이상 ONTAP 9.8 패치 릴리즈를 사용 중이고 System Manager를 사용하여 SnapMirror를 구성한 경우, ONTAP 9.9.1 또는 ONTAP 9.10.1 릴리스로 업그레이드하려면 ONTAP 9.9.1P13 이상 및 ONTAP 9.10.1P10 이상 패치 릴리즈를 사용해야 합니다.
하드웨어 시각화	System Manager의 하드웨어 시각화 기능은 현재 AFF 및 FAS 플랫폼을 모두 지원합니다.
시스템 분석 인사이트	Insights 페이지에 System Manager는 클러스터 및 스토리지 VM 구성에 대한 추가 용량 및 보안 통찰력과 새로운 통찰력을 표시하여 시스템을 최적화하도록 지원합니다.
사용 편의성 향상	• 새로 생성된 볼륨은 기본적으로 공유할 수 없습니다. NFS를 통해 내보내거나 SMB/CIFS를 통해 공유하고 사용 권한 수준을 지정하는 등 기본 액세스 권한을 지정할 수 있습니다. • SAN 단순화: 이니시에이터 그룹을 추가하거나 편집할 때 System Manager 사용자는 그룹에 있는 이니시에이터의 연결 상태를 보고 LUN 데이터에 액세스할 수 있도록 연결된 이니시에이터가 그룹에 포함되어 있는지 확인할 수 있습니다.
고급 로컬 계층(애그리게이트) 작업	System Manager 관리자는 System Manager의 권장 사항을 수락하지 않으려는 경우 로컬 계층의 구성을 지정할 수 있습니다. 또한, 관리자는 기존 로컬 계층의 RAID 구성을 편집할 수 있습니다. ONTAP 9.8P12 이상 ONTAP 9.8 패치 릴리즈를 사용 중이고 System Manager를 사용하여 SnapMirror를 구성한 경우, ONTAP 9.9.1 또는 ONTAP 9.10.1 릴리스로 업그레이드하려면 ONTAP 9.9.1P13 이상 및 ONTAP 9.10.1P10 이상 패치 릴리즈를 사용해야 합니다.
감사 로그 관리	System Manager를 사용하여 ONTAP 감사 로그를 보고 관리할 수 있습니다.

관련 정보

- "스냅미러 쇼"

ONTAP 9.10.1의 새로운 기능

ONTAP 9.10.1에서 사용할 수 있는 새로운 기능에 대해 알아보십시오.

최신 ONTAP 9 릴리스에서 알려진 문제, 제한 사항 및 업그레이드 주의 사항에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 릴리즈 노트". 릴리스 정보에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

- 새로운 기능 및 향상된 기능에 대해 알아봅니다 "ONTAP MetroCluster 기능".
- 에 대해 알아보세요 "AFF, ASA 및 FAS 시스템과 지원되는 스위치에 대한 새롭고 향상된 지원" .
- 의 업데이트에 대해 알아봅니다 "ONTAP REST API를 참조하십시오".

ONTAP를 업그레이드하려면 을 ONTAP 업그레이드를 준비합니다참조하십시오.

데이터 보호

업데이트	설명
SnapLock 보존 기간을 최대 100년으로 설정합니다	ONTAP 9.10.1 이전 릴리스에서 지원되는 최대 보존 시간은 2071년 1월 19일입니다. ONTAP 9.10.1 SnapLock 엔터프라이즈 및 규정 준수부터 보존 기간은 10월 26일, 3058년까지, 보존 기간은 최대 100년까지입니다. 보존 날짜를 늘리면 이전 정책이 자동으로 변환됩니다.
SnapLock 및 비 SnapLock 볼륨을 동일한 애그리게이트에서 생성 가능	ONTAP 9.10.1부터 SnapLock 및 비 SnapLock 볼륨이 동일한 aggregate에 존재할 수 있으므로, SnapLock 볼륨에 대한 별도의 SnapLock 애그리게이트를 생성할 필요가 없습니다.
정합성 보장 그룹	볼륨 및 LUN을 정합성 보장 그룹으로 구성하여 데이터 보호 정책을 관리하고 여러 스토리지 볼륨에 걸쳐 있는 워크로드의 쓰기 순서를 정확히 유지할 수 있습니다.
퍼블릭 클라우드를 사용하여 백업 아카이빙	SnapMirror Cloud는 AWS 및 MS Azure에서 저렴한 퍼블릭 클라우드 오브젝트 스토리지 클래스로 ONTAP 백업을 계층화하여 장기 보존하도록 지원합니다.
안전한 Netlogon 채널 통신을 위한 AES 지원	Netlogon 인증 서비스를 사용하여 Windows 도메인 컨트롤러에 연결하는 경우 보안 채널 통신을 위해 AES(고급 암호화 표준)를 사용할 수 있습니다.
SMB 도메인-터널 인증을 위한 Kerberos	Kerberos 인증은 NTLM 외에도 ONTAP 관리를 위한 도메인 터널 인증에 사용할 수 있습니다. 이렇게 하면 Active Directory 자격 증명을 사용하여 ONTAP CLI 및 System Manager GUI에 더욱 안전하게 로그인할 수 있습니다.
LDAP 통신 보안을 강화하기 위한 채널 바인딩	LDAP 채널 바인딩은 Active Directory 및 이름 서비스 LDAP 연결에 모두 기본적으로 지원됩니다. 그러면 중간자 공격에 대한 보호 기능이 향상됩니다.

파일 액세스 프로토콜

업데이트	설명
NFS over RDMA(NVIDIA만 해당)	RDMA 상의 NFS는 RDMA 어댑터를 사용하므로 스토리지 시스템 메모리와 호스트 시스템 메모리 간에 데이터를 직접 복사할 수 있으므로 CPU 중단과 오버헤드를 피할 수 있습니다. NFS over RDMA를 사용하면 지원되는 NVIDIA GPU가 있는 호스트에서 GPU 가속 워크로드에 NVIDIA GPUDirect Storage를 사용할 수 있습니다.

네트워킹

업데이트	설명
RDMA 클러스터 상호 연결	A400 또는 ASA A400 스토리지 시스템과 X1151A 클러스터 NIC를 사용하면 클러스터 내부 트래픽에 RDMA를 활용하여 다중 노드 클러스터에서 고성능 워크로드를 가속화할 수 있습니다
시스템 SVM에서 LIF의 상태 admin을 DOWN으로 설정하기 전에 확인이 필요합니다	이렇게 하면 적절한 클러스터 작업에 중요한 LIF를 실수로 사용할 수 없게 됩니다. CLI에서 이 동작을 호출하는 스크립트가 있는 경우 확인 단계를 고려하여 업데이트해야 합니다.
네트워크 배선 문제에 대한 자동 감지 및 수리 권장 사항	포트 연결성 문제가 감지되면 ONTAP System Manager는 문제를 해결하기 위해 복구 작업을 권장합니다.
IPsec(인터넷 프로토콜 보안) 인증서	IPsec 정책은 인증을 위한 인증서와 함께 미리 공유된 키(PSK)를 지원합니다.
LIF 서비스 정책	방화벽 정책은 더 이상 사용되지 않으며 LIF 서비스 정책으로 대체됩니다. 아웃바운드 NTP 요청에 사용되는 LIF를 보다 효과적으로 제어할 수 있도록 새로운 NTP LIF 서비스 정책이 추가되었습니다.

S3 오브젝트 스토리지

업데이트	설명
S3 오브젝트 데이터 보호, 백업 및 재해 복구	SnapMirror S3는 ONTAP S3 구성에 대한 버킷 미러링, NetApp 및 비 NetApp 대상에 대한 버킷 백업을 비롯하여 ONTAP S3 오브젝트 스토리지를 위한 데이터 보호 서비스를 제공합니다.
S3 감사	ONTAP S3 환경에서 데이터 및 관리 이벤트를 감사할 수 있습니다. S3 감사 기능은 기존의 NAS 감사 기능과 유사하며, S3 및 NAS 감사가 클러스터에 공존할 수 있습니다.

산

업데이트	설명
NVMe 네임스페이스	ONTAP CLI를 사용하여 네임스페이스 크기를 늘리거나 줄일 수 있습니다. System Manager를 사용하여 네임스페이스 크기를 늘릴 수 있습니다.
TCP에 대한 NVMe 프로토콜 지원	비휘발성 메모리 익스프레스(NVMe) 프로토콜은 TCP 네트워크를 통해 SAN 환경에서 사용할 수 있습니다.

보안

업데이트	설명
자율 랜섬웨어 보호	NAS 환경의 워크로드 분석을 사용하면 자율적 랜섬웨어 공격을 시사할 수 있는 비정상적인 활동에 대해 경고합니다. 자율적 랜섬웨어 방어는 공격이 감지되면 자동 스냅샷 백업을 생성하고 예약된 스냅샷으로부터 기존 보호를 제공합니다.
암호화 키 관리	Azure Key Vault 및 Google Cloud Platform 키 관리 서비스를 사용하여 ONTAP 키를 저장, 보호, 활용하고 키 관리 및 액세스를 간소화하십시오.

스토리지 효율성

업데이트	설명
온도에 민감한 스토리지 효율성	새 볼륨이나 기존 AFF 볼륨에서 "기본" 모드 또는 "효율적" 모드를 사용하여 온도에 민감한 스토리지 효율성을 활성화할 수 있습니다.
클러스터 간에 SVM을 중단 없이 이동	로드 밸런싱, 성능 향상, 장비 업그레이드, 데이터 센터 마이그레이션을 위해 소스에서 타겟으로 물리적 AFF 클러스터 간에 SVM을 재배치할 수 있습니다.

스토리지 리소스 관리 기능 향상

업데이트	설명
FSA(File System Analytics)를 사용한 핫 객체에 대한 작업 추적	시스템 성능 평가를 개선하기 위해 FSA는 핫 객체(파일, 디렉토리, 사용자 및 트래픽 및 처리량이 가장 많은 클라이언트)를 식별할 수 있습니다.
글로벌 파일 읽기 잠금	모든 캐시와 오리진 간에 단일 지점에서 읽기 잠금을 설정합니다. 마이그레이션 시 영향을 받는 문서입니다.
FlexCache용 NFSv4 지원	FlexCache 볼륨은 NFSv4 프로토콜을 지원합니다.
기존 FlexGroup 볼륨에서 클론을 생성합니다	기존 FlexGroup 볼륨을 사용하여 FlexClone 볼륨을 생성할 수 있습니다.
SVM 재해 복구 소스에서 FlexVol 볼륨을 FlexGroup으로 변환합니다	SVM 재해 복구 소스에서 FlexVol 볼륨을 FlexGroup 볼륨으로 변환할 수 있습니다.

SVM 관리 개선 사항

업데이트	설명
클러스터 간에 SVM을 중단 없이 이동 가능	로드 밸런싱, 성능 향상, 장비 업그레이드, 데이터 센터 마이그레이션을 위해 소스에서 타겟으로 물리적 AFF 클러스터 간에 SVM을 재배치할 수 있습니다.

시스템 관리자

업데이트	설명
System Manager 로그에서 성능 원격 측정 로깅을 활성화합니다	관리자는 System Manager에서 성능 문제가 발생한 경우 원격 측정 로깅을 활성화한 다음 지원 팀에 문의하여 문제를 분석할 수 있습니다.
NetApp 라이센스 파일	모든 라이센스 키는 개별 28자 라이센스 키 대신 NetApp 라이센스 파일로 제공되므로 하나의 파일을 사용하여 여러 기능에 대한 라이센스를 부여할 수 있습니다.
펌웨어를 자동으로 업데이트합니다	System Manager 관리자는 ONTAP에서 펌웨어를 자동으로 업데이트하도록 구성할 수 있습니다.
위험 완화 권장 사항을 검토하고 Digital Advisor가 보고한 위험을 확인합니다	System Manager 사용자는 Digital Advisor가 보고한 위험을 확인하고 위험 완화에 대한 권장 사항을 검토할 수 있습니다. 9.10.1부터 사용자는 위험을 인지할 수도 있습니다.
EMS 이벤트 알림의 관리자 수신 설정	System Manager 관리자는 EMS(이벤트 관리 시스템) 이벤트 알림이 전송되는 방식을 구성하여 주의가 필요한 시스템 문제에 대해 알림을 받을 수 있습니다.

업데이트	설명
인증서를 관리합니다	System Manager 관리자는 신뢰할 수 있는 인증 기관, 클라이언트/서버 인증서 및 로컬(온보드) 인증 기관을 관리할 수 있습니다.
System Manager를 사용하여 용량 사용량 기록을 확인하고 향후 용량 요구사항을 예측할 수 있습니다	Digital Advisor와 System Manager의 통합을 통해 관리자는 클러스터의 용량 사용 내역에 대한 기간별 데이터를 볼 수 있습니다.
System Manager를 사용하여 Cloud Backup Service를 사용하여 StorageGRID에 데이터를 백업합니다	Cloud Manager를 사내에 구축한 경우 Cloud Backup Service 관리자는 StorageGRID로 백업할 수 있습니다. 또한, AWS 또는 Azure에서 Cloud Backup Service를 사용하여 오브젝트를 아카이브할 수 있습니다.
사용 편의성 향상	ONTAP 9.10.1부터 다음을 수행할 수 있습니다. • 상위 볼륨(VMware, Linux, Windows) 대신 LUN에 QoS 정책 할당 • LUN QoS 정책 그룹을 편집합니다 • LUN을 이동합니다 • LUN을 오프라인 상태로 전환합니다 • 롤링 ONTAP 이미지 업그레이드를 수행합니다 • 포트 세트를 생성하여 igroup에 바인딩합니다 • 네트워크 배선 문제에 대한 자동 감지 및 수리 권장 사항 • 스냅샷 디렉토리에 대한 클라이언트 액세스를 설정하거나 해제합니다 • 스냅샷을 삭제하기 전에 재확보 가능한 공간을 계산합니다 • SMB 공유에서 지속적으로 사용 가능한 현장 변경 사항에 액세스합니다 • 보다 정확한 표시 단위를 사용하여 용량 측정값을 볼 수 있습니다 • Windows 및 Linux에 대한 호스트별 사용자 및 그룹을 관리합니다 • AutoSupport 설정을 관리합니다 • 별도의 작업으로 볼륨 크기를 조정합니다

ONTAP 9.9.1의 새로운 기능

ONTAP 9.9.1에서 사용할 수 있는 새로운 기능에 대해 알아보십시오.

최신 ONTAP 9 릴리스에서 알려진 문제, 제한 사항 및 업그레이드 주의 사항에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 릴리즈 노트". 릴리스 정보에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

- 새로운 기능 및 향상된 기능에 대해 알아봅니다 "ONTAP MetroCluster 기능".
- 에 대해 알아보세요 "AFF, ASA 및 FAS 시스템과 지원되는 스위치에 대한 새롭고 향상된 지원" .
- 의 업데이트에 대해 알아봅니다 "ONTAP REST API를 참조하십시오".

최신 버전의 ONTAP로 업그레이드하려면 를 참조하십시오ONTAP 업그레이드를 준비합니다.

데이터 보호

업데이트	설명
"SnapLock 볼륨 및 애그리게이트에서 스토리지 효율성 지원"	데이터 컴팩션, 볼륨 간 중복제거, 적응형 압축 및 TSSE(온도에 민감한 스토리지 효율성)를 포함하도록 SnapLock 볼륨 및 애그리게이트의 스토리지 효율성 기능이 확장되어 WORM 데이터의 공간을 더 절약할 수 있습니다.
"SVM DR 소스 및 대상에 대해 서로 다른 스냅샷 정책을 구성할 수 있도록 지원합니다"	SVM DR 구성은 미러 소산 정책을 사용하여 소스와 대상에서 서로 다른 스냅샷 정책을 구성할 수 있으며, 타겟의 정책을 소스 정책으로 덮어쓰지 않습니다.
"SnapMirror Cloud에 대한 System Manager 지원"	SnapMirror Cloud가 이제 System Manager에서 지원됩니다.
감사 지원 SVM	클러스터에서 지원되는 감사 가능 SVM의 최대 수가 50개에서 400개로 증가했습니다.
SnapMirror Synchronous	HA 쌍당 지원되는 SnapMirror Synchronous 엔드포인트의 최대 수가 80개에서 160개로 증가했습니다.
FlexGroup SnapMirror 토폴로지	FlexGroup 볼륨은 2개 이상의 팬아웃 관계를 지원합니다(예: A → B, A → C) FlexVol 볼륨과 마찬가지로 FlexGroup 팬아웃은 최대 8개의 팬아웃 레그를 지원하며 최대 2개 레벨(예: A → B → C)까지 계단식 구성을 지원합니다

파일 액세스 프로토콜

업데이트	설명
"LDAP 조회 추적 기능 향상"	LDAP 조회 추적은 LDAP 서명 및 봉인, 암호화된 TLS 연결 및 LDAPS 포트 636을 통한 통신에서 지원됩니다.
"모든 포트에서 LDAPS 지원"	LDAPS는 모든 포트에서 구성할 수 있으며 포트 636은 기본값으로 유지됩니다.
"NFSv4.x 버전은 기본적으로 활성화되어 있습니다"	NFSv4.0, NFSv4.1 및 NFSv4.2는 기본적으로 설정됩니다.
"레이블이 지정된 NFSv4.2 지원"	NFSv4.2가 설정되면 NFS 레이블이 지정된 MAC(필수 액세스 제어)가 지원됩니다. 이 기능을 통해 ONTAP NFS 서버는 MAC 인식, 저장 및 검색이 가능합니다 `sec_label` 클라이언트에서 보낸 속성

네트워킹

업데이트	설명
"클러스터 복원력"	• 스위치가 없는 2노드 클러스터의 포트 모니터링 및 방지(이전에는 스위치 구성에서만 사용 가능) • 노드가 클러스터 네트워크를 통해 데이터를 제공할 수 없는 경우 자동 노드 페일오버를 수행합니다 • 패킷 손실이 발생한 클러스터 경로를 표시하는 새로운 도구

업데이트	설명
"VIP(가상 IP) LIF 확장"	• BGP(Border Gateway Protocol)의 ASN(Autonomous System Number)은 4바이트 비음의 정수를 지원합니다. • MED(Multi-exit 판별자)는 경로 우선 순위 지정을 지원하여 고급 경로 선택을 가능하게 합니다. Med는 BGP 업데이트 메시지에서 선택적 속성입니다. • VIP BGP는 BGP 피어 그룹화를 사용하여 기본 경로 자동화를 제공하여 구성을 간소화합니다.

S3 오브젝트 스토리지

업데이트	설명
"S3 메타데이터 및 태그 지원"	ONTAP S3 서버는 사용자 정의 오브젝트 메타데이터 및 오브젝트 태깅을 지원하여 S3 클라이언트 및 애플리케이션에 향상된 자동화 기능을 제공합니다.

산

업데이트	설명
FLI(Foreign LUN Import)	NetApp Support 사이트의 SAN LUN 마이그레이션 앱을 사용하여 FLI 상호 운용성 매트릭스에 나열되지 않은 외부 어레이를 검증할 수 있습니다.
NVMe - 원격 경로 액세스입니다	페일오버 시 직접 경로 액세스가 손실되면 원격 I/O를 통해 시스템이 원격 경로로 페일오버하고 데이터 액세스를 계속할 수 있습니다.
ASA에서 12노드 클러스터 지원	12노드 클러스터는 AFF ASA 구성에 지원됩니다. ASA 클러스터에는 다양한 ASA 시스템 유형이 혼합되어 있을 수 있습니다.
ASA에 대한 NVMe-oF 프로토콜	AFF ASA 시스템을 통해 NVMe-oF 프로토콜 지원을 사용할 수도 있습니다.
Igroup 개선 사항	• 기존 igroup으로 구성된 igroup을 생성할 수 있습니다. • igroup 또는 호스트 이니시에이터의 별칭 역할을 하는 igroup 또는 호스트 이니시에이터에 설명을 추가할 수 있습니다. • igroup을 2개 이상의 LUN에 동시에 매핑할 수 있습니다.
단일 LUN 성능 향상	AFF의 단일 LUN 성능이 크게 향상되어 가상화 환경에서 구축을 간소화하는 데 이상적입니다. 예를 들어, A800은 최대 400% 더 많은 랜덤 읽기 IOP를 제공할 수 있습니다.

보안

업데이트	설명
System Manager에 로그인할 때 Cisco Duo를 통해 다단계 인증을 지원합니다	ONTAP 9.9.1P3부터 Cisco Duo를 SAML ID 공급자(IDP)로 구성하여 사용자가 System Manager에 로그인할 때 Cisco Duo를 사용하여 인증할 수 있습니다.

스토리지 효율성

업데이트	설명
"파일 수를 볼륨에 대해 최대로 설정합니다"	volume 매개 변수를 사용하여 파일 최대값을 자동화합니다 `-files-set-maximum`파일 제한을 모니터링할 필요가 없습니다.

스토리지 리소스 관리 기능 향상

업데이트	설명
System Manager의 FSA(File System Analytics) 관리 기능 향상	FSA는 검색 및 필터링, FSA 권장 사항에 대한 조치 수행을 위한 추가 System Manager 기능을 제공합니다.
네거티브 조회 캐시 지원	오리진 호출로 인한 네트워크 트래픽을 줄이기 위해 FlexCache 볼륨에 "파일을 찾을 수 없음" 오류를 캐시합니다.
FlexCache 재해 복구	한 캐시에서 다른 캐시로 클라이언트를 중단 없이 마이그레이션할 수 있습니다.
FlexGroup 볼륨에 대한 SnapMirror 계단식 및 팬아웃 지원	FlexGroup 볼륨에 대한 SnapMirror 계단식 및 SnapMirror 팬아웃 관계를 지원합니다.
FlexGroup 볼륨에 대한 SVM 재해 복구 지원	FlexGroup 볼륨에 대한 SVM 재해 복구 지원은 SnapMirror를 사용하여 SVM의 구성과 데이터를 복제하고 동기화함으로써 이중화를 제공합니다.
FlexGroup 볼륨에 대한 논리적 공간 보고 및 적용 지원	FlexGroup 볼륨 사용자가 사용하는 논리적 공간을 표시하고 제한할 수 있습니다.
qtree에서 SMB 액세스 지원	SMB 액세스는 FlexVol의 qtree 및 SMB가 활성화된 FlexGroup 볼륨에서 지원됩니다.

시스템 관리자

업데이트	설명
System Manager에 Digital Advisor에서 보고한 위험이 표시됩니다	System Manager를 사용하여 Active IQ Digital Advisor(Digital Advisor라고도 함)에 연결하면 스토리지 환경의 위험을 줄이고 성능 및 효율성을 개선할 수 있는 기회를 보고할 수 있습니다.
로컬 계층을 수동으로 할당합니다	System Manager 사용자는 볼륨 및 LUN을 생성하고 추가할 때 로컬 계층을 수동으로 할당할 수 있습니다.
비동기식 디렉토리 삭제	대기 시간이 짧은 비동기 디렉토리 삭제 기능을 사용하여 System Manager에서 디렉토리를 삭제할 수 있습니다.
Ansible Playbook 생성	System Manager 사용자는 UI에서 몇 가지 엄선된 워크플로에 대한 Ansible Playbook을 생성하고 자동화 툴에서 이 Playbook을 사용하여 볼륨 또는 LUN을 반복적으로 추가 또는 편집할 수 있습니다.
하드웨어 시각화	ONTAP 9.8에 처음 도입된 하드웨어 시각화 기능이 이제 모든 AFF 플랫폼을 지원합니다.

업데이트	설명
Digital Advisor 통합	System Manager 사용자는 클러스터와 관련된 지원 사례를 보고 다운로드할 수 있습니다. 또한 NetApp Support 사이트에서 새로운 지원 케이스를 제출하는 데 필요한 클러스터 세부 정보를 복사할 수 있습니다. System Manager 사용자는 새로운 펌웨어 업데이트가 사용 가능한 경우 Digital Advisor로부터 경고를 받을 수 있습니다. 그런 다음 펌웨어 이미지를 다운로드한 후 System Manager를 사용하여 업로드할 수 있습니다.
Cloud Manager 통합	System Manager 사용자는 Cloud Backup Service를 사용하여 퍼블릭 클라우드 엔드포인트에 데이터를 백업하도록 보호를 설정할 수 있습니다.
데이터 보호 프로비저닝 워크플로우의 개선 사항	System Manager 사용자는 데이터 보호를 설정할 때 SnapMirror 대상 및 igroup 이름을 수동으로 지정할 수 있습니다.
향상된 네트워크 포트 관리	네트워크 인터페이스 페이지에는 홈 포트의 인터페이스를 표시하고 관리할 수 있는 향상된 기능이 있습니다.
시스템 관리 기능 향상	• 중첩된 igroup 지원 • 단일 작업에서 여러 LUN을 igroup에 매핑하고 프로세스 중 필터링에 WWPN 별칭을 사용할 수 있습니다. • NVMe-oF LIF를 생성하는 동안 더 이상 두 컨트롤러에서 동일한 포트를 선택할 필요가 없습니다. • 각 포트에 대해 전환 버튼으로 FC 포트를 사용하지 않도록 설정합니다.
스냅샷에 대한 정보를 System Manager에 표시하는 기능이 향상되었습니다	• System Manager 사용자는 스냅샷의 크기와 SnapMirror 레이블을 볼 수 있습니다. • 스냅샷이 비활성화된 경우 스냅샷 예약이 0으로 설정됩니다.
스토리지 계층의 용량 및 위치 정보에 대한 System Manager의 표시 기능 향상	• 새 계층 열은 각 볼륨이 상주하는 로컬 계층(애그리게이트)을 식별합니다. • System Manager에는 물리적 사용된 용량과 클러스터 레벨의 논리적 사용된 용량 및 로컬 계층(애그리게이트) 레벨이 표시됩니다. • 새 용량 표시 필드를 사용하면 용량을 모니터링하고 용량이 거의 도달했거나 활용도가 낮은 볼륨을 추적할 수 있습니다.
EMS 비상 경보 및 기타 오류 및 경고의 System Manager에 표시됩니다	24시간 동안 받은 EMS 알림의 수와 기타 오류 및 경고가 System Manager의 상태 카드에 표시됩니다.

ONTAP 제한 및 기본값으로 변경합니다

ONTAP 9 릴리스에서 구현된 제한 및 기본값에 대한 몇 가지 변경 사항에 대해 알아봅니다. NetApp은 고객이 각 ONTAP 릴리스에서 가장 중요한 기본 및 제한 변경 사항을 이해할 수 있도록 돕기 위해 노력하고 있습니다.

ONTAP 기본값으로 변경합니다

새로운 ONTAP 릴리즈로 업그레이드하기 전에 ONTAP 기본 설정의 변경 사항이 자동화나 비즈니스 운영에 영향을 미칠 수 있는지 확인해야 합니다.

피처	기본 변경	릴리스 위치가 변경되었습니다.
자율 랜섬웨어 보호(ARP)	지원되는 플랫폼에서는 12시간의 유예 기간 후 모든 새 볼륨에 대해 ARP/AI가 기본적으로 자동으로 활성화됩니다.	ONTAP 9.18.1
볼륨 기본값	NAS 프로토콜에 할당된 ONTAP 클러스터에서 새로 생성된 SVM에 생성된 볼륨에는 기본적으로 FSA(파일 시스템 분석)가 활성화되어 있습니다.	ONTAP 9.17.1
HTTP 엄격한 전송 보안(HSTS)	HSTS는 9.17.1에서 기본적으로 활성화되어 있습니다.	ONTAP 9.17.1
NAS 감사	및 `file-session-io-grouping-duration` 매개 변수의 최대 제한이 `file-session-io-grouping-count` 증가하므로 필요에 따라 더 적은 수의 통합 NAS 감사 이벤트 알림을 선택할 수 있습니다. 이 경우 SVM이 높은 IO 속도를 지원하므로 타겟 볼륨에 대한 스토리지의 영향을 줄일 수 있습니다. NFS_FILE_SESSION_IO_GROUP_COUNT_MAX: 20000 ~ 120000 NFS_FILE_SESSION_IO_GROUP_DURATION_MAX : 600 ~ 3600	ONTAP 9.16.1
FAS 시스템의 노드당 최대 볼륨	컨트롤러당 200GB RAM이 넘는 FAS 시스템의 경우 노드당 지원되는 최대 볼륨 수가 1000개에서 2500개로 증가합니다. 이전 버전의 ONTAP에서는 "데이터 보호 최적화(DPO)"ONTAP FAS 시스템 지원을 노드당 1000개에서 2500개로 늘리려면 라이센스가 필요했습니다.	ONTAP 9.16.1
로드 공유 미러	부하 공유 미러 관계를 생성할 때 SVM에서 저장 용량 제한을 활성화할 수 없습니다.	ONTAP 9.16.1
`vserver object-store-server user show` 명령	ONTAP 9.15.1 이전 릴리스에서는 이(가) `vserver object-store-server user show` 명령은 S3 사용자의 비밀 키를 반환합니다. 이 명령은 S3 사용자에 대한 비밀 키 데이터를 더 이상 반환하지 않습니다.	ONTAP 9.15.1
NAS 감사	NAS 감사 구성을 사용하면 기본적으로 모든 감사 로그 레코드를 유지할 수 있습니다. rotate-limit 매개 변수에 대한 수정된 값은 감사 로그를 지원하는 볼륨에 대해 적절한 크기를 지정하도록 합니다.	ONTAP 9.15.1
공간 할당	새로 생성된 LUN에 대해 공간 할당이 기본적으로 설정됩니다. 이전 버전의 ONTAP(9.14.1 이하)에서는 공간 할당이 기본적으로 해제되었습니다.	ONTAP 9.15.1
NVMe/TCP 자동 호스트 검색	NVMe/TCP 프로토콜을 사용하여 컨트롤러에 대한 호스트 검색은 기본적으로 자동화되어 있습니다.	ONTAP 9.14.1
Kerberos 기반 통신을 위한 AES 암호화	인증을 위한 AES 암호화는 SMB 서버와의 Kerberos 기반 통신에 기본적으로 사용됩니다. 사용자 환경에서 AES 암호화를 지원하지 않는 경우 AES 암호화를 수동으로 비활성화할 수 있습니다.	ONTAP 9.13.1

피처	기본 변경	릴리스 위치가 변경되었습니다.
RAID 애그리게이트	ONTAP 9.12.1부터 집계가 저하된 경우 24시간 후에 시스템 컨트롤러가 기본적으로 종료되지 않습니다. 사용자가 를 변경하는 경우 `raid.timeout` 옵션을 선택하면 가 만료된 후에도 시스템 컨트롤러가 계속 종료됩니다 `raid.timeout` 수행	ONTAP 9.12.1
TLS 1.1은 기본적으로 비활성화되어 있습니다	ONTAP를 새로 설치하는 경우 TLS 1.1은 기본적으로 비활성화되어 있습니다. TLS 1.1이 이미 활성화된 ONTAP 9.12.0 이상으로 업그레이드된 시스템은 TLS 1.1이 활성화된 상태로 유지되므로 영향을 받지 않습니다. 그러나 FIPS를 사용하는 클러스터를 업그레이드하는 경우 ONTAP 9.11.1부터 FIPS에서 TLS 1.1이 지원되지 않으므로 TLS 1.1이 자동으로 비활성화됩니다. 기본적으로 비활성화되면 필요에 따라 수동으로 TLS 1.1을 활성화할 수 있습니다.	ONTAP 9.12.0
TLS 1.0은 기본적으로 비활성화되어 있습니다	ONTAP를 새로 설치할 때는 TLS 1.0이 기본적으로 비활성화되어 있습니다. TLS 1.0이 활성화된 ONTAP 9.8 이상으로 업그레이드된 시스템은 TLS 1.0이 활성화된 상태로 유지되므로 영향을 받지 않습니다. 그러나 FIPS가 활성화된 클러스터를 업그레이드하는 경우 ONTAP 9.8부터 FIPS에서 TLS 1.0이 지원되지 않으므로 TLS 1.0이 자동으로 비활성화됩니다. 기본적으로 비활성화되면 필요에 따라 수동으로 TLS 1.0을 활성화할 수 있습니다.	ONTAP 9.8

ONTAP 제한 변경 사항

새로운 ONTAP 릴리즈로 업그레이드하기 전에 ONTAP 제한 사항이 변경되어 자동화 또는 비즈니스 운영에 영향을 미칠 수 있는지 확인해야 합니다.

피처	제한 변경	릴리스 위치가 변경되었습니다.
Qtree 확장 성능 모니터링	단일 ONTAP 클러스터에서 최대 50,000개의 qtree에 대해 확장된 성능 모니터링을 활성화할 수 있습니다.	ONTAP 9.16.1
SnapMirror 활성 동기화	SnapMirror Active Sync는 일관성 그룹에서 80개의 볼륨을 지원합니다	ONTAP 9.15.1
SnapMirror 비동기	SnapMirror 비동기식 보호를 사용하는 일관성 그룹은 일관성 그룹에서 최대 80개의 볼륨을 지원합니다.	ONTAP 9.15.1
파일 시스템 분석	ONTAP는 성능 문제를 완화하기 위해 파일 시스템 분석을 활성화할 때 볼륨 용량의 5-8%를 가용 용량으로 유지해야 합니다.	ONTAP 9.15.1
SVM 데이터 이동성	SVM 데이터 이동성을 지원하는 SVM당 지원되는 볼륨의 최대 수는 400개로 증가하고 지원되는 HA 쌍 수가 12개로 증가합니다.	ONTAP 9.14.1

피처	제한 변경	릴리스 위치가 변경되었습니다.
FlexGroup 재조정	FlexGroup 재조정 작업의 구성 가능한 최소 파일 크기가 4KB에서 20MB로 증가합니다.	• ONTAP 9.14.1 • ONTAP 9.13.1P1 • ONTAP 9.12.1P10
FlexVol 및 FlexGroup 볼륨 크기 제한	AFF 및 FAS 플랫폼에서 지원되는 최대 FlexVol 및 FlexGroup 볼륨 구성 크기가 100TB에서 300TB로 증가했습니다.	ONTAP 9.12.1P2 를 참조하십시오
LUN 크기 제한	AFF 및 FAS 플랫폼에서 지원되는 최대 LUN 크기가 16TB에서 128TB로 증가했습니다. SnapMirror 구성에서 지원되는 최대 LUN 크기(동기식 및 비동기식 모두)가 16TB에서 128TB로 증가합니다.	ONTAP 9.12.1P2 를 참조하십시오
FlexVol 볼륨 크기 제한	AFF 및 FAS 플랫폼에서 지원되는 최대 볼륨 크기가 100TB에서 300TB로 증가했습니다. SnapMirror 동기식 구성에서 지원되는 최대 FlexVol 볼륨 크기가 100TB에서 300TB로 증가했습니다.	ONTAP 9.12.1P2 를 참조하십시오
파일 크기 제한	AFF 및 FAS 플랫폼에서 NAS 파일 시스템에 지원되는 최대 파일 크기가 16TB에서 128TB로 증가했습니다. SnapMirror 동기식 구성에서 지원되는 최대 파일 크기가 16TB에서 128TB로 증가했습니다.	ONTAP 9.12.1P2 를 참조하십시오
클러스터 볼륨 제한	컨트롤러에서 CPU 및 메모리를 보다 완벽하게 활용하고 클러스터의 최대 볼륨 수를 15,000개에서 30,000개로 늘립니다.	ONTAP 9.12.1
FlexVol 볼륨의 SVM-DR 관계	FlexVol 볼륨의 경우 최대 SVM-DR 관계 수가 64개에서 128개로 증가했습니다(클러스터당 128개의 SVM).	ONTAP 9.11.1
SnapMirror 동기식	HA 쌍당 허용되는 최대 SnapMirror 동기식 작업 수가 200개에서 400개로 증가했습니다.	ONTAP 9.11.1
NAS FlexVol 볼륨	NAS FlexVol 볼륨의 클러스터 제한이 12,000개에서 15,000개로 증가했습니다.	ONTAP 9.10.1
SAN FlexVol 볼륨	SAN FlexVol 볼륨의 클러스터 제한이 12,000개에서 15,000개로 증가했습니다.	ONTAP 9.10.1
FlexGroup 볼륨을 사용하는 SVM-DR	• FlexGroup 볼륨에서는 최대 32개의 SVM-DR 관계가 지원됩니다. • SVM-DR 관계에서 단일 SVM에서 지원되는 최대 볼륨 수는 300이며, 여기에는 FlexVol 볼륨 및 FlexGroup 구성요소의 수가 포함됩니다. • FlexGroup의 최대 구성요소 수는 20개를 초과할 수 없습니다. • SVM-DR 볼륨 제한은 노드당 500개, 클러스터당 1000개입니다(FlexVol 볼륨 및 FlexGroup 구성요소 포함).	ONTAP 9.10.1

피처	제한 변경	릴리스 위치가 변경되었습니다.
감사 지원 SVM	클러스터에서 지원되는 감사 가능 SVM의 최대 수가 50개에서 400개로 증가했습니다.	ONTAP 9.9.1
SnapMirror 동기식	HA 쌍당 지원되는 SnapMirror 동기식 끝의 수가 80개에서 160개로 증가했습니다.	ONTAP 9.9.1
FlexGroup SnapMirror 토폴로지	FlexGroup 볼륨은 2개 이상의 팬아웃 관계를 지원합니다 (예: A-B, A-C) FlexVol 볼륨과 마찬가지로 FlexGroup 팬아웃은 최대 8개의 팬아웃 레그를 지원하고 최대 2개 레벨(예: A_BC)까지 계단식 구성을 지원합니다	ONTAP 9.9.1
SnapMirror 동시 전송	비동기 볼륨 수준 동시 전송의 최대 수가 100에서 200으로 증가했습니다. SnapMirror 클라우드 전송은 하이엔드 시스템에서는 32개에서 100개로, SnapMirror 엔드 시스템에서는 6개에서 20개로 증가했습니다.	ONTAP 9.8
FlexVol 볼륨 제한이 있습니다	ASA 플랫폼에서 FlexVol 볼륨이 사용하는 공간이 100TB에서 300TB로 증가했습니다.	ONTAP 9.8

ONTAP 9 릴리스 지원

ONTAP 9.8 릴리스부터 NetApp는 매년 두 번 ONTAP 릴리스를 제공합니다. 이 계획은 변경될 수 있지만 매년 2/4분기에 새로운 ONTAP 릴리즈를 제공하려는 것입니다. 최신 ONTAP 릴리즈를 활용할 수 있도록 업그레이드 기간을 계획하려면 이 정보를 사용하십시오.

버전	출시일
9.18.1	2025년 11월
9.17.1	2025년 9월
9.16.1	2025년 1월
9.15.1	2024년 7월
9.14.1	2024년 1월
9.13.1	2023년 6월
9.12.1	2023년 2월
9.11.1	2022년 7월
9.10.1	2022년 1월

버전	출시일
9.9.1	2021년 6월

지원 수준

특정 버전의 ONTAP에 사용할 수 있는 지원 수준은 소프트웨어가 출시된 시기에 따라 다릅니다.

지원 레벨	완벽한 지원			제한된 지원		셀프서비스 지원		
년	1	2	3	4	5	6	7	8
온라인 설명서 액세스	예	예	예	예	예	예	예	예
기술 지원	예	예	예	예	예			
근본 원인 분석	예	예	예	예	예			
소프트웨어 다운로드	예	예	예	예	예			
서비스 업데이트(패치 릴리스 [P-releases])	예	예	예					
취약점에 대한 경고	예	예	예					

ONTAP의 최신 릴리즈로 업그레이드하려면 를 참조하십시오 ONTAP의 최신 버전으로 업그레이드하십시오 및 언제 ONTAP를 업그레이드해야 합니까?

시작하십시오

ONTAP에 대해 알아보십시오

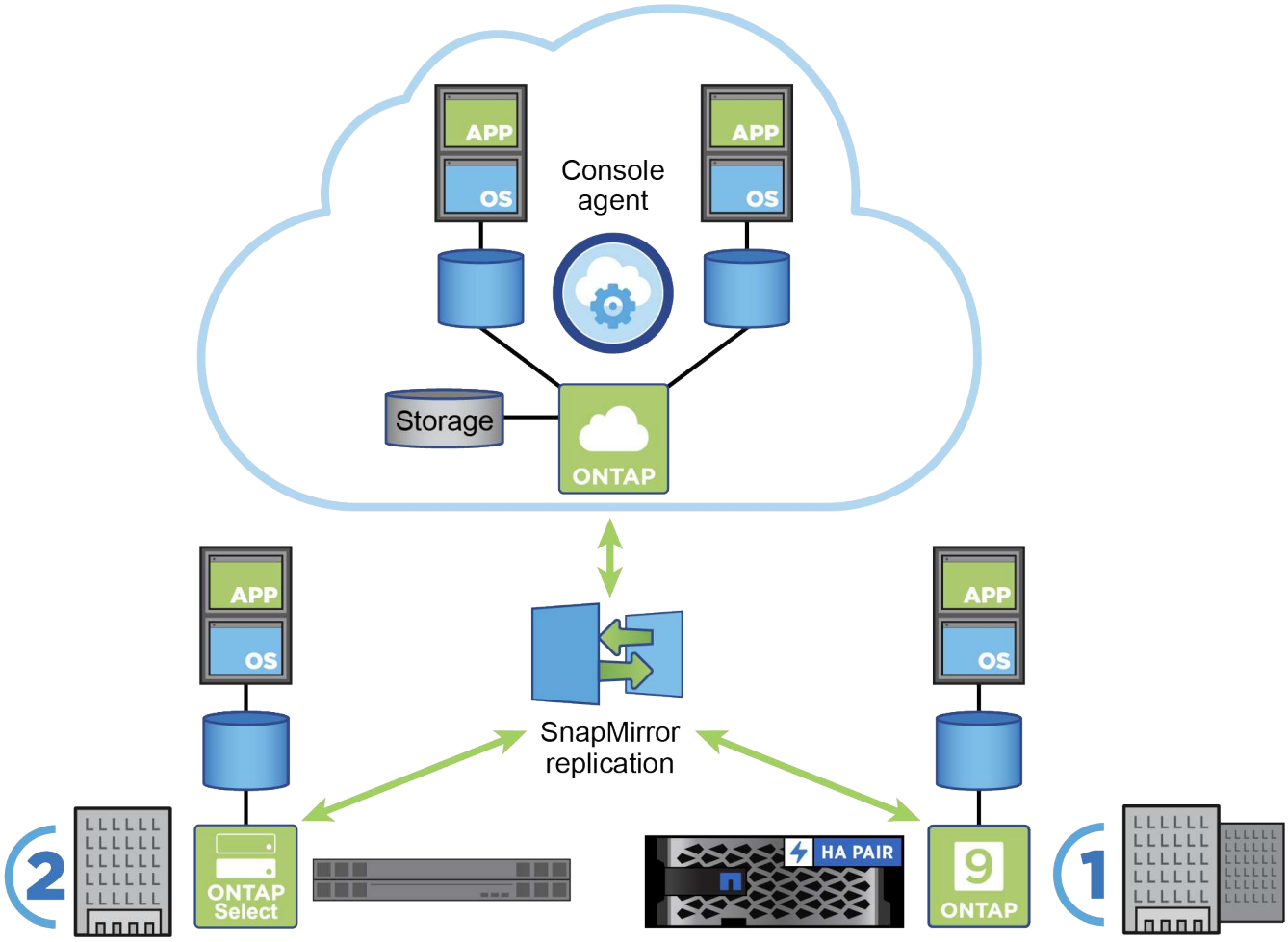
ONTAP 플랫폼

ONTAP 데이터 관리 소프트웨어는 블록 또는 파일 데이터를 읽고 쓰는 애플리케이션을 위한 유니파이드 스토리지를 제공합니다. 스토리지 구성의 옵션은 고속 플래시부터 저렴한 회전식 미디어까지, 클라우드 기반 오브젝트 스토리지에 이르기까지 다양합니다.

ONTAP 구현은 다음과 같이 실행됩니다.

- * NetApp 엔지니어링 시스템*: "AFF, AFX, ASA 및 FAS 저장 시스템"
- * ONTAP 스토리지 특성*: "AFX 및 ASA r2 스토리지 시스템" 특정 프로토콜에 초점을 맞춘 분산된 ONTAP 스토리지를 제공하는 전담 ONTAP 개성을 실행합니다.
- * 상용 하드웨어 *: "ONTAP Select"
- 프라이빗, 퍼블릭 또는 하이브리드 클라우드: "Cloud Volumes ONTAP" , "NetApp ONTAP용 Amazon FSx" , "Azure NetApp Files" , 그리고 "Google Cloud NetApp 볼륨"
- * 동급 최고의 컨버지드 인프라를 제공하는 를 포함한 특수 구현 * "FlexPod 데이터 센터"

이러한 구현은 _ 지능형 데이터 인프라 _ 의 기본 프레임워크를 형성하며 소프트웨어 정의 방식의 데이터 관리 및 플랫폼 간의 빠르고 효율적인 복제를 지원합니다.



ONTAP 사용자 인터페이스

ONTAP 데이터 관리 소프트웨어는 ONTAP 클러스터를 관리하는 데 사용할 수 있는 다양한 인터페이스를 제공합니다. 이러한 인터페이스 옵션은 다양한 수준의 액세스 및 기능을 제공하며 환경에 따라 ONTAP 클러스터를 적절하게 관리할 수 있는 유연성을 제공합니다.

이 인터페이스 중 하나를 사용하여 ONTAP 클러스터를 관리하고 데이터 관리 작업을 수행할 수 있습니다

ONTAP 시스템 관리자

ONTAP System Manager는 웹 기반 사용자 인터페이스로, 클러스터를 관리하기 위한 간단하고 직관적인 방법을 제공합니다. 스토리지 구성, 데이터 보호, 네트워크 설정 및 관리 등의 일반 작업을 관리할 수 있습니다. 또한 System Manager는 위험 및 클러스터 성능 모니터링과 인사이트를 제공합니다. 이를 통해 클러스터 문제에 대응하고 문제가 발생하기 전에 미리 파악할 수 있습니다. "자세한 정보".

ONTAP 9.7은 ONTAP System Manager에서 중요한 역할을 했던 것으로 나타났습니다. 이 릴리즈에서 NetApp은 두 가지 버전의 ONTAP System Manager를 제공했으며, ONTAP 9.7 이전 버전과 함께 더욱 간소화되고 직관적인 버전을 새롭게 설계했습니다. ONTAP 9.7 이후, 다시 설계된 버전은 ONTAP System Manager로 계속 바뀌었으며, 이전 버전은 System Manager Classic으로 바뀌었습니다. System Manager Classic은 ONTAP 9.7에서 마지막으로 업데이트되었습니다. System Manager Classic을 사용하는 경우 해당 설명서를 사용할 수 "별로입니다"있습니다.

NetApp 콘솔

ONTAP 9.12.1부터 NetApp 콘솔 웹 기반 인터페이스를 사용하여 익숙한 System Manager 대시보드를 유지하면서 단일 제어 평면에서 하이브리드 멀티클라우드 인프라를 관리할 수 있습니다. 콘솔을 사용하면 클라우드 스토리지(예: NetApp Backup and Recovery)를 생성하고 관리하고, NetApp의 데이터 서비스(예: Cloud Backup)를 사용하고, 다양한 온프레미스 및 엣지 스토리지 장치를 제어할 수 있습니다. 온프레미스 ONTAP 시스템을 콘솔에 추가하면 단일 인터페이스에서 모든 스토리지와 데이터 자산을 관리할 수 있습니다. "자세한 정보" .

ONTAP 명령줄 인터페이스입니다

를 클릭합니다 "ONTAP CLI(명령줄 인터페이스)" 는 를 사용하여 클러스터, 노드, SVM 및 기타 사용자와 상호 작용할 수 있는 텍스트 기반 인터페이스입니다 "명령". CLI 명령은 를 기반으로 사용할 수 있습니다 "역할 유형". SSH 또는 클러스터의 노드에 대한 콘솔 연결을 통해 ONTAP CLI에 액세스할 수 있습니다.

ONTAP REST API를 참조하십시오

ONTAP 9.6부터 RESTful API에 액세스하여 클러스터 운영을 프로그래밍 방식으로 관리 및 자동화할 수 있습니다. 이 API를 사용하여 볼륨, 스냅샷 및 애그리게이트 생성 및 관리와 같은 다양한 ONTAP 관리 작업은 물론 클러스터 성능 모니터링도 수행할 수 있습니다. curl과 같은 유틸리티를 사용하거나 Python, PowerShell, Java 등과 같은 REST 클라이언트를 지원하는 프로그래밍 언어를 사용하여 ONTAP REST API에 직접 액세스할 수 있습니다. "자세한 정보"..

ONTAPI는 ONTAP REST API보다 앞선 ONTAP 전용 API입니다. ONTAPI를 사용하는 경우 다음을 계획해야 합니다. "ONTAP REST API로 마이그레이션" .

NetApp 툴킷 및 프레임워크

NetApp는 ONTAP REST API를 추상화하고 자동화 코드를 더 쉽게 작성할 수 있도록 특정 개발 언어 및 환경에 적합한 클라이언트 툴킷을 제공합니다.
"자세한 정보".

이러한 툴킷 외에도 프레임워크를 사용하여 자동화 코드를 생성하고 배포할 수 있습니다. "자세한 정보".

ONTAP System Manager를 NetApp 콘솔과 통합

NetApp 콘솔의 시스템 관리자를 사용하여 ONTAP 9.10.1 및 이후 릴리스를 관리할 수 있습니다. 이러한 통합을 통해 통합된 제어 평면을 사용하여 하이브리드 멀티클라우드 인프라를 효율적으로 감독할 수 있으며, 동시에 익숙한 System Manager 사용자 인터페이스를 유지할 수 있습니다.

콘솔을 사용하면 클라우드 스토리지(예: Cloud Volumes ONTAP)를 생성하고 관리하고, NetApp 데이터 서비스(예: Cloud Backup)를 사용하고, 다양한 온프레미스 및 엣지 스토리지 장치를 제어할 수 있습니다.

콘솔은 클러스터를 검색하고 관리하는 두 가지 방법을 제공합니다.

- System Manager(ONTAP 9.12.1 이상)를 통한 관리를 위한 직접 검색
- 콘솔 에이전트를 통한 검색.

콘솔 에이전트는 사용자 환경에 설치되는 소프트웨어입니다. 이를 통해 System Manager를 통해 관리 기능에 액세스하고 데이터 복제, 백업 및 복구, 데이터 분류, 데이터 계층화 등의 기능을 제공하는 NetApp 클라우드 서비스에 액세스할 수 있습니다.

자세히 알아보세요 "NetApp 콘솔을 사용한 온프레미스 ONTAP 클러스터 관리" .

단계

1. NetApp 콘솔에 로그인합니다.
   a. 콘솔 로그인이 있다면 사용하세요.
   b. 처음이시라면 NetApp 지원 사이트 자격 증명으로 로그인을 선택하고 콘솔 로그인 페이지에 자격 증명을 입력하세요.
2. 콘솔 에이전트나 직접 검색을 사용하여 콘솔에서 온프레미스 클러스터를 검색하세요. 자세한 내용은 링크 https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html [온프레미스 ONTAP 클러스터 검색^]에서 확인하세요.
   a. 자세한 내용은 "직접 발견된 클러스터를 관리합니다." .
   b. 자세한 내용은 "콘솔 에이전트로 검색된 클러스터 관리" .
3. System Manager를 사용하여 온프레미스 클러스터를 관리하세요. 내 작업 환경 시스템 페이지에서 클러스터를 선택하고 서비스 목록에서 시스템 관리자를 클릭합니다.
   a. 자세히 알아보세요 "직접 발견된 클러스터 관리" .
   b. 자세한 내용은 "콘솔 에이전트로 검색된 클러스터 관리" .

NetApp 콘솔 및 **ONTAP 9.12.1**

참고: ONTAP 9.12.1을 사용하는 경우 NetApp 콘솔을 사용해 보라는 메시지가 나타납니다.

+ 클러스터가 NetApp 콘솔에 연결되어 있는 경우 로그인 프롬프트가 표시됩니다.

1. 콘솔 링크를 따라가려면 * NetApp 콘솔로 계속*을 클릭하세요.

   시스템 설정에서 외부 네트워크가 차단된 경우 콘솔에 액세스할 수 없습니다. 콘솔을 사용하여 System Manager에 액세스하려면 시스템에서 “cloudmanager.cloud.netapp.com” 주소에 액세스할 수 있는지 확인해야 합니다. 그렇지 않은 경우 프롬프트에서 ONTAP 시스템과 함께 설치된 System Manager 버전을 사용하도록 선택할 수 있습니다.

2. 콘솔 로그인 페이지에서 * NetApp 지원 사이트 자격 증명으로 로그인*을 선택하고 자격 증명을 입력합니다.

   이미 콘솔을 사용했고 이메일과 비밀번호를 사용하여 로그인한 경우, 계속해서 해당 로그인 옵션을 사용해야 합니다.

   "NetApp 콘솔에 로그인하는 방법에 대해 자세히 알아보세요." .

3. 메시지가 표시되면 새 NetApp 콘솔 계정의 이름을 입력하세요.

   대부분의 경우 콘솔은 클러스터의 데이터를 기반으로 자동으로 계정을 생성합니다.

4. 클러스터의 클러스터 관리자 자격 증명을 입력합니다.

결과

시스템 관리자가 표시되고 이제 콘솔에서 클러스터를 관리할 수 있습니다.

NetApp 콘솔에 대해 자세히 알아보세요

- "NetApp 콘솔 개요"
- "NetApp 콘솔을 통해 NetApp AFF 및 FAS 시스템을 관리하세요"

클러스터 스토리지

ONTAP의 현재 반복은 원래 NetApp의 스케일아웃_클러스터_스토리지 아키텍처용으로 개발되었습니다. 이 아키텍처는 ONTAP의 데이터 센터 구현에서 일반적으로 볼 수 있는 아키텍처입니다. 이 구축 과정에서는 ONTAP의 대부분의 기능을 사용하기 때문에 ONTAP 기술에 대한 개념을 이해하는 것이 좋습니다.

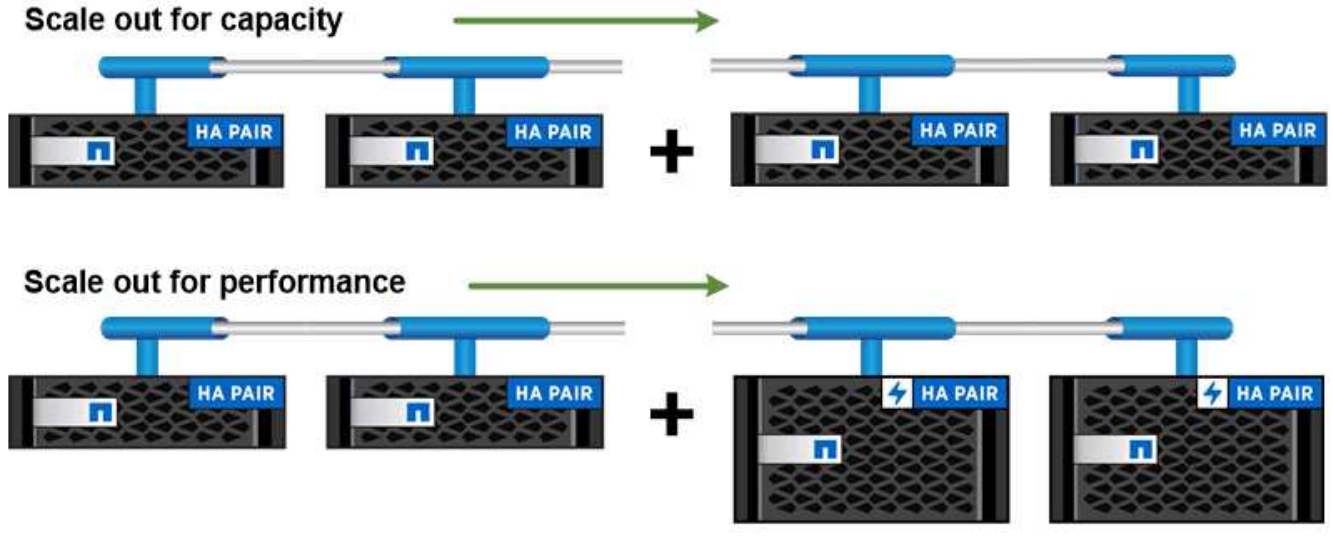
데이터센터 아키텍처는 일반적으로 ONTAP 데이터 관리 소프트웨어를 실행하는 전용 AFF, ASA 또는 FAS 시스템을 구축합니다. 각 컨트롤러, 스토리지, 네트워크 연결, 그리고 컨트롤러에서 실행되는 ONTAP 인스턴스를 _노드_라고 합니다.

HA(고가용성)를 위해 노드가 페어링되었습니다. 이 두 쌍(SAN의 경우 최대 12개 노드, NAS의 경우 최대 24개 노드)이 클러스터를 구성합니다. 노드는 전용 클러스터 인터커넥트를 통해 서로 통신합니다.

컨트롤러 모델에 따라 노드 스토리지는 플래시 디스크, 용량 드라이브 또는 둘 모두로 구성됩니다. 컨트롤러의 네트워크 포트는 데이터에 대한 액세스를 제공합니다. 물리적 스토리지 및 네트워크 연결 리소스는 가상화되어 클러스터 관리자만 볼 수 있고 NAS 클라이언트 또는 SAN 호스트에는 표시되지 않습니다.

HA 쌍의 노드는 동일한 스토리지 어레이 모델을 사용해야 합니다. 그렇지 않으면 지원되는 모든 컨트롤러 조합을 사용할 수 있습니다. 스토리지 어레이 모델과 같은 노드를 추가하거나 하이엔드 스토리지 어레이가 포함된 노드를 추가하여 성능을 위해 용량을 확장할 수 있습니다.

물론 필요에 따라 디스크 또는 컨트롤러를 업그레이드하면서 기존의 모든 방법으로 스케일업할 수 있습니다. ONTAP의 가상화 스토리지 인프라를 사용하면 데이터를 중단 없이 쉽게 이동할 수 있으므로 다운타임 없이 수직 또는 수평으로 확장할 수 있습니다.



You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.

고가용성 쌍

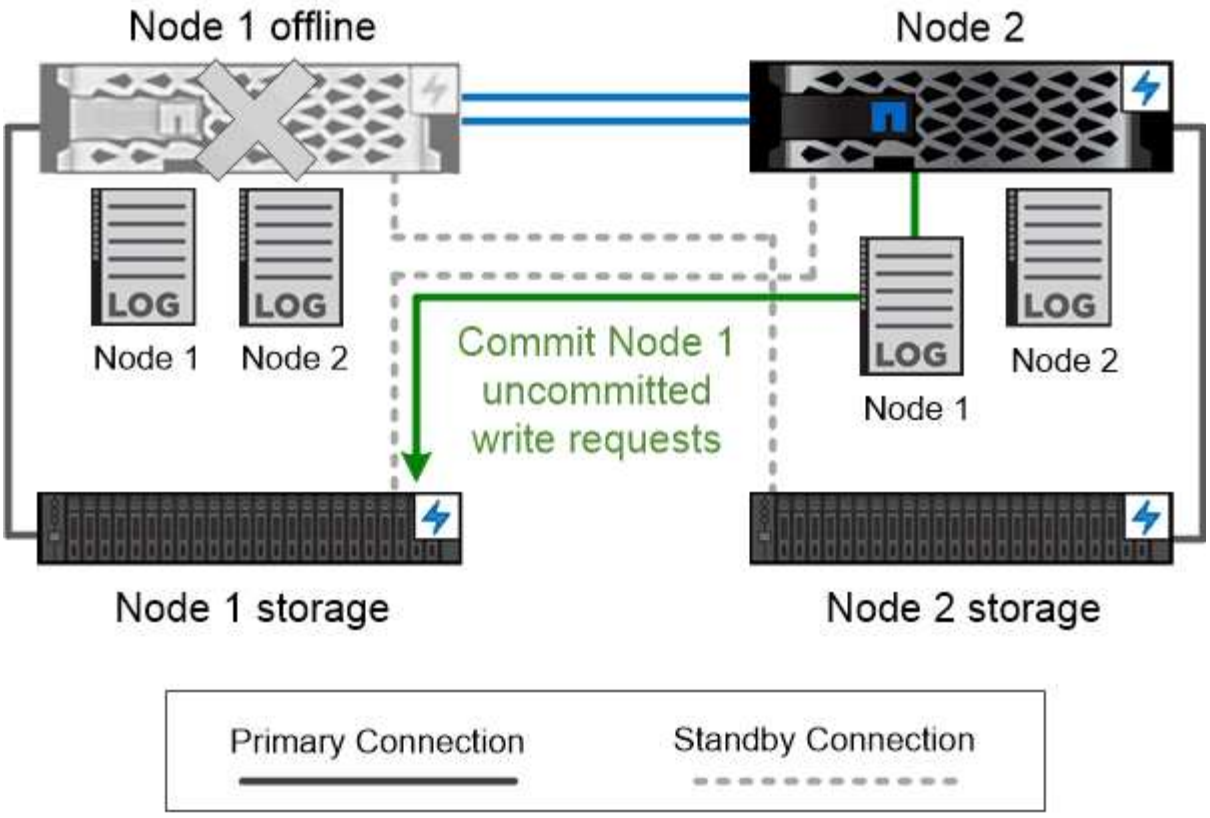
클러스터 노드는 내결함성 및 무중단 운영을 위해 _ HA(고가용성) 쌍으로 구성됩니다. 노드에 장애가 발생할 경우 또는 정기적인 유지보수를 위해 노드를 구축해야 하는 경우 파트너는 스토리지를 _ 테이크오버하고 해당 스토리지에서 데이터를 계속 제공할 수 있습니다. 노드가 다시 온라인 상태가 되면 PARTNER_에서 BACK_STORAGE를 제공합니다.

HA 쌍은 항상 같은 컨트롤러 모델로 구성됩니다. 일반적으로 컨트롤러는 중복 전원 공급 장치가 있는 동일한 섀시에 위치합니다.

HA 쌍은 서로 다른 방식으로 통신할 수 있는 장애 허용 노드로, 각 노드가 파트너가 제대로 작동하는지 지속적으로 확인하고 다른 노드의 비휘발성 메모리에 로그 데이터를 미러링할 수 있습니다. 노드에 쓰기 요청이 이루어지면, 클라이언트나 호스트로 응답이 전송되기 전에 두 노드의 NVRAM 에 해당 요청이 기록됩니다. 장애 조치 시, 살아남은 파트너는 실패한 노드의 커밋되지 않은 쓰기 요청을 디스크에 커밋하여 데이터 일관성을 보장합니다. 살아남은 노드는 이전에 실패한 노드의 NVRAM 의 미러 역할을 했던 NVRAM 파티션에 쓰기를 계속 기록합니다.

다른 컨트롤러의 스토리지 미디어에 연결하면 테이크오버가 수행되는 경우 각 노드가 다른 컨트롤러의 스토리지에 액세스할 수 있습니다. 네트워크 경로 페일오버 메커니즘을 통해 클라이언트 및 호스트가 정상 작동하는 노드와 계속 통신할 수 있습니다.

가용성을 보장하기 위해 페일오버 사례에 추가 워크로드를 수용할 수 있도록 두 노드 중 하나의 성능 용량 활용률을 50%로 유지해야 합니다. 같은 이유로 노드에 대한 최대 NAS 가상 네트워크 인터페이스 수의 50% 이상을 구성하려고 할 수 있습니다.



On failover, the surviving partner commits the failed node's uncommitted write requests to disk, ensuring data consistency.

가상화 ONTAP 구축 환경에서 * _테이크오버와 반환 _ *

ONTAP Select 와 같은 가상화된 "공유되지 않는(shared-nothing)" ONTAP 구현에서는 노드 간에 스토리지가 공유되지 않습니다. 노드가 다운되면 해당 노드의 파트너는 노드 데이터의 동기식 미러링된 복사본에서 데이터를 계속 제공합니다. 파트너는 노드의 스토리지를 인계받지 않고, 데이터 제공 기능만 수행합니다.

AutoSupport 및 디지털 자문업체

ONTAP는 웹 포털과 모바일 앱을 통해 인공 지능 기반의 시스템 모니터링 및 보고를 제공합니다. ONTAP의 AutoSupport 구성 요소는 Active IQ 디지털 어드바이저(Digital Advisor라고도 함)가 분석하는 원격 측정 장치를 전송합니다.

Digital Advisor를 사용하면 클라우드 기반 포털 및 모바일 앱을 통해 실행 가능한 예측 분석과 사전 예방적 지원을 제공하여 글로벌 하이브리드 클라우드 전반에서 데이터 인프라를 최적화할 수 있습니다. 활성 SupportEdge 계약을 보유한 모든 NetApp 고객은 디지털 어드바이저의 데이터 중심 인사이트와 권장 사항을 이용할 수 있습니다(기능은 제품 및 지원 계층에 따라 다름).

Digital Advisor로 할 수 있는 작업은 다음과 같습니다.

- 업그레이드 계획 Digital Advisor는 최신 버전의 ONTAP로 업그레이드하여 해결할 수 있는 환경 문제를 식별하며 업그레이드 관리자 구성 요소는 성공적인 업그레이드를 계획하는 데 도움이 됩니다.

- 시스템 상태 보기 Digital Advisor 대시보드에서 웰니스 문제를 보고하고 이러한 문제를 해결할 수 있습니다. 시스템 용량을 모니터링하여 스토리지 공간이 부족하지 않도록 하십시오.
- 성능 관리 Digital Advisor는 System Manager에서 볼 수 있는 것보다 더 오랜 기간 동안 시스템 성능을 표시합니다. 성능에 영향을 주는 구성 및 시스템 문제를 식별합니다.
- 효율성 극대화 스토리지 효율성 메트릭을 확인하고 더 적은 공간에 더 많은 데이터를 저장하는 방법을 알아보십시오.
- 인벤토리 및 구성을 봅니다. Digital Advisor는 전체 인벤토리와 소프트웨어 및 하드웨어 구성 정보를 표시합니다. 서비스 계약이 만료되는 시점을 확인하여 서비스 계약이 계속 보장되는지 확인합니다.

관련 정보

"NetApp 설명서: 디지털 어드바이저"

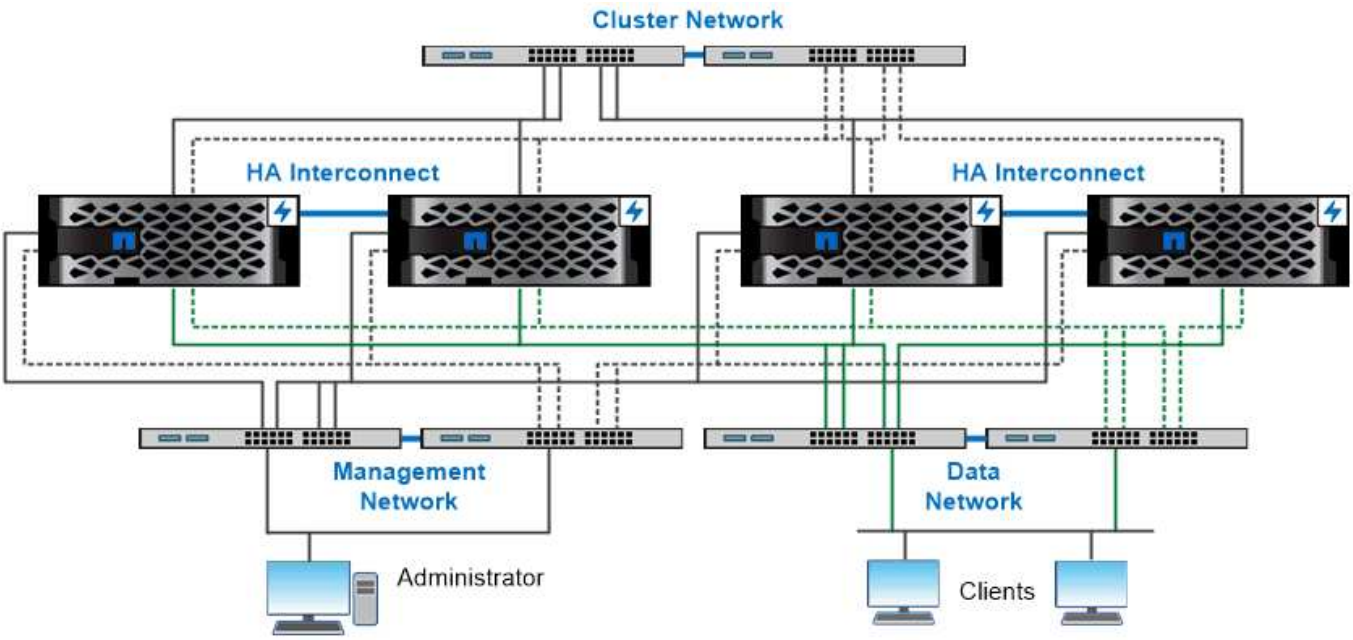
"Digital Advisor를 실행합니다"

"SupportEdge 서비스"

네트워크 아키텍처

네트워크 아키텍처 개요

ONTAP 데이터 센터 구축을 위한 네트워크 아키텍처는 일반적으로 클러스터 인터커넥트, 클러스터 관리를 위한 관리 네트워크 및 데이터 네트워크로 구성됩니다. NIC(네트워크 인터페이스 카드)는 이더넷 연결을 위한 물리적 포트를 제공합니다. HBA(호스트 버스 어댑터)는 FC 연결을 위한 물리적 포트를 제공합니다.



The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.

각 노드에 제공되는 물리적 포트 외에 _logical port_를 사용하여 네트워크 트래픽을 관리할 수 있습니다. 논리 포트는 인터페이스 그룹 또는 VLAN입니다.

인터페이스 그룹

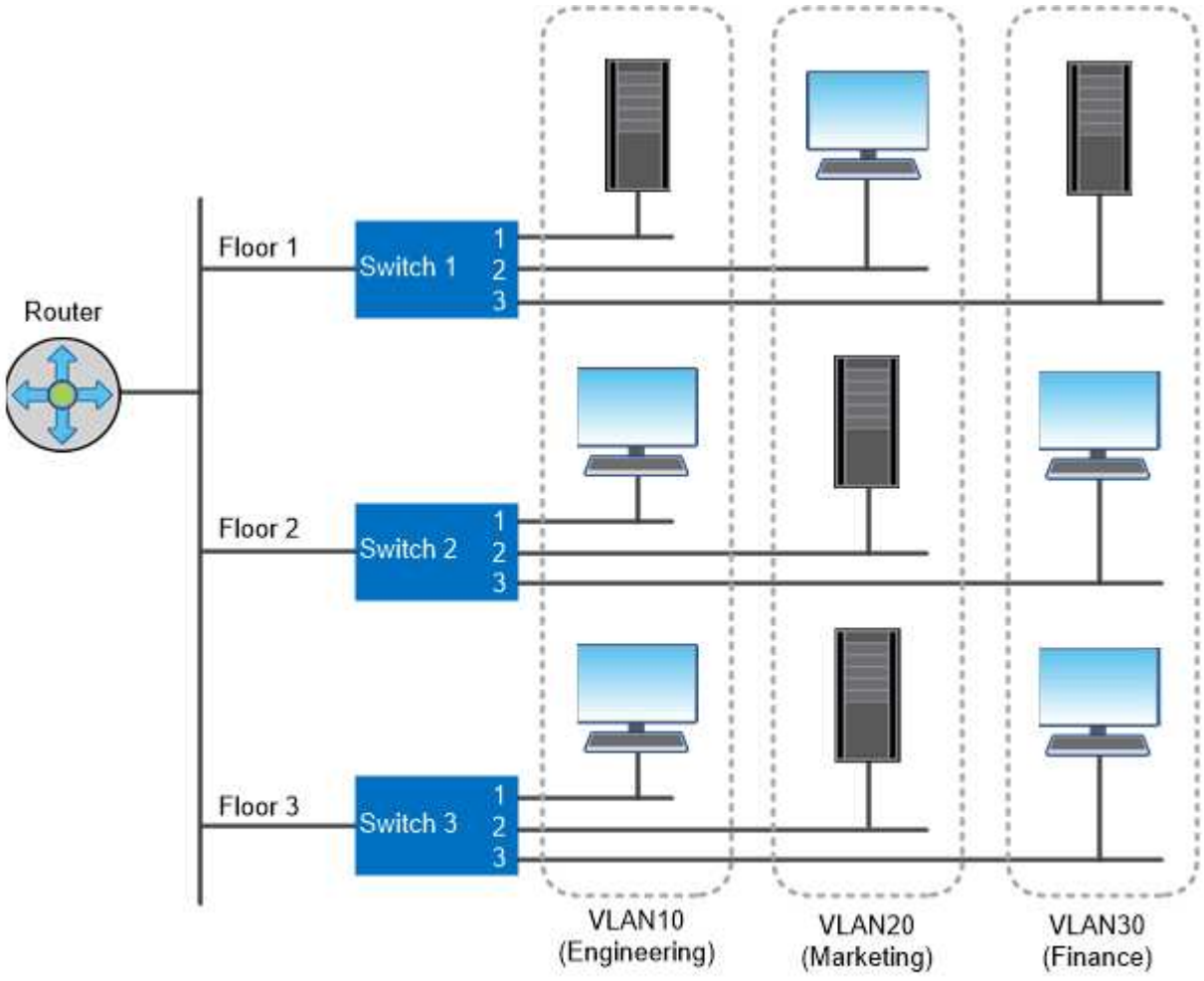
인터페이스 그룹 여러 개의 물리적 포트를 하나의 논리적 " 트렁크 포트 "로 결합합니다. 다른 PCI 슬롯에 있는 NIC의 포트로 구성된 인터페이스 그룹을 만들어 슬롯 장애가 발생하여 업무상 중요한 트래픽이 감소되도록 할 수 있습니다.

인터페이스 그룹은 단일 모드, 다중 모드 또는 동적 다중 모드일 수 있습니다. 각 모드는 다양한 수준의 내결함성을 제공합니다. 두 유형의 다중 모드 인터페이스 그룹을 사용하여 네트워크 트래픽의 로드 밸런싱을 수행할 수 있습니다.

VLAN

_VLANs_물리적 경계가 아닌 스위치 포트 기반에 정의된 논리 세그먼트로 네트워크 포트(인터페이스 그룹)에서 트래픽을 분리합니다. VLAN에 속한 _end-stations_는 기능 또는 애플리케이션에 의해 관련된다.

엔지니어링 및 마케팅 등의 부서나 릴리스1 및 릴리스2 등의 프로젝트별로 최종 스테이션을 그룹화할 수 있습니다. 최종 스테이션의 물리적 근접성이 VLAN에서 무관하기 때문에 최종 스테이션은 지리적으로 원격일 수 있습니다.



You can use VLANs to segregate traffic by department.

업계 표준 네트워크 기술 지원

ONTAP는 모든 주요 업계 표준 네트워크 기술을 지원합니다. 주요 기술에는 IPspace, DNS 로드 밸런싱, SNMP 트랩이 포함됩니다.

브로드캐스트 도메인, 페일오버 그룹 및 서브넷은 에 설명되어 있습니다 NAS 경로 페일오버.

IPspace

_IPspace_를 사용하여 클러스터의 각 가상 데이터 서버에 대해 별개의 IP 주소 공간을 만들 수 있습니다. 이렇게 하면 관리자가 별도의 네트워크 도메인에 있는 클라이언트가 동일한 IP 주소 서브넷 범위의 중복 IP 주소를 사용하면서 클러스터 데이터에 액세스할 수 있습니다.

예를 들어, 서비스 공급자는 동일한 IP 주소를 사용하여 테넌트에 대해 다른 IPspace를 구성하여 클러스터에 액세스할 수 있습니다.

DNS 로드 밸런싱

DNS 부하 분산 _ 을(를) 사용하여 사용 가능한 포트 간에 사용자 네트워크 트래픽을 분산할 수 있습니다. DNS 서버는 인터페이스에 마운트된 클라이언트 수를 기반으로 트래픽에 대한 네트워크 인터페이스를 동적으로 선택합니다.

SNMP 트랩

_snmp trap_을 사용하여 주기적으로 작동 임계값 또는 오류를 확인할 수 있습니다. SNMP 트랩은 SNMP 에이전트에서 SNMP 관리자로 비동기적으로 전송되는 시스템 모니터링 정보를 캡처합니다.

FIPS 규정 준수

ONTAP는 모든 SSL 연결에 대해 FIPS(Federal Information Processing Standards) 140-2를 준수합니다. SSL FIPS 모드를 설정 및 끄고, SSL 프로토콜을 전역적으로 설정하고, RC4와 같은 약한 암호를 해제할 수 있습니다.

RDMA 개요

ONTAP의 RDMA(Remote Direct Memory Access) 솔루션은 지연 시간에 민감한 고대역폭 워크로드를 지원합니다. RDMA를 사용하면 스토리지 시스템 메모리와 호스트 시스템 메모리 간에 데이터를 직접 복사하여 CPU 중단과 오버헤드를 피할 수 있습니다.

RDMA 상의 NFS

ONTAP 9.10.1부터 구성할 수 있습니다 "RDMA 상의 NFS" 지원되는 NVIDIA GPU가 있는 호스트에서 GPU 가속 워크로드에 NVIDIA GPUDirect 스토리지를 사용할 수 있도록 합니다.

RDMA는 SMB 프로토콜을 지원하지 않습니다.

클러스터 인터커넥트 RDMA

클러스터 인터커넥트 RDMA는 지연 시간을 단축하고, 페일오버 시간을 줄이고, 클러스터 노드 간의 통신을 가속화합니다.

ONTAP 9.10.1부터 X1151A 클러스터 NIC와 함께 사용할 경우 특정 하드웨어 시스템에서 클러스터 상호 연결 RDMA가 지원됩니다. ONTAP 9.13.1부터 X91153A NIC는 클러스터 인터커넥트 RDMA도 지원합니다. 표를 참조하여

다양한 ONTAP 릴리스에서 지원되는 시스템에 대해 알아보십시오.

시스템	지원되는 **ONTAP** 버전
• AFF A50 를 참조하십시오 • AFF A30 를 참조하십시오 • AFF A20 를 참조하십시오 • AFF C80 를 참조하십시오 • AFF C60 를 참조하십시오 • AFF C30 를 참조하십시오 • ASA A50 • ASA A30 • ASA A20	ONTAP 9.16.1 이상
• AFF A1K 를 참조하십시오 • AFF A90 를 참조하십시오 • AFF A70 를 참조하십시오 • ASA A1K • ASA A90 • ASA A70 • FAS90를 참조하십시오 • FAS70를 참조하십시오	ONTAP 9.15.1 이상
• AFF A900 탑재 • ASA A900 • FAS9500	ONTAP 9.13.1 이상
• AFF A400 • ASA A400	ONTAP 9.10.1 이상

적절한 스토리지 시스템 설정을 감안하면 클러스터 인터커넥트 RDMA를 사용하기 위해 추가 구성이 필요하지 않습니다.

클라이언트 프로토콜

ONTAP는 NFS, SMB, FC, FCoE, iSCSI, NVMe 및 S3:

NFS 를 참조하십시오

NFS는 UNIX 및 Linux 시스템을 위한 기존 파일 액세스 프로토콜입니다. 클라이언트는 다음 프로토콜을 사용하여 ONTAP 볼륨의 파일에 액세스할 수 있습니다.

- NFSv3
- NFSv4
- NFSv4.2
- NFSv4.1
- pNFS를 사용합니다

UNIX 스타일 사용 권한, NTFS 스타일 사용 권한 또는 이 두 가지를 혼합하여 파일 액세스를 제어할 수 있습니다.

클라이언트는 NFS 및 SMB 프로토콜을 모두 사용하여 동일한 파일에 액세스할 수 있습니다.

중소기업

SMB는 Windows 시스템을 위한 기존 파일 액세스 프로토콜입니다. 클라이언트는 SMB 2.0, SMB 2.1, SMB 3.0 및 SMB 3.1.1 프로토콜을 사용하여 ONTAP 볼륨의 파일에 액세스할 수 있습니다. NFS와 마찬가지로 사용 권한 스타일의 조합이 지원됩니다.

SMB 1.0은 사용 가능하지만 ONTAP 9.3 이상 릴리스에서 기본적으로 비활성화되어 있습니다.

FC

Fibre Channel은 원래 네트워크 블록 프로토콜입니다. 블록 프로토콜은 파일 대신 전체 가상 디스크를 클라이언트에 제공합니다. 기존 FC 프로토콜은 전용 FC 스위치를 사용하는 전용 FC 네트워크를 사용하며, 클라이언트 컴퓨터에 FC 네트워크 인터페이스가 있어야 합니다.

LUN은 가상 디스크를 나타내고, 하나 이상의 LUN은 ONTAP 볼륨에 저장됩니다. FC, FCoE 및 iSCSI 프로토콜을 통해 동일한 LUN에 액세스할 수 있지만 여러 클라이언트가 쓰기 충돌을 방지하는 클러스터의 일부인 경우에만 동일한 LUN에 액세스할 수 있습니다.

FCoE 를 참조하십시오

FCoE는 기본적으로 FC와 동일한 프로토콜이지만 기존 FC 전송 대신 데이터 센터급 이더넷 네트워크를 사용합니다. 클라이언트에는 여전히 FCoE 전용 네트워크 인터페이스가 필요합니다.

iSCSI

iSCSI는 표준 이더넷 네트워크에서 실행할 수 있는 블록 프로토콜입니다. 대부분의 클라이언트 운영 체제는 표준 이더넷 포트를 통해 실행되는 소프트웨어 이니시에이터를 제공합니다. iSCSI는 특정 애플리케이션에 대한 블록 프로토콜이 필요하지만 전용 FC 네트워킹을 사용할 수 없는 경우에 적합합니다.

NVMe/FC 및 **NVMe/TCP**

최신 블록 프로토콜인 NVMe는 플래시 기반 스토리지에서 작동하도록 특별히 설계되었습니다. 확장 가능한 세션, 지연 시간 대폭 감소, 병렬 처리 수 증가 등을 제공하므로 메모리 내 데이터베이스 및 분석과 같은 대기 시간이 짧고 처리량이 높은 애플리케이션에 적합합니다.

FC 및 iSCSI와 달리 NVMe는 LUN을 사용하지 않습니다. 대신 ONTAP 볼륨에 저장된 네임스페이스를 사용합니다. NVMe 네임스페이스는 NVMe 프로토콜을 통해서만 액세스할 수 있습니다.

S3

ONTAP 9.8부터 ONTAP 클러스터에서 ONTAP S3(Simple Storage Service) 서버를 활성화하여 S3 버킷을 사용하여

오브젝트 스토리지에서 데이터를 제공할 수 있습니다.

ONTAP은 S3 오브젝트 스토리지를 지원하기 위한 두 가지 사내 사용 사례 시나리오를 지원합니다.

- 로컬 클러스터(로컬 버킷에 계층화) 또는 원격 클러스터(클라우드 계층)의 버킷에 대한 FabricPool 계층
- S3 클라이언트 애플리케이션이 로컬 클러스터 또는 원격 클러스터의 버킷에 액세스합니다.

ONTAP S3는 추가 하드웨어 및 관리 없이 기존 클러스터에서 S3 기능을 원하는 경우에 적합합니다. 300TB 이상의 배포를 위해 NetApp StorageGRID 소프트웨어는 계속해서 오브젝트 스토리지를 위한 NetApp의 대표적인 솔루션입니다. 에 대해 자세히 "StorageGRID" 알아보십시오.

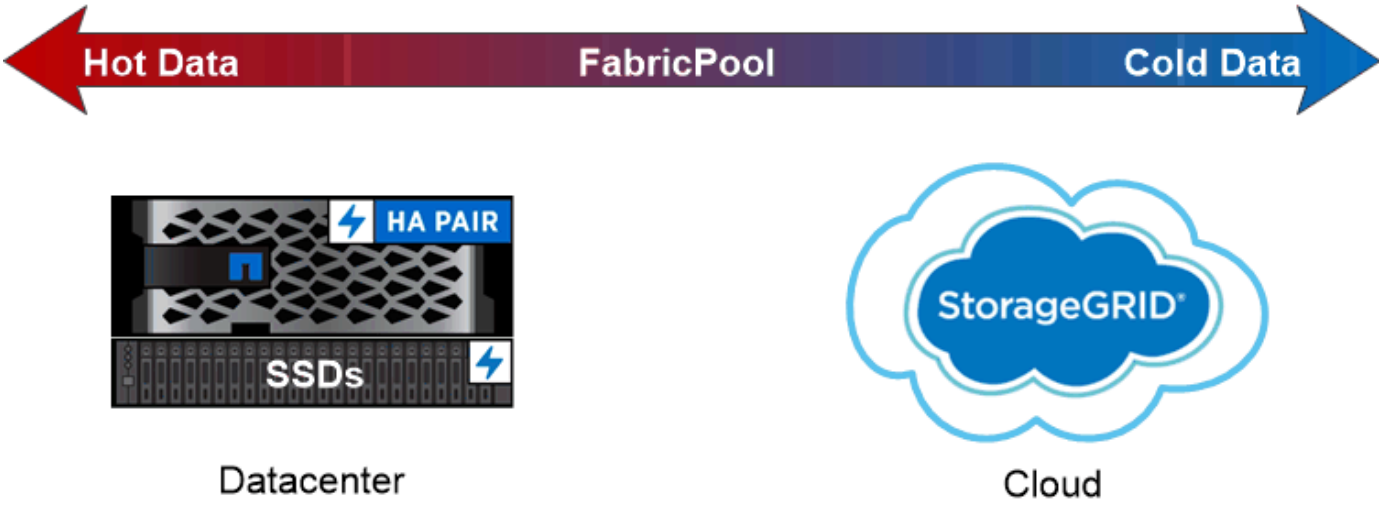
디스크 및 로컬 계층

디스크 및 **ONTAP** 로컬 계층

_local tiers_는 _aggregates_라고도 하며 노드에서 관리하는 디스크에 대한 논리적 컨테이너입니다. 로컬 계층을 사용하여 다양한 성능 요구사항에 따라 워크로드를 격리하거나, 다른 액세스 패턴으로 데이터를 계층화하거나, 규정 준수를 위해 데이터를 분리할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다.

- 지연 시간이 가장 짧고 성능이 가장 높은 비즈니스 크리티컬 애플리케이션의 경우 SSD로만 구성된 로컬 계층을 생성할 수 있습니다.
- 서로 다른 액세스 패턴으로 데이터를 계층화하려면 _ 하이브리드 로컬 계층 _ 을(를) 생성하고, 사용 중인 데이터 세트에 플래시를 고성능 캐시로 구축하는 동시에, 액세스 빈도가 낮은 데이터에 저비용 HDD 또는 오브젝트 스토리지를 사용할 수 있습니다.
  - 는 "_플래시 풀 _"SSD와 HDD로 구성됩니다.
  - 는 "*FabricPool*"오브젝트 저장소가 연결된 All-SSD 로컬 계층으로 구성됩니다.
- 규정 준수를 위해 아카이빙된 데이터를 활성 데이터에서 분리해야 하는 경우 용량 HDD로 구성된 로컬 계층 또는 성능과 용량 HDD를 조합하여 사용할 수 있습니다.



You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed "hot" data and object storage for rarely accessed "cold" data.

MetroCluster 구성에서 로컬 계층으로 작업

MetroCluster 구성을 사용하는 경우 초기 구성에 대한 설명서의 절차와 로컬 계층 및 디스크 관리에 대한 지침을 따라야 "MetroCluster"합니다.

관련 정보

- "로컬 계층 관리"
- "디스크를 관리합니다"
- "RAID 구성을 관리합니다"
- "Flash Pool 계층 관리"
- "FabricPool 클라우드 계층 관리"

ONTAP RAID 그룹 및 로컬 계층

최신 RAID 기술은 장애가 발생한 디스크의 데이터를 스페어 디스크에 재구축하여 디스크 장애로부터 보호합니다. 시스템은 "패리티 디스크"의 인덱스 정보를 나머지 정상 디스크에 있는 데이터와 비교하여 다운타임 또는 상당한 성능 비용 없이 누락된 데이터를 재구성합니다.

로컬 계층은 하나 이상의 RAID 그룹 _ 으로 구성됩니다. 로컬 계층의 _RAID type_은 RAID 그룹의 패리티 디스크 수와 RAID 구성에서 보호하는 동시 디스크 장애 수를 결정합니다.

기본 RAID 유형인 RAID-DP(RAID-이중 패리티)에는 RAID 그룹당 2개의 패리티 디스크가 필요하며 동시에 2개의 디스크에 장애가 발생할 경우 데이터 손실을 방지합니다. RAID-DP의 경우 권장 RAID 그룹 크기는 12~20개의 HDD와 20~28개의 SSD입니다.

사이징 권장 사항 끝에 RAID 그룹을 생성하여 패리티 디스크의 오버헤드 비용을 분산할 수 있습니다. 특히 SSD의 경우 용량 드라이브보다 훨씬 안정적입니다. HDD를 사용하는 로컬 계층의 경우 대용량 RAID 그룹에 필요한 더 긴 재구축 시간과 같은 카운트베링 요소에 대해 디스크 스토리지를 극대화해야 할 필요성을 균형 있게 조정해야 합니다.

ONTAP_SyncMirror_를 사용하여 다른 RAID 그룹에 저장된 복사본 또는 _plexes_의 로컬 계층 데이터를 동기식으로 미러링할 수 있습니다. 플렉스는 RAID 유형보다 더 많은 디스크에 장애가 발생하거나 RAID 그룹 디스크에 대한 연결이 끊어지면 데이터 손실을 방지합니다.

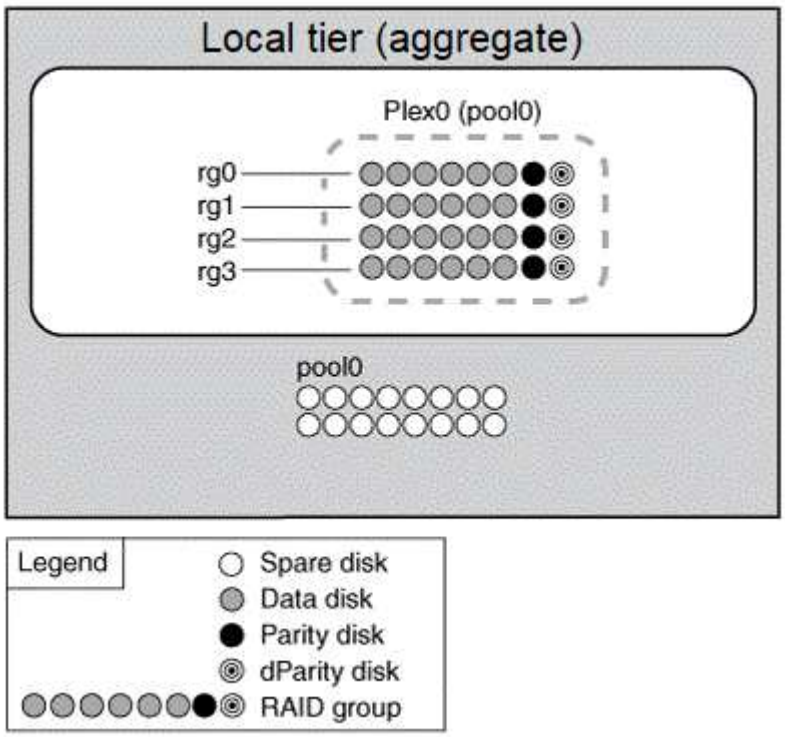
로컬 계층을 만들 때 로컬 계층이 미러링되는지 미러링되지 않는지 지정할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

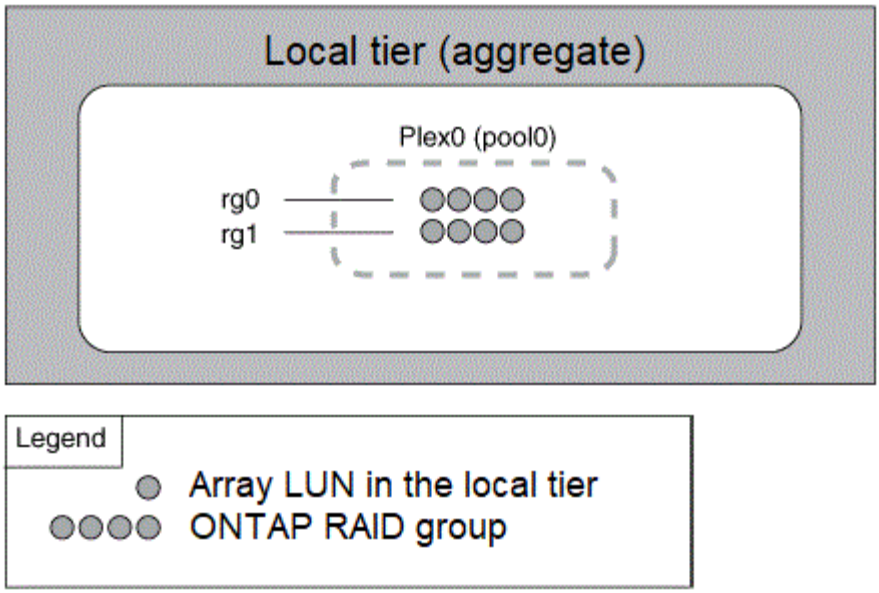
미러링되지 않은 로컬 계층의 작동 방식

로컬 계층이 미러링되도록 지정하지 않으면 미러링되지 않은 계층으로 생성됩니다. 미러링되지 않은 로컬 계층에는 해당 로컬 계층에 속한 모든 RAID 그룹이 포함된 1_plex_(데이터 복사본)만 있습니다.

다음 다이어그램은 하나의 플렉스로 그룹화된 디스크로 구성된 미러링되지 않은 로컬 계층을 보여 줍니다. 로컬 계층에는 rg0, rg1, RG2 및 rg3의 4개의 RAID 그룹이 있습니다. 각 RAID 그룹에는 6개의 데이터 디스크, 1개의 패리티 디스크 및 1개의 dparity(이중 패리티) 디스크가 있습니다. 로컬 계층에서 사용하는 모든 디스크는 동일한 풀 ""pool0""에서 가져옵니다.



다음 다이어그램은 스토리지 LUN이 포함된 미러링되지 않은 로컬 계층을 하나의 플렉스로 그룹화한 것입니다. 이 그룹에는 rg0과 rg1이라는 두 개의 RAID 그룹이 있습니다. 로컬 계층에서 사용하는 모든 스토리지 LUN은 동일한 풀 ""pool0""에서 가져옵니다.



미러링된 로컬 계층의 작동 방식

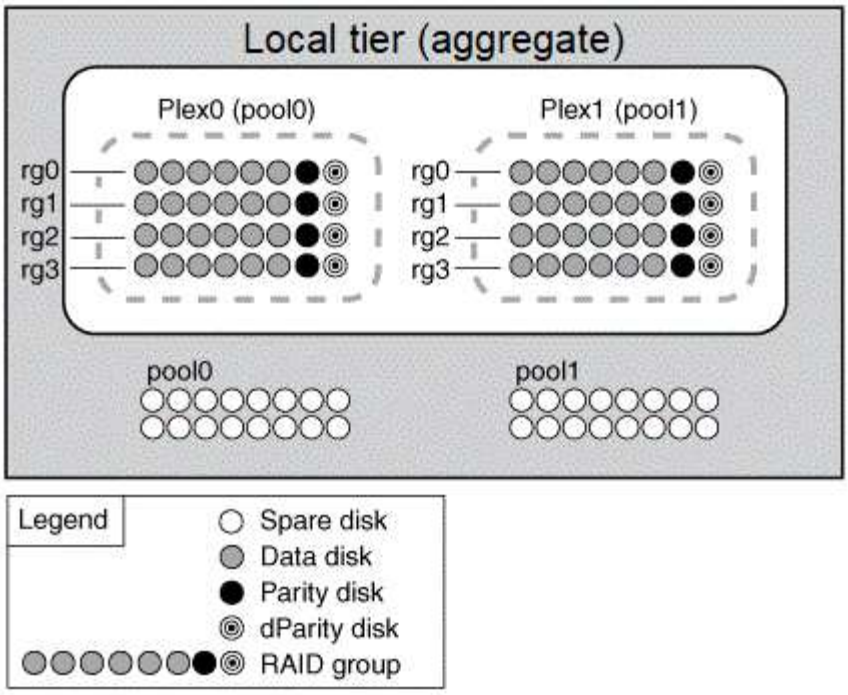
미러링된 로컬 계층은 SyncMirror 기능을 사용하여 이중화를 제공하는 2_plexes_(데이터 복사본)를 가집니다.

로컬 계층을 생성할 때 해당 계층을 미러링하도록 지정할 수 있습니다. 또한 기존 미러링되지 않은 로컬 계층에 두 번째 플렉스를 추가하여 미러링된 계층으로 만들 수도 있습니다. ONTAP는 SyncMirror를 사용하여 원래 plex(plex0)의 데이터를 새 plex(plex1)로 복사합니다. 플렉스는 물리적으로 분리되어(각 플렉스는 자체 RAID 그룹과 자체 풀을 가지고 있음) 플렉스가 동시에 업데이트됩니다.

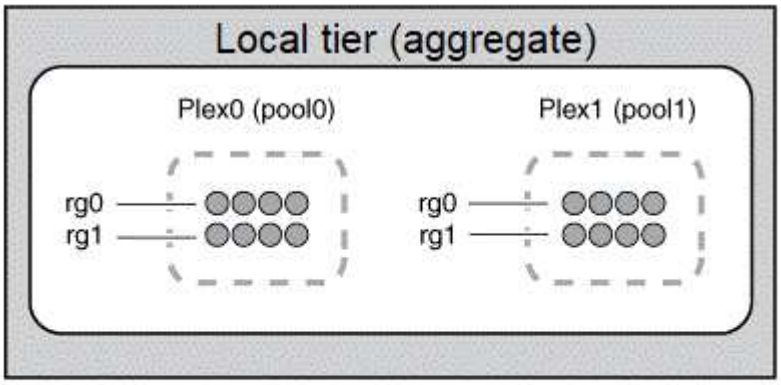
이 구성은 장애가 발생한 원인을 해결하는 동안 영향을 받지 않는 플렉스가 데이터를 계속 제공하기 때문에 로컬 계층의 RAID 레벨보다 더 많은 디스크에 장애가 발생하거나 연결이 끊긴 경우 데이터 손실에 대한 추가적인 보호 기능을 제공합니다. 문제가 발생한 플렉스가 해결된 후 두 플렉스가 미러 관계를 재동기화하여 다시 설정합니다.

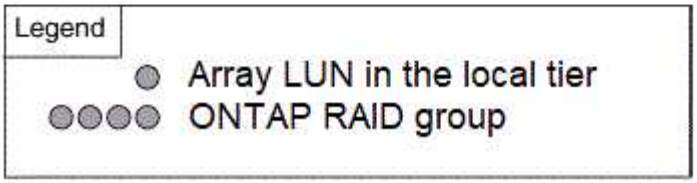
시스템의 디스크와 스토리지 LUN은 두 개의 풀, 즉 `pool0` 및 `pool1`로 구분됩니다. Plex0은 pool0에서 스토리지를 가져오고 plex1은 pool1에서 스토리지를 가져옵니다.

다음 다이어그램은 SyncMirror가 활성화 및 구현된 디스크로 구성된 로컬 계층을 보여 줍니다. 로컬 계층에 대해 두 번째 플렉스가 `plex1` 생성되었습니다. Plex1의 데이터는 Plex0에 있는 데이터의 복제본이며 RAID 그룹도 동일합니다. 32개의 스페어 디스크는 풀당 16개의 디스크를 사용하여 pool0 또는 pool1에 할당됩니다.



다음 다이어그램은 SyncMirror 기능이 설정 및 구현된 스토리지 LUN으로 구성된 로컬 계층을 보여 줍니다. 로컬 계층에 대해 두 번째 플렉스가 `plex1` 생성되었습니다. Plex1은 Plex0의 사본이며 RAID 그룹도 동일합니다.





최적의 스토리지 성능과 가용성을 위해 미러링된 집계에 최소 20%의 여유 공간을 유지하는 것이 좋습니다. 미러링되지 않은 집계의 경우 권장 사항은 10%이지만, 추가된 10%의 공간은 파일 시스템에서 증분 변경 사항을 흡수하는 데 사용될 수 있습니다. ONTAP의 쓰기 시 리디렉션 스냅샷 기반 아키텍처로 인해 증분적 변경으로 인해 미러링된 집계의 공간 활용도가 높아집니다. 이러한 모범 사례를 준수하지 않으면 성과에 부정적인 영향을 미칠 수 있습니다.

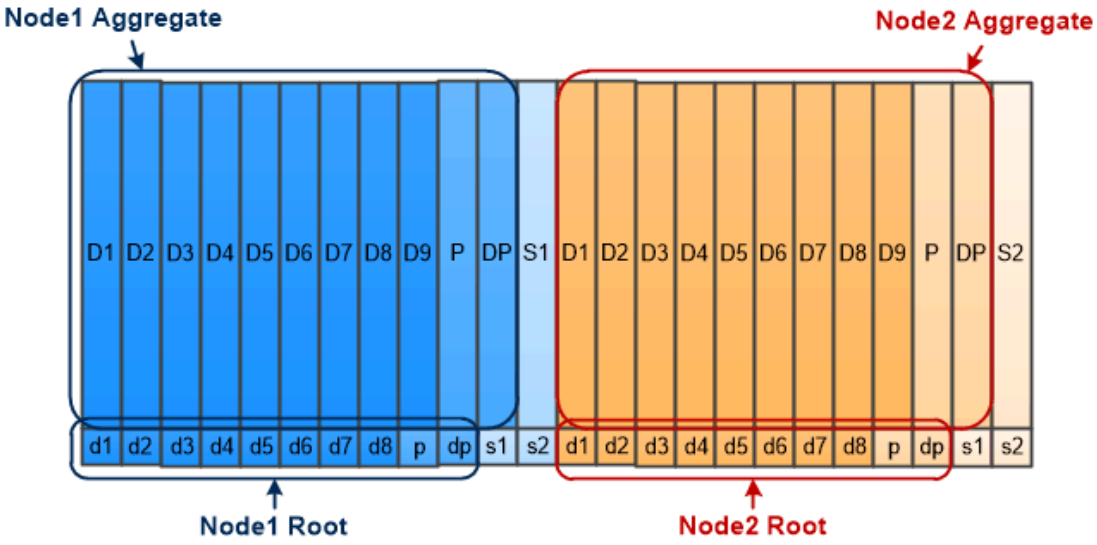
루트 데이터 파티셔닝

모든 노드에는 스토리지 시스템 구성 파일에 대한 루트 애그리게이트가 있어야 합니다. 루트 애그리게이트에는 데이터 애그리게이트의 RAID 유형이 있습니다.

System Manager에서는 루트 데이터 또는 루트 데이터 데이터 파티셔닝을 지원하지 않습니다.

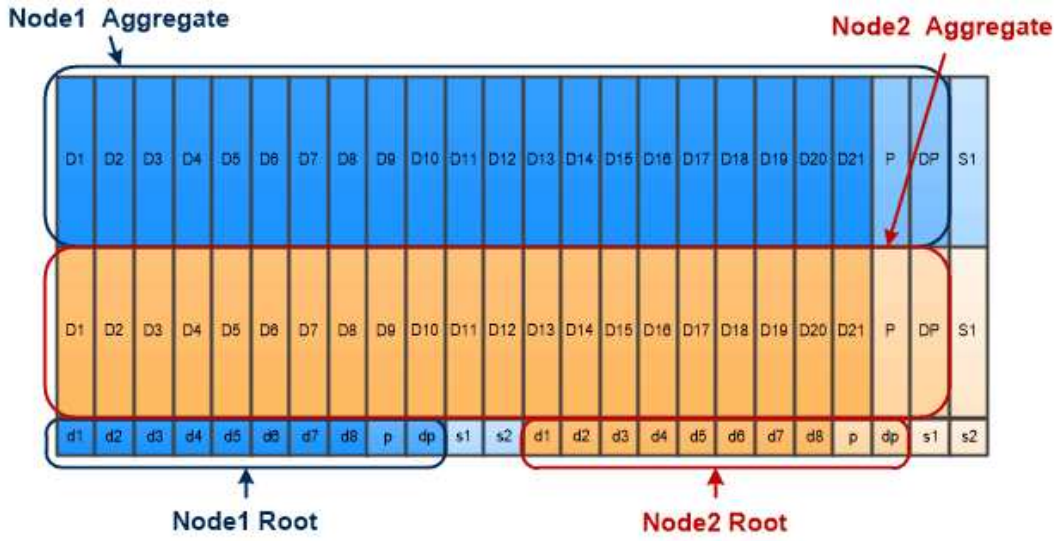
일반적으로 RAID-DP 유형의 루트 애그리게이트는 데이터 디스크 1개와 패리티 디스크 2개로 구성됩니다. 시스템에서 각 RAID 그룹의 패리티 디스크로 두 디스크를 이미 예약하고 있는 경우 스토리지 시스템 파일에 대한 비용을 지불하는 것은 상당한 "패리티 부담"입니다.

_Root - 데이터 파티셔닝 _ 은 디스크 파티션 전체에 루트 애그리게이트를 할당함으로써 패리티 세금을 줄이고 각 디스크에 루트 파티션으로 작은 파티션을 하나, 데이터를 위한 하나의 큰 파티션을 예약합니다.



Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk for data.

그림에서 알 수 있듯이 루트 애그리게이트를 저장하는 데 사용되는 디스크가 많을수록 루트 파티션이 작아집니다. 이는 또한 루트 파티션으로 작은 파티션을 하나 만들고 데이터를 위해 크기가 같은 큰 두 개의 파티션을 만드는 _root-data-data partitioning_이라는 루트 데이터 파티션 형태의 경우도 해당됩니다.



Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.

두 가지 유형의 루트 데이터 파티셔닝은 ONTAP_ADP(고급 드라이브 파티셔닝)_기능의 일부입니다. 두 가지 모두

엔트리 레벨 FAS2xxx, FAS9000, FAS8200, FAS80xx 및 AFF 시스템을 위한 루트 데이터 파티셔닝, AFF 시스템만을 위한 루트 데이터 데이터 파티셔닝으로 구성되어 있습니다.

에 대해 자세히 알아보십시오 "고급 드라이브 파티셔닝".

드라이브를 파티셔닝하고 루트 애그리게이트에 사용됩니다

루트 애그리게이트에서 사용하도록 분할된 드라이브는 시스템 구성에 따라 다릅니다.

루트 애그리게이트에 사용되는 드라이브 수를 알면 루트 파티션에 예약된 드라이브 용량과 데이터 애그리게이트에 사용할 수 있는 드라이브 용량을 확인하는 데 도움이 됩니다.

루트 데이터 파티셔닝 기능은 SSD만 연결된 엔트리 레벨 플랫폼, All Flash FAS 플랫폼, FAS 플랫폼에 지원됩니다.

엔트리 레벨 플랫폼의 경우 내부 드라이브만 파티셔닝됩니다.

SSD만 연결된 All Flash FAS 플랫폼 및 FAS 플랫폼의 경우 시스템을 초기화할 때 컨트롤러에 연결된 모든 드라이브는 노드당 최대 24개까지 파티셔닝됩니다. 시스템 구성 후 추가되는 드라이브는 파티셔닝되지 않습니다.

볼륨, Qtree, 파일 및 LUN

ONTAP는 _FlexVol 볼륨이라는 논리적 컨테이너의 클라이언트와 호스트에 데이터를 제공합니다. _ 이러한 볼륨은 포함된 집합체에만 느슨하게 결합되어 있기 때문에 기존 볼륨보다 데이터 관리 유연성이 뛰어납니다.

Aggregate에 여러 FlexVol 볼륨을 할당할 수 있으며 각 볼륨은 서로 다른 애플리케이션 또는 서비스 전용으로 할당됩니다. FlexVol 볼륨을 확장 및 축소하고, FlexVol 볼륨을 이동하고, FlexVol 볼륨의 효율적인 복사본을 생성할 수 있습니다. _qtree_를 사용하여 FlexVol 볼륨을 관리 가능한 단위로 파티셔닝하고 _quotas_를 사용하여 볼륨 리소스 사용을 제한할 수 있습니다.

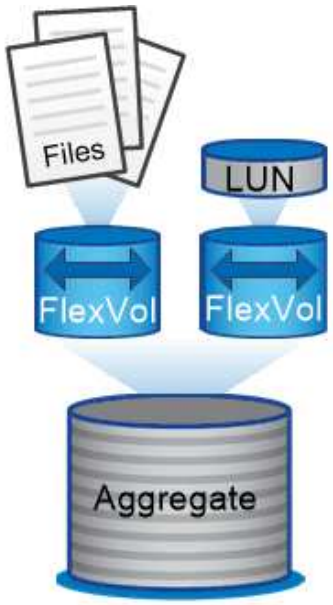
볼륨에는 NAS 환경의 파일 시스템과 SAN 환경의 LUN이 포함됩니다. LUN(논리 단위 번호)은 SAN 프로토콜에 의해 지정된 _logical unit_이라는 디바이스의 식별자입니다.

LUN은 SAN 구성의 기본 스토리지 단위입니다. Windows 호스트는 스토리지 시스템의 LUN을 가상 디스크로 인식합니다. 필요에 따라 LUN을 다른 볼륨으로 중단 없이 이동할 수 있습니다.

데이터 볼륨 외에 다음과 같은 몇 가지 특별한 볼륨에 대해 알아야 합니다.

- a_node root volume_(일반적으로 ""vol0"")에는 노드 구성 정보와 로그가 포함됩니다.
- SVM 루트 볼륨 _ 은(는) SVM에서 제공하는 네임스페이스의 진입점 역할을 하며 네임스페이스 디렉토리 정보를 포함합니다.
- _System volumes_에는 서비스 감사 로그와 같은 특수 메타데이터가 포함되어 있습니다.

이러한 볼륨을 사용하여 데이터를 저장할 수 없습니다.



Volumes contain files in a NAS environment and LUNs in a SAN environment.

- *FlexGroup* 볼륨 *

일부 기업에서는 단일 네임스페이스를 페타바이트 단위의 스토리지로 사용해야 할 수 있으며, 이는 FlexVol 볼륨의 100TB 용량을 훨씬 초과합니다.

A_FlexGroup volume_은 200개의 구성 멤버 볼륨으로 최대 4천억 개의 파일을 지원하며, 이 볼륨을 서로 협력하여 모든 구성원에 걸쳐 로드 및 공간 할당을 균등하게 동적으로 조정합니다.

FlexGroup 볼륨에는 유지보수 또는 관리 오버헤드가 필요하지 않습니다. FlexGroup 볼륨을 생성하여 NAS 클라이언트와 공유하기만 하면 됩니다. ONTAP가 나머지 기능을 수행합니다.

스토리지 가상화

스토리지 가상화 개요

SVM(Storage Virtual Machine)_을 사용하여 클라이언트 및 호스트에 데이터를 제공할 수 있습니다. 하이퍼바이저에서 실행되는 가상 머신과 마찬가지로 SVM은 물리적 리소스를 추상화하는 논리적 엔터티입니다. SVM을 통해 액세스하는 데이터는 스토리지의 위치에 바인딩되지 않습니다. SVM에 대한 네트워크 액세스는 물리적 포트에 바인딩되지 않습니다.

SVM은 이전 명칭 "vserver"였습니다. ONTAP 명령줄 인터페이스에서는 "vserver"라는 용어를 계속 사용합니다.

SVM은 하나 이상의 LIF(network_logical 인터페이스) _ 를 통해 하나 이상의 볼륨에서 클라이언트와 호스트에 데이터를 제공합니다. 볼륨은 클러스터의 모든 데이터 애그리게이트에 할당될 수 있습니다. LIF는 모든 물리적 또는 논리적 포트에서 호스팅할 수 있습니다. 하드웨어 업그레이드, 노드 추가, 성능 밸런싱 또는 애그리게이트 전체에서 용량 최적화 작업을 수행하든 볼륨 및 LIF를 모두 데이터 서비스를 중단하지 않고 이동할 수 있습니다.

동일한 SVM에서 NAS 트래픽을 위한 LIF와 SAN 트래픽을 위한 LIF를 사용할 수 있습니다. 클라이언트 및 호스트는 SVM에 액세스하기 위해 LIF의 주소(NFS, SMB 또는 iSCSI의 IP 주소, FC의 WWPN)만 필요합니다. LIF는 주소를 이동하면서 유지합니다. 포트에서 여러 LIF를 호스팅할 수 있습니다. 각 SVM에는 자체 보안, 관리, 네임스페이스가 있습니다.

ONTAP는 데이터 SVM 외에도 관리를 위해 특별한 SVM을 구축합니다.

- 클러스터 설정 시 _admin SVM_이 생성됩니다.
- 노드가 새 클러스터 또는 기존 클러스터에 결합할 때 _ 노드 SVM _ 이(가) 생성됩니다.
- IPspace에서 클러스터 레벨 통신을 위해 _ 시스템 SVM _ 이(가) 자동으로 생성됩니다.

이러한 SVM을 사용하여 데이터를 제공할 수 없습니다. 또한 클러스터 내부는 물론 클러스터 및 노드 관리용 특수 LIF도 있습니다.

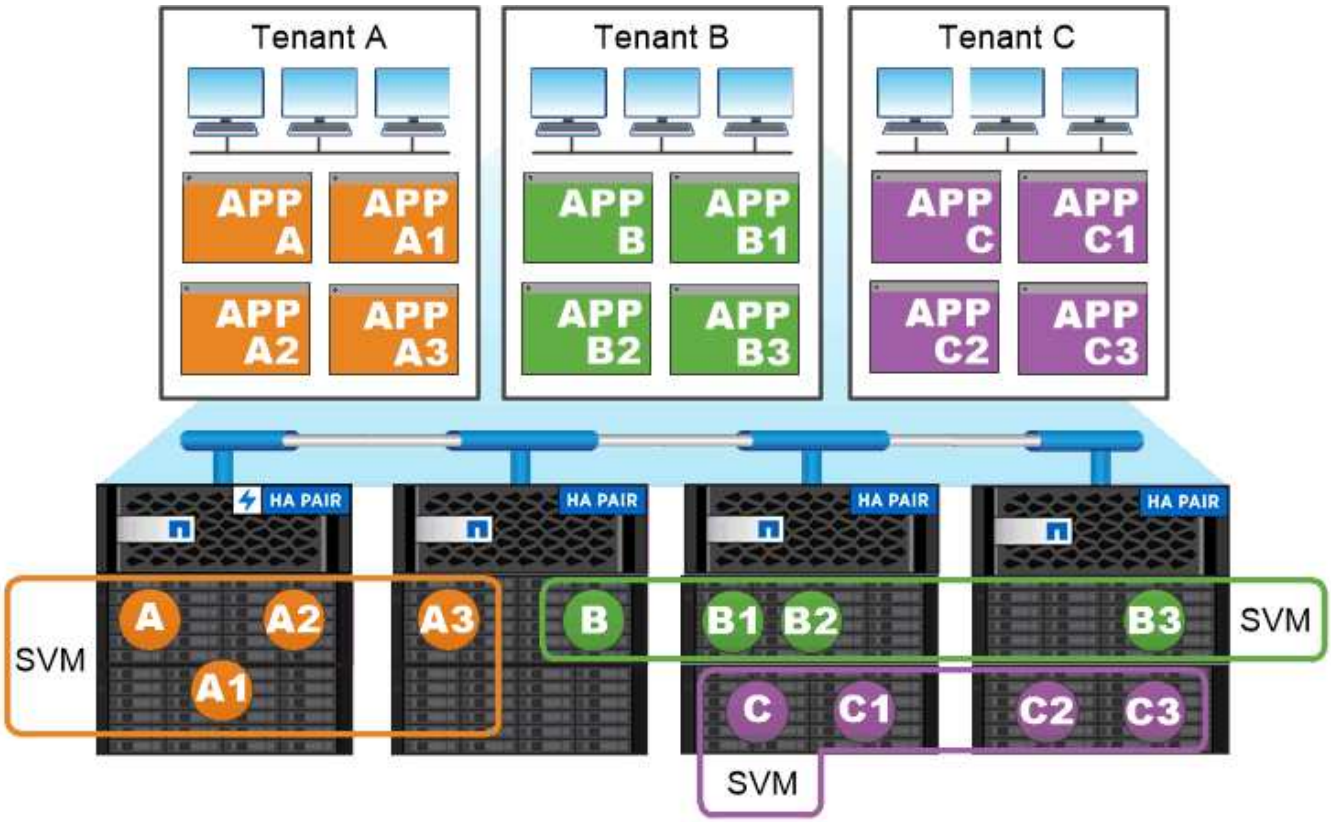
ONTAP가 미들웨어와 같은 이유

ONTAP가 스토리지 관리 작업에 사용하는 논리적 객체는 잘 설계된 미들웨어 패키지의 친숙한 목표를 제공합니다. 즉, 관리자가 낮은 수준의 구현 세부 사항으로부터 보호하면서 노드 및 포트와 같은 물리적 특성의 변경으로부터 구성을 절연합니다. 기본 아이디어는 관리자가 볼륨 및 LIF를 쉽게 이동할 수 있어야 하며 전체 스토리지 인프라가 아닌 몇 개의 필드를 재구성해야 한다는 것입니다.

SVM 사용 사례

서비스 공급자는 SVM을 안전한 멀티 테넌시 방식으로 사용하여 각 테넌트의 데이터를 격리하고, 각 테넌트에게 고유한 인증 및 관리를 제공하며, 비용 청구를 간소화합니다. 여러 LIF를 동일한 SVM에 할당하여 다양한 고객 요구사항을 충족할 수 있으며, QoS를 사용하여 다른 테넌트의 워크로드 ""불링""을 방지할 수 있습니다.

관리자는 SVM을 기업에서 유사한 용도로 사용합니다. 서로 다른 부서에서 데이터를 격리하거나 호스트가 한 SVM에서 스토리지 볼륨에 액세스하는 것을 유지하고 사용자가 다른 SVM에서 볼륨을 공유할 수 있습니다. 일부 관리자는 iSCSI/FC LUN 및 NFS 데이터 저장소를 한 SVM과 SMB 공유에 둡니다.



Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.

클러스터 및 **SVM** 관리

클러스터 관리자는 _ 클러스터에 대한 admin SVM에 액세스합니다. 클러스터 설정 시 admin이라는 예약 이름의 클러스터 관리자와 SVM 관리자가 자동으로 생성됩니다.

기본 'admin' 역할을 가진 클러스터 관리자는 전체 클러스터와 리소스를 관리할 수 있습니다. 클러스터 관리자는 필요에 따라 서로 다른 역할을 가진 추가 클러스터 관리자를 생성할 수 있습니다.

SVM 관리자는 _ 데이터 SVM에 액세스합니다. 클러스터 관리자가 필요에 따라 데이터 SVM 및 SVM 관리자를 생성합니다.

SVM 관리자는 기본적으로 'vsadmin' 역할이 할당됩니다. 클러스터 관리자는 필요에 따라 SVM 관리자에게 다양한 역할을 할당할 수 있습니다.

- _ 역할 기반 액세스 제어(RBAC) _ *

관리자에게 할당된 _role_은 관리자가 액세스할 수 있는 명령을 결정합니다. 관리자 계정을 만들 때 역할을 할당합니다. 필요에 따라 다른 역할을 할당하거나 사용자 지정 역할을 정의할 수 있습니다.

네임스페이스 및 교차점

nas_namespace_는 단일 파일 시스템 계층을 생성하기 위해 _junction points_에 함께 결합된

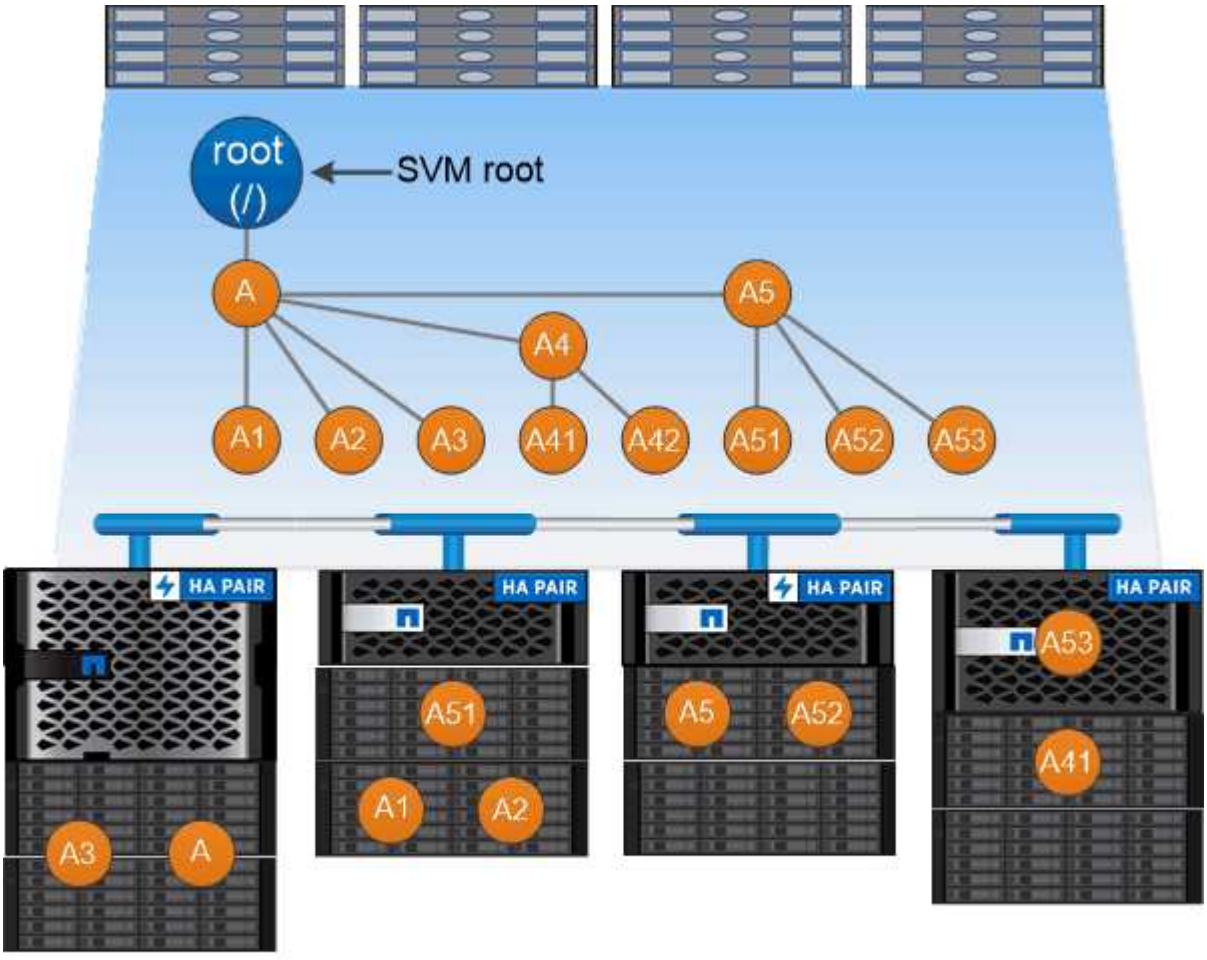
볼륨의 논리적 그룹입니다. 권한이 충분한 클라이언트는 저장소에 있는 파일의 위치를 지정하지 않고 네임스페이스의 파일에 액세스할 수 있습니다. Junced 볼륨은 클러스터의 모든 위치에 상주할 수 있습니다.

관심 파일이 포함된 모든 볼륨을 마운트하는 대신 NAS 클라이언트는 nfs_export_를 마운트하거나 smb_share에 액세스합니다. _ 내보내기 또는 공유는 전체 네임스페이스 또는 네임스페이스 내의 중간 위치를 나타냅니다. 클라이언트는 해당 액세스 지점 아래에 마운트된 볼륨만 액세스합니다.

필요에 따라 네임스페이스에 볼륨을 추가할 수 있습니다. 상위 볼륨 접합 바로 아래 또는 볼륨 내의 디렉토리에 접합 지점을 생성할 수 있습니다. "vol3"이라는 이름의 볼륨에 대한 볼륨 접합부의 경로는 "/vol1/vol2/vol3" 또는 "/vol1/dir2/vol3" 또는 "/dir1/dir2/vol3"일 수 있습니다. 이 경로를 _junction path ._라고 합니다

모든 SVM에는 고유한 네임스페이스가 있습니다. SVM 루트 볼륨은 네임스페이스 계층 구조의 진입점입니다.

노드 운영 중단 또는 페일오버 발생 시에도 데이터가 계속 사용 가능하도록 하려면 SVM 루트 볼륨에 대해 _load-sharing mirror_copy를 생성해야 합니다.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

예

다음 예에서는 junction path "/eng/home"이 있는 SVM VS1 상에 ""home4""라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

경로 페일오버

경로 페일오버 개요

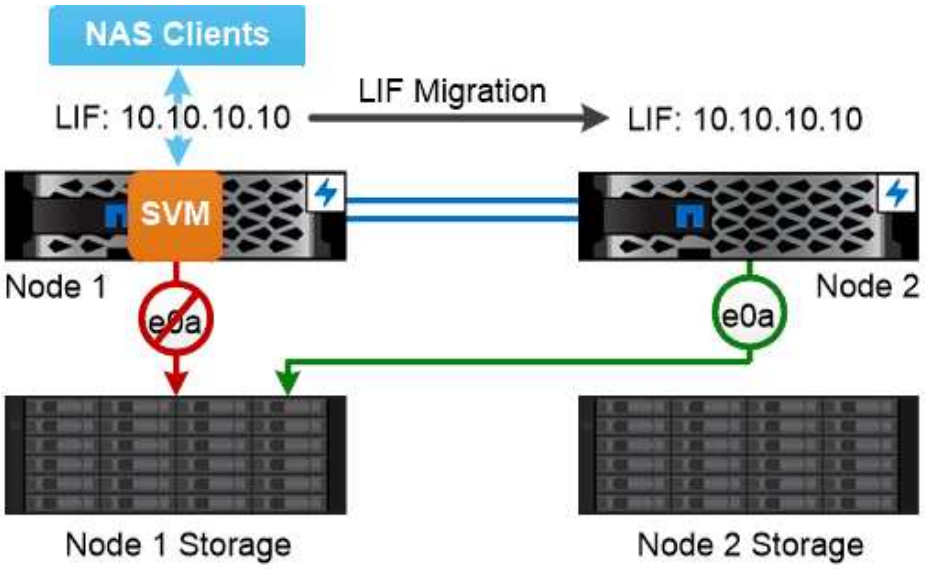
ONTAP가 NAS 및 SAN 토폴로지에서 경로 페일오버를 관리하는 방식에 있어 중요한 차이점이 있습니다. NAS LIF는 링크 장애 후 다른 네트워크 포트로 자동 마이그레이션됩니다. SAN LIF는 마이그레이션하지 않습니다(장애 후 수동으로 이동하지 않는 경우). 대신, 호스트의 다중 경로 기술은 동일한 SVM에서 트래픽을 다른 LIF로 전환하지만 다른 네트워크 포트에 액세스합니다.

NAS 경로 페일오버

NAS LIF는 현재 포트에서 링크 장애가 발생하면 작동 가능한 네트워크 포트로 자동 마이그레이션됩니다. LIF가 마이그레이션되는 포트는 LIF의 _페일오버 그룹 _ 의 구성원이어야 합니다. failover group policy_narrows는 데이터 LIF의 페일오버 목표를 데이터와 해당 HA 파트너가 속한 노드의 포트로 좁힙니다.

관리 편의를 위해 ONTAP는 네트워크 아키텍처에서 각 _broadcast domain_에 대한 페일오버 그룹을 생성합니다. 브로드캐스트 도메인은 동일한 계층 2 네트워크에 속하는 포트를 그룹화합니다. VLAN을 사용하여 트래픽을 부서(엔지니어링, 마케팅, 재무 등)별로 분리하는 경우 각 VLAN은 별도의 브로드캐스트 도메인을 정의합니다. 브로드캐스트 도메인 포트를 추가하거나 제거할 때마다 브로드캐스트 도메인과 연결된 페일오버 그룹이 자동으로 업데이트됩니다.

페일오버 그룹이 최신 상태를 유지하도록 브로드캐스트 도메인을 사용하여 페일오버 그룹을 정의하는 것이 좋습니다. 그러나 브로드캐스트 도메인과 연결되지 않은 페일오버 그룹을 정의하려는 경우도 있습니다. 예를 들어, LIF가 브로드캐스트 도메인에 정의된 포트의 하위 집합에 있는 포트에만 페일오버되도록 할 수 있습니다.



A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.

- 서브넷*

a_subnet_은 브로드캐스트 도메인에서 IP 주소 블록을 예약합니다. 이러한 주소는 같은 계층 3 네트워크에 속하며 LIF를 생성할 때 브로드캐스트 도메인의 포트에 할당됩니다. 일반적으로 LIF 주소를 정의할 때 IP 주소와 네트워크 마스크를 지정하는 것보다 서브넷 이름을 지정하는 것이 더 쉽고 오류가 발생하기 쉽습니다.

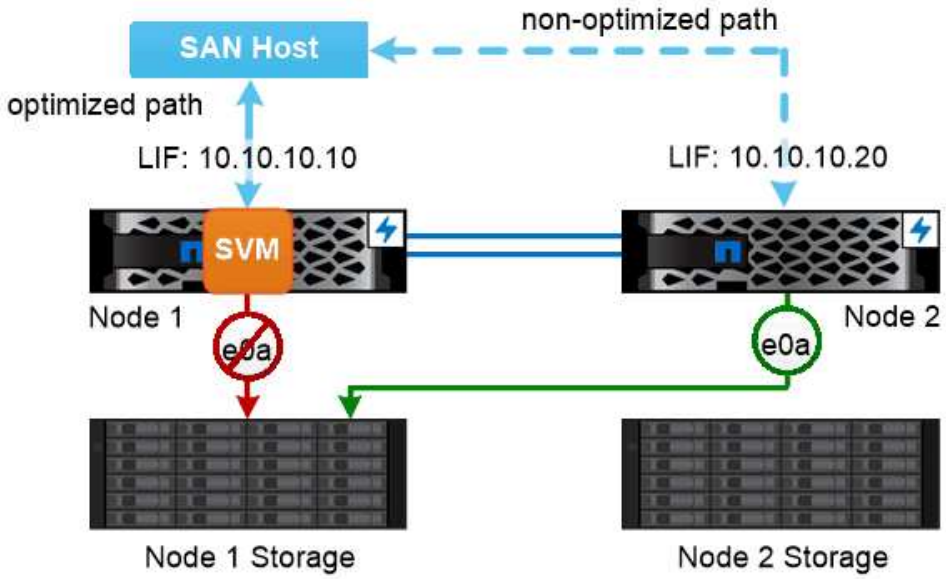
SAN 경로 페일오버

SAN 호스트는 ALUA(Asymmetric Logical Unit Access) 및 MPIO(다중 경로 I/O)를 사용하여 링크 장애 후 정상 LIF로 트래픽을 다시 라우팅합니다. 사전 정의된 경로는 SVM이 제공하는 LUN으로 연결되는 가능한 경로를 결정합니다.

SAN 환경에서 호스트는 lun_targets에 대한 요청의 _initiators_로 간주됩니다. _ MPIO 이니시에이터에서 타겟으로의 다중 경로를 활성화합니다. ALUA는 _optimized paths._라고 하는 가장 직접적인 경로를 식별합니다

일반적으로 LUN의 소유 노드에 있는 LIF에 대한 최적화된 경로를 여러 개 구성하고 HA 파트너에 대한 LIF에 최적화되지 않은 경로를 여러 개 구성합니다. 소유 노드에서 포트 중 하나에 장애가 발생하면 호스트는 트래픽을 나머지 포트로 라우팅합니다. 모든 포트에 장애가 발생하면 호스트는 최적화되지 않은 경로를 통해 트래픽을 라우팅합니다.

ONTAP 선택적 LUN 맵(SLM: Selective LUN Map)은 기본적으로 호스트에서 LUN으로의 경로 수를 제한합니다. 새로 생성된 LUN은 LUN 또는 해당 HA 파트너가 속한 노드의 경로를 통해서만 액세스할 수 있습니다. 이니시에이터에 대해 _port set_에서 LIF를 구성하여 LUN에 대한 액세스를 제한할 수도 있습니다.



A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.

- _SAN 환경에서 볼륨 이동 _ *

기본적으로 ONTAP_선택적 LUN 맵(SLM)_은 SAN 호스트에서 LUN에 대한 경로 수를 제한합니다. 새로 생성된 LUN은 LUN 또는 해당 HA 파트너인 LUN의 _ 보고 노드 _ 에 대한 경로를 통해서만 액세스할 수 있습니다.

즉, 볼륨을 다른 HA 쌍의 노드로 이동할 경우 대상 HA 쌍의 보고 노드를 LUN 매핑에 추가해야 합니다. 그런 다음 MPIO 설정에서 새 경로를 지정할 수 있습니다. 볼륨 이동이 완료된 후 매핑에서 소스 HA 쌍에 대한 보고 노드를 삭제할 수 있습니다.

ONTAP의 로드 밸런싱

노드의 작업 양이 사용 가능한 리소스를 초과하면 워크로드의 성능이 지연 시간의 영향을 받기 시작합니다. 사용 가능한 리소스를 증가(디스크 또는 CPU 업그레이드)하거나 로드를 감소(필요에 따라 볼륨 또는 LUN을 다른 노드로 이동)하여 과부하된 노드를 관리할 수 있습니다.

또한 ONTAP_스토리지 QoS(Quality of Service)_를 사용하여 경쟁 워크로드에 의해 중요 워크로드의 성능이 저하되지 않도록 보장할 수 있습니다.

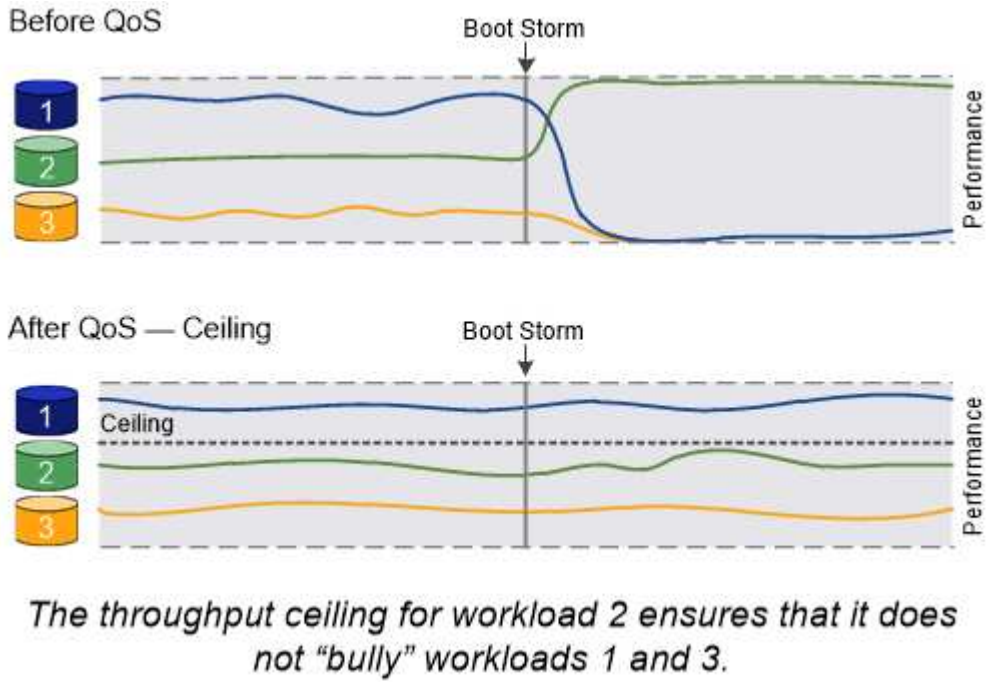
- 경쟁 워크로드에 QoS throughput_ceiling_을 설정하여 시스템 리소스에 미치는 영향을 제한할 수 있습니다(QoS Max).
- 중요 워크로드에 대해 QoS throughput_floor_를 설정하여 경쟁업체 워크로드(QoS Min)를 통해 수요에 관계없이 최소 처리량 목표를 충족할 수 있도록 합니다.
- 동일한 워크로드에 대해 QoS 상한과 최저값을 설정할 수 있습니다.

처리량 천정

처리량 상한은 워크로드의 처리량을 최대 IOPS 또는 MB/s로 제한합니다 아래 그림에서 워크로드 2의 처리량 상한은 워크로드 1과 3의 "불운" 워크로드가 되지 않도록 합니다.

policy group_은 하나 이상의 워크로드에 대한 처리량 한도를 정의합니다. 워크로드는 _ 스토리지 객체에 대한 입출력 작업을 나타냅니다. _ 볼륨, 파일 또는 LUN 또는 SVM의 모든 볼륨, 파일 또는 LUN입니다. 정책 그룹을 생성할 때 상한을 지정하거나 워크로드를 모니터링하여 지정할 때까지 기다릴 수 있습니다.

워크로드에 대한 처리량은 지정된 최대 10%까지 초과할 수 있으며, 특히 워크로드에 처리량이 급격하게 변경될 경우 더욱 그렇습니다. 천장은 버스트를 처리하기 위해 최대 50%까지 초과될 수 있습니다.



The throughput ceiling for workload 2 ensures that it does not "bully" workloads 1 and 3.

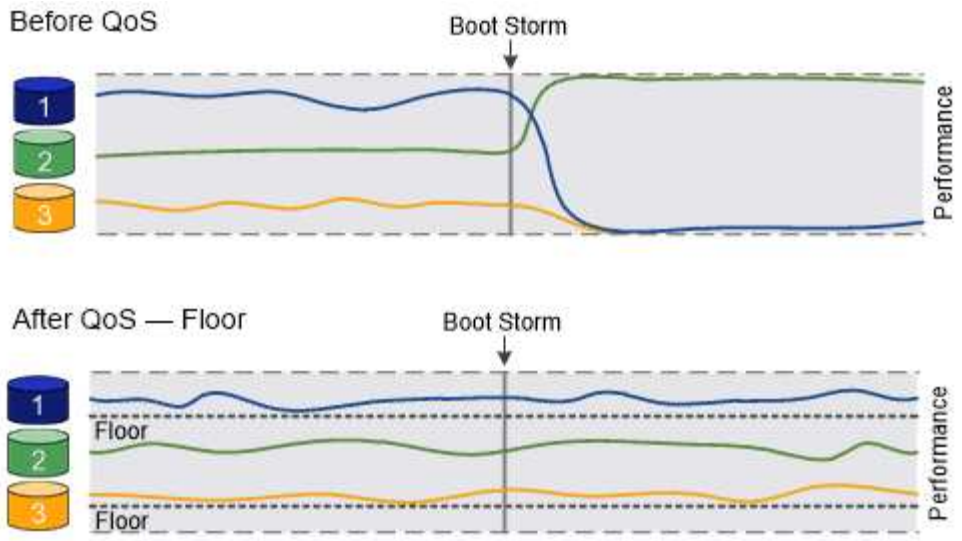
처리량 층

처리량 한도 에서는 워크로드의 처리량이 최소 IOPS 미만으로 떨어지지 않도록 보장합니다. 아래 그림에서 워크로드 1과 워크로드 3의 처리량 플로어는 워크로드 2의 수요에 관계없이 최소 처리량 목표를 충족할 수 있도록 합니다.

예를 들어, 처리량 상한은 처리량을 직접 조절합니다. 처리량 플로어에서는 플로어가 설정된 워크로드에 우선 순위를 부여하여 간접적으로 처리량을 조절합니다.

워크로드는 ONTAP 9.3 파일부터 볼륨, LUN 또는 파일에 대한 I/O 작업을 나타냅니다. 처리량 플로어를 정의하는 정책 그룹은 SVM에 적용할 수 없습니다. 정책 그룹을 생성할 때 층을 지정하거나 워크로드를 모니터링하여 지정할 때까지 기다릴 수 있습니다.

노드나 애그리게이트에 성능 용량(여유 공간)이 충분하지 않거나 '볼륨 이동 트리거-컷오버'와 같은 중요 운영 중에 워크로드에 대한 처리량이 지정된 바닥 아래로 떨어질 수 있습니다. 충분한 용량을 사용할 수 있고 중요한 작업이 마련되어 있지 않더라도 워크로드에 대한 처리량은 지정된 설치 공간 아래로 최대 5% 떨어질 수 있습니다.



The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

적응형 **QoS**

일반적으로 스토리지 객체에 할당한 정책 그룹의 값은 고정됩니다. 스토리지 오브젝트의 크기가 변경되면 값을 수동으로 변경해야 합니다. 예를 들어, 볼륨에 사용된 공간의 양을 늘리려면 일반적으로 볼륨에 지정된 처리량 상한을 늘려야 합니다.

_Adaptive QoS_는 워크로드 크기에 따라 정책 그룹 값을 자동으로 확장하며 워크로드 크기 변화에 따라 IOPS와 TB|GB의 비율을 유지합니다. 이는 대규모 구축 환경에서 수백 또는 수천 개의 워크로드를 관리할 때 큰 이점입니다.

일반적으로 적응형 QoS를 사용하여 처리량 한도를 조정할 수 있지만 워크로드 크기가 증가하는 경우 이를 사용하여 처리량 플로어를 관리할 수도 있습니다. 워크로드 크기는 스토리지 객체에 할당된 공간 또는 스토리지 객체가 사용하는 공간으로 표시됩니다.

ONTAP 9.5 이상의 처리량 층에서는 사용된 공간을 사용할 수 있습니다. ONTAP 9.4 이하 버전에서는 처리량 수준이 지원되지 않습니다.

+ ONTAP 9.13.1부터 적응형 QoS를 사용하여 SVM 레벨에서 처리량 하한과 상한을 설정할 수 있습니다.

- allocated space_policy는 스토리지 객체의 공칭 크기에 따라 IOPS/TB|GB 비율을 유지합니다. 비율이 100 IOPS/GB인 경우, 볼륨이 해당 크기로 유지되는 한 150 GB 볼륨의 처리량은 최대 15,000 IOPS입니다. 볼륨의 크기를 300GB로 변경하면 적응형 QoS는 처리량의 상한을 30,000 IOPS로 조정합니다.
- a_used space_policy(기본값)는 스토리지 효율성 이전에 저장된 실제 데이터의 양에 따라 IOPS/TB|GB 비율을 유지합니다. 비율이 100 IOPS/GB인 경우 100GB 데이터가 저장된 150GB 볼륨의 처리량은 최대 10,000 IOPS입니다. 사용된 공간의 양이 변경되면 적응형 QoS는 비율에 따라 처리량 상한을 조정합니다.

복제

스냅샷 수

기존에는 ONTAP 복제 기술을 사용하여 DR(재해 복구) 및 데이터 아카이빙에 대한 요구사항을 해결했습니다. 클라우드 서비스가 등장하면서 ONTAP 복제는 NetApp Data Fabric의

엔드포인트 간 데이터 전송에 맞게 조정되었습니다. 이러한 모든 사용의 기반은 ONTAP 스냅샷 기술입니다.

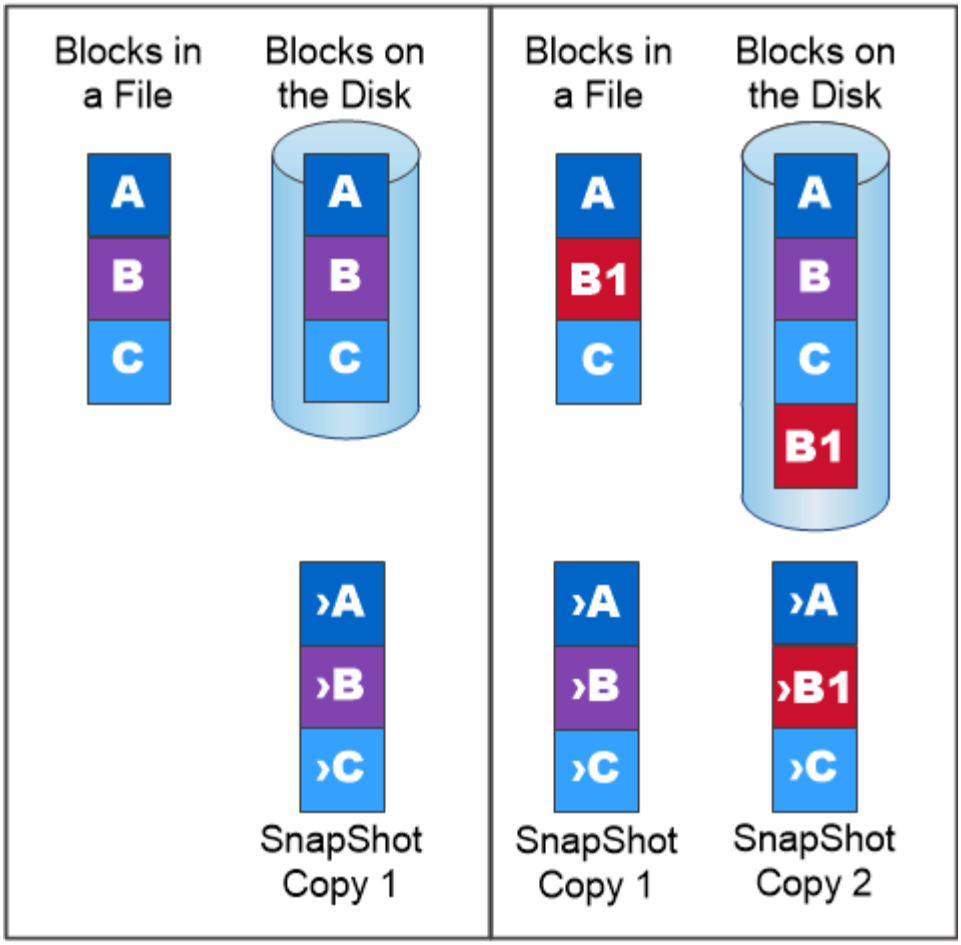
스냅샷 _ (이전 _ 스냅샷 사본 _)은(는) 볼륨의 읽기 전용 시점 이미지입니다. 스냅샷이 생성된 후에는 활성 파일 시스템과 스냅샷이 동일한 디스크 블록을 가리키므로 스냅샷은 추가 디스크 공간을 사용하지 않습니다. 시간이 지남에 따라 이미지는 최소한의 저장 공간을 소비하며 마지막 스냅샷이 생성된 이후 파일의 변경 사항만 기록하기 때문에 성능 오버헤드가 거의 발생하지 않습니다.

스냅샷은 ONTAP의 핵심 스토리지 가상화 기술인 ITS_WAFL(Write Anywhere File Layout)에 효율성을 가져다 줍니다._데이터베이스와 마찬가지로 WAFL은 메타데이터를 사용하여 디스크의 실제 데이터 블록을 가리킵니다. 하지만 WAFL은 데이터베이스와 달리 기존 블록을 덮어쓰지 않습니다. 업데이트된 데이터를 새 블록에 쓰고 메타데이터를 변경합니다.

ONTAP는 스냅샷 생성 시 데이터 블록이 아니라 메타데이터를 참조하기 때문에 스냅샷이 효율적입니다. 이렇게 하면 다른 시스템에서 복사할 블록을 찾는 데 발생하는 "탐색 시간"과 복사 자체를 만드는 비용이 모두 제거됩니다.

스냅샷을 사용하여 개별 파일 또는 LUN을 복구하거나 볼륨의 전체 내용을 복원할 수 있습니다. ONTAP는 스냅샷의 포인터 정보를 디스크의 데이터와 비교하여 누락되거나 손상된 개체를 재구성합니다. 이는 가동 중지 시간이나 상당한 성능 비용 없이 수행됩니다.

스냅샷 정책 _ 은(는) 시스템에서 볼륨의 스냅샷을 생성하는 방법을 정의합니다. 정책은 스냅샷을 생성할 시기, 보존할 복제본 수, 복제본 이름 지정 방법 및 복제를 위해 스냅샷 레이블을 지정하는 방법을 지정합니다. 예를 들어 시스템은 매일 오전 12시 10분에 스냅샷 하나를 생성하고 가장 최근의 사본 2개를 보존하고 ""daily""(타임 스탬프가 추가됨)로 이름을 지정하고 복제를 위해 ""daily""로 레이블을 지정할 수 있습니다.



A Snapshot copy records only changes to the active file system since the last Snapshot copy.

SnapMirror 재해 복구 및 데이터 전송

_SnapMirror_는 지리적으로 원격 사이트의 운영 스토리지에서 보조 스토리지로 페일오버하도록 설계된 재해 복구 기술입니다. 그 이름이 시사하듯이 SnapMirror는 운영 사이트에서 재해가 발생한 경우에도 데이터를 계속 제공할 수 있는 보조 스토리지에 작업 데이터의 복제본 또는 _MIRROR_를 생성합니다.

데이터가 볼륨 레벨에서 미러링됩니다. 운영 스토리지의 소스 볼륨과 2차 스토리지의 타겟 볼륨 간의 관계를 _ 데이터 보호 관계라고 합니다. _ 볼륨이 상주하는 클러스터와 볼륨에서 데이터를 제공하는 SVM은 _ 피어링되어야 합니다. _ 피어 관계를 통해 클러스터와 SVM이 서로 교환할 수 있습니다 안전하게 데이터 관리

SVM 간에 데이터 보호 관계를 생성할 수도 있습니다. 이러한 유형의 관계에서 NFS 엑스포트, SMB 공유에서 RBAC에 이르는 SVM 구성의 전체 또는 일부는 SVM이 소유한 볼륨의 데이터뿐만 아니라 복제됩니다.

ONTAP 9.10.1부터 SnapMirror S3를 사용하여 S3 버킷 간에 데이터 보호 관계를 생성할 수 있습니다. 타겟 버킷은 로컬 또는 원격 ONTAP 시스템 또는 StorageGRID 및 AWS와 같은 비 ONTAP 시스템에 있을 수 있습니다.

SnapMirror를 처음 호출하면 소스 볼륨에서 대상 볼륨으로 _baseline transfer_를 수행합니다. 기본 전송에는

일반적으로 다음 단계가 포함됩니다.

- 소스 볼륨의 스냅샷을 생성합니다.
- 스냅샷과 해당 스냅샷이 참조하는 모든 데이터 블록을 대상 볼륨으로 전송합니다.
- ""활성"" 미러가 손상된 경우 사용할 수 있도록 소스 볼륨의 나머지 덜 최근의 스냅샷을 대상 볼륨으로 전송합니다.

기본 전송이 완료되면 SnapMirror는 새 스냅샷만 미러에 전송합니다. 업데이트는 구성한 일정에 따라 비동기식입니다. 보존은 소스의 스냅샷 정책을 미러링합니다. 운영 사이트에서 재해가 발생할 경우 중단을 최소화하면서 대상 볼륨을 활성화하고 서비스가 복원될 때 소스 볼륨을 다시 활성화할 수 있습니다.

SnapMirror는 기준이 생성된 후에 스냅샷만 전송하므로 복제가 빠르고 중단되지 않습니다. 페일오버 사용 사례에서 알 수 있듯이, 2차 시스템의 컨트롤러는 미러링된 스토리지의 데이터를 효율적으로 지원하기 위해 운영 시스템의 컨트롤러와 동등하거나 거의 동등해야 합니다.

A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.

- _ 데이터 전송에 SnapMirror 사용 _ *

SnapMirror를 사용하여 NetApp Data Fabric의 엔드포인트 간에 데이터를 복제할 수도 있습니다. SnapMirror 정책을 생성할 때 1회 복제 또는 반복 복제 중에서 선택할 수 있습니다.

오브젝트 스토리지에 **SnapMirror** 클라우드를 백업

_SnapMirror CLOUD_는 데이터 보호 워크플로우를 클라우드로 전환하려는 ONTAP 사용자를 위해 설계된 백업 및 복구 기술입니다. 기존의 테이프 백업 아키텍처에서 벗어나 있는 조직은 오브젝트 스토리지를 장기 데이터 보존 및 아카이빙을 위한 대체 저장소로 사용할 수 있습니다. SnapMirror 클라우드는 증분 영구 백업 전략의 일부로 ONTAP-to-오브젝트 스토리지 복제를 제공합니다.

SnapMirror 클라우드 복제는 ONTAP 라이센스로 제공되는 기능입니다. SnapMirror 클라우드는 ONTAP 9 .8에 SnapMirror 복제 기술 제품군의 확장으로 도입되었습니다. SnapMirror는 ONTAP-to-ONTAP 백업에 자주 사용되지만,

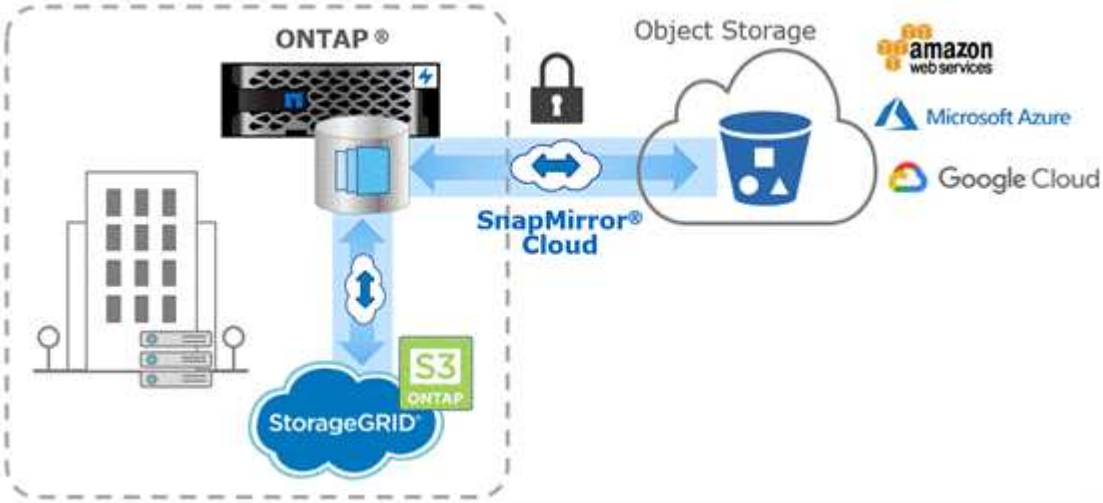
SnapMirror 클라우드는 동일한 복제 엔진을 사용하여 ONTAP의 스냅샷을 S3 호환 오브젝트 스토리지 백업으로 전송합니다.

백업 사용 사례에 적합한 SnapMirror 클라우드는 장기 보존 및 아카이브 워크플로우를 모두 지원합니다. SnapMirror와 마찬가지로, 초기 SnapMirror 클라우드 백업은 볼륨의 기본 전송을 수행합니다. 이후 백업의 경우 SnapMirror 클라우드는 소스 볼륨의 스냅샷을 생성하고 변경된 데이터 블록만 가진 스냅샷을 오브젝트 스토리지 타겟으로 전송합니다.

SnapMirror 클라우드 관계는 ONTAP 시스템 간에 구성할 수 있으며 Amazon S3, Google Cloud Storage, Microsoft Azure Blob Storage를 포함한 온프레미스 및 퍼블릭 클라우드 오브젝트 스토리지 타겟을 선택할 수 있습니다. 추가 사내 오브젝트 스토리지 타겟에는 StorageGRID 및 ONTAP S3가 포함됩니다.

ONTAP System Manager를 사용하여 SnapMirror 클라우드 구성을 관리하는 것 외에도 SnapMirror 클라우드 백업을 관리하는 데 다음과 같은 다양한 오케스트레이션 옵션을 사용할 수 있습니다.

- SnapMirror 클라우드 복제를 지원하는 여러 타사 백업 파트너 참여 공급업체는 에서 이용할 수 "NetApp 블로그 "있습니다.
- ONTAP 환경을 위한 NetApp 네이티브 솔루션을 위한 NetApp 백업 및 복구
- 데이터 보호 워크플로우를 위한 맞춤형 소프트웨어를 개발하거나 자동화 툴을 활용하기 위한 API



SnapVault 아카이빙

SnapMirror 라이센스는 백업에 대한 SnapVault 관계와 재해 복구를 위한 SnapMirror 관계를 모두 지원하는 데 사용됩니다. ONTAP 9.3부터 SnapVault 사용권은 더 이상 사용되지 않으며, SnapMirror 사용권은 볼트, 미러, 미러 및 볼트 간 관계를 구성하는 데 사용할 수 있습니다. SnapMirror 복제는 스냅샷의 ONTAP-to-ONTAP 복제에 사용되며 백업 및 재해 복구 사용 사례를 모두 지원합니다.

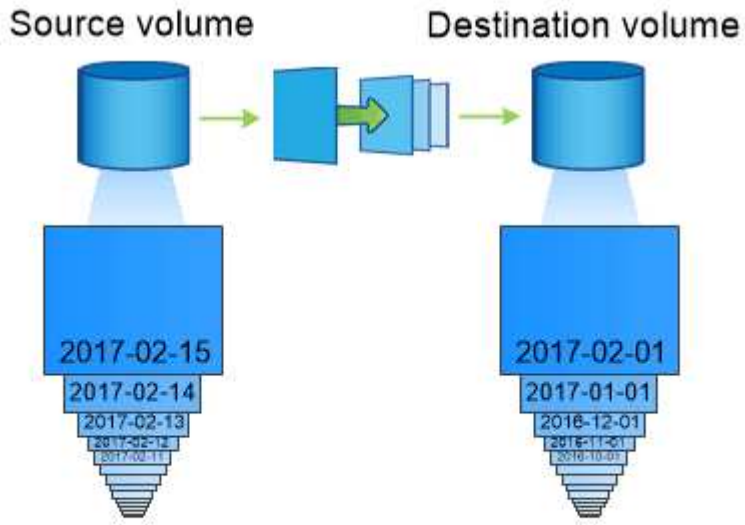
_SnapVault_는 표준 준수 및 기타 거버넌스 관련 목적을 위해 디스크 간 스냅샷 복제를 위해 설계된 아카이빙 기술입니다. 일반적으로 타겟에는 소스 볼륨에 있는 현재 스냅샷만 포함하는 SnapMirror 관계와는 달리, SnapVault 대상은 훨씬 더 오랜 기간 동안 생성된 시점 스냅샷을 보존합니다.

예를 들어, 비즈니스의 정부 회계 규정을 준수하기 위해 데이터의 월별 스냅샷을 20년 동안 보관할 수 있습니다. 볼트 스토리지에서 데이터를 제공할 필요가 없으므로 대상 시스템에서 느리고 저렴한 디스크를 사용할 수 있습니다.

SnapMirror와 마찬가지로 SnapVault은 사용자가 처음으로 호출할 때 기본 전송을 수행합니다. 소스 볼륨의 스냅샷을 생성한 다음 복사본과 해당 복사본이 타겟 볼륨에 참조하는 데이터 블록을 전송합니다. SnapMirror과 달리 SnapVault은 이전 스냅샷을 베이스라인에 포함하지 않습니다.

업데이트는 구성한 일정에 따라 비동기식입니다. 관계 정책에 정의된 규칙은 업데이트에 포함할 새 스냅샷과 보존할 복제본 수를 식별합니다. 정책에 정의된 레이블(예: ""월")은 소스의 스냅샷 정책에 정의된 하나 이상의 레이블과 일치해야 합니다. 그렇지 않으면 복제가 실패합니다.

SnapMirror와 SnapVault는 동일한 명령 인프라를 공유합니다. 정책을 생성할 때 사용할 방법을 지정합니다. 두 방법 모두 피어링된 클러스터와 피어링된 SVM이 필요합니다.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

클라우드 백업 및 기존 백업 지원

ONTAP 9.7 이하 버전을 위한 디스크-디스크 전용이었던 SnapMirror 및 SnapVault 데이터 보호 관계 외에도, 이제 여러 백업 솔루션을 통해 장기적인 데이터 보존을 위한 저렴한 대안을 제공합니다.

수많은 타사 데이터 보호 애플리케이션에서 ONTAP로 관리하는 데이터에 대한 기존 백업을 제공합니다. Veeam, Veritas, Commvault 중에서도 ONTAP 시스템을 위한 통합 백업을 제공합니다.

ONTAP 9.8부터 SnapMirror 클라우드는 ONTAP 인스턴스에서 오브젝트 스토리지 엔드포인트로 스냅샷의 비동기 복제를 제공합니다. SnapMirror 클라우드 복제를 사용하려면 데이터 보호 워크플로우의 오케스트레이션 및 관리를 위한 라이센스 애플리케이션이 필요합니다. SnapMirror 클라우드 관계는 ONTAP 시스템에서 지원되며 AWS S3, Google Cloud Storage Platform 또는 Microsoft Azure Blob Storage를 포함한 온프레미스 및 퍼블릭 클라우드 오브젝트 스토리지 타겟을 선택할 수 있어 공급업체 백업 소프트웨어의 효율성을 개선합니다. 지원되는 인증 애플리케이션 및 오브젝트 스토리지 공급업체 목록은 NetApp 담당자에게 문의하십시오.

클라우드 기반 데이터 보호에 관심이 있다면 NetApp 콘솔을 사용하여 온프레미스 볼륨과 퍼블릭 클라우드의 Cloud Volumes ONTAP 인스턴스 간의 SnapMirror 또는 SnapVault 관계를 구성할 수 있습니다.

콘솔은 SaaS(Software as a Service) 모델을 사용하여 Cloud Volumes ONTAP 인스턴스의 백업도 제공합니다.

사용자는 NetApp Backup and Recovery를 사용하여 Cloud Volumes ONTAP 인스턴스를 S3 및 S3 호환 퍼블릭 클라우드 개체 스토리지에 백업할 수 있습니다.

"Cloud Volumes ONTAP 설명서"

"NetApp 콘솔 설명서"

"NetApp 콘솔"

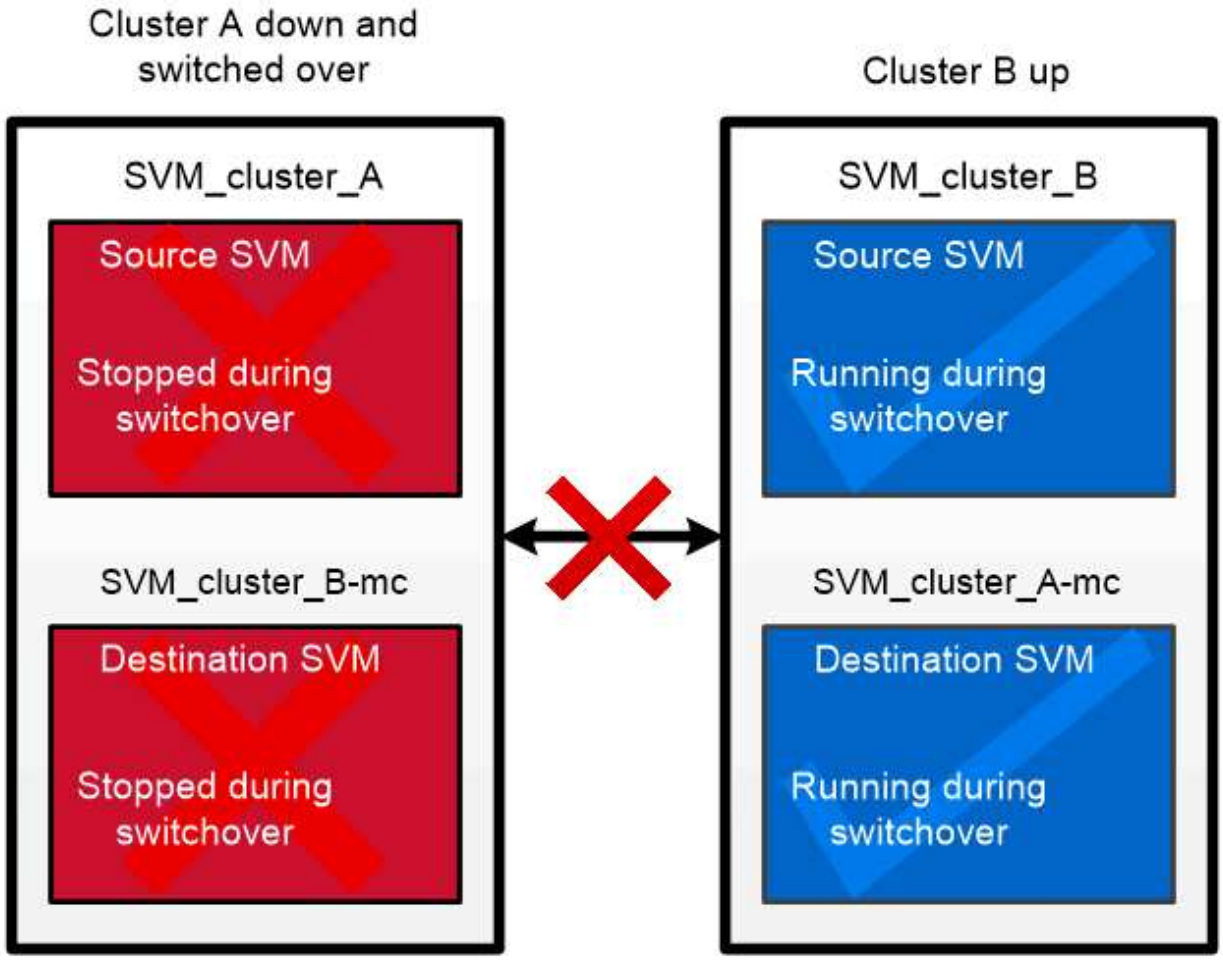
MetroCluster 지속적인 가용성

MetroCluster 구성은 물리적으로 분리된 2개의 미러링된 클러스터를 구현하여 데이터를 보호합니다. 각 클러스터는 다른 클러스터의 데이터와 SVM 구성을 동기식으로 복제합니다. 한 사이트에서 재해가 발생할 경우 관리자는 미러링된 SVM을 활성화하고 정상적인 사이트에서 데이터를 제공할 수 있습니다.

- _Fabric에 연결된 MetroCluster_및_MetroCluster IP_구성은 대도시 전역 클러스터를 지원합니다.
- *Stretch MetroCluster* 구성은 캠퍼스 전체 클러스터를 지원합니다.

클러스터는 어떠한 경우에도 자세히 살펴봐야 합니다.

MetroCluster는 _SyncMirror_라는 ONTAP 기능을 사용하여 각 클러스터의 집계 데이터를 다른 클러스터의 스토리지에서 복사 또는 _Plex_로 동기식으로 미러링합니다. 스위치오버가 발생하면 작동하는 클러스터의 원격 플렉스에서 온라인 상태가 되고 보조 SVM에서 데이터 제공을 시작합니다.



When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.

- 비 *MetroCluster* 구축에서 *SyncMirror* 사용 * 비 MetroCluster 구현에서 SyncMirror를 선택적으로 사용하여 RAID 유형이 보호하는 것보다 많은 디스크에 장애가 발생하거나 RAID 그룹 디스크에 대한 연결이 손실된 경우 데이터 손실을 방지할 수 있습니다. 이 기능은 HA 쌍에만 사용할 수 있습니다.

애그리게이트 데이터는 다른 디스크 쉘프에 저장된 플렉스로 미러링됩니다. 쉘프 중 하나를 사용할 수 없게 되면 장애 발생 원인을 해결하는 동안 영향을 받지 않는 플렉스가 계속해서 데이터를 제공합니다.

SyncMirror를 사용하여 미러링된 Aggregate는 미러링되지 않은 Aggregate보다 두 배 많은 스토리지가 필요합니다. 각 플렉스에는 플렉스 IT 미러 만큼 많은 디스크가 필요합니다. 예를 들어, 각 플렉스에 1,440GB Aggregate, 1,440GB를 미러링하려면 2,880GB의 디스크 공간이 필요합니다.

SyncMirror에서는 최적의 스토리지 성능과 가용성을 위해 미러링된 애그리게이트를 위한 여유 공간을 20% 이상 유지하는 것이 좋습니다. 미러링되지 않은 애그리게이트의 권장사항은 10%이지만, 파일 시스템이 증분 변경을 흡수하기 위해 추가 10%의 공간을 사용할 수 있습니다. 증분 변경은 ONTAP의 COW(Copy-on-Write) 스냅샷 기반 아키텍처로 인해 미러링된 애그리게이트의 공간 활용도를 증가시킵니다. 이 모범 사례를 준수하지 않을 경우 SyncMirror 재동기화 성능에 부정적인 영향을 미칠 수 있으며, 이는 비공유 클라우드 구축을 위한 NDU 및 MetroCluster 구축을 위한 스위치백과 같은 운영 워크플로우에 간접적으로 영향을 줄 수 있습니다.

스토리지 효율성

ONTAP 스토리지 효율성 개요

스토리지 효율성은 스토리지 리소스를 최적화하고, 낭비되는 공간을 최소화하고, 쓰인 데이터의 물리적 설치 공간을 줄임으로써 스토리지 시스템이 사용 가능한 공간을 얼마나 효과적으로 사용하는지를 측정한 것입니다. 스토리지 효율성을 높이면 최소 공간 내에 최저 비용으로 최대한 많은 양의 데이터를 저장할 수 있습니다. 예를 들어, 중복 데이터 블록과 0으로 채워진 데이터 블록을 감지하여 제거하는 스토리지 효율적인 기술을 사용하면 필요한 전체 물리적 스토리지의 양을 줄이고 전체 비용을 절감할 수 있습니다.

ONTAP은 다양한 스토리지 효율성 기술을 제공하여 데이터에 사용되는 물리적 하드웨어 또는 클라우드 스토리지의 양을 줄이고, 데이터 읽기 속도 향상, 데이터 세트 복사 속도 향상, VM 프로비저닝 속도 향상 등 시스템 성능을 크게 개선합니다.

ONTAP 스토리지 효율성 기술은 다음과 같습니다**.**

- * 씬 프로비저닝 *

  씬 프로비저닝 스토리지를 미리 예약하는 대신 필요한 만큼 볼륨 또는 LUN을 할당할 수 있습니다. 따라서 현재 사용되고 있지 않은 공간을 예약하지 않고 잠재적 사용량을 기반으로 볼륨 또는 LUN을 초과 할당할 수 있으므로 필요한 물리적 스토리지의 양이 줄어듭니다.

- * 데이터 중복 제거 *

  중복 제거 볼륨에 필요한 물리적 스토리지의 양을 세 가지 방법으로 줄입니다.

  - * 제로 블록 중복 제거 *

    제로 블록 중복제거는 0으로 채워진 데이터 블록을 감지하여 제거하고 메타데이터만 업데이트합니다. 그런 다음 일반적으로 제로 블록에 사용되는 공간의 100% 절약 중복제거된 모든 볼륨에 대해 제로 블록 중복제거가 기본적으로 활성화됩니다.

  - * 인라인 중복제거 *

    인라인 중복제거는 중복 데이터 블록을 감지하여 데이터를 디스크에 쓰기 전에 고유한 공유 블록에 대한 참조로 대체합니다. 인라인 중복제거 기능으로 VM 프로비저닝 속도를 20~30% 높일 수 있습니다. ONTAP의 버전과 플랫폼에 따라 볼륨 또는 애그리게이트 레벨에서 인라인 중복제거를 사용할 수 있습니다. AFF 및 ASA 시스템에서는 기본적으로 사용하도록 설정되어 있습니다. FAS 시스템에서 인라인 중복제거를 수동으로 활성화해야 합니다.

  - * 백그라운드 중복 제거 *

    백그라운드 중복제거는 또한 중복 데이터 블록을 감지하여 고유한 공유 블록에 대한 참조로 교체하지만, 데이터를 디스크에 쓴 후 이를 통해 스토리지 효율성을 더욱 높여줍니다. 스토리지 시스템에서 특정 조건이 충족될 때 실행되도록 백그라운드 중복제거를 설정할 수 있습니다. 예를 들어, 볼륨이 10% 활용도에 도달할 때 백그라운드 중복 제거를 사용하도록 설정할 수 있습니다. 또한 백그라운드 중복제거를 수동으로 트리거하거나 특정 일정에 따라 실행되도록 설정할 수 있습니다. AFF 및 ASA 시스템에서는 기본적으로 사용하도록 설정되어 있습니다. FAS 시스템에서 백그라운드 중복제거를 수동으로 활성화해야 합니다.

  중복제거는 애그리게이트 내의 볼륨 및 볼륨 전체에서 지원됩니다. 중복 제거된 데이터를 읽으면 일반적으로 성능 저하가 발생하지 않습니다.

- * 압축 *

  압축 각각 단일 블록으로 저장되는 압축 그룹의 데이터 블록을 결합하여 볼륨에 필요한 물리적 스토리지 양을 줄입니다. 읽기 또는 덮어쓰기 요청을 받으면 전체 파일이 아닌 소규모 블록 그룹만 읽습니다. 따라서 이 프로세스에서는 읽기 및 덮어쓰기 성능이 최적화되며 압축하는 파일의 크기 면에서 더 나은 확장성을 제공합니다.

  압축은 인라인으로 실행하거나 사후에 실행할 수 있습니다. 인라인 압축은 디스크에 쓰기 전에 메모리의 데이터를 압축하여 공간을 즉각적으로 절약해 줍니다. 사후 처리 압축은 먼저 블록을 압축되지 않은 상태로 디스크에 기록한 다음 예약된 시간에 데이터를 압축합니다. 이 솔루션은 AFA 시스템에서 기본적으로 활성화되어 있습니다. 다른 모든 시스템에서 압축을 수동으로 활성화해야 합니다.

- * 압축 *

  컴팩션은 4KB 블록에 저장되지만 크기가 4KB 미만인 데이터 청크를 가져와 단일 블록으로 결합함으로써 볼륨에 필요한 물리적 스토리지의 양을 줄입니다. 컴팩션은 데이터가 메모리에 아직 있는 상태에서 수행되므로 디스크에서 불필요한 공간을 사용하지 않습니다. AFF 및 ASA 시스템에서는 기본적으로 사용하도록 설정되어 있습니다. FAS 시스템에서 컴팩션을 수동으로 활성화해야 합니다.

- * FlexClone 볼륨, 파일 및 LUN *

  FlexClone 기술 스냅샷 메타데이터를 활용하여 볼륨, 파일 또는 LUN의 쓰기 가능한 시점 복사본을 생성합니다. 복사본은 데이터 블록을 부모와 공유하므로 복사본 또는 해당 부모에 변경 사항이 기록될 때까지 메타데이터에 필요한 것을 제외하고 스토리지를 소비하지 않습니다. 변경 사항이 기록되면 델타만 저장됩니다.

  기존 데이터 세트 복사본을 생성하는 데 몇 분 또는 몇 시간이 걸릴 수 있습니다. FlexClone 기술을 사용하면 가장 큰 데이터 세트도 거의 즉시 복사할 수 있습니다.

- * 온도에 민감한 스토리지 효율성 *

  ONTAP는 "온도에 민감한 스토리지 효율성" 볼륨의 데이터에 액세스하는 빈도를 평가하고 해당 데이터에 적용되는 압축 수준에 해당 빈도를 매핑함으로써 이점을 제공합니다. 자주 액세스하지 않는 콜드 데이터의 경우 더 큰 데이터 블록이 압축됩니다. 자주 액세스하여 자주 덮어쓰는 핫 데이터의 경우 더 작은 데이터 블록이 압축되므로 프로세스 효율성이 향상됩니다.

  ONTAP 9.8에서 도입된 온도 감응형 스토리지 효율(TSSE)은 새로 생성된 씬 프로비저닝 AFF 볼륨에서 자동으로 활성화됩니다. 해당 기능은 활성화되어 있지 않습니다."AFF A70, AFF A90 및 AFF A1K 플랫폼" ONTAP 9.15.1에 도입된 이 기능은 하드웨어 오프로드 프로세서를 사용합니다.

  TSSE는 두꺼운 프로비저닝 볼륨에서만 지원되지 않습니다.

- * CPU 또는 전용 오프로드 프로세서 스토리지 효율성 *

  ONTAP 9.15.1부터"CPU 또는 전용 오프로드 프로세서 스토리지 효율성" 특정 AFF 및 FAS 플랫폼에서는 자동으로 활성화되며 구성이 필요하지 않습니다. 이러한 플랫폼은 온도에 민감한 저장 효율성을 사용하지 않습니다. 압축은 데이터가 차가워질 때까지 기다리지 않고 시작되며, 메인 CPU나 전용 오프로드 프로세서를 사용하여 수행됩니다. 이러한 플랫폼은 압축 데이터의 저장 효율성을 더욱 개선하기 위해 연속적인 물리적 블록을 순차적으로 패킹하는 방식도 사용합니다.

최소한의 노력으로 일상적인 운영에서 이러한 기술의 이점을 실현할 수 있습니다. 예를 들어 5,000명의 사용자에게 홈 디렉토리에 대한 스토리지를 제공해야 하고, 모든 사용자에게 필요한 최대 공간이 1GB라고 가정할 수 있습니다. 잠재적인 총 스토리지 요구 사항을 충족하기 위해 5TB 애그리게이트를 미리 예약할 수 있습니다. 하지만 홈 디렉토리 용량 요구 사항은 조직 전반에 걸쳐 매우 다양합니다. 조직에 총 5TB의 공간을 예약하는 대신 2TB 애그리게이트를

생성할 수 있습니다. 그런 다음 씬 프로비저닝을 사용하여 각 사용자에게 1GB의 스토리지를 할당하지만 필요한 경우에만 스토리지를 할당할 수 있습니다. 시간에 따라 애그리게이트를 능동적으로 모니터링하고 필요에 따라 실제 물리적 크기를 늘릴 수 있습니다.

다른 예로, 가상 데스크톱 간에 많은 양의 중복 데이터가 있는 VDI(가상 데스크톱 인프라)를 사용한다고 가정합니다. 중복 제거는 VDI에서 중복된 정보 블록을 자동으로 제거하고 원래 블록에 대한 포인터로 대체하여 스토리지 사용량을 줄입니다. 사용자 개입 없이 압축과 같은 다른 ONTAP 스토리지 효율성 기술을 백그라운드에서 실행할 수 있습니다.

ONTAP 디스크 파티셔닝 기술을 통해 스토리지 효율성도 향상됩니다. RAID DP 기술은 성능을 저하시키거나 디스크 미러링 오버헤드를 더하지 않고 이중 디스크 장애를 방지합니다. ONTAP 9의 고급 SSD 파티셔닝은 사용 가능한 용량을 20% 가까이 늘려 줍니다.

NetApp 클라우드에서 온프레미스 ONTAP 과 동일한 스토리지 효율성 기능을 제공합니다. 온프레미스 ONTAP 에서 클라우드로 데이터를 마이그레이션하면 기존 스토리지 효율성이 유지됩니다. 예를 들어, 비즈니스에 중요한 데이터가 포함된 SQL 데이터베이스를 온프레미스 시스템에서 클라우드로 옮기고 싶다고 가정해 보겠습니다. NetApp 콘솔에서 데이터 복제를 사용하여 데이터를 마이그레이션할 수 있으며, 마이그레이션 프로세스의 일부로 클라우드의 스냅샷에 대한 최신 온프레미스 정책을 활성화할 수 있습니다.

씬 프로비저닝

ONTAP은 스냅샷과 더불어 다양한 스토리지 효율성 기술을 제공합니다. 주요 기술에는 씬 프로비저닝, 중복제거, 압축 및 FlexClone 볼륨, 파일, 및 LUN을 누릅니다. 스냅샷과 마찬가지로 모든 것이 ONTAP의 WAFL(Write Anywhere File Layout)을 기반으로 구축되었습니다.

_thin-provisioned_volume 또는 LUN은 스토리지를 미리 예약하지 않는 것입니다. 대신 필요에 따라 스토리지가 동적으로 할당됩니다. 볼륨 또는 LUN의 데이터가 삭제되면 사용 가능한 공간이 스토리지 시스템으로 다시 해제됩니다.

귀사에서 5,000명의 사용자에게 홈 디렉토리용 스토리지를 제공해야 한다고 가정합니다. 가장 큰 홈 디렉토리는 1GB의 공간을 차지할 것으로 예상됩니다.

이 경우 5TB 물리적 스토리지를 구입할 수 있습니다. 홈 디렉토리를 저장하는 각 볼륨에 대해, 가장 큰 소비자의 요구를 충족시킬 수 있는 충분한 공간을 확보하게 됩니다.

그러나 현실적으로 홈 디렉토리 용량 요구 사항은 지역마다 크게 다르다는 점도 알고 있습니다. 모든 대용량 스토리지 사용자에게는 공간을 거의 또는 전혀 사용하지 않는 10명의 스토리지 관리자가 있습니다.

씬 프로비저닝을 사용하면 사용하지 않을 수도 있는 스토리지를 구입하지 않고도 대규모 스토리지 소비자의 요구를 충족할 수 있습니다. 스토리지 공간이 소비될 때까지 할당되지 않으므로, 일반적으로 집계에 포함된 5,000개 볼륨 각각에 1GB의 크기를 할당하여 2TB의 애그리게이트를 "오버""할 수 있습니다.

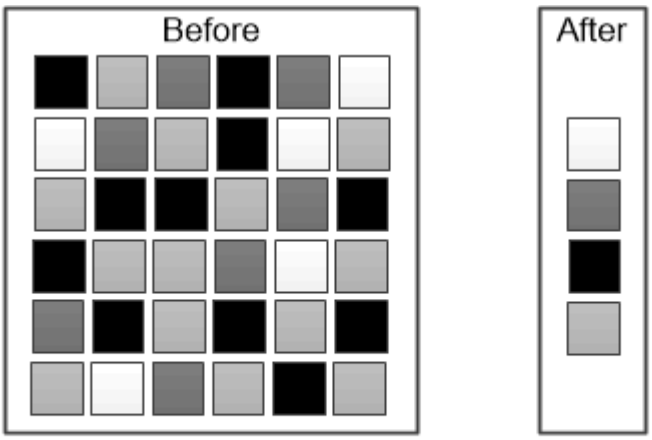
사용량이 많은 사용자에 대한 10:1 비율의 광량이 있고 애그리게이트의 여유 공간을 모니터링하는 데 적극적인 역할을 수행하는 한 공간 부족으로 인해 볼륨 쓰기가 실패하지 않을 수 있습니다.

중복 제거

_Deduplication_은 중복 블록을 버리고 단일 공유 블록에 대한 참조로 교체하여 볼륨에 필요한 물리적 스토리지의 양을 줄입니다(또는 AFF 애그리게이트의 모든 볼륨). 중복 제거된 데이터를 읽으면 일반적으로 성능 저하가 발생하지 않습니다. 쓰기 작업은 오버로드된 노드를 제외하고 무시할 만한 비용이 발생합니다.

정상적인 사용 중에 데이터가 기록될 때 WAFL는 배치 프로세스를 사용하여 _BLOCK 시그니처 카탈로그를 만듭니다. _ 중복 제거가 시작된 후 ONTAP는 카탈로그의 서명을 비교하여 중복된 블록을 식별합니다. 일치하는 항목이 있으면

카탈로그를 생성한 후 대상 블록이 변경되지 않았는지 확인하기 위해 바이트 단위로 비교됩니다. 모든 바이트가 일치하는 경우에만 중복된 블록이 삭제되고 해당 디스크 공간이 재확보됩니다.



Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.

압축

_Compression_은 각각 단일 블록으로 저장되는 _ 압축 그룹의 데이터 블록을 결합하여 볼륨에 필요한 물리적 스토리지의 양을 줄입니다. ONTAP는 전체 파일 또는 LUN이 아니라 요청된 데이터가 들어 있는 압축 그룹만 압축 해제하므로 압축된 데이터의 읽기는 기존 압축 방법보다 빠릅니다.

인라인 압축 또는 사후 처리 압축을 별도로 수행하거나 다음과 같이 조합하여 수행할 수 있습니다.

- _인라인 압축_디스크에 쓰기 전에 메모리에 있는 데이터를 압축하여 볼륨에 대한 쓰기 I/O 양을 크게 줄이지만 쓰기 성능을 저하시켜 줄 수 있습니다. 높은 성능이 필요한 작업은 다음 후처리 압축 작업(있는 경우)까지 지연됩니다.
- _후처리 압축_은 디스크에 기록된 데이터를 중복 제거와 동일한 일정에 따라 압축합니다.

- 인라인 데이터 컴팩션 * 0 으로 채워진 작은 파일 또는 입출력은 4KB 블록에 저장됩니다. _인라인 데이터 컴팩션 _ 는 일반적으로 여러 4KB 블록을 사용하는 데이터 청크를 디스크의 단일 4KB 블록으로 결합합니다. 컴팩션은 데이터가 메모리에 있는 동안 적용되므로 더 빠른 컨트롤러에 가장 적합합니다.

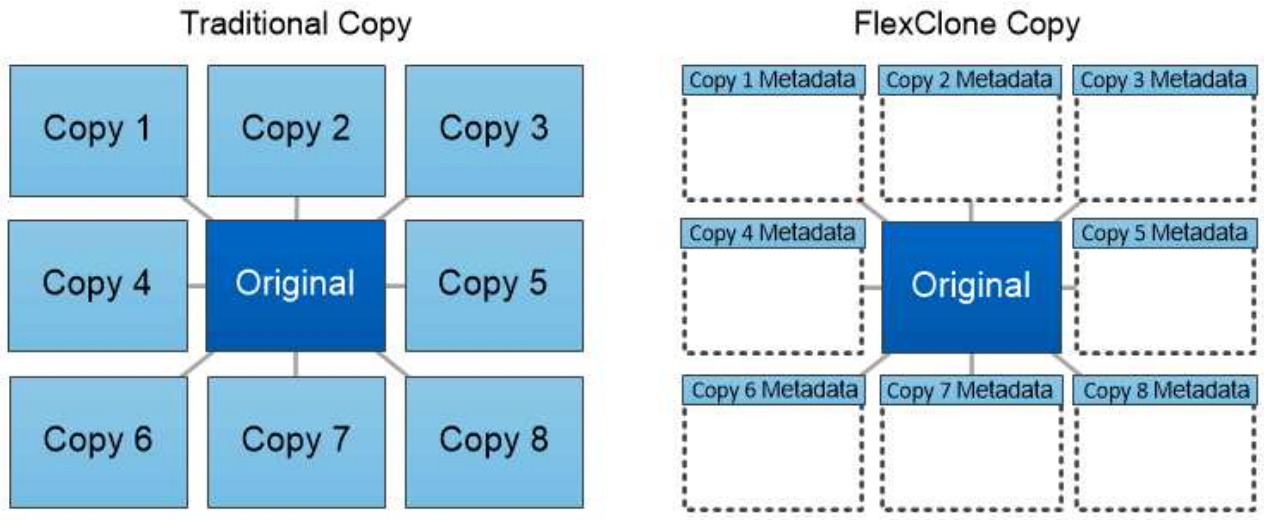
FlexClone 볼륨**,** 파일 및 **LUN**을 사용할 수 있습니다

_FlexClone_technology는 스냅샷 메타데이터를 참조하여 볼륨의 쓰기 가능한 시점 복제본을 생성합니다. 복사본은 데이터 블록을 부모님과 공유하므로 변경 사항이 복사본에 기록될 때까지 메타데이터에 필요한 것만 제외하고 스토리지가 필요하지 않습니다. FlexClone 파일 및 FlexClone LUN은 백업 스냅샷이 필요하지 않다는 점을 제외하고 동일한 기술을 사용합니다.

FlexClone 소프트웨어를 사용하면 기존 복사본을 생성하는 데 몇 분 또는 몇 시간이 걸릴 수 있으며 최대 규모의 데이터 세트도 거의 즉시 복사할 수 있습니다. 따라서 동일한 데이터 세트의 여러 복사본(예: 가상 데스크톱 구축)이 필요하거나 데이터 세트의 임시 복사본(운영 데이터 세트에 대해 애플리케이션 테스트)이 필요한 경우에 적합합니다.

기존 FlexClone 볼륨을 클론 복제하거나, LUN 클론을 포함하는 볼륨을 클론 복제하거나, 미러 및 소산 데이터를 클론

복제할 수 있습니다. 부모로부터 FlexClone 볼륨을 _split_할 수 있습니다. 이 경우 사본이 자체 스토리지를 할당하게 됩니다.



FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.

ONTAP 용량 보고 및 측정에 대해 알아보세요

ONTAP 스토리지 용량은 물리적 공간과 논리적 공간으로 측정할 수 있습니다. 이러한 측정값의 표시 방식은 ONTAP 버전과 System Manager 또는 Command Line Interface(CLI) 사용 여부에 따라 다릅니다. 스토리지 사용량을 모니터링할 때는 용량 관련 용어, 물리적 용량과 논리적 용량의 차이점, 그리고 용량 유형이 표시되는 방식을 이해하는 것이 중요합니다.

- * 물리적 용량 *: 물리적 공간은 볼륨 또는 로컬 계층에서 사용되는 스토리지의 물리적 블록을 의미합니다. 일반적으로 물리적 사용 용량의 값은 스토리지 효율성 기능(예: 중복제거, 압축)에서 데이터가 축소되기 때문에 논리적 사용 용량의 값보다 작습니다.
- * 논리적 용량 *: 논리적 공간은 볼륨 또는 로컬 계층에서 사용 가능한 공간(논리적 블록)을 의미합니다. 논리적 공간은 중복제거 또는 압축 결과를 고려하지 않고 이론적 공간을 사용할 수 있는 방법을 나타냅니다. 사용된 논리적 공간의 값은 사용된 물리적 공간의 양과 함께 구성된 스토리지 효율성 기능(예: 중복제거 및 압축)의 절감액을 기준으로 도출됩니다. 이 측정값은 스냅샷, 클론 및 기타 구성 요소가 포함되고 데이터 압축 및 물리적 공간의 기타 감소가 반영되지 않기 때문에 실제 사용된 용량보다 큰 것으로 나타나는 경우가 많습니다. 따라서 총 논리적 용량이 프로비저닝된 공간보다 클 수 있습니다.

CLI의 용량 보고

ONTAP CLI에서 물리적으로 사용된 공간은 ONTAP 버전에 따라 다르게 보고됩니다. ONTAP 9.13.1 및 이전 버전에서는 `physical used` 매개변수가 `volume show` 명령어 출력에 표시되며, 볼륨에 적용된 모든 스토리지 효율성 절감 효과를 포함합니다. ONTAP 9.14.1부터는 `physical used` 매개변수가 온도 민감 스토리지(TSSE), 인라인 압축, 컴팩션, 볼륨 간 중복제거와 같은 애그리게이트 수준의 스토리지 효율성 절감 효과를 포함하지 않으므로, 볼륨의 실제 물리적 사용 공간을 정확하게 반영하지 않습니다. ONTAP 9.14.1 및 이후 버전에서는 볼륨의 정확한 물리적 사용 공간을 확인하려면 `vol show-footprint` 명령어와 `effective_total_footprint` 매개변수를 사용해야 합니다.

ONTAP 버전	명령	매개 변수	설명
9.14.1 이상	볼륨 쇼 풋프린트	effective_total_footprint	애그리게이트의 절감 효과를 포함하여 실제 사용된 디스크 공간을 반영합니다.
	volume show-space	physical used	애그리게이트의 절감 효과를 포함하여 볼륨 레벨 스토리지 효율성 절감 효과를 반영합니다.
	'볼륨 쇼'	physical used	집계 수준의 스토리지 효율성 절감 효과가 포함되지 않으므로 "TSSE 지원 플랫폼"의 볼륨 물리적 사용 공간을 정확하게 반영하지 않습니다.
9.13.1 이하	볼륨 쇼 풋프린트	effective_total_footprint	애그리게이트의 절감 효과를 포함하여 실제 사용된 디스크 공간을 반영합니다.
	volume show-space	physical used	볼륨 레벨 스토리지 효율성 절감 효과만 반영합니다.
	'볼륨 쇼'	total physical used	볼륨 레벨 스토리지 효율성 절감 효과만 반영합니다.

관련 정보

- "9.14.1 이상에서 물리적 사용 공간 보고의 변경 사항"에 대해 자세히 알아보십시오.
- "공간 사용 정보를 표시하는 명령"에 대해 자세히 알아보십시오.

System Manager의 용량 보고

시스템 관리자에서 사용 용량 측정값은 ONTAP 버전에 따라 다르게 표시됩니다. ONTAP 9.7부터 시스템 관리자는 물리적 용량과 논리적 용량 모두를 측정하여 제공합니다.

System Manager에서 용량 표현은 루트 스토리지 계층(애그리게이트) 용량을 고려하지 않습니다.

System Manager의 버전입니다	용량에 사용되는 용어입니다	참조되는 용량 유형입니다
9.9.1 이상	논리적 사용	사용된 논리적 공간입니다 스토리지 효율성 설정이 사용된 경우)
9.7 및 9.8	사용됨	사용된 논리적 공간(스토리지 효율성 설정이 사용된 경우)
9.5 및 9.6(클래식 보기)	사용됨	사용된 물리적 공간입니다

용량 측정 용어

용량을 설명할 때 다음 용어가 사용됩니다.

- * 할당된 용량 *: 스토리지 VM의 볼륨에 할당된 공간의 양입니다.
- * 사용 가능 *: 데이터를 저장하거나 스토리지 VM 또는 로컬 계층에 볼륨을 프로비저닝하는 데 사용할 수 있는 물리적 공간의 양입니다.
- * 볼륨 간 용량 *: 스토리지 VM에 있는 모든 볼륨의 사용 가능한 스토리지 및 사용된 스토리지의 합계입니다.
- * 클라이언트 데이터 *: 클라이언트 데이터가 사용하는 공간(물리적 또는 논리적)입니다.
  - ONTAP 9.13.1부터 클라이언트 데이터가 사용하는 용량을 * 논리적 사용 * 이라고 하며 스냅샷이 사용하는 용량은 별도로 표시됩니다.
  - ONTAP 9.12.1 이하에서는 스냅샷이 사용하는 용량에 추가된 클라이언트 데이터가 사용하는 용량을 * 논리적 사용됨 * 이라고 합니다.
- * Committed *: 로컬 계층에 대해 커밋된 용량의 양입니다.
- * 데이터 축소 *: 수집된 데이터 크기와 저장된 데이터 크기의 비율.
  - ONTAP 9.13.1부터 데이터 축소는 중복제거, 압축과 같은 대부분의 스토리지 효율성 기능의 결과를 고려하지만, 스냅샷과 씬 프로비저닝은 데이터 축소율에 포함되지 않습니다.
  - ONTAP 9.12.1 및 이전 버전에서는 데이터 축소율이 다음과 같이 표시됩니다.
    - Capacity * 패널에 표시되는 데이터 축소 값은 물리적 사용 공간과 비교한 모든 논리적 사용 공간의 전체 비율이며, 스냅샷 및 기타 스토리지 효율성 기능을 사용하여 얻을 수 있는 이점이 포함됩니다.
    - 세부 정보 패널을 표시하면 개요 패널에 표시된 * 전체 * 비율과 클라이언트 데이터에서만 사용된 논리적 사용된 공간 대비 클라이언트 데이터에서만 사용된 물리적 사용 공간 비율(스냅샷 및 클론 없음 *)을 모두 볼 수 있습니다.
- * 논리적 사용 *:
  - ONTAP 9.13.1부터 클라이언트 데이터가 사용하는 용량을 * 논리적 사용 * 이라고 하며 스냅샷이 사용하는 용량은 별도로 표시됩니다.
  - ONTAP 9.12.1 이하에서는 스냅샷이 사용하는 용량에 추가된 클라이언트 데이터가 사용하는 용량을 * 논리적 사용됨 * 이라고 합니다.
- * 논리적 사용된 용량 % *: 프로비저닝된 크기와 비교한 현재 논리적 사용 용량의 백분율입니다(스냅샷 예비 공간 제외). 이 값에는 볼륨의 효율성 절약이 포함되어 있으므로 100%보다 클 수 있습니다.
- * 최대 용량 *: 스토리지 VM의 볼륨에 할당되는 최대 공간입니다.
- * 물리적 사용 *: 볼륨 또는 로컬 계층의 물리적 블록에 사용된 용량입니다.
- * 물리적 사용 % *: 프로비저닝된 크기에 비해 볼륨의 물리적 블록에 사용된 용량의 비율입니다.
- * 프로비저닝된 용량 *: Cloud Volumes ONTAP 시스템에서 할당되었으며 사용자 또는 애플리케이션 데이터를 저장할 준비가 된 파일 시스템(볼륨)입니다.
- * 예약됨 *: 로컬 계층에서 이미 프로비저닝된 볼륨에 예약된 공간입니다.
- * 사용됨 *: 데이터가 포함된 공간의 크기입니다.
- * 사용 및 예약 *: 물리적 사용 공간과 예약된 공간의 합계입니다.

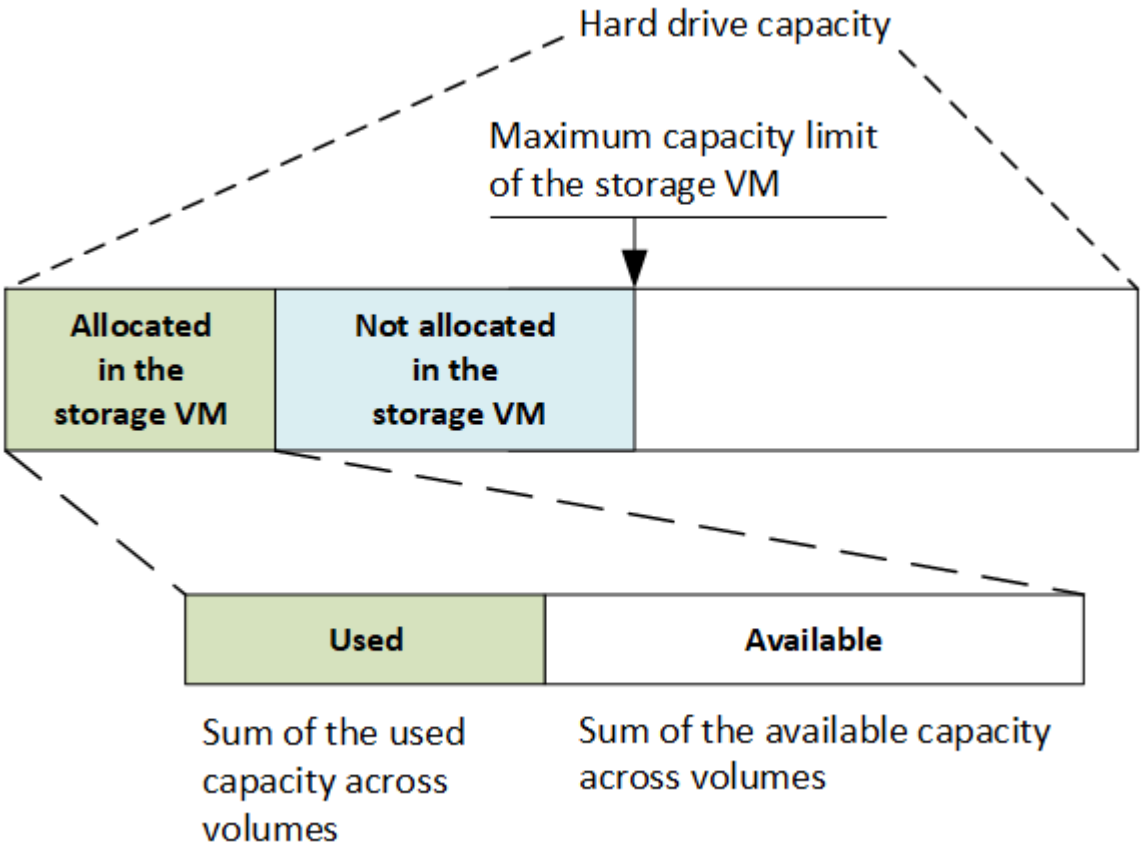
스토리지 **VM**의 용량입니다

스토리지 VM의 최대 용량은 볼륨에 할당된 총 공간과 할당되지 않은 나머지 공간에 따라 결정됩니다.

- 볼륨에 할당된 공간은 사용된 용량과 FlexVol 볼륨, FlexGroup 볼륨 및 FlexCache 볼륨의 사용 가능한 용량 합입니다.

- 볼륨 용량은 제한, 오프라인 또는 삭제 후 복구 대기열에 있는 경우에도 합에 포함됩니다.
- 볼륨이 자동 증량으로 구성된 경우 볼륨의 최대 자동 크기 조정 값이 합에 사용됩니다. 자동 확장이 없으면 볼륨의 실제 용량이 합에 사용됩니다.

다음 차트는 볼륨 전체의 용량을 측정하는 방식이 최대 용량 제한과 어떤 관련이 있는지 설명합니다.



ONTAP 9.13.1 을 시작으로 클러스터 관리자가 할 수 있습니다 "스토리지 VM의 최대 용량 한도 설정". 그러나 데이터 보호용 볼륨, SnapMirror 관계 또는 MetroCluster 구성이 포함된 스토리지 VM에 대해 스토리지 제한을 설정할 수 없습니다. 또한 할당량을 스토리지 VM의 최대 용량을 초과하도록 구성할 수 없습니다.

최대 용량 제한이 설정된 후에는 현재 할당된 용량보다 작은 크기로 변경할 수 없습니다.

스토리지 VM이 최대 용량 제한에 도달하면 특정 작업을 수행할 수 없습니다. System Manager에서는 의 다음 단계를 수행할 것을 제안합니다 "* 인사이트 *".

System Manager의 용량 측정 단위

System Manager는 1024바이트(2^{10})바이트의 이진 단위를 기준으로 스토리지 용량을 계산합니다.

- ONTAP 9.10.1부터 스토리지 용량 유닛이 시스템 관리자에 KiB, MiB, GiB, TiB 및 PiB로 표시됩니다.
- ONTAP 9.10.0 이전 버전에서는 이러한 유닛이 시스템 관리자에 KB, MB, GB, TB 및 PB로 표시됩니다.

시스템 관리자에서 처리량을 위해 사용되는 단위는 모든 ONTAP 릴리즈에서 KB/s, MB/s, GB/s, TB/s 및 PB/s입니다.

용량 단위는 ONTAP 9.10.0 이하 버전에 대한 System Manager에 표시됩니다	용량 단위는 ONTAP 9.10.1 이상인 경우 시스템 관리자에 표시됩니다	계산	바이트 단위의 값입니다
KB를 클릭합니다	KiB	1024	1024바이트
MB	MIB	1024 * 1024	1,048,576바이트
GB	GiB	1024 * 1024 * 1024	1,073,741,824바이트
TB	TiB	1024 * 1024 * 1024	1,099,511,627,776바이트
PB	PIB	1024 * 1024 * 1024 * 1024	1,125,899,906,842,624바이트

관련 정보

"System Manager에서 클러스터, 계층, SVM 용량 모니터링"

"볼륨에 대한 논리적 공간 보고 및 적용"

ONTAP 온도 민감형 스토리지 효율성에 대해 알아보세요

ONTAP 볼륨의 데이터에 액세스하는 빈도를 평가하고 해당 빈도를 데이터에 적용된 압축 정도에 매핑하여 온도 민감형 스토리지 효율성(TSSE) 이점을 제공합니다. 자주 액세스되지 않는 콜드 데이터의 경우 더 큰 데이터 블록이 압축되고, 자주 액세스되고 더 자주 덮어쓰이는 핫 데이터의 경우 더 작은 데이터 블록이 압축되어 프로세스의 효율성이 높아집니다.

TSSE는 ONTAP 9.8에서 도입되었으며 새로 생성된 씬 프로비저닝 AFF 볼륨에서 자동으로 활성화됩니다. 기존의 씬 프로비저닝된 AFF 볼륨과 씬 프로비저닝된 비 AFF DP 볼륨에서 온도에 따른 스토리지 효율성 향상 기능을 활성화할 수 있습니다. TSSE는 고밀도 프로비저닝 볼륨에서 지원되지 않습니다.

다음 플랫폼에는 온도에 따른 저장 효율성이 적용되지 않습니다.

플랫폼	**ONTAP** 버전입니다
• AFF A1K 를 참조하십시오 • AFF A90 를 참조하십시오 • AFF A70 를 참조하십시오 • FAS90를 참조하십시오 • FAS70를 참조하십시오	9.15.1 이상

플랫폼	**ONTAP** 버전입니다
• AFF C80 를 참조하십시오 • AFF C60 를 참조하십시오 • AFF C30 를 참조하십시오 • AFF A50 를 참조하십시오 • AFF A30 를 참조하십시오	9.16.1 이상

이 플랫폼은 다음을 사용합니다."CPU 또는 전용 오프로드 프로세서 스토리지 효율성" . 압축은 메인 CPU나 전용 오프로드 프로세서를 사용하여 수행되며 핫 데이터나 콜드 데이터에 기반하지 않습니다.

시간이 지남에 따라 볼륨에서 사용되는 공간의 양은 8K 적응형 압축에 비해 TSSE에서 더 두드러질 수 있습니다. 이러한 동작은 TSSE와 8K 적응형 압축 간의 아키텍처 차이로 인해 예상됩니다.

"기본" 및 "효율적인" 모드 도입

ONTAP 9.10.1부터 _default_and_efficient_볼륨 수준 스토리지 효율성 모드는 AFF 시스템에만 도입되었습니다. 두 가지 모드를 통해 파일 압축(기본값) 중에서 선택할 수 있으며, 새 AFF 볼륨을 생성할 때의 기본 모드인 파일 압축(기본값) 또는 온도에 민감한 스토리지 효율성(효율적) 중에서 선택할 수 있습니다. 이 방식은 자동 적응형 압축을 사용하여 자주 액세스하지 않는 콜드 데이터에 대해 압축 절약 효과를 높입니다.

ONTAP 9.10.1 이상으로 업그레이드할 때 볼륨에 현재 활성화된 압축 유형을 기준으로 기존 볼륨에 스토리지 효율성 모드가 할당됩니다. 업그레이드하는 동안 압축이 활성화된 볼륨에 기본 모드가 할당되고, 온도에 민감한 스토리지 효율성을 활성화한 볼륨에 효율적인 모드가 할당됩니다. 압축이 사용되지 않을 경우 스토리지 효율성 모드는 빈 상태로 유지됩니다.

ONTAP 9.10.1"온도에 민감한 스토리지 효율성을 명시적으로 설정해야 합니다"을 사용하여 자동 적응형 압축을 활성화합니다. 하지만 AFF 플랫폼에서 데이터 컴팩션, 자동 중복제거 일정, 인라인 중복제거, 볼륨 간 인라인 중복제거, 볼륨 간 백그라운드 중복제거 등과 같은 기타 스토리지 효율성 기능은 기본 모드와 효율적인 모드 모두에서 기본적으로 사용됩니다.

FabricPool 지원 애그리게이트 및 모든 계층화 정책 유형에서 스토리지 효율성 모드(기본값 및 효율성)가 모두 지원됩니다.

C-Series 플랫폼에서 온도에 민감한 스토리지 효율성을 지원합니다

온도에 민감한 스토리지 효율성(TSSE)은 AFF C-Series 플랫폼에서 기본적으로 활성화되며, 대상 플랫폼에 다음 릴리스가 설치된 상태에서 볼륨 이동 또는 SnapMirror 사용하여 TSSE가 활성화되지 않은 플랫폼에서 TSSE가 활성화된 C-Series 플랫폼으로 씬 프로비저닝된 볼륨을 마이그레이션할 때도 활성화됩니다.

- ONTAP 9.12.1P4 이상
- ONTAP 9.13.1 이상

자세한 내용은 을 "볼륨 이동 및 SnapMirror 작업에 대한 스토리지 효율성 동작"참조하십시오.

기존의 씬 프로비저닝 볼륨의 경우 온도에 민감한 스토리지 효율성이 자동으로 활성화되지 않습니다. 하지만 다음과 같이 설정할 수 있습니다. "스토리지 효율성 모드를 수정합니다" 수동으로 효율 모드로 전환하세요.

스토리지 효율성 모드를 효율적으로 변경한 후에는 다시 변경할 수 없습니다.

인접한 물리적 블록을 순차적으로 압축하여 스토리지 효율성 향상

ONTAP 9.13.1 을 시작으로, 온도에 민감한 스토리지 효율성이 인접한 물리적 블록을 순차적으로 압축하여 스토리지 효율성을 더욱 향상합니다. 온도에 민감한 스토리지 효율성을 사용하는 볼륨은 시스템을 ONTAP 9.13.1 로 업그레이드할 때 자동으로 순차적 패킹을 지원합니다. 순차적 패킹이 활성화된 후에는 다음을 수행해야 "기존 데이터를 수동으로 다시 압축합니다"합니다.

ONTAP 전용 오프로드 프로세서 스토리지 효율성에 대해 알아보세요

전용 오프로드 프로세서 저장 효율성은 연속적인 물리적 블록의 순차적 패킹을 수행하고 32k 데이터 압축을 위해 전용 오프로드 프로세서를 사용합니다. 32k 압축을 사용하면 8k 적응형 압축을 사용하는 플랫폼과 달리 볼륨 수준에서 공간 절약이 실현되는 것과 달리 집계 수준에서 공간 절약이 실현됩니다. 전용 오프로드 프로세서 스토리지 효율성을 사용하는 플랫폼은 온도 민감 스토리지 효율성(TSSE)을 사용하지 않습니다. 즉, 압축은 핫 데이터나 콜드 데이터에 기반하지 않습니다. 이를 통해 성능에 영향을 미치지 않으면서 즉각적인 공간 절약 효과를 얻을 수 있습니다.

다음 플랫폼과 ONTAP 버전에서는 전용 오프로드 프로세서 스토리지 효율성이 기본적으로 활성화되어 있습니다.

AFF A20 플랫폼은 전용 오프로드 프로세서 저장 효율성을 지원하지 않습니다. AFF A20 플랫폼의 경우 SnapMirror 기술을 사용하여 마이그레이션된 데이터는 메인 CPU를 사용하여 자동으로 32k 인라인 압축으로 변환됩니다.

플랫폼	**ONTAP** 버전입니다
• AFF A1K 를 참조하십시오 • AFF A90 를 참조하십시오 • AFF A70 를 참조하십시오 • FAS90를 참조하십시오 • FAS70를 참조하십시오	9.15.1 이상
• AFF C80 를 참조하십시오 • AFF C60 를 참조하십시오 • AFF C30 를 참조하십시오 • AFF A50 를 참조하십시오 • AFF A30 를 참조하십시오	9.16.1 이상

다음 플랫폼의 경우 스토리지 효율성이 자동으로 활성화되므로 구성이 필요하지 않습니다. 이는 새로 생성된 모든 씬 프로비저닝 볼륨과 기존 데이터(다른 플랫폼에서 이동된 볼륨 포함)에 적용됩니다. 중복 제거는 공간 보장 설정에 관계없이 활성화됩니다. 압축과 데이터 압축은 모두 공간 보장을 없음으로 설정해야 합니다. 볼륨 이동이나 SnapMirror 기술을 사용하여 마이그레이션된 데이터는 자동으로 32k 인라인 압축으로 변환됩니다.

- AFF C80 를 참조하십시오
- AFF C60 를 참조하십시오
- AFF C30 를 참조하십시오

- AFF A1K 를 참조하십시오
- AFF A90 를 참조하십시오
- AFF A70 를 참조하십시오
- AFF A50 를 참조하십시오
- AFF A30 를 참조하십시오

다음 플랫폼의 경우, ONTAP 9.15.1 이상으로 업그레이드하기 전에 스토리지 효율성이 활성화되었던 기존 씬 프로비저닝 볼륨에서만 스토리지 효율성이 기본적으로 활성화됩니다. CLI 또는 REST API 방법을 사용하여 새로 생성된 볼륨에서 스토리지 효율성을 활성화할 수 있습니다. 볼륨 이동이나 SnapMirror 기술을 사용하여 마이그레이션된 데이터는 원래 플랫폼에서 압축이 활성화된 경우에만 32k 인라인 압축으로 변환됩니다.

- FAS90를 참조하십시오
- FAS70를 참조하십시오

지원되는 플랫폼 중 하나로 컨트롤러를 업그레이드하는 방법에 대한 정보는 다음을 참조하세요. "ONTAP 하드웨어 업그레이드 설명서" .

보안

클라이언트 인증 및 권한 부여

ONTAP는 표준 방법을 사용하여 클라이언트 및 관리자의 스토리지 액세스를 보호하고 바이러스로부터 보호합니다. 사용되지 않는 데이터의 암호화 및 WORM 스토리지의 고급 기술을 사용할 수 있습니다.

ONTAP는 신뢰할 수 있는 소스로 ID를 확인하여 클라이언트 시스템과 사용자를 인증합니다. ONTAP는 사용자의 자격 증명을 파일 또는 디렉터리에 구성된 권한과 비교하여 사용자가 파일 또는 디렉터리에 액세스할 수 있도록 승인합니다.

인증

로컬 또는 원격 사용자 계정을 생성할 수 있습니다.

- 로컬 계정은 계정 정보가 스토리지 시스템에 상주하는 계정입니다.
- 원격 계정은 계정 정보가 Active Directory 도메인 컨트롤러, LDAP 서버 또는 NIS 서버에 저장되는 계정입니다.

ONTAP는 로컬 또는 외부 이름 서비스를 사용하여 호스트 이름, 사용자, 그룹, 넷그룹 및 이름 매핑 정보를 조회합니다. ONTAP는 다음과 같은 이름 서비스를 지원합니다.

- 로컬 사용자
- DNS
- 외부 NIS 도메인입니다
- 외부 LDAP 도메인입니다

_name 서비스 스위치 table_은 네트워크 정보를 검색할 소스 및 검색 순서를 지정합니다(UNIX 시스템의 /etc/nsswitch.conf 파일에 해당하는 기능 제공). NAS 클라이언트가 SVM에 연결되면 ONTAP는 지정된 이름 서비스를 확인하여 필요한 정보를 얻습니다.

- *Kerberos* 지원* Kerberos는 클라이언트-서버 구현에서 사용자 암호를 암호화하여 "성 인증"을 제공하는 네트워크 인증 프로토콜입니다. ONTAP는 무결성 검사(krb5i)와 Kerberos 5 인증 및 개인 정보 검사(krb5p)를 지원합니다.

권한 부여

ONTAP은 세 가지 보안 수준을 평가하여 엔티티가 SVM에 있는 파일 및 디렉토리에 대해 요청된 작업을 수행할 수 있는 권한이 있는지 확인합니다. 액세스 권한은 보안 수준을 평가한 후 유효한 사용 권한에 따라 결정됩니다.

- 내보내기(NFS) 및 공유(SMB) 보안

  내보내기 및 공유 보안은 지정된 NFS 내보내기 또는 SMB 공유에 대한 클라이언트 액세스에 적용됩니다. 관리 권한이 있는 사용자는 SMB 및 NFS 클라이언트의 내보내기 및 공유 수준 보안을 관리할 수 있습니다.

- 스토리지 레벨 Access Guard 파일 및 디렉토리 보안

  스토리지 레벨 액세스 가드 보안은 SMB 및 NFS 클라이언트가 SVM 볼륨에 액세스하는 데 적용됩니다. NTFS 액세스 권한만 지원됩니다. ONTAP에서 UNIX 사용자에 대한 보안 검사를 수행하여 스토리지 수준 액세스 가드가 적용된 볼륨의 데이터에 액세스하려면 UNIX 사용자는 볼륨을 소유한 SVM에서 Windows 사용자에게 매핑해야 합니다.

- NTFS, UNIX 및 NFSv4 네이티브 파일 레벨 보안

  네이티브 파일 레벨 보안은 스토리지 객체를 나타내는 파일 또는 디렉토리에 존재합니다. 클라이언트에서 파일 수준 보안을 설정할 수 있습니다. 파일 권한은 SMB 또는 NFS를 사용하여 데이터를 액세스하든 관계없이 유효합니다.

SAML을 통한 인증

ONTAP는 원격 사용자 인증을 위해 SAML(Security Assertion Markup Language)을 지원합니다. 몇 가지 인기 ID 공급자(IdP)가 지원됩니다. 지원되는 IdP 및 SAML 인증 설정에 대한 자세한 내용은 을 참조하십시오 "SAML 인증을 구성합니다".

ONTAP REST API 클라이언트가 포함된 **OAuth 2.0**

Open Authorization(OAuth 2.0) 프레임워크에 대한 지원은 ONTAP 9.14부터 제공됩니다. 클라이언트가 REST API를 사용하여 ONTAP에 액세스할 때 OAuth 2.0만 사용하여 권한 부여 및 액세스 결정을 제어할 수 있습니다. 하지만 CLI, System Manager, REST API를 포함한 모든 ONTAP 관리 인터페이스에서 기능을 구성하고 사용하도록 설정할 수 있습니다.

표준 OAuth 2.0 기능은 널리 사용되는 여러 인증 서버와 함께 지원됩니다. 상호 TLS를 기반으로 보낸 사람 제한 액세스 토큰을 사용하면 ONTAP 보안을 더욱 강화할 수 있습니다. 또한 자체 포함된 범위, ONTAP REST 역할 및 로컬 사용자 정의와의 통합 등 다양한 인증 옵션을 사용할 수 있습니다. 을 참조하십시오 "ONTAP OAuth 2.0 구축 개요" 를 참조하십시오.

관리자 인증 및 **RBAC**

관리자는 로컬 또는 원격 로그인 계정을 사용하여 클러스터 및 SVM에서 자신을 인증합니다. 역할 기반 액세스 제어(RBAC)는 관리자가 액세스할 수 있는 명령을 결정합니다.

인증

로컬 또는 원격 클러스터 및 SVM 관리자 계정을 생성할 수 있습니다.

- 로컬 계정은 계정 정보, 공개 키 또는 보안 인증서가 스토리지 시스템에 상주하는 계정입니다.
- 원격 계정은 계정 정보가 Active Directory 도메인 컨트롤러, LDAP 서버 또는 NIS 서버에 저장되는 계정입니다.

DNS를 제외하고 ONTAP는 클라이언트를 인증하는 데 사용되는 것과 동일한 이름 서비스를 사용하여 관리자 계정을 인증합니다.

RBAC

관리자에게 할당된 _role_은 관리자가 액세스할 수 있는 명령을 결정합니다. 관리자 계정을 만들 때 역할을 할당합니다. 필요에 따라 다른 역할을 할당하거나 사용자 지정 역할을 정의할 수 있습니다.

바이러스 검사

스토리지 시스템에서 통합 바이러스 백신 기능을 사용하여 바이러스나 기타 악성 코드에 의해 데이터가 손상되는 것을 방지할 수 있습니다. ONTAP 바이러스 검사(*Vscan*)는 동급 최강의 타사 바이러스 백신 소프트웨어와 ONTAP 기능을 결합하여 언제 어떤 파일을 스캔할지 제어하는 데 필요한 유연성을 제공합니다.

스토리지 시스템은 타사 공급업체의 안티바이러스 소프트웨어를 호스팅하는 외부 서버로 검사 작업을 오프로드합니다. NetApp에서 제공하고 외부 서버에 설치된 *ONTAP* 안티바이러스 커넥터 는 스토리지 시스템과 바이러스 백신 소프트웨어 간의 통신을 처리합니다.

- 액세스 시 검사 _ 를 사용하여 클라이언트가 SMB를 통해 파일을 열거나 읽거나 이름을 바꾸거나 닫을 때 바이러스를 검사할 수 있습니다. 외부 서버가 파일의 스캔 상태를 보고할 때까지 파일 작업이 일시 중단됩니다. 파일이 이미 스캔되면 ONTAP에서 파일 작업을 허용합니다. 그렇지 않으면 서버에서 스캔을 요청합니다.

  NFS에 대해 액세스 시 검사는 지원되지 않습니다.

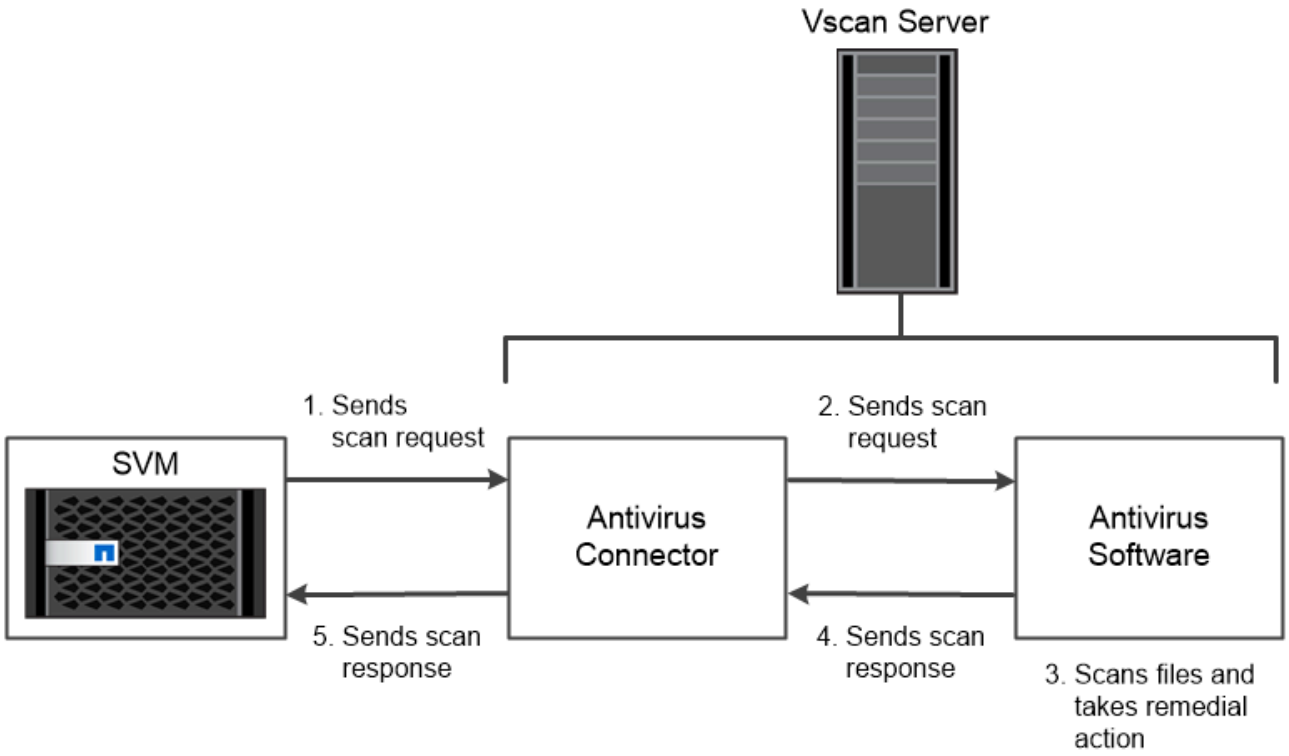
- 주문형 검사 _ 을(를) 사용하여 파일에 바이러스가 있는지 즉시 또는 일정에 따라 확인할 수 있습니다. 예를 들어, 사용량이 적은 시간에만 스캔을 실행할 수 있습니다. 외부 서버는 선택한 파일의 스캔 상태를 업데이트하므로 SMB를 통해 다음에 액세스할 때 해당 파일의 파일 액세스 지연 시간이 일반적으로 줄어듭니다.

  NFS를 통해서만 내보낸 볼륨에서도 SVM 네임스페이스에서 모든 경로에 대해 온디맨드 스캐닝을 사용할 수 있습니다.

일반적으로 SVM에서 두 스캐닝 모드를 모두 사용할 수 있습니다. 어느 모드에서든 바이러스 백신 소프트웨어는 소프트웨어의 설정에 따라 감염된 파일에 대한 치료 조치를 취합니다.

- _ 재해 복구 및 MetroCluster 구성에서 바이러스 검사 _ *

재해 복구 및 MetroCluster 구성을 위해서는 로컬 및 파트너 클러스터용으로 별도의 Vscan 서버를 설정해야 합니다.



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

암호화

ONTAP는 소프트웨어 및 하드웨어 기반 암호화 기술을 모두 제공하여 스토리지 미디어가 용도 변경, 반환, 잘못된 위치 변경 또는 도난된 경우 유휴 데이터를 읽을 수 없도록 합니다.

ONTAP는 모든 SSL 연결에 대해 FIPS(Federal Information Processing Standards) 140-2를 준수합니다. 다음 암호화 솔루션을 사용할 수 있습니다.

- 하드웨어 솔루션:
  - NSE(NetApp 스토리지 암호화)

    NSE는 SED(자체 암호화 드라이브)를 사용하는 하드웨어 솔루션입니다.
  - NVMe SED

    ONTAP는 FIPS 140-2 인증이 없는 NVMe SED에 대한 전체 디스크 암호화를 제공합니다.
- 소프트웨어 솔루션:
  - NetApp 애그리게이트 암호화(NAE)

    NAE는 각 애그리게이트의 고유 키를 사용하여 활성화된 모든 드라이브 유형의 모든 데이터 볼륨을 암호화할 수 있는 소프트웨어 솔루션입니다.
  - NetApp 볼륨 암호화(NVE)

    NVE는 각 볼륨의 고유 키를 사용해 활성화된 모든 드라이브 유형의 모든 데이터 볼륨을 암호화할 수 있는

소프트웨어 솔루션입니다.

소프트웨어(NAE 또는 NVE) 및 하드웨어(NSE 또는 NVMe SED) 암호화 솔루션을 모두 사용하여 유휴 데이터를 두 배로 암호화합니다. 스토리지 효율성은 NAE 또는 NVE 암호화의 영향을 받지 않습니다.

NetApp 스토리지 암호화

NSE(NetApp Storage Encryption)는 데이터를 쓸 때 암호화하는 SED를 지원합니다. 디스크에 저장된 암호화 키가 없으면 데이터를 읽을 수 없습니다. 암호화 키는 인증된 노드에서만 액세스할 수 있습니다.

I/O 요청 시 노드는 외부 키 관리 서버 또는 Onboard Key Manager에서 검색된 인증 키를 사용하여 SED에 대해 자신을 인증합니다.

- 외부 키 관리 서버는 KMIP(Key Management Interoperability Protocol)를 사용하여 노드에 인증 키를 제공하는 스토리지 환경의 타사 시스템입니다.
- Onboard Key Manager는 데이터와 동일한 스토리지 시스템의 노드에 인증 키를 제공하는 기본 제공 도구입니다.

NSE는 자체 암호화 HDD 및 SSD를 지원합니다. NSE와 함께 NetApp 볼륨 암호화를 사용하여 NSE 드라이브의 데이터를 이중 암호화할 수 있습니다.

> Flash Cache 모듈이 있는 시스템에서 NSE를 사용하는 경우, NVE 또는 NAE도 활성화해야 합니다. NSE는 Flash Cache 모듈에 상주하는 데이터를 암호화하지 않습니다.

NVMe 자체 암호화 드라이브

NVMe SED는 FIPS 140-2 인증을 보유하고 있지 않지만, 이러한 디스크는 AES 256비트 투명한 디스크 암호화를 사용하여 유휴 데이터를 보호합니다.

인증 키 생성과 같은 데이터 암호화 작업은 내부적으로 수행됩니다. 스토리지 시스템에서 디스크를 처음 액세스할 때 인증 키가 생성됩니다. 그런 다음, 데이터 작업이 요청될 때마다 스토리지 시스템 인증을 요구하여 유휴 데이터를 보호합니다.

NetApp 애그리게이트 암호화

NetApp Aggregate Encryption(NAE)은 애그리게이트의 모든 데이터를 암호화하는 소프트웨어 기반 기술입니다. NAE의 이점은 볼륨이 애그리게이트 레벨 중복제거에 포함되는 반면, NVE 볼륨은 제외된다는 것입니다.

NAE를 사용하도록 설정하면 애그리게이트 내의 볼륨을 애그리게이트 키로 암호화할 수 있습니다.

ONTAP 9.7부터"NVE 라이센스", 온보드 키 또는 외부 키 관리가 있는 경우 새로 생성된 애그리게이트와 볼륨은 기본적으로 암호화됩니다.

NetApp 볼륨 암호화

NetApp Volume Encryption(NVE)은 유휴 데이터를 한 번에 하나의 볼륨으로 암호화하는 소프트웨어 기반 기술입니다. 스토리지 시스템에서만 액세스할 수 있는 암호화 키를 사용하면 기본 디바이스가 시스템에서 분리되어 있는 경우 볼륨 데이터를 읽을 수 없습니다.

스냅샷 및 메타데이터를 포함한 두 데이터가 모두 암호화됩니다. 데이터에 대한 액세스는 볼륨별로 고유한 XTS-AES-256 키를 통해 제공됩니다. 내장 Onboard Key Manager는 동일한 시스템에 있는 키를 데이터와 함께 보호합니다.

NVE는 모든 유형의 애그리게이트(HDD, SSD, 하이브리드, 어레이 LUN), RAID 유형, ONTAP Select를 비롯한

지원되는 모든 ONTAP 구현에서 사용할 수 있습니다. NSE(NetApp 스토리지 암호화)와 NVE를 사용하여 NSE 드라이브의 데이터를 이중 암호화할 수 있습니다.

- *KMIP* 서버 사용 시기 * 저렴한 비용으로 일반적으로 Onboard Key Manager를 사용하는 것이 더 편리하지만, 다음 중 하나라도 해당되는 경우 KMIP 서버를 설치해야 합니다.
- 암호화 키 관리 솔루션은 FIPS(Federal Information Processing Standards) 140-2 또는 KMIP OASIS KMIP 표준을 준수해야 합니다.
- 다중 클러스터 솔루션이 필요합니다. KMIP 서버는 암호화 키를 중앙에서 관리하여 여러 클러스터를 지원합니다.

  KMIP 서버는 암호화 키를 중앙에서 관리하여 여러 클러스터를 지원합니다.
- 기업은 인증 키를 시스템 또는 데이터와 다른 위치에 저장하는 추가적인 보안을 필요로 합니다.

  KMIP 서버는 데이터와 별도로 인증 키를 저장합니다.

관련 정보

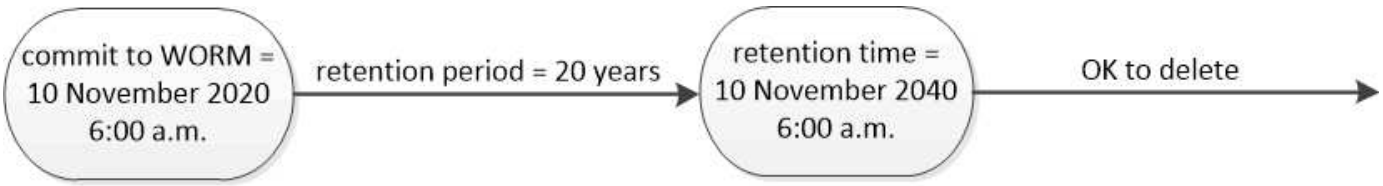
"FAQ - NetApp 볼륨 암호화 및 NetApp 애그리게이트 암호화"

WORM 스토리지

*SnapLock*_는 규정 및 거버넌스 목적을 위해 중요한 파일을 수정되지 않은 형태로 유지하기 위해 _*WORM(Write Once, Read Many)* 스토리지를 사용하는 조직을 위한 고성능 규정 준수 솔루션입니다.

단일 라이선스로 SnapLock를 Strict_Compliance 모드로 사용하고, SEC Rule 17a-4(f) 및 Loser_Enterprise 모드와 같은 외부 규정을 준수하여 디지털 자산 보호를 위한 내부 규정을 준수할 수 있습니다. SnapLock는 변조 방지 _ComplianceClock_을 사용하여 WORM 파일의 보존 기간이 경과되었는지 확인합니다.

SnapVault_에 _SnapLock를 사용하여 보조 스토리지에서 WORM-보호 스냅샷을 만들 수 있습니다. SnapMirror를 사용하여 재해 복구 및 기타 목적으로 WORM 파일을 다른 지리적 위치에 복제할 수 있습니다.



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.

ONTAP 및 VMware vSphere

ONTAP 및 관련 NetApp 제품을 VMware vSphere와 통합할 수 있습니다. 기술 환경 및 비즈니스 요구 사항에 따라 몇 가지 옵션을 사용할 수 있습니다.

선택한 개념 및 용어

VMware 환경에서 ONTAP 및 관련 NetApp 제품을 사용하기 시작하면서 몇 가지 핵심 용어와 개념을 숙지하는 것이 좋습니다.

논리 유닛 번호입니다

LUN은 SAN(Storage Area Network)에서 _logical unit_을 식별하는 데 사용되는 번호입니다. 이러한 주소 지정 가능한 디바이스는 일반적으로 SCSI(Small Computer System Interface) 프로토콜 또는 캡슐화된 파생 모델 중 하나를 통해 액세스되는 논리 디스크입니다.

VMware vSphere 가상 볼륨

VVOL(가상 볼륨)은 가상 머신에서 사용되는 스토리지에 대한 볼륨 수준 추상화를 제공합니다. 여기에는 여러 가지 이점이 있으며 기존 LUN을 사용하는 대신 사용할 수 있습니다.

영구 예약

영구 예약은 SCSI-3에서 지원되며 이전 SCSI-2 예약보다 향상되었습니다. 이를 통해 여러 클라이언트 이니시에이터가 다른 노드를 잠그는 동안 단일 대상과 통신할 수 있습니다. 오류 복구를 위해 버스를 재설정한 경우에도 예약이 지속될 수 있습니다.

ONTAP 9.15.1부터 SCSI-3을 사용하여 가상 볼륨에 대한 영구 예약을 생성할 수 있습니다. 이 기능은 WSFC(Windows Server Failover Cluster)가 있는 VMware vSphere 9용 ONTAP 툴을 사용하는 경우에만 지원됩니다.

Windows Server 장애 조치 클러스터링

Microsoft WSFC는 Windows Server 운영 체제의 기능으로 내결함성과 고가용성을 제공합니다. 일련의 서버 노드(물리적 또는 가상)가 클러스터로 결합되어 장애 발생 시 복원력을 제공합니다. WSFC는 일반적으로 데이터베이스, 파일 및 네임스페이스 서버를 비롯한 인프라 서비스를 배포하는 데 사용됩니다.

VMware vSphere Storage API - 스토리지 인식

VASA는 관리 및 관리를 위해 스토리지 어레이를 vCenter와 통합하는 API 세트입니다. 이 아키텍처는 VMware vSphere와 스토리지 시스템 간의 통신을 처리하는 _VASA Provider_를 비롯한 여러 구성 요소를 기반으로 합니다. ONTAP를 통해 이 공급자는 VMware vSphere용 ONTAP 툴의 일부로 구현됩니다.

VMware vSphere Storage API - 어레이 통합

VAAI는 VMware vSphere ESXi 호스트와 스토리지 디바이스 간의 통신을 지원하는 API 집합입니다. API에는 호스트에서 스토리지 작업을 스토리지로 오프로드하는 데 사용하는 기본 작업 세트가 포함되어 있습니다. VAAI는 스토리지 집약적인 작업에 대해 상당한 성능 향상을 제공할 수 있습니다.

NetApp SnapCenter를 참조하십시오

SnapCenter는 ONTAP 스토리지 시스템을 사용하는 애플리케이션, 데이터베이스, 호스트 파일 시스템 및 가상 머신에 대한 데이터 보호를 제공하는 확장 가능한 중앙 집중식 플랫폼입니다. SnapShot, SnapRestore, FlexClone, SnapMirror, SnapVault 등의 기본 ONTAP 기술을 활용합니다.

NetApp 플러그인 및 관련 기술

NetApp는 ONTAP 및 관련 제품을 VMware vSphere 기술과 통합하기 위한 강력한 지원을 제공합니다.

VMware vSphere용 **ONTAP** 툴

VMware vSphere용 ONTAP 툴은 ONTAP와 vSphere를 통합하기 위한 툴 세트입니다. VASA API 프레임워크의

공급자 기능을 구현합니다. ONTAP 툴에는 vCenter 플러그인, VMware 사이트 복구 관리자를 위한 SRA(스토리지 복제 어댑터), 자동화 애플리케이션을 구축하는 데 사용할 수 있는 REST API 서버도 포함되어 있습니다.

VMware VAAI용 NFS 플러그인

VMware VAAI용 NetApp NFS 플러그인을 사용하면 VAAI 기능에 액세스할 수 있습니다. 플러그인을 ESXi 호스트에 설치할 수 있으며 호스트에서 ONTAP의 NFS 데이터 저장소와 함께 VAAI를 활용할 수 있습니다. 클론 생성, 공간 예약 및 스냅샷 오프로딩을 비롯한 여러 작업을 제공합니다.

VMware 사이트 복구 관리자

VMware SRM(Site Recovery Manager)은 재해 복구 기능을 제공합니다. SRM은 VMware vSphere용 ONTAP 툴과 통합되어 ONTAP 데이터 관리 기능을 액세스하고 활용합니다.

vSphere Metro 스토리지 클러스터

vMSC(vSphere Metro Storage Cluster)는 _stretched cluster_deployment에서 vSphere를 활성화하고 지원하는 기술입니다. vMSC 솔루션은 NetApp MetroCluster 및 SnapMirror Active Sync(이전의 SMBC)에서 지원됩니다. 이러한 솔루션은 도메인 장애 시 향상된 비즈니스 연속성을 제공합니다. 복원력 모델은 특정한 구성 선택에 따라 달라집니다.

VMware vSphere용 SnapCenter 플러그인

SCV(SnapCenter Plug-in for VMware vSphere)는 SnapCenter 서버와 함께 구축하거나 독립 실행형 애플리케이션으로 구축할 수 있는 Linux 기반 가상 어플라이언스입니다. 두 경우 모두 SCV는 VM, 데이터 저장소 및 VMDK에 대한 백업 및 복원 작업을 제공합니다. 이 작업은 빠르고 공간 효율적이며 충돌 시에도 정합성이 보장되며 VM 정합성을 보장합니다.

자세한 정보를 확인하십시오

VMware vSphere 환경에서 ONTAP를 구축할 준비를 위해 사용할 수 있는 몇 가지 추가 리소스가 있습니다.

- "VMware vSphere용 ONTAP 툴 설명서"
- "엔터프라이즈 애플리케이션: ONTAP이 탑재된 VMware vSphere"
- "NetApp KB: SCSI 예약 및 SCSI 영구 예약이란 무엇입니까?"
- "VMware vSphere용 SnapCenter 플러그인 설명서"

FabricPool

많은 NetApp 고객은 거의 액세스하지 않는 저장된 데이터의 양이 상당히 많습니다. 이를 _cold_data 라고 합니다. 또한 고객은 자주 액세스되는 데이터를 가지고 있으며, 이를 _hot_data 라고 합니다. 가장 빠른 스토리지에 핫 데이터를 유지하여 최적의 성능을 발휘해야 합니다. 필요한 경우 즉시 사용 가능한 경우 콜드 데이터를 더 느린 스토리지로 이동할 수 있습니다. 하지만 데이터의 어떤 부분이 핫 데이터인지, 그리고 콜드 부품인지 어떻게 알 수 있을까요?

FabricPool는 액세스 패턴에 따라 고성능 로컬 계층과 클라우드 계층 간에 데이터를 자동으로 이동하는 ONTAP 기능입니다. 계층화는 클라우드에 있는 저비용 오브젝트 스토리지에서 콜드 데이터를 즉시 사용할 수 있도록 하면서 핫 데이터에 대한 값비싼 로컬 스토리지를 확보하게 됩니다. FabricPool는 데이터 액세스를 지속적으로 모니터링하고 계층 간에 데이터를 이동하여 최상의 성능과 최대 절감 효과를 제공합니다.

FabricPool를 사용하여 콜드 데이터를 클라우드에 계층화하면 클라우드 효율성을 확보하고 하이브리드 클라우드 구성을 생성하는 가장 쉬운 방법 중 하나가 됩니다. FabricPool는 스토리지 블록 레벨에서 작동하므로 파일 및 LUN 데이터 모두에서 작동합니다.

하지만 FabricPool는 온프레미스 데이터를 클라우드로 계층화하는 데만 목적이 아닙니다. 많은 고객이 Cloud Volumes ONTAP의 FabricPool를 사용하여 클라우드 공급자 내에서 비용이 높은 클라우드 스토리지의 콜드 데이터를 저렴한 오브젝트 스토리지로 계층화합니다. ONTAP 9.8부터 또는 를 사용하여 FabricPool가 활성화된 볼륨에 대한 분석을 캡처할 수 "파일 시스템 분석""온도에 민감한 스토리지 효율성"있습니다.

데이터를 사용하는 애플리케이션은 데이터가 계층화된다는 것을 알지 못하므로 애플리케이션을 변경할 필요가 없습니다. 계층화는 완전히 자동으로 이루어지므로 지속적인 관리가 필요하지 않습니다.

주요 클라우드 공급자 중 하나에서 오브젝트 스토리지에 콜드 데이터를 저장할 수 있습니다. 또는 NetApp StorageGRID를 선택하여 콜드 데이터를 자체 프라이빗 클라우드에 보관하면 최고의 성능과 완벽한 데이터 제어가 가능합니다.

관련 정보

"FabricPool 시스템 관리자 문서"

"NetApp 클라우드 계층화"

"NetApp TechComm TV의 FabricPool 재생 목록"

ONTAP를 위한 빠른 시작

ONTAP를 시작하려면 클러스터를 설정하고, 네트워크를 구성하고, BMC 자동 네트워크 구성을 활성화하고, 로컬 계층을 생성하고, 프로토콜을 구성하고, 스토리지를 프로비저닝해야 합니다.

클러스터 설정

NetApp은 경우에 System Manager를 사용할 것을 "새 ONTAP 클러스터 설정"권장합니다. System Manager에서 노드 관리 IP 주소의 할당 및 클러스터 초기화를 포함하여 클러스터 설정을 위한 간단하고 쉬운 워크플로를 제공합니다.

네트워크를 구성합니다

"브로드캐스트 도메인", "서브넷"및 선택적으로 를 만들어 네트워크를 "IP 공간"구성합니다.

BMC 자동 네트워크 구성을 활성화합니다

"BMC 자동 네트워크 구성을 활성화합니다", 따라서 각 노드의 BMC에 대한 IP 주소를 수동으로 할당할 필요가 없습니다.

로컬 계층을 생성합니다

"로컬 계층 생성" 노드의 가용 디스크 또는 SSD에서 데이터를 관리합니다. System Manager는 하드웨어에 따라 최적의 계층 구성을 자동으로 계산합니다.

5 프로토콜을 구성합니다

"NAS, SAN 또는 NVMe 프로토콜을 지원합니다" 클러스터 위에 있습니다.

6 스토리지를 프로비저닝합니다

또는 "산" 구성을 위한 스토리지 프로비저닝"NAS"

다음 단계

- "시스템 최적화를 위한 통찰력 확보"..
- "ONTAP 관리자 인증 및 RBAC(역할 기반 액세스 제어) 설정" 관리자의 기능을 정의합니다.
- "중요한 이벤트 관리 시스템(EMS) 알림을 보내도록 ONTAP 구성" 시스템 문제가 발생하여 주의가 필요할 경우 즉시 알림을 받을 수 있습니다.
- 에서 ONTAP를 사용하는 방법과 에서 를 "랜섬웨어 공격으로부터 데이터를 보호합니다"사용하는 방법에 대해 "재해 복구를 위해 데이터를 백업합니다"알아봅니다.
- "디지털 자문 및 AutoSupport에 대해 알아보기"..
- 에 System Manager를 "클러스터의 상태를 모니터링합니다"사용합니다.

ONTAP 클러스터 설정

ONTAP 클러스터 설정 워크플로 요약

클러스터를 설정하려면 설정을 완료하는 데 필요한 정보를 수집하고, 클러스터를 생성하고 노드를 조인하고, 관리 LIF를 IPv4에서 IPv6로 변환하고, Active IQ Config Advisor 로 클러스터를 확인하고, 클러스터 전체에서 시스템 시간을 동기화해야 합니다.

이 절차는 FAS, AFF 및 ASA 시스템에 적용됩니다.

- AFX 시스템이 있는 경우 다음을 따르세요. "수행할 수 있습니다" ONTAP 클러스터를 설정합니다.
- ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" ONTAP 클러스터를 설정합니다. ASA r2 시스템은 SAN 전용 고객에게 최적화된 간소화된 ONTAP 환경을 제공합니다.

1 **"정보를 수집합니다"**

클러스터 설정을 시작하기 전에 설정 프로세스를 완료하는 데 필요한 정보를 수집합니다.

2 **"ONTAP 클러스터를 생성하고 노드를 결합합니다"**

NetApp은 System Manager를 사용하여 새 클러스터를 설정할 것을 권장합니다. System Manager에서 노드 관리 IP 주소의 할당 및 클러스터 초기화를 포함하여 클러스터 설정을 위한 간단하고 쉬운 워크플로를 제공합니다.

3 "관리 **LIF**를 **IPv4**에서 **IPv6**로 변환합니다"

ONTAP 9.13.1부터 초기 클러스터 설정 중에 ONTAP CLI(Command Line Interface)를 사용하여 IPv6 주소를 AFF A800 및 FAS 8700 플랫폼의 관리 LIF에 할당할 수 있습니다. ONTAP 9.13.1 이전 릴리즈 또는 다른 플랫폼에서 9.13.1 이상인 경우, 먼저 관리 LIF에 IPv4 주소를 할당한 다음 클러스터 설정을 완료한 후 IPv6 주소로 변환해야 합니다.

4 "**Active IQ Config Advisor**에서 클러스터를 확인하십시오"

모든 노드를 새 클러스터에 결합했으면 Active IQ Config Advisor를 실행하여 구성을 검증하고 일반적인 구성 오류를 확인해야 합니다.

5 "클러스터 전체에서 시스템 시간을 동기화합니다"

클러스터 전체의 시스템 시간을 동기화하여 클러스터의 모든 노드가 동일한 시간을 유지하고 CIFS 및 Kerberos 장애를 방지합니다.

ONTAP 클러스터 설정 정보를 수집합니다

클러스터 설정을 시작하기 전에 클러스터 관리 인터페이스 포트 및 IP 주소 등과 같은 클러스터 설정을 완료하는 데 필요한 정보를 수집해야 합니다. 먼저 클러스터 설정 워크시트에 모든 관련 정보를 수집합니다. 클러스터 설정 워크시트를 사용하면 클러스터 설정 프로세스 중에 필요한 값을 기록할 수 있습니다. 기본값이 제공되는 경우 해당 값을 사용하거나 직접 입력할 수 있습니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" ONTAP 클러스터를 설정합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

시스템 기본값

시스템 기본값은 프라이빗 클러스터 네트워크의 기본값입니다. 이러한 기본값을 사용하는 것이 가장 좋습니다. 그러나 요구 사항을 충족하지 않는 경우에는 표를 사용하여 값을 기록할 수 있습니다.

ⓘ 네트워크 스위치를 사용하도록 구성된 클러스터의 경우 각 클러스터 스위치는 9000 MTU 크기를 사용해야 합니다.

정보 유형	당신의 가치
전용 클러스터 네트워크 포트	
클러스터 네트워크 넷마스크입니다	
클러스터 인터페이스 IP 주소(각 노드의 각 클러스터 네트워크 포트에 대해) 각 노드의 IP 주소는 같은 서브넷에 있어야 합니다.	

클러스터 정보

정보 유형	당신의 가치
클러스터 이름 이름은 문자로 시작해야 하며 44자 미만이어야 합니다. 이름은 다음과 같은 특수 문자를 포함할 수 있습니다 '-', _'	

기능 라이센스 키

초기 또는 애드온 소프트웨어 주문에 대한 라이센스 키는 NetApp Support 사이트 * My Support * > * Software Licenses * 에서 찾을 수 있습니다.

정보 유형	당신의 가치
기능 라이센스 키	

관리 스토리지 가상 시스템**(SVM)**

정보 유형	당신의 가치
클러스터 관리자 암호입니다 클러스터 관리자에게 콘솔에 대한 액세스 권한을 부여하거나 보안 프로토콜을 통해 액세스하기 전에 클러스터가 필요로 하는 admin 계정의 암호입니다. 보안을 위해 이 워크시트에 암호를 기록하는 것은 권장되지 않습니다. 암호의 기본 규칙은 다음과 같습니다. • 암호는 8자 이상이어야 합니다. • 암호는 하나 이상의 문자와 숫자를 포함해야 합니다.	
클러스터 관리 인터페이스 포트입니다 데이터 네트워크에 연결되어 클러스터 관리자가 클러스터를 관리할 수 있도록 하는 물리적 포트입니다.	

정보 유형	당신의 가치
클러스터 관리 인터페이스 IP 주소입니다 클러스터 관리 인터페이스의 고유 IPv4 또는 IPv6 주소입니다. 클러스터 관리자는 이 주소를 사용하여 admin SVM에 액세스하고 클러스터를 관리합니다. 일반적으로 이 주소는 데이터 네트워크에 있어야 합니다. 조직의 IP 주소 할당 담당자로부터 이 IP 주소를 얻을 수 있습니다. 예: 192.0.2.66	
클러스터 관리 인터페이스 넷마스크(IPv4) 클러스터 관리 네트워크에서 유효한 IPv4 주소 범위를 정의하는 서브넷 마스크입니다. 예: 255.255.255.0	
클러스터 관리 인터페이스 넷마스크 길이(IPv6) 클러스터 관리 인터페이스에서 IPv6 주소를 사용하는 경우 이 값은 클러스터 관리 네트워크에서 유효한 IPv6 주소 범위를 정의하는 접두사 길이를 나타냅니다. 예: 64	
클러스터 관리 인터페이스의 기본 게이트웨이입니다 클러스터 관리 네트워크의 라우터에 대한 IP 주소입니다.	
DNS 도메인 이름입니다 네트워크 DNS 도메인의 이름입니다. 도메인 이름은 영숫자로 구성되어야 합니다. 여러 DNS 도메인 이름을 입력하려면 각 이름을 쉼표 또는 공백으로 구분합니다.	
네임 서버 IP 주소 DNS 이름 서버의 IP 주소입니다. 각 주소를 쉼표 또는 공백으로 구분합니다.	

노드 정보(클러스터의 각 노드에 대해)

정보 유형	당신의 가치
컨트롤러의 물리적 위치(선택 사항) 컨트롤러의 물리적 위치에 대한 설명입니다. 클러스터에서 이 노드를 찾을 위치를 식별하는 설명을 사용하십시오(예: "'Lab 5, Row 7, Rack B').	
노드 관리 인터페이스 포트입니다 노드 관리 네트워크에 연결되어 있고 클러스터 관리자가 노드를 관리할 수 있도록 하는 물리적 포트입니다.	
노드 관리 인터페이스 IP 주소입니다 관리 네트워크의 노드 관리 인터페이스에 대한 고유한 IPv4 또는 IPv6 주소입니다. 노드 관리 인터페이스 포트를 데이터 포트로 정의한 경우 이 IP 주소는 데이터 네트워크에서 고유한 IP 주소여야 합니다. 조직의 IP 주소 할당 담당자로부터 이 IP 주소를 얻을 수 있습니다. 예: 192.0.2.66	
노드 관리 인터페이스 넷마스크(IPv4) 노드 관리 네트워크에서 유효한 IP 주소의 범위를 정의하는 서브넷 마스크입니다. 노드 관리 인터페이스 포트를 데이터 포트로 정의한 경우 넷마스크는 데이터 네트워크의 서브넷 마스크입니다. 예: 255.255.255.0	
노드 관리 인터페이스 넷마스크 길이(IPv6) 노드 관리 인터페이스에서 IPv6 주소를 사용하는 경우 이 값은 노드 관리 네트워크에서 유효한 IPv6 주소 범위를 정의하는 접두사 길이를 나타냅니다. 예: 64	
노드 관리 인터페이스의 기본 게이트웨이입니다 노드 관리 네트워크의 라우터에 대한 IP 주소입니다.	

NTP 서버 정보입니다

정보 유형	당신의 가치
NTP 서버 주소입니다 사이트에 있는 NTP(Network Time Protocol) 서버의 IP 주소입니다. 이러한 서버는 클러스터 전체에서 시간을 동기화하는 데 사용됩니다.	

ONTAP 클러스터를 생성하고 노드를 결합합니다

NetApp은 System Manager를 사용하여 새 클러스터를 생성하는 것이 좋습니다. System Manager는 클러스터 설정을 위한 간단하고 쉬운 워크플로를 제공합니다. MetroCluster 구성에서 ONTAP 9.7 이하를 실행 중이거나 특정 플랫폼에서 IPv6 전용 클러스터를 구성해야 하는 경우에만 ONTAP CLI(명령줄 인터페이스)를 사용해야 합니다.

이 작업에 대해

이 절차는 다음 사항에 적용됩니다. "AFF, ASA FAS" 그리고 "AFX 시스템". ASA R2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)을 사용 중인 경우 다음 단계를 따르십시오. "수행할 수 있습니다" 시스템 관리자를 사용하여 ONTAP 클러스터를 설정합니다. ASA r2 시스템은 SAN 전용 고객을 위해 간소화된 ONTAP 환경을 제공합니다.

ONTAP 9.13.1부터는 ONTAP CLI를 사용하여 초기 클러스터 설정 중에 AFF A800 및 FAS8700 플랫폼의 관리 LIF에 IPv6 주소를 할당할 수 있습니다. ONTAP 9.13.1 이전 버전의 ONTAP 릴리즈나 다른 플랫폼의 ONTAP 9.13.1 이상 버전의 경우, System Manager를 사용하여 IPv4 주소를 사용하여 클러스터를 생성한 다음 클러스터 설정을 완료한 후 주소를 생성해야 "IPv6로 변환합니다"합니다.

System Manager는 ONTAP 9.6 이하 버전에서 IPv6 네트워킹이 필요한 배포를 지원하지 않습니다.

시작하기 전에

- 해당 플랫폼 모델의 설치 및 설정 지침에 따라 새 스토리지 시스템에 케이블을 연결하고 전원을 켜야 합니다.

  를 "AFF and FAS 설명서"참조하십시오.

- "필요한 정보를 수집합니다" 을 눌러 클러스터 설정을 완료합니다.
- 클러스터 내 통신을 위해 클러스터의 각 노드에서 클러스터 네트워크 인터페이스를 구성해야 합니다.
- CLI를 사용하여 IPv6를 구성하는 경우 SSH를 사용하여 시스템에 액세스할 수 있도록 BMC(기본 관리 컨트롤러)에서 IPv6를 구성해야 합니다.

예 **1.** 단계

시스템 관리자

1. 노드 관리 IP 주소를 할당합니다

   - Windows 컴퓨터
     i. Windows 컴퓨터를 컨트롤러와 동일한 서브넷에 연결합니다.

        이렇게 하면 노드 관리 IP 주소가 시스템에 자동으로 할당됩니다.

     ii. 네트워크 * 드라이브를 열어 노드를 검색합니다.
     iii. 노드를 선택하여 클러스터 설정 마법사를 시작합니다.
   - Windows 이외의 컴퓨터
     i. 클러스터에 추가할 모든 노드의 전원을 켭니다.

        이는 클러스터 설정을 검색할 수 있도록 하는 데 필요합니다.

     ii. 첫 번째 노드의 콘솔에 연결합니다.

        노드가 부팅된 다음 콘솔에서 클러스터 설정 마법사가 시작됩니다.

```
Welcome to the cluster setup wizard....
```

   i. AutoSupport 설명을 확인합니다.

```
Type yes to confirm and continue {yes}: yes
```

      AutoSupport는 기본적으로 사용하도록 설정되어 있습니다.

   ii. 화면의 지침에 따라 노드에 관리 IP 주소를 할당합니다.
   iii. 웹 브라우저에서 구성한 노드 관리 IP 주소를 입력합니다"https://node-management-IP".

      System Manager가 클러스터의 나머지 노드를 자동으로 검색합니다.

2. Initialize storage system * 에 클러스터 이름과 admin 암호를 입력합니다.
3. 네트워킹 * 에 클러스터 관리 IP 주소, 서브넷 마스크 및 게이트웨이를 입력합니다.
4. 도메인 이름 서비스를 사용하여 호스트 이름을 확인하려면 * DNS(도메인 이름 서비스) 사용 * 을 선택한 다음 DNS 서버 정보를 입력합니다.
5. 클러스터 전체에서 시간을 동기화하기 위해 NTP(네트워크 시간 프로토콜)를 사용하려면 * 기타 * 에서 * 시간 서비스 사용(NTP) * 을 선택하고 NTP 서버 정보를 입력합니다.
6. 제출 * 을 선택합니다.

ONTAP CLI를 참조하십시오

1. 클러스터에 추가할 모든 노드의 전원을 켭니다.

   이 작업은 클러스터 설정을 검색하는 데 필요합니다.

2. 첫 번째 노드의 콘솔에 연결합니다.

   노드가 부팅된 다음 콘솔에서 클러스터 설정 마법사가 시작됩니다.

   ```
   Welcome to the cluster setup wizard....
   ```

3. AutoSupport 설명을 확인합니다.

   ```
   Type yes to confirm and continue {yes}: yes
   ```

   AutoSupport는 기본적으로 사용하도록 설정되어 있습니다.

4. 화면의 지침에 따라 노드에 관리 IP 주소를 할당합니다.

   ONTAP 9.13.1부터 A800 및 FAS8700 플랫폼에서 관리 LIF에 IPv6 주소를 할당할 수 있습니다. ONTAP 9.13.1 이전 릴리즈 또는 다른 플랫폼에서 9.13.1 이상인 경우 관리 LIF에 IPv4 주소를 할당한 다음 클러스터 설정을 완료한 후 IPv6로 변환해야 합니다.

5. 계속하려면 * Enter * 를 누르십시오.

   ```
   Do you want to create a new cluster or join an existing cluster?
   {create, join}:
   ```

6. 새 클러스터 생성:

   a. 를 입력합니다 `create`

   b. 시스템 기본값을 그대로 사용하거나 값을 직접 입력합니다.

   c. 설정이 완료된 후 클러스터에 로그인하여 클러스터가 활성 상태이고 첫 번째 노드가 정상 상태인지 확인합니다. `cluster show`

      다음 예에서는 첫 번째 노드(cluster1-01)가 정상이고 참여할 자격이 있는 클러스터를 보여 줍니다.

   ```
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   cluster1-01           true    true
   ```

   +
   필요한 경우, 명령을 사용하여 클러스터 설정 마법사에 액세스하고 admin 또는 노드 SVM에 대해 입력한 값을 변경할 수 있습니다 `cluster setup`.

7. 클러스터에 노드 연결:

   한 번에 하나의 노드를 클러스터에 결합할 수 있습니다. 각 노드에 대해 결합 작업을 완료해야 하며, 다음 노드에 대한 연결을 시작하려면 노드가 클러스터의 일부여야 합니다.

   NL-SAS 드라이브가 24개 이하인 FAS2720를 사용하는 경우 스토리지 구성 기본값이 액티브/패시브로 설정되어 있는지 확인하여 성능을 최적화해야 합니다. 자세한 내용은 의 설명서를 "루트 데이터 파티셔닝을 사용하여 노드에 대한 액티브-패시브 구성을 설정합니다"참조하십시오.

   a. 클러스터에 참여하려는 노드에 로그인합니다.

      콘솔에서 클러스터 설정 마법사가 시작됩니다.

      ```
      Welcome to the cluster setup wizard....
      ```

   b. AutoSupport 설명을 확인합니다.

      AutoSupport는 기본적으로 사용하도록 설정되어 있습니다.

      ```
      Type yes to confirm and continue {yes}: yes
      ```

   c. 화면의 지침에 따라 노드에 IP 주소를 할당합니다.

      ONTAP 9.13.1부터 A800 및 FAS8700 플랫폼에서 관리 LIF에 IPv6 주소를 할당할 수 있습니다. ONTAP 9.13.1 이전 릴리즈 또는 다른 플랫폼에서 9.13.1 이상인 경우 관리 LIF에 IPv4 주소를 할당한 다음 클러스터 설정을 완료한 후 IPv6로 변환해야 합니다.

   d. 계속하려면 * Enter * 를 누르십시오.

      ```
      Do you want to create a new cluster or join an existing cluster?
      {create, join}:
      ```

   e. 를 입력합니다 `join`

   f. 화면의 지침에 따라 노드를 설정하고 클러스터에 연결합니다.

   g. 설정이 완료되면 노드가 정상 상태이며 클러스터에 참여할 수 있는지 확인합니다. `cluster show`

      다음 예에서는 두 번째 노드(cluster1-02)가 클러스터에 결합된 후의 클러스터를 보여 줍니다.

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-01           true    true
cluster1-02           true    true
```

8. 7단계를 반복하여 나머지 노드를 모두 연결합니다.

다음 단계

- 필요한 경우 "IPv4에서 IPv6로 변환".
- "Active IQ Config Advisor를 실행하여 구성을 검증하고 일반적인 구성 오류를 확인합니다"..

선택적으로 **ONTAP** 관리 **LIF**를 **IPv4**에서 **IPv6**로 변환합니다

ONTAP 9.13.1부터 초기 클러스터 설정 중에 ONTAP CLI(Command Line Interface)를 사용하여 IPv6 주소를 AFF A800 및 FAS 8700 플랫폼의 관리 LIF에 할당할 수 있습니다. ONTAP 9.13.1 이전 릴리즈 또는 다른 플랫폼에서 9.13.1 이상인 경우, 먼저 관리 LIF에 IPv4 주소를 할당한 다음 클러스터 설정을 완료한 후 IPv6 주소로 변환해야 합니다.

자동으로 할당된 IP 주소와 DHCP를 사용하여 하드웨어 설정을 완료하고 Windows 검색을 통해 System Manager를 시작하면 System Manager에서 IPv6 관리 주소를 구성할 수 있습니다.

단계

1. 클러스터에 대해 IPv6 사용:

```
network options ipv6 modify -enable true
```

2. 권한을 고급으로 설정:

```
set priv advanced
```

3. 다양한 인터페이스에서 학습한 RA 접두사 목록을 봅니다.

```
network ndp prefix show
```

4. IPv6 관리 LIF 생성:

   형식을 사용합니다 `prefix::id` IPv6 주소를 수동으로 구성할 address 매개 변수에 있습니다.

```
network interface create -vserver <svm_name> -lif <LIF> -home-node
<home_node> -home-port <home_port> -address <IPv6prefix::id> -netmask
-length <netmask_length> -failover-policy <policy> -service-policy
<service_policy> -auto-revert true
```

5. LIF가 생성되었는지 확인합니다.

```
network interface show
```

6. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

```
network ping6
```

7. IPv4 LIF를 관리 목적으로 사용 중지됨으로 표시합니다.

```
network interface modify -vserver <svm_name> -lif <lif_name> -status
-admin down
```

8. IPv4 관리 LIF를 삭제합니다.

```
network interface delete -vserver <svm_name> -lif <lif_name>
```

9. IPv4 관리 LIF가 삭제되었는지 확인합니다.

```
network interface show
```

관련 정보

- "네트워크 인터페이스"
- "네트워크 NDP 접두사가 표시됩니다"
- "네트워크 옵션 IPv6 수정"

Digital Advisor Config Advisor로 ONTAP 클러스터를 확인하십시오

모든 노드를 새 클러스터에 결합했으면 Active IQ Config Advisor를 실행하여 구성을 검증하고 일반적인 구성 오류를 확인해야 합니다.

Config Advisor는 랩톱, 가상 컴퓨터 또는 서버에 설치하는 웹 기반 응용 프로그램이며 Windows, Linux 및 Mac 플랫폼에서 작동합니다.

Config Advisor은 일련의 명령을 실행하여 설치를 검증하고 클러스터 및 스토리지 스위치를 포함한 구성의 전체 상태를 확인합니다.

1. Active IQ Config Advisor를 다운로드하고 설치합니다.

   "Active IQ Config Advisor"

2. Digital Advisor를 실행하고 메시지가 표시되면 암호를 설정합니다.
3. 설정을 검토하고 * 저장 * 을 클릭합니다.

4. Objectives * 페이지에서 * ONTAP 배포 후 검증 * 을 클릭합니다.
5. 안내 모드 또는 전문가 모드를 선택합니다.

   안내 모드를 선택하면 연결된 스위치가 자동으로 검색됩니다.

6. 클러스터 자격 증명을 입력합니다.
7. (선택 사항) * 양식 유효성 검사 * 를 클릭합니다.
8. 데이터 수집을 시작하려면 * 저장 및 평가 * 를 클릭합니다.
9. 데이터 수집이 완료되면 * Job Monitor > Actions * 에서 * Data View * 아이콘을 클릭하여 수집된 데이터를 보고 * Results * 아이콘을 클릭하여 결과를 확인합니다.
10. Config Advisor에서 식별한 문제를 해결합니다.

ONTAP 클러스터 전체에서 시스템 시간을 동기화합니다

시간을 동기화하면 클러스터의 모든 노드가 동일한 시간을 가지고 CIFS 및 Kerberos 장애를 방지할 수 있습니다.

사이트에서 NTP(Network Time Protocol) 서버를 설정해야 합니다. ONTAP 9.5부터 대칭 인증을 사용하여 NTP 서버를 설정할 수 있습니다. 자세한 내용은 의 설명서를 "클러스터 시간 관리(클러스터 관리자만 해당)"참조하십시오.

클러스터를 하나 이상의 NTP 서버와 연결하여 클러스터 전체에서 시간을 동기화할 수 있습니다.

1. 각 노드에 대해 시스템 시간과 시간대가 올바르게 설정되었는지 확인합니다.

   ```
   cluster date show
   ```

   클러스터의 모든 노드는 동일한 시간대로 설정되어야 합니다.

   이 예는 클러스터의 각 노드에 대한 날짜 및 시간대를 보여줍니다.

   ```
   cluster1::> cluster date show
   Node         Date                Time zone
   ------------ ------------------- -----------------
   cluster1-01  01/06/2015 09:35:15 America/New_York
   cluster1-02  01/06/2015 09:35:15 America/New_York
   cluster1-03  01/06/2015 09:35:15 America/New_York
   cluster1-04  01/06/2015 09:35:15 America/New_York
   4 entries were displayed.
   ```

2. 모든 노드의 날짜 또는 시간대를 변경합니다.

   ```
   cluster date modify
   ```

이 예에서는 클러스터의 시간대를 GMT로 변경합니다.

```
cluster1::> cluster date modify -timezone GMT
```

3. 클러스터를 NTP 서버에 연결합니다.

   대칭 인증 없이 NTP 서버를 설정하려면 다음 명령을 입력합니다.

   ```
   cluster time-service ntp server create -server <server_name>
   ```

   대칭 인증을 사용하여 NTP 서버를 설정하려면 다음 명령을 입력합니다.

   ```
   cluster time-service ntp server create -server <server_ip_address> -key
   -id <key_id>
   ```

   ⓘ 대칭 인증은 ONTAP 9.5부터 사용할 수 있습니다. ONTAP 9.4 이하에서는 사용할 수 없습니다.

   이 예에서는 클러스터에 DNS가 구성되어 있다고 가정합니다. DNS를 구성하지 않은 경우 NTP 서버의 IP 주소를 지정해야 합니다.

   ```
   cluster1::> cluster time-service ntp server create -server
   ntp1.example.com
   ```

4. 클러스터가 NTP 서버와 연결되어 있는지 확인합니다.

   ```
   cluster time-service ntp server show
   ```

   이 예에서는 클러스터가 NTP 서버 ntp1.example.com 에 연결되어 있음을 보여 줍니다.

   ```
   cluster1::> cluster time-service ntp server show
   Server               Version
   -------------------- -----------
   ntp1.example.com     auto
   ```

NTP 서버에서 대칭 인증을 관리하는 명령입니다

ONTAP 9.5부터 NTP(네트워크 시간 프로토콜) 버전 3이 지원됩니다. NTPv3에는 SHA-1 키를 사용한 대칭 인증이 포함되어 있어 네트워크 보안을 강화합니다.

수행할 작업...	이 명령 사용...
대칭 인증 없이 NTP 서버를 구성합니다	`cluster time-service ntp server create -server server_name`
대칭 인증을 사용하여 NTP 서버를 구성합니다	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
기존 NTP 서버에 대해 대칭 인증을 설정합니다 필요한 키 ID를 추가하여 인증을 사용하도록 기존 NTP 서버를 수정할 수 있습니다	`cluster time-service ntp server modify -server server_name -key-id key_id`
공유 NTP 키를 구성합니다	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` • 참고: * 공유 키는 ID로 참조됩니다. ID, 유형 및 값은 노드와 NTP 서버 모두에서 동일해야 합니다
알 수 없는 키 ID로 NTP 서버를 구성합니다	`cluster time-service ntp server create -server server_name -key-id key_id`
NTP 서버에 키 ID가 구성되지 않은 서버를 구성합니다.	`cluster time-service ntp server create -server server_name -key-id key_id` • 참고: * 키 ID, 유형 및 값은 NTP 서버에 구성된 키 ID, 유형 및 값과 동일해야 합니다.
대칭 인증을 사용하지 않도록 설정합니다	`cluster time-service ntp server modify -server server_name -authentication disabled`

관련 정보

- "시스템 관리"
- "클러스터 시간 - 서비스 NTP"

ONTAP 소프트웨어 및 펌웨어를 업그레이드하고 되돌립니다

ONTAP를 업그레이드합니다

ONTAP 업그레이드에 대해 알아봅니다

ONTAP 소프트웨어를 업그레이드할 때 새롭고 개선된 ONTAP 기능을 활용하여 비용 절감, 중요한 워크로드 가속화, 보안 향상, 조직에 제공되는 데이터 보호 범위 확장에 도움이 됩니다.

주요 ONTAP 업그레이드는 ONTAP 번호가 낮은 릴리즈에서 상위 릴리즈로 이전하는 작업으로 구성됩니다. 예를 들어 ONTAP 9.8에서 ONTAP 9.12.1로 클러스터를 업그레이드할 수 있습니다. 부(또는 패치) 업그레이드는 동일한 번호가 지정된 릴리스 내에서 낮은 ONTAP 버전에서 상위 ONTAP 버전으로 이동하는 것으로 구성됩니다. 예를 들어, ONTAP 9.12.1P1에서 9.12.1P4로 클러스터를 업그레이드할 수 있습니다.

시작하려면 업그레이드를 준비해야 합니다. Active IQ Digital Advisor(디지털 어드바이저)에 대해 유효한 SupportEdge 계약을 보유한 경우 해야 "Upgrade Advisor로 업그레이드 준비"합니다. Upgrade Advisor는 클러스터를 평가하고 구성에 맞는 업그레이드 계획을 생성하여 불확실성과 위험을 최소화하는 데 도움이 되는 인텔리전스를 제공합니다. Active IQ 디지털 어드바이저에 대해 유효한 SupportEdge 계약이 없는 경우, 해야 "Upgrade Advisor 없이 업그레이드 준비"합니다.

업그레이드를 준비하고 나면 을 사용하여 업그레이드를 수행하는 것이 좋습니다"System Manager에서 자동 무중단 업그레이드(ANDU". ANDU는 ONTAP의 고가용성(HA) 장애 조치 기술을 활용하여 클러스터에서 업그레이드 중에 중단 없이 데이터를 계속 제공할 수 있도록 합니다.

> ONTAP 9.12.1부터 System Manager가 NetApp Console과 완벽하게 통합되었습니다. 시스템에 콘솔이 구성된 경우 시스템 페이지를 통해 업그레이드할 수 있습니다.

ONTAP 소프트웨어 업그레이드에 도움이 필요한 경우 NetApp 프로페셔널 서비스는 을 제공합니다 "관리형 업그레이드 서비스". 이 서비스를 사용하는 데 관심이 있는 경우 NetApp 세일즈 담당자 또는 에게 문의하십시오 "NetApp의 영업 문의 양식 제출". Managed Upgrade Service 및 기타 유형의 업그레이드 지원은 를 사용하는 고객에게 제공됩니다 "SupportEdge Expert 서비스" 추가 비용 없음.

관련 정보

- "지원되는 업그레이드 경로"

언제 ONTAP를 업그레이드해야 합니까?

정기적으로 ONTAP 소프트웨어를 업그레이드해야 합니다. ONTAP를 업그레이드하면 새로운 기능과 향상된 기능을 활용하고 알려진 문제에 대한 현재 수정 사항을 구현할 수 있습니다.

주요 ONTAP 업그레이드

주요 ONTAP 업그레이드 또는 기능 릴리즈에는 일반적으로 다음이 포함됩니다.

- 새로운 ONTAP 기능
- NetApp WAFL 작업 또는 RAID 작업의 기본 변경 사항 등 주요 인프라 변경 사항

- NetApp의 새로운 하드웨어 시스템 지원
- 최신 네트워크 인터페이스 카드 또는 호스트 버스 어댑터와 같은 하드웨어 구성 요소 교체 지원

새로운 ONTAP 릴리즈는 3년간 완벽한 지원을 받을 수 있습니다. NetApp은 GA(General Availability) 이후 1년간 최신 릴리즈를 실행한 다음, 전체 지원 기간 내의 남은 시간을 사용하여 최신 ONTAP 릴리즈로의 전환을 계획하는 것을 권장합니다.

ONTAP 패치 업그레이드

패치 업그레이드를 통해 다음 주요 ONTAP 기능 릴리스를 기다릴 수 없는 중요한 버그에 대한 수정 사항을 적시에 제공할 수 있습니다. 중요하지 않은 패치 업그레이드는 3-6개월마다 적용해야 합니다. 중요한 패치 업그레이드는 가능한 한 빨리 적용해야 합니다.

에 대해 자세히 알아보십시오 "최소 권장 패치 수준" ONTAP 릴리스의 경우.

ONTAP 릴리즈 날짜

ONTAP 9.8 릴리스부터 NetApp는 매년 두 번 ONTAP 릴리스를 제공합니다. 이 계획은 변경될 수 있지만 매년 2/4분기에 새로운 ONTAP 릴리즈를 제공하려는 것입니다. 최신 ONTAP 릴리즈를 활용할 수 있도록 업그레이드 기간을 계획하려면 이 정보를 사용하십시오.

버전	출시일
9.18.1	2025년 11월
9.17.1	2025년 9월
9.16.1	2025년 1월
9.15.1	2024년 7월
9.14.1	2024년 1월
9.13.1	2023년 6월
9.12.1	2023년 2월
9.11.1	2022년 7월
9.10.1	2022년 1월
9.9.1	2021년 6월

ONTAP 지원 레벨

특정 버전의 ONTAP에 사용할 수 있는 지원 수준은 소프트웨어가 출시된 시기에 따라 다릅니다.

지원 레벨	완벽한 지원			제한된 지원		셀프서비스 지원		
년	1	2	3	4	5	6	7	8
온라인 설명서 액세스	예	예	예	예	예	예	예	예
기술 지원	예	예	예	예	예			
근본 원인 분석	예	예	예	예	예			
소프트웨어 다운로드	예	예	예	예	예			
서비스 업데이트(패치 릴리스 [P-releases])	예	예	예					
취약점에 대한 경고	예	예	예					

관련 정보

- 학습 "현재 지원되는 ONTAP 릴리스의 새로운 기능".
- 에 대해 자세히 알아보십시오 "최소 권장 ONTAP 릴리스".
- 에 대해 자세히 알아보십시오 "ONTAP 소프트웨어 버전 지원".
- 에 대해 자세히 알아보십시오 "ONTAP 릴리스 모델".

계획된 업그레이드 전에 **ONTAP** 자동 업그레이드 사전 검사를 실행합니다

ONTAP 자동 업그레이드 사전 검사를 실행하기 위해 ONTAP 소프트웨어를 업그레이드하는 과정에 있을 필요가 없습니다. ONTAP의 자동화된 업그레이드 프로세스와 별도로 업그레이드 전 검사를 실행하면 클러스터에 대해 수행되는 검사를 확인하고 실제 업그레이드를 시작하기 전에 수정해야 하는 오류 또는 경고 목록을 확인할 수 있습니다. 예를 들어, 2주 후에 발생하도록 예정된 유지보수 기간 중에 ONTAP 소프트웨어를 업그레이드할 것으로 예상된다고 가정합니다. 예약된 날짜를 기다리는 동안 자동화된 업그레이드 사전 점검을 실행하고 유지보수 윈도우에 앞서 필요한 수정 조치를 취할 수 있습니다. 이렇게 하면 업그레이드를 시작한 후 예기치 않은 구성 오류의 위험이 줄어듭니다.

ONTAP 소프트웨어 업그레이드를 시작할 준비가 되었으면 이 절차를 수행할 필요가 없습니다. 를 따라야 합니다 "업그레이드 프로세스가 자동화되었습니다"에는 자동화된 업그레이드 사전 점검 실행이 포함됩니다.

MetroCluster 구성의 경우 먼저 클러스터 A에서 이러한 단계를 실행한 다음 클러스터 B에서 동일한 단계를 실행해야 합니다

시작하기 전에

당신은 해야 한다 "대상 ONTAP 소프트웨어 이미지를 다운로드합니다".

에 대한 자동 업그레이드 사전 검사를 실행하려면 "직접 멀티 홉 업그레이드"대상 ONTAP 버전에 대한 소프트웨어

패키지만 다운로드하면 됩니다. 실제 업그레이드를 시작하기 전에는 중간 ONTAP 버전을 로드할 필요가 없습니다. 예를 들어 9.7에서 9.11.1로 업그레이드하는 자동 업그레이드 사전 검사를 실행하는 경우 ONTAP 9.11.1용 소프트웨어 패키지를 다운로드해야 합니다. ONTAP 9.8.1용 소프트웨어 패키지는 다운로드할 필요가 없습니다.

예 **2.** 단계

시스템 관리자

1. ONTAP 대상 이미지를 검증합니다.

   MetroCluster 구성을 업그레이드하는 경우 클러스터 A를 검증한 다음 클러스터 B에서 검증 프로세스를 반복해야 합니다

   a. 실행 중인 ONTAP 버전에 따라 다음 단계 중 하나를 수행합니다.

실행 중인 경우…	수행할 작업…
ONTAP 9.8 이상	클러스터 > 개요 * 를 클릭합니다.
ONTAP 9.5, 9.6 및 9.7	구성 * > * 클러스터 * > * 업데이트 * 를 클릭합니다.
ONTAP 9.4 이하	구성 * > * 클러스터 업데이트 * 를 클릭합니다.

   b. 개요 * 창의 오른쪽 모서리에서 를 클릭합니다 ⋮.

   c. ONTAP 업데이트 * 를 클릭합니다.

   d. 클러스터 업데이트 * 탭에서 새 이미지를 추가하거나 사용 가능한 이미지를 선택합니다.

원하는 작업	그러면…
로컬 폴더에서 새로운 소프트웨어 이미지를 추가합니다. 이미 있어야 합니다 "이미지를 다운로드했습니다" 로컬 클라이언트로.	i. Available Software Images * 아래에서 * Add from Local * 을 클릭합니다. ii. 소프트웨어 이미지를 저장한 위치로 이동하여 이미지를 선택한 다음 * 열기 * 를 클릭합니다.
HTTP 또는 FTP 서버에서 새 소프트웨어 이미지를 추가합니다	i. 서버에서 추가 * 를 클릭합니다. ii. 새 소프트웨어 이미지 추가 * 대화 상자에서 NetApp Support 사이트에서 ONTAP 소프트웨어 이미지를 다운로드한 HTTP 또는 FTP 서버의 URL을 입력합니다. 익명 FTP의 경우 에서 URL을 지정해야 합니다 ftp://anonymous@ftpserver 형식. iii. 추가 * 를 클릭합니다.
사용 가능한 이미지를 선택합니다	나열된 이미지 중 하나를 선택합니다.

   e. 업그레이드 전 확인 검사를 실행하려면 * Validate * 를 클릭합니다.

   유효성 검사 중에 오류 또는 경고가 발견되면 시정 조치 목록과 함께 표시됩니다. 업그레이드를 진행하기

전에 모든 오류를 해결해야 합니다. 경고도 해결하는 것이 가장 좋습니다.

CLI를 참조하십시오

1. 타겟 ONTAP 소프트웨어 이미지를 클러스터 패키지 저장소에 로드합니다.

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.15.1/image.tgz

Package download completed.
Package processing completed.
```

2. 소프트웨어 패키지를 클러스터 패키지 리포지토리에서 사용할 수 있는지 확인합니다.

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.15.1              MM/DD/YYYY 10:32:15
```

3. 자동화된 업그레이드 사전 검사 실행:

```
cluster image validate -version <package_version_number> -show
-validation-details true
```

```
cluster1::> cluster image validate -version 9.15.1 -show-validation
-details true

It can take several minutes to complete validation...
Validation checks started successfully.  Run the "cluster image
show-update-progress" command to check validation status.
```

4. 검증 상태 확인:

```
cluster image show-update-progress
```

Status * 가 "In-progress"인 경우, 잠시 기다렸다가 명령이 완료될 때까지 명령을 다시 실행하십시오.

```
cluster1::*> cluster image show-update-progress

Update Phase         Status                    Duration
Duration
-------------------- ----------------- ---------------
---------------
Pre-update checks    completed                 00:10:00
00:01:03

Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
---------------------------------------
AMPQ Router and      OK                N/A
Broker Config
Cleanup
Aggregate online     OK                N/A
status and parity
check
Aggregate plex       OK                N/A
resync status check
Application          OK                N/A
Provisioning Cleanup
Autoboot Bootargs    OK                N/A
Status
Backend              OK                N/A
...
Volume Conversion    OK                N/A
In Progress Check
Volume move          OK                N/A
progress status
check
Volume online        OK                N/A
status check
iSCSI target portal  OK                N/A
groups status check
Overall Status       Warning           Warning
75 entries were displayed.
```

업그레이드 프로세스를 시작하기 전에 해결해야 할 오류나 경고와 함께 전체 자동 업그레이드 사전 검사 목록이 표시됩니다.

예제 출력

업그레이드 사전 검사의 전체 출력 예

```
cluster1::*> cluster image validate -version 9.14.1 -show-validation
-details true
It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed successfully.
Refer to the Upgrade Advisor Plan or the "What should I verify before I
upgrade with or without Upgrade Advisor" section in the "Upgrade ONTAP"
documentation for the remaining manual validation checks that need to
be performed before update.
Upgrade ONTAP documentation available at: https://docs.netapp.com/us-
en/ontap/upgrade/index.html
The list of checks are available at: https://docs.netapp.com/us-
en/ontap/upgrade/task_what_to_check_before_upgrade.html
Failing to do so can result in an update failure or an I/O disruption.
Use the Interoperability Matrix Tool (IMT
http://mysupport.netapp.com/matrix) to verify host system
supportability configuration information.

Validation checks started successfully.  Run the "cluster image show-
update-progress" command to check validation status.


fas2820-2n-wic-1::*> cluster image show-update-progress

                                          Estimated         Elapsed
Update Phase         Status                Duration        Duration
-------------------- ----------------- --------------- ---------------
Pre-update checks    in-progress            00:10:00        00:00:42

Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
--------------------------------------

fas2820-2n-wic-1::*> cluster image show-update-progress

                                          Estimated         Elapsed
Update Phase         Status                Duration        Duration
-------------------- ----------------- --------------- ---------------
Pre-update checks    completed              00:10:00        00:01:03
```

```
Details:

Pre-update Check     Status            Error-Action
-------------------- ----------------
--------------------------------------
AMPQ Router and      OK                N/A
Broker Config
Cleanup
Aggregate online     OK                N/A
status and parity
check
Aggregate plex       OK                N/A
resync status check
Application          OK                N/A
Provisioning Cleanup
Autoboot Bootargs    OK                N/A
Status
Backend              OK                N/A
Configuration Status
Boot Menu Status     Warning           Warning: bootarg.init.bootmenu
is
                                       enabled on nodes: fas2820-wic-
1a,
                                       fas2820-wic-1b. The boot process
of
                                       the nodes will be delayed.
                                       Action: Set the
bootarg.init.bootmenu
                                       bootarg to false before
proceeding
                                       with the upgrade.
Broadcast Domain     OK                N/A
availability and
uniqueness for HA
pair status
CIFS compatibility   OK                N/A
status check
CLAM quorum online   OK                N/A
status check
CPU Utilization      OK                N/A
Status
Capacity licenses    OK                N/A
install status check
Check For SP/BMC     OK                N/A
Connectivity To
Nodes
```

```
Check LDAP fastbind  OK              N/A
users using
unsecure connection.
Check for unsecure   OK              N/A
kex algorithm
configurations.
Check for unsecure   OK              N/A
mac configurations.
Cloud keymanager     OK              N/A
connectivity check
Cluster health and   OK              N/A
eligibility status
Cluster quorum       OK              N/A
status check
Cluster/management   OK              N/A
switch check
Compatible New       OK              N/A
Image Check
Current system       OK              N/A
version check if it
is susceptible to
possible outage
during NDU
Data ONTAP Version   OK              N/A
and Previous
Upgrade Status
Data aggregates HA   OK              N/A
policy check
Disk status check    OK              N/A
for failed, broken
or non-compatibility
Duplicate Initiator  OK              N/A
Check
Encryption key       OK              N/A
migration status
check
External             OK              N/A
key-manager with
legacy KMIP client
check
External keymanager  OK              N/A
key server status
check
Fabricpool Object    OK              N/A
Store Availability
High Availability    OK              N/A
```

```
configuration
status check
Infinite Volume      OK                N/A
availibility check
LIF failover         OK                N/A
capability status
check
LIF health check     OK                N/A
LIF load balancing   OK                N/A
status check
LIFs is on home      OK                N/A
node status
Logically over       OK                N/A
allocated DP
volumes check
MetroCluster         OK                N/A
configuration
status check for
compatibility
Minimum number of    OK                N/A
aggregate disks
check
NAE Aggregate and    OK                N/A
NVE Volume
Encryption Check
NDMP sessions check  OK                N/A
NFS mounts status    Warning           Warning: This cluster is serving
NFS
check                                  clients. If NFS soft mounts are
used,
                                       there is a possibility of
frequent
                                       NFS timeouts and race conditions
that
                                       can lead to data corruption
during
                                       the upgrade.
                                       Action: Use NFS hard mounts, if
                                       possible. To list Vservers
running
                                       NFS, run the following command:
                                       vserver nfs show
Name Service         OK                N/A
Configuration DNS
Check
Name Service         OK                N/A
```

```
Configuration LDAP
Check
Node to SP/BMC       OK                N/A
connectivity check
OKM/KMIP enabled     OK                N/A
systems - Missing
keys check
ONTAP API to REST    Warning           Warning: NetApp ONTAP API has
been
transition warning                     used on this cluster for ONTAP
data
                                       storage management within the
last 30
                                       days. NetApp ONTAP API is
approaching
                                       end of availability.
                                       Action: Transition your
automation
                                       tools from ONTAP API to ONTAP
REST
                                       API. For more details, refer to
                                       CPC-00410 - End of availability:
                                       ONTAPI

https://mysupport.netapp.com/info/
                                       communications/ECMLP2880232.html
ONTAP Image          OK                N/A
Capability Status
OpenSSL 3.0.x        OK                N/A
upgrade validation
check
Openssh 7.2 upgrade  OK                N/A
validation check
Platform Health      OK                N/A
Monitor check
Pre-Update           OK                N/A
Configuration
Verification
RDB Replica Health   OK                N/A
Check
Replicated database  OK                N/A
schema consistency
check
Running Jobs Status  OK                N/A
SAN LIF association  OK                N/A
status check
```

```
SAN compatibility    OK                N/A
for manual
configurability
check
SAN kernel agent     OK                N/A
status check
Secure Purge         OK                N/A
operation Check
Shelves and Sensors  OK                N/A
check
SnapLock Version     OK                N/A
Check
SnapMirror           OK                N/A
Synchronous
relationship status
check
SnapMirror           OK                N/A
compatibility
status check
Supported platform   OK                N/A
check
Target ONTAP         OK                N/A
release support for
FiberBridge 6500N
check
Upgrade Version      OK                N/A
Compatibility Status
Verify all bgp       OK                N/A
peer-groups are in
the up state
Verify if a cluster  OK                N/A
management LIF
exists
Verify that e0M is   OK                N/A
home to no LIFs
with high speed
services.
Volume Conversion    OK                N/A
In Progress Check
Volume move          OK                N/A
progress status
check
Volume online        OK                N/A
status check
iSCSI target portal  OK                N/A
groups status check
```

```
Overall Status       Warning           Warning
75 entries were displayed.
```

ONTAP 업그레이드를 준비합니다

ONTAP 업그레이드에 걸리는 시간을 결정합니다

ONTAP 업그레이드 준비 단계를 완료하는 데 30분 이상, 각 HA 쌍 업그레이드에 60분, 업그레이드 후 단계를 완료하는 데 30분 이상 계획을 세워야 합니다.

> 외부 키 관리 서버 및 KMIP(Key Management Interoperability Protocol)와 함께 NetApp Encryption을 사용하는 경우 각 HA 쌍의 업그레이드가 1시간 이상 길 것으로 예상해야 합니다.

이러한 업그레이드 기간 지침은 일반 구성 및 워크로드를 기반으로 합니다. 이러한 지침을 사용하여 무중단 업그레이드를 수행하는 데 걸리는 시간을 추정할 수 있습니다. 실제 업그레이드 프로세스 기간은 개별 환경과 노드 수에 따라 다릅니다.

Upgrade Advisor로 ONTAP 업그레이드 준비

에 대한 활성 계약이 있는 경우 "SupportEdge 서비스""디지털 자문업체"Upgrade Advisor를 사용하여 업그레이드 계획을 생성하는 것이 좋습니다.

Digital Advisor의 Upgrade Advisor 서비스는 업그레이드를 계획하고 불확실성과 위험을 최소화할 수 있는 인텔리전스를 제공합니다.

Digital Advisor는 최신 버전의 ONTAP로 업그레이드하여 해결할 수 있는 환경 문제를 식별합니다. 업그레이드 관리자 서비스는 성공적인 업그레이드를 계획하는 데 도움이 되며, 업그레이드하는 ONTAP 버전에서 알아야 할 문제에 대한 보고서를 제공합니다.

> Upgrade Advisor에서 보고서를 생성하려면 AutoSupport 로그가 필요합니다. AutoSupport를 사용하도록 설정한 경우 업그레이드 관리자는 로그에 액세스할 수 있으며 보고서를 성공적으로 만들 수 있습니다. AutoSupport를 활성화하지 않은 경우 수행할 수 "AutoSupport 파일을 수동으로 업로드합니다"있습니다.

Digital Advisor에 대해 유효한 Support Edge Services 계약이 없는 경우, 해야 "Upgrade Advisor 없이 업그레이드를 준비합니다"합니다.

단계

1. "Active IQ Digital Advisor를 시작합니다"
2. 디지털 자문"클러스터와 관련된 모든 위험을 확인하고 수동으로 수정 조치를 취할 수 있습니다".

   ONTAP 업그레이드를 수행하기 전에 * 소프트웨어 구성 변경 *, * 하드웨어 구성 변경 * 및 * 하드웨어 교체 * 범주에 포함된 위험을 해결해야 합니다.

3. 권장 업그레이드 경로 및 를 검토합니다 "업그레이드 계획을 생성합니다".

다음 단계

- 를 검토해야 합니다 "ONTAP 릴리즈 노트" Upgrade Advisor가 클러스터에 권장하는 타겟 ONTAP 릴리즈의 경우 Upgrade Advisor에서 생성한 계획에 따라 클러스터를 업그레이드해야 합니다.
- 당신은 해야 한다 "SP 또는 BMC를 재부팅합니다" 업그레이드 시작 전.

Upgrade Advisor 없이 업그레이드 준비

Upgrade Advisor 없이 ONTAP 소프트웨어 업그레이드 준비

ONTAP 소프트웨어 업그레이드를 올바르게 준비하면 업그레이드 프로세스를 시작하기 전에 잠재적 업그레이드 위험 또는 방해 요인을 식별하고 완화할 수 있습니다. 업그레이드 준비 중에 업그레이드하기 전에 고려해야 할 특별한 사항을 확인할 수도 있습니다. 예를 들어 클러스터에서 SSL FIPS 모드가 활성화되어 있고 관리자 계정이 인증을 위해 SSH 공개 키를 사용하는 경우 대상 ONTAP 릴리즈에서 호스트 키 알고리즘이 지원되는지 확인해야 합니다.

에 대해 활성 SupportEdge 계약이 있는 "디지털 자문업체" "Upgrade Advisor로 업그레이드를 계획하십시오"경우. Active IQ 디지털 어드바이저(디지털 어드바이저)에 액세스할 수 없는 경우 다음을 수행하여 ONTAP 업그레이드를 준비해야 합니다.

1. "대상 ONTAP 릴리스를 선택합니다".
2. 대상 릴리스에 대한 의 _업그레이드 주의_및_알려진 문제 및 제한 사항_섹션을 검토하십시오"ONTAP 9 릴리즈 노트".

   업그레이드 주의 사항 업그레이드하기 전에 알아야 할 잠재적인 문제에 대해 설명합니다. 알려진 문제 및 제한 사항 업그레이드 후 발생할 수 있는 예기치 않은 시스템 동작을 설명합니다.

   릴리스 정보에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

3. "하드웨어 구성에 대한 ONTAP 지원을 확인합니다".

   하드웨어 플랫폼, 클러스터 관리 스위치, MetroCluster IP 스위치가 타겟 릴리즈를 지원해야 합니다. 클러스터가 SAN용으로 구성된 경우 SAN 구성이 완전히 지원되어야 합니다.

4. "Active IQ Config Advisor를 사용하여 일반적인 구성 오류가 없는지 확인합니다."
5. 지원되는 ONTAP를 검토합니다 "업그레이드 경로" 직접 업그레이드를 수행할 수 있는지 또는 업그레이드를 단계별로 완료해야 하는지 여부를 확인하려면
6. "LIF 페일오버 구성을 확인합니다".

   업그레이드를 수행하기 전에 클러스터의 페일오버 정책과 페일오버 그룹이 올바르게 구성되어 있는지 확인해야 합니다.

7. "SVM 라우팅 구성을 확인합니다".
8. "특별 고려 사항을 확인합니다" 확인할 수 있습니다.

   클러스터에 특정 구성이 있는 경우 ONTAP 소프트웨어 업그레이드를 시작하기 전에 수행해야 할 특정 작업이 있습니다.

9. "SP 또는 BMC를 재부팅합니다".

업그레이드를 위해 **NetApp** 권장 대상 **ONTAP** 버전을 선택합니다

Upgrade Advisor를 사용하여 클러스터에 대한 업그레이드 계획을 생성하면 계획에 업그레이드에 권장되는 타겟 ONTAP 릴리즈가 포함됩니다. Upgrade Advisor에서 제공하는 권장 사항은 현재 구성과 현재 ONTAP 버전에 따라 다릅니다.

업그레이드 관리자를 사용하여 업그레이드를 계획하지 않는 경우 NetApp 권장 사항에 따라 업그레이드를 위한 대상 ONTAP 릴리스를 선택하거나 성능 요구 사항에 맞는 최소 릴리스를 선택해야 합니다.

- 사용 가능한 최신 릴리스로 업그레이드(권장)

  NetApp은 ONTAP 소프트웨어를 최신 버전의 번호가 매겨진 ONTAP 릴리스로 업그레이드할 것을 권장합니다. 클러스터의 스토리지 시스템에서 최신 번호 릴리스를 지원하지 않기 때문에 이 작업을 수행할 수 없는 경우 지원되는 최신 번호 릴리즈로 업그레이드해야 합니다.

- 최소 권장 릴리스

  업그레이드를 클러스터에 대해 권장되는 최소 릴리즈로 제한하려면 을 참조하십시오 "최소 권장 ONTAP 릴리스" 로 업그레이드해야 하는 ONTAP 버전을 확인하려면

사용 중인 하드웨어 구성에 대한 **ONTAP** 대상 릴리스 지원을 확인합니다

ONTAP를 업그레이드하기 전에 하드웨어 구성이 대상 ONTAP 릴리스를 지원할 수 있는지 확인해야 합니다.

모든 설정

를 사용하여 "NetApp Hardware Universe를 참조하십시오" 하드웨어 플랫폼, 클러스터 및 관리 스위치가 대상 ONTAP 릴리즈에서 지원되는지 확인합니다.

업그레이드할 수 있는 ONTAP 버전은 하드웨어 구성에 따라 제한될 수 있습니다. 하드웨어에서 업그레이드할 ONTAP 소프트웨어 버전을 지원하지 않는 경우 먼저 클러스터에 새 노드를 추가하고, 데이터를 마이그레이션하고, 이전 노드를 제거한 다음 ONTAP 소프트웨어를 업그레이드해야 합니다. 의 절차를 "ONTAP 클러스터에 새 노드를 추가합니다 "따릅니다.

클러스터 및 관리 스위치에는 NX-OS(클러스터 네트워크 스위치), 관리 네트워크 스위치(IOS) 및 RCF(참조 구성 파일)가 포함됩니다. 클러스터 및 관리 스위치가 지원되지만 타겟 ONTAP 릴리즈에 필요한 최소 소프트웨어 버전이 실행되고 있지 않은 경우 스위치를 지원되는 소프트웨어 버전으로 업그레이드하십시오.

- "NetApp 다운로드: Broadcom 클러스터 스위치"
- "NetApp 다운로드: Cisco 이더넷 스위치"
- "NetApp 다운로드: NetApp 클러스터 스위치"

스위치를 업그레이드해야 하는 경우 NetApp은 먼저 ONTAP 소프트웨어 업그레이드를 완료한 다음 스위치에 대한 소프트웨어 업그레이드를 수행하는 것이 좋습니다.

MetroCluster 구성

ONTAP를 업그레이드하기 전에 MetroCluster 구성이 있는 경우 를 사용합니다 "NetApp 상호 운용성 매트릭스 툴" MetroCluster IP 스위치가 대상 ONTAP 릴리즈에서 지원되는지 확인

SAN 구성

ONTAP를 업그레이드하기 전에 클러스터가 SAN용으로 구성된 경우 를 사용합니다 "NetApp 상호 운용성 매트릭스 툴" SAN 구성이 완전히 지원되는지 확인합니다.

대상 ONTAP 소프트웨어 버전, 호스트 OS 및 패치, 필요한 호스트 유틸리티 소프트웨어, 다중 경로 소프트웨어, 어댑터 드라이버 및 펌웨어를 비롯한 모든 SAN 구성 요소가 지원되어야 합니다.

Active IQ Config Advisor를 사용하여 **ONTAP**을 업그레이드하기 전에 일반적인 구성 오류를 식별합니다.

ONTAP를 업그레이드하기 전에 Active IQ Config Advisor 도구를 사용하여 일반적인 구성 오류를 확인할 수 있습니다.

Active IQ Config Advisor는 NetApp 시스템용 구성 검증 툴입니다. 보안된 사이트는 물론이고 보안되지 않은 사이트에서도 Config Advisor를 구축하여 데이터를 수집하고 시스템 분석을 수행할 수 있습니다.

Active IQ Config Advisor에 대한 지원은 제한적이며 온라인으로만 제공됩니다.

단계

1. 에 로그인합니다 "NetApp Support 사이트"를 클릭하고 * tools * > * Tools * 를 클릭합니다.
2. Active IQ Config Advisor * 에서 를 클릭합니다 "앱을 다운로드합니다".
3. Active IQ Config Advisor를 다운로드, 설치 및 실행합니다.
4. Active IQ Config Advisor를 실행한 후 도구의 출력을 검토하고 도구에서 발견된 문제를 해결하기 위해 제공되는 권장 사항을 따릅니다.

지원되는 **ONTAP** 업그레이드 경로

업그레이드할 수 있는 ONTAP 버전은 하드웨어 플랫폼과 현재 클러스터의 노드에서 실행 중인 ONTAP 버전에 따라 다릅니다.

하드웨어 플랫폼이 대상 업그레이드 릴리스에 대해 지원되는지 확인하려면 을 참조하십시오 "NetApp Hardware Universe를 참조하십시오". 를 사용합니다 "NetApp 상호 운용성 매트릭스 툴" 를 선택합니다 "구성에 대한 지원을 확인합니다".

현재 **ONTAP** 버전을 확인하려면**:**

- System Manager에서 * Cluster > Overview * 를 클릭합니다.
- CLI(Command Line Interface)에서 를 사용합니다 `cluster image show` 명령. 를 누릅니다 를 사용할 수도 있습니다 `system node image show` 명령을 고급 권한 수준에서 설정하여 세부 정보를 표시합니다.

업그레이드 경로의 유형입니다

가능하면 항상 자동 무중단 업그레이드(ANDU)가 권장됩니다. 현재 및 대상 릴리스에 따라 업그레이드 경로는 * DIRECT *, * DIRECT multi-hop * 또는 * multi-stage * 입니다.

- * 직접 *

  언제든지 단일 소프트웨어 이미지를 사용하여 인접한 다음 ONTAP 릴리스 제품군으로 직접 업그레이드할 수 있습니다. 대부분의 릴리스의 경우 소프트웨어 이미지를 설치하여 실행 중인 릴리스보다 최대 4개의 릴리스로 직접

업그레이드할 수도 있습니다.

예를 들어, 9.12.1에서 9.13.1로, 또는 9.13.1에서 9.17.1로 직접 업그레이드 경로를 사용할 수 있습니다.

ALL_DIRECT_UPGRADE 경로는 에서 지원됩니다 "혼합 버전 클러스터".

- * 직접 멀티 홉 *

  인접하지 않은 릴리즈로 일부 자동 ANDU(무중단 업그레이드)를 사용하려면 중간 릴리즈와 대상 릴리즈용 소프트웨어 이미지를 설치해야 합니다. 자동 업그레이드 프로세스는 백그라운드에서 중간 이미지를 사용하여 대상 릴리스에 대한 업데이트를 완료합니다.

  예를 들어, 클러스터에서 9.3을 실행 중이고 9.7로 업그레이드하려는 경우 9.5와 9.7 모두에 대해 ONTAP 설치 패키지를 로드한 다음 9.7로 ANDU를 시작합니다. ONTAP는 먼저 클러스터를 9.5로 업그레이드한 다음 9.7로 자동 업그레이드합니다. 프로세스 중에 여러 테이크오버/반환 작업 및 관련 재부팅이 예상되어야 합니다.

- * 다단계 *

  직접 또는 직접 다중 홉 경로를 인접하지 않은 대상 릴리스에 사용할 수 없는 경우 먼저 지원되는 중간 릴리스로 업그레이드한 다음 대상 릴리스로 업그레이드해야 합니다.

  예를 들어, 현재 9.8을 실행 중이고 9.16.1로 업그레이드하려는 경우 여러 단계로 구성된 업그레이드를 완료해야 합니다. 먼저 9.8에서 9.12.1로 업그레이드한 다음, 9.12.1에서 9.16.1로 업그레이드합니다. 이전 릴리스에서 업그레이드하려면 중간 업그레이드를 여러 번 거쳐야 하며, 3단계 이상이 필요할 수도 있습니다.

  다단계 업그레이드를 시작하기 전에 대상 릴리스가 하드웨어 플랫폼에서 지원되는지 확인하십시오.

주요 업그레이드를 시작하기 전에 클러스터에서 실행 중인 ONTAP 버전의 최신 패치 릴리즈로 먼저 업그레이드하는 것이 좋습니다. 이렇게 하면 업그레이드하기 전에 현재 버전의 ONTAP에서 문제가 해결됩니다.

예를 들어, 시스템에서 ONTAP 9.3P9를 실행 중이고 9.11.1로 업그레이드할 계획이라면 먼저 최신 9.3 패치 릴리스로 업그레이드한 다음 9.3에서 9.11.1로 업그레이드 경로를 따라야 합니다.

에 대해 자세히 알아보십시오 "NetApp Support 사이트에서 권장되는 최소 ONTAP 릴리즈".

지원되는 업그레이드 경로

다음 업그레이드 경로는 ONTAP 소프트웨어의 자동 및 수동 업그레이드에 지원됩니다. 이러한 업그레이드 경로는 온프레미스 ONTAP 및 ONTAP Select 에 적용됩니다. 다양한 것이 있습니다 "Cloud Volumes ONTAP에 대해 지원되는 업그레이드 경로" .

* 혼합 버전 ONTAP 클러스터 *: all_direct_and_direct multi-hop_upgrade 경로에는 혼합 버전 클러스터와 호환되는 ONTAP 버전이 포함되어 있습니다. multi-stage_upgrades에 포함된 ONTAP 버전은 혼합 버전 클러스터와 호환되지 않습니다. 예를 들어 9.8에서 9.12.1로 업그레이드하는 것은 _DIRECT_UPGRADE입니다. 9.8 및 9.12.1을 실행하는 노드가 있는 클러스터는 지원되는 혼합 버전 클러스터입니다. 9.8에서 9.13.1로의 업그레이드는 _ multi-stage_upgrade입니다. 9.8 및 9.13.1을 실행하는 노드가 있는 클러스터는 지원되는 혼합 버전 클러스터가 아닙니다.

ONTAP 9.10.1 이상

현재 **ONTAP** 릴리스를 사용하는 경우…	대상 **ONTAP** 릴리스는 다음과 같습니다.	자동 또는 수동 업그레이드 경로는…
9.17.1	9.18.1	직접
9.16.1	9.18.1	직접
	9.17.1	직접
9.15.1	9.18.1	직접
	9.17.1	직접
	9.16.1	직접
9.14.1	9.18.1	직접
	9.17.1	직접
	9.16.1	직접
	9.15.1	직접
9.13.1	9.18.1	다단계 • 9.13.1 → 9.17.1 • 9.17.1 → 9.18.1
	9.17.1	직접
	9.16.1	직접
	9.15.1	직접
	9.14.1	직접
9.12.1	9.18.1	다단계 • 9.12.1 → 9.16.1 • 9.16.1 → 9.18.1
	9.17.1	다단계 • 9.12.1 → 9.16.1 • 9.16.1 → 9.17.1
	9.16.1	직접
	9.15.1	직접
	9.14.1	직접
	9.13.1	직접

현재 **ONTAP** 릴리스를 사용하는 경우…	대상 **ONTAP** 릴리스는 다음과 같습니다.	자동 또는 수동 업그레이드 경로는…
9.11.1	9.18.1	다단계 • 9.11.1 → 9.15.1 • 9.15.1 → 9.18.1
	9.17.1	다단계 • 9.11.1 → 9.15.1 • 9.15.1 → 9.17.1
	9.16.1	다단계 • 9.11.1 → 9.15.1 • 9.15.1 → 9.16.1
	9.15.1	직접
	9.14.1	직접
	9.13.1	직접
	9.12.1	직접

현재 **ONTAP** 릴리스를 사용하는 경우…	대상 **ONTAP** 릴리스는 다음과 같습니다.	자동 또는 수동 업그레이드 경로는…
9.10.1	9.18.1	다단계 • 9.10.1 → 9.14.1 • 9.14.1 → 9.18.1
	9.17.1	다단계 • 9.10.1 → 9.14.1 • 9.14.1 → 9.17.1
	9.16.1	다단계 • 9.10.1 → 9.14.1 • 9.14.1 → 9.16.1
	9.15.1	다단계 • 9.10.1 → 9.14.1 • 9.14.1 → 9.15.1
	9.14.1	직접
	9.13.1	직접
	9.12.1	직접
	9.11.1	직접

ONTAP 9.9.1에서

현재 **ONTAP** 릴리스를 사용하는 경우…	대상 **ONTAP** 릴리스는 다음과 같습니다.	자동 또는 수동 업그레이드 경로는…
9.9.1	9.18.1	다단계 • 9.9.1 → 9.13.1 • 9.13.1→9.17.1 • 9.17.1→9.18.1
	9.17.1	다단계 • 9.9.1 → 9.13.1 • 9.13.1→9.17.1
	9.16.1	다단계 • 9.9.1 → 9.13.1 • 9.13.1 → 9.16.1
	9.15.1	다단계 • 9.9.1 → 9.13.1 • 9.13.1 → 9.15.1
	9.14.1	다단계 • 9.9.1 → 9.13.1 • 9.13.1 → 9.14.1
	9.13.1	직접
	9.12.1	직접
	9.11.1	직접
	9.10.1	직접

ONTAP 9.8에서

MetroCluster IP 구성에서 ONTAP 9.8에서 9.10.1 이상으로 다음 플랫폼 모델을 업그레이드하려면 먼저 ONTAP 9.9.1로 업그레이드해야 합니다.

- FAS2750
- 500f로 설정합니다
- AFF A220
- AFF A250

현재 **ONTAP** 릴리스를 사용하는 경우…	대상 **ONTAP** 릴리스는 다음과 같습니다.	자동 또는 수동 업그레이드 경로는…
9.8	9.18.1	다단계 • 9.8 → 9.12.1 • 9.12.1 → 9.16.1 • 9.16.1 → 9.18.1
	9.17.1	다단계 • 9.8 → 9.12.1 • 9.12.1 → 9.16.1 • 9.16.1 → 9.17.1
	9.16.1	다단계 • 9.8 → 9.12.1 • 9.12.1 → 9.16.1
	9.15.1	다단계 • 9.8 → 9.12.1 • 9.12.1 → 9.15.1
	9.14.1	다단계 • 9.8 → 9.12.1 • 9.12.1 → 9.14.1
	9.13.1	다단계 • 9.8 → 9.12.1 • 9.12.1 → 9.13.1
	9.12.1	직접
	9.11.1	직접
	9.10.1	직접
	9.9.1	직접

ONTAP 9.7에서

ONTAP 9.7의 업그레이드 경로는 자동 업그레이드 또는 수동 업그레이드 수행 여부에 따라 다를 수 있습니다.

자동화된 경로

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...
9.7		

	9.12.1	다단계 • 9.7 → 9.8 • 9.8 → 9.12.1
현재 **ONTAP** 릴리스를 사용하는 경우…	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 업그레이드 경로는…
	9.11.1	직접 멀티 홉(9.8 및 9.11.1의 이미지 필요)
	9.10.1	직접 멀티 홉(9.8 및 9.10.1P1 이상의 P 릴리즈에 대한 이미지 필요)
	9.9.1	직접
	9.8	직접

수동 경로

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	수동 업그레이드 경로
9.7		

	9.12.1	다단계 • 9.7 → 9.8 • 9.8 → 9.12.1
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	수동 업그레이드 경로
	9.11.1	다단계 • 9.7 → 9.8 • 9.8 → 9.11.1
	9.10.1	다단계 • 9.7 → 9.8 • 9.8 → 9.10.1
	9.9.1	직접
	9.8	직접

ONTAP 9.6에서

ONTAP 9.6의 업그레이드 경로는 자동 업그레이드 또는 수동 업그레이드 수행 여부에 따라 다를 수 있습니다.

자동화된 경로

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...
9.6		

		• 9.6 → 9.8 • 9.8 → 9.12.1
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...
	9.12.1	다단계 • 9.6 → 9.8 • 9.8 → 9.12.1
	9.11.1	다단계 • 9.6 → 9.8 • 9.8 → 9.11.1
	9.10.1	직접 멀티 홉(9.8 및 9.10.1P1 이상의 P 릴리즈에 대한 이미지 필요)
	9.9.1	다단계 • 9.6 → 9.8 • 9.8 → 9.9.1
	9.8	직접
	9.7	직접

수동 경로

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	수동 업그레이드 경로
9.6		

		• 9.6 → 9.8 • 9.8 → 9.12.1
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	수동 업그레이드 경로
	9.12.1	다단계 • 9.6 → 9.8 • 9.8 → 9.12.1
	9.11.1	다단계 • 9.6 → 9.8 • 9.8 → 9.11.1
	9.10.1	다단계 • 9.6 → 9.8 • 9.8 → 9.10.1
	9.9.1	다단계 • 9.6 → 9.8 • 9.8 → 9.9.1
	9.8	직접
	9.7	직접

ONTAP 9.5에서

ONTAP 9.5의 업그레이드 경로는 자동 업그레이드 또는 수동 업그레이드 수행 여부에 따라 다를 수 있습니다.

자동화된 경로

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...
9.5		

		• 9.5 → 9.9.1(직접 다중 홉, 9.7 및 9.9.1용 이미지 필요)
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...
	9.12.1	다단계 • 9.5 → 9.9.1(직접 다중 홉, 9.7 및 9.9.1용 이미지 필요) • 9.9.1 → 9.12.1
	9.11.1	다단계 • 9.5 → 9.9.1(직접 다중 홉, 9.7 및 9.9.1용 이미지 필요) • 9.9.1 → 9.11.1
	9.10.1	다단계 • 9.5 → 9.9.1(직접 다중 홉, 9.7 및 9.9.1용 이미지 필요) • 9.9.1 → 9.10.1
	9.9.1	직접 멀티 홉(9.7 및 9.9.1의 이미지 필요)
	9.8	다단계 • 9.5 → 9.7 • 9.7 → 9.8
	9.7	직접
	9.6	직접

수동 업그레이드 경로

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	수동 업그레이드 경로
9.5		

		• 9.7 → 9.9.1 • 9.9.1 → 9.13.1
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	수동 업그레이드 경로
	9.13.1	다단계 • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.13.1
	9.12.1	다단계 • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.12.1
	9.11.1	다단계 • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.11.1
	9.10.1	다단계 • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.10.1
	9.9.1	다단계 • 9.5 → 9.7 • 9.7 → 9.9.1
	9.8	다단계 • 9.5 → 9.7 • 9.7 → 9.8
	9.7	직접
	9.6	직접

ONTAP 9.4-9.0부터

ONTAP 9.4, 9.3, 9.2, 9.1 및 9.0의 업그레이드 경로는 자동 업그레이드를 수행하는지 또는 수동 업그레이드를 수행하는지에 따라 다를 수 있습니다.

자동화된 업그레이드 경로

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...
9.4		

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...

	9.8	다단계 • 9.4 → 9.5
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동화 계획에 대한 지침을 보려면 9.7 및 9.8의 이미지 필요)
	9.7	다단계 • 9.4 → 9.5 • 9.5 → 9.7
	9.6	다단계 • 9.4 → 9.5 • 9.5 → 9.6
	9.5	직접

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...
9.3		

		• 9.7 → 9.9.1 • 9.9.1 → 9.13.1
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...
	9.13.1	다단계 • 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요) • 9.7 → 9.9.1 • 9.9.1 → 9.13.1
	9.12.1	다단계 • 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요) • 9.7 → 9.9.1 • 9.9.1 → 9.12.1
	9.11.1	다단계 • 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요) • 9.7 → 9.9.1 • 9.9.1 → 9.11.1
	9.10.1	다단계 • 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요) • 9.7 → 9.10.1(직접 다중 홉, 9.8 및 9.10.1의 이미지 필요)
	9.9.1	다단계 • 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요) • 9.7 → 9.9.1
	9.8	다단계 • 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요) • 9.7 → 9.8
	9.7	직접 멀티 홉(9.5 및 9.7의 경우 이미지 필요)
	9.6	다단계 • 9.3 → 9.5 • 9.5 → 9.6
	9.5	직접
	9.4	사용할 수 없습니다

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...
9.2		

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...

		• 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요) • 9.7 → 9.10.1(직접 다중 홉, 9.8 및 9.10.1의 이미지 필요)
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하에 가능한 업그레이드 경로는...
	9.9.1	다단계 • 9.2 → 9.3 • 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요) • 9.7 → 9.9.1
	9.8	다단계 • 9.2 → 9.3 • 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요) • 9.7 → 9.8
	9.7	다단계 • 9.2 → 9.3 • 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요)
	9.6	다단계 • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5	다단계 • 9.3 → 9.5 • 9.5 → 9.6
	9.4	사용할 수 없습니다
	9.3	직접

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...
9.1		

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...

		• 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요) • 9.7 → 9.10.1(직접 다중 홉, 9.8 및 9.10.1의 이미지 필요)
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하에게 적용되는 업그레이드 경로는...
	9.9.1	다단계 • 9.1 → 9.3 • 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요) • 9.7 → 9.9.1
	9.8	다단계 • 9.1 → 9.3 • 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요) • 9.7 → 9.8
	9.7	다단계 • 9.1 → 9.3 • 9.3 → 9.7(직접 다중 홉, 9.5 및 9.7의 이미지 필요)
	9.6	다단계 • 9.1 → 9.3 • 9.3→ 9.6(직접 다중 홉, 9.5 및 9.6의 이미지 필요)
	9.5	다단계 • 9.1 → 9.3 • 9.3 → 9.5
	9.4	사용할 수 없습니다
	9.3	직접
	9.2	사용할 수 없습니다

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...
9.0		

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동 업그레이드 경로는...

		• 9.0 → 9.1 • 9.1 → 9.3
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	귀하의 자동업그레이드 경로는...
	9.4	사용할 수 없습니다
	9.3	다단계 • 9.0 → 9.1 • 9.1 → 9.3
	9.2	사용할 수 없습니다
	9.1	직접

수동 업그레이드 경로

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**ANDU** 업그레이드 경로는 다음과 같습니다.
9.4		

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**ANDU** 업그레이드 경로는 다음과 같습니다.

		• 9.5 → 9.7 • 9.7 → 9.9.1
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**AND** 업그레이드 경로는 다음과 같습니다.
	9.9.1	다단계 • 9.4 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1
	9.8	다단계 • 9.4 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9.7	다단계 • 9.4 → 9.5 • 9.5 → 9.7
	9.6	다단계 • 9.4 → 9.5 • 9.5 → 9.6
	9.5	직접

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**ANDU** 업그레이드 경로는 다음과 같습니다.
9.3		

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**ANDU** 업그레이드 경로는 다음과 같습니다.

		• 9.5 → 9.7 • 9.7 → 9.9.1
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**AND** 업그레이드 경로는 다음과 같습니다.
	9.9.1	다단계 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1
	9.8	다단계 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9.7	다단계 • 9.3 → 9.5 • 9.5 → 9.7
	9.6	다단계 • 9.3 → 9.5 • 9.5 → 9.6
	9.5	직접
	9.4	사용할 수 없습니다

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**ANDU** 업그레이드 경로는 다음과 같습니다.
9.2		

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**ANDU** 업그레이드 경로는 다음과 같습니다.

		• 9.5 → 9.7 • 9.7 → 9.9.1
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**AND** 업그레이드 경로는 다음과 같습니다.
	9.10.1	다단계 • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.10.1
	9.9.1	다단계 • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1
	9.8	다단계 • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9.7	다단계 • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7
	9.6	다단계 • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5	다단계 • 9.2 → 9.3 • 9.3 → 9.5
	9.4	사용할 수 없습니다
	9.3	직접

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**ANDU** 업그레이드 경로는 다음과 같습니다.
9.1		

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**ANDU** 업그레이드 경로는 다음과 같습니다.

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**ANDU** 업그레이드 경로는 다음과 같습니다.

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**ANDU** 업그레이드 경로는 다음과 같습니다.
	9.4	사용할 수 없습니다
	9.3	• 9.3 → 9.5 직접
	9.2	사용할 수 없습니다

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**ANDU** 업그레이드 경로는 다음과 같습니다.
9.0		

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**ANDU** 업그레이드 경로는 다음과 같습니다.

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**ANDU** 업그레이드 경로는 다음과 같습니다.

		• 9.3 → 9.5 • 9.5 → 9.7
현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	**AND** 업그레이드 경로는 다음과 같습니다.
	9.7	다단계 • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7
	9.6	다단계 • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5	다단계 • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5
	9.4	사용할 수 없습니다
	9.3	다단계 • 9.0 → 9.1 • 9.1 → 9.3
	9.2	사용할 수 없습니다
	9.1	직접

Data ONTAP 8

을 사용하여 플랫폼이 타겟 ONTAP 릴리즈를 실행할 수 있는지 확인하십시오 "NetApp Hardware Universe를 참조하십시오".

- 참고: * Data ONTAP 8.3 업그레이드 가이드에 4노드 클러스터의 경우 epsilon을 마지막으로 보유하는 노드를 업그레이드할 계획이라는 오류 메시지가 표시됩니다. Data ONTAP 8.2.3부터 계속 업그레이드할 필요는 없습니다. 자세한 내용은 을 참조하십시오 "NetApp 버그 온라인 버그 ID 805277".

  Data ONTAP 8.3.x에서

  ONTAP 9.1로 직접 업그레이드한 다음 이후 릴리즈로 업그레이드할 수 있습니다.

8.2.x를 포함한 **Data ONTAP 8.3.x** 이전 버전에서

먼저 Data ONTAP 8.3.x로 업그레이드한 다음 ONTAP 9.1로 업그레이드한 다음 이후 릴리즈로 업그레이드해야 합니다.

관련 정보

- "ONTAP 명령 참조입니다"
- "클러스터 이미지가 표시됩니다"
- "시스템 노드 이미지가 표시됩니다"

업그레이드하기 전에 **ONTAP** 클러스터 **LIF** 페일오버 구성을 확인하십시오

ONTAP를 업그레이드하기 전에 클러스터의 페일오버 정책과 페일오버 그룹이 올바르게 구성되어 있는지 확인해야 합니다.

업그레이드 프로세스 중에 업그레이드 방법을 기반으로 LIF가 마이그레이션됩니다. 업그레이드 방법에 따라 LIF 페일오버 정책을 사용하거나 사용하지 않을 수 있습니다.

클러스터에 8개 이상의 노드가 있는 경우 배치 방법을 사용하여 자동 업그레이드가 수행됩니다. 일괄 업그레이드 방법에서는 클러스터를 여러 업그레이드 일괄 처리로 나누고, 첫 번째 일괄 작업에서 노드 집합을 업그레이드하고, 고가용성(HA) 파트너를 업그레이드한 다음, 나머지 일괄 처리에 대해 이 프로세스를 반복합니다. ONTAP 9.7 이하에서 배치 방법을 사용하면 LIF가 업그레이드 중인 노드의 HA 파트너로 마이그레이션됩니다. ONTAP 9.8 이상에서는 일괄 처리 방법을 사용하면 LIF가 다른 일괄 그룹으로 마이그레이션됩니다.

클러스터에 노드가 8개 미만인 경우 롤링 방법을 사용하여 자동 업그레이드가 수행됩니다. 롤링 업그레이드 방법에는 HA 쌍의 각 노드에서 페일오버 작업을 시작하고, 페일오버된 노드를 업데이트하고, 기브백을 시작한 다음, 클러스터의 각 HA 쌍에 대해 프로세스를 반복하는 작업이 포함됩니다. 롤링 방법을 사용하는 경우 LIF 페일오버 정책에 정의된 대로 LIF가 페일오버 타겟 노드로 마이그레이션됩니다.

단계

1. 각 데이터 LIF의 페일오버 정책을 표시합니다.

ONTAP 버전이…	이 명령을 사용합니다
9.6 이상	`network interface show -service-policy *data* -failover`
9.5 이하	네트워크 인터페이스 show-role data-failover를 선택합니다

이 예는 2개의 데이터 LIF가 있는 2노드 클러스터의 기본 페일오버 구성을 보여줍니다.

```
cluster1::> network interface show -role data -failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------
---------------
vs0
         lif0            node0:e0b             nextavail       system-
defined
                         Failover Targets: node0:e0b, node0:e0c,
                                           node0:e0d, node0:e0e,
                                           node0:e0f, node1:e0b,
                                           node1:e0c, node1:e0d,
                                           node1:e0e, node1:e0f
vs1
         lif1            node1:e0b             nextavail       system-
defined
                         Failover Targets: node1:e0b, node1:e0c,
                                           node1:e0d, node1:e0e,
                                           node1:e0f, node0:e0b,
                                           node0:e0c, node0:e0d,
                                           node0:e0e, node0:e0f
```

장애 조치 타겟 * 필드에는 각 LIF에 대한 장애 조치 타겟의 우선 순위가 지정된 목록이 표시됩니다. 예를 들어, 'lif0'이 홈 포트(Node0의 e0b)에서 페일오버되는 경우 먼저 Node0의 포트 e0c로 페일오버를 시도합니다. lif0이 e0c로 페일오버할 수 없는 경우 Node0의 포트 e0d 등으로 페일오버를 시도합니다.

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. SAN LIF 이외의 LIF에 대해 페일오버 정책을 * disabled * 로 설정한 경우, 를 사용하십시오 `network interface modify` 명령을 사용하여 페일오버를 설정합니다.

   에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 각 LIF에 대해 * 페일오버 타겟 * 필드에 LIF의 홈 노드가 업그레이드 중인 동안 유지될 다른 노드의 데이터 포트가 포함되어 있는지 확인합니다.

   'network interface failover-groups modify' 명령을 사용하여 페일오버 그룹에 장애 조치 대상을 추가할 수 있습니다.

   예

```
network interface failover-groups modify -vserver vs0 -failover-group
fg1 -targets sti8-vsim-ucs572q:e0d,sti8-vsim-ucs572r:e0d
```

관련 정보

- "네트워크 및 LIF 관리"

- "네트워크 인터페이스"
- "네트워크 인터페이스 페일오버 그룹 수정"

업그레이드 전에 **ONTAP** 클러스터 **SVM** 라우팅 구성을 확인합니다

운영 중단을 방지하려면 ONTAP 소프트웨어를 업그레이드하기 전에 기본 SVM 경로가 특정 경로로 연결할 수 없는 네트워크 주소에 연결할 수 있는지 확인해야 합니다. SVM을 위한 기본 경로 하나를 구성하는 것이 모범 사례입니다. 자세한 내용은 을 참조하십시오 "SU134: ONTAP의 잘못된 라우팅 구성으로 인해 네트워크 액세스가 중단될 수 있습니다".

SVM을 위한 라우팅 테이블은 SVM이 대상과 통신하는 데 사용하는 네트워크 경로를 결정합니다. 라우팅 테이블이 작동하는 방식을 이해하여 네트워크 문제가 발생하기 전에 이를 방지하는 것이 중요합니다.

라우팅 규칙은 다음과 같습니다.

- ONTAP는 가장 구체적인 사용 가능한 경로를 통해 트래픽을 라우팅합니다.
- ONTAP는 더 구체적인 경로를 사용할 수 없는 경우 기본 게이트웨이 경로(넷마스크 0비트)를 통해 트래픽을 마지막 수단으로 라우팅합니다.

동일한 대상, 넷마스크 및 메트릭이 있는 라우트의 경우, 재부팅 후 또는 업그레이드 후에 시스템이 동일한 경로를 사용할 것이라는 보장은 없습니다. 특히 여러 기본 경로를 구성한 경우 이 문제가 발생할 수 있습니다.

특별한 고려 사항

업그레이드하기 전에 특정 **ONTAP** 구성을 확인합니다

특정 클러스터 구성의 경우, ONTAP 소프트웨어 업그레이드를 시작하기 전에 특정 작업을 수행해야 합니다. 예를 들어 SAN 구성을 사용하는 경우 업그레이드를 시작하기 전에 각 호스트가 올바른 수의 직접 및 간접 경로로 구성되었는지 확인해야 합니다.

다음 표를 검토하여 수행해야 할 추가 단계를 결정합니다.

ONTAP를 업그레이드하기 전에 스스로에게 물어보십시오.	답변이 * 예 * 인 경우 다음을 수행하십시오.
현재 클러스터가 혼합 버전입니까?	혼합 버전 요구 사항을 확인합니다
MetroCluster 구성이 있습니까?	MetroCluster 구성에 대한 구체적인 업그레이드 요구 사항을 검토합니다
SAN 구성이 있습니까?	SAN 호스트 구성을 확인합니다
클러스터에 SnapMirror 관계가 정의되어 있습니까?	"SnapMirror 관계에 대해 ONTAP 버전의 호환성을 확인합니다"
DP 유형 SnapMirror 관계가 정의되어 있으며 ONTAP 9.12.1 이상으로 업그레이드됩니까?	"기존 DP 유형 관계를 XDP로 변환합니다"
SnapMirror S3를 사용하고 있고 ONTAP 9.12.1 이상으로 업그레이드합니까?	"SnapMirror S3 구성에 대한 라이센스를 확인합니다"

ONTAP를 업그레이드하기 전에 스스로에게 물어보십시오.	답변이 * 예 * 인 경우 다음을 수행하십시오.
캐스케이드의 중간 볼륨에서 장기 보존 스냅샷을 활성화했습니까?	"계단식 토폴로지의 중간 볼륨에서 장기 보존 스냅샷을 비활성화합니다"
외부 키 관리 서버와 함께 NetApp Storage Encryption을 사용하고 있습니까?	기존 키 관리 서버 연결을 삭제합니다
SVM에 넷그룹이 로드되어 있습니까?	각 노드에 넷그룹 파일이 있는지 확인합니다
SVM을 생성했고 ONTAP 9.12.1 이전 버전에서 최신 버전으로 업그레이드합니까?	v4.2-xattrs 옵션에 명시적 값을 할당합니다
SSLv3을 사용하는 LDAP 클라이언트가 있습니까?	TLS를 사용하도록 LDAP 클라이언트를 구성합니다
세션 지향 프로토콜을 사용하고 있습니까?	세션 지향 프로토콜의 부작용 검토
관리자 계정이 SSH 공개 키로 인증하는 클러스터에서 SSL FIPS 모드가 활성화됩니까?	SSH 호스트 키 알고리즘 지원을 확인합니다
Autonomous 랜섬웨어 Protection에 활성 경고가 있습니까?	비정상적인 활동에 대한 자율적 랜섬웨어 방어 경고에 대응

혼합 버전 클러스터에 대한 **ONTAP** 버전의 호환성을 확인합니다

혼합 버전 ONTAP 클러스터에서 노드는 서로 다른 두 주요 ONTAP 버전을 단시간 동안 실행합니다. 예를 들어, ONTAP 9.8 및 9.12.1 또는 ONTAP 9.9.1 및 9.13.1을 실행하는 노드가 포함된 클러스터는 혼합 버전 클러스터입니다. ONTAP 9.9.1P1 및 9.9.1P5와 같이 동일한 버전 내에서 서로 다른 패치 수준을 실행하는 노드가 있는 클러스터는 혼합 버전 클러스터가 아닙니다.

혼합 버전 클러스터는 Cloud Volumes ONTAP에 대해 지원되지 않습니다.

NetApp는 제한된 기간 및 특정 시나리오에서 혼합 버전 ONTAP 클러스터를 지원합니다.

다음은 ONTAP 클러스터가 혼합 버전 상태가 되는 가장 일반적인 시나리오입니다.

- 대규모 클러스터에서 ONTAP 소프트웨어 업그레이드

  대규모 클러스터의 모든 노드를 업그레이드하는 데 며칠 또는 몇 주가 걸릴 수 있습니다. 클러스터는 모든 노드가 업그레이드될 때까지 혼합 버전으로 전환되고 유지됩니다.

- 클러스터에 새 노드를 추가할 계획이라면 ONTAP 소프트웨어 업그레이드가 필요합니다

  클러스터에 새 노드를 추가하여 용량을 확장하거나, 컨트롤러를 완전히 교체하는 프로세스에서 새 노드를 추가할 수 있습니다. 어느 경우든 기존 컨트롤러에서 새 시스템의 새로운 노드로 데이터를 마이그레이션할 수 있도록 혼합 버전 상태를 입력해야 할 수 있습니다.

최적의 클러스터 운영을 위해서는 클러스터가 혼합 버전 상태에 있는 시간이 최대한 짧아야 합니다. 혼합 버전 상태에서 클러스터가 지원을 받을 수 있는 최대 기간은 클러스터에서 가장 낮은 ONTAP 버전에 따라 다릅니다.

혼합 버전 클러스터에서 실행 중인 **ONTAP**의 최하위 버전이 다음과 같은 경우...	그런 다음 최대 혼합 버전 상태를 유지할 수 있습니다.
ONTAP 9.8 이상	90일
ONTAP 9.7 이하	7일

클러스터가 혼합 버전 상태에 있는 동안에는 업그레이드 또는 데이터 마이그레이션 프로세스에 필요한 명령을 제외하고 클러스터 작업 또는 구성을 변경하는 명령을 입력할 수 없습니다. 예를 들어, LIF 마이그레이션, 계획된 스토리지 페일오버 작업 또는 대규모 오브젝트 생성 또는 삭제 등의 작업은 업그레이드 및 데이터 마이그레이션이 완료될 때까지 수행해서는 안 됩니다.

ONTAP 소프트웨어 업그레이드에 지원되는 혼합 버전 클러스터

최신 릴리스에서 직접 업그레이드할 수 있도록 지원되는 모든 ONTAP 버전과 함께 혼합 버전 상태를 입력할 수 있습니다. 예를 들어, ONTAP 9.11.1을 실행하는 경우 ONTAP 9.15.1을 실행하는 노드와 혼합 버전 상태를 입력할 수 있습니다. ONTAP 9.11.1 및 ONTAP 9.16.1을 실행하는 노드에서는 혼합 버전 상태를 입력할 수 없습니다. ONTAP 9.16.1은 ONTAP 9.11.1에서 직접 업그레이드할 수 없습니다.

ONTAP 패치(P) 릴리스 버전은 혼합 버전 클러스터의 호환성에 영향을 미치지 않습니다. 예를 들어 ONTAP 9.11.1P6을 실행 중인 경우, 혼합 버전 클러스터 호환성을 위한 현재 ONTAP 릴리스는 ONTAP 9.11.1입니다. 또는 ONTAP 9.12.1을 실행 중이고 ONTAP 9.15.1P2로 업그레이드하려는 경우, 혼합 버전 클러스터 호환성을 위한 대상 ONTAP 릴리스는 ONTAP 9.15.1입니다.

현재 릴리스에서 직접 업그레이드를 지원하지 않는 ONTAP 버전으로 업그레이드하려면 다단계 업그레이드를 수행해야 합니다. 다단계 업그레이드에서는 먼저 현재 릴리스에서 직접 업그레이드할 수 있도록 지원되는 가장 높은 릴리스의 혼합 버전 상태를 입력합니다. 업그레이드를 완료한 다음 대상 릴리스로 별도의 업그레이드를 수행합니다. 예를 들어, 최신 릴리즈가 ONTAP 9.10.1이고 ONTAP 9.16.1로 업그레이드하려는 경우 먼저 혼합 버전 상태를 입력하여 모든 노드를 ONTAP 9.14.1로 업그레이드한 다음 ONTAP 9.14.1에서 ONTAP 9.16.1로 별도로 업그레이드합니다. 및 에 대해 자세히 "다단계 업그레이드""지원되는 업그레이드 경로"알아보십시오.

혼합 버전 클러스터에는 두 개의 주요 ONTAP 릴리즈만 포함될 수 있습니다. 예를 들어, ONTAP 9.13.1 및 9.15.1을 실행하는 노드 또는 ONTAP 9.13.1 및 9.16.1을 실행하는 노드와 혼합 버전 클러스터를 구성할 수 있습니다. ONTAP 9.13.1, 9.15.1 및 9.16.1을 실행하는 노드에서는 혼합 버전 클러스터를 사용할 수 없습니다.

현재 **ONTAP** 릴리스를 사용하는 경우...	대상 **ONTAP** 릴리스는 다음과 같습니다.	업그레이드를 위한 혼합 버전 상태는...
9.17.1	9.18.1	지원
9.16.1	9.18.1	지원
	9.17.1	지원
9.15.1	9.18.1	지원
	9.17.1	지원
	9.16.1	지원
9.14.1	9.18.1	지원
	9.17.1	지원
	9.16.1	지원
	9.15.1	지원

현재 **ONTAP** 릴리스를 사용하는 경우…	대상 **ONTAP** 릴리스는 다음과 같습니다.	업그레이드를 위한 혼합 버전 상태는…
9.13.1	9.18.1	지원되지 않습니다
	9.17.1	지원
	9.16.1	지원
	9.15.1	지원
	9.14.1	지원
9.12.1	9.17.1 이상	지원되지 않습니다
	9.16.1	지원
	9.15.1	지원
	9.14.1	지원
	9.13.1	지원
9.11.1	9.16.1 이상	지원되지 않습니다
	9.15.1	지원
	9.14.1	지원
	9.13.1	지원
	9.12.1	지원
9.10.1	9.15.1 이상	지원되지 않습니다
	9.14.1	지원
	9.13.1	지원
	9.12.1	지원
	9.11.1	지원
9.9.1	9.14.1 이상	지원되지 않습니다
	9.13.1	지원
	9.12.1	지원
	9.11.1	지원
	9.10.1	지원
9.8	9.13.1 이상	지원되지 않습니다
	9.12.1	지원
	9.11.1	지원
	9.10.1	지원
	9.9.1	지원

ONTAP 클러스터에 새 노드 추가

클러스터에 새 노드를 추가할 계획이고 해당 노드에 현재 클러스터에서 실행 중인 버전보다 더 최신 버전의 ONTAP가 필요한 경우, 새 노드를 추가하기 전에 클러스터에서 기존 노드에서 지원되는 소프트웨어 업그레이드를 수행해야 합니다. 클러스터에 추가할 노드에 필요한 최소 버전의 ONTAP로 기존 노드를 모두 업그레이드하는 것이 좋습니다. 그러나 기존 노드 중 일부가 최신 버전의 ONTAP를 지원하지 않기 때문에 이 작업이 불가능할 경우 업그레이드 프로세스의 일부로 제한된 시간 동안 혼합 버전 상태를 입력해야 합니다.

단계

1. "업그레이드" 새 컨트롤러에 필요한 최소 ONTAP 버전을 지원하지 않는 노드는 지원하는 가장 높은 ONTAP 버전으로 변경합니다.

   예를 들어 ONTAP 9.5를 실행하는 FAS8080이 있고 ONTAP 9.12.1을 실행하는 새로운 C-시리즈 플랫폼을 추가하는 경우 FAS8080을 ONTAP 9.8(지원하는 가장 높은 ONTAP 버전)로 업그레이드해야 합니다.

2. "클러스터에 새 노드를 추가합니다".
3. "데이터를 마이그레이션합니다" 클러스터에서 제거 중인 노드에서 새로 추가한 노드로 이동합니다.
4. "클러스터에서 지원되지 않는 노드를 제거합니다"..
5. "업그레이드" 클러스터를 새 노드에서 실행 중인 동일한 ONTAP 버전 및 패치 수준으로 변경하거나 "권장되는 최신 패치 릴리스" 새로운 노드에서 실행되는 ONTAP 버전에 대한 것입니다.
6. 모든 노드가 동일한 ONTAP 버전을 실행하고 있는지 확인하세요.

   a. 클러스터에서 실행 중인 ONTAP 버전을 표시합니다.

   ```
   version
   ```

   b. 클러스터의 각 노드에서 실행 중인 ONTAP 버전을 표시합니다.

   ```
   version *
   ```

   출력에 보고된 ONTAP 버전과 차이가 있는 경우 `version *` (클러스터) 및 `version` (개별 노드) 명령을 실행하여 모든 노드를 동일한 ONTAP 및 패치 버전으로 업데이트합니다. "클러스터 이미지 업데이트".

데이터 마이그레이션에 대한 자세한 내용은 다음을 참조하십시오.

- "애그리게이트를 생성하고 볼륨을 새 노드로 이동합니다"
- "SAN 볼륨 이동에 대한 새 iSCSI 연결을 설정합니다"
- "암호화를 사용하여 볼륨 이동"

MetroCluster 구성에 대한 **ONTAP** 업그레이드 요구 사항을 확인합니다

MetroCluster 구성에서 ONTAP 소프트웨어를 업그레이드하기 전에 클러스터가 특정 요구사항을 충족해야 합니다.

- 두 클러스터 모두 동일한 버전의 ONTAP를 실행해야 합니다.

version 명령을 사용하여 ONTAP 버전을 확인할 수 있습니다.

- 주요 ONTAP 업그레이드를 수행하는 경우 MetroCluster 구성이 정상 모드여야 합니다.
- 패치 ONTAP 업그레이드를 수행하는 경우 MetroCluster 구성은 정상 또는 전환 모드일 수 있습니다.
- 2노드 클러스터를 제외한 모든 구성에서 두 클러스터를 중단 없이 업그레이드할 수 있습니다.

  2노드 클러스터에서 무중단 업그레이드를 위해서는 클러스터를 한 번에 하나의 노드씩 업그레이드해야 합니다.

- 두 클러스터의 애그리게이트는 RAID 상태를 재동기화하지 않아야 합니다.

  MetroCluster 복구하는 동안 미러링된 집계가 다시 동기화됩니다. MetroCluster 구성이 이 상태인지 확인하려면 다음을 사용하십시오. `storage aggregate plex show -in-progress true` 명령. 집계가 동기화되는 경우 재동기화가 완료될 때까지 업그레이드를 수행해서는 안 됩니다.

  자세히 알아보세요 `storage aggregate plex show` 에서 "ONTAP 명령 참조입니다" .

- 업그레이드 진행 중에는 협상된 전환 작업이 실패합니다.

  업그레이드 또는 복원 작업 관련 문제를 방지하려면 두 클러스터의 모든 노드가 동일한 버전의 ONTAP를 실행하지 않는 한 업그레이드 또는 복원 작업 중에 계획되지 않은 전환을 시도하지 마십시오.

MetroCluster 정상 작동을 위한 구성 요구 사항

- 소스 SVM LIF가 홈 노드에 위치해야 합니다.

  타겟 SVM에 대한 데이터 LIF는 홈 노드에 있을 필요가 없습니다.

- 로컬 사이트의 모든 애그리게이트는 온라인 상태여야 합니다.
- 로컬 클러스터의 SVM이 소유하는 모든 루트 및 데이터 볼륨은 온라인 상태여야 합니다.

MetroCluster 전환을 위한 구성 요구사항

- 모든 LIF는 홈 노드에 위치해야 합니다.
- DR 사이트의 루트 애그리게이트를 제외하고 모든 애그리게이트는 온라인 상태여야 합니다.

  DR 사이트의 루트 애그리게이트는 특정 전환 단계 중에 오프라인 상태입니다.

- 모든 볼륨이 온라인 상태여야 합니다.

관련 정보

"MetroCluster 구성에 대한 네트워킹 및 스토리지 상태 확인"

ONTAP를 업그레이드하기 전에 **SAN** 호스트 구성을 확인합니다

SAN 환경에서 ONTAP를 업그레이드하면 경로가 직접 변경됩니다. SAN 클러스터를 업그레이드하기 전에 각 호스트가 올바른 수의 직접 및 간접 경로로 구성되었는지, 각 호스트가 올바른 LIF에 연결되었는지 확인해야 합니다.

단계

1. 각 호스트에서 충분한 수의 직접 및 간접 경로가 구성되어 있고 각 경로가 활성 상태인지 확인합니다.

   각 호스트에는 클러스터의 각 노드에 대한 경로가 있어야 합니다.

2. 각 호스트가 각 노드의 LIF에 연결되어 있는지 확인합니다.

   업그레이드 후 비교할 이니시에이터 목록을 기록해야 합니다. ONTAP 9.11.1 이상을 실행 중인 경우 System Manager를 사용하여 연결 상태를 확인할 수 있으므로 CLI보다 훨씬 명확합니다.

   시스템 관리자

   a. System Manager에서 * 호스트 > SAN 이니시에이터 그룹 * 을 클릭합니다.

      페이지에 이니시에이터 그룹(igroup) 목록이 표시됩니다. 목록이 큰 경우 페이지의 오른쪽 아래 모서리에 있는 페이지 번호를 클릭하여 목록의 추가 페이지를 볼 수 있습니다.

      열에는 igroup에 대한 다양한 정보가 표시됩니다. 9.11.1부터 igroup의 연결 상태도 표시됩니다. 상태 알림 위로 마우스를 가져가면 세부 정보가 표시됩니다.

   CLI를 참조하십시오

   - iSCSI 이니시에이터 나열:

     ```
     iscsi initiator show -fields igroup,initiator-name,tpgroup
     ```

   - FC 이니시에이터 나열:

     ```
     fcp initiator show -fields igroup,wwpn,lif
     ```

SnapMirror를 참조하십시오

SnapMirror 관계에 대한 호환 **ONTAP** 버전

소스 및 타겟 볼륨에서 SnapMirror 데이터 보호 관계를 생성하기 전에 호환되는 ONTAP 버전을 실행해야 합니다. ONTAP를 업그레이드하기 전에 현재 ONTAP 버전이 SnapMirror 관계에 대한 대상 ONTAP 버전과 호환되는지 확인해야 합니다.

통합 복제 관계

사내 또는 Cloud Volumes ONTAP 릴리즈를 사용하여 "XDP" 유형의 SnapMirror 관계 구축:

ONTAP 9.9.0부터:

- ONTAP 9.x.0 릴리즈는 클라우드 전용 릴리즈이며 Cloud Volumes ONTAP 시스템을 지원합니다. 릴리스 버전 뒤의 별표(*)는 클라우드 전용 릴리스를 나타냅니다.

ONTAP 9.16.0은 클라우드 전용 규칙에 대한 예외입니다."ASA r2 시스템" . 릴리스 버전 뒤에 있는 더하기 기호(+)는 ASA r2와 클라우드 지원 릴리스를 모두 나타냅니다. ASA r2 시스템은 다른 ASA r2 시스템에 대해서만 SnapMirror 관계를 지원합니다.

- ONTAP 9.x.1 릴리스는 일반 릴리스이며 온-프레미스 및 Cloud Volumes ONTAP 시스템을 모두 지원합니다.

경우 "고급 용량 밸런싱"ONTAP 9.16.1 이상을 실행하는 클러스터의 볼륨에서 이 설정된SnapMirror 전송이 ONTAP ONTAP 9.16.1 이전 버전을 실행하는 클러스터에 지원되지 않습니다.

상호 운용성은 양방향입니다.

- ONTAP 버전 9.4 이상에 대한 상호 운용성*

ONTAP 버전…	이러한 이전 ONTAP 버전과의 상호 작용…																				
	9.18.1	9.17.1	9.16.1	9.16.0 이상	9.15.1	9.15.0 *	9.14.1	9.14.0 *	9.13.1	9.13.0 *	9.12.1	9.12.0 *	9.11.1	9.11.0 *	9.10.1	9.10.0 *	9.9.1	9.9.0 *	9.8	9.7	9.6	9.5
9.18.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.17.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.16.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.16.0 이상	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.15.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요
9.15.0 *	아니요	* 예 *	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	아니요	아니요	아니요	아니요
9.14.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요
9.14.0 *	아니요	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	아니요	아니요	아니요	아니요

9.13.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요
9.13.0 *	아니요	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	아니요	아니요
9.12.1	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요
9.12.0 *	아니요	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	아니요
9.11.1	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요
9.11.0 *	아니요	아니요	아니요	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요
9.10.1	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.10.0 *	아니요	아니요	아니요	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	* 예 *	* 예 *	* 예 *
9.9.1	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.9.0 *	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.8	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.7	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.6	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.5	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *

SnapMirror 동기식 관계

SnapMirror 동기식은 ONTAP 클라우드 인스턴스에 지원되지 않습니다.

ONTAP 버전…	이러한 이전 ONTAP 버전과의 상호 작용…													
	9.18.1	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.18.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.17.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.16.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요
9.15.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요
9.14.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요
9.13.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요
9.12.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요
9.11.1	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요
9.10.1	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요
9.9.1	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요
9.8	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요
9.7	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.6	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *
9.5	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *

SnapMirror SVM 재해 복구 관계

- 이 매트릭스는 ONTAP 9.10.1부터 시작되는 SVM 데이터 이동성 마이그레이션 기능에 적용됩니다.
- SVM DR을 사용하면 표시된 제한 사항을 충족하지 않는 SVM을 마이그레이션할 수 있습니다. "SVM 마이그레이션(SVM 데이터 이동성)".
- 두 경우 모두 최대 2개의 주요 최신 ONTAP 버전으로 소스 클러스터와 대상 클러스터를 분리할 수 있으며, 대상 버전은 소스 ONTAP 버전과 동일하거나 더 최신 버전이어야 합니다.

SVM 재해 복구 데이터 및 **SVM** 보호**:**

SVM 재해 복구는 동일한 버전의 ONTAP를 실행하는 클러스터 간에만 지원됩니다. * SVM 복제에 대해 버전 독립성이 지원되지 않습니다 *.

SVM 마이그레이션을 위한 **SVM** 재해 복구**:**

- 복제는 소스의 이전 ONTAP 버전에서 대상에 있는 동일한 버전 또는 이후 버전의 ONTAP로 단일 방향으로 지원됩니다.
- 타겟 클러스터의 ONTAP 버전은 아래 표와 같이 최신 주요 온프레미스 버전 2개 또는 최신 주요 클라우드 버전 2개(ONTAP 9.9.0부터 시작)를 초과할 수 없습니다.
  - 장기 데이터 보호 사용 사례에는 복제가 지원되지 않습니다.

릴리스 버전 뒤의 별표(*)는 클라우드 전용 릴리스를 나타냅니다.

지원을 확인하려면 왼쪽 표 열에서 소스 버전을 찾은 다음 맨 위 행에서 대상 버전을 찾습니다(같은 버전에 대한 DR/마이그레이션 및 최신 버전에 대한 마이그레이션만).

ONTAP 9.10.1 이상을 사용하는 경우 다음을 사용할 수 있습니다. "SVM 데이터 이동성" SVM DR 대신 SVM을 한 클러스터에서 다른 클러스터로 마이그레이션하는 기능을 제공합니다.

출처	목적지																				
	9.5	9.6	9.7	9.8	9.9.0 *	9.9.1	9.10.0 *	9.10.1	9.11.0 *	9.11.1	9.12.0 *	9.12.1	9.13.0 *	9.13.1	9.14.0 *	9.14.1	9.15.0 *	9.15.1	9.16.0	9.16.1	9.17.1	9.18.1
9.5	DR/마이그레이션	마이그레이션	마이그레이션																		
9.6		DR/마이그레이션	마이그레이션	마이그레이션																	
9.7			DR/마이그레이션	마이그레이션	마이그레이션																
9.8				DR/마이그레이션	마이그레이션	마이그레이션		마이그레이션													
9.9.0 *					DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션											
9.9.1						DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션											

9.10.0*							DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션										
9.10.1								DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션										
9.11.0*									DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션								
9.11.1										DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션								
9.12.0*											DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션						
9.12.1												DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션						
9.13.0*													DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션				

9.13.1														DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션		
9.14.0*															DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	
9.14.1																DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	
9.15.0*																	DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	
9.15.1																		DR/마이그레이션	마이그레이션	마이그레이션	
9.16.0																			DR/마이그레이션	마이그레이션	마이그레이션
9.16.1																				DR/마이그레이션	마이그레이션

9.17.1																				DR/마이그레이션	마이그레이션
9.18.1																					DR/마이그레이션

SnapMirror 재해 복구 관계

"DP" 유형의 SnapMirror 관계 및 정책 유형 ""비동기 미러""의 경우:

DP 유형 미러는 ONTAP 9.11.1부터 초기화할 수 없으며 ONTAP 9.12.1에서 완전히 사용되지 않습니다. 자세한 내용은 을 참조하십시오 "데이터 보호 SnapMirror 관계의 사용 중단".

다음 표에서 왼쪽에 있는 열은 소스 볼륨의 ONTAP 버전을 나타내고, 맨 위 행은 대상 볼륨에 있을 수 있는 ONTAP 버전을 나타냅니다.

출처	목적지								
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3
9.11.1	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.10.1	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.9.1	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요
9.8	아니요	예	예	예	아니요	아니요	아니요	아니요	아니요
9.7	아니요	아니요	예	예	예	아니요	아니요	아니요	아니요
9.6	아니요	아니요	아니요	예	예	예	아니요	아니요	아니요
9.5	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요
9.4	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요
9.3	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예

상호 운용성은 양방향성이 아닙니다.

기존 **ONTAP SnapMirror DP** 유형 관계를 **XDP**로 변환합니다

ONTAP 9.12.1 이상으로 업그레이드하는 경우 업그레이드하기 전에 DP 유형 관계를 XDP로 변환해야 합니다. ONTAP 9.12.1 이상은 DP 유형 관계를 지원하지 않습니다. 기존 DP 유형 관계를 XDP로 쉽게 변환하여 버전에 상관없이 유연한 SnapMirror를 활용할 수 있습니다.

ONTAP 9.12.1로 업그레이드하기 전에 기존 DP 유형 관계를 XDP로 변환해야 ONTAP 9.12.1 이상 릴리즈로 업그레이드할 수 있습니다.

이 작업에 대해

- SnapMirror는 기존 DP 유형 관계를 XDP로 자동 변환하지 않습니다. 관계를 변환하려면 기존 관계를 분리 및 삭제하고 새로운 XDP 관계를 생성한 다음 관계를 다시 동기화해야 합니다.
- 전환을 계획할 때는 XDP SnapMirror 관계의 백그라운드 준비 및 데이터 웨어하우징 단계에 시간이 오래 걸릴 수 있습니다. SnapMirror 관계가 오랫동안 "준비 중" 상태를 보고하는 것을 보면 흔히 볼 수 있습니다.

SnapMirror 관계 유형을 DP에서 XDP로 변환한 후에는 자동 크기 조정 및 공간 보장과 같은 공간 관련 설정이 더 이상 대상에 복제되지 않습니다.

단계

1. 대상 클러스터에서 SnapMirror 관계가 DP 유형이고, 미러 상태가 SnapMired 상태이고, 관계 상태가 Idle 상태이고, 관계가 정상 상태인지 확인합니다.

```
snapmirror show -destination-path <SVM:volume>
```

다음 예제는 'napmirror show' 명령의 출력을 보여줍니다.

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

명령 출력의 복사본을 유지하여 기존 관계 설정을 추적하는 것이 유용할 수 있습니다 `snapmirror show`. 에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 소스 볼륨과 대상 볼륨에서 두 볼륨에 모두 공통 스냅샷이 있는지 확인합니다.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

다음 예에서는 를 보여 줍니다 `volume snapshot show` 소스 및 대상 볼륨의 출력:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. 변환 중에 예약된 업데이트가 실행되지 않도록 하려면 기존 DP 유형 관계를 중지합니다.

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 설정합니다.

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror quiesce` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 기존 DP 유형 관계 끊기:

```
snapmirror break -destination-path <SVM:volume>
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst의 관계를 나눕니다.

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 대상 볼륨에 스냅샷 자동 삭제가 설정되어 있는 경우 비활성화합니다.

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

다음 예에서는 대상 볼륨에서 스냅샷 자동 삭제를 `volA_dst` 비활성화합니다.

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. 기존 DP 유형 관계 삭제:

```
snapmirror delete -destination-path <SVM:volume>
```

에 대한 자세한 내용은 `snapmirror-delete` "ONTAP 명령 참조입니다"을 참조하십시오.

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 삭제합니다.

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. 소스에서 원본 SVM 재해 복구 관계 해제:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

다음 예에서는 SVM 재해 복구 관계를 해제합니다.

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

에 대한 자세한 내용은 `snapmirror release` "ONTAP 명령 참조입니다"을 참조하십시오.

8. 'napmirror show' 명령에서 보존한 출력을 사용하여 새로운 XDP 유형 관계를 생성할 수 있습니다.

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

새 관계는 동일한 소스 볼륨과 타겟 볼륨을 사용해야 합니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 소스 볼륨 간에 SnapMirror 재해 복구 관계를 생성합니다 `volA` 켜짐 `svm1` 및 타겟 볼륨입니다 `volA_dst` 켜짐 `svm_backup` 기본값 사용 `MirrorAllSnapshots` 정책:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. 소스 및 대상 볼륨 재동기화:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

재동기화 시간을 개선하려면 다음을 사용할 수 있습니다. `-quick-resync` 옵션은 있지만 저장 효율성으로 인한 절감 효과가 사라질 수 있다는 점을 알아야 합니다.

> ⓘ 이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다. 재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 재동기화한다.

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

자세히 알아보세요 `snapmirror resync` 에서 "ONTAP 명령 참조입니다" .

10. 스냅샷의 자동 삭제를 해제한 경우 다시 설정합니다.

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

작업을 마친 후

1. 를 사용합니다 `snapmirror show` 명령을 사용하여 SnapMirror 관계가 생성되었는지 확인합니다.

   에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. SnapMirror XDP 대상 볼륨이 SnapMirror 정책에 정의된 대로 스냅샷 업데이트를 시작하면 소스 클러스터의 명령 출력을 사용하여 `snapmirror list-destinations` 새 SnapMirror XDP 관계를 표시합니다.

DP 유형 관계에 대한 추가 정보

ONTAP 9.3부터 XDP 모드가 기본값이며 명령줄이나 새 스크립트 또는 기존 스크립트에서 DP 모드를 호출하면 자동으로 XDP 모드로 변환됩니다.

기존 관계는 영향을 받지 않습니다. 관계가 이미 DP 유형인 경우 DP 유형이 됩니다. ONTAP 9.5부터 MirrorAndVault는 데이터 보호 모드가 지정되지 않았거나 XDP 모드가 관계 유형으로 지정된 경우 기본 정책입니다. 아래 표는 예상되는 동작을 보여줍니다.

지정하는 경우…	유형은…	기본 정책(정책을 지정하지 않은 경우)은…
DP	XDP	MirrorAllSnapshots(SnapMirror DR)
아무것도 없습니다	XDP	MirrorAndVault(통합 복제)
XDP	XDP	MirrorAndVault(통합 복제)

표에서 볼 수 있듯이 다른 상황에서 XDP에 할당된 기본 정책은 변환이 이전 유형과 동일한 기능을 유지하도록 합니다. 물론 필요에 따라 통합 복제에 대한 정책을 비롯한 다양한 정책을 사용할 수 있습니다.

지정하는 경우…	정책은…	그 결과…
DP	MirrorAllSnapshots을 선택합니다	SnapMirror DR
XDPDefault	SnapVault	MirrorAndVault를 선택합니다
통합 복제	XDP	MirrorAllSnapshots을 선택합니다
SnapMirror DR	XDPDefault	SnapVault

변환 예외 사항은 다음과 같습니다.

- SVM 데이터 보호 관계는 ONTAP 9.3 및 이전 버전에서 DP 모드로 계속 기본값입니다.

  ONTAP 9.4부터 SVM 데이터 보호 관계는 기본적으로 XDP 모드로 설정됩니다.

- 루트 볼륨 로드 공유 데이터 보호 관계는 기본적으로 DP 모드로 유지됩니다.
- SnapLock 데이터 보호 관계는 ONTAP 9.4 이하 버전에서 DP 모드로 계속 기본값입니다.

  ONTAP 9.5부터 SnapLock 데이터 보호 관계는 XDP 모드로 기본 설정됩니다.

- DP의 명시적 호출은 다음 클러스터 전체 옵션을 설정한 경우 계속해서 DP 모드로 설정됩니다.

  ```
  options replication.create_data_protection_rels.enable on
  ```

  DP를 명시적으로 호출하지 않으면 이 옵션은 무시됩니다.

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 중지"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"

ONTAP 업그레이드 전에 장기 보존 스냅샷을 비활성화합니다

계층형 볼륨 관계에서 장기 보존 스냅샷은 모든 ONTAP 9 버전에서 계층 구조의 최종 SnapMirror 대상 볼륨에서만 지원됩니다. 캐스케이드 구조의 중간 볼륨에서 장기 보존 스냅샷을 활성화하면 백업 및 스냅샷이 누락될 수 있습니다.

자세히 알아보세요"장기 보존 스냅샷" .

캐스케이드 구성에서 중간 볼륨에 장기 보존 스냅샷이 활성화된 지원되지 않는 구성이 있는 경우 기술 지원팀에 문의하고 다음 링크를 참조하십시오. https://kb.netapp.com/on-prem/ontap/DP/SnapMirror/SnapMirror-KBs/Cascading_a_volume_with_Long-Term_Retention_ (long-term

retention)_snapshots_enabled_is_not_supported[NetApp 기술 자료: 장기 보존(LTR) 스냅샷이 활성화된 볼륨의 캐스케이드 구성은 지원되지 않습니다^]

다음 ONTAP 버전에서는 최종 SnapMirror 대상 볼륨을 제외한 캐스케이드의 모든 볼륨에서 장기 보존 스냅샷을 활성화할 수 없습니다.

- 9.15.1 이상
- 9.14.1P2 및 P4부터 P14까지
- 9.13.1P9부터 P17까지
- 9.12.1 P12부터 P19까지
- 9.11.1P15부터 P20까지
- 9.10.1P18부터 P20까지
- 9.9.1P20

캐스케이드 구성의 중간 볼륨에 장기 보존 스냅샷을 활성화할 수 있는 ONTAP 버전에서 해당 기능을 차단하는 ONTAP 버전으로 업그레이드하기 전에 백업 및 스냅샷 누락을 방지하기 위해 장기 보존 스냅샷을 비활성화해야 합니다.

다음 시나리오에서 조치를 취해야 합니다.

- 장기 보존 스냅샷은 **A › B › C** SnapMirror 캐스케이드에서 "B" 볼륨 또는 더 큰 캐스케이드의 다른 중간 SnapMirror 대상 볼륨에 구성됩니다.
- 장기 보존 스냅샷은 SnapMirror 정책 규칙에 적용되는 일정에 따라 정의됩니다. 이 규칙은 소스 볼륨의 스냅샷을 복제하지 않고 대상 볼륨에 직접 스냅샷을 생성합니다.

> ⓘ 일정 및 SnapMirror 정책에 대한 자세한 내용은 다음을 참조하세요."NetApp 지식 기반: ONTAP 9 SnapMirror 정책 규칙의 "일정" 매개변수는 어떻게 작동합니까?" .

단계

1. 캐스케이드의 중간 볼륨에 있는 SnapMirror 정책에서 장기 보존 규칙을 제거합니다.

```
Secondary::> snapmirror policy remove-rule -vserver <> -policy <>
-snapmirror-label <>
```

자세히 알아보세요 `snapmirror policy remove-rule` 에서 "ONTAP 명령 참조입니다" .

2. 장기 보존 일정 없이 SnapMirror 레이블에 대한 규칙을 다시 추가하세요.

```
Secondary::> snapmirror policy add-rule -vserver <> -policy <>
-snapmirror-label <> -keep <>
```

> ⓘ SnapMirror 정책 규칙에서 장기 보존 스냅샷을 제거하면 SnapMirror 지정된 레이블이 있는 스냅샷을 소스 볼륨에서 가져옵니다. 적절한 레이블이 지정된 스냅샷을 생성하려면 소스 볼륨의 스냅샷 정책에 일정을 추가하거나 수정해야 할 수도 있습니다.

에 대한 자세한 내용은 `snapmirror policy add-rule` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 필요한 경우 소스 볼륨 스냅샷 정책에 대한 일정을 수정하거나 생성하여 SnapMirror 레이블을 사용하여 스냅샷을 생성할 수 있습니다.

```
Primary::> volume snapshot policy modify-schedule -vserver <> -policy <>
-schedule <> -snapmirror-label <>
```

```
Primary::> volume snapshot policy add-schedule -vserver <> -policy <>
-schedule <> -snapmirror-label <> -count <>
```

SnapMirror 캐스케이드 구성에서 최종 SnapMirror 대상 볼륨에 대해 장기 보존 스냅샷을 활성화할 수 있습니다.

SnapMirror S3 구성에 대한 **ONTAP** 라이센스 확인

ONTAP를 업그레이드하기 전에 SnapMirror S3를 사용하고 있고 ONTAP 9.12.1 이상으로 업그레이드하는 경우 적절한 SnapMirror 라이센스가 있는지 확인해야 합니다.

ONTAP를 업그레이드한 후 ONTAP 9.11.1 이전 버전과 ONTAP 9.12.1 이상 간에 발생한 라이선스 변경 사항으로 인해 SnapMirror S3 관계가 실패할 수 있습니다.

ONTAP 9.11.1 이전 버전

- SnapMirror S3는 NetApp 호스팅 대상 버킷(ONTAP S3 또는 StorageGRID)으로 복제할 때 "ONTAP 1 을 참조하십시오"소프트웨어 제품군이 도입되기 전에 데이터 보호 번들에 포함된 SnapMirror 동기식 라이센스를 확인합니다.
- NetApp가 아닌 타겟 버킷으로 복제할 때 SnapMirror S3는 "ONTAP 1 을 참조하십시오"소프트웨어 제품군 출시 이전에 사용할 수 있었던 하이브리드 클라우드 번들에 포함된 SnapMirror 클라우드 라이센스를 확인합니다.

ONTAP 9.12.1 이상

- SnapMirror S3는 NetApp 호스팅 대상 버킷(ONTAP S3 또는 StorageGRID)으로 복제할 때 "ONTAP 1 을 참조하십시오"소프트웨어 제품군이 도입되기 전에 제공되었던 데이터 보호 번들에 포함된 SnapMirror S3 라이센스를 확인합니다.
- 비 NetApp 대상 버킷으로 복제할 때 SnapMirror S3는 "ONTAP 1 을 참조하십시오"소프트웨어 제품군과 가 도입되기 전에 사용 가능한 하이브리드 클라우드 번들에 포함된 SnapMirror S3 외부 라이센스를 확인합니다 ."ONTAP One 호환성 번들"

기존 **SnapMirror S3** 관계

기존 SnapMirror S3 관계는 ONTAP 9.11.1 이하에서 ONTAP 9.12.1 이상으로 업그레이드한 후에도 계속 작동해야 합니다. 클러스터에 새 라이센스가 없는 경우에도 마찬가지입니다.

클러스터에 적절한 라이센스가 설치되어 있지 않으면 새 SnapMirror S3 관계 생성이 실패합니다.

ONTAP를 업그레이드하기 전에 NetApp Storage Encryption(NSE)을 통해 ONTAP 9.2 이상을 실행하고 ONTAP 9.3 이상으로 업그레이드하는 경우 CLI(Command Line Interface)를 사용하여 기존의 외부 키 관리(KMIP) 서버 연결을 삭제해야 합니다.

단계

1. NSE 드라이브가 잠금 해제되고 열리며 기본 제조 보안 ID 0x0으로 설정되어 있는지 확인합니다.

```
storage encryption disk show -disk *
```

에 대한 자세한 내용은 `storage encryption disk show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 고급 권한 모드로 들어갑니다.

```
set -privilege advanced
```

에 대한 자세한 내용은 `set` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 기본 제조업체 보안 ID 0x0을 사용하여 SED(자체 암호화 디스크)에 FIPS 키를 할당합니다.

```
storage encryption disk modify -fips-key-id 0x0 -disk *
```

에 대한 자세한 내용은 `storage encryption disk modify` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 모든 디스크에 FIPS 키 할당이 완료되었는지 확인합니다.

```
storage encryption disk show-status
```

에 대한 자세한 내용은 `storage encryption disk show-status` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 모든 디스크의 * 모드 * 가 데이터로 설정되어 있는지 확인합니다

```
storage encryption disk show
```

에 대한 자세한 내용은 `storage encryption disk show` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 구성된 KMIP 서버 보기:

```
security key-manager keystore show
```

자세히 알아보세요 `security key-manager keystore show` 에서"ONTAP 명령 참조입니다" .

7. 구성된 KMIP 서버를 삭제합니다.

```
security key-manager delete -address <kmip_ip_address>
```

에 대한 자세한 내용은 `security key-manager delete` "ONTAP 명령 참조입니다"을 참조하십시오.

8. 외부 키 관리자 구성을 삭제합니다.

```
security key-manager external disable
```

자세히 알아보세요 `security key-manager external disable` 에서"ONTAP 명령 참조입니다" .

ⓘ 이 단계에서는 NSE 인증서가 제거되지 않습니다.

다음 단계

업그레이드가 완료되면 를 수행해야 합니다 KMIP 서버 연결을 재구성합니다.

ONTAP를 업그레이드하기 전에 모든 노드에 **Netgroup** 파일이 있는지 확인합니다

ONTAP를 업그레이드하기 전에 넷그룹을 스토리지 가상 머신(SVM)에 로드한 경우 각 노드에 넷그룹 파일이 있는지 확인해야 합니다. 노드에 넷그룹 파일이 없으면 업그레이드가 실패할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 각 SVM에 대한 넷그룹 상태를 표시합니다.

```
vserver services netgroup status
```

3. 각 SVM에 대해 각 노드에 동일한 넷그룹 파일 해시 값이 표시되는지 확인합니다.

```
vserver services name-service netgroup status
```

이 경우 다음 단계를 건너뛰고 업그레이드 또는 되돌리기 작업을 진행할 수 있습니다. 그렇지 않으면 다음 단계를 진행하십시오.

4. 클러스터의 한 노드에서 넷그룹 파일을 수동으로 로드합니다.

```
vserver services netgroup load -vserver vserver_name -source uri
```

이 명령은 모든 노드에서 넷그룹 파일을 다운로드합니다. 넷그룹 파일이 이미 노드에 있는 경우 해당 파일을 덮어씁니다.

관련 정보

"넷그룹 작업"

ONTAP 업그레이드 전에 **v4.2-xattrs** 옵션에 명시적 값을 할당합니다

NFSv4.2 클라이언트가 있는 경우 ONTAP 9.12.1 이상의 특정 릴리스 및 패치에서 업그레이드하기 전에 업그레이드 후 NFS 응답 오류를 방지하기 위해 NFSv4.2 확장 속성 옵션에 대해 명시적 값을 지정해야 합니다.

영향을 받는 버전으로 ONTAP를 업그레이드하기 전에 이 `v4.2-xattrs` 옵션에 값이 명시적으로 할당되지 않은 경우 NFSv4.2 클라이언트에 서버의 확장 속성 옵션이 변경되었음을 알리지 않습니다. 이로 인해 클라이언트와 서버 불일치로 인해 특정 호출에 NFS 응답 오류가 `xattrs` 발생합니다.

시작하기 전에

다음과 같은 경우 NFSv4.2 확장 속성 옵션에 대해 명시적 값을 할당해야 합니다.

- ONTAP 9.11.1 이전 버전을 사용하여 생성된 SVM에서 NFSv4.2를 사용하고 있습니다
- 영향을 받는 이러한 릴리스 및 패치에서 ONTAP를 업그레이드합니다.
  - 9.12.1RC1 ~ 9.12.1P11
  - 9.13.1RC1 ~ 9.13.1P8
  - 9.14.1RC1 ~ 9.14.1P1

이 작업에 대해

이 절차에서 설명하는 명령을 사용하여 값을 설정하려면 ONTAP 9.12.1 이상을 실행해야 합니다.

가 이미 으로 설정된 `enabled` 경우에는 `v4.2-xattrs` 향후 운영 중단을 방지하기 위해 이 속성을 명시적으로 설정해야 `enabled` 합니다. `v4.2-xattrs`disabled로 설정하면 NFSv4.2 클라이언트가 다시 마운트되거나 옵션이 로 `enabled` 설정될 때까지 "잘못된 인수" 응답을 받을 수 있습니다 `v4.2-xattrs`.

단계

- 옵션에 명시적 값을 `v4.2-xattrs` 할당합니다.

```
nfs modify -v4.2-xattrs <enabled/disabled> -vserver <vserver_name>
```

관련 정보

"NFS v4.2-xattrs 필드가 업그레이드 후 뒤집힙니다"

ONTAP 업그레이드 전에 **TLS**를 사용하도록 **LDAP** 클라이언트를 구성합니다

ONTAP를 업그레이드하기 전에 TLS를 사용하도록 LDAP 서버와의 보안 통신을 위해 SSLv3을 사용하여 LDAP 클라이언트를 구성해야 합니다. 업그레이드 후에는 SSL을 사용할 수 없습니다.

기본적으로 클라이언트와 서버 응용 프로그램 간의 LDAP 통신은 암호화되지 않습니다. SSL 사용을 허용하지 않고 TLS 사용을 적용해야 합니다.

단계

1. 사용자 환경의 LDAP 서버가 TLS를 지원하는지 확인합니다.

   그렇지 않으면 계속 진행하지 마십시오. LDAP 서버를 TLS를 지원하는 버전으로 업그레이드해야 합니다.

2. SSL/TLS를 통해 LDAP가 활성화된 ONTAP LDAP 클라이언트 구성을 확인합니다.

   ```
   vserver services name-service ldap client show
   ```

   없는 경우 나머지 단계를 건너뛸 수 있습니다. 하지만 보안을 강화하기 위해 TLS를 통한 LDAP 사용을 고려해야 합니다.

3. 각 LDAP 클라이언트 구성에 대해 SSL이 TLS를 사용하도록 허용하지 않습니다.

   ```
   vserver services name-service ldap client modify -vserver <vserver_name>
   -client-config <ldap_client_config_name> -allow-ssl false
   ```

4. 모든 LDAP 클라이언트에 대해 SSL 사용이 더 이상 허용되지 않는지 확인합니다.

   ```
   vserver services name-service ldap client show
   ```

관련 정보

"NFS 관리"

ONTAP 업그레이드 중 세션 지향 프로토콜의 부정적인 영향에 대해 알아보세요**.**

클러스터 및 세션 지향 프로토콜은 업그레이드하는 동안 I/O 서비스와 같은 특정 영역에서 클라이언트 및 애플리케이션에 악영향을 미칠 수 있습니다.

세션 지향 프로토콜을 사용하는 경우 다음 사항을 고려하십시오.

- 중소기업

  SMBv3에서 지속적으로 사용 가능한(CA) 공유를 제공하는 경우 System Manager 또는 CLI를 통해 자동화된 무중단 업그레이드 방법을 사용할 수 있으며 클라이언트에서 중단이 발생하지 않습니다.

  SMBv1 또는 SMBv2와 함께 공유 또는 SMBv3과 비 CA 공유를 제공하는 경우 업그레이드 테이크오버 및 재부팅 작업 중에 클라이언트 세션이 중단됩니다. 업그레이드하기 전에 사용자에게 세션을 종료하도록 안내해야 합니다.

SMB를 통한 Hyper-V 및 SQL Server는 무중단 운영(NDO)을 지원합니다. SMB 솔루션을 통해 Hyper-V 또는 SQL Server를 구성한 경우, 애플리케이션 서버와 포함된 가상 머신 또는 데이터베이스는 ONTAP 업그레이드 중에 온라인 상태를 유지하고 지속적인 가용성을 제공합니다.

- NFSv4.x

  NFSv4.x 클라이언트는 정상 NFSv4.x 복구 절차를 사용하여 업그레이드 중에 발생한 연결 손실로부터 자동으로 복구합니다. 이 프로세스 중에 애플리케이션이 일시적으로 I/O 지연을 겪을 수 있습니다.

- NDMP

  상태가 손실되었으며 클라이언트 사용자가 작업을 재시도해야 합니다.

- 백업 및 복원

  상태가 손실되었으며 클라이언트 사용자가 작업을 재시도해야 합니다.

  > 업그레이드 도중이나 업그레이드 직전에 백업 또는 복원을 시작하지 마십시오. 이렇게 하면 데이터가 손실될 수 있습니다.

- 애플리케이션(예: Oracle 또는 Exchange)

  효과는 애플리케이션에 따라 다릅니다. 시간 초과 기반 응용 프로그램의 경우 시간 초과 설정을 ONTAP 재부팅 시간보다 길게 변경하여 부작용을 최소화할 수 있습니다.

ONTAP를 업그레이드하기 전에 **SSH** 호스트 키 알고리즘 지원을 확인합니다

ONTAP를 업그레이드하기 전에 관리자 계정이 SSH 공개 키로 인증하는 클러스터에서 SSL FIPS 모드가 활성화되어 있으면 대상 ONTAP 릴리즈에서 호스트 키 알고리즘이 지원되는지 확인해야 합니다.

다음 표에는 ONTAP SSH 연결에 지원되는 호스트 키 유형 알고리즘이 나와 있습니다. 이러한 키 유형은 SSH 공개 인증 구성에 적용되지 않습니다.

ONTAP 릴리즈	FIPS 모드에서 지원되는 키 유형입니다	FIPS 이외의 모드에서 지원되는 키 유형입니다
9.11.1 이상	ECDSA-SHA2-nistp256	ECDSA-SHA2-nistp256+RSA-SHA2-512+RSA-SHA2-256+ssh-ed25519+ssh-dss+ssh-ssh-rsa
9.10.1 이하	ECDSA-SHA2-nistp256+ssh-ed25519	ECDSA-SHA2-nistp256+ssh-ed25519+ssh-dss+ssh-rsa

> ONTAP 9.11.1부터 ssh-ed25519 호스트 키 알고리즘에 대한 지원이 제거되었습니다.

자세한 내용은 을 "FIPS를 사용하여 네트워크 보안을 구성합니다"참조하십시오.

지원되는 키 알고리즘이 없는 기존 SSH 공개 키 계정을 지원되는 키 유형으로 다시 구성해야 업그레이드 또는 관리자 인증이 실패합니다.

"SSH 공개 키 계정 설정에 대해 자세히 알아보십시오."

ONTAP를 업그레이드하기 전에 **ARP(**자율적 랜섬웨어 차단)에서 활동 경고를 해결합니다

ONTAP 9.16.1 이상으로 업그레이드하기 전에 ARP(자율적 랜섬웨어 방어)에서 보고하는 비정상적인 활동 경고에 대응해야 합니다. ONTAP 9.16.1에서 ARP는 머신 러닝/인공 지능(AI) 기반 모델로 변경되었습니다. 이 변경으로 인해 ONTAP 9.15.1 또는 이전 버전의 기존 ARP에서 해결되지 않은 활성 경고는 업그레이드 후 손실됩니다.

단계

1. 에서 보고한 비정상적인 활동 경고에 응답하고 "아프"잠재적인 문제를 해결합니다.
2. 업그레이드 전에 * 업데이트 및 의심되는 파일 유형 지우기 * 를 선택하여 이러한 문제의 해결을 확인하고 결정을 기록하고 정상적인 ARP 모니터링을 재개하십시오.

ONTAP 업그레이드 중에 펌웨어 업데이트를 준비하려면 **SP** 또는 **BMC**를 재부팅합니다

ONTAP 업그레이드 전에 펌웨어를 수동으로 업데이트할 필요는 없습니다. 클러스터의 펌웨어는 ONTAP 업그레이드 패키지에 포함되어 있으며 각 노드의 부팅 장치에 복사됩니다. 그런 다음 새 펌웨어가 업그레이드 프로세스의 일부로 설치됩니다.

클러스터의 버전이 ONTAP 업그레이드 패키지와 함께 제공되는 펌웨어보다 오래된 경우 다음 구성 요소의 펌웨어가 자동으로 업데이트됩니다.

- BIOS/로더
- 서비스 프로세서(SP) 또는 베이스보드 관리 컨트롤러(BMC)
- 스토리지 쉘프
- 디스크
- Flash Cache를 참조하십시오

원활한 업데이트를 준비하려면 업그레이드를 시작하기 전에 SP 또는 BMC를 재부팅해야 합니다.

ONTAP CLI, SP 또는 BMC 사용하여 재부팅하십시오.

CLI를 참조하십시오

1. SP 또는 BMC 재부팅하십시오.

```
system service-processor reboot-sp -node <node_name>
```

SP

1. SP 를 재부팅하세요:

```
sp reboot
```

BMC

1. BMC 를 재부팅하세요:

```
bmc reboot
```

한 번에 하나의 SP 또는 BMC만 재부팅합니다. 재부팅된 SP 또는 BMC가 완전히 재활용될 때까지 기다린 후 다음 SP를 재부팅합니다.

또한 "펌웨어를 수동으로 업데이트합니다"ONTAP 업그레이드 사이에 가능합니다. Digital Advisor가 있으면 "ONTAP 이미지에 현재 포함되어 있는 펌웨어 버전 목록을 봅니다"가능합니다.

업데이트된 펌웨어 버전은 다음과 같습니다.

- "시스템 펌웨어(BIOS, BMC, SP)"
- "쉘프 펌웨어"
- "디스크 및 Flash Cache 펌웨어"

업그레이드하기 전에 **ONTAP** 소프트웨어 이미지를 다운로드합니다

ONTAP를 업그레이드하기 전에 먼저 NetApp Support 사이트에서 대상 ONTAP 소프트웨어 이미지를 다운로드해야 합니다. ONTAP 릴리스에 따라 ONTAP 소프트웨어를 네트워크의 HTTPS, HTTP 또는 FTP 서버 또는 로컬 폴더에 다운로드할 수 있습니다.

실행 중인 경우...	이 위치로 이미지를 다운로드할 수 있습니다...
ONTAP 9.6 이상	• HTTPS 서버 + 서버의 CA 인증서가 로컬 시스템에 설치되어 있어야 합니다. • 로컬 폴더입니다 • HTTP 또는 FTP 서버

실행 중인 경우...	이 위치로 이미지를 다운로드할 수 있습니다...
ONTAP 9.4 이상	• 로컬 폴더입니다 • HTTP 또는 FTP 서버
ONTAP 9.0 이상	HTTP 또는 FTP 서버

이 작업에 대해

- 를 사용하여 자동 무중단 업그레이드(ANDU)를 수행하는 경우 "직접 멀티 홉 업그레이드 경로", 당신은 필요합니다 "다운로드" 업그레이드에 필요한 중간 ONTAP 버전과 대상 ONTAP 버전 모두를 위한 소프트웨어 패키지입니다. 예를 들어, ONTAP 9.8에서 ONTAP 9.13.1로 업그레이드하는 경우 ONTAP 9.12.1 및 ONTAP 9.13.1 모두에 대한 소프트웨어 패키지를 다운로드해야 합니다. 을 참조하십시오 "지원되는 업그레이드 경로" 업그레이드 경로에 중간 소프트웨어 패키지를 다운로드해야 하는지 확인하려면
- NetApp 볼륨 암호화가 있는 시스템을 ONTAP 9.5 이상으로 업그레이드할 경우 NetApp 볼륨 암호화를 포함하는 비제한 국가의 ONTAP 소프트웨어 이미지를 다운로드해야 합니다.

  제한된 국가에서 ONTAP 소프트웨어 이미지를 사용하여 NetApp 볼륨 암호화를 사용하는 시스템을 업그레이드하면 시스템 패닉이 발생하고 볼륨에 대한 액세스가 손실됩니다.

- 펌웨어에 대해 별도의 소프트웨어 패키지를 다운로드할 필요가 없습니다. 클러스터에 대한 펌웨어 업데이트는 ONTAP 소프트웨어 업그레이드 패키지에 포함되어 있으며 각 노드의 부팅 장치에 복사됩니다. 그런 다음 새 펌웨어가 업그레이드 프로세스의 일부로 설치됩니다.

단계

1. 에서 대상 ONTAP 소프트웨어를 찾습니다 "소프트웨어 다운로드" NetApp Support 사이트의 영역입니다.

   ONTAP Select 업그레이드의 경우 * ONTAP Select 노드 업그레이드 * 를 선택합니다.

2. 소프트웨어 이미지(예: 97_q_image.tgz)를 적절한 위치에 복사합니다.

   ONTAP 릴리스에 따라 이미지는 로컬 시스템 또는 스토리지 시스템의 로컬 폴더에 서비스될 HTTP, HTTPS 또는 FTP 서버 디렉토리입니다.

ONTAP 업그레이드 방법

ONTAP 소프트웨어 업그레이드 방법

System Manager를 사용하여 ONTAP 소프트웨어를 자동으로 업그레이드할 수 있습니다. 또는 ONTAP 명령줄 인터페이스(CLI)를 사용하여 자동 또는 수동 업그레이드를 수행할 수 있습니다. ONTAP 업그레이드 방법은 구성, 현재 ONTAP 버전 및 클러스터의 노드 수에 따라 다릅니다. NetApp은 사용자의 구성에 다른 방식이 필요하지 않은 한 System Manager를 사용하여 자동화된 업그레이드를 수행할 것을 권장합니다. 예를 들어, ONTAP 9.3 이상을 실행하는 4노드 MetroCluster 구성이 있는 경우 System Manager를 사용하여 자동 업그레이드(자동 무중단 업그레이드 또는 ANDU라고도 함)를 수행해야 합니다.

NetApp 콘솔을 통해 ONTAP 9.15.1 이상으로 업그레이드하는 경우 다음을 따르세요."NetApp 콘솔 설명서의 업그레이드 절차" .

업그레이드는 롤링 업그레이드 프로세스 또는 일괄 업그레이드 프로세스를 사용하여 실행할 수 있습니다. 둘 다 무중단 운영을 제공합니다.

자동화된 업그레이드를 위해 ONTAP는 각 노드에 타겟 ONTAP 이미지를 자동으로 설치하고, 클러스터 구성 요소를 확인하여 클러스터를 중단 없이 업그레이드할 수 있는지 확인한 다음, 노드 수에 따라 백그라운드에서 일괄 처리 또는 롤링 업그레이드를 실행합니다. 수동 업그레이드의 경우 관리자는 클러스터의 각 노드를 업그레이드할 준비가 되었음을 수동으로 확인한 다음 롤링 업그레이드를 실행하는 단계를 수행합니다.

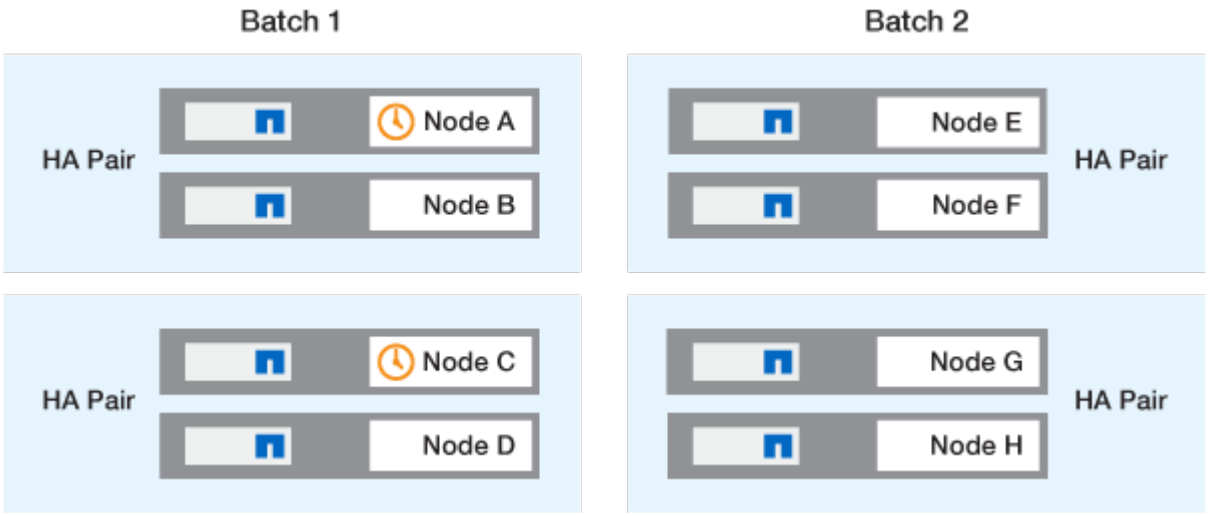
ONTAP 롤링 업그레이드

롤링 업그레이드 프로세스는 노드 수가 8개 미만인 클러스터의 기본값입니다. 롤링 업그레이드 프로세스에서 노드가 오프라인 상태로 전환되고 파트너가 스토리지를 인계하는 동안 업그레이드됩니다. 노드 업그레이드가 완료되면 파트너 노드가 원래 소유 노드에 제어권을 다시 제공하며 이 프로세스는 파트너 노드에서 반복됩니다. 모든 HA 쌍이 타겟 릴리즈를 실행할 때까지 각 HA 쌍이 추가로 업그레이드됩니다.

ONTAP 일괄 업그레이드

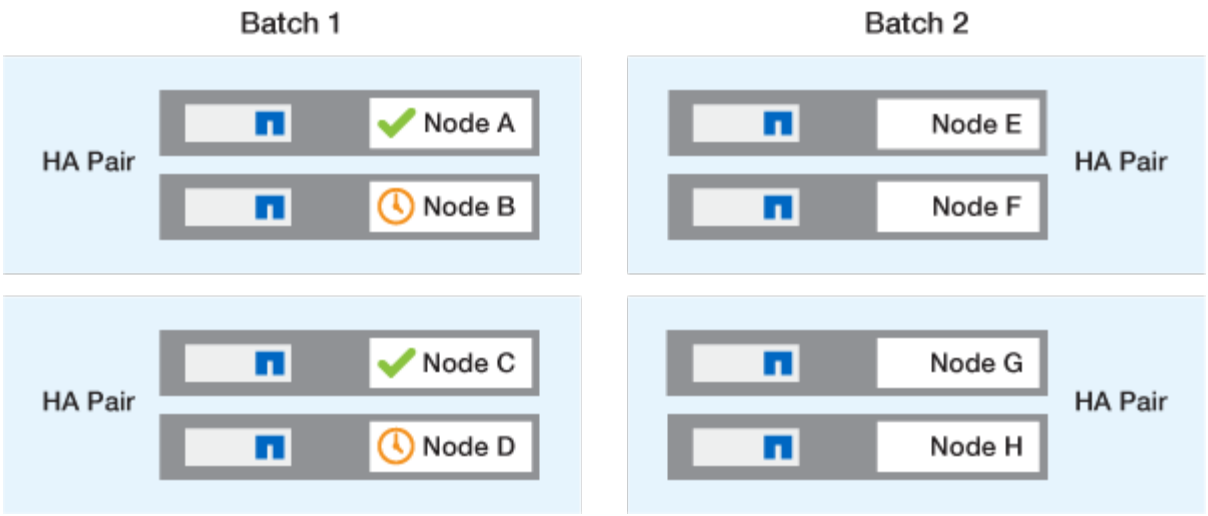
일괄 업그레이드 프로세스는 8개 노드 이상의 클러스터에서 기본값입니다. 일괄 업그레이드 프로세스에서 클러스터는 두 개의 배치로 나뉩니다. 각 배치에는 여러 HA 쌍이 포함됩니다. 첫 번째 일괄 처리에서 각 HA 쌍의 첫 번째 노드는 일괄 처리의 다른 모든 HA 쌍의 첫 번째 노드와 동시에 업그레이드됩니다.

다음 예에서는 각 배치에 2개의 HA 쌍이 있습니다. 일괄 업그레이드가 시작되면 노드 A와 노드 C가 동시에 업그레이드됩니다.



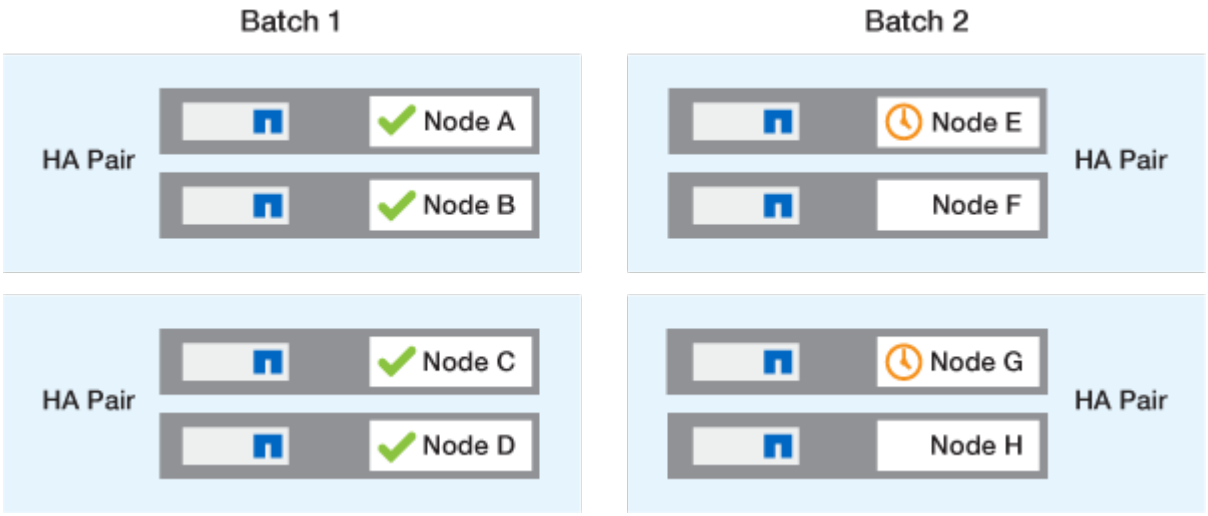
각 HA Pair의 첫 번째 노드 업그레이드가 완료된 후 배치 1의 파트너 노드가 동시에 업그레이드됩니다.

다음 예에서는 노드 A와 노드 C가 업그레이드된 후 노드 B와 노드 D가 동시에 업그레이드됩니다.



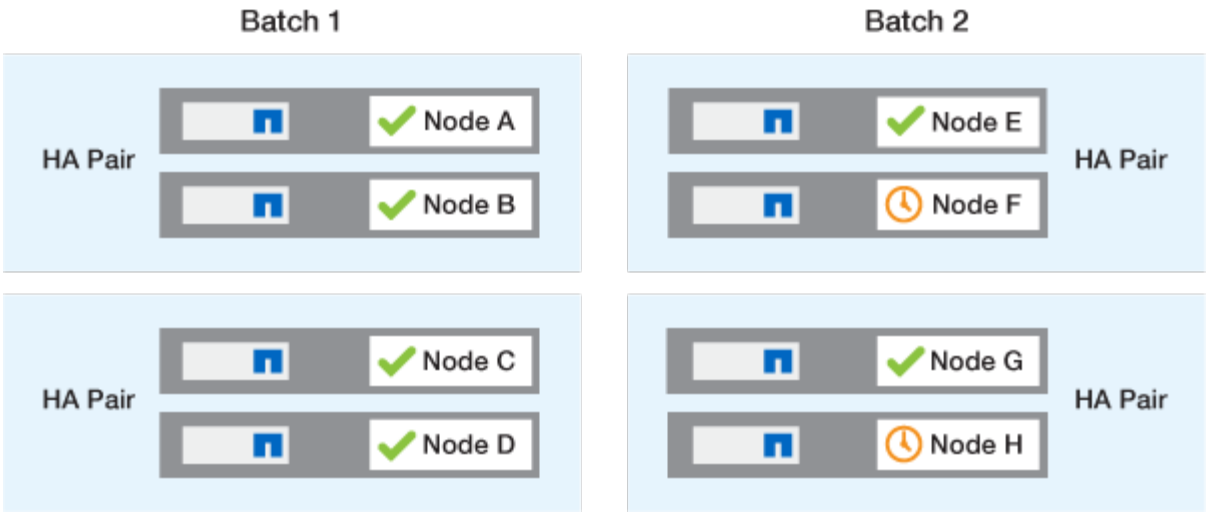
그런 다음 배치 2의 노드에 대해 프로세스가 반복됩니다. 각 HA 쌍의 첫 번째 노드는 일괄 처리 내의 다른 모든 HA 쌍의 첫 번째 노드와 동시에 업그레이드됩니다.

다음 예에서는 노드 E와 노드 G가 동시에 업그레이드됩니다.



각 HA Pair의 첫 번째 노드 업그레이드가 완료된 후 배치 2의 파트너 노드가 동시에 업그레이드됩니다.

다음 예에서는 노드 F와 노드 H를 동시에 업그레이드하여 일괄 업그레이드 프로세스를 완료합니다.



구성에 따라 권장되는 **ONTAP** 업그레이드 방법

구성에서 지원되는 업그레이드 방법은 권장 사용 순서에 따라 나열됩니다.

구성	**ONTAP** 버전입니다	노드 수	권장되는 업그레이드 방법입니다
표준	9.0 이상	2 이상	• System Manager를 사용하여 무중단 자동화 • CLI를 사용하여 무중단 자동화
표준	9.0 이상	단일	"중단 자동화"
MetroCluster	9.3 이상	8	• CLI를 사용하여 무중단 자동화 • CLI를 사용한 4 또는 8노드 MetroCluster의 수동 무중단 운영
MetroCluster	9.3 이상	2,4	• System Manager를 사용하여 무중단 자동화 • CLI를 사용하여 무중단 자동화
MetroCluster	9.2 이하	4, 8	CLI를 사용한 4 또는 8노드 MetroCluster의 수동 무중단 운영
MetroCluster	9.2 이하	2	CLI를 사용한 2노드 MetroCluster의 수동 무중단 운영

System Manager를 사용하는 ANDU는 구성에 관계없이 모든 패치 업그레이드에 권장되는 업그레이드 방법입니다.

A 중단 없는 수동 업그레이드 모든 구성에서 수행할 수 있습니다. 하지만 업그레이드 기간 동안 클러스터를 오프라인으로 전환할 수 없는 경우에는 중단 업그레이드를 수행하지 않아야 합니다. SAN 환경에서 작업 중인 경우 중단 업그레이드를 수행하기 전에 모든 SAN 클라이언트를 종료하거나 일시 중단할 준비를 해야 합니다. ONTAP CLI를 사용하여 시스템 중단을 업그레이드할 수 있습니다.

자동화된 무중단 **ONTAP** 업그레이드로 **ONTAP** 이미지를 설치합니다

자동 업그레이드를 수행하면 ONTAP가 각 노드에 대상 ONTAP 이미지를 자동으로 설치하고 클러스터를 성공적으로 업그레이드할 수 있는지 확인한 다음 중 하나를 실행합니다 일괄 또는 롤링 업그레이드 백그라운드에서 클러스터의 노드 수를 기반으로 합니다.

사용 중인 구성에서 지원되는 경우에는 System Manager를 사용하여 자동화된 업그레이드를 수행해야 합니다. 사용 중인 구성에서 System Manager를 사용한 자동 업그레이드를 지원하지 않는 경우에는 ONTAP CLI(Command Line Interface)를 사용하여 자동화된 업그레이드를 수행할 수 있습니다.

NetApp 통해 ONTAP 9.15.1 이상으로 업그레이드하는 경우 다음을 따르세요."NetApp 콘솔 설명서의 업그레이드 절차" .

자동 무중단 업그레이드(ANDU)를 시작하기 전에 명령 옵션 설정을 수정해도 `storage failover modify-auto-giveback` 업그레이드 프로세스에는 영향을 미치지 않습니다. ANDU 프로세스는 업데이트에 필요한 Takeover/Giveback 중 이 옵션의 사전 설정 값을 무시합니다. 예를 들어, ANDU를 시작하기 전에 false로 설정하면 `-autogiveback` 반환 전에 자동 업그레이드가 중단되지 않습니다. 에 대한 자세한 내용은 `storage failover modify-auto-giveback` "ONTAP 명령 참조입니다"을 참조하십시오.

시작하기 전에

- 당신은 해야 한다 "업그레이드를 준비합니다".
- 당신은 해야 한다 "ONTAP 소프트웨어 이미지 다운로드" 대상 ONTAP 릴리스의 경우

  를 수행하는 경우 "직접 멀티 홉 업그레이드"특정 에 필요한 ONTAP 이미지를 모두 다운로드해야 "업그레이드 경로"합니다.

- 각 HA 쌍에 대해 각 노드에는 동일한 브로드캐스트 도메인에 하나 이상의 포트가 있어야 합니다.

  ONTAP 클러스터에 8개 이상의 노드가 있는 경우, 자동 무중단 업그레이드에 일괄 업그레이드 방법이 사용되므로 SFO 테이크오버 전에 데이터 LIF 마이그레이션을 미리 강제 적용합니다. 일괄 업그레이드 중에 LIF가 마이그레이션되는 방식은 ONTAP 버전에 따라 다릅니다.

ONTAP를 실행하는 경우...	**LIF** 마이그레이션...
• 9.15.1 이상 • 9.14.1P5 • 9.13.1P10 • 2013년 9월 12일 • 9.11.1P16, P17 • 9.10.1P19입니다	다른 배치 그룹의 노드 다른 배치 그룹으로의 마이그레이션에 실패하면 LIF는 같은 배치 그룹에 있는 노드의 HA 파트너로 마이그레이션됩니다.

ONTAP를 실행하는 경우…	**LIF** 마이그레이션…
9.8 ~ 9.14.1	다른 배치 그룹의 노드 네트워크 브로드캐스트 도메인에서 다른 배치 그룹으로의 LIF 마이그레이션을 허용하지 않을 경우 LIF 마이그레이션이 실패하고 ANDU가 일시 중지됩니다.
9.7 이하	업그레이드하는 노드의 HA 파트너에게 적용됩니다. 파트너의 동일한 브로드캐스트 도메인에 포트가 없는 경우 LIF 마이그레이션이 실패하고 ANDU가 일시 중지됩니다.

- MetroCluster FC 구성에서 ONTAP를 업그레이드하려면 클러스터가 비계획 자동 전환을 위해 활성화되어야 합니다.
- 업그레이드 프로세스의 진행 상황을 모니터링할 계획이 없는 경우 를 수행해야 합니다 "수동 개입이 필요할 수 있는 오류에 대한 EMS 알림을 요청합니다".
- 단일 노드 클러스터가 있는 경우 를 따릅니다 "무중단 업그레이드 자동화" 프로세스.

  단일 노드 클러스터의 업그레이드에는 중단이 발생합니다.

예 **3.** 단계

시스템 관리자

1. ONTAP 대상 이미지를 검증합니다.

   MetroCluster 구성을 업그레이드하는 경우 클러스터 A를 검증한 다음 클러스터 B에서 검증 프로세스를 반복해야 합니다

   a. 실행 중인 ONTAP 버전에 따라 다음 단계 중 하나를 수행합니다.

실행 중인 경우…	수행할 작업…
ONTAP 9.8 이상	클러스터 > 개요 * 를 클릭합니다.
ONTAP 9.5, 9.6 및 9.7	구성 * > * 클러스터 * > * 업데이트 * 를 클릭합니다.
ONTAP 9.4 이하	구성 * > * 클러스터 업데이트 * 를 클릭합니다.

   b. 개요 * 창의 오른쪽 모서리에서 를 클릭합니다 ⋮.

   c. ONTAP 업데이트 * 를 클릭합니다.

   d. 클러스터 업데이트 * 탭에서 새 이미지를 추가하거나 사용 가능한 이미지를 선택합니다.

원하는 작업	그러면…
로컬 폴더에서 새 소프트웨어 이미지를 추가합니다 이미 있어야 합니다 "이미지를 다운로드했습니다" 로컬 클라이언트로.	i. Available Software Images * 아래에서 * Add from Local * 을 클릭합니다. ii. 소프트웨어 이미지를 저장한 위치로 이동하여 이미지를 선택한 다음 * 열기 * 를 클릭합니다.
HTTP 또는 FTP 서버에서 새 소프트웨어 이미지를 추가합니다	i. 서버에서 추가 * 를 클릭합니다. ii. 새 소프트웨어 이미지 추가 * 대화 상자에서 NetApp Support 사이트에서 ONTAP 소프트웨어 이미지를 다운로드한 HTTP 또는 FTP 서버의 URL을 입력합니다. 익명 FTP의 경우 에서 URL을 지정해야 합니다 ftp://anonymous@ftpserver 형식. iii. 추가 * 를 클릭합니다.
사용 가능한 이미지를 선택합니다	나열된 이미지 중 하나를 선택합니다.

   e. 업그레이드 전 확인 검사를 실행하려면 * Validate * 를 클릭합니다.

   유효성 검사 중에 오류 또는 경고가 발견되면 시정 조치 목록과 함께 표시됩니다. 업그레이드를 진행하기

전에 모든 오류를 해결해야 합니다. 경고도 해결하는 것이 가장 좋습니다.

2. 다음 * 을 클릭합니다.
3. Update * 를 클릭합니다.

   유효성 검사가 다시 수행됩니다. 남아 있는 오류 또는 경고가 수정 조치 목록과 함께 표시됩니다. 업그레이드를 진행하기 전에 오류를 수정해야 합니다. 유효성 검사가 경고와 함께 완료되면 경고를 수정하거나 * 경고와 함께 업데이트 * 를 선택합니다.

   > 기본적으로 ONTAP는 를 사용하여 "일괄 업그레이드 프로세스"8개 이상의 노드로 클러스터를 업그레이드합니다. ONTAP 9.10.1부터 시작하는 경우 * 한 번에 하나의 HA 쌍 업데이트 * 를 선택하여 기본값을 재정의하고 롤링 업그레이드 프로세스를 통해 클러스터에서 한 번에 하나의 HA 쌍만 업그레이드할 수 있습니다.

   3개 이상의 노드가 있는 MetroCluster 구성의 경우 두 사이트의 HA 쌍에서 ONTAP 업그레이드 프로세스가 동시에 시작됩니다. 2노드 MetroCluster 구성의 경우 업그레이드가 시작되지 않는 사이트에서 업그레이드가 먼저 시작됩니다. 나머지 사이트의 업그레이드는 첫 번째 업그레이드가 완료된 후 시작됩니다.

4. 오류로 인해 업그레이드가 일시 중지되면 오류 메시지를 클릭하여 세부 정보를 확인한 다음 오류를 수정하고 "업그레이드를 재개합니다".

작업을 마친 후

업그레이드가 성공적으로 완료되면 노드가 재부팅되고 System Manager 로그인 페이지로 리디렉션됩니다. 노드가 재부팅되는 데 시간이 오래 걸리면 브라우저를 새로 고쳐야 합니다.

CLI를 참조하십시오

1. ONTAP 대상 소프트웨어 이미지를 검증합니다

   > MetroCluster 구성을 업그레이드하는 경우 먼저 클러스터 A에서 다음 단계를 실행한 다음 클러스터 B에서 동일한 단계를 실행해야 합니다

   a. 이전 ONTAP 소프트웨어 패키지를 삭제합니다.

   ```
   cluster image package delete -version <previous_ONTAP_Version>
   ```

   b. 타겟 ONTAP 소프트웨어 이미지를 클러스터 패키지 저장소에 로드합니다.

   ```
   cluster image package get -url location
   ```

   ```
   cluster1::> cluster image package get -url
   http://www.example.com/software/9.13.1/image.tgz

   Package download completed.
   Package processing completed.
   ```

를 수행하는 경우 "직접 멀티 홉 업그레이드"업그레이드에 필요한 중간 버전의 ONTAP용 소프트웨어 패키지도 로드해야 합니다. 예를 들어 9.8에서 9.13.1로 업그레이드하는 경우 ONTAP 9.12.1용 소프트웨어 패키지를 로드한 다음 같은 명령을 사용하여 9.13.1용 소프트웨어 패키지를 로드해야 합니다.

c. 소프트웨어 패키지를 클러스터 패키지 리포지토리에서 사용할 수 있는지 확인합니다.

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.13.1              MM/DD/YYYY 10:32:15
```

d. 자동화된 업그레이드 사전 검사 실행:

```
cluster image validate -version <package_version_number>
```

를 수행하는 경우 "직접 멀티 홉 업그레이드"확인을 위해 대상 ONTAP 패키지만 사용하면 됩니다. 중간 업그레이드 이미지를 별도로 검증할 필요는 없습니다. 예를 들어 9.8에서 9.13.1로 업그레이드하는 경우 9.13.1 패키지를 검증에 사용하십시오. 9.12.1 패키지를 별도로 검증할 필요는 없습니다.

```
cluster1::> cluster image validate -version 9.13.1

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed...
```

a. 검증 진행 상황 모니터링:

```
cluster image show-update-progress
```

b. 검증에서 식별된 모든 필수 조치를 완료하십시오.

c. MetroCluster 구성을 업그레이드하는 경우 클러스터 B에서 위의 단계를 반복합니다

2. 소프트웨어 업그레이드 예상 생성:

```
cluster image update -version <package_version_number> -estimate
-only
```

MetroCluster 구성을 업그레이드하는 경우 클러스터 A 또는 클러스터 B에서 이 명령을 실행할 수 있습니다 두 클러스터 모두에서 실행할 필요가 없습니다.

소프트웨어 업그레이드 예상에는 업데이트할 각 구성 요소에 대한 세부 정보와 예상 업그레이드 기간이 표시됩니다.

3. 소프트웨어 업그레이드 수행:

```
cluster image update -version <package_version_number>
```

   - 를 수행하는 경우 "직접 멀티 홉 업그레이드"package_version_number 에 대해 대상 ONTAP 버전을 사용합니다. 예를 들어 ONTAP 9.8에서 9.13.1 로 업그레이드하는 경우 package_version_number 로 9.13.1 을 사용합니다.
   - 기본적으로 ONTAP는 를 사용합니다 "일괄 업그레이드 프로세스" 8개 이상의 노드로 클러스터를 업그레이드하려면 원하는 경우 를 사용할 수 있습니다 `-force-rolling` 기본 프로세스를 재정의하고 롤링 업그레이드 프로세스를 사용하여 클러스터에서 한 번에 하나의 노드를 업그레이드하도록 하는 매개 변수입니다.
   - 각각의 테이크오버 및 반환을 완료한 후, 업데이트는 클라이언트 애플리케이션이 테이크오버 및 반환 중에 발생하는 I/O의 일시 중지에서 복구될 수 있도록 8분 동안 대기합니다. 고객 안정화에 필요한 시간이 환경에 더 많이 또는 더 적게 필요한 경우 '-안정화-분' 매개변수를 사용하여 다른 안정화 시간을 지정할 수 있습니다.
   - 4개 노드가 더 많은 MetroCluster 구성의 경우 두 사이트의 HA 쌍에서 동시에 자동화된 업그레이드를 시작합니다. 2노드 MetroCluster 구성의 경우 업그레이드가 시작되지 않는 사이트에서 업그레이드가 시작됩니다. 나머지 사이트의 업그레이드는 첫 번째 업그레이드가 완료된 후 시작됩니다.

```
cluster1::> cluster image update -version 9.13.1

Starting validation for this update. Please wait..

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks...

Pre-update Check      Status     Error-Action
--------------------- ----------
-------------------------------------------
...
20 entries were displayed

Would you like to proceed with update ? {y|n}: y
Starting update...

cluster-1::>
```

4. 클러스터 업데이트 진행률을 표시합니다.

```
cluster image show-update-progress
```

4노드 또는 8노드 MetroCluster 구성을 업그레이드할 경우 'cluster image show-update-progress' 명령은 명령을 실행하는 노드의 진행진만 표시합니다. 개별 노드의 진행률을 보려면 각 노드에서 명령을 실행해야 합니다.

5. 각 노드에서 업그레이드가 성공적으로 완료되었는지 확인합니다.

```
cluster image show-update-progress
```

```
cluster1::> cluster image show-update-progress

                                                 Estimated
Elapsed
Update Phase         Status                       Duration
Duration
-------------------- ----------------- ---------------
---------------
Pre-update checks    completed                    00:10:00
00:02:07
Data ONTAP updates   completed                    01:31:00
01:39:00
Post-update checks   completed                    00:10:00
00:02:00
3 entries were displayed.

Updated nodes: node0, node1.
```

6. AutoSupport 알림 트리거:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

클러스터가 AutoSupport 메시지를 전송하도록 구성되지 않은 경우 알림 복사본이 로컬에 저장됩니다.

7. 2노드 MetroCluster FC 구성을 업그레이드하는 경우 클러스터가 계획되지 않은 자동 스위치오버가 활성화되어 있는지 확인하십시오.

표준 구성, MetroCluster IP 구성 또는 2노드보다 큰 MetroCluster FC 구성을 업그레이드하는 경우 이 단계를 수행할 필요가 없습니다.

a. 예기치 않은 자동 전환이 활성화되어 있는지 확인합니다.

```
metrocluster show
```

자동 비계획 전환이 활성화된 경우 명령 출력에 다음 설명이 표시됩니다.

```
AUSO Failure Domain    auso-on-cluster-disaster
```

a. 명령문이 출력에 표시되지 않으면 예기치 않은 자동 전환을 설정합니다.

```
metrocluster modify -auto-switchover-failure-domain auso-on-
cluster-disaster
```

b. 예기치 않은 자동 전환이 활성화되어 있는지 확인:

```
metrocluster show
```

자동화된 업그레이드 프로세스에서 오류가 발생한 후 **ONTAP** 소프트웨어 업그레이드를 다시 시작합니다

오류로 인해 자동화된 ONTAP 소프트웨어 업그레이드가 일시 중지되면 오류를 해결한 다음 업그레이드를 계속해야 합니다. 오류가 해결되면 자동 업그레이드 프로세스를 계속하거나 수동으로 업그레이드 프로세스를 완료할 수 있습니다. 자동 업그레이드를 계속하도록 선택한 경우 업그레이드 단계를 수동으로 수행하지 마십시오.

예 **4.** 단계

시스템 관리자

1. 실행 중인 ONTAP 버전에 따라 다음 단계 중 하나를 수행합니다.

실행 중인 경우…	그러면…
ONTAP 9.8 이상	클러스터 * > * 개요 * 를 클릭합니다
ONTAP 9.7, 9.6 또는 9.5	구성 * > * 클러스터 * > * 업데이트 * 를 클릭합니다.
ONTAP 9.4 이하	• 구성 * > * 클러스터 업데이트 * 를 클릭합니다. • 개요* 창의 오른쪽 모서리에서 파란색 세로 점 3개를 클릭하고 * ONTAP 업데이트 * 를 선택합니다.

2. 자동 업그레이드를 계속하거나 취소하고 수동으로 계속하십시오.

원하는 작업	그러면…
자동 업그레이드를 다시 시작합니다	Resume * 을 클릭합니다.
자동 업그레이드를 취소하고 수동으로 계속합니다	취소 * 를 클릭합니다.

CLI를 참조하십시오

1. 업그레이드 오류 보기:

```
cluster image show-update-progress
```

2. 오류를 해결합니다.
3. 업그레이드를 다시 시작합니다.

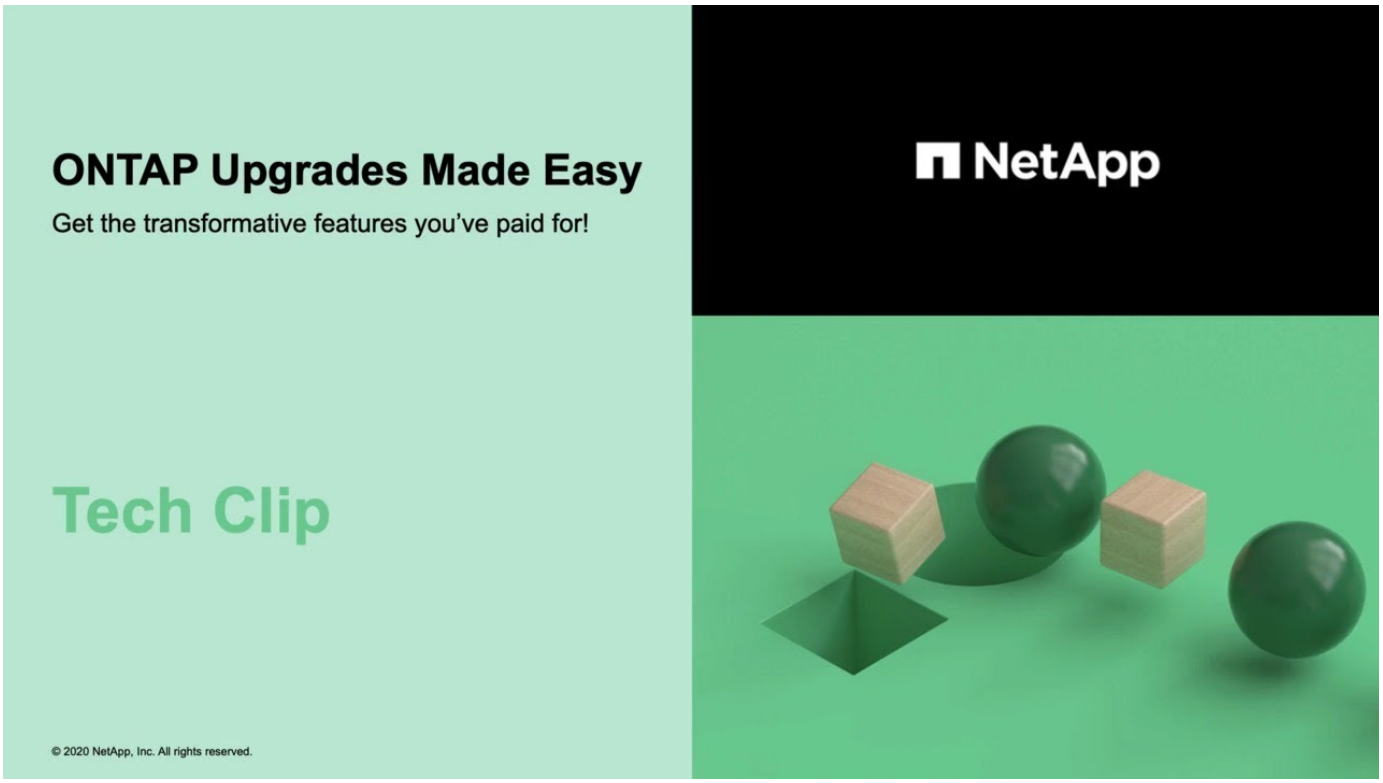
원하는 작업	다음 명령을 입력합니다…
자동 업그레이드를 다시 시작합니다	`cluster image resume-update`
자동 업그레이드를 취소하고 수동으로 계속합니다	`cluster image cancel-update`

작업을 마친 후

"업그레이드 후 검사를 수행합니다".

비디오: 업그레이드가 쉽습니다

ONTAP 9.8에서 System Manager의 간소화된 ONTAP 업그레이드 기능을 살펴보십시오.



관련 정보

- "Active IQ Digital Advisor를 시작합니다"
- "Active IQ 디지털 자문 문서"
- "클러스터 이미지"
- "AutoSupport 호출"
- "MetroCluster"

수동 업그레이드

수동 업그레이드를 위해 **ONTAP** 소프트웨어 패키지를 설치합니다

수동 업그레이드를 위해 ONTAP 소프트웨어 패키지를 다운로드한 후에는 업그레이드를 시작하기 전에 로컬로 설치해야 합니다.

단계

1. "Set-Privilege advanced"라는 메시지가 나타나면 * y * 를 입력하여 권한 수준을 advanced로 설정합니다

   고급 프롬프트('*>')가 나타납니다.

2. 이미지를 설치합니다.

다음과 같은 구성이 있는 경우...	이 명령 사용...
• MetroCluster가 아닙니다 • 2노드 MetroCluster입니다	`system node image update -node * -package <location> -replace -package true -setdefault true -background true` <location> ONTAP 버전에 따라 웹 서버 또는 로컬 폴더일 수 있습니다. 에 대한 자세한 내용은 `system node image update` "ONTAP 명령 참조입니다"을 참조하십시오. 이 명령은 모든 노드에 소프트웨어 이미지를 동시에 설치합니다. 각 노드에 이미지를 한 번에 하나씩 설치하려면 를 지정하지 마십시오 `-background` 매개변수.
• 4노드 MetroCluster입니다 • 8노드 MetroCluster 구성	`system node image update -node * -package <location> -replace -package true -background true -setdefault false` 두 클러스터 모두에서 이 명령을 실행해야 합니다. 이 명령은 확장 쿼리를 사용하여 각 노드에 대체 이미지로 설치된 대상 소프트웨어 이미지를 변경합니다.

3. 메시지가 나타나면 y를 입력하여 계속합니다.
4. 각 노드에 소프트웨어 이미지가 설치되어 있는지 확인합니다.

```
system node image show-update-progress -node *
```

이 명령은 소프트웨어 이미지 설치의 현재 상태를 표시합니다. 모든 노드에서 * 종료 * 의 * 실행 상태 * 와 * 성공 * 의 * 종료 상태 * 가 보고될 때까지 이 명령을 계속 실행해야 합니다.

시스템 노드 이미지 업데이트 명령이 실패하고 오류 또는 경고 메시지가 표시될 수 있습니다. 오류 또는 경고를 해결한 후에는 명령을 다시 실행할 수 있습니다.

이 예에서는 두 노드에 소프트웨어 이미지가 성공적으로 설치된 2노드 클러스터를 보여줍니다.

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

CLI를 사용한 수동 무중단 ONTAP 업그레이드(표준 구성)

System Manager를 사용한 자동 업그레이드가 기본적인 업그레이드 방법입니다. 시스템 관리자가 구성을 지원하지 않는 경우 ONTAP CLI(Command Line Interface)를 사용하여 수동 무중단 업그레이드를 수행할 수 있습니다. 수동 무중단 방법을 사용하여 2개 이상의 노드 클러스터를 업그레이드하려면 HA 쌍의 각 노드에서 페일오버 작업을 시작하고, ""장애 발생" 노드를 업데이트하고, 반환을 시작한 다음 클러스터의 각 HA 쌍에 대해 프로세스를 반복해야 합니다.

시작하기 전에

업그레이드를 만족해야 합니다 "준비" 요구사항.

HA 쌍의 첫 번째 노드 업데이트

노드의 파트너가 테이크오버를 시작하여 HA 쌍의 첫 번째 노드를 업데이트할 수 있습니다. 첫 번째 노드가 업그레이드되는 동안 파트너가 노드의 데이터를 제공합니다.

대규모 업그레이드를 수행하는 경우 업그레이드할 첫 번째 노드는 외부 연결을 위해 데이터 LIF를 구성하고 첫 번째 ONTAP 이미지를 설치한 동일한 노드여야 합니다.

첫 번째 노드를 업그레이드한 후 가능한 한 빨리 파트너 노드를 업그레이드해야 합니다. 두 노드가 에 남아 있지 않도록 하십시오 "혼합 버전" 필요 이상으로 길게 말합니다.

단계

1. AutoSupport 메시지를 호출하여 클러스터의 첫 번째 노드를 업데이트합니다.

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

이 AutoSupport 알림에는 업데이트 직전에 시스템 상태에 대한 기록이 포함됩니다. 업데이트 프로세스에 문제가 있는 경우 유용한 문제 해결 정보를 저장합니다.

클러스터가 AutoSupport 메시지를 전송하도록 구성되지 않은 경우 알림 복사본이 로컬에 저장됩니다.

2. 권한 수준을 advanced로 설정하고 계속할지 묻는 메시지가 표시되면 * y * 를 입력합니다.

```
set -privilege advanced
```

고급 프롬프트('*>')가 나타납니다.

3. 새 ONTAP 소프트웨어 이미지를 기본 이미지로 설정합니다.

```
system image modify {-node nodenameA -iscurrent false} -isdefault true
```

system image modify 명령은 확장 쿼리를 사용하여 새 ONTAP 소프트웨어 이미지(대체 이미지로 설치됨)를 노드의 기본 이미지로 변경합니다.

4. 업데이트 진행 상황 모니터링:

```
system node upgrade-revert show
```

5. 새 ONTAP 소프트웨어 이미지가 기본 이미지로 설정되어 있는지 확인합니다.

```
system image show
```

다음 예제에서 image2는 새 ONTAP 버전이며 Node0에서 기본 이미지로 설정됩니다.

```
cluster1::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version    Date
-------- -------  ------- ------- --------- -------------------
node0
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   true    true    X.X.X     MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

6. 활성화된 경우 파트너 노드에서 자동 반환 비활성화:

```
storage failover modify -node nodenameB -auto-giveback false
```

클러스터가 2노드 클러스터인 경우 자동 반환이 비활성화되면 대체 장애 시나리오에서 관리 클러스터 서비스가 온라인 상태가 되지 않는다는 경고 메시지가 표시됩니다. 계속하려면 y를 입력하십시오.

7. 노드 파트너에 대해 자동 반환이 비활성화되었는지 확인:

```
storage failover show -node nodenameB -fields auto-giveback
```

```
cluster1::> storage failover show -node node1 -fields auto-giveback
node     auto-giveback
-------- -------------
node1    false
1 entry was displayed.
```

8. 다음 명령을 두 번 실행하여 업데이트할 노드가 현재 클라이언트를 제공하고 있는지 확인합니다

```
system node run -node nodenameA -command uptime
```

Uptime 명령은 노드가 마지막 부팅된 이후 NFS, SMB, FC 및 iSCSI 클라이언트에 대해 노드에서 수행한 총 작업 수를 표시합니다. 각 프로토콜에 대해 명령을 두 번 실행하여 작업 수가 증가하는지 여부를 확인해야 합니다. 노드가 증가하면 현재 해당 프로토콜에 대한 클라이언트를 제공하고 있는 것입니다. 증가되지 않는 경우 노드는 현재 해당 프로토콜에 대한 클라이언트를 제공하지 않습니다.

노드가 업데이트된 후 클라이언트 트래픽이 다시 시작되었는지 확인할 수 있도록 클라이언트 작업이 증가하는 각 프로토콜을 기록해 두어야 합니다.

다음 예는 NFS, SMB, FC 및 iSCSI 작업이 있는 노드를 보여줍니다. 하지만 노드는 현재 NFS 및 iSCSI 클라이언트만 제공하고 있습니다.

```
cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

9. 다음 노드에서 모든 데이터 LIF를 마이그레이션:

```
network interface migrate-all -node nodenameA
```

10. 마이그레이션한 LIF 확인:

```
network interface show
```

에서 LIF 상태를 확인하는 데 사용할 수 있는 매개 변수와 에 대해 자세히 `network interface show`"ONTAP 명령 참조입니다" 알아보십시오.

다음 예에서는 Node0의 데이터 LIF가 성공적으로 마이그레이션되었음을 보여 줍니다. 이 예에 포함된 필드를 각 LIF의 홈 노드 및 포트, LIF가 마이그레이션된 현재 노드 및 포트, LIF의 운영 및 관리 상태를 확인할 수 있습니다.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node0 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node0     e0a       node1     e0a       up          up
vs0     data002 node0     e0b       node1     e0b       up          up
vs0     data003 node0     e0b       node1     e0b       up          up
vs0     data004 node0     e0a       node1     e0a       up          up
4 entries were displayed.
```

11. 테이크오버 시작:

```
storage failover takeover -ofnode nodenameA
```

즉시 실행 매개 변수를 지정하지 마십시오. 새 소프트웨어 이미지로 부팅하기 위해 테이크오버가 수행되는 노드에 일반 테이크오버가 필요합니다. LIF를 노드에서 수동으로 마이그레이션하지 않은 경우 서비스 중단이 발생하지 않도록 LIF가 노드의 HA 파트너로 자동으로 마이그레이션됩니다.

첫 번째 노드가 반환 대기 상태로 부팅됩니다.

> AutoSupport가 활성화된 경우 노드가 클러스터 쿼럼을 벗어났음을 나타내는 AutoSupport 메시지가 전송됩니다. 이 알림을 무시하고 업데이트를 진행할 수 있습니다.

12. 테이크오버가 성공했는지 확인:

```
storage failover show
```

버전 불일치와 사서함 형식 문제를 나타내는 오류 메시지가 나타날 수 있습니다. 이는 예상되는 동작으로, 주요 무중단 업그레이드에서 일시적인 상태를 나타내며 유해하지 않습니다.

다음 예제는 Takeover가 성공했음을 보여줍니다. 노드 Node0이 반환 상태를 기다리고 있으며, 해당 파트너가

Takeover 상태에 있습니다.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node0          node1          -        Waiting for giveback (HA
mailboxes)
node1          node0          false    In takeover
2 entries were displayed.
```

13. 다음 조건이 적용될 때까지 8분 이상 기다립니다.
    - 클라이언트 다중 경로(배포된 경우)가 안정화됩니다.
    - 클라이언트는 테이크오버 중에 발생하는 입출력 작업에서 일시 중지로부터 복구됩니다.

      복구 시간은 클라이언트에 따라 다르며 클라이언트 애플리케이션의 특성에 따라 8분 이상 걸릴 수 있습니다.

14. 애그리게이트를 첫 번째 노드에 반환:

```
storage failover giveback -ofnode nodenameA
```

반환 프로그램이 루트 애그리게이트를 파트너 노드로 반환한 다음, 해당 노드에서 부팅을 완료한 후 루트가 아닌 애그리게이트와 자동으로 되돌리도록 설정된 LIF를 반환합니다. 새로 부팅된 노드는 Aggregate가 반환되는 즉시 각 Aggregate의 클라이언트에 데이터를 제공하기 시작합니다.

15. 모든 애그리게이트가 반환되었는지 확인:

```
storage failover show-giveback
```

GiveStatus 필드에 반환할 애그리게이트가 없다고 표시되면 모든 애그리게이트가 반환된 것입니다. Giveback이 거부되면 명령은 반환 진행률을 표시하고 어떤 서브시스템이 Giveback을 거부하는지 표시합니다.

16. 애그리게이트가 반환되지 않은 경우 다음 단계를 수행하십시오.
    a. 거부권을 행사할 수 있는 대안을 검토하여 "받는 사람" 조건을 해결할지 또는 거부권을 무시할지 여부를 결정합니다.
    b. 필요한 경우 오류 메시지에 설명된 "받는 사람" 조건을 해결하여 식별된 작업이 정상적으로 종료되도록 합니다.
    c. 다시 실행 `storage failover giveback` 명령.

       만약 "to" 조건을 무시하기로 결정했다면 -override-vetoes 매개변수를 TRUE로 설정하십시오.

17. 다음 조건이 적용될 때까지 8분 이상 기다립니다.
    - 클라이언트 다중 경로(배포된 경우)가 안정화됩니다.

◦ 클라이언트는 반환 중에 발생하는 I/O 작업의 일시 중지로부터 복구됩니다.

복구 시간은 클라이언트에 따라 다르며 클라이언트 애플리케이션의 특성에 따라 8분 이상 걸릴 수 있습니다.

18. 노드에 대한 업데이트가 성공적으로 완료되었는지 확인합니다.

a. advanced 권한 수준으로 이동합니다.

```
set -privilege advanced
```

b. 노드에 대한 업데이트 상태가 완료되었는지 확인합니다.

```
system node upgrade-revert show -node nodenameA
```

상태는 완료 로 표시되어야 합니다.

상태가 완전하지 않은 경우 기술 지원 부서에 문의하십시오.

a. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

19. 노드의 포트가 작동 중인지 확인합니다.

```
network port show -node nodenameA
```

상위 버전의 ONTAP 9로 업그레이드된 노드에서 이 명령을 실행해야 합니다.

다음 예는 노드의 모든 포트가 작동 중인 것을 보여줍니다.

```
cluster1::> network port show -node node0
                                                                        Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node0
       e0M       Default      -                up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

20. LIF를 노드로 다시 되돌리기:

```
network interface revert *
```

이 명령을 실행하면 노드에서 마이그레이션된 LIF가 반환됩니다.

```
cluster1::> network interface revert *
8 entries were acted on.
```

21. 노드의 데이터 LIF가 노드로 성공적으로 되돌려졌고 노드가 실행 중인지 확인합니다.

```
network interface show
```

다음 예에서는 노드에서 호스팅하는 모든 데이터 LIF가 노드로 다시 되돌려지고 해당 운영 상태가 Up이면 다음을 수행합니다.

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0          e0a
true
            data002      up/up    192.0.2.121/24     node0          e0b
true
            data003      up/up    192.0.2.122/24     node0          e0b
true
            data004      up/up    192.0.2.123/24     node0          e0a
true
4 entries were displayed.
```

22. 이전에 이 노드가 클라이언트를 지원한다고 결정한 경우 노드가 이전에 서비스했던 각 프로토콜에 대해 서비스를 제공하고 있는지 확인합니다.

```
system node run -node nodenameA -command uptime
```

업데이트 중에 작업 수가 0으로 재설정됩니다.

다음 예에서는 업데이트된 노드가 NFS 및 iSCSI 클라이언트 서비스를 재개했음을 보여 줍니다.

```
cluster1::> system node run -node node0 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

23. 이전에 파트너 노드에서 자동 반환을 비활성화한 경우 다시 활성화합니다.

```
storage failover modify -node nodenameB -auto-giveback true
```

노드의 HA 파트너를 최대한 빨리 업데이트해야 합니다. 어떤 이유로든 업데이트 프로세스를 일시 중단해야 하는 경우 HA 쌍의 두 노드에서 동일한 ONTAP 버전을 실행해야 합니다.

HA 쌍에서 파트너 노드를 업데이트 중입니다

HA 쌍의 첫 번째 노드를 업데이트한 후 이를 테이크오버로 시작하여 파트너를 업데이트합니다. 파트너 노드가 업그레이드되는 동안 첫 번째 노드에서 파트너의 데이터를 제공합니다.

1. 권한 수준을 advanced로 설정하고 계속할지 묻는 메시지가 표시되면 * y * 를 입력합니다.

```
set -privilege advanced
```

고급 프롬프트('*>')가 나타납니다.

2. 새 ONTAP 소프트웨어 이미지를 기본 이미지로 설정합니다.

```
system image modify {-node nodenameB -iscurrent false} -isdefault true
```

system image modify 명령은 확장 쿼리를 사용하여 새 ONTAP 소프트웨어 이미지(대체 이미지로 설치됨)를 노드의 기본 이미지로 변경합니다.

3. 업데이트 진행 상황 모니터링:

```
system node upgrade-revert show
```

4. 새 ONTAP 소프트웨어 이미지가 기본 이미지로 설정되어 있는지 확인합니다.

```
system image show
```

다음 예에서 'image2'는 ONTAP의 새 버전이며 노드의 기본 이미지로 설정됩니다.

```
cluster1::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version    Date
-------- -------  ------- ------- --------- -------------------
node0
         image1   false   false   X.X.X     MM/DD/YYYY TIME
         image2   true    true    Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

5. 활성화된 경우 파트너 노드에서 자동 반환 비활성화:

```
storage failover modify -node nodenameA -auto-giveback false
```

클러스터가 2노드 클러스터인 경우 자동 반환이 비활성화되면 대체 장애 시나리오에서 관리 클러스터 서비스가 온라인 상태가 되지 않는다는 경고 메시지가 표시됩니다. 계속하려면 y를 입력하십시오.

6. 파트너 노드에 대해 자동 반환이 비활성화되었는지 확인

```
storage failover show -node nodenameA -fields auto-giveback
```

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node     auto-giveback
-------- -------------
node0    false
1 entry was displayed.
```

7. 다음 명령을 두 번 실행하여 업데이트할 노드가 현재 클라이언트를 제공하고 있는지 확인합니다.

```
system node run -node nodenameB -command uptime
```

Uptime 명령은 노드가 마지막 부팅된 이후 NFS, SMB, FC 및 iSCSI 클라이언트에 대해 노드에서 수행한 총 작업 수를 표시합니다. 각 프로토콜에 대해 명령을 두 번 실행하여 작업 수가 증가하는지 여부를 확인해야 합니다. 노드가 증가하면 현재 해당 프로토콜에 대한 클라이언트를 제공하고 있는 것입니다. 증가되지 않는 경우 노드는 현재 해당 프로토콜에 대한 클라이언트를 제공하지 않습니다.

노드가 업데이트된 후 클라이언트 트래픽이 다시 시작되었는지 확인할 수 있도록 클라이언트 작업이 증가하는 각 프로토콜을 기록해 두어야 합니다.

다음 예는 NFS, SMB, FC 및 iSCSI 작업이 있는 노드를 보여줍니다. 하지만 노드는 현재 NFS 및 iSCSI 클라이언트만 제공하고 있습니다.

```
cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

8. 다음 노드에서 모든 데이터 LIF를 마이그레이션:

```
network interface migrate-all -node nodenameB
```

9. 마이그레이션한 LIF의 상태를 확인합니다.

```
network interface show
```

에서 LIF 상태를 확인하는 데 사용할 수 있는 매개 변수와 에 대해 자세히 `network interface show`"ONTAP 명령 참조입니다" 알아보십시오.

다음 예에서는 node1의 데이터 LIF가 성공적으로 마이그레이션되었음을 보여 줍니다. 이 예에 포함된 필드를 각 LIF의 홈 노드 및 포트, LIF가 마이그레이션된 현재 노드 및 포트, LIF의 운영 및 관리 상태를 확인할 수 있습니다.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node1 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node1     e0a       node0     e0a       up          up
vs0     data002 node1     e0b       node0     e0b       up          up
vs0     data003 node1     e0b       node0     e0b       up          up
vs0     data004 node1     e0a       node0     e0a       up          up
4 entries were displayed.
```

10. 테이크오버 시작:

```
storage failover takeover -ofnode nodenameB -option allow-version-
mismatch
```

즉시 실행 매개 변수를 지정하지 마십시오. 새 소프트웨어 이미지로 부팅하기 위해 테이크오버가 수행되는 노드에 일반 테이크오버가 필요합니다. LIF를 노드에서 수동으로 마이그레이션하지 않은 경우 서비스 중단이 발생하지 않도록 LIF가 노드의 HA 파트너로 자동으로 마이그레이션됩니다.

경고가 표시됩니다. 을 입력해야 합니다 `y` 를 눌러 계속합니다.

페일오버된 노드가 반환 대기 상태로 부팅됩니다.

AutoSupport가 활성화된 경우 노드가 클러스터 쿼럼을 벗어났음을 나타내는 AutoSupport 메시지가 전송됩니다. 이 알림을 무시하고 업데이트를 진행할 수 있습니다.

11. 테이크오버가 성공했는지 확인:

```
storage failover show
```

다음 예제는 Takeover가 성공했음을 보여줍니다. 노드 1이 반환 대기 상태이며 해당 파트너가 Takeover 상태에 있습니다.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node0          node1          -        In takeover
node1          node0          false    Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

12. 다음 조건이 적용될 때까지 8분 이상 기다립니다.
를 누릅니다
    - 클라이언트 다중 경로(배포된 경우)가 안정화됩니다.
    - 테이크오버가 수행되는 동안 입출력이 일시 중지되어 클라이언트가 복구됩니다.

      복구 시간은 클라이언트에 따라 다르며 클라이언트 애플리케이션의 특성에 따라 8분 이상 걸릴 수 있습니다.

13. 파트너 노드에 애그리게이트를 반환합니다.

```
storage failover giveback -ofnode nodenameB
```

    반환 작업은 먼저 루트 애그리게이트를 파트너 노드로 반환한 다음, 해당 노드의 부팅을 완료한 후 루트가 아닌 애그리게이트와 자동으로 되돌리도록 설정된 LIF를 반환합니다. 새로 부팅된 노드는 Aggregate가 반환되는 즉시 각 Aggregate의 클라이언트에 데이터를 제공하기 시작합니다.

14. 모든 애그리게이트가 반환되었는지 확인:

```
storage failover show-giveback
```

    GiveStatus 필드에 반환할 애그리게이트가 없는 경우 모든 애그리게이트가 반환됩니다. Giveback이 거부되면 명령은 반환 진행률을 표시하고 어떤 서브시스템이 반환 작업을 거부하는지 표시합니다.

15. 애그리게이트가 반환되지 않는 경우 다음 단계를 수행하십시오.
    a. 거부권을 행사할 수 있는 대안을 검토하여 "받는 사람" 조건을 해결할지 또는 거부권을 무시할지 여부를 결정합니다.
    b. 필요한 경우 오류 메시지에 설명된 "받는 사람" 조건을 해결하여 식별된 작업이 정상적으로 종료되도록 합니다.
    c. 다시 실행 `storage failover giveback` 명령.

       만약 "to" 조건을 무시하기로 결정했다면 -override-vetoes 매개변수를 TRUE로 설정하십시오.

16. 다음 조건이 적용될 때까지 8분 이상 기다립니다.
    - 클라이언트 다중 경로(배포된 경우)가 안정화됩니다.
    - 클라이언트는 반환 중에 발생하는 I/O 작업의 일시 중지로부터 복구됩니다.

복구 시간은 클라이언트에 따라 다르며 클라이언트 애플리케이션의 특성에 따라 8분 이상 걸릴 수 있습니다.

17. 노드에 대한 업데이트가 성공적으로 완료되었는지 확인합니다.

    a. advanced 권한 수준으로 이동합니다.

    ```
    set -privilege advanced
    ```

    b. 노드에 대한 업데이트 상태가 완료되었는지 확인합니다.

    ```
    system node upgrade-revert show -node nodenameB
    ```

    상태는 완료 로 표시되어야 합니다.

    상태가 Complete가 아닌 경우 노드에서 `system node upgrade-revert upgrade` 명령을 실행합니다. 명령을 실행해도 업데이트가 완료되지 않으면 기술 지원 팀에 문의하십시오.

    a. 관리자 권한 레벨로 돌아갑니다.

    ```
    set -privilege admin
    ```

18. 노드의 포트가 작동 중인지 확인합니다.

    ```
    network port show -node nodenameB
    ```

    ONTAP 9.4로 업그레이드된 노드에서 이 명령을 실행해야 합니다.

    다음 예제는 노드의 모든 데이터 포트가 작동 중인 것을 보여줍니다.

    ```
    cluster1::> network port show -node node1
                                                                  Speed
    (Mbps)
    Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
    ------ --------- ------------ ---------------- ----- -------
    ------------
    node1
           e0M       Default      -                up       1500  auto/100
           e0a       Default      -                up       1500  auto/1000
           e0b       Default      -                up       1500  auto/1000
           e1a       Cluster      Cluster          up       9000  auto/10000
           e1b       Cluster      Cluster          up       9000  auto/10000
    5 entries were displayed.
    ```

에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

19. LIF를 노드로 다시 되돌리기:

```
network interface revert *
```

이 명령을 실행하면 노드에서 마이그레이션된 LIF가 반환됩니다.

```
cluster1::> network interface revert *
8 entries were acted on.
```

20. 노드의 데이터 LIF가 노드로 성공적으로 되돌려졌고 노드가 실행 중인지 확인합니다.

```
network interface show
```

다음 예에서는 노드에서 호스팅하는 모든 데이터 LIF가 노드로 다시 되돌려지고 해당 운영 상태가 Up이면 다음을 수행합니다.

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node1         e0a
true
            data002      up/up    192.0.2.121/24     node1         e0b
true
            data003      up/up    192.0.2.122/24     node1         e0b
true
            data004      up/up    192.0.2.123/24     node1         e0a
true
4 entries were displayed.
```

21. 이전에 이 노드가 클라이언트를 지원한다고 결정한 경우 노드가 이전에 서비스했던 각 프로토콜에 대해 서비스를 제공하고 있는지 확인합니다.

```
system node run -node nodenameB -command uptime
```

업데이트 중에 작업 수가 0으로 재설정됩니다.

다음 예에서는 업데이트된 노드가 NFS 및 iSCSI 클라이언트 서비스를 재개했음을 보여 줍니다.

```
cluster1::> system node run -node node1 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

22. 이 노드가 업데이트할 클러스터의 마지막 노드인 경우 AutoSupport 알림을 트리거합니다.

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

이 AutoSupport 알림에는 업데이트 직전에 시스템 상태에 대한 기록이 포함됩니다. 업데이트 프로세스에 문제가 있는 경우 유용한 문제 해결 정보를 저장합니다.

클러스터가 AutoSupport 메시지를 전송하도록 구성되지 않은 경우 알림 복사본이 로컬에 저장됩니다.

23. 새 ONTAP 소프트웨어가 HA 쌍의 두 노드에서 실행되고 있는지 확인합니다.

```
set -privilege advanced
```

```
system node image show
```

다음 예제에서 image2는 ONTAP의 업데이트된 버전이며 두 노드의 기본 버전입니다.

```
cluster1::*> system node image show
                  Is      Is                Install
Node     Image    Default Current Version    Date
-------- -------  ------- ------- --------- -------------------
node0
         image1   false   false   X.X.X     MM/DD/YYYY TIME
         image2   true    true    Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   false   false   X.X.X     MM/DD/YYYY TIME
         image2   true    true    Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

24. 이전에 파트너 노드에서 자동 반환을 비활성화한 경우 다시 활성화합니다.

```
storage failover modify -node nodenameA -auto-giveback true
```

25. 클러스터가 쿼럼에 있고 를 사용하여 서비스가 실행 중인지 확인합니다 `cluster show` 및 `cluster ring show` (고급 권한 수준) 명령을 사용할 수 있습니다.

추가 HA 쌍을 업그레이드하기 전에 이 단계를 수행해야 합니다.

및 `cluster ring show` 에 대한 자세한 `cluster show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

26. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

27. 추가 HA 쌍을 업그레이드합니다.

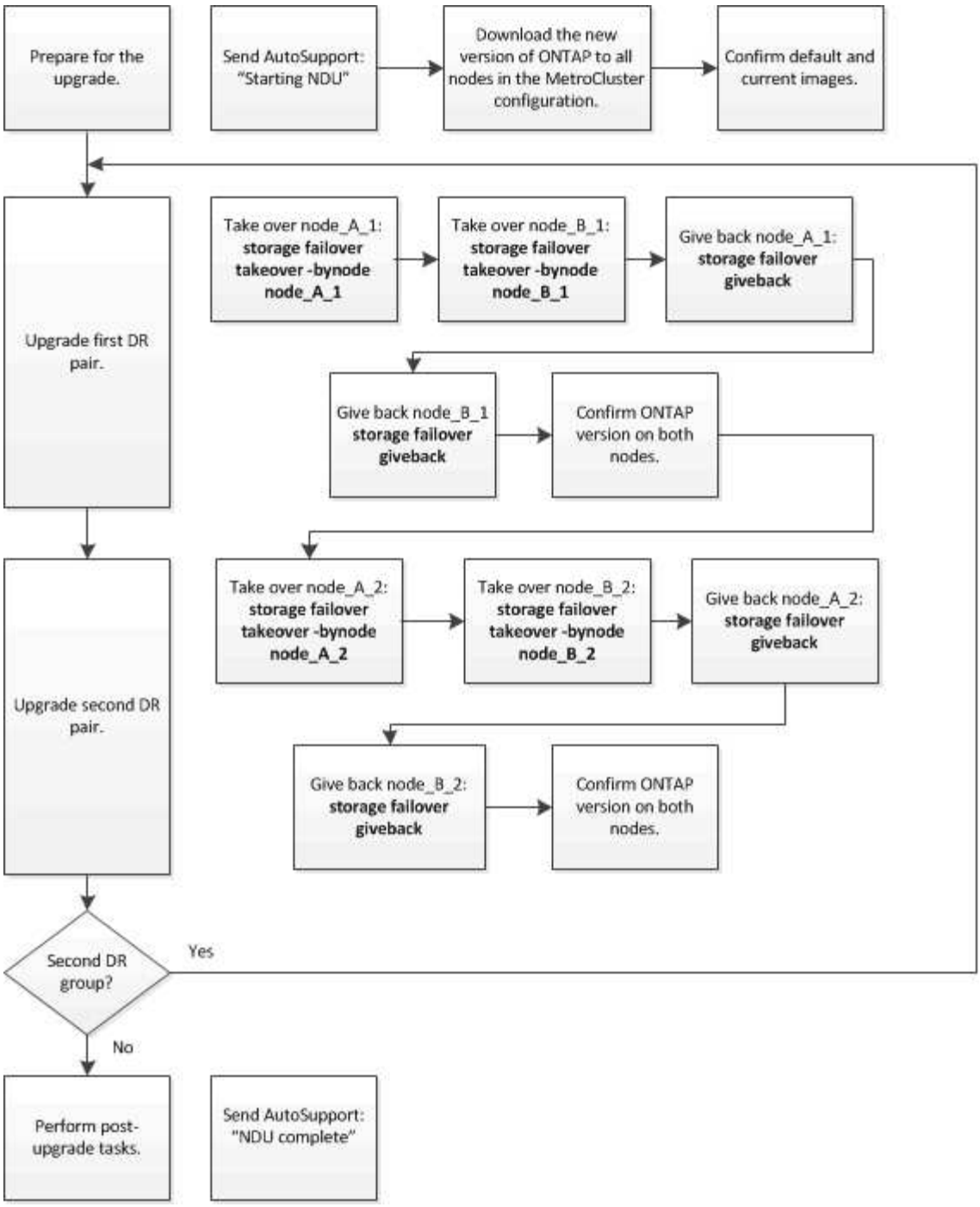
관련 정보

- "AutoSupport 호출"
- "시스템 이미지"
- "시스템 노드"
- "스토리지 페일오버"
- "네트워크 인터페이스"
- "네트워크 포트가 표시됩니다"
- "고급 설정 권한"

CLI를 사용하여 **4** 또는 **8**노드 **MetroCluster** 구성의 무중단 **ONTAP**를 수동으로 업그레이드

4노드 또는 8노드 MetroCluster 구성을 수동으로 업그레이드하려면 업데이트 준비, 1개 또는 2개의 각 DR 그룹에서 동시에 DR 쌍 업데이트, 업그레이드 후 작업 수행이 포함됩니다.

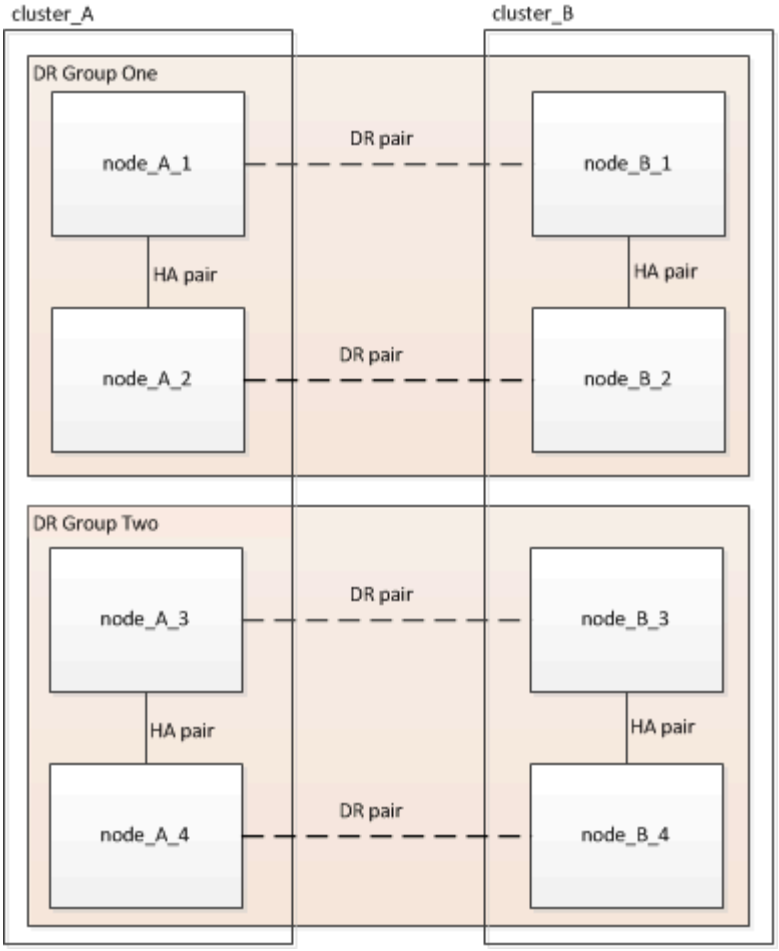
- 이 작업은 다음 구성에 적용됩니다.
  - ONTAP 9.2 이하를 실행하는 4노드 MetroCluster FC 또는 IP 구성
  - ONTAP 버전에 상관없이 8노드 MetroCluster FC 구성
- 2노드 MetroCluster 구성이 있는 경우 이 절차를 사용하지 마십시오.
- 다음 작업은 ONTAP의 이전 버전과 새 버전을 나타냅니다.
  - 업그레이드할 때 이전 버전은 ONTAP의 이전 버전이며, 새 버전의 ONTAP보다 버전 번호가 낮습니다.
  - 다운그레이드할 때 이전 버전은 최신 버전의 ONTAP로, 새 버전의 ONTAP보다 높은 버전 번호가 있습니다.
- 이 작업은 다음과 같은 고급 워크플로를 사용합니다.



8노드 또는 **4**노드 **MetroCluster** 구성에서 **ONTAP** 소프트웨어를 업데이트할 때의 차이점

MetroCluster 소프트웨어 업그레이드 프로세스는 MetroCluster 구성에 8개 또는 4개 노드가 있는지에 따라 다릅니다.

MetroCluster 구성은 1개 또는 2개의 DR 그룹으로 구성됩니다. 각 DR 그룹은 2개의 HA 쌍으로 구성되며, 각 MetroCluster 클러스터에 하나의 HA 쌍이 있습니다. 8노드 MetroCluster에는 2개의 DR 그룹이 포함되어 있습니다.



한 번에 하나의 DR 그룹을 업그레이드합니다.

4노드 **MetroCluster** 구성의 경우**:**

1. DR 그룹 1 업그레이드:
   a. node_A_1 및 node_B_1을 업그레이드합니다.
   b. node_A_2 및 node_B_2를 업그레이드합니다.

8노드 **MetroCluster** 구성의 경우 **DR** 그룹 업그레이드 절차를 두 번 수행합니다**.**

1. DR 그룹 1 업그레이드:
   a. node_A_1 및 node_B_1을 업그레이드합니다.
   b. node_A_2 및 node_B_2를 업그레이드합니다.
2. DR 그룹 2 업그레이드:
   a. node_A_3 및 node_B_3을 업그레이드합니다.
   b. node_A_4 및 node_B_4를 업그레이드합니다.

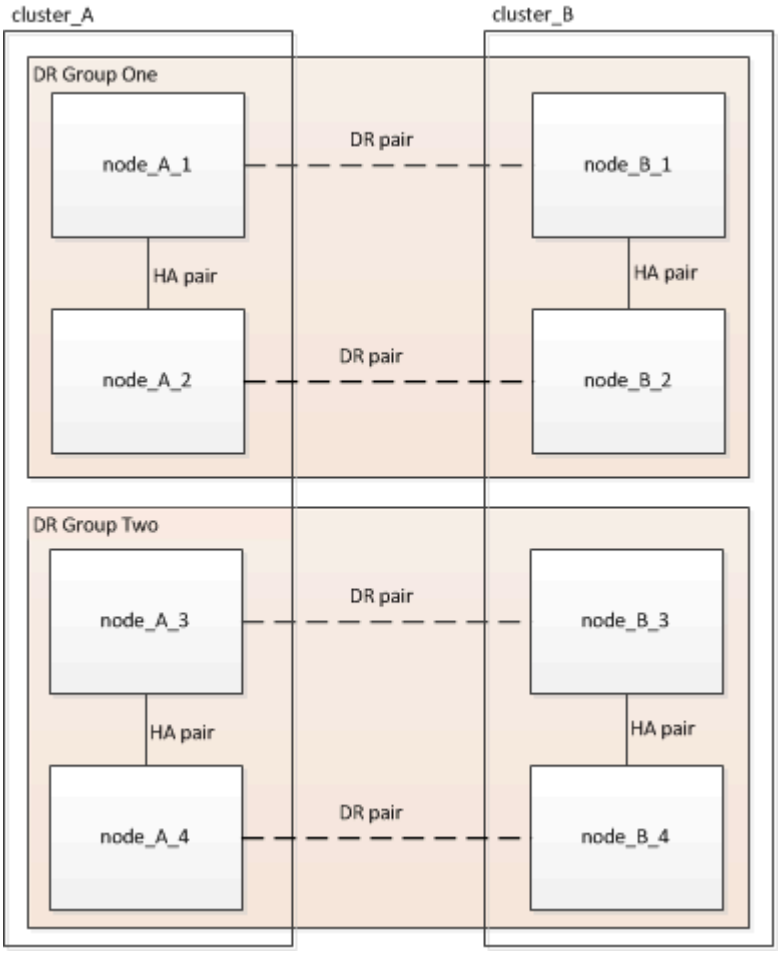
MetroCluster DR 그룹 업그레이드 준비 중

노드에서 ONTAP 소프트웨어를 업그레이드하기 전에 노드 간의 DR 관계를 식별하고 업그레이드를 시작한다는 AutoSupport 메시지를 전송하고 각 노드에서 실행 중인 ONTAP 버전을 확인해야 합니다.

이(가) 있어야 합니다 "다운로드되었습니다" 및 "설치되어 있습니다" 소프트웨어 이미지

이 작업은 각 DR 그룹에서 반복해야 합니다. MetroCluster 구성이 8개 노드로 구성된 경우 2개의 DR 그룹이 있습니다. 따라서 이 작업은 각 DR 그룹에서 반복해야 합니다.

이 작업에 제공된 예제에서는 다음 그림에 표시된 이름을 사용하여 클러스터와 노드를 식별합니다.



1. 구성에서 DR 페어를 식별합니다.

```
metrocluster node show -fields dr-partner
```

```
cluster_A::> metrocluster node show -fields dr-partner
  (metrocluster node show)
dr-group-id cluster     node       dr-partner
----------- -------     --------   ----------
1           cluster_A   node_A_1   node_B_1
1           cluster_A   node_A_2   node_B_2
1           cluster_B   node_B_1   node_A_1
1           cluster_B   node_B_2   node_A_2
4 entries were displayed.

cluster_A::>
```

2. 권한 수준을 admin에서 advanced로 설정하고 계속할지 묻는 메시지가 표시되면 * y * 를 입력합니다.

```
set -privilege advanced
```

고급 프롬프트('*>')가 나타납니다.

3. cluster_A에서 ONTAP 버전을 확인합니다.

```
system image show
```

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- -------   -------------------
node_A_1
         image1   true    true    X.X.X     MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y     MM/DD/YYYY TIME
node_A_2
         image1   true    true    X.X.X     MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

4. cluster_B에서 버전을 확인합니다.

```
system image show
```

```
cluster_B::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- -------     -------------------
node_B_1
         image1   true    true    X.X.X       MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
node_B_2
         image1   true    true    X.X.X       MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.

cluster_B::>
```

5. AutoSupport 알림 트리거:

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

이 AutoSupport 알림에는 업그레이드 전의 시스템 상태 기록이 포함됩니다. 업그레이드 프로세스에 문제가 있는 경우 유용한 문제 해결 정보를 저장합니다.

클러스터가 AutoSupport 메시지를 전송하도록 구성되지 않은 경우 알림 복사본이 로컬에 저장됩니다.

6. 첫 번째 세트의 각 노드에 대해 대상 ONTAP 소프트웨어 이미지를 기본 이미지로 설정합니다.

```
system image modify {-node nodename -iscurrent false} -isdefault true
```

이 명령은 확장 쿼리를 사용하여 대체 이미지로 설치된 대상 소프트웨어 이미지를 노드의 기본 이미지로 변경합니다.

7. cluster_a에서 타겟 ONTAP 소프트웨어 이미지가 기본 이미지로 설정되어 있는지 확인합니다.

```
system image show
```

다음 예제에서 image2는 새 ONTAP 버전이며 첫 번째 집합의 각 노드에서 기본 이미지로 설정됩니다.

```
cluster_A::*> system image show
                  Is      Is               Install
Node     Image    Default Current Version  Date
-------- -------  ------- ------- -------  -------------------
node_A_1
         image1   false   true    X.X.X    MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y    MM/DD/YYYY TIME
node_A_2
         image1   false   true    X.X.X    MM/DD/YYYY TIME
         image2   true   false   Y.Y.Y    MM/DD/YYYY TIME

2 entries were displayed.
```

a. cluster_B에서 타겟 ONTAP 소프트웨어 이미지가 기본 이미지로 설정되어 있는지 확인합니다.

```
system image show
```

다음 예에서는 타겟 버전이 첫 번째 세트의 각 노드에서 기본 이미지로 설정되었음을 보여 줍니다.

```
cluster_B::*> system image show
                  Is      Is               Install
Node     Image    Default Current Version  Date
-------- -------  ------- ------- -------  -------------------
node_A_1
         image1   false   true    X.X.X    MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y    MM/YY/YYYY TIME
node_A_2
         image1   false   true    X.X.X    MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y    MM/DD/YYYY TIME

2 entries were displayed.
```

8. 업그레이드할 노드가 현재 각 노드에 대해 두 번 클라이언트를 제공하는지 확인합니다.

```
system node run -node target-node -command uptime
```

Uptime 명령은 노드가 마지막으로 부팅된 이후 NFS, CIFS, FC 및 iSCSI 클라이언트에 대해 노드에서 수행한 총 작업 수를 표시합니다. 각 프로토콜에 대해 명령을 두 번 실행하여 작업 수가 증가하는지 여부를 확인해야 합니다. 노드가 증가하면 현재 해당 프로토콜에 대한 클라이언트를 제공하고 있는 것입니다. 증가되지 않는 경우 노드는 현재 해당 프로토콜에 대한 클라이언트를 제공하지 않습니다.

노드가 업그레이드된 후 클라이언트 트래픽이 다시 시작되었는지 확인할 수 있도록 클라이언트 작업이 증가하는 각 프로토콜을 기록해 두어야 합니다.

이 예에서는 NFS, CIFS, FC 및 iSCSI 작업이 있는 노드를 보여 줍니다. 하지만 노드는 현재 NFS 및 iSCSI 클라이언트만 제공하고 있습니다.

```
 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

MetroCluster DR 그룹의 첫 번째 **DR** 쌍을 업데이트합니다

새로운 버전의 ONTAP를 노드의 현재 버전으로 만들려면 노드에 대해 테이크오버 및 반환을 올바른 순서로 수행해야 합니다.

모든 노드에서 이전 버전의 ONTAP를 실행해야 합니다.

이 작업에서는 node_A_1 및 node_B_1이 업그레이드됩니다.

첫 번째 DR 그룹에서 ONTAP 소프트웨어를 업그레이드하고 현재 8노드 MetroCluster 구성에서 두 번째 DR 그룹을 업그레이드하는 경우 이 작업에서 node_A_3과 node_B_3을 업데이트합니다.

1. MetroCluster Tiebreaker 소프트웨어가 활성화되면 사용하지 않도록 설정합니다.
2. HA Pair의 각 노드에 대해 자동 반환 비활성화:

   ```
   storage failover modify -node target-node -auto-giveback false
   ```

   이 명령은 HA 쌍의 각 노드에 대해 반복해야 합니다.

3. 자동 반환이 비활성화되었는지 확인:

   ```
   storage failover show -fields auto-giveback
   ```

   이 예제는 두 노드에서 자동 반환이 사용되지 않도록 설정되었음을 보여 줍니다.

```
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
-------- -------------
node_x_1 false
node_x_2 false
2 entries were displayed.
```

4. I/O가 각 컨트롤러에 대해 ~50%를 초과하지 않고 CPU 활용률이 컨트롤러당 ~50%를 초과하지 않는지 확인합니다.
5. cluster_A에서 타겟 노드의 테이크오버 시작:

   즉시 실행 매개 변수를 지정하지 마십시오. 새 소프트웨어 이미지로 부팅하기 위해 테이크오버가 수행되는 노드에 일반 테이크오버가 필요합니다.

   a. cluster_A(node_A_1)에서 DR 파트너 인수:

      ```
      storage failover takeover -ofnode node_A_1
      ```

      노드가 "Waiting for 반환" 상태로 부팅됩니다.

      AutoSupport가 활성화된 경우 노드가 클러스터 쿼럼을 벗어났음을 나타내는 AutoSupport 메시지가 전송됩니다. 이 알림을 무시하고 업그레이드를 진행할 수 있습니다.

   b. 테이크오버가 성공했는지 확인:

      ```
      storage failover show
      ```

      다음 예제는 Takeover가 성공했음을 보여줍니다. node_a_1은 "반환 대기 중" 상태이고 node_a_2는 "인수 중" 상태입니다.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1       node_A_2       -        Waiting for giveback (HA
mailboxes)
node_A_2       node_A_1       false    In takeover
2 entries were displayed.
```

6. cluster_B(node_B_1)에서 DR 파트너를 인수합니다.

   즉시 실행 매개 변수를 지정하지 마십시오. 새 소프트웨어 이미지로 부팅하기 위해 테이크오버가 수행되는 노드에

일반 테이크오버가 필요합니다.

a. node_B_1 인수:

```
storage failover takeover -ofnode node_B_1
```

노드가 "Waiting for 반환" 상태로 부팅됩니다.

AutoSupport가 활성화된 경우 노드가 클러스터 쿼럼을 벗어났음을 나타내는 AutoSupport 메시지가 전송됩니다. 이 알림을 무시하고 업그레이드를 진행할 수 있습니다.

b. 테이크오버가 성공했는지 확인:

```
storage failover show
```

다음 예제는 Takeover가 성공했음을 보여줍니다. node_B_1은 "반환 대기 중" 상태이고 node_B_2는 "인수 중" 상태입니다.

```
 cluster1::> storage failover show
                                Takeover
 Node           Partner        Possible State Description
 -------------- -------------- --------
-------------------------------------
 node_B_1       node_B_2       -        Waiting for giveback (HA
mailboxes)
 node_B_2       node_B_1       false    In takeover
 2 entries were displayed.
```

7. 다음 조건이 충족되도록 8분 이상 기다리십시오.
   - 클라이언트 다중 경로(배포된 경우)가 안정화됩니다.
   - 테이크오버가 수행되는 동안 입출력이 일시 중지되어 클라이언트가 복구됩니다.

   복구 시간은 클라이언트에 따라 다르며 클라이언트 애플리케이션의 특성에 따라 8분 이상 걸릴 수 있습니다.

8. 애그리게이트를 타겟 노드로 반환:

MetroCluster IP 구성을 ONTAP 9.5 이상으로 업그레이드한 후, 애그리게이트는 짧은 기간 동안 성능 저하 상태가 된 후에 재동기화되어 미러링된 상태로 돌아갑니다.

a. cluster_A의 DR 파트너에게 애그리게이트를 반환합니다.

```
storage failover giveback -ofnode node_A_1
```

b. cluster_B의 DR 파트너에게 애그리게이트를 반환합니다.

```
storage failover giveback -ofnode node_B_1
```

반환 작업은 먼저 루트 애그리게이트를 노드로 반환한 다음, 노드가 부팅을 완료한 후 루트가 아닌 애그리게이트를 반환합니다.

9. 두 클러스터에서 다음 명령을 실행하여 모든 애그리게이트가 반환되었는지 확인합니다.

```
storage failover show-giveback
```

GiveStatus 필드에 반환할 애그리게이트가 없다고 표시되면 모든 애그리게이트가 반환된 것입니다. Giveback이 거부되면 명령은 반환 진행률을 표시하고 어떤 서브시스템이 Giveback을 거부하는지 표시합니다.

10. 애그리게이트가 반환되지 않은 경우 다음을 수행합니다.
    a. 거부권을 행사할 수 있는 대안을 검토하여 "받는 사람" 조건을 해결할지 또는 거부권을 무시할지 여부를 결정합니다.
    b. 필요한 경우 오류 메시지에 설명된 "받는 사람" 조건을 해결하여 식별된 작업이 정상적으로 종료되도록 합니다.
    c. 스토리지 페일오버 반환 명령을 다시 입력합니다.

    만약 "to" 조건을 무시하기로 결정했다면 -override-vetoes 매개변수를 TRUE로 설정하십시오.

11. 다음 조건이 충족되도록 8분 이상 기다리십시오.
    - 클라이언트 다중 경로(배포된 경우)가 안정화됩니다.
    - 클라이언트는 반환 중에 발생하는 I/O의 일시 중지로부터 복구됩니다.

    복구 시간은 클라이언트에 따라 다르며 클라이언트 애플리케이션의 특성에 따라 8분 이상 걸릴 수 있습니다.

12. 권한 수준을 admin에서 advanced로 설정하고 계속할지 묻는 메시지가 표시되면 * y * 를 입력합니다.

```
set -privilege advanced
```

고급 프롬프트('*>')가 나타납니다.

13. cluster_A에서 버전을 확인합니다.

```
system image show
```

다음 예제는 System image2가 node_A_1의 기본 버전과 현재 버전임을 보여 줍니다.

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- --------- ------------------
node_A_1
         image1   false   false    X.X.X    MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y    MM/DD/YYYY TIME
node_A_2
         image1   false   true     X.X.X    MM/DD/YYYY TIME
         image2   true    false    Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

14. cluster_B에서 버전을 확인합니다.

```
system image show
```

다음 예제는 system image2(ONTAP 9.0.0)가 node_A_1의 기본 및 현재 버전임을 보여 줍니다.

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- --------- -------------------
node_B_1
         image1   false   false    X.X.X    MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y    MM/DD/YYYY TIME
node_B_2
         image1   false   true     X.X.X    MM/DD/YYYY TIME
         image2   true    false    Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

MetroCluster DR 그룹의 두 번째 **DR** 쌍을 업데이트합니다

새 버전의 ONTAP를 노드의 현재 버전으로 만들려면 노드에 대해 테이크오버 및 반환을 올바른 순서로 수행해야 합니다.

첫 번째 DR 쌍(node_A_1 및 node_B_1)을 업그레이드해야 합니다.

이 작업에서는 node_A_2와 node_B_2가 업그레이드됩니다.

첫 번째 DR 그룹에서 ONTAP 소프트웨어를 업그레이드하고 현재 8노드 MetroCluster 구성에서 두 번째 DR 그룹을

업데이트하는 경우 이 작업에서 node_A_4 및 node_B_4를 업데이트합니다.

1. 다음 노드에서 모든 데이터 LIF를 마이그레이션:

```
network interface migrate-all -node nodenameA
```

2. cluster_A에서 타겟 노드의 테이크오버 시작:

   즉시 실행 매개 변수를 지정하지 마십시오. 새 소프트웨어 이미지로 부팅하기 위해 테이크오버가 수행되는 노드에 일반 테이크오버가 필요합니다.

   a. cluster_A에서 DR 파트너를 인수합니다.

```
storage failover takeover -ofnode node_A_2 -option allow-version-
mismatch
```

   ONTAP 9.0에서 ONTAP 9.1 또는 패치 업그레이드에는 "버전 불일치 허용" 옵션이 필요하지 않습니다.

   노드가 "Waiting for 반환" 상태로 부팅됩니다.

   AutoSupport가 활성화된 경우 노드가 클러스터 쿼럼을 벗어났음을 나타내는 AutoSupport 메시지가 전송됩니다. 이 알림을 무시하고 업그레이드를 진행할 수 있습니다.

   b. 테이크오버가 성공했는지 확인:

```
storage failover show
```

   다음 예제는 Takeover가 성공했음을 보여줍니다. node_a_2가 "반환 대기 중" 상태이고 node_a_1이 "인수 중" 상태입니다.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1       node_A_2       false    In takeover
node_A_2       node_A_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

3. cluster_B에서 타겟 노드의 테이크오버 시작:

   즉시 실행 매개 변수를 지정하지 마십시오. 새 소프트웨어 이미지로 부팅하기 위해 테이크오버가 수행되는 노드에

일반 테이크오버가 필요합니다.

a. cluster_B(node_B_2)에서 DR 파트너를 인수합니다.

에서 업그레이드하는 경우...	이 명령을 입력하십시오...
ONTAP 9.2 또는 ONTAP 9.1	`storage failover takeover -ofnode node_B_2`
ONTAP 9.0 또는 Data ONTAP 8.3.x	`storage failover takeover -ofnode node_B_2 -option allow-version-mismatch` ONTAP 9.0에서 ONTAP 9.1 또는 패치 업그레이드에는 "버전 불일치 허용" 옵션이 필요하지 않습니다.

노드가 "Waiting for 반환" 상태로 부팅됩니다.

AutoSupport가 활성화된 경우 노드가 클러스터 쿼럼을 벗어났음을 나타내는 AutoSupport 메시지가 전송됩니다. 이 알림을 무시해도 되고 업그레이드를 진행할 수 있습니다.

b. 테이크오버가 성공했는지 확인:

```
storage failover show
```

다음 예제는 Takeover가 성공했음을 보여줍니다. node_B_2가 "반환 대기 중" 상태이고 node_B_1이 "인수 중" 상태입니다.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_B_1       node_B_2       false    In takeover
node_B_2       node_B_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

4. 다음 조건이 충족되도록 8분 이상 기다리십시오.
   - 클라이언트 다중 경로(배포된 경우)가 안정화됩니다.

◦ 테이크오버가 수행되는 동안 입출력이 일시 중지되어 클라이언트가 복구됩니다.

복구 시간은 클라이언트에 따라 다르며 클라이언트 애플리케이션의 특성에 따라 8분 이상 걸릴 수 있습니다.

5. 애그리게이트를 타겟 노드로 반환:

MetroCluster IP 구성을 ONTAP 9.5로 업그레이드한 후 재동기화하여 미러링된 상태로 되돌리기 전에 잠시 동안 애그리게이트가 성능 저하 상태가 됩니다.

a. cluster_A의 DR 파트너에게 애그리게이트를 반환합니다.

```
storage failover giveback -ofnode node_A_2
```

b. cluster_B의 DR 파트너에게 애그리게이트를 반환합니다.

```
storage failover giveback -ofnode node_B_2
```

반환 작업은 먼저 루트 애그리게이트를 노드로 반환한 다음, 노드가 부팅을 완료한 후 루트가 아닌 애그리게이트를 반환합니다.

6. 두 클러스터에서 다음 명령을 실행하여 모든 애그리게이트가 반환되었는지 확인합니다.

```
storage failover show-giveback
```

GiveStatus 필드에 반환할 애그리게이트가 없다고 표시되면 모든 애그리게이트가 반환된 것입니다. Giveback이 거부되면 명령은 반환 진행률을 표시하고 어떤 서브시스템이 Giveback을 거부하는지 표시합니다.

7. 애그리게이트가 반환되지 않은 경우 다음을 수행합니다.

a. 거부권을 행사할 수 있는 대안을 검토하여 "받는 사람" 조건을 해결할지 또는 거부권을 무시할지 여부를 결정합니다.

b. 필요한 경우 오류 메시지에 설명된 "받는 사람" 조건을 해결하여 식별된 작업이 정상적으로 종료되도록 합니다.

c. 스토리지 페일오버 반환 명령을 다시 입력합니다.

만약 "to" 조건을 무시하기로 결정했다면 -override-vetoes 매개변수를 TRUE로 설정하십시오.

8. 다음 조건이 충족되도록 8분 이상 기다리십시오.

◦ 클라이언트 다중 경로(배포된 경우)가 안정화됩니다.

◦ 클라이언트는 반환 중에 발생하는 I/O의 일시 중지로부터 복구됩니다.

복구 시간은 클라이언트에 따라 다르며 클라이언트 애플리케이션의 특성에 따라 8분 이상 걸릴 수 있습니다.

9. 권한 수준을 admin에서 advanced로 설정하고 계속할지 묻는 메시지가 표시되면 * y * 를 입력합니다.

```
set -privilege advanced
```

고급 프롬프트('*>')가 나타납니다.

10. cluster_A에서 버전을 확인합니다.

```
system image show
```

다음 예제는 system image2(대상 ONTAP 이미지)가 node_A_2의 기본 버전과 현재 버전임을 보여 줍니다.

```
cluster_B::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- ----------- -------------------
node_A_1
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
node_A_2
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

11. cluster_B에서 버전을 확인합니다.

```
system image show
```

다음 예제는 system image2(대상 ONTAP 이미지)가 node_B_2의 기본 버전과 현재 버전임을 보여 줍니다.

```
cluster_B::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- ----------  -------------------
node_B_1
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
node_B_2
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

12. HA 쌍의 각 노드에 대해 자동 반환을 활성화합니다.

```
storage failover modify -node target-node -auto-giveback true
```

이 명령은 HA 쌍의 각 노드에 대해 반복해야 합니다.

13. 자동 반환이 활성화되었는지 확인:

```
storage failover show -fields auto-giveback
```

이 예에서는 두 노드에서 자동 반환이 설정되었음을 보여 줍니다.

```
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
-------- -------------
node_x_1 true
node_x_2 true
2 entries were displayed.
```

관련 정보

- "스토리지 장애 조치 포기"
- "스토리지 장애 조치 수정"
- "스토리지 장애 조치 쇼-기브백"
- "스토리지 장애 조치 인수"

2노드 MetroCluster 구성을 업그레이드하는 방법은 ONTAP 버전에 따라 다릅니다. ONTAP 9.2 이전 버전을 실행 중인 경우 이 절차를 사용하여 협상된 전환 시작, ""장애" 사이트에서 클러스터 업데이트, 스위치백 시작, 다른 사이트에서 클러스터 프로세스 반복 등을 포함하여 수동 무중단 업그레이드를 수행해야 합니다.

ONTAP 9.3 이상을 실행하는 2노드 MetroCluster 구성이 있는 경우 을 수행합니다 System Manager를 사용한 자동 업그레이드.

단계

1. 권한 수준을 advanced로 설정하고 계속할지 묻는 메시지가 표시되면 * y * 를 입력합니다.

```
set -privilege advanced
```

고급 프롬프트('*>')가 나타납니다.

2. 업그레이드할 클러스터에서 새 ONTAP 소프트웨어 이미지를 기본값으로 설치합니다.

```
system node image update -package package_location -setdefault true
-replace-package true
```

```
cluster_B::*> system node image update -package
http://www.example.com/NewImage.tgz -setdefault true -replace-package
true
```

3. 대상 소프트웨어 이미지가 기본 이미지로 설정되어 있는지 확인합니다.

```
system node image show
```

다음 예에서는 "NewImage"가 기본 이미지로 설정되어 있음을 보여 줍니다.

```
cluster_B::*> system node image show
                     Is      Is                            Install
Node     Image       Default Current Version               Date
-------- -------     ------- ------- --------------------
-------------------
node_B_1
         OldImage  false   true    X.X.X                 MM/DD/YYYY TIME
         NewImage  true    false   Y.Y.Y                 MM/DD/YYYY TIME
2 entries were displayed.
```

4. 대상 소프트웨어 이미지가 기본 이미지로 설정되어 있지 않으면 다음과 같이 변경합니다.

```
system image modify {-node * -iscurrent false} -isdefault true
```

5. 모든 클러스터 SVM이 상태 상태인지 확인:

```
metrocluster vserver show
```

6. 업데이트되지 않는 클러스터에서 협상된 전환을 시작합니다.

```
metrocluster switchover
```

이 작업은 몇 분 정도 걸릴 수 있습니다. MetroCluster operation show 명령을 사용하여 전환이 완료되었는지 확인할 수 있습니다.

다음 예에서는 원격 클러스터(""cluster_a"")에서 협상된 전환이 수행됩니다. 이로 인해 로컬 클러스터 ("cluster_B")가 중지되어 업데이트할 수 있습니다.

```
cluster_A::> metrocluster switchover

Warning: negotiated switchover is about to start. It will stop all the
data
         Vservers on cluster "cluster_B" and
         automatically re-start them on cluster
         "cluster_A". It will finally gracefully shutdown
         cluster "cluster_B".
Do you want to continue? {y|n}: y
```

7. 모든 클러스터 SVM이 상태 상태인지 확인:

```
metrocluster vserver show
```

8. "surviving" 클러스터의 데이터 집계를 재동기화합니다.

```
metrocluster heal -phase aggregates
```

MetroCluster IP 구성을 ONTAP 9.5 이상으로 업그레이드한 후, 애그리게이트는 짧은 기간 동안 성능 저하 상태가 된 후에 재동기화되어 미러링된 상태로 돌아갑니다.

```
cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

9. 복구 작업이 성공적으로 완료되었는지 확인합니다.

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

10. "surviving" 클러스터의 루트 집계를 재동기화합니다.

```
metrocluster heal -phase root-aggregates
```

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

11. 복구 작업이 성공적으로 완료되었는지 확인합니다.

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. 중지된 클러스터에서 LOADER 프롬프트에서 노드를 부팅합니다.

```
boot_ontap
```

13. 부팅 프로세스가 완료될 때까지 기다린 다음 모든 클러스터 SVM이 상태 상태인지 확인합니다.

```
metrocluster vserver show
```

14. "surviving" 클러스터에서 스위치백을 수행합니다.

```
metrocluster switchback
```

15. 스위치백이 성공적으로 완료되었는지 확인합니다.

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. 모든 클러스터 SVM이 상태 상태인지 확인:

```
metrocluster vserver show
```

17. 다른 클러스터에서 이전 단계를 모두 반복합니다.
18. MetroCluster 구성이 정상인지 확인합니다.
    a. 구성을 확인합니다.

```
metrocluster check run
```

```
cluster_A::> metrocluster check run
Last Checked On: MM/DD/YYYY TIME
Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

b. 보다 자세한 결과를 보려면 MetroCluster check run 명령을 사용하십시오.

```
metrocluster check aggregate show
```

```
metrocluster check config-replication show
```

```
metrocluster check lif show
```

```
metrocluster check node show
```

c. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

d. 스위치오버 작업 시뮬레이션:

```
metrocluster switchover -simulate
```

e. 전환 시뮬레이션 결과를 검토합니다.

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
    Operation: switchover
        State: successful
   Start time: MM/DD/YYYY TIME
     End time: MM/DD/YYYY TIME
       Errors: -
```

f. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

g. 다른 클러스터에서 이러한 하위 단계를 반복합니다.

작업을 마친 후

아무 작업도 수행합니다 "업그레이드 후 작업".

관련 정보

"MetroCluster 재해 복구"

CLI를 사용한 수동 Disruptive ONTAP 업그레이드

클러스터를 오프라인으로 전환하여 새 ONTAP 릴리즈로 업그레이드할 수 있는 경우 중단이 필요한 업그레이드 방법을 사용할 수 있습니다. 이 방법에는 여러 단계가 있습니다. 즉, 각 HA 쌍에 대해 스토리지 페일오버를 사용하지 않도록 설정하고, 클러스터의 각 노드를 재부팅한 다음 스토리지 페일오버를 다시 사용하도록 설정합니다.

- 반드시 해야 합니다 "다운로드" 및 "설치합니다" 소프트웨어 이미지
- SAN 환경에서 작업 중인 경우 업그레이드가 완료될 때까지 모든 SAN 클라이언트를 종료하거나 일시 중지해야 합니다.

  중단 업그레이드 전에 SAN 클라이언트가 종료되거나 일시 중지되지 않으면 클라이언트 파일 시스템 및 애플리케이션은 업그레이드가 완료된 후 수동 복구가 필요할 수 있는 오류가 발생합니다.

각 HA Pair에 대해 스토리지 페일오버가 사용되지 않고 각 노드가 업데이트되므로 중단 업그레이드에는 다운타임이 필요합니다. 스토리지 페일오버가 비활성화되면 각 노드는 단일 노드 클러스터로 작동합니다. 즉, 시스템이 재부팅되는 동안 노드와 연결된 시스템 서비스가 중단됩니다.

단계

1. 권한 수준을 admin에서 advanced로 설정하고 계속할지 묻는 메시지가 표시되면 * y * 를 입력합니다.

```
set -privilege advanced
```

고급 프롬프트('*>')가 나타납니다.

2. 새 ONTAP 소프트웨어 이미지를 기본 이미지로 설정합니다.

```
system image modify {-node * -iscurrent false} -isdefault true
```

이 명령은 확장 쿼리를 사용하여 대상 ONTAP 소프트웨어 이미지(대체 이미지로 설치됨)를 각 노드의 기본 이미지로 변경합니다.

3. 새 ONTAP 소프트웨어 이미지가 기본 이미지로 설정되어 있는지 확인합니다.

```
system image show
```

다음 예에서는 이미지 2가 새로운 ONTAP 버전이며 두 노드에서 기본 이미지로 설정됩니다.

```
cluster1::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version    Date
-------- -------  ------- ------- --------- -------------------
node0
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

4. 다음 단계 중 하나를 수행합니다.

클러스터가 다음으로 구성된 경우:	수행할 작업...
1개 노드	다음 단계를 계속 진행합니다.

클러스터가 다음으로 구성된 경우:	수행할 작업...

2개 노드	a. 클러스터 고가용성 비활성화:
	`cluster ha modify -configured false`
	메시지가 나타나면 y를 입력하여 계속합니다.
	b. HA 쌍에 대해 스토리지 페일오버 비활성화:
	`storage failover modify -node * -enabled false`

2개 이상의 노드	클러스터의 각 HA 쌍에 대해 스토리지 페일오버 비활성화: `storage failover modify -node * -enabled false`

5. 클러스터의 노드 재부팅:

```
system node reboot -node nodename -ignore-quorum-warnings
```

ⓘ 한 번에 둘 이상의 노드를 재부팅하지 마십시오.

노드가 새 ONTAP 이미지를 부팅합니다. 재부팅 프로세스가 완료되었음을 나타내는 ONTAP 로그인 프롬프트가 나타납니다.

6. 노드 또는 노드 세트가 새 ONTAP 이미지로 재부팅된 후 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

계속하라는 메시지가 나타나면 * y * 를 입력합니다

7. 새 소프트웨어가 실행 중인지 확인합니다.

```
system node image show
```

다음 예제에서 image1은 새 ONTAP 버전이며 Node0에서 현재 버전으로 설정됩니다.

```
cluster1::*> system node image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   true    true    X.X.X        MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
node1
         image1   true    false   X.X.X       MM/DD/YYYY TIME
         image2   false   true    Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.
```

8. 업그레이드가 성공적으로 완료되었는지 확인합니다.

   a. 권한 수준을 고급으로 설정합니다.

   ```
   set -privilege advanced
   ```

   b. 각 노드에 대한 업그레이드 상태가 완료되었는지 확인합니다.

   ```
   system node upgrade-revert show -node nodename
   ```

   상태는 완료 로 표시되어야 합니다.

   상태가 완료되지 않은 "NetApp 지원에 문의하십시오"경우 즉시 를 선택합니다.

   a. 관리자 권한 레벨로 돌아갑니다.

   ```
   set -privilege admin
   ```

9. 각 추가 노드에 대해 5단계부터 8단계까지 반복합니다.
10. 클러스터가 두 개 이상의 노드로 구성된 경우 클러스터의 각 HA 쌍에 대해 스토리지 페일오버를 사용하도록 설정합니다.

```
storage failover modify -node * -enabled true
```

11. 클러스터가 두 노드로만 구성된 경우 클러스터 고가용성을 설정합니다.

```
cluster ha modify -configured true
```

관련 정보

- "스토리지 장애 조치 수정"

ONTAP 업그레이드 후 수행할 작업

ONTAP 업그레이드 후 수행할 작업

ONTAP를 업그레이드한 후 클러스터 준비 상태를 확인하기 위해 수행해야 하는 몇 가지 작업이 있습니다.

1. "클러스터를 확인합니다".

   ONTAP를 업그레이드한 후에는 클러스터 버전, 클러스터 상태 및 스토리지 상태를 확인해야 합니다. MetroCluster FC 구성을 사용하는 경우 비계획 자동 스위치오버가 활성화되어 있는지도 확인해야 합니다.

2. "모든 LIF가 홈 포트에 있는지 확인합니다".

   재부팅 중 일부 LIF는 할당된 페일오버 포트로 마이그레이션되었을 수 있습니다. 클러스터를 업그레이드한 후에는 홈 포트에 없는 모든 LIF를 설정 및 되돌려야 합니다.

3. 확인합니다 "특별 고려 사항" 클러스터에 따라 다릅니다.

   클러스터에 특정 구성이 있는 경우 업그레이드 후 추가 단계를 수행해야 할 수 있습니다.

4. "DQP(Disk Qualification Package) 업데이트".

   DQP는 ONTAP 업그레이드의 일부로 업데이트되지 않습니다.

ONTAP 업그레이드 후 클러스터를 확인합니다

ONTAP를 업그레이드한 후 클러스터 버전, 클러스터 상태 및 스토리지 상태를 확인합니다. 또한 MetroCluster FC 구성의 경우 클러스터가 계획되지 않은 자동 스위치오버가 활성화되어 있는지 확인하십시오.

클러스터 버전을 확인합니다

모든 HA 쌍이 업그레이드된 후에는 version 명령을 사용하여 모든 노드가 타겟 릴리즈를 실행 중인지 확인해야 합니다.

클러스터 버전은 클러스터의 모든 노드에서 실행되는 ONTAP의 가장 낮은 버전입니다. 클러스터 버전이 타겟 ONTAP 릴리즈가 아닌 경우 클러스터를 업그레이드할 수 있습니다.

1. 고급 권한 레벨로 변경:

   ```
   set -privilege advanced
   ```

2. 클러스터 버전이 타겟 ONTAP 릴리즈인지 확인합니다.

```
system node image show -version
```

3. 클러스터 버전이 타겟 ONTAP 릴리즈가 아닌 경우 모든 노드의 업그레이드 상태를 확인해야 합니다.

```
system node upgrade-revert show
```

클러스터 상태를 확인합니다

클러스터를 업그레이드한 후 노드가 정상 상태이며 클러스터에 참여할 수 있고 클러스터가 쿼럼에 있는지 확인해야 합니다.

1. 클러스터의 노드가 온라인 상태이며 클러스터에 참여할 자격이 있는지 확인합니다.

```
cluster show
```

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

노드가 정상 상태가 아니거나 적합하지 않은 경우 EMS 로그에서 오류를 확인하고 수정 조치를 취합니다.

2. 각 RDB 프로세스에 대한 구성 세부 정보를 확인합니다.
   - 관계형 데이터베이스 epoch 및 데이터베이스 epoch는 각 노드에 대해 일치해야 합니다.
   - 링당 쿼럼 마스터는 모든 노드에 대해 동일해야 합니다.

     각 링에는 다른 쿼럼 마스터가 있을 수 있습니다.

이 RDB 프로세스를 표시하려면…	이 명령을 입력하십시오…
기능과	클러스터 링 쇼-unitname 관리
볼륨 위치 데이터베이스	클러스터 링 쇼-언이트네임 VLDB
Virtual-Interface Manager를 참조하십시오	클러스터 링 쇼-unitname vifmgr
SAN 관리 데몬	'클러스터 링 쇼-언이트네임 bcomd'

에 대한 자세한 내용은 `cluster ring show` "ONTAP 명령 참조입니다"을 참조하십시오.

이 예에서는 볼륨 위치 데이터베이스 프로세스를 보여 줍니다.

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

3. SAN 환경에서 작동 중인 경우 각 노드가 SAN 쿼럼에 있는지 확인합니다.

```
cluster kernel-service show
```

```
cluster1::*> cluster kernel-service show
Master            Cluster           Quorum        Availability
Operational
Node              Node              Status        Status        Status
----------------- ----------------- ------------- -------------
-------------
cluster1-01       cluster1-01       in-quorum     true
operational
                  cluster1-02       in-quorum     true
operational
2 entries were displayed.
```

4. 권한 수준을 admin으로 되돌립니다.

```
set -privilege admin
```

관련 정보

"시스템 관리"

계획되지 않은 자동 전환이 활성화되었는지 확인(MetroCluster FC 구성만 해당)

클러스터가 MetroCluster FC 구성인 경우 ONTAP를 업그레이드한 후 계획되지 않은 자동 전환이 활성화되는지 확인해야 합니다.

MetroCluster IP 구성을 사용하는 경우 이 절차를 건너뜁니다.

단계

1. 예기치 않은 자동 전환이 활성화되어 있는지 확인합니다.

```
metrocluster show
```

   자동 비계획 전환이 활성화된 경우 명령 출력에 다음 설명이 표시됩니다.

```
AUSO Failure Domain  auso-on-cluster-disaster
```

2. 명령문이 나타나지 않으면 예기치 않은 자동 전환을 설정합니다.

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
disaster
```

3. 예기치 않은 자동 전환이 활성화되었는지 확인합니다.

```
metrocluster show
```

관련 정보

"디스크 및 애그리게이트 관리"

ONTAP 업그레이드 후 모든 **LIFS**가 홈 포트에 있는지 확인합니다

ONTAP 업그레이드 프로세스의 일부로 발생하는 재부팅 중 일부 LIF가 홈 포트에서 할당된 페일오버 포트로 마이그레이션될 수 있습니다. 업그레이드 후 홈 포트에 없는 LIF를 사용하도록 설정하고 되돌려야 합니다.

단계

1. 모든 LIF의 상태를 표시합니다.

```
network interface show -fields home-port,curr-port
```

   모든 LIF에 대해 * Status Admin * 이 "Down"이거나 * is home * 이 "false"인 경우 다음 단계를 계속합니다.

2. 데이터 LIF 지원:

```
network interface modify {-role data} -status-admin up
```

3. LIF를 홈 포트로 되돌리기:

```
network interface revert *
```

4. 모든 LIF가 홈 포트에 있는지 확인:

```
network interface show
```

이 예에서는 SVM vs0용 모든 LIF가 홈 포트에 있음을 보여 줍니다.

```
cluster1::> network interface show -vserver vs0
         Logical    Status     Network          Current  Current Is
Vserver  Interface  Admin/Oper Address/Mask     Node     Port    Home
-------- ---------- ---------- ---------------- -------- ------- ----
vs0
         data001    up/up      192.0.2.120/24   node0    e0e     true
         data002    up/up      192.0.2.121/24   node0    e0f     true
         data003    up/up      192.0.2.122/24   node0    e2a     true
         data004    up/up      192.0.2.123/24   node0    e2b     true
         data005    up/up      192.0.2.124/24   node1    e0e     true
         data006    up/up      192.0.2.125/24   node1    e0f     true
         data007    up/up      192.0.2.126/24   node1    e2a     true
         data008    up/up      192.0.2.127/24   node1    e2b     true
8 entries were displayed.
```

관련 정보

- "네트워크 인터페이스"

특수 구성

업그레이드 후 특정 **ONTAP** 구성을 확인합니다

클러스터가 다음 기능 중 하나로 구성된 경우, ONTAP 소프트웨어를 업그레이드한 후 추가 단계를 수행해야 할 수 있습니다.

스스로에게 물어보십시오.	답변이 * 예 * 인 경우 다음을 수행하십시오.
ONTAP 9.7 이하에서 ONTAP 9.8 이상으로 업그레이드했습니까?	네트워크 구성을 확인합니다 EMS 대상에 대한 접근성을 제공하지 않는 네트워크 서비스 정책에서 EMS LIF 서비스를 제거합니다.
클러스터가 MetroCluster 구성입니까?	네트워킹 및 스토리지 상태를 확인합니다
SAN 구성이 있습니까?	SAN 구성을 확인합니다
ONTAP 9.3 이하에서 업그레이드했으며 NetApp 저장소 암호화를 사용하고 있습니까?	KMIP 서버 연결을 재구성합니다

스스로에게 물어보십시오.	답변이 * 예 * 인 경우 다음을 수행하십시오.
로드 공유 미러가 있습니까?	이동된 로드 공유 미러 소스 볼륨을 재배치합니다
ONTAP 9.9.1 이전에 생성된 SP(서비스 프로세서) 액세스에 대한 사용자 계정이 있습니까?	서비스 프로세서에 액세스할 수 있는 계정의 변경 사항을 확인합니다

업그레이드 후 **ONTAP** 네트워킹 구성을 확인합니다

ONTAP 9.7x 이하에서 ONTAP 9.8 이상으로 업그레이드한 후에는 네트워크 구성을 확인해야 합니다. 업그레이드 후 ONTAP는 레이어 2 내 상태를 자동으로 모니터링합니다.

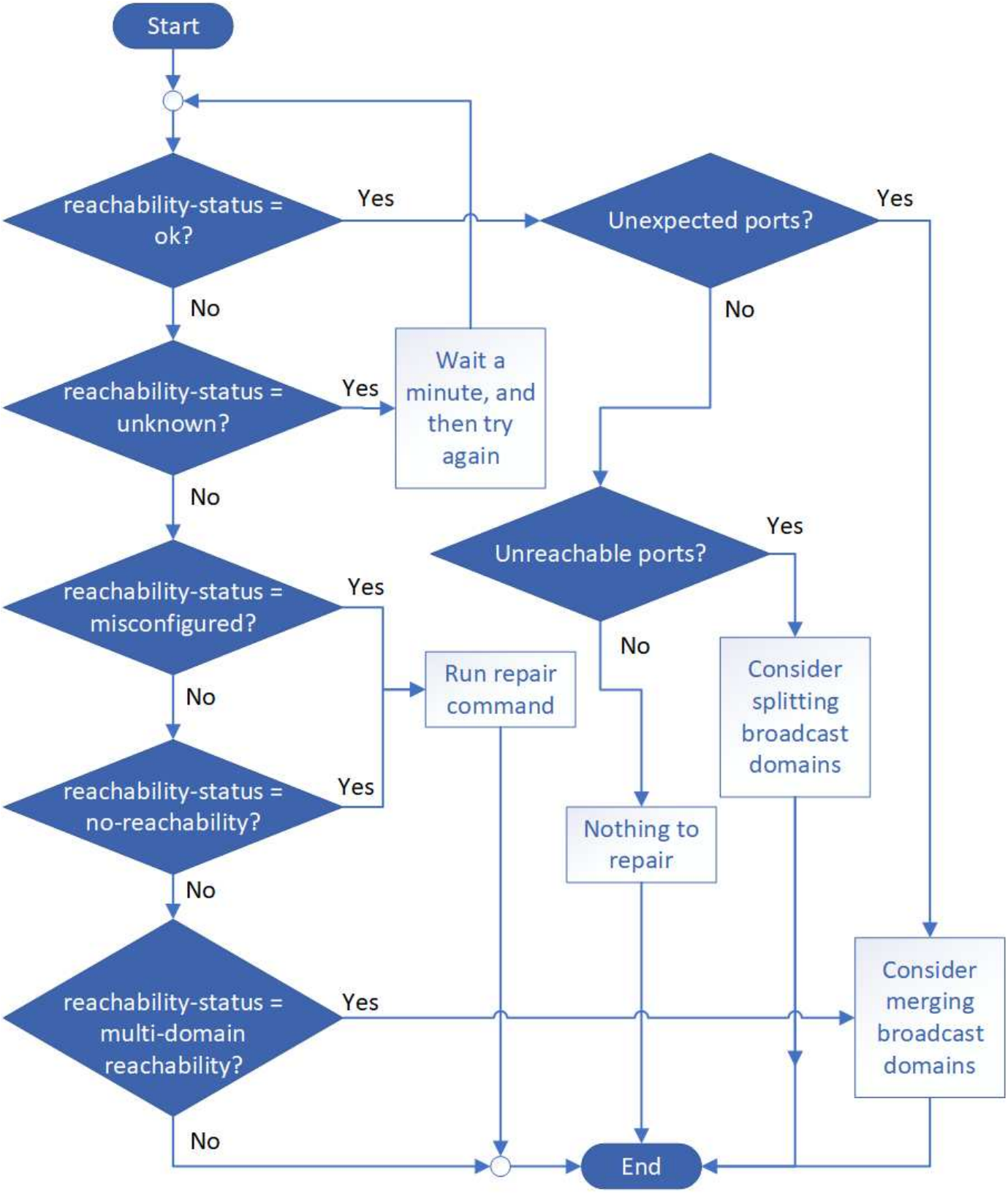
단계

1. 각 포트가 예상 브로드캐스트 도메인에 연결할 수 있는지 확인합니다.

```
network port reachability show -detail
```

에 대한 자세한 내용은 `network port reachability show` "ONTAP 명령 참조입니다"을 참조하십시오.

명령 출력에 연결 가능 결과가 포함되어 있습니다. 다음 진단트리와 표를 사용하여 내 상태 결과(내 상태)를 이해하고 다음에 수행할 작업(있는 경우)을 결정합니다.


Start
reachability-status = ok?
Yes
Unexpected ports?
Yes
No
reachability-status = unknown?
Yes
Wait a minute, and then try again
No
Unreachable ports?
Yes
reachability-status = misconfigured?
Yes
Run repair command
No
Consider splitting broadcast domains
No
reachability-status = no-reachability?
Yes
Nothing to repair
No
reachability-status = multi-domain reachability?
Yes
Consider merging broadcast domains
No
End

도달 가능성 - 상태	설명

좋습니다	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있습니다. 도달 가능성 - 상태가 "정상"이지만 "예상치 못한 포트"가 있는 경우 하나 이상의 브로드캐스트 도메인을 병합하는 것이 좋습니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 병합합니다". 도달 가능성 - 상태가 "정상"이지만 "연결할 수 없는 포트"인 경우 하나 이상의 브로드캐스트 도메인을 분할하는 것이 좋습니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 분할합니다". 도달 가능성 - 상태가 "정상"이고 예기치 않거나 연결할 수 없는 포트가 없는 경우 구성이 올바른 것입니다.
잘못 구성되었습니다. - 도달 가능성	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 없지만 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있습니다. 포트 연결을 복구할 수 있습니다. 다음 명령을 실행하면 시스템에서 해당 포트가 재연결 가능한 브로드캐스트 도메인에 포트를 할당합니다. 네트워크 포트 도달 가능성 복구 노드 포트 자세한 내용은 을 참조하십시오 "수리 포트 도달 가능성". 에 대한 자세한 내용은 `network port reachability repair` "ONTAP 명령 참조입니다"을 참조하십시오.
아니오 - 내 상태	이 포트에는 기존 브로드캐스트 도메인에 대한 계층 2 도달 기능이 없습니다. 포트 연결을 복구할 수 있습니다. 다음 명령을 실행하면 시스템이 기본 IPspace에서 자동으로 생성된 새 브로드캐스트 도메인에 포트를 할당합니다. 네트워크 포트 도달 가능성 복구 노드 포트 자세한 내용은 을 참조하십시오 "수리 포트 도달 가능성".
다중 도메인 내의 도달 가능성	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있지만 하나 이상의 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능도 있습니다. 물리적 연결 및 스위치 구성을 검사하여 올바르지 않거나 포트에 할당된 브로드캐스트 도메인을 하나 이상의 브로드캐스트 도메인과 병합해야 하는지 확인합니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 병합합니다" 또는 "수리 포트 도달 가능성".
알 수 없음	도달 가능성 - 상태가 "알 수 없음"인 경우 몇 분 정도 기다린 후 명령을 다시 시도하십시오.

포트를 복구한 후에는 교체된 LIF 및 VLAN을 확인하고 해결해야 합니다. 포트가 인터페이스 그룹의 일부인 경우 해당 인터페이스 그룹의 변경 사항도 이해해야 합니다. 자세한 내용은 을 참조하십시오 "수리 포트 도달 가능성".

ONTAP 9.7 이전 버전에서 ONTAP 9.8 이상으로 업그레이드하기 전에 이벤트 관리 시스템(EMS) 메시지를 설정한 경우, 업그레이드 후에는 EMS 메시지가 전달되지 않을 수 있습니다.

업그레이드하는 동안, `management-ems` EMS LIF 서비스인 는 관리 SVM의 모든 기존 서비스 정책에 추가됩니다. 이를 통해 서비스 정책과 연결된 모든 LIF에서 EMS 메시지를 전송할 수 있습니다. 선택한 LIF에 이벤트 알림 대상에 대한 연결 기능이 없으면 메시지가 전달되지 않습니다.

이를 방지하려면 업그레이드 후 대상에 대한 도달성을 제공하지 않는 네트워크 서비스 정책에서 EMS LIF 서비스를 제거해야 합니다.

"ONTAP LIF 및 서비스 정책에 대해 자세히 알아보세요"..

단계

1. EMS 메시지를 보낼 수 있는 LIF 및 관련 네트워크 서비스 정책을 식별합니다.

```
network interface show -fields service-policy -services management-ems
```

```
vserver        lif            service-policy
-------------- ------------   ------------------
cluster-1      cluster_mgmt   default-management
cluster-1      node1-mgmt     default-management
cluster-1      node2-mgmt     default-management
cluster-1      inter_cluster  default-intercluster
4 entries were displayed.
```

2. 각 LIF에서 EMS 대상에 대한 연결을 확인합니다.

```
network ping -lif <lif_name> -vserver <svm_name> -destination
<destination_address>
```

각 노드에서 이 작업을 수행합니다.

예

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

3. 고급 권한 수준 입력:

```
set advanced
```

4. 도달 가능성이 없는 LIF의 경우 제거하세요. `management-ems` 해당 서비스 정책에 따른 LIF 서비스:

```
network interface service-policy remove-service -vserver <svm_name>
-policy <service_policy_name> -service management-ems
```

에 대한 자세한 내용은 `network interface service-policy remove-service` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 관리 - EMS LIF가 이제 EMS 타겟에 대한 연결 기능을 제공하는 LIF에만 연결되어 있는지 확인합니다.

```
network interface show -fields service-policy -services management-ems
```

ONTAP 업그레이드 후 **MetroCluster** 구성의 네트워크 및 스토리지 상태를 확인합니다

MetroCluster 구성에서 ONTAP 클러스터를 업그레이드한 후에는 각 클러스터의 LIF, 애그리게이트, 볼륨의 상태를 확인해야 합니다.

1. LIF 상태를 확인합니다.

```
network interface show
```

정상 운영 시 소스 SVM에 대한 LIF의 관리 상태가 가동이고 홈 노드에 있어야 합니다. 타겟 SVM을 위한 LIF는 홈 노드에 배치하거나 설치할 필요가 없습니다. 스위치오버에서 모든 LIF는 관리 상태가 Up 이지만 홈 노드에 있을 필요가 없습니다.

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            cluster1-a1_clus1
                         up/up    192.0.2.1/24       cluster1-01
                                                                  e2a
true
            cluster1-a1_clus2
                         up/up    192.0.2.2/24       cluster1-01
                                                                  e2b
true


cluster1-01
            clus_mgmt    up/up    198.51.100.1/24    cluster1-01
                                                                  e3a
true
            cluster1-a1_inet4_intercluster1
                         up/up    198.51.100.2/24    cluster1-01
                                                                  e3c
true
            ...

27 entries were displayed.
```

2. 애그리게이트의 상태를 확인합니다.

```
storage aggregate show -state !online
```

이 명령은 _not_online 상태인 모든 애그리게이트를 표시합니다. 정상 운영 시 로컬 사이트에 있는 모든 애그리게이트는 온라인 상태여야 합니다. 하지만 MetroCluster 구성이 전환 중인 경우 재해 복구 사이트의 루트 애그리게이트를 오프라인 상태로 전환할 수 있습니다.

이 예는 정상 작동 중인 클러스터를 보여줍니다.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

이 예에서는 재해 복구 사이트의 루트 애그리게이트가 오프라인 상태인 전환 클러스터를 보여 줍니다.

```
cluster1::> storage aggregate show -state !online
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b1
                0B        0B    0% offline      0 cluster2-01
raid_dp,

mirror

degraded
aggr0_b2
                0B        0B    0% offline      0 cluster2-02
raid_dp,

mirror

degraded
2 entries were displayed.
```

3. 볼륨의 상태를 확인합니다.

```
volume show -state !online
```

이 명령은 _not_online 상태인 모든 볼륨을 표시합니다.

MetroCluster 구성이 정상 작동 중인 경우(스위치오버 상태가 아님), 클러스터에 있는 보조 SVM이 소유한 모든 볼륨(SVM 이름이 "-mc"로 추가된 볼륨)이 출력에 표시되어야 합니다.

전환 시에만 볼륨은 온라인 상태가 됩니다.

이 예에서는 재해 복구 사이트의 볼륨이 온라인 상태가 아닌 정상적인 상태의 클러스터를 보여 줍니다.

```
cluster1::> volume show -state !online
  (volume show)
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2-mc    vol1         aggr1_b1     -          RW            -
-     -
vs2-mc    root_vs2     aggr0_b1     -          RW            -
-     -
vs2-mc    vol2         aggr1_b1     -          RW            -
-     -
vs2-mc    vol3         aggr1_b1     -          RW            -
-     -
vs2-mc    vol4         aggr1_b1     -          RW            -
-     -
5 entries were displayed.
```

4. 일치하지 않는 볼륨이 없는지 확인합니다.

```
volume show -is-inconsistent true
```

를 참조하십시오"NetApp 지식 기반: 볼륨에 WAFL 일관되지 않음 표시" 일관되지 않은 볼륨을 해결하는 방법에 대해.

ONTAP 업그레이드 후 **SAN** 구성을 확인합니다

ONTAP를 업그레이드한 후 SAN 환경에서 LIF에 접속된 각 이니시에이터가 LIF에 성공적으로 다시 연결되었는지 확인해야 합니다.

1. 각 이니시에이터가 올바른 LIF에 연결되어 있는지 확인합니다.

   이니시에이터 목록을 업그레이드 준비 중에 수행한 목록과 비교해야 합니다. ONTAP 9.11.1 이상을 실행 중인 경우 System Manager를 사용하여 연결 상태를 확인할 수 있으므로 CLI보다 훨씬 명확합니다.

시스템 관리자

a. System Manager에서 * 호스트 > SAN 이니시에이터 그룹 * 을 클릭합니다.

   페이지에 이니시에이터 그룹(igroup) 목록이 표시됩니다. 목록이 큰 경우 페이지의 오른쪽 아래 모서리에 있는 페이지 번호를 클릭하여 목록의 추가 페이지를 볼 수 있습니다.

   열에는 igroup에 대한 다양한 정보가 표시됩니다. 9.11.1부터 igroup의 연결 상태도 표시됩니다. 상태 알림 위로 마우스를 가져가면 세부 정보가 표시됩니다.

CLI를 참조하십시오

- iSCSI 이니시에이터 나열:

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

- FC 이니시에이터 나열:

```
fcp initiator show -fields igroup,wwpn,lif
```

ONTAP 9.2 이전 버전에서 업그레이드한 후 **KMIP** 서버 연결을 다시 구성합니다

ONTAP 9.2 이상에서 ONTAP 9.3 이상으로 업그레이드한 후에는 모든 외부 키 관리(KMIP) 서버 연결을 다시 구성해야 합니다.

단계

1. Key Manager 연결을 구성합니다.

```
security key-manager setup
```

2. KMIP 서버 추가:

```
security key-manager add -address <key_management_server_ip_address>
```

3. KMIP 서버가 연결되었는지 확인합니다.

```
security key-manager show -status
```

4. 키 서버를 쿼리합니다.

```
security key-manager query
```

5. 새 인증 키 및 암호 구문을 생성합니다.

```
security key-manager create-key -prompt-for-key true
```

최소 32자의 암호를 설정하세요.

6. 새 인증 키를 쿼리합니다.

```
security key-manager query
```

7. SED(자체 암호화 디스크)에 새 인증 키를 할당합니다.

```
storage encryption disk modify -disk <disk_ID> -data-key-id <key_ID>
```

ⓘ 쿼리에서 새로운 인증 키를 사용하세요.

8. 필요한 경우 SED에 FIPS 키를 할당합니다.

```
storage encryption disk modify -disk <disk_id> -fips-key-id
<fips_authentication_key_id>
```

보안 설정에서 데이터 인증과 FIPS 140-2 인증에 대해 서로 다른 키를 사용해야 하는 경우 각각에 대해 별도의 키를 만들어야 합니다. 그렇지 않은 경우 두 가지 모두에 동일한 인증 키를 사용하세요.

관련 정보

- "보안 키 관리자 설정"
- "저장 암호화 디스크 수정"

ONTAP 업그레이드 후 이동된 로드 공유 미러 소스 볼륨을 재배치합니다

ONTAP를 업그레이드한 후에는 로드 공유 미러 소스 볼륨을 업그레이드 이전 위치로 다시 이동해야 합니다.

단계

1. 로드 공유 미러 소스 볼륨을 이동하기 전에 생성한 레코드를 사용하여 로드 공유 미러 소스 볼륨을 이동할 위치를 식별합니다.
2. 로드 공유 미러 소스 볼륨을 원래 위치로 다시 이동:

```
volume move start
```

ONTAP 업그레이드 후 서비스 프로세서에 액세스할 수 있는 사용자 계정 변경 사항

ONTAP 9.8 이하 버전에서 비 관리자 역할을 사용하여 SP(서비스 프로세서)에 액세스할 수 있는 사용자 계정을 만들고 ONTAP 9.9.1 이상으로 업그레이드하는 경우 에서 관리자가 아닌 모든 값을 반환합니다 `-role` 매개 변수가 로 수정되었습니다 `admin`.

자세한 내용은 을 참조하십시오 "SP에 액세스할 수 있는 계정입니다".

ONTAP 업그레이드 후 디스크 자격 패키지를 업데이트합니다

ONTAP 소프트웨어를 업그레이드한 후 ONTAP 디스크 자격 패키지(DQP)를 다운로드하여 설치해야 합니다. DQP는 ONTAP 업그레이드의 일부로 업데이트되지 않습니다.

DQP에는 새로 검증된 모든 드라이브와의 ONTAP 상호 작용을 위한 적절한 매개변수가 포함되어 있습니다. DQP 버전에 새로 인증된 드라이브에 대한 정보가 포함되어 있지 않으면 ONTAP에 드라이브를 올바르게 구성하기 위한 정보가 없습니다.

분기마다 DQP를 업데이트하는 것이 가장 좋습니다. 또한 다음과 같은 이유로 DQP를 업데이트해야 합니다.

- 클러스터의 노드에 새 드라이브 유형 또는 크기를 추가할 때마다

  예를 들어 이미 1TB 드라이브를 사용하고 2TB 드라이브를 추가한 경우 최신 DQP 업데이트를 확인해야 합니다.

- 디스크 펌웨어를 업데이트할 때마다
- 최신 디스크 펌웨어 또는 DQP 파일을 사용할 수 있는 경우

관련 정보

- "NetApp 다운로드: 디스크 검증 패키지"
- "NetApp 다운로드: 디스크 드라이브 펌웨어"

펌웨어, 시스템 및 보안 업데이트

ONTAP의 펌웨어, 시스템 및 보안 업데이트 개요

ONTAP 버전에 따라 자동 펌웨어, 시스템 및 보안 업데이트를 활성화할 수 있습니다.

ONTAP 버전	자동 업데이트에 포함된 내용
9.16.1 이상	• 인공 지능(ARP/AI)을 이용한 자율적 랜섬웨어 방어 • ONTAP 시간대 데이터베이스 • 스토리지 장치, 디스크 및 디스크 쉘프를 위한 스토리지 펌웨어 • 서비스 프로세서 및 BMC 모듈용 SP/BMC 펌웨어

ONTAP 버전	자동 업데이트에 포함된 내용
9.13.1 이상	• ONTAP 시간대 데이터베이스 • 스토리지 장치, 디스크 및 디스크 쉘프를 위한 스토리지 펌웨어 • 서비스 프로세서 및 BMC 모듈용 SP/BMC 펌웨어
9.10.1 이상	• 스토리지 장치, 디스크 및 디스크 쉘프를 위한 스토리지 펌웨어 • 서비스 프로세서 및 BMC 모듈용 SP/BMC 펌웨어
9.9.1 이전 버전	지원되지 않습니다

사용 중인 ONTAP 버전에 대해 자동 업데이트를 사용할 수 없거나 자동 업데이트를 사용하도록 설정하지 않은 경우 펌웨어, 시간대 데이터베이스 및 보안 업데이트를 수동으로 수행할 수 있습니다.

관련 링크

- "펌웨어 업데이트를 수동으로 수행하는 방법을 알아봅니다"
- "기술 자료 문서, ONTAP 9에서 표준 시간대 정보를 업데이트하는 방법"
- "수동으로 보안 업데이트를 수행하는 방법을 알아봅니다"

비디오: 자동 펌웨어 업데이트 기능

ONTAP 9.10.1부터 제공되는 자동 펌웨어 업데이트 기능을 살펴보십시오.

자동 업데이트 설치 예약 방법

동일한 클러스터에 포함된 적격 노드는 모두 자동 업데이트를 위해 그룹화됩니다. 대상 노드가 자동 업데이트를 예약하는 기간은 업데이트의 우선 순위 수준과 업데이트가 필요한 환경의 시스템 비율에 따라 달라집니다.

예를 들어, 전체 시스템의 10% 이하가 우선 순위가 아닌 업데이트를 받을 수 있는 경우 1주일 이내에 모든 대상 시스템에 대한 업데이트가 예약됩니다. 하지만 전체 시스템의 76% 이상이 우선 순위가 아닌 업데이트를 받을 수 있는 경우 8주 동안 대상 시스템에 대해 업데이트 시차가 발생합니다. 이 지그재그형 설치는 해결해야 할 업데이트에 문제가 있는 경우 전체 환경에 대한 위험을 줄이는 데 도움이 됩니다.

매주 자동 업데이트가 예약된 전체 시스템의 비율은 다음과 같습니다.

- 중요 업데이트 *

업데이트가 필요한 시스템의 비율	**1**주에 발생한 업데이트 비율	**2**주에 발생한 업데이트 비율
50% 이하	100%	
50-100%	30%	70%

높은 우선 순위의 업데이트 *

업데이트가 필요한 시스템의 비율	업데이트 중 매주 발생하는 비율			
	* 1주차 *	* 2주차 *	* 3주차 *	* 4주차 *
* 25% 이하 *	100%			
* 26-50% *	30%	70%		
* 50-100% *	10%	20%	30%	40%

- 일반 우선 순위 업데이트 *

업데이트가 필요한 시스템의 비율	업데이트 중 매주 발생하는 비율							
	* 1주차 *	* 2주차 *	* 3주차 *	* 4주차 *	5주차 *	* 6주차 *	* 7주차 *	* 8주차 *
* 10% 이하 *	100%							
* 11-20% *	30%	70%						
* 21-50% *	10%	20%	30%	40%				
* 51-75% *	5%	10%	15%	20%	20%	30%		
* 76-100% *	5%	5%	10%	10%	15%	15%	20%	20%

자동 업데이트를 활성화합니다

자동 업데이트를 활성화하여 ONTAP가 사용자의 개입 없이 펌웨어, 시스템 및 보안 업데이트를 다운로드하고 설치할 수 있도록 합니다.

자동 업데이트를 활성화하려면 EULA 약관에 동의하고 사용자 환경에 맞게 각 시스템 구성 요소의 기본 업데이트 동작을 확인하거나 구성해야 합니다.

각 시스템 구성 요소에 대한 자동 업데이트의 가용성은 ONTAP 버전에 따라 다릅니다.

ONTAP 버전입니다	사용 가능한 자동 업데이트
9.16.1 이상	• 인공 지능(ARP/AI)을 이용한 자율적 랜섬웨어 방어 • ONTAP 시간대 데이터베이스 • 스토리지 장치, 디스크 및 디스크 쉘프를 위한 스토리지 펌웨어 • 서비스 프로세서 및 BMC 모듈용 SP/BMC 펌웨어 • 디스크 자격 평가 패키지(DQP)
9.13.1 이상	• ONTAP 시간대 데이터베이스 • 스토리지 장치, 디스크 및 디스크 쉘프를 위한 스토리지 펌웨어 • 서비스 프로세서 및 BMC 모듈용 SP/BMC 펌웨어 • 디스크 자격 평가 패키지(DQP)
9.10.1 이상	• 스토리지 장치, 디스크 및 디스크 쉘프를 위한 스토리지 펌웨어 • 서비스 프로세서 및 BMC 모듈용 SP/BMC 펌웨어 • 디스크 자격 평가 패키지(DQP)

시작하기 전에

- 현재 지원 권한이 있어야 합니다. 시스템 세부 정보 * 페이지에서 확인할 수 "NetApp Support 사이트"있습니다.
- 자동 업데이트를 사용하려면 먼저 HTTPS가 포함된 AutoSupport를 활성화해야 합니다. 클러스터에서 AutoSupport가 활성화되어 있지 않거나 클러스터에서 다른 전송 프로토콜을 사용하여 AutoSupport가 활성화되어 있는 경우, 이 절차 중에 HTTPS로 사용하도록 설정할 수 있습니다.

> AutoSupport OnDemand는 HTTPS 전송 프로토콜을 사용하여 기술 지원 부서로 메시지를 보내도록 구성된 경우 기본적으로 활성화되며 작동합니다.

- ONTAP 9.10.1부터 자동 업데이트를 사용하도록 설정한 경우 다음 추가 URL에 HTTPS 연결이 있는지 확인합니다.
  - https://support-sg-naeast.netapp.com 으로 문의하십시오
  - https://support-sg-nawest.netapp.com 으로 문의하십시오

이 작업에 대해

ONTAP 9.16.1 이전에 생성되어 9.16.1 이상으로 업그레이드된 클러스터의 경우:

- 자동 업데이트 기능이 이미 활성화된 경우, 시스템 구성 요소 업데이트 기본값은 업그레이드 후에도 변경되지 않습니다.
- 자동 업데이트가 아직 활성화되어 있지 않으면 ONTAP 9.16.1 이상에서 기본적으로 적용되는 시스템 구성 요소 업데이트가 적용됩니다.

자동 시스템 구성 요소 업데이트 기본값은 ONTAP 버전에 따라 자동으로 업데이트되거나 알림을 표시하도록 설정되어 있습니다. 절차를 완료하기 전에 이러한 설정이 사용자 환경에 맞는지 확인하세요.

다음은 "비디오" 자동 업데이트 프로세스 사용에 대한 간략한 개요를 보여 줍니다.

예 **5.** 단계

System Manager - ONTAP 9.16.1 이상

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. HTTPS에서 AutoSupport OnDemand를 사용하도록 설정하지 않은 경우 를 선택하여 ⋮계속 진행하는 데 필요한 설정을 활성화합니다.
3. 소프트웨어 업데이트 * 섹션에서 * 사용 * 을 선택합니다.
4. 각 업데이트 유형에 대해 수행할 작업을 지정합니다.

   각 업데이트 유형에 대한 업데이트를 자동으로 업데이트하거나 알림을 표시하거나 자동으로 해제하도록 선택할 수 있습니다.

5. 이용 약관에 동의하고 * 저장 * 을 선택합니다.

시스템 관리자 **- ONTAP 9.15.1** 이하

1. System Manager에서 * Events * 를 선택합니다.
2. 개요 * 섹션에서 * 자동 업데이트 사용 * 옆의 * 작업 > 활성화 * 를 선택합니다.
3. HTTPS가 활성화된 AutoSupport가 없는 경우 선택하여 활성화합니다.
4. 이용 약관에 동의하고 * 저장 * 을 선택합니다.

CLI를 참조하십시오

1. 자동 펌웨어 업데이트 활성화:

```
system service-processor image modify -node <node_name> -autoupdate
true
```

관련 정보

- "AutoSupport 사용을 준비합니다"
- "HTTPS를 통한 AutoSupport 메시지 전달 문제를 해결합니다"

자동 업데이트를 수정합니다

자동 업데이트 기능이 활성화되어 있고 기본 시스템 구성 요소 기본 설정이 구성되어 있으면

ONTAP 권장되는 모든 업데이트를 자동으로 감지, 다운로드 및 설치할 수 있습니다. 설치 전에 권장 업데이트를 보거나 권장 업데이트를 자동으로 해제하려면 기본 동작을 원하는 대로 수정할 수 있습니다.

예 **6.** 단계

ONTAP 9.16.1 이상

1. System Manager에서 * 클러스터 > 설정 * 으로 이동합니다.
2. 소프트웨어 업데이트 * 섹션에서 를 선택합니다 →.
3. 다른 모든 업데이트 * 탭을 선택하고 * 자동 업데이트 설정 편집 * 을 클릭합니다.
4. 각 업데이트 유형에 대해 수행할 기본 작업을 지정합니다.

   각 업데이트 유형에 대한 업데이트를 자동으로 업데이트하거나 알림을 표시하거나 자동으로 해제하도록 선택할 수 있습니다.

   ⓘ ONTAP 시간대 데이터베이스는 * 시스템 파일 * 업데이트 유형에 의해 제어됩니다.

5. 이용 약관에 동의하고 * 저장 * 을 선택합니다.

ONTAP 9.15.1 이하

1. System Manager에서 * 클러스터 > 설정 * 을 클릭합니다.
2. 자동 업데이트 * 섹션에서 을 ⋮ 클릭하여 작업 목록을 봅니다.
3. 자동 업데이트 설정 편집 * 을 클릭합니다.
4. 각 업데이트 유형에 대해 수행할 기본 작업을 지정합니다.

   각 유형의 업데이트를 자동으로 업데이트하거나 알림을 표시하거나 자동으로 해제하도록 선택할 수 있습니다.

   ⓘ ONTAP 시간대 데이터베이스는 시스템 파일 업데이트 유형에 의해 제어됩니다.

권장 자동 업데이트를 관리합니다

자동 업데이트 로그에는 설명, 범주, 설치 예정 시간, 상태 및 오류를 포함하여 각 업데이트에 대한 권장 사항과 세부 정보가 표시됩니다. 로그를 보고 각 권장 사항에 대해 수행할 작업을 결정할 수 있습니다.

단계

1. 권장 사항 목록 보기:

클러스터 설정에서 보기	업데이트 탭에서 보기
a. 클러스터 > 설정 * 을 클릭합니다. b. 사용 중인 ONTAP 버전에 따라 다음 중 하나를 수행합니다. ◦ ONTAP 9.15.1 이하 버전의 경우 * 자동 업데이트 * 섹션에서 을 ⋮ 클릭한 다음 옵션을 클릭하여 모든 업데이트를 봅니다. ◦ ONTAP 9.16.1 이상의 경우 * 소프트웨어 업데이트 * 섹션에서 을 선택합니다 →. 모든 기타 업데이트 * 창의 오른쪽 모서리에서 * 자세히 * 를 ⋮ 클릭한 다음 옵션을 클릭하여 모든 업데이트를 봅니다.	a. 클러스터 > 개요 * 를 클릭합니다. b. 개요 * 섹션에서 * 자세히 * 를 ⋮ 클릭한 다음 * ONTAP 업데이트 * 를 클릭합니다. c. 사용 중인 ONTAP 버전에 따라 다음을 수행합니다. ◦ ONTAP 9.15.1 이하 버전의 경우 * 펌웨어 업데이트 * 를 클릭합니다. ◦ ONTAP 9.16.1 이상의 경우 * 기타 모든 업데이트 * 를 클릭합니다. d. 업데이트 페이지에서 * 자세히 * 를 ⋮ 클릭한 다음 옵션을 클릭하여 모든 업데이트를 봅니다.

2. 설명 옆에 있는 을 ⋮ 클릭하여 권장 사항에 대해 수행할 수 있는 작업 목록을 봅니다.

   권장 사항의 상태에 따라 다음 작업 중 하나를 수행할 수 있습니다.

업데이트가 이 상태인 경우…	할 수 있는 일…
예약되지 않았습니다	• 업데이트 *: 업데이트 프로세스를 시작합니다. • 일정 *: 업데이트 프로세스를 시작할 날짜를 설정할 수 있습니다. • Dismiss *: 목록에서 권장 사항을 제거합니다.
이(가) 예약되었습니다	• 업데이트 *: 업데이트 프로세스를 시작합니다. • 일정 편집 *: 업데이트 프로세스를 시작하기 위해 예약된 날짜를 수정할 수 있습니다. 별표 취소 *: 예약된 날짜를 취소합니다.
이(가) 해고되었습니다	• 해제 *: 권장 사항을 목록으로 반환합니다.
이(가) 적용 중이거나 다운로드 중입니다	• 취소 *: 업데이트를 취소합니다.

펌웨어를 수동으로 업데이트합니다

에 등록한 경우 ONTAP 9.9.1부터 시작합니다 "Active IQ Unified Manager"에서는 디스크, 디스크 쉘프, 서비스 프로세서(SP) 또는 베이스보드 관리 컨트롤러(BMC)와 같은 지원되는 장치에 대한 펌웨어 업데이트가 클러스터에서 보류 중임을 알리는 경고를 System Manager에서 받을 수 있습니다.

ONTAP 9 .8을 실행 중이거나 Active IQ Unified Manager에 등록되어 있지 않은 경우 NetApp 지원 사이트 로 이동하여 펌웨어 업데이트를 다운로드하십시오.

시작하기 전에

원활한 펌웨어 업데이트를 준비하려면 업데이트를 시작하기 전에 SP 또는 BMC를 재부팅해야 합니다. `system service-processor reboot-sp -node node_name`명령을 사용하여 재부팅합니다. 에 대한 자세한 내용은 `system service-processor reboot-sp` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

사용 중인 ONTAP 버전과 Active IQ Unified Manager에 등록된 경우 해당 절차를 따르십시오.

Digital Advisor를 사용하는 **ONTAP 9.16.1** 이상

단계

1. System Manager에서 * 대시보드 * 로 이동합니다.

   클러스터에 대해 권장되는 펌웨어 업데이트가 있으면 * 상태 * 섹션에 메시지가 표시됩니다.

2. 경고 메시지를 클릭합니다.
3. 권장 업데이트 목록에서 보안 업데이트 옆에 있는 * 작업 * 을 선택합니다.
4. 업데이트를 즉시 설치하려면 * 업데이트 * 를 클릭하고, 나중에 업데이트 일정을 예약하려면 * 일정 * 을 클릭합니다.

   업데이트가 이미 예약된 경우 * 편집 * 또는 * 취소 * 할 수 있습니다.

ONTAP 9.9.1 ~ 9.15.1(디지털 어드바이저 포함**)**

1. System Manager에서 * 대시보드 * 로 이동합니다.

   클러스터에 대해 권장되는 펌웨어 업데이트가 있으면 * 상태 * 섹션에 메시지가 표시됩니다.

2. 경고 메시지를 클릭합니다.

   펌웨어 업데이트 * 탭이 * 업데이트 * 페이지에 표시됩니다.

3. 수행하려는 펌웨어 업데이트에 대해 * NetApp 지원 사이트에서 다운로드 * 를 클릭합니다.

   NetApp Support 사이트가 표시됩니다.

4. NetApp Support 사이트에 로그인하여 업데이트에 필요한 펌웨어 이미지 패키지를 다운로드합니다.
5. 네트워크 또는 로컬 폴더에 있는 HTTP 또는 FTP 서버로 파일을 복사합니다.
6. System Manager에서 * Cluster > Overview * 를 클릭합니다.
7. 개요 * 창의 오른쪽 모서리에서 * 자세히 * 를 ⋮ 클릭하고 * ONTAP 업데이트 * 를 선택합니다.
8. 펌웨어 업데이트 * 를 클릭합니다.
9. 사용 중인 ONTAP 버전에 따라 다음을 수행합니다.

ONTAP 9.9.1 및 **9.10.0**	**ONTAP 9.10.1** 이상
a. 서버 * 또는 * 로컬 클라이언트 * 에서 * 를 선택합니다 b. 서버 URL 또는 파일 위치를 제공합니다.	a. 권장 업데이트 목록에서 * 작업 * 을 선택합니다. b. 업데이트를 즉시 설치하려면 * 업데이트 * 를 클릭하고, 나중에 업데이트 일정을 예약하려면 * 일정 * 을 클릭합니다. 업데이트가 이미 예약된 경우 * 편집 * 또는 * 취소 * 할 수 있습니다. c. 펌웨어 업데이트 * 버튼을 선택합니다.

Digital Advisor가 없는 **ONTAP 9 .8** 이상

1. 로 이동합니다 "NetApp Support 사이트" 로그인한 다음
2. 클러스터 펌웨어를 업데이트하는 데 사용할 펌웨어 패키지를 선택합니다.
3. 네트워크 또는 로컬 폴더에 있는 HTTP 또는 FTP 서버로 파일을 복사합니다.
4. System Manager에서 * Cluster > Overview * 를 클릭합니다.
5. 개요 * 창의 오른쪽 모서리에서 * 자세히 * 를 ⋮ 클릭하고 * ONTAP 업데이트 * 또는 * 소프트웨어 업데이트 * 를 선택합니다(버전에 따라 다름).
6. 사용 중인 ONTAP 버전에 따라 다음을 수행합니다.
   - ONTAP 9.15.1 이하 버전의 경우 * 펌웨어 업데이트 * 를 클릭합니다.
   - ONTAP 9.16.1 이상의 경우 * 기타 모든 업데이트 * 를 클릭합니다.
7. 사용 중인 ONTAP 버전에 따라 다음을 수행합니다.

ONTAP 9.8, 9.9.1 및 **9.10.0**	**ONTAP 9.10.1** 이상
1. 서버 * 또는 * 로컬 클라이언트 * 에서 * 를 선택합니다 2. 서버 URL 또는 파일 위치를 제공합니다.	1. 권장 업데이트 목록에서 * 작업 * 을 선택합니다. 2. 업데이트를 즉시 설치하려면 * 업데이트 * 를 클릭하고, 나중에 업데이트 일정을 예약하려면 * 일정 * 을 클릭합니다. 업데이트가 이미 예약된 경우 * 편집 * 또는 * 취소 * 할 수 있습니다. 3. 펌웨어 업데이트 * 버튼을 선택합니다.

작업을 마친 후

펌웨어 업데이트 요약 * 에서 업데이트를 모니터링하거나 확인할 수 있습니다. 해제되었거나 설치에 실패한 업데이트를 보려면 사용 중인 ONTAP 버전에 따라 다음 중 하나를 실행합니다.

- ONTAP 9.15.1 이하의 경우 * 클러스터 > 설정 > 자동 업데이트 > 모든 자동 업데이트 보기 * 를 클릭합니다
- ONTAP 9.16.1 이상에서는 * 클러스터 > 설정 > 소프트웨어 업데이트 * 를 클릭합니다. 모든 기타 업데이트 * 창의 오른쪽 모서리에서 * 자세히 * 를 ⋮ 클릭하고 * 모든 자동 업데이트 보기 * 를 선택합니다.

ONTAP를 되돌립니다

ONTAP 클러스터를 복구하려면 기술 지원이 필요합니까?

다음과 같은 상황에서 ONTAP 클러스터를 복구하기 전에 기술 지원 부서에 문의해야 합니다.

- 프로덕션 환경

  기술 지원 부서의 도움 없이 운영 클러스터를 복구하려고 하지 마십시오.

- ONTAP 9.5 이상에서 볼륨을 생성했으며 이전 버전으로 되돌려야 합니다.

되돌리기 전에 적응형 압축을 사용하는 볼륨의 압축을 해제해야 합니다.

도움 없이 새 클러스터 또는 테스트 클러스터를 되돌릴 수 있습니다. 클러스터를 직접 되돌리려고 할 때 다음 문제가 발생하는 경우 기술 지원 부서에 문의하십시오.

- 되돌리기가 실패하거나 완료할 수 없습니다.
- 되돌리기가 완료되지만 운영 환경에서 클러스터를 사용할 수 없습니다.
- 되돌리기가 완료되고 클러스터가 운영 환경으로 전환되지만 이 동작이 만족스럽지 않습니다.

지원되는 **ONTAP** 되돌리기 경로

ONTAP 소프트웨어를 현재 ONTAP 버전보다 한 단계 이전 릴리스로만 직접 되돌릴 수 있습니다. 예를 들어, 9.15.1을 실행 중인 경우 9.13.1로 바로 되돌릴 수 없습니다. 먼저 9.14.1로 되돌려야 합니다. 그런 다음 9.14.1에서 9.13.1로 별도로 되돌려야 합니다.

ONTAP 9.4 이하 버전으로 되돌리는 것은 지원되지 않습니다. 지원되지 않는 ONTAP 버전으로 되돌리면 안 됩니다.

명령을 사용하여 각 노드에서 실행 중인 ONTAP 버전을 확인할 수 `system image show` 있습니다.

다음과 같은 지원되는 되돌리기 경로는 사내 ONTAP 릴리즈에만 해당됩니다. 클라우드에서 ONTAP를 되돌리는 방법에 대한 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP를 되돌리거나 다운그레이드하는 중입니다".

"AFX 스토리지 시스템"ONTAP 소프트웨어 되돌리기를 지원하지 않습니다.

복구할 수 있는 대상...	대상...
ONTAP 9.18.1	ONTAP 9.17.1
ONTAP 9.17.1	ONTAP 9.16.1
ONTAP 9.16.1	ONTAP 9.15.1
ONTAP 9.15.1	ONTAP 9.14.1
ONTAP 9.14.1	ONTAP 9.13.1
ONTAP 9.13.1	ONTAP 9.12.1
ONTAP 9.12.1	ONTAP 9.11.1
ONTAP 9.11.1	ONTAP 9.10.1
ONTAP 9.10.1	ONTAP 9.9.1
ONTAP 9.9.1	ONTAP 9.8

복구할 수 있는 대상...	대상...
ONTAP 9.8	ONTAP 9.7
ONTAP 9.7	ONTAP 9.6
ONTAP 9.6	ONTAP 9.5

ONTAP 복원 문제 및 제한 사항

ONTAP 클러스터를 복구하기 전에 되돌리기 문제 및 제한 사항을 고려해야 합니다.

- 되돌리기 - 중단이 발생합니다.

  재버전 중에는 클라이언트 액세스가 발생하지 않습니다. 운영 클러스터를 되돌려주는 경우 계획에 이 운영 중단을 포함해야 합니다.

- 되돌리기 작업은 클러스터의 모든 노드에 영향을 미칩니다.

  이 재버전은 클러스터의 모든 노드에 영향을 미치지만, 다른 HA 쌍을 되돌리기 전에 각 HA 쌍에서 재버전을 수행 및 완료해야 합니다.

  "AFX 스토리지 시스템"복귀를 지원하지 않습니다.

- 모든 노드에서 새 타겟 릴리즈가 실행되고 있으면 재버전이 완료됩니다.

  클러스터가 혼합 버전 상태인 경우, 재조정 요구사항을 충족하는 데 필요한 경우를 제외하고 클러스터 작업 또는 구성을 변경하는 명령을 입력할 수 없으며 모니터링 작업이 허용됩니다.

  > 일부 노드만 되돌렸지만 모든 노드를 되돌린 경우 클러스터를 소스 릴리스로 업그레이드하지 마세요.

- 노드를 되돌리면 Flash Cache 모듈에 캐시된 데이터가 지워집니다.

  Flash Cache 모듈에는 캐싱된 데이터가 없으므로, 노드가 디스크에서 초기 읽기 요청을 처리할 수 있으므로 이 기간 동안 읽기 성능이 저하됩니다. 노드가 읽기 요청을 처리할 때 캐시를 다시 채웁니다.

- ONTAP 9.x에서 실행 중인 테이프에 백업된 LUN은 이전 릴리즈가 아닌 9.x 이상 릴리즈에만 복원할 수 있습니다.
- 현재 버전의 ONTAP가 IBACP(In-Band ACP) 기능을 지원하고 IBACP를 지원하지 않는 ONTAP 버전으로 복원하면 디스크 쉘프의 대체 경로가 비활성화됩니다.
- SVM(스토리지 가상 시스템)에서 LDAP를 사용하는 경우, 다시 버전하기 전에 LDAP 조회를 비활성화해야 합니다.
- MetroCluster 호환이지만 MetroCluster 검증을 받지 않은 스위치를 사용하는 MetroCluster IP 시스템에서 ONTAP 9.7에서 9.6으로 복귀하면 ONTAP 9.6 및 이전 버전을 사용하는 시스템에 대한 지원이 없으므로 중단이 발생합니다.
- 노드를 ONTAP 9.13.1 이전 버전으로 되돌리려면 먼저 암호화된 SVM 루트 볼륨을 암호화되지 않은 볼륨으로 변환해야 합니다

  SVM 루트 볼륨 암호화를 지원하지 않는 ONTAP 버전으로 되돌리려고 하면 시스템은 경고를 표시하고 되돌리기를

차단합니다.

ONTAP 복원을 준비합니다

ONTAP 클러스터를 되돌리기 전에 검토할 리소스

ONTAP 클러스터를 복구하기 전에 하드웨어 지원을 확인하고 리소스를 검토하여 발생 가능하거나 해결해야 할 문제를 파악해야 합니다.

1. 대상 릴리스에 대한 를 "ONTAP 9 릴리즈 노트"검토합니다.

   ""중요 주의 사항" 섹션에서는 다운그레이드 또는 되돌리기 전에 숙지해야 할 잠재적인 문제에 대해 설명합니다.

2. 대상 릴리즈에서 하드웨어 플랫폼이 지원되는지 확인합니다.

   "NetApp Hardware Universe를 참조하십시오"

3. 타겟 릴리즈에서 클러스터 및 관리 스위치가 지원되는지 확인하십시오.

   NX-OS(클러스터 네트워크 스위치), IOS(관리 네트워크 스위치) 및 참조 구성 파일(RCF) 소프트웨어 버전이 되돌리려고 하는 ONTAP 버전과 호환되는지 확인해야 합니다.

   "NetApp 다운로드: Cisco 이더넷 스위치"

4. 클러스터가 SAN용으로 구성된 경우 SAN 구성이 완전히 지원되는지 확인합니다.

   대상 ONTAP 소프트웨어 버전, 호스트 OS 및 패치, 필요한 호스트 유틸리티 소프트웨어, 어댑터 드라이버 및 펌웨어를 비롯한 모든 SAN 구성 요소가 지원되어야 합니다.

   "NetApp 상호 운용성 매트릭스 툴"

ONTAP 클러스터를 되돌리기 전에 수행할 시스템 확인

ONTAP 클러스터를 되돌리려면 먼저 클러스터 상태, 스토리지 상태 및 시스템 시간을 확인해야 합니다. 또한 클러스터에서 실행 중인 작업이 없는지 확인해야 합니다.

클러스터 상태를 확인합니다

ONTAP 클러스터를 되돌리려면 먼저 노드가 정상 상태이고 클러스터에 참여할 자격이 있는지, 클러스터가 쿼럼에 있는지 확인해야 합니다.

단계

1. 클러스터의 노드가 온라인 상태이며 클러스터에 참여할 자격이 있는지 확인합니다.

   ```
   cluster show
   ```

   이 예에서는 모든 노드가 정상 상태이며 클러스터에 참여할 수 있습니다.

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

노드가 정상 상태가 아니거나 적합하지 않은 경우 EMS 로그에서 오류를 확인하고 수정 조치를 취합니다.

2. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

계속하려면 y를 입력하십시오.

3. 각 RDB 프로세스에 대한 구성 세부 정보를 확인합니다.
   - 관계형 데이터베이스 epoch 및 데이터베이스 epoch는 각 노드에 대해 일치해야 합니다.
   - 링당 쿼럼 마스터는 모든 노드에 대해 동일해야 합니다.

     각 링에는 다른 쿼럼 마스터가 있을 수 있습니다.

이 **RDB** 프로세스를 표시하려면...	이 명령을 입력하십시오...
기능과	`cluster ring show -unitname mgmt`
볼륨 위치 데이터베이스	`cluster ring show -unitname vldb`
Virtual-Interface Manager를 참조하십시오	`cluster ring show -unitname vifmgr`
SAN 관리 데몬	`cluster ring show -unitname bcomd`

이 예에서는 볼륨 위치 데이터베이스 프로세스를 보여 줍니다.

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

5. SAN 환경에서 작동 중인 경우 각 노드가 SAN 쿼럼에 있는지 확인합니다.

```
event log show  -severity informational -message-name scsiblade.*
```

각 노드에 대한 가장 최근의 scsib블레이드 이벤트 메시지는 SCSI 블레이드가 quorum에 있음을 나타내야 합니다.

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time              Node       Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

관련 정보

"시스템 관리"

스토리지 상태를 확인합니다

ONTAP 클러스터를 되돌리려면 먼저 디스크, 애그리게이트 및 볼륨의 상태를 확인해야 합니다.

단계

1. 디스크 상태 확인:

확인하려면...	수행할 작업...
손상된 디스크	a. 손상된 디스크를 표시합니다. `storage disk show -state broken` b. 손상된 디스크를 제거하거나 교체합니다.
유지보수 또는 재구성이 진행 중인 디스크	a. 유지 보수, 보류 또는 재구성 상태의 디스크를 표시합니다. `storage disk show -state maintenance`
pending	reconstructing ---- .. 유지보수 또는 재구성 작업이 완료될 때까지 기다린 후 계속 진행하십시오.

2. 스토리지 애그리게이트를 포함하여 물리적 스토리지와 논리적 스토리지의 상태를 표시하여 모든 애그리게이트가 온라인 상태인지 확인합니다

```
storage aggregate show -state !online
```

이 명령은 _not_online 인 애그리게이트를 표시합니다. 주요 업그레이드 또는 리버전을 수행하기 전과 후의 모든 애그리게이트는 온라인 상태여야 합니다.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. _NOT_ONLINE 상태인 볼륨을 표시하여 모든 볼륨이 온라인 상태인지 확인합니다.

```
volume show -state !online
```

주요 업그레이드 또는 재버전을 수행하기 전과 후에 모든 볼륨이 온라인 상태여야 합니다.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. 일치하지 않는 볼륨이 없는지 확인합니다.

```
volume show -is-inconsistent true
```

를 참조하십시오"NetApp 지식 기반: 볼륨에 WAFL 일관되지 않음 표시" 일관되지 않은 볼륨을 해결하는 방법에 대해.

관련 정보

"디스크 및 애그리게이트 관리"

시스템 시간을 확인합니다

ONTAP 클러스터를 되돌리려면 먼저 NTP가 구성되어 있고 클러스터 전체에서 시간이 동기화되는지 확인해야 합니다.

단계

1. 클러스터가 NTP 서버와 연결되어 있는지 확인합니다.

```
cluster time-service ntp server show
```

2. 각 노드의 날짜와 시간이 동일한지 확인합니다.

```
cluster date show
```

```
cluster1::> cluster date show
Node      Date                Timezone
--------- ------------------- -------------------------
node0     4/6/2013 20:54:38   GMT
node1     4/6/2013 20:54:38   GMT
node2     4/6/2013 20:54:38   GMT
node3     4/6/2013 20:54:38   GMT
4 entries were displayed.
```

실행 중인 작업이 없는지 확인합니다

ONTAP 클러스터를 되돌리려면 먼저 클러스터 작업의 상태를 확인해야 합니다. 집계, 볼륨, NDMP(덤프 또는 복원) 또는 스냅샷 작업(예: 생성, 삭제, 이동, 수정, 복제 및 마운트 작업)이 실행 중이거나 대기 중인 경우 작업이 성공적으로 완료되도록 허용하거나 대기 중인 항목을 중지해야 합니다.

단계

1. 실행 중이거나 대기열에 있는 집계, 볼륨 또는 스냅샷 작업의 목록을 검토합니다.

```
job show
```

이 예에서는 대기열에 있는 두 개의 작업이 있습니다.

```
cluster1::> job show
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
8629   Vol Reaper           cluster1   -              Queued
       Description: Vol Reaper Job
8630   Certificate Expiry Check
                            cluster1   -              Queued
       Description: Certificate Expiry Check
```

2. 실행 중이거나 대기열에 있는 모든 집계, 볼륨 또는 스냅샷 작업을 삭제합니다.

```
job delete -id <job_id>
```

3. 집계, 볼륨 또는 스냅샷 작업이 실행 중이거나 대기열에 있는지 확인합니다.

```
job show
```

이 예에서는 실행 중인 작업과 대기열에 있는 작업이 모두 삭제되었습니다.

```
cluster1::> job show
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
9944   SnapMirrorDaemon_7_2147484678
                            cluster1   node1          Dormant
       Description: Snapmirror Daemon for 7_2147484678
18377  SnapMirror Service Job
                            cluster1   node0          Dormant
       Description: SnapMirror Service Job
2 entries were displayed
```

관련 정보

- "저장 디스크 표시"

ONTAP 버전별 되돌리기 전 검사를 수행합니다

ONTAP 버전에 필요한 되돌리기 전 작업

ONTAP 버전에 따라 되돌리기 프로세스를 시작하기 전에 추가 준비 작업을 수행해야 할 수도

있습니다.

다음으로 되돌리는 경우...	되돌리기 프로세스를 시작하기 전에 다음을 수행하십시오.
모든 ONTAP 9 버전	• "지속적으로 사용할 수 없는 SMB 세션을 종료합니다".. • "SnapMirror 및 SnapVault 관계에 대한 개정 요구사항을 검토합니다".. • "중복제거된 볼륨에 충분한 여유 공간이 있는지 확인합니다".. • "스냅샷을 준비합니다".. • "SnapLock 볼륨의 자동 커밋 기간을 시간 으로 설정합니다".. • MetroCluster 구성이 있는 경우"자동 계획되지 않은 전환을 비활성화합니다" • "비정상적인 활동에 대한 자율적 랜섬웨어 방어 경고에 대응"되돌리기 전에.
ONTAP 9.18.1	• ONTAP 9.18.1 업그레이드의 일부로 ARP에 대한 자동 활성화가 설정된 경우 "사용하지 않도록 설정합니다"해야 합니다.
ONTAP 9.17.1	• SAN에 대해 ONTAP ARP 기능을 활성화한 경우 "사용하지 않도록 설정합니다" .
ONTAP 9.16.1	• NVMe/TCP 연결을 위해 TLS를 구성한 경우"NVMe 호스트에서 TLS 구성을 사용하지 않도록 설정합니다", • 확장 qtree 성능 모니터링을 활성화한 "사용하지 않도록 설정합니다"경우, • CORS를 사용하여 ONTAP S3 버킷에 액세스하는 경우"CORS 구성을 제거합니다"
ONTAP 9.14.1	클라이언트 연결에 대해 트렁킹을 설정한 경우"모든 NFSv4.1 서버에서 트렁킹을 해제합니다",
ONTAP 9.12.1	• NAS 데이터에 대해 S3 클라이언트 액세스를 구성한 경우 "S3 NAS 버킷 구성을 제거합니다." • NVMe 프로토콜을 실행 중이고 대역 내 인증을 구성한 경우,"대역내 인증을 비활성화합니다" • MetroCluster 구성이 있는 경우"IPsec을 비활성화합니다"
ONTAP 9.11.1	ARP(Autonomous 랜섬웨어 Protection)를 구성한 경우 ,"ARP 라이센스를 확인합니다"

다음으로 되돌리는 경우...	되돌리기 프로세스를 시작하기 전에 다음을 수행하십시오.
ONTAP 9.6	SnapMirror 동기식 관계가 있는 "되돌릴 관계를 준비합니다"경우,

모든 **ONTAP 9** 버전

ONTAP를 되돌리기 전에 특정 **SMB** 세션을 종료하십시오

ONTAP 9의 모든 버전에서 ONTAP 클러스터를 되돌리려면 먼저 지속적으로 사용할 수 없는 SMB 세션을 식별하고 올바르게 종료해야 합니다.

Hyper-V 또는 Microsoft SQL Server 클라이언트가 SMB 3.0 프로토콜을 사용하여 액세스하는 지속적으로 사용 가능한 SMB 공유는 업그레이드 또는 다운그레이드하기 전에 종료할 필요가 없습니다.

단계

1. 지속적으로 사용할 수 없는 설정된 SMB 세션을 식별합니다.

```
vserver cifs session show -continuously-available No -instance
```

이 명령은 무중단 가용성이 없는 SMB 세션에 대한 자세한 정보를 표시합니다. ONTAP 다운그레이드를 진행하기 전에 종료해야 합니다.

```
cluster1::> vserver cifs session show -continuously-available No
-instance

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
      Workstation IP address: 203.0.113.20
    Authentication Mechanism: NTLMv2
                Windows User: CIFSLAB\user1
                   UNIX User: nobody
                 Open Shares: 1
                  Open Files: 2
                  Open Other: 0
              Connected Time: 8m 39s
                   Idle Time: 7m 45s
           Protocol Version: SMB2_1
      Continuously Available: No
1 entry was displayed.
```

2. 필요한 경우 확인한 각 SMB 세션에 대해 열려 있는 파일을 확인합니다.

```
vserver cifs session file show -session-id session_ID
```

```
cluster1::> vserver cifs session file show -session-id 1

Node:       node1
Vserver:    vs1
Connection: 4160072788
Session:    1
File    File      Open Hosting
Continuously
ID      Type      Mode Volume          Share                 Available
------- --------- ---- --------------- ---------------------
------------
1       Regular   rw   vol10           homedirshare          No
Path: \TestDocument.docx
2       Regular   rw   vol10           homedirshare          No
Path: \file1.txt
2 entries were displayed.
```

SnapMirror 및 **SnapVault** 관계에 대한 **ONTAP** 복원 요구사항

이 `system node revert-to` 명령은 되돌리기 프로세스를 완료하기 위해 삭제 또는 재구성해야 하는 SnapMirror 및 SnapVault 관계를 알려 줍니다. 그러나 재버전을 시작하기 전에 이러한 요구 사항을 알고 있어야 합니다.

- 모든 SnapVault 및 데이터 보호 미러링 관계를 중지했다가 해제해야 합니다.

  재버전이 완료된 후 공통 스냅샷이 있는 경우 이러한 관계를 다시 동기화하고 재개할 수 있습니다.

- SnapVault 관계에는 다음 SnapMirror 정책 유형이 포함되지 않아야 합니다.
  - 비동기식 - 미러

    이 정책 유형을 사용하는 모든 관계를 삭제해야 합니다.

  - MirrorAndVault를 선택합니다

    이러한 관계가 있으면 SnapMirror 정책을 미러 볼트로 변경해야 합니다.
- 모든 로드 공유 미러 관계 및 대상 볼륨을 삭제해야 합니다.
- FlexClone 대상 볼륨과의 SnapMirror 관계를 삭제해야 합니다.
- 각 SnapMirror 정책에 대해 네트워크 압축을 해제해야 합니다.
- ALL_SOURCE_SNSHOT 규칙을 모든 비동기식 미러 유형 SnapMirror 정책에서 제거해야 합니다.

단일 파일 스냅샷 복원(SFSR) 및 부분 파일 스냅샷 복원(PFSR) 작업은 루트 볼륨에서 더 이상 사용되지 않습니다.

- 현재 실행 중인 단일 파일 및 스냅샷 복구 작업은 재버전을 진행하기 전에 완료해야 합니다.

  복원 작업이 완료될 때까지 기다리거나 작업을 중단할 수 있습니다.

- 불완전한 단일 파일 및 스냅샷 복구 작업은 명령을 사용하여 제거해야 `snapmirror restore` 합니다.

  에 대한 자세한 내용은 `snapmirror restore` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP를 되돌리기 전에 중복제거된 볼륨의 여유 공간을 확인하십시오

모든 ONTAP 9 버전에서 ONTAP 클러스터를 되돌리려면 먼저 되돌리기 작업을 위해 볼륨에 충분한 여유 공간이 있는지 확인해야 합니다.

볼륨에는 0 블록의 인라인 감지를 통해 달성된 절감을 수용할 수 있는 충분한 공간이 있어야 합니다. 를 참조하십시오"NetApp 지식 기반: ONTAP 9에서 중복 제거, 압축 및 압축을 통해 공간 절약 효과를 확인하는 방법" .

되돌리려는 볼륨에서 중복제거 및 데이터 압축을 모두 사용하도록 설정한 경우, 중복제거를 되돌리기 전에 데이터 압축을 되돌려야 합니다.

단계

1. 볼륨에 대해 실행 중인 효율성 작업의 진행 상황을 봅니다.

```
volume efficiency show -fields vserver,volume,progress
```

2. 모든 활성 및 대기 중인 중복 제거 작업을 중지합니다.

```
volume efficiency stop -vserver <svm_name> -volume <volume_name> -all
```

3. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

4. 볼륨의 효율성 메타데이터를 ONTAP의 대상 버전으로 다운그레이드:

```
volume efficiency revert-to -vserver <svm_name> -volume <volume_name>
-version <version>
```

다음 예에서는 볼륨 VolA의 효율성 메타데이터를 ONTAP 9.x로 되돌립니다

```
volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x
```

볼륨 효율성 되돌리기-to 명령은 이 명령이 실행되는 노드에 있는 볼륨을 되돌립니다. 이 명령은 노드 간에 볼륨을 되돌리지 않습니다.

5. 다운그레이드 진행 상황 모니터링:

```
volume efficiency show -vserver <svm_name> -op-status Downgrading
```

6. 되돌리기에 성공하지 못하면 인스턴스를 표시하여 되돌리기가 실패한 이유를 확인합니다.

```
volume efficiency show -vserver <svm_name> -volume <volume_name> -
instance
```

7. 되돌리기 작업이 완료된 후 admin 권한 수준으로 돌아갑니다.

```
set -privilege admin
```

에 대해 자세히 "논리적 스토리지 관리"알아보십시오.

ONTAP 클러스터를 되돌리기 전에 스냅샷을 준비합니다

모든 ONTAP 9 버전에서 ONTAP 클러스터를 되돌리려면 먼저 모든 스냅샷 정책을 사용하지 않도록 설정하고 현재 릴리즈로 업그레이드한 후에 생성된 모든 스냅샷을 삭제해야 합니다.

SnapMirror 환경에서 되돌리는 경우 먼저 다음과 같은 미러링 관계를 삭제해야 합니다.

- 모든 로드 공유 미러 관계
- ONTAP 8.3.x에서 생성된 모든 데이터 보호 미러링 관계
- ONTAP 8.3.x에서 클러스터가 다시 생성된 경우 모든 데이터 보호 미러링 관계가 형성됩니다

단계

1. 모든 데이터 SVM에 대해 스냅샷 정책 비활성화:

```
volume snapshot policy modify -vserver * -enabled false
```

2. 각 노드의 애그리게이트에 대해 스냅샷 정책 비활성화:
   a. 노드의 애그리게이트를 식별합니다.

```
run -node <nodename> -command aggr status
```

b. 각 애그리게이트에 대해 스냅샷 정책을 사용하지 않도록 설정합니다.

```
run -node <nodename> -command aggr options aggr_name nosnap on
```

c. 나머지 각 노드에 대해 이 단계를 반복합니다.

3. 각 노드의 루트 볼륨에 대해 스냅샷 정책을 사용하지 않도록 설정합니다.

a. 노드의 루트 볼륨 식별:

```
run -node <node_name> -command vol status
```

명령 출력의 * Options * 열에서 root 라는 단어로 루트 볼륨을 `vol status` 식별합니다.

```
vs1::> run -node node1 vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

a. 루트 볼륨에서 스냅샷 정책을 해제합니다.

```
run -node <node_name> vol options root_volume_name nosnap on
```

b. 나머지 각 노드에 대해 이 단계를 반복합니다.

4. 현재 릴리즈로 업그레이드한 후 생성된 모든 스냅샷을 삭제합니다.

a. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

b. 스냅샷을 비활성화합니다.

```
snapshot policy modify -vserver * -enabled false
```

c. 노드의 최신 버전 스냅샷을 삭제합니다.

```
volume snapshot prepare-for-revert -node <node_name>
```

이 명령은 각 데이터 볼륨, 루트 애그리게이트 및 루트 볼륨에서 최신 버전의 스냅샷을 삭제합니다.

스냅샷을 삭제할 수 없는 경우 명령이 실패하고 스냅샷을 삭제하기 전에 수행해야 하는 모든 필요한 작업을 알립니다. 다음 단계로 진행하기 전에 필요한 작업을 완료한 다음 명령을 다시 실행해야 `volume snapshot prepare-for-revert` 합니다.

```
cluster1::*> volume snapshot prepare-for-revert -node node1

Warning: This command will delete all snapshots that have the format
used by the current version of ONTAP. It will fail if any snapshot
policies are enabled, or
         if any snapshots have an owner. Continue? {y|n}: y
```

a. 스냅샷이 삭제되었는지 확인합니다.

```
volume snapshot show -node nodename
```

b. 최신 버전의 스냅샷이 남아 있는 경우 강제로 삭제합니다.

```
volume snapshot delete {-fs-version 9.0 -node nodename -is
-constituent true} -ignore-owners -force
```

c. 나머지 각 노드에 대해 이 단계를 반복합니다.

d. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

MetroCluster 구성의 두 클러스터에서 이 단계를 수행해야 합니다.

SnapLock 볼륨을 되돌리기 전에 **ONTAP** 볼륨에 대해 자동 커밋 기간을 설정합니다

ONTAP 9의 모든 버전에서 ONTAP 클러스터를 되돌리려면 먼저 SnapLock 볼륨에 대한 자동 커밋 기간의 값을 며칠이 아닌 몇 시간 내에 설정해야 합니다. SnapLock 볼륨의 자동 커밋 값을 확인하고 필요한 경우 며칠에서 몇 시간으로 수정해야 합니다.

단계

1. 클러스터에 지원되지 않는 자동 커밋 기간이 있는 SnapLock 볼륨이 있는지 확인합니다.

```
volume snaplock show -autocommit-period *days
```

2. 지원되지 않는 자동 커밋 기간을 시간 단위로 수정합니다

```
volume snaplock modify -vserver <vserver_name> -volume <volume_name>
-autocommit-period value hours
```

MetroCluster 구성을 되돌리기 전에 자동 계획되지 않은 전환을 비활성화합니다.

ONTAP 9 버전을 실행하는 MetroCluster 구성을 되돌리려면 자동 계획되지 않은 전환(AUSO)을 비활성화해야 합니다.

단계

1. MetroCluster의 클러스터 모두에서 계획되지 않은 자동 전환이 사용되지 않도록 설정합니다.

```
metrocluster modify -auto-switchover-failure-domain auso-disabled
```

관련 정보

"MetroCluster 관리 및 재해 복구"

ONTAP 되돌리기 전에 **ARP(Autonomous Ransomware Protection)**에서 활동 경고를 해결합니다.

ONTAP 9.17.1 또는 이전 버전으로 되돌리기 전에 ARP(Autonomous Ransomware Protection)에서 보고된 비정상 활동 경고에 대응하고 관련된 ARP 스크린샷을 삭제해야 합니다.

시작하기 전에

ARP 스냅샷을 삭제하려면 "고급" 권한이 필요합니다.

단계

1. 에서 보고한 비정상적인 활동 경고에 응답하고 "아프"잠재적인 문제를 해결합니다.
2. 이러한 문제가 해결되었는지 확인한 후, *의심스러운 파일 유형 업데이트 및 지우기*를 선택하여 결정을 기록하고 정상적인 ARP 모니터링을 재개합니다.
3. 다음 명령을 실행하여 경고와 관련된 ARP 스크린샷을 나열하세요.

```
volume snapshot snapshot show -fs-version 9.18
```

4. 경고와 관련된 모든 ARP 스크린샷을 삭제하세요.

> ⓘ 이 명령은 ONTAP 의 현재 버전에서 사용하는 형식을 가진 모든 스냅샷을 삭제하며, ARP 스냅샷만 삭제하는 것은 아닙니다. 이 명령을 실행하기 전에 제거될 모든 스냅샷에 대해 필요한 조치를 취했는지 확인하세요.

```
volume snapshot prepare-for-revert -node <node_name>
```

ONTAP 9.18.1

ONTAP 9.18.1에서 이전 버전으로 되돌리기 전에 자율형 랜섬웨어 보호 기능의 자동 활성화를 비활성화하십시오

볼륨을 ONTAP 9.18.1로 업그레이드한 경우, 짧은 유예 기간(12시간) 후 ONTAP ARP 자동 활성화가 볼륨에 대해 설정되었을 수 있습니다. ONTAP 9.17.1 또는 이전 버전으로 되돌리기 전에 ONTAP 9.18.1로 업그레이드된 볼륨에서 이 자동 활성화 설정을 비활성화하는 것이 좋습니다.

단계

1. ONTAP 9.18.1 이상으로 업그레이드된 볼륨에서 자동 활성화 옵션이 활성화되었는지 확인합니다.

```
security anti-ransomware auto-enable show
```

2. SVM의 모든 볼륨에서 랜섬웨어 보호에 대한 자동 활성화 옵션을 비활성화합니다.

```
security anti-ransomware volume disable -volume * -auto-enabled-volumes
-only true
```

ONTAP 9.17.1

ONTAP 9.17.1에서 복귀하기 전에 **SAN** 볼륨에서 자율 랜섬웨어 보호 기능을 비활성화하세요**.**

SAN 볼륨에 대한 ONTAP ARP 기능은 ONTAP 9.16.1 이하 버전에서는 지원되지 않습니다. ONTAP 9.16.1 이하 버전으로 되돌리기 전에 SAN 볼륨에서 ARP 기능을 비활성화하는 것이 좋습니다. 이렇게 하면 해당 기능이 활성 상태로 유지되어 되돌린 버전에서 실제 감지를 수행하지 않고 CPU 및 디스크 리소스를 사용하는 것을 방지할 수 있습니다.

예 **7.** 단계

시스템 관리자

1. *저장소 > 볼륨*을 선택한 다음 볼륨 이름을 선택합니다.
2. 볼륨 개요의 보안 탭에서 *상태*를 선택하여 사용에서 사용 안 함으로 전환합니다.

CLI를 참조하십시오

1. 볼륨에서 랜섬웨어 보호 비활성화:

```
security anti-ransomware volume disable -volume <vol_name> -vserver
<svm_name>
```

ONTAP 9.16.1

ONTAP 9.16.1에서 되돌리기 전에 **NVMe** 호스트에서 **TLS**를 사용하지 않도록 설정합니다

NVMe 호스트에 NVMe/TCP 연결을 위한 TLS 보안 채널이 구성되어 있는 경우, ONTAP 9.16.1에서 클러스터를 복구하기 전에 이 채널을 비활성화해야 합니다.

단계

1. 호스트에서 TLS 보안 채널 구성을 제거합니다.

```
vserver nvme subsystem host unconfigure-tls-for-revert -vserver
<svm_name> -subsystem <subsystem> -host-nqn <host_nqn>
```

이 명령은 서브시스템에서 호스트를 제거한 다음 TLS 구성 없이 서브시스템에서 호스트를 다시 생성합니다.

2. TLS 보안 채널이 호스트에서 제거되었는지 확인합니다.

```
vserver nvme subsystem host show
```

ONTAP 9.16.1에서 되돌리기 전에 확장 **Qtree** 성능 모니터링을 비활성화하십시오

ONTAP 9.16.1부터 ONTAP REST API를 사용하여 지연 시간 메트릭 및 기간별 통계를 비롯한 확장된 qtree 모니터링 기능에 액세스할 수 있습니다. 모든 qtree에서 확장 모니터링이 활성화되어 있는 경우 9.16.1에서 되돌리려면 먼저 false로 설정해야 합니다 `ext_performance_monitoring.enabled`.

에 대해 자세히 "확장된 qtree 성능 모니터링으로 클러스터 되돌리기"알아보십시오.

ONTAP 9.16.1에서 되돌리기 전에 **CORS** 구성을 제거합니다

CORS(Cross-Origin Resource Sharing)를 사용하여 ONTAP S3 버킷을 액세스하는 경우 ONTAP 9.16.1에서 되돌리기 전에 이를 제거해야 합니다.

에 대해 자세히 "CORS를 사용하여 ONTAP 클러스터 되돌리기"알아보십시오.

ONTAP 9.14.1

ONTAP 9.14.1에서 되돌리기 전에 **NFSv4.1** 세션 트렁킹을 해제합니다

클라이언트 연결에 대해 트렁킹을 사용하도록 설정한 경우 ONTAP 9.14.1에서 되돌리기 전에 모든 NFSv4.1 서버에서 트렁킹을 해제해야 합니다.

를 입력할 때 `revert-to` 명령을 실행하면 계속하기 전에 트렁킹을 해제하라는 경고 메시지가 표시됩니다.

ONTAP 9.13.1로 되돌리면 트렁킹된 연결을 사용하는 클라이언트가 다시 단일 연결을 사용하는 것으로 전환됩니다. 이러한 데이터 처리량에 영향을 주지만 중단은 없습니다. 되돌리기 동작은 SVM에 대한 NFSv4.1 트렁킹 옵션을 Enabled에서 Disabled로 수정하는 것과 동일합니다.

단계

1. NFSv4.1 서버에서 트렁킹을 해제합니다.

```
vserver nfs modify -vserver _svm_name_ -v4.1-trunking disabled
```

2. NFS가 원하는 대로 구성되었는지 확인합니다.

```
vserver nfs show -vserver _svm_name_
```

ONTAP 9.12.1

ONTAP 9.12.1에서 되돌리기 전에 **S3 NAS** 버킷 구성을 제거합니다

NAS 데이터에 대해 S3 클라이언트 액세스를 구성한 경우 ONTAP 9.12.1에서 되돌리기 전에 ONTAP CLI(Command Line Interface)를 사용하여 NAS 버킷 구성을 제거하고 이름 매핑(S3 사용자를 Windows 또는 Unix 사용자로)을 제거해야 합니다.

이 작업에 대해

되돌리기 프로세스 동안 백그라운드에서 다음 작업이 완료됩니다.

- 부분적으로 완료된 모든 Singleton 개체 만들기(즉, 숨겨진 디렉터리의 모든 항목)를 제거합니다.
- 숨겨진 디렉토리를 모두 제거합니다. S3 NAS 버킷에서 매핑된 내보내기 루트에서 액세스할 수 있는 각 볼륨에 대해 하나가 있을 수 있습니다.
- 업로드 테이블을 제거합니다.
- 구성된 모든 S3 서버에 대해 default-unix-user 및 default-windows-user 값을 삭제합니다.

단계

1. S3 NAS 버킷 구성 제거:

```
vserver object-store-server bucket delete -vserver <svm_name> -bucket
<s3_nas_bucket_name>
```

에 대한 자세한 내용은 `vserver object-store-server bucket delete` "ONTAP 명령 참조입니다"을 참조하십시오.

2. UNIX에 대한 이름 매핑 제거:

```
vserver name-mapping delete -vserver <svm_name> -direction s3-unix
```

에 대한 자세한 내용은 `vserver name-mapping delete` "ONTAP 명령 참조입니다"을 참조하십시오.

3. Windows에 대한 이름 매핑 제거:

```
vserver name-mapping delete -vserver <svm_name> -direction s3-win
```

4. SVM에서 S3 프로토콜 제거:

```
vserver remove-protocols -vserver <svm_name> -protocols s3
```

에 대한 자세한 내용은 `vserver remove-protocols` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 9.12.1에서 되돌리기 전에 **NVMe** 대역 내 인증을 비활성화한다

NVMe 프로토콜을 실행 중인 경우 클러스터를 ONTAP 9.12.1에서 되돌리기 전에 대역 내 인증을 비활성화해야 합니다. DH-HMAC-CHAP를 사용한 대역내 인증이 해제되지 않은 경우 되돌리기가 실패합니다.

단계

1. DH-HMAC-CHAP 인증을 비활성화하려면 서브시스템에서 호스트를 제거합니다.

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. DH-HMAC-CHAP 인증 프로토콜이 호스트에서 제거되었는지 확인합니다.

```
vserver nvme subsystem host show
```

3. 인증 없이 호스트를 하위 시스템에 다시 추가합니다.

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

ONTAP 9.12.1에서 되돌리기 전에 **MetroCluster** 구성에서 **IPsec**을 비활성화합니다

ONTAP 9.12.1에서 MetroCluster 구성을 되돌리려면 먼저 IPsec을 비활성화해야 합니다.

MetroCluster 구성 내에 IPsec 구성이 없는지 확인하기 위해 되돌리기 전에 검사가 수행됩니다. 복원을 계속하기 전에 존재하는 IPsec 구성을 제거하고 IPsec을 비활성화해야 합니다. 사용자 정책을 구성하지 않은 경우에도 IPsec을 사용하도록 설정하면 ONTAP를 되돌릴 수 없습니다.

ONTAP 9.11.1

ONTAP 9.11.1에서 되돌리기 전에 자율적 랜섬웨어 방어 라이센스를 확인하십시오

ARP(자율적 랜섬웨어 방어)를 구성한 후 ONTAP 9.11.1에서 ONTAP 9.10.1로 되돌리면 경고 메시지와 제한된 ARP 기능이 발생할 수 있습니다.

ONTAP 9.11.1에서 Anti-랜섬웨어 라이센스는 멀티 테넌트 키 관리(MTKM) 라이센스를 대체합니다. 시스템에 Anti_랜섬웨어 라이센스가 있지만 MT_EK_MGMT 라이센스가 없는 경우 되돌리기 중에 ARP가 새 볼륨에 대해 활성화될 수 없다는 경고가 표시됩니다.

기존 보호 기능이 있는 볼륨은 복원 후에도 계속 정상적으로 작동하며 ONTAP CLI를 사용하여 ARP 상태를 표시할 수 있습니다. MTKM 라이센스가 없으면 System Manager에서 ARP 상태를 표시할 수 없습니다.

따라서 ONTAP 9.10.1로 되돌린 후 ARP를 계속하려면 되돌리기 전에 MTKM 라이센스가 설치되어 있는지 확인하십시오. "ARP 라이센스에 대해 알아보십시오."

ONTAP 9.6

SnapMirror 동기식 관계를 사용하여 **ONTAP 9.6**에서 시스템을 되돌리기 위한 고려 사항

ONTAP 9 .6에서 ONTAP 9.5로 되돌리려면 먼저 SnapMirror 동기 관계에 대한 고려 사항을 알고 있어야 합니다.

SnapMirror 동기식 관계가 있는 경우 되돌리기 전에 다음 단계를 수행해야 합니다.

- 소스 볼륨에서 NFSv4 또는 SMB를 통해 데이터를 제공하는 SnapMirror 동기식 관계를 삭제해야 합니다.

  ONTAP 9.5는 NFSv4 및 SMB를 지원하지 않습니다.

- 미러 계단식 구축 환경에서는 SnapMirror 동기식 관계를 모두 삭제해야 합니다.

  미러-미러 캐스케이드 구축은 ONTAP 9.5의 SnapMirror 동기식 관계에 대해서는 지원되지 않습니다.

- 되돌리기 중에 ONTAP 9.5의 공통 스냅샷을 사용할 수 없는 경우 되돌리기 후 SnapMirror 동기식 관계를 초기화해야 합니다.

ONTAP 9.6으로 2시간 동안 업그레이드한 후 ONTAP 9.5의 일반 스냅샷이 ONTAP 9.6의 일반 스냅샷으로 자동 대체됩니다. 따라서 ONTAP 9.5의 일반 스냅샷을 사용할 수 없는 경우 복구한 후 SnapMirror 동기식 관계를 다시 동기화할 수 없습니다.

ONTAP 소프트웨어 이미지를 다운로드하고 설치합니다

현재 ONTAP 소프트웨어를 되돌리려면 먼저 NetApp Support 사이트에서 대상 소프트웨어 버전을 다운로드한 다음 설치해야 합니다.

ONTAP 소프트웨어 이미지 다운로드

소프트웨어 이미지는 플랫폼 모델에 따라 다릅니다. 클러스터에 맞는 올바른 이미지를 얻어야 합니다. 플랫폼 모델의 소프트웨어 이미지, 펌웨어 버전 정보 및 최신 펌웨어는 NetApp Support 사이트에서 제공됩니다. 소프트웨어 이미지에는 특정 버전의 ONTAP가 릴리스되었을 때 사용할 수 있는 최신 버전의 시스템 펌웨어가 포함되어 있습니다.

ONTAP 9.5 이상에서 NetApp 볼륨 암호화를 사용하여 시스템을 되돌리는 경우 NetApp 볼륨 암호화를 포함하는 비제한 국가의 ONTAP 소프트웨어 이미지를 다운로드해야 합니다. 제한된 국가의 ONTAP 소프트웨어 이미지를 사용하여 NetApp 볼륨 암호화로 시스템을 되돌리면 시스템이 패닉 상태가 되어 볼륨에 액세스할 수 없게 됩니다.

단계

1. "소프트웨어 다운로드"NetApp Support 사이트 영역에서 대상 ONTAP 소프트웨어를 찾습니다.
2. 소프트웨어 이미지를 복사합니다(예: `97_q_image.tgz`) NetApp 지원 사이트에서

   이미지를 제공할 HTTP 서버 또는 FTP 서버의 디렉토리 또는 로컬 폴더로 복사할 수 있습니다.

ONTAP 소프트웨어 이미지를 설치합니다

NetApp Support 사이트에서 타겟 ONTAP 소프트웨어 이미지를 다운로드한 후 클러스터 노드에 설치합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   ```
   set -privilege advanced
   ```

   고급 프롬프트('*>')가 나타납니다.

2. 메시지가 표시되면 를 `y` 입력하여 계속합니다.
3. 소프트웨어 이미지를 설치합니다.
   - 표준 구성 또는 2노드 MetroCluster 구성의 경우 다음 명령을 입력합니다.

     ```
     system node image update -node * -package
     <http://example.com/downloads/image.tgz> -replace-package true
     -replace {image1|image2} -background true -setdefault true
     ```

이 명령은 모든 노드에 소프트웨어 이미지를 동시에 다운로드하고 설치합니다. 이미지를 한 번에 하나씩 다운로드하여 설치하려면 매개 변수를 지정하지 마십시오 `-background`. 또한 이 명령은 확장 쿼리를 사용하여 대체 이미지로 설치된 대상 소프트웨어 이미지를 노드의 기본 이미지로 변경합니다.

◦ 4노드 또는 8노드 MetroCluster 구성의 경우 두 클러스터에서 다음 명령을 입력합니다.

```
system node image update -node * -package
<http://example.com/downloads/image.tgz> -replace-package true
-replace {image1|image2} -background true -setdefault false
```

이 명령은 모든 노드에 소프트웨어 이미지를 동시에 다운로드하고 설치합니다. 이미지를 한 번에 하나씩 다운로드하여 설치하려면 매개 변수를 지정하지 마십시오 `-background`. 또한 이 명령은 확장 쿼리를 사용하여 각 노드에 대체 이미지로 설치되는 대상 소프트웨어 이미지를 변경합니다.

4. 메시지가 나타나면 y를 입력하여 계속합니다.
5. 각 노드에 소프트웨어 이미지가 다운로드되고 설치되어 있는지 확인합니다.

```
system node image show-update-progress -node *
```

이 명령은 소프트웨어 이미지 다운로드 및 설치의 현재 상태를 표시합니다. 모든 노드가 *실행 상태*가 "종료"이고, *종료 상태*가 "성공"이라고 보고할 때까지 이 명령을 계속 실행해야 합니다.

시스템 노드 이미지 업데이트 명령이 실패하고 오류 또는 경고 메시지가 표시될 수 있습니다. 오류 또는 경고를 해결한 후에는 명령을 다시 실행할 수 있습니다.

이 예는 소프트웨어 이미지가 다운로드되어 두 노드에 성공적으로 설치되는 2노드 클러스터를 보여줍니다.

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

관련 정보

- "시스템 노드 이미지 업데이트"

ONTAP 클러스터를 되돌립니다

ONTAP 클러스터를 되돌리는 것은 중단이 발생합니다. 재버전을 수행할 때는 클러스터를 오프라인으로 전환해야 합니다. 기술 지원의 도움 없이 운영 클러스터를 되돌리면 안 됩니다.

새 클러스터를 되돌리거나 테스트 클러스터를 되돌리려면 스토리지 페일오버 및 데이터 LIF와 주소 변환 사전 조건을 사용하지 않도록 설정해야 합니다. 그런 다음 클러스터의 각 노드에서 클러스터 및 파일 시스템 구성을 되돌려야 합니다.

시작하기 전에.

- 를 완료했어야 "복원 전 검증"합니다.
- 필수 항목을 완료해야 "특정 ONTAP 버전을 미리 확인합니다"합니다.
- 당신은해야합니다 "대상 ONTAP 소프트웨어 이미지를 다운로드하고 설치했습니다." .

1단계**:** 재버전을 위해 클러스터를 준비합니다

클러스터 노드를 되돌리려면 먼저 타겟 ONTAP 이미지가 설치되었는지 확인하고 클러스터에서 모든 데이터 LIF를 비활성화해야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   ```
   set -privilege advanced
   ```

   계속하라는 메시지가 나타나면 * y * 를 입력합니다.

2. 대상 ONTAP 소프트웨어가 설치되었는지 확인합니다.

   ```
   system image show
   ```

   다음 예에서는 버전 9.13.1 이 두 노드에 대체 이미지로 설치되어 있음을 보여 줍니다.

```
cluster1::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   true    true    9.14.1       MM/DD/YYYY TIME
         image2   false   false   9.13.1       MM/DD/YYYY TIME
node1
         image1   true    true    9.14.1       MM/DD/YYYY TIME
         image2   false   false   9.13.1       MM/DD/YYYY TIME
4 entries were displayed.
```

3. 클러스터의 모든 데이터 LIF를 비활성화합니다.

```
network interface modify {-role data} -status-admin down
```

4. 클러스터 간 FlexCache 관계가 있는지 확인:

```
flexcache origin show-caches -relationship-type inter-cluster
```

5. 클러스터 간 변통이 있는 경우 캐시 클러스터에서 데이터 리프터를 해제합니다.

```
network interface modify -vserver <vserver_name> -lif <lif_name> -status
-admin down
```

2단계**:** 클러스터 노드 되돌리기

클러스터를 되돌리려면 HA 페어의 첫 번째 노드를 되돌린 다음 파트너 노드를 되돌려야 합니다. 그런 다음 모든 노드가 되돌려질 때까지 클러스터의 각 HA 쌍에 대해 이 프로세스를 반복합니다. MetroCluster 구성이 있는 경우 구성의 두 클러스터에 대해 이러한 단계를 반복해야 합니다.

4개 이상의 노드

단계

1. 되돌리려는 노드에 로그인합니다.

   노드를 되돌리려면 노드의 노드 관리 LIF를 통해 클러스터에 로그인해야 합니다.

2. HA Pair의 노드에 대해 스토리지 페일오버 비활성화:

   ```
   storage failover modify -node <nodename> -enabled false
   ```

   HA 쌍에 대해 스토리지 페일오버를 한 번만 해제하면 됩니다. 노드에 대해 스토리지 페일오버를 해제하면 노드의 파트너에서도 스토리지 페일오버가 해제됩니다.

3. 노드의 대상 ONTAP 소프트웨어 이미지를 기본 이미지로 설정합니다.

   ```
   system image modify -node <nodename> -image <target_image>
   -isdefault true
   ```

4. 타겟 ONTAP 소프트웨어 이미지가 되돌리는 노드의 기본 이미지로 설정되어 있는지 확인합니다.

   ```
   system image show
   ```

   다음 예에서는 Node0에서 버전 9.13.1 이 기본 이미지로 설정되어 있음을 보여 줍니다.

   ```
   cluster1::*> system image show
                    Is      Is                  Install
   Node     Image   Default Current Version     Date
   -------- ------- ------- ------- --------    -------------------
   node0
            image1  false   true    9.14.1       MM/DD/YYYY TIME
            image2  true    false   9.13.1       MM/DD/YYYY TIME
   node1
            image1  true    true    9.14.1       MM/DD/YYYY TIME
            image2  false   false   9.13.1       MM/DD/YYYY TIME
   4 entries were displayed.
   ```

5. 노드 재버전이 준비되었는지 확인합니다.

   ```
   system node revert-to -node <nodename> -check-only true -version 9.x
   ```

`check-only`매개 변수는 스냅샷 정책 비활성화 또는 최신 버전의 ONTAP로 업그레이드한 후 생성된 스냅샷 삭제와 같이 되돌리기 전에 해결해야 할 모든 사전 조건을 식별합니다.

`-version`옵션은 되돌리는 ONTAP 릴리즈를 나타냅니다. 예를 들어 9.14.1에서 9.13.1로 되돌리는 경우 올바른 `-version` 옵션 값은 9.13.1입니다.

6. 노드의 클러스터 구성을 되돌립니다.

```
system node revert-to -node <nodename> -version 9.x
```

클러스터 구성을 되돌린 다음 클러스터 쉘에서 로그아웃됩니다.

7. 로그인 프롬프트가 표시될 때까지 기다린 다음 시스템 쉘에 로그인할지 묻는 메시지가 표시되면 * No * 를 입력합니다.

로그인 프롬프트가 나타나는 데 최대 30분 이상 걸릴 수 있습니다.

8. admin 을 사용하여 클러스터 쉘에 로그인합니다.
9. 노드 쉘로 전환:

```
run -node <nodename>
```

클러스터 쉘에 다시 로그온한 후 노드 쉘을 수락하는 데 몇 분 정도 걸릴 수 있습니다. 따라서 명령이 실패하면 몇 분 정도 기다린 후 다시 시도하십시오.

10. 노드의 파일 시스템 구성을 되돌립니다.

```
revert_to 9.x
```

이 명령은 노드의 파일 시스템 구성을 되돌릴 준비가 되었는지 확인한 다음 되돌립니다. 전제 조건이 식별되는 경우 조건을 해결한 다음 명령을 다시 실행해야 `revert_to` 합니다.

시스템 콘솔을 사용하여 복원 프로세스를 모니터링하면 노드 쉘에서 볼 수 있는 것보다 더 자세한 정보가 표시됩니다.

명령이 완료되면 자동 부팅 기능이 ONTAP로 재부팅됩니다.

AUTOBOOT이 FALSE인 경우 명령이 완료되면 Loader 프롬프트가 표시됩니다. 를 `yes` 입력하여 되돌린 다음 를 사용하여 `boot_ontap` 노드를 수동으로 재부팅합니다.

11. 노드가 재부팅된 후 새 소프트웨어가 실행 중인지 확인합니다.

```
system node image show
```

다음 예제에서 image1은 새 ONTAP 버전이며 Node0에서 현재 버전으로 설정됩니다.

```
cluster1::*> system node image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   true    true    X.X.X        MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
node1
         image1   true    false   X.X.X       MM/DD/YYYY TIME
         image2   false   true    Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.
```

12. 노드의 복원 상태가 완료되었는지 확인합니다.

```
system node upgrade-revert show -node <nodename>
```

상태는 "완료", "필요 없음" 또는 "반환된 테이블 항목이 없습니다."로 표시되어야 합니다.

13. HA 쌍의 다른 노드에서 이러한 단계를 반복한 다음, 각 추가 HA 쌍에 대해 이 단계를 반복합니다.

MetroCluster 구성이 있는 경우 구성의 두 클러스터에서 이 단계를 반복해야 합니다

14. 모든 노드를 되돌린 후 클러스터에 대해 고가용성을 다시 설정합니다.

```
storage failover modify -node* -enabled true
```

2노드 클러스터

1. 되돌리려는 노드에 로그인합니다.

노드를 되돌리려면 노드의 노드 관리 LIF를 통해 클러스터에 로그인해야 합니다.

2. 클러스터 고가용성(HA) 비활성화:

```
cluster ha modify -configured false
```

3. 스토리지 페일오버 해제:

```
storage failover modify -node <nodename> -enabled false
```

HA 쌍에 대해 스토리지 페일오버를 한 번만 해제하면 됩니다. 노드에 대해 스토리지 페일오버를 해제하면 노드의 파트너에서도 스토리지 페일오버가 해제됩니다.

4. 노드의 대상 ONTAP 소프트웨어 이미지를 기본 이미지로 설정합니다.

```
system image modify -node <nodename> -image <target_image>
-isdefault true
```

5. 타겟 ONTAP 소프트웨어 이미지가 되돌리는 노드의 기본 이미지로 설정되어 있는지 확인합니다.

```
system image show
```

다음 예에서는 Node0에서 버전 9.13.1 이 기본 이미지로 설정되어 있음을 보여 줍니다.

```
cluster1::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   false   true    9.14.1       MM/DD/YYYY TIME
         image2   true    false   9.13.1       MM/DD/YYYY TIME
node1
         image1   true    true    9.14.1       MM/DD/YYYY TIME
         image2   false   false   9.13.1       MM/DD/YYYY TIME
4 entries were displayed.
```

6. 노드에 현재 epsilon이 있는지 확인합니다.

```
cluster show -node <nodename>
```

다음 예는 노드가 epsilon를 보유하고 있음을 보여줍니다.

```
cluster1::*> cluster show -node node1

          Node: node1
          UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
       Epsilon: true
   Eligibility: true
        Health: true
```

a. 노드에 epsilon이 있는 경우 노드에 epsilon을 FALSE로 표시하여 epsilon을 노드의 파트너로 전송할 수 있도록 합니다.

```
cluster modify -node <nodename> -epsilon false
```

b. 파트너 노드에서 epsilon true를 표시하여 epsilon을 노드의 파트너로 전송합니다.

```
cluster modify -node <node_partner_name> -epsilon true
```

7. 노드 재버전이 준비되었는지 확인합니다.

```
system node revert-to -node <nodename> -check-only true -version 9.x
```

`check-only`매개 변수는 스냅샷 정책 비활성화 또는 최신 버전의 ONTAP로 업그레이드한 후 생성된 스냅샷 삭제와 같이 되돌리기 전에 해결해야 할 모든 조건을 식별합니다.

그만큼 `-version` 옵션은 되돌릴 ONTAP 릴리스 버전을 나타냅니다. ONTAP 버전의 경우 처음 두 값만 필수입니다. 예를 들어, 9.14.1에서 9.13.1로 되돌리는 경우, 올바른 값은 다음과 같습니다. `-version` 옵션은 9.13입니다.

클러스터 구성을 되돌린 다음 클러스터 쉘에서 로그아웃됩니다.

8. 노드의 클러스터 구성을 되돌립니다.

```
system node revert-to -node <nodename> -version 9.x
```

9. 로그인 프롬프트가 표시될 때까지 기다린 다음 시스템 쉘에 로그인할지 묻는 메시지가 나타나면 를 `No` 입력합니다.

로그인 프롬프트가 나타나는 데 최대 30분 이상 걸릴 수 있습니다.

10. admin 을 사용하여 클러스터 쉘에 로그인합니다.

11. 노드 쉘로 전환:

```
run -node <nodename>
```

클러스터 쉘에 다시 로그온한 후 노드 쉘을 수락하는 데 몇 분 정도 걸릴 수 있습니다. 따라서 명령이 실패하면 몇 분 정도 기다린 후 다시 시도하십시오.

12. 노드의 파일 시스템 구성을 되돌립니다.

```
revert_to 9.x
```

이 명령은 노드의 파일 시스템 구성을 되돌릴 준비가 되었는지 확인한 다음 되돌립니다. 전제 조건이 식별되는 경우 조건을 해결한 다음 명령을 다시 실행해야 `revert_to` 합니다.

> 시스템 콘솔을 사용하여 복원 프로세스를 모니터링하면 노드 쉘에서 볼 수 있는 것보다 더 자세한 정보가 표시됩니다.

명령이 완료되면 자동 부팅 기능이 ONTAP로 재부팅됩니다.

autoboot가 false 이면 명령이 로더 프롬프트를 표시합니다. 되돌리려면 yes를 입력하고 노드를 수동으로 재부팅하려면 boot_ONTAP을 사용합니다.

13. 노드가 재부팅된 후 새 소프트웨어가 실행 중인지 확인합니다.

```
system node image show
```

다음 예제에서 image1은 새 ONTAP 버전이며 Node0에서 현재 버전으로 설정됩니다.

```
cluster1::*> system node image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   true    true    X.X.X        MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
node1
         image1   true    false   X.X.X       MM/DD/YYYY TIME
         image2   false   true    Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.
```

14. 노드에 대한 되돌리기 상태가 완료되었는지 확인합니다.

```
system node upgrade-revert show -node <nodename>
```

상태는 "완료", "필요 없음" 또는 "반환된 테이블 항목이 없습니다."로 표시되어야 합니다.

15. HA 쌍의 다른 노드에서 이 단계를 반복합니다.
16. 두 노드를 모두 되돌린 후 클러스터에 대해 고가용성을 다시 설정합니다.

```
cluster ha modify -configured true
```

17. 두 노드에서 스토리지 페일오버 재활성화:

```
storage failover modify -node <nodename> -enabled true
```

관련 정보

- "스토리지 장애 조치 수정"

ONTAP 복원 후 수행할 작업

ONTAP 되돌리기 후 클러스터 및 스토리지 상태를 확인합니다

ONTAP 클러스터를 되돌린 후에는 노드가 정상 상태이고 클러스터에 참여할 자격이 있는지, 클러스터가 쿼럼에 있는지 확인해야 합니다. 또한 디스크, 애그리게이트 및 볼륨의 상태도 확인해야 합니다.

클러스터 상태를 확인합니다

단계

1. 클러스터의 노드가 온라인 상태이며 클러스터에 참여할 자격이 있는지 확인합니다.

```
cluster show
```

이 예에서는 클러스터가 정상 상태이며 모든 노드가 클러스터에 참여할 수 있습니다.

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

노드가 정상 상태가 아니거나 적합하지 않은 경우 EMS 로그에서 오류를 확인하고 수정 조치를 취합니다.

2. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

계속하려면 y를 입력하십시오.

3. 각 RDB 프로세스에 대한 구성 세부 정보를 확인합니다.

◦ 관계형 데이터베이스 epoch 및 데이터베이스 epoch는 각 노드에 대해 일치해야 합니다.

◦ 링당 쿼럼 마스터는 모든 노드에 대해 동일해야 합니다.

각 링에는 다른 쿼럼 마스터가 있을 수 있습니다.

이 **RDB** 프로세스를 표시하려면...	이 명령을 입력하십시오...
기능과	`cluster ring show -unitname mgmt`
볼륨 위치 데이터베이스	`cluster ring show -unitname vldb`
Virtual-Interface Manager를 참조하십시오	`cluster ring show -unitname vifmgr`
SAN 관리 데몬	`cluster ring show -unitname bcomd`

이 예에서는 볼륨 위치 데이터베이스 프로세스를 보여 줍니다.

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

5. SAN 환경에서 작동 중인 경우 각 노드가 SAN 쿼럼에 있는지 확인합니다.

```
event log show  -severity informational -message-name scsiblade.*
```

각 노드에 대한 가장 최근의 scsib블레이드 이벤트 메시지는 SCSI 블레이드가 quorum에 있음을 나타내야 합니다.

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time              Node        Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0       INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1       INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

관련 정보

"시스템 관리"

스토리지 상태를 확인합니다

클러스터를 되돌리거나 다운그레이드한 후에는 디스크, 애그리게이트 및 볼륨의 상태를 확인해야 합니다.

단계

1. 디스크 상태 확인:

확인하려면...	수행할 작업...
손상된 디스크	a. 손상된 디스크를 표시합니다. `storage disk show -state broken` b. 손상된 디스크를 제거하거나 교체합니다.

확인하려면...	수행할 작업...
유지보수 또는 재구성이 진행 중인 디스크	a. 유지 보수, 보류 또는 재구성 상태의 디스크를 표시합니다. `storage disk show -state maintenance`
pending	reconstructing ---- .. 유지보수 또는 재구성 작업이 완료될 때까지 기다린 후 계속 진행하십시오.

2. 스토리지 애그리게이트를 포함하여 물리적 스토리지와 논리적 스토리지의 상태를 표시하여 모든 애그리게이트가 온라인 상태인지 확인합니다.

```
storage aggregate show -state !online
```

이 명령은 _not_online 인 애그리게이트를 표시합니다. 주요 업그레이드 또는 리버전을 수행하기 전과 후의 모든 애그리게이트는 온라인 상태여야 합니다.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. _NOT_ONLINE 상태인 볼륨을 표시하여 모든 볼륨이 온라인 상태인지 확인합니다.

```
volume show -state !online
```

주요 업그레이드 또는 재버전을 수행하기 전과 후에 모든 볼륨이 온라인 상태여야 합니다.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. 일치하지 않는 볼륨이 없는지 확인합니다.

```
volume show -is-inconsistent true
```

를 참조하십시오"NetApp 지식 기반: 볼륨에 WAFL 일관되지 않음 표시" 일관되지 않은 볼륨을 해결하는 방법에 대해.

클라이언트 액세스 확인(**SMB** 및 **NFS**)

구성된 프로토콜의 경우 SMB 및 NFS 클라이언트의 액세스를 테스트하여 클러스터에 액세스할 수 있는지 확인합니다.

관련 정보

- "디스크 및 애그리게이트 관리"
- "저장 디스크 표시"

ONTAP 되돌리기 후 **MetroCluster** 구성에 대해 자동 전환이 활성화된다

ONTAP MetroCluster 구성을 되돌린 후 계획되지 않은 자동 전환을 활성화하여 MetroCluster 구성이 완전히 작동하는지 확인해야 합니다.

단계

1. 계획되지 않은 자동 전환 지원:

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
disaster
```

2. MetroCluster 구성을 검증합니다.

```
metrocluster check run
```

ONTAP 되돌리기 후 **LIF**를 홈 포트로 설정 및 되돌리기

재부팅 중 일부 LIF는 할당된 페일오버 포트로 마이그레이션되었을 수 있습니다. ONTAP 클러스터를 되돌린 후 홈 포트에 없는 LIF를 사용하도록 설정하고 되돌려야 합니다.

네트워크 인터페이스 되돌리기 명령은 홈 포트가 작동하고 있을 경우 홈 포트에 없는 LIF를 홈 포트로 되돌립니다. LIF의 홈 포트는 LIF가 생성될 때 지정됩니다. 네트워크 인터페이스 show 명령을 사용하여 LIF의 홈 포트를 확인할 수 있습니다.

단계

1. 모든 LIF의 상태를 표시합니다.

```
network interface show
```

이 예는 SVM(스토리지 가상 머신)에 대한 모든 LIF의 상태를 표시합니다.

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001    down/down  192.0.2.120/24     node0         e0e
true
            data002    down/down  192.0.2.121/24     node0         e0f
true
            data003    down/down  192.0.2.122/24     node0         e2a
true
            data004    down/down  192.0.2.123/24     node0         e2b
true
            data005    down/down  192.0.2.124/24     node0         e0e
false
            data006    down/down  192.0.2.125/24     node0         e0f
false
            data007    down/down  192.0.2.126/24     node0         e2a
false
            data008    down/down  192.0.2.127/24     node0         e2b
false
8 entries were displayed.
```

Status Admin 상태가 DOWN 이거나 is home 상태가 false인 LIF가 나타나면 다음 단계를 계속 진행합니다.

2. 데이터 LIF 지원:

```
network interface modify {-role data} -status-admin up
```

3. LIF를 홈 포트로 되돌리기:

```
network interface revert *
```

4. 모든 LIF가 홈 포트에 있는지 확인:

```
network interface show
```

이 예에서는 SVM vs0용 모든 LIF가 홈 포트에 있음을 보여 줍니다.

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0          e0e
true
            data002      up/up    192.0.2.121/24     node0          e0f
true
            data003      up/up    192.0.2.122/24     node0          e2a
true
            data004      up/up    192.0.2.123/24     node0          e2b
true
            data005      up/up    192.0.2.124/24     node1          e0e
true
            data006      up/up    192.0.2.125/24     node1          e0f
true
            data007      up/up    192.0.2.126/24     node1          e2a
true
            data008      up/up    192.0.2.127/24     node1          e2b
true
8 entries were displayed.
```

관련 정보

- "네트워크 인터페이스"

ONTAP 되돌리기 후 스냅샷 정책을 사용하도록 설정합니다

이전 버전의 ONTAP로 되돌린 후 스냅샷 생성을 다시 시작하려면 스냅샷 정책을 활성화해야 합니다.

이전 버전의 ONTAP로 되돌리기 전에 비활성화한 스냅샷 스케줄을 다시 설정하려고 합니다.

단계

1. 모든 데이터 SVM에 대해 스냅샷 정책 활성화:

```
volume snapshot policy modify -vserver * -enabled true
```

```
snapshot policy modify pg-rpo-hourly -enable true
```

2. 각 노드에 대해 루트 볼륨의 스냅샷 정책을 설정합니다.

```
run -node <node_name> vol options <volume_name> nosnap off
```

ONTAP 복원 후 **IPv6** 방화벽 항목을 확인합니다

ONTAP 9 버전에서 다시 버전을 사용하면 방화벽 정책의 일부 서비스에 대한 기본 IPv6 방화벽 항목이 누락될 수 있습니다. 필요한 방화벽 항목이 시스템에 복원되었는지 확인해야 합니다.

단계

1. 모든 방화벽 정책을 기본 정책과 비교하여 올바른지 확인합니다.

```
system services firewall policy show
```

다음 예에서는 기본 정책을 보여 줍니다.

```
cluster1::*> system services firewall policy show
Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
cluster
                 dns        allow  0.0.0.0/0
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
                 ndmp       allow  0.0.0.0/0
                 ntp        allow  0.0.0.0/0
                 rsh        allow  0.0.0.0/0
                 snmp       allow  0.0.0.0/0
                 ssh        allow  0.0.0.0/0
                 telnet     allow  0.0.0.0/0
data
                 dns        allow  0.0.0.0/0, ::/0
                 http       deny   0.0.0.0/0, ::/0
                 https      deny   0.0.0.0/0, ::/0
                 ndmp       allow  0.0.0.0/0, ::/0
                 ntp        deny   0.0.0.0/0, ::/0
                 rsh        deny   0.0.0.0/0, ::/0
.
.
.
```

2. 새 방화벽 정책을 생성하여 누락된 기본 IPv6 방화벽 항목을 수동으로 추가합니다.

```
system services firewall policy create -policy <policy_name> -service
ssh -action allow -ip-list <ip_list>
```

3. LIF에 새 정책을 적용하여 네트워크 서비스에 대한 액세스를 허용합니다.

```
network interface modify -vserve <svm_name> -lif <lif_name> -firewall
-policy <policy_name>
```

ONTAP 9.8로 되돌린 후 서비스 프로세서에 액세스할 수 있는 사용자 계정을 확인합니다

ONTAP 9.9.1 이상에서는 `-role` 사용자 계정에 대한 매개 변수가 로 `admin`변경됩니다. `ONTAP 9.8` 이하에서 사용자 계정을 만들고 `ONTAP 9.9.1` 이상으로 업그레이드한 다음 `ONTAP 9.8`로 다시 되돌리면 `-role` 매개 변수가 원래 값으로 복원됩니다. 수정된 값이 허용 가능한지 확인해야 합니다.

되돌리는 동안 SP 사용자의 역할이 삭제된 경우 "rbac.spuser.role.notfound" EMS 메시지가 기록됩니다.

자세한 내용은 을 참조하십시오 "SP에 액세스할 수 있는 계정입니다".

클러스터 관리

System Manager를 이용한 클러스터 관리

ONTAP System Manager를 사용한 클러스터 관리에 대해 알아보세요

System Manager는 HTML5 기반의 그래픽 관리 인터페이스로, 웹 브라우저를 사용하여 스토리지 시스템과 스토리지 객체(예: 디스크, 볼륨 및 스토리지 계층)를 관리하고 스토리지 시스템과 관련된 일반적인 관리 작업을 수행할 수 있습니다.

- System Manager는 ONTAP 소프트웨어에 웹 서비스로 포함되어 있으며, 기본적으로 활성화되어 있으며 브라우저를 통해 액세스할 수 있습니다.
- System Manager의 이름이 ONTAP 9.6부터 변경되었습니다. ONTAP 9.5 이전 버전에서는 OnCommand 시스템 관리자라고 했습니다. ONTAP 9.6 이상에서는 시스템 관리자라고 합니다.
- 기존 System Manager(ONTAP 9.7 이하 버전에서만 사용 가능)를 사용하는 경우 을 참조하십시오 "System Manager Classic(ONTAP 9.0 ~ 9.7)"

System Manager 대시보드를 사용하면 중요한 경고 및 알림, 스토리지 계층 및 볼륨의 효율성 및 용량, 클러스터에서 사용 가능한 노드, HA 쌍의 노드 상태, 가장 활성화된 애플리케이션 및 객체 등에 대한 정보를 한 눈에 확인할 수 있습니다. 클러스터 또는 노드의 성능 메트릭과

ONTAP 9.7 이상 릴리즈의 System Manager를 사용하면 다음과 같은 일반적인 작업을 수행할 수 있습니다.

- 클러스터를 생성하고, 네트워크를 구성하고, 클러스터에 대한 지원 세부 정보를 설정합니다.
- 디스크, 로컬 계층, 볼륨, Qtree, 디스크 등의 스토리지 오브젝트 구성 및 관리 있습니다.
- SMB 및 NFS와 같은 프로토콜을 구성하고 파일 공유를 프로비저닝합니다.
- 블록 액세스를 위해 FC, FCoE, NVMe 및 iSCSI와 같은 프로토콜을 구성합니다.
- 서브넷, 브로드캐스트 도메인, 데이터 및 관리 인터페이스, 인터페이스 그룹 등의 네트워크 구성 요소를 만들고 구성합니다.
- 미러링 및 보관 관계 설정 및 관리
- 클러스터 관리, 스토리지 노드 관리 및 스토리지 가상 머신(스토리지 VM) 관리 작업을 수행합니다.
- 스토리지 VM 생성 및 구성, 스토리지 VM과 연결된 스토리지 객체 관리, 스토리지 VM 서비스 관리
- 클러스터의 고가용성(HA) 구성 모니터링 및 관리
- 노드의 상태에 관계없이 노드를 원격으로 로그인, 관리, 모니터링 및 관리하도록 서비스 프로세서를 구성합니다.

System Manager 용어

System Manager에서는 일부 ONTAP 키 기능에 CLI와 다른 용어를 사용합니다.

- * 로컬 계층 * : 데이터를 저장하는 물리적 솔리드 스테이트 드라이브 또는 하드 디스크 드라이브 세트. 이런 것을 Aggregate으로 알고 계실 것입니다. 실제로 ONTAP CLI를 사용하는 경우 로컬 계층을 나타내는 데 사용되는 _aggregate_라는 용어가 계속 표시됩니다.
- * 클라우드 계층 *: ONTAP에서 사용하는 클라우드 스토리지 여러 가지 이유 중 하나로 인해 데이터를 외부에

저장하려는 경우 FabricPool의 클라우드 부분을 생각한다면 이미 알아낸 것입니다. 또한 StorageGRID 시스템을 사용하는 경우 클라우드가 사외 환경에 있지 않을 수 있습니다. (온프레미스의 클라우드형 경험을 _ 프라이빗 클라우드라고 합니다.)

- * 스토리지 VM *: ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에 스토리지 및 데이터 서비스를 제공합니다. 이를 *SVM* 또는 _vserver_로 알고 있을 수 있습니다.
- 네트워크 인터페이스: 물리적 네트워크 포트에 할당된 주소 및 속성입니다. _논리 인터페이스(LIF)_라고도 합니다.
- 일시 중지: 작업을 중단하는 동작입니다. ONTAP 9.8 이전 버전의 System Manager에서는 _quiesce_를 사용했을 수 있습니다.

시스템 관리자를 사용하여 **ONTAP** 클러스터에 액세스합니다.

CLI(Command-Line Interface) 대신 그래픽 인터페이스를 사용하여 클러스터를 액세스하고 관리하려면 ONTAP에 웹 서비스로 포함되어 있는 System Manager를 기본적으로 사용해야 하며 브라우저를 사용하여 액세스할 수 있습니다.

ONTAP 9.12.1부터 System Manager가 NetApp Console과 완벽하게 통합되었습니다.

콘솔을 사용하면 익숙한 System Manager 대시보드를 유지하면서 단일 제어 평면에서 하이브리드 멀티클라우드 인프라를 관리할 수 있습니다.

보다 "NetApp 콘솔과 시스템 관리자 통합" .

이 작업에 대해

클러스터 관리 네트워크 인터페이스(LIF) 또는 노드 관리 네트워크 인터페이스(LIF)를 사용하여 System Manager에 액세스할 수 있습니다. System Manager에 중단 없이 액세스하려면 클러스터 관리 네트워크 인터페이스(LIF)를 사용해야 합니다.

시작하기 전에

- "admin" 역할과 ""http""" 및 ""console""" 애플리케이션 유형으로 구성된 클러스터 사용자 계정이 있어야 합니다.
- 브라우저에서 쿠키 및 사이트 데이터를 활성화해야 합니다.

단계

1. 웹 브라우저에서 클러스터 관리 네트워크 인터페이스의 IP 주소를 가리킵니다.
   - IPv4를 사용하는 경우: `https://cluster-mgmt-LIF*`
   - IPv6를 사용하는 경우: `https://[cluster-mgmt-LIF]*`

     System Manager의 브라우저 액세스에는 HTTPS만 지원됩니다.

   클러스터에서 자체 서명된 디지털 인증서를 사용하는 경우 브라우저에서 인증서를 신뢰할 수 없음을 나타내는 경고를 표시할 수 있습니다. 액세스를 계속할 위험을 확인하거나 서버 인증을 위해 클러스터에 CA(인증 기관) 서명 디지털 인증서를 설치할 수 있습니다.

2. * 선택 사항: * CLI를 사용하여 액세스 배너를 구성한 경우 * 경고 * 대화 상자에 표시된 메시지를 읽고 필요한 옵션을 선택하여 계속 진행합니다.

   SAML(Security Assertion Markup Language) 인증이 활성화된 시스템에서는 이 옵션이 지원되지 않습니다.

◦ 계속 진행하지 않으려면 * 취소 * 를 클릭하고 브라우저를 닫습니다.

◦ 계속하려면 * 확인 * 을 클릭하여 System Manager 로그인 페이지로 이동하십시오.

3. 클러스터 관리자 자격 증명을 사용하여 System Manager에 로그인합니다.

> ONTAP 9.11.1부터 시스템 관리자에 로그인할 때 로캘을 지정할 수 있습니다. 로캘은 언어, 통화, 시간 및 날짜 형식, 유사한 설정 등의 특정 지역화 설정을 지정합니다. ONTAP 9.10.1 이하의 경우 브라우저에서 시스템 관리자의 로캘이 검색됩니다. System Manager의 로캘을 변경하려면 브라우저의 로캘을 변경해야 합니다.

4. * 선택 사항*: ONTAP 9.12.1부터 시스템 관리자의 모양에 대한 기본 설정을 지정할 수 있습니다.

   a. System Manager의 오른쪽 위에서 를 클릭하여 사용자 옵션을 관리합니다.

   b. 시스템 테마 * 전환 스위치를 원하는 위치로 맞춥니다.

위치를 전환합니다	모양 설정
(왼쪽)	밝은 테마(어두운 텍스트가 있는 밝은 배경)
OS(중앙)	기본적으로 운영 체제의 응용 프로그램에 설정된 테마 기본 설정(일반적으로 System Manager에 액세스하는 데 사용되는 브라우저의 테마 설정)이 사용됩니다.
(오른쪽)	어두운 테마(밝은 텍스트가 있는 어두운 배경)

관련 정보

"웹 서비스에 대한 액세스 관리"

"웹 브라우저를 사용하여 노드의 로그, 코어 덤프 및 MIB 파일에 액세스합니다"

ONTAP 클러스터에 프로토콜을 구성합니다

클러스터에서 활성화된 라이센스에 따라 클러스터에서 원하는 프로토콜을 활성화할 수 있습니다. 그런 다음 스토리지를 액세스할 수 있는 네트워크 인터페이스를 생성합니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" System Manger를 사용하여 ONTAP 클러스터를 설정합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

단계

1. Dashboard * 를 선택한 다음 * Configure Protocols * 를 클릭합니다.

   ◦ NAS 프로토콜을 활성화하려면 * NFS * 또는 * SMB * 를 선택합니다.

   ◦ SAN 프로토콜을 활성화하려면 * iSCSI * 또는 * FC * 를 선택합니다.

   ◦ NVMe 프로토콜을 활성화하려면 * NVMe * 를 선택하십시오.

ONTAP System Manager를 사용하여 라이선스 키를 추가하여 새로운 기능을 활성화하세요.

ONTAP 9.10.1 이전 릴리스에서는 ONTAP 기능이 라이센스 키로 활성화되고 ONTAP 9.10.1 이상의 기능은 NetApp 라이센스 파일에서 사용하도록 설정됩니다. 시스템 관리자를 사용하여 라이센스 키와 NetApp 라이센스 파일을 추가할 수 있습니다.

ONTAP 9.10.1부터는 System Manager를 사용하여 NetApp 라이센스 파일을 한 번에 여러 라이센스 기능을 사용할 수 있습니다. NetApp 라이센스 파일을 사용하면 더 이상 별도의 기능 라이센스 키를 추가할 필요가 없으므로 라이센스 설치를 간소화할 수 있습니다. NetApp Support 사이트에서 NetApp 라이센스 파일을 다운로드합니다.

일부 기능에 대한 라이센스 키가 이미 있고 ONTAP 9.10.1로 업그레이드하는 경우 해당 라이센스 키를 계속 사용할 수 있습니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. 라이센스 * 에서 를 선택합니다 →.
3. 찾아보기 * 를 선택합니다. 다운로드한 NetApp 라이센스 파일을 선택합니다.
4. 추가하려는 라이센스 키가 있는 경우 * 28자 라이센스 키 사용 * 을 선택하고 키를 입력합니다.

ONTAP 시스템 관리자를 사용하여 클러스터 구성 다운로드

ONTAP 9.11.1부터 System Manager를 사용하여 클러스터 및 노드에 대한 몇 가지 구성 세부 정보를 다운로드할 수 있습니다. 이 정보는 재고 관리, 하드웨어 교체 및 수명 주기 활동에 사용될 수 있습니다. 이 정보는 ASUP(AutoSupport) 데이터를 보내지 않는 사이트에 특히 유용합니다.

클러스터 구성 세부 정보에는 클러스터 이름, 클러스터 ONTAP 버전, 클러스터 관리 LIF, 볼륨 및 LIF 수가 포함됩니다.

노드 구성 세부 정보에는 노드 이름, 시스템 일련 번호, 시스템 ID, 시스템 모델, ONTAP 버전, MetroCluster 정보, SP/BMC 네트워크 정보, 암호화 구성 정보가 포함됩니다.

단계

1. 클러스터 > 개요 * 를 클릭합니다.
2. 드롭다운 메뉴를 표시하려면 클릭합니다

.
3. 구성 다운로드 * 를 선택합니다.
4. HA 쌍을 선택한 다음 * 다운로드 * 를 클릭합니다.

   설정이 Excel 스프레드시트로 다운로드됩니다.

   - 첫 번째 시트에는 클러스터 세부 정보가 포함되어 있습니다.
   - 다른 시트에는 노드 세부 정보가 포함되어 있습니다.

ONTAP 시스템 관리자를 사용하여 클러스터에 태그 지정

ONTAP 9.14.1부터 System Manager를 사용하여 클러스터에 태그를 할당하면 프로젝트 또는 비용 센터 같은 범주에 속하는 오브젝트를 식별할 수 있습니다.

이 작업에 대해

클러스터에 태그를 할당할 수 있습니다. 먼저 태그를 정의하고 추가해야 합니다. 그런 다음 태그를 편집하거나 삭제할 수도 있습니다.

태그는 클러스터를 생성할 때 추가하거나 나중에 추가할 수 있습니다.

키를 지정하고 ""키:값"" 형식을 사용하여 값을 연결하여 태그를 정의합니다. 예: "'dEPT:engineering"" 또는 "'location:san-jose".

태그를 만들 때 다음 사항을 고려해야 합니다.

- 키의 최소 길이는 1자이며 null일 수 없습니다. 값은 null일 수 있습니다.
- 키는 ""location: san-jose, Toronto""와 같이 값을 쉼표로 구분하여 여러 값과 쌍을 이룰 수 있습니다.
- 태그를 여러 리소스에 사용할 수 있습니다.
- 키는 소문자로 시작해야 합니다.

단계

태그를 관리하려면 다음 단계를 수행하십시오.

1. System Manager에서 * Cluster * 를 클릭하여 개요 페이지를 표시합니다.

   태그는 * 태그 * 섹션에 나열됩니다.

2. 기존 태그를 수정하거나 새 태그를 추가하려면 * 태그 관리 * 를 클릭합니다.

   태그를 추가, 편집 또는 삭제할 수 있습니다.

이 작업을 수행하려면…	다음 단계를 수행합니다.
태그를 추가합니다	a. 태그 추가 * 를 클릭합니다. b. 키와 해당 값 또는 값을 지정합니다(여러 값을 쉼표로 구분). c. 저장 * 을 클릭합니다.
태그를 편집합니다	a. 키 * 및 * 값(선택 사항) * 필드의 내용을 수정합니다. b. 저장 * 을 클릭합니다.
태그를 삭제합니다	a. 삭제할 태그 옆에 있는 을 클릭합니다.

ONTAP System Manager를 사용하여 지원 사례 보기 및 제출

ONTAP 9.9.1부터 클러스터와 관련된 Active IQ Digital Advisor (Digital Advisor 라고도 함)에서 지원 사례를 확인할 수 있습니다. NetApp 지원 사이트에서 새 지원 사례를 제출하는 데 필요한 클러스터 세부 정보를 복사할 수도 있습니다. ONTAP 9.10.1부터는 지원 담당자가 문제를 해결하는 데 도움이 되는 원격 측정 로깅을 활성화할 수 있습니다.

펌웨어 업데이트에 대한 알림을 받으려면 Active IQ Unified Manager에 등록되어 있어야 합니다. 을 참조하십시오 "Active IQ Unified Manager 문서 리소스".

단계

1. System Manager에서 * Support * 를 선택합니다.

   이 클러스터와 관련된 지원 케이스 목록이 표시됩니다.

2. 절차를 수행하려면 다음 링크를 클릭하십시오.
   - * 케이스 번호 *: 사례에 대한 자세한 내용을 참조하십시오.
   - * NetApp Support 사이트로 이동 *: NetApp Support 사이트에서 * My AutoSupport * 페이지로 이동하여 기술 자료 문서를 확인하거나 새로운 지원 케이스를 제출하십시오.
   - * 내 케이스 보기 *: NetApp Support 사이트에서 * 내 케이스 * 페이지로 이동합니다.
   - * 클러스터 세부 정보 보기 *: 새 케이스를 제출할 때 필요한 정보를 보고 복사합니다.

원격 측정 로깅을 활성화합니다

ONTAP 9.10.1부터 System Manager를 사용하여 원격 측정 로깅을 활성화할 수 있습니다. 원격 측정 로깅이 허용되는 경우 System Manager에 의해 기록되는 메시지에는 메시지를 트리거한 정확한 프로세스를 나타내는 특정 원격 측정 식별자가 제공됩니다. 해당 프로세스와 관련하여 발급된 모든 메시지는 동일한 식별자를 가지며, 이 식별자는 작업 워크플로의 이름과 번호(예: "add-volume-1941290")로 구성됩니다.

성능 문제가 발생할 경우 원격 측정 로깅을 활성화하여 지원 담당자가 메시지가 발행된 특정 프로세스를 보다 쉽게 식별할 수 있습니다. 원격 측정 식별자가 메시지에 추가되면 로그 파일이 약간 확대됩니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. UI 설정 * 섹션에서 * 원격 측정 로깅 허용 * 확인란을 클릭합니다.

ONTAP System Manager에서 스토리지 VM의 최대 용량 한도를 관리합니다.

ONTAP 9.13.1 부터는 System Manager를 사용하여 스토리지 VM에 대한 최대 용량 제한을 설정하고 사용된 스토리지가 최대 용량의 특정 비율에 도달하면 경고를 트리거하도록 임계값을 설정할 수 있습니다.

스토리지 VM의 최대 용량 한도 설정

ONTAP 9.13.1 부터는 스토리지 VM의 모든 볼륨에 할당할 수 있는 최대 용량을 지정할 수 있습니다. 스토리지 VM을 추가하거나 기존 스토리지 VM을 편집할 때 최대 용량을 설정할 수 있습니다.

단계

1. 스토리지 * > * 스토리지 VM * 을 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 스토리지 VM을 추가하려면 을 + Add 클릭합니다.
   - 스토리지 VM을 편집하려면 스토리지 VM 이름 옆에 있는 을 클릭한 ⋮ 다음 * 편집 * 을 클릭합니다.

3. 스토리지 VM의 설정을 입력하거나 수정하고 "최대 용량 제한 사용" 확인란을 선택합니다.
4. 최대 용량 크기를 지정합니다.
5. 알림을 트리거하는 임계값으로 사용할 최대 용량의 백분율을 지정합니다.
6. 저장 * 을 클릭합니다.

스토리지 **VM**의 최대 용량 한도를 편집합니다

ONTAP 9.13.1 부터는 기존 스토리지 VM의 최대 용량 한도(있는 경우)를 편집할 수 있습니다 최대 용량 제한이 설정되었습니다 이미 있습니다.

단계

1. 스토리지 * > * 스토리지 VM * 을 선택합니다.
2. 스토리지 VM 이름 옆에 있는 을 ⋮ 클릭한 다음 * 편집 * 을 클릭합니다.

   "최대 용량 제한 사용" 확인란이 이미 선택되어 있습니다.

3. 다음 단계 중 하나를 수행합니다.

조치	단계
최대 용량 제한을 비활성화합니다	1. 확인란을 선택 취소합니다. 2. 저장 * 을 클릭합니다.
최대 용량 제한을 수정합니다	1. 새 최대 용량 크기를 지정합니다. 스토리지 VM에서 이미 할당된 공간보다 작은 크기는 지정할 수 없습니다. 2. 알림을 트리거하는 임계값으로 사용할 최대 용량의 새 백분율을 지정합니다. 3. 저장 * 을 클릭합니다.

관련 정보

- "스토리지 VM의 최대 용량 한도를 봅니다"
- "System Manager의 용량 측정"
- "SVM 용량 한도 관리"

ONTAP System Manager에서 클러스터, 계층, SVM 용량 모니터링

System Manager를 사용하면 사용된 스토리지 용량과 클러스터, 로컬 계층 또는 스토리지 VM에 대해 사용 가능한 스토리지 용량을 모니터링할 수 있습니다.

각 ONTAP 버전에서 System Manager는 더욱 강력한 용량 모니터링 정보를 제공합니다.

- ONTAP 9.13.1 부터는 스토리지 VM에 대해 최대 용량 제한을 설정하고 사용된 스토리지가 최대 용량의 특정 비율에 도달하면 경고를 트리거하도록 임계값을 설정할 수 있습니다.
- ONTAP 9.12.1부터 시스템 관리자는 로컬 계층에 대해 커밋된 용량을 표시합니다.

- ONTAP 9.10.1부터 System Manager에서는 클러스터 용량에 대한 기간별 데이터를 확인하고 향후 사용하거나 사용할 수 있는 용량에 대한 예측을 볼 수 있습니다. 로컬 계층 및 볼륨의 용량을 모니터링할 수도 있습니다.

> 사용된 용량의 측정치는 ONTAP 버전에 따라 다르게 표시됩니다. 자세한 내용은 을 "System Manager의 용량 측정"참조하십시오.

클러스터의 용량을 봅니다

System Manager의 대시보드에서 클러스터의 용량 측정값을 볼 수 있습니다.

시작하기 전에

클라우드의 용량과 관련된 데이터를 보려면 Digital Advisor 계정이 있고 연결되어 있어야 합니다.

단계

1. System Manager에서 * 대시보드 * 를 클릭합니다.
2. Capacity * 섹션에서 다음을 볼 수 있습니다.
   - 클러스터의 총 사용 용량입니다
   - 클러스터의 총 가용 용량입니다
   - 사용된 용량 및 사용 가능한 용량의 비율입니다.
   - 데이터 축소율:
   - 클라우드에서 사용되는 용량입니다.
   - 용량 사용 기록.
   - 용량 사용에 대한 예상 사용량

   > System Manager에서 용량 표현은 루트 스토리지 계층(애그리게이트) 용량을 고려하지 않습니다.
3. 차트를 클릭하여 클러스터 용량에 대한 자세한 정보를 확인하십시오.

   용량 측정값은 두 개의 막대 차트로 표시됩니다.

   - 위 차트에는 물리적 용량, 즉 물리적 용량, 예약된 공간 및 사용 가능한 공간이 표시됩니다.
   - 아래쪽 차트에는 논리적 용량, 즉 클라이언트 데이터, 스냅샷 및 클론의 크기와 총 논리적 사용된 공간이 표시됩니다.

   막대 차트 아래에는 데이터 감소를 위한 측정값이 나와 있습니다.

   - 클라이언트 데이터에 대한 데이터 축소율입니다(스냅샷과 클론은 포함되지 않음).
   - 전체 데이터 축소율:

자세한 내용은 을 참조하십시오 "System Manager의 용량 측정".

로컬 계층의 용량을 봅니다

로컬 계층의 용량에 대한 세부 정보를 볼 수 있습니다. ONTAP 9.12.1부터 용량 뷰에는 로컬 계층에 할당된 용량도

포함되어 할당된 용량을 수용하고 여유 공간 부족을 방지하기 위해 로컬 계층에 용량을 추가해야 하는지 여부를 판단할 수 있습니다.

단계

1. Storage > Tiers * 를 클릭합니다.
2. 로컬 계층의 이름을 선택합니다.
3. 개요 * 페이지의 * 용량 * 섹션에서 용량이 다음 세 가지 측정값과 함께 막대 차트에 표시됩니다.
   - 사용된 용량과 예약된 용량입니다
   - 사용 가능한 용량입니다
   - 커밋된 용량(ONTAP 9.12.1부터 시작)
4. 로컬 계층의 용량에 대한 세부 정보를 보려면 차트를 클릭하십시오.

   용량 측정값은 두 개의 막대 차트로 표시됩니다.

   - 위쪽 막대 차트에는 물리적 용량, 즉 물리적 사용 공간, 예약된 공간 및 사용 가능한 공간이 표시됩니다.
   - 아래쪽 막대 차트에는 논리적 용량, 즉 클라이언트 데이터, 스냅샷 및 클론의 크기와 총 논리적 사용된 공간이 표시됩니다.

   막대 차트 아래에는 데이터 감소를 위한 측정 비율이 나와 있습니다.

   - 클라이언트 데이터에 대한 데이터 축소율입니다(스냅샷과 클론은 포함되지 않음).
   - 전체 데이터 축소율:

자세한 내용은 을 참조하십시오 "System Manager의 용량 측정".

선택적 작업입니다

- 커밋된 용량이 로컬 계층의 용량보다 큰 경우 사용 가능한 공간이 부족해지기 전에 로컬 계층에 용량을 추가하는 것을 고려할 수 있습니다. 을 참조하십시오 "로컬 계층에 용량 추가(애그리게이트에 디스크 추가)".
- 볼륨 * 탭을 선택하여 특정 볼륨이 로컬 계층에서 사용하는 스토리지를 볼 수도 있습니다.

스토리지 **VM**의 볼륨 용량을 봅니다

스토리지 VM의 볼륨에서 사용하는 스토리지 양과 사용 가능한 용량을 확인할 수 있습니다. 사용 중인 스토리지와 사용 가능한 스토리지의 총 측정값을 "볼륨 간 용량"이라고 합니다.

단계

1. 스토리지 * > * 스토리지 VM * 을 선택합니다.
2. 스토리지 VM의 이름을 클릭합니다.
3. 다음 측정값이 있는 막대 차트를 보여 주는 * Capacity * 섹션으로 스크롤합니다.
   - * 물리적 사용 *: 이 스토리지 VM의 모든 볼륨에서 사용된 물리적 스토리지의 합계
   - * 사용 가능 *: 이 스토리지 VM의 모든 볼륨에서 사용 가능한 용량의 합계입니다.
   - * Logical Used *: 이 스토리지 VM의 모든 볼륨에서 사용된 논리적 스토리지의 합계

측정에 대한 자세한 내용은 을 참조하십시오 "System Manager의 용량 측정".

스토리지 VM의 최대 용량 한도를 봅니다

ONTAP 9.13.1 부터는 스토리지 VM의 최대 용량 한도를 확인할 수 있습니다.

시작하기 전에

반드시 해야 합니다 "스토리지 VM의 최대 용량 제한을 설정합니다" 먼저 볼 수 있습니다.

단계

1. 스토리지 * > * 스토리지 VM * 을 선택합니다.

   최대 용량 측정값은 다음 두 가지 방법으로 볼 수 있습니다.

   - 스토리지 VM의 행에서 사용된 용량, 사용 가능한 용량 및 최대 용량을 보여주는 막대 차트가 포함된 * 최대 용량 * 열을 확인합니다.
   - 스토리지 VM의 이름을 클릭합니다. Overview * (개요 *) 탭에서 왼쪽 열의 최대 용량, 할당된 용량 및 용량 경고 임계값을 스크롤하여 봅니다.

관련 정보

- "스토리지 VM의 최대 용량 한도를 편집합니다"
- "System Manager의 용량 측정"

ONTAP 시스템 관리자의 문제를 파악하기 위해 하드웨어 구성을 확인하세요.

ONTAP 9.8부터 System Manager를 사용하여 네트워크 하드웨어 구성을 확인하고 하드웨어 시스템 및 케이블 연결 구성의 상태를 확인할 수 있습니다.

단계

하드웨어 구성을 보려면 다음 단계를 수행하십시오.

1. System Manager에서 * Cluster > Hardware * 를 선택합니다.
2. 구성 요소 위에 마우스를 올려 놓으면 상태 및 기타 세부 정보를 볼 수 있습니다.

   다양한 유형의 정보를 볼 수 있습니다.

   - 컨트롤러에 대한 정보
   - 디스크 쉘프 정보
   - 스토리지 스위치에 대한 정보
3. ONTAP 9.12.1부터 시스템 관리자에서 케이블 연결 정보를 볼 수 있습니다. 케이블 표시 * 확인란을 클릭하여 케이블 연결을 확인한 다음 케이블 위로 마우스를 가져가면 연결 정보를 볼 수 있습니다.
   - 케이블 연결에 대한 정보

컨트롤러에 대한 정보

다음을 볼 수 있습니다.

노드

- 전면과 후면을 볼 수 있습니다.
- 내부 디스크 쉘프가 있는 모델의 경우 전면 보기에서 디스크 레이아웃을 볼 수도 있습니다.
- 다음 플랫폼을 볼 수 있습니다.

플랫폼	ONTAP 버전의 System Manager에서 지원됨…										
	9.18.1	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8(미리보기 모드만 해당)
AFF A20 를 참조하십시오	예	예	예								
AFF A30 를 참조하십시오	예	예	예								
AFF A50 를 참조하십시오	예	예	예								
AFF A70 를 참조하십시오	예	예	예	예							
AFF A90 를 참조하십시오	예	예	예	예							
AFF A1K 를 참조하십시오	예	예	예	예							
AFF A150				예	예	예					
AFF A220				예	예	예	예	예	예	예	예

AFF A250				예	예	예	예	예	예	예	
AFF A300				예	예	예	예	예	예	예	예
AFF A320				예	예	예	예	예	예	예	
AFF A400				예	예	예	예	예	예	예	예
AFF A700				예	예	예	예	예	예	예	예
AFF A700s를 참조하십시오				예	예	예	예	예	예	예	
AFF A800				예	예	예	예	예	예	예	
AFF A900 탑재	예	예	예	예	예	예	예	예	예		
AFF C30 를 참조하십시오	예	예	예								
AFF C60 를 참조하십시오	예	예	예								
AFF C80 를 참조하십시오	예	예	예								
AFF C190				예	예	예	예	예	예	예	예
AFF C250				예	예	예	예 *	예 *	예 *		

AFF C400				예	예	예	예 *	예 *	예 *		
AFF C800	예	예	예	예	예	예	예 *	예 *	예 *		
ASA A150				예	예	예					
ASA A250				예	예	예					
ASA A400				예	예	예					
ASA A800				예	예	예					
ASA A900				예	예	예					
ASA C250을 참조하십시오	예	예	예	예	예	예					
ASA C400을 참조하십시오	예	예	예	예	예	예					
ASA C800을 참조하십시오	예	예	예	예	예	예					
AFX 1X	예	예									
FAS50	예	예	예								
FAS70를 참조하십시오	예	예	예	예							

FAS90를 참조하십시오	예	예	예	예							
500f로 설정합니다				예	예	예	예	예	예	예	
FAS2720				예	예	예	예	예			
FAS2750	예	예	예	예	예	예	예	예	예	예	예
FAS8300				예	예	예	예	예			
FAS8700				예	예	예	예	예			
FAS9000					예	예	예	예	예		
FAS9500					예	예	예	예	예		

포트

- 포트가 다운된 경우 빨간색으로 강조 표시된 포트가 표시됩니다.
- 포트 위로 마우스를 가져가면 포트 상태와 기타 세부 정보를 볼 수 있습니다.
- 콘솔 포트는 볼 수 없습니다.
- 참고 *:
  - ONTAP 9.11.1부터 SAS 포트가 오류 상태이거나 사용 중인 케이블로 연결된 포트가 오프라인이 되는 경우에만 빨간색으로 강조 표시됩니다. 포트가 오프라인이고 비활성화 상태이면 흰색으로 표시됩니다.
  - ONTAP 9.10.1 이하 버전의 경우 SAS 포트를 비활성화하면 빨간색으로 강조 표시됩니다.

FRU

FRU에 대한 정보는 FRU 상태가 최적이 아닌 경우에만 나타납니다.

- 노드나 섀시에서 PSU 장애가 발생했습니다.
- 노드에서 고온도가 감지되었습니다.
- 노드나 섀시의 팬 오류가 발생했습니다.

어댑터 카드

- 외부 카드를 삽입하면 부품 번호 필드가 정의된 카드가 슬롯에 표시됩니다.

- 포트가 카드에 표시됩니다.
- 지원되는 카드의 경우 해당 카드의 이미지를 볼 수 있습니다. 카드가 지원되는 부품 번호 목록에 없으면 일반 그래픽이 나타납니다.

디스크 쉘프 정보

다음을 볼 수 있습니다.

디스크 쉘프

- 전면 및 후면 보기를 표시할 수 있습니다.
- 다음 디스크 쉘프 모델을 볼 수 있습니다.

시스템이 실행 중인 경우…	그런 다음 System Manager를 사용하여 다음을 볼 수 있습니다.
ONTAP 9.9.1 이상	NOT_이(가) 있는 모든 셸프가 "서비스 종료" 또는 "가용성 종료"로 지정됨
ONTAP 9.8	DS4243, DS4486, DS212C, DS2246, DS224C, 및 NS224를 참조하십시오

쉘프 포트

- 포트 상태를 볼 수 있습니다.
- 포트가 연결되어 있는 경우 원격 포트 정보를 볼 수 있습니다.

쉘프 **FRU**

- PSU 장애 정보가 표시됩니다.

스토리지 스위치에 대한 정보

다음을 볼 수 있습니다.

스토리지 스위치

- 이 디스플레이에는 쉘프를 노드에 연결하는 데 사용되는 스토리지 스위치 역할을 하는 스위치가 표시됩니다.
- ONTAP 9.9.1부터 시스템 관리자는 스토리지 스위치와 클러스터 역할을 모두 수행하는 스위치에 대한 정보를 표시하며, 이 정보는 HA 쌍의 노드 간에도 공유할 수 있습니다.
- 다음 정보가 표시됩니다.
  - 스위치 이름
  - IP 주소입니다
  - 일련 번호입니다
  - SNMP 버전입니다
  - 시스템 버전입니다
- 다음과 같은 스토리지 스위치 모델을 볼 수 있습니다.

시스템이 실행 중인 경우…	그런 다음 System Manager를 사용하여 다음을 볼 수 있습니다.
ONTAP 9.11.1 이상	Cisco Nexus 3232C Cisco Nexus 9336C-FX2 NVIDIA SN2100
ONTAP 9.10.1 및 9.9.1	Cisco Nexus 3232C Cisco Nexus 9336C-FX2
ONTAP 9.8	Cisco Nexus 3232C

스토리지 스위치 포트

- 다음 정보가 표시됩니다.
  - ID 이름입니다
  - ID 인덱스입니다
  - 상태
  - 원격 연결
  - 기타 세부 정보

케이블 연결에 대한 정보

ONTAP 9.12.1부터 다음 케이블 연결 정보를 볼 수 있습니다.

- * 스토리지 브리지를 사용하지 않는 경우 컨트롤러, 스위치 및 쉘프 간 케이블 * 연결
- 케이블 양쪽 끝에 있는 포트의 ID 및 MAC 주소를 표시하는 * 연결 *

ONTAP 시스템 관리자를 사용하여 노드 관리

System Manager를 사용하면 클러스터에 노드를 추가하고 이름을 바꿀 수 있습니다. 또한 노드를 재부팅하고, 테이크오버하고, 제공할 수도 있습니다.

클러스터에 노드 추가

새 노드를 추가하여 클러스터의 크기와 기능을 확장할 수 있습니다.

시작하기 전에

새 노드를 클러스터에 이미 케이블로 연결했어야 합니다.

이 작업에 대해

ONTAP 9.8 이상 또는 ONTAP 9.7에서는 시스템 관리자를 사용하기 위한 별도의 프로세스가 있습니다.

ONTAP 9.8 이상 절차

- System Manager를 사용하여 클러스터에 노드 추가(ONTAP 9.8 이상) *

단계

1. 클러스터 > 개요 * 를 선택합니다.

   새 컨트롤러는 클러스터 네트워크에 연결된 노드로 표시되지만 클러스터에는 표시되지 않습니다.

2. 추가 * 를 선택합니다.
   - 노드가 클러스터에 추가됩니다.
   - 저장소가 암시적으로 할당됩니다.

ONTAP 9.7 절차

- System Manager(ONTAP 9.7)를 사용하여 클러스터에 노드 추가 *

단계

1. (클래식 버전으로 돌아가기) * 를 선택합니다.
2. 구성 > 클러스터 확장 * 을 선택합니다.

   System Manager가 새 노드를 자동으로 검색합니다.

3. 새 환경으로 전환 * 을 선택합니다.
4. 클러스터 > 개요 * 를 선택하여 새 노드를 확인하십시오.

서비스 프로세서를 종료, 재부팅 또는 편집합니다

노드를 재부팅 또는 종료할 때 HA 파트너가 자동으로 테이크오버를 실행합니다.

> 이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 노드를 종료하고 재부팅합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

단계

1. 클러스터 > 개요 * 를 선택합니다.

2. 노드 * 아래에서 를 선택합니다 ⋮.
3. 노드를 선택한 다음 * 시스템 종료 *, * 재부팅 * 또는 * 서비스 프로세서 편집 * 을 선택합니다.

   노드가 재부팅되어 반환을 기다리는 경우 * Giveback * 옵션도 사용할 수 있습니다.

   서비스 프로세서 편집 * 을 선택한 경우 * 수동 * 을 선택하여 IP 주소, 서브넷 마스크 및 게이트웨이를 입력하거나 * DHCP * 를 선택하여 동적 호스트 구성을 수행할 수 있습니다.

노드 이름을 바꿉니다

ONTAP 9.14.1부터 클러스터 개요 페이지에서 노드 이름을 변경할 수 있습니다.

> ⓘ 이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 노드의 이름을 바꾸려면. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

단계

1. 클러스터 * 를 선택합니다. 클러스터 개요 페이지가 표시됩니다.
2. 아래로 스크롤하여 * Nodes * 섹션으로 이동합니다.
3. 이름을 바꾸려는 노드 옆에 있는 을 선택하고 ⋮* Rename * 을 선택합니다.
4. 노드 이름을 수정한 다음 * Rename * 을 선택합니다.

라이센스 관리

ONTAP 라이센스 개요

라이센스는 하나 이상의 소프트웨어 사용 권한의 기록입니다. ONTAP 9.10.1부터 모든 라이센스는 여러 기능을 사용할 수 있는 단일 파일인 NetApp 라이센스 파일(NLF)로 제공됩니다. 2023년 5월부터 모든 AFF 시스템(A-series 및 C-series 모두)과 FAS 시스템은 ONTAP One 소프트웨어 제품군 또는 ONTAP 기본 소프트웨어 제품군과 함께 판매되며, 2023년 6월부터 모든 ASA 시스템은 SAN용 ONTAP One과 함께 판매됩니다. 각 소프트웨어 제품군은 ONTAP 9.10.1에 처음 도입된 별도의 NLF 번들을 대체하여 단일 NLF로 제공됩니다.

ONTAP One에 포함된 라이선스

ONTAP One에는 사용 가능한 모든 라이센스 기능이 포함되어 있습니다. 표에 나와 있는 것처럼 이전 코어 번들, 데이터 보호 번들, 보안 및 규정 준수 번들, 하이브리드 클라우드 번들 및 암호화 번들의 콘텐츠가 함께 포함됩니다. 암호화는 제한된 국가에서만 사용할 수 있습니다.

이전 번들 이름입니다	ONTAP 키가 포함됩니다

코어 번들	플랙스클론
	SnapRestore
	NFS, SMB, S3
	FC, iSCSI를 지원합니다
	NVMe-oF
보안 및 규정 준수 번들	자율 랜섬웨어 보호
	MTKM입니다
	SnapLock
데이터 보호 번들	SnapMirror(비동기식, 동기식, 액티브 동기식)
	SnapCenter
	NetApp 타겟에 대한 SnapMirror S3
하이브리드 클라우드 번들	SnapMirror 클라우드
	NetApp 이외의 타겟에 대한 SnapMirror S3
암호화 번들	NetApp 볼륨 암호화
	신뢰할 수 있는 플랫폼 모듈

라이센스는 **ONTAP One**에 포함되지 않습니다

ONTAP One에는 다음을 포함하여 NetApp의 클라우드 제공 서비스가 포함되지 않습니다.

- NetApp 클라우드 계층화
- 데이터 인프라 인사이트
- NetApp 백업 및 복구
- 데이터 거버넌스

기존 시스템을 위한 **ONTAP One**

현재 NetApp 지원을 받고 있지만 ONTAP One으로 업그레이드되지 않은 기존 시스템이 있는 경우 해당 시스템의 기존 라이센스는 계속 유효하며 예상대로 계속 작동합니다. 예를 들어, SnapMirror 라이센스가 기존 시스템에 이미 설치되어 있는 경우, 새로운 SnapMirror 라이센스를 얻기 위해 ONTAP One으로 업그레이드할 필요가 없습니다. 그러나 기존 시스템에 SnapMirror 라이센스가 설치되어 있지 않은 경우 이 라이센스를 얻는 유일한 방법은 추가 비용을 지불하고 ONTAP One으로 업그레이드하는 것입니다.

2023년 6월부터 28자 라이센스 키를 사용하는 ONTAP 시스템도 지원합니다 "ONTAP One 또는 ONTAP 기본 호환성 번들로 업그레이드하십시오".

ONTAP Base에 포함된 라이센스

ONTAP Base는 ONTAP 시스템용 ONTAP One을 대체하는 선택적 소프트웨어 제품군입니다. 전용 테스트 또는 개발 환경을 위한 비운영 시스템과 같이 SnapMirror, SnapCenter 등의 데이터 보호 기술과 자율적 랜섬웨어와 같은 보안 기능이 필요하지 않은 특정 사용 사례를 위한 것입니다. 추가 라이센스는 ONTAP Base에 추가할 수 없습니다. SnapMirror와 같은 추가 라이센스를 사용하려면 ONTAP One으로 업그레이드해야 합니다.

이전 번들 이름입니다	ONTAP 키가 포함됩니다
코어 번들	플랙스클론
	SnapRestore
	NFS, SMB, S3
	FC, iSCSI를 지원합니다
	NVMe-oF
암호화 번들	NetApp 볼륨 암호화
	신뢰할 수 있는 플랫폼 모듈

ONTAP One for SAN에 포함된 라이센스입니다

SAN용 ONTAP One은 ASA A-Series 및 C-Series 시스템에 사용할 수 있습니다. 이 제품군은 SAN에 사용할 수 있는 유일한 소프트웨어 제품군입니다. ONTAP One for SAN에는 다음 라이센스가 포함되어 있습니다.

ONTAP 키가 포함됩니다
플랙스클론
SnapRestore
FC, iSCSI를 지원합니다
NVMe-oF
MTKM입니다
SnapLock
SnapMirror(비동기식, 동기식, 액티브 동기식)
SnapCenter
SnapMirror 클라우드
NetApp 볼륨 암호화
신뢰할 수 있는 플랫폼 모듈

그 밖의 라이센스 제공 방법

ONTAP 8.2 ~ ONTAP 9.9.1에서는 라이센스 키가 28자 문자열로 전달되고 ONTAP 기능당 키가 하나씩 있습니다. ONTAP 8.2~ONTAP 9.9.1을 사용하는 경우 ONTAP CLI를 사용하여 라이센스 키를 설치합니다.

ONTAP 9.10.1에서는 System Manager 또는 CLI를 사용하여 28자 라이센스 키 설치를 지원합니다. 그러나 기능에 대해 NLF 라이센스가 설치된 경우 동일한 기능에 대해 NetApp 라이센스 파일 위에 28자의 라이센스 키를 설치할 수 없습니다. System Manager를 사용하여 NLF 또는 라이센스 키를 설치하는 방법에 대한 자세한 내용은 를 참조하십시오."ONTAP 라이센스를 설치합니다"

관련 정보

"시스템에 NLF가 이미 있는 경우 ONTAP One 라이센스를 얻는 방법"

"지원 사이트를 사용하여 ONTAP 소프트웨어 권한 및 관련 라이센스 키를 확인하는 방법"

"NetApp: ONTAP 소유 권한 위험 상태입니다"

NetApp Support 사이트에서 NetApp 라이센스 파일(NLF)을 다운로드합니다

시스템에서 ONTAP 9.10.1 이상을 실행 중인 경우 NetApp Support 사이트에서 ONTAP One용 NLF 또는 ONTAP Core용 NLF를 다운로드하여 기존 시스템의 번들 라이센스 파일을 업그레이드할 수 있습니다.

SnapMirror 클라우드 및 SnapMirror S3 라이센스는 ONTAP One에 포함되지 않습니다. ONTAP One 호환성 번들의 일부이며, ONTAP One과 를 사용하는 경우 무료로 이용할 수 있습니다"별도로 요청하십시오".

단계

기존 NetApp 라이센스 파일 번들이 있는 시스템 및 ONTAP 9.10.1 이상을 실행하는 시스템에서 NetApp 라이센스 파일로 변환된 28자 라이센스 키가 있는 시스템의 경우 ONTAP One 라이센스 파일을 다운로드할 수 있습니다. 유료로 ONTAP Base에서 ONTAP One으로 시스템을 업그레이드할 수도 있습니다.

기존 **NLF**를 업그레이드합니다

1. NetApp 세일즈 팀에 문의하여 업그레이드하거나 변환할 라이센스 파일 번들을 요청합니다(예: ONTAP Base에서 ONTAP One으로 또는 코어 번들 및 데이터 보호 번들을 ONTAP One으로).

   요청이 처리되면 netappsw@netapp.com 에서 "SO#[SO 번호]에 대한 NetApp 소프트웨어 라이센스 알림 "이라는 제목의 이메일을 받게 되며 이메일에는 라이센스 일련 번호가 포함된 PDF 첨부 파일이 포함됩니다.

2. 에 로그인합니다 "NetApp Support 사이트".
3. 시스템 > 소프트웨어 라이센스 * 를 선택합니다.
4. 메뉴에서 * 일련 번호 * 를 선택하고 받은 일련 번호를 입력한 다음 * 새 검색 * 을 클릭합니다.
5. 변환할 라이센스 번들을 찾습니다.
6. 각 라이센스 번들에 대해 * Get NetApp License File * 을 클릭하고 NLF를 사용할 수 있으면 다운로드합니다.
7. "설치합니다" ONTAP One 파일.

라이센스 키에서 변환된 **NLF** 업그레이드

1. 에 로그인합니다 "NetApp Support 사이트".
2. 시스템 > 소프트웨어 라이센스 * 를 선택합니다.
3. 메뉴에서 * 일련 번호 * 를 선택하고 시스템 일련 번호를 입력한 다음 * 새 검색 * 을 클릭합니다.
4. 변환할 라이센스를 찾은 다음 * Eligibility * 열에서 * Check * 를 클릭합니다.
5. 적합성 확인 양식 * 에서 * 9.10.x 이상에 대한 라이센스 생성 * 을 클릭합니다.
6. 적합성 확인 양식 * 을 닫습니다.

   라이센스가 생성되려면 최소 2시간 동안 기다려야 합니다.

7. 1-3단계를 반복합니다.
8. ONTAP One 라이센스를 찾아 * Get NetApp License File * 을 클릭하고 전달 방법을 선택합니다.
9. "설치합니다" ONTAP One 파일.

ONTAP에서 NetApp 라이센스를 설치합니다

NLF를 설치하는 기본 방법인 System Manager를 사용하여 NLF(NetApp 라이센스 파일) 및 라이센스 키를 설치하거나 ONTAP CLI를 사용하여 라이센스 키를 설치할 수 있습니다. ONTAP 9.10.1 이상에서는 NetApp 라이센스 파일을 통해 기능이 활성화되고, ONTAP 9.10.1 이전 릴리스에서는 라이센스 키를 사용하여 ONTAP 기능을 사용할 수 있습니다.

단계

이미 "NetApp 라이센스 파일을 다운로드했습니다" 또는 라이센스 키가 있는 경우, System Manager 또는 ONTAP CLI를 사용하여 NLF 및 28자 라이센스 키를 설치할 수 있습니다.

System Manager - ONTAP 9.8 이상

1. 클러스터 > 설정 * 을 선택합니다.
2. 라이센스 * 에서 를 선택합니다 →.
3. 찾아보기 * 를 선택합니다. 다운로드한 NetApp 라이센스 파일을 선택합니다.
4. 추가하려는 라이센스 키가 있는 경우 * 28자 라이센스 키 사용 * 을 선택하고 키를 입력합니다.

System Manager - ONTAP 9.7 이하

1. 구성 > 클러스터 > 라이센스 * 를 선택합니다.
2. 라이센스 * 에서 를 선택합니다 →.
3. 패키지 * 창에서 * 추가 * 를 클릭합니다.
4. 라이센스 패키지 추가 * 대화 상자에서 * 파일 선택 * 을 클릭하여 다운로드한 NetApp 라이센스 파일을 선택한 다음 * 추가 * 를 클릭하여 파일을 클러스터에 업로드합니다.

CLI를 참조하십시오

1. 하나 이상의 라이센스 키 추가:

```
system license add
```

다음 예에서는 파일이 이 위치에 있는 경우 로컬 노드 "/mroot/etc/lic_file"에서 라이센스를 설치합니다.

```
cluster1::> system license add -use-license-file true
```

다음 예에서는 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA 및 BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB 키가 포함된 라이선스 목록을 클러스터에 추가한다.

```
cluster1::> system license add -license-code
AAAAAAAAAAAAAAAAAAAAAAAAAAA, BBBBBBBBBBBBBBBBBBBBBBBBBBB
```

ONTAP 명령 참조에서 https://docs .NetApp.com/us-en/ONTAP-cli/system-license-add.html 명령 링크에 대해 자세히[`system license add` 알아보십시오.

ONTAP 라이센스 관리

System Manager 또는 ONTAP CLI를 사용하여 라이센스 일련 번호 보기, 라이센스 상태 확인, 라이센스 제거 등 시스템에 설치된 라이센스를 보고 관리할 수 있습니다.

라이센스에 대한 세부 정보를 봅니다

단계

라이센스에 대한 세부 정보를 보는 방법은 사용 중인 ONTAP 버전과 System Manager를 사용하는지 ONTAP CLI를

사용하는지 여부에 따라 다릅니다.

System Manager - ONTAP 9.8 이상

1. 특정 기능 라이센스에 대한 세부 정보를 보려면 * 클러스터 > 설정 * 을 선택합니다.
2. 라이센스 * 에서 를 선택합니다 →.
3. 기능 * 을 선택합니다.
4. 보려는 라이센스 기능을 찾아 선택하여 ⌄ 라이센스 세부 정보를 봅니다.

System Manager - ONTAP 9.7 이하

1. 구성 > 클러스터 > 라이센스 * 를 선택합니다.
2. Licenses * 창에서 적절한 작업을 수행합니다.
3. 세부 정보 * 탭을 클릭합니다.

CLI를 참조하십시오

1. 설치된 라이센스에 대한 세부 정보 표시:

```
system license show
```

라이센스를 삭제합니다

System Manager - ONTAP 9.8 이상

1. 라이센스를 삭제하려면 * 클러스터 > 설정 * 을 선택합니다.
2. 라이센스 * 에서 를 선택합니다 →.
3. 기능 * 을 선택합니다.
4. 삭제하려는 라이센스 기능을 선택하고 * 기존 키 삭제 * 를 선택합니다.

System Manager - ONTAP 9.7 이하

1. 구성 > 클러스터 > 라이센스 * 를 선택합니다.
2. Licenses * 창에서 적절한 작업을 수행합니다.

원하는 작업	수행할 작업...
노드나 마스터 라이센스에서 특정 라이센스 패키지를 삭제합니다	세부 정보 * 탭을 클릭합니다.
클러스터의 모든 노드에서 특정 라이센스 패키지를 삭제합니다	패키지 * 탭을 클릭합니다.

3. 삭제할 소프트웨어 라이센스 패키지를 선택한 다음 * 삭제 * 를 클릭합니다.

   한 번에 하나의 라이센스 패키지만 삭제할 수 있습니다.

4. 확인 확인란을 선택한 다음 * 삭제 * 를 클릭합니다.

CLI를 참조하십시오

1. 라이센스 삭제:

```
system license delete
```

다음 예제에서는 클러스터에서 CIFS 및 일련 번호 1-81-0000000000000000123456이라는 라이센스를 삭제합니다.

```
cluster1::> system license delete -serial-number 1-81-
0000000000000000000123456 -package CIFS
```

다음 예에서는 일련 번호 123456789에 대해 설치된 라이센스 코어 번들에 있는 모든 라이센스를 클러스터에서 삭제합니다.

```
cluster1::> system license delete { -serial-number 123456789
-installed-license "Core Bundle" }
```

관련 정보

"라이센스 관리를 위한 ONTAP CLI 명령"

"ONTAP 명령 참조입니다"

라이센스 유형 및 라이센스 방식

라이센스 유형과 라이센스 방법을 이해하면 클러스터의 라이센스를 관리하는 데 도움이 됩니다.

사용권 유형

패키지에는 다음 라이센스 유형 중 하나 이상이 클러스터에 설치될 수 있습니다. 'system license show' 명령은 설치된 패키지 라이센스 유형 또는 유형을 표시합니다.

- Standard 라이선스('라이선스')

  표준 라이센스는 노드 잠김 라이센스입니다. 특정 시스템 일련 번호(_controller 일련 번호 _ 라고도 함)가 있는 노드에 대해 발행됩니다. 표준 라이센스는 일련 번호가 일치하는 노드에 대해서만 유효합니다.

  표준 노드 잠금 라이센스를 설치하면 노드에 라이센스가 부여된 기능이 부여됩니다. 클러스터에 라이센스가 부여된 기능을 사용하려면 해당 기능에 대해 하나 이상의 노드에 라이센스가 있어야 합니다. 기능에 대한 사용 권한이 없는 노드에서 라이센스가 부여된 기능을 사용하지 못할 수 있습니다.

- 사이트 라이선스('사이트')

  사이트 라이센스는 특정 시스템 일련 번호에 연결되지 않습니다. 사이트 라이센스를 설치하면 클러스터의 모든 노드에 라이센스가 부여된 기능이 부여됩니다. 'system license show' 명령은 클러스터 일련 번호 아래에 사이트 라이센스를 표시합니다.

  클러스터에 사이트 라이센스가 있고 클러스터에서 노드를 제거할 경우 노드에 사이트 라이센스가 포함되지 않으며 라이센스가 부여된 기능을 더 이상 사용할 수 없습니다. 사이트 라이센스가 있는 클러스터에 노드를 추가하면 해당 노드는 사이트 라이센스에 의해 부여된 기능을 자동으로 사용할 수 있습니다.

- 평가판 라이센스(데모)

  평가판은 일정 기간(system license show 명령으로 표시됨) 이후에 만료되는 임시 라이선스입니다. 이 기능을 사용하면 사용 권한을 구입하지 않고도 특정 소프트웨어 기능을 사용할 수 있습니다. 클러스터 전체 라이센스이며 노드의 특정 일련 번호에 연결되지 않습니다.

  클러스터에 패키지에 대한 평가 라이센스가 있고 클러스터에서 노드를 제거하는 경우 노드에 평가판 라이센스가 포함되지 않습니다.

라이센스 방식

클러스터 전체 라이선스(사이트)와 노드 잠금 라이선스(라이선스 유형)를 모두 설치할 수 있다. 따라서 설치된 패키지에 클러스터에 여러 라이센스 유형이 있을 수 있습니다. 그러나 클러스터에는 패키지에 대해 하나의 _licensed 메소드_만 있습니다. system license status show 명령의 'licensed method' 필드에 패키지에 사용되는 권한이 표시됩니다. 명령은 다음과 같이 라이센스가 부여된 방법을 결정합니다.

- 패키지에 클러스터에 하나의 라이센스 유형만 설치되어 있는 경우 설치된 라이센스 유형이 라이센스 방식입니다.
- 패키지에 클러스터에 설치된 라이센스가 없는 경우 라이센스 부여 방법은 "없음"입니다.

- 패키지에 클러스터에 여러 개의 사용권 유형이 설치되어 있는 경우 사용권 유형은 '사이트', '사용권', '데모' 순으로 결정됩니다.

  예를 들면 다음과 같습니다.

  - 사이트 라이센스, 표준 라이센스 및 패키지 평가 라이센스가 있는 경우 클러스터의 패키지에 대한 라이센스 부여 방법은 '사이트'입니다.
  - 패키지에 대한 표준 라이센스와 평가판 라이센스가 있는 경우 클러스터의 패키지에 대한 라이센스 방법은 "라이센스"입니다.
  - 패키지에 대한 평가판 라이선스만 있는 경우 클러스터의 패키지에 대한 라이선스 방식은 '데모'입니다.

ONTAP에서 라이센스를 관리하는 명령입니다

ONTAP CLI를 사용할 수 있습니다 `system license` 클러스터에 대한 기능 라이센스를 관리하는 명령입니다. 를 사용합니다 `system feature-usage` 기능 사용을 모니터링하는 명령입니다.

이 항목에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

다음 표에는 라이센스 관리를 위한 몇 가지 일반적인 CLI 명령과 추가 정보를 위한 Command man 페이지에 대한 링크가 나와 있습니다.

원하는 작업	이 명령 사용...
다음을 포함하여 라이센스가 필요한 모든 패키지와 현재 라이센스 상태를 표시합니다. • 패키지 이름입니다 • 라이센스 방식 • 만료 날짜(해당하는 경우	"시스템 라이센스 표시 - 상태"
만료되었거나 사용되지 않은 라이센스를 표시하거나 제거합니다	"시스템 라이센스 정리"
노드별로 클러스터의 기능 사용 요약 정보를 표시합니다	"시스템 기능 - 사용법 표시 - 요약"
노드별 및 주별로 클러스터의 기능 사용 상태를 표시합니다	"시스템 기능 - 사용법 표시 - 기록"
각 라이센스 패키지에 대한 라이센스 권한 위험 상태를 표시합니다	"시스템 라이센스 소유 권한 - 위험이 표시됩니다"

관련 정보

- "ONTAP 명령 참조입니다"

- "NetApp 기술 자료: ONTAP 9.10.1 이상 라이선스 개요"
- "시스템 관리자를 사용하여 NetApp 라이센스 파일을 설치합니다"
- "시스템 기능"

CLI를 통한 클러스터 관리

ONTAP CLI를 사용한 클러스터 관리에 대해 자세히 알아보십시오

CLI(Command-Line Interface)를 사용하여 ONTAP 시스템을 관리할 수 있습니다. ONTAP 관리 인터페이스, 클러스터에 액세스, 노드 관리 등을 사용할 수 있습니다.

다음과 같은 상황에서 이러한 절차를 사용해야 합니다.

- ONTAP 관리자 기능의 범위를 이해하려고 합니다.
- System Manager나 자동화된 스크립팅 도구가 아니라 CLI를 사용하려고 합니다.

관련 정보

CLI 구문 및 사용에 대한 자세한 내용은 "ONTAP 명령 참조입니다" 설명서를 참조하십시오.

클러스터 및 SVM 관리자

ONTAP 클러스터 및 SVM 관리자 역할에 대해 알아보십시오

클러스터 관리자는 전체 클러스터와 SVM(이전 명칭: vserver)에 포함된 스토리지 가상 머신(SVM)을 관리합니다. SVM 관리자는 자체 데이터 SVM만 관리합니다.

클러스터 관리자는 전체 클러스터와 리소스를 관리할 수 있습니다. 또한 데이터 SVM을 설정하고 SVM 관리를 SVM 관리자에게 위임할 수도 있습니다. 클러스터 관리자가 보유한 특정 기능은 액세스 제어 역할에 따라 다릅니다. 기본적으로 ""admin" 계정 이름 또는 역할 이름을 가진 클러스터 관리자에는 클러스터 및 SVM을 관리하는 모든 기능이 있습니다.

SVM 관리자는 볼륨, 프로토콜, LIF 및 서비스와 같은 자체 SVM 스토리지 및 네트워크 리소스만 관리할 수 있습니다. SVM 관리자가 보유한 특정 기능은 클러스터 관리자가 할당한 액세스 제어 역할에 따라 다릅니다.

ONTAP CLI(Command-Line Interface)는 출력에서 _Vserver_를 계속 사용하며, 명령 또는 매개 변수 이름으로 'vserver'를 사용하는 것은 변경되지 않았습니다.

ONTAP System Manager에 대한 웹 브라우저 액세스를 사용하거나 사용하지 않도록 설정합니다

웹 브라우저에서 System Manager에 액세스할 수 있도록 설정하거나 해제할 수 있습니다. System Manager 로그도 볼 수 있습니다.

[`true|false`] 를 사용하여 웹 브라우저의 System Manager 액세스를 제어할 수 `vserver services web modify -name sysmgr -vserver <cluster_name> -enabled` 있습니다.

System Manager 로깅은 System Manager에 액세스할 때 클러스터 관리 LIF를 호스팅하는 노드의 '/mroot/etc/log/mgmtg.log' 파일에 기록됩니다. 브라우저를 사용하여 로그 파일을 볼 수 있습니다. System Manager

로그는 AutoSupport 메시지에도 포함되어 있습니다.

ONTAP 클러스터 관리 서버에 대해 자세히 알아보십시오

클러스터 관리 서버는 *admin*SVM이라고 하며, 클러스터를 관리할 수 있는 단일 엔티티로 제공하는 전문화된 스토리지 가상 시스템(SVM) 구현입니다. 클러스터 관리 서버는 최상위 관리 도메인 역할을 할 뿐만 아니라 데이터 SVM에 논리적으로 속하지 않는 리소스를 소유합니다.

클러스터 관리 서버는 항상 클러스터에서 사용할 수 있습니다. 콘솔 또는 클러스터 관리 LIF를 통해 클러스터 관리 서버에 액세스할 수 있습니다.

홈 네트워크 포트에 장애가 발생하면 클러스터 관리 LIF가 자동으로 클러스터의 다른 노드로 페일오버됩니다. 사용 중인 관리 프로토콜의 연결 특성에 따라 페일오버를 인지할 수도 있고 그렇지 않을 수도 있습니다. 연결 없는 프로토콜(예: SNMP)을 사용하거나 제한된 연결(예: HTTP)이 있는 경우 장애 조치를 알아차리지 못할 수 있습니다. 하지만 장기적인 연결(예: SSH)을 사용하는 경우 페일오버 후에 클러스터 관리 서버에 다시 연결해야 합니다.

클러스터를 생성할 때 해당 IP 주소, 넷마스크, 게이트웨이 및 포트를 포함한 클러스터 관리 LIF의 모든 특성이 구성됩니다.

데이터 SVM 또는 노드 SVM과 달리 클러스터 관리 서버에는 시스템 볼륨을 호스팅할 수 있지만 루트 볼륨 또는 호스트 사용자 볼륨이 없습니다. 또한 클러스터 관리 서버에는 클러스터 관리 유형의 LIF만 있을 수 있습니다.

'vserver show' 명령을 실행하면 클러스터 관리 서버가 해당 명령의 출력 목록에 표시됩니다.

ONTAP 클러스터의 **SVM** 유형

클러스터는 4가지 SVM 유형으로 구성되어 클러스터와 리소스, 클라이언트 및 애플리케이션에 대한 데이터 액세스를 관리하는 데 도움이 됩니다.

클러스터에는 다음과 같은 SVM 유형이 포함됩니다.

- SVM 관리

  클러스터 설정 프로세스에서 클러스터용 SVM 관리자를 자동으로 생성합니다. admin SVM은 클러스터를 나타냅니다.

- 노드 SVM

  노드가 클러스터에 결합될 때 노드 SVM이 생성되고, 노드 SVM은 클러스터의 개별 노드를 나타냅니다.

- 시스템 SVM(고급)

  IPspace에서 클러스터 레벨 통신을 위해 시스템 SVM이 자동으로 생성됩니다.

- 데이터 SVM

  데이터 SVM은 SVM을 제공하는 데이터를 나타냅니다. 클러스터 설정 후 클러스터 관리자는 데이터 SVM을 생성하고 볼륨을 이러한 SVM에 추가하여 클러스터에서 데이터를 쉽게 액세스할 수 있도록 해야 합니다.

  클러스터에서 클라이언트에 데이터를 제공하려면 하나 이상의 데이터 SVM이 있어야 합니다.

달리 지정되지 않은 경우 SVM이란 용어는 데이터(데이터 지원) SVM을 의미합니다.

CLI에서 SVM은 vserver로 표시됩니다.

CLI를 사용하여 클러스터에 액세스(클러스터 관리자만 해당)

노드의 시리얼 포트를 사용하여 **ONTAP** 클러스터에 액세스합니다

노드의 시리얼 포트에 연결된 콘솔에서 클러스터에 직접 액세스할 수 있습니다.

단계

1. 콘솔에서 Enter 키를 누릅니다.

   시스템이 로그인 프롬프트로 응답합니다.

2. 로그인 프롬프트에서 다음 중 하나를 수행합니다.

를 사용하여 클러스터에 액세스하는 방법	다음 계정 이름을 입력하십시오...
기본 클러스터 계정입니다	' * admin * '
대체 관리 사용자 계정입니다	'*username*'

   시스템이 암호 프롬프트로 응답합니다.

3. admin 또는 administrative 사용자 계정의 암호를 입력한 다음 Enter 키를 누릅니다.

SSH 요청을 사용하여 **ONTAP** 클러스터에 액세스합니다

ONTAP 클러스터에 SSH 요청을 전송하여 관리 작업을 수행할 수 있습니다. SSH는 기본적으로 사용하도록 설정됩니다.

시작하기 전에

- 'sh'를 액세스 방법으로 사용하도록 구성된 사용자 계정이 있어야 합니다.

  `-application`명령의 매개 변수는 `security login` 사용자 계정에 대한 액세스 방법을 지정합니다. 에 대한 자세한 내용은 `security login` link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html#description["ONTAP 명령 참조입니다"^]을 참조하십시오.

- AD(Active Directory) 도메인 사용자 계정을 사용하여 클러스터에 액세스하는 경우 CIFS 지원 스토리지 VM을 통해 클러스터에 대한 인증 터널을 설정해야 하며 AD 도메인 사용자 계정도 를 사용하여 클러스터에 추가되어야 합니다 `ssh` 액세스 방법 및 로 `domain` 인증 방법으로 사용합니다.

이 작업에 대해

- OpenSSH 5.7 이상 클라이언트를 사용해야 합니다.

- SSH v2 프로토콜만 지원되며 SSH v1은 지원되지 않습니다.
- ONTAP는 노드당 최대 64개의 동시 SSH 세션을 지원합니다.

  클러스터 관리 LIF가 노드에 상주하는 경우 이 제한을 노드 관리 LIF와 공유합니다.

  들어오는 연결의 비율이 초당 10보다 높을 경우 서비스가 60초 동안 일시적으로 비활성화됩니다.

- ONTAP는 SSH에 대해 AES 및 3DES 암호화 알고리즘(_ciphers _ 라고도 함)만 지원합니다.

  AES는 키 길이가 128, 192 및 256비트인 경우 지원됩니다. 3DES는 원래 DES와 마찬가지로 키 길이가 56비트이지만 세 번 반복됩니다.

- FIPS 모드가 켜져 있는 경우 SSH 클라이언트는 연결이 성공할 수 있도록 Elliptic Curve Digital Signature Algorithm(ECDSA) 공개 키 알고리즘과 협상해야 합니다.
- Windows 호스트에서 ONTAP CLI에 액세스하려는 경우 PuTTY와 같은 타사 유틸리티를 사용할 수 있습니다.
- Windows AD 사용자 이름을 사용하여 ONTAP에 로그인하는 경우 ONTAP에서 AD 사용자 이름과 도메인 이름을 만들 때 사용한 대문자나 소문자를 동일하게 사용해야 합니다.

  AD 사용자 이름과 도메인 이름은 대소문자를 구분하지 않습니다. 그러나 ONTAP 사용자 이름은 대/소문자를 구분합니다. ONTAP에서 생성된 사용자 이름과 AD에서 생성된 사용자 이름 간의 케이스 불일치로 인해 로그인 오류가 발생합니다.

SSH 인증 옵션

- ONTAP 9.3부터 가능합니다 "SSH 다단계 인증 지원" 로컬 관리자 계정의 경우.

  SSH 다단계 인증을 사용하면 공개 키와 암호를 사용하여 사용자를 인증할 수 있습니다.

- ONTAP 9.4부터 가능합니다 "SSH 다단계 인증 지원" LDAP 및 NIS 원격 사용자의 경우
- ONTAP 9.13.1 부터는 선택적으로 SSH 인증 프로세스에 인증서 유효성 검사를 추가하여 로그인 보안을 강화할 수 있습니다. 이렇게 하려면 "X.509 인증서를 공개 키와 연결합니다" 계정이 사용하는 것입니다. SSH 공개 키와 X.509 인증서를 모두 사용하여 SSH에 로그인하는 경우 ONTAP는 SSH 공개 키로 인증하기 전에 X.509 인증서의 유효성을 검사합니다. 인증서가 만료되거나 해지되고 SSH 공개 키가 자동으로 비활성화되면 SSH 로그인이 거부됩니다.
- ONTAP 9.14.1부터 ONTAP 관리자는 다음을 수행할 수 있습니다 "SSH 인증 프로세스에 Cisco Duo 2단계 인증을 추가합니다" 로그인 보안 강화 Cisco Duo 인증을 활성화한 후 처음 로그인할 때 사용자는 SSH 세션에 대한 인증자로 사용할 장치를 등록해야 합니다.
- ONTAP 9.15.1부터 관리자가 수행할 수 있습니다 "동적 권한 부여를 구성합니다" 사용자의 신뢰 점수에 따라 SSH 사용자에게 추가 적응형 인증을 제공합니다.

단계

1. ONTAP 클러스터의 네트워크에 액세스할 수 있는 호스트에서 를 입력합니다 `ssh` 다음 형식 중 하나로 된 명령:
   - '* ssh_username@hostname_or_ip_[*command*] *'
   - '* ssh-l_username hostname_or_ip_[*command*] * '

AD 도메인 사용자 계정을 사용하는 경우 '*username*'을 '*domainname\\AD_accountname*'(도메인 이름 뒤에 이중 백슬래시를 사용하여) 또는 '"*domainname\AD_accountname*"'(큰따옴표로 묶고 도메인 이름 뒤에 백슬래시를 하나씩 붙여야 합니다) 형식으로 지정해야 합니다.

'*hostname_or_ip*'은 클러스터 관리 LIF 또는 노드 관리 LIF의 호스트 이름 또는 IP 주소입니다. 클러스터 관리 LIF를 사용하는 것이 좋습니다. IPv4 또는 IPv6 주소를 사용할 수 있습니다.

SSH-Interactive 세션에는 '*command*'가 필요하지 않습니다.

SSH 요청의 예

다음 예에서는 사용자 계정 ""Joe""가 클러스터 관리 LIF가 10.72.137.28인 클러스터에 액세스하는 SSH 요청을 발행하는 방법을 보여줍니다.

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

다음 예에서는 "DOMAIN1" 도메인의 사용자 계정 ""John""이 클러스터 관리 LIF가 10.72.137.28인 클러스터에 액세스하기 위한 SSH 요청을 실행할 수 있는 방법을 보여줍니다.

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

다음 예에서는 사용자 계정 ""Joe""가 클러스터 관리 LIF가 10.72.137.32인 클러스터에 액세스하는 SSH MFA 요청을 발행하는 방법을 보여줍니다.

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

관련 정보

"관리자 인증 및 RBAC"

ONTAP SSH 로그인 보안

ONTAP 9.5부터 이전 로그인에 대한 정보, 로그인 시도 실패 및 마지막으로 성공한 로그인 이후 권한 변경 내용을 볼 수 있습니다.

SSH admin 사용자로 로그인하면 보안 관련 정보가 표시됩니다. 다음 조건에 대한 경고가 표시됩니다.

- 계정 이름이 마지막으로 로그인한 시간입니다.
- 마지막으로 성공한 로그인 이후 실패한 로그인 시도 횟수입니다.
- 마지막 로그인 이후 역할이 변경되었는지 여부(예: admin 계정의 역할이 "admin"에서 "backup"으로 변경된 경우)
- 마지막 로그인 이후 역할의 추가, 수정 또는 삭제 기능이 수정되었는지 여부

표시된 정보가 의심스러운 경우 즉시 보안 부서에 문의해야 합니다.

로그인할 때 이 정보를 얻으려면 다음 필수 구성 요소가 충족되어야 합니다.

- ONTAP에서 SSH 사용자 계정을 프로비저닝해야 합니다.
- SSH 보안 로그인을 생성해야 합니다.
- 로그인 시도가 성공해야 합니다.

SSH 로그인 보안에 대한 제한 및 기타 고려 사항

SSH 로그인 보안 정보에는 다음과 같은 제한 및 고려 사항이 적용됩니다.

- 이 정보는 SSH 기반 로그인에만 사용할 수 있습니다.
- LDAP/NIS 및 AD 계정과 같은 그룹 기반 관리자 계정의 경우, 사용자는 자신이 속한 그룹이 ONTAP에서 관리자 계정으로 할당된 경우 SSH 로그인 정보를 볼 수 있습니다.

  그러나 이러한 사용자에 대해서는 사용자 계정의 역할 변경에 대한 알림을 표시할 수 없습니다. 또한 ONTAP에서 admin 계정으로 프로비저닝된 AD 그룹에 속한 사용자는 마지막으로 로그인한 이후 실패한 로그인 시도 횟수를 볼 수 없습니다.
- ONTAP에서 사용자 계정을 삭제하면 해당 사용자에 대해 유지되는 정보가 삭제됩니다.
- SSH가 아닌 애플리케이션 접속에 대한 정보는 표시되지 않습니다.

SSH 로그인 보안 정보의 예

다음 예에서는 로그인 후 표시되는 정보의 유형을 보여 줍니다.

- 이 메시지는 로그인에 성공할 때마다 표시됩니다.

```
Last Login : 7/19/2018 06:11:32
```

- 마지막으로 성공한 로그인 이후 로그인 시도가 실패한 경우 다음 메시지가 표시됩니다.

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- 로그인 시도 실패 및 마지막 로그인 후 권한이 수정된 경우 다음 메시지가 표시됩니다.

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

ONTAP 클러스터에 대한 텔넷 또는 RSH 액세스를 설정합니다

보안 모범 사례로 Telnet 및 RSH는 기본적으로 비활성화되어 있습니다. 클러스터가 텔넷 또는 RSH 요청을 수락하도록 하려면 기본 관리 서비스 정책에서 서비스를 사용하도록 설정해야 합니다.

Telnet과 RSH는 보안 프로토콜이 아니므로 SSH를 사용하여 클러스터에 액세스하는 것을 고려해야 합니다. SSH는 보안 원격 셸 및 대화형 네트워크 세션을 제공합니다. 자세한 내용은 을 "SSH를 사용하여 클러스터에 액세스합니다 "참조하십시오.

이 작업에 대해

- ONTAP는 노드당 최대 50개의 동시 텔넷 또는 RSH 세션을 지원합니다.

  클러스터 관리 LIF가 노드에 상주하는 경우 이 제한을 노드 관리 LIF와 공유합니다.

  들어오는 연결의 비율이 초당 10보다 높을 경우 서비스가 60초 동안 일시적으로 비활성화됩니다.

- RSH 명령에는 고급 권한이 필요합니다.

ONTAP 9.10.1 이상

단계

1. RSH 또는 텔넷 보안 프로토콜이 활성화되어 있는지 확인합니다.

   ```
   security protocol show
   ```

   a. RSH 또는 텔넷 보안 프로토콜이 활성화된 경우 다음 단계를 계속 진행하십시오.

   b. RSH 또는 텔넷 보안 프로토콜이 활성화되지 않은 경우 다음 명령을 사용하여 활성화하십시오.

      ```
      security protocol modify -application <rsh/telnet> -enabled true
      ```

   및 `security protocol modify` 에 대한 자세한 `security protocol show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

2. 관리 LIF에 또는 서비스가 있는지 확인 `management-rsh-server` `management-telnet-server` :

   ```
   network interface show -services management-rsh-server
   ```

   또는

   ```
   network interface show -services management-telnet-server
   ```

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

   a. 또는 서비스가 있는 경우 `management-rsh-server` `management-telnet-server` 다음 단계를 계속합니다.

   b. 또는 서비스가 없는 경우 `management-rsh-server` `management-telnet-server` 다음 명령을 사용하여 서비스를 추가합니다.

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server

      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

   에 대한 자세한 내용은 `network interface service-policy add-service` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 9.9 이하

이 작업에 대해

ONTAP를 사용하면 미리 정의된 방화벽 정책을 변경할 수 없지만 미리 정의된 `mgmt` 관리 방화벽 정책을 복제하고 새 정책에 따라 텔넷 또는 RSH를 활성화하여 새 정책을 만들 수 있습니다.

단계

1. 고급 권한 모드로 들어갑니다.

   진일진일보한 것

2. 보안 프로토콜 활성화(RSH 또는 Telnet):

   ```
   security protocol modify -application security_protocol -enabled true
   ```

3. `mgmt`관리 방화벽 정책을 기반으로 새 관리 방화벽 정책을 생성합니다.

   ```
   system services firewall policy clone -policy mgmt -destination-policy
   policy-name
   ```

4. 새 관리 방화벽 정책에서 텔넷 또는 RSH를 활성화합니다.

   ```
   system services firewall policy create -policy policy-name -service
   security_protocol -action allow -ip-list ip_address/netmask
   ```

   모든 IP 주소를 허용하려면 을 지정해야 합니다 `-ip-list 0.0.0.0/0`

5. 새 정책을 클러스터 관리 LIF와 연결합니다.

   ```
   network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
   -firewall-policy policy-name
   ```

   에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

텔넷 요청을 사용하여 **ONTAP** 클러스터에 액세스합니다

클러스터에 텔넷 요청을 실행하여 관리 작업을 수행할 수 있습니다. 텔넷은 기본적으로 비활성화되어 있습니다.

Telnet과 RSH는 보안 프로토콜이 아니므로 SSH를 사용하여 클러스터에 액세스하는 것을 고려해야 합니다. SSH는 보안 원격 셸 및 대화형 네트워크 세션을 제공합니다. 자세한 내용은 을 "SSH를 사용하여 클러스터에 액세스합니다 "참조하십시오.

시작하기 전에

텔넷을 사용하여 클러스터에 액세스하려면 다음 조건이 충족되어야 합니다.

- 텔넷을 액세스 방법으로 사용하도록 구성된 클러스터 로컬 사용자 계정이 있어야 합니다.

  `-application`명령의 매개 변수는 `security login` 사용자 계정에 대한 액세스 방법을 지정합니다. 에 대한 자세한 내용은 `security login` link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+login["ONTAP 명령 참조입니다"^]을 참조하십시오.

이 작업에 대해

- ONTAP는 노드당 최대 50개의 동시 텔넷 세션을 지원합니다.

  클러스터 관리 LIF가 노드에 상주하는 경우 이 제한을 노드 관리 LIF와 공유합니다.

들어오는 연결의 비율이 초당 10보다 높을 경우 서비스가 60초 동안 일시적으로 비활성화됩니다.

- Windows 호스트에서 ONTAP CLI에 액세스하려는 경우 PuTTY와 같은 타사 유틸리티를 사용할 수 있습니다.
- RSH 명령에는 고급 권한이 필요합니다.

ONTAP 9.10.1 이상

단계

1. 텔넷 보안 프로토콜이 활성화되어 있는지 확인합니다.

   ```
   security protocol show
   ```

   a. 텔넷 보안 프로토콜이 활성화된 경우 다음 단계를 계속합니다.

   b. 텔넷 보안 프로토콜이 활성화되지 않은 경우 다음 명령을 사용하여 활성화하십시오.

      ```
      security protocol modify -application telnet -enabled true
      ```

   및 `security protocol modify` 에 대한 자세한 `security protocol show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

2. 관리 LIF에 서비스가 있는지 `management-telnet-server` 확인합니다.

   ```
   network interface show -services management-telnet-server
   ```

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

   a. 서비스가 있는 경우 `management-telnet-server` 다음 단계를 계속 진행하십시오.

   b. 서비스가 없는 경우 `management-telnet-server` 다음 명령을 사용하여 서비스를 추가합니다.

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

   에 대한 자세한 내용은 `network interface service-policy add-service` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 9.9 이하

시작하기 전에

텔넷을 사용하여 클러스터에 액세스하려면 다음 조건이 충족되어야 합니다.

- Telnet 요청이 방화벽을 통과할 수 있도록 클러스터나 노드 관리 LIF에서 사용하는 관리 방화벽 정책에서 텔넷이 이미 활성화되어 있어야 합니다.

  기본적으로 텔넷은 비활성화되어 있습니다. `system services firewall policy show -service telnet`매개 변수가 있는 명령은 텔넷이 방화벽 정책에서 활성화되었는지 여부를 표시합니다. 에 대한 자세한 내용은 `system services firewall policy` "ONTAP 명령 참조입니다"을 참조하십시오.

- IPv6 연결을 사용하는 경우 IPv6가 이미 클러스터에서 구성 및 활성화되어 있어야 하며, 방화벽 정책이 이미 IPv6 주소로 구성되어 있어야 합니다.

  이 `network options ipv6 show` 명령을 실행하면 IPv6 사용 여부가 표시됩니다. 에 대한 자세한 내용은 `network options ipv6 show` "ONTAP 명령 참조입니다"을 참조하십시오. `system services firewall policy show`명령은 방화벽 정책을 표시합니다.

단계

1. 관리 호스트에서 다음 명령을 입력합니다.

   ```
   telnet hostname_or_IP
   ```

   `hostname_or_IP` 클러스터 관리 LIF 또는 노드 관리 LIF의 호스트 이름 또는 IP 주소입니다. 클러스터 관리 LIF를 사용하는 것이 좋습니다. IPv4 또는 IPv6 주소를 사용할 수 있습니다.

텔넷 요청의 예

다음 예에서는 Telnet 액세스 권한이 설정된 "joe"라는 사용자가 클러스터 관리 LIF가 10.72.137.28인 클러스터에 액세스하기 위해 Telnet 요청을 발행하는 방법을 보여줍니다.

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

RSH 요청을 사용하여 **ONTAP** 클러스터에 액세스합니다

RSH 요청을 클러스터에 발행하여 관리 작업을 수행할 수 있습니다. RSH는 보안 프로토콜이 아니며 기본적으로 비활성화되어 있습니다.

Telnet과 RSH는 보안 프로토콜이 아니므로 SSH를 사용하여 클러스터에 액세스하는 것을 고려해야 합니다. SSH는 보안 원격 셸 및 대화형 네트워크 세션을 제공합니다. 자세한 내용은 을 "SSH를 사용하여 클러스터에 액세스합니다 "참조하십시오.

시작하기 전에

RSH를 사용하여 클러스터에 액세스하려면 다음 조건을 충족해야 합니다.

- RSH를 액세스 방법으로 사용하도록 구성된 클러스터 로컬 사용자 계정이 있어야 합니다.

  `-application`명령의 매개 변수는 `security login` 사용자 계정에 대한 액세스 방법을 지정합니다. 에 대한 자세한 내용은 `security login` link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+login["ONTAP 명령 참조입니다"^]을 참조하십시오.

이 작업에 대해

- ONTAP는 노드당 최대 50개의 동시 RSH 세션을 지원한다.

  클러스터 관리 LIF가 노드에 상주하는 경우 이 제한을 노드 관리 LIF와 공유합니다.

  들어오는 연결의 비율이 초당 10보다 높을 경우 서비스가 60초 동안 일시적으로 비활성화됩니다.

- RSH 명령에는 고급 권한이 필요합니다.

ONTAP 9.10.1 이상

단계

1. RSH 보안 프로토콜이 활성화되어 있는지 확인합니다.

   ```
   security protocol show
   ```

   a. RSH 보안 프로토콜이 활성화된 경우 다음 단계를 계속합니다.

   b. RSH 보안 프로토콜이 활성화되지 않은 경우 다음 명령을 사용하여 활성화합니다.

      ```
      security protocol modify -application rsh -enabled true
      ```

   및 `security protocol modify` 에 대한 자세한 `security protocol show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

2. 관리 LIF에 서비스가 있는지 `management-rsh-server` 확인합니다.

   ```
   network interface show -services management-rsh-server
   ```

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

   a. 서비스가 있는 경우 `management-rsh-server` 다음 단계를 계속 진행하십시오.

   b. 서비스가 없는 경우 `management-rsh-server` 다음 명령을 사용하여 서비스를 추가합니다.

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server
      ```

   에 대한 자세한 내용은 `network interface service-policy add-service` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 9.9 이하

시작하기 전에

RSH를 사용하여 클러스터에 액세스하려면 다음 조건을 충족해야 합니다.

- RSH 요청이 방화벽을 통과할 수 있도록 클러스터 또는 노드 관리 LIF에서 사용하는 관리 방화벽 정책에서 RSH가 이미 활성화되어 있어야 합니다.

  기본적으로 RSH는 비활성화되어 있습니다. `-service rsh`매개 변수가 있는 `system services firewall policy show` 명령은 방화벽 정책에서 `RSH`가 활성화되었는지 여부를 표시합니다. 에 대한 자세한 내용은 `system services firewall policy` "ONTAP 명령 참조입니다"을 참조하십시오.

- IPv6 연결을 사용하는 경우 IPv6가 이미 클러스터에서 구성 및 활성화되어 있어야 하며, 방화벽 정책이 이미 IPv6 주소로 구성되어 있어야 합니다.

  이 `network options ipv6 show` 명령을 실행하면 IPv6 사용 여부가 표시됩니다. 에 대한 자세한 내용은 `network options ipv6 show` "ONTAP 명령 참조입니다"을 참조하십시오. `system services firewall policy show`명령은 방화벽 정책을 표시합니다.

단계

1. 관리 호스트에서 다음 명령을 입력합니다.

   ```
   rsh hostname_or_IP -l username:passwordcommand
   ```

   `hostname_or_IP` 클러스터 관리 LIF 또는 노드 관리 LIF의 호스트 이름 또는 IP 주소입니다. 클러스터 관리 LIF를 사용하는 것이 좋습니다. IPv4 또는 IPv6 주소를 사용할 수 있습니다.

   `command` RSH를 통해 실행할 명령입니다.

RSH 요청의 예

다음 예에서는 RSH 액세스를 사용하여 설정된 ""Joe""라는 사용자가 "cluster show" 명령을 실행하도록 RSH 요청을 실행하는 방법을 보여줍니다.

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

에 대한 자세한 내용은 `cluster show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 명령줄 인터페이스를 사용합니다

ONTAP 명령줄 인터페이스에 대해 알아봅니다

ONTAP CLI(Command-Line Interface)는 관리 인터페이스의 명령 기반 뷰를 제공합니다. 스토리지 시스템 프롬프트에서 명령을 입력하면 명령 결과가 텍스트로 표시됩니다.

CLI 명령 프롬프트는 cluster_name:::>'로 표시됩니다.

권한 수준(즉, 'set' 명령의 '-Privilege' 매개 변수)을 'advanced'로 설정하면 다음과 같은 별표(*)가 표시됩니다.

'cluster_name
*>'

에 대한 자세한 내용은 `set` "ONTAP 명령 참조입니다"을 참조하십시오.

CLI 명령의 다른 ONTAP 셸에 대해 알아봅니다

클러스터에는 CLI 명령을 위한 *clustershell*, *nodeshell* 및 _systemshell_의 세 가지 셸이 있습니다. 쉘은 서로 다른 용도로 사용되며 각각 다른 명령 집합을 가집니다.

- 클러스터 쉘은 클러스터에 로그인할 때 자동으로 시작되는 네이티브 셸입니다.

  클러스터 구성 및 관리에 필요한 모든 명령을 제공합니다. clustershell CLI 도움말(clustershell 프롬프트에서 트리거됨)에는 ? 사용 가능한 clustershell 명령이 표시됩니다. `man clustershell`의 명령은 지정된 `clustershell` 명령에 대한 `man` 페이지를 (`man <command_name>`표시합니다.) 에 대한 자세한 내용은 `man "ONTAP 명령 참조입니다"`을 참조하십시오.

- 노드 수준에서만 적용되는 명령을 위한 특수 셸입니다.

  노드 쉘은 명령을 통해 액세스할 수 `system node run` 있습니다. 에 대한 자세한 내용은 `system node run` "ONTAP 명령 참조입니다"을 참조하십시오.

  노드 쉘 CLI 도움말(또는 `help` 노드 쉘 프롬프트에서 트리거됨 ?)에는 사용 가능한 노드 쉘 명령이 표시됩니다. `man`노드 쉘의 명령은 지정된 노드 쉘 명령에 대한 man 페이지를 표시합니다.

  일반적으로 사용되는 노드 쉘의 명령 및 옵션은 클러스터 쉘에 터널링되거나 별칭되어 클러스터 쉘에서도 실행될 수 있습니다.

- 시스템 셸은 진단 및 문제 해결용으로만 사용되는 하위 셸입니다.

  시스템 셸 및 관련 `diag` 계정은 저수준 진단 목적으로 사용됩니다. 이러한 액세스를 위해서는 진단 권한 수준이 필요하며, 문제 해결 작업을 수행하기 위한 기술 지원용으로만 예약되어 있습니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

클러스터 쉘에서 노드 명령 및 옵션 액세스

노드 쉘을 통해 명령 및 옵션을 액세스할 수 있습니다.

'system node run – node_nodename_'

일반적으로 사용되는 노드 쉘의 명령 및 옵션은 클러스터 쉘에 터널링되거나 별칭되어 클러스터 쉘에서도 실행될 수 있습니다.

클러스터 셸에서 지원되는 Nodeshell 옵션은 다음을 사용하여 액세스할 수 있습니다. `vserver options clustershell` 명령. 이러한 옵션을 보려면 다음을 사용하여 클러스터셸 CLI를 쿼리할 수 있습니다. `vserver options -vserver` *`nodename_or_clustername`* `-option-name ?`

클러스터 쉘에 노드 쉘이나 레거시 명령 또는 옵션을 입력하고 명령 또는 옵션에 동일한 클러스터 셸 명령이 있으면 ONTAP에서 사용할 클러스터 셸 명령을 알려줍니다.

클러스터 쉘에서 지원되지 않는 노드 쉘이나 레거시 명령 또는 옵션을 입력하면 ONTAP에서 명령이나 옵션에 대한 ""지원되지 않음" 상태를 알려줍니다.

사용 가능한 노드 대체 명령을 표시합니다

CLI 도움말을 사용하여 노드 쉘에서 사용 가능한 노드 쉘의 명령 목록을 얻을 수 있습니다.

단계

1. 노드 쉘에 액세스하려면 클러스터 쉘의 시스템 프롬프트에 다음 명령을 입력합니다.

   '* 시스템 노드 run-node {*nodename*|local} *'

로컬 은 클러스터에 액세스하는 데 사용한 노드입니다.

'system node run' 명령에는 'run'이라는 별칭 명령이 있습니다.

2. 노드 쉘에 다음 명령을 입력하여 사용 가능한 노드 쉘 명령 목록을 표시합니다.

   "*[*CommandName*] 도움말 * "

   '*CommandName*'은 표시할 수 있는 명령의 이름입니다. '*CommandName*'을 포함하지 않으면 CLI는 사용 가능한 모든 notes지옥명령을 표시합니다.

   'exit'를 입력하거나 Ctrl-d를 입력하여 클러스터 쉘 CLI로 돌아갑니다.

   에 대한 자세한 내용은 `exit` "ONTAP 명령 참조입니다"을 참조하십시오.

사용 가능한 노드 쉘의 명령 표시 예

다음 예에서는 node2라는 노드의 노드 중 노드 쉘에 액세스하여 노드 쉘의 명령 "환경"에 대한 정보를 표시합니다.

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
     [status] [shelf [<adapter>[.<shelf-number>]]] |
     [status] [shelf_log] |
     [status] [shelf_stats] |
     [status] [shelf_power_status] |
     [status] [chassis [all | list-sensors | Temperature | PSU 1 |
     PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

ONTAP CLI 명령 디렉토리를 탐색하는 방법

CLI의 명령은 명령 디렉토리별로 계층 구조로 구성됩니다. 전체 명령 경로를 입력하거나 디렉토리 구조를 탐색하여 계층에서 명령을 실행할 수 있습니다.

CLI를 사용하는 경우 프롬프트에 디렉토리 이름을 입력하고 Enter 키를 눌러 명령 디렉토리에 액세스할 수 있습니다. 그러면 디렉토리 이름이 프롬프트 텍스트에 포함되어 해당 명령 디렉터리와 상호 작용하고 있음을 나타냅니다. 명령 계층 구조로 더 자세히 이동하려면 명령 하위 디렉터리의 이름을 입력한 다음 Enter 키를 누릅니다. 그러면 하위 디렉터리 이름이 프롬프트 텍스트에 포함되고 컨텍스트는 해당 하위 디렉터리로 이동합니다.

전체 명령을 입력하여 여러 명령 디렉토리를 탐색할 수 있습니다. 예를 들어, 프롬프트에 'storage disk show' 명령을 입력하여 디스크 드라이브에 대한 정보를 표시할 수 있습니다. 다음 예제와 같이 한 번에 하나의 명령 디렉토리를 탐색하여 명령을 실행할 수도 있습니다.

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

에 대한 자세한 내용은 `storage disk show` "ONTAP 명령 참조입니다"을 참조하십시오.

현재 디렉터리에 고유한 명령을 만드는 명령의 최소 문자 수만 입력하여 명령을 축약할 수 있습니다. 예를 들어, 이전 예제의 명령을 축약하려면 'st d sh'를 입력할 수 있습니다. Tab 키를 사용하여 약식 명령을 확장하고 기본 매개 변수 값을 비롯한 명령의 매개 변수를 표시할 수도 있습니다.

'top' 명령을 사용하여 명령어 계층구조의 최상위 수준으로 이동하고 'up' 명령이나…' 명령을 사용하여 명령어 계층구조에서 한 단계 위로 이동할 수 있습니다.

CLI에서 별표(*)가 앞에 오는 명령 및 명령 옵션은 고급 권한 수준 이상에서만 실행할 수 있습니다.

관련 정보

- "위쪽"
- "위로"

ONTAP CLI에서 값을 지정하는 규칙을 이해합니다

대부분의 명령에는 하나 이상의 필수 매개 변수 또는 선택적 매개 변수가 포함됩니다. 많은 매개 변수는 값을 지정해야 합니다. CLI에서 값을 지정할 때 적용되는 몇 가지 규칙이 있습니다.

- 값은 숫자, 부울 지정자 또는 텍스트 문자열이거나 사전 정의된 값의 열거 목록 중 한 값을 선택하여 사용할 수 있습니다.

  일부 매개 변수에는 둘 이상의 값을 쉼표로 구분하여 지정할 수 있습니다. 쉼표로 구분된 값 목록은 따옴표(" ")에 있을 필요가 없습니다. 텍스트, 공백 또는 쿼리 문자(보다 작음 또는 보다 큰 기호로 시작하는 텍스트나 쿼리가 아닌 경우)를 지정할 때는 항상 엔티티를 따옴표로 묶어야 합니다.

- CLI에서 물음표(?)는 특정 명령의 도움말 정보를 표시하는 명령으로 해석됩니다.
- 명령 이름, 매개 변수 및 특정 값과 같이 CLI에서 입력하는 일부 텍스트는 대/소문자를 구분하지 않습니다.

  예를 들어, 'vserver cifs' 명령에 대한 매개 변수 값을 입력하면 대문자 표시가 무시됩니다. 하지만 노드 이름, SVM(스토리지 가상 머신), 애그리게이트, 볼륨, 논리 인터페이스 등과 같은 대부분의 매개 변수 값은 대/소문자를 구분합니다.

- 문자열이나 목록을 사용하는 매개 변수 값을 지우려면 빈 따옴표("") 또는 대시("-")를 지정합니다.
- (`#`파운드 기호라고도 하는 해시 기호는 명령줄 입력에 대한 주석을 나타냅니다. 사용할 경우 명령줄에서 마지막 매개 변수 뒤에 표시되어야 합니다.

  CLI에서는 과 줄 사이의 텍스트를 # 무시합니다.

다음 예에서는 텍스트 코멘트로 SVM을 작성합니다. 그런 다음 SVM이 수정되어 설명을 삭제합니다.

```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspace ipspaceA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

다음 예제에서 부호를 사용하는 명령줄 주석은 # 명령이 수행하는 작업을 나타냅니다.

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 명령 기록을 보고 기록에서 명령을 다시 실행합니다

각 CLI 세션은 해당 세션에서 실행된 모든 명령의 기록을 유지합니다. 현재 사용 중인 세션의 명령 기록을 볼 수 있습니다. 명령을 다시 실행할 수도 있습니다.

명령어 이력을 보기 위해 'history' 명령어를 사용할 수 있다.

명령을 재발급하려면 다음 인수 중 하나와 함께 "redo" 명령을 사용할 수 있습니다.

- 이전 명령의 일부와 일치하는 문자열입니다

  예를 들어, 실행한 유일한 'volume' 명령이 'volume show'인 경우 'redo volume' 명령을 사용하여 명령을 다시 실행할 수 있습니다.

- history 명령으로 나열한 이전 명령의 숫자 ID

  예를 들어, 'redo 4' 명령을 사용하여 기록 목록에서 네 번째 명령을 다시 실행할 수 있습니다.

- 기록 목록의 끝에서 음수 오프셋

  예를 들어, redo-2 명령을 사용하여 이전에 두 명령을 실행한 명령을 다시 실행할 수 있습니다.

예를 들어, 명령 기록 끝에서 세 번째 명령을 다시 실행하려면 다음 명령을 입력합니다.

```
cluster1::> redo -3
```

관련 정보

- "기록"
- "다시 실행"

- "볼륨"

CLI 명령 편집을 위한 **ONTAP** 바로 가기 키

현재 명령 프롬프트에 있는 명령은 활성 명령입니다. 바로 가기 키를 사용하면 활성 명령을 빠르게 편집할 수 있습니다. 이러한 바로 가기 키는 UNIX tcsh 셸 및 Emacs 편집기의 바로 가기와 유사합니다.

다음 표에는 CLI 명령을 편집하기 위한 바로 가기 키가 나와 있습니다. `Ctrl`- Ctrl 키를 누른 상태에서 뒤에 지정된 문자를 입력함을 나타냅니다. `Esc`- Esc 키를 눌렀다가 놓은 다음 그 뒤에 지정된 문자를 입력함을 나타냅니다.

원하는 작업	다음 바로 가기 키 중 하나를 사용합니다.
커서를 한 문자씩 뒤로 이동합니다	• Ctrl+B를 누릅니다 • 뒤로 화살표
커서를 한 문자씩 앞으로 이동합니다	• Ctrl + F • 앞으로 화살표
커서를 한 단어씩 뒤로 이동합니다	Esc-B를 누릅니다
커서를 한 단어씩 앞으로 이동합니다	Esc - F
커서를 줄의 시작 부분으로 이동합니다	Ctrl-A를 누릅니다
커서를 줄의 끝으로 이동합니다	Ctrl-E
줄의 시작 부분에서 커서까지의 명령줄 내용을 제거하고 잘라낸 버퍼에 저장합니다. 잘라내기 버퍼는 일부 프로그램에서 _clipboard_라고 하는 것과 유사한 임시 메모리처럼 작동합니다.	Ctrl+U
커서에서 줄의 끝까지 명령줄의 내용을 제거하고 절단 버퍼에 저장합니다	Ctrl+K를 누릅니다
커서에서 다음 단어의 끝까지 명령줄 내용을 제거하고 절단 버퍼에 저장합니다	Esc-D 를 누릅니다
커서 앞에 있는 단어를 제거하고 잘라낸 버퍼에 저장합니다	Ctrl+W
절단 버퍼의 내용을 뱅킹하고 커서의 명령줄에 밀어 넣습니다	Ctrl+Y

원하는 작업	다음 바로 가기 키 중 하나를 사용합니다.
커서 앞의 문자를 삭제합니다	• Ctrl + H • 백스페이스
커서가 있는 문자를 삭제합니다	Ctrl+D를 누릅니다
선을 지웁니다	Ctrl+C
화면을 지웁니다	Ctrl+L
명령줄의 현재 내용을 기록 목록의 이전 항목으로 바꿉니다. 키보드 단축키를 반복할 때마다 기록 커서가 이전 항목으로 이동합니다.	• Ctrl+P • Esc-P • 위쪽 화살표
명령줄의 현재 내용을 기록 목록의 다음 항목으로 바꿉니다. 키보드 단축키를 반복할 때마다 기록 커서가 다음 항목으로 이동합니다.	• Ctrl+N • Esc-N • 아래쪽 화살표
부분적으로 입력한 명령을 확장하거나 현재 편집 위치에서 유효한 입력을 나열합니다	• 탭을 클릭합니다 • Ctrl+I
상황에 맞는 도움말을 표시합니다	?
물음표 ?) 문자에 대한 특수 매핑을 해제합니다. 예를 들어 명령 인수에 물음표를 입력하려면 Esc 키를 누른 다음 ? 문자를 누릅니다.	Esc-?
TTY 출력을 시작합니다	Ctrl-Q를 누릅니다
TTY 출력을 중지합니다	Ctrl+S

ONTAP CLI 명령에 대한 권한 수준을 이해합니다

ONTAP 명령 및 매개 변수는 *admin*,*advanced* 및 _diagnostic_의 세 가지 권한 레벨로 정의됩니다. 권한 수준은 작업을 수행하는 데 필요한 기술 수준을 반영합니다.

- * 관리자 *

  대부분의 명령과 매개변수는 이 레벨에서 사용할 수 있습니다. 일반 또는 일상적인 작업에 사용됩니다.

- 고급 *

이 레벨의 명령 및 매개 변수는 자주 사용되지 않으며, 고급 지식이 필요하며 부적절하게 사용될 경우 문제를 일으킬 수 있습니다.

고급 명령 또는 매개변수는 지원 담당자의 조언과 함께 사용해야 합니다.

- * 진단 *

  진단 명령 및 매개 변수가 잠재적으로 중단될 수 있습니다. 문제 진단 및 해결을 위해 지원 담당자만이 사용합니다.

ONTAP CLI에서 권한 수준을 설정한다

CLI에서 '설정' 명령어를 이용하여 권한 수준을 설정할 수 있다. 권한 수준 설정 변경 사항은 현재 진행 중인 세션에만 적용됩니다. 세션 간에 지속적이지 않습니다.

단계

1. CLI에서 권한 수준을 설정하려면 '-Privilege' 파라미터와 함께 '설정' 명령어를 사용한다.

권한 수준 설정의 예

다음 예제에서는 권한 수준을 Advanced 로 설정한 다음 admin 으로 설정합니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

에 대한 자세한 내용은 `set` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP CLI에 대한 디스플레이 기본 설정을 지정합니다

'설정' 명령과 '행' 명령을 사용하여 CLI 세션에 대한 디스플레이 기본 설정을 설정할 수 있습니다. 설정한 기본 설정은 현재 진행 중인 세션에만 적용됩니다. 세션 간에 지속적이지 않습니다.

이 작업에 대해

다음과 같은 CLI 디스플레이 기본 설정을 설정할 수 있습니다.

- 명령 세션의 권한 수준입니다
- 잠재적으로 운영 중단 명령에 대해 확인을 수행할지 여부를 나타냅니다
- '표시' 명령이 모든 필드를 표시하는지 여부
- 필드 구분 기호로 사용할 문자 또는 문자입니다
- 데이터 크기를 보고할 때의 기본 단위입니다
- 인터페이스가 출력을 일시 중지하기 전에 화면이 현재 CLI 세션에 표시되는 행의 수입니다

  원하는 행 수를 지정하지 않으면 터미널의 실제 높이에 따라 자동으로 조정됩니다. 실제 높이가 정의되지 않은 경우 기본 행 수는 24입니다.

- 기본 스토리지 가상 시스템(SVM) 또는 노드
- 오류가 발생할 경우 계속 명령을 중지할지 여부를 나타냅니다

단계

1. CLI display preference를 설정하려면 '설정' 명령어를 사용한다.

   현재 CLI 세션에서 화면에 표시되는 행의 수를 설정하려면 "rows" 명령을 사용할 수도 있습니다.

   및 `rows` 에 대한 자세한 `set` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

CLI에서 디스플레이 기본 설정을 설정하는 예

다음 예제에서는 쉼표를 필드 구분 기호로 설정하고 기본 데이터 크기 단위로 GB를 설정하고 행 수를 50으로 설정합니다.

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

관련 정보

- "표시"
- "설정"
- "행"

ONTAP CLI에서 쿼리 연산자를 사용합니다

관리 인터페이스는 쿼리 및 UNIX 스타일 패턴과 와일드카드를 지원하여 명령 매개 변수 인수의 여러 값을 일치시킬 수 있습니다.

다음 표에서는 지원되는 쿼리 연산자를 설명합니다.

운영자	설명
*	모든 항목과 일치하는 와일드카드입니다. 예를 들어, 'volume show-volume\ * tmp *' 명령은 이름에 'tmp' 문자열이 포함된 모든 볼륨의 목록을 표시합니다.
!	연산자가 아닙니다. 일치하지 않는 값을 나타냅니다. 예를 들어, '**!vs0**'은 값 "vs0"과 일치하지 않음을 나타냅니다.

운영자	설명
있습니다. 비교할 두 개의 값을 구분합니다. 예를 들어, '* vs0	vs2*'는 vs0 또는 vs2와 일치합니다.
b *	\ * c * 와 같이 여러 개 또는 구문을 지정할 수 있습니다. 이 항목은 a 항목, b로 시작하는 모든 항목, c를 포함하는 모든 항목과 일치합니다.
…	범위 연산자. 예를 들어, ' * 5..10 *'은 '5'에서 '10'까지의 모든 값을 포함합니다.
를 누릅니다	보다 작음 연산자입니다. 예를 들어, "*<20 *"은 "20"보다 작은 모든 값과 일치합니다.
를 누릅니다	보다 큰 연산자. 예를 들어, ' * > 5 * '는 '5'보다 큰 값을 찾습니다.
=	보다 작거나 같음 연산자. 예를 들어, "* ⇐5*"는 "5"보다 작거나 같은 값을 찾습니다.
>=	보다 크거나 같음 연산자입니다. 예를 들어, '**>=5**'는 '5'보다 크거나 같은 값을 찾습니다.
{'query'}	확장된 쿼리. 확장 쿼리는 다른 매개 변수 앞에 명령 이름 뒤의 첫 번째 인수로 지정해야 합니다. 예를 들어, 'volume modify{-volume\ * tmp *} -state offline' 명령은 이름에 'tmp' 문자열이 포함된 모든 볼륨을 오프라인으로 설정합니다.

쿼리 문자를 리터럴로 구문 분석하려면 문자를 큰따옴표로 묶어야 합니다(예: `"<10"`, `"0..100"`, `"*abc*"`, 또는 `"a|b"`)를 참조하십시오.

특수 문자가 해석되지 않도록 원시 파일 이름을 큰따옴표로 묶어야 합니다. 이는 클러스터 쉘에서 사용하는 특수 문자에도 적용됩니다.

한 명령줄에 여러 쿼리 연산자를 사용할 수 있습니다. 예를 들어 명령은 `volume show -size >1GB -percent -used <50 -vserver !vs1` 크기가 1GB보다 크고, 50% 미만이고, 이름이 ""VS1""인 SVM(스토리지 가상 머신)에 없는 모든 볼륨을 표시합니다.

관련 정보

"CLI 명령 편집을 위한 바로 가기 키"

ONTAP CLI에서 **modify** 및 **delete** 명령에 확장 쿼리를 사용합니다

확장 쿼리를 사용하여 지정된 값이 있는 개체를 일치시키고 작업을 수행할 수 있습니다.

확장 쿼리는 중괄호({})로 둘러싸서 지정합니다. 확장 쿼리는 다른 매개 변수 앞에 명령 이름 뒤의 첫 번째 인수로 지정해야 합니다. 예를 들어 이름이 "tmp"인 모든 볼륨을 오프라인으로 설정하려면 다음 예제에서 명령을 실행합니다.

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

확장 쿼리는 일반적으로 수정 및 삭제 명령에만 유용합니다. 이들은 창조나 표현에 아무런 의미가 없습니다.

쿼리와 수정 작업의 조합은 유용한 도구입니다. 그러나 잘못 구현하면 혼동과 오류가 발생할 수 있습니다. 예를 들어, (advanced 권한) 'system node image modify' 명령을 사용하여 노드의 기본 소프트웨어 이미지를 설정하면 다른 소프트웨어 이미지가 자동으로 기본값이 아닌 기본값으로 설정됩니다. 다음 예제의 명령은 null 작업입니다.

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

이 명령은 현재 기본 이미지를 기본 이미지가 아닌 이미지로 설정한 다음 새 기본 이미지(이전의 기본 이미지가 아닌 이미지)를 기본 이미지가 아닌 이미지로 설정하여 원래 기본 설정을 유지합니다. 다음 예제와 같이 명령을 사용하여 작업을 올바르게 수행할 수 있습니다.

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

fields 매개 변수를 사용하여 **ONTAP show** 명령의 출력을 제한합니다

매개 변수를 명령과 함께 `show` 사용하여 세부 정보를 표시하면 `-instance` 출력이 오래 걸리고 필요한 것보다 더 많은 정보가 포함될 수 있습니다. `-fields`명령의 매개 변수를 `show` 사용하면 지정한 정보만 표시할 수 있습니다.

예를 들어 를 실행하면 `volume show -instance` 여러 개의 정보 화면이 표시될 수 있습니다. 을 사용하여 항상 표시되는 기본 필드 외에 지정된 필드만 포함하도록 출력을 사용자 지정할 수 있습니다 `volume show -fields` *`fieldname[,fieldname…]`*. 를 사용하면 명령에 대한 유효한 필드를 표시할 `show` 수 `-fields ?` 있습니다.

다음 예제는 매개 변수와 `-fields` 매개 변수 간의 출력 차이를 보여줍니다 `-instance`.

```
cluster1::> volume show -instance

                                    Vserver Name: cluster1-1
                                     Volume Name: vol0
                                  Aggregate Name: aggr0
                                     Volume Size: 348.3GB
                              Volume Data Set ID: -
                       Volume Master Data Set ID: -
                                    Volume State: online
                                     Volume Type: RW
                                    Volume Style: flex
                                             ...
                           Space Guarantee Style: volume
                        Space Guarantee in Effect: true
                                             ...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume space-guarantee space-guarantee-enabled
-------- ------ --------------- ----------------------
cluster1-1 vol0   volume          true
cluster1-2 vol0   volume          true
vs1      root_vol
                  volume          true
vs2      new_vol
                  volume          true
vs2      root_vol
                  volume          true
...
cluster1::>
```

명령 입력에서 **ONTAP CLI** 위치 매개 변수를 사용합니다

ONTAP CLI의 위치 매개 변수 기능을 활용하여 명령 입력의 효율성을 높일 수 있습니다. 명령을 쿼리하여 명령의 위치 매개 변수를 식별할 수 있습니다.

위치 매개 변수란 무엇입니까

- 위치 매개 변수는 매개 변수 값을 지정하기 전에 매개 변수 이름을 지정할 필요가 없는 매개 변수입니다.
- "***command_name?***" 출력에 표시된 것과 같이 명령 입력에서 상대 시퀀스를 동일한 명령에서 다른 위치 매개변수와 관찰하는 한 위치 매개 변수를 위치 매개 변수와 함께 사용할 수 있습니다.
- 위치 매개 변수는 명령에 대한 필수 매개 변수이거나 선택적 매개 변수일 수 있습니다.

- 매개 변수는 한 명령에 대한 위치일 수 있지만 다른 명령에는 위치 지정되지 않을 수 있습니다.

> 특히 위치 매개 변수가 명령에서 선택 항목이거나 선택 매개 변수가 앞에 나열되는 경우에는 스크립트의 위치 매개 변수 기능을 사용하지 않는 것이 좋습니다.

위치 매개 변수를 식별합니다

'***command_name?***' 명령 출력에서 위치 매개변수를 식별할 수 있습니다. 위치 매개 변수에는 다음 형식 중 하나로 매개 변수 이름을 둘러싸는 대괄호가 있습니다.

- ['*-parameter_name*']'*parameter_value*'는 위치 매개 변수를 나타냅니다.
- [['*-parameter_name*']'*parameter_value*']는 위치 매개 변수를 선택적으로 표시합니다.

예를 들어, '***command_name?***' 출력에 다음과 같이 표시될 경우 매개 변수는 표시되는 명령의 위치 입니다.

- '[-lif]<lif-name>'
- '[[-lif]<lif-name>]'

그러나 다음과 같이 표시될 경우 매개 변수는 표시되는 명령의 위치 이외의 매개 변수입니다.

- '-lif<lif-name>'
- '[-lif<lif-name>]'

위치 매개 변수 사용 예

다음 예제에서 ' **volume create?* * ' 출력에서는 '-volume', '-aggregate', '-size' 명령의 위치를 나타내는 세 개의 매개 변수가 표시됩니다.

```
cluster1::> volume create ?
   -vserver <vserver name>                Vserver Name
   [-volume] <volume name>                Volume Name
   [-aggregate] <aggregate name>          Aggregate Name
  [[-size] {<integer>[KB|MB|GB|TB|PB]}]   Volume Size
  [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                          Volume State (default: online)
  [ -type {RW|DP|DC} ]                    Volume Type (default: RW)
  [ -policy <text> ]                      Export Policy
  [ -user <user name> ]                   User ID
  ...
  [ -space-guarantee|-s {none|volume} ]   Space Guarantee Style (default:
volume)
  [ -percent-snapshot-space <percent> ]   Space Reserved for Snapshot
Copies
  ...
```

다음 예에서는 positional parameter 기능을 이용하지 않고 'volume create' 명령을 지정합니다.

'cluster1::> volume create-vserver svm1-volume vol1-aggregate * aggr1-size 1g * - percent-snapshot-space 0'

다음 예제에서는 위치 매개 변수 기능을 사용하여 명령 입력의 효율성을 높입니다. 'volume create' 명령에서 위치 매개 변수가 위치 매개 변수와 비위치 매개 변수가 서로 연결되어 있으며 위치 매개 변수 값은 매개 변수 이름 없이 지정됩니다. 위치 매개변수는 '* volume create?*' 출력에 표시된 것과 동일한 순서로 지정됩니다. 즉, -volume의 값은 -size의 앞에 차례로 지정된 -aggregate의 값 앞에 지정됩니다.

'cluster1::> 볼륨 create * vol2 * aggr1 * * 1g * -vserver svm1-percent-snapshot-space 0'

'cluster1::> volume create -vserver svm1 * vol3 * -snapshot-policy default * aggr1 * -nvfail off * 1g * -space-보증 없음'

ONTAP CLI man 페이지에 액세스하는 방법

ONTAP 수동(man) 페이지에서는 ONTAP CLI 명령을 사용하는 방법을 설명합니다. 이러한 페이지는 명령줄에서 사용할 수 있으며 release-specific_command references_에도 게시됩니다.

ONTAP 명령줄에서 명령을 사용하여 `man <command_name>` 지정된 명령의 수동 페이지를 표시합니다. 명령 이름을 지정하지 않으면 수동 페이지 인덱스가 표시됩니다. 명령을 사용하여 명령 자체에 대한 정보를 볼 `man` 수 `man man` 있습니다. 를 입력하여 man 페이지를 종료할 수 **`q`** 있습니다.

해당 릴리즈에서 사용할 수 있는 관리자 레벨 및 고급 레벨 ONTAP 명령에 대해 자세히 "ONTAP 명령 참조입니다 "알아보십시오.

ONTAP CLI 세션을 기록하고 녹화된 세션을 관리합니다

CLI 세션을 지정된 이름 및 크기 제한이 있는 파일에 기록한 다음 파일을 FTP 또는 HTTP 대상으로 업로드할 수 있습니다. 이전에 CLI 세션을 기록한 파일을 표시하거나 삭제할 수도 있습니다.

CLI 세션을 기록합니다

CLI 세션의 레코드는 녹화를 중지하거나 CLI 세션을 종료할 때 또는 파일이 지정된 크기 제한에 도달할 때 끝납니다. 기본 파일 크기 제한은 1MB입니다. 최대 파일 크기 제한은 2GB입니다.

예를 들어, 문제를 해결하고 상세 정보를 저장하려는 경우 또는 특정 시점에 공간 사용에 대한 영구 기록을 작성하려는 경우 CLI 세션을 기록하는 것이 유용합니다.

단계

1. 파일에 현재 CLI 세션 녹화를 시작합니다.

   ```
   system script start
   ```

   에 대한 자세한 내용은 `system script start` "ONTAP 명령 참조입니다"을 참조하십시오.

   ONTAP가 CLI 세션을 지정된 파일에 기록하기 시작합니다.

2. CLI 세션을 진행합니다.

3. 완료되면 세션 녹화를 중지합니다.

```
system script stop
```

에 대한 자세한 내용은 `system script stop` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP는 CLI 세션 녹화를 중지합니다.

CLI 세션의 레코드를 관리하는 명령입니다

'system script' 명령어를 이용하여 CLI 세션 기록을 관리한다.

원하는 작업	이 명령 사용...
지정된 파일에 현재 CLI 세션 녹화를 시작합니다	'시스템 스크립트 시작
현재 CLI 세션 녹화를 중지합니다	'시스템 스크립트 중지'
CLI 세션 레코드에 대한 정보를 표시합니다	'시스템 스크립트 쇼'
CLI 세션의 레코드를 FTP 또는 HTTP 대상으로 업로드합니다	'시스템 스크립트 업로드'
CLI 세션의 레코드를 삭제합니다	'시스템 스크립트 삭제

관련 정보

"ONTAP 명령 참조입니다"

CLI session의 자동 **timeout** 기간을 관리하는 명령어

timeout 값은 CLI 세션이 자동으로 종료되기 전까지 유휴 상태로 유지되는 시간을 지정합니다. CLI 시간 초과 값은 클러스터 전체에 적용됩니다. 즉, 클러스터의 모든 노드에서 동일한 CLI 시간 초과 값을 사용합니다.

기본적으로 CLI 세션의 자동 제한 시간은 30분입니다.

'system timeout' 명령어를 이용하여 CLI session의 자동 timeout 기간을 관리한다.

원하는 작업	이 명령 사용...
CLI 세션의 자동 제한 시간을 표시합니다	'시스템 시간 초과 표시'
CLI 세션의 자동 시간 제한 기간을 수정합니다	'시스템 시간 제한 수정'

관련 정보

"ONTAP 명령 참조입니다"

ONTAP 클러스터에서 노드 레벨의 세부 정보를 봅니다

노드 이름, 노드 상태 및 해당 노드가 클러스터에 참여할 수 있는지 여부를 확인할 수 있습니다. 고급 권한 수준에서는 노드에 epsilon이 있는지 여부도 표시할 수 있습니다.

단계

1. 클러스터의 노드에 대한 정보를 보려면 `cluster show` 명령을 사용하십시오.

   출력에 노드가 epsilon을 보유하고 있는지 여부를 표시하려면 고급 권한 수준에서 명령을 실행합니다.

   에 대한 자세한 내용은 `cluster show` "ONTAP 명령 참조입니다"을 참조하십시오.

클러스터의 노드 표시 예

다음 예는 4노드 클러스터의 모든 노드에 대한 정보를 표시합니다.

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
node3                 true    true
node4                 true    true
```

다음 예제에서는 고급 권한 수준의 ""node1"" 노드에 대한 자세한 정보를 표시합니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

       Node: node1
  Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
    Epsilon: false
Eligibility: true
     Health: true
```

ONTAP 클러스터 레벨의 세부 정보를 봅니다

클러스터의 UUID(고유 식별자), 이름, 일련 번호, 위치 및 연락처 정보를 표시할 수 있습니다.

단계

1. 클러스터의 속성을 표시하려면 'cluster identity show' 명령을 사용합니다.

클러스터 속성을 표시하는 예

다음 예제에는 클러스터의 이름, 일련 번호, 위치 및 연락처 정보가 표시됩니다.

```
cluster1::> cluster identity show

          Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
          Cluster Name: cluster1
 Cluster Serial Number: 1-80-123456
      Cluster Location: Sunnyvale
       Cluster Contact: jsmith@example.com
```

에 대한 자세한 내용은 `cluster identity show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 클러스터 특성을 수정합니다

필요에 따라 클러스터 이름, 위치, 연락처 정보 등과 같은 클러스터의 속성을 수정할 수 있습니다.

이 작업에 대해

클러스터 생성 시 설정되는 클러스터의 UUID는 변경할 수 없습니다.

단계

1. 클러스터 속성을 수정하려면 'cluster identity modify' 명령을 사용합니다.

   `-name`매개 변수는 클러스터의 이름을 지정합니다. 및 에서 클러스터 이름을 지정하는 규칙에 대해 자세히 `cluster identity modify`link:https://docs.netapp.com/us-en/ontap-cli/cluster-identity-modify.html["ONTAP 명령 참조입니다"^] 알아보십시오.

   '-location' 매개 변수는 클러스터의 위치를 지정합니다.

   '-contact' 파라미터는 이름, 이메일 주소 등의 연락처 정보를 지정한다.

클러스터 이름을 바꾸는 예

다음 명령을 실행하면 현재 클러스터(""cluster1")의 이름이 ""cluster2""로 변경됩니다.

```
cluster1::> cluster identity modify -name cluster2
```

ONTAP 클러스터 링의 복제 상태를 봅니다

클러스터 복제 링의 상태를 확인하여 클러스터 전체의 문제를 진단하는 데 도움이 될 수 있습니다. 클러스터에 문제가 있는 경우 지원 담당자가 문제 해결을 위해 이 작업을 수행하도록

요청할 수 있습니다.

단계

1. 클러스터 복제 링의 상태를 표시하려면 고급 권한 수준에서 'cluster ring show' 명령을 사용합니다.

클러스터 링 복제 상태 표시 예

다음 예에서는 Node0이라는 노드의 VLDB 복제 링 상태를 표시합니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
          Node: node0
     Unit Name: vldb
        Status: master
         Epoch: 5
   Master Node: node0
    Local Node: node0
      DB Epoch: 5
DB Transaction: 56
 Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

에 대한 자세한 내용은 `cluster ring show` "ONTAP 명령 참조입니다"을 참조하십시오.

quorum 및 **epsilon**을 사용한 **ONTAP** 클러스터 상태 평가

쿼럼 및 epsilon은 클러스터 상태 및 기능의 중요한 측정치로서, 클러스터를 통해 잠재적인 통신 및 연결 문제를 해결하는 방법을 함께 나타냅니다.

_Quorum_은 완전히 작동하는 클러스터를 위한 전제 조건입니다. 클러스터가 쿼럼에 있으면 대부분의 노드가 정상 상태이며 서로 통신할 수 있습니다. 쿼럼이 손실되면 클러스터는 정상적인 클러스터 작업을 수행할 수 없게 됩니다. 모든 노드가 데이터의 단일 뷰를 공유하므로 한 번에 하나의 노드 집합만 쿼럼을 가질 수 있습니다. 따라서 서로 통신하지 않는 두 개의 노드가 서로 다른 방식으로 데이터를 수정할 수 있는 경우 더 이상 데이터를 단일 데이터 뷰로 조정할 수 없습니다.

클러스터의 각 노드는 하나의 node_master_를 선택하는 voting 프로토콜에 참여하며 나머지 각 노드는 _secondary_입니다. 마스터 노드는 클러스터 전체에서 정보를 동기화하는 역할을 합니다. 쿼럼이 형성되면 투표가 계속된다. 마스터 노드가 오프라인이 되고 클러스터가 여전히 쿼럼에 있으면 새 마스터는 온라인 상태로 유지되는 노드에 의해 선택됩니다.

노드의 수가 짝수인 클러스터에서 타이 가능성이 있기 때문에 노드 하나에 _epsilon_라는 추가 분수 투표 가중치가 있습니다. 대규모 클러스터의 동일한 두 부분 간의 연결이 실패할 경우 epsilon이 포함된 노드 그룹은 모든 노드가 정상 상태라고 가정하고 quorum을 유지합니다. 예를 들어, 다음 그림에서는 노드 2개에 장애가 발생한 4노드 클러스터를 보여 줍니다. 그러나 남아 있는 노드 중 하나가 epsilon을 보유하기 때문에 양호한 노드의 대부분이 단순하지 않더라도 클러스터가 쿼럼에 남아 있습니다.

Epsilon은 클러스터를 생성할 때 첫 번째 노드에 자동으로 할당됩니다. epsilon이 있는 노드가 정상 상태가 아니거나 고가용성 파트너를 인수하거나 고가용성 파트너가 인수하는 경우 epsilon은 다른 HA 쌍의 정상 노드에 자동으로 재할당됩니다.

노드를 오프라인 상태로 전환하면 클러스터의 쿼럼 유지 기능에 영향을 줄 수 있습니다. 따라서 클러스터를 쿼럼에서 제외시키거나 quorum이 손실된 상태에서 한 번의 작동 중지가 발생하지 않는 작업을 시도할 경우 ONTAP에서 경고 메시지를 표시합니다. advanced 권한 수준에서 명령을 사용하여 쿼럼 경고 메시지를 사용하지 않도록 설정할 수 `cluster quorum-service options modify` 있습니다. 에 대한 자세한 내용은 `cluster quorum-service options modify` "ONTAP 명령 참조입니다"을 참조하십시오.

일반적으로, 클러스터의 노드 간에 안정적인 연결을 가정하면 더 큰 클러스터는 더 작은 클러스터보다 더 안정적입니다. 노드 과반수의 단순한 정수에 epsilon을 더한 quorum 요구 사항은 노드 2개로 구성된 클러스터보다 노드 24개로 구성된 클러스터에서 유지하기가 더 쉽습니다.

2노드 클러스터는 쿼럼을 유지 관리하는 데 몇 가지 고유한 문제를 제시합니다. 2노드 클러스터는 epsilon을 보유하지 않는 _cluster HA_를 사용합니다. 대신 두 노드는 모두 지속적으로 폴링되므로 한 노드에 장애가 발생할 경우 다른 노드가 데이터에 대한 읽기/쓰기 액세스 권한을 완벽하게 갖추고 논리 인터페이스 및 관리 기능에 액세스할 수 있습니다.

ONTAP 클러스터에 있는 시스템 볼륨의 스토리지 용량 활용률을 확인합니다

시스템 볼륨은 파일 서비스 감사 로그의 메타데이터와 같은 특수 메타데이터가 포함된 FlexVol 볼륨입니다. 이러한 볼륨은 클러스터에서 볼 수 있으므로 클러스터에서 스토리지 사용을 완전히 고려할 수 있습니다.

시스템 볼륨은 클러스터 관리 서버(관리 SVM라고도 함)에서 소유하며 파일 서비스 감사가 활성화되어 있을 때 자동으로 생성됩니다.

'volume show' 명령을 사용하여 시스템 볼륨을 볼 수 있지만 다른 대부분의 볼륨 작업은 허용되지 않습니다. 예를 들어, 'volume modify' 명령을 사용하여 시스템 볼륨을 수정할 수 없습니다.

이 예에서는 클러스터 내의 데이터 SVM에 대해 파일 서비스 감사를 활성화할 때 자동으로 생성된 admin SVM의 시스템 볼륨 4개를 보여 줍니다.

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          2GB     1.90GB
5%
4 entries were displayed.
```

노드 관리

ONTAP 클러스터에 노드를 추가합니다

클러스터가 생성된 후 노드를 추가하여 클러스터를 확장할 수 있습니다. 노드를 한 번에 하나만 추가할 수 있습니다.

시작하기 전에

- 다중 노드 클러스터에 노드를 추가하는 경우 클러스터의 모든 기존 노드가 정상 상태(로 표시됨)여야 합니다 `cluster show`. 에 대한 자세한 내용은 `cluster show` "ONTAP 명령 참조입니다"을 참조하십시오.
- 스위치가 없는 2노드 클러스터에 노드를 추가하려면 NetApp 지원 클러스터 스위치를 사용하여 스위치가 없는 2노드 클러스터를 스위치 연결 클러스터로 변환해야 합니다.

  스위치가 없는 클러스터 기능은 2노드 클러스터에서만 지원됩니다.

- 단일 노드 클러스터에 두 번째 노드를 추가하는 경우 두 번째 노드가 설치되었고 클러스터 네트워크를 구성해야 합니다.
- 클러스터에 SP 자동 구성이 설정되어 있는 경우 SP에 대해 지정된 서브넷에 사용 가능한 리소스가 있어야 연결 노드에서 지정된 서브넷을 사용하여 SP를 자동으로 구성할 수 있습니다.
- 새 노드의 노드 관리 LIF에 대해 다음 정보를 수집해야 합니다.
  - 포트
  - IP 주소입니다
  - 넷마스크
  - 기본 게이트웨이

이 작업에 대해

노드는 HA Pair를 구성할 수 있도록 짝수여야 합니다. 클러스터에 노드를 추가하기 시작한 후 프로세스를 완료해야 합니다. 다른 노드를 추가하기 전에 노드가 클러스터의 일부여야 합니다.

단계

1. 클러스터에 추가할 노드의 전원을 켭니다.

   노드가 부팅되고 노드 설정 마법사가 콘솔에서 시작됩니다.

   ```
   Welcome to node setup.

   You can enter the following commands at any time:
     "help" or "?" - if you want to have a question clarified,
     "back" - if you want to change previously answered questions, and
     "exit" or "quit" - if you want to quit the setup wizard.
        Any changes you made before quitting will be saved.

   To accept a default or omit a question, do not enter a value.

   Enter the node management interface port [e0M]:
   ```

2. 노드 설정 마법사를 종료합니다

   노드 설정 마법사가 종료되고 설치 작업을 완료하지 않았다는 로그인 프롬프트가 나타납니다.

   에 대한 자세한 내용은 `exit` "ONTAP 명령 참조입니다"을 참조하십시오.

3. admin 사용자 이름을 사용하여 admin 계정에 로그인합니다.
4. 클러스터 설정 마법사를 시작합니다.

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
 "help" or "?" - if you want to have a question clarified,
 "back" - if you want to change previously answered questions, and
 "exit" or "quit" - if you want to quit the cluster setup wizard.
 Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing
https://<node_mgmt_or_e0M_IP_address>

Otherwise, press Enter to complete cluster setup using the
command line interface:
```

설정 GUI를 사용하여 클러스터를 설정하는 방법에 대한 자세한 내용은 다음을 참조하세요. "노드 관리 문서" . 에 대한 자세한 내용은 `cluster setup` "ONTAP 명령 참조입니다"을 참조하십시오.

5. Enter 키를 눌러 CLI를 사용하여 이 작업을 완료합니다. 새 클러스터를 생성하거나 기존 클러스터에 가입하라는 메시지가 표시되면 ' * join * '을 입력합니다.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

새 노드에서 실행 중인 ONTAP 버전이 기존 클러스터에서 실행 중인 버전과 다르면 시스템이 오류를 보고합니다 `System checks Error: Cluster join operation cannot be performed at this time.` 이는 정상적인 동작입니다. 계속하려면 `cluster add-node -allow-mixed-version-join true -cluster-ips <IP address> -node-names <new_node_name>` 클러스터의 기존 노드에서 advanced 권한 수준에서 명령을 실행하십시오.

6. 프롬프트에 따라 노드를 설정하고 클러스터에 연결합니다.
   - 프롬프트의 기본값을 그대로 사용하려면 Enter 키를 누릅니다.
   - 프롬프트에 대한 값을 직접 입력하려면 값을 입력한 다음 Enter 키를 누릅니다.
7. 추가할 각 추가 노드에 대해 위의 단계를 반복합니다.

작업을 마친 후

클러스터에 노드를 추가한 후에는 각 HA 쌍에 대해 스토리지 페일오버를 설정해야 합니다.

관련 정보

- "ONTAP 소프트웨어 업그레이드에 지원되는 혼합 버전 클러스터"
- "클러스터 추가 노드"

ONTAP 클러스터에서 노드를 제거합니다

클러스터에서 필요 없는 노드를 한 번에 하나씩 제거할 수 있습니다. 노드를 제거한 후에는 해당 페일오버 파트너도 제거해야 합니다. 노드를 제거하면 해당 데이터에 액세스할 수 없거나 데이터가 지워집니다.

시작하기 전에

클러스터에서 노드를 제거하기 전에 다음 조건을 충족해야 합니다.

- 클러스터 내 노드의 절반 이상이 정상 상태여야 합니다.
- 모든 데이터, 볼륨 및 루트가 아닌 집계는 노드에서 다시 배치하거나 제거해야 합니다.
  - 제거하려는 노드의 모든 데이터가 비워져야 합니다. 여기에는 다음이 "암호화된 볼륨에서 데이터를 제거하는 중입니다"포함될 수 있습니다.
  - 루트가 아닌 모든 볼륨은 입니다 "이동됨" 노드에서 소유하는 Aggregate에서.
  - 루트가 아닌 모든 애그리게이트는 입니다 "삭제됨" 노드에서.
- 모든 LIF 및 VLAN이 노드에서 재배치되거나 제거되었습니다.
  - 데이터 LIF는 이미 존재했습니다 "삭제됨" 또는 "위치가 재조정되었습니다" 노드에서.
  - 클러스터 관리 LIF는 입니다 "위치가 재조정되었습니다" 노드 및 홈 포트가 변경되었습니다.
  - 모든 인터클러스터 LIF가 "제거되었습니다"적용되었습니다. 인터클러스터 LIF를 제거하면 무시할 수 있는 경고가 표시됩니다.
  - 노드의 모든 VLAN은 입니다 "삭제됨".
- 노드가 페일오버 관계에 관여하지 않습니다.
  - 스토리지 페일오버가 수행되었습니다 "사용 안 함" 를 선택합니다.
  - 모든 LIF 페일오버 규칙은 입니다 "수정됨" 노드에서 포트를 제거합니다.
- 노드가 FIPS(Federal Information Processing Standards) 디스크 또는 SED(자체 암호화 디스크)를 소유한 경우 "디스크 암호화가 제거되었습니다" 디스크를 보호되지 않는 모드로 되돌리는 것입니다.
  - 원하는 경우도 있을 것입니다 "FIPS 드라이브 또는 SED를 살균합니다".
- 제거할 노드에 LUN이 있는 경우 노드를 제거하기 전에 을 수행해야 "SLM(Selective LUN Map) 보고 노드 목록을 수정합니다"합니다.

  SLM 보고 노드 목록에서 노드 및 해당 HA 파트너를 제거하지 않을 경우 LUN이 포함된 볼륨이 다른 노드로 이동되었더라도 노드에서 이전에 LUN에 액세스하지 못할 수 있습니다.

AutoSupport 메시지를 발행하여 노드 제거가 진행 중임을 NetApp 기술 지원에 알리는 것이 좋습니다.

> 자동화된 ONTAP 업그레이드가 진행 중인 경우에는, `cluster unjoin` 및 `node rename` 같은 작업을 수행하지 마십시오 `cluster remove-node`.

이 작업에 대해

- 혼합 버전 클러스터를 실행 중인 경우 ONTAP 9.3으로 시작하는 고급 권한 명령 중 하나를 사용하여 마지막 하위 버전 노드를 제거할 수 있습니다.
  - ONTAP 9.3: 클러스터 unjoin-skip-last-low-version-node-check
  - ONTAP 9.4 이상: cluster remove-node-skip-last-low-version-node-check
- 4노드 클러스터에서 2개의 노드를 제거하면 나머지 2개의 노드에서 클러스터 HA가 자동으로 설정됩니다.

> ⓘ 클러스터에서 노드를 제거하기 전에 해당 노드에 연결된 모든 디스크의 모든 시스템 및 사용자 데이터에 대한 접근을 차단해야 합니다.
>
> 클러스터에서 노드가 잘못 제거된 경우 복구 옵션에 대한 지원을 받으려면 NetApp 지원 팀에 문의하십시오.

단계

1. 권한 수준을 고급으로 변경합니다.

```
set -privilege advanced
```

2. 클러스터에서 epsilon을 가진 노드를 식별하십시오.

```
cluster show
```

다음 예에서 "node0"은 현재 epsilon을 보유하고 있습니다.

```
cluster::*>
Node                  Health  Eligibility  Epsilon
--------------------- ------- ------------ ------------
node0                 true    true         true
node1                 true    true         false
node2                 true    true         false
node3                 true    true         false
```

3. 제거하려는 노드가 epsilon을 보유하고 있는 경우:
   a. 제거하려는 노드에서 epsilon을 이동합니다.

```
cluster modify -node <name_of_node_to_be_removed> -epsilon false
```

   b. 제거하지 않을 노드로 epsilon을 이동합니다.

```
cluster modify -node <node_name> -epsilon true
```

4. 현재 마스터 노드를 식별합니다.

```
cluster ring show
```

마스터 노드는 `vldb` , , `vifmgr`, `bcomd` 및 `crs` 같은 프로세스를 포함하는 노드입니다. `mgmt`

5. 제거하려는 노드가 현재 master 노드인 경우, 클러스터의 다른 노드가 master 노드로 선출될 수 있도록 설정하십시오.

a. 현재 마스터 노드가 클러스터에 참여할 수 없는 상태가 되도록 합니다.

```
cluster modify -node <node_name> -eligibility false
```

해당 노드는 자격이 복원될 때까지 비정상 상태로 표시됩니다. 마스터 노드가 자격을 상실하면 클러스터 쿼럼에 의해 나머지 노드 중 하나가 새로운 마스터로 선출됩니다.

HA 쌍에서 첫 번째 노드에 대해 이 단계를 수행하는 경우 해당 노드만 부적격으로 표시해야 합니다. HA 파트너의 상태는 수정하지 마십시오.

파트너 노드를 새로운 마스터로 선택한 경우, 해당 노드가 epsilon을 보유하고 있는지 확인한 후 마스터 자격 박탈을 진행해야 합니다. 파트너 노드가 epsilon을 보유하고 있다면, 해당 노드를 마스터 자격 박탈하기 전에 클러스터에 남아 있는 다른 노드로 epsilon을 이동해야 합니다. 이 작업은 파트너 노드를 제거하기 위해 위의 단계를 반복할 때 수행합니다.

a. 이전 마스터 노드가 클러스터에 다시 참여할 수 있도록 합니다.

```
cluster modify -node <node_name> -eligibility true
```

6. 클러스터에서 제거하지 않을 노드의 원격 노드 관리 LIF 또는 클러스터 관리 LIF에 로그인하십시오.
7. 클러스터에서 노드를 제거합니다.

이 **ONTAP** 버전의 경우…	이 명령 사용…
ONTAP 9.3	`cluster unjoin`

이 **ONTAP** 버전의 경우…	이 명령 사용…

ONTAP 9.4 이상	노드 이름:
	`cluster remove-node -node <node_name>`
	노드 IP 사용:
	`cluster remove-node -cluster_ip <node_ip>`

혼합 버전 클러스터가 있고 마지막 하위 버전 노드를 제거하는 경우 이 명령과 함께 '-skip-last-low-version-node-check' 매개 변수를 사용합니다.

시스템에서 다음 정보를 알려줍니다.

- 또한 클러스터의 페일오버 파트너도 제거해야 합니다.
- 노드가 제거된 후 클러스터에 다시 참여하기 전에 부팅 메뉴 옵션 **(4) Clean configuration and initialize all disks** 또는 옵션 *(9) Configure Advanced Drive Partitioning*을 사용하여 노드의 구성을 지우고 모든 디스크를 초기화해야 합니다.

  노드를 제거하기 전에 해결해야 하는 조건이 있는 경우 실패 메시지가 생성됩니다. 예를 들어, 메시지에서 제거해야 하는 공유 리소스가 노드에 포함되어 있거나 해당 노드가 반드시 해제해야 하는 클러스터 HA 구성 또는 스토리지 페일오버 구성에 포함되어 있음을 나타낼 수 있습니다.

노드가 쿼럼 마스터인 경우 클러스터가 잠시 손실되었다가 쿼럼으로 돌아갑니다. 이 쿼럼 손실은 일시적이며 데이터 작업에 영향을 주지 않습니다.

8. 오류 메시지에 오류 상태가 표시되면 해당 조건을 해결하고 클러스터 remove-node 또는 cluster unjoin 명령을 다시 실행합니다.

   노드는 클러스터에서 성공적으로 제거된 후 자동으로 재부팅됩니다.

9. 노드를 용도 변경할 경우 노드 구성을 지우고 모든 디스크를 초기화합니다.
   a. 부팅 프로세스 중에 부팅 메뉴가 표시되면 Ctrl-C를 눌러 부팅 메뉴를 표시합니다.
   b. 부팅 메뉴 옵션 *(4) Clean configuration and initialize all disks*를 선택합니다.
10. admin 권한 수준으로 돌아갑니다:

```
set -privilege admin
```

11. 1에서 9까지의 단계를 반복하여 클러스터에서 페일오버 파트너를 제거합니다.

관련 정보

- "클러스터 제거 노드"

웹 브라우저를 사용하여 ONTAP 노드 로그, 코어 덤프 및 MIB 파일에 액세스합니다

Service Processor Infrastructure(S pi) 웹 서비스는 기본적으로 활성화되어 웹 브라우저가 클러스터에 있는 노드의 로그, 코어 덤프 및 MIB 파일에 액세스할 수 있도록 합니다. 노드가 다운된 경우에도 파일이 액세스 가능 상태로 유지됩니다. 단, 해당 노드가 파트너에 의해 인계됩니다.

시작하기 전에

- 클러스터 관리 LIF가 가동되어야 합니다.

  클러스터의 관리 LIF나 노드를 사용하여 'pi' 웹 서비스에 액세스할 수 있습니다. 그러나 클러스터 관리 LIF를 사용하는 것이 좋습니다.

  network interface show 명령은 클러스터에 있는 모든 LIF의 상태를 표시합니다.

  에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

- 에 액세스하려면 로컬 사용자 계정을 사용해야 합니다 `spi` 웹 서비스, 도메인 사용자 계정은 지원되지 않습니다.
- 사용자 계정에 다음이 없는 경우 `admin` 역할(액세스 권한이 있음) `spi` 기본적으로 웹 서비스)의 경우 액세스 제어 역할에 액세스 권한이 부여되어야 합니다. `spi` 웹 서비스.

  'vserver services web access show' 명령은 어떤 역할이 어떤 웹 서비스에 대한 액세스 권한이 부여되어 있는지 보여줍니다.

- 사용하지 않는 경우 `admin` 사용자 계정(다음을 포함함) `http` 기본적으로 액세스 방법)을 사용하려면 사용자 계정을 다음과 같이 설정해야 합니다. `http` 접근 방법.

  '보안 로그인 표시' 명령은 사용자 계정의 액세스 및 로그인 방법과 액세스 제어 역할을 표시합니다.

  에 대한 자세한 내용은 `security login show` "ONTAP 명령 참조입니다"을 참조하십시오.

- 보안 웹 액세스를 위해 HTTPS를 사용하려면 SSL을 활성화하고 디지털 인증서를 설치해야 합니다.

  'system services web show' 명령은 클러스터 수준에서 웹 프로토콜 엔진의 구성을 표시합니다.

이 작업에 대해

기본적으로 'spi' 웹 서비스가 활성화되어 있으며 서비스를 수동으로 비활성화할 수 있습니다('vserver services web modify -vserver * -name spi -enabled false').

그만큼 `admin` 역할에 대한 액세스 권한이 부여됩니다. `spi` 기본적으로 웹 서비스이며 액세스를 수동으로 비활성화할 수 있습니다. (`services web access delete -vserver` *`cluster_name`* `-name spi -role admin`).

단계

1. 다음 형식 중 하나로 웹 브라우저를 'pi' 웹 서비스 URL로 지정합니다.
   - "http://*cluster-mgmt-LIF*/spi/`
   - "https://*cluster-mgmt-LIF*/spi/`

클러스터 관리 LIF의 IP 주소는 클러스터 관리 LIF의 IP 주소입니다.

2. 브라우저에서 메시지가 표시되면 사용자 계정 및 암호를 입력합니다.

   계정이 인증되면 브라우저는 클러스터에 있는 각 노드의 '/mroot/etc/log/', '/mroot/etc/crash/' 및 '/mroot/etc/mib/' 디렉토리에 대한 링크를 표시합니다.

ONTAP 노드의 시스템 콘솔에 액세스합니다

부팅 메뉴 또는 부팅 환경 프롬프트에 노드가 있는 경우 시스템 콘솔(_serial console_이라고도 함)을 통해서만 액세스할 수 있습니다. 노드의 SP 또는 클러스터에 대한 SSH 연결로부터 노드의 시스템 콘솔에 액세스할 수 있습니다.

이 작업에 대해

SP와 ONTAP는 모두 시스템 콘솔에 액세스할 수 있는 명령을 제공합니다. 그러나 SP에서는 자체 노드의 시스템 콘솔에만 액세스할 수 있습니다. 클러스터에서 클러스터의 다른 노드(로컬 노드 제외)의 시스템 콘솔에 액세스할 수 있습니다.

단계

1. 노드의 시스템 콘솔에 액세스합니다.

에 있는 경우...	이 명령을 입력하십시오...
노드의 SP CLI입니다	시스템 콘솔
ONTAP CLI를 참조하십시오	'시스템 노드 실행 콘솔

2. 시스템 콘솔에 로그인하라는 메시지가 표시되면 로그인합니다.
3. 시스템 콘솔을 종료하려면 Ctrl-D를 누릅니다

시스템 콘솔에 액세스하는 예

다음 예제는 'S node2' 프롬프트에서 'system console' 명령어를 입력한 결과를 보여준다. 시스템 콘솔에 부팅 환경 프롬프트에서 node2가 멈추는 것으로 표시됩니다. 노드를 ONTAP로 부팅하려면 콘솔에서 boot_ontap 명령을 입력합니다. 그런 다음 Ctrl+D를 눌러 콘솔을 종료하고 SP로 돌아갑니다.

```
SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
...
```

(시스템 콘솔을 종료하려면 Ctrl+D를 누릅니다.)

```
Connection to 123.12.123.12 closed.
SP node2>
```

다음 예제는 ONTAP에서 System node run-console 명령을 입력하여 부팅 환경 프롬프트에 있는 node2의 시스템 콘솔에 액세스하는 결과를 보여 줍니다. 콘솔에서 boot_ontap 명령을 입력하여 node2를 ONTAP로 부팅합니다. 그런 다음 Ctrl-D를 눌러 콘솔을 종료하고 ONTAP로 돌아갑니다.

```
cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you might
open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
...
```

(시스템 콘솔을 종료하려면 Ctrl+D를 누릅니다.)

```
Connection to 123.12.123.12 closed.
cluster1::>
```

ONTAP 노드 루트 볼륨 및 루트 애그리게이트를 관리합니다

노드의 루트 볼륨은 공장 출하 시 또는 설치 소프트웨어에 의해 설치되는 FlexVol 볼륨입니다. 시스템 파일, 로그 파일 및 코어 파일용으로 예약되어 있습니다. 디렉토리 이름은 '/mroot'로, 시스템 셸을 통해서만 기술 지원 부서에서 액세스할 수 있습니다. 노드 루트 볼륨의 최소 크기는 플랫폼 모델에 따라 다릅니다.

노드 루트 볼륨 및 루트 애그리게이트 개요를 제어하는 규칙

노드의 루트 볼륨에는 해당 노드에 대한 특수 디렉토리와 파일이 포함되어 있습니다. 루트 Aggregate는 루트 볼륨을 포함합니다. 노드의 루트 볼륨 및 루트 애그리게이트에 대한 몇 가지 규칙이 적용됩니다.

- 다음 규칙은 노드의 루트 볼륨에 적용됩니다.
  - 기술 지원 부서에서 지시하지 않는 한 루트 볼륨의 구성 또는 콘텐츠를 수정하지 마십시오.
  - 루트 볼륨에 사용자 데이터를 저장하지 마십시오.

    사용자 데이터를 루트 볼륨에 저장하면 HA 쌍의 노드 간 스토리지 반환 시간이 늘어납니다.

  - 루트 볼륨을 다른 애그리게이트로 이동할 수 있습니다. 을 참조하십시오 [relocate-root].
- 루트 애그리게이트는 노드의 루트 볼륨에만 사용됩니다.

  ONTAP을 사용하면 루트 애그리게이트에 다른 볼륨을 생성할 수 없습니다.

"NetApp Hardware Universe를 참조하십시오"

노드의 루트 볼륨에서 공간을 확보합니다

노드의 루트 볼륨이 꽉 찼거나 거의 꽉 찼을 때 경고 메시지가 나타납니다. 루트 볼륨이 꽉 찼을 때 노드가 제대로 작동하지 않습니다. 코어 덤프 파일, 패킷 추적 파일 및 루트 볼륨 스냅샷을 삭제하여 노드의 루트 볼륨에서 공간을 확보할 수 있습니다.

단계

1. 노드의 코어 덤프 파일과 해당 이름을 표시합니다.

   '시스템 노드 코어 덤프 표시'

2. 노드에서 필요 없는 코어 덤프 파일을 삭제합니다.

   시스템 노드 코어 덤프 삭제

3. 노데스 액세스:

   '* 시스템 노드 run-node_nodename_*'

   '*nodename*'은 루트 볼륨 공간을 확보하려는 노드의 이름입니다.

4. 노드 쉘에서 노드 고급 권한 레벨로 전환합니다.

   ``한자 세트 어드밴스드 *''

5. 노드 패킷 추적 파일을 노드 쉘을 통해 표시 및 삭제:
   a. 노드의 루트 볼륨에 있는 모든 파일을 표시합니다.

      ' * ls /etc * '

   b. 노드의 루트 볼륨에 패킷 추적 파일('*.trc')이 있으면 개별적으로 삭제합니다.

      ' * rm/etc/log/packet_trace/*file_name.trc* *'

6. 노드 쉘을 통해 노드의 루트 볼륨 스냅샷을 식별하고 삭제합니다.
   a. 루트 볼륨 이름 확인:

      ' * vol status * '

      루트 볼륨은 "vol status" 명령 출력의 "Options" 열에 "root"라는 단어가 표시됩니다.

      다음 예에서는 루트 볼륨이 "vol0"입니다.

```
node1*> vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

   a. 루트 볼륨 스냅샷 표시:

      `snap list root_vol_name`

   b. 원하지 않는 루트 볼륨 스냅샷 삭제:

      `snap delete root_vol_namesnapshot_name`

7. 노드 쉘을 종료하고 클러스터 쉘로 돌아갑니다.

   ' * exit * '

루트 볼륨을 새 애그리게이트로 재배치

루트 교체 절차는 운영 중단 없이 현재 루트 애그리게이트를 다른 디스크 세트로 마이그레이션합니다.

이 작업에 대해

루트 볼륨을 재배치하려면 스토리지 페일오버가 활성화되어 있어야 합니다. 'storage failover modify -node_nodename_ -enable true' 명령을 사용하여 페일오버를 활성화할 수 있습니다.

다음 시나리오에서 루트 볼륨의 위치를 새 애그리게이트로 변경할 수 있습니다.

- 루트 애그리게이트가 원하는 디스크에 없을 경우
- 노드에 연결된 디스크를 재정렬하려는 경우

- EOS 디스크 쉘프의 쉘프 교체를 수행할 때

단계

1. 권한 수준을 고급으로 설정합니다.

   '* 권한 고급 설정 * '

2. 루트 애그리게이트 재배치:

   '* 시스템 노드 migrate-root-node_nodename_-disklist_disklist_-raid-type_raid-type_*'

   ◦ * -노드 *

     마이그레이션할 루트 애그리게이트를 소유하는 노드를 지정합니다.

   ◦ * -디스크 목록 *

     새 루트 애그리게이트를 생성할 디스크 목록을 지정합니다. 모든 디스크가 동일한 노드에서 소유하고 있어야 합니다. 필요한 최소 디스크 수는 RAID 유형에 따라 다릅니다.

   ◦ * -RAID-유형 *

     루트 애그리게이트의 RAID 유형을 지정합니다. 기본값은 "RAID-DP"입니다.

3. 작업 진행 상황 모니터링:

   '* job show-id_jobid_-instance*'

결과

모든 사전 검사가 성공하면 명령이 루트 볼륨 교체 작업을 시작하고 종료됩니다. 노드가 다시 시작될 것으로 예상합니다.

관련 정보

- "스토리지 장애 조치 수정"

유지보수 또는 문제 해결을 위해 **ONTAP** 노드를 시작하거나 중지합니다

유지보수 또는 문제 해결을 위해 노드를 시작하거나 중지해야 할 수 있습니다. ONTAP CLI, 부팅 환경 프롬프트 또는 SP CLI에서 이 작업을 수행할 수 있습니다.

SP CLI 명령 'system power off' 또는 'system power cycle'을 사용하여 노드를 끄거나 전원을 껐다 켜면 노드(또는 *dirty shutdown*)가 비정상적으로 종료될 수 있으며 ONTAP 'system node halt' 명령을 사용한 정상 종료를 대신할 수 없습니다.

시스템 프롬프트에서 노드를 재부팅합니다

시스템 프롬프트에서 일반 모드로 노드를 재부팅할 수 있습니다. 노드는 PC CompactFlash 카드와 같은 부팅 장치에서 부팅하도록 구성됩니다.

단계

1. 클러스터에 4개 이상의 노드가 포함된 경우 재부팅될 노드에 epsilon이 포함되지 않는지 확인합니다.

a. 권한 수준을 고급으로 설정합니다.

' * set-Privilege advanced * '

b. 어떤 노드에 epsilon가 있는지 확인합니다.

``클러스터 쇼 *'

다음 예에서는 ""node1""에 epsilon 이 있음을 보여 줍니다.

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  ------------
node1                 true    true          true
node2                 true    true          false
node3                 true    true          false
node4                 true    true          false
4 entries were displayed.
```

a. 재부팅될 노드에 epsilon가 있는 경우 노드에서 epsilon을 제거합니다.

' * cluster modify -node_node_name_-epsilon FALSE * '

b. epsilon을 계속 가동되는 다른 노드에 할당합니다.

' * cluster modify -node_node_name_-epsilon TRUE * '

c. 관리자 권한 레벨로 돌아갑니다.

' * set-privilege admin * '

2. 노드를 재부팅하려면 'system node reboot' 명령을 사용합니다.

'-skip-lif-migration' 매개 변수를 지정하지 않으면 재부팅하기 전에 데이터 및 클러스터 관리 LIF를 다른 노드로 동기식으로 마이그레이션합니다. LIF 마이그레이션이 실패하거나 시간이 초과되면 재부팅 프로세스가 중단되고 ONTAP에 LIF 마이그레이션 실패를 나타내는 오류가 표시됩니다.

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

노드가 재부팅 프로세스를 시작합니다. 재부팅 프로세스가 완료되었음을 나타내는 ONTAP 로그인 프롬프트가 나타납니다.

부팅 환경 프롬프트에서 **ONTAP**를 부팅합니다

노드의 부팅 환경 프롬프트에서 현재 릴리즈 또는 ONTAP의 백업 릴리즈를 부팅할 수 있습니다.

단계

1. 'system node halt' 명령을 사용하여 스토리지 시스템 프롬프트에서 부팅 환경 프롬프트에 액세스합니다.

스토리지 시스템 콘솔에 부팅 환경 프롬프트가 표시됩니다.

2. 부팅 환경 프롬프트에서 다음 명령 중 하나를 입력합니다.

부팅하려면...	입력...
ONTAP의 현재 릴리즈입니다	부트 ONTAP
부팅 장치의 ONTAP 기본 이미지	boot_primary를 선택합니다
부팅 장치의 ONTAP 백업 이미지	boot_backup입니다

어떤 이미지를 사용해야 할지 잘 모를 경우 첫 번째 인스턴스에서 boot_ONTAP을 사용해야 합니다.

노드를 종료합니다

노드가 응답하지 않거나 지원 담당자가 문제 해결 작업의 일부로 종료하도록 안내하는 경우 노드를 종료할 수 있습니다.

단계

1. 클러스터에 4개 이상의 노드가 포함된 경우 종료할 노드에 epsilon이 포함되지 않는지 확인합니다.

   a. 권한 수준을 고급으로 설정합니다.

      ' * set-Privilege advanced * '

   b. 어떤 노드에 epsilon가 있는지 확인합니다.

      ``클러스터 쇼 *'

      다음 예에서는 ""node1""에 epsilon 이 있음을 보여 줍니다.

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  ------------
node1                 true    true          true
node2                 true    true          false
node3                 true    true          false
node4                 true    true          false
4 entries were displayed.
```

   a. 종료할 노드에 epsilon가 있으면 노드에서 epsilon을 제거합니다.

      ' * cluster modify -node_node_name_-epsilon FALSE * '

   b. epsilon을 계속 가동되는 다른 노드에 할당합니다.

      ' * cluster modify -node_node_name_-epsilon TRUE * '

c. 관리자 권한 레벨로 돌아갑니다.

' * set-privilege admin * '

2. 'system node halt' 명령어를 사용하여 노드를 종료한다.

'-skip-lif-migration' 매개 변수를 지정하지 않으면 명령이 종료되기 전에 데이터 및 클러스터 관리 LIF를 다른 노드로 동기식으로 마이그레이션합니다. LIF 마이그레이션이 실패하거나 시간이 초과되면 종료 프로세스가 중단되고 ONTAP에 LIF 마이그레이션 실패를 나타내는 오류가 표시됩니다.

'-dump' 매개 변수를 모두 사용하여 종료로 코어 덤프를 수동으로 트리거할 수 있습니다.

다음 예에서는 하드웨어 유지 보수를 위해 ""node1""이라는 노드를 종료합니다.

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

부팅 메뉴를 사용하여 **ONTAP** 노드를 관리합니다

부팅 메뉴를 사용하여 노드의 구성 문제를 해결하고, admin 암호를 재설정하고, 디스크를 초기화하고, 노드 구성을 재설정하고, 노드 구성 정보를 부팅 장치로 복원할 수 있습니다.

HA 쌍이 를 사용 중인 경우 "SAS 또는 NVMe 드라이브(SED, NSE, FIPS) 암호화", 항목의 지침을 따라야 합니다 "FIPS 드라이브 또는 SED를 보호되지 않는 모드로 되돌리는 중입니다" 시스템을 초기화하기 전에 HA 쌍 내의 모든 드라이브(부팅 옵션 4 또는 9) 이렇게 하지 않을 경우 드라이브를 용도 변경할 경우 향후의 데이터 손실이 발생할 수 있습니다.

단계

1. 노드를 재부팅하여 시스템 프롬프트에서 'system node reboot' 명령을 사용하여 부팅 메뉴에 액세스합니다.

노드가 재부팅 프로세스를 시작합니다.

2. 재부팅 프로세스 중에 메시지가 표시되면 Ctrl-C를 눌러 부팅 메뉴를 표시합니다.

부팅 메뉴에 대한 다음 옵션이 노드에 표시됩니다.

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set onboard key management recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

ⓘ 부트 메뉴 옵션(2) /etc/rc 없이 부팅은 사용되지 않으며 시스템에 영향을 주지 않습니다.

3. 해당 번호를 입력하여 다음 옵션 중 하나를 선택합니다.

대상...	선택...
정상 모드에서 노드를 계속 부팅합니다	1) 정상 부팅
"admin" 계정 암호이기도 한 노드의 암호를 변경합니다	3) 암호 변경
노드의 디스크를 초기화하고 노드의 루트 볼륨을 생성합니다	구성을 청소하고 모든 디스크를 초기화합니다 ⓘ 이 메뉴 옵션은 노드 디스크의 모든 데이터를 지우고 노드 구성을 공장 출하시 기본 설정으로 재설정합니다. 노드가 클러스터에서 제거되었고 다른 클러스터에 가입되지 않은 경우에만 이 메뉴 항목을 선택하십시오. 내부 또는 외부 디스크 쉘프가 있는 노드의 경우 내부 디스크의 루트 볼륨이 초기화됩니다. 내부 디스크 쉘프가 없는 경우, 외부 디스크의 루트 볼륨이 초기화됩니다. 초기화하려는 노드에 루트 데이터 파티셔닝을 위한 디스크가 있는 경우, 노드를 초기화하기 전에 디스크를 파티셔닝하지 않아야 합니다. 참조: * 9) 고급 드라이브 파티셔닝 구성 * 및 "디스크 및 애그리게이트 관리".
Aggregate 및 디스크 유지보수 작업을 수행하고 자세한 Aggregate 및 디스크 정보를 얻습니다.	유지 관리 모드 부팅 'halt' 명령어를 이용하여 Maintenance Mode를 종료한다.

대상...	선택...
노드의 루트 볼륨에서 PC CompactFlash 카드와 같은 부팅 장치로 구성 정보를 복원합니다	6) 백업 구성에서 플래시를 업데이트합니다 ONTAP는 일부 노드 구성 정보를 부팅 장치에 저장합니다. 노드가 재부팅되면 부팅 디바이스의 정보가 노드의 루트 볼륨에 자동으로 백업됩니다. 부팅 장치가 손상되거나 교체해야 하는 경우 이 메뉴 옵션을 사용하여 노드의 루트 볼륨에서 부팅 장치로 구성 정보를 복원해야 합니다.
노드에 새 소프트웨어를 설치합니다	새 소프트웨어를 먼저 설치합니다 부팅 장치의 ONTAP 소프트웨어에 루트 볼륨에 사용할 스토리지 배열에 대한 지원이 포함되지 않은 경우, 이 메뉴 옵션을 사용하여 스토리지 배열을 지원하는 소프트웨어 버전을 얻고 노드에 설치할 수 있습니다. 이 메뉴 옵션은 루트 볼륨이 설치되지 않은 노드에 최신 버전의 ONTAP 소프트웨어를 설치하는 경우에만 사용됩니다. ONTAP를 업그레이드하려면 이 메뉴 옵션을 사용합니다.
노드를 재부팅합니다	8) 노드를 재부팅합니다

모든 디스크의 파티션을 해제하고 해당 소유권 정보를 제거하거나 구성을 청소하고 전체 또는 분할된 디스크로 시스템을 초기화합니다	9) 고급 드라이브 파티셔닝을 구성합니다
	
	고급 드라이브 분할 옵션은 루트 데이터 또는 루트 데이터-데이터 분할을 위해 구성된 디스크에 대한 추가 관리 기능을 제공합니다. 부팅 옵션 9에서 다음 옵션을 사용할 수 있습니다.
	
	`(9a) Unpartition all disks and remove their ownership information.`
	`(9b) Clean configuration and initialize system with partitioned disks.`
	`(9c) Clean configuration and initialize system with whole disks.`
	`(9d) Reboot the node.`
	`(9e) Return to main boot menu.`

ONTAP 클러스터에 있는 노드의 특성을 봅니다

클러스터에 있는 하나 이상의 노드 특성(예: 이름, 소유자, 위치, 모델 번호, 일련 번호, 노드 실행 시간, 상태 및 클러스터에 참여할 자격)을 볼 수 있습니다.

단계

1. 특정 노드의 속성 또는 클러스터의 모든 노드에 대한 속성을 표시하려면 'system node show' 명령을 사용합니다.

노드에 대한 정보를 표시하는 예

다음 예제에서는 node1에 대한 자세한 정보를 표시합니다.

```
cluster1::> system node show -node node1
                            Node: node1
                           Owner: Eng IT
                        Location: Lab 5
                           Model: model_number
                   Serial Number: 12345678
                       Asset Tag: -
                          Uptime: 23 days 04:42
                NVRAM System ID: 118051205
                       System ID: 0118051205
                          Vendor: NetApp
                          Health: true
                     Eligibility: true
       Differentiated Services: false
           All-Flash Optimized: true
            Capacity Optimized: false
                 QLC Optimized: false
    All-Flash Select Optimized: false
 SAS2/SAS3 Mixed Stack Support: none
```

ONTAP 노드의 특성을 수정합니다

필요에 따라 노드의 특성을 수정할 수 있습니다. 수정할 수 있는 속성에는 노드의 소유자 정보, 위치 정보, 자산 태그 및 클러스터에 참여할 자격이 포함됩니다.

이 작업에 대해

클러스터의 참여 자격은 system node modify 또는 cluster modify 명령의 ``–eligibility' 매개 변수를 사용하여 고급 권한 수준에서 수정할 수 있습니다. 노드의 적격성을 "false"로 설정하면 클러스터에서 노드가 비활성화됩니다.

로컬에서 노드 자격을 수정할 수 없습니다. 다른 노드에서 수정해야 합니다. 클러스터 HA 구성을 사용하여 노드 링도 수정할 수 없습니다.

노드 구성 복원 또는 노드 유지 보수 연장 등의 경우를 제외하고 노드의 적격성을 'false'로 설정하지 않아야 합니다. 노드에 대한 SAN 및 NAS 데이터 액세스는 노드가 부적격 상태일 때 영향을 받을 수 있습니다.

단계

1. 'system node modify' 명령을 사용하여 노드의 특성을 수정합니다.

노드 특성 수정 예

다음 명령을 실행하면 ""node1"" 노드의 특성이 수정됩니다. 노드 소유자가 ""Joe Smith""로 설정되고 자산 태그가 ""js1234""로 설정됩니다.

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag
js1234
```

관련 정보

- "시스템 노드 수정"
- "클러스터 수정"

ONTAP 노드의 이름을 바꿉니다

필요에 따라 노드 이름을 변경할 수 있습니다.

단계

1. 노드 이름을 바꾸려면 'system node rename' 명령어를 사용한다.

   `-newname`매개 변수는 노드의 새 이름을 지정합니다. 에 대한 자세한 내용은 `system node rename` link:https://docs.netapp.com/us-en/ontap-cli/system-node-rename.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

   클러스터에서 여러 노드의 이름을 바꾸려면 각 노드에 대해 명령을 개별적으로 실행해야 합니다.

   노드 이름은 모두(all)가 시스템 예약 이름이기 때문에 모두(all)일 수 없습니다.

노드 이름 바꾸기 예

다음 명령을 실행하면 노드 ""node1""의 이름이 ""node1a""로 변경됩니다.

```
cluster1::> system node rename -node node1 -newname node1a
```

단일 노드 **ONTAP** 클러스터를 관리합니다

단일 노드 클러스터는 독립 실행형 노드에서 실행되는 클러스터의 특수한 구현입니다. 단일 노드 클러스터는 이중화를 제공하지 않기 때문에 권장되지 않습니다. 노드가 다운되면 데이터 액세스가 손실됩니다.

내결함성 및 무중단 운영을 위해 클러스터를 구성하는 것이 좋습니다 "고가용성(HA 쌍)".

단일 노드 클러스터를 구성하거나 업그레이드하도록 선택하는 경우 다음 사항에 유의해야 합니다.

- 루트 볼륨 암호화는 단일 노드 클러스터에서 지원되지 않습니다.
- 단일 노드 클러스터를 가지고 있는 노드를 제거하는 경우 클러스터 포트를 데이터 포트로 수정한 다음 데이터 포트에 데이터 LIF를 생성하여 데이터 트래픽을 서비스하도록 클러스터 포트를 수정해야 합니다.
- 단일 노드 클러스터의 경우 소프트웨어 설치 중에 구성 백업 대상을 지정할 수 있습니다. 설정 후 ONTAP 명령을 사용하여 이러한 설정을 수정할 수 있습니다.

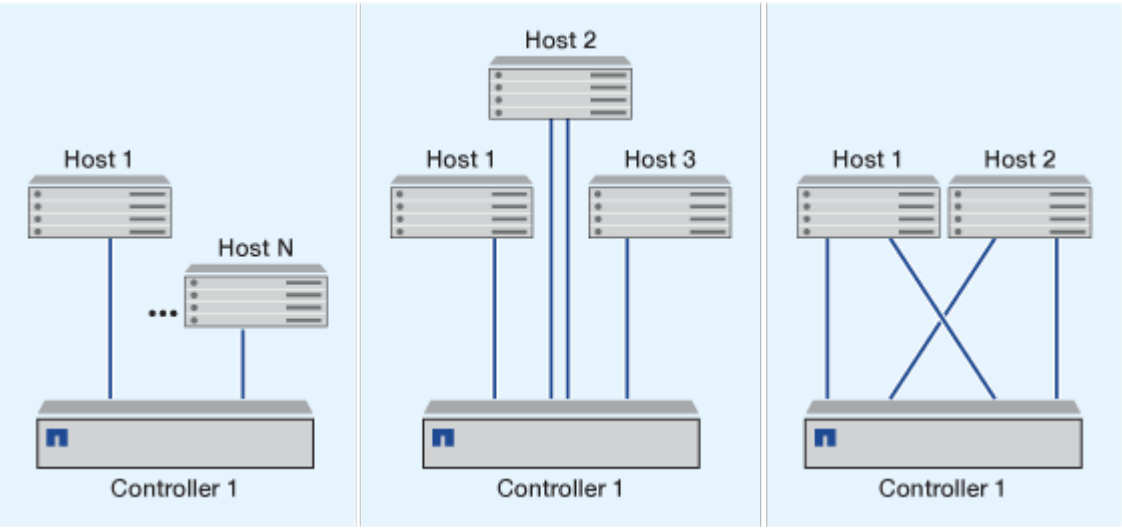
- 노드에 접속하는 호스트가 여러 개인 경우 각 호스트를 Windows 또는 Linux와 같은 다른 운영 체제로 구성할 수 있습니다. 호스트에서 컨트롤러로의 경로가 여러 개인 경우 호스트에서 ALUA를 활성화해야 합니다.

단일 노드로 **iSCSI SAN** 호스트를 구성하는 방법

iSCSI SAN 호스트를 단일 노드에 직접 연결하거나 하나 이상의 IP 스위치를 통해 연결하도록 구성할 수 있습니다. 노드는 스위치에 대한 여러 iSCSI 연결을 가질 수 있습니다.

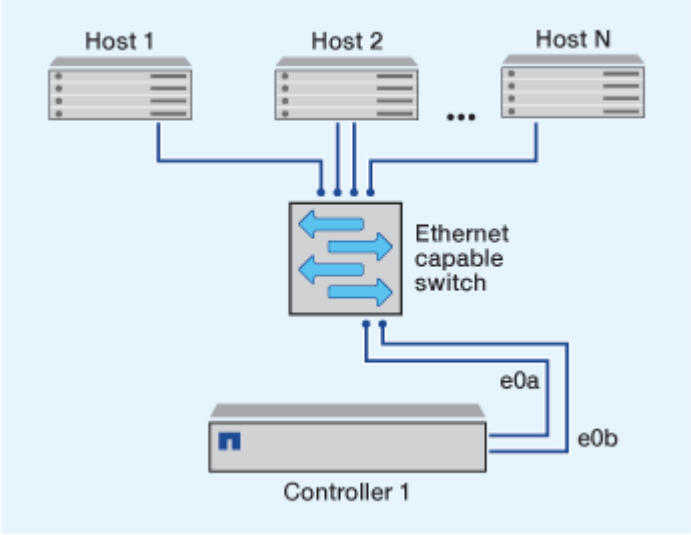
직접 연결 단일 노드 구성

직접 연결된 단일 노드 구성에서는 하나 이상의 호스트가 노드에 직접 연결됩니다.



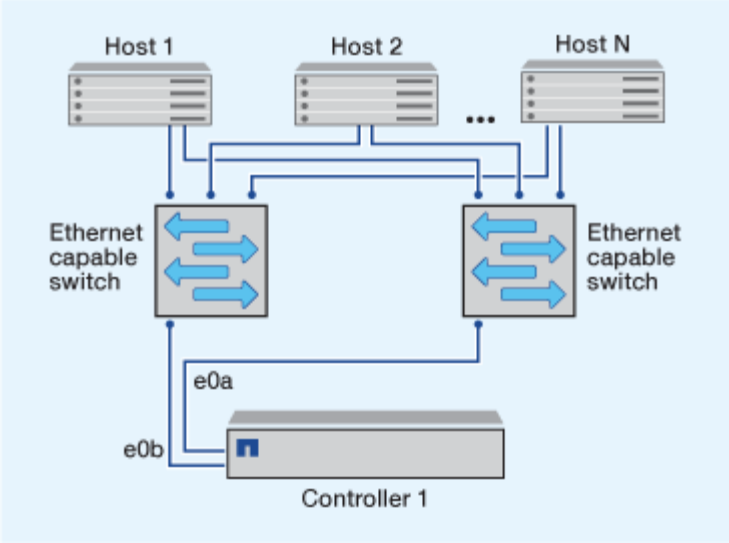
단일 네트워크 단일 노드 구성

단일 네트워크 단일 노드 구성에서는 하나의 스위치를 하나 이상의 호스트에 연결합니다. 단일 스위치가 있으므로 이 구성은 완전히 중복되지 않습니다.



다중 네트워크 단일 노드 구성

다중 네트워크 단일 노드 구성에서는 두 개 이상의 스위치가 단일 노드를 하나 이상의 호스트에 연결합니다. 스위치가 여러 개 있으므로 이 구성은 완전히 중복됩니다.



단일 노드로 **FC** 및 **FC-NVMe SAN** 호스트를 구성하는 방법

하나 이상의 패브릭을 통해 단일 노드로 FC 및 FC-NVMe SAN 호스트를 구성할 수 있습니다. N-포트 ID 가상화(NPIV)가 필요하며 Fabric의 모든 FC 스위치에서 활성화해야 합니다. FC 스위치를 사용하지 않고 FC 또는 FC-NMVE SAN 호스트를 단일 노드에 직접 연결할 수는 없습니다.

단일 패브릭 단일 노드 구성

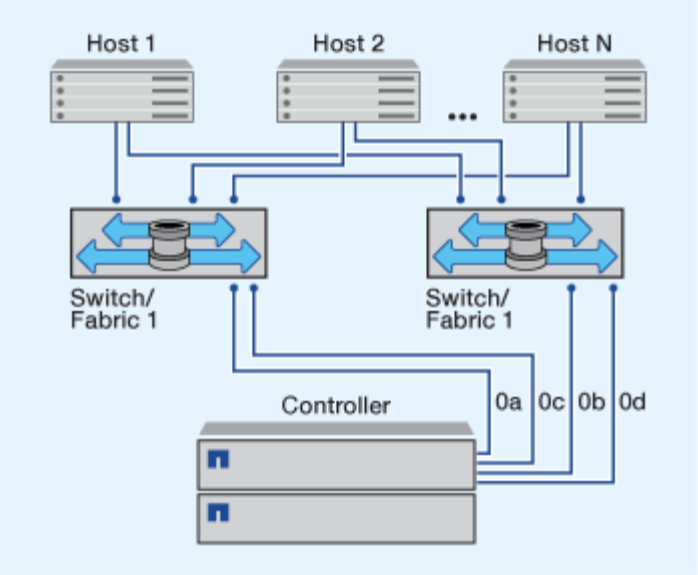
단일 패브릭 단일 노드 구성에서는 단일 노드를 하나 이상의 호스트에 연결하는 하나의 스위치가 있습니다. 단일 스위치가 있으므로 이 구성은 완전히 중복되지 않습니다.

단일 패브릭 단일 노드 구성에서는 호스트에서 노드로 연결되는 단일 경로만 있으면 다중 경로 소프트웨어가 필요하지 않습니다.

멀티패브릭 단일 노드 구성

다중 패브릭 단일 노드 구성에는 단일 노드를 하나 이상의 호스트에 연결하는 스위치가 2개 이상 있습니다. 다음 그림은 간소화를 위해 두 개의 패브릭만 있는 다중 패브릭 단일 노드 구성을 보여 주며 여러 개의 패브릭 구성에서 두 개 이상의 패브릭을 사용할 수 있습니다. 이 그림에서 스토리지 컨트롤러는 상단 섀시에 마운트되며, 하단 섀시는 이 예제에서와 같이 비어 있거나 IOMX 모듈이 있을 수 있습니다.

그림의 FC 타겟 포트(0a, 0c, 0b, 0d)가 예제입니다. 실제 포트 번호는 스토리지 노드의 모델 및 확장 어댑터를 사용하고 있는지에 따라 다릅니다.



관련 정보

"NetApp 기술 보고서 4684: NVMe-oF를 사용하여 최신 SAN 구현 및 구성"

단일 노드 클러스터에 대한 **ONTAP** 업그레이드

ONTAP CLI를 사용하여 단일 노드 클러스터의 자동 업데이트를 수행할 수 있습니다. 단일 노드 클러스터는 중복성이 부족하여 업데이트가 항상 중단을 초래합니다. System Manager를 사용하여 중단을 초래하는 업그레이드를 수행할 수 없습니다.

시작하기 전에

업그레이드를 완료해야 합니다 "준비" 단계.

단계

1. 이전 ONTAP 소프트웨어 패키지를 삭제합니다.

```
cluster image package delete -version <previous_package_version>
```

2. 대상 ONTAP 소프트웨어 패키지를 다운로드합니다.

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz

Package download completed.
Package processing completed.
```

3. 소프트웨어 패키지를 클러스터 패키지 리포지토리에서 사용할 수 있는지 확인합니다.

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.7              M/DD/YYYY 10:32:15
```

4. 클러스터를 업그레이드할 준비가 되었는지 확인합니다.

```
cluster image validate -version <package_version_number>
```

```
cluster1::> cluster image validate -version 9.7

WARNING: There are additional manual upgrade validation checks that must
be performed after these automated validation checks have completed...
```

5. 검증 진행 상황 모니터링:

```
cluster image show-update-progress
```

6. 검증에서 식별된 모든 필수 조치를 완료하십시오.
7. 필요한 경우 소프트웨어 업그레이드 예상치를 생성합니다.

```
cluster image update -version <package_version_number> -estimate-only
```

소프트웨어 업그레이드 추정치는 업데이트할 각 구성 요소에 대한 세부 정보와 예상 업그레이드 기간을 표시합니다.

8. 소프트웨어 업그레이드 수행:

```
cluster image update -version <package_version_number>
```

> 문제가 발생하면 업데이트가 일시 중지되고 수정 조치를 취하라는 메시지가 표시됩니다. 클러스터 image show-update-progress 명령을 사용하여 문제 및 업데이트 진행 상황에 대한 세부 정보를 볼 수 있습니다. 문제를 해결한 후 cluster image resume-update 명령을 사용하여 업데이트를 다시 시작할 수 있습니다.

9. 클러스터 업데이트 진행률을 표시합니다.

```
cluster image show-update-progress
```

노드가 업데이트의 일부로 재부팅되며 재부팅 중에 액세스할 수 없습니다.

10. 알림 트리거:

```
autosupport invoke -node * -type all -message "Finishing_Upgrade"
```

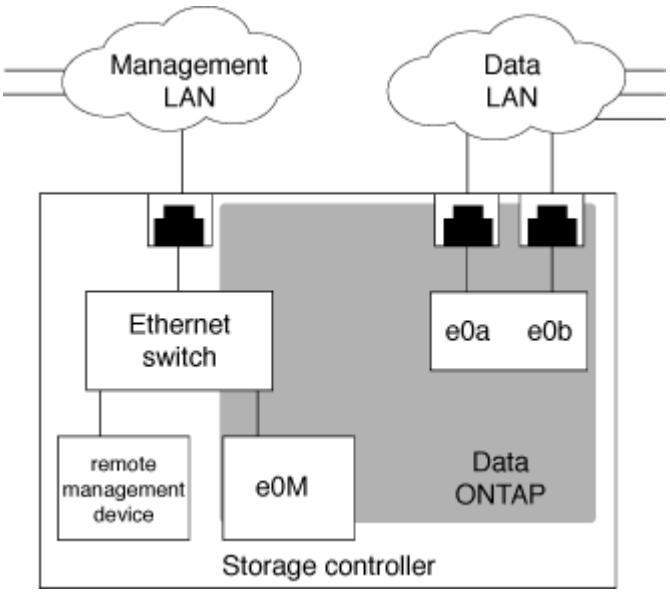
클러스터가 메시지를 전송하도록 구성되지 않은 경우 알림 복사본이 로컬에 저장됩니다.

SP/BMC 네트워크를 구성합니다

네트워크에서 **ONTAP** 관리 트래픽 격리

관리 트래픽 전용 서브넷에 SP/BMC 및 e0M 관리 인터페이스를 구성하는 것이 좋습니다. 관리 네트워크를 통해 데이터 트래픽을 실행하면 성능 저하 및 라우팅 문제가 발생할 수 있습니다.

대부분의 스토리지 컨트롤러의 관리 이더넷 포트(섀시 뒤쪽에 렌치 아이콘으로 표시됨)는 내부 이더넷 스위치에 연결됩니다. 내부 스위치는 SP/BMC 및 e0M 관리 인터페이스에 대한 연결을 제공하며, 이 인터페이스를 사용하여 텔넷, SSH 및 SNMP와 같은 TCP/IP 프로토콜을 통해 스토리지 시스템에 액세스할 수 있습니다.



원격 관리 장치와 e0M을 모두 사용하려는 경우 동일한 IP 서브넷에 구성해야 합니다. 이러한 인터페이스는 대역폭이 낮은 인터페이스이므로 관리 트래픽 전용 서브넷에 SP/BMC 및 e0M을 구성하는 것이 좋습니다.

관리 트래픽을 격리할 수 없거나 전용 관리 네트워크가 비정상적으로 큰 경우 네트워크 트래픽 볼륨을 가능한 낮게 유지해야 합니다. 브로드캐스트 또는 멀티캐스트 트래픽이 과도하게 유입될 경우 SP/BMC 성능이 저하될 수 있습니다.

AFF A800과 같은 일부 스토리지 컨트롤러에는 BMC용 포트 2개와 e0M용 포트 1개가 있습니다. 이러한 컨트롤러의 경우 동일한 IP 서브넷에 BMC 및 e0M을 구성할 필요가 없습니다.

SP에 대해 클러스터 레벨의 자동 네트워크 구성을 설정할 수 있습니다(권장). 또한 SP 자동 네트워크 구성을 기본값인 사용하지 않도록 설정하고 SP 네트워크 구성을 노드 레벨에서 수동으로 관리할 수도 있습니다. 각 사례별로 몇 가지 고려 사항이 있습니다.

이 항목은 SP와 BMC 모두에 적용됩니다.

SP의 자동 네트워크 구성을 사용하면 SP가 지정된 서브넷의 주소 리소스(IP 주소, 서브넷 마스크 및 게이트웨이 주소 포함)를 사용하여 네트워크를 자동으로 설정할 수 있습니다. SP 자동 네트워크 구성을 사용하면 각 노드의 SP에 IP 주소를 수동으로 할당할 필요가 없습니다. 기본적으로 SP 자동 네트워크 구성은 비활성화되어 있습니다. 구성을 활성화하려면 먼저 클러스터에서 구성에 사용할 서브넷을 정의해야 하기 때문입니다.

SP 자동 네트워크 구성을 사용하도록 설정하면 다음과 같은 시나리오와 고려 사항이 적용됩니다.

- SP를 구성한 적이 없을 경우 SP 자동 네트워크 구성에 지정된 서브넷에 따라 SP 네트워크가 자동으로 구성됩니다.
- 이전에 SP를 수동으로 구성했거나 기존 SP 네트워크 구성이 다른 서브넷을 기반으로 한 경우, 클러스터에 있는 모든 노드의 SP 네트워크는 SP 자동 네트워크 구성에 지정한 서브넷에 따라 재구성됩니다.

  재구성을 수행하면 SP에 다른 주소가 할당되며, 이는 DNS 구성과 SP 호스트 이름 확인 기능에 영향을 줄 수 있습니다. 따라서 DNS 구성을 업데이트해야 할 수 있습니다.

- 클러스터를 연결하는 노드는 지정된 서브넷을 사용하여 SP 네트워크를 자동으로 구성합니다.
- 'system service-processor network modify' 명령을 사용해도 SP IP 주소를 변경할 수 없습니다.

  SP 자동 네트워크 구성이 설정된 경우 명령을 사용하면 SP 네트워크 인터페이스를 설정 또는 해제할 수만 있습니다.

  - SP 자동 네트워크 구성이 이전에 설정된 경우 SP 네트워크 인터페이스를 해제하면 할당된 주소 리소스가 해제되고 서브넷에 반환됩니다.
  - SP 네트워크 인터페이스를 해제한 다음 다시 설정하는 경우 SP를 다른 주소로 재구성할 수 있습니다.

SP 자동 네트워크 구성이 비활성화되어 있는 경우(기본값), 다음과 같은 시나리오 및 고려 사항이 적용됩니다.

- SP를 구성되지 않은 경우 SP IPv4 네트워크 구성의 기본값은 IPv4 DHCP를 사용하고 IPv6은 사용되지 않도록 설정됩니다.

  클러스터에 연결된 노드는 기본적으로 SP 네트워크 구성에 IPv4 DHCP도 사용합니다.

- 'system service-processor network modify' 명령을 사용하면 노드의 SP IP 주소를 구성할 수 있습니다.

  서브넷에 할당된 주소를 사용하여 SP 네트워크를 수동으로 구성하려고 하면 경고 메시지가 표시됩니다. 경고를 무시하고 수동으로 주소를 할당하면 중복된 주소가 있는 시나리오가 발생할 수 있습니다.

이전에 SP 자동 네트워크 구성을 사용하도록 설정한 후 SP 자동 네트워크 구성을 사용하지 않도록 설정한 경우 다음과 같은 시나리오 및 고려 사항이 적용됩니다.

- SP의 자동 네트워크 구성에 IPv4 주소 제품군이 비활성화되어 있으면 SP IPv4 네트워크는 기본적으로 DHCP를 사용합니다. 또한 'system service-processor network modify' 명령을 사용하면 개별 노드의 SP IPv4 구성을 수정할 수 있습니다.

- SP의 자동 네트워크 구성에 IPv6 주소 제품군이 비활성화되어 있으면 SP IPv6 네트워크도 비활성화되고, 'system service-processor network modify' 명령을 사용하면 개별 노드에 대해 SP IPv6 구성을 설정 및 수정할 수 있습니다.

ONTAP SP/BMC 자동 네트워크 구성을 활성화합니다

SP 네트워크를 수동으로 구성하는 대신 자동 네트워크 구성을 사용하도록 SP를 설정하는 것이 좋습니다. SP 자동 네트워크 구성은 클러스터 전체에 있으므로 개별 노드의 SP 네트워크를 수동으로 관리할 필요가 없습니다.

이 태스크는 SP와 BMC 모두에 적용됩니다.

- SP 자동 네트워크 구성에 사용할 서브넷이 이미 클러스터에 정의되어 있어야 하며 SP 네트워크 인터페이스와 리소스 충돌이 없어야 합니다.

  network subnet show 명령은 클러스터의 서브넷 정보를 표시합니다.

  에 대한 자세한 내용은 `network subnet show` "ONTAP 명령 참조입니다"을 참조하십시오.

  네트워크 서브넷 명령의 서브넷 연관(-force-update-lif-associations) 매개 변수를 강제하는 매개변수는 SP 네트워크 인터페이스가 아닌 네트워크 LIF에서만 지원됩니다.

- SP에 대해 IPv6 연결을 사용하려면 ONTAP에 대해 IPv6가 이미 구성 및 설정되어 있어야 합니다.

  `network options ipv6 show`명령을 실행하면 ONTAP에 대한 IPv6 설정의 현재 상태가 표시됩니다. 에 대한 자세한 내용은 `network options ipv6 show` link:https://docs.netapp.com/us-en/ontap-cli/network-options-ipv6-show.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

단계

1. 'system service-processor network auto-configuration enable' 명령어를 사용하여 SP가 사용할 서브넷의 IPv4 또는 IPv6 주소 제품군과 이름을 지정한다.
2. 'system service-processor network auto-configuration show' 명령을 사용하여 SP 자동 네트워크 구성을 표시합니다.
3. 이후에 쿼럼에 있는 모든 노드에 대해 SP IPv4 또는 IPv6 네트워크 인터페이스를 비활성화하거나 다시 활성화하려면 '-address-family'['IPv4'|'IPv6'] 및 '-enable'['true'|'false'] 매개 변수를 사용하여 'system service-processor network modify' 명령을 사용하십시오.

   SP 자동 네트워크 구성이 설정된 경우 쿼럼에 있는 노드의 SP IP 주소를 수정할 수 없습니다. SP IPv4 또는 IPv6 네트워크 인터페이스만 사용하거나 사용하지 않도록 설정할 수 있습니다.

   노드가 쿼럼을 벗어난 경우 노드에서 '시스템 서비스 프로세서 네트워크 수정'을 실행하고 노드의 SP 자동 네트워크 구성을 재정의할지 확인하여 SP IP 주소를 포함한 노드의 SP 네트워크 구성을 수정할 수 있습니다. 그러나 노드가 쿼럼에 연결되면 지정된 서브넷에 따라 노드에 대한 SP 자동 재구성이 수행됩니다.

SP에 자동 네트워크 구성이 설정되어 있지 않은 경우 IP 주소를 사용하여 SP에 액세스할 수 있도록 노드의 SP 네트워크를 수동으로 구성해야 합니다.

시작하기 전에

SP에 대해 IPv6 연결을 사용하려면 ONTAP에 대해 IPv6가 이미 구성 및 설정되어 있어야 합니다. `network options ipv6`명령에서 ONTAP의 IPv6 설정을 관리합니다. 에 대한 자세한 내용은 `network options ipv6` "ONTAP 명령 참조입니다"을 참조하십시오.

이 태스크는 SP와 BMC 모두에 적용됩니다.

SP에서 IPv4, IPv6 또는 둘 다를 사용하도록 구성할 수 있습니다. SP IPv4 구성은 정적 및 DHCP 주소 할당을 지원하며, SP IPv6 구성은 정적 주소 지정만 지원합니다.

SP 자동 네트워크 구성이 설정된 경우 개별 노드에 대해 SP 네트워크를 수동으로 구성할 필요가 없으며 'system service-processor network modify' 명령을 사용하면 SP 네트워크 인터페이스만 설정하거나 해제할 수 있습니다.

단계

1. 'system service-processor network modify' 명령어를 사용하여 노드에 대한 SP 네트워크를 설정한다.
   - '-address-family' 매개변수는 SP의 IPv4 또는 IPv6 구성을 수정할지 여부를 지정합니다.
   - '-enable' 파라미터는 지정된 IP 주소 제품군의 네트워크 인터페이스를 활성화한다.
   - '-DHCP' 매개변수는 DHCP 서버의 네트워크 구성을 사용할지 또는 사용자가 제공하는 네트워크 주소를 사용할지 여부를 지정합니다.

     IPv4를 사용하는 경우에만 DHCP('-DHCP'를 'v4'로 설정)를 활성화할 수 있습니다. IPv6 구성에 대해 DHCP를 활성화할 수 없습니다.

   - '-ip-address' 매개 변수는 SP의 공용 IP 주소를 지정합니다.

     서브넷에 할당된 주소를 사용하여 SP 네트워크를 수동으로 구성하려고 하면 경고 메시지가 표시됩니다. 경고를 무시하고 수동 주소 할당을 계속하면 주소가 중복 할당될 수 있습니다.

   - '-netmask' 매개변수는 SP의 넷마스크를 지정합니다(IPv4를 사용하는 경우).
   - prefix-length 매개 변수는 SP에 대한 서브넷 마스크의 네트워크 접두사-길이를 지정합니다(IPv6를 사용하는 경우).
   - '-gateway' 매개변수는 SP의 게이트웨이 IP 주소를 지정합니다.
2. 1단계를 반복하여 클러스터의 나머지 노드에 대해 SP 네트워크를 구성합니다.
3. SP 네트워크 구성을 표시하고 '–instance' 또는 '–field setup-status' 매개 변수를 사용하여 'system service-processor network show' 명령을 사용하여 SP 설정 상태를 확인합니다.

   노드의 SP 설정 상태는 다음 중 하나일 수 있습니다.

   - '설정 안 됨' — 구성되지 않음
   - '성공' — 구성에 성공했습니다
   - 진행 중 — 구성이 진행 중입니다

◦ 실패 — 구성에 실패했습니다

SP 네트워크 구성의 예

다음 예에서는 노드의 SP에서 IPv4를 사용하도록 구성하고 SP를 사용하도록 설정하며 SP 네트워크 구성을 표시하여 설정을 확인합니다.

```
cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

                             Node: node1
                     Address Type: IPv4
                Interface Enabled: true
                   Type of Device: SP
                           Status: online
                      Link Status: up
                      DHCP Status: none
                       IP Address: 192.168.123.98
                      MAC Address: ab:cd:ef:fe:ed:02
                          Netmask: 255.255.255.0
       Prefix Length of Subnet Mask: -
         Router Assigned IP Address: -
              Link Local IP Address: -
                 Gateway IP Address: 192.168.123.1
                  Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
                        Subnet Name: -
Enable IPv6 Router Assigned Address: -
            SP Network Setup Status: succeeded
    SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>
```

ONTAP 서비스 프로세서 **API** 구성을 수정합니다

SP API는 ONTAP가 네트워크를 통해 SP와 통신할 수 있도록 지원하는 보안 네트워크 API입니다. SP API 서비스에 사용되는 포트를 변경하거나, 서비스가 내부 통신에 사용하는 인증서를 갱신하거나, 서비스를 완전히 해제할 수 있습니다. 드문 경우에만 구성을 수정해야 합니다.

이 작업에 대해

- SP API 서비스는 기본적으로 포트 50000을 사용합니다.

예를 들어 다른 네트워킹 응용 프로그램의 통신에 포트 '50000’이 사용되는 네트워크 설정에 있거나 다른 응용 프로그램과 SP API 서비스에서 생성된 트래픽을 구별하려는 경우 포트 값을 변경할 수 있습니다.

- SP API 서비스에서 사용하는 SSL 및 SSH 인증서는 클러스터 내부에 있으며 외부에 배포되지 않습니다.

  드물지만 인증서가 손상된 경우 인증서를 갱신할 수 있습니다.

- SP API 서비스는 기본적으로 사용하도록 설정됩니다.

  SP가 구성되어 있지 않거나 사용되지 않고 서비스를 해제하려는 전용 LAN과 같은 드문 경우에만 SP API 서비스를 사용하지 않도록 설정해야 합니다.

  SP API 서비스가 해제되어 있으면 API는 들어오는 연결을 허용하지 않습니다. 또한 네트워크 기반 SP 펌웨어 업데이트 및 네트워크 기반 SP "자체 시스템" 로그 수집 등의 기능을 사용할 수 없게 됩니다. 시스템이 직렬 인터페이스를 사용하여 로 전환됩니다.

단계

1. Set-Privilege advanced 명령을 사용하여 고급 권한 레벨로 전환합니다.
2. SP API 서비스 구성을 수정합니다.

원하는 작업	다음 명령을 사용합니다...
SP API 서비스에서 사용하는 포트를 변경합니다	'-port'{'49152'….65535' 매개변수를 사용하여 시스템 서비스 프로세서 API 서비스를 수정합니다
내부 통신을 위해 SP API 서비스에서 사용하는 SSL 및 SSH 인증서를 갱신합니다	• ONTAP 9.5 이상의 경우 'system service-processor api-service renew-internal-certificate’를 사용한다 • ONTAP 9.4 및 그 이전 버전의 경우 • '시스템 서비스 - 프로세서 API - 서비스 갱신 - 인증서' 매개 변수를 지정하지 않으면 호스트 인증서(클라이언트 및 서버 인증서 포함)만 갱신됩니다. '-renew-all true' 매개 변수가 지정된 경우 호스트 인증서와 루트 CA 인증서가 모두 갱신됩니다.
통신	
SP API 서비스를 사용하지 않도록 설정하거나 다시 설정합니다	'-is-enabled'{'true'

3. 'system service-processor api-service show' 명령을 사용하여 SP API 서비스 구성을 표시합니다.

SP/BMC를 사용하여 노드를 원격으로 관리합니다

SP/BMC를 사용하여 ONTAP 노드를 원격으로 관리합니다

서비스 프로세서(SP) 또는 베이스보드 관리 컨트롤러(BMC)라고 하는 온보드 컨트롤러를 사용하여 노드를 원격으로 관리할 수 있습니다. 이 원격 관리 컨트롤러는 현재 모든 플랫폼 모델에 포함되어 있습니다. 노드의 작동 상태에 관계없이 컨트롤러가 작동 상태를 유지합니다.

플랫폼 SP 및 BMC 지원에 대한 자세한 내용은 NetApp Support 사이트에서 을 참조하십시오"지원 매트릭스".

ONTAP 서비스 프로세서를 사용한 원격 노드 관리

서비스 프로세서(SP)는 노드를 원격으로 액세스, 모니터링 및 문제 해결할 수 있는 원격 관리 디바이스입니다.

SP의 주요 기능은 다음과 같습니다.

- SP를 사용하면 노드 컨트롤러의 상태에 관계없이 노드를 원격으로 액세스하여 진단, 종료, 전원 껐다 켜기 또는 재부팅할 수 있습니다.

  SP는 대기 전압을 통해 전원을 공급받습니다. 이 경우 노드에 전원 공급 장치 중 하나 이상의 전원이 공급되는 경우 이 전압을 사용할 수 있습니다.

  관리 호스트에서 Secure Shell 클라이언트 애플리케이션을 사용하여 SP에 로그인할 수 있습니다. 그런 다음 SP CLI를 사용하여 노드를 원격으로 모니터링하고 문제를 해결할 수 있습니다. 또한 SP를 사용하여 시리얼 콘솔에 액세스하고 ONTAP 명령을 원격으로 실행할 수 있습니다.

  시리얼 콘솔에서 SP에 액세스하거나 SP에서 시리얼 콘솔에 액세스할 수 있습니다. SP를 사용하면 SP CLI 세션과 별도의 콘솔 세션을 동시에 열 수 있습니다.

  예를 들어, 온도 센서가 심각하게 높거나 낮으면 ONTAP가 SP를 트리거하여 마더보드를 정상적으로 종료합니다. 시리얼 콘솔이 응답하지 않게 되지만 콘솔에서 Ctrl-G를 눌러 SP CLI에 액세스할 수 있습니다. 그런 다음 SP의 '시스템 전원 켜기' 또는 '시스템 전원 주기' 명령을 사용하여 노드 전원을 켜거나 전원을 껐다가 켤 수 있습니다.

- SP는 환경 센서를 모니터링하고 이벤트를 기록하여 서비스 작업을 시기적절하고 효과적으로 수행하도록 지원합니다.

  SP는 노드 온도, 전압, 전류 및 팬 속도와 같은 환경 센서를 모니터링합니다. 환경 센서가 비정상 상태에 도달하면 SP가 비정상 판독값을 기록하고 ONTAP에 문제를 알리며, 노드가 AutoSupport 메시지를 보낼 수 있는지 여부와 관계없이 AutoSupport 메시지를 통해 필요에 따라 알림과 "시스템 소유" 알림을 보냅니다.

  SP는 부팅 진행률, FRU(Field Replaceable Unit) 변경 사항, ONTAP에서 생성된 이벤트 및 SP 명령 기록과 같은 이벤트도 기록합니다. AutoSupport 메시지를 수동으로 호출하여 지정된 노드에서 수집된 SP 로그 파일을 포함할 수 있습니다.

  AutoSupport 메시지에 추가 진단 정보를 첨부하여 중단된 노드를 대신하여 이 메시지를 생성하는 것 외에 SP는 AutoSupport 기능에 영향을 주지 않습니다. AutoSupport 구성 설정 및 메시지 내용 동작은 ONTAP에서 상속됩니다.

SP는 시스템 노드 AutoSupport modify 명령의 '-transport' 매개 변수 설정에 의존하여 알림을 보내지 않습니다. SP는 SMTP(Simple Mail Transport Protocol)만 사용하며 호스트의 AutoSupport 구성이 있어야 메일 호스트 정보를 포함할 수 있습니다.

SNMP가 설정된 경우 SP는 모든 "자체 시스템" 이벤트에 대해 구성된 트랩 호스트에 대한 SNMP 트랩을 생성합니다.

- SP에는 시스템 이벤트 로그(SEL)에 최대 4,000개의 이벤트를 저장할 수 있는 비휘발성 메모리 버퍼가 있기 때문에 문제 진단에 도움이 됩니다.

  SEL은 각 감사 로그 항목을 감사 이벤트로 저장합니다. SP의 온보드 플래시 메모리에 저장됩니다. SEL의 이벤트 목록은 SP에서 AutoSupport 메시지를 통해 지정된 수신자에게 자동으로 전송됩니다.

  SEL에는 다음 정보가 포함됩니다.

  - SP에서 감지한 하드웨어 이벤트 - 예를 들어 전원 공급 장치, 전압 또는 기타 구성 요소에 대한 센서 상태
  - SP에서 감지된 오류 — 예를 들어 통신 오류, 팬 장애 또는 메모리 또는 CPU 오류
  - SP의 시스템 리셋 또는 시스템 전원 사이클 명령을 실행하여 장애, 통신 장애, 부팅 장애, 사용자 트리거된 "자체 시스템"과 같은 중요한 소프트웨어 이벤트가 노드에 의해 SP로 전송됩니다
- SP는 관리자가 콘솔에 로그인했는지 또는 연결되어 있는지 여부에 관계없이 직렬 콘솔을 모니터링합니다.

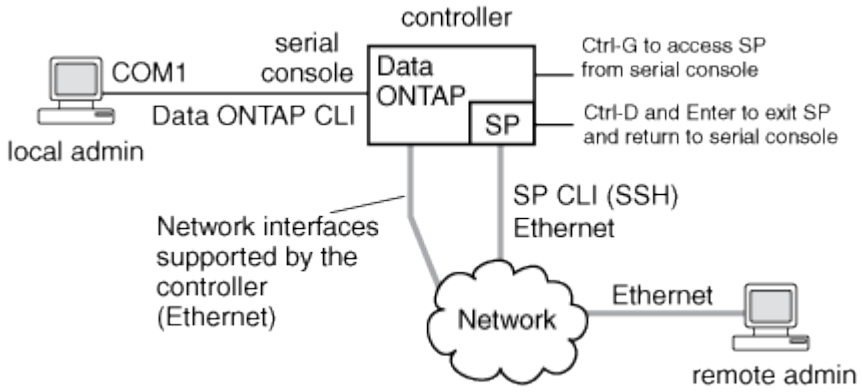
  메시지가 콘솔에 전송되면 SP는 해당 메시지를 콘솔 로그에 저장합니다. 콘솔 로그는 SP가 노드 전원 공급 장치 중 하나에서 전원을 공급받는 동안 유지됩니다. SP는 대기 전력으로 작동하므로 노드의 전원을 껐다가 켜거나 전원을 끄더라도 사용 가능한 상태로 유지됩니다.

- SP가 구성된 경우 하드웨어 지원 테이크오버를 사용할 수 있습니다.
- SP API 서비스를 사용하면 ONTAP가 네트워크를 통해 SP와 통신할 수 있습니다.

  이 서비스는 SP 펌웨어 업데이트에 네트워크 인터페이스를 사용하고, 노드가 다른 노드의 SP 기능 또는 시스템 콘솔에 액세스하고, 다른 노드에서 SP 로그를 업로드할 수 있도록 하는 등 네트워크 기반 기능을 지원하여 SP의 ONTAP 관리를 향상합니다.

  서비스가 사용하는 포트를 변경하거나, 내부 통신에 사용되는 SSL 및 SSH 인증서를 갱신하거나, 서비스를 완전히 비활성화하여 SP API 서비스의 구성을 수정할 수 있습니다.

다음 다이어그램에서는 노드의 ONTAP 및 SP에 대한 액세스를 보여 줍니다. SP 인터페이스는 이더넷 포트를 통해 액세스합니다(섀시 후면에 렌치 아이콘이 표시됨).



ONTAP 베이스보드 관리 컨트롤러를 사용하여 노드를 원격으로 관리합니다

특정 하드웨어 플랫폼에서는 베이스보드 관리 컨트롤러(BMC)의 새 온보드 컨트롤러를 지원하도록 소프트웨어가 사용자 정의됩니다. BMC에는 장치를 원격으로 관리하는 데 사용할 수 있는 CLI(Command-Line Interface) 명령이 있습니다.

BMC는 서비스 프로세서(SP)와 유사하게 작동하며 동일한 명령을 많이 사용합니다. BMC를 사용하면 다음을 수행할 수 있습니다.

- BMC 네트워크 설정을 구성합니다.
- 노드를 원격으로 액세스하고 진단, 종료, 전원 껐다 켜기 또는 재부팅과 같은 노드 관리 작업을 수행합니다.

SP와 BMC 간에는 몇 가지 차이점이 있습니다.

- BMC는 전원 공급 장치 요소, 냉각 요소, 온도 센서, 전압 센서 및 전류 센서의 환경 모니터링을 완벽하게 제어합니다. BMC는 IPMI를 통해 센서 정보를 ONTAP에 보고합니다.
- 일부 고가용성(HA) 및 스토리지 명령은 서로 다릅니다.
- BMC는 AutoSupport 메시지를 보내지 않습니다.

다음 요구 사항을 충족하는 경우 ONTAP 실행하는 경우에도 자동 펌웨어 업데이트를 사용할 수 있습니다.

- BMC 펌웨어 버전 1.15 이상이 설치되어 있어야 합니다.

  BMC 펌웨어를 1.12에서 1.15 이상으로 업그레이드하려면 수동 업데이트가 필요합니다.

- 펌웨어 업데이트가 완료되면 BMC가 자동으로 재부팅됩니다.

  BMC 재부팅 중 노드 작업은 영향을 받지 않습니다.

ONTAP SP/BMC 펌웨어 업데이트를 관리합니다

ONTAP에는 _baseline image_라고 하는 SP 펌웨어 이미지가 포함되어 있습니다. 이후에 새로운 버전의 SP 펌웨어를 사용할 수 있게 되면 ONTAP 버전을 업그레이드하지 않고 SP 펌웨어를 다운로드하여 다운로드한 버전으로 업데이트할 수 있습니다.

이 항목은 SP와 BMC 모두에 적용됩니다.

ONTAP에서는 SP 펌웨어 업데이트를 관리하는 다음과 같은 방법을 제공합니다.

- SP 자동 업데이트 기능은 기본적으로 활성화되어 다음과 같은 경우 SP 펌웨어가 자동으로 업데이트됩니다.
  - 새 버전의 ONTAP로 업그레이드하는 경우

    ONTAP 업그레이드 프로세스에는 SP 펌웨어 업데이트가 자동으로 포함됩니다. 단, ONTAP와 함께 번들로 제공되는 SP 펌웨어 버전이 노드에서 실행 중인 SP 버전보다 최신이어야 합니다.

ONTAP SP 자동 업데이트에 실패한 것을 감지하고 최대 3회까지 SP 자동 업데이트를 다시 시도하기 위한 시정 조치를 실행합니다. 세 번의 재시도가 모두 실패하면 다음을 참조하세요 ."NetApp 기술 자료: Health Monitor SPAutoUpgradeFailedMajorAlert SP 업그레이드 실패 - AutoSupport 메시지" .

- NetApp Support 사이트에서 SP 펌웨어 버전을 다운로드하고 다운로드한 버전이 현재 SP에서 실행 중인 버전보다 최신입니다
- 이전 버전의 ONTAP로 다운그레이드하거나 되돌릴 때

  SP 펌웨어는 이전 또는 다운그레이드한 ONTAP 버전에서 지원하는 최신 호환 버전으로 자동 업데이트됩니다. 수동 SP 펌웨어 업데이트는 필요하지 않습니다.

'system service-processor image modify' 명령을 사용하여 SP 자동 업데이트 기능을 비활성화할 수 있습니다. 그러나 이 기능을 활성 상태로 두는 것이 좋습니다. 이 기능을 사용하지 않도록 설정하면 ONTAP 이미지와 SP 펌웨어 이미지 간에 최적화되지 않은 또는 비정규화된 조합이 발생할 수 있습니다.

- ONTAP를 사용하면 수동으로 SP 업데이트를 트리거하고 'system service-processor image update' 명령을 사용하여 업데이트 방법을 지정할 수 있습니다.

  다음 옵션을 지정할 수 있습니다.

  - 사용할 SP 펌웨어 패키지('-package')

    패키지 파일 이름을 지정하여 SP 펌웨어를 다운로드한 패키지로 업데이트할 수 있습니다. advance 'system image package show' 명령어는 노드에서 사용할 수 있는 모든 패키지 파일(SP 펌웨어 패키지의 파일 포함)을 출력한다.

  - SP 업데이트에 기본 SP 펌웨어 패키지를 사용할지 여부('-baseline')

    현재 실행 중인 ONTAP 버전에 번들로 제공되는 기본 버전으로 SP 펌웨어를 업데이트할 수 있습니다.

  고급 업데이트 옵션 또는 매개 변수 중 일부를 사용하는 경우 BMC의 구성 설정이 일시적으로 지워질 수 있습니다. 재부팅 후 ONTAP가 BMC 구성을 복원하는 데 최대 10분이 걸릴 수 있습니다.

- ONTAP를 사용하면 'system service-processor image update-progress show' 명령을 사용하여 ONTAP에서 트리거된 최신 SP 펌웨어 업데이트의 상태를 표시할 수 있습니다.

SP 펌웨어를 업데이트하는 동안 SP에 대한 기존 연결이 모두 종료됩니다. 이는 SP 펌웨어 업데이트가 자동으로 수행되는지 아니면 수동으로 실행되는지 여부입니다.

관련 정보

"NetApp 다운로드: 시스템 펌웨어 및 진단"

펌웨어 업데이트에 **ONTAP SP/BMC** 및 네트워크 인터페이스를 사용합니다

버전 1.5, 2.5, 3.1 이상을 실행하는 SP에서 ONTAP에서 트리거되는 SP 펌웨어 업데이트는 SP 네트워크 인터페이스를 통해 IP 기반 파일 전송 메커니즘을 사용할 수 있도록 지원합니다.

이 항목은 SP와 BMC 모두에 적용됩니다.

네트워크 인터페이스를 통한 SP 펌웨어 업데이트가 직렬 인터페이스를 통한 업데이트보다 빠릅니다. SP 펌웨어를 업데이트하는 동안 유지 관리 시간이 줄어들며 ONTAP 작업도 중단되지 않습니다. 이 기능을 지원하는 SP 버전은 ONTAP에 포함되어 있습니다. 또한 NetApp Support 사이트에서 제공되며 호환되는 ONTAP 버전을 실행 중인 컨트롤러에 설치할 수 있습니다.

SP 버전 1.5, 2.5, 3.1 이상을 실행하는 경우 다음과 같은 펌웨어 업그레이드 동작이 적용됩니다.

- ONTAP에서 _automatically_triggered인 SP 펌웨어 업데이트는 기본적으로 업데이트를 위한 네트워크 인터페이스를 사용합니다. 그러나 다음 조건 중 하나가 발생할 경우 SP 자동 업데이트는 펌웨어 업데이트를 위한 직렬 인터페이스를 사용하도록 전환됩니다.
  - SP 네트워크 인터페이스가 구성되지 않았거나 사용할 수 없습니다.
  - IP 기반 파일 전송에 실패했습니다.
  - SP API 서비스가 해제되었습니다.

실행 중인 SP 버전에 관계없이 SP CLI에서 트리거된 SP 펌웨어 업데이트는 항상 SP 네트워크 인터페이스를 사용하여 업데이트합니다.

관련 정보

"NetApp 다운로드: 시스템 펌웨어 및 진단"

클러스터 사용자 계정을 사용하여 **ONTAP** 서비스 프로세서에 액세스합니다

SP에 액세스하려고 하면 자격 증명을 묻는 메시지가 표시됩니다. '서비스 프로세서' 애플리케이션 유형으로 생성된 클러스터 사용자 계정은 클러스터의 모든 노드에서 SP CLI에 액세스할 수 있습니다. SP 사용자 계정은 ONTAP에서 관리되며 암호로 인증됩니다. ONTAP 9.9.1부터 SP 사용자 계정에는 admin 역할이 있어야 합니다.

SP에 액세스하기 위한 사용자 계정은 SP CLI 대신 ONTAP에서 관리됩니다. 'security login create' 명령의 '-application' 매개 변수를 'service-processor'로 설정하고 '-AuthMethod' 매개 변수를 'password'로 설정하면 클러스터 사용자 계정이 SP에 액세스할 수 있습니다. SP는 암호 인증만 지원합니다.

SP 사용자 계정을 생성할 때 '-role' 매개 변수를 지정해야 합니다.

- ONTAP 9.9.1 이상 릴리즈에서는 '-role' 매개 변수에 admin을 지정해야 하며, 계정을 수정하려면 "admin" 역할이 필요합니다. 다른 역할은 더 이상 보안상의 이유로 허용되지 않습니다.
  - ONTAP 9.9.1 이상 릴리즈로 업그레이드하는 경우 을 참조하십시오 "서비스 프로세서에 액세스할 수 있는 사용자 계정의 변경".
  - ONTAP 9.8 이전 릴리즈로 되돌리는 경우 를 참조하십시오 "서비스 프로세서에 액세스할 수 있는 사용자 계정을 확인합니다".
- ONTAP 9.8 및 이전 릴리즈에서는 모든 역할이 SP에 액세스할 수 있지만 admin을 사용하는 것이 좋습니다.

기본적으로 admin이라는 클러스터 사용자 계정에는 서비스 프로세서 애플리케이션 유형이 포함되며 SP에 액세스할 수 있습니다.

ONTAP는 시스템에 예약된 이름을 가진 사용자 계정(""root" 및 ""naroot"" 등)을 만들지 못하도록 합니다. 시스템 예약 이름을 사용하여 클러스터 또는 SP에 액세스할 수 없습니다.

보안 로그인 show 명령어의 '-application service-processor' 파라미터를 사용하면 현재 SP 사용자 계정을 표시할 수 있다.

에 대한 자세한 내용은 `security login show` "ONTAP 명령 참조입니다"을 참조하십시오.

관리 호스트에서 노드의 **ONTAP SP/BMC**에 액세스합니다

관리 호스트에서 노드의 SP에 로그인하여 노드 관리 작업을 원격으로 수행할 수 있습니다.

시작하기 전에

다음 조건을 충족해야 합니다.

- SP에 액세스하는 데 사용하는 관리 호스트는 SSHv2를 지원해야 합니다.
- SP에 액세스할 수 있도록 사용자 계정이 이미 설정되어 있어야 합니다.

  SP에 액세스하려면 'secervice-processor'로 설정된 'security login create' 명령의 '-application' 매개 변수와 'password'로 설정된 '-AuthMethod' 매개 변수를 사용하여 사용자 계정을 생성해야 합니다.

이 태스크는 SP와 BMC 모두에 적용됩니다.

SP가 IPv4 또는 IPv6 주소를 사용하도록 구성되어 있고 호스트에서 5번의 SSH 로그인 시도가 10분 이내에 연속으로 실패하면 SP는 SSH 로그인 요청을 거부하고 호스트의 IP 주소와의 통신을 15분 동안 일시 중단합니다. 15분 후에 통신이 다시 시작되고 SP에 다시 로그인할 수 있습니다.

ONTAP는 클러스터 또는 SP에 액세스하기 위해 시스템 예약 이름("루트" 및 ""naroot" 등)을 생성하거나 사용하는 것을 방지합니다.

단계

1. 관리 호스트에서 SP에 로그인합니다.

   '* ssh 사용자 이름@sp_ip_address *'

2. 메시지가 나타나면 사용자 이름 비밀번호를 입력합니다.

   SP 프롬프트가 나타나고 SP CLI에 액세스할 수 있음을 나타냅니다.

관리 호스트의 **SP** 액세스 예

다음 예에서는 SP에 액세스하도록 설정된 사용자 계정 "Joe"를 사용하여 SP에 로그인하는 방법을 보여 줍니다.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

다음 예에서는 IPv6 글로벌 주소 또는 IPv6 라우터 알림 주소를 사용하여 IPv6에 대해 SSH가 설정되어 있고 IPv6에 대해 SP가 구성된 노드에서 SP에 로그인하는 방법을 보여 줍니다.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

시스템 콘솔에서 노드의 **ONTAP SP/BMC**에 액세스합니다

시스템 콘솔(_serial console_이라고도 함)에서 SP에 액세스하여 모니터링 또는 문제 해결 작업을 수행할 수 있습니다.

이 작업에 대해

이 태스크는 SP와 BMC 모두에 적용됩니다.

단계

1. 프롬프트에서 Ctrl+G를 눌러 시스템 콘솔에서 SP CLI에 액세스합니다.
2. 프롬프트가 표시되면 SP CLI에 로그인합니다.

   SP 프롬프트가 나타나고 SP CLI에 액세스할 수 있음을 나타냅니다.

3. SP CLI를 종료하고 Ctrl+D를 눌러 시스템 콘솔로 돌아온 다음, Enter 키를 누릅니다.

시스템 콘솔에서 **SP CLI**에 액세스하는 예

다음 예에서는 시스템 콘솔에서 Ctrl-G를 눌러 SP CLI에 액세스한 결과를 보여 줍니다. SP 프롬프트에서 "help system power" 명령을 입력한 다음 Ctrl+D를 누르고 Enter를 눌러 시스템 콘솔로 돌아갑니다.

```
cluster1::>
```

(SP CLI에 액세스하려면 Ctrl-G를 누릅니다.)

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

(Ctrl-D를 누른 다음 Enter 키를 눌러 시스템 콘솔로 돌아갑니다.)

```
cluster1::>
```

ONTAP SP CLI, SP 콘솔 및 시스템 콘솔 세션이 어떻게 관련되어 있는지 알아보십시오

SP CLI 세션을 열어 노드를 원격으로 관리하고 별도의 SP 콘솔 세션을 열어 노드 콘솔에 액세스할 수 있습니다. SP 콘솔 세션은 동시 시스템 콘솔 세션에 표시되는 출력을 미러링합니다. SP와 시스템 콘솔에는 독립 로그인 인증이 있는 독립 셸 환경이 있습니다.

SP CLI, SP 콘솔 및 시스템 콘솔 세션의 연결 방식을 이해하면 노드를 원격으로 관리하는 데 도움이 됩니다. 다음은 세션 간의 관계에 대해 설명합니다.

- 한 번에 하나의 관리자만 SP CLI 세션에 로그인할 수 있지만 SP를 사용하면 SP CLI 세션과 별도의 SP 콘솔 세션을 동시에 열 수 있습니다.

  SP CLI는 SP 프롬프트('S>')로 표시됩니다. SP CLI 세션에서 SP의 system console 명령을 사용하여 SP 콘솔 세션을 시작할 수 있습니다. 동시에 SSH를 통해 별도의 SP CLI 세션을 시작할 수 있습니다. Ctrl+D를 눌러 SP 콘솔 세션을 종료하면 SP CLI 세션으로 자동으로 돌아갑니다. SP CLI 세션이 이미 있는 경우 기존 SP CLI 세션을 종료할지 묻는 메시지가 표시됩니다. ""y""를 입력하면 기존 SP CLI 세션이 종료되므로 SP 콘솔에서 SP CLI로 돌아갈 수 있습니다. 이 작업은 SP 이벤트 로그에 기록됩니다.

  SSH를 통해 연결된 ONTAP CLI 세션에서 다른 노드의 ONTAP 'system node run-console' 명령을 실행하여 노드의 시스템 콘솔로 전환할 수 있습니다.

- 보안상의 이유로 SP CLI 세션과 시스템 콘솔 세션에는 서로 독립적인 로그인 인증이 있습니다.

  SP CLI에서 SP 콘솔 세션을 시작할 때(SP의 'system console' 명령 사용) 시스템 콘솔 자격 증명을 묻는 메시지가 표시됩니다. Ctrl+G를 눌러 시스템 콘솔 세션에서 SP CLI에 액세스하면 SP CLI 자격 증명을 묻는 메시지가 표시됩니다.

- SP 콘솔 세션과 시스템 콘솔 세션에는 독립적인 셸 환경이 있습니다.

  SP 콘솔 세션은 동시 시스템 콘솔 세션에 표시되는 출력을 미러링합니다. 하지만 동시 시스템 콘솔 세션은 SP 콘솔 세션을 미러링하지 않습니다.

  SP 콘솔 세션은 동시 SSH 세션의 출력을 미러링하지 않습니다.

관리 호스트 **IP** 주소를 추가하여 **ONTAP** 서비스 프로세서에 액세스합니다

기본적으로 SP는 모든 IP 주소의 관리 호스트에서 SSH 연결 요청을 수락합니다. 지정한 IP 주소가 있는 관리 호스트에서만 SSH 연결 요청을 허용하도록 SP를 구성할 수 있습니다. 변경 사항은 클러스터에 있는 노드의 SP에 대한 SSH 액세스에 적용됩니다.

단계

1. 'system service-processor ssh add-allowed-addresses' 명령어를 사용한 '-allowed-addresses' 파라미터로 지정한 IP 주소만 SP에 대한 액세스를 부여한다.
   - '-allowed-addresses' 파라미터의 값은 'address'/'netmask' 형식으로 지정해야 하며, 여러

'address'/'netmask' 쌍의 값은 콤마로 구분되어야 합니다(예: 10.98.150.10/24, FD20:8b1e:B255:c09b:/64).

'-allowed-addresses' 매개 변수를 '0.0.0.0/0,:/0'으로 설정하면 모든 IP 주소가 SP(기본값)에 액세스할 수 있습니다.

- SP 액세스를 지정한 IP 주소로만 제한하여 기본값을 변경하면 ONTAP에서 지정된 IP 주소가 ""모두 허용"" 기본 설정('0.0.0.0/0,:/0')을 대체할지 묻는 메시지를 표시합니다.
- 'system service-processor ssh show' 명령은 SP를 액세스할 수 있는 IP 주소를 표시합니다.

2. 지정된 IP 주소가 SP에 액세스하지 못하도록 차단하려면 시스템 service-processor ssh remove-allowed-addresses 명령을 -allowed-addresses 매개변수와 함께 사용하십시오.

   모든 IP 주소가 SP에 액세스하지 못하도록 차단하면 관리 호스트에서 SP에 액세스할 수 없게 됩니다.

SP에 액세스할 수 있는 **IP** 주소 관리의 예

다음 예에서는 SP에 대한 SSH 액세스에 대한 기본 설정을 보여 주고, SP 액세스를 지정된 IP 주소로만 제한하고, 액세스 목록에서 지정된 IP 주소를 제거한 다음, 모든 IP 주소에 대해 SP 액세스를 복구하여 기본값을 변경합니다.

```
cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
         with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
         addresses will be denied access. To restore the "allow all"
default,
         use the "system service-processor ssh add-allowed-addresses
         -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
          {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0
```

ONTAP SP/BMC CLI에서 도움말 정보를 봅니다

온라인 도움말에는 SP/BMC CLI 명령 및 옵션이 표시됩니다.

이 작업에 대해

이 태스크는 SP와 BMC 모두에 적용됩니다.

단계

1. SP/BMC 명령에 대한 도움말 정보를 표시하려면 다음을 입력합니다.

SP 도움말을 액세스하려면…	**BMC** 도움말에 액세스하려면…
SP 프롬프트에 help를 입력합니다.	BMC 프롬프트에 '시스템'을 입력합니다.

다음 예는 SP CLI 온라인 도움말을 보여 줍니다.

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

다음 예에서는 BMC CLI 온라인 도움말을 보여 줍니다.

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

2. SP/BMC 명령 옵션에 대한 도움말 정보를 표시하려면 SP/BMC 명령 앞이나 뒤에 "help"를 입력합니다.

   다음 예에서는 SP 'events' 명령에 대한 SP CLI 온라인 도움말을 보여 줍니다.

```
SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events
```

다음 예에서는 BMC '시스템 전원' 명령에 대한 BMC CLI 온라인 도움말을 보여 줍니다.

```
BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>
```

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

관련 정보

- "이벤트"
- "시스템 전원"

원격 노드 관리를 위한 **ONTAP** 명령

SP 에 액세스하여 SP CLI 명령을 실행하거나 BMC 에 액세스하여 BMC CLI 명령을 실행하여 원격으로 노드 관리 작업을 수행할 수 있습니다. 일반적으로 수행되는 여러 원격 노드 관리 작업의 경우 클러스터의 다른 노드에서 ONTAP 명령을 사용할 수도 있습니다. 일부 SP 및 BMC 명령은 플랫폼에 따라 다르므로 사용자 플랫폼에서 사용하지 못할 수 있습니다.

특정 명령 유형은 SP 와 BMC 명령 세트 모두에서 사용할 수 있습니다. 명령줄에 입력하면 두 가지의 차이점이 표시됩니다.

예

- 그만큼 `help` SP 의 명령: `SP> help`
- 그만큼 `help` BMC 의 명령: `BMC> help`

자세히 알아보세요 `help` SP 및 BMC 에 사용 가능한 명령 옵션"ONTAP SP/BMC CLI에서 도움말 정보를 봅니다" .

해당 ONTAP BMC CLI에 대해 자세히 알아보세요."ONTAP 베이스보드 관리 컨트롤러에 대해 지원되는 CLI 명령" .

원하는 작업	이 **SP** 명령 사용…	이 **BMC** 명령 사용…	이 **ONTAP** 명령을 사용하세요…
SP/ BMC/ ONTAP 에 대해 지정된 명령의 사용 가능한 명령 또는 하위 명령을 표시합니다.	도움말 ['명령']	도움말 ['명령']	해당 없음
SP/ BMC/ ONTAP CLI에 대한 현재 권한 수준을 표시합니다.	'한자 쇼'	`priv show`	해당 없음
SP/ BMC/ ONTAP CLI에 대해 지정된 모드에 액세스하기 위한 권한 수준을 설정합니다.	`priv set` {admin	`advanced`	`diag }`
`priv set` {admin	`advanced`	`diag`	`test }`
해당 없음	시스템 날짜 및 시간을 표시합니다	다	다
다	SP/ BMC/ ONTAP 에서 기록한 이벤트를 표시합니다.	`events` {all	`info`
`newest number`	`oldest number`	`search keyword }`	`events` {all
`info`	`newest`	`oldest`	`search }`
해당 없음	SP/ BMC/ ONTAP 상태 및 네트워크 구성 정보 표시	`sp status` [-v	`-d ]` * 그만큼 `-v` 이 옵션은 SP 통계를 자세한 형식으로 표시합니다. * 그만큼 `-d` 이 옵션을 선택하면 SP 디버그 로그가 디스플레이에 추가됩니다.
`bmc status` [-v	`-d ]` * 그만큼 `-v` 이 옵션은 SP 통계를 자세한 형식으로 표시합니다. * 그만큼 `-d` 이 옵션을 선택하면 SP 디버그 로그가 디스플레이에 추가됩니다.	'시스템 서비스 프로세서 쇼'	SP/ BMC/ ONTAP 이 작동한 시간과 지난 1분, 5분, 15분 동안 실행 대기열에 있는 작업의 평균 수를 표시합니다.

원하는 작업	이 **SP** 명령 사용…	이 **BMC** 명령 사용…	이 **ONTAP** 명령을 사용하세요…
'가동 시간'	BMC 가동 시간	해당 없음	시스템 콘솔 로그를 표시합니다
'시스템 로그'	'시스템 로그' [-a]	'시스템 로그' (시스템 콘솔 로그를 인쇄합니다)	SP/ BMC/ ONTAP 로그 아카이브 또는 아카이브의 파일을 표시합니다.
`sp log history show` [-archive {latest	{all	archive-name }][-dump {all	file-name }]
`bmc log history show` [-archive {latest	{all	archive-name }][-dump {all	file-name }]
해당 없음	노드의 컨트롤러에 대한 전원 상태를 표시합니다	시스템 전원 상태	시스템 전원 상태
'시스템 노드 파워쇼	배터리 정보를 표시합니다	'시스템 배터리 쇼'	'시스템 배터리 쇼'
해당 없음	ACP 정보 또는 확장기 센서의 상태를 표시합니다	`system acp` [show	`sensors show`]
해당 없음	해당 없음	모든 시스템 FRU 및 해당 ID를 나열합니다	'시스템 FRU 목록'
'시스템 FRU 목록'	해당 없음	지정된 FRU에 대한 제품 정보를 표시합니다	시스템 FRU 쇼 FRU_id
`system fru show` [`show <id>`]	해당 없음	FRU 데이터 기록 로그를 표시합니다	`system fru log show` (고급 권한 레벨)

`system fru log show`	해당 없음	환경 센서의 상태 및 현재 값을 포함한 상태를 표시합니다	`system sensors`
			
			또는
			
			`system sensors show`

원하는 작업	이 **SP** 명령 사용…	이 **BMC** 명령 사용…	이 **ONTAP** 명령을 사용하세요…
`system sensors` {show	`filter <sensor_string>}`	시스템 노드 환경 센서가 표시됩니다	지정된 센서의 상태 및 세부 정보를 표시합니다
'시스템 센서에는 'sensor_name'이 있습니다 'system sensors' 또는 'system sensors show' 명령을 사용하면 'sensor_name'을 얻을 수 있습니다.	`system sensors` [`get`]	해당 없음	SP/ BMC/ ONTAP 펌웨어 버전 정보 표시
'내전'	'내전'	'시스템 서비스 프로세서 이미지 쇼'	SP/ BMC/ ONTAP 명령 내역 표시
`sp log audit` (고급 권한 레벨)	BMC 로그 감사 (고급 권한 레벨)	해당 없음	SP/ BMC/ ONTAP 디버그 정보 표시
`sp log debug` (고급 권한 레벨)	`bmc log debug` (고급 권한 레벨)	해당 없음	SP/ BMC/ ONTAP 메시지 파일 표시
`sp log messages` (고급 권한 레벨)	`bmc log messages` (고급 권한 레벨)	해당 없음	감시 재설정 이벤트에서 시스템 조사 정보를 수집하거나, 감시 재설정 이벤트 중에 수집된 시스템 조사 정보를 표시하거나, 수집된 시스템 조사 정보를 지우는 설정을 표시합니다
`system forensics` [show	`log dump`	`log clear`]	해당 없음
해당 없음	시스템 콘솔에 로그인합니다	시스템 콘솔	시스템 콘솔
'시스템 노드 실행 콘솔	시스템 콘솔 세션을 종료하려면 Ctrl+D를 눌러야 합니다.	노드 켜기/끄기 또는 전원 끄기(전원 끄기 후 다시 켜기)	'시스템 파워' 켜기

원하는 작업	이 **SP** 명령 사용…	이 **BMC** 명령 사용…	이 **ONTAP** 명령을 사용하세요…
'시스템 파워' 켜기	`system node power on` (고급 권한 레벨)	'시스템 전원' OFF	'시스템 전원' OFF
해당 없음	'시스템 파워' 사이클	'시스템 파워' 사이클	해당 없음
SP를 중단 없이 계속 실행하기 위해 대기 전원이 계속 켜져 있습니다. 전원을 껐다 켜는 동안 전원이 다시 켜지기 전에 잠시 멈춥니다. 이러한 명령을 사용하여 노드를 끄거나 전원을 껐다 켜면 노드가 부적절하게 종료될 수 있으며(*dirty shutdown* 이라고도 함) ONTAP 'system node halt' 명령을 사용하여 정상적인 종료를 대신할 수 없습니다.	코어 덤프를 생성하고 노드를 재설정합니다	'시스템 코어'['-f''] '-f' 옵션은 코어 덤프의 생성과 노드 재설정을 강제합니다.	`system core`

원하는 작업	이 **SP** 명령 사용…	이 **BMC** 명령 사용…	이 **ONTAP** 명령을 사용하세요…
시스템 노드 코어 덤프 트리거 (고급 권한 레벨)	이러한 명령은 노드의 NMI(Non-Maskable Interrupt) 단추를 눌러 노드를 중단할 때 노드가 비정상적으로 종료되고 코어 파일의 덤프를 수행하는 것과 동일한 효과를 가집니다. 이러한 명령은 노드의 ONTAP가 중단되거나 '시스템 노드 종료' 같은 명령에 응답하지 않는 경우에 유용합니다. 생성된 core dump 파일은 system node coredump show 명령의 출력에 출력된다. SP는 노드에 대한 입력 전원이 중단되지 않는 한 작동 가능한 상태를 유지합니다.	선택적으로 지정된 BIOS 펌웨어 이미지(기본, 백업 또는 현재)를 사용하여 노드를 재부팅하여 노드 부팅 장치의 손상된 이미지와 같은 문제를 복구합니다	`system reset` {`primary`
`backup`	`current` }	`system reset` { `current`	`primary`
`backup` }	`system node reset`와 함께 `-firmware` {`primary`	`backup`	`current` } 매개변수 (고급 권한 레벨)
이 작업으로 인해 노드가 비정상 종료됩니다. BIOS 펌웨어 이미지를 지정하지 않으면 현재 이미지가 재부팅에 사용됩니다. SP는 노드에 대한 입력 전원이 중단되지 않는 한 작동 가능한 상태를 유지합니다.	현재 배터리 펌웨어 이미지를 지정된 펌웨어 이미지와 비교합니다	'시스템 배터리 확인'['IMAGE_URL'] (고급 권한 레벨) IMAGE_URL을 지정하지 않으면 기본 배터리 펌웨어 이미지가 비교용으로 사용됩니다.	'시스템 배터리 확인'['IMAGE_URL'] (고급 권한 레벨) IMAGE_URL을 지정하지 않으면 기본 배터리 펌웨어 이미지가 비교용으로 사용됩니다.

원하는 작업	이 **SP** 명령 사용…	이 **BMC** 명령 사용…	이 **ONTAP** 명령을 사용하세요…
해당 없음	지정된 위치의 이미지에서 배터리 펌웨어를 업데이트합니다	`system battery flash [image_URL]` (고급 권한 레벨) 어떤 이유로 자동 배터리 펌웨어 업그레이드 프로세스가 실패한 경우 이 명령을 사용합니다.	해당 없음

해당 없음	지정된 위치의 이미지를 사용하여 SP/ BMC/ ONTAP 펌웨어를 업데이트합니다.	`sp update`
		
		`image_URL`
		
		`image_URL`200자를 초과할 수 없습니다.
			`bmc update`
			
			`image_URL`
			
			`image_URL`200자를 초과할 수 없습니다.

'시스템 서비스 프로세서 이미지 업데이트	SP/ BMC/ ONTAP 재부팅	'재부팅'	`bmc reboot`
'시스템 서비스 프로세서 재부팅 - SP'	NVRAM 플래시 콘텐츠를 지웁니다	`system nvram flash clear` (고급 권한 레벨) 컨트롤러 전원이 꺼진 경우('시스템 전원 꺼짐') 이 명령을 시작할 수 없습니다.	해당 없음
해당 없음	SP/ BMC/ ONTAP CLI를 종료합니다.	종료	종료

관련 정보

- "ONTAP 명령 참조입니다"

임계값 기반 **SP** 센서 판독 및 상태를 사용하여 **ONTAP** 노드 상태 모니터링

임계값 기반 센서는 다양한 시스템 구성 요소의 판독값을 주기적으로 읽습니다. SP는 임계값 기반 센서의 판독값을 구성 요소의 허용 가능한 작동 조건을 정의하는 사전 설정된 임계값 제한과 비교합니다.

센서에서 읽은 정보를 기반으로 SP는 사용자가 해당 구성 요소의 상태를 모니터링할 수 있도록 센서 상태를 표시합니다.

임계값 기반 센서의 예로 시스템 온도 센서, 전압 센서, 전류 센서 및 팬 속도 센서가 있습니다. 특정 임계값 기반 센서 목록은 플랫폼에 따라 다릅니다.

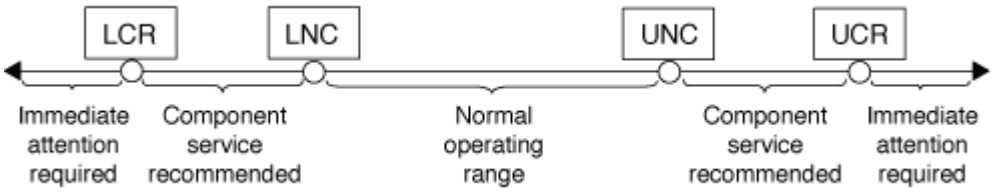
임계값 기반 센서의 경우 SP 'system sensors' 명령의 출력에 표시되는 임계값은 다음과 같습니다.

- 하한 위험(LCR)
- 하한 비위험(LNC)
- 상한 비위험(UNC)
- 상한 위험(UCR)

센서 상태가 LNC와 LCR 사이이거나 UNC와 UCR 사이일 경우, 해당 구성 요소에 문제의 징후가 있고 그 결과 시스템 장애가 발생할 수 있음을 나타냅니다. 따라서 빨리 구성 요소 서비스 계획을 세워야 합니다.

센서 상태가 LCR보다 낮거나 UCR보다 높을 경우 해당 구성 요소가 오작동 중이며 시스템 장애가 곧 발생할 수 있음을 나타냅니다. 따라서 구성 요소에 즉각적인 주의가 필요합니다.

다음 다이어그램에서는 임계값에 의해 지정된 심각도 범위를 보여 줍니다.



'시스템 센서' 명령 출력의 Current' 열에서 임계값 기반 센서의 판독값을 확인할 수 있습니다. 시스템 센서의 get' sensor_name' 명령은 지정된 센서에 대한 추가 세부 정보를 표시합니다. 임계값 기반 센서의 판독값이 비위험 임계값 범위와 임계 임계값 범위를 넘어가면 센서에서 심각도가 증가하는 문제를 보고합니다. 값이 임계값 제한을 초과하면 '시스템 센서' 명령 출력의 센서 상태가 'ok'에서 'nc'(비위험) 또는 'cr'(위험)로 변경되고 이벤트 메시지가 SEL 이벤트 로그에 기록됩니다.

일부 임계값 기반 센서의 경우 네 가지 임계값 중 일부가 없습니다. 이러한 센서의 경우 누락된 임계값은 '시스템 센서' 명령 출력에서 해당 제한값으로 'na'가 표시됩니다. 이는 특정 센서의 임계값 관련 제한이나 심각도가 없고 SP가 센서에서 해당 임계값을 모니터링하지 않음을 나타냅니다.

시스템 센서 명령 출력의 예

다음 예제는 SP CLI에서 'system sensors' 명령으로 표시되는 일부 정보를 보여 줍니다.

```
SP node1> system sensors

Sensor Name       | Current    | Unit        | Status| LCR        | LNC
| UNC        | UCR
------------------+------------+-------------+-------+------------+
-----------+-----------+-----------
CPU0_Temp_Margin | -55.000    | degrees C   | ok    | na         | na
| -5.000     | 0.000
CPU1_Temp_Margin | -56.000    | degrees C   | ok    | na         | na
| -5.000     | 0.000
In_Flow_Temp      | 32.000     | degrees C   | ok    | 0.000      | 10.000
| 42.000     | 52.000
Out_Flow_Temp     | 38.000     | degrees C   | ok    | 0.000      | 10.000
| 59.000     | 68.000
CPU1_Error        | 0x0        | discrete    | 0x0180| na         | na
| na         | na
CPU1_Therm_Trip   | 0x0        | discrete    | 0x0180| na         | na
| na         | na
CPU1_Hot          | 0x0        | discrete    | 0x0180| na         | na
| na         | na
IO_Mid1_Temp      | 30.000     | degrees C   | ok    | 0.000      | 10.000
| 55.000     | 64.000
IO_Mid2_Temp      | 30.000     | degrees C   | ok    | 0.000      | 10.000
| 55.000     | 64.000
CPU_VTT           | 1.106      | Volts       | ok    | 1.028      | 1.048
| 1.154      | 1.174
CPU0_VCC          | 1.154      | Volts       | ok    | 0.834      | 0.844
| 1.348      | 1.368
3.3V              | 3.323      | Volts       | ok    | 3.053      | 3.116
| 3.466      | 3.546
5V                | 5.002      | Volts       | ok    | 4.368      | 4.465
| 5.490      | 5.636
STBY_1.8V         | 1.794      | Volts       | ok    | 1.678      | 1.707
| 1.892      | 1.911
…
```

임계값 기반 센서에 대한 **system sensors sensor_name** 명령 출력의 예

다음 예제는 임계값 기반 센서 5V에 대해 SP CLI에서 시스템 센서의 get' sensor_name을 입력한 결과를 보여줍니다.

```
SP node1> system sensors get 5V

Locating sensor record...
Sensor ID               : 5V (0x13)
 Entity ID              : 7.97
 Sensor Type (Analog)   : Voltage
 Sensor Reading         : 5.002 (+/- 0) Volts
 Status                 : ok
 Lower Non-Recoverable  : na
 Lower Critical         : 4.246
 Lower Non-Critical     : 4.490
 Upper Non-Critical     : 5.490
 Upper Critical         : 5.758
 Upper Non-Recoverable  : na
 Assertion Events       :
 Assertions Enabled     : lnc- lcr- ucr+
 Deassertions Enabled   : lnc- lcr- ucr+
```

시스템 센서 명령 출력의 **ONTAP SP** 센서 상태 값입니다

개별 센서에는 임계값이 없습니다. SP CLI의 system sensors 명령 출력에서 Current 열 아래에 표시되는 이 값은 실제 의미가 없으므로 SP에서 무시됩니다. '시스템 센서' 명령어 출력의 '상태' 열에는 개별 센서의 상태 값이 16진수 형식으로 표시됩니다.

개별 센서의 예로 팬 센서, 전원 공급 장치(PSU) 장애 센서 및 시스템 장애 센서가 있습니다. 개별 센서의 특정 목록은 플랫폼에 따라 다릅니다.

대부분의 개별 센서의 상태 값을 해석하는 데 도움이 되도록 SP CLI의 시스템 센서의 get ' sensor_name ' 명령을 사용할 수 있습니다. 다음 예는 개별 센서 CPU0_Error 및 IO_Slot1_Present에 대한 시스템 센서의 get' sensor_name을 입력한 결과를 보여줍니다.

```
SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID               : CPU0_Error (0x67)
 Entity ID              : 7.97
 Sensor Type (Discrete): Temperature
 States Asserted        : Digital State
                          [State Deasserted]
```

```
SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID               : IO_Slot1_Present (0x74)
 Entity ID              : 11.97
 Sensor Type (Discrete): Add-in Card
 States Asserted        : Availability State
                          [Device Present]
```

'system sensor_name' 명령은 대부분의 개별 센서의 상태 정보를 표시하지만 System_FW_Status, System_Watchdog, PSU1_Input_Type 및 PSU2_Input_Type 개별 센서의 상태 정보는 제공하지 않습니다. 다음 정보를 사용하여 이러한 센서의 상태 값을 해석할 수 있습니다.

System_FW_Status를 선택합니다

System_FW_Status 센서의 상태는 0xAABB 형태로 나타납니다. AA와 BB의 정보를 조합하여 센서의 상태를 확인할 수 있습니다.

AA는 다음 값 중 하나일 수 있습니다.

값	센서의 상태입니다
01	시스템 펌웨어 오류입니다
02	시스템 펌웨어가 중단됩니다
04	시스템 펌웨어 진행률이 표시됩니다

BB는 다음 값 중 하나일 수 있습니다.

값	센서의 상태입니다
00	시스템 소프트웨어가 올바르게 종료되었습니다
01	메모리 초기화가 진행 중입니다
02	NVMEM 초기화 진행 중(NVMEM이 있을 경우)
04	메모리 컨트롤러 허브(MCH) 값 복원(NVMEM이 있을 경우)
05	사용자가 설치를 시작했습니다
13	운영 체제 또는 로더 부팅 중
1F	BIOS가 시작하는 중입니다

값	센서의 상태입니다
20	로더가 실행 중입니다
21	로더가 기본 BIOS 펌웨어를 프로그래밍하는 중입니다. 시스템 전원을 끄지 않아야 합니다.
22	로더가 대체 BIOS 펌웨어를 프로그래밍하는 중입니다. 시스템 전원을 끄지 않아야 합니다.
2F	ONTAP가 실행 중입니다
60	SP가 시스템 전원을 껐습니다
61	SP가 시스템의 전원을 켜왔습니다
62	SP가 시스템을 재설정했습니다
63	SP watchdog 전원 사이클
64	SP watchdog 콜드 리셋

예를 들어, System_FW_Status 센서 상태가 0x042F일 경우 "시스템 펌웨어 진행(04), ONTAP 실행 중(2F)"을 의미합니다.

System_Watchdog(시스템 감시 장치

System_Watchdog 센서는 다음 상태 중 하나일 수 있습니다.

- * 0x0080 *

  이 센서의 상태는 변경되지 않았습니다

값	센서의 상태입니다
0x0081	타이머 중단
0x0180	타이머가 만료되었습니다
0x0280	하드 리셋
0x0480	전원을 끕니다
0x0880)을 참조하십시오	전원을 껐다 켜십시오

예를 들어, System_Watchdog 센서 상태 0x0880은 watchdog 시간 초과가 발생하고 시스템의 전원 주기가 수행됨을 의미합니다.

PSU1_Input_Type 및 PSU2_Input_Type

직류(DC) 전원 공급 장치의 경우 PSU1_Input_Type 및 PSU2_Input_Type 센서가 적용되지 않습니다. 교류(AC) 전원 공급 장치의 경우 센서 상태는 다음 값 중 하나일 수 있습니다.

값	센서의 상태입니다
0x01 xx	220V PSU 유형
0x02 xx	110V PSU 유형

예를 들어 PSU1_Input_Type 센서 상태 0x0280은 PSU 유형이 110V임을 센서가 보고하는 것을 의미합니다.

서비스 프로세서 관리를 위한 **ONTAP** 명령

ONTAP에서는 SP 네트워크 구성, SP 펌웨어 이미지, SP에 대한 SSH 액세스, 일반 SP 관리를 비롯한 SP 관리를 위한 명령을 제공합니다.

SP 네트워크 구성을 관리하는 명령입니다

원하는 작업	이 **ONTAP** 명령 실행…
SP에서 지정된 서브넷의 IPv4 또는 IPv6 주소 제품군을 사용할 수 있도록 SP의 자동 네트워크 구성을 설정합니다	'system service-processor network auto-configuration enable
SP에 대해 지정된 서브넷의 IPv4 또는 IPv6 주소 제품군에 대한 SP 자동 네트워크 구성을 해제합니다	'system service-processor network auto-configuration disable
SP의 자동 네트워크 구성을 표시합니다	'system service-processor network auto-configuration show

원하는 작업	이 **ONTAP** 명령 실행…
다음을 포함하여 노드에 대해 SP 네트워크를 수동으로 구성합니다. • IP 주소 제품군(IPv4 또는 IPv6) • 지정된 IP 주소 제품군의 네트워크 인터페이스를 사용할지 여부를 나타냅니다 • IPv4를 사용하는 경우 DHCP 서버의 네트워크 구성을 사용할지 또는 지정하는 네트워크 주소를 사용할지 여부를 지정합니다 • SP의 공용 IP 주소입니다 • SP의 넷마스크(IPv4를 사용하는 경우) • SP에 대한 서브넷 마스크의 네트워크 접두사-길이(IPv6를 사용하는 경우) • SP의 게이트웨이 IP 주소입니다	'시스템 서비스 프로세서 네트워크 수정
다음을 포함하여 SP 네트워크 구성을 표시합니다. • 구성된 주소 패밀리(IPv4 또는 IPv6) 및 설정 여부 • 원격 관리 장치 유형입니다 • 현재 SP 상태 및 링크 상태입니다 • IP 주소, MAC 주소, 넷마스크, 서브넷 마스크의 접두사-길이, 라우터 할당 IP 주소, 링크 로컬 IP 주소 및 게이트웨이 IP 주소와 같은 네트워크 구성 • SP가 마지막으로 업데이트된 시간입니다 • SP 자동 구성에 사용되는 서브넷의 이름입니다 • IPv6 라우터 할당 IP 주소의 활성화 여부이다 • SP 네트워크 설정 상태입니다 • SP 네트워크 설정 실패 이유	'시스템 서비스 프로세서 네트워크 쇼' SP 네트워크 세부 정보를 모두 표시하려면 '-instance' 매개 변수가 필요합니다.
다음을 포함하여 SP API 서비스 구성을 수정합니다. • SP API 서비스에서 사용하는 포트를 변경하는 중입니다 • SP API 서비스 설정 또는 해제	'시스템 서비스 프로세서 API 서비스 수정 (고급 권한 레벨)
SP API 서비스 구성을 표시합니다	'시스템 서비스 프로세서 API 서비스 쇼' (고급 권한 레벨)

원하는 작업	이 **ONTAP** 명령 실행…
내부 통신을 위해 SP API 서비스에서 사용하는 SSL 및 SSH 인증서를 갱신합니다	• ONTAP 9.5 이상: '시스템 서비스 - 프로세서 API - 서비스 갱신 - 내부 - 인증서 • ONTAP 9.4 이하: '시스템 서비스 - 프로세서 API - 서비스 갱신 - 인증서' (고급 권한 레벨)

SP 펌웨어 이미지를 관리하는 명령입니다

원하는 작업	이 **ONTAP** 명령 실행…
다음을 포함하여 현재 설치된 SP 펌웨어 이미지의 세부 정보를 표시합니다. • 원격 관리 장치 유형입니다 • SP가 부팅되는 이미지(운영 또는 백업), 상태 및 펌웨어 버전 • 펌웨어 자동 업데이트의 활성화 여부와 마지막 업데이트 상태	'시스템 서비스 프로세서 이미지 쇼' '-is-current' 매개 변수는 설치된 펌웨어 버전이 최신 버전이 아닌 현재 SP가 부팅된 이미지(운영 또는 백업)를 나타냅니다.
SP 자동 펌웨어 업데이트를 사용하거나 사용하지 않도록 설정합니다	'시스템 서비스 프로세서 이미지 수정 기본적으로 SP 펌웨어는 ONTAP를 업데이트하거나 새로운 버전의 SP 펌웨어를 수동으로 다운로드할 때 자동으로 업데이트됩니다. 자동 업데이트를 사용하지 않도록 설정하면 ONTAP 이미지와 SP 펌웨어 이미지 간에 최적화되지 않은 또는 비정규화된 조합이 발생할 수 있으므로 사용하지 않는 것이 좋습니다.
노드에서 SP 펌웨어 이미지를 수동으로 다운로드합니다	'시스템 노드 이미지 가져오기' ⓘ 'system node image' 명령어를 실행하기 전에, 진행하라는 메시지가 나타나면, 권한 수준을 advanced('set-Privilege advanced')로 설정하고, * y * 를 입력해야 한다. SP 펌웨어 이미지는 ONTAP와 함께 패키지로 제공됩니다. ONTAP와 함께 제공된 것과 다른 SP 펌웨어 버전을 사용하려는 경우가 아니라면 SP 펌웨어를 수동으로 다운로드할 필요가 없습니다.

원하는 작업	이 **ONTAP** 명령 실행…
다음 정보를 포함하여 ONTAP에서 트리거된 최신 SP 펌웨어 업데이트의 상태를 표시합니다. • 최신 SP 펌웨어 업데이트의 시작 및 종료 시간입니다 • 업데이트가 진행 중인지 여부 및 완료율을 나타냅니다	'시스템 서비스 프로세서 이미지 업데이트 - 진행률 표시

SP에 대한 **SSH** 액세스를 관리하는 명령입니다

원하는 작업	이 **ONTAP** 명령 실행…
지정된 IP 주소에만 SP 액세스 권한을 부여합니다	'시스템 서비스 프로세서 ssh add-allowed-address'
지정된 IP 주소가 SP에 액세스하지 못하도록 차단합니다	'시스템 서비스 프로세서 ssh remove-allowed-address'
SP에 액세스할 수 있는 IP 주소를 표시합니다	'시스템 서비스 프로세서 ssh show'

일반 **SP** 관리를 위한 명령입니다

원하는 작업	이 **ONTAP** 명령 실행…
다음을 비롯한 일반 SP 정보를 표시합니다. • 원격 관리 장치 유형입니다 • 현재 SP 상태입니다 • SP 네트워크가 구성되었는지 여부를 나타냅니다 • 공용 IP 주소 및 MAC 주소와 같은 네트워크 정보 • SP 펌웨어 버전과 IPMI(Intelligent Platform Management Interface) 버전입니다 • SP 펌웨어 자동 업데이트가 설정되었는지 여부를 나타냅니다	'system service-processor show' SP의 전체 정보를 표시하려면 -instance 매개변수가 필요합니다.
노드에서 SP를 재부팅합니다	'시스템 서비스 프로세서 재부팅 - SP'
지정된 노드에서 수집된 SP 로그 파일을 포함하는 AutoSupport 메시지를 생성하고 전송합니다	'시스템 노드 AutoSupport invoke-splog'
각 수집 노드에 있는 SP 로그 파일의 시퀀스 번호를 포함하여 클러스터에서 수집된 SP 로그 파일의 할당 맵을 표시합니다	'시스템 서비스 프로세서 로그 show-allocaiton

관련 정보

"ONTAP 명령 참조입니다"

BMC 관리용 **ONTAP** 명령

이러한 ONTAP 명령은 베이스보드 관리 컨트롤러(BMC)에서 지원됩니다.

BMC는 서비스 프로세서(SP)와 동일한 명령 중 일부를 사용합니다. BMC에서 지원되는 SP 명령은 다음과 같습니다.

원하는 작업	이 명령을 사용합니다
BMC 정보를 표시합니다	'* 시스템 서비스 프로세서 쇼 * '
BMC 네트워크 구성을 표시/수정합니다	'* 시스템 서비스 프로세서 네트워크 표시/수정 * '
BMC를 재설정합니다	'* 시스템 서비스 프로세서 재부팅 - SP*'
현재 설치된 BMC 펌웨어 이미지의 세부 정보를 표시/수정합니다	'* 시스템 서비스 프로세서 이미지 표시/수정 * '
BMC 펌웨어를 업데이트합니다	'* 시스템 서비스 프로세서 이미지 업데이트 * '
최신 BMC 펌웨어 업데이트의 상태를 표시합니다	``시스템 서비스 프로세서 이미지 업데이트 - 진행률 표시*'
BMC가 지정된 서브넷에서 IPv4 또는 IPv6 주소를 사용할 수 있도록 자동 네트워크 구성을 활성화합니다	'* 시스템 서비스 프로세서 네트워크 자동 구성 활성화*'
BMC에 대해 지정된 서브넷의 IPv4 또는 IPv6 주소에 대한 자동 네트워크 구성을 비활성화합니다	'* 시스템 서비스 프로세서 네트워크 자동 구성 비활성화*'
BMC 자동 네트워크 구성을 표시합니다	'* 시스템 서비스 프로세서 네트워크 자동 구성 표시*'

BMC 펌웨어에서 지원하지 않는 명령의 경우 다음 오류 메시지가 반환됩니다.

```
::> Error: Command not supported on this platform.
```

관련 정보

- "시스템 서비스 - 프로세서"

ONTAP 베이스보드 관리 컨트롤러에 대해 지원되는 **CLI** 명령

SSH를 사용하여 BMC에 로그인할 수 있습니다. BMC 명령행에서 지원되는 명령은 다음과 같습니다.

명령	기능
시스템	모든 명령 목록을 표시합니다.

명령	기능
시스템 콘솔	시스템 콘솔에 연결합니다. 세션을 종료하려면 Ctrl+D를 사용합니다.
시스템 코어	시스템 코어를 덤프하고 재설정합니다.
시스템 전원을 껐다가 켭니다	시스템 전원을 껐다가 다시 켭니다.
시스템 전원을 끕니다	시스템 전원을 끕니다.
시스템 전원이 켜져 있습니다	시스템 전원을 켭니다.
시스템 전원 상태	시스템 전원 상태를 인쇄합니다.
시스템이 재설정되었습니다	시스템을 재설정합니다.
시스템 로그	시스템 콘솔 로그를 인쇄합니다
시스템 FRU 표시 [id]	모든/선택한 현장 교체 장치(FRU) 정보를 덤프합니다.

ONTAP 클러스터 시간 관리(클러스터 관리자만 해당)

클러스터 시간이 정확하지 않을 수 있습니다. ONTAP를 사용하여 클러스터에서 표준 시간대, 날짜 및 시간을 수동으로 설정할 수 있지만 클러스터 시간을 동기화하도록 NTP(네트워크 시간 프로토콜) 서버를 구성해야 합니다.

ONTAP 9.5부터 대칭 인증을 사용하여 NTP 서버를 구성할 수 있습니다.

NTP는 항상 활성화되어 있습니다. 하지만 클러스터가 외부 시간 소스와 동기화하기 위해서는 구성이 여전히 필요합니다. ONTAP를 사용하면 다음과 같은 방법으로 클러스터의 NTP 구성을 관리할 수 있습니다.

- 최대 10개의 외부 NTP 서버를 클러스터에 연결할 수 있습니다('클러스터 시간 서비스 NTP 서버 생성').
  - 시간 서비스의 이중화 및 품질을 위해 최소 3개의 외부 NTP 서버를 클러스터에 연결해야 합니다.
  - IPv4 또는 IPv6 주소 또는 정규화된 호스트 이름을 사용하여 NTP 서버를 지정할 수 있습니다.
  - 사용할 NTP 버전(v3 또는 v4)을 수동으로 지정할 수 있습니다.

    기본적으로 ONTAP는 지정된 외부 NTP 서버에 지원되는 NTP 버전을 자동으로 선택합니다.

  지정한 NTP 버전이 NTP 서버에 지원되지 않으면 시간 교환이 불가능합니다.

  - 고급 권한 수준에서는 클러스터와 연결된 외부 NTP 서버를 클러스터 시간을 수정 및 조정하기 위한 기본 시간 소스로 지정할 수 있습니다.
- 클러스터와 연결된 NTP 서버를 표시할 수 있습니다('cluster time-service ntp server show').

- 클러스터의 NTP 구성을 수정할 수 있습니다('cluster time-service NTP server modify').
- 외부 NTP 서버에서 클러스터를 연결 해제할 수 있습니다('클러스터 시간 서비스 NTP 서버 삭제').
- 고급 권한 수준에서는 클러스터와 연결된 모든 외부 NTP 서버('클러스터 시간 서비스 NTP 서버 재설정')를 지워 구성을 재설정할 수 있습니다.

클러스터를 결합하는 노드는 클러스터의 NTP 구성을 자동으로 채택합니다.

ONTAP에서는 NTP를 사용할 뿐만 아니라 클러스터 시간도 수동으로 관리할 수 있습니다. 이 기능은 오류가 있는 시간을 수정해야 하는 경우(예: 재부팅 후 노드의 시간이 크게 올바르지 않음) 유용합니다. 이 경우 NTP가 외부 시간 서버와 동기화될 때까지 클러스터에 대한 대략적인 시간을 지정할 수 있습니다. 수동으로 설정하는 시간은 클러스터의 모든 노드에 적용됩니다.

다음과 같은 방법으로 클러스터 시간을 수동으로 관리할 수 있습니다.

- 클러스터에서 시간대, 날짜 및 시간을 설정하거나 수정할 수 있습니다('클러스터 날짜 수정').
- 클러스터의 현재 시간대, 날짜 및 시간 설정을 표시할 수 있습니다('클러스터 날짜 표시').

> 작업 일정이 수동 클러스터 날짜 및 시간 변경에 맞게 조정되지 않습니다. 이러한 작업은 작업이 생성된 현재 클러스터 시간 또는 가장 최근에 실행된 작업을 기준으로 실행되도록 예약되어 있습니다. 따라서 클러스터 날짜 또는 시간을 수동으로 변경하는 경우 "job show" 및 "job history show" 명령을 사용하여 예약된 모든 작업이 요구 사항에 따라 대기열에 추가되고 완료되었는지 확인해야 합니다.

클러스터 시간을 관리하는 명령입니다

클러스터의 NTP 서버를 관리하기 위해 'cluster time-service ntp server' 명령어를 사용한다. 클러스터 날짜 명령을 사용하여 수동으로 클러스터 시간을 관리할 수 있습니다.

ONTAP 9.5부터 대칭 인증을 사용하여 NTP 서버를 구성할 수 있습니다.

다음 명령을 사용하여 클러스터의 NTP 서버를 관리할 수 있습니다.

원하는 작업	이 명령 사용...
대칭 인증 없이 클러스터를 외부 NTP 서버에 연결합니다	'cluster time-service ntp server create-server server_name
클러스터를 외부 NTP 서버와 ONTAP 9.5 이상에서 사용할 수 있는 대칭 인증으로 연결합니다	'cluster time-service ntp server create-server_ip_address-key-id key_id 'key_id'는 "cluster time-service ntp key'로 설정된 기존 공유 키를 참조해야 합니다.
기존 NTP 서버에 대칭 인증 사용 기존 NTP 서버는 필요한 키 ID를 추가하여 인증을 사용하도록 수정할 수 있습니다 ONTAP 9.5 이상에서 사용할 수 있습니다	'cluster time-service ntp server modify -server server_name -key-id key_id

원하는 작업	이 명령 사용...
대칭 인증을 사용하지 않도록 설정합니다	`cluster time-service ntp server modify -server server_name -is-authentication -enabled false`
공유 NTP 키를 구성합니다	'cluster time-service ntp key create-id shared_key_id-type shared_key_type-value shared_key_value' 공유 키는 ID로 참조됩니다. ID, 유형 및 값은 노드와 NTP 서버 모두에서 동일해야 합니다
클러스터와 연결된 NTP 서버에 대한 정보를 표시합니다	클러스터 시간 서비스 NTP 서버가 표시됩니다
클러스터와 연결된 외부 NTP 서버의 구성을 수정합니다	클러스터 시간 서비스 NTP 서버 수정
클러스터에서 NTP 서버를 해제합니다	클러스터 시간 서비스 NTP 서버 삭제
클러스터와의 모든 외부 NTP 서버 연결을 선택 취소하여 구성을 재설정합니다	클러스터 시간 서비스 NTP 서버 리셋 이 명령을 사용하려면 고급 권한 수준이 필요합니다.

다음 명령을 사용하면 클러스터 시간을 수동으로 관리할 수 있습니다.

원하는 작업	이 명령 사용...
시간대, 날짜 및 시간을 설정하거나 수정합니다	클러스터 날짜 수정
클러스터의 시간대, 날짜 및 시간 설정을 표시합니다	'클러스터 날짜 표시'

관련 정보

- "클러스터 날짜가 표시됩니다"
- "클러스터 날짜 수정"
- "클러스터 시간 - 서비스 NTP"
- "작업 표시"

배너 및 **MOTD** 관리

ONTAP 로그인 배너 및 오늘의 메시지 텍스트에 대해 자세히 알아보십시오

ONTAP를 사용하면 로그인 배너 또는 오늘의 메시지(MOTD)를 구성하여 클러스터 또는 SVM(스토리지 가상 머신)의 System Manager 및 CLI 사용자에게 관리 정보를 전달할 수

있습니다.

사용자에게 암호 등의 인증 프롬프트가 표시되기 전에 콘솔 세션(클러스터 액세스만 해당) 또는 SSH 세션(클러스터 또는 SVM 액세스를 위한)에 배너가 표시됩니다. 예를 들어, 배너를 사용하면 시스템에 로그인하려는 사람에게 다음과 같은 경고 메시지를 표시할 수 있습니다.

```
$ ssh admin@cluster1-01

This system is for authorized users only. Your IP Address has been logged.

Password:
```

MOTD는 사용자를 인증한 후 클러스터 셸 프롬프트가 나타나기 전에 콘솔 세션(클러스터 액세스만 해당) 또는 SSH 세션(클러스터 또는 SVM 액세스용)에 표시됩니다. 예를 들어 MOTD를 사용하여 인증된 사용자만 볼 수 있는 다음과 같은 환영 메시지 또는 정보 메시지를 표시할 수 있습니다.

```
$ ssh admin@cluster1-01

Password:

Greetings. This system is running ONTAP 9.0.
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015
from 10.72.137.28.
```

다음과 같은 방법으로 '보안 로그인 배너 수정' 또는 '보안 로그인 motd 수정' 명령을 사용하여 배너 또는 MOTD의 내용을 만들거나 수정할 수 있습니다.

- CLI를 대화형으로 사용하거나 대화형으로 사용하지 않고 배너 또는 MOTD에 사용할 텍스트를 지정할 수 있습니다.

  '-message' 또는 '-Uri' 매개 변수 없이 명령을 사용할 때 실행되는 대화형 모드에서는 메시지에 줄 끝(line end)이라고도 함)을 사용할 수 있습니다.

  메시지 문자열을 지정하기 위해 '-message' 매개 변수를 사용하는 비대화형 모드는 줄 바꿈을 지원하지 않습니다.

- 배너 또는 MOTD에 사용할 FTP 또는 HTTP 위치에서 콘텐츠를 업로드할 수 있습니다.
- 동적 콘텐츠를 표시하도록 MOTD를 구성할 수 있습니다.

  동적으로 표시되도록 MOTD를 구성할 수 있는 예는 다음과 같습니다.

  - 클러스터 이름, 노드 이름 또는 SVM 이름
  - 클러스터 날짜 및 시간입니다
  - 로그인한 사용자의 이름입니다
  - 클러스터의 모든 노드에서 사용자에 대한 마지막 로그인
  - 로그인 장치 이름 또는 IP 주소입니다
  - 운영 체제 이름입니다

◦ 소프트웨어 릴리스 버전

◦ 효과적인 클러스터 버전 문자열

배너는 동적 콘텐츠를 지원하지 않습니다. MOTD가 동적으로 생성된 콘텐츠를 에서 표시할 수 있도록 하는 데 사용할 수 있는 이스케이프 시퀀스와 에 대해 자세히 `security login motd modify`"ONTAP 명령 참조입니다" 알아보십시오.

클러스터 또는 SVM 레벨에서 배너 및 MOTD를 관리할 수 있습니다.

- 배너에는 다음과 같은 사실이 적용됩니다.
  - 배너 메시지가 정의되지 않은 모든 SVM에 대해 클러스터에 구성된 배너도 사용됩니다.
  - 각 SVM에 대해 SVM 레벨 배너를 구성할 수 있습니다.

    클러스터 레벨 배너가 구성된 경우 해당 SVM에 대한 SVM 레벨 배너에 의해 재정의됩니다.
- 다음 사항이 MOTD에 적용됩니다.
  - 기본적으로 클러스터에 구성된 MOTD도 모든 SVM에 대해 활성화됩니다.
  - 또한 SVM별로 MOTD를 구성할 수 있습니다.

    이 경우 SVM에 로그인하면 클러스터 레벨에 정의된 MOD와 SVM 레벨에서 정의된 MOD가 두 개 표시됩니다.
  - 클러스터 관리자가 SVM별로 클러스터 레벨 MOTD를 활성화 또는 비활성화할 수 있습니다.

    클러스터 관리자가 SVM에 대해 클러스터 레벨 MOTD를 비활성화하면 SVM에 로그인한 사용자에게 클러스터 레벨 MOTD가 표시되지 않습니다.

ONTAP 로그인 배너를 만듭니다

클러스터 또는 SVM에 액세스하려고 하는 사람에게 메시지를 표시하는 배너를 생성할 수 있습니다. 사용자에게 인증 프롬프트가 표시되기 전에 콘솔 세션(클러스터 액세스만 해당) 또는 SSH 세션(클러스터 또는 SVM 액세스를 위한)에 배너가 표시됩니다.

단계

1. 'Security login banner modify' 명령을 사용하여 클러스터나 SVM용 배너를 생성합니다.

원하는 작업	그러면...
한 줄인 메시지를 지정합니다	`<text>""` 매개변수를 사용하여 `-message` 텍스트를 지정합니다.
메시지에 줄 바꿈(줄 끝이라고도 함)을 포함합니다	'-message' 또는 '-Uri' 매개 변수 없이 명령을 사용하여 배너 편집을 위한 대화형 모드를 실행합니다.
배너에 사용할 위치에서 콘텐츠를 업로드합니다	'-Uri' 매개 변수를 사용하여 콘텐츠의 FTP 또는 HTTP 위치를 지정합니다.

배너의 최대 크기는 줄 바꿈을 포함하여 2,048바이트입니다.

'-Uri' 파라미터를 사용하여 만든 배너는 정적입니다. 소스 콘텐츠의 후속 변경 사항을 반영하기 위해 자동으로 새로 고쳐지지 않습니다.

클러스터에 대해 생성된 배너는 기존 배너가 없는 모든 SVM에 대해서도 표시됩니다. 이후에 SVM을 위해 생성된 배너는 해당 SVM을 위한 클러스터 레벨 배너보다 우선합니다. SVM에 대한 "-""" 큰따옴표 안에 하이픈을 사용하여 "-message" 매개 변수를 지정하면 SVM이 클러스터 레벨 배너를 사용하도록 재설정됩니다.

2. 'Security login banner show' 명령으로 배너를 표시하여 배너가 생성되었는지 확인한다.

   빈 문자열(""")로 '-message' 매개 변수를 지정하면 내용이 없는 배너가 표시됩니다.

   "-"로 "-message" 매개 변수를 지정하면 배너가 구성되지 않은 모든 (admin 또는 data) SVM이 표시됩니다.

배너 작성의 예

다음 예제에서는 비대화형 모드를 사용하여 ""cluster1" 클러스터에 대한 배너를 만듭니다.

```
cluster1::> security login banner modify -message "Authorized users only!"

cluster1::>
```

다음 예에서는 대화형 모드를 사용하여 SVM에 대한 배너를 `svm1` 생성합니다.

```
cluster1::> security login banner modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!


cluster1::>
```

다음 예제는 만들어진 배너를 표시합니다.

```
cluster1::> security login banner show
Vserver: cluster1
Message
-------------------------------------------------------------------------
---
Authorized users only!

Vserver: svm1
Message
-------------------------------------------------------------------------
---
The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>
```

관련 정보

- 배너 관리
- "보안 로그인 배너 수정"
- "보안 로그인 배너가 표시됩니다"

ONTAP 클러스터 및 **SVM** 레벨에 표시되는 배너 텍스트를 관리합니다

클러스터 또는 SVM 레벨에서 배너를 관리할 수 있습니다. 배너 메시지가 정의되지 않은 모든 SVM에 대해 클러스터에 구성된 배너도 사용됩니다. 이후에 SVM을 위해 생성된 배너는 해당 SVM을 위한 클러스터 배너보다 우선합니다.

선택

- 클러스터 레벨에서 배너 관리:

원하는 작업	그러면...
모든 로그인 세션에 표시할 배너를 만듭니다	클러스터 레벨 배너 설정: `security login banner modify -vserver <cluster_name> { [-message "text"]
[-uri <ftp_or_http_addr>] }`	모든(클러스터 및 SVM) 로그인의 배너를 제거합니다
배너를 빈 문자열(``)로 설정합니다. `security login banner modify -vserver * -message`	SVM 관리자가 생성한 배너를 재정의합니다

원하는 작업	그러면...
SVM 배너 메시지를 수정합니다. `security login banner modify -vserver <svm_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] }`

- SVM 레벨에서 배너 관리

  SVM 컨텍스트에서 지정할 `-vserver <svm_name>` 필요가 없습니다.

원하는 작업	그러면...
클러스터 관리자가 제공하는 배너를 SVM용 다른 배너로 재정의합니다	SVM을 위한 배너 생성: `security login banner modify -vserver <svm_name> { [-message "text"]
[-uri <ftp_or_http_addr>] }`	SVM에 대한 배너가 표시되지 않도록 클러스터 관리자가 제공하는 배너를 표시하지 않습니다
SVM 배너를 SVM용 빈 문자열로 설정합니다. `security login banner modify -vserver <svm_name> -message`	SVM에서 현재 SVM 레벨 배너를 사용하는 경우 클러스터 레벨 배너를 사용합니다

관련 정보

- "보안 로그인 배너 수정"

ONTAP 사용자를 위한 오늘의 메시지 텍스트를 만듭니다

MOTD(오늘의 메시지)를 생성하여 인증된 CLI 사용자에게 정보를 전달할 수 있습니다. MOTD는 사용자를 인증한 후 클러스터 셸 프롬프트가 나타나기 전에 콘솔 세션(클러스터 액세스만 해당) 또는 SSH 세션(클러스터 또는 SVM 액세스용)에 표시됩니다.

단계

1. 'security login mtd modify' 명령을 사용하여 클러스터 또는 SVM에 대한 MOTD를 생성합니다.

원하는 작업	그러면...
한 줄인 메시지를 지정합니다	텍스트를 지정하려면 "- message "[.code]""text"" 매개 변수를 사용합니다.
줄 바꿈 포함(줄 끝이라고도 함)	MOTD 편집을 위한 대화형 모드를 실행하려면 '-message' 또는 '-Uri' 매개 변수 없이 명령을 사용합니다.

원하는 작업	그러면...
MOTD에 사용할 위치에서 콘텐츠를 업로드합니다	'-Uri' 매개 변수를 사용하여 콘텐츠의 FTP 또는 HTTP 위치를 지정합니다.

MOTD의 최대 크기는 새 행을 포함하여 2,048바이트입니다.

`Security login motd modify` MOTD에서 동적으로 생성된 콘텐츠를 표시할 수 있도록 하는 데 사용할 수 있는 이스케이프 시퀀스에 대해 설명합니다.

'-Uri' 파라미터를 사용하여 만든 MOTD는 정적입니다. 소스 콘텐츠의 후속 변경 사항을 반영하기 위해 자동으로 새로 고쳐지지 않습니다.

클러스터를 위해 생성된 MOTD는 기본적으로 모든 SVM 로그인을 위해 표시되며, SVM 레벨의 MOTD를 통해 특정 SVM에 대해 별도로 생성할 수 있습니다. SVM에 대해 '-is-cluster-message-enabled' 매개 변수를 'false'로 설정하면 해당 SVM에 대해 클러스터 레벨 MOTD가 표시되지 않습니다.

2. MOTD를 'security login mott show' 명령으로 출력하여 생성했는지 확인한다.

   지정 `-message` 빈 문자열(``)이 있는 매개변수는 구성되지 않았거나 내용이 없는 MOTD를 표시합니다.

   MOTD가 동적으로 생성된 콘텐츠를 에서 표시할 수 있도록 하는 및 매개 변수에 대해 자세히 `security login motd modify`"ONTAP 명령 참조입니다" 알아보십시오.

MOD 작성의 예

다음 예제에서는 비대화형 모드를 사용하여 MOTD를 생성합니다. `cluster1` 무리:

```
cluster1::> security login motd modify -message "Greetings!"
```

다음 예제에서는 대화형 모드를 사용하여 MOTD를 생성합니다. `svm1` 동적으로 생성된 콘텐츠를 표시하기 위해 이스케이프 시퀀스를 사용하는 SVM:

```
cluster1::> security login motd modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

다음 예는 생성된 MOD를 표시합니다.

```
cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------
---
Greetings!

Vserver: svm1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------
---
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.

2 entries were displayed.
```

에 대한 자세한 내용은 `security login motd show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 클러스터 및 **SVM** 레벨에 표시되는 오늘의 메시지를 관리합니다

클러스터 또는 SVM 레벨에서 하루 중 메시지(MOTD)를 관리할 수 있습니다. 기본적으로 클러스터에 구성된 MOTD도 모든 SVM에 대해 활성화됩니다. 또한 SVM별로 MOTD를 구성할 수 있습니다. 클러스터 관리자가 각 SVM에 대해 클러스터 레벨 MOTD를 설정하거나 해제할 수 있습니다.

MOTD의 컨텐츠를 동적으로 생성하는 데 사용할 수 있는 에 대한 자세한 "이스케이프 시퀀스"내용은 ONTAP 명령 참조를 참조하십시오.

선택

- 클러스터 레벨에서 MOTD 관리:

원하는 작업	그러면...
기존 MOTD가 없는 경우 모든 로그인에 대해 MOTD를 생성합니다	클러스터 레벨 MOTD 설정: `security login motd modify -vserver <cluster_name> { [-message "<text>"]
[-uri <ftp_or_http_addr>] }`	SVM 레벨의 MOD가 구성되지 않은 경우 모든 로그인에 대해 MOTD를 변경합니다

원하는 작업	그러면...
클러스터 레벨 MOTD 수정: `security login motd modify -vserver <cluster_name> { [-message "<text>"] }	[-uri <ftp_or_http_addr>] }`
SVM 레벨의 MOD가 구성되지 않은 경우 모든 로그인에 대해 MOTD를 제거합니다	클러스터 수준 MOTD를 빈 문자열("")로 설정합니다. `security login motd modify -vserver <cluster_name> -message ""`
SVM 레벨의 MOTD를 사용하는 대신 모든 SVM에 클러스터 레벨 MOTD를 표시하도록 하십시오	클러스터 레벨 MOTD를 설정한 다음 클러스터 레벨 MOTD를 사용하도록 설정한 상태에서 모든 SVM 레벨 MOD를 빈 문자열로 설정합니다. a. `security login motd modify -vserver <cluster_name> { [-message "<text>"]
[-uri <ftp_or_http_addr>] }` .. `security login motd modify { -vserver !"<cluster_name>" } -message "" -is -cluster-message-enabled true`	선택한 SVM에 대해서만 MOTD를 표시하고 클러스터 레벨 MOTD는 사용하지 않습니다
클러스터 레벨 MOTD를 빈 문자열로 설정한 다음 선택한 SVM에 대해 SVM 레벨 MOD를 설정합니다. a. `security login motd modify -vserver <cluster_name> -message ""` b. `security login motd modify -vserver <svm_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] }` + 필요에 따라 각 SVM에 대해 이 단계를 반복할 수 있습니다.
모든 SVM(데이터 및 관리) SVM에 동일한 SVM 레벨 MOTD를 사용합니다	클러스터 및 모든 SVM에서 동일한 MOTD를 사용하도록 설정: `security login motd modify -vserver * { [-message "<text>"]
[-uri <ftp_or_http_addr>] }` [NOTE] ==== 대화식 모드를 사용하는 경우 CLI에서 클러스터와 각 SVM에 대해 MOTD를 개별적으로 입력하라는 메시지가 표시됩니다. 메시지가 표시되면 각 인스턴스에 동일한 MOTD를 붙여 넣을 수 있습니다. ====	모든 SVM에 선택적으로 클러스터 레벨 MOTD를 사용할 수 있지만 클러스터 로그인에 MOTD를 표시하지 않으려는 경우

원하는 작업	그러면...
클러스터 레벨 MOTD를 설정하되, 클러스터에 대해 해당 표시를 해제합니다. `security login motd modify -vserver <cluster_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] } -is-cluster-message -enabled false`
일부 SVM에만 클러스터 레벨 및 SVM 레벨 MOD가 모두 있는 경우 클러스터에서 모든 MOD와 SVM 수준을 제거합니다	MOTD에 대해 빈 문자열을 사용하도록 클러스터와 모든 SVM 설정: `security login motd modify -vserver * -message ""`
비어 있지 않은 문자열이 있는 SVM, 다른 SVM이 빈 문자열을 사용하고, 클러스터 레벨에서 다른 MOTD를 사용하는 SVM에 대해서만 MOTD를 수정합니다	확장 쿼리를 사용하여 MOTD를 선택적으로 수정합니다. `security login motd modify { -vserver !"<cluster_name>" -message !"" } { [-message "<text>"]
[-uri <ftp_or_http_addr>] }`	단일 또는 다중 줄 메시지의 어느 곳에나 특정 텍스트(예: "1월" 뒤에 "2015")가 포함된 모든 MOTD를 표시합니다. 텍스트가 여러 줄로 나뉘어 있는 경우에도 마찬가지입니다.
쿼리를 사용하여 MOD 표시: `security login motd show -message *"January"*"2015"*`	여러 줄 또는 연속된 줄 바꿈(라인 끝 또는 OLs라고도 함)을 포함하는 MOTD를 대화형으로 만듭니다.

- SVM 레벨에서 MOTD 관리:

  SVM 컨텍스트에서 지정할 `-vserver <svm_name>` 필요가 없습니다.

원하는 작업	그러면...
SVM에 기존 SVM 레벨 MOTD가 있는 경우 다른 SVM 레벨 MOTD를 사용하십시오	SVM 레벨 MOTD 수정: `security login motd modify -vserver <svm_name> { [-message "<text>"]
[-uri <ftp_or_http_addr>] }`	SVM에 SVM 레벨 MOTD가 이미 있는 경우 SVM에 클러스터 레벨 MOTD만 사용하십시오

원하는 작업	그러면...
SVM 레벨 MOTD를 빈 문자열로 설정한 다음, 클러스터 관리자에게 SVM을 위한 클러스터 레벨 MOTD를 사용하도록 요청하십시오. a. `security login motd modify -vserver <svm_name> -message ""` b. (클러스터 관리자의 경우) `security login motd modify -vserver <svm_name> -is -cluster-message-enabled true`	클러스터 레벨 및 SVM 레벨 MOD가 모두 SVM에 대해 현재 표시된 경우 SVM에 MOTD가 표시되지 않습니다

관련 정보

- "보안 로그인 motd 수정"
- "보안 로그인 mott show"

ONTAP 작업 및 작업 일정 관리

작업이 작업 대기열에 배치되어 자원을 사용할 수 있을 때 백그라운드에서 실행됩니다. 작업이 클러스터 리소스를 너무 많이 사용하는 경우, 클러스터에 대한 수요가 적어질 때까지 작업을 중지하거나 일시 중지할 수 있습니다. 작업을 모니터링하고 다시 시작할 수도 있습니다.

작업 범주

관리할 수 있는 작업 범주는 서버 계열 작업, 클러스터 계열 작업 및 개인입니다.

작업은 다음 범주에 포함될 수 있습니다.

- * 서버 계열 작업 *

  이러한 작업은 관리 프레임워크에서 실행할 특정 노드로 대기됩니다.

- * 클러스터 계열 작업 *

  이러한 작업은 관리 프레임워크에서 실행할 클러스터의 모든 노드에 대해 대기합니다.

- * 개인 작업 *

  이러한 작업은 특정 노드에만 해당되며 복제된 데이터베이스(RDB) 또는 다른 클러스터 메커니즘을 사용하지 않습니다. 비공개 작업을 관리하는 명령은 고급 권한 수준 이상이 필요합니다.

작업 관리를 위한 명령입니다

작업을 호출하는 명령을 입력하면 일반적으로 명령은 작업이 대기열에 있음을 알려 주는 다음 CLI 명령 프롬프트로 돌아갑니다. 그러나 일부 명령은 작업 진행률을 보고하고 작업이 완료될 때까지 CLI 명령 프롬프트로 돌아가지 않습니다. 이러한 경우 Ctrl+C를 눌러 작업을 백그라운드로 이동할 수 있습니다.

원하는 작업	이 명령 사용...
모든 작업에 대한 정보를 표시합니다	일자리 쇼
노드 단위로 작업에 대한 정보를 표시합니다	'job show bynode'
클러스터 관련 작업에 대한 정보를 표시합니다	잡쇼 클러스터
완료된 작업에 대한 정보를 표시합니다	일자리 보이기 완료
작업 기록에 대한 정보를 표시합니다	직업 연혁 쇼 클러스터의 각 노드에 대해 최대 25,000개의 작업 레코드가 저장됩니다. 따라서 전체 작업 기록을 표시하려고 하면 시간이 오래 걸릴 수 있습니다. 대기 시간이 오래 걸릴 수 있으므로 노드, SVM(스토리지 가상 머신) 또는 레코드 ID별로 작업을 표시해야 합니다.
개인 작업 목록을 표시합니다	잡사쇼(고급특권)
완료된 개인 작업에 대한 정보를 표시합니다	취직 사적 공연 완료(고급 특권 수준)
작업 관리자의 초기화 상태에 대한 정보를 표시합니다	'job initstate show'(고급 권한 수준)
작업의 진행 상황을 모니터링합니다	직업감시-진척도
개인 작업의 진행 상황을 모니터링합니다	취직사감시-진전(고급특권)
작업을 일시정지합니다	"작업 일시정지"
개인 작업을 일시 중지합니다	작업 비공개 일시 중지(고급 권한 수준)
일시 중지된 작업을 다시 시작합니다	일자리 재개다
일시 중지된 개인 작업을 다시 시작합니다	일자리 민영(Advanced Privilege)
작업을 중지합니다	잡지중지
개인 작업을 중지합니다	일자리 전용 경유지고(고급 특권 수준)
작업을 삭제합니다	일자리 삭제
개인 작업을 삭제합니다	'job private delete'(고급 권한 수준)

원하는 작업	이 명령 사용...
클러스터 관련 작업을 해당 작업을 소유하는 사용 불가능한 노드와 연결을 끊는 경우 다른 노드가 해당 작업의 소유권을 가질 수 있습니다	잡무청구(Advanced Privilege Level)

명령을 사용하여 완료된 작업의 결과를 확인할 수 `event log show` 있습니다. 에 대한 자세한 내용은 `event log show` "ONTAP 명령 참조입니다"을 참조하십시오.

작업 스케줄 관리를 위한 명령입니다

볼륨 스냅샷과 같은 많은 작업을 지정된 스케줄에서 실행하도록 구성할 수 있습니다. 특정 시간에 실행되는 스케줄을 _cron_schedules라고 합니다(UNIX 스케줄과 유사 `cron`). 일정 간격으로 실행되는 스케줄을 _INTERVAL_schedules 라고 합니다. 명령을 사용하여 `job schedule` 작업 일정을 관리할 수 있습니다.

작업 일정은 클러스터 날짜 및 시간의 수동 변경에 맞게 조정되지 않습니다. 이러한 작업은 작업이 생성된 현재 클러스터 시간 또는 가장 최근에 실행된 작업을 기준으로 실행되도록 예약되어 있습니다. 따라서 클러스터 날짜 또는 시간을 수동으로 변경하는 경우 "job show" 및 "job history show" 명령을 사용하여 예약된 모든 작업이 요구 사항에 따라 대기열에 추가되고 완료되었는지 확인해야 합니다.

클러스터가 MetroCluster 구성에 포함된 경우 두 클러스터의 작업 일정이 동일해야 합니다. 따라서 작업 스케줄을 생성, 수정 또는 삭제하는 경우 원격 클러스터에서 동일한 작업을 수행해야 합니다.

원하는 작업	이 명령 사용...
모든 스케줄에 대한 정보를 표시합니다	일자리스케줄 쇼
일정별로 작업 목록을 표시합니다	일자리일정=일자리다
cron 일정에 대한 정보를 표시합니다	작업 스케줄 cron 쇼
간격 일정에 대한 정보를 표시합니다	작업 일정 간격 표시
cron 일정을 생성합니다	작업 스케줄 cron 생성 ONTAP 9.10.1부터 작업 일정에 SVM을 포함할 수 있습니다.
간격 일정을 만듭니다	작업 일정 간격 만들기 일, 시간, 분, 초 중 하나 이상의 매개 변수를 지정해야 합니다.
cron 일정을 수정합니다	작업 스케줄 cron 수정
간격 일정을 수정합니다	작업 일정 간격 수정

원하는 작업	이 명령 사용...
스케줄을 삭제합니다	작업 일정 삭제
cron 일정을 삭제합니다	작업 스케줄 cron 삭제
간격 일정을 삭제합니다	작업 일정 간격 삭제

관련 정보

- "있습니다"

클러스터 구성 백업 및 복원(클러스터 관리자만 해당)

ONTAP 구성 백업 파일에 대해 알아봅니다

구성 백업 파일은 클러스터에 필요한 구성 가능한 모든 옵션과 해당 클러스터 내의 노드가 올바르게 작동하는 데 필요한 정보를 포함하는 아카이브 파일(.7z)입니다.

이러한 파일은 각 노드의 로컬 구성과 클러스터 차원의 복제 구성을 저장합니다. 구성 백업 파일을 사용하여 클러스터의 구성을 백업 및 복원할 수 있습니다.

두 가지 유형의 구성 백업 파일이 있습니다.

- * 노드 구성 백업 파일 *

  클러스터의 정상 상태인 각 노드에는 노드에서 정상 작동하는 데 필요한 모든 구성 정보와 메타데이터가 포함된 노드 구성 백업 파일이 포함되어 있습니다.

- * 클러스터 구성 백업 파일 *

  이러한 파일에는 클러스터에 있는 모든 노드 구성 백업 파일의 아카이브와 복제된 클러스터 구성 정보(복제된 데이터베이스 또는 RDB 파일)가 포함됩니다. 클러스터 구성 백업 파일을 사용하면 전체 클러스터 또는 클러스터 내의 모든 노드에 대한 구성을 복원할 수 있습니다. 클러스터 구성 백업 스케줄은 이러한 파일을 자동으로 생성하여 클러스터의 여러 노드에 저장합니다.

구성 백업 파일에는 구성 정보만 포함되어 있습니다. 사용자 데이터는 포함되지 않습니다. 사용자 데이터 복원에 대한 자세한 내용은 을 참조하십시오 "데이터 보호".

ONTAP 클러스터 및 노드 구성 백업 파일의 백업 예약에 대해 자세히 알아보십시오

세 개의 별도 일정으로 클러스터 및 노드 구성 백업 파일이 자동으로 생성되어 클러스터의 노드 간에 복제됩니다.

구성 백업 파일은 다음 일정에 따라 자동으로 생성됩니다.

- 8시간마다
- 매일

- 매주

이 각 시점에서 노드의 구성 백업 파일이 클러스터의 정상 상태인 각 노드에 생성됩니다. 이러한 모든 노드 구성 백업 파일은 복제된 클러스터 구성과 함께 단일 클러스터 구성 백업 파일에서 수집되고 클러스터의 하나 이상의 노드에 저장됩니다.

구성 백업 일정을 관리하기 위한 **ONTAP** 명령

'시스템 구성 백업 설정' 명령을 사용하여 구성 백업 스케줄을 관리할 수 있습니다.

이러한 명령은 고급 권한 수준에서 사용할 수 있습니다.

원하는 작업	이 명령 사용...
구성 백업 스케줄의 설정을 변경합니다. • 클러스터의 기본 위치 외에 구성 백업 파일이 업로드될 원격 URL(HTTP, HTTPS, FTP 또는 FTPS)을 지정합니다. • 원격 URL에 로그인하는 데 사용할 사용자 이름을 지정합니다 • 각 구성 백업 스케줄에 대해 유지할 백업 수를 설정합니다	'시스템 구성 백업 설정 수정 원격 URL에서 HTTPS를 사용하는 경우 '-validate-certification' 옵션을 사용하여 디지털 인증서 유효성 검사를 활성화하거나 비활성화합니다. 인증서 유효성 검사는 기본적으로 사용되지 않습니다. 구성 백업 파일을 업로드하는 웹 서버는 HTTPS에 대해 HTTP 및 POST 작업에 대해 PUT 작업을 활성화해야 합니다. 자세한 내용은 웹 서버 설명서를 참조하십시오.
원격 URL에 로그인하는 데 사용할 암호를 설정합니다	'System configuration backup settings set-password'를 선택합니다
구성 백업 스케줄에 대한 설정을 봅니다	'시스템 구성 백업 설정 표시 '-instance' 매개 변수를 설정하여 각 스케줄에 대해 유지할 사용자 이름과 백업 수를 봅니다.

노드 구성 백업 파일을 관리하기 위한 **ONTAP** 명령

'시스템 구성 백업' 명령을 사용하여 클러스터 및 노드 구성 백업 파일을 관리합니다.

이러한 명령은 고급 권한 수준에서 사용할 수 있습니다.

원하는 작업	이 명령 사용...
새 노드 또는 클러스터 구성 백업 파일을 생성합니다	'시스템 구성 백업 생성
노드의 구성 백업 파일을 클러스터의 다른 노드로 복사합니다	'시스템 구성 백업 복사

원하는 작업	이 명령 사용...
클러스터의 노드에서 원격 URL(FTP, HTTP, HTTPS 또는 FTPS)로 구성 백업 파일을 업로드합니다.	'system configuration backup upload 원격 URL에서 HTTPS를 사용하는 경우 '-validate-certification' 옵션을 사용하여 디지털 인증서 유효성 검사를 활성화하거나 비활성화합니다. 인증서 유효성 검사는 기본적으로 사용되지 않습니다. 구성 백업 파일을 업로드하는 웹 서버에서는 HTTP에 대한 PUT 작업이 활성화되어 있어야 하고 HTTPS에 대한 POST 작업이 활성화되어 있어야 합니다. 일부 웹 서버에는 추가 모듈을 설치해야 할 수도 있습니다. 자세한 내용은 웹 서버 설명서를 참조하세요. 지원되는 URL 형식은 ONTAP 릴리스에 따라 다릅니다. 시스템 구성 명령에 대해 자세히 알아보세요. "ONTAP 명령 참조입니다".
원격 URL에서 클러스터의 노드로 구성 백업 파일을 다운로드하고, 지정된 경우 디지털 인증서의 유효성을 검사합니다	'system configuration backup download 원격 URL에서 HTTPS를 사용하는 경우 '-validate-certification' 옵션을 사용하여 디지털 인증서 유효성 검사를 활성화하거나 비활성화합니다. 인증서 유효성 검사는 기본적으로 사용되지 않습니다.
클러스터의 노드에서 구성 백업 파일 이름을 바꿉니다	'system configuration backup rename'
클러스터에 있는 하나 이상의 노드에 대한 노드 및 클러스터 구성 백업 파일을 봅니다	'system configuration backup show'
노드에서 구성 백업 파일을 삭제합니다	'system configuration backup delete 이 명령은 지정된 노드에서만 구성 백업 파일을 삭제합니다. 구성 백업 파일이 클러스터의 다른 노드에도 있는 경우 해당 노드에 남아 있습니다.

관련 정보

- "시스템 구성 백업"

노드를 복구할 **ONTAP** 노드 구성 백업 파일을 찾습니다

원격 URL 또는 클러스터의 노드에 있는 구성 백업 파일을 사용하여 노드 구성을 복구할 수 있습니다.

이 작업에 대해

클러스터 또는 노드 구성 백업 파일을 사용하여 노드 구성을 복원할 수 있습니다.

단계

1. 구성을 복원해야 하는 노드에서 구성 백업 파일을 사용할 수 있도록 합니다.

구성 백업 파일이 있는 경우...	그러면...
원격 URL에서	고급 권한 레벨의 '시스템 구성 백업 다운로드' 명령을 사용하여 복구 노드로 다운로드합니다.
클러스터에 있는 노드	a. 복구 노드의 구성이 포함된 클러스터에서 사용 가능한 구성 백업 파일 목록을 보려면 고급 권한 수준에서 'system configuration backup show' 명령을 사용하십시오. b. 확인한 구성 백업 파일이 복구 노드에 없으면 'system configuration backup copy' 명령을 사용하여 복구 노드에 복사합니다.

이전에 클러스터를 다시 생성한 경우 클러스터를 재생성한 후에 생성된 구성 백업 파일을 선택해야 합니다. 클러스터를 재생성하기 전에 생성된 구성 백업 파일을 사용해야 하는 경우 노드를 복구한 후에 클러스터를 다시 생성해야 합니다.

관련 정보

- "시스템 구성 백업 사본"

ONTAP 노드 구성 백업 파일을 사용하여 노드를 복구합니다

복구 노드에서 식별하여 사용할 수 있도록 만든 구성 백업 파일을 사용하여 노드 구성을 복원합니다.

이 작업에 대해

이 작업은 노드의 로컬 구성 파일이 손실되는 재해에서만 수행해야 합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 노드가 정상 상태인 경우 다른 노드의 고급 권한 수준에서 를 사용합니다 `cluster modify` 명령과 함께 `-node` 및 `-eligibility` 매개 변수를 사용하여 부적격으로 표시하고 클러스터에서 분리합니다.

   노드가 정상이 아닌 경우 이 단계를 건너뛰어야 합니다.

   이 예제에서는 노드 2가 클러스터에 참여할 수 없도록 수정하여 해당 구성을 복원할 수 있도록 합니다.

```
cluster1::*> cluster modify -node node2 -eligibility false
```

에 대한 자세한 내용은 `cluster modify` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 를 사용합니다 `system configuration recovery node restore` 고급 권한 레벨의 명령을 사용하여 구성 백업 파일에서 노드의 구성을 복원합니다.

   노드 이름을 포함하여 노드의 ID가 손실되면 를 사용해야 합니다 `-nodename-in-backup` 구성 백업 파일에 노드 이름을 지정하는 매개 변수입니다.

   다음 예에서는 노드에 저장된 구성 백업 파일 중 하나를 사용하여 노드의 구성을 복구합니다.

   ```
   cluster1::*> system configuration recovery node restore -backup
   cluster1.8hour.2011-02-22.18_15_00.7z

   Warning: This command overwrites local configuration files with
            files contained in the specified backup file. Use this
            command only to recover from a disaster that resulted
            in the loss of the local configuration files.
            The node will reboot after restoring the local configuration.
   Do you want to continue? {y|n}: y
   ```

   구성이 복원되고 노드가 재부팅됩니다.

4. 노드 부적격으로 표시한 경우 'system configuration recovery cluster sync' 명령을 사용하여 노드를 적합한 것으로 표시하고 클러스터와 동기화합니다.
5. SAN 환경에서 작동 중인 경우 'system node reboot' 명령을 사용하여 노드를 재부팅하고 SAN quorum을 다시 설정하십시오.

작업을 마친 후

이전에 클러스터를 다시 생성한 경우, 해당 클러스터를 다시 생성하기 전에 생성된 구성 백업 파일을 사용하여 노드 구성을 복원하는 경우 클러스터를 다시 생성해야 합니다.

클러스터를 복구할 **ONTAP** 클러스터 구성 백업 파일을 찾습니다

클러스터의 노드 또는 클러스터 구성 백업 파일의 구성을 사용하여 클러스터를 복구할 수 있습니다.

단계

1. 클러스터를 복구할 구성 유형을 선택합니다.

   - 클러스터의 노드

     클러스터가 둘 이상의 노드로 구성되어 있고 노드 중 하나에 클러스터가 원하는 구성에 있을 때의 클러스터 구성이 있는 경우, 해당 노드에 저장된 구성을 사용하여 클러스터를 복구할 수 있습니다.

     대부분의 경우 가장 최근의 트랜잭션 ID가 있는 복제 링이 포함된 노드는 클러스터 구성을 복구하는 데 가장 적합한 노드입니다. 고급 권한 레벨의 'cluster ring show' 명령을 사용하면 클러스터의 각 노드에서 사용할 수 있는 복제된 링 목록을 볼 수 있습니다.

◦ 클러스터 구성 백업 파일

올바른 클러스터 구성의 노드를 식별할 수 없거나 클러스터가 단일 노드로 구성된 경우 클러스터 구성 백업 파일을 사용하여 클러스터를 복구할 수 있습니다.

구성 백업 파일에서 클러스터를 복구하는 경우 백업이 수행된 이후에 변경된 모든 구성은 손실됩니다. 복구 후에는 구성 백업 파일과 현재 구성 간의 불일치를 해결해야 합니다. 를 참조하십시오"NetApp 기술 자료: ONTAP 구성 백업 해결 가이드" 문제 해결 지침.

2. 클러스터 구성 백업 파일을 사용하도록 선택한 경우, 클러스터 복구에 사용할 노드에서 해당 파일을 사용할 수 있도록 설정합니다.

구성 백업 파일이 있는 경우...	그러면...
원격 URL에서	고급 권한 레벨의 '시스템 구성 백업 다운로드' 명령을 사용하여 복구 노드로 다운로드합니다.
클러스터에 있는 노드	a. 고급 권한 레벨의 'system configuration backup show' 명령을 사용하여 클러스터가 원하는 구성에 있을 때 생성된 클러스터 구성 백업 파일을 찾습니다. b. 클러스터 구성 백업 파일이 클러스터 복구에 사용할 노드에 없으면 'system configuration backup copy' 명령을 사용하여 복구 노드에 복사합니다.

관련 정보

- "클러스터 링 쇼"
- "시스템 구성 백업 사본"

ONTAP 클러스터 구성 백업 파일을 사용하여 클러스터를 복원합니다

클러스터 장애 후 기존 구성에서 클러스터 구성을 복원하려면 선택한 클러스터 구성을 사용하여 클러스터를 다시 생성한 다음 복구 노드에 사용할 수 있도록 설정한 다음 각 추가 노드를 새 클러스터에 다시 연결합니다.

이 작업에 대해

이 작업은 클러스터의 구성 손실을 초래한 재해에서 복구하려는 경우에만 수행해야 합니다.

> 구성 백업 파일에서 클러스터를 다시 생성하는 경우 기술 지원 부서에 문의하여 구성 백업 파일과 클러스터에 있는 구성 간의 불일치 문제를 해결해야 합니다.
>
> 구성 백업 파일에서 클러스터를 복구하는 경우 백업이 수행된 이후에 변경된 모든 구성은 손실됩니다. 복구 후에는 구성 백업 파일과 현재 구성 간의 불일치를 해결해야 합니다. 를 참조하십시오"NetApp 기술 자료: ONTAP 구성 백업 해결 가이드" 문제 해결 지침.

단계

1. 각 HA 쌍에 대해 스토리지 페일오버 해제:

' * storage failover modify -node_node_name _ -enabled false * '

각 HA 쌍에 대해 스토리지 페일오버를 한 번만 해제하면 됩니다. 노드에 대해 스토리지 페일오버를 해제하면 노드의 파트너에서도 스토리지 페일오버가 해제됩니다.

2. 복구 노드를 제외하고 각 노드를 중단합니다.

"* 시스템 노드 halt-node_node_name_ - 이유 "text" * "

```
cluster1::*> system node halt -node node0 -reason "recovering cluster"

Warning: Are you sure you want to halt the node? {y|n}: y
```

3. 권한 수준을 고급으로 설정합니다.

' * set-Privilege advanced * '

4. 복구 노드에서 ' * system configuration recovery cluster recreate * ' 명령을 사용하여 클러스터를 다시 생성합니다.

이 예에서는 복구 노드에 저장된 구성 정보를 사용하여 클러스터를 다시 생성합니다.

```
cluster1::*> configuration recovery cluster recreate -from node

Warning: This command will destroy your existing cluster. It will
         rebuild a new single-node cluster consisting of this node
         and its current configuration. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

복구 노드에 새 클러스터가 생성됩니다.

5. 구성 백업 파일에서 클러스터를 다시 생성하는 경우 클러스터 복구가 진행 중인지 확인합니다.

"* 시스템 구성 복구 클러스터 표시 * '

정상적인 노드에서 클러스터를 다시 생성하는 경우에는 클러스터 복구 상태를 확인할 필요가 없습니다.

```
cluster1::*> system configuration recovery cluster show
 Recovery Status: in-progress
 Is Recovery Status Persisted: false
```

6. 재생성된 클러스터에 다시 결합해야 하는 각 노드를 부팅합니다.

노드를 한 번에 하나씩 재부팅해야 합니다.

7. 재생성된 클러스터에 결합해야 하는 각 노드에 대해 다음을 수행합니다.

   a. 다시 생성된 클러스터의 정상 노드에서 타겟 노드를 다시 연결합니다.

      '* 시스템 구성 복구 클러스터가 다시 참가합니다 - node_node_name_ *

      이 예에서는 ""node2"" 타겟 노드를 다시 생성된 클러스터에 다시 연결합니다.

      ```
      cluster1::*> system configuration recovery cluster rejoin -node node2

      Warning: This command will rejoin node "node2" into the local
               cluster, potentially overwriting critical cluster
               configuration files. This command should only be used
               to recover from a disaster. Do not perform any other
               recovery operations while this operation is in progress.
               This command will cause node "node2" to reboot.
      Do you want to continue? {y|n}: y
      ```

      타겟 노드가 재부팅된 다음 클러스터에 추가됩니다.

   b. 대상 노드가 정상이고 클러스터의 나머지 노드와 함께 쿼럼을 형성했는지 확인합니다.

      `* 클러스터 표시 - 자격 True*'

      다른 노드를 다시 참가하려면 타겟 노드가 다시 생성된 클러스터에 다시 참가해야 합니다.

      ```
      cluster1::*> cluster show -eligibility true
      Node                 Health  Eligibility   Epsilon
      -------------------- ------- ------------  ------------
      node0                true    true          false
      node1                true    true          false
      2 entries were displayed.
      ```

8. 구성 백업 파일에서 클러스터를 다시 생성한 경우 복구 상태를 완료로 설정합니다.

   '* 시스템 구성 복구 클러스터 수정-복구-상태 완료 * '

9. 관리자 권한 레벨로 돌아갑니다.

   ' * set-privilege admin * '

10. 클러스터가 2개의 노드로만 구성된 경우, 클러스터 HA를 다시 활성화하려면 ' * cluster ha modify * ' 명령을 사용하십시오.
11. 각 HA 쌍의 스토리지 페일오버를 다시 설정하려면 ' * storage failover modify * ' 명령을 사용합니다.

작업을 마친 후

클러스터에 SnapMirror 피어 관계가 있는 경우 이러한 관계도 다시 생성해야 합니다. 자세한 내용은 을 참조하십시오

"데이터 보호".

관련 정보

- "ONTAP 명령 참조입니다"
- "스토리지 장애 조치 수정"

노드를 **ONTAP** 클러스터와 동기화하여 클러스터 전체 쿼럼을 보장합니다

클러스터 전체 쿼럼이 있지만 하나 이상의 노드가 클러스터와 동기화되지 않은 경우 노드를 동기화하여 노드에서 복제된 데이터베이스(RDB)를 복원하고 쿼럼으로 가져와야 합니다.

단계

1. 정상 노드에서 고급 권한 레벨의 시스템 구성 복구 클러스터 동기화 명령을 사용하여 클러스터 구성과 동기화되지 않은 노드를 동기화합니다.

   이 예에서는 노드(*node2*)를 나머지 클러스터와 동기화합니다.

```
cluster1::*> system configuration recovery cluster sync -node node2

Warning: This command will synchronize node "node2" with the cluster
         configuration, potentially overwriting critical cluster
         configuration files on the node. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress. This
         command will cause all the cluster applications on node
         "node2" to restart, interrupting administrative CLI and Web
         interface on that node.
Do you want to continue? {y|n}: y
All cluster applications on node "node2" will be restarted. Verify that
the cluster applications go online.
```

결과

RDB가 노드로 복제되고 노드가 클러스터에 참여할 수 있게 됩니다.

ONTAP 클러스터의 노드 코어 덤프 관리(클러스터 관리자만 해당)

노드에서 패닉이 발생하면 코어 덤프가 발생하고 기술 지원 부서에서 문제를 해결하는 데 사용할 수 있는 코어 덤프 파일이 시스템에서 생성됩니다. 코어 덤프 속성을 구성하거나 표시할 수 있습니다. 코어 덤프 파일을 저장, 표시, 분할, 업로드 또는 삭제할 수도 있습니다.

다음과 같은 방법으로 코어 덤프를 관리할 수 있습니다.

- 코어 덤프를 구성하고 구성 설정을 표시합니다
- 코어 덤프의 기본 정보, 상태 및 속성을 표시합니다

코어 덤프 파일 및 보고서는 노드의 '/mroot/etc/crash/' 디렉토리에 저장됩니다. 시스템 노드 coredump 명령이나 웹 브라우저를 사용하여 디렉토리 컨텐츠를 표시할 수 있다.

- 코어 덤프 콘텐츠를 저장하고 저장된 파일을 지정된 위치 또는 기술 지원에 업로드합니다

  ONTAP에서는 테이크오버, 애그리게이트 재배치 또는 반환 중에 코어 덤프 파일의 저장을 시작하지 못합니다.

- 더 이상 필요하지 않은 코어 덤프 파일을 삭제하는 중입니다

코어 덤프를 관리하는 명령입니다

'system node coredump config' 명령어를 사용해 코어 덤프의 구성, 코어 덤프 파일을 관리하는 시스템 노드 coredump 명령, 애플리케이션 코어 리포트를 관리하는 시스템 노드 coredump reports 명령 등을 관리할 수 있다.

이 항목에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

원하는 작업	이 명령 사용...
코어 덤프를 구성합니다	시스템 노드 코어 덤프 구성 수정
코어 덤프에 대한 구성 설정을 표시합니다	'시스템 노드 코어 덤프 구성 표시'
코어 덤프에 대한 기본 정보를 표시합니다	'시스템 노드 코어 덤프 표시'
노드를 재부팅할 때 코어 덤프를 수동으로 트리거합니다	`system node reboot` 두 가지 모두 `-dump` 및 `-skip-lif-migration-before-reboot` 매개 변수 링크: `skip-lif-migration-before-reboot` [매개 변수는 재부팅 전에 LIF 마이그레이션을 건너뛰도록 지정합니다.
노드를 종료할 때 코어 덤프를 수동으로 트리거합니다	`system node halt` 두 가지 모두 `-dump` 및 `-skip-lif-migration-before-shutdown` 매개 변수 링크: `skip-lif-migration-before-shutdown` [매개 변수는 종료 전의 LIF 마이그레이션을 건너뛰도록 지정합니다.
지정된 코어 덤프를 저장합니다	시스템 노드 코어 덤프 저장
지정한 노드에 있는 저장되지 않은 모든 코어 덤프를 저장합니다	시스템 노드 코어 덤프 save-all

원하는 작업	이 명령 사용...
지정한 코어 덤프 파일이 있는 AutoSupport 메시지를 생성하고 보냅니다	'system node AutoSupport invoke-core-upload '-Uri' 선택적 매개 변수는 AutoSupport 메시지의 대체 대상을 지정합니다.
코어 덤프에 대한 상태 정보를 표시합니다	시스템 노드 코어 덤프 상태
지정된 코어 덤프를 삭제합니다	시스템 노드 코어 덤프 삭제
저장되지 않은 모든 코어 덤프 또는 노드에 저장된 모든 코어 파일을 삭제합니다	'시스템 노드 코어 덤프 삭제 - 모두'
응용 프로그램 코어 덤프 보고서를 표시합니다	시스템 노드 코어 덤프 보고서가 표시됩니다
응용 프로그램 코어 덤프 보고서를 삭제합니다	시스템 노드 코어 덤프 보고서 삭제

관련 정보

"ONTAP 명령 참조입니다"

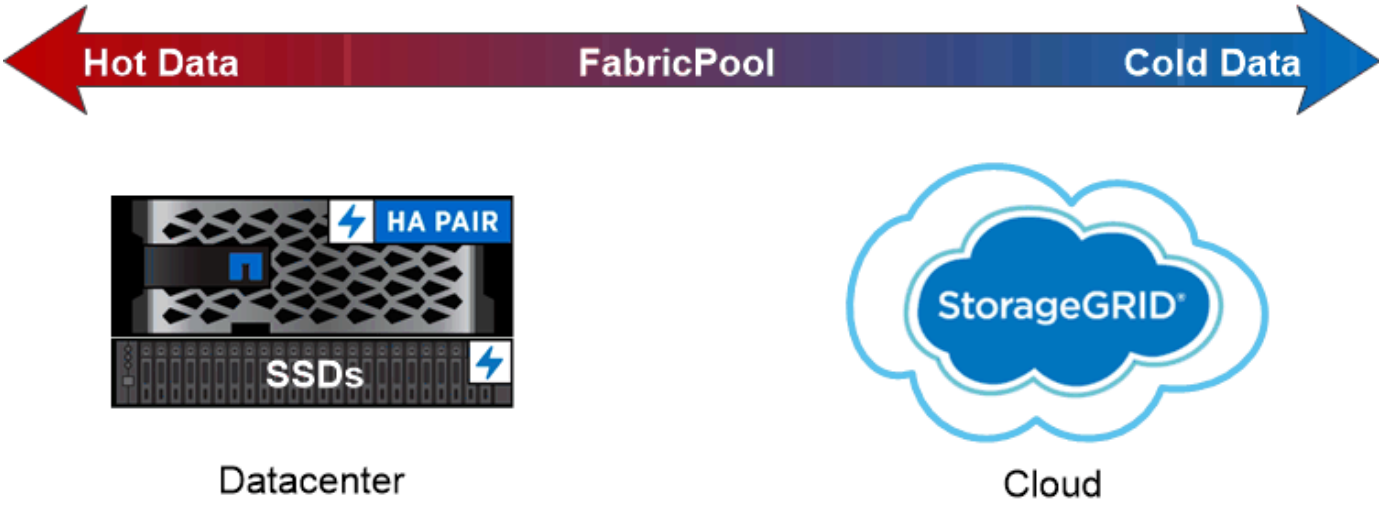
디스크 및 계층 관리

디스크 및 **ONTAP** 로컬 계층

_local tiers_는 _aggregates_라고도 하며 노드에서 관리하는 디스크에 대한 논리적 컨테이너입니다. 로컬 계층을 사용하여 다양한 성능 요구사항에 따라 워크로드를 격리하거나, 다른 액세스 패턴으로 데이터를 계층화하거나, 규정 준수를 위해 데이터를 분리할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다.

- 지연 시간이 가장 짧고 성능이 가장 높은 비즈니스 크리티컬 애플리케이션의 경우 SSD로만 구성된 로컬 계층을 생성할 수 있습니다.
- 서로 다른 액세스 패턴으로 데이터를 계층화하려면 _ 하이브리드 로컬 계층 _ 을(를) 생성하고, 사용 중인 데이터 세트에 플래시를 고성능 캐시로 구축하는 동시에, 액세스 빈도가 낮은 데이터에 저비용 HDD 또는 오브젝트 스토리지를 사용할 수 있습니다.
  - 는 "_플래시 풀 _"SSD와 HDD로 구성됩니다.
  - 는 "*FabricPool*"오브젝트 저장소가 연결된 All-SSD 로컬 계층으로 구성됩니다.
- 규정 준수를 위해 아카이빙된 데이터를 활성 데이터에서 분리해야 하는 경우 용량 HDD로 구성된 로컬 계층 또는 성능과 용량 HDD를 조합하여 사용할 수 있습니다.



You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed "hot" data and object storage for rarely accessed "cold" data.

MetroCluster 구성에서 로컬 계층으로 작업

MetroCluster 구성을 사용하는 경우 초기 구성에 대한 설명서의 절차와 로컬 계층 및 디스크 관리에 대한 지침을 따라야 "MetroCluster"합니다.

관련 정보

- "로컬 계층 관리"
- "디스크를 관리합니다"
- "RAID 구성을 관리합니다"
- "Flash Pool 계층 관리"
- "FabricPool 클라우드 계층 관리"

로컬 계층 관리

ONTAP 로컬 계층 관리에 대해 자세히 알아보십시오

System Manager 또는 ONTAP CLI를 사용하여 로컬 계층을 추가하고, 사용을 관리하고, 용량(디스크)을 추가할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

다음 작업을 수행할 수 있습니다.

- "로컬 계층을 추가(생성)합니다"

로컬 계층을 추가하려면 특정 워크플로를 따릅니다. 로컬 계층에 필요한 디스크 또는 디스크 파티션 수를 결정하고 로컬 계층을 생성하는 데 사용할 방법을 결정합니다. ONTAP에서 구성을 할당하도록 하여 로컬 계층을 자동으로 추가하거나 수동으로 구성을 지정할 수 있습니다.

- "로컬 계층의 사용을 관리합니다"

  기존 로컬 계층의 경우 이름을 바꾸거나 미디어 비용을 설정하거나 드라이브 및 RAID 그룹 정보를 확인할 수 있습니다. 로컬 계층의 RAID 구성을 수정하고 로컬 계층을 스토리지 VM(SVM)에 할당할 수 있습니다. 로컬 계층의 RAID 구성을 수정하고 로컬 계층을 스토리지 VM(SVM)에 할당할 수 있습니다. 로컬 계층에 상주하는 볼륨과 로컬 계층에서 사용하는 공간을 확인할 수 있습니다. 볼륨에서 사용할 수 있는 공간의 양을 제어할 수 있습니다. HA 쌍으로 로컬 계층 소유권을 재배치할 수 있습니다. 로컬 계층을 삭제할 수도 있습니다.

- "로컬 계층에 용량(디스크)을 추가합니다"

  다른 방법을 사용하여 특정 워크플로우를 따라 용량을 추가합니다. 디스크를 로컬 계층에 추가하고 드라이브를 노드 또는 쉘프에 추가할 수 있습니다. 필요한 경우 잘못 정렬된 스페어 파티션을 수정할 수 있습니다.

로컬 계층을 추가(생성)합니다

ONTAP 로컬 계층을 추가하는 워크플로입니다

로컬 계층을 생성하면 시스템의 볼륨에 스토리지가 제공됩니다.

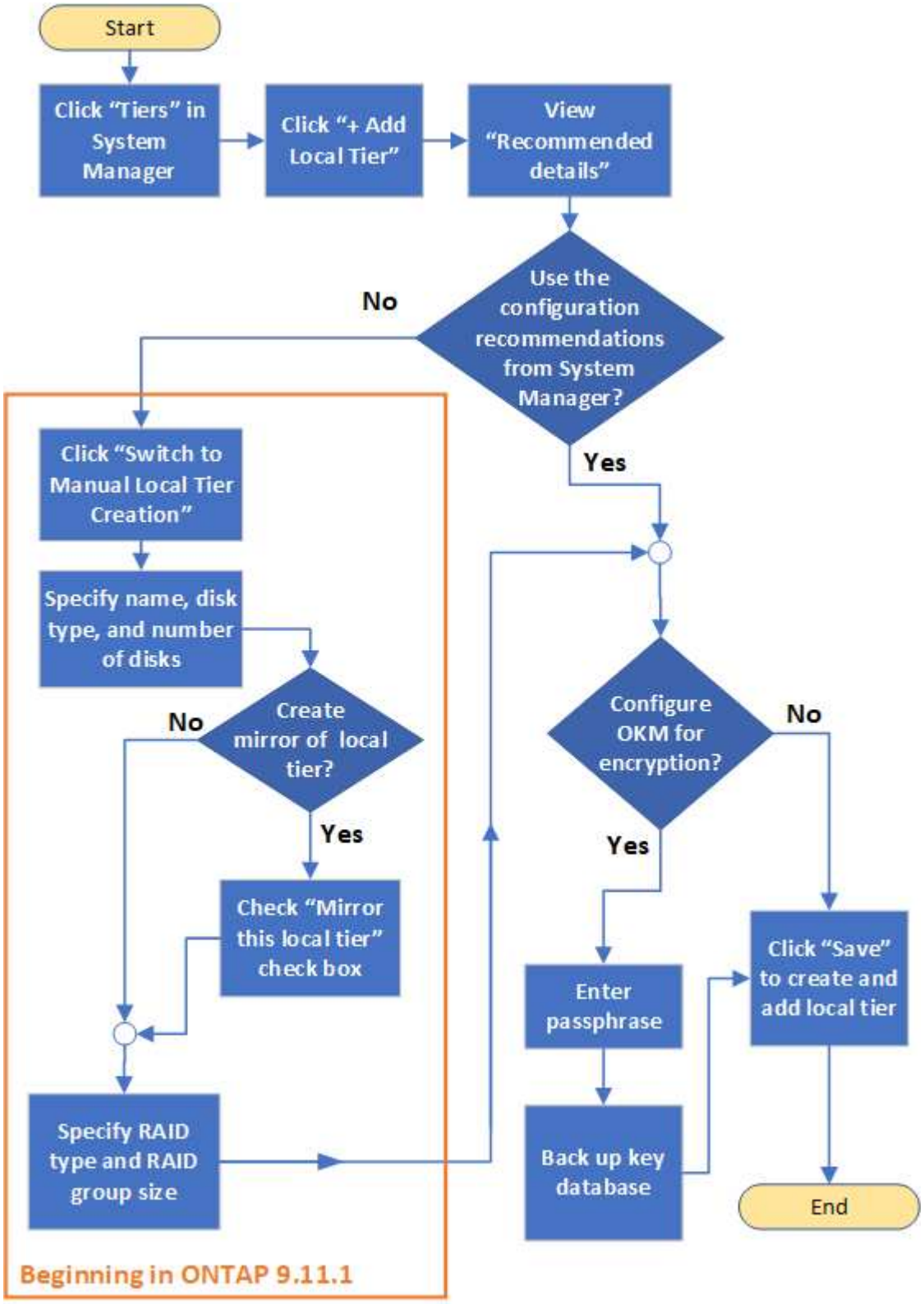
ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

로컬 계층을 생성하는 워크플로는 사용하는 인터페이스인 System Manager 또는 CLI에 따라 다릅니다.

시스템 관리자

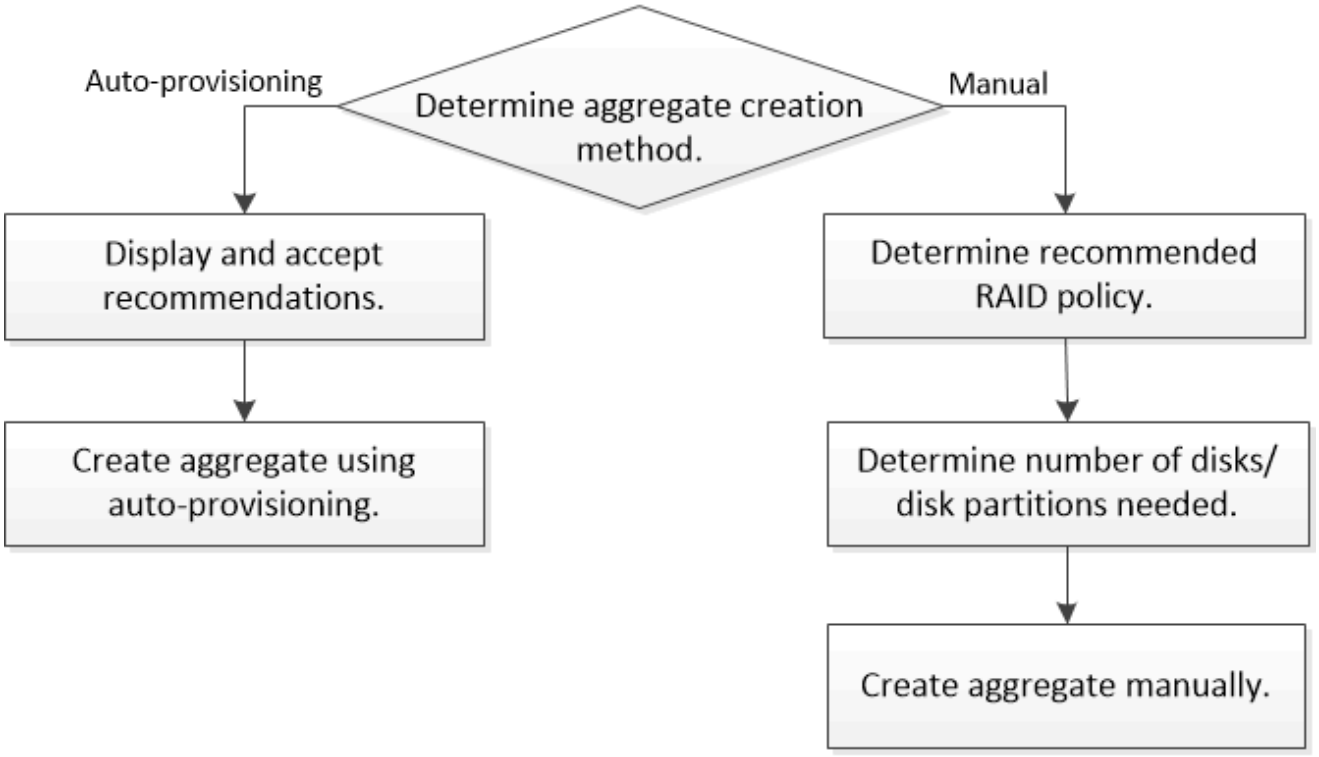
System Manager에서는 로컬 계층 구성에 대한 권장 모범 사례를 기반으로 로컬 계층을 생성합니다.

ONTAP 9.11.1부터 로컬 계층을 추가하기 위해 자동 프로세스 중에 권장된 것과 다른 구성을 원하는 경우 로컬 계층을 수동으로 구성할 수 있습니다.



CLI를 참조하십시오

ONTAP 로컬 계층(자동 프로비저닝)을 생성할 때 권장 구성을 제공할 수 있습니다. Best Practice에 따라 권장되는 구성이 환경에 적합한 경우 해당 구성을 수락하여 로컬 계층을 생성할 수 있습니다. 그렇지 않으면 로컬 계층을 수동으로 생성할 수 있습니다.



ONTAP 로컬 계층에 필요한 디스크 또는 디스크 파티션 수를 확인합니다

로컬 계층에 시스템 및 비즈니스 요구 사항을 충족하기에 충분한 디스크 또는 디스크 파티션이 있어야 합니다. 또한 데이터 손실 가능성을 최소화하기 위해 권장되는 수의 핫 스페어 디스크 또는 핫 스페어 디스크 파티션이 있어야 합니다.

루트 데이터 파티셔닝은 특정 구성에서 기본적으로 활성화되어 있습니다. 루트 데이터 파티셔닝이 설정된 시스템은 디스크 파티션을 사용하여 로컬 계층을 생성합니다. 루트 데이터 파티셔닝이 설정되어 있지 않은 시스템은 분할되지 않은 디스크를 사용합니다.

RAID 정책에 필요한 최소 수와 최소 용량 요구 사항을 충족할 수 있을 만큼 충분한 디스크 또는 디스크 파티션이 있어야 합니다.

ONTAP에서 드라이브의 사용 가능한 공간이 드라이브의 물리적 용량보다 작습니다. 에서 특정 드라이브의 사용 가능한 공간과 각 RAID 정책에 필요한 최소 디스크 또는 디스크 파티션 수를 찾을 수 있습니다 "Hardware Universe".

특정 디스크의 사용 가능한 공간을 결정합니다

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 디스크의 사용 가능한 공간을 확인합니다 *

디스크의 사용 가능한 크기를 보려면 다음 단계를 수행하십시오.

단계

1. Storage > Tiers * 로 이동합니다
2. 로컬 계층 이름 옆에 있는 을 클릭합니다 ⋮ .
3. 디스크 정보 * 탭을 선택합니다.

CLI를 참조하십시오

- CLI를 사용하여 디스크의 사용 가능한 공간을 결정합니다 *

사용 가능한 디스크 크기를 보려면 다음 단계를 수행하십시오.

단계

1. 스페어 디스크 정보 표시:

   '스토리지 집계 show-spare-disks'

RAID 그룹을 만들고 용량 요구 사항을 충족하는 데 필요한 디스크 또는 디스크 파티션 수 외에도 로컬 계층에 권장되는 최소 핫 스페어 디스크 또는 핫 스페어 디스크 파티션 수가 있어야 합니다.

- 모든 플래시 로컬 계층의 경우 핫 스페어 디스크 또는 디스크 파티션이 하나 이상 있어야 합니다.

  AFF C190에는 스페어 드라이브가 기본적으로 없습니다. 이 예외는 완전히 지원됩니다.

- 비플래시 동질적인 로컬 계층의 경우 핫 스페어 디스크 또는 디스크 파티션이 최소 2개 있어야 합니다.
- SSD 스토리지 풀의 경우 각 HA 쌍에 대해 하나 이상의 핫 스페어 디스크를 포함해야 합니다.
- Flash Pool 로컬 계층의 경우 각 HA 쌍에 대해 최소 2개의 스페어 디스크가 있어야 합니다. 에서 Flash Pool 로컬 계층에 대해 지원되는 RAID 정책에 대한 자세한 내용을 확인할 수 "Hardware Universe" 있습니다.
- 유지보수 센터의 사용을 지원하고 여러 개의 동시 디스크 장애로 인한 문제를 방지하려면 다중 디스크 캐리어에 최소 4개의 핫 스페어가 있어야 합니다.

관련 정보

- "NetApp Hardware Universe를 참조하십시오"
- "NetApp 기술 보고서 3838: 스토리지 서브시스템 구성 가이드"
- "스토리지 애그리게이트 보기"

ONTAP 로컬 계층을 생성하는 데 사용할 방법을 결정합니다

ONTAP는 로컬 계층을 자동으로 추가하기 위한 Best Practice 권장 사항을 제공하지만 권장 구성이 사용자 환경에서 지원되는지 여부를 결정해야 합니다. 그렇지 않은 경우 RAID 정책 및 디스크 구성에 대한 결정을 내린 다음 로컬 계층을 수동으로 생성해야 합니다.

로컬 계층이 자동으로 생성되면 ONTAP는 클러스터에서 사용 가능한 스페어 디스크를 분석하고 Best Practice에 따라 스페어 디스크를 사용하여 로컬 계층을 추가하는 방법에 대한 권장 사항을 생성합니다. ONTAP에서 권장 구성을 표시합니다. 권장 사항을 수락하거나 로컬 계층을 수동으로 추가할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

ONTAP 권장 사항을 수락하기 전에

다음 디스크 조건 중 하나라도 있는 경우 ONTAP의 권장 사항을 수락하기 전에 해결해야 합니다.

- 디스크가 누락되었습니다
- 스페어 디스크 숫자의 변동
- 할당되지 않은 디스크
- 제로화되지 않은 스페어
- 유지 관리 테스트를 진행 중인 디스크

수동 방법을 사용해야 하는 경우

대부분의 경우 로컬 계층의 권장 레이아웃은 사용자 환경에 가장 적합합니다. 그러나 환경에 다음 구성이 포함된 경우 수동 방법을 사용하여 로컬 계층을 생성해야 합니다.

ONTAP 9.11.1부터 System Manager를 사용하여 로컬 계층을 수동으로 추가할 수 있습니다.

- 타사 어레이 LUN을 사용하는 로컬 계층
- Cloud Volumes ONTAP 또는 ONTAP Select가 있는 가상 디스크
- MetroCluster 시스템
- SyncMirror
- mSATA 디스크
- Flash Pool 계층
- 노드에 여러 디스크 유형 또는 크기가 접속되어 있습니다

로컬 계층을 생성할 방법을 선택합니다

사용할 방법 선택:

- "로컬 계층을 자동으로 추가(생성"
- "로컬 계층을 수동으로 추가(생성)합니다"

관련 정보

- "ONTAP 명령 참조입니다"
- "스토리지 집계 자동 프로비저닝"

로컬 계층을 자동으로 추가하기 위해 ONTAP에서 제공하는 Best Practice 권장 사항이 환경에 적합한 경우 권장 사항을 수락하고 ONTAP에서 로컬 계층을 추가하도록 할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

시작하기 전에

디스크를 로컬 계층에서 사용하려면 먼저 노드에서 소유해야 합니다. 클러스터가 자동 디스크 소유권 할당을 사용하도록 구성되어 있지 않은 경우, 반드시 해야 "소유권을 수동으로 할당합니다"합니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

시스템 관리자

단계

1. System Manager에서 * Storage > Tiers * 를 클릭합니다.
2. Tiers * 페이지에서 을 클릭합니다

새 로컬 계층을 생성하려면 다음을 수행합니다.

   Add Local Tier * 페이지에는 노드에서 생성할 수 있는 권장 로컬 계층 수와 사용 가능한 스토리지가 표시됩니다.

3. System Manager에서 권장하는 구성을 보려면 * 권장 세부 정보 * 를 클릭하십시오.

   시스템 관리자는 ONTAP 9.8부터 다음과 같은 정보를 표시합니다.

   - * 로컬 계층 이름 * (ONTAP 9.10.1로 시작하는 로컬 계층 이름을 편집할 수 있음)
   - * 노드 이름 *
   - * 사용 가능한 크기 *
   - * 스토리지 유형 *

     ONTAP 9.10.1부터 추가 정보가 표시됩니다.

   - * 디스크 *: 디스크 수, 크기 및 유형을 표시합니다
   - * Layout *: RAID 그룹 레이아웃을 표시합니다. 여기에는 패리티 또는 데이터인 디스크와 사용하지 않는 슬롯이 포함됩니다.
   - * 스페어 디스크 *: 노드 이름, 스페어 디스크의 수와 크기 및 스토리지 유형을 표시합니다.
4. 다음 단계 중 하나를 수행합니다.

원하는 사항	그런 다음…
System Manager의 권장 사항을 수락합니다.	로 진행합니다 암호화를 위해 Onboard Key Manager를 구성하는 단계입니다.
로컬 계층을 수동으로 구성하고 *NOT * 는 System Manager의 권장 사항을 사용합니다.	"로컬 계층을 수동으로 추가합니다"다음으로 진행합니다. • ONTAP 9.10.1 이전 버전의 경우 CLI 사용 단계를 따릅니다. • ONTAP 9.11.1부터 시스템 관리자 사용 단계를 따릅니다.

5. [[step5-okm-encrypt](선택 사항): Onboard Key Manager가 설치된 경우 암호화를 위해 구성할 수 있습니다. 암호화에 대해 Onboard Key Manager 구성 * 확인란을 선택합니다.
   a. 암호를 입력합니다.
   b. 암호를 다시 입력하여 확인합니다.
   c. 시스템을 복구해야 하는 경우 나중에 사용할 수 있도록 암호를 저장합니다.

d. 나중에 사용할 수 있도록 키 데이터베이스를 백업합니다.

6. 저장 * 을 클릭하여 로컬 계층을 생성하고 스토리지 솔루션에 추가합니다.

CLI를 참조하십시오

`storage aggregate auto-provision`명령을 실행하여 로컬 계층 레이아웃 권장 사항을 생성합니다. 그런 다음 ONTAP 권장 사항을 검토하고 승인한 후에 로컬 계층을 생성할 수 있습니다.

이 작업에 대해

명령을 사용하여 생성된 기본 요약에는 `storage aggregate auto-provision` 이름 및 사용 가능한 크기 등 생성할 권장 로컬 계층이 나열됩니다. 목록을 보고 메시지가 표시되면 권장되는 로컬 계층을 생성할지 여부를 결정할 수 있습니다.

다음 보고서를 표시하는 '-verbose' 옵션을 사용하여 자세한 요약을 표시할 수도 있습니다.

- 로컬 계층 생성 후 스페어 생성, 검색된 스페어, 남은 스페어 디스크 및 파티션을 생성할 새 로컬 계층의 노드별 요약
- 사용할 디스크 및 파티션 수가 포함된 새로운 데이터 로컬 계층
- 생성할 새 데이터 로컬 계층에서 스페어 디스크 및 파티션을 사용하는 방법을 보여 주는 RAID 그룹 레이아웃입니다
- 로컬 계층 생성 후 남은 스페어 디스크 및 파티션에 대한 세부 정보입니다

자동 프로비저닝 방법에 익숙하고 환경이 올바르게 준비된 경우 옵션을 사용하여 표시 및 확인 없이 권장 로컬 계층을 생성할 수 `-skip-confirmation` 있습니다. `storage aggregate auto-provision`명령은 CLI 세션 설정의 영향을 받지 `-confirmations` 않습니다.

에 대한 자세한 내용은 `storage aggregate auto-provision` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 원하는 표시 옵션으로 'Storage aggregate auto-provision' 명령을 실행합니다.
   - 옵션 없음: 표준 요약을 표시합니다
   - '-verbose' 옵션: 상세 요약 표시
   - `-skip-confirmation` 옵션: 표시 또는 확인 없이 권장되는 로컬 계층을 생성합니다
2. 다음 단계 중 하나를 수행합니다.

원하는 사항	그런 다음…

ONTAP의 권장 사항을 수락합니다.	권장 로컬 계층 표시를 검토한 다음 권장 로컬 계층을 생성하라는 메시지에 응답합니다.
	
	`myA400-44556677::> storage aggregate auto-provision`
	`Node New Data Aggregate Usable Size`
	`---`
	`--- ---`
	`myA400-364 myA400_364_SSD_1 3.29TB`
	`myA400-363 myA400_363_SSD_1 1.46TB`
	`---`
	`--- ---`
	`Total: 2 new data aggregates 4.75TB`
	
	`Do you want to create recommended aggregates? {y`

n}: y Info: Aggregate auto provision has started. Use the "storage aggregate show-auto-provision-progress" command to track the progress. myA400-44556677::> ----	로컬 계층을 수동으로 구성하고 ONTAP의 권장 사항을 * *NOT** 사용하십시오.

관련 정보

- "ONTAP 명령 참조입니다"

ONTAP 로컬 계층을 수동으로 추가합니다

ONTAP의 Best Practice 권장 사항을 사용하여 로컬 계층을 추가하지 않으려면 프로세스를 수동으로 수행할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

시작하기 전에

디스크를 로컬 계층에서 사용하려면 먼저 노드에서 소유해야 합니다. 클러스터가 자동 디스크 소유권 할당을 사용하도록 구성되어 있지 않은 경우, 반드시 해야 "소유권을 수동으로 할당합니다"합니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

시스템 관리자

ONTAP 9.11.1부터, System Manager에서 권장하는 구성을 사용하여 로컬 계층을 생성하지 않으려면 원하는 구성을 지정할 수 있습니다.

단계

1. System Manager에서 * Storage > Tiers * 를 클릭합니다.
2. Tiers * 페이지에서 을 클릭합니다 + Add Local Tier 새 로컬 계층을 생성하려면 다음을 수행합니다.

   Add Local Tier * 페이지에는 노드에서 생성할 수 있는 권장 로컬 계층 수와 사용 가능한 스토리지가 표시됩니다.

3. System Manager가 로컬 계층에 대한 스토리지 권장 사항을 표시하면 * Spare Disks * 섹션에서 * Switch to Manual Local Tier Creation * 을 클릭합니다.

   로컬 계층 추가 * 페이지에는 로컬 계층을 구성하는 데 사용하는 필드가 표시됩니다.

4. Add Local Tier * 페이지의 첫 번째 섹션에서 다음을 완료합니다.
   a. 로컬 계층의 이름을 입력합니다.
   b. (선택 사항): 로컬 계층을 미러링하려면 * 이 로컬 계층 미러링 * 확인란을 선택합니다.
   c. 디스크 유형을 선택합니다.
   d. 디스크 수를 선택합니다.
5. RAID 구성* 섹션에서 다음 작업을 완료합니다.
   a. RAID 유형을 선택합니다.
   b. RAID 그룹 크기를 선택합니다.
   c. RAID allocation(RAID 할당) 을 클릭하여 그룹에서 디스크가 할당되는 방식을 확인합니다.
6. (선택 사항): Onboard Key Manager가 설치된 경우, 페이지의 * Encryption * 섹션에서 암호화를 위해 구성할 수 있습니다. 암호화에 대해 Onboard Key Manager 구성 * 확인란을 선택합니다.
   a. 암호를 입력합니다.
   b. 암호를 다시 입력하여 확인합니다.
   c. 시스템을 복구해야 하는 경우 나중에 사용할 수 있도록 암호를 저장합니다.
   d. 나중에 사용할 수 있도록 키 데이터베이스를 백업합니다.
7. 저장 * 을 클릭하여 로컬 계층을 생성하고 스토리지 솔루션에 추가합니다.

CLI를 참조하십시오

로컬 계층을 수동으로 생성하기 전에 디스크 구성 옵션을 검토하고 생성을 시뮬레이션해야 합니다.

그런 다음 'Storage aggregate create' 명령을 실행하여 결과를 확인할 수 있습니다.

시작하기 전에

로컬 계층에 필요한 디스크 수와 핫 스페어 디스크 수를 결정해야 합니다.

이 작업에 대해

루트 데이터 데이터 파티셔닝이 활성화되어 있고 구성에 24개 SSD(Solid State Drive)가 더 적은 경우 데이터 파티션을 다른 노드에 할당하는 것이 좋습니다.

루트 데이터 파티셔닝과 루트 데이터 파티셔닝이 설정된 시스템에서 로컬 계층을 생성하는 절차는 분할되지 않은 디스크를 사용하여 시스템에서 로컬 계층을 생성하는 절차와 같습니다. 시스템에서 루트 데이터 파티셔닝이 활성화되어 있는 경우 옵션에 디스크 파티션 수를 사용해야 `-diskcount` 합니다. 루트-데이터-데이터 파티셔닝의 경우 `-diskcount` 옵션은 사용할 디스크 수를 지정합니다.

FlexGroup 볼륨과 함께 사용할 여러 로컬 계층을 생성할 경우 로컬 계층의 크기가 최대한 비슷해야 합니다.

및 로컬 계층 생성 옵션 및 요구 사항에 대한 자세한 `storage aggregate create` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

단계

1. 스페어 디스크 파티션 목록을 보고 로컬 계층을 생성할 수 있는 충분한 공간이 있는지 확인합니다.

   'Storage aggregate show-spare-disks-original-owner_node_name_'

   데이터 파티션은 Local Data Usable 아래에 표시됩니다. 루트 파티션은 스페어로 사용할 수 없습니다.

2. 로컬 계층 생성을 시뮬레이션합니다.

   '스토리지 집계 create-aggregate_aggregate_name_-node_node_name_-raidtype RAID_DP -diskcount_number_of_disks_or_partitions_-simulate true'

3. 시뮬레이트된 명령에서 경고가 표시되는 경우 명령을 조정하고 시뮬레이션을 반복합니다.
4. 로컬 계층 생성:

   '스토리지 집계 create-aggregate_agr_name_-node_node_name_-raidtype RAID_DP-diskcount_number_of_disks_or_partitions_'

5. 로컬 계층을 표시하여 생성되었는지 확인합니다.

   'Storage aggregate show-status_aggregate_name_'

관련 정보

- "스토리지 애그리게이트 보기"

SyncMirror 활성화된 **ONTAP** 로컬 계층 추가

로컬 계층을 수동으로 생성할 때 SyncMirror 활성화하여 로컬 계층 데이터를 동기적으로 미러링할 수 있습니다.

자세히 알아보세요 "미러링 및 미러링되지 않은 로컬 계층" .

시작하기 전에

- 클러스터는 내부 저장소만으로 초기화되어야 합니다.
- 두 노드 모두에서 클러스터 설정이 완료되어야 합니다.

이 작업에 대해

이 절차는 각 클러스터 노드에 동일한 크기의 미러링된 데이터 로컬 계층을 생성하며, 각 로컬 계층의 디스크 수는 44개입니다.

단계

1. 저장소 자동 할당 비활성화:

   ```
   storage disk option modify -node * -autoassign off
   ```

2. 자동 할당이 비활성화되었는지 확인하세요.

   '스토리지 디스크 옵션 표시'

3. 외부 선반을 부착합니다.
4. 풀 1을 지정하여 각 노드에 외부 드라이브를 할당합니다.

   ```
   storage disk assign -disk <disk ID> -owner <node name> -pool 1
   ```

5. 각 노드에서 루트 로컬 계층을 미러링합니다.

   ```
   storage aggregate mirror -aggregate <node1 root-aggr>

   storage aggregate mirror -aggregate <node2 root-aggr>
   ```

   ⓘ 풀 1의 드라이브는 플렉스 0의 드라이브와 일치하도록 자동으로 분할됩니다.

6. 노드 1에서 디스크 수를 44개로 설정하여 미러링된 데이터 로컬 계층을 만듭니다. 이렇게 하면 풀 0에서 22개의 파티션이 선택되고, 풀 1에서 22개의 파티션이 선택됩니다.

   ```
   storage aggregate create -node <node1 name> -aggregate <node1 aggr-name>
   -diskcount 44 -mirror true
   ```

7. 노드 2에서 디스크 수를 44개로 설정하여 미러링된 데이터 로컬 계층을 만듭니다. 이렇게 하면 풀 0에서 22개의 파티션이 선택되고, 풀 1에서 22개의 파티션이 선택됩니다.

   ```
   storage aggregate create -node <node2 name> -aggregate <node2 aggr-name>
   -diskcount 44 -mirror true
   ```

8. 동일한 크기의 로컬 계층이 성공적으로 생성되었는지 확인하세요.

   '스토리지 집계 쇼'

관련 정보

- "저장 디스크 할당"
- "저장 디스크 옵션 수정"
- "저장 디스크 옵션 표시"

ONTAP 로컬 계층의 이름을 바꿉니다

로컬 계층의 이름을 바꿀 수 있습니다. 수행할 방법은 사용하는 인터페이스에 따라 다릅니다. - System Manager 또는 CLI입니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

시스템 관리자

- System Manager를 사용하여 로컬 계층의 이름을 바꿉니다. *

ONTAP 9.10.1부터 로컬 계층의 이름을 수정할 수 있습니다.

단계

1. System Manager에서 * Storage > Tiers * 를 클릭합니다.
2. 로컬 계층 이름 옆에 있는 을 클릭합니다 ⋮ .
3. 이름 바꾸기 * 를 선택합니다.
4. 로컬 계층의 새 이름을 지정합니다.

CLI를 참조하십시오

- CLI를 사용하여 로컬 계층의 이름을 바꿉니다 *

단계

1. CLI를 사용하여 로컬 계층의 이름을 다음과 같이 변경합니다.

   'Storage aggregate rename - aggregate_agr-name_-newname_aggr-new-name_'

   다음 예에서는 ""aggr5""라는 이름의 집계 이름을 "Sales-aggr"로 바꿉니다.

   ```
   > storage aggregate rename -aggregate aggr5 -newname sales-aggr
   ```

관련 정보

- "저장소 집계 이름 바꾸기"

ONTAP 로컬 계층의 미디어 비용을 설정합니다

ONTAP 9.11.1부터 System Manager를 사용하여 로컬 계층의 미디어 비용을 설정할 수 있습니다.

단계

1. System Manager에서 * 스토리지 > 계층 * 을 클릭한 다음, 원하는 로컬 계층 타일에서 * 미디어 비용 설정 * 을

클릭합니다.

2. 비교를 활성화하려면 * 활성 및 비활성 계층 * 을 선택합니다.
3. 통화 유형 및 금액을 입력합니다.

미디어 비용을 입력하거나 변경하면 모든 미디어 유형에 변경 사항이 적용됩니다.

ONTAP 드라이브를 수동으로 빠르게 **0**으로 설정합니다

ONTAP 9.4 이상 버전이 새로 설치된 시스템에서 ONTAP 9.4 이상으로 시스템이 재초기화되는 경우 _fast zeroing_을 사용하여 드라이브를 제로화할 수 있습니다.

빠른 제로화 _ 를 사용하면 드라이브가 초 내에 제로화됩니다. 이 작업은 프로비저닝 전에 자동으로 수행되며, 스페어 드라이브가 추가될 때 시스템 초기화, 로컬 계층 생성 또는 로컬 계층 확장에 걸리는 시간을 크게 줄여줍니다.

_Fast zeroing_은 SSD와 HDD에서 모두 지원됩니다.

_Fast zeroing_은 ONTAP 9.3 이전 버전에서 업그레이드된 시스템에서는 지원되지 않습니다. ONTAP 9.4 이상을 새로 설치하거나 시스템을 다시 초기화해야 합니다. 또한 ONTAP 9.3 이하에서는 ONTAP에 의해 드라이브가 자동으로 제로화되지만 프로세스가 더 오래 걸립니다.

드라이브를 수동으로 제로화할 필요가 있는 경우 다음 방법 중 하나를 사용할 수 있습니다. ONTAP 9.4 이상에서는 수동으로 드라이브를 제로화하는 데 몇 초 밖에 걸리지 않습니다.

CLI 명령

- CLI 명령을 사용하여 드라이브를 빠르게 제로합니다 *

이 작업에 대해

이 명령을 사용하려면 관리자 권한이 필요합니다.

단계

1. CLI 명령을 입력합니다.

```
storage disk zerospares
```

부팅 메뉴 옵션

- 부팅 메뉴에서 옵션을 선택하여 드라이브를 빠르게 제로화 * 합니다

이 작업에 대해

- 빠른 제로화 기능 향상은 ONTAP 9.4 이전의 릴리즈에서 업그레이드된 시스템을 지원하지 않습니다.

단계

1. 부팅 메뉴에서 다음 옵션 중 하나를 선택합니다.
   - (4) 구성을 청소하고 모든 디스크를 초기화합니다
   - (9a) 모든 디스크의 파티션을 해제하고 해당 소유권 정보를 제거합니다
   - (9b) 전체 디스크로 구성 정리 및 노드 초기화

관련 정보

- "저장 디스크 제로 스페어"

ONTAP 디스크 소유권을 수동으로 할당합니다

디스크를 로컬 계층에서 사용하려면 먼저 노드에서 소유해야 합니다.

이 작업에 대해

- 초기화되지 않고 DS460C 쉘프만 없는 HA 쌍에서 소유권을 수동으로 할당하는 경우 옵션 1을 사용합니다.
- DS460C 쉘프만 있는 HA 쌍을 초기화하는 경우 옵션 2를 사용하여 루트 드라이브에 대한 소유권을 수동으로 할당합니다.

옵션 **1:** 대부분의 **HA** 쌍

초기화되지 않고 DS460C 쉘프만 없는 HA 쌍의 경우 다음 절차를 사용하여 소유권을 수동으로 할당할 수 있습니다.

이 작업에 대해

- 소유권을 할당할 디스크는 소유권을 할당할 노드에 물리적으로 케이블로 연결된 셸프에 있어야 합니다.
- 로컬 계층(집계)에서 디스크를 사용하는 경우:
  - 디스크를 로컬 계층(애그리게이트)에서 사용하려면 먼저 노드가 디스크를 소유해야 합니다.
  - 로컬 계층(집계)에서 사용 중인 디스크의 소유권을 재할당할 수 없습니다.

단계

1. CLI를 사용하여 소유하지 않은 모든 디스크를 표시합니다.

   스토리지 디스크 show-container-type unassigned

2. 각 디스크 할당:

   'Storage disk assign-disk_name_-owner_owner_name_'

   와일드카드 문자를 사용하여 한 번에 두 개 이상의 디스크를 할당할 수 있습니다. 다른 노드에 이미 있는 스페어 디스크를 재할당하는 경우 ""-force" 옵션을 사용해야 합니다.

옵션 **2: DS460C** 쉘프만 있는 **HA** 쌍

초기화 중이며 DS460C 쉘프만 있는 HA 쌍의 경우 다음 절차를 사용하여 루트 드라이브에 대한 소유권을 수동으로 할당합니다.

이 작업에 대해

- DS460C 쉘프만 포함된 HA 쌍을 초기화할 경우, 절반 드로어 정책을 준수하도록 루트 드라이브를 수동으로 할당해야 합니다.

  HA Pair 초기화(부팅) 후 디스크 소유권 자동 할당이 자동으로 활성화되고 하프 드로어 정책을 사용하여 나머지 드라이브(루트 드라이브 제외) 및 나중에 추가된 드라이브(예: 장애가 발생한 디스크 교체, "스페어 부족" 메시지에 대한 응답 또는 용량 추가)에 소유권을 할당합니다.

  "하프 드로어 정책에 대해 알아봅니다"..

- RAID에는 DS460C 쉘프에 있는 8TB NL-SAS 드라이브 이상의 각 HA 쌍에 대해 최소 10개의 드라이브(노드당 5개)가 필요합니다.

단계

1. DS460C 선반이 완전히 채워지지 않은 경우 다음 하위 단계를 완료하십시오. 그렇지 않으면 다음 단계로 이동합니다.

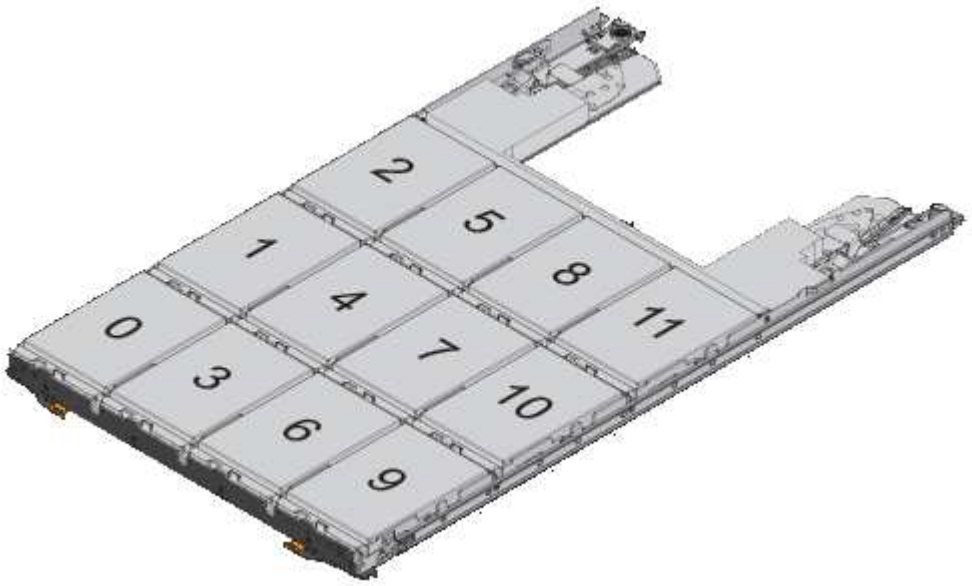
   a. 먼저 각 드로어의 첫 줄(드라이브 베이 0, 3, 6, 9)에 드라이브를 설치합니다.

      각 드로어의 첫 행에 드라이브를 설치하면 공기가 적절하게 흐르고 과열이 방지됩니다.

   b. 나머지 드라이브의 경우 각 드로어에 균등하게 분배합니다.

      서랍을 앞쪽에서 뒤쪽으로 채웁니다. 행을 채울 만큼 충분한 드라이브가 없는 경우, 드라이브가 드로어의 왼쪽과 오른쪽에 균일하게 오도록 쌍으로 설치하십시오.

      다음 그림에서는 DS460C 드로어의 드라이브 베이 번호 및 위치를 보여 줍니다.



2. 노드 관리 LIF 또는 클러스터 관리 LIF를 사용하여 클러스터 쉘에 로그인합니다.

3. 다음 하위 단계를 사용하여 각 드로어의 루트 드라이브를 수동으로 할당하여 하프 드로어 정책을 준수합니다.

   하프 드로어 정책에서는 드로어 드라이브의 왼쪽 절반(베이 0 ~ 5)을 노드 A에 할당하고 드로어 드라이브의 오른쪽 절반(베이 6 ~ 11)을 노드 B에 할당합니다

   a. 소유되지 않은 모든 디스크 표시:
      `storage disk show -container-type unassigned`
   b. 루트 디스크 할당:
      `storage disk assign -disk disk_name -owner owner_name`

      와일드카드 문자를 사용하여 한 번에 두 개 이상의 디스크를 할당할 수 있습니다.

에 대한 자세한 내용은 `storage disk` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "저장 디스크 할당"
- "저장 디스크 표시"

ONTAP 로컬 계층의 드라이브 및 **RAID** 그룹 정보를 확인합니다

일부 로컬 계층 관리 작업에는 로컬 계층을 구성하는 드라이브 유형, 크기, 체크섬 및 상태, 다른 로컬 계층과 공유되는지 여부, RAID 그룹의 크기 및 구성을 알아야 합니다.

단계

1. 로컬 계층의 드라이브를 RAID 그룹별로 표시합니다.

   'Storage aggregate show-status_aggr_name_'

   로컬 계층의 각 RAID 그룹에 대한 드라이브가 표시됩니다.

   '위치' 열에서 드라이브의 RAID 유형(데이터, 패리티, dparity)을 확인할 수 있습니다. Position 열에 'Shared'가 표시되면 드라이브가 공유되고 HDD인 경우 분할된 디스크이고, SSD인 경우 스토리지 풀의 일부입니다.

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11       0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13       0   SSD       -  186.2GB  745.2GB (normal)
     shared   2.0.12       0   SSD       -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

관련 정보

- "스토리지 집계 표시 상태"

SVM(스토리지 VM)에 ONTAP 로컬 계층 할당

스토리지 가상 머신(스토리지 VM 또는 SVM, 이전의 Vserver)에 하나 이상의 로컬 계층을 할당하는 경우 해당 스토리지 VM(SVM)의 볼륨을 포함하는 로컬 계층만 사용할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

시작하기 전에

스토리지 VM에 할당할 스토리지 VM과 로컬 계층이 이미 있어야 합니다.

이 작업에 대해

스토리지 VM에 로컬 계층을 할당하면 스토리지 VM이 서로 격리되도록 할 수 있습니다. 이는 멀티 테넌시 환경에서

특히 중요합니다.

단계

1. SVM에 이미 할당된 로컬 계층 목록을 확인하십시오.

   'vserver show-fields aggr-list'를 선택합니다

   SVM에 현재 할당된 로컬 계층이 표시됩니다. 할당된 로컬 계층이 없는 경우 – 이 표시됩니다.

2. 요구사항에 따라 다음과 같이 할당된 로컬 계층을 추가 또는 제거합니다.

원하는 작업	이 명령 사용…
추가 로컬 계층을 할당합니다	'vserver add-aggregate'를 선택합니다
로컬 계층의 할당을 취소합니다	'vserver remove-aggregate'

   나열된 로컬 계층이 SVM에 할당되거나 SVM에서 제거됩니다. SVM에 할당되지 않은 애그리게이트를 사용하는 볼륨이 SVM에 이미 있는 경우 경고 메시지가 표시되지만 명령이 성공적으로 완료됩니다. SVM에 이미 할당되었고 명령에 이름을 지정하지 않은 로컬 계층은 영향을 받지 않습니다.

예

다음 예에서는 로컬 계층 aggr1 및 aggr2가 SVM svm1에 할당됩니다.

'vserver add-aggregate-vserver svm1 - aggr1, aggr2'

ONTAP 로컬 계층에 상주하는 볼륨을 확인합니다

로컬 계층에 대해 작업을 수행하기 전에 재배치 또는 오프라인 상태로 전환 등의 작업을 수행하기 전에 로컬 계층에 상주하는 볼륨을 확인해야 할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

단계

1. 로컬 계층에 있는 볼륨을 표시하려면 를 입력합니다

   'volume show-aggregate aggregate_name'입니다

   지정된 로컬 계층에 있는 모든 볼륨이 표시됩니다.

ONTAP 로컬 계층에 있는 볼륨의 공간 사용량을 확인하고 제어합니다

로컬 계층에서 가장 많은 공간을 사용하는 FlexVol 볼륨과 특히 볼륨 내의 기능을 확인할 수 있습니다.

`volume show-footprint`명령은 볼륨의 설치 공간 또는 포함된 로컬 계층 내의 공간 사용에 대한 정보를 제공합니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

`volume show-footprint`명령을 실행하면 오프라인 볼륨을 비롯하여 로컬 계층에 있는 각 볼륨의 공간 사용에 대한 세부 정보가 표시됩니다. 이 명령은 및 `aggregate show-space` 명령의 출력 사이의 간격을 `volume show-space` 연결합니다. 모든 백분율은 로컬 계층 크기의 백분율로 계산됩니다.

다음 예에서는 testvol이라는 볼륨에 대한 'volume show-footprint' 명령 출력을 보여 줍니다.

```
cluster1::> volume show-footprint testvol

      Vserver : thevs
      Volume  : testvol

      Feature                                     Used    Used%
      --------------------------------    ----------    -----
      Volume Data Footprint                    120.6MB       4%
      Volume Guarantee                          1.88GB      71%
      Flexible Volume Metadata                 11.38MB       0%
      Delayed Frees                             1.36MB       0%
      Total Footprint                           2.01GB      76%
```

다음 표에서는 'volume show-footprint' 명령의 출력 중 일부 주요 행과 해당 기능을 통해 공간 사용을 줄이기 위해 수행할 수 있는 작업을 설명합니다.

행/피처 이름	행의 설명/내용	줄일 수 있는 방법이 있습니다
'볼륨 데이터 사용 공간'	활성 파일 시스템에 있는 볼륨의 데이터에 의해 포함된 로컬 계층에서 사용된 총 공간 및 볼륨의 스냅숏에 사용된 공간입니다. 이 행에는 예약된 공간이 포함되지 않습니다.	• 볼륨에서 데이터를 삭제하는 중입니다. • 볼륨에서 스냅샷을 삭제하는 중입니다.
볼륨 보증	로컬 계층의 볼륨에서 향후 쓰기를 위해 예약한 공간의 양입니다. 예약된 공간의 양은 볼륨의 보장 유형에 따라 다릅니다.	보장 유형을 없음으로 변경합니다.

'유연한 볼륨 메타데이터'	로컬 계층에서 볼륨의 메타데이터 파일이 사용하는 총 공간입니다.	제어할 직접적인 방법이 없습니다.
'해방된'	ONTAP이 성능에 사용했으며 즉시 해제할 수 없는 블록입니다. SnapMirror 대상의 경우 이 행의 값은 "0"이며 표시되지 않습니다.	제어할 직접적인 방법이 없습니다.
파일 작업 메타데이터	파일 작업 메타데이터에 예약된 총 공간입니다.	제어할 직접적인 방법이 없습니다.
토털 풋프린트	로컬 계층에서 볼륨이 사용하는 총 공간입니다. 모든 행의 합계입니다.	볼륨에서 사용하는 공간을 줄이는 데 사용되는 모든 방법

관련 정보

"NetApp 기술 보고서 3483: NetApp SAN 또는 IP SAN 엔터프라이즈 환경에서 씬 프로비저닝"

ONTAP 로컬 계층의 공간 사용량을 확인합니다

하나 이상의 로컬 계층에 있는 모든 볼륨에서 사용되는 공간을 확인하여 추가 공간을 확보하기 위한 조치를 취할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

WAFL는 로컬 계층 레벨 메타데이터 및 성능을 위해 총 디스크 공간의 비율을 예약합니다. 로컬 계층에서 볼륨을 유지하는 데 사용된 공간은 WAFL 예비 공간을 벗어나서 변경할 수 없습니다.

30TB 미만의 로컬 계층에서는 WAFL가 로컬 계층 수준 메타데이터 및 성능을 위해 총 디스크 공간의 10%를 예약합니다.

ONTAP 9.12.1부터 30TB 이상의 로컬 계층에서는 로컬 계층 수준 메타데이터 및 성능을 위해 예약된 디스크 공간이 줄어들기 때문에 로컬 계층에서 사용 가능한 공간이 5% 더 많아집니다. 절약되는 공간의 가용성은 해당 플랫폼 및 ONTAP 버전에 따라 다릅니다.

로컬 계층에서 **ONTAP**가 예약한 디스크 공간 **30TB** 이상	플랫폼에 적용됩니다	**ONTAP** 버전
5%	알아봅니다 AFF FAS	ONTAP 9.14.1 이상
5%	AFF 플랫폼 및 FAS500f 플랫폼	ONTAP 9.12.1 이상
10%	모든 플랫폼	ONTAP 9.11.1 이상

명령을 사용하여 하나 이상의 로컬 계층에 있는 모든 볼륨의 공간 사용량을 볼 수 있습니다 `aggregate show-space`. 이렇게 하면 포함된 로컬 계층에서 가장 많은 공간을 사용하고 있는 볼륨을 확인하여 더 많은 공간을 확보하기 위한 조치를 취할 수 있습니다.

로컬 계층에서 사용된 공간은 포함된 FlexVol 볼륨에서 사용된 공간의 영향을 직접 받습니다. 볼륨에서 공간을 늘리기

위해 취한 조치는 로컬 계층의 공간에도 영향을 줍니다.

ONTAP 9.15.1부터 두 개의 새로운 메타데이터 카운터를 사용할 수 있습니다. 여러 기존 카운터의 변경 사항과 함께 할당된 사용자 데이터의 양을 보다 명확하게 확인할 수 있습니다. 자세한 내용은 을 "볼륨 또는 로컬 계층의 공간 사용량을 확인합니다" 참조하십시오.

다음 행은 'aggregate show-space' 명령 출력에 포함됩니다.

- * 볼륨 풋프린트 *

  로컬 계층 내의 모든 볼륨 사용 공간의 총합입니다. 포함하는 로컬 계층에 있는 모든 볼륨의 모든 데이터와 메타데이터에 의해 사용되거나 예약되는 모든 공간이 포함됩니다.

- * 집계 메타데이터 *

  할당 비트맵 및 inode 파일과 같이 로컬 계층에 필요한 총 파일 시스템 메타데이터입니다.

- * 스냅숏 예비 공간 *

  볼륨 크기를 기준으로 로컬 계층 스냅샷에 예약된 공간의 양입니다. 사용된 공간으로 간주되며 볼륨 또는 로컬 계층 데이터 또는 메타데이터에 사용할 수 없습니다.

- * Snapshot Reserve Unusable(스냅샷 예비 공간 사용 불가

  로컬 계층 스냅샷 예약에 원래 할당되었지만 로컬 계층 스냅샷에 사용할 수 없는 공간의 양입니다. 로컬 계층과 연결된 볼륨에서 사용되고 있기 때문입니다. 0이 아닌 로컬 계층 스냅숏 예비 공간이 있는 로컬 계층에 대해서만 발생할 수 있습니다.

- * 총 사용량 *

  볼륨, 메타데이터 또는 스냅샷별로 로컬 계층에서 사용되거나 예약된 모든 공간의 합계입니다.

- * 총 물리적 사용량 *

  현재 데이터에 사용 중인 공간(향후 사용을 위해 예약되지 않음). 로컬 계층 스냅샷에 사용되는 공간이 포함됩니다.

다음 예에서는 스냅숏 예비 공간이 5%인 로컬 계층에 대한 명령 출력을 보여 `aggregate show-space` 줍니다. 스냅숏 예비 공간이 0인 경우 행이 표시되지 않습니다.

```
cluster1::> storage aggregate show-space

                        Aggregate : wqa_gx106_aggr1

      Feature                                   Used      Used%
      --------------------------------    ----------     ------
      Volume Footprints                       101.0MB         0%
      Aggregate Metadata                        300KB         0%
      Snapshot Reserve                         5.98GB         5%

      Total Used                               6.07GB         5%
      Total Physical Used                     34.82KB         0%
```

관련 정보

- "Knowledge Base 문서: 공간 사용"
- "ONTAP 9.12.1로 업그레이드하여 스토리지 용량의 5%를 확보하십시오"
- "저장 집합 쇼 공간"

HA 쌍 내에서 **ONTAP** 로컬 계층의 소유권을 이동합니다

로컬 계층에서 서비스를 중단하지 않고 HA 쌍의 노드 간에 로컬 계층의 소유권을 변경할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

HA 쌍의 두 노드는 서로의 디스크 또는 어레이 LUN에 물리적으로 연결됩니다. 각 디스크 또는 어레이 LUN은 노드 중 하나가 소유합니다.

테이크오버가 발생하면 로컬 계층 내의 모든 디스크 또는 스토리지 LUN의 소유권이 한 노드에서 다른 노드로 일시적으로 변경됩니다. 그러나 로컬 계층 재배치 작업은 소유권을 영구적으로 변경할 수도 있습니다(예: 로드 밸런싱에 대해 수행된 경우). 데이터 복제 프로세스나 디스크 또는 어레이 LUN의 물리적 이동 없이 소유권이 변경됩니다.

이 작업에 대해

- 로컬 계층 재배치 작업 중에 볼륨 수 제한이 프로그래밍 방식으로 검사되므로 수동으로 확인할 필요가 없습니다.

  볼륨 수가 지원되는 제한을 초과하면 로컬 계층 재배치 작업이 실패하고 관련 오류 메시지가 표시됩니다.

- 소스 또는 대상 노드에서 시스템 레벨 작업이 진행 중인 경우에는 로컬 계층 재배치를 시작하지 않아야 합니다. 마찬가지로 로컬 계층 재배치 중에는 이러한 작업을 시작하지 않아야 합니다.

  이러한 작업에는 다음이 포함될 수 있습니다.

  - 테이크오버
  - 반환

- 종료
- 다른 로컬 계층 재배치 작업
- 디스크 소유권이 변경됩니다
- 로컬 계층 또는 볼륨 구성 작업
- 스토리지 컨트롤러 교체
- ONTAP 업그레이드
- ONTAP 복원

- MetroCluster 구성이 있는 경우 재해 복구 작업(*switchover*,*recovery* 또는 스위치백)이 진행 중인 동안에는 로컬 계층 재배치를 시작하지 않아야 합니다.
- MetroCluster 구성이 있고 전환된 로컬 계층에서 로컬 계층 재배치를 시작하는 경우 DR 파트너의 볼륨 제한 수를 초과하기 때문에 작업이 실패할 수 있습니다.
- 손상되었거나 유지 보수 중인 로컬 계층에 대해 로컬 계층 재배치를 시작해서는 안 됩니다.
- 로컬 계층 재배치를 시작하기 전에 소스 및 대상 노드에 코어 덤프를 저장해야 합니다.

단계

1. 노드의 로컬 계층을 확인하여 이동할 로컬 계층을 확인하고 해당 계층이 온라인 상태이고 양호한 상태인지 확인합니다.

   'Storage aggregate show -node_source-node_'

   다음 명령은 클러스터의 4개 노드에 있는 6개의 로컬 계층을 보여 줍니다. 모든 로컬 계층이 온라인 상태입니다. 노드 1과 노드 3은 HA 쌍을 형성하고 노드 2와 노드 4는 HA 쌍을 형성합니다.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_4     239.0GB   238.9GB    0% online       5 node3  raid_dp,
                                                         normal
aggr_5     239.0GB   239.0GB    0% online       4 node4  raid_dp,
                                                         normal
6 entries were displayed.
```

2. 명령을 실행하여 로컬 계층 재배치를 시작합니다.

   'Storage aggregate Relocation start-aggregate-list_aggregate-1_,*aggregate-2*… -node_source-node_

-destination_destination-node_'입니다

다음 명령을 실행하면 로컬 계층 aggr_1 및 aggr_2가 Node1에서 Node3로 이동합니다. NODE3은 Node1의 HA 파트너입니다. HA 쌍 내에서만 로컬 계층을 이동할 수 있습니다.

```
cluster::> storage aggregate relocation start -aggregate-list aggr_1,
aggr_2 -node node1 -destination node3
Run the storage aggregate relocation show command to check relocation
status.
node1::storage aggregate>
```

3. 다음 명령을 사용하여 로컬 계층 재배치 진행 상황을 모니터링합니다 `storage aggregate relocation show`.

'Storage aggregate relocation show -node_source-node_'

다음 명령을 실행하면 Node3로 이동되는 로컬 계층의 진행률이 표시됩니다.

```
cluster::> storage aggregate relocation show -node node1
Source Aggregate   Destination    Relocation Status
------ ----------- -------------  ------------------------
node1
       aggr_1      node3          In progress, module: wafl
       aggr_2      node3          Not attempted yet
2 entries were displayed.
node1::storage aggregate>
```

재배치가 완료되면 이 명령의 출력에는 재배치 상태가 ""완료""인 각 로컬 계층이 표시됩니다.

관련 정보

- "저장소 집계 이전 표시"
- "저장소 집계 재배치 시작"
- "스토리지 애그리게이트 보기"

ONTAP 로컬 계층을 삭제합니다

로컬 계층에 볼륨이 없는 경우 로컬 계층을 삭제할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

`storage aggregate delete`명령은 스토리지 로컬 계층을 삭제합니다. 로컬 계층에 볼륨이 있는 경우 명령이 실패합니다. 로컬 계층에 객체 저장소가 연결되어 있는 경우 이 명령은 로컬을 삭제하는 것 외에 객체 저장소의 객체도 삭제합니다. 이 명령의 일부로 오브젝트 저장소 구성이 변경되지 않습니다.

다음 예제에서는 이름이 ""aggr1""인 로컬 계층을 삭제합니다.

```
> storage aggregate delete -aggregate aggr1
```

관련 정보

- "저장소 집계 삭제"

로컬 계층 재배치를 위한 **ONTAP** 명령입니다

HA 쌍 내에서 로컬 계층 소유권을 재배치하기 위한 특정 ONTAP 명령이 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

원하는 작업	이 명령 사용…
로컬 계층 재배치 프로세스를 시작합니다	'스토리지 집계 재배치 시작
로컬 계층 재배치 프로세스 모니터링	스토리지 골재 재배치 쇼

관련 정보

- "저장소 집계 이전 표시"
- "저장소 집계 재배치 시작"

로컬 계층 관리를 위한 **ONTAP** 명령

명령을 사용하여 `storage aggregate` 로컬 계층을 관리합니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

원하는 작업	이 명령 사용…
All Flash Pool 로컬 계층의 캐시 크기를 표시합니다	'Storage aggregate show-fields hybrid-cache-size-total-hybrid-cache-size-total > 0'

원하는 작업	이 명령 사용...
로컬 계층의 디스크 정보 및 상태를 표시합니다	'스토리지 집계 표시 상태'
노드별 스페어 디스크를 표시합니다	'스토리지 집계 show-spare-disks'
클러스터의 루트 로컬 계층을 표시합니다	'Storage aggregate show-has-mroot true'입니다
로컬 계층의 기본 정보 및 상태를 표시합니다	'스토리지 집계 쇼'
로컬 계층에 사용되는 스토리지의 유형을 표시합니다	'스토리지 집계 표시 필드 스토리지 유형'입니다
로컬 계층을 온라인으로 전환합니다	'Storage aggregate online
로컬 계층을 삭제합니다	'저장소 집계 삭제'
로컬 계층을 Restricted 상태로 전환합니다	'저장소 집계 제한'
로컬 계층의 이름을 바꿉니다	'저장소 집계 이름 바꾸기'
로컬 계층을 오프라인으로 전환합니다	'저장소 집계 오프라인'
로컬 계층의 RAID 유형을 변경합니다	'스토리지 집계 수정-raidtype'

관련 정보

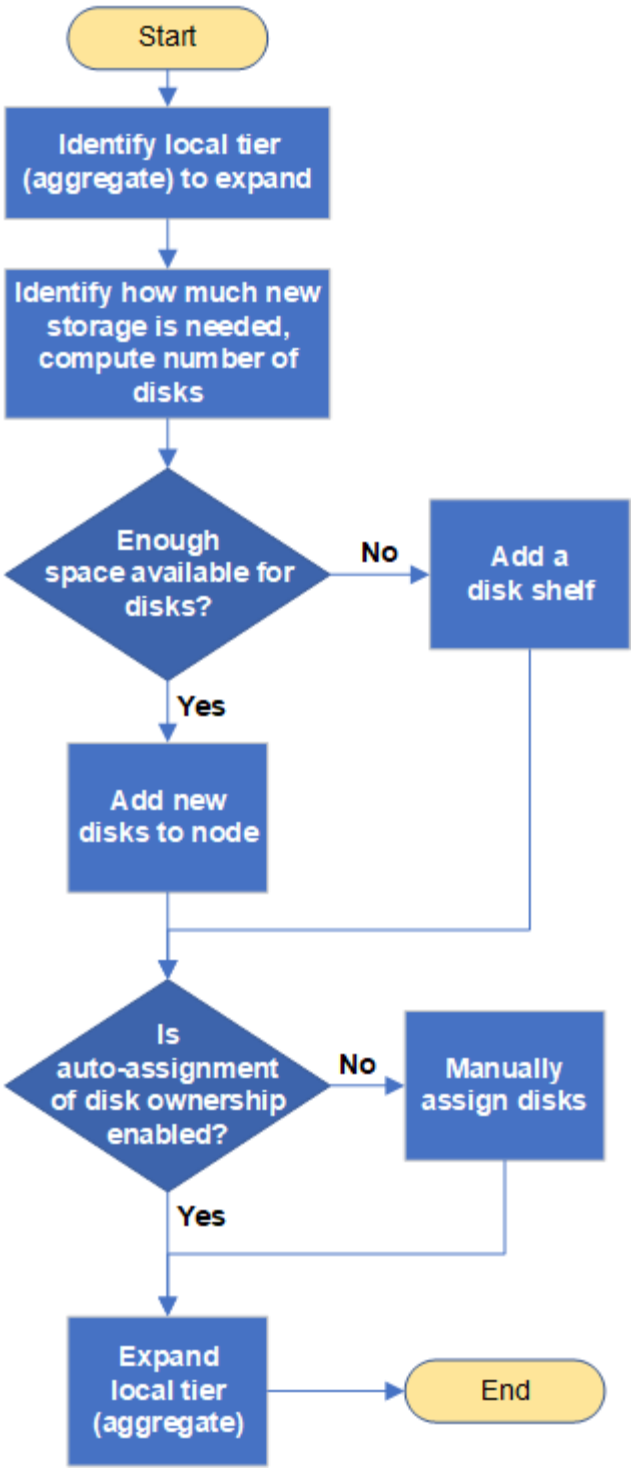
- "저장소 집계 삭제"
- "저장소 집계 수정"
- "저장소 집계 오프라인"
- "온라인 스토리지 집계"
- "저장소 집계 이름 바꾸기"
- "저장 집계 제한"
- "스토리지 애그리게이트 보기"

로컬 계층에 용량(디스크)을 추가합니다

ONTAP 로컬 계층에 용량을 추가하기 위한 워크플로우

로컬 계층에 용량을 추가하려면 먼저 추가할 로컬 계층을 식별하고, 필요한 새 스토리지를 결정하고, 새 디스크를 설치하고, 디스크 소유권을 할당하고, 필요한 경우 새 RAID 그룹을 생성해야 합니다.

System Manager 또는 ONTAP CLI를 사용하여 용량을 추가할 수 있습니다.



ONTAP 로컬 계층에 공간을 생성하는 방법입니다

로컬 계층에 사용 가능한 공간이 부족할 경우 데이터 손실부터 볼륨 보장을 해제하는 문제까지 다양한 문제가 발생할 수 있습니다. 로컬 계층에 더 많은 공간을 만드는 방법은 여러 가지가 있습니다.

모든 방법은 다양한 결과를 가지고 있습니다. 작업을 수행하기 전에 설명서의 관련 섹션을 읽어야 합니다.

다음은 가장 작은 결과부터 가장 큰 결과를 얻기 위해 로컬 계층에 공간을 만드는 몇 가지 일반적인 방법입니다.

- 로컬 계층에 디스크를 추가합니다.
- 일부 볼륨을 사용 가능한 공간이 있는 다른 로컬 계층으로 이동합니다.
- 로컬 계층에서 볼륨 보장 볼륨의 크기를 줄입니다.
- 볼륨의 보증 유형이 ""없음"인 경우 불필요한 볼륨 스냅샷을 삭제합니다.
- 불필요한 볼륨을 삭제합니다.
- 중복제거, 압축과 같은 공간 절약 기능을 지원합니다.
- (일시적으로) 많은 양의 메타데이터를 사용하는 기능을 사용하지 않도록 설정합니다.

ONTAP 로컬 계층에 용량을 추가합니다

연결된 볼륨에 더 많은 스토리지를 제공할 수 있도록 디스크를 로컬 계층에 추가할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

시스템 관리자**(ONTAP 9.8** 이상**)**

ONTAP 9.12.1부터 시스템 관리자를 사용하여 로컬 계층의 커밋된 용량을 보고 로컬 계층에 추가 용량이 필요한지 여부를 확인할 수 있습니다. 을 "System Manager에서 용량을 모니터링합니다 "참조하십시오.

단계

1. 스토리지 > 계층 * 을 선택합니다.
2. 용량을 추가할 로컬 계층의 이름 옆에 있는 을 선택합니다.
3. 용량 추가 * 를 선택합니다.

추가할 수 있는 스페어 디스크가 없는 경우 * Add Capacity * 옵션이 표시되지 않으며 로컬 계층의 용량을 늘릴 수 없습니다.

4. 설치된 ONTAP 버전에 따라 다음 단계를 수행하십시오.

이 버전의 ONTAP가 설치된 경우…	다음 단계를 수행합니다.
ONTAP 9.11.1부터 시작합니다	a. 디스크 유형과 디스크 수를 선택합니다. b. 새 RAID 그룹에 디스크를 추가하려면 확인란을 선택합니다. RAID 할당이 표시됩니다. c. 저장 * 을 선택합니다.
ONTAP 9.10.1, 9.9 또는 9.8	a. 노드에 여러 스토리지 계층이 포함된 경우 로컬 계층에 추가할 디스크 수를 선택합니다. 그렇지 않으면 노드에 단일 스토리지 계층만 포함된 경우 추가된 용량이 자동으로 추정됩니다. b. 추가 * 를 선택합니다.

5. (선택 사항) 이 프로세스를 완료하는 데 약간의 시간이 걸립니다. 백그라운드에서 프로세스를 실행하려면 * 백그라운드에서 실행 * 을 선택합니다.
6. 프로세스가 완료되면 * Storage > Tiers * 의 로컬 계층 정보에서 증가된 용량을 볼 수 있습니다.

시스템 관리자**(ONTAP 9.7** 이하**)**

단계

1. (ONTAP 9.7에만 해당) * (클래식 버전으로 돌아가기) * 를 선택합니다.
2. 하드웨어 및 진단 > 애그리게이트 * 를 선택합니다.
3. 용량 디스크를 추가할 로컬 계층을 선택한 다음 * Actions > Add Capacity * 를 선택합니다.

로컬 계층의 다른 디스크와 크기가 같은 디스크를 추가해야 합니다.

4. (ONTAP 9.7에만 해당) * 새 환경으로 전환 * 을 선택합니다.
5. 스토리지 > 계층 * 을 선택하여 새로운 로컬 계층의 크기를 확인합니다.

CLI를 참조하십시오

시작하기 전에

스토리지를 추가할 로컬 계층에 대한 RAID 그룹 크기를 알아야 합니다.

이 작업에 대해

분할된 디스크를 로컬 계층에 추가하는 절차는 분할되지 않은 디스크를 추가하는 절차와 비슷합니다.

로컬 계층을 확장할 때 파티션 또는 분할되지 않은 디스크를 로컬 계층에 추가하는지 여부를 확인해야 합니다. 파티셔닝되지 않은 드라이브를 기존 로컬 계층에 추가하면 기존 RAID 그룹의 크기가 새 RAID 그룹에 상속되어 필요한 패리티 디스크 수에 영향을 줄 수 있습니다. 분할되지 않은 디스크가 분할된 디스크로 구성된 RAID 그룹에 추가되는 경우 새 디스크는 분할되어 사용되지 않은 스페어 파티션을 남겨둡니다.

파티션을 프로비저닝할 때 두 파티션이 모두 스페어로 된 드라이브 없이 노드를 떠나지 않도록 해야 합니다. 이렇게 하면 노드에 컨트롤러 중단이 발생할 경우 문제(코어 파일)에 대한 중요 정보를 기술 지원 팀에 제공하지 못할 수 있습니다.

단계

1. 로컬 계층을 소유하는 시스템에서 사용 가능한 스페어 스토리지를 표시합니다.

   'Storage aggregate show-spare-disks-original-owner_node_name_'

   '-is-disk-shared' 매개 변수를 사용하여 분할된 드라이브만 표시하거나 분할되지 않은 드라이브만 표시할 수 있습니다.

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
  Shared HDD Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                       Type     RPM Checksum         Usable
Usable     Size Status
 -------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                      BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.2                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.3                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.4                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.8                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.9                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.10                     BSAS    7200 block                0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

2. 로컬 계층에 대한 현재 RAID 그룹을 표시합니다.

```
storage aggregate show-status <aggr_name>
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                                 Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ----------- ---- ----- ------ -------- --------
----------
     shared   1.0.10        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.5         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.6         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.11        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.0         0   BSAS    7200  753.8GB  828.0GB
(normal)
5 entries were displayed.
```

3. 스토리지에 Aggregate를 추가하는 시뮬레이션:

```
storage aggregate add-disks -aggregate <aggr_name> -diskcount
<number_of_disks_or_partitions> -simulate true
```

실제로 스토리지를 프로비저닝하지 않고 스토리지를 추가한 결과를 볼 수 있습니다. 시뮬레이트된 명령에서 경고가 표시되는 경우 명령을 조정하고 시뮬레이션을 반복할 수 있습니다.

```
cl1-s2::> storage aggregate add-disks -aggregate aggr_test
-diskcount 5 -simulate true

Disks would be added to aggregate "aggr_test" on node "cl1-s2" in
the
following manner:

First Plex

  RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                        Usable
Physical
    Position   Disk                      Type           Size
Size
    ---------- ------------------------- ---------- --------
--------
    shared     1.11.4                    SSD         415.8GB
415.8GB
    shared     1.11.18                   SSD         415.8GB
415.8GB
    shared     1.11.19                   SSD         415.8GB
415.8GB
    shared     1.11.20                   SSD         415.8GB
415.8GB
    shared     1.11.21                   SSD         415.8GB
415.8GB

Aggregate capacity available for volume use would be increased by
1.83TB.
```

4. 스토리지를 Aggregate에 추가합니다.

```
storage aggregate add-disks -aggregate <aggr_name> -raidgroup new
-diskcount <number_of_disks_or_partitions>
```

Flash Pool 로컬 계층을 생성할 때 로컬 계층과 다른 체크섬을 가진 디스크를 추가하거나 혼합 체크섬 로컬 계층에 디스크를 추가하는 경우 매개 변수를 사용해야 `-checksumstyle` 합니다.

Flash Pool 로컬 계층에 디스크를 추가하는 경우 매개 변수를 사용하여 `-disktype` 디스크 유형을 지정해야 합니다.

매개 변수를 사용하여 추가할 디스크의 크기를 지정할 수 `-disksize` 있습니다. 로컬 계층에 추가할 디스크의 크기가 대략 지정된 디스크만 선택됩니다.

```
cl1-s2::> storage aggregate add-disks -aggregate data_1 -raidgroup
new -diskcount 5
```

5. 스토리지가 성공적으로 추가되었는지 확인합니다.

```
storage aggregate show-status -aggregate <aggr_name>
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                                                    Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     shared   1.0.10                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.5                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.6                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.11                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.0                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.2                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.3                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.4                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.8                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.9                        0   BSAS    7200  753.8GB
828.0GB (normal)
10 entries were displayed.
```

6. 노드에 루트 파티션과 데이터 파티션을 모두 스페어로 사용하는 드라이브가 하나 이상 있는지 확인합니다.

```
storage aggregate show-spare-disks -original-owner <node_name>
```

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
  Shared HDD Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                        Type      RPM Checksum          Usable
Usable     Size Status
 -------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.10                      BSAS    7200 block                0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

관련 정보

- "스토리지 집계 추가 디스크"
- "스토리지 집계 show-spare-disks"
- "스토리지 집계 표시 상태"

ONTAP 노드 또는 쉘프에 드라이브를 추가합니다

노드 또는 쉘프에 드라이브를 추가하여 핫 스페어 수를 늘리거나 로컬 계층에 공간을 추가할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

시작하기 전에

추가하려는 드라이브가 플랫폼에서 지원되어야 합니다. 를 사용하여 확인할 수 있습니다 "NetApp Hardware Universe를 참조하십시오".

단일 절차에서 추가해야 하는 최소 드라이브 수는 6개입니다. 단일 드라이브를 추가하면 성능이 저하될 수 있습니다.

NetApp Hardware Universe를 위한 단계

1. 제품** 드롭다운 메뉴에서 하드웨어 구성을 선택합니다
2. 플랫폼을 선택합니다.
3. 실행 중인 ONTAP 버전을 선택한 다음 결과 표시.
4. 그래픽 아래에서 대체 보기를 보려면 여기를 클릭하십시오를 선택합니다. 구성과 일치하는 보기를 선택합니다.

드라이브 설치 단계

1. 를 확인하십시오 "NetApp Support 사이트" 최신 드라이브 및 셸프 펌웨어 및 디스크 검증 패키지 파일의 경우

   노드나 쉘프에 최신 버전이 없는 경우 새 드라이브를 설치하기 전에 해당 버전을 업데이트하십시오.

   현재 펌웨어 버전이 없는 새 드라이브에서 드라이브 펌웨어가 중단 없이 자동으로 업데이트됩니다.

2. 적절하게 접지합니다.
3. 플랫폼 전면에서 베젤을 조심스럽게 분리합니다.
4. 새 드라이브에 맞는 슬롯을 확인합니다.

   ⓘ 드라이브를 추가할 수 있는 올바른 슬롯은 플랫폼 모델과 ONTAP 버전에 따라 다릅니다. 경우에 따라 특정 슬롯에 순서대로 드라이브를 추가해야 할 수도 있습니다. 예를 들어, AFF A800에서는 특정 간격으로 드라이브를 추가하여 빈 슬롯 클러스터를 남겨 둡니다. 반면, AFF A220에서는 외부에서 쉘프 중앙으로 실행되는 다음 빈 슬롯에 새 드라이브를 추가합니다.

   의 구성에 맞는 올바른 슬롯을 식별하려면 시작하기 전 **의 단계를 참조하십시오 "NetApp Hardware Universe를 참조하십시오".

5. 새 드라이브를 삽입합니다.
   a. 캠 핸들이 열린 위치에 있는 상태에서 두 손을 사용하여 새 드라이브를 삽입합니다.
   b. 드라이브가 멈출 때까지 누릅니다.
   c. 드라이브가 중간 평면에 완전히 장착되고 핸들이 제자리에 고정되도록 캠 핸들을 닫습니다. 캠 핸들이 드라이브 면과 올바르게 정렬되도록 캠 핸들을 천천히 닫아야 합니다.
6. 드라이브의 작동 LED(녹색)가 켜져 있는지 확인합니다.

   드라이브의 작동 LED가 고정되어 있으면 드라이브에 전원이 공급되고 있는 것입니다. 드라이브 작동 LED가 깜박이면 드라이브에 전원이 공급되고 I/O가 진행 중임을 의미합니다. 드라이브 펌웨어가 자동으로 업데이트되면 LED가 깜박입니다.

7. 다른 드라이브를 추가하려면 4-6단계를 반복합니다.

   새 드라이브는 노드에 할당될 때까지 인식되지 않습니다. 새 드라이브를 수동으로 할당하거나, 노드가 드라이브 자동 할당 규칙을 따르는 경우 ONTAP에서 새 드라이브를 자동으로 할당할 때까지 기다릴 수 있습니다.

8. 새 드라이브를 모두 인식한 후 드라이브가 추가되었고 소유권이 올바르게 지정되었는지 확인합니다.

설치 확인 단계

1. 디스크 목록을 표시합니다.

   '스토리지 집계 show-spare-disks'

   올바른 노드가 소유하는 새 드라이브가 표시됩니다.

2. 옵션**(ONTAP 9.3** 및 이전 버전에만 해당**),** 새로 추가된 드라이브를 0으로 설정:

   '스토리지 디스크 제로'

   이전에 ONTAP 로컬 계층에서 사용되었던 드라이브를 다른 로컬 계층에 추가하려면 먼저 0으로 설정해야 합니다. ONTAP 9.3 및 이전 버전에서는 제로화가 완료되는 데 몇 시간이 걸릴 수 있으며, 이는 노드의 비제로화 드라이브 크기에 따라 달라집니다. 이제 드라이브를 제로화하면 로컬 계층의 크기를 빠르게 늘려야 하는 경우 지연이 발생하지 않습니다. 이 문제는 ONTAP 9.4 이상에서 _fast zeroing_을 사용하여 드라이브를 제로화하는 데 몇 초밖에 걸리지 않습니다.

결과

새 드라이브가 준비되었습니다. 로컬 계층에 추가하거나 핫 스페어 목록에 추가하거나 새 로컬 계층을 생성할 때 추가할 수 있습니다.

관련 정보

- "스토리지 집계 show-spare-disks"
- "저장 디스크 제로 스페어"

잘못 정렬된 **ONTAP** 스페어 파티션을 수정합니다

파티션된 디스크를 로컬 계층에 추가하는 경우 루트 파티션과 데이터 파티션이 모두 있는 디스크를 모든 노드에 대해 스페어로 사용할 수 있도록 해야 합니다. 노드가 중단되지 않고 노드가 중단되면 ONTAP은 코어를 스페어 데이터 파티션으로 덤프할 수 없습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

시작하기 전에

동일한 노드에서 소유하는 동일한 디스크 유형에 스페어 데이터 파티션과 스페어 루트 파티션이 모두 있어야 합니다.

단계

1. CLI를 사용하여 노드에 대한 스페어 파티션을 표시합니다.

   'Storage aggregate show-spare-disks-original-owner_node_name_'

   스페어 데이터 파티션(spare_data)이 있는 디스크와 스페어 루트 파티션(spare_root)이 있는 디스크를 확인합니다. 스페어 파티션은 Local Data Usable(로컬 데이터 사용 가능) 또는 Local Root Usable(로컬 루트 사용 가능) 열 아래에 0이 아닌 값을 표시합니다.

2. 디스크를 스페어 루트 파티션이 있는 디스크로 교체합니다.

   'storage disk replace -disk_spare_data_-replacement_spare_root_ - action start'를 선택합니다

   어느 방향으로든 데이터를 복사할 수 있지만 루트 파티션을 복사하는 데 걸리는 시간이 줄어듭니다.

3. 디스크 교체 진행 상황 모니터링:

   'Storage aggregate show-status-aggregate_aggr_name_'

4. 교체 작업이 완료된 후 스페어를 다시 표시하여 전체 스페어 디스크가 있는지 확인합니다.

   'Storage aggregate show-spare-disks-original-owner_node_name_'

   "Local Data Usable" 및 "Local Root Usable" 아래에 사용 가능한 공간이 있는 여유 디스크가 있어야 합니다.

예
노드 C1-01의 스페어 파티션을 표시하고 스페어 파티션이 정렬되지 않은 것을 확인합니다.

```
c1::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                               Local    Local
                                Data     Root  Physical
 Disk    Type   RPM Checksum Usable   Usable      Size
 ------- ----- ---- -------- ------- ------- --------
 1.0.1   BSAS  7200 block    753.8GB     0B   828.0GB
 1.0.10  BSAS  7200 block         0B 73.89GB  828.0GB
```

디스크 교체 작업을 시작합니다.

```
c1::> storage disk replace -disk 1.0.1 -replacement 1.0.10 -action start
```

교체 작업이 완료될 때까지 기다리는 동안 작업 진행률이 표시됩니다.

```
c1::> storage aggregate show-status -aggregate aggr0_1

Owner Node: c1-01
 Aggregate: aggr0_1 (online, raid_dp) (block checksums)
  Plex: /aggr0_1/plex0 (online, normal, active, pool0)
   RAID Group /aggr0_1/plex0/rg0 (normal, block checksums)
                                     Usable Physical
 Position Disk    Pool Type   RPM     Size     Size Status
 -------- ------- ---- ---- ----- -------- -------- ----------
 shared   1.0.1    0   BSAS  7200  73.89GB  828.0GB (replacing,copy in
progress)
 shared   1.0.10   0   BSAS  7200  73.89GB  828.0GB (copy 63% completed)
 shared   1.0.0    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.11   0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.6    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.5    0   BSAS  7200  73.89GB  828.0GB (normal)
```

교체 작업이 완료된 후 전체 스페어 디스크가 있는지 확인합니다.

```
ie2220::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                              Local    Local
                               Data     Root  Physical
 Disk    Type    RPM Checksum Usable   Usable      Size
 ------ ----- ---- -------- -------- ------- --------
 1.0.1  BSAS  7200 block    753.8GB  73.89GB  828.0GB
```

관련 정보

- "스토리지 애그리게이트 보기"
- "저장 디스크 교체"

디스크를 관리합니다

ONTAP 핫 스페어 디스크의 작동 원리

핫 스페어 디스크는 스토리지 시스템에 할당되어 사용할 준비가 되었지만 RAID 그룹에서 사용되지 않으며 데이터를 보유하지 않는 디스크입니다.

RAID 그룹 내에서 디스크 장애가 발생하면 장애가 발생한 디스크를 교체하기 위해 핫 스페어 디스크가 RAID 그룹에 자동으로 할당됩니다. 장애가 발생한 디스크의 데이터는 RAID 패리티 디스크의 백그라운드에서 핫 스페어 교체 디스크에 재구성됩니다. 재구성 작업이 '/etc/message' 파일에 기록되고 AutoSupport 메시지가 전송된다.

사용 가능한 핫 스페어 디스크의 크기가 오류 발생 디스크와 동일하지 않은 경우 다음으로 큰 크기의 디스크를 선택한 다음 교체할 디스크의 크기에 맞게 크기를 축소합니다.

다중 디스크 캐리어 디스크의 예비 요구 사항

다중 디스크 캐리어의 디스크에 대해 적절한 수의 스페어를 유지하는 것은 스토리지 이중화를 최적화하고 ONTAP가 최적의 디스크 레이아웃을 달성하기 위해 디스크를 복사하는 데 소요되는 시간을 최소화하는 데 매우 중요합니다.

다중 디스크 캐리어 디스크용 핫 스페어를 항상 2개 이상 유지해야 합니다. 유지보수 센터의 사용을 지원하고 여러 번의 동시 디스크 장애로 인한 문제를 방지하려면 정상 상태 작동을 위해 최소 4개의 핫 스페어를 유지하고 장애가 발생한 디스크를 즉시 교체해야 합니다.

두 개의 디스크가 동시에 고장나고 사용 가능한 핫 스페어가 두 개뿐인 경우 ONTAP 고장난 디스크와 해당 디스크의 캐리어 메이트의 내용을 스페어 디스크로 스왑하지 못할 수 있습니다. 이런 상황을 교착상태라고 합니다. 이런 일이 발생하면 EMS 메시지와 AutoSupport 메시지를 통해 알려드립니다. 대체 운송업체가 생기면 EMS 메시지에 제공된 지침을 따라야 합니다. 자세한 내용은 다음을 참조하세요."NetApp 기술 자료: RAID 레이아웃을 자동으로 수정할 수 없음 - AutoSupport 메시지"

스페어 경고가 **ONTAP** 스페어 디스크를 관리하는 데 얼마나 도움이 되는지 확인하십시오

스토리지 시스템의 각 드라이브 속성과 일치하는 핫 스페어 드라이브가 하나 이상 있는 경우 기본적으로 콘솔과 로그에 경고가 표시됩니다.

이러한 경고 메시지의 임계값을 변경하여 시스템이 모범 사례를 준수하도록 할 수 있습니다.

이 작업에 대해

"min_spare_count" RAID 옵션을 ""2""로 설정하여 항상 최소 권장 스페어 디스크 수를 사용하도록 해야 합니다.

단계

1. 옵션을 ""2""로 설정합니다.

   'storage raid-options modify -node_nodename_ -name min_spare_count -value 2'

관련 정보

- "스토리지 raid 옵션 수정"

추가적인 **ONTAP** 루트 데이터 파티셔닝 관리 옵션

부트 메뉴에서 루트 데이터 분할 옵션을 사용할 수 있으며, 이 옵션은 루트 데이터 분할을 위해 구성된 디스크에 대한 추가 관리 기능을 제공합니다.

부팅 메뉴 옵션 9에서 다음 관리 기능을 사용할 수 있습니다.

- * 모든 디스크의 파티션을 해제하고 해당 소유권 정보를 제거합니다 *

  이 옵션은 시스템이 루트 데이터 파티셔닝으로 구성되어 있고 다른 구성으로 다시 초기화해야 하는 경우에 유용합니다.

- * 구성 정리 및 분할된 디스크가 있는 노드 초기화 *

이 옵션은 다음과 같은 경우에 유용합니다.

- 시스템이 루트 데이터 파티셔닝으로 구성되지 않아 루트 데이터 파티셔닝으로 구성하려고 합니다
- 시스템이 루트 데이터 파티셔닝으로 잘못 구성되어 있으므로 수정해야 합니다
- 이전 버전의 루트 데이터 파티셔닝에 대해 구성된 SSD만 연결되어 있는 AFF 플랫폼 또는 FAS 플랫폼이 있으며, 최신 버전의 루트 데이터 파티셔닝으로 업그레이드하여 스토리지 효율성을 높이고자 합니다

* * 전체 디스크로 구성 정리 및 노드 초기화 *

이 옵션은 다음과 같은 경우에 유용합니다.

- 기존 파티션 분할 취소
- 로컬 디스크 소유권을 제거합니다
- RAID-DP를 사용하여 전체 디스크로 시스템을 다시 초기화합니다

ONTAP 디스크 검증 패키지를 업데이트해야 하는 시기를 알아봅니다

DQP(Disk Qualification Package)는 새로 검증된 드라이브에 대한 완전한 지원을 추가합니다. 드라이브 펌웨어를 업데이트하거나 새 드라이브 유형 또는 크기를 클러스터에 추가하기 전에 DQP를 업데이트해야 합니다. 모범 사례는 DQP를 정기적으로 업데이트하는 것입니다(예: 매 분기 또는 매 반년).

다음과 같은 상황에서 DQP를 다운로드하여 설치해야 합니다.

- 노드에 새 드라이브 유형 또는 크기를 추가할 때마다

  예를 들어 이미 1TB 드라이브를 사용하고 2TB 드라이브를 추가한 경우 최신 DQP 업데이트를 확인해야 합니다.

- 디스크 펌웨어를 업데이트할 때마다
- 최신 디스크 펌웨어 또는 DQP 파일을 사용할 수 있는 경우
- 새 버전의 ONTAP로 업그레이드할 때마다

  DQP는 ONTAP 업그레이드의 일부로 업데이트되지 않습니다.

관련 정보

"NetApp 다운로드: 디스크 검증 패키지"

"NetApp 다운로드: 디스크 드라이브 펌웨어"

디스크 및 파티션 소유권

ONTAP 디스크 및 파티션의 소유권을 관리합니다

디스크 및 파티션의 소유권을 관리할 수 있습니다.

다음 작업을 수행할 수 있습니다.

- "디스크 및 파티션 소유권을 표시합니다"

디스크 소유권을 확인하여 스토리지를 제어하는 노드를 결정할 수 있습니다. 공유 디스크를 사용하는 시스템에서 파티션 소유권을 볼 수도 있습니다.

- "디스크 소유권을 자동으로 할당하는 설정을 변경합니다"

  자동으로 디스크 소유권을 할당하거나 디스크 소유권을 자동으로 할당하지 않도록 기본 정책이 아닌 정책을 선택할 수 있습니다.

- "분할되지 않은 디스크의 소유권을 수동으로 할당합니다"

  클러스터가 자동 디스크 소유권 할당을 사용하도록 구성되지 않은 경우 소유권을 수동으로 할당해야 합니다.

- "분할된 디스크의 소유권을 수동으로 할당합니다"

  파티션되지 않은 디스크에 대한 것처럼 수동으로 또는 자동 할당을 사용하여 컨테이너 디스크 또는 파티션의 소유권을 설정할 수 있습니다.

- "오류가 발생한 디스크를 제거합니다"

  완전히 장애가 발생한 디스크는 ONTAP에서 더 이상 사용 가능한 디스크로 간주할 수 없으며, 쉘프를 즉시 분리할 수 있습니다.

- "디스크에서 소유권을 제거합니다"

  ONTAP는 디스크 소유권 정보를 디스크에 씁니다. 노드에서 스페어 디스크 또는 해당 쉘프를 제거하려면 먼저 소유권 정보를 제거하여 다른 노드에 올바르게 통합되도록 해야 합니다.

ONTAP 디스크 소유권 자동 할당에 대해 알아봅니다

소유되지 않은 디스크의 자동 할당은 기본적으로 활성화되어 있습니다. 자동 디스크 소유권 할당은 HA 쌍 초기화 후 10분, 정상적인 시스템 작동 중에는 5분마다 이루어집니다.

예를 들어, 실패한 디스크를 교체하거나, "예비 디스크 부족" 메시지에 응답하거나, 용량을 추가하는 등 HA 쌍에 새 디스크를 추가할 때 기본 자동 할당 정책은 디스크 소유권을 예비 디스크로 노드에 할당합니다.

기본 자동 할당 정책은 플랫폼별 특성을 기반으로 하거나, HA 쌍에 이러한 쉘프만 있고 다음 방법(정책) 중 하나를 사용하여 디스크 소유권을 할당하는 경우 DS460C 셸프를 기반으로 합니다.

할당 방법	노드 할당에 미치는 영향	할당 방법에 대한 기본 플랫폼 구성
베이	짝수 번호 베이는 노드 A에 할당되고 홀수 번호 베이는 노드 B에 할당됩니다	HA 쌍 구성에서 단일 공유 쉘프를 제공하는 엔트리 레벨 시스템입니다.
쉘프	쉘프 내의 모든 디스크는 노드 A에 할당됩니다	2개 이상의 셸프로 구성된 단일 스택과 MetroCluster 노드당 하나의 스택, 2개 이상의 셸프로 구성된 HA 쌍 구성의 엔트리 레벨 시스템

쉘프를 분할합니다 이 정책은 기본값에 속한다 `-autoassign-policy` 의 매개 변수입니다 `storage disk option` 해당 플랫폼 및 쉘프 구성에 대한 명령입니다.	쉘프 왼쪽의 디스크는 노드 A에 할당되고 오른쪽의 노드 B에 할당됩니다 HA 쌍의 부분 쉘프는 쉘프 가장자리에서 중앙으로 채워진 디스크가 장착된 상태로 공장에서 출하됩니다.	대부분의 AFF 플랫폼 및 일부 MetroCluster 구성
스택	스택의 모든 디스크가 노드 A에 할당됩니다	독립형 엔트리 레벨 시스템 및 기타 모든 구성
하프 드로어 이 정책은 기본값에 속한다 `-autoassign-policy` 의 매개 변수입니다 `storage disk option` 해당 플랫폼 및 쉘프 구성에 대한 명령입니다.	DS460C 드로어의 왼쪽 절반에 있는 모든 드라이브(드라이브 베이 0 - 5)는 노드 A에 할당되고 드로어의 오른쪽 절반에 있는 모든 드라이브(드라이브 베이 6 - 11)는 노드 B에 할당됩니다 DS460C 쉘프만 사용하여 HA 쌍을 초기화할 때는 디스크 소유권 자동 할당이 지원되지 않습니다. 하프 드로어 정책을 준수하여 루트 파티션이 있는 루트/컨테이너 드라이브가 포함된 드라이브에 대해 소유권을 수동으로 할당해야 합니다.	HA 쌍 초기화(부팅) 후 DS460C 쉘프와 HA 쌍을 제공합니다. HA Pair가 부팅되면 디스크 소유권 자동 할당이 자동으로 활성화되고 1/2 드로어 정책을 사용하여 나머지 드라이브(루트 파티션이 있는 루트 드라이브/컨테이너 드라이브 제외) 및 이후에 추가된 드라이브에 소유권을 할당합니다. HA 쌍에 다른 쉘프 모델 외에 DS460C 쉘프가 있는 경우, 절반 드로어 정책은 사용되지 않습니다. 사용되는 기본 정책은 플랫폼별 특성에 따라 결정됩니다.

자동 할당 설정 및 수정:

- 을 사용하여 현재 자동 할당 설정(켜기/끄기)을 표시할 수 있습니다 `storage disk option show` 명령.
- 를 사용하여 자동 할당을 해제할 수 있습니다 `storage disk option modify` 명령.
- 기본 자동 할당 정책이 사용자 환경에서 바람직하지 않은 경우 를 사용하여 베이, 셸프 또는 스택 할당 방법을 지정(변경)할 수 있습니다 `-autoassign-policy` 매개 변수 을 선택합니다 `storage disk option modify` 명령.

  자세한 내용을 알아보십시오 "디스크 소유권을 자동으로 할당하는 설정을 변경합니다".

> 하프 드로어 및 분할 셸프 기본 자동 할당 정책은 베이, 셸프 및 스택 정책과 같은 사용자가 설정할 수 없기 때문에 고유합니다.

ADP(Advanced Drive Partitioning) 시스템에서 절반 채워진 쉘프에서 자동 할당을 수행하려면, 보유하고 있는 쉘프 유형에 따라 드라이브를 올바른 쉘프 베이에 설치해야 합니다.

- 사용하는 쉘프가 DS460C 쉘프가 아닌 경우, 드라이브를 왼쪽 끝에, 오른쪽 끝에 가운데를 향해 균등하게 설치합니다. 예를 들어, 베이 0-5에 6개의 드라이브가 있고, DS224C 쉘프의 베이 18-23에 6개의 드라이브가 있습니다.
- DS460C 쉘프인 경우, 각 드로어의 앞줄(드라이브 베이 0, 3, 6, 9)에 드라이브를 설치합니다. 나머지 드라이브의

경우, 서랍을 앞면에서 뒤쪽으로 채우면 각 서랍에 균등하게 분산됩니다. 행을 채울 만큼 충분한 드라이브가 없는 경우, 드라이브가 드로어의 왼쪽과 오른쪽에 균일하게 오도록 쌍으로 설치하십시오.

각 드로어의 첫 행에 드라이브를 설치하면 공기가 적절하게 흐르고 과열이 방지됩니다.

드라이브가 반으로 채워진 쉘프의 올바른 쉘프 베이에 설치되어 있지 않은 경우, 컨테이너 드라이브에 장애가 발생하여 교체되면 ONTAP은 소유권을 자동으로 할당하지 않습니다. 이 경우 새 컨테이너 드라이브를 수동으로 할당해야 합니다. 컨테이너 드라이브에 소유권을 할당하면 ONTAP에서 필요한 모든 드라이브 파티셔닝 및 파티셔닝 할당을 자동으로 처리합니다.

자동 할당이 작동하지 않는 일부 상황에서는 를 사용하여 디스크 소유권을 수동으로 할당해야 합니다 `storage disk assign` 명령:

- 자동 할당을 사용하지 않도록 설정하면 새 디스크가 노드에 수동으로 할당될 때까지 스페어로 사용할 수 없습니다.
- 디스크를 자동 할당하고 소유권이 서로 다른 여러 스택 또는 쉘프가 있는 경우, 각 스택 또는 쉘프에 대해 단일 디스크를 수동으로 할당해야 하므로 각 스택 또는 쉘프에 자동 소유권 할당이 작동합니다.
- 자동 할당이 활성화되어 있고 활성 정책에 지정되지 않은 노드에 단일 드라이브를 수동으로 할당하는 경우 자동 할당이 중지되고 EMS 메시지가 표시됩니다.

자세한 내용을 알아보십시오 "분할되지 않은 디스크의 디스크 소유권을 수동으로 할당합니다".

자세한 내용을 알아보십시오 "분할된 디스크의 디스크 소유권을 수동으로 할당합니다".

관련 정보

- "저장 디스크 할당"
- "저장 디스크 옵션 수정"
- "저장 디스크 옵션 표시"

ONTAP 디스크 및 파티션 소유권을 표시합니다

디스크 소유권을 확인하여 스토리지를 제어하는 노드를 결정할 수 있습니다. 공유 디스크를 사용하는 시스템에서 파티션 소유권을 볼 수도 있습니다.

단계

1. 물리 디스크의 소유권을 표시합니다.

   스토리지 디스크 표시 소유권

```
cluster::> storage disk show -ownership
Disk     Aggregate Home     Owner    DR Home  Home ID     Owner ID   DR
Home ID  Reserver    Pool
-------- --------- -------- -------- -------- ---------- -----------
----------- ----------- ------
1.0.0    aggr0_2   node2    node2    -        2014941509 2014941509  -
2014941509  Pool0
1.0.1    aggr0_2   node2    node2    -        2014941509 2014941509  -
2014941509  Pool0
1.0.2    aggr0_1   node1    node1    -        2014941219 2014941219  -
2014941219  Pool0
1.0.3    -         node1    node1    -        2014941219 2014941219  -
2014941219  Pool0
```

2. 공유 디스크를 사용하는 시스템이 있는 경우 파티션 소유권을 표시할 수 있습니다.

   스토리지 디스크 show-partition-ownership입니다

```
cluster::> storage disk show -partition-ownership
                                Root                    Data
Container  Container
Disk     Aggregate Root Owner  Owner ID    Data Owner  Owner ID    Owner
Owner ID
-------- --------- ----------- ----------- ----------- -----------
---------- -----------
1.0.0    -         node1       1886742616  node1       1886742616  node1
1886742616
1.0.1    -         node1       1886742616  node1       1886742616  node1
1886742616
1.0.2    -         node2       1886742657  node2       1886742657  node2
1886742657
1.0.3    -         node2       1886742657  node2       1886742657  node2
1886742657
```

관련 정보

- "저장 디스크 표시"

ONTAP 디스크 소유권 자동 할당에 대한 설정을 변경합니다

를 사용할 수 있습니다 `storage disk option modify` 디스크 소유권을 자동으로 할당하거나 디스크 소유권을 자동으로 할당하지 않도록 하는 기본 정책이 아닌 정책을 선택하는 명령입니다.

에 대해 자세히 알아보십시오 "디스크 소유권을 자동으로 할당합니다".

이 작업에 대해

DS460C 쉘프만 포함된 HA 쌍이 있는 경우, 기본 자동 할당 정책은 1/2 드로어 입니다. 기본 정책이 아닌 정책(베이, 쉘프, 스택)으로 변경할 수 없습니다.

단계

1. 자동 디스크 할당 수정:
   a. 기본값이 아닌 정책을 선택하려면 다음을 입력합니다.

      '스토리지 디스크 옵션 modify-autoassign-policy_autoconfigure_policy_-node_node_name_'

      - 스택 또는 루프 수준에서 자동 소유권을 구성하려면 '*autoassign_policy*'로 'stack'을 사용합니다.
      - shelf 레벨에서 자동 소유권을 구성하려면 '*autoconfigure_policy*'로 'shelf'를 사용합니다.
      - 베이 수준에서 자동 소유권을 구성하려면 '*autoconfigure_policy*'로 'bay'를 사용합니다.

   b. 자동 디스크 소유권 할당을 해제하려면 다음을 입력합니다.

      ```
      storage disk option modify -autoassign off -node node_name
      ```

2. 디스크의 자동 할당 설정을 확인합니다.

   '스토리지 디스크 옵션 표시'

   ```
   cluster1::> storage disk option show

   Node           BKg. FW. Upd.  Auto Copy     Auto Assign    Auto
                                                              Assign Policy
   -------------  -------------  ------------  -------------  --------
   cluster1-1     on             on            on             default
   cluster1-2     on             on            on             default
   ```

관련 정보

- "저장 디스크 옵션 수정"
- "저장 디스크 옵션 표시"

분할되지 않은 디스크의 **ONTAP** 디스크 소유권을 수동으로 할당합니다

HA 2노드가 자동 디스크 소유권 할당을 사용하도록 구성되지 않은 경우 소유권을 수동으로 할당해야 합니다. DS460C 쉘프만 있는 HA 쌍을 초기화하는 경우 루트 드라이브에 대한 소유권을 수동으로 할당해야 합니다.

이 작업에 대해

- 초기화되지 않고 DS460C 쉘프만 없는 HA 쌍에서 소유권을 수동으로 할당하는 경우 옵션 1을 사용합니다.
- DS460C 쉘프만 있는 HA 쌍을 초기화하는 경우 옵션 2를 사용하여 루트 드라이브에 대한 소유권을 수동으로 할당합니다.

옵션 **1:** 대부분의 **HA** 쌍

초기화되지 않고 DS460C 쉘프만 없는 HA 쌍의 경우 다음 절차를 사용하여 소유권을 수동으로 할당할 수 있습니다.

이 작업에 대해

- 소유권을 할당할 디스크는 소유권을 할당할 노드에 물리적으로 케이블로 연결된 셸프에 있어야 합니다.
- 로컬 계층(집계)에서 디스크를 사용하는 경우:
  - 디스크를 로컬 계층(애그리게이트)에서 사용하려면 먼저 노드가 디스크를 소유해야 합니다.
  - 로컬 계층(집계)에서 사용 중인 디스크의 소유권을 재할당할 수 없습니다.

단계

1. CLI를 사용하여 소유하지 않은 모든 디스크를 표시합니다.

   스토리지 디스크 show-container-type unassigned

2. 각 디스크 할당:

   'Storage disk assign-disk_name_-owner_owner_name_'

   와일드카드 문자를 사용하여 한 번에 두 개 이상의 디스크를 할당할 수 있습니다. 다른 노드에 이미 있는 스페어 디스크를 재할당하는 경우 ""-force" 옵션을 사용해야 합니다.

옵션 **2: DS460C** 쉘프만 있는 **HA** 쌍

초기화 중이며 DS460C 쉘프만 있는 HA 쌍의 경우 다음 절차를 사용하여 루트 드라이브에 대한 소유권을 수동으로 할당합니다.

이 작업에 대해

- DS460C 쉘프만 포함된 HA 쌍을 초기화할 경우, 절반 드로어 정책을 준수하도록 루트 드라이브를 수동으로 할당해야 합니다.

  HA Pair 초기화(부팅) 후 디스크 소유권 자동 할당이 자동으로 활성화되고 하프 드로어 정책을 사용하여 나머지 드라이브(루트 드라이브 제외) 및 나중에 추가된 드라이브(예: 장애가 발생한 디스크 교체, "스페어 부족" 메시지에 대한 응답 또는 용량 추가)에 소유권을 할당합니다.

  "하프 드로어 정책에 대해 알아봅니다"..

- RAID에는 DS460C 쉘프에 있는 8TB NL-SAS 드라이브 이상의 각 HA 쌍에 대해 최소 10개의 드라이브(노드당 5개)가 필요합니다.

단계

1. DS460C 선반이 완전히 채워지지 않은 경우 다음 하위 단계를 완료하십시오. 그렇지 않으면 다음 단계로 이동합니다.

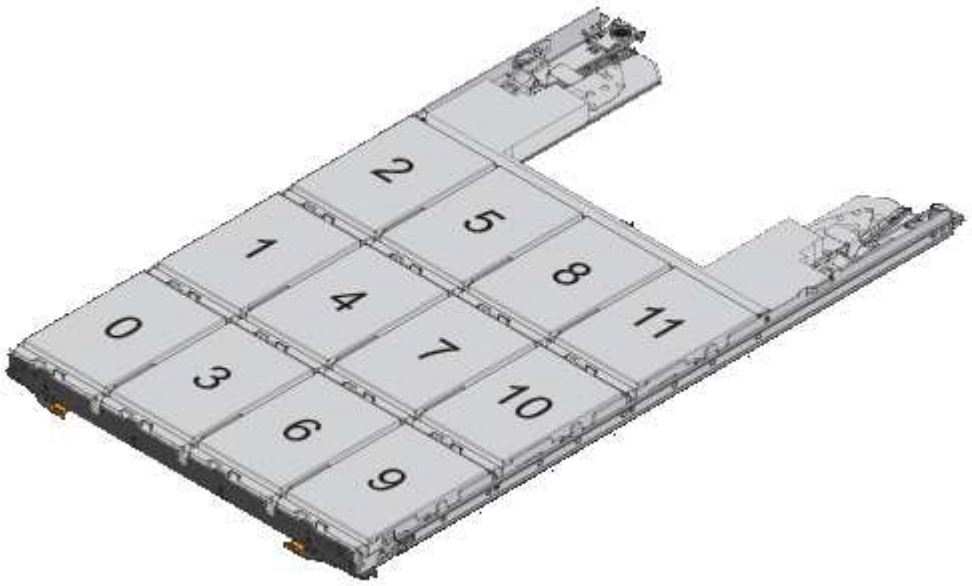
   a. 먼저 각 드로어의 첫 줄(드라이브 베이 0, 3, 6, 9)에 드라이브를 설치합니다.

      각 드로어의 첫 행에 드라이브를 설치하면 공기가 적절하게 흐르고 과열이 방지됩니다.

   b. 나머지 드라이브의 경우 각 드로어에 균등하게 분배합니다.

      서랍을 앞쪽에서 뒤쪽으로 채웁니다. 행을 채울 만큼 충분한 드라이브가 없는 경우, 드라이브가 드로어의 왼쪽과 오른쪽에 균일하게 오도록 쌍으로 설치하십시오.

      다음 그림에서는 DS460C 드로어의 드라이브 베이 번호 및 위치를 보여 줍니다.



2. 노드 관리 LIF 또는 클러스터 관리 LIF를 사용하여 클러스터 쉘에 로그인합니다.

3. 다음 하위 단계를 사용하여 각 드로어의 루트 드라이브를 수동으로 할당하여 하프 드로어 정책을 준수합니다.

   하프 드로어 정책에서는 드로어 드라이브의 왼쪽 절반(베이 0 ~ 5)을 노드 A에 할당하고 드로어 드라이브의 오른쪽 절반(베이 6 ~ 11)을 노드 B에 할당합니다

   a. 소유되지 않은 모든 디스크 표시:
      `storage disk show -container-type unassigned`

   b. 루트 디스크 할당:
      `storage disk assign -disk disk_name -owner owner_name`

      와일드카드 문자를 사용하여 한 번에 두 개 이상의 디스크를 할당할 수 있습니다.

에 대한 자세한 내용은 `storage disk` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "저장 디스크 할당"
- "저장 디스크 표시"

ONTAP 파티션된 디스크의 소유권을 수동으로 할당합니다

컨테이너 디스크 또는 ADP(Advanced Drive Partitioning) 시스템의 파티션에 대한 소유권을 수동으로 할당할 수 있습니다. DS460C 쉘프만 있는 HA 쌍을 초기화하는 경우 루트 파티션을 포함할 컨테이너 드라이브에 대한 소유권을 수동으로 할당해야 합니다.

이 작업에 대해

- 지원하는 ADP 방법, RD(루트 데이터) 또는 RD2(루트 데이터 데이터 데이터 데이터)를 결정하는 스토리지 시스템 유형입니다.

  FAS 스토리지 시스템은 RD 및 AFF 스토리지 시스템을 사용하며 RD2를 사용합니다.

- 초기화되지 않고 DS460C 쉘프만 없는 HA 쌍에 소유권을 수동으로 할당하는 경우 옵션 1을 사용하여 루트 데이터(RD) 파티셔닝으로 디스크를 수동으로 할당하거나 옵션 2를 사용하여 루트 데이터(RD2) 파티셔닝으로 디스크를 수동으로 할당합니다.
- DS460C 쉘프만 있는 HA 쌍을 초기화하는 경우 옵션 3을 사용하여 루트 파티션이 있는 컨테이너 드라이브에 대한 소유권을 수동으로 할당합니다.

옵션 **1:** 루트 데이터**(RD)** 파티셔닝으로 디스크를 수동으로 할당합니다

루트 데이터 파티셔닝의 경우 HA 쌍이 소유하는 세 가지 엔터티(컨테이너 디스크 및 두 파티션)가 있습니다.

이 작업에 대해

- 컨테이너 디스크와 두 파티션이 모두 HA 쌍의 노드 중 하나에 의해 소유되는 한 HA 쌍의 같은 노드에 의해 소유될 필요는 없습니다. 그러나 로컬 계층에서 파티션을 사용하는 경우 로컬 계층을 소유하는 동일한 노드에서 파티션을 소유해야 합니다.
- 반쯤 채워진 쉘프에서 컨테이너 디스크에 장애가 발생하고 교체되는 경우, 이 경우 ONTAP가 소유권을 자동으로 할당하지 않는 경우가 있으므로 디스크 소유권을 수동으로 할당해야 할 수 있습니다.
- 컨테이너 디스크가 할당되면 ONTAP 소프트웨어는 필요한 모든 파티션 및 파티션 할당을 자동으로 처리합니다.

단계

1. CLI를 사용하여 파티션된 디스크의 현재 소유권을 표시합니다.

   스토리지 디스크 show-disk_disk_name_-partition-ownership입니다

2. CLI 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

3. 소유권을 할당할 소유권 엔티티에 따라 적절한 명령을 입력합니다.

   소유권 요소가 이미 소유된 경우 옵션을 포함해야 `-force` 합니다.

다음에 대한 소유권을 할당하려면…	이 명령 사용…
컨테이너 디스크	'Storage disk assign-disk_name_-owner_owner_name_'
데이터 파티션	'storage disk assign-disk_name_-owner_owner_name_-data TRUE'
루트 파티션입니다	'storage disk assign-disk_name_-owner_owner_name_-root true'

옵션 **2:** 루트 데이터**(RD2)** 파티션을 사용하여 디스크를 수동으로 할당합니다

루트 데이터 데이터 파티셔닝의 경우 HA 쌍이 통틀어 4개의 소유 엔터티(컨테이너 디스크 및 3개의 파티션)가 있습니다. 루트 데이터 - 데이터 파티셔닝은 루트 파티션으로 작은 파티션 하나를 생성하고 데이터에 대해 크기가 같은 큰 파티션 두 개를 생성합니다.

이 작업에 대해

- 루트 데이터 파티셔닝된 디스크의 적절한 파티션을 할당하려면 매개 변수를 명령과 함께 사용해야 `disk assign` 합니다. 스토리지 풀의 일부인 디스크에는 이러한 매개 변수를 사용할 수 없습니다. 기본값은 입니다 `false`.
  - `-data1 true`매개 변수는 `data1` 루트-data1-data2 파티셔닝된 디스크의 파티션을 할당합니다.
  - `-data2 true`매개 변수는 `data2` 루트-data1-data2 파티셔닝된 디스크의 파티션을 할당합니다.
- 반쯤 채워진 쉘프에서 컨테이너 디스크에 장애가 발생하고 교체되는 경우, 이 경우 ONTAP가 소유권을 자동으로 할당하지 않는 경우가 있으므로 디스크 소유권을 수동으로 할당해야 할 수 있습니다.
- 컨테이너 디스크가 할당되면 ONTAP 소프트웨어는 필요한 모든 파티션 및 파티션 할당을 자동으로 처리합니다.

단계

1. CLI를 사용하여 파티션된 디스크의 현재 소유권을 표시합니다.

   스토리지 디스크 show-disk_disk_name_-partition-ownership입니다

2. CLI 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

3. 소유권을 할당할 소유권 엔티티에 따라 적절한 명령을 입력합니다.

   소유권 요소가 이미 소유된 경우 옵션을 포함해야 `-force` 합니다.

다음에 대한 소유권을 할당하려면…	이 명령 사용…
컨테이너 디스크	'Storage disk assign-disk_name_-owner_owner_name_'
Data1 파티션	'storage disk assign-disk_name_-owner_owner_name_-data1 TRUE'
데이터 2 파티션	'storage disk assign-disk_name_-owner_owner_name_-data2 TRUE'
루트 파티션입니다	'storage disk assign-disk_name_-owner_owner_name_-root true'

옵션 **3:** 루트 파티션이 있는 **DS460C** 컨테이너 드라이브를 수동으로 할당합니다

DS460C 쉘프만 있는 HA 쌍을 초기화하는 경우 절반 드로어 정책을 준수하여 루트 파티션이 있는 컨테이너 드라이브에 대한 소유권을 수동으로 할당해야 합니다.

이 작업에 대해

- DS460C 셸프만 있는 HA 쌍을 초기화하는 경우 ADP 부팅 메뉴 옵션 9a 및 9b는 자동 드라이브 소유권 할당을 지원하지 않습니다. 하프 드로어 정책을 준수하여 루트 파티션이 있는 컨테이너 드라이브를 수동으로 할당해야 합니다.

  HA 쌍 초기화(부팅) 후 디스크 소유권 자동 할당이 자동으로 활성화되고, 하프 드로어 정책을 사용하여 루트 파티션이 있는 컨테이너 드라이브가 아닌 나머지 드라이브와 향후 추가되는 드라이브(예비 드라이브 교체, "예비 드라이브 부족" 메시지에 대한 응답, 용량 추가 등)에 소유권을 할당합니다.

- "하프 드로어 정책에 대해 알아봅니다"..

단계

1. DS460C 선반이 완전히 채워지지 않은 경우 다음 하위 단계를 완료하십시오. 그렇지 않으면 다음 단계로 이동합니다.

   a. 먼저 각 드로어의 첫 줄(드라이브 베이 0, 3, 6, 9)에 드라이브를 설치합니다.

      각 드로어의 첫 행에 드라이브를 설치하면 공기가 적절하게 흐르고 과열이 방지됩니다.

   b. 나머지 드라이브의 경우 각 드로어에 균등하게 분배합니다.

      서랍을 앞쪽에서 뒤쪽으로 채웁니다. 행을 채울 충분한 드라이브가 없는 경우 드라이브가 드로어의 왼쪽과 오른쪽을 고르게 차지하도록 쌍으로 설치하십시오.

      다음 그림에서는 DS460C 드로어의 드라이브 베이 번호 및 위치를 보여 줍니다.

2. 노드 관리 LIF 또는 클러스터 관리 LIF를 사용하여 클러스터 쉘에 로그인합니다.
3. 각 드로어에 대해 다음 하위 단계를 사용하여 하프 드로어 정책을 준수하여 루트 파티션이 있는 컨테이너 드라이브를 수동으로 할당합니다.

하프 드로어 정책에서는 드로어의 드라이브 왼쪽 절반(베이 0 ~ 5)을 노드 A에 할당하고 드로어의 드라이브 오른쪽 절반(베이 6 ~ 11)을 노드 B에 할당합니다

a. 소유되지 않은 모든 디스크 표시:
   `storage disk show -container-type unassigned`

b. 루트 파티션이 있는 컨테이너 드라이브를 할당합니다.
   `storage disk assign -disk disk_name -owner owner_name`

   와일드카드 문자를 사용하여 한 번에 두 개 이상의 드라이브를 할당할 수 있습니다.

관련 정보

- "저장 디스크 할당"
- "저장 디스크 표시"

루트 데이터 파티셔닝을 사용하여 **ONTAP** 노드에서 액티브-패시브 구성을 설정합니다

HA 쌍이 공장 출하 시 루트 데이터 파티셔닝을 사용하도록 구성된 경우, 데이터 파티션의 소유권은 액티브-액티브 구성에서 사용하기 위해 두 노드 사이에 분할됩니다. 액티브-패시브 구성에서 HA 쌍을 사용하려면 데이터 로컬 계층을 생성하기 전에 파티션 소유권을 업데이트해야 합니다.

시작하기 전에

- 액티브 노드가 될 노드와 패시브 노드가 될 노드를 결정해야 합니다.
- 스토리지 페일오버는 HA 쌍에서 구성해야 합니다.

이 작업에 대해

이 작업은 노드 A와 노드 B의 두 노드에서 수행됩니다

이 절차는 분할된 디스크에서 데이터 로컬 계층이 생성되지 않은 노드를 위해 설계되었습니다.

에 대해 자세히 알아보십시오 "고급 디스크 파티셔닝".

단계

모든 명령은 클러스터 쉘에 입력됩니다.

1. 데이터 파티션의 현재 소유권을 봅니다.

   '스토리지 집계 show-spare-disks'

   출력에서는 데이터 파티션의 절반이 한 노드에 소유되고 절반은 다른 노드에 의해 소유된다는 것을 보여 줍니다. 모든 데이터 파티션은 스페어 파티션이어야 합니다.

```
cluster1::> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
```

```
  Partitioned Spares
                                                                  Local
Local
                                                                   Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.5                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                      BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                                  Local
Local
                                                                   Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB
12 entries were displayed.
```

2. 고급 권한 수준 입력:

   진일진일보한 것

3. 패시브 노드가 될 노드가 소유하는 각 데이터 파티션에 대해 활성 노드에 할당합니다.

   'storage disk assign-force-data TRUE-owner_active_node_name_-disk_disk_name_'

   디스크 이름의 일부로 파티션을 포함할 필요는 없습니다.

   재할당해야 하는 각 데이터 파티션에 대해 다음 예와 유사한 명령을 입력합니다.

   'Storage disk assign-force-data TRUE-owner cluster1-01-disk 1.0.3'을 참조하십시오

4. 모든 파티션이 액티브 노드에 할당되었는지 확인합니다.

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                                  Local
Local
                                                                   Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                       BSAS    7200 block           753.8GB
```

```
0B  828.0GB
 1.0.10                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                       BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                             Local
Local
                                                              Data
Root Physical
 Disk                         Type      RPM Checksum         Usable
Usable     Size
 ---------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                        BSAS    7200 block                0B
73.89GB  828.0GB
13 entries were displayed.
```

cluster1-02는 여전히 스페어 루트 파티션을 소유합니다.

5. 관리 권한으로 돌아가기:

   '관리자 설정'을 선택합니다

6. 하나 이상의 데이터 파티션을 스페어로 남겨두고 데이터 로컬 계층을 만듭니다.

   'Storage aggregate create_new_aggr_name_-diskcount_number_of_partitions_-node_active_node_name_'

   데이터 로컬 계층이 생성되고 활성 노드에서 소유됩니다.

관련 정보

- "저장소 집계 생성"
- "스토리지 애그리게이트 보기"
- "저장 디스크 할당"

루트 데이터-데이터 파티셔닝을 사용하여 **ONTAP** 노드에서 액티브-패시브 구성을 설정합니다

HA 쌍이 공장 출하 시 루트 데이터 데이터 파티셔닝을 사용하도록 구성된 경우, 데이터 파티션의 소유권은 액티브-액티브 구성에서 사용하기 위해 두 노드 사이에 분할됩니다. 액티브-패시브 구성에서 HA 쌍을 사용하려면 데이터 로컬 계층을 생성하기 전에 파티션 소유권을 업데이트해야 합니다.

시작하기 전에

- 액티브 노드가 될 노드와 패시브 노드가 될 노드를 결정해야 합니다.
- 스토리지 페일오버는 HA 쌍에서 구성해야 합니다.

이 작업에 대해

이 작업은 노드 A와 노드 B의 두 노드에서 수행됩니다

이 절차는 분할된 디스크에서 데이터 로컬 계층이 생성되지 않은 노드를 위해 설계되었습니다.

에 대해 자세히 알아보십시오 "고급 디스크 파티셔닝".

단계

모든 명령은 클러스터 쉘에 입력됩니다.

1. 데이터 파티션의 현재 소유권을 봅니다.

   'Storage aggregate show-spare-disks-original-owner_passive_node_name_-fields local-usable-data1-size, local-usable-data2-size'를 입력합니다

   출력에서는 데이터 파티션의 절반이 한 노드에 소유되고 절반은 다른 노드에 의해 소유된다는 것을 보여 줍니다. 모든 데이터 파티션은 스페어 파티션이어야 합니다.

2. 고급 권한 수준 입력:

   진일진일보한 것

3. 패시브 노드가 될 노드가 소유하는 각 데이터 1 파티션에 대해 액티브 노드에 할당합니다.

   'storage disk assign-force-data1-owner_active_node_name_-disk_disk_name_'

   디스크 이름의 일부로 파티션을 포함할 필요는 없습니다

4. 패시브 노드가 될 노드가 소유하는 각 데이터 2 파티션에 대해 액티브 노드에 할당합니다.

   'storage disk assign-force-data2-owner_active_node_name_-disk_disk_name_'

   디스크 이름의 일부로 파티션을 포함할 필요는 없습니다

5. 모든 파티션이 액티브 노드에 할당되었는지 확인합니다.

   '스토리지 집계 show-spare-disks'

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                                 Local
Local
                                                                  Data
Root Physical
```

```
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 -------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                      BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 -------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                       BSAS    7200 block                0B
73.89GB  828.0GB
13 entries were displayed.
```

cluster1-02는 여전히 스페어 루트 파티션을 소유합니다.

6. 관리 권한으로 돌아가기:

   '관리자 설정'을 선택합니다

7. 하나 이상의 데이터 파티션을 스페어로 남겨두고 데이터 애그리게이트를 생성합니다.

   'Storage aggregate create_new_aggr_name_-diskcount_number_of_partitions_-node_active_node_name_'

   데이터 애그리게이트는 생성되며 액티브 노드가 소유합니다.

8. 또는 RAID 그룹 레이아웃 및 스페어 수에 대한 Best Practice가 포함된 ONTAP의 권장 로컬 계층 레이아웃을 사용할 수 있습니다.

   '스토리지 집계 자동 프로비저닝'

관련 정보

- "스토리지 집계 자동 프로비저닝"
- "저장소 집계 생성"
- "스토리지 애그리게이트 보기"
- "저장 디스크 할당"

디스크에서 **ONTAP** 소유권을 제거합니다

ONTAP는 디스크 소유권 정보를 디스크에 씁니다. 노드에서 스페어 디스크 또는 해당 쉘프를 제거하려면 먼저 소유권 정보를 제거하여 다른 노드에 올바르게 통합되도록 해야 합니다.

디스크가 루트 데이터 파티셔닝용으로 분할되어 있고 ONTAP 9.10.1 이상을 실행 중인 경우 NetApp 기술 지원 부서에 소유권 제거에 대한 지원을 요청하십시오. 자세한 내용은 를 참조하십시오 "기술 문서: 디스크 소유자를 제거하지 못했습니다".

시작하기 전에

소유권을 제거할 디스크는 다음 요구 사항을 충족해야 합니다.

- 스페어 디스크여야 합니다.

  로컬 계층에서 사용 중인 디스크에서는 소유권을 제거할 수 없습니다.

- 유지보수 센터에 있을 수 없습니다.
- 완전 삭제를 수행할 수 없습니다.
- 실패했을 수 없습니다.

  오류가 발생한 디스크에서 소유권을 제거할 필요는 없습니다.

이 작업에 대해

자동 디스크 할당을 활성화한 경우 ONTAP은 디스크에서 디스크를 제거하기 전에 소유권을 자동으로 재할당할 수 있습니다. 따라서 디스크를 제거할 때까지 자동 소유권 할당을 해제한 다음 다시 사용하도록 설정합니다.

단계

1. 디스크 소유권 자동 할당이 켜져 있는 경우 CLI를 사용하여 다음을 해제합니다.

   'storage disk option modify -node_node_name_-autoassign off'

2. 필요한 경우 노드의 HA 파트너에 대해 이전 단계를 반복합니다.
3. 디스크에서 소프트웨어 소유권 정보를 제거합니다.

   'Storage disk removeowner_disk_name_'

   여러 디스크에서 소유권 정보를 제거하려면 쉼표로 구분된 목록을 사용합니다.

   예:

   ```
   storage disk removeowner sys1:0a.23,sys1:0a.24,sys1:0a.25
   ```

4. 디스크가 루트 데이터 파티셔닝용으로 분할되어 있고 ONTAP 9.9.1 이하를 실행 중인 경우 파티션에서 소유권을 제거하십시오.

   'storage disk removeowner - disk_disk_name_ - root true'

   "스토리지 디스크 원격 소유자 -disk_disk_name_-data 참"

   두 파티션은 더 이상 어떤 노드에서도 소유하지 않습니다.

5. 이전에 디스크 소유권 자동 할당을 해제했다면 디스크를 제거하거나 재할당한 후에 이 기능을 켜십시오.

   '스토리지 디스크 옵션 modify -node_node_name_-autostassign on'

6. 필요한 경우 노드의 HA 파트너에 대해 이전 단계를 반복합니다.

관련 정보

- "저장 디스크 옵션 수정"
- "저장 디스크 removeowner"

오류가 발생한 **ONTAP** 디스크를 제거합니다

ONTAP에서는 장애가 완전히 발생한 디스크를 사용 가능한 디스크로 더 이상 카운트하지 않으며 디스크 쉘프에서 즉시 디스크를 분리할 수 있습니다. 그러나 Rapid RAID 복구 프로세스가 완료되도록 부분적으로 오류가 발생한 디스크를 충분히 오랫동안 연결된 상태로 두어야 합니다.

이 작업에 대해

디스크에 오류가 발생했거나 과도한 오류 메시지가 발생하여 디스크를 제거하는 경우 이 스토리지 시스템이나 다른 스토리지 시스템에서 디스크를 다시 사용하지 마십시오.

단계

1. CLI를 사용하여 장애가 발생한 디스크의 디스크 ID를 찾습니다.

스토리지 디스크 고장

디스크가 실패한 디스크 목록에 나타나지 않으면 Rapid RAID Recovery 가 진행 중일 때 부분적으로 오류가 발생한 것일 수 있습니다. 이 경우 디스크를 제거하기 전에 디스크가 실패한 디스크 목록(Rapid RAID Recovery 프로세스가 완료되었음을 의미)에 나타날 때까지 기다려야 합니다.

2. 제거할 디스크의 물리적 위치를 확인합니다.

   'storage disk set-led-action on-disk_disk_name_2'

   디스크 면의 오류 LED가 켜져 있습니다.

3. 디스크 쉘프 모델의 하드웨어 가이드에 나와 있는 지침에 따라 디스크 쉘프에서 디스크를 꺼냅니다.

관련 정보

- "저장 디스크 세트-LED"
- "저장 디스크 표시"

디스크 삭제

ONTAP 디스크 삭제에 대해 알아보십시오

디스크 삭제는 디스크 또는 SSD를 지정된 바이트 패턴 또는 랜덤 데이터로 덮어써서 데이터를 물리적으로 삭제함으로써 원래 데이터의 복구가 불가능하게 하는 프로세스입니다. 삭제 프로세스를 사용하면 아무도 디스크에 있는 데이터를 복구할 수 없습니다.

이 기능은 모든 ONTAP 9 릴리스의 노드 쉘을 통해 사용할 수 있으며 유지보수 모드의 ONTAP 9.6부터 시작합니다.

디스크 삭제 프로세스에서는 3개의 연속적인 기본 또는 사용자 지정 바이트 덮어쓰기 패턴을 사용하여 작업당 최대 7주기를 지원합니다. 각 사이클마다 랜덤 덮어쓰기 패턴이 반복됩니다.

디스크 용량, 패턴 및 주기 수에 따라 이 프로세스에는 몇 시간이 걸릴 수 있습니다. 완전 삭제는 백그라운드에서 실행됩니다. 완전 삭제 프로세스의 상태를 시작, 중지 및 표시할 수 있습니다. 완전 삭제 프로세스에는 "포맷 단계"와 "패턴 덮어쓰기 단계"의 두 단계가 포함됩니다.

포맷 단계

포맷 단계에 대해 수행되는 작업은 다음 표와 같이 삭제 중인 디스크 클래스에 따라 달라집니다.

디스크 클래스	포맷 단계 작업
대용량 HDD	건너뜀
고성능 HDD	SCSI 포맷 작업
SSD를 지원합니다	SCSI 완전 삭제 작업

패턴 덮어쓰기 단계

지정한 덮어쓰기 패턴은 지정된 주기 수에 대해 반복됩니다.

완전 삭제 프로세스가 완료되면 지정된 디스크가 삭제된 상태입니다. 예비 상태로 자동 반환되지 않습니다. 새로 살균된 디스크를 다른 로컬 계층에 추가하려면 먼저 살균된 디스크를 스페어 풀로 반환해야 합니다.

ONTAP 디스크 삭제를 수행할 수 없는 경우에 대해 알아보십시오

이러한 상황에서는 디스크 정리를 수행할 수 없습니다.

- HA Pair 시스템의 경우 Takeover 모드에서 지원되지 않습니다.
- 읽기 가능성 또는 쓰기 가능성 문제로 인해 실패한 디스크에서는 이 작업을 수행할 수 없습니다.
- 랜덤 패턴을 사용하는 경우 한 번에 100개 이상의 디스크에서 수행할 수 없습니다.
- 어레이 LUN에서는 지원되지 않습니다.

ONTAP 디스크 삭제가 중단되면 어떻게 됩니까

사용자 개입 또는 정전 등의 예기치 않은 이벤트에 의해 디스크 삭제가 중단된 경우 ONTAP는 삭제 중인 디스크를 알려진 상태로 되돌리기 위한 조치를 취하지만 삭제 프로세스를 완료하기 전에 조치를 취해야 합니다.

디스크 삭제는 오래 실행되는 작업입니다. 완전 삭제 프로세스가 전원 장애, 시스템 장애 또는 수동 개입으로 중단된 경우 완전 삭제 프로세스를 처음부터 다시 수행해야 합니다. 디스크가 삭제로 지정되지 않았습니다.

디스크 삭제의 포맷 단계가 중단될 경우 ONTAP는 중단으로 손상된 디스크를 복구해야 합니다. 시스템을 재부팅한 후 1시간마다 한 번씩 ONTAP는 완전 삭제의 포맷 단계를 완료하지 않은 모든 삭제 대상 디스크를 검사합니다. 이러한 디스크가 있으면 ONTAP에서 해당 디스크를 복구합니다. 복구 방법은 디스크 유형에 따라 다릅니다. 디스크가 복구되면 해당 디스크에서 삭제 프로세스를 다시 실행할 수 있습니다. HDD의 경우 '-s' 옵션을 사용하여 포맷 단계가 다시 반복되지 않도록 지정할 수 있습니다.

삭제할 데이터가 포함된 **ONTAP** 로컬 계층을 만들고 백업하기 위한 팁입니다

삭제가 필요한 데이터를 포함하도록 로컬 계층을 만들거나 백업하는 경우 간단한 지침을 따르면 데이터를 삭제하는 데 걸리는 시간을 줄일 수 있습니다.

- 중요한 데이터가 포함된 로컬 계층이 필요한 것보다 커지지 않도록 하십시오.

  완전 삭제는 필요한 것보다 더 많은 시간, 디스크 공간 및 대역폭을 필요로 합니다.

- 중요한 데이터가 포함된 로컬 계층을 백업할 때는 중요하지 않은 데이터가 많은 로컬 계층에 백업하지 않도록 합니다.

  이렇게 하면 중요한 데이터를 살균하기 전에 중요한 데이터를 이동하는 데 필요한 리소스가 줄어듭니다.

ONTAP 디스크 완전 삭제

디스크를 제거하면 사용 중단되거나 작동 불가능한 시스템의 디스크 또는 디스크 세트에서 데이터를 제거하여 데이터를 복구할 수 없습니다.

CLI를 사용하여 디스크를 삭제하는 방법에는 두 가지가 있습니다.

ONTAP 9.6부터는 유지보수 모드에서 디스크 완전 삭제를 수행할 수 있습니다.

시작하기 전에

- 디스크는 SED(자체 암호화 디스크)가 될 수 없습니다.

  SED를 살균하려면 '스토리지 암호화 디스크 완전 삭제' 명령을 사용해야 합니다.

  "유휴 데이터의 암호화"

  에 대한 자세한 내용은 `storage encryption disk sanitize` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 유지보수 모드로 부팅합니다.
   a. 를 입력하여 현재 셸을 종료합니다 `halt`.

      LOADER 프롬프트가 표시됩니다.

   b. 를 입력하여 유지보수 모드로 전환합니다 `boot_ontap maint`.

      일부 정보가 표시된 후 유지보수 모드 프롬프트가 표시됩니다.

2. 삭제할 디스크가 파티션된 경우 각 디스크의 파티션을 해제합니다.

   > 디스크 파티션을 해제하는 명령은 진단 수준에서만 사용할 수 있으며 NetApp 지원팀의 감독하에 수행해야 합니다. 계속 진행하기 전에 NetApp 지원팀에 문의하는 것이 좋습니다. 또한 다음을 참조할 수도 있습니다."NetApp 지식 기반: ONTAP 에서 스페어 드라이브의 파티션을 해제하는 방법"

   ```
   disk unpartition <disk_name>
   ```

3. 지정된 디스크 완전 삭제:

   ```
   disk sanitize start [-p <pattern1>|-r [-p <pattern2>|-r [-p <pattern3>|-
   r]]] [-c <cycle_count>] <disk_list>
   ```

   > 삭제 중에 노드 전원을 끄거나 스토리지 연결을 중단하거나 타겟 디스크를 제거하지 마십시오. 포맷 단계에서 제거가 중단된 경우 디스크를 삭제하고 스페어 풀로 반환할 준비가 되기 전에 포맷 단계를 다시 시작하고 완료해야 합니다. 완전 삭제 프로세스를 중단해야 하는 경우 "disk sanitize abort" 명령을 사용하여 중단할 수 있습니다. 지정된 디스크가 완전 삭제의 포맷 단계를 진행 중인 경우 단계가 완료될 때까지 중단이 발생하지 않습니다.

`-p` `<pattern1>` `-p` `<pattern2>` `-p` `<pattern3>` 삭제되는 디스크에 연속적으로 적용할 수 있는 사용자 정의 16진수 바이트 덮어쓰기 패턴의 주기를 1-3개 지정합니다. 기본 패턴은 세 단계로, 첫 번째 패스는 0x55, 두 번째 패스는 0xAA, 세 번째 패스는 0x3c를 사용합니다.

'-r'은 패스의 일부 또는 전체에 대해 임의 덮어쓰기를 사용하여 패턴 덮어쓰기를 대체합니다.

-c <cycle_count> 지정된 덮어쓰기 패턴이 적용되는 횟수를 지정합니다. 기본값은 한 사이클입니다. 최대값은 7사이클입니다.

<disk_list> 삭제할 스페어 디스크의 ID 목록을 공백으로 구분하여 지정합니다.

4. 필요한 경우 디스크 삭제 프로세스의 상태를 확인합니다.

   ```
   disk sanitize status [<disk_list>]
   ```

5. 삭제 프로세스가 완료되면 각 디스크의 스페어 상태로 디스크를 반환합니다.

   ```
   disk sanitize release <disk_name>
   ```

6. 유지보수 모드를 종료합니다.

“noteswell ”명령(모든 ONTAP 9 릴리스)을 사용하여 디스크 완전 삭제

노드에서 nodeshell 명령을 사용하여 디스크 완전 삭제 기능을 설정한 후에는 해제할 수 없습니다.

시작하기 전에

- 디스크는 스페어 디스크여야 하며 노드에서 소유해야 하지만 로컬 계층에서는 사용되지 않습니다.

  디스크가 분할된 경우 로컬 계층에서 두 파티션을 사용할 수 없습니다.

- 디스크는 SED(자체 암호화 디스크)가 될 수 없습니다.

  SED를 살균하려면 '스토리지 암호화 디스크 완전 삭제' 명령을 사용해야 합니다.

  "유휴 데이터의 암호화"

- 디스크는 스토리지 풀에 포함될 수 없습니다.

단계

1. 삭제할 디스크가 파티션된 경우 각 디스크의 파티션을 해제합니다.

   ⓘ 디스크 파티션을 해제하는 명령은 진단 수준에서만 사용할 수 있으며 NetApp 지원팀의 감독하에 수행해야 합니다. 계속 진행하기 전에 **NetApp** 지원팀에 문의하는 것이 좋습니다**.** 또한 다음을 참조할 수도 있습니다."NetApp 지식 기반: ONTAP 에서 스페어 드라이브의 파티션을 해제하는 방법" .

   ```
   disk unpartition <disk_name>
   ```

2. 삭제할 디스크를 소유하는 노드에 대한 노드 선택을 입력합니다.

   ```
   system node run -node <node_name>
   ```

3. 디스크 삭제 활성화:

   "options licensed_feature.disk_densure.enable on"

   명령을 취소할 수 없으므로 확인하라는 메시지가 표시됩니다.

4. 노드 쉘의 고급 권한 레벨로 전환합니다.

   '한자 진일보한

5. 지정된 디스크 완전 삭제:

   ```
   disk sanitize start [-p <pattern1>|-r [-p <pattern2>|-r [-p <pattern3>|-
   r]]] [-c <cycle_count>] <disk_list>
   ```

   ⓘ 삭제 중에 노드 전원을 끄거나 스토리지 연결을 중단하거나 타겟 디스크를 제거하지 마십시오. 포맷 단계에서 제거가 중단된 경우 디스크를 삭제하고 스페어 풀로 반환할 준비가 되기 전에 포맷 단계를 다시 시작하고 완료해야 합니다. 완전 삭제 프로세스를 중단해야 하는 경우 disk sanitize abort 명령을 사용하여 중단할 수 있습니다. 지정된 디스크가 완전 삭제의 포맷 단계를 진행 중인 경우 단계가 완료될 때까지 중단이 발생하지 않습니다.

`-p <pattern1> -p <pattern2> -p <pattern3>` 삭제되는 디스크에 연속적으로 적용할 수 있는 사용자 정의 16진수 바이트 덮어쓰기 패턴의 주기를 1-3개 지정합니다. 기본 패턴은 세 단계로, 첫 번째 패스는 0x55, 두 번째 패스는 0xAA, 세 번째 패스는 0x3c를 사용합니다.

'-r'은 패스의 일부 또는 전체에 대해 임의 덮어쓰기를 사용하여 패턴 덮어쓰기를 대체합니다.

`-c <cycle_count>` 지정된 덮어쓰기 패턴이 적용되는 횟수를 지정합니다.

기본값은 한 사이클입니다. 최대값은 7사이클입니다.

`<disk_list>` 삭제할 스페어 디스크의 ID 목록을 공백으로 구분하여 지정합니다.

6. 디스크 삭제 프로세스의 상태를 확인하려면 다음과 같이 하십시오.

   ```
   disk sanitize status [<disk_list>]
   ```

7. 삭제 프로세스가 완료되면 디스크를 스페어 상태로 되돌립니다.

   ```
   disk sanitize release <disk_name>
   ```

8. 노드 관리자 권한 레벨로 돌아갑니다.

   'priv set admin'

9. ONTAP CLI로 돌아가기:

   종료

10. 모든 디스크가 스페어 상태로 돌아갔는지 확인합니다.

    '스토리지 집계 show-spare-disks'

만약…	그러면…
삭제된 모든 디스크가 스페어로 나열됩니다	완료되었습니다. 디스크가 삭제되었으며 예비 상태입니다.

삭제된 디스크 중 일부는 스페어로 나열되지 않습니다	다음 단계를 완료합니다.
	a. 고급 권한 모드 시작:
	세트 프리빌리지 고급
	b. 할당되지 않은 삭제된 디스크를 각 디스크의 적절한 노드에 할당합니다.
	`storage disk assign -disk <disk_name> -owner <node_name>`
	c. 디스크를 각 디스크의 예비 상태로 되돌립니다.
	`storage disk unfail -disk <disk_name> -s -q`
	d. 관리 모드로 돌아가기:
	'Set-Privilege admin'입니다

에 대한 자세한 내용은 `storage aggregate show-spare-disks` "ONTAP 명령 참조입니다"을 참조하십시오.

결과

지정된 디스크가 삭제되어 핫 스페어로 지정됩니다. 삭제된 디스크의 일련 번호는 '/etc/log/살균된_disks'에 기록됩니다.

각 디스크에서 완료된 작업을 보여 주는 지정된 디스크의 삭제 로그가 에 `/mroot/etc/log/sanitization.log`기록됩니다.

관련 정보

- "스토리지 애그리게이트 보기"
- "저장 디스크 할당"
- "저장 디스크가 고장나지 않음"
- "스토리지 암호화 디스크 정리"

디스크 관리를 위한 **ONTAP** 명령

'스토리지 디스크' 및 '스토리지 집계' 명령을 사용하여 디스크를 관리할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

원하는 작업	이 명령 사용…
분할된 디스크를 포함한 예비 디스크 목록을 소유자별로 표시합니다	'스토리지 집계 show-spare-disks'

디스크 RAID 유형, 현재 사용량 및 로컬 계층별 RAID 그룹을 표시합니다	'스토리지 집계 표시 상태'
물리 디스크의 RAID 유형, 현재 사용량, 로컬 계층 및 스페어를 포함한 RAID 그룹을 표시합니다	스토리지 디스크 show-raid
오류가 발생한 디스크 목록을 표시합니다	스토리지 디스크 고장
디스크의 사전 클러스터(notescope) 드라이브 이름을 표시합니다	스토리지 디스크 show-primary-paths(고급)
특정 디스크 또는 쉘프의 LED를 켭니다	'스토리지 디스크 세트 주도'
특정 디스크의 체크섬 유형을 표시합니다	'스토리지 디스크 표시-필드 체크섬-호환성
모든 스페어 디스크의 체크섬 유형을 표시합니다	'스토리지 디스크 표시-필드 체크섬-호환성-컨테이너-유형 스페어'
디스크 연결 및 배치 정보를 표시합니다	'스토리지 디스크 표시 필드 디스크, 운영 포트, 보조 이름, 보조 포트, 쉘프, 베이'
특정 디스크의 사전 클러스터 디스크 이름을 표시합니다	'스토리지 디스크 표시 - 디스크 디스크 이름 - 필드 diskpathnames'
유지보수 센터의 디스크 목록을 표시합니다	스토리지 디스크 show-maintenance
SSD 마모 수명을 표시합니다	'스토리지 디스크 표시-SSD 마모'
공유 디스크의 파티션을 해제합니다	'스토리지 디스크 파티션 해제'(진단 수준에서 사용 가능)
제로화되지 않은 모든 디스크를 제로화하십시오	'스토리지 디스크 제로'
하나 이상의 지정된 디스크에 대해 지속적인 삭제 프로세스를 중지합니다	'system node run-node notdename -command disk sanitize'
스토리지 암호화 디스크 정보를 표시합니다	스토리지 암호화 디스크 표시
연결된 모든 키 관리 서버에서 인증 키를 검색합니다	보안 키 관리자 복원

관련 정보

- "스토리지 애그리게이트 보기"
- "저장 디스크 세트-LED"
- "저장 디스크 표시"

- "저장 디스크 제로 스페어"
- "저장 암호화 디스크 표시"

공간 사용 정보를 표시하기 위한 **ONTAP** 명령입니다

및 `volume` 명령을 사용하여 `storage aggregate` 로컬 계층, 볼륨 및 해당 스냅샷에서 공간이 어떻게 사용되고 있는지 확인할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

정보를 표시하려면…	이 명령 사용…
사용된 공간 및 사용 가능한 공간 비율에 대한 세부 정보, 스냅숏 예비 공간 크기 및 기타 공간 사용 정보가 포함된 로컬 계층	'스토리지 집계 쇼' `storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve`
디스크 및 RAID 그룹이 로컬 계층에서 사용되는 방법 및 RAID 상태	'스토리지 집계 표시 상태'
특정 스냅샷을 삭제할 경우 재확보되는 디스크 공간의 양입니다	'볼륨 스냅샷 계산-재확보 가능'

볼륨에서 사용하는 공간입니다	`volume show -fields size,used,available,percent-used`
	
	`volume show-space`

포함하는 로컬 계층의 볼륨에서 사용하는 공간의 양입니다	볼륨 쇼 풋프린트

관련 정보

- "스토리지 애그리게이트 보기"
- "저장 집합 쇼 공간"
- "스토리지 집계 표시 상태"

스토리지 쉘프에 대한 정보를 표시하기 위한 **ONTAP** 명령입니다

'storage shelf show' 명령을 사용하면 디스크 쉘프의 구성 및 오류 정보를 표시할 수 있습니다.

를 표시하려면…	이 명령 사용…
쉘프 구성 및 하드웨어 상태에 대한 일반 정보입니다	'Storage shelf show'

를 표시하려면...	이 명령 사용...
스택 ID를 포함한 특정 쉘프에 대한 자세한 정보입니다	'Storage shelf show-shelf'
미해결, 고객 실행 가능, 쉘프별 오류	'Storage shelf show-errors'
베이 정보	'Storage shelf show-bay'입니다
연결 정보	'Storage shelf show-connectivity
온도 센서 및 냉각 팬을 포함한 냉각 정보	'Storage shelf show-cooling'
입출력 모듈에 대한 정보입니다	'Storage shelf show-module
포트 정보	'Storage shelf show-port'입니다
전원 정보(PSU(전원 공급 장치), 전류 센서 및 전압 센서 포함	'Storage shelf show-power'입니다

관련 정보

- "보관 선반 쇼"

RAID 구성을 관리합니다

ONTAP 로컬 계층에 대한 기본 RAID 정책

RAID-DP 또는 RAID-TEC는 모든 새로운 로컬 계층에 대한 기본 RAID 정책입니다. RAID 정책은 디스크 장애 시 발생하는 패리티 보호를 결정합니다.

RAID-DP는 단일 또는 이중 디스크 장애 시 이중 패리티 보호를 제공합니다. RAID-DP는 다음 로컬 계층 유형에 대한 기본 RAID 정책입니다.

- All Flash 로컬 계층
- Flash Pool 로컬 계층
- 고성능 하드 디스크 드라이브(HDD) 로컬 계층

RAID-TEC는 모든 디스크 유형과 AFF를 포함한 모든 플랫폼에서 지원됩니다. 더 큰 디스크가 포함된 로컬 계층은 동시 디스크 장애가 발생할 가능성이 더 높습니다. RAID-TEC는 데이터를 최대 3개의 동시 디스크 장애로부터 보호할 수 있도록 3중 패리티 보호를 제공하여 이러한 위험을 완화할 수 있도록 도와줍니다. RAID-TEC는 용량이 6TB 이상인 디스크를 사용하는 대용량 HDD 로컬 계층에 대한 기본 RAID 정책입니다.

각 RAID 정책 유형에는 최소 디스크 수가 필요합니다.

- RAID-DP: 최소 5개의 디스크
- RAID-TEC: 최소 7개의 디스크

디스크에 대한 **ONTAP RAID** 보호 수준

ONTAP는 로컬 계층에 대해 세 가지 수준의 RAID 보호를 지원합니다. RAID 보호 수준에 따라 디스크 장애 시 데이터 복구에 사용할 수 있는 패리티 디스크 수가 결정됩니다.

RAID 보호 기능을 사용하면 RAID 그룹에 데이터 디스크 장애가 있는 경우 ONTAP가 장애가 발생한 디스크를 스페어 디스크로 교체하고 패리티 데이터를 사용하여 장애가 발생한 디스크의 데이터를 재구성할 수 있습니다.

- * RAID4 *

  RAID4 보호 기능을 사용하면 ONTAP는 하나의 스페어 디스크를 사용하여 RAID 그룹 내에서 장애가 발생한 디스크 중 하나에서 데이터를 교체 및 재구성할 수 있습니다.

- RAID-DP * 를 지원합니다

  RAID-DP 보호를 통해 ONTAP는 최대 2개의 예비 디스크를 사용하여 RAID 그룹 내에서 동시에 장애가 발생한 최대 2개의 디스크에서 데이터를 교체 및 재구성할 수 있습니다.

- * RAID-TEC *

  RAID-TEC 보호를 통해 ONTAP는 최대 3개의 예비 디스크를 사용하여 RAID 그룹 내에서 동시에 장애가 발생한 최대 3개의 디스크에서 데이터를 교체 및 재구성할 수 있습니다.

ONTAP 로컬 계층에 대한 드라이브 및 **RAID** 그룹 정보

일부 로컬 계층 관리 작업에는 로컬 계층을 구성하는 드라이브 유형, 크기, 체크섬 및 상태, 다른 로컬 계층과 공유되는지 여부, RAID 그룹의 크기 및 구성을 알아야 합니다.

단계

1. 로컬 계층의 드라이브를 RAID 그룹별로 표시합니다.

   'Storage aggregate show-status_aggr_name_'

   로컬 계층의 각 RAID 그룹에 대한 드라이브가 표시됩니다.

   '위치' 열에서 드라이브의 RAID 유형(데이터, 패리티, dparity)을 확인할 수 있습니다. Position 열에 'Shared'가 표시되면 드라이브가 공유되고 HDD인 경우 분할된 디스크이고, SSD인 경우 스토리지 풀의 일부입니다.

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11       0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13       0   SSD       -  186.2GB  745.2GB (normal)
     shared   2.0.12       0   SSD       -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

관련 정보

- "스토리지 집계 표시 상태"

ONTAP RAID-DP에서 **RAID-TEC**로 변환합니다

3중 패리티 보호를 추가하려면 RAID-DP에서 RAID-TEC로 전환할 수 있습니다. 로컬 계층에 사용되는 디스크 크기가 4TiB보다 큰 경우 RAID-TEC를 사용하는 것이 좋습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

시작하기 전에

변환할 로컬 계층에 최소 7개의 디스크가 있어야 합니다.

이 작업에 대해

- 하드 디스크 드라이브(HDD) 로컬 계층을 RAID-DP에서 RAID-TEC로 변환할 수 있습니다. 여기에는 Flash Pool

로컬 계층의 HDD 계층이 포함됩니다.

-disktype을 사용하여 각 디스크 유형을 변경해야 하는 **flashpools/hybrid aggregates** 프로세스

[-T, -disktype {ATA | BSAS | FCAL | FSAS | LUN | MSATA | SAS | SSD | VMDISK | SSD-NVM | SSD-CAP | SSD-ZNS | VMLUN | VMLUN-SSD}] - 디스크 유형

이 매개변수는 수정할 RAID 그룹의 디스크 유형을 지정합니다. Flash Pool의 경우 HDD 계층 또는 SSD 계층 중 하나를 지정합니다. HDD 계층이 두 가지 이상의 디스크 유형으로 구성된 경우, 사용 중인 디스크 유형 중 하나를 지정하면 해당 계층이 수정됩니다. 현재 aggregate RAID 유형이 mixed_raid_type인 경우 이 매개변수는 필수입니다.

단계

1. 로컬 계층이 온라인 상태이고 최소 6개의 디스크가 있는지 확인합니다.

   'Storage aggregate show-status-aggregate_aggregate_name_'

2. 로컬 계층을 RAID-DP에서 RAID-TEC로 전환:

   'Storage aggregate modify -aggregate_aggregate_name_-raidtype RAID_Tec'

3. 로컬 계층 RAID 정책이 RAID-TEC인지 확인합니다.

   'STORAGE AGGATE SHOW_AGGATE_NAME_'

관련 정보

- "저장소 집계 수정"
- "스토리지 집계 표시 상태"

ONTAP RAID-TEC에서 **RAID-DP**로 변환합니다

로컬 계층의 크기를 줄이고 3중 패리티가 더 이상 필요하지 않은 경우 RAID 정책을 RAID-TEC에서 RAID-DP로 변환하고 RAID 패리티에 필요한 디스크 수를 줄일 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

시작하기 전에

RAID-TEC의 최대 RAID 그룹 크기가 RAID-DP의 최대 RAID 그룹 크기보다 큽니다. 최대 RAID-TEC 그룹 크기가 RAID-DP 제한 범위 내에 있지 않으면 RAID-DP로 변환할 수 없습니다.

이 작업에 대해

RAID 유형 간 변환의 의미를 이해하려면 명령의 를 참조하십시오 "매개 변수" `storage aggregate modify` .

단계

1. 로컬 계층이 온라인 상태이고 최소 6개의 디스크가 있는지 확인합니다.

   'Storage aggregate show-status-aggregate_aggregate_name_'

2. 로컬 계층을 RAID-TEC에서 RAID-DP로 전환:

'Storage aggregate modify -aggregate_aggregate_name_-raidtype RAID_DP'

3. 로컬 계층 RAID 정책이 RAID-DP인지 확인합니다.

   'STORAGE AGGATE SHOW_AGGATE_NAME_'

관련 정보

- "저장소 집계 수정"
- "스토리지 집계 표시 상태"

ONTAP RAID 그룹을 사이징할 때의 고려 사항

최적의 RAID 그룹 크기를 구성하려면 인수를 트레이드오프해야 합니다. RAID 재구성 속도, 드라이브 장애로 인한 데이터 손실 위험에 대한 보증, I/O 성능 최적화, 데이터 스토리지 공간 최대화 등 구성 중인 (로컬 계층) 애그리게이트에 가장 중요한 요소를 결정해야 합니다.

더 큰 RAID 그룹을 생성하면 패리티에 사용되는 것과 동일한 양의 스토리지(""패리티 세금"이라고도 함)에 대해 데이터 스토리지에 사용할 수 있는 공간을 극대화할 수 있습니다. 반면, 더 큰 RAID 그룹의 디스크에 장애가 발생할 경우 재구성 시간이 증가하여 장시간 성능에 영향을 미칩니다. 또한 RAID 그룹에 더 많은 디스크가 있을 경우 동일한 RAID 그룹 내에서 여러 디스크에 오류가 발생할 가능성이 높아집니다.

HDD 또는 어레이 LUN RAID 그룹

HDD 또는 어레이 LUN으로 구성된 RAID 그룹을 사이징할 때는 다음 지침을 따라야 합니다.

- 로컬 계층(애그리게이트)의 모든 RAID 그룹은 디스크 수가 동일해야 합니다.

  하나의 로컬 계층에 서로 다른 RAID 그룹의 디스크 수보다 최대 50% 적게 또는 많이 있을 수 있지만, 이로 인해 일부 경우 성능 병목 현상이 발생할 수 있으므로 피하는 것이 좋습니다.

- 권장되는 RAID 그룹 디스크 번호 범위는 12에서 20 사이입니다.

  성능 디스크의 안정성은 필요한 경우 최대 28개의 RAID 그룹 크기를 지원할 수 있습니다.

- 여러 개의 RAID 그룹 디스크 번호를 사용하여 처음 두 지침을 충족할 수 있는 경우 더 많은 수의 디스크를 선택해야 합니다.

Flash Pool 로컬 계층(애그리게이트)의 SSD RAID 그룹

SSD RAID 그룹 크기는 Flash Pool 로컬 계층(애그리게이트)에 있는 HDD RAID 그룹의 RAID 그룹 크기와 다를 수 있습니다. 일반적으로, 패리티에 필요한 SSD 수를 최소화하기 위해 Flash Pool 로컬 계층에 SSD RAID 그룹을 하나만 있어야 합니다.

SSD 로컬 계층(애그리게이트)의 SSD RAID 그룹

SSD로 구성된 RAID 그룹의 크기를 지정할 때 다음 지침을 따라야 합니다.

- 로컬 계층(애그리게이트)의 모든 RAID 그룹에는 비슷한 수의 드라이브가 있어야 합니다.

  RAID 그룹은 정확히 같은 크기를 가질 필요는 없지만 가능한 경우 동일한 로컬 계층에 있는 다른 RAID 그룹의 크기의 절반보다 작은 RAID 그룹을 가질 필요는 없습니다.

- RAID-DP의 경우 권장되는 RAID 그룹 크기 범위는 20에서 28 사이입니다.

ONTAP RAID 그룹의 크기를 사용자 지정합니다

RAID 그룹의 크기를 사용자 지정하여 RAID 그룹 크기가 로컬 계층에 포함할 스토리지 양에 적합한지 확인할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

이 작업에 대해

표준 로컬 계층의 경우 각 로컬 계층에 대한 RAID 그룹 크기를 개별적으로 변경합니다. Flash Pool 로컬 계층의 경우 SSD RAID 그룹 및 HDD RAID 그룹에 대한 RAID 그룹 크기를 독립적으로 변경할 수 있습니다.

다음 목록에서는 RAID 그룹 크기 변경에 대한 몇 가지 사항을 설명합니다.

- 기본적으로 가장 최근에 생성된 RAID 그룹의 디스크 또는 어레이 LUN 수가 새 RAID 그룹 크기보다 작은 경우 디스크 또는 어레이 LUN은 새 크기에 도달할 때까지 가장 최근에 생성된 RAID 그룹에 추가됩니다.
- 디스크를 명시적으로 추가하지 않는 한 해당 로컬 계층에 있는 다른 모든 기존 RAID 그룹은 동일한 크기를 유지합니다.
- RAID 그룹이 로컬 계층의 현재 최대 RAID 그룹 크기보다 커지게 만들 수는 없습니다.
- 이미 생성된 RAID 그룹의 크기는 줄일 수 없습니다.
- 새 크기는 해당 로컬 계층의 모든 RAID 그룹에 적용됩니다. Flash Pool 로컬 계층의 경우 영향을 받는 RAID 그룹 유형인 SSD 또는 HDD에 대한 모든 RAID 그룹에 적용됩니다.

단계

1. 해당 명령을 사용합니다.

원하는 작업	다음 명령을 입력합니다…
Flash Pool 로컬 계층의 SSD RAID 그룹에 대한 최대 RAID 그룹 크기를 변경합니다	'Storage aggregate modify-aggregate aggr_name-cache-raid-group-size'를 선택합니다
다른 RAID 그룹의 최대 크기를 변경합니다	'Storage aggregate modify -aggregate aggr_name -maxraidsize'를 선택합니다

예

다음 명령을 실행하면 로컬 계층 n1_A4의 최대 RAID 그룹 크기가 20개의 디스크 또는 어레이 LUN으로 변경됩니다.

'Storage aggregate modify -aggregate n1_A4-maxraidsize 20'을 선택합니다

다음 명령을 실행하면 Flash Pool 로컬 계층 n1_cache_A2의 SSD 캐시 RAID 그룹의 최대 RAID 그룹 크기가 24로 변경됩니다.

'Storage aggregate modify-aggregate n1_cache_a2-cache-raid-group-size 24'를 선택합니다

관련 정보

- "저장소 집계 수정"

Flash Pool 로컬 계층 관리

Flash Pool ONTAP 로컬 계층 캐싱 정책

Flash Pool 로컬 계층에 있는 볼륨에 대한 캐싱 정책을 사용하면 사용 중인 데이터 세트에 필요한 고성능 캐시로 플래시를 구축하는 동시에 액세스 빈도가 낮은 데이터에는 경제적인 HDD를 사용할 수 있습니다. 2개 이상의 Flash Pool 로컬 계층에 캐시를 제공하는 경우 Flash Pool SSD 파티셔닝을 사용하여 Flash Pool의 로컬 계층에서 SSD를 공유해야 합니다.

캐싱 정책은 Flash Pool 로컬 계층에 상주하는 볼륨에 적용됩니다. 캐시 정책을 변경하기 전에 캐싱 정책이 어떻게 작동하는지를 이해해야 합니다.

대부분의 경우 의 기본 캐싱 정책이 `auto` 가장 적합한 캐싱 정책입니다. 다른 정책이 워크로드에 더 나은 성능을 제공하는 경우에만 캐싱 정책을 변경해야 합니다. 잘못된 캐싱 정책을 구성하면 볼륨 성능이 심각하게 저하될 수 있으며 시간이 지남에 따라 성능 저하가 점차 증가할 수 있습니다.

캐싱 정책은 읽기 캐싱 정책과 쓰기 캐싱 정책을 결합합니다. 정책 이름은 읽기 캐싱 정책과 쓰기 캐싱 정책의 이름을 하이픈으로 구분하여 연결합니다. 정책 이름에 하이픈이 없으면 정책을 제외하고 쓰기 캐싱 정책은 입니다 `none`. `auto`

읽기 캐싱 정책은 HDD에 저장된 데이터 외에 데이터 복사본을 캐시에 배치하여 향후 읽기 성능을 최적화합니다. 쓰기 작업을 위해 캐시에 데이터를 삽입하는 읽기 캐싱 정책의 경우 캐시는 _write-through_cache로 작동합니다.

쓰기 캐싱 정책을 사용하여 캐시에 삽입된 데이터는 캐시에만 존재하며 HDD에는 복사본이 없습니다. Flash Pool 캐시는 RAID로 보호됩니다. 쓰기 캐시를 사용하면 쓰기 작업에서 데이터를 캐시에서 읽을 수 있도록 즉시 제공할 수 있으며, 캐시에서 노후화될 때까지 HDD에 데이터를 쓰지 지연시킬 수 있습니다.

볼륨을 Flash Pool 로컬 계층에서 단일 계층 로컬 계층으로 이동하면 캐싱 정책이 손실됩니다. 나중에 Flash Pool 로컬 계층으로 다시 이동하면 기본 캐싱 정책이 할당됩니다. `auto` 두 Flash Pool 로컬 계층 간에 볼륨을 이동할 경우 캐싱 정책이 유지됩니다.

캐싱 정책을 변경합니다

CLI를 사용하면 '-caching-policy' 매개 변수와 'volume create' 명령을 사용하여 Flash Pool 로컬 계층에 상주하는 볼륨의 캐싱 정책을 변경할 수 있습니다.

Flash Pool 로컬 계층에 볼륨을 생성하는 경우 기본적으로 `auto` 캐싱 정책이 볼륨에 할당됩니다.

Flash Pool 캐싱 정책 관리

Flash Pool 로컬 계층의 ONTAP 캐싱 정책을 수정할지 여부를 결정합니다

Flash Pool 로컬 계층의 볼륨에 캐시 보존 정책을 할당하여 볼륨 데이터가 Flash Pool 캐시에 유지되는 기간을 결정할 수 있습니다. 그러나 캐시 보존 정책을 변경해도 볼륨의 데이터가 캐시에 남아 있는 시간에 영향을 주지 않는 경우도 있습니다.

이 작업에 대해

데이터가 다음 조건 중 하나를 충족하는 경우 캐시 보존 정책을 변경해도 영향이 없을 수 있습니다.

- 워크로드는 순차적입니다.
- 워크로드가 SSD(Solid State Drive)에 캐시된 랜덤 블록을 다시 읽지는 않습니다.
- 볼륨의 캐시 크기가 너무 작습니다.

단계

다음 단계에서는 데이터가 충족해야 하는 조건을 확인합니다. 고급 권한 모드에서 CLI를 사용하여 작업을 수행해야 합니다.

1. CLI를 사용하여 워크로드 볼륨 확인:

   '스타티틱스 스타트-객체 워크로드_볼륨'

2. 볼륨의 워크로드 패턴 결정:

   'tistics show-object workload_volume-instance_volume-workload_-counter sequential_reads'

3. 볼륨의 적중률을 확인합니다.

   ```
   statistics show -object wafl_hya_vvol -instance volume -counter
   read_ops_replaced_percent|wc_write_blks_overwritten_percent
   ```

4. 볼륨의 '캐시 가능 읽기' 및 '프로젝트 캐시 할당'을 결정합니다.

   'System node run-node node_name WAFL awa start_aggr_name_'

5. AWA 요약 정보를 표시합니다.

   '시스템 노드 run-node node_name WAFL awa print_aggr_name_'

6. 볼륨의 적중률을 "캐시 가능 읽기"와 비교합니다.

   볼륨의 적중률이 '캐시 가능 읽기'보다 높을 경우 SSD에 캐시된 랜덤 블록을 다시 읽을 수 없습니다.

7. 볼륨의 현재 캐시 크기를 Project Cache Alloc과 비교합니다.

   볼륨의 현재 캐시 크기가 Project Cache Alloc보다 크면 볼륨 캐시의 크기가 너무 작습니다.

관련 정보

- "통계에 따르면"
- "통계 시작"

ONTAP Flash Pool 로컬 계층의 캐싱 정책 수정

다른 캐싱 정책이 더 나은 성능을 제공할 것으로 예상되는 경우에만 볼륨의 캐싱 정책을 수정해야 합니다. Flash Pool 로컬 계층에서 볼륨의 캐싱 정책을 수정할 수 있습니다.

시작하기 전에

캐싱 정책을 수정할지 여부를 결정해야 합니다.

이 작업에 대해

대부분의 경우 의 기본 캐싱 정책은 `auto` 사용할 수 있는 최상의 캐싱 정책입니다. 다른 정책이 워크로드에 더 나은 성능을 제공하는 경우에만 캐싱 정책을 변경해야 합니다. 잘못된 캐싱 정책을 구성하면 볼륨 성능이 심각하게 저하될 수 있으며 시간이 지남에 따라 성능 저하가 점차 증가할 수 있습니다. 캐싱 정책을 수정할 때는 주의해야 합니다. 캐싱 정책이 변경된 볼륨에 성능 문제가 발생하면 캐싱 정책을 로 반환해야 `auto` 합니다.

단계

1. CLI를 사용하여 볼륨의 캐싱 정책을 수정합니다.

   'volume modify -volume_volume_name_-caching-policy_policy_name_'

예

다음 예제에서는 이라는 이름의 볼륨에 대한 캐싱 정책을 `vol2` `none` 수정합니다.

'volume modify-volume vol2-caching-policy none'

ONTAP Flash Pool 로컬 계층에 대한 캐시 보존 정책을 설정합니다

Flash Pool 로컬 계층의 볼륨에 캐시 보존 정책을 할당할 수 있습니다. 캐시 보존 정책이 높은 볼륨의 데이터는 더 오랫동안 캐시에 유지되며 캐시 보존 정책이 낮은 볼륨의 데이터는 더 빨리 제거됩니다. 따라서 높은 우선 순위의 정보에 더 빠른 속도로 액세스하여 중요한 워크로드의 성능을 높일 수 있습니다.

시작하기 전에

시스템에 캐시 보존 정책이 캐시에 있는 데이터의 유지 기간에 영향을 미치지 않도록 하는 조건이 있는지 여부를 확인해야 합니다.

단계

고급 권한 모드에서 CLI를 사용하여 다음 단계를 수행합니다.

1. 권한 설정을 고급으로 변경합니다.

   세트 프리빌리지 고급

2. 볼륨의 캐시 보존 정책을 확인합니다.

   기본적으로 캐시 보존 정책은 ""정상""입니다.

3. 캐시 보존 정책 설정:

   ```
   volume modify -volume volume_name -vserver vserver_name -caching-policy
   policy_name
   ```

4. 볼륨의 캐시 보존 정책이 선택한 옵션으로 변경되었는지 확인합니다.
5. 권한 설정을 admin으로 되돌립니다.

   'Set-Privilege admin'입니다

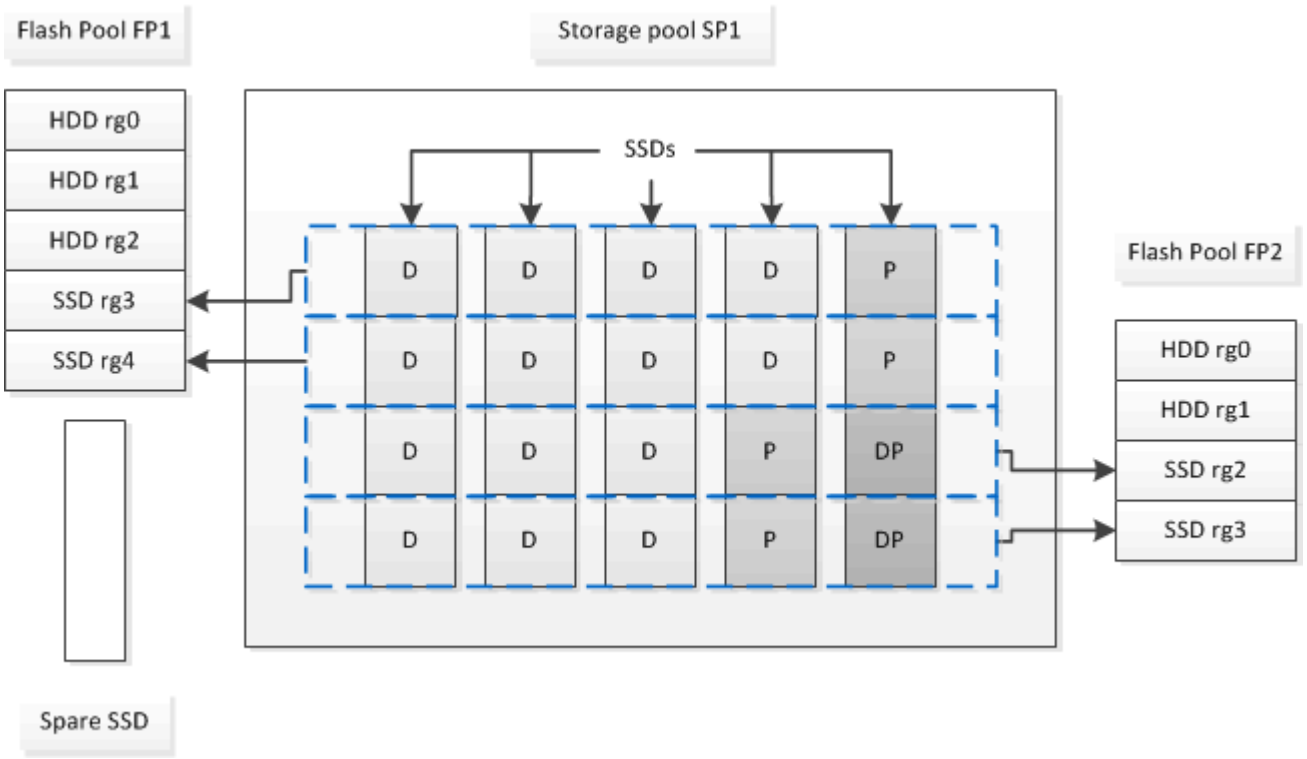
2개 이상의 Flash Pool 로컬 계층에 캐시를 제공하는 경우에는 Flash Pool SSD(Solid State Drive) 파티셔닝을 사용해야 합니다. Flash Pool SSD 파티셔닝으로 Flash Pool을 사용하는 모든 로컬 계층에서 SSD를 공유할 수 있습니다. 이를 통해 여러 로컬 계층에 패리티 비용을 분산하고, SSD 캐시 할당 유연성을 높이고, SSD 성능을 극대화할 수 있습니다.

Flash Pool 로컬 계층에서 SSD를 사용하려면 SSD를 스토리지 풀에 배치해야 합니다. 스토리지 풀에서 루트 데이터 파티셔닝으로 분할된 SSD는 사용할 수 없습니다. SSD를 스토리지 풀에 배치한 후에는 SSD를 더 이상 독립 실행형 디스크로 관리할 수 없으며, Flash Pool에 연결된 로컬 계층을 제거하고 스토리지 풀을 제거하지 않는 한 스토리지 풀에서 제거할 수 없습니다.

SSD 스토리지 풀은 4개의 동일한 할당 유닛으로 나뉩니다. 스토리지 풀에 추가된 SSD는 4개의 파티션으로 분할되며 4개의 할당 유닛 각각에 하나의 파티션이 할당됩니다. 스토리지 풀의 SSD는 동일한 HA 쌍이 소유해야 합니다. 기본적으로 HA 2노드의 각 노드에 2개의 할당 유닛이 할당됩니다. 할당 단위는 서비스가 제공되는 로컬 계층을 소유하는 노드에서 소유해야 합니다. 노드 중 하나의 로컬 계층에 더 많은 플래시 캐시가 필요한 경우 기본 할당 유닛 수를 이동하여 하나의 노드에서 수를 줄이고 파트너 노드의 수를 늘릴 수 있습니다.

예비 SSD를 사용하여 SSD 스토리지 풀에 추가합니다. 스토리지 풀에서 HA 쌍의 두 노드가 소유한 Flash Pool 로컬 계층에 할당 유닛을 제공하는 경우 두 노드 중 하나에서 스페어 SSD를 소유할 수 있습니다. 하지만 스토리지 풀에서 HA 쌍 중 하나의 노드가 소유한 Flash Pool 로컬 계층에만 할당 유닛을 제공하는 경우 해당 SSD 스페어는 동일한 노드에서 소유해야 합니다.

다음 그림은 Flash Pool SSD 파티셔닝의 예입니다. SSD 스토리지 풀은 2개의 Flash Pool 로컬 계층에 캐시를 제공합니다.



스토리지 풀 SP1은 5개의 SSD와 핫 스페어 SSD로 구성됩니다. 스토리지 풀의 할당 유닛 중 2개가 Flash Pool FP1에 할당되고 2개는 Flash Pool FP2에 할당됩니다. FP1에는 RAID4의 캐시 RAID 유형이 있습니다. 따라서 FP1에 제공된 할당 유닛에는 패리티로 지정된 파티션이 하나만 있습니다. FP2에는 RAID-DP의 캐시 RAID 유형이 있습니다. 따라서 FP2에 제공된 할당 유닛에는 패리티 파티션과 이중 패리티 파티션이 포함됩니다.

이 예에서는 각 Flash Pool 로컬 계층에 2개의 할당 유닛이 할당됩니다. 그러나 Flash Pool 로컬 계층 중 하나에 더 큰 캐시가 필요한 경우 해당 Flash Pool 로컬 계층에 3개의 할당 유닛을 할당하고 다른 계층에는 1개만 할당할 수 있습니다.

ONTAP Flash Pool의 적합성과 최적의 캐시 크기를 결정합니다

기존 로컬 계층을 Flash Pool 로컬 계층으로 변환하기 전에 먼저 로컬 계층이 I/O 바인딩인지, 워크로드와 예산에 맞는 최상의 Flash Pool 캐시 크기인지 확인할 수 있습니다. 또한 기존 Flash Pool 로컬 계층의 캐시가 올바르게 사이징되었는지 확인할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

시작하기 전에

분석 중인 로컬 계층에 최대 로드가 발생하는 경우 대략 알아야 합니다.

단계

1. 고급 모드 진입:

   진일진일보한 것

2. 기존 로컬 계층이 Flash Pool 로컬 계층으로 변환하는 데 적합한지 여부를 판단해야 하는 경우, 로컬 계층의 디스크 사용량이 가장 많은 기간 동안 얼마나 사용되고 있는지, 그리고 이것이 지연 시간에 어떤 영향을 미치는지 확인하십시오.

   S tistics show -periodic -object disk:raid_group -instance_raid_group_name _ -counter disk_busy|user_read_latency -interval 1 - iterations 60

   이 로컬 계층에 Flash Pool 캐시를 추가하여 지연 시간 단축 여부를 결정할 수 있습니다.

   다음 명령은 로컬 계층 "'aggr1'"의 첫 번째 RAID 그룹에 대한 통계를 보여 줍니다.

   S tistics show -periodic -object disk:raid_group -instance/aggr1/plex0/rg0 -counter disk_busy|user_read_latency -interval 1 -iterations 60'

3. AWA(Automated Workload Analyzer) 시작:

   'Storage automated-working-set-analyzer start-node_node_name_-aggregate_aggr_name_'

   Awa는 지정된 로컬 계층과 연결된 볼륨에 대한 워크로드 데이터를 수집하기 시작합니다.

4. 고급 모드 종료:

   '관리자 설정'을 선택합니다

   최대 부하 간격이 하나 이상 발생할 때까지 AWA가 실행되도록 합니다. Awa는 지정된 로컬 계층과 연결된 볼륨에 대한 워크로드 통계를 취합하고 최대 1주간의 연속 데이터를 분석합니다. 1주일 이상 AWA를 실행하면 가장 최근 주로부터 수집된 데이터만 보고됩니다. 캐시 크기 추정치는 데이터 수집 기간 동안 가장 높은 로드를 기준으로 하며, 전체 데이터 수집 기간 동안 로드가 높을 필요는 없습니다.

5. 고급 모드 진입:

   진일진일보한 것

6. 워크로드 분석 표시:

   'Storage automated-working-set-analyzer show -node_node_name_-instance'

7. AWA 중지:

   'Storage automated-working-set-analyzer stop_node_name_'

   모든 워크로드 데이터가 플러시되고 더 이상 분석에 사용할 수 없습니다.

8. 고급 모드 종료:

   '관리자 설정'을 선택합니다

관련 정보

- "통계 표시-주기적"
- "저장 자동화 작업 세트 분석기 표시"
- "저장 자동화 작업 세트 분석기 시작"
- "저장 자동화 작업 세트 분석기 중지"

물리적 **SSD**를 사용하여 **ONTAP Flash Pool** 로컬 계층을 생성합니다

Flash Pool 로컬 계층은 HDD RAID 그룹으로 구성된 기존 로컬 계층에 대해 기능을 활성화한 다음 해당 로컬 계층에 하나 이상의 SSD RAID 그룹을 추가하여 Flash Pool 로컬 계층을 생성합니다. 따라서 로컬 계층에 대해 SSD RAID 그룹(SSD 캐시)과 HDD RAID 그룹의 두 RAID 그룹 세트가 생성됩니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

이 작업에 대해

SSD 캐시를 로컬 계층에 추가하여 Flash Pool 로컬 계층을 생성한 후에는 SSD 캐시를 제거하여 로컬 계층을 다시 원래 구성으로 변환할 수 없습니다.

기본적으로 SSD 캐시의 RAID 레벨은 HDD RAID 그룹의 RAID 레벨과 같습니다. 첫 번째 SSD RAID 그룹을 추가할 때 옵션을 지정하여 이 기본 선택 항목을 재정의할 수 있습니다 `raidtype`.

시작하기 전에

- Flash Pool 로컬 계층으로 변환하려면 HDD로 구성된 유효한 로컬 계층을 식별해야 합니다.
- 로컬 계층과 연결된 볼륨의 쓰기 캐싱 적격성을 확인하고 자격 문제를 해결하기 위해 필요한 모든 단계를 완료해야 합니다.
- 추가할 SSD를 결정해야 하며, 이러한 SSD는 Flash Pool 로컬 계층을 생성할 노드에서 소유해야 합니다.

- 추가할 SSD와 HDD가 모두 로컬 계층에 있는지 확인해야 합니다.
- SSD RAID 그룹에 추가할 SSD 수와 최적의 RAID 그룹 크기를 결정해야 합니다.

  SSD 캐시에 더 적은 RAID 그룹을 사용하면 필요한 패리티 디스크 수가 감소하지만, RAID 그룹이 클수록 RAID-DP가 필요합니다.

- SSD 캐시에 사용할 RAID 레벨을 결정해야 합니다.
- 시스템의 최대 캐시 크기를 결정하고 SSD 캐시를 로컬 계층에 추가할 때 캐시 크기를 초과하지 않는지 확인해야 합니다.
- Flash Pool 로컬 계층에 대한 구성 요구사항을 숙지하고 있어야 합니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 Flash Pool 로컬 계층을 생성할 수 있습니다.

시스템 관리자

ONTAP 9.12.1부터는 시스템 관리자를 사용하여 물리적 SSD를 사용하여 Flash Pool 로컬 계층을 생성할 수 있습니다.

단계

1. 스토리지 > 계층 * 을 선택한 후 기존의 로컬 HDD 스토리지 계층을 선택합니다.
2. Add Flash Pool Cache * 를 선택한 후 * 를 선택합니다 ⋮ .
3. 전용 SSD를 캐시로 사용**을 선택합니다.
4. 디스크 유형과 디스크 수를 선택합니다.
5. RAID 유형을 선택합니다.
6. 저장 * 을 선택합니다.
7. 저장 계층을 찾은 다음 선택하세요.⋮
8. More Details * 를 선택합니다. Flash Pool이 * 사용 * 으로 표시되는지 확인합니다.

CLI를 참조하십시오

단계

1. 로컬 계층을 Flash Pool 로컬 계층으로 지정할 수 있음:

   'Storage aggregate modify -aggregate_aggr_name_-hybrid-enabled true'

   이 단계가 성공하지 못하면 타겟 로컬 계층에 대한 쓰기 캐싱 적합성을 확인합니다.

2. 명령을 사용하여 로컬 계층에 SSD를 추가합니다 `storage aggregate add`.
   - ID를 기준으로 또는 disskcount와 dissktype 매개 변수를 사용하여 SSD를 지정할 수 있습니다.
   - HDD와 SSD의 체크섬 유형이 동일하지 않거나 로컬 계층이 혼합 체크섬 로컬 계층인 경우 매개 변수를 사용하여 로컬 계층에 추가할 디스크의 체크섬 `checksumstyle` 유형을 지정해야 합니다.
   - "raidtype" 매개 변수를 사용하여 SSD 캐시에 다른 RAID 유형을 지정할 수 있습니다.
   - 캐시 RAID 그룹 크기를 사용 중인 RAID 유형의 기본값과 다르게 하려면 '-cache-raid-group-size' 매개 변수를 사용하여 캐시 RAID 그룹 크기를 변경해야 합니다.

관련 정보

- "저장소 집계 추가"
- "저장소 집계 수정"

SSD 스토리지 풀을 사용하여 **Flash Pool** 로컬 계층을 생성합니다

ONTAP Flash Pool 로컬 계층에서 **SSD** 스토리지 풀을 사용하고 있는지 확인합니다

SSD 스토리지 풀의 하나 이상의 할당 유닛을 기존 HDD 로컬 계층에 추가하여 Flash Pool 로컬 계층을 구성할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

SSD 스토리지 풀을 사용하여 캐시를 제공할 때는 Flash Pool 로컬 계층이 별도의 SSD를 사용할 때와 다르게 관리됩니다.

단계

1. RAID 그룹별로 로컬 계층의 드라이브를 표시합니다.

   'Storage aggregate show-status_aggr_name_'

   로컬 계층에서 하나 이상의 SSD 스토리지 풀을 사용하는 경우 SSD RAID 그룹의 열 값이 `Position` 로 표시되고 스토리지 풀의 이름이 RAID 그룹 이름 옆에 표시됩니다 `Shared`.

관련 정보

- "스토리지 집계 표시 상태"

SSD 스토리지 풀을 생성하여 **ONTAP** 로컬 계층에 캐시를 추가합니다

SSD(Solid State Drive)를 추가하여 기존 로컬 계층을 Flash Pool 로컬 계층으로 변환하여 캐시를 프로비저닝할 수 있습니다.

SSD(Solid State Drive) 스토리지 풀을 생성하여 2~4개의 Flash Pool 로컬 계층에 SSD 캐시를 제공할 수 있습니다. Flash Pool 로컬 계층을 사용하면 작업 데이터 세트를 위한 고성능 캐시로 플래시를 구축하고 액세스 빈도가 낮은 데이터에는 경제적인 HDD를 사용할 수 있습니다.

이 작업에 대해

- 스토리지 풀에 디스크를 생성하거나 추가할 때 디스크 목록을 제공해야 합니다.

  스토리지 풀은 disskcount 매개 변수를 지원하지 않습니다.

- 스토리지 풀에 사용된 SSD의 크기는 같아야 합니다.

시스템 관리자

시스템 관리자를 사용하여 **SSD** 캐시 추가**(ONTAP 9.12.1** 이상**)**

ONTAP 9.12.1부터 시스템 관리자를 사용하여 SSD 캐시를 추가할 수 있습니다.

AFF 시스템에서는 스토리지 풀 옵션을 사용할 수 없습니다.

단계

1. 클러스터 > 디스크 * 를 클릭한 다음 * 표시/숨기기 * 를 클릭합니다.
2. Type * 을 선택하고 클러스터에 예비 SSD가 있는지 확인합니다.
3. 클릭하여 * 스토리지 > 계층 * 으로 이동한 다음 * 스토리지 풀 추가 * 를 클릭합니다.
4. 디스크 유형을 선택합니다.
5. 디스크 크기를 입력합니다.
6. 스토리지 풀에 추가할 디스크 수를 선택합니다.
7. 예상 캐시 크기를 검토합니다.

System Manager를 사용하여 **SSD** 캐시 추가**(ONTAP 9.7**만 해당**)**

ONTAP 9.7 이상 또는 ONTAP 9.12.1 이전 버전의 ONTAP를 사용하는 경우 CLI 절차를 사용하십시오.

단계

1. (클래식 버전으로 돌아가기) * 를 클릭합니다.
2. 스토리지 > 애그리게이트 및 디스크 > 애그리게이트 * 를 클릭합니다.
3. 로컬 계층을 선택한 다음 * Actions > Add Cache * 를 클릭합니다.
4. 캐시 소스를 "스토리지 풀" 또는 "전용 SSD"로 선택합니다.
5. (새로운 환경으로 전환) * 을 클릭합니다.
6. 스토리지 > 계층 * 을 클릭하여 새로운 로컬 계층의 크기를 확인합니다.

CLI를 참조하십시오

- CLI를 사용하여 SSD 스토리지 풀을 생성합니다 *

단계

1. 사용 가능한 스페어 SSD의 이름을 확인합니다.

   'Storage aggregate show-spare-disks-disk-type ssd'를 선택합니다

   스토리지 풀에 사용된 SSD는 HA 쌍의 두 노드 중 하나에서 소유할 수 있습니다.

2. 스토리지 풀을 생성합니다.

스토리지 풀 create-storage-pool_sp_name_-disk-list_disk1_,*disk2*,

3. * 선택 사항: * 새로 생성된 스토리지 풀을 확인합니다.

   'storage pool show -storage -pool_sp_name_'을 선택합니다

결과

스토리지 풀에 SSD를 배치한 후에는 스토리지 풀에서 제공하는 스토리지가 Flash Pool 캐시에 아직 할당되지 않았더라도 클러스터에서 스페어로 표시되지 않습니다. RAID 그룹에 SSD를 개별 드라이브로 추가할 수는 없습니다. SSD의 스토리지는 SSD가 속한 스토리지 풀의 할당 유닛을 통해서만 프로비저닝할 수 있습니다.

관련 정보

- "스토리지 애그리게이트 보기"
- "스토리지 풀 생성"
- "저장 풀 쇼"

SSD 스토리지 풀 할당 유닛을 사용하여 **ONTAP Flash Pool** 로컬 계층을 생성합니다

SSD 스토리지 풀의 하나 이상의 할당 유닛을 기존 HDD 로컬 계층에 추가하여 Flash Pool 로컬 계층을 구성할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

ONTAP 9.12.1부터는 재설계된 시스템 관리자를 사용하여 스토리지 풀 할당 유닛을 사용하여 Flash Pool 로컬 계층을 생성할 수 있습니다.

시작하기 전에

- Flash Pool 로컬 계층으로 변환하려면 HDD로 구성된 유효한 로컬 계층을 식별해야 합니다.
- 로컬 계층과 연결된 볼륨의 쓰기 캐싱 적격성을 확인하고 자격 문제를 해결하기 위해 필요한 모든 단계를 완료해야 합니다.
- SSD 캐시를 이 Flash Pool 로컬 계층에 제공하려면 SSD 스토리지 풀을 생성해야 합니다.

  사용할 스토리지 풀의 할당 유닛은 Flash Pool 로컬 계층을 소유하는 동일한 노드에서 소유해야 합니다.

- 로컬 계층에 추가할 캐시의 양을 결정해야 합니다.

  할당 단위로 캐시를 로컬 계층에 추가합니다. 여유 공간이 있는 경우 나중에 스토리지 풀에 SSD를 추가하여 할당 유닛의 크기를 늘릴 수 있습니다.

- SSD 캐시에 사용할 RAID 유형을 결정해야 합니다.

  SSD 스토리지 풀에서 로컬 계층에 캐시를 추가한 후에는 캐시 RAID 그룹의 RAID 유형을 변경할 수 없습니다.

- 시스템의 최대 캐시 크기를 결정하고 SSD 캐시를 로컬 계층에 추가할 때 캐시 크기를 초과하지 않는지 확인해야 합니다.

'storage pool show' 명령을 사용하면 총 캐시 크기에 추가될 캐시의 양을 확인할 수 있습니다.

- Flash Pool 로컬 계층에 대한 구성 요구사항을 숙지하고 있어야 합니다.

이 작업에 대해

캐시의 RAID 유형을 HDD RAID 그룹과 다르게 하려면 SSD 용량을 추가할 때 캐시 RAID 유형을 지정해야 합니다. SSD 용량을 로컬 계층에 추가한 후에는 캐시의 RAID 유형을 더 이상 변경할 수 없습니다.

SSD 캐시를 로컬 계층에 추가하여 Flash Pool 로컬 계층을 생성한 후에는 SSD 캐시를 제거하여 로컬 계층을 다시 원래 구성으로 변환할 수 없습니다.

시스템 관리자

ONTAP 9.12.1부터 시스템 관리자를 사용하여 SSD 스토리지 풀에 SSD를 추가할 수 있습니다.

단계

1. Storage > Tiers * 를 클릭하고 기존 로컬 HDD 스토리지 계층을 선택합니다.
2. 를 ⋮ 클릭하고 * Add Flash Pool Cache * 를 선택합니다.
3. 스토리지 풀 사용 * 을 선택합니다.
4. 스토리지 풀을 선택합니다.
5. 캐시 크기 및 RAID 구성을 선택합니다.
6. 저장 * 을 클릭합니다.
7. 저장 계층을 다시 찾아 클릭하세요. ⋮
8. More Details * 를 선택하고 Flash Pool이 * Enabled * 로 표시되는지 확인합니다.

CLI를 참조하십시오

단계

1. 로컬 계층을 Flash Pool 로컬 계층으로 지정할 수 있음:

   'Storage aggregate modify -aggregate_aggr_name_-hybrid-enabled true'

   이 단계가 성공하지 못하면 타겟 로컬 계층에 대한 쓰기 캐싱 적합성을 확인합니다.

2. 사용 가능한 SSD 스토리지 풀 할당 유닛을 표시합니다.

   'Storage pool show-available-capacity'를 표시합니다

3. SSD 용량을 로컬 계층에 추가합니다.

   'storage aggregate add_aggr_name_-storage-pool_sp_name_-allocation-units_number_of_units_'

   캐시의 RAID 유형을 HDD RAID 그룹과 다르게 하려면 이 명령을 입력할 때 "raidtype" 매개 변수를 사용하여 변경해야 합니다.

   새 RAID 그룹을 지정할 필요가 없습니다. ONTAP는 SSD 캐시를 HDD RAID 그룹과 별도의 RAID 그룹으로 자동 배치합니다.

   캐시의 RAID 그룹 크기는 스토리지 풀의 SSD 수에 따라 결정됩니다.

   캐시가 로컬 계층에 추가되고 로컬 계층이 Flash Pool 로컬 계층이 됩니다. 로컬 계층에 추가된 각 할당 유닛은 자체 RAID 그룹이 됩니다.

4. SSD 캐시의 존재 및 크기 확인:

   'STORAGE AGGATE SHOW_AGGATE_NAME_'

   캐시 크기는 총 하이브리드 캐시 크기 아래에 나열됩니다.

관련 정보

- "NetApp 기술 보고서 4070: Flash Pool 설계 및 구축 가이드 를 참조하십시오"
- "저장소 집계 추가"
- "저장소 집계 수정"
- "저장 풀 쇼"
- "스토리지 풀 사용 가능 용량 표시"

SSD를 **SSD** 스토리지 풀에 추가할 때 **ONTAP** 캐시 크기에 미치는 영향을 확인합니다

스토리지 풀에 SSD를 추가하여 플랫폼 모델의 캐시 제한을 초과할 경우 ONTAP은 새로 추가된 용량을 Flash Pool 로컬 계층에 할당하지 않습니다. 이로 인해 새로 추가된 일부 또는 모든 용량을 사용할 수 없게 될 수 있습니다.

이 작업에 대해

Flash Pool 로컬 계층에 이미 할당된 할당 유닛이 있는 SSD 스토리지 풀에 SSD를 추가하면 각 로컬 계층의 캐시 크기와 시스템의 총 캐시가 증가합니다. 스토리지 풀의 할당 유닛이 할당되지 않은 경우 해당 스토리지 풀에 SSD를 추가해도 캐시에 할당된 할당 유닛이 하나 이상 할당될 때까지 SSD 캐시 크기에 영향을 주지 않습니다.

단계

1. 스토리지 풀에 추가할 SSD의 사용 가능한 크기를 결정합니다.

   'storage disk show_disk_name_-fields usable-size'를 선택합니다

2. 스토리지 풀에 할당되지 않은 할당 유닛 수 결정:

   'Storage pool show-available-capacity_sp_name_'

   스토리지 풀의 할당되지 않은 모든 할당 유닛이 표시됩니다.

3. 다음 수식을 적용하여 추가할 캐시의 양을 계산합니다.

   (할당되지 않은 할당 유닛 수 4개) × 25% × 사용 가능 크기 × SSD 수

관련 정보

- "저장 디스크 표시"
- "스토리지 풀 사용 가능 용량 표시"

ONTAP SSD 스토리지 풀에 **SSD**를 추가합니다

SSD(Solid State Drive)를 SSD 스토리지 풀에 추가하면 스토리지 풀의 물리적 크기 및 사용 가능한 크기와 할당 유닛 크기가 증가합니다. 할당 유닛 크기가 클수록 로컬 계층에 이미 할당된 할당 유닛에도 영향을 미칩니다.

시작하기 전에

이 작업으로 인해 HA 쌍의 캐시 제한이 초과되지 않는지 확인해야 합니다. ONTAP에서는 SSD 스토리지 풀에 SSD를 추가할 때 캐시 한도를 초과하지 않도록 방지할 수 없으며 그렇게 할 경우 새로 추가된 스토리지 용량을 사용할 수 없게 될 수 있습니다.

이 작업에 대해

기존 SSD 스토리지 풀에 SSD를 추가할 경우, SSD는 스토리지 풀에서 기존 SSD를 소유한 동일한 HA 쌍 중 하나 또는 둘 다 소유해야 합니다. HA Pair의 노드 중 하나에서 소유하는 SSD를 추가할 수 있습니다.

스토리지 풀에 추가하는 SSD의 크기는 스토리지 풀에서 현재 사용되는 디스크와 같아야 합니다.

시스템 관리자

ONTAP 9.12.1부터 시스템 관리자를 사용하여 SSD 스토리지 풀에 SSD를 추가할 수 있습니다.

단계

1. Storage > Tiers * 를 클릭하고 * Storage Pools * 섹션을 찾습니다.
2. 스토리지 풀을 찾아 를 클릭하고 * 디스크 추가 * 를 선택합니다.
3. 디스크 유형을 선택하고 디스크 수를 선택합니다.
4. 예상 캐시 크기를 검토합니다.

CLI를 참조하십시오

단계

1. * 선택 사항: * 스토리지 풀에 대한 현재 할당 유닛 크기 및 사용 가능한 스토리지를 봅니다.

   'storage pool show -instance_sp_name_'

2. 사용 가능한 SSD 찾기:

   '스토리지 디스크 표시 - 컨테이너형 스페어형 SSD'

3. 스토리지 풀에 SSD를 추가합니다.

   스토리지 풀 add-storage-pool sp_name-disk-list_disk1, disk2…_

   이 작업을 통해 어떤 Flash Pool 로컬 계층이 어느 Flash Pool 로컬 계층에 얼마만큼 증가할 것인지 시스템에 표시되고 작업을 확인하라는 메시지가 표시됩니다.

관련 정보

- "저장 디스크 표시"
- "저장 풀 쇼"
- "스토리지 풀 추가"

ONTAP 명령을 사용하여 **SSD** 스토리지 풀을 관리합니다

ONTAP는 SSD 스토리지 풀 관리를 위한 '스토리지 풀' 명령을 제공합니다.

원하는 작업	이 명령 사용…
스토리지 풀이 어떤 로컬 계층에 제공하고 있는지 표시합니다	스토리지 풀 show-aggregate를 선택합니다

두 RAID 유형(할당 유닛 데이터 크기)의 전체 캐시 용량에 추가되는 캐시의 양을 표시합니다.	'Storage pool show-instance'를 선택합니다
스토리지 풀의 디스크를 표시합니다	스토리지 풀 쇼 디스크
스토리지 풀에 대해 할당되지 않은 할당 유닛을 표시합니다	'Storage pool show-available-capacity'를 표시합니다
스토리지 풀의 하나 이상의 할당 유닛에 대한 소유권을 한 HA 파트너에서 다른 HA 파트너로 변경합니다	'스토리지 풀 재할당'을 선택합니다

관련 정보

- "스토리지 풀 재할당"
- "저장 풀 쇼"
- "스토리지 풀 show-aggregate"
- "스토리지 풀 사용 가능 용량 표시"
- "스토리지 풀 쇼 디스크"

FabricPool 계층 관리

ONTAP FabricPool를 통한 데이터 계층화에 대해 알아보십시오

FabricPool를 사용하면 데이터 액세스 빈도에 따라 데이터를 자동으로 계층화할 수 있습니다.

FabricPool는 AFF 시스템의 하이브리드 스토리지 솔루션으로, All-Flash(All-SSD) 애그리게이트를 사용하고, FAS 시스템에서는 All-Flash(All-SSD) 또는 HDD 애그리게이트를 성능 계층으로 사용하고, 오브젝트 저장소를 클라우드 계층으로 사용합니다. FabricPool를 사용하면 성능, 효율성 또는 보호 기능의 저하 없이 스토리지 비용을 절감할 수 있습니다.

클라우드 계층은 NetApp StorageGRID 또는 ONTAP S3(ONTAP 9.8부터)에 위치할 수 있으며, 다음 서비스 공급자 중 하나 이상에 포함될 수 있습니다.

- Alibaba 클라우드
- Amazon S3
- Amazon 상용 클라우드 서비스
- Google 클라우드
- IBM 클라우드
- Microsoft Azure Blob 저장소

ONTAP 9.7부터는 S3_호환 오브젝트 저장소 공급자를 선택하여 일반 S3 API를 지원하는 추가 오브젝트 저장소 공급자를 사용할 수 있습니다.

관련 정보

- "NetApp 클라우드 계층화 설명서"

ONTAP FabricPool 사용을 위한 요구 사항

FabricPool 구성을 최적화하려면 FabricPool 사용에 대한 몇 가지 고려 사항과 요구 사항을 숙지해야 합니다.

일반 고려 사항 및 요구 사항

ONTAP 9.4

- 다음 FabricPool 기능을 사용하려면 ONTAP 9.4 이상 릴리스를 실행해야 합니다.
  - 를 클릭합니다 `auto` "계층화 정책"
  - 계층화 최소 냉각 기간 지정
  - 비활성 데이터 보고(IDR)
  - 클라우드에 Microsoft Azure Blob Storage를 FabricPool의 클라우드 계층으로 사용
  - ONTAP Select와 함께 FabricPool 사용

ONTAP 9.5

- 다음 FabricPool 기능을 사용하려면 ONTAP 9.5 이상의 릴리스를 실행해야 합니다.
  - 계층화 충만 임계값 지정
  - IBM 클라우드 오브젝트 스토리지를 FabricPool의 클라우드 계층으로 사용
  - 기본적으로 활성화되어 있는 클라우드 계층의 NetApp Volume Encryption(NVE)

ONTAP 9.6

- 다음 FabricPool 기능을 사용하려면 ONTAP 9.6 이상 버전을 실행해야 합니다.
  - 모든 계층화 정책
  - 비활성 데이터 보고는 HDD 애그리게이트에서 수동으로 활성화됩니다
  - ONTAP 9.6으로 업그레이드하고 시점에 애그리게이트를 생성할 때, SSD 애그리게이트에 대해 비활성 데이터 보고가 자동으로 활성화됩니다. 단, CPU가 4개 미만이거나 RAM이 6GB 미만인 로우엔드 시스템 또는 WAFL 버퍼 캐시 크기가 3GB 미만인 경우는 예외입니다.

    ONTAP는 시스템 로드를 모니터링하며, 로드가 4분 동안 계속 높게 유지되면 IDR이 비활성화되고 자동으로 활성화되지 않습니다. 수동으로 IDR을 다시 활성화할 수 있지만 수동으로 활성화된 IDR은 자동으로 비활성화되지 않습니다.

  - Alibaba 클라우드 오브젝트 스토리지를 FabricPool의 클라우드 계층으로 사용
  - Google Cloud Platform을 FabricPool의 클라우드 계층으로 사용
  - 클라우드 계층 데이터 복사본 없이 볼륨 이동

ONTAP 9.7

- 다음 FabricPool 기능을 사용하려면 ONTAP 9.7 이상 릴리즈를 실행 중이어야 합니다.

- 화이트리스트된 액세스 포인트에만 액세스하고 감사 및 보고 기능을 제공하는 비투명 HTTP 및 HTTPS 프록시.
- FabricPool 미러링을 통해 콜드 데이터를 2개의 오브젝트 저장소에 동시에 계층화합니다
- MetroCluster 구성의 FabricPool 미러
- FabricPool 연결 애그리게이트에는 NDMP 덤프 및 복구가 기본적으로 설정됩니다.

> ⓘ 백업 애플리케이션이 NFS 또는 SMB와 같은 NDMP 이외의 프로토콜을 사용하는 경우 성능 계층에서 백업되는 모든 데이터가 핫 상태가 되고 해당 데이터를 클라우드 계층으로 계층화하는 데 영향을 미칠 수 있습니다. 비 NDMP 읽기로 인해 클라우드 계층에서 성능 계층으로 데이터가 다시 마이그레이션할 수 있습니다.

"FabricPool에 대한 NDMP 백업 및 복구 지원"

ONTAP 9.8

- 다음 FabricPool 기능을 사용하려면 ONTAP 9.8 이상을 실행해야 합니다.
  - 클라우드 검색
  - SnapLock 엔터프라이즈 및 FabricPool SnapLock Enterprise를 지원하는 FabricPool에는 FPVR(Feature Product Variance Request)이 필요합니다. FPVR을 생성하려면 세일즈 팀에 문의하십시오.
  - 최소 냉각 기간은 최대 183일입니다
  - 사용자가 만든 사용자 지정 태그를 사용하여 개체 태그 지정
  - HDD FabricPool 애그리게이트로 전환 가능

    HDD FabricPools는 SAS, FSA, BSAS 및 mSATA 디스크와 함께 지원되며 CPU 코어가 6개 이상인 시스템에서만 지원됩니다.

확인합니다 "Hardware Universe" 를 참조하십시오.

ONTAP 9.10.1

- 다음 FabricPool 기능을 사용하려면 ONTAP 9.10.1 이상을 실행해야 합니다.
  - 스로틀링
  - 온도에 민감한 저장 효율성(TSSE).

ONTAP 9.12.1

- 다음 FabricPool 기능을 사용하려면 ONTAP 9.12.1 이상을 실행해야 합니다.
  - SVM 마이그레이션
  - FabricPool, FlexGroup 및 SVM-DR 지원 협력 (9.12.1 이전에는 이 두 가지 기능이 함께 작동했지만 세 가지 기능이 모두 함께 작동되지는 않았습니다.)

ONTAP 9.14.1

- 다음 FabricPool 기능을 사용하려면 ONTAP 9.14.1 이상을 실행해야 합니다.
  - 클라우드 쓰기

◦ 적극적인 미리 읽기

로컬 계층(애그리게이트)

FabricPool는 다음과 같은 애그리게이트 유형을 지원합니다.

- AFF 시스템에서는 FabricPool에 대해 SSD 애그리게이트만 사용할 수 있습니다.
- FAS 시스템에서는 FabricPool에 SSD 또는 HDD 애그리게이트를 사용할 수 있습니다.
- Cloud Volumes ONTAP 및 ONTAP Select에서는 FabricPool에 SSD 또는 HDD 애그리게이트를 사용할 수 있습니다. SSD 애그리게이트를 사용하는 것이 좋습니다.

SSD와 HDD를 모두 포함하는 Flash Pool 애그리게이트는 지원되지 않습니다.

계층에서 실현해 보십시오

FabricPool은 다음과 같은 오브젝트 저장소를 클라우드 계층으로 사용할 수 있도록 지원합니다.

- Alibaba Cloud Object Storage Service(Standard, Infrequent Access)
- Amazon S3(표준, Standard-IA, One Zone-IA, 지능형 계층화, Glacier Instant Retrieval)
- Amazon Commercial Cloud Services(C2S)
- Google Cloud 스토리지(Multi-Regional, Regional, Nearline, Coldline, 아카이브)
- IBM Cloud Object Storage(Standard, Vault, Cold Vault, Flex)
- Microsoft Azure Blob 스토리지(핫 및 쿨)
- NetApp ONTAP S3(ONTAP 9.8 이상)
- NetApp StorageGRID(StorageGRID 10.3 이상)

Glacier Flexible Retrieval 및 Glacier Deep Archive는 지원되지 않습니다.

- 사용하려는 오브젝트 저장소 ""버킷""(컨테이너)이 이미 설정되어 있어야 하고, 최소 10GB의 저장 공간이 있어야 하며, 이름을 바꿀 수 없습니다.
- 클라우드 계층이 연결된 후에는 로컬 계층에서 분리할 수 없지만 를 사용할 수 있습니다 "FabricPool 미러" 로컬 계층을 다른 클라우드 계층에 연결합니다.

인터클러스터 **LIF**

FabricPool을 사용하는 클러스터 고가용성(HA) 쌍에는 클라우드 계층과 통신하기 위해 두 개의 인터클러스터 LIF가 필요합니다. NetApp은 추가 HA 쌍에 대한 인터클러스터 LIF를 생성하여 클라우드 계층을 해당 노드의 로컬 계층에 원활하게 연결할 것을 권장합니다.

인터클러스터 LIF를 비활성화하거나 삭제하면 클라우드 계층과의 통신이 중단됩니다.

동시 SnapMirror 및 SnapVault 복제 작업은 클라우드 계층에 대한 네트워크 링크를 공유하므로 초기화 및 RTO는 클라우드 계층에 대한 가용 대역폭과 지연 시간에 따라 달라집니다. 연결 리소스가 포화 상태가 되면 성능 저하가 발생할 수 있습니다. 여러 LIF의 사전 구성을 사용하면 이러한 네트워크 포화 유형을 크게 줄일 수 있습니다.

서로 다른 라우팅의 노드에서 둘 이상의 인터클러스터 LIF를 사용하는 경우 NetApp 다른 IPspace에 배치하는 것이 좋습니다. 구성 중에 FabricPool는 여러 IPspace에서 선택할 수 있지만 IPspace 내의 특정 인터클러스터 LIF는 선택할 수 없습니다.

네트워크 시간 프로토콜**(NTP)**

클러스터 간의 시간을 동기화하려면 NTP(네트워크 시간 프로토콜) 구성이 필요합니다. "NTP 구성 방법에 대해 알아보세요" .

ONTAP 스토리지 효율성

데이터를 클라우드 계층으로 이동할 때 압축, 중복제거, 컴팩션과 같은 스토리지 효율성이 유지되므로 필요한 오브젝트 스토리지 용량 및 전송 비용이 줄어듭니다.

ONTAP 9.15.1부터 FabricPool는 보다 공격적이고 뛰어난 성능의 스토리지 효율성을 제공하는 인텔 QuickAssist 기술(QAT4)을 지원합니다.

애그리게이트 인라인 중복제거는 로컬 계층에서 지원되지만 관련 스토리지 효율성이 클라우드 계층에 저장된 오브젝트로 이전되지 않습니다.

모든 볼륨 계층화 정책을 사용하면 추가 스토리지 효율성을 적용하기 전에 데이터를 계층화할 수 있기 때문에 백그라운드 중복제거 프로세스와 관련된 스토리지 효율성이 감소할 수 있습니다.

NetApp 클라우드 계층화 라이선스

FabricPool AFF 및 FAS 시스템의 클라우드 계층으로 타사 개체 스토리지 공급자(예: Amazon S3)를 연결할 때 용량 기반 라이선스가 필요합니다. StorageGRID 또는 ONTAP S3를 클라우드 계층으로 사용하거나 Cloud Volumes ONTAP, Amazon FSx for NetApp ONTAP 또는 Azure NetApp Files로 계층화하는 경우 Cloud Tiering 라이선스가 필요하지 않습니다.

NetApp Cloud Tiering 라이선스(기존 FabricPool 라이선스에 대한 추가 기능이나 확장 기능 포함)는 NetApp 콘솔에서 활성화됩니다. 자세히 알아보세요"클라우드 티어링 라이선스 설정" .

StorageGRID 일관성 제어

StorageGRID의 일관성 제어는 StorageGRID이 오브젝트를 추적하는 데 사용하는 메타데이터의 방식에 영향을 줍니다 노드 간에 분산되고 클라이언트 요청에 대해 개체의 가용성이 보장됩니다. NetApp에서는 을 사용할 것을 권장합니다 FabricPool 타겟으로 사용되는 버킷에 대한 새로운 쓰기 후 읽기, 정합성 보장 기본 제어

FabricPool 대상으로 사용되는 버킷에 대해 사용 가능한 정합성 보장 제어를 사용하지 마십시오.

SAN 프로토콜에서 액세스하는 데이터를 계층화하기 위한 추가 고려 사항

SAN 프로토콜에서 액세스하는 데이터를 계층화할 때 NetApp은 연결 고려사항으로 인해 ONTAP S3 또는 StorageGRID와 같은 프라이빗 클라우드를 사용할 것을 권장합니다.

Windows 호스트가 있는 SAN 환경에서 FabricPool 사용하는 경우, 클라우드에 데이터를 계층화할 때 장기간 개체 스토리지를 사용할 수 없게 되면 Windows 호스트의 NetApp LUN에 있는 파일에 액세스할 수 없게 되거나 파일이 사라질 수 있습니다. 를 참조하십시오"NetApp 기술 자료: FabricPool S3 개체 저장소를 사용할 수 없는 동안 Windows SAN 호스트에서 파일 시스템 손상이 보고되었습니다." .

서비스 품질

- 처리량 수준(QoS Min)을 사용하는 경우, FabricPool에 애그리게이트를 연결하기 전에 볼륨에 대한 계층화 정책을 "없음"으로 설정해야 합니다.

  다른 계층화 정책을 사용하면 애그리게이트는 FabricPool에 연결되지 않습니다. QoS 정책은 FabricPool가 활성화된 경우 처리량 플로어를 적용하지 않습니다.

FabricPool에서 지원하지 않는 기능 또는 기능입니다

- WORM 지원 및 오브젝트 버전 관리가 활성화된 오브젝트 저장소
- 오브젝트 저장소 버킷에 적용되는 ILM(정보 라이프사이클 관리) 정책

  FabricPool는 데이터 복제 및 삭제 코딩에 대해서만 StorageGRID의 정보 수명 주기 관리 정책을 지원하여 클라우드 계층 데이터를 장애로부터 보호합니다. 그러나 FabricPool는 사용자 메타데이터 또는 태그에 기반한 필터링과 같은 고급 ILM 규칙을 _NOT_지원합니다. ILM에는 일반적으로 다양한 이동 및 삭제 정책이 포함됩니다. 이러한 정책은 FabricPool의 클라우드 계층에 있는 데이터에 영향을 줄 수 있습니다. 오브젝트 저장소에 구성된 ILM 정책에 FabricPool을 사용하면 데이터 손실이 발생할 수 있습니다.

- ONTAP CLI 명령 또는 7-Mode 전환 툴을 사용하여 7-Mode 데이터 전환
- RAID SyncMirror(MetroCluster 구성 제외
- ONTAP 9.7 이하 릴리즈를 사용할 때 SnapLock 볼륨
- "변조 방지 스냅샷"

  변조 방지 스냅샷은 삭제할 수 없는 변경 불가능한 보호를 제공합니다. FabricPool에는 데이터 삭제 기능이 필요하므로 동일한 볼륨에서 FabricPool 및 스냅샷 잠금을 활성화할 수 없습니다.

- FabricPool 지원 애그리게이트용 SMTape를 사용한 테이프 백업
- 자동 균형 조정 기능
- '없음' 이외의 공간을 사용하는 볼륨

  루트 SVM 볼륨 및 CIFS 감사 스테이징 볼륨을 제외하고 FabricPool은 공간 보장이 아닌 다른 공간을 사용하는 볼륨이 포함된 애그리게이트에 클라우드 계층을 연결할 수 없습니다 `none`. 예를 들어, 의 공간 보장을 사용하는 볼륨입니다 `volume` (`-space-guarantee volume`)는 지원되지 않습니다.

- 와 클러스터 "DP_Optimized 라이센스"
- Flash Pool 애그리게이트로 전환 가능

ONTAP FabricPool 정책을 사용하여 데이터를 효율적으로 계층화

FabricPool 계층화 정책을 사용하면 데이터가 핫 또는 콜드 데이터가 될 때 계층 간에 데이터를 효율적으로 이동할 수 있습니다. 계층화 정책을 이해하면 스토리지 관리 요구 사항에 적합한 정책을 선택할 수 있습니다.

FabricPool 계층화 정책의 유형입니다

FabricPool 계층화 정책은 FabricPool에 있는 볼륨의 사용자 데이터 블록이 핫(액티브) 또는 콜드(비활성)의 볼륨 ""온도""에 따라 클라우드 계층으로 이동되는지 여부를 결정합니다. 자주 접근하면 체적이 증가하고 자주 접근하지

않으면 체적이 감소합니다. 일부 계층화 정책에는 관련 계층화 최소 냉각 기간이 있는데, 이는 데이터를 "콜드"로 간주하고 클라우드 계층으로 이동하기 위해 FabricPool 볼륨의 사용자 데이터가 비활성 상태로 유지되는 시간을 설정합니다.

블록이 콜드 블록으로 식별되면 계층화할 수 있는 것으로 표시됩니다. 매일 백그라운드 계층화 검사에서 콜드 블록이 검색됩니다. 같은 볼륨에서 4KB의 블록이 충분히 수집되면 4MB 개체로 연결되고 볼륨 계층화 정책에 따라 클라우드 계층으로 이동됩니다.

> 를 사용하는 볼륨의 데이터입니다 `all` 계층화 정책은 즉시 '콜드'으로 표시되며 가능한 한 빨리 클라우드 계층으로 계층화를 시작합니다. 일일 계층화 검사가 실행될 때까지 기다릴 필요가 없습니다.

명령을 사용하여 FabricPool 볼륨의 계층화 상태를 확인할 수 있다 `volume object-store tiering show`. 에 대한 자세한 내용은 `volume object-store tiering show` "ONTAP 명령 참조입니다"을 참조하십시오.

FabricPool 계층화 정책은 볼륨 레벨에서 지정됩니다. 다음 4가지 옵션을 사용할 수 있습니다.

- `snapshot-only`계층화 정책(기본값)은 액티브 파일 시스템과 연결되지 않은 볼륨 스냅샷의 사용자 데이터 블록을 클라우드 계층으로 이동합니다.

  계층화 최소 냉각 기간은 2일입니다. 볼륨 생성 및 볼륨 수정 명령의 고급 권한 수준에서 '-Tiering-Minimum-Cooling-Days' 매개 변수를 사용하여 계층화 최소 냉각 기간의 기본 설정을 수정할 수 있습니다. 유효한 값은 ONTAP 9.8 이상을 사용하여 2 ~ 183일입니다. 9.8 이전의 ONTAP 버전을 사용하는 경우 유효한 값은 2-63일입니다.

- `auto`ONTAP 9.4 이상 릴리즈에서만 지원되는 계층화 정책은 스냅샷과 액티브 파일 시스템의 콜드 사용자 데이터 블록을 클라우드 계층으로 이동합니다.

  기본 계층화 최소 냉각 기간은 31일이며 액티브 파일 시스템과 스냅샷 모두에 대해 전체 볼륨에 적용됩니다.

  볼륨 생성 및 볼륨 수정 명령의 고급 권한 수준에서 '-Tiering-Minimum-Cooling-Days' 매개 변수를 사용하여 계층화 최소 냉각 기간의 기본 설정을 수정할 수 있습니다. 유효한 값은 2 ~ 183일입니다.

- `all`ONTAP 9.6 이상에서만 지원되는 계층화 정책은 액티브 파일 시스템 및 스냅샷 모두의 모든 사용자 데이터 블록을 클라우드 계층으로 이동합니다. `backup`계층화 정책을 대체합니다.

  를 클릭합니다 `all` 볼륨 계층화 정책은 정상적인 클라이언트 트래픽이 있는 읽기/쓰기 볼륨에서 사용하면 안 됩니다.

  계층화 검사가 실행되는 즉시 데이터가 클라우드 계층으로 이동하므로 계층화 최소 냉각 기간은 적용되지 않으며 설정을 수정할 수 없습니다.

- 를 클릭합니다 `none` 계층화 정책은 볼륨의 데이터를 성능 계층에 유지하고 콜드 데이터를 클라우드 계층으로 이동하지 않습니다.

  계층화 정책을 으로 설정합니다 `none` 새로운 계층화를 방지합니다. 이전에 클라우드 계층으로 이동된 볼륨 데이터는 핫 데이터가 되고 로컬 계층으로 자동으로 다시 이동될 때까지 클라우드 계층에 남아 있습니다.

  데이터가 클라우드 계층으로 이동되지 않으므로 계층화 최소 냉각 기간은 적용되지 않으며 설정을 수정할 수 없습니다.

  계층화 정책이 으로 설정된 볼륨의 콜드 블록입니다 `none` 읽으면 핫 데이터가 되고 로컬 계층에 기록됩니다.

'volume show' 명령 출력에는 볼륨의 계층화 정책이 표시됩니다. FabricPool에 사용된 적이 없는 볼륨은 출력에 "없음" 계층화 정책을 표시합니다.

SVM DR 관계인 경우 소스 및 타겟 볼륨에서 FabricPool 애그리게이트를 사용할 필요가 없지만 동일한 계층화 정책을 사용해야 합니다.

FabricPool에서 볼륨의 계층화 정책을 수정하면 어떻게 됩니까

볼륨 수정 작업을 수행하여 볼륨의 계층화 정책을 수정할 수 있습니다. 계층화 정책을 변경하면 데이터가 콜드 상태가 되어 클라우드 계층으로 이동하는 데 걸리는 시간이 영향을 받을 수 있음을 이해해야 합니다.

- 계층화 정책을 '스냅샷 전용' 또는 '사용 안 함'에서 '자동'으로 변경하면 ONTAP는 사용자 데이터 블록이 이전에 클라우드 계층에 적합하지 않은 경우에도 이미 사용 중인 파일 시스템의 사용자 데이터 블록을 클라우드 계층으로 전송합니다.
- 계층화 정책을 다른 정책에서 로 `all` 변경하면 ONTAP는 액티브 파일 시스템 및 스냅샷의 모든 사용자 블록을 가능한 한 빨리 클라우드로 이동합니다. ONTAP 9.8 이전에는 다음 계층화 검사가 실행될 때까지 블록이 필요했습니다.

  블록을 성능 계층으로 다시 이동할 수 없습니다.

- 계층화 정책을 'auto'에서 'napshot-only' 또는 'none'으로 변경해도 이미 클라우드 계층으로 이동된 액티브 파일 시스템 블록이 성능 계층으로 다시 이동되는 것은 아닙니다.

  데이터를 성능 계층으로 다시 이동하는 데 볼륨 읽기가 필요합니다.

- 볼륨에 대한 계층화 정책을 변경할 때마다 계층화 최소 냉각 기간이 정책의 기본값으로 재설정됩니다.

볼륨을 이동할 때 계층화 정책은 어떻게 됩니까

- 다른 계층화 정책을 명시적으로 지정하지 않는 한, FabricPool 지원 Aggregate와 그 외부로 이동할 때 볼륨은 원래 계층화 정책을 유지합니다.

  하지만 계층화 정책은 볼륨이 FabricPool 지원 애그리게이트에 있을 때만 적용됩니다.

- 대상에 대해 다른 계층화 정책을 지정하지 않으면 볼륨에 대한 '-Tiering-Minimum-Cooling-Days' 매개 변수의 기존 값이 볼륨과 함께 이동합니다.

  다른 계층화 정책을 지정하는 경우 볼륨은 해당 정책에 대한 기본 계층화 최소 냉각 기간을 사용합니다. 대상이 FabricPool인지 여부에 관계없이 이 경우가 해당됩니다.

- 애그리게이트 전체에서 볼륨을 이동하는 동시에 계층화 정책을 수정할 수 있습니다.
- 볼륨 이동 작업에 자동 계층화 정책이 포함되는 경우 특히 주의해야 합니다.

  소스 및 타겟이 FabricPool 지원 애그리게이트라고 가정하면 다음 표에는 'auto'와 관련된 정책 변경이 포함된 '볼륨 이동' 작업의 결과가 요약되어 있습니다.

계층화 정책이 다음과 같은 볼륨을 이동하는 경우	다음으로 이동하여 계층화 정책을 변경합니다.	그런 다음 볼륨 이동 후…

모두	자동	모든 데이터가 성능 계층으로 이동됩니다.
'냅샷 전용', '없음' 또는 '자동’으로 표시됩니다	자동	데이터 블록이 이전에 소스에 있었던 것과 동일한 대상 계층으로 이동합니다.
자동 또는 모두	'냅샷 전용'	모든 데이터가 성능 계층으로 이동됩니다.
자동	모두	모든 사용자 데이터가 클라우드 계층으로 이동됩니다.
'스냅샷 전용', '자동' 또는 '모두 ’입니다	"없음"	모든 데이터는 성능 계층에 보관됩니다.

볼륨을 클론 복제할 때 계층화 정책은 어떻게 됩니까

- ONTAP 9.8부터 클론 볼륨은 항상 계층화 정책과 클라우드 검색 정책을 상위 볼륨에서 상속합니다.

  ONTAP 9.8 이전 릴리즈에서는 상위 계층에 '모두' 계층화 정책이 있는 경우를 제외하고 클론이 상위 계층으로부터 계층화 정책을 상속합니다.

- 상위 볼륨에 클라우드 검색 정책이 없는 경우 해당 클론 볼륨에 클라우드 검색 정책이 '사용 안 함' 또는 '모두' 계층화 정책, 해당 클라우드 검색 정책 '기본값’이 있어야 합니다.
- 모든 클론 볼륨에 클라우드 검색 정책이 '사용 안 함’으로 되어 있지 않으면 상위 볼륨 클라우드 검색 정책을 '사용 안 함’으로 변경할 수 없습니다.

볼륨을 복제할 때 다음 Best Practice를 염두에 두십시오.

- 클론의 `-Tiering-policy ' 옵션과 ' Tiering-Minimum-Cooling-Days ' 옵션은 클론에만 적용되는 블록의 계층화 동작만 제어합니다. 따라서 동일한 양의 데이터를 이동하거나 모든 클론보다 적은 데이터를 이동하는 상위 FlexVol의 계층화 설정을 사용하는 것이 좋습니다
- 상위 FlexVol의 클라우드 검색 정책은 동일한 양의 데이터를 이동하거나 모든 클론의 검색 정책보다 더 많은 데이터를 이동해야 합니다

계층화 정책이 클라우드 마이그레이션과 작동하는 방식

FabricPool 클라우드 데이터 검색은 읽기 패턴에 따라 클라우드 계층에서 성능 계층으로 데이터 검색을 결정하는 계층화 정책을 통해 제어됩니다. 읽기 패턴은 순차적이거나 무작위일 수 있습니다.

다음 표에는 각 정책의 계층화 정책과 클라우드 데이터 검색 규칙이 나와 있습니다.

계층화 정책	검색 동작
없음	순차적 읽기 및 랜덤 읽기

스냅샷 전용	순차적 읽기 및 랜덤 읽기
자동	랜덤 읽기
모두	데이터를 검색할 수 없습니다

ONTAP 9.8부터 클라우드 마이그레이션 제어 '클라우드 검색 정책' 옵션은 계층화 정책에 의해 제어되는 기본 클라우드 마이그레이션 또는 검색 동작을 재정의합니다.

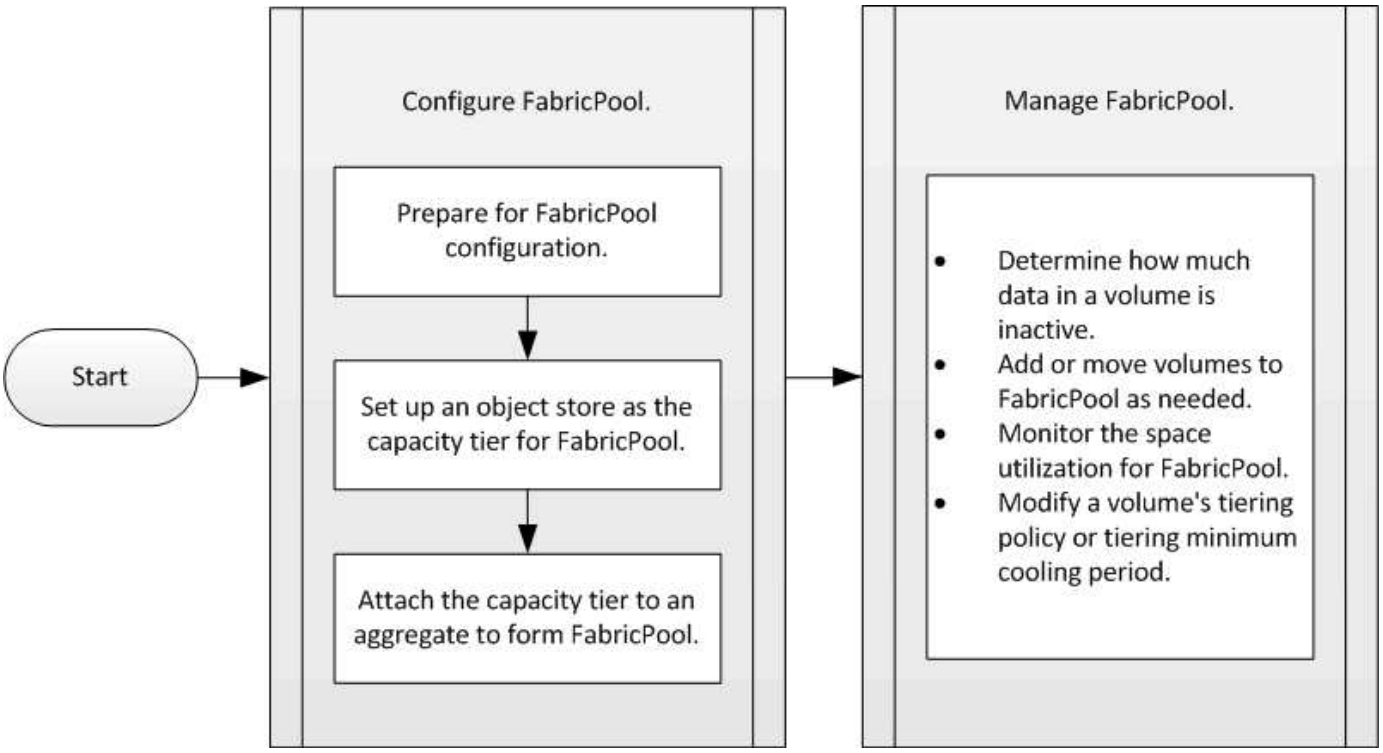
다음 표에는 지원되는 클라우드 검색 정책과 검색 동작이 나와 있습니다.

클라우드 검색 정책	검색 동작
기본값	계층화 정책은 어떤 데이터를 다시 풀어야 할지 결정하므로 "기본값", "클라우드 검색 정책"을 통해 클라우드 데이터 검색에 대한 변경 사항은 없습니다. 이 정책은 호스팅된 애그리게이트 유형에 관계없이 모든 볼륨의 기본값입니다.
읽기	모든 클라이언트 기반 데이터 읽기는 클라우드 계층에서 성능 계층으로 가져옵니다.
안 함	클라우드 계층에서 성능 계층으로 클라이언트 기반 데이터를 끌어오는 기능은 없습니다
승격	• 계층화 정책의 경우 ""없음"", 모든 클라우드 데이터가 클라우드 계층에서 성능 계층으로 풀링됩니다 • 계층화 정책의 경우, "스냅샷 전용", AFS 데이터가 풀링됩니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP FabricPool 구성 및 관리 작업에 대해 알아보세요.

FabricPool 워크플로 다이어그램을 사용하여 구성 및 관리 작업을 계획할 수 있습니다.



FabricPool를 구성합니다

FabricPool 구성을 준비합니다

ONTAP FabricPool과 함께 시작하십시오

FabricPool를 구성하면 데이터의 액세스 빈도 여부를 기준으로 저장할 스토리지 계층(로컬 성능 계층 또는 클라우드 계층) 데이터를 관리할 수 있습니다.

FabricPool 구성에 필요한 준비는 클라우드 계층으로 사용하는 오브젝트 저장소에 따라 다릅니다.

ONTAP 클러스터에 FabricPool 라이센스를 설치합니다

과거에 사용했던 FabricPool 라이선스가 변경되어 NetApp 콘솔에서 지원되지 않는 구성에 대해서만 유지됩니다. 2021년 8월 21일부터 NetApp Cloud Tiering을 사용하여 NetApp Console에서 지원되는 계층화 구성에 대해 NetApp Cloud Tiering BYOL 라이선싱이 도입되었습니다.

"NetApp Cloud Tiering BYOL 라이선싱에 대해 자세히 알아보세요" .

NetApp 콘솔에서 지원하는 구성은 콘솔을 사용하여 ONTAP 클러스터에 대한 계층화 라이선스를 부여해야 합니다. 이렇게 하려면 NetApp 콘솔 계정을 설정하고 사용하려는 특정 개체 스토리지 공급자에 대한 계층화를 설정해야 합니다. 콘솔은 현재 다음 개체 스토리지에 대한 계층화를 지원합니다: Amazon S3, Azure Blob 스토리지, Google Cloud Storage, S3 호환 개체 스토리지 및 StorageGRID.

"NetApp Cloud Tiering 서비스에 대해 자세히 알아보세요" .

콘솔에서 지원되지 않는 구성 중 하나가 있는 경우 System Manager를 사용하여 FabricPool 라이선스를 다운로드하고 활성화할 수 있습니다.

- 다크 사이트에 ONTAP 설치
- 데이터를 IBM Cloud Object Storage 또는 Alibaba Cloud Object Storage로 계층화하는 ONTAP 클러스터

FabricPool 라이센스는 클러스터 차원의 라이센스입니다. 클러스터에서 FabricPool와 연결된 오브젝트 스토리지에 대해 구입한 사용 제한이 포함됩니다. 클러스터 전체의 사용량이 사용 제한 용량을 초과해서는 안 됩니다. 라이센스의 사용 한도를 늘려야 하는 경우 영업 담당자에게 문의하십시오.

FabricPool 라이센스는 영구 또는 기간 기반, 1년 또는 3년 형식으로 제공됩니다.

NetApp 콘솔에서 지원되지 않는 기존 클러스터 구성에 대한 첫 번째 FabricPool 주문에는 10TB의 무료 용량이 제공되는 기간 기반 FabricPool 라이선스가 제공됩니다. 영구 라이선스에는 무료 용량이 제공되지 않습니다. 클라우드 계층에 NetApp StorageGRID 또는 ONTAP S3를 사용하는 경우 라이선스가 필요하지 않습니다. Cloud Volumes ONTAP 사용하는 공급업체에 관계없이 FabricPool 라이선스가 필요하지 않습니다.

이 작업은 System Manager를 사용하여 클러스터에 라이센스 파일을 업로드하는 경우에만 지원됩니다.

단계

1. FabricPool 라이센스용 NetApp 라이센스 파일(NLF)을 에서 다운로드하십시오 "NetApp Support 사이트".
2. System Manager를 사용하여 FabricPool 라이센스를 클러스터에 업로드하려면 다음 작업을 수행합니다.
   a. 클러스터 > 설정 * 창의 * Licenses * 카드에서 을 클릭합니다 →.
   b. 라이센스 * 페이지에서 를 + Add 클릭합니다.
   c. 라이센스 추가 * 대화 상자에서 * 찾아보기 * 를 클릭하여 다운로드한 NLF를 선택한 다음 * 추가 * 를 클릭하여 파일을 클러스터에 업로드합니다.

관련 정보

"FP(ONTAP FabricPool) 라이센스 개요"

"NetApp 소프트웨어 라이센스 검색"

"NetApp TechComm TV: FabricPool 재생 목록"

StorageGRID용 **ONTAP** 클러스터에 **CA** 인증서를 설치합니다

CA 인증서를 사용하면 클라이언트 응용 프로그램과 StorageGRID 간에 신뢰할 수 있는 관계가 만들어집니다.

StorageGRID에 대한 인증서 확인을 사용하지 않도록 설정하려면 ONTAP가 FabricPool의 개체 저장소로 StorageGRID를 인증할 수 있도록 클러스터에 StorageGRID CA 인증서를 설치해야 합니다.

StorageGRID에서는 자체 서명된 인증서를 생성할 수 있지만 타사 인증 기관에서 서명한 인증서를 사용하는 것이 좋습니다.

이 작업에 대해

ONTAP 9.4부터 CA(인증 기관) 인증서를 설치 및 사용하는 것이 권장되지만 StorageGRID에 CA 인증서를 설치할 필요는 없습니다.

단계

1. 를 얻으려면 StorageGRID 관리자에게 "StorageGRID 시스템의 CA 인증서입니다" 문의하십시오.

2. 'server-ca' 매개 변수와 함께 'security certificate install' 명령을 사용하여 클러스터에 StorageGRID CA 인증서를 설치합니다.

   입력하는 FQDN(정규화된 도메인 이름)은 StorageGRID CA 인증서의 사용자 지정 일반 이름과 일치해야 합니다.

만료된 인증서를 업데이트합니다

만료된 인증서를 업데이트하려면 신뢰할 수 있는 CA를 사용하여 새 서버 인증서를 생성하는 것이 가장 좋습니다. 또한 StorageGRID 서버와 ONTAP 클러스터에서 동시에 인증서를 업데이트하여 가동 중지 시간을 최소화해야 합니다.

관련 정보

- "StorageGRID 리소스"
- "보안 인증서 설치"

ONTAP S3용 클러스터에 **CA** 인증서를 설치합니다

CA 인증서를 사용하면 클라이언트 응용 프로그램과 ONTAP S3 개체 저장소 서버 간에 신뢰할 수 있는 관계가 만들어집니다. CA 인증서를 원격 클라이언트에서 액세스할 수 있는 개체 저장소로 사용하기 전에 ONTAP에 설치해야 합니다.

ONTAP S3에 대한 인증서 확인을 사용하지 않도록 설정하려면 ONTAP에서 ONTAP S3를 FabricPool의 개체 저장소로 인증할 수 있도록 클러스터에 ONTAP S3 CA 인증서를 설치해야 합니다.

ONTAP에서는 자체 서명된 인증서를 생성할 수 있지만 타사 인증 기관에서 서명한 인증서를 사용하는 것이 좋습니다.

단계

1. ONTAP S3 시스템의 CA 인증서를 얻습니다.
2. "security certificate install" 명령을 -type 'server-ca' 매개 변수와 함께 사용하여 클러스터에 ONTAP S3 CA 인증서를 설치합니다.

   입력하는 FQDN(정규화된 도메인 이름)은 ONTAP S3 CA 인증서의 사용자 지정 일반 이름과 일치해야 합니다.

만료된 인증서를 업데이트합니다

만료된 인증서를 업데이트하려면 신뢰할 수 있는 CA를 사용하여 새 서버 인증서를 생성하는 것이 가장 좋습니다. 또한 ONTAP S3 서버와 ONTAP 클러스터에서 동시에 인증서를 업데이트해야 가동 중지 시간을 최소화할 수 있습니다.

System Manager를 사용하여 ONTAP 클러스터에서 만료된 인증서를 갱신할 수 있습니다.

단계

1. 클러스터 > 설정 * 으로 이동합니다.
2. 보안 * 섹션으로 스크롤하여 * 인증서 * 창을 찾은 다음 를 클릭합니다 →.
3. 신뢰할 수 있는 인증 기관 * 탭에서 갱신할 인증서의 이름을 찾습니다.
4. 인증서 이름 옆에 있는 * Renew * 를 클릭하고 ⋮ 선택합니다.
5. 신뢰할 수 있는 인증 기관 갱신 * 창에서 인증서 정보를 복사하여 붙여 넣거나 * 인증서 세부 정보 * 영역에 가져옵니다.

6. 갱신 * 을 클릭합니다.

관련 정보

- "S3 구성"
- "보안 인증서 설치"

오브젝트 저장소를 **FabricPool**의 클라우드 계층으로 설정합니다

FabricPool 개요를 위해 오브젝트 저장소를 클라우드 계층으로 설정

FabricPool를 설정하려면 FabricPool의 클라우드 계층으로 사용할 오브젝트 저장소(StorageGRID, ONTAP S3, Alibaba 클라우드 오브젝트 스토리지, Amazon S3, Google 클라우드 스토리지, IBM 클라우드 오브젝트 스토리지 또는 클라우드용 Microsoft Azure Blob 스토리지)의 구성 정보를 지정해야 합니다.

StorageGRID를 **ONTAP FabricPool** 클라우드 계층으로 설정합니다

FabricPool 의 클라우드 계층으로 StorageGRID 설정할 수 있습니다. SAN 프로토콜에서 액세스하는 데이터를 계층화할 경우 연결 고려사항으로 인해 StorageGRID와 같은 프라이빗 클라우드를 사용하는 것이 좋습니다.

FabricPool와 함께 **StorageGRID**를 사용하기 위한 고려 사항

- 인증서 확인을 명시적으로 해제하지 않는 한 StorageGRID용 CA 인증서를 설치해야 합니다.
- 오브젝트 저장소 버킷에서 StorageGRID 오브젝트 버전 관리를 활성화하지 마십시오.
- FabricPool 라이센스는 필요하지 않습니다.
- StorageGRID 노드가 NetApp AFF 시스템에서 할당된 스토리지가 있는 가상 머신에 구축된 경우 해당 볼륨에 FabricPool 계층화 정책이 활성화되어 있지 않은지 확인하십시오.

  StorageGRID 노드와 함께 사용되는 볼륨에 대해 FabricPool 계층화를 사용하지 않도록 설정하면 문제 해결과 스토리지 작업이 간소화됩니다.

  FabricPool를 사용하여 StorageGRID 관련 데이터를 StorageGRID 자체로 계층화하지 마십시오. StorageGRID 데이터를 StorageGRID로 다시 계층화하면 문제 해결과 운영 복잡성이 늘어납니다.

이 작업에 대해

StorageGRID 9.8 이상에서는 ONTAP에 대해 로드 밸런싱이 활성화됩니다. 서버의 호스트 이름이 둘 이상의 IP 주소로 확인되는 경우 ONTAP는 반환된 모든 IP 주소(최대 16개의 IP 주소)를 사용하여 클라이언트 연결을 설정합니다. 연결이 설정되면 IP 주소가 라운드 로빈 방식으로 선택됩니다.

단계

ONTAP System Manager 또는 ONTAP CLI를 사용하여 StorageGRID를 FabricPool의 클라우드 계층으로 설정할 수 있습니다.

시스템 관리자

1. 스토리지 > 계층 > 클라우드 계층 추가 * 를 클릭하고 오브젝트 저장소 공급자로 StorageGRID를 선택합니다.
2. 요청된 정보를 완료합니다.
3. 클라우드 미러를 생성하려면 * FabricPool 미러로 추가 * 를 클릭합니다.

FabricPool 미러는 데이터 저장소를 원활하게 대체할 수 있는 방법을 제공하므로 재해 발생 시 데이터를 사용할 수 있습니다.

CLI를 참조하십시오

1. '-provider-type "sgws' 파라미터를 이용하여 'storage aggregate object-store config create' 명령어를 이용하여 StorageGRID 설정 정보를 지정한다.
   - StorageGRID가 제공된 정보로 ONTAP에 액세스할 수 없는 경우 'Storage aggregate object-store config create' 명령이 실패합니다.
   - '-access-key' 매개 변수를 사용하여 StorageGRID 개체 저장소에 대한 요청을 승인하는 액세스 키를 지정할 수 있습니다.
   - '-secret-password' 매개 변수를 사용하여 StorageGRID 개체 저장소에 대한 요청을 인증하는 암호(암호 액세스 키)를 지정합니다.
   - StorageGRID 암호가 변경된 경우 ONTAP에 저장된 해당 암호를 즉시 업데이트해야 합니다.

     이렇게 하면 ONTAP에서 StorageGRID의 데이터에 중단 없이 액세스할 수 있습니다.
   - 매개 변수를 로 `false` 설정하면 `-is-certificate-validation-enabled` StorageGRID에 대한 인증서 검사가 비활성화됩니다. (`-is-certificate-validation-enabled true`타사 인증 기관에서 서명한 인증서를 사용하는 것이 좋습니다.

```
cluster1::> storage aggregate object-store config create
-object-store-name mySGWS -provider-type SGWS -server mySGWSserver
-container-name mySGWScontainer -access-key mySGWSkey
-secret-password mySGWSpass
```

2. 'Storage aggregate object-store config show' 명령을 사용하여 StorageGRID 구성 정보를 표시하고 확인합니다.

   'Storage aggregate object-store config modify' 명령을 사용하면 FabricPool에 대한 StorageGRID 구성 정보를 수정할 수 있습니다.

관련 정보

- "저장소 집계 객체-저장소 구성 생성"
- "저장소 집계 객체 저장소 구성 수정"
- "저장소 집계 객체-저장소 구성 표시"

ONTAP 9.8 이상을 실행 중인 경우 ONTAP S3를 FabricPool의 클라우드 계층으로 설정할 수 있습니다.

시작하기 전에

- 원격 클러스터에 연결된 LIF의 ONTAP S3 서버 이름과 IP 주소가 있어야 합니다.

  서버 이름은 클라이언트 응용 프로그램에서 FQDN(정규화된 도메인 이름)으로 사용됩니다. ONTAP 외부에서 DNS 레코드가 사용 중인 SVM 데이터 LIF와 일치하는지 확인합니다.

- 로컬 클러스터에 있어야 클러스터 간 LIF합니다.

  로컬 클러스터 계층화를 위해 구성하면 로컬 계층(ONTAP CLI에서 스토리지 애그리게이트라고도 함)이 로컬 버킷에 연결됩니다. FabricPool는 클러스터 간 트래픽에 클러스터 LIF를 사용합니다.

  클러스터 LIF 리소스가 포화 상태가 되면 성능 저하가 발생할 수 있습니다. 이를 방지하기 위해 NetApp은 로컬 버킷에 계층화할 때 로컬 계층의 HA 쌍, 로컬 버킷의 HA 쌍 등과 함께 4노드 이상 클러스터를 사용하는 것이 좋습니다. 단일 HA 쌍에서 로컬 버킷으로 계층화하는 것은 권장되지 않습니다.

- ONTAP S3를 사용하여 원격 FabricPool 용량(클라우드) 계층화를 사용하려면 FabricPool 클라이언트와 "데이터 LIF 구성"오브젝트 저장소 서버에 있어야 합니다"인터클러스터 LIF를 구성합니다".

이 작업에 대해

ONTAP 9.8 이상에서 ONTAP S3 서버에 대해 로드 밸런싱이 활성화됩니다. 서버의 호스트 이름이 둘 이상의 IP 주소로 확인되는 경우 ONTAP는 반환된 모든 IP 주소(최대 16개의 IP 주소)를 사용하여 클라이언트 연결을 설정합니다. 연결이 설정되면 IP 주소가 라운드 로빈 방식으로 선택됩니다.

단계

ONTAP System Manager 또는 ONTAP CLI를 사용하여 ONTAP S3를 FabricPool용 클라우드 계층으로 설정할 수 있습니다.

시스템 관리자

1. 스토리지 > 계층 > 클라우드 계층 추가 * 를 클릭하고 오브젝트 저장소 공급자로 ONTAP S3를 선택합니다.
2. 요청된 정보를 완료합니다.
3. 클라우드 미러를 생성하려면 * FabricPool 미러로 추가 * 를 클릭합니다.

FabricPool 미러는 데이터 저장소를 원활하게 대체할 수 있는 방법을 제공하므로 재해 발생 시 데이터를 사용할 수 있습니다.

CLI를 참조하십시오

1. S3 서버 및 LIF에 대한 항목을 DNS 서버에 추가합니다.

옵션을 선택합니다	설명
• 외부 DNS 서버를 사용하는 경우 *	DNS 서버 관리자에게 S3 서버 이름 및 IP 주소를 지정합니다.
• 로컬 시스템의 DNS 호스트 테이블을 사용하는 경우 *	다음 명령을 입력합니다. `dns host create -vserver <svm_name> -address ip_address -hostname <s3_server_name>`

2. '-provider-type "ontap_s3' 파라미터를 사용하여 'storage aggregate object-store config create' 명령을 사용하여 ONTAP S3 구성 정보를 지정합니다.
   - 로컬 ONTAP 시스템이 제공된 정보로 ONTAP S3 서버에 액세스할 수 없으면 'Storage aggregate object-store config create' 명령이 실패합니다.
   - '-access-key' 매개 변수를 사용하여 ONTAP S3 서버에 요청을 승인하는 데 필요한 액세스 키를 지정할 수 있습니다.
   - '-secret-password' 매개변수를 사용하여 ONTAP S3 서버에 대한 요청을 인증하는 암호(비밀 액세스 키)를 지정합니다.
   - ONTAP S3 서버 암호가 변경되면 로컬 ONTAP 시스템에 저장된 해당 암호를 즉시 업데이트해야 합니다.

     이렇게 하면 ONTAP S3 오브젝트 저장소에서 중단 없이 데이터에 액세스할 수 있습니다.

   - 매개 변수를 로 `false` 설정하면 `-is-certificate-validation-enabled` ONTAP S3에 대한 인증서 검사가 비활성화됩니다. (`-is-certificate-validation-enabled true`타사 인증 기관에서 서명한 인증서를 사용하는 것이 좋습니다.

```
cluster1::> storage aggregate object-store config create
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server
-container-name myS3container -access-key myS3key
-secret-password myS3pass
```

3. 'Storage aggregate object-store config show' 명령을 사용하여 ONTAP_S3 구성 정보를 표시하고 확인합니다.

   'Storage aggregate object-store config modify' 명령을 사용하면 FabricPool의 'ontap_s3' 구성 정보를 수정할 수 있습니다.

관련 정보

- "SMB용 LIF를 생성합니다"
- "NFS용 LIF를 생성합니다"
- "저장소 집계 객체-저장소 구성 생성"
- "저장소 집계 객체 저장소 구성 수정"
- "저장소 집계 객체-저장소 구성 표시"

Alibaba 클라우드 오브젝트 스토리지를 **ONTAP FabricPool** 클라우드 계층으로 설정합니다

ONTAP 9.6 이상을 실행하는 경우 Alibaba 클라우드 오브젝트 스토리지를 FabricPool의 클라우드 계층으로 설정할 수 있습니다.

Alibaba 클라우드 개체 스토리지를 **FabricPool**와 함께 사용할 때의 고려 사항

- 에이"NetApp 클라우드 계층화 라이선스" Alibaba Cloud Object Storage로 계층화하는 경우 필요합니다. 자세한 내용은 다음을 참조하세요. "ONTAP 클러스터에 FabricPool 라이센스를 설치합니다" .
- AFF 및 FAS 시스템과 ONTAP Select에서 FabricPool는 다음 Alibaba 개체 스토리지 서비스 클래스를 지원합니다.
  - Alibaba 개체 스토리지 서비스 표준
  - Alibaba Object Storage Service 낮은 액세스 빈도

    "Alibaba Cloud: 스토리지 클래스 소개"

목록에 없는 스토리지 클래스에 대한 자세한 내용은 NetApp 세일즈 담당자에게 문의하십시오.

단계

1. '-provider-type ' AliCloud' 매개 변수를 사용하여 'storage aggregate object-store config create' 명령을 사용하여 Alibaba Cloud Object Storage 구성 정보를 지정합니다.
   - ONTAP가 제공된 정보로 Alibaba 클라우드 개체 스토리지에 액세스할 수 없으면 'Storage aggregate object-store config create' 명령이 실패합니다.
   - '-access-key' 매개 변수를 사용하여 Alibaba Cloud Object Storage 개체 저장소에 대한 요청 권한 부여에 대한 액세스 키를 지정합니다.
   - Alibaba 클라우드 개체 스토리지 암호가 변경되면 ONTAP에 저장된 해당 암호를 즉시 업데이트해야 합니다.

     이렇게 하면 ONTAP가 Alibaba 클라우드 개체 스토리지의 데이터에 중단 없이 액세스할 수 있습니다.

```
storage aggregate object-store config create my_ali_oss_store_1
-provider-type AliCloud -server oss-us-east-1.aliyuncs.com
-container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. 'Storage aggregate object-store config show' 명령을 사용하여 Alibaba Cloud Object Storage 구성 정보를 표시하고 확인합니다.

   'Storage aggregate object-store config modify' 명령을 사용하면 FabricPool에 대한 Alibaba 클라우드 개체 스토리지 구성 정보를 수정할 수 있습니다.

관련 정보

- "저장소 집계 객체-저장소 구성 생성"
- "저장소 집계 객체 저장소 구성 수정"
- "저장소 집계 객체-저장소 구성 표시"

Amazon S3를 **ONTAP FabricPool** 클라우드 계층으로 설정합니다

FabricPool 의 클라우드 계층으로 Amazon S3를 설정할 수 있습니다. ONTAP 9.5 이상을 실행 중인 경우 FabricPool용 C2S(Amazon Commercial Cloud Services)를 설정할 수 있습니다.

FabricPool에서 **Amazon S3**를 사용하기 위한 고려 사항

- 에이"NetApp 클라우드 계층화 라이선스" Amazon S3에 계층화하려면 필요합니다.
- ONTAP에서 Amazon S3 오브젝트 서버에 연결하는 데 사용하는 LIF는 10Gbps 포트에 연결하는 것이 좋습니다.
- AFF 및 FAS 시스템과 ONTAP Select에서 FabricPool은 다음과 같은 Amazon S3 스토리지 클래스를 지원합니다.
  - Amazon S3 Standard
  - Amazon S3 Standard - 낮은 액세스 빈도(Standard-IA)
  - Amazon S3 ONE Zone - 낮은 액세스 빈도(Zone-IA 1개)
  - Amazon S3 지능형 계층화
  - Amazon 상용 클라우드 서비스
  - ONTAP 9.11.1부터 Amazon S3 Glacier 인스턴트 검색(FabricPool는 Glacier Flexible Retrieval 또는 Glacier Deep Archive를 지원하지 않음)

    "Amazon Web Services 문서: Amazon S3 스토리지 클래스"

  목록에 없는 스토리지 클래스에 대한 자세한 내용은 영업 담당자에게 문의하십시오.

- Cloud Volumes ONTAP에서 FabricPool는 EBS(Elastic Block Store)의 GP2(General Purpose SSD) 및 st1(Throughput Optimized HDD) 볼륨의 계층화를 지원합니다.

단계

1. 를 사용하여 Amazon S3 구성 정보를 지정합니다 `storage aggregate object-store config create` 명령과 함께 `-provider-type AWS_S3` 매개 변수.

◦ C2S 액세스에 대한 자격 증명을 얻으려면 '-auth-type "cap' 매개 변수를 사용합니다.

auth-type의 cap 매개 변수를 사용할 때는 '-cap-url' 매개 변수를 사용하여 C2S 액세스에 대한 임시 자격 증명을 요청하기 위한 전체 URL을 지정해야 합니다.

◦ 를 클릭합니다 `storage aggregate object-store config create` ONTAP가 제공된 정보로 Amazon S3에 액세스할 수 없는 경우 명령이 실패합니다.

◦ 를 사용합니다 `-access-key` Amazon S3 오브젝트 저장소 요청 승인을 위한 액세스 키를 지정하는 매개 변수입니다.

◦ 를 사용합니다 `-secret-password` Amazon S3 오브젝트 저장소 요청을 인증하는 데 사용되는 암호(암호 액세스 키)를 지정하는 매개 변수입니다.

◦ Amazon S3 암호가 변경된 경우 ONTAP에 저장된 해당 암호를 즉시 업데이트해야 합니다.

이렇게 하면 ONTAP에서 Amazon S3의 데이터에 중단 없이 액세스할 수 있습니다.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

+

```
cluster1::> storage aggregate object-store config create -object-store
-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&role
=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-bucket
```

2. 를 사용하여 Amazon S3 구성 정보를 표시하고 확인합니다 `storage aggregate object-store config show` 명령.

   를 클릭합니다 `storage aggregate object-store config modify` 명령을 사용하면 FabricPool의 Amazon S3 구성 정보를 수정할 수 있습니다.

관련 정보

- "저장소 집계 객체-저장소 구성 생성"
- "저장소 집계 객체 저장소 구성 수정"
- "저장소 집계 객체-저장소 구성 표시"

Google Cloud Storage를 **ONTAP FabricPool** 클라우드 계층으로 설정합니다

ONTAP 9.6 이상을 실행 중인 경우 FabricPool용 클라우드 계층으로 Google 클라우드 스토리지를 설정할 수 있습니다.

FabricPool에서 **Google** 클라우드 스토리지를 사용할 때 고려해야 할 추가 사항

- 에이"NetApp 클라우드 계층화 라이선스" Google Cloud Storage로 계층화하는 경우 필요합니다.
- ONTAP에서 Google 클라우드 스토리지 오브젝트 서버에 연결하는 데 사용하는 LIF는 10Gbps 포트에 있는 것이 좋습니다.
- AFF 및 FAS 시스템과 ONTAP Select에서 FabricPool은 다음과 같은 Google Cloud Object 스토리지 클래스를 지원합니다.
  - Google Cloud 다중 지역
  - Google Cloud 지역
  - Google Cloud Nearline
  - Google Cloud Coldline

    "Google Cloud: 스토리지 클래스"

단계

1. '-provider-type ' GoogleCloud ' 매개 변수를 사용하여 'storage aggregate object-store config create' 명령을 사용하여 Google Cloud 스토리지 구성 정보를 지정합니다.
   - ONTAP가 제공된 정보로 Google Cloud Storage에 액세스할 수 없으면 'Storage aggregate object-store config create' 명령이 실패합니다.
   - '-access-key' 매개 변수를 사용하여 Google Cloud Storage 오브젝트 저장소에 대한 요청 승인 액세스 키를 지정할 수 있습니다.
   - Google 클라우드 저장소 암호가 변경된 경우 ONTAP에 저장된 해당 암호를 즉시 업데이트해야 합니다.

     이렇게 하면 ONTAP에서 Google 클라우드 스토리지의 데이터에 중단 없이 액세스할 수 있습니다.

```
storage aggregate object-store config create my_gcp_store_1 -provider
-type GoogleCloud  -container-name my-gcp-bucket1 -access-key
GOOGAUZZUV2USCFGHGQ511I8
```

2. 'Storage aggregate object-store config show' 명령을 사용하여 Google Cloud Storage 구성 정보를 표시하고 확인합니다.

   'Storage aggregate object-store config modify' 명령을 사용하면 FabricPool에 대한 Google 클라우드 스토리지 구성 정보를 수정할 수 있습니다.

관련 정보

- "저장소 집계 객체-저장소 구성 생성"
- "저장소 집계 객체 저장소 구성 수정"
- "저장소 집계 객체-저장소 구성 표시"

IBM 클라우드 오브젝트 스토리지를 **ONTAP FabricPool** 클라우드 계층으로 설정합니다

ONTAP 9.5 이상을 실행 중인 경우 IBM 클라우드 오브젝트 스토리지를 FabricPool의 클라우드

계층으로 설정할 수 있습니다.

FabricPool에서 **IBM** 클라우드 오브젝트 스토리지를 사용할 때의 고려 사항

- 에이"NetApp 클라우드 계층화 라이선스" IBM Cloud Object Storage로 계층화하는 경우 필요합니다.
- ONTAP에서 IBM 클라우드 오브젝트 서버에 연결하는 데 사용하는 LIF는 10Gbps 포트에 있는 것이 좋습니다.

단계

1. '-provider-type "ibm_cos' 매개 변수를 사용하여 'storage aggregate object-store config create' 명령을 사용하여 IBM Cloud Object Storage 구성 정보를 지정합니다.

   ◦ ONTAP가 제공된 정보로 IBM 클라우드 오브젝트 스토리지에 액세스할 수 없으면 'STOage Aggregate object-store config create' 명령이 실패합니다.

   ◦ '-access-key' 매개 변수를 사용하여 IBM 클라우드 오브젝트 스토리지 오브젝트 저장소에 대한 요청을 승인하는 액세스 키를 지정할 수 있습니다.

   ◦ '-secret-password' 매개 변수를 사용하여 IBM Cloud Object Storage 개체 저장소에 대한 요청을 인증하는 암호(비밀 액세스 키)를 지정합니다.

   ◦ IBM 클라우드 오브젝트 스토리지 암호가 변경된 경우 ONTAP에 저장된 해당 암호를 즉시 업데이트해야 합니다.

   이렇게 하면 ONTAP에서 IBM 클라우드 오브젝트 스토리지의 데이터를 중단 없이 액세스할 수 있습니다.

```
storage aggregate object-store config create
-object-store-name MyIBM -provider-type IBM_COS
-server s3.us-east.objectstorage.softlayer.net
-container-name my-ibm-cos-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. 'storage aggregate object-store config show' 명령을 사용하여 IBM Cloud Object Storage 구성 정보를 표시하고 확인합니다.

   'storage aggregate object-store config modify' 명령을 사용하면 FabricPool에 대한 IBM 클라우드 오브젝트 스토리지 구성 정보를 수정할 수 있습니다.

관련 정보

- "저장소 집계 객체-저장소 구성 생성"
- "저장소 집계 객체 저장소 구성 수정"
- "저장소 집계 객체-저장소 구성 표시"

Azure Blob Storage를 **ONTAP FabricPool** 클라우드 계층으로 설정합니다

ONTAP 9.4 이상을 실행 중인 경우 Azure Blob Storage를 FabricPool의 클라우드 계층으로 설정할 수 있습니다.

FabricPool와 함께 **Microsoft Azure Blob Storage**를 사용할 때의 고려 사항

- 에이"NetApp 클라우드 계층화 라이선스" Azure Blob Storage에 계층화하는 경우 필요합니다.

- Cloud Volumes ONTAP와 함께 Azure Blob Storage를 사용하는 경우 FabricPool 라이센스가 필요하지 않습니다.
- ONTAP에서 Azure Blob Storage 오브젝트 서버에 연결하는 데 사용하는 LIF는 10Gbps 포트에 있는 것이 좋습니다.
- FabricPool은 현재 온프레미스 Azure 서비스인 Azure 스택을 지원하지 않습니다.
- Microsoft Azure Blob Storage의 계정 수준에서 FabricPool는 핫 및 쿨 스토리지 계층만 지원합니다.

  FabricPool는 BLOB 레벨 계층화를 지원하지 않습니다. 또한 Azure의 아카이브 스토리지 계층화도 지원하지 않습니다.

이 작업에 대해

FabricPool은 현재 온프레미스 Azure 서비스인 Azure 스택을 지원하지 않습니다.

단계

1. '-provider-type "Azure_Cloud' 매개 변수를 사용하여 'storage aggregate object-store config create' 명령을 사용하여 Azure Blob Storage 구성 정보를 지정합니다.
   - ONTAP가 제공된 정보로 Azure Blob Storage에 액세스할 수 없으면 'STOATE OGATE OBJECT-STORE config create' 명령이 실패합니다.
   - '-Azure-account' 매개 변수를 사용하여 Azure Blob 저장소 계정을 지정합니다.
   - '-Azure-private-key' 매개 변수를 사용하여 Azure Blob 저장소에 대한 요청을 인증하는 액세스 키를 지정할 수 있습니다.
   - Azure Blob 저장소 암호가 변경된 경우 ONTAP에 저장된 해당 암호를 즉시 업데이트해야 합니다.

     이렇게 하면 ONTAP가 Azure Blob 스토리지의 데이터에 중단 없이 액세스할 수 있습니다.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyAzure -provider-type Azure_Cloud
   -server blob.core.windows.net -container-name myAzureContainer
   -azure-account myAzureAcct -azure-private-key myAzureKey
   ```

2. 'Storage aggregate object-store config show' 명령을 사용하여 Azure Blob Storage 구성 정보를 표시하고 확인합니다.

   'Storage aggregate object-store config modify' 명령을 사용하면 FabricPool의 Azure Blob 저장소 구성 정보를 수정할 수 있습니다.

관련 정보

- "저장소 집계 객체-저장소 구성 생성"
- "저장소 집계 객체 저장소 구성 수정"
- "저장소 집계 객체-저장소 구성 표시"

MetroCluster 구성에서 **ONTAP FabricPool**에 대한 개체 저장소 설정

ONTAP 9.7 이상을 실행 중인 경우 FabricPool 구성에서 미러링된 MetroCluster를 설정하여 콜드 데이터를 두 개의 서로 다른 장애 영역에 있는 오브젝트 저장소에 계층화할 수 있습니다.

이 작업에 대해

- MetroCluster의 FabricPool를 사용하려면 미러링된 내부 애그리게이트와 관련 오브젝트 저장소 구성이 동일한 MetroCluster 구성에서 소유되어야 합니다.
- 원격 MetroCluster 사이트에서 만든 개체 저장소에는 애그리게이트를 연결할 수 없습니다.
- Aggregate를 소유한 MetroCluster 구성에서 오브젝트 저장소 구성을 생성해야 합니다.

시작하기 전에

- MetroCluster 구성이 설정되어 올바르게 구성되어 있습니다.
- 적절한 MetroCluster 사이트에 두 개의 오브젝트 저장소가 설정됩니다.
- 컨테이너는 각 오브젝트 저장소에서 구성됩니다.
- 두 MetroCluster 구성에서 IP 공백이 생성되거나 식별되고 이름이 일치합니다.

단계

1. 'storage object-store config create' 명령을 사용하여 각 MetroCluster 사이트의 오브젝트 저장소 구성 정보를 지정합니다.

   이 예에서 FabricPool는 MetroCluster 구성의 한 클러스터에만 필요합니다. 해당 클러스터에 대해 오브젝트 저장소 버킷당 하나씩 두 개의 오브젝트 저장소 구성이 생성됩니다.

   ```
   storage aggregate
       object-store config create -object-store-name mcc1-ostore-config-s1
   -provider-type SGWS -server
       <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
   -secret-password <password> -encrypt
       <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
   ipspace
       <IPSpace>
   ```

   ```
   storage aggregate object-store config create -object-store-name mcc1-
   ostore-config-s2
       -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
   bucket-2> -access-key <key> -secret-password <password> -encrypt
   <true|false> -provider <provider-type>
       -is-ssl-enabled <true|false> ipspace <IPSpace>
   ```

   이 예에서는 MetroCluster 구성의 두 번째 클러스터에 FabricPool를 설정합니다.

```
storage aggregate
    object-store config create -object-store-name mcc2-ostore-config-s1
-provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

```
storage aggregate
    object-store config create -object-store-name mcc2-ostore-config-s2
-provider-type SGWS -server
    <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

관련 정보

- "저장소 객체-저장소 구성 생성"

ONTAP 클라우드 계층 지연 시간 및 처리량 성능을 테스트합니다

개체 저장소를 로컬 계층에 연결하기 전에 개체 저장소 프로파일러를 사용하여 개체 저장소의 지연 시간 및 처리량 성능을 테스트할 수 있습니다.

> 오브젝트 저장소 프로파일러 결과는 4MB의 PUT 및 4MB에서 256KB의 임의 읽기 바이트 범위를 사용하여 ONTAP와 클라우드 계층 객체 저장소 간의 연결을 측정한 것입니다. (SnapMirror와 같은 내부 ONTAP 기능만 32KB보다 큰 GET를 사용할 수 있습니다.)
>
> 경쟁사의 워크로드나 고유한 클라이언트 애플리케이션 동작은 고려하지 않기 때문에 오브젝트 저장소 프로파일러 결과는 계층화 성능을 나타내는 완벽한 지표가 아닙니다.

시작하기 전에

- 개체 저장소 프로파일러에서 클라우드 계층을 사용하려면 먼저 ONTAP에 클라우드 계층을 추가해야 합니다.
- ONTAP CLI 고급 권한 모드에 있어야 합니다.

단계

1. 개체 저장소 프로파일러를 시작합니다.

   ```
   storage aggregate object-store profiler start -object-store-name <name> -node
   <name>
   ```

2. 결과 보기:

```
storage aggregate object-store profiler show
```

관련 정보

- "저장소 집계 객체-저장소 프로파일러 표시"
- "저장소 집계 객체 저장소 프로파일러 시작"

ONTAP 클라우드 계층을 로컬 계층에 연결합니다

오브젝트 저장소를 클라우드 계층으로 설정한 후에는 FabricPool에 연결하여 사용할 로컬 계층을 지정합니다. ONTAP 9.5 이상에서는 적격한 FlexGroup 볼륨 구성요소를 포함하는 로컬 계층도 연결할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

이 작업에 대해

클라우드 계층을 로컬 계층에 연결하는 것은 영구적인 조치입니다. 클라우드 계층은 연결 후 로컬 계층에서 연결을 해제할 수 없습니다. 하지만 를 사용하면 "FabricPool 미러"로컬 계층을 다른 클라우드 계층에 연결할 수 있습니다.

시작하기 전에

ONTAP CLI를 사용하여 FabricPool에 대한 로컬 계층을 설정하는 경우 로컬 계층이 이미 존재해야 합니다.

System Manager를 사용하여 FabricPool의 로컬 계층을 설정하는 경우 로컬 계층을 생성한 후 FabricPool에 동시에 사용하도록 설정할 수 있습니다.

단계

ONTAP System Manager 또는 ONTAP CLI를 사용하여 로컬 계층을 FabricPool 오브젝트 저장소에 연결할 수 있습니다.

시스템 관리자

1. 스토리지 > 계층 * 으로 이동하여 클라우드 계층을 선택한 다음, 를 클릭합니다.
2. Attach local 계층 * 을 선택합니다.
3. Add as Primary * 에서 볼륨을 연결할 수 있는지 확인합니다.
4. 필요한 경우 * 볼륨을 씬 프로비저닝된 볼륨으로 변환 * 을 선택합니다.
5. 저장 * 을 클릭합니다.

CLI를 참조하십시오

CLI를 사용하여 오브젝트 저장소를 **Aggregate**에 연결하려면 다음과 같이 하십시오**.**

1. * 선택 사항 *: 볼륨의 데이터 양이 비활성 상태인지 확인하려면 의 단계를 따르십시오 "비활성 데이터 보고를 사용하여 볼륨의 비활성 데이터 양을 결정합니다".

   볼륨의 비활성 데이터 양을 보면 FabricPool에 사용할 애그리게이트를 결정할 수 있습니다.

2. 'Storage aggregate object-store attach' 명령을 사용하여 오브젝트 저장소를 Aggregate에 연결합니다.

   Aggregate가 FabricPool에 사용되지 않고 기존 볼륨이 포함되어 있는 경우 볼륨에 기본 '스냅샷 전용' 계층화 정책이 할당됩니다.

   ```
   cluster1::> storage aggregate object-store attach -aggregate myaggr
   -object-store-name Amazon01B1
   ```

   "allow-flexgroup" "true" 옵션을 사용하면 FlexGroup 볼륨 구성요소를 포함하는 애그리게이트를 연결할 수 있습니다.

3. 오브젝트 저장소 정보를 표시하고 'storage aggregate object-store show' 명령을 사용하여 연결된 오브젝트 저장소를 사용할 수 있는지 확인합니다.

   ```
   cluster1::> storage aggregate object-store show

   Aggregate    Object Store Name    Availability State
   ---------    -----------------    ------------------
   myaggr       Amazon01B1           available
   ```

관련 정보

- "저장소 집계 객체-저장소 연결"
- "저장소 집계 객체-저장소 표시"

로컬 **ONTAP S3** 버킷에 계층 데이터 추가

ONTAP 9.8부터 ONTAP S3를 사용하여 데이터를 로컬 오브젝트 스토리지에 계층화할 수 있습니다.

데이터를 로컬 버킷으로 계층화하면 데이터를 다른 로컬 계층으로 이동할 때의 간단한 대안이 됩니다. 이 절차에서는 로컬 클러스터의 기존 버킷을 사용하거나 ONTAP에서 자동으로 새 스토리지 VM과 새 버킷을 생성하도록 할 수 있습니다.

기본 로컬 버킷을 부착한 후에는 연결을 해제할 수 없습니다.

시작하기 전에

- 이 워크플로우에는 새 S3 서버 및 새 버킷을 생성하거나 기존 버킷을 사용하는 S3 라이센스가 필요합니다. 이 라이센스는 에 "ONTAP 1 을 참조하십시오"포함되어 있습니다. 이 워크플로우에는 FabricPool 라이센스가 필요하지 않습니다.
- "로컬 FabricPool 계층화에 대해 ONTAP S3 액세스를 설정합니다"..

단계

1. 데이터를 로컬 버킷에 계층화: * 스토리지 > 계층 * 을 클릭하고 * SSD * 창에서 로컬 계층을 선택한 다음 * 계층을 로컬 버킷으로 계층화 * 를 선택합니다.
2. Primary tier * 섹션에서 * Existing * 또는 * New * 를 선택합니다.
3. 저장 * 을 클릭합니다.

FabricPool 관리

비활성 데이터 보고를 통해 비활성 **ONTAP** 데이터를 분석

볼륨에 있는 데이터의 양이 얼마나 비활성 상태인지 보면 스토리지 계층을 잘 활용할 수 있습니다. 비활성 데이터 보고의 정보를 통해 FabricPool에 사용할 애그리게이트, FabricPool에서 볼륨으로 이동할지 또는 볼륨의 계층화 정책을 수정할지 여부를 결정할 수 있습니다.

시작하기 전에

비활성 데이터 보고 기능을 사용하려면 ONTAP 9.4 이상을 실행해야 합니다.

이 작업에 대해

- 일부 애그리게이트에서는 비활성 데이터 보고가 지원되지 않습니다.

  다음 인스턴스를 포함하여 FabricPool를 활성화할 수 없는 경우 비활성 데이터 보고를 활성화할 수 없습니다.

  - 루트 애그리게이트
  - 9.7 이전의 ONTAP 버전을 실행하는 MetroCluster 애그리게이트
  - Flash Pool(하이브리드 애그리게이트 또는 SnapLock 애그리게이트)
- 비활성 데이터 보고는 적응형 압축이 활성화된 볼륨에 대해 기본적으로 활성화됩니다.
- 비활성 데이터 보고는 ONTAP 9.6의 모든 SSD 애그리게이트에서 기본적으로 활성화됩니다.
- 비활성 데이터 보고는 ONTAP 9.4 및 ONTAP 9.5의 FabricPool 집계에서 기본적으로 활성화됩니다.
- ONTAP 9.6부터 HDD 애그리게이트를 포함한 ONTAP CLI를 사용하여 비 FabricPool 애그리게이트에 대해 비활성 데이터 리포팅을 활성화할 수 있습니다.

ONTAP System Manager 또는 ONTAP CLI에서 비활성 데이터 양을 확인할 수 있습니다.

시스템 관리자

1. 다음 옵션 중 하나를 선택합니다.
   - 기존 HDD Aggregate가 있는 경우 * 스토리지 > 계층 * 으로 이동하여 비활성 데이터 보고를 활성화할 애그리게이트를 클릭합니다. ⋮
   - 구성된 클라우드 계층이 없으면 * Dashboard * 로 이동하여 * Capacity * 에서 * Enable inactive data reporting * 링크를 클릭합니다.

CLI를 참조하십시오

CLI를 사용하여 비활성 데이터 보고 활성화하기**:**

1. 비활성 데이터 보고를 확인할 집계가 FabricPool에서 사용되지 않는 경우, '-is-inactive-data-reporting-enabled' true 매개 변수를 사용하여 'storage aggregate modify' 명령을 사용하여 집계에 대한 비활성 데이터 보고를 사용하도록 설정합니다.

   ```
   cluster1::> storage aggregate modify -aggregate aggr1 -is-inactive
   -data-reporting-enabled true
   ```

   FabricPool에 사용되지 않는 애그리게이트에 대해 비활성 데이터 보고 기능을 명시적으로 설정해야 합니다.

   FabricPool 지원 애그리게이트에는 비활성 데이터 보고가 이미 포함되어 있으므로 이러한 애그리게이트는 FabricPool 지원 애그리게이트에 대해 비활성 데이터 리포팅을 활성화할 필요가 없으며 그렇게 할 필요도 없습니다. '-is-inactive-data-reporting-enabled' 매개변수는 FabricPool 지원 애그리게이트에서 작동하지 않습니다.

   'storage aggregate show' 명령의 '-fields is-inactive-data-reporting-enabled' 매개 변수는 비활성 데이터 보고가 집계에서 활성화되어 있는지 여부를 나타냅니다.

2. 볼륨에서 비활성 상태인 데이터의 양을 표시하려면 '-fields performance-tier-inactive-user-data, performance-tier-inactive-user-data-percent' 매개 변수와 함께 'volume show' 명령을 사용합니다.

   ```
   cluster1::> volume show -fields performance-tier-inactive-user-
   data,performance-tier-inactive-user-data-percent

   vserver volume performance-tier-inactive-user-data performance-tier-
   inactive-user-data-percent
   ------- ------ ---------------------------------
   ----------------------------------------
   vsim1   vol0   0B                                0%
   vs1     vs1rv1 0B                                0%
   vs1     vv1    10.34MB                           0%
   vs1     vv2    10.38MB                           0%
   4 entries were displayed.
   ```

   - 'performance-tier-inactive-user-data' 필드에는 애그리게이트에 저장된 사용자 데이터의 비활성 양이 표시됩니다.

- `performance-tier-inactive-user-data-percent`이 필드에는 활성 파일 시스템 및 스냅샷에 걸쳐 비활성 상태의 데이터 비율이 표시됩니다.
- FabricPool에 사용되지 않는 애그리게이트의 경우 비활성 데이터 보고는 계층화 정책을 사용하여 콜드 데이터로 보고할 데이터의 양을 결정합니다.
  - 비계층화 정책에는 31일이 사용됩니다.
  - '스냅샷 전용' 및 '자동'의 경우 비활성 데이터 보고에는 계층화-최소-냉각-일(desting-minimum-cooling-days)이 사용됩니다.
  - "ALL" 정책의 경우 비활성 데이터 보고는 하루 내에 데이터가 계층화된다고 가정합니다.

    기간이 다 될 때까지 출력에는 값이 아닌 비활성 데이터의 양에 대한 ""-"가 표시됩니다.
- FabricPool의 일부인 볼륨에서 ONTAP가 비활성 상태로 보고하는 것은 볼륨에 설정된 계층화 정책에 따라 달라집니다.
  - "없음" 계층화 정책의 경우 ONTAP는 최소 31일 동안 비활성 상태인 전체 볼륨의 양을 보고합니다. none 계층화 정책으로는 `-Tiering-Minimum-Cooling-Days' 매개 변수를 사용할 수 없습니다.
  - ALL, 스냅샷 전용, 자동 계층화 정책의 경우 비활성 데이터 보고는 지원되지 않습니다.

관련 정보

- "저장소 집계 수정"

FabricPool에 대한 볼륨을 관리합니다

FabricPool 지원 **ONTAP** 로컬 계층에 볼륨을 생성합니다

FabricPool 지원 로컬 계층에서 직접 새 볼륨을 생성하거나 기존 볼륨을 다른 로컬 계층에서 FabricPool 지원 로컬 계층으로 이동하여 FabricPool에 볼륨을 추가할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

FabricPool용 볼륨을 생성할 때 계층화 정책을 지정할 수 있습니다. 계층화 정책을 지정하지 않으면 생성된 볼륨은 기본 '스냅샷 전용' 계층화 정책을 사용합니다. '스냅샷 전용' 또는 '자동' 계층화 정책을 사용하는 볼륨의 경우 계층화 최소 냉각 기간을 지정할 수도 있습니다.

시작하기 전에

- '자동' 계층화 정책을 사용하도록 볼륨을 설정하거나 계층화 최소 냉각 기간을 지정하려면 ONTAP 9.4 이상이 필요합니다.
- FlexGroup 볼륨을 사용하려면 ONTAP 9.5 이상이 필요합니다.
- 모든 계층화 정책을 사용하도록 볼륨을 설정하려면 ONTAP 9.6 이상이 필요합니다.
- '-cloud-retrieval-policy' 파라미터를 사용하도록 볼륨을 설정하려면 ONTAP 9.8 이상이 필요합니다.

단계

1. 'volume create' 명령을 사용하여 FabricPool에 대한 새 볼륨을 생성합니다.

◦ '-Tiering-policy' 선택적 매개 변수를 사용하면 볼륨에 대한 계층화 정책을 지정할 수 있습니다.

다음 계층화 정책 중 하나를 지정할 수 있습니다.

- '스냅샷 전용'(기본값)
- 자동
- 모두
- 'backup'(사용 안 함)
- "없음"

"FabricPool 계층화 정책의 유형입니다"

◦ '-cloud-retrieval-policy' 선택적 매개 변수를 사용하면 고급 권한 수준을 가진 클러스터 관리자가 계층화 정책에 의해 제어되는 기본 클라우드 마이그레이션 또는 검색 동작을 재정의할 수 있습니다.

다음 클라우드 검색 정책 중 하나를 지정할 수 있습니다.

- "기본"입니다

  계층화 정책은 어떤 데이터를 다시 가져오는지 결정하므로 '기본' 클라우드 검색 정책을 사용하면 클라우드 데이터 검색에 대한 변경 사항은 없습니다. 즉, 이 동작은 ONTAP 9.8 이전 버전과 동일합니다.

  - 계층화 정책이 "없음" 또는 "스냅샷 전용"인 경우 "기본값"은 모든 클라이언트 기반 데이터 읽기가 클라우드 계층에서 성능 계층으로 풀링됨을 의미합니다.
  - 계층화 정책이 "자동"인 경우 모든 클라이언트 기반 랜덤 읽기는 풀링되지만 순차적 읽기는 풀링되지 않습니다.
  - 계층화 정책이 "ALL"인 경우 클라우드 계층에서 클라이언트 기반 데이터를 추출하지 않습니다.
- "읽기"

  모든 클라이언트 기반 데이터 읽기는 클라우드 계층에서 성능 계층으로 가져옵니다.

- "안 돼.

  클라우드 계층에서 성능 계층으로 클라이언트 기반 데이터를 끌어오는 기능은 없습니다

- "홍보"
  - 계층화 정책이 "없음"인 경우 모든 클라우드 데이터가 클라우드 계층에서 성능 계층으로 풀링됩니다
  - 계층화 정책 '스냅샷 전용'의 경우 모든 활성 파일 시스템 데이터가 클라우드 계층에서 성능 계층으로 풀링됩니다.

◦ 고급 권한 레벨의 '-Tiering-Minimum-Cooling-Days' 선택적 매개 변수를 사용하면 '스냅샷 전용' 또는 '자동' 계층화 정책을 사용하는 볼륨에 대한 계층화 최소 냉각 기간을 지정할 수 있습니다.

ONTAP 9.8부터 계층화 최소 냉각 시간을 2에서 183 사이의 값으로 지정할 수 있습니다. 9.8 이전 버전의 ONTAP를 사용하는 경우 계층화 최소 냉각 요일에 대해 2 - 63 사이의 값을 지정할 수 있습니다.

FabricPool에 대한 볼륨 생성 예

다음 예에서는 ""myFabricPool"" FabricPool 지원 로컬 계층에 ""myvol1""이라는 볼륨을 생성합니다. 계층화 정책이 로

설정되고 `auto` 계층화 최소 냉각 기간은 45일로 설정됩니다.

```
cluster1::*> volume create -vserver myVS -aggregate myFabricPool
-volume myvol1 -tiering-policy auto -tiering-minimum-cooling-days 45
```

관련 정보

"FlexGroup 볼륨 관리"

볼륨을 **FabricPool** 지원 **ONTAP** 로컬 계층으로 이동

A는 "볼륨 이동"ONTAP가 하나의 로컬 계층(소스)에서 다른 타겟(타겟)으로 볼륨을 중단 없이 이동하는 방법입니다. 하드웨어 라이프사이클 관리, 클러스터 확장 및 로드 밸런싱이 가장 일반적인 이유이지만 볼륨 이동은 다양한 이유로 수행할 수 있습니다.

로컬 계층, 연결된 클라우드 계층 및 볼륨(볼륨 계층화 정책)에서 발생하는 변경 사항이 기능에 큰 영향을 미칠 수 있으므로 FabricPool에서 볼륨 이동이 어떻게 작동하는지 이해하는 것이 중요합니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

대상 로컬 계층

볼륨 이동의 타겟 로컬 계층에 연결된 클라우드 계층이 없는 경우 클라우드 계층에 저장된 소스 볼륨의 데이터가 타겟 로컬 계층의 로컬 계층에 기록됩니다.

ONTAP 9.8부터 볼륨을 활성화한 경우 "비활성 데이터 보고"FabricPool는 볼륨의 Heat Map을 사용하여 콜드 데이터가 대상 로컬 계층에 기록되는 즉시 계층화를 시작합니다.

ONTAP 9.8 이전에는 볼륨을 다른 로컬 계층으로 이동하면 로컬 계층에서 블록의 비활성 기간이 재설정됩니다. 예를 들어, 로컬 계층에 20일 동안 비활성 상태였지만 아직 계층화되지 않은 데이터가 있는 자동 볼륨 계층화 정책을 사용하는 볼륨은 볼륨 이동 후 데이터 온도가 0일로 재설정됩니다.

최적화된 볼륨 이동

ONTAP 9.6부터 볼륨 이동의 타겟 로컬 계층이 소스 로컬 계층과 동일한 버킷을 사용할 경우 버킷에 저장된 소스 볼륨의 데이터가 로컬 계층으로 다시 이동하지 않습니다. 계층화된 데이터는 사용되지 않고 핫 데이터만 로컬 계층 간에 이동되어야 합니다. 이렇게 최적화된 볼륨 이동을 통해 네트워크 효율성이 크게 향상됩니다.

예를 들어, 300TB의 최적화된 볼륨 이동은 300TB의 콜드 데이터가 한 로컬 계층에서 다른 로컬 계층으로 이동하더라도 개체 저장소에 대한 300TB의 읽기 및 300TB의 쓰기가 트리거되지 않음을 의미합니다.

최적화되지 않은 볼륨 이동은 추가 네트워크 및 컴퓨팅 트래픽(읽기/가져오기 및 쓰기/출력)을 생성하여 ONTAP 클러스터 및 오브젝트 저장소에 대한 수요를 증가시키며, 퍼블릭 오브젝트 저장소로 계층화할 때 비용이 상승할 가능성이 있습니다.

일부 구성은 최적화된 볼륨 이동과 호환되지 않습니다.

- 볼륨 이동 중에 계층화 정책 변경
- 서로 다른 암호화 키를 사용하는 소스 및 대상 로컬 계층
- FlexClone 볼륨
- FlexClone 상위 볼륨
- MetroCluster(ONTAP 9.8 이상에서 최적화된 볼륨 이동 지원)
- 동기화되지 않은 FabricPool 미러 버킷

볼륨 이동의 대상 로컬 계층에 연결된 클라우드 계층이 있는 경우 클라우드 계층에 저장된 소스 볼륨의 데이터가 먼저 대상 로컬 계층의 로컬 계층에 기록됩니다. 그런 다음 이 접근 방식이 볼륨의 계층화 정책에 적합한 경우 대상 로컬 계층의 클라우드 계층에 기록됩니다.

먼저 로컬 계층에 데이터를 기록하면 볼륨 이동 성능이 향상되고 컷오버 시간이 단축됩니다. 볼륨 이동을 수행할 때 볼륨 계층화 정책이 지정되지 않으면 타겟 볼륨이 소스 볼륨의 계층화 정책을 사용합니다.

볼륨 이동을 수행할 때 다른 계층화 정책을 지정하면 지정된 계층화 정책으로 타겟 볼륨이 생성되고 볼륨 이동이 최적화되지 않습니다.

볼륨 메타데이터

볼륨 이동 최적화 여부와 관계없이 ONTAP은 로컬 및 계층형 데이터의 위치, 스토리지 효율성, 권한, 사용 패턴 등에 대한 상당한 양의 메타데이터를 저장합니다. 메타데이터는 항상 로컬 계층에 저장되며 계층화되지 않습니다. 볼륨이 한 로컬 계층에서 다른 로컬 계층으로 이동되는 경우 이 정보도 대상 로컬 계층으로 이동해야 합니다.

기간

볼륨 이동에는 여전히 시간이 걸리며, 최적화된 볼륨 이동에는 계층화되지 않은 동일한 양의 데이터를 이동하는 데 걸리는 시간과 거의 같을 것으로 예상됩니다.

"처리량"이 보고된다는 것을 이해하는 것이 중요합니다. `volume move show` 명령은 클라우드 계층에서 이동하는 데이터 측면에서 처리량을 나타내는 것이 아니라 로컬에서 업데이트되는 볼륨 데이터를 나타냅니다.

SVM DR 관계에서는 소스 및 타겟 볼륨이 동일한 계층화 정책을 사용해야 한다.

단계

1. 명령을 사용하여 `volume move start` 볼륨을 소스 로컬 계층에서 대상 로컬 계층으로 이동합니다.

볼륨 이동의 예

다음 예에서는 `vs1` SVM이라는 볼륨을 FabricPool 지원 로컬 계층으로 `dest_FabricPool` 이동합니다 `myvol2`.

```
cluster1::> volume move start -vserver vs1 -volume myvol2
-destination-aggregate dest_FabricPool
```

ONTAP 9.14.1부터는 FabricPool의 신규 또는 기존 볼륨에 있는 클라우드에 직접 쓰기를 활성화 및 비활성화하여 NFS 클라이언트가 계층화 스캔을 기다리지 않고도 클라우드에 직접 데이터를 쓸 수 있도록 할 수 있습니다. SMB 클라이언트는 여전히 클라우드 쓰기 지원 볼륨의 성능 계층에 데이터를 씁니다. 클라우드 쓰기 모드는 기본적으로 비활성화되어 있습니다.

클라우드에 직접 쓸 수 있는 기능은 클러스터가 로컬 계층에서 지원할 수 있는 것보다 많은 양의 데이터를 클러스터로 전송하는 마이그레이션과 같은 경우에 유용합니다. 클라우드 쓰기 모드를 사용하지 않으면 마이그레이션 중에 더 적은 양의 데이터가 전송된 후 계층화한 다음, 마이그레이션이 완료될 때까지 다시 전송 및 계층화됩니다. 클라우드 쓰기 모드를 사용하면 데이터가 로컬 계층으로 전송되지 않기 때문에 이러한 유형의 관리가 더 이상 필요하지 않습니다.

시작하기 전에

- 클러스터 또는 SVM 관리자여야 합니다.
- advanced 권한 수준이어야 합니다.
- 볼륨은 읽기-쓰기 유형 볼륨이어야 합니다.
- 볼륨에 모든 계층화 정책이 있어야 한다.

볼륨 생성 시 클라우드에 직접 쓸 수 있습니다

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 볼륨 생성 및 클라우드 쓰기 모드 활성화:

```
volume create -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled <true|false> -aggregate <local tier name>
```

다음 예에서는 FabricPool 로컬 계층(aggr1)에 클라우드 쓰기가 설정된 vol1이라는 볼륨을 생성합니다.

```
volume create -vserver vs1 -volume vol1 -is-cloud-write-enabled true
-aggregate aggr1
```

기존 볼륨의 클라우드에 직접 쓸 수 있습니다

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 클라우드 쓰기 모드를 사용하도록 볼륨을 수정합니다.

```
volume modify -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled true
```

다음 예제에서는 클라우드 쓰기를 사용하도록 vol1 이라는 볼륨을 수정합니다.

```
volume modify -vserver vs1 -volume vol1 -is-cloud-write-enabled true
```

볼륨에 있는 클라우드에 직접 쓰기를 비활성화합니다

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 볼륨에서 클라우드 쓰기 모드 비활성화:

```
volume modify -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled false
```

다음 예에서는 vol1이라는 볼륨에서 클라우드 쓰기 모드를 비활성화합니다.

```
volume modify -vserver vs1 -volume vol1 -is-cloud-write-enabled false
```

FabricPool에서 **ONTAP** 볼륨을 활성화하여 적극적인 읽기-헤드를 수행할 수 있습니다

ONTAP 9.14.1부터는 FabricPools의 볼륨에 대해 공격적인 미리 읽기 모드를 활성화하거나 비활성화할 수 있습니다. ONTAP 9.13.1에서는 공격적 미리 읽기 모드가 클라우드 플랫폼에서만 도입되었습니다. ONTAP 9.14.1부터는 FabricPool이 지원하는 모든 플랫폼(온프레미스 플랫폼 포함)에서 공격적 미리 읽기 모드를 사용할 수 있습니다. 이 기능은 기본적으로 비활성화되어 있습니다.

적극적인 미리 읽기 가 _disabled_인 경우 FabricPool는 클라이언트 응용 프로그램에 필요한 파일 블록만 읽습니다. 전체 파일을 읽을 필요가 없습니다. 이로 인해 네트워크 트래픽, 특히 대용량 GB 및 TB 크기의 파일이 감소할 수 있습니다. _enabling_aggressive read-ahead는 볼륨에서 이 기능을 끄고 FabricPool는 객체 저장소에서 전체 파일을 순차적으로 읽으므로 처리량을 높이고 파일에 대한 클라이언트 읽기 대기 시간을 줄입니다. 기본적으로 계층화된 데이터를 순차적으로 읽으면 콜드 데이터가 로컬 계층에 기록되지 않고

공격적인 미리 읽기 거래 네트워크 효율성을 통해 계층화된 데이터의 성능을 향상시킵니다.

이 작업에 대해

를 클릭합니다 `aggressive-readahead-mode` 명령에는 두 가지 옵션이 있습니다.

- `none`: 미리 읽기를 사용할 수 없습니다.
- `file_prefetch`: 시스템은 클라이언트 응용 프로그램의 앞에 전체 파일을 메모리로 읽어들입니다.

시작하기 전에

- 클러스터 또는 SVM 관리자여야 합니다.
- advanced 권한 수준이어야 합니다.

볼륨을 생성하는 동안 적극적인 미리 읽기 모드를 활성화합니다

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 볼륨을 생성하고 적극적인 미리 읽기 모드를 활성화합니다.

```
volume create -volume <volume name>  -aggressive-readahead-mode
<none|file_prefetch>
```

다음 예에서는 file_prefetch 옵션을 사용하여 적극적인 read-ahead를 사용하도록 설정한 vol1이라는 볼륨을 생성합니다.

```
volume create -volume vol1 -aggressive-readahead-mode file_prefetch
```

적극적인 미리 읽기 모드를 비활성화합니다

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 적극적인 미리 읽기 모드 비활성화:

```
volume modify -volume <volume name>  -aggressive-readahead-mode none
```

다음 예에서는 vol1이라는 볼륨을 수정하여 적극적인 미리 읽기 모드를 비활성화합니다.

```
volume modify -volume vol1 -aggressive-readahead-mode none
```

볼륨에 대해 적극적인 미리 읽기 모드를 봅니다

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 공격적인 미리 읽기 모드 보기:

```
volume show -fields aggressive-readahead-mode
```

사용자가 생성한 맞춤형 태그로 **ONTAP FabricPool** 볼륨 관리

ONTAP 9.8부터 FabricPool는 사용자가 만든 사용자 지정 태그를 사용하여 개체 태그 지정을 지원하므로, 개체를 쉽게 분류하고 정렬할 수 있습니다. admin 권한 수준을 가진 사용자는 새 개체 태그를 만들고 기존 태그를 수정, 삭제 및 볼 수 있습니다.

볼륨을 생성하는 동안 새 태그를 할당합니다

새로 만든 볼륨에서 계층화된 새 개체에 하나 이상의 태그를 할당하려는 경우 새 개체 태그를 만들 수 있습니다. 태그를 사용하여 계층화 객체를 분류하고 정렬하면 데이터를 보다 쉽게 관리할 수 있습니다. ONTAP 9.8부터는 System Manager를 사용하여 개체 태그를 만들 수 있습니다.

이 작업에 대해

FabricPool에 연결된 StorageGRID 볼륨에서만 태그를 설정할 수 있습니다. 이러한 태그는 볼륨 이동 중에 유지됩니다.

- 볼륨당 최대 4개의 태그가 허용됩니다.
- CLI에서 각 개체 태그는 등호로 구분된 키-값 쌍이어야 합니다.
- CLI에서는 여러 태그를 쉼표로 구분해야 합니다.
- 각 태그 값은 최대 127자를 포함할 수 있습니다.
- 각 태그 키는 영문자 또는 밑줄로 시작해야 합니다.

  키에는 영숫자와 밑줄만 포함되어야 하며 허용되는 최대 문자 수는 127입니다.

ONTAP 시스템 관리자 또는 ONTAP CLI를 사용하여 오브젝트 태그를 할당할 수 있습니다.

예 **8.** 단계

시스템 관리자

1. Storage > Tiers * 로 이동합니다.
2. 태그를 지정할 볼륨이 있는 스토리지 계층을 찾습니다.
3. 볼륨 * 탭을 클릭합니다.
4. 태그를 지정할 볼륨을 찾고 * 개체 태그 * 열에서 * 태그를 입력하려면 클릭 * 을 선택합니다.
5. 키와 값을 입력합니다.
6. 적용 * 을 클릭합니다.

CLI를 참조하십시오

1. '-Tiering-object-tags' 옵션과 함께 'volume create' 명령을 사용하여 지정된 태그로 새 볼륨을 생성합니다. 쉼표로 구분된 쌍으로 여러 태그를 지정할 수 있습니다.

```
volume create [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1>
[,<key2=value2>,<key3=value3>,<key4=value4> ]
```

다음 예에서는 개체 태그가 3개인 fp_volume1 볼륨을 생성합니다.

```
vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=abc,content=data
```

기존 태그를 수정합니다

태그 이름을 변경하거나, 개체 저장소의 기존 개체에 있는 태그를 바꾸거나, 나중에 추가할 새 개체에 다른 태그를 추가할 수 있습니다.

예 **9.** 단계

시스템 관리자

1. Storage > Tiers * 로 이동합니다.
2. 수정할 태그가 포함된 볼륨이 있는 스토리지 계층을 찾습니다.
3. 볼륨 * 탭을 클릭합니다.
4. 수정할 태그가 있는 볼륨을 찾은 다음 * 개체 태그 * 열에서 태그 이름을 클릭합니다.
5. 태그를 수정합니다.
6. 적용 * 을 클릭합니다.

CLI를 참조하십시오

1. '-Tiering-object-tags' 옵션과 함께 'volume modify' 명령을 사용하여 기존 태그를 수정합니다.

```
volume modify [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1> [ ,<key2=value2>,
<key3=value3>,<key4=value4> ]
```

다음 예제에서는 기존 태그의 이름을 변경합니다. `type=abc` 에게 `type=xyz` .

```
vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=xyz,content=data
```

태그를 삭제합니다

오브젝트 태그가 더 이상 볼륨 또는 오브젝트 저장소 오브젝트에서 설정되지 않도록 하려면 오브젝트 태그를 삭제할 수 있습니다.

예 **10.** 단계

시스템 관리자

1. Storage > Tiers * 로 이동합니다.
2. 삭제할 태그가 포함된 볼륨이 있는 스토리지 계층을 찾습니다.
3. 볼륨 * 탭을 클릭합니다.
4. 삭제할 태그가 있는 볼륨을 찾고 * 개체 태그 * 열에서 태그 이름을 클릭합니다.
5. 태그를 삭제하려면 휴지통 아이콘을 클릭합니다.
6. 적용 * 을 클릭합니다.

CLI를 참조하십시오

1. 기존 태그를 삭제하려면 '-Tiering-object-tags' 옵션과 함께 'volume modify' 명령을 사용한 다음 빈 값("")을 사용합니다.

   다음 예제에서는 fp_volume1의 기존 태그를 삭제합니다.

   ```
   vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags ""
   ```

볼륨의 기존 태그를 봅니다

볼륨에 있는 기존 태그를 보고 목록에 새 태그를 추가하기 전에 사용 가능한 태그를 확인할 수 있습니다.

단계

1. 명령을 옵션과 함께 `tiering-object-tags` 사용하여 `volume show` 볼륨의 기존 태그를 봅니다.

   ```
   volume show [ -vserver <vserver name> ] -volume <volume_name> -fields
   tiering-object-tags
   ```

FabricPool 볼륨에서 객체 태그 지정 상태를 확인합니다

하나 이상의 FabricPool 볼륨에서 태깅이 완료되었는지 확인할 수 있습니다.

단계

1. 옵션과 함께 명령을 `-fields needs-object-retagging` 사용하여 `vol show` 태깅이 진행 중인지, 작업이 완료되었는지 또는 태깅이 설정되지 않았는지 확인하십시오.

   ```
   vol show -fields needs-object-retagging  [ -instance | -volume <volume
   name>]
   ```

   다음 값 중 하나가 표시됩니다.

- `true`: 개체 태그 지정 스캐너가 아직 실행되지 않았거나 이 볼륨에 대해 다시 실행해야 합니다
- `false`: 개체 태깅 스캐너가 이 볼륨에 대한 태그를 완료했습니다
- `<->`: 이 볼륨에는 개체 태그 지정 스캐너를 사용할 수 없습니다. 이 문제는 FabricPool에 없는 볼륨에 대해 발생합니다.

FabricPool 지원 **ONTAP** 로컬 계층의 공간 활용률 모니터링

FabricPool를 위해 성능 및 클라우드 계층에 얼마나 많은 데이터가 저장되어 있는지 알아야 합니다. 이 정보를 통해 볼륨의 계층화 정책을 변경해야 하는지, 라이센스가 부여된 FabricPool 사용 제한을 늘리거나, 클라우드 계층의 스토리지 공간을 늘려야 하는지 여부를 결정할 수 있습니다.

ONTAP 9.7 이전에는 System Manager에서 _aggregate_를 사용하여 _ 로컬 계층을 설명합니다. ONTAP 버전에 관계없이 ONTAP CLI에서는 _aggregate_라는 용어를 사용합니다. 로컬 계층에 대한 자세한 내용은 을 "디스크 및 로컬 계층"참조하십시오.

이 작업에 대해

ONTAP 9.18.1부터 `storage aggregate show-space` 명령은 논리적 참조 용량 및 논리적 미참조 용량 보고 방식을 변경합니다. 논리적 참조 용량은 모든 객체의 참조된 블록과 조각화된 객체의 미참조 블록을 보고합니다. 논리적 미참조 용량은 전체 임계값을 초과하여 객체 삭제 및 조각 모음 대상이 되는 객체의 미참조 블록만 보고합니다.

예를 들어 ONTAP S3 및 StorageGRID에 대해 기본 애그리게이트 충만도 임계값 40%를 사용하는 경우 객체의 블록 중 60%가 참조되지 않아야 블록이 참조되지 않은 용량으로 보고됩니다.

ONTAP 9.18.1 이전 릴리스에서는 논리적 참조 용량이 모든 객체(전체 객체 및 조각화된 객체 모두)의 참조된 블록을 보고합니다. 논리적 미참조 용량은 모든 객체의 미참조 블록을 보고합니다.

단계

1. 다음 명령 중 하나를 사용하여 FabricPool 사용 로컬 계층의 공간 활용률을 모니터링하여 정보를 표시합니다.

를 표시하려면…	다음 명령을 사용합니다.
로컬 계층에서 사용된 클라우드 계층의 크기입니다	'Storage aggregate show’를 -instance 매개변수로 표시합니다
객체 저장소의 참조 용량을 포함하여 로컬 계층 내의 공간 활용도에 대한 세부 정보입니다	인스턴스 매개 변수가 있는 'Storage aggregate show space’입니다
사용 중인 라이센스 공간을 비롯하여 로컬 계층에 연결된 오브젝트 저장소의 공간 활용도입니다	'스토리지 집계 오브젝트 저장소 표시 공간'
로컬 계층의 볼륨 목록 및 해당 데이터 및 메타데이터의 사용 공간	볼륨 쇼 풋프린트

CLI 명령을 사용할 뿐만 아니라 Active IQ Unified Manager(이전의 OnCommand Unified Manager)와 ONTAP 9.4 이상 클러스터에서 지원하는 FabricPool Advisor 또는 System Manager를 함께 사용하여 공간 사용률을 모니터링할 수 있습니다.

다음 예제는 FabricPool에 대한 공간 사용률 및 관련 정보를 표시하는 방법을 보여줍니다.

```
cluster1::> storage aggregate show-space -instance

                          Aggregate: MyFabricPool
                                                                    ...
                                        Aggregate Display Name:
MyFabricPool
                                                                    ...
                          Total Object Store Logical Referenced
Capacity: -
                          Object Store Logical Referenced Capacity
Percentage: -
                                                                    ...
                                                 Object Store
Size: -
                          Object Store Space Saved by Storage
Efficiency: -
                          Object Store Space Saved by Storage Efficiency
Percentage: -
                                                    Total Logical Used
Size: -
                                                    Logical Used
Percentage: -
                                               Logical Unreferenced
Capacity: -
                                             Logical Unreferenced
Percentage: -
```

```
cluster1::> storage aggregate show -instance

                           Aggregate: MyFabricPool
                           ...
                           Composite: true
                           Capacity Tier Used Size:
                           ...
```

```
cluster1::> volume show-footprint

Vserver : vs1
Volume : rootvol

Feature                             Used       Used%
--------------------------------- ---------- -----
Volume Footprint                  KB          %
Volume Guarantee                  MB          %
Flexible Volume Metadata          KB          %
Delayed Frees                     KB          %
Total Footprint                   MB          %

Vserver : vs1
Volume : vol

Feature                             Used       Used%
--------------------------------- ---------- -----
Volume Footprint                  KB          %
Footprint in Performance Tier     KB          %
Footprint in Amazon01             KB          %
Flexible Volume Metadata          MB          %
Delayed Frees                     KB          %
Total Footprint                   MB          %
...
```

2. 필요에 따라 다음 작업 중 하나를 수행합니다.

원하는 작업	그러면…
볼륨의 계층화 정책을 변경합니다	의 절차를 따릅니다 "볼륨의 계층화 정책을 수정하거나 최소 냉각 기간을 계층화하여 스토리지 계층화 관리".
FabricPool 라이센스 사용 제한을 늘립니다	NetApp 또는 파트너 세일즈 담당자에게 문의하십시오. "NetApp 지원"
클라우드 계층의 스토리지 공간 증가	클라우드 계층에 사용하는 오브젝트 저장소 공급자에 문의하십시오.

관련 정보

- "저장 집계 객체"
- "스토리지 애그리게이트 보기"
- "저장 집합 쇼 공간"

ONTAP 볼륨의 계층화 정책과 최소 냉각 기간을 수정합니다

비활성(*cold*) 상태가 될 때 데이터가 클라우드 계층으로 이동되는지 여부를 제어하기 위해 볼륨의 계층화 정책을 변경할 수 있습니다. '스냅샷 전용' 또는 '자동' 계층화 정책을 사용하는 볼륨의 경우, 사용자 데이터가 클라우드 계층으로 이동되기 전에 비활성 상태를 유지해야 하는 계층화 최소 냉각 기간을 지정할 수도 있습니다.

시작하기 전에

볼륨을 '자동' 계층화 정책으로 변경하거나 계층화 최소 냉각 기간을 수정하려면 ONTAP 9.4 이상이 필요합니다.

이 작업에 대해

볼륨의 계층화 정책을 변경하면 볼륨에 대한 후속 계층화 동작만 변경됩니다. 데이터를 클라우드 계층으로 소급 이동하지 않습니다.

계층화 정책을 변경하면 데이터가 콜드 상태가 되어 클라우드 계층으로 이동하는 데 걸리는 시간이 영향을 받을 수 있습니다.

"FabricPool에서 볼륨의 계층화 정책을 수정하면 어떻게 됩니까"

SVM DR 관계인 경우 소스 및 타겟 볼륨에서 FabricPool 애그리게이트를 사용할 필요가 없지만 동일한 계층화 정책을 사용해야 합니다.

단계

1. '-Tiering-policy' 매개 변수와 함께 'volume modify' 명령을 사용하여 기존 볼륨의 계층화 정책을 수정합니다.

   다음 계층화 정책 중 하나를 지정할 수 있습니다.

   - '스냅샷 전용'(기본값)
   - 자동
   - 모두
   - "없음"

     "FabricPool 계층화 정책의 유형입니다"

2. 볼륨이 '스냅샷 전용' 또는 '자동' 계층화 정책을 사용하고 계층화 최소 냉각 기간을 수정하려면 고급 권한 수준에서 '-Tiering-Minimum-Cooling-Days' 선택적 매개 변수와 함께 'volume modify' 명령을 사용하십시오.

   최소 계층화 냉각 일수는 2에서 183 사이의 값을 지정할 수 있습니다. 9.8 이전 버전의 ONTAP를 사용하는 경우 계층화 최소 냉각 요일에 대해 2 - 63 사이의 값을 지정할 수 있습니다.

계층화 정책 및 볼륨의 최소 계층화 냉각 기간을 수정하는 예

다음 예에서는 SVM의 볼륨 "VS1"에서 볼륨 "myvol"의 계층화 정책을 "auto"로, 계층화 최소 냉각 기간을 45일로 변경합니다.

```
cluster1::> volume modify -vserver vs1 -volume myvol
-tiering-policy auto -tiering-minimum-cooling-days 45
```

FabricPool로 볼륨 아카이브(비디오)

이 비디오에서는 FabricPool를 사용하여 볼륨을 클라우드 계층에 아카이브하는 방법에 대해 간략하게 설명합니다.

"NetApp 비디오: FabricPool로 볼륨 아카이빙(백업 + 볼륨 이동)"

관련 정보

"NetApp TechComm TV: FabricPool 재생 목록"

ONTAP 볼륨의 기본 **FabricPool** 계층화 정책을 수정합니다

ONTAP 9.8에 도입된 '-cloud-retrieval-policy' 옵션을 사용하여 클라우드 계층에서 성능 계층으로 사용자 데이터 검색을 제어하는 볼륨의 기본 계층화 정책을 변경할 수 있습니다.

시작하기 전에

- '-cloud-retrieval-policy' 옵션을 사용하여 볼륨을 수정하려면 ONTAP 9.8 이상이 필요합니다.
- 이 작업을 수행하려면 고급 권한 수준이 있어야 합니다.
- 계층화 정책의 동작을 클라우드 검색 정책으로 이해해야 합니다.

  "계층화 정책이 클라우드 마이그레이션과 작동하는 방식"

단계

1. '-cloud-retrieval-policy' 옵션과 함께 'volume modify' 명령을 사용하여 기존 볼륨의 계층화 정책 동작을 수정합니다.

```
 volume create -volume <volume_name> -vserver <vserver_name> - tiering-
policy <policy_name> -cloud-retrieval-policy
```

```
vol modify -volume fp_volume4 -vserver vs0 -cloud-retrieval-policy
promote
```

ONTAP FabricPool 노드당 입력 속도에 대한 임계값 설정

스토리지 관리자는 PUT 제한을 사용하여 최대 노드당 PUT 속도에 대한 임계값을 설정할 수 있습니다.

PUT 임계치 조절은 네트워크 리소스 또는 개체 저장소 끝점이 리소스가 제한되어 있는 경우에 유용합니다. 드물기는 하지만 성능이 부족한 오브젝트 저장소나 FabricPool 사용량이 처음 발생하는 동안 TB 또는 PB의 콜드 데이터가 계층화되기 시작하면 리소스 제약이 발생할 수 있습니다.

PUT 임계치 조절은 노드마다 적용됩니다. 최소 PUT 제한 PUT 속도 제한은 8MB/s입니다 PUT 속도 제한을 8MB/s 미만의 값으로 설정하면 해당 노드에서 8MB/s의 처리량이 생성됩니다. 여러 노드를 동시에 계층화하면 더 많은 대역폭을 소비하고 용량이 매우 제한된 네트워크 링크가 포화될 수 있습니다.

FabricPool PUT 작업은 리소스를 다른 애플리케이션과 경쟁하지 않습니다. FabricPool PUT 작업은 클라이언트 애플리케이션 및 SnapMirror 같은 기타 ONTAP 워크로드에서 자동으로 낮은 우선순위("중요")에 배치됩니다. PUT 제한 `put-rate-limit` 사용은 FabricPool 계층화와 관련된 네트워크 트래픽을 줄이는 데 유용할 수 있지만 동시 ONTAP 트래픽과는 관련이 없습니다.

시작하기 전에

고급 권한 수준이 필요합니다.

단계

1. ONTAP CLI를 사용하여 FabricPool Put 작업 임계치 조절:

```
storage aggregate object-store put-rate-limit modify -node <name>
-default <true|false> -put-rate-bytes-limit <integer>[KB|MB|GB|TB|PB]
```

관련 정보

- "스토리지 애그리게이트 오브젝트 저장소 금률 제한 수정"

ONTAP FabricPool 객체 삭제 및 조각 모음 사용자 지정

FabricPool는 연결된 오브젝트 저장소에서 블록을 삭제하지 않습니다. 대신, FabricPool는 개체의 특정 블록 비율이 더 이상 ONTAP에서 참조되지 않으면 개체를 삭제합니다.

예를 들어, Amazon S3로 계층화된 4MB 오브젝트에 1,024개의 4KB 블록이 있습니다. 조각 모음 및 삭제는 ONTAP에서 참조되는 4KB 블록 205개(1,024개 중 20%)가 될 때까지 발생하지 않습니다. 충분한(1,024) 블록에 참조가 없으면 원래 4MB 개체가 삭제되고 새 개체가 만들어집니다.

회수되지 않은 공간 임계값 비율을 사용자 지정하고 오브젝트 저장소마다 다른 기본 수준으로 설정할 수 있습니다. 기본 설정은 다음과 같습니다.

오브젝트 저장소	ONTAP 9.8 이상	ONTAP 9.7~9.4	ONTAP 9.3 및 이전 버전	Cloud Volumes ONTAP
Amazon S3	20%	20%	0%	30%
Google 클라우드 스토리지	20%	12%	해당 없음	35%
Microsoft Azure Blob 저장소	25%	15%	해당 없음	35%
NetApp ONTAP S3를 참조하십시오	40%	해당 없음	해당 없음	해당 없음
NetApp StorageGRID를 참조하십시오	40%	40%	0%	해당 없음

재확보된 공간 임계값입니다

재확보되지 않은 기본 공간 임계값 설정을 변경하면 허용되는 개체 조각화 양이 증가하거나 줄어듭니다. 조각화를 줄이면 추가 오브젝트 저장소 리소스(읽기 및 쓰기)를 희생하면서 클라우드 계층에서 사용하는 물리적 용량이 줄어듭니다.

임계값 감소

추가 비용을 방지하려면 스토리지 비용은 줄이고 읽기 비용은 높이는 오브젝트 저장소 가격 체계를 사용할 때 회수되지 않는 공간 임계값을 줄이는 것이 좋습니다. Amazon의 Standard-IA 및 Azure Blob Storage의 Cool을 예로 들 수 있습니다.

예를 들어, 법적 이유로 저장된 10년 된 프로젝트의 볼륨을 계층화하면 표준 가격 체계를 사용하는 경우보다 Standard-IA 또는 Cool과 같은 가격 체계를 사용하는 데 비용이 적게 들 수 있습니다. 이러한 볼륨에서 읽기는 개체 조각 모음에 필요한 읽기를 포함하여 비용이 더 많이 들지만 자주 발생할 가능성은 낮습니다.

임계값이 증가합니다

또는 객체 조각화로 인해 ONTAP에서 참조하는 데이터에 필요한 것보다 훨씬 더 많은 오브젝트 저장소 용량을 사용할 경우 재확보되지 않은 공간 임계값을 늘리는 것이 좋습니다. 예를 들어, 모든 오브젝트가 최대 허용 익스텐트로 균등하게 분할되는 최악의 경우 20%의 재확보된 공간 임계값을 사용하면 클라우드 계층의 총 용량의 80%가 ONTAP에서 참조하지 않을 수 있습니다. 예를 들면 다음과 같습니다.

ONTAP + ONTAP에서 참조하지 않는 8TB = 클라우드 계층에서 사용하는 총 10TB 용량

이 경우 재확보된 공간 임계값을 높이거나 볼륨 최소 냉각 날짜를 늘려서 참조되지 않은 블록이 사용하는 용량을 줄이는 것이 유리할 수 있습니다.

> 시스템에서 오브젝트를 조각 모음하고 스토리지 효율성을 높이면 참조된 블록을 새롭고 더 효율적인 오브젝트에 작성하여 기본 파일을 단편화할 수 있습니다. 재확보된 공간 임계값을 크게 증가시키면 스토리지 효율성이 더 높지만 순차적 읽기 성능이 저하된 오브젝트를 생성할 수 있습니다.
>
> 이러한 추가 활동을 통해 AWS, Azure, Google 등의 타사 S3 공급자가 제공하는 비용이 증가하게 됩니다.
>
> NetApp은 재확보된 공간 임계값이 60%보다 높지 않도록 하는 것이 좋습니다.

재확보된 공간 임계값을 변경합니다

여러 오브젝트 저장소에 대해 재확보된 공간 임계값 비율을 사용자 지정할 수 있습니다.

시작하기 전에

고급 권한 수준이 필요합니다.

단계

1. 재확보되지 않은 기본 공간 임계값을 변경하려면 다음 명령을 사용자 지정하고 실행합니다.

```
storage aggregate object-store modify -aggregate <name> -object-store
-name <name> -unreclaimed-space-threshold <%> (0%-99%)
```

관련 정보

- "저장소 집계 객체-저장소 수정"

ONTAP 데이터를 성능 계층으로 승격한다

ONTAP 9.8부터 고급 권한 수준의 클러스터 관리자라면 계층화-정책과 클라우드 검색-정책 설정을 조합하여 클라우드 계층에서 성능 계층으로 데이터를 사전 예방적으로 승격할 수 있습니다.

이 작업에 대해

볼륨에서 FabricPool 사용을 중지하거나 계층화 정책이 있고 복원된 스냅샷 데이터를 성능 계층으로 다시 가져오려는 경우 이 작업을 수행할 수 `snapshot-only` 있습니다.

FabricPool 볼륨의 모든 데이터를 성능 계층으로 상향 이동합니다

클라우드 계층에서 FabricPool 볼륨의 모든 데이터를 사전에 검색하여 성능 계층으로 승격할 수 있습니다.

단계

1. 볼륨 수정 명령을 사용하여 계층화-정책을 없음으로 설정하고 클라우드 검색-정책을 상향 이동 정책으로 설정합니다.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy none -cloud-retrieval-policy promote
```

파일 시스템 데이터를 성능 계층으로 상향 이동합니다

클라우드 계층의 복원된 스냅샷에서 활성 파일 시스템 데이터를 사전에 검색하여 성능 계층으로 승격할 수 있습니다.

단계

1. 볼륨 수정 명령을 사용하여 계층화-정책을 '스냅샷 전용'으로 설정하고 '승격'을 위한 클라우드 검색 정책을 설정하십시오.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy snapshot-only cloud-retrieval-policy promote
```

성능 계층 프로모션의 상태를 확인합니다

성능 계층 프로모션의 상태를 확인하여 작업이 완료되는 시기를 결정할 수 있습니다.

단계

1. '계층화' 옵션과 함께 volume 'object-store' 명령을 사용하여 성능 계층 프로모션의 상태를 확인합니다.

```
volume object-store tiering show [ -instance | -fields <fieldname>, ...
] [ -vserver <vserver name> ] *Vserver
[[-volume] <volume name>] *Volume [ -node <nodename> ] *Node Name [ -vol
-dsid <integer> ] *Volume DSID
[ -aggregate <aggregate name> ] *Aggregate Name
```

```
volume object-store tiering show v1 -instance

                                  Vserver: vs1
                                   Volume: v1
                                Node Name: node1
                              Volume DSID: 1023
                           Aggregate Name: a1
                                    State: ready
                      Previous Run Status: completed
                  Aborted Exception Status: -
               Time Scanner Last Finished: Mon Jan 13 20:27:30 2020
                 Scanner Percent Complete: -
                      Scanner Current VBN: -
                         Scanner Max VBNs: -
     Time Waiting Scan will be scheduled: -
                           Tiering Policy: snapshot-only
    Estimated Space Needed for Promotion: -
                       Time Scan Started: -
  Estimated Time Remaining for scan to complete: -
                    Cloud Retrieve Policy: promote
```

예약된 마이그레이션 및 계층화 트리거

ONTAP 9.8부터 기본 계층화 스캔을 기다리지 않으려는 경우 언제든지 계층화 스캔 요청을 트리거할 수 있습니다.

단계

1. 'trigger' 옵션과 함께 'volume object-store' 명령을 사용하여 마이그레이션 및 계층화를 요청합니다.

```
volume object-store tiering trigger [ -vserver <vserver name> ] *VServer
Name [-volume] <volume name> *Volume Name
```

FabricPool 미러를 관리합니다

ONTAP FabricPool 미러에 대해 알아봅니다

재해 발생 시 데이터 저장소에서 데이터에 액세스할 수 있도록 하고 데이터 저장소를 교체할 수

있도록 하려면 두 번째 데이터 저장소를 추가하여 FabricPool 미러를 구성하여 데이터를 두 개의 데이터 저장소에 동기적으로 계층화할 수 있습니다. 새 또는 기존 FabricPool 구성에 두 번째 데이터 저장소를 추가하고, 미러 상태를 모니터링하고, FabricPool 미러 세부 정보를 표시하고, 미러를 프로모션하고, 미러를 제거할 수 있습니다. ONTAP 9.7 이상을 실행 중이어야 합니다.

ONTAP FabricPool 미러를 생성합니다

FabricPool 미러를 생성하려면 두 개의 오브젝트 저장소를 단일 FabricPool에 연결합니다. 두 번째 개체 저장소를 기존 단일 개체 저장소 FabricPool 구성에 연결하여 FabricPool 미러를 만들거나, 새 단일 개체 저장소 FabricPool 구성을 만든 다음 두 번째 개체 저장소를 연결할 수 있습니다. MetroCluster 구성에서 FabricPool 미러를 생성할 수도 있습니다.

시작하기 전에

- 'Storage aggregate object-store config' 명령을 사용하여 이미 두 개의 오브젝트 저장소를 만들어야 합니다.
- MetroCluster 구성에서 FabricPool 미러를 생성하는 경우
  - MetroCluster를 이미 설정하고 구성해야 합니다
  - 선택한 클러스터에 오브젝트 저장소 구성을 생성해야 합니다.

    MetroCluster 구성에서 두 클러스터에 모두 FabricPool 미러를 생성하는 경우 두 클러스터 모두에서 오브젝트 저장소 구성을 생성해야 합니다.

  - MetroCluster 구성에 온-프레미스 개체 저장소를 사용하지 않는 경우 다음 시나리오 중 하나가 있는지 확인해야 합니다.
    - 오브젝트 저장소는 다른 가용성 영역에 있습니다
    - 오브젝트 저장소는 오브젝트의 복사본을 여러 가용성 영역에 보관하도록 구성됩니다

      "MetroCluster 구성에서 FabricPool에 대한 오브젝트 저장소 설정"

이 작업에 대해

FabricPool 미러에 사용하는 오브젝트 저장소는 운영 오브젝트 저장소와 달라야 합니다.

FabricPool 미러를 생성하는 절차는 MetroCluster 구성과 비 MetroCluster 구성 모두에서 동일합니다.

단계

1. 기존 FabricPool 구성을 사용하지 않는 경우 명령을 사용하여 개체 저장소를 로컬 계층에 연결하여 새 구성을 `storage aggregate object-store attach` 생성합니다.

   이 예제에서는 개체 저장소를 로컬 계층에 연결하여 새 FabricPool을 생성합니다.

   ```
   cluster1::> storage aggregate object-store attach -aggregate aggr1 -name
   my-store-1
   ```

2. 명령을 사용하여 두 번째 오브젝트 저장소를 로컬 계층에 `storage aggregate object-store mirror` 연결합니다.

이 예에서는 두 번째 객체 저장소를 로컬 계층에 연결하여 FabricPool 미러를 생성합니다.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name
my-store-2
```

관련 정보

- "저장소 집계 객체-저장소 연결"
- "저장소 집계 객체 저장소 구성"
- "저장소 집계 객체-저장소 미러"

ONTAP FabricPool 미러 세부 정보를 표시합니다

FabricPool 미러에 대한 세부 정보를 표시하여 구성에 있는 오브젝트 저장소 및 객체 저장소 미러가 운영 오브젝트 저장소와 동기화되어 있는지 여부를 확인할 수 있습니다.

단계

1. 'storage aggregate object-store show' 명령을 사용하여 FabricPool 미러에 대한 정보를 표시합니다.

   이 예제에서는 FabricPool 미러에 저장된 운영 및 미러 객체에 대한 세부 정보를 표시합니다.

```
cluster1::> storage aggregate object-store show
```

```
Aggregate      Object Store Name Availability    Mirror Type
-------------- ----------------- -------------   ----------
aggr1          my-store-1        available       primary
               my-store-2        available       mirror
```

   이 예에서는 재동기화 작업으로 인한 미러 성능 저하 여부를 비롯하여 FabricPool 미러에 대한 세부 정보를 표시합니다.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-store-1        primary           -
               my-store-2        mirror          false
```

관련 정보

- "저장소 집계 객체-저장소 표시"

ONTAP FabricPool 미러를 상향 이동합니다

객체 저장소 미러를 프로모션하여 운영 오브젝트 저장소로 재할당할 수 있습니다. 객체 저장소 미러가 1차 미러가 되면 원래 1차 미러가 자동으로 미러가 됩니다.

시작하기 전에

- FabricPool 미러가 동기화되어 있어야 합니다
- 오브젝트 저장소가 운영되어야 합니다

이 작업에 대해

원래 오브젝트 저장소를 다른 클라우드 공급자의 오브젝트 저장소로 대체할 수 있습니다. 예를 들어, 원래 미러는 AWS 오브젝트 저장소이지만 Azure 오브젝트 저장소로 대체할 수 있습니다.

단계

1. 명령을 사용하여 FabricPool 미러가 동기화되어 있는지 `storage aggregate object-store show-resync-status` 확인합니다. FabricPool 미러가 동기화되어 있으면 항목이 표시되지 않습니다. 미러가 동기화되어 있지 않으면 재동기화가 완료될 때까지 기다립니다.

```
aggregate1::> storage aggregate object-store show-resync-status
-aggregate aggr1
```

```
                                          Complete
Aggregate    Primary       Mirror         Percentage
---------    -----------   ----------     ----------
aggr1        my-store-1     my-store-2      40%
```

2. 'storage aggregate object-store modify-aggregate' 명령을 사용하여 오브젝트 저장소 미러를 상향 이동합니다.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name
my-store-2 -mirror-type primary
```

관련 정보

- "저장소 집계 객체-저장소 수정"
- "저장소 집계 객체 저장소 show-resync-status"

ONTAP FabricPool 미러를 탈거하십시오

더 이상 오브젝트 저장소를 복제할 필요가 없는 경우 FabricPool 미러를 제거할 수 있습니다.

시작하기 전에

운영 오브젝트 저장소가 작동 중이어야 하며, 그렇지 않으면 명령이 실패합니다.

단계

1. 'storage aggregate object-store unmirror-aggregate' 명령을 사용하여 FabricPool에서 오브젝트 저장소 미러를 제거합니다.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

관련 정보

- "저장소 집계 객체-저장소 미러링 해제"

기존 오브젝트 저장소를 **ONTAP FabricPool** 미러로 교체합니다

FabricPool 미러 기술을 사용하여 한 오브젝트 저장소를 다른 오브젝트 저장소로 대체할 수 있습니다. 새 오브젝트 저장소는 원래 오브젝트 저장소와 동일한 클라우드 공급자를 사용할 필요가 없습니다.

이 작업에 대해

원래 오브젝트 저장소를 다른 클라우드 공급자를 사용하는 오브젝트 저장소로 대체할 수 있습니다. 예를 들어, 원래 오브젝트 저장소에서 AWS를 클라우드 공급자로 사용할 수 있지만, Azure를 클라우드 공급자로 사용하는 오브젝트 저장소로 대체할 수 있습니다. 그러나 새 오브젝트 저장소는 원본과 동일한 오브젝트 크기를 유지해야 합니다.

단계

1. 'Storage aggregate object-store mirror' 명령을 사용하여 기존 FabricPool에 새 오브젝트 저장소를 추가하여 FabricPool 미러를 생성합니다.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1
-object-store-name my-AZURE-store
```

2. 'storage aggregate object-store show-resync-status' 명령을 사용하여 미러 재동기화 상태를 모니터링합니다.

```
cluster1::> storage aggregate object-store show-resync-status -aggregate
aggr1
```

```
                                                  Complete
Aggregate    Primary          Mirror          Percentage
---------    -----------      ----------      ----------
aggr1        my-AWS-store     my-AZURE-store      40%
```

3. 'Storage aggregate object-store > show-fields mirror-type, is-mirror-degraded' 명령을 사용하여 미러가 동기화되어 있는지 확인합니다.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AWS-store        primary           -
               my-AZURE-store      mirror          false
```

4. 'Storage aggregate object-store modify' 명령을 사용하여 운영 오브젝트 저장소를 미러 오브젝트 저장소로 바꾸십시오.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1
-object-store-name my-AZURE-store -mirror-type primary
```

5. 'Storage aggregate object-store show-fields mirror-type, is-mirror-degraded' 명령을 사용하여 FabricPool 미러에 대한 세부 정보를 표시합니다.

   이 예에서는 미러의 성능 저하(동기식 아님) 여부를 비롯하여 FabricPool 미러에 대한 정보를 표시합니다.

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
               my-AWS-store        mirror          false
```

6. 'storage aggregate object-store unmirror' 명령어를 사용해 FabricPool 미러를 제거한다.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

7. 'storage aggregate object-store show-fields mirror-type, is-mirror-degraded' 명령을 사용하여 FabricPool가 단일 오브젝트 저장소 구성으로 다시 설정되었는지 확인합니다.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
```

관련 정보

- "저장소 집계 객체-저장소 미러"
- "저장소 집계 객체-저장소 수정"
- "저장소 집계 객체 저장소 show-resync-status"
- "저장소 집계 객체-저장소 표시"
- "저장소 집계 객체-저장소 미러링 해제"

ONTAP MetroCluster 구성에서 **FabricPool** 미러를 교체합니다

FabricPool 미러에 저장된 객체 중 하나가 제거되거나 MetroCluster 구성에서 영구적으로 사용할 수 없게 되는 경우 미러가 아직 미러가 아닌 경우 손상된 객체 저장소를 FabricPool 미러에서 제거할 수 있습니다. 그런 다음 새 오브젝트 저장소 미러를 FabricPool에 추가합니다.

단계

1. 손상된 오브젝트 저장소가 아직 미러가 아닌 경우 'Storage aggregate object-store modify' 명령을 사용하여 미러를 저장합니다.

```
storage aggregate object-store modify -aggregate -aggregate fp_aggr1_A01
-name mcc1_ostore1 -mirror-type mirror
```

2. 'Storage aggregate object-store unmirror' 명령을 사용하여 FabricPool에서 오브젝트 저장소 미러를 제거합니다.

```
storage aggregate object-store unmirror -aggregate <aggregate name>
-name mcc1_ostore1
```

3. "force-Tiering-on-MetroCluster true" 옵션을 사용하여 'Storage aggregate object-store modify"를 사용하여 미러 데이터 저장소를 제거한 후 운영 데이터 저장소에서 계층화를 강제로 다시 시작할 수 있습니다.

   미러가 없으면 MetroCluster 구성의 복제 요구 사항에 방해가 됩니다.

```
storage aggregate object-store modify -aggregate <aggregate name> -name
mcc1_ostore1 -force-tiering-on-metrocluster true
```

4. 'Storage aggregate object-store config create' 명령을 사용하여 대체 오브젝트 저장소를 생성합니다.

```
storage aggregate object-store config create -object-store-name
mcc1_ostore3 -cluster clusterA -provider-type SGWS -server <SGWS-server-
1> -container-name <SGWS-bucket-1> -access-key <key> -secret-password
<password> -encrypt <true|false> -provider <provider-type> -is-ssl
-enabled <true|false> ipspace <IPSpace>
```

5. 'Storage aggregate object-store mirror' 명령을 사용하여 FabricPool 미러에 객체 저장소 미러를 추가합니다.

```
storage aggregate object-store mirror -aggregate aggr1 -name
mcc1_ostore3-mc
```

6. 'storage aggregate object-store show' 명령을 사용하여 오브젝트 저장소 정보를 표시합니다.

```
storage aggregate object-store show -fields mirror-type,is-mirror-
degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          mcc1_ostore1-mc    primary            -
               mcc1_ostore3-mc    mirror           true
```

7. 'storage aggregate object-store show-resync-status' 명령을 사용하여 미러 재동기화 상태를 모니터링합니다.

```
storage aggregate object-store show-resync-status -aggregate aggr1
```

```
                                                Complete
     Aggregate    Primary        Mirror          Percentage
     ---------    -----------    ----------      ----------
     aggr1        mcc1_ostore1-mc mcc1_ostore3-mc   40%
```

관련 정보

- "저장소 집계 객체-저장소 구성 생성"
- "저장소 집계 객체-저장소 미러"
- "저장소 집계 객체-저장소 수정"
- "저장소 집계 객체-저장소 표시"
- "저장소 집계 객체 저장소 show-resync-status"
- "저장소 집계 객체-저장소 미러링 해제"

FabricPool 리소스를 관리하기 위한 ONTAP 명령

'Storage aggregate object-store' 명령을 사용하여 FabricPool의 오브젝트 저장소를 관리할 수 있습니다. '스토리지 애그리게이트' 명령을 사용하여 FabricPool의 애그리게이트를 관리할 수 있습니다. 'volume' 명령을 사용하여 FabricPool의 볼륨을 관리할 수 있습니다.

원하는 작업	다음 명령을 사용합니다.
ONTAP에서 액세스할 수 있도록 객체 저장소에 대한 구성을 정의합니다	'스토리지 집계 객체 저장소 구성 생성'을 선택합니다
오브젝트 저장소 구성 특성을 수정합니다	'Storage aggregate object-store config modify'를 참조하십시오
기존 오브젝트 저장소 구성의 이름을 바꿉니다	'스토리지 집계 객체 저장소 구성 이름 바꾸기'를 선택합니다
오브젝트 저장소 구성을 삭제합니다	'스토리지 집계 객체 저장소 구성 삭제'를 선택합니다
오브젝트 저장소 구성 목록을 표시합니다	'Storage aggregate object-store config show'를 선택합니다
새 FabricPool 또는 기존에 미러로 두 번째 오브젝트 저장소를 연결합니다	관리 권한 수준에서 '-aggregate' 및 '-name' 매개 변수가 있는 스토리지 집계 오브젝트 저장소 미러
기존 FabricPool 미러에서 오브젝트 저장소 미러를 제거합니다	관리 권한 수준에서 '-aggregate' 및 '-name' 매개 변수가 있는 '스토리지 집계 객체 저장소 언미러'입니다
FabricPool 미러 재동기화 상태를 모니터링합니다	'Storage aggregate object-store show-resync-status'를 참조하십시오
FabricPool 미러 세부 정보를 표시합니다	'스토리지 골재 오브젝트 저장소 쇼'
FabricPool 미러 구성에서 운영 오브젝트 저장소를 대체하도록 오브젝트 저장소 미러를 승격합니다	관리 권한 수준에서 '-aggregate' 매개 변수를 사용하여 '스토리지 애그리게이트 오브젝트 저장소 수정'을 수행합니다
오브젝트 저장소를 Aggregate에 연결하지 않고 오브젝트 저장소의 지연 시간과 성능을 테스트합니다	스토리지 집계 오브젝트 저장소 프로파일러는 고급 권한 수준에서 '-object-store-name' 및 '-node' 매개변수로 시작됩니다
오브젝트 저장소 프로파일러 상태를 모니터링합니다	스토리지 집계 오브젝트 저장소 프로파일러는 고급 권한 수준에서 '-object-store-name' 및 '-node' 매개 변수를 사용하여 표시합니다

실행 중인 개체 저장소 프로파일러를 중단합니다	고급 권한 수준에서 '-object-store-name' 및 '-node' 매개변수를 사용하여 '저장소 집계 개체 저장소 프로파일러 중단'을 실행하십시오
FabricPool를 사용하기 위해 오브젝트 저장소를 Aggregate에 연결합니다	'스토리지 골재 오브젝트 저장소 연결'을 참조하십시오
FabricPool를 사용하기 위해 FlexGroup 볼륨이 포함된 애그리게이트에 오브젝트 저장소를 연결합니다	'allow-flexgroup'이 true인 'tTRUE'로 'STOATTATE OBJECT-STORE ATTACH'가 가능합니다
FabricPool 지원 애그리게이트에 연결된 오브젝트 저장소의 세부 정보를 표시합니다	'스토리지 골재 오브젝트 저장소 쇼'
계층화 스캔에서 사용되는 애그리게이트 충만 임계값을 표시합니다	고급 권한 레벨의 필드 계층화-충만함-임계값 매개변수를 사용하여 '스토리지 집계 오브젝트 저장소 표시'를 표시합니다
FabricPool 지원 애그리게이트에 연결된 오브젝트 저장소의 공간 활용률을 표시합니다	'스토리지 집계 오브젝트 저장소 표시 공간'
FabricPool에 사용되지 않는 애그리게이트에 대해 비활성 데이터 보고를 설정합니다	'스토리지 집계 수정'을 '-is-inactive-data-reporting-enabled true' 매개변수로 사용합니다
비활성 데이터 보고가 집계에서 활성화되어 있는지 여부를 표시합니다	"필드 is-inactive-data-reporting-enabled" 매개 변수가 있는 '스토리지 집계 표시'입니다
집계 내에서 얼마나 많은 사용자 데이터가 콜드 데이터인지 표시합니다	'fields performance-tier-inactive-user-data, performance-tier-inactive-user-data-percent' 매개 변수가 있는 'storage aggregate show space'입니다
다음을 지정하는 등 FabricPool용 볼륨을 생성합니다. • 계층화 정책 • 계층화 최소 냉각 기간('스냅샷 전용' 또는 '자동' 계층화 정책)	'볼륨 생성' • 계층화 정책을 지정하려면 '-Tiering-policy' 매개 변수를 사용합니다. • 고급 권한 수준에서 '-Tiering-Minimum-Cooling-Days' 매개 변수를 사용하여 계층화 최소 냉각 기간을 지정합니다.
다음 사항을 수정하는 등 FabricPool의 볼륨을 수정합니다. • 계층화 정책 • 계층화 최소 냉각 기간('스냅샷 전용' 또는 '자동' 계층화 정책)	볼륨 수정 • 계층화 정책을 지정하려면 '-Tiering-policy' 매개 변수를 사용합니다. • 고급 권한 수준에서 '-Tiering-Minimum-Cooling-Days' 매개 변수를 사용하여 계층화 최소 냉각 기간을 지정합니다.

다음과 같은 볼륨 관련 FabricPool 정보를 표시합니다. • 계층화 최소 냉각 기간 • 사용 빈도가 낮은 사용자 데이터의 양	'볼륨 쇼' • 고급 권한 수준에서 '-fields Tiering-minimum-cooling-days' 매개 변수를 사용하여 계층화 최소 냉각 기간을 표시합니다. • '-fields performance-tier-inactive-user-data, performance-tier-inactive-user-data-percent' 매개 변수를 사용하여 사용자 데이터의 사용 빈도가 낮은 양을 표시할 수 있습니다.
FabricPool로 또는 밖으로 볼륨을 이동합니다	볼륨 이동 시작 '-Tiering-policy' 선택적 매개 변수를 사용하여 볼륨에 대한 계층화 정책을 지정합니다.
FabricPool에 대해 참조되지 않은 공간(조각 모음 임계값)을 회수하기 위한 임계값을 수정합니다	고급 권한 레벨의 unrecla재확보된 공간 임계값 매개변수를 사용하여 스토리지 집계 오브젝트 저장소를 수정합니다
계층화 검사가 FabricPool에 대한 데이터 계층화를 시작하기 전에 애그리게이트의 전체 비율을 위한 임계값을 수정합니다 FabricPool은 로컬 계층이 98%에 도달할 때까지 콜드 데이터를 클라우드 계층으로 계속 계층화합니다.	고급 권한 레벨의 계층화-fullness-threshold로 스토리지 집계 객체 저장소 수정
참조되지 않은 FabricPool 공간을 재확보하기 위한 임계값을 표시합니다	고급 권한 수준에서 '-unrecla재확보된-공간-임계값' 매개 변수를 사용하는 '스토리지 집계 객체 저장소 표시' 또는 '저장소 집계 오브젝트 저장소 표시 공간' 명령

관련 정보

- "저장소 집계 수정"
- "저장 집계 객체"
- "저장 집합 쇼 공간"

SVM 데이터 이동성

ONTAP SVM 데이터 이동성에 대해 알아보세요

ONTAP 9.10.1부터 클러스터 관리자는 용량 및 부하 분산을 관리하거나 장비 업그레이드 또는 데이터 센터 통합을 지원하기 위해 소스 클러스터에서 대상 클러스터로 SVM을 중단 없이 이전할 수 있습니다.

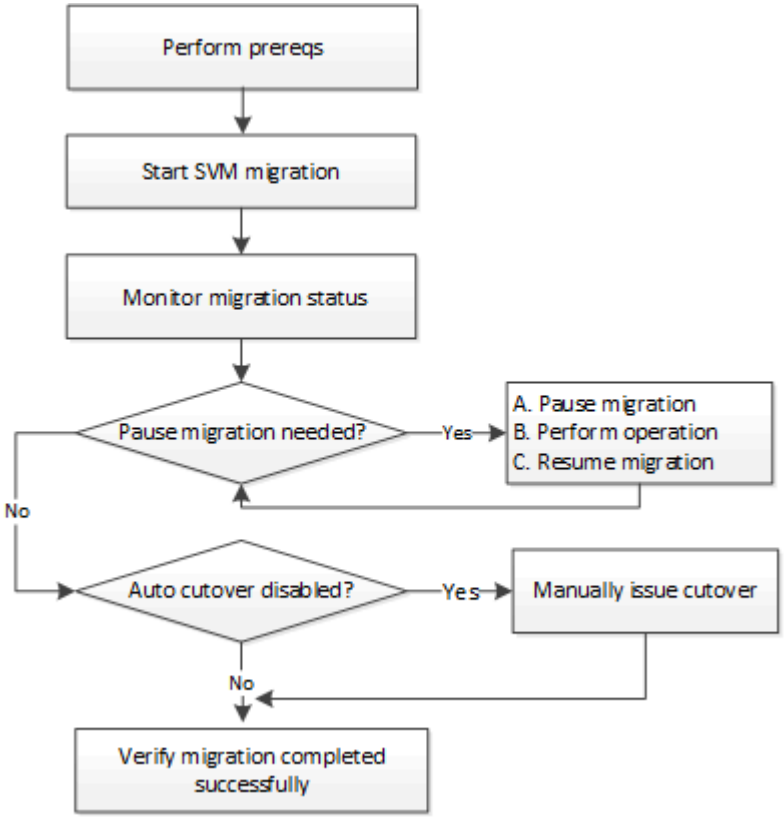
비중단 SVM 재배치는 ONTAP 9.10.1 및 9.11.1의 AFF 시스템에서 지원됩니다. ONTAP 9.12.1부터 이 기능은 FAS 및 AFF 시스템과 하이브리드 집계에서 모두 지원됩니다.

마이그레이션 후에도 SVM의 이름과 UUID는 변경되지 않으며 데이터 LIF 이름, IP 주소, 볼륨 이름과 같은 개체 이름도 그대로 유지됩니다. SVM에서 개체의 UUID는 다릅니다.

ONTAP 9.18.1부터 ASA 스토리지 시스템에서 ASA r2 스토리지 시스템으로의 SVM 마이그레이션이 지원됩니다. ASA r2 스토리지 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있고 ASA 시스템에서 ASA r2 시스템으로 SVM을 마이그레이션하려는 경우 다음을 따르세요."수행할 수 있습니다" .

SVM 마이그레이션 워크플로우

이 다이어그램은 SVM 마이그레이션을 위한 일반적인 워크플로우를 보여 줍니다. 대상 클러스터에서 SVM 마이그레이션을 시작합니다. 소스 또는 대상에서 마이그레이션을 모니터링할 수 있습니다. 수동 컷오버나 자동 컷오버를 수행할 수 있습니다. 자동 컷오버는 기본적으로 수행됩니다.



SVM 마이그레이션 시스템 지원

컨트롤러 제품군	ONTAP 버전이 지원됩니다
ASA	ONTAP 9.18.1 이상 팔로우"수행할 수 있습니다" ASA에서 ASA r2 시스템으로 SVM 마이그레이션을 위해.
AFF C-시리즈	ONTAP 9.12.1 패치 4 이상
FAS	ONTAP 9.12.1 이상
AFF A-시리즈	ONTAP 9.10.1 이상

하이브리드 집계를 사용하여 AFF 클러스터에서 FAS 클러스터로 마이그레이션할 때 자동 볼륨 배치는 유사 간 집계 일치를 시도합니다. 예를 들어, 소스 클러스터에 60개의 볼륨이 있는 경우 볼륨 배치는 볼륨을 배치하기 위해 대상에서 AFF 집계를 찾으려고 시도합니다. AFF 집계에 충분한 공간이 없는 경우 볼륨은 플래시 디스크가 아닌 집계에 배치됩니다.

ONTAP 버전별 확장성 지원

ONTAP 버전입니다	소스와 대상의 HA 쌍
ONTAP 9.14.1 이상	12
ONTAP 9.13.1	6
ONTAP 9.11.1	3
ONTAP 9.10.1	1

소스와 대상 클러스터 간의 **TCP RTT(Round Trip Time)**에 대한 네트워크 인프라스트럭처 성능 요구 사항

클러스터에 설치된 ONTAP 버전에 따라 소스 및 대상 클러스터를 연결하는 네트워크의 왕복 시간이 그림과 같이 최대값이어야 합니다.

ONTAP 버전입니다	최대 RTT
ONTAP 9.12.1 이상	10ms
ONTAP 9.11.1 이전 버전	2ms

SVM당 지원되는 최대 볼륨 수

혼합 또는 하이브리드 클러스터에서 SVM당 마이그레이션할 수 있는 볼륨의 최대 수는 더 적은 수의 볼륨을 지원하는 클러스터 멤버를 기준으로 합니다.

출처	목적지	ONTAP 9.14.1 이상	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1 이전 버전
AFF	AFF	400	200	100	100
FAS	FAS	80	80	80	해당 없음
FAS	AFF	80	80	80	해당 없음
AFF	FAS	80	80	80	해당 없음

필수 구성 요소

SVM 마이그레이션을 시작하기 전에 다음 사전 요구사항을 충족해야 합니다.

- 클러스터 관리자입니다.
- "소스 및 대상 클러스터는 서로 피어링됩니다.".
- 소스 및 대상 클러스터에는 SnapMirror 동기가 있습니다. "라이센스가 설치되었습니다". 이 라이센스는 다음에 포함됩니다. "ONTAP 1 을 참조하십시오".
- 소스 클러스터의 모든 노드는 ONTAP 9.10.1 이상을 실행합니다. 특정 ONTAP 어레이 컨트롤러 지원에 대해서는 다음을 참조하세요. "Hardware Universe".
- 소스 클러스터의 모든 노드는 동일한 ONTAP 버전을 실행합니다.
- 대상 클러스터의 모든 노드는 동일한 ONTAP 버전을 실행합니다.
- 대상 클러스터 ONTAP 버전은 소스 클러스터와 동일하거나 두 개 이상의 주요 최신 버전입니다.

- 소스 및 대상 클러스터는 데이터 LIF 액세스를 위해 동일한 IP 서브넷을 지원합니다.
- 소스 클러스터와 대상 클러스터 모두 마이그레이션할 모든 SVM의 네트워크에 액세스할 수 있는 인터페이스를 하나 이상 보유해야 합니다. 그렇지 않으면 마이그레이션 사전 검사가 실패합니다.
- 소스 SVM에는 다음보다 적은 것이 포함되어 있습니다. 릴리스에 대해 지원되는 최대 데이터 볼륨 수입니다.
- 목적지에 볼륨을 배치할 수 있는 충분한 공간이 있습니다.
- 소스 SVM에 암호화된 볼륨이 있는 경우 대상의 클러스터 수준에서 온보드 키 관리자 또는 외부 키 관리가 구성됩니다.
  - 이 경우 소스의 SVM 수준에서 구성된 키 관리자는 대상으로 마이그레이션되지 않습니다. 목적지는 클러스터 수준 키 관리자를 사용합니다.
- 소스에 암호화된 볼륨이 있고 NetApp Aggregate Encryption(NAE)에 대해 구성된 경우 대상도 NAE에 대해 구성해야 합니다.
- 비 MetroCluster 구성과 MetroCluster 구성 간 또는 두 MetroCluster 구성 간에 SVM을 마이그레이션할 경우, 구성이 다음 요구사항을 충족하는지 확인하십시오.

  MetroCluster 구성에서 로컬 클러스터와 파트너 클러스터 간에 SVM을 마이그레이션하는 것은 지원되지 않습니다.

  - 소스 및 대상 MetroCluster 클러스터가 "정상" 상태입니다. 즉, 전환 모드나 "전환 대기 중" 상태에 있을 수 없습니다.
  - 소스 및 대상 MetroCluster 클러스터는 FC-to-IP 전환 또는 하드웨어 교체 프로세스를 진행 중이 아닙니다.
  - 소스 클러스터와 대상 클러스터는 모두 ONTAP 9.16.1 이상을 실행해야 합니다.
  - 소스가 MetroCluster 클러스터인 경우 SVM 하위 유형은 "sync-source"("sync-destination" 아님)입니다.

    타겟이 MetroCluster 클러스터인 경우 타겟에 생성된 SVM은 항상 "sync-source"입니다. 타겟이 비 MetroCluster 클러스터인 경우 SVM 하위 유형은 항상 "기본값"입니다.

모범 사례

SVM 마이그레이션을 수행할 때 CPU 워크로드를 실행할 수 있도록 소스 클러스터와 타겟 클러스터 모두에 30%의 CPU 여유 공간을 두는 것이 모범 사례입니다.

SVM 운영

SVM 마이그레이션과 충돌할 수 있는 작업을 확인하세요.

- 진행 중인 페일오버 작업이 없습니다
- WAFLIRON을 실행할 수 없습니다
- 지문이 진행 중이 아닙니다
- Vol 이동, 리호스팅, 복제, 생성, 변환 또는 분석이 실행되지 않습니다.
- 대상 클러스터에서 SVM 마이그레이션이 실행되고 있지 않습니다. 한 번에 하나의 SVM 마이그레이션만 허용됩니다.

지원 및 지원되지 않는 기능입니다

이 표에는 SVM 데이터 이동성이 지원하는 ONTAP 기능과 지원을 이용할 수 있는 ONTAP 릴리즈가 나와 있습니다.

SVM 마이그레이션에서 소스와 대상 간의 ONTAP 버전 상호 운용성에 대한 자세한 내용은 를 참조하십시오 "SnapMirror 관계에 대한 호환 ONTAP 버전".

피처	첫 번째 릴리스가 지원됩니다	설명
감사 로그(NFS 및 SMB)	ONTAP 9.13.1	감사가 활성화된 온프레미스 SVM 마이그레이션의 경우 소스 SVM에 대한 감사를 비활성화한 다음 마이그레이션을 수행해야 합니다. SVM 마이그레이션 전: • "대상 클러스터에서 감사 로그를 활성화해야 합니다.". • "소스 SVM의 감사 로그 대상 경로를 대상 클러스터에 생성해야 합니다".
자율 랜섬웨어 보호	ONTAP 9.12.1	
클라우드 인스턴스	지원되지 않습니다	온프레미스 인스턴스에서 클라우드로 또는 클라우드에서 온프레미스 인스턴스로 SVM을 마이그레이션하는 것은 지원되지 않습니다.
Cloud Volumes ONTAP	지원되지 않습니다	
외부 키 관리자	ONTAP 9.11.1	
FabricPool	지원되지 않습니다	
팬아웃 관계(마이그레이션 소스에는 둘 이상의 대상이 있는 SnapMirror 소스 볼륨이 있음)	ONTAP 9.11.1	
FC SAN	지원되지 않습니다	
Flash Pool을 참조하십시오	ONTAP 9.12.1	
FlexCache 볼륨	지원되지 않습니다	
FlexGroup 볼륨	지원되지 않습니다	
IPsec 정책	지원되지 않습니다	

IPv6 LIF	지원되지 않습니다	
iSCSI SAN	지원되지 않습니다	
작업 스케줄 복제	ONTAP 9.11.1	ONTAP 9.10.1에서는 마이그레이션 중에 작업 일정이 복제되지 않으므로 대상에서 수동으로 생성해야 합니다. ONTAP 9.11.1부터는 마이그레이션 중에 소스에서 사용하는 작업 일정이 자동으로 복제됩니다.
로드 공유 미러	지원되지 않습니다	
MetroCluster SVM	ONTAP 9.16.1	ONTAP 9.16.1부터 다음 MetroCluster SVM 마이그레이션이 지원됩니다. • 비 MetroCluster 구성과 MetroCluster IP 구성 간에 SVM 마이그레이션 • 2개의 MetroCluster IP 구성 간에 SVM 마이그레이션 • MetroCluster FC 구성과 MetroCluster IP 구성 간에 SVM 마이그레이션 참고: SVM 마이그레이션을 지원하려면 소스 및 대상 클러스터가 모두 ONTAP 9.16.1 이상을 실행해야 합니다. 다음 MetroCluster SVM 마이그레이션은 일부 ONTAP 버전에 대해 지원되지 않습니다. • 2개의 MetroCluster FC 구성 간에 SVM 마이그레이션 • 비 MetroCluster 구성과 MetroCluster FC 구성 간에 SVM 마이그레이션 • 동일한 MetroCluster 구성에서 로컬 클러스터와 파트너 클러스터 간에 SVM을 마이그레이션합니다. 를 참조하십시오 전제 조건 MetroCluster 구성에서 SVM을 마이그레이션하는 방법.
NetApp 애그리게이트 암호화(NAE)	ONTAP 9.11.1	NAE 볼륨은 NAE 지원 대상에 배치되어야 합니다. NAE 대상을 사용할 수 없는 경우 마이그레이션 작업이 실패합니다.
NDMP 구성	지원되지 않습니다	
NetApp 볼륨 암호화(NVE)	ONTAP 9.10.1	NVE 볼륨은 대상의 NVE 볼륨으로 마이그레이션됩니다.
NFS v3, NFS v4.1 및 NFS v4.2	ONTAP 9.10.1	
NFS v4.0	ONTAP 9.12.1	

pNFS를 사용하는 NFSv4.1	ONTAP 9.14.1	
NVMe over Fabric을 참조하십시오	지원되지 않습니다	
소스 클러스터에서 일반 조건 모드가 활성화된 온보드 키 관리자(OKM	지원되지 않습니다	
ONTAP Select	지원되지 않습니다	ONTAP Select 인스턴스에서 SVM을 마이그레이션하는 것은 지원되지 않습니다.
Qtree	ONTAP 9.14.1	
할당량	ONTAP 9.14.1	
S3	지원되지 않습니다	
SMB 프로토콜	ONTAP 9.12.1 버전에서는 SMB1 프로토콜이 지원되지 않습니다.	SMB 마이그레이션은 중단을 초래하며 마이그레이션 후 클라이언트를 새로 고쳐야 합니다.
SnapMirror 클라우드 관계	ONTAP 9.12.1	ONTAP 9.12.1부터 SnapMirror 클라우드 관계를 사용하여 온프레미스 SVM을 마이그레이션할 경우 타겟 클러스터에 가 설치되어 있어야 "SnapMirror 클라우드 라이센스"하며, 클라우드로 미러링되는 볼륨의 용량 이동을 지원할 수 있는 충분한 용량이 있어야 합니다.
SnapMirror 비동기식 타겟	ONTAP 9.12.1	

SnapMirror 비동기식 소스	ONTAP 9.11.1	• 대부분의 마이그레이션 동안 FlexVol SnapMirror 관계에서도 정상적으로 전송을 계속할 수 있습니다. • 전환 중에 진행 중이던 모든 전송은 취소되고, 전환 중에 새로운 전송은 실패합니다. 마이그레이션이 완료될 때까지 다시 시작할 수 없습니다. • 마이그레이션 중에 취소되거나 누락된 예약된 전송은 마이그레이션이 완료된 후 자동으로 시작되지 않습니다. SnapMirror 소스가 마이그레이션되면 ONTAP에서 SnapMirror 업데이트가 수행될 때까지 마이그레이션 후에 볼륨이 삭제되지 않도록 합니다. 이는 마이그레이션된 SnapMirror 소스 볼륨에 대한 SnapMirror 관련 정보는 마이그레이션이 완료된 후와 첫 번째 업데이트가 완료된 후에만 사용할 수 있기 때문입니다.
SMTape 설정	지원되지 않습니다	
SnapLock	지원되지 않습니다	
SnapMirror 활성 동기화	지원되지 않습니다	
SnapMirror SVM 피어 관계	ONTAP 9.12.1	
SnapMirror SVM 재해 복구	지원되지 않습니다	
SnapMirror 동기식	지원되지 않습니다	
스냅샷 수	ONTAP 9.10.1	
변조 방지 스냅샷 잠금	ONTAP 9.14.1	변조 방지 스냅샷 잠금은 SnapLock와 동일하지 않습니다. SnapLock Enterprise 및 SnapLock Compliance는 지원되지 않습니다.
가상 IP LIF/BGP	지원되지 않습니다	
Virtual Storage Console 7.0 이상	지원되지 않습니다	
볼륨 클론	지원되지 않습니다	
브이스캔	지원되지 않습니다	Vscan 지원 SVM의 마이그레이션은 지원되지 않습니다.

vStorage	지원되지 않습니다	vStorage가 설정된 경우 마이그레이션이 허용되지 않습니다. 마이그레이션을 수행하려면 vStorage 옵션을 비활성화한 다음 마이그레이션이 완료된 후 다시 사용하도록 설정합니다.

마이그레이션 중 지원되는 작업

다음 표에는 마이그레이션 상태에 따라 마이그레이션 SVM 내에서 지원되는 볼륨 작업이 나와 있습니다.

볼륨 작업입니다	SVM 마이그레이션 상태		
	* 진행 중 *	* 일시 중지됨 *	* 컷오버 *
생성	허용되지 않습니다	허용됨	지원되지 않습니다
삭제	허용되지 않습니다	허용됨	지원되지 않습니다
File System Analytics가 해제되었습니다	허용됨	허용됨	지원되지 않습니다
File System Analytics가 설정되었습니다	허용되지 않습니다	허용됨	지원되지 않습니다
수정	허용됨	허용됨	지원되지 않습니다
오프라인/온라인	허용되지 않습니다	허용됨	지원되지 않습니다
이동/재호스팅	허용되지 않습니다	허용됨	지원되지 않습니다
Qtree 생성/수정	허용되지 않습니다	허용됨	지원되지 않습니다
할당량 생성/수정	허용되지 않습니다	허용됨	지원되지 않습니다
이름 바꾸기	허용되지 않습니다	허용됨	지원되지 않습니다
크기 조정	허용됨	허용됨	지원되지 않습니다
제한	허용되지 않습니다	허용됨	지원되지 않습니다
스냅샷 특성이 수정합니다	허용됨	허용됨	지원되지 않습니다
스냅샷 자동 삭제 수정	허용됨	허용됨	지원되지 않습니다
스냅샷 생성	허용됨	허용됨	지원되지 않습니다
스냅샷 삭제	허용됨	허용됨	지원되지 않습니다
스냅샷에서 파일을 복원합니다	허용됨	허용됨	지원되지 않습니다

이주 후 정보

- 마이그레이션 후 로컬 스냅샷 정책에 -MIG 확장자가 추가되어 일부 자동화 기능이 제대로 작동하지 않을 수 있습니다. 해당 확장 프로그램을 검색하고 정책 및 필요한 항목의 이름을 변경해야 합니다.
- 마이그레이션된 볼트 대상 SnapMirror 볼륨은 보호 기능을 다시 활성화하려면 재동기화를 수행해야 합니다. 마이그레이션 과정에서 마이그레이션 SVM 간에 이전 기준선보다 최신 기준선이 새로 생성되기 때문에 볼트 재동기화가 필요합니다. 재동기화를 수행하면 볼트가 다시 활성화되고, 현재 볼트 기준선보다 최신 데이터(특히 마이그레이션 중에 생성된 스냅샷)가 모두 삭제됩니다.

ONTAP SVM 마이그레이션

SVM 마이그레이션이 완료된 후 클라이언트가 타겟 클러스터로 자동으로 컷오버되고 불필요한

SVM이 소스 클러스터에서 제거됩니다. 자동 컷오버 및 자동 소스 클린업이 기본적으로 설정됩니다. 필요한 경우, 컷오버를 시작하기 전에 마이그레이션을 일시 중지하고 자동 소스 SVM 정리를 사용하지 않도록 설정할 수 있습니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요."수행할 수 있습니다" SVM을 마이그레이션하려면. ASA r2 시스템은 SAN 전용 고객에게 최적화된 간소화된 ONTAP 환경을 제공합니다.

- 자동 클라이언트 컷오버가 정상적으로 수행되는 경우 '-auto-cutover false' 옵션을 사용하여 마이그레이션을 일시 중지한 다음 나중에 수동으로 컷오버를 수행할 수 있습니다.

  SVM 마이그레이션 후 클라이언트 수동 컷오버

- advance privilege '-auto-source-cleanup false' 옵션을 사용하여 컷오버 이후 소스 SVM의 제거를 해제한 다음 나중에 컷오버를 통해 수동으로 소스 정리를 트리거할 수 있습니다.

  컷오버 이후 소스 SVM 수동 제거

자동 컷오버가 활성화된 **ONTAP SVM** 마이그레이션

기본적으로 마이그레이션은 완료되면 클라이언트가 대상 클러스터로 자동으로 컷오버되고 불필요한 SVM이 소스 클러스터에서 제거됩니다.

단계

1. 타겟 클러스터에서 사전 점검을 수행합니다.

   ```
   vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
   -check-only true`
   ```

2. 대상 클러스터에서 SVM 마이그레이션을 시작합니다.

   ```
   vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
   ```

3. 마이그레이션 상태 확인:

   ```
   vserver migrate show
   ```

   SVM 마이그레이션이 완료되면 상태가 Migrate-Complete로 표시됩니다.

자동 클라이언트 전환이 비활성화된 **ONTAP SVM** 마이그레이션

자동 클라이언트 컷오버가 정상적으로 수행되는 경우 -auto-cutover false 옵션을 사용하여 마이그레이션을 일시 중지한 다음 나중에 수동으로 컷오버를 수행할 수 있습니다. 을 참조하십시오 SVM 마이그레이션 후 클라이언트 수동 컷오버.

단계

1. 타겟 클러스터에서 사전 점검을 수행합니다.

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
-check-only true`
```

2. 대상 클러스터에서 SVM 마이그레이션을 시작합니다.

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
-auto-cutover false`
```

3. 마이그레이션 상태 확인:

```
vserver migrate show
```

SVM 마이그레이션이 비동기 데이터 전송을 완료하고 컷오버 작업을 수행할 준비가 되면 상태가 '컷오버 준비'로 표시됩니다.

소스 정리가 비활성화된 **ONTAP SVM** 마이그레이션

advance privilege-auto-source-cleanup false 옵션을 사용하여 컷오버 이후 소스 SVM의 제거를 해제한 다음 나중에 컷오버를 통해 소스 정리를 수동으로 트리거할 수 있습니다. 을 참조하십시오 소스 SVM을 수동으로 제거합니다.

단계

1. 타겟 클러스터에서 사전 점검을 수행합니다.

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
-check-only true`
```

2. 대상 클러스터에서 SVM 마이그레이션을 시작합니다.

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
-auto-source-cleanup false`
```

3. 마이그레이션 상태 확인:

```
vserver migrate show
```

상태는 SVM 마이그레이션 컷오버가 완료된 후 소스 클러스터에서의 SVM을 제거할 준비가 되면 소스 정리를 위해 준비됨으로 표시됩니다.

ONTAP 볼륨 마이그레이션 모니터링

'vserver migrate show' 명령을 사용하여 전체 SVM 마이그레이션을 모니터링하는 것 외에도 SVM에 포함된 볼륨의 마이그레이션 상태를 모니터링할 수 있습니다.

단계

1. 대상 클러스터에서 볼륨 마이그레이션 상태를 확인합니다.

```
vserver migrate show-volume
```

ONTAP SVM 마이그레이션 일시 중지 및 재개

마이그레이션 컷오버를 시작하기 전에 SVM 마이그레이션을 일시 중지할 수 있습니다. "vserver migrate pause" 명령을 사용하여 SVM 마이그레이션을 일시 중지할 수 있습니다.

마이그레이션을 일시 중지합니다

'vserver migrate pause' 명령을 사용하여 클라이언트 컷오버를 시작하기 전에 SVM 마이그레이션을 일시 중지할 수 있습니다.

일부 구성 변경은 마이그레이션 작업이 진행 중일 때 제한됩니다. 그러나 ONTAP 9.12.1부터는 마이그레이션을 일시 중지하여 일부 제한된 구성을 수정하고 일부 실패 상태에 대해 오류를 발생시킨 구성 문제를 해결할 수 있습니다. SVM 마이그레이션을 일시 중지할 때 수정할 수 있는 장애 상태는 다음과 같습니다.

- `setup-configuration-failed`
- `migrate-failed`

단계

1. 대상 클러스터에서 마이그레이션을 일시 중지합니다.

```
vserver migrate pause -vserver <vserver name>
```

마이그레이션을 다시 시작하십시오

일시 중지된 SVM 마이그레이션을 다시 시작할 준비가 되거나 SVM 마이그레이션에 장애가 발생한 경우 명령을 사용할 수 있습니다. `vserver migrate resume`

단계

1. 대상 클러스터에서 SVM 마이그레이션을 다시 시작합니다.

```
vserver migrate resume
```

2. SVM 마이그레이션이 재개되었는지 확인하고 진행률을 모니터링합니다.

```
vserver migrate show
```

ONTAP SVM 마이그레이션 취소

SVM 마이그레이션이 완료되기 전에 취소해야 하는 경우 다음을 사용할 수 있습니다. `vserver migrate abort` 명령. 작업이 일시 중지되거나 실패한 상태에서만 SVM 마이그레이션을 취소할 수 있습니다. 상태가 "전환 시작"이거나 전환이 완료된 후에는 SVM 마이그레이션을 취소할 수 없습니다. 당신은 사용할 수 없습니다 `abort` SVM 마이그레이션이 진행 중일 때의 옵션입니다.

단계

1. 대상 클러스터에서 마이그레이션 상태를 확인하세요.

```
vserver migrate show -vserver <SVM_name>
```

2. 마이그레이션 취소:

```
vserver migrate abort -vserver <SVM_name>
```

3. 취소 작업의 진행 상태를 점검한다.

```
vserver migrate show
```

취소 작업이 진행 중인 동안 마이그레이션 상태가 migrate-aborting으로 표시됩니다. 취소 작업이 완료되면 마이그레이션 상태가 아무것도 표시되지 않습니다.

ONTAP SVM 마이그레이션 후 클라이언트를 수동으로 컷오버합니다.

기본적으로, SVM 마이그레이션이 "컷오버를 위한 준비" 상태에 도달하면 타겟 클러스터로 전환하는 클라이언트가 자동으로 수행됩니다. 자동 클라이언트 컷오버를 사용하지 않도록 선택하는 경우 클라이언트 컷오버를 수동으로 수행해야 합니다.

단계

1. 클라이언트 컷오버를 수동으로 실행:

```
vserver migrate cutover -vserver <SVM_name>
```

2. 컷오버 작업의 상태를 점검한다.

```
vserver migrate show
```

클라이언트 전환 후 소스 **ONTAP SVM**을 수동으로 제거합니다**.**

소스 정리를 사용하지 않도록 설정한 상태에서 SVM 마이그레이션을 수행한 경우, 클라이언트 컷오버가 완료된 후 소스 SVM을 수동으로 제거할 수 있습니다.

단계

1. 소스 정리를 위해 상태가 준비되었는지 확인하세요.

```
vserver migrate show
```

2. 소스 정리:

```
vserver migrate source-cleanup -vserver <SVM_name>
```

HA 쌍 관리

ONTAP 클러스터에서 HA 쌍 관리에 대해 알아보세요

클러스터 노드는 장애 허용 및 중단 없는 운영을 위해 고가용성(HA) 쌍으로 구성됩니다. 노드에 장애가 발생하거나 정기적인 유지 관리를 위해 노드를 중단해야 하는 경우, 해당 파트너가 해당 노드의 스토리지를 인수하여 계속해서 데이터를 제공할 수 있습니다. 노드가 다시 온라인 상태가 되면 파트너는 스토리지를 돌려줍니다.

HA 쌍 컨트롤러 구성은 일치하는 스토리지 컨트롤러 쌍(로컬 노드와 파트너 노드)으로 구성됩니다. 각 노드는 다른 노드의 디스크 셸프에 연결됩니다. HA 쌍의 한 노드에서 오류가 발생하여 데이터 처리가 중단되면 해당 파트너는 파트너의 실패 상태를 감지하고 해당 컨트롤러에서 모든 데이터 처리를 인계받습니다.

_테이크오버는 노드가 파트너의 스토리지를 제어하는 프로세스입니다.

_Giveback_은 스토리지를 파트너에게 반환하는 프로세스입니다.

기본적으로 테이크오버는 다음과 같은 상황에서 자동으로 수행됩니다.

- 소프트웨어 또는 시스템 장애가 노드에서 발생하고 패닉이 발생합니다. HA 쌍 컨트롤러는 자동으로 해당 파트너 노드로 페일오버됩니다. 파트너가 패닉 상태에서 복구되고 부팅된 후에 노드가 자동으로 반환을 수행하고 파트너를 정상 운영으로 반환합니다.
- 노드에서 시스템 장애가 발생하고 노드를 재부팅할 수 없습니다. 예를 들어, 전원 손실로 인해 노드에 장애가 발생할 경우 HA 쌍 컨트롤러가 자동으로 파트너 노드로 페일오버되고 정상적인 스토리지 컨트롤러에서 데이터를 제공합니다.

노드의 스토리지 파워도 동시에 손실되면 표준 테이크오버가 가능하지 않습니다.

- 하트비트 메시지는 노드의 파트너로부터 수신되지 않습니다. 파트너가 하드웨어 또는 소프트웨어 장애(예: 상호 연결 장애)를 겪어 패닉이 발생하지 않지만 제대로 작동하지 않는 경우 이러한 문제가 발생할 수 있습니다.
- '-f' 또는 '-inhibit-takeover true' 매개 변수를 사용하지 않고 노드 중 하나를 중단시킵니다.

클러스터 HA가 활성화된 2노드 클러스터에서 '-inhibit-Takeover true' 매개변수를 사용하여 노드를 중단 또는 재부팅하면 먼저 클러스터 HA를 비활성화한 다음 온라인 상태를 유지할 노드에 epsilon을 할당하지 않는 한 두 노드가 데이터 제공을 중지합니다.

- '-INHIBIT-Takeover TRUE' 매개 변수를 사용하지 않고 노드 중 하나를 재부팅합니다. (Storage failover 명령의 '-ONBOOT' 매개변수는 기본적으로 설정되어 있습니다.)
- 원격 관리 장치(서비스 프로세서)가 파트너 노드의 장애를 감지합니다. 하드웨어 지원 테이크오버를 사용하지 않도록 설정한 경우에는 적용되지 않습니다.

'Storage failover' 명령을 사용하여 수동으로 테이크오버를 시작할 수도 있습니다.

ONTAP 9.18.1부터 HA 쌍 노드 간에 암호화된 통신을 구성할 수 있습니다. 자세한 내용은 다음을 참조하세요."ONTAP HA 트래픽에 대한 암호화 구성" .

클러스터 복원력 및 진단 기능 향상

ONTAP 9.9.1부터 다음과 같은 복원력과 진단 기능이 클러스터 작동을 향상시킵니다.

- * 포트 모니터링 및 방지 *: 스위치가 없는 2노드 클러스터 구성에서 시스템은 전체 패킷 손실(연결 손실)을 경험하는 포트를 방지합니다. ONTAP 9.8.1 이하에서는 스위치 구성에서만 이 기능을 사용할 수 있었습니다.
- 자동 노드 장애 조치: 노드가 클러스터 네트워크를 통해 데이터를 제공할 수 없는 경우 해당 노드가 디스크를 소유해서는 안 됩니다. 대신 파트너의 상태가 양호하면 HA 파트너가 대신 대신 맡아야 합니다.
- * 연결 문제를 분석하는 명령 *: 다음 명령을 사용하여 패킷 손실이 발생한 클러스터 경로를 표시합니다. `network interface check cluster-connectivity show`

  에 대한 자세한 내용은 `network interface check cluster-connectivity show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 클러스터에서 하드웨어 지원 인수에 대해 알아보세요

기본적으로 사용되는 하드웨어 지원 테이크오버 기능은 노드의 원격 관리 장치(서비스 프로세서)를 사용하여 인수 프로세스의 속도를 높일 수 있습니다.

원격 관리 장치에서 장애를 감지하면 ONTAP가 파트너의 하트비트가 중지되었음을 인식하기 위해 대기하지 않고 테이크오버가 신속하게 시작됩니다. 이 기능을 활성화하지 않고 오류가 발생하면 파트너는 노드가 하트비트를 더 이상 제공하지 않음을 확인하고 하트비트 손실을 확인한 다음 테이크오버 시작을 대기합니다.

하드웨어 지원 테이크오버 기능은 다음 프로세스를 사용하여 대기를 방지합니다.

1. 원격 관리 장치는 로컬 시스템에서 특정 유형의 오류를 모니터링합니다.
2. 오류가 감지되면 원격 관리 장치가 즉시 파트너 노드로 알림을 보냅니다.

3. 알림을 받으면 파트너가 테이크오버 시작

하드웨어 지원 테이크오버를 트리거하는 시스템 이벤트입니다

파트너 노드는 원격 관리 장치(서비스 프로세서)에서 수신하는 경고 유형에 따라 테이크오버 를 생성할 수 있습니다.

경고	인수 시 테이크오버가 시작됩니까?	설명
abnormal_reboot(비정상 재부팅	아니요	노드의 비정상적인 재부팅이 발생했습니다.
L2_Watchdog_reset입니다	예	시스템 감시 하드웨어가 L2 재설정을 감지했습니다. 원격 관리 장치가 시스템 CPU에서 응답이 없음을 감지하여 시스템을 재설정합니다.
Heartbeat 손실	아니요	원격 관리 장치가 노드에서 하트비트 메시지를 더 이상 수신하지 않습니다. 이 알림은 HA 쌍의 노드 간 하트비트 메시지를 의미하지 않으며, 노드와 로컬 원격 관리 디바이스 간의 하트비트를 나타냅니다.
PERIODIC_MESSAGE를	아니요	정상적인 하드웨어 지원 테이크오버 작동 중에 주기적으로 메시지가 전송됩니다.
power_cycle_via_sp	예	원격 관리 장치에서 시스템 전원을 껐다가 켰습니다.
POWER_Loss(전원 손실)	예	노드에서 전원 손실이 발생했습니다. 원격 관리 장치에는 전원 손실 후 잠시 동안 전원을 유지하는 전원 공급 장치가 있어 파트너에 전원 손실을 보고할 수 있습니다.
Power_off_via_SP를 선택합니다	예	원격 관리 장치에서 시스템 전원을 껐습니다.
VIA_SP를 재설정합니다	예	원격 관리 장치가 시스템을 재설정합니다.
테스트	아니요	하드웨어 지원 테이크오버 작동을 확인하기 위한 테스트 메시지가 전송됩니다.

관련 정보

"하드웨어 지원(HWassistant) 인수 - 해결 가이드 를 참조하십시오"

ONTAP 클러스터의 자동 인수 및 반환에 대해 알아보세요

자동 테이크오버 및 반환 작업이 함께 작동하여 클라이언트 중단을 줄이고 방지할 수 있습니다.

기본적으로 HA 쌍의 노드 중 하나가 패닉, 재부팅 또는 중지되면 파트너 노드가 자동으로 작업을 인계받은 다음 해당 노드가 재부팅될 때 스토리지를 반환합니다. 그런 다음 HA 쌍이 정상 운영 상태를 재개합니다.

노드 중 하나가 응답하지 않는 경우에도 자동 테이크오버가 발생할 수 있습니다.

자동 반환은 기본적으로 발생합니다. 반환이 클라이언트에 미치는 영향을 제어하려는 경우 자동 반환을 사용하지 않도록 설정하고 명령을 사용할 수 `storage failover modify -auto-giveback false -node <node>` 있습니다. 자동 기브백을 수행하기 전에(트리거된 항목에 관계없이) 파트너 노드는 명령의 매개 변수에 `storage failover modify` 의해 제어되는 고정 시간 동안 대기합니다. `-delay- seconds` 기본 지연은 600초입니다.

이 프로세스는 다음에 필요한 시간을 포함하여 장기간의 단일 중단을 방지합니다.

- 테이크오버 작동
- 반환이 준비가 된 시점까지 부트에 대해 인과된 노드
- 반환 작업

루트가 아닌 Aggregate에 대해 자동 반환이 실패하면 시스템에서 자동으로 반환 완료를 두 번 시도합니다.

> 테이크오버 프로세스 중에 파트너 노드가 기브백에 대비하기 전에 자동 반환 프로세스가 시작됩니다. 자동 반환 프로세스의 시간 제한이 만료되고 파트너 노드가 아직 준비되지 않은 경우 타이머가 다시 시작됩니다. 따라서 준비 중인 파트너 노드와 수행 중인 실제 반환 시간 사이의 시간이 자동 반환 시간보다 짧아질 수 있습니다.

테이크오버 중 발생하는 동작

파트너가 노드를 인수하면 파트너 애그리게이트와 볼륨의 데이터가 계속해서 제공 및 업데이트됩니다.

테이크오버 프로세스 중에 다음 단계가 발생합니다.

1. 협상된 테이크오버가 사용자 시작된 경우 통합된 데이터가 파트너 노드에서 테이크오버 수행 중인 노드로 이동됩니다. 루트 애그리게이트(루트 애그리게이트 제외)를 제외한 각 애그리게이트의 현재 소유자가 테이크오버 노드로 변경되면 간단한 운영 중단이 발생합니다. 이러한 운영 중단은 애그리게이트 재배치를 수행하지 않고 테이크오버 중에 발생하는 중단보다 더 짧은 시간에 수행됩니다.

   > 패닉이 발생하는 경우 패닉 중에 협상된 테이크오버가 발생할 수 없습니다. 테이크오버 발생하면 패닉이 발생하지 않는 고장이 발생할 수 있습니다. 노드와 파트너 간에 통신이 끊기면 장애가 발생하고 하트비트 손실이라고도 합니다. 장애로 인해 테이크오버가 발생하면 파트너 노드에서 하트비트 손실을 감지할 시간이 필요하므로 중단 시간이 더 길어질 수 있습니다.

   - 명령을 사용하여 진행 상황을 모니터링할 수 `storage failover show-takeover` 있습니다.
   - 이 테이크오버 인스턴스 중에 매개 변수를 명령과 함께 `storage failover takeover` 사용하면 애그리게이트 재배치를 방지할 수 `-bypass-optimization` 있습니다.

     계획된 테이크오버 작업 중에 애그리게이트를 순차적으로 재배치하여 클라이언트 운영 중단을 줄입니다. 애그리게이트 재배치를 무시할 경우 계획된 테이크오버 이벤트 중에 더 긴 클라이언트 중단이 발생합니다.

2. 사용자 시작 테이크오버가 협상된 테이크오버인 경우 타겟 노드가 정상적으로 종료되고 타겟 노드의 루트 애그리게이트와 첫 번째 단계에서 재배치되지 않은 애그리게이트가 테이크오버됩니다.
3. 데이터 LIF(논리 인터페이스): LIF 페일오버 규칙에 따라 타겟 노드에서 테이크오버 노드 또는 클러스터의 다른 노드로 마이그레이션합니다. 매개 변수를 명령과 함께 `storage failover takeover` 사용하면 LIF 마이그레이션을 방지할 수 `-skip-lif-migration` 있습니다. 사용자가 시작한 테이크오버의 경우 스토리지 테이크오버가 시작되기 전에 데이터 LIF가 마이그레이션됩니다. 패닉 또는 장애가 발생할 경우 구성에 따라 데이터 LIF를 스토리지와 함께 마이그레이션하거나 테이크오버가 완료된 후 마이그레이션할 수 있습니다.
4. 테이크오버가 발생하면 기존 SMB 세션의 연결이 끊어집니다.

   > SMB 프로토콜의 특성 때문에 모든 SMB 세션이 중단됩니다(Continuous Availability 속성 세트가 있는 공유에 연결된 SMB 3.0 세션은 제외). SMB 1.0 및 SMB 2.x 세션에서는 Takeover 이벤트 후에 열려 있는 파일 핸들을 다시 연결할 수 없습니다. 따라서 테이크오버가 중단되고 데이터 손실이 어느 정도 발생할 수 있습니다.

5. Continuous Availability 속성을 사용하도록 설정된 공유로 설정된 SMB 3.0 세션은 테이크오버 이벤트 후에 연결이 끊긴 공유에 다시 연결될 수 있습니다. 사이트에서 Microsoft Hyper-V에 대한 SMB 3.0 연결을 사용하고 연결된 공유에 대해 Continuous Availability 속성이 설정된 경우 테이크오버는 해당 세션에 대해 무중단 운영을 제공합니다.

테이크오버 수행 중인 노드가 패닉 상태인 경우 어떻게 됩니까

테이크오버 시작 후 60초 내에 Takeover를 수행하는 노드가 발생하면 다음 이벤트가 발생합니다.

- 패닉이 발생하는 노드가 재부팅됩니다.
- 재부팅 후 노드는 자체 복구 작업을 수행하며 더 이상 테이크오버 모드가 아닙니다.
- 페일오버가 비활성화되었습니다.
- 노드에서 여전히 일부 파트너 애그리게이트를 소유하고 있으면 스토리지 페일오버를 활성화한 후 'Storage Failover 반환' 명령을 사용하여 해당 애그리게이트를 파트너에게 반환합니다.

반환 중 발생하는 현상

문제가 해결되거나, 파트너 노드가 부팅될 때 또는 반환이 시작될 때 로컬 노드가 파트너 노드에 소유권을 반환합니다.

정상적인 반환 작업에서 다음 프로세스가 발생합니다. 이 토론에서는 노드 A가 노드 B를 인수했습니다 노드 B의 모든 문제가 해결되었으며 데이터 제공을 재개할 준비가 되었습니다.

1. 노드 B의 모든 문제가 해결되고 '반환 대기 중' 메시지가 표시됩니다
2. 반환 작업은 'storage failover 반환' 명령 또는 시스템이 구성된 경우 자동 반환에 의해 시작됩니다. 그러면 노드 B의 애그리게이트 및 볼륨 소유권이 노드 A에서 노드 B로 반환되는 프로세스가 시작됩니다
3. 노드 A는 루트 애그리게이트의 제어를 먼저 반환합니다.
4. 노드 B는 정상 작동 상태로 부팅하는 프로세스를 완료합니다.
5. 노드 B가 부팅 프로세스에서 루트가 아닌 애그리게이트를 수용할 수 있는 지점에 도달하면 노드 A는 반환이 완료될 때까지 한 번에 하나씩 다른 애그리게이트의 소유권을 반환합니다. 'storage failover show -반환' 명령을 사용하여 반환 진행률을 모니터링할 수 있습니다.

> 'storage failover show-반환' 명령은 스토리지 페일오버 반환 작업 중에 발생하는 모든 작업에 대한 정보를 표시하지 않습니다(또는 표시하지 않습니다). 'storage failover show' 명령을 사용하면 노드가 완전히 작동하고 테이크오버가 가능하며 반환이 완료된 경우와 같이 노드의 현재 페일오버 상태에 대한 추가 세부 정보를 표시할 수 있습니다.

   해당 애그리게이트에 대해 기브백이 완료된 후 각 애그리게이트의 I/O가 재개되어 전체 운영 중단 기간이 단축됩니다.

HA 정책과 그 영향이 **Takeover** 및 **Giveback**에 미치는 영향

ONTAP은 CFO(컨트롤러 페일오버) 및 SFO(스토리지 페일오버)의 HA 정책을 자동으로 Aggregate에 할당합니다. 이 정책은 애그리게이트 및 해당 볼륨에 대해 스토리지 페일오버 작업이 수행되는 방법을 결정합니다.

두 가지 옵션, CFO 및 SFO는 스토리지 페일오버 및 반환 작업 중에 ONTAP이 사용하는 애그리게이트 제어 시퀀스를 결정합니다.

CFO 및 SFO는 종종 비공식적으로 스토리지 페일오버(테이크오버 및 반환) 운영을 지칭하기 위해 사용되기도 하지만,

실제로는 Aggregate에 할당된 HA 정책을 나타냅니다. 예를 들어, SFO 애그리게이트 또는 CFO 애그리게이트는 단순히 애그리게이트의 HA 정책 할당을 참조하기만 하면 됩니다.

HA 정책은 다음과 같이 Takeover 및 Giveback 작업에 영향을 미칩니다.

- ONTAP 시스템에서 생성된 애그리게이트(루트 볼륨이 포함된 루트 애그리게이트 제외)에는 SFO의 HA 정책이 있습니다. 수동으로 시작된 테이크오버는 테이크오버 전에 SFO(비루트) 애그리게이트를 순차적으로 파트너에게 재배치함으로써 성능에 최적화되어 있습니다. 반환 프로세스 중에 애그리게이트는 페일오버된 시스템 부팅 후 순차적으로 다시 전달되고 관리 애플리케이션이 온라인 상태가 되어 노드가 애그리게이트를 받을 수 있게 됩니다.
- 애그리게이트 재배치 작업으로 인해 애그리게이트 디스크 소유권을 재할당하고 제어를 노드에서 파트너로 전환할 수 있기 때문에 SFO의 HA 정책이 적용된 애그리게이트만 애그리게이트 재배치할 수 있습니다.
- 루트 애그리게이트에는 항상 CFO의 HA 정책이 있고 반환 작업을 시작할 때 이 정책이 제공됩니다. 이는 가져온 시스템이 부팅되도록 하기 위해 필요합니다. 다른 모든 애그리게이트는 페일오버된 시스템이 부팅 프로세스를 완료하고 관리 애플리케이션이 온라인 상태가 된 이후에 순차적으로 다시 제공되므로 노드에서 애그리게이트를 받을 수 있습니다.

> 애그리게이트의 HA 정책을 SFO에서 CFO로 변경하는 것은 유지 관리 모드 작업입니다. 고객 지원 담당자의 지시가 없는 한 이 설정을 수정하지 마십시오.

백그라운드 업데이트가 **Takeover** 및 **Giveback**에 미치는 영향

디스크 펌웨어의 백그라운드 업데이트가 HA 쌍의 테이크오버, 반환 및 애그리게이트 재배치 작업에 영향을 미치는 것은 해당 작업의 시작 방식에 따라 다릅니다.

다음 목록에서는 백그라운드 디스크 펌웨어 업데이트가 테이크오버, 반환 및 애그리게이트 재배치에 미치는 영향을 설명합니다.

- 두 노드 중 하나의 디스크에서 백그라운드 디스크 펌웨어 업데이트가 발생하는 경우 수동으로 시작된 테이크오버 작업은 해당 디스크에서 디스크 펌웨어 업데이트가 완료될 때까지 지연됩니다. 백그라운드 디스크 펌웨어 업데이트가 120초 이상 걸리는 경우 Takeover 작업이 중단되고 디스크 펌웨어 업데이트가 완료된 후 수동으로 다시 시작해야 합니다. 명령의 매개 변수를 `storage failover takeover` 로 설정하여 `true` 테이크오버가 시작되면 `-bypass-optimization` 타겟 노드에서 발생하는 백그라운드 디스크 펌웨어 업데이트가 테이크오버에 영향을 미치지 않습니다.
- 소스(또는 테이크오버) 노드의 디스크에서 백그라운드 디스크 펌웨어 업데이트가 진행되고 있고 명령의 매개 변수를 `storage failover takeover` 로 `immediate` 설정하여 테이크오버가 수동으로 시작된 경우 테이크오버 `-options` 작업이 즉시 시작됩니다.
- 노드의 디스크에서 백그라운드 디스크 펌웨어 업데이트가 수행되고 IT 패닉이 발생하면 패닉이 발생한 노드의 테이크오버가 즉시 시작됩니다.
- 백그라운드 디스크 펌웨어 업데이트가 두 노드 중 하나의 디스크에서 발생하는 경우, 디스크 펌웨어 업데이트가 해당 디스크에서 완료될 때까지 데이터 애그리게이트의 기브백이 지연됩니다.
- 백그라운드 디스크 펌웨어 업데이트가 120초 이상 걸리는 경우 반환 작업이 중단되고 디스크 펌웨어 업데이트가 완료된 후 수동으로 다시 시작해야 합니다.
- 백그라운드 디스크 펌웨어 업데이트가 두 노드 중 하나의 디스크에서 발생하는 경우, 디스크 펌웨어 업데이트가 해당 디스크에서 완료될 때까지 애그리게이트 재배치 작업이 지연됩니다. 백그라운드 디스크 펌웨어 업데이트가 120초 이상 걸리는 경우, 애그리게이트 재배치 작업이 중단되고 디스크 펌웨어 업데이트가 완료된 후 수동으로 다시 시작해야 합니다. 'true'로 설정된 'Storage aggregate relocation' 명령의 '-override-destination-checks'로 애그리게이트 재배치를 시작한 경우, 대상 노드에서 백그라운드 디스크 펌웨어 업데이트가 애그리게이트 재배치에 영향을 미치지 않습니다.

관련 정보

- "저장소 집계 재배치"
- "스토리지 장애 조치 포기"
- "스토리지 장애 조치 수정"
- "스토리지 장애 조치 쇼-기브백"
- "스토리지 장애 조치 인수"

ONTAP 자동 인수 명령

자동 테이크오버 기능은 지원되는 모든 NetApp FAS, AFF, ASA 플랫폼에서 기본적으로 활성화됩니다. 파트너 노드가 재부팅, 패닉 또는 중지되었을 때 자동 테이크오버 발생하면 기본 동작과 제어를 변경해야 할 수 있습니다.

파트너 노드에서 테이크오버 발생 여부를 자동으로 수행하려는 경우…	이 명령 사용…
재부팅 또는 중지	'Storage failover modify-node nodename-onreboot true'
패닉	'스토리지 페일오버 수정 - 노드 노데나미 - on패닉 true'

테이크오버 기능이 비활성화된 경우 이메일 알림을 활성화하십시오

탈취 기능이 비활성화된 경우 프롬프트 알림을 받으려면 ""탈취 불가능" EMS 메시지에 대한 자동 이메일 알림을 사용하도록 시스템을 구성해야 합니다.

- 하 테이크오버임버전
- 하-테이크오버임로엠을 선택합니다
- 하 테이크오버임팩드드
- 하 테이크오버임팩싱크
- 하 테이크오버임팩IC
- 하 테이크오버ImpHotShelf
- A.테이크오버임NotDef

관련 정보

- "스토리지 장애 조치 수정"

ONTAP 자동 포기 명령

기본적으로 오프라인 노드가 다시 온라인 상태가 되면 테이크오버파트너 노드가 자동으로 스토리지를 다시 제공하여 고가용성 쌍 관계를 복원합니다. 대부분의 경우 이것은 바람직한 동작입니다. 예를 들어, 되돌리기 전에 테이크오버 원인을 조사하려는 경우 기본값이 아닌 설정의 상호 작용에 대해 알고 있어야 합니다.

원하는 작업	이 명령 사용…
반환 노드가 부팅되고, Giveback 대기 상태에 도달하고, Auto Giveback 기간이 만료되기 전에 지연이 발생하는 즉시 반환이 발생하도록 자동 반환 설정 기본 설정은 TRUE입니다.	'Storage failover modify-node_nodename_-auto-반환 true'
자동 반환 비활성화 기본 설정은 TRUE입니다. • 참고: * 이 매개 변수를 false로 설정하면 패닉 시 테이크오버 후 자동 반환이 비활성화되지 않습니다. 패닉 시 테이크오버 후 자동 반환은 ``auto-반환-after-패닉" 매개 변수를 false로 설정하여 비활성화해야 합니다.	'Storage failover modify-node_nodename_-auto-반환 false'
패닉 상태에서 테이크오버 후 자동 반환을 사용하지 않도록 설정합니다(이 설정은 기본적으로 활성화됨).	'Storage failover modify-node_nodename_-auto-반환-after-panic false'
지정된 시간(초) 동안 자동 반환 지연(기본값 600) 이 옵션은 자동 반환을 수행하기 전에 노드가 테이크오버 상태로 유지되는 최소 시간을 결정합니다.	'Storage failover modify-node_nodename_-delay -seconds_seconds_'

스토리지 페일오버 수정 명령의 변화가 자동 반환에 미치는 영향

자동 반환 작업은 스토리지 페일오버 수정 명령의 매개 변수를 구성하는 방법에 따라 달라집니다.

다음 표에는 패닉이 발생하지 않는 테이크오버 이벤트에 적용되는 '스토리지 페일오버 수정' 명령 매개 변수의 기본 설정이 나와 있습니다.

매개 변수	기본 설정
'-auto-반환_true_	*false*'
'*TRUE*'	'-delay-seconds_integer_(초)'
600	'-onreboot_true_
false'	'*TRUE*'

다음 표에서는 '-onreboot' 및 '-auto-반환' 매개 변수의 조합이 패닉으로 인해 발생하지 않은 테이크오버 이벤트의 자동 반환에 미치는 영향을 설명합니다.

'스토리지 페일오버 수정' 매개 변수가 사용됩니다	테이크오버 원인	자동 반환이 발생합니까?

'-onreboot_true_' '-auto-반환_true_'	reboot 명령	예
서비스 프로세서에서 실행된 중지 명령 또는 전원 사이클 작업입니다	예	'-onreboot_true_' '-auto-반환_false_'
reboot 명령	예	서비스 프로세서에서 실행된 중지 명령 또는 전원 사이클 작업입니다
아니요	'-onreboot_false_' '-auto-반환_true_'	reboot 명령
해당 없음 이 경우 테이크오버 발생하지 않습니다	서비스 프로세서에서 실행된 중지 명령 또는 전원 사이클 작업입니다	예
'-onreboot_false_' '-auto-반환_false_'	reboot 명령	아니요

'-auto-반환' 매개 변수는 패닉 후 반환과 다른 모든 자동 테이크오버 후 반환을 제어합니다. 만약 `-onreboot' 매개변수가 'true'로 설정되어 있고 재부팅으로 인해 테이크오버가 발생하는 경우 '-auto-반환' 매개 변수가 'true'로 설정되었는지 여부에 상관없이 자동 반환이 항상 수행됩니다.

'-onreboot' 매개 변수는 ONTAP에서 실행된 재부팅 및 중지 명령에 적용됩니다. `-onreboot' 매개 변수가 false로 설정되면 노드 재부팅의 경우 테이크오버가 발생하지 않습니다. 따라서 '-auto-반환' 매개 변수가 true로 설정되었는지 여부에 관계없이 자동 반환이 발생할 수 없습니다. 클라이언트 중단이 발생합니다.

패닉 상황에 적용되는 자동 반환 매개 변수 조합의 효과

다음 표에는 패닉 상황에 적용되는 '스토리지 페일오버 수정' 명령 매개 변수가 나와 있습니다.

매개 변수	기본 설정
'-onpanic_true	false_'
'*TRUE*'	'-auto-반환-after-panic_true
false_' (권한: 고급)	'*TRUE*'
'-auto-반환_true	false_'

다음 표에서는 '스토리지 페일오버 수정' 명령의 매개 변수 조합이 패닉 상황에서 자동 반환에 미치는 영향에 대해 설명합니다.

'스토리지 페일오버' 매개 변수가 사용됩니다	패닉 후 자동 반환이 발생합니까?

`-onpanic true '-auto-반환 true '-auto-반환-after-panic true'	예
`-on패닉 true '-auto-반환 true '-auto-반환-after-panic false'	예
`-on패닉 true '- auto-반환 false '- auto-반환-after-panic true'	예
'-on패닉 true'- 자동 반환 false'- 자동 반환 -패닉 후 false	아니요
'-on패닉 false' -onpanic이 false로 설정되어 있으면 '-auto-반환' 또는 '-auto-반환-after-패닉'에 설정된 값에 관계없이 Takeover/Giveback이 수행되지 않습니다	아니요

테이크오버 발생하면 패닉이 발생하지 않는 고장이 발생할 수 있습니다. 노드 및 해당 파트너 간의 통신이 끊길 때 _FAILURE_가 발생합니다(또는 _HEARTBEAT Loss_라고도 함). 테이크오버 장애로 인해 발생하는 경우 반환은 에 의해 제어됩니다 `-onfailure` 매개 변수 대신 를 사용합니다 `-auto -giveback-after-panic parameter`.

노드에서 패닉이 발생할 경우 패닉 패킷이 파트너 노드로 전송됩니다. 어떤 이유로든 파트너 노드에서 패닉 패킷을 수신하지 못하면 패닉이 오류로 잘못 해석될 수 있습니다. 패닉 패킷을 받지 않으면 파트너 노드는 통신이 끊어졌다는 것만 알고 패닉 상태가 발생했음을 알지 못합니다. 이 경우 파트너 노드는 장애가 아니라 장애가 발생한 통신을 처리하며 Giveback은 에 의해 제어됩니다 `-onfailure` 매개 변수(에 의해 아님) `-auto-giveback-after-panic parameter`)를 클릭합니다.

에 대한 자세한 내용은 `storage failover modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 수동 인수 명령

파트너의 유지 관리가 필요한 상황이나 기타 유사한 상황에서 수동으로 테이크오버 수행 가능 파트너 상태에 따라 테이크오버 수행에 사용하는 명령이 달라집니다.

원하는 작업	이 명령 사용…
파트너 노드를 인수합니다	스토리지 페일오버 인수
파트너 애그리게이트가 테이크오버 실행 노드로 이동될 때 테이크오버 진행 상황을 모니터링합니다	'스토리지 페일오버 표시 - 테이크오버
클러스터의 모든 노드에 대한 스토리지 페일오버 상태를 표시합니다	'스토리지 페일오버 쇼'
LIF를 마이그레이션하지 않고 파트너 노드를 테이크오버합니다	'Storage failover takeover-skip-lif-migration-before -takeover true'
디스크 불일치가 있더라도 파트너 노드를 인수하십시오	`storage failover takeover -allow-disk -inventory-mismatch true`
ONTAP 버전이 일치하지 않더라도 파트너 노드를 인수하십시오. * 참고: * 이 옵션은 무중단 ONTAP 업그레이드 프로세스 중에만 사용됩니다.	'Storage failover takeover-option allow-version -mismatch'를 참조하십시오
애그리게이트 재배치를 수행하지 않고 파트너 노드를 인수합니다	'스토리지 페일오버 테이크오버가 무시가 최적화 true'입니다
파트너가 스토리지 리소스를 올바르게 종료할 시간이 되기 전에 파트너 노드를 테이크오버합니다	'스토리지 페일오버 테이크오버옵션 즉시

즉시 옵션을 사용하여 스토리지 페일오버 명령을 실행하기 전에 'network interface migrate -all -node_node_' 명령을 사용하여 데이터 LIF를 다른 노드로 마이그레이션해야 합니다

에 대한 자세한 내용은 `network interface migrate-all` "ONTAP 명령 참조입니다"을 참조하십시오.

데이터 LIF를 먼저 마이그레이션하지 않고 '스토리지 페일오버 테이크오버하기 옵션 즉시' 명령을 지정하면 'ip-lif-migration-before-Takeover' 옵션을 지정하지 않아도 노드에서 데이터 LIF 마이그레이션이 크게 지연됩니다.

마찬가지로 즉시 옵션을 지정하면 바이패스 최적화 옵션이 _false_로 설정되어 있어도 협상된 테이크오버 최적화가 무시됩니다.

수동으로 시작된 특정 테이크오버에 대한 **epsilon** 이동

수동으로 시작된 테이크오버로 인해 스토리지 시스템에서 예기치 않은 노드 장애가 발생할 수 있으므로 클러스터 전체의 쿼럼 손실로 인한 손실이 발생할 수 있다고 생각되면 epsilon을 이동해야 합니다.

이 작업에 대해

계획된 유지 관리를 수행하려면 HA 쌍 중 하나를 페일오버해야 합니다. 나머지 노드에 대해 계획되지 않은 클라이언트 데이터 중단을 방지하기 위해 클러스터 전체 쿼럼을 유지해야 합니다. 경우에 따라 Takeover를 수행하면 클러스터 전체의 쿼럼 손실에서 예기치 않은 노드 장애 1개가 발생하는 클러스터를 생성할 수 있습니다.

이 문제는 인수되는 노드가 epsilon을 보유하고 있거나 epsilon이 있는 노드가 정상이 아닌 경우 발생할 수 있습니다. 보다 탄력적인 클러스터를 유지하기 위해 epsilon을 인수되지 않은 정상 노드로 전송할 수 있습니다. 일반적으로 HA 파트너가 될 것입니다.

정상 및 자격을 갖춘 노드만 쿼럼 투표에 참여합니다. 클러스터 전체 쿼럼을 유지하려면 N/2 이상의 표가 필요합니다. 여기서 _N_은 자격이 있는 정상 온라인 노드의 합을 나타냅니다. 온라인 노드의 수가 짝수인 클러스터에서 epsilon은 할당된 노드에 대한 쿼럼을 유지 관리하기 위해 추가 투표 가중치를 추가합니다.

'cluster modify -eligibility false' 명령을 사용하여 클러스터 형성 투표를 수정할 수 있지만 노드 구성 복원이나 노드 유지 보수 연장 같은 상황을 제외하고는 이러한 상황을 피해야 합니다. 노드를 부적격 노드로 설정한 경우 노드가 적격으로 재설정되고 재부팅될 때까지 SAN 데이터 제공을 중단합니다. 노드에 대한 NAS 데이터 액세스는 노드가 부적격 상태일 때도 영향을 받을 수 있습니다.

단계

1. 클러스터 상태를 확인하고 epsilon이 인수되지 않은 정상 노드에 보관되어 있는지 확인합니다.

   a. 고급 권한 수준으로 변경하여 고급 모드 프롬프트가 나타나면 계속 진행할지 확인합니다(*>).

      세트 프리빌리지 고급

   b. 어떤 노드에 epsilon가 있는지 확인합니다.

      '클러스터 쇼'

      다음 예제에서 Node1은 epsilon을 보유합니다.

노드	상태	자격	Epsilon의

노드1 노드2	참입니다	참입니다	참 거짓

인수하려는 노드에 epsilon이 없는 경우 4단계를 진행합니다.

에 대한 자세한 내용은 `cluster show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 인수하려는 노드에서 epsilon을 제거합니다.

   'cluster modify-node Node1-epsilon FALSE'

3. 파트너 노드에 epsilon 할당(이 예에서는 Node2):

   'cluster modify-node Node2-epsilon TRUE'

4. 테이크오버 작업 수행:

   'storage failover takeover-ofnode_name_'

5. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

관련 정보

- "스토리지 장애 조치 표시"
- "스토리지 장애 조치 인수"

ONTAP 수동 포기 명령

정상적인 반환, 파트너 노드에서 프로세스를 종료하는 반환 또는 강제 반환을 수행할 수 있습니다.

기브백을 수행하기 전에 에 설명된 대로 페일오버된 시스템에서 장애가 발생한 드라이브를 제거해야 합니다 "디스크 및 애그리게이트 관리".

반환이 중단된 경우

반환 프로세스 중 테이크오버 노드에 장애 또는 정전이 발생하는 경우 해당 프로세스가 중지되고 테이크오버 노드가 테이크오버 모드로 되돌아가 장애가 복구되거나 전원이 복원됩니다.

그러나 오류가 발생한 반환 단계에 따라 다릅니다. 루트 애그리게이트를 반환한 후 부분 반환 상태 중에 노드에서 장애가 발생하거나 정전이 발생한 경우 테이크오버 모드로 돌아오지 않습니다. 대신 노드가 부분 반환 모드로 돌아갑니다. 이 경우 반환 작업을 반복하여 프로세스를 완료합니다.

Giveback에 거부되는 경우

기브백이 거부되면 EMS 메시지를 점검하여 원인을 확인해야 합니다. 이유나 이유에 따라, 거부권을 안전하게 무시할 수 있는지 여부를 결정할 수 있습니다.

'Storage failover show-반환' 명령은 반환 진행률을 표시하고 반환에 거부된 하위 시스템이 있는 경우 이를 표시합니다.

소프트 베인을 무시할 수 있지만, 하드 베인을 강제해도 무시할 수 없습니다. 다음 표에는 재지정할 수 없는 소프트 베트레인이 권장 해결 방법과 함께 요약되어 있습니다.

다음 명령을 사용하여 반환 거부의 EMS 세부 정보를 검토할 수 있습니다.

'이벤트 로그 show-node * -event gb *'

에 대한 자세한 내용은 `event log show` "ONTAP 명령 참조입니다"을 참조하십시오.

루트 애그리게이트의 반환

이러한 거부는 집계 재배치 작업에 적용되지 않습니다.

하위 시스템 모듈을 확인합니다	해결 방법
vFiler_low_level입니다	거부권을 유발한 SMB 세션을 종료하거나, 열려 있는 세션을 설정한 SMB 애플리케이션을 종료합니다. 이 거부권을 무시하면 SMB를 사용하는 응용 프로그램이 갑자기 연결을 끊고 데이터를 잃게 될 수 있습니다.
디스크 검사	반환하기 전에 모든 오류 또는 바이패스된 디스크를 제거해야 합니다. 디스크가 삭제 중이면 작업이 완료될 때까지 기다려야 합니다. 이 거부권을 덮어쓰면 예약 충돌 또는 액세스할 수 없는 디스크로 인해 애그리게이트 또는 볼륨이 오프라인 상태가 되어 정전이 발생할 수 있습니다.

SFO 애그리게이트의 반환

이러한 거부는 집계 재배치 작업에 적용되지 않습니다.

하위 시스템 모듈을 확인합니다	해결 방법
잠금 관리자	열린 파일이 있는 SMB 애플리케이션을 우아하게 종료하거나 이러한 볼륨을 다른 애그리게이트로 이동하십시오. 이 거부권을 무시하면 SMB 잠금 상태가 손실되어 중단 및 데이터 손실이 발생합니다.
매니저 NDO 잠금	잠금이 미러링될 때까지 기다립니다. 이 거부권을 무시하면 Microsoft Hyper-V 가상 시스템이 중단됩니다.

RAID	EMS 메시지를 확인하여 거부의 원인을 파악합니다. nvfile로 인해 거부권을 행사하는 경우 오프라인 볼륨과 애그리게이트를 온라인으로 전환합니다. 디스크 추가 또는 디스크 소유권 재할당 작업이 진행 중인 경우 완료될 때까지 기다립니다. 거부권이 애그리게이트 이름 또는 UUID 충돌로 인해 발생한 경우 문제를 해결하고 해결합니다. 거부권이 미러 재동기화, 미러 확인 또는 오프라인 디스크에 의한 것이라면 거부권을 무효화할 수 있으며 반환 후 작업이 다시 시작됩니다.
디스크 인벤토리	문제 해결을 통해 문제의 원인을 파악하고 해결합니다. 대상 노드에서 마이그레이션 중인 애그리게이트에 속한 디스크를 볼 수 없습니다. 액세스할 수 없는 디스크로 인해 애그리게이트 또는 볼륨에 액세스할 수 없습니다.
볼륨 이동 작업	문제 해결을 통해 문제의 원인을 파악하고 해결합니다. 이 거부권은 중요한 컷오버 단계에서 볼륨 이동 작업이 중단되는 것을 방지합니다. 컷오버 중에 작업이 중단되면 볼륨에 액세스할 수 없게 될 수 있습니다.

수동 반환을 수행하기 위한 명령입니다

유지 관리를 완료하거나 테이크오버 발생하는 문제를 해결한 후 HA 쌍의 노드에서 반환을 수동으로 시작하여 스토리지를 원래 소유자에게 반환할 수 있습니다.

원하는 작업	이 명령 사용…
스토리지를 파트너 노드로 다시 제공합니다	'Storage failover 반환-ofnode_nodename_'
파트너가 반환 모드를 대기 중인 상태가 아닌 경우에도 스토리지를 제공합니다	'Storage failover sofnode_nodename_"-Require -PARTNER-waiting false' 더 긴 클라이언트 중단을 허용할 수 없는 한 이 옵션을 사용하지 마십시오.
프로세스가 반환 작업을 거부하더라도 스토리지를 반환(강제 반환)	'Storage failover votmover-ofnode_nodename_" -override-vetoes true 이 옵션을 사용하면 클라이언트 중단 시간이 길어지거나, 반환 후 애그리게이트와 볼륨이 온라인으로 전환되지 않을 수 있습니다.

CFO 애그리게이트(루트 애그리게이트)만 돌려줍니다.	'Storage failover 반환-ofnode_nodename_' ``유일한 CFO"는 진실이라고 말했습니다
반환 명령을 실행한 후 반환 진행률을 모니터링합니다	'Storage failover show-반환'을 참조하십시오

관련 정보

- "스토리지 장애 조치 포기"
- "스토리지 장애 조치 쇼-기브백"

ONTAP 클러스터에서 인수 및 반환 테스트

HA 쌍의 모든 측면을 구성한 후에는 Takeover 및 Giveback 작업 시 두 노드의 스토리지에 중단 없이 액세스할 수 있도록 HA 쌍이 예상대로 작동하는지 확인해야 합니다. 테이크오버 프로세스 내내 로컬(또는 테이크오버) 노드가 파트너 노드가 일반적으로 제공하는 데이터를 계속 제공해야 합니다. 반환 시 파트너 스토리지의 제어 및 제공이 파트너 노드로 반환되어야 합니다.

단계

1. HA 인터커넥트 케이블의 케이블이 단단히 연결되었는지 확인합니다.
2. 라이센스가 있는 각 프로토콜에 대해 두 노드에서 파일을 생성하고 검색할 수 있는지 확인합니다.
3. 다음 명령을 입력합니다.

   'Storage failover-ofnode partnernode'

   에 대한 자세한 내용은 `storage failover takeover` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 다음 명령 중 하나를 입력하여 테이크오버 발생 여부를 확인합니다.

   '스토리지 페일오버 표시-테이크오버

   '스토리지 페일오버 쇼'

   '스토리지 페일오버' 명령의 '-auto-반환' 옵션이 활성화된 경우:

노드	파트너	테이크오버가 가능합니다	상태 설명
노드 1	노드 2	-	반환을 기다리는 중입니다
노드 2	노드 1	거짓	테이크오버 중 자동 반환이 몇 초 만에 시작됩니다

   '스토리지 페일오버' 명령의 '-auto-반환' 옵션이 비활성화되어 있는 경우:

노드	파트너	테이크오버가 가능합니다	상태 설명
노드 1	노드 2	-	반환을 기다리는 중입니다
노드 2	노드 1	거짓	제공합니다

5. 인수 노드(Node1)에서 검색할 수 있는 파트너 노드(Node2)에 속한 모든 디스크를 표시합니다.

   'Storage disk show-home node2-ownership'을 선택합니다

   다음 명령을 실행하면 Node1이 검색할 수 있는 Node2에 속하는 모든 디스크가 표시됩니다. "cluster:::> storage disk show-home node2-ownership"

디스크	집계	홈	소유자	DR 홈	홈 ID입니다	소유자 ID입니다	DR 홈 ID입니다	예비 장치	수영장
1.0.2	-	노드2	노드2	-	4078312453	4078312453	-	4078312452	수영장 0
1.0.3	-	노드2	노드2	-	4078312453	4078312453	-	4078312452	수영장 0

6. 인수 노드(Node1)에서 파트너 노드(Node2) 애그리게이트를 제어하는지 확인합니다.

   'aggr show-fields home-id, home-name'은 집입니다

집계	홈 ID입니다	홈 - 이름	홈입니다
aggr0_1	2014942045	노드1	참
aggr0_2	4078312453	노드2	거짓
aggr1_1	2014942045	노드1	참
aggr1_2	4078312453	노드2	거짓

   테이크오버 중에 파트너 노드 애그리게이트의 "홈" 가치는 FALSE입니다.

7. ""반환 대기 중" 메시지가 표시된 후 파트너 노드의 데이터 서비스를 다시 제공합니다.

   '스토리지 페일오버 기브백 - 노드 파트너십'

8. 반환 작업의 진행률을 확인하려면 다음 명령 중 하나를 입력합니다.

   'Storage failover show-반환'을 참조하십시오

   '스토리지 페일오버 쇼'

9. 반환이 성공적으로 완료되었다는 메시지를 보았는지 여부에 따라 다음 단계를 진행하십시오.

Takeover와 Giveback 중…	그러면…
성공적으로 완료되었습니다	파트너 노드에서 2단계부터 8단계까지 반복합니다.
실패	테이크오버 또는 반환 장애를 수정한 후 이 절차를 반복하십시오.

관련 정보

- "저장 디스크 표시"
- "스토리지 장애 조치 포기"
- "스토리지 장애 조치 표시"
- "스토리지 장애 조치 쇼-기브백"

HA 쌍 모니터링을 위한 ONTAP 명령

ONTAP 명령을 사용하여 HA 쌍의 상태를 모니터링할 수 있습니다. Takeover가 발생하는 경우 Takeover의 원인도 파악할 수 있습니다.

확인합니다	이 명령을 사용합니다
장애 조치가 설정되었는지 또는 발생했는지 여부 또는 장애 조치가 현재 가능하지 않은 이유	'스토리지 페일오버 쇼'
스토리지 페일오버 HA-모드 설정이 활성화된 노드를 확인합니다 노드가 스토리지 페일오버(HA 쌍) 구성에 참여하려면 이 값을 ha로 설정해야 합니다.	'스토리지 페일오버 표시 필드 모드'
하드웨어 지원 테이크오버가 설정되었는지 여부	스토리지 페일오버 hwassist show
발생한 하드웨어 지원 테이크오버 이벤트의 기록	스토리지 페일오버 hwassist 통계 표시
파트너의 애그리게이트가 테이크오버 실행 노드로 이동될 때 테이크오버 작업의 진행률이	'스토리지 페일오버 표시 - 테이크오버
파트너 노드로 애그리게이트를 반환하는 반환 반환 작업의 진행률	'Storage failover show-반환'을 참조하십시오
Takeover 또는 Giveback 작업 중 Aggregate가 홈인지 여부	'집계 표시 필드 홈 ID, 소유자 ID, 집 이름, 소유자 이름'은 집입니다
클러스터 HA 설정 여부(2노드 클러스터에만 적용)	군산쇼
HA Pair의 구성 요소(HA 상태를 사용하는 시스템에서)의 HA 상태	ha-config show 이것은 유지 관리 모드 명령이다.

스토리지 페일오버 **show-type** 명령으로 표시되는 노드 상태입니다

다음 목록은 'Storage failover show' 명령이 표시되는 노드에 대해 설명합니다.

노드 상태	설명
PARTNER_NAME에 연결되었고 자동 테이크오버 비활성화됨	HA 인터커넥트는 활성 상태이며 데이터를 파트너 노드로 전송할 수 있습니다. 파트너의 자동 테이크오버 기능이 해제됩니다.

partner_name, Giveback of partner spare 디스크를 기다리는 중입니다.	로컬 노드는 HA 인터커넥트를 통해 파트너 노드와 정보를 교환할 수 없습니다. 파트너에 대한 SFO 애그리게이트의 기브백이 완료되지만 파트너 스페어 디스크는 로컬 노드가 소유합니다. • 자세한 내용은 'storage failover show-반환' 명령을 실행합니다.
PARTNER_NAME을 기다리는 중입니다. 파트너 잠금 동기화를 기다리는 중입니다.	로컬 노드는 HA 인터커넥트를 통해 파트너 노드와 정보를 교환할 수 없으며 파트너 잠금 동기화가 수행되기를 기다리고 있습니다.
PARTNER_NAME을 기다리는 중입니다. 로컬 노드에서 클러스터 애플리케이션이 온라인 상태가 될 때까지 기다리는 중입니다.	로컬 노드는 HA 인터커넥트를 통해 파트너 노드와 정보를 교환할 수 없으며 클러스터 애플리케이션이 온라인 상태로 전환되기를 기다리고 있습니다.
Takeover 예약됨. 테이크오버 준비 과정에서 타겟 노드가 SFO 애그리게이트를 재배치하고,	인수 처리가 시작되었습니다. 타겟 노드가 테이크오버 준비 과정에서 SFO 애그리게이트의 소유권을 재배치하고 있습니다.
Takeover 예약됨. 타겟 노드가 테이크오버 준비 과정에서 SFO 애그리게이트를 재배치했습니다.	인수 처리가 시작되었습니다. 타겟 노드가 테이크오버에 대비하여 SFO 애그리게이트의 소유권을 재배치했습니다.
Takeover 예약됨. 로컬 노드에서 백그라운드 디스크 펌웨어 업데이트를 비활성화하기 위해 기다리는 중입니다. 노드에서 펌웨어 업데이트가 진행 중입니다.	인수 처리가 시작되었습니다. 시스템에서 로컬 노드의 백그라운드 디스크 펌웨어 업데이트 작업이 완료될 때까지 기다리는 중입니다.
테이크오버 준비 시 SFO 애그리게이트를 테이크오버로 재배치	테이크오버에 대비하여 로컬 노드가 SFO 애그리게이트의 소유권을 테이크오버노드로 재배치하고 있습니다.
SFO 애그리게이트를 재배치하여 노드를 인수했습니다. 노드가 테이크오버될 때까지 기다리는 중입니다.	로컬 노드에서 페일오버된 노드로 SFO 애그리게이트의 소유권 재배치가 완료되었습니다. 테이크오버가 수행되는 동안 시스템이 테이크오버 대기 중입니다.
SFO 애그리게이트를 partner_name에 재배치 중입니다. 로컬 노드에서 백그라운드 디스크 펌웨어 업데이트를 비활성화하기 위해 기다리는 중입니다. 노드에서 펌웨어 업데이트가 진행 중입니다.	로컬 노드에서 페일오버된 노드로 SFO 애그리게이트의 소유권 재배치가 진행 중입니다. 시스템에서 로컬 노드의 백그라운드 디스크 펌웨어 업데이트 작업이 완료될 때까지 기다리는 중입니다.
SFO 애그리게이트를 partner_name에 재배치 중입니다. PARTNER_NAME에서 백그라운드 디스크 펌웨어 업데이트를 비활성화하기 위해 기다리는 중입니다. 노드에서 펌웨어 업데이트가 진행 중입니다.	로컬 노드에서 페일오버된 노드로 SFO 애그리게이트의 소유권 재배치가 진행 중입니다. 시스템에서 파트너 노드의 백그라운드 디스크 펌웨어 업데이트 작업이 완료되기를 기다리는 중입니다.

PARTNER_NAME에 연결되었습니다. 이유 때문에 이전 테이크오버 시도가 중단되었습니다. 로컬 노드가 파트너의 일부 SFO 애그리게이트를 소유합니다. 나머지 애그리게이트를 테이크오버하려면 true로 설정된 ``우회 최적화' 매개 변수를 사용하여 파트너의 테이크오버 재발행하거나, 파트너 반환을 제출하십시오.	HA 인터커넥트는 활성 상태이며 데이터를 파트너 노드로 전송할 수 있습니다. 이유 아래에 표시된 원인으로 인해 이전 테이크오버 시도가 중단되었습니다. 로컬 노드는 파트너의 SFO 애그리게이트 중 일부를 소유합니다. • 파트너 노드의 테이크오버를 다시 발행하고-Bypass -optimization 매개 변수를 true 로 설정하여 나머지 SFO 애그리게이트를 테이크오버하거나, 파트너 반환에 대한 반환을 수행하십시오.
PARTNER_NAME에 연결되었습니다. 이전 테이크오버 시도가 중단되었습니다. 로컬 노드가 파트너의 일부 SFO 애그리게이트를 소유합니다. 나머지 애그리게이트를 테이크오버하려면 true로 설정된 ``우회 최적화' 매개 변수를 사용하여 파트너의 테이크오버 재발행하거나, 파트너 반환을 제출하십시오.	HA 인터커넥트는 활성 상태이며 데이터를 파트너 노드로 전송할 수 있습니다. 이전 테이크오버 시도가 중단되었습니다. 로컬 노드는 파트너의 SFO 애그리게이트 중 일부를 소유합니다. • 파트너 노드의 테이크오버를 다시 발행하고-Bypass -optimization 매개 변수를 true 로 설정하여 나머지 SFO 애그리게이트를 테이크오버하거나, 파트너 반환에 대한 반환을 수행하십시오.
PARTNER_NAME을 기다리는 중입니다. 이유 때문에 이전 테이크오버 시도가 중단되었습니다. 로컬 노드가 파트너의 일부 SFO 애그리게이트를 소유합니다. 나머지 애그리게이트를 테이크오버하려면 "-Bypass-optimization" 매개 변수를 true로 설정하여 파트너의 테이크오버 또는 파트너의 반환을 발행하십시오.	로컬 노드는 HA 인터커넥트를 통해 파트너 노드와 정보를 교환할 수 없습니다. 이유 아래에 표시된 원인으로 인해 이전 테이크오버 시도가 중단되었습니다. 로컬 노드는 파트너의 SFO 애그리게이트 중 일부를 소유합니다. • 파트너 노드의 테이크오버를 다시 발행하고-Bypass -optimization 매개 변수를 true 로 설정하여 나머지 SFO 애그리게이트를 테이크오버하거나, 파트너 반환에 대한 반환을 수행하십시오.
PARTNER_NAME을 기다리는 중입니다. 이전 테이크오버 시도가 중단되었습니다. 로컬 노드가 파트너의 일부 SFO 애그리게이트를 소유합니다. 나머지 애그리게이트를 테이크오버하려면 "-Bypass-optimization" 매개 변수를 true로 설정하여 파트너의 테이크오버 또는 파트너의 반환을 발행하십시오.	로컬 노드는 HA 인터커넥트를 통해 파트너 노드와 정보를 교환할 수 없습니다. 이전 테이크오버 시도가 중단되었습니다. 로컬 노드는 파트너의 SFO 애그리게이트 중 일부를 소유합니다. • 파트너 노드의 테이크오버를 다시 발행하고-Bypass -optimization 매개 변수를 true 로 설정하여 나머지 SFO 애그리게이트를 테이크오버하거나, 파트너 반환에 대한 반환을 수행하십시오.
PARTNER_NAME에 연결되었습니다. 로컬 노드에서 백그라운드 디스크 펌웨어 업데이트(BDFU)를 해제하지 못해 이전 테이크오버 시도가 중단되었습니다.	HA 인터커넥트는 활성 상태이며 데이터를 파트너 노드로 전송할 수 있습니다. 로컬 노드의 백그라운드 디스크 펌웨어 업데이트가 비활성화되지 않아 이전 테이크오버 시도가 중단되었습니다.
PARTNER_NAME에 연결되었습니다. 이유 때문에 이전 테이크오버 시도가 중단되었습니다.	HA 인터커넥트는 활성 상태이며 데이터를 파트너 노드로 전송할 수 있습니다. 이유 아래에 표시된 원인으로 인해 이전 테이크오버 시도가 중단되었습니다.

PARTNER_NAME을 기다리는 중입니다. 이유 때문에 이전 테이크오버 시도가 중단되었습니다.	로컬 노드는 HA 인터커넥트를 통해 파트너 노드와 정보를 교환할 수 없습니다. 이유 아래에 표시된 원인으로 인해 이전 테이크오버 시도가 중단되었습니다.
PARTNER_NAME에 연결되었습니다. PARTNER_NAME에 의한 이전 테이크오버 시도가 이유로 중단되었습니다.	HA 인터커넥트는 활성 상태이며 데이터를 파트너 노드로 전송할 수 있습니다. 이유 아래에 표시된 이유로 파트너 노드에서 이전 테이크오버 시도가 중단되었습니다.
PARTNER_NAME에 연결되었습니다. PARTNER_NAME에 의한 이전 테이크오버 시도가 중단되었습니다.	HA 인터커넥트는 활성 상태이며 데이터를 파트너 노드로 전송할 수 있습니다. 파트너 노드에서 이전 테이크오버 시도가 중단되었습니다.
PARTNER_NAME을 기다리는 중입니다. PARTNER_NAME에 의한 이전 테이크오버 시도가 이유로 중단되었습니다.	로컬 노드는 HA 인터커넥트를 통해 파트너 노드와 정보를 교환할 수 없습니다. 이유 아래에 표시된 이유로 파트너 노드에서 이전 테이크오버 시도가 중단되었습니다.
모듈:모듈 이름에서 이전 반환이 실패했습니다. 자동 반환은 초 후에 시작됩니다.	module_name 모듈에서 이전 반환 시도가 실패했습니다. 자동 반환은 초 후에 시작됩니다. • 자세한 내용은 'storage failover show-반환' 명령을 실행합니다.
노드가 무중단 컨트롤러 업그레이드 절차의 일부로 파트너 애그리게이트를 소유합니다.	현재 진행 중인 무중단 컨트롤러 업그레이드 절차로 인해 노드에 파트너 애그리게이트가 있습니다.
PARTNER_NAME에 연결되었습니다. 노드가 클러스터의 다른 노드에 속한 애그리게이트를 소유합니다.	HA 인터커넥트는 활성 상태이며 데이터를 파트너 노드로 전송할 수 있습니다. 이 노드는 클러스터의 다른 노드에 속한 애그리게이트를 소유합니다.
PARTNER_NAME에 연결되었습니다. 파트너 잠금 동기화를 기다리는 중입니다.	HA 인터커넥트는 활성 상태이며 데이터를 파트너 노드로 전송할 수 있습니다. 시스템에서 파트너 잠금 동기화가 완료될 때까지 기다리는 중입니다.
PARTNER_NAME에 연결되었습니다. 로컬 노드에서 클러스터 애플리케이션이 온라인 상태가 될 때까지 기다리는 중입니다.	HA 인터커넥트는 활성 상태이며 데이터를 파트너 노드로 전송할 수 있습니다. 시스템이 로컬 노드에서 클러스터 애플리케이션이 온라인 상태로 전환되기를 기다리고 있습니다.
비 HA 모드, 전체 NVRAM을 사용하려면 재부팅하십시오.	스토리지 페일오버가 가능하지 않습니다. HA 모드 옵션은 non_ha로 구성됩니다. • 모든 NVRAM을 사용하려면 노드를 재부팅해야 합니다.
비 HA 모드: HA를 활성화하려면 노드를 재부팅합니다.	스토리지 페일오버가 가능하지 않습니다. • HA 기능을 사용하려면 노드를 재부팅해야 합니다.

비 HA 모드:	스토리지 페일오버가 가능하지 않습니다. HA 모드 옵션은 non_ha로 구성됩니다. • HA 쌍의 두 노드에서 'Storage failover modify -mode ha-node nodename' 명령을 실행한 다음 노드를 재부팅하여 HA 기능을 활성화해야 합니다.

관련 정보

- "ONTAP 명령 참조입니다"
- "클러스터 ha show"
- "스토리지 장애 조치 hwassist"
- "스토리지 장애 조치 수정"
- "스토리지 장애 조치 표시"
- "스토리지 장애 조치 쇼-기브백"

스토리지 장애 조치를 활성화 및 비활성화하기 위한 ONTAP 명령

다음 명령을 사용하여 스토리지 페일오버 기능을 설정 및 해제합니다.

원하는 작업	이 명령 사용…
테이크오버가 사용되도록 설정합니다	'Storage failover modify -enabled true-node_nodename_'
테이크오버를 사용하지 않도록 설정합니다	'Storage failover modify -enabled false-node_nodename_'

유지보수 절차의 일부로 필요한 경우에만 스토리지 페일오버를 해제해야 합니다.

관련 정보

- "스토리지 장애 조치 수정"

2노드 클러스터에서 인수를 시작하지 않고 ONTAP 노드를 중지하거나 재부팅합니다.

노드 또는 쉘프에 대해 특정 하드웨어 유지 관리를 수행할 때 테이크오버 없이 2노드 클러스터의 노드를 중단하거나 재부팅하는 경우 파트너 노드를 가동하여 중단 시간을 제한하려는 경우 또는 수동 테이크오버(takeover)에 방해가 되는 문제가 있고 파트너 노드의 집계를 유지하고 데이터를 서비스하려는 경우 또한 기술 지원 부서에서 문제 해결을 지원하는 경우 이러한 작업의 일부로 이 절차를 수행할 수 있습니다.

이 작업에 대해

- Takeover를 금지('-inhibit-takeover TRUE' 매개 변수 사용)하기 전에 클러스터 HA를 비활성화합니다.

- 2노드 클러스터에서 클러스터 HA는 노드 1개의 장애가 클러스터를 비활성화하지 않도록 보장합니다. 하지만 '-inhibit-takeover true' 매개 변수를 사용하기 전에 클러스터 HA를 해제하지 않으면 두 노드 모두 데이터 제공을 중단합니다.
- 클러스터 HA를 해제하기 전에 노드를 중단 또는 재부팅하려고 시도하면 ONTAP는 경고를 표시하고 클러스터 HA를 비활성화하라는 메시지를 표시합니다.

- LIF(논리 인터페이스)를 온라인 상태로 유지하려는 파트너 노드로 마이그레이션합니다.
- 중단하거나 재부팅하는 노드에서 유지할 애그리게이트가 있는 경우 온라인 상태로 유지하려는 노드로 이동합니다.

단계

1. 두 노드가 모두 정상 상태인지 확인하십시오. 'cluster show'

   두 노드 모두 '건강' 칼럼에 '참'이 나타납니다.

   ```
   cluster::> cluster show
   Node          Health  Eligibility
   ------------ ------- ------------
   node1         true     true
   node2         true     true
   ```

   에 대한 자세한 내용은 `cluster show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 중단하거나 재부팅될 노드의 모든 LIF를 'network interface migrate-all-node_node_name_' 파트너 노드로 마이그레이션합니다

   에 대한 자세한 내용은 `network interface migrate-all` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 노드에서 중단하거나 재부팅하는 경우 노드가 다운될 때 온라인 상태로 유지하려는 애그리게이트가 있는 경우, 해당 애그리게이트를 파트너 노드로 재배치하고, 그렇지 않으면 다음 단계로 이동하십시오.

   a. 중단하거나 재부팅할 노드에 있는 애그리게이트를 표시합니다. 'storage aggregate show -node_name_'

      예를 들어, node1은 중단되거나 재부팅될 노드입니다.

```
cluster::> storage aggregates show -node node1
Aggregate  Size  Available  Used%  State  #Vols   Nodes   RAID
Status
---------  ----  ---------  -----  -----  -----   -----   ----
------
aggr0_node_1_0
           744.9GB   32.68GB   96% online       2 node1    raid_dp,

normal
aggr1       2.91TB    2.62TB   10% online       8 node1    raid_dp,

normal
aggr2
            4.36TB    3.74TB   14% online      12 node1    raid_dp,

normal
test2_aggr  2.18TB    2.18TB    0% online       7 node1    raid_dp,

normal
4 entries were displayed.
```

b. 파트너 노드로 애그리게이트를 이동합니다. 'storage aggregate Relocation start -node_node_name_ -destination_node_name_-aggregate-list_aggregate_name_'

예를 들어, aggr1, aggr2 및 test2_aggr 애그리게이트를 노드 1에서 노드 2로 이동하는 경우:

'Storage aggregate relocation start -node_node1_-destination_node2_-aggregate-list_aggr1_,*aggr2*,*test2_aggr*'

4. Cluster HA:'cluster ha modify-configured false'를 비활성화합니다

반환 출력에서는 HA가 비활성화 되어 Notice:HA가 disabled로 확인된다

이 작업을 수행해도 스토리지 페일오버가 비활성화되지 않습니다.

5. 적절한 명령을 사용하여 대상 노드의 테이크오버를 중지하거나 재부팅하지 않고 인수를 금지합니다.
   - 'system node halt-node_node_name_-inhibit-takeover TRUE
   - 'system node reboot -node_node_name_-inhibit-takeover TRUE

명령 출력에 계속할 것인지 묻는 경고가 표시됩니다. y를 입력합니다.

6. 아직 온라인 상태인 노드가 정상 상태(파트너가 다운된 상태)인 클러스터 쇼(cluster show)인지 확인합니다

온라인 노드의 경우 "참"이 "상태" 열에 나타납니다.

명령 출력에 클러스터 HA가 구성되지 않았다는 경고가 표시됩니다. 지금은 경고를 무시할 수 있습니다.

7. 노드를 중지하거나 재부팅하는 데 필요한 작업을 수행합니다.
8. LOADER 프롬프트에서 오프라인 노드를 부팅합니다. boot_ONTAP입니다
9. 두 노드가 모두 정상 상태인지 확인하십시오. 'cluster show'

   두 노드 모두 '건강' 칼럼에 '참'이 나타납니다.

   명령 출력에 클러스터 HA가 구성되지 않았다는 경고가 표시됩니다. 지금은 경고를 무시할 수 있습니다.

10. 클러스터 HA 재활성화: '클러스터 ha 수정 - 구성됨 true'
11. 이 절차의 앞부분에서 애그리게이트를 파트너 노드로 재배치한 경우 해당 애그리게이트를 홈 노드로 다시 이동하거나, 그렇지 않은 경우 'Storage aggregate Relocation start -node_name_-destination_node_name_ -aggregate-list_aggregate_name_'으로 이동합니다

    예를 들어, aggr1, aggr2 및 test2_aggr을 노드 node2에서 노드 node1로 이동하는 경우:'storage aggregate relocation start -node_node2_-destination_node1_-aggregate-list_aggr1_,*aggr2*,*test2_aggr*'입니다

12. LIF를 홈 포트로 되돌리기:
    a. 집에 없는 LIF를 보면 네트워크 인터페이스 show-is-home false를 알 수 있습니다

       에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

    b. 다운 노드에서 마이그레이션되지 않은 비홈 LIF가 있는 경우 되돌리기 전에 LIF를 이동해도 되는지 확인하십시오.
    c. 안전한 경우 모든 LIF를 홈으로 되돌리십시오. `network interface revert *` + 에서 에 대해 자세히 `network interface revert` "ONTAP 명령 참조입니다"알아보십시오.

관련 정보

- "클러스터 ha 수정"
- "저장소 집계 재배치 시작"

ONTAP HA 트래픽에 대한 암호화 구성

ONTAP 9.18.1부터 고가용성(HA) 쌍 노드 간 네트워크 트래픽에 대한 암호화를 구성할 수 있습니다. 이 암호화는 HA 쌍의 노드 간에 전송되는 고객 데이터와 메타데이터를 보호합니다.

이 작업에 대해

- HA 트래픽 암호화는 기본적으로 비활성화되어 있습니다.
- HA 트래픽 암호화를 활성화하거나 비활성화하면 클러스터의 모든 HA 쌍에 영향을 미칩니다. 개별 노드에 대해 암호화를 활성화하거나 비활성화할 수 없습니다.
- HA 트래픽 암호화를 활성화하면 HA 쌍 노드 간에 전송되는 모든 고객 데이터와 메타데이터가 암호화됩니다. 파일 시스템 메타데이터 및 하트비트 메시지와 같은 일부 HA 트래픽은 암호화되지 않습니다.

- HA 트래픽 암호화가 활성화되고 클러스터에 새 HA 쌍이 추가되면 다음을 다시 실행하여 새 노드에 대한 HA 트래픽 암호화를 수동으로 활성화해야 합니다. `security ha-network modify -enabled true` 명령.

시작하기 전에

- 당신은 ONTAP 관리자여야 합니다. `admin` 다음 절차를 수행하려면 권한 수준이 필요합니다.
- HA 트래픽 암호화를 활성화하기 전에 다음을 수행해야 합니다."외부 키 관리를 구성합니다" .
- HA 트래픽 암호화를 활성화하려면 클러스터의 모든 노드에서 ONTAP 9.18.1 이상을 실행해야 합니다.

단계

1. HA 트래픽에 대한 현재 암호화 상태를 확인하세요.

```
security ha-network show
```

이 명령은 각 노드의 HA 트래픽 암호화의 현재 상태를 보여줍니다.

```
security ha-network show
Node                  Enabled
--------------------- --------------------
node1                 true
node2                 true
node3                 true
node4                 true
4 entries were displayed.
```

2. HA 트래픽에 대한 암호화를 활성화하거나 비활성화합니다.

```
security ha-network modify -enabled <true|false>
```

이 명령은 클러스터의 모든 노드에 대해 암호화된 HA 트래픽을 활성화하거나 비활성화합니다. 클러스터에 새로운 HA 쌍이 추가되면 이 명령을 다시 실행하여 새 노드에 대한 HA 트래픽 암호화를 활성화해야 합니다.

System Manager를 통한 REST API 관리

System Manager를 통한 REST API 관리

REST API 로그는 System Manager에서 ONTAP로 발급하는 API 호출을 캡처합니다. 로그를 사용하여 다양한 ONTAP 관리 작업을 수행하는 데 필요한 통화의 특성과 순서를 이해할 수 있습니다.

System Manager에서 REST API 및 API 로그를 사용하는 방법

System Manager에서 ONTAP로 REST API 호출을 수행하는 방법에는 여러 가지가 있습니다.

System Manager에서 API 호출을 수행하는 경우

다음은 System Manager에서 ONTAP REST API 호출을 실행할 때의 가장 중요한 예입니다.

자동 페이지 새로 고침

System Manager는 백그라운드에서 자동으로 API 호출을 발행하여 대시보드 페이지와 같이 표시된 정보를 새로 고칩니다.

사용자별 작업을 표시합니다

특정 스토리지 리소스를 표시하거나 System Manager UI의 리소스 컬렉션을 표시할 때 하나 이상의 API 호출이 실행됩니다.

사용자별 업데이트 작업입니다

API 호출은 ONTAP 리소스를 System Manager UI에서 추가, 수정 또는 삭제할 때 실행됩니다.

API 호출을 재발행하는 중입니다

로그 항목을 클릭하여 API 호출을 수동으로 다시 실행할 수도 있습니다. 통화의 원시 JSON 출력을 표시합니다.

추가 정보

- "ONTAP 9 자동화 문서"

REST API 로그에 액세스 중입니다

System Manager에서 수행한 ONTAP REST API 호출 기록이 포함된 로그에 액세스할 수 있습니다. 로그를 표시할 때 API 호출을 재발급하고 출력을 검토할 수도 있습니다.

단계

1. 페이지 맨 위에서 를 클릭하여 REST API 로그를 표시합니다.

   가장 최근 항목이 페이지 하단에 표시됩니다.

2. 왼쪽에서 * 인스트루먼트 패널 * 을 클릭하고 페이지를 새로 고치기 위해 발급된 API 호출에 대해 새로 생성되는 항목을 확인합니다.
3. 스토리지 * 를 클릭한 다음 * qtree * 를 클릭합니다.

   이로 인해 System Manager에서 특정 API 호출을 발행하여 qtree 목록을 검색합니다.

4. 다음과 같은 형식의 API 호출을 설명하는 로그 항목을 찾습니다.

   'get/api/storage/qtree'

   항목에 포함된 추가 HTTP 쿼리 매개 변수(예: max_records)가 표시됩니다.

5. 로그 항목을 클릭하여 Get API 호출을 재발행하고 원시 JSON 출력을 표시합니다.

예


```
{
  "records": [
    {
      "svm": {
        "uuid": "19507946-e801-11e9-b984-00a0986ab770",
        "name": "SMQA",
        "_links": {
          "self": {
            "href": "/api/svm/svms/19507946-e801-11e9-b984-00a0986ab770"
          }
        }
      },
      "volume": {
        "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
        "name": "vol_vol_test2_dest_dest",
        "_links": {
          "self": {
            "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-
00a0986abd71"
          }
        }
      },
      "id": 1,
      "name": "test2",
      "security_style": "mixed",
      "unix_permissions": 777,
      "export_policy": {
        "name": "default",
        "id": 12884901889,
        "_links": {
          "self": {
            "href": "/api/protocols/nfs/export-policies/12884901889"
          }
        }
      },
      "path": "/vol_vol_test2_dest_dest/test2",
      "_links": {
        "self": {
          "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-
00a0986abd71/1"
        }
      }
    },
    ],
```

```
    "num_records": 1,
    "_links": {
      "self": {
        "href":
"/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"
      }
    }
  }
```

볼륨 관리

System Manager를 사용하여 볼륨 및 LUN 관리

볼륨 관리

System Manager를 사용하여 **ONTAP** 볼륨 관리

System Manager에 볼륨 목록을 표시한 후 다양한 작업을 수행하여 볼륨을 관리할 수 있습니다.

다음 볼륨을 비롯한 일부 볼륨 유형은 System Manager에서 사용할 수 없습니다.

- Vol0를 참조하십시오
- Del 및 TMP 유형 볼륨
- FlexGroup 구성 요소입니다
- MetroCluster 구성에서 복제된 볼륨

단계

1. System Manager에서 * 스토리지 > 볼륨 * 을 클릭합니다.

   볼륨 목록이 표시됩니다.

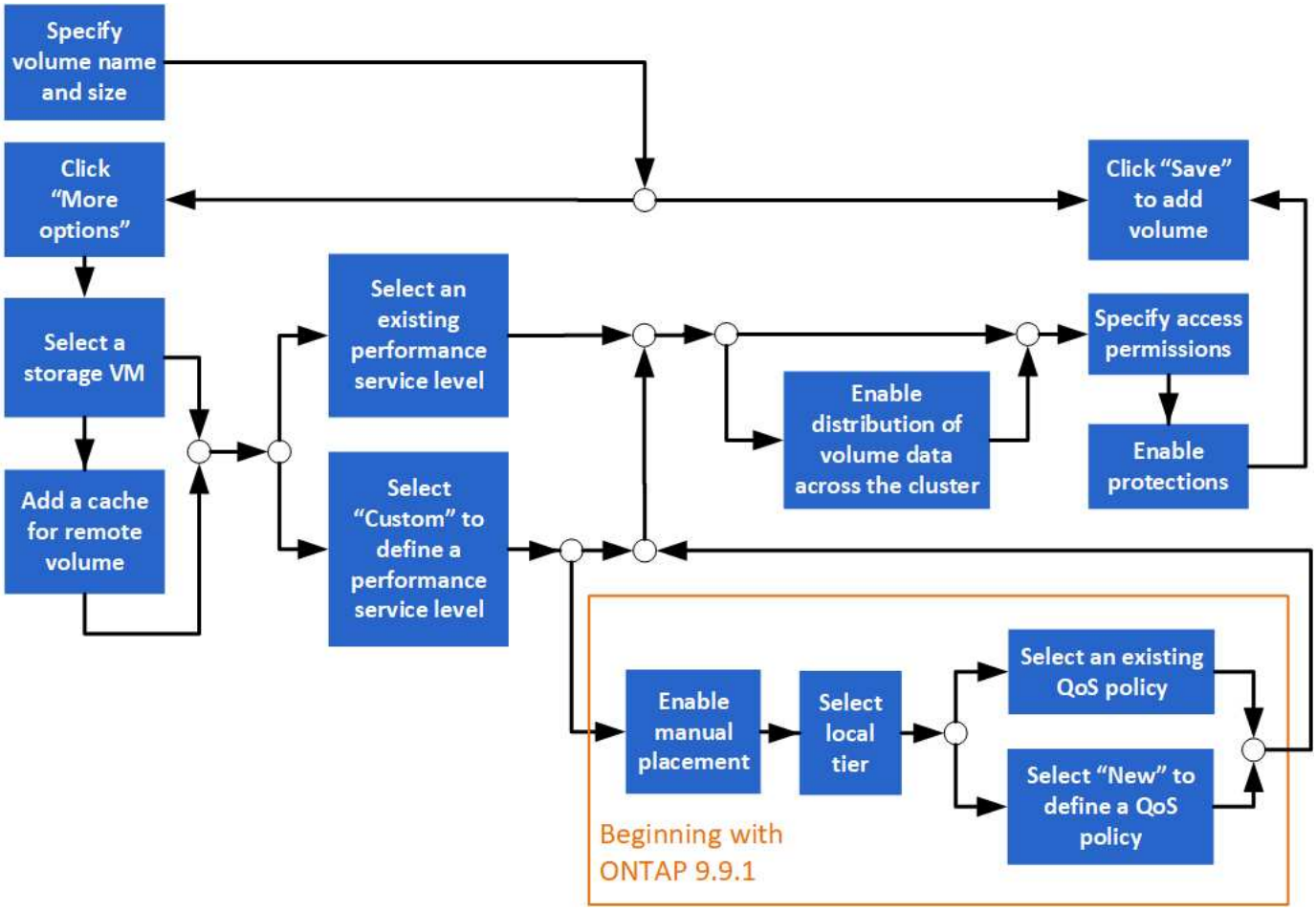
2. 다음을 수행할 수 있습니다.

이 작업을 수행하려면…	다음 작업 수행…
볼륨을 추가합니다	을 + Add 클릭합니다. 을 "볼륨을 추가합니다"참조하십시오.
여러 볼륨을 관리합니다	볼륨 옆의 확인란을 선택합니다. • Delete 선택한 볼륨을 삭제하려면 클릭합니다. • Protect 선택한 볼륨에 보호 정책을 할당하려면 클릭합니다. • 을 클릭합니다 ⋮ More 선택한 모든 볼륨에 대해 수행할 다음 작업 중 하나를 선택합니다. ◦ 할당량을 설정합니다 ◦ 오프라인 상태로 전환 ◦ 이동 ◦ 삭제된 볼륨 표시

단일 볼륨 관리	볼륨 옆에 있는 을 클릭한 후 수행할 다음 작업 중 하나를 선택합니다. • 편집 • 크기 조정(ONTAP 9.10.1부터 온라인 볼륨 및 DP FlexVol 볼륨에만 해당) • 삭제 • 복제 • 오프라인 상태로 전환(또는 온라인 상태로 전환) • 할당량 활성화(또는 할당량 비활성화) • 내보내기 정책을 편집합니다 • 마운트 경로 편집 • 이동 • 클라우드 계층 설정을 편집합니다 • 보호
볼륨 이름을 바꿉니다	개요 페이지에서 볼륨의 이름을 변경할 수 있습니다. 볼륨 이름 옆에 있는 을 클릭한 다음 볼륨 이름을 수정합니다.

볼륨을 추가합니다

볼륨을 생성하여 NFS 또는 SMB 서비스용으로 구성된 기존 스토리지 VM에 추가할 수 있습니다.



시작하기 전에

- NFS 또는 SMB 서비스용으로 구성된 스토리지 VM이 클러스터에 존재해야 합니다.
- ONTAP 9.13.1부터 새로운 볼륨에 대해 용량 분석 및 활동 추적을 기본적으로 사용할 수 있습니다. System Manager에서 클러스터 또는 스토리지 VM 레벨의 기본 설정을 관리할 수 있습니다. 자세한 내용은 을 "파일 시스템 분석 설정"참조하십시오.

단계

1. 스토리지 > 볼륨 * 으로 이동합니다.
2. 를 선택합니다 + Add .
3. 볼륨의 이름과 크기를 지정합니다.
4. 다음 단계 중 하나를 수행합니다.

이 버튼 선택…	이 작업을 수행하려면…
* 저장 *	시스템 기본값을 사용하여 볼륨이 생성되고 추가됩니다. 추가 단계가 필요하지 않습니다.
* 추가 옵션 *	로 진행합니다 [step5] 볼륨에 대한 사양을 정의합니다.

5. [[5단계, 5단계] 이전에 지정한 경우 볼륨 이름과 크기가 표시됩니다. 그렇지 않으면 이름과 크기를 입력합니다.
6. 풀다운 목록에서 스토리지 VM을 선택합니다.

NFS 프로토콜로 구성된 스토리지 VM만 나열됩니다. NFS 프로토콜로 구성된 스토리지 VM을 하나만 사용할 수 있는 경우 * Storage VM * 필드가 표시되지 않습니다.

7. 원격 볼륨에 대한 캐시를 추가하려면 * 원격 볼륨에 대한 캐시 추가 * 를 선택하고 다음 값을 지정합니다.
   - 클러스터를 선택합니다.
   - 스토리지 VM을 선택합니다.
   - 캐시 볼륨으로 사용할 볼륨을 선택합니다.
8. 스토리지 및 최적화 * 섹션에서 다음 값을 지정합니다.
   a. 볼륨의 용량이 이미 표시되어 있지만 수정할 수 있습니다.
   b. 성능 서비스 수준 * 필드에서 서비스 수준을 선택합니다.

이 서비스 수준을 선택할 때…	이 문제는…
"익스트림", "성능" 또는 "가치"와 같은 기존 서비스 수준. 시스템 플랫폼(AFF, FAS 또는 기타)에 유효한 서비스 수준만 표시됩니다.	로컬 계층 또는 계층이 자동으로 선택됩니다. 로 진행합니다 [step9].
맞춤형	로 진행합니다 Step 8C 새 서비스 수준을 정의합니다.

   c. ONTAP 9.9.1부터 시스템 관리자를 사용하여 생성 중인 볼륨을 배치할 로컬 계층을 수동으로 선택할 수 있습니다("사용자 지정" 서비스 수준을 선택한 경우).

> ⓘ 원격 볼륨의 캐시로 추가 * 또는 * 클러스터 전체에 볼륨 데이터 배포 * 를 선택한 경우에는 이 옵션을 사용할 수 없습니다(아래 참조).

이 옵션을 선택할 때…	다음 단계를 수행합니다.
* 수동 배치 *	수동 배치가 활성화됩니다. 클러스터에서 볼륨 데이터 분산 * 선택 사항이 비활성화됩니다(아래 참조). 로 진행합니다 stStep 8d 를 눌러 프로세스를 완료합니다.
선택 항목이 없습니다	수동 배치가 활성화되지 않았습니다. 로컬 계층이 자동으로 선택됩니다. 로 진행합니다 [step9].

   a. 풀다운 메뉴에서 로컬 계층을 선택합니다.
   b. QoS 정책을 선택합니다.

      기존 정책 목록에서 선택하려면 "기존"을 선택하고, 새 정책의 사양을 입력하려면 "새로 만들기"를 선택합니다.

9. [[9단계, 9단계] * 최적화 옵션 * 섹션에서 볼륨 데이터를 클러스터 전체에 배포할지 여부를 결정합니다.

이 옵션을 선택할 때…	이 문제는…
* 클러스터 전체에 볼륨 데이터 배포 * 를 참조하십시오	추가하려는 볼륨이 FlexGroup 볼륨이 됩니다. 이전에 수동 배치 * 를 선택한 경우에는 이 옵션을 사용할 수 없습니다.
선택 항목이 없습니다	추가하는 볼륨은 기본적으로 FlexVol 볼륨이 됩니다.

10. 액세스 권한 * 섹션에서 볼륨이 구성된 프로토콜에 대한 액세스 권한을 지정합니다.

    ONTAP 9.11.1부터는 새 볼륨을 기본적으로 공유할 수 없습니다. 다음 확인란이 선택되어 있는지 확인하여 기본 액세스 권한을 지정할 수 있습니다.

    - **NGS**를 통한 내보내기: 볼륨을 생성합니다. `default` 사용자에게 데이터에 대한 전체 액세스 권한을 부여하는 내보내기 정책입니다.
    - * SMB/CIFS를 통한 공유 *: 자동 생성 이름으로 공유를 생성하고 편집할 수 있습니다. 접근 권한이 부여됩니다 `Everyone` . 또한 사용 권한 수준을 지정할 수도 있습니다.

11. 보호 * 섹션에서 볼륨에 대한 보호를 지정합니다.
    - ONTAP 9.12.1부터 *스냅샷 사용(로컬)*을 선택하고 기본값을 사용하는 대신 스냅샷 정책을 선택할 수 있습니다.
    - SnapMirror(로컬 또는 원격) * 활성화 를 선택한 경우 풀다운 목록에서 대상 클러스터에 대한 보호 정책 및 설정을 지정합니다.
12. 저장 * 을 선택합니다.

    볼륨이 생성되고 클러스터 및 스토리지 VM에 추가됩니다.

    또한 이 볼륨의 사양을 Ansible 플레이북에 저장할 수도 있습니다. 자세한 내용은 를 참조하십시오 "Ansible 플레이북을 사용하여 볼륨 또는 LUN을 추가 또는 편집합니다".

볼륨에 태그를 할당합니다

ONTAP 9.14.1부터 System Manager를 사용하여 볼륨에 태그를 할당하면 프로젝트 또는 비용 센터와 같은 범주에 속하는 오브젝트를 식별할 수 있습니다.

이 작업에 대해

볼륨에 태그를 할당할 수 있습니다. 먼저 태그를 정의하고 추가해야 합니다. 그런 다음 태그를 편집하거나 삭제할 수도 있습니다.

태그를 볼륨을 생성할 때 추가하거나 나중에 추가할 수 있습니다.

키를 지정하고 ""키:값"" 형식을 사용하여 값을 연결하여 태그를 정의합니다. 예: "'dEPT:engineering"" 또는 "'location:san-jose".

태그를 만들 때 다음 사항을 고려해야 합니다.

- 키의 최소 길이는 1자이며 null일 수 없습니다. 값은 null일 수 있습니다.
- 키는 ""location: san-jose, Toronto""와 같이 값을 쉼표로 구분하여 여러 값과 쌍을 이룰 수 있습니다.
- 태그를 여러 리소스에 사용할 수 있습니다.
- 키는 소문자로 시작해야 합니다.
- 볼륨이 삭제되면 볼륨에 할당된 태그가 삭제됩니다.
- 복구 대기열에서 볼륨을 복구한 경우에는 태그가 복구되지 않습니다.
- 볼륨이 이동되거나 복제되는 경우 태그가 유지됩니다.

- 재해 복구 관계에서 스토리지 VM에 할당된 태그는 파트너 사이트의 볼륨에 복제됩니다.

단계

태그를 관리하려면 다음 단계를 수행하십시오.

1. System Manager에서 * Volumes * 를 클릭한 다음 태그를 추가할 볼륨을 선택합니다.

   태그는 * 태그 * 섹션에 나열됩니다.

2. 기존 태그를 수정하거나 새 태그를 추가하려면 * 태그 관리 * 를 클릭합니다.

   태그를 추가, 편집 또는 삭제할 수 있습니다.

이 작업을 수행하려면…	다음 단계를 수행합니다.
태그를 추가합니다	a. 태그 추가 * 를 클릭합니다. b. 키와 해당 값 또는 값을 지정합니다(여러 값을 쉼표로 구분). c. 저장 * 을 클릭합니다.
태그를 편집합니다	a. 키 * 및 * 값(선택 사항) * 필드의 내용을 수정합니다. b. 저장 * 을 클릭합니다.
태그를 삭제합니다	a. 삭제할 태그 옆에 있는 을 클릭합니다.

삭제된 볼륨을 복구합니다

하나 이상의 FlexVol 볼륨을 실수로 삭제한 경우, System Manager를 사용하여 해당 볼륨을 복구할 수 있습니다. ONTAP 9.8부터 System Manager를 사용하여 FlexGroup 볼륨을 복구할 수도 있습니다. 볼륨을 삭제하여 볼륨을 영구적으로 삭제할 수도 있습니다.

스토리지 VM 레벨에서 볼륨 보존 시간을 설정할 수 있습니다. 기본적으로 볼륨 보존 시간은 12시간으로 설정됩니다.

삭제된 볼륨 선택

단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 자세히 > 삭제된 볼륨 표시 * 를 클릭합니다.
3. 볼륨을 선택하고 원하는 작업을 클릭하여 볼륨을 복구하거나 영구적으로 삭제합니다.

볼륨 구성을 재설정합니다

볼륨을 삭제하면 볼륨과 연결된 구성이 삭제됩니다. 볼륨을 복구해도 모든 구성이 재설정되지 않습니다. 볼륨을 원래 상태로 되돌리기 위해 볼륨을 복구한 후 다음 작업을 수동으로 수행합니다.

단계

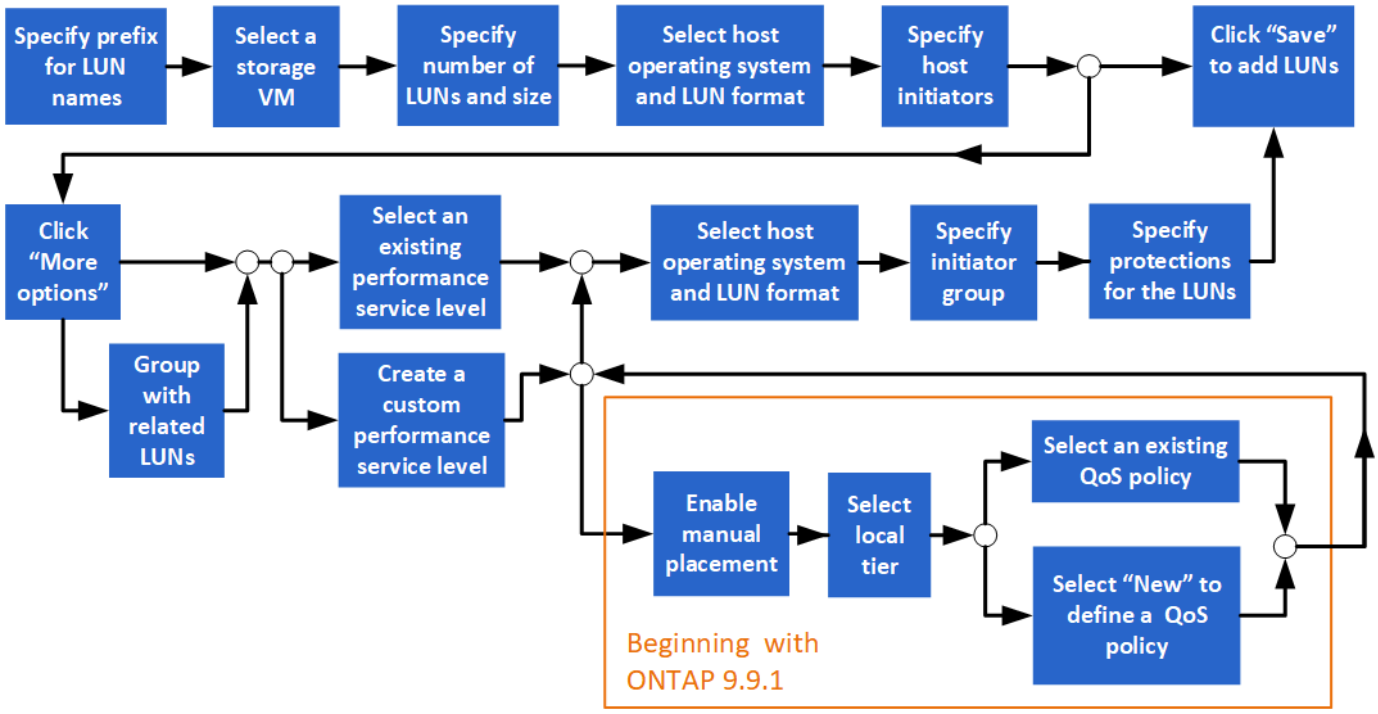
1. 볼륨 이름을 바꿉니다.

2. 연결 경로(NAS)를 설정합니다.
3. 볼륨의 LUN(SAN)에 대한 매핑을 생성합니다.
4. 스냅샷 정책 및 엑스포트 정책을 볼륨에 연결합니다.
5. 볼륨에 대한 새 할당량 정책 규칙을 추가합니다.
6. 볼륨에 대한 QoS 정책을 추가합니다.

ONTAP 시스템 관리자를 사용하여 LUN 관리

LUN을 생성하여 SAN 프로토콜로 구성된 기존 스토리지 VM에 추가할 수 있습니다. LUN을 그룹화하거나 이름을 바꿀 수도 있습니다.

LUN을 추가합니다



시작하기 전에

SAN 서비스용으로 구성된 스토리지 VM이 클러스터에 있어야 합니다.

단계

1. 스토리지 > LUN * 으로 이동합니다.
2. 을 클릭합니다 + Add .
3. 각 LUN 이름의 시작 시에 사용할 접두사를 지정합니다. (LUN을 하나만 생성하는 경우 LUN 이름을 입력합니다.)
4. 풀다운 목록에서 스토리지 VM을 선택합니다.

   SAN 프로토콜에 대해 구성된 스토리지 VM만 나열됩니다. SAN 프로토콜에 대해 구성된 스토리지 VM을 하나만 사용할 수 있는 경우 * 스토리지 VM * 필드가 표시되지 않습니다.

5. 생성할 LUN의 수와 각 LUN의 크기를 나타냅니다.

6. 풀다운 목록에서 호스트 운영 체제 및 LUN 형식을 선택합니다.
7. 호스트 이니시에이터를 입력하고 쉼표로 구분합니다.
8. 다음 작업 중 하나를 수행합니다.

이 단추를 클릭합니다…	이 작업을 수행하려면…
* 저장 *	LUN은 입력한 사양으로 생성됩니다. 시스템 기본값은 다른 사양에 사용됩니다. 추가 단계가 필요하지 않습니다.
* 추가 옵션 *	로 진행합니다 [step9-define-add-specs] LUN에 대한 추가 사양을 정의합니다.

9. [[9단계 - Define - add - specs, 9단계]] 이전에 LUN 접두사를 입력한 경우에는 LUN 접두사가 이미 표시되어 있지만 수정할 수 있습니다. 그렇지 않으면 접두사를 입력합니다.
10. 풀다운 목록에서 스토리지 VM을 선택합니다.

    SAN 프로토콜에 대해 구성된 스토리지 VM만 나열됩니다. SAN 프로토콜에 대해 구성된 스토리지 VM을 하나만 사용할 수 있는 경우 * 스토리지 VM * 필드가 표시되지 않습니다.

11. LUN을 그룹화할 방법을 결정합니다.

이 옵션을 선택할 때…	이 문제는…
* 관련 LUN이 있는 그룹 *	LUN은 스토리지 VM의 기존 볼륨에서 관련 LUN과 함께 그룹화됩니다.
선택 항목이 없습니다	LUN은 "컨테이너"라는 볼륨에서 함께 그룹화됩니다.

12. 스토리지 및 최적화 * 섹션에서 다음 값을 지정합니다.
    a. 이전에 LUN을 입력한 경우 LUN의 수와 용량이 이미 표시되지만 수정할 수 있습니다. 그렇지 않으면 값을 입력합니다.
    b. 성능 서비스 수준 * 필드에서 서비스 수준을 선택합니다.

이 서비스 수준을 선택할 때…	이 문제는…
"익스트림", "성능" 또는 "가치"와 같은 기존 서비스 수준. 시스템 플랫폼(AFF, FAS 또는 기타)에 유효한 서비스 수준만 표시됩니다.	로컬 계층이 자동으로 선택됩니다. 로 진행합니다 [step13].
맞춤형	로 진행합니다 step12c 새 서비스 수준을 정의합니다.

    c. ONTAP 9.9.1부터 시스템 관리자를 사용하여 생성할 LUN을 배치할 로컬 계층을 수동으로 선택할 수 있습니다("사용자 지정" 서비스 수준을 선택한 경우).

이 옵션을 선택할 때…	다음 단계를 수행합니다.
* 수동 배치 *	수동 배치가 활성화됩니다. 로 진행합니다 [step12d] 를 눌러 프로세스를 완료합니다.

선택 항목이 없습니다	수동 선택이 활성화되지 않았습니다. 로컬 계층이 자동으로 선택됩니다. 로 진행합니다 [step13].

d. [[12d, 12d 단계]] 풀다운 메뉴에서 로컬 계층을 선택합니다.

e. QoS 정책을 선택합니다.

기존 정책 목록에서 선택하려면 "기존"을 선택하고, 새 정책의 사양을 입력하려면 "새로 만들기"를 선택합니다.

13. [[13단계, 13단계] * 호스트 정보 * 섹션에 호스트 운영 체제와 LUN 형식이 이미 표시되어 있지만 수정할 수 있습니다.

14. 호스트 매핑 * 에서 LUN의 이니시에이터 유형을 선택합니다.

- * 기존 이니시에이터 그룹 *: 목록이 표시되면 이니시에이터 그룹을 선택합니다.
- * 기존 이니시에이터 그룹을 사용하여 새 이니시에이터 그룹 *: 새 그룹의 이름을 지정하고 새 그룹을 생성하는 데 사용할 그룹을 선택합니다.
- * 호스트 이니시에이터 *: 새 이니시에이터 그룹의 이름을 지정하고 * + 이니시에이터 추가 * 를 클릭하여 이니시에이터를 그룹에 추가합니다.

15. 보호 * 섹션에서 LUN에 대한 보호 기능을 지정합니다.

SnapMirror(로컬 또는 원격) * 활성화 를 선택한 경우 풀다운 목록에서 대상 클러스터에 대한 보호 정책 및 설정을 지정합니다.

16. 저장 * 을 클릭합니다.

LUN이 생성되어 클러스터 및 스토리지 VM에 추가됩니다.

이러한 LUN의 사양을 Ansible 플레이북에 저장할 수도 있습니다. 자세한 내용은 을 "Ansible 플레이북을 사용하여 볼륨 또는 LUN을 추가 또는 편집합니다"참조하십시오.

LUN의 이름을 바꿉니다

개요 페이지에서 LUN의 이름을 바꿀 수 있습니다.

단계

1. System Manager에서 * LUNs * 를 클릭합니다.
2. 이름을 바꾸려는 LUN 이름 옆의 을 클릭하고 LUN 이름을 수정합니다.
3. 저장 * 을 클릭합니다.

ONTAP 시스템 관리자로 스토리지 확장

System Manager를 사용하면 호스트에서 더 많은 공간을 사용할 수 있도록 볼륨 또는 LUN의 크기를 늘릴 수 있습니다. LUN 크기는 포함된 볼륨의 크기를 초과할 수 없습니다.

ONTAP 9.12.1부터 볼륨의 새 용량을 입력하면 * 볼륨 크기 조정 * 창에 볼륨 크기가 데이터 공간 및 스냅숏 예비 공간에 미치는 영향이 표시됩니다.

- 볼륨 크기를 늘립니다

- LUN의 크기를 늘립니다

또한 기존 볼륨에 LUN을 추가할 수 있습니다. ONTAP 9.8 이상에서 System Manager를 사용하는 경우 프로세스가 다릅니다.

- 기존 볼륨에 LUN 추가(ONTAP 9.8)
- 기존 볼륨에 LUN 추가(ONTAP 9.7)

볼륨 크기를 늘립니다

단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 크기를 늘릴 볼륨의 이름 위에 마우스를 놓습니다.
3. 을 ⋮클릭합니다.
4. 편집 * 을 선택합니다.
5. 용량 값을 늘립니다.
6. 기존 * 및 * 새 * 데이터 공간과 스냅숏 예비 공간 세부 정보를 검토합니다.

LUN의 크기를 늘립니다

단계

1. 스토리지 > LUN * 을 클릭합니다.
2. 크기를 늘릴 LUN 이름 위로 마우스를 가져갑니다.
3. 을 ⋮클릭합니다.
4. 편집 * 을 선택합니다.
5. 용량 값을 늘립니다.

기존 볼륨에 **LUN** 추가**(ONTAP 9.8)**

ONTAP 9.8부터 System Manager를 사용하여 이미 LUN이 하나 이상 있는 기존 볼륨에 LUN을 추가할 수 있습니다.

단계

1. 스토리지 > LUN * 을 클릭합니다.
2. 추가 + * 를 클릭합니다.
3. Add LUNs * 창에서 필드를 작성합니다.
4. 추가 옵션 * 을 선택합니다.
5. Group with related LUNs * 확인란을 선택합니다.
6. 드롭다운 필드에서 다른 LUN을 추가할 볼륨에 있는 LUN을 선택합니다.
7. 나머지 필드를 작성합니다. 호스트 매핑 * 의 경우 라디오 버튼 중 하나를 클릭합니다.
    - * 기존 이니시에이터 그룹 * 목록에서 기존 그룹을 선택할 수 있습니다.
    - * 새 이니시에이터 그룹 * 필드에 새 그룹을 입력할 수 있습니다.

기존 볼륨에 **LUN** 추가**(ONTAP 9.7)**

ONTAP 9.7과 함께 System Manager를 사용하여 기존 볼륨에 LUN을 추가하려면 먼저 클래식 보기로 전환해야 합니다.

단계

1. ONTAP 9.7에서 System Manager에 로그인합니다.
2. 클래식 보기 * 를 클릭합니다.
3. 스토리지 > LUN > 생성 * 을 선택합니다
4. LUN을 생성할 세부 정보를 지정합니다.
5. LUN을 추가할 기존 볼륨 또는 qtree를 지정합니다.

ONTAP System Manager를 사용하여 압축**,** 압축 및 중복 제거를 사용하여 저장 공간을 절약하세요**.**

비 AFF 클러스터의 볼륨의 경우 중복제거, 데이터 압축, 데이터 컴팩션을 함께 실행하거나 독립적으로 실행하여 최적의 공간 절약 효과를 달성할 수 있습니다.

- 중복 제거는 중복되는 데이터 블록을 제거합니다.
- 데이터 압축: 데이터 블록을 압축하여 필요한 물리적 스토리지의 양을 줄입니다.
- 데이터 컴팩션은 더 적은 공간에 더 많은 데이터를 저장하여 스토리지 효율성을 높입니다.

이러한 작업은 AFF가 아닌 클러스터의 볼륨에 대해 지원됩니다. 인라인 중복 제거 및 인라인 압축과 같은 모든 인라인 스토리지 효율성 기능은 AFF 볼륨에서 기본적으로 활성화됩니다.

단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 스토리지를 저장할 볼륨의 이름 옆에 있는 을 클릭합니다 .
3. Edit * 를 클릭하고 * Storage Efficiency * 로 스크롤합니다.
4. *Optional*: 백그라운드 중복 제거를 설정하려면 확인란이 선택되어 있는지 확인합니다.
5. 선택 사항: 백그라운드 압축을 설정하려면 스토리지 효율성 정책을 지정하고 확인란이 선택되어 있는지 확인합니다.
6. *Optional*: 인라인 압축을 활성화하려면 확인란이 선택되어 있는지 확인합니다.

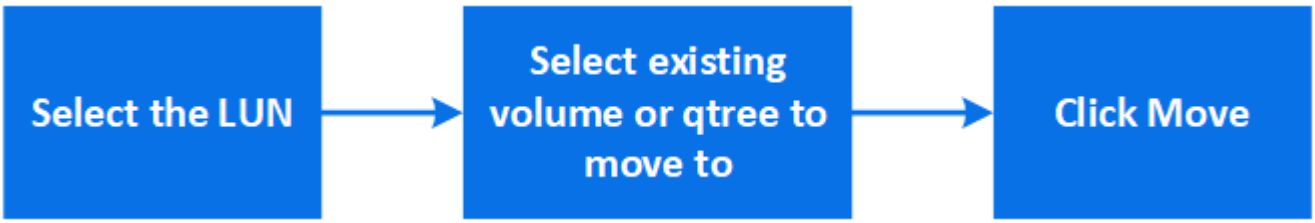
ONTAP 시스템 관리자를 사용하여 **LUN**을 이동하여 부하를 균형 있게 조정합니다**.**

스토리지 VM 내의 다른 볼륨으로 LUN을 이동하여 로드 밸런싱을 수행하거나 성능 서비스 수준이 높은 볼륨으로 LUN을 이동하여 성능을 향상할 수 있습니다.

이동 제한

- LUN을 동일한 볼륨 내의 qtree로 이동할 수 없습니다.
- CLI를 사용하여 파일에서 생성한 LUN은 System Manager를 사용하여 이동할 수 없습니다.
- 온라인 상태이고 데이터를 제공하는 LUN은 이동할 수 없습니다.

- 대상 볼륨에 할당된 공간에 LUN이 포함될 수 없는 경우(볼륨에 자동 확장 이 설정된 경우에도) LUN을 이동할 수 없습니다.
- SnapLock 볼륨의 LUN은 System Manager를 사용하여 이동할 수 없습니다.



단계

1. 스토리지 > LUN * 을 클릭합니다.
2. 이동할 LUN을 선택하고 * 이동 * 을 클릭합니다.
3. LUN을 이동할 기존 볼륨을 선택합니다. 볼륨에 Qtree가 포함된 경우 qtree를 선택합니다.

이동 작업이 진행 중인 동안에는 원본 볼륨과 대상 볼륨 모두에 LUN이 표시됩니다.

ONTAP 시스템 관리자를 사용하여 볼륨을 다른 계층으로 이동하여 부하를 균형 있게 조정합니다.

ONTAP 9.9.1부터 활성 및 비활성 데이터 저장소 분석을 기반으로 볼륨을 이동할 수 있습니다. ONTAP 9.8에서는 시스템 관리자를 사용하여 볼륨을 다른 계층으로 이동하여 부하를 분산할 수도 있습니다.

자세한 내용은 다음을 참조하세요. "파일 시스템 분석 개요" .

단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 이동할 볼륨을 선택한 다음 * 이동 * 을 클릭합니다.
3. 볼륨 또는 볼륨을 이동할 기존 계층(애그리게이트)을 선택합니다.

ONTAP 시스템 관리자를 사용하여 Ansible Playbook을 사용하여 볼륨이나 LUN을 추가하거나 편집합니다.

ONTAP 9.9.1부터 볼륨 또는 LUN을 추가하거나 편집하려는 경우 시스템 관리자와 함께 Ansible 플레이북을 사용할 수 있습니다.

이 기능을 사용하면 동일한 구성을 여러 번 사용하거나 볼륨 또는 LUN을 추가 또는 편집할 때 약간 변경된 동일한 구성을 사용할 수 있습니다.

Ansible Playbook을 사용하거나 사용하지 않도록 설정합니다

System Manager에서 Ansible Playbook 사용을 설정하거나 해제할 수 있습니다.

단계

1. System Manager에서 클러스터 설정 페이지의 UI 설정으로 이동합니다.
   - 클러스터 > 설정 *
2. UI 설정 * 에서 슬라이더 스위치를 "사용" 또는 "사용 안 함"으로 변경합니다.

볼륨 구성을 **Ansible Playbook**에 저장합니다

볼륨 구성을 생성하거나 수정할 때 구성을 Ansible Playbook 파일로 저장할 수 있습니다.

단계

1. 볼륨 추가 또는 편집:

   볼륨 > 추가 * (또는 * 볼륨 > 편집 *)

2. 볼륨의 구성 값을 지정하거나 편집합니다.
3. 구성을 Ansible Playbook 파일에 저장하려면 * Save to Ansible Playbook * 을 선택하십시오.

   다음 파일이 포함된 zip 파일이 다운로드됩니다.

   - (* variable.YAML *): 볼륨을 추가하거나 편집하기 위해 입력 또는 수정한 값입니다.
   - ' * volumeAdd.YAML * '(또는 ' * volumeEdit.YAML * '): 'variable.YAML' 파일에서 입력을 읽을 때 값을 생성하거나 수정하는 데 필요한 테스트 케이스.

LUN 구성을 **Ansible** 플레이북에 저장합니다

LUN 구성을 생성하거나 수정할 때 구성을 Ansible Playbook 파일로 저장할 수 있습니다.

단계

1. LUN 추가 또는 편집:

   LUN > 추가 * (또는 * LUN > 편집 *)

2. LUN의 구성 값을 지정하거나 편집합니다.
3. 구성을 Ansible Playbook 파일에 저장하려면 * Save to Ansible Playbook * 을 선택하십시오.

   다음 파일이 포함된 zip 파일이 다운로드됩니다.

   - ' * variable.YAML *': LUN 추가 또는 편집을 위해 입력하거나 수정한 값입니다.
   - ' * lunAdd.YAML * '(또는 ' * lunEdit.YAML * '): 'variable.YAML' 파일에서 입력을 읽을 때 값을 생성하거나 수정하는 데 필요한 테스트 케이스.

글로벌 검색 결과에서 **Ansible Playbook** 파일을 다운로드합니다

글로벌 검색을 수행할 때 Ansible Playbook 파일을 다운로드할 수 있습니다.

단계

1. 검색 필드에 "볼륨" 또는 "LUN" 또는 "플레이북"을 입력합니다.
2. "볼륨 관리(Ansible Playbook)" 또는 "LUN 관리(Ansible Playbook)"라는 검색 결과를 찾으세요.

3. Ansible Playbook 파일을 다운로드하려면 를 클릭하십시오.

Ansible Playbook 파일 사용

Ansible Playbook 파일을 수정하고 실행하여 볼륨 및 LUN의 구성을 지정할 수 있습니다.

이 작업에 대해

두 개의 파일을 사용하여 작업("추가" 또는 "편집")을 수행합니다.

원하는 작업	이 변수 파일 사용…	이 실행 파일 사용…
볼륨을 추가합니다	'볼륨만다변형 YAML'	Valueadd.YAML
볼륨을 편집합니다	'volumeEdit-variable.YAML'	'volumeEdit.YAML'
LUN을 추가합니다	'음주변수.YAML'	오찬 YAML
LUN을 편집합니다	오찬-변수.YAML	오찬.요아ML

단계

1. 변수 파일을 수정합니다.

   파일에는 볼륨 또는 LUN을 구성하는 데 사용되는 다양한 값이 들어 있습니다.

   - 값을 변경하지 않으면 코멘트를 남겨둡니다.
   - 값을 수정할 경우 메모를 제거합니다.

2. 연결된 실행 파일을 실행합니다.

   실행 파일에는 변수 파일에서 입력을 읽을 때 값을 만들거나 수정하는 데 필요한 테스트 사례가 들어 있습니다.

3. 사용자 로그인 자격 증명을 입력합니다.

ONTAP System Manager를 사용하여 스토리지 효율성 정책을 관리하세요

ONTAP 9.8부터 System Manager를 사용하여 FAS 시스템의 스토리지 VM에 대한 효율성 정책을 설정, 해제, 추가, 편집 또는 삭제할 수 있습니다.

AFF 시스템에서는 이 기능을 사용할 수 없습니다.

단계

1. 스토리지 > 스토리지 VM * 을 선택합니다
2. 효율성 정책을 관리할 스토리지 VM을 선택합니다.
3. 설정 * 탭에서 * 효율성 정책 * 섹션을 선택합니다 → . 해당 스토리지 VM의 효율성 정책이 표시됩니다.

다음 작업을 수행할 수 있습니다.

- * 상태 열에서 전환 버튼을 클릭하여 효율성 정책을 활성화 또는 비활성화합니다.
- * 추가 + * 를 클릭하여 효율성 정책을 추가합니다.

- * 정책 이름 오른쪽을 클릭하고 * 편집 * 을 선택하여 효율성 정책을 ⋮ 편집합니다.
- * 정책 이름 오른쪽을 클릭하고 * Delete * 를 선택하여 효율성 정책을 ⋮ 삭제합니다.

효율성 정책 목록

- * 자동 *

  백그라운드에서 중복 제거가 지속적으로 수행되도록 지정합니다. 이 정책은 새로 생성된 모든 볼륨과 백그라운드 중복제거를 위해 수동으로 구성되지 않은 업그레이드된 모든 볼륨에 대해 설정됩니다. 정책을 "기본값" 또는 다른 정책으로 변경하면 "자동" 정책이 비활성화됩니다.

  볼륨이 비 AFF 시스템에서 AFF 시스템으로 이동하는 경우 기본적으로 타겟 노드에서 ""자동"" 정책이 활성화되어 있습니다. 볼륨이 AFF 노드에서 비 AFF 노드로 이동하는 경우 대상 노드의 "자동" 정책은 기본적으로 "인라인 전용" 정책으로 대체됩니다.

- * 정책 *

  효율성 정책의 이름을 지정합니다.

- * 상태 *

  효율성 정책의 상태를 지정합니다. 상태는 다음 중 하나일 수 있습니다.

  ◦ 활성화됨

  중복 제거 작업에 효율성 정책을 할당할 수 있도록 지정합니다.

  ◦ 사용 안 함

  효율성 정책이 비활성화되도록 지정합니다. 상태 드롭다운 메뉴를 사용하여 정책을 사용하도록 설정하고 나중에 중복 제거 작업에 할당할 수 있습니다.

- * 실행 기준 *

  스토리지 효율성 정책을 스케줄에 따라 실행할지 또는 임계값(변경 로그 임계값)을 기반으로 실행할지 여부를 지정합니다.

- * QoS 정책 *

  스토리지 효율성 정책의 QoS 유형을 지정합니다. QoS 유형은 다음 중 하나일 수 있습니다.

  ◦ 배경

  QoS 정책이 백그라운드에서 실행되고 있음을 지정함으로써 클라이언트 작업에 대한 잠재적인 성능 영향을 줄입니다.

  ◦ 최선의 노력

  QoS 정책이 최선 노력 기반으로 실행되도록 지정합니다. 이를 통해 시스템 리소스 활용률을 최대화할 수 있습니다.

- * 최대 런타임 *

효율성 정책의 최대 런타임 기간을 지정합니다. 이 값을 지정하지 않으면 작업이 완료될 때까지 효율성 정책이 실행됩니다.

세부 정보 영역

효율성 정책 목록 아래의 영역에는 일정 이름, 일정 기반 정책의 일정 세부 정보, 임계값 기반 정책의 임계값 등 선택한 효율성 정책에 대한 추가 정보가 표시됩니다.

ONTAP System Manager를 사용하여 할당량을 사용하여 리소스 관리

ONTAP 9.7부터 System Manager를 사용하여 사용량 할당량을 구성 및 관리할 수 있습니다.

ONTAP CLI를 사용하여 사용 할당량을 구성 및 관리하는 경우 를 참조하십시오 "논리적 스토리지 관리".

OnCommand 9.7 및 이전 릴리즈용 기존 ONTAP System Manager를 사용하여 사용 할당량을 구성 및 관리하는 경우 릴리즈에 대한 내용은 다음을 참조하십시오.

- "ONTAP 9.7 및 9.6 문서"
- "ONTAP 9.5 문서"
- "ONTAP 9.4 문서"
- "ONTAP 9.3 문서"

할당량 개요

할당량을 통해 사용자, 그룹 또는 qtree가 사용하는 파일 수와 디스크 공간을 제한하거나 추적할 수 있습니다. 할당량은 특정 볼륨 또는 qtree에 적용됩니다.

할당량을 사용하여 볼륨의 리소스 사용량을 추적하고 제한할 수 있으며 리소스 사용량이 특정 레벨에 도달하면 알림을 제공할 수 있습니다.

할당량은 소프트 또는 하드일 수 있습니다. 소프트 할당량을 사용하면 ONTAP에서 지정된 제한을 초과할 때 알림을 보내고, 하드 할당량을 사용하면 지정된 제한을 초과할 때 쓰기 작업이 성공하지 못합니다.

ONTAP 시스템 관리자를 사용하여 리소스 사용을 제한하기 위한 할당량 설정

할당량을 추가하여 할당량 대상이 사용할 수 있는 디스크 공간의 양을 제한합니다.

할당량에 대한 하드 제한값 및 소프트 제한값을 설정할 수 있습니다.

하드 할당량은 시스템 리소스에 엄격한 제한을 부과하며, 제한을 초과하는 작업은 모두 실패합니다. 소프트 할당량은 리소스 사용량이 특정 수준에 도달해도 데이터 액세스 작업에 영향을 주지 않으므로 할당량이 초과되기 전에 적절한 조치를 취할 수 있도록 경고 메시지를 보냅니다.

단계

1. 스토리지 > 할당량 * 을 클릭합니다.
2. 추가 * 를 클릭합니다.

ONTAP 시스템 관리자를 사용하여 테스트를 위해 볼륨 및 LUN 복제

볼륨 및 LUN을 클론 복제하여 테스트를 위한 쓰기 가능한 임시 복사본을 생성할 수 있습니다. 클론은 데이터의 현재 시점 상태를 반영합니다. 또한 클론을 사용하면 운영 데이터에 대한 액세스 권한을 부여하지 않고 추가 사용자에게 데이터에 대한 액세스 권한을 부여할 수 있습니다.

시작하기 전에

FlexClone 라이센스는 이어야 합니다 "설치되어 있습니다" 스토리지 시스템에서

볼륨 클론 생성

다음과 같이 볼륨의 클론을 생성합니다.

단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 복제할 볼륨의 이름 옆에 있는 을 클릭합니다 ⋮ .
3. 목록에서 * Clone * 을 선택합니다.
4. 클론의 이름을 지정하고 다른 선택을 완료합니다.
5. 클론 * 을 클릭하고 볼륨 목록에 볼륨 클론이 나타나는지 확인합니다.

또는 * Overview * 에서 볼륨 세부 정보를 볼 때 표시되는 볼륨을 복제할 수도 있습니다.

LUN 클론 복제

활성 볼륨의 LUN을 클론 복제하여 LUN의 복사본을 생성할 수 있습니다. 이러한 FlexClone LUN은 활성 볼륨에 있는 원본 LUN의 읽기 및 쓰기 가능한 복사본입니다.

공간 예약 FlexClone LUN에는 공간 예약 상위 LUN과 동일한 공간이 필요합니다. FlexClone LUN이 공간 예약되지 않은 경우 FlexClone LUN의 변경 사항을 수용할 수 있는 충분한 공간이 볼륨에 있는지 확인해야 합니다.

ⓘ 이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 데이터를 복제합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

예 **11.** 단계

시스템 관리자

1. 스토리지 > LUN * 을 클릭합니다.
2. 클론 복제할 LUN 이름 옆의 을 클릭합니다 ⋮ .
3. 목록에서 * Clone * 을 선택합니다.
4. 클론의 이름을 지정하고 다른 선택을 완료합니다.
5. 클론 * 을 클릭하고 LUN 클론이 LUN 목록에 표시되는지 확인합니다.

또는 LUN 세부 정보를 볼 때 표시되는 * Overview * 에서 LUN을 클론 복제할 수도 있습니다.

LUN 클론을 생성할 때 공간이 필요할 때 System Manager에서 자동으로 클론 삭제를 설정합니다.

CLI를 참조하십시오

1. LUN이 igroup에 매핑되어 있지 않은지, 아니면 클론을 생성하기 전에 LUN이 에 기록되어 있는지 확인합니다.
2. 'lun show' 명령을 사용하여 LUN이 있는지 확인하십시오.

   'lun show -vserver vs1'

```
Vserver  Path               State     Mapped    Type      Size
-------- ----------------- --------- --------- -------- -------
vs1      /vol/vol1/lun1    online   unmapped  windows  47.07MB
```

3. 'volume file clone create' 명령을 사용하여 FlexClone LUN을 생성합니다.

   '볼륨 파일 클론 생성 - vserver vs1-volume vol1-source-path lun1-destination-path/lun1_clone'

   자동 삭제를 위해 FlexClone LUN을 사용할 수 있어야 하는 경우 '-autom자동 삭제 true'를 포함합니다. 반씩 프로비저닝을 사용하여 볼륨에 FlexClone LUN을 생성하는 경우 모든 FlexClone LUN에 대해 자동 삭제를 활성화해야 합니다.

4. 'lun show' 명령을 사용하여 LUN을 생성했는지 확인하십시오.

   'lun show -vserver vs1'

```
Vserver  Path                      State    Mapped   Type      Size
-------- ------------------------ -------- -------- -------- ------
vs1      /vol/volX/lun1           online   unmapped windows  47.07MB
vs1      /vol/volX/lun1_clone     online   unmapped windows  47.07MB
```

ONTAP 시스템 관리자에서 정보 검색, 필터링 및 정렬

System Manager에서 다양한 작업, 개체 및 정보 항목을 검색할 수 있습니다. 특정 항목에 대한

테이블 데이터를 검색할 수도 있습니다.

System Manager에서는 두 가지 유형의 검색을 제공합니다.

- 전체 검색

  각 페이지 상단의 필드에 검색 인수를 입력하면 System Manager가 인터페이스 전체를 검색하여 일치하는 항목을 찾습니다. 그런 다음 결과를 정렬하고 필터링할 수 있습니다.

  ONTAP 9.12.1부터 시스템 관리자는 NetApp Support 사이트에서 검색 결과를 제공하여 관련 지원 정보에 대한 링크를 제공합니다.

- 표-그리드 검색

  ONTAP 9.8부터 표 눈금 맨 위의 필드에 검색 인수를 입력하면, System Manager에서는 해당 테이블의 열과 행만 검색하여 일치하는 항목을 찾습니다.

전체 검색

System Manager의 각 페이지 맨 위에서 글로벌 검색 필드를 사용하여 인터페이스에서 다양한 개체와 작업을 검색할 수 있습니다. 예를 들어 이름, 탐색기 열(왼쪽)에서 사용할 수 있는 페이지, "볼륨 추가" 또는 "라이센스 추가"와 같은 다양한 작업 항목, 외부 도움말 항목에 대한 링크를 기준으로 다양한 개체를 검색할 수 있습니다. 결과를 필터링하고 정렬할 수도 있습니다.

더 나은 결과를 얻으려면 로그인한 후 1분, 개체를 생성, 수정 또는 삭제한 후 5분 후에 검색, 필터링 및 정렬을 수행합니다.

검색 결과를 가져오는 중입니다

검색은 대/소문자를 구분하지 않습니다. 필요한 페이지, 작업 또는 정보 항목을 찾기 위해 다양한 텍스트 문자열을 입력할 수 있습니다. 최대 20개의 결과가 나열됩니다. 더 많은 결과가 검색되면 * 더 보기 * 를 클릭하여 모든 결과를 볼 수 있습니다. 다음 예에서는 일반적인 검색을 설명합니다.

검색 유형입니다	샘플 검색 문자열	검색 결과의 예
개체 이름별	볼륨 _	스토리지 VM의 vol_LUN_dest: svm0(볼륨)/vol/vol…est1/스토리지 VM의 LUN: svm0(LUN) svm0:vol_LUN_dest1 역할: 대상(관계)
인터페이스 내 위치별	볼륨	볼륨 추가(작업) 보호 – 개요(페이지) 삭제된 볼륨 복구(도움말)
행동별	추가	볼륨 추가(작업) 네트워크 – 개요(페이지) 볼륨 및 LUN 확장(도움말)
도움말 콘텐츠별	산	스토리지 – 개요(페이지) SAN 개요(도움말) 데이터베이스를 위한 SAN 스토리지 용량 할당(도움말)

NetApp Support 사이트의 글로벌 검색 결과

ONTAP 9.12.1부터 Active IQ Digital Advisor(디지털 어드바이저)에 등록된 사용자를 위해 System Manager에는 System Manager 제품 정보를 비롯한 NetApp 지원 사이트 정보에 대한 링크를 제공하는 또 다른 결과 열이 표시됩니다.

검색 결과에 포함되는 정보는 다음과 같습니다.

- HTML, PDF, EPUB 또는 기타 형식의 문서에 대한 링크인 정보의 * 제목 *.
- * 콘텐츠 유형 * - 제품 설명서 항목인지, 기술 자료 문서 또는 다른 유형의 정보인지 여부를 식별합니다.
- * 내용에 대한 요약 설명 *.
- 처음 게시된 * 날짜.
- * 업데이트 * 마지막 업데이트 날짜.

다음 작업을 수행할 수 있습니다.

조치	결과
ONTAP 시스템 관리자 * 를 클릭한 다음 검색 필드에 텍스트를 입력합니다.	검색 결과에 시스템 관리자에 대한 NetApp Support 사이트 정보가 포함됩니다.
모든 제품 * 을 클릭한 다음 검색 필드에 텍스트를 입력합니다.	검색 결과에는 시스템 관리자뿐만 아니라 모든 NetApp 제품에 대한 NetApp Support 사이트 정보가 포함되어 있습니다.
검색 결과를 클릭합니다.	NetApp Support 사이트의 정보는 별도의 브라우저 창 또는 탭에 표시됩니다.
더 많은 결과 보기 * 를 클릭합니다.	결과가 10개 이상인 경우, 10번째 결과 뒤에 * 더 많은 결과 보기 * 를 클릭하여 더 많은 결과를 볼 수 있습니다. 더 많은 결과 보기 * 를 클릭할 때마다 가능한 경우 다른 10개의 결과가 표시됩니다.
링크를 복사합니다.	링크가 클립보드에 복사됩니다. 파일 또는 브라우저 창에 링크를 붙여 넣을 수 있습니다.
을 클릭합니다.	결과가 표시되는 패널은 다른 패널에서 작업할 때 계속 표시되도록 고정되어 있습니다.
을 클릭합니다.	결과 패널이 더 이상 고정되어 있지 않고 닫힙니다.

검색 결과 필터링

다음 예와 같이 필터를 사용하여 결과의 범위를 좁힐 수 있습니다.

필터	구문	샘플 검색 문자열
개체 유형별	type>:<objectName>	볼륨: vol_2

개체 크기별	type><size-symbol><number><units>	LUN < 500MB
손상된 디스크로	"손상된 디스크" 또는 "건강에 해로운 디스크"	디스크가 정상 상태가 아닙니다
네트워크 인터페이스	IP 주소>	172.22.108.21

검색 결과 정렬

모든 검색 결과를 볼 때 알파벳 순으로 정렬됩니다. 을 클릭하고 결과를 정렬할 방법을 선택하여 결과를 정렬할 수 Filter 있습니다.

표-그리드 검색

ONTAP 9.8부터 System Manager가 테이블 그리드 형식으로 정보를 표시할 때마다 테이블 상단에 검색 단추가 나타납니다.

검색 * 을 클릭하면 검색 인수를 입력할 수 있는 텍스트 필드가 나타납니다. System Manager는 전체 테이블을 검색하여 검색 인수와 일치하는 텍스트를 포함하는 행만 표시합니다.

별표(*)를 문자 대신 "와일드카드" 문자로 사용할 수 있습니다. 예를 들어, 'vol *'을 검색하면 다음 항목이 포함된 행이 제공됩니다.

- Vol_122_D9
- vol_LUN_dest1
- vol2866
- 볼륨1
- Volum_dest_765
- 볼륨
- VOLUME_new4
- 볼륨 9987

CLI를 통한 논리적 스토리지 관리

CLI를 통한 논리적 스토리지 관리 개요

ONTAP CLI를 사용하면 FlexVol 볼륨을 생성 및 관리하고, FlexClone 기술을 사용하여 볼륨, 파일 및 LUN의 효율적인 복사본을 생성하고, qtree 및 할당량을 생성하고, 중복제거 및 압축과 같은 효율성 기능을 관리할 수 있습니다.

다음과 같은 상황에서 이러한 절차를 사용해야 합니다.

- ONTAP FlexVol의 볼륨 기능 및 스토리지 효율성 기능에 대해 알고 싶어 합니다.
- System Manager나 자동화된 스크립팅 도구가 아니라 CLI(Command-Line Interface)를 사용하려는 경우

볼륨 생성 및 관리

볼륨을 생성합니다

볼륨을 생성하고 "volume create" 명령을 사용하여 해당 접합 지점 및 기타 속성을 지정할 수 있습니다.

이 작업에 대해

클라이언트에서 데이터를 사용할 수 있도록 하려면 볼륨에 _junction path_가 포함되어야 합니다. 새 볼륨을 생성할 때 접합 경로를 지정할 수 있습니다. 접합 경로를 지정하지 않고 볼륨을 생성하는 경우, "volume mount" 명령을 사용하여 SVM 네임스페이스에서 볼륨을 _mount_해야 합니다.

시작하기 전에

- 새 볼륨용 SVM과 볼륨에 스토리지를 제공할 애그리게이트가 이미 존재해야 합니다.
- SVM에 관련 애그리게이트 목록이 있는 경우, 애그리게이트를 목록에 포함해야 합니다.
- ONTAP 9.13.1부터 용량 분석 및 활동 추적이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 `volume create` 또는 `-activity-tracking-state` 를 로 설정하여 `on` 명령을 `-analytics-state` 실행합니다.

  용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 "파일 시스템 분석 설정". 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 볼륨 생성:

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -user
   user_name_or_number -group group_name_or_number -junction-path junction_path
   [-policy export_policy_name]
   ```

   보안스타일, 사용자 그룹, 교차경로, 정책 옵션은 NAS 네임스페이스에만 사용됩니다.

   '-junction-path'의 선택 항목은 다음과 같습니다.

   - 루트 바로 아래, 예: '/new_vol'

     새 볼륨을 생성하고 SVM 루트 볼륨에 직접 마운트하도록 지정할 수 있습니다.

   - 기존 디렉토리 아래에 '/existing_dir/new_vol' 등이 있습니다

     새 볼륨을 생성하고 기존 계층 구조에서 기존 볼륨에 마운트하도록 지정할 수 있습니다. 이 볼륨은 디렉토리로 표시됩니다.

   새 볼륨 아래의 새 계층 구조에서 "/new_dir/new_vol"과 같은 새 디렉토리에 볼륨을 생성하려면 먼저 SVM 루트 볼륨에 대한 분기인 새 상위 볼륨을 생성해야 합니다. 그런 다음 새 상위 볼륨(새 디렉토리)의 접합 경로에 새 하위 볼륨을 생성합니다.

2. 볼륨이 원하는 접합 지점으로 생성되었는지 확인합니다.

`volume show -vserver svm_name -volume volume_name -junction`

에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 명령을 실행하면 SVM에 user1이라는 새 볼륨이 생성됩니다 `vs1.example.com` 집계 `aggr1`. 새 볼륨은 에서 사용할 수 있습니다 `/users`. 볼륨의 크기는 750GB이고 볼륨 유형은 볼륨 유형입니다(기본값).

```
cluster1::> volume create -vserver vs1.example.com -volume users1
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users1 -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- -------  -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

다음 명령을 실행하면 SVM의 ""home4" vs1.example.com`""와 애그리게이트 ""aggr1""에 새 볼륨이 생성됩니다. VS1 SVM은 이름 공간에 /ENG/ 디렉토리가 이미 있으며, '/ENG/' 네임스페이스의 홈 디렉토리가 되는 '/ENG/HOME'에서 새 볼륨을 사용할 수 있습니다. 볼륨 크기는 750GB이고 볼륨 보장은 볼륨 유형입니다(기본값).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   Path Source
---------------- -------  -------- --------------- -----------
vs1.example.com  home4    true     /eng/home       RW_volume
```

ONTAP에서 대용량 및 대용량 파일 지원을 지원합니다

ONTAP 9.12.1 P2부터 새 볼륨을 생성하거나 기존 볼륨을 수정하여 최대 볼륨 크기 300TB, 최대 크기 60PB 및 최대 파일(LUN) 크기 128TB를 지원할 수 "FlexGroup 볼륨"있습니다.

시작하기 전에

- ONTAP 9.12.1 P2 이상이 클러스터에 설치되어 있습니다.
- SnapMirror 관계에서 소스 클러스터에서 대규모 볼륨 지원을 활성화하려면 소스 볼륨을 호스팅하는 클러스터와 대상 볼륨을 호스팅하는 클러스터에 ONTAP 9.12.1 P2 이상이 설치되어 있어야 합니다.
- 귀하는 클러스터 또는 SVM 관리자입니다.
- 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

새 볼륨을 생성합니다

단계

1. 대용량 볼륨 및 파일 지원이 활성화된 볼륨 생성:

```
volume create -vserver <svm_name> -volume <volume_name> -aggregate
<aggregate_name> -is-large-size-enabled true
```

예

다음 예에서는 대용량 및 파일 크기 지원이 활성화된 새 볼륨을 생성합니다.

```
volume create -vserver vs1 -volume big_vol1 -aggregate aggr1 -is-large
-size-enabled true
```

기존 볼륨을 수정합니다

단계

1. 볼륨을 수정하여 대용량 볼륨 및 파일 지원:

```
volume modify -vserver <svm_name> -volume <volume_name> -is-large-size
-enabled true
```

예

다음 예에서는 큰 볼륨과 파일 크기를 지원하도록 기존 볼륨을 수정합니다.

```
volume modify -vserver vs2 -volume data_vol -is-large-size-enabled true
```

2. 볼륨을 다시 마운트하여 새 구성 설정을 활성화합니다.

```
volume unmount -vserver <svm_name> -volume <volume_name>
```

```
volume mount -vserver <svm_name> -volume <volume_name>
```

관련 정보

- "ONTAP NFS 볼륨 생성"
- "ONTAP 명령 참조입니다"

SAN 볼륨

SAN 볼륨 프로비저닝 개요

ONTAP는 SAN 볼륨 프로비저닝을 위한 몇 가지 기본 옵션을 제공합니다. 각 옵션에서는 ONTAP 블록 공유 기술에 대한 볼륨 공간 및 공간 요구사항을 관리하는 다른 방법을 사용합니다. 각 프로비저닝 옵션이 어떻게 작동하는지 이해하면 환경에 가장 적합한 옵션을 선택할 수 있습니다.

SAN LUN과 NAS 공유를 동일한 FlexVol volume에 배치하는 것은 권장되지 않습니다. 대신 SAN LUN과 NAS 공유에 대해 별도의 FlexVol 볼륨을 프로비저닝해야 합니다. 따라서 관리 및 복제 구축이 간소화됩니다. 또한 Active IQ Unified Manager(이전의 OnCommand Unified Manager)에서 FlexVol 볼륨이 지원되는 방식과 유사합니다.

볼륨에 대한 씬 프로비저닝

씬 프로비저닝된 볼륨이 생성된 경우 ONTAP는 볼륨이 생성될 때 추가 공간을 예약하지 않습니다. 볼륨에 데이터가 기록될 때 볼륨은 쓰기 작업을 수용하기 위해 Aggregate에서 필요한 스토리지를 요청합니다. 씬 프로비저닝된 볼륨을 사용하면 애그리게이트를 오버 커밋할 수 있으므로 애그리게이트에 여유 공간이 부족할 때 볼륨이 필요한 공간을 확보할 수 없게 됩니다.

'-space-보증' 옵션을 '없음'으로 설정하여 씬 프로비저닝된 FlexVol 볼륨을 만듭니다.

볼륨에 대한 일반 프로비저닝입니다

씩 프로비저닝된 볼륨이 생성되면 ONTAP는 언제든지 볼륨의 블록을 쓸 수 있도록 애그리게이트에 충분한 스토리지를 남겨 둡니다. 일반 프로비저닝을 사용하도록 볼륨을 구성할 경우 압축 및 중복제거와 같은 ONTAP 스토리지 효율성 기능을 사용하여 대규모 초기 스토리지 요구사항을 상쇄할 수 있습니다.

'-space-slo'(서비스 수준 목표) 옵션을 'thick'으로 설정하여 씩 프로비저닝된 FlexVol 볼륨을 만듭니다.

볼륨에 반씩 프로비저닝

반씩 프로비저닝을 사용하는 볼륨이 생성된 경우 ONTAP에서는 애그리게이트에서 볼륨 크기를 고려하여 스토리지 공간을 별도로 설정합니다. 블록 공유 기술에서 블록을 사용하고 있기 때문에 볼륨에 여유 공간이 부족해지면 ONTAP이 보호 데이터 오브젝트(스냅샷 및 FlexClone 파일 및 LUN)를 삭제하여 보유 중인 공간을 확보하도록 시도합니다. ONTAP가 덮어쓰기 작업에 필요한 공간과 보조를 맞출 수 있을 만큼 보호 데이터 객체를 빠르게 삭제할 수 있는 한 쓰기 작업은 계속 성공합니다. 이를 '최선 노력'이라고 합니다.

반씩 프로비저닝을 사용하는 볼륨에는 중복제거, 압축, 컴팩션과 같은 스토리지 효율성 기술을 사용할 수 없습니다.

semi-thick-provisioned FlexVol 볼륨은 '-space-slo'(서비스 수준 목표) 옵션을 'sEMI-thick'으로 설정하여 생성합니다.

공간 예약 파일 및 LUN과 함께 사용

공간 예약 파일 또는 LUN은 생성 시 스토리지가 할당되는 파일입니다. 역사적으로 NetApp은 공간 예약이 사용되지 않는 LUN(비공간 예약 LUN)을 지칭하기 위해 ""씬 프로비저닝된 LUN"이라는 용어를 사용했습니다.

공간이 예약되지 않은 파일은 일반적으로 ""씬 프로비저닝 파일"이라고 하지 않습니다.

다음 표에는 세 가지 볼륨 프로비저닝 옵션을 공간 예약 파일 및 LUN과 함께 사용하는 방법의 주요 차이점이 요약되어 있습니다.

볼륨 프로비저닝	**LUN**/파일 공간 예약	덮어쓰기	보호 데이터 [2]	스토리지 효율성 [3]
두껍게	지원	[1]을(를) 보장합니다	NetApp이 보장합니다	지원
얇음	효과 없음	없음	NetApp이 보장합니다	지원
약간 두껍습니다	지원	최선의 노력 [1]	최선을 다하세요	지원되지 않습니다

- 참고 *
  1. 덮어쓰기 보장 또는 최선의 덮어쓰기 보장을 제공하려면 LUN 또는 파일에 공간 예약을 설정해야 합니다.
  2. 보호 데이터에는 스냅샷, 자동 삭제로 표시된 FlexClone 파일 및 LUN(백업 클론)이 포함됩니다.
  3. 스토리지 효율성에는 중복제거, 압축, 자동 삭제로 표시되지 않은 모든 FlexClone 파일 및 LUN(활성 클론), FlexClone 하위 파일(복사본 오프로드로 사용)이 포함됩니다.

SCSI 씬 프로비저닝된 **LUN** 지원

ONTAP는 T10 SCSI 씬 프로비저닝 LUN과 NetApp 씬 프로비저닝 LUN을 지원합니다. T10 SCSI 씬 프로비저닝을 사용하면 호스트 애플리케이션에서 LUN 공간 재확보, 블록 환경의 LUN 공간 모니터링 기능 등 SCSI 기능을 지원할 수 있습니다. T10 SCSI 씬 프로비저닝은 SCSI 호스트 소프트웨어에서 지원해야 합니다.

ONTAP의 pace-allocation 설정을 사용하면 LUN에서 T10 씬 프로비저닝 지원을 활성화/비활성화할 수 있습니다. ONTAP의 pace-allocation enable 설정을 사용하여 LUN에 T10 SCSI 씬 프로비저닝을 활성화합니다.

그만큼 `[-space-allocation {enabled|disabled}]` 에서 명령 "ONTAP 명령 참조입니다" T10 씬 프로비저닝에 대한 지원을 활성화/비활성화하고 LUN에서 T10 SCSI 씬 프로비저닝을 활성화하는 방법에 대한 자세한 정보가 있습니다.

볼륨 프로비저닝 옵션을 구성합니다

공간 요구 사항에 따라 씬 프로비저닝, 일반 프로비저닝 또는 반씩 프로비저닝을 위해 볼륨을 구성할 수 있습니다.

이 작업에 대해

'-space-slo' 옵션을 'thick'으로 설정하면 다음과 같은 이점이 있습니다.

- 전체 볼륨이 Aggregate에 사전 할당됩니다. 볼륨의 '-space-보증' 옵션을 구성하려면 'volume create' 또는 'volume modify' 명령을 사용할 수 없습니다.
- 덮어쓰기에 필요한 공간의 100%가 예약됩니다. 볼륨의 '-fractional-reserve' 옵션을 구성하려면 'volume modify' 명령을 사용할 수 없습니다

'-space-slo' 옵션을 'EMI-thick'으로 설정하면 다음과 같은 이점이 있습니다.

- 전체 볼륨이 Aggregate에 사전 할당됩니다. 볼륨의 '-space-보증' 옵션을 구성하려면 'volume create' 또는 'volume modify' 명령을 사용할 수 없습니다.

- 덮어쓰기용으로 예약된 공간이 없습니다. 'volume modify' 명령을 사용하여 볼륨의 '-fractional-reserve' 옵션을 구성할 수 있습니다.
- 스냅샷 자동 삭제가 설정되었습니다.

단계

1. 볼륨 프로비저닝 옵션 구성:

   'volume create-vserver_vserver_name_-volume_volume_name_-aggregate_aggregate_name_-space-slo none|thick|semi-thick-space-보증 없음|볼륨'

   '-space-보증' 옵션은 AFF 시스템과 비 AFF DP 볼륨에 대해 기본적으로 '없음'으로 설정됩니다. 그렇지 않으면 볼륨(volume)으로 기본 설정됩니다. 기존 FlexVol 볼륨의 경우 'volume modify' 명령을 사용하여 프로비저닝 옵션을 구성합니다.

   다음 명령은 씬 프로비저닝을 위해 SVM VS1 에서 vol1을 구성합니다.

   ```
   cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee
   none
   ```

   다음 명령을 실행하면 일반 프로비저닝을 위해 SVM VS1 vol1에 대해 vol1이 구성됩니다.

   ```
   cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
   ```

   다음 명령을 실행하면 반씩 프로비저닝을 위해 SVM VS1 vol1에 대해 vol1이 구성됩니다.

   ```
   cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-
   thick
   ```

관련 정보

- "볼륨 생성"
- "볼륨 수정"

ONTAP에서 볼륨 또는 애그리게이트의 공간 사용량을 확인합니다

경우에 따라 ONTAP에서 기능을 사용하도록 설정하는 데 예상보다 많은 공간이 필요할 수 있습니다. ONTAP은 공간을 볼 수 있는 세 가지 관점, 즉 볼륨, 애그리게이트 내 볼륨 공간 및 애그리게이트의 공간을 제공하여 공간이 얼마나 소비되는지를 결정하도록 지원합니다.

공간 할당을 봅니다

볼륨, 애그리게이트 또는 둘 모두의 조합 내에 공간 소비나 공간이 부족하여 볼륨이 공간 부족 으로 인해 실행될 수 있습니다. 다양한 관점에서 공간 사용량을 기능 중심으로 분석함으로써 어떤 기능을 조정하거나 해제할지 또는 다른 작업을 수행해야 하는지(예: 집계 또는 볼륨 크기 증가) 평가할 수 있습니다.

다음과 같은 관점에서 공간 사용 세부 정보를 볼 수 있습니다.

- 볼륨의 공간 사용량입니다

  이 관점은 스냅샷별 사용을 포함하여 볼륨 내의 공간 사용량에 대한 세부 정보를 제공합니다.

  를 사용합니다 `volume show-space` 볼륨의 공간 사용량을 확인하는 명령입니다.

  에 대한 자세한 내용은 `volume show-space` "ONTAP 명령 참조입니다"을 참조하십시오.

  ONTAP 9.14.1부터, 를 포함한 볼륨에서 실행됩니다 온도에 민감한 스토리지 효율성(TSSE) Enabled(사용) - 에서 보고한 볼륨에서 사용된 공간의 크기입니다 `volume show-space -physical used` 명령에는 TSSE를 통해 실현된 공간 절약 효과가 포함됩니다.

- 애그리게이트 내 볼륨의 설치 공간

  이 관점에서는 볼륨의 메타데이터를 포함하여 각 볼륨이 포함하는 애그리게이트에서 사용하는 공간의 양에 대한 자세한 정보를 제공합니다.

  를 사용합니다 `volume show-footprint` 명령을 사용하여 애그리게이트와 함께 볼륨의 설치 공간을 확인합니다.

  에 대한 자세한 내용은 `volume show-footprint` "ONTAP 명령 참조입니다"을 참조하십시오.

- 애그리게이트의 공간 사용

  이 관점에는 애그리게이트에 포함된 모든 볼륨의 볼륨 설치 공간, 애그리게이트 스냅샷을 위해 예약된 공간 및 기타 애그리게이트 메타데이터의 합계가 포함됩니다.

  WAFL는 애그리게이트 레벨의 메타데이터 및 성능을 위해 전체 디스크 공간의 10%를 예약합니다. Aggregate에서 볼륨을 유지 관리하는 데 사용되는 공간은 WAFL 예비 공간에서 나오며 변경할 수 없습니다.

  ONTAP 9.12.1부터는 AFF 플랫폼 및 FAS500f 플랫폼에 대해 30TB 이상의 애그리게이트에 대한 WAFL 예비 공간이 10%에서 5%로 줄어듭니다. ONTAP 9.14.1부터 이와 같은 축소 효과는 모든 FAS 플랫폼의 애그리게이트에 적용됩니다. 따라서 애그리게이트에서 사용 가능한 공간이 5% 더 많아집니다.

  를 사용합니다 `storage aggregate show-space` 명령을 사용하여 애그리게이트의 공간 사용량을 확인합니다.

  에 대한 자세한 내용은 `storage aggregate show-space` "ONTAP 명령 참조입니다"을 참조하십시오.

테이프 백업 및 중복 제거와 같은 특정 기능은 메타데이터의 공간을 볼륨과 애그리게이트에서 직접 사용합니다. 이러한 기능은 볼륨 및 볼륨 풋프린트의 관점에서 다양한 공간 사용을 보여줍니다.

볼륨 메타데이터 및 데이터 메트릭 보고

일반적으로 여러 볼륨 공간 메트릭에서 메타데이터와 사용자 데이터라는 두 가지 메트릭의 조합으로 사용된 총 데이터를 보고했습니다. ONTAP 9.15.1부터 메타데이터와 사용자 데이터 메트릭이 별도로 보고됩니다. 이를 지원하기 위해 두 개의 새로운 메타데이터 카운터가 도입되었습니다.

- 총 메타데이터

  이 카운터는 볼륨 내의 총 메타데이터 크기를 제공합니다. 애그리게이트 상주 볼륨 메타데이터는 포함되지 않습니다. 별도로 보고하면 사용자가 할당한 논리적 데이터를 확인하는 데 도움이 됩니다.

- 총 메타데이터 설치 공간

  이 카운터는 볼륨 상주 메타데이터와 애그리게이트 상주 볼륨 메타데이터의 합계입니다. 애그리게이트 내 볼륨의 총 메타데이터 사용 공간을 제공합니다. 별도로 보고하면 사용자가 할당한 물리적 데이터를 확인하는 데 도움이 됩니다.

또한 메타데이터 구성 요소를 제거하고 사용자 데이터만 표시하도록 몇 개의 기존 카운터가 업데이트되었습니다.

- 사용자 데이터
- 볼륨 데이터 공간

이러한 변경 사항을 통해 사용자가 소비한 데이터를 보다 정확하게 볼 수 있습니다. 이를 통해 보다 정확한 비용 청구 결정을 내릴 수 있는 기능 등 여러 가지 이점을 얻을 수 있습니다.

관련 정보

- "NetApp 지식 기반: 공간 사용"
- "ONTAP 9.12.1로 업그레이드하여 스토리지 용량의 5%를 확보하십시오"

공간을 관리하기 위해 자동 스냅샷 및 **LUN** 삭제를 활성화합니다

스냅샷 및 FlexClone LUN을 자동으로 삭제하는 정책을 정의하고 설정할 수 있습니다. 스냅샷 및 FlexClone LUN을 자동으로 삭제하면 공간 활용도를 관리하는 데 도움이 됩니다.

이 작업에 대해

읽기-쓰기 볼륨의 스냅숏과 읽기-쓰기 상위 볼륨의 FlexClone LUN을 자동으로 삭제할 수 있습니다. 읽기 전용 볼륨(예: SnapMirror 대상 볼륨)에서 스냅샷 자동 삭제를 설정할 수 없습니다.

단계

1. 명령을 사용하여 스냅샷을 자동으로 삭제하는 정책을 정의하고 `volume snapshot autodelete modify` 설정합니다.

   에서 요구 사항을 충족하는 정책을 정의하고 에 대해 자세히 `volume snapshot autodelete modify`"ONTAP 명령 참조입니다" 알아보십시오.

   다음 명령을 실행하면 스냅샷을 자동으로 삭제할 수 있고 vs0.example.com SVM(스토리지 가상 머신)의 일부인 vol3 볼륨에 대한 트리거를 로 설정합니다 `snap_reserve`.

   ```
   cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
   -volume vol3 -enabled true -trigger snap_reserve
   ```

   다음 명령을 실행하면 vs0.example.com SVM(스토리지 가상 머신)의 일부인 vol3 볼륨에 대해 자동 삭제하도록 표시된 FlexClone LUN과 스냅샷의 자동 삭제가 활성화됩니다.

   ```
   cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
   -volume vol3 -enabled true -trigger volume -commitment try -delete-order
   oldest_first -destroy-list lun_clone,file_clone
   ```

애그리게이트 레벨 스냅샷은 볼륨 레벨 스냅샷과 다르게 작동하며 ONTAP을 통해 자동으로 관리됩니다. 애그리게이트 스냅샷을 삭제하는 옵션은 항상 활성화되어 공간 활용률을 관리하는 데 도움이 됩니다.

애그리게이트에 대해 트리거 매개 변수가 (으)로 설정된 `snap_reserve` 경우 예약된 공간이 임계값 용량을 넘어설 때까지 스냅샷이 유지됩니다. 따라서 trigger 매개 변수가 로 설정되어 있지 않은 경우에도 `snap_reserve` 해당 스냅샷이 자동으로 삭제되기 때문에 명령에서 스냅샷에 사용된 공간이 로 `0` 나열됩니다. 또한 애그리게이트에서 스냅샷이 사용하는 공간은 사용 가능한 공간으로 간주되며 명령의 가용 공간 매개 변수에 포함됩니다.

볼륨이 꽉 차면 자동으로 더 많은 공간을 제공하도록 볼륨을 구성합니다

FlexVol 볼륨이 꽉 차면 ONTAP는 다양한 방법을 사용하여 볼륨에 사용 가능한 공간을 자동으로 더 많이 제공할 수 있습니다. ONTAP에서 사용할 수 있는 방법과 애플리케이션 및 스토리지 아키텍처의 요구사항에 따라 사용할 순서를 선택할 수 있습니다.

이 작업에 대해

ONTAP는 다음 방법 중 하나 또는 모두를 사용하여 전체 볼륨에 더 많은 여유 공간을 자동으로 제공할 수 있습니다.

- 볼륨의 크기를 늘립니다(자동 증가).

  이 방법은 Aggregate가 포함된 볼륨에 더 큰 볼륨을 지원할 수 있는 충분한 공간이 있는 경우에 유용합니다. 볼륨에 대한 최대 크기를 설정하도록 ONTAP를 구성할 수 있습니다. 증가값은 사용된 공간의 현재 양과 설정된 임계값을 기준으로 볼륨에 기록되는 데이터의 양을 기준으로 자동으로 트리거됩니다.

  스냅샷 생성을 지원하기 위해 자동 확장이 트리거되지 않습니다. 스냅샷을 생성하려고 하는데 공간이 부족하면 자동 증가가 설정된 경우에도 스냅샷 생성이 실패합니다.

- 스냅샷, FlexClone 파일 또는 FlexClone LUN을 삭제합니다.

  예를 들어 클론 복제된 볼륨 또는 LUN의 스냅샷에 연결되지 않은 스냅샷을 자동으로 삭제하도록 ONTAP를 구성하거나 ONTAP에서 가장 오래된 스냅샷 또는 최신 스냅샷을 먼저 삭제할 스냅샷을 정의할 수 있습니다. 또한 볼륨이 거의 가득 차거나 볼륨의 스냅숏 예비 공간이 거의 가득 찬 경우와 같이 ONTAP에서 스냅숏 삭제를 시작해야 하는 시기를 결정할 수 있습니다.

이 두 방법을 모두 사용하면 볼륨이 거의 꽉 찼을 때 ONTAP에서 먼저 시도하는 방법을 지정할 수 있습니다. 첫 번째 방법이 볼륨에 충분한 추가 공간을 제공하지 않으면 ONTAP는 다음 방법을 시도합니다.

기본적으로 ONTAP에서는 볼륨의 크기를 먼저 늘리려고 합니다. 스냅샷이 삭제되면 복구할 수 없기 때문에 대부분의 경우 기본 구성이 더 좋습니다. 그러나 가능한 경우 볼륨 크기를 늘리지 않도록 해야 하는 경우 볼륨 크기를 늘리기 전에 스냅샷을 삭제하도록 ONTAP를 구성할 수 있습니다.

단계

1. ONTAP에서 볼륨이 꽉 찰 때 볼륨 크기를 늘리려고 시도하려면 와 함께 명령을 `grow` 사용하여 볼륨에 대한 자동 확장 기능을 사용하도록 `volume autosize` 설정합니다. 에 대한 자세한 내용은 `volume autosize` "ONTAP 명령 참조입니다"을 참조하십시오.

   볼륨이 증가할수록 연결된 애그리게이트로부터 더 많은 여유 공간이 소모된다는 점을 기억하십시오. 필요할 때마다 볼륨의 확장 능력에 따라 관련 애그리게이트의 여유 공간을 모니터링하고 필요 시 추가 를 추가해야 합니다.

2. 볼륨이 가득 찰 때 ONTAP에서 스냅샷, FlexClone 파일 또는 FlexClone LUN을 삭제하도록 하려면 해당 객체 유형에 대해 자동 삭제를 설정합니다.
3. 볼륨 자동 확장 기능과 하나 이상의 자동 삭제 기능을 모두 활성화한 경우, 명령을 옵션과 함께 `-space-mgmt -try-first` 사용하여 ONTAP에서 볼륨에 여유 공간을 제공하는 데 사용할 첫 번째 방법을 선택합니다 `volume modify`. 에 대한 자세한 내용은 `volume modify` "ONTAP 명령 참조입니다"을 참조하십시오.

   볼륨 크기를 먼저 늘리도록 지정하려면(기본값) 을 `volume_grow`사용합니다. 먼저 스냅샷 삭제를 지정하려면 을 `snap_delete`사용합니다.

크기를 자동으로 확대 및 축소하도록 볼륨을 구성합니다

FlexVol 볼륨이 현재 필요한 공간에 따라 자동으로 확장 및 축소되도록 구성할 수 있습니다. 자동 증가를 통해 aggregate에서 공간을 더 많이 제공할 경우 볼륨 공간이 부족해지는 것을 방지할 수 있습니다. 자동 축소는 볼륨이 필요한 크기보다 커지는 것을 방지하여 Aggregate의 공간을 다른 볼륨에서 사용할 수 있도록 합니다.

이 작업에 대해

자동 축소는 자동 증가 와 함께 사용할 경우에만 변화하는 공간 요구를 충족할 수 있으며 단독으로 사용할 수는 없습니다. 자동 축소가 활성화되면 ONTAP는 볼륨의 축소 동작을 자동으로 관리하여 자동 증가 및 자동 축소 작업이 무한 루프를 방지합니다.

볼륨이 증가하면 포함할 수 있는 최대 파일 수가 자동으로 증가할 수 있습니다. 볼륨이 축소되면 포함할 수 있는 최대 파일 수가 변경되지 않고 그대로 남아 있으며 볼륨은 현재 최대 파일 수에 해당하는 크기보다 자동으로 축소될 수 없습니다. 따라서 볼륨을 원래 크기로 자동 축소하지 못할 수 있습니다.

기본적으로 볼륨을 확장할 수 있는 최대 크기는 자동 확장이 설정된 크기의 120%입니다. 볼륨이 이보다 더 크게 증가할 수 있도록 해야 하는 경우 볼륨에 대한 최대 크기를 적절하게 설정해야 합니다.

시작하기 전에

FlexVol 볼륨이 온라인 상태여야 합니다.

단계

1. 크기를 자동으로 확대 및 축소하도록 볼륨 구성:

   ```
   volume autosize -vserver SVM_name -volume volume_name -mode grow_shrink
   ```

   다음 명령을 실행하면 test2라는 볼륨에 대한 자동 크기 변경이 설정됩니다. 볼륨이 60% 차면 축소하기 시작하도록 구성됩니다. 기본값은 확장이 시작되는 시기 및 최대 크기에 사용됩니다.

   ```
   cluster1::> volume autosize -vserver vs2 test2 -shrink-threshold-percent
   60
   vol autosize: Flexible volume "vs2:test2" autosize settings UPDATED.

   Volume modify successful on volume: test2
   ```

자동 축소 기능은 특정 구성 요구 사항이 충족되는 경우 자동 스냅샷 삭제와 함께 사용할 수 있습니다.

자동 축소 기능과 자동 스냅샷 삭제를 모두 사용하려면 구성이 다음 요구 사항을 충족해야 합니다.

- 스냅샷을 삭제하기 전에 볼륨 크기를 늘리도록 ONTAP를 구성해야 합니다(`-space-mgmt-try-first`옵션을 로 설정해야 함 `volume_grow`).
- 자동 스냅샷 삭제 트리거는 볼륨이 가득 찼어야 합니다(`trigger`매개 변수를 로 설정해야 `volume` 함).

자동 축소 기능은 FlexVol volume 크기를 축소하므로 볼륨 스냅샷이 자동으로 삭제되는 경우에도 영향을 미칠 수 있습니다.

자동 축소 기능은 다음과 같은 방법으로 자동 볼륨 스냅샷 삭제와 상호 작용합니다.

- 자동 크기 조정 모드와 자동 스냅샷 삭제가 모두 설정된 경우 `grow_shrink` 볼륨 크기가 축소되면 자동 스냅샷 삭제를 트리거할 수 있습니다.

  이는 스냅샷 예비 공간이 볼륨 크기의 비율(기본적으로 5%)을 기반으로 하며 이 비율은 더 작은 볼륨 크기를 기준으로 하기 때문입니다. 이로 인해 스냅샷이 예약에서 유출되어 자동으로 삭제될 수 있습니다.

- `grow_shrink`자동 크기 조정 모드가 설정되어 있고 스냅샷을 수동으로 삭제하면 자동 볼륨 축소가 트리거될 수 있습니다.

ONTAP는 FlexVol 볼륨 공간이 부족할 때 EMS 메시지를 발행하므로 전체 볼륨에 더 많은 공간을 제공하여 수정 조치를 취할 수 있습니다. 알림의 유형과 해결 방법을 알면 데이터 가용성을 보장하는 데 도움이 됩니다.

볼륨이 _FULL_으로 설명되면 활성 파일 시스템(사용자 데이터)에서 사용할 수 있는 볼륨의 공간 백분율이 (구성 가능) 임계값 아래로 떨어졌다는 의미입니다. 볼륨이 _overallocated_가 되면 ONTAP에서 메타데이터에 사용하고 기본 데이터 액세스를 지원하는 데 사용하는 공간이 소진되었습니다. 경우에 따라 다른 목적으로 일반적으로 예약된 공간을 사용하여 볼륨 기능을 유지할 수 있지만, 공간 예약 또는 데이터 가용성이 위험할 수 있습니다.

초과 할당은 논리적 또는 물리적 할당일 수 있습니다. _논리적 초과 할당_은 공간 예약과 같은 향후 공간 약속을 지키기 위해 예약된 공간이 다른 용도로 사용되었음을 의미합니다. _physical overallocation_은 볼륨에서 사용할 물리적 블록이 부족함을 의미합니다. 이 상태의 볼륨은 쓰기를 거부하거나, 오프라인 상태가 되거나, 컨트롤러 중단을 일으킬 위험이 있습니다.

메타데이터에서 사용되거나 예약된 공간이 있기 때문에 볼륨에는 100% 이상의 공간이 부족할 수 있습니다. 그러나 100% 이상의 꽉 찬 볼륨은 초과 할당되거나 할당되지 않을 수 있습니다. qtree 레벨 및 볼륨 레벨 공유가 동일한 FlexVol 또는 SCVMM 풀에 있을 경우 qtree가 FlexVol 공유의 디렉토리로 표시됩니다. 따라서 실수로 삭제하지 않도록 주의해야 합니다.

다음 표는 볼륨 충만 및 초과 할당 알림, 문제 해결을 위해 취할 수 있는 조치 및 조치를 취하지 않을 경우의 위험에 대해 설명합니다.

경고 유형	**EMS** 레벨	구성 가능**?**	정의	해결 방법	조치를 취하지 않을 경우 위험이 있습니다
거의 꽉 찼습니다	디버그	예	파일 시스템이 이 알림에 대해 설정된 임계값을 초과했습니다(기본값은 95%). 이 백분율은 총 값에서 `Used` 스냅숏 예비 공간의 크기를 뺀 값입니다.	• 볼륨 크기를 늘리는 중입니다 • 사용자 데이터 감소	아직 쓰기 작업 또는 데이터 가용성에 대한 위험이 없습니다.
가득 참	디버그	예	파일 시스템이 이 알림에 대해 설정된 임계값을 초과했습니다(기본값은 98%). 이 백분율은 총 값에서 `Used` 스냅숏 예비 공간의 크기를 뺀 값입니다.	• 볼륨 크기를 늘리는 중입니다 • 사용자 데이터 감소	아직 쓰기 작업 또는 데이터 가용성에 대한 위험이 없지만 쓰기 작업이 위험한 단계에 볼륨이 접근하고 있습니다.
논리적으로 초과 할당됨	SVC 오류입니다	해당 없음	파일 시스템이 꽉 찬 것 외에도 메타데이터에 사용된 볼륨의 공간이 소진되었습니다.	• 볼륨 크기를 늘리는 중입니다 • 스냅샷을 삭제하는 중입니다 • 사용자 데이터 감소 • 파일 또는 LUN에 대한 공간 예약을 사용하지 않도록 설정합니다	예약되지 않은 파일에 대한 쓰기 작업이 실패할 수 있습니다.
물리적으로 초과 할당되었습니다	노드 오류입니다	해당 없음	볼륨에 쓸 수 있는 물리적 블록이 부족하고 있습니다.	• 볼륨 크기를 늘리는 중입니다 • 스냅샷을 삭제하는 중입니다 • 사용자 데이터 감소	쓰기 작업이 위험에 처하고 데이터 가용성이 향상됩니다. 볼륨이 오프라인 상태가 될 수 있습니다.

전체 백분율 상승 또는 하강 여부와 관계없이 볼륨에 대한 임계값을 초과할 때마다 EMS 메시지가 생성됩니다. 전체 볼륨 레벨이 임계값 아래로 떨어지면 'volume ok' EMS 메시지가 생성됩니다.

애그리게이트 전체도 및 초과 할당 경고를 처리합니다

ONTAP는 Aggregate의 공간이 부족할 때 EMS 메시지를 발행하므로 전체 애그리게이트에 더 많은 공간을 제공하여 수정 조치를 취할 수 있습니다. 알림의 유형과 해결 방법을 알면 데이터 가용성을 보장하는 데 도움이 됩니다.

Aggregate가 _FULL_으로 설명되면 볼륨에서 사용할 수 있는 애그리게이트의 공간 백분율이 사전 정의된 임계값 아래로 떨어졌다는 의미입니다. Aggregate가 _overallocated_가 되면 ONTAP에서 메타데이터에 사용하고 기본 데이터 액세스를 지원하는 데 사용되는 공간이 소진되었습니다. 경우에 따라 다른 목적으로 일반적으로 예약된 공간을 사용하여 애그리게이트의 기능을 유지할 수 있지만, 애그리게이트 또는 데이터 가용성과 연결된 볼륨의 볼륨 보장이 위험에 노출될 수 있습니다.

초과 할당은 논리적 또는 물리적 할당일 수 있습니다. _논리적 초과 할당_은 볼륨 보증과 같은 향후 공간 약속을 지키기 위해 예약된 공간이 다른 용도로 사용되었음을 의미합니다. _physical overallocation_은 사용할 물리적 블록이 Aggregate에 부족함을 의미합니다. 이 상태의 애그리게이트는 쓰기 작업을 거부하거나, 오프라인 상태가 되거나, 컨트롤러 중단을 일으킬 위험이 있습니다.

다음 표에서는 전체 및 초과 할당 알림, 문제 해결을 위해 수행할 수 있는 작업 및 조치를 취하지 않을 경우의 위험에 대해 설명합니다.

경고 유형	EMS 레벨	구성 가능?	정의	해결 방법	조치를 취하지 않을 경우 위험이 있습니다
거의 꽉 찼습니다	디버그	해당 없음	볼륨에 할당된 공간(보장 포함)이 이 알림에 대해 설정된 임계값(95%)을 초과했습니다. 이 백분율은 총 값에서 `Used` 스냅숏 예비 공간의 크기를 뺀 값입니다.	• Aggregate에 스토리지 추가 • 볼륨 축소 또는 삭제 • 공간을 더 많이 확보한 다른 애그리게이트로 볼륨 이동 • 볼륨 보장 제거('없음'으로 설정)	아직 쓰기 작업 또는 데이터 가용성에 대한 위험이 없습니다.
가득 참	디버그	해당 없음	파일 시스템이 이 알림에 대해 설정된 임계값(98%)을 초과했습니다. 이 백분율은 총 값에서 `Used` 스냅숏 예비 공간의 크기를 뺀 값입니다.	• Aggregate에 스토리지 추가 • 볼륨 축소 또는 삭제 • 공간을 더 많이 확보한 다른 애그리게이트로 볼륨 이동 • 볼륨 보장 제거('없음'으로 설정)	볼륨에 대한 쓰기 작업뿐만 아니라 애그리게이트에서 볼륨에 대한 볼륨 보증이 위험에 노출될 수 있습니다.

경고 유형	EMS 레벨	구성 가능?	정의	해결 방법	조치를 취하지 않을 경우 위험이 있습니다
논리적으로 초과 할당됨	SVC 오류입니다	해당 없음	볼륨이 꽉 찼을 때 예약된 공간 외에 메타데이터에 사용되는 애그리게이트의 공간이 소진되었습니다.	• Aggregate에 스토리지 추가 • 볼륨 축소 또는 삭제 • 공간을 더 많이 확보한 다른 애그리게이트로 볼륨 이동 • 볼륨 보장 제거('없음'으로 설정)	볼륨에 대한 쓰기 작업뿐만 아니라 애그리게이트의 볼륨이 위험에 노출됩니다.
물리적으로 초과 할당되었습니다	노드 오류입니다	해당 없음	aggregate에 쓸 수 있는 물리적 블록이 부족하고 있습니다.	• Aggregate에 스토리지 추가 • 볼륨 축소 또는 삭제 • 공간을 더 많이 확보한 다른 애그리게이트로 볼륨 이동	애그리게이트에서 볼륨에 대한 쓰기 작업이 위험에 처하고 데이터 가용성이 향상됩니다. 애그리게이트는 오프라인 상태가 될 수 있습니다. 극단적인 경우 노드가 중단될 수 있습니다.

전체 백분율 상승 또는 하강 여부와 관계없이 집계에 대해 임계값을 초과할 때마다 EMS 메시지가 생성됩니다. 전체 레벨의 전체도가 임계치 이하로 내려가면 집계 ok EMS 메시지가 생성된다.

분할 예약 설정 시 고려 사항

lun 덮어쓰기 예약 _ 이라고도 하는 분할 예약을 통해 FlexVol 볼륨의 공간 예약 LUN 및 파일에 대한 덮어쓰기 예약 기능을 해제할 수 있습니다. 이를 통해 스토리지 활용도를 극대화할 수 있습니다.

공간 부족으로 인해 쓰기 작업 실패로 인해 환경이 부정적인 영향을 받는 경우 이 구성이 적용할 수 있는 요구사항을 이해해야 합니다.

분수 예약 설정은 백분율로 표시되며 유효한 값은 `0` 및 `100` 백분율뿐입니다. 분할 예약 설정은 볼륨의 속성입니다. `0`**`스토리지 활용률을 높이기 위해 부분 예약을 설정합니다. 하지만 볼륨에 여유 공간이 부족할 경우, 볼륨 보장이 로 설정된 경우에도 볼륨에 상주하는 데이터에 액세스하는 애플리케이션에서 데이터가 중단될 수 있습니다.** `volume` 그러나 적절한 볼륨 구성 및 사용을 통해 쓰기 실패 가능성을 최소화할 수 있습니다. ONTAP는 다음 요구 사항 중 _ALL_로 설정된 부분 예약 용량을 가진 볼륨에 대해 "최선의 노력" 쓰기 보증을 `0` 제공합니다.

- 중복 제거가 사용되지 않습니다
- 압축이 사용되지 않습니다
- FlexClone 하위 파일을 사용하지 않습니다
- 모든 FlexClone 파일과 FlexClone LUN이 자동으로 삭제됩니다

  이 설정은 기본 설정이 아닙니다. 생성 시 또는 FlexClone 파일 또는 FlexClone LUN을 생성한 후에 이를 수정하여 자동 삭제를 명시적으로 설정해야 합니다.

- ODX 및 FlexClone 복사 오프로드가 사용되지 않습니다
- 볼륨 보장이 '볼륨'으로 설정되어 있습니다
- 파일 또는 LUN 공간 예약이 '사용'되었습니다
- 볼륨 스냅숏 예비 공간이 로 설정되어 있습니다 `0`
- 볼륨 스냅샷 자동 삭제는 의 약정 수준 `destroy`, 제거 목록 `lun_clone,vol_clone,cifs_share,file_clone,sfsr` 및 트리거로 `volume` 이루어집니다 `enabled`

  이 설정은 필요한 경우 FlexClone 파일 및 FlexClone LUN도 삭제되도록 합니다.

> - 위의 모든 요구 사항이 충족되지만 변경률이 높을 경우 스냅샷 자동 삭제가 지연되어 볼륨에 공간이 부족해질 수 있습니다.
> - 위의 모든 요구 사항이 충족되고 스냅샷이 사용되지 않는 경우 볼륨 쓰기는 공간이 부족하지 않도록 보장합니다.

또한 필요에 따라 볼륨 자동 확장 기능을 사용하여 볼륨 스냅샷이 자동으로 삭제될 가능성을 줄일 수 있습니다. 자동 확장 기능을 사용하도록 설정한 경우 연결된 애그리게이트의 여유 공간을 모니터링해야 합니다. Aggregate가 가득 차서 볼륨 증가를 막을 수 없을 경우, 볼륨의 여유 공간이 고갈되면 더 많은 스냅샷이 삭제될 수 있습니다.

위 구성 요구사항을 모두 충족하지 못할 경우 볼륨에서 공간이 부족하지 않도록 해야 하는 경우 볼륨의 분할 예약 설정을 '100'으로 설정해야 합니다. 이를 위해서는 공간을 미리 확보해야 하지만, 위에 나열된 기술이 사용 중일 때도 데이터 수정 작업이 성공하도록 보장합니다.

분할 예약 설정의 기본값 및 허용되는 값은 볼륨의 보장에 따라 다릅니다.

볼륨 보장	기본 분할 예약	허용되는 값
볼륨	100	0, 100
없음	0	0, 100

볼륨에 대한 파일 및 **inode** 사용을 확인합니다

FlexVol 볼륨에는 포함할 수 있는 최대 파일 수가 있습니다. CLI 명령을 사용하여 FlexVol 볼륨의 (공용) inode 수를 늘려야 파일 제한에 도달하지 않도록 해야 하는지 여부를 결정할 수 있습니다.

이 작업에 대해

공용 inode는 사용 가능(파일과 연결되지 않음) 또는 사용(파일을 가리함)일 수 있습니다. 볼륨에 대한 사용 가능한 inode 수는 볼륨의 총 inode 수에서 사용된 inode 수(파일 수)를 뺀 값입니다.

qtree 레벨 및 볼륨 레벨 공유가 동일한 FlexVol 또는 SCVMM 풀에 있을 경우 qtree가 FlexVol 공유의 디렉토리로 표시됩니다. 따라서 실수로 삭제하지 않도록 주의해야 합니다.

단계

1. 볼륨에 대한 inode 사용량을 표시하려면 다음 명령을 입력합니다.

```
volume show -vserver <SVM_name> -volume <volume_name> -fields files-used
```

예

```
cluster1::*> volume show -vserver vs1 -volume vol1 -fields files-used
Vserver Name: vs1
Files Used (for user-visible data): 98
```

스토리지 **QoS**로 **FlexVol volume I/O** 성능을 제어 및 모니터링합니다

스토리지 QoS 정책 그룹에 볼륨을 할당하여 FlexVol 볼륨에 대한 입출력 성능을 제어할 수 있습니다. 입출력 성능을 제어하여 워크로드가 특정 성능 목표를 달성하도록 보장하고, 다른 워크로드에 부정적인 영향을 주는 워크로드를 조절할 수 있습니다.

이 작업에 대해

정책 그룹은 최대 처리량 제한(예: 100MB/s)을 적용합니다. 최대 처리량을 지정하지 않고 정책 그룹을 생성할 수 있으므로 워크로드를 제어하기 전에 성능을 모니터링할 수 있습니다. 또한 선택적으로 최소 처리량 제한을 지정할 수 있습니다.

SVM, LUN 및 파일을 정책 그룹에 할당할 수도 있습니다.

정책 그룹에 볼륨을 할당하는 것에 대한 다음 요구 사항을 참고하십시오.

- 정책 그룹이 속한 SVM에서 볼륨을 포함해야 합니다.

  정책 그룹을 생성할 때 SVM을 지정합니다.

- ONTAP 9.18.1부터 QoS 정책이 있는 SVM에 포함된 볼륨에 QoS 정책을 할당할 수 있습니다. 중첩된 QoS 정책을 사용하는 경우 가장 제한적인 정책이 적용됩니다.
- ONTAP 9.14.0부터 QoS 정책이 있는 볼륨에 포함된 qtree에 정책을 할당할 수 있습니다.

스토리지 QoS를 사용하는 방법에 대한 자세한 내용은 를 참조하십시오 "시스템 관리 참조".

단계

1. QoS policy-group create 명령을 사용하여 정책 그룹을 생성합니다.
2. 정책 그룹에 볼륨을 할당하려면 'volume create' 명령 또는 '-qos-policy-group' 매개 변수와 함께 'volume modify' 명령을 사용하십시오.
3. QoS 통계 명령어를 이용하여 성능 데이터를 확인할 수 있다.
4. 필요한 경우 QoS policy-group modify 명령을 사용하여 정책 그룹의 최대 처리량 한도를 조정합니다.

관련 정보

- "qos 정책 그룹"
- 링크: https://docs.netapp.com/us-en/ontap-cli/qos-policy-group-create.html [qos 정책 그룹 생성]
- "볼륨 생성"

- "볼륨 수정"
- "QoS 통계"

FlexVol 볼륨을 삭제합니다

더 이상 필요하지 않은 FlexVol 볼륨은 삭제할 수 있습니다.

시작하기 전에

삭제할 볼륨의 데이터에 액세스하는 애플리케이션이 없어야 합니다.

실수로 볼륨을 삭제한 경우 다음을 참조하세요."NetApp 기술 자료: 볼륨 복구 대기열 사용 방법" .

단계

1. 볼륨이 마운트된 경우 마운트 해제합니다.

   '볼륨 마운트 해제 - vserver vserver_name - volume volume volume_name'

2. 볼륨이 SnapMirror 관계의 일부인 경우 'napmirror delete' 명령을 사용하여 관계를 삭제합니다.
3. 볼륨이 온라인 상태인 경우 볼륨을 오프라인으로 전환합니다.

   'volume offline-vserver vserver_name volume_name'

4. 볼륨 삭제:

   '볼륨 삭제 - vserver vserver_name volume_name'

결과

연관된 할당량 정책 및 qtree와 함께 볼륨이 삭제됩니다.

관련 정보

- "SnapMirror 삭제"
- "볼륨 마운트 해제"
- "볼륨이 오프라인 상태입니다"
- "볼륨 삭제"

우발적인 볼륨 삭제로부터 보호

기본 볼륨 삭제 동작은 실수로 삭제된 FlexVol 볼륨을 복구하는 데 도움이 됩니다.

RW 또는 DP(volume show 명령 출력에서 볼 수 있음)가 있는 볼륨에 대한 볼륨 삭제 요청이 발생하면 볼륨이 부분적으로 삭제된 상태로 이동합니다. 기본적으로 이 항목은 완전히 삭제되기 전에 최소 12시간 동안 복구 대기열에 유지됩니다.

삭제된 볼륨을 포함하는 SVM을 삭제하면 볼륨 복구 큐(VRQ)가 비워집니다. SVM이 소유한 볼륨을 복구할 필요가 없다는 것이 확실한 경우에만 SVM을 삭제하십시오. 소유 SVM이 삭제되면 볼륨 복구 큐에 있는 볼륨은 존재할 수 없습니다.

관련 정보

- "볼륨 복구 대기열 사용 방법"
- "볼륨 삭제"
- "볼륨 표시"

ONTAP에서 **FlexVol** 볼륨을 관리하는 명령입니다

ONTAP CLI는 FlexVol 볼륨을 관리하기 위한 특정 명령을 제공합니다. 수행해야 하는 작업에 따라 다음 명령을 사용하여 FlexVol 볼륨을 관리할 수 있습니다.

원하는 작업	이 명령 사용...
볼륨을 온라인으로 설정합니다	온라인 볼륨
볼륨의 크기를 변경합니다	볼륨 크기
볼륨과 연결된 애그리게이트를 확인합니다	'볼륨 쇼'
SVM(스토리지 가상 시스템)의 모든 볼륨에서 관련 애그리게이트 결정	'volume show-vserver-fields aggregate'
볼륨의 형식을 확인합니다	'볼륨 표시-필드 블록-유형'입니다
교차점을 사용하여 볼륨을 다른 볼륨에 마운트합니다	'볼륨 마운트'입니다
볼륨을 제한 상태로 설정합니다	볼륨 제한
볼륨 이름을 바꿉니다	볼륨 이름 바꾸기
볼륨을 오프라인 상태로 전환합니다	'볼륨 오프라인'

에 대한 자세한 내용은 `volume` "ONTAP 명령 참조입니다"을 참조하십시오.

공간 사용 정보를 표시하는 명령입니다

및 `volume` 명령을 사용하여 `storage aggregate` Aggregate, 볼륨 및 해당 스냅샷에서 공간이 어떻게 사용되고 있는지 확인할 수 있습니다.

ONTAP 9.18.1부터 `storage aggregate show-space` 명령은 논리적 참조 용량 및 논리적 미참조 용량 보고 방식을 변경합니다. 논리적 참조 용량은 모든 객체의 참조된 블록과 조각화된 객체의 미참조 블록을 보고합니다. 논리적 미참조 용량은 전체 임계값을 초과하여 객체 삭제 및 조각 모음 대상이 되는 객체의 미참조 블록만 보고합니다.

예를 들어 ONTAP S3 및 StorageGRID에 대해 기본 애그리게이트 충만도 임계값 40%를 사용하는 경우 객체의 블록 중 60%가 참조되지 않아야 블록이 참조되지 않은 용량으로 보고됩니다.

ONTAP 9.18.1 이전 릴리스에서는 논리적 참조 용량이 모든 객체(전체 객체 및 조각화된 객체 모두)의 참조된 블록을

보고합니다. 논리적 미참조 용량은 모든 객체의 미참조 블록을 보고합니다.

정보를 표시하려면...	이 명령 사용...
사용된 공간 및 사용 가능한 공간 비율, 스냅샷 예약 크기 및 기타 공간 사용 정보에 대한 세부 정보를 포함한 애그리게이트	'스토리지 집계 쇼' `storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve`
디스크 및 RAID 그룹이 애그리게이트에서 사용하는 방법 및 RAID 상태	'스토리지 집계 표시 상태'
특정 스냅샷을 삭제할 경우 재확보되는 디스크 공간의 양입니다	'볼륨 스냅샷 계산-재확보 가능'(고급)

볼륨에서 사용하는 공간입니다	`volume show -fields size,used,available,percent-used`
	
	`volume show-space`

포함하는 애그리게이트의 볼륨이 사용하는 공간 크기입니다	볼륨 쇼 풋프린트

관련 정보

- "스토리지 애그리게이트 보기"
- "저장 집합 쇼 공간"
- "스토리지 집계 표시 상태"
- "볼륨 스냅샷 계산 - 재확보 가능"
- "볼륨 표시"

볼륨 이동 및 복사

FlexVol 볼륨 개요 이동

용량 활용률, 성능 향상, 서비스 수준 계약 충족을 위해 볼륨을 이동 또는 복사할 수 있습니다. FlexVol 볼륨의 이동 방법을 알면 볼륨 이동이 서비스 수준 계약을 충족하는지 확인하고 볼륨 이동 프로세스에서 볼륨 이동이 어느 단계에 있는지 파악하는 데 도움이 됩니다.

FlexVol 볼륨은 동일한 SVM(스토리지 가상 머신) 내에서 하나의 애그리게이트 또는 노드에서 다른 애그리게이트로 이동됩니다. 볼륨 이동이 이동 중에 클라이언트 액세스를 방해하지 않습니다.

볼륨 이동 작업의 컷오버 단계에서는 FlexVol 볼륨의 FlexClone 파일 또는 FlexClone LUN을 생성할 수 없습니다.

볼륨 이동에는 여러 단계가 있습니다.

- 대상 애그리게이트에 새 볼륨이 작성되고
- 원래 볼륨의 데이터가 새 볼륨으로 복사됩니다.

  이 시간 동안 원래 볼륨은 온전하며 클라이언트가 액세스할 수 있습니다.

- 이동 프로세스가 끝나면 클라이언트 액세스가 일시적으로 차단됩니다.

  이 시간 동안 시스템은 소스 볼륨에서 대상 볼륨으로 최종 복제를 수행하고 소스 볼륨과 대상 볼륨의 ID를 스왑하며 대상 볼륨을 소스 볼륨으로 변경합니다.

- 이동을 완료하면 시스템은 클라이언트 트래픽을 새 소스 볼륨으로 라우팅하고 클라이언트 액세스를 재개합니다.

클라이언트가 중단 및 시간 초과를 인지하기 전에 클라이언트 액세스가 차단되므로 이동이 클라이언트 액세스에 영향을 주지 않습니다. 클라이언트 액세스는 기본적으로 30초 동안 차단됩니다. 액세스가 거부된 시간에 볼륨 이동 작업을 완료할 수 없는 경우, 시스템은 볼륨 이동 작업의 이 마지막 단계를 중단하고 클라이언트 액세스를 허용합니다. 시스템은 기본적으로 최종 단계를 세 번 시도합니다. 세 번째 시도 후 시스템은 1시간을 기다린 후 최종 단계 시퀀스를 다시 시도합니다. 시스템은 볼륨 이동이 완료될 때까지 볼륨 이동 작업의 마지막 단계를 실행합니다.

볼륨 이동 시 고려 사항 및 권장 사항

볼륨을 이동할 때 고려해야 할 몇 가지 고려 사항과 권장 사항이 있습니다. 이러한 볼륨은 MetroCluster와 같은 시스템 구성과 함께 이동 중인 볼륨을 기반으로 합니다. 볼륨을 이동하기 전에 모든 관련 문제를 이해해야 합니다.

일반 고려 사항 및 권장 사항

- 클러스터의 릴리즈 제품군을 업그레이드하는 경우에는 클러스터의 모든 노드를 업그레이드할 때까지 볼륨을 이동하지 마십시오.

  이 권장 사항을 사용하면 실수로 볼륨을 새 릴리즈 제품군에서 이전 릴리즈 제품군으로 이동하려고 하는 것을 방지할 수 있습니다.

- 소스 볼륨은 정합성이 보장되어야 합니다.
- 하나 이상의 애그리게이트를 관련 SVM(스토리지 가상 머신)에 할당한 경우, 대상 애그리게이트는 할당된 애그리게이트 중 하나여야 합니다.
- 볼륨을 최신 ONTAP 버전으로만 이동해야 합니다.
- 대신 가져온 CFO 애그리게이트로 또는 CFO 애그리게이트로 볼륨을 이동할 수 없습니다.
- LUN이 포함된 볼륨이 이동하기 전에 NVFAIL이 활성화되지 않은 경우, 볼륨을 이동한 후 NVFAIL이 활성화됩니다.
- Flash Pool 애그리게이트에서 다른 Flash Pool 애그리게이트로 볼륨을 이동할 수 있습니다.
  - 해당 볼륨의 캐싱 정책도 이동됩니다.
  - 이동은 볼륨 성능에 영향을 미칠 수 있습니다.
- Flash Pool 애그리게이트와 비 Flash Pool 애그리게이트 간에 볼륨을 이동할 수 있습니다.
  - Flash Pool 애그리게이트에서 비 Flash Pool 애그리게이트로 볼륨을 이동하는 경우, ONTAP에서 볼륨 성능에 영향을 줄 수 있으며 계속할 것인지 묻는 메시지가 표시됩니다.
  - 비 Flash Pool 애그리게이트에서 Flash Pool 애그리게이트로 볼륨을 이동하는 경우 ONTAP는 '자동' 캐싱 정책을 할당합니다.

- 볼륨은 유휴 상태의 데이터 보호를 통해 애그리게이트로 안전하게 보호합니다. NSE 드라이브가 포함된 Aggregate에서 NSE 드라이브가 아닌 볼륨으로 볼륨을 이동하면 볼륨에 NSE 데이터 -유휴 보호 기능이 없습니다.
- ONTAP 9.13.1 이하에서 ONTAP 9.15.1 이상으로 FabricPool 최적화 볼륨을 이동하는 경우 다음을 참조하세요 ."NetApp 기술 자료: CONTAP-307878 - 소스 ONTAP 이 9.14.1보다 작고 대상이 9.14.1보다 큰 경우 FabricPool 최적화된 볼륨 이동 중 예기치 않은 재부팅이 발생합니다." .
- ONTAP 9.15.1부터 A400 시스템에서 A70, A90 또는 A1K 시스템으로 볼륨을 이동하면 읽기 지연 문제가 증가할 수 있습니다. 자세한 내용과 권장 조치는 다음을 참조하세요. "NetApp 기술 자료: CONTAP-556247 - A400에서 A70, A90 및 A1K로 볼륨을 이동한 후 볼륨의 압축/압축 해제 속도가 느림".

FlexClone 볼륨 고려 사항 및 권장 사항

- FlexClone 볼륨은 이동 중에 오프라인 상태가 될 수 없습니다.
- 'vol clone split start' 명령을 실행하지 않고도 동일한 노드 또는 동일한 SVM의 다른 노드에 있는 하나의 Aggregate에서 다른 aggregate로 FlexClone 볼륨을 이동할 수 있습니다.

  FlexClone 볼륨에서 볼륨 이동 작업을 초기화하면 이동 중에 클론 볼륨이 다른 애그리게이트로 분리됩니다. 클론 볼륨에서 볼륨 이동이 완료된 후 이동한 볼륨이 더 이상 클론으로 표시되지 않고 이전 상위 볼륨과의 클론 관계 없이 독립 볼륨으로 표시됩니다.

- FlexClone 볼륨 스냅샷은 클론을 이동한 후 손실되지 않습니다.
- FlexClone 상위 볼륨을 한 Aggregate에서 다른 aggregate로 이동할 수 있습니다.

  FlexClone 상위 볼륨을 이동할 때 임시 볼륨은 모든 FlexClone 볼륨의 상위 볼륨으로 작동하는 상태로 남아 있습니다. 임시 볼륨을 오프라인 상태로 만들거나 삭제하는 경우를 제외하고는 해당 볼륨에 대한 작업이 허용되지 않습니다. 모든 FlexClone 볼륨이 분할되거나 제거된 후에는 임시 볼륨이 자동으로 지워집니다.

- FlexClone 하위 볼륨을 이동하면 볼륨은 더 이상 FlexClone 볼륨이 아닙니다.
- FlexClone 이동 작업은 FlexClone 복사본 또는 분할 작업에서만 사용할 수 있습니다.
- 클론 분할 작업이 진행 중인 경우 볼륨을 이동하지 못할 수 있습니다.

  클론 분할 작업이 완료될 때까지 볼륨을 이동하면 안 됩니다.

MetroCluster 고려 사항 및 권장 사항

- MetroCluster 구성에서 볼륨을 이동하는 동안 소스 클러스터의 대상 애그리게이트에 임시 볼륨이 생성되면 미러링된 볼륨의 볼륨에 해당하는 임시 볼륨에 대한 기록이나 흡수되지 않은 aggregate가 나머지 클러스터에도 생성됩니다.
- 컷오버가 발생하기 전에 MetroCluster 전환이 발생하면 대상 볼륨에 레코드가 있고 임시 볼륨(TMP 유형의 볼륨)이 됩니다.

  남아 있는(재해 복구) 클러스터에서 작업 재시작을 이동하고, 오류를 보고하고, 임시 볼륨을 비롯한 이동 관련 항목을 모두 정리합니다. 정리가 제대로 수행되지 않는 경우 시스템 관리자에게 필요한 정리가 수행되도록 알리는 EMS가 생성됩니다.

- 컷오버 단계가 시작된 후 이동 작업이 완료되기 전에(즉, 대상 애그리게이트를 가리키도록 클러스터를 업데이트할 수 있는 단계에 도달한 이동) MetroCluster 전환이 작동 가능(재해 복구)에서 다시 시작됩니다. 클러스터 및 가 완료까지 실행됩니다.

  임시 볼륨(원본 소스)을 포함하여 모든 이동 관련 항목이 정리됩니다. 정리가 제대로 수행되지 않는 경우 시스템

관리자에게 필요한 정리가 수행되도록 알리는 EMS가 생성됩니다.

- Switched over Site에 속한 볼륨에 대해 진행 중인 볼륨 이동 작업이 있는 경우 강제 또는 비강제 MetroCluster 전환이 허용되지 않습니다.

  정상 사이트에 로컬인 볼륨에 대해 볼륨 이동 작업이 진행 중이면 전환이 차단되지 않습니다.

- 강제 적용 MetroCluster 전환은 차단되지만, 진행 중인 볼륨 이동 작업이 있는 경우에는 강제 적용 MetroCluster 전환은 차단되지 않습니다.

SAN 환경에서 볼륨을 이동하기 위한 요구 사항

SAN 환경에서 볼륨을 이동하기 전에 준비해야 합니다.

LUN 또는 네임스페이스를 포함하는 볼륨을 이동하기 전에 다음 요구사항을 충족해야 합니다.

- 하나 이상의 LUN이 포함된 볼륨의 경우 클러스터의 각 노드에 연결되는 LUN(LIF)당 경로가 2개 이상 있어야 합니다.

  따라서 단일 장애 지점이 발생하지 않으며 시스템에서 구성 요소 장애를 극복할 수 있습니다.

- 네임스페이스가 포함된 볼륨의 경우 클러스터는 ONTAP 9.6 이상을 실행해야 합니다.

  ONTAP 9.5를 실행하는 NVMe 구성에는 볼륨 이동이 지원되지 않습니다.

ONTAP 볼륨 이동

스토리지 용량 불균형이 있다고 판단된 후 FlexVol 볼륨을 동일한 스토리지 가상 시스템(SVM) 내에서 다른 애그리게이트, 노드 또는 둘 모두로 이동하여 스토리지 용량의 균형을 조정할 수 있습니다.

이 작업에 대해

기본적으로 컷오버 작업이 30초 이내에 완료되지 않으면 다시 시도합니다. 및 `-cutover-action` 매개 변수를 사용하여 기본 동작을 조정할 수 `-cutover-window` 있으며, 둘 다 고급 권한 수준 액세스가 필요합니다.

이 작업을 수행하려면 클러스터 관리자여야 합니다.

시작하기 전에

- 8K 적응 압축을 사용하는 볼륨을 다음 플랫폼 중 하나로 이동하는 경우 다음을 수행해야 합니다."볼륨의 활성 파일 시스템 크기를 늘립니다." 볼륨을 이동하기 전에. 이러한 플랫폼에서는 데이터가 다른 방식으로 압축되므로 볼륨 수준이 아닌 집계 수준에서 공간이 절약됩니다. 이러한 차이로 인해 볼륨 이동 중에 볼륨 공간이 부족해지는 것을 방지하기 위해 볼륨의 활성 파일 시스템 크기는 8k 압축 절감량만큼 늘어나야 합니다.
  - 전용 오프로드 프로세서 스토리지 효율성을 지원하는 AFF 및 FAS 플랫폼

    AFF 및 FAS 플랫폼에 대해 자세히 알아보세요."전용 오프로드 프로세서 스토리지 효율성" .

  - AFF C 시리즈 플랫폼

    를 참조하십시오"Hardware Universe" C 시리즈 플랫폼의 전체 목록은 여기에서 확인하세요.

- 데이터 보호 미러를 이동하고 미러 관계를 초기화하지 않은 경우 다음을 사용하십시오. `snapmirror initialize` 미러 관계를 초기화하는 명령입니다. 자세히 알아보세요 `snapmirror initialize` 에서 "ONTAP 명령 참조입니다" .

  볼륨 중 하나를 이동하려면 먼저 데이터 보호 미러 관계를 초기화해야 합니다.

단계

1. 볼륨을 이동할 수 있는 집계를 결정합니다.

```
volume move target-aggr show
```

선택하는 Aggregate는 볼륨에 충분한 공간을 가져야 합니다. 즉, 사용 가능한 용량이 이동 중인 볼륨보다 큽니다.

다음 예에서는 VS2 볼륨을 나열된 Aggregate 중 한 곳으로 이동할 수 있음을 보여 줍니다.

```
cluster1::> volume move target-aggr show -vserver vs2 -volume user_max
Aggregate Name   Available Size   Storage Type
--------------   --------------   ------------
aggr2            467.9GB          hdd
node12a_aggr3    10.34GB          hdd
node12a_aggr2    10.36GB          hdd
node12a_aggr1    10.36GB          hdd
node12a_aggr4    10.36GB          hdd
5 entries were displayed.
```

에 대한 자세한 내용은 `volume move target-aggr show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 볼륨을 의도한 집계로 이동할 수 있는지 확인하기 위해 유효성 검사를 수행합니다.

```
volume move start -perform-validation-only
```

에 대한 자세한 내용은 `volume move start` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 볼륨을 이동합니다.

```
volume move start
```

다음 명령을 실행하면 VS2 SVM의 user_max 볼륨이 node12a_aggr3 애그리게이트로 이동합니다. 이동은 백그라운드 프로세스로 실행됩니다.

```
cluster1::> volume move start -vserver vs2 -volume user_max
-destination-aggregate node12a_aggr3
```

4. 볼륨 이동 작업의 상태를 확인합니다.

```
volume move show
```

다음 예에서는 복제 단계를 완료하고 컷오버 단계에 있는 볼륨 이동 상태를 보여줍니다.

```
cluster1::> volume move show
Vserver   Volume     State    Move Phase  Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------  ----------------
----------------
vs2       user_max   healthy  cutover     -                -
```

볼륨 이동은 'volume move show' 명령 출력에 더 이상 나타나지 않으면 완료됩니다.

에 대한 자세한 내용은 `volume move show` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 선택적으로 압축 절감액을 확인하세요.

```
volume show-footprint -vserver <SVM> -volume <volume_name>
```

> ⓘ 볼륨 이동이 완료된 직후에 자동으로 실행되는 사후 처리 변환 스캔을 통해 추가적인 집계 수준의 절감 효과를 실현할 수 있습니다.

관련 정보

- "볼륨 이동 시 고려 사항 및 권장 사항"

8k 적응 압축에서 마이그레이션하기 전에 **ONTAP** 볼륨의 활성 파일 시스템을 늘립니다**.**

8K 적응형 압축을 지원하는 플랫폼은 볼륨 수준에서 공간을 절약합니다. AFF C 시리즈 플랫폼과 32k 압축을 지원하는 플랫폼은 전체 수준에서 공간을 절약합니다. 8k 적응 압축에서 AFF C 시리즈 플랫폼이나 32k 압축을 사용하는 플랫폼으로 볼륨을 마이그레이션하는 경우 8k 압축으로 인한 절감 효과만큼 볼륨의 활성 파일 시스템 크기를 늘려야 합니다. 이렇게 하면 볼륨을 이동하는 동안 볼륨의 여유 공간이 부족해지는 것을 방지할 수 있습니다.

다음 시스템은 32k 압축을 지원합니다.

플랫폼	**ONTAP** 버전입니다
• AFF A1K 를 참조하십시오 • AFF A90 를 참조하십시오 • AFF A70 를 참조하십시오 • FAS90를 참조하십시오 • FAS70를 참조하십시오	9.15.1 이상
• AFF C80 를 참조하십시오 • AFF C60 를 참조하십시오 • AFF C30 를 참조하십시오 • AFF A50 를 참조하십시오 • AFF A30 를 참조하십시오	9.16.1 이상

자세히 알아보세요 "32k 압축을 지원하는 AFF 및 FAS 플랫폼" .

를 참조하십시오"Hardware Universe" AFF C 시리즈 플랫폼의 전체 목록은 여기에서 확인하세요.

이 작업에 대해

볼륨 이동 작업을 사용하여 데이터를 마이그레이션하는 경우 다음 단계를 수행합니다. SnapMirror 작업을 사용하여 데이터를 마이그레이션하는 경우 활성 파일 시스템의 크기를 수동으로 늘릴 필요가 없습니다. SnapMirror 대상 볼륨은 기본적으로 볼륨 자동 크기 조정을 사용하므로 볼륨 계층이 아닌 집계 계층에서 압축 절감이 실현되어 공간이 부족해질 것으로 예상되지 않습니다.

시작하기 전에

볼륨에서 논리적 공간 보고 및 적용이 활성화되지 않은 경우 선택적으로 다음을 설정하여 활성화할 수 있습니다. `-is-space-reporting-logical` 그리고 `-is-space-enforcement-logical` 매개변수를 *true*로 설정합니다. 볼륨을 이동하기 전에 이러한 설정을 활성화하면 8k 압축에서 변환할 때 볼륨 계층에서 압축 절감 손실을 수용할 만큼 볼륨이 충분히 큰지 평가하는 데 도움이 됩니다. 볼륨에서 이러한 설정을 활성화해야 합니다. SVM 수준에서 이러한 설정을 활성화하면 새로 생성된 볼륨에만 적용됩니다.

단계

1. 볼륨의 현재 크기와 스냅샷 예약을 확인하세요.

```
volume show-space
```

2. 볼륨의 압축 공간 절약을 확인하세요.

```
volume show -vserver -volume -fields compression-space-saved
```

3. 표시된 양만큼 볼륨의 활성 파일 시스템 크기를 늘리십시오. `compression-space-saved` 스냅샷 예약도 포함.

```
volume size -vserver <vserver_name> -volume <volume_name> -new-size
+<size>
```

예

볼륨이 100GB이고 스냅샷 예약이 20%인 경우, 활성 파일 시스템은 80GB이고 스냅샷 예약은 20GB입니다. 활성 파일 시스템을 20GB 늘리려면 전체 볼륨 크기에 25GB를 추가해야 합니다. 즉, 활성 파일 시스템에 20GB를 추가하고 스냅샷 예약에 5GB(20%)를 추가해야 합니다.

```
volume size -vserver svm1 -volume volx -size +20GB
```

4. 볼륨 크기가 증가했는지 확인하세요.

```
volume show -vserver <vserver_name> -volume <volume_name> -fields size
```

결과

볼륨의 활성 파일 시스템 크기가 늘어났으며 볼륨을 이동할 준비가 되었습니다.

다음 단계

수행하다"볼륨 이동" 데이터를 마이그레이션하려면.

ONTAP에서 볼륨을 이동하기 위한 명령입니다

ONTAP CLI는 볼륨 이동을 관리하기 위한 특정 명령을 제공합니다. 수행해야 하는 작업에 따라 다음 명령을 사용하여 할당량 규칙 및 할당량 정책을 관리할 수 있습니다.

원하는 작업	이 명령 사용...
활성 볼륨 이동 작업을 중단합니다.	'볼륨 이동 중단'
한 Aggregate에서 다른 aggregate로 이동하는 볼륨의 상태를 표시합니다.	'볼륨 이동 쇼'
한 Aggregate에서 다른 Aggregate로 볼륨을 이동하기 시작합니다.	볼륨 이동 시작
볼륨 이동을 위한 타겟 애그리게이트를 관리합니다.	'볼륨 이동 대상-집계'
이동 작업의 컷오버를 트리거합니다.	'볼륨 이동 트리거-컷오버
기본값이 적절하지 않은 경우 클라이언트 액세스가 차단되는 시간을 변경합니다.	'-cutover-window' 매개 변수를 사용하여 볼륨 이동 시작 또는 볼륨 이동 수정. 볼륨 이동 수정 명령은 고급 명령이고 -cutover-window는 고급 매개 변수입니다.

원하는 작업	이 명령 사용...
클라이언트 액세스가 차단된 시간 동안 볼륨 이동 작업을 완료할 수 없는 경우 시스템에서 어떤 작업을 수행하는지 확인합니다.	'-cutover-action' 매개 변수를 사용하여 볼륨 이동 시작 또는 볼륨 이동 수정 볼륨 이동 수정 명령은 고급 명령이고 -cutover-action은 고급 매개 변수입니다.

관련 정보

- "볼륨 이동"

볼륨을 복사하는 방법입니다

볼륨을 복사하는 방법은 볼륨을 동일한 Aggregate에 복사하는지 아니면 다른 Aggregate에 복사하는지, 원래 볼륨의 스냅샷을 보존할지 여부에 따라 달라집니다. 볼륨을 복사하면 테스트 및 기타 목적으로 사용할 수 있는 볼륨의 독립 실행형 복사본이 생성됩니다.

다음 표에는 복제본의 특성 및 복제본을 생성하는 데 사용되는 방법이 나와 있습니다.

볼륨을 복사하려는 경우...	사용하는 방법은 다음과 같습니다.
동일한 애그리게이트 내에 있으며 원본 볼륨의 스냅샷을 복제하지 않으려는 경우	원래 볼륨의 FlexClone 볼륨 생성
다른 애그리게이트로 복제하며 원본 볼륨의 스냅샷을 복제하지 않으려는 경우	원래 볼륨의 FlexClone 볼륨을 생성한 다음 'volume move' 명령을 사용하여 볼륨을 다른 애그리게이트로 이동합니다.
원래 볼륨의 모든 스냅샷을 보존하고 다른 Aggregate로 이동합니다.	SnapMirror를 사용하여 원래 볼륨을 복제한 다음 SnapMirror 관계를 끊어 읽기-쓰기 볼륨 복사본을 만듭니다.

FlexClone 볼륨을 사용하여 FlexVol 볼륨의 효율적인 복사본을 생성합니다

FlexClone 볼륨 사용 개요

FlexClone 볼륨은 상위 FlexVol 볼륨의 쓰기 가능한 특정 시점 복사본입니다. FlexClone 볼륨은 공통 데이터에 대해 부모 FlexVol 볼륨과 동일한 데이터 블록을 공유하므로 공간 효율성이 뛰어납니다. FlexClone 볼륨을 생성하는 데 사용되는 스냅샷은 상위 볼륨과도 공유됩니다.

기존 FlexClone 볼륨을 클론 복제하여 다른 FlexClone 볼륨을 생성할 수 있습니다. LUN 및 LUN 클론이 포함된 FlexVol 볼륨의 클론을 생성할 수도 있습니다.

FlexClone 볼륨을 상위 볼륨에서 분할할 수도 있습니다. ONTAP 9.4부터 AFF 시스템의 보장되지 않는 볼륨의 경우 FlexClone 볼륨의 분할 작업은 물리적 블록을 공유하며 데이터를 복사하지 않습니다. 따라서 AFF 시스템에서 FlexClone 볼륨을 분할하는 작업이 ONTAP 9.4 이상 릴리즈의 다른 FAS 시스템에서 FlexClone 분할 작업보다 빠릅니다.

FlexClone 볼륨은 읽기-쓰기 FlexClone 볼륨과 데이터 보호 FlexClone 볼륨의 두 가지 유형의 FlexClone 볼륨을 생성할 수 있습니다. 일반 FlexVol 볼륨의 읽기-쓰기 FlexClone 볼륨을 생성할 수 있지만 SnapVault 보조 볼륨만

사용하여 데이터 보호 FlexClone 볼륨을 생성해야 합니다.

FlexClone 볼륨을 생성합니다

SnapMirror 타겟 볼륨 또는 SnapVault 2차 볼륨인 상위 FlexVol 볼륨에서 데이터 보호 FlexClone 볼륨을 생성할 수 있습니다. ONTAP 9.7부터 FlexGroup 볼륨으로부터 FlexClone 볼륨을 생성할 수 있습니다. FlexClone 볼륨을 생성한 후에는 FlexClone 볼륨이 있는 동안에는 상위 볼륨을 삭제할 수 없습니다.

시작하기 전에

- FlexClone 라이센스가 클러스터에 설치되어 있어야 합니다. 이 라이센스는 에 "ONTAP 1 을 참조하십시오 "포함되어 있습니다.
- 복제할 볼륨이 온라인 상태여야 합니다.

> 볼륨을 다른 SVM에서 FlexClone 볼륨으로 클론 복제하는 것은 MetroCluster 구성에서 지원되지 않습니다.

FlexVol 또는 FlexGroup의 FlexClone 볼륨을 생성합니다

단계

1. FlexClone 볼륨 생성:

   '볼륨 클론 생성'

> 읽기-쓰기 상위 볼륨에서 읽기-쓰기 FlexClone 볼륨을 생성하는 동안 기본 스냅샷을 지정할 필요가 없습니다. 클론의 기본 스냅샷으로 사용될 특정 스냅샷의 이름을 지정하지 않으면 ONTAP에서 스냅샷을 생성합니다. 상위 볼륨이 데이터 보호 볼륨인 경우 FlexClone 볼륨을 생성하기 위한 기본 스냅샷을 지정해야 합니다.

예

- 다음 명령을 실행하면 상위 볼륨 vol1에서 읽기-쓰기 FlexClone 볼륨 vol1_clone이 생성됩니다.

  '볼륨 클론 생성 - vserver vs0-FlexClone vol1_clone-type rw-parent-volume vol1'

- 다음 명령을 실행하면 기본 스냅샷 snap1을 사용하여 상위 볼륨 DP_vol에서 데이터 보호 FlexClone volume vol_dp_clone이 생성됩니다.

  '볼륨 클론 생성 - vserver vs1-FlexClone vol_DP_clone-type DP-parent-volume DP_vol-parent-snap1'

모든 SnapLock 유형의 FlexClone을 생성합니다

ONTAP 9.13.1 부터는 세 가지 SnapLock 유형 중 하나를 지정할 수 있습니다. `compliance`, `enterprise`, `non-snaplock`, RW 볼륨의 FlexClone을 만들 때. 기본적으로 FlexClone 볼륨은 상위 볼륨과 동일한 SnapLock 유형으로 생성됩니다. 그러나 을 사용하여 기본값을 재정의할 수 있습니다 `snaplock-type` 옵션을 사용하여 FlexClone 볼륨을 생성할 수 있습니다.

를 사용합니다 `non-snaplock` 매개 변수 `snaplock-type` SnapLock 상위 볼륨에서 비 SnapLock 유형의 FlexClone 볼륨을 생성하여 필요한 경우 데이터를 다시 온라인 상태로 전환하는 더 빠른 방법을 제공할 수 있습니다.

에 대해 자세히 "SnapLock"알아보십시오.

시작하기 전에

SnapLock 유형이 상위 볼륨과 다른 경우 다음 FlexClone 볼륨 제한에 대해 알고 있어야 합니다.

- RW 유형의 클론만 지원됩니다. SnapLock 유형이 상위 볼륨과 다른 DP 유형의 클론은 지원되지 않습니다.
- SnapLock 볼륨이 LUN을 지원하지 않으므로 SnapLock 유형 옵션을 '비 SnapLock' 이외의 값으로 설정하여 LUN이 있는 볼륨을 복제할 수 없습니다.
- SnapLock 규정 준수 볼륨이 MetroCluster 미러링된 애그리게이트에서 지원되지 않으므로 MetroCluster 미러링된 Aggregate의 볼륨은 Compliance SnapLock 유형으로 복제할 수 없습니다.
- 법적 증거 자료 보관 기능이 있는 SnapLock 준수 볼륨은 다른 SnapLock 유형으로 복제할 수 없습니다. Legal-Hold는 SnapLock 준수 볼륨에서만 지원됩니다.
- SVM DR은 SnapLock 볼륨을 지원하지 않습니다. SVM DR 관계의 일부인 SVM의 볼륨에서 SnapLock 클론을 생성하려고 하면 실패합니다.
- FabricPool 모범 사례에서는 클론이 상위 항목과 같은 계층화 정책을 유지할 것을 권장합니다. 하지만 FabricPool 지원 볼륨의 SnapLock 규정 준수 클론은 상위 볼륨과 동일한 계층화 정책을 가질 수 없습니다. 계층화 정책을 로 설정해야 합니다 `none`. 이외의 계층화 정책을 사용하는 상위 항목에서 SnapLock 규정 준수 클론을 생성하려고 합니다 `none` 실패할 것입니다.

단계

1. SnapLock 유형으로 FlexClone 볼륨 생성: `volume clone create -vserver` *`svm_name`* `-flexclone` *`flexclone_name`* `-type RW [ -snaplock-type {non-snaplock|compliance|enterprise} ]`

   예:

   ```
   > volume clone create -vserver vs0 -flexclone vol1_clone -type RW
   -snaplock-type enterprise -parent-volume vol1
   ```

상위 볼륨에서 **FlexClone** 볼륨을 분할합니다

FlexClone 볼륨을 상위 볼륨에서 분할하여 클론을 일반 FlexVol 볼륨으로 만들 수 있습니다.

클론 분할 작업은 백그라운드에서 수행됩니다. 분할 중에 클론과 상위 항목에서 데이터에 액세스할 수 있습니다. ONTAP 9.4부터는 공간 효율성이 유지됩니다. 분할 프로세스는 메타데이터만 업데이트하며 최소 입출력을 필요로 합니다. 데이터 블록은 복사되지 않습니다.

이 작업에 대해

- 분할 작업 중에는 FlexClone 볼륨의 새 스냅샷을 생성할 수 없습니다.
- FlexClone 볼륨이 데이터 보호 관계에 속해 있거나 로드 공유 미러에 속하는 경우 상위 볼륨에서 분할할 수 없습니다.
- 분할이 진행되는 동안 FlexClone 볼륨을 오프라인으로 전환하면 분할 작업이 일시 중단되고 FlexClone 볼륨을 다시 온라인 상태로 전환하면 분할 작업이 재개됩니다.
- 분할 후에는 상위 FlexVol 볼륨과 복제본 모두에 볼륨 보장에 따라 결정된 전체 공간 할당이 필요합니다.

- FlexClone 볼륨이 상위 볼륨에서 분할된 후에는 두 볼륨을 다시 연결할 수 없습니다.
- ONTAP 9.4부터 AFF 시스템의 보장되지 않는 볼륨의 경우 FlexClone 볼륨의 분할 작업은 물리적 블록을 공유하며 데이터를 복사하지 않습니다. 따라서 AFF 시스템에서 FlexClone 볼륨을 분할하는 작업이 ONTAP 9.4 이상의 다른 FAS 시스템에서 FlexClone 분할 작업보다 빠릅니다. AFF 시스템에서 향상된 FlexClone 분할 작업은 다음과 같은 이점을 제공합니다.
  - 상위 클론에서 클론을 분할한 후에는 스토리지 효율성이 유지됩니다.
  - 기존 스냅샷은 삭제되지 않습니다.
  - 작업이 더 빠릅니다.
  - FlexClone 볼륨은 클론 계층 구조의 모든 지점에서 분할할 수 있습니다.

시작하기 전에

- 클러스터 관리자여야 합니다.
- 분할 작업을 시작할 때 FlexClone 볼륨은 온라인 상태여야 합니다.
- 분할이 성공하려면 상위 볼륨이 온라인 상태여야 합니다.

단계

1. 분할 작업을 완료하는 데 필요한 여유 공간을 결정합니다.

   `volume clone show -estimate -vserver` *`vserver_name`* `-flexclone` *`clone_volume_name`* `-parent-volume` *`parent_vol_name`*

   다음 예에서는 상위 볼륨 ""vol1""에서 FlexClone 볼륨 ""clone1""을 분할하는 데 필요한 여유 공간에 대한 정보를 제공합니다.

   ```
   cluster1::> volume clone show -estimate -vserver vs1 -flexclone clone1
   -parent-volume volume1
                                Split
   Vserver   FlexClone       Estimate
   --------- ------------- ----------
   vs1       clone1           40.73MB
   ```

2. FlexClone 볼륨과 상위 항목이 포함된 애그리게이트에 충분한 공간이 있는지 확인합니다.
   a. FlexClone 볼륨과 상위 항목이 들어 있는 애그리게이트의 여유 공간 크기를 확인합니다.

      '스토리지 집계 쇼'

   b. 포함된 Aggregate에 사용 가능한 여유 공간이 충분하지 않은 경우 스토리지를 Aggregate에 추가합니다.

      '스토리지 집계 추가 디스크'

3. 분할 작업을 시작합니다.

   '볼륨 클론 분할 시작 - vserver_vserver_name_-FlexClone_clone_volume_name_'

   다음 예제에서는 상위 볼륨 ""vol1""에서 FlexClone 볼륨 ""clone1""을 분할하는 프로세스를 시작하는 방법을 보여

줍니다.

```
cluster1::> volume clone split start -vserver vs1 -flexclone clone1

Warning: Are you sure you want to split clone volume clone1 in Vserver
vs1 ?
{y|n}: y
[Job 1617] Job is queued: Split clone1.
```

4. FlexClone 분할 작업의 상태를 모니터링합니다.

   '볼륨 클론 분할 표시 - vserver_vserver_name_-FlexClone_clone_volume_name_'

   다음 예제는 AFF 시스템에서 FlexClone 분할 작업의 상태를 보여줍니다.

```
cluster1::> volume clone split show -vserver vs1 -flexclone clone1
                                                 Inodes
Blocks
                                      ----------------------
----------------------
Vserver   FlexClone    Processed Total    Scanned  Updated      % Inode
% Block

Complete  Complete
vs1       clone1        0         0       411247   153600         0
37
```

5. 분할 볼륨이 더 이상 FlexClone 볼륨이 아닌지 확인합니다.

   `volume show -volume *volume_name* -fields clone-volume`

   의 값 `clone-volume` FlexClone 볼륨이 아닌 볼륨의 경우 ""false"" 옵션이 있습니다.

   다음 예제에서는 부모로부터 분할된 볼륨 ""clone1""이 FlexClone 볼륨이 아닌지 여부를 확인하는 방법을 보여줍니다.

```
cluster1::> volume show -volume clone1 -fields clone-volume
vserver volume **clone-volume**
------- ------ **-------------**
vs1     clone1 **false**
```

관련 정보

- "스토리지 집계 추가 디스크"

FlexClone 볼륨에서 사용하는 공간을 결정합니다

FlexClone 볼륨의 공칭 크기와 상위 FlexVol 볼륨과 공유하는 공간의 크기를 기준으로 FlexClone 볼륨에서 사용되는 공간을 결정할 수 있습니다. FlexClone 볼륨이 생성되면 상위 볼륨과 모든 데이터를 공유합니다. FlexVol volume의 공칭 크기가 부모 크기와 같지만 Aggregate에서 사용하는 여유 공간은 거의 없습니다.

이 작업에 대해

새로 생성된 FlexClone 볼륨에서 사용하는 여유 공간은 공칭 크기의 약 0.5%입니다. 이 공간은 FlexClone 볼륨의 메타데이터를 저장하는 데 사용됩니다.

상위 또는 FlexClone 볼륨에 쓴 새 데이터는 볼륨 간에 공유되지 않습니다. FlexClone 볼륨에 기록되는 새 데이터의 양이 증가하면 FlexClone 볼륨에 포함된 aggregate에서 필요한 공간이 증가합니다.

단계

1. 'volume show' 명령을 사용하여 FlexClone 볼륨에서 사용하는 실제 물리적 공간을 확인합니다.

   다음 예에서는 FlexClone 볼륨에서 사용하는 총 물리적 공간을 보여 줍니다.

```
cluster1::> volume show -vserver vs01 -volume clone_vol1 -fields
size,used,available,
percent-used,physical-used,physical-used-percent
vserver    volume     size  available  used   percent-used   physical-
used     physical-used-percent
-------    ----------  ----  ---------  -----  ------------
-------------   ---------------------
vs01     clone_vol1   20MB   18.45MB   564KB       7%             196KB
1%
```

   에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

SnapMirror 소스 또는 타겟 볼륨에서 FlexClone 볼륨을 생성할 때의 고려 사항

기존 볼륨 SnapMirror 관계의 소스 또는 타겟 볼륨에서 FlexClone 볼륨을 생성할 수 있습니다. 그러나 이렇게 하면 이후의 SnapMirror 복제 작업이 성공적으로 완료되지 못할 수 있습니다.

FlexClone 볼륨을 생성할 때 SnapMirror에서 사용하는 스냅샷을 잠글 수 있기 때문에 복제가 작동하지 않을 수 있습니다. 이 경우 SnapMirror는 FlexClone 볼륨이 제거되거나 부모로부터 분리될 때까지 대상 볼륨에 대한 복제를 중지합니다. 이 문제를 해결할 수 있는 두 가지 옵션이 있습니다.

- FlexClone 볼륨이 일시적으로 필요하고 SnapMirror 복제가 일시적으로 중단될 수 있는 경우, FlexClone 볼륨을 생성하여 이를 삭제하거나 상위 볼륨에서 분할할 수 있습니다.

  FlexClone 볼륨이 삭제되거나 부모에서 분할될 때 SnapMirror 복제가 정상적으로 계속됩니다.

- SnapMirror 복제의 임시 중단을 허용할 수 없는 경우 SnapMirror 소스 볼륨에 스냅샷을 생성한 다음 해당 스냅샷을 사용하여 FlexClone 볼륨을 생성할 수 있습니다. (대상 볼륨에서 FlexClone 볼륨을 생성하는 경우 해당 스냅샷이 SnapMirror 대상 볼륨에 복제될 때까지 기다려야 합니다.)

SnapMirror 소스 볼륨에 스냅샷을 생성하는 이 방법을 사용하면 SnapMirror에서 사용 중인 스냅샷을 잠그지 않고 클론을 생성할 수 있습니다.

FlexClone 파일 및 FlexClone LUN을 사용하여 파일 및 LUN의 효율적인 복사본을 생성합니다

FlexClone 파일 및 FlexClone LUN 사용 개요

FlexClone 파일 및 FlexClone LUN은 부모 파일 및 부모 LUN의 쓰기 가능한 공간 효율적인 클론이며 물리적 애그리게이트 공간의 효율적인 활용에 도움을 줍니다. FlexClone 파일 및 FlexClone LUN은 FlexVol 볼륨에만 지원됩니다.

FlexClone 파일 및 FlexClone LUN은 크기의 0.4%를 사용하여 메타데이터를 저장합니다. 클론은 상위 파일 및 상위 LUN의 데이터 블록을 공유하며, 클라이언트가 상위 파일 또는 LUN 또는 클론에 새 데이터를 쓸 때까지 최소한의 스토리지 공간을 사용합니다.

클라이언트는 상위 항목과 클론 항목 모두에서 모든 파일 및 LUN 작업을 수행할 수 있습니다.

여러 방법을 사용하여 FlexClone 파일과 FlexClone LUN을 삭제할 수 있습니다.

ONTAP에서 FlexClone 파일 또는 FlexClone LUN을 생성합니다

'volume file clone create' 명령을 사용하여 FlexVol 볼륨이나 FlexClone 볼륨에 있는 파일 및 LUN의 공간 효율적이고 시간 효율적인 클론을 생성할 수 있습니다.

시작하기 전에

- FlexClone 라이센스가 클러스터에 설치되어 있어야 합니다. 이 라이센스는 에 "ONTAP 1 을 참조하십시오 "포함되어 있습니다.
- 하위 LUN 클론 복제나 하위 파일 클론 복제에 여러 블록 범위를 사용하는 경우 블록 번호가 중복되지 않아야 합니다.
- 적응형 압축이 활성화된 볼륨에 대해 하위 LUN 또는 하위 파일을 생성하는 경우 블록 범위가 잘못 정렬되어서는 안 됩니다.

  즉, 소스 시작 블록 번호와 대상 시작 블록 번호는 짝수로 정렬되거나 홀수로 정렬되어야 합니다.

이 작업에 대해

클러스터 관리자가 할당한 권한에 따라 SVM 관리자가 FlexClone 파일 및 FlexClone LUN을 생성할 수 있습니다.

클론 생성 및 수정 시 FlexClone 파일 및 FlexClone LUN에 대한 자동 삭제 설정을 지정할 수 있습니다. 자동 삭제 설정은 기본적으로 해제되어 있습니다.

'volume file clone create' 명령을 '-overwrite-destination' 매개 변수로 사용하여 클론을 생성할 때 기존 FlexClone 파일 또는 FlexClone LUN을 덮어쓸 수 있습니다.

노드가 최대 분할 로드에 도달하면 FlexClone 파일 및 FlexClone LUN 생성 요청을 일시적으로 중단하고 "EBUSY" 오류 메시지를 표시합니다. 노드의 분할 부하가 최대 아래로 떨어지면 노드에서 FlexClone 파일 및 FlexClone LUN 생성 요청을 다시 수락합니다. 생성 요청을 다시 시도하기 전에 노드에 클론을 생성할 수 있는 용량이 있을 때까지 기다려야 합니다.

FlexClone LUN은 상위 LUN의 공간 예약 속성을 상속합니다. 공간 예약 FlexClone LUN에는 공간 예약 상위 LUN과 동일한 공간이 필요합니다. FlexClone LUN이 공간 예약되지 않은 경우 볼륨에 클론의 변경 사항을 수용할 수 있는 충분한 공간이 있어야 합니다.

단계

1. LUN을 클론 복제하는 경우 LUN이 매핑되어 있지 않거나 쓰이지 않는지 확인합니다.
2. FlexClone LUN 또는 파일을 생성합니다.

   `volume file clone create -vserver vserver_name -volume volume_name -source -path source_path -destination-path destination_path`

   다음 예에서는 볼륨 vol1에서 상위 파일 file1_source의 FlexClone 파일 file1_clone을 생성하는 방법을 보여 줍니다.

   ```
   cluster1::> volume file clone create -vserver vs0 -volume vol1 -source
   -path /file1_source -destination-path /file1_clone
   ```

   에 대한 자세한 내용은 `volume file clone create` "ONTAP 명령 참조입니다"을 참조하십시오.

볼륨의 스냅샷에서 **FlexClone LUN**을 생성합니다

볼륨의 스냅샷을 사용하여 LUN의 FlexClone 복사본을 생성할 수 있습니다. LUN의 FlexClone 복사본은 읽기 및 쓰기가 모두 가능합니다.

시작하기 전에

FlexClone 라이센스를 설치해야 합니다. 이 라이센스는 에 "ONTAP 1 을 참조하십시오"포함되어 있습니다.

이 작업에 대해

FlexClone LUN은 상위 LUN의 공간 예약 속성을 상속합니다. 공간 예약 FlexClone LUN에는 공간 예약 상위 LUN과 동일한 공간이 필요합니다. FlexClone LUN이 공간 예약되지 않은 경우 볼륨에 클론의 변경 사항을 수용할 수 있는 충분한 공간이 있어야 합니다.

단계

1. LUN이 매핑되지 않았거나 쓰기 중인지 확인합니다.
2. LUN이 포함된 볼륨의 스냅샷을 생성합니다.

   '볼륨 스냅샷 생성 - vserver_vserver_name_-volume_volume_name_-snapshot_snapshot_name_'

   클론을 생성할 LUN의 스냅샷(백업 스냅샷)을 생성해야 합니다.

3. 스냅샷에서 FlexClone LUN을 생성합니다.

   `volume file clone create -vserver vserver_name -volume volume_name -source -path source_path -snapshot-name snapshot_name -destination-path destination_path`

   자동 삭제를 위해 FlexClone LUN을 사용할 수 있어야 하는 경우 '-autom자동 삭제 true'를 포함합니다. 반씩 프로비저닝을 사용하여 볼륨에 FlexClone LUN을 생성하는 경우 모든 FlexClone LUN에 대해 자동 삭제를

활성화해야 합니다.

4. FlexClone LUN이 올바른지 확인합니다.

   'lun show -vserver_vserver_name _'

```
Vserver Path                      State    Mapped    Type     Size
------- ----------------------    -------- --------- -------- -------
vs1     /vol/vol1/lun1_clone      online   unmapped windows   47.07MB
vs1     /vol/vol1/lun1_snap_clone online   unmapped windows   47.07MB
```

FlexClone 파일 및 **FlexClone LUN**을 생성 및 삭제하기 전에 노드 용량을 확인합니다

노드에 FlexClone 파일 및 FlexClone LUN 생성 및 삭제 요청을 수신하는 용량이 있는지 확인해야 합니다. 이 작업은 노드에 대한 분할 로드를 확인하여 수행할 수 있습니다. 최대 분할 로드에 도달하면 분할 부하가 최대 아래로 떨어질 때까지 새 요청이 수락되지 않습니다.

이 작업에 대해

노드가 최대 분할 로드에 도달하면 요청을 생성하고 삭제하는 데 대한 응답으로 EBUSY 오류 메시지가 표시됩니다. 노드의 분할 부하가 최대 아래로 떨어지면 노드에서 FlexClone 파일 및 FlexClone LUN을 다시 생성하고 삭제하는 요청을 수락합니다.

`Allowable Split Load`필드에 용량이 표시되고 생성 요청이 사용 가능한 용량에 맞을 때 노드는 새 요청을 수락할 수 있습니다.

단계

1. 'volume file clone split load show' 명령을 사용하여 노드에서 FlexClone 파일 및 FlexClone LUN을 생성하고 삭제하는 데 필요한 용량을 확인하십시오.

   다음 예제에서 분할 로드는 cluster1의 모든 노드에 대해 표시됩니다. 클러스터의 모든 노드에는 Allowable Split Load 필드가 나타내는 FlexClone 파일 및 FlexClone LUN을 생성 및 삭제할 수 있는 용량이 있습니다.

```
cluster1::> volume file clone split load show
Node        Max         Current    Token          Allowable
            Split Load  Split Load Reserved Load  Split Load
----------- ----------  ---------- -------------  ----------
node1          15.97TB          0B          100MB    15.97TB
node2          15.97TB          0B          100MB    15.97TB
2 entries were displayed.
```

관련 정보

- "볼륨 파일 클론 분할 로드가 표시됩니다"

FlexClone 파일 및 **FlexClone LUN**을 사용하여 공간 절약 효과를 확인하십시오

FlexClone 파일 및 FlexClone LUN이 포함된 볼륨에서 블록 공유를 통해 절약된 디스크 공간의 비율을 볼 수 있습니다. 이 작업은 용량 계획의 일부로 수행할 수 있습니다.

단계

1. FlexClone 파일 및 FlexClone LUN으로 인해 절약된 공간을 보려면 다음 명령을 입력합니다.

   'df-s volname'입니다

   volname은 FlexVol 볼륨의 이름입니다.

   중복 제거가 설정된 FlexVol 볼륨에 대해 df -s 명령을 실행하면 중복 제거 파일과 FlexClone 파일 및 LUN에서 저장한 공간을 볼 수 있습니다.

예

다음 예제에서는 FlexClone 볼륨 테스트1에서 절약되는 공간을 보여 줍니다.

```
systemA> df -s test1

Filesystem          used    saved    %saved Vserver
/vol/test1/         4828     5744      54%  vs1
```

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

FlexClone 파일 및 **FlexClone LUN**을 삭제하는 방법입니다

여러 방법을 사용하여 FlexClone 파일과 FlexClone LUN을 삭제할 수 있습니다. 사용 가능한 방법을 이해하면 클론을 관리하는 방법을 계획하는 데 도움이 됩니다.

다음 방법을 사용하여 FlexClone 파일 및 FlexClone LUN을 삭제할 수 있습니다.

- FlexVol 볼륨의 사용 가능한 공간이 특정 임계값 아래로 감소할 경우 자동 삭제가 설정된 상태에서 클론을 자동으로 삭제하도록 FlexVol 볼륨을 구성할 수 있습니다.
- NetApp Manageability SDK를 사용하여 클라이언트가 클론을 삭제하도록 구성할 수 있습니다.
- NAS 및 SAN 프로토콜을 사용하여 클라이언트를 사용하여 클론을 삭제할 수 있습니다.

  이 방법은 NetApp Manageability SDK를 사용하지 않으므로 더 느린 삭제 방법은 기본적으로 활성화됩니다. 그러나 볼륨 파일 클론 삭제 명령을 사용하여 FlexClone 파일을 삭제할 때 더 빠른 삭제 방법을 사용하도록 시스템을 구성할 수 있습니다.

FlexVol 볼륨이 자동 삭제 설정을 통해 사용 가능한 공간을 재확보하는 방법

자동 삭제 개요 를 통해 **FlexVol** 볼륨 및 여유 공간 재확보

FlexVol 볼륨의 자동 삭제 설정을 사용하여 FlexClone 파일 및 FlexClone LUN을 자동으로

삭제할 수 있습니다. 자동 삭제를 사용하면 볼륨이 거의 꽉 찼을 때 볼륨에서 사용 가능한 타겟 공간을 재확보할 수 있습니다.

볼륨의 사용 가능한 공간이 특정 임계값 아래로 감소할 경우 FlexClone 파일 및 FlexClone LUN 삭제를 자동으로 시작하도록 볼륨을 구성한 다음, 볼륨의 사용 가능한 타겟 공간이 회수될 때 클론 삭제를 자동으로 중지할 수 있습니다. 클론 자동 삭제를 시작하는 임계값을 지정할 수는 없지만, 클론을 삭제할 수 있는지 여부를 지정하고 볼륨에 사용할 수 있는 가용 공간의 타겟 크기를 지정할 수 있습니다.

볼륨의 사용 가능한 공간이 특정 임계값 아래로 감소하거나 다음 요구 사항 중 _both_가 충족되면 볼륨은 FlexClone 파일과 FlexClone LUN을 자동으로 삭제합니다.

- 자동 삭제 기능은 FlexClone 파일과 FlexClone LUN이 포함된 볼륨에 대해 활성화됩니다.

  명령을 사용하여 FlexVol volume에 대해 자동 삭제 기능을 사용하도록 설정할 수 `volume snapshot autodelete modify` 있습니다. 볼륨에서 FlexClone 파일 및 FlexClone LUN을 자동으로 삭제하려면 매개 변수를 또는 `snap_reserve` 로 `volume` 설정해야 `-trigger` 합니다. 에 대한 자세한 내용은 `volume snapshot autodelete modify` "ONTAP 명령 참조입니다"을 참조하십시오.

- FlexClone 파일 및 FlexClone LUN에 대해 자동 삭제 기능이 활성화됩니다.

  명령을 매개 변수와 함께 `-autodelete` 사용하면 FlexClone 파일 또는 FlexClone LUN에 대해 자동 삭제를 설정할 수 있습니다 `file clone create`. 따라서 클론에 대한 자동 삭제를 사용하지 않도록 설정하고 다른 볼륨 설정이 클론 설정을 재정의하지 않도록 하여 특정 FlexClone 파일 및 FlexClone LUN을 보존할 수 있습니다. 에 대한 자세한 내용은 `file clone create` "ONTAP 명령 참조입니다"을 참조하십시오.

FlexClone 파일과 FlexClone LUN을 자동으로 삭제하도록 FlexVol 볼륨을 구성합니다

볼륨의 사용 가능한 공간이 특정 임계값 아래로 감소할 경우 FlexClone 파일 및 FlexClone LUN 삭제를 자동으로 시작하도록 볼륨을 구성한 다음, 볼륨의 사용 가능한 타겟 공간이 회수될 때 클론 삭제를 자동으로 중지할 수 있습니다. 클론 자동 삭제를 시작하는 임계값을 지정할 수는 없지만, 클론을 삭제할 수 있는지 여부를 지정하고 볼륨에 사용할 수 있는 가용 공간의 타겟 크기를 지정할 수 있습니다.

볼륨의 사용 가능한 공간이 특정 임계값 아래로 감소하거나 다음 요구 사항 중 _both_가 충족되면 볼륨은 FlexClone 파일과 FlexClone LUN을 자동으로 삭제합니다.

- 자동 삭제 기능은 FlexClone 파일과 FlexClone LUN이 포함된 볼륨에 대해 활성화됩니다.

  'volume snapshot Autodelete modify' 명령을 사용하여 FlexVol 볼륨에 대한 자동 삭제 기능을 설정할 수 있습니다. FlexClone 파일 및 FlexClone LUN을 자동으로 삭제하려면 볼륨에 대해 '-trigger' 매개 변수를 'volume' 또는 'snap_reserve'로 설정해야 합니다.

- FlexClone 파일 및 FlexClone LUN에 대해 자동 삭제 기능이 활성화됩니다.

  '-Autodelete' 매개 변수와 함께 'file clone create' 명령을 사용하여 FlexClone 파일 또는 FlexClone LUN에 대한 자동 삭제를 활성화할 수 있습니다. 따라서 클론에 대한 자동 삭제를 사용하지 않도록 설정하고 다른 볼륨 설정이 클론 설정을 재정의하지 않도록 하여 특정 FlexClone 파일 및 FlexClone LUN을 보존할 수 있습니다.

시작하기 전에

- FlexVol 볼륨은 FlexClone 파일과 FlexClone LUN을 포함해야 하며 온라인 상태여야 합니다.

- FlexVol 볼륨은 읽기 전용 볼륨이 아니어야 합니다.

단계

1. 명령을 사용하여 FlexVol volume에서 FlexClone 파일과 FlexClone LUN을 자동으로 삭제할 수 `volume snapshot autodelete modify` 있습니다. 에 대한 자세한 내용은 `volume snapshot autodelete modify` "ONTAP 명령 참조입니다"을 참조하십시오.
   - '-trigger' 파라미터는 volume 또는 snap_reserve를 지정할 수 있다.
   - '-destroy-list' 매개 변수의 경우 한 가지 유형의 클론만 삭제할지 여부와 관계없이 항상 lun_clone, file_clone을 지정해야 합니다. 다음 예에서는 볼륨의 25%가 사용 가능한 공간으로 구성될 때까지 공간 재확보를 위해 FlexClone 파일 및 FlexClone LUN의 자동 삭제를 트리거하도록 볼륨 vol1을 설정하는 방법을 보여줍니다.

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
vol1 -enabled true -commitment disrupt -trigger volume -target-free
-space 25 -destroy-list lun_clone,file_clone

Volume modify successful on volume:vol1
```

> 자동 삭제를 위해 FlexVol 볼륨을 설정하는 동안 '-delitment' 매개 변수의 값을 'estroy'로 설정하면 볼륨의 여유 공간이 지정된 임계값 아래로 떨어지면 '-automete' 매개 변수가 설정된 모든 FlexClone 파일 및 FlexClone LUN이 삭제될 수 있습니다. 그러나 '-Autodelete' 매개 변수가 false로 설정된 FlexClone 파일 및 FlexClone LUN은 삭제되지 않습니다.

2. 명령을 사용하여 FlexVol volume에서 FlexClone 파일 및 FlexClone LUN 자동 삭제가 설정되어 있는지 확인합니다 `volume snapshot autodelete show`. 에 대한 자세한 내용은 `volume snapshot autodelete show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 FlexClone 파일 및 FlexClone LUN을 자동으로 삭제하기 위해 볼륨 vol1이 활성화되어 있는 것을 보여 줍니다.

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1

         Vserver Name: vs1
          Volume Name: vol1
          Enabled: true
            Commitment: disrupt
         Defer Delete: user_created
         Delete Order: oldest_first
  Defer Delete Prefix: (not specified)
    Target Free Space: 25%
              Trigger: volume
     *Destroy List: lun_clone,file_clone*
Is Constituent Volume: false
```

3. 다음 단계를 수행하여 삭제할 볼륨의 FlexClone 파일 및 FlexClone LUN에 대해 자동 삭제를 사용하도록 설정했는지 확인합니다.

a. 명령을 사용하여 특정 FlexClone 파일이나 FlexClone LUN을 자동으로 삭제할 수 있습니다 `volume file clone autodelete`. 에 대한 자세한 내용은 `volume file clone autodelete` "ONTAP 명령 참조입니다"을 참조하십시오.

   '-force' 매개 변수와 함께 'volume file clone autom자동 삭제' 명령을 사용하면 특정 FlexClone 파일 또는 FlexClone LUN을 강제로 자동으로 삭제할 수 있습니다.

   다음 예에서는 볼륨 vol1에 포함된 FlexClone LUN lun1_clone을 자동으로 삭제하는 것을 보여 줍니다.

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path
/vol/vol1/lun1_clone -enabled true
```

   FlexClone 파일 및 FlexClone LUN을 생성할 때 자동 삭제를 설정할 수 있습니다.

b. 명령을 사용하여 FlexClone 파일 또는 FlexClone LUN이 자동 삭제되도록 설정되어 있는지 확인합니다 `volume file clone show-autodelete`. 에 대한 자세한 내용은 `volume file clone show-autodelete` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 FlexClone LUN lun1_clone이 자동 삭제를 위해 설정되었음을 보여 줍니다.

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone
-path vol/vol1/lun1_clone
Vserver Name: vs1
Clone Path: vol/vol1/lun1_clone
**Autodelete Enabled: true**
```

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

FlexClone 파일 또는 **FlexClone LUN**이 자동으로 삭제되지 않도록 방지합니다

FlexClone 파일 및 FlexClone LUN을 자동으로 삭제하도록 FlexVol 볼륨을 구성하는 경우 지정한 조건에 맞는 모든 클론을 삭제할 수 있습니다. 보존하려는 특정 FlexClone 파일 또는 FlexClone LUN이 있는 경우 자동 FlexClone 삭제 프로세스에서 해당 LUN을 제외할 수 있습니다.

시작하기 전에

FlexClone 라이센스를 설치해야 합니다. 이 라이센스는 에 "ONTAP 1 을 참조하십시오"포함되어 있습니다.

이 작업에 대해

FlexClone 파일 또는 FlexClone LUN을 생성할 때 기본적으로 클론에 대한 자동 삭제 설정이 사용되지 않습니다. 자동 삭제가 비활성화된 FlexClone 파일 및 FlexClone LUN은 FlexVol 볼륨을 구성하여 볼륨의 공간을 자동으로 재확보하도록 구성할 때 보존됩니다.

볼륨에 대해 'try' 또는 'disrupt'로 'preserve' 수준을 설정하면 해당 클론에 대해 자동 삭제를 비활성화하여 특정 FlexClone 파일이나 FlexClone LUN을 개별적으로 보존할 수 있습니다. 그러나 볼륨에 대한 '약정' 레벨을 'Destroy'로 설정하고 destroy 목록에 'lun_clone, file_clone'이 포함된 경우 볼륨 설정이 클론 설정을 재정의하고 클론의 자동 삭제 설정에 관계없이 모든 FlexClone 파일과 FlexClone LUN을 삭제할 수 있습니다.

단계

1. '볼륨 파일 클론 자동 삭제' 명령을 사용하여 특정 FlexClone 파일 또는 FlexClone LUN이 자동으로 삭제되지 않도록 합니다.

   다음 예에서는 vol1에 포함된 FlexClone LUN lun1_clone에 대해 자동 삭제를 해제하는 방법을 보여 줍니다.

   ```
   cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
   -clone-path lun1_clone -enable false
   ```

   자동 삭제가 비활성화된 FlexClone 파일 또는 FlexClone LUN은 볼륨의 공간을 재확보하기 위해 자동으로 삭제할 수 없습니다.

2. 'volume file clone show -Autodelete' 명령을 사용하여 FlexClone 파일 또는 FlexClone LUN에 대해 자동 삭제가 비활성화되어 있는지 확인합니다.

   다음 예제에서는 FlexClone LUN lun1_clone에 대한 자동 삭제가 거짓인 것을 보여 줍니다.

   ```
   cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
   vol/vol1/lun1_clone
                                                                  Vserver
   Name: vs1
                                                                  Clone Path:
   vol/vol1/lun1_clone
                                                                  Autodelete
   Enabled: false
   ```

FlexClone 파일 삭제를 구성하는 명령입니다

클라이언트가 NetApp Manageability SDK를 사용하지 않고 FlexClone 파일을 삭제할 때 '볼륨 파일 클론 삭제' 명령을 사용하면 FlexVol 볼륨에서 FlexClone 파일을 더 빠르게 삭제할 수 있습니다. FlexClone 파일의 확장명과 최소 크기를 사용하여 더 빠르게 삭제할 수 있습니다.

볼륨 파일 클론 삭제 명령을 사용하여 지원되는 확장 목록과 볼륨의 FlexClone 파일에 대한 최소 크기 요구 사항을 지정할 수 있습니다. 더 빠른 삭제 방법은 요구사항을 충족하는 FlexClone 파일에만 사용됩니다. 요구 사항을 충족하지 않는 FlexClone 파일의 경우 느린 삭제 방법이 사용됩니다.

NetApp Manageability SDK를 사용하여 고객이 볼륨에서 FlexClone 파일과 FlexClone LUN을 삭제할 경우 더 빠른 삭제 방법이 항상 사용되므로 확장 및 크기 요구사항은 적용되지 않습니다.

대상...	이 명령 사용...
지원되는 볼륨 확장 목록에 확장을 추가합니다	'볼륨 파일 클론 삭제 추가 확장
더 빠른 삭제 방법을 사용하여 볼륨에서 삭제할 수 있는 FlexClone 파일의 최소 크기를 변경합니다	'볼륨 파일 클론 삭제 수정
지원되는 볼륨 확장 목록에서 확장 프로그램을 제거합니다	'볼륨 파일 클론 삭제 제거 - 확장'
더 빠른 삭제 방법을 사용하여 지원되는 확장명 목록과 클라이언트에서 볼륨에서 삭제할 수 있는 FlexClone 파일의 최소 크기를 확인합니다	'볼륨 파일 클론 삭제 표시

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

관련 정보

- "볼륨 파일 클론 삭제"

Qtree를 사용하여 FlexVol 볼륨을 분할합니다

Qtree 및 ONTAP FlexVol volume 파티셔닝

Qtree를 사용하면 FlexVol 볼륨을 개별적으로 관리할 수 있는 더 작은 세그먼트로 파티셔닝할 수 있습니다. qtree가 지원하는 볼륨 파티셔닝은 프로젝트, 사용자 또는 그룹별로 스토리지를 관리할 때 보다 세부적인 제어 수준을 제공합니다. Qtree를 사용하여 할당량, 보안 스타일 및 CIFS oplocks를 효율적으로 관리할 수 있습니다.

ONTAP는 각 볼륨에 대해 * qtree0 * 이라는 기본 qtree를 생성합니다. 데이터를 특정 qtree에 배치하지 않으면 qtree0에 배치됩니다.

일반 제한 사항

운영 환경에서 Qtree를 사용하기 전에 해당 한계를 알아야 합니다. 또한 확장된 qtree 성능 모니터링 기능을 사용할 때 를 작동 및 제한 사항검토하십시오.

- qtree 이름은 64자를 초과할 수 없습니다.
- 쉼표, 공백과 같은 qtree 이름에 사용되는 특정 특수 문자는 다른 ONTAP 기능에 문제가 발생할 수 있으므로 사용하지 않아야 합니다.
- 서로 다른 qtree 간에 디렉토리를 이동할 수 없습니다. Qtree 간에 파일만 이동할 수 있습니다.
- 동일한 FlexVol 또는 SCVMM 풀에 qtree 레벨 및 볼륨 레벨 공유를 생성하는 경우 qtree가 FlexVol 공유에 디렉토리로 표시됩니다. 실수로 삭제하지 않도록 주의해야 합니다.

Qtree 관리 및 구성을 위한 명령

ONTAP CLI를 사용하여 qtree를 관리하고 구성할 수 있습니다. 수행하려는 작업에 따라 다음 명령을 사용하여 qtree를 관리해야 합니다.

이 명령으로 `volume rehost` 인해 동일한 볼륨을 대상으로 하는 다른 동시 관리 작업이 실패할 수 있습니다.

원하는 작업	이 명령 사용…
qtree를 생성합니다	'볼륨 qtree 생성'
qtree의 필터링된 목록을 표시합니다	'볼륨 qtree 표시'
qtree를 삭제합니다	'볼륨 qtree 삭제' qtree가 비어 있거나 플래그를 사용하지 않으면 이 명령은 `-force true` 실패합니다.
qtree의 UNIX 사용 권한을 수정합니다	볼륨 qtree 수정 - unix - 권한
qtree의 CIFS oplocks 설정을 수정합니다	'볼륨 qtree oplocks'
qtree의 보안 설정을 수정합니다	볼륨 qtree 보안
qtree의 이름을 바꿉니다	'볼륨 qtree 이름 변경'
qtree의 통계를 표시합니다	볼륨 qtree 통계
qtree의 통계를 재설정합니다	'볼륨 qtree 통계 - 재설정'

확장된 **qtree** 성능 모니터링

ONTAP 9.16.1부터 ONTAP REST API를 사용하여 지연 시간 메트릭 및 기간별 통계를 비롯한 확장된 qtree 모니터링 기능에 액세스할 수 있습니다.

ONTAP REST API에는 Qtree와 관련된 여러 엔드포인트가 포함됩니다. ONTAP 9.16.1 이전에는 IOPS(초당 IO 작업), 읽기, 쓰기 및 기타 작업을 위한 처리량 등의 qtree에 대한 실시간 통계에 액세스할 수 있었습니다.

ONTAP 9.16.1부터 제공되는 확장된 qtree 성능 모니터링을 통해 NFSv3, NFSv4.0, NFSv4.1, NFSv4.2, pNFS(기술적으로 NFSv4.1 및 NFSv4.2의 일부) 및 CIFS에 대한 IOP 및 처리량뿐만 아니라 실시간 지연 시간 통계를 모니터링할 수 있습니다. 또한 통계를 수집 및 보관하여 성능 기록 데이터를 볼 수 있습니다.

이러한 확장된 모니터링은 스토리지 관리자가 시스템 성능에 대한 보다 뛰어난 통찰력을 제공합니다. 이 데이터를 사용하여 서비스 품질 향상을 위해 작업할 때 고용량 qtree, 잠재적 병목 현상 및 기타 영역을 식별할 수 있습니다. 이러한 지표를 분석하면 더 많은 정보에 입각한 데이터 기반 의사 결정을 내릴 수 있습니다.

작동 및 제한 사항

운영 환경에서 확장 qtree 성능 모니터링 기능을 사용하기 전에 고려해야 할 몇 가지 운영 특성들을 고려해야 합니다.

다시 마운트해야 합니다

Qtree 확장 모니터링을 활성화한 후 이 기능을 활성화하려면 영향을 받은 볼륨을 다시 마운트해야 합니다.

통계의 가용성

확장 성능 모니터링을 활성화한 후에는 통계 데이터를 즉시 사용할 수 없습니다. 여기에는 IOPS, 처리량, 지연 시간 통계가 포함됩니다. qtree의 경우 이 데이터가 표시되기까지 최대 5분이 걸릴 수 있습니다.

클러스터당 **qtree**

ONTAP 클러스터에서 최대 50,000개의 qtree에 대해 확장된 성능 모니터링을 활성화할 수 있습니다.

ONTAP REST API를 사용하여 확장된 메트릭에 액세스할 수 있습니다

ONTAP 9.16.1부터 ONTAP REST API를 통해 확장된 qtree 성능 모니터링 기능에 액세스할 수 있습니다. 기본 기능은 아래 설명된 바와 같이 몇 가지 범주로 분류됩니다.

확장 성능 모니터링을 활성화 및 비활성화합니다

끝점에서 `/api/storage/qtrees` 속성에 액세스하여 확장 모니터링 기능을 사용하거나 사용하지 않도록 설정할 수 `ext_performance_monitoring.enabled` 있습니다. POST 및 패치 방법은 새 qtree를 생성하는지 또는 기존 qtree를 구성하는지에 따라 사용할 수 있습니다.

글로벌 모니터링 메트릭 및 설정을 검색합니다

끝점에 여러 개의 새 글로벌 속성이 `/api/storage/qtrees` 추가되었습니다. Get 메서드를 사용하여 이러한 필드를 검색할 수 있습니다.

특정 **qtree**에 대한 메트릭을 검색합니다

엔드포인트에서 get 방법을 사용하여 특정 볼륨에 정의된 특정 qtree에 대한 새 통계 및 메트릭 속성을 검색할 수 있습니다 `/api/storage/qtrees/{volume.uuid}/{id}/metrics`.

업그레이드 및 되돌리기

ONTAP 9.16.1에서 이 기능을 사용하도록 설정하면 제한 없이 후속 ONTAP 릴리스로 업그레이드할 수 있습니다. 그러나 두 가지 시나리오를 고려해야 합니다.

9.16.1로 업그레이드하고 혼합 버전 클러스터를 처리합니다

클러스터의 유효 클러스터 버전(ECV)이 9.16.1이 될 때까지 확장 성능 모니터링 기능을 사용할 수 없습니다(즉, `ext_performance_monitoring.enabled` 로 설정할 수 없음 `true`).

9.16.1에서 되돌립니다

속성이 로 설정된 `true` qtree가 있으면 `ext_performance_monitoring.enabled` 9.16.1에서 9.15.1로 되돌릴 수 없습니다. 되돌리기 작업이 차단되었습니다. 모범 사례는 이전 ONTAP 릴리즈로 되돌리기 전에 모든 qtree에 대해 로 `false` 설정하는 `ext_performance_monitoring.enabled` 것입니다.

자세한 정보

를 비롯한 ONTAP REST API에 대한 자세한 내용은 ONTAP 자동화 설명서 를 "ONTAP REST API의 새로운 기능" 참조하십시오. ONTAP REST API에 대한 자세한 내용은 ONTAP 자동화 설명서를 "Qtree 엔드포인트" 검토해야 합니다.

qtree 접합 경로를 확보합니다

qtree의 접합 경로 또는 네임스페이스 경로를 획득하여 개별 qtree를 마운트할 수 있습니다. CLI 명령 'qtree show-instance'에 표시되는 qtree 경로는 '/vol/<volume_name>/<qtree_name>' 형식입니다. 그러나 이 경로는 qtree의 접합 경로 또는 네임스페이스 경로를 참조하지 않습니다.

에 대한 자세한 내용은 `qtree show` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

Qtree의 접합 경로 또는 네임스페이스 경로를 확인하려면 볼륨의 접합 경로를 알아야 합니다.

단계

1. 'vserver volume junction-path' 명령을 사용하여 볼륨의 junction path를 구합니다.

   다음 예에서는 vs0이라는 이름의 스토리지 가상 시스템(SVM)에 있는 vol1이라는 볼륨의 접합 경로를 표시합니다.

   ```
   cluster1::> volume show -volume vol1 -vserver vs0 -fields junction-path

   ------- ------ -------------

   vs0 vol1 /vol1
   ```

   위 출력에서 볼륨의 접합 경로는 '/vol1'입니다. Qtree는 항상 볼륨에 루팅되므로 Qtree의 접합 경로 또는 네임스페이스 경로는 '/vol1/qtree1'이 됩니다.

에 대한 자세한 내용은 `vserver volume junction-path` "ONTAP 명령 참조입니다"을 참조하십시오.

디렉토리에서 qtree로 전환

디렉토리를 qtree로 변환합니다

FlexVol volume의 루트에 qtree로 전환하려는 디렉토리가 있는 경우 클라이언트 애플리케이션을 사용하여 디렉토리에 있는 데이터를 같은 이름의 새 qtree로 마이그레이션해야 합니다.

이 작업에 대해

디렉토리를 qtree로 변환하기 위한 단계는 사용하는 클라이언트에 따라 다릅니다. 다음 프로세스에서는 완료해야 하는 일반적인 작업을 간략하게 설명합니다.

시작하기 전에

기존 CIFS 공유와 연결된 디렉토리는 삭제할 수 없습니다.

단계

1. qtree로 만들 디렉토리의 이름을 바꿉니다.
2. 원래 디렉토리 이름을 사용하여 새 qtree를 생성합니다.
3. 클라이언트 애플리케이션을 사용하여 디렉토리의 컨텐츠를 새 qtree로 이동합니다.

4. 지금 빈 디렉토리를 삭제합니다.

Windows 클라이언트를 사용하여 디렉토리를 **qtree**로 변환합니다

Windows 클라이언트를 사용하여 디렉토리를 qtree로 변환하려면 디렉토리의 이름을 바꾸고 스토리지 시스템에 qtree를 생성한 다음 디렉토리의 콘텐츠를 qtree로 이동합니다.

이 작업에 대해

이 절차를 수행하려면 Windows 탐색기를 사용해야 합니다. Windows 명령줄 인터페이스 또는 DOS 프롬프트 환경에서는 사용할 수 없습니다.

단계

1. Windows 탐색기를 엽니다.
2. 변경할 디렉토리의 폴더 표현을 클릭합니다.

   디렉토리는 포함하는 볼륨의 루트에 있어야 합니다.

3. 파일 * 메뉴에서 * 이름 바꾸기 * 를 선택하여 이 디렉터리에 다른 이름을 지정합니다.
4. 스토리지 시스템에서 명령을 사용하여 `volume qtree create` 원래 디렉토리 이름을 가진 새 qtree를 생성합니다. 에 대한 자세한 내용은 `volume qtree create` "ONTAP 명령 참조입니다"을 참조하십시오.
5. Windows 탐색기에서 이름이 바뀐 디렉토리 폴더를 열고 폴더 안의 파일을 선택합니다.
6. 이러한 파일을 새 qtree의 폴더 표시로 끕니다.

   이동하는 폴더에 포함된 하위 폴더가 많을수록 이동 작업이 오래 걸립니다.

7. 파일 * 메뉴에서 * 삭제 * 를 선택하여 이름이 바뀐 지금 비어 있는 디렉토리 폴더를 삭제합니다.

UNIX 클라이언트를 사용하여 디렉토리를 **qtree**로 변환합니다

UNIX에서 디렉토리를 qtree로 변환하려면 디렉토리의 이름을 바꾸고 스토리지 시스템에서 qtree를 생성한 다음 디렉토리의 컨텐츠를 qtree로 이동합니다.

단계

1. UNIX 클라이언트 창을 엽니다.
2. mv 명령을 사용하여 디렉토리의 이름을 바꿉니다.

```
client: mv /n/user1/vol1/dir1 /n/user1/vol1/olddir
```

3. 스토리지 시스템에서 'volume qtree create' 명령을 사용하여 원래 이름의 qtree를 생성합니다.

```
system1: volume qtree create /n/user1/vol1/dir1
```

에 대한 자세한 내용은 `volume qtree create` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 클라이언트에서 mv 명령을 사용하여 이전 디렉토리의 컨텐츠를 qtree로 이동합니다.

   이동 중인 디렉토리에 있는 하위 디렉토리가 많을수록 이동 작업이 더 오래 걸립니다.

```
client: mv /n/user1/vol1/olddir/* /n/user1/vol1/dir1
```

5. rmdir 명령을 사용하여 현재 비어 있는 이전 디렉토리를 삭제합니다.

```
client: rmdir /n/user1/vol1/olddir
```

작업을 마친 후

UNIX 클라이언트가 mv 명령을 구현하는 방법에 따라 파일 소유권 및 권한이 유지되지 않을 수 있습니다. 이 경우 파일 소유자와 권한을 이전 값으로 업데이트합니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

볼륨에 대한 논리적 공간 보고 및 적용

볼륨 개요를 위한 논리적 공간 보고 및 적용

ONTAP 9.4부터 볼륨에 사용된 논리적 공간과 사용자에게 표시할 남은 스토리지 공간의 양을 허용할 수 있습니다. ONTAP 9.5부터 사용자가 사용하는 논리적 공간의 양을 제한할 수 있습니다.

논리적 공간 보고 및 적용은 기본적으로 해제되어 있습니다.

다음 볼륨 유형은 논리 공간 보고 및 적용을 지원합니다.

볼륨 유형입니다	공간 보고가 지원됩니까?	공간 적용이 지원됩니까?
FlexVol 볼륨	예, ONTAP 9.4부터 시작합니다	예, ONTAP 9.5부터 시작합니다
SnapMirror 타겟 볼륨	예, ONTAP 9.8부터 시작합니다	예, ONTAP 9.13.1
FlexGroup 볼륨	예, ONTAP 9.9.1부터 시작합니다	예, ONTAP 9.9.1부터 시작합니다
FlexCache 볼륨	오리진 설정이 캐시에 사용됩니다	해당 없음

논리적 공간 적용

논리적 공간 적용은 볼륨이 꽉 찼거나 거의 꽉 찼을 때 사용자에게 알림을 제공합니다. ONTAP 9.5 이상에서 논리적 공간 적용을 활성화하면 ONTAP는 볼륨에서 논리적 사용 블록을 계산하여 해당 볼륨에서 여전히 사용 가능한 공간을 결정합니다. 볼륨에 사용 가능한 공간이 없는 경우 시스템은 ENOSPC(공간 부족) 오류 메시지를 반환합니다.

논리적 공간 적용은 볼륨에서 사용 가능한 공간을 알리기 위해 세 가지 유형의 경고를 반환합니다.

- monitor.vol.full.inc.sav`: 이 알림은 볼륨에서 논리적 공간의 98%가 사용된 경우에 트리거됩니다.
- monitor.vol.nearFull.inc.sav`: 이 알림은 볼륨에서 논리적 공간의 95%가 사용된 경우에 트리거됩니다.
- "Vol.log.overalloc.inc.sav`: 볼륨에 사용된 논리적 공간이 볼륨의 총 크기보다 클 경우 이 경고가 트리거됩니다.

  이 알림은 초과 할당된 논리 블록에서 공간이 이미 소비되므로 볼륨 크기에 추가하지 않으면 사용 가능한 공간을 생성하지 않을 수 있음을 알려줍니다.

> 총(논리적 공간)은 논리적 공간 적용이 있는 볼륨의 스냅숏 예비 공간을 제외하고 프로비저닝된 공간과 같아야 합니다.

자세한 내용은 을 "가득 차면 추가 공간을 자동으로 제공하도록 볼륨을 구성합니다"참조하십시오.

논리적 공간 보고

볼륨에서 논리적 공간 보고를 활성화하면 시스템에서 볼륨의 총 공간 외에 논리적 사용 공간 및 사용 가능한 공간의 양을 표시할 수 있습니다. 또한 Linux 및 Windows 클라이언트 시스템의 사용자는 물리적 사용 공간과 물리적 사용 가능한 공간 대신 논리적 사용 공간 및 사용 가능한 공간을 확인할 수 있습니다.

정의:

- 물리적 공간은 볼륨에서 사용 가능하거나 사용되는 스토리지의 물리적 블록을 나타냅니다.
- 논리적 공간은 볼륨의 사용 가능한 공간을 나타냅니다.
- 사용된 논리적 공간은 물리적 공간과 함께 사용된 공간 및 구성된 스토리지 효율성 기능(예: 중복제거 및 압축)을 통한 절약입니다.

ONTAP 9.5부터 공간 보고와 함께 논리적 공간 적용을 활성화할 수 있습니다.

활성화된 경우 논리적 공간 보고는 'volume show' 명령을 사용하여 다음 매개 변수를 표시합니다.

매개 변수	의미
논리적 사용	지정된 논리적 사용 크기가 있는 볼륨 또는 볼륨에 대한 정보만 표시합니다. 이 값에는 물리적으로 사용된 공간과 함께 스토리지 효율성 기능으로 절약되는 모든 공간이 포함됩니다. 여기에는 스냅숏 예비 공간은 포함되지 않지만 스냅숏 유출이 고려됩니다.
논리적-사용-AFS	활성 파일 시스템에서 사용하는 지정된 논리적 크기를 가진 볼륨에만 정보를 표시합니다. 이 값은`-logical-used` 스냅샷 예비 공간을 초과하는 스냅숏 유출 양의 값과 다릅니다.
'-logical-available'(논리적-사용 가능)	논리적 공간 보고만 활성화되면 물리적 가용 공간만 표시됩니다. 공간 보고와 적용이 모두 설정된 경우 스토리지 효율성 기능에 의해 사용 중인 공간을 고려하여 현재 사용 가능한 여유 공간의 양이 표시됩니다. 여기에는 스냅숏 예비 공간이 포함되지 않습니다.

매개 변수	의미
논리적-사용-퍼센트	볼륨의 스냅숏 예비 공간을 제외하고 프로비저닝된 크기의 현재 값의 백분율을 표시합니다 `-logical-used`. 이 값에는 볼륨의 효율성 절감이 포함되므로 이 값은 100%보다 클 수 있습니다. `-logical-used-by-afs` `-logical-used-by-afs`볼륨 값에는 사용된 공간으로 스냅숏 유출이 포함되지 않습니다. `-physical-used`볼륨 값에는 사용된 공간으로 스냅숏 유출이 포함됩니다.
중고	사용자 데이터와 파일 시스템 메타데이터가 차지하는 공간의 크기를 표시합니다. 향후 쓰기를 위해 예약되는 공간과 애그리게이트 스토리지 효율성에 의해 절약되는 공간의 합계에 따라 공간과는 다릅니다 `physical-used`. 여기에는 스냅샷 오버플로(스냅샷이 스냅숏 예비 공간을 초과하는 공간)가 포함됩니다. 스냅숏 예비 공간은 포함되지 않습니다.

CLI에서 논리 공간 보고를 활성화하면 System Manager에 논리 사용 공간(%) 및 논리 공간 값이 표시됩니다

클라이언트 시스템은 다음 시스템 디스플레이에 ""사용된"" 공간으로 표시되는 논리 공간을 확인합니다.

- Linux 시스템에서 * df * 출력
- Windows 시스템에서 Windows 탐색기를 사용하여 속성 아래의 공간 세부 정보를 표시합니다.

> 논리적 공간 강제 적용 없이 논리 공간 보고를 사용하는 경우 클라이언트 시스템에 표시되는 총 용량이 프로비저닝된 공간보다 클 수 있습니다.

논리적 공간 보고 및 적용을 설정합니다

ONTAP 9.4부터 논리 공간 보고를 활성화할 수 있습니다. 9.5부터 논리 공간 적용 또는 보고와 적용을 함께 사용할 수 있습니다.

이 작업에 대해

개별 볼륨 레벨에서 논리적 공간 보고 및 적용을 활성화할 뿐만 아니라 기능을 지원하는 모든 볼륨에서 SVM 레벨에서 활성화할 수 있습니다. 전체 SVM에 대해 논리적 공간 기능을 활성화할 경우 개별 볼륨에 대해 LUN을 비활성화할 수도 있습니다.

ONTAP 9.8부터 SnapMirror 소스 볼륨에서 논리적 공간 리포팅을 활성화하면 전송 후에 타겟 볼륨에서 자동으로 활성화됩니다.

ONTAP 9.13.1 부터 SnapMirror 소스 볼륨에서 적용 옵션이 활성화된 경우, 타겟은 논리적 공간 소비를 보고하고 성능 적용을 존중하여 더 나은 용량 계획을 수립합니다.

> ONTAP 9.13.1 이전의 ONTAP 릴리즈를 실행 중인 경우 적용 설정이 SnapMirror 대상 볼륨으로 전송되지만 대상 볼륨은 적용을 지원하지 않는다는 점을 이해해야 합니다. 따라서 대상은 논리 공간 소비를 보고하지만 해당 적용을 존중하지 않습니다.

에 대해 자세히 "논리적 공간 보고를 위한 ONTAP 릴리즈 지원"알아보십시오.

단계

다음 중 하나 이상을 활성화합니다.

- 볼륨에 대한 논리 공간 보고 활성화:

  ```
  volume modify -vserver svm_name -volume volume_name -size volume_size -is
  -space-reporting-logical true
  ```

- 볼륨에 대한 논리적 공간 적용 활성화:

  ```
  volume modify -vserver svm_name -volume volume_name -size volume_size -is
  -space-enforcement-logical true
  ```

- 볼륨에 대한 논리적 공간 보고 및 적용을 함께 활성화합니다.

  ```
  volume modify -vserver svm_name -volume volume_name -size volume_size -is
  -space-reporting-logical true -is-space-enforcement-logical true
  ```

- 새로운 SVM에 대한 논리적 공간 보고 또는 적용 지원

  ```
  vserver create -vserver _svm_name_ -rootvolume root-_volume_name_ -rootvolume
  -security-style unix -data-services {desired-data-services} [-is-space-
  reporting-logical true] [-is-space-enforcement-logical true]
  ```

- 기존 SVM에 대해 논리 공간 보고 또는 적용 지원

  ```
  vserver modify -vserver _svm_name_ {desired-data-services} [-is-space-
  reporting-logical true] [-is-space-enforcement-logical true]
  ```

SVM 용량 한도 관리

ONTAP 9.13.1 부터 스토리지 VM(SVM)의 최대 용량을 설정할 수 있습니다. SVM이 임계값 용량 수준에 도달할 경우에도 경고를 구성할 수 있습니다.

이 작업에 대해

SVM의 용량은 FlexVol, FlexGroup 볼륨, FlexClone, FlexCache 볼륨의 합으로 계산됩니다. 볼륨이 제한, 오프라인 또는 삭제 후 복구 대기열에 있더라도 용량 계산에 영향을 미칩니다. 자동 증량으로 구성된 볼륨이 있는 경우 볼륨의 최대 자동 크기 조정 값은 SVM 크기를 기준으로 계산되며, 자동 증가 없이 볼륨의 실제 크기가 계산됩니다.

다음 표는 방법을 보여줍니다 `autosize-mode` 매개 변수는 용량 계산에 영향을 줍니다.

`autosize-mode off`	크기 매개 변수는 계산에 사용됩니다
`autosize-mode grow`	를 클릭합니다 `max-autosize` 매개 변수는 계산에 사용됩니다
`autosize-mode grow-shrink`	를 클릭합니다 `max-autosize` 매개 변수는 계산에 사용됩니다

시작하기 전에

- SVM 한도를 설정하려면 클러스터 관리자여야 합니다.
- ONTAP 9.16.1부터 다음 데이터 보호 유형을 포함한 데이터 보호 볼륨을 포함하는 SVM에 대해 스토리지 한도를

구성할 수 있습니다.

  - 다중 구간 없이 비동기식 DR의 FlexVol 볼륨을 지원합니다
  - 동기식 DR의 FlexVol 볼륨(동기식 및 엄격한 동기화 정책 모두)
  - "복원"

- 다음 구성에서는 SVM에 대한 스토리지 제한이 _not_지원되지 않습니다.
  - SnapMirror 볼트 관계
  - SnapMirror 활성 동기화
  - FlexGroup 볼륨
  - 정합성 보장 그룹
  - SVM DR
  - 계단식 배열
  - MetroCluster
- ONTAP 9.16.1부터 로드 공유 미러 관계를 생성할 때 대상 SVM에서 저장소 제한을 활성화할 수 없습니다.
- SVM을 마이그레이션할 때 소스 SVM에서 스토리지 제한을 설정할 수 없습니다. 마이그레이션 작업을 완료하려면 소스에서 스토리지 제한을 해제한 다음 마이그레이션을 완료합니다.
- SVM 용량은 와 다릅니다 할당량. 할당량은 최대 크기를 초과할 수 없습니다.
- SVM에서 다른 작업이 진행 중인 경우에는 스토리지 제한을 설정할 수 없습니다. `job show vserver <svm_name>`기존 작업을 보려면 명령을 사용하십시오. 작업이 완료되면 명령을 다시 실행해 보십시오. 에 대한 자세한 내용은 `job show "ONTAP 명령 참조입니다"을 참조하십시오.

용량 영향

용량 제한에 도달하면 다음 작업이 실패합니다.

- LUN, 네임스페이스 또는 볼륨 생성
- LUN, 네임스페이스 또는 볼륨의 클론 생성
- LUN, 네임스페이스 또는 볼륨 수정
- LUN, 네임스페이스 또는 볼륨의 크기 늘리기
- LUN, 네임스페이스 또는 볼륨 확장
- LUN, 네임스페이스 또는 볼륨을 재호스팅

새 **SVM**에 용량 한도를 설정합니다

시스템 관리자

단계

1. 스토리지 * > * 스토리지 VM * 을 선택합니다.
2. + Add 를 선택하여 SVM을 생성합니다.
3. SVM의 이름을 지정하고 * 액세스 프로토콜 * 을 선택합니다.
4. 스토리지 VM 설정 * 에서 * 최대 용량 제한 사용 * 을 선택합니다.

   SVM의 최대 용량 크기를 제공합니다.

5. 저장 * 을 선택합니다.

CLI를 참조하십시오

단계

1. SVM을 생성합니다. 저장소 제한을 설정하려면 을 제공합니다 `storage-limit` 값. 스토리지 제한에 대한 임계값 알림을 설정하려면 에 대한 백분율 값을 제공합니다 `-storage-limit-threshold-alert`.

```
vserver create -vserver <vserver_name> -aggregate <aggregate_name>
-rootvolume <root_volume_name> -rootvolume-security-style
{unix|ntfs|mixed} -storage-limit <value> [GiB|TIB] -storage-limit
-threshold-alert <percentage> [-ipspace <IPspace_name>] [-language
<language>] [-snapshot-policy <snapshot_policy_name>] [-quota-policy
<quota_policy_name>] [-comment <comment>]
```

   임계값을 제공하지 않으면 기본적으로 SVM이 90% 용량에 도달하면 경고가 트리거됩니다. 임계값 경고를 비활성화하려면 값을 0으로 입력합니다.

2. SVM이 성공적으로 생성되었는지 확인합니다.

```
vserver show -vserver <vserver_name>
```

3. 스토리지 제한을 비활성화하려면 SVM에 대한 매개 변수를 0으로 설정합니다 `-storage-limit`.

```
vserver modify -vserver <vserver_name> -storage-limit 0
```

기존 **SVM**의 용량 제한을 설정하거나 수정합니다

기존 SVM에 대해 용량 한도 및 임계값 알림을 설정하거나 용량 한도를 비활성화할 수 있습니다.

용량 제한을 설정한 후에는 현재 할당된 용량보다 작은 값으로 제한을 수정할 수 없습니다.

시스템 관리자

단계

1. 스토리지 * > * 스토리지 VM * 을 선택합니다.
2. 수정할 SVM을 선택합니다. SVM 이름 옆에 있는 * Edit * (편집 *)를 선택합니다 ⋮ .
3. 용량 제한을 활성화하려면 * Enable capacity limit(용량 제한 활성화) * 옆의 상자를 선택합니다. 최대 용량 * 의 값과 * 경고 임계값 * 의 백분율 값을 입력합니다.

   용량 제한을 비활성화하려면 * Enable capacity limit * (용량 제한 활성화 *) 옆의 확인란을 선택 취소합니다.
4. 저장 * 을 선택합니다.

CLI를 참조하십시오

단계

1. SVM을 호스팅하는 클러스터에서 를 실행합니다 `vserver modify` 명령. 에 대한 숫자 값을 입력합니다 `-storage-limit` 에 대한 백분율 값을 표시합니다 `-storage-limit-threshold-alert`.

   ```
   vserver modify -vserver <vserver_name> -storage-limit <value>
   [GiB|TIB] -storage-limit-threshold-alert <percentage>
   ```

   임계값을 제공하지 않으면 기본 경고가 90% 용량으로 표시됩니다. 임계값 경고를 비활성화하려면 값을 0으로 입력합니다.
2. 스토리지 제한을 해제하려면 SVM에 대해 를 0으로 설정합니다 `-storage-limit`.

   ```
   vserver modify -vserver <vserver_name> -storage-limit 0
   ```

용량 제한에 도달했습니다

최대 용량 또는 경고 임계값에 도달하면 를 참조할 수 있습니다 `vserver.storage.threshold` EMS 메시지를 표시하거나 System Manager의 * Insights * 페이지를 사용하여 가능한 작업에 대해 알아봅니다. 가능한 해결 방법은 다음과 같습니다.

- SVM의 최대 용량 한도 편집
- 볼륨 복구 대기열을 삭제하여 공간을 확보합니다
- 볼륨을 위한 공간을 제공하려면 스냅샷을 삭제하십시오

관련 정보

- System Manager의 용량 측정
- System Manager에서 클러스터, 계층, SVM 용량 모니터링
- "SVM 생성"
- "vserver show 를 참조하십시오"

- "SVM 수정"

할당량을 사용하여 리소스 사용을 제한하거나 추적합니다

할당량 프로세스 개요

할당량, 할당량 규칙 및 할당량 정책을 이해합니다

할당량은 FlexVol 볼륨에 대한 할당량 규칙에서 정의됩니다. 이러한 할당량 규칙은 스토리지 가상 머신(SVM)의 할당량 정책에서 함께 수집되고 SVM의 각 볼륨에서 활성화됩니다.

할당량 규칙은 항상 볼륨에 따라 다릅니다. 할당량 규칙에 정의된 볼륨에서 할당량을 활성화할 때까지는 할당량 규칙이 적용되지 않습니다.

할당량 정책은 SVM의 모든 볼륨에 대한 할당량 규칙의 모음입니다. 할당량 정책은 SVM 간에 공유되지 않습니다. SVM에는 할당량 정책의 백업 복사본을 만들 수 있는 할당량 정책을 최대 5개까지 지정할 수 있습니다. 한 번에 하나의 할당량 정책이 SVM에 할당됩니다. 볼륨에서 할당량을 초기화하거나 크기를 조정할 때 현재 SVM에 할당된 할당량 정책의 할당량 규칙을 활성화할 수 있습니다.

할당량은 ONTAP에서 적용하는 실제 제한이나 ONTAP가 수행하는 실제 추적입니다. 할당량 규칙은 항상 하나 이상의 할당량을 발생시키고 이로 인해 많은 추가 파생 할당량이 발생할 수 있습니다. 적용된 할당량의 전체 목록은 할당량 보고서에만 표시됩니다.

활성화는 ONTAP를 트리거하여 할당된 할당량 정책의 현재 할당량 규칙 집합에서 적용된 할당량을 생성하는 프로세스입니다. 활성화는 볼륨별로 발생합니다. 볼륨에서 처음으로 할당량을 활성화하는 것을 초기화라고 합니다. 이후의 활성화는 변경 범위에 따라 재초기화 또는 크기 조정이라고 합니다.

할당량 사용의 이점

할당량을 사용하여 FlexVol 볼륨의 리소스 사용량을 관리하고 모니터링할 수 있습니다.

할당량을 정의하면 몇 가지 이점이 있습니다. 기본값, 명시적, 파생 및 추적 할당량을 사용하여 가장 효율적인 방법으로 디스크 사용량을 관리할 수 있습니다.

리소스 사용을 제한합니다

디스크 공간이나 사용자 또는 그룹이 사용하거나 qtree에 포함된 파일의 수를 제한할 수 있습니다.

리소스 사용을 추적합니다

제한 없이 사용자, 그룹 또는 qtree에서 사용되는 디스크 공간 또는 파일 수를 추적할 수 있습니다.

사용자에게 알립니다

리소스 사용량이 특정 수준에 도달하면 알림을 생성할 수 있습니다. 디스크 또는 파일 사용량이 너무 높을 때 사용자에게 경고합니다.

할당량 프로세스

할당량을 통해 사용자, 그룹 또는 qtree가 사용하는 파일 수와 디스크 공간을 제한하거나 추적할 수 있습니다. 할당량은 특정 FlexVol 볼륨 또는 qtree에 적용됩니다.

할당량은 소프트 또는 하드일 수 있습니다. 소프트 할당량을 사용하면 ONTAP에서 지정된 제한을 초과할 때 알림을

보내고, 하드 할당량을 사용하면 지정된 제한을 초과할 때 쓰기 작업이 성공하지 못합니다.

ONTAP가 사용자 또는 사용자 그룹으로부터 FlexVol 볼륨에 쓰기 요청을 수신하면 사용자 또는 사용자 그룹의 해당 볼륨에서 할당량이 활성화되었는지 확인하고 다음을 확인합니다.

- 하드 제한값에 도달할지 여부

  yes인 경우 하드 제한값에 도달하고 하드 할당량 알림이 전송되면 쓰기 작업이 실패합니다.

- 소프트 제한값을 위반할지 여부

  yes인 경우 소프트 제한값이 위반되고 소프트 할당량 알림이 전송되면 쓰기 작업이 성공합니다.

- 쓰기 작업이 소프트 제한값을 초과하지 않는지 여부

  예 인 경우 쓰기 작업이 성공하고 알림이 전송되지 않습니다.

하드, 소프트 및 임계값 할당량 간의 차이

하드 할당량은 작업을 차단하는 반면 소프트 할당량은 알림을 트리거합니다.

하드 할당량은 시스템 리소스에 엄격한 제한을 부과하며, 제한을 초과하는 작업은 모두 실패합니다. 다음 설정은 하드 할당량을 생성합니다.

- Disk Limit 매개 변수입니다
- 파일 제한 매개 변수

소프트 할당량은 리소스 사용량이 특정 수준에 도달해도 데이터 액세스 작업에는 영향을 주지 않으므로 할당량이 초과되기 전에 적절한 조치를 취할 수 있도록 경고 메시지를 보냅니다. 다음 설정은 소프트 할당량을 생성합니다.

- Disk Limit 매개 변수의 임계값입니다
- 소프트 디스크 제한 매개 변수입니다
- 소프트 파일 제한 매개 변수

임계값 및 소프트 디스크 할당량을 통해 관리자는 할당량에 대한 알림을 두 개 이상 받을 수 있습니다. 일반적으로 관리자는 디스크 한계 임계값을 디스크 한계보다 약간 작은 값으로 설정하여 쓰기 시작 전에 임계값이 "최종 경고"를 제공할 수 있도록 합니다.

할당량 알림에 대해 알아봅니다

할당량 알림은 EMS(이벤트 관리 시스템)로 전송되고 SNMP 트랩으로도 구성된 메시지입니다.

알림은 다음 이벤트에 대한 응답으로 전송됩니다.

- 즉, 하드 할당량에 도달했습니다. 즉, 할당량을 초과하려고 합니다
- 소프트 할당량을 초과했습니다
- 소프트 할당량을 더 이상 초과하지 않습니다

임계값은 다른 소프트 할당량과 약간 다릅니다. 임계값은 알림이 더 이상 초과하지 않는 경우에만 알림을 트리거합니다.

볼륨 할당량 수정 명령을 사용하여 하드 할당량 알림을 구성할 수 있습니다. 이러한 메시지를 완전히 끌 수 있으며, 예를 들어 중복된 메시지를 보내지 않도록 간격을 변경할 수 있습니다.

할당량 소프트 알림은 중복 메시지를 생성할 가능성이 낮고 유일한 목적은 알림이므로 구성할 수 없습니다.

다음 표에는 할당량이 EMS 시스템으로 전송되는 이벤트가 나열되어 있습니다.

이 경우...	이 이벤트는 **EMS**로 전송됩니다.
트리 할당량의 하드 제한값에 도달했습니다	WAFL.quota.qtree.exceeded
볼륨의 사용자 할당량이 하드 제한값에 도달했습니다	'wafl.quota.user.exceeded` (UNIX 사용자의 경우)' wafl.quota.user.exceeded.win` (Windows 사용자의 경우)
qtree의 사용자 할당량에서 하드 제한값에 도달했습니다	'wafl.quota.userQtree.exceeded` (UNIX 사용자의 경우)' wafl.quota.userQtree.exceeded.win` (Windows 사용자의 경우)
볼륨의 그룹 할당량이 하드 제한값에 도달했습니다	"wafl.quota.group.exceeded`
qtree의 그룹 할당량에서 하드 제한값에 도달했습니다	"wafl.quota.groupQtree.exceeded`
임계값을 포함한 소프트 제한값을 초과했습니다	쿼터소프트리미트 초과
소프트 제한값을 더 이상 초과하지 않습니다	"quota.softlimit.normal`

다음 표에는 할당량이 생성하는 SNMP 트랩이 나열되어 있습니다.

이 경우...	이 **SNMP** 트랩이 전송되었습니다...
하드 제한값에 도달했습니다	쿼타Exceeded.(쿼타Exceed
임계값을 포함한 소프트 제한값을 초과했습니다	QuotaExceeded 및 softQuotaExceeded.를 참조하십시오
소프트 제한값을 더 이상 초과하지 않습니다	QuotaNormal 및 softQuotaNormal을 참조하십시오

알림에는 qtree 이름이 아닌 qtree ID 번호가 포함되어 있습니다. 'volume qtree show-id' 명령을 사용하여 qtree 이름과 ID 번호를 상호 연결할 수 있습니다.

할당량 대상 및 유형

모든 할당량에는 특정 유형이 있습니다. 할당량 대상은 유형에서 파생되며 할당량 제한이 적용되는 사용자, 그룹 또는 qtree를 지정합니다.

다음 표에는 할당량 타겟, 각 할당량 타겟이 연결되는 할당량 유형 및 각 할당량 타겟이 표시되는 방법이 나와 있습니다.

할당량 대상	할당량 유형입니다	대상 표시 방법	참고
사용자	사용자 할당량	UNIX 사용자 이름 UNIX UID입니다 UID가 사용자와 일치하는 파일 또는 디렉토리입니다 Windows 2000 이전 형식의 Windows 사용자 이름입니다 Windows SID 사용자의 SID가 소유한 ACL이 있는 파일 또는 디렉토리입니다	사용자 할당량은 특정 볼륨 또는 qtree에 적용할 수 있습니다.
그룹	그룹 할당량	UNIX 그룹 이름 UNIX GID입니다 GID가 그룹과 일치하는 파일 또는 디렉토리입니다	그룹 할당량은 특정 볼륨 또는 qtree에 적용할 수 있습니다. ONTAP는 Windows ID를 기준으로 그룹 할당량을 적용하지 않습니다.
qtree입니다	트리 할당량	qtree 이름입니다	트리 할당량은 특정 볼륨에 적용되며 다른 볼륨의 qtree에 영향을 주지 않습니다.
""""	사용자 quotagrop 할당량입니다 트리 할당량	큰따옴표("")	""의 할당량 대상은 _ 기본 할당량 _ 을(를) 나타냅니다. 기본 할당량의 경우 할당량 유형은 유형 필드의 값에 의해 결정됩니다.

특별한 종류의 할당량입니다

기본 할당량의 작동 방식

기본 할당량을 사용하여 지정된 할당량 유형의 모든 인스턴스에 할당량을 적용할 수 있습니다. 예를 들어, 기본 사용자 할당량은 지정된 FlexVol 볼륨 또는 qtree의 시스템 모든 사용자에게 영향을 미칩니다. 또한 기본 할당량을 통해 할당량을 쉽게 수정할 수 있습니다.

기본 할당량을 사용하면 각 타겟에 대해 별도의 할당량을 생성하지 않고 대규모 할당량 타겟 세트에 제한을 자동으로 적용할 수 있습니다. 예를 들어 대부분의 사용자를 10GB의 디스크 공간으로 제한하려면 각 사용자에 대한 할당량을 생성하는 대신 10GB의 디스크 공간으로 기본 사용자 할당량을 지정할 수 있습니다. 다른 제한을 적용할 특정 사용자가 있는 경우 해당 사용자에 대해 명시적 할당량을 생성할 수 있습니다. (명시적 할당량 — 특정 타겟 또는 타겟 목록이 있는 할당량 — 기본 할당량을 재정의합니다.)

또한 기본 할당량을 사용하면 할당량 변경 사항을 적용하려는 경우 다시 초기화하는 대신 크기 조정을 사용할 수 있습니다. 예를 들어 기본 사용자 할당량이 이미 있는 볼륨에 명시적 사용자 할당량을 추가하는 경우 크기를 조정하여 새

할당량을 활성화할 수 있습니다.

기본 할당량은 세 가지 유형의 할당량 대상(사용자, 그룹 및 qtree)에 모두 적용될 수 있습니다.

기본 할당량에 지정된 제한이 없을 필요는 없습니다. 기본 할당량은 추적 할당량일 수 있습니다.

할당량은 컨텍스트에 따라 빈 문자열("") 또는 별표(*)로 표시됩니다.

- 'volume quota policy rule create' 명령을 사용하여 할당량을 생성할 때 '-target' 매개 변수를 빈 문자열("")로 설정하면 기본 할당량이 생성됩니다.

  에 대한 자세한 내용은 `volume quota policy rule create` "ONTAP 명령 참조입니다"을 참조하십시오.

- 'volume quota policy rule create' 명령에서 '-qtree' 매개 변수는 할당량 규칙이 적용되는 qtree의 이름을 지정합니다. 트리 유형 규칙에는 이 매개 변수를 사용할 수 없습니다. 볼륨 레벨의 사용자 또는 그룹 유형 규칙의 경우 이 매개 변수에 ""가 포함되어야 합니다.
- 'volume quota policy rule show' 명령의 출력에서 기본 할당량이 빈 문자열("")과 함께 타겟으로 표시됩니다.

  에 대한 자세한 내용은 `volume quota policy rule show` "ONTAP 명령 참조입니다"을 참조하십시오.

- 'volume quota report' 명령의 출력에서 기본 할당량은 ID 및 할당량 지정자로 별표(*)와 함께 표시됩니다.

  에 대한 자세한 내용은 `volume quota report` "ONTAP 명령 참조입니다"을 참조하십시오.

기본 사용자 할당량의 예

다음 할당량 규칙은 기본 사용자 할당량을 사용하여 vol1의 각 사용자에 50MB 제한을 적용합니다.

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                Soft             Soft
                         User          Disk     Disk    Files    Files
Type    Target    Qtree  Mapping      Limit    Limit    Limit    Limit
Threshold
-----  --------  -------  -------  --------  -------  ------  -------
---------
user    ""        ""       off          50MB        -       -        -
-
```

시스템의 사용자가 사용자의 데이터가 vol1에서 50MB 이상(예: 편집기에서 파일에 쓰기)을 이용하도록 하는 명령을 입력하면 명령이 실패합니다.

명시적 할당량을 사용하여 특정 할당량 타겟의 할당량을 지정하거나 특정 타겟의 기본 할당량을 재정의할 수 있습니다.

명시적 할당량은 특정 사용자, 그룹 또는 qtree에 대한 제한을 지정합니다. 명시적 할당량은 동일한 타겟에 대해 설정된 기본 할당량을 대체합니다.

파생된 사용자 할당량이 있는 사용자에 대해 명시적 사용자 할당량을 추가할 때는 기본 사용자 할당량으로 동일한 사용자 매핑 설정을 사용해야 합니다. 그렇지 않으면 할당량의 크기를 조정할 때 명시적 사용자 할당량이 새 할당량으로 간주되므로 거부됩니다.

명시적 할당량은 동일한 레벨(볼륨 또는 qtree)의 기본 할당량에만 영향을 줍니다. 예를 들어, qtree에 대한 명시적 사용자 할당량은 해당 qtree가 포함된 볼륨의 기본 사용자 할당량에 영향을 주지 않습니다. 그러나 qtree에 대한 명시적 사용자 할당량이 해당 qtree에 대한 기본 사용자 할당량보다 우선합니다(에 정의된 제한 대체).

명시적 할당량의 예

다음 할당량 규칙은 vol1의 모든 사용자를 50MB의 공간으로 제한하는 기본 사용자 할당량을 정의합니다. 그러나 명시적 할당량(굵은 글씨로 표시) 때문에 jsmith 사용자 한 명은 80MB의 공간이 허용됩니다.

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith" -qtree "" -disk-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                Soft             Soft
                          User          Disk     Disk   Files    Files
Type   Target    Qtree   Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off           50MB        -       -        -
-
user   jsmith    ""      off           80MB        -       -        -
-
```

다음 할당량 규칙은 4개의 ID로 표시되는 지정된 사용자를 vol1 볼륨에서 550MB의 디스크 공간과 10,000개의 파일로 제한합니다.

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "
jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544" -qtree "" -disk
-limit 550m -file-limit 10000

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   "jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544"
                 ""      off         550MB        -   10000        -
-
```

다음 할당량 규칙은 ENG1 그룹을 150MB의 디스크 공간과 proj1 qtree에 있는 파일 개수에 제한이 없습니다.

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type group -target "eng1" -qtree "proj1" -disk-limit
150m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol2

Vserver: vs0               Policy: default           Volume: vol2
                                                Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
group  eng1      proj1   off         150MB        -       -        -
-
```

다음 할당량 규칙은 vol2 볼륨의 proj1 qtree를 750MB의 디스크 공간과 75,000개의 파일로 제한합니다.

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type tree -target "proj1" -disk-limit 750m -file
-limit 75000

cluster1::> volume quota policy rule show -vserver vs0 -volume vol2

Vserver: vs0               Policy: default           Volume: vol2
                                                  Soft             Soft
                          User          Disk      Disk    Files    Files
Type    Target    Qtree   Mapping      Limit     Limit    Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree    proj1     ""      -           750MB        -    75000        -
-
```

파생 할당량의 작동 방식

명시적 할당량(특정 대상을 가진 할당량)이 아닌 기본 할당량의 결과로 적용되는 할당량을 _ 파생 할당량 _ 이라고 합니다.

파생된 할당량의 수와 위치는 할당량 유형에 따라 다릅니다.

- 볼륨의 기본 트리 할당량은 볼륨의 모든 qtree에 대해 파생된 기본 트리 할당량을 생성합니다.
- 기본 사용자 또는 그룹 할당량은 동일한 레벨(볼륨 또는 qtree)의 파일을 소유한 모든 사용자 또는 그룹에 대해 파생된 사용자 또는 그룹 할당량을 생성합니다.
- 볼륨의 기본 사용자 또는 그룹 할당량은 트리 할당량도 있는 모든 qtree에 대해 파생된 기본 사용자 또는 그룹 할당량을 생성합니다.

파생 할당량의 제한 및 사용자 매핑 포함 설정은 해당 기본 할당량의 설정과 동일합니다. 예를 들어, 볼륨에 20GB 디스크 제한이 있는 기본 트리 할당량은 볼륨의 qtree에서 20GB의 디스크 제한으로 유도된 트리 할당량을 생성합니다. 기본 할당량이 할당량 추적(제한 없음)인 경우 파생 할당량도 할당량을 추적합니다.

파생된 할당량을 보려면 할당량 보고서를 생성할 수 있습니다. 보고서에서 파생된 사용자 또는 그룹 할당량은 비어 있거나 별표(*)인 할당량 지정자로 표시됩니다. 그러나 파생된 트리 할당량에는 할당량 지정자가 있습니다. 파생된 트리 할당량을 식별하려면 볼륨에서 동일한 제한을 가진 기본 트리 할당량을 찾아야 합니다.

명시적 할당량은 다음과 같은 방식으로 파생 할당량과 상호 작용합니다.

- 동일한 타겟에 대해 명시적 할당량이 이미 있는 경우에는 파생 할당량이 생성되지 않습니다.
- 대상에 대한 명시적 할당량을 생성할 때 파생 할당량이 있는 경우 전체 할당량 초기화를 수행하지 않고 크기를 조정하여 명시적 할당량을 활성화할 수 있습니다.

추적 할당량을 사용합니다

추적 할당량은 디스크 및 파일 사용량 보고서를 생성하며 리소스 사용량을 제한하지 않습니다.

할당량을 추적할 때 할당량 값을 수정한 경우 할당량 값을 껐다가 다시 켜는 대신 할당량 크기를 조정할 수 있으므로 작업 중단이 덜 발생합니다.

추적 할당량을 생성하려면 디스크 제한 및 파일 제한 매개 변수를 생략합니다. 이를 통해 ONTAP은 아무런 제한 없이 해당 레벨(볼륨 또는 qtree)에서 타겟의 디스크 및 파일 사용량을 모니터링할 수 있습니다. 추적 할당량은 의 출력에 표시됩니다 `show` 모든 제한에 대해 대시("-")가 있는 명령 및 할당량 보고서 ONTAP에서는 System Manager UI를 사용하여 명시적 할당량(특정 타겟을 가진 할당량)을 생성할 때 추적 할당량을 자동으로 생성합니다. CLI를 사용하는 경우 스토리지 관리자는 명시적 할당량 외에 추적 할당량을 생성합니다.

또한 대상의 모든 인스턴스에 적용되는 _default tracking quota_를 지정할 수도 있습니다. 기본 추적 할당량을 사용하면 할당량 유형의 모든 인스턴스(예: 모든 qtree 또는 모든 사용자)에 대한 사용량을 추적할 수 있습니다. 또한 할당량 변경 사항을 적용하려는 경우 다시 초기화하는 대신 크기 조정을 사용할 수 있습니다.

예

추적 규칙의 출력에는 볼륨 수준 추적 규칙에 대한 다음 예에 나와 있는 것처럼 qtree, 사용자 및 그룹에 대한 추적 할당량이 표시됩니다.

```
Vserver: vs0              Policy: default             Volume: fv1

                                        Soft          Soft
                        User    Disk    Disk   Files  Files
Type  Target   Qtree    Mapping Limit   Limit  Limit  Limit  Threshold
----- -------- ------- ------- ------ ------ ------ ------ ---------
tree  ""       ""      -       -      -      -      -      -
user  ""       ""      off     -      -      -      -      -
group ""       ""      -       -      -      -      -      -
```

할당량을 적용하는 방법

할당량이 적용되는 방식을 이해하면 할당량을 올바르게 구성하고 예상 한도를 설정할 수 있습니다.

할당량을 설정한 FlexVol 볼륨의 파일에 파일을 생성하거나 데이터를 쓰려고 할 때마다 작업이 진행되기 전에 할당량 제한이 확인됩니다. 작업이 디스크 제한이나 파일 제한을 초과하면 작업이 금지됩니다.

할당량 제한은 다음 순서로 확인됩니다.

1. 해당 qtree의 트리 할당량(파일이 qtree0에 생성 또는 기록되는 경우에는 이 검사가 적용되지 않음)
2. 볼륨의 파일을 소유하는 사용자의 사용자 할당량
3. 볼륨의 파일을 소유하는 그룹의 그룹 할당량입니다
4. qtree에 있는 파일을 소유한 사용자의 할당량(파일이 qtree0에 생성 또는 기록되는 경우에는 이 검사가 적합하지 않음)
5. Qtree에서 파일을 소유한 그룹의 그룹 할당량(파일이 qtree0에 생성 또는 기록되는 경우에는 이 검사가 적합하지 않음)

가장 작은 제한을 가진 할당량이 먼저 초과되는 할당량이 아닐 수도 있습니다. 예를 들어 볼륨 vol1의 사용자 할당량이 100GB인 경우 볼륨 vol1에 포함된 Q2의 사용자 할당량은 20GB이며, 해당 사용자가 이미 볼륨 vol1에 80GB 이상의

데이터를 기록한 경우 볼륨 제한에 먼저 도달할 수 있습니다(단, Q2가 아닌 경우).

관련 정보

- "루트 사용자에게 할당량을 적용하는 방법"
- "ID가 여러 개인 사용자에게 할당량을 적용하는 방법"

할당량 정책을 할당할 때 고려해야 할 사항입니다

할당량 정책은 SVM의 모든 FlexVol 볼륨에 대한 할당량 규칙을 그룹화한 것입니다. 할당량 정책을 할당할 때는 특정 고려 사항을 염두에 두어야 합니다.

- SVM에는 특정 시간에 하나의 할당량 정책이 할당됩니다. SVM이 생성되면 새 할당량 정책이 생성되어 SVM에 할당됩니다. SVM을 생성할 때 다른 이름을 지정하지 않는 한 이 기본 할당량 정책의 이름은 "default"로 지정됩니다.
- SVM에는 최대 5개의 할당량 정책이 있을 수 있습니다. SVM에 5개의 할당량 정책이 있으면 기존 할당량 정책을 삭제할 때까지 SVM에 대한 새 할당량 정책을 생성할 수 없습니다.
- 할당량 정책에 대한 할당량 규칙을 생성하거나 할당량 규칙을 변경해야 하는 경우 다음 방법 중 하나를 선택할 수 있습니다.
  - SVM에 할당된 할당량 정책을 사용 중인 경우 SVM에 할당량 정책을 할당할 필요가 없습니다.
  - 할당되지 않은 할당량 정책을 사용하여 SVM에 할당량 정책을 할당하는 경우 필요한 경우 되돌릴 수 있는 할당량 정책의 백업이 있어야 합니다.

    예를 들어, 할당된 할당량 정책의 복사본을 만들고 복사본을 변경하고 SVM에 복사본을 할당한 다음 원래 할당량 정책의 이름을 바꿀 수 있습니다.
- SVM에 할당되었더라도 할당량 정책의 이름을 바꿀 수 있습니다.

사용자 및 그룹에서 할당량이 작동하는 방식

사용자 및 그룹에서 할당량이 작동하는 방식에 대한 개요입니다

사용자 또는 그룹을 할당량의 타겟으로 지정할 수 있습니다. 할당량을 정의할 때 고려해야 할 몇 가지 구축 차이점이 있습니다.

알아야 할 몇 가지 차이점이 있습니다.

- 사용자 또는 그룹
- Unix 또는 Windows입니다
- 특수 사용자 및 그룹
- 여러 ID가 포함되어 있습니다

환경에 따라 사용자의 ID를 지정하는 방법도 다양합니다.

할당량에 대해 **UNIX** 사용자를 지정합니다

할당량에 대해 UNIX 사용자를 여러 가지 형식 중 하나로 지정할 수 있습니다.

할당량에 대해 UNIX 사용자를 지정할 때 사용할 수 있는 세 가지 형식은 다음과 같습니다.

- 사용자 이름(예: jsmith)

> UNIX 사용자 이름을 사용하여 해당 이름에 백슬래시(\) 또는 @ 기호가 포함된 경우 할당량을 지정할 수 없습니다. ONTAP에서는 이러한 문자를 포함하는 이름을 Windows 이름으로 취급하기 때문입니다.

- 사용자 ID 또는 UID(예: 20)
- 파일의 UID가 사용자와 일치하도록 해당 사용자가 소유한 파일 또는 디렉토리의 경로입니다.

> 파일 또는 디렉토리 이름을 지정하는 경우 사용자 계정이 시스템에 남아 있는 한, 사용할 파일 또는 디렉토리를 선택해야 합니다.
>
> UID에 대한 파일 또는 디렉토리 이름을 지정해도 ONTAP에서 해당 파일 또는 디렉토리에 할당량을 적용하지는 않습니다.

할당량에 대한 **Windows** 사용자를 지정합니다

할당량에 대한 Windows 사용자를 여러 가지 형식 중 하나로 지정할 수 있습니다.

할당량에 대해 Windows 사용자를 지정할 때 사용할 수 있는 세 가지 형식은 다음과 같습니다.

- Windows 2000 이전 형식의 Windows 이름입니다.
- Windows에서 텍스트 형식으로 표시되는 SID(보안 ID) `S-1-5-32-544`입니다(예:).
- 해당 사용자의 SID가 소유한 ACL이 있는 파일 또는 디렉토리의 이름입니다.

> 파일 또는 디렉토리 이름을 지정하는 경우 사용자 계정이 시스템에 남아 있는 한, 사용할 파일 또는 디렉토리를 선택해야 합니다.
>
> ONTAP가 ACL에서 SID를 가져오려면 ACL이 유효해야 합니다.
>
> 파일 또는 디렉토리가 UNIX 스타일 qtree에 있거나 스토리지 시스템에서 사용자 인증에 UNIX 모드를 사용하는 경우 ONTAP는 사용자 할당량을 파일 또는 디렉토리의 UID * 가 아닌 * UID * 에 해당하는 사용자에게 적용합니다.
>
> 할당량에 대한 사용자를 식별하기 위해 파일 또는 디렉토리 이름을 지정해도 ONTAP에서는 해당 파일 또는 디렉토리에 할당량을 적용하지 않습니다.

기본 사용자 및 그룹 할당량이 파생 할당량을 생성하는 방법

기본 사용자 또는 그룹 할당량을 생성하면 동일한 레벨의 파일을 소유한 모든 사용자 또는 그룹에 대해 해당 파생 사용자 또는 그룹 할당량이 자동으로 생성됩니다.

파생된 사용자 및 그룹 할당량은 다음과 같은 방식으로 생성됩니다.

- FlexVol 볼륨의 기본 사용자 할당량은 볼륨의 어느 곳에서든 파일을 소유하는 모든 사용자에 대해 파생된 사용자 할당량을 생성합니다.
- qtree의 기본 사용자 할당량은 qtree의 파일을 소유한 모든 사용자에 대해 파생 사용자 할당량을 생성합니다.

- FlexVol 볼륨의 기본 그룹 할당량은 볼륨의 어느 곳에서든 파일을 소유하는 모든 그룹에 대해 파생된 그룹 할당량을 생성합니다.
- qtree의 기본 그룹 할당량은 qtree에 있는 파일을 소유한 모든 그룹에 대해 파생 그룹 할당량을 생성합니다.

사용자 또는 그룹이 기본 사용자 또는 그룹 할당량 수준의 파일을 소유하지 않으면 사용자 또는 그룹에 대해 파생 할당량이 생성되지 않습니다. 예를 들어, qtree proj1에 대해 기본 사용자 할당량이 생성되고 사용자 jsmith가 다른 qtree에 있는 파일을 소유하는 경우 jsmith에 대해 파생된 사용자 할당량이 생성되지 않습니다.

파생 할당량은 제한 및 사용자 매핑을 포함하여 기본 할당량과 동일한 설정을 가집니다. 예를 들어 기본 사용자 할당량에 50MB 디스크 제한이 있고 사용자 매핑이 설정되어 있는 경우 결과 파생 할당량에도 50MB 디스크 제한이 있고 사용자 매핑이 설정되어 있습니다.

그러나 세 가지 특수 사용자 및 그룹에 대한 파생 할당량에는 제한이 없습니다. 다음 사용자 및 그룹이 기본 사용자 또는 그룹 할당량 수준에서 파일을 소유하는 경우 기본 사용자 또는 그룹 할당량과 동일한 사용자 매핑 설정을 사용하여 파생 할당량이 생성되지만 할당량 추적만 가능합니다(제한 없음).

- Unix 루트 사용자(UID 0)
- UNIX 루트 그룹(GID 0)
- Windows BUILTIN\Administrators 그룹입니다

  Windows 그룹의 할당량은 사용자 할당량으로 추적되므로 이 그룹의 파생 할당량은 기본 그룹 할당량이 아닌 기본 사용자 할당량에서 파생된 사용자 할당량입니다.

파생된 사용자 할당량의 예

루트, jsmith, bob-own 파일 등 세 명의 사용자가 있는 볼륨이 있고 볼륨에 기본 사용자 할당량을 생성하면 ONTAP는 자동으로 세 개의 파생 사용자 할당량을 생성합니다. 따라서 볼륨에 대해 할당량을 다시 초기화하면 할당량 보고서에 네 개의 새 할당량이 나타납니다.

```
cluster1::> volume quota report
  Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *          0B   50MB       0       -   *
vol1               user    root       5B      -       1       -
vol1               user    jsmith    30B   50MB      10       -   *
vol1               user    bob       40B   50MB      15       -   *
4 entries were displayed.
```

첫 번째 새 줄은 사용자가 생성한 기본 사용자 할당량이며, 이 할당량은 별표(*)를 ID로 식별할 수 있습니다. 다른 새로운 행은 파생된 사용자 할당량입니다. jsmith 및 bob의 파생 할당량은 기본 할당량과 50MB 디스크 제한이 동일합니다. 루트 사용자의 파생 할당량은 제한 없는 추적 할당량입니다.

루트 사용자에게 할당량을 적용하는 방법

UNIX 클라이언트의 루트 사용자(UID=0)에는 트리 할당량이 적용되지만 사용자 또는 그룹 할당량은 적용되지 않습니다. 이렇게 하면 루트 사용자가 할당량에 의해 차단되는 다른 사용자를 대신하여 작업을 수행할 수 있습니다.

루트 사용자가 `chown` Privileges가 적은 사용자를 대신하여 파일 또는 디렉토리 소유권 변경 또는 기타 작업(예: UNIX 명령)을 수행하는 경우 ONTAP는 새 소유자를 기준으로 할당량을 확인하지만 새 소유자의 하드 할당량 제한을 초과하더라도 오류를 보고하거나 작업을 중지하지 않습니다. 이는 손실된 데이터 복구와 같은 관리 작업으로 인해 할당량이 일시적으로 초과되는 경우에 유용할 수 있습니다.

그러나 소유권 전송이 수행된 후, 할당량이 여전히 초과되는 동안 사용자가 디스크 공간을 더 할당하려고 하면 클라이언트 시스템에서 디스크 공간 오류를 보고합니다.

관련 정보

- "할당량을 적용하는 방법"
- "ID가 여러 개인 사용자에게 할당량을 적용하는 방법"

특수 **Windows** 그룹에서 할당량을 사용하는 방법

다른 Windows 그룹과 다르게 할당량을 처리하는 몇 가지 특수 Windows 그룹이 있습니다. 이러한 특수 그룹에 할당량이 적용되는 방식을 이해해야 합니다.

ONTAP는 Windows 그룹 ID 기반의 그룹 할당량을 지원하지 않습니다. Windows 그룹 ID를 할당량 타겟으로 지정하면 할당량이 사용자 할당량으로 간주됩니다.

모두

할당량 대상이 Everyone 그룹이면 소유자가 Everyone으로 표시된 ACL이 있는 파일이 Everyone의 SID 아래에 계산됩니다.

BUILTIN\Administrators입니다

할당량 대상이 BUILTIN\Administrators 그룹인 경우 이 항목은 사용자 할당량으로 간주되며 추적에만 사용됩니다. BUILTIN\Administrators에는 제한을 적용할 수 없습니다. BUILTIN\Administrators의 구성원이 파일을 만들면 해당 파일은 BUILTIN\Administrators가 소유하며 사용자의 개인 SID가 아닌 BUILTIN\Administrators에 대한 SID로 계산됩니다.

ID가 여러 개인 사용자에게 할당량을 적용하는 방법

사용자는 여러 ID로 나타낼 수 있습니다. ID 목록을 할당량 대상으로 지정하여 이러한 사용자에 대한 단일 사용자 할당량을 정의할 수 있습니다. 이러한 ID가 소유한 파일은 사용자 할당량의 제한을 받습니다.

사용자에게 UNIX UID `20`와 `Windows ID` 및 가 있다고 `corp\john_smith engineering\jsmith` 가정합니다. 이 사용자의 경우 할당량 대상이 UID 및 Windows ID의 목록인 할당량을 지정할 수 있습니다. 이 사용자가 스토리지 시스템에 쓸 때 쓰기가 UID에서 시작되었는지 `20`, `corp\john_smith` 또는 에서 시작되었는지에 관계없이 지정된 할당량이 `engineering\jsmith` 적용됩니다.

ID가 동일한 사용자에 속하더라도 별도의 할당량 규칙은 별도의 타겟으로 간주됩니다. 예를 들어, 동일한 사용자의 경우

UID를 20 1GB의 디스크 공간으로 제한하는 할당량 하나와 corp\John_Smith의 디스크 공간을 2GB로 제한하는 할당량 하나를 지정할 수 있습니다. 두 ID가 모두 동일한 사용자를 나타내더라도 마찬가지입니다. ONTAP에서는 UID에 할당량이 20 `corp\john_smith` 별도로 적용됩니다. 이 경우 `engineering\jsmith` 동일한 사용자가 사용하는 다른 ID에 제한이 적용되더라도 에는 제한이 적용되지 않습니다.

관련 정보

- "할당량을 적용하는 방법"
- "루트 사용자에게 할당량을 적용하는 방법"

ONTAP에서 혼합 환경의 사용자 **ID**를 확인하는 방법

사용자가 Windows 및 UNIX 클라이언트 모두에서 ONTAP 스토리지에 액세스하는 경우 Windows 및 UNIX 보안을 모두 사용하여 파일 소유권을 확인합니다. 사용자 할당량을 적용할 때 ONTAP에서 UNIX 또는 Windows ID를 사용할지 여부를 결정하는 요인은 여러 가지입니다.

파일이 들어 있는 qtree 또는 FlexVol 볼륨의 보안 스타일이 NTFS이거나 UNIX에만 해당하는 경우에는 사용자 할당량을 적용할 때 사용되는 ID의 유형이 보안 스타일에 따라 결정됩니다. 혼합 보안 스타일을 사용하는 qtree의 경우 사용된 ID의 유형은 파일에 ACL이 있는지 여부에 따라 결정됩니다.

다음 표에는 사용되는 ID 유형이 요약되어 있습니다.

보안 스타일	**ACL**	**ACL** 없음
Unix	Unix ID입니다	Unix ID입니다
혼합	Windows ID입니다	Unix ID입니다
NTFS입니다	Windows ID입니다	Windows ID입니다

여러 사용자에게 할당량이 작동하는 방식

동일한 할당량 대상에 여러 사용자를 배치하면 할당량으로 정의된 제한이 각 개별 사용자에게 적용되지 않습니다. 할당량 제한값은 할당량 대상의 모든 사용자 간에 공유됩니다.

볼륨 및 Qtree와 같은 객체 관리를 위한 명령과 달리, 다중 사용자 할당량을 비롯한 할당량 타겟의 이름을 바꿀 수 없습니다. 즉, 다중 사용자 할당량이 정의된 후에는 할당량 타겟의 사용자를 수정할 수 없으며 대상에 사용자를 추가하거나 대상에서 사용자를 제거할 수 없습니다. 다중 사용자 할당량에서 사용자를 추가하거나 제거하려면 해당 사용자를 포함하는 할당량과 정의된 타겟의 사용자 집합을 포함하는 새 할당량 규칙을 삭제해야 합니다.

> 개별 사용자 할당량을 하나의 다중 사용자 할당량으로 결합하는 경우 할당량의 크기를 조정하여 변경을 활성화할 수 있습니다. 그러나 사용자가 여러 명인 할당량 대상에서 사용자를 제거하거나 사용자가 이미 여러 명인 대상에 사용자를 추가하려면 변경 사항이 적용되기 전에 할당량을 다시 초기화해야 합니다.

할당량 규칙에 둘 이상의 사용자가 있는 예

다음 예에서는 할당량 항목에 두 명의 사용자가 나열되어 있습니다. 두 사용자는 최대 80MB의 공간을 사용할 수 있습니다. 75MB를 사용할 경우 다른 하나는 5MB만 사용할 수 있습니다.

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith,chen" -qtree "" -disk
-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                    Soft             Soft
                              User          Disk     Disk    Files    Files
Type    Target         Qtree  Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------       ------- -------  --------  -------  ------  -------
---------
user    "jsmith,chen"  ""      off           80MB        -       -        -
-
```

할당량에 대한 **UNIX** 및 **Windows** 이름 링크

혼합 환경에서는 Windows 사용자 또는 UNIX 사용자로 로그인할 수 있습니다. 사용자 UNIX ID와 Windows ID가 동일한 사용자를 나타내도록 할당량을 구성할 수 있습니다.

Windows 사용자 이름에 대한 할당량은 다음 두 조건이 모두 충족되면 UNIX 사용자 이름으로 매핑되거나 그 반대로 매핑됩니다.

- 사용자 할당 규칙에서 사용자 매핑 매개변수가 "ON"으로 설정됩니다.
- 사용자 이름은 'vserver name-mapping' 명령으로 매핑되었습니다.

UNIX와 Windows 이름이 함께 매핑되면 할당량 사용을 결정하는 동일한 사람으로 간주됩니다.

트리 할당량의 작동 방식

트리 할당량의 작동 방식에 대한 개요

타겟 qtree의 크기가 될 수 있는 범위를 제한하기 위해 qtree를 타겟으로 사용하여 할당량을 생성할 수 있습니다. 이러한 할당량을 _tree quotas_라고도 합니다.

특정 qtree에 대해 사용자 및 그룹 할당량을 생성할 수도 있습니다. 또한 FlexVol 볼륨의 할당량은 해당 볼륨에 포함된 qtree에 의해 상속되는 경우도 있습니다.

qtree에 할당량을 적용하면 디스크 파티션과 비슷한 결과가 발생합니다. 단, 할당량을 변경하여 언제든지 qtree의 최대 크기를 변경할 수 있다는 점이 다릅니다. 트리 할당량을 적용할 때 ONTAP은 소유자의 종류에 관계없이 qtree의 파일 수와 디스크 공간을 제한합니다. 루트 및 BUILTIN\Administrators 그룹의 구성원을 포함하여 어떤 사용자도 쓰기 작업으로 인해 트리 할당량이 초과되는 경우 qtree에 쓸 수 없습니다.

할당량의 크기는 사용 가능한 공간의 특정 양을 보장하지 않습니다. 할당량의 크기는 qtree에 사용할 수 있는 사용 가능한 공간보다 클 수 있습니다. 'volume quota report' 명령을 사용하여 qtree의 사용 가능한 실제 공간을 확인할 수 있습니다.

에 대한 자세한 내용은 `volume quota report` "ONTAP 명령 참조입니다"을 참조하십시오.

사용자 및 그룹 할당량이 **Qtree**에서 작동하는 방식

트리 할당량은 qtree의 전체 크기를 제한합니다. 개별 사용자 또는 그룹이 전체 qtree를 사용하지 않도록 하려면 해당 qtree에 대한 사용자 또는 그룹 할당량을 지정합니다.

qtree의 사용자 할당량 예시

다음과 같은 할당량 규칙이 있다고 가정합니다.

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                Soft             Soft
                         User          Disk     Disk   Files    Files
Type    Target    Qtree  Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user    ""        ""     off           50MB        -       -        -
45MB
user    jsmith    ""     off           80MB        -       -        -
75MB
```

특정 사용자인 kjones가 vol1에 상주하는 중요한 qtree인 proj1에서 공간을 너무 많이 차지하고 있음을 알 수 있습니다. 다음 할당량 규칙을 추가하여 이 사용자의 공간을 제한할 수 있습니다.

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "kjones" -qtree "proj1" -disk
-limit 20m -threshold 15m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                  Soft             Soft
                         User         Disk       Disk    Files    Files
Type    Target    Qtree  Mapping      Limit      Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user    ""        ""     off           50MB        -       -        -
45MB
user    jsmith    ""     off           80MB        -       -        -
75MB
user    kjones    proj1  off           20MB        -       -        -
15MB
```

FlexVol 볼륨의 기본 트리 할당량이 파생 트리 할당량을 생성하는 방법

FlexVol 볼륨에 기본 트리 할당량을 생성하면 해당 볼륨의 모든 qtree에 대해 해당 파생 트리 할당량이 자동으로 생성됩니다.

이러한 파생 트리 할당량은 기본 트리 할당량과 동일한 제한을 가집니다. 추가 할당량이 없는 경우 제한 사항은 다음과 같은 영향을 줍니다.

- 사용자는 전체 볼륨에 할당된 qtree의 공간을 사용할 수 있습니다(루트 또는 다른 qtree의 공간을 사용하여 볼륨 제한을 초과하지 않은 경우).
- 각 qtree는 전체 볼륨을 사용하도록 증가할 수 있습니다.

볼륨에 기본 트리 할당량이 있어도 볼륨에 추가된 모든 새 qtree에 계속 영향을 미칩니다. 새 qtree가 생성될 때마다 파생 트리 할당량도 생성됩니다.

모든 파생 할당량과 마찬가지로 파생된 트리 할당량에는 다음과 같은 동작이 표시됩니다.

- 타겟에 명시적 할당량이 없는 경우에만 생성됩니다.
- 할당량 보고서에는 표시되지만 명령을 사용하여 할당량 규칙을 표시할 때는 나타나지 않습니다 `volume quota policy rule show`. 에 대한 자세한 내용은 `volume quota policy rule show` "ONTAP 명령 참조입니다"을 참조하십시오.

파생된 트리 할당량의 예

qtree 3개(proj1, proj2, proj3)의 볼륨이 있고 디스크 크기를 10GB로 제한하는 proj1 qtree의 명시적 할당량만 트리 할당량입니다. 볼륨에 기본 트리 할당량을 생성하고 볼륨에서 할당량을 다시 초기화하면 할당량 보고서에 네 개의 트리 할당량이 포함됩니다.

```
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     proj1     tree    1           0B   10GB       1       -   proj1
vol1               tree    *           0B   20GB       0       -   *
vol1     proj2     tree    2           0B   20GB       1       -   proj2
vol1     proj3     tree    3           0B   20GB       1       -   proj3
...
```

첫 번째 줄에는 proj1 qtree의 원래 명시적 할당량이 표시됩니다. 이 할당량은 변경되지 않습니다.

두 번째 줄에는 볼륨의 새 기본 트리 할당량이 표시됩니다. 별표(*) 할당량 지정자는 기본 할당량임을 나타냅니다. 이 할당량은 사용자가 생성한 할당량 규칙의 결과입니다.

마지막 두 줄에는 proj2 및 proj3 qtree에 대한 새로운 파생 트리 할당량이 표시됩니다. ONTAP는 볼륨에 대한 기본 트리 할당량의 결과로 이러한 할당량을 자동으로 생성했습니다. 이러한 파생된 트리 할당량은 볼륨의 기본 트리 할당량과 20GB 디스크 제한이 동일합니다. proj1 qtree에 명시적 할당량이 이미 있으므로 ONTAP에서는 proj1 qtree에 대해 파생 트리 할당량을 생성하지 않았습니다.

FlexVol 볼륨의 기본 사용자 할당량이 해당 볼륨의 **qtree**에 대한 할당량에 미치는 영향

기본 사용자 할당량이 FlexVol 볼륨에 대해 정의된 경우 명시적 또는 파생 트리 할당량이 있는 해당 볼륨에 포함된 모든 qtree에 대해 기본 사용자 할당량이 자동으로 생성됩니다.

qtree의 기본 사용자 할당량이 이미 있는 경우, 볼륨에 대한 기본 사용자 할당량이 생성될 때 영향을 받지 않습니다.

Qtree에서 자동으로 생성된 기본 사용자 할당량은 볼륨에 대해 생성한 기본 사용자 할당량과 동일한 제한이 있습니다.

qtree에 대한 명시적 사용자 할당량이 관리자가 생성한 qtree의 기본 사용자 할당량을 재정의하는 것과 동일한 방식으로 자동으로 생성된 기본 사용자 할당량을 재정의합니다.

Qtree 변경이 할당량에 미치는 영향

qtree의 보안 스타일을 삭제, 이름 바꾸기 또는 변경할 때 현재 적용된 할당량에 따라 ONTAP에서 적용하는 할당량이 변경될 수 있습니다.

Qtree 삭제 및 트리 할당량

qtree를 삭제할 경우 명시적 또는 파생된 qtree에 적용되는 모든 할당량이 ONTAP에서 더 이상 적용되지 않습니다.

할당량 규칙이 계속 유지되는지 여부는 qtree를 삭제하는 위치에 따라 달라집니다.

- ONTAP를 사용하여 qtree를 삭제하는 경우 트리 할당량 규칙과 해당 qtree에 대해 구성된 사용자 및 그룹 할당량 규칙을 포함하여 해당 qtree에 대한 할당량 규칙이 자동으로 삭제됩니다.
- CIFS 또는 NFS 클라이언트를 사용하여 qtree를 삭제하는 경우 할당량을 다시 초기화할 때 오류가 발생하지 않도록 해당 qtree에 대한 할당량 규칙을 삭제해야 합니다. 삭제한 qtree와 동일한 이름을 가진 새 qtree를 생성하는 경우,

할당량을 다시 초기화하기 전에는 기존 할당량 규칙이 새 qtree에 적용되지 않습니다.

Qtree 이름을 변경하면 할당량에 미치는 영향이 변경됩니다

ONTAP를 사용하여 qtree의 이름을 변경하면 해당 qtree의 할당량 규칙이 자동으로 업데이트됩니다. CIFS 또는 NFS 클라이언트를 사용하여 qtree의 이름을 바꾸는 경우 해당 qtree에 대한 할당량 규칙을 업데이트해야 합니다.

CIFS 또는 NFS 클라이언트를 사용하여 qtree의 이름을 변경하고 할당량을 다시 초기화하기 전에 해당 qtree의 할당량 규칙을 새 이름으로 업데이트하지 않으면 qtree에 할당량이 적용되지 않습니다. 트리 할당량, qtree의 사용자 또는 그룹 할당량을 비롯한 qtree의 명시적 할당량이 파생 할당량으로 변환될 수 있습니다.

Qtree 보안 스타일 및 사용자 할당량

NTFS 또는 혼합 보안 스타일을 사용하여 qtree에 ACL(액세스 제어 목록)을 적용할 수 있지만 UNIX 보안 스타일을 사용하지는 않습니다. qtree의 보안 스타일을 변경하면 할당량 계산 방식에 영향을 미칠 수 있습니다. Qtree의 보안 스타일을 변경한 후에는 항상 할당량을 다시 초기화해야 합니다.

qtree의 보안 스타일을 NTFS 또는 MIXED에서 UNIX로 변경하면 해당 qtree의 파일에 대한 모든 ACL이 무시되고 UNIX 사용자 ID에 대해 파일 사용량이 청구됩니다.

Qtree의 보안 스타일을 UNIX에서 혼합 또는 NTFS로 변경하면 이전에 숨겨진 ACL이 표시됩니다. 또한 무시된 모든 ACL이 다시 유효해지고 NFS 사용자 정보가 무시됩니다. 이전에 ACL이 없는 경우 할당량 계산에 NFS 정보가 계속 사용됩니다.

qtree의 보안 스타일을 변경한 후 UNIX 사용자와 Windows 사용자 모두의 할당량 사용이 올바르게 계산되도록 하려면 해당 qtree가 포함된 볼륨의 할당량을 다시 초기화해야 합니다.

예

다음 예에서는 qtree의 보안 유형이 변경되어 다른 사용자가 특정 qtree의 파일 사용에 대해 청구되는 방법을 보여줍니다.

NTFS 보안이 qtree A에 적용되고 ACL이 Windows 사용자에게 `corp\joe` 5MB 파일의 소유권을 제공한다고 가정합니다. 사용자에게 `corp\joe` qtree A에 대해 5MB의 디스크 공간 사용이 청구됩니다

이제 qtree A의 보안 스타일을 NTFS에서 UNIX로 변경합니다. 할당량이 재초기화되면 Windows 사용자에게 `corp\joe` 이 파일에 대한 비용이 청구되지 않고, 대신 파일의 UID에 해당하는 UNIX 사용자에게 해당 파일에 대한 비용이 청구됩니다. UID는 `corp\joe` 또는 루트 사용자에 매핑된 UNIX 사용자일 수 있습니다.

할당량이 활성화되는 방식

할당량 활성화 방법에 대한 개요입니다

새 할당량 및 기존 할당량에 대한 변경 사항을 활성화해야 효과를 적용할 수 있습니다. 활성화는 볼륨 레벨에서 수행됩니다. 할당량 활성화의 작동 방식을 알면 업무 중단을 최소화하면서 할당량을 관리하는 데 도움이 됩니다.

할당량은 *initializing*(설정 중) 또는 _refizing_에 의해 활성화됩니다. 할당량을 해제했다가 다시 설정하는 것을 다시 초기화 중이라고 합니다.

활성화 프로세스의 길이와 할당량 적용에 미치는 영향은 활성화 유형에 따라 달라집니다.

- 초기화 프로세스에는 두 가지 부분, 즉 "할당량" 작업과 볼륨의 전체 파일 시스템에 대한 할당량 검사가 포함됩니다. 할당량 설정 작업이 성공적으로 완료된 후 검사가 시작됩니다. 할당량 검사에는 시간이 걸릴 수 있습니다. 볼륨에 파일이 많을수록 더 오래 걸립니다. 검사가 완료될 때까지 할당량 활성화가 완료되지 않으며 할당량이 적용되지 않습니다.
- 크기 조정 프로세스에는 만 포함됩니다 `quota resize` 작업. 크기 조정에는 할당량 검사가 필요하지 않으므로 할당량 초기화보다 시간이 적게 걸립니다. 크기 조정 프로세스 중에 할당량이 계속 적용됩니다.

기본적으로 "할당량 설정" 및 "할당량 크기 조정" 작업은 백그라운드에서 실행되므로 다른 명령을 동시에 사용할 수 있습니다.

활성화 프로세스의 오류 및 경고가 이벤트 관리 시스템으로 전송됩니다. 볼륨 할당량 설정 또는 볼륨 할당량 크기 조정 명령과 함께 '-foreground' 매개 변수를 사용하면 작업이 완료될 때까지 명령이 반환되지 않으므로 스크립트에서 다시 초기화하는 경우에 유용합니다. 나중에 오류와 경고를 표시하려면 '-instance' 매개 변수와 함께 'volume quota show' 명령을 사용할 수 있습니다.

할당량 활성화는 중지 및 재부팅 후에도 유지됩니다. 할당량 활성화 프로세스는 스토리지 시스템 데이터의 가용성에 영향을 주지 않습니다.

관련 정보

- "볼륨 할당량이 켜져 있습니다"
- "볼륨 할당량 크기 조정"
- "볼륨 할당량이 표시됩니다"

크기 조정 사용 시기 이해

할당량 크기 조정은 유용한 ONTAP 기능입니다. 또한 크기 조정이 할당량 초기화보다 빠르므로 가능한 경우 크기 조정을 사용해야 합니다. 그러나 몇 가지 제한 사항을 알아야 합니다.

크기 조정은 특정 유형의 할당량 변경에만 적용됩니다. 할당량 규칙을 다음과 같이 변경할 때 할당량 크기를 조정할 수 있습니다.

- 기존 할당량 변경.

  예를 들어, 기존 할당량의 제한을 변경합니다.

- 기본 할당량 또는 기본 추적 할당량이 있는 할당량 타겟에 대한 할당량 추가
- 기본 할당량 또는 기본 추적 할당량 항목이 지정된 할당량을 삭제합니다.
- 개별 사용자 할당량을 하나의 다중 사용자 할당량으로 결합합니다.

> 할당량을 광범위하게 변경한 후에는 전체 재초기화를 수행하여 모든 변경 사항이 적용되도록 해야 합니다.

> 크기 조정 작업을 사용하여 모든 할당량 변경 사항을 통합할 수 없는 경우 ONTAP에서 경고를 표시합니다. 할당량 보고서를 통해 스토리지 시스템이 특정 사용자, 그룹 또는 qtree의 디스크 사용량을 추적하는지 확인할 수 있습니다. 할당량 보고서에 할당량이 표시되는 경우, 이는 스토리지 시스템이 디스크 공간과 할당량 대상이 소유한 파일 수를 추적하고 있음을 의미합니다.

할당량 변경 예제 크기를 조정하여 효과적으로 변경할 수 있습니다

일부 할당량 규칙 변경은 크기 조정을 통해 적용할 수 있습니다. 다음 할당량을 고려해 보십시오.

```
#Quota Target type             disk  files thold sdisk sfile
#------------ ----              ----  ----- ----- ----- -----
*             user@/vol/vol2    50M   15K
*             group@/vol/vol2  750M   85K
*             tree@/vol/vol2     -     -
jdoe          user@/vol/vol2/  100M   75K
kbuck         user@/vol/vol2/  100M   75K
```

다음과 같이 변경한다고 가정합니다.

- 기본 사용자 대상의 파일 수를 늘립니다.
- 기본 사용자 할당량보다 더 많은 디스크 제한이 필요한 새 사용자 할당량인 Boris를 추가합니다.
- kbuck 사용자의 명시적 할당량 항목을 삭제합니다. 이제 새 사용자는 기본 할당량 제한만 필요합니다.

이러한 변경 사항으로 인해 다음과 같은 할당량이 발생합니다.

```
#Quota Target type             disk  files thold sdisk sfile
#------------ ----              ----  ----- ----- ----- -----
*             user@/vol/vol2    50M   25K
*             group@/vol/vol2  750M   85K
*             tree@/vol/vol2     -     -
jdoe          user@/vol/vol2/  100M   75K
boris         user@/vol/vol2/  100M   75K
```

크기를 조정하면 이러한 모든 변경 사항이 활성화되지만 전체 할당량을 다시 초기화할 필요는 없습니다.

전체 할당량 재초기화가 필요한 경우

할당량의 크기를 조정하는 것이 더 빠르기는 하지만, 할당량에 대한 소규모의 변경 또는 광범위한 변경 작업을 수행하는 경우에는 전체 할당량을 다시 초기화해야 합니다.

다음과 같은 상황에서는 전체 할당량 재초기화가 필요합니다.

- 이전에 할당량이 없는 대상에 대해 할당량을 생성합니다(명시적 할당량이나 기본 할당량에서 파생된 할당량도 아님).
- Qtree의 보안 스타일을 UNIX에서 혼합 또는 NTFS로 변경합니다.
- Qtree의 보안 스타일을 혼합 또는 NTFS에서 UNIX로 변경할 수 있습니다.
- 사용자가 여러 명인 할당량 대상에서 사용자를 제거하거나 사용자가 이미 여러 명인 대상에 사용자를 추가합니다.
- 할당량을 광범위하게 변경합니다.

초기화가 필요한 할당량 변경 사항의 예

볼륨에 3개의 Qtree가 포함된 볼륨이 있고 볼륨의 유일한 할당량이 3개의 명시적 트리 할당량이라고 가정합니다. 다음 사항을 변경하기로 결정합니다.

- 새 qtree를 추가하고 새 트리 할당량을 생성합니다.
- 볼륨에 대한 기본 사용자 할당량을 추가합니다.

이러한 변경 사항 모두 전체 할당량 초기화가 필요합니다. 크기를 조정해도 할당량은 적용되지 않습니다.

할당량 정보를 보는 방법

할당량 정보 보기 개요

할당량 보고서를 사용하여 할당량 규칙 및 정책 구성, 적용 및 구성된 할당량, 할당량 크기 조정 및 다시 초기화 중에 발생한 오류 등의 세부 정보를 볼 수 있습니다.

할당량 정보는 다음과 같은 상황에서 유용합니다.

- 할당량 구성. 예를 들어 할당량을 구성하고 구성을 확인합니다
- 디스크 공간 또는 파일 제한에 곧 도달하거나 도달했다는 알림에 응답합니다
- 더 많은 공간에 대한 요청에 응답합니다

할당량 보고서를 사용하여 어떤 할당량이 유효한지 확인합니다

할당량이 상호 작용하는 다양한 방법 때문에 명시적으로 생성한 할당량보다 더 많은 할당량이 적용됩니다. 사용 중인 할당량을 확인하려면 할당량 보고서를 보면 됩니다.

다음 예에서는 FlexVol 볼륨 vol1에 적용된 다양한 유형의 할당량과 해당 볼륨에 포함된 qtree Q1에 대한 할당량 보고서를 보여 줍니다.

qtree에 대해 지정된 사용자 할당량이 없는 예

이 예에서는 볼륨 vol1에 포함된 qtree 1Q1이 있습니다. 관리자가 할당량 3개를 생성했습니다.

- 400MB의 vol1에 대한 기본 트리 할당량 제한입니다
- 100MB의 vol1에 대한 기본 사용자 할당량 제한입니다
- 사용자 jsmith에 대한 vol1의 명시적 사용자 할당량 제한입니다

이러한 할당량에 대한 할당량 규칙은 다음 예제와 비슷합니다.

```
cluster1::*> volume quota policy rule show -vserver vs1 -volume vol1

Vserver: vs1               Policy: default           Volume: vol1
                                                 Soft             Soft
                          User          Disk     Disk   Files    Files
Type   Target    Qtree   Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree   ""        ""      -           400MB        -       -        -
-
user   ""        ""      off         100MB        -       -        -
-
user   jsmith    ""      off         200MB        -       -        -
-
```

이러한 할당량에 대한 할당량 보고서는 다음 예제와 유사합니다.

```
cluster1::> volume quota report
Vserver: vs1
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     -          tree   *           0B  400MB       0       -   *
vol1     -          user   *           0B  100MB       0       -   *
vol1     -          user   jsmith    150B  200MB       7       -   jsmith
vol1     q1         tree   1           0B  400MB       6       -   q1
vol1     q1         user   *           0B  100MB       0       -
vol1     q1         user   jsmith      0B  100MB       5       -
vol1     -          user   root        0B    0MB       1       -
vol1     q1         user   root        0B    0MB       8       -
```

할당량 보고서의 처음 세 줄에는 관리자가 지정한 세 개의 할당량이 표시됩니다. 이 할당량 중 두 개가 기본 할당량이므로 ONTAP는 자동으로 파생 할당량을 생성합니다.

네 번째 줄에는 vol1의 모든 qtree에 대한 기본 트리 할당량에서 파생된 트리 할당량이 표시됩니다(이 예에서는 Q1만 해당).

다섯 번째 줄에는 볼륨에 기본 사용자 할당량과 qtree 할당량이 있으므로 qtree에 대해 생성되는 기본 사용자 할당량이 표시됩니다.

6번째 줄에는 qtree(줄 5)에 대한 기본 사용자 할당량이 있고 사용자 jsmith가 해당 qtree에 파일을 소유하기 때문에 jsmith에 대해 생성된 파생 사용자 할당량이 표시됩니다. Qtree Q1 에서 사용자 jsmith에 적용되는 제한은 명시적

사용자 할당량 한도(200MB)에 의해 결정되지 않습니다. 이는 명시적 사용자 할당량 제한이 볼륨에 있기 때문에 qtree의 제한에는 영향을 미치지 않습니다. 대신 qtree의 파생된 사용자 할당량 제한은 qtree의 기본 사용자 할당량(100MB)에 의해 결정됩니다.

마지막 두 줄에는 볼륨 및 qtree의 기본 사용자 할당량에서 파생된 더 많은 사용자 할당량이 표시됩니다. 루트 사용자가 볼륨과 qtree의 파일을 소유하기 때문에 볼륨과 qtree의 루트 사용자에 대해 파생된 사용자 할당량이 생성되었습니다. 루트 사용자는 할당량과 관련하여 특별한 치료를 받게 되므로, 파생 할당량은 할당량만 추적합니다.

qtree에 대해 지정된 사용자 할당량의 예

이 예는 관리자가 qtree에 할당량을 2개 추가했다는 점을 제외하면 이전 쿼터와 비슷합니다.

Q1에는 여전히 볼륨 1과 볼륨 1과 qtree 1이 있습니다. 관리자가 다음 할당량을 생성했습니다.

- 400MB의 vol1에 대한 기본 트리 할당량 제한입니다
- 100MB의 vol1에 대한 기본 사용자 할당량 제한입니다
- 200MB의 사용자 jsmith에 대한 vol1의 명시적 사용자 할당량 제한입니다
- qtree 1분기에 기본 사용자 할당량 한도 50MB
- 75MB의 사용자 jsmith에 대해 Qtree Q1 에 대한 명시적 사용자 할당량 제한입니다

이러한 할당량에 대한 할당량 규칙은 다음과 같습니다.

```
cluster1::> volume quota policy rule show -vserver vs1 -volume vol1

Vserver: vs1               Policy: default           Volume: vol1
                                                Soft             Soft
                          User          Disk     Disk    Files    Files
Type    Target    Qtree   Mapping      Limit    Limit    Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree    ""        ""      -           400MB        -       -        -
-
user    ""        ""      off         100MB        -       -        -
-
user    ""        q1      off          50MB        -       -        -
-
user    jsmith    ""      off         200MB        -       -        -
-
user    jsmith    q1      off          75MB        -       -        -
-
```

이러한 할당량에 대한 할당량 보고서는 다음과 같습니다.

```
cluster1::> volume quota report
Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     -          tree   *           0B  400MB       0       -   *
vol1     -          user   *           0B  100MB       0       -   *
vol1     -          user   jsmith   2000B  200MB       7       -   jsmith
vol1     q1         user   *           0B   50MB       0       -   *
vol1     q1         user   jsmith      0B   75MB       5       -   jsmith
vol1     q1         tree   1           0B  400MB       6       -   q1
vol1     -          user   root        0B    0MB       2       -
vol1     q1         user   root        0B    0MB       1       -
```

할당량 보고서의 처음 다섯 줄에는 관리자가 생성한 할당량 5개가 표시됩니다. 이러한 할당량 중 일부는 기본 할당량이므로 ONTAP는 자동으로 파생 할당량을 생성합니다.

6번째 줄에는 vol1의 모든 qtree에 대한 기본 트리 할당량에서 파생된 트리 할당량이 표시됩니다(이 예제에서는 Q1만 해당).

마지막 두 줄에는 볼륨 및 qtree의 기본 사용자 할당량에서 파생된 사용자 할당량이 표시됩니다. 루트 사용자가 볼륨과 qtree의 파일을 소유하기 때문에 볼륨과 qtree의 루트 사용자에 대해 파생된 사용자 할당량이 생성되었습니다. 루트 사용자는 할당량과 관련하여 특별한 치료를 받게 되므로, 파생 할당량은 할당량만 추적합니다.

다음과 같은 이유로 다른 기본 할당량 또는 파생 할당량이 생성되지 않았습니다.

- 사용자가 두 레벨에서 이미 명시적 할당량을 가지고 있기 때문에 볼륨과 qtree에 있는 파일을 소유하고 있더라도 jsmith 사용자에 대해 파생된 사용자 할당량이 생성되지 않았습니다.
- 다른 사용자가 볼륨 또는 qtree에 있는 파일을 소유하지 않기 때문에 다른 사용자에 대해 파생된 사용자 할당량이 생성되지 않았습니다.
- qtree에 기본 사용자 할당량이 이미 있기 때문에 볼륨에 있는 기본 사용자 할당량이 qtree에 기본 사용자 할당량을 생성하지 않았습니다.

사용자 추가 할당량이 구성된 할당량과 다른 이유

파생 할당량은 구성 없이 적용되지만 구성된 할당량은 성공적으로 초기화된 후에만 적용되기 때문에 적용된 할당량과 구성된 할당량이 다릅니다. 이러한 차이점을 이해하면 할당량 보고서에 표시되는 강제 할당량을 구성한 할당량과 비교할 수 있습니다.

할당량 보고서에 표시되는 강제 할당량은 다음과 같은 이유로 구성된 할당량 규칙과 다를 수 있습니다.

- 파생된 할당량은 할당량 규칙으로 구성되지 않고 적용됩니다. ONTAP는 기본 할당량에 대한 응답으로 파생된 할당량을 자동으로 생성합니다.
- 할당량 규칙을 구성한 후 볼륨에 대해 할당량이 다시 초기화되지 않았을 수 있습니다.

- 볼륨에 할당량을 초기화할 때 오류가 발생했을 수 있습니다.

할당량 보고서를 사용하여 특정 파일에 대한 쓰기를 제한하는 할당량을 결정합니다

특정 파일 경로와 함께 volume quota report 명령을 사용하여 파일에 대한 쓰기 작업에 영향을 주는 할당량 한도를 결정할 수 있습니다. 이렇게 하면 어떤 할당량이 쓰기 작업을 방해하는지 이해하는 데 도움이 됩니다.

단계

1. path 매개 변수와 함께 volume quota report 명령을 사용합니다.

특정 파일에 영향을 주는 할당량을 보여 주는 예

다음 예제에서는 FlexVol 볼륨 vol2의 qtree Q1 내에 있는 파일 1에 쓸 때 적용되는 할당량을 결정하는 명령 및 출력을 보여 줍니다.

```
cluster1:> volume quota report -vserver vs0 -volume vol2 -path
/vol/vol2/q1/file1
Virtual Server: vs0
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol2     q1        tree    jsmith     1MB  100MB       2   10000   q1
vol2     q1        group   eng        1MB  700MB       2   70000
vol2               group   eng        1MB  700MB       6   70000   *
vol2               user    corp\jsmith
                                      1MB   50MB       1       -   *
vol2     q1        user    corp\jsmith
                                      1MB   50MB       1       -
5 entries were displayed.
```

ONTAP의 할당량에 대한 정보를 표시하는 명령입니다

명령을 사용하면 적용된 할당량과 리소스 사용량이 포함된 할당량 보고서를 표시하고, 할당량 상태 및 오류에 대한 정보를 표시하거나, 할당량 정책 및 할당량 규칙에 대한 정보를 표시할 수 있습니다.

다음 명령은 FlexVol 볼륨에서만 실행할 수 있습니다.

원하는 작업	이 명령 사용...
적용된 할당량에 대한 정보를 봅니다	볼륨 할당량 보고서

원하는 작업	이 명령 사용...
할당량 타겟의 리소스 사용량(디스크 공간 및 파일 수)을 봅니다	볼륨 할당량 보고서
파일에 쓸 수 있을 때 영향을 받는 할당량 제한을 확인합니다	path 매개 변수가 있는 볼륨 할당량 보고서
on, off, initializing 등의 할당상태를 표시합니다	볼륨 할당량 표시
할당량 메시지 로깅에 대한 정보를 봅니다	logmsg 매개 변수가 있는 볼륨 할당량 표시
할당량 초기화 및 크기 조정 중에 발생하는 오류를 봅니다	인스턴스 매개 변수를 사용한 볼륨 할당량 표시
할당량 정책에 대한 정보를 봅니다	볼륨 할당량 정책이 표시됩니다
할당량 규칙에 대한 정보를 봅니다	볼륨 할당량 정책 규칙이 표시됩니다
스토리지 가상 머신(SVM, 이전의 Vserver)에 할당된 할당량 정책의 이름을 봅니다.	vserver show와 -instance 매개 변수를 함께 사용합니다

에 대한 자세한 내용은 `volume quota` "ONTAP 명령 참조입니다"을 참조하십시오.

볼륨 할당량 정책 규칙 표시 및 볼륨 할당량 보고서 명령을 사용하는 경우

두 명령 모두 할당량에 대한 정보를 표시하지만 볼륨 할당량 정책 규칙은 구성된 할당량 규칙을 빠르게 표시하고, 시간과 리소스를 더 많이 사용하는 볼륨 할당량 보고서 명령은 적용된 할당량과 리소스 사용량을 표시합니다.

'volume quota policy rule show' 명령은 다음과 같은 용도로 유용합니다.

- 할당량 규칙을 활성화하기 전에 구성을 확인하십시오

  이 명령은 할당량이 초기화되었는지 또는 크기가 조정되었는지 여부에 관계없이 구성된 모든 할당량 규칙을 표시합니다.

- 시스템 리소스에 영향을 주지 않고 할당량 규칙을 빠르게 봅니다

  이 명령은 디스크 및 파일 사용량을 표시하지 않으므로 할당량 보고서만큼 리소스를 많이 사용하지 않습니다.

- SVM에 할당되지 않은 할당량 정책에 할당량 규칙을 표시합니다.

에 대한 자세한 내용은 `volume quota policy rule show` "ONTAP 명령 참조입니다"을 참조하십시오.

볼륨 할당량 보고서 명령은 다음과 같은 용도로 유용합니다.

- 파생 할당량을 비롯한 적용된 할당량을 봅니다

- 파생 할당량의 영향을 받는 대상을 포함하여 모든 할당량이 사용하는 디스크 공간 및 파일 수를 확인합니다

  기본 할당량의 경우, 결과 파생 할당량에 대해 사용량이 추적되므로 사용량이 "0"으로 표시됩니다.

- 파일에 대한 쓰기가 허용되는 경우 어떤 할당량 제한이 영향을 미치는지 확인합니다

  볼륨 할당량 보고서 명령에 '-path' 매개 변수를 추가합니다.

> 할당량 보고서는 리소스를 많이 사용하는 작업입니다. 클러스터의 많은 FlexVol 볼륨에서 실행하는 경우 완료하는 데 오랜 시간이 걸릴 수 있습니다. 더 효율적인 방법은 SVM의 특정 볼륨에 대한 할당량 보고서를 보는 것입니다.

에 대한 자세한 내용은 `volume quota report` "ONTAP 명령 참조입니다"을 참조하십시오.

할당량 보고서 및 **UNIX** 클라이언트에 의해 표시되는 공간 사용량 차이

할당량 보고서와 **UNIX** 클라이언트에 의해 표시되는 공간 사용량 차이에 대한 개요입니다

FlexVol volume 또는 qtree의 할당량 보고서에 표시되는 사용된 디스크 공간의 값은 같은 볼륨 또는 qtree에 대해 UNIX 클라이언트에서 표시하는 값과 다를 수 있습니다. 이 값의 차이는 볼륨 또는 qtree의 데이터 블록을 계산하기 위한 다양한 방법 뒤에 할당량 보고서와 UNIX 명령이 있기 때문입니다.

예를 들어, 볼륨에 데이터가 기록되지 않은 빈 데이터 블록이 있는 파일이 포함된 경우 볼륨에 대한 할당량 보고서에서 공간 사용량을 보고하는 동안 빈 데이터 블록이 계산되지 않습니다. 그러나 볼륨이 UNIX 클라이언트에 마운트되어 있고 파일이 "ls" 명령의 출력으로 표시되면 빈 데이터 블록도 공간 사용량에 포함됩니다. 따라서 "ls" 명령은 할당량 보고서에 표시되는 공간 사용량과 비교하여 더 큰 파일 크기를 표시합니다.

마찬가지로 할당량 보고서에 표시되는 공간 사용량 값도 "df", "du"와 같은 UNIX 명령의 결과로 표시되는 값과 다를 수 있습니다.

할당량 보고서에서 디스크 공간 및 파일 사용량을 확인하는 방법

FlexVol 볼륨 또는 qtree에 대해 할당량 보고서에 지정된 파일 수와 디스크 공간 크기는 볼륨 또는 qtree의 모든 inode에 해당하는 사용된 데이터 블록의 수에 따라 달라집니다.

블록 수에는 일반 및 스트림 파일에 사용되는 직접 및 간접 블록이 모두 포함됩니다. 디렉토리, ACL(액세스 제어 목록), 스트림 디렉토리 및 메타파일에 사용되는 블록이 할당량 보고서에 고려되지 않습니다. UNIX 스파스 파일의 경우 빈 데이터 블록이 할당량 보고서에 포함되지 않습니다.

할당량 하위 시스템은 사용자가 제어할 수 있는 파일 시스템 측면만 고려하고 포함하도록 설계되었습니다. 디렉토리, ACL 및 스냅샷 공간은 모두 할당량 계산에서 제외된 공간의 예입니다. 할당량은 보장이 아닌 제한을 적용하는 데 사용되며 활성 파일 시스템에서만 작동합니다. 할당량 계산에서는 특정 파일 시스템 구문을 계산하지 않으며 압축 또는 중복 제거와 같은 스토리지 효율성을 고려하지 않습니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ls 명령과 공간 사용에 대한 할당량 보고서 간의 불일치입니다

`ls`명령을 사용하여 UNIX 클라이언트에 마운트된 FlexVol volume의 컨텐츠를 볼 때 출력에 표시되는 파일 크기는 파일의 데이터 블록 유형에 따라 볼륨에 대한 할당량 보고서에 표시되는 공간 사용량과 다를 수 있습니다.

ls 명령의 출력은 파일의 크기만 표시하고 파일에 사용되는 간접 블록은 포함하지 않습니다. 파일의 빈 블록도 명령의 출력에 포함됩니다.

따라서 파일에 빈 블록이 없는 경우 할당량 보고서에 간접 블록이 포함되기 때문에 "ls" 명령으로 표시되는 크기가 할당량 보고서에 지정된 디스크 사용량보다 작을 수 있습니다. 반대로, 파일에 빈 블록이 있으면 "ls" 명령으로 표시되는 크기가 할당량 보고서에 지정된 디스크 사용량보다 클 수 있습니다.

ls 명령의 출력은 파일의 크기만 표시하고 파일에 사용되는 간접 블록은 포함하지 않습니다. 파일의 빈 블록도 명령의 출력에 포함됩니다.

ls 명령과 할당량 보고서에 사용된 공간 사용량 간의 차이 예

다음 할당량 보고서는 qtree Q1: 10MB의 한도를 보여줍니다.

```
                                      ----Disk----  ----Files-----   Quota
  Volume   Tree       Type    ID        Used  Limit    Used   Limit
Specifier
  -------  ---------  ------  --------  -----  -----  ------  ------
---------
  vol1     q1           tree    user1   10MB  10MB        1       -   q1

...
```

다음 예와 같이 UNIX 클라이언트에서 "ls" 명령을 사용하여 동일한 qtree에 있는 파일의 크기가 할당량 제한을 초과할 수 있습니다.

```
[user1@lin-sys1 q1]$ ls -lh
-rwxr-xr-x  1 user1 nfsuser  **27M** Apr 09  2013 file1
```

에 대한 자세한 내용은 `ls` "ONTAP 명령 참조입니다"을 참조하십시오.

df 명령이 파일 크기를 어떻게 계산하는지 확인합니다

'df' 명령에서 공간 사용을 보고하는 방식은 qtree가 포함된 볼륨에 대해 할당량을 설정하거나 해제할지 여부와 qtree 내의 할당량 사용을 추적할지 여부와 같은 두 가지 조건에 따라 달라집니다.

qtree가 포함된 볼륨에 대해 할당량을 설정하고 qtree 내의 할당량 사용을 추적할 때 df 명령으로 보고되는 공간 사용은 할당량 보고서에 지정된 값과 동일합니다. 이 경우 할당량 사용 시 디렉토리, ACL, 스트림 디렉토리 및 메타파일에서 사용되는 블록이 제외됩니다.

볼륨에 할당량이 설정되어 있지 않거나 qtree에 할당량 규칙이 구성되어 있지 않은 경우 보고된 공간 사용에는 볼륨 내의

다른 qtree를 포함하여 전체 볼륨에 대한 디렉토리, ACL, 스트림 디렉토리 및 메타파일에서 사용되는 블록이 포함됩니다. 이 경우 'df' 명령으로 보고되는 공간 사용량이 할당량을 추적할 때 보고되는 예상 값보다 큽니다.

할당량 사용을 추적할 qtree의 마운트 지점에서 df 명령을 실행하면 명령 출력에 할당량 보고서에 지정된 값과 동일한 공간 사용량이 표시됩니다. 대부분의 경우 트리 할당량 규칙에 하드 디스크 제한이 있는 경우 df 명령이 보고하는 총 크기는 디스크 제한과 같고 사용 가능한 공간은 할당량 디스크 제한과 할당량 사용 간의 차이입니다.

그러나 일부 경우 df 명령으로 보고되는 공간은 볼륨 전체에서 사용 가능한 공간과 동일할 수 있습니다. 이 문제는 qtree에 대해 구성된 하드 디스크 제한이 없을 때 발생합니다. ONTAP 9.9.1부터 볼륨 전체에서 사용 가능한 공간이 나머지 트리 할당량 공간보다 작을 때도 발생할 수 있습니다. 이러한 조건 중 하나가 발생할 경우 df 명령으로 보고되는 총 크기는 qtree 내에서 사용된 할당량과 FlexVol 볼륨에서 사용 가능한 공간을 더한 값과 같은 합성 숫자입니다.

> ⓘ 이 총 크기는 qtree 디스크 제한이나 볼륨 구성 크기가 아닙니다. 다른 qtree나 백그라운드 스토리지 효율성 활동에 대한 쓰기 활동에도 따라 달라질 수 있습니다.

에서 설명하는 공간 사용량의 예 `df` 명령 및 할당량 보고서

다음 할당량 보고서는 qtree Alice의 경우 디스크 제한인 1GB, qtree Bob의 경우 2GB, qtree Project1의 경우 제한 없음을 보여줍니다.

```
C1_vsim1::> quota report -vserver vs0
Vserver: vs0
                                     ----Disk----  ----Files-----   Quota
Volume   Tree       Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol2     alice     tree    1
                                   502.0MB    1GB       2       -   alice
vol2     bob       tree    2
                                    1003MB    2GB       2       -   bob
vol2     project1  tree    3
                                   200.8MB      -       2       -
project1
vol2               tree    *           0B      -       0       -   *
4 entries were displayed.
```

다음 예에서는 qtree Alice와 bob에 대한 'df' 명령의 출력이 할당량 보고서와 같은 사용된 공간 및 디스크 제한과 동일한 총 크기(100만 블록)를 보고합니다. 이는 qtree Alice와 bob에 대한 할당량 규칙에 정의된 디스크 제한이 있고 볼륨 가용 공간(1211MB)이 qtree Alice(523MB) 및 qtree bob(1045MB)에 대해 남아 있는 트리 할당량 공간보다 크기 때문입니다.

```
linux-client1 [~]$ df -m /mnt/vol2/alice
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      1024   502       523  50% /mnt/vol2

linux-client1 [~]$ df -m /mnt/vol2/bob
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      2048  1004      1045  50% /mnt/vol2
```

다음 예제에서 qtree Project1의 df 명령 출력은 할당량 보고서와 같은 사용된 공간을 보고합니다. 그러나 총 크기는 총 1412MB의 용량을 제공하기 위해 qtree Project1(201 MB)의 할당량 사용에 전체(1211 MB)의 사용 가능한 공간을 추가하여 합성됩니다. 이는 Qtree Project1의 할당량 규칙에 디스크 제한이 없기 때문입니다.

```
linux-client1 [~]$ df -m /mnt/vol2/project1
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      1412   201      1211  15% /mnt/vol2
```

다음 예제는 전체 볼륨에 대한 df 명령의 출력이 Project1과 동일한 사용 가능한 공간을 보고하는 방법을 보여줍니다.

```
linux-client1 [~]$ df -m /mnt/vol2
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      2919  1709      1211  59% /mnt/vol2
```

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

du 명령과 공간 사용에 대한 할당량 보고서 간 불일치입니다

du 명령을 실행하여 UNIX 클라이언트에 마운트된 qtree 또는 FlexVol 볼륨의 디스크 공간 사용량을 확인할 때 사용 값이 qtree 또는 볼륨에 대한 할당량 보고서에 표시되는 값보다 높을 수 있습니다.

du 명령의 출력에는 명령이 실행되는 디렉토리 레벨에서 시작되는 디렉토리 트리를 통해 모든 파일의 전체 공간 사용량이 포함됩니다. du 명령으로 표시되는 사용 값에는 디렉토리의 데이터 블록도 포함되므로 할당량 보고서에 표시되는 값보다 높습니다.

du 명령과 할당량 보고서에서 확인된 공간 사용량 간의 차이입니다

다음 할당량 보고서는 qtree Q1: 10MB의 한도를 보여줍니다.

```
                                        ----Disk----  ----Files-----   Quota
  Volume   Tree       Type    ID        Used  Limit    Used   Limit
Specifier
  -------  --------  ------  -------  -----  -----  ------  ------
---------
  vol1     q1        tree    user1    10MB   10MB   1       -        q1

...
```

다음 예에서는 du 명령의 출력에서 디스크 공간 사용량이 할당량 제한을 초과하는 더 높은 값을 표시합니다.

```
[user1@lin-sys1 q1]$ du -sh
**11M**     q1
```

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

할당량 구성의 예

이 예에서는 할당량을 구성하고 할당량 보고서를 읽는 방법을 이해하는 데 도움이 됩니다.

예를 참조하십시오

다음 예에서는 `vs1` 볼륨 하나가 포함된 SVM이 포함된 스토리지 시스템을 사용한다고 가정합니다 `vol1`.

1. 할당량 설정을 시작하려면 SVM에 대한 새 할당량 정책을 생성합니다.

```
cluster1::>volume quota policy create -vserver vs1 -policy-name
quota_policy_vs1_1
```

2. 할당량 정책이 새로운 내용이므로 SVM에 할당하면 됩니다.

```
cluster1::>vserver modify -vserver vs1 -quota-policy quota_policy_vs1_1
```

예 **1:** 기본 사용자 할당량

1. 에서 각 사용자에 대해 50MB의 하드 제한값을 적용하기로 `vol1` 결정합니다.

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 50MB
-qtree ""
```

2. 새 규칙을 활성화하려면 볼륨에 대해 할당량을 초기화해야 합니다.

```
cluster1::>volume quota on -vserver vs1 -volume vol1 -foreground
```

3. 할당량 보고서를 볼 수 있습니다.

```
cluster1::>volume quota report
```

결과 할당량 보고서는 다음 보고서와 유사합니다.

```
Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith     49MB   50MB      37       -   *
vol1               user    root        0B      -       1       -
```

첫 번째 줄에는 디스크 제한을 포함하여 사용자가 생성한 기본 사용자 할당량이 표시됩니다. 모든 기본 할당량과 마찬가지로 이 기본 사용자 할당량에는 디스크 또는 파일 사용에 대한 정보가 표시되지 않습니다. 생성된 할당량 외에 두 개의 다른 할당량이 표시됩니다. 현재 에서 파일을 소유하고 있는 사용자마다 할당량이 하나씩 `vol1` 있습니다. 이러한 추가 할당량은 기본 사용자 할당량에서 자동으로 파생된 사용자 할당량입니다. 사용자에 대해 파생된 사용자 할당량은 `jsmith` 기본 사용자 할당량과 50MB 디스크 제한이 동일합니다. 루트 사용자의 파생 사용자 할당량은 추적 할당량(제한 없음)입니다.

시스템의 사용자(루트 사용자 제외)가 에서 50MB 이상 사용하는 작업 `vol1`(예: 편집기에서 파일에 쓰기)을 수행하려고 하면 작업이 실패합니다.

예제 **2:** 기본 사용자 할당량을 재정의하는 명시적 사용자 할당량

1. `vol1`사용자에게 볼륨에 더 많은 공간을 제공해야 하는 경우 `jsmith` 다음 명령을 입력합니다.

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit
80MB -qtree ""
```

사용자가 할당량 규칙의 타겟으로 명시적으로 나열되기 때문에 명시적 사용자 할당량입니다.

이는 `jsmith` 볼륨에서 사용자에 대해 파생된 사용자 할당량의 디스크 제한을 변경하기 때문에 기존 할당량 제한에 대한 변경 사항입니다. 따라서 변경을 활성화하기 위해 볼륨에서 할당량을 다시 초기화할 필요가 없습니다.

2. 할당량 크기 조정하기:

```
cluster1::>volume quota resize -vserver vs1 -volume vol1 -foreground
```

크기를 조정하는 동안 할당량이 계속 적용되고 크기 조정 프로세스는 짧습니다.

결과 할당량 보고서는 다음 보고서와 유사합니다.

```
cluster1::> volume quota report
Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith     50MB   80MB      37       -   jsmith
vol1               user    root        0B      -       1       -
3 entries were displayed.
```

두 번째 줄에는 의 디스크 제한과 `80MB` 할당량 지정자가 `jsmith` 표시됩니다.

따라서 `jsmith` `vol1` 다른 모든 사용자는 50MB로 제한되지만 에서 최대 80MB의 공간을 사용할 수 있습니다.

예 **3:** 임계값

사용자가 디스크 제한으로부터 5MB 이내에 도달할 때 알림을 받고자 한다고 가정합니다.

1. 모든 사용자에 대해 임계값이 45MB이고 에 대해 임계값이 75MB인 경우 `jsmith` 기존 할당량 규칙을 변경합니다.

   ```
   cluster1::>volume quota policy rule modify -vserver vs1 -policy
   quota_policy_vs1_1 -volume vol1 -type user -target "" -qtree ""
   -threshold 45MB
   cluster1::>volume quota policy rule modify -vserver vs1 -policy
   quota_policy_vs1_1 -volume vol1 -type user -target jsmith -qtree ""
   -threshold 75MB
   ```

   기존 규칙의 크기가 변경되므로 변경 사항을 활성화하기 위해 볼륨의 할당량 크기를 조정합니다. 크기 조정 프로세스가 완료될 때까지 기다립니다.

2. 임계값이 포함된 할당량 보고서를 보려면 '-thresholds' 매개 변수를 'volume quota report' 명령에 추가합니다.

```
cluster1::>volume quota report -thresholds
Vserver: vs1
                                     ----Disk----  ----Files-----
Volume   Tree      Type    ID        Used  Limit   Used    Limit  Quota
                                          (Thold)
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -  *
                                         (45MB)
vol1               user    jsmith     59MB   80MB      55       -  jsmith
                                         (75MB)
vol1               user    root        0B      -       1       -
                                         ( -)
3 entries were displayed.
```

임계값은 디스크 제한 열에 괄호 안에 표시됩니다.

에 대한 자세한 내용은 `volume quota report` "ONTAP 명령 참조입니다"을 참조하십시오.

예 **4: qtree**의 할당량

두 프로젝트의 공간을 분할해야 한다고 가정해 보겠습니다. `proj1`와 라는 두 개의 `qtree`를 `proj2` 생성하여 에서 이러한 프로젝트를 수용할 수 있습니다 `vol1`.

현재 사용자는 전체 볼륨에 할당된 qtree의 공간을 사용할 수 있습니다(루트 또는 다른 qtree의 공간을 사용하여 볼륨 제한을 초과하지 않은 경우). 또한 각 qtree는 전체 볼륨을 사용하기 위해 증가할 수 있습니다.

1. 두 qtree가 20GB를 초과하여 확장되지 않도록 하려면 볼륨에 기본 트리 할당량을 생성할 수 있습니다.

```
cluster1:>>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type tree -target "" -disk-limit 20GB
```

올바른 유형은 qtree가 아니라 _tree_입니다.

2. 새 할당량이므로 크기를 조정하여 활성화할 수 없습니다. 볼륨에 대해 할당량을 다시 초기화합니다.

```
cluster1:>>volume quota off -vserver vs1 -volume vol1
cluster1:>>volume quota on -vserver vs1 -volume vol1 -foreground
```

명령을 실행한 후 거의 즉시 할당량을 활성화하려고 하면 오류가 발생할 수 있으므로 영향을 받는 각 볼륨에 대해 할당량을 다시 활성화하기 전에 약 5분 정도 기다려야 합니다. `volume quota off` 또는 명령을 실행하여 특정 볼륨이 포함된 노드에서 볼륨에 대한 할당량을 다시 초기화할 수 있습니다. 에 대한 자세한 내용은 `volume quota off` "ONTAP 명령 참조입니다"을 참조하십시오.

재초기화 프로세스 중에는 할당량이 적용되지 않으므로 크기 조정 프로세스보다 시간이 더 오래 걸립니다.

할당량 보고서를 표시하면 몇 개의 새 줄이 표시됩니다. 일부 줄은 트리 할당량용이고 일부 줄은 파생된 사용자 할당량용입니다.

트리 할당량에 대한 새로운 줄은 다음과 같습니다.

```
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
...
vol1              tree    *           0B   20GB       0       -   *
vol1     proj1    tree    1           0B   20GB       1       -   proj1
vol1     proj2    tree    2           0B   20GB       1       -   proj2
...
```

새로 만든 기본 트리 할당량이 ID 열에 별표(*)가 있는 첫 번째 새 줄에 나타납니다. 볼륨의 기본 트리 할당량에 대응하여 ONTAP은 볼륨의 각 qtree에 대해 자동으로 파생 트리 할당량을 생성합니다. 이러한 항목은 `proj1` `proj2` `Tree` 열에 및 가 표시되는 줄에 표시됩니다.

파생된 사용자 할당량에 대한 새로운 줄은 다음과 같습니다.

```
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
...
vol1     proj1     user    *           0B   50MB       0       -
vol1     proj1     user    root        0B      -       1       -
vol1     proj2     user    *           0B   50MB       0       -
vol1     proj2     user    root        0B      -       1       -
...
```

qtree에 대해 할당량이 설정된 경우, 볼륨에 포함된 모든 qtree에 대해 볼륨에 대한 기본 사용자 할당량이 자동으로 상속됩니다. 첫 번째 qtree 할당량을 추가하면 Qtree에서 할당량이 설정됩니다. 따라서 각 qtree에 대해 파생 기본 사용자 할당량이 생성되었습니다. ID가 별표(*)인 줄에 표시됩니다.

루트 사용자는 파일의 소유자이므로 각 qtree에 대해 기본 사용자 할당량이 생성되었을 때 각 qtree에 대해 루트 사용자에 대해 특수 추적 할당량도 생성되었습니다. ID가 root 인 줄에 표시됩니다.

예 **5: qtree**의 사용자 할당량

1. 사용자는 `proj1` qtree에서 볼륨 전체에서 확보하는 것보다 더 적은 공간을 사용하도록 제한해야 합니다. 이 `proj1` 경우 qtree에서 10MB 이상의 데이터를 사용하지 않도록 합니다. 따라서 qtree에 대한 기본 사용자

할당량을 생성합니다.

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 10MB
-qtree proj1
```

볼륨의 기본 사용자 할당량에서 파생된 proj1 qtree의 기본 사용자 할당량을 변경하기 때문에 기존 할당량이 변경됩니다. 따라서 할당량의 크기를 조정하여 변경을 활성화합니다. 크기 조정 프로세스가 완료되면 할당량 보고서를 볼 수 있습니다.

할당량 보고서에 qtree에 대한 새로운 명시적 사용자 할당량을 보여주는 다음과 같은 새로운 줄이 나타납니다.

```
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     proj1     user    *           0B   10MB       0       -   *
```

그러나 `jsmith` 기본 사용자 할당량을 재정의하기 위해 생성한 할당량이 볼륨에 있기 때문에 사용자가 proj1 qtree에 더 많은 데이터를 쓸 수 없습니다. `proj1`qtree에 기본 사용자 할당량을 추가하면 해당 할당량이 적용되고 해당 `qtree`에서 을 포함하여 모든 사용자 공간이 제한됩니다. `jsmith`

2. 사용자에게 더 많은 공간을 제공하기 위해 `jsmith` 80MB 디스크 제한을 사용하여 qtree에 대한 명시적 사용자 할당량 규칙을 추가하여 qtree의 기본 사용자 할당량 규칙을 재정의합니다.

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit
80MB -qtree proj1
```

이 할당량은 기본 할당량이 이미 존재하는 명시적 할당량이므로 할당량 크기를 조정하여 변경 사항을 활성화합니다. 크기 조정 프로세스가 완료되면 할당량 보고서가 표시됩니다.

할당량 보고서에 다음과 같은 새 줄이 나타납니다.

```
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     proj1     user    jsmith    61MB   80MB      57       -   jsmith
```

최종 할당량 보고서는 다음 보고서와 비슷합니다.

```
cluster1::>volume quota report
Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               tree    *           0B   20GB       0       -   *
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith    70MB   80MB      65       -   jsmith
vol1     proj1     tree    1           0B   20GB       1       -   proj1
vol1     proj1     user    *           0B   10MB       0       -   *
vol1     proj1     user    root        0B      -       1       -
vol1     proj2     tree    2           0B   20GB       1       -   proj2
vol1     proj2     user    *           0B   50MB       0       -
vol1     proj2     user    root        0B      -       1       -
vol1               user    root        0B      -       3       -
vol1     proj1     user    jsmith    61MB   80MB      57       -   jsmith
11 entries were displayed.
```

사용자는 `jsmith` 에서 파일에 쓰려면 다음과 같은 할당량 제한을 충족해야 `proj1` 합니다.

1. `proj1`qtree의 트리 할당량입니다.
2. `proj1`qtree의 사용자 할당량입니다.
3. 볼륨의 사용자 할당량입니다.

SVM에서 할당량 설정

새로운 SVM에 할당량을 설정하여 리소스 활용률을 관리하고 모니터링할 수 있습니다.

이 작업에 대해

할당량을 구성할 때 다음과 같은 몇 가지 단계가 포함됩니다.

1. 할당량 정책을 생성합니다
2. 정책에 할당량 규칙을 추가합니다
3. SVM에 정책을 할당합니다
4. SVM의 각 FlexVol volume에 대한 할당량을 초기화합니다

단계

1. 명령을 입력합니다 `vserver show -instance` SVM이 생성될 때 자동으로 생성된 기본 할당량 정책의 이름을 표시합니다.

   SVM을 생성할 때 이름을 지정하지 않은 경우 이름이 "기본값"이 됩니다. 를 사용할 수 있습니다 `vserver quota policy rename` 기본 정책에 이름을 지정하는 명령입니다.

볼륨 할당량 정책 생성 명령을 사용하여 새 정책을 생성할 수도 있습니다.

2. "volume quota policy rule create" 명령을 사용하여 SVM의 각 볼륨에 대해 다음 할당량 규칙 중 _any_를 생성합니다.
   - 모든 사용자에 대한 기본 할당량 규칙입니다
   - 특정 사용자에 대한 명시적 할당량 규칙
   - 모든 그룹에 대한 기본 할당량 규칙입니다
   - 특정 그룹에 대한 명시적 할당량 규칙을 나타냅니다
   - 모든 qtree에 대한 기본 할당량 규칙
   - 특정 qtree에 대한 명시적 할당량 규칙
3. 'volume quota policy rule show' 명령을 사용하여 할당량 규칙이 올바르게 구성되었는지 확인합니다.
4. 새 정책을 작업 중인 경우 "vserver modify" 명령을 사용하여 SVM에 새 정책을 할당합니다.
5. "volume quota on" 명령을 사용하여 SVM의 각 볼륨에 대한 할당량을 초기화합니다.

   다음과 같은 방법으로 초기화 프로세스를 모니터링할 수 있습니다.
   - 'volume quota on' 명령을 사용하면 포그라운드에 있는 작업에서 할당량을 실행하기 위해 '-foreground' 매개 변수를 추가할 수 있습니다. (기본적으로 작업은 백그라운드에서 실행됩니다.)

     작업이 백그라운드에서 실행되면 job show 명령을 사용하여 진행 상황을 모니터링할 수 있습니다.
   - 'volume quota show' 명령을 사용하여 할당량 초기화 상태를 모니터링할 수 있습니다.
6. "volume quota show -instance" 명령을 사용하여 초기화에 실패한 할당량 규칙과 같은 초기화 오류를 확인합니다.
7. "volume quota report" 명령을 사용하여 할당량 보고서를 표시하면 적용된 할당량이 기대에 맞는지 확인할 수 있습니다.

관련 정보

- "vserver show 를 참조하십시오"
- "SVM 수정"
- "작업 표시"
- "볼륨 할당량"

할당량 제한을 수정하거나 크기를 조정합니다

영향을 받는 모든 볼륨에서 할당량을 변경하거나 크기를 조정할 수 있으며 이 경우 해당 볼륨에 대한 할당량을 다시 초기화하는 것보다 빠릅니다.

이 작업에 대해

스토리지 가상 머신(SVM, 이전 명칭 Vserver)에 강제 할당량이 있고, 기존 할당량의 크기 제한을 변경하거나, 이미 파생 할당량이 있는 타겟에 할당량을 추가하거나 삭제할 수 있습니다.

단계

1. '-instance' 매개 변수와 함께 'vserver show' 명령을 사용하여 현재 SVM에 할당된 정책의 이름을 확인합니다.

2. 다음 작업을 수행하여 할당량 규칙을 수정합니다.
   - 'volume quota policy rule modify' 명령을 사용하여 기존 할당량 규칙의 디스크 또는 파일 제한을 수정합니다.
   - "volume quota policy rule create" 명령을 사용하여 현재 파생 할당량이 있는 타겟(사용자, 그룹 또는 qtree)에 대한 명시적 할당량 규칙을 생성합니다.
   - "volume quota policy rule delete" 명령을 사용하여 기본 할당량이 있는 타겟(사용자, 그룹 또는 qtree)에 대한 명시적 할당량 규칙을 삭제합니다.
3. 'volume quota policy rule show' 명령을 사용하여 할당량 규칙이 올바르게 구성되었는지 확인합니다.
4. 할당량을 변경한 각 볼륨에 대해 '볼륨 할당량 크기 조정' 명령을 사용하여 각 볼륨의 변경 사항을 활성화합니다.

   다음 방법 중 하나를 사용하여 크기 조정 프로세스를 모니터링할 수 있습니다.
   - 'volume quota resize' 명령어를 사용할 때 foreground' 파라미터를 추가하여 foreground에서 resize 작업을 실행할 수 있다. (기본적으로 작업은 백그라운드에서 실행됩니다.)

     작업이 백그라운드에서 실행되면 job show 명령을 사용하여 진행 상황을 모니터링할 수 있습니다.
   - 'volume quota show' 명령을 사용하여 크기 조정 상태를 모니터링할 수 있습니다.
5. 'volume quota show-instance' 명령을 사용하여 크기를 조정하지 못한 할당량 규칙과 같은 크기 조정 오류를 확인합니다.

   특히 파생 할당량이 아직 없는 타겟에 대해 명시적 할당량을 추가한 후 할당량의 크기를 조정할 때 발생하는 ""새 정의" 오류를 확인하십시오.
6. "volume quota report" 명령을 사용하여 할당량 보고서를 표시하여 사용자 요구 사항에 맞게 적용된 할당량을 설정할 수 있습니다.

관련 정보

- "볼륨 할당량 정책 규칙입니다"
- "볼륨 할당량"
- "작업 표시"

대대적인 변경 작업을 수행한 후 할당량을 다시 초기화합니다

기존 할당량 정의를 크게 변경한 후에는 영향을 받는 모든 볼륨에서 할당량을 다시 초기화해야 합니다. 이러한 유형의 변경은 적용된 할당량이 없는 대상에 대한 할당량을 추가하거나 삭제하는 경우를 예로 들 수 있습니다.

이 작업에 대해

할당량을 강제 적용한 SVM(스토리지 가상 시스템)이 있으며, 할당량을 완전히 재초기화해야 하는 변경 작업을 수행할 수 있습니다.

단계

1. '-instance' 매개 변수와 함께 'vserver show' 명령을 사용하여 현재 SVM에 할당된 정책의 이름을 확인합니다.
2. 다음 작업을 수행하여 할당량 규칙을 수정합니다.

원하는 작업	그러면...
새 할당량 규칙을 생성합니다	볼륨 할당량 정책 규칙 생성 명령을 사용합니다
기존 할당량 규칙 설정을 수정합니다	볼륨 할당량 정책 규칙 수정 명령을 사용합니다
기존 할당량 규칙을 삭제합니다	'volume quota policy rule delete' 명령어를 사용한다

3. 'volume quota policy rule show' 명령을 사용하여 할당량 규칙이 올바르게 구성되었는지 확인합니다.
4. 할당량을 해제한 다음 해당 볼륨에 대해 할당량을 설정하면 할당량을 변경한 각 볼륨에서 할당량을 다시 초기화합니다.
   a. 영향을 받는 각 볼륨에서 'volume quota off' 명령을 사용하여 해당 볼륨에 대한 할당량을 해제하십시오.
   b. 영향을 받는 각 볼륨에 대해 'volume quota on' 명령을 사용하여 해당 볼륨에 대한 할당량을 활성화합니다.

   "volume quota off" 명령을 실행한 후 거의 즉시 할당량을 활성화하려고 하면 오류가 발생할 수 있으므로 영향을 받는 각 볼륨에서 할당량을 다시 활성화하기 전에 약 5분 정도 기다려야 합니다.

   또는 명령을 실행하여 특정 볼륨이 포함된 노드에서 볼륨에 대한 할당량을 다시 초기화할 수 있습니다.

   다음 방법 중 하나를 사용하여 초기화 프로세스를 모니터링할 수 있습니다.

   - 'volume quota on' 명령을 사용하면 포그라운드에 있는 작업에서 할당량을 실행하기 위해 '-foreground' 매개 변수를 추가할 수 있습니다. (기본적으로 작업은 백그라운드에서 실행됩니다.)

     작업이 백그라운드에서 실행되면 job show 명령을 사용하여 진행 상황을 모니터링할 수 있습니다.

   - 'volume quota show' 명령을 사용하여 할당량 초기화 상태를 모니터링할 수 있습니다.
5. "volume quota show -instance" 명령을 사용하여 초기화에 실패한 할당량 규칙과 같은 초기화 오류를 확인합니다.
6. "volume quota report" 명령을 사용하여 할당량 보고서를 표시하면 적용된 할당량이 기대에 맞는지 확인할 수 있습니다.

관련 정보

- "vserver show 를 참조하십시오"
- "볼륨 할당량 정책 규칙입니다"
- "볼륨 할당량"
- "작업 표시"

할당량 규칙 및 할당량 정책을 관리하는 명령입니다

`volume quota policy rule`명령을 사용하여 할당량 규칙을 구성할 수 있으며 `volume quota policy` 명령과 일부 `vserver` 명령을 사용하여 할당량 정책을 구성할 수 있습니다. 수행해야 하는 작업에 따라 다음 명령을 사용하여 할당량 규칙 및 할당량 정책을 관리할 수 있습니다.

다음 명령은 FlexVol 볼륨에서만 실행할 수 있습니다.

할당량 규칙을 관리하는 명령입니다

원하는 작업	이 명령 사용...
새 할당량 규칙을 생성합니다	볼륨 할당량 정책 규칙 생성
기존 할당량 규칙을 삭제합니다	볼륨 할당량 정책 규칙 삭제
기존 할당량 규칙을 수정합니다	볼륨 할당량 정책 규칙 수정
구성된 할당량 규칙에 대한 정보를 표시합니다	볼륨 할당량 정책 규칙이 표시됩니다

할당량 정책을 관리하는 명령입니다

원하는 작업	이 명령 사용...
할당량 정책과 포함된 할당량 규칙을 복제합니다	볼륨 할당량 정책 복사
비어 있는 새 할당량 정책을 생성합니다	볼륨 할당량 정책 생성
현재 SVM(스토리지 가상 머신)에 할당되지 않은 기존 할당량 정책 삭제	볼륨 할당량 정책 삭제
할당량 정책의 이름을 바꿉니다	볼륨 할당량 정책 이름 바꾸기
할당량 정책에 대한 정보를 표시합니다	볼륨 할당량 정책이 표시됩니다
SVM에 할당량 정책을 지정합니다	`vserver modify -quota-policy` *`policy_name`*
SVM에 할당된 할당량 정책의 이름을 표시합니다	'vserver show'

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

관련 정보

- "볼륨 할당량 정책입니다"

- "vserver modify -quota -policy policy_name입니다"
- "vserver show 를 참조하십시오"

ONTAP에서 할당량을 활성화하고 수정하는 명령입니다

`volume quota` 명령을 사용하여 할당량의 상태를 변경하고 할당량의 메시지 로깅을 구성할 수 있습니다. 수행해야 하는 작업에 따라 다음 명령을 사용하여 할당량을 활성화하고 수정할 수 있습니다.

원하는 작업	이 명령 사용...
할당량 설정(_initializing_otas라고도 함)	볼륨 할당량 설정
기존 할당량 크기 조정	볼륨 할당량 크기 조정
할당량을 해제합니다	볼륨 할당량이 꺼졌습니다
할당량에 대한 메시지 로깅 변경, 할당량 설정, 할당량 해제 또는 기존 할당량 크기 조정	볼륨 할당량 수정

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

관련 정보

- "볼륨 할당량이 켜져 있습니다"
- "볼륨 할당량 크기 조정"
- "볼륨 할당량이 꺼져 있습니다"
- "볼륨 할당량 수정"

중복제거, 데이터 압축, 데이터 컴팩션을 사용하여 스토리지 효율성을 높입니다

중복제거, 데이터 압축, 데이터 컴팩션, 스토리지 효율성

중복제거, 데이터 압축, 데이터 컴팩션을 함께 실행하거나 독립적으로 실행하여 FlexVol 볼륨에서 최적의 공간 절약 효과를 달성할 수 있습니다. 중복 제거는 중복되는 데이터 블록을 제거합니다. 데이터 압축: 데이터 블록을 압축하여 필요한 물리적 스토리지의 양을 줄입니다. 데이터 컴팩션은 더 적은 공간에 더 많은 데이터를 저장하여 스토리지 효율성을 높입니다.

인라인 중복 제거 및 인라인 압축과 같은 모든 인라인 스토리지 효율성 기능은 AFF 볼륨에서 기본적으로 활성화됩니다.

볼륨에 대해 중복 제거를 설정합니다

FlexVol 볼륨에서 중복 제거를 활성화하여 스토리지 효율성을 달성할 수 있습니다. AFF 또는 Flash Pool 애그리게이트에 있는 볼륨의 모든 볼륨과 인라인 중복제거에서 사후 처리

중복제거를 사용할 수 있습니다.

다른 유형의 볼륨에서 인라인 중복 제거를 활성화하려면 다음을 참조하세요."NetApp 기술 자료: 비 AFF (All Flash FAS) 집계에서 볼륨 인라인 중복 제거를 활성화하는 방법" .

시작하기 전에

FlexVol 볼륨의 경우 볼륨 및 애그리게이트에서 중복제거 메타데이터를 위한 충분한 여유 공간이 있는지 확인해야 합니다. 중복제거 메타데이터는 애그리게이트에서 최소한의 여유 공간만 필요로 합니다. 이 양은 중복제거된 애그리게이트에 있는 모든 FlexVol 볼륨 또는 데이터 구성요소의 총 물리적 데이터 양의 3%입니다. 각 FlexVol 볼륨 또는 데이터 구성요소에는 전체 물리적 데이터가 차지하는 여유 공간의 4%가 필요하므로 총 7%가 됩니다.

AFF 시스템에서는 인라인 중복 제거가 기본적으로 활성화되어 있습니다.

선택

- 명령을 사용하여 `volume efficiency on` 사후 처리 중복제거를 활성화합니다. 에 대한 자세한 내용은 `volume efficiency on` "ONTAP 명령 참조입니다"을 참조하십시오.

  다음 명령을 실행하면 볼륨 VolA에서 사후 처리 중복제거가 활성화됩니다.

  'vserver vs1-volume vola의 볼륨 효율성'

- 사후 처리 중복제거와 인라인 중복제거를 모두 사용하도록 설정하려면 명령을 실행한 후 `volume efficiency modify` 옵션으로 `true` 명령을 `-inline-deduplication` 사용합니다 `volume efficiency on`. 에 대한 자세한 내용은 `volume efficiency modify` "ONTAP 명령 참조입니다"을 참조하십시오.

  다음 명령을 실행하면 볼륨 VolA에서 사후 처리 중복제거 및 인라인 중복제거가 모두 활성화됩니다.

  'vserver vs1-volume vola의 볼륨 효율성'

  '볼륨 효율성 수정 - vserver vs1-volume vola-inline-dedupe true'

- 'volume Efficiency on' 명령과 'volume Efficiency modify' 명령을 차례로 사용하고 '-inline-deduplication' 옵션을 true로 설정하고 '-policy' 옵션을 'inline-only'로 설정하여 인라인 중복 제거만 활성화합니다.

  다음 명령을 실행하면 볼륨 VolA에서 인라인 중복제거만 활성화됩니다.

  'vserver vs1-volume vola의 볼륨 효율성'

  '볼륨 효율성 수정 - vserver vs1-volume vola-policy inline-only-inline-dedupe true'

작업을 마친 후

볼륨 효율성 설정인 '볼륨 효율성 표시 인스턴스'를 확인하여 설정이 변경되었는지 확인합니다

에 대한 자세한 내용은 `volume efficiency show -instance` "ONTAP 명령 참조입니다"을 참조하십시오.

볼륨에서 중복 제거를 해제합니다

사후 처리 중복제거 및 인라인 중복제거는 볼륨에 독립적으로 비활성화할 수 있습니다.

시작하기 전에

현재 볼륨에서 활성화되어 있는 볼륨 효율성 작업('볼륨 효율성 중지')을 중지합니다

에 대한 자세한 내용은 `volume efficiency stop` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

볼륨에 데이터 압축이 활성화되어 있는 경우 `volume efficiency off` 명령을 실행하면 데이터 압축이 비활성화됩니다. 에 대한 자세한 내용은 `volume efficiency off` "ONTAP 명령 참조입니다"을 참조하십시오.

선택

- 'volume Efficiency off' 명령을 사용하면 후처리 중복 제거와 인라인 중복 제거를 모두 비활성화할 수 있습니다.

  다음 명령을 실행하면 볼륨 VolA에서 사후 처리 중복제거 및 인라인 중복제거가 모두 비활성화됩니다.

  '볼륨 효율성 꺼짐 - vserver vs1 - 볼륨 VolA'

- 후처리 중복 제거를 비활성화하려면 '-policy' 옵션을 '인라인만'으로 설정하고 '볼륨 효율성 수정' 명령을 사용하십시오. 하지만 인라인 중복제거는 계속 사용할 수 있습니다.

  다음 명령을 실행하면 사후 처리 중복제거가 비활성화되지만 볼륨 VolA에서는 인라인 중복제거가 계속 활성화되어 있습니다.

  '볼륨 효율성 수정 - vserver vs1-volume vola-policy inline-only'

- 인라인 중복 제거만 비활성화하려면 '-inline-deduplication' 옵션을 'false'로 설정한 상태에서 'volume Efficiency modify' 명령을 사용합니다.

  다음 명령을 실행하면 볼륨 VolA에서 인라인 중복제거만 해제됩니다.

  '볼륨 효율성 수정 - vserver vs1-volume vola-inline-deduplication false'

  에 대한 자세한 내용은 `volume efficiency modify` "ONTAP 명령 참조입니다"을 참조하십시오.

AFF 시스템의 볼륨 레벨 자동 백그라운드 중복 제거

ONTAP 9.3부터는 사전 정의된 을 사용하여 볼륨 레벨 백그라운드 중복제거를 자동으로 실행하도록 구성할 수 있습니다 `auto` AFF 정책: 스케줄을 수동으로 구성할 필요가 없습니다. 를 클릭합니다 `auto` 정책은 백그라운드에서 지속적인 중복 제거를 수행합니다.

를 클릭합니다 `auto` 정책은 새로 생성된 모든 볼륨과 백그라운드 중복 제거를 위해 수동으로 구성되지 않은 모든 업그레이드된 볼륨에 대해 설정됩니다. 가능합니다 "정책을 변경합니다" 를 선택합니다 `default` 또는 기능을 사용하지 않도록 설정하는 다른 정책입니다.

볼륨이 비 AFF 시스템에서 AFF 시스템으로 이동하는 경우 기본적으로 타겟 노드에서 '자동' 정책이 설정됩니다. 볼륨이 AFF 노드에서 비 AFF 노드로 이동하는 경우 대상 노드의 자동 정책은 기본적으로 '인라인 전용' 정책으로 대체됩니다.

AFF에서 시스템은 '자동' 정책이 있는 모든 볼륨을 모니터링하고 절약 효과가 적거나 자주 덮어쓰기가 발생하는 볼륨의 우선 순위를 정하지 않습니다. 우선 순위가 제거된 볼륨은 더 이상 자동 백그라운드 중복제거에 포함되지 않습니다. 우선 순위가 지정되지 않는 볼륨의 변경 로깅이 비활성화되고 볼륨의 메타데이터가 잘립니다.

사용자는 고급 권한 레벨에서 제공되는 '볼륨 효율성 프로모션' 명령을 사용하여 우선 순위가 제거된 볼륨을 승격하여 자동 백그라운드 중복 제거에 다시 참여할 수 있습니다.

에 대한 자세한 내용은 `volume efficiency promote` "ONTAP 명령 참조입니다"을 참조하십시오.

AFF 시스템에서 애그리게이트 레벨의 인라인 중복제거를 관리합니다

Aggregate 레벨의 데이터 중복 제거를 통해 동일한 애그리게이트에 속한 볼륨 전체에서 중복 블록을 제거할 수 있습니다. AFF 시스템에서는 집계 수준 중복 제거를 인라인으로 수행할 수 있습니다. 이 기능은 새로 생성된 모든 볼륨과 볼륨 인라인 중복제거가 활성화되어 있는 모든 업그레이드된 볼륨에 대해 기본적으로 활성화됩니다.

이 작업에 대해

중복제거 작업은 디스크에 데이터를 쓰기 전에 중복 블록을 제거합니다. '속도 보장'이 '없음'으로 설정된 볼륨만 집계 수준 인라인 데이터 중복 제거에 참여할 수 있습니다. AFF 시스템의 기본 설정입니다.

애그리게이트 레벨 인라인 중복제거는 교차 볼륨 인라인 중복제거라고도 합니다.

단계

1. AFF 시스템에서 애그리게이트 레벨의 인라인 중복제거 관리

원하는 작업	이 명령을 사용합니다
애그리게이트 레벨 인라인 중복제거 지원	'볼륨 효율성 수정 - vserver vserver_name - volume vol_name - cross-volume-inline-dedupe true'
애그리게이트 레벨 인라인 중복제거를 사용하지 않도록 설정합니다	'볼륨 효율성 수정 - vserver vserver_name - volume vol_name - cross-volume-inline-dedupe FALSE'
애그리게이트 레벨의 인라인 중복제거 상태를 표시합니다	'볼륨 효율성 구성 - 볼륨 vol_name'

예

다음 명령을 실행하면 애그리게이트 레벨 인라인 중복제거 상태가 표시됩니다.

```
wfit-8020-03-04::> volume efficiency config -volume choke0_wfit_8020_03_0
Vserver:                                        vs0
Volume:                                         choke0_wfit_8020_03_0
Schedule:                                       -
Policy:                                         choke_VE_policy
Compression:                                    true
Inline Compression:                             true
Inline Dedupe:                                  true
Data Compaction:                                true
Cross Volume Inline Deduplication:              false
```

AFF 시스템에서 애그리게이트 레벨의 백그라운드 중복제거를 관리합니다

Aggregate 레벨의 데이터 중복 제거를 통해 동일한 애그리게이트에 속한 볼륨 전체에서 중복 블록을 제거할 수 있습니다. ONTAP 9.3부터는 AFF 시스템의 백그라운드에서 애그리게이트 레벨의 중복제거를 수행할 수 있습니다. 이 기능은 새로 생성된 모든 볼륨과 볼륨 백그라운드 중복제거가 활성화되어 있는 모든 업그레이드된 볼륨에 대해 기본적으로 활성화됩니다.

이 작업에 대해

변경 로그의 비율이 충분히 채워지면 작업이 자동으로 트리거됩니다. 작업과 연결된 스케줄 또는 정책이 없습니다.

ONTAP 사용자는 AFF 9.4부터 애그리게이트 레벨의 중복제거 스캐너를 실행하여 애그리게이트 내 볼륨 전체의 기존 데이터 중복을 제거할 수도 있습니다. '-scan-old-data=true' 옵션과 함께 'storage aggregate Efficiency cross-volume-dedupe start' 명령을 사용하여 스캐너를 시작할 수 있습니다.

```
cluster-1::> storage aggregate efficiency cross-volume-dedupe start
-aggregate aggr1 -scan-old-data true
```

중복 제거 스캔에 시간이 많이 걸릴 수 있습니다. 사용량이 적은 시간에 작업을 실행할 수 있습니다.

Aggregate 레벨의 백그라운드 중복제거를 볼륨 간 백그라운드 중복제거라고도 합니다.

에 대한 자세한 내용은 `storage aggregate efficiency cross-volume-dedupe start` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. AFF 시스템에서 애그리게이트 레벨의 백그라운드 중복제거 관리:

원하는 작업	이 명령을 사용합니다
Aggregate 레벨의 백그라운드 중복제거를 지원합니다	'볼륨 효율성 수정 - vserver <vserver_name\> - volume <vol_name\> - cross-volume-background-dedupe true
애그리게이트 레벨의 백그라운드 중복제거를 사용하지 않도록 설정합니다	'볼륨 효율성 수정 - vserver <vserver_name\> - volume <vol_name\> - cross-volume-background-dedupe false
애그리게이트 레벨의 백그라운드 중복제거 상태를 표시합니다	'집계 효율성 교차 볼륨 - 중복 제거 표시'

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

관련 정보

- "볼륨 효율성 수정"
- "애그리게이트 효율성 볼륨 간 중복제거 표시"

ONTAP 온도 민감형 스토리지 효율성에 대해 알아보세요

ONTAP 볼륨의 데이터에 액세스하는 빈도를 평가하고 해당 빈도를 데이터에 적용된 압축 정도에 매핑하여 온도 민감형 스토리지 효율성(TSSE) 이점을 제공합니다. 자주 액세스되지 않는 콜드 데이터의 경우 더 큰 데이터 블록이 압축되고, 자주 액세스되고 더 자주 덮어쓰이는 핫 데이터의 경우 더 작은 데이터 블록이 압축되어 프로세스의 효율성이 높아집니다.

TSSE는 ONTAP 9.8에서 도입되었으며 새로 생성된 씬 프로비저닝 AFF 볼륨에서 자동으로 활성화됩니다. 기존의 씬 프로비저닝된 AFF 볼륨과 씬 프로비저닝된 비 AFF DP 볼륨에서 온도에 따른 스토리지 효율성 향상 기능을 활성화할 수 있습니다. TSSE는 고밀도 프로비저닝 볼륨에서 지원되지 않습니다.

다음 플랫폼에는 온도에 따른 저장 효율성이 적용되지 않습니다.

플랫폼	**ONTAP** 버전입니다
• AFF A1K 를 참조하십시오 • AFF A90 를 참조하십시오 • AFF A70 를 참조하십시오 • FAS90를 참조하십시오 • FAS70를 참조하십시오	9.15.1 이상
• AFF C80 를 참조하십시오 • AFF C60 를 참조하십시오 • AFF C30 를 참조하십시오 • AFF A50 를 참조하십시오 • AFF A30 를 참조하십시오	9.16.1 이상

이 플랫폼은 다음을 사용합니다."CPU 또는 전용 오프로드 프로세서 스토리지 효율성" . 압축은 메인 CPU나 전용 오프로드 프로세서를 사용하여 수행되며 핫 데이터나 콜드 데이터에 기반하지 않습니다.

시간이 지남에 따라 볼륨에서 사용되는 공간의 양은 8K 적응형 압축에 비해 TSSE에서 더 두드러질 수 있습니다. 이러한 동작은 TSSE와 8K 적응형 압축 간의 아키텍처 차이로 인해 예상됩니다.

"기본" 및 "효율적인" 모드 도입

ONTAP 9.10.1부터 _default_and_efficient_볼륨 수준 스토리지 효율성 모드는 AFF 시스템에만 도입되었습니다. 두 가지 모드를 통해 파일 압축(기본값) 중에서 선택할 수 있으며, 새 AFF 볼륨을 생성할 때의 기본 모드인 파일 압축(기본값) 또는 온도에 민감한 스토리지 효율성(효율적) 중에서 선택할 수 있습니다. 이 방식은 자동 적응형 압축을 사용하여 자주 액세스하지 않는 콜드 데이터에 대해 압축 절약 효과를 높입니다.

ONTAP 9.10.1 이상으로 업그레이드할 때 볼륨에 현재 활성화된 압축 유형을 기준으로 기존 볼륨에 스토리지 효율성 모드가 할당됩니다. 업그레이드하는 동안 압축이 활성화된 볼륨에 기본 모드가 할당되고, 온도에 민감한 스토리지 효율성을 활성화한 볼륨에 효율적인 모드가 할당됩니다. 압축이 사용되지 않을 경우 스토리지 효율성 모드는 빈 상태로 유지됩니다.

ONTAP 9.10.1"온도에 민감한 스토리지 효율성을 명시적으로 설정해야 합니다"을 사용하여 자동 적응형 압축을 활성화합니다. 하지만 AFF 플랫폼에서 데이터 컴팩션, 자동 중복제거 일정, 인라인 중복제거, 볼륨 간 인라인 중복제거,

볼륨 간 백그라운드 중복제거 등과 같은 기타 스토리지 효율성 기능은 기본 모드와 효율적인 모드 모두에서 기본적으로 사용됩니다.

FabricPool 지원 애그리게이트 및 모든 계층화 정책 유형에서 스토리지 효율성 모드(기본값 및 효율성)가 모두 지원됩니다.

C-Series 플랫폼에서 온도에 민감한 스토리지 효율성을 지원합니다

온도에 민감한 스토리지 효율성(TSSE)은 AFF C-Series 플랫폼에서 기본적으로 활성화되며, 대상 플랫폼에 다음 릴리스가 설치된 상태에서 볼륨 이동 또는 SnapMirror 사용하여 TSSE가 활성화되지 않은 플랫폼에서 TSSE가 활성화된 C-Series 플랫폼으로 씬 프로비저닝된 볼륨을 마이그레이션할 때도 활성화됩니다.

- ONTAP 9.12.1P4 이상
- ONTAP 9.13.1 이상

자세한 내용은 을 "볼륨 이동 및 SnapMirror 작업에 대한 스토리지 효율성 동작"참조하십시오.

기존의 씬 프로비저닝 볼륨의 경우 온도에 민감한 스토리지 효율성이 자동으로 활성화되지 않습니다. 하지만 다음과 같이 설정할 수 있습니다. "스토리지 효율성 모드를 수정합니다" 수동으로 효율 모드로 전환하세요.

> ⓘ 스토리지 효율성 모드를 효율적으로 변경한 후에는 다시 변경할 수 없습니다.

인접한 물리적 블록을 순차적으로 압축하여 스토리지 효율성 향상

ONTAP 9.13.1 을 시작으로, 온도에 민감한 스토리지 효율성이 인접한 물리적 블록을 순차적으로 압축하여 스토리지 효율성을 더욱 향상합니다. 온도에 민감한 스토리지 효율성을 사용하는 볼륨은 시스템을 ONTAP 9.13.1 로 업그레이드할 때 자동으로 순차적 패킹을 지원합니다. 순차적 패킹이 활성화된 후에는 다음을 수행해야 "기존 데이터를 수동으로 다시 압축합니다"합니다.

볼륨 이동 및 SnapMirror 작업에 대한 스토리지 효율성 동작

스토리지 효율성의 동작은 활성 상태이거나 동시에 시작되는 다른 스토리지 작업의 영향을 받을 수 있습니다. 이러한 작업이 스토리지 효율성에 미치는 영향을 숙지해야 합니다.

볼륨 이동, SnapMirror 관계, FabricPool 볼륨 및 를 비롯한 다른 작업으로 인해 볼륨의 스토리지 효율성이 영향을 받을 수 있는 몇 가지 상황이 "온도에 민감한 스토리지 효율성(TSSE)"있습니다.

FabricPool

`all`계층화 정책은 데이터 보호 볼륨에 일반적으로 데이터를 즉시 사용 콜드 데이터로 표시하고 가능한 한 빨리 계층화하는 데 사용됩니다. 데이터가 콜드 및 계층화되기 전에 최소 일 수가 경과할 때까지 기다릴 필요가 없습니다.

계층화 정책은 가능한 한 빨리 데이터를 계층화하므로 `all` 32K 효율적인 적응형 압축(TSSE)과 같이 백그라운드 프로세스를 활용하는 스토리지 효율성을 적용할 시간이 충분하지 않습니다. 8K 압축과 같은 인라인 스토리지 효율성이 정상적으로 적용됩니다.

다음 표에서는 이러한 작업 중 하나를 수행할 때 소스 볼륨과 대상 볼륨의 동작을 설명합니다.

소스 볼륨 효율성	대상 볼륨 기본 동작입니다			TSSE를 수동으로 활성화한 후의 기본 동작(SnapMirror 중단 후)		
	* 스토리지 효율성 유형 *	* 새 쓰기 *	* 콜드 데이터 압축 *	* 스토리지 효율성 유형 *	* 새 쓰기 *	* 콜드 데이터 압축 *
스토리지 효율성 없음(FAS 가능성 높음)	파일 압축	새로 쓴 데이터에 대해 파일 압축이 인라인으로 시도됩니다	콜드 데이터 압축이 없으며 데이터가 있는 그대로 유지됩니다	콜드 데이터 스캔 알고리즘을 ZSTD로 사용하는 TSSE	8K 인라인 압축이 TSSE 형식으로 시도됩니다	* 파일 압축 데이터 *:N/A를 누릅니다 * 비압축 데이터 *: 임계값 일 충족 후 시도한 32K 압축를 누릅니다 * 새로 작성된 데이터 *: 임계값 일 이후에 시도된 32K 압축
스토리지 효율성 없음(FAS 가능성 높음)	ONTAP 9.11.1P10 또는 ONTAP 9.12.1P3을 사용하는 C 시리즈 플랫폼의 파일 압축	TSSE 사용 콜드 데이터 압축이 없습니다	* 파일 압축 데이터 *:N/A	콜드 데이터 스캔 알고리즘을 ZSTD로 사용하는 TSSE	8K 인라인 압축	* 파일 압축 데이터 *:N/A를 누릅니다 * 비압축 데이터 *: 임계값 일 충족 후 시도한 32K 압축를 누릅니다 * 새로 작성된 데이터 *: 임계값 일 이후에 시도된 32K 압축
스토리지 효율성 없음(FAS 가능성 높음)	ONTAP 9.12.1P4 이상 또는 ONTAP 9.13.1 이상을 사용하는 C 시리즈 플랫폼의 TSSE	8K 인라인 압축이 TSSE 형식으로 시도됩니다	* 파일 압축 데이터 *:N/A를 누릅니다 * 비압축 데이터 *: 임계값 일 충족 후 시도한 32K 압축를 누릅니다 * 새로 작성된 데이터 *: 임계값 일 이후에 시도된 32K 압축	콜드 데이터 스캔 알고리즘을 ZSTD로 사용하는 TSSE	8K 인라인 압축이 TSSE 형식으로 시도됩니다	* 파일 압축 데이터 *:N/A를 누릅니다 * 비압축 데이터 *: 임계값 일 충족 후 시도한 32K 압축를 누릅니다 * 새로 작성된 데이터 *: 임계값 일 이후에 시도된 32K 압축
파일 압축 그룹	소스와 동일합니다	새로 쓴 데이터에 대해 파일 압축이 인라인으로 시도됩니다	콜드 데이터 압축이 없으며 데이터가 있는 그대로 유지됩니다	콜드 데이터 스캔 알고리즘을 ZSTD로 사용하는 TSSE	8K 인라인 압축이 TSSE 형식으로 시도됩니다	* 파일 압축 데이터 *: 압축되지 않음를 누릅니다 * 비압축 데이터 *: 임계값 일이 충족된 후 32K 압축이 시도됩니다를 누릅니다 * 새로 작성된 데이터 *: 임계값 일이 충족된 후 32K 압축이 시도됩니다

TSSE 콜드 데이터 스캔	소스 볼륨과 동일한 압축 알고리즘을 사용하는 TSSE(LZOPro → LZOPro 및 ZSTD → ZSTD)	TSSE 형식에서 8K 인라인 압축을 시도했습니다	기존 데이터와 새로 작성된 데이터 모두에 대해 임계값 일 기반 대기가 완료된 후 LzoPro에서 시도한 32K 압축.	TSSE가 활성화되었습니다. 참고: LZOPro 콜드 데이터 스캔 알고리즘은 ZSTD로 변경할 수 있습니다.	8K 인라인 압축이 TSSE 형식으로 시도됩니다	기존 데이터와 새로 작성된 데이터 모두에 대해 임계값 일수를 충족한 후 32K 압축을 시도합니다.

볼륨 생성 중에 스토리지 효율성 모드를 설정합니다

ONTAP 9.10.1부터 새 AFF 볼륨을 생성할 때 스토리지 효율성 모드를 설정할 수 있습니다.

이 작업에 대해

매개변수를 사용하여 새 AFF 볼륨의 저장 효율성 모드를 제어할 수 있습니다. `-storage-efficiency-mode`. 저장 효율성 모드를 설정하려면 두 가지 옵션 중에서 선택할 수 있습니다. `default` 또는 `efficient`. 선택하는 저장 효율성 모드는 볼륨에서 더 높은 성능을 원하는지, 더 높은 저장 효율성을 원하는지에 따라 달라집니다. 매개변수 `-storage-efficiency-mode` AFF 아닌 볼륨이나 데이터 보호 볼륨에서는 지원되지 않습니다.

저장 효율성을 높여 새로운 AFF 볼륨을 생성하면 기본적으로 성능 모드가 설정됩니다.

"온도에 민감한 스토리지 효율성 및 스토리지 효율성 모드에 대해 자세히 알아보십시오"..

단계

1. 새 볼륨을 만들고 효율성 모드를 설정합니다.

```
volume create -vserver <vserver name> -volume <volume name> -aggregate
<aggregate name> -size <volume size> -storage-efficiency-mode
<efficient|default>
```

세트 `-storage-efficiency-mode` 에게 `efficient` 효율성 모드 또는 `default` 성능 모드용.

다음 예에서는 aff_vol1이 효율성 모드로 생성됩니다.

```
volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1 -storage
-efficiency-mode efficient -size 10g
```

ONTAP에서 볼륨 비활성 데이터 압축 임계값을 변경합니다

온도에 민감한 스토리지 효율성을 사용하여 볼륨에 대한 효율성 임계값을 수정하여 ONTAP이 콜드 데이터 스캔을 수행하는 빈도를 변경할 수 있습니다.

시작하기 전에

클러스터 또는 SVM 관리자여야 하며 ONTAP CLI 고급 권한 수준을 사용해야 합니다.

이 작업에 대해

감기 임계값은 1일에서 60일 사이의 값일 수 있습니다. 기본 임계값은 14일입니다.

단계

1. 권한 수준 설정:

   세트 프리빌리지 고급

2. 볼륨에 대한 비활성 데이터 압축 수정:

   ```
   volume efficiency inactive-data-compression modify -vserver <vserver_name>
   -volume <volume_name> -threshold-days <integer>
   ```

에 대한 자세한 내용은 `volume efficiency inactive-data-compression modify` "ONTAP 명령 참조입니다"을 참조하십시오.

볼륨 효율성 모드를 확인합니다

AFF 볼륨에서 'volume-Efficiency-show' 명령을 사용하여 효율성이 설정되었는지 확인하고 현재 효율성 모드를 확인할 수 있습니다.

단계

1. 볼륨의 효율성 모드를 확인합니다.

   ```
   volume efficiency show -vserver <vserver name> -volume <volume name> -fields
   storage-efficiency-mode
   ```

에 대한 자세한 내용은 `volume efficiency show` "ONTAP 명령 참조입니다"을 참조하십시오.

볼륨 효율성 모드를 변경합니다

ONTAP 9.10.1부터 볼륨 수준 스토리지 효율성 모드인 *default* 및 _efficient_는 AFF 시스템에서만 지원됩니다. 이러한 모드는 파일 압축(기본값) 또는 온도 감응형 스토리지 효율성(효율적) 중에서 선택할 수 있도록 합니다. 파일 압축은 새 AFF 볼륨을 생성할 때 기본 모드이며, 효율적 모드는 온도 감응형 스토리지 효율성(TSSE)을 활성화합니다.

TSSE는 씬 프로비저닝된 볼륨에서만 지원됩니다. "TSSE에 대해 자세히 알아보세요".

단계

ONTAP 시스템 관리자 또는 ONTAP CLI를 사용하여 이 작업을 수행할 수 있습니다.

시스템 관리자

ONTAP 9.10.1부터, 온도에 민감한 스토리지 효율성 기능을 사용하여 시스템 관리자를 사용하여 스토리지 효율성을 높일 수 있습니다. 성능 기반 스토리지 효율성은 기본적으로 활성화되어 있습니다.

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 스토리지 효율성을 설정하거나 해제할 볼륨을 찾은 다음 을 클릭합니다 ⋮.
3. Edit > Volumes * 를 클릭하고 * Storage Efficiency * 로 스크롤합니다.
4. Enable 상위 스토리지 효율성 * 을 선택합니다.

CLI를 참조하십시오

당신은 사용할 수 있습니다 `volume efficiency modify` AFF 볼륨의 저장 효율성 모드를 변경하는 명령 `default` 에게 `efficient`또는 볼륨 효율성이 아직 설정되지 않은 경우 효율성 모드를 설정할 수 있습니다.

1. 볼륨 효율성 모드를 변경합니다.

```
volume efficiency modify -vserver <vserver name> -volume <volume
name> -storage-efficiency-mode <default|efficient>
```

에 대한 자세한 내용은 `volume efficiency modify` "ONTAP 명령 참조입니다"을 참조하십시오.

온도에 민감한 스토리지 효율성 유무에 관계없이 볼륨 설치 공간을 절약할 수 있습니다

ONTAP 릴리즈에 따라 각 볼륨의 물리적인 설치 공간 절약 효과를 확인할 수 있습니다. 이를 통해 관리 프로세스의 효과를 평가하거나 용량 계획의 일부로 평가할 수 있습니다.

이 작업에 대해

ONTAP 9.11.1부터 명령을 사용하여 `volume show-footprint` 온도에 민감한 스토리지 효율성(TSSE)을 활성화한 상태에서 볼륨의 물리적 설치 공간 절약 효과를 확인할 수 있습니다. ONTAP 9.13.1부터 동일한 명령을 사용하여 TSSE가 활성화되지 않은 볼륨의 물리적 설치 공간 절약 효과를 볼 수 있습니다.

단계

1. 볼륨 설치 공간 절감 보기:

```
volume show-footprint
```

TSSE가 활성화된 경우의 출력 예

```
Vserver : vs0
Volume  : vol_tsse_75_per_compress

Feature                                    Used       Used%
--------------------------------        ----------    -----
Volume Data Footprint                      10.15GB       13%
Volume Guarantee                               0B        0%
Flexible Volume Metadata                   64.25MB        0%
Delayed Frees                              235.0MB        0%
File Operation Metadata                        4KB        0%

Total Footprint                            10.45GB       13%

Footprint Data Reduction                    6.85GB        9%
     Auto Adaptive Compression              6.85GB        9%
Effective Total Footprint                   3.59GB        5%
```

TSSE가 활성화되지 않은 경우의 출력 예

```
Vserver : vs0
Volume  : vol_file_cg_75_per_compress

Feature                                    Used       Used%
--------------------------------        ----------    -----
Volume Data Footprint                       5.19GB        7%
Volume Guarantee                               0B        0%
Flexible Volume Metadata                   32.12MB        0%
Delayed Frees                              90.17MB        0%
File Operation Metadata                        4KB        0%

Total Footprint                             5.31GB        7%

Footprint Data Reduction                    1.05GB        1%
     Data Compaction                        1.05GB        1%
Effective Total Footprint                   4.26GB        5%
```

관련 정보

- "볼륨 생성 중에 스토리지 효율성 모드를 설정합니다"

볼륨에 대해 데이터 압축을 설정합니다

FlexVol volume에서 데이터 압축을 활성화하면 명령을 사용하여 공간을 절약할 수 있습니다. `volume efficiency modify` 기본 압축 유형을 사용하지 않으려면 볼륨에 압축 유형을

할당할 수도 있습니다. 에 대한 자세한 내용은 `volume efficiency modify` "ONTAP 명령 참조입니다"을 참조하십시오.

시작하기 전에

볼륨에 대해 중복 제거를 설정해야 합니다.

- 중복 제거는 활성화만 필요하며 볼륨에서는 실행할 필요가 없습니다.
- 압축 스캐너는 AFF 플랫폼에 있는 볼륨의 기존 데이터를 압축하는 데 사용해야 합니다.

"볼륨에 대해 중복 제거를 설정합니다"

이 작업에 대해

- HDD 애그리게이트 및 Flash Pool 애그리게이트에서는 인라인 압축과 사후 처리 압축을 모두 활성화하거나 볼륨에 대해 사후 처리 압축만 활성화할 수 있습니다.

  둘 다 설정하는 경우 인라인 압축을 활성화하기 전에 볼륨에 대해 사후 처리 압축을 활성화해야 합니다.

- AFF 플랫폼에서는 인라인 압축만 지원됩니다.

  인라인 압축을 활성화하기 전에 볼륨에 대해 사후 처리 압축을 활성화해야 합니다. 그러나 후처리 압축은 AFF 플랫폼에서 지원되지 않으므로 사후 처리 압축은 해당 볼륨에 대해 발생하지 않으며 EMS 메시지가 생성되어 사후 처리 압축을 건너뛰었음을 알립니다.

- 온도에 민감한 스토리지 효율성은 ONTAP 9.8에 도입되었습니다. 이 기능을 사용하면 데이터가 핫 데이터인지 콜드 데이터인지에 따라 스토리지 효율성이 적용됩니다. 콜드 데이터의 경우 대용량 데이터 블록이 압축되며, 자주 덮어쓰는 핫 데이터의 경우 작은 데이터 블록이 압축되어 프로세스가 더 효율적입니다. 온도에 민감한 스토리지 효율성은 새로 생성된 씬 프로비저닝된 AFF 볼륨에서 자동으로 활성화됩니다.
- 압축 유형은 애그리게이트의 플랫폼을 기반으로 자동으로 할당됩니다.

플랫폼/애그리게이트	압축 유형입니다
AFF	적응형 압축
Flash Pool 애그리게이트로 전환 가능	적응형 압축
HDD 애그리게이트	보조 압축

선택

- 기본 압축 유형을 사용하여 데이터 압축을 활성화하려면 '볼륨 효율성 수정' 명령을 사용하십시오.

  다음 명령을 실행하면 SVM VS1 볼륨의 사후 처리 압축이 활성화됩니다.

  '볼륨 효율성 수정 - vserver vs1-volume vola-compression TRUE'

  다음 명령을 실행하면 SVM VS1 볼륨의 볼륨 VolA에서 사후 처리 및 인라인 압축이 모두 활성화됩니다.

  '볼륨 효율성 수정 - vserver vs1-volume vola-compression true-inline-compression true'

- 고급 권한 수준에서 '볼륨 효율성 수정' 명령을 사용하여 특정 압축 유형의 데이터 압축을 활성화할 수 있습니다.

  a. Set-Privilege advanced 명령을 사용하여 권한 수준을 Advanced로 변경합니다.

  b. 'volume Efficiency modify' 명령을 사용하여 볼륨에 압축 유형을 할당합니다.

     다음 명령은 사후 처리 압축을 활성화하고 SVM VS1 의 볼륨 볼에 적응형 압축 유형을 할당합니다.

     '볼륨 효율성 수정 - vserver vs1-volume vola-compression true-compression-type adaptive'

     다음 명령을 실행하면 사후 처리 및 인라인 압축이 모두 설정되고 적응형 압축 유형이 SVM VS1 볼륨의 VolA에 할당됩니다.

  '볼륨 효율성 수정 - vserver vs1-volume vola-compression true-compression-type adaptive-inline-compression true'

  a. 권한 수준을 admin으로 변경하려면 'Set-Privilege admin' 명령을 사용합니다.

보조 압축과 적응형 압축 간에 이동

데이터 읽기의 양에 따라 보조 압축과 적응형 압축 간에 전환할 수 있습니다. 시스템에서 대량의 랜덤 읽기가 수행되는 경우 적응형 압축이 더 높은 성능이 필요합니다. 2차 압축은 데이터를 순차적으로 쓸 때 더 높은 압축 절약 효과가 필요한 경우에 적합합니다.

이 작업에 대해

기본 압축 유형은 애그리게이트 및 플랫폼을 기반으로 선택됩니다.

단계

1. 볼륨의 효율성 비활성화:

   ```
   volume efficiency off
   ```

   예를 들어, 다음 명령을 실행하면 볼륨 vol1의 효율성이 비활성화됩니다.

   ```
   volume efficiency off -vserver vs1 -volume vol1
   ```

2. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

3. 압축 데이터의 압축을 풉니다.

   볼륨 효율성 실행 취소

   예를 들어, 다음 명령은 볼륨 vol1에서 압축된 데이터를 압축 해제합니다.

   '볼륨 효율성 실행 취소 - vserver vs1-volume vol1-compression TRUE'

   ⓘ 압축 해제된 데이터를 수용할 수 있는 충분한 공간이 볼륨에 있는지 확인해야 합니다.

4. 관리자 권한 레벨로 변경:

'Set-Privilege admin'입니다

5. 작업 상태가 IDLE인지 확인합니다.

   볼륨 효율성 쇼

   예를 들어, 다음 명령은 볼륨 vol1에 대한 효율성 작업의 상태를 표시합니다.

   '볼륨 효율성 표시 - vserver vs1-volume vol1'

6. 볼륨의 효율성 지원:

   `volume efficiency on` 예를 들어, 다음 명령을 사용하면 볼륨 vol1의 효율성이 활성화됩니다.

   ```
   volume efficiency on -vserver vs1 -volume vol1
   ```

7. 데이터 압축을 사용하도록 설정한 다음 압축 유형을 설정합니다.

   볼륨 효율성 수정

   예를 들어, 다음 명령을 실행하면 데이터 압축이 활성화되고 압축 유형이 볼륨 vol1에서 보조 압축으로 설정됩니다.

   '볼륨 효율성 수정 - vserver vs1-volume vol1-compression true-compression-type secondary'

   > 이 단계에서는 볼륨에 대한 보조 압축만 활성화합니다. 볼륨의 데이터는 압축되지 않습니다.
   >
   > - AFF 시스템에서 기존 데이터를 압축하려면 백그라운드 압축 검사기를 실행해야 합니다.
   > - Flash Pool 애그리게이트 또는 HDD 애그리게이트에서 기존 데이터를 압축하려면 백그라운드 압축을 실행해야 합니다.

8. 선택 사항: 인라인 압축 사용:

   볼륨 효율성 수정

   예를 들어, 다음 명령을 실행하면 볼륨 vol1에 대해 인라인 압축이 활성화됩니다.

   '볼륨 효율성 수정 - vserver vs1-volume vol1-inline-compression TRUE'

볼륨에 대한 데이터 압축을 비활성화합니다

명령을 사용하여 볼륨에 대해 데이터 압축을 사용하지 않도록 설정할 수 `volume efficiency modify` 있습니다. 에 대한 자세한 내용은 `volume efficiency modify` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

사후 압축 기능을 비활성화하려면 먼저 볼륨에 대해 인라인 압축을 비활성화해야 합니다.

단계

1. 현재 볼륨에서 활성화되어 있는 볼륨 효율성 작업을 중지합니다.

볼륨 효율성 중지

2. 데이터 압축 해제:

   볼륨 효율성 수정

   압축된 기존 데이터가 볼륨에 압축된 상태로 남아 있습니다. 볼륨에 들어오는 새 쓰기만 압축되지 않습니다.

예

다음 명령을 실행하면 볼륨 VolA에 대한 인라인 압축이 비활성화됩니다.

'볼륨 효율성 수정 - vserver vs1-volume vola-inline-compression false'

다음 명령을 실행하면 볼륨 VolA에 대해 사후 처리 압축 및 인라인 압축이 모두 비활성화됩니다.

'볼륨 효율성 수정 - vserver vs1-volume vola-compression false-inline-compression false'

에 대한 자세한 내용은 `volume efficiency stop` "ONTAP 명령 참조입니다"을 참조하십시오.

AFF 시스템의 인라인 데이터 컴팩션을 관리합니다

'볼륨 효율성 수정' 명령을 사용하여 볼륨 레벨에서 AFF 시스템의 인라인 데이터 컴팩션을 제어할 수 있습니다. AFF 시스템의 모든 볼륨에 대해 데이터 컴팩션이 기본적으로 활성화됩니다.

시작하기 전에

데이터 컴팩션에서는 볼륨 공간 보장이 "없음"으로 설정되어 있어야 합니다. AFF 시스템의 기본값입니다.

비 AFF 데이터 보호 볼륨의 기본 공간 보장은 없음으로 설정됩니다.

단계

1. 볼륨에 대한 공간 보장 설정을 확인하려면 다음을 수행하십시오.

   'volume show -vserver vserver_name -volume volume_name –fields space-보증

2. 데이터 컴팩션을 활성화하려면:

   '볼륨 효율성 수정 - vserver vserver_name - volume volume_name - data-다짐 TRUE

3. 데이터 컴팩션을 사용하지 않도록 설정하려면 다음을 따르십시오.

   '볼륨 효율성 수정 - vserver vserver_name - volume volume_name - data-다짐 FALSE

4. 데이터 컴팩션 상태를 표시하려면 다음을 수행합니다.

   '볼륨 효율성 표시 인스턴스'

예

'cluster1::> 볼륨 효율성 수정 - vserver vs1-volume vol1-data-comp컴팩션 TRUE"cluster1::> 볼륨 효율성 수정 - vserver vs1-volume vol1-data-comp컴팩션 FALSE'

FAS 시스템에 대해 인라인 데이터 컴팩션을 사용하도록 설정합니다

1. 클러스터 셸 명령을 사용하여 볼륨 수준에서 Flash Pool(하이브리드) 애그리게이트 또는 HDD 애그리게이트가 포함된 FAS 시스템에서 인라인 데이터 컴팩션을 설정할 수 있습니다 `volume efficiency`. FAS 시스템에 생성된 볼륨에 대해 데이터 컴팩션은 기본적으로 비활성화되어 있습니다. 에 대한 자세한 내용은 `volume efficiency` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

볼륨에 대해 인라인 데이터 컴팩션을 활성화하려면 `-space-guarantee` 옵션을 로 설정해야 `none` 합니다. HDD 애그리게이트의 볼륨에 데이터 컴팩션을 활성화하면 추가 CPU 리소스가 사용됩니다.

단계

1. 고급 권한 레벨로 변경:

```
set -privilege advanced
```

에 대한 자세한 내용은 `set` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 원하는 노드에 대해 볼륨 및 애그리게이트의 데이터 컴팩션 상태를 확인합니다.

```
volume efficiency show -volume <volume_name>
```

에 대한 자세한 내용은 `volume efficiency show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 볼륨에 대한 데이터 컴팩션 지원:

```
volume efficiency modify -volume <volume_name> -data-compaction true
```

에 대한 자세한 내용은 `volume efficiency modify` "ONTAP 명령 참조입니다"을 참조하십시오.

> ⓘ 데이터 컴팩션이 애그리게이트 또는 볼륨에 대해 으로 설정된 경우 `false` 컴팩션이 실패합니다. 컴팩션을 사용하도록 설정하면 기존 데이터가 압축되지 않고 시스템에 대한 새로운 쓰기만 컴팩션됩니다. 이 `volume efficiency start` 명령에는 기존 데이터를 압축하는 방법에 대한 자세한 내용이 포함되어 있습니다. 에 대한 자세한 내용은 `volume efficiency start` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 컴팩션 통계를 확인합니다.

```
volume efficiency show -volume <volume_name>
```

AFF 시스템에서 기본적으로 인라인 스토리지 효율성이 활성화되어 있습니다

AFF 시스템에서 새로 생성된 모든 볼륨에 대해 스토리지 효율성 기능이 기본적으로 활성화됩니다. 모든 인라인 스토리지 효율성 기능은 모든 AFF 시스템의 모든 기존 볼륨과 새로

생성된 볼륨에서 기본적으로 활성화됩니다.

스토리지 효율성 기능에는 인라인 중복제거, 인라인 교차 볼륨 중복제거, 인라인 압축이 포함되며, 표에 나와 있는 대로 AFF 시스템에서 기본적으로 활성화됩니다.

AFF 볼륨의 데이터 압축 동작은 기본적으로 활성화되어 있습니다.

용적 조건	기본적으로 활성화된 스토리지 효율성 기능		
	인라인 중복제거	인라인 볼륨 간 중복제거	인라인 압축
클러스터 업그레이드	예	예	예
ONTAP 7-Mode를 clustered ONTAP으로 전환합니다	예	예	예
볼륨 이동	예	예	예
일반 프로비저닝된 볼륨	예	아니요	예
암호화된 볼륨	예	아니요	예

하나 이상의 인라인 스토리지 효율성 기능에는 다음 예외가 적용됩니다.

- 읽기-쓰기 볼륨만 기본 인라인 스토리지 효율성 지원을 지원할 수 있습니다.
- 압축 축소가 있는 볼륨은 인라인 압축을 활성화할 때 생략됩니다.
- 사후 처리 중복제거가 활성화된 볼륨은 인라인 압축 활성화에서 생략됩니다.
- 볼륨 효율성이 꺼져 있는 볼륨의 경우, 시스템은 기존 볼륨 효율성 정책 설정을 재정의하고 인라인 전용 정책을 사용하도록 설정합니다.

스토리지 효율성 시각화

사용하세요 `storage aggregate show-efficiency` 시스템의 모든 집계에 대한 저장 효율성에 대한 정보를 표시하는 명령입니다.

'Storage aggregate show-Efficiency' 명령에는 명령 옵션을 전달하여 호출할 수 있는 세 가지 보기가 있습니다.

자세히 알아보세요 `storage aggregate show-efficiency` 에서 "ONTAP 명령 참조입니다" .

기본 보기

기본 보기에는 각 애그리게이트의 전체 비율이 표시됩니다.

'cluster1::> storage aggregate show-Efficiency'

상세보기

'-details' 명령 옵션으로 상세도를 호출한다. 이 보기에는 다음이 표시됩니다.

- 각 애그리게이트의 전체 효율성 비율
- 스냅샷을 사용하지 않는 전체 비율입니다.
- 볼륨 중복제거, 볼륨 압축, 스냅샷, 클론, 데이터 컴팩션, 애그리게이트 인라인 중복제거 기술에 대한 비율 분할입니다.

'cluster1::> storage aggregate show-Efficiency-details'

고급 보기

고급 보기는 상세 보기와 유사하며 논리적 및 물리적 사용 세부 정보를 모두 표시합니다.

고급 권한 수준에서 이 명령을 실행해야 합니다. Set-Privilege advanced 명령을 사용하여 Advanced 권한으로 전환합니다.

명령 프롬프트가 **'cluster**

*>'로 바뀝니다.

'cluster1::> set-Privilege advanced'

'-advanced' 명령 옵션으로 고급 보기를 호출합니다.

'cluster1

* > storage aggregate show-Efficiency-advanced'

단일 Aggregate의 비율을 보려면 '-aggregate_aggregate_name_' 명령을 개별적으로 호출합니다. 이 명령은 admin 레벨 및 advanced 권한 레벨에서 실행할 수 있습니다.

'cluster1::> storage aggregate show-Efficiency-aggregate aggr1'

에 대한 자세한 내용은 `set -privilege advanced` "ONTAP 명령 참조입니다"을 참조하십시오.

효율성 작업을 실행할 볼륨 효율성 정책을 생성합니다

볼륨 효율성 정책을 생성합니다

특정 기간 동안 볼륨에 대해 중복제거 또는 데이터 압축을 실행한 후 볼륨 효율성 정책을 생성하고 '볼륨 효율성 정책 생성' 명령을 사용하여 작업 일정을 지정할 수 있습니다.

시작하기 전에

명령을 사용하여 cron 일정을 만들어야 `job schedule cron create` 합니다. cron 일정 관리에 대한 자세한 내용은 을 "시스템 관리 참조"참조하십시오. 에 대한 자세한 내용은 `job schedule cron create` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

기본 사전 정의된 역할을 가진 SVM 관리자는 중복제거 정책을 관리할 수 없습니다. 그러나 클러스터 관리자는 맞춤형 역할을 사용하여 SVM 관리자에게 할당된 권한을 수정할 수 있습니다. SVM 관리자 기능에 대한 자세한 내용은 를 참조하십시오 "관리자 인증 및 RBAC".

예약된 시간에 중복제거 또는 데이터 압축 작업을 실행하거나, 특정 기간으로 스케줄을 생성하거나, 새 데이터가 임계값을 초과할 때까지 대기하는 임계값 비율을 지정한 다음 중복제거 또는 데이터 압축 작업을 트리거할 수 있습니다. 이 임계값은 볼륨에서 사용된 총 블록 수의 백분율입니다. 예를 들어, 볼륨에 사용된 총 블록 수가 50%일 때 볼륨에 대한 임계값을 20%로 설정하면 볼륨에 기록된 새 데이터가 10%(사용된 50% 블록의 20%)에 도달하면 데이터 중복제거 또는 데이터 압축이 자동으로 트리거됩니다. 필요한 경우 에서 사용되는 총 블록 수를 얻을 수 있습니다 `df` 명령 출력.

단계

1. 'volume Efficiency policy create' 명령을 사용하여 볼륨 효율성 정책을 생성합니다.

예

다음 명령을 실행하면 효율성 작업을 매일 트리거하는 pol1이라는 볼륨 효율성 정책이 생성됩니다.

'볼륨 효율성 정책 생성 - vserver vs1-policy pol1-schedule daily'

다음 명령을 실행하면 임계값 비율이 20%에 도달할 때 효율성 작업을 트리거하는 pol2 라는 볼륨 효율성 정책이 생성됩니다.

'볼륨 효율성 정책 생성 - vserver vs1-policy pol2-type threshold-start-threshold - percent 20%'

에 대한 자세한 내용은 `volume efficiency policy create` "ONTAP 명령 참조입니다"을 참조하십시오.

볼륨에 볼륨 효율성 정책을 할당합니다

`volume efficiency modify`명령을 사용하여 중복제거 또는 데이터 압축 작업을 실행할 효율성 정책을 볼륨에 할당할 수 있습니다.

시작하기 전에

다음을 확인하십시오 "볼륨 효율성 정책을 생성합니다" 볼륨에 할당하기 전에

이 작업에 대해

효율성 정책이 SnapVault 2차 볼륨에 할당된 경우 볼륨 효율성 작업을 실행할 때 볼륨 효율성 우선순위 속성만 고려됩니다. SnapVault 보조 볼륨에 대한 증분 업데이트가 수행되면 작업 일정이 무시되고 중복 제거 작업이 실행됩니다.

단계

1. 볼륨 효율성 수정 명령을 사용하여 볼륨에 정책을 할당합니다.

예

다음 명령을 실행하면 이라는 볼륨 효율성 정책이 할당됩니다 `new_policy` 볼륨을 조정합니다 `VolA`:

'볼륨 효율성 수정 - vserver vs1-volume vola-policy new_policy'

에 대한 자세한 내용은 `volume efficiency modify` "ONTAP 명령 참조입니다"을 참조하십시오.

볼륨 효율성 정책을 수정합니다

볼륨 효율성 정책을 수정하여 다른 기간 동안 중복제거 및 데이터 압축을 실행하거나 명령을

사용하여 작업 일정을 변경할 수 있습니다 `volume efficiency policy modify`. 에 대한 자세한 내용은 `volume efficiency policy modify` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 볼륨 효율성 정책을 수정하려면 'volume Efficiency policy modify' 명령을 사용하십시오.

예

다음 명령을 실행하면 정책1이라는 볼륨 효율성 정책이 매시간마다 실행되도록 수정됩니다.

'볼륨 효율성 정책 수정 - vserver vs1-policy policy1-schedule hourly'

다음 명령을 실행하면 이름이 pol2인 볼륨 효율성 정책이 임계값인 30%로 수정됩니다.

'볼륨 효율성 정책 수정 - vserver vs1-policy pol1-type threshold-start-threshold - percent 30%'

ONTAP에서 볼륨 효율성 정책을 봅니다

이름, 일정, 기간, 설명이 포함된 볼륨 효율성 정책을 볼 수 있습니다.

이 작업에 대해

명령은 `volume efficiency policy show` 볼륨 효율성 정책을 표시하는 데 사용됩니다. 클러스터 범위에서 명령을 실행하면 클러스터 범위 정책이 표시되지 않습니다. 하지만 SVM 컨텍스트에서 클러스터 범위 정책을 볼 수 있습니다. 에 대한 자세한 내용은 `volume efficiency policy show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 볼륨 효율성 정책에 대한 정보를 보려면 'volume Efficiency policy show' 명령을 사용하십시오.

   출력은 사용자가 지정한 매개 변수에 따라 달라집니다. 에 대한 자세한 내용은 `volume efficiency policy show` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 명령을 실행하면 SVM VS1에 대해 생성된 정책에 대한 정보가 표시됩니다.

```
volume efficiency policy show -vserver vs1
```

다음 명령을 실행하면 기간이 10시간으로 설정된 정책이 표시됩니다.

```
volume efficiency policy show -duration 10
```

볼륨 효율성 정책을 볼륨에서 연결 해제합니다

볼륨에서 볼륨 효율성 정책을 연결 해제함으로써 볼륨에 대한 추가 일정 기반 중복제거 및 데이터 압축 작업의 실행을 중지할 수 있습니다. 볼륨 효율성 정책의 연결을 끊으면 수동으로 트리거해야 합니다.

단계

1. 'volume Efficiency modify' 명령을 사용하여 볼륨에서 볼륨 효율성 정책의 연결을 해제합니다.

예

다음 명령을 실행하면 볼륨 VolA에서 볼륨 효율성 정책이 해제됩니다. '볼륨 효율성 수정 - SVM VS1 - 볼륨 VolA - 정책 -'

에 대한 자세한 내용은 `volume efficiency modify` "ONTAP 명령 참조입니다"을 참조하십시오.

볼륨 효율성 정책을 삭제합니다

'volume Efficiency policy delete' 명령을 사용하면 볼륨 효율성 정책을 삭제할 수 있습니다.

시작하기 전에

삭제할 정책이 볼륨과 연결되어 있지 않은지 확인해야 합니다.

inline-only_와 _default_predefined 효율성 정책은 삭제할 수 없습니다.

단계

1. 볼륨 효율성 정책을 삭제하려면 'volume Efficiency policy delete' 명령을 사용하십시오.

예

다음 명령을 실행하면 policy1:'볼륨 효율성 정책 삭제 - vserver vs1-policy policy1'이라는 볼륨 효율성 정책이 삭제됩니다

에 대한 자세한 내용은 `volume efficiency policy delete` "ONTAP 명령 참조입니다"을 참조하십시오.

수동으로 볼륨 효율성 작업을 관리합니다

수동으로 볼륨 효율성 작업 관리 개요

효율성 작업을 수동으로 실행하여 볼륨에서 효율성 작업이 실행되는 방법을 관리할 수 있습니다.

또한 다음 조건에 따라 효율성 작업이 실행되는 방법을 제어할 수 있습니다.

- 체크포인트 사용 안 합니다
- 기존 데이터 또는 새 데이터에 대해 효율성 작업을 실행합니다
- 필요한 경우 효율성 작업을 중지합니다

'-fields' 옵션의 값으로 'schedule'과 함께 'volume Efficiency show' 명령을 사용하여 볼륨에 할당된 스케줄을 볼 수 있습니다.

에 대한 자세한 내용은 `volume efficiency show` "ONTAP 명령 참조입니다"을 참조하십시오.

효율성 작업을 수동으로 실행합니다

볼륨에 대해 수동으로 효율성 작업을 실행할 수 있습니다. 효율성 작업을 예약하는 것이 적절하지 않은 경우에는 이 작업을 수행할 수 있습니다.

시작하기 전에

수동으로 실행할 효율성 작업에 따라 볼륨에서 중복제거 또는 데이터 압축과 중복제거가 모두 활성화되어 있어야 합니다.

이 작업에 대해

이 작업은 `volume efficiency start` 명령을 사용하여 수행됩니다. 볼륨에 대해 온도에 민감한 스토리지 효율성을 설정하면 중복제거를 먼저 실행한 다음 데이터 압축을 수행합니다.

중복제거는 실행 중에 시스템 리소스를 사용하는 백그라운드 프로세스입니다. 볼륨에서 데이터가 자주 변경되지 않는 경우 중복제거를 더 자주 실행하는 것이 좋습니다. 스토리지 시스템에서 여러 개의 중복 제거 작업을 동시에 실행하면 시스템 리소스가 더 많이 소모됩니다.

노드당 최대 8개의 동시 중복제거 또는 데이터 압축 작업을 실행할 수 있습니다. 더 많은 효율성 작업이 예약되면 작업이 큐에 대기됩니다.

ONTAP 9.13.1 부터 볼륨에 온도에 민감한 스토리지 효율성이 활성화되어 있으면 기존 데이터에 대해 볼륨 효율성을 실행하여 순차적 압축을 활용하여 스토리지 효율성을 더욱 향상할 수 있습니다.

효율성을 수동으로 실행합니다

단계

1. 볼륨에 대한 효율성 작업을 시작합니다. `volume efficiency start`

예

+ 다음 명령을 사용하면 볼륨 VolA에서 중복제거 또는 중복제거만 수동으로 시작한 다음 논리적 압축 및 컨테이너 압축을 수행할 수 있습니다

를 누릅니다

```
volume efficiency start -vserver vs1 -volume VolA
```

기존 데이터를 다시 압축합니다

온도에 민감한 스토리지 효율성을 사용하는 볼륨에 대해 ONTAP 9.13.1 에 도입된 순차적 데이터 압축 기능을 활용하려면 기존 데이터를 다시 포장할 수 있습니다. 이 명령을 사용하려면 고급 권한 모드여야 합니다.

단계

1. 권한 수준 설정: `set -privilege advanced`
2. 기존 데이터 리팩: `volume efficiency inactive-data-compression start -vserver` *`vserver_name`* `-volume` *`volume_name`* `-scan-mode extended_recompression`

예

```
volume efficiency inactive-data-compression start -vserver vs1 -volume
vol1 -scan-mode extended_recompression
```

관련 정보

- "기존 데이터에 대해 수동으로 효율성 작업을 실행합니다"

체크포인트는 효율성 작업의 실행 프로세스를 기록하는 데 내부적으로 사용됩니다. 어떤 이유(예: 시스템 중단, 시스템 중단, 재부팅 또는 마지막 효율성 작업이 실패하거나 중지됨)로 인해 효율성 작업이 중지되고 체크포인트 데이터가 있는 경우 최신 체크포인트 파일에서 효율성 작업을 재개할 수 있습니다.

체크포인트가 생성됩니다.

- 작업의 각 단계 또는 하위 단계에서
- 'is stop' 명령을 실행하면
- 기간이 만료되는 경우

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

중단된 효율성 작업을 다시 시작합니다

시스템 중단, 시스템 중단 또는 재부팅으로 인해 효율성 작업이 중지되면 중단된 지점부터 효율성 작업을 재개할 수 있습니다. 따라서 작업을 처음부터 다시 시작할 필요가 없으므로 시간과 리소스를 절약할 수 있습니다.

이 작업에 대해

볼륨에 대해서만 중복 제거를 활성화하면 데이터가 중복 제거를 실행합니다. 볼륨에 대해 중복제거 및 데이터 압축을 둘 다 설정한 경우 데이터 압축이 먼저 실행된 후 중복제거가 실행됩니다.

명령을 사용하여 볼륨에 대한 체크포인트의 세부 정보를 볼 수 `volume efficiency show` 있습니다. 에 대한 자세한 내용은 `volume efficiency show` "ONTAP 명령 참조입니다"을 참조하십시오.

기본적으로 효율성 작업은 체크포인트에서 다시 시작됩니다. 그러나 이전 효율성 작업에 해당하는 체크포인트('볼륨 효율성 시작'-scan-old-data' 명령이 실행되는 단계)가 24시간 이상 오래된 경우에는 이전 체크포인트에서 효율성 작업이 자동으로 다시 시작되지 않습니다. 이 경우 효율성 작업은 처음부터 시작됩니다. 그러나 마지막 스캔 이후 볼륨에 상당한 변화가 일어나지 않았다면 '-use-checkpoint' 옵션을 사용하여 이전 체크포인트에서 강제로 계속할 수 있습니다.

단계

1. 효율성 작업을 재개하려면 '-use-checkpoint' 옵션과 함께 'volume Efficiency start' 명령을 사용하십시오.

   다음 명령을 사용하여 볼륨 VolA의 새 데이터에 대한 효율성 작업을 재개할 수 있습니다.

   '볼륨 효율성 시작 - vserver vs1-volume vola-use-checkpoint true'

   다음 명령을 사용하여 볼륨 VolA의 기존 데이터에 대한 효율성 작업을 다시 시작할 수 있습니다.

   '볼륨 효율성 시작 - vserver vs1-volume vola-scan-old-data TRUE-use-checkpoint true'

   에 대한 자세한 내용은 `volume efficiency start` "ONTAP 명령 참조입니다"을 참조하십시오.

기존 데이터에 대해 수동으로 효율성 작업 실행

온도에 민감하지 않은 스토리지 효율성 볼륨에 있는 데이터에 대해 중복제거, 데이터 압축 또는

데이터 컴팩션을 활성화하기 전에 효율성 작업을 수동으로 실행할 수 있습니다. ONTAP 9.8 이전 버전의 ONTAP에서 이러한 작업을 실행할 수 있습니다.

이 작업에 대해

이 작업은 `volume efficiency start` 명령을 `-scan-old-data` 매개 변수와 함께 사용하여 수행됩니다. 이 `-compression` 옵션은 온도에 민감한 스토리지 효율성 볼륨에 대해서는 작동하지 `-scan-old-data` 않습니다. 비활성 데이터 압축은 기존 데이터에 대해 자동으로 실행되어 ONTAP 9.8 이상에서는 온도에 민감한 스토리지 효율성을 높입니다.

볼륨에 대해 중복 제거만 사용하도록 설정하면 데이터에서 중복제거가 실행됩니다. 볼륨에 중복제거, 데이터 압축 및 데이터 컴팩션을 사용하도록 설정하면 데이터 압축이 먼저 실행된 후 중복제거가 실행되고 데이터 컴팩션이 적용됩니다.

기존 데이터에 대해 데이터 압축을 실행하면 기본적으로 데이터 압축 작업은 중복제거에서 공유하는 데이터 블록 및 스냅샷에 의해 잠기는 데이터 블록을 건너뜁니다. 공유 블록에 대해 데이터 압축을 실행하도록 선택하면 최적화가 꺼지고 지문 정보가 캡처되어 다시 공유용으로 사용됩니다. 기존 데이터를 압축할 때 데이터 압축의 기본 동작을 변경할 수 있습니다.

노드당 최대 8개의 중복제거, 데이터 압축 또는 데이터 컴팩션 작업을 동시에 실행할 수 있습니다. 나머지 작업은 대기열에 추가됩니다.

> AFF 플랫폼에서는 사후 처리 압축이 실행되지 않습니다. 이 작업을 건너뛰었음을 알리는 EMS 메시지가 생성됩니다.

에 대한 자세한 내용은 `volume efficiency start` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 'volume Efficiency start-scan-old-data' 명령을 사용하여 기존 데이터에서 중복제거, 데이터 압축 또는 데이터 컴팩션을 수동으로 실행하십시오.

   다음 명령을 사용하면 볼륨 VolA의 기존 데이터에 대해 이러한 작업을 수동으로 실행할 수 있습니다.

   '볼륨 효율성 시작 - vserver vs1-volume vola-scan-old-data TRUE[-compression|-dedupe|-다짐] TRUE'

관련 정보

- "효율성 작업을 수동으로 실행합니다"

스케줄을 사용하여 볼륨 효율성 작업을 관리합니다

기록되는 새 데이터의 양에 따라 효율성 작업을 실행합니다

이전 효율성 작업 이후에 볼륨에 기록되는 새 블록의 수가 지정된 임계값 비율을 초과할 경우 중복제거 또는 데이터 압축을 실행하도록 효율성 작업 일정을 수정할 수 있습니다. 이전 효율성 작업이 수동으로 수행되었는지 또는 일정에 따라 수행되었는지에 적용됩니다.

이 작업에 대해

'스케줄' 옵션이 '자동'으로 설정되어 있으면 새 데이터의 양이 지정된 비율을 초과하면 예약된 효율성 작업이 실행됩니다. 기본 임계값은 20%입니다. 이 임계값은 효율성 작업에서 이미 처리된 총 블록 수의 백분율입니다.

단계

1. 'auto@num' 옵션과 함께 'volume Efficiency modify' 명령을 사용하여 임계값 백분율 값을 수정합니다.

   num은 백분율을 지정하는 두 자리 숫자입니다.

예

다음 명령을 실행하면 볼륨 VolA에 대한 임계값 백분율 값이 30%로 수정됩니다.

'볼륨 효율성 수정 - vserver vs1-volume-vola-schedule auto@30'

관련 정보

- "일정을 사용하여 효율성 작업을 실행합니다"
- "볼륨 효율성 수정"

예약을 통해 효율성 작업을 실행합니다

볼륨에 대한 중복제거 또는 데이터 압축 작업의 예약을 수정할 수 있습니다. 일정 및 볼륨 효율성 정책의 구성 옵션은 상호 배타적입니다.

이 작업에 대해

이 작업은 `volume efficiency modify` 명령을 사용하여 수행됩니다. 에 대한 자세한 내용은 `volume efficiency modify` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 'volume Efficiency modify' 명령을 사용하여 볼륨에 대한 중복제거 또는 데이터 압축 작업의 일정을 수정합니다.

예

다음 명령을 실행하면 VolA의 효율성 작업 예약이 월요일부터 금요일까지 오후 11시에 실행되도록 수정됩니다.

'볼륨 효율성 수정 - vserver vs1-volume vola-schedule mon - 금@23'

관련 정보

- "작성된 새 데이터의 양에 따라 효율성 작업을 실행합니다"

볼륨 효율성 작업을 모니터링합니다

효율성 작업 및 상태 보기

볼륨에 대해 중복제거 또는 데이터 압축이 활성화되어 있는지 여부를 확인할 수 있습니다. 볼륨의 효율성 작업의 상태, 상태, 압축 유형 및 진행률을 확인할 수도 있습니다.

두 가지 작업을 사용할 수 있습니다. 둘 다 명령을 `volume efficiency show`사용합니다.

효율성 상태를 봅니다

단계

1. 볼륨에 대한 효율성 작업의 상태를 봅니다. `volume efficiency show`

   다음 명령을 실행하면 적응형 압축 유형이 할당된 볼륨 VolA의 효율성 작업 상태가 표시됩니다.

'볼륨 효율성 표시-인스턴스-가상 서버 VS1-볼륨 볼라'

볼륨 VolA에서 효율성 작업이 활성화되어 있고 작업이 유휴 상태인 경우 시스템 출력에서 다음을 확인할 수 있습니다.

```
cluster1::> volume efficiency show -vserver vs1 -volume VolA

  Vserver Name: vs1
   Volume Name: VolA
   Volume Path: /vol/VolA
         State: Enabled
        Status: Idle
      Progress: Idle for 00:03:20
```

볼륨에 순차적으로 압축된 데이터가 포함되어 있는지 확인합니다

예를 들어 9.13.1 이전의 ONTAP 릴리즈로 되돌려야 하는 경우 순차적 패킹이 활성화된 볼륨 목록을 표시할 수 있습니다. 이 명령을 사용하려면 고급 권한 모드여야 합니다.

단계

1. 권한 수준 설정: `set -privilege advanced`
2. 순차적 패킹이 활성화된 볼륨 나열:

   ```
   volume efficiency show -extended-auto-adaptive-compression true
   ```

효율성 공간 절약 효과 확인

볼륨에서 중복제거 및 데이터 압축을 통해 절약되는 공간을 확인할 수 있습니다. 이를 통해 관리 프로세스의 효과를 평가하거나 용량 계획의 일부로 평가할 수 있습니다.

이 작업에 대해

명령을 사용하여 `volume show` 볼륨의 공간 절약 공간을 표시해야 합니다. 볼륨에서 얻은 공간 절약 효과는 계산할 때 스냅샷의 공간 절약 비율은 포함되지 않습니다. 중복 제거를 사용해도 볼륨 할당량은 영향을 받지 않습니다. 할당량은 논리적 레벨에서 보고되며 변경되지 않습니다.

단계

1. 'volume show' 명령을 사용하면 중복제거 및 데이터 압축을 통해 볼륨에서 실현된 공간 절약 효과를 볼 수 있습니다.

예

다음 명령을 사용하면 볼륨 VolA에서 중복 제거 및 데이터 압축을 사용하여 얻은 공간 절약 효과를 볼 수 있습니다. 'volume show -vserver vs1 -volume vola

```
cluster1::> volume show -vserver vs1 -volume VolA

                                    Vserver Name: vs1
                                     Volume Name: VolA

...
            Space Saved by Storage Efficiency: 115812B
       Percentage Saved by Storage Efficiency: 97%
                 Space Saved by Deduplication: 13728B
            Percentage Saved by Deduplication: 81%
                Space Shared by Deduplication: 1028B
                   Space Saved by Compression: 102084B
        Percentage Space Saved by Compression: 97%

...
```

에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

FlexVol 볼륨의 효율성 통계를 확인합니다

FlexVol volume에서 실행되는 효율성 작업의 세부 정보를 볼 수 있습니다. 이를 통해 관리 프로세스의 효과를 평가하거나 용량 계획의 일부로 평가할 수 있습니다.

단계

1. 'volume Efficiency stat' 명령을 사용하여 FlexVol 볼륨의 효율성 작업 통계를 볼 수 있습니다.

예

다음 명령을 사용하면 볼륨 VolA에 대한 효율성 작업의 통계를 볼 수 있습니다. '볼륨 효율성 stat -vserver vs1 -volume vola

```
cluster1::> volume efficiency stat -vserver vs1 -volume VolA

               Vserver Name: vs1
                Volume Name: VolA
                Volume Path: /vol/VolA
Inline Compression Attempts: 0
```

에 대한 자세한 내용은 `volume efficiency stat` "ONTAP 명령 참조입니다"을 참조하십시오.

볼륨 효율성 작업을 중지합니다

중복제거 또는 사후 처리 압축 작업을 중지할 수 있습니다.

이 작업에 대해

이 작업은 명령을 `volume efficiency stop`사용합니다. 이 명령은 체크포인트를 자동으로 생성합니다.

단계

1. 활성 중복제거 또는 사후 압축 작업을 중지하려면 '볼륨 효율성 중지' 명령을 사용합니다.

   '-ALL' 옵션을 지정하면 활성 및 대기 중인 효율성 작업이 중단됩니다.

예

다음 명령을 실행하면 볼륨 VolA에서 현재 활성 상태인 중복제거 또는 사후 처리 압축 작업이 중지됩니다.

'볼륨 효율성 중지 - 가상 서버 VS1 - 볼륨 볼라'

다음 명령을 실행하면 볼륨 VolA에서 활성 및 대기 상태의 중복제거 또는 사후 처리 압축 작업이 모두 중단됩니다.

'볼륨 효율성 중지 - vserver vs1-volume vola - 모두 TRUE'

에 대한 자세한 내용은 `volume efficiency stop` "ONTAP 명령 참조입니다"을 참조하십시오.

볼륨에서 공간 절약 효과를 제거하는 방법에 대한 추가 정보입니다

효율성 작업을 볼륨에 대해 실행하여 달성된 공간 절약 효과를 제거하도록 선택할 수 있습니다. 그러나 역전을 수용할 수 있는 충분한 공간이 있어야 합니다.

공간 절약 제거를 계획하고 구현하는 데 도움이 되는 여러 관련 리소스가 있습니다.

관련 정보

- "ONTAP 9에서 중복제거, 압축, 컴팩션을 통한 공간 절약 효과를 확인하는 방법"
- "ONTAP의 스토리지 효율성 절감 효과를 취소하는 방법"

한 **SVM**에서 다른 **SVM**으로 볼륨을 다시 호스팅

SVM 간에 볼륨을 재호스팅할 준비가 필요합니다

볼륨 재호스트 작업을 통해 SnapMirror 복사본 없이 NAS 또는 SAN 볼륨을 한 SVM에서 다른 SVM으로 재할당할 수 있습니다. 정확한 재호스트 절차는 사용되는 클라이언트 액세스 프로토콜과 볼륨 유형에 따라 다릅니다. 볼륨 재호스팅은 데이터 액세스 및 볼륨 관리를 위한 운영 중단 작업입니다.

SVM 간에 볼륨을 재호스팅할 수 있으려면 먼저 다음 조건이 충족되어야 합니다.

- 볼륨이 온라인 상태여야 합니다
- 볼륨 프로토콜은 SAN 또는 NAS여야 합니다
  - NAS 프로토콜 볼륨의 경우 볼륨은 접합 경로의 일부가 아니어야 하며 마운트 해제해야 합니다
- 볼륨이 SnapMirror 관계에 있는 경우 관계를 삭제한 후 관계 정보만 해제하거나 볼륨 재호스트를 시작하기 전에 관계를 해제해야 합니다
  - 볼륨 재호스트 작업 후에 SnapMirror 관계를 다시 동기화할 수 있습니다
- SVM 하위 유형은 소스 및 대상 SVM에서 모두 같아야 합니다

- 동일한 하위 유형의 SVM 간에만 볼륨을 재호스팅할 수 있습니다

- 볼륨은 FlexClone 또는 FlexClone 상위 볼륨일 수 없습니다
  - FlexClone은 상위 볼륨 또는 클론 볼륨을 재호스팅하기 전에 분할해야 합니다

SMB 볼륨을 재호스팅합니다

SMB 프로토콜을 사용하여 데이터를 제공하는 볼륨을 재호스팅할 수 있습니다. 재호스팅 작업 후 클라이언트가 계속 데이터에 액세스할 수 있도록 하려면 정책 및 관련 규칙을 수동으로 구성해야 합니다.

이 작업에 대해

- 재호스팅은 중단을 야기하는 작업입니다.
- 재호스팅 작업이 실패하면 소스 볼륨에서 볼륨 정책 및 관련 규칙을 다시 구성해야 할 수 있습니다.
- 소스 SVM 및 대상 SVM Active Directory 도메인이 서로 다르면 볼륨의 개체에 액세스하지 못할 수 있습니다.
- ONTAP 9.8부터 NetApp 볼륨 암호화(NVE)를 통한 볼륨 재호스팅이 지원됩니다. 온보드 키 관리자를 사용하는 경우 재호스팅 작업 중에 암호화된 메타데이터가 수정됩니다. 사용자 데이터는 변경되지 않습니다.

  ONTAP 9.8 이상을 사용하는 경우 재호스트 작업을 수행하기 전에 볼륨을 암호화해야 합니다.

- 소스 SVM에 로컬 사용자 및 그룹이 있을 경우 설정된 파일 및 디렉토리(ACL)에 대한 사용 권한은 볼륨 재호스트 작업 후에 더 이상 유효하지 않습니다.

  감사 ACL(SACL)에도 마찬가지입니다.

- 재호스팅 작업 후에는 소스 볼륨에서 다음 볼륨 정책, 정책 규칙 및 구성이 손실되며 재호스트된 볼륨에서 수동으로 재구성해야 합니다.
  - 볼륨 및 qtree 엑스포트 정책
  - 안티바이러스 정책
  - 볼륨 효율성 정책
  - QoS(서비스 품질) 정책
  - 스냅샷 정책
  - 할당량 규칙
  - NS-SWITCH 및 NAME SERVICES 구성 엑스포트 정책 및 규칙
  - 사용자 및 그룹 ID

시작하기 전에

- 볼륨이 온라인 상태여야 합니다.
- 볼륨 이동 또는 LUN 이동 같은 볼륨 관리 작업이 실행되고 있지 않아야 합니다.
- 재호스팅 중인 볼륨에 대한 데이터 액세스를 중지해야 합니다.
- 대상 SVM의 ns-switch 및 name 서비스 구성은 재호스팅 볼륨의 데이터 액세스를 지원하도록 구성해야 합니다.
- 소스 SVM 및 타겟 SVM에는 동일한 Active Directory 및 realmDNS 도메인이 있어야 합니다.

- 볼륨의 사용자 ID 및 그룹 ID는 타겟 SVM에서 사용하거나 호스팅 볼륨에서 변경해야 합니다.

> 로컬 사용자 및 그룹이 구성되어 있고 해당 사용자 또는 그룹에 대해 설정된 권한이 있는 해당 볼륨에 파일 및 디렉토리가 있는 경우 이러한 권한은 더 이상 유효하지 않습니다.

단계

1. 볼륨 재호스트 작업이 실패할 경우 CIFS 공유에 대한 정보가 손실되지 않도록 CIFS 공유에 대한 정보를 기록합니다.
2. 상위 볼륨에서 볼륨을 마운트 해제합니다.

   '볼륨 마운트 해제'
3. 고급 권한 레벨로 전환합니다.

   세트 프리빌리지 고급
4. 대상 SVM에서 볼륨 재호스팅:

   `volume rehost -vserver source_svm -volume vol_name -destination-vserver destination_svm`
5. 대상 SVM의 적절한 접합 경로 아래에 볼륨을 마운트합니다.

   '볼륨 마운트'입니다
6. 재호스트된 볼륨에 대한 CIFS 공유 생성:

   'vserver cifs share create
7. 소스 SVM과 타겟 SVM 간에 DNS 도메인이 서로 다른 경우 새로운 사용자와 그룹을 생성합니다.
8. 새로 대상 SVM LIF와 재호스팅 볼륨의 접합 경로로 CIFS 클라이언트를 업데이트합니다.

작업을 마친 후

재호스트된 볼륨에서 정책 및 관련 규칙을 수동으로 재구성해야 합니다.

"SMB 구성"

"SMB 및 NFS 멀티 프로토콜 구성"

NFS 볼륨을 재호스팅합니다

NFS 프로토콜을 사용하여 데이터를 제공하는 볼륨을 재호스팅할 수 있습니다. 재호스팅 작업 후에도 클라이언트가 계속 데이터에 액세스할 수 있도록 하려면 볼륨을 SVM의 엑스포트 정책과 연결하고 정책 및 관련 규칙을 수동으로 구성해야 합니다.

이 작업에 대해

- 재호스팅은 중단을 야기하는 작업입니다.
- 재호스팅 작업이 실패하면 소스 볼륨에서 볼륨 정책 및 관련 규칙을 다시 구성해야 할 수 있습니다.

- ONTAP 9.8부터 NetApp 볼륨 암호화(NVE)를 통한 볼륨 재호스팅이 지원됩니다. 온보드 키 관리자를 사용하는 경우 재호스팅 작업 중에 암호화된 메타데이터가 수정됩니다. 사용자 데이터는 변경되지 않습니다.

  ONTAP 9.8 이상을 사용하는 경우 재호스트 작업을 수행하기 전에 볼륨을 암호화해야 합니다.

- 재호스팅 작업 후에는 소스 볼륨에서 다음 볼륨 정책, 정책 규칙 및 구성이 손실되며 재호스트된 볼륨에서 수동으로 재구성해야 합니다.
  - 볼륨 및 qtree 엑스포트 정책
  - 안티바이러스 정책
  - 볼륨 효율성 정책
  - QoS(서비스 품질) 정책
  - 스냅샷 정책
  - 할당량 규칙
  - NS-SWITCH 및 NAME SERVICES 구성 엑스포트 정책 및 규칙
  - 사용자 및 그룹 ID

시작하기 전에

- 볼륨이 온라인 상태여야 합니다.
- 볼륨 이동 또는 LUN 이동과 같은 볼륨 관리 작업이 실행되지 않아야 합니다.
- 재호스팅 중인 볼륨에 대한 데이터 액세스를 중지해야 합니다.
- 대상 SVM의 ns-switch 및 name 서비스 구성은 재호스팅 볼륨의 데이터 액세스를 지원하도록 구성해야 합니다.
- 볼륨의 사용자 ID 및 그룹 ID는 타겟 SVM에서 사용하거나 호스팅 볼륨에서 변경해야 합니다.

단계

1. 볼륨 재호스트 작업이 실패할 경우 NFS 정책에 대한 정보가 손실되지 않도록 NFS 엑스포트 정책에 대한 정보를 기록합니다.
2. 상위 볼륨에서 볼륨을 마운트 해제합니다.

   '볼륨 마운트 해제'

3. 고급 권한 레벨로 전환합니다.

   세트 프리빌리지 고급

4. 대상 SVM에서 볼륨 재호스팅:

   `volume rehost -vserver` *`source_svm`* `-volume` *`volume_name`* `-destination-vserver` *`destination_svm`*

   대상 SVM의 기본 엑스포트 정책이 재호스팅 볼륨에 적용됩니다.

5. 엑스포트 정책 생성:

   'vserver export-policy create'

6. 재호스트된 볼륨의 내보내기 정책을 사용자 정의 엑스포트 정책으로 업데이트합니다.

   볼륨 수정

7. 대상 SVM의 적절한 접합 경로 아래에 볼륨을 마운트합니다.

   '볼륨 마운트'입니다

8. NFS 서비스가 대상 SVM에서 실행되고 있는지 확인합니다.
9. 재호스트된 볼륨에 대한 NFS 액세스를 재개합니다.
10. 대상 SVM LIF를 반영하도록 NFS 클라이언트 자격 증명 및 LIF 구성을 업데이트합니다.

    볼륨 액세스 경로(LIF 및 접합 경로)가 변경되었기 때문입니다.

작업을 마친 후

재호스트된 볼륨에서 정책 및 관련 규칙을 수동으로 재구성해야 합니다. 자세한 내용은 을 "NFS 구성" 참조하십시오.

SAN 볼륨을 재호스팅합니다

매핑된 LUN을 통해 데이터를 제공하는 SAN 볼륨을 재호스팅할 수 있습니다. 대상 SVM에서 이니시에이터 그룹(igroup)을 다시 생성한 후 볼륨 재호스트 작업에서 동일한 SVM에서 볼륨을 자동으로 재매핑할 수 있습니다.

이 작업에 대해

- 재호스팅은 중단을 야기하는 작업입니다.
- 재호스팅 작업이 실패하면 소스 볼륨에서 볼륨 정책 및 관련 규칙을 다시 구성해야 할 수 있습니다.
- ONTAP 9.8부터 NetApp 볼륨 암호화(NVE)를 통한 볼륨 재호스팅이 지원됩니다. 온보드 키 관리자를 사용하는 경우 재호스팅 작업 중에 암호화된 메타데이터가 수정됩니다. 사용자 데이터는 변경되지 않습니다.

  ONTAP 9.8 이상을 사용하는 경우 재호스트 작업을 수행하기 전에 볼륨을 암호화해야 합니다.

- 재호스팅 작업 후 소스 볼륨에서 다음 볼륨 정책, 정책 규칙 및 구성이 손실되며 재호스트된 볼륨에서 수동으로 재구성해야 합니다.
  - 안티바이러스 정책
  - 볼륨 효율성 정책
  - QoS(서비스 품질) 정책
  - 스냅샷 정책
  - NS-SWITCH 및 NAME SERVICES 구성 엑스포트 정책 및 규칙
  - 사용자 및 그룹 ID

시작하기 전에

- 볼륨이 온라인 상태여야 합니다.
- 볼륨 이동 또는 LUN 이동과 같은 볼륨 관리 작업이 실행되지 않아야 합니다.
- 볼륨 또는 LUN에 활성 I/O가 없어야 합니다.

- 대상 SVM에 동일한 이름의 igroup이 없지만 다른 이니시에이터가 있는지 확인해야 합니다.

  igroup의 이름이 동일한 경우 SVM(소스 또는 타겟) 중 하나에서 igroup의 이름을 변경해야 합니다.

- 'force-unmap-LUNs' 옵션을 설정해야 합니다.
  - 'force-unmap-LUNs' 옵션의 기본값은 'false'입니다.
  - "force-unmap-LUNs" 옵션을 "true"로 설정하면 경고 또는 확인 메시지가 표시되지 않습니다.

단계

1. 타겟 볼륨에 LUN 매핑 정보 기록:

   `lun mapping show volume` *`volume`* `vserver` *`source_svm`*

   이 단계는 볼륨 재호스트에 장애가 발생할 경우 LUN 매핑에 대한 정보가 손실되지 않도록 하는 사전 예방 단계입니다.

   에 대한 자세한 내용은 `lun mapping show volume` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 타겟 볼륨과 연결된 igroup을 삭제합니다.
3. 타겟 볼륨을 대상 SVM으로 다시 호스팅:

   `volume rehost -vserver` *`source_svm`* `-volume` *`volume_name`* `-destination-vserver` *`destination_svm`*

4. 타겟 볼륨의 LUN을 적절한 igroup에 매핑:
   - 볼륨 재호스트는 타겟 볼륨에서 LUN을 보존하지만 LUN은 매핑 해제된 상태로 유지됩니다.
   - LUN을 매핑할 때 대상 SVM 포트 세트를 사용합니다.
   - 자동 재매핑-LUN 옵션이 true로 설정되어 있으면 재호스팅 후 LUN이 자동으로 매핑됩니다.

SnapMirror 관계에서 볼륨 재호스팅

SnapMirror 관계의 일부로 정의된 볼륨을 재호스팅할 수 있습니다. 관계를 다시 호스팅하기 전에 고려해야 할 몇 가지 문제가 있습니다.

이 작업에 대해

- 재호스팅은 중단을 야기하는 작업입니다.
- 재호스팅 작업이 실패하면 소스 볼륨에서 볼륨 정책 및 관련 규칙을 다시 구성해야 할 수 있습니다.
- 재호스팅 작업 후 소스 볼륨에서 다음 볼륨 정책, 정책 규칙 및 구성이 손실되며 재호스트된 볼륨에서 수동으로 재구성해야 합니다.
  - 볼륨 및 qtree 엑스포트 정책
  - 안티바이러스 정책
  - 볼륨 효율성 정책
  - QoS(서비스 품질) 정책
  - 스냅샷 정책

- 할당량 규칙
- NS-SWITCH 및 NAME SERVICES 구성 엑스포트 정책 및 규칙
- 사용자 및 그룹 ID

시작하기 전에

- 볼륨이 온라인 상태여야 합니다.
- 볼륨 이동 또는 LUN 이동과 같은 볼륨 관리 작업이 실행되지 않아야 합니다.
- 재호스팅 중인 볼륨에 대한 데이터 액세스를 중지해야 합니다.
- 대상 SVM의 ns-switch 및 name 서비스 구성은 재호스팅 볼륨의 데이터 액세스를 지원하도록 구성해야 합니다.
- 볼륨의 사용자 ID 및 그룹 ID는 타겟 SVM에서 사용하거나 호스팅 볼륨에서 변경해야 합니다.

단계

1. SnapMirror 관계 유형을 기록합니다.

   스냅미러 쇼

   이 단계는 볼륨 재호스트에 장애가 발생할 경우 SnapMirror 관계 유형에 대한 정보가 손실되지 않도록 하는 사전 예방 단계입니다.

2. 대상 클러스터에서 SnapMirror 관계를 삭제합니다.

   스냅미러 삭제

   SnapMirror 관계를 해제하지 마십시오. 그렇지 않으면 타겟 볼륨의 데이터 보호 기능이 손실되고 재호스팅 작업 후에는 관계를 다시 설정할 수 없습니다.

3. 소스 클러스터에서 SnapMirror 관계 정보를 제거합니다.

   ```
   snapmirror release -relationship-info-only true
   ```

   `-relationship-info-only`스냅샷을 삭제하지 않고 소스 관계 정보를 제거하도록 매개 변수를 `true` 설정합니다.

4. 볼륨이 마운트된 경우 마운트 해제합니다.

   ```
   volume unmount -vserver <source_svm> -volume <vol_name>
   ```

5. 고급 권한 레벨로 전환합니다.

   세트 프리빌리지 고급

6. 대상 SVM에서 볼륨 재호스팅:

   ```
   volume rehost -vserver <source_svm> -volume <vol_name> -destination-vserver
   <destination_svm>
   ```

7. SVM 피어링 관계가 없을 경우, 소스 SVM과 타겟 SVM 간에 SVM 피어 관계를 생성합니다.

'vserver peer create

8. 소스 볼륨과 타겟 볼륨 간의 SnapMirror 관계를 생성합니다.

   스냅미러 생성

   DP 볼륨을 호스팅하는 SVM에서 'napmirror create' 명령을 실행해야 합니다. 재호스트된 볼륨은 SnapMirror 관계의 소스 또는 대상이 될 수 있습니다.

9. SnapMirror 관계를 다시 동기화합니다.

관련 정보

- "설정"
- "SnapMirror를 참조하십시오"
- "볼륨 재호스팅"
- "볼륨 마운트 해제"
- "SVM 피어 생성"

ONTAP에서 볼륨 재호스트에서는 기능이 지원되지 않습니다

볼륨 재호스트를 지원하지 않는 ONTAP 기능에는 몇 가지가 있습니다. 재호스트 작업을 시도하기 전에 이러한 기능을 숙지해야 합니다.

다음 기능은 볼륨 재호스트에서는 지원되지 않습니다.

- SVM DR
- MetroCluster 구성

  다른 SVM에서 볼륨을 FlexClone 볼륨으로 클론 복제하는 것은 MetroCluster 구성에서도 지원되지 않습니다.

- SnapLock 볼륨
- NetApp 볼륨 암호화(NVE) 볼륨(ONTAP 9.8 이전 버전)

  9.8 이전의 ONTAP 릴리스에서는 볼륨을 다시 호스팅하기 전에 볼륨의 암호화를 해제해야 합니다. 볼륨 암호화 키는 SVM 키에 따라 다릅니다. 볼륨이 다른 SVM으로 이동하고 소스 또는 타겟 SVM에서 멀티테넌트 키 구성이 활성화된 경우 볼륨 및 SVM 키가 일치하지 않습니다.

  ONTAP 9.8부터 NVE로 볼륨을 재호스팅할 수 있습니다.

- FlexGroup 볼륨
- 클론 볼륨

권장되는 볼륨 및 파일 또는 **LUN** 구성 조합

권장되는 볼륨 및 파일 또는 **LUN** 구성 조합 개요

애플리케이션 및 관리 요구사항에 따라 FlexVol 볼륨과 파일 또는 LUN 구성의 특정 조합이 사용할 수 있습니다. 이러한 조합의 이점과 비용을 이해하면 환경에 적합한 구성을 결정하는 데 도움이 됩니다.

권장되는 볼륨 및 LUN 구성 조합은 다음과 같습니다.

- 일반 볼륨 프로비저닝이 있는 공간 예약 파일 또는 LUN
- 씬 볼륨 프로비저닝이 있는 공간 예약 파일이 아닌 LUN
- 반씩 볼륨 프로비저닝을 사용하는 공간 예약 파일 또는 LUN

이러한 구성 조합과 함께 LUN에서 SCSI 씬 프로비저닝을 사용할 수 있습니다.

일반 볼륨 프로비저닝이 있는 공간 예약 파일 또는 **LUN**

- 이점: *
- 공간 예약 파일 내의 모든 쓰기 작업이 보장되며 공간 부족으로 인해 작업이 실패하지 않습니다.
- 볼륨의 스토리지 효율성 및 데이터 보호 기술에는 제한이 없습니다.
- 비용 및 제한: *
- 전체적으로 프로비저닝된 볼륨을 지원할 수 있도록 충분한 공간을 집합체로부터 충분히 미리 설정해야 합니다.
- LUN 생성 시 볼륨에서 LUN의 2배에 해당하는 공간이 할당됩니다.

씬 볼륨 프로비저닝이 있는 공간 예약 파일이 아닌 **LUN**

- 이점: *
- 볼륨의 스토리지 효율성 및 데이터 보호 기술에는 제한이 없습니다.
- 공간은 사용되는 경우에만 할당됩니다.
- 비용 및 제한: *
- 쓰기 작업은 보장되지 않으며, 볼륨에 여유 공간이 없을 경우 실패할 수 있습니다.
- Aggregate에 여유 공간이 부족하지 않도록 하려면 Aggregate의 여유 공간을 효과적으로 관리해야 합니다.

반씩 볼륨 프로비저닝을 사용하는 공간 예약 파일 또는 **LUN**

- 이점: *

공간을 일반 볼륨 프로비저닝보다 미리 예약하므로 최선의 쓰기 보장이 제공됩니다.

- 비용 및 제한: *
- 이 옵션을 사용하면 쓰기 작업이 실패할 수 있습니다.

  볼륨의 여유 공간과 데이터 휘발성의 균형을 적절하게 유지하여 이 위험을 완화할 수 있습니다.

- 스냅샷, FlexClone 파일 및 LUN과 같은 데이터 보호 객체의 보존에 의존할 수는 없습니다.
- 중복제거, 압축, ODX/복사 오프로드 등 자동으로 삭제할 수 없는 ONTAP 블록 공유 스토리지 효율성 기능은 사용할

수 없습니다.

요구 사항에 적합한 볼륨 및 **LUN** 구성을 결정합니다

환경에 대한 몇 가지 기본적인 질문에 답변하면 환경에 가장 적합한 FlexVol 볼륨 및 LUN 구성을 파악하는 데 도움이 됩니다.

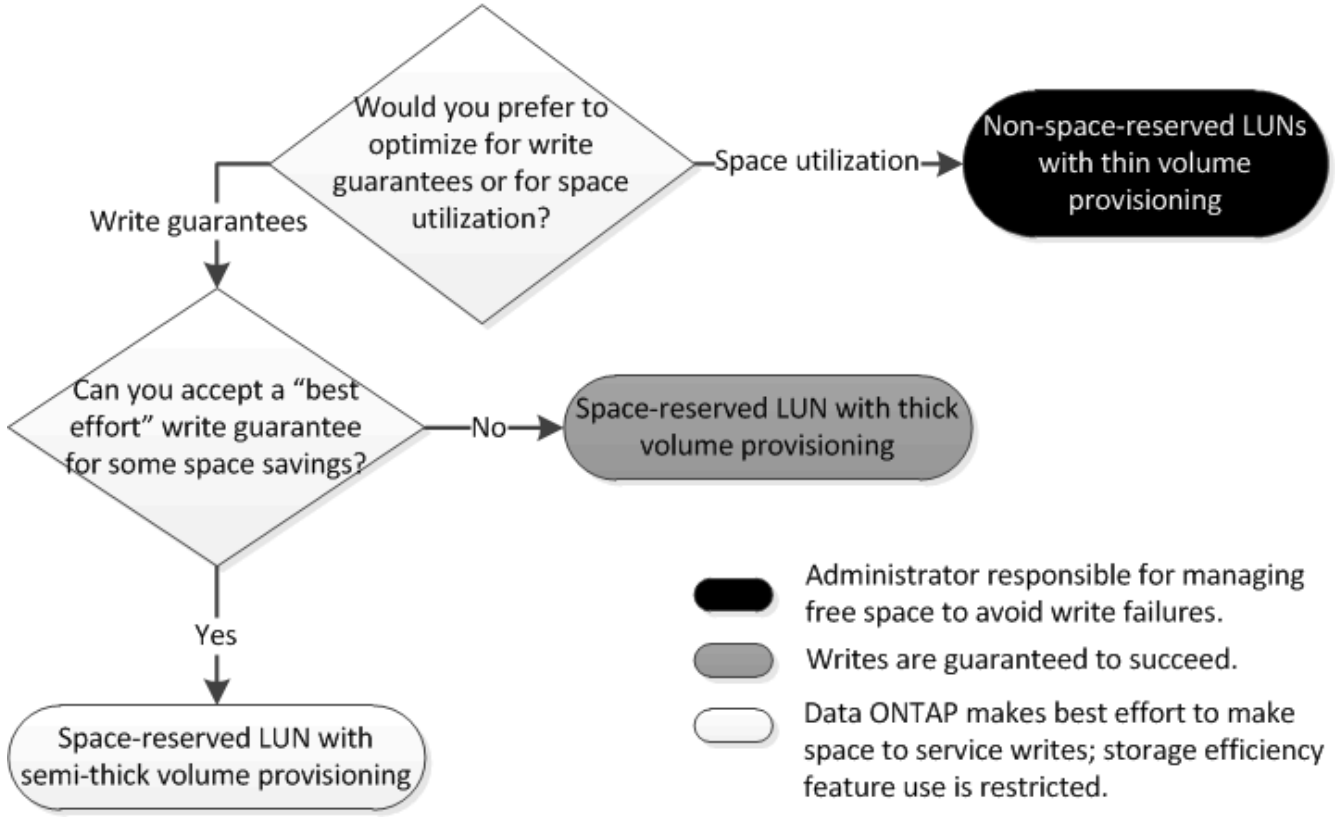
이 작업에 대해

LUN 및 볼륨 구성을 최적화하여 스토리지 활용률을 극대화하거나 쓰기 보장을 극대화할 수 있습니다. 스토리지 활용률의 요구사항과 여유 공간을 신속하게 모니터링 및 보충하는 기능을 기준으로 설치에 적합한 FlexVol 볼륨 및 LUN 볼륨을 결정해야 합니다.

각 LUN에 대해 별도의 볼륨이 필요하지 않습니다.

단계

1. 다음 진단트리를 사용하여 환경에 가장 적합한 볼륨 및 LUN 구성 조합을 결정합니다.



일반 프로비저닝된 볼륨이 있는 공간 예약 파일 또는 **LUN**에 대한 구성 설정입니다

FlexVol volume 구성과 파일 또는 LUN 구성의 조합에는 여러 가지가 있습니다. 일반 프로비저닝된 볼륨을 기반으로 하는 이러한 조합은 스토리지 효율성 기술을 사용할 수 있는 기능을 제공하며 충분한 공간이 사전에 할당되므로 사용 가능한 공간을 능동적으로 모니터링할 필요가 없습니다.

일반 프로비저닝을 사용하여 볼륨에서 공간 예약 파일 또는 LUN을 구성하려면 다음 설정이 필요합니다.

볼륨 설정	값
보장	볼륨
부분 예약	100
스냅숏 예비 공간입니다	모두
스냅샷 자동 삭제	선택 사항
자동 확장	선택 사항: 사용하도록 설정한 경우 애그리게이트 가용 공간을 능동적으로 모니터링해야 합니다.

파일 또는 **LUN** 설정	값
공간 예약	활성화됨

관련 정보

- "권장되는 볼륨 및 파일 또는 LUN 구성 조합 개요"

비공간 예약 파일 또는 씬 프로비저닝된 볼륨이 있는 **LUN**에 대한 설정입니다

이 FlexVol 볼륨 및 파일 또는 LUN 구성 조합을 사용하려면 가장 적은 양의 스토리지를 미리 할당해야 하지만 공간 부족으로 인한 오류를 방지하기 위해 활성 여유 공간 관리가 필요합니다.

씬 프로비저닝된 볼륨에서 공간이 예약되지 않은 파일 또는 LUN을 구성하려면 다음 설정이 필요합니다.

볼륨 설정	값
보장	없음
부분 예약	0
스냅숏 예비 공간입니다	모두
스냅샷 자동 삭제	선택 사항
자동 확장	선택 사항

파일 또는 **LUN** 설정	값
공간 예약	사용 안 함

추가 고려 사항

볼륨 또는 애그리게이트의 공간이 부족해지면 파일 또는 LUN에 대한 쓰기 작업이 실패할 수 있습니다.

볼륨과 애그리게이트의 여유 공간을 적극적으로 모니터링하지 않으려면 볼륨에 대해 Autogrow를 활성화하고 볼륨의 최대 크기를 애그리게이트 크기로 설정해야 합니다. 이 구성에서는 aggregate 여유 공간을 적극적으로 모니터링해야 하지만, 볼륨의 여유 공간을 모니터링할 필요는 없습니다.

반씩 볼륨 프로비저닝을 사용하는 공간 예약 파일 또는 **LUN**에 대한 구성 설정입니다

FlexVol volume 구성과 파일 또는 LUN 구성의 조합에는 여러 가지가 있습니다. 반씩 씩 볼륨 프로비저닝을 기반으로 하는 이 조합은 완전히 프로비저닝되는 조합보다 더 적은 수의 스토리지를 먼저 할당할 필요가 있습니다. 그러나 볼륨에 사용할 수 있는 효율성 기술에는 제한이 있습니다. 이러한 구성 조합의 경우 덮어쓰기의 작업이 가장 효율적으로 처리됩니다.

반씩 프로비저닝을 사용하여 볼륨에서 공간 예약 LUN을 구성하려면 다음 설정이 필요합니다.

볼륨 설정	값
보장	볼륨
부분 예약	0
스냅숏 예비 공간입니다	0
스냅샷 자동 삭제	제거 약속 수준에서는 모든 오브젝트, 볼륨으로 설정된 트리거, 자동 삭제를 위해 활성화된 모든 FlexClone LUN 및 FlexClone 파일이 포함된 제거 목록이 있습니다.
자동 확장	선택 사항: 사용하도록 설정한 경우 애그리게이트 가용 공간을 능동적으로 모니터링해야 합니다.

파일 또는 **LUN** 설정	값
공간 예약	활성화됨

기술 제한

이 구성 조합에는 다음 볼륨 스토리지 효율성 기술을 사용할 수 없습니다.

- 압축
- 중복 제거
- ODX 및 FlexClone 복사 오프로드
- FlexClone LUN 및 FlexClone 파일이 자동 삭제용으로 표시되지 않음(활성 클론)
- FlexClone 하위 파일
- ODX/복사 오프로드

추가 고려 사항

이 구성 조합을 사용할 때는 다음 사항을 고려해야 합니다.

- 해당 LUN을 지원하는 볼륨의 공간이 부족하면 보호 데이터(FlexClone LUN 및 파일, 스냅샷)가 삭제됩니다.
- 볼륨에 여유 공간이 부족하면 쓰기 작업이 시간 초과되어 실패할 수 있습니다.

압축은 AFF 플랫폼에 대해 기본적으로 사용하도록 설정되어 있습니다. AFF 플랫폼에서 반씩 프로비저닝을 사용하려는 모든 볼륨에 대해 압축을 명시적으로 해제해야 합니다.

관련 정보

- "권장되는 볼륨 및 파일 또는 LUN 구성 조합 개요"

파일 또는 디렉토리 용량 변경에 대한 주의 및 고려 사항

ONTAP 의 **FlexVol** 볼륨에 허용되는 기본 및 최대 파일 수

FlexVol 볼륨에는 포함할 수 있는 기본 및 최대 파일 수가 있습니다. 데이터에 많은 수의 파일이 필요한 경우 볼륨에서 허용되는 사용자 표시 파일 수를 최대값까지 늘릴 수 있습니다. 계속 진행하기 전에 제한 사항과 주의사항을 이해해야 합니다.

볼륨에 포함될 수 있는 사용자가 볼 수 있는 파일의 수는 볼륨의 사용 가능한 inode 용량에 따라 결정됩니다. inode는 파일 정보를 담고 있는 데이터 구조입니다.

ONTAP 새로 생성된 볼륨에 대해 사용 가능한 inode의 기본 및 최대 개수를 볼륨 크기에 따라 다음과 같이 자동으로 설정합니다.

기본 **inode** 수	최대 **inode** 수
볼륨 크기 32KB당 1개	볼륨 크기 4KB당 1개

볼륨의 크기가 관리자가 수동으로 늘리거나 ONTAP의 자동 크기 조정 기능을 사용하여 자동으로 늘어나면 ONTAP 필요한 경우 사용 가능한 inode의 수도 늘려 볼륨 크기 32KB당 최소 1개의 inode가 있도록 합니다. 이렇게 하여 볼륨 크기가 약 680GB에 도달할 때까지 계속합니다.

ONTAP 9.12.1 및 이전 버전에서는 새 볼륨을 생성하거나 기존 볼륨의 크기를 680GB 이상으로 조정해도 자동으로 추가 inode 용량이 생성되지 않습니다. 모든 크기의 볼륨에 대해 기본 개수보다 더 많은 파일이 필요한 경우 다음을 사용할 수 있습니다. `volume modify` 볼륨에 사용 가능한 inode 수를 최대치까지 늘리는 명령입니다.

ONTAP 9.13.1부터 새 볼륨을 생성하거나 기존 볼륨의 크기를 조정하면 볼륨이 680GB보다 크더라도 사용 가능한 inode의 기본 개수가 볼륨 공간 32KB당 1개의 inode로 설정됩니다. 이 비율은 볼륨이 2,040,109,451의 절대 inode 최대값에 도달할 때까지 지속됩니다.

사용 가능한 inode 수를 줄일 수도 있습니다. 이렇게 하면 inode에 할당된 공간의 양은 바뀌지 않지만, 공개 inode 파일이 사용할 수 있는 최대 공간의 양은 줄어듭니다. inode에 공간이 할당된 후에는 해당 공간이 볼륨으로 반환되지 않습니다. 따라서 현재 할당된 inode 수보다 최대 inode 수를 낮추는 것은 불가능합니다.

추가 정보

- 볼륨에 대한 파일 및 inode 사용을 확인합니다
- "NetApp 기술 자료: FAQ - ONTAP 기본 및 최대 파일 수(inode)"

FlexVol 볼륨의 최대 디렉토리 크기입니다

다음을 사용하여 특정 FlexVol volume 의 기본 최대 디렉토리 크기를 늘릴 수 있습니다. `-maxdir-size` 옵션 `volume modify` 명령을 실행할 수 있지만, 그렇게 하면 시스템 성능에 영향을 미칠 수 있습니다. 를 참조하십시오"NetApp 지식 기반: maxdirsize란 무엇입니까?" .

FlexVol 볼륨의 모델 종속 최대 디렉토리 크기에 대한 자세한 내용은 를 참조하십시오 "NetApp Hardware Universe를 참조하십시오".

에 대한 자세한 내용은 `volume modify` "ONTAP 명령 참조입니다"을 참조하십시오.

노드 루트 볼륨 및 루트 애그리게이트에 대한 제한 사항

노드의 루트 볼륨 및 루트 애그리게이트를 관리하는 제한 사항을 알고 있어야 합니다.

노드의 루트 볼륨에는 노드에 대한 특수 디렉토리와 파일이 포함되어 있습니다. 루트 볼륨은 루트 애그리게이트에 포함되어 있습니다.

노드의 루트 볼륨은 공장 출하 시 또는 설치 소프트웨어에 의해 설치되는 FlexVol 볼륨입니다. 시스템 파일, 로그 파일 및 코어 파일용으로 예약되어 있습니다. 디렉토리 이름은 '/mroot'로, 시스템 셸을 통해서만 기술 지원 부서에서 액세스할 수 있습니다. 노드 루트 볼륨의 최소 크기는 플랫폼 모델에 따라 다릅니다.

- 다음 규칙은 노드의 루트 볼륨에 적용됩니다.
  - 기술 지원 부서에서 지시하지 않는 한 루트 볼륨의 구성 또는 콘텐츠를 수정하지 마십시오.
  - 루트 볼륨에 사용자 데이터를 저장하지 마십시오.

    사용자 데이터를 루트 볼륨에 저장하면 HA 쌍의 노드 간 스토리지 반환 시간이 늘어납니다.
  - 루트 볼륨을 다른 애그리게이트로 이동할 수 있습니다.

    "루트 볼륨을 새 애그리게이트로 재배치"
- 루트 애그리게이트는 노드의 루트 볼륨에만 사용됩니다.

  ONTAP을 사용하면 루트 애그리게이트에 다른 볼륨을 생성할 수 없습니다.

"NetApp Hardware Universe를 참조하십시오"

루트 볼륨을 새 애그리게이트로 재배치합니다

루트 교체 절차는 운영 중단 없이 현재 루트 애그리게이트를 다른 디스크 세트로 마이그레이션합니다. 디스크 교체 또는 예방 유지 보수 프로세스의 일부로 이 작업을 수행해야 할 수도 있습니다.

이 작업에 대해

다음 시나리오에서 루트 볼륨의 위치를 새 애그리게이트로 변경할 수 있습니다.

- 루트 애그리게이트가 원하는 디스크에 없을 경우

- 노드에 연결된 디스크를 재정렬하려는 경우
- EOS 디스크 쉘프의 쉘프 교체를 수행할 때

단계

1. 루트 애그리게이트 재배치:

   'system node migrate-root-node_name-disklist disk_list-raid-type raid_type'

   ◦ * -노드 *

     마이그레이션할 루트 애그리게이트를 소유하는 노드를 지정합니다.

   ◦ * -디스크 목록 *

     새 루트 애그리게이트를 생성할 디스크 목록을 지정합니다. 모든 디스크가 동일한 노드에서 소유하고 있어야 합니다. 필요한 최소 디스크 수는 RAID 유형에 따라 다릅니다.

   ◦ * -RAID-유형 *

     루트 애그리게이트의 RAID 유형을 지정합니다. 기본값은 "RAID-DP"입니다. 고급 모드에서 지원되는 유일한 유형입니다.

2. 작업 진행 상황 모니터링:

   job show-id jobid-instance입니다

결과

모든 사전 검사가 성공하면 명령이 루트 볼륨 교체 작업을 시작하고 종료됩니다.

FlexClone 파일 및 FlexClone LUN에서 지원하는 기능입니다

FlexClone 파일 및 **FlexClone LUN**에서 지원하는 기능입니다

FlexClone 파일 및 FlexClone LUN은 중복 제거, 스냅샷, 할당량, 볼륨 SnapMirror 등 다양한 ONTAP 기능을 지원합니다.

다음 기능은 FlexClone 파일 및 FlexClone LUN에서 지원됩니다.

- 중복 제거
- 스냅샷 수
- 액세스 제어 목록
- 할당량
- FlexClone 볼륨
- NDMP
- volume SnapMirror를 선택합니다
- '볼륨 이동' 명령

- 공간 예약
- HA 구성

FlexClone 파일 및 **FlexClone LUN**을 사용한 데이터 중복 제거

중복제거 사용 볼륨에서 상위 파일 및 상위 LUN의 FlexClone 파일 또는 FlexClone LUN을 생성하여 데이터 블록의 물리적 스토리지 공간을 효율적으로 사용할 수 있습니다.

FlexClone 파일 및 LUN에서 사용하는 블록 공유 메커니즘은 중복 제거에서도 사용됩니다. 볼륨에서 중복제거를 활성화한 다음 중복제거 사용 볼륨을 클론 복제하여 FlexVol 볼륨에서 공간 절약을 최대화할 수 있습니다.

중복 제거가 설정된 볼륨에서 '실행 취소 중' 명령을 실행하는 동안에는 해당 볼륨에 상주하는 상위 파일 및 상위 LUN의 FlexClone 파일과 FlexClone LUN을 생성할 수 없습니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

스냅샷이 **FlexClone** 파일 및 **FlexClone LUN**에서 작동하는 방식

스냅샷과 FlexClone 파일 및 FlexClone LUN 간에는 시너지 효과가 있습니다. 이러한 기술을 사용할 경우 가능한 것은 물론 관련 제한도 알고 있어야 합니다.

FlexClone 파일 및 **LUN** 생성

기존 스냅샷에서 FlexClone 파일 또는 FlexClone LUN을 생성할 수 있습니다. 복사본은 FlexVol volume에 포함된 상위 파일과 상위 LUN을 기반으로 합니다.

스냅샷을 삭제하는 중입니다

FlexClone 파일 또는 FlexClone LUN이 현재 생성되고 있는 스냅샷은 수동으로 삭제할 수 없습니다. 스냅샷은 백그라운드 블록 공유 프로세스가 완료될 때까지 잠긴 상태로 유지됩니다. 잠긴 스냅샷을 삭제하려고 하면 일정 시간 후에 작업을 다시 시도하라는 메시지가 표시됩니다. 이 경우 삭제 작업을 계속 다시 시도해야 합니다. 블록 공유가 완료된 후에는 스냅샷을 삭제할 수 있습니다.

FlexClone 파일 및 **FlexClone LUN**에 의한 액세스 제어 목록 상속

FlexClone 파일 및 FlexClone LUN은 부모 파일 및 LUN의 액세스 제어 목록을 상속합니다.

상위 파일에 Windows NT 스트림이 포함되어 있으면 FlexClone 파일도 스트림 정보를 상속합니다. 그러나 스트림이 6개 이상인 상위 파일은 복제할 수 없습니다.

FlexClone 파일 및 **FlexClone LUN**에서 할당량이 작동하는 방식

FlexClone 파일 및 FlexClone LUN을 사용하기 전에 할당량이 어떻게 작동하는지 잘 알고 있어야 합니다.

할당량 제한은 FlexClone 파일 또는 FlexClone LUN의 총 논리적 크기에 적용됩니다. 클론 생성 작업으로 인해 할당량이 초과되더라도 블록 공유가 실패하지 않습니다.

FlexClone 파일 또는 FlexClone LUN을 생성할 때 할당량은 절약 공간을 인식하지 못합니다. 예를 들어, 상위 파일 10GB 의 FlexClone 파일을 만드는 경우, 물리적 공간 크기는 10GB만 사용하고 할당량 활용률은 20GB(상위 파일의 경우 10GB, FlexClone 파일의 경우 10GB)로 기록됩니다.

FlexClone 파일 또는 LUN을 생성하면 그룹 또는 사용자 할당량이 초과되는 경우, FlexVol 볼륨에 클론의 메타데이터를 보관할 공간이 충분하다면 클론 작업이 성공합니다. 그러나 해당 사용자 또는 그룹의 할당량이 초과 할당되었습니다.

FlexClone 볼륨 및 관련 **FlexClone** 파일 및 **FlexClone LUN**

FlexClone 파일과 FlexClone LUN이 모두 있는 FlexVol 볼륨의 FlexClone 볼륨과 해당 상위 파일 또는 LUN을 생성할 수 있습니다.

FlexClone 볼륨에 있는 FlexClone 파일 또는 FlexClone LUN과 그 상위 파일 또는 LUN은 상위 FlexVol 볼륨과 동일한 방식으로 블록을 계속 공유합니다. 실제로 모든 FlexClone 엔터티와 부모는 동일한 기본 물리적 데이터 블록을 공유하여 물리적 디스크 공간 사용을 최소화합니다.

FlexClone 볼륨이 상위 볼륨에서 분리되면 FlexClone 파일 또는 FlexClone LUN과 해당 상위 파일 또는 LUN이 FlexClone 볼륨의 클론 내 블록 공유를 중지합니다. 그 이후에는 독립 파일 또는 LUN으로 존재합니다. 즉, 볼륨 클론은 분할 작업 이전보다 더 많은 공간을 사용합니다.

NDMP가 **FlexClone** 파일 및 **FlexClone LUN**과 작동하는 방식

NDMP는 FlexClone 파일 및 FlexClone LUN과 함께 논리적 레벨에서 작동합니다. 모든 FlexClone 파일 또는 LUN은 별도의 파일 또는 LUN으로 백업됩니다.

NDMP 서비스를 사용하여 FlexClone 파일 또는 FlexClone LUN이 포함된 qtree 또는 FlexVol 볼륨을 백업할 경우 상위 항목과 클론 항목 간의 블록 공유는 유지되지 않으며 클론 엔터티가 별도의 파일 또는 LUN으로 테이프에 백업됩니다. 공간 절약이 손실됩니다. 따라서 백업 중인 테이프에 확장된 양의 데이터를 저장할 충분한 공간이 있어야 합니다. 복원할 때 모든 FlexClone 파일과 FlexClone LUN이 별도의 물리적 파일 및 LUN으로 복원됩니다. 볼륨에서 중복 제거를 활성화하여 블록 공유 이점을 복원할 수 있습니다.

> FlexClone 파일 및 FlexClone LUN을 FlexVol volume의 기존 스냅샷에서 생성하는 경우 백그라운드에서 발생하는 블록 공유 프로세스가 완료될 때까지 볼륨을 테이프에 백업할 수 없습니다. 블록 공유 프로세스가 진행 중일 때 볼륨에 NDMP를 사용하면 일정 시간 후에 작업을 다시 시도하라는 메시지가 표시됩니다. 이러한 경우 블록 공유가 완료된 후 성공적으로 테이프 백업 작업을 다시 시도해야 합니다.

volume SnapMirror가 **FlexClone** 파일 및 **FlexClone LUN**과 작동하는 방식

FlexClone 파일 및 FlexClone LUN과 함께 볼륨 SnapMirror을 사용하면 클론 복제된 엔터티가 한 번만 복제되므로 공간 절약 효과를 유지하는 데 도움이 됩니다.

FlexVol 볼륨이 volume SnapMirror 소스이고 FlexClone 파일 또는 FlexClone LUN이 포함된 경우 volume SnapMirror는 공유된 물리적 블록과 소량의 메타데이터만 볼륨 SnapMirror 타겟으로 전송합니다. 대상은 물리적 블록의 복사본을 하나만 저장하고 이 블록은 상위 엔티티와 클론 복제된 엔터티 간에 공유됩니다. 따라서 대상 볼륨은 소스 볼륨의 정확한 복제본이며 대상 볼륨의 모든 클론 파일 또는 LUN은 동일한 물리적 블록을 공유합니다.

FlexClone 파일 및 **FlexClone LUN**에서 공간 예약이 작동하는 방식

FlexClone 파일과 FlexClone LUN을 사용할 때는 공간 예약 속성이 작동하는 방식을 이해해야 합니다.

기본적으로 FlexClone 파일과 LUN은 각각 상위 파일과 상위 LUN에서 공간 예약 속성을 상속합니다. 그러나 FlexVol volume에 공간이 부족한 경우 공간 예약을 해제한 상태로 FlexClone 파일과 FlexClone LUN을 생성할 수 있습니다.

이는 각 상위 항목의 속성이 활성화된 경우에도 가능합니다.

FlexVol volume에 공간이 부족하여 상위 LUN과 공간 예약이 동일한 FlexClone 파일 또는 FlexClone LUN을 생성할 수 없는 경우 클론 생성 작업이 실패합니다.

FlexClone 파일 및 **FlexClone LUN**에서 **HA** 구성의 작동 방식

FlexClone 파일 및 FlexClone LUN 작업은 HA 구성에서 지원됩니다.

HA pair에서는 테이크오버 또는 반환 작업이 진행 중인 동안에는 파트너에 FlexClone 파일 또는 FlexClone LUN을 생성할 수 없습니다. 테이크오버 또는 반환 작업이 완료된 후 파트너에 대해 보류 중인 모든 블록 공유 작업이 재개됩니다.

FlexGroup 볼륨 관리

CLI를 사용한 ONTAP FlexGroup 볼륨 관리에 대해 자세히 알아보십시오

확장성과 성능을 위해 FlexGroup 볼륨을 설정, 관리, 보호할 수 있습니다. FlexGroup 볼륨은 자동 로드 분산 기능과 함께 고성능을 제공하는 스케일아웃 볼륨입니다.

다음과 같은 경우에 FlexGroup 볼륨을 구성할 수 있습니다.

- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.
- SVM 관리자 권한이 아닌 클러스터 관리자 권한이 있습니다.

ONTAP 9.5부터 FlexGroup 볼륨은 ONTAP 9.5 이상 릴리즈에서 지원되지 않는 무한 확장 볼륨을 대체합니다.

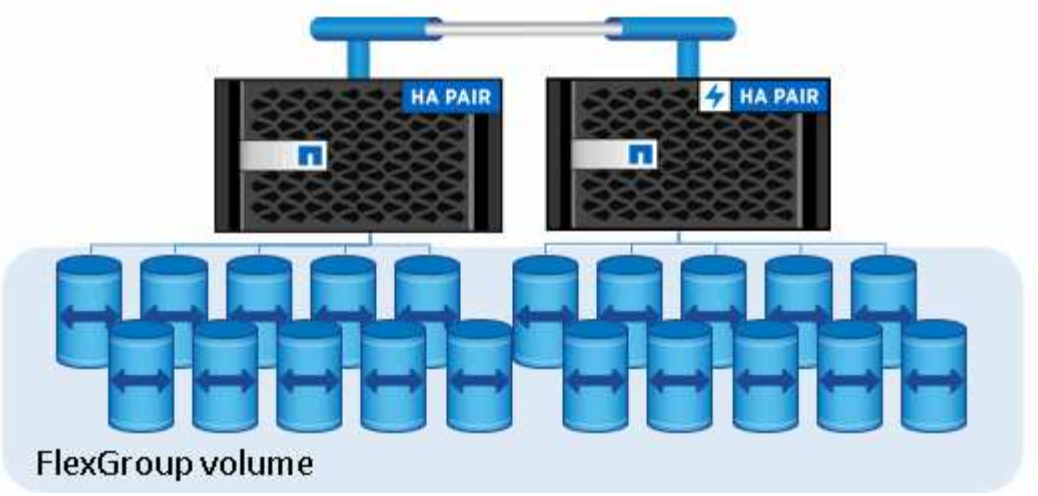
를 참조하십시오 "FlexGroup 볼륨에 대해 지원되고 지원되지 않는 구성입니다" 를 참조하십시오.

관련 정보

FlexVol 볼륨에 대한 개념 정보는 FlexGroup 볼륨에 적용됩니다. FlexVol 볼륨 및 ONTAP 기술에 대한 정보는 ONTAP 참조 라이브러리 및 TR(기술 보고서)에서 확인할 수 있습니다.

ONTAP FlexGroup 볼륨에 대해 알아보십시오

FlexGroup 볼륨은 자동 로드 분산 및 확장성과 함께 고성능을 제공하는 스케일아웃 NAS 컨테이너입니다. FlexGroup 볼륨에는 트래픽을 자동으로 투명하게 공유하는 여러 구성원 볼륨(구성 요소)이 포함되어 있습니다. _멤버 볼륨 _ 은(는) FlexGroup 볼륨을 구성하는 기본 FlexVol 볼륨입니다.



FlexGroup 볼륨은 다음과 같은 이점을 제공합니다.

- 높은 확장성

  구성원 볼륨 수가 노드 또는 클러스터의 제한을 초과하지 않는 한 하나의 클러스터에서 여러 FlexGroup 볼륨을 프로비저닝할 수 있습니다.

  ONTAP 9.12.1P2부터 단일 FlexGroup 볼륨의 최대 용량은 60PB이며, 10노드 클러스터에 4천억 개의 파일을 저장할 수 있습니다."대용량 지원이 활성화되었습니다" 대규모 볼륨 지원이 없으면 단일 FlexGroup 볼륨의 최대 용량은 20PB입니다.

  > 단일 FlexGroup 볼륨의 최대 용량은 60PB(200개 구성원 볼륨 x 300TB = 60PB)이지만 구성원 볼륨의 사용 용량이 80%(200개 구성원 볼륨 x 240TB = 48PB) 미만으로 유지될 때 최상의 성능을 얻을 수 있습니다.

- 고성능

  FlexGroup 볼륨은 클러스터의 리소스를 사용하여 처리량이 높고 지연 시간이 짧은 워크로드를 처리할 수 있습니다.

- 관리 기능의 단순화

  FlexGroup 볼륨은 FlexVol 볼륨과 비슷한 방식으로 관리할 수 있는 단일 네임스페이스 컨테이너입니다.

ONTAP FlexGroup 볼륨에 대해 지원되고 지원되지 않는 구성입니다

ONTAP 9의 FlexGroup 볼륨에서 지원되고 지원되지 않는 ONTAP 기능에 대해 알고 있어야 합니다.

ONTAP 9.18.1부터 지원되는 기능

- 중첩된 QoS 정책다음 객체 쌍에 대해 지원됩니다.
  - SVM에 포함된 SVM 및 FlexGroup 볼륨
  - 볼륨 내의 FlexGroup 볼륨 및 Qtree

ONTAP 9.16.1부터 지원되는 기능

- 고급 용량 밸런싱

ONTAP 9.15.1부터 지원되는 기능

- 자동 프로비저닝 기능 향상

ONTAP 9.14.1부터 지원되는 기능

- 스냅샷 태그 지정: 명령을 사용하여 FlexGroup 볼륨의 스냅샷에 대한 스냅샷 태그(SnapMirror 레이블 및 설명)를 생성, 수정 및 삭제할 `volume snapshot` 수 있습니다.

ONTAP 9.13.1 버전부터 지원되는 기능

- 자율 랜섬웨어 보호(ARP) 지원되는 다음 기능을 포함한 FlexGroup 볼륨의 경우:
  - FlexGroup 확장 운영: 새로운 구성원 볼륨이 자율적 랜섬웨어 방어 특성을 상속합니다.
  - FlexVol에서 FlexGroup로 전환: 능동적 자율 랜섬웨어 보호를 사용하여 FlexVol을 변환할 수 있습니다.
  - FlexGroup 재조정: 운영 중단 및 무중단 재조정 작업 중에 자율적 랜섬웨어 보호가 지원됩니다.
- 단일 FlexGroup 재조정 작업을 예약합니다.
- SnapMirror 팬아웃 FlexGroup 볼륨의 SVM DR과 관계 8개 사이트로 팬아웃 지원

ONTAP 9.12.1부터 지원되는 기능입니다

- FlexGroup 재조정
- SnapVault용 SnapLock
- SnapMirror 클라우드
- FabricPool, FlexGroup 및 SVM DR이 함께 작동합니다. (ONTAP 9.12.1 이전 버전에서는 이러한 기능 중 두 가지가 함께 작동하지만 세 가지 기능이 모두 함께 작동하지는 않습니다.)
- 대용량 지원 FlexGroup 볼륨 구성원 크기를 최대 100TB에서 최대 300TB로 늘립니다.

ONTAP 9.11.1부터 지원되는 기능입니다

- SnapLock 볼륨

  SnapLock는 FlexGroup 볼륨에서 다음 기능을 지원하지 않습니다.

  - 법적 증거 자료 보관
  - 이벤트 기반 보존
  - SnapVault용 SnapLock

FlexGroup 레벨에서 SnapLock를 구성합니다. 구성원 볼륨 수준에서 SnapLock를 구성할 수 없습니다.

- 클라이언트 비동기 디렉토리 삭제

ONTAP 9.10.1부터 지원되는 피처

- SVM DR 관계 내에서 FlexVol volume을 FlexGroup 볼륨으로 변환합니다
- FlexGroup 볼륨에 대한 SVM DR FlexClone 지원

ONTAP 9.9.1부터 지원되는 기능

- SVM 재해 복구

  SVM DR 관계에 있는 FlexGroup 볼륨의 클론 복제는 지원되지 않습니다.

- 최대 8개의 팬아웃 다리로 구성된 2개 이상의 SnapMirror 팬아웃 관계(A에서 B, A에서 C까지)입니다.

  FlexGroup 볼륨에 대한 SnapMirror 캐스케이드 및 팬아웃 관계를 생성할 때의 고려 사항

- 최대 2개 수준(A_BC)의 SnapMirror 계단식 관계

  FlexGroup 볼륨에 대한 SnapMirror 캐스케이드 및 팬아웃 관계를 생성할 때의 고려 사항

ONTAP 9.8부터 지원되는 기능

- FlexGroup SnapMirror 볼트 또는 UDP 대상에서 단일 파일 복원
  - 모든 지오메트리의 FlexGroup 볼륨에서 모든 지오메트리의 FlexGroup 볼륨으로 복원할 수 있습니다
  - 복구 작업당 하나의 파일만 지원됩니다
- 7-Mode 시스템에서 FlexGroup 볼륨으로 전환된 볼륨을 변환

  자세한 내용은 다음을 참조하세요."NetApp 지식 기반: 전환된 FlexVol FlexGroup 으로 변환하는 방법" .

- NFSv4.2
- 파일 및 디렉토리의 비동기식 삭제
- 파일 시스템 분석(FSA)
- FlexGroup를 VMware vSphere 데이터 저장소로 사용합니다
- 다음 기능을 포함하여 NDMP를 사용한 테이프 백업 및 복구에 대한 추가 지원:
  - NDMP RBE(재시작 가능한 백업 확장) 및 SSME(Snapshot Management Extension)
  - 환경 변수는 제외되고 multi_subtree_names는 FlexGroup 백업을 지원합니다
  - FlexGroup 백업에 대한 ignore_ctime_MTIME 환경 변수 도입
  - FlexGroup에서 0x2050 덤프 및 복구 세션의 일부인 ndmp_snap_recover 메시지를 사용하는 개별 파일 복구는 업그레이드 또는 복원 중에 중단됩니다.

ONTAP 9.7부터 지원되는 기능

- FlexClone 볼륨
- NFSv4 및 NFSv4.1
- pNFS를 사용합니다

- NDMP를 사용하여 테이프 백업 및 복구

  FlexGroup 볼륨에서 NDMP를 지원하려면 다음 사항을 염두에 두어야 합니다.

  - 확장 클래스 0x2050의 ndmp_snap_recover 메시지는 전체 FlexGroup 볼륨을 복구하는 데만 사용할 수 있습니다.

    FlexGroup 볼륨의 개별 파일을 복구할 수 없습니다.

  - FlexGroup 볼륨에 대해 NDMP RBE(재시작 가능한 백업 확장)가 지원되지 않습니다.
  - FlexGroup 볼륨에서는 환경 변수 exclude 및 multi_subtree_names가 지원되지 않습니다.
  - FlexVol와 FlexGroup 볼륨 간 데이터 전송에 대해 ndmpcopy 명령이 지원됩니다.

    Data ONTAP 9.7에서 이전 버전으로 되돌릴 경우 이전 전송의 증분 전송 정보가 유지되지 않으므로 되돌리기 후 기본 복사를 수행해야 합니다.

- VMware VAAI(vStorage APIs for Array Integration)
- FlexVol 볼륨을 FlexGroup 볼륨으로 변환
- FlexGroup 볼륨을 FlexCache 원본 볼륨으로 사용

ONTAP 9.6부터 지원되는 기능

- 지속적으로 사용 가능한 SMB 공유
- "MetroCluster 구성"
- FlexGroup 볼륨 이름 바꾸기('볼륨 이름 바꾸기' 명령)
- FlexGroup 볼륨 크기 축소 또는 축소('볼륨 크기' 명령)
- 탄력적인 사이징
- NetApp 애그리게이트 암호화(NAE)
- Cloud Volumes ONTAP

ONTAP 9.5부터 지원되는 기능입니다

- ODX 복사 오프로드
- 스토리지 레벨 액세스 가드
- SMB 공유에 대한 변경 알림 기능이 향상되었습니다

  변경 알림은 'changenotify' 속성이 설정된 상위 디렉토리의 변경 사항과 해당 상위 디렉토리의 모든 하위 디렉토리에 대한 변경 사항을 위해 전송됩니다.

- FabricPool
- 할당량 적용
- qtree 통계
- FlexGroup 볼륨의 파일에 대한 적응형 QoS
- FlexCache(캐시만 해당, FlexGroup as origin ONTAP 9.7에서 지원됨)

ONTAP 9.4부터 지원되는 기능

- FPolicy를 참조하십시오
- 파일 감사
- FlexGroup 볼륨에 대한 처리량(QoS Min) 및 적응형 QoS
- FlexGroup 볼륨의 파일에 대한 처리량 상한(QoS Max) 및 처리량 플로어(QoS Min

  'volume file modify' 명령을 사용하여 파일과 연결된 QoS 정책 그룹을 관리할 수 있습니다.
- SnapMirror의 제한 사항을 완화했습니다
- SMB 3.x 다중 채널

ONTAP 9.3 이하 버전에서 지원되는 기능

- 안티바이러스 구성
- SMB 공유에 대한 알림을 변경합니다

  알림은 'changenotify' 속성이 설정된 상위 디렉토리의 변경 사항에 대해서만 전송됩니다. 상위 디렉토리의 하위 디렉토리에 대한 변경 사항은 변경 알림이 전송되지 않습니다.
- Qtree
- 처리량 상한(QoS 최대)
- SnapMirror 관계에서 소스 FlexGroup 볼륨과 타겟 FlexGroup 볼륨을 확장합니다
- SnapVault 백업 및 복원
- 통합 데이터 보호 관계
- 자동 확장 옵션 및 자동 축소 옵션
- 인제스트 카운트를 인제스트했습니다
- 볼륨 암호화
- 애그리게이트 인라인 중복제거(볼륨 간 중복제거)
- NetApp 볼륨 암호화(NVE)
- SnapMirror 기술
- 스냅샷 수
- 디지털 자문업체
- 인라인 적응형 압축
- 인라인 중복제거
- 인라인 데이터 컴팩션
- AFF
- 할당량 보고
- NetApp Snapshot 기술
- SnapRestore 소프트웨어(FlexGroup 레벨)

- 하이브리드 애그리게이트
- 구성 요소 또는 구성원 볼륨 이동
- 사후 중복제거
- NetApp RAID-TEC 기술
- 애그리게이트당 정합성 보장 지점
- 동일한 SVM에서 FlexGroup를 FlexVol 볼륨과 공유

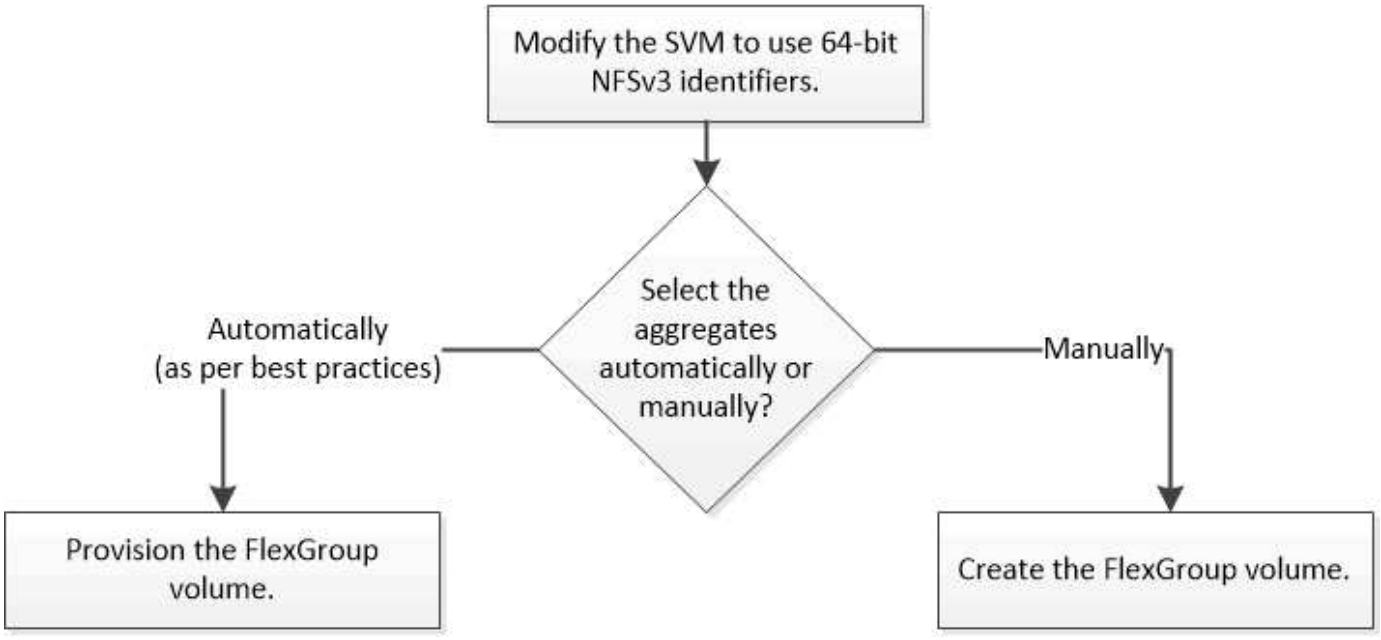
ONTAP 9에서 지원되지 않는 **FlexGroup** 볼륨 구성입니다

지원되지 않는 프로토콜입니다	지원되지 않는 데이터 보호 기능입니다	기타 지원되지 않는 ONTAP 기능입니다
• pNFS를 사용합니다 (ONTAP 9 .6 이하) • SMB 1.0 • SMB 투명한 페일오버 (ONTAP 9 .5 이하) • 산	• SnapLock 볼륨 (ONTAP 9.10.1 이하) • SMTape • SnapMirror 동기식 • FabricPools를 포함하는 FlexGroup 볼륨을 지원하는 SVM DR(ONTAP 9.11.1 이하)	• 원격 볼륨 섀도 복사본 서비스(VSS) • SVM 데이터 이동성

FlexGroup 볼륨 설정

ONTAP FlexGroup 볼륨 설정 워크플로

최적의 성능을 위한 모범 사례에 따라 ONTAP가 애그리게이트를 자동으로 선택하는 FlexGroup 볼륨을 프로비저닝하거나, 데이터 액세스를 위해 애그리게이트를 수동으로 선택하고 구성하여 FlexGroup 볼륨을 생성할 수 있습니다.



시작하기 전에

SVM에 대해 허용되는 프로토콜 목록에 NFS 및 SMB를 추가하여 SVM을 생성해야 합니다.

이 작업에 대해

4개 미만의 노드가 있는 클러스터에서만 FlexGroup 볼륨을 자동으로 프로비저닝할 수 있습니다. 노드가 4개 이상인 클러스터에서는 FlexGroup 볼륨을 수동으로 생성해야 합니다.

FlexGroups를 사용하여 **ONTAP SVM**에서 **64**비트 **NFSv3** 식별자 활성화

높은 파일 개수의 FlexGroup 볼륨을 지원하고 파일 ID 충돌을 방지하려면 FlexGroup 볼륨을 생성해야 하는 SVM에서 64비트 파일 식별자를 활성화해야 합니다.

단계

1. 고급 권한 수준 'Set-Privilege Advanced'에 로그인합니다
2. 64비트 NFSv3 FSID 및 파일 ID를 사용하도록 SVM을 수정합니다. 'vserver nfs modify -vserver svm_name -v3 -64bit-identifier enabled'

```
cluster1::*> vserver nfs modify -vserver vs0 -v3-64bit-identifiers
enabled

Warning: You are attempting to increase the number of bits used for
NFSv3
         FSIDs and File IDs from 32 to 64 on Vserver "vs0". This could
         result in older client software no longer working with the
volumes
         owned by Vserver "vs0".
Do you want to continue? {y|n}: y

Warning: Based on the changes you are making to the NFS server on
Vserver
         "vs0", it is highly recommended that you remount all NFSv3
clients
         connected to it after the command completes.
Do you want to continue? {y|n}: y
```

작업을 마친 후

모든 클라이언트를 다시 마운트해야 합니다. 이는 파일 시스템 ID가 변경되고 클라이언트가 NFS 작업을 시도할 때 오래된 파일 처리 메시지를 수신하기 때문에 필요합니다.

ONTAP FlexGroup 볼륨을 자동으로 프로비저닝합니다

FlexGroup 볼륨을 생성할 때 ONTAP에서 기본 로컬 계층(애그리게이트)을 선택하여 FlexGroup 볼륨을 자동으로 프로비저닝하도록 선택할 수 있습니다. 최적의 성능과 용량을 위한 Best Practice에 따라 로컬 계층을 선택합니다.

시작하기 전에

클러스터의 각 노드에는 하나 이상의 로컬 계층이 있어야 합니다.

> 비활성 데이터를 계층화할 FlexGroup 볼륨을 생성할 경우 각 노드에 FabricPool가 활성화된 로컬 계층이 하나 이상 있어야 합니다.

이 작업에 대해

ONTAP는 각 노드에서 사용 가능한 공간이 가장 많은 2개의 로컬 계층을 선택하여 FlexGroup 볼륨을 생성합니다. 2개의 로컬 계층을 사용할 수 없는 경우 ONTAP는 노드당 하나의 로컬 계층을 선택하여 FlexGroup 볼륨을 생성합니다.

ONTAP 9.15.1부터 FlexGroup 볼륨을 자동으로 프로비저닝할 때 ONTAP는 BP(균형 잡힌 배치)를 사용하여 로컬 계층과 FlexGroup 구성원(구성) 볼륨 레이아웃을 선택합니다. BP의 한 가지 측면은 '없음' 보장(씬 프로비저닝) FlexGroup 볼륨을 생성할 때 로컬 계층의 오버 프로비저닝을 제한하는 방법입니다. 전체 FlexGroup 볼륨의 크기는 로컬 계층에서 사용 가능한 공간의 양에 따라 제한되지만, 이 제한은 '볼륨'이 보장하는(씩 프로비저닝된) FlexGroup 볼륨에 대한 제한보다 큽니다. REST API 또는 ONTAP CLI를 사용하여 FlexGroup 볼륨을 생성할 `auto-provision-as` 경우 이 제한으로 인해 공간이 부족하여 프로비저닝이 실패할 수 있습니다. 더 작은 FlexGroup 볼륨을 생성하거나 매개 변수를 사용하면 이러한 문제를 방지할 수 "FlexGroup 볼륨을 생성하고 로컬 계층을 수동으로 선택합니다" `aggr-list` 있습니다.

단계

1. FlexGroup 볼륨 프로비저닝:

   ```
   volume create -vserver svm_name -volume fg_vol_name -auto-provision-as
   flexgroup -size fg_size [-encrypt true] [-qos-policy-group
   qos_policy_group_name] [-support-tiering true] [-granular-data advanced]
   ```

   ONTAP 9.16.1부터 (`-granular-data advanced`CLI에서 를 활성화하여 파일이 10GB보다 클 때 여러 FlexGroup 멤버 볼륨에 걸쳐 데이터를 쓸 수 "고급 용량 밸런싱"있습니다.

   ONTAP 9.5부터 FabricPool를 사용하는 로컬 계층에 FlexGroup 볼륨을 생성할 수 있습니다. FabricPool가 활성화된 상태에서 로컬 계층에서 FlexGroup 볼륨을 자동으로 프로비저닝하려면 매개 변수 를 로 `true` 설정해야 `-support-tiering` 합니다. FabricPool에 대해서는 볼륨 보증이 항상 으로 설정되어야 `none` 합니다. FlexGroup 볼륨에 대한 계층화 정책 및 계층화 최소 냉각 기간을 지정할 수도 있습니다.

   "디스크 및 애그리게이트 관리"

   FlexGroup 볼륨의 처리량 한도(QoS Max)를 지정할 수 있습니다. 이로 인해 FlexGroup 볼륨이 사용할 수 있는 성능 리소스가 제한됩니다. ONTAP 9.4부터 FlexGroup 볼륨에 대한 처리량 층(QoS Min) 및 적응형 QoS를 지정할 수 있습니다.

   "성능 관리"

   FlexGroup 볼륨에서 암호화를 활성화하려면 매개 변수를 로 `true` 설정할 수 `-encrypt` 있습니다. 암호화된 볼륨을 만들려면 볼륨 암호화 라이센스와 키 관리자를 설치해야 합니다.

   > 생성 시 FlexGroup 볼륨에서 암호화를 활성화해야 합니다. 기존 FlexGroup 볼륨에서는 암호화를 설정할 수 없습니다.

   "유휴 데이터의 암호화"

   "size" 매개 변수는 FlexGroup 볼륨의 크기를 KB, MB, GB, TB 또는 PB 단위로 지정합니다.

다음 예에서는 400TB 크기의 FlexGroup 볼륨을 프로비저닝하는 방법을 보여줍니다.

```
cluster-1::> volume create -vserver vs0 -volume fg –auto-provision-as
flexgroup -size 400TB
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

다음 예에서는 처리량 상한에 대한 QoS 정책 그룹을 생성하는 방법과 FlexGroup 볼륨에 적용하는 방법을 보여줍니다.

```
cluster1::> qos policy-group create -policy group pg-vs1 -vserver vs1
-max-throughput 5000iops
```

```
cluster-1::> volume create -vserver vs0 -volume fg –auto-provision-as
flexgroup -size 400TB -qos-policy-group pg-vs1
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

다음 예에서는 FabricPool가 활성화된 상태에서 로컬 계층에서 400TB 크기의 FlexGroup 볼륨을 프로비저닝하는 방법을 보여줍니다.

```
cluster-1::> volume create -vserver vs0 -volume fg –auto-provision-as
flexgroup -size 400TB -support-tiering true -tiering-policy auto
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

FlexGroup 볼륨은 클러스터의 각 노드에 8개의 구성원 볼륨으로 생성됩니다. 구성원 볼륨은 각 노드에서 가장 큰 두 로컬 계층 간에 균등하게 분산됩니다.

기본적으로 FlexGroup 볼륨은 AFF 시스템을 제외하고 '볼륨' 공간 보장 설정으로 생성됩니다. AFF 시스템의 경우 기본적으로 FlexGroup 볼륨은 'none' 공간 보장으로 생성됩니다.

2. 접합 경로로 FlexGroup 볼륨을 마운트합니다.

   ```
   volume mount -vserver vserver_name -volume vol_name -junction-path
   junction_path
   ```

   ```
   cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg2
   ```

작업을 마친 후

클라이언트에서 FlexGroup 볼륨을 마운트해야 합니다.

ONTAP 9.6 이하 버전을 실행 중이고 SVM(스토리지 가상 시스템)에 NFSv3 및 NFSv4가 모두 구성되어 있는 경우 클라이언트에서 FlexGroup 볼륨을 마운트하지 못할 수 있습니다. 이러한 경우 클라이언트에서 FlexGroup 볼륨을 마운트할 때 NFS 버전을 명시적으로 지정해야 합니다.

```
# mount -t nfs -o vers=3 192.53.19.64:/fg2 /mnt/fg2
# ls /mnt/fg2
file1  file2
```

관련 정보

- "QoS 정책 - 그룹 생성"

ONTAP FlexGroup 볼륨을 생성합니다

FlexGroup 볼륨을 생성할 로컬 계층(애그리게이트)을 수동으로 선택한 다음, 각 로컬 계층에 구성원 볼륨(구성요소) 수를 지정하여 FlexGroup 볼륨을 생성할 수 있습니다.

또는 최적의 성능과 용량을 위한 Best Practice에 따라 ONTAP에서 구성원 볼륨 수를 설정하도록 로컬 계층을 선택하여 ONTAP를 "자동으로 프로비저닝"FlexGroup 볼륨으로 설정할 수 있습니다.

이 작업에 대해

FlexGroup 볼륨을 생성하기 위해 로컬 계층에 필요한 공간을 알고 있어야 합니다.

FlexGroup 볼륨에서 최상의 성능 결과를 얻으려면 FlexGroup 볼륨을 생성할 때 다음 지침을 고려해야 합니다.

- FlexGroup 볼륨은 동일한 하드웨어 시스템에 있는 로컬 계층을 사용해야 합니다.

  동일한 하드웨어 시스템을 사용하면 FlexGroup 볼륨 전체에서 예측 가능한 성능을 제공하는 데 도움이 됩니다. 참고: C-시리즈 r1과 C-시리즈 r2 시스템은 동일한 시스템이 아닙니다. 예를 들어, AFF C80 r1과 AFF C80 r2는 동일하지 않습니다.

- FlexGroup 볼륨은 동일한 디스크 유형 및 RAID 그룹 구성을 사용하여 로컬 계층으로 확장되어야 합니다.

  일관된 성능을 얻으려면 모든 로컬 계층이 SSD, 모든 HDD 또는 All Flash Pool(하이브리드) 로컬 계층으로 구성되도록 해야 합니다. 또한 로컬 계층의 FlexGroup 볼륨 전체에 동일한 수의 드라이브와 RAID 그룹이 있어야 합니다.

- FlexGroup 볼륨은 클러스터의 일부를 포괄할 수 있습니다.

FlexGroup 볼륨을 전체 클러스터로 구성할 필요는 없지만 사용할 수 있는 하드웨어 리소스를 더 많이 활용할 수 있습니다.

- FlexGroup 볼륨을 생성할 때 FlexGroup 볼륨이 구축되는 로컬 계층에 다음과 같은 특성이 있는 것이 가장 좋습니다.
  - 특히 씬 프로비저닝을 사용하는 경우, 여러 로컬 계층에서 거의 동일한 양의 사용 가능한 공간을 사용할 수 있어야 합니다.
  - FlexGroup 볼륨을 생성한 후 사용 가능한 공간의 약 3%를 로컬 계층 메타데이터용으로 예약해야 합니다.
- FAS 시스템의 경우 노드당 로컬 계층이 2개인 것이 가장 좋으며 AFF 시스템의 경우 FlexGroup 볼륨에 대해 노드당 로컬 계층이 하나씩 있어야 합니다.
- 각 FlexGroup 볼륨에 대해 FAS 시스템의 두 개 이상의 로컬 계층과 AFF 시스템의 하나 이상의 로컬 계층에 분산되는 8개 이상의 구성원 볼륨을 생성해야 합니다.
- ONTAP 9.9.1부터 2개 이상의 FlexGroup 볼륨에 대한 SnapMirror 팬아웃 관계가 지원되며 최대 8개의 팬아웃 레그를 지원합니다. System Manager는 계단식 SnapMirror FlexGroup 볼륨 관계를 지원하지 않습니다.
- System Manager를 사용하여 FlexGroup 볼륨을 생성하면 ONTAP FlexGroup 볼륨을 생성하는 데 필요한 로컬 계층을 자동으로 선택합니다.
- ONTAP 9.8부터는 스토리지 용량 할당 시 QoS가 기본적으로 사용하도록 설정됩니다. 프로비저닝 프로세스 도중 또는 나중에 QoS를 사용하지 않도록 설정하거나 사용자 지정 QoS 정책을 선택할 수 있습니다.

시작하기 전에

- ONTAP 9.13.1부터 용량 분석 및 활동 추적이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 `volume create` 또는 `-activity-tracking-state` 를 로 설정하여 `on` 명령을 `-analytics-state` 실행합니다.

  용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 "파일 시스템 분석 설정". 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

시스템 관리자

시스템 관리자를 사용하여 FlexGroup 볼륨을 생성할 수 있습니다.

단계

1. *저장소 > 볼륨*으로 이동하여 선택하십시오. + Add .
2. 볼륨 추가 창에서 볼륨 이름과 크기를 입력한 다음 *기타 옵션*을 선택합니다.
3. 저장 및 최적화 섹션에서 *클러스터 전체에 볼륨 데이터 배포(FlexGroup)*를 선택합니다.

> ONTAP 9.8 이상을 실행 중인 경우 QoS를 비활성화하거나 사용자 지정 QoS 정책을 선택하려면 * 추가 옵션 * 을 클릭한 다음 * 스토리지 및 최적화 * 에서 * 성능 서비스 수준 * 을 선택합니다.

4. 해당 볼륨에 대한 나머지 정보를 입력하고 *저장*을 선택하세요.

CLI를 참조하십시오

1. FlexGroup 볼륨을 생성합니다.

```
volume create -vserver <svm_name> -volume <flexgroup_name> -aggr
-list aggr1,aggr2,.. -aggr-list-multiplier <constituents_per_aggr>
-size <fg_size> [-encrypt true] [-qos-policy-group
qos_policy_group_name] [-granular-data advanced]
```

   - `-aggr-list`매개 변수는 FlexGroup 구성원 볼륨에 사용할 로컬 계층의 목록을 지정합니다.

     FlexGroup 볼륨에서 일관된 성능을 얻으려면 모든 로컬 계층에서 동일한 디스크 유형 및 RAID 그룹 구성을 사용해야 합니다.

   - `-aggr-list-multiplier`매개 변수는 매개 변수와 함께 나열된 각 로컬 계층에 생성될 구성원 볼륨 수를 `-aggr-list` 지정합니다.

     '-aggr-list-multiplier' 파라미터의 기본값은 4이다.

   - "size" 매개 변수는 FlexGroup 볼륨의 크기를 KB, MB, GB, TB 또는 PB 단위로 지정합니다.
   - ONTAP 9.16.1부터 (`-granular-data advanced`CLI에서 를 활성화하여 파일이 10GB보다 클 때 여러 FlexGroup 멤버 볼륨에 걸쳐 데이터를 쓸 수 "고급 용량 밸런싱"있습니다.
   - ONTAP 9.5부터 FabricPool가 활성화된 로컬 계층을 사용하여 FlexGroup 볼륨을 생성할 수 있습니다.

     FabricPool에 대한 FlexGroup 볼륨을 생성하려면 매개 변수로 지정한 모든 로컬 계층에 `-aggr-list` FabricPool가 활성화되어 있어야 합니다. FabricPool를 사용할 경우 볼륨 보장은 항상 로 설정해야 `none` 합니다. FlexGroup 볼륨에 대한 계층화 정책 및 계층화 최소 냉각 기간을 지정할 수도 있습니다.

     디스크 및 애그리게이트 관리

   - ONTAP 9.4부터 FlexGroup 볼륨에 대한 처리량 층(QoS Min) 및 적응형 QoS를 지정할 수 있습니다.

     "성능 관리"

- FlexGroup 볼륨에 대해 처리량 상한(QoS Max)을 지정하여 FlexGroup 볼륨이 사용할 수 있는 성능 리소스를 제한할 수 있습니다.
- FlexGroup 볼륨에서 암호화를 활성화하려면 매개 변수를 로 `true` 설정할 수 `-encrypt` 있습니다.

  암호화된 볼륨을 만들려면 볼륨 암호화 라이센스와 키 관리자를 설치해야 합니다.

  > 생성 시 FlexGroup 볼륨에서 암호화를 활성화해야 합니다. 기존 FlexGroup 볼륨에서는 암호화를 설정할 수 없습니다.

  "유휴 데이터의 암호화"

```
cluster-1::> volume create -vserver vs0 -volume fg2 -aggr-list
aggr1,aggr2,aggr3,aggr1 -aggr-list-multiplier 2 -size 500TB

Warning: A FlexGroup "fg2" will be created with the following number
of constituents of size 62.50TB: 8.
Do you want to continue? {y|n}: y

[Job 43] Job succeeded: Successful
```

이전 예에서는 FabricPool에 대한 FlexGroup 볼륨을 생성하려면 모든 로컬 계층(aggr1, aggr2 및 aggr3)에 FabricPool가 활성화되어 있어야 합니다. 연결 경로를 사용하여 FlexGroup 볼륨 마운트: `volume mount -vserver vserver_name -volume vol_name -junction-path junction_path`

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg
```

작업을 마친 후

클라이언트에서 FlexGroup 볼륨을 마운트해야 합니다.

ONTAP 9.6 이하 버전을 실행 중이고 SVM(스토리지 가상 시스템)에 NFSv3 및 NFSv4가 모두 구성되어 있는 경우 클라이언트에서 FlexGroup 볼륨을 마운트하지 못할 수 있습니다. 이러한 경우 클라이언트에서 FlexGroup 볼륨을 마운트할 때 NFS 버전을 명시적으로 지정해야 합니다.

```
# mount -t nfs -o vers=3 192.53.19.64:/fg /mnt/fg2
# ls /mnt/fg2
file1  file2
```

관련 정보

"NetApp 기술 보고서 4571: NetApp FlexGroup 모범 사례 및 구현 가이드"

FlexGroup 볼륨 관리

ONTAP FlexGroup 볼륨의 공간 사용량을 모니터링합니다

FlexGroup 볼륨 및 구성 구성요소를 확인하고 FlexGroup 볼륨에서 사용하는 공간을 모니터링할 수 있습니다.

이 작업에 대해

ONTAP 9.6부터 탄력적인 사이징을 지원합니다. ONTAP는 여유 공간이 있는 FlexGroup 볼륨의 다른 구성요소를 축소함으로써 FlexGroup 볼륨의 구성요소를 자동으로 확장하며, 공간이 부족한 경우 볼륨의 구성요소를 자동으로 이동합니다. 탄력적인 사이징은 하나 이상의 FlexGroup 구성 볼륨에 공간이 부족하여 생성되는 공간 부족 오류를 방지합니다.

ONTAP 9.9.1부터 FlexGroup 볼륨에 대한 논리적 공간 보고 및 적용이 가능합니다. 자세한 내용은 을 "볼륨에 대한 논리적 공간 보고 및 적용"참조하십시오.

단계

1. FlexGroup 볼륨 및 해당 구성 요소에서 사용하는 'volume show-vserver vserver_name-volume-style-extended [FlexGroup|flexgroup-fod요소]'를 확인하십시오

```
cluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs1       fg1          -            online     RW         500GB
207.5GB   56%
```

```
ccluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup-
constituent
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs1       fg1__0001    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0002    aggr1        online     RW      31.25GB
12.98GB   56%
vs1       fg1__0003    aggr1        online     RW      31.25GB
13.00GB   56%
vs1       fg1__0004    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0005    aggr1        online     RW      31.25GB
13.00GB   56%
vs1       fg1__0006    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0007    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0008    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0009    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0010    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0011    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0012    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0013    aggr3        online     RW      31.25GB
12.95GB   56%
vs1       fg1__0014    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0015    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0016    aggr1        online     RW      31.25GB
13.01GB   56%
16 entries were displayed.
```

FlexGroup 볼륨의 공간 사용을 모니터링하는 데 사용되는 사용 가능한 공간과 백분율 공간을 사용할 수 있습니다.

ONTAP FlexGroup 볼륨의 크기를 늘립니다

FlexGroup 볼륨의 크기를 늘리려면 FlexGroup 볼륨의 모든 기존 멤버 볼륨(구성 요소)에

용량을 추가하거나 새로운 멤버 볼륨으로 FlexGroup 볼륨을 확장하면 됩니다. FlexGroup 볼륨은 200개를 초과하는 멤버 볼륨을 가질 수 없습니다.

필요한 경우 FlexGroup 볼륨 내의 개별 볼륨 크기를 늘릴 수도 있습니다.

시작하기 전에

Aggregate에 충분한 공간이 있어야 합니다.

이 작업에 대해

공간을 더 추가하려면 FlexGroup 볼륨의 전체 크기를 늘릴 수 있습니다. FlexGroup 볼륨의 크기를 늘리면 FlexGroup 볼륨의 기존 구성원 볼륨의 크기가 조정됩니다.

성능을 향상시키려면 FlexGroup 볼륨을 확장할 수 있습니다. 다음과 같은 경우 FlexGroup 볼륨을 확장하고 새 구성원 볼륨을 추가할 수 있습니다.

- 클러스터에 새 노드가 추가되었습니다.
- 기존 노드에 새 로컬 계층(애그리게이트)이 생성되었습니다.
- FlexGroup 볼륨의 기존 구성원 볼륨이 하드웨어의 최대 FlexVol 크기(100TB 또는 300TB(가 활성화된 경우)에 도달했으므로 "대용량 지원"구성원 볼륨을 추가하지 않으면 FlexGroup 볼륨의 크기를 조정할 수 없습니다.

> 더 많은 멤버를 포함하도록 FlexGroup 볼륨을 수정하는 경우 이전에 생성된 스냅샷은 "부분"으로 간주되며 클라이언트에서만 액세스할 수 있습니다. `.snapshot` 디렉토리 또는 이전 버전 탭.
>
> 스냅샷이 "부분"으로 간주되면 SnapRestore 작업에 사용할 수 없습니다. 그러나 부분 스냅샷을 사용하여 개별 파일을 복원할 수 있습니다. `.snapshot` 디렉토리 또는 이전 버전 탭.

ONTAP 9.3 이전 릴리즈에서는 SnapMirror 관계가 설정된 후 FlexGroup 볼륨을 확장하지 마십시오. ONTAP 9.3 이전의 릴리즈에서 SnapMirror 관계를 끊은 후 소스 FlexGroup 볼륨을 확장하는 경우 대상 FlexGroup 볼륨에 대한 기본 전송을 다시 수행해야 합니다. ONTAP 9.3부터 SnapMirror 관계에 있는 FlexGroup 볼륨을 확장할 수 있습니다.

단계

1. 필요에 따라 FlexGroup 볼륨의 용량 또는 성능을 늘려서 FlexGroup 볼륨의 크기를 늘립니다.

를 증가하려면…	다음을 수행하십시오.
FlexGroup 볼륨의 용량입니다	FlexGroup 볼륨의 모든 멤버 볼륨 크기를 조정합니다. `volume modify -vserver <svm_name> -volume <fg_name> -size <new_size>`

FlexGroup 볼륨의 성능입니다	새 구성원 볼륨(구성 요소)을 추가하여 FlexGroup 볼륨 확장: 'volume expand-vserver vserver_name-volume fg_name-aggr-list 집계 이름,... [-aggr-list-multiplier f구성요소_per_aggr]' '-aggr-list-multiplier' 파라미터의 기본값은 1이다. 를 사용하여 FlexGroup 볼륨을 확장할 "FabricPool"경우 모든 로컬 계층(애그리게이트)을 동일한 클라우드 계층에 연결해야 합니다.

기존 애그리게이트(로컬 계층) 또는 구성원 볼륨이 최대 용량(각각 100/300TB 또는 20억 개의 파일)에 도달하지 않았다면 구성원 볼륨을 추가하는 대신 FlexGroup 볼륨의 전체 크기를 늘리는 것이 더 낫습니다.

기존 볼륨 크기 또는 파일 수를 늘릴 수 없거나 FlexGroup를 새 하드웨어로 확장하는 경우에만 볼륨 확장을 사용하십시오. 일관된 성능을 보장하려면 모든 노드에 동일한 수의 구성원 볼륨을 추가해야 합니다. 예를 들어, 기존 FlexGroup 볼륨에 노드당 4개의 구성원 볼륨이 있는 8개의 구성원 볼륨이 있는 경우 노드당 두 개의 구성원을 추가하면 구성원 볼륨 12개가 되고 노드당 6개의 구성원 볼륨이 됩니다.

새 노드에 새 구성원을 추가할 때 기존 노드와 같이 노드당 구성원 볼륨의 일관된 수를 유지하십시오. 예를 들어, 기존 FlexGroup 볼륨에 노드당 4개의 구성원 볼륨이 있는 8개의 구성원 볼륨이 있는 경우 FlexGroup 볼륨을 새 노드로 확장할 경우 4개의 구성원 볼륨을 추가하여 12개의 구성원 FlexGroup 볼륨을 추가해야 합니다.

FlexGroup 볼륨에 새 멤버를 추가하면 빈 새 멤버 볼륨을 사용하기 위해 수집 휴리스틱이 변경되며, 새 멤버 볼륨이 기존 멤버 볼륨과 밸런싱될 때까지 새 데이터 수집의 전체 시스템 성능에 영향을 미칠 수 있습니다.

예

- 기존 구성원 볼륨의 용량을 늘리는 예 *

다음 예에서는 FlexGroup 볼륨 volX에 20TB 공간을 추가하는 방법을 보여 줍니다.

```
cluster1::> volume modify -vserver svm1 -volume volX -size +20TB
```

FlexGroup 볼륨에 16개의 구성원 볼륨이 있는 경우 각 구성원 볼륨의 공간이 1.25TB씩 증가합니다.

- 새 구성원 볼륨을 추가하여 성능을 향상시키는 예 *

다음 예에서는 FlexGroup 볼륨에 기본 로컬 계층(집계) 각각에 2개씩 총 4개의 추가 멤버 볼륨을 추가하는 방법을 보여줍니다. `fg1` :

```
cluster1::> volume expand -vserver svm1 -volume fg1 -aggr-list aggr1,aggr2
-aggr-list-multiplier 2
```

새 구성원 볼륨의 크기는 기존 구성원 볼륨의 크기와 동일합니다.

개별 볼륨의 크기를 늘리세요

FlexGroup 볼륨에서 개별 멤버 볼륨의 크기를 늘리려면 다음을 사용할 수 있습니다. `volume resize` 명령.

단계

1. 단일 FlexGroup 멤버 볼륨의 크기를 늘리세요.

   ```
   volume size -volume <volume_name> -vserver <svm1> -new-size <new_size>
   ```

   다음 예제에서는 FlexGroup 멤버 볼륨 FG_0003의 크기를 3.7GB로 늘립니다.

   ```
   volume size -volume FG__0003 -vserver svm1 -new-size 3.7GB
   vol size: Volume "svm1:FG__0003" size set to 3.70g.
   ```

ONTAP FlexGroup 볼륨의 크기를 줄입니다

ONTAP 9.6부터 FlexGroup 볼륨의 크기를 현재 크기보다 작은 값으로 조정하여 볼륨에서 사용되지 않는 공간을 확보할 수 있습니다. FlexGroup 볼륨의 크기를 줄일 경우 ONTAP는 모든 FlexGroup 구성요소의 크기를 자동으로 조정합니다.

단계

1. 현재 FlexGroup 볼륨 크기 확인: 'volume size - vserver_vserver_name_-volume_fg_name_'
2. FlexGroup 볼륨의 크기를 줄입니다. `volume size -vserver` *`vserver_name`* `-volume` *`fg_name new_size`*

   새 크기를 지정할 때 FlexGroup 볼륨의 현재 크기가 축소되는 빼기 기호(-)를 사용하여 현재 크기보다 작은 값 또는 음수 값을 지정할 수 있습니다.

   > ⓘ 볼륨('볼륨 자동 크기 조정' 명령)에 대해 자동 축소가 활성화된 경우 최소 자동 크기 조정이 볼륨의 새 크기로 설정됩니다.

   다음 예에서는 volX라는 FlexGroup 볼륨의 현재 볼륨 크기를 표시하고 볼륨을 10TB로 조정합니다.

   ```
   cluster1::> volume size -vserver svm1 -volume volX
   (volume size)
   vol size: FlexGroup volume 'svm1:volX' has size 15TB.

   cluster1::> volume size -vserver svm1 -volume volX 10TB
   (volume size)
   vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
   ```

   다음 예에서는 volX라는 FlexGroup 볼륨의 현재 볼륨 크기를 표시하고 볼륨의 크기를 5TB까지 줄여 줍니다.

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX -5TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

크기를 자동으로 늘리거나 줄일 수 있도록 **ONTAP FlexGroup** 볼륨을 구성합니다

ONTAP 9.3부터는 현재 필요한 공간에 따라 FlexGroup 볼륨이 자동으로 증가 및 축소되도록 구성할 수 있습니다.

시작하기 전에

FlexGroup 볼륨이 온라인 상태여야 합니다.

이 작업에 대해

FlexGroup 볼륨은 다음 두 가지 모드로 자동 조정할 수 있습니다.

- 자동으로 볼륨의 크기를 늘립니다('확대' 모드).

  자동 증가를 통해 aggregate에서 공간을 더 많이 제공할 수 있다면 FlexGroup 볼륨의 공간이 부족해지는 것을 방지할 수 있습니다. 볼륨의 최대 크기를 구성할 수 있습니다. 증가값은 사용된 공간의 현재 양과 설정된 임계값을 기준으로 볼륨에 기록되는 데이터의 양을 기준으로 자동으로 트리거됩니다.

  기본적으로 볼륨을 확장할 수 있는 최대 크기는 자동 확장이 설정된 크기의 120%입니다. 볼륨이 이보다 더 크게 증가할 수 있도록 해야 하는 경우 볼륨에 대한 최대 크기를 적절하게 설정해야 합니다.

- 볼륨의 크기를 자동으로 축소합니다('grow_shrink' 모드).

  자동 축소는 볼륨이 필요한 크기보다 커지는 것을 방지하여 Aggregate의 공간을 다른 볼륨에서 사용할 수 있도록 합니다.

  자동 축소는 자동 증가 와 함께 사용할 경우에만 변화하는 공간 요구를 충족할 수 있으며 단독으로 사용할 수는 없습니다. 자동 축소가 활성화되면 ONTAP는 볼륨의 축소 동작을 자동으로 관리하여 자동 증가 및 자동 축소 작업이 무한 루프를 방지합니다.

볼륨이 증가하면 포함할 수 있는 최대 파일 수가 자동으로 증가할 수 있습니다. 볼륨이 축소되면 포함할 수 있는 최대 파일 수가 변경되지 않고 그대로 남아 있으며 볼륨은 현재 최대 파일 수에 해당하는 크기보다 자동으로 축소될 수 없습니다. 따라서 볼륨을 원래 크기로 자동 축소하지 못할 수 있습니다.

단계

1. 볼륨 자동 크기 조정 - vserver_name - volume vol_name - mode [grow | grow_shrink]'가 자동으로 크기 증가 및 축소되도록 볼륨을 구성합니다

   또한 볼륨 증가 또는 축소에 대한 최대 크기, 최소 크기 및 임계값을 지정할 수 있습니다.

   다음 명령은 볼륨에 대한 자동 크기 변경을 활성화합니다. `fg1` . 70%가 차면 볼륨이 최대 5TB까지 확장되도록

구성됩니다.

```
cluster1::> volume autosize -volume fg1 -mode grow -maximum-size 5TB
-grow-threshold-percent 70
vol autosize: volume "vs_src:fg1" autosize settings UPDATED.
```

ONTAP FlexGroup 볼륨에서 디렉토리를 비동기적으로 삭제합니다.

ONTAP 9.8부터 Linux 및 Windows 클라이언트 공유에서 디렉터리를 비동기적으로(즉, 백그라운드에서) 삭제할 수 있습니다. 클러스터 및 SVM 관리자는 FlexVol 및 FlexGroup 볼륨 모두에서 비동기 삭제 작업을 수행할 수 있습니다.

이 작업에 대해

고급 권한 모드를 사용하는 클러스터 관리자 또는 SVM 관리자여야 합니다.

ONTAP 9.8부터 ONTAP CLI를 사용하여 비동기 삭제 기능을 사용할 수 있습니다. ONTAP 9.9.1부터 이 기능을 시스템 관리자와 함께 사용할 수 있습니다. 이 프로세스에 대한 자세한 내용은 을 "FSA에서 ONTAP 분석을 기반으로 시정 조치를 취하세요"참조하십시오.

ONTAP 9.11.1부터 스토리지 관리자는 볼륨에 대한 권한을 부여하여 NFS 및 SMB 클라이언트가 비동기식 삭제 작업을 수행할 수 있도록 할 수 있습니다. 자세한 내용은 을 "디렉토리를 비동기적으로 삭제하는 클라이언트 권한을 관리합니다 "참조하십시오.

당신은 사용할 수 있습니다 `volume file async-delete show` 진행 중인 비동기 삭제 작업의 상태를 확인하는 명령이 추가되었으며, ONTAP 9.17.1부터는 클라이언트에서 실행된 비동기 삭제 작업의 상태도 표시됩니다.

디렉터리를 비동기적으로 삭제

시스템 관리자나 ONTAP CLI를 사용하여 디렉토리를 비동기적으로 삭제할 수 있습니다.

시스템 관리자

ONTAP 9.10.1부터 시작합니다	**ONTAP 9.9.1**에서
1. *저장소 > 볼륨*을 선택하고 원하는 볼륨 이름을 선택합니다. 2. 개별 볼륨 페이지에서 파일 시스템 탭을 선택한 다음 탐색기 탭을 선택합니다. 3. 탐색기 보기에서 원하는 디렉토리를 선택합니다. 4. 삭제하려면 파일이나 폴더 위에 마우스를 올려놓고 삭제를 클릭합니다. 옵션이 나타납니다. 한 번에 하나의 개체만 삭제할 수 있습니다. 디렉토리와 파일이 삭제되면 새 스토리지 용량 값이 즉시 표시되지 않습니다.	1. 스토리지 > 볼륨 * 을 선택합니다. 2. 원하는 볼륨을 선택한 다음 * Explorer * 를 선택합니다. 3. 탐색기 보기에서 원하는 디렉토리를 선택합니다. 4. 삭제하려면 파일이나 폴더 위에 마우스를 올려놓고 삭제를 클릭합니다. 옵션이 나타납니다.

CLI를 참조하십시오

*CLI를 사용하여 비동기 삭제를 수행합니다 *

1. 고급 권한 모드 시작:

   세트 프리빌리지 고급

2. FlexVol 또는 FlexGroup 볼륨에서 디렉토리 삭제:

   ```
   volume file async-delete start -vserver <SVM_name> -volume <volume_name>
   -path <file_path> -throttle <throttle>
   ```

   최소 제한 값은 10이고, 최대 값은 100,000이며, 기본값은 5000입니다. 제한 값이 낮을수록 리소스를 적게 사용하므로 삭제 속도가 느려질 수 있고, 제한 값이 높을수록 리소스를 많이 사용하지만 삭제 속도가 빨라질 수 있습니다.

   다음 예제에서는 d1 이라는 디렉터리에 있는 d2 라는 디렉터리를 삭제합니다.

   ```
   cluster::*> volume file async-delete start -vserver vs1 -volume vol1
   -path d1/d2
   ```

3. (선택 사항) 진행 중인 비동기 삭제 작업의 상태를 확인하세요.

   '볼륨 파일 비동기 삭제 표시'

4. 디렉토리가 삭제되었는지 확인합니다.

   이벤트 로그 쇼

다음 예제에서는 디렉터리가 성공적으로 삭제되었을 때 이벤트 로그의 출력을 보여 줍니다.

```
cluster::*> event log show

Time                 Node              Severity      Event
-------------------- ----------------- -------------
---------------------------
7/7/2025 09:04:04    cluster-vsim      NOTICE
asyncDelete.message.success: Async delete job on path d1/d2 of
volume (MSID: 2162149232) was completed. Number of files deleted: 7,
Number of directories deleted: 5. Total number of bytes deleted:
135168.
```

에 대한 자세한 내용은 `event log show` "ONTAP 명령 참조입니다"을 참조하십시오.

디렉토리 삭제 작업 취소

1. 고급 권한 모드 시작:

   세트 프리빌리지 고급

2. 디렉토리 삭제가 진행 중인지 확인합니다.

   '볼륨 파일 비동기 삭제 표시'

   디렉토리의 SVM, 볼륨, jobid 및 경로가 표시되면 작업을 취소할 수 있습니다.

3. 디렉토리 삭제 취소:

   ```
   volume file async-delete cancel -vserver <SVM_name> -volume <volume_name>
   -jobid <job_id>
   ```

FlexGroups를 사용하여 **ONTAP** 디렉토리를 비동기적으로 삭제하기 위한 클라이언트 권한 관리

ONTAP 9.11.1부터 스토리지 관리자는 볼륨에 대한 권한을 부여하여 NFS 및 SMB 클라이언트가 비동기 삭제 작업을 수행할 수 있도록 할 수 있습니다. 클러스터에서 비동기 삭제가 활성화되면 Linux 클라이언트 사용자는 다음을 사용할 수 있습니다. `mv` 명령 및 Windows 클라이언트 사용자는 다음을 사용할 수 있습니다. `rename` 기본적으로 .ontaptrashbin이라는 이름의 숨겨진 디렉토리로 이동하여 지정된 볼륨의 디렉토리를 삭제하는 명령입니다.

저작권은 권별로 부여됩니다. NFS 클라이언트 사용자는 NFS 클라이언트에 대한 루트 액세스 권한과 NFS 내보내기에 대한 슈퍼유저 액세스 권한이 있어야 합니다.

디렉토리만 이동할 수 있습니다. .ontaptrashbin 디렉토리로 파일을 이동할 수 없습니다.

"ONTAP 사용하여 FlexGroup 볼륨에서 디렉토리를 비동기적으로 삭제하는 방법에 대해 알아보세요." .

단계

1. 클러스터 CLI에서 고급 권한 모드(- Privilege advance)를 입력합니다
2. 볼륨의 마운트 지점에서 클라이언트 비동기 삭제를 활성화하고, 원하는 경우 휴지통 디렉토리에 대한 대체 이름을 제공합니다.

   '볼륨 파일 비동기 삭제 클라이언트 활성화 volume_volname_vserver_vserverName_trashbinname_name_'

   기본 휴지통 이름을 사용한 예:

   ```
   cluster1::*> volume file async-delete client enable -volume v1 -vserver
   vs0

   Info: Async directory delete from the client has been enabled on volume
   "v1" in
         Vserver "vs0".
   ```

   대체 휴지통 이름을 지정하는 예:

   ```
   cluster1::*> volume file async-delete client enable -volume test
   -trashbin .ntaptrash -vserver vs1

   Success: Async directory delete from the client is enabled on volume
   "v1" in
         Vserver "vs0".
   ```

3. 클라이언트 비동기식 삭제가 설정되었는지 확인합니다.

   '볼륨 파일 비동기 삭제 클라이언트 표시'

   예:

   ```
   cluster1::*> volume file async-delete client show

   Vserver Volume      async-delete client TrashBinName
   ------------ ------------ ---------------------- -------------
   vs1          vol1         Enabled          .ntaptrash
   vs2          vol2         Disabled          -

   2 entries were displayed.
   ```

단계

1. 클러스터 CLI에서 client asychronous directory delete:

   'volume file async-delete client disable volume_volname_vserver_Name_'

   예:

```
cluster1::*> volume file async-delete client disable -volume vol1
-vserver vs1

       Success: Asynchronous directory delete client disabled
successfully on volume.
```

2. 클라이언트 비동기식 삭제가 비활성화되어 있는지 확인합니다.

   '볼륨 파일 비동기 삭제 클라이언트 표시'

   예:

```
cluster1::*> volume file async-delete client show

Vserver      Volume      async-delete client      TrashBinName
------------ ------------ ----------------------- -------------
vs1          vol1         Disabled                -
vs2          vol2         Disabled                -

2 entries were displayed.
```

ONTAP FlexGroup 볼륨으로 **qtree**를 생성합니다

ONTAP 9.3부터 FlexGroup 볼륨으로 qtree를 생성할 수 있습니다. Qtree를 사용하면 FlexGroup 볼륨을 작은 세그먼트로 파티셔닝하여 개별적으로 관리할 수 있습니다.

이 작업에 대해

- 소스 FlexGroup 볼륨에서 SnapMirror 관계에 qtree가 있는 경우, 타겟 클러스터에서 ONTAP 9.3 이상(qtree를 지원하는 ONTAP 소프트웨어 버전)을 실행해야 합니다.
- ONTAP 9.5부터는 FlexGroup 볼륨에 대해 qtree 통계가 지원됩니다.

단계

1. FlexGroup 볼륨에서 qtree를 생성합니다.

```
volume qtree create -vserver <vserver_name> -volume <volume_name> -qtree
<qtree_name>
```

필요에 따라 qtree에 대한 보안 스타일, SMB oplocks, UNIX 권한 및 엑스포트 정책을 지정할 수 있습니다.

```
cluster1::> volume qtree create -vserver vs0 -volume fg1 -qtree qtree1
-security-style mixed
```

관련 정보

"논리적 스토리지 관리"

ONTAP FlexGroup 볼륨에 할당량을 사용합니다

ONTAP 9.4 이하 버전에서는 할당량 제한을 적용하는 것이 아니라 보고 목적으로만 FlexGroup 볼륨에 할당량 규칙을 적용할 수 있습니다. ONTAP 9.5부터 FlexGroup 볼륨에 적용되는 할당량 규칙에 제한을 적용할 수 있습니다.

이 작업에 대해

- ONTAP 9.5부터 FlexGroup 볼륨에 대한 하드, 소프트 및 임계값 제한 할당량을 지정할 수 있습니다.

  이러한 제한을 지정하여 공간, 특정 사용자, 그룹 또는 qtree에서 생성할 수 있는 파일 수 또는 둘 다를 제한할 수 있습니다. 할당량 제한에서는 다음과 같은 경우에 경고 메시지가 생성됩니다.

  - 사용량이 설정된 소프트 제한값을 초과하면 ONTAP에서 경고 메시지를 발생하지만 추가 트래픽은 여전히 허용됩니다.

    나중에 사용량이 설정된 소프트 제한값 아래로 다시 떨어지면 메시지가 모두 표시됩니다.

  - 사용량이 구성된 임계값 제한을 초과하면 ONTAP에서 두 번째 경고 메시지를 표시합니다.

    사용량이 나중에 구성된 임계값 제한 아래로 떨어지면 모든 지우기 관리 메시지가 표시되지 않습니다.

  - 사용량이 구성된 하드 제한에 도달하면 ONTAP는 트래픽을 거부하여 추가 리소스 소비를 방지합니다.
- ONTAP 9.5에서는 SnapMirror 관계의 대상 FlexGroup 볼륨에서 할당량 규칙을 생성하거나 활성화할 수 없습니다.
- 할당량 초기화 중에는 할당량이 적용되지 않으며 할당량 초기화 후 위반된 할당량에 대한 알림이 없습니다.

  할당량 초기화 중에 할당량이 위반되었는지 확인하려면 'volume quota report' 명령을 사용합니다.

할당량 대상 및 유형

할당량은 사용자, 그룹 또는 트리일 수 있습니다. 할당량 지정 대상은 할당량 제한이 적용되는 사용자, 그룹 또는 qtree를 지정합니다.

다음 표에는 할당량 타겟의 종류, 각 할당량 목표와 연결된 할당량 유형, 각 할당량 대상이 표시되는 방식이 나와 있습니다.

할당량 대상	할당량 유형입니다	대상 표시 방법	참고
사용자	사용자 할당량	UNIX 사용자 이름 UNIX UID입니다 Windows 2000 이전 형식의 Windows 사용자 이름입니다 Windows SID	사용자 할당량은 특정 볼륨 또는 qtree에 적용할 수 있습니다.
그룹	그룹 할당량	UNIX 그룹 이름 UNIX GID입니다	그룹 할당량은 특정 볼륨 또는 qtree에 적용할 수 있습니다. ONTAP는 Windows ID를 기준으로 그룹 할당량을 적용하지 않습니다.
qtree입니다	트리 할당량	qtree 이름입니다	트리 할당량은 특정 볼륨에 적용되며 다른 볼륨의 qtree에 영향을 주지 않습니다.
""""	사용자 quotagrop 할당량입니다 트리 할당량	큰따옴표("")	""의 할당량 대상은 _ 기본 할당량 _ 을(를) 나타냅니다. 기본 할당량의 경우 할당량 유형은 유형 필드의 값에 의해 결정됩니다.

할당량 제한을 초과할 때 **FlexGroup** 볼륨의 동작

ONTAP 9.5부터 FlexGroup 볼륨에서 할당량 제한이 지원됩니다. FlexGroup 볼륨과 비교할 때 FlexVol 볼륨에 할당량 제한이 적용되는 방식은 몇 가지 차이가 있습니다.

FlexGroup 볼륨은 할당량 제한을 초과할 때 다음과 같은 동작을 표시할 수 있습니다.

- FlexGroup 볼륨의 공간 및 파일 사용은 추가 트래픽을 거부하여 할당량 제한을 적용하기 전에 구성된 하드 제한보다 최대 5% 높을 수 있습니다.

  최상의 성능을 제공하기 위해 ONTAP에서는 할당량 적용이 시작되기 전에 공간 소비가 구성된 하드 제한값을 약간 초과할 수 있습니다. 이 추가 공간 소비는 구성된 하드 제한값, 1GB 또는 65536 파일 중 더 낮은 쪽의 5%를 초과하지 않습니다.

- 할당량 제한에 도달한 후 사용자 또는 관리자가 할당량 사용이 현재 제한 아래로 내려갈 수 있도록 일부 파일 또는 디렉토리를 삭제하면 이후의 할당량 사용 파일 작업이 지연되어 다시 시작될 수 있습니다(다시 시작하는 데 최대

5초가 걸릴 수 있음).

- FlexGroup 볼륨의 총 공간 및 파일 사용량이 구성된 할당량 제한을 초과하면 이벤트 로그 메시지 로깅이 약간 지연될 수 있습니다.
- FlexGroup 볼륨의 일부 구성 요소로는 꽉 찼지만 할당량 제한에 도달하지 않으면 ""공간 없음" 오류가 발생할 수 있습니다.
- 할당량 하드 제한값이 구성된 할당량 타겟의 경우 파일 또는 디렉토리 이름을 바꾸거나 qtree 간에 파일을 이동하는 등의 작업은 FlexVol 볼륨의 유사 작업에 비해 시간이 더 오래 걸릴 수 있습니다.

FlexGroup 볼륨에 대한 할당량 적용의 예

이 예제를 사용하여 ONTAP 9.5 이상에서 할당량을 제한하는 방법을 이해할 수 있습니다.

예 1: 디스크 제한으로 할당량 규칙 적용

1. 달성 가능한 소프트 디스크 제한과 하드 디스크 제한을 모두 사용하여 'user' 유형의 할당량 정책 규칙을 만들어야 합니다.

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
default -volume FG -type user -target "" -qtree "" -disk-limit 1T -soft
-disk-limit 800G
```

2. 할당량 정책 규칙을 볼 수 있습니다.

```
cluster1::> volume quota policy rule show -vserver vs0 -policy-name
default -volume FG

Vserver: vs0               Policy: default           Volume: FG

                                                Soft             Soft
                         User          Disk     Disk   Files    Files
Type   Target    Qtree   Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off           1TB    800GB       -        -
-
```

3. 새 할당량 규칙을 활성화하려면 볼륨에 대해 할당량을 초기화해야 합니다.

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. 할당량 보고서를 사용하여 FlexGroup 볼륨의 디스크 사용량 및 파일 사용량 정보를 볼 수 있습니다.

```
cluster1::> volume quota report -vserver vs0 -volume FG
Vserver: vs0

                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    root      50GB      -       1       -
FG                 user    *         800GB    1TB      0       -   *
2 entries were displayed.
```

하드 디스크 제한에 도달하면 할당량 정책 규칙 대상(이 경우 사용자)이 파일에 더 많은 데이터를 쓸 수 없도록 차단됩니다.

예 **2:** 여러 사용자에 대해 할당량 규칙 적용

1. 할당량 대상(UNIX 사용자, SMB 사용자 또는 둘 다 조합)에 여러 사용자가 지정되어 있고 규칙에 달성 가능한 소프트 디스크 제한과 하드 디스크 제한이 모두 있는 할당량 정책 규칙 유형을 'user' 유형으로 생성해야 합니다.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target "rdavis,ABCCORP\RobertDavis" -qtree ""
-disk-limit 1TB -soft-disk-limit  800GB
```

2. 할당량 정책 규칙을 볼 수 있습니다.

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG

Vserver: vs0               Policy: default           Volume: FG

                                              Soft             Soft
                        User         Disk     Disk   Files    Files
Type   Target    Qtree  Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   "rdavis,ABCCORP\RobertDavis"  "" off  1TB  800GB  -  -
```

3. 새 할당량 규칙을 활성화하려면 볼륨에 대해 할당량을 초기화해야 합니다.

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. 할당량 상태가 활성 상태인지 확인할 수 있습니다.

```
cluster1::> volume quota show -vserver vs0 -volume FG
               Vserver Name: vs0
                Volume Name: FG
                Quota State: on
                Scan Status: -
          Logging Messages: on
          Logging Interval: 1h
          Sub Quota Status: none
  Last Quota Error Message: -
Collection of Quota Errors: -
```

5. 할당량 보고서를 사용하여 FlexGroup 볼륨의 디스크 사용량 및 파일 사용량 정보를 볼 수 있습니다.

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0

                                      ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    rdavis,ABCCORP\RobertDavis  0B  1TB  0  -
rdavis,ABCCORP\RobertDavis
```

할당량 제한값은 할당량 대상에 나열된 모든 사용자 간에 공유됩니다.

하드 디스크 제한에 도달하면 할당량 대상에 나열된 사용자가 파일에 더 많은 데이터를 쓸 수 없도록 차단됩니다.

예 **3:** 사용자 매핑을 사용하여 할당량 적용

1. 'user' 유형의 할당량 정책 규칙을 생성하고, 'user-mapping'을 'on'으로 설정한 할당량 타겟으로 UNIX 사용자나 Windows 사용자를 지정하고, 달성 가능한 소프트 디스크 제한과 하드 디스크 제한을 모두 사용하여 규칙을 생성해야 합니다.

   UNIX 사용자와 Windows 사용자 간의 매핑은 "vserver name-mapping create" 명령을 사용하여 미리 구성해야 합니다.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target rdavis -qtree "" -disk-limit 1TB -soft
-disk-limit  800GB -user-mapping on
```

2. 할당량 정책 규칙을 볼 수 있습니다.

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG

Vserver: vs0               Policy: default           Volume: FG

                                                 Soft             Soft
                         User         Disk       Disk    Files    Files
Type    Target    Qtree  Mapping      Limit      Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user    rdavis    ""     on            1TB    800GB       -        -
-
```

3. 새 할당량 규칙을 활성화하려면 볼륨에 대해 할당량을 초기화해야 합니다.

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. 할당량 상태가 활성 상태인지 확인할 수 있습니다.

```
cluster1::> volume quota show -vserver vs0 -volume FG
              Vserver Name: vs0
               Volume Name: FG
               Quota State: on
                Scan Status: -
          Logging Messages: on
          Logging Interval: 1h
          Sub Quota Status: none
  Last Quota Error Message: -
Collection of Quota Errors: -
```

5. 할당량 보고서를 사용하여 FlexGroup 볼륨의 디스크 사용량 및 파일 사용량 정보를 볼 수 있습니다.

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0

                                       ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    rdavis,ABCCORP\RobertDavis  0B  1TB  0  -
rdavis
```

할당량 제한은 할당량 대상에 나열된 사용자와 해당 Windows 또는 UNIX 사용자 간에 공유됩니다.

하드 디스크 제한에 도달하면 할당량 대상에 나열된 사용자와 해당 Windows 또는 UNIX 사용자가 파일에 더 많은 데이터를 쓸 수 없도록 차단됩니다.

예 **4:** 할당량이 설정된 경우 **qtree** 크기 확인

1. "트리" 유형의 할당량 정책 규칙을 생성하고 규칙에 달성 가능한 소프트 디스크 제한과 하드 디스크 제한이 모두 있는 규칙을 만들어야 합니다.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type tree -target tree_4118314302 -qtree "" -disk-limit 48GB
-soft-disk-limit 30GB
```

2. 할당량 정책 규칙을 볼 수 있습니다.

```
cluster1::> quota policy rule show -vserver vs0

Vserver: vs0               Policy: default           Volume: FG

                                              Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree   tree_4118314302  "" -          48GB        -      20        -
```

3. 새 할당량 규칙을 활성화하려면 볼륨에 대해 할당량을 초기화해야 합니다.

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

a. 할당량 보고서를 사용하여 FlexGroup 볼륨의 디스크 사용량 및 파일 사용량 정보를 볼 수 있습니다.

```
cluster1::> quota report -vserver vs0
Vserver: vs0
----Disk---- ----Files----- Quota
Volume Tree Type ID Used Limit Used Limit Specifier
------- -------- ------ ------- ----- ----- ------ ------ ---------
FG tree_4118314302 tree 1 30.35GB 48GB 14 20 tree_4118314302
```

할당량 제한은 할당량 대상에 나열된 사용자와 해당 Windows 또는 UNIX 사용자 간에 공유됩니다.

4. NFS 클라이언트에서 df 명령을 사용하여 총 공간 사용량, 사용 가능한 공간 및 사용된 공간을 확인합니다.

```
scsps0472342001# df -m /t/10.53.2.189/FG-3/tree_4118314302
Filesystem 1M-blocks Used Available Use% Mounted on
10.53.2.189/FG-3 49152 31078 18074 63% /t/10.53.2.189/FG-3
```

하드 제한에서는 NFS 클라이언트에서 다음과 같이 공간 사용량이 계산됩니다.

- 총 공간 사용량 = 트리의 하드 제한입니다
- 여유 공간 = 하드 제한에서 qtree 공간 사용을 뺀 값 하드 제한값은 다음과 같이 NFS 클라이언트에서 공간 사용을 계산합니다.
- 공간 사용 = 할당량 사용
- 총 공간 = 할당량 사용 및 볼륨의 물리적 사용 가능한 공간의 합계입니다

5. SMB 공유에서 Windows 탐색기를 사용하여 전체 공간 사용량, 사용 가능한 공간 및 사용된 공간을 확인합니다.

SMB 공유에서는 공간 사용량을 계산할 때 다음 사항을 고려해야 합니다.

- 사용자 및 그룹에 대한 사용자 할당량 하드 제한값을 고려하여 총 사용 가능한 공간을 계산합니다.
- 트리 할당량 규칙, 사용자 할당량 규칙 및 그룹 할당량 규칙의 사용 가능한 공간 중 최소값은 SMB 공유의 사용 가능한 공간으로 간주됩니다.
- 전체 공간 사용은 SMB의 경우 가변적이며 트리, 사용자 및 그룹 간의 최소 사용 가능 공간에 해당하는 하드 제한값에 따라 달라집니다.

FlexGroup 볼륨에 규칙 및 제한을 적용합니다

단계

1. 대상에 대한 할당량 규칙 생성: ' 볼륨 할당량 정책 규칙 create -vserver vs0 -policy -name quota_policy_of_the_rule -volume flexgroup_vol -type {tree | user | group} -target target_for_rule -qtree_name [-disk -limit hard_disk_limit_number] 소프트 제한값 [-file_limit_soft_file
   - 할당량 대상 유형은 `group`, 또는 `tree` FlexGroup 볼륨의 경우 일 수 `user` 있습니다.
   - FlexGroup 볼륨에 대한 할당량 규칙을 생성할 때 경로는 타겟으로 지원되지 않습니다.
   - ONTAP 9.5부터 FlexGroup 볼륨에 대한 하드 디스크 제한, 하드 파일 제한, 소프트 디스크 제한, 소프트 파일

제한 및 임계값 제한 할당량을 지정할 수 있습니다.

ONTAP 9.4 이하 버전에서는 FlexGroup 볼륨에 대한 할당량 규칙을 생성할 때 디스크 제한, 파일 제한, 디스크 한계 임계값, 소프트 디스크 한계 또는 소프트 파일 제한을 지정할 수 없습니다.

다음 예에서는 사용자 타겟 유형에 대해 생성되는 기본 할당량 규칙을 보여 줍니다.

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
quota_policy_vs0_1 -volume fg1 -type user -target "" -qtree ""
```

다음 예에서는 qtree1 이라는 qtree에 대해 생성되는 트리 할당량 규칙을 보여 줍니다.

```
cluster1::> volume quota policy rule create -policy-name default -vserver
vs0 -volume fg1 -type tree -target "qtree1"
```

1. 지정된 FlexGroup 볼륨에 대한 할당량을 활성화합니다. 'volume quota on-vserver svm_name -volume flexgroup_vol-foreground true'

```
cluster1::> volume quota on -vserver vs0 -volume fg1 -foreground true
```

1. 할당량 초기화 상태 'volume quota show -vserver svm_name'을 모니터링합니다

FlexGroup 볼륨은 모든 구성 볼륨이 아직 동일한 상태가 아님을 나타내는 '혼합' 상태를 표시할 수 있습니다.

```
cluster1::> volume quota show -vserver vs0
                                          Scan
Vserver    Volume        State            Status
---------  ------------  ---------------  ------
vs0        fg1           initializing         95%
vs0        vol1          off                   -
2 entries were displayed.
```

1. 활성 할당량이 있는 FlexGroup 볼륨에 대한 할당량 보고서('volume quota report-vserver svm_name-volume flexgroup_vol')를 봅니다

   FlexGroup 볼륨에 대한 'volume quota report' 명령을 사용하여 경로를 지정할 수 없습니다.

   다음 예에서는 FlexGroup 볼륨에 대한 사용자 할당량을 보여줍니다. `fg1` :

```
cluster1::> volume quota report -vserver vs0 -volume fg1
  Vserver: vs0
                                       ----Disk----  ----Files-----
Quota
  Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
  -------  --------  ------  -------  -----  -----  ------  ------
---------
  fg1                user    *           0B      -       0       -   *
  fg1                user    root       1GB      -       1       -   *
  2 entries were displayed.
```

다음 예에서는 FlexGroup 볼륨에 대한 트리 할당량을 보여줍니다. `fg1` :

```
cluster1::> volume quota report -vserver vs0 -volume fg1
Vserver: vs0

                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
fg1      qtree1  tree      1         68KB      -      18       -
qtree1
fg1              tree      *           0B      -       0       -   *
2 entries were displayed.
```

결과

할당량 규칙 및 제한은 FlexGroup 볼륨에 적용됩니다.

ONTAP에서 추가 트래픽을 거부하여 할당량을 적용하기 전에 사용량이 구성된 하드 제한보다 최대 5% 높을 수 있습니다.

관련 정보

- "ONTAP 명령 참조입니다"

ONTAP FlexGroup 볼륨에서 스토리지 효율성 활성화

중복제거 및 데이터 압축을 함께 실행하거나 FlexGroup 볼륨에서 독립적으로 실행하여 최적의 공간 절약 효과를 달성할 수 있습니다.

시작하기 전에

FlexGroup 볼륨이 온라인 상태여야 합니다.

단계

1. FlexGroup 볼륨에서 'volume Efficiency on-vserver svm_name-volume volume volume_name'을 활성화합니다

   FlexGroup 볼륨의 모든 구성요소에 대해 스토리지 효율성 작업이 활성화됩니다.

   볼륨에 스토리지 효율성이 설정된 후 FlexGroup 볼륨을 확장하면 새 구성요소에 대해 스토리지 효율성이 자동으로 활성화됩니다.

2. 'volume Efficiency modify' 명령을 사용하여 FlexGroup 볼륨에 필요한 스토리지 효율성 작업을 설정합니다.

   FlexGroup 볼륨에서 인라인 중복제거, 사후 처리 중복제거, 인라인 압축 및 사후 처리 압축을 활성화할 수 있습니다. 압축 유형(2차 또는 적응형)을 설정하고 FlexGroup 볼륨에 대한 일정 또는 효율성 정책을 지정할 수도 있습니다.

3. 스토리지 효율성 작업을 실행하기 위한 일정 또는 효율성 정책을 사용하지 않는 경우 효율성 작업('볼륨 효율성 시작 - vserver svm_name - volume volume volume volume_name')을 시작합니다

   볼륨에 중복제거 및 데이터 압축이 활성화되어 있으면 데이터 압축이 처음에 실행된 후 중복제거가 실행됩니다. 효율성 작업이 FlexGroup 볼륨에서 이미 활성 상태인 경우 이 명령은 실패합니다.

4. FlexGroup 볼륨에서 활성화된 효율성 작업을 확인합니다. 'volume enCOVERY show -vserver svm_name -volume volume volume_name'

```
cluster1::> volume efficiency show -vserver vs1 -volume fg1
             Vserver Name: vs1
              Volume Name: fg1
              Volume Path: /vol/fg1
                    State: Enabled
                   Status: Idle
                 Progress: Idle for 17:07:25
                     Type: Regular
                 Schedule: sun-sat@0

...

             Compression: true
      Inline Compression: true
Incompressible Data Detection: false
      Constituent Volume: false
Compression Quick Check File Size: 524288000
           Inline Dedupe: true
         Data Compaction: false
```

스냅샷을 사용하여 **ONTAP FlexGroup** 볼륨을 보호합니다

스냅샷 생성을 자동으로 관리하는 스냅샷 정책을 생성하거나 FlexGroup 볼륨에 대한 스냅샷을 수동으로 생성할 수 있습니다. ONTAP에서 FlexGroup 볼륨의 각 구성요소에 대한 스냅샷을

생성할 수 있는 경우에만 FlexGroup 볼륨에 대해 유효한 스냅샷이 생성됩니다.

이 작업에 대해

- 스냅샷 정책과 연결된 FlexGroup 볼륨이 여러 개인 경우 FlexGroup 볼륨 일정이 겹치지 않도록 해야 합니다.
- ONTAP 9.8부터 FlexGroup 볼륨에서 지원되는 최대 스냅샷 수는 1023개입니다.

> ONTAP 9.8부터 `volume snapshot show` FlexGroup 볼륨에 대한 명령은 가장 최근에 소유한 블록을 계산하지 않고 논리적 블록을 사용하여 스냅샷 크기를 보고합니다. 이 새로운 크기 계산 방법을 사용하면 스냅샷 크기가 이전 버전의 ONTAP에서 계산한 크기보다 크게 나타날 수 있습니다.

단계

1. 스냅샷 정책을 생성하거나 스냅샷을 수동으로 생성합니다.

을(를) 만들려면…	이 명령을 입력하십시오…
스냅샷 정책	볼륨 스냅샷 정책 생성 FlexGroup 볼륨의 스냅샷 정책과 연결된 스케줄의 간격은 30분 이상이어야 합니다. FlexGroup 볼륨을 생성할 때 `default` 스냅샷 정책이 FlexGroup 볼륨에 적용됩니다.
수동으로 스냅샷 생성	'볼륨 스냅샷 생성' FlexGroup 볼륨에 대한 스냅샷을 생성한 후에는 스냅샷의 속성을 수정할 수 없습니다. 속성을 수정하려면 스냅샷을 삭제한 다음 다시 생성해야 합니다.

스냅샷이 생성되면 FlexGroup 볼륨에 대한 클라이언트 액세스가 잠시 중단됩니다.

1. FlexGroup 볼륨에 대해 유효한 스냅샷이 생성되었는지 확인합니다. `volume snapshot show -volume volume_name -fields state`

```
cluster1::> volume snapshot show -volume fg -fields state
vserver volume snapshot                state
------- ------ ----------------------- -----
fg_vs   fg     hourly.2016-08-23_0505 valid
```

2. FlexGroup 볼륨 구성 요소에 대한 스냅샷 보기: `volume snapshot show -is-constituent true`

```
cluster1::> volume snapshot show -is-constituent true

---Blocks---
Vserver  Volume   Snapshot                                  Size Total%
Used%
-------- -------- ------------------------------------ -------- ------
-----
fg_vs    fg__0001
                  hourly.2016-08-23_0505                    72MB     0%
27%
         fg__0002
                  hourly.2016-08-23_0505                    72MB     0%
27%
         fg__0003
                  hourly.2016-08-23_0505                    72MB     0%
27%
...
         fg__0016
                  hourly.2016-08-23_0505                    72MB     0%
27%
```

ONTAP FlexGroup 볼륨에서 구성요소를 이동합니다

FlexGroup 볼륨의 구성요소를 한 애그리게이트에서 다른 애그리게이트로 이동하여 특정 구성요소에 더 많은 트래픽이 발생하는 경우 로드 밸런싱을 수행할 수 있습니다. 또한 구성요소를 이동하면 기존 구성요소의 크기를 조정할 수 있도록 애그리게이트의 공간을 확보할 수 있습니다.

시작하기 전에

SnapMirror 관계에 있는 FlexGroup 볼륨 구성요소를 이동하려면 SnapMirror 관계를 초기화해야 합니다.

이 작업에 대해

FlexGroup 볼륨의 구성요소를 확장하는 동안에는 볼륨 이동 작업을 수행할 수 없습니다.

단계

1. 이동할 FlexGroup 볼륨 구성요소를 식별합니다.

   ```
   volume show -vserver svm_name -is-constituent true
   ```

```
cluster1::> volume show -vserver vs2 -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2       fg1          -            online     RW        400TB
15.12TB   62%
vs2       fg1__0001    aggr1        online     RW         25TB
8.12MB   59%
vs2       fg1__0002    aggr2        online     RW         25TB
2.50TB   90%
...
```

2. FlexGroup 볼륨 구성요소를 이동할 수 있는 애그리게이트 식별:

   `volume move target-aggr show -vserver svm_name -volume vol_constituent_name`

   선택한 애그리게이트의 사용 가능한 공간이 이동 중인 FlexGroup 볼륨 구성요소의 크기보다 커야 합니다.

```
cluster1::> volume move target-aggr show -vserver vs2 -volume fg1_0002
Aggregate Name   Available Size   Storage Type
--------------   --------------   ------------
aggr2            467.9TB          hdd
node12a_aggr3    100.34TB         hdd
node12a_aggr2    100.36TB         hdd
node12a_aggr1    100.36TB         hdd
node12a_aggr4    100.36TB         hdd
5 entries were displayed.
```

3. FlexGroup 볼륨 구성요소를 원하는 애그리게이트로 이동할 수 있는지 검증:

   `volume move start -vserver svm_name -volume vol_constituent_name -destination -aggregate aggr_name -perform-validation-only true`

```
cluster1::> volume move start -vserver vs2 -volume fg1_0002 -destination
-aggregate node12a_aggr3 -perform-validation-only true
Validation succeeded.
```

4. FlexGroup 볼륨 구성 요소 이동:

   `volume move start -vserver svm_name -volume vol_constituent_name -destination -aggregate aggr_name [-allow-mixed-aggr-types {true|false}]`

   볼륨 이동 작업은 백그라운드 프로세스로 실행됩니다.

ONTAP 9.5부터, '-allow-mixed-agr-types' 매개 변수를 true로 설정하여 FlexGroup 볼륨 구성요소를 Fabric 풀에서 비 패브릭 풀로 이동하거나 그 반대로 이동할 수 있습니다. 기본적으로 '-allow-mixed-aggr-types' 옵션은 false로 설정됩니다.

FlexGroup 볼륨에서 암호화를 사용하도록 설정하기 위해 'volume move' 명령을 사용할 수 없습니다.

```
cluster1::> volume move start -vserver vs2 -volume fg1_002 -destination
-aggregate node12a_aggr3
```

활성 SnapMirror 작업으로 인해 볼륨 이동 작업이 실패할 경우 명령을 사용하여 SnapMirror 작업을 중단해야 `snapmirror abort -h` 합니다. 경우에 따라 SnapMirror 중단 작업도 실패할 수 있습니다. 이러한 경우 볼륨 이동 작업을 중단하고 나중에 다시 시도하십시오. 에 대한 자세한 내용은 `snapmirror abort` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 볼륨 이동 작업의 상태를 확인합니다.

   `volume move show -volume vol_constituent_name`

   다음 예에서는 복제 단계를 완료하고 볼륨 이동 작업의 컷오버 단계에 있는 FlexGroup 구성요소 볼륨의 상태를 보여줍니다.

```
cluster1::> volume move show -volume fg1_002
Vserver   Volume     State    Move Phase  Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------  ----------------
----------------
vs2       fg1_002    healthy  cutover     -                -
```

기존 **ONTAP FlexGroup** 볼륨에 대해 **FabricPool**의 **Aggregate**를 사용합니다

ONTAP 9.5부터 FlexGroup는 FabricPool 볼륨에 대해 지원됩니다. 기존 FlexGroup 볼륨에 FabricPool의 애그리게이트를 사용하려면 FlexGroup 볼륨이 상주하는 애그리게이트를 FabricPool의 애그리게이트로 변환하거나 FlexGroup 볼륨 구성요소를 FabricPool의 애그리게이트로 마이그레이션할 수 있습니다.

시작하기 전에

- FlexGroup 볼륨에는 공간 보장이 "없음"으로 설정되어 있어야 합니다.
- FlexGroup 볼륨이 상주하는 애그리게이트를 FabricPool에서 애그리게이트로 변환하려면 모든 SSD 디스크를 사용해야 합니다.

이 작업에 대해

기존 FlexGroup 볼륨이 비 SSD 애그리게이트에 상주하는 경우 FlexGroup 볼륨 구성요소를 FabricPool의 애그리게이트로 마이그레이션해야 합니다.

선택

- FlexGroup 볼륨이 상주하는 애그리게이트를 FabricPool에서 애그리게이트로 변환하려면 다음 단계를 수행하십시오.

  a. 기존 FlexGroup 볼륨에 대한 계층화 정책을 'volume modify -volume flexgroup_name -Tiering -policy [auto|snapshot|none|backup]'로 설정합니다

  ```
  cluster-2::> volume modify -volume fg1 -tiering-policy auto
  ```

  b. FlexGroup 볼륨이 상주하는 집계('volume show-volume flexgroup_name-fields aggr-list')를 식별합니다

  ```
  cluster-2::> volume show -volume fg1 -fields aggr-list
  vserver volume aggr-list
  ------- ------ -----------
  vs1     fg1    aggr1,aggr3
  ```

  c. 집계 목록에 나열된 각 집계에 오브젝트 저장소를 첨부합니다. '스토리지 집계 객체-저장-집계 집계 이름-이름 객체-저장-이름-허용-굽힘 그룹 TRUE'

  모든 애그리게이트를 오브젝트 저장소에 연결해야 합니다.

```
cluster-2::> storage aggregate object-store attach -aggregate aggr1
-object-store-name Amazon01B1
```

- FabricPool 볼륨 구성요소를 FlexGroup에서 애그리게이트로 마이그레이션하려면 다음 단계를 수행하십시오.

  a. 기존 FlexGroup 볼륨에 대한 계층화 정책을 'volume modify -volume flexgroup_name -Tiering -policy [auto|snapshot|none|backup]'로 설정합니다

  ```
  cluster-2::> volume modify -volume fg1 -tiering-policy auto
  ```

  b. FlexGroup 볼륨의 각 구성요소를 FabricPool의 동일한 클러스터에 있는 애그리게이트로 이동: 'volume move start-volume festination-aggregate FabricPool_aggregate-allow-mixed-agr-types true

  모든 FlexGroup 볼륨 구성요소를 FabricPool에서 애그리게이트로 이동하고(FlexGroup 볼륨 구성요소가 혼합 애그리게이트 유형에 있는 경우) 클러스터 내의 노드 전체에서 모든 구성요소의 균형을 조정해야 합니다.

```
cluster-2::> volume move start -volume fg1_001 -destination-aggregate
FP_aggr1 -allow-mixed-aggr-types true
```

관련 정보

- "디스크 및 애그리게이트 관리"

- "저장소 집계 객체-저장소 연결"

파일 데이터를 재배포하여 **ONTAP FlexGroup** 볼륨의 균형을 조정합니다

ONTAP 9.16.1부터 고급 용량 밸런싱을 활성화하여 매우 큰 파일이 확장되어 하나의 구성원 볼륨에서 공간을 사용할 때 FlexGroup 구성원 볼륨 간에 데이터를 배포할 수 있습니다.

고급 용량 밸런싱은 ONTAP 9.12.1에 도입된 세분화된 데이터 기능을 확장하므로 ONTAP에서 파일을 다른 구성원으로 이동할 수 "FlexGroup 볼륨의 균형 조정"있습니다. ONTAP 9.16.1부터 고급 용량 균형 조정 옵션을 사용하도록 설정하면 `-granular-data advanced` "기본" 파일 재조정 기능과 고급 용량 기능이 모두 활성화됩니다.

> 파일 재조정과 고급 용량 균형 조정은 기본적으로 해제되어 있습니다. 이러한 기능을 활성화한 후에는 비활성화할 수 없습니다. 용량 밸런싱을 해제해야 하는 경우 고급 용량 밸런싱을 사용하기 전에 생성된 스냅샷에서 복원해야 합니다.

고급 용량 균형 조정은 새로운 쓰기가 볼륨의 여유 공간의 10GB 또는 1%에 도달하면 시작됩니다.

파일 배포 방법

고급 용량 밸런싱을 트리거할 정도로 파일이 생성되거나 커질 경우, 해당 파일은 구성원 FlexGroup 볼륨에 걸쳐 1GB~10GB 사이에 스트라이프로 배포됩니다.

고급 용량 균형 조정이 활성화된 경우 ONTAP는 기존 대용량 파일을 소급 스트라이핑하지 않습니다. 고급 용량 균형 조정이 활성화된 후에도 기존 대용량 파일이 계속 증가하는 경우 기존 대용량 파일의 새 컨텐츠가 파일 크기와 사용 가능한 공간에 따라 멤버 FlexGroup 볼륨에 걸쳐 스트라이핑될 수 있습니다.

고급 용량 밸런싱이 스트라이프 폭을 결정하는 한 가지 방법은 멤버 볼륨에서 사용 가능한 여유 공간을 사용하는 것입니다. 고급 용량 균형 조정은 사용 가능한 여유 공간의 1%인 파일 스트라이프를 생성합니다. 즉, 사용 가능한 공간이 더 많으면 스트라이프가 더 커질 수 있으며 FlexGroup가 가득 차면 더 작아집니다.

지원되는 프로토콜

다음 프로토콜에서는 고급 용량 밸런싱이 지원됩니다.

- NFSv3, NFSv4, NFSv4.1
- pNFS를 사용합니다
- 중소기업

고급 용량 밸런싱 활성화

고급 용량 균형 조정은 기본적으로 해제되어 있습니다. FlexGroup 용량의 균형을 자동으로 조정하려면 고급 용량 밸런싱을 활성화해야 합니다. 이 기능을 사용하도록 설정한 후에는 해제할 수 없지만 고급 용량 밸런싱을 사용하도록 설정하기 전에 생성된 스냅샷에서 복원할 수 있습니다.

시작하기 전에

- 클러스터의 모든 노드에서 ONTAP 9.16.1 이상이 실행되고 있어야 합니다.
- 고급 용량 밸런싱을 사용하는 경우 ONTAP 9.16.1 이전 릴리즈로 되돌릴 수 없습니다. 되돌려야 하는 경우 먼저 고급 용량 밸런싱을 사용하도록 설정하기 전에 생성된 스냅샷에서 복구해야 합니다.
- NFS 복사본 오프로드가 사용된 (`vserver nfs -vstorage enabled`경우)SVM에서 FlexGroup 볼륨에 대해 고급

용량 밸런싱을 활성화할 수 없습니다. 마찬가지로 SVM의 모든 FlexGroup 볼륨에 고급 용량 밸런싱을 활성화한 경우 NFS 복사본 오프로드를 활성화할 수 없습니다.

- FlexCache write-back에서는 고급 용량 밸런싱이 지원되지 않습니다.
- ONTAP 9.16.1 이상을 실행하는 클러스터의 볼륨에서 고급 용량 밸런싱을 사용하는 경우 ONTAP 9.16.1 이전 버전의 ONTAP에서는 SnapMirror 전송이 지원되지 않습니다.
- 고급 용량 균형 조정을 활성화하기 전에 SMB Multichannel을 비활성화하십시오. 고급 용량 재균형 조정과 함께 SMB Multichannel을 사용하면 지연 시간이 길어질 수 있습니다. 자세한 내용은 "CONTAP-400433: SMB 멀티채널이 활성화된 클라이언트에서 FlexGroup 리밸런싱/GDD를 사용할 때 읽기/쓰기 지연 시간이 높게 나타남"을 참조하십시오.

이 작업에 대해

세부적인 데이터 옵션(기본 또는 고급)을 사용하여 DP 대상 볼륨을 생성하는 동안 대상은 SnapMirror 전송이 완료될 때까지 설정을 "사용 안 함"으로 표시합니다. 전송이 완료되면 DP 대상에 세분화된 데이터가 "활성화됨"으로 표시됩니다.

FlexGroup 생성 중에 고급 용량 밸런싱을 사용합니다

단계

System Manager 또는 ONTAP CLI를 사용하여 새 FlexGroup 볼륨을 생성할 때 고급 용량 밸런싱을 설정할 수 있습니다.

시스템 관리자

1. Storage > Volumes * 로 이동한 후 를 클릭합니다 + Add .
2. Add volume * (볼륨 추가 *) 창에서 볼륨 이름과 크기를 입력합니다. 그런 다음 * 추가 옵션 * 을 클릭합니다.
3. 저장 및 최적화 * 아래에서 * 클러스터 전체에 볼륨 데이터 배포(FlexGroup) * 를 선택합니다.
4. Advanced capacity balancing * 을 선택합니다.
5. 볼륨 구성을 마치고 * Save * 를 클릭합니다.

CLI를 참조하십시오

1. 고급 용량 밸런싱이 활성화된 볼륨 생성:

```
volume create -vserver <svm name> -volume <volume name> -size <volume size> -auto-provision-as flexgroup -junction-path /<path> -granular-data advanced
```

예:

```
volume create -vserver vs0 -volume newvol -size 1TB -auto-provision-as flexgroup -junction-path /newvol -granular-data advanced
```

기존 **FlexGroup** 볼륨에서 고급 용량 밸런싱을 지원합니다

단계

System Manager 또는 ONTAP CLI를 사용하여 고급 용량 밸런싱을 설정할 수 있습니다.

시스템 관리자

1. 스토리지 > 볼륨 * 으로 이동한 후 를 클릭하고 * 편집 > 볼륨 * 을 선택합니다.
2. Edit volume * 창의 * Storage and optimization * 에서 * Advanced capacity balancing * 을 선택합니다.
3. 저장 * 을 클릭합니다.

CLI를 참조하십시오

1. 기존 FlexGroup 볼륨을 수정하여 고급 용량 밸런싱 지원:

```
volume modify -vserver <svm name> -volume <volume name> -granular
-data advanced
```

예:

```
volume modify -vserver vs0 -volume newvol  -granular-data advanced
```

파일을 이동하여 **ONTAP FlexGroup** 볼륨의 균형을 조정합니다

ONTAP 9.12.1부터 FlexGroup의 한 구성 요소에서 다른 구성 요소까지 중단 없이 파일을 이동하여 FlexGroup 볼륨의 균형을 재조정할 수 있습니다.

FlexGroup 재조정은 새 파일과 파일 증가로 인해 시간이 지남에 따라 불균형이 발생할 때 용량을 재분배하는 데 도움이 됩니다. 재조정 작업을 수동으로 시작한 후 ONTAP가 파일을 선택하고 중단 없이 자동으로 이동합니다.

FlexGroup 재조정은 여러 부분으로 구성된 inode를 생성하여 많은 수의 파일을 단일 재조정 이벤트의 일부로 이동하거나 여러 재조정 이벤트를 초과하는 경우 시스템 성능을 저하시킨다는 점을 기억해야 합니다. 재조정 이벤트의 일부로 이동된 모든 파일에는 해당 파일과 연결된 2개의 멀티 파트 inode가 있습니다. 멀티 파트 inode가 포함된 파일 수가 FlexGroup의 총 파일 수에 대한 백분율로 클수록 성능에 미치는 영향이 커집니다. FlexVol에서 FlexGroup로 변환하는 것과 같은 특정 사용 사례에서는 많은 양의 inode가 생성될 수 있습니다.

재조정은 클러스터의 모든 노드에서 ONTAP 9.12.1 이상 릴리즈를 실행 중인 경우에만 사용할 수 있습니다. 재조정 작업을 실행하는 모든 FlexGroup 볼륨에 대해 세분화된 데이터 기능을 활성화해야 합니다. 이 기능을 사용하도록 설정한 후에는 이 볼륨을 삭제하거나 설정을 사용하기 전에 생성된 스냅샷에서 복원하지 않는 한 ONTAP 9.11.1 이전 버전으로 되돌릴 수 없습니다.

ONTAP 9.14.1부터 ONTAP는 사용자 개입 없이 세분화된 데이터가 활성화된 볼륨에서 파일을 사전 예방적으로 이동하는 알고리즘을 도입했습니다. 이 알고리즘은 성능 병목 현상을 완화하기 위해 매우 구체적이고 대상이 지정된 시나리오에서 작동합니다. 이 알고리즘이 작동할 수 있는 시나리오에는 클러스터의 한 노드에 있는 특정 파일 세트에 대한 매우 높은 쓰기 부하가 발생하거나 매우 핫 상위 디렉토리에서 지속적으로 증가하는 파일이 포함됩니다.

ONTAP 9.16.1부터 를 사용하여 FlexGroup 멤버 볼륨 간에 대용량 파일의 데이터를 재배포할 수도 "고급 용량 밸런싱 "있습니다.

FlexGroup 재조정 고려 사항

FlexGroup 재조정의 작동 방식과 이 기능이 다른 ONTAP 기능과 어떻게 상호 작용하는지 알고 있어야 합니다.

- FlexVol에서 FlexGroup로의 변환

  FlexVol 에서 FlexGroup 으로 변환한 후에는 자동 FlexGroup 재조정을 사용하지 않는 것이 좋습니다. 대신 다음을 사용하여 기존 파일을 재배포할 수 있습니다. `volume rebalance file-move start` ONTAP 9.10.1 이상에서 사용 가능한 명령입니다. 이 작업은 기본적으로 중단되지 않습니다.(`-is-disruptive false`). 일부 바쁜 파일을 이동할 수 없는 경우 중단 모드에서 명령을 다시 실행할 수 있습니다.(`-is-disruptive true`) 계획된 유지 관리 기간 동안. 자세히 알아보세요 `volume rebalance file-move start` 에서 "ONTAP 명령 참조입니다" .

  자동 FlexGroup 재조정 기능을 통해 재조정하면 FlexVol를 FlexGroup로 변환하는 경우와 같이 대량의 파일을 이동할 때 성능이 저하될 수 있으며, FlexVol 볼륨의 데이터를 50~85%까지 새로운 구성요소로 이동할 수 있습니다.

- 최소 및 최대 파일 크기입니다

  자동 재조정을 위한 파일 선택은 저장된 블록을 기반으로 합니다. 재조정을 위해 고려되는 최소 파일 크기는 기본적으로 100MB이며(아래에 나와 있는 최소 파일 크기 매개 변수를 사용하여 최소 20MB로 구성할 수 있음) 최대 파일 크기는 100GB입니다.

- 스냅샷의 파일

  현재 스냅샷에 존재하지 않는 파일을 이동할 것만 고려하도록 FlexGroup 재조정을 구성할 수 있습니다. 재조정이 시작되면 재조정 작업 중에 언제든지 스냅샷 작업이 예약되면 알림이 표시됩니다.

  파일이 이동 중이고 대상에서 프레이밍을 진행 중인 경우 스냅샷이 제한됩니다. 파일 재조정이 진행 중인 동안에는 스냅샷 복구 작업이 허용되지 않습니다.

  이 옵션을 설정한 후에 생성된 스냅샷은 ONTAP 9.11.1 이하 버전을 `granular-data` 실행하는 시스템에 복제할 수 없습니다. ONTAP 9.11.1 및 이전 버전에서는 멀티 파트 inode를 지원하지 않기 때문입니다.

- SnapMirror 작업

  FlexGroup 재조정은 예약된 SnapMirror 작업 간에 수행해야 합니다. 24분 SnapMirror 재시도 기간 내에 파일 이동이 완료되지 않은 경우 SnapMirror 작업을 시작하기 전에 파일을 재배치하면 SnapMirror 작업이 실패할 수 있습니다. SnapMirror 전송이 시작된 후 시작되는 새 파일 재배치가 실패하지 않습니다.

- 파일 기반 압축 스토리지 효율성

  파일 기반 압축 스토리지 효율성을 사용하면 파일이 타겟으로 이동하기 전에 압축이 풀리기 때문에 압축 절약 효과가 사라집니다. 재조정 후 FlexGroup 볼륨에서 백그라운드 검사기를 수동으로 시작한 후 압축 축소가 다시 실현됩니다. 그러나 모든 볼륨에 있는 스냅샷과 연결된 파일이 있는 경우 이 파일은 압축에 대해 무시됩니다.

- 중복 제거

  중복제거된 파일을 이동하면 FlexGroup 볼륨의 전체 사용량이 증가할 수 있습니다. 파일 재조정 중에 고유한 블록만 타겟으로 이동되므로 소스에서 해당 용량을 확보할 수 있습니다. 공유 블록은 소스에 남아 있고 타겟으로 복제됩니다. 이는 거의 전체 소스 구성요소에서 사용된 용량을 줄이는 것을 목표로 하지만, 새 대상의 공유 블록

복사본으로 인해 FlexGroup 볼륨의 전체 사용량이 증가할 수도 있습니다. 스냅샷의 일부인 파일이 이동된 경우에도 가능합니다. 스냅샷 스케줄이 재사용되고 스냅샷에 더 이상 파일 복제본이 없을 때까지 공간 절약 효과가 완전히 인식되지 않습니다.

- FlexClone 볼륨

  FlexClone 볼륨 생성 시 파일 재조정이 진행되고 있으면 FlexClone 볼륨에서 재조정이 수행되지 않습니다. FlexClone 볼륨에서 재조정은 생성된 후에 수행해야 합니다.

- 파일 이동

  FlexGroup 재조정 작업 중에 파일이 이동되면 소스 및 대상 구성 요소 모두에서 파일 크기가 할당량 고려의 일부로 보고됩니다. 이동이 완료되면 할당량 계정이 정상으로 돌아가고 파일 크기는 새 대상에서만 보고됩니다.

- 자율 랜섬웨어 보호

  ONTAP 9.13.1부터 자율적 랜섬웨어 방어는 운영 중단 및 무중단 재조정 작업 중에 지원됩니다.

- 오브젝트 저장소 볼륨

  S3 버킷과 같은 오브젝트 저장소 볼륨에서는 볼륨 용량 재조정이 지원되지 않습니다.

FlexGroup 재조정을 활성화합니다

ONTAP 9.12.1부터 FlexGroup 볼륨 자동 균형 재조정을 통해 FlexGroup 구성요소 간에 파일을 재배포할 수 있습니다.

ONTAP 9.13.1 버전부터는 단일 FlexGroup 재조정 작업이 미래의 날짜와 시간에 시작되도록 예약할 수 있습니다.

시작하기 전에

을(를) 활성화해야 합니다 `granular-data` FlexGroup 재조정을 활성화하기 전에 FlexGroup 볼륨에 대한 옵션입니다. 다음 방법 중 하나를 사용하여 활성화할 수 있습니다.

- 를 사용하여 FlexGroup 볼륨을 생성할 때 `volume create` 명령
- 를 사용하여 설정을 활성화하기 위해 기존 FlexGroup 볼륨을 수정합니다 `volume modify` 명령
- 을 사용하여 FlexGroup 재조정이 시작될 때 자동으로 설정합니다 `volume rebalance` 명령

> ONTAP 9.16.1 이상을 사용하고 ONTAP CLI의 옵션을 사용하여 사용하거나 System Manager를 사용하여 사용하도록 설정한 `granular-data advanced` 경우 "FlexGroup 고급 용량 밸런싱 "FlexGroup 재조정도 사용하도록 설정됩니다.

단계

ONTAP System Manager 또는 ONTAP CLI를 사용하여 FlexGroup 재조정을 관리할 수 있습니다.

시스템 관리자

1. 저장소 > 볼륨 * 으로 이동하고 재조정할 FlexGroup 볼륨을 찾습니다.
2. 볼륨 세부 정보를 보려면 선택합니다.
3. FlexGroup 잔액 상태 * 에서 * 재조정 * 을 선택합니다.

   재조정 * 옵션은 FlexGroup 상태가 불균형 상태인 경우에만 사용할 수 있습니다.

4. Rebalance Volume * (볼륨 재조정 *) 창에서 필요에 따라 기본 설정을 변경합니다.
5. 재조정 작업을 예약하려면 * Rebalance later * 를 선택하고 날짜와 시간을 입력합니다.

CLI를 참조하십시오

1. 자동 재조정 시작:

   ```
   volume rebalance start -vserver <SVM name> -volume <volume name>
   ```

   필요에 따라 다음 옵션을 지정할 수 있습니다.

   [[-max-runtime] <time interval>] 최대 런타임

   [-max-threshold <percent>](최대 임계값) Institutent별 최대 불균형 임계값

   [-min-threshold <percent>] 제헌당 최소 불균형 임계값

   [-max-file-Moves <integer>] 제헌당 최대 동시 파일 이동 수

   [-min-file-size{<integer>[KB|MB|GB|TB|PB]}] 최소 파일 크기

   [-start-time <mm/dd/yyyy-00:00:00>] 시작 날짜와 시간의 균형을 재조정합니다

   [-exclude-snapshots{true|false}] 스냅샷에 걸린 파일을 제외합니다

   예:

   ```
   volume rebalance start -vserver vs0 -volume fg1
   ```

FlexGroup 재조정 구성을 수정합니다

FlexGroup 재조정 구성을 변경하여 불균형 임계값, 동시 파일 수, 최소 파일 크기, 최대 런타임 및 스냅샷 포함 또는 제외를 업데이트할 수 있습니다. FlexGroup 재조정 일정을 수정하는 옵션은 ONTAP 9.13.1 부터 사용할 수 있습니다.

시스템 관리자

1. 저장소 > 볼륨 * 으로 이동하고 재조정할 FlexGroup 볼륨을 찾습니다.
2. 볼륨 세부 정보를 보려면 선택합니다.
3. FlexGroup 잔액 상태 * 에서 * 재조정 * 을 선택합니다.

   재조정 * 옵션은 FlexGroup 상태가 불균형 상태인 경우에만 사용할 수 있습니다.

4. Rebalance Volume * (볼륨 재조정 *) 창에서 필요에 따라 기본 설정을 변경합니다.

CLI를 참조하십시오

1. 자동 재조정 수정:

   ```
   volume rebalance modify -vserver <SVM name> -volume <volume name>
   ```

   다음 옵션 중 하나 이상을 지정할 수 있습니다.

   [[-max-runtime] <time interval>] 최대 런타임

   [-max-threshold <percent>](최대 임계값) Institutent별 최대 불균형 임계값

   [-min-threshold <percent>] 제헌당 최소 불균형 임계값

   [-max-file-Moves <integer>] 제헌당 최대 동시 파일 이동 수

   [-min-file-size{<integer>[KB|MB|GB|TB|PB]}] 최소 파일 크기

   [-start-time <mm/dd/yyyy-00:00:00>] 시작 날짜와 시간의 균형을 재조정합니다

   [-exclude-snapshots{true|false}] 스냅샷에 걸린 파일을 제외합니다

FlexGroup 재조정을 중지합니다

FlexGroup 재조정이 활성화 또는 예약되면 언제든지 중지할 수 있습니다.

시스템 관리자

1. 저장소 > 볼륨 * 으로 이동하여 FlexGroup 볼륨을 찾습니다.
2. 볼륨 세부 정보를 보려면 선택합니다.
3. Stop Rebalance * 를 선택합니다.

CLI를 참조하십시오

1. FlexGroup 재조정 중지:

```
volume rebalance stop -vserver <SVM name> -volume <volume name>
```

FlexGroup 재조정 상태를 봅니다

FlexGroup 재조정 작업, FlexGroup 재조정 구성, 재조정 작업 시간 및 재조정 인스턴스 세부 정보에 대한 상태를 표시할 수 있습니다.

시스템 관리자

1. 저장소 > 볼륨 * 으로 이동하여 FlexGroup 볼륨을 찾습니다.
2. FlexGroup 세부 정보를 보려면 선택합니다 ⌄ .
3. * FlexGroup 잔액 상태 * 는 세부 정보 창의 하단 근처에 표시됩니다.
4. 마지막 재조정 작업에 대한 정보를 보려면 * Last Volume Rebalance Status * 를 선택합니다.

CLI를 참조하십시오

1. FlexGroup 재조정 작업의 상태를 봅니다.

```
volume rebalance show
```

재조정 상태의 예:

```
> volume rebalance show
Vserver: vs0
                                                                  Target
Imbalance
Volume       State                  Total      Used     Used
Size     %
------------ ------------------ --------- --------- ---------
--------- -----
fg1          idle                     4GB   115.3MB         -
8KB    0%
```

재조정 구성 세부 정보의 예:

```
> volume rebalance show -config
Vserver: vs0
                    Max            Threshold         Max
Min          Exclude
Volume              Runtime        Min     Max       File Moves
File Size    Snapshot
---------------     ------------   -----   -----     ----------
---------    ---------
fg1                 6h0m0s         5%      20%          25
4KB          true
```

재조정 시간 세부 정보의 예:

```
> volume rebalance show -time
Vserver: vs0
Volume               Start Time                    Runtime
Max Runtime
---------------     -------------------------     -----------
-----------
fg1                  Wed Jul 20 16:06:11 2022      0h1m16s
6h0m0s
```

인스턴스 재조정 세부 정보의 예:

```
    > volume rebalance show -instance
    Vserver Name: vs0
    Volume Name: fg1
    Is Constituent: false
    Rebalance State: idle
    Rebalance Notice Messages: -
    Total Size: 4GB
    AFS Used Size: 115.3MB
    Constituent Target Used Size: -
    Imbalance Size: 8KB
    Imbalance Percentage: 0%
    Moved Data Size: -
    Maximum Constituent Imbalance Percentage: 1%
    Rebalance Start Time: Wed Jul 20 16:06:11 2022
    Rebalance Stop Time: -
    Rebalance Runtime: 0h1m32s
    Rebalance Maximum Runtime: 6h0m0s
    Maximum Imbalance Threshold per Constituent: 20%
    Minimum Imbalance Threshold per Constituent: 5%
    Maximum Concurrent File Moves per Constituent: 25
    Minimum File Size: 4KB
    Exclude Files Stuck in snapshots: true
```

FlexGroup 볼륨에 대한 데이터 보호

ONTAP FlexGroup 볼륨에 대한 데이터 보호 워크플로우 요약

FlexGroup 볼륨에 대한 SnapMirror DR(재해 복구) 관계를 생성할 수 있습니다. SnapVault 기술을 사용하여 FlexGroup 볼륨을 백업 및 복원할 수도 있으며, 백업 및 DR에 동일한 대상을 사용하는 통합 데이터 보호 관계를 만들 수도 있습니다.

이 작업에 대해

SnapMirror 관계 유형은 항상 `XDP` FlexGroup 볼륨에 해당합니다. SnapMirror 관계에서 제공하는 데이터 보호 유형은 사용하는 복제 정책에 따라 결정됩니다. 생성할 복제 관계에 필요한 유형의 기본 정책이나 사용자 지정 정책을 사용할 수 있습니다.

1 클러스터 및 **SVM**을 피어링합니다

클러스터와 SVM이 이미 피어링되지 않은 경우"클러스터 피어", 및 를 "SVM 피어"생성합니다.

2 작업 일정을 작성합니다

SnapMirror 업데이트가 언제 수행되는지 확인해야 "작업 일정을 작성합니다"합니다.

3 데이터 보호의 유형에 따라 다음 경로 중 하나를 수행합니다.

- * SnapMirror 재해 복구인 경우: *

  "SnapMirror 관계를 생성합니다." 관계를 만들 때 기본 정책 또는 유형의 사용자 지정 정책을 `async-mirror` 선택할 수 `MirrorAllSnapshots` 있습니다.

- * SnapMirror 볼트인 경우: *

  "SnapMirror 볼트 관계를 작성합니다." 관계를 만들 때 기본 정책 또는 유형의 사용자 지정 정책을 `vault` 선택할 수 `XDPDefault` 있습니다.

- * 통합 데이터 보호의 경우: *

  "통합 데이터 보호 관계를 생성합니다." 관계를 만들 때 기본 정책 또는 유형의 사용자 지정 정책을 `mirror-vault` 선택할 수 `MirrorAndVault` 있습니다.

ONTAP FlexGroup 볼륨에 대한 **SnapMirror** 관계 생성

재해 복구를 위한 데이터 복제를 위해 소스 FlexGroup 볼륨과 타겟 FlexGroup 볼륨 사이에 SnapMirror 관계를 구축할 수 있습니다. 재해가 발생할 경우 FlexGroup 볼륨의 미러 복사본을 사용하여 데이터를 복구할 수 있습니다.

시작하기 전에

클러스터 피어링 관계와 SVM 피어링 관계를 생성해야 합니다.

"클러스터 및 SVM 피어링"

이 작업에 대해

- ONTAP 9.9.1부터 ONTAP CLI를 사용하여 FlexGroup 볼륨에 대한 SnapMirror 계단식 배열 및 팬아웃 관계를 생성할 수 있습니다. 자세한 내용은 을 참조하십시오 "FlexGroup 볼륨에 대한 SnapMirror 캐스케이드 및 팬아웃 관계를 생성할 때의 고려 사항".
- FlexGroup 볼륨에 대한 인터클러스터 SnapMirror 관계와 클러스터 간 SnapMirror 관계를 모두 생성할 수 있습니다.
- ONTAP 9.3부터 SnapMirror 관계에 있는 FlexGroup 볼륨을 확장할 수 있습니다.

ONTAP 9.3 이전 버전의 ONTAP를 사용 중인 경우 SnapMirror 관계가 구축된 후 FlexGroup 볼륨을 확장하지 마십시오. 그러나 SnapMirror 관계를 설정한 후 FlexGroup 볼륨의 용량을 늘릴 수 있습니다. ONTAP 9.3 이전의 릴리즈에서 SnapMirror 관계를 끊은 후 소스 FlexGroup 볼륨을 확장하는 경우 대상 FlexGroup 볼륨에 대한 기본 전송을 수행해야 합니다.

단계

1. 소스 FlexGroup 볼륨과 구성 요소 수가 동일한 dP 유형의 대상 FlexGroup 볼륨을 생성합니다.
   a. 소스 클러스터에서 소스 FlexGroup 볼륨의 구성요소 수('volume show-volume volume_name * -is-f성분 TRUE')를 결정합니다

```
cluster1::> volume show  -volume srcFG* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vss       srcFG          -            online     RW         400TB
172.86GB  56%
vss       srcFG__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vss       srcFG__0002    aggr1        online     RW         25TB
10.86TB   56%
vss       srcFG__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vss       srcFG__0004    aggr1        online     RW         25TB
10.73TB   57%
vss       srcFG__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vss       srcFG__0006    aggr1        online     RW         25TB
10.64TB   57%
vss       srcFG__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

   b. 대상 클러스터에서 소스 FlexGroup 볼륨과 동일한 수의 구성 요소와 함께 dP 유형의 대상 FlexGroup 볼륨을 생성합니다.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG

Warning: The FlexGroup volume "dstFG" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

c. 대상 클러스터에서 대상 FlexGroup 볼륨에 있는 구성 요소 수('volume show-volume volume volume_name * -is-f성분 TRUE')를 확인합니다

```
cluster2::> volume show  -volume dstFG* -is-constituent true
Vserver   Volume        Aggregate    State      Type       Size
Available  Used%
--------- ------------  ------------ ---------- ---- ----------
---------- -----
vsd       dstFG          -            online     DP         400TB
172.86GB  56%
vsd       dstFG__0001    Aggr_cmode   online     DP         25GB
10.86TB   56%
vsd       dstFG__0002    aggr1        online     DP         25TB
10.86TB   56%
vsd       dstFG__0003    Aggr_cmode   online     DP         25TB
10.72TB   57%
vsd       dstFG__0004    aggr1        online     DP         25TB
10.73TB   57%
vsd       dstFG__0005    Aggr_cmode   online     DP         25TB
10.67TB   57%
vsd       dstFG__0006    aggr1        online     DP         25TB
10.64TB   57%
vsd       dstFG__0007    Aggr_cmode   online     DP         25TB
10.63TB   57%
...
```

2. 작업 일정 생성:'작업 일정 cron create-name job_name-month month-DayOfWeek day_of_week-day day_of_month-hour-minute'입니다

   월-일-일-주-시간 옵션을 선택하면 월, 요일, 시간마다 작업을 실행하도록 모두 를 지정할 수 있습니다.

   다음 예에서는 토요일 오전 3시에 실행되는 my_weekly라는 작업 일정을 생성합니다.

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. SnapMirror 관계에 대해 '비동기 미러' 유형의 사용자 지정 정책을 생성합니다. '스냅샷 정책 생성 - SVM SVM-정책 SnapMirror_policy-type async-mirror'

   사용자 지정 정책을 만들지 않는 경우 SnapMirror 관계에 대한 "irrorAllSnapshots" 정책을 지정해야 합니다.

4. 대상 클러스터에서 소스 FlexGroup 볼륨과 대상 FlexGroup 볼륨 간에 SnapMirror 관계를 생성합니다. 'sapmirror create-source-path src_svm:src_flexgroup-destination-path dest_svm:dest_flexgroup-type XDP 정책 snapmirror_policy-schedule sched_name'

   FlexGroup 볼륨의 SnapMirror 관계는 XDP 유형이어야 합니다.

FlexGroup 볼륨에 대한 SnapMirror 관계의 스로틀 값을 지정하는 경우 각 구성요소에서 동일한 스로틀 값을 사용합니다. 스로틀 값은 구성 요소별로 나누지 않습니다.

FlexGroup 볼륨에 대해 스냅샷의 SnapMirror 레이블을 사용할 수 없습니다.

ONTAP 9.4 이하 버전에서는, 정책이 '스냅샷 생성' 명령으로 지정되지 않으면 기본적으로 'irorAllSnapshots' 정책이 사용됩니다. ONTAP 9.5에서는 '스냅샷 생성' 명령으로 정책을 지정하지 않으면 기본적으로 'MirorAndVault' 정책이 사용됩니다.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path
vsd:dstFG -type XDP -policy MirrorAllSnapshots -schedule hourly
Operation succeeded: snapmirror create for the relationship with
destination "vsd:dstFG".
```

5. 대상 클러스터에서 기본 전송인 '스냅샷 초기화 - 대상 경로 dest_svm: dest_flexgroup'을 수행하여 SnapMirror 관계를 초기화합니다

   기본 전송이 완료되면 SnapMirror 관계의 일정에 따라 대상 FlexGroup 볼륨이 정기적으로 업데이트됩니다.

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```

ONTAP 9.3을 실행하는 소스 클러스터와 ONTAP 9.2 이하를 실행하는 타겟 클러스터 간에 FlexGroup 볼륨 간에 SnapMirror 관계가 생성되었으며 소스 FlexGroup 볼륨에서 qtree를 생성하는 경우 SnapMirror 업데이트가 실패합니다. 이 상황에서 복구하려면 FlexGroup 볼륨에서 기본값이 아닌 모든 qtree를 삭제하고 FlexGroup 볼륨에서 qtree 기능을 사용하지 않도록 설정한 다음 qtree 기능을 통해 사용하도록 설정된 스냅샷을 모두 삭제해야 합니다.

작업을 마친 후

LIF 및 엑스포트 정책과 같은 필수 구성을 설정하여 데이터 액세스를 위한 타겟 SVM을 설정해야 합니다.

관련 정보

- "SnapMirror 생성"
- "SnapMirror 초기화"
- "스냅미러 정책 생성"
- "스냅미러 업데이트"

ONTAP FlexGroup 볼륨에 대한 **SnapVault** 관계 생성

SnapVault 관계를 구성하고 관계에 SnapVault 정책을 할당하여 SnapVault 백업을 생성할 수 있습니다.

시작하기 전에

FlexGroup 볼륨에 대한 SnapVault 관계를 생성할 때 고려해야 할 사항에 대해 알고 있어야 합니다.

단계

1. 소스 FlexGroup 볼륨과 구성 요소 수가 동일한 dP 유형의 대상 FlexGroup 볼륨을 생성합니다.

   a. 소스 클러스터에서 소스 FlexGroup 볼륨의 구성요소 수('volume show-volume volume_name * -is-f성분 TRUE')를 결정합니다

```
cluster1::> volume show  -volume src* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vss       src          -            online     RW         400TB
172.86GB  56%
vss       src__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vss       src__0002    aggr1        online     RW         25TB
10.86TB   56%
vss       src__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vss       src__0004    aggr1        online     RW         25TB
10.73TB   57%
vss       src__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vss       src__0006    aggr1        online     RW         25TB
10.64TB   57%
vss       src__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

   b. 대상 클러스터에서 소스 FlexGroup 볼륨과 동일한 수의 구성 요소와 함께 dP 유형의 대상 FlexGroup 볼륨을 생성합니다.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dst

Warning: The FlexGroup volume "dst" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

   c. 대상 클러스터에서 대상 FlexGroup 볼륨에 있는 구성 요소 수('volume show-volume volume volume_name * -is-f성분 TRUE')를 확인합니다

```
cluster2::> volume show  -volume dst* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dst          -            online     RW         400TB
172.86GB  56%
vsd       dst__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vsd       dst__0002    aggr1        online     RW         25TB
10.86TB   56%
vsd       dst__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vsd       dst__0004    aggr1        online     RW         25TB
10.73TB   57%
vsd       dst__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vsd       dst__0006    aggr1        online     RW         25TB
10.64TB   57%
vsd       dst__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

2. 작업 일정 생성:'작업 일정 cron create-name job_name-month month-DayOfWeek day_of_week-day day_of_month-hour-minute'입니다

   월-일-일-주-시-시간의 경우 월, 일, 시 순으로 모두 작업을 실행하도록 지정할 수 있습니다.

   다음 예에서는 토요일 오전 3시에 실행되는 my_weekly라는 작업 일정을 생성합니다.

   ```
   cluster1::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

3. SnapVault 정책을 생성한 다음 SnapVault 정책에 대한 규칙을 정의합니다.

   a. SnapVault 관계를 위한 '볼트' 유형의 사용자 정의 정책을 작성합니다: '스냅샷 정책 생성 - vserver svm_name - policy_name - type vault'

   b. 초기화 및 업데이트 작업 중에 전송되는 스냅샷을 결정하는 SnapVault 정책에 대한 규칙을 정의합니다. `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule -snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

   사용자 지정 정책을 만들지 않는 경우 SnapVault 관계에 대해 "XDPDefault" 정책을 지정해야 합니다.

4. SnapVault 관계를 생성합니다. 'sapmirror create-source-path src_svm:src_flexgroup-destination-path dest_svm:dest_flexgroup-type xDP-schedule_name-policy XDPDefault'

ONTAP 9.4 이하 버전에서는, 정책이 '스냅샷 생성' 명령으로 지정되지 않으면 기본적으로 'irorAllSnapshots' 정책이 사용됩니다. ONTAP 9.5에서는 '스냅샷 생성' 명령으로 정책을 지정하지 않으면 기본적으로 'MirorAndVault' 정책이 사용됩니다.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path
vsd:dstFG -type XDP -schedule Daily -policy XDPDefault
```

에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 대상 클러스터에서 기본 전송:스냅샷 미러 초기화-대상-경로 dest_svm:dest_flexgroup'을 수행하여 SnapVault 관계를 초기화합니다

```
cluster2::> snapmirror initialize -destination-path vsd:dst
Operation is queued: snapmirror initialize of destination "vsd:dst".
```

관련 정보

- "SnapMirror 생성"
- "SnapMirror 초기화"
- "스냅미러 정책 추가 규칙"
- "스냅미러 정책 생성"

ONTAP FlexGroup 볼륨에 대한 통합 데이터 보호 관계를 구축합니다

ONTAP 9.3부터는 SnapMirror 통합 데이터 보호 관계를 생성 및 구성하여 동일한 타겟 볼륨에서 재해 복구 및 아카이빙을 구성할 수 있습니다.

시작하기 전에

FlexGroup 볼륨에 대한 통합 데이터 보호 관계를 생성할 때 고려해야 할 사항에 대해 알고 있어야 합니다.

"SnapVault 백업 관계를 생성할 때의 고려 사항 및 FlexGroup 볼륨에 대한 통합 데이터 보호 관계"

단계

1. 소스 FlexGroup 볼륨과 구성 요소 수가 동일한 dP 유형의 대상 FlexGroup 볼륨을 생성합니다.
   a. 소스 클러스터에서 소스 FlexGroup 볼륨의 구성요소 수('volume show-volume volume_name * -is-f성분 TRUE')를 결정합니다

```
cluster1::> volume show  -volume srcFG* -is-constituent true
Vserver   Volume         Aggregate    State      Type       Size
Available  Used%
--------- ------------   ------------ ---------- ---- ----------
---------- -----
vss       srcFG          -            online     RW         400TB
172.86GB  56%
vss       srcFG__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vss       srcFG__0002    aggr1        online     RW         25TB
10.86TB   56%
vss       srcFG__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vss       srcFG__0004    aggr1        online     RW         25TB
10.73TB   57%
vss       srcFG__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vss       srcFG__0006    aggr1        online     RW         25TB
10.64TB   57%
vss       srcFG__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

b. 대상 클러스터에서 소스 FlexGroup 볼륨과 동일한 수의 구성 요소와 함께 dP 유형의 대상 FlexGroup 볼륨을 생성합니다.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG

Warning: The FlexGroup volume "dstFG" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

c. 대상 클러스터에서 대상 FlexGroup 볼륨에 있는 구성 요소 수('volume show-volume volume volume_name * -is-f성분 TRUE')를 확인합니다

```
cluster2::> volume show  -volume dstFG* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dstFG          -            online     RW         400TB
172.86GB  56%
vsd       dstFG__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vsd       dstFG__0002    aggr1        online     RW         25TB
10.86TB   56%
vsd       dstFG__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vsd       dstFG__0004    aggr1        online     RW         25TB
10.73TB   57%
vsd       dstFG__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vsd       dstFG__0006    aggr1        online     RW         25TB
10.64TB   57%
vsd       dstFG__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

2. 작업 일정 생성:'작업 일정 cron create-name job_name-month month-DayOfWeek day_of_week-day day_of_month-hour-minute'입니다

   월-일-일-주-시간 옵션을 선택하면 월, 요일, 시간마다 작업을 실행하도록 모두 를 지정할 수 있습니다.

   다음 예에서는 토요일 오전 3시에 실행되는 my_weekly라는 작업 일정을 생성합니다.

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. 'Mirror-vault' 유형의 사용자 지정 정책을 만든 다음 미러 및 볼트 정책에 대한 규칙을 정의합니다.

   a. 'Mirror policy create-vserver svm_name-policy_name-type mirror-vault'라는 통합 데이터 보호 관계를 위한 'Mirror-vault' 유형의 사용자 지정 정책을 생성합니다

   b. 초기화 및 업데이트 작업 중에 전송되는 스냅샷을 결정하는 미러 및 볼트 정책에 대한 규칙을 정의합니다. `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule -snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

   사용자 지정 정책을 지정하지 않으면 통합 데이터 보호 관계에 MirorAndVault 정책이 사용됩니다.

4. 통합 데이터 보호 관계를 생성합니다. 'napmirror create-source-path src_svm:src_flexgroup-destination-path dest_svm:dest_flexgroup-type XDP -schedule schedule_name -policy MirrorAndVault'

ONTAP 9.4 이하 버전에서는, 정책이 '스냅샷 생성' 명령으로 지정되지 않으면 기본적으로 'irorAllSnapshots' 정책이 사용됩니다. ONTAP 9.5에서는 '스냅샷 생성' 명령으로 정책을 지정하지 않으면 기본적으로 'MirorAndVault' 정책이 사용됩니다.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path
vsd:dstFG -type XDP -schedule Daily -policy MirrorAndVault
```

에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 대상 클러스터에서 기본 전송인 'napmirror initialize-destination-path dest_svm:dest_flexgroup'을 수행하여 통합 데이터 보호 관계를 초기화합니다

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```

관련 정보

- "SnapMirror 생성"
- "SnapMirror 초기화"
- "스냅미러 정책 추가 규칙"
- "스냅미러 정책 생성"

ONTAP FlexGroup 볼륨에 대한 **SVM** 재해 복구 관계 생성

ONTAP 9.9.1부터 FlexGroup 볼륨을 사용하여 SVM 재해 복구(SVM DR) 관계를 생성할 수 있습니다. SVM DR 관계는 SVM 구성과 해당 데이터를 동기화 및 복제하여 재해 발생 시 FlexGroup 볼륨을 복구하는 기능과 이중화를 제공합니다. SVM DR에는 SnapMirror 라이센스가 필요합니다.

시작하기 전에

다음 항목을 사용하여 FlexGroup SVM DR 관계를 _ 생성할 수 없습니다.

- FlexClone FlexGroup 구성이 있습니다
- FlexGroup 볼륨은 계단식 관계의 일부입니다
- FlexGroup 볼륨은 팬아웃 관계의 일부이며 클러스터에서 ONTAP 9.12.1 이전의 ONTAP 버전을 실행하고 있습니다. (ONTAP 9.13.1 부터는 팬아웃 관계가 지원됩니다.)

이 작업에 대해

- 두 클러스터의 모든 노드는 SVM DR 지원을 추가한 노드(ONTAP 9.9.1 이상)와 동일한 ONTAP 버전을 실행해야 합니다.
- 1차 사이트와 2차 사이트 간의 SVM DR 관계는 상태가 양호해야 하며, FlexGroup 볼륨을 지원할 수 있는 1차 및 2차 SVM 모두에 충분한 공간이 있어야 합니다.
- ONTAP 9.12.1부터 FabricPool, FlexGroup 및 SVM DR이 함께 작동할 수 있습니다. ONTAP 9.12.1 이전 버전에서는 이러한 기능 중 두 가지가 함께 작동하지만 세 가지 기능이 모두 함께 작동하지는 않습니다.

- FlexGroup 볼륨이 팬아웃 관계에 속하는 FlexGroup SVM DR 관계를 생성할 때 다음 요구사항을 알아야 합니다.
  - 소스 및 타겟 클러스터에서 ONTAP 9.13.1 이상이 실행되고 있어야 합니다.
  - FlexGroup 볼륨을 사용하는 SVM DR은 8개 사이트에 대한 SnapMirror 팬아웃 관계를 지원합니다.

SVM DR 관계 생성에 대한 자세한 내용은 을 참조하십시오"SnapMirror SVM 복제 관리".

단계

1. SVM DR 관계를 생성하거나 기존 관계를 사용합니다.

   "전체 SVM 구성을 복제합니다"

2. 필요한 구성 요소 수로 운영 사이트에 FlexGroup 볼륨을 생성합니다.

   "FlexGroup 볼륨을 생성하는 중입니다".

   계속하기 전에 FlexGroup 및 모든 구성 구성요소가 생성될 때까지 기다리십시오.

3. FlexGroup 볼륨을 복제하려면 2차 사이트에서 SVM을 업데이트합니다. `snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:`

   를 입력하여 예약된 SnapMirror 업데이트가 이미 있는지 확인할 수도 있습니다 `snapmirror show -fields schedule`

4. 2차 사이트에서 SnapMirror 관계가 정상인지 '스냅샷 표시'인지 확인합니다

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                 Idle           -         true    -
```

5. 보조 사이트에서 새 FlexGroup 볼륨과 해당 구성 요소 '스냅샷 표시-확장'이 있는지 확인합니다

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                    Idle           -         true    -
vs1:fg_src  XDP  vs1_dst:fg_src
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0001
            XDP  vs1_dst:fg_src__0001
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0002
            XDP  vs1_dst:fg_src__0002
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0003
            XDP  vs1_dst:fg_src__0003
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0004
            XDP  vs1_dst:fg_src__0004
                             Snapmirrored
                                    Idle           -         true    -
6 entries were displayed.
```

관련 정보

- "스냅미러 쇼"
- "스냅미러 업데이트"

ONTAP FlexGroup SnapMirror 관계를 **SVM DR**으로 전환

기존 FlexGroup 볼륨 SnapMirror 관계를 전환하여 FlexGroup SVM DR 관계를 생성할 수 있습니다.

시작하기 전에

- FlexGroup 볼륨 SnapMirror 관계가 양호한 상태입니다.
- 소스 및 대상 FlexGroup 볼륨의 이름이 같습니다.

단계

1. SnapMirror 대상에서 FlexGroup 레벨 SnapMirror 관계인 '스냅샷 재동기화'를 다시 동기화합니다
2. FlexGroup SVM DR SnapMirror 관계를 생성합니다. FlexGroup 볼륨 SnapMirror 관계에 구성된 동일한 SnapMirror 정책을 사용하십시오. 'napmirror create-destination-path dest_svm: -source-path src_svm: -identity-preserve true-policy MirrorAllSnapshots'

   복제 관계를 생성할 때 'napmirror create' 명령의 '-identity-preserve true' 옵션을 사용해야 합니다.

   에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 'sapmirror show-destination-path dest_svm:-source-path src_svm:'의 관계가 끊어졌는지 확인합니다

```
snapmirror show -destination-path fg_vs_renamed: -source-path fg_vs:


Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
fg_vs:        XDP  fg_vs1_renamed:     Broken-off
                                      Idle           -         true    -
```

4. 대상 SVM을 중지합니다. 'vserver stop-vserver vs_name'

```
vserver stop -vserver fg_vs_renamed
[Job 245] Job is queued: Vserver Stop fg_vs_renamed.
[Job 245] Done
```

5. SVM SnapMirror 관계를 재동기화합니다. 'sapmirror resync-destination-path dest_svm:-source-path src_svm:

```
snapmirror resync -destination-path fg_vs_renamed: -source-path fg_vs:
Warning: This Vserver has volumes which are the destination of FlexVol
or FlexGroup SnapMirror relationships. A resync on the Vserver
SnapMirror relationship will cause disruptions in data access
```

6. SVM DR 레벨 SnapMirror 관계가 '스냅샷 표시-확장'이라는 양호한 유휴 상태에 도달하는지 확인합니다
7. FlexGroup SnapMirror 관계가 '스냅샷 표시'라는 양호한 상태인지 확인합니다

관련 정보

- "SnapMirror 생성"
- "스냅미러 재동기화"
- "스냅미러 쇼"

SVM-DR 관계 내에서 **ONTAP FlexVol** 볼륨을 **FlexGroup** 볼륨으로 변환합니다

ONTAP 9.10.1부터 FlexGroup 볼륨을 SVM-DR 소스의 FlexVol 볼륨으로 변환할 수 있습니다.

시작하기 전에

- 변환 중인 FlexVol 볼륨은 온라인이어야 합니다.
- FlexVol 볼륨의 작업 및 구성은 변환 프로세스와 호환되어야 합니다.

  FlexVol 볼륨에 비호환성이 있으며 볼륨 변환이 취소되면 오류 메시지가 생성됩니다. 수정 조치를 취하고 변환을 다시 시도할 수 있습니다.
  자세한 내용은 을 참조하십시오 "FlexVol 볼륨을 FlexGroup 볼륨으로 변환할 때의 고려 사항"

단계

1. 고급 권한 모드를 사용하여 로그인: `set -privilege advanced`
2. 대상에서 SVM-DR 관계를 업데이트합니다.

   ```
   snapmirror update -destination-path <destination_svm_name>: -source-path
   <source_svm_name>:
   ```

   옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 `-destination-path` 합니다.

3. SVM-DR 관계가 SnapMirro 상태에 있고 끊지 않았는지 확인합니다.

   ```
   snapmirror show
   ```

4. 대상 SVM에서 FlexVol 볼륨을 변환할 준비가 되었는지 확인합니다.

   ```
   volume conversion start -vserver <svm_name> -volume <vol_name> -check
   -only true
   ```

   이 명령에서 "This is a destination SVMDR volume" 이외의 오류가 발생하는 경우 적절한 수정 조치를 수행하고 명령을 다시 실행한 다음 변환을 계속할 수 있습니다.

5. 대상에서 SVM-DR 관계의 전송을 사용하지 않도록 설정:

   ```
   snapmirror quiesce -destination-path <dest_svm>:
   ```

옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 `-destination-path` 합니다.

6. 소스 클러스터에서 변환을 시작합니다.

```
volume conversion start -vserver <svm_name> -volume <vol_name>
```

7. 변환이 성공적인지 확인합니다.

```
volume show <vol_name> -fields volume-style-extended,state
```

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state

vserver  volume     state    volume-style-extended
-------  ---------  ------   ---------------------
vs0      my_volume  online   flexgroup
```

8. 대상 클러스터에서 관계에 대한 전송을 재개합니다.

```
snapmirror resume -destination-path <dest_svm>:
```

옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 `-destination-path` 합니다.

9. 대상 클러스터에서 업데이트를 수행하여 변환을 대상으로 전파합니다.

```
snapmirror update -destination-path <dest_svm>:
```

옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 `-destination-path` 합니다.

10. SVM-DR 관계가 SnapMirro 상태에 있고 끊지 않았는지 확인합니다.

```
snapmirror show
```

11. 대상에서 변환이 수행되었는지 확인합니다.

```
volume show <vol_name> -fields volume-style-extended,state
```

```
cluster-2::*> volume show my_volume -fields volume-style-extended,state

vserver  volume     state   volume-style-extended
-------  -------    ------  ---------------------
vs0_dst  my_volume  online  flexgroup
```

관련 정보

- "스냅미러 이력서"
- "SnapMirror 중지"
- "스냅미러 쇼"
- "스냅미러 업데이트"

ONTAP FlexGroup 볼륨에 대한 **SnapMirror** 캐스케이드 및 팬아웃 관계를 생성할 때의 고려 사항

FlexGroup 볼륨에 대한 계단식 배열 및 팬아웃 관계를 만들 때 유의해야 할 지원 고려 사항 및 제한 사항이 있습니다.

다중 구간 관계를 만들 때의 고려 사항

- 각 관계는 클러스터 간 또는 클러스터 내 관계일 수 있습니다.
- 비동기 미러, 미러 볼트, 볼트를 포함한 모든 비동기 정책 유형은 두 관계 모두에서 지원됩니다.
- "MirrorAllSnapshots"만 지원되며 "MirrorLatest" 비동기식 미러 정책은 지원되지 않습니다.
- 장기 보존 스냅샷은 지원되지 않습니다.

  자세히 알아보세요"장기 보존 스냅샷" .

- 다중 구간 XDP 관계의 동시 업데이트가 지원됩니다.
- A에서 B로, B에서 C로, A에서 C로 다시 동기화하거나 C에서 A로 다시 동기화하는 것을 지원합니다
- 또한 모든 노드에서 ONTAP 9.9.1 이상을 실행 중인 경우 A 및 B FlexGroup 볼륨도 팬아웃을 지원합니다.
- B 또는 C FlexGroup 볼륨에서 복원 작업이 지원됩니다.
- 대상이 복구 관계의 소스인 동안에는 FlexGroup 관계의 전송이 지원되지 않습니다.
- FlexGroup 복원 대상은 다른 FlexGroup 관계의 대상이 될 수 없습니다.
- FlexGroup 파일 복원 작업은 일반 FlexGroup 복원 작업과 동일한 제한 사항을 갖습니다.
- B 및 C FlexGroup 볼륨이 상주하는 클러스터의 모든 노드에서 ONTAP 9.9.1 이상을 실행해야 합니다.
- 모든 확장 및 자동 확장 기능이 지원됩니다.
- A에서 B와 C 사이의 다중 구간 구성에서는 A에서 B로 B에서 B로, B에서 C로 구성되는 서로 다른 수의 구성 SnapMirror 관계가 있으면 B에서 C로 SnapMirror 관계에 대해 소스의 중단 작업이 지원되지 않습니다.
- System Manager는 ONTAP 버전에 관계없이 계단식 관계를 지원하지 않습니다.
- A를 B에서 C로 변환하는 경우 FlexVol 관계를 FlexGroup 관계로 변환할 때 먼저 B를 C 홉으로 변환해야 합니다.

- REST에서 지원하는 정책 유형과 관련된 모든 FlexGroup 캐스케이드 구성은 Cascading FlexGroup 구성의 REST API에서도 지원됩니다.
- FlexVol 관계와 마찬가지로 FlexGroup cascading은 'napmirror protect' 명령에서는 지원되지 않습니다.

팬아웃 관계를 만들기 위한 고려 사항

- 2개 이상의 FlexGroup 팬아웃 관계가 지원됩니다(예: A ~ B, A ~ C, 최대 8개의 팬아웃 다리).
- 각 관계는 클러스터 간 또는 클러스터 내가 될 수 있습니다.
- 동시 업데이트는 두 관계에 대해 지원됩니다.
- 모든 확장 및 자동 확장 기능이 지원됩니다.
- 관계의 팬아웃 레그의 구성 요소 SnapMirror 관계 수가 서로 다른 경우 소스에서 B 및 A와 C 사이의 관계에 대해 중단 작업이 지원되지 않습니다.
- 소스 및 대상 FlexGroup 볼륨이 상주하는 클러스터의 모든 노드에서 ONTAP 9.9.1 이상을 실행해야 합니다.
- 현재 FlexGroup SnapMirror에 대해 지원되는 모든 비동기식 정책 유형은 팬아웃 관계에서 지원됩니다.
- B에서 C FlexGroup 볼륨으로 복원 작업을 수행할 수 있습니다.
- REST에서 지원하는 정책 유형의 모든 팬아웃 구성은 FlexGroup 팬아웃 구성의 REST API에도 지원됩니다.

관련 정보

- "SnapMirror 보호"

ONTAP FlexGroup 볼륨에 대한 **SnapVault** 백업 관계 및 통합 데이터 보호 관계를 생성할 때의 고려 사항

SnapVault 볼륨에 대한 FlexGroup 백업 관계 및 통합 데이터 보호 관계를 생성할 때 고려해야 할 사항에 대해 알고 있어야 합니다.

- 최신 공용 스냅샷보다 최신 상태의 대상 볼륨에 스냅샷을 보존할 수 있는 옵션을 사용하여 SnapVault 백업 관계 및 통합 데이터 보호 관계를 다시 동기화할 수 `-preserve` 있습니다.
- FlexGroup 볼륨에서는 장기 보존이 지원되지 않습니다.

  장기 보존을 통해 소스 볼륨에 스냅샷을 저장할 필요 없이 대상 볼륨에 스냅샷을 직접 생성할 수 있습니다.

- FlexGroup 볼륨에 대해서는 '스냅샷' 명령 '만료 시간' 옵션이 지원되지 않습니다.
- SnapVault 백업 관계 및 통합 데이터 보호 관계의 대상 FlexGroup 볼륨에서는 스토리지 효율성을 구성할 수 없습니다.
- FlexGroup 볼륨에 대한 SnapVault 백업 관계 및 통합 데이터 보호 관계의 스냅샷의 이름은 변경할 수 없습니다.
- FlexGroup 볼륨은 하나의 백업 관계나 복구 관계의 소스 볼륨일 수 있습니다.

  FlexGroup 볼륨은 두 SnapVault 관계, 두 개의 복구 관계 또는 SnapVault 백업 관계 및 복구 관계의 소스가 될 수 없습니다.

- 소스 FlexGroup 볼륨에서 스냅샷을 삭제하고 동일한 이름의 스냅샷을 다시 생성하는 경우 대상 볼륨에 동일한 이름의 스냅샷이 있을 경우 대상 FlexGroup 볼륨으로의 다음 업데이트 전송이 실패합니다.

  FlexGroup 볼륨에 대해 스냅샷 이름을 바꿀 수 없기 때문입니다.

ONTAP FlexGroup 볼륨의 SnapMirror 데이터 전송을 모니터링합니다

FlexGroup 볼륨 SnapMirror 관계의 상태를 주기적으로 모니터링하여 대상 FlexGroup 볼륨이 지정된 일정에 따라 정기적으로 업데이트되는지 확인해야 합니다.

이 작업에 대해

대상 클러스터에서 이 작업을 수행해야 합니다.

단계

1. '스냅미러 show-relationship-group-type FlexGroup'와 같은 모든 FlexGroup 볼륨 관계의 SnapMirror 관계 상태를 봅니다

```
cluster2::> snapmirror show -relationship-group-type flexgroup

Progress
Source             Destination Mirror  Relationship   Total
Last
Path        Type   Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:d        Snapmirrored
                                    Idle           -         true    -
vss:s2      XDP  vsd:d2       Uninitialized
                                    Idle           -         true    -
2 entries were displayed.
```

관련 정보

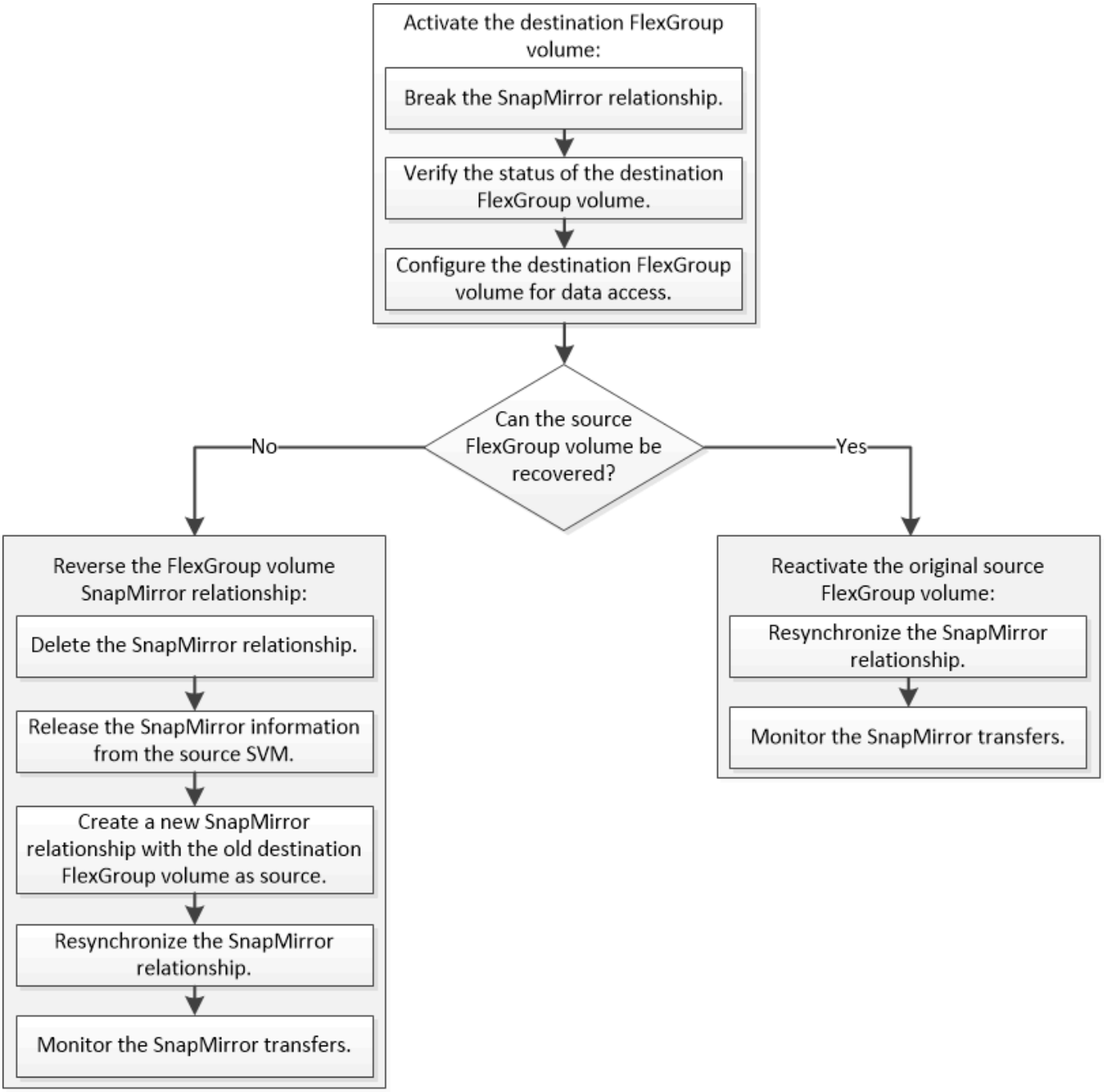
- "스냅미러 쇼"

FlexGroup 볼륨에 대한 데이터 보호 작업을 관리합니다

FlexGroup 볼륨의 재해 복구

ONTAP FlexGroup 볼륨의 재해 복구 워크플로우

소스 FlexGroup 볼륨에서 재해가 발생하면 대상 FlexGroup 볼륨을 활성화하고 클라이언트 액세스를 리디렉션해야 합니다. 소스 FlexGroup 볼륨을 복구할 수 있는지 여부에 따라 소스 FlexGroup 볼륨을 다시 활성화하거나 SnapMirror 관계를 반대로 해야 합니다.



이 작업에 대해

SnapMirror 중단 및 재동기화와 같은 일부 SnapMirror 작업이 실행 중인 경우 대상 FlexGroup 볼륨에 대한 클라이언트 액세스가 잠시 차단됩니다. SnapMirror 작업이 실패하면 일부 구성요소가 이 상태로 남아 FlexGroup 볼륨에 대한 액세스가 거부될 수 있습니다. 이 경우 SnapMirror 작업을 다시 시도해야 합니다.

대상 **ONTAP FlexGroup** 볼륨을 활성화합니다

데이터 손상, 실수로 인한 삭제 또는 오프라인 상태와 같은 이벤트로 인해 소스 FlexGroup 볼륨에서 데이터를 처리할 수 없는 경우 소스 FlexGroup 볼륨의 데이터를 복구할 때까지 대상 FlexGroup 볼륨을 활성화하여 데이터 액세스를 제공해야 합니다. 앞으로 SnapMirror 데이터 전송을 중지하고 SnapMirror 관계를 끊는 작업이 활성화 됩니다.

이 작업에 대해

대상 클러스터에서 이 작업을 수행해야 합니다.

단계

1. FlexGroup 볼륨 SnapMirror 관계에 대한 향후 전송을 해제합니다. 'napmirror quiesdest_svm:dest_flexgroup'

```
cluster2::> snapmirror quiesce -destination-path vsd:dst
```

2. FlexGroup 볼륨 SnapMirror 관계를 끊습니다: 'napmirror break dest_svm: dest_flexgroup'

```
cluster2::> snapmirror break -destination-path vsd:dst
```

3. SnapMirror 관계의 '스냅샷 표시-확장' 상태를 봅니다

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:dst        Broken-off
                                    Idle           -         true    -
vss:s__0001 XDP  vsd:dst__0001  Broken-off
                                    Idle           -         true    -
vss:s__0002 XDP  vsd:dst__0002  Broken-off
                                    Idle           -         true    -
vss:s__0003 XDP  vsd:dst__0003  Broken-off
                                    Idle           -         true    -
vss:s__0004 XDP  vsd:dst__0004  Broken-off
                                    Idle           -         true    -
vss:s__0005 XDP  vsd:dst__0005  Broken-off
                                    Idle           -         true    -
vss:s__0006 XDP  vsd:dst__0006  Broken-off
                                    Idle           -         true    -
vss:s__0007 XDP  vsd:dst__0007  Broken-off
                                    Idle           -         true    -
vss:s__0008 XDP  vsd:dst__0008  Broken-off
                                    Idle           -         true    -
...
```

각 구성요소의 SnapMirror 관계 상태는 '부분-오프'입니다.

4. 대상 FlexGroup 볼륨이 읽기/쓰기인지 확인합니다. 'volume show -vserver svm_name'

```
cluster2::> volume show -vserver vsd
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dst          -            online     **RW**          2GB
1.54GB   22%
vsd       d2           -            online     DP           2GB
1.55GB   22%
vsd       root_vs0     aggr1        online     RW        100MB
94.02MB    5%
3 entries were displayed.
```

5. 대상 FlexGroup 볼륨으로 클라이언트를 리디렉션합니다.

관련 정보

- "SnapMirror가 깨졌습니다"
- "SnapMirror 중지"
- "스냅미러 쇼"

재해 발생 후 원래 소스 **ONTAP FlexGroup** 볼륨을 다시 활성화합니다

소스 FlexGroup 볼륨을 사용할 수 있게 되면 원래 소스 및 원래 대상 FlexGroup 볼륨을 재동기화할 수 있습니다. 대상 FlexGroup 볼륨의 새 데이터가 손실됩니다.

이 작업에 대해

대상 볼륨에 대한 활성 할당량 규칙이 비활성화되고 재동기화가 수행되기 전에 할당량 규칙이 삭제됩니다.

"volume quota policy rule create" 및 "volume quota modify" 명령을 사용하여 재동기화 작업이 완료된 후 할당량 규칙을 생성하고 다시 활성화할 수 있습니다.

단계

1. 대상 클러스터에서 FlexGroup 볼륨 SnapMirror 관계를 재동기화합니다. 'sapmirror resync-destination-path dst_svm:dest_flexgroup'
2. SnapMirror 관계의 '스냅샷 표시-확장' 상태를 봅니다

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:dst        Snapmirrored
                                    Idle           -         true    -
vss:s__0001 XDP  vsd:dst__0001  Snapmirrored
                                    Idle           -         true    -
vss:s__0002 XDP  vsd:dst__0002  Snapmirrored
                                    Idle           -         true    -
vss:s__0003 XDP  vsd:dst__0003  Snapmirrored
                                    Idle           -         true    -
vss:s__0004 XDP  vsd:dst__0004  Snapmirrored
                                    Idle           -         true    -
vss:s__0005 XDP  vsd:dst__0005  Snapmirrored
                                    Idle           -         true    -
vss:s__0006 XDP  vsd:dst__0006  Snapmirrored
                                    Idle           -         true    -
vss:s__0007 XDP  vsd:dst__0007  Snapmirrored
                                    Idle           -         true    -
vss:s__0008 XDP  vsd:dst__0008  Snapmirrored
                                    Idle           -         true    -
...
```

각 구성요소의 SnapMirror 관계 상태는 '스냅샷 미러링'입니다.

관련 정보

- "스냅미러 재동기화"
- "스냅미러 쇼"

재해 복구 중에 **ONTAP FlexGroup** 볼륨 간의 역방향 **SnapMirror** 관계

재해로 인해 SnapMirror 관계의 소스 FlexGroup 볼륨이 비활성화되면 소스 FlexGroup 볼륨을 복구하거나 교체하는 동안 대상 FlexGroup 볼륨을 사용하여 데이터를 제공할 수 있습니다. 소스 FlexGroup 볼륨이 온라인 상태가 되면 원래 소스 FlexGroup 볼륨을 읽기 전용 타겟으로 설정하고 SnapMirror 관계를 반대로 전환할 수 있습니다.

이 작업에 대해

대상 볼륨에 대한 활성 할당량 규칙이 비활성화되고 재동기화가 수행되기 전에 할당량 규칙이 삭제됩니다.

"volume quota policy rule create" 및 "volume quota modify" 명령을 사용하여 재동기화 작업이 완료된 후 할당량 규칙을 생성하고 다시 활성화할 수 있습니다.

단계

1. 원래 대상 FlexGroup 볼륨에서 소스 FlexGroup 볼륨과 대상 FlexGroup 볼륨 간의 데이터 보호 미러 관계를 제거합니다. 'sapmirror delete -destination-path svm_name: volume_name'

```
cluster2::> snapmirror delete -destination-path vsd:dst
```

2. 원본 소스 FlexGroup 볼륨에서 소스 FlexGroup 볼륨에서 'sapmirror release-destination-path svm_name:volume_name-relationship-info-only' 관계 정보를 제거합니다

   SnapMirror 관계를 삭제한 후에는 재동기화 작업을 시도하기 전에 소스 FlexGroup 볼륨에서 관계 정보를 제거해야 합니다.

```
cluster1::> snapmirror release -destination-path vsd:dst -relationship
-info-only true
```

3. 새 대상 FlexGroup 볼륨에서 미러 관계를 생성합니다. 'napmirror create-source-path src_svm_name:volume_name-destination-path dst_svm_name:volume_name-type XDP-policy MirrorAllSnapshots'

```
cluster1::> snapmirror create -source-path vsd:dst -destination-path
vss:src -type XDP -policy MirrorAllSnapshots
```

   에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 새 대상 FlexGroup 볼륨에서 소스 FlexGroup 'sapmirror resync-source-path svm_name:volume_name'을 다시 동기화합니다

```
cluster1::> snapmirror resync -source-path vsd:dst
```

5. SnapMirror 전송, '스냅샷 표시-확장'을 모니터링합니다

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vsd:dst       XDP  vss:src        Snapmirrored
                                      Idle           -         true    -
vss:dst__0001 XDP  vss:src__0001  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0002 XDP  vss:src__0002  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0003 XDP  vss:src__0003  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0004 XDP  vss:src__0004  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0005 XDP  vss:src__0005  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0006 XDP  vss:src__0006  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0007 XDP  vss:src__0007  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0008 XDP  vss:src__0008  Snapmirrored
                                      Idle           -         true    -
...
```

각 구성요소의 SnapMirror 관계 상태는 재동기화가 성공했음을 나타내는 '스냅샷 미러링'으로 표시됩니다.

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"
- "스냅미러 쇼"

SnapMirror 관계에서 FlexGroup 볼륨을 확장합니다

SnapMirror 관계에서 ONTAP FlexGroup 볼륨 확장

ONTAP 9.3부터는 새 구성요소를 볼륨에 추가하여 SnapMirror 관계에 있는 소스 FlexGroup 볼륨과 타겟 FlexGroup 볼륨을 확장할 수 있습니다. 대상 볼륨을 수동 또는 자동으로 확장할 수

있습니다.

이 작업에 대해

- 이 작업은 FlexGroup 볼륨 확장을 자동으로 관리하는 SVM-DR 관계에는 적용되지 않습니다.
- 확장 후에는 소스 FlexGroup 볼륨과 SnapMirror 관계의 타겟 FlexGroup 볼륨에 있는 구성 수가 일치해야 합니다.

  볼륨의 구성요소 수가 일치하지 않는 경우 SnapMirror 전송이 실패합니다.

- 확장 프로세스가 진행 중일 때는 SnapMirror 작업을 수행하지 않아야 합니다.
- 확장 프로세스가 완료되기 전에 재해가 발생할 경우 SnapMirror 관계를 끊은 후 작업이 성공할 때까지 기다려야 합니다.

> 확장 프로세스가 진행 중일 때는 재해 발생 시에만 SnapMirror 관계를 끊어야 합니다. 재해가 발생할 경우 중단 작업을 완료하는 데 약간의 시간이 걸릴 수 있습니다. 재동기화 작업을 수행하기 전에 중단 작업이 성공적으로 완료될 때까지 기다려야 합니다. 중단 작업이 실패하면 중단 작업을 다시 시도해야 합니다. 중단 작업이 실패하면 중단 작업 후 일부 새 구성 요소들이 대상 FlexGroup 볼륨에 남아 있을 수 있습니다. 계속 진행하기 전에 이러한 구성 요소들을 수동으로 삭제하는 것이 좋습니다.

SnapMirror 관계의 소스 **ONTAP FlexGroup** 볼륨을 확장합니다

ONTAP 9.3부터 소스 볼륨에 새 구성요소를 추가하여 SnapMirror 관계의 소스 FlexGroup 볼륨을 확장할 수 있습니다. 일반 FlexGroup 볼륨(읽기-쓰기 볼륨)을 확장하는 것과 동일한 방식으로 소스 볼륨을 확장할 수 있습니다.

단계

1. 소스 FlexGroup 볼륨(+ volume expand -vserver vserver_name -volume fg_src -aggr -list aggregate name)을 확장합니다. [-aggr-list-multiplier f구성요소_per_aggr]+'

```
cluster1::> volume expand -volume src_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_src

Warning: The following number of constituents of size 50GB will be added
to FlexGroup "src_fg": 2.
Expanding the FlexGroup will cause the state of all Snapshot copies to
be set to "partial".
Partial Snapshot copies cannot be restored.
Do you want to continue? {y|n}: Y
[Job 146] Job succeeded: Successful
```

   볼륨이 확장되기 전에 생성된 모든 스냅샷의 상태가 Partial로 변경됩니다.

SnapMirror 관계의 대상 **ONTAP FlexGroup** 볼륨을 확장합니다

대상 FlexGroup 볼륨을 확장하고 SnapMirror 관계를 자동 또는 수동으로 다시 설정할 수 있습니다. 기본적으로 SnapMirror 관계는 자동 확장을 위해 설정되고 소스 볼륨이 확장되면 대상

FlexGroup 볼륨이 자동으로 확장됩니다.

시작하기 전에

- 소스 FlexGroup 볼륨이 확장되어야 합니다.
- SnapMirror 관계는 '미스네이ed' 상태여야 합니다.

  SnapMirror 관계를 끊거나 삭제할 수 없습니다.

이 작업에 대해

- 대상 FlexGroup 볼륨이 생성되면 기본적으로 자동 확장이 가능하도록 볼륨이 설정됩니다.

  필요한 경우 수동 확장을 위해 대상 FlexGroup 볼륨을 수정할 수 있습니다.

  가장 좋은 방법은 대상 FlexGroup 볼륨을 자동으로 확장하는 것입니다.

- 소스 FlexGroup 볼륨과 타겟 FlexGroup 볼륨 모두에 동일한 수의 구성요소가 있을 때까지 모든 SnapMirror 작업이 실패합니다.
- SnapMirror 관계가 끊거나 삭제된 후 대상 FlexGroup 볼륨을 확장하는 경우 원래 관계를 다시 동기화할 수 없습니다.

  대상 FlexGroup 볼륨을 재사용하려면 SnapMirror 관계를 삭제한 후 볼륨을 확장하지 마십시오.

선택

- 업데이트 전송을 수행하여 대상 FlexGroup 볼륨을 자동으로 확장합니다.

  a. 'sapmirror update-destination-path svm:vol_name'이라는 SnapMirror 업데이트 전송을 수행합니다

  b. SnapMirror 관계의 상태가 '스냅샷 표시' 상태인지 확인합니다

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress
Healthy Updated
----------- ---- ------------ ------- -------------- ---------
------- --------
vs_src:src_fg
            XDP  vs_dst:dst_fg
                              Snapmirrored
                                      Idle           -         true
-
```

  애그리게이트의 크기와 가용성에 따라 애그리게이트가 자동으로 선택되고, 소스 FlexGroup 볼륨의 구성요소에 맞는 새로운 구성요소가 타겟 FlexGroup 볼륨에 추가됩니다. 확장 후 재동기화 작업이 자동으로 트리거됩니다.

- 대상 FlexGroup 볼륨을 수동으로 확장합니다.

  a. SnapMirror 관계가 자동 확장 모드에 있는 경우 SnapMirror 관계를 수동 확장 모드인 '스냅샷 수정-대상-경로 svm:vol_name-is-auto-expand-enabled false'로 설정합니다

```
cluster2::> snapmirror modify -destination-path vs_dst:dst_fg -is
-auto-expand-enabled false
Operation succeeded: snapmirror modify for the relationship with
destination "vs_dst:dst_fg".
```

  b. SnapMirror 관계 중지:'sapmirror-destination-path svm:vol_name'입니다

```
cluster2::> snapmirror quiesce -destination-path vs_dst:dst_fg
Operation succeeded: snapmirror quiesce for destination
"vs_dst:dst_fg".
```

  c. 대상 FlexGroup 볼륨을 확장합니다. '+ volume expand -vserver vserver_name -volume fg_name -aggr -list aggregate name,… [-aggr-list-multiplier f구성요소_per_aggr]+'

```
cluster2::> volume expand -volume dst_fg -aggr-list aggr1 -aggr-list
-multiplier 2  -vserver vs_dst

Warning: The following number of constituents of size 50GB will be
added to FlexGroup "dst_fg": 2.
Do you want to continue? {y|n}: y
[Job 68] Job succeeded: Successful
```

  d. SnapMirror 관계 'sapmirror resync-destination-path svm:vol_name'을 재동기화합니다

```
cluster2::> snapmirror resync -destination-path vs_dst:dst_fg
Operation is queued: snapmirror resync to destination
"vs_dst:dst_fg".
```

  e. SnapMirror 관계의 상태가 '스냅샷 표시':'스냅샷 표시'인지 확인합니다

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress
Healthy Updated
----------- ---- ------------ ------- -------------- ---------
------- --------
vs_src:src_fg
            XDP  vs_dst:dst_fg
                              Snapmirrored
                                      Idle           -         true
-
```

관련 정보

- "SnapMirror 중지"
- "스냅미러 재동기화"
- "스냅미러 쇼"

ONTAP FlexGroup 볼륨에서 **SnapMirror** 단일 파일 복원을 수행합니다

ONTAP 9.8부터 FlexGroup SnapMirror 볼트 또는 UDP 대상에서 단일 파일을 복원할 수 있습니다.

이 작업에 대해

- 모든 기하 구조의 FlexGroup 볼륨에서 모든 기하 구조의 FlexGroup 볼륨으로 복원할 수 있습니다.
- 복원 작업당 하나의 파일만 지원됩니다.
- 원래 소스 FlexGroup 볼륨이나 새로운 FlexGroup 볼륨으로 복원할 수 있습니다.
- 원격 펜싱된 파일 조회는 지원되지 않습니다.

  소스 파일이 펜싱된 경우 단일 파일 복구가 실패합니다.

- 중단된 단일 파일 복원을 다시 시작하거나 정리할 수 있습니다.
- 실패한 단일 파일 복원 전송은 다음을 사용하여 정리해야 합니다. `clean-up-failure` 옵션 `snapmirror restore` 명령.

  에 대한 자세한 내용은 `snapmirror restore` "ONTAP 명령 참조입니다"을 참조하십시오.

- FlexGroup 단일 파일 복원이 진행 중이거나 중단된 상태일 때 FlexGroup 볼륨 확장이 지원됩니다.

단계

1. FlexGroup 볼륨에서 파일 복원: `snapmirror restore -destination-path destination_path -source-path source_path -file-list /f1 -throttle throttle -source-snapshot`

snapshot

다음은 FlexGroup 볼륨 단일 파일 복원 작업의 예입니다.

```
vserverA::> snapmirror restore -destination-path vs0:fg2 -source-path
vs0:fgd -file-list /f1 -throttle 5 -source-snapshot snapmirror.81072ce1-
d57b-11e9-94c0-005056a7e422_2159190496.2019-09-19_062631
[Job 135] Job is queued: snapmirror restore from source "vs0:fgd" for
the snapshot snapmirror.81072ce1-d57b-11e9-94c0-
005056a7e422_2159190496.2019-09-19_062631.
vserverA::> snapmirror show

Source              Destination Mirror   Relationship
Total Last
Path       Type   Path            State    Status           Progress
Healthy Updated
---------- ----      ------------     -------    ---------
----- --------- ------- --------
vs0:v1d RST    vs0:v2          -           Transferring Idle 83.12KB
true 09/19 11:38:42

vserverA::*> snapmirror show vs0:fg2

Source Path: vs0:fgd
Source Cluster: -
Source Vserver: vs0
Source Volume: fgd
Destination Path: vs0:fg2
Destination Cluster: -
Destination Vserver: vs0
Destination Volume: fg2
Relationship Type: RST
Relationship Group Type: none
Managing Vserver: vs0
SnapMirror Schedule: -
SnapMirror Policy Type: -
SnapMirror Policy: -
Tries Limit: -
Throttle (KB/sec): unlimited
Current Transfer Throttle (KB/sec): 2
Mirror State: -
Relationship Status: Transferring
File Restore File Count: 1
File Restore File List: f1
Transfer Snapshot: snapmirror.81072ce1-d57b-11e9-94c0-
005056a7e422_2159190496.2019-09-19_062631
```

```
Snapshot Progress: 2.87MB
Total Progress: 2.87MB
Network Compression Ratio: 1:1
Snapshot Checkpoint: 2.97KB
Newest Snapshot: -
Newest Snapshot Timestamp: -
Exported Snapshot: -
Exported Snapshot Timestamp: -
Healthy: true
Physical Replica: -
Relationship ID: e6081667-dacb-11e9-94c0-005056a7e422
Source Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Destination Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Current Operation ID: 138f12e6-dacc-11e9-94c0-005056a7e422
Transfer Type: cg_file_restore
Transfer Error: -
Last Transfer Type: -
Last Transfer Error: -
Last Transfer Error Codes: -
Last Transfer Size: -
Last Transfer Network Compression Ratio: -
Last Transfer Duration: -
Last Transfer From: -
Last Transfer End Timestamp: -
Unhealthy Reason: -
Progress Last Updated: 09/19 07:07:36
Relationship Capability: 8.2 and above
Lag Time: -
Current Transfer Priority: normal
SMTape Operation: -
Constituent Relationship: false
Destination Volume Node Name: vserverA
Identity Preserve Vserver DR: -
Number of Successful Updates: 0
Number of Failed Updates: 0
Number of Successful Resyncs: 0
Number of Failed Resyncs: 0
Number of Successful Breaks: 0
Number of Failed Breaks: 0
Total Transfer Bytes: 0
Total Transfer Time in Seconds: 0
Source Volume MSIDs Preserved: -
OpMask: ffffffffffffffff
Is Auto Expand Enabled: -
Source Endpoint UUID: -
Destination Endpoint UUID: -
```

```
Is Catalog Enabled: false
```

관련 정보

- "스냅미러 쇼"

SnapVault 백업에서 ONTAP FlexGroup 볼륨을 복원합니다

SnapVault 2차 볼륨의 스냅숏에서 FlexGroup 볼륨의 전체 볼륨 복원 작업을 수행할 수 있습니다. FlexGroup 볼륨을 원래 소스 볼륨이나 새 FlexGroup 볼륨으로 복원할 수 있습니다.

시작하기 전에

FlexGroup 볼륨에 대한 SnapVault 백업에서 복구할 때는 특정 고려 사항을 염두에 두어야 합니다.

- SnapVault 백업의 부분 스냅샷에 대해서는 기준 복구만 지원됩니다. 대상 볼륨의 구성 요소 수는 스냅샷을 생성할 때 소스 볼륨의 구성 요소 수와 일치해야 합니다.
- 복구 작업이 실패하면 복구 작업이 완료될 때까지 다른 작업은 허용되지 않습니다. 복구 작업을 다시 시도하거나 cleanup 매개 변수를 사용하여 복구 작업을 실행할 수 있습니다.
- FlexGroup 볼륨은 하나의 백업 관계나 복구 관계의 소스 볼륨일 수 있습니다. FlexGroup 볼륨은 두 SnapVault 관계, 두 개의 복원 관계 또는 SnapVault 관계 및 복원 관계의 소스가 될 수 없습니다.
- SnapVault 백업 및 복원 작업을 병렬로 실행할 수 없습니다. 기준 복원 작업 또는 증분 복원 작업이 진행 중인 경우 백업 작업을 중지해야 합니다.
- 대상 FlexGroup 볼륨에서 부분 스냅샷의 복구 작업을 중단해야 합니다. 소스 볼륨에서 부분 스냅샷의 복구 작업은 중단할 수 없습니다.
- 복구 작업을 중단하는 경우 이전 복구 작업에 사용된 것과 동일한 스냅샷을 사용하여 복구 작업을 다시 시작해야 합니다.

이 작업에 대해

복구를 수행하기 전에 대상 FlexGroup 볼륨의 활성 할당량 규칙이 비활성화됩니다.

복원 작업이 완료된 후 "volume quota modify" 명령을 사용하여 할당량 규칙을 다시 활성화할 수 있습니다.

단계

1. Restore the FlexGroup volume: `snapmirror restore -source-path` *`src_svm:src_flexgroup`* `-destination-path` *`dest_svm:dest_flexgroup`* `-snapshot` *`snapshot_name`* `snapshot_name` 소스 볼륨에서 대상 볼륨으로 복구할 스냅샷입니다. 스냅샷이 지정되지 않은 경우 대상 볼륨이 최신 스냅샷에서 복구됩니다.

```
vserverA::> snapmirror restore -source-path vserverB:dstFG -destination
-path vserverA:newFG -snapshot daily.2016-07-15_0010
Warning: This is a disruptive operation and the volume vserverA:newFG
will be read-only until the operation completes
Do you want to continue? {y|n}: y
```

관련 정보

- "SnapMirror 복원"

ONTAP FlexGroup 볼륨에서 **SVM** 보호 비활성화

FlexGroup 볼륨에서 SVM DR 플래그가 '보호'로 설정된 경우 해당 플래그를 보호되지 않음으로 설정하여 FlexGroup 볼륨에서 SVM DR '보호'를 비활성화할 수 있습니다.

시작하기 전에

- 1차 및 2차 시스템 간의 SVM DR 관계가 양호합니다.
- SVM DR 보호 매개 변수가 '보호됨'으로 설정됩니다.

단계

1. FlexGroup 볼륨에 대한 vserver-dr-protection 매개변수를 '보호되지 않음'으로 변경하려면 'volume modify' 명령을 사용하여 보호를 해제하십시오.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection unprotected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. 보조 사이트에서 'sapmirror update-destination-path destination_svm_name: - source-path source_svm_name:'을(를) 업데이트하십시오
3. SnapMirror 관계가 정상인지 '스냅샷 표시'로 확인합니다
4. FlexGroup SnapMirror 관계가 '스냅샷 표시-확장'으로 제거되었는지 확인합니다

관련 정보

- "스냅미러 쇼"
- "스냅미러 업데이트"

ONTAP FlexGroup 볼륨에서 **SVM** 보호 활성화

FlexGroup 볼륨에서 SVM DR 보호 플래그가 '보호되지 않음'으로 설정된 경우 SVM DR 보호를 위해 플래그를 '보호됨'으로 설정할 수 있습니다.

시작하기 전에

- 1차 및 2차 시스템 간의 SVM DR 관계가 양호합니다.
- SVM DR 보호 매개 변수를 '보호되지 않음'으로 설정합니다.

단계

1. FlexGroup 볼륨에 대한 vserver-dr-protection 매개변수를 'protected'로 변경하려면 볼륨 수정을 사용하여 보호를 활성화하십시오.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection protected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. 보조 사이트에서 'sapmirror update-destination-path destination_svm_name-source-path source_svm_name'이라는 SVM을 업데이트합니다

```
snapmirror update -destination-path vs1_dst: -source-path vs1:
```

3. SnapMirror 관계가 정상인지 '스냅샷 표시'로 확인합니다

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                 Idle           -         true    -
```

4. FlexGroup SnapMirror 관계가 정상인지 '스냅샷 표시-확장'으로 확인합니다

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                  Idle           -         true    -
vs1:fg_src  XDP  vs1_dst:fg_src
                              Snapmirrored
                                  Idle           -         true    -
vs1:fg_src__0001
            XDP  vs1_dst:fg_src__0001
                              Snapmirrored
                                  Idle           -         true    -
vs1:fg_src__0002
            XDP  vs1_dst:fg_src__0002
                              Snapmirrored
                                  Idle           -         true    -
vs1:fg_src__0003
            XDP  vs1_dst:fg_src__0003
                              Snapmirrored
                                  Idle           -         true    -
vs1:fg_src__0004
            XDP  vs1_dst:fg_src__0004
                              Snapmirrored
                                  Idle           -         true    -
6 entries were displayed.
```

관련 정보

- "스냅미러 쇼"

FlexVol 볼륨을 FlexGroup 볼륨으로 변환합니다

ONTAP FlexVol 볼륨을 FlexGroup 볼륨으로 변환하는 방법에 대해 알아봅니다

FlexVol 볼륨을 공간 제한 이상으로 확장하려면 FlexVol 볼륨을 FlexGroup 볼륨으로 변환할 수 있습니다. ONTAP 9.7부터는 SnapMirror 관계에 있는 독립 실행형 FlexVol 볼륨 또는 FlexVol 볼륨을 FlexGroup 볼륨으로 변환할 수 있습니다.

FlexVol 볼륨을 FlexGroup 볼륨으로 변환할 때의 고려 사항

당신은 이것을 알고 있어야 합니다 "지원되는 기능 및 작업" FlexVol 볼륨을 FlexGroup 볼륨으로 변환하기로 결정하기 전에.

변환 중에는 작업이 지원되지 않습니다

볼륨 변환이 진행 중일 때는 다음 작업이 허용되지 않습니다.

- 볼륨 이동
- 애그리게이트 재배치
- 고가용성 구성에서 계획된 테이크오버 및 반환
- 고가용성 구성에서 수동 및 자동 반환
- 클러스터 업그레이드 및 되돌리기
- FlexClone 볼륨 분할
- 볼륨 재호스팅
- 볼륨 수정 및 자동 크기 조정
- 볼륨 이름 바꾸기
- 오브젝트 저장소를 Aggregate에 연결합니다
- MetroCluster 구성에서 협상된 전환
- SnapMirror 작업
- 스냅샷에서 복구 중입니다
- 할당량 작업
- 스토리지 효율성 작업

성공적인 변환 후 FlexGroup 볼륨에서 이러한 작업을 수행할 수 있습니다.

FlexGroup 볼륨에서 지원되지 않는 구성입니다

- 오프라인 또는 제한된 볼륨
- SVM 루트 볼륨
- 산
- SMB 1.0
- NVMe 네임스페이스
- 원격 볼륨 섀도 복사본 서비스(VSS)

ONTAP FlexVol 볼륨을 ONTAP FlexGroup 볼륨으로 변환합니다

ONTAP 9.7부터 데이터 복사본이나 추가 디스크 공간 없이 FlexVol 볼륨을 FlexGroup 볼륨으로 데이터 이동 없이 전환할 수 있습니다.

시작하기 전에

- 전환된 볼륨은 ONTAP 9.8부터 FlexGroup 볼륨으로 변환할 수 있습니다.
- 변환 중인 FlexVol 볼륨은 온라인이어야 합니다.
- FlexVol 볼륨의 작업 및 구성은 변환 프로세스와 호환되어야 합니다.

  변환이 성공하지 못하게 할 수 있는 다음 조건을 확인합니다.

  - 7MTT(ONTAP 9.7)를 사용하여 FlexVol 볼륨을 7-Mode에서 전환했습니다.

    전환된 볼륨은 ONTAP 9.8부터 변환될 수 있습니다.

  - 볼륨에서 아직 FlexGroup 볼륨에서 지원하지 않는 기능이 활성화되어 있습니다. 예를 들어 SAN LUN, Windows NFS, SMB1, 스냅샷 명명/자동 삭제, vmalign 설정, ONTAP 9.11.1 이전 릴리스의 SnapLock(SnapLock은 ONTAP 9.11.1부터 지원됨), 공간 SLO 또는 논리적 공간 적용/보고 등이 있습니다. 자세한 내용은 을 "FlexGroup 볼륨에 대해 지원 및 지원되지 않는 구성입니다"참조하십시오.
  - 변환하려는 FlexVol 볼륨이 위치한 SVM이 현재 SVM DR을 사용하고 있습니다.
  - NetApp FlexClone 볼륨이 있고 FlexVol 볼륨이 상위 볼륨입니다. 변환 중인 볼륨은 상위 볼륨이거나 클론일 수 없습니다.
  - 볼륨이 NetApp FlexCache 원본 볼륨입니다.
  - ONTAP 9.7 이하 버전의 경우 NetApp 스냅샷이 255를 초과하지 않아야 합니다. ONTAP 9.8 이상에서는 1023개의 스냅샷이 지원됩니다.
  - 스토리지 효율성이 지원됩니다. 이러한 설정은 비활성화해야 하며 변환 후 다시 활성화할 수 있습니다.
  - 볼륨이 SnapMirror 관계의 소스이고 타겟이 아직 변환되지 않았습니다.
  - 이 볼륨은 활성(정지되지 않음) SnapMirror 관계의 일부입니다.
  - 볼륨에서 자율 랜섬웨어 보호(ARP)가 비활성화되었습니다. 변환이 완료될 때까지 다시 활성화하지 마세요.
  - 할당량이 설정되었습니다. 이러한 설정은 비활성화해야 하며 변환 후 다시 활성화할 수 있습니다.
  - 볼륨 이름은 197자를 초과합니다.
  - 볼륨이 애플리케이션에 연결되어 있습니다.

    이는 ONTAP 9.7에만 적용됩니다. ONTAP 9.8에서는 제한이 제거되었습니다.

  - 미러링, 작업, wapliron, ndmp 백업 ONTAP, 및 inode 변환이 진행 중입니다.
  - 볼륨이 SVM 루트 볼륨입니다.
  - 볼륨이 너무 가득 찼습니다.

    이러한 비호환성이 존재하는 경우 FlexVol 볼륨이 생성되고 볼륨 변환이 중단되면 오류 메시지가 생성됩니다. 수정 조치를 취하고 변환을 다시 시도할 수 있습니다.

- FlexVol 볼륨의 현재 최대 용량이 80% 이상인 경우 데이터 이동 없이 변환을 수행하는 대신 새로 생성된 FlexGroup 볼륨에 데이터를 복사하는 것이 좋습니다. FlexGroup 구성원 볼륨은 시간이 지남에 따라 자연스럽게 재조정되지만 대용량 FlexVol 볼륨을 FlexGroup 볼륨으로 변환하면 성능 또는 균형 문제가 발생하여 구성원 볼륨 간에 신속하게 재조정되지 않을 수 있습니다.

매우 큰 FlexGroup 볼륨을 변환하면 FlexGroup 볼륨 멤버 구성요소가 가득 차서 성능 문제가 발생할 수 있습니다. 자세한 내용은 TR에서 "FlexGroup 볼륨을 생성하지 않을 경우"라는 섹션을 참조하십시오 "FlexGroup 볼륨 - 모범 사례 및 구현 가이드".

단계

1. FlexVol 볼륨이 온라인 상태인지 확인합니다. `volume show -fields vol_name volume-style-extended,state`

```
cluster-1::> volume show my_volume -fields volume-style-extended,state
vserver volume    state  volume-style-extended
------- --------- ------ ---------------------
vs0     my_volume online flexvol
```

2. FlexVol 볼륨을 문제 없이 변환할 수 있는지 확인합니다.

   a. 'Set-Privilege advanced'라는 고급 권한 모드로 로그인합니다

   b. 변환 프로세스 'volume conversion start - vserver vs1-volume FlexVol - check-only true'를 확인합니다

   볼륨을 변환하기 전에 모든 오류를 수정해야 합니다.

   FlexGroup 볼륨을 FlexVol 볼륨으로 다시 변환할 수 없습니다.

3. 'volume conversion start -vserver svm_name -volume vol_name' 변환을 시작합니다

```
cluster-1::*> volume conversion start -vserver vs0 -volume my_volume

Warning: Converting flexible volume "my_volume" in Vserver "vs0" to a
FlexGroup
         will cause the state of all Snapshot copies from the volume to
be set
         to "pre-conversion". Pre-conversion Snapshot copies cannot be
         restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

4. 변환이 성공적인지 확인합니다. `volume show vol_name -fields volume-style-extended,state`

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state
vserver volume    state  volume-style-extended
------- --------- ------ ---------------------
vs0     my_volume online flexgroup
```

결과

FlexVol 볼륨은 단일 멤버 FlexGroup 볼륨으로 변환됩니다.

작업을 마친 후

필요에 따라 FlexGroup 볼륨을 확장할 수 있습니다.

ONTAP FlexVol volume SnapMirror 관계를 ONTAP FlexGroup 볼륨 SnapMirror 관계로 변환합니다

FlexVol 볼륨 SnapMirror 관계를 ONTAP에서 FlexGroup 볼륨 SnapMirror 관계로 변환하려면 먼저 대상 FlexVol 볼륨을 변환한 다음 소스 FlexVol 볼륨을 변환해야 합니다.

이 작업에 대해

- SnapMirror/ SnapVault 관계에서 FlexGroups와 FlexVol 볼륨을 혼합하는 것은 변환 프로세스를 넘어서는 지원되지 않습니다.
- FlexGroup 변환은 SnapMirror 비동기 관계에 대해서만 지원됩니다.
- SnapMirror 클라우드 관계에서는 FlexGroup 변환이 지원되지 않습니다.
- 변환 시간은 여러 변수에 따라 달라집니다. 일부 변수는 다음과 같습니다.
  - 컨트롤러의 CPU입니다
  - 다른 애플리케이션의 CPU 사용률
  - 초기 스냅샷의 데이터 양입니다
  - 네트워크 대역폭
  - 다른 응용 프로그램에서 사용하는 대역폭

시작하기 전에

- 변환 중인 FlexVol 볼륨은 온라인이어야 합니다.
- SnapMirror 관계의 소스 FlexVol 볼륨은 여러 SnapMirror 관계의 소스 볼륨이 아니어야 합니다.

  ONTAP 9.9.1부터 팬아웃 SnapMirror 관계가 FlexGroup 볼륨에 대해 지원됩니다. 자세한 내용은 을 "FlexGroup 볼륨에 대한 SnapMirror 캐스케이드 및 팬아웃 관계를 생성할 때의 고려 사항"참조하십시오.

- FlexVol 볼륨의 작업 및 구성은 변환 프로세스와 호환되어야 합니다.

  FlexVol 볼륨에 비호환성이 있으며 볼륨 변환이 중단된 경우 오류 메시지가 생성됩니다. 수정 조치를 취하고 변환을 다시 시도할 수 있습니다.

단계

1. SnapMirror 관계가 정상 상태인지 확인:

   ```
   snapmirror show
   ```

   XDP 유형의 미러 관계만 변환할 수 있습니다.

   예:

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:src_dpv DP   vs2:dst_dpv  Snapmirrored
                                     Idle           -         true    -
vs0:src_xdp XDP  vs2:dst_xdp  Snapmirrored
                                     Idle           -         true    -
```

2. 소스 볼륨이 변환에 대해 호환되는지 확인합니다.

   a. advance 권한 모드로 로그인합니다.

   ```
   set -privilege advanced
   ```

   b. 변환 프로세스를 확인합니다.

   ```
   volume conversion start -vserver <src_svm_name> -volume <src_vol>
   -check-only true
   ```

   예:

```
volume conversion start -vserver vs1 -volume src_vol -check-only true
```

+
볼륨을 변환하기 전에 모든 오류를 수정해야 합니다.

3. 대상 FlexVol 볼륨을 FlexGroup 볼륨으로 변환합니다.

   a. FlexVol SnapMirror 관계 중지:

   ```
   snapmirror quiesce -destination-path <dest_svm:dest_volume>
   ```

   예:

   ```
   cluster2::> snapmirror quiesce -destination-path vs2:dst_xdp
   ```

b. 변환 시작:

```
volume conversion start -vserver <dest_svm> -volume <dest_volume>
```

예:

```
cluster-1::> volume conversion start -vserver vs2 -volume dst_xdp

Warning: After the volume is converted to a FlexGroup, it will not be
possible
to change it back to a flexible volume.
Do you want to continue? {y|n}: y

[Job 510] Job succeeded: SnapMirror destination volume "dst_xdp" has
been successfully converted to a FlexGroup volume.
You must now convert the relationship's source volume, "vs0:src_xdp", to
a FlexGroup.
Then, re-establish the SnapMirror relationship using the "snapmirror
resync" command.
```

4. 소스 FlexVol 볼륨을 FlexGroup 볼륨으로 변환:'

```
volume conversion start -vserver <src_svm_name> -volume <src_vol_name>
```

예:

```
cluster-1::> volume conversion start -vserver vs0 -volume src_xdp

Warning: Converting flexible volume "src_xdp" in Vserver "vs0" to a
FlexGroup
         will cause the state of all Snapshot copies from the volume to
be set
         to "pre-conversion". Pre-conversion snapshots cannot be
         restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

5. 관계 다시 동기화:

```
snapmirror resync -destination-path dest_svm_name:dest_volume
```

예:

```
cluster2::> snapmirror resync -destination-path vs2:dst_xdp
```

작업을 마친 후

소스 FlexGroup 볼륨을 확장하여 더 많은 구성 요소까지 포함할 때는 대상 볼륨도 확장되어야 합니다.

관련 정보

- "SnapMirror 중지"
- "스냅미러 재동기화"
- "스냅미러 쇼"

FlexCache 볼륨 관리

ONTAP FlexCache 볼륨에 대해 알아보십시오

NetApp FlexCache 기술은 데이터 액세스를 가속하고 WAN 대기 시간을 줄이며, 클라이언트가 동일한 데이터에 반복적으로 액세스해야 하는 읽기 집약적인 워크로드의 WAN 대역폭 비용을 줄여줍니다. FlexCache 볼륨을 생성할 때 원래 볼륨의 활성 데이터(핫 데이터)만 포함된 기존(오리진) 볼륨의 원격 캐시를 생성합니다.

FlexCache 볼륨이 포함된 핫 데이터의 읽기 요청을 받으면 데이터가 클라이언트에 도달하기 위해 멀리 이동할 필요가 없기 때문에 원본 볼륨보다 빠르게 응답할 수 있습니다. FlexCache 볼륨이 자주 읽지 않는 데이터(콜드 데이터)에 대한 읽기 요청을 수신하는 경우, 원래 볼륨에서 필요한 데이터를 검색한 다음 클라이언트 요청을 처리하기 전에 데이터를 저장합니다. 그런 다음 해당 데이터에 대한 후속 읽기 요청이 FlexCache 볼륨에서 직접 처리됩니다. 첫 번째 요청을 받은 이후에는 더 이상 네트워크를 통해 데이터를 이동하거나 과부하 상태인 시스템에서 데이터를 처리할 필요가 없습니다. 예를 들어, 자주 요청하는 데이터에 대한 단일 액세스 포인트에서 클러스터 내에 병목 현상이 발생한다고 가정합니다. 클러스터 내에서 FlexCache 볼륨을 사용하여 핫 데이터에 여러 마운트 지점을 제공할 수 있으므로 병목 현상이 줄어들고 성능이 향상됩니다. 다른 예로, 여러 클러스터에서 액세스하는 볼륨으로 네트워크 트래픽을 줄여야 한다고 가정합니다. FlexCache 볼륨을 사용하여 원본 볼륨의 핫 데이터를 네트워크 내의 클러스터를 통해 배포할 수 있습니다. 따라서 사용자에게 보다 가까운 액세스 지점을 제공하여 WAN 트래픽이 감소합니다.

또한 FlexCache 기술을 사용하여 클라우드 및 하이브리드 클라우드 환경의 성능을 향상할 수 있습니다. FlexCache 볼륨은 온프레미스 데이터 센터의 데이터를 클라우드로 캐싱하여 워크로드를 하이브리드 클라우드로 전환하는 데 도움이 될 수 있습니다. 또한 FlexCache 볼륨을 사용하여 한 클라우드 공급자에서 다른 클라우드 공급자로 또는 동일한 클라우드 공급자의 두 지역 간에 데이터를 캐싱하여 클라우드 사일로를 제거할 수 있습니다.

ONTAP 9.10.1부터 가능합니다 "글로벌 파일 잠금 사용" 모든 FlexCache 볼륨에 걸쳐 있습니다. 전역 파일 잠금은 사용자가 이미 다른 사용자가 연 파일에 액세스하지 못하도록 합니다. 그런 다음, 원래 볼륨의 업데이트가 모든 FlexCache 볼륨에 동시에 배포됩니다.

ONTAP 9.9.1부터 FlexCache 볼륨은 찾을 수 없는 파일 목록을 유지합니다. 이렇게 하면 클라이언트가 존재하지 않는 파일을 검색할 때 오리진으로 여러 통화를 전송할 필요가 없도록 하여 네트워크 트래픽을 줄일 수 있습니다.

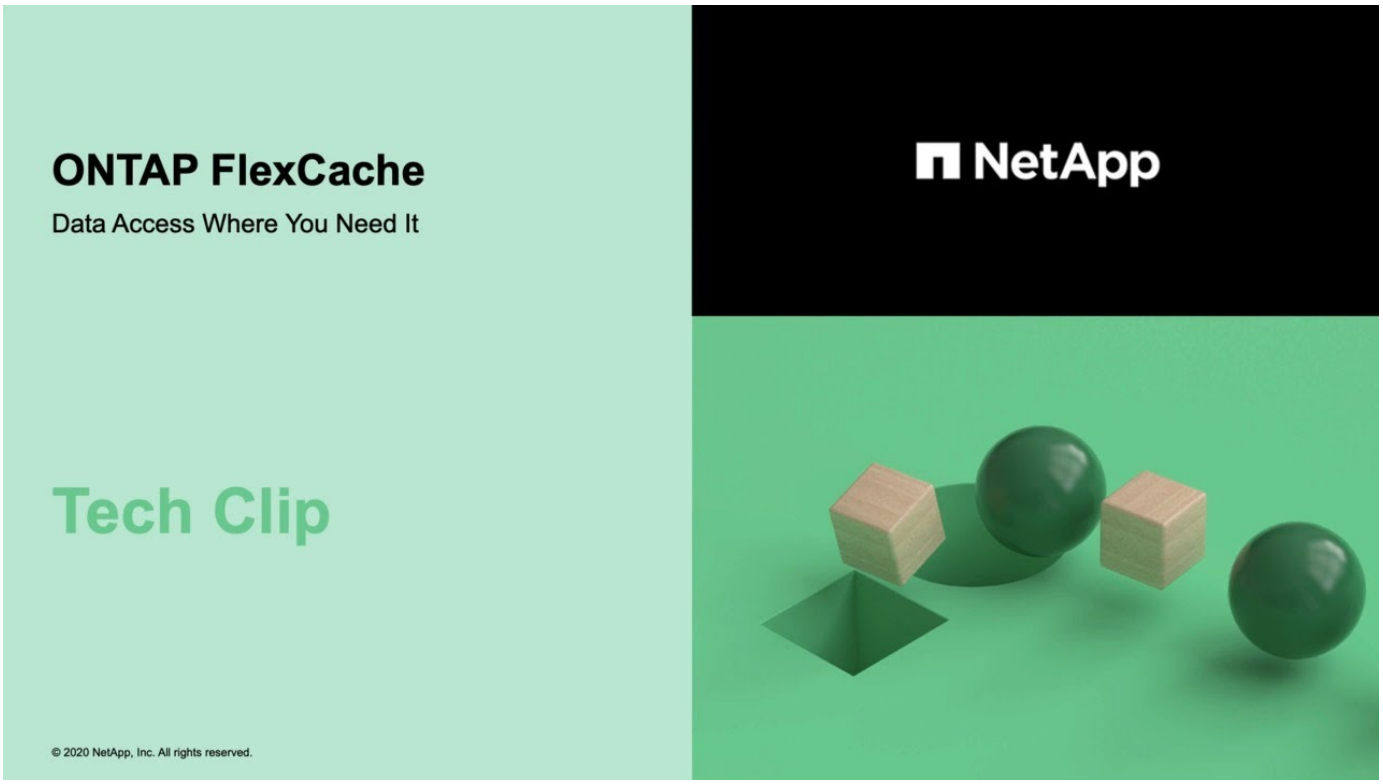
추가 목록 "FlexCache 볼륨 및 원래 볼륨에 대해 지원되는 기능"ONTAP 버전에서 지원되는 프로토콜 목록을 포함하여 를 사용할 수도 있습니다.

ONTAP FlexCache 기술의 아키텍처에 대한 자세한 내용은 에서 확인할 수 있습니다 "TR-4743: ONTAP의 FlexCache".

비디오

FlexCache를 통해 글로벌 데이터의 **WAN** 지연 시간 및 읽기 시간을 줄이는 방법

ONTAP FlexCache의 성능 이점에 대해 알아보십시오**!**



ONTAP FlexCache 볼륨에 대해 지원되거나 지원되지 않는 기능

ONTAP 9.5부터 FlexCache 볼륨을 구성할 수 있습니다. FlexVol 볼륨은 원본 볼륨으로 지원되며 FlexGroup 볼륨은 FlexCache 볼륨으로 지원됩니다. ONTAP 9.7부터 FlexVol 볼륨과 FlexGroup 볼륨이 모두 원본 볼륨으로 지원됩니다. 원래 볼륨과 FlexCache 볼륨에 대해 지원되는 기능 및 프로토콜은 다양합니다.

캐시 볼륨과 원본 볼륨이 모두 지원되는 ONTAP 버전에서 실행되는 한 상호 운용할 수 있습니다. 기능은 지원 기능이 도입된 ONTAP 버전 또는 이후 ONTAP 버전을 실행하는 캐시와 오리진 둘 다 실행 중인 경우에만 지원됩니다.

FlexCache 볼륨과 원래 볼륨 간 **ONTAP** 버전 지원

오리진 볼륨과 캐시 볼륨 간에 지원되는 권장 ONTAP 버전은 이전 버전 4개 또는 이후 버전 4개를 넘지 않습니다. 예를 들어 캐시가 ONTAP 9.14.1을 사용하는 경우 오리진에서 사용할 수 있는 가장 초기 버전은 ONTAP 9.10.1입니다.

지원되는 프로토콜

프로토콜	원본 볼륨에서 지원됩니까?	FlexCache 볼륨에서 지원됩니까?
NFSv3	예	예

NFSv4	예 NFSv4.x 프로토콜을 사용하여 캐시 볼륨을 액세스하려면 오리진 클러스터와 캐시 클러스터 모두 ONTAP 9.10.1 이상을 사용해야 합니다. 오리진 클러스터와 FlexCache 클러스터는 서로 다른 ONTAP 버전을 가질 수 있지만 둘 다 ONTAP 9.10.1 이상 버전이어야 합니다. 예를 들어 오리진에는 ONTAP 9.10.1이 있고 캐시에는 ONTAP 9.11.1이 포함될 수 있습니다.	예 ONTAP 9.10.1부터 지원됩니다. NFSv4.x 프로토콜을 사용하여 캐시 볼륨을 액세스하려면 오리진 클러스터와 캐시 클러스터 모두 ONTAP 9.10.1 이상을 사용해야 합니다. 오리진 클러스터와 FlexCache 클러스터는 서로 다른 ONTAP 버전을 가질 수 있지만 둘 다 ONTAP 9.10.1 이상 버전이어야 합니다. 예를 들어 오리진에는 ONTAP 9.10.1이 있고 캐시에는 ONTAP 9.11.1이 포함될 수 있습니다.
NFSv4.2	예	아니요
중소기업	예	예 ONTAP 9.8부터 지원됩니다.

지원되는 기능

피처	원본 볼륨에서 지원됩니까?	FlexCache 볼륨에서 지원됩니까?
자율적 랜섬웨어 방어	예 ONTAP 9.10.1부터 FlexVol 원본 볼륨에 대해 지원되며 ONTAP 9.13.1부터 FlexGroup 원본 볼륨에 대해 지원됩니다. 을 참조하십시오 "자율 랜섬웨어 보호 사용 사례 및 고려사항".	아니요
안티바이러스	예 ONTAP 9.7부터 지원됩니다.	해당 없음 오리진에서 바이러스 백신 검사를 구성하는 경우 캐시에 필요하지 않습니다. 원본 바이러스 백신 검사는 쓰기 소스에 관계없이 쓰기가 커밋되기 전에 바이러스에 감염된 파일을 감지합니다. FlexCache에서 바이러스 백신 검사를 사용하는 방법에 대한 자세한 내용은 를 참조하십시오 "FlexCache with ONTAP 기술 보고서".

감사	예 ONTAP 9.7부터 지원됩니다. 기본 ONTAP 감사를 사용하여 FlexCache 관계에서 NFS 파일 액세스 이벤트를 감사할 수 있습니다. 자세한 내용은 을 참조하십시오 FlexCache 볼륨을 감사할 때의 고려 사항	예 ONTAP 9.7부터 지원됩니다. 기본 ONTAP 감사를 사용하여 FlexCache 관계에서 NFS 파일 액세스 이벤트를 감사할 수 있습니다. 자세한 내용은 을 참조하십시오 FlexCache 볼륨을 감사할 때의 고려 사항
Cloud Volumes ONTAP	예 ONTAP 9.6부터 지원됩니다	예 ONTAP 9.6부터 지원됩니다
컴팩션	예 ONTAP 9.6부터 지원됩니다	예 ONTAP 9.7부터 지원됩니다
압축	예 ONTAP 9.6부터 지원됩니다	예 ONTAP 9.6부터 지원됩니다
중복 제거	예	예 인라인 중복제거는 ONTAP 9.6부터 FlexCache 볼륨에서 지원됩니다. ONTAP 9.7부터 시작되는 FlexCache 볼륨에서는 다중 볼륨 중복제거가 지원됩니다.
FabricPool	예	예 ONTAP 9.7부터 지원됩니다 FabricPool 계층화가 활성화된 원본 볼륨에 대한 캐시로 FlexCache 볼륨을 생성할 수 있지만 FlexCache 볼륨 자체는 계층화할 수 없습니다.
FlexCache 재해 복구	예	예 ONTAP 9.9.1부터 지원됨, NFSv3 프로토콜 포함, 전용. FlexCache 볼륨은 개별 SVM 또는 개별 클러스터에 있어야 합니다.

FlexGroup 볼륨	예 ONTAP 9.7부터 지원됩니다	예
FlexVol 볼륨	예	아니요
FPolicy를 참조하십시오	예 ONTAP 9.7부터 지원됩니다	예 ONTAP 9.7부터 NFS에 대해 지원됩니다. ONTAP 9.14.1부터 SMB에 대해 지원됩니다.
MetroCluster 구성	예 ONTAP 9.7부터 지원됩니다	예 ONTAP 9.7부터 지원됩니다
Microsoft ODX(Offloaded Data Transfer)	예	아니요
NetApp 애그리게이트 암호화(NAE)	예 ONTAP 9.6부터 지원됩니다	예 ONTAP 9.6부터 지원됩니다
NetApp 볼륨 암호화(NVE)	예 ONTAP 9.6부터 지원됩니다	예 ONTAP 9.6부터 지원됩니다
ONTAP S3 NAS 버킷	예 ONTAP 9.12.1부터 지원됩니다	예 ONTAP 9.18.1부터 지원됩니다.
QoS를 참조하십시오	예	예 FlexCache 볼륨에 대해 파일 레벨 QoS가 지원되지 않습니다.
Qtree	예 ONTAP 9.6부터 qtree를 작성하고 수정할 수 있습니다. 소스에서 생성된 qtree는 캐시에서 액세스할 수 있습니다.	아니요

할당량	예 ONTAP 9.6부터 FlexCache 원본 볼륨에 대한 할당량 적용은 사용자, 그룹, qtree가 지원됩니다.	아니요 FlexCache 쓰기 사운드 모드(기본 모드)를 사용하면 캐시의 쓰기가 원본 볼륨으로 전달됩니다. 할당량은 오리진에서 적용됩니다. ONTAP 9.6부터 FlexCache 볼륨에서 원격 할당량(rquota)이 지원됩니다.
SMB 변경 통지	예	예 ONTAP 9.14.1부터 SMB 변경 알림이 캐시에서 지원됩니다.
SnapLock 볼륨	아니요	아니요
SnapMirror 비동기식 관계 *	예	아니요
	• FlexCache 원점: • 원본 FlexVol의 FlexCache 볼륨을 가질 수 있습니다 • 원본 FlexGroup의 FlexCache 볼륨을 가질 수 있습니다 • SnapMirror 관계의 원본 기본 볼륨에서 FlexCache 볼륨을 가질 수 있습니다. • ONTAP 9.8부터 SnapMirror 보조 볼륨은 FlexCache 원본 볼륨이 될 수 있습니다. SnapMirror 2차 볼륨은 활성 SnapMirror 업데이트 없이 유휴 상태여야 하며, 그렇지 않으면 FlexCache 생성이 실패합니다.	SnapMirror 동기식 관계
아니요	아니요	SnapRestore
예	아니요	스냅샷 수
예	아니요	SVM DR 구성

예 ONTAP 9.5 버전부터 지원됩니다. SVM DR 관계의 기본 SVM은 원본 볼륨을 사용할 수 있습니다. 그러나 ONTAP ONTAP 이전 버전을 실행 중인 경우 SVM DR 관계가 끊어지면 새 원본 볼륨을 사용하여 FlexCache 관계를 다시 생성해야 합니다. ONTAP 9.18.1 버전부터 원본 SVM이 장애 조치를 수행하면 캐시가 자동으로 재해 복구 사이트의 원본으로 전환됩니다. 수동 복구 단계가 필요 없어집니다. FlexCache 볼륨 생성 방법에 대해 알아보세요.	아니요 FlexCache 볼륨은 1차 SVM에 존재할 수 있지만, 2차 SVM에는 존재할 수 없습니다. 1차 SVM의 모든 FlexCache 볼륨은 SVM DR 관계의 일부로 복제되지 않습니다.	스토리지 레벨 액세스 가드(슬래그)
아니요	아니요	씬 프로비저닝
예	예 ONTAP 9.7부터 지원됩니다	볼륨 클론 복제
예 원본 볼륨 및 원본 볼륨의 파일 복제는 ONTAP 9.6부터 지원됩니다.	아니요	볼륨 이동
예	예(볼륨 구성요소에만 해당) FlexCache 볼륨의 볼륨 구성 요소 이동은 ONTAP 9.6 이상에서 지원됩니다.	볼륨 재호스팅
아니요	아니요	어레이 통합을 위한 vStorage API(VAAI)

FlexVol 9 릴리즈 9.5 이전 버전에서는 원본 FlexCache 볼륨이 7-Mode에서 작동하는 Data ONTAP 8.2.x를 실행하는 시스템에서 생성된 ONTAP 볼륨에만 데이터를 제공할 수 있습니다. FlexVol 9.5부터 오리진 ONTAP 볼륨은 ONTAP 9 시스템의 FlexCache 볼륨에 데이터를 제공할 수도 있습니다. 7-Mode FlexCache에서 ONTAP 9 FlexCache로 마이그레이션하는 방법에 대한 자세한 내용은 를 참조하십시오."NetApp 기술 보고서 4743: FlexCache in ONTAP"

ONTAP FlexCache 볼륨 사이징 지침을 참조하십시오

볼륨 프로비저닝을 시작하기 전에 FlexCache 볼륨의 제한을 알고 있어야 합니다.

FlexVol 볼륨의 크기 제한은 원본 볼륨에 적용됩니다. FlexCache 볼륨의 크기는 원본 볼륨보다 작거나 같을 수 있습니다. FlexCache 볼륨 크기에 대한 모범 사례는 원본 볼륨 크기의 10% 이상이어야 합니다.

또한 FlexCache 볼륨에 대한 다음과 같은 추가 제한도 알고 있어야 합니다.

제한	ONTAP 9.8 이상	ONTAP 9.7	ONTAP 9.6 - 9.5
원본 볼륨에서 생성할 수 있는 최대 FlexCache 볼륨 수입니다	100	10	10
노드당 권장되는 최대 오리진 볼륨 수입니다	100	100	10
노드당 권장되는 최대 FlexCache 볼륨 수입니다	100	100	10
노드당 FlexCache 볼륨에 권장되는 최대 FlexGroup 구성 수	800	800	40
노드당 FlexCache 볼륨당 최대 구성요소 수	32	32	32

관련 정보

- "NetApp 상호 운용성"

ONTAP FlexCache 볼륨을 생성합니다

자주 사용되는 객체에 액세스할 때 성능을 향상시키기 위해 동일한 ONTAP 클러스터 내에 FlexCache 볼륨을 생성할 수 있습니다. 데이터 센터가 여러 위치에 있는 경우 원격 ONTAP 클러스터에 FlexCache 볼륨을 생성하여 데이터 액세스 속도를 높일 수 있습니다.

이 작업에 대해

- ONTAP 9.18.1부터 볼륨 생성 시 `-is-s3-enabled` 옵션을 `true`로 설정하여 FlexCache 볼륨에서 NAS S3 버킷 액세스를 활성화할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있습니다.
- ONTAP 9.18.1부터 FlexCache SVM-DR 관계에 속하는 SVM이 있는 원본 볼륨에 대한 캐시 볼륨을 생성하는 것을 지원합니다.

  ONTAP 9.18.1 이상을 실행하는 경우 스토리지 관리자는 SVM-DR 관계에 속한 원본 볼륨의 캐시 볼륨을 생성하기 전에 SVM-DR 관계에 속한 기본 및 보조 원본 SVM 모두와 캐시 SVM을 피어링해야 합니다.
- ONTAP 9.14.0부터 암호화된 소스에서 암호화되지 않은 FlexCache 볼륨을 만들 수 있습니다.
- ONTAP 9.7부터 FlexVol 볼륨과 FlexGroup 볼륨 모두 원본 볼륨으로 지원됩니다.
- ONTAP 9.5부터 FlexCache는 FlexVol 볼륨을 원본 볼륨으로, FlexGroup 볼륨을 FlexCache 볼륨으로 지원합니다.

시작하기 전에

- ONTAP 9.5 이상을 실행 중이어야 합니다.
- ONTAP 9 .6 이하를 실행 중인 경우 를 실행해야 "FlexCache 라이센스를 추가합니다"합니다.

  ONTAP 9.7 이상에는 FlexCache 라이센스가 필요하지 않습니다. ONTAP 9.7부터는 FlexCache 기능이 ONTAP에 포함되어 더 이상 라이센스나 활성화가 필요하지 않습니다.

HA 쌍이 를 사용 중인 경우 "SAS 또는 NVMe 드라이브(SED, NSE, FIPS) 암호화", 항목의 지침을 따라야 합니다 "FIPS 드라이브 또는 SED를 보호되지 않는 모드로 되돌리는 중입니다" 시스템을 초기화하기 전에 HA 쌍 내의 모든 드라이브(부팅 옵션 4 또는 9) 이렇게 하지 않을 경우 드라이브를 용도 변경할 경우 향후의 데이터 손실이 발생할 수 있습니다.

예 **12.** 단계

시스템 관리자

1. FlexCache 볼륨이 원본 볼륨과 다른 ONTAP 클러스터에 있는 경우 클러스터 피어 관계를 생성합니다.
   a. 로컬 클러스터에서 * 보호 > 개요 * 를 클릭합니다.
   b. Intercluster Settings * 를 확장하고 * Add Network Interfaces * 를 클릭한 후 클러스터에 대한 클러스터 간 네트워크 인터페이스를 추가합니다.

      원격 클러스터에서 이 단계를 반복합니다.

   c. 원격 클러스터에서 * 보호 > 개요 * 를 클릭합니다. Cluster Peers 섹션을 클릭하고 * Generate Passphrase * 를 클릭합니다.
   d. 생성된 암호를 복사하여 로컬 클러스터에 붙여넣습니다.
   e. 로컬 클러스터의 클러스터 피어에서 * 피어 클러스터 * 를 클릭하고 로컬 및 원격 클러스터를 피어로 지정합니다.
2. SVM 피어 관계 생성:

   스토리지 VM 피어 아래에서 및 * 피어 스토리지 VM * 을 클릭하여 스토리지 VM을 피어링합니다.

3. 스토리지 > 볼륨 * 을 선택합니다.
4. 추가 * 를 선택합니다.
5. More Options * 를 선택한 다음 * Add as cache for a remote volume * 를 선택합니다.

   ONTAP 9.8 이상을 실행 중인 경우 QoS를 비활성화하거나 사용자 지정 QoS 정책을 선택하려면 * 추가 옵션 * 을 클릭한 다음 * 스토리지 및 최적화 * 에서 * 성능 서비스 수준 * 을 선택합니다.

CLI를 참조하십시오

1. 생성할 FlexCache 볼륨이 다른 클러스터에 있는 경우 클러스터 피어 관계를 생성합니다.
   a. 대상 클러스터에서 데이터 보호 소스 클러스터와 피어 관계를 생성합니다.

```
cluster peer create -generate-passphrase -offer-expiration
MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addrs
<peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,..|*
-ipspace <ipspace_name>
```

   ONTAP 9.6부터는 클러스터 피어 관계를 만들 때 TLS 암호화가 기본적으로 활성화됩니다. TLS 암호화는 오리진과 FlexCache 볼륨 간의 인터클러스터 통신에 지원됩니다. 필요한 경우 클러스터 피어 관계에 대해 TLS 암호화를 비활성화할 수도 있습니다.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
              Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: *
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

a. 소스 클러스터에서 소스 클러스터를 대상 클러스터에 인증합니다.

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship,
use a phrase or sequence of characters that would be hard to
guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

2. FlexCache 볼륨이 원본 볼륨과 다른 SVM에 있는 경우 애플리케이션으로서 "FlexCache"와 SVM 피어 관계를 생성합니다.

a. SVM이 다른 클러스터에 있는 경우 피어링 SVM에 대한 SVM 권한을 생성합니다.

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

다음 예에서는 모든 로컬 SVM에 적용되는 SVM 피어 권한을 생성하는 방법을 보여줍니다.

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache

Warning: This Vserver peer permission applies to all local Vservers.
After that no explict
"vserver peer accept" command required for Vserver peer relationship
creation request
from peer cluster "cluster2" with any of the local Vservers. Do you
want to continue? {y|n}: y
```

a. SVM 피어 관계 생성:

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. FlexCache 볼륨 생성:

```
volume flexcache create -vserver <cache_svm> -volume
<cache_vol_name> -auto-provision-as flexgroup -size <vol_size>
-origin-vserver <origin_svm> -origin-volume <origin_vol_name> -is-s3
-enabled true|false
```

다음 예에서는 FlexCache 볼륨을 생성하고 프로비저닝할 기존 애그리게이트를 자동으로 선택합니다.

```
cluster1::> volume flexcache create -vserver vs_1 -volume fc1 -auto
-provision-as flexgroup -origin-volume vol_1 -size 160MB -origin
-vserver vs_1
[Job 443] Job succeeded: Successful
```

다음 예에서는 FlexCache 볼륨을 생성하고 접합 경로를 설정합니다.

```
cluster1::> volume flexcache create -vserver vs34 -volume fc4 -aggr
-list aggr34,aggr43 -origin-volume origin1 -size 400m -junction-path
/fc4
[Job 903] Job succeeded: Successful
```

다음 예제는 FlexCache 볼륨에서 S3 액세스를 활성화합니다.

```
cluster1::> volume flexcache create -vserver vs3 -volume
cache_vs3_vol33 -origin-volume vol33 -origin-vserver vs3 -junction
-path /cache_vs3_vol33 -is-s3-enabled true
```

4. FlexCache 볼륨과 원본 볼륨에서 FlexCache 관계를 확인합니다.

   a. 클러스터에서 FlexCache 관계 보기:

   ```
   volume flexcache show
   ```

   ```
   cluster1::> volume flexcache show
   Vserver Volume      Size       Origin-Vserver Origin-Volume
   Origin-Cluster
   ------- ----------- ---------- -------------- -------------
   --------------
   vs_1    fc1         160MB      vs_1           vol_1
   cluster1
   ```

   b. 오리진 클러스터의 모든 FlexCache 관계 보기: + 'volume FlexCache origin show-caches'

   ```
   cluster::> volume flexcache origin show-caches
   Origin-Vserver Origin-Volume   Cache-Vserver    Cache-Volume
   Cache-Cluster
   -------------- --------------- ---------------  --------------
   ---------------
   vs0            ovol1           vs1              cfg1
   clusA
   vs0            ovol1           vs2              cfg2
   clusB
   vs_1           vol_1           vs_1             fc1
   cluster1
   ```

결과

FlexCache 볼륨이 성공적으로 생성되었습니다. 클라이언트는 FlexCache 볼륨의 연결 경로를 사용하여 볼륨을 마운트할 수 있습니다.

관련 정보

"클러스터 및 SVM 피어링"

FlexCache 다시 쓰기

ONTAP FlexCache Write-Back에 대해 자세히 알아보십시오

ONTAP 9.15.1에 도입된 FlexCache Write-Back은 캐시에서 쓰는 대체 작업 모드입니다. Write-back을 사용하면 데이터가 오리진으로 전달될 때까지 기다리지 않고 캐시의 안정적인 스토리지에 쓰기를 커밋하고 클라이언트에서 이를 확인할 수 있습니다. 데이터는 비동기적으로 오리진으로 다시 플러시됩니다. 그 결과, 특정 워크로드 및 환경에서 거의 로컬에 가까운 속도로 쓰기를 수행할 수 있는 전 세계적으로 분산된 파일 시스템이 탄생하여 탁월한 성능 이점을 제공합니다.

ONTAP 9.12.1에서는 공개 미리 보기로 쓰기 저장 기능을 도입했습니다. 이 기능을 다시 쓰기 버전 1(wbv1)이라고 하며, ONTAP 9.15.1에서 다시 쓰기 버전 2(wbv2)라고 하는 Write-back과 동일하다고 간주해서는 안 됩니다.

Write-back 대 write-around

FlexCache는 ONTAP 9.5에 도입된 이후 읽기 쓰기 가능한 캐시였지만 write-around 모드로 작동했습니다. 캐시의 쓰기가 안정적인 스토리지로 커밋되도록 오리진으로 전송되었습니다. 오리진에서 쓰기 작업을 안정적인 스토리지에 커밋한 후 캐시에 대한 쓰기를 확인했습니다. 그러면 캐시는 클라이언트에 대한 쓰기를 승인합니다. 이로 인해 모든 쓰기는 캐시와 오리진 사이에서 네트워크를 통과해야 하는 페널티가 발생합니다. FlexCache WRITE-Back(후기입)

ONTAP 9.15.1로 업그레이드한 후 기존의 write-around 캐시를 write-back 캐시로 변환하고 필요한 경우 다시 write-around로 변환할 수 있습니다. 그러나 이로 인해 문제가 발생할 경우 진단 로그를 읽기가 더 어려워질 수 있습니다.

	쓰기	다시 쓰기
ONTAP 버전	9.6 이상	9.15.1 이상
사용 사례	읽기 집약적 워크로드	쓰기 집약적 워크로드
데이터가 에 커밋되었습니다	원점	캐시
고객 경험	WAN과 유사합니다	LAN과 유사합니다
제한	오리진당 100개	오리진당 10개
"CAP 정리"	파티션에 사용할 수 있으며 허용 가능합니다	사용 가능하고 일관적입니다

FlexCache Write-Back 용어

FlexCache Write-Back과 관련된 주요 개념 및 용어 이해

기간	정의
* 더티 데이터 *	캐시의 안정적인 스토리지에 커밋되었지만 오리진으로 플러시되지 않은 데이터
* 독점 잠금 위임(XLD) *	캐시에 파일 단위로 부여된 프로토콜 수준 잠금 권한입니다. 이 권한을 통해 캐시는 오리진에 접속하지 않고 클라이언트에 전용 쓰기 잠금을 제공할 수 있습니다.

기간	정의
* 공유 잠금 위임(SLD) *	캐시에 파일 단위로 부여된 프로토콜 수준 잠금 권한입니다. 이 권한을 통해 캐시는 오리진에 접속하지 않고 공유 읽기 잠금을 클라이언트에 배포할 수 있습니다.
* 다시 쓰기 *	캐시에 대한 쓰기가 해당 캐시의 안정적인 스토리지에 커밋되어 클라이언트에 즉시 인식되는 FlexCache 작업 모드입니다. 데이터는 원본에 비동기적으로 다시 기록됩니다.
* 기입 *	캐시에 대한 쓰기가 오리진으로 전달되어 안정적인 스토리지에 커밋되는 FlexCache 작업 모드입니다. 커밋되면 오리진에서 캐시에 대한 쓰기를 승인하고 캐시가 클라이언트에 대한 쓰기를 확인합니다.
* DDR(Dirty Data Record System) *	파일별로 다시 쓰기 가능 캐시에서 더티 데이터를 추적하는 독점 메커니즘입니다.
* 원점 *	모든 FlexCache 캐시 볼륨의 소스 데이터를 포함하는 FlexGroup 또는 FlexVol 단일 데이터 소스로서 잠금을 오케스트레이션하고 100% 데이터 일관성, 통화 및 일관성을 보장합니다.
* 캐시 *	FlexCache 오리진의 스파스 캐시 볼륨인 FlexGroup입니다.

정합성 보장, 전류 및 일관성

FlexCache는 언제 어디서나 원하는 데이터를 사용할 수 있는 NetApp의 솔루션입니다. FlexCache는 100% 일관된, 전류 및 일관적인 시간입니다.

- * 정합성: * 데이터는 액세스 위치에 관계없이 동일합니다.
- * 현재: * 데이터는 항상 최신 상태입니다.
- * Coherent : * 데이터가 올바르거나 손상되지 않았습니다.

ONTAP FlexCache write-back 지침

FlexCache 쓰기 저장에는 원본과 캐시 간의 많은 복잡한 상호작용이 포함됩니다. 최적의 성능을 얻으려면 환경이 다음 지침을 따라야 합니다. 이 가이드라인은 콘텐츠 생성 당시 사용 가능한 최신 주요 ONTAP 버전(ONTAP 9.17.1)을 기반으로 합니다.

비운영 환경에서 운영 워크로드를 테스트하는 것이 가장 좋습니다. 이 지침을 벗어나는 FlexCache Write-Back을 구현할 경우 더욱 중요합니다.

다음 지침은 NetApp에서 내부적으로 잘 테스트되었습니다. 이 호텔 안에 머무시는 것이 좋습니다. 그렇지 않으면 예기치 않은 동작이 발생할 수 있습니다.

- ONTAP 9.17.1P1에서는 FlexCache 쓰기 저장 기능에 대한 중요한 개선 사항이 도입되었습니다. 9.17.1P1 이후에는 원본 클러스터와 캐시 클러스터 모두에서 현재 권장되는 릴리스를 실행하는 것이 강력히 권장됩니다. 9.17.1 코드라인을 실행할 수 없는 경우, 다음으로 제안되는 릴리스는 최신 P 릴리스인 9.16.1입니다. ONTAP 9.15.1에는 FlexCache 쓰기 저장에 필요한 모든 수정 사항과 개선 사항이 포함되어 있지 않으므로 프로덕션 워크로드에는 권장되지 않습니다.
- 현재 반복에서 FlexCache write-back 캐시는 전체 FlexCache 볼륨에 대해 단일 구성요소로 구성해야 합니다. 다중 구성 FlexCache는 캐시에서 원치 않는 데이터 제거를 초래할 수 있습니다.
- 100GB 미만의 파일에 대해 테스트를 실행했으며, 캐시와 원본 간의 WAN 왕복 시간이 200ms를 초과하지 않도록 했습니다. 이러한 한도를 벗어나는 작업 부하로 인해 예상치 못한 성능 특성이 나타날 수 있습니다.
- SMB 대체 데이터 스트림에 쓰면 주 파일이 캐시에서 제거됩니다. 기본 파일의 모든 더티 데이터를 오리진으로

플러시해야 해당 파일에 대해 다른 작업을 수행할 수 있습니다. 대체 데이터 스트림도 오리진으로 전달됩니다.

- 파일 이름을 바꾸면 파일이 캐시에서 제거됩니다. 파일의 모든 더티 데이터를 오리진으로 플러시해야 해당 파일에 대해 다른 작업을 수행할 수 있습니다.
- 이때 write-back 지원 FlexCache 볼륨의 파일에 대해 변경하거나 설정할 수 있는 유일한 속성은 다음과 같습니다.
  - 타임스탬프
  - 모드 비트
  - NT ACL을 선택합니다
  - 소유자
  - 그룹
  - 크기

    변경되거나 설정된 다른 특성은 오리진으로 전달되어 캐시에서 파일을 제거할 수 있습니다. 캐시에서 다른 속성을 변경하거나 설정해야 할 경우, 어카운트 팀에 PVR을 개설하도록 요청하십시오.
- 오리진에서 생성된 스냅샷으로 인해 해당 오리진 볼륨과 연결된 모든 write-back 지원 캐시에서 미처리 더티 데이터를 모두 불러옵니다. 이렇게 하려면 많은 양의 쓰기 저장 작업이 진행 중인 경우 이러한 더티 파일을 제거하는 데 시간이 걸릴 수 있으므로 여러 번 작업을 다시 시도해야 할 수 있습니다.
- 쓰기를 위한 SMB 기회 잠금(Oplock)은 쓰기 백이 활성화된 FlexCache 볼륨에서 지원되지 않습니다.
- 원점은 80% 미만으로 남아 있어야 합니다. 오리진 볼륨에 20% 이상의 공간이 남아 있지 않으면 캐시 볼륨에 전용 잠금 위임이 부여되지 않습니다. 이 경우 다시 쓰기 가능 캐시에 대한 호출은 오리진으로 전달됩니다. 이렇게 하면 오리진에서 공간이 부족해지는 것을 방지할 수 있으며, 이로 인해 다시 쓰기 가능 캐시에 더티 데이터가 분리된 상태로 남게 됩니다.
- 낮은 대역폭 및/또는 손실이 많은 클러스터 간 네트워크는 FlexCache 쓰기 성능에 상당한 부정적인 영향을 미칠 수 있습니다. 작업 부하에 따라 크게 달라지므로 특정 대역폭 요구 사항은 없지만 캐시와 원본 간의 클러스터 간 링크 상태를 확인하는 것이 강력히 권장됩니다.

ONTAP FlexCache 후기입 아키텍처

FlexCache는 쓰기 작업 모드인 Write-back 및 Write-around를 포함하여 강력한 일관성을 염두에 두고 설계되었습니다. 기존의 Write-Around 작동 모드와 ONTAP 9.15.1에 도입된 새로운 Write-back 작동 모드 모두 액세스된 데이터가 항상 100% 일관적이고, 최신 상태이며, 정합성이 보장됩니다.

다음 개념은 FlexCache Write-Back 작동 방식을 자세히 설명합니다.

위임

잠금 위임 및 데이터 위임을 통해 FlexCache는 Write-back 및 Write-around 캐시를 모두 유지할 수 있으며, 데이터의 정합성이 보장되고 최신 상태를 유지할 수 있습니다. 오리진은 두 대표단을 조율합니다.

잠금 위임

잠금 위임은 프로토콜 수준 잠금 권한입니다. 오리진에서 필요에 따라 클라이언트에 프로토콜 잠금을 발급하기 위해 파일별로 캐시에 권한을 부여합니다. 여기에는 배타적 잠금 위임(XLD) 및 SLD(공유 잠금 위임)가 포함됩니다.

XLD 및 **write-back**

ONTAP가 충돌하는 쓰기를 조정할 필요가 없도록 하기 위해 클라이언트가 파일에 쓰기를 요청하는 캐시에 XLD가 부여됩니다. 중요한 것은 모든 파일에 대해 XLD가 한 번에 하나만 존재할 수 있다는 것입니다. 즉, 한 파일에 대해 한 번에 여러 writer가 있을 수 없습니다.

파일 쓰기 요청이 다시 쓰기 가능 캐시에 들어오면 다음 단계가 수행됩니다.

1. 캐시는 요청된 파일에 대한 XLD가 이미 있는지 확인합니다. 이 경우 다른 클라이언트가 캐시의 파일에 쓰지 않는 한 클라이언트에 쓰기 잠금을 부여합니다. 요청된 파일에 대한 XLD가 캐시에 없는 경우 오리진에서 해당 파일을 요청합니다. 이것은 클러스터 간 네트워크를 통과하는 독점 호출입니다.
2. 캐쉬로부터 XLD 요청을 수신하면 오리진에서 다른 캐쉬에 해당 파일에 대해 미처리 XLD가 있는지 확인합니다. 이 경우 해당 파일의 XLD를 호출하면 해당 캐시에서 오리진으로 플러시를 트리거합니다. 더티 데이터
3. 해당 캐시의 더티 데이터가 다시 플러시되고 오리진의 안정적인 스토리지로 커밋되면 오리진에서 해당 파일에 대한 XLD를 요청 캐시에 부여합니다.
4. 파일의 XLD가 수신되면 캐시는 클라이언트에 잠금을 부여하고 쓰기가 시작됩니다.

이러한 단계 중 일부를 다루는 상위 수준 시퀀스 다이어그램은 시퀀스 [write-back-sequence-diagram] 다이어그램에서 다룹니다.

클라이언트 관점에서 볼 때 모든 잠금은 쓰기 잠금이 요청될 때 약간의 지연이 발생할 수 있는 표준 FlexVol 또는 FlexGroup에 쓰는 것처럼 작동합니다.

현재 반복에서 쓰기 저장 가능 캐시에 파일의 XLD가 있는 경우 ONTAP는 작업을 포함하여 다른 캐시에 있는 해당 파일에 대한 * 모든 * 액세스를 차단합니다. `READ`

원점 구성요소당 170개의 XLD 제한이 있습니다.

데이터 위임

데이터 위임은 해당 파일에 대해 캐시된 데이터가 최신 상태임을 오리진에서 캐시에 제공하는 파일별 보증입니다. 캐시에 파일에 대한 데이터 위임이 있는 한, 오리진에 연결할 필요 없이 해당 파일에 대한 캐시된 데이터를 클라이언트에 제공할 수 있습니다. 캐시에 파일에 대한 데이터 위임이 없는 경우 클라이언트에서 요청한 데이터를 받으려면 원본에 연결해야 합니다.

다시 쓰기 모드에서는 다른 캐시나 오리진에서 해당 파일에 대해 XLD를 사용하는 경우 파일의 데이터 위임이 취소됩니다. 이렇게 하면 다른 모든 캐시 및 오리진에 있는 클라이언트에서 파일을 효과적으로 차단하고 읽기 작업을 수행할 수도 있습니다. 이는 오래된 데이터에 절대 액세스하지 못하도록 하기 위해 반드시 해결해야 하는 절충입니다.

Write-back이 설정된 캐시에서 읽기는 일반적으로 Write-around 캐시의 읽기처럼 작동합니다. Write-Around 및 Write-back이 설정된 캐시 모두에서 요청된 파일이 읽기가 실행되는 위치와 다른 Write-back이 설정된 캐시에 단독 쓰기 잠금이 있는 경우 초기 성능 저하가 발생할 수 `READ` 있습니다. XLD를 해지해야 하며, 다른 캐시의 읽기를 서비스하기 전에 더티 데이터를 오리진으로 커밋해야 합니다.

더티 데이터 추적

캐시에서 오리진으로 다시 쓰기는 비동기적으로 수행됩니다. 즉, 더티 데이터는 오리진에 즉시 다시 기록되지 않습니다. ONTAP는 파일당 더티 데이터를 추적하기 위해 더티 데이터 레코드 시스템을 사용합니다. 각 DDR(더티 데이터 레코드)은 특정 파일에 대해 약 20MB의 더티 데이터를 나타냅니다. 파일이 활발하게 작성되면 ONTAP는 두 개의 DDR이 채워지고 세 번째 DDR이 쓰여진 후에 더티 데이터를 다시 플러시하기 시작합니다. 따라서 쓰기 중에 캐시에 약 40MB의 더티 데이터가 남아 있습니다. 상태 저장 프로토콜(NFSv4.x, SMB)의 경우 파일을 닫을 때 나머지 40MB의 데이터가 오리진으로 다시 플러시됩니다. 상태 비저장 프로토콜(NFSv3)의 경우, 다른 캐시에서 파일에 대한 액세스를 요청하거나 파일이 2분 이상 유휴 상태가 되면 최대 5분 동안 40MB의 데이터가 다시 플러시됩니다. 타이머가 트리거되거나 공간이

트리거되는 더티 데이터 플러싱에 대한 자세한 내용은 을 참조하십시오. 캐시 스크러버

DDR 및 스크러버 외에도 일부 프런트엔드 NAS 작업은 파일에 대한 모든 더티 데이터를 플러시합니다.

- `SETATTR`
  - mtime, atime 및/또는 ctime만 수정하는 SETATTR은 캐시에서 처리할 수 있으므로 WAN의 페널티를 피할 수 있습니다.
- `CLOSE`
- `OPEN` 확인할 수 있습니다
- `READ` 확인할 수 있습니다
- `READDIR` 확인할 수 있습니다
- `READDIRPLUS` 확인할 수 있습니다
- `WRITE` 확인할 수 있습니다

연결 해제 모드

파일의 XLD가 write-around 캐시에 보관되고 해당 캐시가 오리진에서 연결이 끊기면 해당 파일에 대한 읽기는 다른 캐시와 오리진에서 계속 허용됩니다. 이 동작은 다시 쓰기 가능 캐시에 의해 XLD가 유지되는 경우에 다릅니다. 이 경우 캐시의 연결이 끊긴 경우 파일 읽기가 모든 곳에서 중단됩니다. 이를 통해 100% 일관성, 통화 및 일관성을 유지할 수 있습니다. 오리진에서 클라이언트에 쓰기 승인되어 있는 모든 데이터를 사용할 수 있으므로 읽기는 write-around 모드로 허용됩니다. 연결 해제 중 Write-back 모드에서는 오리진에서 다시 쓰기 가능 캐시에 기록되고 인식되는 모든 데이터가 연결 해제되기 전에 오리진으로 만들어지는 것을 보장할 수 없습니다.

파일에 대한 XLD가 있는 캐시의 연결이 장시간 끊어진 경우 시스템 관리자는 원본에서 XLD를 수동으로 취소할 수 있습니다. 이렇게 하면 정상적인 캐시 및 오리진에서 파일에 대한 입출력이 재개됩니다.

> XLD를 수동으로 해지하면 연결이 끊어진 캐시에서 파일에 대한 더티 데이터가 손실됩니다. XLD를 수동으로 취소하는 작업은 캐시와 원본 간에 심각한 장애가 발생한 경우에만 수행해야 합니다.

캐시 스크러버

ONTAP에는 타이머 만료 또는 공간 임계값이 위반되는 것과 같은 특정 이벤트에 대한 응답으로 실행되는 스크러버가 있습니다. 스크러버는 스크러브되는 파일에 대해 배타적인 잠금을 가지고 스크럽이 완료될 때까지 해당 파일에 대한 입출력을 효과적으로 동결합니다.

스크러버에는 다음이 포함됩니다.

- *mtime-based scrubber on the cache: * 이 스크러버는 5분마다 시작되며 2분 동안 수정되지 않은 모든 파일을 스크러브합니다. 파일에 대한 더티 데이터가 여전히 캐시에 있는 경우 해당 파일에 대한 입출력이 정지되고 다시 쓰기가 트리거됩니다. 다시 쓰기가 완료된 후 IO가 재개됩니다.
- * mtime-based scrubber on origin: * 캐시의 mtime 기반 scrubber와 마찬가지로 5분마다 실행됩니다. 하지만 수정되지 않은 파일을 15분 동안 스크럽하여 inode의 위임을 불러옵니다. 이 스크러버는 다시 쓰기를 시작하지 않습니다.
- * RW limit-based scrubber on origin: * ONTAP는 오리진 구성요소당 얼마나 많은 RW 잠금 위임이 처리되는지 모니터링합니다. 이 숫자가 170을 초과하면 ONTAP는 LRU(Least-Recently-Used)를 기준으로 쓰기 잠금 위임을 스크럽하기 시작합니다.
- * 캐시 상의 공간 기반 스크러버: * FlexCache 볼륨이 90%에 도달하면 캐시가 스크러빙되어 LRU 기준으로

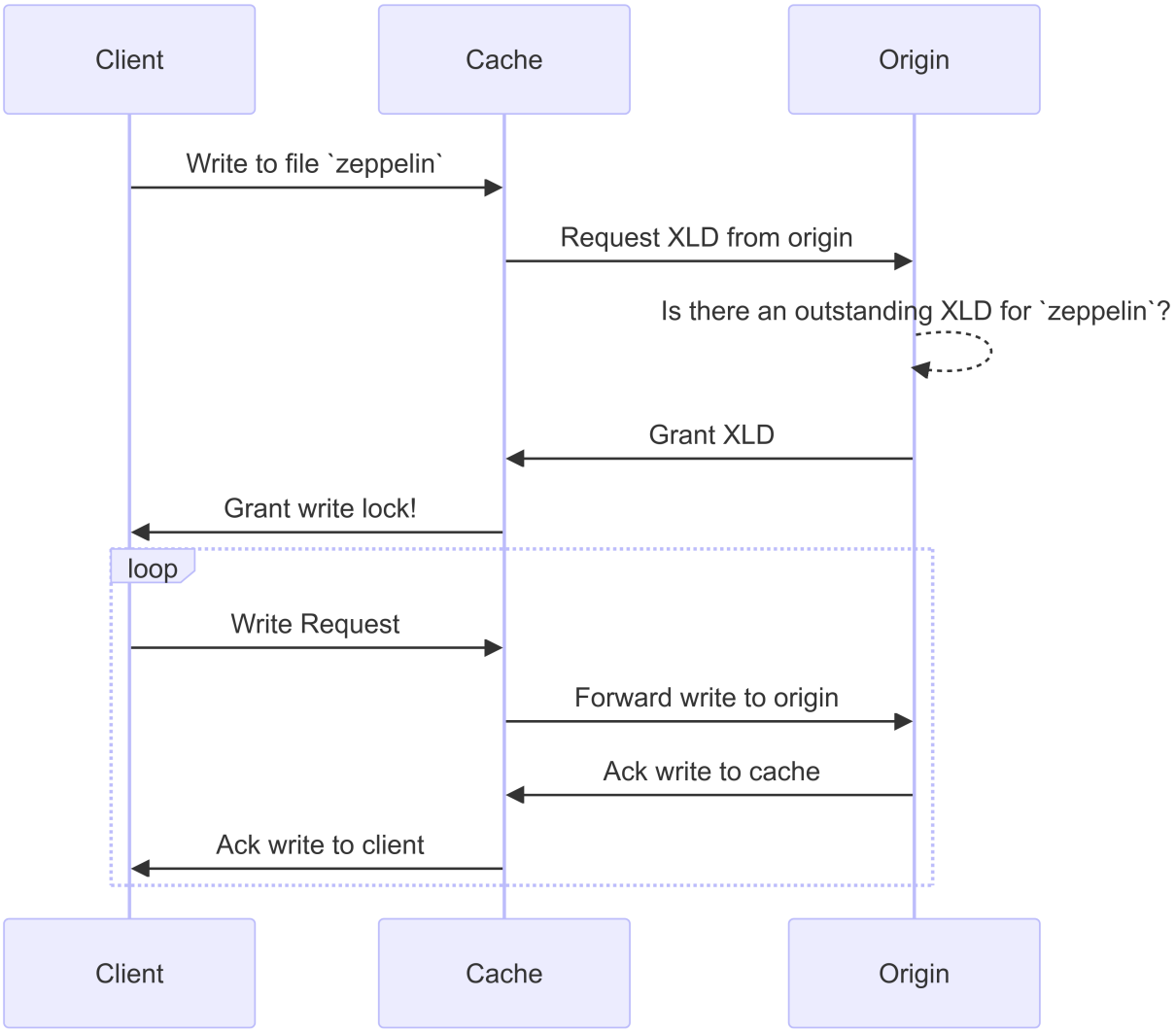
제거됩니다.

- * 오리진에서 공간 기반 스크러버: * FlexCache 오리진 볼륨이 90%에 도달하면 캐시가 스크러빙되어 LRU 기준으로 제거됩니다.

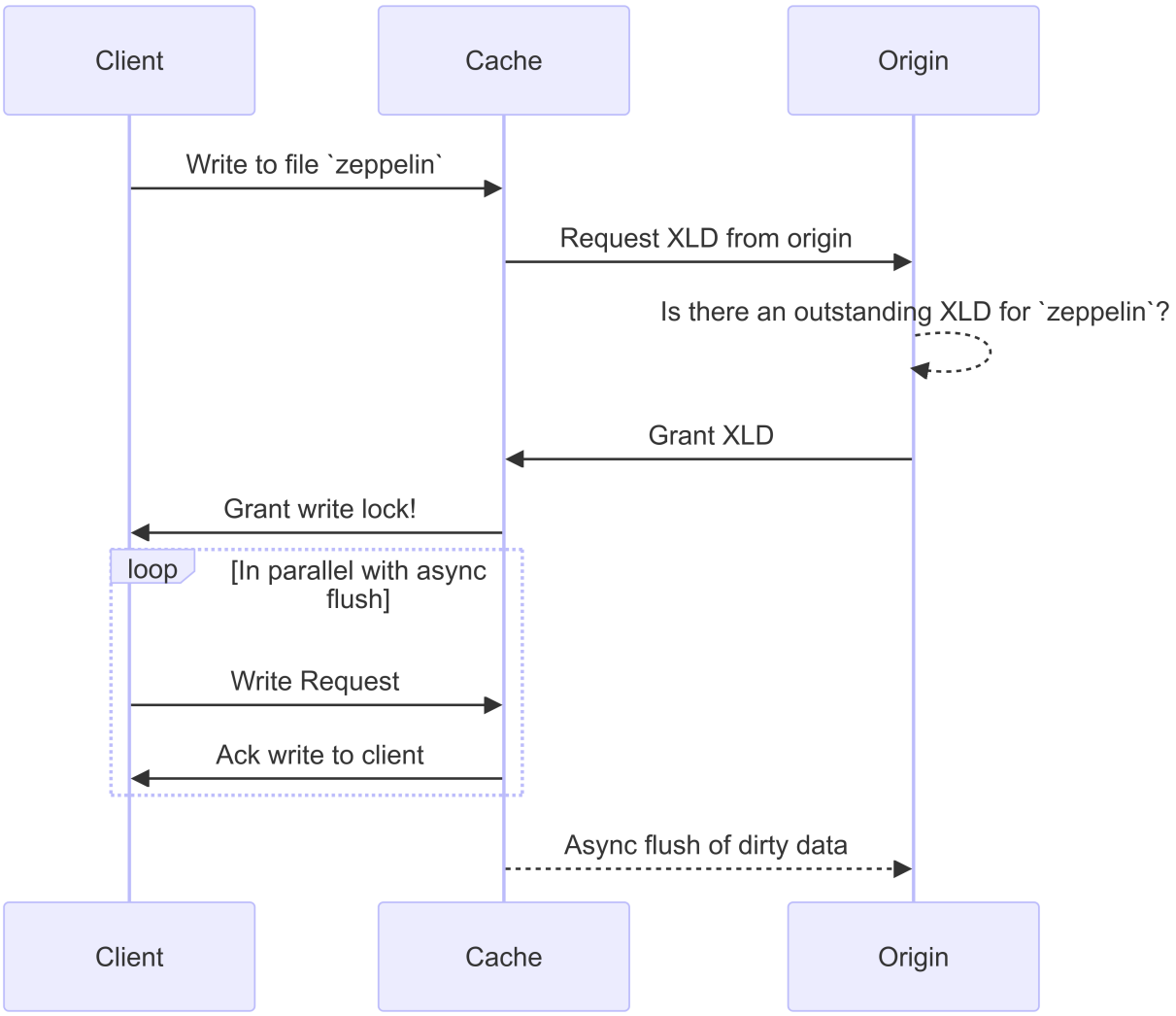
시퀀스 다이어그램

이러한 시퀀스 다이어그램은 write-around 모드와 write-back 모드 간의 쓰기 확인의 차이를 나타냅니다.

쓰기



다시 쓰기



ONTAP FlexCache 후기입 사용 사례

쓰기 프로파일은 다시 쓰기 가능 FlexCache에 가장 적합합니다. 작업을 테스트하여 Write-back 또는 write-around가 최상의 성능을 제공하는지 확인해야 합니다.

Write-back은 write-around를 대체하는 것이 아닙니다. 쓰기 작업이 많은 워크로드를 처리하기 위해 쓰기팅을 설계했지만 여전히 많은 워크로드에서 쓰기 작업이 더 적합합니다.

타겟 워크로드

파일 크기

파일 크기는 및 파일 호출 사이에 실행된 쓰기 수보다 덜 `OPEN CLOSE` 중요합니다. 작은 파일은 기본적으로 호출 수가 적기 때문에 `WRITE` 다시 쓰기에 적합하지 않습니다. 큰 파일은 및 호출 사이에 더 많은 쓰기를 가질 수 `OPEN CLOSE` 있지만, 이는 보장되지 않습니다.

"FlexCache write-back 지침"최대 파일 크기에 대한 최신 권장 사항은 페이지를 참조하십시오.

쓰기 크기

클라이언트에서 쓸 때 쓰기 호출이 아닌 다른 수정 NAS 호출이 관련됩니다. 여기에는 다음이 포함되지만 이에 국한되지 않습니다.

- CREATE
- OPEN
- CLOSE
- SETATTR
- SET_INFO

SETATTR SET_INFO atime , , ctime, , owner group 또는 를 size 설정한 호출이 mtime 캐시에서 처리됩니다. 이러한 나머지 호출은 오리진에서 처리되어야 하며, 작업 중인 파일에 대해 Write-back이 활성화된 캐시에 누적된 더티 데이터의 Write-Back을 트리거해야 합니다. 파일 입출력은 쓰기가 완료될 때까지 정지됩니다.

이러한 호출이 WAN을 통과해야 한다는 것을 알면 다시 쓰기에 적합한 워크로드를 식별하는 데 도움이 됩니다. 일반적으로 OPEN CLOSE 위에 나열된 다른 호출 중 하나를 실행하지 않고 및 호출 간에 수행할 수 있는 쓰기가 많을수록 성능 향상 Write-Back이 더 좋습니다.

쓰기 후 읽기

지금까지 FlexCache에서 쓰기 후 읽기 워크로드의 성능은 좋지 않았습니다. 이는 9.15.1 이전의 write-around 동작 방식 때문이다. WRITE`파일에 대한 호출은 오리진에서 커밋되어야 하며, 후속 `READ 호출은 데이터를 다시 캐시로 가져와야 합니다. 이로 인해 두 작업 모두 WAN 페널티가 발생합니다. 따라서 FlexCache의 경우 쓰기 후 읽기 워크로드는 쓰기 방지 모드로 사용하지 않습니다. 9.15.1에 쓰기 저장 기능이 도입됨에 따라 데이터가 캐시에서 커밋되고 캐시에서 즉시 읽을 수 있으므로 WAN 페널티가 없어집니다. 워크로드에 FlexCache 볼륨에 쓰기 후 읽기 가 포함된 경우에는 write-back 모드로 작동하도록 캐시를 구성해야 합니다.

쓰기 후 읽기가 작업 부하에서 중요한 부분인 경우 다시 쓰기 모드로 작동하도록 캐시를 구성해야 합니다.

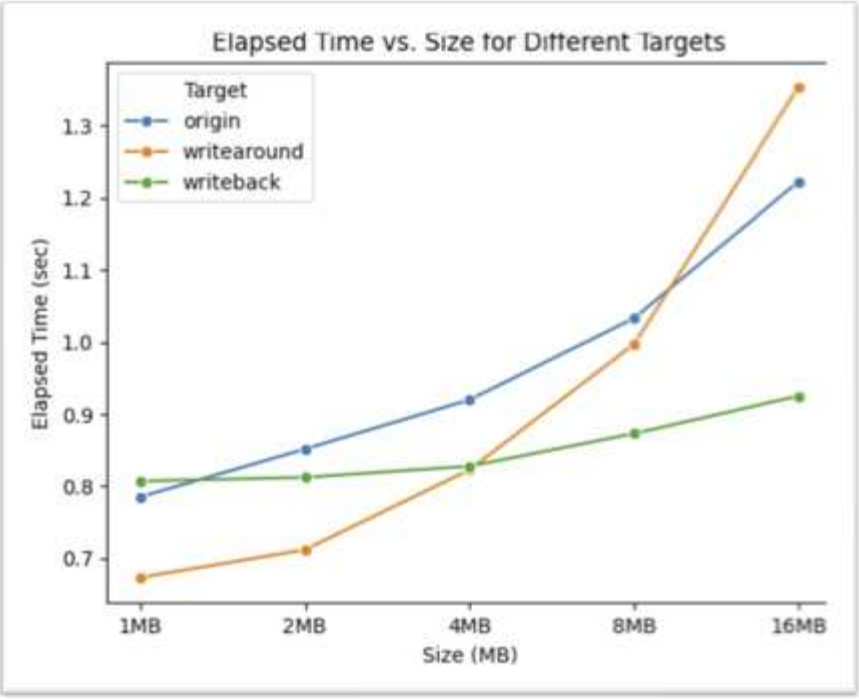
쓰기 후 쓰기

파일이 캐시에 더티 데이터를 축적하면 캐시는 데이터를 원본에 비동기적으로 씁니다. 이렇게 되면 원래 위치로 다시 플러시될 때까지 계속 대기 중인 더티 데이터로 파일이 닫히는 경우가 발생합니다. 방금 닫은 파일에 대해 다른 열기 또는 쓰기가 들어오면 더티 데이터가 모두 오리진으로 플러시될 때까지 쓰기가 일시 중단됩니다.

지연 시간 고려

FlexCache가 Write-back 모드로 작동하는 경우 지연 시간이 증가함에 따라 NAS 클라이언트에 더 많은 이점을 제공합니다. 하지만 지연 시간이 짧은 환경에서 얻을 수 있는 이점보다 쓰기 작업의 오버헤드가 훨씬 더 중요합니다. 일부 NetApp 테스트에서는 캐시와 원본 간 지연 시간이 8ms를 최소한으로 초과했을 때 쓰기 저장 이점이 시작되었습니다. 이 지연 시간은 워크로드에 따라 달라지므로 워크로드의 반환 시점을 테스트해야 합니다.

다음 그래프는 NetApp 랩 테스트에서 Write-back에 대한 반환 지점을 보여 줍니다. x`축은 파일 크기이고 `y 축은 경과 시간입니다. 이 테스트에서는 NFSv3, 256KB 및 64ms의 WAN 지연 시간으로 마운트했습니다. rsize wsize 이 테스트는 캐시와 오리진에 대해 작은 ONTAP Select 인스턴스와 단일 스레드 쓰기 작업을 사용하여 수행되었습니다. 결과는 다를 수 있습니다.



클러스터 내 캐싱에는 Write-back을 사용해서는 안 됩니다. 클러스터 내 캐싱은 오리진과 캐시가 같은 클러스터에 있을 때 발생합니다.

ONTAP FlexCache write-back 사전 요구 사항

쓰기 저장 모드로 FlexCache를 배포하기 전에 이러한 성능, 소프트웨어, 라이센스 및 시스템 구성 요구 사항을 충족하는지 확인하십시오.

CPU 및 메모리

쓰기 저장이 활성화된 캐시에서 시작된 쓰기 저장 메시지를 수용하기 위해 각 원본 클러스터 노드에 최소 128GB의 RAM과 20개의 CPU가 있는 것이 강력히 권장됩니다. A400 이상과 동일합니다. 오리진 클러스터가 복수 쓰기 가능 FlexCaches의 오리진으로 작동하는 경우 더 많은 CPU와 RAM이 필요합니다.

작업 부하에 크기가 작은 원본을 사용하면 다시 쓰기 가능 캐시 또는 오리진에서 성능에 큰 영향을 줄 수 있습니다.

ONTAP 버전입니다

- 오리진 *_MUST_ * 에서 ONTAP 9.15.1 이상을 실행하고 있습니다.
- write-back 모드에서 작동해야 하는 캐싱 클러스터는 *_must_ * ONTAP 9.15.1 이상을 실행하고 있습니다.
- write-back 모드로 작동할 필요가 없는 캐싱 클러스터는 일반적으로 지원되는 모든 ONTAP 버전을 실행할 수 있습니다.

라이센싱

ONTAP 구매에 쓰기 작업 모드를 포함한 FlexCache가 포함됩니다. 추가 라이센스가 필요하지 않습니다.

피어링

- 오리진 및 캐시 클러스터는 이어야 합니다 "클러스터 피어링된"
- 원본 및 캐시 클러스터의 SVM(서버 가상 머신)은 FlexCache 옵션을 사용해야 합니다 "SVM 피어링이 발생했습니다" .

캐시 클러스터를 다른 캐시 클러스터로 피어링할 필요가 없습니다. 또한 캐시 SVM을 다른 캐시 SVM에 피어링할 필요가 없습니다.

ONTAP FlexCache write-back 상호 운용성

write-back 모드로 FlexCache를 구축할 때 고려해야 할 상호 운용성 사항을 이해합니다.

ONTAP 버전입니다

쓰기 저장 모드를 사용하려면 캐시와 오리진 * 둘 다에서 ONTAP 9.15.1 이상을 실행하고 있어야 합니다.

Write-back 사용 캐시가 필요하지 않은 클러스터는 이전 버전의 ONTAP를 실행할 수 있지만 해당 클러스터는 write-around 모드에서만 작동할 수 있습니다.

사용자 환경에서 ONTAP 버전을 혼합하여 사용할 수 있습니다.

클러스터	ONTAP 버전입니다	후기입 지원 여부
* 원점 *	ONTAP 9.15.1	해당 없음 †
* 클러스터 1 *	ONTAP 9.15.1	예
* 클러스터 2 *	ONTAP 9.14.1	아니요

클러스터	ONTAP 버전입니다	후기입 지원 여부
* 원점 *	ONTAP 9.14.1	해당 없음 †
* 클러스터 1 *	ONTAP 9.15.1	아니요
* 클러스터 2 *	ONTAP 9.15.1	아니요

†_Origins는 캐시가 아니므로 write-back 또는 write-around 지원은 적용할 수 없습니다. _

에서는 [example2-table]오리진이 엄격한 요구 사항인 ONTAP 9.15.1 이상을 실행하고 있지 않기 때문에 두 클러스터 모두 다시 쓰기 모드를 활성화할 수 없습니다.

클라이언트 상호 운용성

ONTAP에서 일반적으로 지원하는 모든 클라이언트는 FlexCache 볼륨이 write-around 모드로 작동하든 write-back 모드로 작동하든 상관없이 볼륨에 액세스할 수 있습니다. 지원되는 클라이언트의 최신 목록은 NetApp을 참조하십시오. "상호 운용성 매트릭스"

클라이언트 버전은 특별히 중요하지 않지만 NFSv3, NFSv4.0, NFSv4.1, SMB2.x 또는 SMB3.x를 지원할 수 있을 만큼 새로운 클라이언트여야 합니다 SMB1 및 NFSv2는 더 이상 사용되지 않는 프로토콜이며 지원되지 않습니다.

다시 쓰기 및 덮어쓰기를 수행합니다

에서 볼 수 있듯이 [example1-table]write-back 모드에서 작동하는 FlexCache는 write-around 모드로 작동하는 캐시와 함께 존재할 수 있습니다. 특정 작업 부하와 Write-Back을 비교하여 사용하는 것이 좋습니다.

write-back과 write-around 간에 워크로드 성능이 동일할 경우 write-around를 사용합니다.

ONTAP 기능 상호 운용성

FlexCache 기능 상호 운용성에 대한 최신 목록은 을 참조하십시오 "FlexCache 볼륨에 대해 지원되는 기능과 지원되지 않는 기능".

ONTAP FlexCache write-back 설정 및 관리

ONTAP 9.15.1부터 FlexCache 볼륨에서 FlexCache Write-back 모드를 활성화하여 에지 컴퓨팅 환경 및 쓰기 작업이 많은 워크로드가 있는 캐시에 더 나은 성능을 제공할 수 있습니다. 또한 필요한 경우 FlexCache 볼륨에 write-back이 설정되어 있는지 아니면 볼륨에 대한 write-back을 사용하지 않도록 설정할 수도 있습니다.

캐시 볼륨에 다시 쓰기가 설정되어 있으면 쓰기 요청이 원본 볼륨이 아닌 로컬 캐시로 전송됩니다.

시작하기 전에

고급 권한 모드여야 합니다.

Write-back이 설정된 새 **FlexCache** 볼륨을 생성합니다

단계

ONTAP System Manager 또는 ONTAP CLI를 사용하여 write-back을 사용하도록 설정한 새 FlexCache 볼륨을 생성할 수 있습니다.

시스템 관리자

1. FlexCache 볼륨이 원본 볼륨과 다른 클러스터에 있는 경우 클러스터 피어 관계를 생성합니다.
   a. 로컬 클러스터에서 * 보호 > 개요 * 를 클릭합니다.
   b. Intercluster Settings * 를 확장하고 * Add Network Interfaces * 를 클릭한 후 클러스터에 클러스터 간 인터페이스를 추가합니다.

      원격 클러스터에서 이 작업을 반복합니다.

   c. 원격 클러스터에서 * 보호 > 개요 * 를 클릭합니다. Cluster Peers 섹션을 클릭하고 * Generate Passphrase * 를 클릭합니다.
   d. 생성된 암호를 복사하여 로컬 클러스터에 붙여넣습니다.
   e. 로컬 클러스터의 클러스터 피어 아래에서 * 피어 클러스터 * 를 클릭하고 로컬 및 원격 클러스터를 피어링합니다.
2. FlexCache 볼륨이 원본 볼륨과 다른 클러스터에 있는 경우 SVM 피어 관계를 생성합니다.

   스토리지 VM 피어 * 아래에서 * 피어 스토리지 VM * 을 클릭한 다음 * 피어 스토리지 VM * 을 클릭하여 스토리지 VM을 피어링합니다.

   FlexCache 볼륨이 동일한 클러스터에 있는 경우 System Manager를 사용하여 SVM 피어 관계를 생성할 수 없습니다.
3. 스토리지 > 볼륨 * 을 선택합니다.
4. 추가 * 를 선택합니다.
5. More Options * 를 선택한 다음 * Add as cache for a remote volume * 를 선택합니다.
6. Enable FlexCache write-back * 을 선택합니다.

CLI를 참조하십시오

1. 생성할 FlexCache 볼륨이 다른 클러스터에 있는 경우 클러스터 피어 관계를 생성합니다.
   a. 대상 클러스터에서 데이터 보호 소스 클러스터와 피어 관계를 생성합니다.

```
cluster peer create -generate-passphrase -offer-expiration
MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addrs
<peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,..|*
-ipspace <ipspace_name>
```

      ONTAP 9.6부터는 클러스터 피어 관계를 만들 때 TLS 암호화가 기본적으로 활성화됩니다. TLS 암호화는 오리진과 FlexCache 볼륨 간의 인터클러스터 통신에 지원됩니다. 필요한 경우 클러스터 피어 관계에 대해 TLS 암호화를 비활성화할 수도 있습니다.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
              Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: *
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

a. 소스 클러스터에서 소스 클러스터를 대상 클러스터에 인증합니다.

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship,
use a phrase or sequence of characters that would be hard to
guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

2. FlexCache 볼륨이 원본 볼륨과 다른 SVM에 있는 경우 애플리케이션으로서 "FlexCache"와 SVM 피어 관계를 생성합니다.

a. SVM이 다른 클러스터에 있는 경우 피어링 SVM에 대한 SVM 권한을 생성합니다.

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

다음 예에서는 모든 로컬 SVM에 적용되는 SVM 피어 권한을 생성하는 방법을 보여줍니다.

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache

Warning: This Vserver peer permission applies to all local Vservers.
After that no explict
"vserver peer accept" command required for Vserver peer relationship
creation request
from peer cluster "cluster2" with any of the local Vservers. Do you
want to continue? {y|n}: y
```

a. SVM 피어 관계 생성:

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. Write-Back(후기입)이 설정된 FlexCache 볼륨 생성:

```
volume flexcache create -vserver <cache_vserver_name> -volume
<cache_flexgroup_name> -aggr-list <list_of_aggregates> -origin
-volume <origin flexgroup> -origin-vserver <origin_vserver name>
-junction-path <junction_path> -is-writeback-enabled true
```

기존 **FlexCache** 볼륨에서 **FlexCache write-back**을 활성화합니다

ONTAP System Manager 또는 ONTAP CLI를 사용하여 기존 FlexCache 볼륨에서 FlexCache write-back을 활성화할 수 있습니다.

시스템 관리자

1. 스토리지 > 볼륨 * 을 선택하고 기존 FlexCache 볼륨을 선택합니다.
2. 볼륨의 개요 페이지에서 오른쪽 상단에 있는 * 편집 * 을 클릭합니다.
3. 볼륨 편집 * 창에서 * FlexCache 다시 쓰기 활성화 * 를 선택합니다.

CLI를 참조하십시오

1. 기존 FlexCache 볼륨에서 write-back 활성화:

```
volume flexcache config modify -volume <cache_flexgroup_name> -is
-writeback-enabled true
```

FlexCache write-back이 활성화되어 있는지 확인한다

단계

System Manager 또는 ONTAP CLI를 사용하여 FlexCache write-back이 활성화되어 있는지 확인할 수 있습니다.

시스템 관리자

1. 스토리지 > 볼륨 * 을 선택하고 볼륨을 선택합니다.
2. 볼륨 * 개요 * 에서 * FlexCache details * 를 찾아 FlexCache 볼륨에서 FlexCache write-back이 * Enabled * 로 설정되어 있는지 확인합니다.

CLI를 참조하십시오

1. FlexCache write-back이 활성화되어 있는지 확인합니다.

```
volume flexcache config show -volume <cache_flexgroup_name> -fields
is-writeback-enabled
```

FlexCache 볼륨에서 write-back을 비활성화합니다

FlexCache 볼륨을 삭제하려면 먼저 FlexCache Write-Back을 비활성화해야 합니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 FlexCache write-back을 사용하지 않도록 설정할 수 있습니다.

시스템 관리자

1. 스토리지 > 볼륨 * 을 선택하고 FlexCache write-back이 활성화된 기존 FlexCache 볼륨을 선택합니다.
2. 볼륨의 개요 페이지에서 오른쪽 상단에 있는 * 편집 * 을 클릭합니다.
3. 볼륨 편집 * 창에서 * FlexCache 다시 쓰기 활성화 * 를 선택 해제합니다.

CLI를 참조하십시오

1. 후기입 해제:

```
volume flexcache config modify -volume <cache_vol_name> -is
-writeback-enabled false
```

ONTAP FlexCache 후기입(Write-Back)에 대한 질문과 대답(FAQ

이 FAQ는 질문에 대한 빠른 답변을 찾는 경우에 도움이 될 수 있습니다.

다시 쓰기를 사용하고 싶습니다. 어떤 버전의 ONTAP를 실행해야 합니까?

캐시와 오리진 모두 ONTAP 9.15.1 이상을 실행해야 합니다. 최신 P 릴리스를 실행하는 것이 좋습니다. 엔지니어링은 Write-back 사용 캐시의 성능과 기능을 지속적으로 개선하고 있습니다.

오리진에 액세스하는 클라이언트가 다시 쓰기 가능 캐시에 액세스하는 클라이언트에 영향을 줄 수 있습니까**?**

예. 오리진에는 캐시와 동일한 데이터 권한이 있습니다. 캐시에서 파일을 제거하거나 잠금/데이터 위임을 취소해야 하는 파일에 대해 작업이 실행되는 경우 캐시의 클라이언트에서 파일 액세스가 지연될 수 있습니다.

Write-back 지원 **FlexCaches**에 **QoS**를 적용할 수 있습니까**?**

예. 모든 캐시와 오리진에는 독립적인 QoS 정책이 적용될 수 있습니다. 이 기능은 write-back이 시작되는 인터클러스터 트래픽에 직접적인 영향을 주지 않습니다. 간접적으로 write-back 지원 캐시에서 프런트 엔드 트래픽을 제한하여 인터클러스터 write-back 트래픽을 줄일 수 있습니다.

멀티 프로토콜 **NAS**는 후기입 가능 **FlexCaches**에서 지원됩니까**?**

예. 멀티 프로토콜은 후기입 가능 FlexCaches에서 완벽하게 지원됩니다. 현재 NFSv4.2 및 S3는 write-around 또는 write-back 모드로 작동하는 FlexCache에서 지원되지 않습니다.

SMB 대체 데이터 스트림은 후기입 지원 **FlexCaches**에서 지원됩니까**?**

SMB ADS(대체 데이터 스트림)는 지원되지만 Write-Back을 통해 가속화되지는 않습니다. ADS에 대한 쓰기가 오리진으로 전달되어 WAN 지연 시간이 줄어듭니다. 또한 쓰기는 ADS가 캐시의 일부인 주 파일을 제거합니다.

캐시를 생성한 후 **write-around** 모드와 **write-back** 모드 간에 전환할 수 있습니까**?**

예. 당신은 할 일은 링크의 플래그를 토글하는 것입니다 `is-writeback-enabled`:../FlexCache-writeback/FlexCache -writeback-enable-task.html[`flexcache modify` 명령].

캐시와 원본 간의 클러스터 간 링크에 대해 알아야 할 대역폭 고려 사항이 있습니까**?**

네. FlexCache 쓰기 저장은 캐시와 원본 간의 클러스터 간 링크에 크게 의존합니다. 대역폭이 낮거나 손실이 많은 네트워크는 성능에 상당한 부정적인 영향을 미칠 수 있습니다. 작업 부하에 따라 크게 달라지므로 특정 대역폭 요구 사항은 없습니다.

FlexCache 이중성

FlexCache 이중성에 대한 **FAQ**

이 FAQ는 ONTAP 9.18.1에서 도입된 FlexCache 이중화에 대한 일반적인 질문에 답변합니다.

자주 묻는 질문

"이원성**"**이란 무엇입니까**?**

듀얼리티(Duality)는 파일(NAS) 및 객체(S3) 프로토콜을 모두 사용하여 동일한 데이터에 통합적으로 접근할 수 있도록 합니다. FlexCache 지원 없이 ONTAP 9.12.1에서 처음 도입된 듀얼리티는 ONTAP 9.18.1에서 FlexCache 볼륨을 포함하도록 확장되어 FlexCache 볼륨에 캐시된 NAS 파일에 S3 프로토콜 액세스를 허용합니다.

FlexCache S3 버킷에서 지원되는 **S3** 작업에는 어떤 것들이 있습니까**?**

표준 S3 NAS 버킷에서 지원되는 S3 작업은 FlexCache S3 NAS 버킷에서도 지원되지만 `COPY` 작업은 예외입니다. 표준 S3 NAS 버킷에서 지원되지 않는 작업의 최신 목록은 "상호 운용성 문서"를 참조하십시오.

FlexCache 이중성 기능을 사용하여 **FlexCache**를 쓰기 후 저장 모드로 사용할 수 있습니까**?**

아니요. FlexCache 볼륨에 FlexCache S3 NAS 버킷을 생성하려면 FlexCache 볼륨이 반드시 쓰기 우회 모드여야 합니다. 쓰기 백 모드로 설정된 FlexCache 볼륨에 FlexCache S3 NAS 버킷을 생성하려고 하면 작업이 실패합니다.

하드웨어 제한 때문에 클러스터 중 하나를 **ONTAP 9.18.1**로 업그레이드할 수 없습니다**.** 캐시 클러스터만 **ONTAP 9.18.1**을 실행하는 경우 내 클러스터에서 **duality**가 계속 작동합니까**?**

아니요. 캐시 클러스터와 오리진 클러스터 모두 최소 유효 클러스터 버전이 9.18.1 이상이어야 합니다. ONTAP 버전 9.18.1보다 이전 버전인 오리진 클러스터와 피어링된 캐시 클러스터에 FlexCache S3 NAS 버킷을 생성하려고 하면 작업이 실패합니다.

MetroCluster 구성이 있습니다**. FlexCache** 이중화 기능을 사용할 수 있습니까**?**

아니요. FlexCache 이중성은 MetroCluster 구성에서 지원되지 않습니다.

FlexCache S3 NAS 버킷에 있는 파일에 대한 **S3** 액세스를 감사할 수 있습니까**?**

S3 감사는 FlexCache 볼륨에서 사용하는 NAS 감사 기능을 통해 제공됩니다. FlexCache 볼륨의 NAS 감사에 대한 자세한 내용은 "FlexCache 감사에 대해 자세히 알아보세요"를 참조하십시오.

캐시 클러스터가 원본 클러스터에서 연결이 끊어지면 어떻게 됩니까**?**

FlexCache S3 NAS 버킷에 대한 S3 요청은 캐시 클러스터가 원본 클러스터에서 연결이 끊어진 경우 `503 Service Unavailable` 오류와 함께 실패합니다.

FlexCache 이중성을 사용하여 **S3** 멀티파트 작업을 수행할 수 있습니까**?**

멀티파트 S3 작업이 제대로 작동하려면 기본 FlexCache 볼륨의 granular-data 필드가 'advanced'로 설정되어 있어야 합니다. 이 필드는 원본 볼륨에 설정된 값으로 설정됩니다.

FlexCache 이중화 기능은 **HTTP**와 **HTTPS** 액세스를 모두 지원합니까**?**

예. 기본적으로 HTTPS가 필요합니다. 필요한 경우 S3 서비스에서 HTTP 액세스를 허용하도록 구성할 수 있습니다.

NAS FlexCache 볼륨에 대한 **S3** 액세스를 활성화합니다

ONTAP 9.18.1부터 NAS FlexCache 볼륨에 대한 S3 액세스를 활성화할 수 있으며, 이를 "이중성"이라고도 합니다. 이를 통해 클라이언트는 NFS 및 SMB와 같은 기존 NAS 프로토콜 외에도 S3 프로토콜을 사용하여 FlexCache 볼륨에 저장된 데이터에 액세스할 수 있습니다. 다음 정보를 사용하여 FlexCache 이중성을 설정할 수 있습니다.

필수 구성 요소

시작하기 전에 다음 필수 조건을 모두 완료했는지 확인하십시오.

- S3 프로토콜과 원하는 NAS 프로토콜(NFS, SMB 또는 둘 다)에 대한 라이센스가 부여되고 SVM에 구성되어 있는지 확인하십시오.
- DNS 및 기타 필요한 서비스가 구성되어 있는지 확인하십시오.
- 클러스터 및 SVM 피어링됨
- FlexCache 볼륨 생성
- 데이터 LIF가 생성되었습니다

FlexCache 이중성에 대한 더 자세한 문서는 "ONTAP S3 멀티프로토콜 지원"을 참조하십시오.

1단계**:** 인증서 생성 및 서명

FlexCache 볼륨에 대한 S3 액세스를 활성화하려면 FlexCache 볼륨을 호스팅하는 SVM에 인증서를 설치해야 합니다. 이 예제에서는 자체 서명 인증서를 사용하지만 운영 환경에서는 신뢰할 수 있는 인증 기관(CA)에서 서명한 인증서를 사용해야 합니다.

1. SVM 루트 CA 생성:

```
security certificate create -vserver <svm> -type root-ca -common-name
<arbitrary_name>
```

2. 인증서 서명 요청 생성:

```
security certificate generate-csr -common-name <dns_name_of_data_lif>
-dns-name <dns_name_of_data_lif> -ipaddr <data_lif_ip>
```

출력 예:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICzjCCAbYCAQAwHzEdMBsGA1UEAxMUY2FjaGUxZy1kYXRhLm5hcy5sYWIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCusJk075O8Uh329cHI6x+BaRS2
w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK1CI2VEkrXGUg
...
vMIGN351+FgzLQ4X5lKfoMXCV70NqIakxzEmkTIUDKv7n9EVZ4b5DTTlrL03X/nK
+Bim2y2y180PaFB3NauZHTnIIzIc8zCp2IEqmFWyMDcdBjP9KS0+jNm4QhuXiM8F
D7gm3g/O70qa5OxbAEal5o4NbOl95U0T0rwqTaSzFG0XQnK2PmA1OIwS5ET35p3Z
dLU=
-----END CERTIFICATE REQUEST-----
```

개인 키 예:

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCusJk075O8Uh32
9cHI6x+BaRS2w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK
1CI2VEkrXGUgwBtx1K4IlrCTB829Q1aLGAQXVyWnzhQc4tS5PW/DsQ8t7olZ9zEI
...
rXGEdDaqp7jQGNXUGlbxO3zcBil1/A9Hc6oalNECgYBKwe3PeZamiwhIHLy9ph7w
dJfFCshsPalMuAp2OuKIAnNa9l6fT9y5kf9tIbskT+t5Dth8bmV9pwe8UZaK5eC4
Svxm19jHT5QqloDaZVUmMXFKyKoqPDdfvcDk2Eb5gMfIIb0a3TPC/jqqpDn9BzuH
TO02fuRvRR/G/HUz2yRd+A==
-----END PRIVATE KEY-----
```

나중에 참조할 수 있도록 인증서 요청서와 개인 키 사본을 보관하십시오.

3. 인증서에 서명합니다.

`root-ca`는 <<anchor1-step,SVM 루트 CA 생성>>에서 생성한 것입니다.

```
certificate sign -ca <svm_root_ca> -ca-serial <svm_root_ca_sn> -expire
-days 364 -format PEM -vserver <svm>
```

4. 인증서 서명 요청 생성에서 생성된 CSR(Certificate Signing Request)을 붙여넣습니다.

   예:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICzjCCAbYCAQAwHzEdMBsGA1UEAxMUY2FjaGUxZy1kYXRhLm5hcy5sYWIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCusJk075O8Uh329cHI6x+BaRS2
w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK1CI2VEkrXGUg
...
vMIGN351+FgzLQ4X5lKfoMXCV70NqIakxzEmkTIUDKv7n9EVZ4b5DTTlrL03X/nK
+Bim2y2y180PaFB3NauZHTnIIzIc8zCp2IEqmFWyMDcdBjP9KS0+jNm4QhuXiM8F
D7gm3g/O70qa5OxbAEal5o4NbOl95U0T0rwqTaSzFG0XQnK2PmA1OIwS5ET35p3Z
dLU=
-----END CERTIFICATE REQUEST-----
```

   이 명령은 다음 예와 유사한 서명된 인증서를 콘솔에 출력합니다.

   서명된 인증서 예:

```
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIIGHolbgv5DPowDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMWY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMAkGA1UEBhMCVVMwHhcNMjUxMTIx
MjIxNTU4WhcNMjYxMTIwMjIxNTU4WjAfMR0wGwYDVQQDExRjYWNoZTFnLWRhdGEu
...
qS7zhj3ikWE3Gp9s+QijKWXx/0HDd1UuGqy0QZNqNm/M0mqVnokJNk5F4fBFxMiR
1o63BxL8xGIRdtTCjjb2Gq2Wj7EClUw6CykEkxAcVk+XrRtArGkNtcYdtHfUsKVE
wswvv0rNydrNnWhJLhSl8TW5Tex+OMyTXgk9/3K8kB0mAMrtxxYjt8tm+gztkivf
J0eo1uDJhaNxqwEZRzFyGaa4k1+56oFzRfTc
-----END CERTIFICATE-----
```

5. 다음 단계를 위해 인증서를 복사합니다.
6. SVM에 서버 인증서를 설치합니다.

```
certificate install -type server -vserver <svm> -cert-name flexcache-
duality
```

7. 인증서에 서명합니다에서 서명된 인증서를 붙여넣습니다.

   예:

```
Please enter Certificate: Press <Enter> [twice] when done
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIIGHolbgv5DPowDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMWY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMAkGA1UEBhMCVVMwHhcNMjUxMTIx
MjIxNTU4WhcNMjYxMTIwMjIxNTU4WjAfMR0wGwYDVQQDExRjYWNoZTFnLWRhdGEu
bmFzLmxhYjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK6wmTTvk7xS
...
qS7zhj3ikWE3Gp9s+QijKWXx/0HDd1UuGqy0QZNqNm/M0mqVnokJNk5F4fBFxMiR
1o63BxL8xGIRdtTCjjb2Gq2Wj7EClUw6CykEkxAcVk+XrRtArGkNtcYdtHfUsKVE
wswvv0rNydrNnWhJLhSl8TW5Tex+OMyTXgk9/3K8kB0mAMrtxxYjt8tm+gztkivf
J0eo1uDJhaNxqwEZRzFyGaa4k1+56oFzRfTc
-----END CERTIFICATE-----
```

8. 인증서 서명 요청 생성에서 생성된 개인 키를 붙여넣습니다.

   예:

```
Please enter Private Key: Press <Enter> [twice] when done
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCusJk075O8Uh32
9cHI6x+BaRS2w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK
1CI2VEkrXGUgwBtx1K4IlrCTB829Q1aLGAQXVyWnzhQc4tS5PW/DsQ8t7olZ9zEI
W/gaEIajgpXIwGNWZ+weKQK+yoolxC+gy4IUE7WvnEUiezaIdoqzyPhYq5GC4XWf
0johpQugOPe0/w2nVFRWJoFQp3ZP3NZAXc8H0qkRB6SjaM243XV2jnuEzX2joXvT
wHHH+IBAQ2JDs7s1TY0I20e49J2Fx2+HvUxDx4BHao7CCHA1+MnmEl+9E38wTaEk
NLsU724ZAgMBAAECggEABHUy06wxcIk5hO3S9Ik1FDZV3JWzsu5gGdLSQOHRd5W+
...
rXGEdDaqp7jQGNXUGlbxO3zcBil1/A9Hc6oalNECgYBKwe3PeZamiwhIHLy9ph7w
dJfFCshsPalMuAp2OuKIAnNa9l6fT9y5kf9tIbskT+t5Dth8bmV9pwe8UZaK5eC4
Svxm19jHT5QqloDaZVUmMXFKyKoqPDdfvcDk2Eb5gMfIIb0a3TPC/jqqpDn9BzuH
TO02fuRvRR/G/HUz2yRd+A==
-----END PRIVATE KEY-----
```

9. 서버 인증서의 인증서 체인을 구성하는 인증 기관(CA)의 인증서를 입력하십시오.

   이는 서버 인증서를 발급한 CA 인증서부터 시작하여 루트 CA 인증서까지 이어질 수 있습니다.

```
Do you want to continue entering root and/or intermediate certificates
{y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.

The installed certificate's CA and serial number for reference:
CA: cache-164g-svm-root-ca
serial: 187A256E0BF90CFA
```

10. SVM 루트 CA의 공개 키를 가져옵니다.

```
security certificate show -vserver <svm> -common-name <root_ca_cn> -ca
<root_ca_cn> -type root-ca -instance

-----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIIGHokTnbsHKEwDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMWY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMAkGA1UEBhMCVVMwHhcNMjUxMTIx
MjE1NTIzWhcNMjYxMTIxMjE1NTIzWjAuMR8wHQYDVQQDExZjYWNoZS0xNjRnLXN2
bS1yb290LWNhMQswCQYDVQQGEwJVUzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
...
DoOL7vZFFt44xd+rp0DwafhSnLH5HNhdIAfa2JvZW+eJ7rgevH9wmOzyc1vaihl3
Ewtb6cz1a/mtESSYRNBmGkIGM/SFCy5v1ROZXCzF96XPbYQN4cW0AYI3AHYBZP0A
HlNzDR8iml4k9IuKf6BHLFA+VwLTJJZKrdf5Jvjgh0trGAbQGI/Hp2Bjuiopkui+
n4aa5Rz0JFQopqQddAYnMuvcq10CyNn7S0vF/XLd3fJaprH8kQ==
-----END CERTIFICATE-----
```

이는 클라이언트가 SVM 루트 CA에서 서명한 인증서를 신뢰하도록 구성하는 데 필요합니다. 공개 키가 콘솔에 출력됩니다. 공개 키를 복사하여 저장하십시오. 이 명령의 값은 SVM 루트 CA 생성에 입력한 값과 동일합니다.

2단계**: S3** 서버 구성

1. S3 프로토콜 액세스 활성화:

```
vserver show -vserver <svm> -fields allowed-protocols
```

S3는 기본적으로 SVM 수준에서 허용됩니다.

2. 기존 정책 복제:

```
network interface service-policy clone -vserver <svm> -policy default-
data-files -target-vserver <svm> -target-policy <any_name>
```

3. 복제된 정책에 S3를 추가합니다.

```
network interface service-policy add-service -vserver <svm> -policy
<any_name> -service data-s3-server
```

4. 데이터 LIF에 새 정책을 추가합니다.

```
network interface modify -vserver <svm> -lif <data_lif> -service-policy
duality
```

> 기존 LIF의 서비스 정책을 수정하면 중단이 발생할 수 있습니다. LIF를 중지했다가 새 서비스에 대한 리스너와 함께 다시 시작해야 합니다. TCP는 이 작업에서 빠르게 복구되어야 하지만 잠재적인 영향을 인지하고 있어야 합니다.

5. SVM에 S3 오브젝트 저장소 서버를 생성합니다.

```
vserver object-store-server create -vserver <svm> -object-store-server
<dns_name_of_data_lif> -certificate-name flexcache-duality
```

6. FlexCache 볼륨에서 S3 기능을 활성화합니다.

`flexcache config`옵션 `-is-s3-enabled`을 버킷을 생성하기 전에 `true`로 설정해야 합니다. 또한 `-is-writeback-enabled`옵션을 `false`로 설정해야 합니다.

다음 명령은 기존 FlexCache를 수정합니다.

```
flexcache config modify -vserver <svm> -volume <fcache_vol> -is
-writeback-enabled false -is-s3-enabled true
```

7. S3 버킷 생성:

```
vserver object-store-server bucket create -vserver <svm> -bucket
<bucket_name> -type nas -nas-path <flexcache_junction_path>
```

8. 버킷 정책 생성:

```
vserver object-store-server bucket policy add-statement -vserver <svm>
-bucket <bucket_name> -effect allow
```

9. S3 사용자 생성:

```
vserver object-store-server user create -user <user> -comment ""
```

출력 예:

```
    Vserver: <svm>>
       User: <user>>
 Access Key: WCOT7...Y7D6U
 Secret Key: 6143s...pd__P
    Warning: The secret key won't be displayed again. Save this key for
future use.
```

10. 루트 사용자의 키 재생성:

```
vserver object-store-server user regenerate-keys -vserver <svm> -user
root
```

출력 예:

```
    Vserver: <svm>>
       User: root
 Access Key: US791...2F1RB
 Secret Key: tgYmn...8_3o2
    Warning: The secret key won't be displayed again. Save this key for
future use.
```

3단계**:** 클라이언트 설정

다양한 S3 클라이언트를 사용할 수 있습니다. AWS CLI를 사용하는 것이 좋은 시작점입니다. 자세한 내용은 "AWS CLI 설치"을 참조하십시오.

FlexCache 볼륨 관리

ONTAP FlexCache 볼륨 감사에 대해 자세히 알아보십시오

ONTAP 9.7부터는 기본 ONTAP 감사 및 FPolicy를 사용한 파일 정책 관리를 통해 FlexCache 관계에서 NFS 파일 액세스 이벤트를 감사할 수 있습니다.

ONTAP 9.14.1부터 NFS 또는 SMB가 있는 FlexCache 볼륨에 대해 FPolicy가 지원됩니다. 이전에는 SMB가 있는 FlexCache 볼륨에 대해 FPolicy가 지원되지 않았습니다.

기본 감사 및 FPolicy는 FlexVol 볼륨에 사용되는 동일한 CLI 명령으로 구성 및 관리됩니다. 그러나 FlexCache 볼륨에는 몇 가지 다른 동작이 있습니다.

- * 기본 감사 *
  - FlexCache 볼륨을 감사 로그의 대상으로 사용할 수 없습니다.
  - FlexCache 볼륨의 읽기 및 쓰기를 감사하려면 캐시 SVM과 원본 SVM 모두에 대해 감사를 구성해야 합니다.

    이는 파일 시스템 작업이 처리되는 곳에서 감사되기 때문입니다. 즉, 캐시 SVM에서 읽기를 감사하고 원본 SVM에서 쓰기를 감사합니다.

  - 쓰기 작업의 출처를 추적하기 위해 SVM UUID 및 MSID가 감사 로그에 추가되어 쓰기 작업이 시작된 FlexCache 볼륨을 식별합니다.
- FPolicy * 를 사용합니다
  - FlexCache 볼륨에 대한 쓰기가 원본 볼륨에서 커밋되더라도 FPolicy 구성은 캐시 볼륨의 쓰기를 모니터링합니다. 이는 원본 볼륨에서 쓰기를 감사하는 네이티브 감사와는 다릅니다.
  - ONTAP는 캐시 및 원본 SVM에 동일한 FPolicy 구성을 요구하지 않지만, 유사한 구성을 두 개 구축하는 것이 좋습니다. 원래 SVM과 같이 구성된 캐시에 대한 새로운 FPolicy 정책을 생성하지만, 새 정책 범위는 캐시 SVM으로 제한됩니다.
  - FPolicy 구성의 확장 크기는 20KB(20480바이트)로 제한됩니다. FlexCache 볼륨에서 FPolicy 구성에 사용되는 확장의 크기가 20KB를 초과하면 EMS 메시지가 `nblade.fpolicy.extn.failed` 트리거됩니다.

원본 볼륨의 **ONTAP FlexCache** 볼륨 속성을 동기화합니다

FlexCache 볼륨의 일부 볼륨 속성은 항상 원본 볼륨의 볼륨 속성과 동기화되어야 합니다. 원본 볼륨에서 속성이 수정된 후 FlexCache 볼륨의 볼륨 속성이 자동으로 동기화되지 않으면 속성을 수동으로 동기화할 수 있습니다.

이 작업에 대해

FlexCache 볼륨의 다음 볼륨 속성은 항상 원본 볼륨의 볼륨 속성과 동기화되어야 합니다.

- 보안 스타일('-security-style')
- 볼륨 이름('-volume-name')
- 최대 디렉토리 크기("-maxdir-size")
- 최소 미리 읽기('-min-readahead')

단계

1. FlexCache 볼륨에서 볼륨 속성을 동기화합니다.

   'volume FlexCache sync-properties-vserver svm_name-volume flexcache_volume

```
cluster1::> volume flexcache sync-properties -vserver vs1 -volume fc1
```

ONTAP FlexCache 관계 구성을 업데이트합니다

볼륨 이동, 애그리게이트 재배치 또는 스토리지 페일오버와 같은 이벤트가 발생하면 원래 볼륨 및 FlexCache 볼륨의 볼륨 구성 정보가 자동으로 업데이트됩니다. 자동 업데이트가 실패하는 경우 EMS 메시지가 생성되어 FlexCache 관계에 대한 구성을 수동으로 업데이트해야 합니다.

원본 볼륨과 FlexCache 볼륨이 연결 해제 모드에 있는 경우 FlexCache 관계를 수동으로 업데이트하려면 몇 가지 추가 작업을 수행해야 할 수 있습니다.

이 작업에 대해

FlexCache 볼륨의 구성을 업데이트하려면 원본 볼륨에서 명령을 실행해야 합니다. 원본 볼륨의 구성을 업데이트하려면 FlexCache 볼륨에서 명령을 실행해야 합니다.

단계

1. FlexCache 관계의 구성을 업데이트합니다.

   'volume FlexCache config-refresh-peer-vserver peer_svm-peer-volume peer_volume_to_update-peer-endpoint-type [origin|cache]'

ONTAP FlexCache 볼륨에서 파일 액세스 시간 업데이트를 활성화합니다

ONTAP 9.11.1부터 FlexCache 볼륨의 '-atime-update' 필드를 활성화하여 파일 액세스 시간 업데이트를 허용할 수 있습니다. 또한 '-atime-update-period' 속성을 사용하여 액세스 시간 업데이트 기간을 설정할 수 있습니다. '-atime-update-period' 속성은 액세스 시간 업데이트가 발생할 수 있는 빈도와 오리진 볼륨으로 전파될 수 있는 시기를 제어합니다.

개요

ONTAP는 읽기, READLINK 및 readdir을 사용하여 읽은 파일 및 디렉터리에 대한 액세스 시간 업데이트를 관리할 수 있는 "-atime-update"라는 볼륨 수준 필드를 제공합니다. aTime은 자주 액세스하지 않는 파일과 디렉토리의 데이터 수명 주기 결정에 사용됩니다. 자주 액세스하지 않는 파일은 결국 아카이브 스토리지로 마이그레이션되며 나중에 테이프로 이동하는 경우가 많습니다.

atime-update 필드는 기존 볼륨과 새로 생성된 FlexCache 볼륨에서 기본적으로 비활성화됩니다. 9.11.1 이전 버전의 ONTAP 릴리스에서 FlexCache 볼륨을 사용하는 경우 원본 볼륨에서 읽기 작업을 수행할 때 캐시가 불필요하게 제거되지 않도록 atime-update 필드를 비활성화해야 합니다. 그러나 대규모 FlexCache 캐시를 사용하는 경우 관리자는 특수한 도구를 사용하여 데이터를 관리하고 핫 데이터가 캐시에 남아 있고 콜드 데이터가 제거되도록 합니다. atime-update가 비활성화된 경우에는 이 기능을 사용할 수 없습니다. 그러나 ONTAP 9.11.1부터 `-atime-update-period`, 캐시된 데이터를 관리하는 데 필요한 도구를 사용하고 사용할 수 `-atime-update` 있습니다.

시작하기 전에

- 모든 FlexCache 볼륨에서 ONTAP 9.11.1 이상이 실행되고 있어야 합니다.
- 권한 모드를 사용해야 `advanced` 합니다.

이 작업에 대해

'-atime-update-period'를 86400초로 설정하면 파일에 대해 수행된 읽기 유사 작업의 수에 관계없이 24시간 간격으로 한 번 이상의 액세스 시간을 업데이트할 수 없습니다.

'-atime-update-period'를 0으로 설정하면 각 읽기 액세스에 대한 메시지가 오리진으로 전송됩니다. 그런 다음 오리진에서 각 FlexCache 볼륨에 atime이 오래되어 성능에 영향을 미친다는 정보를 제공합니다.

단계

1. 권한 모드를 다음과 같이 설정합니다. `advanced`

   세트 프리빌리지 고급

2. 파일 액세스 시간 업데이트를 활성화하고 업데이트 빈도를 설정합니다.

   ```
   volume modify -volume vol_name -vserver <SVM name> -atime-update true -atime
   -update-period <seconds>
   ```

   다음 예에서는 `-atime-update'를 활성화하고 '-atime-update-period'를 86400초 또는 24시간으로 설정합니다.

   ```
   c1: volume modify -volume origin1 vs1_c1 -atime-update true -atime
   -update-period 86400
   ```

3. '-atime-update'가 활성화되어 있는지 확인합니다.

   'volume show-volume_vol_name_-fields atime-update, atime-update-period'

   ```
   c1::*> volume show -volume cache1_origin1 -fields atime-update,atime-
   update-period
   vserver volume         atime-update atime-update-period
   ------- -------------- ------------ -------------------
   vs2_c1  cache1_origin1 true         86400
   ```

4. 이 설정된 후에는 `-atime-update` FlexCache 볼륨의 파일을 자동으로 스크러빙할 수 있는지 여부와 스크러빙 간격을 지정할 수 있습니다.

   ```
   volume flexcache config modify -vserver <SVM name> -volume <volume_name> -is
   -atime-scrub-enabled <true|false> -atime-scrub-period <integer>
   ```

매개 변수에 대한 자세한 `-is-atime-scrub-enabled` 내용은 "ONTAP 명령 참조입니다"를 참조하십시오.

ONTAP FlexCache 볼륨에 대한 글로벌 파일 잠금을 사용합니다

ONTAP 9.10.1부터 전역 파일 잠금을 적용하여 모든 관련 캐시 파일에 대한 읽기를 방지할 수 있습니다.

글로벌 파일 잠금을 사용하면 모든 FlexCache 볼륨이 온라인 상태가 될 때까지 원본 볼륨의 수정 사항이 일시 중단됩니다. FlexCache 볼륨이 오프라인 상태일 때 일시 중지 및 수정 시간 초과로 인해 캐시와 원본 간 연결의 안정성을 제어할 수 있는 경우에만 전역 파일 잠금을 활성화해야 합니다.

시작하기 전에

- 글로벌 파일 잠금에서는 오리진이 포함된 클러스터와 모든 연결된 캐시에서 ONTAP 9.9.1 이상을 실행해야 합니다.

글로벌 파일 잠금은 새 FlexCache 볼륨 또는 기존 볼륨에 대해 활성화할 수 있습니다. 명령은 하나의 볼륨에서 실행할 수 있으며 모든 관련 FlexCache 볼륨에 적용됩니다.

- 전역 파일 잠금을 설정하려면 고급 권한 수준이어야 합니다.
- 9.9.1 이전 버전의 ONTAP로 되돌리는 경우 원본 및 연결된 캐시에서 글로벌 파일 잠금을 먼저 해제해야 합니다. 비활성화하려면 원본 볼륨에서 다음을 실행합니다. `volume flexcache prepare-to-downgrade -disable-feature-set 9.10.0`
- 글로벌 파일 잠금을 설정하는 프로세스는 오리진에 기존 캐시가 있는지 여부에 따라 달라집니다.
  - [enable-gfl-new]
  - [enable-gfl-existing]

새 **FlexCache** 볼륨에서 글로벌 파일 잠금을 설정합니다

단계

1. TRUE로 설정된 '-is-global-file-locking'으로 FlexCache 볼륨 생성:

   'Volume FlexCache create volume_volume_name_-is-global-file-locking-enabled true

   > 기본값은 '-is-global-file-locking'입니다. 이후에 볼륨에 대해 볼륨 FlexCache 생성 명령을 실행할 때는 "true'로 설정된 '-is-global-file-locking enabled'로 전달해야 합니다.

기존 **FlexCache** 볼륨에서 글로벌 파일 잠금을 설정합니다

단계

1. 글로벌 파일 잠금은 원본 볼륨에서 설정해야 합니다.
2. 오리진에는 다른 기존 관계(예: SnapMirror)를 포함할 수 없습니다. 기존의 모든 관계는 분리되어야 합니다. 명령을 실행할 때 모든 캐시 및 볼륨이 연결되어 있어야 합니다. 연결 상태를 확인하려면 다음을 실행합니다.

   볼륨 FlexCache 연결 상태 표시

   나열된 모든 볼륨의 상태는 로 표시되어야 합니다 `connected`. 자세한 내용은 을 참조하십시오 "FlexCache 관계의 상태를 봅니다" 또는 "원점에서 FlexCache 볼륨의 속성을 동기화합니다".

3. 캐시에 글로벌 파일 잠금 설정:

   'volume FlexCache origin config show/modify -volume_volume_name_-is-global-file-locking-enabled true

관련 정보

- "ONTAP 명령 참조입니다"

ONTAP FlexCache 볼륨을 미리 채웁니다

FlexCache 볼륨을 미리 채워 캐시된 데이터에 액세스하는 데 걸리는 시간을 줄일 수 있습니다.

시작하기 전에

- 고급 권한 레벨의 클러스터 관리자여야 합니다
- Prepopulation에 대해 전달하는 경로가 존재해야 하거나 미리 채우기 작업이 실패합니다.

이 작업에 대해

- 미리 채우기는 파일만을 읽고 디렉토리를 통과합니다
- 를 클릭합니다 `-isRecursion` Flag 미리 채우기에 전달된 전체 디렉터리 목록에 적용됩니다

단계

1. FlexCache 볼륨을 미리 채웁니다.

   ```
   volume flexcache prepopulate -cache-vserver vserver_name -cache-volume -path
   -list path_list -isRecursion true|false
   ```

   - 를 클릭합니다 `-path-list` 매개 변수는 원래 루트 디렉터리부터 시작하여 미리 채울 상대 디렉터리 경로를 나타냅니다. 예를 들어, 오리진 루트 디렉토리의 이름이 /origin이고 디렉토리 /origin/dir1 및 /origin/dir2가 포함된 경우 다음과 같이 경로 목록을 지정할 수 있습니다. `-path-list dir1, dir2` 또는 `-path-list /dir1, /dir2`.
   - 의 기본값입니다 `-isRecursion` 매개 변수는 True입니다.

     이 예에서는 단일 디렉토리 경로를 미리 채웁니다.

     ```
     cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
     -volume fg_cachevol_1 -path-list /dir1
       (volume flexcache prepopulate start)
     [JobId 207]: FlexCache prepopulate job queued.
     ```

     다음 예제에서는 여러 디렉터리의 파일을 미리 채웁니다.

     ```
     cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
     -volume fg_cachevol_1 -path-list /dir1,/dir2,/dir3,/dir4
       (volume flexcache prepopulate start)
     [JobId 208]: FlexCache prepopulate job queued.
     ```

     다음 예제에서는 단일 파일을 미리 채웁니다.

     ```
     cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
     -volume fg_cachevol_1 -path-list /dir1/file1.txt
       (volume flexcache prepopulate start)
     [JobId 209]: FlexCache prepopulate job queued.
     ```

     이 예제에서는 오리진에서 가져온 모든 파일을 미리 채웁니다.

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list / -isRecursion true
  (volume flexcache prepopulate start)
[JobId 210]: FlexCache prepopulate job queued.
```

이 예제에는 선행 모집단의 잘못된 경로가 포함되어 있습니다.

```
cluster1::*> flexcache prepopulate start -cache-volume
vol_cache2_vs3_c2_vol_origin1_vs1_c1 -cache-vserver vs3_c2 -path-list
/dir1, dir5, dir6
  (volume flexcache prepopulate start)

Error: command failed: Path(s) "dir5, dir6" does not exist in origin
volume
       "vol_origin1_vs1_c1" in Vserver "vs1_c1".
```

2. 읽은 파일 수 표시:

   job show-id job_ID-ins를 선택합니다

관련 정보

- "작업 표시"

ONTAP FlexCache 관계 삭제

더 이상 FlexCache 볼륨이 필요하지 않은 경우 FlexCache 관계 및 FlexCache 볼륨을 삭제할 수 있습니다.

시작하기 전에

FlexCache 쓰기 되돌림 기능이 활성화된 경우 FlexCache 볼륨을 삭제하기 전에 먼저 해당 기능을 비활성화해야 합니다. "FlexCache 볼륨에서 write-back을 비활성화합니다"을 참조하십시오.

단계

1. FlexCache 볼륨이 있는 클러스터에서 FlexCache 볼륨을 오프라인으로 설정합니다.

   'volume offline-vserver svm_name-volume volume volume_name'

2. FlexCache 볼륨을 삭제합니다.

   '볼륨 FlexCache 삭제 - vserver svm_name - volume volume volume_name'

   FlexCache 관계 세부 정보가 원본 볼륨 및 FlexCache 볼륨에서 제거됩니다.

핫스팟 교정을 위한 **FlexCache**

ONTAP FlexCache 볼륨으로 고성능 컴퓨팅 워크로드의 핫 스팟 해결

애니메이션 렌더링 또는 EDA와 같은 여러 고성능 컴퓨팅 워크로드에서 흔히 발생하는 문제는 주목을 받고 있습니다. 핫스팟팅은 클러스터 또는 네트워크의 특정 부분이 다른 영역에 비해 상당한 부하를 경험하여 해당 위치에 집중된 과도한 데이터 트래픽으로 인해 성능 병목 현상이 발생하고 전반적인 효율성이 감소되는 상황을 말합니다. 예를 들어, 파일 또는 여러 파일이 실행 중인 작업에 대한 수요가 많아 해당 파일에 대한 요청을 처리하는 데 사용되는 CPU에 병목 현상이 발생합니다(볼륨 선호도를 통해). FlexCache는 이 병목 현상을 완화할 수 있지만 올바르게 설정해야 합니다.

이 문서에서는 핫 스팟팅을 개선하기 위해 FlexCache를 설정하는 방법에 대해 설명합니다.

> 2024년 7월부터 이전에 PDF로 게시된 기술 보고서의 콘텐츠가 ONTAP 제품 문서와 통합되었습니다. 이 ONTAP 핫스팟 개선 기술 보고서 내용은 발행일 현재 완전히 새로 작성되었으며 이전 형식은 아직 작성되지 않았습니다.

주요 개념

핫스팟 개선 계획을 세울 때는 이러한 필수 개념을 이해하는 것이 중요합니다.

- * 고밀도 FlexCache(HDF) *: 캐시 용량 요구 사항이 허용하는 한 몇 개의 노드로 확장되도록 압축된 FlexCache
- * HDF Array(HDFA) *: 클러스터 전체에 분산된 동일한 오리진의 캐시인 HDFS 그룹입니다
- * SVM 간 HDFA *: 서버 가상 머신(SVM)당 HDFA의 HDF 1개
- * 내부 SVM HDFA *: HDFA의 모든 HDFS가 하나의 SVM에 있음
- * 동서 트래픽 *: 클러스터 백엔드 트래픽은 간접 데이터 액세스로부터 생성됩니다

다음 단계

- "고밀도 FlexCache를 사용하여 핫 스팟을 개선하는 방법을 이해합니다"
- "FlexCache 어레이 밀도를 결정합니다"
- "HDFS의 밀도를 결정하고 SVM 간 HDFA 및 SVM 내 HDFA와 함께 NFS를 사용하여 HDFS에 액세스할지 여부를 결정합니다"
- "HDFA 및 데이터 LIF를 구성하여 ONTAP 구성에서 클러스터 내 캐싱을 사용할 경우의 이점을 실현하십시오"
- "클라이언트 구성을 사용하여 ONTAP NAS 연결을 분산하도록 클라이언트를 구성하는 방법에 대해 알아봅니다"

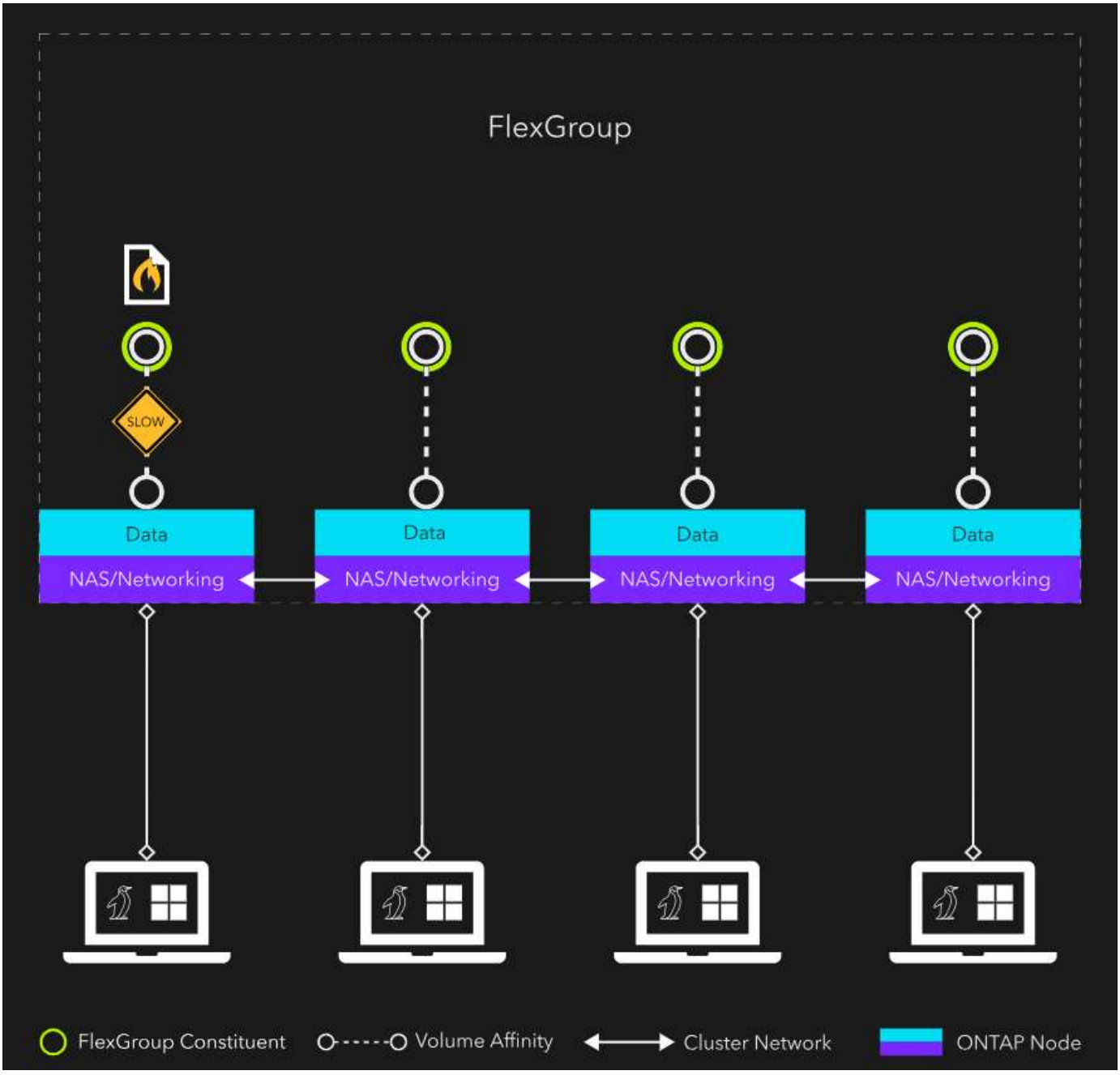
ONTAP FlexCache 핫스팟 개선 솔루션 설계

핫스팟을 해결하려면 병목 현상의 근본 원인, 자동 프로비저닝 FlexCache가 충분하지 않은 이유, FlexCache 솔루션을 효과적으로 설계하는 데 필요한 기술 세부 사항을 살펴봅니다. 고밀도 FlexCache 스토리지(HDFA)를 이해하고 구현하면 성능을 최적화하고 수요가 많은 작업 부하에서 병목 현상을 제거할 수 있습니다.

다음은 이미지일반적인 단일 파일 핫 스팟팅 시나리오를 보여 줍니다. 이 볼륨은 노드당 단일 구성요소가 있는 FlexGroup이며 파일은 노드 1에 상주합니다.

모든 NAS 클라이언트의 네트워크 연결을 클러스터의 서로 다른 노드에 분산시키는 경우 핫 파일이 상주하는 볼륨 선호도를 지원하는 CPU의 병목 현상이 발생합니다. 또한 파일이 상주하는 위치가 아닌 노드에 연결된 클라이언트에서 수신되는 통화에 클러스터 네트워크 트래픽(동부-서부 트래픽)을 도입합니다. 동서부의 트래픽 오버헤드는 일반적으로 작지만 고성능 컴퓨팅 워크로드의 경우에는 비트 수가 거의 없습니다.

그림 **1: FlexGroup** 단일 파일 핫스팟 시나리오

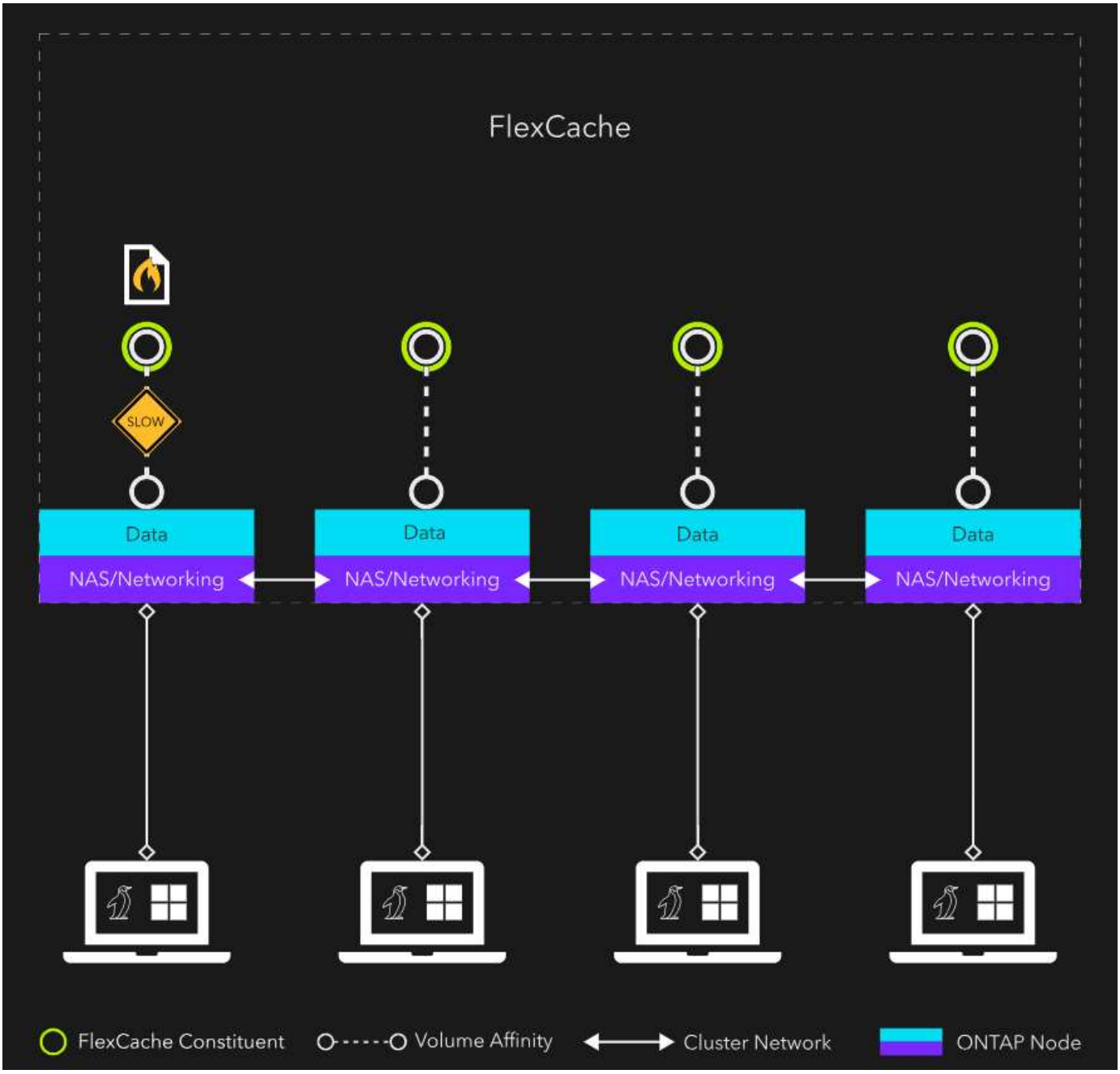


자동 프로비저닝된 **FlexCache**가 해답이 아닌 이유

핫스팟을 해결하려면 CPU 병목 현상을 제거하고 동서 트래픽도 제거합니다. FlexCache가 제대로 설정되어 있으면 도움이 될 수 있습니다.

다음 예에서 FlexCache System Manager, NetApp Console 또는 기본 CLI 인수를 통해 자동으로 프로비저닝됩니다. 그림 1 그리고그림 2 처음에는 똑같아 보입니다. 둘 다 4노드, 단일 구성 NAS 컨테이너입니다. 유일한 차이점은 그림 1의 NAS 컨테이너가 FlexGroup 이고, 그림 2의 NAS 컨테이너가 FlexCache 라는 것입니다. 각 그림은 동일한 병목 현상을 보여줍니다. 즉, 핫 파일에 대한 액세스를 제공하는 볼륨 친화성을 위한 노드 1의 CPU와 지연 시간에 영향을 미치는 동서 트래픽입니다. 자동 프로비저닝된 FlexCache 병목 현상을 제거하지 못했습니다.

그림 **2:** 자동 프로비저닝 **FlexCache** 시나리오



FlexCache의 해부 구조

핫스팟 교정을 위한 FlexCache를 효과적으로 설계하려면 FlexCache에 대한 몇 가지 기술 세부 사항을 이해해야 합니다.

FlexCache는 항상 스파스 FlexGroup입니다. FlexGroup는 여러 개의 FlexVol으로 구성됩니다. 이러한 FlexVol을 FlexGroup 구성요소라고 합니다. 기본 FlexGroup 레이아웃의 경우, 클러스터의 노드당 구성요소가 하나 이상

있습니다. 구성 요소는 추상화 계층 아래에 "함께 결합"되어 단일 대형 NAS 컨테이너로 클라이언트에 제공됩니다. 파일이 FlexGroup에 기록되면 수집 휴리스틱에서 파일이 저장될 구성요소를 결정합니다. 클라이언트의 NAS 연결을 포함하는 구성요소이거나 다른 노드일 수 있습니다. 모든 것이 추상화 계층 아래에서 작동하고 클라이언트에게 보이지 않기 때문에 위치는 관련이 없습니다.

FlexGroup에 대한 이해도를 FlexCache에 적용해 보겠습니다. FlexCache는 FlexGroup을 기반으로 구축되기 때문에 에 설명된 대로 클러스터의 모든 노드에 대해 단일 FlexCache가 기본적으로 제공됩니다.그림 1 대부분의 경우 이것은 매우 유용합니다. 클러스터의 모든 리소스를 활용하고 있습니다.

하지만 핫 파일을 수정하는 경우에는 단일 파일 및 동서 트래픽의 CPU와 같은 두 가지 병목 현상 때문에 이 방법이 적합하지 않습니다. 핫 파일의 모든 노드에 구성 요소가 있는 FlexCache를 생성하는 경우 해당 파일은 여전히 구성요소 중 하나에 상주합니다. 즉, 핫 파일에 대한 모든 액세스를 서비스하는 CPU가 하나 있습니다. 또한 핫 파일에 도달하는 데 필요한 동서 트래픽의 양을 제한해야 합니다.

이 솔루션은 고밀도 FlexCaches의 어레이입니다.

고밀도 **FlexCache**의 해부 구조

고집적 HDF(FlexCache)는 캐시된 데이터의 용량 요구 사항이 허용하는 만큼 소수의 노드에 구성 요소가 있습니다. 목표는 단일 노드에서 캐시를 활성화하는 것입니다. 용량 요구사항에 따라 그렇게 할 수 없는 경우 몇 개의 노드에만 구성요소를 사용할 수 있습니다.

예를 들어, 24노드 클러스터에는 3개의 고밀도 FlexCh가 있을 수 있습니다.

- 노드 1에서 8까지 확장되는 경로입니다
- 노드 9에서 16까지 확장되는 초입니다
- 노드 17-24에 걸쳐 3분의 1을 제공합니다

이 세 개의 HDFS는 하나의 HDFA(High-Density FlexCache Array)를 구성합니다. 각 HDF 내에 파일이 균등하게 배포되면 클라이언트가 요청한 파일이 프런트엔드 NAS 접속에 로컬로 상주할 확률은 8%입니다. 각각 2개의 노드만 사용하는 12개의 HDFS를 사용하는 경우 파일이 로컬일 가능성이 50% 높습니다. HDF를 단일 노드로 축소하여 24개 노드로 만들 수 있다면 파일이 로컬임을 보증할 수 있습니다.

이 구성은 모든 동서 트래픽을 제거하며 가장 중요한 것은 핫 파일에 액세스하기 위한 24개의 CPU/볼륨 선호도를 제공합니다.

다음 단계

"FlexCache 어레이 밀도를 결정합니다"

관련 정보

"FlexGroup 및 TR에 대한 설명서"

ONTAP FlexCache 밀도 결정

첫 번째 핫스팟 개선 설계 결정은 FlexCache 밀도를 파악하는 것입니다. 다음 예는 4노드 클러스터입니다. 파일 수가 각 HDF의 모든 구성 요소에 균등하게 분포되어 있다고 가정합니다. 또한 모든 노드에 걸쳐 프런트엔드 NAS 연결이 고르게 분포되어 있다고 가정합니다.

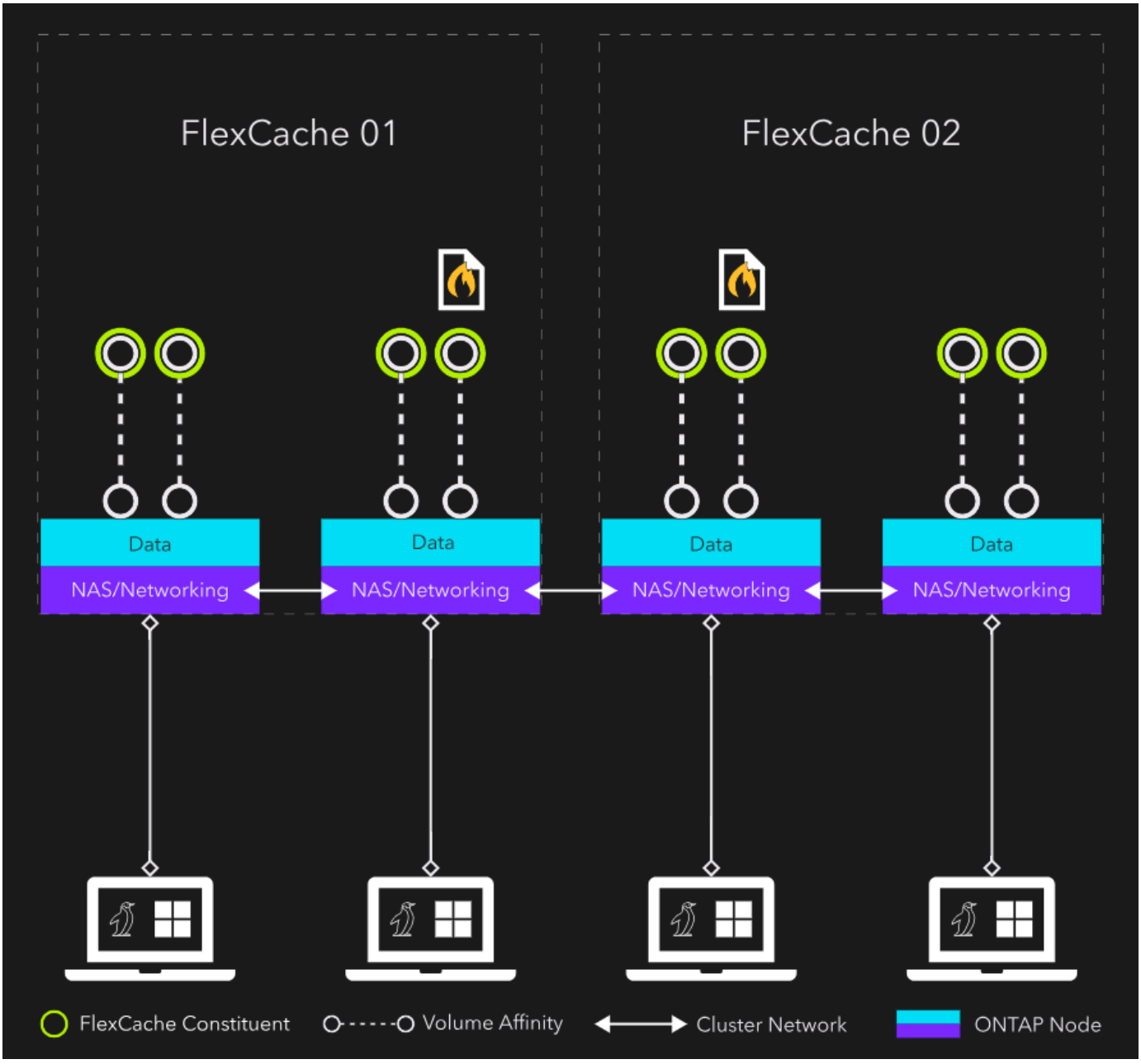
이러한 예만 사용할 수 있는 구성은 아니지만 공간 요구 사항과 사용 가능한 리소스가 허용하는 한 많은 HDFS를 만드는 기본 설계 원칙을 이해해야 합니다.

HDFA는 다음 구문을 사용하여 표현됩니다. `HDFs per HDFA x nodes per HDF x constituents per node per HDF`

2x2x2 HDFA 구성

그림 1 은 2x2x2x2 HDFA 구성의 예입니다. 두 개의 HDFS, 각각 두 개의 노드를 스패닝하고 각 노드는 두 개의 구성 볼륨을 포함합니다. 이 예에서 각 클라이언트는 핫 파일에 직접 액세스할 확률이 50%입니다. 네 고객 중 두 명은 동서 트래픽을 가지고 있습니다. 중요한 것은 이제 두 개의 HDFS가 존재한다는 것입니다. 즉, 핫 파일의 두 가지 캐시를 의미합니다. 현재 핫 파일에 대한 액세스를 처리하는 CPU/볼륨 선호도가 2개 있습니다.

그림 **1: 2x2x2 HDFA** 구성

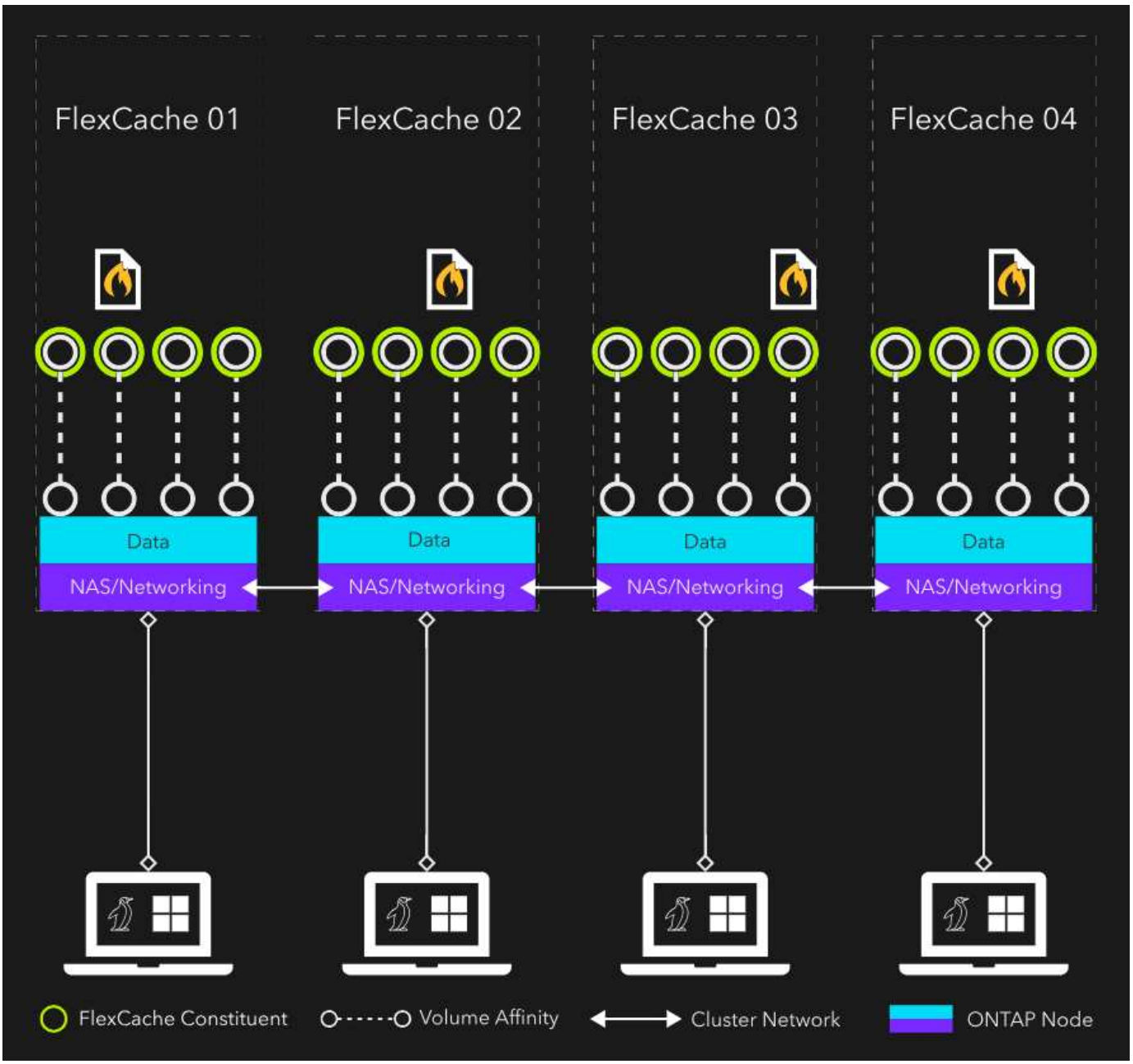


4x1x4 HDFA 구성

그림 2 최적의 구성을 나타냅니다. 4x1x4 HDFA 구성의 한 예로 4개의 HDFS가 단일 노드에 포함되고 각 노드는 4개의 구성 요소를 포함합니다. 이 예에서는 각 클라이언트가 핫 파일의 캐시에 직접 액세스할 수 있도록 보장합니다. 4개의

다른 노드에 4개의 캐시된 파일이 있으므로 4개의 서로 다른 CPU/볼륨 선호도가 핫 파일에 대한 서비스 액세스를 지원합니다. 또한 동서 트래픽이 생성되지 않습니다.

그림 **2: 4x1x4 HDFA** 구성



다음 단계

HDFS의 집적도를 결정한 후 NFS를 사용하여 HDFS에 액세스할 경우 다른 설계 결정을 내려야 "SVM 간 HDFA 및 SVM 내 HDFA"합니다.

ONTAP SVM 간 또는 **SVM** 내 **HDFA** 옵션을 결정합니다

HDFS의 밀도를 확인한 후 NFS를 사용하여 HDFS에 액세스할지 여부를 결정하고 SVM 간 HDFA 및 SVM 내 HDFA 옵션에 대해 알아봅니다.

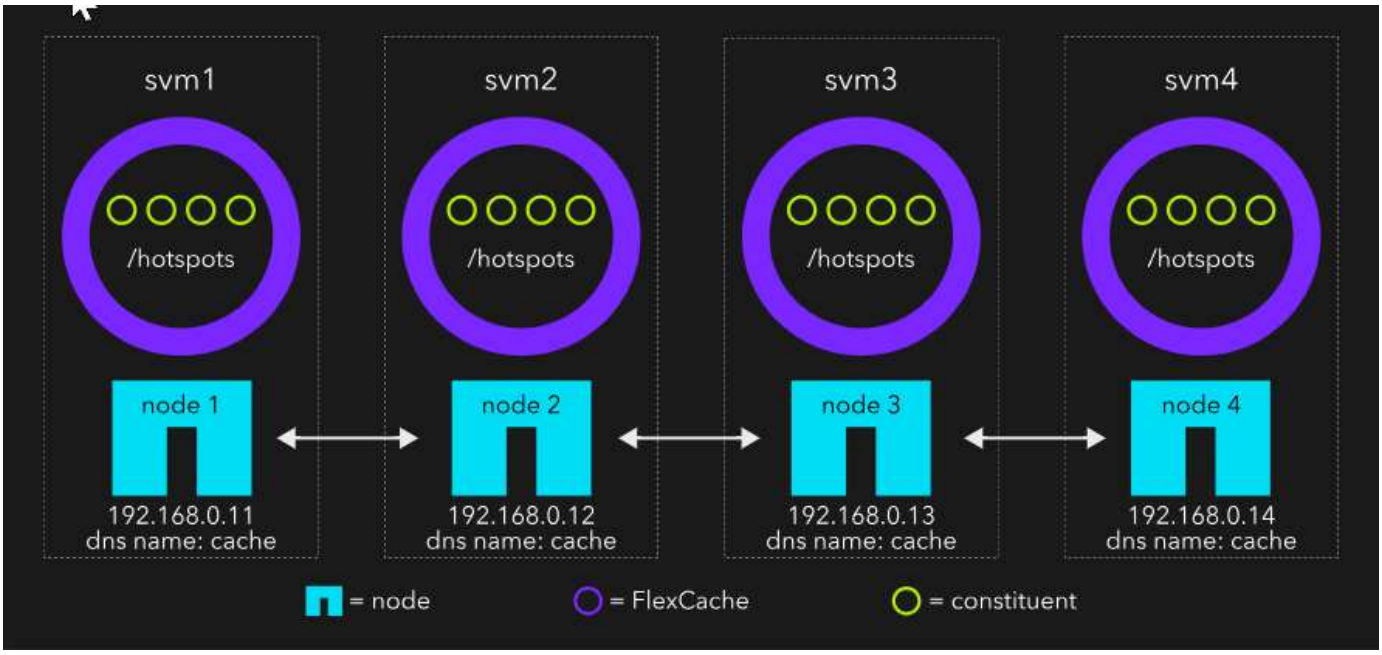
SMB 클라이언트만 HDFS에 액세스하는 경우 모든 HDFS를 단일 SVM에 생성해야 합니다. DFS 대상을 로드 밸런싱에 사용하는 방법은 Windows 클라이언트 구성을 참조하십시오.

SVM 간 HDFA 구축

SVM 간 HDFA는 HDFA의 각 HDF에 대해 SVM을 생성해야 합니다. 따라서 HDFA 내의 모든 HDFS가 동일한 접합 경로를 갖게 되므로 클라이언트 측에서 보다 쉽게 구성할 수 있습니다.

이 그림 1 예에서 각 HDF는 자체 SVM에 있습니다. 이는 SVM 간 HDFA 구축입니다. 각 HDF에는 /핫스팟의 접합 경로가 있습니다. 또한 모든 IP에는 호스트 이름 캐시의 DNS A 레코드가 있습니다. 이 구성은 DNS 라운드 로빈을 활용하여 다양한 HDFS에 대한 로드 밸런싱 마운트를 수행합니다.

그림 **1: 4x1x4 SVM** 간 **HDFA** 구성

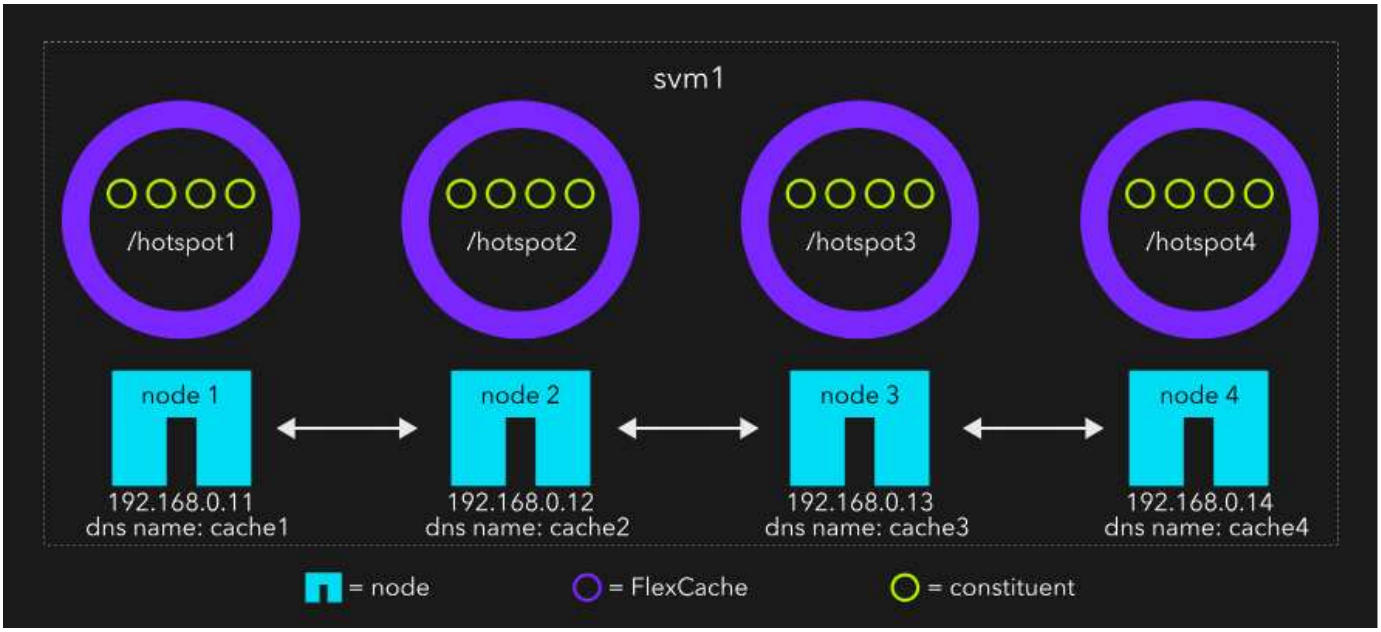


SVM HDFA 내부 구축

SVM 내부의 경우 각 HDF에 고유한 접합 경로가 필요하지만 모든 HDFS는 하나의 SVM에 있습니다. ONTAP에서는 하나의 SVM만 필요하기 때문에 이 설정은 더 쉬울 수 있지만 Linux 측면에서는 고급 구성이 필요하며 ONTAP에 데이터 LIF가 배치되어야 `autofs` 합니다.

이 그림 2 예에서 모든 HDF는 동일한 SVM에 있습니다. 이는 SVM 내 HDFA 구축이며 접합 경로가 고유해야 합니다. 로드 밸런싱이 제대로 작동하려면 각 IP에 대해 고유한 DNS 이름을 생성하고 호스트 이름이 확인되는 데이터 LIF를 HDF가 상주하는 노드에만 배치해야 합니다. 또한 에서 설명한 대로 여러 항목으로 를 구성해야 `autofs`"Linux 클라이언트 구성" 합니다.

그림 **2: 4x1x4** 내부 **SVM HDFA** 구성



다음 단계

이제 HDFA를 구축하는 방법에 대해 알아보았습니다."HDFA를 배포하고 클라이언트가 분산 방식으로 액세스할 수 있도록 구성합니다"

HDFA 및 **ONTAP** 데이터 **LIF**를 구성합니다

이 핫스팟 교정 솔루션의 이점을 실현하려면 HDFA 및 데이터 LIF를 적절히 구성해야 합니다. 이 솔루션은 동일한 클러스터에서 오리진 및 HDFA와 함께 클러스터 내 캐싱을 사용합니다.

다음은 두 가지 HDFA 샘플 구성입니다.

- 2x2x2 SVM 간 HDFA
- 4x1x4 내부 SVM HDFA

이 작업에 대해

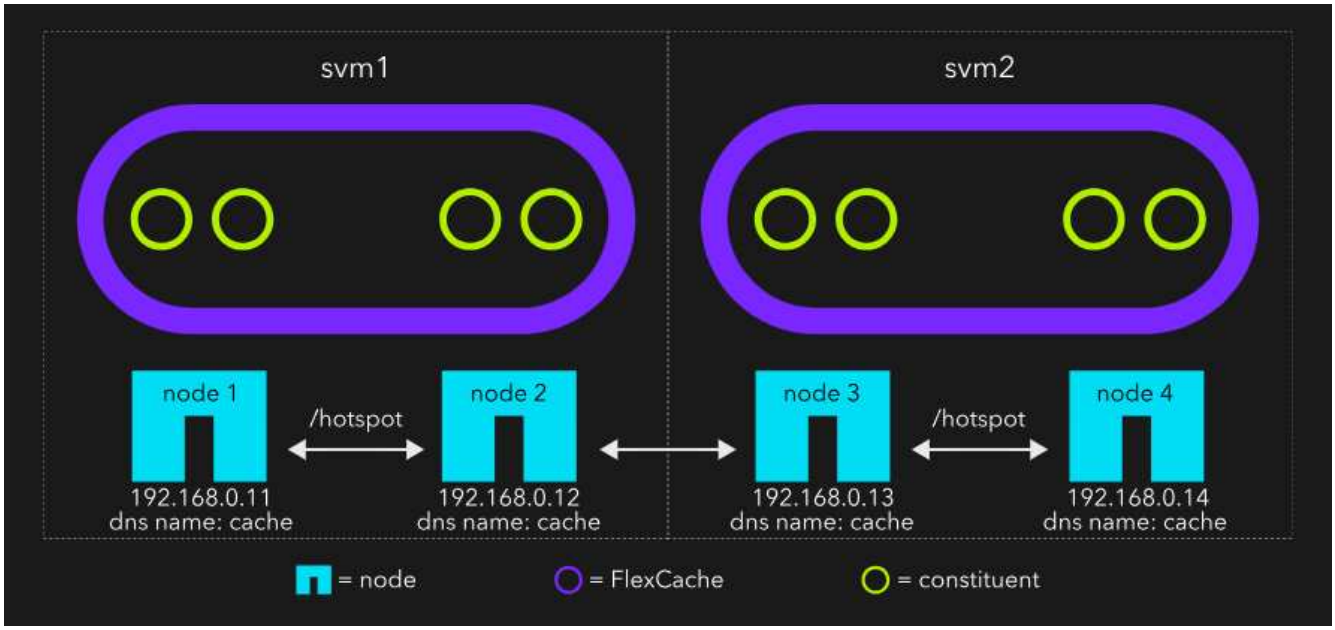
ONTAP CLI를 사용하여 이 고급 구성을 수행합니다. 명령에서 두 가지 구성을 사용해야 `flexcache create` 하며 한 가지 구성을 구성하지 않도록 해야 합니다.

- `-aggr-list`: HDF를 제한하려는 노드의 노드 또는 하위 집합에 상주하는 애그리게이트 또는 애그리게이트 목록을 제공합니다.
- `-aggr-list-multiplier`: 옵션에 나열된 애그리게이트당 생성할 구성 요소의 수를 `aggr-list` 결정합니다. 두 개의 애그리게이트가 나열되고 이 값을 로 설정하면 `2` 4개의 구성요소가 됩니다. NetApp에서는 애그리게이트당 최대 8개의 구성요소를 사용할 것을 권장하지만 16개로도 충분합니다.
- `-auto-provision-as`: 탭 아웃 경우, CLI는 자동 채우기를 시도하고 값을 로 `flexgroup`설정합니다. 이 설정이 구성되어 있지 않은지 확인합니다. 이 메시지가 나타나면 삭제합니다.

2x2x2 Inter-SVM HDFA 구성을 생성합니다

1. 그림 1과 같이 2x2x2x2 SVM 간 HDFA 구성을 지원하려면 준비 시트를 작성합니다.

   그림 **1: 2x2x2 Inter-SVM HDFA** 레이아웃



SVM	HDF당 노드 수	애그리게이트	노드당 구성 요소	접합 경로	데이터 LIF IP
svm1를 참조하십시오	node1, node2	aggr1, aggr2	2	/핫스팟	192.168.0.11,192.168.0.12
svm2를 참조하십시오	node3, node4	aggr3, aggr4	2	/핫스팟	192.168.0.13,192.168.0.14

2. HDFS를 생성합니다. 준비 시트의 각 행에 대해 다음 명령을 두 번 실행합니다. 두 번째 반복의 및 `aggr-list` 값을 조정해야 `vserver` 합니다.

```
cache::> flexcache create -vserver svm1 -volume hotspot -aggr-list
aggr1,aggr2 -aggr-list-multiplier 2 -origin-volume <origin_vol> -origin
-vserver <origin_svm> -size <size> -junction-path /hotspot
```

3. 데이터 LIF를 생성합니다. 명령을 4회 실행하여 준비 시트에 나열된 노드에서 SVM당 데이터 LIF 두 개를 생성합니다. 각 반복에 맞게 값을 적절히 조정해야 합니다.

```
cache::> net int create -vserver svm1 -home-port e0a -home-node node1
-address 192.168.0.11 -netmask-length 24
```

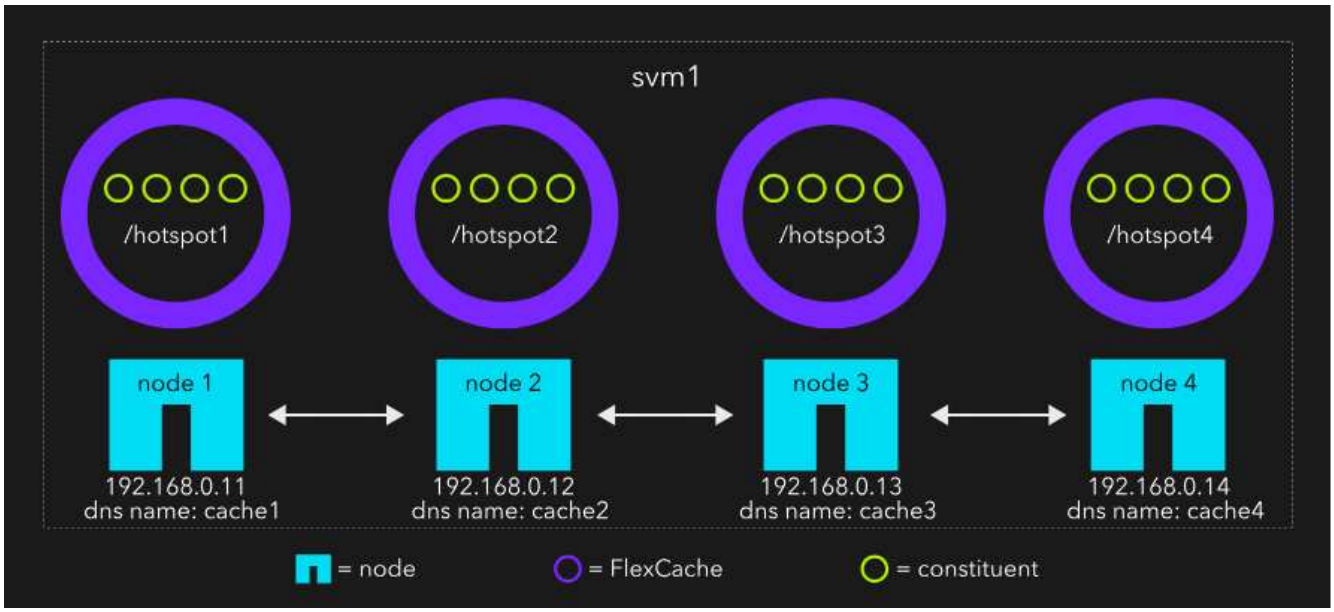
다음 단계

이제 HDFA를 적절히 활용할 수 있도록 클라이언트를 구성해야 합니다. 을 "클라이언트 구성"참조하십시오.

4x1x4 내부 SVM HDFA를 생성합니다

1. 그림 2와 같이 4x1x4 SVM 간 HDFA 구성을 지원하려면 준비 시트를 작성합니다.

그림 **2: 4x1x4** 내부 **SVM HDFA** 레이아웃



SVM	HDF당 노드 수	애그리게이트	노드당 구성 요소	접합 경로	데이터 LIF IP
svm1를 참조하십시오	노드1	aggr1를 참조하십시오	4	/hotspot1 을 참조하십시오	192.168.0.11
svm1를 참조하십시오	노드2	aggr2를 참조하십시오	4	/hotspot2 를 참조하십시오	192.168.0.12
svm1를 참조하십시오	node3를 참조하십시오	aggr3를 참조하십시오	4	/hotspot3 을 참조하십시오	192.168.0.13
svm1를 참조하십시오	node4를 참조하십시오	aggr4를 참조하십시오	4	/hotspot4 를 참조하십시오	192.168.0.14

2. HDFS를 생성합니다. 준비 시트의 각 행에 대해 다음 명령을 네 번 실행합니다. 각 반복에 대한 및 `junction-path` 값을 조정해야 `aggr-list` 합니다.

```
cache::> flexcache create -vserver svm1 -volume hotspot1 -aggr-list
aggr1 -aggr-list-multiplier 4 -origin-volume <origin_vol> -origin
-vserver <origin_svm> -size <size> -junction-path /hotspot1
```

3. 데이터 LIF를 생성합니다. 명령을 4회 실행하여 SVM에 총 4개의 데이터 LIF를 생성합니다. 노드당 데이터 LIF는 하나만 있어야 합니다. 각 반복에 맞게 값을 적절히 조정해야 합니다.

```
cache::> net int create -vserver svm1 -home-port e0a -home-node node1
-address 192.168.0.11 -netmask-length 24
```

다음 단계

이제 HDFA를 적절히 활용할 수 있도록 클라이언트를 구성해야 합니다. 을 "클라이언트 구성"참조하십시오.

ONTAP NAS 연결을 분산하도록 클라이언트를 구성합니다

핫스팟을 해결하려면 CPU 병목 현상을 방지하기 위해 클라이언트를 적절히 구성합니다.

Linux 클라이언트 구성

SVM 내 또는 SVM 간 HDFA 구축을 선택하든 Linux에서 를 사용하여 클라이언트가 서로 다른 HDFS 간에 로드 밸런싱을 수행할 수 있어야 `autofs` 합니다. `autofs`구성은 SVM 간 및 내부 SVM에 따라 다릅니다.

시작하기 전에

적절한 종속성이 설치되어 있어야 `autofs` 합니다. 이에 대한 자세한 내용은 Linux 설명서를 참조하십시오.

이 작업에 대해

설명된 단계에서는 다음 항목이 포함된 예제 `/etc/auto_master` 파일을 사용합니다.

```
/flexcache auto_hotspot
```

`autofs` `/etc`프로세스가 디렉터리에 액세스하려고 할 때마다 디렉터리에서 `/flexcache` 호출된 파일을 찾도록 `auto_hotspot` 구성합니다. 파일의 내용은 `auto_hotspot` 디렉토리 내에 마운트할 `NFS` 서버 및 접속 경로를 `/flexcache` 지정합니다. 설명된 예는 파일에 대한 서로 다른 `auto_hotspot` 설정입니다.

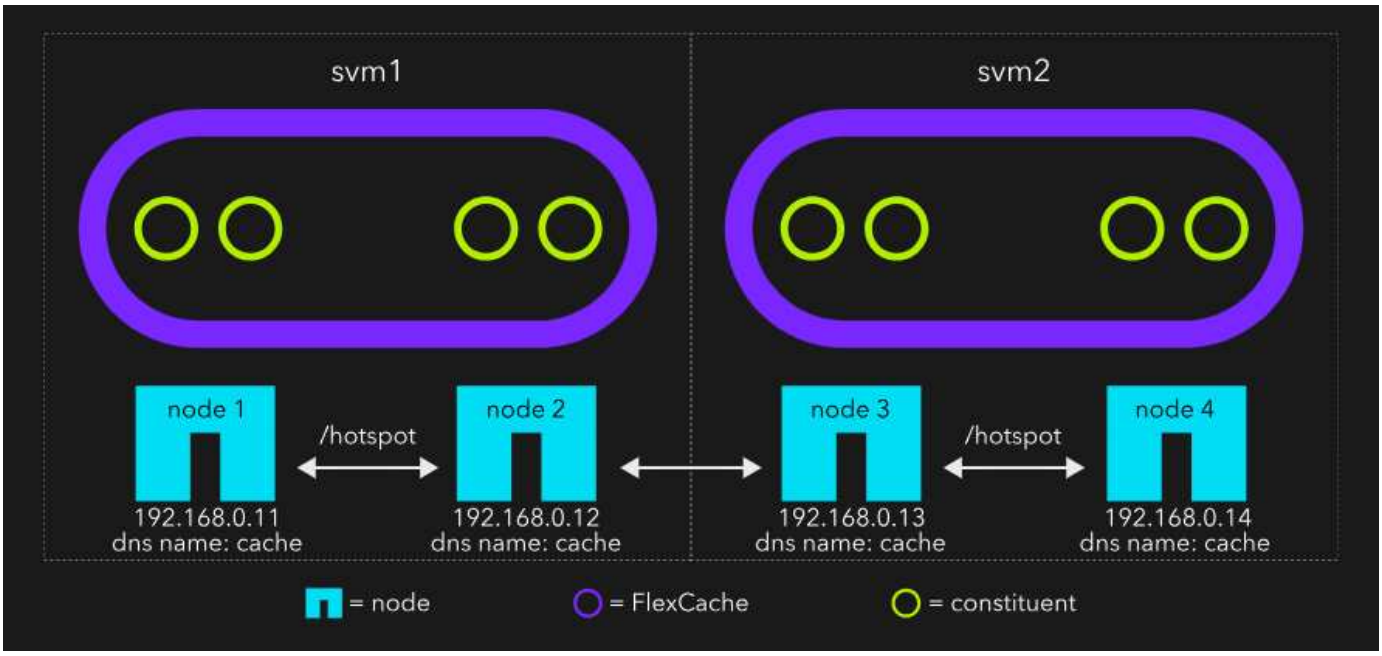
내부 **SVM HDFA** 자동 전송 구성

다음 예제에서는 의 다이어그램에 대한 지도를 만듭니다 `autofs`그림 1. 각 캐시에는 동일한 접합 경로가 있고 호스트 이름에 4개의 DNS A 레코드가 있으므로 `cache` 한 줄만 있으면 됩니다.

```
hotspot cache:/hotspot
```

이 간단한 한 줄은 NFS 클라이언트가 호스트 이름에 대한 DNS 조회를 `cache` 수행하도록 합니다. DNS가 라운드 로빈 방식으로 IP를 반환하도록 설정됩니다. 이렇게 하면 프런트엔드 NAS 연결이 고르게 분산됩니다. 클라이언트는 IP를 수신한 후 에서 `/flexcache/hotspot` 접합 경로를 마운트합니다 `/hotspot`. SVM1, SVM2, SVM3 또는 SVM4에 연결할 수 있지만 특정 SVM은 중요하지 않습니다.

그림 **1: 2x2x2 SVM** 간 **HDFA**



내부 **SVM HDFA** 자동 전송 구성

다음 예제에서는 의 다이어그램에 대한 지도를 만듭니다 `autofs`그림 2. NFS 클라이언트가 HDF 접합 경로 배포의 일부인 IP를 마운트해야 합니다. 즉, IP 192.168.0.11이 아닌 다른 것을 탑재하고 싶지 않습니다. `/hotspot1` 이를 위해 맵에서 하나의 로컬 마운트 위치에 대한 IP/접합 경로 쌍 4개를 모두 나열할 수 `auto_hotspot` 있습니다.

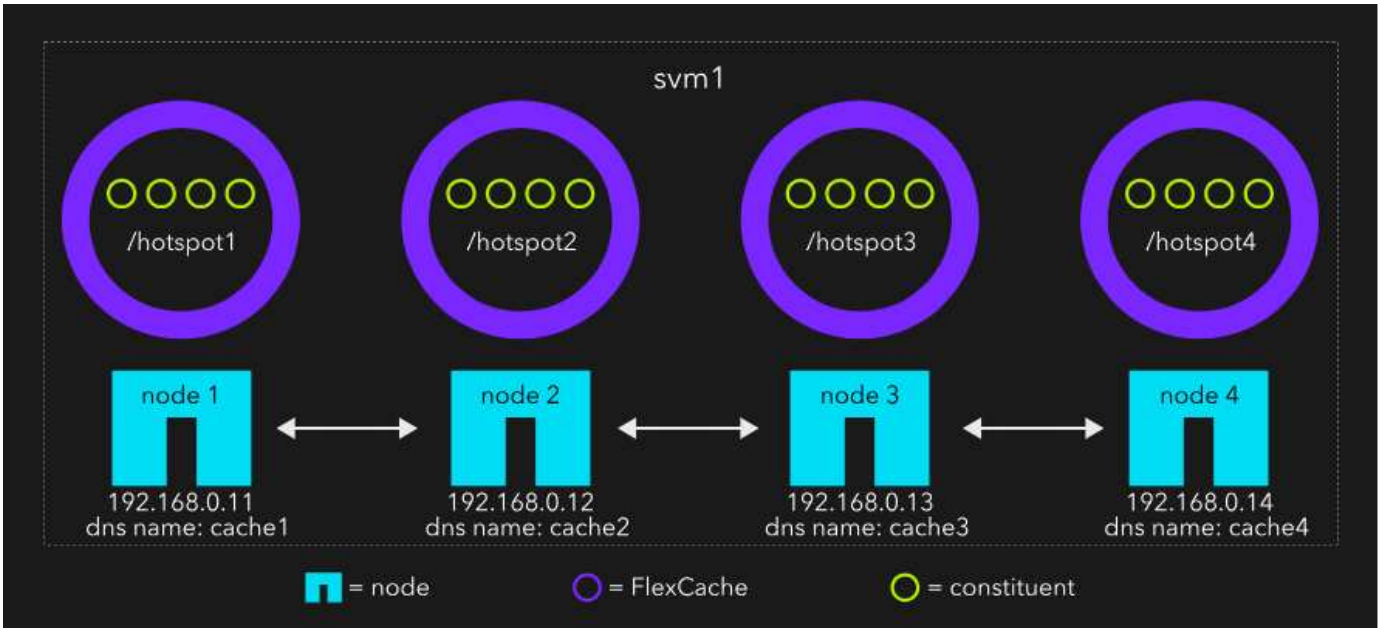
(`\`다음 예제의 백슬래시)는 항목을 다음 줄로 이어가며 읽기 쉽도록 합니다.

```
hotspot     cache1:/hostspot1 \
            cache2:/hostspot2 \
            cache3:/hostspot3 \
            cache4:/hostspot4
```

클라이언트가 액세스를 시도할 때 `/flexcache/hotspot` 은 `autofs` 네 개의 호스트 이름 모두에 대해 정방향 조회를 수행합니다. 4개의 IP가 모두 클라이언트와 동일한 서브넷에 있거나 다른 서브넷에 있다고 가정하면 는 `autofs` 각 IP에 대해 NFS NULL ping을 실행합니다.

이 NULL ping을 수행하려면 ONTAP의 NFS 서비스에서 패킷을 처리해야 하지만 디스크 액세스가 필요하지 않습니다. 반환할 첫 번째 ping은 마운트하도록 선택한 IP 및 접합 경로입니다. `autofs`

그림 **2: 4x1x4** 내부 **SVM HDFA**



Windows 클라이언트 구성

Windows 클라이언트에서는 내부 SVM HDFA를 사용해야 합니다. SVM의 여러 HDFS 간에 로드 밸런싱을 수행하려면 각 HDF에 고유한 공유 이름을 추가해야 합니다. 그런 다음 의 단계를 따라 "Microsoft 설명서"동일한 폴더에 대해 여러 DFS 대상을 구현합니다.

네트워크 관리

시작하십시오

System Manager를 사용하여 ONTAP 네트워크를 시각화합니다

ONTAP 9.8부터는 System Manager를 사용하여 네트워크의 구성 요소와 구성을 보여주는 그래픽을 표시할 수 있으며, 호스트, 포트, SVM, 볼륨 등에 걸친 네트워크 연결 경로를 볼 수 있습니다. ONTAP 9.12.1부터 네트워크 인터페이스 그리드에서 LIF 및 서브넷 연결을 볼 수 있습니다.

그래픽은 * 네트워크 > 개요 * 를 선택하거나 대시보드의 * 네트워크 * 섹션에서 선택하면 표시됩니다 → .

그림에 표시된 구성 요소는 다음과 같습니다.

- 호스트
- 스토리지 포트
- 네트워크 인터페이스
- 스토리지 VM
- 데이터 액세스 구성 요소

각 섹션에는 네트워크 관리 및 구성 작업을 수행하기 위해 마우스를 가져가거나 선택할 수 있는 추가 세부 정보가 표시됩니다.

기존 시스템 관리자(ONTAP 9 .7 이하 버전에서만 사용 가능)를 사용하는 경우 를 참조하십시오."네트워크 관리"

예

다음은 각 구성 요소에 대한 세부 정보를 보거나 네트워크를 관리하기 위한 작업을 시작하기 위해 그래픽과 상호 작용할 수 있는 여러 가지 방법의 예입니다.

- 포트, 네트워크 인터페이스, 스토리지 VM 및 연결된 데이터 액세스 구성 요소와 같은 해당 구성을 보려면 호스트를 클릭합니다.
- 스토리지 VM의 볼륨 수 위에 마우스 커서를 올려 놓으면 세부 정보를 볼 볼륨을 선택할 수 있습니다.
- 지난 주 동안의 성능을 보려면 iSCSI 인터페이스를 선택합니다.
- 구성 요소 옆에 있는 을 ⋮ 클릭하여 해당 구성 요소를 수정하는 작업을 시작합니다.
- 비정상적인 구성 요소 옆에 "X"가 표시되어 네트워크에서 문제가 발생할 수 있는 위치를 빠르게 확인할 수 있습니다.

System Manager 네트워크 시각화 비디오

ONTAP 클러스터의 네트워킹 구성 요소에 대해 알아봅니다

클러스터를 설정하기 전에 클러스터의 네트워킹 구성 요소를 숙지해야 합니다. 클러스터의 물리적 네트워킹 구성 요소를 논리적 구성 요소로 구성하면 ONTAP의 유연성과 멀티 테넌시 기능을 활용할 수 있습니다.

클러스터의 다양한 네트워킹 구성 요소는 다음과 같습니다.

- 물리적 포트

  네트워크 인터페이스 카드(NIC) 및 호스트 버스 어댑터(HBA)는 각 노드에서 물리적 네트워크(관리 및 데이터 네트워크)로의 물리적(이더넷 및 파이버 채널) 연결을 제공합니다.

  사이트 요구사항, 스위치 정보, 포트 케이블 연결 정보 및 컨트롤러 온보드 포트 케이블은 에서 Hardware Universe를 참조하십시오 "hwu.netapp.com".

- 논리 포트

  VLAN(Virtual Local Area Network) 및 인터페이스 그룹은 논리 포트를 구성합니다. 인터페이스 그룹은 여러 물리적 포트를 단일 포트로 취급하며 VLAN은 물리적 포트를 여러 개의 개별 포트로 세분화합니다.

- IPspace

  IPspace를 사용하여 클러스터의 각 SVM에 대해 별개의 IP 주소 공간을 생성할 수 있습니다. 이렇게 하면 관리자가 별도의 네트워크 도메인에 있는 클라이언트가 동일한 IP 주소 서브넷 범위의 중복 IP 주소를 사용하면서 클러스터 데이터에 액세스할 수 있습니다.

- 브로드캐스트 도메인

브로드캐스트 도메인은 IPspace에 상주하며 동일한 계층 2 네트워크에 속하는 클러스터 내의 여러 노드에서 잠재적으로 네트워크 포트 그룹을 포함합니다. 그룹의 포트는 SVM에서 데이터 트래픽을 위해 사용됩니다.

- 서브넷

  서브넷은 브로드캐스트 도메인 내에서 생성되며 동일한 계층 3 서브넷에 속하는 IP 주소 풀을 포함합니다. 이 IP 주소 풀은 LIF 생성 중에 IP 주소 할당을 간소화합니다.

- 논리 인터페이스

  논리 인터페이스(LIF)는 포트에 연결된 IP 주소 또는 WWPN(Worldwide Port Name)입니다. 페일오버 그룹, 페일오버 규칙 및 방화벽 규칙과 같은 속성과 연결됩니다. LIF는 현재 바인딩된 포트(물리적 또는 논리적)를 통해 네트워크를 통해 통신합니다.

  클러스터의 다양한 LIF 유형에는 데이터 LIF, 클러스터 범위 관리 LIF, 노드 범위 관리 LIF, 인터클러스터 LIF, 클러스터 LIF 등이 있습니다. LIF의 소유권은 LIF가 상주하는 SVM에 따라 다릅니다. 데이터 LIF는 데이터 SVM, 노드 범위 관리 LIF, 클러스터 범위 관리 LIF, 인터클러스터 LIF가 관리 SVM에서 소유하며 클러스터 LIF는 클러스터 SVM에서 소유합니다.

- DNS 영역

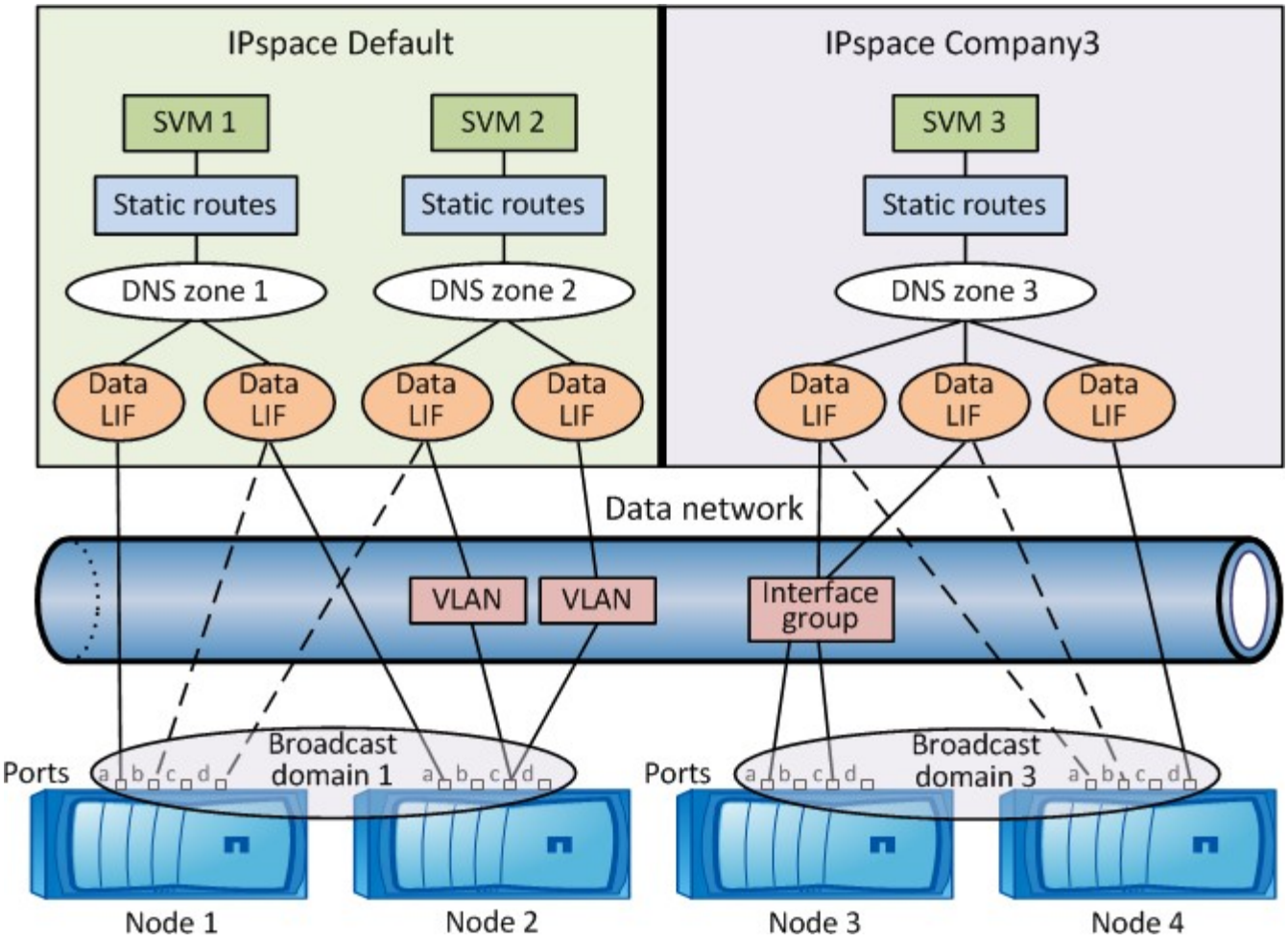
  LIF 생성 중에 DNS 존을 지정할 수 있으며, 클러스터의 DNS 서버를 통해 LIF를 내보낼 이름을 제공합니다. 여러 LIF가 동일한 이름을 공유할 수 있으므로 DNS 로드 밸런싱 기능이 로드에 따라 이름에 대한 IP 주소를 배포할 수 있습니다.

  SVM은 여러 DNS 존을 포함할 수 있습니다.

- 라우팅

  각 SVM은 네트워킹과 관련하여 자체적으로 충분합니다. SVM은 구성된 각 외부 서버에 연결할 수 있는 LIF 및 경로를 소유합니다.

  다음 그림에서는 4노드 클러스터에서 서로 다른 네트워킹 구성 요소가 연결되는 방식을 보여 줍니다.

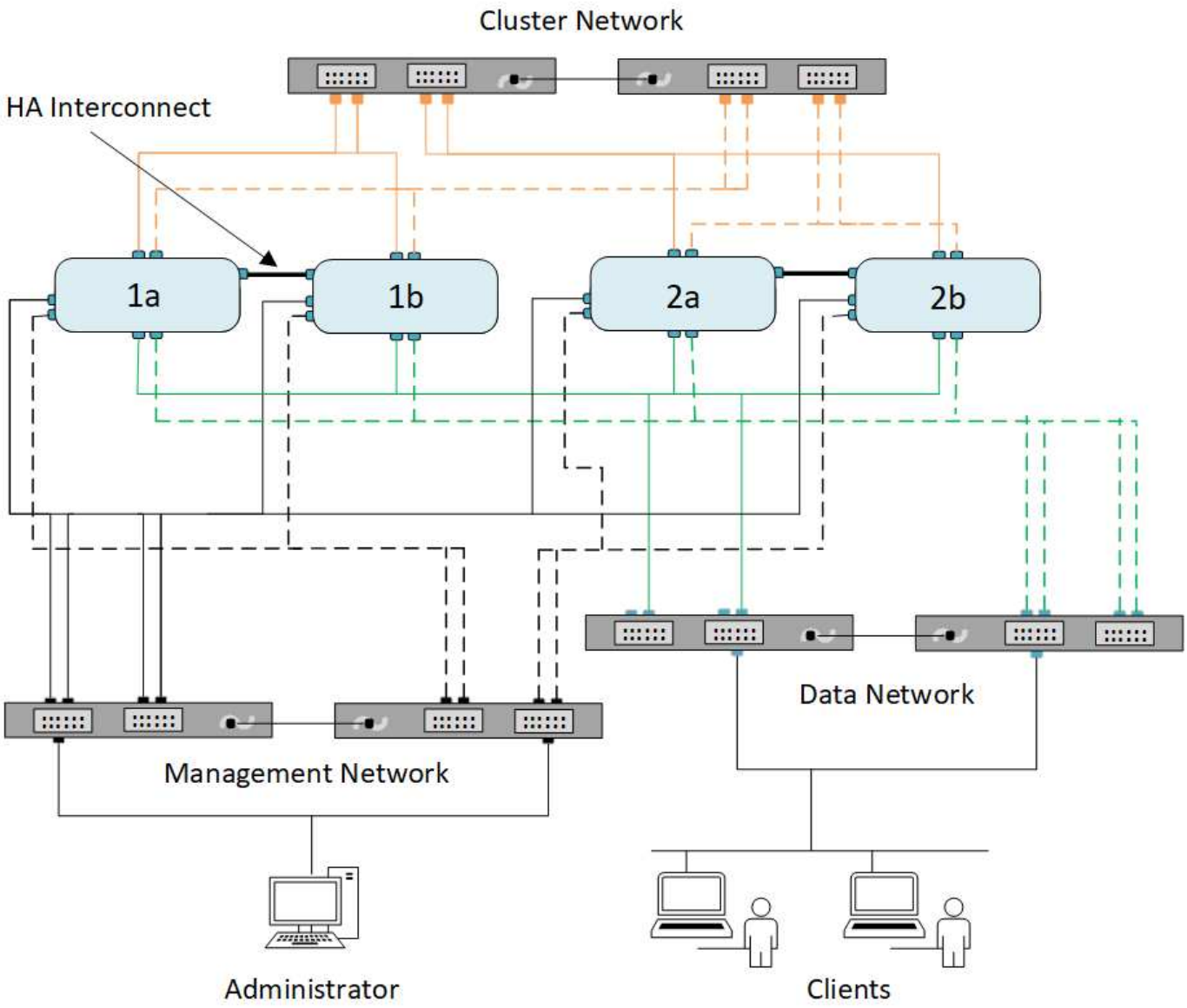


ONTAP 네트워크 케이블 연결에 대한 모범 사례

네트워크 케이블 연결 모범 사례는 트래픽을 클러스터, 관리 및 데이터와 같은 네트워크로 분리합니다.

클러스터 트래픽이 다른 모든 트래픽과 별도의 네트워크에 있도록 클러스터에 케이블을 연결해야 합니다. 이는 선택 사항이지만 데이터와 클러스터 내 트래픽과 네트워크 관리 트래픽을 분리하는 것이 좋습니다. 별도의 네트워크를 유지 관리하여 성능 향상, 관리 용이성, 노드에 대한 보안 및 관리 액세스 개선을 실현할 수 있습니다.

다음 다이어그램에서는 3개의 개별 네트워크를 포함하는 4노드 HA 클러스터의 네트워크 케이블을 연결합니다.



네트워크 연결을 연결할 때는 다음과 같은 특정 지침을 따라야 합니다.

- 각 노드는 3개의 개별 네트워크에 연결되어야 합니다.

  하나의 네트워크는 관리용으로, 하나는 데이터 액세스용으로, 다른 하나는 클러스터 간 통신용으로 사용됩니다. 관리 네트워크와 데이터 네트워크를 논리적으로 분리할 수 있습니다.

- 클라이언트(데이터) 트래픽 흐름을 개선하기 위해 각 노드에 둘 이상의 데이터 네트워크 연결을 가질 수 있습니다.
- 데이터 네트워크 연결 없이 클러스터를 생성할 수 있지만 클러스터 인터커넥트 연결이 포함되어야 합니다.
- 각 노드에 대해 항상 2개 이상의 클러스터 연결이 있어야 합니다.

네트워크 케이블 연결에 대한 자세한 내용은 를 참조하십시오 "AFF and FAS 시스템 설명서 센터 를 참조하십시오" 및 "Hardware Universe".

ONTAP 네트워크에서 사용할 LIF 페일오버 정책을 결정합니다

브로드캐스트 도메인, 페일오버 그룹 및 페일오버 정책이 함께 작동하여 LIF가 구성된 노드 또는 포트에 장애가 발생할 경우 어떤 포트가 대체할지 결정합니다.

브로드캐스트 도메인은 동일한 계층 2 이더넷 네트워크에서 연결할 수 있는 모든 포트를 나열합니다. 포트 중 하나에서 전송된 이더넷 브로드캐스트 패킷은 브로드캐스트 도메인의 다른 모든 포트에서 표시됩니다. LIF가 브로드캐스트 도메인의 다른 포트로 페일오버되더라도 원래 포트에서 연결할 수 있는 모든 로컬 및 원격 호스트에 연결할 수 있으므로 브로드캐스트 도메인의 이러한 공통 도달 가능성 특성이 LIF에 중요합니다.

페일오버 그룹은 브로드캐스트 도메인 내에서 LIF 페일오버 커버리지를 제공하는 포트를 정의합니다. 각 브로드캐스트 도메인에는 모든 포트가 포함된 하나의 페일오버 그룹이 있습니다. 브로드캐스트 도메인의 모든 포트가 포함된 이 페일오버 그룹이 LIF에 대한 기본 페일오버 그룹이며 권장되는 페일오버 그룹입니다. 브로드캐스트 도메인 내에서 동일한 링크 속도를 갖는 포트의 페일오버 그룹과 같이 사용자가 정의하는 작은 하위 집합을 사용하여 페일오버 그룹을 생성할 수 있습니다.

페일오버 정책은 노드 또는 포트가 다운될 때 LIF가 페일오버 그룹의 포트를 사용하는 방법을 결정합니다. 페일오버 정책을 페일오버 그룹에 적용되는 필터 유형으로 고려하십시오. LIF의 페일오버 타겟(LIF가 페일오버가 가능한 포트 세트)은 브로드캐스트 도메인의 LIF 페일오버 그룹에 LIF의 페일오버 정책을 적용하여 결정됩니다.

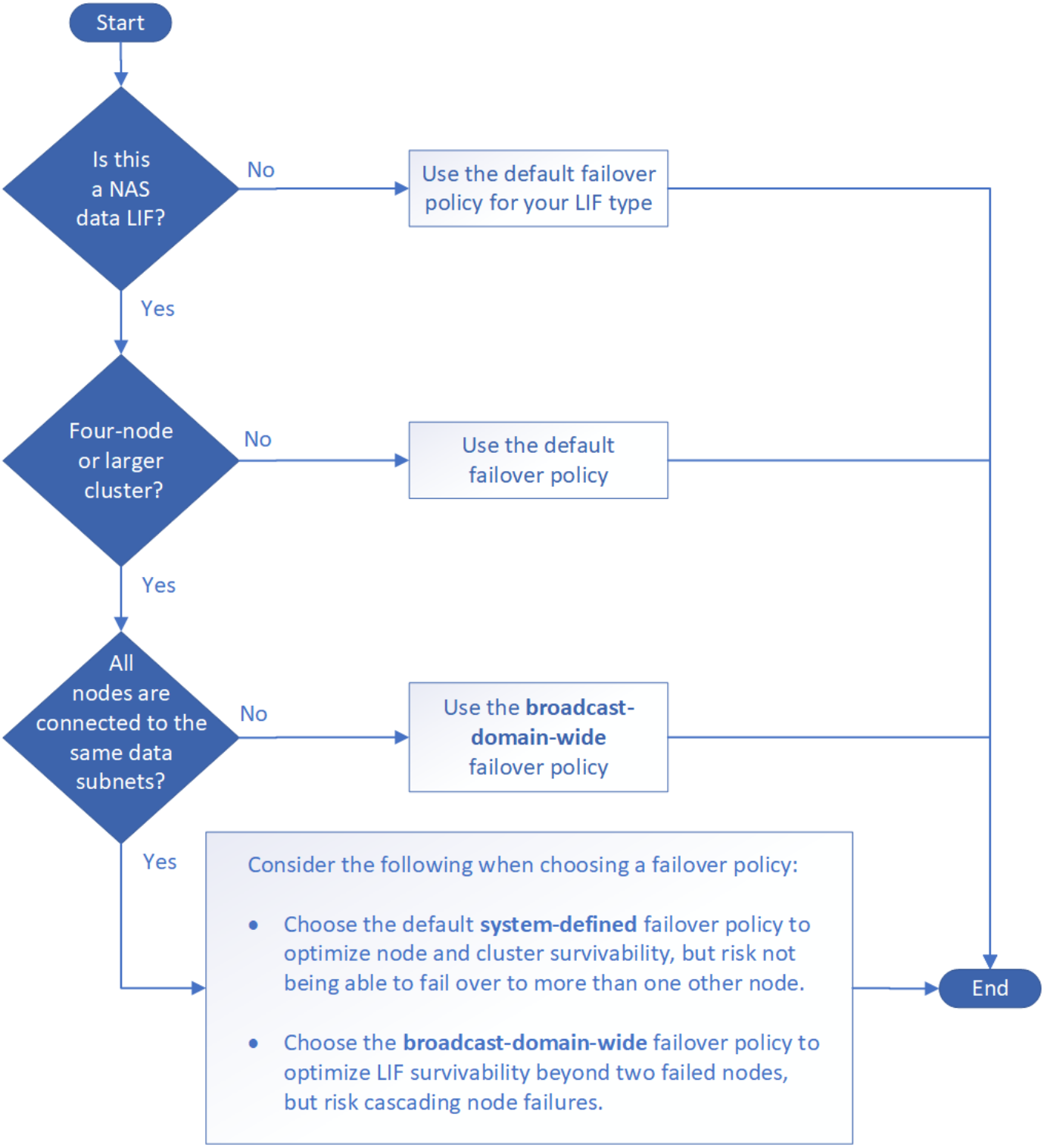
다음 CLI 명령을 사용하여 LIF의 페일오버 타겟을 볼 수 있습니다.

```
network interface show -failover
```

LIF 유형에 기본 페일오버 정책을 사용하는 것이 좋습니다.

사용할 LIF 페일오버 정책을 결정합니다

권장 기본 페일오버 정책을 사용할지, LIF 유형 및 환경에 따라 정책을 변경할지 결정합니다.



LIF 유형별 기본 페일오버 정책

LIF 유형입니다	기본 페일오버 정책입니다	설명
BGP LIF	사용 안 함	LIF가 다른 포트로 페일오버되지 않습니다.
클러스터 LIF	로컬 전용	LIF는 같은 노드의 포트로만 페일오버됩니다.
클러스터 관리 LIF	브로드캐스트 도메인 전체에 적용됩니다	LIF는 클러스터의 모든 노드에 있는 동일한 브로드캐스트 도메인의 포트로 페일오버됩니다.

인터클러스터 LIF	로컬 전용	LIF는 같은 노드의 포트로만 페일오버됩니다.
NAS 데이터 LIF	시스템 정의	LIF가 HA 파트너가 아닌 다른 노드 하나로 페일오버합니다.
노드 관리 LIF	로컬 전용	LIF는 같은 노드의 포트로만 페일오버됩니다.
SAN 데이터 LIF	사용 안 함	LIF가 다른 포트로 페일오버되지 않습니다.

"SFO-파트너 전용" 페일오버 정책은 기본이 아니지만 LIF가 홈 노드 또는 SFO 파트너의 포트로 페일오버되도록 하려는 경우에만 사용할 수 있습니다.

관련 정보

- "네트워크 인터페이스가 표시됩니다"

NAS 경로 페일오버 워크플로우

ONTAP 네트워크에서 NAS 경로 페일오버를 구성합니다

기본 네트워킹 개념에 이미 익숙한 경우 NAS 경로 페일오버 구성에 대한 이 "실습" 워크플로우를 검토하여 네트워크 설정 시간을 절약할 수 있습니다.

NAS 경로 페일오버 구성을 위한 워크플로는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 NAS 페일오버를 구성해야 하는 경우 워크플로우를 "NAS 경로 페일오버 워크플로우(ONTAP 9.7 이하)"참조하십시오.

NAS LIF는 현재 포트에서 링크 장애가 발생하면 작동 가능한 네트워크 포트로 자동 마이그레이션됩니다. ONTAP 기본값을 사용하여 경로 페일오버를 관리할 수 있습니다.

SAN LIF는 마이그레이션되지 않습니다(링크 장애 후 수동으로 이동하지 않는 경우). 대신 호스트의 다중 경로 기술은 트래픽을 다른 LIF로 전환합니다. 자세한 내용은 을 참조하십시오 "SAN 관리".

1 "워크시트를 작성합니다"

워크시트를 사용하여 NAS 경로 페일오버를 계획합니다.

2 "IPspace 생성"

클러스터의 각 SVM에 대해 고유한 IP 주소 공간을 생성합니다.

3 "브로드캐스트 도메인을 IPspace로 이동"

브로드캐스트 도메인을 IPspace로 이동합니다.

4 "SVM을 생성합니다"

SVM을 생성하여 클라이언트에 데이터 제공

5 **"LIF를 생성합니다"**

데이터에 액세스하는 데 사용할 포트에 LIF를 생성합니다.

6 **"SVM에 대한 DNS 서비스를 구성합니다"**

NFS 또는 SMB 서버를 생성하기 전에 SVM에 대한 DNS 서비스를 구성합니다.

ONTAP 네트워크에서 NAS 경로 페일오버를 위한 워크시트

NAS 경로 페일오버를 구성하기 전에 워크시트의 모든 섹션을 완료해야 합니다.

ONTAP 네트워크의 NAS 장애 조치에 대한 정보는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 NAS 페일오버를 구성해야 하는 경우 을 참조하십시오"NAS 경로 페일오버 구성용 워크시트(ONTAP 9.7 이하)".

IPSpace 구성

IPspace를 사용하여 클러스터의 각 SVM에 대해 별개의 IP 주소 공간을 생성할 수 있습니다. 이렇게 하면 관리자가 별도의 네트워크 도메인에 있는 클라이언트가 동일한 IP 주소 서브넷 범위의 중복 IP 주소를 사용하면서 클러스터 데이터에 액세스할 수 있습니다.

정보	요구한?	당신의 가치
IPSpace 이름 IPspace의 고유 식별자입니다.	예	

브로드캐스트 도메인 구성

브로드캐스트 도메인은 동일한 계층 2 네트워크에 속한 포트를 그룹화하고 브로드캐스트 도메인 포트에 대한 MTU를 설정합니다.

브로드캐스트 도메인은 IPspace에 할당됩니다. IPspace는 하나 이상의 브로드캐스트 도메인을 포함할 수 있습니다.

LIF가 페일오버되는 포트는 LIF의 페일오버 그룹의 구성원이어야 합니다. ONTAP에서 생성된 각 브로드캐스트 도메인에 대해 동일한 이름의 페일오버 그룹이 생성되어 브로드캐스트 도메인의 모든 포트가 포함됩니다.

정보	요구한?	당신의 가치
IPSpace 이름 브로드캐스트 도메인이 할당된 IPspace입니다. 이 IPspace가 있어야 합니다.	예	
브로드캐스트 도메인 이름 브로드캐스트 도메인의 이름입니다. 이 이름은 IPspace에서 고유해야 합니다.	예	

MTU 브로드캐스트 도메인의 최대 전송 단위 값으로, 일반적으로 * 1500 * 또는 * 9000 * 로 설정됩니다. MTU 값은 브로드캐스트 도메인의 모든 포트와 나중에 브로드캐스트 도메인에 추가된 모든 포트에 적용됩니다. MTU 값은 해당 네트워크에 연결된 모든 장치와 일치해야 합니다. e0M 포트 처리 관리 및 서비스 프로세서 트래픽은 MTU를 1500바이트 이상으로 설정해야 합니다.	예	
포트 포트는 도달 가능 여부에 따라 브로드캐스트 도메인에 할당됩니다. 포트 할당이 완료되면 네트워크 포트 도달 가능성 표시 명령을 실행하여 연결 상태를 확인합니다. 이러한 포트는 물리적 포트, VLAN 또는 인터페이스 그룹이 될 수 있습니다. 에 대한 자세한 내용은 `network port reachability show` "ONTAP 명령 참조입니다"을 참조하십시오.	예	

서브넷 구성

서브넷에는 IP 주소 풀과 IPspace에 상주하는 SVM에서 사용하는 LIF에 할당할 수 있는 기본 게이트웨이가 포함되어 있습니다.

- SVM에서 LIF를 생성할 때 IP 주소와 서브넷을 제공하는 대신 서브넷 이름을 지정할 수 있습니다.
- 서브넷을 기본 게이트웨이로 구성할 수 있기 때문에 SVM을 생성할 때 별도의 단계에서 기본 게이트웨이를 생성할 필요가 없습니다.
- 브로드캐스트 도메인은 하나 이상의 서브넷을 포함할 수 있습니다.
- IPspace의 브로드캐스트 도메인에 하나 이상의 서브넷을 연결하여 다른 서브넷에 있는 SVM LIF를 구성할 수 있습니다.
- 각 서브넷에는 동일한 IPspace에서 다른 서브넷에 할당된 IP 주소와 중복되지 않는 IP 주소가 포함되어야 합니다.
- SVM 데이터 LIF에 특정 IP 주소를 할당하고 서브넷 대신 SVM을 위한 기본 게이트웨이를 생성할 수 있습니다.

정보	요구한?	당신의 가치
IPSpace 이름 서브넷이 할당될 IPspace입니다. 이 IPspace가 있어야 합니다.	예	

서브넷 이름 서브넷의 이름입니다. 이 이름은 IPspace에서 고유해야 합니다.	예	
브로드캐스트 도메인 이름 서브넷이 할당될 브로드캐스트 도메인입니다. 이 브로드캐스트 도메인은 지정된 IPspace에 있어야 합니다.	예	
서브넷 이름 및 IP 주소가 상주하는 서브넷 및 마스크를 마스킹합니다.	예	
게이트웨이 서브넷에 대한 기본 게이트웨이를 지정할 수 있습니다. 서브넷을 생성할 때 게이트웨이를 할당하지 않으면 나중에 할당할 수 있습니다.	아니요	
IP 주소 범위 IP 주소 또는 특정 IP 주소 범위를 지정할 수 있습니다. 예를 들어 다음과 같은 범위를 지정할 수 있습니다. 192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145 IP 주소 범위를 지정하지 않으면 지정된 서브넷의 전체 IP 주소 범위를 LIF에 할당할 수 있습니다.	아니요	
LIF 연결의 강제 업데이트 기존 LIF 연결을 강제로 업데이트할지 여부를 지정합니다. 기본적으로 서비스 프로세서 인터페이스 또는 네트워크 인터페이스가 제공된 범위의 IP 주소를 사용하는 경우 서브넷 생성이 실패합니다. 이 매개 변수를 사용하면 수동으로 주소를 지정한 모든 인터페이스를 서브넷에 연결하고 명령이 성공할 수 있습니다.	아니요	

SVM 구성

SVM을 사용하여 클라이언트 및 호스트에 데이터를 제공할 수 있습니다.

귀사가 기록하는 값은 기본 데이터 SVM을 생성하는 것입니다. MetroCluster 소스 SVM을 생성하는 경우 를 참조하십시오 "패브릭 연결 MetroCluster 설치 및 구성 가이드" 또는 을 누릅니다 "스트레치 MetroCluster 설치 및 구성 가이드".

정보	요구한?	당신의 가치
SVM은 SVM의 FQDN(정규화된 도메인 이름)을 지정합니다. 이 이름은 클러스터 리그 전체에서 고유해야 합니다.	예	
루트 볼륨 이름 SVM 루트 볼륨의 이름입니다.	예	
애그리게이트 이름 SVM 루트 볼륨을 포함하는 애그리게이트의 이름입니다. 이 집계가 있어야 합니다.	예	
보안 스타일 SVM 루트 볼륨의 보안 스타일입니다. 가능한 값은 * NTFS *, * UNIX * 및 * MIXED * 입니다.	예	
IPspace 이름 SVM이 할당된 IPspace입니다. 이 IPspace가 있어야 합니다.	아니요	
SVM 언어 SVM 및 해당 볼륨에 사용할 기본 언어를 설정합니다. 기본 언어를 지정하지 않으면 기본 SVM 언어가 * c UTF-8 * 로 설정됩니다. SVM 언어 설정에 따라 SVM의 모든 NAS 볼륨에 대한 파일 이름과 데이터를 표시하는 데 사용되는 문자 세트가 결정됩니다. SVM이 생성된 후 언어를 수정할 수 있습니다.	아니요	

LIF 구성

SVM은 하나 이상의 네트워크 논리 인터페이스(LIF)를 통해 클라이언트와 호스트에 데이터를 제공합니다.

정보	요구한?	당신의 가치
SVM은 LIF의 SVM 이름 입니다.	예	
LIF 이름 LIF의 이름입니다. 노드당 여러 개의 데이터 LIF를 할당할 수 있으며, 노드에 사용 가능한 데이터 포트가 있는 경우 클러스터의 모든 노드에 LIF를 할당할 수 있습니다. 이중화를 제공하려면 각 데이터 서브넷에 대해 최소 2개의 데이터 LIF를 생성해야 하며, 특정 서브넷에 할당된 LIF에는 서로 다른 노드의 홈 포트가 할당되어야 합니다. * 중요: * SMB를 통해 Hyper-V 또는 SQL Server를 호스팅하도록 SMB 서버를 구성하는 경우, SVM은 클러스터의 모든 노드에 하나 이상의 데이터 LIF가 있어야 합니다.	예	
LIF에 대한 서비스 정책 서비스 정책입니다. 서비스 정책은 LIF를 사용할 수 있는 네트워크 서비스를 정의합니다. 기본 제공 서비스 및 서비스 정책을 사용하여 데이터 및 시스템 SVM에서 데이터 및 관리 트래픽을 관리할 수 있습니다.	예	

허용된 프로토콜 IP 기반 LIF에는 허용되는 프로토콜이 필요하지 않습니다. 대신 서비스 정책 행을 사용하십시오. FiberChannel 포트의 SAN LIF에 대해 허용되는 프로토콜을 지정합니다. 이러한 LIF를 사용할 수 있는 프로토콜입니다. LIF가 생성된 후에는 LIF를 사용하는 프로토콜을 수정할 수 없습니다. LIF를 구성할 때 모든 프로토콜을 지정해야 합니다.	아니요	
홈 노드 LIF가 홈 포트로 되돌아갈 때 LIF가 반환되는 노드입니다. 각 데이터 LIF에 대한 홈 노드를 기록해야 합니다.	예	
홈 포트 또는 브로드캐스트 도메인이 다음 중 하나를 선택했습니다. * 포트 *: LIF가 홈 포트로 되돌아갈 때 논리 인터페이스가 반환되는 포트를 지정합니다. IPspace의 서브넷에서 첫 번째 LIF에서만 수행되었지만, 그렇지 않으면 필요하지 않습니다. * 브로드캐스트 도메인 *: 브로드캐스트 도메인을 지정하면 LIF가 홈 포트로 되돌아갈 때 논리 인터페이스가 반환될 적절한 포트가 선택됩니다.	예	
서브넷 이름 SVM에 할당할 서브넷입니다. 애플리케이션 서버에 지속적으로 사용 가능한 SMB 연결을 생성하는 데 사용되는 모든 데이터 LIF는 동일한 서브넷에 있어야 합니다.	예(서브넷을 사용하는 경우)	

DNS 구성

NFS 또는 SMB 서버를 생성하기 전에 SVM에서 DNS를 구성해야 합니다.

정보	요구한?	당신의 가치
SVM 이름 NFS 또는 SMB 서버를 생성하려는 SVM의 이름입니다.	예	
DNS 도메인 이름 호스트-IP 이름 확인을 수행할 때 호스트 이름에 추가할 도메인 이름 목록입니다. 먼저 로컬 도메인을 나열한 다음 DNS 쿼리를 가장 자주 만드는 도메인 이름을 나열합니다.	예	

DNS 서버의 IP 주소 NFS 또는 SMB 서버의 이름 확인을 제공할 DNS 서버의 IP 주소 목록입니다. 나열된 DNS 서버에는 SMB 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다. SRV 레코드는 서비스 이름을 해당 서비스를 제공하는 서버의 DNS 컴퓨터 이름에 매핑하는 데 사용됩니다. ONTAP가 로컬 DNS 쿼리를 통해 서비스 위치 레코드를 가져올 수 없는 경우 SMB 서버 생성이 실패합니다. ONTAP가 Active Directory SRV 레코드를 찾을 수 있도록 하는 가장 간단한 방법은 SVM DNS 서버로 Active Directory 통합 DNS 서버를 구성하는 것입니다. DNS 관리자가 Active Directory 도메인 컨트롤러에 대한 정보가 포함된 DNS 영역에 SRV 레코드를 수동으로 추가한 경우 Active Directory 통합 DNS 서버가 아닌 서버를 사용할 수 있습니다. Active Directory 통합 SRV 레코드에 대한 자세한 내용은 항목을 참조하십시오 "Microsoft TechNet의 Active Directory에 대한 DNS 지원 방법".	예	

동적 **DNS** 구성

동적 DNS를 사용하여 Active Directory 통합 DNS 서버에 DNS 항목을 자동으로 추가하려면 SVM에서 DDNS(동적 DNS)를 구성해야 합니다.

SVM의 모든 데이터 LIF에 대해 DNS 레코드가 생성됩니다. SVM에 여러 데이터 LIF를 생성하여 할당된 데이터 IP 주소에 클라이언트 연결을 로드 밸런싱할 수 있습니다. DNS 로드는 호스트 이름을 사용하여 생성된 연결을 라운드 로빈 방식으로 할당된 IP 주소로 조정합니다.

정보	요구한?	당신의 가치
SVM은 NFS 또는 SMB 서버를 생성할 SVM의 이름을 지정합니다.	예	
DDNS 사용 여부 DDNS 사용 여부를 지정합니다. SVM에 구성된 DNS 서버가 DDNS를 지원해야 합니다. 기본적으로 DDNS는 비활성화되어 있습니다.	예	
보안 DDNS 보안 DDNS 사용 여부는 Active Directory 통합 DNS에서만 지원됩니다. Active Directory 통합 DNS에서 보안 DDNS 업데이트만 허용하는 경우 이 매개 변수의 값은 참이어야 합니다. 기본적으로 보안 DDNS는 비활성화되어 있습니다. SVM을 위해 SMB 서버 또는 Active Directory 계정을 생성한 후에만 보안 DDNS를 활성화할 수 있습니다.	아니요	
DNS 도메인의 FQDN DNS 도메인의 FQDN 입니다. SVM에서 DNS 이름 서비스로 구성된 동일한 도메인 이름을 사용해야 합니다.	아니요	

네트워크 포트

ONTAP 네트워크 포트 구성에 대해 자세히 알아보십시오

포트는 물리적 포트(NIC) 또는 인터페이스 그룹 또는 VLAN과 같은 가상 포트입니다.

VLAN(Virtual Local Area Network) 및 인터페이스 그룹은 가상 포트를 구성합니다. 인터페이스 그룹은 여러 물리적 포트를 단일 포트로 취급하며 VLAN은 물리적 포트를 여러 개의 개별 논리 포트로 세분화합니다.

- 물리적 포트: LIF는 물리적 포트에서 직접 구성할 수 있습니다.
- 인터페이스 그룹: 단일 트렁크 포트로 작동하는 2개 이상의 물리적 포트를 포함하는 포트 애그리게이트. 인터페이스 그룹은 단일 모드, 다중 모드 또는 동적 다중 모드일 수 있습니다.
- VLAN: VLAN 태그 지정(IEEE 802.1Q 표준) 트래픽을 수신 및 전송하는 논리 포트입니다. VLAN 포트 특성에는 포트의 VLAN ID가 포함됩니다. 기본 물리적 포트 또는 인터페이스 그룹 포트는 VLAN 트렁크 포트로 간주되며 연결된 스위치 포트는 VLAN ID를 트렁킹하도록 구성해야 합니다.

  VLAN 포트의 기본 물리적 포트 또는 인터페이스 그룹 포트는 태그 없는 트래픽을 전송 및 수신하는 LIF를 계속 호스팅할 수 있습니다.

- 가상 IP(VIP) 포트: VIP LIF의 홈 포트로 사용되는 논리 포트입니다. VIP 포트는 시스템에서 자동으로 생성되며 제한된 수의 작업만 지원합니다. VIP 포트는 ONTAP 9.5부터 지원됩니다.

포트 명명 규칙은 _ enumberletter _ 입니다.

- 첫 번째 문자는 포트 유형을 나타냅니다. "e"는 이더넷을 나타냅니다.
- 두 번째 문자는 포트 어댑터가 있는 번호가 매겨진 슬롯을 나타냅니다.
- 세 번째 문자는 다중 포트 어댑터의 포트 위치를 나타냅니다. "a"는 첫 번째 포트를 나타내고, "b"는 두 번째 포트를 나타냅니다.

예를 들어, "e0b"은 이더넷 포트가 노드 마더보드의 두 번째 포트임을 나타냅니다.

VLAN은 'port_name-vlan-id' 구문을 사용하여 이름을 지정해야 합니다.

port_name은 물리적 포트 또는 인터페이스 그룹을 지정합니다.

VLAN-id는 네트워크의 VLAN 식별을 지정합니다. 예를 들어, "e1c-80"은 유효한 VLAN 이름입니다.

네트워크 포트를 구성합니다

물리적 포트를 결합하여 **ONTAP** 인터페이스 그룹을 생성합니다

LAG(Link Aggregation Group)라고도 하는 인터페이스 그룹은 동일한 노드에 있는 두 개 이상의 물리적 포트를 단일 논리 포트로 결합하여 생성됩니다. 논리 포트는 향상된 복구 성능, 향상된 가용성 및 로드 공유를 제공합니다.

인터페이스 그룹 유형입니다

스토리지 시스템에서는 단일 모드, 정적 멀티모드 및 동적 멀티모드 등 세 가지 유형의 인터페이스 그룹이 지원됩니다.

각 인터페이스 그룹은 서로 다른 수준의 내결함성을 제공합니다. 다중 모드 인터페이스 그룹은 네트워크 트래픽의 로드 밸런싱을 위한 방법을 제공합니다.

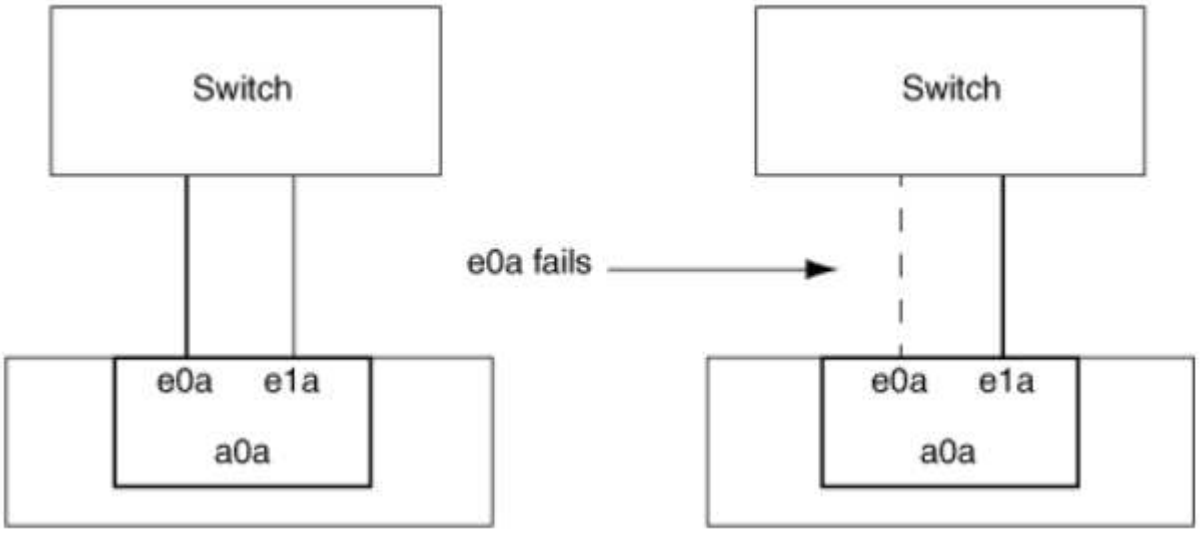
단일 모드 인터페이스 그룹의 특성

단일 모드 인터페이스 그룹에서는 인터페이스 그룹에 있는 인터페이스 중 하나만 활성화됩니다. 다른 인터페이스는 대기 상태이며 활성 인터페이스가 실패한 경우 대신 사용할 수 있습니다.

단일 모드 인터페이스 그룹의 특징:

- 페일오버의 경우 클러스터에서 액티브 링크를 모니터링하고 페일오버를 제어합니다. 클러스터가 액티브 링크를 모니터링하므로 스위치 구성이 필요하지 않습니다.
- 단일 모드 인터페이스 그룹에서 대기 중인 인터페이스가 두 개 이상 있을 수 있습니다.
- 단일 모드 인터페이스 그룹이 여러 스위치에 걸쳐 있는 경우 ISL(Inter-Switch Link)을 사용하여 스위치를 연결해야 합니다.
- 단일 모드 인터페이스 그룹의 경우 스위치 포트는 동일한 브로드캐스트 도메인에 있어야 합니다.
- 소스 주소가 0.0.0.0인 링크 모니터링 ARP 패킷은 포트를 통해 전송되어 포트가 동일한 브로드캐스트 도메인에 있는지 확인합니다.

다음 그림은 단일 모드 인터페이스 그룹의 예입니다. 그림에서 e0a 및 E1A는 a0a 단일 모드 인터페이스 그룹의 일부입니다. 활성 인터페이스인 e0a에 장애가 발생하면 대기 E1A 인터페이스가 스위치 연결을 대신 사용합니다.



단일 모드 기능을 수행하려면 페일오버 그룹을 사용하는 것이 좋습니다. 페일오버 그룹을 사용하면 다른 LIF에 두 번째 포트를 계속 사용할 수 있으며 사용하지 않은 상태로 둘 필요가 없습니다. 또한 페일오버 그룹은 2개 이상의 포트에 걸쳐 있을 수 있으며 여러 노드의 포트를 포괄할 수 있습니다.

정적 멀티모드 인터페이스 그룹의 특성

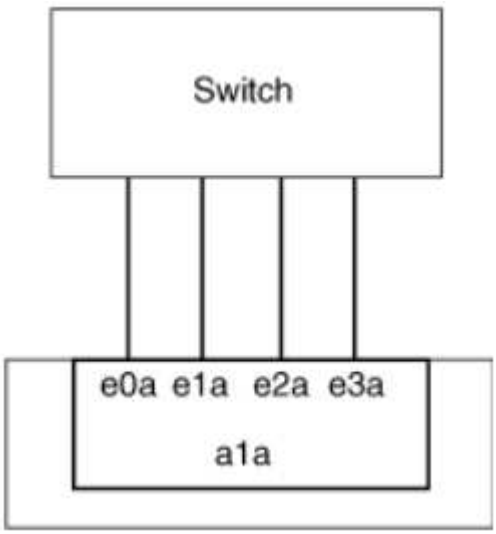
ONTAP의 정적 멀티모드 인터페이스 그룹 구현은 IEEE 802.3ad(정적)를 준수합니다. 집계를 지원하지만 집계를 구성하기 위한 제어 패킷 교환이 없는 스위치는 정적 멀티모드 인터페이스 그룹과 함께 사용할 수 있습니다.

정적 멀티모드 인터페이스 그룹은 LACP(Link Aggregation Control Protocol)라고도 하는 IEEE 802.3ad(동적)를 준수하지 않습니다. LACP는 Cisco의 독점 링크 통합 프로토콜인 PAgP(Port Aggregation Protocol)와 동일합니다.

다음은 정적 멀티모드 인터페이스 그룹의 특성입니다.

- 인터페이스 그룹의 모든 인터페이스가 활성 상태이고 단일 MAC 주소를 공유합니다.
  - 여러 개의 개별 연결이 인터페이스 그룹의 인터페이스 간에 분산됩니다.
  - 각 연결 또는 세션은 인터페이스 그룹 내에서 하나의 인터페이스를 사용합니다. 순차 로드 밸런싱 체계를 사용하면 모든 세션이 패킷 단위로 사용 가능한 링크 전체에 분산되며 인터페이스 그룹의 특정 인터페이스에 바인딩되지 않습니다.
- 정적 멀티모드 인터페이스 그룹은 최대 "n-1" 인터페이스의 오류에서 복구할 수 있습니다. 여기서 n은 인터페이스 그룹을 구성하는 총 인터페이스 수입니다.
- 포트에 장애가 발생하거나 연결이 끊어지면 장애가 발생한 링크를 통과하는 트래픽이 나머지 인터페이스 중 하나에 자동으로 재분배됩니다.
- 정적 멀티모드 인터페이스 그룹은 링크 손실을 감지할 수 있지만 연결 및 성능에 영향을 줄 수 있는 클라이언트 또는 스위치 구성 오류로 인한 연결 손실을 감지할 수 없습니다.
- 정적 멀티모드 인터페이스 그룹에는 여러 스위치 포트를 통한 Link Aggregation을 지원하는 스위치가 필요합니다. 인터페이스 그룹의 링크가 연결되는 모든 포트가 단일 논리 포트에 속하도록 스위치가 구성됩니다. 일부 스위치는 점보 프레임에 구성된 포트의 링크 집계를 지원하지 않을 수 있습니다. 자세한 내용은 스위치 공급업체의 설명서를 참조하십시오.
- 정적 멀티모드 인터페이스 그룹의 인터페이스 간에 트래픽을 분산하기 위해 몇 가지 로드 밸런싱 옵션을 사용할 수 있습니다.

다음 그림은 정적 멀티모드 인터페이스 그룹의 예입니다. 인터페이스 e0a, E1A, e2a 및 e3a는 A1A 다중 모드 인터페이스 그룹의 일부입니다. A1A 멀티모드 인터페이스 그룹의 4개 인터페이스가 모두 활성화됩니다.



단일 통합 링크의 트래픽을 여러 물리적 스위치에 분산하는 여러 기술이 존재합니다. 이 기능을 지원하는 데 사용되는 기술은 네트워킹 제품에 따라 다릅니다. ONTAP의 정적 멀티모드 인터페이스 그룹은 IEEE 802.3 표준을 준수합니다. 특정 다중 스위치 링크 통합 기술이 IEEE 802.3 표준과 상호 운용되거나 이를 준수한다고 말한다면 ONTAP와 함께 작동해야 합니다.

IEEE 802.3 표준에는 집계된 링크의 전송 장치가 전송할 물리적 인터페이스를 결정한다고 명시되어 있습니다. 따라서 ONTAP는 아웃바운드 트래픽을 분산하는 데만 책임이 있으며 인바운드 프레임이 도착하는 방식을 제어할 수 없습니다. 집계된 링크에서 인바운드 트래픽의 전송을 관리 또는 제어하려면 직접 연결된 네트워크 장치에서 해당 전송을 수정해야 합니다.

동적 멀티모드 인터페이스 그룹

동적 멀티모드 인터페이스 그룹은 직접 연결된 스위치에 그룹 구성원을 전달하기 위해 링크 통합 제어 프로토콜(LACP)을 구현합니다. LACP를 사용하면 링크 상태 손실과 노드가 직접 연결 스위치 포트와 통신할 수 없음을 감지할 수 있습니다.

ONTAP의 동적 멀티모드 인터페이스 그룹 구현은 IEEE 802.3 AD(802.1 AX)를 준수합니다. ONTAP는 Cisco의 독점 링크 집계 프로토콜인 PAgP(포트 집계 프로토콜)를 지원하지 않습니다.

동적 멀티모드 인터페이스 그룹에는 LACP를 지원하는 스위치가 필요합니다.

ONTAP는 활성 모드 또는 수동 모드로 구성된 스위치와 잘 작동하는 구성 불가능한 활성 모드에서 LACP를 구현합니다. ONTAP는 IEEE 802.3 AD(802.1ax)에 지정된 대로 긴 LACP 타이머 및 짧은 LACP 타이머(구성 불가능한 값 3초 및 90초용)를 구현합니다.

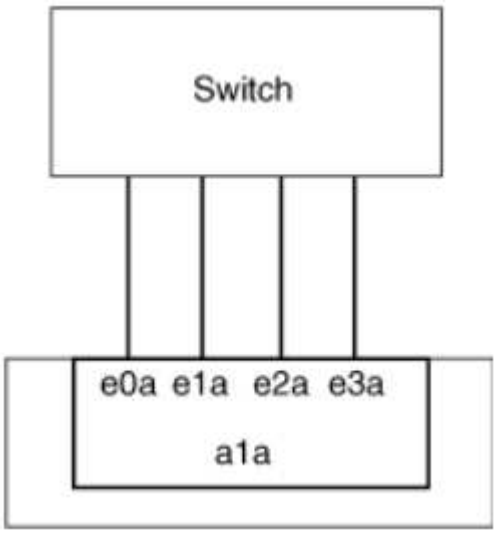
ONTAP 로드 밸런싱 알고리즘은 아웃바운드 트래픽 전송에 사용할 구성원 포트를 결정하며 인바운드 프레임 수신 방식을 제어하지 않습니다. 스위치는 스위치의 포트 채널 그룹에 구성된 로드 밸런싱 알고리즘에 따라 전송에 사용할 포트 채널 그룹의 구성원(개별 물리적 포트)을 결정합니다. 따라서 스위치 구성에 따라 트래픽을 수신할 스토리지 시스템의 구성원 포트(개별 물리적 포트)가 결정됩니다. 스위치 구성에 대한 자세한 내용은 스위치 공급업체의 설명서를 참조하십시오.

개별 인터페이스에서 연속적인 LACP 프로토콜 패킷을 수신하지 못하면 해당 개별 인터페이스는 "ifgrp status" 명령 출력에서 "lag_inactive"로 표시됩니다. 기존 트래픽은 나머지 활성 인터페이스로 자동으로 재라우팅됩니다.

동적 멀티모드 인터페이스 그룹을 사용할 때 다음 규칙이 적용됩니다.

- 동적 멀티모드 인터페이스 그룹은 포트 기반, IP 기반, MAC 기반 또는 라운드 로빈 로드 밸런싱 방법을 사용하도록 구성되어야 합니다.
- 동적 멀티모드 인터페이스 그룹에서 모든 인터페이스는 활성 상태이고 단일 MAC 주소를 공유해야 합니다.

다음 그림은 동적 멀티모드 인터페이스 그룹의 예입니다. 인터페이스 e0a, E1A, e2a 및 e3a는 A1A 다중 모드 인터페이스 그룹의 일부입니다. A1A 동적 멀티모드 인터페이스 그룹의 4개 인터페이스가 모두 활성화됩니다.



다중 모드 인터페이스 그룹의 로드 밸런싱

IP 주소, MAC 주소, 순차 또는 포트 기반 로드 밸런싱 방법을 사용하여 다중 모드 인터페이스 그룹의 네트워크 포트를 통해 네트워크 트래픽을 균등하게 분산함으로써 나가는 트래픽에 다중 모드 인터페이스 그룹의 모든 인터페이스가

동일하게 사용되도록 할 수 있습니다.

다중 모드 인터페이스 그룹에 대한 로드 밸런싱 방법은 인터페이스 그룹이 생성된 경우에만 지정할 수 있습니다.

- 모범 사례 *: 가능하면 포트 기반 로드 밸런싱이 권장됩니다. 네트워크에서 포트 기반 로드 밸런싱을 사용하는 것이 금지되는 특별한 이유 또는 제한이 없는 경우.

포트 기반 로드 밸런싱

포트 기반 로드 밸런싱이 권장되는 방법입니다.

포트 기반 로드 밸런싱 방법을 사용하여 전송 계층(TCP/UDP) 포트를 기반으로 다중 모드 인터페이스 그룹의 트래픽을 균등화할 수 있습니다.

포트 기반 로드 밸런싱 방법은 전송 계층 포트 번호와 함께 소스 및 대상 IP 주소에 대한 빠른 해싱 알고리즘을 사용합니다.

IP 주소 및 **MAC** 주소 로드 밸런싱

IP 주소 및 MAC 주소 로드 밸런싱은 다중 모드 인터페이스 그룹의 트래픽을 균등하게 조정하는 방법입니다.

이러한 로드 밸런싱 방법은 소스 및 대상 주소(IP 주소 및 MAC 주소)에서 빠른 해싱 알고리즘을 사용합니다. 해싱 알고리즘의 결과가 UP 링크 상태가 아닌 인터페이스에 매핑되면 다음 활성 인터페이스가 사용됩니다.

> 라우터에 직접 연결하는 시스템에 인터페이스 그룹을 생성할 때 MAC 주소 로드 밸런싱 방법을 선택하지 마십시오. 이러한 설정에서 모든 발신 IP 프레임에 대해 대상 MAC 주소는 라우터의 MAC 주소입니다. 따라서 인터페이스 그룹의 인터페이스가 하나만 사용됩니다.

IP 주소 로드 밸런싱은 IPv4와 IPv6 주소 모두에서 동일한 방식으로 작동합니다.

순차적 로드 밸런싱

순차 로드 밸런싱을 사용하여 라운드 로빈 알고리즘을 사용하여 여러 링크 간에 패킷을 균등하게 분산할 수 있습니다. 순차적 옵션을 사용하여 단일 연결의 트래픽을 여러 링크에서 로드 밸런싱하여 단일 연결 처리량을 높일 수 있습니다.

그러나 순차적 로드 밸런싱으로 인해 순서가 잘못된 패킷 전달이 발생할 수 있기 때문에 성능이 매우 저하될 수 있습니다. 따라서 순차적 로드 밸런싱은 일반적으로 권장되지 않습니다.

인터페이스 그룹 또는 **LAG**를 만듭니다

인터페이스 그룹 또는 LAG(단일 모드, 정적 멀티모드 또는 동적 멀티모드(LACP))를 생성하여 집계된 네트워크 포트의 기능을 결합하여 클라이언트에 단일 인터페이스를 제공할 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 LAG * 를 만듭니다

단계

1. LAG를 만들려면 네트워크 > 이더넷 포트 > + Link Aggregation Group * 을 선택합니다.
2. 드롭다운 목록에서 노드를 선택합니다.
3. 다음 중에서 선택합니다.
   a. ONTAP to * automatically select broadcast domain (recommended) *.
   b. 브로드캐스트 도메인을 수동으로 선택합니다.
4. LAG를 구성할 포트를 선택합니다.
5. 모드를 선택합니다.
   a. 단일: 한 번에 하나의 포트만 사용됩니다.
   b. 다중: 모든 포트를 동시에 사용할 수 있습니다.
   c. LACP: LACP 프로토콜이 사용할 수 있는 포트를 결정합니다.
6. 로드 밸런싱 선택:
   a. IP 기반
   b. Mac 기반
   c. 포트
   d. 순차적
7. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 인터페이스 그룹을 생성합니다 *

다중 모드 인터페이스 그룹을 생성할 때 다음 로드 밸런싱 방법 중 하나를 지정할 수 있습니다.

- 포트 : 네트워크 트래픽은 전송 계층(TCP/UDP) 포트를 기반으로 분산됩니다. 이것은 권장되는 로드 밸런싱 방법입니다.
- MAC 주소 기준으로 네트워크 트래픽이 분산된다.
- IP: 네트워크 트래픽은 IP 주소를 기반으로 분산됩니다.
- '등전위': 네트워크 트래픽이 수신될 때 분산됩니다.

인터페이스 그룹의 MAC 주소는 기본 포트의 순서 및 부팅 시 이러한 포트가 초기화되는 방식에 따라 결정됩니다. 따라서 재부팅 또는 ONTAP 업그레이드 시 ifgrp MAC 주소가 영구하다고 가정해서는 안 됩니다.

단계

interface group을 생성하기 위해 'network port ifgrp create' 명령어를 사용한다.

인터페이스 그룹의 이름은 "a<number><letter>" 구문을 사용하여 지정해야 합니다. 예를 들어, a0a, a0b, A1c 및

A2A는 유효한 인터페이스 그룹 이름입니다.

에 대한 자세한 내용은 `network port ifgrp create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 포트 및 다중 모드 분산 기능을 사용하여 a0a라는 인터페이스 그룹을 만드는 방법을 보여 줍니다.

'network port ifgrp create-node_cluster-1-01_-ifgrp_a0a_-Distr-func_port_-mode_multimode_'

인터페이스 그룹 또는 **LAG**에 포트를 추가합니다

모든 포트 속도에 대해 인터페이스 그룹 또는 LAG에 최대 16개의 물리적 포트를 추가할 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 LAG*에 포트를 추가합니다

단계

1. LAG를 편집하려면 * 네트워크 > 이더넷 포트 > LAG * 를 선택합니다.
2. LAG에 추가할 같은 노드의 추가 포트를 선택합니다.
3. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 인터페이스 그룹에 포트를 추가합니다 *

단계

인터페이스 그룹에 네트워크 포트를 추가합니다.

'network port ifgrp add-port'를 참조하십시오

다음 예에서는 a0a라는 인터페이스 그룹에 e0c 포트를 추가하는 방법을 보여줍니다.

'network port ifgrp add-port-node_cluster-1-01_-ifgrp_a0a_-port_e0c_'

ONTAP 9.8부터 인터페이스 그룹은 인터페이스 그룹에 첫 번째 물리적 포트가 추가된 후 약 1분 후에 적절한 브로드캐스트 도메인에 자동으로 배치됩니다. ONTAP가 이 작업을 수행하지 않도록 하고 ifgrp를 브로드캐스트 도메인에 수동으로 배치하려는 경우에는 '-skip-broadcast-domain-placement' 매개 변수를 'ifgrp add-port' 명령의 일부로 지정합니다.

에서 포트 인터페이스 그룹에 적용되는 및 구성 제한에 대해 자세히 `network port ifgrp add-port`"ONTAP 명령 참조입니다" 알아보십시오.

인터페이스 그룹 또는 **LAG**에서 포트를 제거합니다

인터페이스 그룹의 마지막 포트가 아닌 경우 LIF를 호스팅하는 인터페이스 그룹에서 포트를 제거할 수 있습니다. 인터페이스 그룹에서 마지막 포트를 제거하지 않는 점을 고려할 때 인터페이스 그룹이 LIF를 호스팅하거나 인터페이스 그룹이 LIF의 홈 포트가 아니어야 합니다. 그러나 마지막 포트를 제거하는 경우 먼저 인터페이스 그룹에서 LIF를 마이그레이션하거나 이동해야 합니다.

이 작업에 대해

인터페이스 그룹 또는 LAG에서 최대 16개의 포트(물리적 인터페이스)를 제거할 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- 시스템 관리자를 사용하여 LAG*에서 포트를 제거합니다

단계

1. LAG를 편집하려면 * 네트워크 > 이더넷 포트 > LAG * 를 선택합니다.
2. LAG에서 제거할 포트를 선택합니다.
3. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 인터페이스 그룹에서 포트를 제거합니다 *

단계

인터페이스 그룹에서 네트워크 포트 제거:

'network port ifgrp remove-port

에 대한 자세한 내용은 `network port ifgrp remove-port` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예는 a0a라는 인터페이스 그룹에서 포트 e0c를 제거하는 방법을 보여줍니다.

'network port ifgrp remove-port-node_cluster-1-01_-ifgrp_a0a_-port_e0c_'

인터페이스 그룹 또는 **LAG**를 삭제합니다

기본 물리적 포트에서 직접 LIF를 구성하거나 인터페이스 그룹, LAG 모드 또는 배포 기능을 변경하려는 경우 인터페이스 그룹 또는 LAG를 삭제할 수 있습니다.

시작하기 전에

- 인터페이스 그룹 또는 LAG가 LIF를 호스팅하지 않아야 합니다.
- 인터페이스 그룹 또는 LAG는 LIF의 홈 포트나 페일오버 타겟이 아니어야 합니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- 시스템 관리자를 사용하여 LAG * 를 삭제합니다

단계

1. LAG를 삭제하려면 * 네트워크 > 이더넷 포트 > LAG * 를 선택합니다.
2. 제거할 LAG를 선택합니다.
3. LAG를 삭제합니다.

CLI를 참조하십시오

- CLI를 사용하여 인터페이스 그룹을 삭제합니다 *

단계

interface group을 삭제하려면 network port ifgrp delete 명령을 사용한다.

에 대한 자세한 내용은 `network port ifgrp delete` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 a0b라는 인터페이스 그룹을 삭제하는 방법을 보여줍니다.

'network port ifgrp delete-node_cluster-1-01_-ifgrp_a0b_'

물리적 포트를 통해 **ONTAP VLAN**을 구성합니다

ONTAP의 VLAN을 사용하여 물리적 경계에 정의된 기존 브로드캐스트 도메인과 달리 스위치 포트 단위로 정의된 별도의 브로드캐스트 도메인을 생성하여 네트워크의 논리적 분할을 제공할 수 있습니다.

VLAN은 여러 물리적 네트워크 세그먼트에 걸쳐 있을 수 있습니다. VLAN에 속한 엔드스테이션은 기능 또는 애플리케이션에 의해 관련된다.

예를 들어, VLAN의 최종 스테이션은 엔지니어링 및 회계 등의 부서 또는 릴리스1 및 릴리스2와 같은 프로젝트별로 그룹화할 수 있습니다. 최종 스테이션의 물리적 근접성이 VLAN에 반드시 필요한 것은 아니므로, 최종 스테이션을 지리적으로 분산시키고 스위치 네트워크에 브로드캐스트 도메인을 포함할 수 있습니다.

ONTAP 9.14.1 및 9.13.1에서는 논리 인터페이스(LIF)에서 사용되지 않고 연결된 스위치에서 기본 VLAN 연결이 없는 태그가 지정되지 않은 포트는 저하된 것으로 표시됩니다. 이는 사용되지 않는 포트를 식별하는 데 도움이 되며, 서비스 중단을 나타내는 것은 아닙니다. 네이티브 VLAN은 ONTAP CFM 브로드캐스트와 같은 ifgrp 기반 포트에서 태그가 지정되지 않은 트래픽을 허용합니다. 태그가 지정되지 않은 트래픽이 차단되는 것을 방지하려면 스위치에 네이티브 VLAN을 구성합니다.

VLAN에 대한 정보를 생성, 삭제 또는 표시하여 VLAN을 관리할 수 있습니다.

스위치의 네이티브 VLAN과 ID가 동일한 네트워크 인터페이스에 VLAN을 생성해서는 안 됩니다. 예를 들어, 네트워크 인터페이스 e0b가 네이티브 VLAN 10에 있는 경우 해당 인터페이스에 VLAN e0b-10을 생성할 수 없습니다.

VLAN을 생성합니다

System Manager 또는 'network port vlan create' 명령을 사용하여 동일한 네트워크 도메인 내에서 별도의 브로드캐스트 도메인을 유지 관리하기 위한 VLAN을 생성할 수 있습니다.

시작하기 전에

다음 요구 사항이 충족되었는지 확인합니다.

- 네트워크에 배포된 스위치는 IEEE 802.1Q 표준을 준수하거나 공급업체별로 VLAN을 구현해야 합니다.
- 여러 VLAN을 지원하려면 하나 이상의 VLAN에 속하도록 최종 스테이션을 정적으로 구성해야 합니다.
- VLAN이 클러스터 LIF를 호스팅하는 포트에 연결되어 있지 않습니다.
- VLAN이 클러스터 IPspace에 할당된 포트에 연결되어 있지 않습니다.
- VLAN은 구성원 포트가 없는 인터페이스 그룹 포트에 생성되지 않습니다.

이 작업에 대해

VLAN을 생성하면 클러스터에 있는 지정된 노드의 네트워크 포트에 VLAN이 연결됩니다.

처음으로 포트를 통해 VLAN을 구성할 때 포트가 다운되어 일시적으로 네트워크 연결이 끊길 수 있습니다. 이후에 동일한 포트에 VLAN을 추가해도 포트 상태는 영향을 받지 않습니다.

> ⓘ 스위치의 네이티브 VLAN과 ID가 동일한 네트워크 인터페이스에 VLAN을 생성해서는 안 됩니다. 예를 들어, 네트워크 인터페이스 e0b가 네이티브 VLAN 10에 있는 경우 해당 인터페이스에 VLAN e0b-10을 생성할 수 없습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 VLAN * 을 생성합니다

ONTAP 9.12.0부터는 자동으로 브로드캐스트 도메인을 선택하거나 목록에서 On을 수동으로 선택할 수 있습니다. 이전에는 2계층 연결을 기반으로 브로드캐스트 도메인이 항상 자동으로 선택되었습니다. 브로드캐스트 도메인을 수동으로 선택하면 브로드캐스트 도메인을 수동으로 선택하면 연결이 끊기라는 경고가 나타납니다.

단계

1. 네트워크 > 이더넷 포트 > + VLAN * 을 선택합니다.
2. 드롭다운 목록에서 노드를 선택합니다.
3. 다음 중에서 선택합니다.
   a. ONTAP to * automatically select broadcast domain (recommended) *.
   b. 목록에서 브로드캐스트 도메인을 수동으로 선택합니다.
4. VLAN을 구성할 포트를 선택합니다.
5. VLAN ID를 지정합니다.
6. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 VLAN * 을 생성합니다

하드웨어 문제나 소프트웨어 구성 오류를 해결하지 않고 성능 저하 포트에 VLAN 포트를 생성하려면 네트워크 포트 수정 명령의 '-ignore-health-status' 매개변수를 TRUE로 설정해야 합니다.

에 대한 자세한 내용은 `network port modify` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 'network port vlan create' 명령어를 사용하여 VLAN을 생성한다.
2. VLAN을 생성할 때는 VLAN-name이나 port, vlan-id 옵션을 지정해야 합니다. VLAN 이름은 포트 이름(또는 인터페이스 그룹)과 네트워크 스위치 VLAN 식별자의 조합으로, 사이에 하이픈을 사용합니다. 예를 들어, "e0c-24"와 "e1c-80"은 유효한 VLAN 이름입니다.

다음 예에서는 노드 cluster-1-01의 네트워크 포트 e1c에 연결된 VLAN e1c-80을 생성하는 방법을 보여 줍니다.

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

ONTAP 9.8부터 VLAN은 생성 후 1분 정도 적절한 브로드캐스트 도메인에 자동으로 배치됩니다. ONTAP가 이 작업을 수행하지 않고 수동으로 VLAN을 브로드캐스트 도메인에 배치하려는 경우 "VLAN create" 명령의 일부로 '-skip-broadcast-domain-placement' 매개 변수를 지정합니다.

에 대한 자세한 내용은 `network port vlan create` "ONTAP 명령 참조입니다"을 참조하십시오.

VLAN을 편집합니다

브로드캐스트 도메인을 변경하거나 VLAN을 비활성화할 수 있습니다.

System Manager를 사용하여 VLAN을 편집합니다

ONTAP 9.12.0부터는 자동으로 브로드캐스트 도메인을 선택하거나 목록에서 On을 수동으로 선택할 수 있습니다. 이전의 브로드캐스트 도메인은 항상 계층 2 연결을 기반으로 자동으로 선택되었습니다. 브로드캐스트 도메인을 수동으로 선택하면 브로드캐스트 도메인을 수동으로 선택하면 연결이 끊기라는 경고가 나타납니다.

단계

1. 네트워크 > 이더넷 포트 > VLAN * 을 선택합니다.
2. 편집 아이콘을 선택합니다.
3. 다음 중 하나를 수행합니다.
   - 목록에서 다른 도메인을 선택하여 브로드캐스트 도메인을 변경합니다.
   - 사용 * 확인란의 선택을 취소합니다.
4. 변경 사항을 저장합니다.

VLAN을 삭제한다

NIC를 슬롯에서 제거하기 전에 VLAN을 삭제해야 할 수 있습니다. VLAN을 삭제하면 해당 VLAN을 사용하는 모든 페일오버 규칙 및 그룹에서 자동으로 제거됩니다.

시작하기 전에

VLAN에 연결된 LIF가 없는지 확인합니다.

이 작업에 대해

포트에서 마지막 VLAN을 삭제하면 네트워크에서 일시적으로 연결이 끊길 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 VLAN을 삭제합니다 *

단계

1. 네트워크 > 이더넷 포트 > VLAN * 을 선택합니다.
2. 제거할 VLAN을 선택합니다.
3. 삭제 * 를 클릭합니다.

CLI를 참조하십시오

- CLI를 사용하여 VLAN * 을 삭제합니다

단계

VLAN을 삭제하려면 network port vlan delete 명령을 사용한다.

다음 예에서는 노드 cluster-1-01의 네트워크 포트 e1c에서 VLAN e1c-80을 삭제하는 방법을 보여 줍니다.

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

에 대한 자세한 내용은 `network port vlan delete` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크 포트 특성을 수정합니다

물리적 네트워크 포트의 자동 협상, 이중, 흐름 제어, 속도 및 상태 설정을 수정할 수 있습니다.

시작하기 전에

수정할 포트가 LIF를 호스팅하지 않아야 합니다.

이 작업에 대해

- 100GbE, 40GbE, 10GbE 또는 1GbE 네트워크 인터페이스의 관리 설정을 수정하지 않는 것이 좋습니다.

  이중 모드 및 포트 속도에 대해 설정한 값을 관리 설정이라고 합니다. 네트워크 제한에 따라 관리 설정은 작동 설정과 다를 수 있습니다(즉, 포트가 실제로 사용하는 이중 모드 및 속도).

- 인터페이스 그룹에 있는 기본 물리적 포트의 관리 설정을 수정하지 않는 것이 좋습니다.

  '-up-admin' 매개 변수(고급 권한 수준에서 사용 가능)는 포트의 관리 설정을 수정합니다.

- 노드의 모든 포트 또는 노드의 마지막 운영 클러스터 LIF를 호스팅하는 포트에 대해 '-up-admin' 관리 설정을 false로 설정하지 않는 것이 좋습니다.
- 관리 포트 e0M의 MTU 크기를 수정하지 않는 것이 좋습니다.
- 브로드캐스트 도메인에 있는 포트의 MTU 크기는 브로드캐스트 도메인에 설정된 MTU 값에서 변경할 수 없습니다.
- VLAN의 MTU 크기는 기본 포트의 MTU 크기 값을 초과할 수 없습니다.

단계

1. 네트워크 포트의 속성을 수정합니다.

   네트워크 포트 수정

2. 시스템이 지정된 포트의 네트워크 포트 상태를 무시하도록 지정하려면 '-ignore-health-status' 필드를 true로 설정합니다.

   네트워크 포트 상태가 성능 저하에서 정상 상태로 자동으로 변경되고 이 포트를 LIF를 호스팅하는 데 사용할 수 있습니다. 클러스터 포트의 흐름 제어를 "없음"으로 설정해야 합니다. 기본적으로 흐름 제어는 'full'로 설정됩니다.

다음 명령을 실행하면 흐름 제어를 none으로 설정하여 포트 e0b의 흐름 제어가 비활성화됩니다.

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

에 대한 자세한 내용은 `network port modify` "ONTAP 명령 참조입니다"을 참조하십시오.

40GbE NIC 포트를 변환하여 **ONTAP** 네트워크용 **10GbE** 포트를 생성합니다

X1144A-R6 및 X91440A-R6 40GbE 네트워크 인터페이스 카드(NIC)를 4개의 10GbE 포트를 지원하도록 변환할 수 있습니다.

이러한 NIC 중 하나를 지원하는 하드웨어 플랫폼을 10GbE 클러스터 인터커넥트 및 고객 데이터 연결을 지원하는 클러스터에 연결하는 경우 NIC를 변환하여 필요한 10GbE 연결을 제공해야 합니다.

시작하기 전에

지원되는 브레이크아웃 케이블을 사용해야 합니다.

이 작업에 대해

NIC를 지원하는 전체 플랫폼 목록은 를 참조하십시오 "Hardware Universe".

> X1144A-R6 NIC에서는 포트 A만 10GbE 연결 4개를 지원하도록 변환할 수 있습니다. 포트 A가 변환되면 포트 e를 사용할 수 없습니다.

단계

1. 유지보수 모드로 전환합니다.
2. NIC를 40GbE 지원에서 10GbE 지원으로 변환합니다.

   ```
   nicadmin convert -m [40G | 10G] [port-name]
   ```

3. convert 명령을 사용한 후 노드를 중단한다.
4. 케이블을 설치하거나 변경합니다.
5. 하드웨어 모델에 따라 SP(서비스 프로세서) 또는 BMC(베이스보드 관리 컨트롤러)를 사용하여 변환을 적용하기 위해 노드 전원을 껐다가 켭니다.

ONTAP 네트워크를 위해 **UTA X1143A-R6** 포트를 구성합니다

기본적으로 X1143A-R6 유니파이드 타겟 어댑터는 FC 타겟 모드로 구성되지만, 포트를 10Gb 이더넷 및 FCoE(CNA) 포트 또는 16Gb FC 이니시에이터 또는 타겟 포트로 구성할 수 있습니다. 여기에는 다른 SFP+ 어댑터가 필요합니다.

이더넷 및 FCoE용으로 구성된 경우 X1143A-R6 어댑터는 동일한 10GbE 포트에서 동시 NIC 및 FCoE 타겟 트래픽을 지원합니다. FC용으로 구성한 경우 동일한 ASIC를 공유하는 각 2포트 쌍은 FC 타겟 또는 FC 이니시에이터 모드에 대해 개별적으로 구성할 수 있습니다. 즉, 단일 X1143A-R6 어댑터는 하나의 2포트 쌍에서 FC 타겟 모드를, 다른 2포트 쌍에서 FC 이니시에이터 모드를 지원할 수 있습니다. 동일한 ASIC에 연결된 포트 쌍은 같은 모드로 구성해야 합니다.

FC 모드에서 X1143A-R6 어댑터는 최대 16Gbps의 속도를 제공하는 기존 FC 장치와 동일하게 작동합니다. CNA 모드에서 X1143A-R6 어댑터를 사용하여 동일한 10GbE 포트를 공유하는 동시 NIC 및 FCoE 트래픽을 공유할 수 있습니다. CNA 모드는 FCoE 기능에 대해 FC 타겟 모드만 지원합니다.

통합 타겟 어댑터(X1143A-R6)를 구성하려면 동일한 퍼스낼리티 모드에서 동일한 칩에 두 개의 인접 포트를 구성해야 합니다.

단계

1. 포트 구성 보기:

```
system hardware unified-connect show
```

2. FC(Fibre Channel) 또는 CNA(Converged Network Adapter)에 필요한 포트를 구성합니다.

```
system node hardware unified-connect modify -node <node_name> -adapter
<adapter_name> -mode {fcp|cna}
```

3. FC 또는 10Gb 이더넷에 적합한 케이블을 연결합니다.
4. 올바른 SFP+가 설치되었는지 확인합니다.

```
network fcp adapter show -instance -node -adapter
```

CNA의 경우 10Gb 이더넷 SFP를 사용해야 합니다. FC의 경우 연결 중인 FC 패브릭을 기반으로 8Gb SFP 또는 16Gb SFP를 사용해야 합니다.

ONTAP 네트워크에서 사용할 **UTA2** 포트를 변환합니다

UTA2 포트를 CNA(Converged Network Adapter) 모드에서 파이버 채널(FC) 모드로 전환하거나 그 반대로 전환할 수 있습니다.

포트를 네트워크에 연결하거나 FC 이니시에이터 및 타겟을 지원하는 물리적 미디어를 변경해야 하는 경우 UTA2 속성을 CNA 모드에서 FC 모드로 변경해야 합니다.

CNA 모드에서 **FC** 모드로 전환

단계

1. 어댑터를 오프라인 상태로 전환:

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. 포트 모드를 변경합니다.

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode fcp
```

3. 노드를 재부팅한 다음 어댑터를 온라인 상태로 전환합니다.

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin up
```

4. 필요에 따라 관리자 또는 VIF 관리자에게 포트를 삭제하거나 제거하도록 알립니다.
   - 포트가 LIF의 홈 포트로 사용되고, 인터페이스 그룹(ifgrp) 또는 호스트 VLAN의 구성원인 경우 관리자는 다음을 수행해야 합니다.
     - LIF를 이동하거나, ifgrp에서 포트를 제거하거나, VLAN을 각각 삭제합니다.
     - 명령을 실행하여 포트를 수동으로 삭제합니다 `network port delete`. 명령이 실패하면 `network port delete` 관리자가 오류를 해결한 다음 명령을 다시 실행해야 합니다.
   - 포트가 LIF의 홈 포트로 사용되지 않고, ifgrp의 구성원이 아니며 VLAN을 호스팅하지 않는 경우, VIF 관리자는 재부팅 시 기록에서 포트를 제거해야 합니다. VIF 관리자가 포트를 제거하지 않는 경우, 관리자는 재부팅 후 명령을 사용하여 수동으로 포트를 제거해야 `network port delete` 합니다.

     에 대한 자세한 내용은 `network port delete` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 올바른 SFP+가 설치되었는지 확인합니다.

```
network fcp adapter show -instance -node -adapter
```

   CNA의 경우 10Gb 이더넷 SFP를 사용해야 합니다. FC의 경우 노드에서 구성을 변경하기 전에 8Gb SFP 또는 16Gb SFP를 사용해야 합니다.

FC 모드에서 **CNA** 모드로 전환합니다

단계

1. 어댑터를 오프라인 상태로 전환:

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. 포트 모드를 변경합니다.

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode cna
```

3. 노드를 재부팅합니다
4. 올바른 SFP+가 설치되었는지 확인합니다.

   CNA의 경우 10Gb 이더넷 SFP를 사용해야 합니다.

ONTAP 네트워크의 **CNA/UTA2** 광 모듈을 변환합니다

어댑터에 대해 선택한 퍼스낼리티 모드를 지원하도록 유니파이드 타겟 어댑터(CNA/UTA2)의 광 모듈을 변경해야 합니다.

단계

1. 카드에 사용된 현재 SFP+를 확인합니다. 그런 다음 기본 설정 특성(FC 또는 CNA)에 대해 현재 SFP+를 적절한 SFP+로 교체합니다.
2. X1143A-R6 어댑터에서 현재 광 모듈을 제거합니다.
3. 기본 퍼스낼리티 모드(FC 또는 CNA) 광학장치에 맞는 모듈을 삽입합니다.
4. 올바른 SFP+가 설치되었는지 확인합니다.

```
network fcp adapter show -instance -node -adapter
```

   지원되는 SFP+ 모듈 및 Cisco Twinax(Copper) 케이블이 에 나열되어 있습니다 "NetApp Hardware Universe를 참조하십시오".

ONTAP 클러스터 노드에서 **NIC** 제거

유지 관리를 위해 결함이 있는 NIC를 슬롯에서 제거하거나 NIC를 다른 슬롯으로 이동해야 할 수 있습니다.

NIC 제거 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 ONTAP 클러스터 노드에서 NIC를 제거해야 하는 경우 절차를 "노드에서 NIC 제거(ONTAP 9.7 이하)"참조하십시오.

단계

1. 노드 전원을 끕니다.

2. 슬롯에서 NIC를 물리적으로 분리합니다.
3. 노드의 전원을 켭니다.
4. 포트가 삭제되었는지 확인합니다.

```
network port show
```

ONTAP는 모든 인터페이스 그룹에서 포트를 자동으로 제거합니다. 포트가 인터페이스 그룹의 유일한 구성원인 경우 인터페이스 그룹이 삭제됩니다. 에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 포트에 구성된 VLAN이 있으면 포트가 교체된 것입니다. 다음 명령을 사용하여 교체된 VLAN을 볼 수 있습니다.

```
cluster controller-replacement network displaced-vlans show
```

dissplac된 interface show, dissplac된-vlan show, dissplac된-vLANs restore 명령은 고유하며 클러스터 컨트롤러 교체 네트워크로 시작하는 정규화된 명령 이름이 필요하지 않습니다.

6. 이러한 VLAN은 삭제되지만 다음 명령을 사용하여 복원할 수 있습니다.

```
displaced-vlans restore
```

7. 포트에 LIF가 구성되어 있는 경우 ONTAP는 동일한 브로드캐스트 도메인의 다른 포트에 있는 LIF에 대한 새 홈 포트를 자동으로 선택합니다. 동일한 파일러에 적절한 홈 포트가 없으면 해당 LIF가 교체된 것으로 간주됩니다. 다음 명령을 사용하여 교체된 LIF를 볼 수 있습니다.

   디시퍼인터페이스 쇼

8. 새 포트가 같은 노드의 브로드캐스트 도메인에 추가되면 LIF의 홈 포트가 자동으로 복원됩니다. 또는 네트워크 인터페이스 modify-home-port-home-node를 사용하여 홈 포트를 설정하거나 교체된 인터페이스 restore 명령을 사용할 수 있습니다.

관련 정보

- "클러스터 컨트롤러 교체 네트워크 - 인터페이스 삭제"
- "네트워크 인터페이스 수정"

네트워크 포트를 모니터링합니다

ONTAP 네트워크 포트의 상태를 모니터링합니다

ONTAP의 네트워크 포트 관리에는 자동 상태 모니터링 및 LIF 호스팅에 적합하지 않은 네트워크 포트를 식별하는 데 도움이 되는 상태 모니터링 세트가 포함됩니다.

이 작업에 대해

상태 모니터에서 네트워크 포트가 정상 상태가 아닌 것으로 확인되면 EMS 메시지를 통해 관리자에게 경고를

표시하거나 해당 포트를 성능 저하로 표시합니다. ONTAP는 해당 LIF에 대한 정상적인 대체 페일오버 대상이 있을 경우 성능이 저하된 네트워크 포트에서 LIF를 호스팅하지 않습니다. 링크 플래핑(링크가 위아래로 빠르게 튀어 나며 튀어 나며 튀어 나오는 경우) 또는 네트워크 파티셔닝과 같은 소프트 장애 이벤트로 인해 포트의 성능이 저하될 수 있습니다.

- 클러스터 IPspace의 네트워크 포트는 브로드캐스트 도메인의 다른 네트워크 포트에 대한 링크 플래핑 또는 L2(계층 2) 재연결이 끊어지면 성능이 저하된 것으로 표시됩니다.
- 클러스터 이외의 IPspace의 네트워크 포트는 링크 플래핑 기능이 있을 때 성능이 저하된 것으로 표시됩니다.

성능이 저하된 포트의 다음과 같은 동작을 알고 있어야 합니다.

- 성능이 저하된 포트는 VLAN 또는 인터페이스 그룹에 포함될 수 없습니다.

  인터페이스 그룹의 구성원 포트가 성능 저하로 표시되어 있지만 인터페이스 그룹이 계속 정상 상태로 표시되어 있는 경우 해당 인터페이스 그룹에서 LIF를 호스팅할 수 있습니다.

- LIF는 성능이 저하된 포트에서 정상 포트로 자동 마이그레이션됩니다.
- 페일오버 이벤트 중에 성능 저하된 포트는 페일오버 타겟으로 간주되지 않습니다. 정상 상태의 포트를 사용할 수 없는 경우 성능이 저하된 포트 호스트 LIF는 일반 페일오버 정책에 따라 작동합니다.
- LIF를 생성, 마이그레이션 또는 성능이 저하된 포트로 되돌릴 수 없습니다.

  네트워크 포트의 '상태 무시' 설정을 '참'으로 수정할 수 있습니다. 그런 다음 양호한 포트에서 LIF를 호스팅할 수 있습니다.

단계

1. 고급 권한 모드로 로그인합니다.

   ```
   set -privilege advanced
   ```

2. 네트워크 포트 상태 모니터링을 위해 활성화된 상태 모니터를 확인합니다.

   ```
   network options port-health-monitor show
   ```

   포트의 상태는 상태 모니터의 값에 의해 결정됩니다.

   ONTAP에서는 기본적으로 다음 상태 모니터를 사용할 수 있으며 사용하도록 설정되어 있습니다.

   - 링크 플래핑 상태 모니터: 링크 플래핑 모니터링

     포트에 5분 내에 두 번 이상 링크 플래핑이 있는 경우 이 포트는 성능 저하로 표시됩니다.

   - L2 연결 상태 모니터: 동일한 브로드캐스트 도메인에 구성된 모든 포트가 서로 L2 연결 가능 여부를 모니터링합니다

     이 상태 모니터는 모든 IPspace에서 L2 도달 가능성 문제를 보고하지만 클러스터 IPspace의 포트만 성능 저하로 표시합니다.

   - CRC 모니터: 포트에서 CRC 통계를 모니터링합니다

이 상태 모니터는 포트를 성능 저하로 표시하지 않지만 매우 높은 CRC 실패율이 관찰되면 EMS 메시지를 생성합니다.

에 대한 자세한 내용은 `network options port-health-monitor show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 'network options port-health-monitor modify' 명령을 사용하여 원하는 대로 IPspace에 대한 상태 모니터를 사용하거나 사용하지 않도록 설정합니다.

   에 대한 자세한 내용은 `network options port-health-monitor modify` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 포트의 세부 상태를 봅니다.

```
network port show -health
```

명령 출력에는 포트의 상태, '상태 무시' 설정 및 포트가 성능 저하로 표시된 이유 목록이 표시됩니다.

항만 건강상태는 건강하거나 등급이 매겨질 수 있다.

상태 무시 설정이 참이면 항만 상태가 평가됨에서 건강으로 변경되었음을 나타냅니다.

상태 무시 설정이 false이면 포트 상태는 시스템에 의해 자동으로 결정됩니다.

에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크 포트의 연결 상태를 모니터링합니다

내후성 모니터링은 ONTAP 9.8 이상에 내장되어 있습니다. 이 모니터링을 사용하여 물리적 네트워크 토폴로지가 ONTAP 구성과 일치하지 않는 시점을 식별할 수 있습니다. 경우에 따라 ONTAP에서 포트 연결을 복구할 수 있습니다. 다른 경우에는 추가 단계가 필요합니다.

이 작업에 대해

다음 명령을 사용하여 물리적 케이블 연결 또는 네트워크 스위치 구성과 일치하지 않는 ONTAP 구성에서 비롯되는 네트워크 구성 오류를 확인, 진단 및 복구할 수 있습니다.

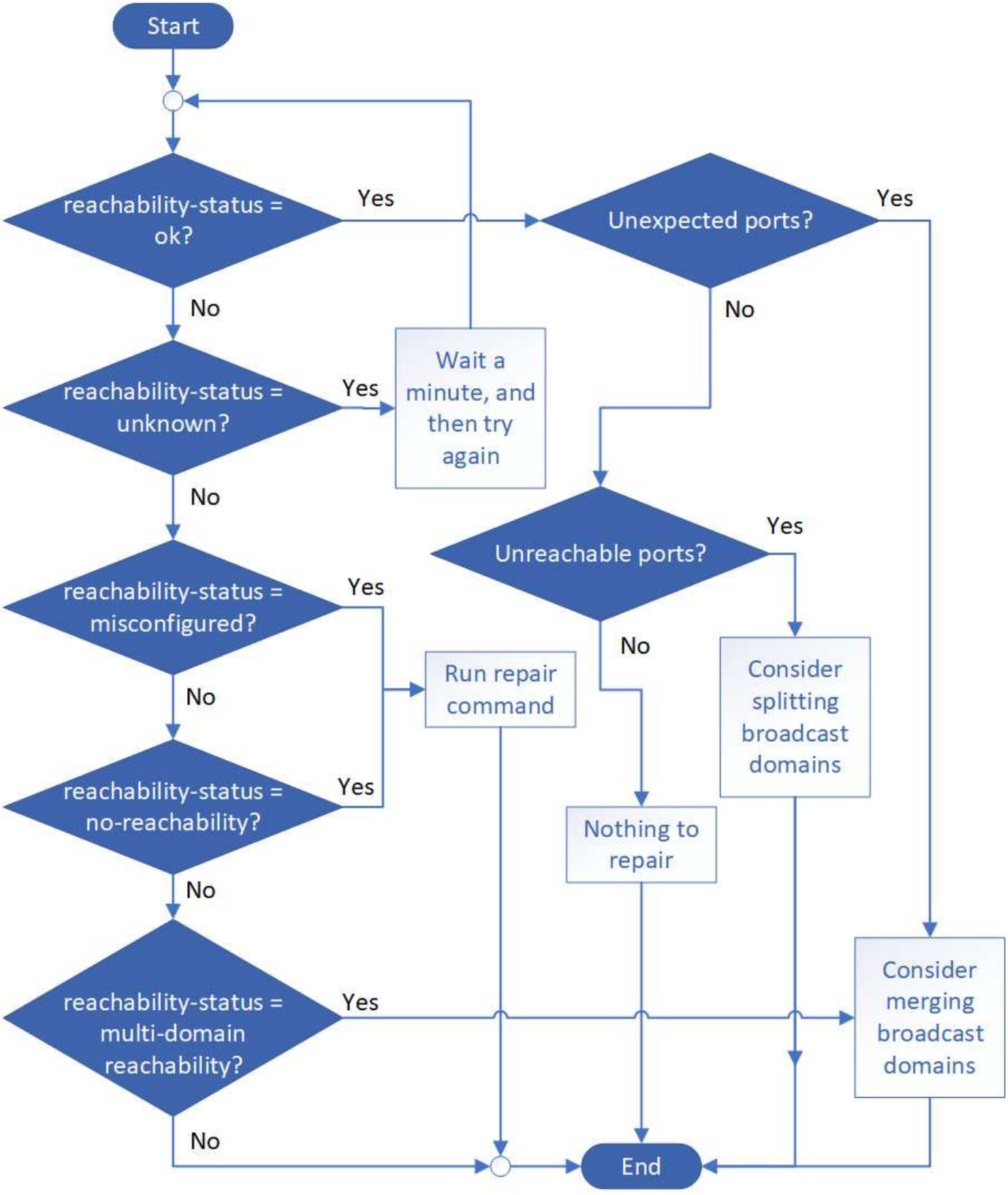
단계

1. 포트 도달 가능성 보기:

```
network port reachability show
```

   에 대한 자세한 내용은 `network port reachability show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 다음 진단트리와 테이블을 사용하여 다음 단계(있는 경우)를 결정합니다.


Start
reachability-status = ok?
Yes
Unexpected ports?
Yes
No
No
reachability-status = unknown?
Yes
Wait a minute, and then try again
No
Unreachable ports?
Yes
reachability-status = misconfigured?
Yes
No
Run repair command
Consider splitting broadcast domains
No
Nothing to repair
reachability-status = no-reachability?
Yes
No
reachability-status = multi-domain reachability?
Yes
Consider merging broadcast domains
No
End

도달 가능성 - 상태	설명

좋습니다	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있습니다. 도달 가능성 - 상태가 "정상"이지만 "예상치 못한 포트"가 있는 경우 하나 이상의 브로드캐스트 도메인을 병합하는 것이 좋습니다. 자세한 내용은 다음_예기치 않은 포트_행을 참조하십시오. 도달 가능성 - 상태가 "정상"이지만 "연결할 수 없는 포트"인 경우 하나 이상의 브로드캐스트 도메인을 분할하는 것이 좋습니다. 자세한 내용은 _Unreachable ports_row를 참조하십시오. 도달 가능성 - 상태가 "정상"이고 예기치 않거나 연결할 수 없는 포트가 없는 경우 구성이 올바른 것입니다.
예기치 않은 포트	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있지만 하나 이상의 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능도 있습니다. 물리적 연결 및 스위치 구성을 검사하여 올바르지 않거나 포트에 할당된 브로드캐스트 도메인을 하나 이상의 브로드캐스트 도메인과 병합해야 하는지 확인합니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 병합합니다".
연결할 수 없는 포트	단일 브로드캐스트 도메인이 두 개의 서로 다른 도달 가능성 집합으로 분할되는 경우, 브로드캐스트 도메인을 분할하여 ONTAP 구성을 물리적 네트워크 토폴로지와 동기화할 수 있습니다. 일반적으로 연결할 수 없는 포트 목록은 물리적 및 스위치 구성이 정확한지 확인한 후 다른 브로드캐스트 도메인으로 분할해야 하는 포트 집합을 정의합니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 분할합니다".
잘못 구성되었습니다. - 도달 가능성	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 없지만 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있습니다. 포트 연결을 복구할 수 있습니다. 다음 명령을 실행하면 시스템에서 해당 포트가 재연결 가능한 브로드캐스트 도메인에 포트를 할당합니다. 네트워크 포트 연결 복구 노드 포트 자세한 내용은 을 참조하십시오 "수리 포트 도달 가능성".
아니오 - 내 상태	이 포트에는 기존 브로드캐스트 도메인에 대한 계층 2 도달 기능이 없습니다. 포트 연결을 복구할 수 있습니다. 다음 명령을 실행하면 시스템이 기본 IPspace에서 자동으로 생성된 새 브로드캐스트 도메인에 포트를 할당합니다. `network port reachability repair -node -port` 자세한 내용은 을 "수리 포트 도달 가능성"참조하십시오. 에 대한 자세한 내용은 `network port reachability repair` "ONTAP 명령 참조입니다"을 참조하십시오.

다중 도메인 내의 도달 가능성	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있지만 하나 이상의 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능도 있습니다. 물리적 연결 및 스위치 구성을 검사하여 올바르지 않거나 포트에 할당된 브로드캐스트 도메인을 하나 이상의 브로드캐스트 도메인과 병합해야 하는지 확인합니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 병합합니다" 또는 "수리 포트 도달 가능성".
알 수 없음	도달 가능성 - 상태가 "알 수 없음"인 경우 몇 분 정도 기다린 후 명령을 다시 시도하십시오.

포트를 복구한 후에는 교체된 LIF 및 VLAN을 확인하고 해결해야 합니다. 포트가 인터페이스 그룹의 일부인 경우 해당 인터페이스 그룹의 변경 사항도 이해해야 합니다. 자세한 내용은 을 참조하십시오 "수리 포트 도달 가능성".

ONTAP 네트워크의 포트 사용에 대해 알아봅니다

잘 알려진 여러 포트가 특정 서비스와의 ONTAP 통신용으로 예약되어 있습니다. 스토리지 네트워크 환경의 포트 값이 ONTAP 포트의 값과 같으면 포트 충돌이 발생합니다.

인바운드 트래픽

ONTAP 스토리지의 인바운드 트래픽은 다음 프로토콜 및 포트를 사용합니다.

프로토콜	포트	목적
모든 ICMP	모두	인스턴스에 Ping을 수행 중입니다
TCP	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 대한 보안 셸 액세스
TCP	80	클러스터 관리 LIF의 IP 주소에 대한 웹 페이지 액세스
TCP/UDP입니다	111	rpcbind, NFS에 대한 원격 프로시저 호출
UDP입니다	123을 선택합니다	NTP, 네트워크 시간 프로토콜
TCP	135	MSRPC, Microsoft 원격 프로시저 호출
TCP	139	NetBIOS - SSN, CIFS에 대한 NetBIOS 서비스 세션입니다
TCP/UDP입니다	161-162 을 참조하십시오	SNMP, 단순 네트워크 관리 프로토콜
TCP	443	클러스터 관리 LIF의 IP 주소에 대한 웹 페이지 액세스를 보호합니다
TCP	445	MS Active Domain Services, NetBIOS 프레이밍이 있는 TCP 기반 Microsoft SMB/CIFS
TCP/UDP입니다	635	NFS 마운트로 원격 파일 시스템이 로컬인 것처럼 상호 작용합니다
TCP	749	Kerberos
UDP입니다	953	이름 데몬입니다
TCP/UDP입니다	2049	NFS 서버 데몬

TCP	2050	NRV, NetApp 원격 볼륨 프로토콜
TCP	3260	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP/UDP입니다	4045	NFS 잠금 데몬
TCP/UDP입니다	4046	NFS에 대한 네트워크 상태 모니터
UDP입니다	4049	NFS RPC 견적
UDP입니다	4444	KRB524, Kerberos 524
UDP입니다	5353	멀티캐스트 DNS
TCP	10000	NDMP(Network Data Management Protocol)를 사용한 백업
TCP	11104	SnapMirror용 클러스터 간 통신 세션의 클러스터 피어링, 양방향 관리
TCP	11105	클러스터 피어링, 양방향으로 SnapMirror 데이터를 통해 인터클러스터 LIF를 사용하여 전송
SSL/TLS	30000	보안 소켓(SSL/TLS)을 통해 DMA와 NDMP 서버 간의 NDMP 보안 제어 연결을 허용합니다. 보안 스캐너는 포트 30000의 취약점을 보고할 수 있습니다.

아웃바운드 트래픽

비즈니스 요구사항에 따라 ONTAP 스토리지의 아웃바운드 트래픽은 기본 규칙 또는 고급 규칙을 사용하여 설정할 수 있습니다.

기본 아웃바운드 규칙

ICMP, TCP 및 UDP 프로토콜을 통한 모든 아웃바운드 트래픽에 모든 포트를 사용할 수 있습니다.

프로토콜	포트	목적
모든 ICMP	모두	모든 아웃바운드 트래픽
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	모든 아웃바운드 트래픽

고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 ONTAP의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

Active Directory를 클릭합니다

프로토콜	포트	출처	목적지	목적
TCP	88	노드 관리 LIF, 데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트입니다	Kerberos V 인증
UDP입니다	137	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다

UDP입니다	138	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
TCP	139	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
TCP	389	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	LDAP를 지원합니다
UDP입니다	389	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	LDAP를 지원합니다
TCP	445	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
TCP	464	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 암호 변경 및 설정(set_change)
UDP입니다	464	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos 키 관리
TCP	749	노드 관리 LIF, 데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 암호 변경 및 설정(RPCSEC_GSS)

AutoSupport

프로토콜	포트	출처	목적지	목적
TCP	80	노드 관리 LIF	support.netapp.com	AutoSupport(전송 프로토콜이 HTTPS에서 HTTP로 변경된 경우에만 해당)

SNMP를 선택합니다

프로토콜	포트	출처	목적지	목적
TCP/UDP입니다	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링

SnapMirror를 참조하십시오

프로토콜	포트	출처	목적지	목적
TCP	11104	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리

기타 서비스

프로토콜	포트	출처	목적지	목적
TCP	25	노드 관리 LIF	메일 서버	AutoSupport에 사용할 수 있는 SMTP 경고

UDP입니다	53	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
UDP입니다	67	노드 관리 LIF	DHCP를 선택합니다	DHCP 서버
UDP입니다	68	노드 관리 LIF	DHCP를 선택합니다	처음으로 설정하는 DHCP 클라이언트
UDP입니다	514	노드 관리 LIF	Syslog 서버	Syslog 메시지를 전달합니다
TCP	5010	인터클러스터 LIF	엔드포인트 백업 또는 복원	S3로 백업 기능의 백업 및 복원 작업
TCP	18600 - 18699	노드 관리 LIF	대상 서버	NDMP 복제

ONTAP 내부 포트에 대해 알아봅니다

다음 표는 ONTAP이 내부적으로 사용하는 포트와 그 기능을 나열합니다. ONTAP은 이러한 포트를 클러스터 내 LIF 통신 설정과 같은 다양한 기능에 사용합니다.

이 목록은 모든 내용을 담고 있지 않으며 환경에 따라 달라질 수 있습니다.

포트/프로토콜	구성 요소/기능
514	Syslog를 클릭합니다
900	NetApp 클러스터 RPC
902	NetApp 클러스터 RPC
904	NetApp 클러스터 RPC
905	NetApp 클러스터 RPC
910	NetApp 클러스터 RPC
911	NetApp 클러스터 RPC
913	NetApp 클러스터 RPC
914	NetApp 클러스터 RPC
915	NetApp 클러스터 RPC
918	NetApp 클러스터 RPC
920	NetApp 클러스터 RPC
921)를 참조하십시오	NetApp 클러스터 RPC
924	NetApp 클러스터 RPC
925	NetApp 클러스터 RPC
927)를 참조하십시오	NetApp 클러스터 RPC
928	NetApp 클러스터 RPC
929)를 누릅니다	NetApp 클러스터 RPC

930	커널 서비스 및 관리 기능(KSMF)
931	NetApp 클러스터 RPC
932	NetApp 클러스터 RPC
933	NetApp 클러스터 RPC
934	NetApp 클러스터 RPC
935	NetApp 클러스터 RPC
936	NetApp 클러스터 RPC
937	NetApp 클러스터 RPC
939	NetApp 클러스터 RPC
940	NetApp 클러스터 RPC
951을 참조하십시오	NetApp 클러스터 RPC
954를 참조하십시오	NetApp 클러스터 RPC
955	NetApp 클러스터 RPC
956을 참조하십시오	NetApp 클러스터 RPC
958	NetApp 클러스터 RPC
961	NetApp 클러스터 RPC
963	NetApp 클러스터 RPC
964	NetApp 클러스터 RPC
966	NetApp 클러스터 RPC
967	NetApp 클러스터 RPC
975	키 관리 상호 운용성 프로토콜(KMIP)
982	NetApp 클러스터 RPC
983	NetApp 클러스터 RPC
5125	디스크의 대체 제어 포트
5133	디스크의 대체 제어 포트
5144	디스크의 대체 제어 포트
65502	노드 범위 SSH
65503	LIF 공유
7700	클러스터 세션 관리자(CSM)
7810)를 참조하십시오	NetApp 클러스터 RPC
7811	NetApp 클러스터 RPC
7812)를 참조하십시오	NetApp 클러스터 RPC
7813)를 참조하십시오	NetApp 클러스터 RPC
7814)를 참조하십시오	NetApp 클러스터 RPC

7815)를 참조하십시오	NetApp 클러스터 RPC
7816	NetApp 클러스터 RPC
7817	NetApp 클러스터 RPC
7818)를 참조하십시오	NetApp 클러스터 RPC
7819)를 참조하십시오	NetApp 클러스터 RPC
7820)를 참조하십시오	NetApp 클러스터 RPC
7821)를 참조하십시오	NetApp 클러스터 RPC
7822)를 참조하십시오	NetApp 클러스터 RPC
7823)를 참조하십시오	NetApp 클러스터 RPC
7824)를 참조하십시오	NetApp 클러스터 RPC
7835-7839 및 7845-7849	클러스터 내부 통신을 위한 TCP 포트
8023	노드 범위 텔넷
8443	Amazon FSx용 ONTAP S3 NAS 포트
8514	노드 범위 RSH
9877	KMIP 클라이언트 포트(내부 로컬 호스트만 해당)
10006	HA 상호 연결 통신을 위한 TCP 포트

IPspace

ONTAP IPspace 구성에 대해 자세히 알아보십시오

IPspace를 사용하면 단일 ONTAP 클러스터를 구성하여 클라이언트가 동일한 IP 주소 서브넷 범위를 사용 중인 경우에도 관리를 목적으로 서로 다른 여러 네트워크 도메인의 클라이언트에서 액세스할 수 있습니다. 이를 통해 개인 정보 보호와 보안을 위해 클라이언트 트래픽을 분리할 수 있습니다.

IPspace는 SVM(스토리지 가상 머신)이 상주하는 고유 IP 주소 공간을 정의합니다. IPspace에 정의된 포트 및 IP 주소는 해당 IPspace 내에서만 적용 가능합니다. IPspace 내에서 각 SVM에 대해 별개의 라우팅 테이블이 유지되므로 교차 SVM 또는 교차 IPspace 트래픽 라우팅이 발생하지 않습니다.

IPspace는 라우팅 도메인에서 IPv4 및 IPv6 주소를 모두 지원합니다.

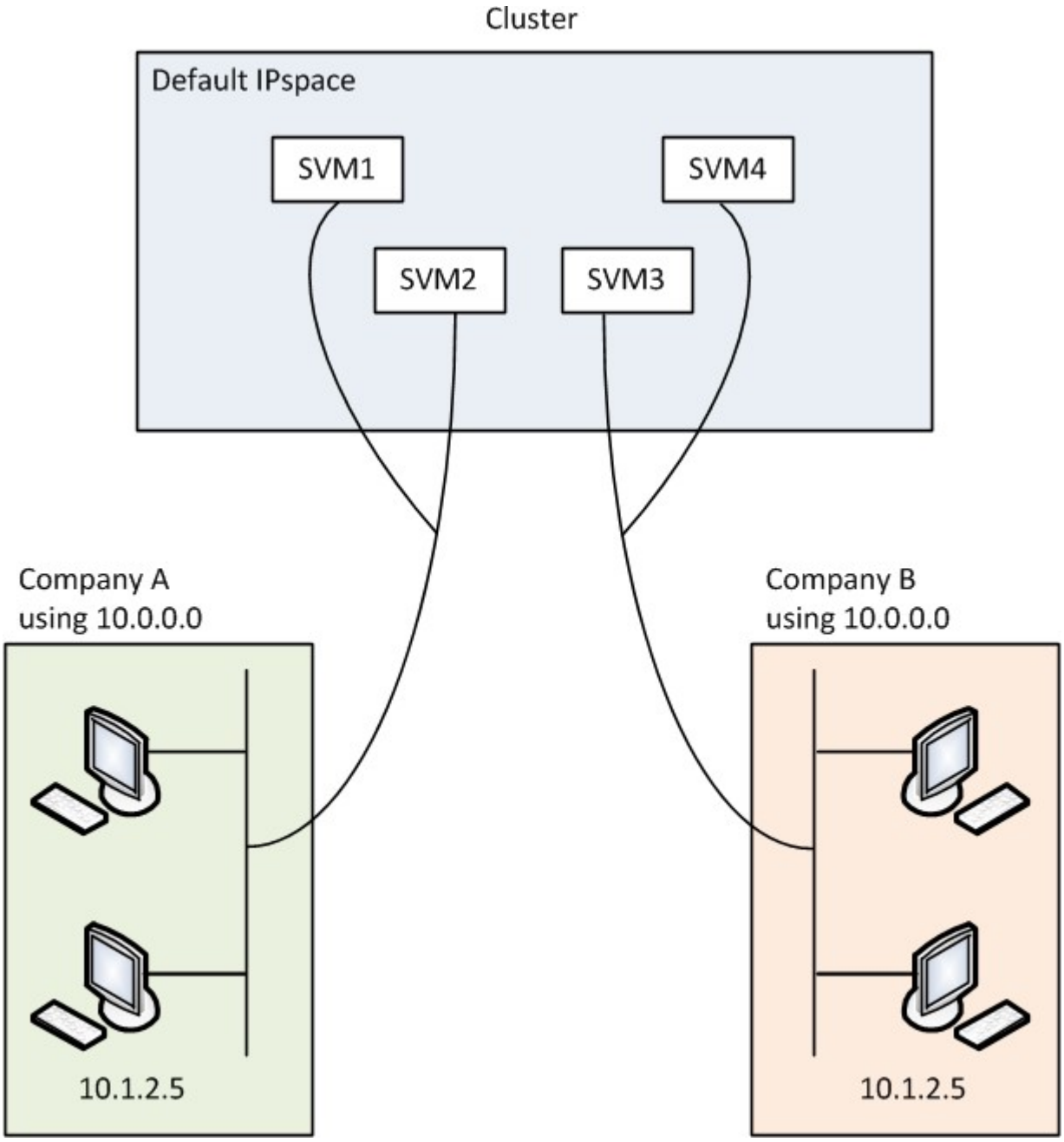
단일 조직의 스토리지를 관리하는 경우 IPspace를 구성할 필요가 없습니다. 단일 ONTAP 클러스터에서 여러 회사의 스토리지를 관리하는 경우 충돌하는 네트워킹 구성이 없을 수도 있으므로 IPspace를 사용할 필요가 없습니다. 대부분의 경우, 고유한 IP 라우팅 테이블을 사용하는 SVM(스토리지 가상 머신)을 사용하여 IPspace를 사용하는 대신 고유한 네트워킹 구성을 분리할 수 있습니다.

IPspace 사용 예

IPspace를 사용하는 일반적인 애플리케이션 은 SSP(스토리지 서비스 공급자)에서 SSP(회사 A)와 B의 고객을 SSP 단지의 ONTAP 클러스터에 연결해야 하며, 두 회사 모두 동일한 프라이빗 IP 주소 범위를 사용합니다.

SSP는 각 고객에 대해 클러스터에 SVM을 생성하고 두 SVM에서 회사 A의 네트워크 및 다른 두 SVM에서 회사 B의 네트워크로 전용 네트워크 경로를 제공합니다.

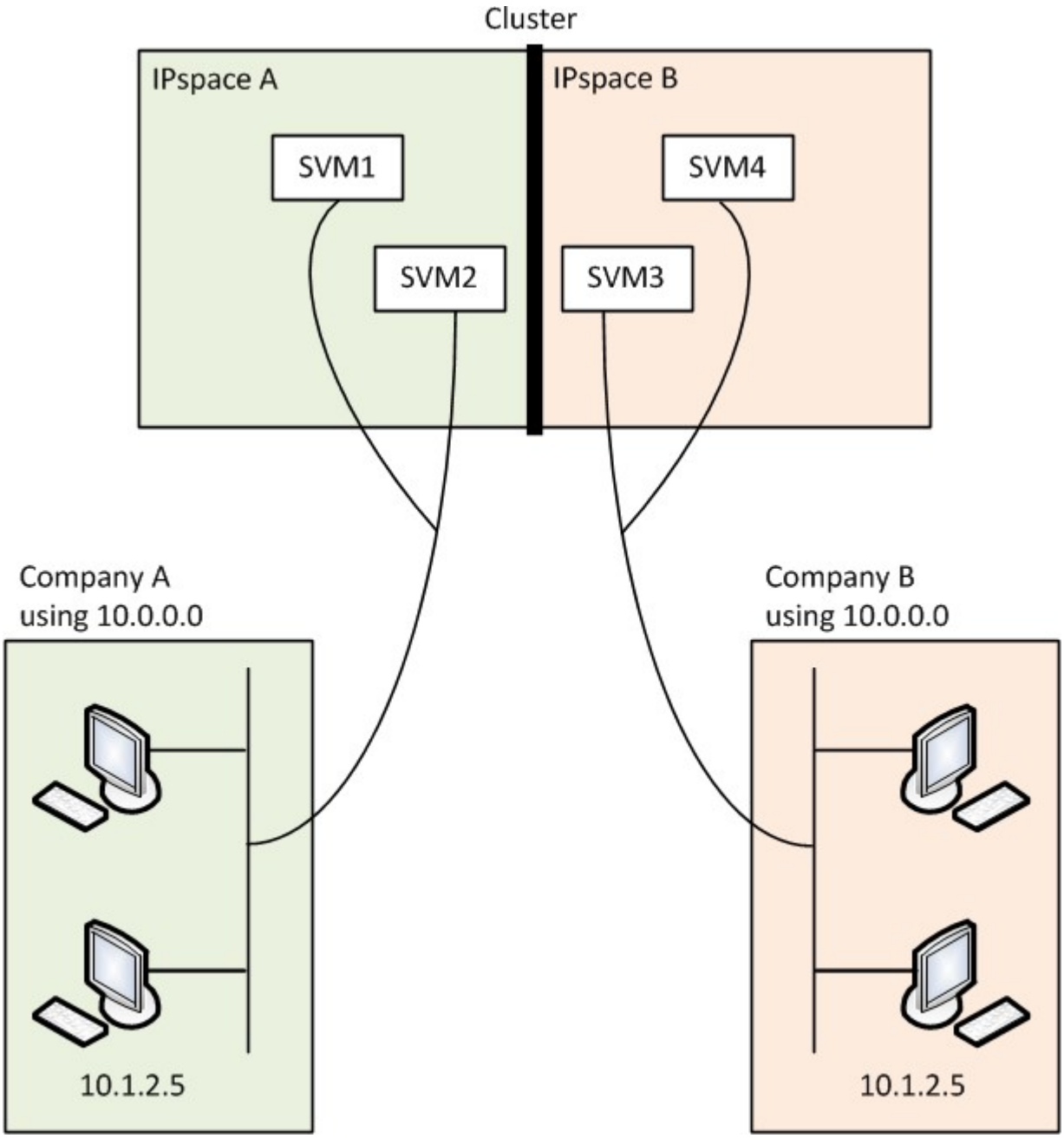
이 유형의 배포는 다음 그림에 나와 있으며 두 회사 모두 비전용 IP 주소 범위를 사용하는 경우 작동합니다. 그러나 그림에서는 문제를 일으키는 동일한 개인 IP 주소 범위를 사용하는 두 회사를 보여 줍니다.



두 회사 모두 전용 IP 주소 서브넷 10.0.0.0을 사용하므로 다음과 같은 문제가 발생합니다.

- 두 회사 모두 해당 SVM에 동일한 IP 주소를 사용하기로 결정한 경우 SSP 위치의 클러스터에 있는 SVM에서 IP 주소가 서로 충돌합니다.
- 두 회사가 SVM에 서로 다른 IP 주소를 사용하는 데 동의하더라도 문제가 발생할 수 있습니다.
- 예를 들어, A의 네트워크에 있는 클라이언트의 IP 주소가 B의 네트워크에 있는 클라이언트와 동일한 경우, A의 주소 공간에 있는 클라이언트에 대한 패킷은 B의 주소 공간에 있는 클라이언트로 라우팅될 수 있으며 그 반대의 경우도 마찬가지입니다.

- 두 회사가 상호 배타적인 주소 공간을 사용하기로 결정한 경우(예: A는 10.0.0.0, 네트워크 마스크 255.128.0.0, B는 10.128.0.0, 네트워크 마스크 255.128.0.0 사용), SSP는 트래픽을 A 및 B의 네트워크에 적절하게 라우팅하도록 클러스터의 정적 경로를 구성해야 합니다.
- 이 솔루션은 고정 경로로 인해 확장성이 뛰어나도 보안이 보장되지 않습니다.(브로드캐스트 트래픽이 클러스터의 모든 인터페이스로 전송됨) 이러한 문제를 해결하기 위해 SSP는 클러스터에서 2개의 IPspace를 정의합니다(각 회사당 하나씩). IPspace 트래픽이 라우팅되지 않기 때문에 다음 그림과 같이 모든 SVM이 10.0.0.0 주소 공간에 구성되어 있어도 각 회사의 데이터가 해당 네트워크로 안전하게 라우팅됩니다.



또한, '/etc/hosts' 파일, '/etc/hosts.equv' 파일 및 '/etc/rc' 파일과 같은 다양한 구성 파일에서 참조하는 IP 주소는 해당 IPspace와 관련이 있습니다. 따라서 IPspace를 사용하면 SSP에서 여러 SVM에 대한 구성 및 인증 데이터에 대해 충돌 없이 동일한 IP 주소를 구성할 수 있습니다.

IPspace의 표준 속성

특수 IPspace는 클러스터를 처음 생성할 때 기본적으로 생성됩니다. 또한 IPspace별로 특수 스토리지 가상 머신(SVM)을 생성합니다.

2개의 IPspace가 클러스터 초기화 시 자동으로 생성됨:

- "기본" IPspace

  이 IPspace는 포트, 서브넷 및 SVM에서 데이터를 제공하는 컨테이너입니다. 클라이언트에 대해 별도의 IPspace가 필요 없는 경우 이 IPspace에서 모든 SVM을 생성할 수 있습니다. 이 IPspace는 클러스터 관리 및 노드 관리 포트도 포함합니다.

- "클러스터" IPspace

  이 IPspace는 클러스터 내의 모든 노드에 있는 클러스터 포트를 모두 포함하고 있습니다. 이 생성된 클러스터는 클러스터 생성 시 자동으로 생성됩니다. 내부 프라이빗 클러스터 네트워크에 대한 연결을 제공합니다. 추가 노드가 클러스터에 추가될 때 해당 노드의 클러스터 포트가 "클러스터" IPspace에 추가됩니다.

IPspace별로 존재하는 "시스템" SVM IPspace를 생성하는 경우 동일한 이름의 기본 시스템 SVM이 생성됩니다.

- 내부 프라이빗 클러스터 네트워크에서 클러스터 노드 간에 클러스터 트래픽을 전달하는 "클러스터" IPspace용 시스템 SVM

  클러스터 관리자가 관리하며 "Cluster"라는 이름이 있습니다.

- 클러스터 간 트래픽을 포함하여 클러스터 및 노드에 대한 관리 트래픽을 전달하는 "기본" IPspace용 시스템 SVM

  클러스터 관리자가 관리하며 클러스터와 동일한 이름을 사용합니다.

- 생성한 사용자 지정 IPspace용 시스템 SVM은 해당 SVM에 대한 관리 트래픽을 전달

  클러스터 관리자가 관리하며 IPspace와 동일한 이름을 사용합니다.

IPspace에 클라이언트용 SVM이 하나 이상 존재할 수 있습니다. 각 클라이언트 SVM은 자체 데이터 볼륨 및 구성을 제공하며 다른 SVM과 독립적으로 관리됩니다.

ONTAP 네트워크용 IPspace를 생성합니다

IPspace는 SVM(스토리지 가상 머신)이 상주하는 고유 IP 주소 공간입니다. 안전한 스토리지, 관리 및 라우팅을 위해 SVM이 필요한 경우 IPspace를 생성할 수 있습니다. IPspace를 사용하여 클러스터의 각 SVM에 대해 별개의 IP 주소 공간을 생성할 수 있습니다. 이렇게 하면 관리자가 별도의 네트워크 도메인에 있는 클라이언트가 동일한 IP 주소 서브넷 범위의 중복 IP 주소를 사용하면서 클러스터 데이터에 액세스할 수 있습니다.

이 작업에 대해

512개의 IPspace를 클러스터 전체에서 사용할 수 있습니다. 6GB의 RAM이 있는 노드를 포함하는 클러스터의 경우 클러스터 전체 제한이 256개의 IPspace로 줄어듭니다. 플랫폼에 추가적인 제한이 적용되는지 확인하려면 Hardware Universe를 참조하십시오.

"NetApp Hardware Universe를 참조하십시오"

"ALL"이 시스템 예약 이름이므로 IPspace 이름은 "ALL"일 수 없습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. IPspace 생성:

```
network ipspace create -ipspace ipspace_name
```

IPSpace_name은 만들려는 IPspace의 이름입니다. 다음 명령을 실행하면 클러스터에서 IPspace ipspace1 이 생성됩니다.

```
network ipspace create -ipspace ipspace1
```

에 대한 자세한 내용은 `network ipspace create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. IPspace 표시:

네트워크 IPspace 쇼

```
IPspace              Vserver List          Broadcast Domains
-------------------- --------------------- ----------------------------
Cluster              Cluster               Cluster
Default              Cluster1              Default
ipspace1             ipspace1              -
```

IPspace용 시스템 SVM과 함께 IPspace가 생성됨 시스템 SVM은 관리 트래픽을 전달합니다.

작업을 마친 후

MetroCluster 구성으로 클러스터에서 IPspace를 생성하는 경우 파트너 클러스터로 IPspace 객체를 수동으로 복제해야 합니다. IPspace가 복제되기 전에 IPspace에 생성 및 할당된 SVM은 파트너 클러스터에 복제되지 않습니다.

브로드캐스트 도메인은 "기본" IPspace에서 자동으로 생성되며 다음 명령을 사용하여 IPspace 간에 이동할 수 있습니다.

```
network port broadcast-domain move
```

예를 들어, 다음 명령을 사용하여 브로드캐스트 도메인을 "Default"에서 "IPS1"으로 이동하려는 경우:

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

ONTAP 네트워크에서 IPspace를 확인합니다

클러스터에 존재하는 IPspace 목록을 표시할 수 있으며 SVM(스토리지 가상 머신), 브로드캐스트 도메인 및 각 IPspace에 할당된 포트를 볼 수 있습니다.

단계

클러스터에서 IPspace 및 SVM 표시:

```
network ipspace show [-ipspace ipspace_name]
```

다음 명령을 실행하면 클러스터에서 모든 IPspace, SVM 및 브로드캐스트 도메인이 표시됩니다.

```
network ipspace show
IPspace        Vserver List             Broadcast Domains
-------------  -----------------------  -------------------
Cluster
               Cluster                  Cluster
Default
               vs1, cluster-1            Default
ipspace1
               vs3, vs4, ipspace1       bcast1
```

다음 명령을 실행하면 IPspace 1의 일부인 노드 및 포트가 표시됩니다.

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

에 대한 자세한 내용은 `network ipspace show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크에서 IPspace를 삭제합니다

IPspace가 더 이상 필요하지 않은 경우 삭제할 수 있습니다.

시작하기 전에

삭제할 IPspace와 연결된 브로드캐스트 도메인, 네트워크 인터페이스 또는 SVM이 없어야 합니다.

시스템 정의 "기본" 및 "클러스터" IPspace는 삭제할 수 없습니다.

단계

IPspace 삭제:

```
network ipspace delete -ipspace ipspace_name
```

다음 명령을 실행하면 클러스터에서 IPspace ipspace1 이 삭제됩니다.

```
network ipspace delete -ipspace ipspace1
```

에 대한 자세한 내용은 `network ipspace delete` "ONTAP 명령 참조입니다"을 참조하십시오.

브로드캐스트 도메인

ONTAP 브로드캐스트 도메인에 대해 알아봅니다

브로드캐스트 도메인은 동일한 계층 2 네트워크에 속하는 네트워크 포트를 그룹화하는 데 사용됩니다. 그런 다음 SVM(스토리지 가상 시스템)에서 그룹의 포트를 사용하여 데이터 또는 관리 트래픽을 처리할 수 있습니다.

> ⓘ 브로드캐스트 도메인의 관리는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 브로드캐스트 도메인을 관리해야 하는 경우 을 참조하십시오"브로드캐스트 도메인 개요(ONTAP 9.7 이하)".

브로드캐스트 도메인은 IPspace에 상주합니다. 클러스터 초기화 중에 시스템은 두 개의 기본 브로드캐스트 도메인을 생성합니다.

- "기본" 브로드캐스트 도메인에는 "기본" IPspace에 있는 포트가 포함되어 있습니다.

  이러한 포트는 주로 데이터를 제공하는 데 사용됩니다. 클러스터 관리 및 노드 관리 포트도 이 브로드캐스트 도메인에 있습니다.

- "클러스터" 브로드캐스트 도메인에는 "클러스터" IPspace에 있는 포트가 포함되어 있습니다.

  이러한 포트는 클러스터 통신에 사용되며 클러스터의 모든 노드에 있는 모든 클러스터 포트를 포함합니다.

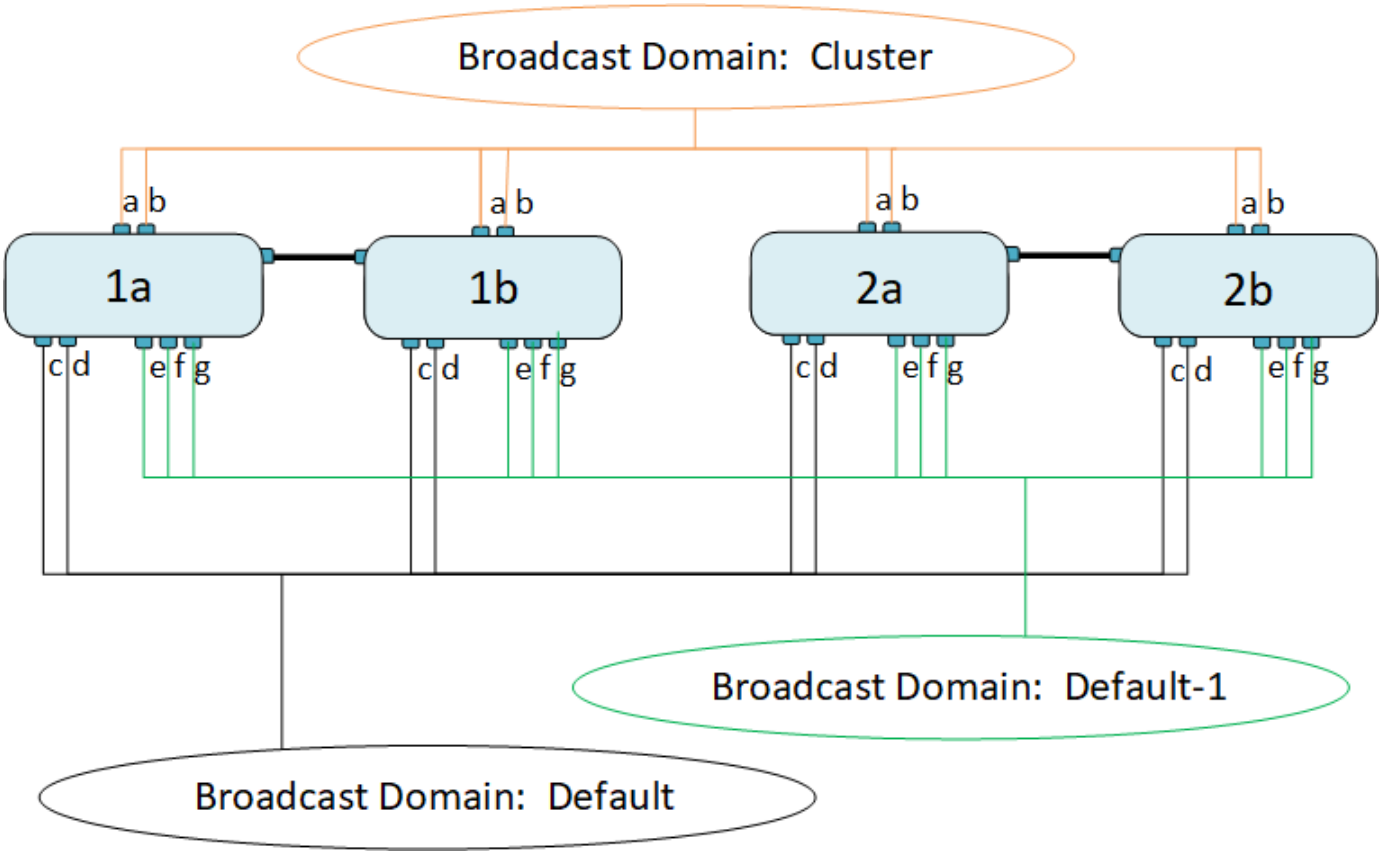
  필요한 경우 시스템이 기본 IPspace에 추가 브로드캐스트 도메인을 생성합니다. "기본" 브로드캐스트 도메인에는 관리 LIF의 홈 포트와 계층 2의 기능이 있는 다른 포트가 포함됩니다. 추가 브로드캐스트 도메인 이름은 "Default-1", "Default-2" 등으로 지정됩니다.

브로드캐스트 도메인 사용 예

브로드캐스트 도메인은 동일한 IPspace에서 네트워크 포트 집합으로, 일반적으로 클러스터에 있는 여러 노드의 포트를 포함하여 계층 2 상호 도달 기능을 가지고 있습니다.

그림에서는 4노드 클러스터의 3개 브로드캐스트 도메인에 할당된 포트를 보여 줍니다.

- "클러스터" 브로드캐스트 도메인은 클러스터 초기화 중에 자동으로 생성되며, 클러스터의 각 노드에서 포트 a와 b를 포함합니다.
- "Default" 브로드캐스트 도메인은 클러스터 초기화 중에 자동으로 생성되며, 클러스터의 각 노드에서 c 및 d 포트를 포함합니다.
- 시스템은 계층 2 네트워크 내 기능을 기반으로 클러스터 초기화 중에 추가 브로드캐스트 도메인을 자동으로 생성합니다. 이러한 추가 브로드캐스트 도메인은 Default-1, Default-2 등으로 명명됩니다.



각 브로드캐스트 도메인과 동일한 네트워크 포트를 가진 동일한 이름의 페일오버 그룹이 자동으로 생성됩니다. 이 페일오버 그룹은 시스템에서 자동으로 관리됩니다. 즉, 포트가 브로드캐스트 도메인에서 추가되거나 제거될 때 포트가 이 페일오버 그룹에서 자동으로 추가 또는 제거됩니다.

ONTAP 브로드캐스트 도메인을 생성합니다

브로드캐스트 도메인은 동일한 계층 2 네트워크에 속한 클러스터의 네트워크 포트를 그룹화합니다. 그런 다음 SVM에서 포트를 사용할 수 있습니다.

브로드캐스트 도메인은 클러스터 생성 또는 연결 작업 중에 자동으로 생성됩니다. ONTAP 9.12.0부터는 자동으로 생성된 브로드캐스트 도메인 외에도 시스템 관리자에서 수동으로 브로드캐스트 도메인을 추가할 수 있습니다.

브로드캐스트 도메인을 만드는 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 브로드캐스트 도메인을 만들어야 하는 경우 을 참조하십시오"브로드캐스트 도메인 생성(ONTAP 9.7 이하)".

시작하기 전에

브로드캐스트 도메인에 추가할 포트는 다른 브로드캐스트 도메인에 속하지 않아야 합니다. 사용하려는 포트가 다른 브로드캐스트 도메인에 속하지만 사용되지 않는 경우 원래 브로드캐스트 도메인에서 해당 포트를 제거합니다.

이 작업에 대해

- 모든 브로드캐스트 도메인 이름은 IPspace 내에서 고유해야 합니다.
- 브로드캐스트 도메인에 추가되는 포트는 물리적 네트워크 포트, VLAN 또는 링크 집계 그룹/인터페이스 그룹(LAG/ifgrp)일 수 있습니다.
- 사용하려는 포트가 다른 브로드캐스트 도메인에 속하지만 사용되지 않는 경우 새 브로드캐스트 도메인에 추가하기 전에 기존 브로드캐스트 도메인에서 제거하십시오.
- 브로드캐스트 도메인에 추가된 포트의 MTU(Maximum Transmission Unit)가 브로드캐스트 도메인에 설정된 MTU 값으로 업데이트됩니다.
- MTU 값은 e0M 포트 처리 관리 트래픽을 제외하고 해당 계층 2 네트워크에 연결된 모든 장치와 일치해야 합니다.
- IPspace 이름을 지정하지 않으면 브로드캐스트 도메인이 "기본" IPspace에 생성됩니다.

시스템 구성을 더 쉽게 하기 위해 같은 이름의 페일오버 그룹이 자동으로 생성되어 동일한 포트가 포함되어 있습니다.

시스템 관리자

단계

1. 네트워크 > 개요 > 브로드캐스트 도메인 * 을 선택합니다.
2. 을 클릭합니다 + Add
3. 브로드캐스트 도메인의 이름을 지정합니다.
4. MTU를 설정합니다.
5. IPspace를 선택합니다.
6. 브로드캐스트 도메인을 저장합니다.

브로드캐스트 도메인을 추가한 후에는 해당 도메인을 편집하거나 삭제할 수 있습니다.

CLI를 참조하십시오

ONTAP 9.8 이상을 사용 중인 경우, 레이어 2 접근성에 따라 브로드캐스트 도메인이 자동으로 생성됩니다. 자세한 내용은 을 참조하십시오 "수리 포트 도달 가능성".

브로드캐스트 도메인을 수동으로 만들 수도 있습니다.

단계

1. 브로드캐스트 도메인에 현재 할당되지 않은 포트 보기:

   네트워크 포트 쇼

   디스플레이가 큰 경우 네트워크 포트 show-broadcast-domain 명령을 사용하여 할당되지 않은 포트만 봅니다.

2. 브로드캐스트 도메인 생성:

   'network port broadcast-domain create-broadcast-domain_domain_name_-MTU_MTU_value_[-IPSpace_IPSpace_name_][-ports_ports_list_]'

   a. broadcast_domain_name은 만들려는 브로드캐스트 도메인의 이름입니다.
   b. mtu_value는 IP 패킷의 MTU 크기이고 1500 및 9000은 일반적인 값입니다.

      이 값은 이 브로드캐스트 도메인에 추가되는 모든 포트에 적용됩니다.

   c. IPSpace_name은 이 브로드캐스트 도메인을 추가할 IPspace의 이름입니다.

      이 매개 변수에 값을 지정하지 않으면 "기본" IPspace가 사용됩니다.

   d. port_list는 브로드캐스트 도메인에 추가될 포트의 목록입니다.

      포트는 노드1:e0c 등의 노드_이름:포트_번호 형식으로 추가됩니다.

3. 브로드캐스트 도메인이 원하는 대로 생성되었는지 확인합니다.

   'network port show-instance-broadcast-domain new_domain'

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 명령은 기본 IPspace에서 브로드캐스트 도메인 bcast1을 생성하고 MTU를 1500으로 설정하고 포트 4개를 추가합니다.

'network port broadcast-domain create-broadcast-domain_bcast1_-mtu_1500_-ports_cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f_'

에 대한 자세한 내용은 `network port broadcast-domain create` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

서브넷을 생성하여 브로드캐스트 도메인에서 사용할 IP 주소 풀을 정의하거나, 현재 IPspace에 SVM 및 인터페이스를 할당할 수 있습니다. 자세한 내용은 을 "클러스터 및 SVM 피어링"참조하십시오.

기존 브로드캐스트 도메인의 이름을 변경해야 할 경우 'network port broadcast-domain rename' 명령어를 사용한다.

에 대한 자세한 내용은 `network port broadcast-domain rename` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 브로드캐스트 도메인에서 포트를 추가하거나 제거합니다

브로드캐스트 도메인은 클러스터 생성 또는 연결 작업 중에 자동으로 생성됩니다. 브로드캐스트 도메인에서 포트를 수동으로 제거할 필요는 없습니다.

물리적 네트워크 연결 또는 스위치 구성을 통해 네트워크 포트 도달 능력이 변경되었고 네트워크 포트가 다른 브로드캐스트 도메인에 속해 있는 경우 다음 항목을 참조하십시오.

"수리 포트 도달 가능성"

브로드캐스트 도메인의 포트를 추가하거나 제거하는 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크의 브로드캐스트 도메인에서 포트를 추가하거나 제거해야 하는 경우 을 참조하십시오"브로드캐스트 도메인에서 포트 추가 또는 제거(ONTAP 9.7 이하)".

시스템 관리자

ONTAP 9.14.1부터 System Manager를 사용하여 브로드캐스트 도메인에 이더넷 포트를 재할당할 수 있습니다. 모든 이더넷 포트를 브로드캐스트 도메인에 할당하는 것이 좋습니다. 따라서 브로드캐스트 도메인에서 이더넷 포트를 할당 해제하는 경우 다른 브로드캐스트 도메인에 다시 할당해야 합니다.

단계

이더넷 포트를 재할당하려면 다음 단계를 수행하십시오.

1. 네트워크 > 개요 * 를 선택합니다.
2. 브로드캐스트 도메인 * 섹션에서 도메인 이름 옆에 있는 을 선택합니다 ⋮ .
3. 드롭다운 메뉴에서 * 편집 * 을 선택합니다.
4. 브로드캐스트 도메인 편집 * 페이지에서 다른 도메인에 재할당할 이더넷 포트를 선택 취소합니다.
5. 선택 해제된 각 포트에 대해 * 이더넷 포트 재할당 * 창이 표시됩니다. 포트를 재할당할 브로드캐스트 도메인을 선택한 다음 * 재할당 * 을 선택합니다.
6. 현재 브로드캐스트 도메인에 할당할 모든 포트를 선택하고 변경 내용을 저장합니다.

CLI를 참조하십시오

물리적 네트워크 연결 또는 스위치 구성을 통해 네트워크 포트 도달 능력이 변경되었고 네트워크 포트가 다른 브로드캐스트 도메인에 속해 있는 경우 다음 항목을 참조하십시오.

"수리 포트 도달 가능성"

또는 을 사용하여 브로드캐스트 도메인에서 포트를 수동으로 추가하거나 제거할 수 있습니다 `network port broadcast-domain add-ports` 또는 을 누릅니다 `network port broadcast-domain remove-ports` 명령.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 브로드캐스트 도메인에 추가할 포트는 다른 브로드캐스트 도메인에 속하지 않아야 합니다.
- 인터페이스 그룹에 이미 속해 있는 포트는 브로드캐스트 도메인에 개별적으로 추가할 수 없습니다.

이 작업에 대해

네트워크 포트를 추가하거나 제거할 때 다음 규칙이 적용됩니다.

포트를 추가할 때…	포트를 제거할 때…
포트는 네트워크 포트, VLAN 또는 인터페이스 그룹(ifgrp)일 수 있습니다.	해당 없음
포트는 브로드캐스트 도메인의 시스템 정의 페일오버 그룹에 추가됩니다.	브로드캐스트 도메인의 모든 페일오버 그룹에서 포트가 제거됩니다.
포트의 MTU가 브로드캐스트 도메인에서 설정된 MTU 값으로 업데이트됩니다.	포트의 MTU는 변경되지 않습니다.
포트의 IPspace가 브로드캐스트 도메인의 IPspace 값으로 업데이트됩니다.	포트는 브로드캐스트 도메인 속성이 없는 '기본' IPspace로 이동됩니다.

명령을 사용하여 인터페이스 그룹의 마지막 구성원 포트를 제거하면 `network port ifgrp remove-port` 브로드캐스트 도메인에서 빈 인터페이스 그룹 포트가 허용되지 않으므로 인터페이스 그룹 포트가 브로드캐스트 도메인에서 제거됩니다. 에 대한 자세한 내용은 `network port ifgrp remove-port` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. network port show 명령을 사용하여 브로드캐스트 도메인에 현재 할당되거나 할당되지 않은 포트를 표시합니다.
2. 브로드캐스트 도메인에서 네트워크 포트 추가 또는 제거:

원하는 작업	사용…
브로드캐스트 도메인에 포트를 추가합니다	네트워크 포트 브로드캐스트 도메인 추가 포트
브로드캐스트 도메인에서 포트를 제거합니다	네트워크 포트 브로드캐스트 도메인 제거 포트

3. 브로드캐스트 도메인에서 포트가 추가되거나 제거되었는지 확인합니다.

   네트워크 포트 쇼

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

포트 추가 및 제거의 예

다음 명령을 실행하면 노드 클러스터 -1-01의 포트 e0g 및 노드 클러스터 -1-02의 포트 e0g가 기본 IPspace의 브로드캐스트 도메인 bcast1에 추가됩니다.

'cluster-1::> network port broadcast-domain add-ports-broadcast-domain bcast1-ports cluster-1-01:e0g, cluster1-02:e0g'

다음 명령을 실행하면 클러스터 IPspace의 브로드캐스트 도메인 클러스터에 클러스터 포트 2개가 추가됩니다.

'cluster-1::> network port broadcast-domain add-ports-broadcast-domain Cluster-ports cluster-2-03:e0f, cluster2-04:e0f-IPSpace Cluster'

다음 명령은 기본 IPspace의 브로드캐스트 도메인 bcast1에서 노드 cluster1-01의 포트 e0e를 제거합니다.

'cluster-1::> network port broadcast-domain remove-ports-broadcast-domain bcast1-ports cluster-1-01:e0e'

에 대한 자세한 내용은 `network port broadcast-domain remove-ports` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "ONTAP 명령 참조입니다"

ONTAP 포트 가용성을 복구합니다

브로드캐스트 도메인은 자동으로 생성됩니다. 그러나 포트가 다시 설정되거나 스위치 구성이 변경되면 포트를 다른 브로드캐스트 도메인(신규 또는 기존)으로 복구해야 할 수도 있습니다.

ONTAP는 브로드캐스트 도메인 구성(이더넷 포트) 계층 2 내 기능을 기반으로 네트워크 배선 문제에 대한 솔루션을 자동으로 감지하고 추천할 수 있습니다.

동안 배선이 잘못되면 브로드캐스트 도메인 포트가 예기치 않게 할당될 수 있습니다. ONTAP 9.10.1부터 클러스터는 클러스터 설정 후 또는 새 노드가 기존 클러스터에 연결된 경우 포트 재연결을 확인하여 네트워크 배선 문제를 자동으로 확인합니다.

시스템 관리자

포트 도달 가능성 문제가 감지되면 System Manager에서 문제 해결을 위한 복구 작업을 권장합니다.

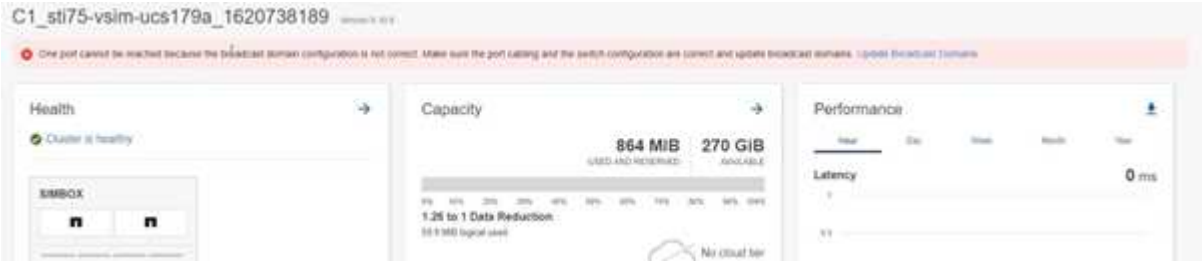
클러스터를 설정한 후 네트워크 배선 문제가 대시보드에 보고됩니다.

클러스터에 새 노드를 연결하면 노드 페이지에 네트워크 배선 문제가 나타납니다.

네트워크 다이어그램에서 네트워크 배선 상태를 볼 수도 있습니다. 포트 도달 가능성 문제는 네트워크 다이어그램에 빨간색 오류 아이콘으로 표시됩니다.

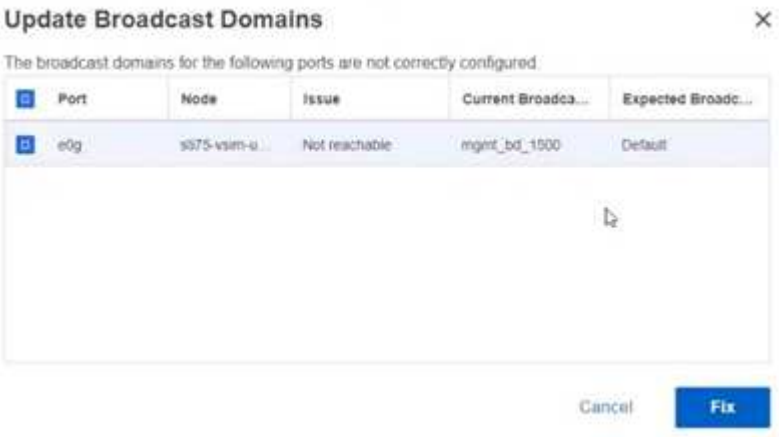
클러스터 설정 후

클러스터를 설정한 후 시스템에서 네트워크 배선 문제가 감지되면 대시보드에 메시지가 표시됩니다.



단계

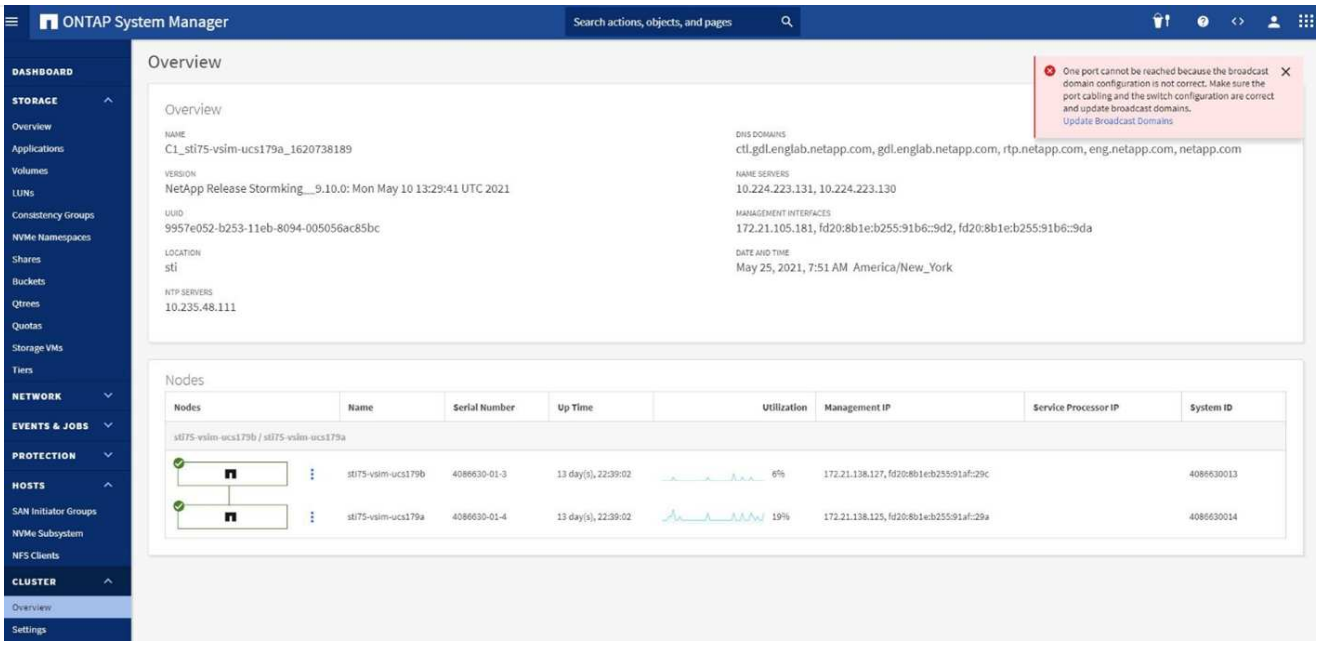
1. 메시지에 제시된 대로 배선을 수정한다.
2. 링크를 클릭하여 브로드캐스트 도메인 업데이트 대화 상자를 시작합니다. 브로드캐스트 도메인 업데이트 대화



   상자가 열립니다.
3. 노드, 문제, 현재 브로드캐스트 도메인 및 예상 브로드캐스트 도메인을 포함하여 포트에 대한 정보를 검토합니다.
4. 복구할 포트를 선택하고 * Fix * 를 클릭합니다. 시스템이 현재 브로드캐스트 도메인에서 예상된 브로드캐스트 도메인으로 포트를 이동합니다.

사후 노드 조인을 선택합니다

새 노드를 클러스터에 조인 후 시스템이 네트워크 배선 문제를 감지하면 노드 페이지에 메시지가 나타납니다.



단계

1. 메시지에 제시된 대로 배선을 수정한다.
2. 링크를 클릭하여 브로드캐스트 도메인 업데이트 대화 상자를 시작합니다. 브로드캐스트 도메인 업데이트 대화

상자가 열립니다.

3. 노드, 문제, 현재 브로드캐스트 도메인 및 예상 브로드캐스트 도메인을 포함하여 포트에 대한 정보를 검토합니다.
4. 복구할 포트를 선택하고 * Fix * 를 클릭합니다. 시스템이 현재 브로드캐스트 도메인에서 예상된 브로드캐스트 도메인으로 포트를 이동합니다.

CLI를 참조하십시오

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

이 작업에 대해

ONTAP에서 감지한 계층 2 도달 가능 여부에 따라 포트에 대한 브로드캐스트 도메인 구성을 자동으로 복구하는 명령을 사용할 수 있습니다.

단계

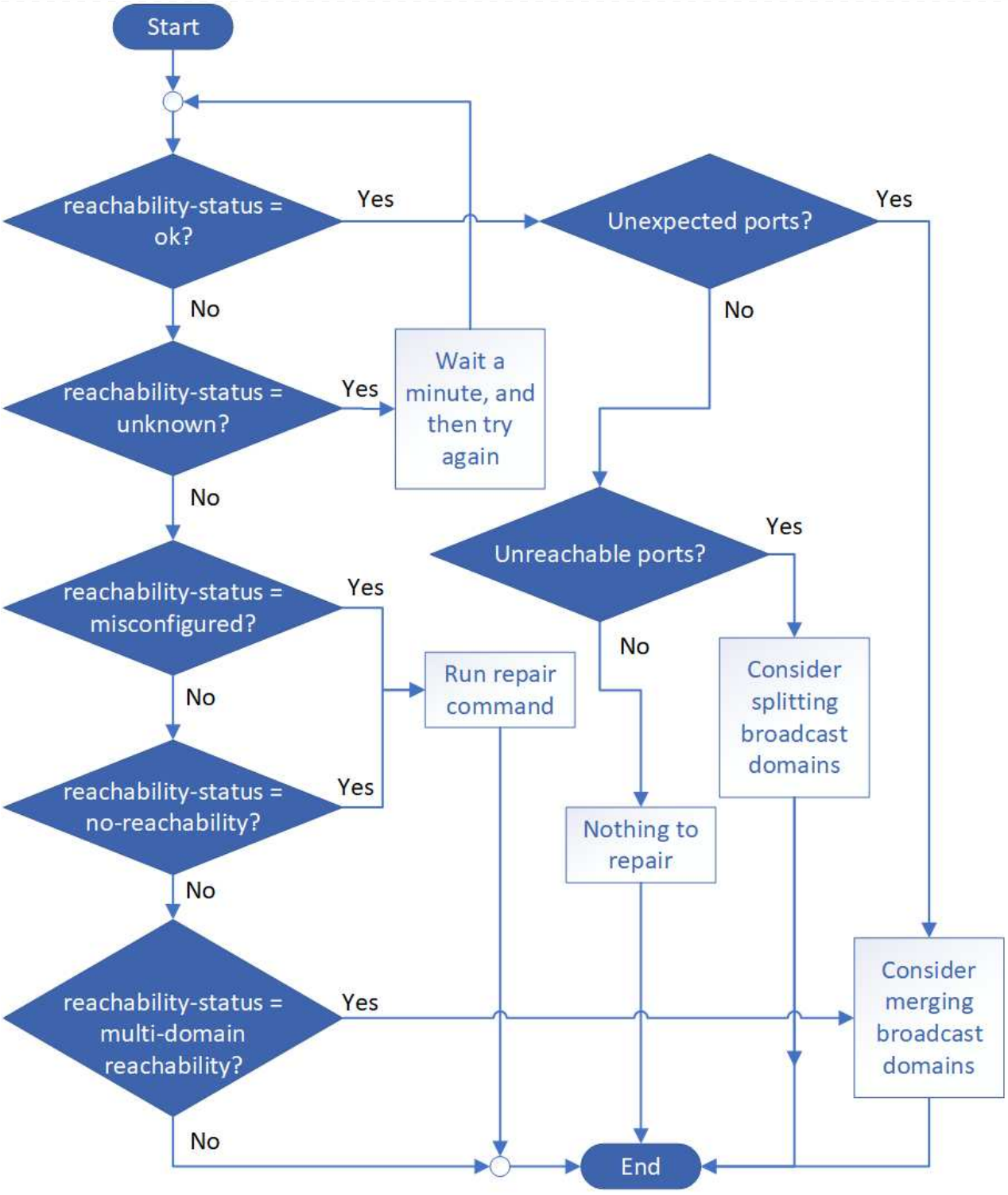
1. 스위치 구성 및 케이블 연결을 확인합니다.
2. 포트의 연결 상태를 확인합니다.

   네트워크 포트 도달 가능성 show-detail-node-port

   명령 출력에 연결 가능 결과가 포함되어 있습니다.

   에 대한 자세한 내용은 `network port reachability show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 다음 진단트리와 표를 사용하여 달성 가능 결과를 파악하고 다음에 수행할 작업을 결정합니다.


Start
reachability-status = ok?
Yes
Unexpected ports?
Yes
No
No
reachability-status = unknown?
Yes
Wait a minute, and then try again
No
Unreachable ports?
Yes
reachability-status = misconfigured?
Yes
No
Run repair command
Consider splitting broadcast domains
No
Nothing to repair
reachability-status = no-reachability?
Yes
No
reachability-status = multi-domain reachability?
Yes
Consider merging broadcast domains
No
End

도달 가능성 - 상태	설명

좋습니다	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있습니다. 도달 가능성 - 상태가 "정상"이지만 "예상치 못한 포트"가 있는 경우 하나 이상의 브로드캐스트 도메인을 병합하는 것이 좋습니다. 자세한 내용은 다음_예기치 않은 포트_행을 참조하십시오. 도달 가능성 - 상태가 "정상"이지만 "연결할 수 없는 포트"인 경우 하나 이상의 브로드캐스트 도메인을 분할하는 것이 좋습니다. 자세한 내용은 _Unreachable ports_row를 참조하십시오. 도달 가능성 - 상태가 "정상"이고 예기치 않거나 연결할 수 없는 포트가 없는 경우 구성이 올바른 것입니다.
예기치 않은 포트	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있지만 하나 이상의 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능도 있습니다. 물리적 연결 및 스위치 구성을 검사하여 올바르지 않거나 포트의 할당된 브로드캐스트 도메인을 하나 이상의 브로드캐스트 도메인과 병합해야 하는지 확인합니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 병합합니다".
연결할 수 없는 포트	단일 브로드캐스트 도메인이 두 개의 서로 다른 도달 가능성 집합으로 분할되는 경우, 브로드캐스트 도메인을 분할하여 ONTAP 구성을 물리적 네트워크 토폴로지와 동기화할 수 있습니다. 일반적으로 연결할 수 없는 포트 목록은 물리적 및 스위치 구성이 정확한지 확인한 후 다른 브로드캐스트 도메인으로 분할해야 하는 포트 집합을 정의합니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 분할합니다".
잘못 구성되었습니다. - 도달 가능성	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 없지만 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있습니다. 포트 연결을 복구할 수 있습니다. 다음 명령을 실행하면 시스템에서 해당 포트가 재연결 가능한 브로드캐스트 도메인에 포트를 할당합니다. 네트워크 포트 도달 가능성 복구 노드 포트

아니오 - 내 상태	이 포트에는 기존 브로드캐스트 도메인에 대한 계층 2 도달 기능이 없습니다. 포트 연결을 복구할 수 있습니다. 다음 명령을 실행하면 시스템이 기본 IPspace에서 자동으로 생성된 새 브로드캐스트 도메인에 포트를 할당합니다. 네트워크 포트 도달 가능성 복구 노드 포트 • 참고: * 모든 인터페이스 그룹(ifgrp) 구성원 포트가 보고되면 `no-reachability`를 실행합니다 `network port reachability repair` 각 멤버 포트의 명령은 각 멤버를 ifgrp에서 제거하고 새 브로드캐스트 도메인에 배치하도록 하여 결국 ifgrp 자체를 제거합니다. 를 실행하기 전에 `network port reachability repair` 명령을 실행하여 포트의 연결 가능한 브로드캐스트 도메인이 물리적 네트워크 토폴로지를 기준으로 예상한 것인지 확인합니다. 에 대한 자세한 내용은 `network port reachability repair` "ONTAP 명령 참조입니다"을 참조하십시오.
다중 도메인 내의 도달 가능성	이 포트에는 할당된 브로드캐스트 도메인에 대한 계층 2 도달 기능이 있지만 하나 이상의 다른 브로드캐스트 도메인에 대한 계층 2 도달 기능도 있습니다. 물리적 연결 및 스위치 구성을 검사하여 올바르지 않거나 포트의 할당된 브로드캐스트 도메인을 하나 이상의 브로드캐스트 도메인과 병합해야 하는지 확인합니다. 자세한 내용은 을 참조하십시오 "브로드캐스트 도메인을 병합합니다".
알 수 없음	도달 가능성 - 상태가 "알 수 없음"인 경우 몇 분 정도 기다린 후 명령을 다시 시도하십시오.

포트를 복구한 후에는 교체된 LIF 및 VLAN을 확인하십시오. 포트가 인터페이스 그룹의 일부인 경우 해당 인터페이스 그룹의 변경 사항도 이해해야 합니다.

LIF

포트가 복구되어 다른 브로드캐스트 도메인으로 이동되면 복구된 포트에 구성된 모든 LIF에 새 홈 포트가 자동으로 할당됩니다. 가능한 경우 동일한 노드의 동일한 브로드캐스트 도메인에서 해당 홈 포트가 선택됩니다. 또는 다른 노드의 홈 포트를 선택하거나 적합한 홈 포트가 없는 경우 홈 포트가 지워집니다.

LIF의 홈 포트를 다른 노드로 이동하거나 확보하면 LIF가 "변위"된 것으로 간주됩니다. 교체된 LIF는 다음 명령을 통해 확인할 수 있습니다.

디시퍼인터페이스 쇼

교체된 LIF가 있는 경우 다음 중 하나를 수행해야 합니다.

- 교체된 LIF의 홈을 복원합니다.

  인터페이스 복구

- LIF의 홈을 수동으로 설정합니다.

  네트워크 인터페이스 수정-홈-포트-홈-노드

  에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

- LIF의 현재 구성된 홈에 만족하는 경우 "교체된 인터페이스" 테이블에서 항목을 제거합니다.

  dissplac된 인터페이스 삭제

VLAN

복구된 포트에 VLAN이 있는 경우 해당 VLAN은 자동으로 삭제되지만 "교체된" VLAN으로 기록됩니다. 다음과 같은 교체된 VLAN을 볼 수 있습니다.

디세퍼드-VLAN 쇼

교체된 VLAN이 있는 경우 다음 중 하나를 수행해야 합니다.

- VLAN을 다른 포트로 복구합니다.

  디즈퍼스VLAN 복원

- "교체된 VLAN" 테이블에서 항목을 제거합니다.

  dissplac된 - vLANs delete

인터페이스 그룹

복구된 포트가 인터페이스 그룹의 일부인 경우 해당 인터페이스 그룹에서 제거됩니다. 인터페이스 그룹에 할당된 유일한 구성원 포트인 경우 인터페이스 그룹 자체가 제거됩니다.

관련 정보

- "업그레이드 후 네트워크 구성을 확인합니다"
- "네트워크 포트의 연결 상태를 모니터링합니다"
- "ONTAP 명령 참조입니다"

ONTAP 브로드캐스트 도메인을 IPspace로 이동합니다

ONTAP 9.8부터 계층 2 접근성을 기반으로 시스템이 만든 브로드캐스트 도메인을 사용자가 만든 IPspace로 이동할 수 있습니다.

브로드캐스트 도메인을 이동하기 전에 브로드캐스트 도메인의 포트 도달 가능 여부를 확인해야 합니다.

포트의 자동 스캐닝은 서로 연결할 수 있는 포트를 확인하여 동일한 브로드캐스트 도메인에 배치할 수 있지만 이 스캐닝에서 적절한 IPspace를 확인할 수 없습니다. 브로드캐스트 도메인이 기본 IPspace에 속한 경우 이 섹션의 단계를 사용하여 수동으로 이동해야 합니다.

시작하기 전에

브로드캐스트 도메인은 클러스터 생성 및 연결 작업의 일부로 자동으로 구성됩니다. ONTAP는 "기본" 브로드캐스트 도메인을 "클러스터에서 생성된 첫 번째 노드의 관리 인터페이스 홈 포트에 대한 계층 2 연결이 있는 포트 세트로 정의합니다. 필요한 경우 다른 브로드캐스트 도메인이 생성되고 이름이 * Default-1 *, * Default-2 * 등으로 지정됩니다.

노드가 기존 클러스터에 연결되면 해당 네트워크 포트는 계층 2 도달 가능 여부에 따라 기존 브로드캐스트 도메인에 자동으로 연결됩니다. 기존 브로드캐스트 도메인에 대한 도달 기능이 없는 경우 포트가 하나 이상의 새 브로드캐스트 도메인에 배치됩니다.

이 작업에 대해

- 클러스터 LIF가 있는 포트는 "클러스터" IPspace에 자동으로 배치되며
- 노드 관리 LIF의 홈 포트에 대한 연결 기능이 있는 포트는 "기본" 브로드캐스트 도메인에 배치됩니다.
- 다른 브로드캐스트 도메인은 클러스터 생성 또는 연결 작업의 일부로 ONTAP에 의해 자동으로 생성됩니다.
- VLAN 및 인터페이스 그룹을 추가하면 생성된 후 약 1분 후에 해당 브로드캐스트 도메인에 자동으로 배치됩니다.

단계

1. 브로드캐스트 도메인의 포트 도달 가능 여부를 확인합니다. ONTAP는 레이어 2 내 상태를 자동으로 모니터링합니다. 다음 명령을 사용하여 각 포트가 브로드캐스트 도메인에 추가되고 "확인" 기능이 있는지 확인합니다.

   네트워크 포트 도달 가능성 세부 정보

   에 대한 자세한 내용은 `network port reachability show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 필요한 경우 브로드캐스트 도메인을 다른 IPspace로 이동:

   네트워크 포트 브로드캐스트 도메인 이동

   예를 들어 브로드캐스트 도메인을 "기본값"에서 "IPS1"으로 이동하려면:

   네트워크 포트 브로드캐스트-도메인 이동-IPSpace 기본-브로드캐스트-도메인 기본-IPSpace IPS1

관련 정보

- "네트워크 포트 브로드캐스트 - 도메인 이동"

ONTAP 브로드캐스트 도메인을 분할합니다

물리적 네트워크 연결 또는 스위치 구성을 통해 네트워크 포트 도달 능력이 변경된 경우 또한 단일 브로드캐스트 도메인에 이전에 구성된 네트워크 포트 그룹이 두 개의 서로 다른 도달 가능성 집합으로 분할되어 ONTAP 구성을 물리적 네트워크 토폴로지와 동기화할 수 있습니다.

> 브로드캐스트 도메인을 분할하는 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 브로드캐스트 도메인을 분할해야 하는 경우 을 "브로드캐스트 도메인 분할(ONTAP 9.7 이하)"참조하십시오.

네트워크 포트 브로드캐스트 도메인이 둘 이상의 연결 집합으로 분할되었는지 확인하려면 명령을 사용하여 `network port reachability show -details` 서로 연결되지 않은 포트("연결할 수 없는 포트")에 주의를 기울이십시오. 일반적으로 연결할 수 없는 포트 목록은 물리적 및 스위치 구성이 정확한지 확인한 후 다른 브로드캐스트 도메인으로 분할해야 하는 포트 집합을 정의합니다. 에 대한 자세한 내용은 `network port reachability show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

브로드캐스트 도메인을 두 개의 브로드캐스트 도메인으로 분할:

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- IPSpace_name은 브로드캐스트 도메인이 있는 IPSpace의 이름입니다.
- 브로드캐스트 도메인은 분할될 브로드캐스트 도메인의 이름입니다.
- 새 브로드캐스트 도메인은 생성되는 새 브로드캐스트 도메인의 이름입니다.
- 포트란 새 브로드캐스트 도메인에 추가될 노드 이름과 포트입니다.

관련 정보

- "네트워크 포트 브로드캐스트 - 도메인 분할입니다"

ONTAP 브로드캐스트 도메인을 병합합니다

물리적 네트워크 연결 또는 스위치 구성을 통해 네트워크 포트 도달 능력이 변경되었고 이전에 여러 브로드캐스트 도메인에 구성된 두 개의 네트워크 포트 그룹이 이제 모두 공유 도달 가능 상태로 변경된 경우 두 개의 브로드캐스트 도메인을 병합하여 ONTAP 구성을 물리적 네트워크 토폴로지와 동기화할 수 있습니다.

브로드캐스트 도메인을 병합하는 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 브로드캐스트 도메인을 병합해야 하는 경우 을 "브로드캐스트 도메인 병합(ONTAP 9.7 이하)"참조하십시오.

여러 브로드캐스트 도메인이 하나의 도달 가능성 집합에 속하는지 확인하려면 다음을 사용하십시오. `network port reachability show -details` 명령을 내리고 다른 브로드캐스트 도메인에 구성된 포트 중 실제로 서로 연결되어 있는 포트가 무엇인지 주의 깊게 살펴보세요("예기치 않은 포트"). 일반적으로 예기치 않은 포트 목록은 물리적 및 스위치 구성이 정확한지 확인한 후 브로드캐스트 도메인에 병합되어야 하는 포트 집합을 정의합니다.

에 대한 자세한 내용은 `network port reachability show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

한 브로드캐스트 도메인의 포트를 기존 브로드캐스트 도메인으로 병합:

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- IPSpace_name은 브로드캐스트 도메인이 있는 IPSpace의 이름입니다.
- '-broadcast-domain'은 통합될 브로드캐스트 도메인의 이름입니다.
- '-브로드캐스트-도메인'은 추가 포트를 받을 브로드캐스트 도메인의 이름입니다.

관련 정보

- "네트워크 포트 브로드캐스트-도메인-병합"

ONTAP 브로드캐스트 도메인의 포트에 대한 MTU 값을 변경합니다

브로드캐스트 도메인의 MTU 값을 수정하여 해당 브로드캐스트 도메인의 모든 포트에 대한 MTU 값을 변경할 수 있습니다. 이 작업은 네트워크에서 수행된 토폴로지 변경을 지원하기 위해 수행할 수 있습니다.

브로드캐스트 도메인 포트의 MTU 값을 변경하는 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 브로드캐스트 도메인 포트의 MTU 값을 변경해야 하는 경우을 참조하십시오"브로드캐스트 도메인의 포트에 대한 MTU 값 변경(ONTAP 9.7 이하)".

시스템 관리자

ONTAP 9.12.1부터 System Manager를 사용하여 브로드캐스트 도메인의 MTU 값을 수정하면 해당 브로드캐스트 도메인의 모든 포트에 대한 MTU 값을 변경할 수 있습니다.

단계

1. *Network > Broadcast Domains*를 선택합니다.
2. 브로드캐스트 도메인 섹션에서 MTU 값을 변경하려는 브로드캐스트 도메인의 이름을 선택합니다.
3. 브로드캐스트 도메인의 모든 포트에 대한 MTU 값을 변경할 것인지 확인하는 메시지가 나타납니다. 변경을 진행하려면 *Yes*를 클릭하십시오.
4. 필요에 따라 MTU 값을 수정하고 변경 사항을 저장하십시오.

   시스템은 브로드캐스트 도메인의 모든 포트에 새 MTU 값을 적용하므로 해당 포트를 통한 트래픽이 잠시 중단됩니다.

CLI를 참조하십시오

시작하기 전에

MTU 값은 e0M 포트 처리 관리 트래픽을 제외하고 해당 계층 2 네트워크에 연결된 모든 장치와 일치해야 합니다.

이 작업에 대해

MTU 값을 변경하면 해당 포트를 통한 트래픽이 잠시 중단됩니다. 시스템에 메시지가 표시되며, MTU 변경을 위해서는 *y*를 입력해야 합니다.

단계

브로드캐스트 도메인의 모든 포트에 대한 MTU 값을 변경합니다.

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

위치:

- broadcast_domain은 브로드캐스트 도메인의 이름입니다.
- Mtu는 IP 패킷의 MTU 크기이고 1500과 9000은 일반적인 값입니다.
- `ipspace`는 이 브로드캐스트 도메인이 상주하는 IPspace의 이름입니다. 이 옵션에 값을 지정하지 않으면 "Default" IPspace가 사용됩니다.

  다음 명령은 브로드캐스트 도메인 bcast1의 모든 포트에 대한 MTU를 9000으로 변경합니다.

  ```
  network port broadcast-domain modify -broadcast-domain <Default-1>
  -mtu < 9000 >
  Warning: Changing broadcast domain settings will cause a momentary
  data-serving interruption.
  Do you want to continue? {y|n}: <y>
  ```

관련 정보

- "네트워크 포트 브로드캐스트 - 도메인 수정"

ONTAP 브로드캐스트 도메인을 봅니다

클러스터의 각 IPspace 내에서 브로드캐스트 도메인 목록을 표시할 수 있습니다. 출력에는 각 브로드캐스트 도메인의 포트 목록과 MTU 값도 표시됩니다.

브로드캐스트 도메인을 표시하는 절차는 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에 브로드캐스트 도메인을 표시해야 하는 경우 을 참조하십시오"브로드캐스트 도메인 표시(ONTAP 9.7 이하)".

단계

클러스터의 브로드캐스트 도메인 및 관련 포트를 표시합니다.

```
network port broadcast-domain show
```

다음 명령을 실행하면 클러스터의 모든 브로드캐스트 도메인 및 관련 포트가 표시됩니다.

```
network port broadcast-domain show
IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  ---------------------- --------------
Cluster Cluster      9000
                           cluster-1-01:e0a       complete
                           cluster-1-01:e0b       complete
                           cluster-1-02:e0a       complete
                           cluster-1-02:e0b       complete
Default Default      1500
                           cluster-1-01:e0c       complete
                           cluster-1-01:e0d       complete
                           cluster-1-02:e0c       complete
                           cluster-1-02:e0d       complete
        Default-1    1500
                           cluster-1-01:e0e       complete
                           cluster-1-01:e0f       complete
                           cluster-1-01:e0g       complete
                           cluster-1-02:e0e       complete
                           cluster-1-02:e0f       complete
                           cluster-1-02:e0g       complete
```

다음 명령을 실행하면 Default-1 브로드캐스트 도메인의 포트가 오류 상태로 표시되며, 이는 포트를 올바르게 업데이트할 수 없음을 나타냅니다.

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ------------ -----  ---------------------- --------------
Default Default-1    1500
                            cluster-1-02:e0g       error
```

관련 정보

- "네트워크 포트 브로드캐스트 - 도메인 표시"

ONTAP 브로드캐스트 도메인을 삭제합니다

브로드캐스트 도메인이 더 이상 필요하지 않으면 삭제할 수 있습니다. 이렇게 하면 해당 브로드캐스트 도메인과 연결된 포트가 "기본" IPspace로 이동합니다.

시작하기 전에

삭제할 브로드캐스트 도메인에 연결된 서브넷, 네트워크 인터페이스 또는 SVM이 없어야 합니다.

이 작업에 대해

- 시스템에서 생성한 "클러스터" 브로드캐스트 도메인은 삭제할 수 없습니다.
- 브로드캐스트 도메인을 삭제하면 브로드캐스트 도메인과 관련된 모든 페일오버 그룹이 제거됩니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- ONTAP 9.12.0부터 시스템 관리자를 사용하여 브로드캐스트 도메인 * 을 삭제할 수 있습니다

브로드캐스트 도메인에 포트가 포함되어 있거나 서브넷에 연결되어 있는 경우에는 삭제 옵션이 표시되지 않습니다.

단계

1. 네트워크 > 개요 > 브로드캐스트 도메인 * 을 선택합니다.
2. 제거할 브로드캐스트 도메인 옆의 * > 삭제 * 를 선택합니다 ⋮ .

CLI를 참조하십시오

- CLI를 사용하여 브로드캐스트 도메인 * 을 삭제합니다

단계

브로드캐스트 도메인 삭제:

'network port broadcast-domain delete-broadcast-domain_broadcast_domain_name_[-IPSpace_IPSpace_name_]'

다음 명령을 실행하면 IPspace ipspac1에서 브로드캐스트 도메인 Default-1이 삭제됩니다.

'network port broadcast-domain delete-broadcast-domain_Default-1_-IPSpace_ipspace1_'

관련 정보

- "네트워크 포트 브로드캐스트 - 도메인 삭제"

페일오버 그룹 및 정책

ONTAP 네트워크에서의 LIF 페일오버에 대해 알아보십시오

LIF 페일오버는 LIF의 현재 포트에서 링크 장애가 발생할 경우 LIF가 다른 네트워크 포트로 자동 마이그레이션되는 것을 의미합니다. 이 기능은 SVM에 대한 연결을 위한 고가용성을 제공하는 핵심 구성요소입니다. LIF 페일오버를 구성하려면 페일오버 그룹을 생성하고, 페일오버 그룹을 사용하도록 LIF를 수정하고, 페일오버 정책을 지정해야 합니다.

페일오버 그룹에는 클러스터에 있는 하나 이상의 노드의 네트워크 포트 세트(물리적 포트, VLAN 및 인터페이스 그룹)가 포함됩니다. 페일오버 그룹에 있는 네트워크 포트는 LIF에 사용할 수 있는 페일오버 타겟을 정의합니다. 페일오버 그룹은 클러스터 관리, 노드 관리, 인터클러스터 및 NAS 데이터 LIF가 할당될 수 있습니다.

ⓘ LIF가 유효한 페일오버 대상이 없이 구성되면 LIF가 페일오버를 시도할 때 중단이 발생합니다. 명령을 사용하여 페일오버 구성을 확인할 수 `network interface show -failover` 있습니다. 에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

브로드캐스트 도메인을 생성하면 동일한 네트워크 포트를 포함하는 동일한 이름의 페일오버 그룹이 자동으로 생성됩니다. 이 페일오버 그룹은 시스템에서 자동으로 관리됩니다. 즉, 포트가 브로드캐스트 도메인에서 추가되거나 제거될 때 포트가 이 페일오버 그룹에서 자동으로 추가 또는 제거됩니다. 이 기능은 고유한 페일오버 그룹을 관리하지

않으려는 관리자에게 효율적으로 제공됩니다.

ONTAP 페일오버 그룹을 생성합니다

네트워크 포트의 페일오버 그룹을 생성하면 LIF의 현재 포트에서 링크 장애가 발생할 경우 LIF가 자동으로 다른 포트로 마이그레이션할 수 있습니다. 이렇게 하면 시스템이 네트워크 트래픽을 클러스터의 사용 가능한 다른 포트로 재라우팅할 수 있습니다.

이 작업에 대해

'network interface failover-groups create' 명령을 사용하여 그룹을 생성하고 그룹에 포트를 추가합니다.

- 페일오버 그룹에 추가된 포트는 네트워크 포트, VLAN 또는 인터페이스 그룹(ifgrp)일 수 있습니다.
- 페일오버 그룹에 추가된 모든 포트는 동일한 브로드캐스트 도메인에 속해야 합니다.
- 단일 포트는 여러 페일오버 그룹에 상주할 수 있습니다.
- 다른 VLAN 또는 브로드캐스트 도메인에 LIF가 있는 경우 각 VLAN 또는 브로드캐스트 도메인에 대해 페일오버 그룹을 구성해야 합니다.
- SAN iSCSI 또는 FC 환경에서는 페일오버 그룹이 적용되지 않습니다.

단계

페일오버 그룹 생성:

'network interface failover-groups create-vserver_vserver_name_-failover-group_failover_group_name_-targets_ports_list_'

- '*vserver_name*'은 페일오버 그룹을 사용할 수 있는 SVM의 이름입니다.
- '*failover_group_name*'은 생성할 페일오버 그룹의 이름입니다.
- '*ports_list*'는 페일오버 그룹에 추가될 포트 목록입니다. 포트는 format_node_name>:<port_number>_에 추가됩니다(예: node1:e0c).

다음 명령을 실행하면 SVM vs3용 페일오버 그룹 fg3이 생성되고 2개의 포트가 추가됩니다.

```
network interface failover-groups create -vserver vs3 -failover-group fg3
-targets cluster1-01:e0e,cluster1-02:e0e
```

작업을 마친 후

- 페일오버 그룹이 생성되었으므로 페일오버 그룹을 LIF에 적용해야 합니다.
- LIF에 유효한 페일오버 타겟을 제공하지 않는 페일오버 그룹을 적용하면 경고 메시지가 표시됩니다.

  유효한 페일오버 목표가 없는 LIF가 페일오버를 시도하면 운영 중단이 발생할 수 있습니다.

- 에 대한 자세한 내용은 `network interface failover-groups create` "ONTAP 명령 참조입니다"을 참조하십시오.

LIF에 대한 ONTAP 페일오버 설정을 구성합니다

페일오버 정책과 페일오버 그룹을 LIF에 적용하여 LIF를 특정 네트워크 포트 그룹으로 페일오버할 수 있습니다. LIF가 다른 포트로 페일오버되지 않도록 설정할 수도 있습니다.

이 작업에 대해

- LIF가 생성되면 LIF 페일오버가 기본적으로 활성화되며 사용 가능한 타겟 포트 목록은 LIF 유형 및 서비스 정책에 따라 기본 페일오버 그룹 및 페일오버 정책에 따라 결정됩니다.

  9.5부터 LIF를 사용할 수 있는 네트워크 서비스를 정의하는 LIF의 서비스 정책을 지정할 수 있습니다. 일부 네트워크 서비스에서는 LIF에 페일오버 제한을 적용합니다.

  LIF의 서비스 정책이 페일오버를 더욱 제한하는 방식으로 변경되면 LIF의 페일오버 정책이 시스템에 의해 자동으로 업데이트됩니다.

- network interface modify 명령에서 -failover -group 및 -failover -policy 매개 변수의 값을 지정하여 LIF의 페일오버 동작을 수정할 수 있습니다.
- LIF가 수정되어 LIF에 유효한 페일오버 타겟이 없게 되면 경고 메시지가 표시됩니다.

  유효한 페일오버 목표가 없는 LIF가 페일오버를 시도하면 운영 중단이 발생할 수 있습니다.

- ONTAP 9.11.1부터 ASA(All-Flash SAN 어레이) 플랫폼에서는 새로 생성된 스토리지 VM에서 새로 생성된 iSCSI LIF에 대해 iSCSI LIF 페일오버가 자동으로 활성화됩니다.

  또한, 할 수 있습니다 "기존 iSCSI LIF에서 iSCSI LIF 페일오버를 수동으로 활성화합니다"는 ONTAP 9.11.1 이상으로 업그레이드하기 전에 생성된 LIF를 의미합니다.

- 다음 목록에서는 -failover-policy 설정이 페일오버 그룹에서 선택한 타겟 포트에 미치는 영향에 대해 설명합니다.

  iSCSI LIF 페일오버의 경우 페일오버 정책 '로컬 전용', 'fo 파트너 전용', '사용 안 함'만 지원됩니다.

- 브로드캐스트 도메인 전체에 적용되는 것은 페일오버 그룹의 모든 노드에 있는 모든 포트에 적용됩니다.
- '시스템 정의'는 LIF 홈 노드의 포트와 클러스터의 다른 노드(일반적으로 SFO가 아닌 파트너)에만 적용됩니다.
- '로컬 전용'은 LIF의 홈 노드에 있는 포트에만 적용됩니다.
- 'fo 파트너 전용'은 LIF 홈 노드와 SFO 파트너에 있는 포트에만 적용됩니다.
- "사용 안 함"은 LIF가 페일오버 대상으로 구성되지 않았음을 나타냅니다.

단계

기존 인터페이스에 대한 페일오버 설정을 구성합니다.

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

페일오버 설정 구성 및 페일오버 해제의 예

다음 명령은 페일오버 정책을 브로드캐스트 도메인 전체에 설정하고 페일오버 그룹 fg3의 포트를 SVM vs3의 LIF

data1의 페일오버 타겟으로 사용합니다.

```
network interface modify -vserver vs3 -lif data1 -failover-policy
broadcast-domain-wide -failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif              failover-policy       failover-group
------- -------------- ---------------        --------------
vs3     data1          broadcast-domain-wide  fg3
```

다음 명령을 실행하면 SVM vs3에서 LIF 데이터 1의 페일오버가 사용되지 않습니다.

```
network interface modify -vserver vs3 -lif data1 -failover-policy disabled
```

관련 정보

- "네트워크 인터페이스"

ONTAP 명령으로 페일오버 그룹 및 정책을 관리할 수 있습니다

네트워크 인터페이스 페일오버 그룹 명령을 사용하여 페일오버 그룹을 관리할 수 있습니다. 'network interface modify' 명령을 사용하여 LIF에 적용되는 페일오버 그룹 및 페일오버 정책을 관리할 수 있습니다.

원하는 작업	이 명령 사용…
페일오버 그룹에 네트워크 포트를 추가합니다	네트워크 인터페이스 페일오버 그룹 추가 타겟
페일오버 그룹에서 네트워크 포트를 제거합니다	네트워크 인터페이스 페일오버 그룹 제거 대상
페일오버 그룹의 네트워크 포트를 수정합니다	네트워크 인터페이스 페일오버 그룹 수정
현재 페일오버 그룹을 표시합니다	네트워크 인터페이스 페일오버 그룹들이 보여줌
LIF에서 페일오버를 구성합니다	네트워크 인터페이스 수정-페일오버-그룹-페일오버-정책
각 LIF에서 사용 중인 페일오버 그룹 및 페일오버 정책을 표시합니다	네트워크 인터페이스 보기 필드 장애 조치 그룹 장애 조치 정책
페일오버 그룹의 이름을 바꿉니다	네트워크 인터페이스 페일오버 그룹 이름 바꾸기
페일오버 그룹을 삭제합니다	네트워크 인터페이스 페일오버 그룹 삭제

페일오버 그룹을 수정하여 클러스터의 모든 LIF에 유효한 페일오버 목표를 제공하지 않으면 LIF에서 페일오버를 시도할 때 운영 중단이 발생할 수 있습니다.

관련 정보

- "네트워크 인터페이스"

서브넷(클러스터 관리자만 해당)

ONTAP 네트워크의 서브넷에 대해 알아봅니다

서브넷을 사용하면 ONTAP 네트워크 구성을 위해 특정 블록 또는 IP 주소 풀을 할당할 수 있습니다. 따라서 IP 주소와 네트워크 마스크 값을 지정하지 않고 서브넷 이름을 지정하여 LIF를 더 쉽게 생성할 수 있습니다.

서브넷은 브로드캐스트 도메인 내에서 생성되며 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함됩니다. LIF가 생성될 때 서브넷의 IP 주소가 브로드캐스트 도메인의 포트에 할당됩니다. LIF가 제거되면 IP 주소가 서브넷 풀로 반환되며 향후 LIF에서 사용할 수 있습니다.

서브넷을 사용하면 IP 주소를 훨씬 쉽게 관리할 수 있으며 LIF를 더 쉽게 생성할 수 있으므로 서브넷을 사용하는 것이 좋습니다. 또한, 서브넷을 정의할 때 게이트웨이를 지정하면 해당 서브넷을 사용하여 LIF가 생성될 때 해당 게이트웨이에 대한 기본 경로가 SVM에 자동으로 추가됩니다.

ONTAP 네트워크에 대한 서브넷을 생성합니다

나중에 SVM에 대한 LIF를 생성할 때 사용할 IPv4 또는 IPv6 주소의 특정 블록을 할당하는 서브넷을 생성할 수 있습니다.

따라서 각 LIF에 대한 IP 주소와 네트워크 마스크 값을 지정하지 않고 서브넷 이름을 지정하여 LIF를 더 쉽게 생성할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

서브넷을 추가하려는 브로드캐스트 도메인 및 IPspace가 이미 있어야 합니다.

이 작업에 대해

- 모든 서브넷 이름은 IPspace 내에서 고유해야 합니다.
- 서브넷에 IP 주소 범위를 추가할 때 네트워크에 중복되는 IP 주소가 없는지 확인해야 합니다. 이렇게 하면 다른 서브넷 또는 호스트가 동일한 IP 주소를 사용하지 않도록 할 수 있습니다.
- 서브넷을 정의할 때 게이트웨이를 지정하면 해당 서브넷을 사용하여 LIF가 생성될 때 해당 게이트웨이에 대한 기본 경로가 SVM에 자동으로 추가됩니다. 서브넷을 사용하지 않거나 서브넷을 정의할 때 게이트웨이를 지정하지 않으면 수동으로 SVM에 경로를 추가하려면 'route create' 명령을 사용해야 합니다.
- NetApp은 데이터 SVM의 모든 LIF에 대한 서브넷 개체를 생성할 것을 권장합니다. 이는 각 서브넷 객체에 연결된 브로드캐스트 도메인이 있기 때문에 ONTAP에서 대상 클러스터의 페일오버 대상을 결정할 수 있도록 서브넷 객체를 사용하는 MetroCluster 구성에서 특히 중요합니다.

단계

ONTAP System Manager 또는 ONTAP CLI를 사용하여 서브넷을 생성할 수 있습니다.

시스템 관리자

ONTAP 9.12.0부터는 시스템 관리자를 사용하여 서브넷을 생성할 수 있습니다.

단계

1. 네트워크 > 개요 > 서브넷 * 을 선택합니다.
2. 서브넷을 만들려면 + Add 클릭합니다.
3. 서브넷 이름을 지정합니다.
4. 서브넷 IP 주소를 지정합니다.
5. 서브넷 마스크를 설정합니다.
6. 서브넷을 구성하는 IP 주소의 범위를 정의합니다.
7. 유용한 경우 게이트웨이를 지정합니다.
8. 서브넷이 속한 브로드캐스트 도메인을 선택합니다.
9. 변경 사항을 저장합니다.
   a. 입력한 IP 주소 또는 범위가 이미 인터페이스에서 사용되는 경우 다음 메시지가 표시됩니다. "이 범위의 IP 주소는 LIF에서 이미 사용 중입니다. LIF를 이 서브넷과 연결하시겠습니까?"라는 문구입니다
   b. OK * 를 클릭하면 기존 LIF가 서브넷에 연결됩니다.

CLI를 참조하십시오

CLI를 사용하여 서브넷을 생성합니다.

```
network subnet create -subnet-name subnet_name -broadcast-domain
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet
<subnet_address> [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- 'subnet_name'은 만들려는 계층 3 서브넷의 이름입니다.

  이름은 "Mgmt"와 같은 텍스트 문자열이거나 192.0.2.0/24와 같은 특정 서브넷 IP 값일 수 있습니다.

- broadcast_domain_name은 서브넷이 상주할 브로드캐스트 도메인의 이름입니다.
- IPSpace_name은 브로드캐스트 도메인이 속한 IPspace의 이름입니다.

  이 옵션에 대한 값을 지정하지 않으면 "기본" IPspace가 사용됩니다.

- Subnet_address는 서브넷의 IP 주소와 마스크입니다(예: 192.0.2.0/24).
- gateway_address는 192.0.2.1과 같이 서브넷의 기본 라우트에 대한 게이트웨이입니다.
- IP_address_list는 서브넷에 할당할 IP 주소의 목록 또는 범위입니다.

  IP 주소는 개별 주소, IP 주소 범위 또는 쉼표로 구분된 목록의 조합이 될 수 있습니다.

- TRUE 값은 '-force-update-lif-associations' 옵션에 설정할 수 있습니다.

서비스 프로세서 또는 네트워크 인터페이스가 현재 지정된 범위의 IP 주소를 사용하는 경우 이 명령은 실패합니다. 이 값을 true 로 설정하면 수동으로 주소를 지정한 모든 인터페이스가 현재 서브넷에 연결되어 명령이 성공할 수 있습니다.

다음 명령을 실행하면 기본 IPspace에 브로드캐스트 도메인 Default-1에 서브넷 하위 1이 생성됩니다. IPv4 서브넷 IP 주소 및 마스크, 게이트웨이 및 IP 주소 범위를 추가합니다.

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

다음 명령을 실행하면 "기본" IPspace에서 브로드캐스트 도메인 Default에 서브넷 하위 2가 생성됩니다. 다음과 같은 다양한 IPv6 주소가 추가됩니다.

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

에 대한 자세한 내용은 `network subnet create` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

서브넷의 주소를 사용하여 SVM 및 인터페이스를 IPspace에 할당할 수 있습니다.

기존 서브넷의 이름을 변경해야 할 경우에는 네트워크 서브넷 이름 바꾸기 명령을 사용합니다.

에 대한 자세한 내용은 `network subnet rename` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크의 서브넷에서 IP 주소를 추가하거나 제거합니다

처음에 서브넷을 생성할 때 IP 주소를 추가하거나 이미 존재하는 서브넷에 IP 주소를 추가할 수 있습니다. 기존 서브넷에서 IP 주소를 제거할 수도 있습니다. 따라서 SVM에 필요한 IP 주소만 할당할 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- ONTAP 9.12.0부터 시스템 관리자를 사용하여 서브넷 * 에 IP 주소를 추가하거나 제거할 수 있습니다

단계

1. 네트워크 > 개요 > 서브넷 * 을 선택합니다.
2. 변경할 서브넷 옆의 * > 편집 * 을 선택합니다 ⋮ .
3. IP 주소를 추가하거나 제거합니다.
4. 변경 사항을 저장합니다.
   a. 입력한 IP 주소 또는 범위가 이미 인터페이스에서 사용되는 경우 다음 메시지가 표시됩니다. "이 범위의 IP 주소는 LIF에서 이미 사용 중입니다. LIF를 이 서브넷과 연결하시겠습니까?"라는 문구입니다
   b. OK * 를 클릭하면 기존 LIF가 서브넷에 연결됩니다.

CLI를 참조하십시오

- CLI를 사용하여 IP 주소를 서브넷 * 에 추가하거나 서브넷에서 제거합니다

이 작업에 대해

IP 주소를 추가할 때 서비스 프로세서 또는 네트워크 인터페이스가 추가되는 범위의 IP 주소를 사용하는 경우 오류가 발생합니다. 수동으로 주소를 지정한 인터페이스를 현재 서브넷에 연결하려면 '-force-update-lif-associations' 옵션을 'true'로 설정합니다.

IP 주소를 제거할 때 서비스 프로세서 또는 네트워크 인터페이스에서 제거 중인 IP 주소를 사용하는 경우 오류가 발생합니다. 서브넷에서 IP 주소를 제거한 후에도 인터페이스가 계속 사용하도록 하려면 "-force-update-lif-associations" 옵션을 "true"로 설정합니다.

단계

서브넷에서 IP 주소 추가 또는 제거:

원하는 작업	이 명령 사용…
IP 주소를 서브넷에 추가합니다	네트워크 서브넷 추가 범위
서브넷에서 IP 주소를 제거합니다	네트워크 서브넷 remove-range

다음 명령을 실행하면 서브넷 sub1에 IP 주소 192.0.2.82 ~ 192.0.2.85 가 추가됩니다.

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-
192.0.2.85>
```

다음 명령을 실행하면 서브넷 하위 3에서 IP 주소 198.51.100.9가 제거됩니다.

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges
<198.51.100.9>
```

현재 범위에 1 ~ 10 및 20 ~ 40이 포함되어 있고 11 ~ 19 및 41 ~ 50(기본적으로 1 ~ 50을 허용)을 추가하려는 경우 다음 명령을 사용하여 기존 주소 범위와 겹칠 수 있습니다. 이 명령은 새 주소만 추가하며 기존 주소에는 영향을 주지 않습니다.

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-
198.51.10.50>
```

및 `network subnet remove-ranges` 에 대한 자세한 `network subnet add-ranges` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP 네트워크의 서브넷 속성을 변경합니다

기존 서브넷에서 서브넷 주소 및 마스크 값, 게이트웨이 주소 또는 IP 주소 범위를 변경할 수 있습니다.

이 작업에 대해

- IP 주소를 수정할 때 다른 서브넷 또는 호스트가 동일한 IP 주소를 사용하지 않도록 네트워크에 중복되는 IP 주소가 없는지 확인해야 합니다.
- 게이트웨이 IP 주소를 추가하거나 변경할 경우, 서브넷을 사용하여 LIF를 생성할 때 수정된 게이트웨이가 새로운 SVM에 적용됩니다. 경로가 존재하지 않을 경우 SVM을 위해 게이트웨이로 가는 기본 경로가 생성됩니다. 게이트웨이 IP 주소를 변경할 때 SVM에 새 경로를 수동으로 추가해야 할 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- ONTAP 9.12.0부터 시스템 관리자를 사용하여 서브넷 속성을 변경할 수 있습니다 *

단계

1. 네트워크 > 개요 > 서브넷 * 을 선택합니다.
2. 변경할 서브넷 옆의 * > 편집 * 을 선택합니다 ⋮.
3. 변경합니다.
4. 변경 사항을 저장합니다.
   a. 입력한 IP 주소 또는 범위가 이미 인터페이스에서 사용되는 경우 다음 메시지가 표시됩니다. "이 범위의 IP 주소는 LIF에서 이미 사용 중입니다. LIF를 이 서브넷과 연결하시겠습니까?"라는 문구입니다
   b. OK * 를 클릭하면 기존 LIF가 서브넷에 연결됩니다.

CLI를 참조하십시오

- CLI를 사용하여 서브넷 속성을 변경합니다 *

단계

서브넷 속성 수정:

```
network subnet modify -subnet-name <subnet_name> [-ipspace
<ipspace_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- 'subnet_name'은 수정하려는 서브넷의 이름입니다.
- IPSpace는 서브넷이 상주하는 IPspace의 이름입니다.
- 'Subnet'은 192.0.2.0/24와 같이 해당되는 경우 서브넷의 새로운 주소 및 마스크입니다.
- 게이트웨이(gateway)는 192.0.2.1과 같이 해당되는 경우 서브넷의 새로운 게이트웨이입니다. "" * 를 입력하면 게이트웨이 항목이 제거됩니다.
- IP_range는 해당되는 경우 서브넷에 할당될 IP 주소의 새 목록 또는 범위입니다. IP 주소는 개별 주소, 범위 또는 IP 주소 또는 쉼표로 구분된 목록의 조합이 될 수 있습니다. 여기에 지정된 범위가 기존 IP 주소를 대체합니다.
- IP 주소 범위를 변경할 때 'force-update-lif-associations'가 필요합니다. IP 주소 범위를 수정할 때 이 옵션에 대해 값을 * TRUE * 로 설정할 수 있습니다. 서비스 프로세서 또는 네트워크 인터페이스가 지정된 범위의 IP 주소를 사용하는 경우 이 명령은 실패합니다. 이 값을 * true * 로 설정하면 수동으로 주소를 지정한 모든 인터페이스가 현재 서브넷에 연결되어 명령이 성공할 수 있습니다.

다음 명령을 실행하면 서브넷 sub3의 게이트웨이 IP 주소가 수정됩니다.

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

에 대한 자세한 내용은 `network subnet modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크의 서브넷을 봅니다

IPspace 내의 각 서브넷에 할당된 IP 주소 목록을 표시할 수 있습니다. 출력에는 각 서브넷에서 사용할 수 있는 총 IP 주소 수와 현재 사용 중인 주소 수도 표시됩니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- ONTAP 9.12.0부터 시스템 관리자를 사용하여 서브넷 * 을 표시할 수 있습니다

단계

1. 네트워크 > 개요 > 서브넷 * 을 선택합니다.
2. 서브넷 목록을 봅니다.

CLI를 참조하십시오

- CLI를 사용하여 서브넷 * 을 표시합니다

단계

서브넷 목록과 해당 서브넷에서 사용되는 관련 IP 주소 범위를 표시합니다.

```
network subnet show
```

다음 명령을 실행하면 서브넷 및 서브넷 속성이 표시됩니다.

```
network subnet show

IPspace: Default
Subnet                  Broadcast               Avail/
Name    Subnet          Domain    Gateway       Total   Ranges
------  --------------- --------- ------------ --------
-----------------------
sub1    192.0.2.0/24     bcast1   192.0.2.1     5/9     192.0.2.92-
192.0.2.100
sub3    198.51.100.0/24  bcast3   198.51.100.1   3/3
198.51.100.7,198.51.100.9
```

에 대한 자세한 내용은 `network subnet show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크에서 서브넷을 삭제합니다

서브넷이 더 이상 필요하지 않고 서브넷에 할당된 IP 주소를 할당 해제하려는 경우 삭제할 수 있습니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- ONTAP 9.12.0부터는 시스템 관리자를 사용하여 서브넷 * 을 삭제할 수 있습니다

단계

1. 네트워크 > 개요 > 서브넷 * 을 선택합니다.
2. 제거하려는 서브넷 옆의 * > 삭제 * 를 선택합니다 ⋮ .
3. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 서브넷을 삭제합니다 *

이 작업에 대해

서비스 프로세서 또는 네트워크 인터페이스가 현재 지정된 범위의 IP 주소를 사용하는 경우 오류가 발생합니다. 서브넷이 삭제된 후에도 인터페이스가 IP 주소를 계속 사용하도록 하려면 -force-update-lif-associations 옵션을 true 로 설정하여 LIF와 서브넷의 연결을 제거할 수 있습니다.

단계

서브넷 삭제:

'network subnet delete -subnet-name subnet_name[-IPSpace IPSpace_name][-force-update-lif-associations true]'

다음 명령을 실행하면 IPspace ipspac1에서 서브넷 sub1이 삭제됩니다.

네트워크 서브넷 delete-subnet-name sub1-IPSpace ipspace1

에 대한 자세한 내용은 `network subnet delete` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크용 SVM을 생성합니다

SVM을 생성하여 고객에게 데이터를 제공해야 합니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- SVM 루트 볼륨에 있을 보안 스타일을 알아야 합니다.

  이 SVM에서 Hyper-V 또는 SQL Server over SMB 솔루션을 구축하려는 경우 루트 볼륨에 NTFS 보안 스타일을 사용해야 합니다. Hyper-V 파일 또는 SQL 데이터베이스 파일이 포함된 볼륨은 만들 때 NTFS 보안으로 설정되어야 합니다. 루트 볼륨 보안 스타일을 NTFS로 설정하면 실수로 UNIX 또는 혼합 보안 스타일 데이터 볼륨을 만들지 않아도 됩니다.

- ONTAP 9.13.1부터 스토리지 VM에 대한 최대 용량을 설정할 수 있습니다. SVM이 임계값 용량 수준에 도달할 경우에도 경고를 구성할 수 있습니다. 자세한 내용은 을 SVM 용량 관리참조하십시오.

시스템 관리자

System Manager를 사용하여 스토리지 VM을 생성할 수 있습니다.

단계

1. 스토리지 VM * 을 선택합니다.
2. + Add 스토리지 VM을 생성하려면 클릭하십시오.
3. 스토리지 VM의 이름을 지정합니다.
4. 액세스 프로토콜을 선택합니다.
   - SMB/CIFS, NFS를 지원합니다
   - iSCSI
   - FC
   - NVMe를 참조하십시오
     i. SMB/CIFS 활성화 * 를 선택한 경우 다음 구성을 완료합니다.

필드 또는 확인란	설명
관리자 이름	SMB/CIFS 스토리지 VM의 관리자 사용자 이름을 지정합니다.
암호	SMB/CIFS 스토리지 VM의 관리자 암호를 지정합니다.
서버 이름	SMB/CIFS 스토리지 VM의 서버 이름을 지정합니다.
Active Directory 도메인	SMB/CIFS 스토리지 VM에 대한 사용자 인증을 제공할 Active Directory 도메인을 지정합니다.
조직 구성 단위	SMB/CIFS 서버와 연결된 Active Directory 도메인 내의 조직 단위를 지정합니다. "CN=Computers"가 기본값입니다. 이 값은 수정할 수 있습니다.
스토리지 VM의 공유에 액세스하는 동안 데이터를 암호화합니다	SMB 3.0을 사용하여 데이터를 암호화하여 SMB/CIFS 스토리지 VM의 공유에 대한 무단 파일 액세스를 방지합니다.
도메인	SMB/CIFS 스토리지 VM에 대해 나열된 도메인을 추가, 제거 또는 재정렬합니다.
이름 서버	SMB/CIFS 스토리지 VM의 이름 서버를 추가, 제거 또는 재정렬합니다.
기본 언어	스토리지 VM 및 해당 볼륨에 대한 기본 언어 인코딩 설정을 지정합니다. CLI를 사용하여 스토리지 VM 내의 개별 볼륨에 대한 설정을 변경할 수 있습니다.

네트워크 인터페이스	스토리지 VM에 대해 구성한 각 네트워크 인터페이스에 대해 기존 서브넷을 선택하거나(하나 이상의 서브넷이 있는 경우) * 서브넷 없이 * 를 지정하고 * IP 주소 * 및 * 서브넷 마스크 * 필드를 작성합니다. 필요한 경우 다음 모든 인터페이스에 대해 동일한 서브넷 마스크 및 게이트웨이 사용 * 확인란을 선택합니다. 시스템에서 자동으로 홈 포트를 선택하도록 하거나 목록에서 사용할 포트를 수동으로 선택할 수 있습니다.
관리자 계정을 관리합니다	스토리지 VM 관리자 계정을 관리하려면 이 확인란을 선택합니다. 이 옵션을 선택한 경우 사용자 이름, 암호를 지정하고 암호를 확인한 다음 스토리지 VM 관리를 위한 네트워크 인터페이스를 추가할 것인지 여부를 지정합니다.

1. Enable NFS * 를 선택한 경우 다음 구성을 완료합니다.

필드 또는 확인란	설명
NFS 클라이언트 액세스 허용 확인란을 선택합니다	NFS 스토리지 VM에서 생성된 모든 볼륨이 루트 볼륨 경로 "/"를 사용하여 마운트하고 트래버스해야 할 경우 이 확인란을 선택합니다. 엑스포트 정책 "기본값"에 규칙을 추가하여 무중단 마운트 트래버설을 허용합니다.

규칙	규칙을 만들려면 + Add 클릭하십시오. • 클라이언트 사양: 호스트 이름, IP 주소, 넷그룹 또는 도메인을 지정합니다. • 액세스 프로토콜: 다음 옵션의 조합을 선택합니다. ◦ SMB/CIFS ◦ FlexCache ◦ NFS 를 참조하십시오 ▪ NFSv3 ▪ NFSv4 • 액세스 세부 정보: 각 사용자 유형에 대해 읽기 전용, 읽기/쓰기 또는 고급 사용자 액세스 수준을 지정합니다. 사용자 유형은 다음과 같습니다. ◦ 모두 ◦ 모두(익명 사용자) ◦ Unix ◦ Kerberos 5 ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM 규칙을 저장합니다.
기본 언어	스토리지 VM 및 해당 볼륨에 대한 기본 언어 인코딩 설정을 지정합니다. CLI를 사용하여 스토리지 VM 내의 개별 볼륨에 대한 설정을 변경할 수 있습니다.
네트워크 인터페이스	스토리지 VM에 대해 구성한 각 네트워크 인터페이스에 대해 기존 서브넷을 선택하거나(하나 이상의 서브넷이 있는 경우) * 서브넷 없이 * 를 지정하고 * IP 주소 * 및 * 서브넷 마스크 * 필드를 작성합니다. 필요한 경우 다음 모든 인터페이스에 대해 동일한 서브넷 마스크 및 게이트웨이 사용 * 확인란을 선택합니다. 시스템에서 자동으로 홈 포트를 선택하도록 하거나 목록에서 사용할 포트를 수동으로 선택할 수 있습니다.
관리자 계정을 관리합니다	스토리지 VM 관리자 계정을 관리하려면 이 확인란을 선택합니다. 이 옵션을 선택한 경우 사용자 이름, 암호를 지정하고 암호를 확인한 다음 스토리지 VM 관리를 위한 네트워크 인터페이스를 추가할 것인지 여부를 지정합니다.

1. iSCSI 활성화 * 를 선택한 경우 다음 구성을 완료합니다.

필드 또는 확인란	설명
네트워크 인터페이스	스토리지 VM에 대해 구성한 각 네트워크 인터페이스에 대해 기존 서브넷을 선택하거나(하나 이상의 서브넷이 있는 경우) * 서브넷 없이 * 를 지정하고 * IP 주소 * 및 * 서브넷 마스크 * 필드를 작성합니다. 필요한 경우 다음 모든 인터페이스에 대해 동일한 서브넷 마스크 및 게이트웨이 사용 * 확인란을 선택합니다. 시스템에서 자동으로 홈 포트를 선택하도록 하거나 목록에서 사용할 포트를 수동으로 선택할 수 있습니다.
관리자 계정을 관리합니다	스토리지 VM 관리자 계정을 관리하려면 이 확인란을 선택합니다. 이 옵션을 선택한 경우 사용자 이름, 암호를 지정하고 암호를 확인한 다음 스토리지 VM 관리를 위한 네트워크 인터페이스를 추가할 것인지 여부를 지정합니다.

1. FC * 활성화 를 선택한 경우 다음 구성을 완료합니다.

필드 또는 확인란	설명
FC 포트를 구성합니다	스토리지 VM에 포함할 노드에서 네트워크 인터페이스를 선택합니다. 노드당 두 개의 네트워크 인터페이스를 사용하는 것이 좋습니다.
관리자 계정을 관리합니다	스토리지 VM 관리자 계정을 관리하려면 이 확인란을 선택합니다. 이 옵션을 선택한 경우 사용자 이름, 암호를 지정하고 암호를 확인한 다음 스토리지 VM 관리를 위한 네트워크 인터페이스를 추가할 것인지 여부를 지정합니다.

1. Enable NVMe/FC * 를 선택한 경우 다음 구성을 완료합니다.

필드 또는 확인란	설명
FC 포트를 구성합니다	스토리지 VM에 포함할 노드에서 네트워크 인터페이스를 선택합니다. 노드당 두 개의 네트워크 인터페이스를 사용하는 것이 좋습니다.
관리자 계정을 관리합니다	스토리지 VM 관리자 계정을 관리하려면 이 확인란을 선택합니다. 이 옵션을 선택한 경우 사용자 이름, 암호를 지정하고 암호를 확인한 다음 스토리지 VM 관리를 위한 네트워크 인터페이스를 추가할 것인지 여부를 지정합니다.

1. NVMe/TCP * 활성화 를 선택한 경우 다음 구성을 완료합니다.

필드 또는 확인란	설명

네트워크 인터페이스	스토리지 VM에 대해 구성한 각 네트워크 인터페이스에 대해 기존 서브넷을 선택하거나(하나 이상의 서브넷이 있는 경우) * 서브넷 없이 * 를 지정하고 * IP 주소 * 및 * 서브넷 마스크 * 필드를 작성합니다. 필요한 경우 다음 모든 인터페이스에 대해 동일한 서브넷 마스크 및 게이트웨이 사용 * 확인란을 선택합니다. 시스템에서 자동으로 홈 포트를 선택하도록 하거나 목록에서 사용할 포트를 수동으로 선택할 수 있습니다.
관리자 계정을 관리합니다	스토리지 VM 관리자 계정을 관리하려면 이 확인란을 선택합니다. 이 옵션을 선택한 경우 사용자 이름, 암호를 지정하고 암호를 확인한 다음 스토리지 VM 관리를 위한 네트워크 인터페이스를 추가할 것인지 여부를 지정합니다.

1. 변경 사항을 저장합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 서브넷을 생성합니다.

단계

1. SVM 루트 볼륨을 포함할 Aggregate를 결정합니다.

   '스토리지 집계 show-has-mroot false'

   루트 볼륨을 포함할 최소 1GB의 여유 공간이 있는 애그리게이트를 선택해야 합니다. SVM에서 NAS 감사를 구성하려면 감사가 활성화된 경우 감사 스테이징 볼륨을 생성하는 데 사용 중인 추가 공간이 있어야 하며 루트 애그리게이트에 최소 3GB의 여유 공간이 있어야 합니다.

   > 기존 SVM에서 NAS 감사가 이미 활성화되어 있는 경우 애그리게이트 생성이 성공적으로 완료된 직후 애그리게이트의 스테이징 볼륨이 생성됩니다.

2. SVM 루트 볼륨을 생성할 애그리게이트의 이름을 기록합니다.
3. SVM을 생성할 때 언어를 지정할 계획이고 사용할 값을 모르는 경우 지정할 언어의 값을 식별하고 기록하십시오.

   "vserver create-language?

4. SVM을 생성할 때 스냅샷 정책을 지정할 계획이지만 정책 이름을 모르는 경우, 사용 가능한 정책을 나열하고 사용할 스냅샷 정책의 이름을 식별하여 기록합니다.

   '볼륨 스냅샷 정책 표시 - vserver_vserver_name_'

5. SVM을 생성할 때 할당량 정책을 지정할 계획이고 정책 이름을 모를 경우, 사용 가능한 정책을 나열하고 사용할 할당량 정책의 이름을 식별하고 기록합니다.

   '볼륨 할당량 정책 표시 - vserver_vserver_name_'

6. SVM 생성:

'vserver create-vserver_vserver_name_-aggregate_aggregate_name_-rootvolume_root_volume_name_-rootvolume-security-style{unix|ntfs|mixed}[-IPSpace_hIPspace_name_] [-language>] [-snapshot-policy_snapshot_snapshot_policy_name_] [-quota-policy_policy_name_ comment_comment_comment_comment]'] - comment_

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
-rootvolume-security-style ntfs -ipspace ipspace1 -language
en_US.UTF-8
```

([Job 72] Job Succeeded: Vserver creation completed.

7. SVM 구성이 올바른지 확인합니다.

   'vserver show-vserver vs1'

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

   이 예제에서 명령은 IPspace "ipspace1"에서 "vs1"이라는 SVM을 생성합니다. 루트 볼륨의 이름은 "VS1_root"이며 NTFS 보안 스타일로 aggr3에 생성됩니다.

ONTAP 9.13.1부터 SVM의 볼륨에 처리량 하한 및 상한 제한을 적용하여 적응형 QoS 정책 그룹 템플릿을 설정할 수 있습니다. SVM을 생성한 후에만 이 정책을 적용할 수 있습니다. 이 프로세스에 대한 자세한 내용은 을 적응형 정책 그룹 템플릿을 설정합니다참조하십시오.

논리 인터페이스(LIF)

LIF 개요

ONTAP 클러스터의 **LIF** 구성에 대해 자세히 알아보십시오

LIF(논리 인터페이스)는 클러스터의 노드에 대한 네트워크 액세스 지점을 나타냅니다. 클러스터가 네트워크를 통해 통신을 주고받는 포트에 LIF를 구성할 수 있습니다.

클러스터 관리자는 다음을 생성, 보기, 수정, 마이그레이션, 되돌리기, 또는 LIF를 삭제합니다. SVM 관리자는 SVM과 연결된 LIF만 볼 수 있습니다.

LIF는 서비스 정책, 홈 포트, 홈 노드, 페일오버할 포트 목록, 방화벽 정책과 같은 관련 특성을 가진 IP 주소 또는 WWPN입니다. 클러스터가 네트워크를 통해 통신을 주고받는 포트에 LIF를 구성할 수 있습니다.

ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 참조하십시오 "LIF의 방화벽 정책을 구성합니다".

LIF는 다음 포트에서 호스팅할 수 있습니다.

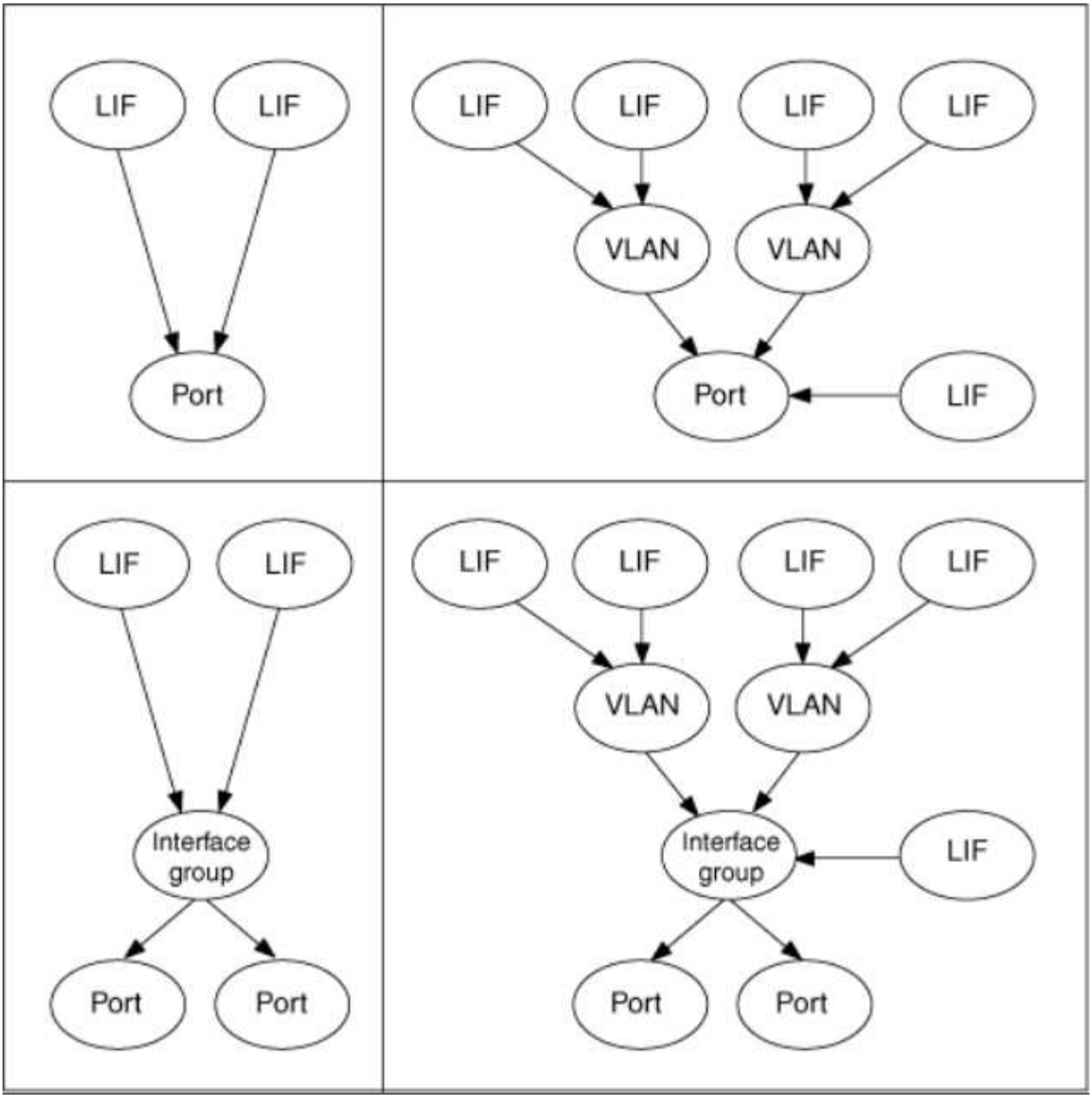
- 인터페이스 그룹에 속하지 않는 물리적 포트입니다
- 인터페이스 그룹
- VLAN
- VLAN을 호스팅하는 물리적 포트 또는 인터페이스 그룹
- 가상 IP(VIP) 포트

  ONTAP 9.5부터 VIP LIF가 지원되며 VIP 포트에서 호스팅됩니다.

LIF에서 FC와 같은 SAN 프로토콜을 구성하는 동안에는 WWPN과 연결됩니다.

"SAN 관리"

다음 그림에서는 ONTAP 시스템의 포트 계층을 보여 줍니다.



LIF 페일오버 및 반환

LIF 페일오버는 LIF가 홈 노드 또는 포트에서 HA 파트너 노드 또는 포트로 이동할 때 발생합니다. LIF 페일오버는 ONTAP에 의해 자동으로 트리거되거나, 클러스터 관리자가 물리적 이더넷 링크 다운 또는 복제된 데이터베이스(RDB) 쿼럼에서 노드 드롭과 같은 특정 이벤트에 대해 수동으로 트리거할 수 있습니다. LIF 페일오버가 발생할 경우 ONTAP은 페일오버 이유가 해결될 때까지 파트너 노드에서 정상 작업을 계속합니다. 홈 노드나 포트가 상태를 회복하면 LIF가 HA 파트너로부터 홈 노드 또는 포트로 되돌아갑니다. 이 재버전을 반환이라고 합니다.

LIF 페일오버 및 기브백의 경우 각 노드의 포트는 동일한 브로드캐스트 도메인에 속해야 합니다. 각 노드의 관련 포트가 동일한 브로드캐스트 도메인에 속해 있는지 확인하려면 다음을 참조하십시오.

- ONTAP 9.8 이상: "수리 포트 도달 가능성"
- ONTAP 9.7 이하: "브로드캐스트 도메인에서 포트를 추가하거나 제거합니다"

LIF 페일오버가 사용되도록 설정된 LIF의 경우(자동 또는 수동) 다음이 적용됩니다.

- 데이터 서비스 정책을 사용하는 LIF의 경우 페일오버 정책 제한 사항을 확인할 수 있습니다.
  - ONTAP 9.6 이상: "ONTAP 9.6 이상의 LIF 및 서비스 정책"
  - ONTAP 9.5 이하: "ONTAP 9.5 이전 버전에서 LIF 역할"
- LIF 자동 되돌리기는 자동 되돌리기가 로 설정된 경우 발생합니다 `true` LIF의 홈 포트가 정상 상태이고 LIF를 호스팅할 수 있는 경우,
- 계획된 또는 계획되지 않은 노드 테이크오버 경우, 테이크오버된 노드의 LIF가 HA 파트너로 페일오버됩니다. LIF가 페일오버되는 포트는 VIF Manager에 의해 결정됩니다.
- 페일오버가 완료된 후 LIF는 정상적으로 작동합니다.
- 반환이 시작되면 자동 되돌리기가 로 설정된 경우 LIF는 홈 노드와 포트로 되돌아갑니다 `true`.
- 이더넷 링크가 하나 이상의 LIF를 호스팅하는 포트에서 중지되면 VIF Manager가 LIF를 주 포트에서 같은 브로드캐스트 도메인의 다른 포트로 마이그레이션합니다. 새 포트가 같은 노드 또는 해당 HA 파트너에 있을 수 있습니다. 링크가 복구되고 자동 되돌리기가 로 설정된 경우 `true`VIF Manager가 LIF를 홈 노드와 홈 포트로 되돌립니다.
- 노드가 복제된 데이터베이스(RDB) 쿼럼에서 벗어나면 VIF Manager가 쿼럼 노드의 LIF를 HA 파트너로 마이그레이션합니다. 노드가 쿼럼으로 돌아온 후 자동 되돌리기가 로 설정된 경우 `true`VIF Manager가 LIF를 홈 노드와 홈 포트로 되돌립니다.

포트 유형별 **ONTAP LIF** 호환성에 대해 알아보십시오

LIF는 다양한 포트 유형을 지원하는 다양한 특성을 가질 수 있습니다.

인터클러스터 및 관리 LIF가 동일한 서브넷에 구성된 경우 관리 트래픽이 외부 방화벽에 의해 차단될 수 있으며 AutoSupport 및 NTP 연결이 실패할 수 있습니다. 'network interface modify -vserver_vserver name_-lif_인터클러스터 LIF_-status-admin up|down' 명령을 실행하여 인터클러스터 LIF를 전환하여 시스템을 복구할 수 있습니다. 그러나 이 문제를 방지하려면 인터클러스터 LIF 및 관리 LIF를 다른 서브넷에 설정해야 합니다.

LIF	설명
데이터 LIF	스토리지 가상 시스템(SVM)과 연결되고 클라이언트와 통신하는 데 사용되는 LIF 한 포트에 여러 개의 데이터 LIF가 존재할 수 있습니다. 이러한 인터페이스는 전체 클러스터에서 마이그레이션하거나 페일오버할 수 있습니다. 방화벽 정책을 관리 LIF로 수정하여 SVM 관리 LIF로 사용할 수 있습니다. NIS, LDAP, Active Directory, WINS 및 DNS 서버에 설정된 세션에서 데이터 LIF를 사용합니다.
클러스터 LIF	클러스터 내 노드 간에 클러스터 간 트래픽을 전송하는 데 사용되는 LIF. 클러스터 LIF는 항상 클러스터 포트에 생성해야 합니다. 클러스터 LIF는 동일한 노드의 클러스터 포트 간에 페일오버할 수 있으며 원격 노드로 마이그레이션하거나 페일오버할 수 없습니다. 새 노드가 클러스터에 연결되면 IP 주소가 자동으로 생성됩니다. 그러나 IP 주소를 클러스터 LIF에 수동으로 할당하려면 새 IP 주소가 기존 클러스터 LIF와 동일한 서브넷 범위에 있어야 합니다.
클러스터 관리 LIF	LIF는 전체 클러스터에 대한 단일 관리 인터페이스를 제공합니다. 클러스터 관리 LIF는 클러스터의 모든 노드로 페일오버할 수 있습니다. 클러스터 또는 인터클러스터 포트로 페일오버할 수 없습니다

인터클러스터 LIF	클러스터 간 통신, 백업 및 복제에 사용되는 LIF. 클러스터 피어링을 설정하려면 먼저 클러스터의 각 노드에 대한 인터클러스터 LIF를 생성해야 합니다. 이러한 LIF는 동일한 노드의 포트로만 페일오버할 수 있습니다. 클러스터의 다른 노드로 마이그레이션하거나 페일오버할 수 없습니다.
노드 관리 LIF	LIF는 클러스터의 특정 노드를 관리하기 위한 전용 IP 주소를 제공합니다. 노드 관리 LIF는 클러스터를 생성하거나 결합할 때 생성됩니다. 이러한 LIF는 클러스터에서 노드에 액세스할 수 없을 때와 같이 시스템 유지 관리에 사용됩니다.
VIP LIF	VIP LIF는 VIP 포트에 생성된 모든 데이터 LIF입니다. 자세한 내용은 을 참조하십시오"가상 IP(VIP) LIF를 구성합니다".

관련 정보

- "네트워크 인터페이스 수정"

ONTAP 버전에 지원되는 **LIF** 서비스 정책 및 역할

시간이 지남에 따라 ONTAP에서 LIF에서 지원되는 트래픽 유형을 관리하는 방식이 변경되었습니다.

- ONTAP 9 .5 이전 릴리즈에서는 LIF 역할 및 방화벽 서비스를 사용합니다.
- ONTAP 9 .6 이상 릴리즈에서는 LIF 서비스 정책을 사용합니다.
  - ONTAP 9 .5 릴리스에는 LIF 서비스 정책이 도입되었습니다.
  - ONTAP 9 .6은 LIF 역할을 LIF 서비스 정책으로 교체했습니다.
  - ONTAP 9.10.1은 방화벽 서비스를 LIF 서비스 정책으로 교체했습니다.

구성하는 방법은 사용 중인 ONTAP 릴리스에 따라 다릅니다.

추가 정보:

- 방화벽 정책은 "명령: firewall-policy-show"을 참조하십시오.
- LIF 역할은 를 참조하십시오"LIF 역할(ONTAP 9.5 이하)".
- LIF 서비스 정책은 을 "LIF 및 서비스 정책(ONTAP 9.6 이상)"참조하십시오.

ONTAP LIF 및 서비스 정책에 대해 자세히 알아보십시오

LIF에서 지원되는 트래픽 유형을 결정하는 LIF에 서비스 정책(LIF 역할 또는 방화벽 정책 대신)을 할당할 수 있습니다. 서비스 정책은 LIF에서 지원하는 네트워크 서비스 모음을 정의합니다. ONTAP는 LIF와 연결할 수 있는 기본 서비스 정책 세트를 제공합니다.

네트워크 트래픽을 관리하는 방법은 ONTAP 9.7 및 이전 버전에서 다릅니다. ONTAP 9.7 이하를 실행하는 네트워크에서 트래픽을 관리해야 하는 경우 을 참조하십시오"LIF 역할(ONTAP 9.5 이하)".

FCP 및 NVMe/FCP 프로토콜은 현재 서비스 정책이 필요하지 않습니다.

네트워크 인터페이스 service-policy show 명령을 사용하여 서비스 정책과 세부 정보를 표시할 수 있습니다

에 대한 자세한 내용은 `network interface service-policy show` "ONTAP 명령 참조입니다"을 참조하십시오.

특정 서비스에 바인딩되지 않은 기능은 시스템 정의 동작을 사용하여 아웃바운드 연결에 대해 LIF를 선택합니다.

빈 서비스 정책이 있는 LIF에서 애플리케이션이 예기치 않게 동작할 수 있습니다.

시스템 **SVM**에 대한 서비스 정책

관리 SVM과 모든 시스템 SVM에는 관리 및 인터클러스터 LIF를 포함하여 해당 SVM의 LIF에 사용할 수 있는 서비스 정책이 포함되어 있습니다. 이러한 정책은 IPspace가 생성될 때 시스템에서 자동으로 생성됩니다.

다음 표에는 ONTAP 9.12.1부터 시작하는 시스템 SVM에 있는 LIF에 대한 내장 정책이 나와 있습니다. 다른 릴리즈의 경우 다음 명령을 사용하여 서비스 정책과 세부 정보를 표시합니다.

네트워크 인터페이스 서비스 정책 쇼

정책	포함된 서비스	동등한 역할	설명
기본값 - 인터클러스터	인터클러스터 코어, 관리 - https	인터클러스터	인터클러스터 트래픽을 전송하는 LIF에서 사용됩니다. 참고: 서비스 인터클러스터 코어는 net-인터클러스터 서비스 정책이라는 이름의 ONTAP 9.5에서 사용할 수 있습니다.
default-route-공지	관리 - BGP	-	BGP 피어 연결을 전달하는 LIF에서 사용됩니다. 참고: net-route-공지 서비스 정책과 함께 ONTAP 9.5에서 사용할 수 있습니다.
기본 관리	관리 코어, 관리 - https, management-http, management-ssh, management-autosupport, 관리 - EMS, 관리 - DNS - 클라이언트, 관리 - ad - 클라이언트, 관리 - LDAP - 클라이언트, 관리 - NIS - 클라이언트, 관리 - NTP - 클라이언트, 관리 - 로그 전달	노드 관리 또는 클러스터 관리	시스템 범위 관리 정책을 사용하여 시스템 SVM이 소유하는 노드 및 클러스터 범위 관리 LIF를 생성할 수 있습니다. 이러한 LIF는 DNS, AD, LDAP 또는 NIS 서버에 대한 아웃바운드 연결뿐만 아니라 전체 시스템을 대신하여 실행되는 애플리케이션을 지원하기 위한 일부 추가 연결에 사용할 수 있습니다. ONTAP 9.12.1부터 서비스를 사용하여 감사 로그를 원격 syslog 서버에 전달하는 데 사용되는 LIF를 제어할 수 `management-log-forwarding` 있습니다.

다음 표에는 ONTAP 9.11.1부터 시작하는 시스템 SVM에서 LIF가 사용할 수 있는 서비스가 나와 있습니다.

서비스	페일오버 제한 사항	설명
인터클러스터 코어	홈 노드 전용	핵심 인터클러스터 서비스
관리 코어	-	핵심 관리 서비스

관리 - ssh	-	SSH 관리 액세스를 위한 서비스
관리 - http	-	HTTP 관리 액세스를 위한 서비스입니다
관리 - https	-	HTTPS 관리 액세스를 위한 서비스
AutoSupport에 대해 설명합니다	-	AutoSupport 페이로드 게시와 관련된 서비스
관리 - BGP	홈 포트 전용	BGP 피어 상호 작용과 관련된 서비스
backup-ndmp-control입니다	-	NDMP 백업 제어를 위한 서비스
관리 - EMS	-	관리 메시징 액세스를 위한 서비스
관리 - NTP - 클라이언트	-	ONTAP 9.10.1에서 도입되었습니다. NTP 클라이언트 액세스를 위한 서비스입니다.
관리 - NTP - 서버	-	ONTAP 9.10.1에서 도입되었습니다. NTP 서버 관리 액세스를 위한 서비스입니다
관리 - portmap	-	포트맵 관리 서비스
관리 - rsh - 서버	-	rsh 서버 관리를 위한 서비스
관리 - SNMP - 서버	-	SNMP 서버 관리를 위한 서비스입니다
관리 - 텔넷 - 서버	-	텔넷 서버 관리를 위한 서비스
관리 - 로그 전달	-	ONTAP 9.12.1에서 도입되었습니다. 감사 로그 전달을 위한 서비스

데이터 **SVM**에 대한 서비스 정책

모든 데이터 SVM에는 해당 SVM의 LIF에서 사용할 수 있는 서비스 정책이 포함되어 있습니다.

다음 표에는 ONTAP 9.11.1부터 데이터 SVM에 있는 LIF에 대한 기본 제공 정책이 나와 있습니다. 다른 릴리즈의 경우 다음 명령을 사용하여 서비스 정책과 세부 정보를 표시합니다.

네트워크 인터페이스 서비스 정책 쇼

정책	포함된 서비스	등가 데이터 프로토콜	설명

기본 관리	data-core, management-https, management-ssh, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	없음	SVM 범위 관리 정책을 사용하여 데이터 SVM이 소유하는 SVM 관리 LIF를 생성할 수 있습니다. 이러한 LIF는 SVM 관리자에게 SSH 또는 HTTPS 액세스를 제공하는 데 사용할 수 있습니다. 필요한 경우 이러한 LIF를 외부 DNS, AD, LDAP 또는 NIS 서버에 대한 아웃바운드 연결에 사용할 수 있습니다.
default-data-blocks입니다	데이터 코어, 데이터 - iSCSI	iSCSI	블록 지향 SAN 데이터 트래픽을 전송하는 LIF에서 사용됩니다. ONTAP 9.10.1부터 "default-data-blocks" 정책은 사용되지 않습니다. 대신 "default-data-iscsi" 서비스 정책을 사용합니다.
default-data-files 를 선택합니다	데이터 코어, 데이터 -FPolicy-Client, 데이터-dns-server, 데이터-FlexCache, 데이터-cifs, 데이터 -nfs, 관리-dns-client, 관리-add-client, 관리 -ldap-client, 관리 -NIS-client	NFS, CIFS, FCache가 있습니다	기본 데이터 파일 정책을 사용하여 파일 기반 데이터 프로토콜을 지원하는 NAS LIF를 생성합니다. SVM에는 하나의 LIF만 있을 수 있으므로 이 정책을 통해 외부 DNS, AD, LDAP 또는 NIS 서버에 대한 아웃바운드 연결에 LIF를 사용할 수 있습니다. 연결 시 관리 LIF만 사용하도록 설정하려면 이 정책에서 이러한 서비스를 제거할 수 있습니다.
default-data-iscsi 를 참조하십시오	데이터 코어, 데이터 - iSCSI	iSCSI	iSCSI 데이터 트래픽을 전송하는 LIF에서 사용됩니다.
default-data-NVMe-TCP를 참조하십시오	데이터 코어, 데이터 - NVMe-TCP	NVMe-TCP	NVMe/TCP 데이터 트래픽을 전송하는 LIF에서 사용됩니다.

다음 표에는 데이터 SVM에서 사용할 수 있는 서비스와 각 서비스가 ONTAP 9.11.1부터 LIF의 페일오버 정책에 적용되는 모든 제한이 나와 있습니다.

서비스	페일오버 제한 사항	설명
관리 - ssh	-	SSH 관리 액세스를 위한 서비스
관리 - http	-	HTTP 관리 액세스를 위한 ONTAP 9.10.1 서비스에 도입되었습니다
관리 - https	-	HTTPS 관리 액세스를 위한 서비스
관리 - portmap	-	포트맵 관리 액세스를 위한 서비스
관리 - SNMP - 서버	-	SNMP 서버 관리 액세스를 위한 ONTAP 9.10.1 서비스에 도입되었습니다

데이터 코어	-	핵심 데이터 서비스
데이터 - NFS	-	NFS 데이터 서비스
데이터 - CIFS	-	CIFS 데이터 서비스
데이터 - FlexCache	-	FlexCache 데이터 서비스
데이터 - iSCSI	홈 포트 - AFF/FAS 전용, SFO 파트너 - ASA 전용	iSCSI 데이터 서비스
backup-ndmp-control입니다	-	ONTAP 9.10.1 백업 NDMP에서 도입되어 데이터 서비스를 제어합니다
data-dns-server 를 참조하십시오	-	ONTAP 9.10.1 DNS 서버 데이터 서비스에 도입되었습니다
데이터 - FPolicy - 클라이언트	-	파일 스크리닝 정책 데이터 서비스
데이터 NVMe-TCP	홈 포트 전용	ONTAP 9.10.1 NVMe TCP 데이터 서비스에 도입되었습니다
Data-S3-서버	-	S3(Simple Storage Service) 서버 데이터 서비스

서비스 정책이 데이터 SVM의 LIF에 할당되는 방식에 대해 알고 있어야 합니다.

- 데이터 서비스 목록을 사용해 데이터 SVM을 생성할 경우 지정된 서비스를 사용하여 해당 SVM에 내장된 "기본 데이터 파일" 및 "기본 데이터 블록" 서비스 정책을 생성합니다.
- 데이터 서비스 목록을 지정하지 않고 SVM 데이터 생성 시 기본 데이터 서비스 목록을 사용하여 해당 SVM에 내장된 "default-data-files" 및 "default-data-blocks" 서비스 정책이 생성됩니다.

  기본 데이터 서비스 목록에는 iSCSI, NFS, NVMe, SMB 및 FlexCache 서비스가 포함됩니다.

- LIF가 데이터 프로토콜 목록으로 작성되면 지정된 데이터 프로토콜에 해당하는 서비스 정책이 LIF에 할당됩니다.
- 동등한 서비스 정책이 없으면 사용자 지정 서비스 정책이 만들어집니다.
- 서비스 정책이나 데이터 프로토콜 목록 없이 LIF를 생성할 경우 기본적으로 기본 데이터 파일 서비스 정책이 LIF에 할당됩니다.

데이터 코어 서비스

데이터 코어 서비스는 LIF 역할(ONTAP 9.6에서 더 이상 사용되지 않음)을 사용하여 서비스 정책을 관리하는 LIF를 관리하도록 업그레이드된 클러스터에서 데이터 역할의 LIF를 사용한 구성 요소가 예상대로 작동할 수 있도록 합니다.

데이터 코어를 서비스로 지정해도 방화벽에서 어떠한 포트도 열리지 않지만 데이터 SVM의 서비스 정책에는 서비스가 포함되어야 합니다. 예를 들어 기본 데이터 파일 서비스 정책에는 기본적으로 다음 서비스가 포함됩니다.

- 데이터 코어
- 데이터 - NFS
- 데이터 - CIFS
- 데이터 - FlexCache

데이터 코어 서비스를 정책에 포함하여 LIF를 사용하는 모든 애플리케이션이 예상대로 작동하도록 해야 하지만, 필요한 경우 다른 세 서비스를 제거할 수 있습니다.

클라이언트 측 **LIF** 서비스

ONTAP는 ONTAP 9.10.1부터 여러 애플리케이션을 위한 클라이언트측 LIF 서비스를 제공합니다. 이러한 서비스를 통해 각 애플리케이션을 대신하여 아웃바운드 연결에 사용되는 LIF를 제어할 수 있습니다.

관리자는 다음과 같은 새로운 서비스를 통해 특정 애플리케이션의 소스 주소로 사용되는 LIF를 제어할 수 있습니다.

서비스	SVM 제한	설명
관리 - ad-client	-	ONTAP 9.11.1부터 ONTAP는 외부 AD 서버에 대한 아웃바운드 연결을 위한 Active Directory 클라이언트 서비스를 제공합니다.
관리 - DNS - 클라이언트	-	ONTAP는 ONTAP 9.11.1부터 외부 DNS 서버에 대한 아웃바운드 연결을 위한 DNS 클라이언트 서비스를 제공합니다.
관리 - LDAP - 클라이언트	-	ONTAP 9.11.1부터 ONTAP는 외부 LDAP 서버에 대한 아웃바운드 연결을 위한 LDAP 클라이언트 서비스를 제공합니다.
Management - NIS - 클라이언트입니다	-	ONTAP는 ONTAP 9.11.1부터 외부 NIS 서버에 대한 아웃바운드 연결을 위한 NIS 클라이언트 서비스를 제공합니다.
관리 - NTP - 클라이언트	시스템 전용	ONTAP 9.10.1부터 ONTAP는 외부 NTP 서버에 대한 아웃바운드 연결을 위한 NTP 클라이언트 서비스를 제공합니다.
데이터 - FPolicy - 클라이언트	데이터 전용	ONTAP 9.8부터 ONTAP는 아웃바운드 FPolicy 연결을 위한 클라이언트 서비스를 제공합니다.

새로운 서비스 각각은 자동으로 일부 기본 제공 서비스 정책에 포함되지만 관리자는 기본 제공 정책에서 해당 서비스를 제거하거나 사용자 지정 정책에 추가하여 각 애플리케이션을 대신하여 아웃바운드 연결에 사용되는 LIF를 제어할 수 있습니다.

관련 정보

- "네트워크 인터페이스 service-policy show를 참조하십시오"

LIF 관리

ONTAP 클러스터에 대한 **LIF** 서비스 정책을 구성합니다

LIF 서비스 정책을 구성하여 LIF를 사용할 단일 서비스 또는 서비스 목록을 식별할 수 있습니다.

LIF에 대한 서비스 정책을 생성합니다

LIF에 대한 서비스 정책을 생성할 수 있습니다. 하나 이상의 LIF에 서비스 정책을 할당할 수 있으므로 LIF에서 단일 서비스 또는 서비스 목록에 대한 트래픽을 전송할 수 있습니다.

'network interface service-policy create' 명령을 실행하려면 고급 권한이 필요합니다.

이 작업에 대해

기본 제공 서비스 및 서비스 정책을 사용하여 데이터 및 시스템 SVM에서 데이터 및 관리 트래픽을 관리할 수 있습니다. 대부분의 사용 사례는 사용자 지정 서비스 정책을 만들지 않고 기본 제공 서비스 정책을 사용하여 충족됩니다.

필요한 경우 이러한 기본 제공 서비스 정책을 수정할 수 있습니다.

단계

1. 클러스터에서 사용 가능한 서비스를 봅니다.

```
network interface service show
```

서비스는 LIF에서 액세스하는 애플리케이션 및 클러스터에서 지원하는 애플리케이션을 나타냅니다. 각 서비스에는 응용 프로그램이 수신 대기 중인 0개 이상의 TCP 및 UDP 포트가 포함됩니다.

다음과 같은 추가 데이터 및 관리 서비스를 사용할 수 있습니다.

```
cluster1::> network interface service show

Service                     Protocol:Ports
-------                     --------------
cluster-core                -
data-cifs                   -
data-core                   -
data-flexcache              -
data-iscsi                  -
data-nfs                    -
intercluster-core           tcp:11104-11105
management-autosupport      -
management-bgp              tcp:179
management-core             -
management-https            tcp:443
management-ssh              tcp:22
12 entries were displayed.
```

2. 클러스터에 존재하는 서비스 정책을 확인합니다.

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

7 entries were displayed.
```

3. 서비스 정책 생성:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- "service_name"은 정책에 포함되어야 하는 서비스 목록을 지정합니다.
- "ip_address/mask"는 서비스 정책의 서비스에 액세스할 수 있는 주소에 대한 서브넷 마스크 목록을 지정합니다. 기본적으로 지정된 모든 서비스는 모든 서브넷의 트래픽을 허용하는 기본 허용 주소 목록인 0.0.0.0/0으로 추가됩니다. 기본값이 아닌 허용 주소 목록이 제공되는 경우 정책을 사용하는 LIF는 지정된 마스크와 일치하지 않는 소스 주소를 가진 모든 요청을 차단하도록 구성됩니다.

  다음 예에서는 _nfs_and_smb_services를 포함하는 SVM에 대해 _svm1_data_policy_라는 데이터 서비스 정책을 생성하는 방법을 보여 줍니다.

  ```
  cluster1::> set -privilege advanced
  Warning: These advanced commands are potentially dangerous; use them
  only when directed to do so by technical support.
  Do you wish to continue? (y or n): y

  cluster1::> network interface service-policy create -vserver svm1
  -policy svm1_data_policy -services data-nfs,data-cifs,data-core
  ```

  다음 예제에서는 인터클러스터 서비스 정책을 만드는 방법을 보여 줍니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. 서비스 정책이 생성되었는지 확인합니다.

```
cluster1::> network interface service-policy show
```

다음 출력에는 사용 가능한 서비스 정책이 나와 있습니다.

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          intercluster1                intercluster-core: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          svm1_data_policy             data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0

9 entries were displayed.
```

작업을 마친 후

서비스 정책을 생성할 때 또는 기존 LIF를 수정하여 LIF에 할당합니다.

LIF에 서비스 정책을 할당합니다

LIF를 생성할 때 또는 LIF를 수정하여 서비스 정책을 LIF에 할당할 수 있습니다. 서비스 정책은 LIF에서 사용할 수 있는 서비스 목록을 정의합니다.

이 작업에 대해

admin 및 Data SVM에서 LIF에 서비스 정책을 할당할 수 있습니다.

단계

서비스 정책을 LIF에 할당할 시기에 따라 다음 작업 중 하나를 수행합니다.

만약...	서비스 정책 할당...
LIF 생성	네트워크 인터페이스 create-vserver svm_name -lif <lif_name> -home-node <node_name> -home-port <port_name> {(-address <ip_address> -netmask <ip_address>) -subnet-name <subnet_name>} -service-policy <service_policy_name>
LIF 수정	네트워크 인터페이스 modify -vserver <svm_name> -lif <lif_name> -service-policy <service_policy_name>

LIF에 서비스 정책을 지정할 때 LIF의 데이터 프로토콜과 역할을 지정할 필요가 없습니다. 역할 및 데이터 프로토콜을 지정하여 LIF를 생성할 수도 있습니다.

서비스 정책은 서비스 정책을 생성할 때 지정한 SVM에 있는 LIF에서만 사용할 수 있습니다.

예

다음 예에서는 LIF의 서비스 정책을 수정하여 기본 관리 서비스 정책을 사용하는 방법을 보여 줍니다.

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

LIF 서비스 정책을 관리하는 명령입니다

네트워크 인터페이스 서비스 정책 명령을 사용하여 LIF 서비스 정책을 관리합니다.

에 대한 자세한 내용은 `network interface service-policy` "ONTAP 명령 참조입니다"을 참조하십시오.

시작하기 전에

활성 SnapMirror 관계에서 LIF의 서비스 정책을 수정하면 복제 일정이 중단됩니다. LIF를 인터클러스터에서 비인터클러스터(또는 그 반대로)로 변환하면 해당 변경 사항이 피어링된 클러스터에 복제되지 않습니다. LIF 서비스 정책을 수정한 후 피어 클러스터를 업데이트하려면 먼저 를 수행합니다 `snapmirror abort` 작동 후 복제 관계를 다시 동기화합니다.

원하는 작업	이 명령 사용...
서비스 정책 생성(고급 권한 필요)	네트워크 인터페이스 서비스 정책 만들기

원하는 작업	이 명령 사용...
기존 서비스 정책에 추가 서비스 항목 추가(고급 권한 필요)	네트워크 인터페이스 서비스 정책 추가 서비스
기존 서비스 정책 클론 생성(고급 권한 필요)	네트워크 인터페이스 서비스 정책 클론
기존 서비스 정책의 서비스 항목 수정(고급 권한 필요)	네트워크 인터페이스 서비스 정책 수정 서비스
기존 서비스 정책에서 서비스 항목 제거(고급 권한 필요)	네트워크 인터페이스 서비스 정책 제거 서비스
기존 서비스 정책 이름 바꾸기(고급 권한 필요)	네트워크 인터페이스 서비스 정책 이름 바꾸기
기존 서비스 정책 삭제(고급 권한 필요)	네트워크 인터페이스 서비스 정책 삭제
기본 제공 서비스 정책을 원래 상태로 복원(고급 권한 필요)	네트워크 인터페이스 서비스 정책 복원 - 기본값
기존 서비스 정책을 표시합니다	네트워크 인터페이스 서비스 정책 쇼

관련 정보

- "네트워크 인터페이스 서비스가 표시됩니다"
- "네트워크 인터페이스 서비스 - 정책"
- "SnapMirror가 중단되었습니다"

ONTAP LIF를 생성합니다

SVM은 하나 이상의 네트워크 논리 인터페이스(LIF)를 통해 클라이언트에 데이터를 제공합니다. 데이터에 액세스하는 데 사용할 포트에 LIF를 생성해야 합니다. LIF(네트워크 인터페이스)는 물리적 포트 또는 논리적 포트와 연결된 IP 주소입니다. 구성요소 장애가 발생할 경우 LIF가 다른 물리적 포트로 페일오버되거나 마이그레이션되어 네트워크와 계속 통신할 수 있습니다.

모범 사례

LIF 마이그레이션 중에 지연을 줄이려면 ONTAP에 연결된 스위치 포트를 스패닝 트리 에지 포트로 구성해야 합니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 기본 물리적 또는 논리적 네트워크 포트가 관리 작동 상태로 구성되어 있어야 합니다.
- 서브넷 이름을 사용하여 LIF에 대한 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 이미 존재해야 합니다.

  서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. System Manager나 network subnet create 명령을 사용하여 생성됩니다.

  에 대한 자세한 내용은 `network subnet create` "ONTAP 명령 참조입니다"을 참조하십시오.

- LIF가 처리하는 트래픽 유형을 지정하는 메커니즘이 변경되었습니다. ONTAP 9.5 이전 버전의 경우 LIF는 역할을 사용하여 처리할 트래픽 유형을 지정합니다. ONTAP 9.6부터 LIF는 서비스 정책을 사용하여 처리할 트래픽 유형을 지정합니다.

이 작업에 대해

- NAS 및 SAN 프로토콜은 동일한 LIF에 할당할 수 없습니다.

  지원되는 프로토콜은 SMB, NFS, FlexCache, iSCSI 및 FC입니다. iSCSI 및 FC는 다른 프로토콜과 결합할 수 없습니다. 그러나 NAS 및 이더넷 기반 SAN 프로토콜은 동일한 물리적 포트에 존재할 수 있습니다.

  - SMB 트래픽이 있는 LIF가 홈 노드로 자동 복구되도록 구성하지 않아야 합니다. SMB를 통해 Hyper-V 또는 SQL Server의 무중단 운영을 지원하는 솔루션을 호스팅하려는 SMB 서버의 경우 이 권장 사항이 필수입니다.
- 동일한 네트워크 포트에서 IPv4 및 IPv6 LIF를 모두 생성할 수 있습니다.
- SVM에서 사용하는 DNS, NIS, LDAP, Active Directory 등의 모든 이름 매핑 및 호스트 이름 확인 서비스 SVM의 데이터 트래픽을 처리하는 하나 이상의 LIF에서 연결할 수 있어야 합니다.
- 클러스터 간 노드 트래픽을 처리하는 LIF는 LIF가 관리 트래픽을 처리하거나 데이터 트래픽을 처리하는 LIF와 같은 서브넷에 있으면 안 됩니다.
- 유효한 페일오버 목표가 없는 LIF를 생성하면 경고 메시지가 표시됩니다.
- 클러스터에 LIF가 많은 경우 클러스터에서 지원되는 LIF 용량을 확인할 수 있습니다.
  - 시스템 관리자: ONTAP 9.12.0부터 네트워크 인터페이스 그리드의 처리량을 확인합니다.
  - CLI: 고급 권한 수준에서 network interface capacity details show 명령을 사용하여 각 노드에서 지원되는 LIF 용량과 network interface capacity show 명령을 사용하십시오.

    및 `network interface capacity details show` 에 대한 자세한 `network interface capacity show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.
- ONTAP 9.7부터 동일한 서브넷에 있는 SVM에 대한 다른 LIF가 이미 있는 경우 LIF의 홈 포트를 지정할 필요가 없습니다. ONTAP는 동일한 서브넷에 이미 구성된 다른 LIF와 동일한 브로드캐스트 도메인에 있는 지정된 홈 노드에서 랜덤 포트를 자동으로 선택합니다.

  ONTAP 9.4부터는 FC-NVMe가 지원됩니다. FC-NVMe LIF를 생성하는 경우 다음 사항을 알아야 합니다.

  - NVMe 프로토콜은 LIF가 생성된 FC 어댑터에서 지원되어야 합니다.
  - FC-NVMe는 데이터 LIF에서 유일한 데이터 프로토콜일 수 있습니다.
- SAN을 지원하는 모든 SVM(스토리지 가상 머신)에서 관리 트래픽을 처리하는 하나의 LIF를 구성해야 합니다.
- NVMe LIF 및 네임스페이스는 동일한 노드에서 호스팅되어야 합니다.
- SVM당, 노드당 최대 2개의 NVMe LIF를 구성할 수 있다.
- 서브넷을 사용하여 네트워크 인터페이스를 만들면 ONTAP는 선택한 서브넷에서 사용 가능한 IP 주소를 자동으로 선택하고 네트워크 인터페이스에 할당합니다. 서브넷이 두 개 이상인 경우 서브넷을 변경할 수 있지만 IP 주소는 변경할 수 없습니다.
- 네트워크 인터페이스를 위해 SVM을 생성(추가)할 때 기존 서브넷 범위에 있는 IP 주소를 지정할 수 없습니다. 서브넷 충돌 오류가 발생합니다. 이 문제는 SVM 설정 또는 클러스터 설정에서 클러스터 간 네트워크 인터페이스를 생성하거나 수정하는 등 네트워크 인터페이스를 위한 다른 워크플로우에서 발생합니다.
- ONTAP 9.10.1부터 `network interface` CLI 명령에 RDMA 기반 NFS 구성에 대한 매개 변수가 포함됩니다 `-rdma-protocols`. RDMA 기반 NFS 구성용 네트워크 인터페이스 생성은 ONTAP 9.12.1부터 System

Manager에서 지원됩니다. 자세한 내용은 을 RDMA를 통해 NFS에 대해 LIFS를 구성합니다참조하십시오.

- ONTAP 9.11.1부터 ASA(All-Flash SAN 어레이) 플랫폼에서 자동 iSCSI LIF 페일오버를 사용할 수 있습니다.

  iSCSI LIF 페일오버가 자동으로 활성화됨(페일오버 정책은 'fo-partner-only'로 설정되고 자동 되돌리기 값은 'true'로 설정됨) 새로 생성된 iSCSI LIF에서 지정된 SVM에 iSCSI LIF가 없거나 지정된 SVM에 있는 기존 iSCSI LIF가 iSCSI LIF 페일오버로 이미 활성화되어 있는 경우.

  ONTAP 9.11.1 이상으로 업그레이드한 후 iSCSI LIF 페일오버 기능을 사용하도록 설정되지 않은 SVM에 기존 iSCSI LIF가 있고 동일한 SVM에 새 iSCSI LIF를 생성하고, 새로운 iSCSI LIF는 SVM에 있는 기존 iSCSI LIF와 동일한 페일오버 정책(비활성화)을 가정합니다.

  "ASA 플랫폼의 iSCSI LIF 페일오버"

ONTAP 9.7부터 ONTAP는 해당 IPspace의 동일한 서브넷에 이미 있는 LIF가 하나 이상 있으면 LIF의 홈 포트를 자동으로 선택합니다. ONTAP은 해당 서브넷에 있는 다른 LIF와 동일한 브로드캐스트 도메인에서 홈 포트를 선택합니다. 홈 포트는 여전히 지정할 수 있지만 더 이상 필요하지 않습니다(지정된 IPspace의 해당 서브넷에 LIF가 아직 없는 경우).

ONTAP 9.12.0부터는 — System Manager 또는 CLI를 사용하는 인터페이스에 따라 절차가 달라집니다.

시스템 관리자

- System Manager를 사용하여 네트워크 인터페이스를 추가합니다 *

단계

1. Network > Overview > Network Interfaces * 를 선택합니다.
2. 를 선택합니다 + Add .
3. 다음 인터페이스 역할 중 하나를 선택합니다.
   a. 데이터
   b. 인터클러스터
   c. SVM 관리
4. 프로토콜을 선택합니다.
   a. SMB/CIFS 및 NFS
   b. iSCSI
   c. FC
   d. NVMe/FC
   e. NVMe/TCP
5. LIF의 이름을 지정하거나 이전 선택 사항에서 생성한 이름을 그대로 사용합니다.
6. 홈 노드를 수락하거나 드롭다운을 사용하여 하나를 선택합니다.
7. 선택한 SVM의 IPspace에서 하나 이상의 서브넷이 구성된 경우 서브넷 드롭다운이 표시됩니다.
   a. 서브넷을 선택한 경우 드롭다운에서 선택합니다.
   b. 서브넷 없이 진행하면 브로드캐스트 도메인 드롭다운이 표시됩니다.
      i. IP 주소를 지정합니다. IP 주소를 사용 중인 경우 경고 메시지가 표시됩니다.
      ii. 서브넷 마스크를 지정합니다.
8. 브로드캐스트 도메인에서 홈 포트를 자동으로(권장) 선택하거나 드롭다운 메뉴에서 선택합니다. 홈 포트 컨트롤은 브로드캐스트 도메인 또는 서브넷 선택에 따라 표시됩니다.
9. 네트워크 인터페이스를 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 LIF * 를 생성합니다

단계

1. LIF에 사용할 브로드캐스트 도메인 포트를 결정합니다.

   '네트워크 포트 브로드캐스트-도메인 쇼-IPSpace_ipspace1_'

```
IPspace     Broadcast                         Update
Name        Domain name   MTU   Port List     Status Details
ipspace1
            default       1500
                                node1:e0d     complete
                                node1:e0e     complete
                                node2:e0d     complete
                                node2:e0e     complete
```

에 대한 자세한 내용은 `network port broadcast-domain show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. LIF에 사용할 서브넷에 사용되지 않는 IP 주소가 충분히 있는지 확인합니다.

   'network subnet show - IPSpace_ipspace1_'

   에 대한 자세한 내용은 `network subnet show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 데이터에 액세스하는 데 사용할 포트에 하나 이상의 LIF를 생성합니다.

   NetApp은 데이터 SVM의 모든 LIF에 대한 서브넷 개체를 생성할 것을 권장합니다. 이는 각 서브넷 객체에 연결된 브로드캐스트 도메인이 있기 때문에 ONTAP에서 대상 클러스터의 페일오버 대상을 결정할 수 있도록 서브넷 객체를 사용하는 MetroCluster 구성에서 특히 중요합니다. 자세한 내용은 을 "서브넷을 생성합니다"참조하십시오.

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

   - 홈 노드는 LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환하는 노드입니다.

     또한 LIF가 -auto-revert 옵션을 사용하여 홈 노드 및 홈 포트로 자동으로 되돌아가는지 여부를 지정할 수도 있습니다.

   에 대한 자세한 내용은 `network interface revert` "ONTAP 명령 참조입니다"을 참조하십시오.

   - '-home-port'는 LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 물리적 또는 논리적 포트입니다.
   - IP 주소는 '-address' 및 '-netmask' 옵션을 사용하여 지정하거나 '-subnet_name' 옵션을 사용하여 서브넷에서 할당을 활성화할 수 있습니다.
   - 서브넷을 사용하여 IP 주소와 네트워크 마스크를 제공하면, 서브넷에 정의된 서브넷이 해당 서브넷을 사용하여 LIF를 생성할 때 해당 게이트웨이에 대한 기본 경로가 SVM에 자동으로 추가됩니다.
   - 서브넷을 사용하지 않고 수동으로 IP 주소를 할당하는 경우 다른 IP 서브넷에 클라이언트 또는 도메인 컨트롤러가 있는 경우 게이트웨이에 대한 기본 라우트를 구성해야 할 수 있습니다. 에 대한 자세한 내용은

network route create "ONTAP 명령 참조입니다"을 참조하십시오.

- '-자동 되돌리기'를 사용하면 시작, 관리 데이터베이스의 상태 변경 또는 네트워크 연결이 이루어지는 시기에 데이터 LIF가 홈 노드로 자동 복구되는지 여부를 지정할 수 있습니다. 기본 설정은 false로 설정되어 있지만 사용자 환경의 네트워크 관리 정책에 따라 true로 설정할 수 있습니다.
- '-service-policy' ONTAP 9.5부터 '-service-policy' 옵션을 통해 LIF에 대한 서비스 정책을 할당할 수 있습니다. LIF에 서비스 정책을 지정한 경우, 이 정책을 사용하여 LIF에 대한 기본 역할, 페일오버 정책 및 데이터 프로토콜 목록을 구성합니다. ONTAP 9.5에서는 서비스 정책이 인터클러스터 및 BGP 피어 서비스에 대해서만 지원됩니다. ONTAP 9.6에서는 여러 데이터 및 관리 서비스에 대한 서비스 정책을 작성할 수 있습니다.
- '-data-protocol'을 사용하면 FCP 또는 NVMe/FC 프로토콜을 지원하는 LIF를 생성할 수 있습니다. IP LIF를 생성할 때는 이 옵션이 필요하지 않습니다.

4. * 선택 사항 *: -address 옵션에서 IPv6 주소 할당:

   a. network NDP prefix show 명령을 사용하여 다양한 인터페이스에서 습득한 RA prefix 목록을 볼 수 있다.

      고급 권한 수준에서 network NDP prefix show 명령을 사용할 수 있다.

      에 대한 자세한 내용은 network ndp prefix show "ONTAP 명령 참조입니다"을 참조하십시오.

   b. IPv6 주소를 수동으로 구성하려면 접두사::id 형식을 사용합니다.

      접두사는 다양한 인터페이스에서 습득한 접두사입니다.

   ID를 도출하려면 임의의 64비트 16진수 숫자를 선택합니다.

5. LIF 인터페이스 구성이 올바른지 확인합니다.

   네트워크 인터페이스 show-vserver vs1

```
          Logical    Status     Network          Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask     Node      Port
Home
--------- ---------- ---------- ---------------- --------- -------
----
vs1
           lif1        up/up      10.0.0.128/24   node1      e0d
true
```

   에 대한 자세한 내용은 network interface show "ONTAP 명령 참조입니다"을 참조하십시오.

6. 페일오버 그룹 구성이 원하는 대로 되어 있는지 확인합니다.

   'network interface show-failover-vserver_vs1_'

```
         Logical    Home       Failover        Failover
Vserver  interface  Node:Port  Policy          Group
-------- ---------- ---------  ---------       --------
vs1
         lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

다음을 확인하려면…	사용…
IPv4 주소입니다	네트워크 Ping
IPv6 주소입니다	네트워크 ping6

예

다음 명령을 실행하면 LIF가 생성되고 '-address' 및 '-netmask' 매개 변수를 사용하여 IP 주소와 네트워크 마스크 값이 지정됩니다.

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

다음 명령을 실행하면 LIF가 생성되고 지정된 서브넷(client1_sub 이름)의 IP 주소와 네트워크 마스크 값이 할당됩니다.

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

다음 명령은 NVMe/FC LIF를 생성하고 'NVMe-FC' 데이터 프로토콜을 지정합니다.

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

ONTAP LIF 수정

홈 노드 또는 현재 노드, 관리 상태, IP 주소, 넷마스크, 페일오버 정책 등의 특성을 변경하여 LIF를 수정할 수 있습니다. 방화벽 정책 및 서비스 정책을 참조하십시오. LIF의 주소 제품군을 IPv4에서 IPv6로 변경할 수도 있습니다.

이 작업에 대해

- LIF의 관리 상태를 중지 상태로 수정할 때 LIF의 관리 상태가 위로 돌아갈 때까지 진행 중인 모든 NFSv4 잠금이 유지됩니다.

  다른 LIF가 잠긴 파일에 액세스하려고 할 때 발생할 수 있는 잠금 충돌을 방지하려면 관리 상태를 낮춤 으로 설정하기 전에 NFSv4 클라이언트를 다른 LIF로 이동해야 합니다.

- FC LIF에서 사용되는 데이터 프로토콜은 수정할 수 없습니다. 하지만 서비스 정책에 할당된 서비스를 수정하거나 IP LIF에 할당된 서비스 정책을 변경할 수 있습니다.

  FC LIF에서 사용되는 데이터 프로토콜을 수정하려면 LIF를 삭제하고 다시 생성해야 합니다. IP LIF에서 서비스 정책을 변경하기 위해 업데이트를 수행하는 동안 잠시 중단이 발생합니다.

- 노드 범위 관리 LIF의 홈 노드 또는 현재 노드를 수정할 수 없습니다.
- 서브넷을 사용하여 LIF의 IP 주소 및 네트워크 마스크 값을 변경할 경우, IP 주소는 지정된 서브넷에서 할당됩니다. LIF의 이전 IP 주소가 다른 서브넷에 있는 경우 IP 주소는 해당 서브넷으로 반환됩니다.
- LIF의 주소 제품군을 IPv4에서 IPv6로 수정하려면 IPv6 주소에 대한 콜론 표기법을 사용하고 '-netmask-length' 매개 변수에 새 값을 추가해야 합니다.
- 자동 구성된 링크 로컬 IPv6 주소는 수정할 수 없습니다.
- LIF가 수정되어 LIF에 유효한 페일오버 타겟이 없게 되면 경고 메시지가 표시됩니다.

  유효한 페일오버 목표가 없는 LIF가 페일오버를 시도하면 운영 중단이 발생할 수 있습니다.

- ONTAP 9.5부터 LIF와 연결된 서비스 정책을 수정할 수 있습니다.

  ONTAP 9.5에서는 서비스 정책이 인터클러스터 및 BGP 피어 서비스에 대해서만 지원됩니다. ONTAP 9.6에서는 여러 데이터 및 관리 서비스에 대한 서비스 정책을 작성할 수 있습니다.

- ONTAP 9.11.1부터 ASA(All-Flash SAN 어레이) 플랫폼에서 자동 iSCSI LIF 페일오버를 사용할 수 있습니다.

  기존 iSCSI LIF의 경우, 9.11.1 이상으로 업그레이드하기 전에 생성된 LIF를 의미하며 페일오버 정책을 로 수정할 수 있습니다 "자동 iSCSI LIF 페일오버를 사용합니다".

- ONTAP NTP(네트워크 시간 프로토콜)를 활용하여 클러스터 전체에서 시간을 동기화합니다. LIF IP 주소를 변경한 후에는 동기화 실패를 방지하기 위해 NTP 구성을 업데이트해야 할 수도 있습니다. 자세한 내용은 다음을 참조하세요."NetApp 지식 기반: LIF IP 변경 후 NTP 동기화가 실패함" .

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- ONTAP 9.12.0부터는 시스템 관리자를 사용하여 네트워크 인터페이스를 편집할 수 있습니다 *

단계

1. Network > Overview > Network Interfaces * 를 선택합니다.
2. 변경할 네트워크 인터페이스 옆의 * > 편집 * 을 선택합니다 ⋮ .
3. 하나 이상의 네트워크 인터페이스 설정을 변경합니다. 자세한 내용은 을 참조하십시오 "LIF를 생성합니다".
4. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 LIF를 수정합니다 *

단계

1. 'network interface modify' 명령을 사용하여 LIF의 특성을 수정합니다.

   다음 예에서는 서브넷 client1_sub의 IP 주소와 네트워크 마스크 값을 사용하여 LIF datalif2의 IP 주소와 네트워크 마스크를 수정하는 방법을 보여 줍니다.

   ```
   network interface modify -vserver vs1 -lif datalif2 -subnet-name
   client1_sub
   ```

   다음 예에서는 LIF의 서비스 정책을 수정하는 방법을 보여 줍니다.

   ```
   network interface modify -vserver siteA -lif node1_inter1 -service
   -policy example
   ```

   에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. IP 주소에 연결할 수 있는지 확인합니다.

사용 중인 경우…	그 다음에…
IPv4 주소	네트워크 핑
IPv6 주소	네트워크 핑6

   에 대한 자세한 내용은 `network ping` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP LIF 마이그레이션

포트에 장애가 발생하거나 유지 관리가 필요한 경우 LIF를 동일한 노드의 다른 포트 또는 클러스터 내의 다른 노드로 마이그레이션해야 할 수 있습니다. LIF 마이그레이션은 LIF

페일오버와 비슷하지만, LIF 마이그레이션은 수동 작업이며, LIF 페일오버는 LIF의 현재 네트워크 포트에서 링크 장애가 발생할 경우 LIF의 자동 마이그레이션입니다.

시작하기 전에

- LIF에 대해 페일오버 그룹을 구성해야 합니다.
- 대상 노드와 포트가 작동 중이고 소스 포트와 동일한 네트워크에 액세스할 수 있어야 합니다.

이 작업에 대해

- BGP LIF는 홈 포트에 상주하며 다른 노드 또는 포트로 마이그레이션할 수 없습니다.
- 노드에서 NIC를 제거하기 전에 NIC에 속한 포트에서 호스팅되는 LIF를 클러스터의 다른 포트로 마이그레이션해야 합니다.
- 클러스터 LIF가 호스팅된 노드에서 클러스터 LIF를 마이그레이션하기 위한 명령을 실행해야 합니다.
- 노드 범위의 관리 LIF, 클러스터 LIF, LIF와 같은 노드 범위의 LIF는 원격 인터클러스터 노드로 마이그레이션할 수 없습니다.
- NFSv4 LIF를 노드 간에 마이그레이션할 경우 LIF가 새 포트에서 사용 가능해지기 전에 최대 45초가 지연됩니다.

  이 문제를 해결하려면 지연이 발생하지 않는 NFSv4.1을 사용하십시오.

- ONTAP 9.11.1 이상을 실행하는 ASA(All-Flash SAN 어레이) 플랫폼에서 iSCSI LIF를 마이그레이션할 수 있습니다.

  iSCSI LIF 마이그레이션은 홈 노드 또는 HA 파트너의 포트로 제한됩니다.

- 사용 중인 플랫폼이 ONTAP 버전 9.11.1 이상을 실행하는 ASA(All-Flash SAN 어레이) 플랫폼이 아닌 경우 한 노드에서 다른 노드로 iSCSI LIF를 마이그레이션할 수 없습니다.

  이 제한을 해결하려면 대상 노드에 iSCSI LIF를 생성해야 합니다. 에 대해 자세히 "iSCSI LIF를 생성하는 중입니다 "알아보십시오.

- RDMA를 통해 NFS용 LIF(네트워크 인터페이스)를 마이그레이션하려면 대상 포트가 RoCE를 지원하는지 확인해야 합니다. CLI에서 LIF를 마이그레이션하려면 ONTAP 9.10.1 이상을 실행해야 하며, System Manager를 사용하여 마이그레이션하려면 ONTAP 9.12.1을 실행해야 합니다. System Manager에서 RoCE 가능 대상 포트를 선택한 후에는 * RoCE 포트 사용 * 옆의 확인란을 선택하여 마이그레이션을 성공적으로 완료해야 합니다. 에 대해 자세히 알아보십시오 "RDMA를 통해 NFS용 LIF 구성".
- 소스 또는 대상 LIF를 마이그레이션할 때 VMware VAAI 복사본 오프로드 작업이 실패합니다. Copy Off-load에 대한 자세한 내용:
  - "알아보십시오"
  - "알아보십시오"

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 네트워크 인터페이스를 마이그레이션합니다 *

단계

1. Network > Overview > Network Interfaces * 를 선택합니다.
2. 변경할 네트워크 인터페이스 옆에 있는 *>Migrate * 를 선택합니다 ⋮ .

   iSCSI LIF의 경우 * Migrate Interface * 대화 상자에서 HA 파트너의 대상 노드 및 포트를 선택합니다.

   iSCSI LIF를 영구적으로 마이그레이션하려면 확인란을 선택합니다. iSCSI LIF는 영구적으로 마이그레이션되기 전에 오프라인 상태여야 합니다. 또한 iSCSI LIF를 영구적으로 마이그레이션한 후에는 취소할 수 없습니다. 되돌리기 옵션은 없습니다.

3. 마이그레이션 * 을 클릭합니다.
4. 변경 사항을 저장합니다.

CLI를 참조하십시오

- CLI를 사용하여 LIF를 마이그레이션합니다 *

단계

특정 LIF를 마이그레이션할지 또는 모든 LIF를 마이그레이션할지 여부에 따라 적절한 작업을 수행합니다.

마이그레이션하려면…	다음 명령을 입력합니다…
특정 LIF	네트워크 인터페이스 마이그레이션
노드의 모든 데이터 및 클러스터 관리 LIF	네트워크 인터페이스 마이그레이션 모두
모든 LIF가 포트에서 해제됩니다	'network interface migrate-all-node <node> - port <port>'

다음 예제에서는 이라는 LIF를 마이그레이션하는 방법을 보여 줍니다 `datalif1` SVM에서 `vs0` 포트에 연결합니다 `e0d` 켜짐 `node0b`:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

다음 예에서는 현재(로컬) 노드에서 모든 데이터 및 클러스터 관리 LIF를 마이그레이션하는 방법을 보여 줍니다.

```
network interface migrate-all -node local
```

관련 정보

- "네트워크 인터페이스 마이그레이션"

ONTAP 노드 페일오버 또는 포트 마이그레이션 후에 **LIF**를 홈 포트로 되돌립니다

LIF가 페일오버된 후 홈 포트로 되돌아가거나 수동으로 또는 자동으로 다른 포트로 마이그레이션될 수 있습니다. 특정 LIF의 홈 포트를 사용할 수 없는 경우 LIF는 현재 포트에 남아 있으며 되돌릴 수 없습니다.

이 작업에 대해

- 관리상 자동 되돌리기 옵션을 설정하기 전에 LIF의 홈 포트를 설정 상태로 전환할 경우 LIF는 홈 포트로 돌아가지 않습니다.
- "자동 되돌리기" 옵션의 값이 true로 설정되어 있지 않으면 LIF가 자동으로 복구되지 않습니다.
- LIF가 홈 포트로 되돌아가려면 "자동 되돌리기" 옵션이 설정되어 있는지 확인해야 합니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 네트워크 인터페이스를 홈 포트로 되돌립니다 *

단계

1. Network > Overview > Network Interfaces * 를 선택합니다.
2. 변경할 네트워크 인터페이스 옆의 *>되돌리기 * 를 선택합니다 ⋮ .
3. 네트워크 인터페이스를 홈 포트로 되돌리려면 * Revert * 를 선택합니다.

CLI를 참조하십시오

- CLI를 사용하여 LIF를 홈 포트로 되돌릴 수 있습니다 *

단계

LIF를 홈 포트로 수동 또는 자동으로 되돌리기:

LIF를 홈 포트로 되돌리려면…	그런 다음 다음 다음 명령을 입력합니다.
수동	'network interface revert-vserver vserver_name-lif lif_name'
자동으로	'network interface modify -vserver vserver_name -lif lif_name -auto -revert true'

에 대한 자세한 내용은 `network interface` "ONTAP 명령 참조입니다"을 참조하십시오.

잘못 구성된 **ONTAP LIF**를 복구합니다

클러스터 네트워크가 스위치에 케이블로 연결되어 있지만 클러스터 IPspace에 구성된 모든 포트가 클러스터 IPspace에 구성된 다른 포트에 연결할 수 있는 것은 아닙니다.

이 작업에 대해

전환된 클러스터에서 클러스터 네트워크 인터페이스(LIF)가 잘못된 포트에 구성되어 있거나 클러스터 포트가 잘못된

네트워크에 연결되어 있는 경우 "cluster create" 명령이 실패하고 다음 오류가 표시될 수 있습니다.

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

에 대한 자세한 내용은 `cluster create` "ONTAP 명령 참조입니다"을 참조하십시오.

이 `network port show` 명령의 결과는 여러 포트가 클러스터 LIF로 구성된 포트에 연결되기 때문에 클러스터 IPspace에 추가된 것을 보여 줄 수 있습니다. 그러나 결과는 `network port reachability show -detail` 명령어는 어떤 포트가 서로 연결되지 않았는지 보여줍니다.

에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

클러스터 LIF로 구성된 다른 포트에 연결할 수 없는 포트에 구성된 클러스터 LIF에서 복구하려면 다음 단계를 수행하십시오.

단계

1. 클러스터 LIF의 홈 포트를 올바른 포트로 재설정합니다.

   ```
   network port modify -home-port
   ```

   에 대한 자세한 내용은 `network port modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 클러스터 LIF가 구성되어 있지 않은 포트를 클러스터 브로드캐스트 도메인에서 제거합니다.

   ```
   network port broadcast-domain remove-ports
   ```

   에 대한 자세한 내용은 `network port broadcast-domain remove-ports` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 클러스터를 생성합니다.

   ```
   cluster create
   ```

결과

클러스터 생성을 완료하면 시스템이 올바른 구성을 감지하고 포트를 올바른 브로드캐스트 도메인에 배치합니다.

관련 정보

- "네트워크 포트 도달 가능성 표시"

ONTAP LIF를 삭제합니다

더 이상 필요하지 않은 네트워크 인터페이스(LIF)를 삭제할 수 있습니다.

시작하기 전에

삭제할 LIF는 사용 중이 아니어야 합니다.

단계

1. 다음 명령을 사용하여 삭제할 LIF를 관리 목적으로 사용 중지하도록 표시합니다.

```
network interface modify -vserver vserver_name -lif lif_name -status
-admin down
```

2. "network interface delete" 명령을 사용하여 하나 또는 모든 LIF를 삭제합니다.

삭제하려면…	명령 입력…
특정 LIF	'network interface delete -vserver vserver_name -lif lif_name'
모든 LIF	'network interface delete-vserver vserver_name-lif *'

에 대한 자세한 내용은 `network interface delete` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 LIF mgmtd LIF가 삭제됩니다. 2:

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. LIF가 삭제되었는지 확인하려면 'network interface show' 명령을 사용하십시오.

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 가상 IP(VIP) LIF를 구성합니다

일부 차세대 데이터 센터에서는 여러 서브넷에서 LIF를 페일오버해야 하는 계층 3(IP) 네트워크 메커니즘을 사용합니다. ONTAP는 이러한 차세대 네트워크의 페일오버 요구사항을 충족하기 위해 VIP(가상 IP) 데이터 LIF와 관련 라우팅 프로토콜, BGP(Border Gateway Protocol)를 지원합니다.

이 작업에 대해

VIP 데이터 LIF는 서브넷의 일부가 아닌 LIF로, 동일한 IPspace에서 BGP LIF를 호스팅하는 모든 포트에서 연결할 수 있습니다. VIP 데이터 LIF는 개별 네트워크 인터페이스에 대한 호스트의 종속성을 제거합니다. 여러 개의 물리적 어댑터가 데이터 트래픽을 전달하므로 전체 로드가 단일 어댑터와 관련 서브넷에 집중되지 않습니다. VIP 데이터 LIF는 라우팅 프로토콜인 BGP(Border Gateway Protocol)를 통해 피어 라우터에 보급됩니다.

VIP 데이터 LIF는 다음과 같은 이점을 제공합니다.

- 브로드캐스트 도메인 또는 서브넷 이상의 LIF 이동성: VIP 데이터 LIF는 BGP를 통해 각 VIP 데이터 LIF의 현재 위치를 공유함으로써 네트워크의 모든 서브넷에 페일오버할 수 있습니다.
- 총 처리량: VIP 데이터 LIF는 여러 서브넷 또는 포트에서 데이터를 동시에 송수신할 수 있으므로 개별 포트의

대역폭을 초과하는 총 처리량을 지원할 수 있습니다.

BGP(Border Gateway Protocol) 설정

VIP LIF를 생성하기 전에 피어 라우터에 대한 VIP LIF의 존재를 알리는 데 사용되는 라우팅 프로토콜인 BGP를 설정해야 합니다.

ONTAP 9.9.1부터 VIP는 BGP 피어 그룹을 사용하여 기본 경로 자동화를 옵션으로 제공하여 구성을 간소화합니다.

ONTAP는 BGP 피어가 동일한 서브넷에 있을 때 BGP 피어를 다음 홉 라우터로 사용하여 기본 라우트를 학습할 수 있는 간단한 방법을 제공합니다. 이 기능을 사용하려면 '-use-peer-as-next-hop' 속성을 true로 설정합니다. 기본적으로 이 속성은 false 입니다.

정적 라우트가 구성된 경우 이러한 자동 기본 라우트보다 더 선호됩니다.

시작하기 전에

ASN(Autonomous System Number)이 구성된 BGP LIF에서 BGP 연결을 허용하도록 피어 라우터를 구성해야 합니다.

> ONTAP는 라우터에서 수신되는 라우트 알림을 처리하지 않으므로, 피어 라우터가 클러스터에 대한 라우트 업데이트를 보내지 않도록 구성해야 합니다. 이렇게 하면 피어와 통신하는 데 걸리는 시간이 단축되고 ONTAP 내의 내부 메모리 사용량이 줄어듭니다.

이 작업에 대해

BGP를 설정하려면 선택적으로 BGP 구성을 생성하고, BGP LIF를 생성하고, BGP 피어 그룹을 생성해야 합니다. ONTAP는 특정 노드에서 첫 번째 BGP 피어 그룹이 생성될 때 기본값으로 기본 BGP 구성을 자동으로 생성합니다.

BGP LIF는 피어 라우터를 사용하여 BGP TCP 세션을 설정하는 데 사용됩니다. 피어 라우터의 경우 BGP LIF는 VIP LIF에 도달하기 위한 다음 홉입니다. BGP LIF에서 페일오버가 비활성화되었습니다. BGP 피어 그룹은 피어 그룹이 사용하는 IPspace의 모든 SVM에 대한 VIP 경로를 알립니다. 피어 그룹에서 사용하는 IPspace는 BGP LIF에서 상속됩니다.

ONTAP 9.16.1부터는 BGP 피어 그룹에서 MD5 인증이 지원되어 BGP 세션을 보호합니다. MD5가 활성화되면 승인된 피어 사이에서만 BGP 세션을 설정 및 처리할 수 있으므로 권한이 없는 행위자에 의한 세션 중단을 방지할 수 있습니다.

및 `network bgp peer-group modify` 명령에 다음 필드가 `network bgp peer-group create` 추가되었습니다.

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

이러한 매개 변수를 사용하면 보안을 강화하기 위해 MD5 서명을 사용하여 BGP 피어 그룹을 구성할 수 있습니다. MD5 인증 사용에 적용되는 요구 사항은 다음과 같습니다.

- 매개 변수가 (으)로 설정된 `true` 경우에만 매개 변수를 `-md5-enabled` 지정할 수 `-md5-secret` 있습니다.
- MD5 BGP 인증을 활성화하려면 IPsec을 전역적으로 활성화해야 합니다. BGP LIF는 활성 IPsec 구성을 가질 필요가 없습니다. 을 "유선 암호화를 통해 IP 보안(IPsec)을 구성합니다"참조하십시오.
- NetApp는 ONTAP 컨트롤러에서 MD5를 구성하기 전에 라우터에 MD5를 구성하는 것이 좋습니다.

ONTAP 9.9.1부터 다음 필드가 추가되었습니다.

- `-asn` 또는 `-peer-asn` (4바이트 값) 특성 자체는 새로운 것이 아니지만 4바이트 정수를 사용합니다.
- `-med`
- `-use-peer-as-next-hop`

경로 우선 순위 지정을 위해 MED(Multi-Exit Discriminator) 지원을 통해 고급 경로 선택을 수행할 수 있습니다. Med는 라우터에 트래픽에 가장 적합한 경로를 선택하도록 지시하는 BGP 업데이트 메시지의 선택적 속성입니다. MED는 부호 없는 32비트 정수(0-4294967295)이며 더 낮은 값을 사용하는 것이 좋습니다.

ONTAP 9.8부터 이러한 필드는 'network BGP peer-group' 명령에 추가되었습니다.

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

이러한 BGP 특성을 사용하면 를 BGP 피어 그룹에 대한 경로 및 커뮤니티 속성으로 구성할 수 있습니다.

ONTAP는 위의 BGP 속성을 지원하지만 라우터는 이를 인정할 필요가 없습니다. NetApp은 라우터에서 지원하는 속성을 확인하고 그에 따라 BGP 피어 그룹을 구성할 것을 적극 권장합니다. 자세한 내용은 라우터에서 제공한 BGP 설명서를 참조하십시오.

단계

1. 고급 권한 레벨에 로그인합니다.

   세트 프리빌리지 고급

2. 선택 사항: 다음 작업 중 하나를 수행하여 BGP 구성을 생성하거나 클러스터의 기본 BGP 구성을 수정합니다.

   a. BGP 구성 생성:

```
network bgp config create -node {node_name | local} -asn <asn_number>
-holdtime
<hold_time> -routerid <router_id>
```

- 이 `-routerid` 매개 변수는 AS 도메인 내에서만 고유해야 하는 점분리 십진수 32비트 값을 허용합니다. NetApp은 고유성을 보장하는 노드 관리 IP(v4) 주소를 사용할 것을 `<router_id>` 권장합니다.
- ONTAP BGP는 32비트 ASN 숫자를 지원하지만 표준 10진수 표기법만 지원됩니다. 사설 ASN에 대해 4259840001 대신 65000.1과 같은 점선 ASN 표기법은 지원되지 않습니다.

   2바이트 ASN이 포함된 샘플:

```
network bgp config create -node node1 -asn 65502 -holdtime 180
-routerid 1.1.1.1
```

   4바이트 ASN이 포함된 샘플:

```
network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid
1.1.1.1
```

a. 기본 BGP 구성을 수정합니다.

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

- `<asn_number>` ASN 번호를 지정합니다. ONTAP 9.8부터 BGP의 ASN은 2바이트 비음수를 지원합니다. 16비트 숫자입니다(1 - 65534 사용 가능한 값). ONTAP 9.9.1부터 BGP용 ASN은 4바이트 비음의 정수(1 ~ 4294967295)를 지원합니다. 기본 ASN은 65501입니다. ASN 23456은 4바이트 ASN 기능을 발표하지 않는 피어와의 ONTAP 세션 설정을 위해 예약되어 있습니다.
- `<hold_time>` 보류 시간을 초 단위로 지정합니다. 기본값은 180입니다.

ONTAP는 여러 IPspaces에 대해 BGP를 구성한 경우에도 하나의 글로벌, `<hold_time>` 및 `<router_id>` 만 `<asn_number>` 지원합니다. BGP와 모든 IP 라우팅 정보는 하나의 IPspace 내에서 완전히 격리된다. IPspace는 가상 라우팅 및 전달(VRF) 인스턴스와 같습니다.

3. 시스템 SVM을 위한 BGP LIF 생성:

기본 IPspace의 경우 SVM 이름은 클러스터 이름입니다. 추가 IPspace의 경우 SVM 이름은 IPspace 이름과 동일합니다.

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-route-announce -home-node <home_node> -home-port
<home_port> -address <ip_address> -netmask <netmask>
```

BGP LIF에 대한 'default-route-공지' 서비스 정책 또는 "management-BGP" 서비스가 포함된 사용자 지정 서비스 정책을 사용할 수 있습니다.

```
network interface create -vserver cluster1 -lif bgp1 -service-policy
default-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

4. 원격 피어 라우터로 BGP 세션을 설정하고 피어 라우터에 보급된 VIP 라우트 정보를 구성하는 데 사용되는 BGP 피어 그룹을 생성합니다.

샘플 1: 자동 기본 경로 없이 피어 그룹을 생성합니다

이 경우 관리자는 BGP 피어에 대한 정적 경로를 생성해야 합니다.

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
{-community BGP community list <0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
-asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
9000:900,8000:800
```

샘플 2: 자동 기본 라우트가 있는 피어 그룹을 생성합니다

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
prepend-count <integer>} {-med <integer>} {-community BGP community list
<0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

샘플 3: MD5가 활성화된 피어 그룹을 만듭니다

a. IPsec 활성화:

   보안 IPsec config modify -is -enabled true

b. MD5가 활성화된 BGP 피어 그룹을 생성합니다.

   ```
   network bgp peer-group create -ipspace Default -peer-group
   <group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
   {-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
   ```

   16진수 키 사용 예:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
0x7465737420736563726574
```

문자열 사용 예:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

BGP 피어 그룹을 생성한 후 명령을 실행하면 가상 이더넷 포트(v0a..v0z, v1a… 로 시작)가 `network port show` 나열됩니다. 이 인터페이스의 MTU는 항상 1500으로 보고됩니다. 트래픽에 사용되는 실제 MTU는 트래픽을 전송할 때 결정되는 물리적 포트(BGP LIF)에서 파생됩니다. 에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

가상 IP(VIP) 데이터 LIF를 생성합니다

VIP 데이터 LIF는 라우팅 프로토콜인 BGP(Border Gateway Protocol)를 통해 피어 라우터에 보급됩니다.

시작하기 전에

- BGP 피어 그룹을 설정하고 LIF를 생성할 SVM을 위한 BGP 세션을 활성화해야 합니다.
- SVM의 나가는 VIP 트래픽에 대해 BGP 라우터 또는 BGP LIF 서브넷의 다른 라우터에 대한 정적 경로를 생성해야 합니다.
- 나가는 VIP 트래픽이 사용 가능한 모든 경로를 사용할 수 있도록 다중 경로 라우팅을 켜야 합니다.

  다중 경로 라우팅이 활성화되지 않은 경우 나가는 모든 VIP 트래픽은 단일 인터페이스에서 이동합니다.

단계

1. VIP 데이터 LIF 생성:

```
network interface create -vserver <svm_name> -lif <lif_name> -role data
-data-protocol
{nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
<ip_address> -is-vip true -failover-policy broadcast-domain-wide
```

네트워크 인터페이스 생성 명령으로 홈 포트를 지정하지 않으면 VIP 포트가 자동으로 선택됩니다.

기본적으로 VIP 데이터 LIF는 각 IPspace에 대해 'VIP'라는 시스템 생성 브로드캐스트 도메인에 속해 있습니다. VIP 브로드캐스트 도메인은 수정할 수 없습니다.

VIP 데이터 LIF는 IPspace의 BGP LIF를 호스팅하는 모든 포트에서 동시에 연결할 수 있습니다. 로컬 노드에서 VIP의 SVM을 위한 활성 BGP 세션이 없는 경우, VIP 데이터 LIF는 해당 SVM을 위해 BGP 세션이 설정된 노드에서 다음 VIP 포트로 페일오버됩니다.

2. BGP 세션이 VIP 데이터 LIF의 SVM에 대한 UP 상태인지 확인합니다.

```
network bgp vserver-status show

Node        Vserver  bgp status
          ----------  -------- ---------
          node1       vs1      up
```

노드의 SVM에 대해 BGP 상태가 'down'이면 VIP 데이터 LIF가 SVM에 대해 BGP 상태가 가동 중인 다른 노드로 페일오버됩니다. 모든 노드에서 BGP 상태가 '소유'인 경우 VIP 데이터 LIF는 어느 곳에서나 호스팅할 수 없으며 LIF 상태가 '다운'입니다.

BGP 관리를 위한 명령입니다

ONTAP 9.5부터 ONTAP에서 BGP 세션을 관리하기 위해 'network BGP' 명령어를 사용한다.

BGP 구성 관리

원하는 작업	이 명령 사용…
BGP 구성을 생성합니다	`network bgp config create`
BGP 구성을 수정합니다	`network bgp config modify`
BGP 구성을 삭제합니다	`network bgp config delete`
BGP 구성을 표시합니다	`network bgp config show`
VIP LIF의 SVM에 대한 BGP 상태를 표시합니다	`network bgp vserver-status show`

BGP 기본값을 관리합니다

원하는 작업	이 명령 사용…
BGP 기본값을 수정합니다	`network bgp defaults modify`
BGP 기본값을 표시합니다	`network bgp defaults show`

BGP 피어 그룹을 관리합니다

원하는 작업	이 명령 사용…
BGP 피어 그룹을 생성합니다	`network bgp peer-group create`
BGP 피어 그룹을 수정합니다	`network bgp peer-group modify`
BGP 피어 그룹을 삭제합니다	`network bgp peer-group delete`
BGP 피어 그룹 정보를 표시합니다	`network bgp peer-group show`
BGP 피어 그룹의 이름을 바꿉니다	`network bgp peer-group rename`

MD5를 사용하여 BGP 피어 그룹을 관리합니다

ONTAP 9.16.1부터 기존 BGP 피어 그룹에서 MD5 인증을 사용하거나 사용하지 않도록 설정할 수 있습니다.

> 기존 BGP 피어 그룹에서 MD5를 활성화 또는 비활성화하면 BGP 연결이 종료되고 MD5 구성 변경 사항을 적용하기 위해 다시 생성됩니다.

원하는 작업	이 명령 사용…
기존 BGP 피어 그룹에서 MD5를 활성화합니다	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
기존 BGP 피어 그룹에서 MD5를 비활성화합니다	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

관련 정보

- "ONTAP 명령 참조입니다"
- "네트워크 BGP"
- "네트워크 인터페이스"
- "보안 IPsec 구성 수정"

네트워크 로드 밸런싱

DNS 로드 밸런싱을 사용하여 ONTAP 네트워크 트래픽을 최적화합니다

적절하게 로드된 LIF의 클라이언트 요청을 처리하도록 클러스터를 구성할 수 있습니다. 그 결과, LIF 및 포트의 활용률이 더욱 높아질수록 클러스터의 성능이 향상됩니다.

DNS 로드 밸런싱은 적절하게 로드된 데이터 LIF를 선택하고 사용 가능한 모든 포트(물리적, 인터페이스 그룹 및 VLAN)에서 사용자 네트워크 트래픽의 균형을 조정하는 데 도움이 됩니다.

DNS 로드 밸런싱을 통해 LIF는 SVM의 로드 밸런싱 영역과 연결됩니다. 사이트 전체의 DNS 서버는 모든 DNS 요청을 전달하고 네트워크 트래픽과 포트 리소스의 가용성(CPU 사용량, 처리량, 개방형 연결 등)을 기준으로 가장 적게 로드된 LIF를 반환하도록 구성됩니다. DNS 로드 밸런싱은 다음과 같은 이점을 제공합니다.

- 사용 가능한 리소스 간에 새 클라이언트 연결이 균형 있게 조정됩니다.
- 특정 SVM을 마운트할 때 사용할 LIF를 결정하기 위해 수작업이 필요하지 않습니다.
- DNS 로드 밸런싱이 NFSv3, NFSv4, NFSv4.1, SMB 2.0, SMB 2.1, SMB 3.0 및 S3.

ONTAP 네트워크의 DNS 로드 밸런싱에 대해 알아봅니다

클라이언트는 IP 주소(LIF와 연결) 또는 호스트 이름(여러 IP 주소와 연결)을 지정하여 SVM을

마운트합니다. 기본적으로 LIF는 라운드 로빈 방식으로 사이트 전체 DNS 서버에서 선택되어 있으며, 이 방식을 통해 모든 LIF에서 워크로드의 균형을 조정할 수 있습니다.

라운드 로빈 로드 밸런싱으로 인해 일부 LIF가 오버로드될 수 있으므로 SVM에서 호스트 이름 확인을 처리하는 DNS 로드 밸런싱 존을 사용할 수 있습니다. DNS 로드 밸런싱 존을 사용하면 사용 가능한 리소스 전체에서 새 클라이언트 연결의 균형을 보다 효율적으로 유지할 수 있어 클러스터의 성능이 향상됩니다.

DNS 로드 밸런싱 존은 클러스터 내의 DNS 서버로서 모든 LIF의 로드를 동적으로 평가하고 적절하게 로드된 LIF를 반환합니다. 로드 밸런싱 영역에서 DNS는 각 LIF에 로드(메트릭)를 기준으로 가중치를 할당합니다.

모든 LIF에는 홈 노드의 포트 로드 및 CPU 활용률을 기준으로 가중치가 할당됩니다. 로드가 적은 포트에 있는 LIF는 DNS 쿼리에서 반환될 가능성이 높습니다. 가중치는 수동으로 지정할 수도 있습니다.

ONTAP 네트워크에 대한 DNS 로드 밸런싱 존을 생성합니다

DNS 로드 밸런싱 영역을 생성하여 LIF에 마운트된 클라이언트 수, 즉 로드를 기반으로 LIF를 동적으로 선택할 수 있습니다. 데이터 LIF를 생성하는 동안 로드 밸런싱 존을 생성할 수 있습니다.

시작하기 전에

로드 밸런싱 존에 대한 모든 요청을 구성된 LIF로 전달하도록 사이트 전체 DNS 서버의 DNS 전달자를 구성해야 합니다.

그만큼"NetApp 지식 기반: 클러스터 모드에서 DNS 부하 분산을 설정하는 방법" 조건부 전달을 사용하여 DNS 부하 분산을 구성하는 방법에 대한 자세한 정보가 포함되어 있습니다.

이 작업에 대해

- 모든 데이터 LIF는 DNS 로드 밸런싱 존 이름에 대한 DNS 쿼리에 응답할 수 있습니다.
- DNS 로드 밸런싱 존은 클러스터에서 고유한 이름을 가져야 하며 영역 이름은 다음 요구 사항을 충족해야 합니다.
  - 256자를 초과하면 안 됩니다.
  - 최소 하나의 기간을 포함해야 합니다.
  - 첫 번째 문자와 마지막 문자는 마침표 또는 기타 특수 문자여야 합니다.
  - 문자 사이에 공백을 포함할 수 없습니다.
  - DNS 이름의 각 레이블은 63자를 초과할 수 없습니다.

    레이블은 기간 전후에 나타나는 텍스트입니다. 예를 들어 storage.company.com 이라는 DNS 영역에는 세 개의 레이블이 있습니다.

단계

명령을 옵션과 함께 `dns-zone` 사용하여 `network interface create` DNS 로드 밸런싱 존을 생성합니다. 에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

로드 밸런싱 영역이 이미 존재하는 경우 LIF가 이 영역에 추가됩니다.

다음 예제에서는 LIF 'lif1'을 생성하는 동안 storage.company.com 이라는 DNS 로드 밸런싱 존을 생성하는 방법을 보여 줍니다.

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

로드 밸런싱 존에서 **ONTAP LIF**를 추가 또는 제거합니다

SVM(가상 머신)의 DNS 로드 밸런싱 영역에서 LIF를 추가하거나 제거할 수 있습니다. 로드 밸런싱 영역에서 모든 LIF를 동시에 제거할 수도 있습니다.

시작하기 전에

- 로드 밸런싱 존의 모든 LIF는 동일한 SVM에 속해야 합니다.
- LIF는 하나의 DNS 로드 밸런싱 존에 포함될 수 있습니다.
- LIF가 다른 서브넷에 속한 경우 각 서브넷에 대한 페일오버 그룹을 설정해야 합니다.

이 작업에 대해

관리 다운 상태인 LIF는 DNS 로드 밸런싱 영역에서 일시적으로 제거됩니다. LIF가 관리 설정 상태로 돌아가면 LIF가 DNS 로드 밸런싱 존에 자동으로 추가됩니다.

단계

LIF를 로드 밸런싱 존에 추가하거나 LIF에서 제거합니다.

원하는 작업	입력…
LIF를 추가합니다	'network interface modify -vserver_vserver_name_-lif_lif_name_-dns -zone_zone_name_' 예: 'network interface modify -vserver vs1-lif data1-dns-zone cifs.company.com`
단일 LIF를 제거합니다	'network interface modify -vserver_vserver_name_-lif_lif_name_-dns-zone none' 예: 'network interface modify -vserver vs1-lif data1-dns-zone none
모든 LIF를 제거합니다	'network interface modify -vserver_vserver_name_-lif * -dns-zone none' 예: 'network interface modify -vs0 -lif * -dns-zone none' SVM의 모든 LIF를 해당 영역에서 제거하여 로드 밸런싱 영역에서 SVM을 제거할 수 있습니다.

관련 정보

- "네트워크 인터페이스 수정"

ONTAP 네트워크에 대한 **DNS** 서비스를 구성합니다

NFS 또는 SMB 서버를 생성하기 전에 SVM을 위한 DNS 서비스를 구성해야 합니다. 일반적으로 DNS 이름 서버는 NFS 또는 SMB 서버가 연결할 도메인의 Active Directory 통합 DNS 서버입니다.

이 작업에 대해

Active Directory 통합 DNS 서버에는 도메인 LDAP 및 도메인 컨트롤러 서버에 대한 SRV(서비스 위치 레코드)가

포함되어 있습니다. SVM이 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾을 수 없는 경우 NFS 또는 SMB 서버 설정에 실패합니다.

SVM은 hosts name services ns-switch 데이터베이스를 사용하여 호스트에 대한 정보를 찾을 때 사용할 이름 서비스와 순서를 결정합니다. 호스트 데이터베이스에 대해 지원되는 두 가지 이름 서비스는 파일과 DNS입니다.

SMB 서버를 생성하기 전에 DNS가 소스 중 하나인지 확인해야 합니다.

mgwd 프로세스 및 SecD 프로세스의 DNS 이름 서비스에 대한 통계를 보려면 통계 UI를 사용합니다.

단계

1. 호스트 이름 서비스 데이터베이스에 대한 현재 구성을 확인합니다. 이 예에서는 호스트 이름 서비스 데이터베이스가 기본 설정을 사용합니다.

   'vserver services name-service_ns-switch_show-vserver_vs1_-database_hosts_'

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Vserver: vs1 Name Service Switch Database: hosts
   Name Service Source Order: files, dns
   ```

2. 필요한 경우 다음 작업을 수행합니다.

   a. DNS 이름 서비스를 호스트 이름 서비스 데이터베이스에 원하는 순서로 추가하거나 소스를 다시 정렬합니다.

      이 예에서는 호스트 데이터베이스가 DNS 및 로컬 파일을 순서대로 사용하도록 구성되어 있습니다.

      'vserver services name-service_ns-switch_modify -vserver_vs1_-database_hosts_-sources_dns, files_'

   b. 이름 서비스 구성이 올바른지 확인합니다.

      'vserver services name-service_ns-switch_show-vserver_vs1_-database_hosts_'

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Name Service Source Order: dns, files
   ```

3. DNS 서비스를 구성합니다.

   'vserver services name-service dns create-vserver_vs1_-domain *example.com,example2.com* -name -servers_10.0.0.50,10.0.0.51_'

   vserver services name-service dns create 명령은 자동 구성 검증을 수행하고 ONTAP가 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

4. DNS 구성이 올바르고 서비스가 활성화되었는지 확인합니다.

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. 이름 서버의 상태를 확인합니다.

   'vserver services name-service dns check-vserver_vs1_'

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

SVM에서 동적 **DNS**를 구성합니다

Active Directory 통합 DNS 서버가 DNS에 있는 NFS 또는 SMB 서버의 DNS 레코드를 동적으로 등록하도록 하려면 SVM에서 DDNS(동적 DNS)를 구성해야 합니다.

시작하기 전에

SVM에서 DNS 이름 서비스를 구성해야 합니다. 보안 DDNS를 사용하는 경우 Active Directory 통합 DNS 이름 서버를 사용해야 하며 SVM을 위해 NFS 또는 SMB 서버 또는 Active Directory 계정을 생성해야 합니다.

이 작업에 대해

지정된 FQDN(정규화된 도메인 이름)은 고유해야 합니다.

지정된 FQDN(정규화된 도메인 이름)은 고유해야 합니다.

- NFS의 경우 'vserver services name-service dns dynamic-update' 명령의 일부로 '-vserver-FQDN'에 지정된 값이 LIF의 등록 FQDN이 됩니다.
- SMB의 경우 CIFS 서버 NetBIOS 이름 및 CIFS 서버 정규화된 도메인 이름으로 지정된 값이 LIF의 등록 FQDN이 됩니다. ONTAP에서는 구성할 수 없습니다. 다음 시나리오에서 LIF FQDN은 "CIFS_VS1.EXAMPLE.COM": 입니다

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                                Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

DDNS 업데이트에 대한 RFC 규칙을 준수하지 않는 SVM FQDN의 구성 오류를 방지하려면 RFC와 호환되는 FQDN 이름을 사용합니다. 자세한 내용은 을 참조하십시오 "RFC 1123".

단계

1. SVM에서 DDNS 구성:

   'vserver services name-service dns dynamic-update modify -vserver_vserver_name_-is-enabled_true_[-use-secure{true|false}-vserver-FQDN_FQDN_used_for_dns_updates_'

   'vserver services name-service dns dynamic-update modify -vserver_vs1_-is-enabled_true_-use -secure_true_-vserver-FQDN *vs1.example.com*`

   별표는 사용자 지정 FQDN의 일부로 사용할 수 없습니다. 예를 들어, '* .netapp.com'은(는) 유효하지 않습니다.

2. DDNS 구성이 올바른지 확인합니다.

   'vserver services name-service dns dynamic-update show'

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

ONTAP 네트워크에 대한 동적 DNS 서비스를 구성합니다

Active Directory 통합 DNS 서버가 DNS에 있는 NFS 또는 SMB 서버의 DNS 레코드를 동적으로 등록하도록 하려면 SVM에서 DDNS(동적 DNS)를 구성해야 합니다.

시작하기 전에

SVM에서 DNS 이름 서비스를 구성해야 합니다. 보안 DDNS를 사용하는 경우 Active Directory 통합 DNS 이름 서버를 사용해야 하며 SVM을 위해 NFS 또는 SMB 서버 또는 Active Directory 계정을 생성해야 합니다.

이 작업에 대해

지정된 FQDN은 고유해야 합니다.

> DDNS 업데이트에 대한 RFC 규칙을 준수하지 않는 SVM FQDN의 구성 오류를 방지하려면 RFC와 호환되는 FQDN 이름을 사용합니다.

단계

1. SVM에서 DDNS 구성:

   'vserver services name-service dns dynamic-update modify -vserver_vserver_name_-is-enabled_true_[-use-secure{true|false}-vserver-FQDN_FQDN_used_for_dns_updates_'

   'vserver services name-service dns dynamic-update modify -vserver_vs1_-is-enabled_true_-use -secure_true_-vserver-FQDN *vs1.example.com*`

   별표는 사용자 지정 FQDN의 일부로 사용할 수 없습니다. 예를 들어, '* .netapp.com'은(는) 유효하지 않습니다.

2. DDNS 구성이 올바른지 확인합니다.

   'vserver services name-service dns dynamic-update show'

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

호스트 이름 확인

ONTAP 네트워크의 호스트 이름 확인에 대해 알아봅니다

클라이언트에 대한 액세스를 제공하고 서비스에 액세스하려면 ONTAP가 호스트 이름을 숫자 IP 주소로 변환할 수 있어야 합니다. 로컬 또는 외부 이름 서비스를 사용하여 호스트 정보를 확인하도록 SVM(스토리지 가상 시스템)을 구성해야 합니다. ONTAP에서는 외부 DNS 서버 구성 또는 호스트 이름 확인을 위한 로컬 호스트 파일 구성을 지원합니다.

외부 DNS 서버를 사용하는 경우 DDNS(동적 DNS)를 구성하여 스토리지 시스템에서 DNS 서버로 새 DNS 정보 또는 변경된 DNS 정보를 자동으로 전송할 수 있습니다. 동적 DNS 업데이트가 없으면 새 시스템을 온라인으로 연결하거나 기존 DNS 정보가 변경될 때 DNS 정보(DNS 이름 및 IP 주소)를 식별된 DNS 서버에 수동으로 추가해야 합니다. 이 프로세스는 느리고 오류가 발생하기 쉽습니다. 재해 복구 중에 수동 구성으로 인해 다운타임이 오래 발생할 수 있습니다.

ONTAP 네트워크의 호스트 이름 확인을 위해 DNS를 구성합니다

DNS를 사용하여 로컬 또는 원격 소스에 액세스하여 호스트 정보를 확인할 수 있습니다. 이러한 소스 중 하나 또는 둘 다에 액세스하려면 DNS를 구성해야 합니다.

ONTAP는 클라이언트에 대한 적절한 액세스를 제공하기 위해 호스트 정보를 조회해야 합니다. 호스트 정보를 얻기 위해 ONTAP가 로컬 또는 외부 DNS 서비스에 액세스하도록 이름 서비스를 구성해야 합니다.

ONTAP는 UNIX 시스템의 '/etc/nsswitch.conf' 파일에 해당하는 테이블에 이름 서비스 구성 정보를 저장합니다.

외부 **DNS** 서버를 사용하여 호스트 이름 확인을 위해 **SVM** 및 데이터 **LIF**를 구성합니다

SVM에서 DNS를 사용하도록 설정하려면 'vserver services name-service dns' 명령을 사용하고, 호스트 이름 확인을 위해 DNS를 사용하도록 구성할 수 있습니다. 호스트 이름은 외부 DNS 서버를 사용하여 확인됩니다.

시작하기 전에

호스트 이름 조회에 사이트 전체 DNS 서버를 사용할 수 있어야 합니다.

단일 장애 지점을 방지하려면 둘 이상의 DNS 서버를 구성해야 합니다. DNS 서버 이름을 하나만 입력하면 'vserver services name-service dns create' 명령이 경고를 보냅니다.

이 작업에 대해

을 참조하십시오 동적 DNS 서비스를 구성합니다 SVM에서 동적 DNS 구성에 대한 자세한 내용은 를 참조하십시오.

단계

1. SVM에서 DNS 활성화:

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

다음 명령을 실행하면 SVM VS1 에서 외부 DNS 서버 서버가 활성화됩니다.

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```

> ⓘ 를 클릭합니다 `vserver services name-service dns create` Command는 자동 구성 유효성 검사를 수행하고 ONTAP에서 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

2. 'vserver services name-service dns check' 명령어를 이용하여 이름 서버의 상태를 확인한다.

```
vserver services name-service dns check -vserver vs1.example.com
                                    Name Server
Vserver             Name Server     Status       Status Details
-------------       --------------- ------------
--------------------------
vs1.example.com     10.0.0.50       up           Response time (msec): 2
vs1.example.com     10.0.0.51       up           Response time (msec): 2
```

DNS와 관련된 서비스 정책에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9.6 이상의 LIF 및 서비스 정책".

호스트 이름 확인을 위해 이름 서비스 스위치 테이블을 구성합니다

ONTAP가 로컬 또는 외부 이름 서비스에 문의하여 호스트 정보를 검색할 수 있도록 이름 서비스 스위치 테이블을 올바르게 구성해야 합니다.

시작하기 전에

사용자 환경에서 호스트 매핑에 사용할 이름 서비스를 결정해야 합니다.

단계

1. 이름 서비스 스위치 테이블에 필요한 항목을 추가합니다.

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. 이름 서비스 스위치 테이블에 원하는 순서대로 필요한 항목이 포함되어 있는지 확인합니다.

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

예

다음 예에서는 SVM VS1에 대한 이름 서비스 스위치 테이블의 항목을 수정하여 먼저 로컬 호스트 파일을 사용한 다음 외부 DNS 서버를 사용하여 호스트 이름을 확인합니다.

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

ONTAP hosts 테이블을 관리하는 **ONTAP** 명령

클러스터 관리자는 SVM(관리 스토리지 가상 시스템)의 호스트 테이블에 있는 호스트 이름 항목을 추가, 수정, 삭제 및 볼 수 있습니다. SVM 관리자는 할당된 SVM에 대해서만 호스트 이름 항목을 구성할 수 있습니다.

로컬 호스트 이름 항목을 관리하는 명령입니다

'vserver services name-service dns hosts' 명령을 사용하여 DNS 호스트 테이블 항목을 생성, 수정 또는 삭제할 수 있습니다.

DNS 호스트 이름 항목을 만들거나 수정할 때 쉼표로 구분된 여러 개의 별칭 주소를 지정할 수 있습니다.

원하는 작업	이 명령 사용…
DNS 호스트 이름 항목을 생성합니다	'vserver services name-service DNS hosts create'

DNS 호스트 이름 항목을 수정합니다	'vserver services name-service dns hosts modify'
DNS 호스트 이름 항목을 삭제합니다	'vserver services name-service DNS hosts delete'

명령에 대한 자세한 `vserver services name-service dns hosts` 내용은 를 참조하십시오 "ONTAP 명령 참조입니다".

네트워크 보안

모든 **SSL** 연결에 **FIPS**를 사용하여 **ONTAP** 네트워크 보안을 구성합니다

ONTAP 모든 SSL 연결에 대해 연방 정보 처리 표준(FIPS) 140-2를 준수합니다. ONTAP 내에서 SSL FIPS 모드를 켜고 끌 수 있고, SSL 프로토콜을 전역적으로 설정하고, 취약한 암호를 끌 수 있습니다.

기본적으로 ONTAP의 SSL은 FIPS 준수가 비활성화되고 다음 TLS 프로토콜이 활성화된 상태로 설정됩니다.

- TLSv1.3(ONTAP 9.11.1부터 시작)
- TLSv1.2

이전 ONTAP 릴리스에는 기본적으로 다음과 같은 TLS 프로토콜이 활성화되어 있었습니다.

- TLSv1.1(ONTAP 9.12.1부터 기본적으로 비활성화됨)
- TLSv1(ONTAP 9.8부터 기본적으로 비활성화됨)

SSL FIPS 모드가 활성화되면 ONTAP에서 외부 클라이언트 또는 ONTAP 외부의 서버 구성 요소로의 SSL 통신은 SSL에 FIPS 호환 암호화를 사용합니다.

관리자 계정이 SSH 공개 키로 SVM에 액세스하려면 SSL FIPS 모드를 활성화하기 전에 호스트 키 알고리즘이 지원되는지 확인해야 합니다.

- 참고: * ONTAP 9.11.1 이상 릴리스에서 호스트 키 알고리즘 지원이 변경되었습니다.

ONTAP 릴리즈	지원되는 키 유형	지원되지 않는 키 유형입니다
9.11.1 이상	ECDSA-SHA2-nistp256	RSA-SHA2-512 + RSA - SHA2-256 + ssh-ed25519 + ssh-dss+ssh-rssh-rsa
9.10.1 이하	ECDSA-SHA2-nistp256+ssh-ed25519	SSH-DSS+ssh-rsa를 사용합니다

FIPS를 활성화하기 전에 지원되는 키 알고리즘이 없는 기존 SSH 공개 키 계정을 지원되는 키 유형으로 재구성해야 합니다. 그렇지 않으면 관리자 인증이 실패합니다.

자세한 내용은 을 참조하십시오 "SSH 공개 키 계정을 활성화합니다".

ONTAP 9.18.1은 SSL을 위한 ML-KEM, ML-DSA 및 SLH-DSA 포스트 양자 컴퓨팅 암호화 알고리즘에 대한 지원을 도입하여 향후 발생할 수 있는 양자 컴퓨터 공격에 대비한 보안 계층을 추가로 제공합니다. 이러한 알고리즘은 다음과 같은 경우에만 사용할 수 있습니다.FIPS가 비활성화되었습니다 . FIPS가 비활성화되어 있고 피어가 이를 지원하는 경우 포스트 양자 암호화 알고리즘이 협상됩니다.

FIPS를 사용하도록 설정합니다

모든 보안 사용자는 시스템 설치 또는 업그레이드 직후 보안 구성을 조정하는 것이 좋습니다. SSL FIPS 모드가 활성화되면 ONTAP에서 외부 클라이언트 또는 ONTAP 외부의 서버 구성 요소로의 SSL 통신은 SSL에 FIPS 호환 암호화를 사용합니다.

FIPS가 설정되어 있으면 RSA 키 길이 4096으로 인증서를 설치하거나 생성할 수 없습니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. FIPS 활성화:

   ```
   security config modify * -is-fips-enabled true
   ```

3. 계속하라는 메시지가 나타나면 y를 입력합니다
4. ONTAP 9.9.1부터 재부팅이 필요하지 않습니다. ONTAP 9.8 또는 이전 버전을 사용하는 경우 클러스터의 각 노드를 하나씩 수동으로 재부팅하세요.

예

ONTAP 9.9.1 이상을 실행 중인 경우 경고 메시지가 표시되지 않습니다.

```
security config modify -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

및 SSL FIPS 모드 구성에 대한 자세한 `security config modify` 내용은 를 "ONTAP 명령 참조입니다 "참조하십시오.

FIPS를 비활성화합니다

ONTAP 9.18.1부터 ONTAP 의 SSL은 ML-KEM, ML-DSA, SLH-DSA 포스트 양자 컴퓨팅 암호화 알고리즘을 지원합니다. 이러한 알고리즘은 FIPS가 비활성화되어 있고 피어가 이를 지원하는 경우에만 사용할 수 있습니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 다음을 입력하여 FIPS를 비활성화합니다.

   ```
   security config modify -is-fips-enabled false
   ```

3. 계속하라는 메시지가 나타나면 y를 입력합니다.
4. ONTAP 9.9.1부터 재부팅이 필요하지 않습니다. ONTAP 9.8 또는 이전 버전을 사용하는 경우 클러스터의 각 노드를 수동으로 재부팅하세요.

SSLv3 프로토콜을 사용해야 하는 경우 위의 절차에 따라 FIPS를 비활성화해야 합니다. FIPS가 비활성화된 경우에만 SSLv3를 활성화할 수 있습니다.

다음 명령을 사용하여 SSLv3를 활성화할 수 있습니다. ONTAP 9.9.1 이상을 실행 중인 경우 경고 메시지가 나타나지 않습니다.

```
security config modify -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

FIPS 준수 상태를 봅니다

전체 클러스터에서 현재 보안 구성 설정이 실행되고 있는지 확인할 수 있습니다.

단계

1. ONTAP 9.8 또는 이전 버전을 사용하는 경우 클러스터의 각 노드를 하나씩 수동으로 재부팅하세요.
2. 현재 준수 상태 보기:

   '보안 구성 쇼'

```
cluster1::> security config show
Cluster    Supported
FIPS Mode  Protocols Supported Cipher Suites
---------- ---------
-----------------------------------------------------------
false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
TLS_RSA_WITH_AES_128_CCM_8,
           TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                     TLS_RSA_WITH_AES_128_CBC_SHA,
                     TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CCM,
                     TLS_RSA_WITH_AES_256_CCM_8,
                     ...
```

에 대한 자세한 내용은 `security config show` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "FIPS 203: 모듈 격자 기반 키 캡슐화 메커니즘 표준(ML-KEM)"
- "FIPS 204: 모듈 격자 기반 디지털 서명 표준(ML-DSA)"
- "FIPS 205: 상태 비저장 해시 기반 디지털 서명 표준(SLH-DSA)"

IPsec 전송 중 암호화를 구성합니다

ONTAP 네트워크에서 IP 보안 사용을 준비합니다

ONTAP 9.8부터 IP 보안(IPsec)을 사용하여 네트워크 트래픽을 보호할 수 있습니다. IPsec은 ONTAP에서 사용할 수 있는 여러 가지 데이터 이동 중 또는 전송 중 암호화 옵션 중 하나입니다. IPsec을 프로덕션 환경에서 사용하기 전에 구성할 준비를 해야 합니다.

ONTAP에서 IP 보안 구현

IPSec은 IETF에서 관리하는 인터넷 표준입니다. IP 레벨에서 네트워크 엔드포인트 간에 흐르는 트래픽에 대한 인증뿐 아니라 데이터 암호화 및 무결성을 제공합니다.

ONTAP를 통해 IPsec은 ONTAP와 NFS, SMB 및 iSCSI 프로토콜을 포함한 다양한 클라이언트 간의 모든 IP 트래픽을 보호합니다. 네트워크 트래픽은 개인 정보 보호 및 데이터 무결성 외에도 재생 및 메시지 가로채기 공격과 같은 여러 공격으로부터 보호됩니다. ONTAP는 IPsec 전송 모드 구현을 사용합니다. IPv4 또는 IPv6를 사용하여 ONTAP와 클라이언트 간의 키 자료를 협상하는 데 IKE(인터넷 키 교환) 프로토콜 버전 2를 활용합니다.

클러스터에서 IPsec 기능이 활성화된 경우 네트워크에는 다양한 트래픽 특성과 일치하는 ONTAP SPD(보안 정책 데이터베이스)에 하나 이상의 항목이 필요합니다. 이러한 항목은 데이터를 처리하고 전송하는 데 필요한 특정 보호 세부 정보(예: 암호 그룹 및 인증 방법)에 매핑됩니다. 각 클라이언트에는 해당 SPD 항목도 필요합니다.

특정 트래픽 유형의 경우 다른 이동 중인 데이터 암호화 옵션이 더 선호될 수 있습니다. 예를 들어, NetApp SnapMirror 및 클러스터 피어링 트래픽의 암호화를 위해 일반적으로 IPsec 대신 TLS(전송 계층 보안) 프로토콜을 사용하는 것이 좋습니다. TLS는 대부분의 상황에서 더 나은 성능을 제공하기 때문입니다.

관련 정보

- "Internet Engineering Task Force의 약어입니다"
- "RFC 4301: 인터넷 프로토콜에 대한 보안 아키텍처"

ONTAP IPsec 구현의 진화

IPsec은 ONTAP 9.8에서 처음 도입되었습니다. 이후 ONTAP 릴리스에서는 아래에 설명된 대로 구현 방식이 지속적으로 발전해 왔습니다.

ONTAP 9.18.1

IPsec 하드웨어 오프로드에 대한 지원이 IPv6 트래픽으로 확장되었습니다.

ONTAP 9.17.1

IPsec 하드웨어 오프로드에 대한 지원이 확장되었습니다. "링크 집계 그룹" . "포스트퀀텀 사전 공유 키(PPK)" IPsec 사전 공유 키(PSK) 인증이 지원됩니다.

ONTAP 9.16.1

암호화 및 무결성 검사와 같은 여러 암호화 작업을 지원되는 NIC 카드로 오프로드할 수 있습니다. 자세한 내용은 을 IPsec 하드웨어 오프로드 기능 참조하십시오.

ONTAP 9.12.1

MetroCluster IP 및 MetroCluster 패브릭 연결 구성에서 IPsec 프런트엔드 호스트 프로토콜 지원을 사용할 수 있습니다. MetroCluster 클러스터와 함께 제공되는 IPsec 지원은 프런트 엔드 호스트 트래픽으로 제한되며 MetroCluster 인터클러스터 LIF에서는 지원되지 않습니다.

ONTAP 9.10.1

PSK 외에도 인증서를 사용하여 IPsec 인증을 수행할 수 있습니다. ONTAP 9.10.1 이전에는 PSK만 인증에 지원되었습니다.

ONTAP 9.9.1

IPsec에 사용되는 암호화 알고리즘은 FIPS 140-2 검증을 거쳤습니다. 이러한 알고리즘은 FIPS 140-2 검증을 수행하는 ONTAP의 NetApp 암호화 모듈에 의해 처리됩니다.

ONTAP 9.8

IPsec에 대한 지원은 처음에 전송 모드 구현에 따라 사용할 수 있습니다.

IPsec 하드웨어 오프로드 기능

ONTAP 9.16.1 이상을 사용하는 경우 암호화 및 무결성 검사와 같은 계산 집약적인 특정 작업을 스토리지 노드에 설치된 NIC(Network Interface Controller) 카드로 오프로드할 수 있습니다. NIC 카드로 오프로드된 작업의 처리량은 약 5% 이하입니다. 이를 통해 IPsec으로 보호되는 네트워크 트래픽의 성능과 처리량을 크게 향상시킬 수 있습니다.

요구 사항 및 권장 사항

IPsec 하드웨어 오프로드 기능을 사용하기 전에 고려해야 할 몇 가지 요구 사항이 있습니다.

지원되는 이더넷 카드

지원되는 이더넷 카드만 설치하고 사용해야 합니다. ONTAP 9.16.1부터 지원되는 이더넷 카드는 다음과 같습니다.

- X50131A(2p, 40G/100G/200g/400G 이더넷 컨트롤러)

- X60132A(4P, 10G/25G 이더넷 컨트롤러)

ONTAP 9.17.1에서는 다음 이더넷 카드에 대한 지원이 추가되었습니다.

- X50135A(2p, 40G/100G 이더넷 컨트롤러)
- X60135A(2p, 40G/100G 이더넷 컨트롤러)

X50131A 및 X50135A 카드는 다음 플랫폼에서 지원됩니다.

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K 를 참조하십시오
- AFF A90 를 참조하십시오
- AFF A70 를 참조하십시오

X60132A 및 X60135A 카드는 다음 플랫폼에서 지원됩니다.

- ASA A50
- ASA A30
- ASA A20
- AFF A50 를 참조하십시오
- AFF A30 를 참조하십시오
- AFF A20 를 참조하십시오

를 참조하십시오 "NetApp Hardware Universe를 참조하십시오" 지원되는 플랫폼과 카드에 대한 자세한 내용은 여기를 참조하세요.

클러스터 범위

IPsec 하드웨어 오프로드 기능은 클러스터에 대해 전역적으로 구성됩니다. 예를 들어, 명령은 `security ipsec config` 클러스터의 모든 노드에 적용됩니다.

일관된 구성

지원되는 NIC 카드는 클러스터의 모든 노드에 설치되어야 합니다. 지원되는 NIC 카드를 일부 노드에서만 사용할 수 있는 경우 일부 LIF가 오프로드 지원 NIC에 호스팅되지 않으면 페일오버 후 성능이 크게 저하될 수 있습니다.

다시 재생 안 함

ONTAP(기본 구성) 및 IPsec 클라이언트에서 IPsec 재생 방지 보호를 비활성화해야 합니다. 비활성화하지 않으면 조각화 및 다중 경로(중복 경로)가 지원되지 않습니다.

ONTAP IPsec 구성이 기본값에서 재생 방지 보호를 사용하도록 변경된 경우 다음 명령을 사용하여 사용하지 않도록 설정합니다.

```
security ipsec config modify -replay-window 0
```

클라이언트에서 IPsec 재생 방지 보호가 해제되어 있는지 확인해야 합니다. 재생 방지 보호를 비활성화하려면 클라이언트에 대한 IPsec 설명서를 참조하십시오.

제한 사항

IPsec 하드웨어 오프로드 기능을 사용하기 전에 고려해야 할 몇 가지 제한 사항이 있습니다.

IPv6를 참조하십시오

ONTAP 9.18.1부터 IPsec 하드웨어 오프로드 기능에 IPv6가 지원됩니다. ONTAP 9.18.1 이전에는 IPsec 하드웨어 오프로드가 IPv6를 지원하지 않았습니다.

확장 순서 번호

IPsec 확장 시퀀스 번호는 하드웨어 오프로드 기능에서 지원되지 않습니다. 일반적인 32비트 시퀀스 번호만 사용됩니다.

Link Aggregation

ONTAP 9.17.1부터 IPsec 하드웨어 오프로드 기능을 사용할 수 있습니다. "링크 집계 그룹" .

9.17.1 이전 버전에서는 IPsec 하드웨어 오프로드 기능이 링크 집계를 지원하지 않습니다. 다음에서 관리하는 인터페이스 또는 링크 집계 그룹과 함께 사용할 수 없습니다. `network port ifgrp` ONTAP CLI에서 명령을 실행합니다.

ONTAP CLI에서 구성을 지원합니다

ONTAP 9.16.1에서는 아래와 같이 IPsec 하드웨어 오프로드 기능을 지원하도록 기존 CLI 명령 세 개가 업데이트됩니다. 자세한 내용은 를 "ONTAP에서 IP 보안을 구성합니다"참조하십시오.

ONTAP 명령	업데이트
'보안 IPsec 구성 표시'	부울 매개 변수는 `Offload Enabled` 현재 NIC 오프로드 상태를 표시합니다.
`security ipsec config modify`	매개 변수는 `is-offload-enabled` NIC 오프로드 기능을 활성화 또는 비활성화하는 데 사용할 수 있습니다.
`security ipsec config show-ipsecsa`	인바운드와 아웃바운드 트래픽을 바이트 및 패킷으로 표시하기 위해 새로운 카운터 4개가 추가되었습니다.

ONTAP REST API에서 구성 지원

아래에 설명된 대로 IPsec 하드웨어 오프로드 기능을 지원하도록 ONTAP 9.16.1에서 두 개의 기존 REST API 끝점이 업데이트되었습니다.

REST 엔드포인트	업데이트
`/api/security/ipsec`	매개 변수가 `offload_enabled` 추가되었으며 패치 메서드에서 사용할 수 있습니다.
`/api/security/ipsec/security_association`	오프로드 기능에 의해 처리된 총 바이트 및 패킷을 추적하기 위해 두 개의 새로운 카운터 값이 추가되었습니다.

를 비롯한 ONTAP REST API에 대한 자세한 내용은 ONTAP 자동화 설명서 를 "ONTAP REST API의 새로운 기능" 참조하십시오. 에 대한 자세한 내용은 ONTAP 자동화 설명서를 검토해야 "IPsec 끝점" 합니다.

관련 정보

- "보안 ipsec"

ONTAP 네트워크에 대한 **IP** 보안을 구성합니다

ONTAP 클러스터에서 IPsec 전송 중 암호화를 구성하고 활성화하려면 몇 가지 작업을 수행해야 합니다.

IPsec을 구성하기 전에 반드시 "IP 보안 사용을 준비합니다"검토하십시오. 예를 들어, ONTAP 9.16.1부터 사용 가능한 IPsec 하드웨어 오프로드 기능을 사용할지 여부를 결정해야 할 수 있습니다.

클러스터에서 **IPsec**을 활성화합니다

클러스터에서 IPsec을 활성화하여 전송 중에 데이터가 지속적으로 암호화되고 안전하게 보호되도록 할 수 있습니다.

단계

1. IPsec이 이미 활성화되어 있는지 확인:

   '보안 IPsec 구성 표시'

   결과에 "IPsec 사용: 거짓"이 포함된 경우 다음 단계를 진행합니다.

2. IPsec 활성화:

   보안 IPsec config modify -is -enabled true

   부울 매개 변수를 사용하여 IPsec 하드웨어 오프로드 기능을 활성화할 수 `is-offload-enabled` 있습니다.

3. 검색 명령을 다시 실행합니다.

   '보안 IPsec 구성 표시'

   그 결과에는 이제 "IPsec 사용: 참"이 포함됩니다.

인증서 인증을 사용하여 **IPsec** 정책 생성을 준비합니다

인증을 위해 사전 공유 키(PSK)만 사용하고 인증서 인증을 사용하지 않는 경우 이 단계를 건너뛸 수 있습니다.

인증을 위해 인증서를 사용하는 IPsec 정책을 만들기 전에 다음 필수 구성 요소가 충족되었는지 확인해야 합니다.

- ONTAP와 클라이언트 모두 최종 엔터티(ONTAP 또는 클라이언트) 인증서를 양쪽 모두에서 확인할 수 있도록 타사의 CA 인증서가 설치되어 있어야 합니다
- 정책에 참여하는 ONTAP LIF에 대해 인증서가 설치됩니다

ONTAP LIF는 인증서를 공유할 수 있습니다. 인증서와 LIF 간 일대일 매핑은 필요하지 않습니다.

단계

1. 상호 인증 중에 사용되는 모든 CA 인증서(ONTAP 측 CA와 클라이언트측 CA 모두 포함)를 ONTAP 인증서 관리에 설치합니다(ONTAP 자체 서명 루트 CA의 경우처럼).

◦ 샘플 명령 *

```
cluster::> security certificate install -vserver svm_name -type server-ca
-cert-name my_ca_cert
```

2. 설치된 CA가 인증 중에 IPsec CA 검색 경로 내에 있는지 확인하려면 를 사용하여 ONTAP 인증서 관리 CA를 IPsec 모듈에 추가합니다 `security ipsec ca-certificate add` 명령.

◦ 샘플 명령 *

```
cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
my_ca_cert
```

3. ONTAP LIF에서 사용할 인증서를 생성하고 설치합니다. 이 인증서의 발급자 CA가 이미 ONTAP에 설치되어 있고 IPsec에 추가되어야 합니다.

◦ 샘플 명령 *

```
cluster::> security certificate install -vserver svm_name -type server -cert
-name my_nfs_server_cert
```

ONTAP의 인증서에 대한 자세한 내용은 ONTAP 9 설명서의 보안 인증서 명령을 참조하십시오.

보안 정책 데이터베이스**(SPD)** 정의

IPsec은 네트워크에서 트래픽이 흐르도록 허용하기 전에 SPD 항목을 필요로 합니다. PSK 또는 인증서를 인증에 사용하는지에 관계없이 적용됩니다.

단계

1. '보안 IPsec 정책 만들기' 명령을 사용하여 다음을 수행합니다.

a. IPsec 전송에 참여할 IP 주소의 ONTAP IP 주소 또는 서브넷을 선택합니다.

b. ONTAP IP 주소에 연결할 클라이언트 IP 주소를 선택합니다.

ⓘ 클라이언트는 미리 공유된 키(PSK)가 있는 인터넷 키 교환 버전 2(IKEv2)를 지원해야 합니다.

c. 선택적으로 상위 계층 프로토콜(UDP, TCP, ICMP 등), 로컬 포트 번호, 원격 포트 번호 등 트래픽을 보호하기 위한 세부적인 트래픽 매개변수를 선택할 수 있습니다. 해당 매개변수는 다음과 같습니다. `protocols` , `local-ports` 그리고 `remote-ports` 각기.

ONTAP IP 주소와 클라이언트 IP 주소 사이의 모든 트래픽을 보호하려면 이 단계를 건너뜁니다. 모든 트래픽을 보호하는 것이 기본값입니다.

d. 에 대한 PSK 또는 PKI(공개 키 인프라)를 입력합니다 `auth-method` 원하는 인증 방법에 대한 매개 변수입니다.

i. PSK를 입력한 경우 매개변수를 포함시킨 다음 <enter> 키를 눌러 미리 공유된 키를 입력하고 확인합니다.

ⓘ `local-identity`및 `remote-identity` 매개 변수는 호스트와 클라이언트 모두 strongSwan을 사용하고 호스트 또는 클라이언트에 대해 와일드카드 정책을 선택하지 않은 경우 선택 사항입니다.

ii. PKI를 입력하는 경우 도 입력해야 합니다 `cert-name`, `local-identity`, `remote-identity` 매개 변수. 원격 측 인증서 ID를 알 수 없거나 여러 클라이언트 ID가 필요한 경우 특수 ID를 입력합니다 `ANYTHING`.

e. ONTAP 9.17.1부터 선택적으로 포스트퀀텀 사전 공유 키(PPK) ID를 입력합니다. `ppk-identity` 매개변수. PPK는 향후 발생할 수 있는 양자 컴퓨터 공격에 대비하여 추가적인 보안 계층을 제공합니다. PPK ID를 입력하면 PPK 비밀번호를 입력하라는 메시지가 표시됩니다. PPK는 PSK 인증에만 지원됩니다.

자세히 알아보세요 `security ipsec policy create` 에서 "ONTAP 명령 참조입니다" .

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

ONTAP와 클라이언트 모두 일치하는 IPsec 정책을 설정하고 인증 자격 증명(PSK 또는 인증서)이 양쪽 모두에 적용될 때까지 IP 트래픽은 클라이언트와 서버 간에 이동할 수 없습니다.

IPsec ID를 사용합니다

사전 공유 키 인증 방법의 경우 호스트와 클라이언트 모두 strongSwan을 사용하고 호스트 또는 클라이언트에 대해 와일드카드 정책을 선택하지 않은 경우 로컬 및 원격 ID는 선택 사항입니다.

PKI/인증서 인증 방법의 경우 로컬 및 원격 ID가 모두 필수입니다. ID는 각 측의 인증서 내에서 인증되고 확인 프로세스에 사용되는 ID를 지정합니다. 원격 ID를 알 수 없거나 다른 ID가 많을 수 있는 경우 특수 ID를 사용하십시오 `ANYTHING`.

이 작업에 대해

ONTAP 내에서 SPD 항목을 수정하거나 SPD 정책을 생성하는 동안 ID를 지정합니다. SPD는 IP 주소 또는 문자열 형식 ID 이름일 수 있습니다.

단계

1. 다음 명령을 사용하여 기존 SPD ID 설정을 수정합니다.

보안 IPsec 정책 수정

샘플 명령

'보안 IPsec 정책 수정 - vserver_vs1_-name_test34_-local-identity_192.168.134.34_-remote-identity *client.fooboo.com*`

IPsec 다중 클라이언트 구성

적은 수의 클라이언트가 IPsec을 활용해야 하는 경우 각 클라이언트에 대해 단일 SPD 항목을 사용하는 것이 충분합니다. 하지만 수백 또는 수천 개의 클라이언트가 IPsec을 활용해야 하는 경우 NetApp은 IPsec 다중 클라이언트 구성을 사용할 것을 권장합니다.

이 작업에 대해

ONTAP는 IPsec을 사용하여 여러 네트워크의 여러 클라이언트를 단일 SVM IP 주소에 연결할 수 있도록 지원합니다. 다음 방법 중 하나를 사용하여 이 작업을 수행할 수 있습니다.

- * 서브넷 구성 *

  특정 서브넷(예: 192.168.134.0/24)의 모든 클라이언트가 단일 SPD 정책 항목을 사용하여 단일 SVM IP 주소에 연결되도록 하려면 을 지정해야 합니다 `remote-ip-subnets` 서브넷 형식으로 표시됩니다. 또한 를 지정해야 합니다 `remote-identity` 올바른 클라이언트 측 ID를 가진 필드입니다.

  > 서브넷 구성에서 단일 정책 항목을 사용하는 경우 해당 서브넷의 IPsec 클라이언트는 IPsec ID 및 미리 공유된 키(PSK)를 공유합니다. 그러나 인증서 인증에서는 그렇지 않습니다. 인증서를 사용할 때 각 클라이언트는 고유한 인증서 또는 공유 인증서를 사용하여 인증할 수 있습니다. ONTAP IPsec은 로컬 트러스트 저장소에 설치된 CA를 기반으로 인증서의 유효성을 검사합니다. ONTAP는 CRL(인증서 해지 목록) 검사도 지원합니다.

- * 모든 클라이언트 구성 허용 *

  소스 IP 주소와 관계없이 모든 클라이언트가 SVM IPsec 지원 IP 주소에 연결되도록 하려면 을 사용합니다 `0.0.0.0/0` 를 지정할 때 와일드카드입니다 `remote-ip-subnets` 필드에 입력합니다.

  또한 를 지정해야 합니다 `remote-identity` 올바른 클라이언트 측 ID를 가진 필드입니다. 인증서 인증의 경우 를 입력할 수 있습니다 `ANYTHING`.

  또한, 가 있는 경우 `0.0.0.0/0` 와일드카드를 사용하는 경우 사용할 특정 로컬 또는 원격 포트 번호를 구성해야 합니다. 예를 들면, 다음과 같습니다. `NFS port 2049`.

  단계

  a. 다음 명령 중 하나를 사용하여 여러 클라이언트에 대해 IPsec을 구성합니다.

     i. 여러 IPsec 클라이언트를 지원하기 위해 * 서브넷 구성 * 을 사용하는 경우:

        '보안 IPsec 정책 생성 - vserver_vserver_name_-name_policy_name_-local-ip-subnets_ipsec_ip_address /32_-remote-ip_subnets_ip_address/subnet_-local-identity_local_id_-remote-identity_remote_id_'

  샘플 명령

  '보안 IPsec 정책 생성 - vserver_vs1_-name_subnet134_-local-ip-subnet134_-local_192.168.134.34 /32_-remote-ip-subnets_192.168.134.0 /24_-local-identity_ontaity_-remote-identity_client_side_identity_'

     i. 을(를) 사용하여 여러 IPsec 클라이언트를 지원하도록 모든 클라이언트 구성 * 허용 을 사용하는 경우:

        '보안 IPsec 정책 생성 - vserver_vserver_name_-name_policy_name_-local-ip-subnets_ipsec_ip_address /32_-remote-ip-subnets_0.0.0.0/0_-local-ports_port_number_-local-identity_local_id_-remote_identity_remote_id_'입니다

  샘플 명령

  '보안 IPsec 정책 생성 - vserver_vs1_-name_test35_-local-ip-subnets_ipsec_ip_address/32_-remote-ip-subnets_0.0.0.0/0_-local-ports_2049_-local-identity_side_identity_-remote-identity_client_side_identity_'입니다

IPsec 통계를 표시합니다

협상을 통해 ONTAP SVM IP 주소와 클라이언트 IP 주소 간에 IKE SA(Security Association)라는 보안 채널을 설정할 수 있습니다. IPsec SAS는 실제 데이터 암호화 및 암호 해독 작업을 수행할 수 있도록 두 엔드포인트 모두에 설치됩니다. 통계 명령을 사용하여 IPsec SAS 및 IKE SAS의 상태를 확인할 수 있습니다.

IPsec 하드웨어 오프로드 기능을 사용하는 경우 명령과 함께 여러 개의 새 카운터가 표시됩니다 `security ipsec config show-ipsecsa`.

샘플 명령

IKE SA 샘플 명령:

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

IPsec SA 샘플 명령 및 출력:

SECURN IPSEC show -ipsecsa -node_hosting_node_name_for_svm_ip _'

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
             Policy Local           Remote
Vserver      Name   Address         Address         Initator-SPI     State
------------ ------ --------------- --------------- ----------------
------------
vs1          test34
                    192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

IPsec SA 샘플 명령 및 출력:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
             Policy  Local           Remote          Inbound  Outbound
Vserver      Name    Address         Address         SPI      SPI
State
------------ ------- --------------- --------------- -------- --------
---------
vs1          test34
                     192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

관련 정보

- "보안 인증서 설치"
- "보안 ipsec"

ONTAP 백엔드 클러스터 네트워크 암호화 구성

ONTAP 9.18.1부터 백엔드 클러스터 네트워크에서 전송 중인 데이터에 대한 TLS(전송 계층 보안) 암호화를 구성할 수 있습니다. 이 암호화는 백엔드 클러스터 네트워크의 ONTAP 노드 간에 전송될 때 ONTAP 에 저장된 고객 데이터를 보호합니다.

이 작업에 대해

- 백엔드 클러스터 네트워크 암호화는 기본적으로 비활성화되어 있습니다.
- 백엔드 클러스터 네트워크 암호화가 활성화되면 ONTAP 에 저장된 모든 고객 데이터는 백엔드 클러스터 네트워크의 ONTAP 노드 간에 전송될 때 암호화됩니다. 제어 경로 데이터와 같은 일부 클러스터 네트워크 트래픽은 암호화되지 않습니다.
- 기본적으로 백엔드 클러스터 네트워크 암호화는 클러스터의 각 노드에 대해 자동 생성된 인증서를 사용합니다. 당신은 할 수 있습니다클러스터 네트워크 암호화 인증서 관리 각 노드에서 사용자 정의 설치 인증서를 사용합니다.

시작하기 전에

- 당신은 ONTAP 관리자여야 합니다. `admin` 다음 작업을 수행하기 위한 권한 수준입니다.
- 백엔드 클러스터 네트워크 암호화를 활성화하려면 클러스터의 모든 노드에서 ONTAP 9.18.1 이상을 실행해야 합니다.

클러스터 네트워크 통신에 대한 암호화를 활성화하거나 비활성화합니다.

단계

1. 현재 클러스터 네트워크 암호화 상태를 확인하세요.

```
security cluster-network show
```

이 명령은 클러스터 네트워크 암호화의 현재 상태를 보여줍니다.

```
Cluster-1::*> security cluster-network show

Enabled: true

Mode: tls

Status: READY
```

2. TLS 백엔드 클러스터 네트워크 암호화를 활성화하거나 비활성화합니다.

```
security cluster-network modify -enabled <true|false>
```

이 명령은 백엔드 클러스터 네트워크에서 전송 중인 고객 데이터에 대한 암호화된 통신을 활성화하거나 비활성화합니다.

클러스터 네트워크 암호화 인증서 관리

1. 현재 클러스터 네트워크 암호화 인증서 정보를 확인하세요.

```
security cluster-network certificate show
```

이 명령은 현재 클러스터 네트워크 암호화 인증서 정보를 보여줍니다.

```
security cluster-network certificate show
Node                  Certificate Name                       CA
--------------------- -------------------------------------
--------------
node1                 -                                      Cluster-
1_Root_CA
node2                 -                                      Cluster-
1_Root_CA
node3                 google_issued_cert1                    Google_CA1
node4                 google_issued_cert2                    Google_CA1
```

클러스터의 각 노드에 대한 인증서 및 인증 기관(CA) 이름이 표시됩니다.

2. 노드의 클러스터 네트워크 암호화 인증서를 수정합니다.

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

이 명령은 특정 노드에 대한 클러스터 네트워크 암호화 인증서를 수정합니다. 이 명령을 실행하기 전에 인증서를 설치하고 설치된 CA에서 서명해야 합니다. 인증서 관리에 대한 자세한 내용은 다음을 참조하세요."System Manager를 사용하여 ONTAP 인증서를 관리합니다" . 만약에 `-name` 지정하지 않으면 자동 생성된 기본 인증서가 사용됩니다.

ONTAP 네트워크에서 LIF에 대한 방화벽 정책을 구성합니다

방화벽을 설정하면 클러스터의 보안이 강화되고 스토리지 시스템에 대한 무단 액세스가 방지됩니다. 기본적으로 온보드 방화벽은 데이터, 관리 및 인터클러스터 LIF에 대한 특정 IP 서비스 세트에 대한 원격 액세스를 허용하도록 구성됩니다.

ONTAP 9.10.1 시작:

- 방화벽 정책은 더 이상 사용되지 않으며 LIF 서비스 정책으로 교체됩니다. 이전에는 방화벽 정책을 사용하여 온보드 방화벽을 관리했습니다. 이 기능은 이제 LIF 서비스 정책을 사용하여 구현됩니다.
- 모든 방화벽 정책이 비어 있으며 기본 방화벽에서 포트를 열지 않습니다. 대신 LIF 서비스 정책을 사용하여 모든 포트를 열어야 합니다.
- 방화벽 정책에서 LIF 서비스 정책으로 전환하기 위해 9.10.1 이상으로 업그레이드한 후에는 작업이 필요하지

않습니다. 이전 ONTAP 릴리즈에서 사용 중인 방화벽 정책과 일치하는 LIF 서비스 정책이 자동으로 구성됩니다. 사용자 지정 방화벽 정책을 만들고 관리하는 스크립트나 기타 도구를 사용하는 경우 대신 해당 스크립트를 업그레이드하여 사용자 지정 서비스 정책을 만들어야 할 수 있습니다.

자세한 내용은 을 참조하십시오 "ONTAP 9.6 이상의 LIF 및 서비스 정책".

방화벽 정책을 사용하여 SSH, HTTP, HTTPS, Telnet, NTP 등의 관리 서비스 프로토콜에 대한 액세스를 제어할 수 있습니다. NDMP, NDMPS, RSH, DNS 또는 SNMP NFS 또는 SMB와 같은 데이터 프로토콜에 대해 방화벽 정책을 설정할 수 없습니다.

다음과 같은 방법으로 방화벽 서비스 및 정책을 관리할 수 있습니다.

- 방화벽 서비스 활성화 또는 비활성화
- 현재 방화벽 서비스 구성을 표시합니다
- 지정된 정책 이름 및 네트워크 서비스를 사용하여 새 방화벽 정책 생성
- 방화벽 정책을 논리 인터페이스에 적용합니다
- 기존 정책의 정확한 사본인 새 방화벽 정책을 생성합니다

  이를 사용하여 동일한 SVM 내에서 유사한 특성을 갖는 정책을 생성하거나 정책을 다른 SVM으로 복사할 수 있습니다.

- 방화벽 정책에 대한 정보 표시
- 방화벽 정책에서 사용하는 IP 주소 및 넷마스크 수정
- LIF에서 사용되지 않는 방화벽 정책을 삭제합니다

방화벽 정책 및 **LIF**

LIF 방화벽 정책을 사용하여 각 LIF에서 클러스터에 대한 액세스를 제한합니다. 기본 방화벽 정책이 각 LIF 유형에 대한 시스템 액세스에 미치는 영향과 LIF에 대한 보안을 늘리거나 줄일 수 있도록 방화벽 정책을 사용자 지정하는 방법을 이해해야 합니다.

또는 `network interface modify` 명령을 사용하여 LIF를 구성할 때 `network interface create` 매개 변수에 지정된 `-firewall-policy` 값에 따라 LIF에 대한 액세스가 허용된 서비스 프로토콜과 IP 주소가 결정됩니다. 에 대한 자세한 내용은 `network interface` "ONTAP 명령 참조입니다"을 참조하십시오.

대부분의 경우 기본 방화벽 정책 값을 적용할 수 있습니다. 다른 경우에는 특정 IP 주소 및 특정 관리 서비스 프로토콜에 대한 액세스를 제한해야 할 수도 있습니다. 사용 가능한 관리 서비스 프로토콜에는 SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS 및 SNMP를 지원합니다.

모든 클러스터 LIF의 방화벽 정책은 기본적으로 ""로 설정되며 수정할 수 없습니다.

다음 표에서는 LIF를 생성할 때 역할(ONTAP 9.5 이하) 또는 서비스 정책(ONTAP 9.6 이상)에 따라 각 LIF에 할당되는 기본 방화벽 정책을 설명합니다.

방화벽 정책	기본 서비스 프로토콜	기본 액세스	LIF가 에 적용되었습니다
관리	DNS, http, https, NDMP, ndmps, NTP, SNMP, ssh	모든 주소(0.0.0.0/0)	클러스터 관리, SVM 관리, 노드 관리 LIF

관리 - NFS	DNS, http, https, NDMP, ndmps, NTP, 포트 맵, SNMP, ssh	모든 주소(0.0.0.0/0)	데이터 LIF: SVM 관리 액세스도 지원합니다
인터클러스터	HTTPS, NDMP, ndmps	모든 주소(0.0.0.0/0)	모든 인터클러스터 LIF
데이터	DNS, NDMP, ndmps, portmap	모든 주소(0.0.0.0/0)	모든 데이터 LIF

portmap 서비스 구성

portmap 서비스는 RPC 서비스를 수신 대기 포트에 매핑합니다.

포트맵 서비스는 ONTAP 9.3 이전 버전에서 항상 액세스할 수 있었고 ONTAP 9.4에서 ONTAP 9.6까지 구성할 수 있었고 ONTAP 9.7부터 자동으로 관리됩니다.

- ONTAP 9.3 및 이전 버전에서는 타사 방화벽이 아닌 내장 ONTAP 방화벽에 의존하는 네트워크 구성의 포트 111에서 포트맵 서비스(rpcbind)에 항상 액세스할 수 있었습니다.
- ONTAP 9.4에서 ONTAP 9.6까지 방화벽 정책을 수정하여 특정 LIF에서 포트맵 서비스에 액세스할 수 있는지 여부를 제어할 수 있습니다.
- ONTAP 9.7부터 포트 맵 방화벽 서비스가 제거됩니다. 대신, NFS 서비스를 지원하는 모든 LIF에 대해 포트맵 포트가 자동으로 열립니다.
- Portmap 서비스는 ONTAP 9.4 ~ ONTAP 9.6 * 의 방화벽에서 구성할 수 있습니다

이 항목의 나머지 부분에서는 ONTAP 9.4에서 ONTAP 9.6 릴리스까지 포트맵 방화벽 서비스를 구성하는 방법을 설명합니다.

구성에 따라 특정 LIF 유형, 일반적으로 관리 및 인터클러스터 LIF에 대한 서비스에 대한 액세스를 허용하지 않을 수 있습니다. 경우에 따라 데이터 LIF에 대한 액세스를 허용하지 않을 수도 있습니다.

어떤 행동을 기대할 수 있습니까

ONTAP 9.4 ~ ONTAP 9.6 동작은 업그레이드 시 원활한 전환을 제공하도록 설계되었습니다. 특정 유형의 LIF에서 portmap 서비스에 이미 액세스하고 있는 경우 이러한 유형의 LIF에서 계속 액세스할 수 있습니다. ONTAP 9.3 이하 버전에서와 마찬가지로 LIF 유형에 대한 방화벽 정책에서 방화벽 내에서 액세스할 수 있는 서비스를 지정할 수 있습니다.

이 동작이 적용되려면 클러스터의 모든 노드에서 ONTAP 9.4~ONTAP 9.6을 실행해야 합니다. 인바운드 트래픽만 영향을 받습니다.

새로운 규칙은 다음과 같습니다.

- 릴리스 9.4 ~ 9.6으로 업그레이드할 때 ONTAP는 포트맵 서비스를 기존의 모든 방화벽 정책(기본값 또는 사용자 정의)에 추가합니다.
- 새 클러스터 또는 새 IPspace를 생성하는 경우 ONTAP는 기본 관리 또는 인터클러스터 정책이 아니라 기본 데이터 정책에만 포트맵 서비스를 추가합니다.
- 필요에 따라 포트맵 서비스를 기본 또는 사용자 지정 정책에 추가하고 필요에 따라 서비스를 제거할 수 있습니다.

포트맵 서비스를 추가하거나 제거하는 방법

포트맵 서비스를 SVM 또는 클러스터 방화벽 정책에 추가하려면(방화벽 내에서 액세스 가능) 다음을 입력합니다.

'시스템 서비스 방화벽 정책 생성 - vserver SVM-policy mgmt | 인터클러스터 | data | custom-service portmap'

SVM 또는 클러스터 방화벽 정책에서 portmap 서비스를 제거하려면(방화벽 내에서 액세스할 수 없도록 설정) 다음을 입력합니다.

'시스템 서비스 방화벽 정책 삭제 - vserver SVM-policy mgmt | 인터클러스터 | data | custom-service portmap

네트워크 인터페이스 수정 명령을 사용하여 기존 LIF에 방화벽 정책을 적용할 수 있습니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

방화벽 정책을 생성하여 **LIF**에 할당합니다

LIF를 생성할 때 각 LIF에 기본 방화벽 정책이 할당됩니다. 대부분의 경우 기본 방화벽 설정이 잘 작동하고 변경할 필요가 없습니다. LIF에 액세스할 수 있는 네트워크 서비스 또는 IP 주소를 변경하려면 사용자 지정 방화벽 정책을 생성하여 LIF에 할당할 수 있습니다.

이 작업에 대해

- 정책 이름 data, 클러스터 클러스터 클러스터 또는 mGMT로 방화벽 정책을 만들 수 없습니다.

  이러한 값은 시스템 정의 방화벽 정책용으로 예약되어 있습니다.

- 클러스터 LIF에 대한 방화벽 정책을 설정하거나 수정할 수 없습니다.

  클러스터 LIF의 방화벽 정책은 모든 서비스 유형에 대해 0.0.0.0/0 으로 설정됩니다.

- 정책에서 서비스를 제거해야 하는 경우 기존 방화벽 정책을 삭제하고 새 정책을 생성해야 합니다.
- 클러스터에 IPv6이 설정되어 있으면 IPv6 주소를 사용하여 방화벽 정책을 생성할 수 있습니다.

  IPv6을 사용하도록 설정한 후, "데이터", "인터클러스터" 및 "GMT" 방화벽 정책에는 IPv6 와일드카드인 /0이 허용된 주소 목록에 포함됩니다.

- System Manager를 사용하여 클러스터 간에 데이터 보호 기능을 구성하는 경우 LIF IP 주소가 허용 목록에 포함되어 있고 인터클러스터 LIF와 회사 소유 방화벽 모두에 HTTPS 서비스가 허용되는지 확인해야 합니다.

  기본적으로 '인터클러스터' 방화벽 정책은 모든 IP 주소(IPv6의 경우 0.0.0.0/0 또는:/0)의 액세스를 허용하고 HTTPS, NDMP 및 NDMPS 서비스를 활성화합니다. 이 기본 정책을 수정하거나 인터클러스터 LIF에 대한 자체 방화벽 정책을 만드는 경우 각 인터클러스터 LIF IP 주소를 허용된 목록에 추가하고 HTTPS 서비스를 활성화해야 합니다.

- ONTAP 9.6부터는 HTTPS 및 SSH 방화벽 서비스가 지원되지 않습니다.

  ONTAP 9.6에서는 HTTPS 및 SSH 관리 액세스를 위해 관리 https와 관리 ssh LIF 서비스를 사용할 수 있습니다.

단계

1. 특정 SVM의 LIF에서 사용할 수 있는 방화벽 정책을 생성합니다.

   '시스템 서비스 방화벽 정책 생성 - vserver_vserver_name_-policy_policy_name_-service_network_service_-allow-list_ip_address/mask_'

이 명령을 여러 번 사용하여 방화벽 정책에서 각 서비스에 대해 둘 이상의 네트워크 서비스 및 허용된 IP 주소 목록을 추가할 수 있습니다.

2. System services firewall policy show 명령을 사용하여 정책이 올바르게 추가되었는지 확인합니다.
3. 방화벽 정책을 LIF에 적용합니다.

   'network interface modify -vserver_vserver_name_-lif_lif_name_-firewall-policy_policy_name_'

4. 'network interface show-fields firewall -policy' 명령을 사용하여 LIF에 정책이 올바르게 추가되었는지 확인합니다.

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

방화벽 정책을 생성하여 **LIF**에 할당하는 예입니다

다음 명령을 실행하면 10.10 서브넷의 IP 주소에서 HTTP 및 HTTPS 프로토콜 액세스를 지원하는 data_http라는 방화벽 정책이 생성되어 SVM VS1의 data1이라는 LIF에 해당 정책이 적용되고 클러스터의 모든 방화벽 정책이 표시됩니다.

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

방화벽 서비스 및 정책을 관리하는 **ONTAP** 명령

'system services firewall' 명령어를 이용하여 방화벽 서비스를 관리하고, 'system services firewall policy' 명령을 이용하여 방화벽 정책을 관리하고, 'network interface modify' 명령을 사용하여 LIF의 방화벽 설정을 관리할 수 있다.

ONTAP 9.10.1 시작:

- 방화벽 정책은 더 이상 사용되지 않으며 LIF 서비스 정책으로 교체됩니다. 이전에는 방화벽 정책을 사용하여 온보드 방화벽을 관리했습니다. 이 기능은 이제 LIF 서비스 정책을 사용하여 구현됩니다.
- 모든 방화벽 정책이 비어 있으며 기본 방화벽에서 포트를 열지 않습니다. 대신 LIF 서비스 정책을 사용하여 모든 포트를 열어야 합니다.
- 방화벽 정책에서 LIF 서비스 정책으로 전환하기 위해 9.10.1 이상으로 업그레이드한 후에는 작업이 필요하지 않습니다. 이전 ONTAP 릴리즈에서 사용 중인 방화벽 정책과 일치하는 LIF 서비스 정책이 자동으로 구성됩니다. 사용자 지정 방화벽 정책을 만들고 관리하는 스크립트나 기타 도구를 사용하는 경우 대신 해당 스크립트를 업그레이드하여 사용자 지정 서비스 정책을 만들어야 할 수 있습니다.

자세한 내용은 을 참조하십시오 "ONTAP 9.6 이상의 LIF 및 서비스 정책".

원하는 작업	이 명령 사용…
방화벽 서비스를 활성화 또는 비활성화합니다	시스템 서비스 방화벽 수정
방화벽 서비스의 현재 구성을 표시합니다	'시스템 서비스 방화벽 쇼'
방화벽 정책을 생성하거나 기존 방화벽 정책에 서비스를 추가합니다	'시스템 서비스 방화벽 정책 생성
LIF에 방화벽 정책을 적용합니다	네트워크 인터페이스 수정-lif lifname-firewall-policy
방화벽 정책과 연결된 IP 주소 및 넷마스크를 수정합니다	시스템 서비스 방화벽 정책 수정
방화벽 정책에 대한 정보를 표시합니다	'시스템 서비스 방화벽 정책 표시
기존 정책의 정확한 사본인 새 방화벽 정책을 생성합니다	'시스템 서비스 방화벽 정책 클론
LIF에서 사용되지 않는 방화벽 정책을 삭제합니다	'시스템 서비스 방화벽 정책 삭제

관련 정보

- "시스템 서비스 방화벽"
- "네트워크 인터페이스 수정"

QoS 표시(클러스터 관리자만 해당)

ONTAP 네트워크 QoS(Quality of Service)에 대해 알아보기

네트워크 서비스 품질(QoS) 표시를 사용하면 네트워크 상태에 따라 서로 다른 트래픽 유형의 우선 순위를 지정하여 네트워크 리소스를 효과적으로 사용할 수 있습니다. IPspace별로 지원되는 트래픽 유형에 대해 나가는 IP 패킷의 DSCP(Differentiated Services Code Point) 값을 설정할 수 있다.

UC 규정 준수를 위한 DSCP 표시

기본 또는 사용자가 제공한 DSCP 코드를 사용하여 지정된 프로토콜에 대해 발신(송신) IP 패킷 트래픽에 DSCP(Differentiated Services Code Point) 표시를 활성화할 수 있습니다. DSCP 마킹은 네트워크 트래픽을 분류 및 관리하는 메커니즘으로 통합 기능(UC) 규정 준수의 구성 요소입니다.

IPspace, Protocol, DSCP 값을 제공하여 DSCP marking(*Qos marking_or_quality of service marking* 이라고도 함)을 설정할 수 있다. DSCP 마킹을 적용할 수 있는 프로토콜은 NFS, SMB, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet 및 SNMP를 지원합니다.

해당 프로토콜에 대해 DSCP marking을 설정할 때 DSCP 값을 제공하지 않으면 default를 사용한다.

- 데이터 프로토콜/트래픽의 기본값은 0x0A(10)입니다.
- 제어 프로토콜/트래픽의 기본값은 0x30(48)입니다.

ONTAP 네트워크 QoS 표시 값을 수정합니다

IPspace별로 다양한 프로토콜에 대한 QoS(서비스 품질) 표시 값을 수정할 수 있습니다.

시작하기 전에

클러스터의 모든 노드에서 동일한 버전의 ONTAP를 실행해야 합니다.

단계

network QoS-marking modify 명령을 사용하여 QoS marking 값을 수정한다.

- '–IPSpace' 매개변수는 QoS 마킹 항목을 수정할 IPspace를 지정합니다.
- `–protocol`매개 변수는 QoS 표시 항목을 수정할 프로토콜을 지정합니다.
- '–DSCP' 파라미터는 DSCP(Differentiated Services Code Point) 값을 지정한다. 가능한 값의 범위는 0 ~ 63입니다.
- '-is-enabled' 매개 변수는 '–IPSpace' 매개 변수에서 제공하는 IPspace에서 지정된 프로토콜에 대한 QoS 마킹을 활성화 또는 비활성화하는 데 사용됩니다.

다음 명령을 실행하면 기본 IPspace에서 NFS 프로토콜에 대한 QoS 마킹이 설정됩니다.

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

다음 명령을 실행하면 기본 IPspace에서 NFS 프로토콜에 대한 DSCP 값이 20으로 설정됩니다.

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

에서 프로토콜의 가능한 값과 에 대해 자세히 `network qos-marking modify`"ONTAP 명령 참조입니다" 알아보십시오.

ONTAP 네트워크 QoS 표시 값을 확인합니다

IPspace별로 다양한 프로토콜에 대한 QoS 표시 값을 표시할 수 있습니다.

단계

'network QoS-marking show' 명령어를 이용하여 QoS marking 값을 출력한다.

다음 명령을 실행하면 기본 IPspace의 모든 프로토콜에 대한 QoS 마킹이 표시됩니다.

```
network qos-marking show -ipspace Default
IPspace              Protocol            DSCP  Enabled?
-------------------- ----------------- -----  --------
Default
                     CIFS                  10  false
                     FTP                   48  false
                     HTTP-admin            48  false
                     HTTP-filesrv          10  false
                     NDMP                  10  false
                     NFS                   10  true
                     SNMP                  48  false
                     SSH                   48  false
                     SnapMirror            10  false
                     Telnet                48  false
                     iSCSI                 10  false
11 entries were displayed.
```

에 대한 자세한 내용은 `network qos-marking show` "ONTAP 명령 참조입니다"을 참조하십시오.

SNMP 관리(클러스터 관리자만 해당)

ONTAP 네트워크의 SNMP에 대해 알아봅니다

문제가 발생하기 전에 이를 방지하고 문제가 발생할 경우 대응하도록 SNMP를 클러스터의 SVM을 모니터링할 수 있습니다. SNMP를 관리하려면 SNMP 사용자를 구성하고 모든 SNMP 이벤트에 대해 SNMP 트라프호스트 대상(관리 워크스테이션)을 구성해야 합니다. 데이터 LIF에서 SNMP는 기본적으로 해제되어 있습니다.

데이터 SVM에서 읽기 전용 SNMP 사용자를 생성하고 관리할 수 있습니다. SVM에서 SNMP 요청을 받도록 데이터 LIF를 구성해야 합니다.

SNMP 네트워크 관리 워크스테이션 또는 관리자는 SVM SNMP 에이전트에 정보를 쿼리할 수 있습니다. SNMP 에이전트는 정보를 수집하여 SNMP 관리자에게 전달합니다. SNMP 에이전트는 또한 특정 이벤트가 발생할 때마다 트랩 알림을 생성합니다. SVM의 SNMP 에이전트는 읽기 전용 권한을 가지고 있으며 설정된 작업에 사용하거나 트랩에 대한 응답으로 수정 조치를 취하는 데 사용할 수 없습니다. ONTAP는 SNMP 버전 v1, v2c 및 v3과 호환되는 SNMP 에이전트를 제공합니다. SNMPv3는 암호 구문 및 암호화를 사용하여 고급 보안을 제공합니다.

ONTAP 시스템의 SNMP 지원에 대한 자세한 내용은 를 참조하십시오 "TR-4220: Data ONTAP에서 SNMP 지원".

MIB 개요

MIB(Management Information Base)는 SNMP 객체 및 트랩을 설명하는 텍스트 파일입니다.

MIB는 스토리지 시스템의 관리 데이터 구조를 설명하며 OID(객체 식별자)가 포함된 계층적 네임스페이스를 사용합니다. 각 OID는 SNMP를 사용하여 읽을 수 있는 변수를 식별합니다.

MIB는 구성 파일이 아니며 ONTAP는 이러한 파일을 읽지 않기 때문에 MIB 기능은 MIB의 영향을 받지 않습니다. ONTAP는 다음과 같은 MIB 파일을 제공합니다.

- NetApp 맞춤형 MIB('NetApp.MIB')

ONTAP는 IPv6(RFC 2465), TCP(RFC 4022), UDP(RFC 4113) 및 IPv4 및 IPv6 데이터를 모두 표시하는 ICMP(RFC 2466) MIB를 지원합니다.

또한 ONTAP는 "trap.dat" 파일에서 OID(개체 식별자)와 개체 약식 이름 간의 짧은 상호 참조를 제공합니다.

ONTAP MIB 및 traps.dat 파일의 최신 버전은 NetApp Support 사이트에서 확인할 수 있습니다. 그러나 지원 사이트에 있는 이러한 파일의 버전이 ONTAP 버전의 SNMP 기능과 일치하지 않을 수도 있습니다. 이러한 파일은 최신 ONTAP 버전에서 SNMP 기능을 평가하는 데 도움이 됩니다.

SNMP 트랩

SNMP 트랩은 SNMP 에이전트에서 SNMP 관리자로 보내는 비동기 알림으로 전송되는 시스템 모니터링 정보를 캡처합니다.

SNMP 트랩에는 표준, 기본 제공 및 사용자 정의 세 가지 유형이 있습니다. 사용자 정의 트랩은 ONTAP에서 지원되지 않습니다.

트랩을 사용하여 MIB에 정의된 작동 임계값 또는 오류를 정기적으로 확인할 수 있습니다. 임계값에 도달하거나 장애가 감지되면 SNMP 에이전트는 해당 이벤트를 알리는 메시지(트랩)를 Traphosts에 보냅니다.

ONTAP는 SNMPv1 및 SNMPv3 트랩을 지원합니다. ONTAP는 SNMPv2c 트랩 및 정보를 지원하지 않습니다.

표준 SNMP 트랩

이러한 트랩은 RFC 1215에 정의되어 있습니다. ONTAP에서 지원하는 5개의 표준 SNMP 트랩은 coldstart, 웜스타트, Linkdown, Linkup 및 authenticationFailure입니다.

authenticationFailure 트랩은 기본적으로 해제되어 있습니다. 명령을 사용하여 트랩을 활성화해야 `system snmp authtrap` 합니다. 에 대한 자세한 내용은 `system snmp authtrap` "ONTAP 명령 참조입니다"을 참조하십시오.

기본 제공 SNMP 트랩

내장 트랩은 ONTAP에서 미리 정의되며 이벤트가 발생하면 Traphost 목록의 네트워크 관리 스테이션으로 자동으로 전송됩니다. diskFailedShutdown, cpuTooBusy 및 volumeNearlyFull과 같은 이러한 트랩은 사용자 지정 MIB에 정의되어 있습니다.

각 내장 트랩은 고유한 트랩 코드로 식별됩니다.

ONTAP 네트워크용 SNMP 커뮤니티를 생성합니다

SNMPv1 및 SNMPv2c를 사용할 때 관리 스테이션과 SVM(스토리지 가상 머신) 간의 인증 메커니즘 역할을 하는 SNMP 커뮤니티를 생성할 수 있습니다.

데이터 SVM에서 SNMP 커뮤니티를 생성하여 데이터 LIF에서 'snmpwalk', 'snmpget' 등의 명령을 실행할 수 있습니다.

이 작업에 대해

- ONTAP를 새로 설치하면 SNMPv1 및 SNMPv2c가 기본적으로 비활성화됩니다.

  SNMP 커뮤니티를 생성한 후에는 SNMPv1 및 SNMPv2c가 활성화됩니다.

- ONTAP는 읽기 전용 커뮤니티를 지원합니다.
- 기본적으로 데이터 LIF에 할당되는 "데이터" 방화벽 정책은 SNMP 서비스를 "설정"으로 설정합니다.

  데이터 SVM용 SNMP 사용자를 생성할 때 SNMP 서비스 세트가 "허용"인 새 방화벽 정책을 생성해야 합니다.

  ⓘ ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 참조하십시오 "LIF의 방화벽 정책을 구성합니다".

- 관리 SVM과 데이터 SVM 모두에 대해 SNMPv1 및 SNMPv2c 사용자를 위한 SNMP 커뮤니티를 생성할 수 있습니다.
- SVM은 SNMP 표준의 일부가 아니므로 데이터 LIF에 대한 쿼리에는 'smpwalk-v 2c-c snmpNFS 10.238.19.14 1.3.6.1.4.1.789'와 같은 NetApp 루트 OID(1.3.6.1.4.1.789)가 포함되어야 합니다.

단계

1. '시스템 SNMP community add' 명령어를 사용하여 SNMP community를 생성한다. 다음 명령을 실행하면 관리 SVM 클러스터-1에서 SNMP 커뮤니티를 생성하는 방법이 표시됩니다.

   ```
   system snmp community add -type ro -community-name comty1 -vserver
   cluster-1
   ```

   다음 명령을 실행하면 SVM VS1 데이터에 SNMP 커뮤니티를 생성하는 방법이 표시됩니다.

   ```
   system snmp community add -type ro -community-name comty2 -vserver vs1
   ```

2. system snmp community show 명령을 사용하여 커뮤니티가 생성되었는지 확인합니다.

다음 명령을 실행하면 SNMPv1 및 SNMPv2c에 대해 생성된 두 개의 커뮤니티가 표시됩니다.

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. System services firewall policy’show' 명령어를 이용하여 "data" 방화벽 정책에서 SNMP를 서비스로 허용할 수 있는지 확인한다.

   다음 명령을 실행하면 기본 "데이터" 방화벽 정책에서 SNMP 서비스가 허용되지 않습니다(SNMP 서비스는 "관리" 방화벽 정책에서만 허용됨).

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. '시스템 서비스 방화벽 정책 생성' 명령을 사용하여 'NMP' 서비스를 사용하여 액세스할 수 있는 새 방화벽 정책을 만듭니다.

   다음 명령을 실행하면 'data1’이라는 새 데이터 방화벽 정책이 생성되어 'snmp’를 사용할 수 있습니다

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. 명령을 -firewall-policy 매개 변수와 함께 사용하여 데이터 LIF에 방화벽 정책을 `network interface modify` 적용합니다.

   다음 명령을 실행하면 새 "data1" 방화벽 정책이 LIF "datalif1"에 할당됩니다.

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

   에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 클러스터에서 SNMPv3 사용자를 구성합니다

SNMPv3는 SNMPv1 및 SNMPv2c와 비교할 때 보안 프로토콜입니다. SNMPv3을 사용하려면 SNMP 관리자에서 SNMP 유틸리티를 실행하도록 SNMPv3 사용자를 구성해야 합니다.

단계

사용하세요 `security login create` SNMPv3 사용자를 생성하는 명령입니다.

다음 정보를 제공하라는 메시지가 표시됩니다.

- 엔진 ID: 기본값과 권장 값은 로컬 엔진 ID입니다
- 인증 프로토콜
- 인증 암호입니다
- 개인 정보 보호 프로토콜
- 개인 정보 프로토콜 암호

결과

SNMPv3 사용자는 사용자 이름 및 암호를 사용하여 SNMP 관리자에서 로그인하고 SNMP 유틸리티 명령을 실행할 수 있습니다.

SNMPv3 보안 매개 변수

SNMPv3에는 사용자가 명령을 호출할 때 이름, 인증 프로토콜, 인증 키 및 원하는 보안 수준을 입력해야 하는 인증 기능이 포함되어 있습니다.

다음 표에는 SNMPv3 보안 매개 변수가 나열되어 있습니다.

매개 변수	명령줄 옵션입니다	설명
엔진 ID	-e 엔지니어링 ID	SNMP 에이전트의 엔진 ID입니다. 기본값은 Local EngineID(권장)입니다.
보안 이름	-u 이름	사용자 이름은 32자를 초과할 수 없습니다.
authProtocol의 약어입니다	-a {none	MD5
SHA	SHA-256}	인증 유형은 없음, MD5, SHA 또는 SHA-256일 수 있습니다.
인증 키	• 암호문	최소 8자의 암호 구문
보안 수준	-l {authNo암호화	Auth암호화
noAuthNo암호화}	보안 수준은 인증, 개인 정보 보호 없음, 인증, 개인 정보 보호 또는 인증 없음일 수 있습니다. 개인 정보 보호.	개인 프로토콜
-x{none	des	aes128}
개인 정보 보호 프로토콜은 없음, des 또는 aes128일 수 있습니다	privPassword(비밀 번호)	-X 암호

다양한 보안 수준에 대한 예

이 예에서는 서로 다른 보안 수준으로 생성된 SNMPv3 사용자가 'snmpwalk'와 같은 SNMP 클라이언트 측 명령을 사용하여 클러스터 객체를 쿼리하는 방법을 보여 줍니다.

성능을 향상시키려면 테이블에서 단일 개체나 몇 개의 개체를 검색하는 대신 테이블의 모든 개체를 검색해야 합니다.

인증 프로토콜이 SHA 인 경우 'snmpwalk' 5.3.1 이상을 사용해야 합니다.

보안 수준**: auth**암호화

다음 출력에서는 auth암호화 보안 수준으로 SNMPv3 사용자를 생성하는 방법을 보여 줍니다.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

FIPS 모드

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

snmpwalk 테스트

다음 출력에서는 snmpwalk 명령을 실행하는 SNMPv3 사용자를 보여 줍니다.

성능을 향상시키려면 테이블에서 단일 개체나 몇 개의 개체를 검색하는 대신 테이블의 모든 개체를 검색해야 합니다.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

보안 수준: **authNo**암호화

다음 출력에서는 authNo암호화 보안 수준으로 SNMPv3 사용자를 생성하는 방법을 보여 줍니다.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

FIPS 모드

FIPS에서는 개인 정보 프로토콜에 대해 * 없음 * 을 선택할 수 없습니다. 따라서 FIPS 모드에서 authNoSNMPv3 사용자를 구성할 수 없습니다.

snmpwalk 테스트

다음 출력에서는 snmpwalk 명령을 실행하는 SNMPv3 사용자를 보여 줍니다.

성능을 향상시키려면 테이블에서 단일 개체나 몇 개의 개체를 검색하는 대신 테이블의 모든 개체를 검색해야 합니다.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

보안 수준**: noAuthNo**암호화

다음 출력에서는 NOAuthNo암호화 보안 수준으로 SNMPv3 사용자를 생성하는 방법을 보여 줍니다.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

FIPS 모드

FIPS에서는 개인 정보 프로토콜에 대해 * 없음 * 을 선택할 수 없습니다.

snmpwalk 테스트

다음 출력에서는 snmpwalk 명령을 실행하는 SNMPv3 사용자를 보여 줍니다.

성능을 향상시키려면 테이블에서 단일 개체나 몇 개의 개체를 검색하는 대신 테이블의 모든 개체를 검색해야 합니다.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크에서 SNMP용 traphosts를 구성합니다

클러스터에서 SNMP 트랩이 생성될 때 알림(SNMP 트랩 PDU)을 받도록 Traphost(SNMP 관리자)를 구성할 수 있습니다. SNMP traphost의 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)를 지정할 수 있습니다.

시작하기 전에

- 클러스터에서 SNMP 및 SNMP 트랩을 활성화해야 합니다.

  SNMP 및 SNMP 트랩은 기본적으로 사용하도록 설정됩니다.

- traphost 이름을 확인하기 위해 클러스터에서 DNS를 구성해야 합니다.
- IPv6 주소를 사용하여 SNMP traaphosts를 구성하려면 클러스터에서 IPv6을 활성화해야 합니다.
- traphost를 생성할 때 미리 정의된 USM(사용자 기반 보안 모델) 인증 및 개인 정보 보호 자격 증명을 지정해야 합니다.

단계

SNMP traaphost 추가:

```
system snmp traphost add
```

트랩은 하나 이상의 SNMP 관리 스테이션이 트랩 호스트로 지정된 경우에만 보낼 수 있습니다.

다음 명령을 실행하면 알려진 USM 사용자와 함께 yyy.example.com 이라는 새로운 SNMPv3 traphost가 추가됩니다.

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

다음 명령을 실행하면 호스트의 IPv6 주소를 사용하는 traphost가 추가됩니다.

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

ONTAP 클러스터에서 SNMP 폴링을 확인합니다

SNMP를 구성한 후에는 클러스터를 폴링할 수 있는지 확인해야 합니다.

이 작업에 대해

클러스터를 폴링하려면 과 같은 타사 명령을 사용해야 합니다 `snmpwalk`.

단계

1. SNMP 명령을 전송하여 다른 클러스터에서 클러스터를 폴링합니다.

   SNMPv1을 실행하는 시스템의 경우 CLI 명령을 사용합니다 `snmpwalk -v version -c community_stringip_address_or_host_name system` MIB(Management Information Base)의 내용을 검색합니다.

   이 예제에서 폴링할 클러스터 관리 LIF의 IP 주소는 10.11.12.123입니다. 명령은 MIB에서 요청된 정보를 표시합니다.

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

   SNMPv2c를 실행하는 시스템의 경우 CLI 명령을 사용합니다 `snmpwalk -v version -c community_stringip_address_or_host_name system` MIB(Management Information Base)의 내용을 검색합니다.

   이 예제에서 폴링할 클러스터 관리 LIF의 IP 주소는 10.11.12.123입니다. 명령은 MIB에서 요청된 정보를 표시합니다.

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

SNMPv3를 실행하는 시스템의 경우 CLI 명령을 사용합니다 `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` MIB(Management Information Base)의 내용을 검색합니다.

이 예제에서 폴링할 클러스터 관리 LIF의 IP 주소는 10.11.12.123입니다. 명령은 MIB에서 요청된 정보를 표시합니다.

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

SNMP, 트랩 및 traphost를 관리하는 ONTAP 명령입니다

'시스템 SNMP' 명령어를 이용하여 SNMP, 트랩, Traphosts를 관리할 수 있다. SVM별로 SNMP 사용자를 관리하기 위해 '보안' 명령을 사용할 수 있다. 이벤트 명령을 사용하여 SNMP 트랩과 관련된 이벤트를 관리할 수 있습니다.

SNMP를 구성하는 명령입니다

원하는 작업	이 명령 사용…

클러스터에서 SNMP를 설정합니다	'options-option-name snmp.enable-option-value on’입니다 관리(관리) 방화벽 정책에서 SNMP 서비스를 허용해야 합니다. 시스템 서비스 방화벽 policy show 명령을 사용하여 SNMP가 허용되는지 여부를 확인할 수 있습니다.
클러스터에서 SNMP를 해제합니다	'options-option-name snmp.enable-option-value off'

SNMP v1, v2c 및 **v3** 사용자를 관리하는 명령입니다

원하는 작업	이 명령 사용…
SNMP 사용자를 구성합니다	'보안 로그인 생성'
SNMP 사용자를 표시합니다	`security snmpusers`그리고 `security login show -application snmp`
SNMP 사용자를 삭제합니다	'보안 로그인 삭제
SNMP 사용자에 대한 로그인 방법의 액세스 제어 역할 이름을 수정합니다	보안 로그인 수정

연락처 및 위치 정보를 제공하는 명령입니다

원하는 작업	이 명령 사용…
클러스터의 연락처 정보를 표시하거나 수정합니다	'시스템 SNMP 연락처'
클러스터의 위치 세부 정보를 표시하거나 수정합니다	'시스템 SNMP 위치'

SNMP 커뮤니티 관리를 위한 명령입니다

원하는 작업	이 명령 사용…
SVM이나 클러스터의 모든 SVM에 대해 읽기 전용(ro) 커뮤니티를 추가할 수 있습니다	'시스템 SNMP 커뮤니티 추가'
커뮤니티 또는 모든 커뮤니티를 삭제합니다	시스템 SNMP community delete
모든 커뮤니티 목록을 표시합니다	'시스템 SNMP 커뮤니티 쇼'

SVM은 SNMP 표준의 일부가 아니므로 데이터 LIF에 대한 쿼리에는 'snmpwalk-v 2c-c snmpNFS 10.238.19.14 1.3.6.1.4.1.789’와 같은 NetApp 루트 OID(1.3.6.1.4.1.789)가 포함되어야 합니다.

SNMP 옵션 값을 표시하는 명령입니다

원하는 작업	이 명령 사용…
클러스터 연락처, 연락처 위치, 클러스터가 트랩을 전송하도록 구성되었는지 여부, 트랩 목록, 커뮤니티 및 액세스 제어 유형 목록을 포함한 모든 SNMP 옵션의 현재 값을 표시합니다	'시스템 SNMP 쇼'

SNMP 트랩 및 트랩 호스트를 관리하는 명령입니다

원하는 작업	이 명령 사용…
클러스터에서 보낸 SNMP 트랩을 설정합니다	'시스템 SNMP init-init 1'
클러스터에서 보낸 SNMP 트랩을 해제합니다	'시스템 SNMP init-init 0'
클러스터의 특정 이벤트에 대해 SNMP 알림을 수신하는 Traphost를 추가합니다	'시스템 SNMP traaphost add'
traphost를 삭제합니다	'시스템 SNMP traaphost delete
Traphosts 목록을 표시합니다	'시스템 SNMP traaphost show'

SNMP 트랩과 관련된 이벤트를 관리하는 명령입니다

원하는 작업	이 명령 사용…
SNMP 트랩(기본 제공)이 생성되는 이벤트를 표시합니다	이벤트 루트쇼 SNMP 관련 이벤트만 보려면 '-snmp-support true' 매개변수를 사용하십시오. 'instance-messagename<message>' 매개 변수를 사용하여 이벤트가 발생한 이유와 수정 조치에 대해 자세히 설명합니다. 개별 SNMP 트랩 이벤트를 특정 트랩 호스트 대상으로 라우팅하는 것은 지원되지 않습니다. 모든 SNMP 트랩 이벤트가 모든 트랩 호스트 대상으로 전송됩니다.
SNMP 트랩으로 전송된 이벤트 알림인 SNMP 트랩 기록 레코드 목록을 표시합니다	이벤트 스내피스토리 쇼
SNMP 트랩 기록 레코드를 삭제합니다	이벤트 스내피스토리 삭제

관련 정보

- "시스템 SNMP"
- "보안 snmpusers"
- "보안"
- "이벤트"
- "보안 로그인"

SVM에서 라우팅 관리

ONTAP 네트워크에서의 SVM 라우팅에 대해 알아보십시오

SVM을 위한 라우팅 테이블은 SVM이 대상과 통신하는 데 사용하는 네트워크 경로를 결정합니다. 라우팅 테이블이 작동하는 방식을 이해하여 네트워크 문제가 발생하기 전에 이를 방지하는 것이 중요합니다.

라우팅 규칙은 다음과 같습니다.

- ONTAP는 가장 구체적인 사용 가능한 경로를 통해 트래픽을 라우팅합니다.
- ONTAP는 더 구체적인 경로를 사용할 수 없는 경우 기본 게이트웨이 경로(넷마스크 0비트)를 통해 트래픽을 마지막 수단으로 라우팅합니다.

동일한 대상, 넷마스크 및 메트릭이 있는 라우트의 경우, 재부팅 후 또는 업그레이드 후에 시스템이 동일한 경로를 사용할 것이라는 보장은 없습니다. 이는 여러 기본 경로를 구성한 경우 특히 문제가 됩니다.

SVM에 대해서는 기본 경로를 하나만 구성하는 것이 가장 좋습니다. 중단을 방지하려면 기본 경로가 보다 구체적인 경로로는 도달할 수 없는 모든 네트워크 주소에 도달할 수 있는지 확인해야 합니다. 자세한 내용은 다음을 참조하세요 ."NetApp 기술 자료: SU134 - 클러스터형 ONTAP 에서 잘못된 라우팅 구성으로 인해 네트워크 액세스가 중단될 수 있음"

ONTAP 네트워크에 대한 정적 라우트를 생성합니다

SVM(Storage Virtual Machine) 내에서 정적 경로를 생성하여 LIF가 아웃바운드 트래픽에 네트워크를 사용하는 방법을 제어할 수 있습니다.

SVM과 관련된 경로 항목을 생성하면 해당 경로가 지정된 SVM이 소유하고 게이트웨이와 동일한 서브넷에 있는 모든 LIF에서 사용됩니다.

단계

'network route create' 명령어를 이용하여 경로를 생성한다.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

에 대한 자세한 내용은 `network route create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크에 대해 다중 경로 라우팅을 활성화합니다

여러 루트가 목적지에 대해 동일한 메트릭을 가지고 있는 경우, 나가는 트래픽에 대해 하나의 라우트만 선택됩니다. 이로 인해 다른 라우트가 발신 트래픽을 전송하는 데 사용되지 않습니다. 동일한 메트릭의 사용 가능한 라우트에 걸쳐 로드 밸런싱을 수행하는 ECMP 라우팅과 달리, 다중 경로 라우팅을 활성화하여 사용 가능한 모든 라우트에 대한 로드 밸런싱을 수행할 수 있습니다.

단계

1. 고급 권한 레벨에 로그인합니다.

   세트 프리빌리지 고급

2. 다중 경로 라우팅 활성화:

   '네트워크 옵션 다중 경로 라우팅 수정 - 활성화 true'

   클러스터의 모든 노드에 대해 다중 경로 라우팅이 활성화됩니다.

   ```
   network options multipath-routing modify -is-enabled true
   ```

   에 대한 자세한 내용은 `network options multipath-routing modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크에서 정적 라우트를 삭제합니다

SVM(스토리지 가상 머신)에서 불필요한 정적 경로를 삭제할 수 있습니다.

단계

정적 라우트를 삭제하려면 network route delete 명령을 사용한다.

다음 예제에서는 게이트웨이 10.63.0.1 및 대상 IP 주소가 0.0.0.0/0인 SVM vs0과 연관된 정적 경로를 삭제합니다.

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

에 대한 자세한 내용은 `network route delete` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 라우팅 정보를 봅니다

클러스터의 각 SVM에 대한 라우팅 구성 정보를 표시할 수 있습니다. 이를 통해 클라이언트 애플리케이션 또는 서비스 간 연결 문제와 클러스터의 노드 LIF 간 연결 문제를 진단할 수 있습니다.

단계

1. "network route show" 명령을 사용하여 하나 이상의 SVM 내에 경로를 표시합니다. 다음 예는 vs0 SVM에 구성된

경로를 보여줍니다.

```
network route show
  (network route show)
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
vs0
                    0.0.0.0/0       172.17.178.1    20
```

2. "network route show -lifs" 명령을 사용하여 하나 이상의 SVM 내에 있는 경로 및 LIF의 연결을 표시합니다.

   다음 예에서는 vs0 SVM이 소유하는 라우트가 있는 LIF를 보여 줍니다.

```
network route show-lifs
  (network route show-lifs)

Vserver: vs0
Destination             Gateway                 Logical Interfaces
----------------------  --------------          --------------------
0.0.0.0/0               172.17.178.1            cluster_mgmt,
                                                LIF-b-01_mgmt1,
                                                LIF-b-02_mgmt1
```

   및 `network route show-lifs` 에 대한 자세한 `network route show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

3. "network route active-entry show" 명령을 사용하여 하나 이상의 노드, SVM, 서브넷 또는 지정된 목적지를 가진 경로에 설치된 경로를 표시할 수 있습니다.

   다음 예는 특정 SVM에 설치된 모든 경로를 보여줍니다.

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
```

```
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC
fd20:8b1e:b255:814e::1  link#4               e0d              0  UHL
11 entries were displayed.
```

에 대한 자세한 내용은 `network route active-entry show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크의 라우팅 테이블에서 동적 라우트를 제거합니다

IPv4 및 IPv6에 대한 ICMP redirect를 수신하면, 동적 route를 라우팅 테이블에 추가한다. 기본적으로 동적 루트는 300초 후에 제거됩니다. 동적 경로를 다른 시간 동안 유지하려면 시간 초과 값을 변경할 수 있습니다.

이 작업에 대해

시간 초과 값은 0에서 65,535초로 설정할 수 있습니다. 값을 0으로 설정하면 루트가 만료되지 않습니다. 동적 경로를 제거하면 잘못된 경로의 지속성으로 인한 연결 손실을 방지할 수 있습니다.

단계

1. 현재 시간 초과 값을 표시합니다.
   - IPv4의 경우:

```
network tuning icmp show
```

   - IPv6의 경우:

```
network tuning icmp6 show
```

2. 시간 초과 값을 수정합니다.
   - IPv4의 경우:

```
network tuning icmp modify -node node_name -redirect-timeout
timeout_value
```

   - IPv6의 경우:

```
network tuning icmp6 modify -node node_name -redirect-v6-timeout
timeout_value
```

3. 시간 초과 값이 올바르게 수정되었는지 확인합니다.
   - IPv4의 경우:

```
network tuning icmp show
```

   - IPv6의 경우:

```
network tuning icmp6 show
```

에 대한 자세한 내용은 `network tuning icmp` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크 정보

ONTAP 네트워크 정보를 봅니다

CLI를 사용하면 포트, LIF, 경로, 페일오버 규칙, 페일오버 그룹과 관련된 정보를 방화벽 규칙, DNS, NIS 및 연결 ONTAP 9.8부터 System Manager에 표시되는 네트워크 관련 데이터를

다운로드할 수도 있습니다.

이 정보는 네트워킹 설정을 재구성하거나 클러스터 문제를 해결하는 데 유용할 수 있습니다.

클러스터 관리자는 사용 가능한 모든 네트워킹 정보를 볼 수 있습니다. SVM 관리자는 할당된 SVM과 관련된 정보만 볼 수 있습니다.

System Manager에서 _ 목록 보기 _ 에 정보를 표시할 때 * 다운로드 * 를 클릭하면 표시되는 개체 목록이 다운로드됩니다.

- 목록은 CSV(쉼표로 구분된 값) 형식으로 다운로드됩니다.
- 표시된 열의 데이터만 다운로드됩니다.
- CSV 파일 이름의 형식은 개체 이름과 타임 스탬프로 지정됩니다.

ONTAP 네트워크 포트 정보를 봅니다

클러스터의 모든 노드에 있는 특정 포트 또는 모든 포트에 대한 정보를 표시할 수 있습니다.

이 작업에 대해

다음 정보가 표시됩니다.

- 노드 이름
- 포트 이름입니다
- IPspace 이름입니다
- 브로드캐스트 도메인 이름
- 링크 상태(위 또는 아래)
- MTU 설정
- 포트 속도 설정 및 작동 상태(초당 1기가비트 또는 10기가비트)
- 자동 협상 설정(참 또는 거짓)
- 이중 모드 및 작동 상태(반이중 또는 전이중)
- 해당되는 경우 포트의 인터페이스 그룹입니다
- 해당되는 경우 포트의 VLAN 태그 정보입니다
- 포트의 상태(상태 또는 성능 저하)
- 포트가 성능 저하로 표시된 이유

필드에 대한 데이터를 사용할 수 없는 경우(예: 비활성 포트에 대한 작동 이중화 및 속도를 사용할 수 없음) 필드 값이 로 표시됩니다 –.

단계

network port show 명령을 사용하여 네트워크 포트 정보를 표시합니다.

instance 매개변수를 지정하여 각 포트에 대한 상세 정보를 표시하거나 '-fields' 매개변수를 사용하여 필드 이름을 지정하여 특정 정보를 가져올 수 있습니다.

```
network port show
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  degraded
false
e0d       Default      Default          up   1500  auto/1000  degraded
true
Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  healthy
false
e0d       Default      Default          up   1500  auto/1000  healthy
false
8 entries were displayed.
```

에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP VLAN 정보를 봅니다

특정 VLAN에 대한 정보 또는 클러스터의 모든 VLAN에 대한 정보를 표시할 수 있습니다.

이 작업에 대해

`-instance' 매개변수를 지정하여 각 VLAN에 대한 세부 정보를 표시할 수 있습니다. '-fields' 매개 변수를 사용하여 필드

이름을 지정하여 특정 정보를 표시할 수 있습니다.

단계

네트워크 포트 vlan show 명령을 사용하여 VLAN에 대한 정보를 표시합니다. 다음 명령을 실행하면 클러스터의 모든 VLAN에 대한 정보가 표시됩니다.

```
network port vlan show
                  Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

에 대한 자세한 내용은 `network port vlan show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 인터페이스 그룹 정보를 봅니다

인터페이스 그룹에 대한 정보를 표시하여 해당 구성을 확인할 수 있습니다.

이 작업에 대해

다음 정보가 표시됩니다.

- 인터페이스 그룹이 있는 노드입니다
- 인터페이스 그룹에 포함된 네트워크 포트 목록입니다
- 인터페이스 그룹의 이름입니다
- 분배 기능(MAC, IP, 포트 또는 순차)
- 인터페이스 그룹의 MAC(Media Access Control) 주소입니다
- 포트 활동 상태, 즉 모든 집계된 포트가 활성(전체 참여) 상태인지 여부, 일부 포트가 활성(부분 참여) 상태인지 여부 또는 활성 포트가 없는지 여부

단계

network port ifgrp show 명령을 사용하여 interface group에 대한 정보를 출력한다.

'-instance' 매개 변수를 지정하여 각 노드에 대한 세부 정보를 표시할 수 있습니다. '-fields' 매개 변수를 사용하여 필드 이름을 지정하여 특정 정보를 표시할 수 있습니다.

다음 명령을 실행하면 클러스터의 모든 인터페이스 그룹에 대한 정보가 표시됩니다.

```
network port ifgrp show
         Port     Distribution                    Active
Node     IfGrp    Function     MAC Address        Ports   Ports
-------- -------- ------------ -----------------  ------- --------
cluster-1-01
         a0a      ip           02:a0:98:06:10:b2  full    e7a, e7b
cluster-1-02
         a0a      sequential   02:a0:98:06:10:ca  full    e7a, e7b
cluster-1-03
         a0a      port         02:a0:98:08:5b:66  full    e7a, e7b
cluster-1-04
         a0a      mac          02:a0:98:08:61:4e  full    e7a, e7b
```

다음 명령을 실행하면 단일 노드에 대한 상세한 인터페이스 그룹 정보가 표시됩니다.

```
network port ifgrp show -instance -node cluster-1-01

                  Node: cluster-1-01
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
   Port Participation: full
        Network Ports: e7a, e7b
             Up Ports: e7a, e7b
           Down Ports: -
```

에 대한 자세한 내용은 `network port ifgrp show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP LIF 정보 를 참조하십시오

LIF에 대한 자세한 정보를 보고 해당 구성을 확인할 수 있습니다.

또한 이 정보를 확인하여 중복 IP 주소 확인 또는 네트워크 포트가 올바른 서브넷에 속하는지 확인하는 등의 기본 LIF 문제를 진단할 수도 있습니다. SVM(Storage Virtual Machine) 관리자는 SVM과 연결된 LIF에 대한 정보만 볼 수 있습니다.

이 작업에 대해

다음 정보가 표시됩니다.

- LIF와 연결된 IP 주소입니다
- LIF의 관리 상태입니다

- LIF의 운영 상태입니다

  데이터 LIF의 운영 상태는 데이터 LIF가 연결된 SVM의 상태에 따라 결정됩니다. SVM이 중지되면 LIF의 운영 상태가 아래로 변경됩니다. SVM이 다시 시작되면 운영 상태가 가동으로 바뀝니다

- 노드 및 LIF가 상주하는 포트입니다

필드의 데이터를 사용할 수 없는 경우(예: 확장 상태 정보가 없는 경우) 필드 값은 '-'로 표시됩니다.

단계

명령을 사용하여 LIF 정보를 `network interface show` 표시합니다.

instance 매개 변수를 지정하여 각 LIF에 대한 자세한 정보를 보거나 -fields 매개 변수를 사용하여 필드 이름을 지정하여 특정 정보를 얻을 수 있습니다.

다음 명령을 실행하면 클러스터의 모든 LIF에 대한 일반 정보가 표시됩니다.

```
network interface show
           Logical    Status     Network          Current      Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node         Port
Home
---------- ---------- ---------- ---------------- ------------ -------
----
example
           lif1         up/up    192.0.2.129/22   node-01
                                                               e0d
false
node
           cluster_mgmt up/up    192.0.2.3/20     node-02
                                                               e0c
false
node-01
           clus1        up/up    192.0.2.65/18    node-01
                                                               e0a
true
           clus2        up/up    192.0.2.66/18    node-01
                                                               e0b
true
           mgmt1        up/up    192.0.2.1/20     node-01
                                                               e0c
true
node-02
           clus1        up/up    192.0.2.67/18    node-02
                                                               e0a
true
           clus2        up/up    192.0.2.68/18    node-02
                                                               e0b
true
           mgmt2        up/up    192.0.2.2/20     node-02
                                                               e0d
true
vs1
           d1           up/up    192.0.2.130/21   node-01
                                                               e0d
false
           d2           up/up    192.0.2.131/21   node-01
                                                               e0d
true
           data3        up/up    192.0.2.132/20   node-02
                                                               e0c
true
```

다음 명령을 실행하면 단일 LIF에 대한 자세한 정보가 표시됩니다.

```
network interface show -lif data1 -instance

                    Vserver Name: vs1
          Logical Interface Name: data1
                            Role: data
                   Data Protocol: nfs,cifs
                       Home Node: node-01
                       Home Port: e0c
                    Current Node: node-03
                    Current Port: e0c
               Operational Status: up
                  Extended Status: -
                          Is Home: false
                  Network Address: 192.0.2.128
                          Netmask: 255.255.192.0
            Bits in the Netmask: 18
                IPv4 Link Local: -
                    Subnet Name: -
             Administrative Status: up
                  Failover Policy: local-only
                  Firewall Policy: data
                      Auto Revert: false
   Fully Qualified DNS Zone Name: xxx.example.com
         DNS Query Listen Enable: false
             Failover Group Name: Default
                        FCP WWPN: -
                  Address family: ipv4
                         Comment: -
                  IPspace of LIF: Default
```

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 네트워크에 대한 라우팅 정보를 봅니다

SVM 내에서 경로에 대한 정보를 표시할 수 있습니다.

단계

보려는 라우팅 정보의 유형에 따라 해당 명령을 입력합니다.

에 대한 정보를 보려면…	입력…
SVM당 정적 경로	네트워크 라우트 쇼

SVM당 각 경로에 LIF가 있습니다	네트워크 라우트 show-lifs

'-instance' 파라미터를 지정하여 각 라우트에 대한 세부 정보를 표시할 수 있습니다. 다음 명령을 실행하면 SVM 내의 정적 경로가 클러스터-1에 표시됩니다.

```
network route show
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
Cluster
                    0.0.0.0/0       10.63.0.1       10
cluster-1
                    0.0.0.0/0       198.51.9.1      10
vs1
                    0.0.0.0/0       192.0.2.1       20
vs3
                    0.0.0.0/0       192.0.2.1       20
```

다음 명령을 실행하면 클러스터 1의 모든 SVM에 있는 정적 라우트 및 논리 인터페이스(LIF) 연결이 표시됩니다.

```
network route show-lifs
Vserver: Cluster
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               10.63.0.1               -

Vserver: cluster-1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               198.51.9.1              cluster_mgmt,
                                                cluster-1_mgmt1,

Vserver: vs1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data1_1, data1_2

Vserver: vs3
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data2_1, data2_2
```

및 `network route show-lifs` 에 대한 자세한 `network route show` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

ONTAP DNS 호스트 테이블 항목을 봅니다

DNS 호스트 테이블 항목은 호스트 이름을 IP 주소에 매핑합니다. 클러스터의 모든 SVM에 대해 매핑되는 호스트 이름 및 별칭 이름과 IP 주소를 표시할 수 있습니다.

단계

vserver services name-service dns hosts show 명령을 사용하여 모든 SVM에 대한 호스트 이름 항목을 표시합니다.

다음 예는 호스트 테이블 항목을 표시합니다.

```
vserver services name-service dns hosts show
Vserver    Address         Hostname        Aliases
---------- --------------- --------------- ---------------------
cluster-1
           10.72.219.36    lnx219-36       -
vs1
           10.72.219.37    lnx219-37       lnx219-37.example.com
```

SVM에서 DNS를 사용하도록 설정하려면 'vserver services name-service dns' 명령을 사용하고, 호스트 이름 확인을 위해 DNS를 사용하도록 구성할 수 있습니다. 호스트 이름은 외부 DNS 서버를 사용하여 확인됩니다.

ONTAP DNS 도메인 구성 정보를 봅니다

클러스터에 있는 하나 이상의 SVM(스토리지 가상 머신)의 DNS 도메인 구성을 표시하여 올바르게 구성되었는지 확인할 수 있습니다.

단계

'vserver services name-service dns show' 명령을 사용하여 DNS 도메인 구성을 봅니다.

다음 명령을 실행하면 클러스터의 모든 SVM에 대한 DNS 구성이 표시됩니다.

```
vserver services name-service dns show
                                                 Name
Vserver         State     Domains                Servers
--------------- --------- ---------------------- -------------
cluster-1        enabled   xyz.company.com         192.56.0.129,
                                                 192.56.0.130
vs1             enabled   xyz.company.com        192.56.0.129,
                                                 192.56.0.130
vs2             enabled   xyz.company.com        192.56.0.129,
                                                 192.56.0.130
vs3             enabled   xyz.company.com        192.56.0.129,
                                                 192.56.0.130
```

다음 명령을 실행하면 SVM VS1 에 대한 자세한 DNS 구성 정보가 표시됩니다.

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
          Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

ONTAP 페일오버 그룹 정보를 봅니다

각 페일오버 그룹의 노드 및 포트 목록, 페일오버 설정 또는 해제, 각 LIF에 적용되는 페일오버 정책 유형 등 페일오버 그룹에 대한 정보를 볼 수 있습니다.

단계

1. network interface failover-groups show 명령을 사용하여 각 페일오버 그룹의 타겟 포트를 표시합니다.

   다음 명령을 실행하면 2노드 클러스터의 모든 페일오버 그룹에 대한 정보가 표시됩니다.

```
network interface failover-groups show
                                 Failover
Vserver          Group           Targets
---------------- --------------- --------------------------------
Cluster
                 Cluster
                                 cluster1-01:e0a, cluster1-01:e0b,
                                 cluster1-02:e0a, cluster1-02:e0b
vs1
                 Default
                                 cluster1-01:e0c, cluster1-01:e0d,
                                 cluster1-01:e0e, cluster1-02:e0c,
                                 cluster1-02:e0d, cluster1-02:e0e
```

   에 대한 자세한 내용은 `network interface failover-groups show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. network interface failover-groups show 명령을 사용하여 특정 페일오버 그룹의 대상 포트와 브로드캐스트 도메인을 표시합니다.

   다음 명령을 실행하면 SVM VS4 용 페일오버 그룹 data12에 대한 자세한 정보가 표시됩니다.

```
network interface failover-groups show -vserver vs4 -failover-group
data12

       Vserver Name: vs4
Failover Group Name: data12
   Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                     cluster1-02:e0g
   Broadcast Domain: Default
```

3. network interface show 명령을 사용하여 모든 LIF에서 사용되는 페일오버 설정을 표시합니다.

   다음 명령을 실행하면 각 LIF에서 사용 중인 페일오버 정책과 페일오버 그룹이 표시됩니다.

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                  failover-policy         failover-group
--------  -------------------  ----------------------  --------------
Cluster   cluster1-01_clus_1   local-only              Cluster
Cluster   cluster1-01_clus_2   local-only              Cluster
Cluster   cluster1-02_clus_1   local-only              Cluster
Cluster   cluster1-02_clus_2   local-only              Cluster
cluster1  cluster_mgmt         broadcast-domain-wide   Default
cluster1  cluster1-01_mgmt1    local-only              Default
cluster1  cluster1-02_mgmt1    local-only              Default
vs1       data1                disabled                Default
vs3       data2                system-defined          group2
```

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP LIF 페일오버 대상을 봅니다

페일오버 정책과 LIF의 페일오버 그룹이 올바르게 구성되었는지 확인해야 할 수 있습니다. 페일오버 규칙의 구성 오류를 방지하기 위해 단일 LIF 또는 모든 LIF의 페일오버 목표를 표시할 수 있습니다.

이 작업에 대해

LIF 페일오버 타겟을 디스플레이하면 다음을 확인할 수 있습니다.

- LIF가 올바른 페일오버 그룹 및 페일오버 정책으로 구성되었는지 여부를 나타냅니다
- 페일오버 타겟 포트의 결과 목록이 각 LIF에 적합한지 여부
- 데이터 LIF의 페일오버 목표가 관리 포트(e0M)가 아닌지 여부

단계

network interface show 명령의 페일오버 옵션을 사용하여 LIF의 페일오버 타겟을 표시합니다.

다음 명령을 실행하면 2노드 클러스터의 모든 LIF에 대한 페일오버 타겟에 대한 정보가 표시됩니다. 페일오버 타겟 행은 해당 LIF에 대한 노드 포트 조합의 (우선 순위) 목록을 표시합니다.

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------ --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

로드 밸런싱 존에서 **ONTAP LIF**를 확인하십시오

로드 밸런싱 영역이 올바르게 구성되었는지 확인하려면 해당 LIF에 속하는 모든 LIF를 표시할 수 있습니다. 또한 특정 LIF의 로드 밸런싱 존 또는 모든 LIF의 로드 밸런싱 존(Zone)을 볼 수도 있습니다.

단계

다음 명령 중 하나를 사용하여 원하는 LIF 및 로드 밸런싱 세부 정보를 표시합니다

표시 방법	입력…
특정 로드 밸런싱 구역에 있는 LIF입니다	네트워크 인터페이스 show-dns-zone zone zone_name zone_name은 load balancing zone의 이름을 지정한다.
특정 LIF의 로드 밸런싱 존	네트워크 인터페이스 show-lif lif_name-fields DNS-zone
모든 LIF의 로드 밸런싱 존	네트워크 인터페이스 보기 필드 DNS-존

LIF의 로드 밸런싱 존 표시 예

다음 명령을 실행하면 SVM vs0에 대한 로드 밸런싱 존 storage.company.com 에 있는 모든 LIF의 세부 정보가 표시됩니다.

```
net int show -vserver vs0 -dns-zone storage.company.com

          Logical    Status     Network            Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask       Node      Port    Home
--------- ---------- ---------- ------------------ --------- ------- ----
vs0
          lif3         up/up    10.98.226.225/20   ndeux-11  e0c     true
          lif4         up/up    10.98.224.23/20    ndeux-21  e0c     true
          lif5         up/up    10.98.239.65/20    ndeux-11  e0c     true
          lif6         up/up    10.98.239.66/20    ndeux-11  e0c     true
          lif7         up/up    10.98.239.63/20    ndeux-21  e0c     true
          lif8         up/up    10.98.239.64/20    ndeux-21  e0c     true
```

다음 명령을 실행하면 LIF 데이터의 DNS 존 세부 정보가 표시됩니다.3

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

다음 명령을 실행하면 클러스터에 있는 모든 LIF와 해당 DNS 존 목록이 표시됩니다.

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 클러스터 연결을 봅니다

클러스터의 모든 활성 연결 또는 클라이언트, 논리 인터페이스, 프로토콜 또는 서비스별로 노드의 활성 연결 수를 표시할 수 있습니다. 클러스터의 모든 수신 대기 연결을 표시할 수도 있습니다.

클라이언트별 활성 연결 표시(클러스터 관리자만 해당)

클라이언트별로 활성 연결을 확인하여 특정 클라이언트가 사용 중인 노드를 확인하고 노드당 클라이언트 수 간의 불균형을 확인할 수 있습니다.

이 작업에 대해

클라이언트별 활성 연결 수는 다음 시나리오에서 유용합니다.

- 사용 중이거나 과부하 상태인 노드 찾기
- 특정 클라이언트의 볼륨 액세스 속도가 느린 이유 파악

  클라이언트가 액세스하는 노드에 대한 세부 정보를 확인한 다음 볼륨이 상주하는 노드와 비교할 수 있습니다. 볼륨에 액세스해야 할 경우 초과 할당된 원격 노드의 볼륨에 대한 원격 액세스로 인해 클라이언트 성능이 저하될 수 있습니다.

- 모든 노드가 데이터 액세스에 동등하게 사용되는지 확인
- 예기치 않게 많은 수의 연결이 있는 클라이언트를 찾는 중입니다.
- 특정 클라이언트에 노드에 대한 연결이 있는지 확인

단계

network connections active show-clients 명령을 사용하여 노드의 클라이언트별 활성 연결 수를 표시합니다.

에 대한 자세한 내용은 `network connections active show-clients` "ONTAP 명령 참조입니다"을 참조하십시오.

```
network connections active show-clients
Node    Vserver Name    Client IP Address     Count
------  --------------  -----------------     ------
node0   vs0             192.0.2.253                1
        vs0             192.0.2.252                2
        Cluster         192.10.2.124               5
node1   vs0             192.0.2.250                1
        vs0             192.0.2.252                3
        Cluster         192.10.2.123               4
node2   vs1             customer.example.com       1
        vs1             192.0.2.245                3
        Cluster         192.10.2.122               4
node3   vs1             customer.example.org       1
        vs1             customer.example.net       3
        Cluster         192.10.2.121               4
```

프로토콜별 활성 연결 표시(클러스터 관리자만 해당)

노드의 프로토콜(TCP 또는 UDP)별로 활성 연결 수를 표시하여 클러스터 내의 프로토콜 사용량을 비교할 수 있습니다.

이 작업에 대해

프로토콜별 활성 연결 수는 다음 시나리오에서 유용합니다.

- 연결을 끊는 UDP 클라이언트를 찾습니다.

  노드가 연결 제한에 근접하면 UDP 클라이언트가 가장 먼저 삭제됩니다.

- 사용 중인 다른 프로토콜이 없는지 확인

단계

network connections active show-protocols 명령을 사용하여 노드의 프로토콜별 활성 연결 수를 표시합니다.

에 대한 자세한 내용은 `network connections active show-protocols` "ONTAP 명령 참조입니다"을 참조하십시오.

```
network connections active show-protocols
Node     Vserver Name  Protocol   Count
-------  ------------  ---------  ------
node0
         vs0           UDP            19
         Cluster       TCP            11
node1
         vs0           UDP            17
         Cluster       TCP             8
node2
         vs1           UDP            14
         Cluster       TCP            10
node3
         vs1           UDP            18
         Cluster       TCP             4
```

서비스별 활성 연결 표시(클러스터 관리자만 해당)

클러스터의 각 노드에 대해 서비스 유형(예: NFS, SMB, 마운트 등)별로 활성 연결 수를 표시할 수 있습니다. 이 기능은 클러스터 내의 서비스 사용을 비교하여 노드의 운영 워크로드를 확인하는 데 유용합니다.

이 작업에 대해

서비스별 활성 연결 수는 다음 시나리오에서 유용합니다.

- 모든 노드가 적절한 서비스에 사용되고 있는지, 그리고 해당 서비스에 대한 로드 밸런싱이 작동하는지 확인합니다.
- 사용 중인 다른 서비스가 없는지 확인 network connections active show-services 명령을 사용하여 노드의 service별 활성 접속 수를 출력한다.

에 대한 자세한 내용은 `network connections active show-services` "ONTAP 명령 참조입니다"을 참조하십시오.

```
network connections active show-services
Node        Vserver Name    Service    Count
---------  --------------  ---------  ------
node0
            vs0             mount           3
            vs0             nfs            14
            vs0             nlm_v4          4
            vs0             cifs_srv        3
            vs0             port_map       18
            vs0             rclopcp        27
            Cluster         ctlopcp        60
node1
            vs0             cifs_srv        3
            vs0             rclopcp        16
            Cluster         ctlopcp        60
node2
            vs1             rclopcp        13
            Cluster         ctlopcp        60
node3
            vs1             cifs_srv        1
            vs1             rclopcp        17
            Cluster         ctlopcp        60
```

LIF를 사용하여 노드 및 **SVM**에 활성 연결을 표시합니다

노드 및 SVM(스토리지 가상 머신)별로 각 LIF의 활성 연결 수를 표시하여 클러스터 내 LIF 간 연결 불균형을 확인할 수 있습니다.

이 작업에 대해

LIF에 의한 활성 연결 수는 다음 시나리오에서 유용합니다.

- 각 LIF의 연결 수를 비교하여 오버로드된 LIF를 찾습니다.
- 모든 데이터 LIF에서 DNS 로드 밸런싱이 작동하는지 확인
- 다양한 SVM에 대한 연결 수를 비교하여 가장 많이 사용되는 SVM을 찾습니다.

단계

'network connections active show-liff' 명령을 사용하여 SVM과 노드에서 각 LIF의 활성 연결 수를 표시합니다.

에 대한 자세한 내용은 `network connections active show-lifs` "ONTAP 명령 참조입니다"을 참조하십시오.

```
network connections active show-lifs
Node      Vserver Name  Interface Name  Count
--------  ------------  --------------- ------
node0
          vs0           datalif1             3
          Cluster       node0_clus_1         6
          Cluster       node0_clus_2         5
node1
          vs0           datalif2             3
          Cluster       node1_clus_1         3
          Cluster       node1_clus_2         5
node2
          vs1           datalif2             1
          Cluster       node2_clus_1         5
          Cluster       node2_clus_2         3
node3
          vs1           datalif1             1
          Cluster       node3_clus_1         2
          Cluster       node3_clus_2         2
```

클러스터의 활성 연결을 표시합니다

클러스터의 활성 연결에 대한 정보를 표시하여 개별 연결에 사용되는 LIF, 포트, 원격 호스트, 서비스, SVM(스토리지 가상 머신) 및 프로토콜을 볼 수 있습니다.

이 작업에 대해

클러스터에서 활성 연결을 보는 것은 다음 시나리오에서 유용합니다.

- 개별 클라이언트가 올바른 노드에서 올바른 프로토콜 및 서비스를 사용하고 있는지 확인
- 클라이언트가 특정 노드, 프로토콜 및 서비스 조합을 사용하여 데이터에 액세스하는 데 문제가 있는 경우 이 명령을 사용하여 구성 또는 패킷 추적 비교를 위한 유사한 클라이언트를 찾을 수 있습니다.

단계

network connections active show 명령을 사용하여 클러스터의 활성 연결을 표시합니다.

에 대한 자세한 내용은 `network connections active show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 노드 노드 1의 활성 연결이 표시됩니다.

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

다음 명령을 실행하면 SVM VS1 에서의 활성 연결이 표시됩니다.

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

클러스터의 수신 대기 연결을 표시합니다

클러스터에서 수신 대기 중인 연결에 대한 정보를 표시하여 지정된 프로토콜 및 서비스의 연결을 수락하는 LIF 및 포트를 볼 수 있습니다.

이 작업에 대해

클러스터에서 청취 연결을 보는 것은 다음 시나리오에서 유용합니다.

- 클라이언트가 해당 LIF에 일관되게 연결할 수 없을 경우, 원하는 프로토콜 또는 서비스가 LIF에서 청취 가능한지 확인하십시오.
- 다른 노드의 LIF를 통해 한 노드의 볼륨에 대한 원격 데이터 액세스가 장애가 발생할 경우 각 클러스터 LIF에서 UDP/rclopcp 수신기가 열려 있는지 확인합니다.
- SnapMirror가 동일한 클러스터의 두 노드 간에 전송 실패 시 각 클러스터 LIF에서 UDP/rclopcp 수신기가 열렸는지 확인
- SnapMirror가 서로 다른 클러스터에 있는 두 노드 간에 전송하는 데 실패할 경우 각 인터클러스터 LIF에서 TCP/ctlpcp 수신기가 열렸는지 확인합니다.

단계

Network connections listening show 명령을 사용하여 노드별 listening connection을 출력한다.

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

에 대한 자세한 내용은 `network connections listening show` "ONTAP 명령 참조입니다"을 참조하십시오.

네트워크 문제를 진단하는 **ONTAP** 명령

ping, traceroute, NDP, tcpdump 등의 명령어를 이용하여 네트워크 문제를 진단할 수 있다. 또한 ping6, tracerout6 등의 명령을 사용하여 IPv6 문제를 진단할 수도 있습니다.

원하는 작업	이 명령을 입력하십시오...
노드가 네트워크의 다른 호스트에 도달할 수 있는지 테스트합니다	네트워크 핑
노드가 IPv6 네트워크의 다른 호스트에 도달할 수 있는지 테스트합니다	네트워크 핑6
IPv4 패킷이 네트워크 노드에 취하는 경로를 추적한다	네트워크 추적 경로
IPv6 패킷이 네트워크 노드로 전송하는 경로를 추적한다	네트워크 tracerout6
NDP(Neighbor Discovery Protocol) 관리	네트워크 NDP
지정된 네트워크 인터페이스 또는 모든 네트워크 인터페이스에서 수신 및 전송된 패킷에 대한 통계를 표시합니다	'run-node_node_name_ifstat' * 참고 *: 이 명령은 노드 쉘에서 사용할 수 있습니다.
원격 디바이스 유형 및 디바이스 플랫폼을 포함하여 클러스터의 각 노드 및 포트에서 검색된 인접 디바이스에 대한 정보를 표시합니다	네트워크 디바이스 발견 쇼
노드의 CDP 인접 항목 보기(ONTAP는 CDPv1 광고만 지원)	'run-node_node_name_CDPD show -neighbors' * 참고 *: 이 명령은 노드 쉘에서 사용할 수 있습니다.

네트워크에서 송수신되는 패킷을 추적합니다	"network tcpdump start-node_node-name_-port_port_name_' * 참고 *: 이 명령은 노드 쉘에서 사용할 수 있습니다.
클러스터 간 또는 클러스터 간 노드 간의 지연 시간 및 처리량 측정	'network test-path-source-node_source_nodename local_-destination-cluster_destination_clustername_-destination-node_destination_nodename_-session-type_Default_,*AsyncMirrorLocal*,*AsyncMirrorRemote*, *SyncMirrorRemote* 또는 *RemoteDataTransfer*'를 참조하십시오 "성능 관리".

관련 정보

- "ONTAP 명령 참조입니다"
- "네트워크 Ping"
- "네트워크 경로 추적"
- "네트워크 장치 검색 표시"
- "네트워크 NDP"

Neighbor Discovery Protocol을 통한 네트워크 접속 구성 보기

Neighbor Discovery Protocol을 통해 **ONTAP** 네트워크 연결을 확인하십시오

데이터 센터에서 인접 검색 프로토콜을 사용하여 물리적 또는 가상 시스템 쌍과 해당 네트워크 인터페이스 간의 네트워크 연결을 볼 수 있습니다. ONTAP는 CDP(Cisco Discovery Protocol) 및 LLDP(Link Layer Discovery Protocol)라는 두 개의 인접 검색 프로토콜을 지원합니다.

인접 검색 프로토콜을 사용하면 네트워크에서 직접 연결된 프로토콜 지원 장치에 대한 정보를 자동으로 검색하고 볼 수 있습니다. 각 장치는 ID, 용량 및 연결 정보를 네트워크에 알립니다. 이 정보는 이더넷 프레임에서 멀티캐스트 MAC 주소로 전송되며, 인접한 모든 프로토콜 지원 장치에서 수신됩니다.

두 개의 장치가 이웃이 되려면 각각 프로토콜이 활성화되어 있고 올바르게 구성되어 있어야 합니다. 검색 프로토콜 기능은 직접 연결된 네트워크로 제한됩니다. 이웃에는 스위치, 라우터, 브리지 등과 같은 프로토콜 지원 장치가 포함될 수 있습니다. ONTAP는 개별적으로 또는 함께 사용할 수 있는 두 개의 인접 검색 프로토콜을 지원합니다.

- CDP(Cisco Discovery Protocol) *

CDP는 Cisco Systems에서 개발한 독점 링크 계층 프로토콜입니다. 이 기능은 클러스터 포트에 대해 ONTAP에서 기본적으로 활성화되지만 데이터 포트에 대해 명시적으로 설정해야 합니다.

LLDP(Link Layer Discovery Protocol) *

LLDP는 표준 문서 IEEE 802.1AB에 지정된 공급업체 중립적인 프로토콜입니다. 모든 포트에 대해 명시적으로 활성화해야 합니다.

CDP를 사용하여 **ONTAP** 네트워크 연결을 감지합니다

CDP를 사용하여 네트워크 연결을 감지하는 것은 배포 고려 사항 검토, 데이터 포트에서 활성화, 인접 장치 보기 및 필요에 따라 CDP 구성 값 조정으로 구성됩니다. CDP는 클러스터 포트에서 기본적으로 사용하도록 설정됩니다.

인접 장치에 대한 정보를 표시하려면 모든 스위치 및 라우터에서 CDP를 사용하도록 설정해야 합니다.

ONTAP 릴리즈	설명
9.10.1 이하	CDP는 클러스터 스위치 상태 모니터에서 클러스터 및 관리 네트워크 스위치를 자동으로 검색하는 데 사용됩니다.
9.11.1 이상	CDP는 클러스터 스위치 상태 모니터에서 클러스터, 스토리지 및 관리 네트워크 스위치를 자동으로 검색하는 데 사용됩니다.

관련 정보

"시스템 관리"

CDP 사용 시 고려 사항

기본적으로 CDP 호환 장치는 CDPv2 광고를 보냅니다. CDP 호환 장치는 CDPv1 광고를 수신할 때만 CDPv1 광고를 보냅니다. ONTAP는 CDPv1만 지원합니다. 따라서 ONTAP 노드가 CDPv1 광고를 전송할 때 CDP 호환 인접 장치는 CDPv1 광고를 다시 보냅니다.

노드에서 CDP를 사용하도록 설정하기 전에 다음 정보를 고려해야 합니다.

- CDP는 모든 포트에서 지원됩니다.
- CDP 광고는 UP 상태인 포트를 통해 송수신합니다.
- CDP 광고를 보내고 받으려면 전송 및 수신 장치 모두에서 CDP를 사용하도록 설정해야 합니다.
- CDP 광고는 일정한 간격으로 전송되며 시간 간격을 구성할 수 있습니다.
- LIF의 IP 주소가 변경되면 노드는 다음 CDP 광고에서 업데이트된 정보를 보냅니다.
- ONTAP 9.10.1 이하:
  - CDP는 클러스터 포트에서 항상 사용하도록 설정됩니다.
  - CDP는 기본적으로 모든 비클러스터 포트에서 사용할 수 없습니다.
- ONTAP 9.11.1 이상:
  - CDP는 항상 클러스터 및 스토리지 포트에서 사용하도록 설정됩니다.
  - CDP는 기본적으로 모든 비 클러스터 및 비 스토리지 포트에서 사용할 수 없습니다.

> ⓘ 노드에서 LIF가 변경되는 경우 CDP 정보는 수신 디바이스 측(예: 스위치)에서 업데이트되지 않는 경우가 있습니다. 이러한 문제가 발생하는 경우 노드의 네트워크 인터페이스를 DOWN 상태로 구성한 다음 UP 상태로 구성해야 합니다.

- CDP 광고에서는 IPv4 주소만 보급됩니다.
- VLAN이 있는 물리적 네트워크 포트의 경우 해당 포트의 VLAN에 구성된 모든 LIF가 보급됩니다.
- 인터페이스 그룹에 속한 물리적 포트의 경우 해당 인터페이스 그룹에 구성된 모든 IP 주소가 각 물리적 포트에 공고됩니다.
- VLAN을 호스팅하는 인터페이스 그룹의 경우 인터페이스 그룹과 VLAN에 구성된 모든 LIF가 각 네트워크 포트에 공고됩니다.

- CDP 패킷이 1500바이트 이하로 제한되기 때문에 많은 수의 LIF로 구성된 포트에서 이러한 IP 주소 중 일부만 인접 스위치에 보고됩니다.

CDP를 사용하거나 사용하지 않도록 설정합니다

CDP를 준수하는 인접 장치를 검색하고 알림을 보내려면 클러스터의 각 노드에서 CDP를 사용하도록 설정해야 합니다.

ONTAP 9.10.1 이하 버전에서는 기본적으로 CDP가 노드의 모든 클러스터 포트에서 활성화되고 노드의 모든 비클러스터 포트에서 비활성화됩니다.

기본적으로 ONTAP 9.11.1 이상에서는 CDP가 노드의 모든 클러스터 및 스토리지 포트에서 활성화되고 노드의 모든 비클러스터 및 비스토리지 포트에서 비활성화됩니다.

이 작업에 대해

CDPD.ENABLE 옵션은 노드 포트에서 CDP가 활성화 또는 비활성화되는지 여부를 제어합니다.

- ONTAP 9.10.1 이하의 경우, On은 비 클러스터 포트에서 CDP를 사용하도록 설정합니다.
- ONTAP 9.11.1 이상의 경우, On은 비 클러스터 및 비 스토리지 포트에서 CDP를 사용하도록 설정합니다.
- ONTAP 9.10.1 이하 버전의 경우, 클러스터 포트가 아닌 경우 CDP가 사용되지 않으므로 클러스터 포트에서 CDP를 사용하지 않도록 설정할 수 없습니다.
- ONTAP 9.11.1 이상의 경우, OFF는 클러스터링되지 않은 포트와 비스토리지 포트에서 CDP를 사용하지 않도록 설정합니다. 클러스터 포트에서 CDP를 사용하지 않도록 설정할 수 없습니다.

CDP 호환 장치에 연결된 포트에서 CDP가 비활성화되어 있으면 네트워크 트래픽이 최적화되지 않을 수 있습니다.

단계

1. 노드 또는 클러스터의 모든 노드에 대한 현재 CDP 설정을 표시합니다.

CDP 설정을 보려면…	입력…
노드	'run-node <node_name> options CDPD.enable'
클러스터의 모든 노드	옵션 CDPD.ENABLE

2. 노드의 모든 포트 또는 클러스터의 모든 노드 포트에서 CDP를 사용하거나 사용하지 않도록 설정:

에서 CDP를 활성화 또는 비활성화하려면…	입력…
노드	'run-node node_name options CDPD.enable{on or off}'
클러스터의 모든 노드	'options CDPD.enable{on or off}'

CDP 인접 항목 정보를 봅니다

포트가 CDP 호환 장치에 연결되어 있는 경우, 클러스터 노드의 각 포트에 연결된 인접 장치에 대한 정보를 볼 수 있습니다. 명령을 사용하여 Neighbor 정보를 볼 수 있다 `network device-discovery show -protocol cdp`. 에 대한 자세한 내용은 `network device-discovery show` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

ONTAP 9.10.1 이하 버전에서는 클러스터 포트에 대해 CDP가 항상 활성화되어 있기 때문에 해당 포트에 대해 CDP 인접 항목 정보가 항상 표시됩니다. 해당 포트에 대한 인접 정보가 표시되도록 비 클러스터 포트에서 CDP를 사용하도록 설정해야 합니다.

ONTAP 9.11.1 이상에서는 CDP가 항상 클러스터 및 스토리지 포트에 대해 활성화되므로 해당 포트에 대해 CDP 인접 항목 정보가 항상 표시됩니다. 해당 포트에 대해 인접 정보가 표시되도록 클러스터링되지 않은 포트와 비스토리지 포트에서 CDP가 활성화되어 있어야 합니다.

단계

클러스터의 노드의 포트에 연결된 모든 CDP 호환 디바이스에 대한 정보를 표시합니다.

```
network device-discovery show -node node -protocol cdp
```

다음 명령을 실행하면 노드 sti2650-212의 포트에 연결된 인접 항목이 표시됩니다.

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14      N9K-
C93120TX
            e0a    CS:RTP-CS01-510K35        0/8               CN1610
            e0b    CS:RTP-CS01-510K36        0/8               CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21      N9K-
C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22      N9K-
C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23      N9K-
C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24      N9K-
C93180YC-FX
```

출력에는 지정된 노드의 각 포트에 연결된 Cisco 장치가 나열됩니다.

CDP 메시지의 보류 시간을 구성합니다

보류 시간은 CDP 광고가 인접한 CDP 준수 장치의 캐시에 저장되는 기간입니다. 보류 시간은 각 CDPv1 패킷에 공고되며 노드에서 CDPv1 패킷을 수신할 때마다 업데이트됩니다.

- 'CDPD.HoldTime' 옵션의 값은 HA 쌍의 양쪽 노드에서 동일한 값으로 설정해야 합니다.
- 기본 유지 시간 값은 180초이지만 10초에서 255초 사이의 값을 입력할 수 있습니다.
- 보류 시간이 만료되기 전에 IP 주소를 제거하면 보류 시간이 만료될 때까지 CDP 정보가 캐싱됩니다.

단계

1. 노드 또는 클러스터의 모든 노드에 대한 현재 CDP 보류 시간을 표시합니다.

보류 시간을 보려면…	입력…
노드	'run-node node_name options CDPD.HoldTime'
클러스터의 모든 노드	옵션 CDPD.HoldTime

2. 클러스터의 모든 포트 또는 클러스터의 모든 노드에 있는 모든 포트에 대해 CDP 보류 시간을 구성합니다.

보류 시간을 설정하려면…	입력…
노드	'run-node node_name options CDPD.HoldTime HoldTime'
클러스터의 모든 노드	옵션 CDPD.HoldTime HoldTime

CDP 광고 전송 간격을 설정합니다

CDP 광고는 CDP 이웃에게 정기적으로 전송됩니다. 네트워크 트래픽과 네트워크 토폴로지의 변경 내용에 따라 CDP 광고 전송 간격을 늘리거나 줄일 수 있습니다.

- "cdpd.interval` 옵션 값은 HA 쌍의 두 노드에서 같은 값으로 설정해야 합니다.
- 기본 간격은 60초이지만 5초에서 900초 사이의 값을 입력할 수 있습니다.

단계

1. 노드 또는 클러스터의 모든 노드에 대한 현재 CDP 광고 시간 간격을 표시합니다.

간격을 보려면…	입력…
노드	'run-node node_name options cdpd.interval`
클러스터의 모든 노드	옵션 cdpd.interval`

2. 노드의 모든 포트 또는 클러스터의 모든 노드 포트에 대해 CDP 알림을 보내는 간격을 구성합니다.

간격을 설정하려면…	입력…
노드	'run-node node_name options cdpd.interval interval
클러스터의 모든 노드	옵션 cdpd.interval 간격

CDP 통계를 보거나 지웁니다

각 노드의 클러스터 및 비클러스터 포트에 대한 CDP 통계를 보고 잠재적인 네트워크 연결 문제를 감지할 수 있습니다. CDP 통계는 마지막 삭제 시점으로부터 누적됩니다.

이 작업에 대해

ONTAP 9.10.1 이하 버전에서는 포트에 대해 CDP가 항상 활성화되어 있기 때문에 해당 포트의 트래픽에 대해 CDP 통계가 항상 표시됩니다. 해당 포트에 대한 통계를 표시하려면 포트에서 CDP를 사용하도록 설정해야 합니다.

ONTAP 9.11.1 이상에서는 CDP가 항상 클러스터 및 스토리지 포트에 대해 활성화되므로 해당 포트의 트래픽에 대해 CDP 통계가 항상 표시됩니다. 이러한 포트에 대한 통계를 표시하려면 클러스터링되지 않은 포트 또는 비스토리지 포트에서 CDP가 활성화되어 있어야 합니다.

단계

노드의 모든 포트에 대한 현재 CDP 통계를 표시하거나 지웁니다.

원하는 작업	입력…
CDP 통계를 봅니다	'run-node_name CDPD show-stats'
CDP 통계를 지웁니다	'run-node_name CDPD zero-stats'

통계 표시 및 지우기 예

다음 명령을 실행하면 CDP 통계가 지워지기 전에 표시됩니다. 마지막 통계 삭제 이후 송수신된 총 패킷 수가 출력에 표시됩니다.

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:          9116  | Csum Errors:        0  | Unsupported Vers:  4561
 Invalid length:      0  | Malformed:          0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:     0  | Other errors:         0

TRANSMIT
 Packets:          4557  | Xmit fails:         0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:    0  | Other errors:         0

OTHER
 Init failures:       0
```

다음 명령을 실행하면 CDP 통계가 지워집니다.

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:              0   | Csum Errors:         0   | Unsupported Vers:      0
 Invalid length:       0   | Malformed:           0   | Mem alloc fails:       0
 Missing TLVs:         0   | Cache overflow:      0   | Other errors:          0

TRANSMIT
 Packets:              0   | Xmit fails:          0   | No hostname:           0
 Packet truncated:     0   | Mem alloc fails:     0   | Other errors:          0

OTHER
 Init failures:        0
```

통계를 지운 후에는 다음 CDP 보급 알림이 전송되거나 수신된 후에 누적되기 시작합니다.

CDP를 지원하지 않는 이더넷 스위치에 연결 중입니다

여러 공급업체 스위치는 CDP를 지원하지 않습니다. 를 참조하십시오"NetApp 지식 기반: ONTAP 장치 검색 시 스위치 대신 노드가 표시됨" 자세한 내용은.

이 문제를 해결하는 방법에는 두 가지가 있습니다.

- 지원되는 경우 CDP를 사용하지 않도록 설정하고 LLDP를 사용하도록 설정합니다. 을 참조하십시오 "LLDP를 사용하여 네트워크 연결을 감지합니다" 를 참조하십시오.
- CDP 광고를 삭제하도록 스위치에서 MAC 주소 패킷 필터를 구성합니다.

LLDP를 사용하여 ONTAP 네트워크 연결을 검색합니다

LLDP를 사용하여 네트워크 연결을 탐지하는 작업은 배포 고려 사항을 검토하고, 모든 포트에서 활성화하고, 인접 장치를 보고, 필요에 따라 LLDP 구성 값을 조정하는 것으로 구성됩니다.

인접 장치에 대한 정보를 표시하려면 모든 스위치 및 라우터에서 LLDP를 활성화해야 합니다.

ONTAP는 현재 다음과 같은 TLV(type-length-value structures)를 보고합니다.

- 섀시 ID입니다
- 포트 ID입니다
- TTL(Time-to-Live)
- 시스템 이름입니다

  시스템 이름 TLV는 CNA 장치에서 전송되지 않습니다.

X1143 어댑터 및 UTA2 온보드 포트와 같은 특정 통합 네트워크 어댑터(CNA)에는 LLDP에 대한 오프로드 지원 기능이 포함되어 있습니다.

- LLDP 오프로드는 DCB(데이터 센터 브리징)에 사용됩니다.
- 표시된 정보는 클러스터와 스위치 간에 다를 수 있습니다.

  스위치에 표시되는 섀시 ID 및 포트 ID 데이터는 CNA 및 비 CNA 포트에 대해 다를 수 있습니다.

예를 들면 다음과 같습니다.

- 비 CNA 포트의 경우:
  - 섀시 ID는 노드에 있는 포트 중 하나의 고정 MAC 주소입니다
  - 포트 ID는 노드에 있는 해당 포트의 포트 이름입니다
- CNA 포트의 경우:
  - 섀시 ID와 포트 ID는 노드에 있는 각 포트의 MAC 주소입니다.

그러나 클러스터에서 표시하는 데이터는 이러한 포트 유형에 대해 일관적입니다.

LLDP 사양은 SNMP MIB를 통해 수집된 정보에 대한 액세스를 정의합니다. 그러나 ONTAP는 현재 LLDP MIB를 지원하지 않습니다.

LLDP를 활성화 또는 비활성화합니다

LLDP 호환 인접 장치를 검색하고 보급을 보내려면 클러스터의 각 노드에서 LLDP를 활성화해야 합니다. ONTAP 9.7부터 LLDP는 기본적으로 노드의 모든 포트에서 활성화됩니다.

이 작업에 대해

ONTAP 9.10.1 이하 버전의 경우, 노드 포트에서 LLDP가 활성화 또는 비활성화되는지 여부를 제어하는 LAll DP.enable 옵션:

- On은 모든 포트에서 LLDP를 활성화합니다.
- OFF는 모든 포트에서 LLDP를 비활성화합니다.

ONTAP 9.11.1 이상의 경우, "LI DP.enable" 옵션은 노드의 비클러스터 및 비스토리지 포트에서 LLDP가 활성화될지 여부를 제어합니다.

- On은 모든 비 클러스터 및 비 스토리지 포트에서 LLDP를 활성화합니다.
- "off"는 모든 비 클러스터 및 비 스토리지 포트에서 LLDP를 비활성화합니다.

단계

1. 노드 또는 클러스터의 모든 노드에 대한 현재 LLDP 설정을 표시합니다.
   - 단일 노드: 'run-node_name options lldp.enable'
   - 모든 노드: 옵션 ll dp.enable
2. 노드의 모든 포트 또는 클러스터의 모든 노드 포트에서 LLDP를 사용하거나 사용하지 않도록 설정합니다.

에서 LLDP를 활성화 또는 비활성화하려면…	입력…

노드	'run-node node_name options lldp.enable{on
off}'	클러스터의 모든 노드
'options lldp.enable{on	off}'

◦ 단일 노드:

```
run -node node_name options lldp.enable {on|off}
```

◦ 모든 노드:

```
options lldp.enable {on|off}
```

LLDP 인접 정보를 봅니다

포트가 LLDP 호환 장치에 연결되어 있는 경우, 클러스터 노드의 각 포트에 연결된 인접 장치에 대한 정보를 볼 수 있습니다. network device-discovery show 명령을 사용하여 인접 항목 정보를 볼 수 있습니다.

단계

1. 클러스터의 노드의 포트에 연결된 모든 LLDP 호환 장치에 대한 정보를 표시합니다.

```
network device-discovery show -node node -protocol lldp
```

다음 명령을 실행하면 노드 클러스터-1_01의 포트에 연결된 인접 항목이 표시됩니다. 출력에는 지정된 노드의 각 포트에 연결된 LLDP 지원 디바이스가 나열됩니다. '-protocol' 옵션을 생략하면 출력에 CDP 지원 디바이스도 나열됩니다.

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

LLDP 광고 전송 간격을 조정합니다

LLDP 광고는 주기적으로 LLDP 이웃에게 전송됩니다. 네트워크 트래픽과 네트워크 토폴로지의 변경 내용에 따라 LLDP 광고 전송 간격을 늘리거나 줄일 수 있습니다.

이 작업에 대해

IEEE에서 권장하는 기본 간격은 30초이지만 5초에서 300초까지 값을 입력할 수 있습니다.

단계

1. 노드 또는 클러스터의 모든 노드에 대한 현재 LLDP 광고 시간 간격을 표시합니다.
   - 단일 노드:

     ```
     run -node <node_name> options lldp.xmit.interval
     ```

   - 모든 노드:

     ```
     options lldp.xmit.interval
     ```

2. 노드의 모든 포트 또는 클러스터의 모든 노드에 대해 LLDP 광고를 전송하는 간격을 조정합니다.
   - 단일 노드:

     ```
     run -node <node_name> options lldp.xmit.interval <interval>
     ```

   - 모든 노드:

     ```
     options lldp.xmit.interval <interval>
     ```

LLDP 광고의 실시간 값을 조정합니다

TTL(Time-to-Live)은 인접 LLDP 호환 장치의 캐시에 LLDP 광고가 저장되는 기간입니다. TTL은 각 LLDP 패킷에서 공고되며 LLDP 패킷이 노드에 수신될 때마다 업데이트됩니다. TTL은 나가는 LLDP 프레임에서 수정할 수 있습니다.

이 작업에 대해

- TTL은 전송 간격(모든 dp.xmit.interval`) 및 보류 승수(모든 dP.xmit.hold)에 1을 더한 계산된 값입니다.
- 기본 보압 승수 값은 4이지만 1에서 100 사이의 값을 입력할 수 있습니다.
- 따라서 기본 TTL은 IEEE에서 권장하는 121초이지만 전송 간격 및 고정 승수 값을 조정하여 발신 프레임의 값을 6초에서 30001초로 지정할 수 있습니다.
- TTL이 만료되기 전에 IP 주소를 제거하면 TTL이 만료될 때까지 LLDP 정보가 캐싱됩니다.

단계

1. 노드 또는 클러스터의 모든 노드에 대한 현재 보류 승수 값을 표시합니다.

◦ 단일 노드:

```
run -node <node_name> options lldp.xmit.hold
```

◦ 모든 노드:

```
options lldp.xmit.hold
```

2. 노드의 모든 포트 또는 클러스터의 모든 노드 포트에서 고정 승수 값을 조정합니다.

◦ 단일 노드:

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

◦ 모든 노드:

```
options lldp.xmit.hold <hold_value>
```

LLDP 통계를 보거나 지웁니다

각 노드의 클러스터 및 비 클러스터 포트에 대한 LLDP 통계를 보고 잠재적인 네트워크 연결 문제를 감지할 수 있습니다. LLDP 통계는 마지막 삭제 시점으로부터 누적됩니다.

이 작업에 대해

ONTAP 9.10.1 이하의 경우 클러스터 포트에 대해 LLDP가 항상 활성화되므로 해당 포트의 트래픽에 대해 LLDP 통계가 항상 표시됩니다. 해당 포트에 대한 통계가 표시되도록 비 클러스터 포트에서 LLDP가 활성화되어 있어야 합니다.

ONTAP 9.11.1 이상에서는 클러스터 및 스토리지 포트에 대해 LLDP가 항상 활성화되므로 해당 포트의 트래픽에 대해 LLDP 통계가 항상 표시됩니다. 해당 포트에 대한 통계가 표시되도록 클러스터 이외의 포트와 스토리지 이외의 포트에서 LLDP가 활성화되어 있어야 합니다.

단계

노드의 모든 포트에 대한 현재 LLDP 통계를 표시하거나 지웁니다.

원하는 작업	입력…
LLDP 통계를 봅니다	'run-node_name lldp stats'
LLDP 통계를 지웁니다	'run-node_name lldp stats-z'를 선택합니다

통계 예제를 표시하고 지웁니다

다음 명령을 실행하면 LLDP 통계가 지워지기 전에 표시됩니다. 마지막 통계 삭제 이후 송수신된 총 패킷 수가 출력에

표시됩니다.

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
 Total frames:     190k  | Accepted frames:   190k | Total drops:
0
TRANSMIT
 Total frames:     5195  | Total failures:      0
OTHER
 Stored entries:      64
```

다음 명령을 실행하면 LLDP 통계가 지워집니다.

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
 Total frames:        0  | Accepted frames:     0  | Total drops:
0
TRANSMIT
 Total frames:        0  | Total failures:      0
OTHER
 Stored entries:      64
```

통계를 지운 후 다음 LLDP 보급 알림이 전송되거나 수신된 후에 누적되기 시작합니다.

NAS 스토리지 관리

System Manager로 NAS 프로토콜을 관리합니다

ONTAP System Manager를 사용한 NAS 관리에 대해 알아보세요

이 섹션에서는 ONTAP 9.7 이상 릴리즈에서 System Manager를 사용하여 NAS 환경을 구성하고 관리하는 방법을 설명합니다.

클래식 시스템 관리자(ONTAP 9.7 이전에서만 사용 가능)를 사용하는 경우 다음 항목을 참조하십시오.

- "NFS 구성 개요"
- "SMB 구성 개요"

System Manager는 다음과 같은 워크플로우를 지원합니다.

- NAS 파일 서비스에 사용할 클러스터의 초기 구성입니다.
- 변화하는 스토리지 요구사항에 부합하는 추가 볼륨 프로비저닝
- 업계 표준 인증 및 보안 시설을 위한 구성 및 유지 보수

System Manager를 사용하면 구성 요소 레벨에서 NAS 서비스를 관리할 수 있습니다.

- 프로토콜 - NFS, SMB 또는 둘 다(NAS 멀티 프로토콜)
- 이름 서비스 - DNS, LDAP 및 NIS
- 네임 서비스 스위치
- Kerberos 및 TLS 보안
- 수출 및 공유
- Qtree
- 사용자 및 그룹의 이름 매핑

ONTAP System Manager를 사용하여 VMware 데이터 저장소에 NFS 스토리지 프로비저닝

VMware vSphere(VSC)용 가상 스토리지 콘솔을 사용하여 ESXi 호스트용 ONTAP 기반 스토리지 시스템에서 NFS 볼륨을 프로비저닝하기 전에 ONTAP 9.7 이상용 System Manager를 사용하여 NFS를 사용하도록 설정하십시오.

을 만든 후 "NFS 지원 스토리지 VM" System Manager에서 NFS 볼륨을 프로비저닝하고 VSC를 사용하여 데이터 저장소를 관리할 수 있습니다.

VSC 7.0부터는 VSC가 의 일부입니다 "VMware vSphere 가상 어플라이언스인 ONTAP 툴"VSC, VASA(vStorage APIs for Storage Awareness) 공급자, VMware vSphere 기능을 위한 SRA(Storage Replication Adapter) 등이 포함되어 있습니다.

를 확인하십시오 "NetApp 상호 운용성 매트릭스" 현재 ONTAP 및 VSC 릴리스 간의 호환성을 확인합니다.

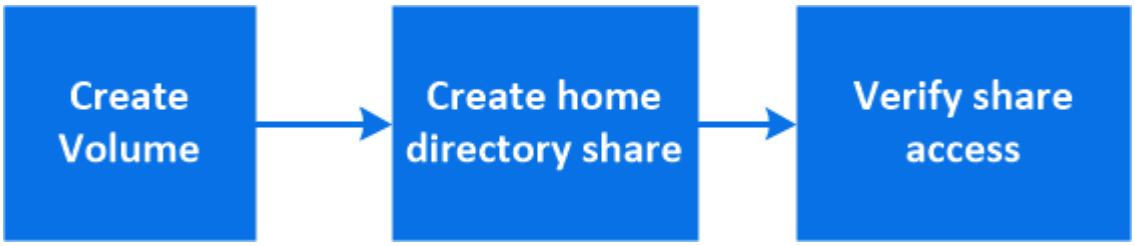
System Manager Classic(ONTAP 9.7 이하 릴리즈용)을 사용하여 ESXi 호스트에 대한 NFS 액세스를 데이터 저장소에 설정하려면 를 참조하십시오 "VSC 개요를 사용한 ESXi용 NFS 구성"

자세한 내용은 을 참조하십시오 "TR-4597: ONTAP용 VMware vSphere" VSC 릴리즈에 대한 설명서를 제공합니다.

ONTAP 시스템 관리자를 사용하여 홈 디렉토리에 대한 NAS 스토리지 제공

볼륨을 생성하여 SMB 프로토콜을 사용하여 홈 디렉토리에 대한 스토리지를 제공합니다.

이 절차를 수행하면 의 홈 디렉토리에 대한 새 볼륨이 생성됩니다 "기존 SMB 지원 스토리지 VM". 볼륨을 구성하거나 사용자 지정 구성을 지정할 때 시스템 기본값을 사용할 수 있습니다.



FlexVol 볼륨을 만들거나, 높은 성능 요구 사항이 있는 대규모 파일 시스템의 경우 FlexGroup 볼륨을 만들 수 있습니다. 또한 참조하세요"FlexGroup 볼륨을 생성합니다" .

또한 이 볼륨의 사양을 Ansible 플레이북에 저장할 수도 있습니다. 자세한 내용은 를 참조하십시오 "Ansible 플레이북을 사용하여 볼륨 또는 LUN을 추가 또는 편집합니다".

단계

1. SMB 지원 스토리지 VM에 새 볼륨을 추가합니다.
   a. 스토리지 > 볼륨 * 을 선택한 다음 * 추가 * 를 클릭합니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력합니다.

      SMB 프로토콜로 구성된 스토리지 VM만 나열됩니다. SMB 프로토콜로 구성된 스토리지 VM을 하나만 사용할 수 있는 경우 * 스토리지 VM * 필드가 표시되지 않습니다.

      - 이때 * 저장 * 을 클릭하면 시스템 관리자가 시스템 기본값을 사용하여 FlexVol 볼륨을 생성하고 추가합니다.
      - 추가 옵션 * 을 클릭하여 권한 부여, 서비스 품질 및 데이터 보호와 같은 서비스를 사용하도록 볼륨 구성을 사용자 지정할 수 있습니다. 을 참조하십시오 볼륨 구성을 사용자 지정합니다그런 다음 여기로 돌아와 다음 단계를 완료합니다.
2. [[워크플로의 2단계, 2단계]] * 스토리지 > 공유 * 를 클릭하고 * 추가 * 를 클릭한 다음 * 홈 디렉토리 * 를 선택합니다.
3. Windows 클라이언트에서 다음을 수행하여 공유에 액세스할 수 있는지 확인합니다.
   a. Windows 탐색기에서 드라이브를 다음 형식으로 공유에 매핑합니다.
      `\\<SMB_Server_Name>\<Share_Name>`

      공유 이름이 변수(%w, %d 또는 %u)로 생성된 경우, 확인된 이름으로 액세스를 테스트하십시오.

   b. 새로 만든 드라이브에서 테스트 파일을 만든 다음 파일을 삭제합니다.

볼륨 구성을 사용자 지정합니다

시스템 기본값을 수락하는 대신 볼륨을 추가할 때 볼륨 구성을 사용자 지정할 수 있습니다.

단계

추가 옵션 * 을 클릭한 후 필요한 기능을 선택하고 필요한 값을 입력합니다.

- 원격 볼륨의 캐시입니다.
- 성능 서비스 수준(서비스 품질, QoS):

  ONTAP 9.8부터 사용자 지정 QoS 정책을 지정하거나 QoS를 사용하지 않도록 설정할 수 있으며, 기본 값 선택도 가능합니다.

  - QoS를 비활성화하려면 * 사용자 정의 *, * 기존 *, * 없음 * 을 차례로 선택합니다.
  - 사용자 정의 * 를 선택하고 기존 서비스 수준을 지정하면 로컬 계층이 자동으로 선택됩니다.
  - ONTAP 9.9.1부터 사용자 지정 성능 서비스 수준을 생성하기로 선택한 경우, 시스템 관리자를 사용하여 생성 중인 볼륨을 배치할 로컬 계층(* 수동 배치*)을 수동으로 선택할 수 있습니다.

    원격 캐시 또는 FlexGroup 볼륨 옵션을 선택한 경우에는 이 옵션을 사용할 수 없습니다.

- FlexGroup 볼륨(* 클러스터 전체에 볼륨 데이터 배포 * 선택).

  이전에 * Performance Service Level * 에서 * Manual Placement * 를 선택한 경우에는 이 옵션을 사용할 수 없습니다. 그렇지 않으면 추가하려는 볼륨이 기본적으로 FlexVol 볼륨이 됩니다.

- 볼륨이 구성된 프로토콜에 대한 액세스 권한
- SnapMirror(로컬 또는 원격)를 통한 데이터 보호를 선택한 다음 풀다운 목록에서 대상 클러스터에 대한 보호 정책 및 설정을 지정합니다.
- 저장 * 을 선택하여 볼륨을 생성하고 클러스터 및 스토리지 VM에 추가합니다.

볼륨을 저장한 후 로 돌아갑니다 [step2] 홈 디렉토리에 대한 프로비저닝을 완료합니다.

ONTAP System Manager를 사용하여 NFS를 사용하여 Linux 서버용 NAS 스토리지 프로비저닝

ONTAP System Manager(9.7 이상)에서 NFS 프로토콜을 사용하여 Linux 서버용 스토리지를 제공할 볼륨을 생성합니다.

이 절차를 수행하면 에 새 볼륨이 생성됩니다 "기존 NFS 지원 스토리지 VM". 볼륨을 구성하거나 사용자 지정 구성을 지정할 때 시스템 기본값을 사용할 수 있습니다.

FlexVol 볼륨을 만들거나, 높은 성능 요구 사항이 있는 대규모 파일 시스템의 경우 FlexGroup 볼륨을 만들 수 있습니다. 또한 참조하세요"FlexGroup 볼륨을 생성합니다" .

또한 이 볼륨의 사양을 Ansible 플레이북에 저장할 수도 있습니다. 자세한 내용은 를 참조하십시오 "Ansible 플레이북을 사용하여 볼륨 또는 LUN을 추가 또는 편집합니다".

다양한 ONTAP NFS 프로토콜 기능에 대한 자세한 내용은 를 참조하십시오"NFS 프로토콜에 대한 ONTAP 파일 액세스에 대해 알아보세요".

단계

1. NFS 지원 스토리지 VM에 새 볼륨을 추가합니다.
   a. 스토리지 > 볼륨 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력합니다.

      NFS 프로토콜로 구성된 스토리지 VM만 나열됩니다. SMB 프로토콜로 구성된 스토리지 VM을 하나만 사용할 수 있는 경우 * 스토리지 VM * 필드가 표시되지 않습니다.

      - 이때 * 저장 * 을 클릭하면 시스템 관리자가 시스템 기본값을 사용하여 FlexVol 볼륨을 생성하고 추가합니다.

        기본 엑스포트 정책은 모든 사용자에게 전체 액세스 권한을 부여합니다.

      - 추가 옵션 * 을 클릭하여 권한 부여, 서비스 품질 및 데이터 보호와 같은 서비스를 사용하도록 볼륨 구성을 사용자 지정할 수 있습니다. 을 참조하십시오 볼륨 구성을 사용자 지정합니다그런 다음 여기로 돌아와 다음 단계를 완료합니다.
2. Linux 클라이언트에서 다음을 수행하여 액세스를 확인합니다.
   a. 스토리지 VM의 네트워크 인터페이스를 사용하여 볼륨을 생성하고 마운트합니다.
   b. 새로 마운트된 볼륨에서 테스트 파일을 생성하고 텍스트를 기록한 다음 파일을 삭제합니다.

액세스를 확인한 후 을(를) 사용할 수 있습니다 "볼륨의 엑스포트 정책으로 클라이언트 액세스 제한" 마운트된 볼륨에 대해 원하는 UNIX 소유권 및 권한을 설정합니다.

볼륨 구성을 사용자 지정합니다

시스템 기본값을 수락하는 대신 볼륨을 추가할 때 볼륨 구성을 사용자 지정할 수 있습니다.

단계

추가 옵션 * 을 클릭한 후 필요한 기능을 선택하고 필요한 값을 입력합니다.

- 원격 볼륨의 캐시입니다.
- 성능 서비스 수준(서비스 품질, QoS):

  ONTAP 9.8부터 사용자 지정 QoS 정책을 지정하거나 QoS를 사용하지 않도록 설정할 수 있으며, 기본 값 선택도 가능합니다.

  - QoS를 비활성화하려면 * 사용자 정의 *, * 기존 *, * 없음 * 을 차례로 선택합니다.
  - 사용자 정의 * 를 선택하고 기존 서비스 수준을 지정하면 로컬 계층이 자동으로 선택됩니다.
  - ONTAP 9.9.1부터 사용자 지정 성능 서비스 수준을 생성하기로 선택한 경우, 시스템 관리자를 사용하여 생성 중인 볼륨을 배치할 로컬 계층(* 수동 배치*)을 수동으로 선택할 수 있습니다.

    원격 캐시 또는 FlexGroup 볼륨 옵션을 선택한 경우에는 이 옵션을 사용할 수 없습니다.

- FlexGroup 볼륨(* 클러스터 전체에 볼륨 데이터 배포 * 선택).

  이전에 * Performance Service Level * 에서 * Manual Placement * 를 선택한 경우에는 이 옵션을 사용할 수 없습니다. 그렇지 않으면 추가하려는 볼륨이 기본적으로 FlexVol 볼륨이 됩니다.

- 볼륨이 구성된 프로토콜에 대한 액세스 권한
- SnapMirror(로컬 또는 원격)를 통한 데이터 보호를 선택한 다음 풀다운 목록에서 대상 클러스터에 대한 보호 정책 및 설정을 지정합니다.
- 저장 * 을 선택하여 볼륨을 생성하고 클러스터 및 스토리지 VM에 추가합니다.

볼륨을 저장한 후 로 돌아갑니다 Step 2 in the workflow NFS를 사용하여 Linux 서버의 프로비저닝을 완료하려면 다음을 수행합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

이 작업을 수행하는 방법	자세한 내용은…
System Manager Classic(ONTAP 9.7 이하)	"NFS 구성 개요"
ONTAP CLI(Command Line Interface)	"ONTAP CLI를 사용한 NFS 구성에 대해 알아보십시오"

ONTAP System Manager를 사용하여 내보내기 정책을 사용하여 액세스 관리

내보내기 정책을 사용하여 NFS 서버에 대한 Linux 클라이언트 액세스를 설정합니다.

이 절차는 에 대한 엑스포트 정책을 생성하거나 수정합니다 "기존 NFS 지원 스토리지 VM".

단계

1. System Manager에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. NFS 지원 볼륨을 클릭하고 * More * 를 클릭합니다.
3. Edit Export Policy * 를 클릭한 다음 * Select an existing policy * 또는 * Add a new policy * 를 클릭합니다.

ONTAP 시스템 관리자를 사용하여 **SMB**를 사용하여 **Windows** 서버용 **NAS** 스토리지 프로비저닝

ONTAP 9.7 이상에서 사용할 수 있는 System Manager를 사용하여 SMB 프로토콜을 사용하여 Windows 서버용 스토리지를 제공할 볼륨을 생성합니다.

이 절차를 수행하면 에 새 볼륨이 생성됩니다 "기존 SMB 지원 스토리지 VM" 볼륨 루트(/) 디렉토리에 대한 공유를 생성합니다. 볼륨을 구성하거나 사용자 지정 구성을 지정할 때 시스템 기본값을 사용할 수 있습니다. 초기 SMB 구성 후 추가 공유를 생성하고 해당 속성을 수정할 수도 있습니다.

FlexVol 볼륨을 만들거나, 높은 성능 요구 사항이 있는 대규모 파일 시스템의 경우 FlexGroup 볼륨을 만들 수 있습니다. 또한 참조하세요"FlexGroup 볼륨을 생성합니다" .

또한 이 볼륨의 사양을 Ansible 플레이북에 저장할 수도 있습니다. 자세한 내용은 를 참조하십시오 "Ansible 플레이북을 사용하여 볼륨 또는 LUN을 추가 또는 편집합니다".

다양한 ONTAP SMB 프로토콜 기능에 대한 자세한 내용은 를 참조하십시오"참고 개요".

시작하기 전에

- ONTAP 9.13.1부터 새로운 볼륨에 대해 용량 분석 및 활동 추적을 기본적으로 사용할 수 있습니다. System Manager에서 클러스터 또는 스토리지 VM 레벨의 기본 설정을 관리할 수 있습니다. 자세한 내용은 을 "파일 시스템

분석 설정"참조하십시오.

단계

1. SMB 지원 스토리지 VM에 새 볼륨을 추가합니다.
   a. 스토리지 > 볼륨 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력합니다.

      SMB 프로토콜로 구성된 스토리지 VM만 나열됩니다. SMB 프로토콜로 구성된 스토리지 VM을 하나만 사용할 수 있는 경우 * 스토리지 VM * 필드가 표시되지 않습니다.

      - 이때 * 저장 * 을 선택하면 시스템 관리자가 시스템 기본값을 사용하여 FlexVol 볼륨을 생성하고 추가합니다.
      - 추가 옵션 * 을 선택하여 권한 부여, 서비스 품질 및 데이터 보호와 같은 서비스를 사용할 수 있도록 볼륨 구성을 사용자 지정할 수 있습니다. 을 참조하십시오 볼륨 구성을 사용자 지정합니다그런 다음 여기로 돌아와 다음 단계를 완료합니다.
2. 공유에 액세스할 수 있는지 확인하기 위해 Windows 클라이언트로 전환합니다.
   a. Windows 탐색기에서 '_SMB_Server_Name__Share_Name_' 형식으로 드라이브를 공유에 매핑합니다
   b. 새로 생성된 드라이브에서 테스트 파일을 만들고 텍스트를 기록한 다음 파일을 삭제합니다.

액세스를 확인한 후 공유 ACL을 사용하여 클라이언트 액세스를 제한하고 매핑된 드라이브에서 원하는 보안 속성을 설정할 수 있습니다. 자세한 내용은 을 "공유 만들기" 참조하십시오.

공유를 추가하거나 수정합니다

초기 SMB 구성 후 공유를 추가할 수 있습니다. 공유는 사용자가 선택한 기본 값과 속성으로 생성됩니다. 나중에 수정할 수 있습니다.

공유를 구성할 때 다음 공유 속성을 설정할 수 있습니다.

- 액세스 권한
- 공유 속성
  - SMB 데이터를 통해 Hyper-V 및 SQL Server를 포함하는 공유에 대해 지속적인 가용성을 지원합니다(ONTAP 9.10.1부터 시작). 참고 항목:
    - "SMB를 통한 Hyper-V의 지속적인 가용성 공유 요구사항"
    - "SMB를 통한 SQL Server의 지속적인 가용성 공유 요구 사항"
  - 이 공유에 액세스하는 동안 SMB 3.0으로 데이터를 암호화합니다.

초기 설정 후 다음 속성을 수정할 수도 있습니다.

- 심볼 링크
  - symlink와 Wipelink를 설정하거나 해제합니다
- 공유 속성
  - 클라이언트가 스냅샷 디렉토리에 액세스할 수 있도록 허용합니다.
  - oplocks를 설정하여 클라이언트가 파일을 잠그고 컨텐츠를 로컬에서 캐시할 수 있도록 합니다(기본값).

◦ 사용자의 액세스 권한을 기반으로 공유 리소스를 표시하려면 ABE(액세스 기반 열거)를 사용합니다.

단계

1. SMB 지원 볼륨에 새 공유를 추가하려면 스토리지 > 공유 를 클릭하고 추가 를 클릭한 다음 공유 를 선택합니다.
2. 기존 공유를 수정하려면 스토리지 > 공유 를 클릭한 다음 ⋮ 편집 을 선택합니다.

볼륨 구성을 사용자 지정합니다

시스템 기본값을 수락하는 대신 볼륨을 추가할 때 볼륨 구성을 사용자 지정할 수 있습니다.

단계

추가 옵션 * 을 클릭한 후 필요한 기능을 선택하고 필요한 값을 입력합니다.

- 원격 볼륨의 캐시입니다.
- 성능 서비스 수준(서비스 품질, QoS):

  ONTAP 9.8부터 사용자 지정 QoS 정책을 지정하거나 QoS를 사용하지 않도록 설정할 수 있으며, 기본 값 선택도 가능합니다.

  ◦ QoS를 비활성화하려면 * 사용자 정의 *, * 기존 *, * 없음 * 을 차례로 선택합니다.

  ◦ 사용자 정의 * 를 선택하고 기존 서비스 수준을 지정하면 로컬 계층이 자동으로 선택됩니다.

  ◦ ONTAP 9.9.1부터 사용자 지정 성능 서비스 수준을 생성하기로 선택한 경우, 시스템 관리자를 사용하여 생성 중인 볼륨을 배치할 로컬 계층(* 수동 배치*)을 수동으로 선택할 수 있습니다.

  원격 캐시 또는 FlexGroup 볼륨 옵션을 선택한 경우에는 이 옵션을 사용할 수 없습니다.

- FlexGroup 볼륨(* 클러스터 전체에 볼륨 데이터 배포 * 선택).

  이전에 * Performance Service Level * 에서 * Manual Placement * 를 선택한 경우에는 이 옵션을 사용할 수 없습니다. 그렇지 않으면 추가하려는 볼륨이 기본적으로 FlexVol 볼륨이 됩니다.

- 볼륨이 구성된 프로토콜에 대한 액세스 권한
- SnapMirror(로컬 또는 원격)를 통한 데이터 보호를 선택한 다음 풀다운 목록에서 대상 클러스터에 대한 보호 정책 및 설정을 지정합니다.
- 저장 * 을 선택하여 볼륨을 생성하고 클러스터 및 스토리지 VM에 추가합니다.

ⓘ 볼륨을 저장한 후 로 돌아갑니다 [step2-compl-prov-win] SMB를 사용하여 Windows 서버에 대한 프로비저닝을 완료하려면 다음을 수행합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

이 작업을 수행하는 방법	자세한 내용은…
System Manager Classic(ONTAP 9.7 이하)	"SMB 구성 개요"
ONTAP 명령줄 인터페이스입니다	"CLI를 사용한 SMB 구성 개요"

ONTAP System Manager를 사용하여 NFS와 SMB를 모두 사용하여 Windows와 Linux 모두에 대한 NAS 스토리지를 프로비저닝합니다.

NFS 또는 SMB 프로토콜을 사용하여 클라이언트에 스토리지를 제공할 볼륨을 생성합니다.

이 절차를 수행하면 에 새 볼륨이 생성됩니다 "NFS 및 SMB 프로토콜 모두에 대해 설정된 기존 스토리지 VM".

NFS 프로토콜은 일반적으로 Linux 환경에서 사용됩니다. SMB 프로토콜은 일반적으로 Windows 환경에서 사용됩니다. 그러나 NFS와 SMB는 모두 Linux 또는 Windows에서 사용할 수 있습니다.

FlexVol 볼륨을 만들거나, 높은 성능 요구 사항이 있는 대규모 파일 시스템의 경우 FlexGroup 볼륨을 만들 수 있습니다. 보다"FlexGroup 볼륨을 생성합니다" .

또한 이 볼륨의 사양을 Ansible 플레이북에 저장할 수도 있습니다. 자세한 내용은 를 참조하십시오 "Ansible 플레이북을 사용하여 볼륨 또는 LUN을 추가 또는 편집합니다".

단계

1. NFS와 SMB 모두에 대해 설정된 스토리지 VM에 새 볼륨을 추가합니다.

   a. 스토리지 > 볼륨 * 을 클릭한 다음 * 추가 * 를 클릭합니다.

   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력합니다.

      NFS 및 SMB 프로토콜을 모두 사용하여 구성된 스토리지 VM만 나열됩니다. NFS 및 SMB 프로토콜로 구성된 스토리지 VM을 하나만 사용할 수 있는 경우 * 스토리지 VM * 필드가 표시되지 않습니다.

   c. More Options * 를 클릭하고 * Export via NFS * 를 선택합니다.

      기본 설정은 모든 사용자에게 전체 액세스 권한을 부여합니다. 나중에 내보내기 정책에 더 제한적인 규칙을 추가할 수 있습니다.

   d. Share via SMB/CIFS * 를 선택합니다.

      공유는 * Everyone * 그룹에 대해 "모든 권한"으로 설정된 기본 ACL(액세스 제어 목록)으로 생성됩니다. 나중에 ACL에 제한을 추가할 수 있습니다.

   e. 이때 * 저장 * 을 클릭하면 시스템 관리자가 시스템 기본값을 사용하여 FlexVol 볼륨을 생성하고 추가합니다.

   또는 인증, 서비스 품질 및 데이터 보호와 같은 추가 필수 서비스를 계속 활성화할 수도 있습니다. 을 참조하십시오 볼륨 구성을 사용자 지정합니다그런 다음 여기로 돌아와 다음 단계를 완료합니다.

2. Linux 클라이언트에서 내보내기에 액세스할 수 있는지 확인합니다.

   a. 스토리지 VM의 네트워크 인터페이스를 사용하여 볼륨을 생성하고 마운트합니다.

   b. 새로 마운트된 볼륨에서 테스트 파일을 생성하고 텍스트를 기록한 다음 파일을 삭제합니다.

3. Windows 클라이언트에서 다음을 수행하여 공유에 액세스할 수 있는지 확인합니다.

a. Windows 탐색기에서 '_SMB_Server_Name__Share_Name_' 형식으로 드라이브를 공유에 매핑합니다

b. 새로 생성된 드라이브에서 테스트 파일을 만들고 텍스트를 기록한 다음 파일을 삭제합니다.

액세스를 확인한 후 "볼륨의 엑스포트 정책으로 클라이언트 액세스를 제한하고 공유 ACL로 클라이언트 액세스를 제한합니다"내보낸 볼륨 및 공유 볼륨에 대해 원하는 소유권 및 권한을 설정할 수 있습니다.

볼륨 구성을 사용자 지정합니다

시스템 기본값을 수락하는 대신 볼륨을 추가할 때 볼륨 구성을 사용자 지정할 수 있습니다.

단계

추가 옵션 * 을 클릭한 후 필요한 기능을 선택하고 필요한 값을 입력합니다.

- 원격 볼륨의 캐시입니다.
- 성능 서비스 수준(서비스 품질, QoS):

  ONTAP 9.8부터 사용자 지정 QoS 정책을 지정하거나 QoS를 사용하지 않도록 설정할 수 있으며, 기본 값 선택도 가능합니다.

  - QoS를 비활성화하려면 * 사용자 정의 *, * 기존 *, * 없음 * 을 차례로 선택합니다.
  - 사용자 정의 * 를 선택하고 기존 서비스 수준을 지정하면 로컬 계층이 자동으로 선택됩니다.
  - ONTAP 9.9.1부터 사용자 지정 성능 서비스 수준을 생성하기로 선택한 경우, 시스템 관리자를 사용하여 생성 중인 볼륨을 배치할 로컬 계층(* 수동 배치*)을 수동으로 선택할 수 있습니다.

    원격 캐시 또는 FlexGroup 볼륨 옵션을 선택한 경우에는 이 옵션을 사용할 수 없습니다.

- FlexGroup 볼륨(* 클러스터 전체에 볼륨 데이터 배포 * 선택).

  이전에 * Performance Service Level * 에서 * Manual Placement * 를 선택한 경우에는 이 옵션을 사용할 수 없습니다. 그렇지 않으면 추가하려는 볼륨이 기본적으로 FlexVol 볼륨이 됩니다.

- 볼륨이 구성된 프로토콜에 대한 액세스 권한
- SnapMirror(로컬 또는 원격)를 통한 데이터 보호를 선택한 다음 풀다운 목록에서 대상 클러스터에 대한 보호 정책 및 설정을 지정합니다.
- 저장 * 을 선택하여 볼륨을 생성하고 클러스터 및 스토리지 VM에 추가합니다.

볼륨을 저장한 후 로 돌아갑니다 [step2-compl-prov-nfs-smb] Windows 및 Linux 서버에 대한 멀티프로토콜 프로비저닝을 완료합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하)	"SMB 및 NFS 멀티 프로토콜 구성 개요"

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
ONTAP 명령줄 인터페이스입니다	• "CLI를 사용한 SMB 구성 개요" • "ONTAP CLI를 사용한 NFS 구성에 대해 알아보십시오" • "보안 스타일과 그 효과에 대해 알아보세요" • "다중 프로토콜 환경에서 파일 및 디렉토리 이름의 대/소문자를 구분하십시오"

ONTAP System Manager를 사용하여 Kerberos로 클라이언트 액세스 보안

NAS 클라이언트에 대한 스토리지 액세스를 보호하기 위해 Kerberos를 설정합니다.

이 절차에서는 에 대해 설정된 기존 스토리지 VM에서 Kerberos를 구성합니다 "NFS 를 참조하십시오" 또는 "중소기업".

시작하기 전에 DNS, NTP 및 를 구성해야 합니다 "LDAP를 지원합니다" 스토리지 시스템에서

단계

1. ONTAP 명령줄에서 스토리지 VM 루트 볼륨에 대한 UNIX 권한을 설정합니다.

   a. 스토리지 VM 루트 볼륨에 대한 관련 권한을 표시합니다 `volume show -volume root_vol_name -fields user,group,unix-permissions`. 에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

      스토리지 VM의 루트 볼륨에는 다음 구성이 있어야 합니다.

이름...	설정 중...
UID	루트 또는 ID 0
GID	루트 또는 ID 0
Unix 사용 권한	755

   a. 이러한 값이 표시되지 않으면 `volume modify` 명령을 사용하여 값을 업데이트합니다. 에 대한 자세한 내용은 `volume modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 스토리지 VM 루트 볼륨에 대한 사용자 권한을 설정합니다.

   a. 로컬 UNIX 사용자를 표시합니다 `vserver services name-service unix-user show -vserver vserver_name`. 에 대한 자세한 내용은 `vserver services name-service unix-user show` "ONTAP 명령 참조입니다"을 참조하십시오.

      스토리지 VM에는 다음과 같은 UNIX 사용자가 구성되어 있어야 합니다.

사용자 이름입니다	사용자 **ID**입니다	기본 그룹 **ID**입니다
NFS 를 참조하십시오	500입니다	0
루트	0	0

+

- 참고: * NFS 클라이언트 사용자의 SPN에 대한 Kerberos-UNIX 이름 매핑이 있는 경우 NFS 사용자는 필요하지 않습니다. 5단계를 참조하십시오.

  a. 이러한 값이 표시되지 않으면 `vserver services name-service unix-user modify` 명령을 사용하여 값을 업데이트합니다. 에 대한 자세한 내용은 `vserver services name-service unix-user modify` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 스토리지 VM 루트 볼륨에 대한 그룹 권한을 설정합니다.

   a. 로컬 UNIX 그룹을 표시합니다 `vserver services name-service unix-group show -vserver` *`vserver_name`*. 에 대한 자세한 내용은 `vserver services name-service unix-group show` "ONTAP 명령 참조입니다"을 참조하십시오.

      스토리지 VM에는 다음과 같은 UNIX 그룹이 구성되어 있어야 합니다.

그룹 이름	그룹 **ID**입니다
데몬	1
루트	0

   a. 이러한 값이 표시되지 않으면 `vserver services name-service unix-group modify` 명령을 사용하여 값을 업데이트합니다. 에 대한 자세한 내용은 `vserver services name-service unix-group modify` "ONTAP 명령 참조입니다"을 참조하십시오.

4. Kerberos를 구성하려면 System Manager로 전환합니다
5. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택합니다.
6. 설정 * 을 클릭합니다.
7. Kerberos 아래에서 를 → 클릭합니다.
8. Kerberos 영역 아래에서 * 추가 * 를 클릭하고 다음 섹션을 완료합니다.
   - Kerberos 영역 추가

     KDC 공급업체에 따라 구성 세부 정보를 입력합니다.

   - Realm에 네트워크 인터페이스를 추가합니다

     추가 * 를 클릭하고 네트워크 인터페이스를 선택합니다.

9. 필요한 경우 Kerberos 사용자 이름에서 로컬 사용자 이름으로 매핑을 추가합니다.
   a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택합니다.
   b. 설정 * 을 클릭한 다음 * 이름 매핑 * 아래에서 를 → 클릭합니다.
   c. UNIX * 에 대한 Kerberos * 에서 정규식을 사용하여 패턴 및 교체를 추가합니다.

ONTAP 시스템 관리자를 사용하여 이름 서비스를 통해 클라이언트 액세스를 제공합니다.

ONTAP에서 LDAP 또는 NIS를 사용하여 호스트, 사용자, 그룹 또는 넷그룹 정보를 조회하여 NAS 클라이언트를 인증합니다.

이 절차는 에 대해 설정된 기존 스토리지 VM에 대한 LDAP 또는 NIS 구성을 생성하거나 수정합니다 "NFS 를 참조하십시오" 또는 "중소기업".

LDAP 구성의 경우 환경에 필요한 LDAP 구성 세부 정보가 있어야 하며 기본 ONTAP LDAP 스키마를 사용해야 합니다.

단계

1. 필요한 서비스를 구성합니다. * 스토리지 > 스토리지 VM * 을 클릭합니다.
2. 스토리지 VM을 선택하고 * Settings * 를 클릭한 다음 LDAP 또는 NIS를 클릭합니다.
3. 이름 서비스 스위치의 변경 내용 포함: 이름 서비스 스위치 아래에서 를 클릭합니다 .

ONTAP System Manager를 사용하여 디렉토리 및 파일 관리

System Manager 볼륨 표시를 확장하여 디렉토리 및 파일을 보고 삭제합니다.

ONTAP 9.9.1부터 지연 시간이 짧은 비동기 디렉토리 삭제 기능으로 디렉토리가 삭제됩니다.

ONTAP 9.9.1 이상에서 파일 시스템을 보는 방법에 대한 자세한 내용은 을 참조하십시오 "파일 시스템 분석 개요".

단계

1. 스토리지 > 볼륨 * 을 선택합니다. 볼륨을 확장하여 내용을 봅니다.

ONTAP System Manager를 사용하여 호스트별 사용자 및 그룹 관리

ONTAP 9.10.1부터 System Manager를 사용하여 UNIX 또는 Windows 호스트별 사용자 및 그룹을 관리할 수 있습니다.

다음 절차를 수행할 수 있습니다.

Windows	Unix
• Windows 사용자 및 그룹을 봅니다 • [add-edit-delete-Windows] • [manage-windows-users]	• UNIX 사용자 및 그룹 보기 • [add-edit-delete-UNIX] • [manage-unix-users]

Windows 사용자 및 그룹을 봅니다

System Manager에서 Windows 사용자 및 그룹 목록을 볼 수 있습니다.

단계

1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭합니다.
2. 스토리지 VM을 선택한 다음 * 설정 * 탭을 선택합니다.

3. 호스트 사용자 및 그룹 * 영역으로 스크롤합니다.

   Windows * 섹션은 선택한 스토리지 VM과 연결된 각 그룹의 사용자 수에 대한 요약을 표시합니다.

4. →Windows * 섹션을 클릭합니다.
5. 그룹 * 탭을 클릭한 다음 그룹 이름 옆에 있는 을 ⌄ 클릭하여 해당 그룹에 대한 세부 정보를 봅니다.
6. 그룹의 사용자를 보려면 그룹을 선택한 다음 * 사용자 * 탭을 클릭합니다.

Windows 그룹을 추가, 편집 또는 삭제합니다

System Manager에서 Windows 그룹을 추가, 편집 또는 삭제하여 관리할 수 있습니다.

단계

1. System Manager에서 Windows 그룹 목록을 봅니다. 을 참조하십시오 Windows 사용자 및 그룹을 봅니다.
2. 그룹 * 탭에서 다음 작업으로 그룹을 관리할 수 있습니다.

이 작업을 수행하려면…	다음 단계를 수행합니다.
그룹을 추가합니다	1. 을 클릭합니다 + Add . 2. 그룹 정보를 입력합니다. 3. 권한을 지정합니다. 4. 그룹 구성원(로컬 사용자, 도메인 사용자 또는 도메인 그룹 추가)을 지정합니다.
그룹을 편집합니다	1. 그룹 이름 옆에 있는 을 ⋮클릭한 다음 * 편집 * 을 클릭합니다. 2. 그룹 정보를 수정합니다.
그룹을 삭제합니다	1. 삭제할 그룹 옆에 있는 확인란을 선택합니다. 2. 을 Delete 클릭합니다. ◦ 참고: * 그룹 이름 옆에 있는 을 클릭한 다음 * 삭제 * 를 클릭하여 단일 그룹을 삭제할 수도 ⋮ 있습니다.

Windows 사용자를 관리합니다

System Manager에서 Windows 사용자를 추가, 편집, 삭제, 활성화 또는 비활성화하여 관리할 수 있습니다. Windows 사용자의 암호를 변경할 수도 있습니다.

단계

1. System Manager에서 그룹의 사용자 목록을 봅니다. 을 참조하십시오 Windows 사용자 및 그룹을 봅니다.
2. 사용자 * 탭에서 다음 작업을 통해 사용자를 관리할 수 있습니다.

이 작업을 수행하려면…	다음 단계를 수행합니다.

사용자를 추가합니다	1. 을 클릭합니다 + Add . 2. 사용자 정보를 입력합니다.
사용자를 편집합니다	1. 사용자 이름 옆에 있는 을 ⋮ 클릭한 다음 * 편집 * 을 클릭합니다. 2. 사용자 정보를 수정합니다.
사용자를 삭제합니다	1. 삭제할 사용자 옆에 있는 확인란을 선택합니다. 2. 을 Delete 클릭합니다. ◦ 참고: * 사용자 이름 옆에 있는 을 클릭한 다음 * 삭제 * 를 클릭하여 단일 사용자를 삭제할 수도 ⋮ 있습니다.
사용자 암호를 변경합니다	1. 사용자 이름 옆에 있는 을 ⋮ 클릭한 다음 * 암호 변경 * 을 클릭합니다. 2. 새 암호를 입력하고 확인합니다.
사용자를 활성화합니다	1. 활성화할 비활성화된 각 사용자 옆에 있는 확인란을 선택합니다. 2. 을 Enable 클릭합니다.
사용자를 비활성화합니다	1. 비활성화할 각 활성화된 사용자 옆에 있는 확인란을 선택합니다. 2. 을 Disable 클릭합니다.

UNIX 사용자 및 그룹 보기

System Manager에서 UNIX 사용자 및 그룹 목록을 볼 수 있습니다.

단계

1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭합니다.
2. 스토리지 VM을 선택한 다음 * 설정 * 탭을 선택합니다.
3. 호스트 사용자 및 그룹 * 영역으로 스크롤합니다.

   UNIX * 섹션에는 선택한 스토리지 VM과 연결된 각 그룹의 사용자 수가 요약되어 표시됩니다.

4. UNIX * 섹션을 클릭합니다 → .
5. 그룹 * 탭을 클릭하여 해당 그룹에 대한 세부 정보를 봅니다.
6. 그룹의 사용자를 보려면 그룹을 선택한 다음 * 사용자 * 탭을 클릭합니다.

UNIX 그룹을 추가, 편집 또는 삭제합니다

System Manager에서는 UNIX 그룹을 추가, 편집 또는 삭제하여 관리할 수 있습니다.

단계

1. System Manager에서 UNIX 그룹 목록을 봅니다. 을 참조하십시오 UNIX 사용자 및 그룹 보기.
2. 그룹 * 탭에서 다음 작업으로 그룹을 관리할 수 있습니다.

이 작업을 수행하려면…	다음 단계를 수행합니다.
그룹을 추가합니다	1. 을 클릭합니다 + Add . 2. 그룹 정보를 입력합니다. 3. (선택 사항) 연결된 사용자를 지정합니다.
그룹을 편집합니다	1. 그룹을 선택합니다. 2. 을 클릭합니다 Edit . 3. 그룹 정보를 수정합니다. 4. (선택 사항) 사용자를 추가하거나 제거합니다.
그룹을 삭제합니다	1. 삭제할 그룹을 선택합니다. 2. 을 Delete 클릭합니다.

UNIX 사용자 관리

System Manager에서 Windows 사용자를 추가, 편집 또는 삭제하여 관리할 수 있습니다.

단계

1. System Manager에서 그룹의 사용자 목록을 봅니다. 을 참조하십시오 UNIX 사용자 및 그룹 보기.
2. 사용자 * 탭에서 다음 작업을 통해 사용자를 관리할 수 있습니다.

이 작업을 수행하려면…	다음 단계를 수행합니다.
사용자를 추가합니다	1. 을 클릭합니다 + Add . 2. 사용자 정보를 입력합니다.
사용자를 편집합니다	1. 편집할 사용자를 선택합니다. 2. 을 클릭합니다 Edit . 3. 사용자 정보를 수정합니다.
사용자를 삭제합니다	1. 삭제할 사용자를 선택합니다. 2. 을 Delete 클릭합니다.

ONTAP 시스템 관리자를 사용하여 NFS 활성 클라이언트 모니터링

ONTAP 9.8부터 System Manager는 NFS 라이센스가 클러스터에서 라이센스될 때 활성 상태인 NFS 클라이언트 연결을 보여 줍니다.

따라서 연결되어 있지만 유휴 상태이며 연결이 끊긴 스토리지 VM에 능동적으로 접속되어 있는 NFS 클라이언트를 빠르게 확인할 수 있습니다.

각 NFS 클라이언트 IP 주소에 대해 * NFS 클라이언트 * 디스플레이에 마지막 액세스 시간 * 네트워크 인터페이스 IP 주소 * NFS 연결 버전 * 스토리지 VM 이름이 표시됩니다

또한 지난 48시간 동안 활성화된 NFS 클라이언트 목록도 * Storage > Volumes * 디스플레이에 표시되고 NFS 클라이언트 수가 * Dashboard * 디스플레이에 포함됩니다.

단계

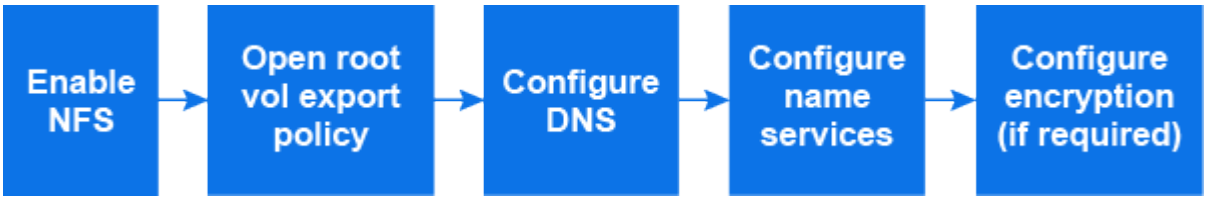
1. NFS 클라이언트 작업 표시: * 호스트 > NFS 클라이언트 * 를 클릭합니다.

NAS 스토리지를 설정합니다

ONTAP 시스템 관리자를 사용하여 **NFS**를 사용하여 **Linux** 서버에 **NAS** 스토리지 활성화

스토리지 VM을 생성하거나 수정하여 NFS 서버에서 Linux 클라이언트에 데이터를 제공할 수 있도록 합니다.

다음 절차를 사용하여 NFS 프로토콜에 새 스토리지 VM 또는 기존 스토리지 VM을 사용하도록 설정합니다.



시작하기 전에

사용자 환경에 필요한 네트워킹, 인증 또는 보안 서비스에 대한 구성 세부 정보를 기록해 두십시오.

단계

1. 스토리지 VM에서 NFS를 사용하도록 설정합니다.
   - 새 스토리지 VM의 경우: * 스토리지 > 스토리지 VM * 을 클릭하고 * 추가 * 를 클릭하고 스토리지 VM 이름을 입력한 다음 * SMB/CIFS, NFS, S3 * 탭에서 * NFS * 활성화 * 를 선택합니다.
     i. 기본 언어를 확인합니다.
     ii. 네트워크 인터페이스를 추가합니다.
     iii. 스토리지 VM 관리자 계정 정보 업데이트(선택 사항)
   - 기존 스토리지 VM의 경우: * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택하고 * 설정 * 을 클릭한 다음 * NFS * 아래를 클릭합니다.
2. 스토리지 VM 루트 볼륨의 엑스포트 정책을 엽니다.
   a. 스토리지 > 볼륨 * 을 클릭하고 스토리지 VM의 루트 볼륨(기본값: _volume-name__root)을 선택한 다음 * 정책

내보내기 * 아래에 표시되는 정책을 클릭합니다.

b. 규칙을 추가하려면 * 추가 * 를 클릭합니다.

- 클라이언트 사양 = 0.0.0.0/0
- 액세스 프로토콜 = NFS
- 액세스 세부 정보 = UNIX 읽기 전용

3. 호스트 이름 확인을 위한 DNS 구성: * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭하고 * DNS * 아래에서 * 를 클릭합니다 .
4. 필요에 따라 이름 서비스를 구성합니다.

a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭하고 LDAP 또는 NIS를 클릭합니다 .

b. 이름 서비스 스위치 타일을 클릭하여 변경 내용을 포함합니다.

5. 필요한 경우 Kerberos 구성:

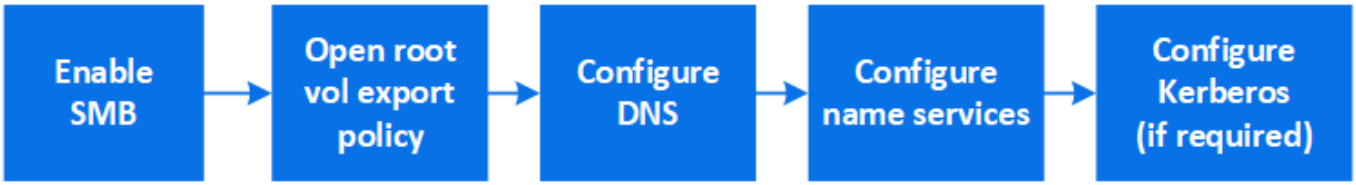
a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭합니다.

b. Kerberos 타일을 클릭한 다음 * 추가 * 를 클릭합니다.

ONTAP 시스템 관리자를 사용하여 **SMB**를 사용하여 **Windows** 서버에 **NAS** 스토리지 활성화

스토리지 VM을 생성 또는 수정하여 SMB 서버에서 Windows 클라이언트에 데이터를 제공할 수 있도록 합니다.

이 절차를 사용하면 SMB 프로토콜을 위한 신규 또는 기존 스토리지 VM을 사용할 수 있습니다. 사용자 환경에 필요한 네트워킹, 인증 또는 보안 서비스에 대해 구성 세부 정보를 사용할 수 있다고 가정합니다.



단계

1. 스토리지 VM에서 SMB를 사용하도록 설정합니다.

a. 새 스토리지 VM의 경우: * 스토리지 > 스토리지 VM * 을 클릭하고 * 추가 * 를 클릭한 다음 스토리지 VM 이름을 입력하고 * SMB/CIFS, NFS, S3 * 탭에서 * SMB/CIFS * 활성화 를 선택합니다.

- 다음 정보를 입력합니다.
  - 관리자 이름 및 암호
  - 서버 이름입니다
  - Active Directory 도메인입니다
- 조직 구성 단위를 확인합니다.
- DNS 값을 확인합니다.
- 기본 언어를 확인합니다.
- 네트워크 인터페이스를 추가합니다.

- 스토리지 VM 관리자 계정 정보 업데이트(선택 사항)

b. 기존 스토리지 VM의 경우:: * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택하고 * 설정 * 을 클릭한 다음 * SMB * 아래를 클릭합니다.

2. 스토리지 VM 루트 볼륨의 엑스포트 정책을 엽니다.

a. 스토리지 > 볼륨 * 을 클릭하고 스토리지 VM의 루트 볼륨(기본값: *volume-name_root*)을 선택한 다음 * 정책 내보내기 * 아래에 표시되는 정책을 클릭합니다.

b. 규칙을 추가하려면 * 추가 * 를 클릭합니다.

- 클라이언트 사양 = 0.0.0.0/0
- 액세스 프로토콜 = SMB
- 액세스 세부 정보 = NTFS 읽기 전용

3. 호스트 이름 확인을 위해 DNS 구성:

a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * Settings * 를 클릭하고 * DNS * 아래에서 * 를 클릭합니다 .

b. DNS 서버로 전환하고 SMB 서버를 매핑합니다.

- 정방향(A-Address 레코드) 및 역방향(PTR-포인터 레코드) 조회 항목을 만들어 SMB 서버 이름을 데이터 네트워크 인터페이스의 IP 주소에 매핑합니다.
- NetBIOS 별칭을 사용하는 경우 별칭 정식 이름(CNAME 리소스 레코드) 조회 항목을 만들어 각 별칭을 SMB 서버의 데이터 네트워크 인터페이스의 IP 주소에 매핑합니다.

4. 필요에 따라 이름 서비스를 구성합니다

a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 후 * Settings * 를 클릭한 다음 * LDAP * 또는 * NIS * 아래를 클릭합니다 .

b. 이름 서비스 스위치 파일에 변경 내용 포함: * 이름 서비스 스위치 * 를 클릭합니다 .

5. 필요한 경우 Kerberos 구성:

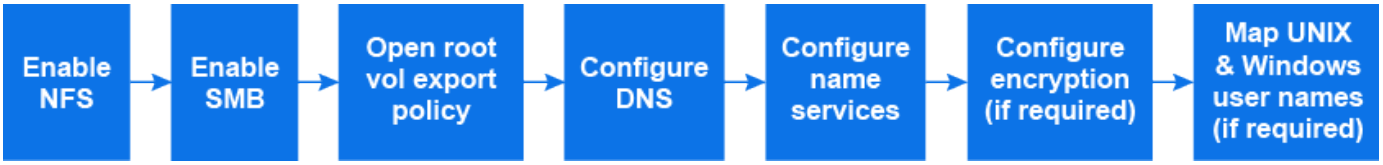
a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭합니다.

b. →Kerberos * 아래에서 * Add * 를 클릭합니다.

ONTAP 시스템 관리자를 사용하여 **NFS**와 **SMB**를 모두 사용하여 **Windows**와 **Linux** 모두에서 **NAS** 스토리지를 활성화합니다**.**

NFS 및 SMB 서버가 Linux 및 Windows 클라이언트에 데이터를 제공할 수 있도록 스토리지 VM을 생성하거나 수정합니다.

다음 절차를 사용하여 신규 또는 기존 스토리지 VM이 NFS 및 SMB 프로토콜을 모두 처리하도록 지원할 수 있습니다.



시작하기 전에

사용자 환경에 필요한 네트워킹, 인증 또는 보안 서비스에 대한 구성 세부 정보를 기록해 두십시오.

단계

1. 스토리지 VM에서 NFS 및 SMB를 사용하도록 설정합니다.
   a. 새 스토리지 VM의 경우: * 스토리지 > 스토리지 VM * 을 클릭하고 * 추가 * 를 클릭한 다음 스토리지 VM 이름을 입력하고 * SMB/CIFS, NFS, S3 * 탭에서 * SMB/CIFS * 활성화 및 * NFS * 활성화 를 선택합니다.
   b. 다음 정보를 입력합니다.
      - 관리자 이름 및 암호
      - 서버 이름입니다
      - Active Directory 도메인입니다
   c. 조직 구성 단위를 확인합니다.
   d. DNS 값을 확인합니다.
   e. 기본 언어를 확인합니다.
   f. 네트워크 인터페이스를 추가합니다.
   g. 스토리지 VM 관리자 계정 정보 업데이트(선택 사항)
   h. 기존 스토리지 VM의 경우: * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭합니다. NFS 또는 SMB가 아직 활성화되지 않은 경우 다음 하위 단계를 완료합니다.
      - NFS * 아래에서 를 클릭합니다.
      - smb * 아래에서 * 를 클릭합니다.
2. 스토리지 VM 루트 볼륨의 엑스포트 정책을 엽니다.
   a. 스토리지 > 볼륨 * 을 클릭하고 스토리지 VM의 루트 볼륨(기본값: *volume-name_root*)을 선택한 다음 * 정책 내보내기 * 아래에 표시되는 정책을 클릭합니다.
   b. 규칙을 추가하려면 * 추가 * 를 클릭합니다.
      - 클라이언트 사양 = 0.0.0.0/0
      - 액세스 프로토콜 = NFS
      - 액세스 세부 정보 = NFS 읽기 전용
3. 호스트 이름 확인을 위해 DNS 구성:
   a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * Settings * 를 클릭하고 * DNS * 아래에서 * 를 클릭합니다 .
   b. DNS 구성이 완료되면 DNS 서버로 전환하고 SMB 서버를 매핑합니다.
      - 정방향(A-Address 레코드) 및 역방향(PTR-포인터 레코드) 조회 항목을 만들어 SMB 서버 이름을 데이터 네트워크 인터페이스의 IP 주소에 매핑합니다.
      - NetBIOS 별칭을 사용하는 경우 별칭 정식 이름(CNAME 리소스 레코드) 조회 항목을 만들어 각 별칭을 SMB 서버의 데이터 네트워크 인터페이스의 IP 주소에 매핑합니다.
4. 필요에 따라 이름 서비스 구성:
   a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭하고 LDAP 또는 NIS를 클릭합니다 .
   b. 이름 서비스 스위치 파일에 변경 내용 포함: * 이름 서비스 스위치 * 를 클릭합니다 .
5. 필요한 경우 Kerberos 구성:

a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭합니다.

b. → Kerberos 타일을 클릭한 다음 * 추가 * 를 클릭합니다.

6. 필요한 경우 UNIX 및 Windows 사용자 이름 매핑: * 이름 매핑 * 아래에서 * 추가 * 를 → 클릭합니다.

   사이트에 암시적으로 매핑되지 않는 Windows 및 UNIX 사용자 계정이 있는 경우에만 이 작업을 수행해야 합니다. 즉, 각 Windows 사용자 이름의 소문자 버전이 UNIX 사용자 이름과 일치하는 경우에만 이 작업을 수행해야 합니다. LDAP, NIS 또는 로컬 사용자를 사용하여 사용자 이름을 매핑할 수 있습니다. 일치하지 않는 두 사용자 세트가 있는 경우 이름 매핑을 구성해야 합니다.

NFS 구성

ONTAP CLI를 사용한 NFS 구성에 대해 알아보십시오

ONTAP 9 CLI 명령을 사용하여 새 SVM(스토리지 가상 머신) 또는 기존 SVM(스토리지 가상 머신)에서 새 볼륨 또는 qtree에 포함된 파일에 대한 NFS 클라이언트 액세스를 구성할 수 있습니다.

다음과 같은 방법으로 볼륨 또는 qtree에 대한 액세스를 구성하려면 다음 절차를 사용하십시오.

- 현재 ONTAP에서 지원하는 모든 버전의 NFS, NFSv3, NFSv4, NFSv4.1, NFSv4.2 또는 pNFS를 사용하는 NFSv4.1을 사용하려고 합니다.
- System Manager나 자동화된 스크립팅 도구가 아니라 CLI(Command-Line Interface)를 사용하려는 경우

  System Manager를 사용하여 NAS 멀티 프로토콜 액세스를 구성하려면 를 참조하십시오"NFS와 SMB를 모두 사용하여 Windows 및 Linux 모두에 대해 NAS 스토리지를 프로비저닝합니다".

- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.

  명령 구문에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

- 새 볼륨의 보안을 위해 UNIX 파일 권한이 사용됩니다.
- SVM 관리자 권한이 아닌 클러스터 관리자 권한이 있습니다.

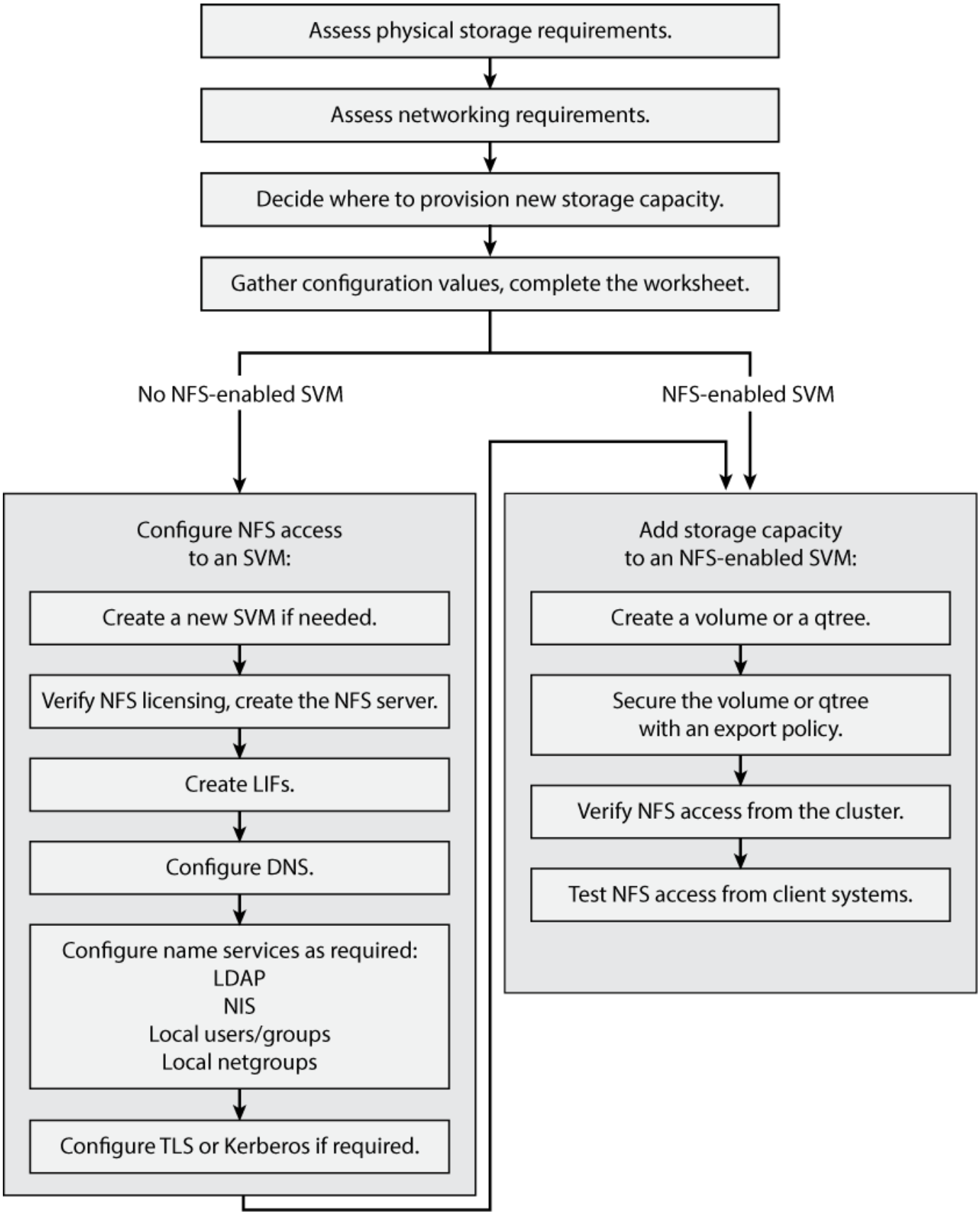
다양한 ONTAP NFS 프로토콜 기능에 대한 자세한 내용은 를 참조하십시오"NFS 프로토콜에 대한 ONTAP 파일 액세스에 대해 알아보세요".

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면…	자세한 내용은…
재설계된 System Manager(ONTAP 9.7 이상에서 사용 가능)	"NFS를 사용하여 Linux 서버용 NAS 스토리지 용량 할당"
System Manager Classic(ONTAP 9.7 이하에서 사용 가능	"NFS 구성 개요"

ONTAP NFS 구성 워크플로에 대해 알아보세요

NFS를 구성하려면 물리적 스토리지 및 네트워킹 요구사항을 평가한 다음, 목표에 맞는 워크플로우를 선택해야 합니다. 새로운 SVM 또는 기존 SVM에 대한 NFS 액세스를 구성하거나, NFS 액세스를 위해 이미 완벽하게 구성된 기존 SVM에 볼륨 또는 qtree를 추가하십시오.


Assess physical storage requirements.
Assess networking requirements.
Decide where to provision new storage capacity.
Gather configuration values, complete the worksheet.
No NFS-enabled SVM
NFS-enabled SVM
Configure NFS access to an SVM:
Create a new SVM if needed.
Verify NFS licensing, create the NFS server.
Create LIFs.
Configure DNS.
Configure name services as required:
LDAP
NIS
Local users/groups
Local netgroups
Configure TLS or Kerberos if required.
Add storage capacity to an NFS-enabled SVM:
Create a volume or a qtree.
Secure the volume or qtree with an export policy.
Verify NFS access from the cluster.
Test NFS access from client systems.

준비

ONTAP NFS의 물리적 스토리지 요구사항을 평가합니다

클라이언트용 NFS 스토리지를 프로비저닝하기 전에 새 볼륨에 대한 기존 애그리게이트에 충분한 공간이 있는지 확인해야 합니다. 없는 경우 디스크를 기존 Aggregate에 추가하거나 원하는 유형의 새 Aggregate를 생성할 수 있습니다.

단계

1. 기존 애그리게이트에서 사용 가능한 공간 표시:

   '스토리지 집계 쇼'

   공간이 충분한 집계가 있는 경우 워크시트에 이름을 기록합니다.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. 충분한 공간이 있는 애그리게이트가 없는 경우 'Storage aggregate add-disks' 명령을 사용하여 기존 애그리게이트에 디스크를 추가하거나 'Storage aggregate create' 명령을 사용하여 새로운 애그리게이트를 생성합니다.

관련 정보

- "로컬 계층에 디스크 추가(애그리게이트)"
- "스토리지 집계 추가 디스크"
- "저장소 집계 생성"

ONTAP NFS 네트워크 구성 요구 사항 평가

NFS 스토리지를 클라이언트에 제공하기 전에 NFS 프로비저닝 요구 사항을 충족하도록 네트워킹이 올바르게 구성되었는지 확인해야 합니다.

시작하기 전에

다음과 같은 클러스터 네트워킹 객체를 구성해야 합니다.

- 물리적 및 논리적 포트
- 브로드캐스트 도메인
- 서브넷(필요한 경우)
- IPspace(기본 IPspace 외에 필요 시)
- 페일오버 그룹(필요에 따라 각 브로드캐스트 도메인의 기본 페일오버 그룹 추가)
- 외부 방화벽

단계

1. 사용 가능한 물리적 포트 및 가상 포트를 표시합니다.

   네트워크 포트 쇼

   - 가능하면 데이터 네트워크에 대해 최고 속도의 포트를 사용해야 합니다.
   - 최상의 성능을 얻으려면 데이터 네트워크의 모든 구성 요소에 동일한 MTU 설정이 있어야 합니다.
   - 에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 서브넷 이름을 사용하여 LIF에 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 존재하는지, 사용 가능한 주소가 충분한지 확인합니다. +

   네트워크 서브넷 쇼

   에 대한 자세한 내용은 `network subnet show` "ONTAP 명령 참조입니다"을 참조하십시오.

   서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 서브넷은 network subnet create 명령을 사용하여 생성된다.

   에 대한 자세한 내용은 `network subnet create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 사용 가능한 IPspace 표시:

   네트워크 IPspace 쇼

   기본 IPspace 또는 사용자 지정 IPspace를 사용할 수 있습니다.

   에 대한 자세한 내용은 `network ipspace show` "ONTAP 명령 참조입니다"을 참조하십시오.

4. IPv6 주소를 사용하려면 클러스터에서 IPv6이 활성화되어 있는지 확인합니다.

   네트워크 옵션 IPv6 쇼

   필요한 경우 'network options ipv6 modify' 명령을 사용하여 IPv6을 사용하도록 설정할 수 있습니다.

   및 `network options ipv6 modify` 에 대한 자세한 `network options ipv6 show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP NFS 스토리지 용량 프로비저닝에 대해 알아보십시오

새 NFS 볼륨 또는 qtree를 생성하기 전에 새로운 SVM이나 기존 SVM에 배치할지 여부와

SVM에 필요한 구성의 크기를 결정해야 합니다. 이 결정에 따라 워크플로가 결정됩니다.

선택

- 새 SVM에서 볼륨 또는 qtree를 프로비저닝하거나 NFS가 활성화되어 있지만 구성되지 않은 기존 SVM에서 프로비저닝하려면 "SVM에 NFS 액세스 구성" 및 "NFS 스토리지를 NFS 지원 SVM에 추가" 단계를 완료하십시오.

  SVM에 대한 NFS 액세스를 구성합니다

  NFS 지원 SVM에 NFS 스토리지를 추가합니다

  다음 중 하나에 해당하는 경우 새 SVM을 생성할 수 있습니다.

  - 클러스터에서 NFS를 처음으로 사용하도록 설정하고 있습니다.
  - NFS 지원을 사용하지 않으려는 클러스터에 기존 SVM이 있습니다.
  - 하나의 클러스터에 NFS 지원 SVM이 하나 이상 있으며 다른 NFS 서버를 격리된 네임스페이스(멀티 테넌시 시나리오)로 사용하려는 경우를 가정해 보겠습니다. NFS가 활성화되었지만 구성되지 않은 기존 SVM에서 스토리지를 프로비저닝하려면 이 옵션을 선택해야 합니다. 이는 SAN 액세스를 위해 SVM을 생성했거나, SVM 생성 시 프로토콜을 사용하지 않은 경우에 발생할 수 있습니다.

  SVM에서 NFS를 사용하도록 설정한 후 볼륨 또는 qtree를 프로비저닝합니다.

- NFS 액세스를 위해 완전히 구성된 기존 SVM에서 볼륨 또는 qtree를 프로비저닝하려면 "NFS 스토리지를 NFS 지원 SVM에 추가"의 단계를 완료하십시오.

  NFS 지원 SVM에 NFS 스토리지 추가

ONTAP NFS 구성 워크시트

NFS 구성 워크시트를 사용하면 클라이언트에 대한 NFS 액세스를 설정하는 데 필요한 정보를 수집할 수 있습니다.

스토리지 용량 할당 위치에 대한 결정에 따라 워크시트의 섹션 중 하나 또는 두 섹션을 모두 완료해야 합니다.

SVM에 대한 NFS 액세스를 구성하는 경우 두 섹션을 모두 완료해야 합니다.

- SVM에 대한 NFS 액세스 구성
- NFS 지원 SVM에 스토리지 용량 추가

NFS 지원 SVM에 스토리지 용량을 추가하는 경우 다음 작업만 완료해야 합니다.

- NFS 지원 SVM에 스토리지 용량 추가

SVM에 대한 **NFS** 액세스를 구성합니다

- SVM 생성을 위한 매개 변수 *

새 SVM을 생성하는 경우 이러한 값을 'vserver create' 명령으로 제공합니다.

필드에 입력합니다	설명	귀사의 가치

'-vserver'	FQDN(정규화된 도메인 이름)이거나 클러스터 전체에 고유한 SVM 이름을 적용하는 다른 규칙을 따르는 새 SVM에 대해 제공하는 이름입니다.	
'-집계'	새 NFS 스토리지 용량을 위한 충분한 공간이 있는 클러스터의 애그리게이트 이름입니다.	
'-rootvolume'	SVM 루트 볼륨에 제공하는 고유 이름입니다.	
'-rootvolume-security-style'	SVM에 UNIX 보안 스타일을 사용합니다.	유닉스
'-언어'	이 워크플로의 기본 언어 설정을 사용합니다.	1. UTF-8
'IPSpace'	IPspace는 SVM(스토리지 가상 머신)이 상주하는 고유 IP 주소 공간입니다.	

- NFS 서버 생성을 위한 매개 변수 *

새 NFS 서버를 생성하고 지원되는 NFS 버전을 지정할 때 이러한 값을 'vserver NFS create' 명령으로 제공합니다.

NFSv4 이상을 설정하는 경우 보안을 강화하기 위해 LDAP를 사용해야 합니다.

필드에 입력합니다	설명	귀사의 가치
v3 -v4.0 -v4.1 -v4.1 -v4.1 -pNFS	필요에 따라 NFS 버전을 사용하도록 설정합니다. v4.2는 v4.1이 활성화된 경우 ONTAP 9.8 이상에서도 지원됩니다.	
'-v4-id-domain'	ID 매핑 도메인 이름입니다.	
'-v4-numeric-ids'	숫자 소유자 ID 지원(사용 또는 사용 안 함)	

- LIF 생성을 위한 매개 변수 *

LIF를 생성할 때 이러한 값을 명령과 함께 `network interface create` 제공합니다. 에 대한 자세한 내용은

`network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

Kerberos를 사용하는 경우 여러 LIF에서 Kerberos를 사용하도록 설정해야 합니다.

필드에 입력합니다	설명	귀사의 가치
'-lif'	새 LIF에 대해 제공한 이름입니다.	
'-역할'	이 워크플로우에서 데이터 LIF 역할을 사용합니다.	다타
'-데이터-프로토콜'	이 워크플로우에서는 NFS 프로토콜만 사용합니다.	'NFS'입니다
홈 노드	LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행할 때 LIF가 반환되는 노드입니다. 에 대한 자세한 내용은 `network interface revert` "ONTAP 명령 참조입니다"을 참조하십시오.	
``홈 포트''	LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 포트 또는 인터페이스 그룹입니다.	
주소	새 LIF가 데이터 액세스에 사용할 클러스터의 IPv4 또는 IPv6 주소입니다.	
넷마스크입니다	LIF의 네트워크 마스크와 게이트웨이입니다.	
'-서브넷'	IP 주소 풀입니다. 주소와 넷마스크를 자동으로 할당하기 위해 -address와 -netmask 대신 사용됩니다.	
방화벽 정책	이 워크플로우에서 기본 데이터 방화벽 정책을 사용합니다.	다타

- DNS 호스트 이름 확인을 위한 매개 변수 *

DNS를 구성할 때 이러한 값을 'vserver services name-service dns create' 명령으로 제공합니다.

필드에 입력합니다	설명	귀사의 가치
``도메인'	최대 5개의 DNS 도메인 이름	

이름-서버	각 DNS 이름 서버에 대해 최대 3개의 IP 주소를 지정할 수 있습니다.	

네임 서비스 정보

- 로컬 사용자 생성을 위한 매개 변수 *

'vserver services name-service unix-user create' 명령을 사용하여 로컬 사용자를 생성하는 경우 이러한 값을 제공합니다. UNIX 사용자가 포함된 파일을 URI(Uniform Resource Identifier)에서 로드하여 로컬 사용자를 구성하는 경우에는 이러한 값을 수동으로 지정할 필요가 없습니다.

	사용자 이름 '(-user)'입니다	사용자 ID '(-id)'입니다	그룹 ID '(-primary-gid)'입니다	전체 이름(-full-name)
예	합니다	123을 선택합니다	100	존 밀러
1				
2				
3				
…				
해당 없음				

- 로컬 그룹 생성을 위한 매개 변수 *

'vserver services name-service unix-group create' 명령을 사용하여 로컬 그룹을 생성하는 경우 이러한 값을 제공합니다. URI에서 UNIX 그룹이 포함된 파일을 로드하여 로컬 그룹을 구성하는 경우에는 이러한 값을 수동으로 지정할 필요가 없습니다.

	그룹 이름('-name')	Group ID('-id')
예	엔지니어링	100
1		
2		
3		
…		
해당 없음		

• NIS용 매개 변수 *

이러한 값은 'vserver services name-service NIS-domain create' 명령을 사용하여 입력합니다.

그만큼 `-nis-servers` 필드는 다음을 대체합니다. `-servers` 필드입니다. 다음을 사용할 수 있습니다. `-nis-servers` NIS 서버의 호스트 이름이나 IP 주소를 지정하는 필드입니다.

필드에 입력합니다	설명	귀사의 가치
``도메인’	SVM이 이름 조회에 사용할 NIS 도메인입니다.	
'-활성'	활성 NIS 도메인 서버입니다.	참 거짓입니다
'-NIS-서버'	도메인 구성에 사용되는 NIS 서버의 IP 주소와 호스트 이름을 쉼표로 구분한 목록입니다.	

• LDAP용 매개 변수 *

이러한 값은 'vserver services name-service ldap client create' 명령을 사용하여 입력합니다.

자체 서명된 루트 CA 인증서 '.pem' 파일도 필요합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	LDAP 클라이언트 구성을 생성할 SVM의 이름입니다.	
'-client-config’입니다	새 LDAP 클라이언트 구성에 할당한 이름입니다.	
'-LDAP-서버'	LDAP 서버의 IP 주소 및 호스트 이름을 쉼표로 구분하여 나열합니다.	
'-query-timeout’입니다	이 워크플로에 기본 3초를 사용합니다.	3
'-min-bind-level'	최소 바인딩 인증 수준입니다. 기본값은 'anonymous’입니다. 서명 및 봉인을 구성한 경우 'ASL’으로 설정해야 합니다.	
'-preferred-ad-servers'	쉼표로 구분된 목록에서 IP 주소별로 하나 이상의 기본 Active Directory 서버가 있습니다.	
'-ad-domain’입니다	Active Directory 도메인입니다.	

필드에 입력합니다	설명	귀사의 가치
'-스키마'	사용할 스키마 템플릿입니다. 기본 스키마나 사용자 지정 스키마를 사용할 수 있습니다.	
``포트''	이 워크플로우에는 기본 LDAP 서버 포트 '389'를 사용합니다.	389
'-bind-dn'	Bind 사용자 고유 이름입니다.	
'-base-dn'	기본 고유 이름입니다. 기본값은 ""(root)입니다.	
``기본범위''	이 워크플로에 기본 기본 검색 범위 'Subnet'을 사용합니다.	'우방'
'-세션-보안'	LDAP 서명 또는 서명 및 봉인을 활성화합니다. 기본값은 '없음'입니다.	
'-use-start-tls'	TLS를 통해 LDAP를 활성화합니다. 기본값은 false 입니다.	

- Kerberos 인증 매개변수 *

이러한 값은 'vserver NFS Kerberos realm create' 명령을 사용하여 입력합니다. 일부 값은 KDC(Key Distribution Center) 서버로 Microsoft Active Directory를 사용할지, MIT 또는 기타 UNIX KDC 서버를 사용하는지에 따라 달라집니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	KDC와 통신할 SVM.	
``영역'	Kerberos 영역.	
시계 편중	클라이언트와 서버 간에 허용되는 클럭 편중.	
'-KDC-IP'	KDC IP 주소입니다.	
``KDC-포트'	KDC 포트 번호입니다.	
'-adserver-name'입니다	Microsoft KDC 전용: AD 서버 이름입니다.	

'-adserver-ip’입니다	Microsoft KDC 전용: AD 서버 IP 주소입니다.	
'-AdminServer-IP’입니다	UNIX KDC 전용: 관리 서버 IP 주소.	
'-AdminServer-port’입니다	UNIX KDC만 해당: 관리 서버 포트 번호입니다.	
'-passwordserver-IP’입니다	UNIX KDC 전용: 암호 서버 IP 주소입니다.	
'-passwordserver-port’입니다	UNIX KDC 전용: 암호 서버 포트.	
``KDC-벤더’	KDC 공급업체.	{'Microsoft'
'기타'}	``논평’	원하는 코멘트.

이러한 값은 'vserver NFS Kerberos interface enable' 명령을 사용하여 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	Kerberos 구성을 생성할 SVM의 이름입니다.	
'-lif'	Kerberos를 사용하도록 설정할 데이터 LIF입니다. 여러 LIF에서 Kerberos를 사용하도록 설정할 수 있습니다.	
'-SPN'	서비스 원칙 이름(SPN)	
``허용된-원력-유형’’	클라이언트 기능에 따라 Kerberos over NFS에 대해 허용되는 암호화 유형인 AES-256을 사용하는 것이 좋습니다.	
'-admin-username’입니다	KDC에서 직접 SPN 암호 키를 검색하는 KDC 관리자 자격 증명입니다. 암호가 필요합니다	
'-keytab-Uri’입니다	KDC 관리자 자격 증명이 없는 경우 SPN 키가 포함된 KDC의 keytab 파일입니다.	

'-ou'	Microsoft KDC의 영역을 사용하여 Kerberos를 설정할 때 Microsoft Active Directory 서버 계정이 생성되는 OU(조직 구성 단위)입니다.	

NFS 지원 **SVM**에 스토리지 용량 추가

- 내보내기 정책 및 규칙 생성을 위한 매개 변수 *

이러한 값은 'vserver export-policy create' 명령을 사용하여 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	새 볼륨을 호스팅할 SVM의 이름입니다.	
정책 이름	새 엑스포트 정책에 대해 제공한 이름입니다.	

각 규칙에 대해 'vserver export-policy rule create' 명령을 사용하여 이러한 값을 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-clientmatch'	클라이언트 일치 사양.	
룰레인덱스	규칙 목록에서 내보내기 규칙의 위치입니다.	
'-프로토콜'	이 워크플로우에서 NFS를 사용합니다.	'NFS'입니다
'-rorule'	읽기 전용 액세스에 대한 인증 방법입니다.	
'-rwrule'	읽기-쓰기 액세스를 위한 인증 방법입니다.	
'-슈퍼유저'	고급 사용자 액세스를 위한 인증 방법입니다.	
'-anon'	익명 사용자가 매핑되는 사용자 ID입니다.	

각 엑스포트 정책에 대해 하나 이상의 규칙을 생성해야 합니다.

'**-ruleindex**'	'* - clientmatch * '	' * -rorule * '	'*-rwrule * '	'*-슈퍼유저 * '	'*-anon * '

예	0.0.0.0/0, @rootaccess_netgroup	모두	krb5	시스템	65534
1					
2					
3					
…					
해당 없음					

- 볼륨 생성을 위한 매개 변수 *

Qtree 대신 볼륨을 생성하는 경우 이 값에 'volume create' 명령을 입력합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	새 볼륨을 호스팅할 새 SVM 또는 기존 SVM의 이름입니다.	
'- 볼륨'	새 볼륨에 제공하는 고유한 설명 이름입니다.	
'-집계'	새 NFS 볼륨을 위한 충분한 공간이 있는 클러스터의 애그리게이트 이름입니다.	
'-size'	새 볼륨의 크기에 대해 제공하는 정수입니다.	
'-user'	볼륨 루트의 소유자로 설정된 사용자의 이름 또는 ID입니다.	
``그룹''	볼륨 루트의 소유자로 설정된 그룹의 이름 또는 ID입니다.	
``보안스타일''	이 워크플로우에는 UNIX 보안 스타일을 사용합니다.	유닉스
``교차점-경로''	새 볼륨을 마운트할 루트(/) 아래의 위치입니다.	

수출정책	기존 엑스포트 정책을 사용하려는 경우 볼륨을 생성할 때 해당 이름을 입력할 수 있습니다.	

- qtree 생성을 위한 매개 변수 *

볼륨 대신 qtree를 생성하는 경우 이 값에 'volume qtree create' 명령을 입력합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	qtree가 포함된 볼륨이 있는 SVM의 이름입니다.	
'- 볼륨'	새 qtree를 포함할 볼륨의 이름입니다.	
'-qtree'	새 qtree를 64자 이하로 설명하는 고유한 이름입니다.	
'-qtree-path'	볼륨과 qtree를 별도의 인수로 지정하는 대신 '/vol/*volume_name/qtree_name*\>' 형식의 qtree 경로 인수를 지정할 수 있습니다.	
'-unix-permissions'	선택 사항: qtree에 대한 UNIX 사용 권한	
수출정책	기존 엑스포트 정책을 사용하려는 경우 qtree를 생성할 때 이름을 입력할 수 있습니다.	

관련 정보

- "ONTAP 명령 참조입니다"

SVM에 대한 NFS 액세스를 구성합니다

NFS 데이터 액세스를 위한 **ONTAP SVM** 생성

NFS 클라이언트에 데이터 액세스를 제공하기 위해 클러스터에 SVM이 하나 이상 없으면 하나 이상의 SVM을 생성해야 합니다.

시작하기 전에

- ONTAP 9.13.1부터 스토리지 VM에 대한 최대 용량을 설정할 수 있습니다. SVM이 임계값 용량 수준에 도달할 경우에도 경고를 구성할 수 있습니다. 자세한 내용은 을 SVM 용량 관리참조하십시오.

단계

1. SVM 생성:

'vserver create-vserver_vserver_name_-rootvolume_root_volume_name_-aggregate_aggregate_name_-rootvolume-security-style UNIX-language C. UTF-8-IPSpace_IPSpace_name_'

- '-rootvolume-security-style' 옵션에 UNIX 설정을 사용합니다.
- 기본 C. UTF-8 '-language' 옵션을 사용합니다.
- IPSpace 설정은 선택 사항입니다.

2. 새로 생성한 SVM의 구성 및 상태 확인:

   'vserver show -vserver_vserver_name_'

   허용되는 프로토콜 필드는 NFS를 포함해야 합니다. 나중에 이 목록을 편집할 수 있습니다.

   'Vserver 작동 상태' 필드에는 '실행 중' 상태가 표시되어야 합니다. 초기화 중 상태가 표시되는 경우 루트 볼륨 생성 등 일부 중간 작업이 실패한 것으로, SVM을 삭제하고 다시 생성해야 합니다.

예

다음 명령은 IPspace에서 데이터 액세스를 위한 SVM을 생성합니다. spaceba:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

다음 명령을 실행하면 루트 볼륨 1GB 단위로 SVM이 생성되고 자동으로 시작되어 '실행 중' 상태에 있음을 알 수 있습니다. 루트 볼륨에는 규칙을 포함하지 않는 기본 엑스포트 정책이 있으므로 생성 시 루트 볼륨을 내보내지 않습니다.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

ONTAP 9.13.1부터 SVM의 볼륨에 처리량 하한 및 상한 제한을 적용하여 적응형 QoS 정책 그룹 템플릿을 설정할 수 있습니다. SVM을 생성한 후에만 이 정책을 적용할 수 있습니다. 이 프로세스에 대한 자세한 내용은 을 적응형 정책 그룹 템플릿을 설정합니다참조하십시오.

ONTAP SVM에서 **NFS** 프로토콜 활성화 확인

SVM에서 NFS를 구성 및 사용하려면 먼저 프로토콜이 활성화되어 있는지 확인해야 합니다.

이 작업에 대해

이는 일반적으로 SVM 설정 중에 수행되지만 설정 중에 프로토콜을 활성화하지 않은 경우 나중에 'vserver add-protocols' 명령을 사용하여 활성화할 수 있습니다.

프로토콜을 생성한 후에는 LIF에서 프로토콜을 추가하거나 제거할 수 없습니다.

"vserver remove-protocols" 명령을 사용하여 SVM에서 프로토콜을 비활성화할 수도 있습니다.

단계

1. 현재 SVM에 대해 활성화 및 비활성화된 프로토콜을 확인합니다.

'vserver show -vserver_vserver_name_-protocols'

"vserver show-protocols" 명령을 사용하여 클러스터의 모든 SVM에서 현재 활성화된 프로토콜을 볼 수도 있습니다.

2. 필요한 경우 프로토콜을 활성화 또는 비활성화합니다.
   - NFS 프로토콜을 활성화하려면: + 'vserver add-protocols-vserver_vserver_name_-protocols nfs'
   - 프로토콜을 작동 불가능하게 하려면: + "vserver remove-protocols-vserver_name_-protocols_protocol_name_[,*protocol_name*,…]
3. 활성화된 프로토콜과 비활성화된 프로토콜이 올바르게 업데이트되었는지 확인합니다.

   'vserver show -vserver_vserver_name_-protocols'

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 현재 설정 및 해제된 프로토콜(허용 및 허용 안 함)이 표시됩니다.

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    ------------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

다음 명령을 사용하면 이름이 VS1 인 SVM에서 활성화된 프로토콜 목록에 NFS를 추가하여 NFS를 통해 액세스할 수 있습니다.

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

ONTAP SVM에서 **NFS** 클라이언트 액세스 열기

SVM 루트 볼륨의 기본 엑스포트 정책에는 NFS를 통해 모든 클라이언트가 액세스할 수 있도록 하는 규칙이 포함되어야 합니다. 이 규칙이 없으면 모든 NFS 클라이언트가 SVM 및 해당 볼륨에 대한 액세스가 거부됩니다.

이 작업에 대해

새 SVM이 생성되면 SVM의 루트 볼륨에 대한 기본 엑스포트 정책(기본값)이 자동으로 생성됩니다. 클라이언트가 SVM에서 데이터에 액세스하려면 기본 엑스포트 정책에 대한 규칙을 하나 이상 생성해야 합니다.

기본 엑스포트 정책에서 모든 NFS 클라이언트에 대한 액세스가 허용되는지 확인하고, 나중에 개별 볼륨 또는 qtree에 대한 사용자 지정 엑스포트 정책을 생성하여 개별 볼륨에 대한 액세스를 제한해야 합니다.

단계

1. 기존 SVM을 사용하는 경우 기본 루트 볼륨 엑스포트 정책을 확인하십시오.

   'vserver export-policy rule show'를 선택합니다

   명령 출력은 다음과 같아야 합니다.

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol:  nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

이러한 규칙이 열려 있는 액세스를 허용하는 경우 이 작업은 완료된 것입니다. 그렇지 않은 경우 다음 단계를 진행하십시오.

2. SVM 루트 볼륨에 대한 엑스포트 규칙 생성:

   'vserver export-policy rule create-vserver_vserver_name_-policyname default-ruleindex 1-protocol nfs-clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any'

   SVM이 Kerberos로 보호되는 볼륨만 포함할 경우 루트 볼륨에 대한 내보내기 규칙 옵션 '-rorule', '-rwrule' 및 '-superuser'를 krb5' 또는 'krb5i'로 설정할 수 있습니다. 예를 들면 다음과 같습니다.

   '-rorule krb5i-rwrule krb5i-superuser krb5i'

3. 'vserver export-policy rule show' 명령을 사용하여 규칙 생성을 확인합니다.

결과

이제 모든 NFS 클라이언트가 SVM에서 생성된 모든 볼륨 또는 qtree에 액세스할 수 있습니다.

ONTAP NFS 서버 생성

클러스터에서 NFS 라이센스가 등록되었는지 확인한 후 "vserver NFS create" 명령을 사용하여 SVM에 NFS 서버를 생성하고 해당 명령이 지원하는 NFS 버전을 지정할 수 있습니다.

이 작업에 대해

SVM은 하나 이상의 NFS 버전을 지원하도록 구성할 수 있습니다. NFSv4 이상을 지원하는 경우:

- NFSv4 사용자 ID 매핑 도메인 이름은 NFSv4 서버 및 타겟 클라이언트에서 동일해야 합니다.

  NFSv4 서버와 클라이언트가 동일한 이름을 사용하는 한 LDAP 또는 NIS 도메인 이름과 같을 필요는 없습니다.

- 타겟 클라이언트는 NFSv4 숫자 ID 설정을 지원해야 합니다.
- 보안을 위해 NFSv4 구축에서는 이름 서비스에 LDAP를 사용해야 합니다.

시작하기 전에

SVM은 NFS 프로토콜을 허용하도록 구성해야 합니다.

단계

1. NFS 라이센스가 클러스터에서 라이센스되었는지 확인합니다.

   'system license show-package nfs'

   그렇지 않은 경우 영업 담당자에게 문의하십시오.

2. NFS 서버 생성:

   'vserver NFS create -vserver_vserver_name_-v3{enabled | disabled} -v4.0{enabled | disabled} -v4-id -domain_NFSv4_id_domain_-v4-numeric-ids{enabled | disabled} -v4.1{enabled | disabled | pNFS{enabled | disabled}'를 선택합니다

   NFS 버전의 조합을 사용하도록 선택할 수 있습니다. pNFS를 지원하려면 '-v4.1'과 '-v4.1-pNFS' 옵션을 모두 사용해야 합니다.

   v4 이상을 사용하는 경우 다음 옵션도 올바르게 설정되어 있어야 합니다.

   - '-v4-id-domain'

     이 선택적 매개 변수는 NFSv4 프로토콜에서 정의된 사용자 및 그룹 이름의 문자열 형식 도메인 부분을 지정합니다. 기본적으로 ONTAP는 NIS 도메인이 설정되어 있는 경우 NIS 도메인을 사용하고, 설정되어 있지 않으면 DNS 도메인이 사용됩니다. 대상 클라이언트가 사용하는 도메인 이름과 일치하는 값을 입력해야 합니다.

   - '-v4-numeric-ids'

     이 선택적 매개 변수는 NFSv4 소유자 속성에서 숫자 문자열 식별자를 지원하도록 설정되었는지 여부를 지정합니다. 기본 설정은 활성화되지만 타겟 클라이언트가 이 설정을 지원하는지 확인해야 합니다.

   나중에 'vserver nfs modify' 명령을 사용하여 추가 NFS 기능을 활성화할 수 있습니다.

3. NFS가 실행 중인지 확인합니다.

   'vserver NFS status-vserver_vserver_name_'

4. NFS가 원하는 대로 구성되었는지 확인합니다.

   'vserver nfs show -vserver_vserver_name_'

예

다음 명령을 실행하면 NFSv3 및 NFSv4.0이 설정된 VS1 이라는 SVM에 NFS 서버가 생성됩니다.

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

다음 명령을 실행하면 이름이 VS1 인 새 NFS 서버의 상태와 구성 값이 검증됩니다.

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                    General NFS Access: true
                                NFS v3: enabled
                              NFS v4.0: enabled
                         UDP Protocol: enabled
                         TCP Protocol: enabled
                  Default Windows User: -
                   NFSv4.0 ACL Support: disabled
      NFSv4.0 Read Delegation Support: disabled
     NFSv4.0 Write Delegation Support: disabled
              NFSv4 ID Mapping Domain: my_domain.com
...
```

ONTAP NFS LIF를 생성합니다

LIF는 물리적 포트 또는 논리적 포트와 연결된 IP 주소입니다. 구성요소 장애가 발생할 경우 LIF가 다른 물리적 포트로 페일오버되거나 마이그레이션되어 네트워크와 계속 통신할 수 있습니다.

시작하기 전에

- 기본 물리적 또는 논리적 네트워크 포트가 관리 `up` 상태로 구성되어야 합니다. 에 대한 자세한 내용은 `up` "ONTAP 명령 참조입니다"을 참조하십시오.
- 서브넷 이름을 사용하여 LIF에 대한 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 이미 존재해야 합니다.

  서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 네트워크 서브넷 만들기 명령을 사용하여 만듭니다.

  에 대한 자세한 내용은 `network subnet create` "ONTAP 명령 참조입니다"을 참조하십시오.

- LIF가 처리하는 트래픽 유형을 지정하는 메커니즘이 변경되었습니다. ONTAP 9.5 이전 버전의 경우 LIF는 역할을 사용하여 처리할 트래픽 유형을 지정합니다. ONTAP 9.6부터 LIF는 서비스 정책을 사용하여 처리할 트래픽 유형을 지정합니다.

이 작업에 대해

- 동일한 네트워크 포트에서 IPv4 및 IPv6 LIF를 모두 생성할 수 있습니다.
- Kerberos 인증을 사용하는 경우 여러 LIF에서 Kerberos를 사용하도록 설정합니다.
- 클러스터에 LIF가 많은 경우 'network interface capacity show' 명령을 사용하여 클러스터에서 지원되는 LIF 용량과 각 노드에서 지원되는 LIF 용량을 확인할 수 있습니다 (고급 권한 수준에서).

  및 `network interface capacity details show` 에 대한 자세한 `network interface capacity`

show 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

- ONTAP 9.7부터 동일한 서브넷에 있는 SVM에 대한 다른 LIF가 이미 있는 경우 LIF의 홈 포트를 지정할 필요가 없습니다. ONTAP는 동일한 서브넷에 이미 구성된 다른 LIF와 동일한 브로드캐스트 도메인에 있는 지정된 홈 노드에서 랜덤 포트를 자동으로 선택합니다.

ONTAP 9.4부터는 FC-NVMe가 지원됩니다. FC-NVMe LIF를 생성하는 경우 다음 사항을 알아야 합니다.

- NVMe 프로토콜은 LIF가 생성된 FC 어댑터에서 지원되어야 합니다.
- FC-NVMe는 데이터 LIF에서 유일한 데이터 프로토콜일 수 있습니다.
- SAN을 지원하는 모든 SVM(스토리지 가상 머신)에서 관리 트래픽을 처리하는 하나의 LIF를 구성해야 합니다.
- NVMe LIF 및 네임스페이스는 동일한 노드에서 호스팅되어야 합니다.
- SVM당 하나의 NVMe LIF에서 데이터 트래픽을 처리할 수 있습니다

단계

1. LIF 생성:

   'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol nfs-home-node_node_name_-home-port_port_name_{-address_{-address_netmask_ip_address_|-subnet-name_subnet_name_}-firewall-policy data-auto-revert{true|false}

   에 대한 자세한 내용은 network interface create "ONTAP 명령 참조입니다"을 참조하십시오.

옵션을 선택합니다	설명
• ONTAP 9.5 이하 *	'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol nfs-home-node_node_name_-home-port_port_name_{-address_{-address_netmask_ip_address_
-subnet-name_subnet_name_}-firewall-policy data-auto-revert{true	false}
• ONTAP 9.6 이상 *	'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol nfs-home-node_node_name_-home-port_port_name_{-address_{-address_netmask_ip_address_
-subnet-name_subnet_name_}-firewall-policy data-auto-revert{true	false}

- 서비스 정책(ONTAP 9.6에서 시작)을 사용하여 LIF를 생성할 때는 '-role' 매개 변수가 필요하지 않습니다.
- LIF를 생성할 때 '-data-protocol' 매개 변수를 지정해야 하며 나중에 데이터 LIF를 삭제 및 다시 생성하지 않고 수정할 수 없습니다.

  서비스 정책(ONTAP 9.6부터)을 사용하여 LIF를 생성할 때는 '-data-protocol' 매개 변수가 필요하지 않습니다.

- 홈 노드는 LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환하는 노드입니다.

  또한 LIF가 '-auto-revert' 옵션을 사용하여 홈 노드 및 홈 포트로 자동으로 되돌아가는지 여부를 지정할 수도

있습니다.

에 대한 자세한 내용은 `network interface revert` "ONTAP 명령 참조입니다"을 참조하십시오.

- '-home-port'는 LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 물리적 또는 논리적 포트입니다.
- IP 주소는 '-address' 및 '-netmask' 옵션을 사용하여 지정하거나 '-subnet_name' 옵션을 사용하여 서브넷에서 할당을 활성화할 수 있습니다.
- 서브넷을 사용하여 IP 주소와 네트워크 마스크를 제공하면, 서브넷에 정의된 서브넷이 해당 서브넷을 사용하여 LIF를 생성할 때 해당 게이트웨이에 대한 기본 경로가 SVM에 자동으로 추가됩니다.
- 서브넷을 사용하지 않고 수동으로 IP 주소를 할당하는 경우 다른 IP 서브넷에 클라이언트 또는 도메인 컨트롤러가 있는 경우 게이트웨이에 대한 기본 라우트를 구성해야 할 수 있습니다. SVM 내에서 정적 라우트를 생성하는 방법에 대한 자세한 `network route create` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.
- '-firewall-policy' 옵션의 경우 LIF 역할과 동일한 기본 data를 사용합니다.

  필요에 따라 나중에 사용자 지정 방화벽 정책을 만들고 추가할 수 있습니다.

  ⓘ ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 참조하십시오 "LIF의 방화벽 정책을 구성합니다".

- '-자동 되돌리기'를 사용하면 시작, 관리 데이터베이스의 상태 변경 또는 네트워크 연결이 이루어지는 시기에 데이터 LIF가 홈 노드로 자동 복구되는지 여부를 지정할 수 있습니다. 기본 설정은 false로 설정되어 있지만 사용자 환경의 네트워크 관리 정책에 따라 false로 설정할 수 있습니다.

  a. 'network interface show' 명령을 사용하여 LIF가 성공적으로 생성되었는지 확인합니다.

  b. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

다음을 확인하려면…	사용…
IPv4 주소입니다	네트워크 핑
IPv6 주소입니다	네트워크 핑6

  c. Kerberos를 사용하는 경우 1단계부터 3단계까지 반복하여 추가 LIF를 생성합니다.

  Kerberos는 이러한 각 LIF에서 별도로 설정해야 합니다.

예

다음 명령을 실행하면 LIF가 생성되고 '-address' 및 '-netmask' 매개 변수를 사용하여 IP 주소와 네트워크 마스크 값이 지정됩니다.

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

다음 명령을 실행하면 LIF가 생성되고 지정된 서브넷(client1_sub 이름)의 IP 주소와 네트워크 마스크 값이 할당됩니다.

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

다음 명령을 실행하면 cluster-1의 모든 LIF가 표시됩니다. 데이터 LIF datalif1 및 datalif3은 IPv4 주소로 구성되고 datalif4는 IPv6 주소로 구성됩니다.

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

다음 명령을 실행하면 기본 데이터 파일 서비스 정책에 할당된 NAS 데이터 LIF를 생성하는 방법이 표시됩니다.

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

관련 정보

- "네트워크 Ping"
- "네트워크 인터페이스"

ONTAP NFS SVM 호스트 이름 확인을 위해 **DNS** 활성화

SVM에서 DNS를 사용하도록 설정하려면 'vserver services name-service dns' 명령을 사용하고, 호스트 이름 확인을 위해 DNS를 사용하도록 구성할 수 있습니다. 호스트 이름은 외부 DNS 서버를 사용하여 확인됩니다.

시작하기 전에

호스트 이름 조회에 사이트 전체 DNS 서버를 사용할 수 있어야 합니다.

단일 장애 지점을 방지하려면 둘 이상의 DNS 서버를 구성해야 합니다. DNS 서버 이름을 하나만 입력하면 'vserver services name-service dns create' 명령이 경고를 보냅니다.

이 작업에 대해

에 대해 자세히 "SVM에서 동적 DNS 구성"알아보십시오.

단계

1. SVM에서 DNS 활성화:

   'vserver services name-service dns create-vserver_vserver_name_-domain_domain_name_-name-servers_ip_address_-state enabled'

   다음 명령을 실행하면 SVM VS1 에서 외부 DNS 서버 서버가 활성화됩니다.

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   를 클릭합니다 `vserver services name-service dns create` Command는 자동 구성 유효성 검사를 수행하고 ONTAP에서 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

2. 'vserver services name-service dns show' 명령을 사용하여 DNS 도메인 구성을 표시합니다.

   다음 명령을 실행하면 클러스터의 모든 SVM에 대한 DNS 구성이 표시됩니다.

```
vserver services name-service dns show
                                                 Name
Vserver           State     Domains              Servers
----------------- --------- -------------------- -------------
cluster1          enabled   example.com          192.0.2.201,
                                                 192.0.2.202
vs1.example.com   enabled   example.com          192.0.2.201,
                                                 192.0.2.202
```

다음 명령을 실행하면 SVM VS1 에 대한 자세한 DNS 구성 정보가 표시됩니다.

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
         Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. 'vserver services name-service dns check' 명령어를 이용하여 이름 서버의 상태를 확인한다.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

이름 서비스 구성

ONTAP NFS 이름 서비스에 대해 알아보세요

스토리지 시스템의 구성에 따라 ONTAP는 클라이언트에 대한 적절한 액세스를 제공하기 위해 호스트, 사용자, 그룹 또는 넷그룹 정보를 조회해야 합니다. 이 정보를 얻으려면 ONTAP가 로컬 또는 외부 이름 서비스에 액세스하도록 이름 서비스를 구성해야 합니다.

클라이언트 인증 중에 NIS 또는 LDAP와 같은 이름 서비스를 사용하여 이름 조회를 용이하게 해야 합니다. 특히 NFSv4 이상을 구축할 때 보안을 강화하기 위해 가능하면 LDAP를 사용하는 것이 좋습니다. 또한 외부 이름 서버를 사용할 수 없는 경우 로컬 사용자 및 그룹을 구성해야 합니다.

이름 서비스 정보는 모든 소스에서 동기화되어야 합니다.

ONTAP가 로컬 또는 외부 이름 서비스에 문의하여 호스트, 사용자, 그룹, 넷그룹 또는 이름 매핑 정보를 검색할 수 있도록 이름 서비스 스위치 테이블을 올바르게 구성해야 합니다.

시작하기 전에

사용자 환경에 적용할 수 있는 호스트, 사용자, 그룹, 넷그룹 또는 이름 매핑에 사용할 이름 서비스를 결정해야 합니다.

넷그룹을 사용할 계획이라면 RFC 5952에 지정된 대로 넷그룹에 지정된 모든 IPv6 주소를 단축하고 압축해야 합니다.

이 작업에 대해

사용하지 않는 정보 소스는 포함하지 마십시오. 예를 들어 NIS가 사용자 환경에서 사용되지 않는 경우 '-Sources NIS' 옵션을 지정하지 마십시오.

단계

1. 이름 서비스 스위치 테이블에 필요한 항목을 추가합니다.

   'vserver services name-service ns-switch create-vserver_vserver_name_-database_database_name_-sources_source_names_'

2. 이름 서비스 스위치 테이블에 원하는 순서대로 필요한 항목이 포함되어 있는지 확인합니다.

   'vserver services name-service ns-switch show -vserver_vserver_name_'

   수정하려면 'vserver services name-service ns-switch modify' 또는 'vserver services name-service ns-switch delete' 명령을 사용해야 합니다.

예

다음 예에서는 SVM VS1 에서 로컬 넷그룹 파일을 사용할 수 있도록 이름 서비스 스위치 테이블에 새 항목을 생성하고 외부 NIS 서버에서 넷그룹 정보를 순서대로 찾습니다.

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

작업을 마친 후

- 데이터 액세스를 제공하려면 SVM에 지정한 이름 서비스를 구성해야 합니다.
- SVM에 대한 네임 서비스를 삭제할 경우 네임 서비스 스위치 테이블에서 해당 서비스를 제거해야 합니다.

  이름 서비스 스위치 테이블에서 이름 서비스를 삭제하지 않으면 스토리지 시스템에 대한 클라이언트 액세스가 예상대로 작동하지 않을 수 있습니다.

로컬 **UNIX** 사용자 및 그룹을 구성합니다

ONTAP NFS SVM에 대한 로컬 **UNIX** 사용자 및 그룹에 대해 알아보세요**.**

SVM에서 로컬 UNIX 사용자 및 그룹을 사용하여 인증 및 이름 매핑을 수행할 수 있습니다. UNIX 사용자 및 그룹을 수동으로 만들거나 UNIX 사용자 또는 그룹이 포함된 파일을 URI(Uniform

Resource Identifier)에서 로드할 수 있습니다.

클러스터에 결합된 로컬 UNIX 사용자 그룹 및 그룹 구성원의 기본 최대 제한은 32,768입니다. 클러스터 관리자가 이 제한을 수정할 수 있습니다.

ONTAP NFS SVM에서 로컬 UNIX 사용자 생성

'vserver services name-service unix-user create' 명령을 사용하여 로컬 UNIX 사용자를 생성할 수 있습니다. 로컬 UNIX 사용자는 이름 매핑 처리에 사용되는 UNIX 이름 서비스 옵션으로 SVM에서 생성하는 UNIX 사용자입니다.

단계

1. 로컬 UNIX 사용자 생성:

   'vserver services name-service unix-user create-vserver_vserver_name_-user_user_name_-id_integer_-primary-gid_integer_-full-name_full_name_'

   '-user_user_name_'은(는) 사용자 이름을 지정합니다. 사용자 이름의 길이는 64자 이하여야 합니다.

   '-id_integer_'는 사용자가 지정하는 사용자 ID를 지정합니다.

   기본 그룹 ID는 -primary-gid_integer_ 로 지정합니다. 그러면 사용자가 기본 그룹에 추가됩니다. 사용자를 생성한 후 원하는 추가 그룹에 사용자를 수동으로 추가할 수 있습니다.

예

다음 명령을 실행하면 이름이 johnm인 로컬 UNIX 사용자가 이름이 vs1 인 SVM에 생성됩니다. 사용자는 ID 123 및 기본 그룹 ID 100을 가지고 있습니다.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

ONTAP NFS SVM에 로컬 UNIX 사용자 목록 로드

SVM에서 개별 로컬 UNIX 사용자를 수동으로 생성하는 대신 로컬 UNIX 사용자 목록을 URI(Uniform Resource Identifier)에서 SVM으로 로드하여 작업을 단순화할 수 있습니다('vserver services name-service unix-user load-from-Uri').

단계

1. 로드할 로컬 UNIX 사용자 목록이 포함된 파일을 생성합니다.

   파일은 UNIX '/etc/passwd' 형식의 사용자 정보를 포함해야 합니다.

   '*user_name:password:user_ID:group_ID:full_name*'

   명령에서는 '*PASSWORD*' 필드 값과 '*FULL_NAME*' 필드 뒤에 있는 필드 값('*HOME_DIRECTORY*' 및 '*shell*')이 삭제됩니다.

지원되는 최대 파일 크기는 2.5MB입니다.

2. 목록에 중복 정보가 없는지 확인합니다.

   목록에 중복 항목이 포함되어 있으면 목록을 로드하지 못하고 오류 메시지가 표시됩니다.

3. 파일을 서버에 복사합니다.

   스토리지 시스템에서 HTTP, HTTPS, FTP 또는 FTPS를 통해 서버에 연결할 수 있어야 합니다.

4. 파일의 URI를 확인합니다.

   URI는 파일이 있는 위치를 나타내기 위해 스토리지 시스템에 제공하는 주소입니다.

5. 로컬 UNIX 사용자 목록이 포함된 파일을 URI에서 SVM으로 로드합니다.

   'vserver services name-service unix-user load-from-Uri-vserver_vserver_name_-Uri{ftp|http|ftps|https}://*Uri* -overwrite{true|false}'

   '-overwrite'{'true'|'false'}는 엔트리를 덮어쓸지 여부를 지정합니다. 기본값은 false 입니다.

예

다음 명령을 실행하면 URI 'ftp://ftp.example.com/passwd` 에서 이름이 VS1 인 SVM으로 로컬 UNIX 사용자 목록이 로드됩니다. SVM의 기존 사용자는 URI의 정보로 덮어써지지 않습니다.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

ONTAP NFS SVM에 로컬 **UNIX** 그룹 생성

"vserver services name-service unix-group create" 명령을 사용하여 SVM에 로컬인 UNIX 그룹을 생성할 수 있습니다. 로컬 UNIX 그룹은 로컬 UNIX 사용자와 함께 사용됩니다.

단계

1. 로컬 UNIX 그룹 생성:

   'vserver services name-service unix-group create-vserver_vserver_name_-name_group_name_-id_integer_'

   `-name_group_name_'은 그룹 이름을 지정합니다. 그룹 이름의 길이는 64자 이하여야 합니다.

   '-id_integer_'는 지정하는 그룹 ID를 지정합니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 eng인 로컬 그룹이 생성됩니다. 그룹에 ID 101이 있습니다.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

ONTAP NFS SVM의 로컬 **UNIX** 그룹에 사용자 추가

'vserver services name-service unix-group adduser' 명령을 사용하여 SVM에 로컬인 보조 UNIX 그룹에 사용자를 추가할 수 있습니다.

단계

1. 로컬 UNIX 그룹에 사용자 추가:

'vserver services name-service unix-group adduser-vserver_vserver_name_-name_group_name_-username_user_name_'

'-name"*group_name*'은 사용자의 기본 그룹 외에도 사용자를 추가할 UNIX 그룹의 이름을 지정합니다.

예

다음 명령을 실행하면 이름이 max인 사용자가 이름이 eng인 로컬 UNIX 그룹에 이름이 vs1 인 SVM에 추가됩니다.

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

ONTAP NFS SVM의 **URI**에서 로컬 **UNIX** 그룹 로드

개별 로컬 UNIX 그룹을 수동으로 생성하는 대신 'vserver services name-service unix-group load-from-Uri' 명령을 사용하여 URI(Uniform Resource Identifier)에서 SVM으로 로컬 UNIX 그룹 목록을 로드할 수 있습니다.

단계

1. 로드할 로컬 UNIX 그룹 목록이 포함된 파일을 생성합니다.

   파일은 UNIX '/etc/group' 형식의 그룹 정보를 포함해야 합니다.

   '*group_name:password:group_ID:comma_separated_list_of_users*'

   이 명령어는 '*PASSWORD*' 필드의 값을 삭제한다.

   지원되는 최대 파일 크기는 1MB입니다.

   그룹 파일에서 각 줄의 최대 길이는 32,768자입니다.

2. 목록에 중복 정보가 없는지 확인합니다.

   목록에 중복 항목이 없어야 합니다. 그렇지 않으면 목록을 로드하지 못합니다. SVM에 이미 있는 항목이 있으면 "-overwrite" 매개 변수를 "true"로 설정하여 모든 기존 항목을 새 파일로 덮어쓰거나 새 파일에 기존 항목을 복제하는 항목이 없는지 확인해야 합니다.

3. 파일을 서버에 복사합니다.

   스토리지 시스템에서 HTTP, HTTPS, FTP 또는 FTPS를 통해 서버에 연결할 수 있어야 합니다.

4. 파일의 URI를 확인합니다.

   URI는 파일이 있는 위치를 나타내기 위해 스토리지 시스템에 제공하는 주소입니다.

5. 로컬 UNIX 그룹 목록이 포함된 파일을 URI에서 SVM으로 로드합니다.

   'vserver services name-service unix-group load-from-Uri-vserver_vserver_name_-Uri{ftp|http|FTPS|https}://*Uri*-overwrite{true|false}'

   '-overwrite'{'true'|'false'}는 엔트리를 덮어쓸지 여부를 지정합니다. 기본값은 false 입니다. 이 매개 변수를 "true"로 지정하면 ONTAP는 지정된 SVM의 기존 로컬 UNIX 그룹 데이터베이스 전체를 로드하는 파일의 항목으로 바꿉니다.

예

다음 명령을 실행하면 URI 'ftp://ftp.example.com/group` 에서 VS1 이라는 SVM으로 로컬 UNIX 그룹 목록이 로드됩니다. SVM의 기존 그룹은 URI의 정보로 덮어써지지 않습니다.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

넷그룹으로 작업합니다

ONTAP NFS SVM의 넷그룹에 대해 알아보세요

사용자 인증 및 내보내기 정책 규칙의 클라이언트와 일치시키기 위해 넷그룹을 사용할 수 있습니다. 외부 이름 서버(LDAP 또는 NIS)에서 넷그룹에 대한 액세스를 제공하거나, 'vserver services name-service netgroup load' 명령을 사용하여 URI(Uniform Resource Identifier)에서 SVM으로 넷그룹을 로드할 수 있습니다.

시작하기 전에

넷그룹을 사용하기 전에 다음 조건이 충족되는지 확인해야 합니다.

- 소스(NIS, LDAP 또는 로컬 파일)에 관계없이 넷그룹의 모든 호스트는 순방향 및 역방향 DNS 조회를 일관되게 제공하기 위해 정방향(A) 및 역방향(PTR) DNS 레코드를 모두 포함해야 합니다.

  또한 클라이언트의 IP 주소에 PTR 레코드가 여러 개 있는 경우 이러한 모든 호스트 이름은 넷그룹의 구성원이어야 하며 해당 레코드가 있어야 합니다.

- 소스(NIS, LDAP 또는 로컬 파일)에 관계없이 넷그룹에 있는 모든 호스트의 이름은 철자가 올바르고 올바른 대소문자를 사용해야 합니다. 넷그룹에서 사용되는 호스트 이름의 대/소문자 불일치로 인해 내보내기 검사 실패와 같은 예기치 않은 동작이 발생할 수 있습니다.
- 넷그룹에 지정된 모든 IPv6 주소는 RFC 5952에 지정된 대로 단축되고 압축되어야 합니다.

  예를 들어 2011:hu9:0:0:0:0:3:1은 2011:hu9:3:1로 단축되어야 합니다.

이 작업에 대해

넷그룹으로 작업하는 경우 다음 작업을 수행할 수 있습니다.

- 'vserver export-policy netgroup check-membership' 명령을 사용하여 클라이언트 IP가 특정 넷그룹의 구성원인지 여부를 확인할 수 있습니다.
- 'vserver services name-service getxxbyy netgrp' 명령을 사용하여 클라이언트가 넷그룹에 속하는지 확인할 수 있습니다.

  조회를 수행하는 기본 서비스는 구성된 이름 서비스 스위치 순서에 따라 선택됩니다.

ONTAP NFS SVM의 **URI**에서 넷그룹 로드

내보내기 정책 규칙에서 클라이언트를 일치시키는 데 사용할 수 있는 방법 중 하나는 netgroup에 나열된 호스트를 사용하는 것입니다. 외부 이름 서버에 저장된 넷그룹을 사용하는 대신 URI(Uniform Resource Identifier)에서 SVM으로 넷그룹을 로드할 수 있습니다('vserver services name-service netgroup load').

시작하기 전에

넷그룹 파일은 SVM에 로드되기 전에 다음 요구 사항을 충족해야 합니다.

- 파일은 NIS를 채우는 데 사용되는 것과 동일한 적절한 넷그룹 텍스트 파일 형식을 사용해야 합니다.

  ONTAP는 넷그룹 텍스트 파일 형식을 로드하기 전에 검사합니다. 파일에 오류가 있으면 로드되지 않고 파일에서 수행해야 하는 수정 사항을 나타내는 메시지가 표시됩니다. 오류를 해결한 후 Netgroup 파일을 지정된 SVM에 다시 로드할 수 있습니다.

- 넷그룹 파일의 호스트 이름에 있는 모든 영문자는 소문자여야 합니다.
- 지원되는 최대 파일 크기는 5MB입니다.
- 네스팅 넷그룹에 대해 지원되는 최대 수준은 1000입니다.
- 넷그룹 파일에 호스트 이름을 정의할 때는 운영 DNS 호스트 이름만 사용할 수 있습니다.

  내보내기 액세스 문제를 방지하려면 DNS CNAME 또는 라운드 로빈 레코드를 사용하여 호스트 이름을 정의하면 안 됩니다.

- 넷그룹 파일에서 3중 그룹의 사용자 및 도메인 부분은 ONTAP에서 지원하지 않으므로 비워 두어야 합니다.

  호스트/IP 부분만 지원됩니다.

이 작업에 대해

ONTAP는 로컬 넷그룹 파일에 대한 호스트 별 검색을 지원합니다. 넷그룹 파일을 로드하면 ONTAP에서 자동으로 netgroup.byhost 맵을 생성하여 넷그룹 기준 호스트 검색을 설정합니다. 이렇게 하면 내보내기 정책 규칙을 처리하여 클라이언트 액세스를 평가할 때 로컬 넷그룹 검색 속도를 크게 높일 수 있습니다.

단계

1. URI를 통해 넷그룹을 SVM에 로드:

   'vserver services name-service netgroup load-vserver_vserver_name_-source{ftp|http|FTPS|https}://*Uri*'

넷그룹 파일을 로드하고 넷그룹을 생성합니다. byhost 맵은 몇 분 정도 걸릴 수 있습니다.

넷그룹을 업데이트하려면 파일을 편집하고 업데이트된 넷그룹 파일을 SVM에 로드할 수 있습니다.

예

다음 명령을 실행하면 HTTP URL 'http://intranet/downloads/corp-netgroup`: 에서 이름이 VS1 인 SVM에 넷그룹 정의가 로드됩니다

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

ONTAP NFS SVM 넷그룹 정의 확인

SVM에 넷그룹을 로드한 후 'vserver services name-service netgroup status' 명령을 사용하여 넷그룹 정의의 상태를 확인할 수 있습니다. 이렇게 하면 SVM을 백업하는 모든 노드에서 넷그룹 정의가 일관되는지 확인할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 넷그룹 정의의 상태를 확인합니다.

   'vserver services name-service netgroup status'

   자세한 보기에 추가 정보를 표시할 수 있습니다.

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin’입니다

예

권한 수준을 설정한 후 다음 명령을 실행하면 모든 SVM에 대한 넷그룹 상태가 표시됩니다.

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

ONTAP NFS SVM에 대한 **NIS** 도메인 구성 생성

사용자 환경에서 NIS(Network Information Service)를 사용하여 이름 서비스를 제공하는 경우 'vserver services name-service NIS-domain create' 명령을 사용하여 SVM에 대한 NIS 도메인 구성을 생성해야 합니다.

시작하기 전에

SVM에서 NIS 도메인을 구성하기 전에 구성된 모든 NIS 서버를 사용할 수 있고 연결할 수 있어야 합니다.

NIS를 사용하여 디렉터리 검색을 수행할 경우 NIS 서버의 맵에는 각 항목에 대해 1,024자를 초과할 수 없습니다. 이 제한을 준수하지 않는 NIS 서버를 지정하지 마십시오. 그렇지 않으면 NIS 항목에 종속된 클라이언트 액세스가 실패할 수 있습니다.

이 작업에 대해

NIS 데이터베이스에 netgroup.byhost 맵이 포함되어 있으면 ONTAP에서 이를 사용하여 더 빨리 검색할 수 있습니다. 클라이언트 액세스 문제를 방지하려면 디렉토리의 netgroup.byhost 및 netgroup 맵을 항상 동기화해야 합니다. ONTAP 9.7부터 NIS 넷그룹.byhost 항목은 vserver services name-service NIS-domain netgroup-database 명령을 사용하여 캐싱될 수 있습니다.

호스트 이름 확인에 NIS를 사용하는 것은 지원되지 않습니다.

단계

1. NIS 도메인 구성 생성:

```
vserver services name-service nis-domain create -vserver vs1 -domain
```

<domain_name> -nis-servers <IP_addresses>

NIS 서버는 최대 10개까지 지정할 수 있습니다.

그만큼 -nis-servers 필드는 다음을 대체합니다. -servers 필드입니다. 다음을 사용할 수 있습니다. -nis-servers NIS 서버의 호스트 이름이나 IP 주소를 지정하는 필드입니다.

2. 도메인이 생성되었는지 확인합니다.

'vserver services name-service NIS-domain show'를 참조하십시오

예

다음 명령을 실행하면 NIS 도메인용 NIS 도메인 구성이 생성됩니다. SVM은 IP 주소의 NIS nisdomain 서버로 이름이 vs1 지정됩니다. 192.0.2.180

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

LDAP를 사용합니다

ONTAP NFS SVM에서 **LDAP** 이름 서비스 사용에 대해 알아보세요

환경에서 LDAP를 네임 서비스로 사용하는 경우 LDAP 관리자와 협력하여 요구사항 및 적절한 스토리지 시스템 구성을 결정한 다음 SVM을 LDAP 클라이언트로 설정해야 합니다.

ONTAP 9.10.1부터 LDAP 채널 바인딩은 Active Directory 및 이름 서비스 LDAP 연결에 대해 기본적으로 지원됩니다. ONTAP는 시작 TLS 또는 LDAPS가 활성화되고 세션 보안이 서명 또는 봉인으로 설정된 경우에만 LDAP 연결을 사용하여 채널 바인딩을 시도합니다. 이름 서버에서 LDAP 채널 바인딩을 비활성화하거나 다시 활성화하려면 LDAP 클라이언트 modify 명령에 '-try-channel-binding' 매개 변수를 사용합니다.

자세한 내용은 을 참조하십시오"Windows의 2020 LDAP 채널 바인딩 및 LDAP 서명 요구 사항".

- ONTAP용 LDAP를 구성하기 전에 사이트 배포가 LDAP 서버 및 클라이언트 구성에 대한 모범 사례를 충족하는지 확인해야 합니다. 특히 다음 조건을 충족해야 합니다.
  - LDAP 서버의 도메인 이름이 LDAP 클라이언트의 항목과 일치해야 합니다.
  - LDAP 서버에서 지원하는 LDAP 사용자 암호 해시 유형에는 ONTAP에서 지원하는 해시 유형이 포함되어야 합니다.
    - 암호화(모든 유형) 및 SHA-1(SHA, SSHA).
    - ONTAP 9.8부터 SHA-2 해시(SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, SSHA-512)도 지원됩니다.
  - LDAP 서버에 세션 보안 조치가 필요한 경우 LDAP 클라이언트에서 이를 구성해야 합니다.

    다음 세션 보안 옵션을 사용할 수 있습니다.

    - LDAP 서명(데이터 무결성 검사 제공) 및 LDAP 서명 및 봉인(데이터 무결성 검사 및 암호화 제공)

        - TLS를 시작합니다
        - LDAPS(TLS 또는 SSL을 통한 LDAP)
    - 서명되고 봉인된 LDAP 쿼리를 사용하려면 다음 서비스를 구성해야 합니다.
        - LDAP 서버는 GSSAPI(Kerberos) SASL 메커니즘을 지원해야 합니다.
        - LDAP 서버에는 DNS 서버에 설정된 PTR 레코드와 DNS A/AAAA 레코드가 있어야 합니다.
        - Kerberos 서버는 DNS 서버에 SRV 레코드가 있어야 합니다.
    - 시작 TLS 또는 LDAPS를 활성화하려면 다음 사항을 고려해야 합니다.
        - LDAPS 대신 Start TLS를 사용하는 것이 NetApp 모범 사례입니다.
        - LDAPS를 사용하는 경우 ONTAP 9.5 이상에서 TLS 또는 SSL에 대해 LDAP 서버를 활성화해야 합니다. SSL은 ONTAP 9.0-9.4에서 지원되지 않습니다.
        - 도메인에 인증서 서버가 이미 구성되어 있어야 합니다.
    - ONTAP 9.5 이상에서 LDAP 조회 추적을 활성화하려면 다음 조건을 충족해야 합니다.
        - 두 도메인은 다음 신뢰 관계 중 하나로 구성해야 합니다.
            - 양방향
            - 원웨이 - 프라이머리(primary)가 추천 도메인을 신뢰하는 곳입니다
            - 부모-자식
        - DNS는 참조된 모든 서버 이름을 확인하도록 구성되어야 합니다.
        - 도메인 암호는 -bind-as-cifs-server가 true로 설정된 경우 인증하기 위해 동일해야 합니다.

> LDAP 조회 추적에는 다음 구성이 지원되지 않습니다.
>
> - 모든 ONTAP 버전:
>   - 관리 SVM의 LDAP 클라이언트
> - ONTAP 9.8 및 이전 버전(9.9.1 이상에서 지원됨):
>   - LDAP 서명 및 봉인('-session-security' 옵션)
>   - 암호화된 TLS 연결('-use-start-tls' 옵션)
>   - LDAPS 포트 636을 통한 통신('-use-ldaps-for-ad-ldap' 옵션)

- SVM에서 LDAP 클라이언트를 구성할 때 LDAP 스키마를 입력해야 합니다.

  대부분의 경우 기본 ONTAP 스키마 중 하나가 적합합니다. 그러나 사용자 환경의 LDAP 스키마가 이러한 스키마와 다른 경우 LDAP 클라이언트를 생성하기 전에 ONTAP에 대한 새 LDAP 클라이언트 스키마를 만들어야 합니다. 사용자 환경의 요구 사항에 대해서는 LDAP 관리자에게 문의하십시오.

- 호스트 이름 확인에 LDAP를 사용하는 것은 지원되지 않습니다.

를 참조하십시오

- "NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법"
- "ONTAP SMB SVM에 자체 서명된 루트 CA 인증서를 설치합니다"

ONTAP NFS SVM에 대한 새 **LDAP** 클라이언트 스키마 생성

사용자 환경의 LDAP 스키마가 ONTAP 기본값과 다른 경우 LDAP 클라이언트 구성을 생성하기 전에 ONTAP에 대한 새 LDAP 클라이언트 스키마를 만들어야 합니다.

이 작업에 대해

대부분의 LDAP 서버는 ONTAP에서 제공하는 기본 스키마를 사용할 수 있습니다.

- MS-AD-BIS(대부분의 Windows 2012 이상 AD 서버에 대한 기본 스키마)
- AD-IDMU(Windows 2008, Windows 2012 이상 AD 서버)
- AD-SFU(Windows 2003 및 이전 AD 서버)
- RFC-2307(UNIX LDAP 서버)

기본값이 아닌 LDAP 스키마를 사용해야 하는 경우 LDAP 클라이언트 구성을 생성하기 전에 만들어야 합니다. 새 스키마를 만들기 전에 LDAP 관리자에게 문의하십시오.

ONTAP에서 제공하는 기본 LDAP 스키마는 수정할 수 없습니다. 새 스키마를 만들려면 복사본을 만든 다음 복사본을 적절하게 수정합니다.

단계

1. 기존 LDAP 클라이언트 스키마 템플릿을 표시하여 복사할 템플릿을 식별합니다.

   'vserver services name-service ldap client schema show'를 참조하십시오

2. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

3. 기존 LDAP 클라이언트 스키마의 복사본을 만듭니다.

   'vserver services name-service LDAP 클라이언트 스키마 복사 - vserver_vserver_name_-schema_existing_schema_name_-new-schema-name_new_schema_name_'

4. 새 스키마를 수정하고 사용자 환경에 맞게 사용자 지정합니다.

   'vserver services name-service LDAP 클라이언트 스키마 수정

5. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

ONTAP NFS 액세스를 위한 **LDAP** 클라이언트 구성 생성

ONTAP가 사용자 환경의 외부 LDAP 또는 Active Directory 서비스에 액세스하도록 하려면 먼저 스토리지 시스템에서 LDAP 클라이언트를 설정해야 합니다.

시작하기 전에

Active Directory 도메인 확인됨 목록의 처음 세 개 서버 중 하나가 작동 중이고 데이터를 제공하고 있어야 합니다. 그렇지 않으면 이 작업이 실패합니다.

여러 대의 서버가 있으며 그 중 어느 시점에서든 3대 이상의 서버가 다운됩니다.

단계

1. "vserver services name-service ldap client create" 명령에 대한 적절한 구성 값을 확인하려면 LDAP 관리자에게 문의하십시오.

   a. LDAP 서버에 대한 도메인 기반 또는 주소 기반 연결을 지정합니다.

      AD-DOMAIN과 -SERS 옵션은 상호 배타적입니다.

      - Active Directory 도메인에서 LDAP 서버 검색을 설정하려면 '-ad-domain' 옵션을 사용합니다.
        - 를 사용할 수 있습니다 `-restrict-discovery-to-site` LDAP 서버 검색을 지정된 도메인의 CIFS 기본 사이트로 제한하는 옵션입니다. 이 옵션을 사용하는 경우 에서 CIFS 기본 사이트도 지정해야 합니다 `-default-site`.
      - '-preferred-ad-servers' 옵션을 사용하여 쉼표로 구분된 목록에서 IP 주소로 하나 이상의 기본 Active Directory 서버를 지정할 수 있습니다. 클라이언트를 생성한 후 'vserver services name-service ldap client modify' 명령을 사용하여 이 목록을 수정할 수 있습니다.
      - 를 사용합니다 `-servers` 쉼표로 구분된 목록의 IP 주소로 하나 이상의 LDAP 서버(Active Directory 또는 UNIX)를 지정하는 옵션입니다.

        은 더 이상 사용되지 않습니다. `-ldap-servers` 필드는 다음을 대체합니다. `-servers` 필드. 이 필드에는 LDAP 서버의 호스트 이름 또는 IP 주소를 사용할 수 있습니다.

   b. 기본 또는 사용자 지정 LDAP 스키마를 지정합니다.

      대부분의 LDAP 서버는 ONTAP에서 제공하는 기본 읽기 전용 스키마를 사용할 수 있습니다. 그렇지 않으면 기본 스키마를 사용하는 것이 좋습니다. 이 경우 기본 스키마(읽기 전용)를 복사한 다음 복사본을 수정하여 고유한 스키마를 만들 수 있습니다.

      기본 스키마:

      - MS-AD-BIS

        RFC-2307bis를 기반으로 하는 이 방식은 대부분의 표준 Windows 2012 이상 LDAP 구축에 선호되는 LDAP 스키마입니다.

      - AD-IDMU

        UNIX용 Active Directory ID 관리를 기반으로 하는 이 스키마는 대부분의 Windows 2008, Windows 2012 이상 AD 서버에 적합합니다.

      - AD-SFU

        UNIX용 Active Directory 서비스를 기반으로 하는 이 스키마는 대부분의 Windows 2003 및 이전 AD 서버에 적합합니다.

      - RFC-2307

        RFC-2307(*LDAP*를 네트워크 정보 서비스로 사용하는 접근 방식)에 따라 이 스키마는 대부분의 UNIX AD 서버에 적합합니다.

c. 바인딩 값을 선택합니다.

- '-min-bind-level{anonymous|simple|sasl}'은 최소 bind authentication level을 지정한다.

  기본값은 ' * anonymous * '입니다.

- '-bind-dn_ldap_DN_'은 바인딩 사용자를 지정합니다.

  Active Directory 서버의 경우 계정(domain\user) 또는 보안 주체(user@domain.com) 양식에서 사용자를 지정해야 합니다. 그렇지 않으면 고유 이름(CN=user, DC=domain, DC=com) 형식으로 사용자를 지정해야 합니다.

- '-BIND-PASSWORD_PASSWORD_'는 바인딩 암호를 지정합니다.

d. 필요한 경우 세션 보안 옵션을 선택합니다.

LDAP 서버에서 필요한 경우 LDAP 서명 및 봉인 또는 TLS를 통한 LDAP를 활성화할 수 있습니다.

- '--세션-보안{none|sign|seal}'

  서명('사인', 데이터 무결성), 서명 및 봉인('씰', 데이터 무결성 및 암호화) 또는 둘 다('없음', 서명 또는 봉인 없음)을 사용할 수 있습니다. 기본값은 '없음'입니다.

  또한 서명과 봉인 바인딩이 실패할 경우 바인딩 인증을 ' * anonymous * ' 또는 ' * simple * '로 되돌리지 않으려면 '-min-bind-level' {'s ASL'}을 설정해야 합니다.

- '-use-start-tls'{'true'|'false'}

  '* true*'로 설정되어 있고 LDAP 서버가 이를 지원하는 경우 LDAP 클라이언트는 서버에 암호화된 TLS 연결을 사용합니다. 기본값은 ' * FALSE * '입니다. 이 옵션을 사용하려면 LDAP 서버의 자체 서명된 루트 CA 인증서를 설치해야 합니다.

> ⓘ 스토리지 VM에 도메인에 추가된 SMB 서버가 있고 LDAP 서버가 SMB 서버의 홈 도메인의 도메인 컨트롤러 중 하나인 경우 을 수정할 수 있습니다 `-session-security-for-ad-ldap` 옵션을 선택합니다 `vserver cifs security modify` 명령.

e. 포트, 쿼리 및 기준 값을 선택합니다.

기본값을 사용하는 것이 좋지만 LDAP 관리자에게 해당 값이 사용자 환경에 적합한지 확인해야 합니다.

- '-port_port_'는 LDAP 서버 포트를 지정합니다.

  기본값은 389입니다.

Start TLS를 사용하여 LDAP 연결을 보호하려면 기본 포트 389를 사용해야 합니다. 시작 TLS는 LDAP 기본 포트 389를 통한 일반 텍스트 연결로 시작되고 해당 연결은 TLS로 업그레이드됩니다. 포트를 변경하면 Start TLS가 실패합니다.

- '-query-timeout_integer_'는 쿼리 시간 제한(초)을 지정합니다.

  허용 범위는 1 ~ 10초입니다. 기본값은 3초입니다.

- `-base-dn_ldap_dn_'은 기본 DN을 지정합니다.

필요한 경우 여러 값을 입력할 수 있습니다(예: LDAP 조회 추적을 사용하는 경우). 기본값은 ""(root)입니다.

- '-base-scope'{'base'|'onelel'|'ubtree'}는 기본 검색 범위를 지정합니다.

  기본값은 'Subtree'입니다.

- '-referral-enabled'{'true'|'false'}는 LDAP 조회 추적 활성화 여부를 지정합니다.

  ONTAP 9.5부터 LDAP 조회 응답이 기본 LDAP 서버에 반환되어 원하는 레코드가 참조된 LDAP 서버에 있음을 나타내는 경우 ONTAP LDAP 클라이언트가 다른 LDAP 서버에 조회 요청을 참조할 수 있습니다. 기본값은 ' * FALSE * '입니다.

참조된 LDAP 서버에 있는 레코드를 검색하려면 LDAP 클라이언트 구성의 일부로 참조된 레코드의 기본 dn을 기본 dn에 추가해야 합니다.

2. 스토리지 VM에서 LDAP 클라이언트 구성을 생성합니다.

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

   LDAP 클라이언트 구성을 생성할 때 스토리지 VM 이름을 제공해야 합니다.

3. LDAP 클라이언트 구성이 성공적으로 생성되었는지 확인합니다.

   'vserver services name-service ldap client show-client-config client_config_name'

예

다음 명령을 실행하면 스토리지 VM VS1이 LDAP용 Active Directory 서버와 함께 작동하도록 ldap1이라는 새 LDAP 클라이언트 구성이 생성됩니다.

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

다음 명령을 실행하면 스토리지 VM VS1이 Active Directory 서버와 작동하여 서명과 봉인이 필요한 LDAP에 대해 ldap1이라는 새 LDAP 클라이언트 구성이 생성되고 LDAP 서버 검색이 지정된 도메인의 특정 사이트로 제한됩니다.

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

다음 명령을 실행하면 스토리지 VM VS1이 LDAP 조회 추적이 필요한 LDAP용 Active Directory 서버와 작동하도록 ldap1이라는 새 LDAP 클라이언트 구성이 생성됩니다.

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

다음 명령을 실행하면 기본 DN을 지정하여 스토리지 VM VS1에 대해 ldap1이라는 LDAP 클라이언트 구성이 수정됩니다.

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

다음 명령을 실행하면 조회 추적을 활성화하여 스토리지 VM VS1에 대해 ldap1이라는 LDAP 클라이언트 구성이 수정됩니다.

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

ONTAP NFS SVM과 **LDAP** 클라이언트 구성 연결

SVM에서 LDAP를 활성화하려면 "vserver services name-service ldap create" 명령을 사용하여 LDAP 클라이언트 구성을 SVM과 연결해야 합니다.

시작하기 전에

- LDAP 도메인은 네트워크 내에 이미 존재해야 하며 SVM이 있는 클러스터에서 액세스할 수 있어야 합니다.
- SVM에 LDAP 클라이언트 구성이 있어야 합니다.

단계

1. SVM에서 LDAP 지원:

'vserver services name-service LDAP create-vserver_vserver_name_-client-config_client_config_name_'

> 그만큼 `vserver services name-service ldap create` 명령은 자동 구성 검증을 수행하고 ONTAP 이름 서버에 접속할 수 없는 경우 오류 메시지를 보고합니다.

다음 명령을 실행하면 "VS1" SVM에서 LDAP를 활성화하고 "ldap1" LDAP 클라이언트 구성을 사용하도록 구성합니다.

```
cluster1::> vserver services name-service ldap create -vserver vs1
-client-config ldap1 -client-enabled true
```

2. vserver services name-service ldap check 명령을 사용하여 이름 서버의 상태를 확인합니다.

   다음 명령은 SVM VS1 에서 LDAP 서버의 유효성을 검사합니다.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                  |
```

ONTAP NFS SVM에 대한 **LDAP** 소스 확인

SVM을 위한 네임 서비스 스위치 테이블에 네임 서비스에 대한 LDAP 소스가 올바르게 나열되어 있는지 확인해야 합니다.

단계

1. 현재 이름 서비스 스위치 테이블 내용을 표시합니다.

   'vserver services name-service ns-switch show -vserver_svm_name_'

   다음 명령을 실행하면 SVM My_SVM의 결과가 표시됩니다.

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                Source
Vserver         Database        Order
--------------- ------------    ---------
My_SVM          hosts           files,
                                dns
My_SVM          group           files,ldap
My_SVM          passwd          files,ldap
My_SVM          netgroup        files
My_SVM          namemap         files
5 entries were displayed.
```

이름 매핑 정보를 검색할 소스 및 순서를 지정합니다. UNIX 전용 환경에서는 이 항목이 필요하지 않습니다. 이름 매핑은 UNIX와 Windows를 모두 사용하는 혼합 환경에서만 필요합니다.

2. 필요에 따라 ns-switch 항목을 업데이트합니다.

ns-switch 항목을 업데이트하려면...	명령 입력...
사용자 정보	'vserver services name-service ns-switch modify -vserver_vserver_name_-database passwd - sources ldap, files'
그룹 정보	'vserver services name-service ns-switch modify -vserver_vserver_name_-database group-sources ldap, files'
넷그룹 정보입니다	'vserver services name-service ns-switch modify -vserver_vserver_name_-database 넷그룹 - 소스 LDAP, 파일

강력한 보안을 위해 **NFS**와 **Kerberos** 사용

보안 인증을 위해 **ONTAP NFS**와 함께 **Kerberos**를 사용하는 방법에 대해 알아보세요**.**

Kerberos가 강력한 인증을 위해 사용자 환경에서 사용되는 경우 Kerberos 관리자와 협력하여 요구사항 및 적절한 스토리지 시스템 구성을 결정한 다음 SVM을 Kerberos 클라이언트로 사용하도록 설정해야 합니다.

환경은 다음 지침을 충족해야 합니다.

- ONTAP용 Kerberos를 구성하기 전에 Kerberos 서버 및 클라이언트 구성에 대한 모범 사례를 따라야 합니다.
- 가능하면 Kerberos 인증이 필요한 경우 NFSv4 이상을 사용합니다.

  NFSv3은 Kerberos와 함께 사용할 수 있습니다. 하지만 Kerberos의 모든 보안 이점은 NFSv4 이상의 ONTAP 구축에서만 실현됩니다.

- 중복 서버 액세스를 프로모션하려면 Kerberos가 동일한 SPN을 사용하여 클러스터의 여러 노드에 있는 여러 데이터 LIF에서 활성화되어야 합니다.
- SVM에서 Kerberos를 사용하도록 설정할 경우 NFS 클라이언트 구성에 따라 볼륨 또는 qtree의 내보내기 규칙에 다음 보안 방법 중 하나를 지정해야 합니다.
  - "krb5"(Kerberos v5 프로토콜)
  - "krb5i"(체크섬을 사용한 무결성 검사를 포함한 Kerberos v5 프로토콜)
  - "krb5p"(개인정보 보호 서비스가 있는 Kerberos v5 프로토콜)

Kerberos 서버 및 클라이언트 외에도 ONTAP가 Kerberos를 지원하도록 다음과 같은 외부 서비스를 구성해야 합니다.

- 디렉터리 서비스

  SSL/TLS를 통해 LDAP를 사용하도록 구성된 Active Directory 또는 OpenLDAP와 같은 환경에서 보안 디렉터리 서비스를 사용해야 합니다. 요청이 일반 텍스트로 전송되므로 안전하지 않은 NIS를 사용하지 마십시오.

- NTP

  NTP를 실행하는 작업 시간 서버가 있어야 합니다. 시간 편중이 발생하여 Kerberos 인증 실패를 방지하려면 이 작업이 필요합니다.

- 도메인 이름 확인(DNS)

  각 UNIX 클라이언트와 각 SVM LIF에는 정방향 및 역방향 조회 영역에서 KDC에 등록된 적절한 서비스 레코드(SRV)가 있어야 합니다. 모든 참가자는 DNS를 통해 제대로 확인할 수 있어야 합니다.

ONTAP SVM에서 **NFS Kerberos** 구성에 대한 **UNIX** 권한 확인

Kerberos를 사용하려면 SVM 루트 볼륨 및 로컬 사용자 및 그룹에 대해 특정 UNIX 사용 권한을 설정해야 합니다.

단계

1. SVM 루트 볼륨에 대한 관련 권한을 표시합니다.

   'volume show-volume_root_vol_name_-fields user, group, unix-permissions

   SVM의 루트 볼륨에는 다음 구성이 있어야 합니다.

이름...	설정 중...
UID	루트 또는 ID 0
GID	루트 또는 ID 0
Unix 사용 권한	755

   이 값이 표시되지 않으면 볼륨 수정 명령을 사용하여 값을 업데이트합니다.

2. 로컬 UNIX 사용자를 표시합니다.

'vserver services name-service unix-user show -vserver_vserver_name_'

SVM에는 다음과 같은 UNIX 사용자가 구성되어 있어야 합니다.

사용자 이름입니다	사용자 **ID**입니다	기본 그룹 **ID**입니다	설명
NFS 를 참조하십시오	500입니다	0	GSS INIT 단계에 필요함. NFS 클라이언트 사용자 SPN의 첫 번째 구성 요소가 사용자로 사용됩니다. NFS 클라이언트 사용자의 SPN에 대한 Kerberos-UNIX 이름 매핑이 있는 경우 NFS 사용자는 필요하지 않습니다.
루트	0	0	마운팅에 필요합니다.

이러한 값이 표시되지 않으면 'vserver services name-service unix-user modify' 명령을 사용하여 해당 값을 업데이트할 수 있습니다.

3. 로컬 UNIX 그룹을 표시합니다.

   'vserver services name-service unix-group show -vserver_vserver__name'

   SVM에는 다음과 같은 UNIX 그룹이 구성되어 있어야 합니다.

그룹 이름	그룹 **ID**입니다
데몬	1
루트	0

이러한 값이 표시되지 않으면 'vserver services name-service unix-group modify' 명령을 사용하여 해당 값을 업데이트할 수 있습니다.

ONTAP SVM에서 **NFS Kerberos** 영역 구성 만들기

ONTAP가 사용자 환경에서 외부 Kerberos 서버에 액세스하도록 하려면 먼저 기존 Kerberos 영역을 사용하도록 SVM을 구성해야 합니다. 이렇게 하려면 Kerberos KDC 서버에 대한 구성 값을 수집한 다음 "vserver NFS Kerberos realm create" 명령을 사용하여 SVM에서 Kerberos 영역 구성을 생성해야 합니다.

시작하기 전에

클러스터 관리자는 인증 문제를 방지하기 위해 스토리지 시스템, 클라이언트 및 KDC 서버에서 NTP를 구성해야 합니다. 클라이언트와 서버 간의 시간 차이(클럭 편중)는 인증 실패의 일반적인 원인입니다.

단계

1. Kerberos 관리자에게 문의하여 "vserver NFS Kerberos realm create" 명령을 제공하는 적절한 구성 값을 확인하십시오.
2. SVM에서 Kerberos 영역 구성 생성:

   "vserver NFS Kerberos 영역 create -vserver_vserver_name_
   -realm_realm_name__{AD_KDC_server_values|AD_KDC_server_values}_-comment "*text*"

3. Kerberos 영역 구성이 성공적으로 생성되었는지 확인합니다.

   가상 NFS Kerberos 영역 표시

예

다음 명령을 실행하면 Microsoft Active Directory 서버를 KDC 서버로 사용하는 SVM VS1 용 NFS Kerberos 영역 구성이 생성됩니다. Kerberos 영역은 AUTH.EXAMPLE.COM 입니다. Active Directory 서버의 이름은 ad-1이고 IP 주소는 10.10.8.14입니다. 허용되는 시간 편중은 300초(기본값)입니다. KDC 서버의 IP 주소는 10.10.8.14이고 포트 번호는 88(기본값)입니다. "Microsoft Kerberos 구성"이 주석입니다.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

다음 명령을 실행하면 MIT KDC를 사용하는 SVM VS1 용 NFS Kerberos 영역 구성이 생성됩니다. Kerberos 영역은 SECURITY.EXAMPLE.COM 입니다. 허용되는 시간 편중은 300초입니다. KDC 서버의 IP 주소는 10.10.9.1이고 포트 번호는 88입니다. KDC 공급업체는 UNIX 공급업체를 나타내는 기타 벤더입니다. 관리 서버의 IP 주소는 10.10.9.1이고 포트 번호는 749(기본값)입니다. 암호 서버의 IP 주소는 10.10.9.1이고 포트 번호는 464(기본값)입니다. "UNIX Kerberos 구성"이 주석입니다.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

ONTAP SVM에 대해 **NFS Kerberos** 허용 암호화 유형 구성

기본적으로 ONTAP는 NFS Kerberos인 DES, 3DES, AES-128, AES-256에 대해 다음 암호화 유형을 지원합니다. "vserver nfs modify" 명령을 `-enc-types' 매개 변수와 함께 사용하면 각 SVM에 대해 허용된 암호화 유형을 특정 환경의 보안 요구사항에 맞게 구성할 수 있습니다.

이 작업에 대해

클라이언트 호환성을 극대화하기 위해 ONTAP는 기본적으로 약한 DES와 강력한 AES 암호화를 모두 지원합니다. 예를 들어, 보안을 강화하려는 경우 사용자 환경에서 이 절차를 사용하여 DES 및 3DES를 비활성화하고 클라이언트가 AES

암호화만 사용하도록 할 수 있습니다.

사용 가능한 가장 강력한 암호화를 사용해야 합니다. ONTAP의 경우, AES-256입니다. 해당 환경에서 이 암호화 수준이 지원되는지 KDC 관리자에게 확인해야 합니다.

- SVM에서 AES를 완전히 활성화 또는 비활성화(AES-128 및 AES-256 모두)하면 원래의 DES 기본/키탭 파일이 삭제되므로 SVM을 위한 모든 LIF에서 Kerberos 구성을 비활성화해야 합니다.

  이를 변경하기 전에 NFS 클라이언트가 SVM에서 AES 암호화를 사용하지 않는지 확인해야 합니다.

- DES 또는 3DES를 활성화 또는 비활성화할 경우 LIF에서 Kerberos 구성을 변경할 필요가 없습니다.

단계

1. 허용되는 암호화 유형을 사용하거나 사용하지 않도록 설정합니다.

활성화 또는 비활성화하려는 경우...	다음 단계를 따르십시오...
DES 또는 3DES입니다	a. SVM의 NFS Kerberos 허용 암호화 유형을 구성합니다. + 'vserver NFS modify -vserver_vserver_name_-enc -types_encryption_types_' 여러 암호화 유형을 쉼표로 구분합니다. b. 성공적으로 변경되었는지 확인합니다. + 'vserver nfs show -vserver_vserver_name_ -fields fitted-enc-types'

활성화 또는 비활성화하려는 경우...	다음 단계를 따르십시오...
AES-128 또는 AES-256	a. SVM 및 LIF Kerberos 사용 설정 식별: + 'vserver NFS Kerberos interface show b. NFS Kerberos에서 허용할 암호화 유형을 수정하려는 SVM의 모든 LIF에서 Kerberos를 해제합니다. + 'vserver NFS Kerberos interface disable-lif_lif_name_' c. SVM의 NFS Kerberos 허용 암호화 유형을 구성합니다. + 'vserver NFS modify -vserver_vserver_name_-enc -types_encryption_types_' 여러 암호화 유형을 쉼표로 구분합니다. d. 성공적으로 변경되었는지 확인합니다. + 'vserver nfs show -vserver_vserver_name_ -fields fitted-enc-types' e. SVM의 모든 LIF에서 Kerberos를 사용하도록 다시 설정합니다. + 'vserver NFS Kerberos interface enable-lif_lif_name_-spN_service_principal_name_' f. 모든 LIF에서 Kerberos가 설정되어 있는지 확인합니다. + "vserver NFS Kerberos interface show

ONTAP LIF에서 **NFS Kerberos** 활성화

데이터 LIF에서 Kerberos를 사용하도록 설정하려면 'vserver NFS Kerberos interface enable' 명령을 사용하십시오. 그러면 SVM에서 NFS에 Kerberos 보안 서비스를 사용할 수 있습니다.

이 작업에 대해

Active Directory KDC를 사용하는 경우 사용되는 SPN의 처음 15자는 영역 또는 도메인 내의 SVM에서 고유해야 합니다.

단계

1. NFS Kerberos 구성 생성:

   'vserver NFS Kerberos interface enable-vserver_vserver_name_-lif_logical_interface_-spN_service_principal_name_'

   ONTAP에서 Kerberos 인터페이스를 활성화하려면 KDC의 SPN에 대한 암호 키가 필요합니다.

   Microsoft KDC의 경우 KDC에 문의하고 CLI에서 사용자 이름 및 암호 프롬프트가 발급되어 비밀 키를 얻습니다. Kerberos 영역의 다른 OU에 SPN을 만들어야 하는 경우 선택적 '-ou' 매개 변수를 지정할 수 있습니다.

   비 Microsoft KDC의 경우 다음 두 가지 방법 중 하나를 사용하여 비밀 키를 얻을 수 있습니다.

만약...	다음 매개 변수도 명령에 포함해야 합니다.
KDC에서 직접 키를 검색하려면 KDC 관리자 자격 증명을 사용합니다	'-admin-username"*kdc_admin_username*'
KDC 관리자 자격 증명이 없지만 키가 포함된 KDC의 keytab 파일이 있습니다	'-keytab-Uri '{ftp

2. Kerberos가 LIF에서 설정되었는지 확인합니다.

   'vserver nfs Kerberos-config show'

3. 1단계와 2단계를 반복하여 여러 LIF에서 Kerberos를 사용하도록 설정합니다.

예

다음 명령을 실행하면 OU lab2ou 에서 SPN NFS /ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM 와 함께 논리 인터페이스 ves03-d1에서 이름이 VS1 인 SVM에 대한 NFS Kerberos 구성이 생성되고 확인됩니다.

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- --------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

NFS 지원 SVM에 스토리지 용량 추가

ONTAP NFS 지원 **SVM**에 스토리지 용량을 추가하는 방법에 대해 알아보세요.

NFS 지원 SVM에 스토리지 용량을 추가하려면 스토리지 컨테이너를 제공할 볼륨 또는 qtree를 생성하고 해당 컨테이너의 엑스포트 정책을 생성하거나 수정해야 합니다. 그런 다음 클러스터에서 NFS 클라이언트 액세스를 확인하고 클라이언트 시스템에서 액세스를 테스트할 수 있습니다.

시작하기 전에

- SVM에서 NFS를 완전히 설정해야 합니다.
- SVM 루트 볼륨의 기본 엑스포트 정책에는 모든 클라이언트에 액세스할 수 있는 규칙이 포함되어 있어야 합니다.
- 이름 서비스 구성에 대한 모든 업데이트를 완료해야 합니다.

- Kerberos 구성에 대한 추가 또는 수정을 완료해야 합니다.

ONTAP NFS 내보내기 정책 만들기

내보내기 규칙을 만들기 전에 해당 규칙을 보유할 내보내기 정책을 만들어야 합니다. 'vserver export-policy create' 명령을 사용하여 엑스포트 정책을 생성할 수 있습니다.

단계

1. 엑스포트 정책 생성:

   'vserver export-policy create-vserver_vserver_name_-policyname_policy_name_'

   정책 이름은 최대 256자까지 지정할 수 있습니다.

2. 엑스포트 정책이 생성되었는지 확인:

   'vserver export-policy show-policyname_policy_name_'

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 exp1 이라는 엑스포트 정책이 생성되는지 검증 및 됩니다.

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

ONTAP NFS 내보내기 정책에 규칙 추가

규칙이 없으면 내보내기 정책은 클라이언트에 데이터에 대한 액세스를 제공할 수 없습니다. 새 내보내기 규칙을 만들려면 클라이언트를 식별하고 클라이언트 일치 형식을 선택하고, 액세스 및 보안 유형을 선택하고, 익명 사용자 ID 매핑을 지정하고, 규칙 인덱스 번호를 선택하고, 액세스 프로토콜을 선택해야 합니다. 그런 다음 'vserver export-policy rule create' 명령을 사용하여 내보내기 정책에 새 규칙을 추가할 수 있습니다.

시작하기 전에

- 내보내기 규칙을 추가할 엑스포트 정책이 이미 있어야 합니다.
- 데이터 SVM에서 DNS를 올바르게 구성해야 하며, DNS 서버는 NFS 클라이언트를 위한 올바른 항목을 가지고 있어야 합니다.

  이는 ONTAP가 특정 클라이언트 일치 형식에 대해 데이터 SVM의 DNS 구성을 사용하여 DNS 조회를 수행하고, 엑스포트 정책 규칙 일치의 실패로 인해 클라이언트 데이터 액세스가 차단되기 때문입니다.

- Kerberos를 사용하여 인증하는 경우 NFS 클라이언트에서 사용되는 다음 보안 방법 중 하나를 결정해야 합니다.
  - "krb5"(Kerberos V5 프로토콜)

- "krb5i"(체크섬을 사용한 무결성 검사가 가능한 Kerberos V5 프로토콜)
- 'krb5p'(개인정보 보호 서비스가 있는 Kerberos V5 프로토콜)

이 작업에 대해

내보내기 정책의 기존 규칙이 클라이언트 일치 및 액세스 요구 사항을 포함하는 경우에는 새 규칙을 생성할 필요가 없습니다.

Kerberos를 사용하여 인증하는 경우 Kerberos를 통해 SVM의 모든 볼륨에 액세스할 경우 루트 볼륨에 대한 내보내기 규칙 옵션 '-rorule', '-rwrule' 및 '-superuser'를 krb5', krb5i 또는 krb5p로 설정할 수 있습니다.

단계

1. 새 규칙의 클라이언트 및 클라이언트 일치 형식을 식별합니다.

   '-clientmatch' 옵션은 규칙이 적용되는 클라이언트를 지정합니다. 하나 또는 여러 개의 클라이언트 일치 값을 지정할 수 있습니다. 여러 값의 사양은 쉼표로 구분해야 합니다. 다음 형식 중 하나로 일치 항목을 지정할 수 있습니다.

클라이언트 일치 형식입니다	예
도메인 이름 앞에 "." 문자가 옵니다	
호스트 이름입니다	'host1' 또는 'host1, host2,...'
IPv4 주소입니다	10.1.12.24 또는 + 10.1.12.24,10.1.12.25,…+
서브넷 마스크가 있는 IPv4 주소는 비트 수로 표시됩니다	10.1.12.10/4, 또는 + 10.1.12.10/4,10.1.12.11/4,…+
네트워크 마스크가 있는 IPv4 주소입니다	10.1.16.0/255.255.255.0 또는 + 10.1.16.0/255.255.255.0, 10.1.17.0/255.255.255.0,…+
점선 형식의 IPv6 주소입니다	'::1.2.3.4' 또는 '::1.2.3.4,::1.2.3.5,...'
서브넷 마스크가 있는 IPv6 주소는 비트 수로 표시됩니다	"ff::00/32" 또는 "ff::00/32, ff: 01/32,..."
넷그룹 이름 앞에 @ 문자가 오는 단일 넷그룹	'@netgroup1' 또는 '@netgroup1,@netgroup2,...'

   클라이언트 정의 형식(예: '.example.com,@netgroup1`)을 결합할 수도 있습니다.

   IP 주소를 지정할 때 다음 사항에 유의하십시오.

   - 10.1.12.10-10.1.12.70 등의 IP 주소 범위를 입력할 수 없습니다.

     이 형식의 항목은 텍스트 문자열로 해석되며 호스트 이름으로 처리됩니다.

   - 클라이언트 액세스의 세부 관리에 대한 내보내기 규칙에서 개별 IP 주소를 지정할 때 동적으로 할당되는 IP 주소(예: DHCP) 또는 임시로 할당된 IP 주소(예: IPv6)를 지정하지 마십시오.

그렇지 않으면 IP 주소가 변경되면 클라이언트가 액세스 권한을 잃게 됩니다.

- 네트워크 마스크로 IPv6 주소(예: ff::12/ff::00)를 입력할 수 없습니다.

2. 클라이언트 일치에 대한 액세스 및 보안 유형을 선택합니다.

지정된 보안 유형으로 인증하는 클라이언트에 대해 다음 액세스 모드 중 하나 이상을 지정할 수 있습니다.

- '-rorule'(읽기 전용 액세스)
- '-rwrule'(읽기-쓰기 액세스)
- '-superuser'(루트 액세스)

> 내보내기 규칙에서 해당 보안 유형에 대한 읽기 전용 액세스도 허용하는 경우 클라이언트는 특정 보안 유형에 대한 읽기-쓰기 액세스만 얻을 수 있습니다. 읽기 전용 매개 변수가 읽기-쓰기 매개 변수보다 보안 형식에 대해 더 제한적인 경우 클라이언트는 읽기-쓰기 액세스를 얻지 못할 수 있습니다. 수퍼유저 액세스도 마찬가지입니다.

규칙에 대해 여러 보안 유형의 쉼표로 구분된 목록을 지정할 수 있습니다. 보안 유형을 "모두" 또는 "사용 안 함"으로 지정하는 경우 다른 보안 유형을 지정하지 마십시오. 다음 유효한 보안 유형 중에서 선택하십시오.

보안 유형을 다음으로 설정한 경우...	일치하는 클라이언트가 내보낸 데이터에 액세스할 수 있습니다...
모두	항상, 들어오는 보안 유형에 관계없이.
"없음"	보안 유형을 가진 클라이언트만 나열되면 익명 액세스 권한이 부여됩니다. 다른 보안 유형과 함께 나열되는 경우 지정된 보안 유형의 클라이언트는 액세스 권한이 부여되고 다른 보안 유형의 클라이언트는 익명 액세스 권한이 부여됩니다.
"안 돼.	수신 보안 유형에 관계없이 사용 안 함.
krb5	Kerberos 5에 의해 인증되는 경우 인증 전용: 각 요청 및 응답의 헤더가 서명됩니다.
krb5i	Kerberos 5i에 의해 인증되는 경우. 인증 및 무결성: 각 요청 및 응답의 헤더와 본문이 서명됩니다.
크르b5p	Kerberos 5p에 의해 인증되는 경우 인증, 무결성 및 개인 정보 보호: 각 요청 및 응답의 헤더와 본문이 서명되고 NFS 데이터 페이로드가 암호화됩니다.
NTLM	CIFS NTLM에 의해 인증되는 경우
'스'입니다	NFS AUTH_SYS에 의해 인증되는 경우

권장 보안 유형은 '시스', 또는 Kerberos를 사용하는 경우 krb5, krb5i, krb5p입니다.

NFSv3에서 Kerberos를 사용하는 경우, 내보내기 정책 규칙은 krb5 이외에 '-rorule' 및 '-rwrule' 액세스를 허용해야 합니다. 이는 내보내기에 대한 NLM(Network Lock Manager) 액세스를 허용해야 하기 때문입니다.

3. 익명 사용자 ID 매핑을 지정합니다.

   '-anon' 옵션은 사용자 ID가 0인 클라이언트 요청에 매핑된 UNIX 사용자 ID 또는 사용자 이름을 지정합니다. 이 사용자 이름은 일반적으로 사용자 이름 루트와 연결됩니다. 기본값은 65534입니다. NFS 클라이언트는 일반적으로 사용자 ID 65534를 사용자 이름 nobody(또는 *root squooting*)와 연결합니다. ONTAP에서 이 사용자 ID는 사용자 pcuser와 연결됩니다. 사용자 ID가 0인 클라이언트에서 액세스를 비활성화하려면 값을 65535로 지정합니다.

4. 규칙 인덱스 순서를 선택합니다.

   ruleindex 옵션은 규칙의 인덱스 번호를 지정합니다. 규칙은 인덱스 번호 목록의 순서에 따라 평가되며, 인덱스 번호가 낮은 규칙은 먼저 평가됩니다. 예를 들어 인덱스 번호가 1인 규칙은 인덱스 번호가 2인 규칙 전에 평가됩니다.

추가하는 경우...	그러면...
엑스포트 정책에 대한 첫 번째 규칙	1을 입력합니다.
엑스포트 정책에 대한 추가 규칙	a. 정책에 기존 규칙을 표시합니다. + 'vserver export-policy rule show-instance-policyname_your_policy_' b. 평가해야 하는 순서에 따라 새 규칙의 인덱스 번호를 선택합니다.

5. 해당 NFS 액세스 값 {'NFS'|'NFS3'|'nfs4'}을 선택합니다.

   NFS는 어떤 버전이든 일치하며 NFS3, nfs4는 특정 버전만을 일치시킵니다.

6. 내보내기 규칙을 만들어 기존 엑스포트 정책에 추가합니다.

   'vserver export-policy rule create-vserver_vserver_name_-policyname_policy_name_-ruleindex_integer_-protocol{nNFS|NFS3|nfs4}-clientmatch {text|*"text,text,…"*}-rorule_security_type_-superuser_security_type_ananID

7. 내보내기 정책의 규칙을 표시하여 새 규칙이 있는지 확인합니다.

   'vserver export-policy rule show-policyname_policy_name_'

   명령은 해당 정책에 적용되는 규칙 목록을 포함하여 해당 엑스포트 정책에 대한 요약을 표시합니다. ONTAP는 각 규칙에 규칙 인덱스 번호를 할당합니다. 규칙 인덱스 번호를 알고 나면 이 번호를 사용하여 지정된 엑스포트 규칙에 대한 자세한 정보를 표시할 수 있습니다.

8. 내보내기 정책에 적용된 규칙이 올바르게 구성되었는지 확인합니다.

   'vserver export-policy rule show -policyname_policy_name_-vserver_vserver_name_-ruleindex_integer_'

예

다음 명령은 RS1이라는 엑스포트 정책에서 VS1이라는 SVM에 엑스포트 규칙이 생성되었는지 확인합니다. 규칙에 인덱스 번호가 1입니다. 이 규칙은 eng.company.com 도메인에 있는 모든 클라이언트와 netgroup@netgroup1과

일치합니다. 이 규칙은 모든 NFS 액세스를 설정합니다. AUTH_SYS로 인증된 사용자에 대한 읽기 전용 및 읽기-쓰기 액세스를 활성화합니다. UNIX 사용자 ID가 0인 클라이언트는 Kerberos로 인증되지 않는 한 익명화됩니다.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                Vserver: vs1
                            Policy Name: exp1
                             Rule Index: 1
                           Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                            RO Access Rule: sys
                            RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

다음 명령은 expol2라는 엑스포트 정책에서 VS2라는 SVM에 엑스포트 규칙이 생성되었는지 확인합니다. 규칙의 인덱스 번호는 21입니다. 이 규칙은 클라이언트를 netgroup dev_netgroup_main의 구성원과 일치시킵니다. 이 규칙은 모든 NFS 액세스를 설정합니다. AUTH_SYS로 인증되고 읽기-쓰기 및 루트 액세스에 Kerberos 인증이 필요한 사용자에 대해 읽기 전용 액세스를 활성화합니다. UNIX 사용자 ID가 0인 클라이언트는 Kerberos로 인증되지 않는 한 루트 액세스가 거부됩니다.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                   Vserver: vs2
                                Policy Name: expol2
                                 Rule Index: 21
                            Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                            @dev_netgroup_main
                             RO Access Rule: sys
                             RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                   Superuser Security Types: krb5
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

볼륨 또는 **qtree** 스토리지 컨테이너를 생성합니다

ONTAP NFS 볼륨 생성

볼륨을 생성하고 "volume create" 명령을 사용하여 해당 접합 지점 및 기타 속성을 지정할 수 있습니다.

이 작업에 대해

클라이언트에서 데이터를 사용할 수 있도록 하려면 볼륨에 _junction path_가 포함되어야 합니다. 새 볼륨을 생성할 때 접합 경로를 지정할 수 있습니다. 접합 경로를 지정하지 않고 볼륨을 생성하는 경우, "volume mount" 명령을 사용하여 SVM 네임스페이스에서 볼륨을 _mount_해야 합니다.

시작하기 전에

- NFS를 설정하고 실행해야 합니다.
- SVM 보안 유형은 UNIX여야 합니다.
- ONTAP 9.13.1부터 용량 분석 및 활동 추적이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 `volume create` 또는 `-activity-tracking-state` 를 로 설정하여 `on` 명령을 `-analytics-state` 실행합니다.

용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 "파일 시스템 분석 설정". 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 교차점으로 볼륨을 생성합니다.

   `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {`*`integer`*`[KB|MB|GB|TB|PB]} -security-style unix -user` *`user_name_or_number`* `-group` *`group_name_or_number`* `-junction-path` *`junction_path`* `[-policy` *`export_policy_name`*`]`

   '-junction-path'의 선택 항목은 다음과 같습니다.

   - 루트 바로 아래, 예: '/*new_vol*'

     새 볼륨을 생성하고 SVM 루트 볼륨에 직접 마운트하도록 지정할 수 있습니다.

   - 기존 디렉토리 아래에, 예: "/*existing_dir/new_vol*"

     새 볼륨을 생성하고 기존 계층 구조에서 기존 볼륨에 마운트하도록 지정할 수 있습니다. 이 볼륨은 디렉토리로 표시됩니다.

     새 볼륨 아래의 새 계층 구조에서 "*/new_dir/new_vol*"와 같은 새 디렉토리에 볼륨을 생성하려면 먼저 SVM 루트 볼륨에 대한 분기인 새 상위 볼륨을 생성해야 합니다. 그런 다음 새 상위 볼륨(새 디렉토리)의 접합 경로에 새 하위 볼륨을 생성합니다.

   + 기존 엑스포트 정책을 사용하려는 경우 볼륨을 생성할 때 지정할 수 있습니다. 나중에 볼륨 수정 명령을 사용하여 내보내기 정책을 추가할 수도 있습니다.

2. 볼륨이 원하는 접합 지점으로 생성되었는지 확인합니다.

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

예

다음 명령을 실행하면 SVM vs1.example.com 및 애그리게이트 aggr1에 user1이라는 새 볼륨이 생성됩니다. 새 볼륨은 '/users'에서 사용할 수 있습니다. 볼륨의 크기는 750GB이고 볼륨 유형은 볼륨 유형입니다(기본값).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- -------  -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

다음 명령을 실행하면 SVM "vs1.example.com" 및 애그리게이트 "aggr1"에 "home4"라는 새 볼륨이 생성됩니다. VS1

SVM은 이름 공간에 /ENG/ 디렉토리가 이미 있으며, '/ENG/' 네임스페이스의 홈 디렉토리가 되는 '/ENG/HOME'에서 새 볼륨을 사용할 수 있습니다. 볼륨 크기는 750GB이고 볼륨 보장은 볼륨 유형입니다(기본값).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

ONTAP NFS qtree 생성

'volume qtree create' 명령을 사용하여 데이터를 포함하는 qtree를 생성하고 해당 속성을 지정할 수 있습니다.

시작하기 전에

- SVM과 새 qtree가 포함될 볼륨이 이미 존재해야 합니다.
- SVM 보안 스타일은 UNIX여야 하며 NFS를 설정하고 실행해야 합니다.

단계

1. qtree 생성:

   '볼륨 qtree create-vserver_vserver_name_{-volume_volume_name_-qtree_qtree_name_|-qtree-path_qtree path_} - 보안 스타일 UNIX [-policy_export_policy_name_]'

   볼륨과 qtree를 별도의 인수로 지정하거나 qtree 경로 인수를 '/vol/*volume_name/_qtree_name*' 형식으로 지정할 수 있습니다.

   기본적으로 Qtree는 상위 볼륨의 엑스포트 정책을 상속하지만, 자체 정책을 사용하도록 구성할 수 있습니다. 기존 엑스포트 정책을 사용하려는 경우 qtree를 생성할 때 지정할 수 있습니다. 나중에 'volume qtree modify' 명령을 사용하여 엑스포트 정책을 추가할 수도 있습니다.

2. qtree가 원하는 접합 경로로 생성되었는지 확인합니다.

   'volume qtree show-vserver_vserver_name_{-volume_volume_name_-qtree_qtree_name_|-qtree-path_qtree path_}'

예

다음 예에서는 junction path '/vol/data1'이 있는 SVM vs1.example.com 에 qt01이라는 이름의 qtree를 생성합니다.

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                  Security Style: unix
                     Oplock Mode: enable
                Unix Permissions: ---rwxr-xr-x
                        Qtree Id: 2
                    Qtree Status: normal
                   Export Policy: default
        Is Export Policy Inherited: true
```

내보내기 정책을 사용하여 **NFS** 액세스를 보호합니다

내보내기 정책을 사용하여 **ONTAP NFS** 액세스 보안에 대해 알아보세요.

엑스포트 정책을 사용하여 볼륨 또는 qtree에 대한 NFS 액세스를 특정 매개 변수와 일치하는 클라이언트로 제한할 수 있습니다. 새 스토리지를 프로비저닝할 때 기존 정책 및 규칙을 사용하거나, 기존 정책에 규칙을 추가하거나, 새 정책 및 규칙을 생성할 수 있습니다. 내보내기 정책의 구성을 확인할 수도 있습니다

ONTAP 9.3부터 오류 규칙 목록에 규칙 위반을 기록하는 백그라운드 작업으로 내보내기 정책 구성 검사를 활성화할 수 있습니다. 'vserver export-policy config-checker' 명령은 checker를 호출하여 결과를 표시합니다. 이 명령을 사용하면 구성을 확인하고 정책에서 잘못된 규칙을 삭제할 수 있습니다. 명령은 호스트 이름, 넷그룹 및 익명 사용자에 대한 내보내기 구성만 검증합니다.

ONTAP NFS 내보내기 규칙의 처리 순서를 관리합니다.

'vserver export-policy rule setindex' 명령을 사용하여 기존 엑스포트 규칙의 인덱스 번호를 수동으로 설정할 수 있습니다. 이렇게 하면 ONTAP가 클라이언트 요청에 내보내기 규칙을 적용하는 우선 순위를 지정할 수 있습니다.

이 작업에 대해

새 인덱스 번호가 이미 사용 중인 경우 명령은 지정된 위치에 규칙을 삽입하고 이에 따라 목록의 순서를 다시 지정합니다.

단계

1. 지정된 엑스포트 규칙의 인덱스 번호 수정:

'vserver export-policy rule setindex-vserver_virtual_server_name_-policyname_policy_name_-ruleindex_integer_-newruleindex_integer_'

예

다음 명령을 실행하면 VS1 이라는 SVM의 RS1 엑스포트 정책에서 인덱스 번호 3에 있는 엑스포트 규칙의 인덱스 번호가 인덱스 번호 2로 변경됩니다.

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

볼륨에 **ONTAP NFS** 내보내기 정책 할당

SVM에 포함된 각 볼륨은 클라이언트의 볼륨 데이터 액세스 엑스포트 규칙이 포함된 엑스포트 정책과 연결되어야 합니다.

이 작업에 대해

볼륨을 생성할 때 또는 볼륨을 생성한 후 언제든지 엑스포트 정책을 볼륨에 연결할 수 있습니다. 하나의 정책을 여러 볼륨에 연결할 수 있지만 하나의 엑스포트 정책을 볼륨에 연결할 수 있습니다.

단계

1. 볼륨을 생성할 때 엑스포트 정책을 지정하지 않은 경우 볼륨에 엑스포트 정책을 할당합니다.

   'volume modify -vserver_vserver_name_-volume_volume_name_-policy_export_policy_name_'

2. 정책이 볼륨에 할당되었는지 확인합니다.

   'volume show-volume_volume_name_-fields policy'입니다

예

다음 명령은 SVM VS1 볼륨 vol1에 엑스포트 정책 NFS_policy를 할당하고 할당을 확인합니다.

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

ONTAP NFS 내보내기 정책을 **qtree**에 할당합니다.

전체 볼륨을 내보내는 대신, 볼륨에 있는 특정 qtree를 엑스포트하여 클라이언트에서 직접 액세스할 수도 있습니다. 엑스포트 정책을 qtree에 할당하여 qtree를 내보낼 수 있습니다. 새 qtree를 생성하거나 기존 qtree를 수정하여 엑스포트 정책을 할당할 수 있습니다.

시작하기 전에

엑스포트 정책이 있어야 합니다.

이 작업에 대해

기본적으로 Qtree는 생성 시 별도로 지정하지 않을 경우 포함하는 볼륨의 상위 엑스포트 정책을 상속합니다.

qtree를 생성하거나 qtree를 생성한 후 언제든지 엑스포트 정책을 qtree에 연결할 수 있습니다. 하나의 정책을 여러 qtree와 연결할 수 있지만 하나의 엑스포트 정책을 qtree에 연결할 수 있습니다.

단계

1. Qtree 생성 시 엑스포트 정책을 지정하지 않은 경우 qtree에 엑스포트 정책을 할당하십시오.

   '볼륨 qtree modify -vserver_vserver_name_-qtree -path /vol/*volume_name /qtree_name*-export -policy_export_policy_name_'

2. 정책이 qtree에 할당되었는지 확인합니다.

   'volume qtree show-qtree_qtree_name_-fields export-policy'

예

다음 명령은 SVM VS1 의 qtree q1에 엑스포트 정책 NFS_policy를 할당하고 할당을 확인합니다.

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

클러스터에서 **ONTAP NFS** 클라이언트 액세스를 확인하세요**.**

UNIX 관리 호스트에서 UNIX 파일 권한을 설정하여 선택한 클라이언트에 공유에 대한 액세스 권한을 부여할 수 있습니다. 'vserver export-policy check-access' 명령을 사용하여 필요에 따라 내보내기 규칙을 조정하여 클라이언트 액세스를 확인할 수 있습니다.

단계

1. 클러스터에서 'vserver export-policy check-access' 명령을 사용하여 내보내기에 대한 클라이언트 액세스를 확인합니다.

   다음 명령은 IP 주소 1.2.4를 사용하여 볼륨 home2에 대한 NFSv3 클라이언트의 읽기/쓰기 액세스를 확인합니다. 명령 출력에서는 볼륨이 내보내기 정책 'exp-home-dir'을 사용하고 액세스가 거부됨을 보여 줍니다.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
                                        Policy    Policy     Rule
Path                    Policy          Owner     Owner Type Index  Access
----------------------- --------------- --------- ---------- ------
----------
/                       default         vs1_root  volume          1 read
/eng                    default         vs1_root  volume          1 read
/eng/home2              exp-home-dir    home2     volume          1 denied

3 entries were displayed.
```

2. 출력을 검사하여 내보내기 정책이 의도한 대로 작동하고 클라이언트 액세스가 예상대로 작동하는지 확인합니다.

   특히, 볼륨 또는 qtree에서 사용하는 엑스포트 정책과 이로 인해 클라이언트가 사용하는 액세스 유형을 확인해야 합니다.

3. 필요한 경우 엑스포트 정책 규칙을 다시 구성하십시오.

클라이언트 시스템에서 **ONTAP NFS** 액세스 테스트

새 스토리지 개체에 대한 NFS 액세스를 검증한 후 NFS 관리 호스트에 로그인하고 SVM에서 데이터를 읽고 쓰는 방법으로 구성을 테스트해야 합니다. 그런 다음 클라이언트 시스템에서 루트 이외의 사용자로 프로세스를 반복해야 합니다.

시작하기 전에

- 클라이언트 시스템에는 이전에 지정한 내보내기 규칙에서 허용하는 IP 주소가 있어야 합니다.
- 루트 사용자에 대한 로그인 정보가 있어야 합니다.

단계

1. 클러스터에서 새 볼륨을 호스팅하는 LIF의 IP 주소를 확인합니다.

   'network interface show –vserver_svm_name_'

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 관리 호스트 클라이언트 시스템에 루트 사용자로 로그인합니다.
3. 디렉토리를 마운트 폴더로 변경합니다.

   "cd /mnt/"

4. SVM의 IP 주소를 사용하여 새 폴더를 생성하고 마운트합니다.

   a. 새 폴더: + mkdir /mnt/*folder*'를 만듭니다

   b. 이 새 디렉토리에 새 볼륨을 마운트합니다. + mount -t nfs -o hard_IPAddress_:/*volume_name*/mnt/*folder*'

c. 디렉터리를 새 폴더 + 'cd_folder_'로 변경합니다

다음 명령을 실행하면 test1이라는 폴더가 생성됩니다. test1 마운트 폴더의 192.0.2.130 IP 주소에 vol1 볼륨을 마운트하고 새 test1 디렉토리로 변경합니다.

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. 새 파일을 만들고 파일이 있는지 확인한 후 다음 파일에 텍스트를 씁니다.
   a. 테스트 파일을 만듭니다. + "touch_filename_"
   b. 파일이 있는지 확인합니다.: + "ls -l_filename_"
   c. cat>_filename_'을 입력합니다

      텍스트를 입력하고 Ctrl+D를 눌러 테스트 파일에 텍스트를 씁니다.

   d. 테스트 파일의 내용을 표시합니다. "cat_filename_"
   e. 테스트 파일: + "rm_filename_"을 제거합니다
   f. 상위 디렉토리로 돌아가기: + "cd…

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. 루트로 마운트된 볼륨에 대해 원하는 UNIX 소유권 및 권한을 설정합니다.
7. 내보내기 규칙에서 식별된 UNIX 클라이언트 시스템에서 이제 새 볼륨에 액세스할 수 있는 권한이 있는 사용자 중 하나로 로그인하고 3-5단계의 절차를 반복하여 볼륨을 마운트하고 파일을 생성할 수 있는지 확인합니다.

추가 **ONTAP NFS** 정보를 찾을 수 있는 곳

NFS 클라이언트 액세스를 성공적으로 테스트한 후 추가 NFS 구성을 수행하거나 SAN 액세스를 추가할 수 있습니다. 프로토콜 액세스가 완료되면 SVM(스토리지 가상 머신)의 루트 볼륨을 보호해야 합니다.

NFS 구성

다음 정보 및 기술 보고서를 사용하여 NFS 액세스를 추가로 구성할 수 있습니다.

- "NFS 관리"

  NFS를 사용하여 파일 액세스를 구성 및 관리하는 방법에 대한 설명은 에 나와 있습니다.

- "NetApp 기술 보고서 4067: NFS 모범 사례 및 구축 가이드"

  NFSv3 및 NFSv4 운영 가이드 역할을 하며 NFSv4를 중심으로 ONTAP 운영 체제에 대한 개요를 제공합니다.

- "NetApp 기술 보고서 4073: 안전한 통합 인증"

  NFS 스토리지 인증을 위한 UNIX 기반 Kerberos 버전 5(krb5) 서버 및 Windows Server Active Directory(AD)를 KDC 및 LDAP(Lightweight Directory Access Protocol) ID 공급자로 사용하도록 ONTAP를 구성하는 방법은 에 나와 있습니다.

- "NetApp 기술 보고서 3580: NFSv4 향상 및 모범 사례 가이드 Data ONTAP 구축"

  에서는 ONTAP를 실행하는 시스템에 접속된 AIX, Linux 또는 Solaris 클라이언트에서 NFSv4 구성 요소를 구축하는 동안 따라야 하는 Best Practice를 설명합니다.

네트워킹 구성

다음 정보 및 기술 보고서를 사용하여 네트워킹 기능 및 이름 서비스를 추가로 구성할 수 있습니다.

- "NFS 관리"

  에서는 ONTAP 네트워킹을 구성하고 관리하는 방법에 대해 설명합니다.

- "NetApp 기술 보고서 4182: 이더넷 스토리지 설계 고려사항 및 clustered Data ONTAP 구성에 대한 모범 사례"

  ONTAP 네트워크 구성의 구현을 설명하고 일반적인 네트워크 배포 시나리오 및 모범 사례 권장 사항을 제공합니다.

- "NetApp 기술 보고서 4668: 이름 서비스 모범 사례 가이드"

  인증을 위해 LDAP, NIS, DNS 및 로컬 파일 구성을 구성하는 방법은 에 나와 있습니다.

SAN 프로토콜 구성

새 SVM에 대한 SAN 액세스를 제공하거나 수정하려는 경우 여러 호스트 운영 체제에서 사용할 수 있는 FC 또는 iSCSI 구성 정보를 사용할 수 있습니다.

루트 볼륨 보호

SVM에서 프로토콜을 구성한 후에는 루트 볼륨이 보호되는지 확인해야 합니다.

- "데이터 보호"

  NAS 지원 SVM에 대한 NetApp의 모범 사례인 SVM 루트 볼륨을 보호하기 위해 로드 공유 미러를 생성하는 방법에 대해 설명합니다. 또한, 로드 공유 미러에서 SVM 루트 볼륨을 프로모션하여 볼륨 장애 또는 손실로부터 빠르게 복구하는 방법을 설명합니다.

ONTAP 내보내기는 7-Mode 내보내기와는 어떻게 다릅니까

ONTAP 내보내기는 **7-Mode** 내보내기와는 어떻게 다릅니까

ONTAP에서 NFS 엑스포트를 구축하는 방법에 대한 생소한 사용자는 7-Mode와 ONTAP 엑스포트 구성 툴을 비교할 수 있을 뿐만 아니라 7-Mode '/etc/exports' 파일을 클러스터 정책 및 규칙과 비교할 수 있습니다.

ONTAP에는 '/etc/exports' 파일과 'exportfs' 명령이 없습니다. 대신 엑스포트 정책을 정의해야 합니다. 엑스포트 정책을 사용하면 7-Mode와 동일한 방식으로 클라이언트 액세스를 제어할 수 있으며, 여러 볼륨에 동일한 엑스포트 정책을 다시 사용할 수 있는 등 기능도 추가로 제공됩니다.

관련 정보

"NFS 관리"

"NetApp 기술 보고서 4067: NFS 모범 사례 및 구축 가이드"

7-Mode 및 **ONTAP NFS** 내보내기 비교에 대해 알아보세요

ONTAP의 내보내기는 7-Mode 환경에 있는 내보내기와 다르게 정의 및 사용됩니다.

차이 영역	향상됩니다	ONTAP
내보내기 정의 방법	내보내기는 '/etc/exports' 파일에 정의되어 있습니다.	내보내기는 SVM 내에서 엑스포트 정책을 생성하여 정의합니다. SVM에는 둘 이상의 엑스포트 정책이 포함될 수 있습니다.
수출 범위	• 내보내기는 지정된 파일 경로 또는 qtree에 적용됩니다. • 각 파일 경로 또는 qtree에 대해 '/etc/exports'에 별도의 항목을 생성해야 합니다. • 내보내기는 '/etc/exports' 파일에 정의되어 있는 경우에만 지속적입니다.	• 엑스포트 정책은 볼륨에 포함된 모든 파일 경로 및 qtree를 포함하여 전체 볼륨에 적용됩니다. • 원하는 경우 둘 이상의 볼륨에 내보내기 정책을 적용할 수 있습니다. • 모든 내보내기 정책은 시스템을 다시 시작할 때마다 유지됩니다.
펜싱(동일한 리소스에 대한 특정 클라이언트에 대해 다른 액세스 지정)	내보낸 단일 리소스에 대해 특정 클라이언트에 서로 다른 액세스 권한을 제공하려면 각 클라이언트와 허용된 액세스 권한을 '/etc/exports' 파일에 나열해야 합니다.	엑스포트 정책은 다양한 개별 엑스포트 규칙으로 구성됩니다. 각 내보내기 규칙은 리소스에 대한 특정 액세스 권한을 정의하고 해당 권한이 있는 클라이언트를 나열합니다. 특정 클라이언트에 대해 다른 액세스를 지정하려면 각 특정 액세스 권한 집합에 대한 내보내기 규칙을 만들고 해당 권한이 있는 클라이언트를 나열한 다음 엑스포트 정책에 규칙을 추가해야 합니다.

이름 앨리어싱	내보내기를 정의할 때 파일 경로 이름과 내보내기 이름을 다르게 지정할 수 있습니다. '/etc/exports' 파일에서 해당 내보내기를 정의할 때 '-actual' 매개변수를 사용해야 합니다.	내보낸 볼륨의 이름을 실제 볼륨 이름과 다르게 설정할 수 있습니다. 이렇게 하려면 SVM 네임스페이스 내에서 사용자 지정 접합 경로 이름을 사용하여 볼륨을 마운트해야 합니다. 기본적으로 볼륨은 해당 볼륨 이름으로 마운트됩니다. 볼륨의 접합 경로 이름을 사용자 지정하려면 마운트를 해제하고 이름을 바꾼 다음 다시 마운트해야 합니다.

ONTAP NFS 내보내기 정책 예제에 대해 알아보세요

내보내기 정책의 예를 검토하여 ONTAP에서 내보내기 정책의 작동 방식을 보다 잘 이해할 수 있습니다.

7-Mode 내보내기의 **ONTAP** 구현 예

다음 예에서는 '/etc/export' 파일에 나타나는 7-Mode 내보내기를 보여 줍니다.

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

이 내보내기를 클러스터된 내보내기 정책으로 복제하려면 세 개의 엑스포트 규칙을 사용하여 엑스포트 정책을 생성한 다음 볼륨 vol1에 엑스포트 정책을 할당해야 합니다.

규칙	요소	값
규칙 1	'-clientmatch'(클라이언트 사양)	'@readonly_netgroup'
'-ruleindex'(규칙 목록에 있는 내보내기 규칙의 위치)	"1"	'-프로토콜'
'NFS'입니다	'-rorule'(읽기 전용 액세스 허용)	Sys(AUTH_SYS로 인증받은 클라이언트)
'-rwrule'(읽기-쓰기 액세스 허용)	"안 돼.	'-superuser'(슈퍼유저 액세스 허용)
'없음'(root_squashed_to anon)	규칙 2	'-clientmatch'
'@rootaccess_netgroup'	룰레인덱스	2

규칙	요소	값
'-프로토콜'	'NFS'입니다	'-rorule'
'스'입니다	'-rwrule'	'스'입니다
'-슈퍼유저'	'스'입니다	규칙 3
'-clientmatch'	'@readwrite_netgroup1, @readwrite_netgroup2'	룰레인덱스
3	'-프로토콜'	'NFS'입니다
'-rorule'	'스'입니다	'-rwrule'
'스'입니다	'-슈퍼유저'	"없음"

1. exp_vol1이라는 엑스포트 정책을 생성합니다.

   'vserver export-policy create-vserver NewSVM-policyname exp_vol1'

2. 기본 명령에 다음 매개 변수를 사용하여 세 개의 규칙을 생성합니다.
   - 기본 명령: + 'vserver export-policy rule create-vserver NewSVM-policyname exp_vol1'
   - 규칙 매개 변수: + ``clientmatch@readonly_netgroup-ruleindex 1-protocol nfs-rorule sys-rwrule never-superuser none'+'-clientmatch@rootaccess_netgroup-rindex 2-protocol nfs-rorule_rule_rule_rule -clientmatch@readwrite_wrule_wrule -rrulule_nfs -rrrrrrule_none
3. 볼륨 vol1에 정책을 할당합니다.

   'volume modify -vserver NewSVM-volume vol1-policy exp_vol1'

7-Mode 엑스포트 통합의 예

다음 예에서는 10개의 qtree당 한 줄이 포함된 7-Mode '/etc/export' 파일을 보여 줍니다.

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

ONTAP에서는 각 qtree에 대해 -clientmatch host1519s 등의 규칙이 있는 정책 또는 -clientmatch host2057s 등의 규칙이 있는 정책 중 하나가 필요합니다.

1. exp_vol1q1 및 exp_vol1q2라는 두 개의 엑스포트 정책을 생성합니다.
   - 'vserver export-policy create-vserver NewSVM-policyname exp_vol1q1'
   - 'vserver export-policy create-vserver NewSVM-policyname exp_vol1q2'
2. 각 정책에 대한 규칙 생성:
   - 'vserver export-policy rule create-vserver newSVM-policyname exp_vol1q1-clientmatch host1519s-rwrule sys-superuser sys'
   - 'vserver export-policy rule create-vserver newSVM-policyname exp_vol1q2-clientmatch host1519s-rwrule sys-superuser sys'
3. qtree에 정책을 적용합니다.
   - '볼륨 qtree modify -vserver NewSVM-qtree-path /vol/vol1/q_1472-export-policy exp_vol1q1'
   - [다음 4 qtree…]
   - '볼륨 qtree modify -vserver NewSVM-qtree-path /vol/vol1/q_2237 -export-policy exp_vol1q2'
   - [다음 4 qtree…]

나중에 이러한 호스트에 대해 추가 qtree를 추가해야 하는 경우 동일한 엑스포트 정책을 사용합니다.

NFS 관리

NFS 프로토콜에 대한 ONTAP 파일 액세스에 대해 알아보세요

ONTAP에는 NFS 프로토콜에 사용할 수 있는 파일 액세스 기능이 포함되어 있습니다. NFS 서버를 사용하도록 설정하고 볼륨 또는 qtree를 내보낼 수 있습니다.

다음과 같은 상황에서 이러한 절차를 수행합니다.

- ONTAP NFS 프로토콜의 기능 범위를 이해하고자 합니다.
- 기본 NFS 구성이 아닌, 덜 일반적인 구성 및 유지보수 작업을 수행하려는 경우
- System Manager나 자동화된 스크립팅 도구가 아니라 CLI(Command-Line Interface)를 사용하려는 경우

NAS 파일 액세스 이해

네임스페이스 및 교차점

ONTAP NAS 네임스페이스 및 연결 지점에 대해 알아보세요

nas_namespace_는 단일 파일 시스템 계층을 생성하기 위해 _junction points_에 함께 결합된 볼륨의 논리적 그룹입니다. 권한이 충분한 클라이언트는 저장소에 있는 파일의 위치를 지정하지 않고 네임스페이스의 파일에 액세스할 수 있습니다. Junced 볼륨은 클러스터의 모든 위치에 상주할 수 있습니다.

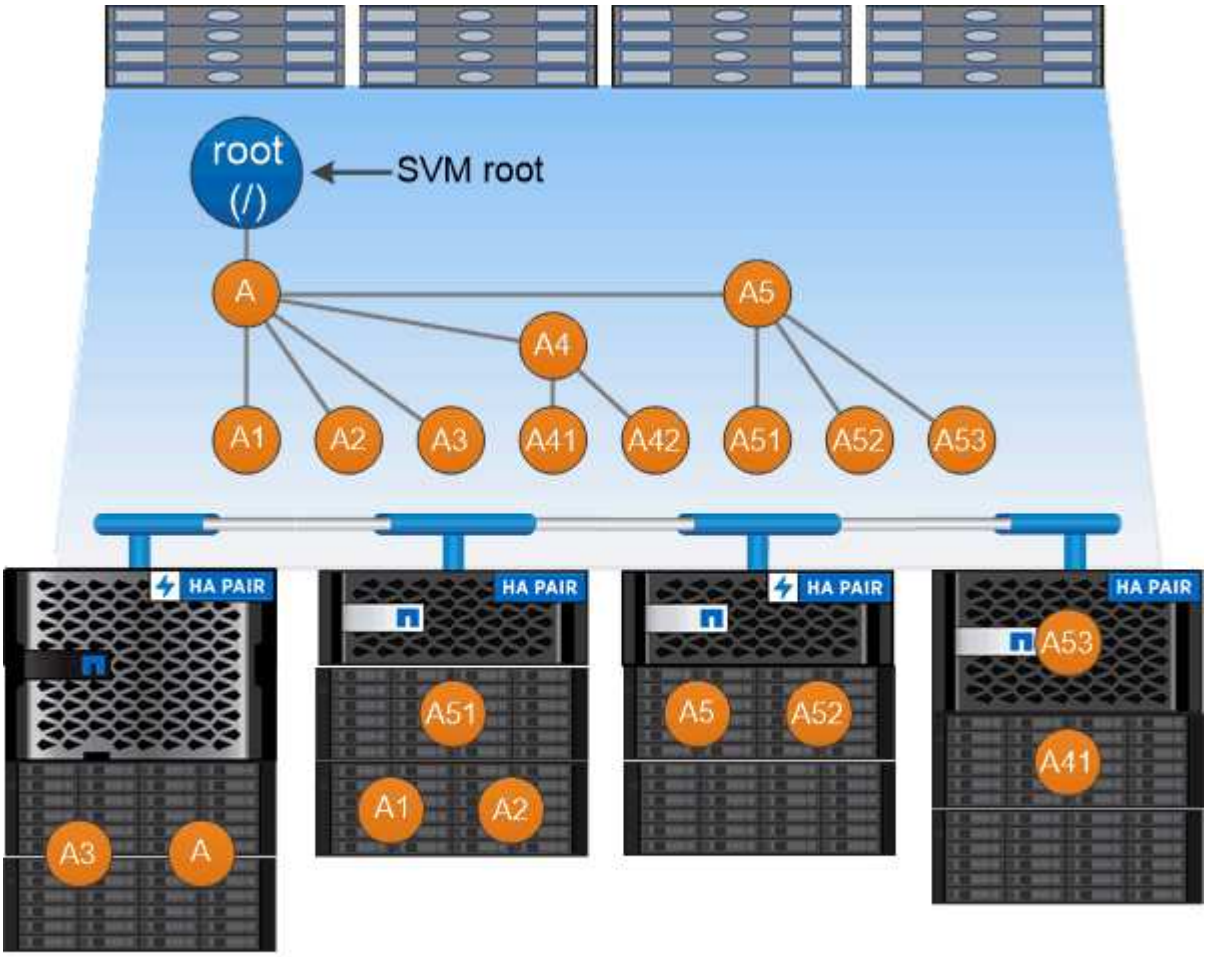
관심 파일이 포함된 모든 볼륨을 마운트하는 대신 NAS 클라이언트는 nfs_export_를 마운트하거나 smb_share에

액세스합니다. _ 내보내기 또는 공유는 전체 네임스페이스 또는 네임스페이스 내의 중간 위치를 나타냅니다. 클라이언트는 해당 액세스 지점 아래에 마운트된 볼륨만 액세스합니다.

필요에 따라 네임스페이스에 볼륨을 추가할 수 있습니다. 상위 볼륨 접합 바로 아래 또는 볼륨 내의 디렉토리에 접합 지점을 생성할 수 있습니다. "vol3"이라는 이름의 볼륨에 대한 볼륨 접합부의 경로는 "/vol1/vol2/vol3" 또는 "/vol1/dir2/vol3" 또는 "/dir1/dir2/vol3"일 수 있습니다. 이 경로를 _junction path ._라고 합니다

모든 SVM에는 고유한 네임스페이스가 있습니다. SVM 루트 볼륨은 네임스페이스 계층 구조의 진입점입니다.

노드 운영 중단 또는 페일오버 발생 시에도 데이터가 계속 사용 가능하도록 하려면 SVM 루트 볼륨에 대해 _load-sharing mirror_copy를 생성해야 합니다.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

예

다음 예에서는 junction path "/eng/home"이 있는 SVM VS1 상에 ""home4""라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

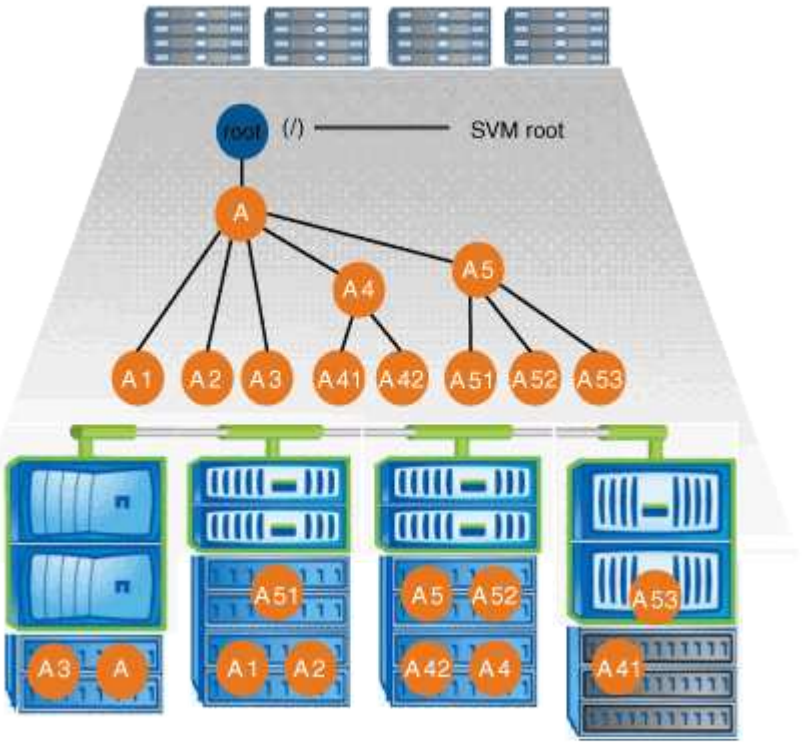
SVM 이름 공간을 생성할 때 사용할 수 있는 몇 가지 일반적인 NAS 네임스페이스 아키텍처가 있습니다. 비즈니스 및 워크플로우 요구사항에 맞는 네임스페이스 아키텍처를 선택할 수 있습니다.

네임스페이스 맨 위에는 항상 루트 볼륨이 있으며, 이 볼륨은 슬래시(/)로 표시됩니다. 루트 아래의 네임스페이스 아키텍처는 세 가지 기본 범주로 분류됩니다.

- 네임스페이스 루트에 대한 단일 분기만 있는 단일 분기 트리
- 여러 개의 분기된 나무는 여러 교차점이 네임스페이스의 루트를 가리킵니다
- 각각 별도의 연결 지점이 있는 여러 독립형 볼륨이 이름 공간의 루트를 가리킵니다

단일 분기 트리가 있는 네임스페이스입니다

단일 분기 트리가 있는 아키텍처는 SVM 네임스페이스의 루트에 대한 단일 삽입 지점을 갖습니다. 단일 삽입 지점은 접합된 볼륨이거나 루트 아래의 디렉토리일 수 있습니다. 다른 모든 볼륨은 단일 삽입 지점(볼륨 또는 디렉토리 가능) 아래의 접합 지점에 마운트됩니다.

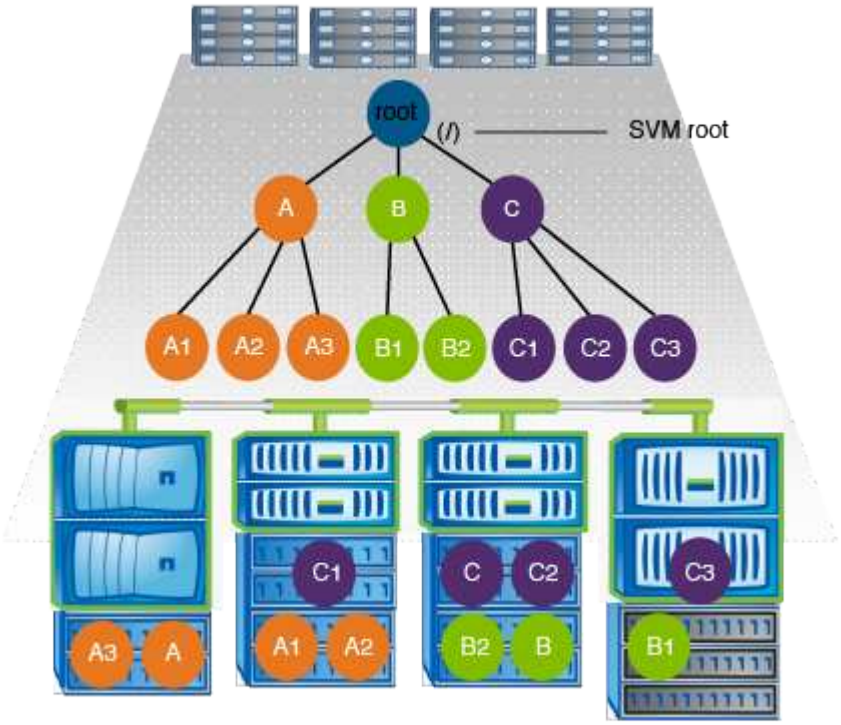


예를 들어, 위의 네임스페이스 아키텍처를 사용하는 일반적인 볼륨 연결 구성은 "데이터"라는 디렉토리인 단일 삽입 지점 아래에 모든 볼륨이 접합되는 다음과 같은 구성으로 보일 수 있습니다.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     corp1       true     /data/dir1/corp1       RW_volume
vs1     corp2       true     /data/dir1/corp2       RW_volume
vs1     data1       true     /data/data1            RW_volume
vs1     eng1        true     /data/data1/eng1       RW_volume
vs1     eng2        true     /data/data1/eng2       RW_volume
vs1     sales       true     /data/data1/sales      RW_volume
vs1     vol1        true     /data/vol1             RW_volume
vs1     vol2        true     /data/vol2             RW_volume
vs1     vol3        true     /data/vol3             RW_volume
vs1     vs1_root    -        /                      -
```

여러 개의 분기 트리가 있는 네임스페이스입니다

여러 개의 분기 트리가 있는 아키텍처에는 SVM 네임스페이스의 루트에 대한 여러 삽입 지점이 있습니다. 삽입 지점은 루트 아래의 분기된 볼륨 또는 디렉토리일 수 있습니다. 다른 모든 볼륨은 삽입 지점(볼륨 또는 디렉토리일 수 있음) 아래의 접합 지점에 마운트됩니다.

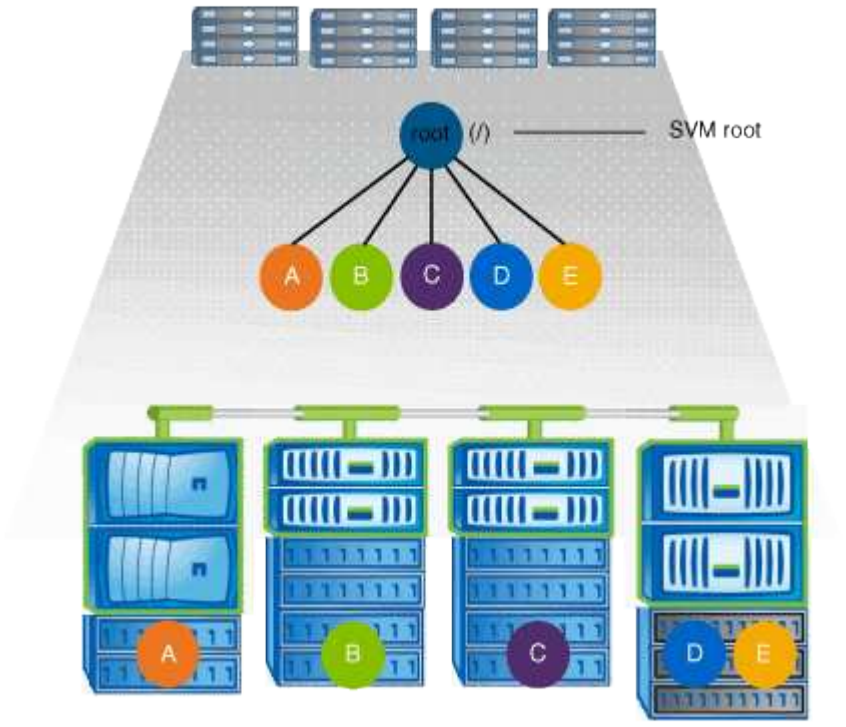


예를 들어, 위의 네임스페이스 아키텍처를 사용하는 일반적인 볼륨 접합 구성은 SVM의 루트 볼륨에 세 개의 삽입 지점이 있는 다음과 같은 구성을 예로 들 수 있습니다. 두 개의 삽입 지점은 "다타"와 "프로젝트"라는 디렉토리입니다. 한 삽입 지점은 "audit"이라는 이름의 접합부입니다.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     audit       true     /audit                 RW_volume
vs1     audit_logs1 true     /audit/logs1           RW_volume
vs1     audit_logs2 true     /audit/logs2           RW_volume
vs1     audit_logs3 true     /audit/logs3           RW_volume
vs1     eng         true     /data/eng              RW_volume
vs1     mktg1       true     /data/mktg1            RW_volume
vs1     mktg2       true     /data/mktg2            RW_volume
vs1     project1    true     /projects/project1     RW_volume
vs1     project2    true     /projects/project2     RW_volume
vs1     vs1_root    -        /                      -
```

여러 개의 독립 실행형 볼륨이 있는 네임스페이스

독립 실행형 볼륨이 있는 아키텍처에서 모든 볼륨은 SVM 네임스페이스의 루트에 대한 삽입 지점을 갖습니다. 하지만 볼륨이 다른 볼륨 아래에 접합되지 않습니다. 각 볼륨은 고유한 경로를 가지고 있으며, 루트 바로 아래에 접합되거나 루트 아래의 디렉토리 아래에 접합됩니다.



예를 들어, 위의 네임스페이스 아키텍처를 사용하는 일반적인 볼륨 접합 구성은 다음 구성과 비슷합니다. 여기서 SVM의 루트 볼륨에 5개의 삽입 지점을 두고 각 삽입 지점을 단일 볼륨의 경로를 나타냅니다.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     eng         true     /eng                   RW_volume
vs1     mktg        true     /vol/mktg              RW_volume
vs1     project1    true     /project1              RW_volume
vs1     project2    true     /project2              RW_volume
vs1     sales       true     /sales                 RW_volume
vs1     vs1_root    -        /                      -
```

ONTAP에서 파일 액세스를 제어하는 방법

ONTAP NAS 파일 액세스 제어에 대해 알아보세요

ONTAP는 사용자가 지정하는 인증 기반 및 파일 기반 제한 사항에 따라 파일에 대한 액세스를 제어합니다.

클라이언트가 스토리지 시스템에 접속하여 파일을 액세스하는 경우 ONTAP는 다음 두 가지 작업을 수행해야 합니다.

- 인증

  ONTAP는 신뢰할 수 있는 소스로 ID를 확인하여 클라이언트를 인증해야 합니다. 또한 클라이언트의 인증 유형은 클라이언트가 내보내기 정책을 구성할 때 데이터에 액세스할 수 있는지 여부를 결정하는 데 사용할 수 있는 방법 중 하나입니다(CIFS의 경우 선택 사항).

- 권한 부여

  ONTAP는 사용자의 자격 증명을 파일 또는 디렉터리에 구성된 권한과 비교하고 제공할 액세스 유형(있는 경우)을 확인하여 사용자를 승인해야 합니다.

파일 액세스 제어를 제대로 관리하려면 ONTAP가 NIS, LDAP 및 Active Directory 서버와 같은 외부 서비스와 통신해야 합니다. CIFS 또는 NFS를 사용하여 파일 액세스를 위한 스토리지 시스템을 구성하려면 ONTAP의 환경에 따라 적절한 서비스를 설정해야 합니다.

ONTAP NAS SVM에 대한 인증 기반 제한 사항에 대해 알아보세요.

인증 기반 제한 사항을 사용하여 SVM(스토리지 가상 머신)에 연결할 수 있는 클라이언트 시스템과 사용자를 지정할 수 있습니다.

ONTAP는 UNIX 서버와 Windows 서버 모두에서 Kerberos 인증을 지원합니다.

ONTAP NAS SVM에 대한 파일 기반 제한 사항에 대해 알아보세요.

ONTAP은 세 가지 보안 수준을 평가하여 엔티티가 SVM에 있는 파일 및 디렉토리에 대해 요청된 작업을 수행할 수 있는 권한이 있는지 확인합니다. 액세스는 세 가지 보안 수준을 평가한 후 유효한 권한에 의해 결정됩니다.

모든 스토리지 객체에는 최대 3가지 유형의 보안 계층이 포함될 수 있습니다.

- 내보내기(NFS) 및 공유(SMB) 보안

  내보내기 및 공유 보안은 지정된 NFS 내보내기 또는 SMB 공유에 대한 클라이언트 액세스에 적용됩니다. 관리 권한이 있는 사용자는 SMB 및 NFS 클라이언트의 내보내기 및 공유 수준 보안을 관리할 수 있습니다.

- 스토리지 레벨 Access Guard 파일 및 디렉토리 보안

  스토리지 레벨 액세스 가드 보안은 SMB 및 NFS 클라이언트가 SVM 볼륨에 액세스하는 데 적용됩니다. NTFS 액세스 권한만 지원됩니다. ONTAP에서 UNIX 사용자에 대한 보안 검사를 수행하여 스토리지 수준 액세스 가드가 적용된 볼륨의 데이터에 액세스하려면 UNIX 사용자는 볼륨을 소유한 SVM에서 Windows 사용자에게 매핑해야 합니다.

  NFS 또는 SMB 클라이언트의 파일 또는 디렉토리에 대한 보안 설정을 볼 경우 Storage-Level Access Guard 보안이 표시되지 않습니다. 시스템(Windows 또는 UNIX) 관리자도 클라이언트에서 스토리지 수준 액세스 가드 보안을 취소할 수 없습니다.

- NTFS, UNIX 및 NFSv4 네이티브 파일 레벨 보안

  네이티브 파일 레벨 보안은 스토리지 객체를 나타내는 파일 또는 디렉토리에 존재합니다. 클라이언트에서 파일 수준 보안을 설정할 수 있습니다. 파일 권한은 SMB 또는 NFS를 사용하여 데이터를 액세스하든 관계없이 유효합니다.

ONTAP가 **NFS** 클라이언트 인증을 처리하는 방식

NAS 클라이언트에 대한 **ONTAP** 인증에 대해 알아보세요

NFS 클라이언트가 SVM에서 데이터에 액세스하려면 먼저 제대로 인증되어야 합니다. ONTAP는 UNIX 자격 증명을 구성하는 이름 서비스와 비교하여 클라이언트를 인증합니다.

NFS 클라이언트가 SVM에 연결되면 ONTAP는 SVM의 이름 서비스 구성에 따라 다른 이름 서비스를 확인하여 사용자의 UNIX 자격 증명을 얻습니다. ONTAP는 로컬 UNIX 계정, NIS 도메인 및 LDAP 도메인에 대한 자격 증명을 확인할 수 있습니다. ONTAP가 사용자를 성공적으로 인증할 수 있도록 하나 이상의 사용자를 구성해야 합니다. 여러 개의 이름 서비스와 ONTAP가 서비스를 검색하는 순서를 지정할 수 있습니다.

UNIX 볼륨 보안 스타일을 사용하는 순수 NFS 환경에서는 이 구성으로 NFS 클라이언트에서 접속하는 사용자에 대해 적절한 파일 액세스를 인증하고 제공할 수 있습니다.

혼합, NTFS 또는 통합 볼륨 보안 스타일을 사용하는 경우 ONTAP는 Windows 도메인 컨트롤러에서 인증을 위해 UNIX 사용자의 SMB 사용자 이름을 얻어야 합니다. 이 문제는 로컬 UNIX 계정이나 LDAP 도메인을 사용하여 개별 사용자를 매핑하거나 기본 SMB 사용자를 대신 사용하여 발생할 수 있습니다. ONTAP에서 검색할 이름 서비스를 순서대로 지정하거나 기본 SMB 사용자를 지정할 수 있습니다.

ONTAP이 이름 서비스를 사용하는 방법을 알아보세요

ONTAP는 이름 서비스를 사용하여 사용자 및 클라이언트에 대한 정보를 얻습니다. ONTAP는 이 정보를 사용하여 스토리지 시스템의 데이터에 액세스하거나 데이터를 관리하는 사용자를 인증하고 혼합 환경에서 사용자 자격 증명을 매핑합니다.

스토리지 시스템을 구성할 때 ONTAP에서 인증에 사용할 사용자 자격 증명을 얻기 위해 사용할 이름 서비스를 지정해야 합니다. ONTAP는 다음과 같은 이름 서비스를 지원합니다.

- 로컬 사용자(파일)

- 외부 NIS 도메인(NIS)
- 외부 LDAP 도메인(LDAP)

'vserver services name-service ns-switch' 명령 제품군을 사용하여 소스로 SVM을 구성하여 네트워크 정보 및 검색 순서를 검색할 수 있습니다. 이러한 명령은 UNIX 시스템에서 '/etc/nsswitch.conf' 파일과 동일한 기능을 제공합니다.

NFS 클라이언트가 SVM에 연결되면 ONTAP는 지정된 이름 서비스를 확인하여 사용자의 UNIX 자격 증명을 얻습니다. 이름 서비스가 올바르게 구성되어 있고 ONTAP에서 UNIX 자격 증명을 얻을 수 있는 경우 ONTAP는 사용자를 성공적으로 인증합니다.

보안 스타일이 혼합된 환경에서는 ONTAP가 사용자 자격 증명을 매핑해야 할 수 있습니다. ONTAP가 사용자 자격 증명을 적절하게 매핑할 수 있도록 사용자 환경에 맞게 이름 서비스를 구성해야 합니다.

ONTAP에서는 SVM 관리자 계정을 인증하는 데에도 이름 서비스를 사용합니다. 이름 서비스 스위치를 구성하거나 수정할 때 실수로 SVM 관리자 계정에 대한 인증을 비활성화하지 않도록 주의해야 합니다. SVM 관리 사용자에 대한 자세한 내용은 를 참조하십시오 "관리자 인증 및 RBAC".

NFS 클라이언트에서 ONTAP SMB 파일 액세스 권한 부여

ONTAP는 Windows NT 파일 시스템(NTFS) 보안 의미를 사용하여 NFS 클라이언트의 UNIX 사용자가 NTFS 권한이 있는 파일에 액세스할 수 있는지 여부를 결정합니다.

ONTAP는 사용자의 UNIX UID(사용자 ID)를 SMB 자격 증명으로 변환한 다음 SMB 자격 증명을 사용하여 사용자에게 파일에 대한 액세스 권한이 있는지 확인합니다. SMB 자격 증명은 일반적으로 사용자의 Windows 사용자 이름인 기본 SID(보안 식별자)와 사용자가 구성원인 Windows 그룹에 해당하는 하나 이상의 그룹 SID로 구성됩니다.

프로세스가 도메인 컨트롤러에 접속하기 때문에 ONTAP가 UNIX UID를 SMB 자격 증명으로 변환하는 데 걸리는 시간은 수십 밀리초에서 수백 밀리초로 지정할 수 있습니다. ONTAP는 UID를 SMB 자격 증명에 매핑하고 자격 증명 캐시에 매핑을 입력하여 변환으로 인한 검증 시간을 줄입니다.

ONTAP NFS 자격 증명 캐시 작동 방식

NFS 사용자가 스토리지 시스템의 NFS 내보내기에 대한 액세스를 요청할 경우 ONTAP는 외부 이름 서버 또는 로컬 파일에서 사용자 자격 증명을 검색하여 사용자를 인증해야 합니다. 그런 다음 ONTAP는 나중에 참조할 수 있도록 이러한 자격 증명을 내부 자격 증명 캐시에 저장합니다. NFS 자격 증명 캐시의 작동 방식을 이해하면 잠재적인 성능 및 액세스 문제를 처리할 수 있습니다.

자격 증명 캐시가 없으면 ONTAP는 NFS 사용자가 액세스를 요청할 때마다 이름 서비스를 쿼리해야 합니다. 사용량이 많은 스토리지 시스템에서 많은 사용자가 액세스하는 경우 심각한 성능 문제가 신속하게 발생하여 원치 않는 지연이 발생하거나 NFS 클라이언트 액세스가 거부 될 수 있습니다.

ONTAP는 자격 증명 캐시를 사용하여 사용자 자격 증명을 검색한 다음 NFS 클라이언트가 다른 요청을 보낼 때 빠르고 쉽게 액세스할 수 있도록 미리 결정된 시간 동안 저장합니다. 이 방법은 다음과 같은 이점을 제공합니다.

- NIS 또는 LDAP와 같은 외부 이름 서버에 대한 요청 수를 줄여 스토리지 시스템의 로드를 간소화합니다.
- 외부 네임 서버에 대한 요청 수를 줄여 부하를 덜어줍니다.
- 외부 소스에서 자격 증명을 얻기 위한 대기 시간을 없애 사용자 액세스 속도를 높입니다.

ONTAP는 자격 증명 캐시에 양의 자격 증명과 음의 자격 증명을 모두 저장합니다. 양의 자격 증명은 사용자가 인증되고

액세스 권한이 부여되었음을 의미합니다. 음수 자격 증명은 사용자가 인증되지 않고 액세스가 거부되었음을 의미합니다.

기본적으로 ONTAP는 24시간 동안 양의 자격 증명을 저장합니다. 즉, 처음에 사용자를 인증한 후 ONTAP는 해당 사용자의 액세스 요청에 대해 24시간 동안 캐시된 자격 증명을 사용합니다. 사용자가 24시간 후에 액세스를 요청하면 주기가 다시 시작됩니다. ONTAP 는 캐시된 자격 증명을 삭제하고 해당 이름 서비스 소스에서 자격 증명을 다시 가져옵니다. 이전 24시간 동안 이름 서버에서 자격 증명이 변경된 경우 ONTAP는 다음 24시간 동안 사용할 수 있도록 업데이트된 자격 증명을 캐시합니다.

기본적으로 ONTAP는 2시간 동안 부정 자격 증명을 저장합니다. 즉, 처음에 사용자에 대한 액세스를 거부하면 ONTAP는 해당 사용자의 액세스 요청을 2시간 동안 계속 거부합니다. 사용자가 2시간 후에 액세스를 요청하는 경우 주기가 다시 시작됩니다. ONTAP 는 해당 이름 서비스 소스에서 자격 증명을 다시 가져옵니다. 이전 2시간 동안 이름 서버에서 자격 증명이 변경된 경우 ONTAP는 다음 2시간 동안 사용할 수 있도록 업데이트된 자격 증명을 캐시합니다.

NAS 네임스페이스에서 데이터 볼륨을 생성하고 관리합니다

지정된 연결 지점으로 ONTAP NAS 볼륨 생성

데이터 볼륨을 생성할 때 교차점을 지정할 수 있습니다. 결과 볼륨은 교차점에 자동으로 마운트되며 NAS 액세스를 위해 즉시 구성할 수 있습니다.

시작하기 전에

- 볼륨을 생성할 애그리게이트가 이미 존재해야 합니다.
- ONTAP 9.13.1부터 용량 분석 및 활동 추적이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 `volume create` 또는 `-activity-tracking-state` 를 로 설정하여 `on` 명령을 `-analytics-state` 실행합니다.

  용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 "파일 시스템 분석 설정". 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

> 다음 문자는 접합 경로에서 사용할 수 없습니다. `* # " > < | ? \`

또한 접합 경로 길이는 255자를 초과할 수 없습니다.

단계

1. 교차점으로 볼륨을 생성합니다.

```
volume create -vserver <vserver_name> -volume <volume_name> -aggregate
<aggregate_name> -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path <junction_path>
```

   접합 경로는 루트(/)로 시작해야 하며 디렉터리와 접합된 볼륨을 모두 포함할 수 있습니다. 접합 경로에는 볼륨의 이름을 포함할 필요가 없습니다. 접합 경로는 볼륨 이름과 무관합니다.

   볼륨 보안 스타일을 지정하는 것은 선택 사항입니다. 보안 스타일을 지정하지 않으면 ONTAP에서 SVM(스토리지 가상 머신)의 루트 볼륨에 적용되는 것과 동일한 보안 스타일로 볼륨을 생성합니다. 그러나 루트 볼륨의 보안 스타일이 만드는 데이터 볼륨에 적용할 보안 스타일이 아닐 수 있습니다. 문제 해결이 어려운 파일 액세스 문제를 최소화하기 위해 볼륨을 생성할 때 보안 스타일을 지정하는 것이 좋습니다.

교차경로는 대/소문자를 구분하지 않고 /eng은 /eng과 같습니다. CIFS 공유를 생성하는 경우 Windows는 연결 경로를 대/소문자를 구분하는 것처럼 처리합니다. 예를 들어, 교차점이 /eng인 경우 SMB 공유의 경로는 /eng가 아니라 /eng로 시작해야 합니다.

데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 여러 가지 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 볼륨이 원하는 접합 지점으로 생성되었는지 확인합니다.

```
volume show -vserver <vserver_name> -volume <volume_name> -junction
```

예

다음 예에서는 접합 경로가 있는 SVM VS1에 `/eng/home` 이라는 이름의 볼륨을 `home4` 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

특정 연결 지점 없이 **ONTAP NAS** 볼륨 생성

교차점을 지정하지 않고 데이터 볼륨을 생성할 수 있습니다. 결과 볼륨은 자동으로 마운트되지 않으며 NAS 액세스에 대해 구성할 수 없습니다. 해당 볼륨에 대해 SMB 공유 또는 NFS 내보내기를 구성하려면 먼저 볼륨을 마운트해야 합니다.

시작하기 전에

- 볼륨을 생성할 애그리게이트가 이미 존재해야 합니다.
- ONTAP 9.13.1부터 용량 분석 및 활동 추적이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 `volume create` 또는 `-activity-tracking-state` 를 로 설정하여 `on` 명령을 `-analytics-state` 실행합니다.

  용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 "파일 시스템 분석 설정". 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 다음 명령을 사용하여 교차점 없이 볼륨을 생성합니다.

   'volume create-vserver vserver_name-volume volume_name-aggregate aggregate_name-size{integer[KB|MB|GB|TB|PB]} - security-style{NTFS|UNIX|MIXED}'입니다

볼륨 보안 스타일을 지정하는 것은 선택 사항입니다. 보안 스타일을 지정하지 않으면 ONTAP에서 SVM(스토리지 가상 머신)의 루트 볼륨에 적용되는 것과 동일한 보안 스타일로 볼륨을 생성합니다. 그러나 루트 볼륨의 보안 스타일이 데이터 볼륨에 적용할 보안 스타일이 아닐 수 있습니다. 문제 해결이 어려운 파일 액세스 문제를 최소화하기 위해 볼륨을 생성할 때 보안 스타일을 지정하는 것이 좋습니다.

데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 여러 가지 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 볼륨이 교차점 없이 생성되었는지 확인합니다.

   'volume show -vserver vserver_name -volume volume_name -junction'

예

다음 예에서는 교차점에 마운트되지 않은 SVM VS1 상에 "sales"라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

NAS 네임스페이스에서 **ONTAP NFS** 볼륨을 마운트하거나 마운트 해제합니다**.**

SVM(스토리지 가상 시스템) 볼륨에 포함된 데이터에 대한 NAS 클라이언트 액세스를 구성하려면 먼저 NAS 네임스페이스에 볼륨을 마운트해야 합니다. 볼륨이 현재 마운트되지 않은 경우 볼륨을 연결 지점에 마운트할 수 있습니다. 볼륨을 마운트 해제할 수도 있습니다.

이 작업에 대해

볼륨을 마운트 해제하고 오프라인으로 전환하면 마운트 해제된 볼륨의 네임스페이스 내에 포함된 접합 지점의 볼륨 데이터를 비롯하여 연결 지점 내의 모든 데이터를 NAS 클라이언트에서 액세스할 수 없습니다.

볼륨에 대한 NAS 클라이언트 액세스를 중단하려면 볼륨을 마운트 해제하는 것만으로는 충분하지 않습니다. 볼륨을 오프라인으로 전환하거나 클라이언트 측 파일 핸들 캐시가 무효화되도록 다른 단계를 수행해야 합니다. 자세한 내용은 다음 기술 자료 문서를 참조하십시오.

"ONTAP의 네임스페이스에서 제거후에도 NFSv3 클라이언트가 볼륨에 계속 액세스할 수 있습니다"

볼륨을 마운트 해제하고 오프라인으로 전환하면 볼륨 내의 데이터가 손실되지 않습니다. 또한 마운트 해제된 볼륨 내의 볼륨이나 디렉토리 및 연결 지점에 생성된 기존 볼륨 내보내기 정책 및 SMB 공유가 보존됩니다. 마운트 해제된 볼륨을 다시 마운트하면 NAS 클라이언트가 기존 엑스포트 정책과 SMB 공유를 사용하여 볼륨 내에 포함된 데이터에 액세스할

수 있습니다.

단계

1. 원하는 작업을 수행합니다.

원하는 작업	명령 입력...
볼륨을 마운트합니다	'volume mount-vserver_svm_name_-volume_volume_name_-junction-path_junction_path_'

볼륨을 마운트 해제합니다	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. 볼륨이 원하는 마운트 상태에 있는지 확인합니다.

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

예

다음 예에서는 SVM ""VS1""에 있는 ""판매""라는 볼륨을 접합 지점 """/판매""에 마운트합니다.

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

다음 예에서는 SVM ""VS1""에 있는 ""데이터""라는 이름의 볼륨을 마운트 해제하고 오프라인으로 전환합니다.

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

ONTAP NAS 볼륨 마운트 및 접합 지점 정보를 표시합니다

스토리지 가상 시스템(SVM)에 대해 마운트된 볼륨 및 볼륨이 마운트된 접합 지점에 대한 정보를 표시할 수 있습니다. 또한 어느 볼륨이 분기점에 마운트되지 않는지 확인할 수 있습니다. 이 정보를 사용하여 SVM 네임스페이스를 이해하고 관리할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

를 표시하려면…	명령 입력…
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 요약 정보	'volume show -vserver_vserver_name_-junction'
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 자세한 정보	'volume show -vserver_vserver_name_-volume_volume_name_ -instance'
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 특정 정보	a. 필요한 경우 볼륨 표시 필드? 명령을 사용하여 '-fields' 매개 변수에 대한 유효한 필드를 표시할 수 있습니다 b. '-fields' 매개 변수 'volume show-vserver_vserver_name_-fields_fieldname_,…'를 사용하여 원하는 정보를 표시합니다

예

다음 예는 SVM VS1 에서 마운트 및 마운트 해제된 볼륨에 대한 요약을 표시합니다.

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

다음 예는 SVM VS2 에 있는 볼륨의 지정된 필드에 대한 정보를 표시합니다.

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

보안 스타일을 구성합니다

보안 스타일이 데이터 액세스에 미치는 영향

ONTAP NAS 보안 스타일 알아보기

UNIX, NTFS, 혼합 및 통합 등 네 가지 보안 유형이 있습니다. 각 보안 스타일은 데이터에 대한 사용 권한이 처리되는 방식에 다른 영향을 줍니다. 용도에 맞는 적절한 보안 스타일을 선택할 수 있도록 다양한 효과를 이해해야 합니다.

보안 스타일은 클라이언트 유형이 데이터에 액세스할 수 있거나 액세스할 수 없는 형식을 결정하지 않는다는 점을 이해하는 것이 중요합니다. 보안 스타일은 ONTAP에서 데이터 액세스를 제어하는 데 사용하는 권한 유형과 이러한 권한을 수정할 수 있는 클라이언트 유형만 결정합니다.

예를 들어, 볼륨이 UNIX 보안 스타일을 사용하는 경우에도 SMB 클라이언트는 ONTAP의 멀티 프로토콜 특성으로 인해 데이터에 액세스(적절하게 인증 및 승인)할 수 있습니다. 그러나 ONTAP에서는 UNIX 클라이언트만 기본 툴을 사용하여 수정할 수 있는 UNIX 권한을 사용합니다.

보안 스타일	사용 권한을 수정할 수 있는 클라이언트입니다	클라이언트가 사용할 수 있는 권한	결과적으로 효율적인 보안 스타일을 제공합니다	파일에 액세스할 수 있는 클라이언트입니다
Unix	NFS 를 참조하십시오	NFSv3 모드 비트	Unix	NFS 및 SMB
		NFSv4.x ACL		
NTFS입니다	중소기업	NTFS ACL	NTFS입니다	
혼합	NFS 또는 SMB	NFSv3 모드 비트	Unix	
		NFSv4.ACL		
		NTFS ACL	NTFS입니다	
통합(ONTAP 9.4 및 이전 릴리즈에서 무한 확장 볼륨에만 해당)	NFS 또는 SMB	NFSv3 모드 비트	Unix	
		NFSv4.1 ACL		
		NTFS ACL	NTFS입니다	

FlexVol 볼륨은 UNIX, NTFS 및 혼합 보안 스타일을 지원합니다. 보안 스타일이 혼합 또는 통합된 경우 사용자가 보안 스타일을 개별적으로 설정하므로 사용자가 마지막으로 권한을 수정한 클라이언트 유형에 따라 유효 사용 권한이 달라집니다. 권한을 수정한 마지막 클라이언트가 NFSv3 클라이언트인 경우 사용 권한은 UNIX NFSv3 모드 비트입니다. 마지막 클라이언트가 NFSv4 클라이언트인 경우 사용 권한은 NFSv4 ACL입니다. 마지막 클라이언트가 SMB 클라이언트인 경우 사용 권한은 Windows NTFS ACL입니다.

통합 보안 스타일은 ONTAP 9.5 이상 릴리스에서 더 이상 지원되지 않는 무한 볼륨에서만 사용할 수 있습니다. 자세한 내용은 을 참조하십시오 FlexGroup 볼륨 관리 개요.

그만큼 `show-effective-permissions` 매개변수를 사용하여 `vserver security file-directory` 명령을 사용하면 지정된 파일이나 폴더 경로에 대해 Windows 또는 UNIX 사용자에게 부여된 유효 권한을 표시할 수 있습니다. 또한 선택적 매개 변수를 `-share-name` 사용하면 효과적인 공유 권한을 표시할 수 있습니다. 에 대한 자세한 내용은 `vserver security file-directory show-effective-permissions` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP는 처음에 일부 기본 파일 권한을 설정합니다. 기본적으로 UNIX, 혼합 및 통합 보안 스타일 볼륨의 모든 데이터에 대한 효과적인 보안 스타일은 UNIX이고, 기본 보안 스타일에 의해 허용되는 대로 클라이언트에 의해 구성될 때까지 유효 사용 권한 유형은 UNIX 모드 비트(별도로 지정하지 않는 경우 0755)입니다. 기본적으로 NTFS 보안 스타일 볼륨의 모든 데이터에 대한 효과적인 보안 스타일은 NTFS이며 ACL을 통해 모든 사람에게 모든 권한을 제공할 수 있습니다.

관련 정보

- "ONTAP 명령 참조입니다"

ONTAP NFS FlexVol 볼륨의 보안 스타일 알아보기

보안 스타일은 FlexVol 볼륨(루트 또는 데이터 볼륨) 및 qtree에서 설정할 수 있습니다. 보안 스타일은 생성 시 수동으로 설정하거나 자동으로 상속하거나 나중에 변경할 수 있습니다.

ONTAP NAS SVM에서 사용할 보안 스타일을 결정하세요**.**

볼륨에 사용할 보안 스타일을 결정하는 데 도움이 되도록 두 가지 요소를 고려해야 합니다. 기본 요소는 파일 시스템을 관리하는 관리자 유형입니다. 2차 요소는 볼륨의 데이터에 액세스하는 사용자 또는 서비스의 유형입니다.

볼륨에 보안 스타일을 구성할 때는 최상의 보안 스타일을 선택하고 사용 권한 관리 문제를 피하기 위해 환경의 요구 사항을 고려해야 합니다. 다음 고려 사항을 통해 결정을 내릴 수 있습니다.

보안 스타일	다음 경우에 선택…
Unix	• 파일 시스템은 UNIX 관리자가 관리합니다. • 대부분의 사용자는 NFS 클라이언트입니다. • 데이터에 액세스하는 애플리케이션은 UNIX 사용자를 서비스 계정으로 사용합니다.
NTFS입니다	• 파일 시스템은 Windows 관리자가 관리합니다. • 대부분의 사용자는 SMB 클라이언트입니다. • 데이터에 액세스하는 응용 프로그램은 Windows 사용자를 서비스 계정으로 사용합니다.
혼합	• 파일 시스템은 UNIX 관리자와 Windows 관리자 모두에서 관리되며 사용자는 NFS 클라이언트와 SMB 클라이언트로 구성됩니다.

ONTAP NFS 보안 스타일 상속에 대해 알아보십시오

새 FlexVol 볼륨 또는 qtree를 생성할 때 보안 스타일을 지정하지 않으면 보안 스타일이 다른 방식으로 상속됩니다.

보안 스타일은 다음과 같은 방식으로 상속됩니다.

- FlexVol 볼륨은 SVM이 포함된 루트 볼륨의 보안 스타일을 상속합니다.
- qtree는 포함된 FlexVol 볼륨의 보안 스타일을 상속합니다.
- 파일 또는 디렉토리는 포함된 FlexVol 볼륨 또는 qtree의 보안 스타일을 상속합니다.

ONTAP NFS UNIX 권한 보존에 대해 알아보세요

현재 UNIX 사용 권한이 있는 FlexVol 볼륨의 파일을 Windows 응용 프로그램에서 편집하고 저장하면 ONTAP에서 UNIX 사용 권한을 보존할 수 있습니다.

Windows 클라이언트의 응용 프로그램이 파일을 편집하고 저장할 때 파일의 보안 속성을 읽고, 새 임시 파일을 만들고, 해당 속성을 임시 파일에 적용한 다음 임시 파일에 원래 파일 이름을 지정합니다.

Windows 클라이언트가 보안 속성에 대한 쿼리를 수행할 때 UNIX 권한을 정확하게 나타내는 생성된 ACL을 받습니다. 이 생성된 ACL의 유일한 목적은 파일이 Windows 애플리케이션에 의해 업데이트되므로 파일의 UNIX 사용 권한을 보존하여 결과 파일이 동일한 UNIX 사용 권한을 갖도록 하는 것입니다. ONTAP는 생성된 ACL을 사용하여 NTFS ACL을 설정하지 않습니다.

Windows 보안 탭을 사용하여 **ONTAP NFS SVM**에서 **UNIX** 권한 관리

SVM에서 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 대한 UNIX 권한을 조작하려는 경우 Windows 클라이언트의 보안 탭을 사용할 수 있습니다. 또는 Windows ACL을 쿼리하고 설정할 수 있는 응용 프로그램을 사용할 수도 있습니다.

- UNIX 사용 권한 수정

  Windows 보안 탭을 사용하여 혼합 보안 스타일 볼륨 또는 qtree에 대한 UNIX 권한을 보고 변경할 수 있습니다. 기본 Windows 보안 탭을 사용하여 UNIX 권한을 변경하는 경우 변경하기 전에 먼저 편집할 기존 ACE(모드 비트를 0으로 설정)를 제거해야 합니다. 또는 고급 편집기를 사용하여 권한을 변경할 수도 있습니다.

  모드 권한을 사용하는 경우 나열된 UID, GID 및 기타(컴퓨터에 계정이 있는 다른 모든 사용자)에 대한 모드 권한을 직접 변경할 수 있습니다. 예를 들어, 표시된 UID에 r-x 권한이 있는 경우 UID 권한을 rwx로 변경할 수 있습니다.

- UNIX 권한을 NTFS 권한으로 변경합니다

  Windows 보안 탭을 사용하면 파일 및 폴더에 UNIX 유효 보안 스타일이 있는 혼합 보안 스타일 볼륨 또는 qtree의 UNIX 보안 개체를 Windows 보안 개체로 대체할 수 있습니다.

  원하는 Windows 사용자 및 그룹 개체로 대체하려면 먼저 나열된 모든 UNIX 권한 항목을 제거해야 합니다. 그런 다음 Windows 사용자 및 그룹 개체에서 NTFS 기반 ACL을 구성할 수 있습니다. 모든 UNIX 보안 개체를 제거하고 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 Windows 사용자 및 그룹만 추가하면 파일 또는 폴더의 효과적인 보안 스타일이 UNIX에서 NTFS로 변경됩니다.

  폴더에 대한 권한을 변경할 때 기본 Windows 동작은 이러한 변경 내용을 모든 하위 폴더 및 파일에 전파하는 것입니다. 따라서 보안 스타일의 변경 사항을 모든 하위 폴더, 하위 폴더 및 파일에 전파하지 않으려면 전파 선택 사항을 원하는 설정으로 변경해야 합니다.

ONTAP NFS SVM 루트 볼륨에서 보안 스타일 구성

SVM(Storage Virtual Machine) 루트 볼륨 보안 스타일을 구성하여 SVM의 루트 볼륨에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 보안 스타일을 정의하려면 '-rootvolume-security-style' 매개 변수와 함께 'vserver create' 명령을 사용하십시오.

   루트 볼륨 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS 또는 혼합 입니다.

2. 생성한 SVM의 루트 볼륨 보안 유형을 포함하여 구성을 표시하고 확인합니다.

   'vserver show -vserver_vserver_name_'

ONTAP NFS FlexVol 볼륨에서 보안 스타일 구성

FlexVol 볼륨 보안 스타일을 구성하여 SVM(스토리지 가상 머신)의 FlexVol 볼륨에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

FlexVol 볼륨이	명령 사용…
아직 없습니다	보안 스타일을 지정하기 위해 볼륨 생성 및 '-security-style' 매개 변수를 포함합니다.
이미 있습니다	볼륨 수정, -security-style 매개 변수를 포함해서 보안 스타일을 지정합니다.

   FlexVol 볼륨 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS 또는 혼합 입니다.

   FlexVol 볼륨을 만들 때 보안 스타일을 지정하지 않으면 볼륨은 루트 볼륨의 보안 스타일을 상속합니다.

   볼륨 생성 또는 볼륨 수정 명령에 대한 자세한 내용은 을 참조하십시오 "논리적 스토리지 관리".

2. 생성한 FlexVol 볼륨의 보안 스타일을 포함하여 구성을 표시하려면 다음 명령을 입력합니다.

   'volume show-volume volume_name-instance'

ONTAP NFS qtree에서 보안 스타일 구성

Qtree 볼륨 보안 스타일을 구성하여 Qtree에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

qtree가…	명령 사용…
아직 없습니다	볼륨 qtree create를 수행하고 보안 스타일을 지정하는 -security-style 매개 변수를 포함합니다.
이미 있습니다	볼륨 qtree 수정과 보안 유형을 지정하는 -security-style 매개 변수를 포함합니다.

   qtree 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS, 혼합 입니다.

   Qtree를 만들 때 보안 스타일을 지정하지 않으면 기본 보안 스타일이 '혼합'으로 설정됩니다.

   '볼륨 qtree 생성' 또는 '볼륨 qtree 수정' 명령에 대한 자세한 내용은 을 참조하십시오 "논리적 스토리지 관리".

2. 생성한 qtree의 보안 스타일을 포함하여 구성을 표시하려면 'volume qtree show-qtree_qtree_name_-instance'

명령을 입력합니다

NFS를 사용하여 파일 액세스를 설정합니다

ONTAP SVM에서 NFS 파일 액세스 설정에 대해 알아보세요

고객이 NFS를 사용하여 SVM(스토리지 가상 시스템)의 파일에 액세스할 수 있도록 하려면 여러 단계를 완료해야 합니다. 환경의 현재 구성에 따라 몇 가지 추가 단계가 선택적으로 제공됩니다.

클라이언트가 NFS를 사용하여 SVM의 파일에 액세스할 수 있으려면 다음 작업을 완료해야 합니다.

1. SVM에서 NFS 프로토콜을 활성화합니다.

   NFS를 통해 클라이언트에서 데이터에 액세스할 수 있도록 SVM을 구성해야 합니다.

2. SVM에서 NFS 서버를 생성합니다.

   NFS 서버는 SVM에서 NFS를 통해 파일을 처리할 수 있는 논리적 엔터티입니다. NFS 서버를 생성하고 허용할 NFS 프로토콜 버전을 지정해야 합니다.

3. SVM에 엑스포트 정책을 구성합니다.

   클라이언트에서 볼륨 및 qtree를 사용할 수 있도록 엑스포트 정책을 구성해야 합니다.

4. 네트워크 및 스토리지 환경에 따라 적절한 보안 및 기타 설정으로 NFS 서버를 구성합니다.

   이 단계에는 Kerberos, LDAP, NIS, 이름 매핑 및 로컬 사용자 구성이 포함될 수 있습니다.

내보내기 정책을 사용하여 NFS 액세스를 보호합니다

내보내기 정책이 ONTAP NFS 볼륨 또는 Qtree에 대한 클라이언트 액세스를 제어하는 방법

엑스포트 정책에는 각 클라이언트 액세스 요청을 처리하는 _export rules_이 하나 이상 포함되어 있습니다. 프로세스 결과에 따라 클라이언트가 거부되었는지, 액세스 권한이 부여되었는지, 액세스 수준이 결정됩니다. 클라이언트가 데이터에 액세스할 수 있도록 SVM(스토리지 가상 시스템)에 엑스포트 규칙과 함께 엑스포트 정책이 있어야 합니다.

볼륨 또는 qtree에 대한 클라이언트 액세스를 구성하기 위해 각 볼륨 또는 qtree에 정확히 하나의 엑스포트 정책을 연결합니다. SVM에는 여러 엑스포트 정책이 포함될 수 있습니다. 따라서 여러 볼륨 또는 qtree를 사용하는 SVM에 대해 다음을 수행할 수 있습니다.

- 개별 클라이언트 액세스 제어를 SVM의 각 볼륨 또는 qtree에 서로 다른 엑스포트 정책을 지정하여 각 볼륨 또는 qtree에 대한 볼륨 또는 qtree를 관리할 수 있습니다.
- 각 볼륨 또는 qtree에 대해 새로운 엑스포트 정책을 생성할 필요 없이 동일한 클라이언트 액세스 제어를 위해 SVM의 여러 볼륨 또는 qtree에 동일한 엑스포트 정책을 할당합니다.

클라이언트가 해당 엑스포트 정책에서 허용하지 않는 액세스 요청을 하는 경우 권한 거부 메시지와 함께 요청이 실패합니다. 클라이언트가 엑스포트 정책의 규칙과 일치하지 않으면 액세스가 거부됩니다. 내보내기 정책이 비어 있으면 모든 액세스가 암시적으로 거부됩니다.

ONTAP를 실행하는 시스템에서 엑스포트 정책을 동적으로 수정할 수 있습니다.

ONTAP NFS SVM에 대한 기본 내보내기 정책

각 SVM에는 규칙이 없는 기본 엑스포트 정책이 있습니다. 클라이언트가 SVM에서 데이터에 액세스하려면 먼저 규칙과 함께 엑스포트 정책이 있어야 합니다. SVM에 포함된 각 FlexVol 볼륨은 엑스포트 정책과 연결되어야 합니다.

SVM을 생성할 때 스토리지 시스템은 SVM의 루트 볼륨에 대한 기본 엑스포트 정책인 'Default'를 자동으로 생성합니다. 클라이언트가 SVM에서 데이터에 액세스하려면 기본 엑스포트 정책에 대한 규칙을 하나 이상 생성해야 합니다. 또는 규칙을 사용하여 사용자 지정 엑스포트 정책을 생성할 수도 있습니다. 기본 엑스포트 정책을 수정 및 변경할 수 있지만, 기본 엑스포트 정책은 삭제할 수 없습니다.

SVM이 포함된 FlexVol 볼륨에서 스토리지 시스템은 볼륨을 생성한 후 SVM의 루트 볼륨에 대한 기본 엑스포트 정책과 연결합니다. 기본적으로 SVM에서 생성된 각 볼륨은 루트 볼륨의 기본 엑스포트 정책과 연결됩니다. SVM에 포함된 모든 볼륨에 기본 엑스포트 정책을 사용하거나, 각 볼륨에 대해 고유한 엑스포트 정책을 생성할 수 있습니다. 여러 볼륨을 동일한 엑스포트 정책에 연결할 수 있습니다.

ONTAP NFS 내보내기 규칙 작동 방식

내보내기 규칙은 엑스포트 정책의 기능 요소입니다. 내보내기 규칙은 클라이언트 액세스 요청을 처리하는 방법을 결정하기 위해 구성한 특정 매개 변수와 볼륨에 대한 클라이언트 액세스 요청을 일치시킵니다.

클라이언트에 대한 액세스를 허용하려면 내보내기 정책에 하나 이상의 내보내기 규칙이 있어야 합니다. 엑스포트 정책에 둘 이상의 규칙이 포함된 경우 규칙은 엑스포트 정책에 표시되는 순서대로 처리됩니다. 규칙 순서는 규칙 인덱스 번호로 지정됩니다. 규칙이 클라이언트와 일치하면 해당 규칙의 권한이 사용되며 추가 규칙은 처리되지 않습니다. 일치하는 규칙이 없으면 클라이언트가 액세스가 거부됩니다.

다음 조건을 사용하여 내보내기 규칙을 구성하여 클라이언트 액세스 권한을 결정할 수 있습니다.

- NFSv4 또는 SMB와 같이 요청을 보내는 클라이언트에서 사용하는 파일 액세스 프로토콜입니다.
- 호스트 이름 또는 IP 주소와 같은 클라이언트 식별자입니다.

  '-clientmatch' 필드의 최대 크기는 4096자입니다.

- Kerberos v5, NTLM 또는 AUTH_SYS와 같이 클라이언트에서 인증하는 데 사용되는 보안 유형입니다.

규칙이 여러 조건을 지정하는 경우 클라이언트는 규칙을 적용하기 위해 모든 조건을 충족해야 합니다.

> ONTAP 9.3부터 오류 규칙 목록에 규칙 위반을 기록하는 백그라운드 작업으로 내보내기 정책 구성 검사를 활성화할 수 있습니다. 'vserver export-policy config-checker' 명령은 checker를 호출하고 결과를 표시하며, 이 명령을 사용하여 구성을 확인하고 정책에서 잘못된 규칙을 삭제할 수 있습니다.
>
> 명령은 호스트 이름, 넷그룹 및 익명 사용자에 대한 내보내기 구성만 검증합니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3

- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '어다나'

클라이언트 액세스 요청은 NFSv3 프로토콜을 사용하여 전송되고 클라이언트의 IP 주소는 10.1.17.37입니다.

클라이언트 액세스 프로토콜이 일치하더라도 클라이언트의 IP 주소는 내보내기 규칙에 지정된 IP 주소와 다른 서브넷에 있습니다. 따라서 클라이언트 일치가 실패하고 이 규칙은 이 클라이언트에 적용되지 않습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '어다나'

클라이언트 액세스 요청은 NFSv4 프로토콜을 사용하여 전송되고 클라이언트의 IP 주소는 10.1.16.54입니다.

클라이언트 액세스 프로토콜이 일치하고 클라이언트의 IP 주소가 지정된 서브넷에 있습니다. 따라서 클라이언트 일치가 성공하고 이 규칙이 이 클라이언트에 적용됩니다. 클라이언트는 보안 유형에 관계없이 읽기-쓰기 액세스를 받습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '-rwrule' krb5, NTLM

클라이언트 #1의 IP 주소는 10.1.16.207이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5로 인증됩니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, AUTH_SYS로 인증됩니다.

클라이언트 액세스 프로토콜과 IP 주소는 두 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수를 사용하면 인증된 보안 유형에 관계없이 모든 클라이언트에 읽기 전용 액세스를 사용할 수 있습니다. 따라서 두 클라이언트 모두 읽기 전용 액세스 권한이 부여됩니다. 그러나 인증된 보안 유형 Kerberos v5를 사용하여 인증되었기 때문에 클라이언트 #1만 읽기-쓰기 액세스를 받습니다. 클라이언트 #2에서 읽기-쓰기 권한이 없습니다.

나열되지 않은 보안 유형을 사용하는 **NFS** 클라이언트에 대한 **ONTAP SVM** 액세스 관리

클라이언트가 엑스포트 규칙의 액세스 매개 변수에 나열되지 않은 보안 유형을 자체적으로 표시할 경우, 액세스 매개 변수에서 "없음" 옵션을 사용하는 대신 클라이언트에 대한 액세스를 거부하거나 익명 사용자 ID에 매핑할 수 있습니다.

클라이언트는 다른 보안 유형으로 인증되었거나 전혀 인증되지 않았기 때문에 액세스 매개 변수에 나열되지 않은 보안

형식(security type AUTH_none)으로 자신을 나타낼 수 있습니다. 기본적으로 클라이언트는 해당 수준에 대한 액세스가 자동으로 거부됩니다. 그러나, 액세스 파라미터에 'none' 옵션을 추가할 수 있습니다. 따라서 목록에 없는 보안 스타일이 있는 클라이언트는 대신 익명 사용자 ID에 매핑됩니다. '-anon' 매개 변수는 해당 클라이언트에 할당되는 사용자 ID를 결정합니다. '-anon' 매개 변수에 지정된 사용자 ID는 익명 사용자에게 적합한 권한으로 구성된 유효한 사용자여야 합니다.

'-anon' 파라미터의 유효 값은 0부터 65535까지입니다.

'-anon'에 할당된 사용자 **ID**입니다	이로 인해 클라이언트 액세스 요청이 처리되었습니다
0-65533	클라이언트 액세스 요청은 익명 사용자 ID에 매핑되며 이 사용자에 대해 구성된 권한에 따라 액세스를 가져옵니다.
65534	클라이언트 액세스 요청이 nobody 사용자에게 매핑되고 이 사용자에 대해 구성된 권한에 따라 액세스 권한이 부여됩니다. 이것이 기본값입니다.
65,535입니다	이 ID에 매핑되면 클라이언트의 액세스 요청이 거부되고 클라이언트는 보안 유형 AUTH_NONE으로 표시됩니다. 사용자 ID가 0인 클라이언트의 액세스 요청은 이 ID에 매핑될 때 거부되며 클라이언트는 다른 보안 유형을 제공합니다.

none 옵션을 사용할 때는 읽기 전용 매개변수가 먼저 처리된다는 점을 기억해야 합니다. 목록에 없는 보안 유형의 클라이언트에 대한 내보내기 규칙을 구성할 때 다음 지침을 고려하십시오.

읽기 전용에는 없음 이 포함됩니다	읽기**-**쓰기에는 없음도 있습니다	목록에 없는 보안 유형의 클라이언트에 대한 액세스
아니요	아니요	거부됨
아니요	예	읽기 전용이 먼저 처리되므로 거부됩니다
예	아니요	익명 읽기 전용
예	예	익명으로서 읽기-쓰기

예

다음 예에서는 다음을 포함하는 내보내기 정책을 보여줍니다. `-rwrule any` 매개변수:

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- "어이, 없습니다.
- '어다나'

- -아노온 70세

클라이언트 #1의 IP 주소는 10.1.16.207이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5로 인증됩니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, AUTH_SYS로 인증됩니다.

클라이언트 #3의 IP 주소는 10.1.16.234이고, NFSv3 프로토콜을 사용하여 액세스 요청을 전송하며, 인증되지 않았습니다(보안 유형 AUTH_NONE).

클라이언트 액세스 프로토콜 및 IP 주소는 세 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수는 AUTH_SYS로 인증된 고유한 사용자 ID를 사용하여 클라이언트에 대한 읽기 전용 액세스를 허용합니다. 읽기 전용 매개 변수는 다른 보안 유형을 사용하여 인증된 클라이언트에 사용자 ID 70을 가진 익명 사용자로 읽기 전용 액세스를 허용합니다. 읽기-쓰기 매개 변수는 모든 보안 유형에 대해 읽기-쓰기 액세스를 허용하지만 이 경우에는 읽기 전용 규칙에 의해 이미 필터링된 클라이언트에만 적용됩니다.

따라서 클라이언트 #1과 #3은 사용자 ID가 70인 익명 사용자로만 읽기-쓰기 권한을 받습니다. 클라이언트 #2는 고유한 사용자 ID를 사용하여 읽기-쓰기 권한을 받습니다.

다음 예에서는 다음을 포함하는 내보내기 정책을 보여줍니다. `-rwrule none` 매개변수:

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- "어이, 없습니다.
- '-rwrule' none
- -아노온 70세

클라이언트 #1의 IP 주소는 10.1.16.207이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5로 인증됩니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, AUTH_SYS로 인증됩니다.

클라이언트 #3의 IP 주소는 10.1.16.234이고, NFSv3 프로토콜을 사용하여 액세스 요청을 전송하며, 인증되지 않았습니다(보안 유형 AUTH_NONE).

클라이언트 액세스 프로토콜 및 IP 주소는 세 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수는 AUTH_SYS로 인증된 고유한 사용자 ID를 사용하여 클라이언트에 대한 읽기 전용 액세스를 허용합니다. 읽기 전용 매개 변수는 다른 보안 유형을 사용하여 인증된 클라이언트에 사용자 ID 70을 가진 익명 사용자로 읽기 전용 액세스를 허용합니다. 읽기-쓰기 매개 변수는 익명 사용자로만 읽기-쓰기 액세스를 허용합니다.

따라서 클라이언트 #1과 클라이언트 #3은 사용자 ID가 70인 익명 사용자로만 읽기-쓰기 권한을 받습니다. 클라이언트 #2는 자체 사용자 ID를 사용하여 읽기 전용 액세스를 얻지만 읽기-쓰기 액세스는 거부됩니다.

ONTAP 보안 유형이 **NFS** 클라이언트 액세스 수준을 결정하는 방식

클라이언트가 에서 인증한 보안 유형은 내보내기 규칙에서 특별한 역할을 합니다. 보안 유형에 따라 클라이언트가 볼륨 또는 qtree에 액세스하는 액세스 수준이 어떻게 결정되는지 이해해야

합니다.

세 가지 액세스 수준은 다음과 같습니다.

1. 읽기 전용
2. 읽기-쓰기
3. 슈퍼유저(사용자 ID가 0인 클라이언트의 경우)

보안 유형별 액세스 수준은 이 순서대로 평가되므로 내보내기 규칙에서 액세스 수준 매개 변수를 구성할 때 다음 규칙을 준수해야 합니다.

클라이언트가 액세스 레벨을 얻는 경우...	이러한 액세스 매개 변수는 클라이언트의 보안 유형과 일치해야 합니다.
일반 사용자 읽기 전용	읽기 전용('-rorule')
일반 사용자 읽기-쓰기	읽기 전용('-rorule') 및 읽기/쓰기('-rwrule')
고급 사용자 읽기 전용	읽기 전용('rorule') 및 '-superuser'
고급 사용자 읽기-쓰기	읽기 전용('rorule') 및 읽기/쓰기('rwrule') 및 '-superuser'

다음은 이러한 세 가지 액세스 매개 변수 각각에 대해 유효한 보안 유형입니다.

- 모두
- "없음"
- "안 돼.

  이 보안 유형은 '-superuser' 매개변수와 함께 사용할 수 없습니다.

- krb5
- krb5i
- 크르b5p
- NTLM
- '스'입니다

클라이언트의 보안 유형을 세 가지 액세스 매개 변수 각각에 일치시킬 경우 다음과 같은 세 가지 결과가 발생할 수 있습니다.

클라이언트의 보안 유형인 경우...	그러면 고객은...
access 매개 변수에 지정된 것과 일치합니다.	해당 사용자 ID를 사용하여 해당 수준에 대한 액세스를 가져옵니다.

클라이언트의 보안 유형인 경우...	그러면 고객은...
지정된 옵션과 일치하지 않지만 액세스 매개 변수에는 '없음' 옵션이 포함됩니다.	'-anon' 매개 변수로 지정한 사용자 ID를 가진 익명 사용자로 해당 수준에 대한 액세스를 가져옵니다.
지정된 옵션과 일치하지 않으며 액세스 매개 변수에 '없음' 옵션이 포함되어 있지 않습니다.	이 수준은 지정되지 않은 경우에도 항상 '없음'을 포함하므로 '-superuser' 매개 변수에는 적용되지 않습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '-rwrule"s, krb5'
- 슈퍼유저 krb5

클라이언트 #1에는 IP 주소가 10.1.16.207이고 사용자 ID가 0이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, Kerberos v5로 인증되었습니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고 사용자 ID 0이 있으며 NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 AUTH_SYS로 인증되었습니다.

클라이언트 #3의 IP 주소는 10.1.16.234이고, 사용자 ID 0이 있으며, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, 인증하지 않았습니다(AUTH_NONE).

클라이언트 액세스 프로토콜 및 IP 주소는 세 클라이언트 모두와 일치합니다. 읽기 전용 매개 변수는 보안 유형에 관계없이 모든 클라이언트에 대한 읽기 전용 액세스를 허용합니다. 읽기-쓰기 매개 변수는 AUTH_SYS 또는 Kerberos v5로 인증된 고유한 사용자 ID를 사용하여 클라이언트에 대한 읽기-쓰기 액세스를 허용합니다. 슈퍼유저 매개 변수를 사용하면 Kerberos v5로 인증된 사용자 ID 0을 가진 클라이언트에 슈퍼유저 액세스가 가능합니다.

따라서 클라이언트 #1은 세 가지 액세스 매개 변수와 모두 일치하기 때문에 수퍼유저 읽기-쓰기 액세스 권한을 얻습니다. 클라이언트 #2에 읽기-쓰기 액세스 권한이 있지만 고급 사용자 액세스 권한이 없습니다. 클라이언트 #3은 읽기 전용 액세스 권한을 얻지만 고급 사용자 액세스는 받지 않습니다.

ONTAP NFS 슈퍼유저 액세스 요청 관리에 대해 알아보세요

엑스포트 정책을 구성할 때는 스토리지 시스템이 사용자 ID 0의 클라이언트 액세스 요청을 받으면 수행할 작업을 고려해야 합니다. 즉, 고급 사용자로서 엑스포트 규칙을 설정해야 합니다.

UNIX 환경에서 사용자 ID 0을 가진 사용자는 일반적으로 시스템에 대한 무제한 액세스 권한이 있는 슈퍼유저라고 합니다. 고급 사용자 권한을 사용하는 것은 시스템 위반 및 데이터 보안을 비롯한 여러 가지 이유로 위험할 수 있습니다.

기본적으로 ONTAP는 사용자 ID 0을 사용하는 클라이언트를 익명 사용자에게 매핑합니다. 그러나 내보내기 규칙에서 '-superuser' 매개 변수를 지정하여 보안 유형에 따라 사용자 ID 0으로 나타나는 클라이언트를 처리하는 방법을 결정할 수 있습니다. 다음은 '-superuser' 파라미터에 대한 유효한 옵션입니다.

- 모두

- "없음"

  이 설정은 '-superuser' 파라미터를 지정하지 않을 경우 기본 설정입니다.

- krb5
- NTLM
- '스'입니다

'-superuser' 매개 변수 구성에 따라 사용자 ID 0으로 표시하는 클라이언트가 처리되는 방법에는 두 가지가 있습니다.

'-superuser' 매개변수와 클라이언트의 보안 유형이…	그러면 고객은…
일치	사용자 ID 0을 사용하여 수퍼유저 액세스 권한을 가져옵니다.
일치하지 않습니다	'-anon' 매개 변수에 지정된 사용자 ID와 할당된 사용 권한을 가진 익명 사용자로 액세스를 가져옵니다. 이는 읽기 전용 또는 읽기/쓰기 매개 변수가 '없음' 옵션을 지정하는지 여부에 관계없이 적용됩니다.

클라이언트가 NTFS 보안 스타일로 볼륨에 액세스하기 위해 사용자 ID 0을 제공하고 '-superuser' 매개 변수가 'none'으로 설정된 경우 ONTAP는 익명 사용자의 이름 매핑을 사용하여 적절한 자격 증명을 얻습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '-rwrule' krb5, NTLM
- '-anon"127

클라이언트 #1에는 IP 주소가 10.1.16.207이고 사용자 ID 746을 가지고 있으며, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5를 사용하여 인증합니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고 사용자 ID 0이 있으며 NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 AUTH_SYS로 인증되었습니다.

클라이언트 액세스 프로토콜과 IP 주소는 두 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수를 사용하면 인증된 보안 유형에 관계없이 모든 클라이언트에 읽기 전용 액세스를 사용할 수 있습니다. 그러나 인증된 보안 유형 Kerberos v5를 사용하여 인증되었기 때문에 클라이언트 #1만 읽기-쓰기 액세스를 받습니다.

클라이언트 #2에서 수퍼유저 액세스 권한을 얻을 수 없습니다. 대신 '-superuser' 매개 변수가 지정되지 않아 익명으로 매핑됩니다. 즉, 기본적으로 '없음'으로 설정되어 있으며 사용자 ID 0을 익명으로 자동 매핑합니다. 또한 보안 형식이 읽기-쓰기 매개 변수와 일치하지 않기 때문에 클라이언트 #2는 읽기 전용 액세스만 받습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '-rwrule' krb5, NTLM
- 슈퍼유저 krb5
- 0

클라이언트 #1에는 IP 주소가 10.1.16.207이고 사용자 ID가 0이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, Kerberos v5로 인증되었습니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고 사용자 ID 0이 있으며 NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 AUTH_SYS로 인증되었습니다.

클라이언트 액세스 프로토콜과 IP 주소는 두 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수를 사용하면 인증된 보안 유형에 관계없이 모든 클라이언트에 읽기 전용 액세스를 사용할 수 있습니다. 그러나 인증된 보안 유형 Kerberos v5를 사용하여 인증되었기 때문에 클라이언트 #1만 읽기-쓰기 액세스를 받습니다. 클라이언트 #2에서 읽기-쓰기 권한이 없습니다.

내보내기 규칙은 사용자 ID가 0인 클라이언트에 대한 수퍼유저 액세스를 허용합니다. 클라이언트 #1은 읽기 전용 및 '-superuser' 매개 변수의 사용자 ID와 보안 유형과 일치하기 때문에 수퍼유저 액세스 권한을 얻습니다. 보안 유형이 읽기-쓰기 매개 변수나 '-superuser' 매개 변수와 일치하지 않기 때문에 클라이언트 #2에서 읽기-쓰기 또는 수퍼유저 액세스 권한을 얻지 못합니다. 대신 클라이언트 #2가 익명 사용자에게 매핑되며 이 경우 사용자 ID 0이 있습니다.

ONTAP NFS 내보내기 정책 캐시에 대해 알아보세요

시스템 성능을 개선하기 위해 ONTAP는 로컬 캐시를 사용하여 호스트 이름 및 넷그룹과 같은 정보를 저장합니다. 이렇게 하면 ONTAP에서 외부 소스에서 정보를 검색하는 것보다 내보내기 정책 규칙을 더 빠르게 처리할 수 있습니다. 캐시의 정의 및 작업을 이해하면 클라이언트 액세스 문제를 해결하는 데 도움이 됩니다.

NFS 내보내기에 대한 클라이언트 액세스를 제어하기 위해 엑스포트 정책을 구성합니다. 각 엑스포트 정책에는 규칙이 포함되어 있으며, 각 규칙에는 액세스를 요청하는 클라이언트와 규칙을 일치시키는 매개 변수가 포함되어 있습니다. 이러한 매개 변수 중 일부는 도메인 이름, 호스트 이름 또는 넷그룹과 같은 개체를 확인하기 위해 ONTAP에서 DNS 또는 NIS 서버와 같은 외부 소스에 연결해야 합니다.

외부 소스와의 이러한 통신에는 약간의 시간이 소요됩니다. 성능을 높이기 위해 ONTAP는 여러 캐시의 각 노드에 정보를 로컬로 저장하여 엑스포트 정책 규칙 개체를 해결하는 데 걸리는 시간을 단축합니다.

캐시 이름입니다	저장된 정보의 유형입니다
액세스	해당 엑스포트 정책에 대한 클라이언트 매핑
이름	UNIX 사용자 이름을 해당 UNIX 사용자 ID에 매핑
ID입니다	UNIX 사용자 ID와 해당 UNIX 사용자 ID 및 확장 UNIX 그룹 ID의 매핑
호스트	호스트 이름을 해당 IP 주소에 매핑

캐시 이름입니다	저장된 정보의 유형입니다
넷그룹	구성원의 해당 IP 주소에 대한 넷그룹 매핑
쇼마운트	SVM 네임스페이스에서 내보낸 디렉토리 목록입니다

ONTAP에서 검색 및 로컬에 저장한 후 환경에 있는 외부 이름 서버의 정보를 변경하면 캐시에 오래된 정보가 포함될 수 있습니다. ONTAP를 새로 고치면 특정 기간이 지나면 자동으로 캐시가 새로 고쳐지지만 다른 캐시에 만료 및 새로 고침 시간과 알고리즘이 다릅니다.

캐시에 오래된 정보가 포함되는 또 다른 가능한 이유는 ONTAP가 캐시된 정보를 새로 고치려고 하지만 이름 서버와 통신하려고 할 때 오류가 발생하는 것입니다. 이 경우 ONTAP는 클라이언트 중단을 방지하기 위해 로컬 캐시에 현재 저장되어 있는 정보를 계속 사용합니다.

따라서 성공해야 하는 클라이언트 액세스 요청이 실패하고 실패해야 하는 클라이언트 액세스 요청이 성공할 수 있습니다. 이러한 클라이언트 액세스 문제를 해결할 때 일부 엑스포트 정책 캐시를 보고 수동으로 플러시할 수 있습니다.

ONTAP NFS 액세스 캐시에 대해 알아보세요

ONTAP은 액세스 캐시를 사용하여 클라이언트 액세스 작업에 대한 엑스포트 정책 규칙 평가 결과를 볼륨 또는 qtree에 저장합니다. 따라서 클라이언트가 입출력 요청을 보낼 때마다 내보내기 정책 규칙 평가 프로세스를 거치는 것보다 액세스 캐시에서 정보를 훨씬 빠르게 검색할 수 있기 때문에 성능이 향상됩니다.

NFS 클라이언트가 볼륨 또는 qtree의 데이터에 액세스하기 위해 I/O 요청을 보낼 때마다 ONTAP는 각 I/O 요청을 평가하여 I/O 요청을 허용하거나 거부할 것인지 결정해야 합니다. 이 평가에서는 볼륨 또는 qtree와 관련된 엑스포트 정책의 모든 엑스포트 정책 규칙을 검사합니다. 볼륨 또는 qtree에 대한 경로에 하나 이상의 접합 지점이 포함되는 경우, 경로를 따라 여러 엑스포트 정책을 위해 이 점검을 수행해야 할 수 있습니다.

이 평가는 초기 마운트 요청뿐만 아니라 읽기, 쓰기, 목록, 복사 및 기타 작업과 같이 NFS 클라이언트에서 전송된 모든 입출력 요청에 대해 수행됩니다.

ONTAP가 해당 엑스포트 정책 규칙을 식별하고 요청을 허용 또는 거부할지 결정한 후에는 ONTAP가 액세스 캐시에 이 정보를 저장하기 위한 항목을 생성합니다.

NFS 클라이언트가 I/O 요청을 보낼 때 ONTAP는 클라이언트의 IP 주소, SVM의 ID, 타겟 볼륨 또는 qtree와 관련된 엑스포트 정책을 기록한 다음, 액세스 캐시에서 일치하는 항목을 확인합니다. 액세스 캐시에 일치하는 항목이 있는 경우 ONTAP는 저장된 정보를 사용하여 I/O 요청을 허용하거나 거부합니다. 일치하는 항목이 없는 경우 ONTAP는 위에서 설명한 모든 해당 정책 규칙을 평가하는 일반적인 프로세스를 수행합니다.

활성 상태로 사용되지 않는 액세스 캐시 항목은 새로 고쳐지지 않습니다. 이렇게 하면 외부 이름 서비스와의 불필요한 소모적인 통신이 줄어듭니다.

액세스 캐시에서 정보를 검색하는 것이 모든 입출력 요청에 대해 전체 엑스포트 정책 규칙 평가 프로세스를 수행하는 것보다 훨씬 빠릅니다. 따라서 액세스 캐시를 사용하면 클라이언트 액세스 검사의 오버헤드를 줄여 성능을 크게 향상시킬 수 있습니다.

ONTAP NFS 액세스 캐시 매개변수에 대해 알아보세요

여러 매개 변수는 액세스 캐시의 항목에 대한 새로 고침 기간을 제어합니다. 이러한 매개 변수의 작동 방식을 이해하면 액세스 캐시를 조정하고 저장된 정보의 최근 성능과 균형을 유지하도록

매개 변수를 수정할 수 있습니다.

액세스 캐시는 볼륨 또는 qtree에 액세스하려는 클라이언트에 적용되는 하나 이상의 엑스포트 규칙으로 구성된 항목을 저장합니다. 이러한 항목은 새로 고쳐지기 전에 일정 시간 동안 저장됩니다. 새로 고침 시간은 액세스 캐시 매개 변수에 의해 결정되며 액세스 캐시 항목의 유형에 따라 달라집니다.

개별 SVM에 대한 액세스 캐시 매개 변수를 지정할 수 있습니다. 따라서 SVM 액세스 요구사항에 따라 매개 변수가 달라질 수 있습니다. 활성 상태로 사용되지 않는 액세스 캐시 항목은 새로 고쳐지지 않으므로 외부 이름 서비스와의 불필요한 소모적인 통신이 줄어듭니다.

액세스 캐시 항목 유형입니다	설명	새로 고침 기간(초
양의 입력	액세스 캐시 항목으로 인해 클라이언트에 대한 액세스 거부가 발생되지 않았습니다.	최소: 300 최대: 86,400 기본값: 3,600
음수 항목	액세스 캐시 항목으로 인해 클라이언트에 대한 액세스 거부가 발생했습니다.	최소: 60 최대: 86,400 기본값: 3,600

예

NFS 클라이언트가 클러스터의 볼륨에 액세스하려고 합니다. ONTAP는 클라이언트를 엑스포트 정책 규칙과 일치시키고 클라이언트가 엑스포트 정책 규칙 구성에 따라 액세스할 수 있는지 확인합니다. ONTAP는 액세스 캐시에 있는 내보내기 정책 규칙을 양의 항목으로 저장합니다. 기본적으로 ONTAP는 액세스 캐시의 양의 항목을 1시간(3,600초) 동안 유지한 다음 해당 항목을 자동으로 새로 고쳐 정보를 최신 상태로 유지합니다.

액세스 캐시가 불필요하게 가득 차는 것을 방지하기 위해 특정 기간 동안 사용하지 않은 기존 액세스 캐시 항목을 지우기 위한 추가 매개 변수가 있습니다. 이 '-하비스트-timeout' 매개 변수는 허용되는 범위는 60초에서 2,592,000초이며 기본 설정은 86,400초입니다.

ONTAP NFS qtree에서 내보내기 정책 제거

특정 엑스포트 정책을 qtree에 더 이상 할당하지 않으려는 경우, qtree를 수정하여 포함하는 볼륨의 엑스포트 정책을 상속하도록 엑스포트 정책을 제거할 수 있습니다. 이렇게 하려면 '-export-policy' 매개 변수와 빈 이름 문자열("")을 사용하여 볼륨 qtree modify 명령을 사용할 수 있습니다.

단계

1. qtree에서 엑스포트 정책을 제거하려면 다음 명령을 입력합니다.

   "볼륨 qtree modify -vserver vserver_name -qtree -path /vol/volume_name /qtree_name -export-policy""

2. qtree가 적절히 수정되었는지 확인합니다.

   '볼륨 qtree show-qtree qtree_name-fields export-policy’입니다

qtree 파일 작업에 대한 ONTAP NFS qtree ID 검증

ONTAP에서는 qtree ID에 대한 선택적 추가 검증을 수행할 수 있습니다. 이 검증에서는 클라이언트 파일 작업 요청이 유효한 qtree ID를 사용하고 클라이언트가 동일한 qtree 내의 파일만 이동할 수 있는지 확인합니다. '-validate-qtree-export' 매개 변수를 수정하여 이 유효성 검사를 활성화 또는 비활성화할 수 있습니다. 이 매개 변수는 기본적으로 사용하도록 설정됩니다.

이 작업에 대해

이 매개 변수는 SVM(스토리지 가상 머신)에서 하나 이상의 qtree에 엑스포트 정책을 직접 할당한 경우에만 효과적입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

Qtree ID 검증을 원하는 경우…	다음 명령을 입력합니다…
활성화됨	'vserver nfs modify -vserver vserver_name -validate -qtree -export enabled'
사용 안 함	'vserver nfs modify -vserver vserver_name -validate -qtree -export disabled'

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

ONTAP NFS FlexVol 볼륨에 대한 정책 제한 및 중첩된 연결 내보내기

중첩 교차점에 덜 제한적인 정책을 설정하지만 상위 수준 교차점에 더 제한적인 정책을 설정하도록 내보내기 정책을 구성한 경우 하위 수준 교차점에 액세스하지 못할 수 있습니다.

상위 레벨의 교차로에서 낮은 레벨의 교차로보다 제한적인 엑스포트 정책이 있는지 확인해야 합니다.

강력한 보안을 위해 NFS와 Kerberos 사용

Kerberos에 대한 ONTAP NFS 지원

Kerberos는 클라이언트/서버 응용 프로그램에 대해 강력한 보안 인증을 제공합니다. 인증을 통해 사용자 및 프로세스 ID를 서버에 확인할 수 있습니다. ONTAP 환경에서 Kerberos는 SVM(스토리지 가상 머신)과 NFS 클라이언트 간에 인증을 제공합니다.

ONTAP 9에서는 다음과 같은 Kerberos 기능이 지원됩니다.

- 무결성 검사를 통한 Kerberos 5 인증(krb5i)

Krb5i는 체크섬을 사용하여 클라이언트와 서버 간에 전송되는 각 NFS 메시지의 무결성을 확인합니다. 이는 보안상의 이유(예: 데이터가 무단 변경되지 않도록 보장) 및 데이터 무결성을 위해(예: 불안정한 네트워크에서 NFS를 사용할 때 데이터 손상을 방지) 모두에 유용합니다.

- Kerberos 5 개인 정보 확인 인증(krb5p)

  Krb5p는 체크섬을 사용하여 클라이언트와 서버 사이의 모든 트래픽을 암호화합니다. 이는 보다 안전하며 부하가 더 많이 발생합니다.

- 128비트 및 256비트 AES 암호화

  AES(Advanced Encryption Standard)는 전자 데이터의 보안을 위한 암호화 알고리즘입니다. ONTAP은 128비트 키(AES-128)로 AES와 256비트 키(AES-256) 암호화를 사용하여 Kerberos를 더욱 강력하게 지원합니다.

- SVM 레벨 Kerberos 영역 구성

  이제 SVM 관리자가 SVM 레벨에서 Kerberos 영역 구성을 생성할 수 있습니다. 즉, SVM 관리자는 더 이상 Kerberos 영역 구성을 위해 클러스터 관리자에 의존하지 않고 다중 테넌시 환경에서 개별 Kerberos 영역 구성을 생성할 수 있습니다.

ONTAP NFS를 사용하여 **Kerberos**를 구성하기 위한 요구 사항

시스템에서 NFS로 Kerberos를 구성하기 전에 네트워크 및 스토리지 환경의 특정 항목이 올바르게 구성되었는지 확인해야 합니다.

> 환경을 구성하는 단계는 사용 중인 클라이언트 운영 체제, 도메인 컨트롤러, Kerberos, DNS 등의 버전과 유형에 따라 다릅니다. 이러한 모든 변수를 문서화하는 것은 이 문서의 범위를 벗어납니다. 자세한 내용은 각 구성 요소에 대한 각 설명서를 참조하십시오.
>
> Windows Server 2008 R2 Active Directory 및 Linux 호스트를 사용하는 환경에서 NFSv3 및 NFSv4를 사용하여 ONTAP 및 Kerberos 5를 설정하는 방법에 대한 자세한 내용은 기술 보고서 4073을 참조하십시오.

다음 항목을 먼저 구성해야 합니다.

네트워크 환경 요구 사항

- Kerberos

  Windows Active Directory 기반 Kerberos 또는 MIT Kerberos와 같은 KDC(키 배포 센터)를 사용하여 작동하는 Kerberos 설정이 있어야 합니다.

  NFS 서버는 시스템 보안 주체의 주요 구성 요소로 NFS를 사용해야 합니다.

- 디렉터리 서비스

  SSL/TLS를 통해 LDAP를 사용하도록 구성된 Active Directory 또는 OpenLDAP와 같은 환경에서 보안 디렉터리 서비스를 사용해야 합니다.

- NTP

  NTP를 실행하는 작업 시간 서버가 있어야 합니다. 시간 편중이 발생하여 Kerberos 인증 실패를 방지하려면 이

작업이 필요합니다.

- 도메인 이름 확인(DNS)

  각 UNIX 클라이언트와 각 SVM LIF에는 정방향 및 역방향 조회 영역에서 KDC에 등록된 적절한 서비스 레코드(SRV)가 있어야 합니다. 모든 참가자는 DNS를 통해 제대로 확인할 수 있어야 합니다.

- 사용자 계정

  각 클라이언트에는 Kerberos 영역에 사용자 계정이 있어야 합니다. NFS 서버는 시스템 보안 주체의 기본 구성 요소로 "NFS"를 사용해야 합니다.

NFS 클라이언트 요구 사항

- NFS 를 참조하십시오

  NFSv3 또는 NFSv4를 사용하여 네트워크를 통해 통신하도록 각 클라이언트를 올바르게 구성해야 합니다.

  고객은 RFC1964 및 RFC2203을 지원해야 합니다.

- Kerberos

  각 클라이언트는 Kerberos 인증을 사용하도록 적절히 구성되어야 하며, 다음과 같은 세부 정보가 포함되어야 합니다.

  - TGS 통신에 대한 암호화가 활성화되었습니다.

    강력한 보안을 위한 AES-256.

  - TGT 통신을 위한 가장 안전한 암호화 유형이 활성화됩니다.
  - Kerberos 영역과 도메인이 올바르게 구성되었습니다.
  - GSS가 활성화되었습니다.

    시스템 자격 증명을 사용하는 경우:

  - gssd를 -n 매개변수로 실행하지 마십시오.
  - 루트 사용자로 "kinit"를 실행하지 마십시오.

- 각 클라이언트는 최신 및 업데이트된 운영 체제 버전을 사용해야 합니다.

  Kerberos와 AES 암호화를 위한 최고의 호환성과 안정성을 제공합니다.

- DNS

  올바른 이름 확인을 위해 DNS를 사용하도록 각 클라이언트를 올바르게 구성해야 합니다.

- NTP

  각 클라이언트는 NTP 서버와 동기화되어야 합니다.

- 호스트 및 도메인 정보

각 클라이언트의 '/etc/hosts' 및 '/etc/resolv.conf' 파일은 각각 올바른 호스트 이름과 DNS 정보를 포함해야 합니다.

- keytab 파일

  각 클라이언트에는 KDC의 keytab 파일이 있어야 합니다. 영역은 대문자여야 합니다. 가장 강력한 보안을 위해서는 암호화 유형이 AES-256이어야 합니다.

- 선택 사항: 최상의 성능을 위해 클라이언트는 최소한 두 개의 네트워크 인터페이스를 가질 수 있습니다. 하나는 로컬 영역 네트워크와 통신하며 다른 하나는 스토리지 네트워크와 통신하기 위한 것입니다.

수행할 수 있습니다

- NFS 라이센스

  스토리지 시스템에 유효한 NFS 라이센스가 설치되어 있어야 합니다.

- CIFS 라이센스

  CIFS 라이센스는 선택 사항입니다. 멀티프로토콜 이름 매핑을 사용할 때는 Windows 자격 증명을 확인하는 데만 필요합니다. 엄격한 UNIX 전용 환경에서는 필요하지 않습니다.

- SVM

  시스템에 SVM이 하나 이상 구성되어 있어야 합니다.

- SVM의 DNS

  각 SVM에서 DNS를 구성해야 합니다.

- NFS 서버

  SVM에서 NFS를 구성해야 합니다.

- AES 암호화

  가장 강력한 보안을 위해서는 Kerberos에 AES-256 암호화만 허용하도록 NFS 서버를 구성해야 합니다.

- SMB 서버

  멀티프로토콜 환경을 실행 중인 경우 SVM에서 SMB를 구성해야 합니다. 멀티 프로토콜 이름 매핑에 SMB 서버가 필요합니다.

- 볼륨

  루트 볼륨과 SVM에서 사용하도록 구성된 데이터 볼륨이 하나 이상 있어야 합니다.

- 루트 볼륨

  SVM의 루트 볼륨에는 다음 구성이 있어야 합니다.

이름	설정
보안 스타일	Unix
UID	루트 또는 ID 0
GID	루트 또는 ID 0
Unix 사용 권한	777

루트 볼륨과 달리 데이터 볼륨은 보안 스타일을 가질 수 있습니다.

- Unix 그룹

  SVM에는 다음과 같은 UNIX 그룹이 구성되어 있어야 합니다.

그룹 이름	그룹 **ID**입니다
데몬	1
루트	0
pcuser	65534(SVM 생성 시 ONTAP에서 자동으로 생성)

- Unix 사용자

  SVM에는 다음과 같은 UNIX 사용자가 구성되어 있어야 합니다.

사용자 이름입니다	사용자 **ID**입니다	기본 그룹 **ID**입니다	설명
NFS 를 참조하십시오	500입니다	0	GSS INIT 단계에 필요함 NFS 클라이언트 사용자 SPN의 첫 번째 구성 요소가 사용자로 사용됩니다.
pcuser	65534	65534	NFS 및 CIFS를 멀티프로토콜 용도로 필요합니다 SVM을 생성할 때 ONTAP이 pcuser 그룹을 자동으로 생성하여 추가했습니다.
루트	0	0	마운팅에 필요합니다

NFS 클라이언트 사용자의 SPN에 대한 Kerberos-UNIX 이름 매핑이 있는 경우 NFS 사용자는 필요하지 않습니다.

- 엑스포트 정책 및 규칙

  루트 및 데이터 볼륨 및 qtree에 필요한 엑스포트 규칙을 사용하여 엑스포트 정책을 구성해야 합니다. Kerberos를 통해 SVM의 모든 볼륨에 액세스할 경우 루트 볼륨에 대한 내보내기 규칙 옵션 '-rorule', '-rwrule' 및 '-superuser'를 krb5', krb5i 또는 krb5p로 설정할 수 있습니다.

- Kerberos - UNIX 이름 매핑

  NFS 클라이언트 사용자 SPN에 의해 식별된 사용자에게 루트 권한을 부여하려면 루트에 대한 이름 매핑을 생성해야 합니다.

관련 정보

"NetApp 기술 보고서 4073: 안전한 통합 인증"

"NetApp 상호 운용성 매트릭스 툴"

"시스템 관리"

"논리적 스토리지 관리"

NFSv4에 대한 **ONTAP** 사용자 **ID** 도메인을 지정합니다.

사용자 ID 도메인을 지정하려면 '-v4-id-domain' 옵션을 설정합니다.

이 작업에 대해

기본적으로 ONTAP에서는 NFSv4 사용자 ID 매핑이 설정된 경우 NIS 도메인을 사용합니다. NIS 도메인이 설정되어 있지 않으면 DNS 도메인이 사용됩니다. 예를 들어 여러 사용자 ID 도메인이 있는 경우 사용자 ID 도메인을 설정해야 할 수 있습니다. 도메인 이름은 도메인 컨트롤러의 도메인 구성과 일치해야 합니다. NFSv3에는 필요하지 않습니다.

단계

1. 다음 명령을 입력합니다.

   'vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name'

이름 서비스 구성

ONTAP NFS 이름 서비스 스위치 구성에 대해 자세히 알아보십시오

ONTAP는 UNIX 시스템의 '/etc/nsswitch.conf' 파일에 해당하는 테이블에 이름 서비스 구성 정보를 저장합니다. 환경에 맞게 적절하게 구성할 수 있도록 표의 기능과 ONTAP에서 표의 사용 방법을 이해해야 합니다.

ONTAP 이름 서비스 스위치 테이블은 ONTAP가 특정 유형의 이름 서비스 정보에 대한 정보를 검색하기 위해 어떤 이름 서비스 소스를 참조합니다. ONTAP는 SVM별로 개별 네임 서비스 스위치 테이블을 유지 관리합니다.

데이터베이스 유형

이 테이블에는 다음과 같은 각 데이터베이스 유형에 대해 별도의 이름 서비스 목록이 저장됩니다.

데이터베이스 유형입니다	다음에 대한 이름 서비스 소스를 정의합니다.	유효한 소스는...
호스트	호스트 이름을 IP 주소로 변환	파일, DNS
그룹	사용자 그룹 정보를 찾는 중입니다	파일, NIS, LDAP
암호	사용자 정보를 찾는 중입니다	파일, NIS, LDAP
넷그룹	넷그룹 정보를 찾는 중입니다	파일, NIS, LDAP
이름맵	사용자 이름 매핑 중	파일, LDAP

소스 유형

소스는 해당 정보를 검색하는 데 사용할 이름 서비스 소스를 지정합니다.

원본 유형 지정...	에서 정보를 조회하려면...	관리 대상 명령 제품군...
파일	로컬 소스 파일	SVM 서비스 이름 서비스 유닉스 사용자 SVM 서비스 이름 서비스 유닉스 그룹 SVM 서비스 이름 서비스 넷그룹 SVM 서비스 이름-서비스 DNS 호스트
NIS를 선택합니다	SVM의 NIS 도메인 구성에 지정된 외부 NIS 서버	'vserver services name-service nis-domain'을 선택합니다
LDAP를 지원합니다	SVM의 LDAP 클라이언트 구성에 지정된 외부 LDAP 서버	'vserver services name-service ldap'
DNS	SVM의 DNS 구성에 지정된 외부 DNS 서버	SVM 서비스 이름-서비스 DNS

데이터 액세스와 SVM 관리 인증 모두에 NIS 또는 LDAP를 사용하려는 경우에도 NIS 또는 LDAP 인증이 실패할 경우 "파일"을 포함하고 로컬 사용자를 대체 수단으로 구성해야 합니다.

외부 소스에 액세스하는 데 사용되는 프로토콜입니다

외부 소스의 서버에 액세스하기 위해 ONTAP는 다음 프로토콜을 사용합니다.

외부 이름 서비스 소스입니다	액세스에 사용되는 프로토콜입니다
NIS를 선택합니다	UDP입니다

외부 이름 서비스 소스입니다	액세스에 사용되는 프로토콜입니다
DNS	UDP입니다
LDAP를 지원합니다	TCP

예

다음 예는 SVM svm_1의 이름 서비스 스위치 구성을 표시합니다.

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                    Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

호스트의 IP 주소를 조회하기 위해 ONTAP는 먼저 로컬 소스 파일을 참조합니다. 쿼리가 결과를 반환하지 않으면 다음으로 DNS 서버가 선택됩니다.

사용자 또는 그룹 정보를 조회하기 위해 ONTAP는 로컬 소스 파일만 참조합니다. 쿼리가 결과를 반환하지 않으면 조회가 실패합니다.

넷그룹 정보를 조회하기 위해 ONTAP는 먼저 외부 NIS 서버를 참조합니다. 쿼리가 결과를 반환하지 않으면 로컬 넷그룹 파일이 다음에 선택됩니다.

SVM svm_1의 테이블에는 이름 매핑에 대한 이름 서비스 항목이 없습니다. 따라서 ONTAP는 기본적으로 로컬 소스 파일만 참조합니다.

관련 정보

"NetApp 기술 보고서 4668: 이름 서비스 모범 사례 가이드"

LDAP를 사용합니다

ONTAP NFS SVM용 **LDAP**에 대해 알아보세요

LDAP(Lightweight Directory Access Protocol) 서버를 사용하면 사용자 정보를 중앙에서 관리할 수 있습니다. 사용자 환경의 LDAP 서버에 사용자 데이터베이스를 저장하는 경우 기존 LDAP 데이터베이스에서 사용자 정보를 조회하도록 스토리지 시스템을 구성할 수 있습니다.

- ONTAP용 LDAP를 구성하기 전에 사이트 배포가 LDAP 서버 및 클라이언트 구성에 대한 모범 사례를 충족하는지 확인해야 합니다. 특히 다음 조건을 충족해야 합니다.
  - LDAP 서버의 도메인 이름이 LDAP 클라이언트의 항목과 일치해야 합니다.

- LDAP 서버에서 지원하는 LDAP 사용자 암호 해시 유형에는 ONTAP에서 지원하는 해시 유형이 포함되어야 합니다.
  - 암호화(모든 유형) 및 SHA-1(SHA, SSHA).
  - ONTAP 9.8부터 SHA-2 해시(SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, SSHA-512)도 지원됩니다.
- LDAP 서버에 세션 보안 조치가 필요한 경우 LDAP 클라이언트에서 이를 구성해야 합니다.

  다음 세션 보안 옵션을 사용할 수 있습니다.

  - LDAP 서명(데이터 무결성 검사 제공) 및 LDAP 서명 및 봉인(데이터 무결성 검사 및 암호화 제공)
  - TLS를 시작합니다
  - LDAPS(TLS 또는 SSL을 통한 LDAP)
- 서명되고 봉인된 LDAP 쿼리를 사용하려면 다음 서비스를 구성해야 합니다.
  - LDAP 서버는 GSSAPI(Kerberos) SASL 메커니즘을 지원해야 합니다.
  - LDAP 서버에는 DNS 서버에 설정된 PTR 레코드와 DNS A/AAAA 레코드가 있어야 합니다.
  - Kerberos 서버는 DNS 서버에 SRV 레코드가 있어야 합니다.
- 시작 TLS 또는 LDAPS를 활성화하려면 다음 사항을 고려해야 합니다.
  - LDAPS 대신 Start TLS를 사용하는 것이 NetApp 모범 사례입니다.
  - LDAPS를 사용하는 경우 ONTAP 9.5 이상에서는 LDAP 서버에서 TLS 또는 SSL을 활성화해야 합니다. ONTAP 9.4~9.0에서는 SSL이 지원되지 않습니다.
  - 도메인에 인증서 서버가 이미 구성되어 있어야 합니다.
- ONTAP 9.5 이상에서 LDAP 조회 추적을 활성화하려면 다음 조건을 충족해야 합니다.
  - 두 도메인은 다음 신뢰 관계 중 하나로 구성해야 합니다.
    - 양방향
    - 원웨이 - 프라이머리(primary)가 추천 도메인을 신뢰하는 곳입니다
    - 부모-자식
  - DNS는 참조된 모든 서버 이름을 확인하도록 구성되어야 합니다.
  - '--bind-as-cifs-server'가 true로 설정된 경우 도메인 암호가 인증을 위해 동일해야 합니다.

LDAP 조회 추적에는 다음 구성이 지원되지 않습니다.

- 모든 ONTAP 버전:
- 관리 SVM의 LDAP 클라이언트
- ONTAP 9.8 및 이전 버전(9.9.1 이상에서 지원됨):
- LDAP 서명 및 봉인('-session-security' 옵션)
- 암호화된 TLS 연결('-use-start-tls' 옵션)
- LDAPS 포트 636을 통한 통신('-use-ldaps-for-ad-ldap' 옵션)

- ONTAP 9.11.1부터 를 사용할 수 있습니다 "ONTAP NFS SVM에 대한 nsswitch 인증을 위해 LDAP 빠른

바인딩을 사용합니다."

- SVM에서 LDAP 클라이언트를 구성할 때 LDAP 스키마를 입력해야 합니다.

  대부분의 경우 기본 ONTAP 스키마 중 하나가 적합합니다. 그러나 사용자 환경의 LDAP 스키마가 이러한 스키마와 다른 경우 LDAP 클라이언트를 생성하기 전에 ONTAP에 대한 새 LDAP 클라이언트 스키마를 만들어야 합니다. 사용자 환경의 요구 사항에 대해서는 LDAP 관리자에게 문의하십시오.

- 호스트 이름 확인에 LDAP를 사용하는 것은 지원되지 않습니다.

자세한 내용은 을 참조하십시오 "NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법".

ONTAP NFS SVM에 대한 **LDAP** 서명 및 봉인에 대해 알아보세요**.**

ONTAP 9부터는 AD(Active Directory) 서버에 대한 쿼리에 대해 LDAP 세션 보안을 사용하도록 서명과 봉인을 구성할 수 있습니다. SVM(스토리지 가상 시스템)의 NFS 서버 보안 설정을 LDAP 서버의 보안 설정에 맞게 구성해야 합니다.

서명은 비밀 키 기술을 사용하여 LDAP 페이로드 데이터의 무결성을 확인합니다. 봉인은 LDAP 페이로드 데이터를 암호화하여 중요한 정보를 일반 텍스트로 전송하지 않도록 합니다. LDAP 보안 수준_ 옵션은 LDAP 트래픽의 서명, 서명 및 봉인 여부를 나타냅니다. 기본값은 '없음'입니다. 테스트

SVM에서 '-session-security-for-ad-ldap' 옵션을 사용하여 SVM에서 SMB 트래픽에 대한 LDAP 서명 및 봉인을 사용할 수 있습니다.

ONTAP NFS SVM용 **LDAPS**에 대해 알아보세요

ONTAP가 LDAP 통신을 보호하는 방법에 대한 특정 용어와 개념을 이해해야 합니다. ONTAP는 Active Directory 통합 LDAP 서버 또는 UNIX 기반 LDAP 서버 간에 인증된 세션을 설정하기 위해 시작 TLS 또는 LDAPS를 사용할 수 있습니다.

용어

ONTAP에서 LDAPS를 사용하여 LDAP 통신을 보호하는 방법에 대해 이해해야 하는 특정 용어가 있습니다.

- * LDAP *

  (Lightweight Directory Access Protocol) 정보 디렉터리에 액세스하고 관리하는 프로토콜입니다. LDAP는 사용자, 그룹 및 넷그룹과 같은 객체를 저장하기 위한 정보 디렉토리로 사용됩니다. 또한 LDAP는 이러한 객체를 관리하고 LDAP 클라이언트의 LDAP 요청을 처리하는 디렉토리 서비스를 제공합니다.

- SSL *

  (Secure Sockets Layer) 인터넷을 통해 정보를 안전하게 전송하기 위해 개발된 프로토콜입니다. SSL은 ONTAP 9 이상에서 지원되지만 TLS 사용을 위해 더 이상 사용되지 않습니다.

- * TLS *

  (전송 계층 보안) IETF 표준 트랙 프로토콜로서 이전 SSL 사양에 기초합니다. SSL의 후속 제품입니다. TLS는 ONTAP 9.5 이상에서 지원됩니다.

- * LDAPS(SSL 또는 TLS를 통한 LDAP) *

LDAP 클라이언트와 LDAP 서버 간의 보안 통신을 위해 TLS 또는 SSL을 사용하는 프로토콜입니다. SSL을 통한 _LDAP_와 TLS를 통한 _LDAP_라는 용어는 서로 바꿔 사용되기도 합니다. LDAPS는 ONTAP 9.5 이상에서 지원됩니다.

- ONTAP 9.8-9.5에서는 LDAPS를 포트 636에서만 활성화할 수 있습니다. 그렇게 하려면 다음을 사용하세요. `-use-ldaps-for-ad-ldap` 매개변수를 사용하여 `vserver cifs security modify` 명령.
- ONTAP 9.9.1부터 포트 636이 기본값으로 유지되지만 LDAPS는 모든 포트에서 활성화할 수 있습니다. 이렇게 하려면 `-ldaps-enabled` 매개 변수를 로 `true` 설정하고 원하는 `-port` 매개 변수를 지정합니다. 에 대한 자세한 내용은 `vserver services name-service ldap client create` "ONTAP 명령 참조입니다"을 참조하십시오.

LDAPS 대신 Start TLS를 사용하는 것이 NetApp 모범 사례입니다.

- * TLS * 를 시작합니다

(*start_tls*, *STARTTLS* 및 *StartTLS* 라고도 함) TLS 프로토콜을 사용하여 보안 통신을 제공하는 메커니즘입니다.

ONTAP는 LDAP 통신 보안을 위해 STARTTLS를 사용하며 기본 LDAP 포트(389)를 사용하여 LDAP 서버와 통신합니다. LDAP 서버는 LDAP 포트 389를 통한 연결을 허용하도록 구성해야 합니다. 그렇지 않으면 SVM에서 LDAP 서버로의 LDAP TLS 연결이 실패합니다.

ONTAP에서 **LDAPS**를 사용하는 방법

ONTAP는 TLS 서버 인증을 지원하므로 SVM LDAP 클라이언트가 바인딩 작업 중에 LDAP 서버의 ID를 확인할 수 있습니다. TLS를 사용하는 LDAP 클라이언트는 공용 키 암호화의 표준 기술을 사용하여 서버의 인증서와 공용 ID가 유효하며 클라이언트의 신뢰할 수 있는 CA 목록에 나열된 CA(인증 기관)에서 발급되었는지 확인할 수 있습니다.

LDAP는 TLS를 사용하여 통신을 암호화하는 STARTTLS를 지원합니다. STARTTLS는 표준 LDAP 포트(389)를 통한 일반 텍스트 연결로 시작되고 해당 연결은 TLS로 업그레이드됩니다.

ONTAP는 다음을 지원합니다.

- Active Directory 통합 LDAP 서버와 SVM 간의 SMB 관련 트래픽을 위한 LDAPS
- 이름 매핑 및 기타 UNIX 정보를 위한 LDAP 트래픽용 LDAPS

  Active Directory 통합 LDAP 서버 또는 UNIX 기반 LDAP 서버를 사용하여 LDAP 이름 매핑과 사용자, 그룹 및 넷그룹과 같은 기타 UNIX 정보에 대한 정보를 저장할 수 있습니다.

- 자체 서명된 루트 CA 인증서

  Active-Directory 통합 LDAP를 사용하는 경우 도메인에 Windows Server 인증서 서비스가 설치될 때 자체 서명된 루트 인증서가 생성됩니다. LDAP 이름 매핑에 UNIX 기반 LDAP 서버를 사용하는 경우 자체 서명된 루트 인증서는 해당 LDAP 애플리케이션에 적합한 방법을 사용하여 생성 및 저장됩니다.

기본적으로 LDAPS는 비활성화되어 있습니다.

ONTAP NFS SVM에 대한 **LDAP RFC2307bis** 지원 활성화

LDAP를 사용하고 중첩된 그룹 구성원을 사용하는 추가 기능이 필요한 경우 ONTAP를 구성하여 LDAP RFC2307bis 지원을 활성화할 수 있습니다.

시작하기 전에

사용할 기본 LDAP 클라이언트 스키마 중 하나의 복사본을 만들어야 합니다.

이 작업에 대해

LDAP 클라이언트 스키마에서 그룹 개체는 memberUid 특성을 사용합니다. 이 속성은 여러 값을 포함할 수 있으며 해당 그룹에 속한 사용자의 이름을 나열합니다. RFC2307bis가 활성화된 LDAP 클라이언트 스키마에서 그룹 객체는 uniqueMember 속성을 사용합니다. 이 속성은 LDAP 디렉토리에 있는 다른 개체의 전체 DN(고유 이름)을 포함할 수 있습니다. 이렇게 하면 그룹이 다른 그룹을 구성원으로 포함할 수 있으므로 중첩된 그룹을 사용할 수 있습니다.

사용자는 중첩된 그룹을 포함하여 256개 이상의 그룹의 구성원이 아니어야 합니다. ONTAP는 256 그룹 제한을 초과하는 모든 그룹을 무시합니다.

기본적으로 RFC2307bis 지원은 비활성화되어 있습니다.

RFC2307bis 지원은 MS-AD-BIS 스키마를 사용하여 LDAP 클라이언트를 생성할 때 ONTAP에서 자동으로 활성화됩니다.

자세한 내용은 을 참조하십시오 "NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법".

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. RFC2307 LDAP 클라이언트 스키마를 수정하여 RFC2307bis 지원을 활성화합니다.

   'vserver services name-service ldap client schema modify -vserver vserver_name -schema schema -name -enable -rfc2307bis true'

3. LDAP 서버에서 지원되는 객체 클래스와 일치하도록 스키마를 수정합니다.

   'vserver services name-service ldap client schema modify -vserver vserver -name -schema schema_name -group-of-unique-names-object-class object_class'

4. LDAP 서버에서 지원되는 속성 이름과 일치하도록 스키마를 수정합니다.

   'vserver services name-service ldap client schema modify -vserver vserver -name -schema schema_name -unique-member-attribute attribute_name'

5. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

LDAP 디렉토리 검색을 위한 **ONTAP NFS** 구성 옵션

사용자, 그룹 및 넷그룹 정보를 포함한 LDAP 디렉토리 검색을 최적화하려면 ONTAP LDAP 클라이언트가 사용자 환경에 가장 적합한 방식으로 LDAP 서버에 접속하도록 구성해야 합니다. 기본 LDAP 기본 및 범위 검색 값이 충분하면 사용자 지정 값이 더 적합한 시기를 지정하는 매개 변수가 무엇인지 이해해야 합니다.

사용자, 그룹 및 넷그룹 정보에 대한 LDAP 클라이언트 검색 옵션을 사용하면 LDAP 쿼리가 실패하여 스토리지 시스템에 대한 클라이언트 액세스가 실패하는 것을 방지할 수 있습니다. 또한 클라이언트 성능 문제를 방지하기 위해 가능한 한 효율적으로 검색을 수행할 수 있습니다.

기본 및 범위 검색 값입니다

LDAP 베이스는 LDAP 클라이언트가 LDAP 쿼리를 수행하는 데 사용하는 기본 DN입니다. 사용자, 그룹 및 넷그룹 검색을 포함한 모든 검색은 기본 DN을 사용하여 수행됩니다. 이 옵션은 LDAP 디렉토리가 상대적으로 작고 모든 관련 항목이 동일한 DN에 있을 때 적합합니다.

사용자 지정 기본 DN을 지정하지 않으면 기본값은 "root"입니다. 즉, 각 쿼리는 전체 디렉터리를 검색합니다. 이렇게 하면 LDAP 쿼리의 성공 가능성이 최대화되지만 비효율적이며 대규모 LDAP 디렉토리의 성능이 크게 저하될 수 있습니다.

LDAP 기본 범위는 LDAP 클라이언트가 LDAP 쿼리를 수행하는 데 사용하는 기본 검색 범위입니다. 사용자, 그룹 및 넷그룹 검색을 포함한 모든 검색은 기본 범위를 사용하여 수행됩니다. LDAP 쿼리가 명명된 항목만 검색할지, DN 아래의 항목 하나 또는 DN 아래의 전체 하위 트리를 검색할지 여부를 결정합니다.

사용자 지정 기본 범위를 지정하지 않으면 기본값은 'Subtree'입니다. 즉, 각 쿼리는 DN 아래의 전체 하위 트리를 검색합니다. 이렇게 하면 LDAP 쿼리의 성공 가능성이 최대화되지만 비효율적이며 대규모 LDAP 디렉토리의 성능이 크게 저하될 수 있습니다.

사용자 지정 기준 및 범위 검색 값

필요에 따라 사용자, 그룹 및 넷그룹 검색에 대해 별도의 기본 값과 범위 값을 지정할 수 있습니다. 이러한 방식으로 검색 기준 및 쿼리 범위를 제한하면 LDAP 디렉토리의 하위 섹션으로 검색이 제한되므로 성능이 크게 향상됩니다.

사용자 지정 기준 및 범위 값을 지정하면 사용자, 그룹 및 넷그룹 검색에 대한 일반 기본 검색 기준 및 범위가 재정의됩니다. 사용자 지정 기준 및 범위 값을 지정하는 매개 변수는 고급 권한 수준에서 사용할 수 있습니다.

LDAP 클라이언트 매개 변수…	사용자 지정…
'-base-dn'	모든 LDAP 검색에 대한 기본 DN입니다. 필요한 경우 여러 값을 입력할 수 있습니다(예: ONTAP 9.5 이상 릴리스에서 LDAP 참조 추적이 활성화된 경우).
``기본범위''	모든 LDAP 검색에 대한 기본 범위입니다.
'-user-dn'	모든 LDAP 사용자 검색에 대한 기본 DN입니다. 이 매개변수는 사용자 이름 매핑 검색에도 적용됩니다.
'- 사용자 범위'	모든 LDAP 사용자 검색의 기본 범위입니다. 이 매개변수는 사용자 이름 매핑 검색에도 적용됩니다.
``그룹-dn''	모든 LDAP 그룹 검색에 대한 기본 DN입니다.
그룹-범위	모든 LDAP 그룹 검색에 대한 기본 범위입니다.
'-넷그룹-dn'	모든 LDAP 넷그룹 검색에 대한 기본 DN입니다.

넷그룹 범위	모든 LDAP 넷그룹 검색에 대한 기본 범위입니다.

여러 사용자 정의 기본 **DN** 값

LDAP 디렉토리 구조가 더 복잡한 경우 여러 기본 DNS를 지정하여 LDAP 디렉토리의 여러 부분을 검색하여 특정 정보를 검색해야 할 수 있습니다. 사용자, 그룹 및 넷그룹 DN 매개 변수에 대해 여러 DNS를 지정할 수 있습니다. 이를 세미콜론(;)으로 분리하고 전체 DN 검색 목록을 큰따옴표(")로 둘러싸서 지정할 수 있습니다. DN에 세미콜론이 포함된 경우 DN의 세미콜론 바로 앞에 이스케이프 문자(\)를 추가해야 합니다.

범위는 해당 매개 변수에 지정된 DNS의 전체 목록에 적용됩니다. 예를 들어 사용자 범위에 대해 서로 다른 세 개의 사용자 DNS 및 하위 트리의 목록을 지정하면 LDAP 사용자는 지정된 세 DNS에 대해 전체 하위 트리를 검색합니다.

ONTAP 9.5부터 LDAP 조회 응답이 기본 LDAP 서버에서 반환되지 않는 경우 ONTAP LDAP 클라이언트가 다른 LDAP 서버에 조회 요청을 참조할 수 있도록 LDAP_READIAL DIADIGING_을 지정할 수도 있습니다. 클라이언트는 추천 데이터를 사용하여 추천 데이터에 설명된 서버에서 대상 객체를 검색합니다. 참조된 LDAP 서버에 있는 객체를 검색하려면, LDAP 클라이언트 구성의 일부로 참조된 객체의 base-dn을 base-dn에 추가할 수 있습니다. 그러나 LDAP 클라이언트 생성 또는 수정 중에 참조 추격이 활성화('-referral-enabled true' 옵션 사용)된 경우에만 참조 객체가 조회됩니다.

사용자 지정 **LDAP** 검색 필터

LDAP 구성 옵션 매개 변수를 사용하여 사용자 지정 검색 필터를 생성할 수 있습니다. `-group-membership-filter`매개 변수는 LDAP 서버에서 그룹 구성원 자격을 조회할 때 사용할 검색 필터를 지정합니다.

유효한 필터의 예는 다음과 같습니다.

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

에 대해 자세히 "ONTAP에서 LDAP를 구성하는 방법"알아보십시오.

ONTAP NFS SVM에 대한 **LDAP** 디렉토리 **netgroup-by-host** 검색 성능 향상

LDAP 환경이 호스트별 넷그룹 검색을 허용하도록 구성된 경우 ONTAP를 구성하여 이를 활용하고 호스트별 넷그룹 검색을 수행할 수 있습니다. 따라서 넷그룹 검색 속도를 크게 높이고 넷그룹 검색 중 대기 시간으로 인해 발생할 수 있는 NFS 클라이언트 액세스 문제를 줄일 수 있습니다.

시작하기 전에

LDAP 디렉토리에는 netgroup.byhost 맵이 포함되어야 합니다.

DNS 서버에는 NFS 클라이언트에 대한 정방향(A) 및 역방향(PTR) 조회 레코드가 모두 포함되어야 합니다.

넷그룹에 IPv6 주소를 지정할 때는 RFC 5952에 지정된 대로 항상 각 주소를 줄이고 압축해야 합니다.

이 작업에 대해

NIS 서버는 넷그룹, 넷그룹, byuser, netgroup.byhost라는 세 개의 개별 맵에 넷그룹 정보를 저장합니다. 넷그룹 byuser와 netgroup.byhost 맵의 목적은 넷그룹 검색 속도를 높이는 것입니다. ONTAP는 NIS 서버에서 호스트 별로 넷그룹 검색을 수행하여 마운트 응답 시간을 향상시킬 수 있습니다.

기본적으로 LDAP 디렉토리에는 NIS 서버와 같은 netgroup.byhost 맵이 없습니다. 하지만 타사 툴을 사용하여 NIS 넷그룹을 LDAP 디렉토리에 가져올 수도 있습니다. byhost 맵을 LDAP 디렉토리에 가져와서 빠르게 넷그룹을 통한 호스트 간 검색을 수행할 수 있습니다. 호스트 별로 넷그룹을 검색할 수 있도록 LDAP 환경을 구성한 경우 netgroup.byhost의 맵 이름, DN 및 검색 범위를 사용하여 ONTAP LDAP 클라이언트를 구성하여 더 빠른 호스트 기준 넷그룹을 검색할 수 있습니다.

Netgroup-by-host 검색에 대한 결과를 더 빨리 수신하면 NFS 클라이언트가 내보내기에 대한 액세스를 요청할 때 ONTAP에서 엑스포트 규칙을 더 빠르게 처리할 수 있습니다. 따라서 넷그룹 검색 지연 문제로 인해 액세스가 지연될 가능성이 줄어듭니다.

단계

1. LDAP 디렉토리로 가져온 NIS 넷그룹 byhost 맵의 정확한 전체 고유 이름을 가져옵니다.

   지도 DN은 가져오기에 사용한 타사 도구에 따라 다를 수 있습니다. 최상의 성능을 얻으려면 정확한 맵 DN을 지정해야 합니다.

2. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다

3. 스토리지 가상 시스템(SVM)의 LDAP 클라이언트 구성에서 Netgroup-by-host 검색을 설정합니다. 'vserver services name-service LDAP client modify -vserver vserver_name -client -config config config_name -is -netgroup-byhost-enabled true-netgroup-byhost-dn netgroup-by-host_map_ninggroup-byhost-scope netgroup-by-host_search_scope

   `-is-netgroup-byhost-enabled '{'true'|'false'}LDAP 디렉토리에 대한 호스트 별 넷그룹 검색을 설정하거나 해제합니다. 기본값은 false 입니다.

   dnetgroup-byhost-dn dnetgroup-by-host_map_ninged_name은 LDAP 디렉토리에 있는 netgroup.byhost 맵의 고유 이름을 지정합니다. 넷그룹별 검색에 대한 기본 DN을 재정의합니다. 이 매개 변수를 지정하지 않으면 ONTAP에서는 기본 DN을 대신 사용합니다.

   `-netgroup-byhost-scope '{'base'|'onelel'|'ubtree'}는 넷그룹-호스트 검색 범위를 지정합니다. 이 매개변수를 지정하지 않으면 기본값은 'Subtree'입니다.

   LDAP 클라이언트 구성이 아직 없는 경우 'vserver services name-service ldap client create' 명령을 사용하여 새 LDAP 클라이언트 구성을 생성할 때 이러한 매개 변수를 지정하여 Netgroup-by-host 검색을 설정할 수 있습니다.

   > 그만큼 `-ldap-servers` 필드는 다음을 대체합니다. `-servers` 필드입니다. 다음을 사용할 수 있습니다. `-ldap-servers` LDAP 서버의 호스트 이름이나 IP 주소를 지정하는 필드입니다.

4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 명령을 실행하면 이름이 netgroup.byhost 맵 ""nisMapName="netgroup.byhost", dc=corp, dc=example, dc=com" 및 기본 검색 범위 'subtree'를 사용하여 넷그룹을 호스트별로 검색할 수 있도록 이름이 ""ldap_corp""인 기존 LDAP 클라이언트 구성이 수정됩니다.

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

작업을 마친 후

클라이언트 액세스 문제를 방지하려면 디렉토리의 netgroup.byhost 및 netgroup 맵을 항상 동기화해야 합니다.

관련 정보

"IETF RFC 5952: IPv6 주소 텍스트 표현에 대한 권장 사항입니다"

ONTAP NFS SVM에 대한 **nsswitch** 인증을 위해 **LDAP** 빠른 바인딩을 사용합니다**.**

ONTAP 9.11.1부터는 LDAP_Fast BIND_FUNGION(*CONNEC*동시 바인드)을 활용하여 클라이언트 인증 요청을 더 빠르고 간편하게 수행할 수 있습니다. 이 기능을 사용하려면 LDAP 서버가 빠른 바인딩 기능을 지원해야 합니다.

이 작업에 대해

빠른 바인딩이 없으면 ONTAP는 LDAP 단순 바인드를 사용하여 LDAP 서버에서 관리자 사용자를 인증합니다. 이 인증 방법을 사용하면 ONTAP에서 사용자 또는 그룹 이름을 LDAP 서버로 보내고, 저장된 해시 암호를 받고, 서버 해시 코드를 사용자 암호에서 로컬로 생성된 해시 암호와 비교합니다. 동일한 경우 ONTAP는 로그인 권한을 부여합니다.

빠른 바인딩 기능을 사용하면 ONTAP는 보안 연결을 통해 사용자 자격 증명(사용자 이름 및 암호)만 LDAP 서버로 전송합니다. 그런 다음 LDAP 서버가 이러한 자격 증명을 검증하고 ONTAP에 로그인 권한을 부여하도록 지시합니다.

빠른 바인딩의 한 가지 장점은 LDAP 서버에서 암호 해싱이 수행되기 때문에 ONTAP가 LDAP 서버에서 지원하는 모든 새로운 해싱 알고리즘을 지원할 필요가 없다는 것입니다.

"빠른 바인딩 사용에 대해 알아보십시오."

시작하기 전에

LDAP 고속 바인딩에 기존 LDAP 클라이언트 구성을 사용할 수 있습니다. 그러나 LDAP 클라이언트를 TLS 또는 LDAPS용으로 구성하는 것이 좋습니다. 그렇지 않으면 암호를 일반 텍스트로 유선으로 보냅니다.

ONTAP 환경에서 LDAP 고속 바인딩을 사용하려면 다음 요구 사항을 충족해야 합니다.

- ONTAP admin 사용자는 빠른 바인딩을 지원하는 LDAP 서버에 구성해야 합니다.
- ONTAP SVM은 이름 서비스 스위치(nsswitch) 데이터베이스에서 LDAP에 대해 구성해야 합니다.
- ONTAP admin 사용자 및 그룹 계정은 빠른 바인딩을 사용하여 nsswitch 인증에 맞게 구성해야 합니다.
- 빠른 바인딩이 성공하려면 관리자의 UID 번호와 GID 번호가 입력되어 있고 조회 가능해야 합니다.

단계

1. LDAP 관리자에게 LDAP 서버에서 LDAP 고속 바인딩이 지원되는지 확인하십시오.
2. ONTAP 관리자 사용자 자격 증명이 LDAP 서버에 구성되어 있는지 확인합니다.
3. LDAP 고속 바인딩에 대해 admin 또는 data SVM이 올바르게 구성되었는지 확인합니다.
    a. LDAP 빠른 바인딩 서버가 LDAP 클라이언트 구성에 나열되는지 확인하려면 다음을 입력합니다.

        'vserver services name-service ldap client show'

        "LDAP 클라이언트 구성에 대해 자세히 알아보십시오."

    b. LDAP가 nsswitch 'passwd' 데이터베이스에 대해 구성된 소스 중 하나인지 확인하려면 다음을 입력합니다.

'vserver services name-service ns-switch show'

"nsswitch 구성에 대해 알아봅니다."

4. admin 사용자가 nsswitch를 사용하여 인증하는지, 그리고 계정에서 LDAP 빠른 바인딩 인증이 활성화되어 있는지 확인합니다.

   ◦ 기존 사용자의 경우 '보안 로그인 수정'을 입력하고 다음 파라미터 설정을 확인합니다.

   '-authentication-method nsswitch'

   '-is-ldap-fastbind true'

   에 대한 자세한 내용은 `security login modify` "ONTAP 명령 참조입니다"을 참조하십시오.

   ◦ 새 관리자는 를 참조하십시오"LDAP 또는 NIS ONTAP 계정 액세스를 설정합니다".

ONTAP NFS SVM에 대한 **LDAP** 통계 표시

스토리지 시스템의 스토리지 가상 머신(SVM)에 대한 LDAP 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

시작하기 전에

- SVM에서 LDAP 클라이언트를 구성해야 합니다.
- 데이터를 볼 수 있는 LDAP 객체를 식별해야 합니다.

단계

1. 카운터 객체에 대한 성능 데이터 보기:

   '스타티틱스 쇼'

예

다음 예제에서는 카운터에 대해 * smpl_1 * 이라는 샘플의 통계를 표시합니다. avg_processor_busy 및 cpu_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

관련 정보

- "통계에 따르면"
- "통계 시작"
- "통계 중지"

이름 매핑을 구성합니다

ONTAP NAS SVM에 대한 이름 매핑 구성에 대해 알아보세요**.**

ONTAP는 이름 매핑을 사용하여 SMB ID를 UNIX ID에 매핑하고, Kerberos ID를 UNIX ID에 매핑하며, UNIX ID를 SMB ID에 매핑합니다. 사용자 자격 증명을 얻고 NFS 클라이언트나 SMB 클라이언트에서 연결 중인지 여부와 관계없이 적절한 파일 액세스를 제공하려면 이 정보가 필요합니다.

이름 매핑을 사용할 필요가 없는 두 가지 예외가 있습니다.

- 순수 UNIX 환경을 구성하고 볼륨에 SMB 액세스 또는 NTFS 보안 스타일을 사용하지 않을 계획입니다.
- 대신 사용할 기본 사용자를 구성합니다.

  이 시나리오에서는 모든 개별 클라이언트 자격 증명을 매핑하지 않고 모든 클라이언트 자격 증명이 동일한 기본 사용자에게 매핑되기 때문에 이름 매핑이 필요하지 않습니다.

사용자 이름 매핑만 사용할 수 있으며 그룹에서는 사용할 수 없습니다.

그러나 개별 사용자 그룹을 특정 사용자에게 매핑할 수 있습니다. 예를 들어, 영업이라는 단어가 있는 모든 AD 사용자를 특정 UNIX 사용자 및 사용자의 UID에 매핑할 수 있습니다.

ONTAP NAS SVM에 대한 이름 매핑에 대해 알아보세요

ONTAP에서 사용자에 대한 자격 증명을 매핑해야 하는 경우 먼저 로컬 이름 매핑 데이터베이스와 LDAP 서버에서 기존 매핑을 확인합니다. SVM의 네임 서비스 구성에 따라 1개 또는 2개 모두를 검사할지 여부를 결정합니다.

- Windows에서 UNIX로의 매핑의 경우

  매핑을 찾을 수 없는 경우 ONTAP는 소문자 Windows 사용자 이름이 UNIX 도메인의 유효한 사용자 이름인지 확인합니다. 이렇게 해도 문제가 해결되지 않으면 기본 UNIX 사용자를 사용합니다(구성된 경우). 기본 UNIX 사용자가 구성되어 있지 않고 ONTAP가 이러한 방식으로 매핑을 얻을 수 없는 경우 매핑이 실패하고 오류가 반환됩니다.

- UNIX에서 Windows로의 매핑의 경우

  매핑을 찾을 수 없는 경우 ONTAP는 SMB 도메인의 UNIX 이름과 일치하는 Windows 계정을 찾으려고 시도합니다. 이 기능이 작동하지 않으면 기본 SMB 사용자를 사용합니다(구성된 경우). 기본 SMB 사용자가 구성되어 있지 않고 ONTAP가 이러한 방식으로 매핑을 얻을 수 없는 경우 매핑이 실패하고 오류가 반환됩니다.

컴퓨터 계정은 기본적으로 지정된 기본 UNIX 사용자에게 매핑됩니다. 기본 UNIX 사용자를 지정하지 않으면 컴퓨터 계정 매핑이 실패합니다.

- ONTAP 9.5부터 기본 UNIX 사용자가 아닌 다른 사용자에게 시스템 계정을 매핑할 수 있습니다.
- ONTAP 9.4 이하 버전에서는 시스템 계정을 다른 사용자에게 매핑할 수 없습니다.

  컴퓨터 계정에 대한 이름 매핑이 정의되어 있더라도 매핑은 무시됩니다.

ONTAP NAS SVM에서 **UNIX-Windows** 사용자 이름 매핑을 위한 다중 도메인 검색

ONTAP는 UNIX 사용자를 Windows 사용자에게 매핑할 때 다중 도메인 검색을 지원합니다. 일치하는 결과가 반환될 때까지 검색된 모든 신뢰할 수 있는 도메인이 대체 패턴과 일치하는 항목을 검색합니다. 또는 검색된 신뢰할 수 있는 도메인 목록 대신 사용되는 기본 신뢰할 수 있는 도메인 목록을 구성할 수 있으며 일치하는 결과가 반환될 때까지 순서대로 검색됩니다.

도메인 트러스트가 **UNIX** 사용자에게 **Windows** 사용자 이름 매핑 검색에 미치는 영향

다중 도메인 사용자 이름 매핑의 작동 방식을 이해하려면 ONTAP에서 도메인 트러스트가 작동하는 방식을 이해해야 합니다. SMB 서버의 홈 도메인과의 Active Directory 트러스트 관계는 양방향 신뢰일 수도 있고 인바운드 신뢰나 아웃바운드 트러스트를 포함한 두 가지 단방향 트러스트 유형 중 하나일 수도 있습니다. 홈 도메인은 SVM의 SMB 서버가 속하는 도메인입니다.

- _양방향 트러스트 _

  양방향 트러스트를 사용하면 두 도메인이 서로 신뢰합니다. SMB 서버의 홈 도메인에 다른 도메인과의 양방향 트러스트가 있는 경우 홈 도메인이 신뢰할 수 있는 도메인에 속한 사용자를 인증하고 권한을 부여할 수 있으며 그 반대의 경우도 마찬가지입니다.

  UNIX 사용자 대 Windows 사용자 이름 매핑 검색은 홈 도메인과 다른 도메인 간의 양방향 트러스트가 있는 도메인에서만 수행할 수 있습니다.

- _아웃바운드 트러스트 _

  아웃바운드 트러스트를 사용하면 홈 도메인이 다른 도메인을 신뢰합니다. 이 경우 홈 도메인이 아웃바운드 신뢰할 수 있는 도메인에 속하는 사용자를 인증하고 권한을 부여할 수 있습니다.

  UNIX 사용자 대 Windows 사용자 이름 매핑 검색을 수행할 때 홈 도메인의 아웃바운드 트러스트가 _not_sunfre검색되었습니다.

- _ 인바운드 신뢰 _

  인바운드 트러스트를 사용하면 다른 도메인이 SMB 서버의 홈 도메인을 신뢰합니다. 이 경우 홈 도메인은 인바운드 신뢰할 수 있는 도메인에 속하는 사용자를 인증하거나 승인할 수 없습니다.

  UNIX 사용자 대 Windows 사용자 이름 매핑 검색을 수행할 때 홈 도메인의 인바운드 트러스트가 _not_sound입니다.

이름 매핑에 대한 다중 도메인 검색을 구성하는 데 와일드카드**(*)**를 사용하는 방법

다중 도메인 이름 매핑 검색은 Windows 사용자 이름의 도메인 섹션에서 와일드카드를 사용하여 쉽게 수행할 수 있습니다. 다음 표에서는 이름 매핑 항목의 도메인 부분에서 와일드카드를 사용하여 다중 도메인 검색을 사용하는 방법을 보여 줍니다.

패턴	교체	결과
루트	* {백슬래시} {백슬래시} 관리자	UNIX 사용자 "root"는 "administrator"라는 사용자에게 매핑됩니다. "administrator"라는 이름의 첫 번째 일치하는 사용자를 찾을 때까지 모든 신뢰할 수 있는 도메인을 순서대로 검색합니다.
*	* {백슬래시} {백슬래시} *	유효한 UNIX 사용자는 해당 Windows 사용자에게 매핑됩니다. 모든 신뢰할 수 있는 도메인은 해당 이름을 가진 첫 번째 일치하는 사용자를 찾을 때까지 순서대로 검색됩니다. * {백슬래시} { 백슬래시} * 패턴은 UNIX에서 Windows로의 이름 매핑에만 유효하며 다른 방법으로는 사용할 수 없습니다.

다중 도메인 이름 검색 수행 방법

다음 두 가지 방법 중 하나를 선택하여 다중 도메인 이름 검색에 사용되는 신뢰할 수 있는 도메인 목록을 확인할 수 있습니다.

- ONTAP에서 컴파일한 자동으로 검색된 양방향 트러스트 목록을 사용합니다
- 컴파일하는 신뢰할 수 있는 기본 도메인 목록을 사용합니다

UNIX 사용자가 사용자 이름의 도메인 섹션에 와일드카드를 사용하여 Windows 사용자에게 매핑된 경우 Windows 사용자는 다음과 같이 모든 신뢰할 수 있는 도메인에서 찾을 수 있습니다.

- 선호하는 트러스트된 도메인 목록이 구성되어 있으면 매핑된 Windows 사용자는 이 검색 목록에서만 순서대로 검색됩니다.
- 신뢰할 수 있는 도메인의 기본 설정 목록이 구성되어 있지 않으면 홈 도메인의 모든 양방향 신뢰할 수 있는 도메인에서 Windows 사용자가 표시됩니다.
- 홈 도메인에 대해 양방향으로 신뢰할 수 있는 도메인이 없는 경우 사용자는 홈 도메인에서 표시됩니다.

UNIX 사용자가 사용자 이름의 도메인 섹션이 없는 Windows 사용자에게 매핑된 경우 Windows 사용자는 홈 도메인에서 찾을 수 있습니다.

ONTAP NAS SVM에 대한 이름 매핑 변환 규칙

ONTAP 시스템은 각 SVM에 대해 일련의 전환 규칙을 유지합니다. 각 규칙은 A_pattern_과 A_replacement_의 두 부분으로 구성됩니다. 변환은 적절한 목록의 시작 부분에서 시작하여 첫 번째 일치 규칙을 기반으로 대체를 수행합니다. 이 패턴은 UNIX 형식의 정규식입니다. 대체는 UNIX 'ed' 프로그램과 마찬가지로 패턴에서 부분식을 나타내는 이스케이프 시퀀스를 포함하는 문자열입니다.

ONTAP NAS SVM에 대한 이름 매핑 만들기

'vserver name-mapping create' 명령을 사용하여 이름 매핑을 생성할 수 있습니다. 이름 매핑을 사용하여 Windows 사용자가 UNIX 보안 스타일 볼륨에 액세스하고 그 반대로 액세스할 수 있습니다.

이 작업에 대해

각 SVM에서 ONTAP은 각 방향에 대해 최대 12,500개의 이름 매핑을 지원합니다.

단계

1. 이름 매핑 생성:

   'vserver name-mapping create-vserver vserver_name-direction{KRB-unix|win-unix|unix-win} - position integer-pattern text-replacement text'

   > ⓘ `-pattern`및 `-replacement` 문은 정규식으로 공식화할 수 있습니다. 또한 이 문을 사용하여 `null` 대체 문자열(공백 문자)을 사용하여 사용자에 대한 매핑을 명시적으로 거부할 `" "` 수도 `-replacement` 있습니다. 에 대한 자세한 내용은 `vserver name-mapping create` link:https://docs.netapp.com/us-en/ontap-cli/vserver-name-mapping-create.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

   Windows와 UNIX 간 매핑이 생성될 때 새 매핑이 생성될 때 ONTAP 시스템에 대한 열린 연결이 있는 모든 SMB

클라이언트는 로그아웃했다가 다시 로그인하여 새 매핑을 확인해야 합니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM에 이름 매핑이 생성됩니다. 매핑은 우선 순위 목록의 위치 1에서 UNIX에서 Windows로의 매핑입니다. 매핑은 UNIX 사용자 johnd를 Windows 사용자 ENG\JohnnDoe에 매핑합니다.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

다음 명령을 실행하면 이름이 VS1 인 SVM에 또 다른 이름 매핑이 생성됩니다. 매핑은 우선 순위 목록의 위치 1에서 Windows에서 UNIX로의 매핑입니다. 여기에는 정규식이 포함됩니다. 매핑은 SVM과 연결된 LDAP 도메인의 사용자에게 도메인 ENG의 모든 CIFS 사용자를 매핑합니다.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

다음 명령을 실행하면 이름이 VS1 인 SVM에 또 다른 이름 매핑이 생성됩니다. 이 패턴에는 이스케이프해야 하는 Windows 사용자 이름의 요소로 ""$"가 포함됩니다. 매핑은 Windows 사용자 ENG\John$ops를 UNIX 사용자 John_ops에 매핑합니다.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

ONTAP NAS SVM의 기본 사용자 구성

사용자의 다른 모든 매핑 시도가 실패하거나 UNIX와 Windows 간에 개별 사용자를 매핑하지 않으려는 경우 사용할 기본 사용자를 구성할 수 있습니다. 또는 매핑되지 않은 사용자의 인증에 실패하도록 하려면 기본 사용자를 구성하지 않아야 합니다.

이 작업에 대해

CIFS 인증의 경우 각 Windows 사용자를 개별 UNIX 사용자에게 매핑하지 않으려면 대신 기본 UNIX 사용자를 지정할 수 있습니다.

NFS 인증의 경우 각 UNIX 사용자를 개별 Windows 사용자에게 매핑하지 않으려면 대신 기본 Windows 사용자를 지정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다…

기본 UNIX 사용자를 구성합니다	'vserver cifs options modify-default-unix-user user_name'을 선택합니다
기본 Windows 사용자를 구성합니다	'vserver nfs modify-default-win-user user_name'을 선택합니다

NFS 이름 매핑을 관리하기 위한 **ONTAP** 명령

이름 매핑을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
이름 매핑을 생성합니다	`vserver name-mapping create`
특정 위치에 이름 매핑을 삽입합니다	`vserver name-mapping insert`
이름 매핑을 표시합니다	`vserver name-mapping show`
두 이름 매핑의 위치를 교환합니다. 참고: 이름 매핑이 IP 한정자 항목으로 구성된 경우에는 스왑이 허용되지 않습니다.	`vserver name-mapping swap`
이름 매핑을 수정합니다	`vserver name-mapping modify`
이름 매핑을 삭제합니다	`vserver name-mapping delete`
올바른 이름 매핑을 확인합니다	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

에 대한 자세한 내용은 `vserver name-mapping` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SVM에 대한 **Windows NFS** 클라이언트의 액세스 활성화

ONTAP는 Windows NFSv3 클라이언트에서 파일 액세스를 지원합니다. 즉, NFSv3을 지원하는 Windows 운영 체제를 실행하는 클라이언트가 클러스터의 NFSv3 내보내기에 있는 파일에 액세스할 수 있습니다. 이 기능을 성공적으로 사용하려면 SVM(스토리지 가상 시스템)을 올바르게 구성하고 특정 요구사항과 제한사항을 숙지해야 합니다.

이 작업에 대해

기본적으로 Windows NFSv3 클라이언트 지원은 비활성화되어 있습니다.

시작하기 전에

SVM에서 NFSv3을 활성화해야 합니다.

단계

1. Windows NFSv3 클라이언트 지원 설정:

   `vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled`

2. Windows NFSv3 클라이언트를 지원하는 모든 SVM에서 를 사용하지 않도록 설정합니다 `-enable-ejukebox` 및 `-v3-connection-drop` 매개 변수:

   `vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection -drop disabled`

   이제 Windows NFSv3 클라이언트가 스토리지 시스템에 내보내기를 마운트할 수 있습니다.

3. 각 Windows NFSv3 클라이언트가 '-o mtype=hard' 옵션을 지정하여 하드 마운트를 사용하는지 확인합니다.

   이 작업은 안정적인 마운트를 보장하기 위해 필요합니다.

   mount-o mtype=hard\\10.53.33.10\vol\vol1 z:\"

ONTAP SVM에 대한 **NFS** 클라이언트에서 내보내기 표시 활성화

NFS 클라이언트는 'howmount -e' 명령을 사용하여 ONTAP NFS 서버에서 사용할 수 있는 내보내기 목록을 볼 수 있습니다. 이렇게 하면 마운트할 파일 시스템을 식별하는 데 도움이 됩니다.

ONTAP 사용하면 기본적으로 NFS 클라이언트가 내보내기 목록을 볼 수 있습니다. 이전 릴리즈에서는 `showmount` 명령의 옵션을 `vserver nfs modify` 명시적으로 설정해야 합니다. 엑스포트 목록을 보려면 SVM에서 NFSv3을 설정해야 합니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM의 showmount 기능이 표시됩니다.

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

NFS 클라이언트에서 실행된 다음 명령은 IP 주소가 10.63.21.9인 NFS 서버의 내보내기 목록을 표시합니다.

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

NFS를 사용하여 파일 액세스를 관리합니다

ONTAP SVM에 대해 NFSv3 활성화 또는 비활성화

'-v3' 옵션을 수정하여 NFSv3을 설정하거나 해제할 수 있습니다. 이렇게 하면 NFSv3 프로토콜을 사용하는 클라이언트에 대한 파일 액세스가 허용됩니다. 기본적으로 NFSv3은 설정되어 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력…
NFSv3을 사용하도록 설정합니다	'vserver NFS modify -vserver vserver_name -v3 enabled'
NFSv3을 사용하지 않도록 설정합니다	'vserver NFS modify -vserver vserver_name -v3 disabled'

ONTAP SVM에 대해 NFSv4.0 활성화 또는 비활성화

'-v4.0' 옵션을 수정하여 NFSv4.0을 설정하거나 해제할 수 있습니다. 이렇게 하면 NFSv4.0 프로토콜을 사용하는 클라이언트에 대한 파일 액세스가 허용됩니다. ONTAP 9.9.1에서는 NFSv4.0이 기본적으로 설정되어 있으며 이전 릴리즈에서는 기본적으로 사용되지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
NFSv4.0을 사용하도록 설정합니다	'vserver nfs modify -vserver vserver_name -v4.0 enabled'
NFSv4.0을 해제합니다	'vserver nfs modify -vserver vserver_name -v4.0 disabled'

ONTAP SVM에 대해 NFSv4.1 활성화 또는 비활성화

'-v4.1' 옵션을 수정하여 NFSv4.1을 설정 또는 해제할 수 있습니다. 따라서 NFSv4.1 프로토콜을 사용하여 클라이언트에 파일을 액세스할 수 있습니다. ONTAP 9.9.1에서는 NFSv4.1이 기본적으로 활성화되어 있지만 이전 릴리즈에서는 기본적으로 사용되지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
NFSv4.1을 활성화하십시오	'vserver nfs modify -vserver vserver_name -v4.1 enabled'
NFSv4.1을 비활성화하십시오	'vserver nfs modify -vserver vserver_name -v4.1 disabled'

ONTAP NFSv4 스토어풀 한도 관리

ONTAP 9.13부터 관리자는 NFSv4 서버가 클라이언트 저장소 풀 리소스 제한당 한도에 도달하면 NFSv4 클라이언트에 대한 리소스를 거부하도록 설정할 수 있습니다. 클라이언트가 NFSv4 저장소 풀 리소스를 너무 많이 사용하면 NFSv4 저장소 풀 리소스를 사용할 수 없어 다른 NFSv4 클라이언트가 차단될 수 있습니다.

또한 이 기능을 사용하면 각 클라이언트에서 사용하는 활성 저장소 리소스를 볼 수 있습니다. 이렇게 하면 시스템 리소스가 소진되는 클라이언트를 쉽게 식별할 수 있으며 클라이언트 리소스 제한에 따라 적용할 수 있습니다.

사용된 저장소 풀 리소스를 봅니다

를 클릭합니다 `vserver nfs storepool show` 명령 사용된 저장소 리소스 수를 표시합니다. 저장소 풀은 NFSv4 클라이언트가 사용하는 리소스 풀입니다.

단계

1. 관리자 권한으로 를 실행합니다 `vserver nfs storepool show` NFSv4 클라이언트의 저장소 풀 정보를 표시하는 명령입니다.

예

이 예에서는 NFSv4 클라이언트의 저장소 풀 정보를 표시합니다.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

저장소 풀 제한 컨트롤을 사용하거나 사용하지 않도록 설정합니다

관리자는 다음 명령을 사용하여 저장소 풀 제한 컨트롤을 사용하거나 사용하지 않도록 설정할 수 있습니다.

단계

1. 관리자는 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
저장소 풀 제한 컨트롤을 활성화합니다	`vserver nfs storepool config modify -limit-enforce enabled`
저장소 풀 제한 컨트롤을 비활성화합니다	`vserver nfs storepool config modify -limit-enforce disabled`

차단된 클라이언트 목록을 봅니다

저장소 풀 제한이 설정된 경우 관리자는 클라이언트별 리소스 임계값에 도달하면 차단된 클라이언트를 확인할 수 있습니다. 관리자는 다음 명령을 사용하여 차단된 클라이언트로 표시된 클라이언트를 확인할 수 있습니다.

단계

1. 를 사용합니다 `vserver nfs storepool blocked-client show` NFSv4 차단된 클라이언트 목록을 표시하는 명령입니다.

차단된 클라이언트 목록에서 클라이언트를 제거합니다

클라이언트별 임계값에 도달한 클라이언트는 연결이 끊어지고 블록 클라이언트 캐시에 추가됩니다. 관리자는 다음

명령을 사용하여 클라이언트를 블록 클라이언트 캐시에서 제거할 수 있습니다. 이렇게 하면 클라이언트가 ONTAP NFSv4 서버에 접속할 수 있습니다.

단계

1. 를 사용합니다 `vserver nfs storepool blocked-client flush -client-ip <ip address>` 차단된 클라이언트 캐시를 플러시하는 명령입니다.
2. 를 사용합니다 `vserver nfs storepool blocked-client show` 클라이언트가 블록 클라이언트 캐시에서 제거되었는지 확인하는 명령입니다.

예

이 예에서는 모든 노드에서 IP 주소 "10.2.1.1"이 플러시되는 차단된 클라이언트를 표시합니다.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

ONTAP SVM에 대한 **pNFS** 활성화 또는 비활성화

pNFS는 NFS 클라이언트가 스토리지 장치에서 직접 및 병렬로 읽기/쓰기 작업을 수행할 수 있도록 지원하여 잠재적 병목 현상으로 NFS 서버를 우회함으로써 성능을 개선합니다. pNFS(parallel NFS)를 활성화 또는 비활성화하려면 '-v4.1-pNFS' 옵션을 수정합니다.

ONTAP 릴리즈가...	**pNFS** 기본값은...
9.8 이상	사용 안 함
9.7 이하	활성화됨

시작하기 전에

pNFS를 사용하려면 NFSv4.1 지원이 필요합니다.

pNFS를 활성화하려면 먼저 NFS 조회를 비활성화해야 합니다. 둘 다 동시에 활성화할 수는 없습니다.

SVM에서 Kerberos와 pNFS를 사용하는 경우 SVM의 모든 LIF에서 Kerberos를 사용하도록 설정해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
pNFS를 활성화합니다	'vserver nfs modify -vserver vserver_name -v4.1 -pNFS enabled'
pNFS를 비활성화합니다	'vserver nfs modify -vserver vserver_name -v4.1 -pNFS disabled'

관련 정보

- NFS 트렁킹 개요

ONTAP SVM에 대한 **TCP** 및 **UDP**를 통한 **NFS** 액세스 제어

TCP와 UDP를 통해 각각 '-TCP' 및 '-UDP' 매개 변수를 수정하여 SVM(스토리지 가상 시스템)에 대한 NFS 액세스를 설정하거나 해제할 수 있습니다. 따라서 NFS 클라이언트가 사용자 환경에서 TCP 또는 UDP를 통해 데이터에 액세스할 수 있는지 여부를 제어할 수 있습니다.

이 작업에 대해

이러한 매개 변수는 NFS에만 적용됩니다. 보조 프로토콜에는 영향을 미치지 않습니다. 예를 들어, TCP를 통한 NFS가 해제되어 있는 경우 TCP를 통한 마운트 작업은 계속 성공합니다. TCP 또는 UDP 트래픽을 완전히 차단하려면 내보내기 정책 규칙을 사용할 수 있습니다.

명령 실패 오류를 방지하려면 NFS용 TCP를 해제하기 전에 SnapDiff RPC Server를 꺼야 합니다. 'vserver snapdiff -rpc -server off -vserver vserver name' 명령을 사용하여 TCP를 비활성화할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

NFS 액세스를 원하는 경우…	명령 입력…
TCP를 통해 활성화되었습니다	'vserver nfs modify -vserver vserver_name -tcp enabled'
TCP를 통해 비활성화되었습니다	'vserver nfs modify -vserver vserver_name -tcp disabled'
UDP를 통해 활성화됩니다	'vserver nfs modify -vserver vserver_name -udp enabled'
UDP를 통해 비활성화되었습니다	'vserver nfs modify -vserver vserver_name -udp disabled'

ONTAP SVM에 대한 예약되지 않은 포트에서 **NFS** 요청 제어

'-mount-rootonly' 옵션을 설정하여 예약되지 않은 포트에서 NFS 마운트 요청을 거부할 수 있습니다. 예약되지 않은 포트의 모든 NFS 요청을 거부하려면 '-nfs-rootonly' 옵션을 설정합니다.

이 작업에 대해

기본적으로 '-mount-rootonly' 옵션은 'enabled'입니다.

기본적으로 '-nfs-rootonly' 옵션은 '사용 안 함'입니다.

이러한 옵션은 NULL 프로시저에는 적용되지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력…
예약되지 않은 포트에서 NFS 마운트 요청을 허용합니다	'vserver nfs modify -vserver vserver_name -mount -rootonly disabled'
예약되지 않은 포트에서 NFS 마운트 요청을 거부합니다	'vserver nfs modify -vserver vserver_name -mount -rootonly enabled'
예약되지 않은 포트에서 모든 NFS 요청을 허용합니다	'vserver nfs modify -vserver vserver_name -nfs-rootonly disabled'
예약되지 않은 포트의 모든 NFS 요청을 거부합니다	'vserver nfs modify -vserver vserver_name -nfs-rootonly enabled'

알 수 없는 **UNIX** 사용자의 **ONTAP NTFS** 볼륨 또는 **qtree**에 대한 **NFS** 액세스를 처리합니다**.**

ONTAP가 NTFS 보안 스타일로 볼륨이나 qtree에 연결하려고 시도하는 UNIX 사용자를 식별할 수 없는 경우 사용자를 Windows 사용자에게 명시적으로 매핑할 수 없습니다. 보다 엄격한 보안을 위해 이러한 사용자에 대한 액세스를 거부하거나 모든 사용자에 대한 최소 액세스 수준을 보장하도록 ONTAP를 기본 Windows 사용자에게 매핑하도록 구성할 수 있습니다.

시작하기 전에

이 옵션을 활성화하려면 기본 Windows 사용자를 구성해야 합니다.

이 작업에 대해

UNIX 사용자가 NTFS 보안 스타일로 볼륨이나 qtree에 액세스하려고 할 경우 ONTAP에서 NTFS 권한을 올바르게 평가할 수 있도록 UNIX 사용자를 Windows 사용자에게 먼저 매핑해야 합니다. 그러나 ONTAP가 구성된 사용자 정보 이름 서비스 소스에서 UNIX 사용자의 이름을 찾을 수 없는 경우 UNIX 사용자를 특정 Windows 사용자에게 명시적으로 매핑할 수 없습니다. 다음과 같은 방법으로 이러한 알 수 없는 UNIX 사용자를 처리하는 방법을 결정할 수 있습니다.

- 알 수 없는 UNIX 사용자에 대한 액세스를 거부합니다.

  이렇게 하면 모든 UNIX 사용자가 NTFS 볼륨이나 qtree에 액세스할 수 있도록 명시적 매핑이 요구되므로 보안이 더욱 강화됩니다.

- 알 수 없는 UNIX 사용자를 기본 Windows 사용자로 매핑합니다.

  따라서 모든 사용자가 기본 Windows 사용자를 통해 NTFS 볼륨 또는 qtree에 대한 최소 액세스 수준을 얻을 수

있으므로 보안이 낮지만 편의성이 높아집니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

알 수 없는 UNIX 사용자에 대해 기본 Windows 사용자를 사용하려는 경우…	명령 입력…
활성화됨	'vserver nfs modify -vserver vserver_name -map -unknown -uid -to -default-windows-user enabled'
사용 안 함	'vserver nfs modify -vserver vserver_name -map -unknown -uid -to -default-windows-user disabled'

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

예약되지 않은 포트에서 **ONTAP NFS** 내보내기를 마운트하는 클라이언트에 대한 고려 사항

'-mount-rootonly' 옵션은 사용자가 루트로 로그인한 경우에도 예약되지 않은 포트를 사용하여 NFS 내보내기를 마운트하는 클라이언트를 지원해야 하는 스토리지 시스템에서 해제되어야 합니다. 이러한 클라이언트에는 Hummingbird 클라이언트와 Solaris NFS/IPv6 클라이언트가 포함됩니다.

'-mount-rootonly' 옵션이 설정된 경우 ONTAP는 예약되지 않은 포트를 사용하는 NFS 클라이언트가 허용되지 않습니다. 즉, 번호가 1,023보다 큰 포트를 사용하여 NFS 내보내기를 마운트할 수 있습니다.

ONTAP NFS SVM에 대한 도메인을 확인하여 넷그룹에 대한 보다 엄격한 액세스 검사를 수행합니다**.**

기본적으로 ONTAP는 넷그룹에 대한 클라이언트 액세스를 평가할 때 추가 검증을 수행합니다. 추가 검사를 통해 클라이언트 도메인이 SVM(스토리지 가상 머신)의 도메인 구성과 일치하는지 확인합니다. 그렇지 않으면 ONTAP는 클라이언트 액세스를 거부합니다.

이 작업에 대해

ONTAP에서 클라이언트 액세스에 대한 엑스포트 정책 규칙을 평가하고 엑스포트 정책 규칙에 넷그룹이 포함되어 있는 경우, ONTAP는 클라이언트의 IP 주소가 넷그룹에 속하는지 여부를 결정해야 합니다. 이를 위해 ONTAP는 DNS를 사용하여 클라이언트의 IP 주소를 호스트 이름으로 변환하고 FQDN(정규화된 도메인 이름)을 얻습니다.

넷그룹 파일에 호스트에 대한 짧은 이름만 나열되고 호스트에 대한 짧은 이름이 여러 도메인에 있는 경우 다른 도메인의 클라이언트가 이 검사 없이 액세스할 수 있습니다.

이를 방지하기 위해 ONTAP는 호스트의 DNS에서 반환된 도메인을 SVM용으로 구성된 DNS 도메인 이름 목록과 비교합니다. 일치하는 경우 액세스가 허용됩니다. 일치하지 않으면 액세스가 거부됩니다.

이 검증은 기본적으로 활성화되어 있습니다. 고급 권한 수준에서 사용할 수 있는 '-netgroup-dns-domain-search' 매개 변수를 수정하여 이 매개 변수를 관리할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

넷그룹에 대한 도메인 확인을 원할 경우...	입력...
활성화됨	'vserver nfs modify -vserver vserver_name -netgroup -dns -domain -search enabled'
사용 안 함	'vserver nfs modify -vserver vserver_name -netgroup -dns -domain -search disabled'

3. 권한 수준을 admin으로 설정합니다.

   'Set-Privilege admin'입니다

ONTAP SVM의 **NFSv3** 서비스에 사용되는 포트 수정

스토리지 시스템의 NFS 서버에서는 마운트 데몬, Network Lock Manager 등의 서비스를 사용하여 특정 기본 네트워크 포트를 통해 NFS 클라이언트와 통신합니다. 대부분의 NFS 환경에서 기본 포트는 올바르게 작동하고 수정할 필요가 없지만, NFSv3 환경에서 다른 NFS 네트워크 포트를 사용하려는 경우에는 변경할 수 있습니다.

시작하기 전에

스토리지 시스템에서 NFS 포트를 변경하려면 모든 NFS 클라이언트가 시스템에 다시 연결해야 하므로 먼저 이 정보를 사용자에게 전달해야 합니다.

이 작업에 대해

각 SVM(스토리지 가상 머신)에 대해 NFS 마운트 데몬, Network Lock Manager, Network Status Monitor, NFS 할당량 데몬 서비스에서 사용하는 포트를 설정할 수 있습니다. 포트 번호 변경은 TCP 및 UDP를 통해 데이터에 액세스하는 NFS 클라이언트에 영향을 줍니다.

NFSv4 및 NFSv4.1의 포트는 변경할 수 없습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. NFS에 대한 액세스 해제:

   'vserver nfs modify -vserver vserver_name -access false'

3. 특정 NFS 서비스의 NFS 포트를 설정합니다.

   'vserver nfs modify -vserver vserver vserver_namenfs_port_parameterport_number'

NFS 포트 매개 변수입니다	설명	기본 포트입니다
'- mountd-port'입니다	NFS 마운트 데몬입니다	635
``NLM-PORT'	네트워크 잠금 관리자	4045
'-NSM-port'입니다	네트워크 상태 모니터	4046
``rquotad-port''	NFS 할당량 데몬입니다	4049

   기본 포트 이외에 허용되는 포트 번호 범위는 1024 ~ 65535입니다. 각 NFS 서비스는 고유한 포트를 사용해야 합니다.

4. NFS에 대한 액세스 설정:

   'vserver nfs modify -vserver vserver_name -access TRUE'

5. 'network connections listening show' 명령어를 이용하여 포트 번호 변화를 확인한다.

   에 대한 자세한 내용은 `network connections listening show` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 NFS 마운트 데몬 포트가 1113으로 설정됩니다.

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

NFS 서버를 관리하기 위한 **ONTAP** 명령입니다

NFS 서버를 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
NFS 서버를 생성합니다	'vserver nfs create
NFS 서버를 표시합니다	'vserver nfs show'
NFS 서버를 수정합니다	'vserver nfs modify(가상 NFS 수정)'
NFS 서버를 삭제합니다	'vserver nfs delete

NFSv3 마운트 지점 아래에 있는 '.snapshot' 디렉토리를 숨깁니다 이 옵션을 사용하는 경우에도 '.snapshot' 디렉토리에 대한 명시적 액세스는 계속 허용됩니다.	'-v3-hide-snapshot' 옵션이 활성화된 'vserver nfs' 명령입니다

에 대한 자세한 내용은 `vserver nfs` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP NAS SVM의 이름 서비스 문제 해결

클라이언트가 이름 서비스 문제로 인해 액세스 오류가 발생하는 경우, 'vserver services name-service getxxbyy' 명령 제품군을 사용하여 다양한 이름 서비스 조회를 수동으로 수행하고 조회에 대한 세부 정보와 결과를 확인하여 문제 해결에 도움이 될 수 있습니다.

이 작업에 대해

- 각 명령에 대해 다음을 지정할 수 있습니다.
  - 조회를 수행할 노드 또는 SVM(스토리지 가상 머신)의 이름입니다.

    이를 통해 특정 노드 또는 SVM에 대한 네임 서비스 조회를 테스트하여 잠재적 네임 서비스 구성 문제에 대한 검색 범위를 좁힐 수 있습니다.
  - 조회에 사용된 소스를 표시할지 여부를 나타냅니다.

    이를 통해 올바른 소스가 사용되었는지 확인할 수 있습니다.
- ONTAP는 구성된 이름 서비스 스위치 순서에 따라 조회를 수행하기 위한 서비스를 선택합니다.
- 이러한 명령은 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

를 검색하려면…	명령 사용…
호스트 이름의 IP 주소입니다	'vserver services name-service getxxyy getaddrinfo"vserver services name-service getxxyy gethostbyname'(IPv4 주소만 해당)
그룹 ID별 그룹 구성원	'vserver services name-service getxxyy getgrbygid'
그룹 이름으로 그룹의 구성원	'vserver services name-service getxxyy getgrbyname'
사용자가 속한 그룹 목록입니다	'vserver services name-service getxxyy getgrlist'

IP 주소의 호스트 이름입니다	'vserver services name-service getxxbyyy GetNameInfo"vserver services name-service getxxyy gethostbyaddr'(IPv4 주소만)
사용자 이름별 사용자 정보	'vserver services name-service getxxbyyy getpwbyname' '-use-RBAC' 매개변수를 TRUE로 지정하여 RBAC 사용자의 이름 확인을 테스트할 수 있습니다.
사용자 ID별 사용자 정보	'vserver services name-service getxxbyyy getpwbyuid' '-use-RBAC' 매개 변수를 true로 지정하여 RBAC 사용자의 이름 확인을 테스트할 수 있습니다.
클라이언트의 넷그룹 구성원 자격	'vserver services name-service getxxbyy netgrp'
Netgroup-by-host 검색을 사용하는 클라이언트의 넷그룹 구성원 자격	'vserver services name-service getxxbyyy netgrpbyhost'

다음 예에서는 acast1.eng.example.com 호스트의 IP 주소를 획득하여 SVM VS1 에 대한 DNS 조회 테스트를 보여 줍니다.

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

다음 예에서는 UID 501768을 가진 사용자의 사용자 정보를 검색함으로써 SVM VS1 에 대한 NIS 조회 테스트를 보여 줍니다.

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

다음 예제는 이름이 ldap1인 사용자의 사용자 정보를 검색함으로써 SVM VS1 에 대한 LDAP 조회 테스트를 보여줍니다.

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

다음 예에서는 클라이언트 dnshost0이 넷그룹 lnetgroup136의 구성원인지 여부를 확인함으로써 SVM V1에 대한 넷그룹 조회 테스트를 보여 줍니다.

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. 수행한 테스트의 결과를 분석하고 필요한 조치를 취합니다.

만약...	다음을 확인하십시오.
호스트 이름 또는 IP 주소 조회에 실패했거나 잘못된 결과가 발생했습니다	DNS 구성
조회가 잘못된 소스를 쿼리했습니다	네임 서비스 스위치 구성
사용자 또는 그룹 조회에 실패했거나 잘못된 결과가 발생했습니다	• 네임 서비스 스위치 구성 • 소스 구성(로컬 파일, NIS 도메인, LDAP 클라이언트) • 네트워크 구성(예: LIF 및 라우트)
호스트 이름 조회가 실패했거나 시간이 초과되었으며 DNS 서버가 DNS 짧은 이름(예: host1)을 확인하지 않습니다.	최상위 도메인(TLD) 쿼리에 대한 DNS 구성 vserver services name-service dns modify 명령에 대한 `-is-tLD-query-enabled false ' 옵션을 사용하여 TLD 쿼리를 비활성화할 수 있습니다.

관련 정보

"NetApp 기술 보고서 4668: 이름 서비스 모범 사례 가이드"

ONTAP NAS SVM에 대한 이름 서비스 연결 확인

DNS 및 LDAP(Lightweight Directory Access Protocol) 이름 서버를 확인하여 ONTAP 에 연결되어 있는지 확인할 수 있습니다. 이러한 명령은 admin 권한 수준에서 사용할 수 있습니다.

이 작업에 대해

이름 서비스 구성 검사기를 사용하여 필요에 따라 유효한 DNS 또는 LDAP 네임 서비스 구성을 확인할 수 있습니다. 이러한 검증 검사는 명령줄 또는 System Manager에서 시작할 수 있습니다.

DNS 구성의 경우 모든 서버가 테스트되고 유효한 구성으로 간주되려면 해당 구성이 제대로 작동되어야 합니다. LDAP 구성의 경우 서버가 가동되는 한 구성이 유효합니다. 'ip-config-validation' 필드가 true(기본값 false)가 아닌 경우 이름 서비스 명령은 구성 검사기를 적용합니다.

단계

1. 적절한 명령을 사용하여 네임 서비스 구성을 확인합니다. UI는 구성된 서버의 상태를 표시합니다.

확인하려면…	이 명령 사용…
DNS 구성 상태입니다	'vserver services name-service dns check'
LDAP 구성 상태입니다	'vserver services name-service ldap check'

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

구성된 서버 중 하나(name-servers/ldap-servers)에 연결할 수 있고 서비스를 제공하는 경우 구성 검증이 성공적으로 수행됩니다. 일부 서버에 연결할 수 없는 경우 경고가 표시됩니다.

NAS 이름 서비스 스위치 항목을 관리하기 위한 ONTAP 명령

이름 서비스 스위치 항목은 생성, 표시, 수정 및 삭제하여 관리할 수 있습니다.

원하는 작업	이 명령 사용…
이름 서비스 스위치 항목을 생성합니다	'vserver services name-service ns-switch create'
이름 서비스 스위치 항목을 표시합니다	'vserver services name-service ns-switch show'
이름 서비스 스위치 항목을 수정합니다	'vserver services name-service ns-switch modify'를 참조하십시오
이름 서비스 스위치 항목을 삭제합니다	'vserver services name-service ns-switch delete'

에 대한 자세한 내용은 `vserver services name-service ns-switch` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

"NetApp 기술 보고서 4668: 이름 서비스 모범 사례 가이드"

NAS 이름 서비스 캐시를 관리하기 위한 ONTAP 명령

TTL(Time To Live) 값을 수정하여 이름 서비스 캐시를 관리할 수 있습니다. TTL 값은 이름 서비스 정보가 캐시에 지속되는 기간을 결정합니다.

TTL 값을 수정하려는 경우…	이 명령 사용…
Unix 사용자	'vserver services name-service cache unix-user settings
Unix 그룹	'vserver services name-service cache unix-group settings'
Unix 넷그룹	'vserver services name-service cache netgroups settings'(SVM 서비스 이름 서비스 캐시 넷그룹 설정)
호스트	'vserver services name-service cache hosts settings'(SVM 서비스 이름 서비스 캐시 호스트 설정)
그룹 구성원 자격	'vserver services name-service cache group-membership settings'

관련 정보

"ONTAP 명령 참조입니다"

NFS 이름 매핑을 관리하기 위한 ONTAP 명령

이름 매핑을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
이름 매핑을 생성합니다	`vserver name-mapping create`
특정 위치에 이름 매핑을 삽입합니다	`vserver name-mapping insert`
이름 매핑을 표시합니다	`vserver name-mapping show`
두 이름 매핑의 위치를 교환합니다. 참고: 이름 매핑이 IP 한정자 항목으로 구성된 경우에는 스왑이 허용되지 않습니다.	`vserver name-mapping swap`
이름 매핑을 수정합니다	`vserver name-mapping modify`
이름 매핑을 삭제합니다	`vserver name-mapping delete`
올바른 이름 매핑을 확인합니다	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

에 대한 자세한 내용은 `vserver name-mapping` "ONTAP 명령 참조입니다"을 참조하십시오.

NAS 로컬 **UNIX** 사용자를 관리하기 위한 **ONTAP** 명령

로컬 UNIX 사용자를 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
로컬 UNIX 사용자를 생성합니다	'vserver services name-service unix-user create'를 참조하십시오
URI에서 로컬 UNIX 사용자를 로드합니다	'vserver services name-service unix-user load-from-Uri'
로컬 UNIX 사용자를 표시합니다	'vserver services name-service unix-user show'를 참조하십시오
로컬 UNIX 사용자를 수정합니다	'vserver services name-service unix-user modify'를 참조하십시오
로컬 UNIX 사용자를 삭제합니다	'vserver services name-service unix-user delete

에 대한 자세한 내용은 `vserver services name-service unix-user` "ONTAP 명령 참조입니다"을 참조하십시오.

NAS 로컬 **UNIX** 그룹을 관리하기 위한 **ONTAP** 명령

로컬 UNIX 그룹을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
로컬 UNIX 그룹을 생성합니다	'vserver services name-service unix-group create’를 참조하십시오
로컬 UNIX 그룹에 사용자를 추가합니다	'vserver services name-service unix-group adduser'
URI에서 로컬 UNIX 그룹을 로드합니다	가상 서버 서비스 이름 서비스 unix-group load-from-Uri
로컬 UNIX 그룹을 표시합니다	'vserver services name-service unix-group show’를 참조하십시오
로컬 UNIX 그룹을 수정합니다	'vserver services name-service unix-group modify’를 참조하십시오
로컬 UNIX 그룹에서 사용자를 삭제합니다	'vserver services name-service unix-group deluser'
로컬 UNIX 그룹을 삭제합니다	'vserver services name-service unix-group delete'

에 대한 자세한 내용은 `vserver services name-service unix-group` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP NFS SVM의 로컬 **UNIX** 사용자, 그룹 및 그룹 멤버에 대한 제한

ONTAP는 클러스터의 최대 UNIX 사용자 및 그룹 수와 이러한 제한을 관리하는 명령에 대한 제한을 도입했습니다. 이러한 제한을 사용하면 관리자가 클러스터에 너무 많은 로컬 UNIX 사용자 및 그룹을 생성하지 못하도록 하여 성능 문제를 방지할 수 있습니다.

로컬 UNIX 사용자 그룹 및 그룹 구성원의 총 수에 대한 제한이 있습니다. 로컬 UNIX 사용자에게는 별도의 제한이 있습니다. 제한은 클러스터 전반에 적용됩니다. 이러한 각 새 제한은 미리 할당된 하드 제한까지 수정할 수 있는 기본값으로 설정됩니다.

데이터베이스	기본 제한	엄격한 제한
로컬 UNIX 사용자	32,768입니다	65,536
로컬 UNIX 그룹 및 그룹 구성원	32,768입니다	65,536

ONTAP NFS SVM에 대한 로컬 **UNIX** 사용자 및 그룹에 대한 제한 관리

로컬 UNIX 사용자 및 그룹에 대한 제한을 관리하기 위한 특정 ONTAP 명령이 있습니다. 클러스터 관리자는 이러한 명령을 사용하여 과도한 수의 로컬 UNIX 사용자 및 그룹과 관련된 것으로 여겨지는 클러스터의 성능 문제를 해결할 수 있습니다.

이 작업에 대해

이러한 명령은 클러스터 관리자가 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 사용...
로컬 UNIX 사용자 제한에 대한 정보를 표시합니다	'vserver services unix-user max-limit show'를 선택합니다
로컬 UNIX 그룹 제한에 대한 정보를 표시합니다	'vserver services unix-group max-limit show'를 선택합니다
로컬 UNIX 사용자 제한을 수정합니다	'vserver services unix-user max-limit modify'를 참조하십시오
로컬 UNIX 그룹 제한을 수정합니다	'vserver services unix-group max-limit modify'를 참조하십시오

에 대한 자세한 내용은 `vserver services unix` "ONTAP 명령 참조입니다"을 참조하십시오.

NFS 로컬 넷그룹을 관리하기 위한 **ONTAP** 명령

로컬 넷그룹을 URI에서 로드하고, 노드 간에 상태를 확인하고, 표시하고, 삭제하여 관리할 수 있습니다.

원하는 작업	명령 사용…
URI에서 넷그룹을 로드합니다	'vserver services name-service netgroup load'
전체 노드에서 넷그룹의 상태를 확인합니다	'vserver services name-service netgroup status' 고급 권한 수준에서 사용할 수 있습니다.
로컬 넷그룹을 표시합니다	'vserver services name-service netgroup file show'를 참조하십시오
로컬 넷그룹을 삭제합니다	'vserver services name-service 넷그룹 파일 삭제

에 대한 자세한 내용은 `vserver services name-service netgroup file` "ONTAP 명령 참조입니다"을 참조하십시오.

NFS NIS 도메인 구성을 관리하기 위한 **ONTAP** 명령

NIS 도메인 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
NIS 도메인 구성을 생성합니다	'vserver services name-service nis-domain create'를 참조하십시오

NIS 도메인 구성을 표시합니다	'vserver services name-service NIS-domain show'를 참조하십시오
NIS 도메인 구성의 바인딩 상태를 표시합니다	'vserver services name-service nis-domain show-bound'
NIS 통계를 표시합니다	고급 권한 수준 이상에서 사용할 수 있는 SVM 서비스 이름 서비스 NIS-도메인 표시-통계.
NIS 통계를 지웁니다	고급 권한 수준 이상에서 사용할 수 있는 SVM 서비스 이름 서비스 NIS-도메인 지우기-통계.
NIS 도메인 구성을 수정합니다	'vserver services name-service NIS-domain modify'를 참조하십시오
NIS 도메인 구성을 삭제합니다	'vserver services name-service nis-domain delete'
호스트 별 넷그룹 검색에 대한 캐싱을 설정합니다	고급 권한 수준 이상에서 사용할 수 있는 'vserver services name-service NIS-domain netgroup-database config modify'입니다.

에 대한 자세한 내용은 `vserver services name-service nis-domain` "ONTAP 명령 참조입니다"을 참조하십시오.

NFS LDAP 클라이언트 구성을 관리하기 위한 **ONTAP** 명령

LDAP 클라이언트 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

SVM 관리자는 클러스터 관리자가 생성한 LDAP 클라이언트 구성을 수정하거나 삭제할 수 없습니다.

원하는 작업	이 명령 사용…
LDAP 클라이언트 구성을 생성합니다	'vserver services name-service ldap client create'
LDAP 클라이언트 구성을 표시합니다	'vserver services name-service ldap client show'
LDAP 클라이언트 구성을 수정합니다	'vserver services name-service ldap client modify'를 참조하십시오
LDAP 클라이언트 바인딩 암호를 변경합니다	'vserver services name-service ldap client modify-bind-password'
LDAP 클라이언트 구성을 삭제합니다	'vserver services name-service ldap client delete'

에 대한 자세한 내용은 `vserver services name-service ldap client` "ONTAP 명령 참조입니다"을 참조하십시오.

NFS LDAP 구성을 관리하기 위한 ONTAP 명령

LDAP 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
LDAP 구성을 생성합니다	'vserver services name-service ldap create'
LDAP 구성을 표시합니다	'vserver services name-service ldap show'
LDAP 구성을 수정합니다	'vserver services name-service ldap modify'를 참조하십시오
LDAP 구성을 삭제합니다	'vserver services name-service ldap delete'

에 대한 자세한 내용은 `vserver services name-service ldap` "ONTAP 명령 참조입니다"을 참조하십시오.

NFS LDAP 클라이언트 스키마 템플릿을 관리하기 위한 ONTAP 명령

LDAP 클라이언트 스키마 템플릿을 관리하기 위한 특정 ONTAP 명령이 있습니다.

SVM 관리자는 클러스터 관리자가 생성한 LDAP 클라이언트 스키마를 수정하거나 삭제할 수 없습니다.

원하는 작업	이 명령 사용…
기존 LDAP 스키마 템플릿을 복사합니다	고급 권한 수준 이상에서 사용할 수 있는 'vserver services name-service LDAP 클라이언트 스키마 복사'입니다.
LDAP 스키마 템플릿을 표시합니다	'vserver services name-service ldap client schema show'를 참조하십시오
LDAP 스키마 템플릿을 수정합니다	고급 권한 수준 이상에서 사용할 수 있는 'vserver services name-service LDAP 클라이언트 스키마 수정'입니다.
LDAP 스키마 템플릿을 삭제합니다	고급 권한 수준 이상에서 사용할 수 있는 'vserver services name-service LDAP 클라이언트 스키마 삭제'입니다.

에 대한 자세한 내용은 `vserver services name-service ldap client schema` "ONTAP 명령 참조입니다"을 참조하십시오.

NFS Kerberos 인터페이스 구성을 관리하기 위한 ONTAP 명령

NFS Kerberos 인터페이스 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…

LIF에서 NFS Kerberos를 사용하도록 설정합니다	'vserver NFS Kerberos interface enable'
NFS Kerberos 인터페이스 구성을 표시합니다	vserver nfs Kerberos interface show를 선택합니다
NFS Kerberos 인터페이스 구성을 수정합니다	가상 NFS Kerberos 인터페이스 수정
LIF에서 NFS Kerberos를 사용하지 않도록 설정합니다	'vserver NFS Kerberos interface disable'

에 대한 자세한 내용은 `vserver nfs kerberos interface` "ONTAP 명령 참조입니다"을 참조하십시오.

NFS Kerberos 영역 구성을 관리하기 위한 **ONTAP** 명령

NFS Kerberos 영역 구성을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
NFS Kerberos 영역 구성을 생성합니다	'vserver NFS Kerberos 영역 생성'
NFS Kerberos 영역 구성을 표시합니다	가상 NFS Kerberos 영역 표시
NFS Kerberos 영역 구성을 수정합니다	가상 NFS Kerberos 영역 수정
NFS Kerberos 영역 구성을 삭제합니다	'vserver NFS Kerberos 영역 삭제'

에 대한 자세한 내용은 `vserver nfs kerberos realm` "ONTAP 명령 참조입니다"을 참조하십시오.

수출 정책 관리를 위한 **ONTAP** 명령

내보내기 정책을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
엑스포트 정책에 대한 정보를 표시합니다	vserver export-policy show를 참조하십시오
엑스포트 정책의 이름을 바꿉니다	'vserver export-policy rename'
엑스포트 정책을 복사합니다	'vserver export-policy copy'
엑스포트 정책을 삭제합니다	'vserver export-policy delete

에 대한 자세한 내용은 `vserver export-policy` "ONTAP 명령 참조입니다"을 참조하십시오.

내보내기 규칙 관리를 위한 **ONTAP** 명령

내보내기 규칙을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
엑스포트 규칙을 생성합니다	'vserver export-policy rule create'
내보내기 규칙에 대한 정보를 표시합니다	'vserver export-policy rule show'를 선택합니다
엑스포트 규칙을 수정합니다	'vserver export-policy rule modify'입니다
엑스포트 규칙을 삭제합니다	'vserver export-policy rule delete

서로 다른 클라이언트와 일치하는 동일한 내보내기 규칙을 여러 개 구성한 경우 내보내기 규칙을 관리할 때 해당 규칙을 동기화 상태로 유지해야 합니다.

에 대한 자세한 내용은 `vserver export-policy` "ONTAP 명령 참조입니다"을 참조하십시오.

NFS 자격 증명 캐시를 구성합니다

ONTAP SVM의 **NFS** 자격 증명 캐시 **TTL(**수명**)**을 수정하는 이유

ONTAP는 보다 빠른 액세스를 제공하고 성능을 향상시키기 위해 자격 증명 캐시를 사용하여 NFS 내보내기 액세스에 대한 사용자 인증에 필요한 정보를 저장합니다. 자격 증명 캐시에 정보가 저장되는 기간을 구성하여 사용자 환경에 맞게 정보를 사용자 지정할 수 있습니다.

NFS 자격 증명 캐시 TTL(Time-to-Live)을 수정하면 문제를 해결하는 데 도움이 되는 몇 가지 시나리오가 있습니다. 이러한 시나리오가 무엇인지, 그리고 이러한 수정 결과로 초래되는 결과를 이해해야 합니다.

이유

다음과 같은 경우 기본 TTL을 변경하십시오.

문제	구제 조치
사용자 환경의 네임 서버에서 ONTAP의 요청 로드가 높기 때문에 성능이 저하됩니다.	캐시된 양의 자격 증명과 음의 자격 증명에 대한 TTL을 늘려 ONTAP에서 이름 서버로 보내는 요청 수를 줄입니다.
이름 서버 관리자가 이전에 거부된 NFS 사용자에 대한 액세스를 허용하도록 변경되었습니다.	캐시된 음수 자격 증명에 대한 TTL을 줄여 NFS 사용자가 외부 이름 서버에서 새 자격 증명을 요청할 때까지 ONTAP를 기다려야 하는 시간을 줄임으로써 액세스 권한을 얻을 수 있습니다.

문제	구제 조치
이름 서버 관리자가 이전에 허용된 NFS 사용자에 대한 액세스를 거부하도록 변경되었습니다.	캐시된 양의 자격 증명에 대한 TTL을 줄여 ONTAP가 외부 이름 서버에서 새 자격 증명을 요청하는 시간을 줄임으로써 NFS 사용자가 액세스를 거부하도록 합니다.

결과

양의 자격 증명과 음수 자격 증명을 캐시하기 위해 시간을 개별적으로 수정할 수 있습니다. 그러나 그렇게 할 때의 장단점을 모두 알아야 합니다.

만약...	장점은...	단점은...
양의 자격 증명 캐시 시간을 늘립니다	ONTAP는 이름 서버에 자격 증명 요청을 덜 자주 전송하여 이름 서버의 부하를 줄입니다.	이전에는 액세스가 허용되었지만 더 이상 허용되지 않았던 NFS 사용자에 대한 액세스를 거부하는 데 시간이 더 오래 걸립니다.
양의 자격 증명 캐시 시간을 줄입니다	이전에는 액세스가 허용되었지만 이제는 그렇지 않은 NFS 사용자에 대한 액세스를 거부하는 데 걸리는 시간이 더 적게 걸립니다.	ONTAP는 이름 서버에 자격 증명 요청을 더 자주 전송하여 이름 서버의 로드를 증가시킵니다.
부정적인 자격 증명 캐시 시간을 늘립니다	ONTAP는 이름 서버에 자격 증명 요청을 덜 자주 전송하여 이름 서버의 부하를 줄입니다.	이전에는 액세스가 허용되지 않았지만 지금은 NFS 사용자에게 액세스 권한을 부여하는 데 시간이 더 오래 걸립니다.
부정적인 자격 증명 캐시 시간을 줄입니다	이전에는 액세스가 허용되지 않았지만 지금은 NFS 사용자에게 액세스 권한을 부여하는 데 시간이 더 적게 걸립니다.	ONTAP는 이름 서버에 자격 증명 요청을 더 자주 전송하여 이름 서버의 로드를 증가시킵니다.

ONTAP SVM에 대한 캐시된 **NFS** 사용자 자격 증명의 수명 구성

SVM(스토리지 가상 시스템)의 NFS 서버를 수정하여 ONTAP에서 NFS 사용자에 대한 자격 증명을 내부 캐시(TTL(Time-to-Live)에 저장하는 시간을 구성할 수 있습니다. 따라서 네임 서버의 높은 부하나 NFS 사용자 액세스에 영향을 미치는 자격 증명의 변경과 관련된 특정 문제를 완화할 수 있습니다.

이 작업에 대해

이러한 매개 변수는 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

캐싱된 TTL을 수정하려는 경우…	명령 사용…
양의 자격 증명	'vserver nfs modify -vserver vserver_name -cached -cred -positive -ttl time_to_live' TTL은 밀리초 단위로 측정됩니다. ONTAP 9.10.1 이상부터 기본값은 1시간(3,600,000밀리초)입니다. ONTAP 9.9.1 이하 버전의 경우 기본값은 24시간(86,400,000밀리초)입니다. 이 값에 허용되는 범위는 1분(60000밀리초)~7일(604,800,000밀리초)입니다.
음수 자격 증명	'vserver nfs modify -vserver vserver_name -cached -cred -negative -tl time_to_live' TTL은 밀리초 단위로 측정됩니다. 기본값은 2시간(7,200,000밀리초)입니다. 이 값에 허용되는 범위는 1분(60000밀리초)~7일(604,800,000밀리초)입니다.

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

엑스포트 정책 캐시 관리

ONTAP NAS SVM에 대한 내보내기 정책 캐시 플러시

ONTAP는 빠른 액세스를 위해 여러 엑스포트 정책 캐시를 사용하여 엑스포트 정책과 관련된 정보를 저장합니다. 내보내기 정책 캐시를 수동으로 플러싱하면('vserver export-policy cache flush') 오래된 정보가 제거되고 ONTAP가 적절한 외부 리소스에서 현재 정보를 검색하도록 합니다. 이렇게 하면 NFS 내보내기에 대한 클라이언트 액세스와 관련된 다양한 문제를 해결할 수 있습니다.

이 작업에 대해

다음과 같은 이유로 인해 엑스포트 정책 캐시 정보가 오래된 것일 수 있습니다.

- 정책 규칙을 내보내기 위한 최근 변경 사항
- 이름 서버의 호스트 이름 레코드에 대한 최근 변경 사항
- 이름 서버의 넷그룹 항목에 대한 최근 변경 사항
- 네트워크 중단 상태에서 복구되어 넷그룹이 완전히 로드되지 않았습니다

단계

1. 이름 서비스 캐시를 사용하지 않는 경우 다음 작업 중 하나를 고급 권한 모드에서 수행합니다.

플러시를 원하는 경우...	명령 입력...
모든 엑스포트 정책 캐시(Showmount 제외)	'vserver export-policy cache flush-vserver vserver_name'
엑스포트 정책 규칙 액세스 캐시	'vserver export-policy cache flush-vserver vserver_name-cache access’는 선택 사항인 '-node' 매개변수를 포함하여 액세스 캐시를 플러시할 노드를 지정할 수 있습니다.
호스트 이름 캐시입니다	'vserver export-policy cache flush-vserver vserver_name-cache host'
넷그룹 캐시입니다	넷그룹의 처리는 리소스를 많이 소모하는 작업입니다. 오래된 넷그룹으로 인해 발생하는 클라이언트 액세스 문제를 해결하려는 경우에만 넷그룹 캐시를 플러시해야 합니다.
showmount 캐시입니다	'vserver export-policy cache flush-vserver vserver_name-cache showmount'

2. 이름 서비스 캐시가 활성화된 경우 다음 작업 중 하나를 수행합니다.

플러시를 원하는 경우...	명령 입력...
엑스포트 정책 규칙 액세스 캐시	'vserver export-policy cache flush-vserver vserver_name-cache access’는 선택 사항인 '-node' 매개변수를 포함하여 액세스 캐시를 플러시할 노드를 지정할 수 있습니다.
호스트 이름 캐시입니다	'vserver services name-service cache hosts forward-lookup delete-all'
넷그룹 캐시입니다	SVM 서비스 이름-서비스 캐시 넷그룹 IP-넷그룹 삭제-모두 SVM 서비스 이름-서비스 캐시 넷그룹 구성원 삭제 -모두(All) 넷그룹 처리는 리소스를 많이 소모합니다. 오래된 넷그룹으로 인해 발생하는 클라이언트 액세스 문제를 해결하려는 경우에만 넷그룹 캐시를 플러시해야 합니다.
showmount 캐시입니다	'vserver export-policy cache flush-vserver vserver_name-cache showmount'

ONTAP NFS SVM에 대한 내보내기 정책 **netgroup** 대기열 및 캐시 표시

ONTAP는 넷그룹 큐를 가져와 확인할 때 넷그룹 큐를 사용하고 넷그룹 캐시를 사용하여 결과 정보를 저장합니다. 엑스포트 정책 넷그룹 관련 문제를 해결할 때 'vserver export-policy netgroup queue show' 및 'vserver export-policy netgroup cache show' 명령을 사용하여

넷그룹 큐의 상태와 넷그룹 캐시의 내용을 표시할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

엑스포트 정책 넷그룹을 표시하려면…	명령 입력…
대기열	'vserver export-policy netgroup queue show'를 선택합니다
캐시	'vserver export-policy netgroup cache show -vserver vserver_name'을 선택합니다

에 대한 자세한 내용은 `vserver export-policy netgroup` "ONTAP 명령 참조입니다"을 참조하십시오.

클라이언트 **IP** 주소가 **ONTAP NFS** 넷그룹의 멤버인지 확인하세요**.**

넷그룹과 관련된 NFS 클라이언트 액세스 문제를 해결할 때 'vserver export-policy netgroup check-membership' 명령을 사용하여 클라이언트 IP가 특정 넷그룹의 구성원인지 여부를 확인할 수 있습니다.

이 작업에 대해

넷그룹 구성원 자격을 확인하면 ONTAP가 클라이언트가 넷그룹의 구성원인지 여부를 확인할 수 있습니다. 또한 넷그룹 정보를 새로 고치는 동안 ONTAP 넷그룹 캐시가 임시 상태인지 여부를 알 수 있습니다. 이 정보는 클라이언트가 예기치 않게 액세스 권한을 부여받거나 거부되는 이유를 이해하는 데 도움이 될 수 있습니다.

단계

1. 클라이언트 IP 주소의 넷그룹 멤버쉽을 확인합니다. 'vserver export-policy netgroup check-membership-vserver vserver_name-netgroup netgroup_name-client-ip client_ip'

   명령을 실행하면 다음 결과가 반환될 수 있습니다.

   - 클라이언트가 넷그룹의 구성원입니다.

     역방향 조회 검사 또는 호스트 별 넷그룹 검색을 통해 확인되었습니다.

   - 클라이언트가 넷그룹의 구성원입니다.

     ONTAP 넷그룹 캐시에서 발견되었습니다.

   - 클라이언트가 넷그룹의 구성원이 아닙니다.
   - ONTAP가 현재 넷그룹 캐시를 새로 고치고 있기 때문에 클라이언트의 구성원을 확인할 수 없습니다.

     이 작업이 수행되지 않을 때까지 멤버 자격은 명시적으로 배제될 수 없습니다. 'vserver export-policy netgroup queue show' 명령을 사용하여 넷그룹의 로드를 모니터링하고 작업이 완료된 후 검사를 다시 시도하십시오.

예

다음 예에서는 IP 주소가 172.17.16.72인 클라이언트가 SVM VS1 에 있는 넷그룹 수은의 구성원인지 여부를

확인합니다.

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

ONTAP NFS SVM에 대한 액세스 캐시 성능 최적화

여러 매개 변수를 구성하여 액세스 캐시를 최적화하고 성능과 액세스 캐시에 저장된 정보의 현재 상태 간에 적절한 균형을 찾을 수 있습니다.

이 작업에 대해

액세스 캐시 새로 고침 기간을 구성할 때는 다음 사항을 염두에 두십시오.

- 값이 높을수록 액세스 캐시에서 항목이 더 오래 유지됩니다.

  ONTAP는 액세스 캐시 항목을 새로 고치는 데 리소스를 적게 사용하기 때문에 성능이 향상됩니다. 단점은 엑스포트 정책 규칙이 변경되고 액세스 캐시 항목이 오래되면 업데이트하는 데 시간이 오래 걸린다는 것입니다. 따라서 액세스를 받아야 하는 클라이언트가 거부되고 거부되어야 하는 클라이언트가 액세스할 수 있습니다.

- 값이 낮을수록 ONTAP에서 액세스 캐시 항목을 더 자주 새로 고칩니다.

  장점은 항목이 더 최신 항목이고 클라이언트가 올바르게 액세스 권한을 부여하거나 거부될 가능성이 더 높다는 점입니다. 단점은 ONTAP에서 액세스 캐시 항목을 새로 고치는 데 더 많은 리소스를 사용하기 때문에 성능이 저하된다는 것입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

수정 방법	입력...
양의 항목에 대한 새로 고침 기간	'vserver export-policy access-cache config modify -all-vservers-refresh-period-positive timeout_value'
음수 항목의 새로 고침 기간	'vserver export-policy access-cache config modify -all-vservers-refresh-period-negative timeout_value'
이전 항목의 제한 시간	'vserver export-policy access-cache config modify -all-vservers-ab하비스트-timeout_value'

3. 새 매개 변수 설정을 확인합니다.

   'vserver export-policy access-cache config show-all-vservers'

4. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

파일 잠금 관리

ONTAP NFS SVM의 프로토콜 간 파일 잠금에 대해 알아보세요**.**

파일 잠금은 사용자가 이전에 다른 사용자가 연 파일에 액세스하지 못하도록 클라이언트 응용 프로그램에서 사용하는 방법입니다. ONTAP가 파일을 잠그는 방법은 클라이언트의 프로토콜에 따라 다릅니다.

클라이언트가 NFS 클라이언트인 경우 잠금이 권고사항이고, 클라이언트가 SMB 클라이언트인 경우 잠금이 필수입니다.

NFS와 SMB 파일 잠금의 차이로 인해 NFS 클라이언트가 SMB 애플리케이션에서 이전에 연 파일에 액세스하지 못할 수 있습니다.

NFS 클라이언트가 SMB 애플리케이션에 의해 잠긴 파일에 액세스하려고 할 때 다음이 발생합니다.

- 혼합 볼륨 또는 NTFS 볼륨에서 rm, rmdir, mv 등의 파일 조작 작업으로 인해 NFS 응용 프로그램이 실패할 수 있습니다.
- NFS 읽기 및 쓰기 작업은 SMB 거부-읽기 및 거부-쓰기 열기 모드에 의해 각각 거부됩니다.
- 배타적 SMB bytelock로 파일의 쓰기 범위가 잠기면 NFS 쓰기 작업이 실패합니다.

UNIX 보안 스타일 볼륨에서 NFS 링크 해제 및 이름 바꾸기 작업은 SMB 잠금 상태를 무시하고 파일에 대한 액세스를 허용합니다. UNIX 보안 스타일 볼륨에서 다른 모든 NFS 작업은 SMB 잠금 상태를 존중합니다.

ONTAP NFS SVM의 읽기 전용 비트에 대해 알아보세요**.**

읽기 전용 비트는 파일을 쓰기 가능(사용 안 함)인지 읽기 전용(사용 가능)인지를 나타내기 위해 파일별로 설정됩니다.

Windows를 사용하는 SMB 클라이언트는 파일당 읽기 전용 비트를 설정할 수 있습니다. NFS 클라이언트는 파일당 읽기 전용 비트를 사용하는 프로토콜 작업이 없으므로 파일당 읽기 전용 비트를 설정하지 않습니다.

ONTAP는 Windows를 사용하는 SMB 클라이언트가 해당 파일을 생성할 때 파일에 읽기 전용 비트를 설정할 수 있습니다. 또한 ONTAP는 NFS 클라이언트와 SMB 클라이언트 간에 파일이 공유될 때 읽기 전용 비트를 설정할 수 있습니다. 일부 소프트웨어는 NFS 클라이언트 및 SMB 클라이언트에서 사용할 때 읽기 전용 비트를 사용하도록 설정해야 합니다.

ONTAP가 NFS 클라이언트와 SMB 클라이언트 간에 공유되는 파일에 대해 적절한 읽기 및 쓰기 권한을 유지하려면 다음 규칙에 따라 읽기 전용 비트를 처리합니다.

- NFS는 읽기 전용 비트가 설정된 파일을 쓰기 권한 비트가 설정되지 않은 것처럼 처리합니다.
- NFS 클라이언트가 모든 쓰기 권한 비트를 사용하지 않도록 설정하고 이전에 해당 비트 중 하나 이상이 활성화된 경우 ONTAP는 해당 파일에 대해 읽기 전용 비트를 설정합니다.
- NFS 클라이언트가 쓰기 권한 비트를 설정하면 ONTAP는 해당 파일에 대해 읽기 전용 비트를 해제합니다.
- 파일에 대한 읽기 전용 비트가 설정되어 있고 NFS 클라이언트가 해당 파일에 대한 권한을 검색하려고 하면 파일에 대한 권한 비트가 NFS 클라이언트로 전송되지 않고 ONTAP는 쓰기 권한 비트가 마스킹된 상태로 NFS 클라이언트에 사용 권한 비트를 전송합니다.

- 파일에 대한 읽기 전용 비트가 설정되어 있고 SMB 클라이언트가 읽기 전용 비트를 사용하지 않도록 설정한 경우 ONTAP는 해당 파일에 대한 소유자의 쓰기 권한 비트를 설정합니다.
- 읽기 전용 비트가 설정된 파일은 루트에서만 쓸 수 있습니다.

읽기 전용 비트는 다음과 같은 방식으로 ACL 및 Unix 모드 비트와 상호 작용합니다.

파일에 읽기 전용 비트가 설정된 경우:

- 해당 파일의 ACL에는 변경 사항이 없습니다. NFS 클라이언트는 읽기 전용 비트가 설정되기 전과 동일한 ACL을 보게 됩니다.
- 파일에 대한 쓰기 접근을 허용하는 모든 Unix 모드 비트는 무시됩니다.
- NFS와 SMB 클라이언트는 모두 파일을 읽을 수 있지만, 수정할 수는 없습니다.
- ACL 및 UNIX 모드 비트는 읽기 전용 비트 때문에 무시됩니다. 즉, ACL이 쓰기 액세스를 허용하더라도 읽기 전용 비트는 수정을 방지합니다.

파일에 읽기 전용 비트가 설정되지 않은 경우:

- ONTAP ACL 및 UNIX 모드 비트를 기반으로 액세스를 결정합니다.
  - ACL 또는 UNIX 모드 비트가 쓰기 액세스를 거부하는 경우 NFS 및 SMB 클라이언트는 파일을 수정할 수 없습니다.
  - ACL이나 UNIX 모드 비트가 쓰기 액세스를 거부하지 않으면 NFS 및 SMB 클라이언트가 파일을 수정할 수 있습니다.

> ⓘ 파일 권한 변경은 SMB 클라이언트에 즉시 적용되지만 NFS 클라이언트가 특성 캐싱을 사용하는 경우 NFS 클라이언트에 즉시 적용되지 않을 수 있습니다.

ONTAP NFS와 **Windows**가 공유 경로 구성 요소의 잠금을 처리하는 방식이 어떻게 다른지 알아보세요**.**

Windows와 달리 ONTAP는 파일이 열려 있는 동안 열려 있는 파일에 대한 경로의 각 구성 요소를 잠그지 않습니다. 이 동작은 SMB 공유 경로에도 영향을 줍니다.

ONTAP는 경로의 각 구성 요소를 잠그지 않으므로 열려 있는 파일 또는 공유 위에 있는 경로 구성 요소의 이름을 바꿀 수 있습니다. 이렇게 하면 특정 응용 프로그램에 문제가 발생하거나 SMB 구성의 공유 경로가 잘못될 수 있습니다. 이로 인해 공유에 액세스할 수 없게 될 수 있습니다.

경로 구성 요소의 이름을 변경하여 발생하는 문제를 방지하기 위해 사용자 또는 응용 프로그램이 중요한 디렉터리의 이름을 바꾸지 못하도록 하는 Windows ACL(액세스 제어 목록) 보안 설정을 적용할 수 있습니다.

에 대해 자세히 알아보십시오 "클라이언트가 액세스하는 동안 디렉토리의 이름을 변경하지 못하도록 하는 방법".

ONTAP NFS SVM에 대한 잠금 정보 표시

현재 파일 잠금에 대한 정보를 표시할 수 있습니다. 여기에는 보유한 잠금의 유형 및 잠금 상태, 바이트 범위 잠금에 대한 세부 정보, 공유 잠금 모드, 위임 잠금 및 편의적 잠금, 잠금이 내구성 또는 지속 핸들로 열렸는지 여부 등이 포함됩니다.

이 작업에 대해

NFSv4 또는 NFSv4.1을 통해 설정된 잠금에 대해 클라이언트 IP 주소를 표시할 수 없습니다.

기본적으로 명령은 모든 잠금에 대한 정보를 표시합니다. 명령 매개 변수를 사용하여 특정 SVM(스토리지 가상 머신)의 잠금에 대한 정보를 표시하거나 명령의 출력을 다른 기준으로 필터링할 수 있습니다.

'vserver lock show' 명령은 네 가지 유형의 잠금에 대한 정보를 표시합니다.

- 바이트 범위 잠금 - 파일의 일부만 잠급니다.
- 공유 잠금 - 열린 파일을 잠급니다.
- SMB를 통한 클라이언트 측 캐싱을 제어하는 편의적 잠금 기능
- 위임 - NFSv4.x에서 클라이언트 측 캐싱을 제어합니다

선택적 매개 변수를 지정하면 각 잠금 유형에 대한 중요한 정보를 확인할 수 있습니다. 에 대한 자세한 내용은 `vserver locks show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 'vserver lock show' 명령을 사용하여 잠금에 대한 정보를 표시합니다.

예

다음 예에서는 '/vol1/file1' 경로가 있는 파일의 NFSv4 잠금에 대한 요약 정보를 표시합니다. sharelock 액세스 모드는 write-deny_none 이며, 잠금이 쓰기 위임과 함께 부여되었습니다.

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

다음 예에서는 경로 '/data2/data2_2/intro.pptx'를 사용하여 파일의 SMB 잠금에 대한 자세한 oplock 및 sharelock 정보를 표시합니다. IP 주소가 10.3.1.3인 클라이언트에 write-deny_none의 공유 잠금 액세스 모드를 가진 파일에 내구성 있는 핸들이 부여됩니다. 배치 oplock 레벨이 있는 리스 oplock이 부여됩니다.

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
```

```
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

파일 잠금으로 인해 클라이언트가 파일에 액세스하지 못하는 경우 현재 보류된 잠금에 대한 정보를 표시한 다음 특정 잠금을 중단할 수 있습니다. 잠금을 해제해야 하는 시나리오의 예로는 응용 프로그램 디버깅이 있습니다.

이 작업에 대해

`vserver locks break`명령은 advanced 권한 수준 이상에서만 사용할 수 있습니다. 에 대한 자세한 내용은 `vserver locks break` link:https://docs.netapp.com/us-en/ontap-cli/vserver-locks-break.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

단계

1. 잠금을 해제해야 하는 정보를 찾으려면 'vserver lock show' 명령을 사용합니다.

   에 대한 자세한 내용은 `vserver locks show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

3. 다음 작업 중 하나를 수행합니다.

다음을 지정하여 잠금을 해제하려면…	명령 입력…
SVM 이름, 볼륨 이름, LIF 이름 및 파일 경로	'vserver lock break - vserver vserver_name - volume volume_name - path path path -lif lif'
잠금 ID입니다	'vserver lock break-lockid UUID

4. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

ONTAP FPolicy의 첫 번째 읽기 및 첫 번째 쓰기 필터가 **NFS**에서 작동하는 방식을 알아보세요.

FPolicy가 읽기/쓰기 작업이 있는 외부 FPolicy 서버를 사용하여 모니터링되는 이벤트로 사용되는 경우 NFS 클라이언트에서 읽기/쓰기 요청의 트래픽이 많을 때 응답 시간이 오래 됩니다. NFS 클라이언트의 경우 FPolicy에서 첫 번째 읽기 및 첫 번째 쓰기 필터를 사용하므로 FPolicy 알림의 수가 줄어들고 성능이 향상됩니다.

NFS에서 클라이언트는 해당 핸들을 페치하여 파일에서 I/O를 수행합니다. 이 핸들은 서버와 클라이언트의 재부팅 후에도 유효합니다. 따라서 클라이언트는 핸들을 캐시하고 핸들을 다시 검색하지 않고 요청을 보낼 수 있습니다. 일반 세션에서 많은 읽기/쓰기 요청이 파일 서버로 전송됩니다. 이러한 모든 요청에 대해 알림이 생성되는 경우 다음과 같은 문제가 발생할 수 있습니다.

- 추가 알림 처리 및 응답 시간 증가로 인한 로드 증가

- 서버가 모든 알림의 영향을 받지 않더라도 FPolicy 서버에 많은 수의 알림이 전송됩니다.

클라이언트에서 특정 파일에 대한 첫 번째 읽기/쓰기 요청을 받으면 캐시 항목이 생성되고 읽기/쓰기 횟수가 증가합니다. 이 요청은 첫 번째 읽기/쓰기 작업으로 표시되며 FPolicy 이벤트가 생성됩니다. NFS 클라이언트에 대한 FPolicy 필터를 계획하고 생성하기 전에 FPolicy 필터 작동 방식에 대한 기본 사항을 이해해야 합니다.

- First-read: 첫 번째 읽기에 대한 클라이언트 읽기 요청을 필터링합니다.

  NFS 이벤트에 이 필터를 사용하면 '-file-session-io-grouping-count' 및 '-file-session-io-grouping-duration' 설정에 따라 FPolicy가 처리되는 첫 번째 읽기 요청이 결정됩니다.

- First-write: 첫 번째 쓰기에 대한 클라이언트 쓰기 요청을 필터링합니다.

  NFS 이벤트에 이 필터를 사용하면 '-file-session-io-grouping-count' 및 '-file-session-io-grouping-duration' 설정에 따라 FPolicy가 처리하는 첫 번째 쓰기 요청이 결정됩니다.

다음 옵션은 NFS 서버 데이터베이스에 추가됩니다.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

ONTAP SVM에 대한 **NFSv4.1** 서버 구현 **ID** 수정

NFSv4.1 프로토콜에는 서버 도메인, 이름 및 날짜를 문서화하는 서버 구현 ID가 포함됩니다. 서버 구현 ID 기본값을 수정할 수 있습니다. 예를 들어, 사용 통계를 수집하거나 상호 운용성 문제를 해결하는 경우 기본값을 변경하면 유용합니다. 자세한 내용은 RFC 5661을 참조하십시오.

이 작업에 대해

세 옵션의 기본값은 다음과 같습니다.

옵션을 선택합니다	옵션 이름입니다	기본값
NFSv4.1 구현 ID 도메인	'-v4.1-구현도메인'	NetApp.com
NFSv4.1 구현 ID 이름	'-v4.1-구현명'	클러스터 버전 이름입니다
NFSv4.1 구현 ID 날짜	'-v4.1-구현일'	클러스터 버전 날짜입니다

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

NFSv4.1 구현 **ID**를 수정하려는 경우…	명령 입력…
도메인	'vserver nfs modify-v4.1-imImplementation-domain domain'
이름	'vserver nfs modify-v4.1-im구현-name 이름'
날짜	'vserver nfs modify-v4.1-dimImplementation-date date

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

NFSv4 ACL 관리

ONTAP SVM에 대한 **NFSv4 ACL** 활성화의 이점에 대해 알아보세요**.**

NFSv4 ACL을 설정하면 많은 이점이 있습니다.

NFSv4 ACL을 설정하면 다음과 같은 이점이 있습니다.

- 파일 및 디렉토리에 대한 사용자 액세스를 세밀하게 제어합니다
- NFS 보안 강화
- CIFS와의 상호 운용성 향상
- 사용자당 16개 그룹의 NFS 제한을 제거합니다

ONTAP SVM에 대한 **NFSv4 ACL**에 대해 알아보세요

NFSv4 ACL을 사용하는 클라이언트는 시스템의 파일 및 디렉토리에 대한 ACL을 설정하고 볼 수 있습니다. 새 파일 또는 하위 디렉토리가 ACL이 있는 디렉토리에 생성되면 새 파일 또는 하위 디렉토리는 적절한 상속 플래그로 태그가 지정된 ACL의 모든 ACE(액세스 제어 항목)를 상속합니다.

NFSv4 요청의 결과로 파일이나 디렉토리가 생성되면 결과 파일 또는 디렉토리의 ACL은 파일 생성 요청에 ACL이 포함되는지, 표준 UNIX 파일 액세스 권한만 포함되는지, 상위 디렉토리에 ACL이 있는지 여부에 따라 달라집니다.

- 요청에 ACL이 포함된 경우 해당 ACL이 사용됩니다.
- 요청에 표준 UNIX 파일 액세스 권한만 포함되어 있지만 상위 디렉토리에 ACL이 있는 경우 ACE에 적절한 상속 플래그가 지정된 경우 상위 디렉토리의 ACL에 있는 ACE는 새 파일 또는 디렉토리에 의해 상속됩니다.

  상위 ACL은 '-v4.0-acl'이 'off'로 설정되어 있어도 상속된다.

- 요청에 표준 UNIX 파일 액세스 권한만 있고 상위 디렉토리에 ACL이 없는 경우 클라이언트 파일 모드를 사용하여 표준 UNIX 파일 액세스 권한을 설정합니다.

- 요청에 표준 UNIX 파일 액세스 권한만 있고 상위 디렉토리에 상속할 수 없는 ACL이 있는 경우 새 객체는 모드 비트로만 생성됩니다.

> 매개 변수가 또는 `vserver export-policy rule` 패밀리의 명령을 사용하여 `vserver nfs` 로 `restricted` 설정된 경우 `-chown-mode` NFSv4 ACL을 사용하여 설정된 온디스크 사용 권한이 루트 사용자가 파일 소유권을 변경할 수 있는 경우에도 수퍼 사용자만 파일 소유권을 변경할 수 있습니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다" 참조하십시오.

ONTAP SVM에 대한 **NFSv4 ACL** 수정을 활성화하거나 비활성화합니다.

ONTAP가 ACL이 있는 파일 또는 디렉토리에 대해 'chmod' 명령을 수신하면 기본적으로 ACL이 유지되고 모드 비트 변경을 반영하도록 수정됩니다. 대신 ACL을 삭제하고자 하는 경우 동작을 변경하기 위해 '-v4-acl-preserve' 파라미터를 비활성화할 수 있습니다.

이 작업에 대해

통합 보안 스타일을 사용할 때 이 매개 변수는 클라이언트가 파일 또는 디렉터리에 대해 chmod, chgroup 또는 chown 명령을 보낼 때 NTFS 파일 권한을 보존할지 또는 삭제할지 여부도 지정합니다.

이 매개 변수의 기본값은 활성화되어 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다…
기존 NFSv4 ACL 보존 및 수정 설정(기본값)	'vserver nfs modify -vserver vserver_name -v4-acl-preserve enabled'
모드 비트를 변경할 때 NFSv4 ACL을 보존하고 삭제합니다	'vserver nfs modify -vserver vserver_name -v4-acl-preserve disabled'

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

ONTAP이 **NFSv4 ACL**을 사용하여 파일을 삭제할 수 있는지 여부를 확인하는 방법을 알아보세요.

파일을 삭제할 수 있는지 여부를 확인하기 위해 ONTAP에서는 파일의 삭제 비트와 포함하는 디렉토리의 delete_child 비트를 함께 사용합니다. 자세한 내용은 NFS 4.1 RFC 5661을 참조하십시오.

ONTAP SVM에 대한 **NFSv4 ACL** 활성화 또는 비활성화

NFSv4 ACL을 설정하거나 해제하려면 '-v4.0-acl' 및 '-v4.1-acl' 옵션을 수정할 수 있습니다. 이러한 옵션은 기본적으로 비활성화되어 있습니다.

이 작업에 대해

'-v4.0-acl' 또는 '-v4.1-acl' 옵션은 NFSv4 ACL의 설정 및 보기를 제어하지만 액세스 검사를 위해 이러한 ACL의 적용을 제어하지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	그러면…
NFSv4.0 ACL을 설정합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.0 -acl enabled'
NFSv4.0 ACL을 해제합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.0 -acl disabled'
NFSv4.1 ACL을 활성화합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.1 -acl enabled'
NFSv4.1 ACL을 해제합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.1 -acl disabled'

ONTAP SVM에 대한 **NFSv4 ACL**의 최대 **ACE** 제한 수정

매개 변수 '-v4-acl-max-aces'를 수정하여 각 NFSv4 ACL에 대해 허용되는 최대 ACE 수를 수정할 수 있습니다. 기본적으로 이 제한은 각 ACL에 대해 400개의 ACE로 설정됩니다. 이 제한을 늘리면 400개 이상의 ACE가 포함된 ACL을 사용하여 ONTAP를 실행하는 스토리지 시스템으로 데이터를 성공적으로 마이그레이션할 수 있습니다.

이 작업에 대해

이 제한을 늘리면 NFSv4 ACL을 사용하여 파일을 액세스하는 클라이언트의 성능에 영향을 줄 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. NFSv4 ACL의 최대 ACE 제한 수정:

   'vserver nfs modify -v4-acl-max-aces max_ace_limit'

의 유효한 범위

최대 에이스 한계는 192에서 1024로

3. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

NFSv4 파일 위임을 관리합니다

ONTAP SVM에 대한 **NFSv4** 읽기 파일 위임을 활성화하거나 비활성화합니다**.**

NFSv4 읽기 파일 위임을 설정하거나 해제하려면 "-v4.0-read-delegation' 또는 '-v4.1-read-delegation' 옵션을 수정할 수 있습니다. 읽기 파일 위임을 사용하면 파일 열기 및 닫기와 관련된 메시지 오버헤드를 상당 정도 제거할 수 있습니다.

이 작업에 대해

기본적으로 읽기 파일 위임은 사용되지 않습니다.

읽기 파일 위임을 설정할 경우 서버 재부팅 또는 재시작, 클라이언트 재부팅 또는 재시작, 네트워크 파티션 발생 후 서버와 클라이언트에서 위임을 복구해야 한다는 단점이 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	그러면…
NFSv4 읽기 파일 위임을 설정합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled'
NFSv4.1 읽기 파일 위임을 사용하도록 설정합니다	다음 명령을 입력합니다. + 'vserver NFS modify -vserver vserver_name -v4.1 -read -delegation enabled'
NFSv4 읽기 파일 위임을 해제합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled'
NFSv4.1 읽기 파일 위임을 사용하지 않도록 설정합니다	다음 명령을 입력합니다. 'vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled'

결과

파일 위임 옵션은 변경되자마자 적용됩니다. NFS를 재부팅하거나 다시 시작할 필요가 없습니다.

ONTAP SVM에 대한 **NFSv4** 쓰기 파일 위임을 활성화하거나 비활성화합니다.

쓰기 파일 위임을 설정하거나 해제하려면 "-v4.0-write-delegation' 또는 '-v4.1-write-delegation' 옵션을 수정할 수 있습니다. 쓰기 파일 위임을 사용하면 파일 열기 및 닫기 외에도 파일 및 레코드 잠금과 관련된 메시지 오버헤드를 상당 정도 제거할 수 있습니다.

이 작업에 대해

기본적으로 쓰기 파일 위임은 사용되지 않습니다.

쓰기 파일 위임을 설정할 경우 서버 재부팅 또는 재시작, 클라이언트 재부팅 또는 재시작, 네트워크 파티션 발생 후 위임을 복구하려면 서버와 해당 클라이언트가 추가 작업을 수행해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	그러면...
NFSv4 쓰기 파일 위임을 설정합니다	'vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled' 명령을 입력합니다
NFSv4.1 쓰기 파일 위임을 사용하도록 설정합니다	'vserver NFS modify -vserver vserver_name -v4.1 -write-delegation enabled' 명령을 입력합니다
NFSv4 쓰기 파일 위임을 해제합니다	'vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled' 명령을 입력합니다
NFSv4.1 쓰기 파일 위임을 사용하지 않도록 설정합니다	'vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled' 명령을 입력합니다

결과

파일 위임 옵션은 변경되자마자 적용됩니다. NFS를 재부팅하거나 다시 시작할 필요가 없습니다.

NFSv4 파일을 구성하고 잠금을 기록합니다

ONTAP SVM에 대한 **NFSv4** 파일 및 레코드 잠금에 대해 알아보세요.

NFSv4 클라이언트의 경우 ONTAP는 NFSv4 파일 잠금 메커니즘을 지원하여 임대 기반 모델에서 모든 파일 잠금의 상태를 유지합니다.

"NetApp 기술 보고서 3580: NFSv4 향상 및 모범 사례 가이드 Data ONTAP 구축"

ONTAP SVM에 대한 **NFSv4** 잠금 임대 기간 지정

NFSv4 잠금 임대 기간(즉, ONTAP가 클라이언트에 잠금을 부여하는 기간)을 지정하려면 '-v4-lease-seconds' 옵션을 수정할 수 있습니다. 리스 기간이 짧을수록 서버 복구 속도가 빨라지며 리스 기간이 길면 매우 많은 양의 클라이언트를 처리하는 서버에 유용합니다.

이 작업에 대해

기본적으로 이 옵션은 30으로 설정되어 있습니다. 이 옵션의 최소값은 10입니다. 이 옵션의 최대값은 'locking.lease_seconds' 옵션으로 설정할 수 있는 locking grace 기간입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 명령을 입력합니다.

   'vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds'

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

ONTAP SVM에 대한 **NFSv4** 잠금 유예 기간 지정

NFSv4 잠금 유예 기간(즉, 서버 복구 중에 클라이언트가 ONTAP에서 잠금 상태를 복구하려는 기간)을 지정하려면 "-v4-grace-seconds" 옵션을 수정할 수 있습니다.

이 작업에 대해

기본적으로 이 옵션은 45로 설정되어 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 명령을 입력합니다.

   'vserver nfs modify -vserver vserver_name -v4-grace-seconds_number_of_seconds _'

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

ONTAP SVM에 대한 **NFSv4** 참조에 대해 알아보세요

NFSv4 조회를 설정하면 ONTAP는 NFSv4 클라이언트에 ""intra-SVM" 조회를 제공합니다. SVM 내 의뢰는 NFSv4 요청을 수신하는 클러스터 노드가 SVM(스토리지 가상 머신)의 다른 논리 인터페이스(LIF)에 NFSv4 클라이언트를 참조하는 경우를 말합니다.

NFSv4 클라이언트는 해당 시점부터 타겟 LIF에서 조회 대상이 된 경로를 액세스해야 합니다. 원래 클러스터 노드는 SVM에 데이터 볼륨이 상주하는 클러스터 노드에 상주하는 LIF가 존재한다고 판단하여 클라이언트가 데이터에 더 빠르게 액세스하고 추가 클러스터 통신을 피할 수 있게 해줍니다.

ONTAP SVM에 대한 NFSv4 참조 활성화 또는 비활성화

'-v4-fsid-change' 및 '-v4.0-referral' 또는 '-v4.1-referral' 옵션을 활성화하여 스토리지 가상 시스템(SVM)에서 NFSv4 조회를 설정할 수 있습니다. NFSv4 조회를 설정하면 이 기능을 지원하는 NFSv4 클라이언트에 대한 데이터 액세스 속도가 빨라집니다.

시작하기 전에

NFS 조회를 설정하려면 먼저 parallel NFS를 해제해야 합니다. 동시에 둘 다 활성화할 수 없습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력…
NFSv4 조회를 설정합니다	'vserver nfs modify -vserver vserver_name -v4 -fsid -change enabled"vserver nfs modify -vserver vserver vserver_name -v4.0 -referral enabled'
NFSv4 조회를 해제합니다	'vserver nfs modify -vserver vserver_name -v4.0 -referral disabled'
NFSv4.1 조회를 사용하도록 설정합니다	'vserver nfs modify -vserver vserver_name -v4 -fsid -change enabled"vserver nfs modify -vserver vserver vserver_name -v4.1 -referral enabled'
NFSv4.1 조회를 비활성화합니다	'vserver nfs modify -vserver vserver_name -v4.1 -referral disabled'

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

ONTAP NFS SVM에 대한 통계 표시

스토리지 시스템에서 SVM(스토리지 가상 머신)에 대한 NFS 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

단계

1. 'tistics catalog object show' 명령을 사용하여 데이터를 볼 수 있는 NFS 객체를 식별합니다.

   '스타티틱스 카탈로그 객체 표시 - 객체 NFS *'

2. 자폐 시작 및 선택적 '자폐 중지' 명령을 사용하여 하나 이상의 객체에서 데이터 샘플을 수집합니다.
3. 'tortisics show' 명령어를 사용해 예시 데이터를 볼 수 있다.

예**: NFSv3** 성능 모니터링

다음 예제에는 NFSv3 프로토콜의 성능 데이터가 나와 있습니다.

다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

다음 명령을 실행하면 성공한 읽기 및 쓰기 요청 수와 총 읽기 및 쓰기 요청 수를 보여 주는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    --------------------------- ---------------------------
    read_success                                40042
    read_total                                  40042
    write_success                             1492052
    write_total                               1492052
```

관련 정보

- "성능 모니터링 설정"
- "통계 카탈로그 객체 표시"
- "통계에 따르면"
- "통계 시작"
- "통계 중지"

ONTAP NFS SVM에 대한 **DNS** 통계 표시

스토리지 시스템에서 SVM(스토리지 가상 머신)에 대한 DNS 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

단계

1. 'tortisics catalog object show' 명령어를 사용하여 데이터를 볼 수 있는 DNS 객체를 확인할 수 있다.

   '통계 카탈로그 객체 표시 - 객체 EXTERNAL_SERVICE_op *'

2. 자폐 시작, 자폐 중지 명령을 사용하여 하나 이상의 객체에서 데이터 샘플을 수집합니다.

3. 'tortisics show' 명령어를 사용해 예시 데이터를 볼 수 있다.

DNS 통계 모니터링

다음 예에서는 DNS 쿼리에 대한 성능 데이터를 보여 줍니다. 다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

다음 명령을 실행하면 전송된 DNS 쿼리 수와 수신, 실패 또는 제한 시간이 초과된 DNS 쿼리 수를 비교하여 표시하는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

다음 명령을 실행하면 특정 서버의 DNS 쿼리에 대해 특정 오류가 수신된 횟수를 표시하는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

관련 정보

- "성능 모니터링 설정"
- "통계 카탈로그 객체 표시"
- "통계에 따르면"
- "통계 시작"
- "통계 중지"

ONTAP NFS SVM에 대한 NIS 통계 표시

스토리지 시스템에 SVM(스토리지 가상 머신)에 대한 NIS 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

단계

1. 'tortisics catalog object show' 명령을 사용하여 데이터를 볼 수 있는 NIS 객체를 식별합니다.

   '통계 카탈로그 객체 표시 - 객체 EXTERNAL_SERVICE_op *'

2. 자폐 시작, 자폐 중지 명령을 사용하여 하나 이상의 객체에서 데이터 샘플을 수집합니다.
3. 'tortisics show' 명령어를 사용해 예시 데이터를 볼 수 있다.

NIS 통계 모니터링

다음 예에서는 NIS 쿼리에 대한 성능 데이터를 보여 줍니다. 다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

다음 명령을 실행하면 전송된 NIS 쿼리 수와 수신, 실패 또는 시간 초과 NIS 쿼리 수를 비교하여 보여 주는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

다음 명령을 실행하면 특정 서버의 NIS 쿼리에 대해 특정 오류가 수신된 횟수를 보여 주는 카운터를 지정하여 샘플의 데이터가 표시됩니다.

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                            YP_NOTFOUND
    server_ip_address                                    10.227.13.221
3 entries were displayed.
```

관련 정보

- "성능 모니터링 설정"
- "통계 카탈로그 객체 표시"
- "통계에 따르면"
- "통계 시작"
- "통계 중지"

ONTAP NFS를 통한 **VMware vStorage** 지원에 대해 알아보세요

ONTAP는 NFS 환경에서 특정 VMware VAAI(vStorage APIs for Array Integration) 기능을 지원합니다.

지원되는 기능

지원되는 기능은 다음과 같습니다.

- 복사본 오프로드

  ESXi 호스트에서 호스트를 사용하지 않고 소스 및 대상 데이터 저장소 위치 간에 직접 VMDK(가상 머신 또는 가상 머신 디스크)를 복제할 수 있습니다. 이렇게 하면 ESXi 호스트 CPU 주기와 네트워크 대역폭이 절약됩니다. 복제 오프로드는 소스 볼륨이 스파스 상태인 경우 공간 효율성을 유지합니다.

- 공간 예약

  VMDK 파일용 공간을 예약하여 스토리지 공간을 보장합니다.

제한 사항

VMware vStorage over NFS에는 다음과 같은 제한 사항이 있습니다.

- 다음과 같은 경우 복사 오프로드 작업이 실패할 수 있습니다.
  - 소스 또는 타겟 볼륨에서 웨이브다리미를 실행하는 동안 일시적으로 볼륨이 오프라인 상태가 되기 때문입니다
  - 소스 또는 타겟 볼륨을 이동하는 동안
  - 소스 또는 타겟 LIF를 이동하는 동안
  - Takeover 또는 Giveback 작업을 수행하는 동안
  - 스위치오버 또는 스위치백 작업을 수행하는 동안
- 다음 시나리오에서 파일 핸들 형식의 차이로 인해 서버 측 복제가 실패할 수 있습니다.

  Qtree를 내보낸 적이 없는 SVM으로 현재 또는 이전에 qtree를 내보낸 SVM에서 데이터를 복사하려고 합니다. 이러한 제한 사항을 해결하려면 대상 SVM에서 qtree를 하나 이상 내보낼 수 있습니다.

관련 정보

"Data ONTAP에서 지원하는 VAAI 오프로드 작업은 무엇입니까?"

ONTAP NFS를 통한 **VMware vStorage** 활성화 또는 비활성화

"vserver NFS modify" 명령을 사용하여 SVM(스토리지 가상 머신)에서 VMware vStorage over NFS에 대한 지원을 설정하거나 해제할 수 있습니다.

이 작업에 대해

기본적으로 VMware vStorage over NFS에 대한 지원은 비활성화되어 있습니다.

단계

1. SVM에 대한 현재 vStorage 지원 상태 표시:

   'vserver nfs show -vserver vserver_name -instance'

2. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
VMware vStorage 지원을 설정합니다	'vserver nfs modify -vserver vserver_name -vStorage enabled'
VMware vStorage 지원을 사용하지 않도록 설정합니다	'vserver nfs modify -vserver vserver_name -vStorage disabled'

작업을 마친 후

이 기능을 사용하려면 먼저 VMware VAAI용 NFS 플러그인을 설치해야 합니다. 자세한 내용은 _VMware VAAI_용 NetApp NFS 플러그인 설치 를 참조하십시오.

관련 정보

"NetApp 설명서: VMware VAAI용 NetApp NFS 플러그인"

ONTAP NFS SVM에서 **rquota** 지원 활성화 또는 비활성화

원격 할당량 프로토콜(rquota)을 사용하면 NFS 클라이언트가 원격 시스템에서 사용자에 대한 할당량 정보를 얻을 수 있습니다. rquota 버전에 대한 지원은 ONTAP 버전에 따라 다릅니다.

- rquota v1은 ONTAP 9 이상에서 지원됩니다.
- rquota v2는 ONTAP 9.12.1 이상에서 지원됩니다.

  rquota v1에서 rquota v2로 업그레이드하면 사용자 할당량 한도에 예상치 못한 변경 사항이 나타날 수 있습니다. 이러한 변경 사항은 rquota v1과 rquota v2의 할당량 계산 방식의 차이로 인해 발생합니다. 자세한 내용은 다음을 참조하세요."NetApp 기술 자료: 사용자 할당량 제한이 예기치 않게 변경된 이유는 무엇입니까?" .

이 작업에 대해

기본적으로 rquota는 비활성화되어 있습니다.

단계

1. rquota 설정 또는 해제:

원하는 작업	다음 명령을 입력합니다...
SVM에 대해 rquota 지원을 설정합니다	`vserver nfs modify -vserver vserver_name -rquota enable`
SVM에 대한 rquota 지원을 비활성화합니다	`vserver nfs modify -vserver vserver_name -rquota disable`

   할당량에 대한 자세한 내용은 을 참조하십시오 "논리적 스토리지 관리".

ONTAP SVM의 **NFSv3** 및 **NFSv4** 성능 개선 사항과 **TCP** 전송 크기에 대해 알아보세요**.**

TCP 최대 전송 크기를 수정하여 지연 시간이 긴 네트워크를 통해 스토리지 시스템에 접속하는 NFSv3 및 NFSv4 클라이언트의 성능을 향상시킬 수 있습니다.

클라이언트가 지연 시간이 10밀리초 이상 인 WAN(Wide Area Network) 또는 MAN(Metro Area Network)과 같이 지연 시간이 긴 네트워크를 통해 스토리지 시스템에 액세스하는 경우 TCP 최대 전송 크기를 수정하여 연결 성능을 향상시킬 수 있습니다. LAN(Local Area Network)과 같이 지연 시간이 짧은 네트워크에서 스토리지 시스템에 액세스하는 클라이언트는 이러한 매개 변수를 수정해도 거의 이점을 얻을 수 없습니다. 처리량 향상이 지연 시간에 미치는 영향을 상쇄하지 않는다면 이러한 매개 변수를 사용해서는 안 됩니다.

스토리지 환경에서 이러한 매개 변수를 수정하여 이점을 얻을 수 있는지 확인하려면 먼저 성능이 떨어지는 NFS 클라이언트에 대한 포괄적인 성능 평가를 수행해야 합니다. 낮은 성능이 클라이언트에 대한 과도한 라운드 트립 지연 및 작은 요청 때문인지 검토합니다. 이러한 조건에서는 클라이언트와 서버가 사용 가능한 대역폭을 완전히 사용할 수 없습니다. 왜냐하면 대부분의 듀티 사이클이 연결을 통해 전송되는 작은 요청과 응답을 대기하는 데 소비하기

때문입니다.

NFSv3 및 NFSv4 요청 크기를 늘리면 클라이언트 및 서버에서 사용 가능한 대역폭을 보다 효율적으로 사용하여 단위 시간당 더 많은 데이터를 이동할 수 있으므로 연결의 전반적인 효율성이 향상됩니다.

스토리지 시스템과 클라이언트 간의 구성은 달라질 수 있습니다. 스토리지 시스템과 클라이언트는 전송 작업에 대해 최대 1MB의 크기를 지원합니다. 그러나 스토리지 시스템이 1MB의 최대 전송 크기를 지원하도록 구성했지만 클라이언트가 64KB만 지원하는 경우 마운트 전송 크기는 64KB 이하로 제한됩니다.

이러한 매개변수를 수정하기 전에 대용량 응답을 조립하고 전송하는 데 필요한 기간 동안 스토리지 시스템에 메모리가 추가로 소비된다는 점을 염두에 두어야 합니다. 스토리지 시스템에 대한 대기 시간이 많을수록 추가 메모리 소비량이 증가합니다. 메모리 용량이 큰 스토리지 시스템은 이 변경으로 인해 거의 영향을 주지 않을 수 있습니다. 메모리 용량이 낮은 스토리지 시스템에서 눈에 띄는 성능 저하가 발생할 수 있습니다.

이 매개 변수를 사용하는 것은 클러스터의 여러 노드에서 데이터를 검색하는 기능에 달려 있습니다. 클러스터 네트워크의 지연으로 인해 전반적인 응답 시간이 길어질 수 있습니다. 이러한 매개 변수를 사용하면 전반적인 지연 시간이 증가하는 경향이 있습니다. 따라서 지연 시간에 민감한 워크로드에 부정적인 영향이 나타날 수 있습니다.

ONTAP SVM에 대한 **NFSv3** 및 **NFSv4 TCP** 최대 전송 크기 수정

NFSv3 및 NFSv4.x 프로토콜을 사용하여 모든 TCP 연결에 대해 최대 전송 크기를 구성하려면 '-tcp-max-xfer-size' 옵션을 수정할 수 있습니다.

이 작업에 대해

각 SVM(스토리지 가상 머신)별로 이러한 옵션을 개별적으로 수정할 수 있습니다.

ONTAP 9부터 v3-tcp-max-read-size와 v3-tcp-max-write-size 옵션은 더 이상 사용되지 않습니다. 대신 '-tcp-max-xfer-size' 옵션을 사용해야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
NFSv3 또는 NFSv4 TCP 최대 전송 크기를 수정합니다	'vserver nfs modify -vserver vserver_name -tcp -max -xfer-size integer_max_xfer_size'

옵션을 선택합니다	범위	기본값
'-tcp-max-xfer-size'를 선택합니다	8192 ~ 1048576바이트	65536바이트

> 입력하는 최대 전송 크기는 4KB(4096바이트)의 배수여야 합니다. 제대로 정렬되지 않은 요청은 성능에 부정적인 영향을 줍니다.

3. 'vserver nfs show-fields tcp-max-xfer-size' 명령을 사용하여 변경 사항을 확인합니다.

4. 클라이언트가 정적 마운트를 사용하는 경우 새 매개 변수 크기를 마운트 해제하고 다시 마운트하여 적용합니다.

예

다음 명령을 실행하면 이름이 VS1인 SVM에서 NFSv3 및 NFSv4.x TCP 최대 전송 크기가 1048576바이트로 설정됩니다.

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

ONTAP SVM에 대해 **NFS** 사용자에게 허용되는 그룹 **ID** 수를 구성합니다**.**

기본적으로 ONTAP는 Kerberos(RPCSEC_GSS) 인증을 사용하여 NFS 사용자 자격 증명을 처리할 때 최대 32개의 그룹 ID를 지원합니다. AUTH_SYS 인증을 사용하는 경우 RFC 5531에 정의된 대로 기본 최대 그룹 ID 수는 16입니다. 기본 그룹 수보다 많은 그룹의 구성원인 사용자가 있는 경우 최대 1,024개까지 늘릴 수 있습니다.

이 작업에 대해

사용자의 자격 증명에 기본 그룹 ID 수보다 많은 수의 그룹 ID가 있는 경우 나머지 그룹 ID가 잘리고 스토리지 시스템에서 파일을 액세스하려고 할 때 오류가 발생할 수 있습니다. SVM당 최대 그룹 수를 환경의 최대 그룹을 나타내는 숫자로 설정해야 합니다.

> 확장 그룹을 활성화하기 위한 AUTH_SYS 인증 전제 조건을 이해하려면(`-auth-sys-extended-groups`) 기본 최대값인 16을 초과하는 그룹 ID를 사용하는 경우 다음을 참조하십시오."NetApp 지식 기반: auth-sys-extended-groups를 활성화하기 위한 전제 조건은 무엇입니까?"

다음 표는 세 가지 샘플 구성에서 최대 그룹 ID 수를 결정하는 "vserver NFS modify" 명령의 두 가지 매개 변수를 보여 줍니다.

매개 변수	설정	결과 그룹 ID 제한
'-확장-그룹-제한' ``auth-sys-extended-groups''	32인치 '비활성화'입니다 기본 설정입니다.	RPCSEC_GSS:32 AUTH_SYS:16
'-확장-그룹-제한' ``auth-sys-extended-groups''	256입니다 '비활성화'입니다	RPCSEC_GSS:256 AUTH_SYS:16
'-확장-그룹-제한' ``auth-sys-extended-groups''	512 "활성화됨"	RPCSEC_GSS:512 AUTH_SYS:512

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

허용된 보조 그룹의 최대 수를 설정하려면…	명령 입력…
RPCSEC_GSS에만 해당하고 AUTH_SYS는 기본값 16으로 설정된 상태로 둡니다	'vserver nfs modify -vserver vserver_name -extended-groups-limit{32-1024} -auth-sys-extended -groups disabled'
RPCSEC_GSS 및 AUTH_SYS의 경우	'vserver nfs modify -vserver vserver_name -extended-groups-limit{32-1024} -auth-sys-extended -groups enabled'

3. '-extended-groups-limit' 값을 확인하고 AUTH_SYS가 확장된 그룹('vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups, extended-groups-limit')을 사용하고 있는지 확인합니다
4. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

예

다음 예에서는 AUTH_SYS 인증에 대해 확장된 그룹을 활성화하고, AUTH_SYS 및 RPCSEC_GSS 인증에 대해 확장 그룹의 최대 수를 512로 설정합니다. 이러한 변경은 VS1 이라는 SVM에 액세스하는 클라이언트에만 적용됩니다.

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ ---------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

관련 정보

- "NetApp 기술 자료: ONTAP 9에 대한 NFS 인증을 위한 AUTH_SYS 확장 그룹 변경 사항"

ONTAP SVM에 대한 **NTFS** 보안 스타일 데이터에 대한 루트 사용자 액세스를 제어합니다.

NFS 클라이언트가 NTFS 보안 스타일 데이터에 액세스하고 NTFS 클라이언트가 NFS 보안 스타일 데이터에 액세스할 수 있도록 ONTAP를 구성할 수 있습니다. NFS 데이터 저장소에서 NTFS 보안 스타일을 사용하는 경우 루트 사용자가 액세스를 처리하는 방법을 결정하고 이에

따라 SVM(스토리지 가상 머신)을 구성해야 합니다.

이 작업에 대해

루트 사용자가 NTFS 보안 스타일 데이터에 액세스할 때 다음 두 가지 옵션이 있습니다.

- 다른 NFS 사용자와 마찬가지로 루트 사용자를 Windows 사용자에게 매핑하고 NTFS ACL에 따라 액세스를 관리합니다.
- NTFS ACL을 무시하고 루트에 대한 전체 액세스를 제공합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 원하는 작업을 수행합니다.

루트 사용자가 다음을 수행할 수 있도록 하려면…	명령 입력…
Windows 사용자에게 매핑되어야 합니다	'vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled'
NT ACL 검사를 생략합니다	'vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled'

   기본적으로 이 매개 변수는 사용되지 않습니다.

   이 매개 변수가 설정되어 있지만 루트 사용자에 대한 이름 매핑이 없는 경우 ONTAP에서는 감사를 위해 기본 SMB 관리자 자격 증명을 사용합니다.

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

지원되는 **NFS** 버전 및 클라이언트

지원되는 **ONTAP NFS** 버전 및 클라이언트에 대해 알아보세요

네트워크에서 NFS를 사용하려면 먼저 ONTAP가 지원하는 NFS 버전과 클라이언트를 알아야 합니다.

이 표에서는 ONTAP에서 주 및 부 NFS 프로토콜 버전이 기본적으로 지원되는 경우 설명합니다. 기본적으로 지원에서는 이 버전이 NFS 프로토콜을 지원하는 ONTAP의 최초 버전임을 표시하지 않습니다.

버전	지원	도입됨
NFSv3	예	모든 ONTAP 릴리스

버전	지원	도입됨
NFSv4.0	예	ONTAP 8 를 참조하십시오
NFSv4.1	예	ONTAP 8.1 를 참조하십시오
NFSv4.2	예	ONTAP 9.8
pNFS를 사용합니다	예	ONTAP 8.1 를 참조하십시오

ONTAP가 지원하는 NFS 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

"NetApp 상호 운용성 매트릭스 툴"

NFSv4.0 기능에 대한 **ONTAP** 지원에 대해 알아보세요

ONTAP는 SPKM3 및 LIPKEY 보안 메커니즘을 제외한 NFSv4.0의 모든 필수 기능을 지원합니다.

지원되는 NFSv4 기능은 다음과 같습니다.

- * 복합 *

  클라이언트가 단일 RPC(원격 프로시저 호출) 요청에서 여러 파일 작업을 요청할 수 있습니다.

- * 파일 위임 *

  서버가 읽기 및 쓰기 액세스를 위해 일부 유형의 클라이언트에 파일 제어를 위임할 수 있도록 합니다.

- * 의사 fs *

  NFSv4 서버에서 스토리지 시스템의 마운트 지점을 결정하는 데 사용됩니다. NFSv4에는 마운트 프로토콜이 없습니다.

- * 잠금 *

  임대 기반. NFSv4에는 별도의 NLM(Network Lock Manager) 또는 NSM(Network Status Monitor) 프로토콜이 없습니다.

NFSv4.0 프로토콜에 대한 자세한 내용은 RFC 3530을 참조하십시오.

NFSv4에 대한 **ONTAP** 지원 제한 사항에 대해 알아보세요**.**

NFSv4에 대한 ONTAP 지원의 몇 가지 제한 사항에 대해 알고 있어야 합니다.

- 위임 기능은 모든 클라이언트 유형에서 지원되지 않습니다.
- ONTAP 9.4 및 이전 릴리즈에서는 UTF8 볼륨 이외의 볼륨에 ASCII가 아닌 문자가 있는 이름이 스토리지 시스템에서 거부됩니다.

ONTAP 9.5 이상 릴리즈에서는 utf8mb4 언어 설정으로 생성하고 NFS v4를 사용하여 마운트된 볼륨이 더 이상 이 제한을 받지 않습니다.

- 모든 파일 핸들은 영구적이며, 서버는 휘발성 파일 핸들을 제공하지 않습니다.
- 마이그레이션 및 복제는 지원되지 않습니다.
- NFSv4 클라이언트는 읽기 전용 로드 공유 미러에서 지원되지 않습니다.

  ONTAP는 직접 읽기 및 쓰기 액세스를 위해 NFSv4 클라이언트를 로드 공유 미러 소스로 라우팅합니다.

- 명명된 특성은 지원되지 않습니다.
- 다음을 제외한 모든 권장 속성이 지원됩니다.
  - '보관'
  - '숨겨짐'
  - 동질성
  - 'mimetype'입니다
  - 쿼터쿼터_AVAIL_HARD를 선택합니다
  - 쿼터가용성 소프트
  - quota_used
  - '시스템'
  - Time_backup을 선택합니다

> "quota *" 특성은 지원하지 않지만 ONTAP는 RQUOTA Side Band 프로토콜을 통해 사용자 및 그룹 할당량을 지원합니다.

NFSv4.1에 대한 **ONTAP** 지원에 대해 알아보세요

ONTAP 9.8부터는 NFSv4.1이 활성화된 경우 기본적으로 nconnect 기능을 사용할 수 있습니다.

이전 버전의 NFS 클라이언트 구축에서는 마운트와 단일 TCP 연결만 사용합니다. ONTAP에서 단일 TCP 연결은 IOPS 증가에 따라 병목 현상을 일으킬 수 있습니다.

nconnect는 단일 마운트에 대해 여러 TCP 연결(최대 16개)을 허용하여 NFS 클라이언트 성능을 개선하고, IOPS가 증가함에 따라 단일 TCP 연결에서 발생할 수 있는 성능 병목 현상을 극복하는 데 도움이 됩니다.

NFSv4.1은 ONTAP 9.9.1 이상에서 기본적으로 활성화되어 있습니다. 이전 릴리즈에서는 SVM(스토리지 가상 머신)에서 NFS 서버를 생성할 때 '-v4.1' 옵션을 지정하고 이를 '사용'으로 설정하여 사용할 수 있습니다.

ONTAP는 NFSv4.1 디렉토리 및 파일 레벨 위임을 지원하지 않습니다.

관련 정보

"NFS 성능을 위한 nconnect에 대해 알아보세요".

NFSv4.2에 대한 **ONTAP** 지원에 대해 알아보세요

ONTAP 9.8부터 ONTAP는 NFSv4.2 사용 클라이언트에 대한 액세스를 허용하는 NFSv4.2 프로토콜을 지원합니다.

ONTAP 9.9.1 이상에서는 NFSv4.2가 기본적으로 활성화되어 있습니다. ONTAP 9.8에서는 다음을 지정하여 v4.2를 수동으로 활성화해야 합니다. `-v4.2` 옵션 및 설정 `enabled` 스토리지 가상 머신(SVM)에 NFS 서버를 생성할 때. NFSv4.1을 활성화하면 클라이언트가 v4.2로 마운트된 동안에도 NFSv4.1 기능을 사용할 수 있습니다.

연속적인 ONTAP 릴리즈는 NFSv4.2 옵션 기능에 대한 지원을 확장합니다.

다음으로 시작...	**NFSv4.2**의 옵션 기능은 다음과 같습니다.
ONTAP 9.12.1	• NFS 확장 속성입니다 • Sparse 파일 • 공간 예약
ONTAP 9.9.1	MAC(Mandatory Access Control) 레이블 NFS

NFS v4.2 보안 레이블

ONTAP 9.9.1부터 NFS 보안 레이블을 활성화할 수 있습니다. 기본적으로 비활성화되어 있습니다.

NFS v4.2 보안 레이블에서 ONTAP NFS 서버는 MAC(Mandatory Access Control)를 인식하여 클라이언트가 전송한 sec_label 특성을 저장 및 검색합니다.

자세한 내용은 을 참조하십시오 "RFC 7240".

ONTAP 9.12.1부터는 NDMP 덤프 작업에 NFS v4.2 보안 레이블이 지원됩니다. 이전 릴리즈의 파일 또는 디렉터리에서 보안 레이블이 발견되면 덤프가 실패합니다.

단계

1. 권한 설정을 고급으로 변경합니다.

```
set -privilege advanced
```

2. 보안 레이블 활성화:

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

NFS 확장 속성입니다

ONTAP 9.12.1부터 NFS 확장 특성(xattrs)이 기본적으로 사용하도록 설정됩니다.

확장 특성은 에 의해 정의된 표준 NFS 속성입니다 "RFC 8276" 최신 NFS 클라이언트에서 사용하도록 설정됩니다. 사용자 정의 메타데이터를 파일 시스템 객체에 연결하는 데 사용할 수 있으며 고급 보안 구축에 관심이 있습니다.

NFS 확장 속성은 현재 NDMP 덤프 작업에 지원되지 않습니다. 파일 또는 디렉토리에서 확장 속성이 발견되면 덤프는 진행되지만 해당 파일 또는 디렉토리의 확장 속성은 백업하지 않습니다.

확장 속성을 비활성화해야 하는 경우 를 사용하십시오 `vserver nfs modify -v4.2-xattrs disabled` 명령.

NFS 성능을 위한 nconnect에 대해 알아보세요

ONTAP 9.8부터 NFSv4.1이 활성화된 경우 nconnect 기능을 기본적으로 사용할 수 있습니다. nconnect는 단일 마운트에 대해 여러 TCP 연결을 허용하여 NFS 클라이언트 성능을 향상시킵니다.

nconnect 작동 방식

이전 버전의 NFS 클라이언트 구축에서는 마운트와 단일 TCP 연결만 사용합니다. ONTAP에서 단일 TCP 연결은 IOPS 증가에 따라 병목 현상을 일으킬 수 있습니다.

nconnect가 활성화된 클라이언트는 단일 NFS 마운트와 연관된 여러 TCP 연결(최대 16개)을 가질 수 있습니다. nconnect는 단 하나의 IP 주소만 사용하고 해당 단일 IP를 통해 여러 TCP 연결을 설정하여 NFS 내보내기를 마운트합니다. NFS 클라이언트는 파일 작업을 라운드 로빈 방식으로 여러 TCP 연결에 분산하여 사용 가능한 네트워크 대역폭에서 더 높은 처리량을 얻습니다.

지원되는 NFS 버전

- nconnect는 NFSv3, NFSv4.2 및 NFSv4.1 마운트에 권장됩니다.
- nconnect는 NFSv4.0 마운트에 권장되지 않습니다.

> 최적의 성능을 위해 NetApp NFSv4.0 대신 nconnect와 함께 NFSv4.1을 사용할 것을 권장합니다. NFSv4.0은 여러 연결을 지원하는 반면, nconnect를 탑재한 NFSv4.1은 더 나은 부하 분산과 향상된 처리량을 제공합니다.

고객 지원

nconnect가 클라이언트 버전에서 지원되는지 확인하려면 NFS 클라이언트 설명서를 참조하십시오.

관련 정보

- "NFSv4.1에 대한 ONTAP 지원에 대해 알아보세요"
- "NFSv4.2에 대한 ONTAP 지원에 대해 알아보세요"

병렬 NFS에 대한 ONTAP 지원에 대해 알아보세요

ONTAP는 pNFS(parallel NFS)를 지원합니다. pNFS 프로토콜은 클라이언트가 클러스터의 여러 노드에 분산된 파일 세트에 직접 액세스할 수 있도록 함으로써 성능을 개선합니다. 클라이언트가 볼륨에 대한 최적의 경로를 찾는 데 도움이 됩니다.

ONTAP NFS 하드 마운트에 대해 알아보세요

장착 문제를 해결할 때 올바른 장착 유형을 사용하고 있는지 확인해야 합니다. NFS는 소프트 마운트와 하드 마운트의 두 가지 마운트 유형을 지원합니다. 안정성을 위해 하드 마운트만

사용해야 합니다.

소프트 마운트를 사용하면 안 됩니다. 특히, NFS 시간 제한이 자주 발생할 가능성이 있습니다. 이러한 시간 초과로 인해 경합 상태가 발생하여 데이터가 손상될 수 있습니다.

병렬 NFS

소개

ONTAP 의 병렬 NFS(pNFS)에 대해 알아보세요

병렬 NFS는 2010년 1월 RFC-5661에 따라 RFC 표준으로 도입되었으며, 이를 통해 클라이언트가 메타데이터와 데이터 경로를 분리하여 NFSv4.1 서버의 파일 데이터에 직접 액세스할 수 있게 되었습니다. 이러한 직접 접근 방식은 데이터 현지화, CPU 효율성, 작업 병렬화를 통해 성능상의 이점을 제공합니다. 이후 2018년에는 pNFS 레이아웃 유형(RFC-8434)을 다루는 RFC가 작성되었으며, 이는 파일, 블록 및 객체 레이아웃에 대한 표준을 정의합니다. ONTAP pNFS 작업에 파일 레이아웃 유형을 활용합니다.

> 2024년 7월부터 이전에 PDF로 게시되었던 기술 보고서의 콘텐츠가 ONTAP 제품 문서에 통합되었습니다. ONTAP NFS 스토리지 관리 설명서에는 이제 _TR-4063: NetApp ONTAP의 병렬 네트워크 파일 시스템(pNFS)_의 내용이 포함되어 있습니다.

수년 동안 NFSv3는 거의 모든 사용 사례에 사용되는 NFS 프로토콜의 표준 버전이었습니다. 그러나 이 프로토콜에는 상태 저장 기능 부족, 기본적인 권한 모델, 기본 잠금 기능 등의 한계가 있었습니다. NFSv4.0(RFC 7530)은 NFSv3에 비해 여러 가지 개선 사항을 도입했으며, 병렬 NFS(pNFS)와 같은 기능이 추가된 후속 NFSv4.1(RFC 5661)과 NFSv4.2(RFC 7862) 버전에서 더욱 개선되었습니다.

NFSv4.x의 이점

NFSv4.x는 NFSv3에 비해 다음과 같은 이점을 제공합니다.

- NFSv4는 운영에 단일 포트(2049)만 사용하므로 방화벽에 친화적입니다.
- NFSv4.x의 위임과 같은 고급적이고 공격적인 캐시 관리
- 암호화를 사용하는 강력한 RPC 보안 선택
- 문자의 국제화
- 복합 연산
- TCP에서만 작동합니다
- 상태 저장 프로토콜(NFSv3와 같은 상태 비저장 프로토콜 아님)
- 효율적인 인증 메커니즘을 위한 전체 Kerberos 통합
- NFS 추천
- UNIX 및 Windows와 호환되는 액세스 제어 지원
- 문자열 기반 사용자 및 그룹 식별자
- pNFS(NFSv4.1)
- 확장된 속성(NFSv4.2)

- 보안 레이블(NFSv4.2)
- 스파스 파일 작업(FALLOCATE)(NFSv4.2)

모범 사례 및 기능에 대한 세부 정보를 포함하여 일반 NFSv4.x에 대한 자세한 내용은 다음을 참조하세요. "NetApp 기술 보고서 4067: NFS 모범 사례 및 구축 가이드".

관련 정보

- "NFS 구성 개요"
- "NFS 관리 개요"
- "FlexGroup 볼륨 관리"
- "NFS 트렁킹 개요"
- https://www.netapp.com/pdf.html?item=/media/19370-tr-4523.pdf
- "NetApp 기술 보고서 4616: ONTAP에서 Microsoft Active Directory와 NFS Kerberos"

ONTAP 의 **pNFS** 아키텍처에 대해 알아보세요

pNFS 아키텍처는 세 가지 주요 구성 요소로 구성됩니다. pNFS를 지원하는 NFS 클라이언트, 메타데이터 작업을 위한 전용 경로를 제공하는 메타데이터 서버, 파일에 대한 로컬 경로를 제공하는 데이터 서버입니다.

pNFS에 대한 클라이언트 액세스에는 NFS 서버에서 사용 가능한 데이터 및 메타데이터 경로에 대한 네트워크 연결이 필요합니다. NFS 서버에 클라이언트가 접근할 수 없는 네트워크 인터페이스가 포함되어 있는 경우, 서버는 접근할 수 없는 클라이언트에 대한 데이터 경로를 광고할 수 있으며, 이로 인해 중단이 발생할 수 있습니다.

메타데이터 서버

pNFS의 메타데이터 서버는 NFS 서버에서 pNFS가 활성화된 경우 클라이언트가 NFSv4.1 이상을 사용하여 마운트를 시작하면 설정됩니다. 이 작업이 완료되면 모든 메타데이터 트래픽이 이 연결을 통해 전송되고 인터페이스가 다른 노드로 마이그레이션되더라도 마운트 기간 동안 이 연결에 남아 있게 됩니다.

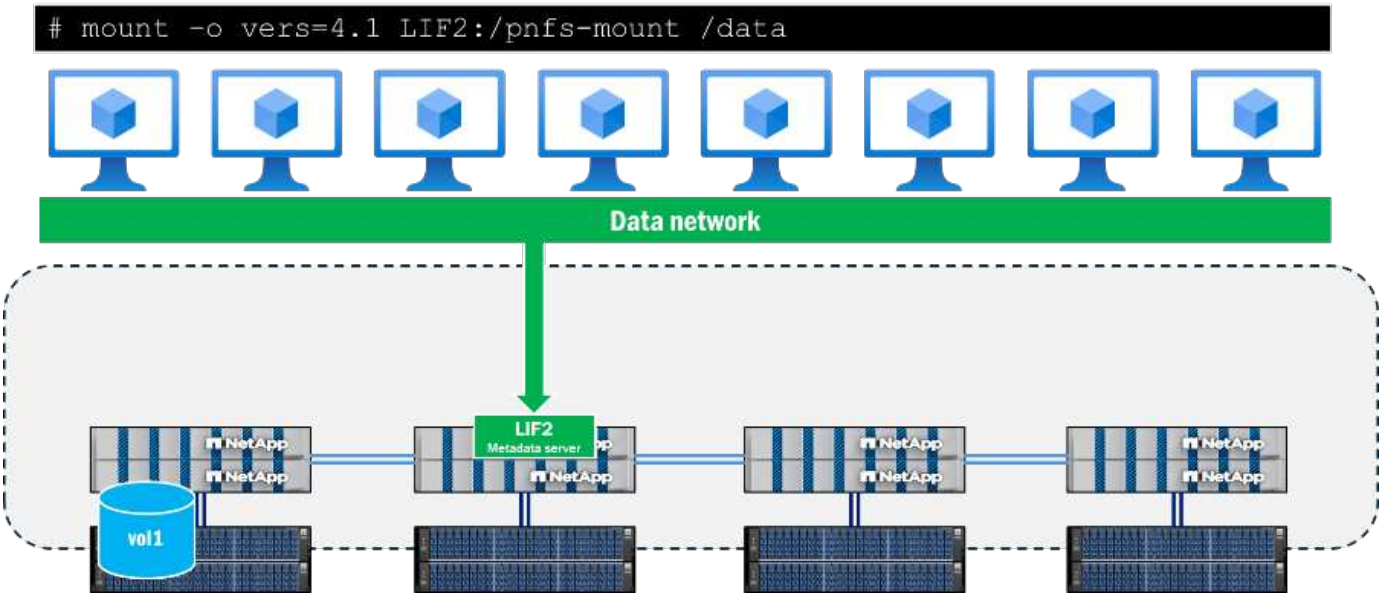


그림 **1. ONTAP** 에서 **pNFS**에 메타데이터 서버를 구축합니다.

pNFS 지원은 마운트 호출 중, 특히 EXCHANGE_ID 호출에서 결정됩니다. 이는 NFS 작업 아래의 패킷 캡처에서 플래그로 볼 수 있습니다. pNFS 플래그가 있는 경우 `EXCHGID4_FLAG_USE_PNFS_DS` 그리고 `EXCHGID4_FLAG_USE_PNFS_MDS` 1로 설정된 경우 해당 인터페이스는 pNFS에서 데이터 작업과 메타데이터 작업 모두에 적합합니다.

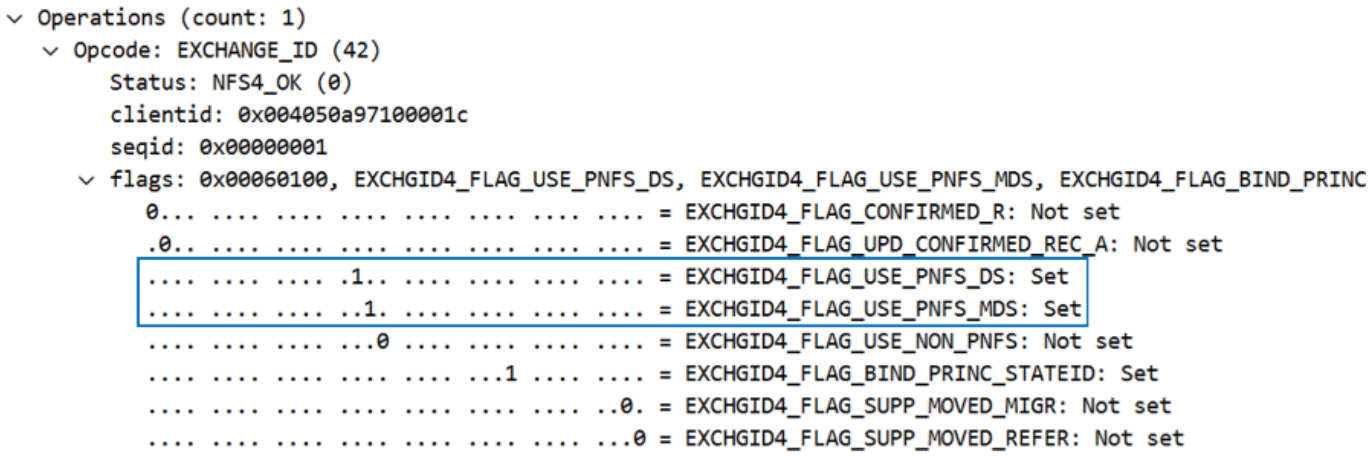


그림 **2. pNFS** 마운트를 위한 패킷 캡처

NFS의 메타데이터는 일반적으로 파일 핸들, 권한, 액세스 및 수정 시간, 소유권 정보와 같은 파일 및 폴더 속성으로 구성됩니다. 메타데이터에는 통화 생성 및 삭제, 통화 연결 및 연결 해제, 이름 변경 등이 포함될 수 있습니다.

pNFS에는 pNFS 기능에 특정한 메타데이터 호출 하위 집합도 있으며 이에 대해서는 다음에서 자세히 설명합니다. "RFC 5661". 이러한 호출은 pNFS 적격 장치, 데이터 세트에 대한 장치 매핑 및 기타 필요한 정보를 결정하는 데 사용됩니다. 다음 표는 이러한 pNFS 관련 메타데이터 작업 목록을 보여줍니다.

작동	설명
레이아웃	메타데이터 서버에서 데이터 서버 맵을 가져옵니다.
레이아웃커밋	서버는 레이아웃을 커밋하고 메타데이터 맵을 업데이트합니다.
레이아웃 반환	데이터가 수정된 경우 레이아웃이나 새 레이아웃을 반환합니다.
장치 정보 가져오기	클라이언트는 스토리지 클러스터의 데이터 서버에서 업데이트된 정보를 받습니다.
장치 목록 가져오기	클라이언트는 스토리지 클러스터에 참여하는 모든 데이터 서버 목록을 요청합니다.
CB_레이아웃리콜	충돌이 감지되면 서버는 클라이언트에서 데이터 레이아웃을 다시 호출합니다.
CB_리콜_ANY	모든 레이아웃을 메타데이터 서버로 반환합니다.
CB_알림_장치ID	장치 ID 변경 사항을 알립니다.

데이터 경로 정보

메타데이터 서버가 설정되고 데이터 작업이 시작되면 ONTAP pNFS 읽기 및 쓰기 작업에 적합한 장치 ID와 클러스터의 볼륨을 로컬 네트워크 인터페이스와 연결하는 장치 매핑을 추적하기 시작합니다. 이 프로세스는 마운트에서 읽기 또는 쓰기 작업이 수행될 때 발생합니다. 메타데이터 호출(예: `GETATTR`. 이러한 장치 매핑은 실행되지 않습니다. 따라서 실행 `ls` 마운트 지점 내부의 명령을 사용해도 매핑이 업데이트되지 않습니다.

아래와 같이 고급 권한으로 ONTAP CLI를 사용하여 장치와 매핑을 볼 수 있습니다.

```
::*> pnfs devices show -vserver DEMO
  (vserver nfs pnfs devices show)
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
DEMO             16              2157024470      available       1

::*> pnfs devices mappings show -vserver SVM
  (vserver nfs pnfs devices mappings show)
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
DEMO            16              2488            10.193.67.211
```

이 명령에는 볼륨 이름이 없습니다. 대신 해당 볼륨과 연관된 숫자 ID, 즉 마스터 세트 ID(MSID)와 데이터 세트 ID(DSID)가 사용됩니다. 매핑과 관련된 볼륨을 찾으려면 다음을 사용할 수 있습니다. `volume show -dsid [dsid_numeric]` 또는 `volume show -msid [msid_numeric]` ONTAP CLI의 고급 권한으로.

클라이언트가 메타데이터 서버 연결과 원격인 노드에 있는 파일을 읽거나 쓰려고 시도하면 pNFS는 해당 작업에 대한 데이터 로컬리티를 보장하기 위해 적절한 액세스 경로를 협상하고 클라이언트는 파일에 액세스하기 위해 클러스터 네트워크를 탐색하는 대신 광고된 pNFS 장치로 리디렉션합니다. 이렇게 하면 CPU 오버헤드와 네트워크 지연 시간을 줄이는 데 도움이 됩니다.

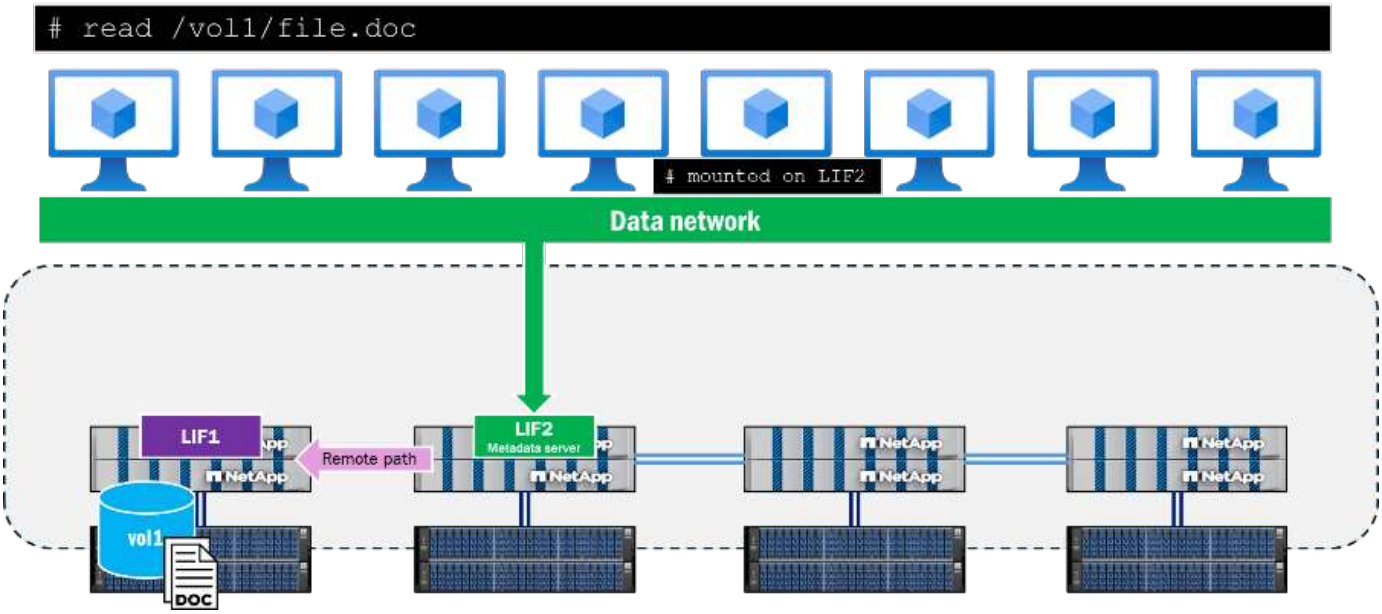


그림 **3. pNFS** 없이 **NFSv4.1**을 사용한 원격 읽기 경로

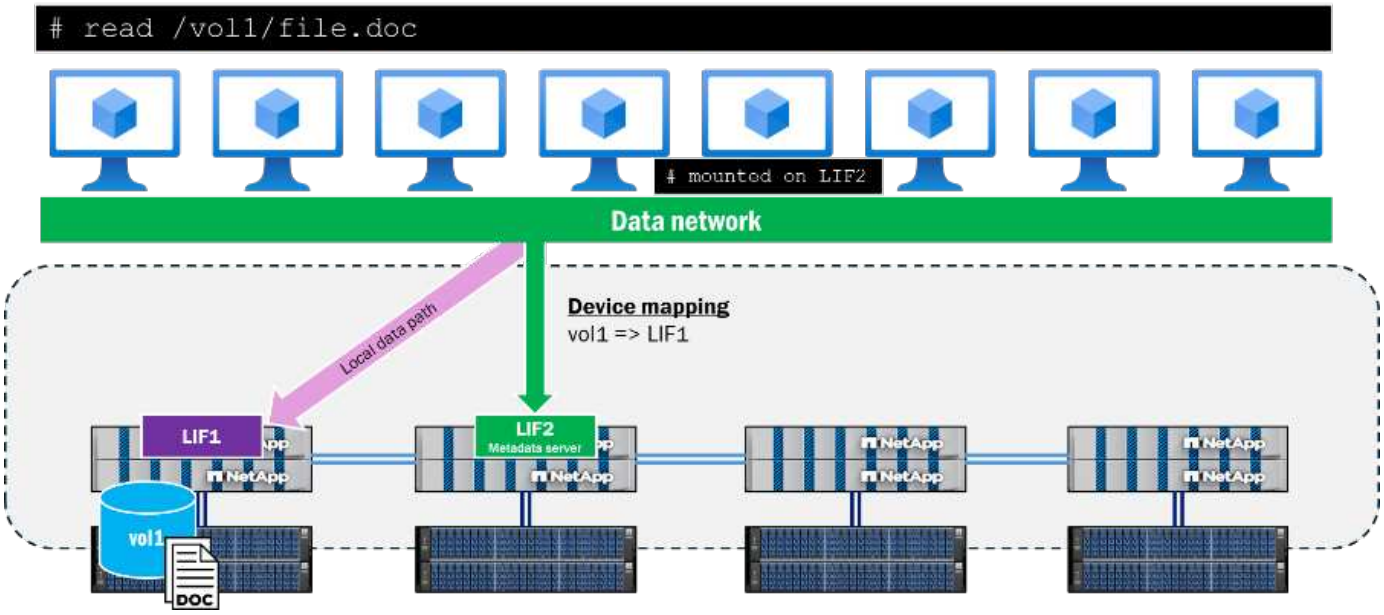


그림 **4. pNFS**를 사용한 로컬화된 읽기 경로

pNFS 제어 경로

pNFS의 메타데이터와 데이터 부분 외에도 pNFS 제어 경로도 있습니다. 제어 경로는 NFS 서버에서 파일 시스템 정보를 동기화하는 데 사용됩니다. ONTAP 클러스터에서 백엔드 클러스터 네트워크는 주기적으로 복제되어 모든 pNFS 장치와 장치 매핑이 동기화되도록 합니다.

pNFS 장치 채우기 워크플로

다음은 클라이언트가 볼륨의 파일을 읽거나 쓰라는 요청을 한 후 ONTAP 에서 pNFS 장치가 채워지는 방식을 설명합니다.

1. 클라이언트가 읽기 또는 쓰기를 요청하면 OPEN이 수행되고 파일 핸들이 검색됩니다.
2. OPEN이 수행되면 클라이언트는 메타데이터 서버 연결을 통해 LAYOUTGET 호출을 통해 파일 핸들을 저장소로 전송합니다.
3. LAYOUTGET은 상태 ID, 스트라이프 크기, 파일 세그먼트, 장치 ID 등 파일 레이아웃에 대한 정보를 클라이언트에 반환합니다.
4. 그런 다음 클라이언트는 장치 ID를 가져와 서버에 GETDEVINFO 호출을 보내 장치와 연결된 IP 주소를 검색합니다.
5. 저장소는 로컬에서 장치에 접속할 수 있는 관련 IP 주소 목록이 포함된 응답을 보냅니다.
6. 클라이언트는 저장소에서 다시 전송된 로컬 IP 주소를 통해 NFS 대화를 계속합니다.

pNFS와 **FlexGroup** 볼륨의 상호 작용

ONTAP 의 FlexGroup 볼륨은 클러스터의 여러 노드에 걸쳐 있는 FlexVol volume 구성 요소로 스토리지를 제공하므로 워크로드가 단일 마운트 지점을 유지하면서 여러 하드웨어 리소스를 활용할 수 있습니다. 여러 네트워크 인터페이스를 갖춘 여러 노드가 작업 부하와 상호 작용하므로 ONTAP 에서 원격 트래픽이 백엔드 클러스터 네트워크를 통과하는 것은 자연스러운 결과입니다.

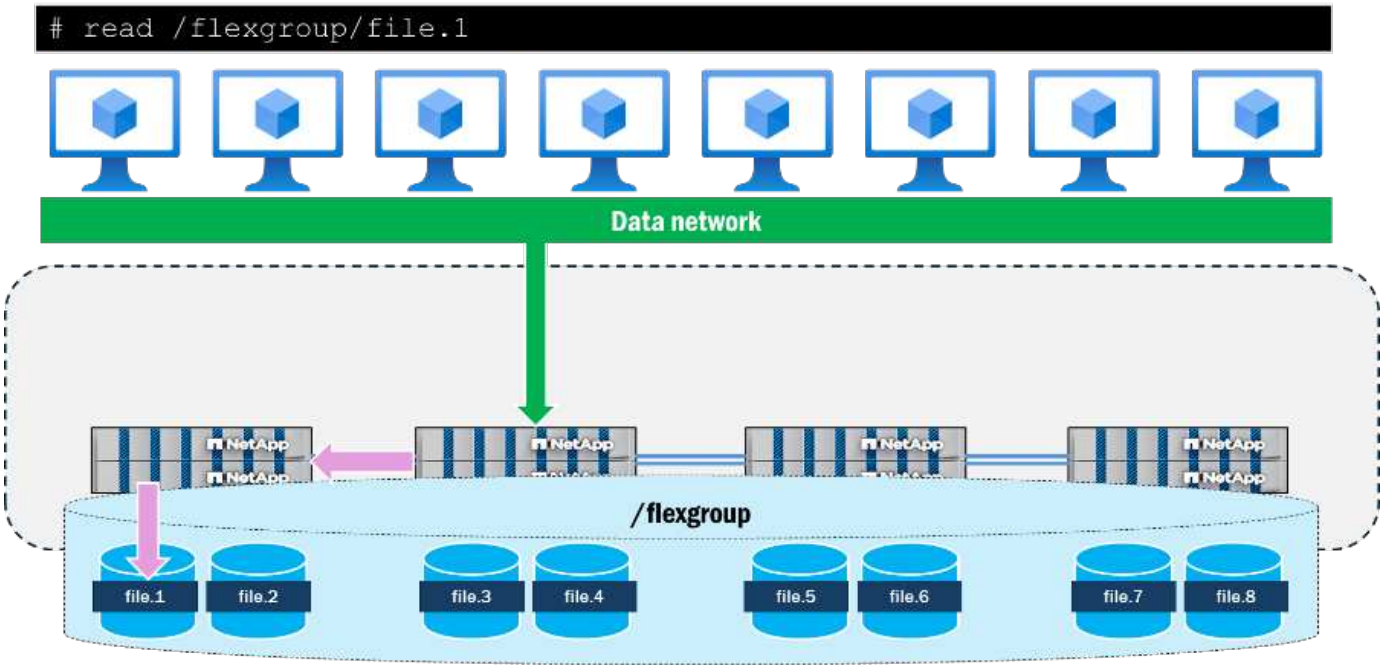


그림 **5. pNFS** 없이 **FlexGroup** 볼륨에서 단일 파일 액세스

pNFS를 활용할 때 ONTAP FlexGroup 볼륨의 파일 및 볼륨 레이아웃을 추적하고 이를 클러스터의 로컬 데이터 인터페이스에 매핑합니다. 예를 들어, 액세스 중인 파일이 포함된 구성 볼륨이 노드 1에 있는 경우 ONTAP 클라이언트에게 데이터 트래픽을 노드 1의 데이터 인터페이스로 리디렉션하도록 알립니다.

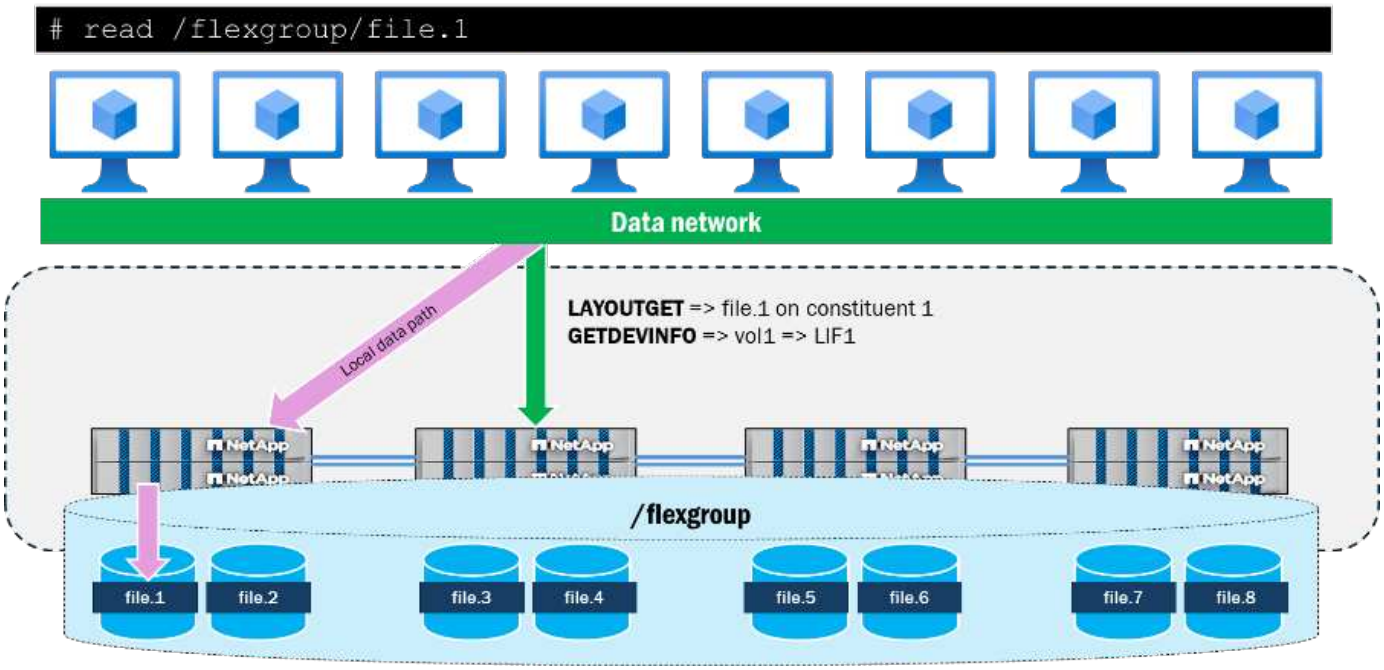


그림 **6. pNFS**를 사용한 **FlexGroup** 볼륨의 단일 파일 액세스

pNFS는 또한 pNFS가 없는 NFSv4.1에서는 제공하지 않는 단일 클라이언트의 파일에 대한 병렬 네트워크 경로를 제공합니다. 예를 들어, 클라이언트가 pNFS 없이 NFSv4.1을 사용하여 동일한 마운트에서 동시에 4개의 파일에 액세스하려는 경우 모든 파일에 동일한 네트워크 경로가 사용되고 ONTAP 클러스터는 대신 해당 파일에 원격 요청을 보냅니다. 모든 작업이 단일 경로를 따라 단일 노드에 도착하고 데이터 작업과 함께 메타데이터 작업도 처리하기 때문에 마운트 경로가 작업의 병목 현상이 될 수 있습니다.

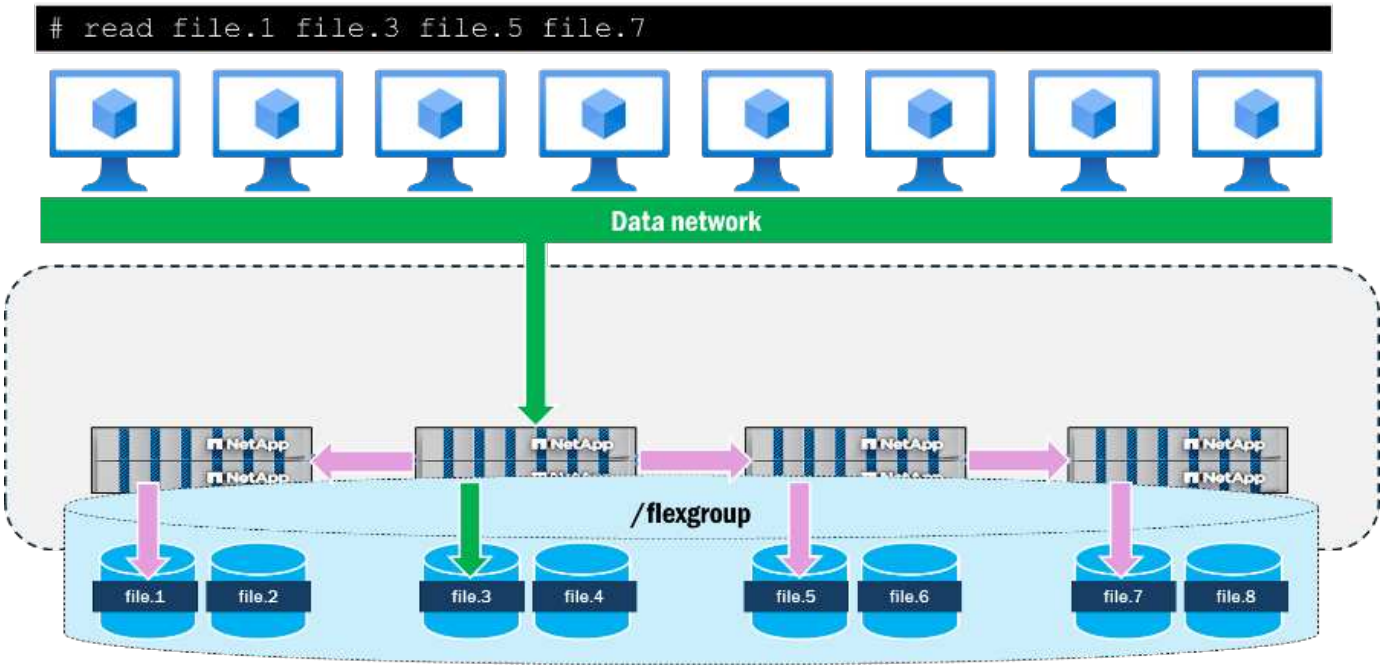


그림 **7. pNFS** 없이 **FlexGroup** 볼륨에서 여러 개의 동시 파일 액세스

pNFS를 사용하여 단일 클라이언트에서 동일한 4개 파일에 동시에 액세스하는 경우, 클라이언트와 서버는 파일을 사용하여 각 노드에 대한 로컬 경로를 협상하고 데이터 작업에 여러 TCP 연결을 사용하는 반면, 마운트 경로는 모든 메타데이터 작업의 위치 역할을 합니다. 이렇게 하면 파일에 대한 로컬 경로를 사용하여 지연 시간을 줄일 수 있을 뿐만 아니라, 클라이언트가 네트워크를 포화시킬 만큼 충분한 데이터를 전송할 수 있다면 여러 네트워크 인터페이스를 사용하여 처리량 이점을 추가할 수도 있습니다.

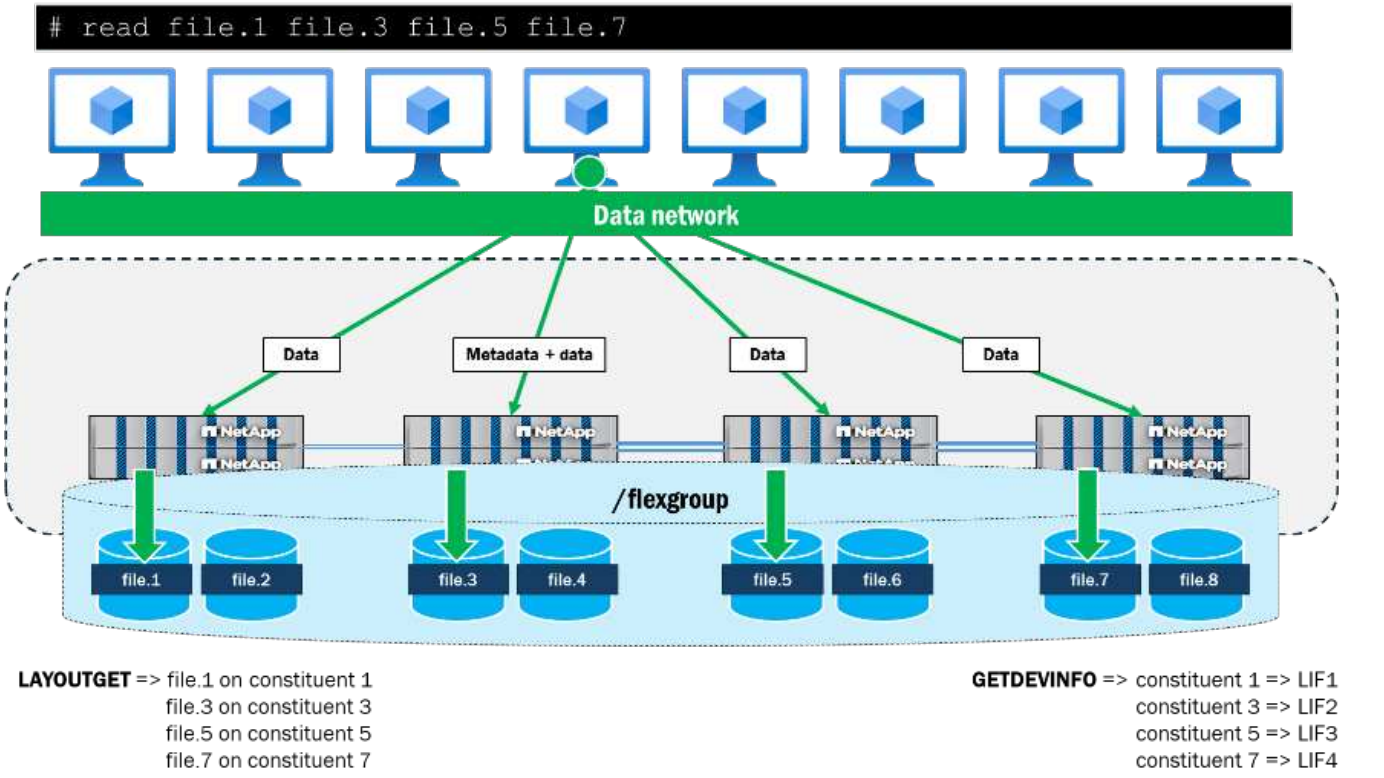


그림 **8. pNFS**를 사용한 **FlexGroup** 볼륨에서 여러 개의 동시 파일 액세스

다음은 4개의 10GB 파일(모두 2개의 ONTAP 클러스터 노드에 걸쳐 있는 다른 구성 볼륨에 있음)을 dd를 사용하여 병렬로 읽는 단일 RHEL 9.5 클라이언트에서 실행한 간단한 테스트 결과를 보여줍니다. 각 파일의 경우, pNFS를

사용하면 전체 처리량과 완료 시간이 향상되었습니다. pNFS 없이 NFSv4.1을 사용하는 경우, 마운트 지점에 로컬인 파일과 원격인 파일 간의 성능 차이가 pNFS를 사용하는 경우보다 컸습니다.

시험	파일당 처리량**(MB/s)**	파일당 완료 시간
NFSv4.1: pNFS 없음	• 파일.1–228(로컬) • 파일.2–227(로컬) • 파일.3–192(원격) • 파일.4–192(원격)	• 파일.1–46(로컬) • 파일.2–46.1(로컬) • 파일.3–54.5(원격) • 파일.4–54.5(원격)
NFSv4.1: pNFS 포함	• 파일.1–248(로컬) • 파일.2–246(로컬) • 파일.3–244(pNFS를 통한 로컬) • 파일.4–244(pNFS를 통한 로컬)	• 파일.1–42.3(로컬) • 파일.2–42.6(로컬) • 파일 3–43(pNFS를 통한 로컬) • 파일.4–43(pNFS를 통한 로컬)

관련 정보

- "FlexGroup 볼륨 관리"
- "NetApp 기술 보고서 4571: FlexGroup 모범 사례"

ONTAP 에서의 **pNFS** 사용 사례

pNFS는 다양한 ONTAP 기능과 함께 사용하여 성능을 개선하고 NFS 워크로드에 대한 유연성을 높일 수 있습니다.

nconnect를 사용한 **pNFS**

NFS는 최근의 일부 클라이언트와 서버에 새로운 마운트 옵션을 도입했는데, 이를 통해 단일 IP 주소를 마운트하는 동안 여러 TCP 연결을 제공할 수 있는 방법이 제공됩니다. 이를 통해 작업을 더 효율적으로 병렬화하고, NFS 서버와 클라이언트의 제한을 해결하고, 특정 작업 부하에 대한 전반적인 성능을 향상시킬 수 있는 메커니즘이 제공됩니다. 클라이언트가 nconnect를 지원하는 경우 ONTAP 9.8 이상에서 nconnect가 지원됩니다.

pNFS와 함께 nconnect를 사용하는 경우, NFS 서버에서 광고한 각 pNFS 장치에 대해 nconnect 옵션을 사용하여 연결이 병렬화됩니다. 예를 들어, nconnect가 4로 설정되어 있고 pNFS에 적합한 인터페이스가 4개 있는 경우, 생성되는 연결의 총 수는 마운트 지점당 최대 16개(nconnect 4개 x IP 주소 4개)가 됩니다.

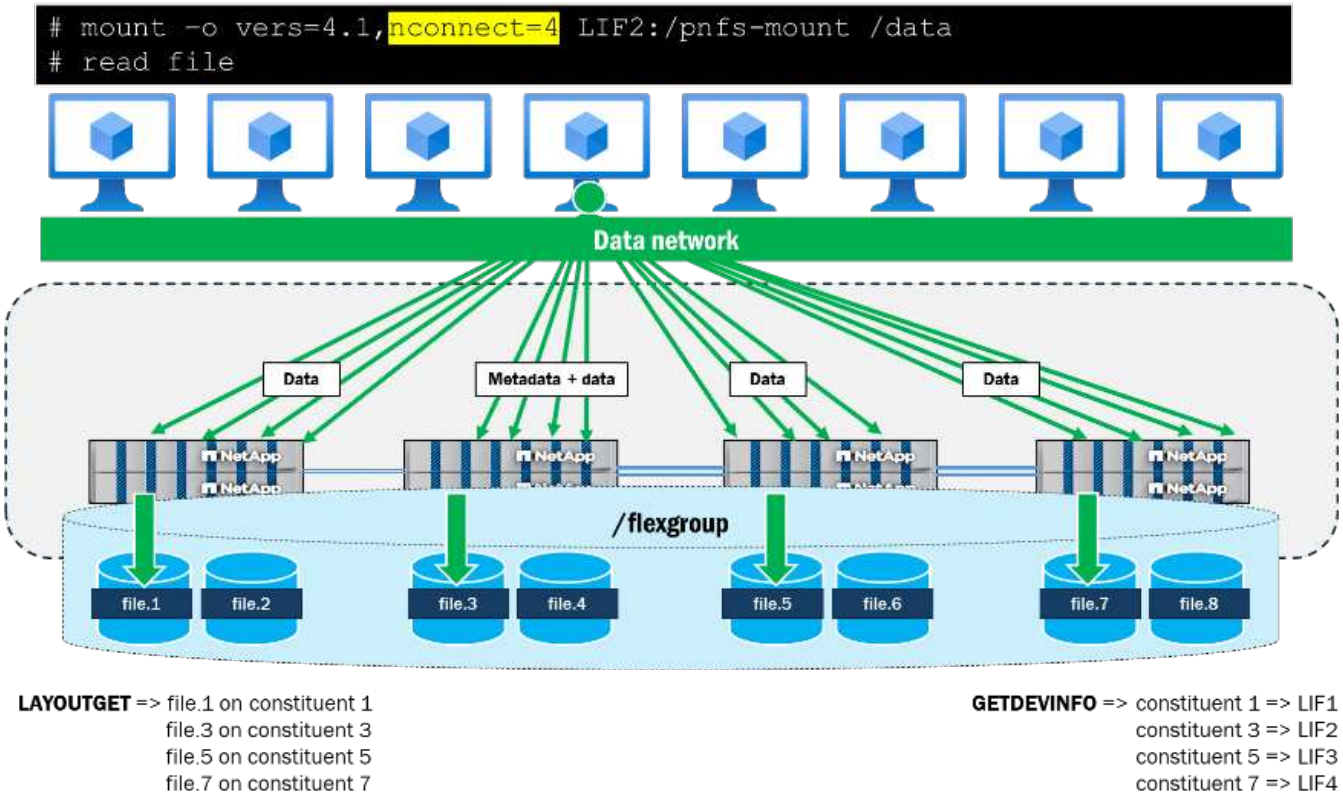


그림 **9. nconnect**가 **4**로 설정된 **pNFS**

"NFSv4.1에 대한 ONTAP 지원에 대해 자세히 알아보세요"

NFSv4.1 세션 트렁킹을 사용한 **pNFS**

NFSv4.1 세션 트렁킹 ("RFC 5661, 섹션 2.10.5")은 클라이언트와 서버 간에 여러 개의 TCP 연결을 사용하여 데이터 전송 속도를 높이는 것입니다. ONTAP 9.14.1에는 NFSv4.1 세션 트렁킹에 대한 지원이 추가되었으며 세션 트렁킹을 지원하는 클라이언트와 함께 사용해야 합니다.

ONTAP 에서는 세션 트렁킹을 클러스터의 여러 노드에 걸쳐 사용하여 연결 전반에 걸쳐 추가 처리량과 중복성을 제공할 수 있습니다.

세션 트렁킹은 여러 가지 방법으로 설정할 수 있습니다.

- 마운트 옵션을 통해 자동으로 검색**:** 대부분의 최신 NFS 클라이언트에서 세션 트렁킹은 마운트 옵션을 통해 설정할 수 있습니다(OS 공급업체의 설명서 확인). 이 옵션은 NFS 서버에 신호를 보내 세션 트렁크에 대한 정보를 클라이언트로 다시 전송합니다. 이 정보는 NFS 패킷을 통해 나타납니다. `fs_location4` 부르다.

  사용되는 마운트 옵션은 클라이언트의 OS 버전에 따라 달라집니다. 예를 들어, Ubuntu Linux 플레이버는 일반적으로 다음을 사용합니다. `max_connect=n` 세션 트렁크를 사용해야 한다는 신호를 보냅니다. RHEL Linux 배포판에서는 `trunkdiscovery` mount 옵션이 사용됩니다.

  우분투 예제

  ```
  mount -o vers=4.1,max_connect=8 10.10.10.10:/pNFS /mnt/pNFS
  ```

RHEL 예제

```
mount -o vers=4.1,trunkdiscovery 10.10.10.10:/pNFS /mnt/pNFS
```

사용하려고 시도하는 경우 `max_connect` RHEL 배포판에서는 nconnect로 처리되며 세션 트렁킹이 예상대로 작동하지 않습니다.

- 수동으로 설정: 각 개별 IP 주소를 동일한 내보내기 경로와 마운트 지점에 마운트하여 세션 트렁킹을 수동으로 설정할 수 있습니다. 예를 들어, 동일한 노드에 두 개의 IP 주소(10.10.10.10 및 10.10.10.11)가 있는 경우 내보내기 경로 `/pNFS`, mount 명령을 두 번 실행합니다.

```
mount -o vers=4.1 10.10.10.10:/pNFS /mnt/pNFS
mount -o vers=4.1 10.10.10.11:/pNFS /mnt/pNFS
```

트렁크에 참여하려는 모든 인터페이스에서 이 과정을 반복합니다.

각 노드는 자체 세션 트렁크를 갖습니다. 줄기는 노드를 가로지르지 않습니다.

pNFS를 사용할 때는 세션 트렁킹 또는 nconnect만 사용하세요. 둘 다 사용하면 바람직하지 않은 동작이 발생할 수 있습니다. 예를 들어, 메타데이터 서버 연결만 nconnect의 이점을 얻고 데이터 서버는 단일 연결을 사용합니다.

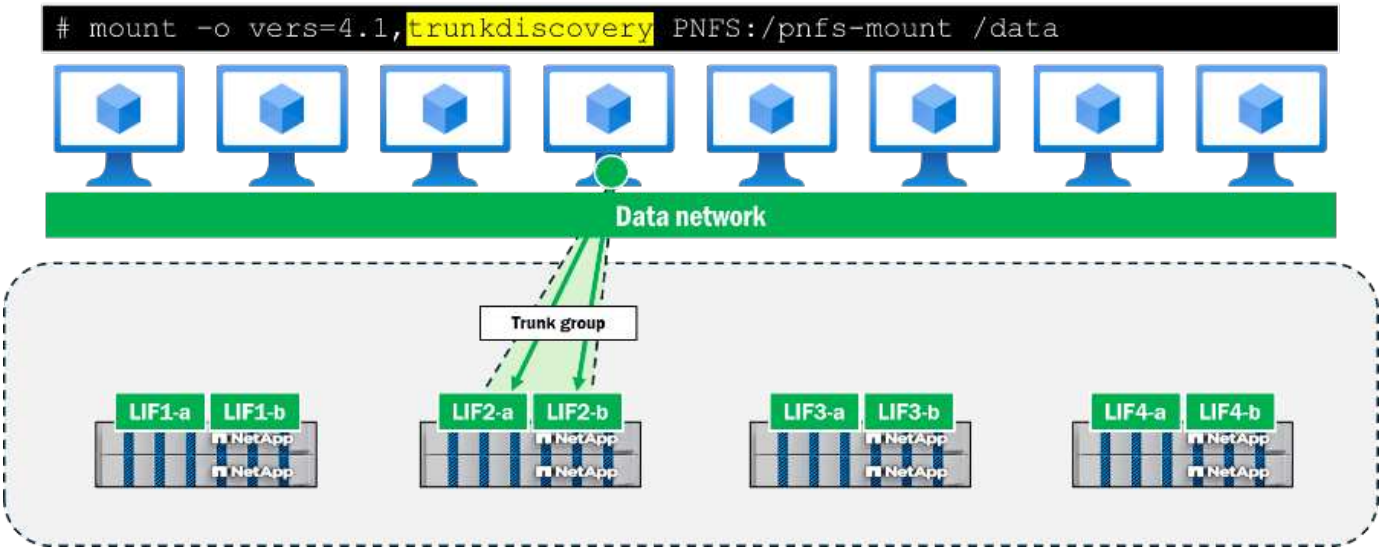
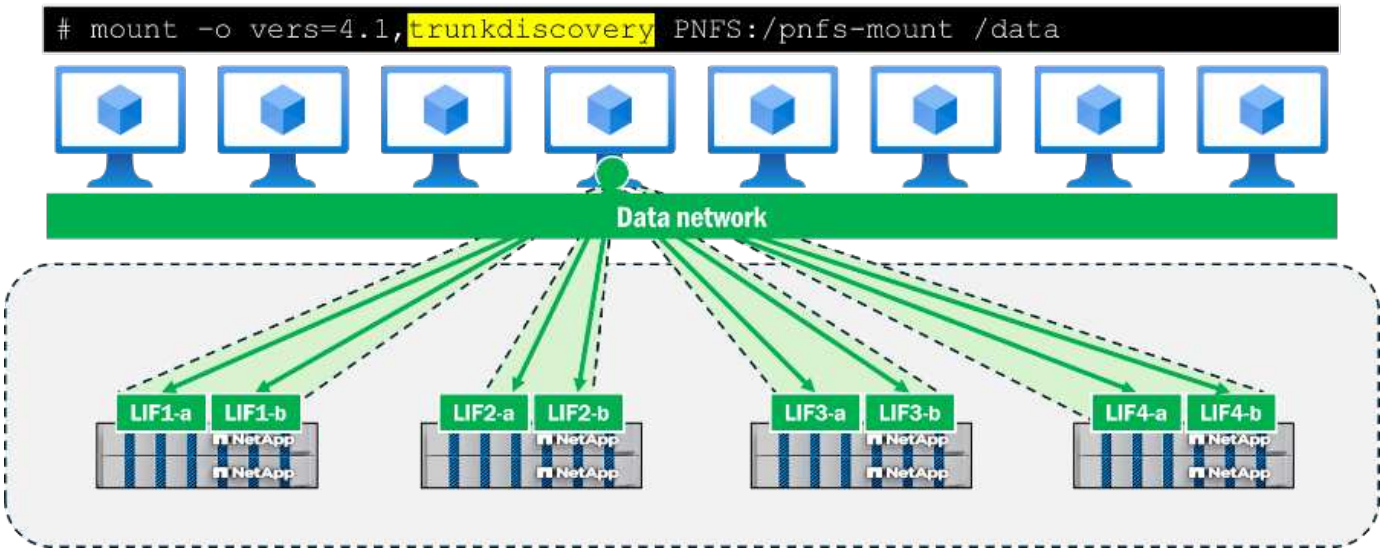


그림 **10. ONTAP** 의 **NFSv4.1** 세션 트렁킹

pNFS는 클러스터에 참여하는 각 노드에 대한 로컬 경로를 제공할 수 있으며, 세션 트렁킹과 함께 사용하면 pNFS는 노드당 세션 트렁크를 활용하여 전체 클러스터의 처리량을 극대화할 수 있습니다.



언제 `trunkdiscovery` 이 사용되는 경우, 마운트 인터페이스가 위치한 NFS 서버 노드의 나열된 세션 트렁크 인터페이스에 대해 추가된 GETATTR 호출(FS_Locations)이 활용됩니다. 해당 주소가 반환되면 반환된 주소로 후속 마운트가 수행됩니다. 이는 마운트 중 패킷 캡처에서 확인할 수 있습니다.

```
198 1.219372  [redacted]  [redacted]  NFS  246 V4 Call (Reply In 199) GETATTR FH: 0x787f5cf1
199 1.219579  [redacted]  [redacted]  NFS  238 V4 Reply (Call In 198) GETATTR

 Opcode: SEQUENCE (53)
     Status: NFS4_OK (0)
     sessionid: 7100001e004090a90000000000000409
     seqid: 0x00000009
     slot id: 0
     high slot id: 63
     target high slot id: 63
   > status flags: 0x00000000
 Opcode: PUTFH (22)
     Status: NFS4_OK (0)
 Opcode: GETATTR (9)
     Status: NFS4_OK (0)
   Attr mask: 0x01000100 (FSID, FS_Locations)
     reqd_attr: FSID (8)
       > fattr4_fsid
     reco_attr: FS_Locations (24)
       fattr4_fs_locations
           pathname components: 0
         fs_location4
             num: 1
           fs_location4
             servers
                 num: 1
               server: [redacted]
                   length: 14
                   contents: [redacted]
                   fill bytes: opaque data
             pathname components: 0
```

그림 **11.** 마운트 중 **NFS** 세션 트렁크 검색**:** 패킷 캡처

"NFS 트렁킹에 대해 자세히 알아보세요"

pNFS 대 **NFSv4.1** 참조

NFSv4.1 참조는 마운트 요청 시 클라이언트를 볼륨 위치로 안내하는 초기 마운트 경로 리디렉션 모드를 제공합니다.

NFSv4.1 참조는 단일 SVM 내에서 작동합니다. 이 기능은 NFS 마운트를 데이터 볼륨과 동일한 노드에 있는 네트워크 인터페이스로 로컬화하려고 시도합니다. 클라이언트에 마운트된 동안 해당 인터페이스나 볼륨이 다른 노드로 이동하면 새로운 마운트가 설정될 때까지 데이터 경로는 더 이상 지역화되지 않습니다.

pNFS는 마운트 경로를 지역화하려고 시도하지 않습니다. 대신 마운트 경로를 사용하여 메타데이터 서버를 구축한 다음 필요에 따라 데이터 경로를 동적으로 로컬화합니다.

NFSv4.1 참조는 pNFS와 함께 사용할 수 있지만 해당 기능은 필요하지 않습니다. pNFS로 추천을 활성화해도 눈에 띄는 결과는 나타나지 않습니다.

"NFSv4 참조 활성화 또는 비활성화"

pNFS와 고급 용량 균형 조정의 상호 작용

"고급 용량 밸런싱" ONTAP 에서는 FlexGroup 볼륨의 구성 볼륨에 파일 데이터의 일부를 기록합니다(단일 FlexVol 볼륨에서는 지원되지 않음). 파일이 커짐에 따라 ONTAP 같은 노드나 다른 노드에 있을 수 있는 다른 구성 볼륨의 새로운 멀티파트 inode에 데이터를 쓰기 시작하기로 결정합니다. 이러한 다중 inode 파일에 대한 쓰기, 읽기 및 메타데이터 작업은 클라이언트에 투명하고 중단 없이 수행됩니다. 고급 용량 밸런싱은 FlexGroup 구성 볼륨 간의 공간 관리를 개선하여 보다 일관된 성능을 제공합니다.

pNFS는 NFS 서버에 저장된 파일 레이아웃 정보에 따라 데이터 IO를 로컬 네트워크 경로로 리디렉션할 수 있습니다. 여러 구성 볼륨에 걸쳐 여러 부분으로 구성된 단일 대용량 파일이 생성되고 잠재적으로 클러스터의 여러 노드에 걸쳐 있을 때 ONTAP 의 pNFS는 각 파일 부분에 로컬 트래픽을 제공할 수 있습니다. ONTAP 모든 파일 부분에 대한 파일 레이아웃 정보도 유지 관리하기 때문입니다. 파일을 읽을 때, 데이터 경로 지역성은 필요에 따라 변경됩니다.

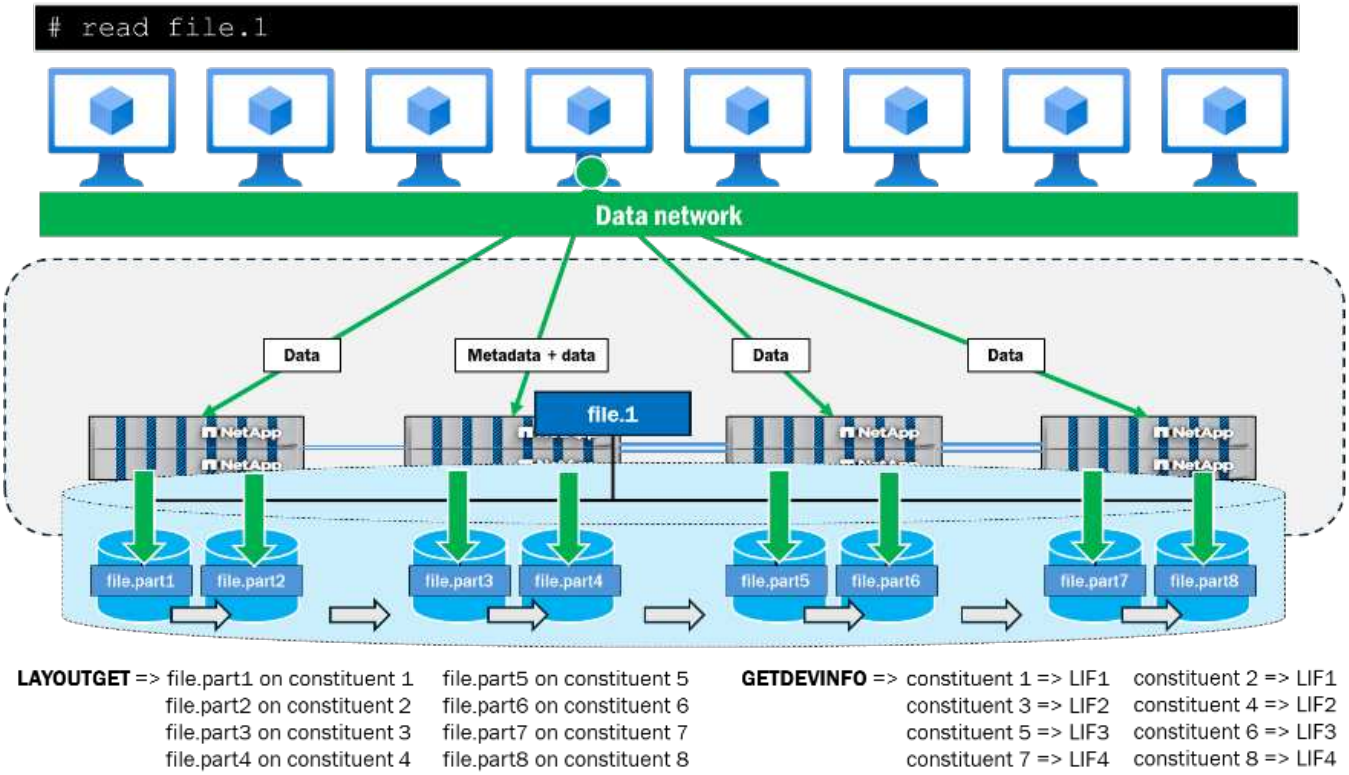


그림 **12. pNFS**를 통한 고급 용량 균형 조정

관련 정보

- "FlexGroup 볼륨 구성"

pNFS는 메타데이터와 데이터 경로를 분리하고, 데이터 지역화를 제공하며, 병렬 작업을 가능하게 하여 기존 NFS를 개선하기 위해 도입되었습니다.

기존 NFS의 과제와 pNFS의 이점

다음 표는 기존 NFS의 문제점을 보여주고 ONTAP 의 pNFS가 이를 어떻게 해결하는지 설명합니다.

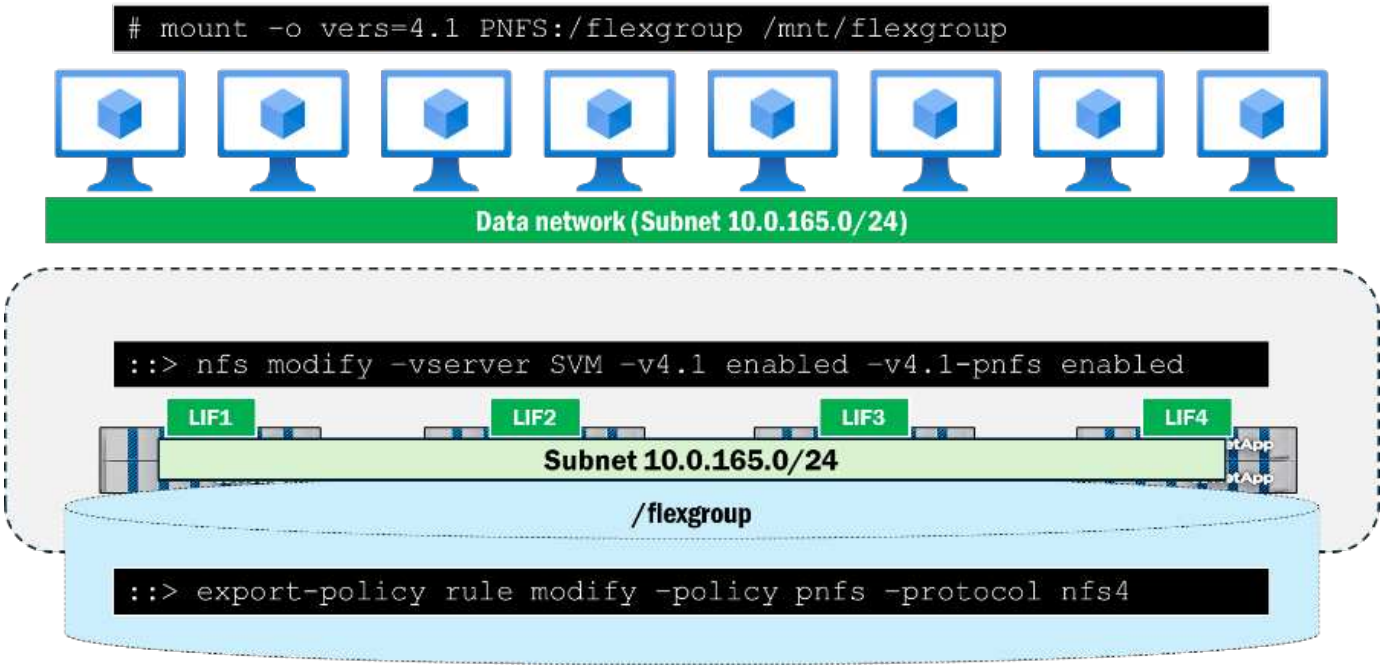
도전	pNFS의 이점
메타데이터와 데이터의 동일한 경로 기존 NFS에서는 메타데이터와 데이터가 동일한 경로를 통과하므로 네트워크와 CPU가 모두 포화 상태가 될 수 있습니다. 단일 경로가 클러스터의 단일 하드웨어 노드에 연결되기 때문입니다. 많은 사용자가 동일한 NFS 내보내기에 액세스하려고 시도하는 경우 이러한 문제는 더욱 악화됩니다.	메타데이터와 데이터 경로가 분리되어 있으며, 데이터 경로가 병렬화되어 있습니다 NFS 트래픽에 대한 메타데이터와 데이터 경로를 분리하고 데이터 경로에 대해 여러 네트워크 경로를 제공함으로써 ONTAP 클러스터에서 CPU 및 네트워크 리소스가 극대화되어 워크로드에 대한 확장성이 향상됩니다.
작업 부하 분산 과제 ONTAP NAS 클러스터에서는 최대 24개의 노드를 가질 수 있으며, 각 노드는 고유한 데이터 볼륨과 네트워크 인터페이스 세트를 가질 수 있습니다. 각 볼륨은 자체 워크로드 또는 워크로드의 하위 집합을 호스팅할 수 있으며 FlexGroup 볼륨을 사용하면 간소화를 위해 해당 워크로드가 단일 네임스페이스에 액세스하는 여러 노드에 존재할 수 있습니다. 클라이언트가 NFS 내보내기를 마운트하면 네트워크 트래픽이 단일 노드에 설정됩니다. 액세스하는 데이터가 클러스터 내의 별도 노드에 있는 경우 원격 트래픽이 발생하여 작업 부하에 지연이 발생하고 관리가 복잡해질 수 있습니다.	데이터 구조에 대한 로컬 병렬 경로 pNFS는 메타데이터에서 데이터 경로를 분리하고 클러스터 내 볼륨의 로컬성에 따라 여러 병렬 데이터 경로를 제공하므로 클러스터 내 네트워크 트래픽의 거리를 줄이고 클러스터 내 여러 하드웨어 리소스를 활용하여 대기 시간을 줄일 수 있습니다. 또한 ONTAP 의 pNFS는 데이터 트래픽을 자동으로 리디렉션하므로 관리자가 여러 개의 내보내기 경로와 위치를 관리할 필요성이 줄어듭니다.
NFS 마운트 지점의 재배치 마운트 지점이 설정된 후에는 볼륨을 마운트 해제하고 다시 마운트하는 것이 방해가 될 수 있습니다. ONTAP 노드 간에 네트워크 인터페이스를 마이그레이션하는 기능을 제공하지만, 이로 인해 관리 오버헤드가 발생하고 NFSv4.x를 사용하는 상태 저장 NFS 연결에 방해가 됩니다. 마운트 지점을 이전하는 이유 중 일부는 데이터 지역성 문제와 관련이 있습니다.	자동 경로 재배치 pNFS를 사용하면 NFS 서버는 네트워크 인터페이스와 볼륨의 위치 테이블을 유지 관리합니다. pNFS의 메타데이터 경로를 통해 클라이언트로부터 데이터 구조가 요청되면 서버는 클라이언트에 최적화된 네트워크 경로를 전달하고, 클라이언트는 해당 경로를 데이터 작업에 사용합니다. 이를 통해 작업 부하에 대한 관리 오버헤드가 크게 줄어들고 어떤 경우에는 성능이 향상될 수 있습니다.

구성 요구 사항

NetApp ONTAP 에서 pNFS를 구성하려면 다음이 필요합니다.

- pNFS를 지원하고 NFSv4.1 이상으로 마운트된 NFS 클라이언트
- ONTAP 의 NFS 서버에서 NFSv4.1이 활성화됨 (`nfs modify -v4.1 enabled`; 기본적으로 꺼짐)
- ONTAP 의 NFS 서버에서 pNFS가 활성화됨 (`nfs modify -v4.1-pnfs enabled`; 기본적으로 비활성화됨)

- 노드당 최소 하나의 네트워크 인터페이스가 NFS 클라이언트로 라우팅 가능
- NFSv4를 허용하는 내보내기 정책 및 규칙이 있는 SVM의 데이터 볼륨



위의 구성 요구 사항을 충족하면 pNFS는 그 자체로 작동합니다.

관련 정보

- "NFS 구성"
- "NFSv4.1에 대한 ONTAP 지원"
- "pNFS용 네트워크 인터페이스 연결"

계획

pNFS 배포 계획

사용자 환경에 pNFS를 배포하기 전에 전제 조건을 충족하는지 확인하고 상호 운용성 요구 사항과 구성 제한 사항을 이해해야 합니다.

필수 구성 요소

ONTAP 에서 pNFS를 활성화하고 사용하기 전에 다음 요구 사항이 충족되는지 확인하세요.

- NFS 서버에서 NFSv4.1 이상이 활성화되어 있습니다.
- 적어도 하나 "데이터 LIF는 노드당 존재합니다." NFS 서버를 호스팅하는 SVM의 클러스터에서
- 모두 "SVM의 데이터 LIF는 라우팅 가능합니다." NFS 클라이언트에
- NFS 클라이언트는 pNFS를 지원합니다(2014년 이후의 대부분의 최신 Linux 배포판).
- SVM의 클라이언트와 모든 데이터 LIF 간의 네트워크 연결이 작동합니다.
- 모든 데이터 LIF에 대해 DNS 확인(호스트 이름 사용 시)이 올바르게 구성되었습니다.

- "FlexGroup 볼륨" 구성됨(최상의 결과를 위해 권장됨)
- "NFSv4.x ID 도메인이 일치합니다." 클라이언트와 ONTAP 간
- "NFS 케르베로스" (사용되는 경우) SVM의 모든 데이터 LIF에서 활성화됩니다.

모범 사례 요약

사용자 환경에서 pNFS를 구현할 때 다음 모범 사례를 따르세요.

- 사용 "FlexGroup 볼륨" 최상의 성능과 용량 확장을 위해
- 모든 것을 확인하십시오 "SVM의 네트워크 인터페이스는 라우팅 가능합니다." 고객에게
- "NFSv4.0을 해제합니다" 클라이언트가 NFSv4.1 이상을 사용하도록 하려면
- 여러 네트워크 인터페이스와 노드에 걸쳐 마운트 포인트를 분산합니다.
- 라운드 로빈 DNS를 사용하세요 "부하 분산 메타데이터 서버"
- 확인하다 "NFSv4.x ID 도메인이 일치합니다." 클라이언트와 서버에서
- 지휘하다 "네트워크 인터페이스 마이그레이션" 그리고 "스토리지 장애 조치" 유지 관리 기간 동안
- 할 수 있게 하다 "NFS 케르베로스" Kerberos 보안을 사용하는 경우 모든 데이터 LIF에 대해
- 사용을 피하세요 "NFSv4.1 참조" pNFS를 사용할 때
- 시험 "nconnect 설정" TCP 연결 제한이 너무 커지지 않도록 주의하세요.
- 고려하다 "세션 트렁킹" 대안으로 "nConnect(연결)" (둘을 함께 사용하지 마세요)
- 확인하다 "클라이언트 OS 공급업체 지원" 배포 전 pNFS용

상호 운용성

ONTAP 의 pNFS는 RFC 호환 NFS 클라이언트와 함께 작동하도록 설계되었습니다. 다음 고려 사항이 적용됩니다.

- 가장 현대적인 "2014년 이후의 Linux 배포판" pNFS 지원(RHEL 6.4, Fedora 17 이상)
- pNFS가 지원되는지 클라이언트 OS 공급업체에 확인하세요.
- pNFS는 FlexVol 과 함께 작동합니다. "FlexGroup 볼륨"
- pNFS는 NFSv4.1에서 지원됩니다. "NFSv4.2"
- pNFS는 다음과 함께 사용할 수 있습니다. "NFS 케르베로스" (krb5, krb5i, krb5p) 하지만 성능에 영향을 미칠 수 있습니다.
- pNFS는 다음과 함께 사용할 수 있습니다. "nConnect(연결)" 또는 "세션 트렁킹" (하지만 동시에 두 가지를 할 수는 없음)
- pNFS는 작동하지 않습니다 "NFSv4.0"

제한

ONTAP 의 pNFS에는 다음 제한이 적용됩니다.

- "TCP 연결 제한" 노드당 플랫폼에 따라 다릅니다(특정 제한 사항은 NetApp Hardware Universe 확인하세요)
- 최대 파일 크기: 볼륨 유형 및 ONTAP 버전에 따라 다름

- 최대 파일 수: 최대 2000억 개의 파일 "FlexGroup 볼륨"
- 최대 용량: 최대 60PB "FlexGroup 볼륨"
- "네트워크 인터페이스 수": 노드당 최소 하나의 데이터 LIF가 필요합니다. 부하 분산을 위해 더 필요할 수 있습니다.

사용시 "pNFS와 연결"TCP 연결 수가 빠르게 증가한다는 점을 알아두세요.

- nconnect를 사용한 각 클라이언트 마운트는 데이터 LIF당 여러 개의 TCP 연결을 생성합니다.
- 많은 클라이언트가 높은 nconnect 값을 사용하므로 "TCP 연결 제한" 초과될 수 있습니다
- TCP 연결 제한을 초과하면 기존 연결이 해제될 때까지 새 연결이 차단됩니다.

관련 정보

- "pNFS용 네트워크 인터페이스 연결"
- "NFSv4.1 활성화 또는 비활성화"
- "NFSv4.1에 대한 ONTAP 지원"
- "NFSv4.2에 대한 ONTAP 지원"
- "NetApp Hardware Universe를 참조하십시오"

pNFS 튜닝 및 성능 모범 사례

ONTAP 에서 pNFS를 사용할 때 최상의 결과를 얻으려면 다음 고려 사항과 모범 사례를 활용하세요.

볼륨 유형 권장 사항

ONTAP 의 pNFS는 FlexVol 볼륨과 FlexGroup 볼륨 모두에서 작동하지만, 가장 좋은 전반적인 결과를 얻으려면 FlexGroup 볼륨을 사용하세요.

FlexGroup 볼륨은 다음을 제공합니다.

- pNFS가 데이터 트래픽을 로컬화할 수 있도록 하면서 클러스터의 여러 하드웨어 리소스를 포괄할 수 있는 단일 마운트 지점
- 대용량 가능성(최대 60PB) 및 많은 파일 수(최대 2000억 개의 파일)
- 용량 균형 조정 및 잠재적 성능 이점을 위한 다중 파트 파일 지원
- 단일 작업 부하를 지원하는 볼륨 및 하드웨어에 대한 병렬 액세스

"FlexGroup 볼륨 관리에 대해 알아보세요"

고객 추천

모든 NFS 클라이언트가 pNFS를 지원하는 것은 아니지만, 대부분의 최신 클라이언트는 pNFS를 지원합니다. RHEL 6.4와 Fedora 17이 최초로 pNFS를 지원한 클라이언트(대략 2014년)였으므로, 지난 몇 년 동안 출시된 클라이언트 버전은 이 기능을 완벽하게 지원한다고 추정하는 것이 타당합니다. ONTAP의 NFS 지원 입장은 "클라이언트가 해당 기능을 지원하고 RFC를 준수하며, 당사가 해당 기능을 지원하는 경우 해당 조합은 지원됩니다."입니다. 하지만 클라이언트 OS 공급업체가 pNFS를 지원하는지 확인하는 것이 가장 좋습니다.

볼륨 이동

ONTAP 동일한 클러스터 내의 노드나 집계 간에 볼륨을 중단 없이 이동할 수 있는 기능을 제공하여 용량과 성능 균형을 유연하게 조절할 수 있습니다. ONTAP 에서 볼륨 이동이 발생하면 pNFS 장치 매핑이 자동으로 업데이트되어 필요한 경우 클라이언트에게 새로운 볼륨-인터페이스 관계를 사용하도록 알립니다.

"볼륨 이동에 대해 알아보세요"

네트워크 인터페이스 마이그레이션

ONTAP 동일한 클러스터 내의 노드 간에 네트워크 인터페이스를 이동하여 성능 균형과 유지 관리 유연성을 제공하는 기능을 제공합니다. 볼륨 이동과 마찬가지로 ONTAP 에서 네트워크 인터페이스 마이그레이션이 발생하면 pNFS 장치 매핑이 자동으로 업데이트되어 필요한 경우 클라이언트에게 새로운 볼륨-인터페이스 관계를 사용하도록 알립니다.

그러나 NFSv4.1은 상태 저장 프로토콜이므로 네트워크 인터페이스 마이그레이션은 NFS 마운트를 적극적으로 사용하는 클라이언트에 방해가 될 수 있습니다. 유지 관리 창에서 네트워크 인터페이스 마이그레이션을 수행하고 잠재적인 네트워크 중단에 대해 클라이언트에게 알리는 것이 가장 좋습니다.

스토리지 장애 조치/환불

pNFS는 NFSv4.1과 동일한 저장소 장애 조치 고려 사항을 따릅니다. 이것들은 다음에서 자세히 다루어집니다. "NetApp 기술 보고서 4067: NFS 모범 사례 및 구축 가이드"일반적으로 pNFS와 관련된 모든 저장소 장애 조치/환불은 프로토콜의 상태성으로 인해 잠재적인 저장소 중단이 예상되므로 유지 관리 창에서 수행해야 합니다.

메타데이터 워크로드

메타데이터 작업은 크기가 작지만 작업 부하에 따라 숫자가 많아질 수 있습니다(대량의 파일을 만들고 있습니까? "찾기" 명령을 실행하고 있나요? 그리고 총 파일 개수. 결과적으로 메타데이터 호출이 많은 작업 부하는 NFS 서버의 CPU에 부담을 주고 단일 연결에서 병목 현상이 발생할 가능성이 있습니다. pNFS(및 일반적으로 NFSv4.x)는 프로토콜 버전의 상태 저장, 잠금 메커니즘 및 일부 보안 기능이 CPU 사용률과 지연 시간에 부정적인 영향을 미칠 수 있으므로 성능에 따라 달라지는 높은 메타데이터 작업 부하는 적합하지 않습니다. 이러한 작업 유형(높은 GETATTR 또는 SETATTR 등)은 일반적으로 NFSv3에서 더 나은 성능을 보입니다.

메타데이터 서버

pNFS의 메타데이터 서버는 NFS 내보내기의 초기 마운트 시 설정됩니다. 마운트 지점이 설정되면 다시 마운트되거나 데이터 인터페이스가 이동될 때까지 그 자리에 유지됩니다. 이러한 이유로 동일한 볼륨에 액세스하는 여러 클라이언트가 SVM 전반에서 서로 다른 노드와 데이터 인터페이스에 마운트되도록 하는 것이 가장 좋습니다. 이 접근 방식은 클러스터의 네트워크 인터페이스를 극대화하는 동시에 노드와 CPU 리소스 전반에 걸쳐 메타데이터 서버의 부하를 분산합니다. 이를 달성하는 한 가지 방법은 라운드 로빈 DNS 설정을 설정하는 것입니다. "NetApp 기술 보고서 4523: ONTAP 의 DNS 부하 분산".

NFSv4.x ID 도메인

NFSv4.x는 여러 가지 방법으로 보안 기능을 제공합니다(자세한 내용은 다음에서 다룹니다. "NetApp 기술 보고서 4067: NFS 모범 사례 및 구축 가이드"). NFSv4.x ID 도메인은 NFS 내보내기에서 사용자와 그룹을 인증하려고 할 때 클라이언트와 서버가 ID 도메인에 동의해야 하는 방법 중 하나입니다. ID 도메인 불일치의 부작용 중 하나는 원치 않는 액세스를 방지하기 위해 사용자 또는 그룹이 익명화된 사용자(기본적으로 압축됨)로 표시되는 것입니다. NFSv4.x(및 pNFS)를 사용하는 경우 클라이언트와 서버에서 NFSv4.x ID 도메인이 일치하는지 확인하는 것이 가장 좋습니다.

nConnect(연결)

앞서 언급했듯이 ONTAP 의 nconnect는 일부 작업 부하에서 성능을 개선하는 데 도움이 될 수 있습니다. pNFS를 사용하는 경우 nconnect가 스토리지 시스템에 대한 총 TCP 연결 수를 크게 늘려 성능을 향상시킬 수 있지만, 많은 클라이언트가 마운트 옵션을 활용할 경우 스토리지의 TCP 연결에 과부하가 걸려 문제가 발생할 수도 있다는 점을 이해하는 것이 중요합니다. NetApp Hardware Universe 노드당 TCP 연결 제한을 다룹니다.

노드의 TCP 연결 제한을 초과하면 기존 연결이 해제될 때까지 새로운 TCP 연결이 허용되지 않습니다. 이는 폭풍우가 잦은 환경에서는 복잡한 문제를 야기할 수 있습니다.

다음 표는 nconnect를 사용한 pNFS가 TCP 연결 제한을 초과할 수 있는 방식을 보여줍니다.

클라이언트 수	**nconnect** 값	마운트당, 노드당 총 잠재적 **TCP** 연결 수
1	4	4
100	4	400
1000입니다	8	8000
10000	8	80000
10000	16	160000[1]

[1] 대부분의 ONTAP 단일 노드 TCP 연결 제한을 초과합니다.

NFSv4.1 세션 트렁킹

ONTAP 의 세션 트렁킹을 사용하면 NFSv4.x 마운트에 대한 처리량과 경로 복원력을 높일 수 있습니다. pNFS와 함께 사용하면 클러스터의 각 노드가 세션 트렁크를 설정할 수 있습니다. 그러나 세션 트렁크는 노드당 최소 두 개의 인터페이스가 필요하고, pNFS는 의도한 대로 작동하려면 노드당 최소 하나의 인터페이스가 필요합니다. 또한 SVM의 모든 인터페이스는 NFS 클라이언트로 라우팅될 수 있어야 합니다. nconnect를 활용할 경우 세션 트렁킹과 pNFS가 제대로 작동하지 않습니다. nconnect와 세션 트렁킹은 상호 배타적인 기능으로 간주하세요.

"NFS 트렁킹에 대해 알아보세요"

네트워크 인터페이스 연결

pNFS가 제대로 작동하려면 클러스터의 각 노드에 라우팅 가능한 네트워크 인터페이스가 필요합니다. pNFS를 호스팅하는 NFS 서버와 동일한 SVM에 NFS 클라이언트로 라우팅할 수 없는 다른 네트워크 인터페이스가 있는 경우 ONTAP 여전히 클라이언트에 대한 장치 매핑에서 해당 인터페이스를 광고합니다. NFS 클라이언트가 다른 서브넷의 인터페이스를 통해 데이터에 액세스하려고 하면 연결할 수 없게 되어 서비스 중단이 발생합니다. pNFS를 사용할 때 클라이언트가 액세스할 수 있는 SVM의 네트워크 인터페이스만 허용하는 것이 가장 좋습니다.

기본적으로 pNFS는 SVM에 있는 모든 데이터 LIF가 NFS 클라이언트의 인터페이스로 라우팅 가능해야 합니다. 왜냐하면 pNFS 장치 목록에는 SVM에 있는 모든 데이터 LIF가 포함되기 때문입니다. 결과적으로 라우팅 불가능한 데이터 LIF가 선택될 수 있으며, 이는 서비스 중단 상황을 초래할 수 있습니다. 모범 사례로, pNFS를 사용할 때만 라우팅 가능한 데이터 LIF를 구성하십시오.

ONTAP 9.18.1 RC1 이상 버전부터는 서브넷별로 pNFS 트래픽에 사용할 수 있는 인터페이스를 지정할 수 있으므로 라우팅 가능한 인터페이스와 라우팅 불가능한 인터페이스를 혼합하여 사용할 수 있습니다. 해당 명령어에 대한 자세한 내용은 NetApp 지원팀에 문의하십시오.

NFSv4.0

NFSv4.0은 NFSv4.1과 함께 ONTAP NFS 서버에서 활성화할 수 있는 옵션입니다. 하지만 pNFS는 NFSv4.0에서는 작동하지 않습니다. NFS 서버에서 NFSv4.0이 활성화된 경우 클라이언트가 자신도 모르게 해당 프로토콜 버전을 마운트할 가능성이 있으며 pNFS를 활용할 수 없습니다. 따라서 pNFS를 사용할 때 NFSv4.0을 명시적으로 비활성화하는 것이 가장 좋습니다. NFSv4.1은 여전히 활성화되어 있어야 하며 NFSv4.0과 독립적으로 작동할 수 있습니다.

NFSv4.1 참조

NFSv4.1 참조는 볼륨을 소유한 노드의 네트워크 인터페이스로의 클라이언트에서 마운트 경로를 지역화합니다. pNFS는 데이터 경로를 지역화하고, 마운트 경로는 메타데이터 서버가 됩니다.

두 기능을 함께 사용할 수는 있지만, pNFS와 함께 NFSv4.1 참조를 사용하면 동일한 노드에 여러 메타데이터 서버를 쌓아 여러 클러스터 노드에 메타데이터 서버를 분산하는 기능이 저하되는 바람직하지 않은 효과가 발생할 수 있습니다. pNFS를 사용할 때 메타데이터 서버가 클러스터 전체에 고르게 분산되지 않으면 단일 노드의 CPU가 메타데이터 요청으로 과부하가 걸려 성능 병목 현상이 발생할 수 있습니다.

따라서 pNFS를 사용할 때 NFSv4.1 참조를 사용하지 않는 것이 가장 좋습니다. 대신, 클러스터의 여러 네트워크 인터페이스와 노드에 마운트 포인트를 분산하세요.

"NFSv4 참조 활성화 또는 비활성화에 대해 알아보세요."

NFS 케르베로스

NFS Kerberos를 사용하면 krb5를 사용하여 인증을 암호화하고 krb5i 및 krb5p를 사용하여 데이터 패킷을 추가로 암호화할 수 있습니다. 이는 SVM에서 네트워크 인터페이스별로 활성화되며 자세한 내용은 다음에서 다룹니다. "NetApp 기술 보고서 4616: ONTAP에서 Microsoft Active Directory와 NFS Kerberos".

pNFS는 SVM의 노드와 네트워크 인터페이스 전반에 걸쳐 데이터 트래픽을 리디렉션할 수 있으므로 SVM의 각 네트워크 인터페이스에서 NFS Kerberos를 활성화하고 작동시켜야 합니다. SVM의 네트워크 인터페이스 중 Kerberos가 활성화되어 있지 않으면 pNFS가 해당 인터페이스의 데이터 볼륨에 액세스하려고 할 때 제대로 작동하지 않습니다.

예를 들어, 두 개의 네트워크 인터페이스(Kerberos에 대해 하나만 활성화됨)가 있는 pNFS 지원 SVM에서 병렬 dd를 사용하여 읽기 테스트를 실행할 때, Kerberos 지원 인터페이스에 있는 파일은 잘 수행되었지만, Kerberos가 활성화되지 않은 인터페이스가 있는 노드의 파일은 읽기를 완료하지 못했습니다. 두 인터페이스 모두에서 Kerberos가 활성화되었을 때 모든 파일이 예상대로 작동했습니다.

SVM의 모든 네트워크 인터페이스에서 NFS Kerberos가 활성화된 경우 pNFS와 함께 NFS Kerberos를 사용할 수 있습니다. NFS Kerberos는 패킷 암호화/복호화로 인해 성능 저하가 발생할 수 있으므로 워크로드에 NFS Kerberos를 적용하여 pNFS를 철저히 테스트하여 성능 저하가 워크로드에 지나치게 큰 영향을 미치지 않는지 확인하는 것이 가장 좋습니다.

아래는 RHEL 9.5 클라이언트에서 pNFS와 함께 krb5(인증) 및 krb5p(종단 간 암호화)를 사용할 때의 병렬 읽기 성능에 대한 예입니다. 이 테스트에서 Krb5p는 70%의 성능 저하를 보였습니다.

케르베로스 맛	MB/초	완료 시간
krb5	• File1-243 • File2-243 • File3-238 • File4-238	• File1-43 • File2-43.1 • File3-44 • File4-44.1
krb5p	• File1-72.9 • File2-72.8 • File3-71.4 • File4-71.2	• File1-143.9 • File2-144.1 • File3-146.9 • File4-147.3

"강력한 보안을 위해 NFS를 사용한 Kerberos에 대해 알아보세요"

NFSv4.2

NFSv4.2는 ONTAP 9.8에 추가되었으며 사용 가능한 최신 NFSv4.x 버전입니다(RFC-7862). NFSv4.2에는 이를 활성화/비활성화하는 명시적인 옵션이 없습니다. 대신 NFSv4.1과 함께 활성화/비활성화됩니다. (`-4.1 enabled`). 클라이언트가 NFSv4.2를 지원하는 경우 별도로 지정하지 않으면 mount 명령 중에 지원되는 가장 높은 NFS 버전을 협상합니다. `minorversion=2` 마운트 옵션.

ONTAP 의 NFSv4.2는 다음 기능을 지원합니다.

- 보안 라벨(MAC 라벨)
- 확장 속성
- 스파스 파일 작업(FALLOCATE)

pNFS는 NFSv4.1에서 처음 도입되었지만 NFSv4.2에서도 지원되며 관련 기능도 제공됩니다.

"NFSv4.2에 대한 ONTAP 지원에 대해 알아보세요"

pNFS 명령, 통계 및 이벤트 로그

이러한 ONTAP CLI 명령은 특히 pNFS와 관련이 있습니다. 이를 사용하여 구성, 문제 해결 및 통계 수집이 가능합니다.

NFSv4.1을 활성화하십시오

```
nfs modify -vserver SVM -v4.1 enabled
```

pNFS를 활성화합니다

```
nfs modify -vserver SVM -v4.1-pnfs enabled
```

pNFS 장치 표시(고급 권한)

```
pnfs devices show -vserver SVM
```

```
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
SVM              17              2157024470      notavailable    2
SVM              18              2157024463      notavailable    2
SVM              19              2157024469      available       3
SVM              20              2157024465      available       4
SVM              21              2157024467      available       3
SVM              22              2157024462      available       1
```

pNFS 장치 매핑 표시(고급 권한)

```
pnfs devices mappings show -vserver SVM
```

```
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
SVM             19              2449            10.x.x.x
SVM             20              2512            10.x.x.y
SVM             21              2447            10.x.x.x
SVM             22              2442            10.x.x.y
```

pNFS 특정 성능 카운터 캡처(고급 권한)

```
statistics start -object nfsv4_1 -vserver SVM -sample-id [optional-name]
```

pNFS 특정 성능 카운터 보기(고급 권한)

```
statistics show -object nfsv4_1 -vserver SVM
```

pNFS 특정 카운터 목록 보기(고급 권한)

```
statistics catalog counter show -object nfsv4_1 -counter *layout*|*device*
```

```
Object: nfsv4_1

Counter                     Description
--------------------------- ----------------------------------------------
getdeviceinfo_avg_latency   Average latency of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_error         The number of failed NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_percent       Percentage of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_success       The number of successful NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_total         Total number of NFSv4.1 GETDEVICEINFO
operations.
getdevicelist_avg_latency   Average latency of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_error         The number of failed NFSv4.1 GETDEVICELIST
operations.
getdevicelist_percent       Percentage of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_success       The number of successful NFSv4.1 GETDEVICELIST
operations.
getdevicelist_total         Total number of NFSv4.1 GETDEVICELIST
operations.
layoutcommit_avg_latency    Average latency of NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_error          The number of failed NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_percent        Percentage of NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_success        The number of successful NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_total          Total number of NFSv4.1 LAYOUTCOMMIT
operations.
layoutget_avg_latency       Average latency of NFSv4.1 LAYOUTGET
operations.
layoutget_error             The number of failed NFSv4.1 LAYOUTGET
operations.
layoutget_percent           Percentage of NFSv4.1 LAYOUTGET operations.
layoutget_success           The number of successful NFSv4.1 LAYOUTGET
operations.
layoutget_total             Total number of NFSv4.1 LAYOUTGET operations.
layoutreturn_avg_latency    Average latency of NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_error          The number of failed NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_percent        Percentage of NFSv4.1 LAYOUTRETURN operations.
```

```
layoutreturn_success        The number of successful NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_total          Total number of NFSv4.1 LAYOUTRETURN
operations.
```

NFS에 대한 활성 네트워크 연결 보기

SVM에 여러 TCP 연결이 이루어지고 있는지 확인하려면 다음을 수행하십시오. `network connections active show` 명령.

예를 들어, NFS 세션 트렁크를 보고 싶다면 노드당 서로 다른 인터페이스에서 동일한 클라이언트의 연결을 찾으세요.

```
cluster::*> network connections active show -node cluster-0* -vserver PNFS
               Vserver   Interface         Remote
      CID Ctx Name      Name:Local Port   Host:Port
Protocol/Service
--------- --- --------- ----------------- --------------------
----------------
Node: node-01
2304333128 14 PNFS      data1:2049        ubuntu22-224:740     TCP/nfs
2304333144 10 PNFS      data3:2049        ubuntu22-224:864     TCP/nfs
2304333151  5 PNFS      data1:2049        ubuntu22-226:848     TCP/nfs
2304333167 15 PNFS      data3:2049        ubuntu22-226:684     TCP/nfs
Node: node-02
2497668321 12 PNFS      data2:2049        ubuntu22-224:963     TCP/nfs
2497668337 18 PNFS      data4:2049        ubuntu22-224:859     TCP/nfs
2497668344 14 PNFS      data2:2049        ubuntu22-226:675     TCP/nfs
2497668360  7 PNFS      data4:2049        ubuntu22-226:903     TCP/nfs
```

연결된 클라이언트의 **NFS** 버전 정보 보기

NFS 연결도 볼 수 있습니다. `nfs connected-clients show` 명령. 표시된 클라이언트 목록은 지난 48시간 동안 활성 NFS 트래픽이 있었던 클라이언트라는 점을 명심하세요. 유휴 NFS 클라이언트(아직 마운트되어 있더라도)는 마운트에 액세스할 때까지 표시되지 않을 수 있습니다. 최근에 액세스한 클라이언트만 표시하도록 필터링하려면 다음을 지정하세요. `-idle-time` 특징.

예를 들어, pNFS SVM에서 지난 10분 동안 활동이 있었던 클라이언트를 보려면 다음을 수행합니다.

```
cluster::*> nfs connected-clients show -vserver PNFS -idle-time <10m>

 Node: node-01

Vserver: PNFS Data-Ip: 10.x.x.x Local Remote Client-Ip Protocol Volume
Policy Idle-Time Reqs Reqs Trunking

10.x.x.a nfs4.2 PNFS_root default 9m 10s 0 149 false 10.x.x.a nfs4.2
FG_0001 default 9m 10s 135847 0 false 10.x.x.b nfs4.2 PNFS_root default 8m
12s 0 157 false 10.x.x.b nfs4.2 FG_0001 default 8m 12s 52111 0 false
```

관련 정보

- "ONTAP 의 병렬 NFS(pNFS)에 대해 알아보세요"

NFS 및 SMB 파일 및 디렉토리 명명 종속성

ONTAP NFS 및 **SMB** 파일 및 디렉토리 명명 종속성에 대해 알아보세요.

파일 및 디렉토리 명명 규칙은 ONTAP 클러스터 및 클라이언트의 언어 설정과 함께 네트워크 클라이언트의 운영 체제 및 파일 공유 프로토콜에 따라 다릅니다.

운영 체제 및 파일 공유 프로토콜에는 다음이 결정됩니다.

- 문자 파일 이름에 사용할 수 있습니다
- 파일 이름의 대/소문자 구분

ONTAP는 ONTAP 릴리즈별 파일, 디렉토리 및 qtree 이름에서 멀티바이트 문자를 지원합니다.

ONTAP NFS SVM에 대한 다양한 운영 체제의 유효한 문자에 대해 알아보세요.

다른 운영 체제를 사용하는 클라이언트에서 파일 또는 디렉토리에 액세스하는 경우 두 운영 체제 모두에서 유효한 문자를 사용해야 합니다.

예를 들어 UNIX를 사용하여 파일 또는 디렉토리를 생성하는 경우 MS-DOS 파일 또는 디렉토리 이름에 콜론이 허용되지 않으므로 이름에 콜론(:)을 사용하지 마십시오. 유효한 문자의 제한 사항은 운영 체제마다 다르므로 금지된 문자에 대한 자세한 내용은 클라이언트 운영 체제 설명서를 참조하십시오.

ONTAP NFS 다중 프로토콜 환경에서 파일 및 디렉토리 이름의 대소문자 구분에 대해 알아보세요.

파일 및 디렉토리 이름은 NFS 클라이언트의 경우 대/소문자를 구분하며, SMB 클라이언트의 경우 대/소문자를 구분하지 않지만 대/소문자를 구분합니다. SMB 공유를 생성하는 동안 그리고 공유 내의 데이터에 액세스할 때 경로를 지정할 때 취해야 할 조치와 멀티 프로토콜 환경에 미치는 영향을 이해해야 합니다.

SMB 클라이언트가 testdir라는 디렉토리를 만들면 SMB 클라이언트와 NFS 클라이언트 모두 파일 이름을 testdir로 표시합니다. 그러나 SMB 사용자가 나중에 디렉터리 이름 testdir을 만들려고 하면 해당 이름이 SMB 클라이언트에 현재

있기 때문에 이 이름은 허용되지 않습니다. NFS 사용자가 나중에 "testdir"이라는 디렉토리를 생성할 경우 NFS 및 SMB 클라이언트는 다음과 같이 디렉토리 이름을 다르게 표시합니다.

- NFS 클라이언트에서는 디렉토리 이름이 대/소문자를 구분하기 때문에 디렉토리 이름이 생성될 때 testdir와 testdir 같은 두 디렉토리 이름을 모두 볼 수 있습니다.
- SMB 클라이언트는 8.3 이름을 사용하여 두 디렉토리를 구분합니다. 한 디렉토리에 기본 파일 이름이 있습니다. 추가 디렉토리에는 8.3 파일 이름이 할당됩니다.
  - SMB 클라이언트에서는 testdir과 testDI~1이 표시됩니다.
  - ONTAP는 두 디렉토리를 구분하기 위해 'TESTDI~1' 디렉토리 이름을 생성한다.

    이 경우 SVM(스토리지 가상 머신)에서 공유를 생성하거나 수정하는 동안 공유 경로를 지정할 때 8.3 이름을 사용해야 합니다.

마찬가지로 SMB 클라이언트가 test.txt를 만들면 SMB 클라이언트와 NFS 클라이언트 모두 파일 이름을 text.txt로 표시합니다. 그러나 SMB 사용자가 나중에 Test.txt를 생성하려고 하면 SMB 클라이언트에 해당 이름이 현재 있기 때문에 이 이름은 허용되지 않습니다. NFS 사용자가 나중에 Test.txt라는 파일을 만들면 NFS 및 SMB 클라이언트는 다음과 같이 파일 이름을 다르게 표시합니다.

- NFS 클라이언트에서는 파일 이름이 대/소문자를 구분하기 때문에 이름이 test.txt와 Test.txt로 만들어지면 두 파일 이름이 모두 표시됩니다.
- SMB 클라이언트는 8.3 이름을 사용하여 두 파일을 구분합니다. 한 파일에 기본 파일 이름이 있습니다. 8.3 파일 이름이 추가로 할당됩니다.
  - SMB 클라이언트의 경우 test.txt와 test~1.TXT가 표시됩니다.
  - ONTAP는 두 파일을 구별하기 위해 'test~1.TXT' 파일 이름을 만듭니다.

> Vserver CIFS 문자 매핑 명령을 사용하여 문자 매핑을 생성한 경우 일반적으로 대/소문자를 구분하지 않는 Windows 조회가 발생할 수 있습니다. 즉, 파일 이름 조회는 문자 매핑이 작성되었고 파일 이름이 해당 문자 매핑을 사용하는 경우에만 대/소문자를 구분합니다.

ONTAP NFS 파일 및 디렉토리 이름 생성에 대해 알아보세요

ONTAP는 SMB 클라이언트에서 액세스할 수 있는 디렉토리인 원래 긴 이름과 8.3 형식의 이름을 사용하여 파일 또는 디렉토리의 이름을 두 개 생성하고 유지합니다.

파일 또는 디렉토리 이름이 8자 이름 또는 3자 확장자 제한(파일의 경우)을 초과하는 경우, ONTAP는 다음과 같이 8.3 형식 이름을 생성합니다.

- 이름이 6자를 초과하면 원본 파일 또는 디렉터리 이름이 6자로 잘립니다.
- 잘려서 더 이상 고유하지 않은 파일 또는 디렉토리 이름에 물결표(~)와 숫자(1 - 5)를 추가합니다.

  비슷한 이름이 5개 이상 있어 숫자가 부족하면 원래 이름과 아무런 관계가 없는 고유한 이름이 만들어집니다.

- 파일의 경우 파일 확장명이 3자로 잘립니다.

예를 들어, NFS 클라이언트가 'specifications.html'이라는 파일을 생성할 경우 ONTAP에서 생성한 8.3 형식 파일 이름은 'specif~1.htm'입니다. 이 이름이 이미 있는 경우 ONTAP에서는 파일 이름 끝에 다른 번호를 사용합니다. 예를 들어, NFS 클라이언트가 'specifications_new.html'이라는 다른 파일을 만들 경우 'specifications_new.html'의 8.3 형식은 'specif~2.htm'입니다.

다중 바이트 파일, 디렉토리 및 **qtree** 이름에 대한 **ONTAP NFS** 처리에 대해 알아보세요.

ONTAP 9.5부터 4바이트 UTF-8 인코딩 이름을 지원하므로 BMP(기본 다국어 플레인) 외부의 유니코드 보조 문자를 포함하는 파일, 디렉터리 및 트리 이름을 만들고 표시할 수 있습니다. 이전 릴리스에서는 이러한 보조 문자가 멀티 프로토콜 환경에서 올바르게 표시되지 않았습니다.

4바이트 UTF-8 인코딩된 이름을 지원하기 위해 새 _utf8mb4_language 코드를 "vserver" 및 "volume" 명령 제품군에 사용할 수 있습니다.

- 다음 방법 중 하나로 새 볼륨을 만들어야 합니다.
- 볼륨 '-language' 옵션을 명시적으로 설정하기:

  '볼륨 생성 - 언어 utf8mb4{…}'

- 옵션으로 생성되거나 수정된 SVM에서 볼륨 '-language' 옵션 상속:

  ``vserver[create|modify] -language utf8mb4{…}"volume create{…}'

- ONTAP 9.6 이하 버전을 사용하는 경우 utf8mb4 지원을 위해 기존 볼륨을 수정할 수 없으며 새로운 utf8mb4 지원 볼륨을 생성한 다음 클라이언트 기반 복사 툴을 사용하여 데이터를 마이그레이션해야 합니다.

  ONTAP 9.7P1 이상을 사용 중인 경우 지원 요청을 통해 utf8mb4에 대한 기존 볼륨을 수정할 수 있습니다. 자세한 내용은 을 참조하십시오 "ONTAP에서 생성한 후 볼륨 언어를 변경할 수 있습니까?".

를 누릅니다
utf8mb4 지원을 위해 SVM을 업데이트할 수 있지만 기존 볼륨에 원래 언어 코드가 유지됩니다.

를 누릅니다

4바이트 UTF-8 문자를 사용하는 LUN 이름은 현재 지원되지 않습니다.

- 유니코드 문자 데이터는 일반적으로 16비트 UTF-16(Unicode Transformation Format)을 사용하는 Windows 파일 시스템 응용 프로그램과 8비트 UTF-8(Unicode Transformation Format)을 사용하는 NFS 파일 시스템에 표시됩니다.

  ONTAP 9.5 이전 버전에서는 Windows 클라이언트에서 생성한 UTF-16 보조 문자를 포함한 이름이 다른 Windows 클라이언트에 올바르게 표시되었지만 NFS 클라이언트용 UTF-8로 올바르게 변환되지 않았습니다. 마찬가지로, 생성된 NFS 클라이언트에서 UTF-8 보완 문자를 사용하는 이름은 Windows 클라이언트의 UTF-16으로 올바르게 변환되지 않았습니다.

- ONTAP 9.4 이하를 실행하는 시스템에서 유효하거나 잘못된 보조 문자가 포함된 파일 이름을 만들면 ONTAP가 파일 이름을 거부하고 잘못된 파일 이름 오류를 반환합니다.

  이 문제를 방지하려면 파일 이름에 BMP 문자만 사용하고 보조 문자는 사용하지 마십시오. 또는 ONTAP 9.5 이상으로 업그레이드하십시오.

유니코드 문자는 qtree 이름에 사용할 수 있습니다.

- 'volume qtree' 명령군 또는 System Manager를 사용하여 qtree 이름을 설정하거나 수정할 수 있습니다.
- Qtree 이름에는 일본어 및 중국어 문자와 같은 유니코드 형식의 멀티바이트 문자가 포함될 수 있습니다.

- ONTAP 9.5 이전 버전에서는 BMP 문자(즉, 3바이트로 표현될 수 있는 문자)만 지원되었습니다.

> ONTAP 9.5 이전의 릴리즈에서는 qtree 상위 볼륨의 연결 경로에 유니코드 문자가 있는 qtree 및 디렉토리 이름이 포함될 수 있습니다. 볼륨 표시 명령은 상위 볼륨에 UTF-8 언어 설정이 있는 경우 이러한 이름을 올바르게 표시합니다. 그러나 상위 볼륨 언어가 UTF-8 언어 설정 중 하나가 아닌 경우 junction-path의 일부 부분은 숫자 NFS 대체 이름을 사용하여 표시됩니다.

- 9.5 이상 릴리즈에서는 qtree 이름이 qtree 이름으로 지원되지만 qtree가 utf8mb4에 대해 활성화된 볼륨에 있습니다.

ONTAP NFS 볼륨에서 **SMB** 파일 이름 변환을 위한 문자 매핑 구성

NFS 클라이언트는 SMB 클라이언트 및 특정 Windows 애플리케이션에 유효하지 않은 문자를 포함하는 파일 이름을 생성할 수 있습니다. SMB 클라이언트가 유효하지 않은 NFS 이름의 파일에 액세스할 수 있도록 볼륨의 파일 이름 변환에 대한 문자 매핑을 구성할 수 있습니다.

이 작업에 대해

NFS 클라이언트가 생성한 파일을 SMB 클라이언트가 액세스할 때 ONTAP는 파일 이름을 찾습니다. 이름이 유효한 SMB 파일 이름이 아닌 경우(예: 포함된 콜론 "":" 문자가 있는 경우) ONTAP는 각 파일에 대해 유지되는 8.3 파일 이름을 반환합니다. 그러나 이로 인해 중요한 정보를 긴 파일 이름으로 인코딩하는 응용 프로그램에 문제가 발생합니다.

따라서 다른 운영 체제의 클라이언트 간에 파일을 공유하는 경우 두 운영 체제 모두에서 유효한 파일 이름에 문자를 사용해야 합니다.

그러나 SMB 클라이언트에 대해 유효한 파일 이름이 아닌 문자를 포함하는 파일 이름을 생성하는 NFS 클라이언트가 있는 경우, 잘못된 NFS 문자를 SMB 및 특정 Windows 애플리케이션이 허용하는 유니코드 문자로 변환하는 맵을 정의할 수 있습니다. 예를 들어, 이 기능은 CATIA MCAD 및 Mathematica 응용 프로그램과 이 요구 사항이 있는 다른 응용 프로그램을 지원합니다.

볼륨별로 문자 매핑을 구성할 수 있습니다.

볼륨에 문자 매핑을 구성할 때 다음 사항을 염두에 두어야 합니다.

- 문자 매핑이 교차점에 적용되지 않습니다.

  각 접합 볼륨에 대해 문자 매핑을 명시적으로 구성해야 합니다.

- 올바르지 않거나 잘못된 문자를 나타내는 데 사용되는 유니코드 문자가 파일 이름에 일반적으로 나타나지 않는 문자인지 확인해야 합니다. 그렇지 않으면 원치 않는 매핑이 발생합니다.

  예를 들어 콜론(:)을 하이픈(-)에 매핑하려고 하지만 파일 이름에 하이픈(-)이 올바르게 사용된 경우 ""a-b""라는 파일에 액세스하려는 Windows 클라이언트의 요청이 ""a:b""(원하는 결과가 아님)의 NFS 이름에 매핑됩니다.

- 문자 매핑을 적용한 후에도 매핑에 여전히 잘못된 Windows 문자가 포함되어 있으면 ONTAP는 Windows 8.3 파일 이름으로 다시 돌아갑니다.
- FPolicy 알림, NAS 감사 로그, 보안 추적 메시지에 매핑된 파일 이름이 표시됩니다.
- DP 유형의 SnapMirror 관계가 생성될 때 소스 볼륨의 문자 매핑이 대상 DP 볼륨에 복제되지 않습니다.
- 대소문자 구분: 매핑된 Windows 이름이 NFS 이름으로 전환되기 때문에 이름 조회는 NFS 의미를 따릅니다. 여기에는 NFS 조회가 대/소문자를 구분한다는 사실도 포함됩니다. 즉, 매핑된 공유에 액세스하는 응용 프로그램이 대/소문자를 구분하지 않는 Windows 동작에 의존해서는 안 됩니다. 그러나 8.3 이름은 사용할 수 있으며 대

/소문자를 구분하지 않습니다.

- 부분 매핑 또는 잘못된 매핑: 이름을 매핑하여 디렉터리 열거("dir")를 수행하는 클라이언트로 반환하면 결과 유니코드 이름이 Windows 유효성을 검사합니다. 이름에 여전히 잘못된 문자가 있거나 Windows에 유효하지 않은 경우(예: "." 또는 공백으로 끝나는 경우) 잘못된 이름 대신 8.3 이름이 반환됩니다.

단계

1. 문자 매핑 구성:

   'vserver cifs character-mapping create-vserver vserver_name-volume volume_name-mapping mapping_text,...'

   매핑은 "":"로 구분된 소스-타겟 문자 쌍 목록으로 구성됩니다. 문자는 16진수를 사용하여 입력한 유니코드 문자입니다. 예: 3C:E03C.

   콜론으로 구분된 각 mapping_text 쌍의 첫 번째 값은 번역할 NFS 문자의 16진수 값이고 두 번째 값은 SMB가 사용하는 유니코드 값입니다. 매핑 쌍은 고유해야 합니다(일대일 매핑이 있어야 함).

   - 소스 매핑

     다음 표에서는 소스 매핑에 사용할 수 있는 유니코드 문자 집합을 보여 줍니다.

유니코드 문자입니다	인쇄된 문자	설명
0x01-0x19	해당 없음	인쇄할 수 없는 제어 문자입니다
0x5C	\	백슬래시
0x3A	:	결장
0x2A	*	별표
0x3F	?	물음표
0x22	"	인용 부호가 있습니다
0x3C	를 누릅니다	보다 작음
0x3E	를 누릅니다	보다 큼
0x7C		
세로선	0xB1	±

   - 타겟 매핑

     U+E0000…U+F8FF 범위의 유니코드 "전용 용도 영역"에서 대상 문자를 지정할 수 있습니다.

예

다음 명령을 실행하면 SVM(스토리지 가상 시스템) VS1 에서 "data"라는 이름의 볼륨에 대한 문자 매핑이 생성됩니다.

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ---------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

SMB 파일 이름 변환을 위한 문자 매핑을 관리하기 위한 **ONTAP NFS** 명령

FlexVol 볼륨에서 SMB 파일 이름 변환에 사용되는 파일 문자 매핑을 생성, 수정, 정보 표시 또는 삭제하여 문자 매핑을 관리할 수 있습니다.

원하는 작업	이 명령 사용…
새 파일 문자 매핑을 만듭니다	'vserver cifs character-mapping create'
파일 문자 매핑에 대한 정보를 표시합니다	'vserver cifs character-mapping show'
기존 파일 문자 매핑을 수정합니다	'vserver cifs character-mapping modify'를 참조하십시오
파일 문자 매핑을 삭제합니다	'vserver cifs character-mapping delete

에 대한 자세한 내용은 `vserver cifs character-mapping` "ONTAP 명령 참조입니다"을 참조하십시오.

NFS 트렁킹을 관리합니다

ONTAP NFS 트렁킹에 대해 알아보십시오

ONTAP 9.14.1부터 NFSv4.1 클라이언트는 세션 트렁킹을 활용하여 NFS 서버의 서로 다른 LIF에 대한 여러 연결을 열 수 있으므로 데이터 전송 속도가 향상되고 다중 경로를 통한 복원력 을 제공할 수 있습니다.

트렁킹은 FlexVol 볼륨을 트렁킹 가능 클라이언트, 특히 VMware 및 Linux 클라이언트 또는 RDMA, TCP 또는 pNFS를 통한 NFS에 내보내는 데 유리합니다.

ONTAP 9.14.1에서는 트렁킹이 단일 노드의 LIF로 제한되며, 트렁킹이 여러 노드에 대한 LIF를 확장할 수 없습니다.

FlexGroup 볼륨은 트렁킹이 지원됩니다. 이는 성능 향상을 제공할 수 있지만, FlexGroup 볼륨에 대한 다중 경로 액세스는 단일 노드에서만 구성할 수 있습니다.

이 릴리즈에서는 세션 트렁킹만 경로 다중화에 지원됩니다.

트렁킹 사용 방법

트렁킹이 제공하는 다중 경로 이점을 활용하려면 트렁킹 사용 NFS 서버가 포함된 SVM에 연결된 LIF 세트(_트렁킹 그룹 _ 이라고도 함)가 필요합니다. 트렁킹 그룹의 LIF는 클러스터의 동일한 노드에 홈 포트가 있어야 하고 이러한 홈 포트에 상주해야 합니다. 트렁킹 그룹의 모든 LIF가 동일한 페일오버 그룹의 구성원이라는 것이 모범 사례입니다.

ONTAP는 지정된 클라이언트에서 노드당 최대 16개의 트렁킹 연결을 지원합니다.

클라이언트가 트렁킹 사용 서버에서 내보내기를 마운트할 때 트렁킹 그룹의 LIF에 대한 IP 주소 수를 지정합니다. 클라이언트가 첫 번째 LIF에 연결되면 추가 LIF가 NFSv4.1 세션에만 추가되고 트렁킹 그룹 요구사항을 준수하는 경우 트렁킹에 사용됩니다. 그런 다음 클라이언트는 자체 알고리즘(예: 라운드 로빈)에 따라 여러 연결을 통해 NFS 작업을 분산합니다.

최상의 성능을 얻으려면 단일 경로 내보내기가 아닌 다중 경로 내보내기 전용 SVM에 트렁킹을 구성해야 합니다. 즉, 트렁킹이 활성화된 클라이언트에만 내보내기가 제공되는 SVM에서 NFS 서버에서만 트렁킹을 활성화해야 합니다.

지원되는 클라이언트

ONTAP NFSv4.1 서버는 NFSv4.1 세션 트렁킹을 지원하는 모든 클라이언트의 트렁킹을 지원합니다.

다음 클라이언트는 ONTAP 9.14.1에서 테스트되었습니다.

- VMware - ESXi 7.0U3F 이상
- Linux - RHEL(Red Hat Enterprise Linux) 8.8 및 9.3

> 컨트롤러 장애 조치(failover)에서 트렁킹된 LIF가 다른 노드로 마이그레이션되는 경우 RHEL NFS 클라이언트는 트렁킹을 다시 설정하지 않습니다. LIF가 다른 노드로 마이그레이션되면 트렁킹 그룹에서 제거됩니다. 트렁킹 그룹의 모든 LIF가 마이그레이션되면 NFS 클라이언트는 첫 번째 LIF만 사용하여 I/O를 계속합니다

> NFS 서버에서 트렁킹이 설정된 경우 트렁킹을 지원하지 않는 NFS 클라이언트에서 내보낸 공유에 액세스하는 사용자가 성능 저하를 겪을 수 있습니다. SVM 데이터 LIF에 대한 여러 마운트에 단일 TCP 연결만 사용되기 때문입니다.

NFS 트렁킹과 **nconnect** 간의 차이

ONTAP 9.8부터는 NFSv4.1이 활성화된 경우 기본적으로 nconnect 기능을 사용할 수 있습니다. nconnect 지원 클라이언트에서는 단일 NFS 마운트로 단일 LIF를 통해 여러 TCP 연결(최대 16개)을 가질 수 있습니다.

반면, 트렁킹은 여러 LIF에 여러 개의 TCP 연결을 제공하는 _multipathing_functionality입니다. 사용자 환경에 추가 NIC를 사용할 수 있는 경우 트렁킹은 nconnect의 기능을 뛰어넘는 병렬 처리 및 성능을 제공합니다.

에 대해 자세히 "nConnect(연결)"알아보십시오.

트렁킹을 위해 새 **NFS** 서버 및 내보내기를 구성합니다

ONTAP SVM에 트렁킹 지원 **NFS** 서버를 생성합니다

ONTAP 9.14.1부터 NFS 서버에서 트렁킹을 활성화할 수 있습니다. NFSv4.1은 NFS 서버가 생성될 때 기본적으로 사용하도록 설정됩니다.

시작하기 전에

트렁킹 지원 NFS 서버를 생성하려면 SVM이 필요합니다. SVM은 다음과 같아야 합니다.

- 클라이언트 데이터 요구 사항을 충족할 수 있는 충분한 저장소 지원.
- NFS에 대해 설정되었습니다.

기존 SVM을 사용할 수 있지만 트렁킹을 활성화하려면 모든 NFSv4.x 클라이언트를 다시 마운트해야 하므로 시스템이 중단될 수 있습니다. 다시 마운트할 수 없는 경우, NFS 서버에 대한 새 SVM을 생성하십시오.

단계

1. 적합한 SVM이 없는 경우 다음을 생성합니다.

   ```
   vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8
   ```

2. 새로 생성한 SVM의 구성 및 상태 확인:

   'vserver show -vserver_svm_name_'

   에 대해 자세히 알아보십시오 "SVM 생성".

3. NFS 서버 생성:

   ```
   vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
   -v4.1-trunking enabled -v4-id-domain my_domain.com
   ```

4. NFS가 실행 중인지 확인합니다.

   ```
   vserver nfs status -vserver svm_name
   ```

5. NFS가 원하는 대로 구성되었는지 확인합니다.

   ```
   vserver nfs show -vserver svm_name
   ```

   에 대해 자세히 알아보십시오 "NFS 서버 구성"

작업을 마친 후

필요에 따라 다음 서비스를 구성합니다.

- "DNS"
- "LDAP를 지원합니다"
- "Kerberos"

ONTAP NFS 트렁킹을 위한 네트워크를 준비합니다

NFSv4.1 트렁킹을 활용하려면 트렁킹 그룹의 LIF가 동일한 노드에 있어야 하고 동일한 노드에 홈 포트가 있어야 합니다. LIF는 같은 노드의 페일오버 그룹에서 구성되어야 합니다.

이 작업에 대해

LIF 및 NIC의 일대일 매핑은 최고의 성능 향상을 생성하지만 트렁킹은 활성화하지 않아도 됩니다. NIC가 2개 이상 설치되어 있으면 성능상의 이점을 얻을 수 있지만 반드시 필요한 것은 아닙니다.

트렁킹 그룹의 모든 LIF는 동일한 페일오버 그룹에 속해야 합니다. LIF가 같은 노드의 페일오버 그룹에 구성되어 있으면 해당 노드의 컨트롤러 페일오버로 인해 LIF가 오프라인 상태가 될 수 있습니다. 같은 노드의 페일오버 그룹에 LIF가 구성되어 있지 않고 다른 노드로 페일오버하면 트렁킹이 더 이상 작동하지 않습니다.

페일오버 그룹에서 접속(및 기본 NIC)을 추가하거나 제거할 때마다 트렁킹 페일오버 그룹을 조정해야 합니다.

시작하기 전에

- 페일오버 그룹을 생성하려면 NIC와 연결된 포트 이름을 알아야 합니다.
- 포트는 모두 같은 노드에 있어야 합니다.

단계

1. 사용할 네트워크 포트의 이름 및 상태를 확인합니다.

```
network port show
```

2. 페일오버 그룹을 생성합니다.

```
network interface failover-groups create -vserver <svm_name> -failover-group
<failover_group_name> -targets <ports_list>
```

> 페일오버 그룹이 반드시 있어야 하는 것은 아니지만 이 그룹이 반드시 권장됩니다.

   - `<svm_name>` 은 NFS 서버가 포함된 SVM의 이름입니다.
   - `<ports_list>` 은 페일오버 그룹에 추가될 포트의 목록입니다.

     포트는 다음과 같이 `node1:e0c` 형식으로 추가됩니다 `<node_name>:<port_number>`.

     다음 명령을 실행하면 SVM VS1에 대한 페일오버 그룹 fg3이 생성되고 포트 3개가 추가됩니다.

```
network interface failover-groups create -vserver vs1 -failover-group fg3
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

     에 대해 자세히 알아보십시오 "페일오버 그룹:"

   에 대한 자세한 내용은 `network interface failover-groups create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 필요한 경우 트렁킹 그룹 구성원에 대한 LIF를 생성합니다.

```
network interface create -vserver <svm_name> -lif <lif_name> -home-node
<node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
[-service-policy <policy>] [-auto-revert <true|false>]
```

   - `-home-node` - LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환되는 노드입니다.

     또한 LIF가 '-auto-revert' 옵션을 사용하여 홈 노드 및 홈 포트로 자동으로 되돌아가는지 여부를 지정할 수도

있습니다.

- `-home-port` LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환되는 물리적 포트 또는 논리 포트입니다.
- 를 사용하여 IP 주소를 지정할 수 있습니다 `-address` 및 `-netmask` 옵션이 아닌 옵션 `-subnet` 옵션을 선택합니다.
- IP 주소를 할당할 때 다른 IP 서브넷에 클라이언트 또는 도메인 컨트롤러가 있는 경우 게이트웨이에 대한 기본 경로를 구성해야 할 수 있습니다. SVM 내에서 정적 라우트를 생성하는 방법에 대한 자세한 `network route create` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.
- `-service-policy` - LIF에 대한 서비스 정책. 정책을 지정하지 않으면 기본 정책이 자동으로 할당됩니다. 를 사용합니다 `network interface service-policy show` 명령을 사용하여 사용 가능한 서비스 정책을 검토합니다.
- `-auto-revert` - 시작, 관리 데이터베이스 상태 변경 또는 네트워크 연결이 이루어질 때 데이터 LIF가 홈 노드로 자동 복구되는지 여부를 지정합니다. 기본 설정은 false 이지만 환경의 네트워크 관리 정책에 따라 true로 설정할 수 있습니다.

  트렁킹 그룹의 모든 LIF에 대해 이 단계를 반복합니다.

  다음 명령을 실행하면 이 생성됩니다 `lif-A` SVM을 위해 `vs1`, 포트에 있습니다 `e0c` 노드 `cluster1_01`:

  ```
  network interface create -vserver vs1 -lif lif-A -service-policy default-
  intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
  ```

에 대해 자세히 알아보십시오 "LIF 생성:"

4. LIF가 생성되었는지 확인:

   ```
   network interface show
   ```

5. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

다음을 확인하려면...	사용...
IPv4 주소입니다	네트워크 핑
IPv6 주소입니다	네트워크 핑6

관련 정보

- "네트워크 Ping"
- "네트워크 인터페이스"
- "네트워크 포트가 표시됩니다"

ONTAP 볼륨 엑스포트 정책을 생성합니다

데이터 공유에 대한 클라이언트 액세스를 제공하려면 하나 이상의 볼륨을 생성해야 하며 볼륨에 하나 이상의 규칙이 포함된 엑스포트 정책이 있어야 합니다.

클라이언트 내보내기 요구 사항:

- Linux 클라이언트는 트렁킹 연결(즉, 각 LIF)에 대해 별도의 마운트 및 마운트 지점을 가져야 합니다.
- VMware 클라이언트에는 여러 LIF가 지정된, 내보낸 볼륨에 대해 단일 마운트 지점만 필요합니다.

  VMware 클라이언트는 엑스포트 정책에서 루트 액세스 권한이 필요합니다.

단계

1. 엑스포트 정책 생성:

   ```
   vserver export-policy create -vserver svm_name -policyname policy_name
   ```

   정책 이름은 최대 256자까지 지정할 수 있습니다.

2. 엑스포트 정책이 생성되었는지 확인:

   'vserver export-policy show-policyname_policy_name_'

   예
   다음 명령을 실행하면 이름이 VS1 인 SVM에서 exp1 이라는 엑스포트 정책이 생성되는지 검증 및 됩니다.

   ```
   vs1::> vserver export-policy create -vserver vs1 -policyname exp1
   ```

3. 엑스포트 규칙을 생성하여 기존 엑스포트 정책에 추가:

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   를 클릭합니다 `-clientmatch` 매개 변수는 내보내기를 마운트할 트렁킹 가능 Linux 또는 VMware 클라이언트를 식별해야 합니다.

   에 대해 자세히 알아보십시오 "내보내기 규칙을 만드는 중입니다."

4. 교차점으로 볼륨을 생성합니다.

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
   -group group_name_or_number -junction-path junction_path -policy
   export_policy_name
   ```

   에 대해 자세히 알아보십시오 "볼륨 생성"

5. 볼륨이 원하는 접합 지점으로 생성되었는지 확인합니다.

   ```
   volume show -vserver svm_name -volume volume_name -junction-path
   ```

ONTAP 볼륨 또는 **NFS** 트렁킹용 데이터 공유를 마운트합니다

트렁킹을 지원하는 Linux 및 VMware 클라이언트는 트렁킹이 활성화된 ONTAP NFSv4.1 서버에서 볼륨 또는 데이터 공유를 마운트할 수 있습니다.

에 대해 자세히 알아보십시오 "지원되는 클라이언트".

Linux 클라이언트 요구 사항

ONTAP 9.16.1 이상 및 Red Hat Enterprise Linux 버전 8.7 이상(RHEL 8의 경우) 또는 9.2 이상(RHEL 9의 경우)을 Linux 클라이언트로 사용하는 경우 트렁킹 그룹에 하나의 마운트 지점만 필요합니다. 다음 옵션을 사용하여 내보낸 볼륨을 이 명령으로 마운트합니다. `trunkdiscovery`

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

그렇지 않으면 트렁킹 그룹의 각 연결에 대해 별도의 마운트 지점이 필요합니다. 옵션을 사용하여 다음과 유사한 명령을 사용하여 내보낸 볼륨을 마운트합니다 `max_connect`.

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

버전 (`vers`) 값은 이어야 합니다 `4.1` 이상.

를 클릭합니다 `max_connect` 값은 트렁킹 그룹의 연결 수에 해당합니다.

VMware 클라이언트 요구 사항

트렁킹 그룹의 각 연결에 대한 IP 주소를 포함하는 마운트 문이 필요합니다.

다음과 유사한 명령을 사용하여 내보낸 데이터 저장소를 마운트합니다.

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

를 클릭합니다 `-H` 값은 트렁킹 그룹의 연결에 해당합니다.

트렁킹을 위해 기존 **NFS** 내보내기 조정

ONTAP NFS 트렁킹을 위한 단일 경로 내보내기 조정

트렁킹을 사용하도록 기존 단일 경로(비트렁킹) NFSv4.1 내보내기를 조정할 수 있습니다. 서버 및 클라이언트 사전 요구 사항이 충족되면 트렁킹을 사용할 수 있는 클라이언트는 서버에서 트렁킹이 활성화되는 즉시 향상된 성능을 활용할 수 있습니다.

트렁킹을 위해 단일 경로 내보내기를 조정함으로써 기존 볼륨 및 SVM에서 내보낸 데이터 세트를 유지할 수 있습니다.

이렇게 하려면 NFS 서버에서 트렁킹을 활성화하고, 네트워킹 및 내보내기 구성을 업데이트하고, 내보낸 공유를 클라이언트에 다시 마운트해야 합니다.

트렁킹을 활성화하면 서버를 다시 시작할 수 있습니다. 그런 다음 VMware 클라이언트는 내보낸 데이터 저장소를 다시 마운트해야 합니다. Linux 클라이언트는 를 사용하여 내보낸 볼륨을 다시 마운트해야 합니다 `max_connect` 옵션을 선택합니다.

ONTAP NFS 서버에서 트렁킹을 활성화합니다

NFS 서버에서 트렁킹을 명시적으로 설정해야 합니다. NFSv4.1은 NFS 서버가 생성될 때 기본적으로 사용하도록 설정됩니다.

트렁킹을 활성화한 후 다음 서비스가 필요에 따라 구성되었는지 확인합니다.

- "DNS"
- "LDAP를 지원합니다"
- "Kerberos"

단계

1. 트렁킹을 활성화하고 다음과 같이 NFSv4.1이 설정되어 있는지 확인합니다.

   ```
   vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
   ```

2. NFS가 실행 중인지 확인합니다.
   `vserver nfs status -vserver svm_name`
3. NFS가 원하는 대로 구성되었는지 확인합니다.

   ```
   vserver nfs show -vserver svm_name
   ```

   에 대해 자세히 알아보십시오 "NFS 서버 구성"
   … 이 SVM에서 Windows 클라이언트를 지원하는 경우 공유를 이동한 다음 서버를 삭제합니다.
   `vserver cifs show -vserver svm_name`

   를 누릅니다
   `vserver cifs delete -vserver svm_name`

ONTAP NFS 트렁킹용 네트워크를 업데이트합니다

NFSv4.1 트렁킹을 활용하려면 트렁킹 그룹의 LIF가 동일한 노드에 있어야 하고 동일한 노드에 홈 포트가 있어야 합니다. LIF는 같은 노드의 페일오버 그룹에서 구성되어야 합니다.

이 작업에 대해

LIF 및 NIC의 일대일 매핑은 최고의 성능 향상을 생성하지만 트렁킹은 활성화하지 않아도 됩니다. NIC가 2개 이상 설치되어 있으면 성능상의 이점을 얻을 수 있지만 반드시 필요한 것은 아닙니다.

트렁킹 그룹의 모든 LIF는 동일한 페일오버 그룹에 속해야 합니다. LIF가 같은 노드의 페일오버 그룹에 구성되어 있으면 해당 노드의 컨트롤러 페일오버로 인해 LIF가 오프라인 상태가 될 수 있습니다. 같은 노드의 페일오버 그룹에 LIF가 구성되어 있지 않고 다른 노드로 페일오버하면 트렁킹이 더 이상 작동하지 않습니다.

페일오버 그룹에서 접속(및 기본 NIC)을 추가하거나 제거할 때마다 트렁킹 페일오버 그룹을 조정해야 합니다.

시작하기 전에

- 페일오버 그룹을 생성하려면 NIC와 연결된 포트 이름을 알아야 합니다.
- 포트는 모두 같은 노드에 있어야 합니다.

단계

1. 사용할 네트워크 포트의 이름 및 상태를 확인합니다.

   네트워크 포트 쇼

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 트렁킹 페일오버 그룹을 생성하거나 트렁킹을 위해 기존 그룹을 수정합니다.

   ```
   network interface failover-groups create -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>

   network interface failover-groups modify -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   ⓘ 페일오버 그룹이 반드시 있어야 하는 것은 아니지만 이 그룹이 반드시 권장됩니다.

   - `<svm_name>` 은 NFS 서버가 포함된 SVM의 이름입니다.
   - `<ports_list>` 은 페일오버 그룹에 추가될 포트의 목록입니다.

     예를 들어, `node1:e0c` 포트는 형식으로 `<node_name>:<port_number>` 추가됩니다.

     다음 명령을 실행하면 페일오버 그룹이 생성됩니다 `fg3` SVM VS1의 경우 다음 3개의 포트 추가:

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

   에 대해 자세히 알아보십시오 "페일오버 그룹:"

3. 필요에 따라 트렁킹 그룹 구성원에 대한 추가 LIF를 생성합니다.

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -home-node
   <node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
   [-service-policy <policy>] [-auto-revert <true|false>]
   ```

   - `-home-node` - LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환되는 노드입니다.

     LIF가 를 사용하여 홈 노드 및 홈 포트로 자동으로 되돌리는지 여부를 지정할 수 있습니다 `-auto-revert` 옵션을 선택합니다.

   - `-home-port` LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환되는 물리적 포트 또는 논리 포트입니다.
   - 를 사용하여 IP 주소를 지정할 수 있습니다 `-address` 및 `-netmask` 옵션.

◦ 서브넷을 사용하지 않고 IP 주소를 수동으로 할당하는 경우 다른 IP 서브넷에 클라이언트 또는 도메인 컨트롤러가 있는 경우 게이트웨이에 대한 기본 경로를 구성해야 할 수 있습니다. `network route create`명령 페이지에는 SVM 내에서 정적 라우트를 생성하는 방법에 대한 정보가 포함되어 있습니다. 에 대한 자세한 내용은 `network route create` "ONTAP 명령 참조입니다"을 참조하십시오.

◦ `-service-policy` - LIF에 대한 서비스 정책. 정책을 지정하지 않으면 기본 정책이 자동으로 할당됩니다. 를 사용합니다 `network interface service-policy show` 명령을 사용하여 사용 가능한 서비스 정책을 검토합니다.

에 대한 자세한 내용은 `network interface service-policy show` "ONTAP 명령 참조입니다"을 참조하십시오.

◦ `-auto-revert` - 시작, 관리 데이터베이스 상태 변경 또는 네트워크 연결이 이루어질 때 데이터 LIF가 홈 노드로 자동 복구되는지 여부를 지정합니다. *기본 설정은 false*이지만 사용자 환경의 네트워크 관리 정책에 따라 true로 설정할 수 있습니다.

트렁킹 그룹에 필요한 각각의 추가 LIF에 대해 이 단계를 반복합니다.

다음 명령을 실행하면 이 생성됩니다 `lif-A` SVM을 위해 `vs1`, 포트에 있습니다 `e0c` 노드 `cluster1_01`:

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

에 대해 자세히 알아보십시오 "LIF 생성:"

4. LIF가 생성되었는지 확인:

```
network interface show
```

5. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

다음을 확인하려면...	사용...
IPv4 주소입니다	네트워크 핑
IPv6 주소입니다	네트워크 핑6

관련 정보

- "네트워크 Ping"
- "네트워크 인터페이스"

ONTAP 볼륨 엑스포트 정책을 수정합니다

클라이언트가 기존 데이터 공유에 대해 트렁킹을 활용할 수 있도록 하려면 엑스포트 정책과 규칙 및 규칙이 연결되는 볼륨을 수정해야 할 수 있습니다. Linux 클라이언트 및 VMware 데이터 저장소에는 서로 다른 내보내기 요구 사항이 있습니다.

클라이언트 내보내기 요구 사항:

- Linux 클라이언트는 트렁킹 연결(즉, 각 LIF)에 대해 별도의 마운트 및 마운트 지점을 가져야 합니다.

  ONTAP 9.14.1로 업그레이드할 때 이미 볼륨을 내보낸 경우에는 트렁킹 그룹에서 해당 볼륨을 계속 사용할 수 있습니다.

- VMware 클라이언트에는 여러 LIF가 지정된, 내보낸 볼륨에 대해 단일 마운트 지점만 필요합니다.

  VMware 클라이언트는 엑스포트 정책에서 루트 액세스 권한이 필요합니다.

단계

1. 기존 엑스포트 정책이 있는지 확인:

   vserver export-policy show를 참조하십시오

2. 기존 내보내기 정책 규칙이 트렁킹 구성에 적합한지 확인합니다.

   'vserver export-policy rule show-policyname_policy_name_'

   특히 를 확인합니다 `-clientmatch` 매개 변수는 내보내기를 마운트할 트렁킹 가능 Linux 또는 VMware 클라이언트를 올바르게 식별합니다.

   조정이 필요한 경우 를 사용하여 규칙을 수정합니다 `vserver export-policy rule modify` 명령을 실행하거나 새 규칙을 만듭니다.

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   에 대해 자세히 알아보십시오 "내보내기 규칙을 만드는 중입니다."

3. 내보낸 기존의 볼륨이 온라인 상태인지 확인합니다.

   ```
   volume show -vserver svm_name
   ```

ONTAP 볼륨 또는 데이터 공유를 **NFS** 트렁킹에 다시 마운트합니다

트렁킹되지 않은 클라이언트 연결을 트렁킹 연결로 변환하려면 Linux 및 VMware 클라이언트의 기존 마운트를 분리하고 LIF에 대한 정보를 사용하여 다시 마운트해야 합니다.

에 대해 자세히 알아보십시오 "지원되는 클라이언트".

> VMware 클라이언트의 마운트를 해제하면 데이터 저장소의 모든 VM에 대해 중단이 발생합니다. 또는 트렁킹을 사용할 수 있는 새 데이터 저장소를 생성하고 * storage vMotion * 을 사용하여 VM을 이전 데이터 저장소에서 새 데이터 저장소로 이동하는 방법도 있습니다. 자세한 내용은 VMware 설명서를 참조하십시오.

Linux 클라이언트 요구 사항

ONTAP 9.16.1 이상 및 Red Hat Enterprise Linux 버전 8.7 이상(RHEL 8의 경우) 또는 9.2 이상(RHEL 9의 경우)을 Linux 클라이언트로 사용하는 경우 트렁킹 그룹에 하나의 마운트 지점만 필요합니다. 다음 옵션을 사용하여 내보낸 볼륨을 이 명령으로 마운트합니다. `trunkdiscovery`

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

그렇지 않으면 트렁킹 그룹의 각 연결에 대해 별도의 마운트 지점이 필요합니다. 옵션을 사용하여 다음과 유사한 명령을 사용하여 내보낸 볼륨을 마운트합니다 `max_connect`.

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

버전 (`vers`) 값은 이어야 합니다 `4.1` 이상.

를 클릭합니다 `max_connect` 값은 트렁킹 그룹의 연결 수에 해당합니다.

VMware 클라이언트 요구 사항

트렁킹 그룹의 각 연결에 대한 IP 주소를 포함하는 마운트 문이 필요합니다.

다음과 유사한 명령을 사용하여 내보낸 데이터 저장소를 마운트합니다.

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

를 클릭합니다 `-H` 값은 트렁킹 그룹의 연결과 일치해야 합니다.

RDMA를 통해 NFS를 관리합니다

ONTAP에서 RDMA를 통한 NFS에 대해 알아보십시오

RDMA 기반 NFS는 RDMA 지원 네트워크 어댑터를 사용하여 스토리지 시스템 메모리와 호스트 시스템 메모리 간에 데이터를 직접 복사할 수 있으므로 CPU 중단과 오버헤드를 피할 수 있습니다.

RDMA 상 NFS 구성은 머신 러닝 및 분석과 같은 지연 시간에 민감하거나 대역폭이 높은 워크로드를 사용하는 고객을 위해 설계되었습니다. RDMA 기반 ONTAP NFS는 모든 NFS 기반 워크로드에 사용할 수 있습니다. 또한 NVIDIA는 GDS(GPU Direct Storage)를 지원하기 위해 RDMA를 통해 NFS를 확장했습니다. GDS는 RDMA를 사용하여 스토리지 시스템과 GPU 메모리 간에 데이터를 직접 전송함으로써 CPU와 메인 메모리를 모두 우회함으로써 GPU 지원 워크로드를 더욱 가속화합니다.

ONTAP 9.10.1부터 NFSv4.0 프로토콜에 대해 NFS over RDMA 구성이 지원됩니다. 이후 ONTAP 릴리스에서는 추가 NFS 버전을 위한 지원이 도입되었습니다.

요구 사항

- 사용할 NFS 버전에 대해 올바른 ONTAP 버전을 실행하고 있는지 확인합니다.

NFS 버전	**ONTAP** 지원
NFSv4.0	ONTAP 9.10.1 이상
NFSv4.1	ONTAP 9.14.1 이상
NFSv3	ONTAP 9.15.1 이상

  - ONTAP 9.12.1로 시작하는 System Manager를 사용하여 RDMA를 통해 NFS를 구성할 수 있습니다. ONTAP 9.10.1 및 9.11.1에서는 CLI를 사용하여 RDMA를 통해 NFS를 구성해야 합니다.

- 고가용성(HA) 쌍의 두 노드는 동일한 버전이어야 합니다.
- 스토리지 시스템 컨트롤러가 RDMA를 지원해야 함:

ONTAP로 시작하는 중...	다음 컨트롤러는 **RDMA**를 지원합니다.
9.10.1 이상	• AFF A400 • AFF A700 • AFF A800
ONTAP 9.14.1 이상	• AFF C-Series로 문의하십시오 • AFF A900 탑재
ONTAP 9.15.1 이상	• AFF A1K 를 참조하십시오 • AFF A90 를 참조하십시오 • AFF A70 를 참조하십시오
ONTAP 9.16.1 이상	• AFF A50 를 참조하십시오 • AFF A30 를 참조하십시오 • AFF A20 를 참조하십시오

- 데이터 LIF는 RDMA를 지원하도록 구성해야 합니다.
- 대상 RNIC 지원에 대한 자세한 내용은 를 "NetApp Hardware Universe를 참조하십시오"참조하십시오.
- RDMA 기반 NFS에 대해 지원되는 클라이언트 운영 체제에 대한 자세한 내용은 를 "NetApp 상호 운용성 매트릭스(IMT)"참조하십시오. RoCE v2 지원 RNIC에 대해서는 해당 RNIC 공급업체 설명서를 참조하십시오.

RDMA 상의 NFS에서는 인터페이스 그룹이 지원되지 않습니다.

다음 단계

- RDMA를 통해 NFS용 NIC를 구성합니다
- RDMA를 통해 NFS용 LIF를 구성합니다

- RDMA를 통한 NFS 설정에 대해 설명합니다

관련 정보

- "RDMA 를 참조하십시오"
- NFS 트렁킹 개요
- "RFC 7530: NFS 버전 4 프로토콜"
- "RFC 8166: 원격 프로시저 호출 버전 1을 위한 원격 직접 메모리 액세스 전송"
- "RFC 8167: RPC-over-RDMA 전송에 대한 양방향 원격 프로시저 호출"
- "RFC 8267: RPC-over-RDMA 버전 1에 NFS 상위 계층의 바인딩"

RDMA를 통해 NFS용 NIC를 구성합니다

RDMA를 통한 NFS를 사용하려면 클라이언트 시스템과 스토리지 플랫폼 모두에 NIC 구성이 필요합니다.

스토리지 플랫폼 구성

대상 RNIC 지원에 대한 자세한 내용은 를 "NetApp Hardware Universe를 참조하십시오"참조하십시오.

고가용성(HA) 구성을 사용하는 경우 두 노드 모두 동일한 RNIC를 사용하여 RDMA 페일오버를 지원해야 합니다. NIC는 RoCE를 지원해야 합니다.

- ONTAP 9.10.1부터 다음 명령을 사용하여 RDMA 오프로드 프로토콜 목록을 볼 수 있습니다.

```
network port show -rdma-protocols roce
```

  에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

- ONTAP 9.16.1부터 우선 순위 흐름 제어(PFC)를 사용하는 것이 좋습니다. 다음 명령을 사용하여 PFC를 구성합니다 `network port modify`.

```
network port modify -node <nodename> -port <portname> -flowcontrol-admin
pfc -pfc-queues-admin 3
```

- ONTAP 9.16.1 이전에는 기본 전역 흐름 제어(GFC)를 사용하는 것이 좋습니다. 흐름 제어 설정이 변경된 경우 다음 명령을 사용하여 GFC를 `network port modify` 구성합니다.

```
network port modify -node <nodename> -port <portname> -flowcontrol-admin
full
```

  에 대한 자세한 내용은 `network port modify` "ONTAP 명령 참조입니다"을 참조하십시오.

클라이언트 시스템 구성

RDMA 기반 NFS에 대해 지원되는 클라이언트 운영 체제에 대한 자세한 내용은 를 "NetApp 상호 운용성 매트릭스(IMT)"참조하십시오. RoCE v2 지원 RNIC에 대해서는 해당 RNIC 공급업체 설명서를 참조하십시오.

클라이언트와 서버를 직접 연결할 수 있지만 페일오버 성능을 향상시키려면 스위치를 사용하는 것이 좋습니다.

클라이언트, 서버, 모든 스위치 및 스위치의 모든 포트는 점보 프레임을 사용하여 구성해야 합니다. 클라이언트 및 스위치의 흐름 제어 구성은 ONTAP의 흐름 제어 구성과 일치해야 합니다. ONTAP 9.16.1부터 ONTAP, 스위치 및 클라이언트에서 우선 순위 흐름 제어를 활성화하고 구성하는 것이 가장 좋습니다. ONTAP 9.16.1 이전에는 전역 흐름 제어를 사용하는 것이 좋습니다.

이 구성이 확인되면 RDMA를 사용하여 NFS 내보내기를 마운트할 수 있습니다.

시스템 관리자

ONTAP 9.12.1 이상을 사용하여 System Manager를 사용하여 RDMA를 통해 NFS와 네트워크 인터페이스를 구성해야 합니다.

단계

1. RDMA가 지원되는지 확인합니다. Network > Ethernet Ports * 로 이동하여 그룹 보기에서 해당 노드를 선택합니다. 노드를 확장할 때 지정된 포트에 대한 * RDMA 프로토콜 * 필드를 확인합니다. 값 * RoCE * 는 RDMA가 지원됨을 나타내고 대시(*- *)는 지원되지 않음을 나타냅니다.
2. VLAN을 추가하려면 * + VLAN * 을 선택합니다. 적절한 노드를 선택합니다. 포트 * 드롭다운 메뉴에서 사용 가능한 포트가 RDMA를 지원하는 경우 * RoCE Enabled * 라는 텍스트가 표시됩니다. RDMA를 지원하지 않으면 텍스트가 표시되지 않습니다.
3. 의 워크플로를 따릅니다 NFS를 사용하여 Linux 서버용 NAS 스토리지를 설정합니다 새 NFS 서버를 구성합니다.

   네트워크 인터페이스를 추가할 때 * RoCE 포트 사용 * 을 선택할 수 있습니다. RDMA 상에서 NFS를 사용하려는 네트워크 인터페이스에 대해 이 옵션을 선택합니다.

CLI를 참조하십시오

1. 다음 명령을 사용하여 NFS 서버에서 RDMA 액세스가 활성화되어 있는지 확인합니다.

   ```
   vserver nfs show-vserver <SVM_name>
   ```

   기본적으로 -RDMA가 활성화되어 있어야 합니다. 그렇지 않은 경우 NFS 서버에서 RDMA 액세스를 설정합니다.

   ```
   vserver nfs modify -vserver <SVM_name> -rdma enabled
   ```

2. RDMA를 통해 NFSv4.0을 통해 클라이언트를 마운트합니다.
   a. proto 매개 변수의 입력은 서버 IP 프로토콜 버전에 따라 다릅니다. IPv4인 경우 를 사용합니다 `proto=rdma`. IPv6인 경우 를 사용합니다 `proto=rdma6`.
   b. NFS 타겟 포트를 로 지정합니다 `port=20049` 표준 포트 2049 대신:

   ```
   mount -o vers=4,minorversion=0,proto=rdma,port=20049
   <Server_IP_address>:/<volume_path> <mount_point>
   ```

3. * 선택 사항 *: 클라이언트를 마운트 해제해야 하는 경우 명령을 실행합니다 `unmount <mount_path>`

추가 정보

- ONTAP NFS 서버 생성
- NFS를 사용하여 Linux 서버용 NAS 스토리지를 설정합니다

RDMA를 통해 NFS용 LIF를 구성합니다

RDMA에서 NFS를 사용하려면 LIF(네트워크 인터페이스)가 RDMA와 호환되도록 구성해야 합니다. LIF와 페일오버 쌍 모두 RDMA를 지원할 수 있어야 합니다.

새 **LIF**를 생성합니다

시스템 관리자

System Manager를 사용하여 RDMA 상의 NFS용 네트워크 인터페이스를 생성하려면 ONTAP 9.12.1 이상을 실행해야 합니다.

단계

1. Network > Overview > Network Interfaces * 를 선택합니다.
2. 를 선택합니다 + Add .
3. NFS, SMB/CIFS, S3 * 를 선택하면 * RoCE 포트 사용 * 옵션이 제공됩니다. RoCE 포트 사용 * 의 확인란을 선택합니다.
4. 스토리지 VM 및 홈 노드를 선택합니다. 이름, **IP** 주소 및 서브넷 마스크 를 할당합니다.
5. IP 주소와 서브넷 마스크를 입력하면 System Manager에서는 브로드캐스트 도메인 목록을 RoCE 지원 포트가 있는 목록으로 필터링합니다. 브로드캐스트 도메인을 선택합니다. 선택적으로 게이트웨이를 추가할 수 있습니다.
6. 저장 * 을 선택합니다.

CLI를 참조하십시오

단계

1. LIF 생성:

   'network interface create-vserver_SVM_name_-lif_lif_name_-service-policy_service_policy_name_-home-node_node_name_-home-port_port_name_{-address_netmask_netmask_value_|-subnet_subnet_name_} -firewall-policy_mdma_policy_name_auto-tridc-midc-midc_name_

   - 서비스 정책은 default-data-files 또는 data-nfs 네트워크 인터페이스 서비스를 포함하는 사용자 지정 정책이어야 합니다.
   - '-RDMA-protocols' 매개변수는 기본적으로 비어 있는 목록을 허용합니다. RoCE를 가치로 추가하면 LIF는 RoCE 오프로드를 지원하는 포트에서만 구성할 수 있으며, 봇 LIF 마이그레이션 및 페일오버에 영향을 줍니다.

LIF를 수정합니다

시스템 관리자

System Manager를 사용하여 RDMA 상의 NFS용 네트워크 인터페이스를 생성하려면 ONTAP 9.12.1 이상을 실행해야 합니다.

단계

1. Network > Overview > Network Interfaces * 를 선택합니다.
2. 변경할 네트워크 인터페이스 옆의 * > 편집 * 을 선택합니다 ⋮ .
3. RoCE 포트 사용 * 을 선택하여 RDMA 상 NFS를 활성화하거나 이 상자의 선택을 취소하여 비활성화합니다. 네트워크 인터페이스가 RoCE 가능 포트에 있는 경우 * RoCE 포트 사용 * 옆에 확인란이 표시됩니다.
4. 필요에 따라 다른 설정을 수정합니다.
5. 변경 사항을 확인하려면 * 저장 * 을 선택합니다.

CLI를 참조하십시오

1. 'network interface show' 명령을 사용하여 LIF의 상태를 확인할 수 있습니다. 서비스 정책은 data-nfs 네트워크 인터페이스 서비스를 포함해야 합니다. RDMA-protocols 목록에는 RoCE가 포함되어야 합니다. 이러한 조건 중 하나가 참이 아니면 LIF를 수정하십시오.

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. LIF를 수정하려면 다음을 실행합니다.

   'network interface modify vserver_SVM_name_-lif_lif_name_-service-policy_service_policy_name_-home-node_name_-home-port_port_name_{-address_-netmask_netmask_value_|-subnet_name_} -firewall-policy_policy_name_mdma-auto-tridf-protocol

   에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ⓘ LIF가 현재 해당 프로토콜을 지원하는 포트에 할당되지 않은 경우 LIF에서 특정 오프로드 프로토콜을 요구하도록 수정하면 오류가 발생합니다.

LIF 마이그레이션

ONTAP을 사용하면 네트워크 인터페이스(LIF)를 마이그레이션하여 RDMA를 통해 NFS를 사용할 수도 있습니다. 이 마이그레이션을 수행할 때는 대상 포트가 RoCE를 지원하는지 확인해야 합니다. ONTAP 9.12.1부터 이 절차를 시스템 관리자에서 완료할 수 있습니다. 네트워크 인터페이스의 대상 포트를 선택할 때 System Manager에서 포트가 RoCE를 지원하는지 여부를 지정합니다.

다음과 같은 경우에만 LIF를 RDMA를 통한 NFS 구성으로 마이그레이션할 수 있습니다.

- RoCE 가능 포트에서 호스팅되는 NFS RDMA 네트워크 인터페이스(LIF)입니다.
- RoCE 가능 포트에서 호스팅되는 NFS TCP 네트워크 인터페이스(LIF)입니다.
- RoCE가 아닌 지원 포트에서 호스팅되는 NFS TCP 네트워크 인터페이스(LIF)입니다.

네트워크 인터페이스 마이그레이션에 대한 자세한 내용은 을 참조하십시오 LIF 마이그레이션.

관련 정보

- LIF를 생성합니다
- LIF를 생성합니다
- LIF를 수정합니다
- LIF 마이그레이션

NFS 구성을 수정합니다

대부분의 경우 RDMA를 통한 NFS용 NFS 지원 스토리지 VM의 구성을 수정할 필요가 없습니다.

그러나 Mellanox 칩 및 LIF 마이그레이션과 관련된 문제를 처리하는 경우 NFSv4 잠금 유예 기간을 늘려야 합니다. 기본적으로 유예 기간은 45초로 설정됩니다. ONTAP 9.10.1부터 유예 기간의 최대값은 180입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 명령을 입력합니다.

   ```
   vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
   ```

이 작업에 대한 자세한 내용은 을 ONTAP SVM에 대한 NFSv4 잠금 유예 기간 지정참조하십시오.

CLI를 사용하여 SMB를 구성합니다

ONTAP CLI를 사용한 SMB 구성에 대해 알아보십시오

ONTAP 9 CLI 명령을 사용하여 새 SVM이나 기존 SVM에서 새 볼륨 또는 qtree에 포함된 파일에 대한 SMB 클라이언트 액세스를 구성할 수 있습니다.

smb(서버 메시지 블록)는 CIFS(Common Internet File System) 프로토콜의 최신 방언을 의미합니다. ONTAP CLI(Command-Line Interface) 및 OnCommand 관리 툴에서도 _cifs_가 계속 표시됩니다.

다음과 같은 방법으로 볼륨 또는 qtree에 대한 SMB 액세스를 구성하려면 다음 절차를 사용하십시오.

- SMB 버전 2 이상을 사용하려고 합니다.
- NFS 클라이언트(멀티 프로토콜 구성 아님)가 아니라 SMB 클라이언트만 지원합니다.
- NTFS 파일 권한은 새 볼륨을 보호하는 데 사용됩니다.
- SVM 관리자 권한이 아닌 클러스터 관리자 권한이 있습니다.

  SVM 및 LIF를 생성하려면 클러스터 관리자 권한이 필요합니다. SVM 관리자 권한으로 다른 SMB 구성 작업을 수행할 수 있습니다.

- System Manager나 자동화된 스크립팅 도구가 아니라 CLI를 사용하려고 합니다.

  System Manager를 사용하여 NAS 멀티 프로토콜 액세스를 구성하려면 를 참조하십시오"NFS와 SMB를 모두

사용하여 Windows 및 Linux 모두에 대해 NAS 스토리지를 프로비저닝합니다".

- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.

  이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

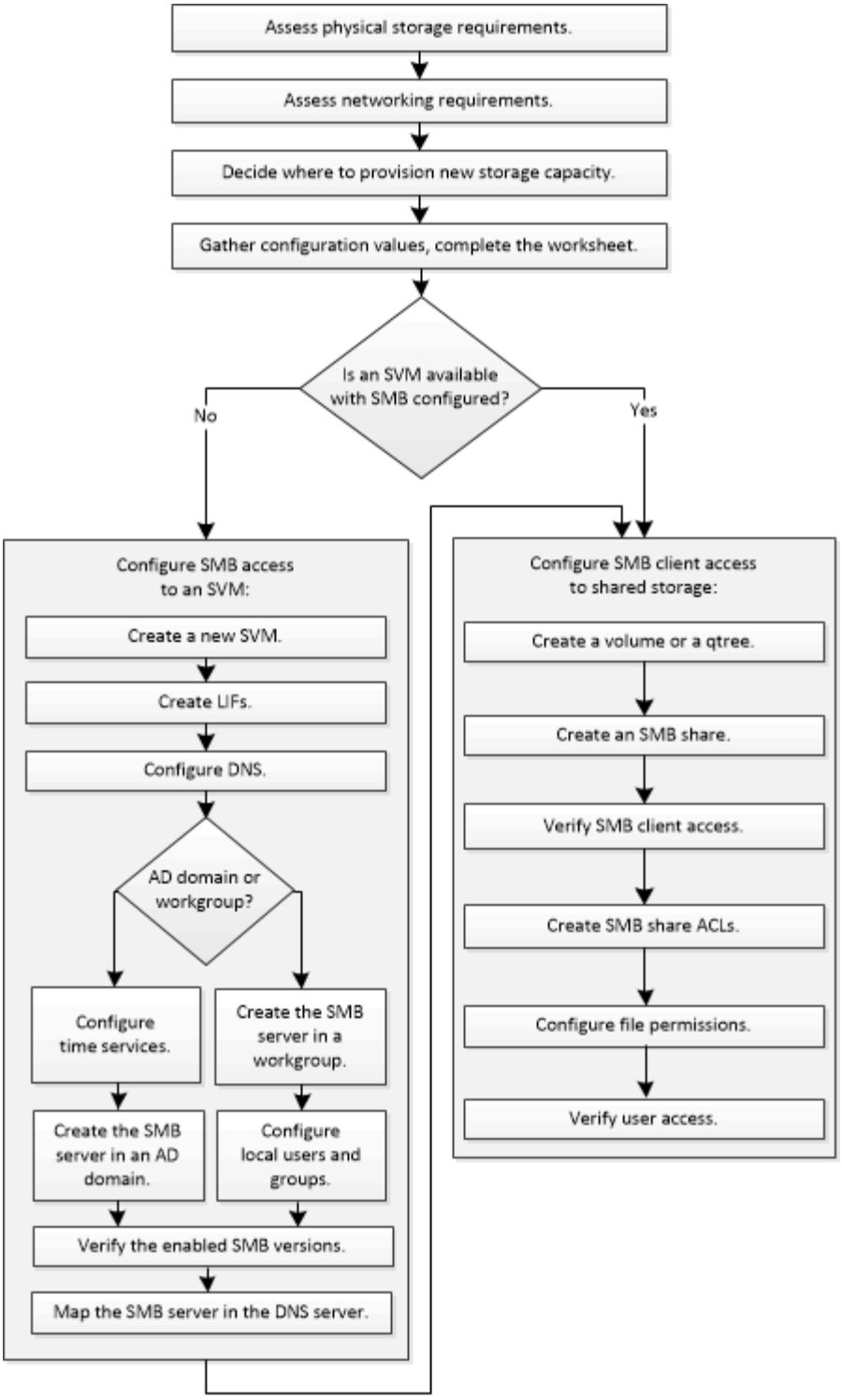
ONTAP SMB 프로토콜 기능 범위에 대한 자세한 내용은 을 참조하십시오 "SMB 참조 개요".

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면…	자세한 내용은…
재설계된 System Manager(ONTAP 9.7 이상에서 사용 가능)	"SMB를 사용하여 Windows 서버용 NAS 스토리지 용량 할당"
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	"SMB 구성 개요"

ONTAP SMB 구성 워크플로우

SMB를 구성하려면 물리적 스토리지 및 네트워킹 요구사항을 평가한 다음 목표에 맞는 워크플로우를 선택하고, 새 SVM 또는 기존 SVM에 SMB 액세스를 구성하거나, SMB 액세스에 대해 이미 완벽하게 구성된 기존 SVM에 볼륨 또는 qtree를 추가해야 합니다.



준비

ONTAP SMB의 물리적 스토리지 요구사항을 평가합니다

클라이언트용 SMB 스토리지를 프로비저닝하기 전에 새 볼륨에 대한 기존 애그리게이트에 충분한 공간이 있는지 확인해야 합니다. 없는 경우 디스크를 기존 Aggregate에 추가하거나 원하는 유형의 새 Aggregate를 생성할 수 있습니다.

단계

1. 기존 집계에서 사용 가능한 공간 표시: '스토리지 집계 표시'

   공간이 충분한 집계가 있는 경우 워크시트에 이름을 기록합니다.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. 충분한 공간이 있는 애그리게이트가 없는 경우 'Storage aggregate add-disks' 명령을 사용하여 기존 애그리게이트에 디스크를 추가하거나 'Storage aggregate create' 명령을 사용하여 새로운 애그리게이트를 생성합니다.

관련 정보

- "스토리지 집계 추가 디스크"
- "저장소 집계 생성"

ONTAP SMB 네트워킹 요구사항을 평가합니다

SMB 스토리지를 클라이언트에 제공하기 전에 네트워킹이 SMB 프로비저닝 요구 사항을 충족하도록 올바르게 구성되었는지 확인해야 합니다.

시작하기 전에

다음과 같은 클러스터 네트워킹 객체를 구성해야 합니다.

- 물리적 및 논리적 포트
- 브로드캐스트 도메인
- 서브넷(필요한 경우)
- IPspace(기본 IPspace 외에 필요 시)
- 페일오버 그룹(필요에 따라 각 브로드캐스트 도메인의 기본 페일오버 그룹 추가)
- 외부 방화벽

단계

1. 사용 가능한 물리적 포트와 가상 포트를 네트워크 포트 쇼로 표시합니다

   ◦ 가능하면 데이터 네트워크에 대해 최고 속도의 포트를 사용해야 합니다.

   ◦ 최상의 성능을 얻으려면 데이터 네트워크의 모든 구성 요소에 동일한 MTU 설정이 있어야 합니다.

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 서브넷 이름을 사용하여 LIF에 대한 IP 주소와 네트워크 마스크 값을 할당하려는 경우, 서브넷이 존재하는지, 사용 가능한 충분한 주소가 있는지 확인하십시오. 'network subnet show

   에 대한 자세한 내용은 `network subnet show` "ONTAP 명령 참조입니다"을 참조하십시오.

   서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 서브넷은 network subnet create 명령을 사용하여 생성된다.

   에 대한 자세한 내용은 `network subnet create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 사용 가능한 IPspace 표시: '네트워크 IPSpace 쇼'

   기본 IPspace 또는 사용자 지정 IPspace를 사용할 수 있습니다.

   에 대한 자세한 내용은 `network ipspace show` "ONTAP 명령 참조입니다"을 참조하십시오.

4. IPv6 주소를 사용하려면 클러스터에서 IPv6가 활성화되어 있는지 확인합니다. 'network options ipv6 show'

   필요한 경우 'network options ipv6 modify' 명령을 사용하여 IPv6을 사용하도록 설정할 수 있습니다.

   및 `network options ipv6 modify` 에 대한 자세한 `network options ipv6 show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP SMB 스토리지 용량 프로비저닝에 대해 알아보십시오

새 SMB 볼륨 또는 qtree를 생성하기 전에 새로운 SVM이나 기존 SVM에 배치할 것인지, SVM에 필요한 구성의 양을 결정해야 합니다. 이 결정에 따라 워크플로가 결정됩니다.

선택

- 새 SVM에서 볼륨 또는 qtree를 프로비저닝하거나 SMB가 활성화되었지만 구성되지 않은 기존 SVM에서 프로비저닝하려는 경우 "'SVM에 SMB 액세스 구성' 및 "'SMB 지원 SVM에 스토리지 용량 추가" 단계를 완료하십시오.

  SVM에 대한 SMB 액세스 구성

  공유 스토리지에 대한 SMB 클라이언트 액세스 구성

  다음 중 하나에 해당하는 경우 새 SVM을 생성할 수 있습니다.

  ◦ 클러스터에서 SMB를 처음으로 활성화하는 경우

  ◦ SMB 지원을 사용하지 않으려는 클러스터에 기존 SVM이 있습니다.

  ◦ 클러스터에 하나 이상의 SMB 지원 SVM이 있으며 다음 연결 중 하나를 원합니다.

- 다른 Active Directory 포리스트 또는 워크그룹에.
- SMB 서버(멀티 테넌시 시나리오) 또한 이 옵션을 선택하여 SMB를 활성화했지만 구성되지 않은 기존 SVM에서 스토리지를 프로비저닝해야 합니다. 이는 SAN 액세스를 위해 SVM을 생성했거나, SVM 생성 시 프로토콜을 사용하지 않은 경우에 발생할 수 있습니다.

SVM에서 SMB를 활성화한 후 볼륨 또는 qtree를 계속해서 프로비저닝합니다.

- SMB 액세스를 위해 완벽하게 구성된 기존 SVM에서 볼륨 또는 qtree를 프로비저닝하려면 "'SMB 지원 SVM에 스토리지 용량 추가' 단계를 완료하십시오.

  공유 스토리지에 대한 SMB 클라이언트 액세스 구성

ONTAP SMB 구성 워크시트

SMB 구성 워크시트를 사용하면 클라이언트에 대한 SMB 액세스를 설정하는 데 필요한 정보를 수집할 수 있습니다.

스토리지 용량 할당 위치에 대한 결정에 따라 워크시트의 섹션 중 하나 또는 두 섹션을 모두 완료해야 합니다.

- SVM에 대한 SMB 액세스를 구성하는 경우 두 섹션을 모두 완료해야 합니다.

  SVM에 대한 SMB 액세스 구성

  공유 스토리지에 대한 SMB 클라이언트 액세스 구성

- SMB 지원 SVM에 스토리지 용량을 추가하려면 두 번째 섹션만 완료해야 합니다.

  공유 스토리지에 대한 SMB 클라이언트 액세스 구성

매개 변수에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

SVM에 대한 **SMB** 액세스 구성

- SVM 생성을 위한 매개 변수 *

새로운 SVM을 생성하는 경우 명령을 통해 이러한 값을 `vserver create` 제공합니다. 에 대한 자세한 내용은 `vserver create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	FQDN(정규화된 도메인 이름)이거나 클러스터 전체에 고유한 SVM 이름을 적용하는 다른 규칙을 따르는 새 SVM에 대해 제공하는 이름입니다.	
'-집계'	새 SMB 스토리지 용량을 위한 충분한 공간이 있는 클러스터의 애그리게이트 이름입니다.	

필드에 입력합니다	설명	귀사의 가치
'-rootvolume'	SVM 루트 볼륨에 제공하는 고유 이름입니다.	
'-rootvolume-security-style'	SVM에 NTFS 보안 스타일을 사용하십시오.	NTFS
'-언어'	이 워크플로의 기본 언어 설정을 사용합니다.	1. UTF-8
'IPSpace'	선택 사항: IPspace는 SVM이 상주하는 별개의 IP 주소 공간입니다.	

- LIF 생성을 위한 매개 변수 *

LIF를 생성할 때 이러한 값을 명령과 함께 `network interface create` 제공합니다. 에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-lif'	새 LIF에 대해 제공한 이름입니다.	
'-역할'	이 워크플로우에서 데이터 LIF 역할을 사용합니다.	다타
'-데이터-프로토콜'	이 워크플로우에서는 SMB 프로토콜만 사용합니다.	'CIFS'입니다
홈 노드	LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행할 때 LIF가 반환되는 노드입니다. 에 대한 자세한 내용은 `network interface revert` "ONTAP 명령 참조입니다"을 참조하십시오.	
``홈 포트''	LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 포트 또는 인터페이스 그룹입니다.	
주소	새 LIF가 데이터 액세스에 사용할 클러스터의 IPv4 또는 IPv6 주소입니다.	

필드에 입력합니다	설명	귀사의 가치
넷마스크입니다	LIF의 네트워크 마스크와 게이트웨이입니다.	
'-서브넷'	IP 주소 풀입니다. 주소와 넷마스크를 자동으로 할당하기 위해 -address와 -netmask 대신 사용됩니다.	
방화벽 정책	이 워크플로우에서 기본 데이터 방화벽 정책을 사용합니다.	다타
자동 되돌리기	선택 사항: 데이터 LIF가 시작 시 또는 다른 상황에서 홈 노드로 자동 전환되는지 여부를 지정합니다. 기본 설정은 false입니다.	

- DNS 호스트 이름 확인을 위한 매개 변수 *

DNS를 구성할 때 명령과 함께 이러한 값을 `vserver services name-service dns create` 제공합니다. 에 대한 자세한 내용은 `vserver services name-service dns create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
``도메인'	최대 5개의 DNS 도메인 이름	
이름-서버	각 DNS 이름 서버에 대해 최대 3개의 IP 주소를 지정할 수 있습니다.	

Active Directory 도메인에서 **SMB** 서버 설정

시간 서비스 구성에 대한 매개 변수 *

시간 서비스를 구성할 때 이러한 값을 명령과 함께 `cluster time-service ntp server create` 제공합니다. 에 대한 자세한 내용은 `cluster time-service ntp server create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-서버'	Active Directory 도메인에 대한 NTP 서버의 호스트 이름 또는 IP 주소입니다.	

- Active Directory 도메인에서 SMB 서버를 생성하기 위한 매개 변수 *

새 SMB 서버를 생성하고 도메인 정보를 지정할 때 이러한 값을 명령과 함께 `vserver cifs create` 제공합니다. 에 대한 자세한 내용은 `vserver cifs create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	SMB 서버를 생성할 SVM의 이름입니다.	
'-cifs-server'	SMB 서버의 이름(최대 15자).	
``도메인’	SMB 서버와 연결할 Active Directory 도메인의 FQDN(정규화된 도메인 이름)입니다.	
'-ou'	선택 사항: SMB 서버와 연결할 Active Directory 도메인 내의 조직 단위입니다. 기본적으로 이 매개 변수는 CN=Computers로 설정됩니다.	
'-NetBIOS-별칭'	선택 사항: NetBIOS 별칭 목록으로, SMB 서버 이름에 대한 대체 이름입니다.	
``논평’	선택 사항: 서버에 대한 텍스트 설명입니다. Windows 클라이언트는 네트워크에서 서버를 검색할 때 이 SMB 서버 설명을 볼 수 있습니다.	

작업 그룹에서 **SMB** 서버 설정

- 작업 그룹에서 SMB 서버를 생성하기 위한 매개 변수 *

새 SMB 서버를 생성하고 지원되는 SMB 버전을 지정할 때 이러한 값에 명령을 입력합니다 `vserver cifs create`. 에 대한 자세한 내용은 `vserver cifs create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	SMB 서버를 생성할 SVM의 이름입니다.	
'-cifs-server'	SMB 서버의 이름(최대 15자).	
``워크그룹’’	작업 그룹의 이름(최대 15자).	
``논평’	선택 사항: 서버에 대한 텍스트 설명입니다. Windows 클라이언트는 네트워크에서 서버를 검색할 때 이 SMB 서버 설명을 볼 수 있습니다.	

- 로컬 사용자 생성을 위한 매개 변수 *

명령을 사용하여 로컬 사용자를 만들 때 이러한 값을 `vserver cifs users-and-groups local-user create` 제공합니다. 이러한 서버는 작업 그룹의 SMB 서버에 필요하며 AD 도메인의 선택적 서버에 필요합니다. 에 대한 자세한 내용은 `vserver cifs users-and-groups local-user create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	로컬 사용자를 생성할 SVM의 이름입니다.	
'-user-name'입니다	로컬 사용자의 이름(최대 20자).	
이름	선택 사항: 사용자의 전체 이름입니다. 전체 이름에 공백이 포함된 경우 전체 이름을 큰따옴표로 묶습니다.	
``설명''	선택 사항: 로컬 사용자에 대한 설명입니다. 설명에 공백이 있으면 매개 변수를 따옴표로 묶어야 합니다.	
'-is-account-disabled'	선택 사항: 사용자 계정의 사용 여부를 지정합니다. 이 매개 변수를 지정하지 않으면 기본값은 사용자 계정을 활성화하는 것입니다.	

- 로컬 그룹 생성을 위한 매개 변수 *

명령을 사용하여 로컬 그룹을 만들 때 이러한 값을 `vserver cifs users-and-groups local-group create` 제공합니다. AD 도메인 및 워크그룹의 SMB 서버에 대해서는 선택 사항입니다. 에 대한 자세한 내용은 `vserver cifs users-and-groups local-group create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	로컬 그룹을 생성할 SVM의 이름입니다.	
``그룹 이름''	로컬 그룹의 이름입니다(최대 256자).	
``설명''	선택 사항: 로컬 그룹에 대한 설명입니다. 설명에 공백이 있으면 매개 변수를 따옴표로 묶어야 합니다.	

SMB 지원 **SVM**에 스토리지 용량 추가

- 볼륨 생성을 위한 매개 변수 *

qtree가 아닌 볼륨을 생성하는 경우 명령과 함께 이러한 값을 `volume create` 제공합니다. 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	새 볼륨을 호스팅할 새 SVM 또는 기존 SVM의 이름입니다.	
'- 볼륨'	새 볼륨에 제공하는 고유한 설명 이름입니다.	
'-집계'	새 SMB 볼륨을 위한 충분한 공간이 있는 클러스터의 애그리게이트 이름입니다.	
'-size'	새 볼륨의 크기에 대해 제공하는 정수입니다.	
'-보안-스타일'	이 워크플로에 NTFS 보안 스타일을 사용합니다.	NTFS
``교차점-경로”	새 볼륨을 마운트할 루트(/) 아래의 위치입니다.	

- qtree 생성을 위한 매개 변수 *

볼륨 대신 qtree를 생성하는 경우 명령과 함께 이러한 값을 `volume qtree create` 제공합니다. 에 대한 자세한 내용은 `volume qtree create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	qtree가 포함된 볼륨이 있는 SVM의 이름입니다.	
'- 볼륨'	새 qtree를 포함할 볼륨의 이름입니다.	
'-qtree'	새 qtree를 64자 이하로 설명하는 고유한 이름입니다.	
'-qtree-path'	볼륨과 qtree를 별도의 인수로 지정하는 대신 '/vol/volume_name/qtree_name\>' 형식의 qtree 경로 인수를 지정할 수 있습니다.	

- SMB 공유 생성을 위한 매개 변수 *

명령을 사용하여 이러한 값을 `vserver cifs share create` 입력합니다. 에 대한 자세한 내용은 `vserver cifs share create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	SMB 공유를 생성할 SVM의 이름입니다.	
'-공유-이름'	생성할 SMB 공유의 이름입니다(최대 256자).	
'-경로'	SMB 공유의 경로 이름(최대 256자). 공유를 생성하기 전에 이 경로가 볼륨에 있어야 합니다.	
'-공유-속성'	선택 사항: 공유 속성 목록입니다. 기본 설정은 oplocks, 탐색 가능, changentify, swing-previous-versions입니다.	
``논평’	선택 사항: 서버에 대한 텍스트 설명입니다(최대 256자). Windows 클라이언트는 네트워크에서 탐색할 때 이 SMB 공유 설명을 볼 수 있습니다.	

- SMB ACL(공유 액세스 제어 목록) 생성을 위한 매개 변수 *

명령을 사용하여 이러한 값을 `vserver cifs share access-control create` 입력합니다. 에 대한 자세한 내용은 `vserver cifs share access-control create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	SMB ACL을 생성할 SVM의 이름입니다.	
'-share'	생성할 SMB 공유의 이름입니다.	
'-user-group-type’입니다	공유의 ACL에 추가할 사용자 또는 그룹의 유형입니다. 기본 유형은 Windows입니다	"창"
'- 사용자 또는 그룹'	공유의 ACL에 추가할 사용자 또는 그룹입니다. 사용자 이름을 지정하는 경우 "domain\username" 형식을 사용하여 사용자의 도메인을 포함해야 합니다.	
허락	사용자 또는 그룹에 대한 권한을 지정합니다.	'[No_access
Read	Change	Full_Control]'

SVM에 대한 SMB 액세스를 구성합니다

ONTAP SVM에 대한 SMB 액세스를 구성합니다

SMB 클라이언트 액세스를 위해 SVM이 아직 구성되지 않은 경우 새 SVM을 생성 및 구성하거나 기존 SVM을 구성해야 합니다. SMB를 구성하려면 SVM 루트 볼륨 액세스를 열고, SMB 서버를 생성하고, LIF를 생성하고, 호스트 이름 확인을 지원하고, 이름 서비스를 구성하고, 필요한 경우 Kerberos 보안 활성화.

ONTAP SVM을 생성하여 SMB 데이터 액세스를 제공합니다

SMB 클라이언트에 데이터 액세스를 제공하기 위해 클러스터에 SVM을 하나 이상 가지고 있지 않은 경우 하나 생성해야 합니다.

시작하기 전에

- ONTAP 9.13.1부터 스토리지 VM에 대한 최대 용량을 설정할 수 있습니다. SVM이 임계값 용량 수준에 도달할 경우에도 경고를 구성할 수 있습니다. 자세한 내용은 을 SVM 용량 관리참조하십시오.

단계

1. SVM 생성: `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`
   - '-rootvolume-security-style' 옵션에 NTFS 설정을 사용합니다.
   - 기본 C. UTF-8 '-language' 옵션을 사용합니다.
   - IPSpace 설정은 선택 사항입니다.
2. 새로 생성한 SVM의 구성 및 상태 확인: `vserver show -vserver vserver_name`

   허용되는 프로토콜 필드에는 CIFS가 포함되어야 합니다. 나중에 이 목록을 편집할 수 있습니다.

   'Vserver 작동 상태' 필드에는 '실행 중' 상태가 표시되어야 합니다. 초기화 중 상태가 표시되는 경우 루트 볼륨 생성 등 일부 중간 작업이 실패한 것으로, SVM을 삭제하고 다시 생성해야 합니다.

예

다음 명령은 IPspace에서 데이터 액세스를 위한 SVM을 생성합니다 `ipspaceA`:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

다음 명령을 실행하면 루트 볼륨 1GB 단위로 SVM이 생성되고 자동으로 시작되어 '실행 중' 상태에 있음을 알 수 있습니다. 루트 볼륨에는 규칙을 포함하지 않는 기본 엑스포트 정책이 있으므로 생성 시 루트 볼륨을 내보내지 않습니다.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

ONTAP 9.13.1부터 SVM의 볼륨에 처리량 하한 및 상한 제한을 적용하여 적응형 QoS 정책 그룹 템플릿을 설정할 수 있습니다. SVM을 생성한 후에만 이 정책을 적용할 수 있습니다. 이 프로세스에 대한 자세한 내용은 을 적응형 정책 그룹 템플릿을 설정합니다참조하십시오.

ONTAP SVM에서 **SMB** 프로토콜이 활성화되었는지 확인합니다

SVM에서 SMB를 구성 및 사용하려면 먼저 프로토콜이 활성화되어 있는지 확인해야 합니다.

이 작업에 대해

이는 일반적으로 SVM 설정 중에 수행되지만 설정 중에 프로토콜을 활성화하지 않은 경우 나중에 'vserver add-protocols' 명령을 사용하여 활성화할 수 있습니다.

프로토콜을 생성한 후에는 LIF에서 프로토콜을 추가하거나 제거할 수 없습니다.

"vserver remove-protocols" 명령을 사용하여 SVM에서 프로토콜을 비활성화할 수도 있습니다.

단계

1. SVM에 대해 현재 활성화 및 비활성화된 프로토콜은 'vserver show -vserver vserver_name -protocols'(vserver show -vserver vserver vserver_name -protocol)를 확인하십시오

"vserver show-protocols" 명령을 사용하여 클러스터의 모든 SVM에서 현재 활성화된 프로토콜을 볼 수도 있습니다.

2. 필요한 경우 프로토콜을 활성화 또는 비활성화합니다.
   - SMB 프로토콜을 활성화하려면: 'vserver add-protocols-vserver vserver_name-protocols cifs'
   - 프로토콜을 작동 불가능하게 하려면: "vserver remove-protocols-vserver vserver_name-protocols protocol_name[,protocol_name,...]"
3. 활성화된 프로토콜과 비활성화된 프로토콜이 'vserver show -vserver vserver_name -protocols'(vserver show -vserver vserver_name -protocol)로 올바르게 업데이트되었는지 확인합니다

예

다음 명령을 실행하면 이름이 VS1 인 SVM에서 현재 설정 및 해제된 프로토콜(허용 및 허용 안 함)이 표시됩니다.

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

다음 명령을 실행하면 VS1 이라는 SVM의 활성화된 프로토콜 목록에 "CIFS"를 추가하여 SMB를 통해 액세스할 수 있습니다.

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

ONTAP SVM 루트 볼륨의 **SMB** 엑스포트 정책을 엽니다

SVM 루트 볼륨의 기본 엑스포트 정책에는 SMB를 통한 모든 클라이언트의 개방형 액세스를 지원하는 규칙이 포함되어야 합니다. 이러한 규칙이 없으면 모든 SMB 클라이언트가 SVM 및 해당 볼륨에 대한 액세스가 거부됩니다.

이 작업에 대해

새 SVM이 생성되면 SVM의 루트 볼륨에 대한 기본 엑스포트 정책(기본값)이 자동으로 생성됩니다. 클라이언트가 SVM에서 데이터에 액세스하려면 기본 엑스포트 정책에 대한 규칙을 하나 이상 생성해야 합니다.

모든 SMB 액세스가 기본 엑스포트 정책에서 열려 있는지 확인하고, 나중에 개별 볼륨 또는 qtree에 대한 사용자 지정 엑스포트 정책을 생성하여 개별 볼륨에 대한 액세스를 제한해야 합니다.

단계

1. 기존 SVM을 사용하는 경우 기본 루트 볼륨 엑스포트 정책('vserver export-policy rule show')을 확인하십시오

   명령 출력은 다음과 같아야 합니다.

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

이러한 규칙이 열려 있는 액세스를 허용하는 경우 이 작업은 완료된 것입니다. 그렇지 않은 경우 다음 단계를 진행하십시오.

2. SVM 루트 볼륨에 대한 엑스포트 규칙을 생성합니다. 'vserver export-policy rule create-vserver vserver_name-policyname default-ruleindex 1-protocol cifs-clientmatch 0.0.0.0/0 -rorule any-rwrule any-superuser any'입니다
3. 'vserver export-policy rule show' 명령을 사용하여 규칙 생성을 확인합니다.

결과

이제 모든 SMB 클라이언트가 SVM에서 생성된 모든 볼륨 또는 qtree에 액세스할 수 있습니다.

ONTAP SMB LIF를 생성합니다

LIF는 물리적 포트 또는 논리적 포트와 연결된 IP 주소입니다. 구성요소 장애가 발생할 경우 LIF가 다른 물리적 포트로 페일오버되거나 마이그레이션되어 네트워크와 계속 통신할 수 있습니다.

시작하기 전에

- 기본 물리적 또는 논리적 네트워크 포트가 관리 `up` 상태로 구성되어야 합니다. 에 대한 자세한 내용은 `up` "ONTAP 명령 참조입니다"을 참조하십시오.
- 서브넷 이름을 사용하여 LIF에 대한 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 이미 존재해야 합니다.

  서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 네트워크 서브넷 만들기 명령을 사용하여 만듭니다.

  에 대한 자세한 내용은 `network subnet create` "ONTAP 명령 참조입니다"을 참조하십시오.

- LIF가 처리하는 트래픽 유형을 지정하는 메커니즘이 변경되었습니다. ONTAP 9.5 이전 버전의 경우 LIF는 역할을 사용하여 처리할 트래픽 유형을 지정합니다. ONTAP 9.6부터 LIF는 서비스 정책을 사용하여 처리할 트래픽 유형을 지정합니다.

이 작업에 대해

- 동일한 네트워크 포트에서 IPv4 및 IPv6 LIF를 모두 생성할 수 있습니다.
- 클러스터에 LIF가 많은 경우 'network interface capacity show' 명령을 사용하여 클러스터에서 지원되는 LIF 용량과 각 노드에서 지원되는 LIF 용량을 확인할 수 있습니다 (고급 권한 수준에서).

  에 대한 자세한 내용은 `network interface` "ONTAP 명령 참조입니다"을 참조하십시오.

- ONTAP 9.7부터 동일한 서브넷에 있는 SVM에 대한 다른 LIF가 이미 있는 경우 LIF의 홈 포트를 지정할 필요가 없습니다. ONTAP는 동일한 서브넷에 이미 구성된 다른 LIF와 동일한 브로드캐스트 도메인에 있는 지정된 홈 노드에서 랜덤 포트를 자동으로 선택합니다.

단계

1. LIF 생성:

   'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol cifs-home-node_node_name_-home-port_port_name_{-address_ip_address_-netmask ip_address|-subnet-name_subnet_name_}-firewall-policy data-auto-revert{true|false}'

* ONTAP 9.5 이하 *
'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol cifs-home-node_node_name_-home-port_port_name_{-address_name_- netmask_ip_address_
- subnet-name_subnet_name_} -firewall-policy data-auto-revert{true
false}

* ONTAP 9.6 이상 *
'network interface create-vserver_vserver_name_-lif_lif_name_-service-policy_service_policy_name_-home-node_node_name_-home-port_port_name_{-address_netmask_ip_address_
-subnet_name_subnet_name_} -firewall-policy data-auto-revert_revert_false

   - 서비스 정책(ONTAP 9.6부터)을 사용하여 LIF를 생성할 때는 '-role' 매개 변수가 필요하지 않습니다.
   - 를 클릭합니다 `-data-protocol` ONTAP 9.6부터 서비스 정책을 사용하여 LIF를 생성할 때 매개 변수가 필요하지 않습니다. ONTAP 9.5 이하 버전을 사용하는 경우 `-data-protocol` LIF를 생성할 때 매개 변수를 지정해야 하며 나중에 데이터 LIF를 폐기 및 재생성하지 않고 수정할 수 없습니다.
   - 홈 노드는 LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환하는 노드입니다.

     또한 LIF가 '-auto-revert' 옵션을 사용하여 홈 노드 및 홈 포트로 자동으로 되돌아가는지 여부를 지정할 수도 있습니다.

   - '-home-port'는 LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 물리적 또는 논리적 포트입니다.
   - IP 주소는 '-address' 및 '-netmask' 옵션을 사용하여 지정하거나 '-subnet_name' 옵션을 사용하여 서브넷에서 할당을 활성화할 수 있습니다.
   - 서브넷을 사용하여 IP 주소와 네트워크 마스크를 제공하면, 서브넷에 정의된 서브넷이 해당 서브넷을 사용하여 LIF를 생성할 때 해당 게이트웨이에 대한 기본 경로가 SVM에 자동으로 추가됩니다.

◦ 서브넷을 사용하지 않고 수동으로 IP 주소를 할당하는 경우 다른 IP 서브넷에 클라이언트 또는 도메인 컨트롤러가 있는 경우 게이트웨이에 대한 기본 라우트를 구성해야 할 수 있습니다. SVM 내에서 정적 라우트를 생성하는 방법에 대한 자세한 `network route create` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

◦ '-firewall-policy' 옵션의 경우 LIF 역할과 동일한 기본 data를 사용합니다.

필요에 따라 나중에 사용자 지정 방화벽 정책을 만들고 추가할 수 있습니다.

ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 참조하십시오 "LIF의 방화벽 정책을 구성합니다".

◦ '-자동 되돌리기'를 사용하면 시작, 관리 데이터베이스의 상태 변경 또는 네트워크 연결이 이루어지는 시기에 데이터 LIF가 홈 노드로 자동 복구되는지 여부를 지정할 수 있습니다. 기본 설정은 false로 설정되어 있지만 사용자 환경의 네트워크 관리 정책에 따라 false로 설정할 수 있습니다.

2. LIF가 성공적으로 생성되었는지 확인합니다.

네트워크 인터페이스 쇼

3. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

다음을 확인하려면…	사용…
IPv4 주소입니다	네트워크 핑
IPv6 주소입니다	네트워크 핑6

예

다음 명령을 실행하면 LIF가 생성되고 '-address' 및 '-netmask' 매개 변수를 사용하여 IP 주소와 네트워크 마스크 값이 지정됩니다.

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

다음 명령을 실행하면 LIF가 생성되고 지정된 서브넷(client1_sub 이름)의 IP 주소와 네트워크 마스크 값이 할당됩니다.

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

다음 명령을 실행하면 cluster-1의 모든 LIF가 표시됩니다. 데이터 LIF datalif1 및 datalif3은 IPv4 주소로 구성되고 datalif4는 IPv6 주소로 구성됩니다.

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

다음 명령을 실행하면 기본 데이터 파일 서비스 정책에 할당된 NAS 데이터 LIF를 생성하는 방법이 표시됩니다.

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

관련 정보

- "네트워크 Ping"
- "네트워크 인터페이스 복원"

ONTAP SMB 호스트 이름 확인을 위해 DNS를 활성화합니다

명령을 사용하여 SVM에서 DNS를 사용하도록 설정하고, 호스트 이름 확인에 DNS를 사용하도록 구성할 수 `vserver services name-service dns` 있습니다. 호스트 이름은 외부 DNS 서버를 사용하여 확인됩니다. 에 대한 자세한 내용은 `vserver services name-service dns` "ONTAP 명령 참조입니다"을 참조하십시오.

시작하기 전에

호스트 이름 조회에 사이트 전체 DNS 서버를 사용할 수 있어야 합니다.

단일 장애 지점을 방지하려면 둘 이상의 DNS 서버를 구성해야 합니다. `vserver services name-service dns create`DNS 서버 이름을 하나만 입력하면 명령이 경고를 표시합니다. 에 대한 자세한 내용은 `vserver services name-service dns create` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

에 대해 자세히 "SVM에서 동적 DNS 구성"알아보십시오.

단계

1. SVM에서 DNS를 활성화합니다. 'vserver services name-service dns create-vserver vserver_name-domain domain_name-name-servers ip_address-state enabled'

   다음 명령을 실행하면 SVM VS1 에서 외부 DNS 서버 서버가 활성화됩니다.

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   를 클릭합니다 `vserver services name-service dns create` Command는 자동 구성 유효성 검사를 수행하고 ONTAP에서 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

2. 'vserver services name-service dns show' 명령을 사용하여 DNS 도메인 구성을 표시합니다.

   다음 명령을 실행하면 클러스터의 모든 SVM에 대한 DNS 구성이 표시됩니다.

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   다음 명령을 실행하면 SVM VS1 에 대한 자세한 DNS 구성 정보가 표시됩니다.

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. 'vserver services name-service dns check' 명령어를 이용하여 이름 서버의 상태를 확인한다.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver            Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Active Directory 도메인에서 **SMB** 서버를 설정합니다

SMB 서버에 대한 **ONTAP** 시간 서비스를 구성합니다

Active Domain 컨트롤러에서 SMB 서버를 생성하기 전에 SMB 서버가 속할 도메인의 도메인 컨트롤러에 대한 클러스터 시간 및 시간이 5분 이내에 일치하는지 확인해야 합니다.

이 작업에 대해

Active Directory 도메인에서 사용하는 것과 동일한 NTP 서버를 동기화에 사용하도록 클러스터 NTP 서비스를 구성해야 합니다.

ONTAP 9.5부터 대칭 인증을 사용하여 NTP 서버를 설정할 수 있습니다.

단계

1. cluster time-service NTP server create 명령을 사용하여 시간 서비스를 구성합니다.
   - 대칭 인증 없이 시간 서비스를 구성하려면 'cluster time-service ntp server create-server_ip_address' 명령을 입력합니다
   - 대칭적 인증으로 시간 서비스를 구성하려면 'cluster time-service ntp server create-server_ip_address-key-id key-id key_id"cluster time-service ntp server create-server 10.10.10.1"cluster time-service ntp server create-server 10.10.10.10.10.10.2' 명령을 입력한다
2. cluster time-service ntp server show 명령을 사용하여 시간 서비스가 올바르게 설정되었는지 확인합니다.

   클러스터 시간 서비스 NTP 서버가 표시됩니다

```
Server                          Version
------------------------------- -------
10.10.10.1                      auto
10.10.10.2                      auto
```

관련 정보

- "클러스터 시간 - 서비스 NTP"

NTP 서버에서 대칭 인증을 관리하기 위한 **ONTAP** 명령

ONTAP 9.5부터 NTP(네트워크 시간 프로토콜) 버전 3이 지원됩니다. NTPv3에는 SHA-1 키를 사용한 대칭 인증이 포함되어 있어 네트워크 보안을 강화합니다.

수행할 작업...	이 명령 사용...
대칭 인증 없이 NTP 서버를 구성합니다	클러스터 시간 서비스 NTP 서버는 서버 서버 서버 서버 이름(server_name)을 만듭니다
대칭 인증을 사용하여 NTP 서버를 구성합니다	클러스터 시간 서비스 NTP 서버는 '-server"server_ip_address"-key-id"key_id'를 생성합니다
기존 NTP 서버에 대칭 인증 사용 기존 NTP 서버는 필요한 키 ID를 추가하여 인증을 사용하도록 수정할 수 있습니다	클러스터 시간서비스NTP 서버 수정 서버 서버 서버 서버 서버 서버 서버 서버 이름 키 ID 키 ID
공유 NTP 키를 구성합니다	클러스터 시간 서비스 NTP 키는 ``id"sshared_key_id' -type'sshared_key_type' -value'sshared_key_value'를 만듭니다 공유 키는 ID로 참조됩니다. ID, 유형 및 값은 노드와 NTP 서버 모두에서 동일해야 합니다
알 수 없는 키 ID로 NTP 서버를 구성합니다	클러스터 시간 서비스 NTP 서버는 서버 서버 서버 이름 키 ID 키 ID를 만듭니다
NTP 서버에 키 ID가 구성되지 않은 서버를 구성합니다.	클러스터 시간 서비스 NTP 서버는 서버 서버 서버 이름 키 ID 키 ID를 만듭니다 키 ID, 유형 및 값은 NTP 서버에 구성된 키 ID, 유형 및 값과 동일해야 합니다.
대칭 인증을 사용하지 않도록 설정합니다	클러스터 시간서비스NTP 서버 수정 서버 서버 서버 서버 서버 서버 서버 서버 이름 인증 비활성화

관련 정보

- "클러스터 시간 - 서비스 NTP"

ONTAP Active Directory 도메인에 **SMB** 서버를 생성합니다

"vserver cifs create" 명령을 사용하여 SVM에 SMB 서버를 생성하고 해당 서버가 속한 AD(Active Directory) 도메인을 지정할 수 있습니다.

시작하기 전에

데이터 제공을 위해 사용하는 SVM 및 LIF는 SMB 프로토콜을 허용하도록 구성되어 있어야 합니다. LIF는 SVM에 구성된 DNS 서버와 SMB 서버에 연결할 도메인의 AD 도메인 컨트롤러에 연결할 수 있어야 합니다.

SMB 서버에 연결할 AD 도메인에서 시스템 계정을 만들 수 있는 권한이 있는 모든 사용자는 SVM에 SMB 서버를 생성할 수 있습니다. 여기에는 다른 도메인의 사용자가 포함될 수 있습니다.

ONTAP 9.7부터 AD 관리자는 권한이 있는 Windows 계정에 이름과 암호를 제공하는 대신 keytab 파일에 대한 URI를 제공할 수 있습니다. URI를 받으면 '-keytab-Uri' 매개 변수에 vserver cifs' 명령을 포함하여 포함시키십시오.

이 작업에 대해

Activity Directory 도메인에서 SMB 서버를 생성하는 경우:

- 도메인을 지정할 때는 FQDN(정규화된 도메인 이름)을 사용해야 합니다.
- 기본 설정은 Active Directory CN=Computer 개체에 SMB 서버 컴퓨터 계정을 추가하는 것입니다.
- '-ou' 옵션을 사용하여 SMB 서버를 다른 OU(조직 구성 단위)에 추가하도록 선택할 수 있습니다.
- SMB 서버에 대해 쉼표로 구분된 하나 이상의 NetBIOS 별칭 목록(최대 200)을 추가하도록 선택할 수도 있습니다.

  SMB 서버에 대한 NetBIOS 별칭을 구성하면 다른 파일 서버의 데이터를 SMB 서버로 통합할 때 SMB 서버가 원래 서버의 이름에 응답하도록 할 때 유용합니다.

및 선택적 매개 변수 및 명명 요구 사항에 대한 자세한 `vserver cifs` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

ONTAP 9.8부터 도메인 컨트롤러에 대한 연결이 암호화되도록 지정할 수 있습니다. ONTAP는 `-encryption-required-for-dc-connection' 옵션이 true로 설정되어 있을 때 도메인 컨트롤러 통신을 암호화해야 하며 기본값은 false입니다. SMB3에서만 암호화가 지원되므로 이 옵션을 설정하면 SMB3 프로토콜만 ONTAP-DC 연결에 사용됩니다. .

"SMB 관리" SMB 서버 구성 옵션에 대한 자세한 내용은 에 나와 있습니다.

단계

1. smb 라이센스가 클러스터에 있는지 확인합니다: 'system license show-package cifs'

   SMB 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오"있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

   SMB 서버가 인증용으로만 사용되는 경우에는 CIFS 라이센스가 필요하지 않습니다.

2. AD 도메인에서 SMB 서버를 생성합니다.(+ vserver cifs create -vserver vserver_name -cifs -server smb_server_name -domain FQDN [-ou 조직_unit] [-NetBIOS-별칭 netbios_name,…] [-keytab -Uri {(ftp | http)://hostname | ip_address}] [-comment text]+'

도메인에 참가할 때 이 명령을 완료하는 데 몇 분 정도 걸릴 수 있습니다.

다음 명령을 실행하면 도메인 " example.com`": 에 SMB 서버 "'smb_server01'"이 생성됩니다

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
smb_server01 -domain example.com
```

다음 명령을 실행하면 도메인 "mydomain.com`" 에 SMB 서버 "sMB_server02"가 생성되고 keytab 파일을 사용하여 ONTAP 관리자를 인증합니다.

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
smb_server02 -domain mydomain.com -keytab-uri
http://admin.mydomain.com/ontap1.keytab
```

3. 'vserver cifs show' 명령을 사용하여 SMB 서버 구성을 확인합니다.

   이 예제에서 명령 출력은 "'sMB_SERVER01'"이라는 SMB 서버가 SVM vs1.example.com 에서 생성되어 "'example.com`" 도메인에 가입된 것을 보여 줍니다.

```
cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: -
```

4. 필요한 경우 도메인 컨트롤러(ONTAP 9.8 이상)와의 암호화된 통신을 활성화합니다. 'vserver cifs security modify -vserver svm_name -encryption -required-for-dc-connection true'

예

다음 명령을 실행하면 ""example.com`"" 도메인의 SVM vs2.example.com 에 "sMB_server02" 이름의 SMB 서버가 생성됩니다. 컴퓨터 계정은 ""OU=ENG,OU=Corp,DC=example,DC=com" 컨테이너에 생성됩니다. SMB 서버에는 NetBIOS 별칭이 할당됩니다.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                          Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

다음 명령을 사용하면 다른 도메인의 사용자(이 경우 신뢰할 수 있는 도메인 관리자)가 SVM vs3.example.com 에 "'smb_server03" 이름의 SMB 서버를 생성할 수 있습니다. '-domain' 옵션은 SMB 서버를 생성하려는 홈 도메인(DNS 구성에 지정됨)의 이름을 지정합니다. 사용자 이름 옵션은 신뢰할 수 있는 도메인의 관리자를 지정합니다.

- 홈 도메인: example.com
- 신뢰할 수 있는 도메인: trust.lab.com
- 신뢰할 수 있는 도메인의 사용자 이름: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

ONTAP SMB 인증을 위한 **keytab** 파일을 생성합니다

ONTAP 9.7부터 ONTAP는 keytab 파일을 사용하여 AD(Active Directory) 서버에서 SVM 인증을 지원합니다. AD 관리자는 keytab 파일을 생성하여 ONTAP 관리자가 이를 URI(Uniform Resource Identifier)로 사용할 수 있도록 합니다. 이 URI는 'vserver cifs' 명령에 AD 도메인과의 Kerberos 인증이 필요한 경우에 제공됩니다.

AD 관리자는 표준 Windows Server "ktpass" 명령을 사용하여 keytab 파일을 만들 수 있습니다. 이 명령은 인증이 필요한 기본 도메인에서 실행해야 합니다. "ktpass" 명령은 기본 도메인 사용자에 대해서만 keytab 파일을 생성하는 데 사용할 수 있으며, trusted-domain 사용자를 사용하여 생성된 키는 지원되지 않습니다.

Keytab 파일은 특정 ONTAP 관리자 사용자를 위해 생성됩니다. admin 사용자의 암호가 변경되지 않는 한, 특정 암호화 유형 및 도메인에 대해 생성된 키는 변경되지 않습니다. 따라서 admin 사용자의 암호를 변경할 때마다 새 keytab 파일이 필요합니다.

지원되는 암호화 유형은 다음과 같습니다.

- AES256-SHA1
- DES-CBC-MD5

  ONTAP는 DES-CBC-CRC 암호화 유형을 지원하지 않습니다.

- RC4-HMAC

AES256은 가장 높은 암호화 유형으로, ONTAP 시스템에서 활성화된 경우 사용해야 합니다.

keytab 파일은 admin 암호를 지정하거나 임의로 생성된 암호를 사용하여 생성할 수 있습니다. 그러나 언제든지 한 개의 암호 옵션만 사용할 수 있습니다. AD 서버에서는 키 탭 파일 내의 키를 해독하기 위해 관리자 사용자 고유의 개인 키가 필요하기 때문입니다. 특정 관리자에 대한 개인 키를 변경하면 keytab 파일이 무효화됩니다.

워크그룹에서 **SMB** 서버를 설정합니다

ONTAP 워크그룹의 **SMB** 서버 구성에 대해 알아보십시오

작업 그룹에서 SMB 서버를 구성원으로 설정하는 작업은 SMB 서버를 생성한 다음 로컬 사용자 및 그룹을 만드는 작업으로 구성됩니다.

Microsoft Active Directory 도메인 인프라를 사용할 수 없는 경우 작업 그룹에서 SMB 서버를 구성할 수 있습니다.

작업 그룹 모드의 SMB 서버는 NTLM 인증만 지원하며 Kerberos 인증을 지원하지 않습니다.

지정된 작업 그룹을 사용하여 **ONTAP SVM**에 **SMB** 서버를 생성합니다

"vserver cifs create" 명령을 사용하여 SVM에 SMB 서버를 생성하고 해당 서버가 속한 작업 그룹을 지정할 수 있습니다.

시작하기 전에

데이터 제공을 위해 사용하는 SVM 및 LIF는 SMB 프로토콜을 허용하도록 구성되어 있어야 합니다. LIF는 SVM에 구성된 DNS 서버에 연결할 수 있어야 합니다.

이 작업에 대해

워크그룹 모드의 SMB 서버는 다음 SMB 기능을 지원하지 않습니다.

- SMB3 Witness 프로토콜
- SMB3 CA 공유
- SMB를 통한 SQL
- 폴더 리디렉션
- 로밍 프로필
- GPO(그룹 정책 개체)
- VSS(볼륨 스냅샷 서비스)

및 선택적 구성 매개 변수 및 명명 요구 사항에 대한 자세한 `vserver cifs` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

단계

1. smb 라이센스가 클러스터에 있는지 확인합니다: 'system license show-package cifs'

   SMB 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오"있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

   SMB 서버가 인증용으로만 사용되는 경우에는 CIFS 라이센스가 필요하지 않습니다.

2. 워크그룹에서 SMB 서버를 생성합니다. 'vserver cifs create-vserver vserver_name-cifs-server cifs_server_name-workgroup workgroup_name[-comment text]'

   다음 명령을 실행하면 워크그룹 workgroup01에 SMB 서버 "smb_server01"이 생성됩니다.

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. 'vserver cifs show' 명령을 사용하여 SMB 서버 구성을 확인합니다.

   다음 예제에서 명령 출력은 "'workgroup01'" 워크그룹의 SVM vs1.example.com 에서 "'smb_server01'" 이름의 SMB 서버가 생성되었음을 보여 줍니다.

   ```
   cluster1::> vserver cifs show -vserver vs0

                                             Vserver: vs1.example.com
                          CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
   Default Site Used by LIFs Without Site Membership: -
                                   Workgroup Name: workgroup01
                              Authentication Style: workgroup
                  CIFS Server Administrative Status: up
                            CIFS Server Description:
                            List of NetBIOS Aliases: -
   ```

작업을 마친 후

작업 그룹의 CIFS 서버의 경우 SVM에서 로컬 사용자와 로컬 그룹을 생성해야 합니다(선택 사항).

관련 정보

"SMB 관리"

로컬 **ONTAP SMB** 사용자 계정을 생성합니다

SMB 연결을 통해 SVM에 포함된 데이터에 대한 액세스를 승인하는 데 사용할 수 있는 로컬 사용자 계정을 생성할 수 있습니다. SMB 세션을 생성할 때 인증에 로컬 사용자 계정을 사용할 수도 있습니다.

이 작업에 대해

SVM이 생성되면 로컬 사용자 기능이 기본적으로 활성화됩니다.

로컬 사용자 계정을 생성할 때 사용자 이름을 지정해야 하며 계정을 연결할 SVM을 지정해야 합니다.

및 선택적 매개 변수 및 명명 요구 사항에 대한 자세한 `vserver cifs users-and-groups local-user` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

단계

1. 로컬 사용자:'vserver cifs users-and-groups local-user create-vserver_vserver_name_-user-name_user_name__optional_parameters_'를 생성합니다

   다음과 같은 선택적 매개 변수가 유용할 수 있습니다.

   - 이름

     사용자의 전체 이름입니다.

   - ``설명''

     로컬 사용자에 대한 설명입니다.

   - '-is-account-disabled{true|false}'

     사용자 계정의 사용 여부를 지정합니다. 이 매개 변수를 지정하지 않으면 기본값은 사용자 계정을 활성화하는 것입니다.

   명령을 실행하면 로컬 사용자 암호를 묻는 메시지가 표시됩니다.

2. 로컬 사용자의 암호를 입력한 다음 암호를 확인합니다.
3. 사용자가 성공적으로 생성되었는지 확인합니다. 'vserver cifs users-and-groups local-user show -vserver_vserver_name_'

예

다음 예에서는 SVM vs1.example.com 과 관련된 "sUE Chang"이라는 전체 이름으로 로컬 사용자 "sMB_SERVER01\sue"를 생성합니다.

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- --------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator             Built-in administrator
account
vs1      SMB_SERVER01\sue             Sue Chang
```

로컬 **ONTAP SMB** 그룹을 생성합니다

SMB 연결을 통해 SVM과 관련된 데이터에 대한 액세스 권한을 부여하는 데 사용할 수 있는 로컬 그룹을 생성할 수 있습니다. 그룹의 구성원이 보유한 사용자 권한 또는 기능을 정의하는 권한을 할당할 수도 있습니다.

이 작업에 대해

SVM이 생성되면 로컬 그룹 기능이 기본적으로 활성화됩니다.

로컬 그룹을 생성할 때 그룹 이름을 지정해야 하며 그룹을 연결할 SVM을 지정해야 합니다. 로컬 도메인 이름을 사용하거나 사용하지 않고 그룹 이름을 지정할 수 있으며, 선택적으로 로컬 그룹에 대한 설명을 지정할 수 있습니다. 로컬 그룹을 다른 로컬 그룹에 추가할 수 없습니다.

및 선택적 매개 변수 및 명명 요구 사항에 대한 자세한 `vserver cifs users-and-groups local-group` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

단계

1. 로컬 그룹 'vserver cifs users-and-groups local-group create-vserver vserver_name-group-name group_name'을 생성합니다

   다음과 같은 선택적 매개 변수가 유용할 수 있습니다.

   - ``설명''

     로컬 그룹에 대한 설명입니다.

2. 그룹이 성공적으로 생성되었는지 확인합니다. 'vserver cifs users-and-groups local-group show-vserver vserver_name'

예

다음 예에서는 SVM VS1 관련 로컬 그룹 "sMB_SERVER01\engineering"을 생성합니다.

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                    Description
---------------- ----------------------------- ----------------------------
vs1.example.com  BUILTIN\Administrators        Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators      Backup Operators group
vs1.example.com  BUILTIN\Power Users           Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                 All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

작업을 마친 후

새 그룹에 구성원을 추가해야 합니다.

로컬 **ONTAP SMB** 그룹 구성원 자격을 관리합니다

로컬 또는 도메인 사용자를 추가 및 제거하거나 도메인 그룹을 추가 및 제거하여 로컬 그룹 구성원 자격을 관리할 수 있습니다. 이 기능은 그룹에 배치된 액세스 제어를 기반으로 데이터에 대한 액세스를 제어하려는 경우 또는 사용자가 해당 그룹에 연결된 권한을 가지도록 하려는 경우에 유용합니다.

이 작업에 대해

더 이상 로컬 사용자, 도메인 사용자 또는 도메인 그룹이 그룹의 구성원 자격에 따라 액세스 권한이나 권한을 가지도록 하지 않으려면 그룹에서 해당 구성원을 제거할 수 있습니다.

로컬 그룹에 구성원을 추가할 때는 다음 사항을 염두에 두어야 합니다.

- special_everyone_group에 사용자를 추가할 수 없습니다.
- 로컬 그룹을 다른 로컬 그룹에 추가할 수 없습니다.
- 도메인 사용자 또는 그룹을 로컬 그룹에 추가하려면 ONTAP에서 SID에 대한 이름을 확인할 수 있어야 합니다.

로컬 그룹에서 구성원을 제거할 때는 다음 사항을 염두에 두어야 합니다.

- special_everyone_group에서 구성원을 제거할 수 없습니다.
- 로컬 그룹에서 구성원을 제거하려면 ONTAP에서 해당 이름을 SID로 확인할 수 있어야 합니다.

단계

1. 그룹에 구성원을 추가하거나 그룹에서 구성원을 제거합니다.
    - 멤버(+ vserver cifs users-and-groups local-group add-member -vserver_name -group-name group_name -member-name name[,…]+')를 추가합니다

로컬 사용자, 도메인 사용자 또는 도메인 그룹의 쉼표로 구분된 목록을 지정하여 지정된 로컬 그룹에 추가할 수 있습니다.

- 멤버(+ vserver cifs users-and-groups local-group remove-member-vserver vserver_name -group-name group_name -member-name[,…]+')를 제거합니다

  로컬 사용자, 도메인 사용자 또는 도메인 그룹의 쉼표로 구분된 목록을 지정하여 지정된 로컬 그룹에서 제거할 수 있습니다.

예

다음 예에서는 SVM vs1.example.com 에서 로컬 사용자 "sMB_SERVER01\SUB""를 로컬 그룹 "sMB_SERVER01\engineering""에 추가합니다.

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

다음 예에서는 SVM vs1.example.com 에서 로컬 그룹 "sMB_SERVER01\engineering"에서 로컬 사용자 "sMB_SERVER01\SUB" 및 "sMB_SERVER01\James"를 제거합니다.

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

활성화된 **ONTAP SMB** 버전을 확인합니다

ONTAP 9 릴리즈에서는 클라이언트 및 도메인 컨트롤러와의 연결에 대해 기본적으로 설정되는 SMB 버전을 결정합니다. SMB 서버가 사용자 환경에 필요한 클라이언트 및 기능을 지원하는지 확인해야 합니다.

이 작업에 대해

클라이언트 및 도메인 컨트롤러 모두에 연결하는 경우 가능하면 SMB 2.0 이상을 활성화해야 합니다. 보안상의 이유로 SMB 1.0은 사용하지 않는 것이 좋습니다. 사용자 환경에서 필요하지 않은 것으로 확인된 경우에는 사용하지 않도록 설정해야 합니다.

ONTAP 9.3부터는 새 SVM에서 기본적으로 비활성화되어 있습니다.

SMB1-enabled-for-dc-connections가 false로 설정되어 있고 -SMB1-enabled가 true로 설정되어 있으면 ONTAP는 SMB 1.0 연결을 클라이언트로 거부하지만 인바운드 SMB 1.0 연결을 서버로 계속 허용합니다.

"SMB 관리" 지원되는 SMB 버전 및 기능에 대한 자세한 내용은 에 나와 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 활성화된 SMB 버전을 확인합니다.

```
vserver cifs options show
```

목록을 아래로 스크롤하여 클라이언트 연결에 대해 설정된 SMB 버전을 볼 수 있으며 AD 도메인 연결에 대해 AD 도메인에서 SMB 서버를 구성하는 경우

3. 필요에 따라 클라이언트 연결에 대해 SMB 프로토콜을 설정하거나 해제합니다.
   - SMB 버전 활성화하기:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
true
```

에 사용할 수 있는 값 `smb_version`:

- '-SMB1-활성화됨'
- '-SMB2-ENABLED'입니다
- '-SMB3-enabled'입니다
- `-smb31-enabled`

다음 명령을 실행하면 SVM vs1.example.com 에서 SMB 3.1이 활성화됩니다.
`cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31 -enabled true`

   - SMB 버전을 사용하지 않도록 설정하려면:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. SMB 서버가 Active Directory 도메인에 있는 경우 필요에 따라 DC 연결에 대한 SMB 프로토콜을 설정하거나 해제합니다.
   - SMB 버전 활성화하기:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

   - SMB 버전을 사용하지 않도록 설정하려면:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

ONTAP SMB 서버를 **DNS** 서버에 매핑합니다

Windows 사용자가 SMB 서버 이름에 드라이브를 매핑할 수 있도록 사이트의 DNS 서버에는 SMB 서버 이름 및 모든 NetBIOS 별칭을 가리키는 항목이 데이터 LIF의 IP 주소에 있어야 합니다.

시작하기 전에

사이트의 DNS 서버에 대한 관리 액세스 권한이 있어야 합니다. 관리 액세스 권한이 없는 경우 DNS 관리자에게 이 작업을 수행하도록 요청해야 합니다.

이 작업에 대해

SMB 서버 이름에 NetBIOS 별칭을 사용하는 경우 각 별칭에 대해 DNS 서버 진입점을 만드는 것이 좋습니다.

단계

1. DNS 서버에 로그인합니다.
2. 정방향(A-Address 레코드) 및 역방향(PTR-포인터 레코드) 조회 항목을 만들어 SMB 서버 이름을 데이터 LIF의 IP 주소에 매핑합니다.
3. NetBIOS 별칭을 사용하는 경우 별칭 정규 이름(CNAME 리소스 레코드) 조회 항목을 만들어 각 별칭을 SMB 서버 데이터 LIF의 IP 주소에 매핑합니다.

결과

매핑이 네트워크를 통해 전파되면 Windows 사용자는 드라이브를 SMB 서버 이름 또는 NetBIOS 별칭에 매핑할 수 있습니다.

공유 스토리지에 대한 **SMB** 클라이언트 액세스를 구성합니다

공유 **ONTAP** 스토리지에 대한 **SMB** 클라이언트 액세스를 구성합니다

SVM에서 공유 스토리지에 SMB 클라이언트가 액세스할 수 있도록 하려면 스토리지 컨테이너를 제공할 볼륨 또는 qtree를 생성한 다음 해당 컨테이너에 대한 공유를 생성하거나 수정해야 합니다. 그런 다음 공유 및 파일 권한을 구성하고 클라이언트 시스템에서 액세스를 테스트할 수 있습니다.

시작하기 전에

- SVM에서 SMB를 완전히 설정해야 합니다.
- 이름 서비스 구성에 대한 모든 업데이트를 완료해야 합니다.

- Active Directory 도메인 또는 작업 그룹 구성에 대한 추가 또는 수정 작업을 완료해야 합니다.

볼륨 또는 **qtree** 스토리지 컨테이너를 생성합니다

ONTAP SMB 볼륨을 생성합니다

볼륨을 생성하고 "volume create" 명령을 사용하여 해당 접합 지점 및 기타 속성을 지정할 수 있습니다.

이 작업에 대해

클라이언트에서 데이터를 사용할 수 있도록 하려면 볼륨에 _junction path_가 포함되어야 합니다. 새 볼륨을 생성할 때 접합 경로를 지정할 수 있습니다. 접합 경로를 지정하지 않고 볼륨을 생성하는 경우, "volume mount" 명령을 사용하여 SVM 네임스페이스에서 볼륨을 _mount_해야 합니다.

시작하기 전에

- SMB를 설정하고 실행해야 합니다.
- SVM 보안 스타일은 NTFS여야 합니다.
- ONTAP 9.13.1부터 용량 분석 및 활동 추적이 활성화된 볼륨을 생성할 수 있습니다. 용량 또는 활동 추적을 활성화하려면 `volume create` 또는 `-activity-tracking-state` 를 로 설정하여 `on` 명령을 `-analytics-state` 실행합니다.

  용량 분석 및 활동 추적에 대한 자세한 내용은 을 참조하십시오 "파일 시스템 분석 설정". 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 교차점으로 볼륨을 생성합니다. `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path` *`junction_path`*`]`

   '-junction-path'의 선택 항목은 다음과 같습니다.

   - 루트 바로 아래, 예: '/new_vol'

     새 볼륨을 생성하고 SVM 루트 볼륨에 직접 마운트하도록 지정할 수 있습니다.

   - 기존 디렉토리 아래에 '/existing_dir/new_vol' 등이 있습니다

     새 볼륨을 생성하고 기존 계층 구조에서 기존 볼륨에 마운트하도록 지정할 수 있습니다. 이 볼륨은 디렉토리로 표시됩니다.

   새 볼륨 아래의 새 계층 구조에서 "/new_dir/new_vol"과 같은 새 디렉토리에 볼륨을 생성하려면 먼저 SVM 루트 볼륨에 대한 분기인 새 상위 볼륨을 생성해야 합니다. 그런 다음 새 상위 볼륨(새 디렉토리)의 접합 경로에 새 하위 볼륨을 생성합니다.

2. 볼륨이 원하는 접합 지점으로 생성되었는지 확인합니다. `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

예

다음 명령을 실행하면 SVM vs1.example.com 및 애그리게이트 aggr1에 user1이라는 새 볼륨이 생성됩니다. 새

볼륨은 '/users'에서 사용할 수 있습니다. 볼륨의 크기는 750GB이고 볼륨 유형은 볼륨 유형입니다(기본값).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

다음 명령을 실행하면 SVM의 ""home4" vs1.example.com`""와 애그리게이트 ""aggr1""에 새 볼륨이 생성됩니다. VS1 SVM은 이름 공간에 /ENG/ 디렉토리가 이미 있으며, '/ENG/' 네임스페이스의 홈 디렉토리가 되는 '/ENG/HOME'에서 새 볼륨을 사용할 수 있습니다. 볼륨 크기는 750GB이고 볼륨 보장은 볼륨 유형입니다(기본값).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4    true     /eng/home       RW_volume
```

ONTAP SMB qtree를 생성합니다

'volume qtree create' 명령을 사용하여 데이터를 포함하는 qtree를 생성하고 해당 속성을 지정할 수 있습니다.

시작하기 전에

- SVM과 새 qtree가 포함될 볼륨이 이미 존재해야 합니다.
- SVM 보안 스타일은 NTFS여야 하며 SMB를 설정하고 실행해야 합니다.

단계

1. qtree:'volume qtree create-vserver vserver_name{-volume volume_name-qtree qtree_name|-qtree-path qtree path qtree path}-security-style NTFS'를 생성합니다

   볼륨과 qtree를 별도의 인수로 지정하거나 qtree 경로 인수를 '/vol/volume_name/_qtree_name' 형식으로 지정할 수 있습니다.

2. qtree가 'volume qtree show-vserver vserver_name{-volume volume_name-qtree qtree qtree_name|-qtree-path qtree path}' 접합 경로로 생성되었는지 확인합니다

예

다음 예에서는 junction path '/vol/data1'이 있는 SVM vs1.example.com 에 qt01이라는 이름의 qtree를 생성합니다.

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: ntfs
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

ONTAP SMB 공유를 생성할 때의 요구 사항 및 고려 사항

SMB 공유를 생성하기 전에 공유 경로 및 공유 속성, 특히 홈 디렉토리에 대한 요구 사항을 이해해야 합니다.

SMB 공유를 생성하려면 클라이언트가 액세스할 디렉토리 경로 구조('vserver cifs share create' 명령의 '-path' 옵션 사용)를 지정해야 합니다. 디렉토리 경로는 SVM 네임스페이스에서 생성한 볼륨 또는 qtree의 접합 경로에 해당합니다. 공유를 생성하기 전에 디렉토리 경로 및 해당 접속 경로가 있어야 합니다.

공유 경로에는 다음과 같은 요구 사항이 있습니다.

- 디렉터리 경로 이름은 최대 255자까지 지정할 수 있습니다.
- 경로 이름에 공백이 있으면 전체 문자열을 따옴표로 묶어야 합니다(예: "/new volume/mount here").
- 공유의 UNC 경로('\\servername\sharename\filepath')에 256자 이상(UNC 경로의 초기 ""\\" 제외)이 포함되어 있으면 Windows 속성 상자의 * Security * 탭을 사용할 수 없습니다.

  이것은 ONTAP 문제가 아니라 Windows 클라이언트 문제입니다. 이 문제를 방지하려면 256자를 초과하는 UNC 경로를 사용하여 공유를 생성하지 마십시오.

공유 속성 기본값은 다음과 같이 변경할 수 있습니다.

- 모든 주식의 기본 초기 속성은 oplocks, 탐색 가능, 변경 및 이전 버전 사용 입니다.
- 공유를 생성할 때 공유 속성을 지정하는 것은 선택 사항입니다.

  그러나 공유를 생성할 때 공유 속성을 지정하면 기본값이 사용되지 않습니다. 공유를 만들 때 '-share-properties'

매개 변수를 사용하는 경우 쉼표로 구분된 목록을 사용하여 공유에 적용할 모든 공유 속성을 지정해야 합니다.

- 홈 디렉토리 공유를 지정하려면 홈 디렉토리 속성을 사용합니다.

  이 기능을 사용하면 연결된 사용자와 변수 집합을 기반으로 서로 다른 디렉토리에 매핑되는 공유를 구성할 수 있습니다. 사용자별로 별도의 공유를 생성할 필요 없이 몇 가지 홈 디렉토리 매개 변수를 사용하여 단일 공유를 구성하여 엔트리 포인트(공유)와 해당 홈 디렉토리(SVM의 디렉토리) 간의 사용자 관계를 정의할 수 있습니다.

  ⓘ 공유를 생성한 후에는 이 속성을 추가하거나 제거할 수 없습니다.

홈 디렉토리 공유에는 다음과 같은 요구 사항이 있습니다.

- SMB 홈 디렉토리를 생성하기 전에 'vserver cifs home-directory search-path add' 명령을 사용하여 적어도 하나의 홈 디렉토리 검색 경로를 추가해야 합니다.
- '-share-properties' 파라미터의 homed디렉토리 값으로 지정된 홈 디렉토리 공유에는 공유 이름에 '%w'(Windows 사용자 이름) 동적 변수가 포함되어야 합니다.

  공유 이름에는 "%d"(도메인 이름) 동적 변수(예: "%d/%w") 또는 공유 이름의 정적 부분(예: " home1_%w")이 추가로 포함될 수 있습니다.

- 관리자 또는 사용자가 공유를 사용하여 다른 사용자의 홈 디렉토리에 연결하는 경우('vserver cifs home-directory modify' 명령 옵션 사용) 동적 공유 이름 패턴 앞에는 물결표('~')가 와야 합니다.

에 대한 자세한 내용은 `vserver cifs share` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "SMB 관리"

ONTAP SMB 공유를 생성합니다

SMB 클라이언트와 SMB 서버의 데이터를 공유하려면 먼저 SMB 공유를 생성해야 합니다. 공유를 생성할 때 공유를 홈 디렉토리로 지정하는 등의 공유 속성을 설정할 수 있습니다. 선택적 설정을 구성하여 공유를 사용자 지정할 수도 있습니다.

시작하기 전에

공유를 생성하기 전에 SVM 네임스페이스에 볼륨 또는 qtree의 디렉토리 경로가 있어야 합니다.

이 작업에 대해

공유를 생성할 때 기본 공유 ACL(기본 공유 권한)은 '모든 사용자/모든 권한'입니다. 공유에 대한 액세스를 테스트한 후에는 기본 공유 ACL을 제거하고 보다 안전한 대체 공유 ACL로 대체해야 합니다.

단계

1. 필요한 경우 공유에 대한 디렉토리 경로 구조를 생성합니다.

   'vserver cifs share create' 명령은 공유 생성 중에 '-path' 옵션에 지정된 경로를 확인합니다. 지정한 경로가 없으면 명령이 실패합니다.

2. 지정된 SVM과 연결된 SMB 공유 생성: "+ vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,…] [Other_attributes] [-comment text]+'

3. 공유가 생성되었는지 확인합니다. "vserver cifs share show-share-name share_name"

예

다음 명령을 실행하면 SVM vs1.example.com "sHARE1"이라는 SMB 공유가 생성됩니다. 디렉터리 경로는 '/users'이며 기본 속성으로 만들어집니다.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                   browsable
                                   changenotify
                                   show-previous-versions
```

ONTAP SMB 클라이언트 액세스를 확인합니다

공유에 데이터를 액세스 및 기록하여 SMB를 올바르게 구성했는지 확인해야 합니다. SMB 서버 이름 및 NetBIOS 별칭을 사용하여 액세스를 테스트해야 합니다.

단계

1. Windows 클라이언트에 로그인합니다.
2. SMB 서버 이름을 사용하여 액세스 테스트:

   a. Windows 탐색기에서 드라이브를 공유 위치에 '\s.\\smb_Server_Name\Share_Name' 형식으로 매핑합니다

      매핑에 성공하지 못한 경우 DNS 매핑이 아직 네트워크 전체에 전파되지 않았을 수 있습니다. 나중에 SMB 서버 이름을 사용하여 액세스를 테스트해야 합니다.

      SMB 서버의 이름이 vs1.example.com 이고 공유 이름이 share1 인 경우 '\n.\vs0.example.com\SHARE1` 을 입력해야 합니다

   b. 새로 만든 드라이브에서 테스트 파일을 만든 다음 파일을 삭제합니다.

   SMB 서버 이름을 사용하여 공유에 대한 쓰기 액세스를 확인했습니다.

3. NetBIOS 별칭에 대해 2단계를 반복합니다.

ONTAP SMB 공유 액세스 제어 목록을 생성합니다

SMB 공유에 대한 ACL(액세스 제어 목록)을 생성하여 공유 권한을 구성하면 사용자 및 그룹의 공유에 대한 액세스 수준을 제어할 수 있습니다.

시작하기 전에

공유에 대한 액세스 권한을 부여할 사용자 또는 그룹을 결정해야 합니다.

이 작업에 대해

로컬 또는 도메인 Windows 사용자 또는 그룹 이름을 사용하여 공유 수준 ACL을 구성할 수 있습니다.

새 ACL을 생성하기 전에 보안 위험을 야기시키는 기본 공유 ACL 'Everyone/Full Control'을 삭제해야 합니다.

워크그룹 모드에서 로컬 도메인 이름은 SMB 서버 이름입니다.

단계

1. 기본 공유 ACL: ``vserver cifs share access-control delete-vserver_vserver_name_-share_share_name_-user-or-group everyone''을 삭제합니다
2. 새 ACL 구성:

을 사용하여 **ACL**을 구성하려면...	명령 입력...
Windows 사용자	'vserver cifs share access-control create-vserver_name_-share_share_name_-user-group-type windows-user-or-group_windows_domain_name\\user_name_-permission access_right'
Windows 그룹	'vserver cifs share access-control create-vserver_name_-share_share_name_-user-group-type windows-user-or-group_windows_group_name_-permission access_right'

3. 'vserver cifs share access-control show' 명령을 사용하여 공유에 적용된 ACL이 올바른지 확인하십시오.

예

다음 명령을 실행하면 vs1.example.com`"SVM: "Sales" 공유에 대한 "Sales Team" Windows 그룹에 대한 "Change" 권한이 부여됩니다

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                 Share       User/Group              User/Group  Access
Vserver          Name        Name                    Type
Permission
---------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\"Sales Team"     windows     Change
```

다음 명령은 로컬 윈도우 그룹인 '타이거 팀'과 'Full_Control'에 대한 'SUE Chang'이라는 이름의 변경 권한을 VS1 SVM의 'datavol5' 공유에 부여합니다.

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

ONTAP SMB 공유에서 **NTFS** 파일 사용 권한을 구성합니다

공유에 대한 액세스 권한이 있는 사용자 또는 그룹에 대한 파일 액세스를 설정하려면 Windows 클라이언트에서 공유하는 파일 및 디렉토리에 대한 NTFS 파일 권한을 구성해야 합니다.

시작하기 전에

이 작업을 수행하는 관리자는 선택한 개체에 대한 권한을 변경할 수 있는 충분한 NTFS 권한이 있어야 합니다.

이 작업에 대해

"SMB 관리" 및 Windows 설명서에는 표준 및 고급 NTFS 권한을 설정하는 방법에 대한 정보가 포함되어 있습니다.

단계

1. Windows 클라이언트에 관리자로 로그인합니다.
2. Windows 탐색기의 * Tools * 메뉴에서 * Map network drive * 를 선택합니다.
3. 네트워크 드라이브 매핑 * 상자를 완료합니다.

    a. 드라이브 * 문자를 선택합니다.

    b. 폴더 * 상자에 사용 권한을 적용할 데이터와 공유 이름을 포함하는 공유가 포함된 SMB 서버 이름을 입력합니다.

    SMB 서버 이름이 smb_SERVER01이고 공유 이름이 "smb_SERVER01"이면 "\\smb_SERVER01\share1"을 입력합니다.

SMB 서버 이름 대신 SMB 서버에 대한 데이터 인터페이스의 IP 주소를 지정할 수 있습니다.

c. 마침 * 을 클릭합니다.

선택한 드라이브가 마운트되고 공유 내에 포함된 파일 및 폴더를 표시하는 Windows 탐색기 창이 준비됩니다.

4. NTFS 파일 권한을 설정할 파일 또는 디렉터리를 선택합니다.
5. 파일 또는 디렉터리를 마우스 오른쪽 단추로 클릭한 다음 * 속성 * 을 선택합니다.
6. 보안 * 탭을 선택합니다.

   보안 탭에는 NTFS 권한이 설정된 사용자 및 그룹 목록이 표시됩니다. Object>에 대한 권한 상자에는 선택한 사용자 또는 그룹에 적용되는 허용 및 거부 권한 목록이 표시됩니다.

7. 편집 * 을 클릭합니다.

   Object> 사용 권한 상자가 열립니다.

8. 원하는 작업을 수행합니다.

원하는 경우	다음을 수행합니다.
새 사용자 또는 그룹에 대한 표준 NTFS 권한을 설정합니다	a. 추가 * 를 클릭합니다. 사용자, 컴퓨터, 서비스 계정 또는 그룹 선택 창이 열립니다. b. 선택할 개체 이름 입력 * 상자에 NTFS 권한을 추가할 사용자 또는 그룹의 이름을 입력합니다. c. 확인 * 을 클릭합니다.
사용자 또는 그룹에서 표준 NTFS 권한을 변경하거나 제거합니다	그룹 또는 사용자 이름 * 상자에서 변경하거나 제거할 사용자 또는 그룹을 선택합니다.

9. 원하는 작업을 수행합니다.

원하는 작업	다음을 수행합니다
새 사용자 또는 기존 사용자 또는 그룹에 대해 표준 NTFS 권한을 설정합니다	Object>*에 대한 권한 상자에서 선택한 사용자 또는 그룹에 대해 허용하거나 허용하지 않을 액세스 유형에 대해 * 허용 * 또는 * 거부 * 상자를 선택합니다.
사용자 또는 그룹을 제거합니다	제거 * 를 클릭합니다.

일부 또는 모든 표준 권한 상자를 선택할 수 없는 경우 상위 개체에서 사용 권한이 상속되기 때문입니다. 특수 권한 * 상자는 선택할 수 없습니다. 이 옵션을 선택하면 선택한 사용자 또는 그룹에 대해 하나 이상의 세분화된 고급 권한이 설정되었음을 의미합니다.

10. 해당 개체에 대한 NTFS 권한을 추가, 제거 또는 편집한 후 * 확인 * 을 클릭합니다.

ONTAP SMB 사용자 공유 액세스를 확인합니다

구성한 사용자가 SMB 공유 및 해당 공유에 포함된 파일에 액세스할 수 있는지 테스트해야 합니다.

단계

1. Windows 클라이언트에서 공유에 대한 액세스 권한이 있는 사용자 중 하나로 로그인합니다.
2. Windows 탐색기의 * Tools * 메뉴에서 * Map network drive * 를 선택합니다.
3. 네트워크 드라이브 매핑 * 상자를 완료합니다.

   a. 드라이브 * 문자를 선택합니다.

   b. 폴더 * 상자에 사용자에게 제공할 공유 이름을 입력합니다.

      SMB 서버 이름이 smb_SERVER01이고 공유 이름이 "smb_SERVER01"이면 "\\smb_SERVER01\share1"을 입력합니다.

   c. 마침 * 을 클릭합니다.

   선택한 드라이브가 마운트되고 공유 내에 포함된 파일 및 폴더를 표시하는 Windows 탐색기 창이 준비됩니다.

4. 테스트 파일을 만들고, 파일이 있는지 확인하고, 텍스트를 작성한 다음 테스트 파일을 제거합니다.

CLI를 사용하여 SMB를 관리합니다

ONTAP SMB에 대해 알아보십시오

SMB 프로토콜에서 ONTAP 파일 액세스 기능을 사용할 수 있습니다. CIFS 서버를 설정하고, 공유를 생성하고, Microsoft 서비스를 설정할 수 있습니다.

smb(서버 메시지 블록)는 CIFS(Common Internet File System) 프로토콜의 최신 방언을 의미합니다. ONTAP CLI(Command-Line Interface) 및 OnCommand 관리 툴에서도 _cifs_가 계속 표시됩니다.

SMB 서버 지원

ONTAP SMB 서버 지원에 대해 알아보십시오

SMB 클라이언트가 클러스터의 파일에 액세스할 수 있도록 SVM(스토리지 가상 머신)에서 SMB 서버를 설정 및 구성할 수 있습니다.

- 클러스터의 각 데이터 SVM은 하나의 Active Directory 도메인에 정확히 바인딩할 수 있습니다.
- Data SVM을 동일한 도메인에 연결할 필요가 없습니다.
- 여러 SVM을 동일한 도메인에 바인딩할 수 있습니다.

SMB 서버를 생성하기 전에 데이터 제공을 위해 사용 중인 SVM 및 LIF를 구성해야 합니다. 데이터 네트워크가 편평하지 않은 경우 IPspace, 브로드캐스트 도메인 및 서브넷을 구성해야 할 수도 있습니다.

관련 정보

"네트워크 관리"

서버 수정

"시스템 관리"

지원되는 **ONTAP SMB** 버전 및 기능

SMB(Server Message Block)는 Microsoft Windows 클라이언트 및 서버에서 사용하는 원격 파일 공유 프로토콜입니다. 모든 SMB 버전이 지원됩니다. ONTAP SMB 서버가 사용자 환경에 필요한 클라이언트 및 기능을 지원하는지 확인해야 합니다.

ONTAP가 지원하는 SMB 클라이언트 및 도메인 컨트롤러에 대한 최신 정보는 _Interoperability Matrix Tool_에서 확인할 수 있습니다.

SMB 2.0 이상 버전은 ONTAP SMB 서버에 대해 기본적으로 활성화되어 있으며 필요에 따라 활성화하거나 비활성화할 수 있습니다. SMB 1.0은 필요에 따라 활성화 또는 비활성화할 수 있습니다.

> 도메인 컨트롤러에 대한 SMB 1.0 및 2.0 연결의 기본 설정은 ONTAP 버전에도 따라 다릅니다. 에 대한 자세한 내용은 `vserver cifs security modify` "ONTAP 명령 참조입니다"을 참조하십시오. SMB 1.0을 실행하는 기존 CIFS 서버가 있는 환경의 경우 보안 및 규정 준수 향상을 준비하기 위해 가능한 한 빨리 최신 SMB 버전으로 마이그레이션해야 합니다. 자세한 내용은 NetApp 담당자에게 문의하십시오.

다음 표에서는 각 SMB 버전에서 지원되는 SMB 기능을 보여 줍니다. 일부 SMB 기능은 기본적으로 활성화되어 있으며 일부는 추가 구성이 필요합니다.

* 이 기능은 * 입니다	* 지원 필요: *	* 는 다음 **SMB** 버전에 대해 **ONTAP 9**에서 지원됩니다. *	
		3.0	3.1.1
레거시 SMB 1.0 기능		X	X
내구성이 뛰어난 핸들		X	X
결합 작업		X	X
비동기 작업		X	X
읽기 및 쓰기 버퍼 크기가 증가되었습니다		X	X
확장성 향상		X	X
SMB 서명	X	X	X

* 이 기능은 * 입니다	* 지원 필요: *	* 는 다음 **SMB** 버전에 대해 **ONTAP 9**에서 지원됩니다. *	
ADS(대체 데이터 스트림) 파일 형식입니다	X	X	X
Large MTU(ONTAP 9.7부터 기본적으로 활성화됨)	X	X	X
oplocks 리스		X	X
지속적으로 사용 가능한 공유	X	X	X
영구 핸들		X	X
증인		X	X
SMB 암호화: AES-128-CCM	X	X	X
스케일아웃(CA 공유에 필요)		X	X
투명한 페일오버		X	X
SMB 멀티 채널(ONTAP 9.4로 시작)	X	X	X
사전 인증 무결성			X
클러스터 클라이언트 페일오버 v.2(CCFv2)			X
SMB 암호화: AES-128-GCM	X		X

관련 정보

ONTAP 서명을 사용하여 네트워크 보안을 강화하는 방법에 대해 알아보세요.

서버 최소 인증 보안 수준 설정

SMB를 통한 데이터 전송을 위해 SMB 서버에서 필요한 SMB 암호화 구성

"NetApp 상호 운용성"

ONTAP SMB에서 지원되지 않는 Windows 기능

네트워크에서 CIFS를 사용하기 전에 ONTAP에서 지원하지 않는 특정 Windows 기능을 알고 있어야 합니다.

ONTAP는 다음 Windows 기능을 지원하지 않습니다.

- 암호화된 파일 시스템(EFS)
- 변경 저널에서 NTFS(NT File System) 이벤트 로깅
- Microsoft FRS(파일 복제 서비스)
- Microsoft Windows 인덱싱 서비스
- HSM(Hierarchical Storage Management)을 통한 원격 스토리지
- Windows 클라이언트의 할당량 관리
- Windows 할당량 의미 체계입니다
- LMHOSTS 파일입니다
- NTFS 네이티브 압축

ONTAP SMB SVM에서 NIS 또는 LDAP 이름 서비스를 구성합니다

SMB 액세스를 사용하면 NTFS 보안 스타일 볼륨에서 데이터에 액세스할 때도 UNIX 사용자에 대한 사용자 매핑이 항상 수행됩니다. 정보가 NIS 또는 LDAP 디렉토리 저장소에 저장되어 있는 해당 UNIX 사용자에게 Windows 사용자를 매핑하거나 이름 매핑에 LDAP를 사용하는 경우 SMB 설정 중에 이러한 이름 서비스를 구성해야 합니다.

시작하기 전에

네임 서비스 데이터베이스 구성을 네임 서비스 인프라에 맞게 사용자 지정해야 합니다.

이 작업에 대해

SVM은 이름 서비스 ns-switch 데이터베이스를 사용하여 지정된 이름 서비스 데이터베이스의 소스를 조회하는 순서를 결정합니다. ns 스위치 소스는 , `nis` 또는 `ldap` 의 조합이 될 수 있습니다 `files`. 그룹 데이터베이스의 경우 ONTAP는 구성된 모든 소스에서 그룹 구성원 자격을 얻은 다음 통합된 그룹 구성원 정보를 사용하여 액세스 검사를 수행합니다. UNIX 그룹 정보를 가져올 때 이러한 소스 중 하나를 사용할 수 없는 경우 ONTAP에서 전체 UNIX 자격 증명을 가져올 수 없으며 이후의 액세스 검사에 실패할 수 있습니다. 따라서 항상 ns-switch 설정에서 그룹 데이터베이스에 대해 모든 ns-switch 소스가 구성되어 있는지 확인해야 합니다.

기본값은 SMB 서버가 모든 Windows 사용자를 로컬 'passwd' 데이터베이스에 저장된 기본 UNIX 사용자에게 매핑하도록 하는 것입니다. 기본 구성을 사용하려면 NIS 또는 LDAP UNIX 사용자 및 그룹 이름 서비스 구성 또는 LDAP 사용자 매핑은 SMB 액세스에 대해 선택 사항입니다.

단계

1. UNIX 사용자, 그룹 및 넷그룹 정보가 NIS 이름 서비스를 통해 관리되는 경우 NIS 이름 서비스를 구성합니다.

   a. 'vserver services name-service ns-switch show' 명령을 사용하여 이름 서비스의 현재 순서를 확인합니다.

      이 예에서는 NIS를 이름 서비스 소스로 사용할 수 있는 세 개의 데이터베이스(group, passwd, netgroup)가 파일(file)만 소스로 사용하고 있습니다.

'vserver services name-service ns-switch show-vserver vs1'

```
                                                 Source
Vserver         Database       Enabled           Order
--------------- ------------   ---------         ---------
vs1             hosts          true              dns,
                                                 files
vs1             group          true              files
vs1             passwd         true              files
vs1             netgroup       true              files
vs1             namemap        true              files
```

그룹 및 암호 데이터베이스에 NIS 소스를 추가하고 선택적으로 넷그룹 데이터베이스에 추가해야 합니다.

b. 'vserver services name-service ns-switch modify' 명령을 사용하여 이름 서비스 ns-switch 데이터베이스 순서를 원하는 대로 조정합니다.

최상의 성능을 위해 SVM에서 네임 서비스를 구성하려는 경우를 제외하고 네임 서비스 데이터베이스에 네임 서비스를 추가할 수 없습니다.

둘 이상의 이름 서비스 데이터베이스에 대한 구성을 수정하는 경우 수정할 각 이름 서비스 데이터베이스에 대해 명령을 별도로 실행해야 합니다.

이 예에서 NIS와 파일은 그룹 데이터베이스와 암호 데이터베이스의 소스로 구성됩니다. 나머지 이름 서비스 데이터베이스는 변경되지 않습니다.

'vserver services name-service ns-switch modify -vserver vs1 -database group -sources nis, files"vserver services name-service ns-switch modify -vserver vs1-database passwd-sources nis, files'

c. 'vserver services name-service ns-switch show' 명령을 사용하여 이름 서비스의 순서가 올바른지 확인합니다.

'vserver services name-service ns-switch show-vserver vs1'

```
                                                 Source
Vserver         Database       Enabled           Order
--------------- ------------   ---------         ---------
vs1             hosts          true              dns,
                                                 files
vs1             group          true              nis,
                                                 files
vs1             passwd         true              nis,
                                                 files
vs1             netgroup       true              files
vs1             namemap        true              files
```

d. NIS 이름 서비스 구성을 만듭니다

```
vserver services name-service nis-domain create -vserver <vserver_name>
-domain <NIS_domain_name> -servers <NIS_server_IPaddress>,…

vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60
```

1. 이 필드는 NIS 서버의 호스트 이름이나 IP 주소를 사용할 수 있습니다

e. NIS 이름 서비스가 올바르게 구성되어 있는지 확인합니다. `vserver services name-service nis-domain show vserver <vserver_name>`

'vserver services name-service nis-domain show vserver vs1'

```
Vserver       Domain              Server
------------- ------------------- ---------------
vs1           example.com         10.0.0.60
```

2. UNIX 사용자, 그룹 및 넷그룹 정보 또는 이름 매핑이 LDAP 이름 서비스에 의해 관리되는 경우 찾은 정보를 사용하여 LDAP 이름 서비스를 구성합니다 "NFS 관리".

ONTAP SMB 이름 서비스 스위치 구성에 대해 자세히 알아보십시오

ONTAP는 UNIX 시스템의 '/etc/nsswitch.conf' 파일에 해당하는 테이블에 이름 서비스 구성 정보를 저장합니다. 환경에 맞게 적절하게 구성할 수 있도록 표의 기능과 ONTAP에서 표의 사용 방법을 이해해야 합니다.

ONTAP 이름 서비스 스위치 테이블은 ONTAP가 특정 유형의 이름 서비스 정보에 대한 정보를 검색하기 위해 어떤 이름 서비스 소스를 참조합니다. ONTAP는 SVM별로 개별 네임 서비스 스위치 테이블을 유지 관리합니다.

데이터베이스 유형

이 테이블에는 다음과 같은 각 데이터베이스 유형에 대해 별도의 이름 서비스 목록이 저장됩니다.

데이터베이스 유형입니다	다음에 대한 이름 서비스 소스를 정의합니다.	유효한 소스는...
호스트	호스트 이름을 IP 주소로 변환	파일, DNS
그룹	사용자 그룹 정보를 찾는 중입니다	파일, NIS, LDAP
암호	사용자 정보를 찾는 중입니다	파일, NIS, LDAP
넷그룹	넷그룹 정보를 찾는 중입니다	파일, NIS, LDAP
이름맵	사용자 이름 매핑 중	파일, LDAP

소스 유형

소스는 해당 정보를 검색하는 데 사용할 이름 서비스 소스를 지정합니다.

원본 유형 지정...	에서 정보를 조회하려면...	관리 대상 명령 제품군...
파일	로컬 소스 파일	SVM 서비스 이름 서비스 유닉스 사용자 SVM 서비스 이름 서비스 유닉스 그룹 SVM 서비스 이름 서비스 넷그룹 SVM 서비스 이름-서비스 DNS 호스트
NIS를 선택합니다	SVM의 NIS 도메인 구성에 지정된 외부 NIS 서버	'vserver services name-service nis-domain'을 선택합니다
LDAP를 지원합니다	SVM의 LDAP 클라이언트 구성에 지정된 외부 LDAP 서버	'vserver services name-service ldap'
DNS	SVM의 DNS 구성에 지정된 외부 DNS 서버	SVM 서비스 이름-서비스 DNS

데이터 액세스와 SVM 관리 인증 모두에 NIS 또는 LDAP를 사용하려는 경우에도 NIS 또는 LDAP 인증이 실패할 경우 "파일"을 포함하고 로컬 사용자를 대체 수단으로 구성해야 합니다.

외부 소스에 액세스하는 데 사용되는 프로토콜입니다

외부 소스의 서버에 액세스하기 위해 ONTAP는 다음 프로토콜을 사용합니다.

외부 이름 서비스 소스입니다	액세스에 사용되는 프로토콜입니다
NIS를 선택합니다	UDP입니다
DNS	UDP입니다
LDAP를 지원합니다	TCP

예

다음 예는 SVM의 VM_1'에 대한 이름 서비스 스위치 구성을 표시합니다.

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

사용자 또는 그룹 정보를 조회하기 위해 ONTAP는 로컬 소스 파일만 참조합니다. 쿼리가 결과를 반환하지 않으면 조회가 실패합니다.

넷그룹 정보를 조회하기 위해 ONTAP는 먼저 외부 NIS 서버를 참조합니다. 쿼리가 결과를 반환하지 않으면 로컬 넷그룹 파일이 다음에 선택됩니다.

SVM svm_1의 테이블에는 이름 매핑에 대한 이름 서비스 항목이 없습니다. 따라서 ONTAP는 기본적으로 로컬 소스 파일만 참조합니다.

SMB 서버를 관리합니다

ONTAP SMB 서버를 수정합니다

"vserver cifs modify" 명령을 사용하여 작업 그룹에서 Active Directory 도메인으로, 작업 그룹에서 다른 작업 그룹으로 또는 Active Directory 도메인에서 작업 그룹으로 SMB 서버를 이동할 수 있습니다.

이 작업에 대해

SMB 서버 이름 및 관리 상태와 같은 SMB 서버의 다른 속성을 수정할 수도 있습니다. 에 대한 자세한 내용은 `vserver cifs modify` "ONTAP 명령 참조입니다"을 참조하십시오.

선택

- 작업 그룹에서 Active Directory 도메인으로 SMB 서버 이동:

  a. SMB 서버의 관리 상태를 'down'으로 설정합니다.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. 작업 그룹에서 Active Directory 도메인으로 SMB 서버를 이동합니다: ' vsserver cifs modify -vserver_vserver_name_-domain_domain_name_'

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

SMB 서버에 대한 Active Directory 컴퓨터 계정을 만들려면 '*example*'.com 도메인 내의 'ou=_example_ou' 컨테이너에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름과 암호를 제공해야 합니다.

ONTAP 9.7부터 AD 관리자는 권한이 있는 Windows 계정에 이름과 암호를 제공하는 대신 keytab 파일에 대한 URI를 제공할 수 있습니다. URI를 받으면 '-keytab-Uri' 매개 변수에 vserver cifs' 명령을 포함하여 포함시키십시오.

- 작업 그룹에서 다른 작업 그룹으로 SMB 서버 이동:
  a. SMB 서버의 관리 상태를 'down'으로 설정합니다.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. SMB 서버의 워크그룹을 수정합니다. 'vserver cifs modify -vserver_vserver_name_ -workgroup_new_workgroup_name_'

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Active Directory 도메인에서 작업 그룹으로 SMB 서버 이동:
  a. SMB 서버의 관리 상태를 'down'으로 설정합니다.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. SMB 서버를 Active Directory 도메인에서 작업 그룹('vserver cifs modify -vserver_vserver_name_ -workgroup_workgroup_name_')으로 이동합니다

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

> 워크그룹 모드로 전환하려면 모든 도메인 기반 기능을 사용하지 않도록 설정하고 지속적으로 사용 가능한 공유, 섀도우 복제본 및 AES를 포함하여 시스템에서 해당 구성을 자동으로 제거해야 합니다. 그러나 "EXAMPLE.COM\userName" 같은 도메인 구성 공유 ACL은 제대로 작동하지 않지만 ONTAP에서는 제거할 수 없습니다. 명령이 완료된 후 외부 툴을 사용하여 가능한 한 빨리 이러한 공유 ACL을 제거합니다. AES가 활성화된 경우 "example.com" 도메인에서 Windows 계정을 비활성화할 수 있는 충분한 권한이 있는 Windows 계정의 이름과 암호를 입력하라는 메시지가 표시될 수 있습니다.

  - 'vserver cifs modify' 명령의 적절한 매개 변수를 사용하여 다른 속성을 수정합니다.

옵션을 사용하여 **SMB** 서버를 사용자 지정합니다

사용 가능한 **ONTAP SMB** 서버 옵션

SMB 서버를 사용자 지정하는 방법을 고려할 때 사용할 수 있는 옵션을 파악하는 것이 유용합니다. 일부 옵션은 SMB 서버에서 일반적으로 사용되지만 일부 옵션은 특정 SMB 기능을 설정하고 구성하는 데 사용됩니다. SMB 서버 옵션은 'vserver cifs options modify' 옵션으로 제어됩니다.

다음 목록은 관리자 권한 수준에서 사용할 수 있는 SMB 서버 옵션을 지정합니다.

- * SMB 세션 시간 초과 값 구성 *

  이 옵션을 구성하면 SMB 세션의 연결이 끊기까지의 유휴 시간(초)을 지정할 수 있습니다. 유휴 세션은 사용자가 클라이언트에 열려 있는 파일이나 디렉토리가 없는 세션입니다. 기본값은 900초입니다.

- * 기본 UNIX 사용자 구성 *

  이 옵션을 구성하면 SMB 서버에서 사용하는 기본 UNIX 사용자를 지정할 수 있습니다. ONTAP는 ""pcuser""(UID 65534)라는 기본 사용자를 자동으로 만들고 ""pcuser""(GID가 65534)라는 그룹을 만든 다음 기본 사용자를 ""pcuser"" 그룹에 추가합니다. SMB 서버를 생성하면 ONTAP는 자동으로 ""pcuser""를 기본 UNIX 사용자로 구성합니다.

- * 게스트 UNIX 사용자 구성 *

  이 옵션을 구성하면 신뢰할 수 없는 도메인에서 로그인하는 사용자가 매핑될 UNIX 사용자의 이름을 지정할 수 있으므로 신뢰할 수 없는 도메인의 사용자가 SMB 서버에 연결할 수 있습니다. 기본적으로 이 옵션은 구성되지 않음(기본값 없음)이므로 신뢰할 수 없는 도메인의 사용자가 SMB 서버에 연결하도록 허용하지 않습니다.

- * 모드 비트에 대한 읽기 권한 실행 활성화 또는 비활성화 *

  이 옵션을 설정하거나 해제하면 UNIX 실행 가능 비트가 설정되지 않은 경우에도 SMB 클라이언트가 읽기 액세스 권한이 있는 UNIX 모드 비트를 사용하여 실행 파일을 실행하도록 허용할지 여부를 지정할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

- * NFS 클라이언트에서 읽기 전용 파일을 삭제하는 기능을 활성화 또는 비활성화합니다

  이 옵션을 설정하거나 해제하면 NFS 클라이언트가 읽기 전용 속성이 설정된 파일 또는 폴더를 삭제할 수 있는지 여부를 결정합니다. NTFS 삭제 의미 체계에서는 읽기 전용 특성이 설정된 경우 파일 또는 폴더를 삭제할 수 없습니다. UNIX 삭제 의미 체계는 읽기 전용 비트를 무시하고 상위 디렉토리 권한을 사용하여 파일 또는 폴더를 삭제할 수 있는지 여부를 결정합니다. 기본 설정은 사용 안 함 으로 NTFS 삭제 의미를 가져옵니다.

- * Windows 인터넷 이름 서비스 서버 주소 구성 *

  이 옵션을 구성하면 WINS(Windows Internet Name Service) 서버 주소 목록을 쉼표로 구분된 목록으로 지정할 수 있습니다. IPv4 주소를 지정해야 합니다. IPv6 주소는 지원되지 않습니다. 기본값이 없습니다.

다음 목록은 고급 권한 수준에서 사용할 수 있는 SMB 서버 옵션을 지정합니다.

- * CIFS 사용자에게 UNIX 그룹 권한 부여 *

  이 옵션을 구성하면 파일 소유자가 아닌 수신 CIFS 사용자에게 그룹 권한을 부여할 수 있는지 여부를 결정합니다. CIFS 사용자가 UNIX 보안 스타일 파일의 소유자가 아니고 이 매개 변수를 "true"로 설정하면 해당 파일에 대한 그룹 권한이 부여됩니다. CIFS 사용자가 UNIX 보안 스타일 파일의 소유자가 아니고 이 매개 변수가 "false"로 설정된 경우 일반 UNIX 규칙을 적용하여 파일 권한을 부여할 수 있습니다. 이 매개 변수는 권한이 '모드 비트'로 설정되어 있고 NTFS 또는 NFSv4 보안 모드가 있는 파일에는 적용되지 않는 UNIX 보안 스타일 파일에 적용됩니다. 기본 설정은 false입니다.

- * SMB 1.0 * 활성화 또는 비활성화

  SMB 1.0은 ONTAP 9.3에서 SMB 서버가 생성된 SVM에서 기본적으로 비활성화되어 있습니다.

ONTAP 9.3부터는 ONTAP 9.3에서 생성된 새 SMB 서버에 대해 SMB 1.0이 기본적으로 사용되지 않습니다. 보안 및 규정 준수 향상을 준비하기 위해 가능한 한 빨리 최신 SMB 버전으로 마이그레이션해야 합니다. 자세한 내용은 NetApp 담당자에게 문의하십시오.

- * SMB 2.x * 활성화 또는 비활성화

  SMB 2.0은 LIF 페일오버를 지원하는 최소 SMB 버전입니다. SMB 2.x를 비활성화하면 ONTAP도 자동으로 SMB 3.X를 비활성화합니다

  SMB 2.0은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * SMB 3.0 * 활성화 또는 비활성화

  SMB 3.0은 지속적으로 사용 가능한 공유를 지원하는 최소 SMB 버전입니다. Windows Server 2012 및 Windows 8은 SMB 3.0을 지원하는 최소 Windows 버전입니다.

  SMB 3.0은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * SMB 3.1 * 활성화 또는 비활성화

  Windows 10은 SMB 3.1을 지원하는 유일한 Windows 버전입니다.

  SMB 3.1은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * ODX 복사 오프로드 설정 또는 해제 *

  ODX 복사 오프로드는 Windows 클라이언트에서 지원하는 데 자동으로 사용됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

- * ODX 복사 오프로드에 대한 직접 복사 메커니즘 설정 또는 해제 *

  직접 복사 메커니즘은 Windows 클라이언트가 복사 진행 중에 파일이 변경되지 않도록 하는 모드에서 복사본의 소스 파일을 열려고 할 때 복제 오프로드 작업의 성능을 향상시킵니다. 기본적으로 직접 복사 메커니즘은 활성화되어 있습니다.

- * 자동 노드 참조 활성화 또는 비활성화 *

  SMB 서버는 자동 노드 조회를 통해 요청된 공유를 통해 액세스한 데이터를 호스팅하는 노드에 대한 데이터 LIF 로컬 클라이언트를 자동으로 참조합니다.

- * SMB*에 대한 내보내기 정책 활성화 또는 비활성화

  이 옵션은 기본적으로 비활성화되어 있습니다.

- * 교차점을 재분석 지점으로 사용하여 활성화 또는 비활성화 *

  이 옵션을 활성화하면 SMB 서버는 재분석 지점으로 SMB 클라이언트에 연결 지점을 노출합니다. 이 옵션은 SMB 2.x 또는 SMB 3.0 연결에만 유효합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

  이 옵션은 SVM에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * TCP 연결당 최대 동시 작업 수 구성 *

기본값은 255입니다.

- * 로컬 Windows 사용자 및 그룹 기능 활성화 또는 비활성화 *

  이 옵션은 기본적으로 활성화되어 있습니다.

- * 로컬 Windows 사용자 인증 활성화 또는 비활성화 *

  이 옵션은 기본적으로 활성화되어 있습니다.

- * VSS 섀도우 복제본 기능 활성화 또는 비활성화 *

  ONTAP는 섀도우 복제본 기능을 사용하여 SMB를 통한 Hyper-V 솔루션을 사용하여 저장된 데이터의 원격 백업을 수행합니다.

  이 옵션은 SVM에서만 지원되며, SMB를 통한 Hyper-V 구성에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * 섀도 복사본 디렉토리 수준 구성 *

  이 옵션을 구성하면 섀도우 복제본 기능을 사용할 때 섀도우 복제본을 생성할 디렉토리의 최대 깊이를 정의할 수 있습니다.

  이 옵션은 SVM에서만 지원되며, SMB를 통한 Hyper-V 구성에서만 지원됩니다. 이 옵션은 SVM에서 기본적으로 활성화됩니다

- * 이름 매핑에 대한 다중 도메인 검색 기능을 활성화 또는 비활성화합니다 *

  활성화된 경우, UNIX 사용자가 Windows 사용자 이름의 도메인 부분에서 와일드카드(*)를 사용하여 Windows 도메인 사용자에게 매핑되면(예: *\Joe) ONTAP는 양방향 트러스트가 있는 모든 도메인에서 홈 도메인으로 지정된 사용자를 검색합니다. 홈 도메인은 SMB 서버의 컴퓨터 계정이 포함된 도메인입니다.

  양방향으로 신뢰할 수 있는 모든 도메인을 검색하는 대신 선호하는 신뢰할 수 있는 도메인 목록을 구성할 수 있습니다. 이 옵션을 사용하도록 설정하고 기본 설정 목록을 구성하면 다중 도메인 이름 매핑 검색을 수행하는 데 기본 설정 목록이 사용됩니다.

  기본값은 다중 도메인 이름 매핑 검색을 사용하는 것입니다.

- * 파일 시스템 섹터 크기 구성 *

  이 옵션을 구성하면 ONTAP에서 SMB 클라이언트에 보고하는 파일 시스템 섹터 크기를 바이트 단위로 구성할 수 있습니다. 이 옵션에는 4096과 512의 두 가지 유효한 값이 있습니다. 기본값은 4096입니다. Windows 응용 프로그램이 512바이트의 섹터 크기만 지원하는 경우 이 값을 '512'로 설정해야 할 수 있습니다.

- * 동적 액세스 제어 활성화 또는 비활성화 *

  이 옵션을 활성화하면 DAC(Dynamic Access Control)를 사용하여 중앙 액세스 정책을 스테이징하고 그룹 정책 개체를 사용하여 중앙 액세스 정책을 구현하는 등 SMB 서버의 개체를 보호할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

  이 옵션은 SVM에서만 지원됩니다.

- * 인증되지 않은 세션에 대한 액세스 제한 설정(익명 제한) *

이 옵션을 설정하면 인증되지 않은 세션에 대한 액세스 제한이 결정됩니다. 제한 사항은 익명 사용자에게 적용됩니다. 기본적으로 익명 사용자에 대한 액세스 제한은 없습니다.

- * UNIX 효과적인 보안(UNIX 보안 스타일 볼륨 또는 UNIX 효과적인 보안이 포함된 혼합 보안 스타일 볼륨)이 있는 볼륨에서 NTFS ACL 표시를 활성화 또는 비활성화합니다. *

  이 옵션을 설정하거나 해제하면 UNIX 보안이 있는 파일 및 폴더의 파일 보안이 SMB 클라이언트에 제공되는 방식이 결정됩니다. 이 옵션을 설정하면 ONTAP는 UNIX 보안 기능이 있는 볼륨의 파일 및 폴더를 NTFS ACL을 사용한 NTFS 파일 보안으로 SMB 클라이언트에 제공합니다. 사용하지 않도록 설정하면 ONTAP는 UNIX 보안이 설정된 볼륨을 파일 보안 없이 FAT 볼륨으로 제공합니다. 기본적으로 볼륨은 NTFS ACL을 사용한 NTFS 파일 보안을 갖는 것으로 표시됩니다.

- * SMB 가짜 열기 기능 활성화 또는 비활성화 *

  이 기능을 사용하면 파일 및 디렉토리에 대한 속성 정보를 쿼리할 때 ONTAP에서 열기 및 닫기 요청을 수행하는 방식을 최적화하여 SMB 2.x 및 SMB 3.0 성능을 향상시킬 수 있습니다. 기본적으로 SMB 가짜 열기 기능이 활성화됩니다. 이 옵션은 SMB 2.x 이상에서 만들어진 연결에만 유용합니다.

- * UNIX 확장 활성화 또는 비활성화 *

  이 옵션을 활성화하면 SMB 서버에서 UNIX 확장이 활성화됩니다. UNIX 확장을 사용하면 POSIX/UNIX 스타일 보안을 SMB 프로토콜을 통해 표시할 수 있습니다. 기본적으로 이 옵션은 비활성화되어 있습니다.

  Mac OSX 클라이언트와 같은 UNIX 기반 SMB 클라이언트가 있는 경우 UNIX 확장을 활성화해야 합니다. UNIX 확장을 사용하면 SMB 서버가 POSIX/UNIX 보안 정보를 SMB를 통해 UNIX 기반 클라이언트로 전송한 다음 보안 정보를 POSIX/UNIX 보안으로 변환합니다.

- * 간단한 이름 검색 지원 활성화 또는 비활성화 *

  이 옵션을 활성화하면 SMB 서버가 짧은 이름으로 검색을 수행할 수 있습니다. 이 옵션을 사용하는 검색 쿼리는 8.3 파일 이름과 긴 파일 이름을 일치시키려고 합니다. 이 파라미터의 기본값은 'false'입니다.

- * DFS 기능 자동 보급에 대한 지원 활성화 또는 비활성화 *

  이 옵션을 활성화 또는 비활성화하면 SMB 서버가 공유에 연결하는 SMB 2.x 및 SMB 3.0 클라이언트에 DFS 기능을 자동으로 보급할지 여부를 결정합니다. ONTAP는 SMB 액세스를 위한 심볼 링크 구현에 DFS 조회를 사용합니다. 활성화된 경우 SMB 서버는 심볼 링크 액세스가 설정되었는지 여부에 관계없이 항상 DFS 기능을 알립니다. 비활성화된 경우 SMB 서버는 클라이언트가 심볼 링크 액세스가 설정된 공유에 연결할 때만 DFS 기능을 알립니다.

- * 최대 SMB 크레딧 수 구성 *

  ONTAP 9.4부터, '-max-credits' 옵션을 구성하면 클라이언트와 서버가 SMB 버전 2 이상을 실행하는 경우 SMB 연결에 부여할 크레딧 수를 제한할 수 있습니다. 기본값은 128입니다.

- * SMB 멀티 채널 * 에 대한 지원 활성화 또는 비활성화

  ONTAP 9.4 이상 릴리스에서 '-is-multichannel-enabled' 옵션을 활성화하면 SMB 서버는 클러스터와 해당 클라이언트에 적절한 NIC가 구축될 때 단일 SMB 세션에 대해 여러 개의 연결을 설정할 수 있습니다. 이렇게 하면 처리량과 내결함성이 개선됩니다. 이 파라미터의 기본값은 'false'입니다.

  SMB 멀티 채널이 활성화되면 다음 매개 변수도 지정할 수 있습니다.

- 다중 채널 세션당 허용되는 최대 연결 수입니다. 이 매개 변수의 기본값은 32입니다.
- Multichannel 세션당 공고되는 최대 네트워크 인터페이스 수입니다. 이 매개 변수의 기본값은 256입니다.

ONTAP SMB 서버 옵션을 구성합니다

SVM(스토리지 가상 시스템)에서 SMB 서버를 생성한 후에는 언제든지 SMB 서버 옵션을 구성할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

SMB 서버 옵션을 구성하려면...	명령 입력...
관리 권한 수준에서 설정합니다	'vserver cifs options modify -vserver_vserver_name options_'
고급 권한 수준에서 설정합니다	a. 세트 프리빌리지 고급 b. 'vserver cifs options modify -vserver_vserver_name options_' c. 'Set-Privilege admin'입니다

SMB 서버 옵션에 대한 자세한 `vserver cifs options modify` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

ONTAP SMB 사용자에게 **UNIX** 그룹 권한 부여 를 구성합니다

들어오는 SMB 사용자가 파일 소유자가 아닌 경우에도 파일 또는 디렉토리에 액세스할 수 있는 그룹 권한을 부여하도록 이 옵션을 구성할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. UNIX 그룹 권한 부여를 적절히 구성합니다.

원하는 경우	명령을 입력합니다
사용자가 파일 소유자가 아니더라도 파일 또는 디렉토리에 대한 액세스를 활성화하여 그룹 권한을 얻습니다	'vserver cifs options modify –grant-unix-group-perms-to-others true'
파일 또는 디렉토리에 대한 액세스를 비활성화하여 사용자가 파일 소유자가 아니더라도 그룹 권한을 얻습니다	'vserver cifs options modify –grant-unix-group-perms-to-others false'

3. 이 옵션이 원하는 값으로 설정되어 있는지 확인합니다. 'vserver cifs options show –fields grant-unix-group-perms-to-others'
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

기본적으로 인증되지 않은 익명 사용자(*null user* 라고도 함)는 네트워크의 특정 정보에 액세스할 수 있습니다. SMB 서버 옵션을 사용하여 익명 사용자의 액세스 제한을 구성할 수 있습니다.

이 작업에 대해

익명 제한 SMB 서버 옵션은 Windows의 RestrictAnonymous 레지스트리 항목에 해당합니다.

익명 사용자는 사용자 이름 및 세부 정보, 계정 정책 및 공유 이름을 포함하여 네트워크의 Windows 호스트에서 특정 유형의 시스템 정보를 나열하거나 열거할 수 있습니다. 다음 세 가지 액세스 제한 설정 중 하나를 지정하여 익명 사용자에 대한 액세스를 제어할 수 있습니다.

값	설명
무제한(기본값)	익명 사용자에 대한 액세스 제한을 지정하지 않습니다.
번호 매기기	익명 사용자에 대해서만 열거를 제한하도록 지정합니다.
"접근 불가"	익명 사용자에 대한 액세스가 제한되도록 지정합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 익명 제한 설정: 'vserver cifs options modify -vserver_vserver_name_-restrict-anonymous{no-restriction|no-enumeration|no-access}'를 구성합니다
3. 옵션이 원하는 값('vserver cifs options show -vserver_vserver_name_')으로 설정되어 있는지 확인합니다
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

관련 정보

사용 가능한 서버 옵션

UNIX 보안 스타일 데이터를 위해 **SMB** 클라이언트에 파일 보안을 제공하는 방법을 관리합니다

UNIX 보안 스타일 데이터를 위해 **SMB** 클라이언트에 **ONTAP** 파일 보안을 제공하는 방법에 대해 알아보십시오

SMB 클라이언트에 NTFS ACL 표시를 활성화 또는 비활성화하여 UNIX 보안 스타일 데이터용 파일 보안을 SMB 클라이언트에 제공하는 방법을 선택할 수 있습니다. 각 설정에는 비즈니스 요구 사항에 가장 적합한 설정을 선택해야 한다는 점을 이해해야 합니다.

기본적으로 ONTAP는 UNIX 보안 스타일 볼륨에 대한 UNIX 권한을 SMB 클라이언트에 NTFS ACL로 제공합니다. 다음과 같이 이 방법이 필요한 시나리오가 있습니다.

- Windows 속성 상자의 * 보안 * 탭을 사용하여 UNIX 권한을 보고 편집하려는 경우

  UNIX 시스템에서 작업이 허용되지 않는 경우 Windows 클라이언트에서 권한을 수정할 수 없습니다. 예를 들어 UNIX 시스템에서는 이 작업을 허용하지 않으므로 소유하지 않는 파일의 소유권을 변경할 수 없습니다. 이 제한 사항으로 인해 SMB 클라이언트가 파일 및 폴더에 설정된 UNIX 권한을 우회하지 못합니다.

- 사용자는 Microsoft Office와 같은 특정 Windows 응용 프로그램을 사용하여 UNIX 보안 스타일 볼륨에서 파일을 편집 및 저장하고 있습니다. 여기서 ONTAP는 저장 작업 중에 UNIX 권한을 유지해야 합니다.
- 사용자 환경에는 사용 중인 파일에 대해 NTFS ACL을 읽을 것으로 예상되는 특정 Windows 애플리케이션이 있습니다.

경우에 따라 UNIX 사용 권한을 NTFS ACL로 표시하지 않도록 설정할 수 있습니다. 이 기능을 비활성화하면 ONTAP는 UNIX 보안 스타일 볼륨을 SMB 클라이언트에 FAT 볼륨으로 제공합니다. UNIX 보안 스타일 볼륨을 SMB 클라이언트에 FAT 볼륨으로 표시하는 이유는 다음과 같습니다.

- UNIX 클라이언트에서 마운트를 사용하여 UNIX 사용 권한만 변경할 수 있습니다.

  UNIX 보안 스타일 볼륨이 SMB 클라이언트에 매핑된 경우에는 보안 탭을 사용할 수 없습니다. 매핑된 드라이브는 파일 권한이 없는 FAT 파일 시스템으로 포맷된 것 같습니다.

- 액세스 파일 및 폴더에 NTFS ACL을 설정하는 SMB를 통해 애플리케이션을 사용 중이며, UNIX 보안 스타일 볼륨에 데이터가 있는 경우 오류가 발생할 수 있습니다.

  ONTAP가 볼륨을 FAT로 보고하는 경우 응용 프로그램은 ACL을 변경하지 않습니다.

관련 정보

- FlexVol 볼륨에서 보안 스타일을 구성합니다
- Qtree에서 보안 스타일 구성

UNIX 보안 스타일 데이터의 경우 **ONTAP SMB** 클라이언트에 **NTFS ACL** 표시를 구성합니다

UNIX 보안 스타일 데이터(UNIX 보안 스타일 볼륨 및 UNIX 효과적인 보안이 포함된 혼합 보안 스타일 볼륨)를 위해 SMB 클라이언트에 NTFS ACL 표시를 활성화 또는 비활성화할 수 있습니다.

이 작업에 대해

이 옵션을 설정하면 ONTAP는 효율적인 UNIX 보안 스타일을 사용하는 볼륨의 파일 및 폴더를 NTFS ACL을 갖는 것으로 SMB 클라이언트에 제공합니다. 이 옵션을 비활성화하면 볼륨이 SMB 클라이언트에 FAT 볼륨으로 표시됩니다. 기본값은 NTFS ACL을 SMB 클라이언트에 제공하는 것입니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. UNIX NTFS ACL 옵션 설정을 구성합니다. 'vserver cifs options modify -vserver_vserver_name_-is-unix-NT -acl-enabled{true|false}'
3. 옵션이 원하는 값('vserver cifs options show -vserver_vserver_name_')으로 설정되어 있는지 확인합니다
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

ONTAP SMB FlexVol 볼륨에 대한 **UNIX** 사용 권한을 유지하는 방법에 대해 알아봅니다

현재 UNIX 사용 권한이 있는 FlexVol 볼륨의 파일을 Windows 응용 프로그램에서 편집하고 저장하면 ONTAP에서 UNIX 사용 권한을 보존할 수 있습니다.

Windows 클라이언트의 응용 프로그램이 파일을 편집하고 저장할 때 파일의 보안 속성을 읽고, 새 임시 파일을 만들고,

해당 속성을 임시 파일에 적용한 다음 임시 파일에 원래 파일 이름을 지정합니다.

Windows 클라이언트가 보안 속성에 대한 쿼리를 수행할 때 UNIX 권한을 정확하게 나타내는 생성된 ACL을 받습니다. 이 생성된 ACL의 유일한 목적은 파일이 Windows 애플리케이션에 의해 업데이트되므로 파일의 UNIX 사용 권한을 보존하여 결과 파일이 동일한 UNIX 사용 권한을 갖도록 하는 것입니다. ONTAP는 생성된 ACL을 사용하여 NTFS ACL을 설정하지 않습니다.

ONTAP SMB 서버의 Windows 보안 탭을 사용하여 UNIX 권한을 관리하는 방법에 대해 알아봅니다

SVM에서 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 대한 UNIX 권한을 조작하려는 경우 Windows 클라이언트의 보안 탭을 사용할 수 있습니다. 또는 Windows ACL을 쿼리하고 설정할 수 있는 응용 프로그램을 사용할 수도 있습니다.

- UNIX 사용 권한 수정

  Windows 보안 탭을 사용하여 혼합 보안 스타일 볼륨 또는 qtree에 대한 UNIX 권한을 보고 변경할 수 있습니다. 기본 Windows 보안 탭을 사용하여 UNIX 권한을 변경하는 경우 변경하기 전에 먼저 편집할 기존 ACE(모드 비트를 0으로 설정)를 제거해야 합니다. 또는 고급 편집기를 사용하여 권한을 변경할 수도 있습니다.

  모드 권한을 사용하는 경우 나열된 UID, GID 및 기타(컴퓨터에 계정이 있는 다른 모든 사용자)에 대한 모드 권한을 직접 변경할 수 있습니다. 예를 들어, 표시된 UID에 r-x 권한이 있는 경우 UID 권한을 rwx로 변경할 수 있습니다.

- UNIX 권한을 NTFS 권한으로 변경합니다

  Windows 보안 탭을 사용하면 파일 및 폴더에 UNIX 유효 보안 스타일이 있는 혼합 보안 스타일 볼륨 또는 qtree의 UNIX 보안 개체를 Windows 보안 개체로 대체할 수 있습니다.

  원하는 Windows 사용자 및 그룹 개체로 대체하려면 먼저 나열된 모든 UNIX 권한 항목을 제거해야 합니다. 그런 다음 Windows 사용자 및 그룹 개체에서 NTFS 기반 ACL을 구성할 수 있습니다. 모든 UNIX 보안 개체를 제거하고 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 Windows 사용자 및 그룹만 추가하면 파일 또는 폴더의 효과적인 보안 스타일이 UNIX에서 NTFS로 변경됩니다.

  폴더에 대한 권한을 변경할 때 기본 Windows 동작은 이러한 변경 내용을 모든 하위 폴더 및 파일에 전파하는 것입니다. 따라서 보안 스타일의 변경 사항을 모든 하위 폴더, 하위 폴더 및 파일에 전파하지 않으려면 전파 선택 사항을 원하는 설정으로 변경해야 합니다.

SMB 서버 보안 설정을 관리합니다

ONTAP SMB 클라이언트 인증 처리에 대해 알아봅니다

사용자가 SVM에 포함된 데이터에 액세스하기 위해 SMB 연결을 생성하려면 먼저 SMB 서버가 속해 있는 도메인에서 인증을 받아야 합니다. SMB 서버는 Kerberos와 NTLM(NTLMv1 또는 NTLMv2)의 두 가지 인증 방법을 지원합니다. Kerberos는 도메인 사용자를 인증하는 데 사용되는 기본 방법입니다.

Kerberos 인증

ONTAP는 인증된 SMB 세션을 생성할 때 Kerberos 인증을 지원합니다.

Kerberos는 Active Directory의 기본 인증 서비스입니다. Kerberos 서버 또는 Kerberos KDC(Key Distribution Center) 서비스는 Active Directory에 보안 원칙에 대한 정보를 저장하고 검색합니다. NTLM 모델과 달리 SMB 서버와

같은 다른 컴퓨터와 세션을 설정하려는 Active Directory 클라이언트는 KDC에 직접 문의하여 세션 자격 증명을 얻습니다.

NTLM 인증

NTLM 클라이언트 인증은 암호를 기반으로 사용자별 비밀번호에 대한 공유 지식을 기반으로 하는 본인 확인 응답 프로토콜을 사용하여 수행됩니다.

사용자가 로컬 Windows 사용자 계정을 사용하여 SMB 연결을 만들면 NTLMv2를 사용하여 SMB 서버에서 로컬로 인증이 수행됩니다.

ONTAP SVM 재해 복구 구성을 위한 **SMB** 서버 보안 설정에 대해 알아보십시오

ID가 보존되지 않는 재해 복구 대상으로 구성된 SVM(SnapMirror 구성에서 '-identity-preserve' 옵션이 'false'로 설정됨)을 생성하기 전에 SVM 대상에서 SMB 서버 보안 설정이 관리되는 방식을 알아야 합니다.

- 기본이 아닌 SMB 서버 보안 설정은 대상에 복제되지 않습니다.

  대상 SVM에서 SMB 서버를 생성할 때 모든 SMB 서버 보안 설정이 기본값으로 설정됩니다. SVM 재해 복구 대상이 초기화, 업데이트 또는 재동기화되면 소스의 SMB 서버 보안 설정이 타겟으로 복제되지 않습니다.

- 기본이 아닌 SMB 서버 보안 설정을 수동으로 구성해야 합니다.

  소스 SVM에 기본값이 아닌 SMB 서버 보안 설정이 구성되어 있는 경우 SnapMirror 관계가 깨진 후, 대상이 읽기-쓰기 상태가 되면 대상 SVM에서 동일한 설정을 수동으로 구성해야 합니다.

ONTAP SMB 서버 보안 설정에 대한 정보를 표시합니다

SMB 서버 보안 설정에 대한 정보를 SVM(스토리지 가상 머신)에 표시할 수 있습니다. 이 정보를 사용하여 보안 설정이 올바른지 확인할 수 있습니다.

이 작업에 대해

표시된 보안 설정은 해당 개체의 기본값이거나 ONTAP CLI를 사용하거나 Active Directory 그룹 정책 개체(GPO)를 사용하여 구성된 기본값이 아닌 값일 수 있습니다.

일부 옵션이 유효하지 않으므로 워크그룹 모드에서 SMB 서버에 대해 "vserver cifs security show" 명령을 사용하지 마십시오.

단계

1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 표시하려면...	명령 입력...
지정된 SVM의 모든 보안 설정	'vserver cifs security show -vserver_vserver_name_'
SVM의 특정 보안 설정 또는 설정	'vserver cifs security show -vserver_vserver_name_ - 필드 [fieldname,...]'를 입력하면 '-fields?'를 입력할 수 있습니다 사용할 수 있는 필드를 결정합니다.

예

다음 예는 SVM VS1 보안 설정을 모두 보여줍니다.

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                           Kerberos Clock Skew:        5 minutes
                           Kerberos Ticket Age:        10 hours
                          Kerberos Renewal Age:        7 days
                          Kerberos KDC Timeout:        3 seconds
                           Is Signing Required:        false
                Is Password Complexity Required:       true
          Use start_tls For AD LDAP connection:        false
                      Is AES Encryption Enabled:       false
                         LM Compatibility Level:       lm-ntlm-ntlmv2-krb
                     Is SMB Encryption Required:       false
                        Client Session Security:       none
               SMB1 Enabled for DC Connections:        false
               SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:         false
              Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:         false
 AES session key enabled for NetLogon channel:         false
  Try Channel Binding For AD LDAP Connections:         false
```

표시되는 설정은 실행 중인 ONTAP 버전에 따라 다릅니다.

다음 예에서는 SVM VS1 Kerberos 클록 편중을 보여 줍니다.

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

관련 정보

GPO 구성에 대한 정보를 표시합니다

로컬 **SMB** 사용자에 대한 **ONTAP** 암호 복잡성을 구성합니다

필수 비밀번호 복잡성은 스토리지 가상 시스템(SVM)의 로컬 SMB 사용자를 위해 향상된 보안을 제공합니다. 필요한 암호 복잡성 기능은 기본적으로 활성화되어 있습니다. 이 기능을 사용하지

않도록 설정하고 언제든지 다시 사용하도록 설정할 수 있습니다.

시작하기 전에

CIFS 서버에서 로컬 사용자, 로컬 그룹 및 로컬 사용자 인증을 설정해야 합니다.

이 작업에 대해

일부 옵션이 유효하지 않으므로 작업 그룹 모드에서 CIFS 서버에 대한 명령을 사용하지 마십시오 `vserver cifs security modify`.

단계

1. 다음 작업 중 하나를 수행합니다.

로컬 **SMB** 사용자에 대한 암호 복잡성에 필요한 경우...	명령 입력...
활성화됨	'vserver cifs security modify -vserver_vserver_name_-is-password-Complexity -required true'
사용 안 함	'vserver cifs security modify -vserver_vserver_name_-is-password-Complexity -required false'

2. 필요한 암호 복잡성에 대한 보안 설정을 확인합니다. 'vserver cifs security show -vserver_vserver_name_'

예

다음 예에서는 SVM VS1 용 로컬 SMB 사용자에 대해 필요한 암호 복잡성이 활성화된 것을 보여 줍니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

관련 정보

- 서버 보안 설정에 대한 정보 표시
- 로컬 사용자 및 그룹에 대해 알아보세요
- 로컬 사용자 암호 요구 사항
- 로컬 사용자 계정 암호를 변경합니다

ONTAP SMB 서버 **Kerberos** 보안 설정을 수정합니다

허용되는 최대 Kerberos 클록 비뚤어짐 시간, Kerberos 티켓 수명 및 티켓 갱신 최대 일 수를

비롯한 특정 CIFS 서버 Kerberos 보안 설정을 수정할 수 있습니다.

이 작업에 대해

'vserver cifs security modify' 명령을 사용하여 CIFS 서버 Kerberos 설정을 수정하면 '-vserver' 매개 변수로 지정한 단일 SVM(스토리지 가상 머신)에서만 설정이 수정됩니다. Active Directory 그룹 정책 개체(GPO)를 사용하여 동일한 Active Directory 도메인에 속한 클러스터의 모든 SVM에 대한 Kerberos 보안 설정을 중앙에서 관리할 수 있습니다.

단계

1. 다음 작업 중 하나 이상을 수행합니다.

원하는 작업	입력…
허용되는 최대 Kerberos 클럭 편중 시간을 분(9.13.1 이상) 또는 초(9.12.1 이하)로 지정합니다.	'vserver cifs security modify -vserver_vserver_name_-Kerberos-clock -suts_integer_in_minutes_' 기본 설정은 5분입니다.
Kerberos 티켓 수명(시간)을 지정합니다.	'vserver cifs security modify -vserver_vserver_name_-Kerberos-티켓-age integer_in_hours'를 선택합니다 기본 설정은 10시간입니다.
티켓 갱신 최대 일 수를 지정하십시오.	'vserver cifs security modify - vserver_vserver_name_ - Kerberos - renew - age_integer_in_days _' 기본 설정은 7일입니다.
모든 KDC가 도달할 수 없음으로 표시되는 KDC의 소켓에 대한 시간 제한을 지정합니다.	'vserver cifs security modify -vserver_vserver_name_-Kerberos-KDC -timeout_integer_in_seconds _' 기본 설정은 3초입니다.

2. Kerberos 보안 설정을 확인합니다.

   'vserver cifs security show -vserver_vserver_name_'

예

다음 예에서는 Kerberos 보안을 다음과 같이 변경합니다. ""Kerberos Clock Skew""는 3분으로 설정되고 ""Kerberos Ticket Age""는 SVM VS1 v1의 경우 8시간으로 설정됩니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                     Kerberos Clock Skew:                     3 minutes
                     Kerberos Ticket Age:                     8 hours
                   Kerberos Renewal Age:                      7 days
                   Kerberos KDC Timeout:                      3 seconds
                    Is Signing Required:                 false
         Is Password Complexity Required:                  true
   Use start_tls For AD LDAP connection:                 false
              Is AES Encryption Enabled:                 false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:                 false
```

관련 정보

"서버 보안 설정에 대한 정보 표시"

"지원되는 GPO"

"CIFS 서버에 그룹 정책 객체 적용"

ONTAP SMB 서버 최소 인증 보안 수준을 설정합니다

SMB 클라이언트 액세스에 대한 비즈니스 보안 요구 사항을 충족하도록 SMB 서버에서 _LMCompatibilityLevel_이라고도 하는 SMB 서버 최소 보안 수준을 설정할 수 있습니다. 최소 보안 수준은 SMB 서버가 SMB 클라이언트에서 허용하는 최소 보안 토큰입니다.

이 작업에 대해

- 워크그룹 모드의 SMB 서버는 NTLM 인증만 지원합니다. Kerberos 인증은 지원되지 않습니다.
- LMCompatibilityLevel 관리자 인증이 아닌 SMB 클라이언트 인증에만 적용됩니다.

최소 인증 보안 수준을 지원되는 네 가지 보안 수준 중 하나로 설정할 수 있습니다.

값	설명
lm-NTLM-NTLMv2-KRB(기본값)	SVM(스토리지 가상 시스템)은 LM, NTLM, NTLMv2 및 Kerberos 인증 보안을 수락합니다.
NTLM-NTLMv2-KRB	SVM은 NTLM, NTLMv2 및 Kerberos 인증 보안을 수락합니다. SVM은 LM 인증을 거부합니다.

값	설명
NTLMv2-KRB	SVM은 NTLMv2 및 Kerberos 인증 보안을 수락합니다. SVM은 LM 및 NTLM 인증을 거부합니다.
KRB	SVM은 Kerberos 인증 보안만 수락합니다. SVM은 LM, NTLM 및 NTLMv2 인증을 거부합니다.

단계

1. 최소 인증 보안 수준을 설정합니다. 'vserver cifs security modify -vserver_vserver_name_-lm -compatibility -level{lm-NTLM-NTLMv2-KRB | NTLM-NTLMv2-KRB | NTLMv2-KRB | KRB | KRB}'
2. 인증 보안 수준이 원하는 수준('vserver cifs security show -vserver_vserver_name_')으로 설정되어 있는지 확인합니다

관련 정보

Kerberos 기반 통신을 위한 AES 암호화 구성

AES 암호화를 사용하여 **Kerberos** 기반 통신을 위한 강력한 **ONTAP SMB** 보안을 구성합니다

Kerberos 기반 통신을 사용하여 보안을 강화하기 위해 SMB 서버에서 AES-256 및 AES-128 암호화를 활성화할 수 있습니다. 기본적으로 SVM에서 SMB 서버를 생성할 때 AES(고급 암호화 표준) 암호화가 사용되지 않습니다. AES 암호화로 제공되는 강력한 보안을 활용하려면 이 기능을 활성화해야 합니다.

SMB를 위한 Kerberos 관련 통신은 SVM에서 SMB 서버를 생성하는 동안이나 SMB 세션 설정 단계에서 사용됩니다. SMB 서버는 Kerberos 통신을 위해 다음과 같은 암호화 유형을 지원합니다.

- AES 256
- AES 128
- DES
- RC4-HMAC

Kerberos 통신에 가장 높은 보안 암호화 유형을 사용하려면 SVM에서 Kerberos 통신에 AES 암호화를 사용하도록 설정해야 합니다.

SMB 서버가 생성되면 도메인 컨트롤러는 Active Directory에 컴퓨터 시스템 계정을 만듭니다. 이때 KDC는 특정 컴퓨터 계정의 암호화 기능을 인식합니다. 그런 다음 인증 중에 클라이언트가 서버에 제공하는 서비스 티켓을 암호화하기 위해 특정 암호화 유형을 선택합니다.

ONTAP 9.12.1부터 Active Directory(AD) KDC에 알릴 암호화 유형을 지정할 수 있습니다. 이 옵션을 사용하여 권장 암호화 유형을 활성화할 수 `-advertised-enc-types` 있으며 이 옵션을 사용하여 약한 암호화 유형을 비활성화할 수 있습니다. 의 방법을 "Kerberos 기반 통신을 위한 AES 암호화 구성"알아보십시오.

인텔 AES 새 명령어(인텔 AES NI)는 SMB 3.0에서 사용할 수 있으며, AES 알고리즘을 개선하고 지원되는 프로세서 제품군에서 데이터 암호화를 가속화합니다. SMB 3.1.1부터 AES-128-GCM은 SMB 암호화에 사용되는 해시 알고리즘으로 AES-128-CCM을 대체합니다.

관련 정보

ONTAP SMB Kerberos 기반 통신에 대해 AES 암호화를 구성합니다

Kerberos 기반 통신에서 가장 강력한 보안을 활용하려면 SMB 서버에서 AES-256 및 AES-128 암호화를 사용해야 합니다. ONTAP 9.13.1부터 AES 암호화는 기본적으로 사용하도록 설정됩니다. SMB 서버가 AD(Active Directory) KDC와 Kerberos 기반 통신을 위해 AES 암호화 유형을 선택하지 않도록 하려면 AES 암호화를 사용하지 않도록 설정할 수 있습니다.

AES 암호화가 기본적으로 사용되는지 여부와 암호화 유형을 지정하는 옵션이 있는지 여부는 ONTAP 버전에 따라 다릅니다.

ONTAP 버전입니다	**AES** 암호화 사용...	암호화 유형을 지정할 수 있습니까**?**
9.13.1 이상	기본적으로 사용됩니다	예
9.12.1	수동	예
9.11.1 이하	수동	아니요

ONTAP 9.12.1부터 AES 암호화는 을 사용하여 활성화 및 비활성화됩니다 `-advertised-enc-types` 옵션: AD KDC에 보급된 암호화 유형을 지정할 수 있습니다. 기본 설정은 입니다 `rc4` 및 `des`그러나 `AES` 유형이 지정되면 `AES` 암호화가 활성화됩니다. 이 옵션을 사용하여 약한 `RC4` 및 `DES` 암호화 유형을 명시적으로 비활성화할 수도 있습니다. `ONTAP 9.11.1` 이하 버전에서는 을 사용해야 합니다 `-is-aes-encryption-enabled` AES 암호화를 활성화 및 비활성화하는 옵션과 암호화 유형을 지정할 수 없습니다.

보안을 강화하기 위해 SVM(Storage Virtual Machine)은 AES 보안 옵션을 수정할 때마다 AD에서 시스템 계정 암호를 변경합니다. 암호를 변경하려면 컴퓨터 계정이 포함된 OU(조직 구성 단위)에 대한 관리 AD 자격 증명이 필요할 수 있습니다.

SVM이 ID가 보존되지 않는 재해 복구 대상으로 구성된 경우(`-identity-preserve` 옵션이 로 설정되어 있습니다 `false` SnapMirror 구성에서 기본 SMB 서버가 아닌 보안 설정은 대상에 복제되지 않습니다. 소스 SVM에서 AES 암호화를 사용하도록 설정한 경우 수동으로 활성화해야 합니다.

예 **13.** 단계

ONTAP 9.12.1 이상

1. 다음 작업 중 하나를 수행합니다.

Kerberos 통신을 위한 **AES** 암호화 유형을 원하는 경우…	명령 입력…
활성화됨	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
사용 안 함	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   ◦ 참고: * `-is-aes-encryption-enabled` 옵션은 ONTAP 9.12.1에서 사용되지 않으며 이후 릴리스에서 제거될 수 있습니다.

2. AES 암호화가 필요에 따라 활성화 또는 비활성화되었는지 확인합니다. `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

예

다음 예에서는 SVM VS1 기반 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

다음 예에서는 SVM VS2에서 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다. 관리자는 SMB 서버가 포함된 OU에 대한 관리 AD 자격 증명을 입력하라는 메시지가 표시됩니다.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1 이전 버전

1. 다음 작업 중 하나를 수행합니다.

Kerberos 통신을 위한 **AES** 암호화 유형을 원하는 경우…	명령 입력…
활성화됨	'vserver cifs security modify -vserver vserver_name -is-aes-encryption-enabled true'
사용 안 함	'vserver cifs security modify -vserver vserver_name -is-aes-encryption-enabled false'

2. AES 암호화가 원하는 대로 설정되거나 비활성화되었는지 확인합니다. 'vserver cifs security show -vserver vserver_name -fields is -aes-encryption-enabled'

   AES 암호화가 활성화된 경우 is-aes-encryption-enabled 필드가 true로 표시되고, 비활성화된 경우 false로 표시됩니다.

예

다음 예에서는 SVM VS1 기반 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

다음 예에서는 SVM VS2에서 SMB 서버에 대한 AES 암호화 유형을 사용하도록 설정합니다. 관리자는 SMB 서버가 포함된 OU에 대한 관리 AD 자격 증명을 입력하라는 메시지가 표시됩니다.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

관련 정보

"도메인 사용자가 Domain-Tunnel을 사용하여 클러스터에 로그인하지 못했습니다"

SMB 서명을 사용하여 네트워크 보안을 강화합니다

ONTAP SMB 서명을 사용하여 네트워크 보안을 향상시키는 방법에 대해 알아보십시오

SMB 서명을 사용하면 SMB 서버와 클라이언트 사이의 네트워크 트래픽이 손상되지 않도록 할 수 있으며, 재생 공격을 차단하여 이 작업을 수행합니다. 기본적으로 ONTAP는 클라이언트가 요청할 때 SMB 서명을 지원합니다. 필요에 따라 스토리지 관리자는 SMB 서명이 필요하도록 SMB 서버를 구성할 수 있습니다.

서명 정책이 **ONTAP SMB** 서버와의 통신에 어떤 영향을 미치는지 알아봅니다

CIFS 서버 SMB 서명 보안 설정 외에도 Windows 클라이언트의 두 SMB 서명 정책은 클라이언트와 CIFS 서버 간의 디지털 통신 서명을 제어합니다. 비즈니스 요구 사항에 맞게 설정을 구성할 수 있습니다.

클라이언트 SMB 정책은 MMC(Microsoft Management Console) 또는 Active Directory GPO를 사용하여 구성되는 Windows 로컬 보안 정책 설정을 통해 제어됩니다. 클라이언트 SMB 서명 및 보안 문제에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

다음은 Microsoft 클라이언트에 대한 두 가지 SMB 서명 정책에 대한 설명입니다.

- 'Microsoft 네트워크 클라이언트: 디지털 서명 통신(서버에서 동의한 경우)'

  이 설정은 클라이언트의 SMB 서명 기능이 설정되었는지 여부를 제어합니다. 기본적으로 활성화되어 있습니다. 클라이언트에서 이 설정을 비활성화하면 CIFS 서버와의 클라이언트 통신은 CIFS 서버의 SMB 서명 설정에 따라 달라집니다.

- 마이크로네트워크 클라이언트: 디지털 서명 통신(항상)

  이 설정은 클라이언트가 서버와 통신하기 위해 SMB 서명을 필요로 하는지 제어합니다. 기본적으로 비활성화되어 있습니다. 클라이언트에서 이 설정을 비활성화하면 SMB 서명 동작은 'Microsoft 네트워크 클라이언트: 디지털 서명 통신(서버에서 동의한 경우)' 및 CIFS 서버의 설정에 대한 정책 설정을 기반으로 합니다.

> ⓘ 환경에 SMB 서명이 필요하도록 구성된 Windows 클라이언트가 포함된 경우 CIFS 서버에서 SMB 서명을 설정해야 합니다. 그렇지 않으면 CIFS 서버가 이러한 시스템에 데이터를 제공할 수 없습니다.

클라이언트 및 CIFS 서버 SMB 서명 설정의 효과적인 결과는 SMB 세션이 SMB 1.0 또는 SMB 2.x 이상을 사용하는지 여부에 따라 달라집니다.

다음 표에는 세션이 SMB 1.0을 사용하는 경우 효과적인 SMB 서명 동작이 요약되어 있습니다.

클라이언트	**ONTAP —** 서명이 필요하지 않습니다	**ONTAP —** 서명이 필요합니다
서명이 비활성화되었으며 필요하지 않습니다	서명되지 않았습니다	서명됨
서명이 활성화되었으며 필요하지 않습니다	서명되지 않았습니다	서명됨
서명이 비활성화되었으며 필수입니다	서명됨	서명됨
서명이 설정되어 있어야 합니다	서명됨	서명됨

> ⓘ 클라이언트에서 서명이 비활성화되었지만 CIFS 서버에서 필요한 경우 이전 Windows SMB 1 클라이언트와 일부 비 Windows SMB 1 클라이언트가 연결되지 않을 수 있습니다.

다음 표에는 세션에서 SMB 2.x 또는 SMB 3.0을 사용하는 경우 효과적인 SMB 서명 동작이 요약되어 있습니다.

SMB 2.x 및 SMB 3.0 클라이언트의 경우 SMB 서명이 항상 사용하도록 설정됩니다. 비활성화할 수 없습니다.

클라이언트	**ONTAP —** 서명이 필요하지 않습니다	**ONTAP —** 서명이 필요합니다
서명이 필요하지 않습니다	서명되지 않았습니다	서명됨
서명이 필요합니다	서명됨	서명됨

다음 표에는 기본 Microsoft 클라이언트 및 서버 SMB 서명 동작이 요약되어 있습니다.

프로토콜	해시 알고리즘입니다	활성화/비활성화할 수 있습니다	필요/필요하지 않습니다	클라이언트 기본값입니다	서버 기본값	**DC** 기본값
SMB 1.0	MD5	예	예	활성화됨(필요하지 않음)	사용 안 함(필수 아님)	필수 요소입니다
SMB 2.x	HMAC SHA-256	아니요	예	필요하지 않습니다	필요하지 않습니다	필수 요소입니다
SMB 3.0	AES-CMAC	아니요	예	필요하지 않습니다	필요하지 않습니다	필수 요소입니다

Microsoft는 더 이상 '고유 서명 통신(클라이언트에서 동의한 경우)' 또는 '고유 서명 통신(서버에서 동의한 경우)' 그룹 정책 설정을 사용할 것을 권장하지 않습니다. Microsoft는 또한 "EnableSecuritySignature" 레지스트리 설정을 더 이상 사용하지 않을 것을 권장합니다. 이러한 옵션은 SMB 1 동작에만 영향을 미치며 Digitally sign communications (Always)(항상 서명 통신) 그룹 정책 설정 또는 RequireSecuritySignature(요구 보안 서명) 레지스트리 설정으로 대체할 수 있습니다. 또한 Microsoft 블로그에서 자세한 정보를 얻을 수 있습니다. The SMB 서명의 기본 사항(SMB1 및 SMB2 모두 포함)

ONTAP SMB 서명의 성능 영향에 대해 알아보십시오

SMB 세션에서 SMB 서명을 사용하면 Windows 클라이언트와 주고 받는 모든 SMB 통신이 성능에 영향을 미치며, 이는 클라이언트와 서버(즉, SMB 서버가 포함된 SVM을 실행하는 클러스터의 노드) 모두에 영향을 미칩니다.

네트워크 트래픽의 양은 변하지 않지만, 클라이언트와 서버 모두에서 CPU 사용량이 증가하면 성능에 미치는 영향이 나타납니다.

성능에 미치는 영향은 실행 중인 ONTAP 9 버전에 따라 달라집니다. ONTAP 9.7부터 새로운 암호화 오프 로드 알고리즘을 통해 서명된 SMB 트래픽의 성능을 향상시킬 수 있습니다. SMB 서명 오프로드는 SMB 서명이 설정된 경우 기본적으로 설정됩니다.

향상된 SMB 서명 성능을 위해서는 AES-NI 오프로드 기능이 필요합니다. 해당 플랫폼에서 AES-NI 오프로드가 지원되는지 확인하려면 HWU(Hardware Universe)를 참조하십시오.

훨씬 빠른 GCM 알고리즘을 지원하는 SMB 버전 3.11을 사용할 수 있다면 더욱 향상된 성능을 얻을 수 있습니다.

네트워크, ONTAP 9 버전, SMB 버전 및 SVM 구축에 따라 SMB 서명의 성능에 미치는 영향은 매우 다양할 수 있으며 네트워크 환경에서 테스트를 통해서만 확인할 수 있습니다.

대부분의 Windows 클라이언트는 서버에서 SMB 서명을 사용하는 경우 기본적으로 협상합니다. 일부 Windows 클라이언트에 대해 SMB 보호가 필요하고 SMB 서명으로 인해 성능 문제가 발생하는 경우 재생 공격에 대한 보호가 필요하지 않은 Windows 클라이언트에서 SMB 서명을 사용하지 않도록 설정할 수 있습니다. Windows 클라이언트에서 SMB 서명을 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

ONTAP SMB 서명 구성 권장 사항

SMB 클라이언트와 CIFS 서버 간에 SMB 서명 동작을 구성하여 보안 요구 사항을 충족할 수 있습니다. CIFS 서버에서 SMB 서명을 구성할 때 선택하는 설정은 보안 요구 사항에 따라 다릅니다.

클라이언트 또는 CIFS 서버에서 SMB 서명을 구성할 수 있습니다. SMB 서명을 구성할 때 다음 권장 사항을 고려하십시오.

만약...	권장 사항...
클라이언트와 서버 간의 통신 보안을 강화하려는 경우	클라이언트에서 'Require Option(Sign Always)' 보안 설정을 활성화하여 클라이언트에서 SMB 서명이 필요하도록 합니다.
모든 SMB 트래픽이 특정 SVM(스토리지 가상 머신)에 서명하기를 원합니다	SMB 서명이 필요하도록 보안 설정을 구성하여 CIFS 서버에 SMB 서명이 필요합니다.

Windows 클라이언트 보안 설정 구성에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

여러 데이터 **LIFS**에 대한 **ONTAP SMB** 서명 구성에 대해 자세히 알아보십시오

SMB 서버에서 필요한 SMB 서명을 설정하거나 해제하는 경우 SVM에 대한 여러 데이터 LIF 구성에 대한 지침을 숙지해야 합니다.

SMB 서버를 구성할 때 여러 데이터 LIF가 구성되어 있을 수 있습니다. 이 경우 DNS 서버에 동일한 SMB 서버 호스트 이름을 사용하는 CIFS 서버에 대한 여러 개의 "A" 레코드 항목이 포함되어 있고 각 항목은 고유한 IP 주소를 사용합니다. 예를 들어, 두 개의 데이터 LIF가 구성된 SMB 서버의 DNS 'A' 레코드 항목은 다음과 같습니다.

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

일반적으로 필요한 SMB 서명 설정을 변경하면 클라이언트의 새 연결만 SMB 서명 설정의 변경 사항에 영향을 받습니다. 그러나 이 동작에 대한 예외는 있습니다. 클라이언트가 공유에 대한 기존 연결을 가지고 있고, 원래 연결을 유지하면서 설정을 변경한 후 클라이언트가 동일한 공유에 대한 새 연결을 생성하는 경우가 있습니다. 이 경우 새로운 SMB 연결과 기존 SMB 연결이 모두 새로운 SMB 서명 요구 사항을 적용합니다.

다음 예제를 고려해 보십시오.

1. CLIENT1은 'O:\' 경로를 사용하여 SMB 서명이 필요 없이 공유에 연결합니다.
2. 스토리지 관리자는 SMB 서명이 필요하도록 SMB 서버 구성을 수정합니다.
3. CLIENT1은 ':\' 경로를 사용하여('O:\' 경로를 사용하여 연결을 유지하면서) 필요한 SMB 서명과 동일한 공유에 연결합니다.
4. 그 결과, "O:\"와 "s:\" 드라이브 모두에서 데이터에 액세스할 때 SMB 서명이 사용됩니다.

수신 **SMB** 트래픽에 대한 **ONTAP** 서명을 구성합니다

필요한 SMB 서명을 설정하여 클라이언트가 SMB 메시지에 서명하도록 요구 사항을 적용할 수 있습니다. 활성화된 경우 ONTAP는 유효한 서명이 있는 경우에만 SMB 메시지를 수락합니다. SMB 서명을 허용하되 SMB 서명이 필요하지 않은 경우 필요한 SMB 서명을 사용하지 않도록 설정할 수 있습니다.

이 작업에 대해

기본적으로 필요한 SMB 서명은 사용되지 않습니다. 필요한 SMB 서명을 언제든지 설정하거나 해제할 수 있습니다.

다음과 같은 상황에서는 SMB 서명이 기본적으로 비활성화되어 있지 않습니다.

1. 필요한 SMB 서명이 설정되어 있고 클러스터가 SMB 서명을 지원하지 않는 ONTAP 버전으로 되돌려집니다.
2. 이후 클러스터는 SMB 서명을 지원하는 ONTAP 버전으로 업그레이드됩니다.

   이러한 경우 지원되는 ONTAP 버전에 원래 구성된 SMB 서명 구성은 재버전과 후속 업그레이드를 통해 유지됩니다.

SVM(Storage Virtual Machine) 재해 복구 관계를 설정할 때 'napMirror create' 명령의 '-identity-preserve' 옵션에 선택한 값에 따라 타겟 SVM에 복제된 구성 세부 정보가 결정됩니다.

만약 '-identity-preserve' 옵션을 'true'(ID-preserve)로 설정하면 SMB 서명 보안 설정이 대상에 복제됩니다.

'-identity-preserve' 옵션을 false(non-ID-preserve)로 설정하면 SMB 서명 보안 설정이 대상에 복제되지 않습니다. 이 경우 대상의 CIFS 서버 보안 설정이 기본값으로 설정됩니다. 소스 SVM에서 필요한 SMB 서명을 사용하도록 설정한 경우, 대상 SVM에서 필요한 SMB 서명을 수동으로 활성화해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

SMB 서명이 필요한 경우	명령 입력…
활성화됨	'vserver cifs security modify -vserver_vserver_name_-is-signing-required true'
사용 안 함	'vserver cifs security modify -vserver_vserver_name_-is-signing-required false'

2. 다음 명령의 출력에서 "is signing required" 필드의 값이 원하는 값으로 설정되어 있는지 확인하여 필요한 SMB 서명이 활성화되어 있는지 또는 비활성화되어 있는지 확인합니다. 'vserver cifs security show

-vserver_vserver_name_-fields is-signing-required'

예

다음 예에서는 SVM VS1 에 필요한 SMB 서명을 활성화합니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

암호화 설정에 대한 변경 사항은 새 연결에 적용됩니다. 기존 연결은 영향을 받지 않습니다.

관련 정보

- "SnapMirror 생성"

ONTAP SMB 세션이 서명되어 있는지 확인합니다

CIFS 서버에서 연결된 SMB 세션에 대한 정보를 표시할 수 있습니다. 이 정보를 사용하여 SMB 세션이 서명되었는지 확인할 수 있습니다. 이 방법은 SMB 클라이언트 세션이 원하는 보안 설정과 연결되어 있는지 여부를 확인하는 데 유용합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 표시하려면...	명령 입력...
지정된 스토리지 가상 시스템(SVM)에서 서명된 모든 세션	'vserver cifs session show -vserver_vserver_name_ -is-session-signed true'
SVM에서 특정 세션 ID와 서명된 세션의 세부 정보	'vserver cifs session show -vserver_vserver_name_ -session-id integer-instance'

예

다음 명령을 실행하면 SVM VS1 에서 서명된 세션에 대한 세션 정보가 표시됩니다. 기본 요약 출력에는 ""세션 서명됨" 출력 필드가 표시되지 않습니다.

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

다음 명령을 실행하면 세션 ID가 2인 SMB 세션에서 세션의 서명 여부를 비롯한 자세한 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

관련 정보

SMB 서명 세션 통계 모니터링

ONTAP SMB 서명 세션 통계를 모니터링합니다

SMB 세션 통계를 모니터링하고 서명된 설정된 세션과 그렇지 않은 세션을 확인할 수 있습니다.

이 작업에 대해

고급 권한 레벨의 '통계' 명령은 서명된 SMB 세션 수를 모니터링하는 데 사용할 수 있는 'signed_sessions' 카운터를 제공합니다. 'Signed_sessions' 카운터는 다음과 같은 통계 객체와 함께 사용할 수 있습니다.

- 'CIFS'를 사용하면 모든 SMB 세션에 대해 SMB 서명을 모니터링할 수 있습니다.

- 'MB1'을 사용하면 SMB 1.0 세션에 대한 SMB 서명을 모니터링할 수 있습니다.
- 'MB2'를 사용하면 SMB 2.x 및 SMB 3.0 세션에 대한 SMB 서명을 모니터링할 수 있습니다.

  SMB 3.0 통계는 'MB2' 객체의 출력에 포함됩니다.

서명된 세션의 수를 총 세션 수와 비교하려면 'signed_sessions' 카운터의 출력을 '설정된_sessions' 카운터의 출력과 비교할 수 있습니다.

결과 데이터를 보려면 먼저 통계 샘플 수집을 시작해야 합니다. 데이터 수집을 중지하지 않으면 샘플의 데이터를 볼 수 있습니다. 데이터 수집을 중지하면 고정된 샘플이 제공됩니다. 데이터 수집을 중지하지 않으면 이전 쿼리와 비교하는 데 사용할 수 있는 업데이트된 데이터를 가져올 수 있습니다. 비교를 통해 추세를 파악할 수 있습니다.

단계

1. 권한 수준을 advanced:+'et-Privilege advanced로 설정합니다
2. 데이터 수집 시작:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   '-sample-id' 매개 변수를 지정하지 않으면 명령이 샘플 식별자를 생성하고 이 샘플을 CLI 세션의 기본 샘플로 정의합니다. '-sample-id'의 값은 텍스트 문자열입니다. 동일한 CLI 세션에서 이 명령을 실행하고 '-sample-id' 매개 변수를 지정하지 않으면 명령이 이전 기본 샘플을 덮어씁니다.

   선택적으로 통계를 수집할 노드를 지정할 수 있습니다. 노드를 지정하지 않으면 이 샘플에서 클러스터의 모든 노드에 대한 통계를 수집합니다.

   에 대한 자세한 내용은 `statistics start` "ONTAP 명령 참조입니다"을 참조하십시오.
3. 'tortistics stop' 명령어를 이용하여 시료에 대한 데이터 수집을 중단한다.

   자세히 알아보세요 `statistics stop` 에서 "ONTAP 명령 참조입니다" .
4. SMB 서명 통계 보기:

에 대한 정보를 보려면...	입력...
서명된 세션	shope-sample-id sample_ID-counter signed_sessions
node_name[-node_node_name_]'	서명된 세션 및 설정된 세션
shope-sample-id_sample_ID_-counter signed_sessions	ESTANCE_SECURIONS

   단일 노드에 대한 정보만 표시하려면 옵션 '-node' 매개 변수를 지정합니다.

   에 대한 자세한 내용은 `statistics show` "ONTAP 명령 참조입니다"을 참조하십시오.
5. 관리자 권한 수준으로 돌아가기: + 'Set-Privilege admin

예

다음 예에서는 SVM(Storage Virtual Machine) VS1 에서 SMB 2.x 및 SMB 3.0 서명 통계를 모니터링하는 방법을 보여 줍니다.

다음 명령을 실행하면 고급 권한 레벨로 이동합니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

다음 명령을 실행하면 샘플의 데이터 수집이 중지됩니다.

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

다음 명령을 실행하면 서명된 SMB 세션과 샘플의 노드별 설정된 SMB 세션이 표시됩니다.

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

다음 명령을 실행하면 샘플에서 노드 2에 대해 서명된 SMB 세션이 표시됩니다.

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    node_name                                                node2
    signed_sessions                                              1
```

다음 명령을 실행하면 admin 권한 레벨로 다시 이동됩니다.

```
cluster1::*> set -privilege admin
```

관련 정보

- SMB 세션이 서명되었는지 확인합니다
- "성능 모니터링 및 관리 개요"

SMB를 통한 데이터 전송을 위해 **SMB** 서버에서 필요한 **SMB** 암호화를 구성합니다

ONTAP SMB 암호화에 대해 알아보십시오

SMB를 통한 데이터 전송을 위한 SMB 암호화는 SMB 서버에서 활성화 또는 비활성화할 수 있는 향상된 보안 기능입니다. 공유 속성 설정을 통해 공유별로 원하는 SMB 암호화 설정을 구성할 수도 있습니다.

기본적으로 SVM(스토리지 가상 머신)에 SMB 서버를 생성할 때 SMB 암호화는 사용하지 않도록 설정됩니다. SMB 암호화를 통해 제공되는 향상된 보안을 활용하려면 이 기능을 활성화해야 합니다.

암호화된 SMB 세션을 생성하려면 SMB 클라이언트가 SMB 암호화를 지원해야 합니다. Windows Server 2012 및 Windows 8부터 시작되는 Windows 클라이언트는 SMB 암호화를 지원합니다.

SVM의 SMB 암호화는 두 가지 설정을 통해 제어됩니다.

- SVM에서 기능을 활성화하는 SMB 서버 보안 옵션
- 공유 단위로 SMB 암호화 설정을 구성하는 SMB 공유 속성입니다

SVM의 모든 데이터에 액세스하려면 암호화를 사용할지, 선택한 공유에서만 데이터에 액세스하려면 SMB 암호화가 필요한지 여부를 결정할 수 있습니다. SVM 레벨 설정이 공유 레벨 설정보다 우선합니다.

효과적인 SMB 암호화 구성은 두 가지 설정의 조합에 따라 달라지며 다음 표에 설명되어 있습니다.

SMB 서버 **SMB** 암호화가 활성화되었습니다	공유 암호화 데이터 설정이 활성화되었습니다	서버측 암호화 동작
참	거짓	SVM의 모든 공유에 대해 서버 레벨 암호화가 활성화됩니다. 이 구성을 사용하면 전체 SMB 세션에 대해 암호화가 수행됩니다.
참	참	공유 레벨 암호화와 관계없이 SVM의 모든 공유에 대해 서버 레벨 암호화가 활성화됩니다. 이 구성을 사용하면 전체 SMB 세션에 대해 암호화가 수행됩니다.
거짓	참	특정 공유에 대해 공유 수준 암호화가 설정됩니다. 이 구성을 사용하면 트리 연결로부터 암호화가 수행됩니다.
거짓	거짓	암호화가 활성화되지 않았습니다.

암호화를 지원하지 않는 SMB 클라이언트는 암호화가 필요한 SMB 서버 또는 공유에 연결할 수 없습니다.

암호화 설정에 대한 변경 사항은 새 연결에 적용됩니다. 기존 연결은 영향을 받지 않습니다.

ONTAP SMB 암호화가 성능에 미치는 영향에 대해 알아보십시오

SMB 세션에서 SMB 암호화를 사용하면 Windows 클라이언트와 서버 간의 모든 SMB 통신이 성능에 영향을 미치며, 이는 클라이언트와 서버 모두에 영향을 미칩니다(즉, SMB 서버가 포함된 SVM을 실행하는 클러스터의 노드).

네트워크 트래픽의 양은 변하지 않지만, 클라이언트와 서버 모두에서 CPU 사용량이 증가하면 성능에 미치는 영향이 나타납니다.

성능에 미치는 영향은 실행 중인 ONTAP 9 버전에 따라 달라집니다. ONTAP 9.7부터 새로운 암호화 오프 로드 알고리즘을 통해 암호화된 SMB 트래픽에서 성능을 향상시킬 수 있습니다. SMB 암호화 오프로드는 SMB 암호화가 활성화된 경우 기본적으로 활성화됩니다.

향상된 SMB 암호화 성능을 위해서는 AES-NI 오프로드 기능이 필요합니다. 해당 플랫폼에서 AES-NI 오프로드가 지원되는지 확인하려면 HWU(Hardware Universe)를 참조하십시오.

훨씬 빠른 GCM 알고리즘을 지원하는 SMB 버전 3.11을 사용할 수 있다면 더욱 향상된 성능을 얻을 수 있습니다.

네트워크, ONTAP 9 버전, SMB 버전 및 SVM 구축에 따라 SMB 암호화가 성능에 미치는 영향은 매우 다양할 수 있으며 네트워크 환경의 테스트를 통해서만 확인할 수 있습니다.

SMB 서버에서 SMB 암호화는 기본적으로 비활성화되어 있습니다. 암호화가 필요한 SMB 공유 또는 SMB 서버에서만 SMB 암호화를 활성화해야 합니다. SMB 암호화를 통해 ONTAP는 요청을 암호 해독하고 모든 요청에 대한 응답을 암호화하는 추가 처리를 수행합니다. 따라서 필요한 경우에만 SMB 암호화를 활성화해야 합니다.

들어오는 트래픽에 대해 **ONTAP SMB** 암호화를 사용하거나 사용하지 않도록 설정합니다

수신 SMB 트래픽에 SMB 암호화가 필요한 경우 CIFS 서버 또는 공유 레벨에서 설정할 수 있습니다. 기본적으로 SMB 암호화는 필요하지 않습니다.

이 작업에 대해

CIFS 서버에서 SMB 암호화를 설정하면 CIFS 서버의 모든 공유에 적용됩니다. CIFS 서버의 모든 공유에 대해 SMB 암호화가 필요하지 않거나 공유 단위로 수신 SMB 트래픽에 대해 필요한 SMB 암호화를 설정하려는 경우 CIFS 서버에서 필요한 SMB 암호화를 해제할 수 있습니다.

SVM(Storage Virtual Machine) 재해 복구 관계를 설정할 때 'napmirror create' 명령의 '-identity-preserve' 옵션에 선택한 값에 따라 타겟 SVM에 복제된 구성 세부 정보가 결정됩니다.

만약 '-identity-preserve' 옵션을 'true'(ID-preserve)로 설정하면 SMB 암호화 보안 설정이 대상에 복제됩니다.

'-identity-preserve' 옵션을 false(non-ID-preserve)로 설정하면 SMB 암호화 보안 설정이 대상에 복제되지 않습니다. 이 경우 대상의 CIFS 서버 보안 설정이 기본값으로 설정됩니다. 소스 SVM에서 SMB 암호화를 사용하도록 설정한 경우 대상에서 CIFS 서버 SMB 암호화를 수동으로 설정해야 합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

CIFS 서버에서 들어오는 **SMB** 트래픽에 대해 **SMB** 암호화가 필요한 경우	명령 입력…
활성화됨	'vserver cifs security modify -vserver_vserver_name_-is-smb-encryption -required true'
사용 안 함	'vserver cifs security modify -vserver_vserver_name_-is-smb-encryption -required false'

2. CIFS 서버에서 필요한 SMB 암호화가 원하는 대로 설정되거나 비활성화되었는지 확인합니다. 'vserver cifs security show -vserver_vserver_name_-fields is-smb-encryption-required'

   CIFS 서버에 필요한 SMB 암호화가 설정되어 있으면 is-smb-encryption-required 필드에 true가 표시되고, 비활성화된 경우에는 false가 표시됩니다.

예

다음 예에서는 SVM VS1에서 CIFS 서버에 대해 수신 SMB 트래픽에 필요한 SMB 암호화를 설정합니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

관련 정보

- "SnapMirror 생성"

클라이언트가 암호화된 **ONTAP SMB** 세션을 사용하여 연결되어 있는지 확인합니다

연결된 SMB 세션에 대한 정보를 표시하여 클라이언트가 암호화된 SMB 연결을 사용하는지 여부를 확인할 수 있습니다. 이 방법은 SMB 클라이언트 세션이 원하는 보안 설정과 연결되어 있는지 여부를 확인하는 데 유용합니다.

이 작업에 대해

SMB 클라이언트 세션은 다음 세 가지 암호화 수준 중 하나를 가질 수 있습니다.

- "암호화되지 않음"

  SMB 세션이 암호화되지 않았습니다. SVM(스토리지 가상 시스템) 레벨 또는 공유 레벨 암호화가 구성되지 않았습니다.

- 부분적으로 암호화되었습니다

트리 연결이 발생하면 암호화가 시작됩니다. 공유 수준 암호화가 구성됩니다. SVM 레벨 암호화가 활성화되지 않았습니다.

- '암호화됨'

  SMB 세션이 완전히 암호화됩니다. SVM 레벨 암호화가 활성화됩니다. 공유 수준 암호화가 활성화되어 있거나 활성화되어 있지 않을 수 있습니다. SVM 레벨 암호화 설정이 공유 레벨 암호화 설정보다 우선합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 표시하려면...	명령 입력...
지정된 SVM의 세션에 대해 지정된 암호화 설정을 갖는 세션	'vserver cifs session show -vserver_vserver_name_{encrypted
sPartially-encrypted	encrypted}-instance'
지정된 SVM에서 특정 세션 ID의 암호화 설정입니다	'vserver cifs session show -vserver_vserver_name_ -session-id_integer_-instance'

예

다음 명령을 실행하면 세션 ID가 2인 SMB 세션에서 암호화 설정을 비롯한 자세한 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                Open Shares: 1
                 Open Files: 1
                 Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

SMB 암호화 통계를 모니터링하고 설정된 세션 및 공유 연결이 암호화되고 암호화되지 않은 세션을 확인할 수 있습니다.

이 작업에 대해

고급 권한 레벨의 '통계' 명령은 다음 카운터를 제공하며, 이 카운터를 사용하여 암호화된 SMB 세션 수를 모니터링하고 연결을 공유할 수 있습니다.

카운터 이름	설명
'암호화 세션'	암호화된 SMB 3.0 세션의 수를 제공합니다
'암호화_공유_연결'	트리 연결이 발생한 암호화된 공유 수를 제공합니다
"암호화되지 않은 세션"이 끼어들었습니다	에서는 클라이언트 암호화 기능이 부족하여 거부된 세션 설정 수를 제공합니다
"암호화되지 않은_공유"가 있습니다	에서는 클라이언트 암호화 기능이 없어 거부된 공유 매핑 수를 제공합니다

이러한 카운터는 다음 통계 개체에서 사용할 수 있습니다.

- 'CIFS'를 사용하면 모든 SMB 3.0 세션에 대해 SMB 암호화를 모니터링할 수 있습니다.

  SMB 3.0 통계는 'CIFS' 객체의 출력에 포함됩니다. 암호화된 세션의 수를 총 세션 수와 비교하려면 "encrypted_sessions" 카운터의 출력과 "encrypted_sessions" 카운터의 출력을 비교할 수 있습니다.

  암호화된 공유 연결 수와 총 공유 연결 수를 비교하려면 에 대한 출력을 비교할 수 있습니다 `encrypted_share_connections` 에 대한 출력이 있는 카운터 `connected_shares` 카운터.

- reped_cencrypted_sessions는 SMB 암호화를 지원하지 않는 클라이언트로부터 암호화를 요구하는 SMB 세션을 설정하려고 시도한 횟수를 제공합니다.
- refened_cencrypted_share는 SMB 암호화를 지원하지 않는 클라이언트의 암호화가 필요한 SMB 공유에 연결하려고 시도한 횟수를 제공합니다.

결과 데이터를 보려면 먼저 통계 샘플 수집을 시작해야 합니다. 데이터 수집을 중지하지 않으면 샘플의 데이터를 볼 수 있습니다. 데이터 수집을 중지하면 고정된 샘플이 제공됩니다. 데이터 수집을 중지하지 않으면 이전 쿼리와 비교하는 데 사용할 수 있는 업데이트된 데이터를 가져올 수 있습니다. 비교를 통해 추세를 파악할 수 있습니다.

단계

1. 권한 수준을 advanced:+'et-Privilege advanced로 설정합니다
2. 데이터 수집 시작:
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   '-sample-id' 매개 변수를 지정하지 않으면 명령이 샘플 식별자를 생성하고 이 샘플을 CLI 세션의 기본 샘플로 정의합니다. '-sample-id'의 값은 텍스트 문자열입니다. 동일한 CLI 세션에서 이 명령을 실행하고 '-sample-id' 매개 변수를 지정하지 않으면 명령이 이전 기본 샘플을 덮어씁니다.

선택적으로 통계를 수집할 노드를 지정할 수 있습니다. 노드를 지정하지 않으면 이 샘플에서 클러스터의 모든 노드에 대한 통계를 수집합니다.

에 대한 자세한 내용은 `statistics start` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 'tortistics stop' 명령어를 이용하여 시료에 대한 데이터 수집을 중단한다.

   자세히 알아보세요 `statistics stop` 에서 "ONTAP 명령 참조입니다" .

4. SMB 암호화 통계 보기:

에 대한 정보를 보려면...	입력...
암호화된 세션	'shope-sample-id_sample_ID_-counter encrypted_sessions
node_name[-node_node_name_]'	암호화된 세션 및 설정된 세션
shope-sample-id_sample_ID_-counter encrypted_sessions	encrypted_sessions
node_name[-node_node_name_]'	암호화된 공유 연결
'shope-sample-id_sample_ID_-counter encrypted_share_connections	*node_name*[-node_node_name_]'
암호화된 공유 연결 및 연결된 공유	'sHow-sample-id_sample_ID_-counter encrypted_share_connections
Connected_share	*node_name*[-node_node_name_]'
암호화되지 않은 세션이 거부되었습니다	shope-sample-id_sample_ID_-counter rejected_sencrypted_sessions
node_name[-node_node_name_]'	암호화되지 않은 공유 연결이 거부되었습니다
'shd-sample-id_sample_ID_-counter rejected_sencrypted_share	*node_name*[-node_node_name_]'

   단일 노드에 대해서만 정보를 표시하려면 옵션 '-node' 매개 변수를 지정합니다.

   에 대한 자세한 내용은 `statistics show` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 관리자 권한 수준으로 돌아가기: + 'Set-Privilege admin

예

다음 예에서는 SVM(Storage Virtual Machine) VS1 에서 SMB 3.0 암호화 통계를 모니터링하는 방법을 보여 줍니다.

다음 명령을 실행하면 고급 권한 레벨로 이동합니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

다음 명령을 실행하면 새 샘플의 데이터 수집이 시작됩니다.

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

다음 명령을 실행하면 해당 샘플의 데이터 수집이 중지됩니다.

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

다음 명령을 실행하면 암호화된 SMB 세션 및 샘플의 노드에 의해 설정된 SMB 세션이 표시됩니다.

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    ----------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

다음 명령을 실행하면 샘플에서 노드에서 암호화되지 않은 암호화되지 않은 SMB 세션이 거부된 수가 표시됩니다.

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

다음 명령을 실행하면 샘플의 노드에 의해 연결된 SMB 공유 및 암호화된 SMB 공유의 수가 표시됩니다.

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

다음 명령을 실행하면 샘플에서 노드에서 암호화되지 않은 암호화되지 않은 SMB 공유 연결이 거부된 수가 표시됩니다.

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

관련 정보

- 서버에서 사용 가능한 통계, 개체 및 카운터를 확인합니다.
- "성능 모니터링 및 관리 개요"

보안 **LDAP** 세션 통신

ONTAP SMB LDAP 서명 및 봉인에 대해 자세히 알아보십시오

ONTAP 9부터는 AD(Active Directory) 서버에 대한 쿼리에 대해 LDAP 세션 보안을 사용하도록

서명과 봉인을 구성할 수 있습니다. SVM(스토리지 가상 시스템)의 CIFS 서버 보안 설정을 LDAP 서버의 보안 설정에 맞게 구성해야 합니다.

서명은 비밀 키 기술을 사용하여 LDAP 페이로드 데이터의 무결성을 확인합니다. 봉인은 LDAP 페이로드 데이터를 암호화하여 중요한 정보를 일반 텍스트로 전송하지 않도록 합니다. LDAP 보안 수준_ 옵션은 LDAP 트래픽의 서명, 서명 및 봉인 여부를 나타냅니다. 기본값은 '없음'입니다.

SVM에서 SVM CIFS 보안 수정 명령에 대한 '-session-security-for-ad-ldap' 옵션을 사용하여 CIFS 트래픽에 대한 LDAP 서명 및 봉인을 사용할 수 있습니다.

ONTAP SMB 서버에서 **LDAP** 서명 및 봉인을 활성화합니다

CIFS 서버가 Active Directory LDAP 서버와의 보안 통신을 위해 서명 및 봉인을 사용하려면 먼저 CIFS 서버 보안 설정을 수정하여 LDAP 서명 및 봉인을 설정해야 합니다.

시작하기 전에

적절한 보안 구성 값을 확인하려면 AD 서버 관리자에게 문의해야 합니다.

단계

1. Active Directory LDAP 서버에서 서명되고 봉인된 트래픽을 사용할 수 있도록 CIFS 서버 보안 설정을 구성합니다. 'vserver cifs security modify -vserver_vserver_name_-session-security-for-ad-ldap{none|sign|seal}'

   서명('사인', 데이터 무결성), 서명 및 봉인('씰', 데이터 무결성 및 암호화) 또는 둘 다('없음', 서명 또는 봉인 없음)을 사용할 수 있습니다. 기본값은 '없음'입니다.

2. LDAP 서명 및 봉인 보안 설정이 올바르게 설정되었는지 확인합니다. 'vserver cifs security show -vserver_vserver_name_'

> SVM이 이름 매핑 또는 사용자, 그룹, 넷그룹과 같은 기타 UNIX 정보를 쿼리하기 위해 동일한 LDAP 서버를 사용하는 경우 'vserver services name-service ldap client modify' 명령의 '-session-security' 옵션을 사용하여 해당 설정을 활성화해야 합니다.

TLS를 통해 **LDAP**를 구성합니다

ONTAP SMB SVM에 대한 자체 서명 루트 **CA** 인증서를 내보냅니다

Active Directory 통신을 보호하기 위해 SSL/TLS를 통한 LDAP를 사용하려면 먼저 Active Directory 인증서 서비스의 자체 서명 루트 CA 인증서 복사본을 인증서 파일로 내보내고 ASCII 텍스트 파일로 변환해야 합니다. 이 텍스트 파일은 ONTAP에서 SVM(스토리지 가상 머신)에 인증서를 설치하는 데 사용됩니다.

시작하기 전에

CIFS 서버가 속한 도메인에 대해 Active Directory 인증서 서비스가 이미 설치 및 구성되어 있어야 합니다. Active Director 인증서 서비스 설치 및 구성에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

"Microsoft TechNet 라이브러리: technet.microsoft.com"

단계

1. '.pem' 텍스트 형식인 도메인 컨트롤러의 루트 CA 인증서를 얻습니다.

   "Microsoft TechNet 라이브러리: technet.microsoft.com"

작업을 마친 후

SVM에 인증서를 설치합니다.

관련 정보

"Microsoft TechNet 라이브러리"

ONTAP SMB SVM에 자체 서명된 루트 **CA** 인증서를 설치합니다

LDAP 서버에 바인딩할 때 TLS를 사용한 LDAP 인증이 필요한 경우 먼저 SVM에 자체 서명된 루트 CA 인증서를 설치해야 합니다.

이 작업에 대해

TLS 통신을 사용하는 ONTAP 내의 모든 응용 프로그램은 OCSP(온라인 인증서 상태 프로토콜)를 사용하여 디지털 인증서 상태를 확인할 수 있습니다. OCSP가 TLS를 통해 LDAP에 대해 활성화된 경우 해지된 인증서가 거부되고 연결이 실패합니다.

단계

1. 자체 서명된 루트 CA 인증서 설치:
   a. 인증서 설치를 시작합니다. 'Security certificate install - vserver vserver_name -type server -ca'

      콘솔 출력에는 'Please enter Certificate: press <Enter> when done(인증서를 입력하십시오. 완료되면 <Enter> 키를 누르십시오)' 메시지가 표시됩니다

   b. 텍스트 편집기로 인증서 '.pem' 파일을 열고 '-----'로 시작하는 줄을 포함하여 인증서를 복사합니다. 인증서 시작 ---- '----'로 끝나는 종료 인증서 ---- 그런 다음 명령 프롬프트 뒤에 인증서를 붙여 넣습니다.
   c. 인증서가 올바르게 표시되는지 확인합니다.
   d. Enter 키를 눌러 설치를 완료합니다.
2. 인증서가 설치되어 있는지 확인합니다. 'Security certificate show -vserver_vserver_name_'

관련 정보

- "보안 인증서 설치"
- "보안 인증서가 표시됩니다"

ONTAP SMB 서버에서 **TLS**를 통한 **LDAP**를 활성화합니다

SMB 서버가 Active Directory LDAP 서버와의 보안 통신에 TLS를 사용하려면 먼저 SMB 서버 보안 설정을 수정하여 TLS를 통한 LDAP를 활성화해야 합니다.

ONTAP 9.10.1부터 LDAP 채널 바인딩은 AD(Active Directory) 및 이름 서비스 LDAP 연결에 대해 기본적으로 지원됩니다. ONTAP는 시작 TLS 또는 LDAPS가 활성화되고 세션 보안이 서명 또는 봉인으로 설정된 경우에만 LDAP 연결을 사용하여 채널 바인딩을 시도합니다. AD 서버에서 LDAP 채널 바인딩을 비활성화하거나 다시 설정하려면 ' vserver cifs security modify ' 명령을 사용하여 '-try-channel-binding-for-ad-ldap' 매개 변수를 사용합니다.

자세한 내용은 다음을 참조하십시오.

- "ONTAP NFS SVM용 LDAP에 대해 알아보세요"
- "Windows의 2020 LDAP 채널 바인딩 및 LDAP 서명 요구 사항".

단계

1. Active Directory LDAP 서버와 보안 LDAP 통신을 허용하는 SMB 서버 보안 설정을 구성합니다. 'vserver cifs security modify -vserver_vserver_name_-use-start-tls-for-ad-ldap true'
2. TLS를 통한 LDAP 보안 설정이 "true"로 설정되어 있는지 확인합니다. vserver cifs security show -vserver_vserver_name_

> SVM이 이름 매핑 또는 기타 UNIX 정보(예: 사용자, 그룹 및 넷그룹)를 쿼리하기 위해 동일한 LDAP 서버를 사용하는 경우 'vserver services name-service ldap client modify' 명령을 사용하여 '-use-start-tls' 옵션도 수정해야 합니다.

성능 및 이중화를 위해 **ONTAP SMB** 다중 채널을 구성합니다

ONTAP 9.4부터 SMB 다중 채널을 구성하여 단일 SMB 세션에서 ONTAP와 클라이언트 간에 여러 연결을 제공할 수 있습니다. 이렇게 하면 처리량과 내결함성이 개선됩니다.

시작하기 전에

SMB 3.0 이상 버전에서 클라이언트가 협상하는 경우에만 SMB 멀티 채널 기능을 사용할 수 있습니다. SMB 3.0 이상은 기본적으로 ONTAP SMB 서버에서 사용하도록 설정됩니다.

이 작업에 대해

ONTAP 클러스터에서 적절한 구성이 식별되는 경우 SMB 클라이언트가 자동으로 여러 네트워크 연결을 감지하고 사용합니다.

SMB 세션의 동시 연결 수는 구축한 NIC에 따라 달라집니다.

- * 클라이언트와 ONTAP 클러스터의 1G NIC *

  클라이언트는 NIC당 하나의 연결을 설정하고 모든 연결에 세션을 바인딩합니다.

- * 클라이언트 및 ONTAP 클러스터에 10G 이상의 대용량 NIC *

  클라이언트는 NIC당 최대 4개의 연결을 설정하고 모든 연결에 세션을 바인딩합니다. 클라이언트는 여러 개의 10G 및 대용량 NIC에 연결을 설정할 수 있습니다.

다음 매개 변수(고급 권한)도 수정할 수 있습니다.

- `-max-connections-per-session`

  다중 채널 세션당 허용되는 최대 연결 수입니다. 기본값은 32개 연결입니다.

  기본값보다 더 많은 연결을 설정하려면 기본값인 32개의 연결을 사용하는 클라이언트 구성을 동일하게 조정해야 합니다.

- `-max-lifs-per-session`

Multichannel 세션당 공고되는 최대 네트워크 인터페이스 수입니다. 기본값은 256개의 네트워크 인터페이스입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. SMB 서버에서 SMB 멀티 채널 활성화:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. ONTAP가 SMB 멀티 채널 세션을 보고하는지 확인합니다.

```
vserver cifs session show
```

4. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

예

다음 예에서는 모든 SMB 세션에 대한 정보를 표시하며 단일 세션에 대해 여러 개의 연결을 표시합니다.

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

다음 예에서는 세션 ID 1이 있는 SMB 세션에 대한 자세한 정보를 표시합니다.

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
                Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
               Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

SMB 서버에서 기본 **Windows** 사용자를 **UNIX** 사용자 매핑으로 구성합니다

기본 **ONTAP SMB UNIX** 사용자를 구성합니다

기본 UNIX 사용자는 사용자의 다른 모든 매핑 시도가 실패하거나 UNIX와 Windows 간에 개별 사용자를 매핑하지 않으려는 경우에 사용하도록 구성할 수 있습니다. 또는 매핑되지 않은 사용자의 인증에 실패하도록 하려면 기본 UNIX 사용자를 구성하지 않아야 합니다.

이 작업에 대해

기본적으로 기본 UNIX 사용자의 이름은 ""pcuser""입니다. 즉, 기본적으로 기본 UNIX 사용자에 대한 사용자 매핑이 설정됩니다. 기본 UNIX 사용자로 사용할 다른 이름을 지정할 수 있습니다. 지정하는 이름은 SVM(스토리지 가상 머신)용으로 구성된 네임 서비스 데이터베이스에 있어야 합니다. 이 옵션이 null 문자열로 설정된 경우 CIFS 서버를 UNIX 기본 사용자로 액세스할 수 없습니다. 즉, 각 사용자는 CIFS 서버를 액세스하기 전에 암호 데이터베이스에 계정이 있어야 합니다.

사용자가 기본 UNIX 사용자 계정을 사용하여 CIFS 서버에 접속하려면 다음과 같은 사전 요구 사항을 충족해야 합니다.

- 사용자가 인증됩니다.
- 사용자가 CIFS 서버의 로컬 Windows 사용자 데이터베이스, CIFS 서버의 홈 도메인 또는 신뢰할 수 있는 도메인에 있습니다(CIFS 서버에서 다중 도메인 이름 매핑 검색이 설정된 경우).
- 사용자 이름이 null 문자열에 명시적으로 매핑되어 있지 않습니다.

단계

1. 기본 UNIX 사용자 구성:

원하는 작업	입력...
기본 UNIX 사용자 ""pcuser"" 사용	'vserver cifs options modify-default-unix-user pcuser'
다른 UNIX 사용자 계정을 기본 사용자로 사용합니다	'vserver cifs options modify-default-unix-user_user_name_'
기본 UNIX 사용자를 비활성화합니다	'vserver cifs options modify-default-unix-user"'

'vserver cifs options modify-default-unix-user pcuser'

2. 기본 UNIX 사용자가 올바르게 구성되었는지 확인합니다. 'vserver cifs options show -vserver_vserver_name_'

다음 예에서는 기본 UNIX 사용자와 SVM VS1 게스트 UNIX 사용자 모두 UNIX 사용자 ""pcuser""를 사용하도록 구성되어 있습니다.

'vserver cifs options show -vserver vs1'을 선택합니다

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

게스트 **ONTAP SMB UNIX** 사용자를 구성합니다

게스트 UNIX 사용자 옵션을 구성하면 신뢰할 수 없는 도메인에서 로그인하는 사용자가 게스트 UNIX 사용자에게 매핑되고 CIFS 서버에 연결할 수 있습니다. 또는 신뢰할 수 없는 도메인의 사용자 인증에 실패하도록 하려면 게스트 UNIX 사용자를 구성하지 않아야 합니다. 기본값은 신뢰할 수 없는 도메인의 사용자가 CIFS 서버에 접속할 수 없도록 하는 것입니다(게스트 UNIX 계정이 구성되지 않음).

이 작업에 대해

게스트 UNIX 계정을 구성할 때 다음 사항을 염두에 두어야 합니다.

- CIFS 서버가 홈 도메인 또는 신뢰할 수 있는 도메인 또는 로컬 데이터베이스에 대한 도메인 컨트롤러에 대해 사용자를 인증할 수 없고 이 옵션이 설정된 경우 CIFS 서버는 사용자를 게스트 사용자로 간주하고 지정된 UNIX 사용자에게 매핑합니다.
- 이 옵션을 null 문자열로 설정하면 게스트 UNIX 사용자가 비활성화됩니다.

- SVM(Storage Virtual Machine) 이름 서비스 데이터베이스 중 하나에서 게스트 UNIX 사용자로 사용할 UNIX 사용자를 생성해야 합니다.
- 게스트 사용자로 로그인한 사용자는 자동으로 CIFS 서버에 있는 BUILTIN\guests 그룹의 구성원입니다.
- 'homedirs-public' 옵션은 인증된 사용자에게만 적용됩니다. 게스트 사용자로 로그인한 사용자는 홈 디렉토리가 없으며 다른 사용자의 홈 디렉토리에 액세스할 수 없습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	입력...
게스트 UNIX 사용자를 구성합니다	'vserver cifs options modify-guest-unix-user_unix_name_'
게스트 UNIX 사용자를 비활성화합니다	'vserver cifs options modify-guest-unix-user"'

   'vserver cifs options modify-guest-unix-user pcuser'

2. 게스트 UNIX 사용자가 올바르게 구성되었는지 확인합니다. 'vserver cifs options show -vserver_vserver_name_'

   다음 예에서는 기본 UNIX 사용자와 SVM VS1 게스트 UNIX 사용자 모두 UNIX 사용자 ""pcuser""를 사용하도록 구성되어 있습니다.

   'vserver cifs options show -vserver vs1'을 선택합니다

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

관리자 그룹을 **ONTAP SMB** 루트에 매핑합니다

사용자 환경에 CIFS 클라이언트만 있고 SVM(스토리지 가상 시스템)을 멀티프로토콜 스토리지 시스템으로 설정한 경우, SVM에서 파일에 액세스할 수 있는 루트 권한이 있는 Windows 계정이 하나 이상 있어야 합니다. 그렇지 않으면 충분한 사용자 권한이 없기 때문에 SVM을 관리할 수 없습니다.

이 작업에 대해

스토리지 시스템이 NTFS 전용으로 설정된 경우 이 `/etc` 디렉토리에는 administrators 그룹이 ONTAP 구성 파일에 액세스할 수 있는 파일 수준 ACL이 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 관리자 그룹을 루트에 적절하게 매핑하는 CIFS 서버 옵션을 구성합니다.

원하는 작업	그러면...
관리자 그룹 구성원을 루트에 매핑합니다	'vserver cifs options modify -vserver_vserver_name_-is-admin-users-mapped-to-root-enabled true' 계정을 루트로 매핑하는 `/etc/usermap.cfg' 항목이 없는 경우에도 administrators 그룹의 모든 계정은 루트로 간주됩니다. administrators 그룹에 속하는 계정을 사용하여 파일을 생성하는 경우 UNIX 클라이언트에서 파일을 볼 때 파일은 루트에서 소유합니다.
관리자 그룹 구성원을 루트에 매핑하도록 해제합니다	"vserver cifs options modify -vserver_vserver_name_-is-admin-users-mapped-to-root-enabled false" administrators 그룹의 계정은 더 이상 루트에 매핑되지 않습니다. 단일 사용자만 루트에 명시적으로 매핑할 수 있습니다.

3. 옵션이 원하는 값('vserver cifs options show -vserver_vserver_name_')으로 설정되어 있는지 확인합니다
4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

ONTAP SMB 세션을 통해 연결된 사용자 유형에 대한 정보를 표시합니다

SMB 세션을 통해 연결된 사용자 유형에 대한 정보를 표시할 수 있습니다. 따라서 적절한 유형의 사용자만 SVM(스토리지 가상 머신)의 SMB 세션을 통해 연결할 수 있습니다.

이 작업에 대해

다음 유형의 사용자는 SMB 세션을 통해 연결할 수 있습니다.

- '로컬 사용자'

  로컬 CIFS 사용자로 인증되었습니다

- '다민 사용자'입니다

  도메인 사용자로 인증됨(CIFS 서버의 홈 도메인 또는 신뢰할 수 있는 도메인)

- 'guest-user'입니다

  게스트 사용자로 인증되었습니다

- 익명의 사용자

  익명 또는 null 사용자로 인증되었습니다

단계

1. SMB 세션을 통해 연결된 사용자 유형을 확인합니다. 'vserver cifs session show -vserver_vserver_name_ -windows-user_windows_user_name_-fields windows-user, address, lif-address, user-type'

설정된 세션에 대한 사용자 유형 정보를 표시하려면...	다음 명령을 입력합니다...
사용자 유형이 지정된 모든 세션에 대해	'vserver cifs session show -vserver_vserver_name_ -user-type{local-user
domain-user	guest-user
anonymous-user}'입니다	특정 사용자의 경우

예

다음 명령을 실행하면 ""iepubs\user1" 사용자가 설정한 SVM VS1 세션의 사용자 유형에 대한 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

과도한 **Windows** 클라이언트 리소스 사용을 제한하는 **ONTAP** 명령 옵션입니다

'vserver cifs options modify' 명령 옵션을 사용하면 Windows 클라이언트의 리소스 사용을 제어할 수 있습니다. 이 기능은 클라이언트가 리소스 사용의 정상적인 범위를 벗어난 경우(예: 열려 있는 파일의 수가 비정상적으로 많거나 세션이 열려 있거나 변경 알림 요청이 있는 경우) 유용합니다.

Windows 클라이언트 리소스 사용을 제어하기 위해 'vserver cifs options modify' 명령에 대한 다음 옵션이 추가되었습니다. 이 옵션 중 최대값이 초과되면 요청이 거부되고 EMS 메시지가 전송됩니다. 이 옵션에 대해 구성된 제한값의 80%에 도달하면 EMS 경고 메시지도 전송됩니다.

- '-max-오픈-파일-트리 단위'

  CIFS 트리당 동일한 파일에 대한 최대 열기 수입니다

- '-max-same-user-sessions-per-connection'

  동일한 사용자가 접속당 연 최대 세션 수입니다

- '-max-same-tree-connect-per-session'

  세션당 동일한 공유에 대한 최대 트리 연결 수입니다

- `-max-s워치-세트당-트리'

트리당 설정된 최대 시계 수(_CHANGE ALBERS_라고도 함)입니다

에 대한 자세한 내용은 `vserver cifs options modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 9.4부터 SMB 버전 2 이상을 실행하는 서버는 클라이언트가 SMB 연결을 통해 서버로 전송할 수 있는 미해결 요청(*smb* 크레딧) 수를 제한할 수 있습니다. SMB 크레딧의 관리는 클라이언트가 시작하고 서버에 의해 제어됩니다.

SMB 연결에서 허용할 수 있는 최대 요청 수는 '-max-credits' 옵션으로 제어됩니다. 이 옵션의 기본값은 128입니다.

기존 **oplocks** 및 리스 **oplocks**로 클라이언트 성능 향상

기존 및 임대 확대를 통해 **ONTAP SMB** 클라이언트 성능을 개선하는 방법에 대해 알아보십시오

기존 oplocks(기회 잠금) 및 리스 oplocks는 특정 파일 공유 시나리오에서 SMB 클라이언트가 미리 읽기, 쓰기 후 및 잠금 정보의 클라이언트측 캐싱을 수행할 수 있도록 합니다. 그러면 클라이언트는 해당 파일에 액세스해야 한다는 사실을 서버에 정기적으로 알려주지 않고 파일을 읽거나 파일에 쓸 수 있습니다. 이렇게 하면 네트워크 트래픽이 줄어들어 성능이 향상됩니다.

리스 oplocks는 SMB 2.1 프로토콜 이상에서 사용할 수 있는 향상된 형태의 oplocks입니다. 리스 oplocks를 사용하면 클라이언트가 자체적으로 시작된 여러 SMB에서 클라이언트 캐싱 상태를 확보하고 유지할 수 있습니다.

oplocks는 다음 두 가지 방법으로 제어할 수 있습니다.

- 공유를 생성할 때 공유 속성에 의해 'vserver cifs share create' 명령을 사용하거나 생성 후 'vserver share properties' 명령을 사용합니다.
- qtree가 생성될 때 'volume qtree create' 명령을 사용하거나 생성 후 'volume qtree oplock' 명령을 사용하여 qtree 속성에 의해 생성됩니다.

oplocks를 사용할 때 **ONTAP SMB** 캐시 데이터 손실 고려 사항을 작성하는 방법에 대해 알아봅니다

경우에 따라 프로세스에 파일에 배타적 oplock이 있고 두 번째 프로세스에서 파일을 열려고 시도할 경우 첫 번째 프로세스에서는 캐시된 데이터를 무효화하고 쓰기 및 잠금을 플러시해야 합니다. 그런 다음 클라이언트는 oplock 및 파일에 대한 액세스를 양도해야 합니다. 이 플러시 중에 네트워크 장애가 발생하면 캐시된 쓰기 데이터가 손실될 수 있습니다.

- 데이터 손실 가능성

  다음과 같은 상황에서는 쓰기 캐싱된 데이터가 있는 모든 애플리케이션에서 해당 데이터가 손실될 수 있습니다.

  - 연결은 SMB 1.0을 사용하여 이루어집니다.
  - 파일에 배타적 oplock이 있습니다.
  - 해당 oplock을 깨거나 파일을 닫도록 합니다.
  - 쓰기 캐시를 플러시하는 프로세스 중에 네트워크 또는 타겟 시스템에서 오류가 발생합니다.
- 오류 처리 및 쓰기 완료

  캐시 자체는 오류 처리를 하지 않습니다. 애플리케이션에서 캐시에 쓰기를 수행할 때는 항상 쓰기가 완료됩니다. 캐시가 네트워크를 통해 타겟 시스템에 쓰기를 수행하는 경우 쓰기가 완료된 것으로 가정해야 합니다. 그렇지 않으면 데이터가 손실되기 때문입니다.

oplocks를 사용하면 클라이언트가 파일을 잠그고 컨텐츠를 로컬에서 캐시할 수 있으므로 파일 작업의 성능이 향상됩니다. oplocks는 스토리지 가상 시스템(SVM)에 상주하는 SMB 공유에 설정됩니다. 경우에 따라 oplocks를 해제할 수 있습니다. 공유별로 oplocks를 설정하거나 해제할 수 있습니다.

이 작업에 대해

공유가 포함된 볼륨에 oplocks가 설정되어 있지만 해당 공유에 대한 oplock 공유 속성이 비활성화되어 있으면 해당 공유에 대해 oplocks가 해제됩니다. 공유에서 oplocks를 비활성화하면 볼륨 oplock 설정보다 우선적으로 적용됩니다. 공유에서 oplocks를 비활성화하면 임시 oplocks와 리스 oplocks가 모두 비활성화됩니다.

쉼표로 구분된 목록을 사용하여 oplock 공유 속성을 지정하는 것 외에도 다른 공유 속성을 지정할 수 있습니다. 다른 공유 매개 변수를 지정할 수도 있습니다.

단계

1. 해당 작업을 수행합니다.

원하는 작업	그러면...
공유를 생성하는 동안 공유에 oplocks를 설정합니다	'vserver cifs share create -vserver_vserver_name_ -share-name share_name -path path_to_share-share-properties [oplocks,...]' 명령을 입력합니다 공유에서 oplocks, browable, changentify의 기본 공유 속성만 사용하려면 SMB 공유를 생성할 때 '-share-properties' 매개 변수를 지정하지 않아도 됩니다. 기본값 이외의 공유 속성을 조합하려면 해당 공유에 사용할 공유 속성 목록과 함께 '-share-properties' 매개 변수를 지정해야 합니다.
공유를 생성하는 동안 공유에 oplocks를 사용하지 않도록 설정합니다	'vserver cifs share create-vserver_vserver_name_-share-name_share_name_-path_to_share_-share-properties[other_share_property,...]' 명령을 입력합니다 oplocks를 해제할 때는 공유를 생성할 때 공유 속성 목록을 지정해야 하지만 "oplocks" 속성을 지정해서는 안 됩니다.

관련 정보

기존 SMB 공유에서 oplocks를 설정하거나 해제합니다

oplock 상태를 모니터링합니다

SMB 볼륨 및 qtree에서 oplocks를 사용하거나 사용하지 않도록 설정하는 ONTAP 명령입니다

oplocks를 사용하면 클라이언트가 파일을 잠그고 컨텐츠를 로컬에서 캐시할 수 있으므로 파일 작업의 성능이 향상됩니다. 볼륨 또는 qtree에서 oplocks를 설정하거나 해제하는 명령을 알아야 합니다. 또한 볼륨 및 qtree에서 oplocks를 설정하거나 해제할 수 있는 시기를 알아야 합니다.

- oplocks는 기본적으로 볼륨에 설정됩니다.
- 볼륨을 생성할 때는 oplocks를 해제할 수 없습니다.
- 언제든지 기존 볼륨에서 SVM에 대한 oplocks를 설정하거나 해제할 수 있습니다.
- SVM에 대해 qtree에서 oplocks를 설정할 수 있습니다.

  oplock 모드 설정은 qtree ID 0의 속성으로, 모든 볼륨에 있는 기본 qtree입니다. qtree를 생성할 때 oplock 설정을 지정하지 않으면 qtree가 기본적으로 사용되는 상위 볼륨의 oplock 설정을 상속합니다. 그러나 새 qtree에 oplock 설정을 지정하면 볼륨의 oplock 설정보다 우선합니다.

원하는 작업	이 명령 사용...
볼륨 또는 qtree에 oplocks를 설정합니다	'-oplock-mode' 매개 변수가 'enable'로 설정된 볼륨 qtree oplocks
볼륨 또는 qtree에서 oplocks를 해제합니다	'-oplock-mode' 매개 변수가 '사용할 수 있음'으로 설정된 볼륨 qtree oplocks입니다

관련 정보

oplock 상태를 모니터링합니다

기존 ONTAP SMB 공유에서 oplocks를 사용하거나 사용하지 않도록 설정합니다

oplocks는 기본적으로 스토리지 가상 시스템(SVM)의 SMB 공유에 설정됩니다. 경우에 따라 oplocks를 해제할 수도 있습니다. 이전에 공유에서 oplocks를 해제한 경우에는 oplocks를 다시 설정할 수도 있습니다.

이 작업에 대해

공유가 포함된 볼륨에 oplocks가 설정되어 있지만 해당 공유에 대한 oplock 공유 속성이 비활성화되어 있으면 해당 공유에 대해 oplocks가 비활성화됩니다. 공유에 oplocks를 사용하지 않도록 설정하면 볼륨에서 oplocks를 설정하는 것이 우선합니다. 공유에서 oplocks를 비활성화하면 임시 oplocks와 리스 oplocks가 모두 비활성화됩니다. 언제든지 기존 공유에 oplocks를 설정하거나 해제할 수 있습니다.

단계

1. 해당 작업을 수행합니다.

원하는 작업	그러면...
기존 공유를 수정하여 공유에 oplocks를 설정합니다	'vserver cifs share properties add -vserver_vserver_name_-share-name share_name-share-properties oplocks' 명령을 입력합니다 쉼표로 구분된 목록을 사용하여 추가할 추가 공유 속성을 지정할 수 있습니다. 새로 추가된 속성은 기존 공유 속성 목록에 추가됩니다. 이전에 지정한 공유 속성은 그대로 유지됩니다.
기존 공유를 수정하여 공유에 oplocks를 사용하지 않도록 설정합니다	'vserver cifs share properties remove-vserver_vserver_name_-share-name_share_name_-share-properties oplocks' 명령을 입력합니다 쉼표로 구분된 목록을 사용하여 제거할 추가 공유 속성을 지정할 수 있습니다. 제거한 공유 속성은 기존 공유 속성 목록에서 삭제되지만 이전에 구성한 공유 속성은 제거하지 않습니다.

예

다음 명령을 실행하면 스토리지 가상 시스템(SVM, 이전 명칭 Vserver) VS1 에서 ""Engineering""이라는 이름의 공유에 대한 oplocks가 설정됩니다.

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

다음 명령을 실행하면 SVM VS1 에서 ""Engineering""이라는 이름의 공유에 대한 oplocks가 해제됩니다.

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

관련 정보

- SMB 공유를 생성할 때 oplocks를 설정하거나 해제합니다
- oplock 상태를 모니터링합니다
- 기존 주식에 주식 속성 추가 또는 제거

ONTAP SMB oplock 상태를 모니터링합니다

oplock 상태에 대한 정보를 모니터링하고 표시할 수 있습니다. 이 정보를 사용하여 oplocks가 있는 파일, oplock 레벨 및 oplock 상태 수준이 무엇인지, oplock 리스가 사용되는지 여부를 확인할 수 있습니다. 수동으로 해제해야 하는 잠금에 대한 정보를 확인할 수도 있습니다.

이 작업에 대해

모든 oplocks에 대한 정보를 요약 양식 또는 세부 목록 양식에 표시할 수 있습니다. 선택적 매개 변수를 사용하여 기존 잠금의 하위 집합에 대한 정보를 표시할 수도 있습니다. 예를 들어, 지정된 클라이언트 IP 주소 또는 지정된 경로를 사용하여 출력 반환만 잠그도록 지정할 수 있습니다.

기존 및 리스 oplocks에 대한 다음 정보를 표시할 수 있습니다.

- oplock이 설정된 SVM, 노드, 볼륨 및 LIF입니다
- UUID를 잠급니다
- oplock을 사용하는 클라이언트의 IP 주소입니다
- oplock이 설정된 경로입니다
- 잠금 프로토콜(SMB) 및 유형(oplock)
- 잠금 상태
- oplock 레벨
- 연결 상태 및 SMB 만료 시간입니다
- 임대 oplock이 부여된 경우 그룹 ID를 엽니다

에 대한 자세한 내용은 `vserver oplocks show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 'vserver lock show' 명령을 사용하여 oplock 상태를 표시합니다.

예

다음 명령을 실행하면 모든 잠금에 대한 기본 정보가 표시됩니다. 표시된 파일의 oplock은 "임시 배치" oplock 레벨로 허가됩니다.

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

다음 예제는 경로 '/data2/data2_2/intro.pptx'를 사용하여 파일의 잠금에 대한 자세한 정보를 표시합니다. IP 주소가 10.3.1.3 인 클라이언트에 배치 oplock 레벨이 있는 파일에 리스 oplock이 부여됩니다.

자세한 정보를 표시할 때 이 명령은 oplock 및 sharelock 정보에 대한 별도의 출력을 제공합니다. 이 예제는 oplock 섹션의 출력만 보여 줍니다.

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

관련 정보

SMB 공유를 생성할 때 oplocks를 설정하거나 해제합니다

기존 SMB 공유에서 oplocks를 설정하거나 해제합니다

SMB 볼륨 및 Qtree에서 Oplock을 활성화하거나 비활성화하기 위한 명령

SMB 서버에 그룹 정책 개체를 적용합니다

그룹 정책 개체를 **ONTAP SMB** 서버에 적용하는 방법에 대해 알아봅니다

SMB 서버는 Active Directory 환경의 컴퓨터에 적용되는 _group 정책 특성_이라는 규칙 집합인 GPO(그룹 정책 개체)를 지원합니다. GPO를 사용하여 동일한 Active Directory 도메인에 속한 클러스터의 모든 SVM(스토리지 가상 머신)에 대한 설정을 중앙에서 관리할 수 있습니다.

SMB 서버에서 GPO를 사용하도록 설정하면 ONTAP가 GPO 정보를 요청하는 Active Directory 서버에 LDAP 쿼리를 보냅니다. SMB 서버에 적용할 수 있는 GPO 정의가 있는 경우 Active Directory 서버는 다음 GPO 정보를 반환합니다.

- GPO 이름입니다
- 현재 GPO 버전입니다
- GPO 정의의 위치입니다
- GPO 정책 집합에 대한 UUID(Universally Unique Identifier) 목록입니다

관련 정보

- 서버의 파일 액세스 보안에 대해 알아보세요
- "SMB 및 NFS 감사 및 보안 추적"

지원되는 **ONTAP SMB GPO**에 대해 알아봅니다

모든 GPO(그룹 정책 개체)가 CIFS 지원 SVM(스토리지 가상 머신)에 적용되는 것은 아니지만 SVM은 관련 GPO 세트를 인식하고 처리할 수 있습니다.

현재 SVM에서 지원되는 GPO는 다음과 같습니다.

- 고급 감사 정책 구성 설정:

  객체 액세스: 중앙 액세스 정책 스테이징

  다음 설정을 포함하여 중앙 액세스 정책(CAP) 스테이징에 대해 감사할 이벤트 유형을 지정합니다.

  - 감사 금지
  - 성공 이벤트만 감사합니다
  - 오류 이벤트만 감사합니다
  - 성공 및 실패 이벤트를 모두 감사합니다

  > ⓘ 세 가지 감사 옵션 중 하나를 설정하면(성공 이벤트만 감사, 실패 이벤트만 감사, 성공 및 실패 이벤트 모두 감사) ONTAP는 성공 및 실패 이벤트를 모두 감사합니다.

  Advanced Audit Policy Configuration/Audit Policies/Object Access GPO에서 Audit Central Access Policy Staging 설정을 이용하여 설정한다.

  > ⓘ 고급 감사 정책 구성 GPO 설정을 사용하려면 이 설정을 적용할 CIFS 지원 SVM에 대해 감사를 구성해야 합니다. SVM에서 감사를 구성하지 않으면 GPO 설정이 적용되지 않고 삭제됩니다.

- 레지스트리 설정:

  - CIFS 지원 SVM에 대한 그룹 정책 업데이트 간격

    레지스트리 GPO를 사용하여 설정합니다.

  - 그룹 정책 무작위 오프셋을 새로 고칩니다

    레지스트리 GPO를 사용하여 설정합니다.

  - BranchCache에 대한 해시 게시

BranchCache GPO의 해시 게시는 BranchCache 운영 모드에 해당합니다. 지원되는 세 가지 작동 모드가 지원됩니다.

- 공유당
- 전체 공유
- '레지스트리' GPO를 사용하여 설정을 비활성화했습니다.

◦ BranchCache에 대한 해시 버전 지원

다음 세 가지 해시 버전 설정이 지원됩니다.

- BranchCache 버전 1
- BranchCache 버전 2
- BranchCache 버전 1 및 2는 레지스트리 GPO를 사용하여 설정합니다.

> BranchCache GPO 설정을 사용하려면 이러한 설정을 적용할 CIFS 지원 SVM에 BranchCache를 구성해야 합니다. SVM에 BranchCache가 구성되어 있지 않으면 GPO 설정이 적용되지 않고 삭제됩니다.

- 보안 설정
  - 감사 정책 및 이벤트 로그
    - 로그온 이벤트를 감사합니다

      다음 설정을 포함하여 감사할 로그온 이벤트의 유형을 지정합니다.

      - 감사 금지
      - 성공 이벤트만 감사합니다
      - 장애 이벤트 감사
      - Local Policies/Audit Policy GPO에서 Audit logon events 설정을 이용하여 성공 및 실패 이벤트를 모두 Audit한다.

        > 세 가지 감사 옵션 중 하나를 설정하면(성공 이벤트만 감사, 실패 이벤트만 감사, 성공 및 실패 이벤트 모두 감사) ONTAP는 성공 및 실패 이벤트를 모두 감사합니다.

    - 개체 액세스를 감사합니다

      다음 설정을 포함하여 감사할 개체 액세스 유형을 지정합니다.

      - 감사 금지
      - 성공 이벤트만 감사합니다
      - 장애 이벤트 감사
      - Local Policies/Audit Policy GPO의 Audit object access 설정을 이용하여 성공 이벤트와 실패 이벤트를 모두 Audit한다.

        > 세 가지 감사 옵션 중 하나를 설정하면(성공 이벤트만 감사, 실패 이벤트만 감사, 성공 및 실패 이벤트 모두 감사) ONTAP는 성공 및 실패 이벤트를 모두 감사합니다.

- 로그 보존 방법입니다

  다음 설정을 포함하여 감사 로그 보존 방법을 지정합니다.

  - 로그 파일의 크기가 최대 로그 크기를 초과할 경우 이벤트 로그를 덮어씁니다
  - 이벤트 로그 GPO의 보안 로그 보관 방법 설정을 사용하여 이벤트 로그(수동으로 로그 지우기) 집합을 덮어쓰지 마십시오.

- 최대 로그 크기입니다

  감사 로그의 최대 크기를 지정합니다.

  이벤트 로그 GPO에서 최대 보안 로그 크기 설정을 사용하여 설정합니다.

  감사 정책 및 이벤트 로그 GPO 설정을 사용하려면 이 설정을 적용할 CIFS 지원 SVM에 감사를 구성해야 합니다. SVM에서 감사를 구성하지 않으면 GPO 설정이 적용되지 않고 삭제됩니다.

◦ 파일 시스템 보안

GPO를 통해 파일 보안을 적용할 파일 또는 디렉터리 목록을 지정합니다.

파일 시스템 GPO를 사용하여 설정합니다.

파일 시스템 보안 GPO를 구성하는 볼륨 경로가 SVM 내에 있어야 합니다.

◦ Kerberos 정책

- 최대 클럭 불균형

  컴퓨터 시계 동기화에 대한 최대 허용 시간(분)을 지정합니다.

  계정 정책/Kerberos 정책 GPO에서 컴퓨터 시계 동기화에 대한 최대 허용 한도를 사용하여 설정합니다.

- 최대 항공권 사용 기간

  사용자 티켓의 최대 수명(시간)을 지정합니다.

  계정 정책/Kerberos 정책 GPO에서 사용자 티켓의 최대 수명 설정을 사용하여 설정합니다.

- 최대 티켓 갱신 기간

  사용자 티켓 갱신에 대한 최대 수명(일)을 지정합니다.

계정 정책/Kerberos 정책 GPO에서 사용자 티켓 갱신을 위한 최대 수명 설정을 사용하여 설정합니다.

◦ 사용자 권한 할당(권한 권한)

- 소유권 가져오기

  보안 개체의 소유권을 가져올 권한이 있는 사용자 및 그룹 목록을 지정합니다.

  Local Policies/User Rights Assignment GPO에서 파일 또는 기타 개체의 소유권 가져오기 설정을

사용하여 설정합니다.

- 보안 권한

  파일, 폴더 및 Active Directory 개체와 같은 개별 리소스의 개체 액세스에 대한 감사 옵션을 지정할 수 있는 사용자 및 그룹 목록을 지정합니다.

  Local Policies/User Rights Assignment GPO에서 MManage auditing and security log 설정을 이용하여 설정한다.

- 알림 권한 변경(통과 확인 무시)

  사용자 및 그룹에 통과 디렉터리에 대한 권한이 없더라도 디렉터리 트리를 통과할 수 있는 사용자 및 그룹 목록을 지정합니다.

사용자가 파일 및 디렉토리의 변경 알림을 수신하는 경우에도 동일한 권한이 필요합니다. Local Policies/User Rights Assignment GPO에서 통과 확인 무시 설정을 사용하여 설정합니다.

◦ 레지스트리 값

- 서명 필요 설정

  필요한 SMB 서명을 설정 또는 해제할지 여부를 지정합니다.

보안 옵션 GPO의 'Microsoft 네트워크 서버: 디지털 서명 통신(항상)' 설정을 사용하여 설정합니다.

◦ 익명 제한

익명 사용자의 제한 사항을 지정하고 다음 세 가지 GPO 설정을 포함합니다.

- SAM(보안 계정 관리자) 계정의 열거 없음:

  이 보안 설정은 컴퓨터에 대한 익명 연결에 대해 부여되는 추가 권한을 결정합니다. 이 옵션이 활성화된 경우 ONTAP에서 "no-enumeration"으로 표시됩니다.

  Local Policies/Security Options GPO에서 Network access: do not allow anonymous enumeration of SAM accounts(SAM 계정의 익명 열거 허용 안 함) 설정을 사용하여 설정합니다.

- SAM 계정 및 공유의 열거 없음

  이 보안 설정은 SAM 계정과 공유의 익명 열거가 허용되는지 여부를 결정합니다. 이 옵션이 활성화된 경우 ONTAP에서 "no-enumeration"으로 표시됩니다.

  Local Policies/Security Options GPO에서 Network access: do not allow anonymous enumeration of SAM accounts and 공유 설정을 이용하여 설정한다.

- 공유 및 명명된 파이프에 대한 익명 액세스를 제한합니다

  이 보안 설정은 공유 및 파이프에 대한 익명 액세스를 제한합니다. 이 옵션이 활성화된 경우 ONTAP에서 이 옵션이 "no-access"로 표시됩니다.

  Local Policies/Security Options GPO에서 Network access: restrict anonymous access to named pipes and Shares 설정을 이용하여 설정한다.

정의된 그룹 정책과 적용된 그룹 정책에 대한 정보를 표시할 때 "익명 사용자에 대한 결과 제한" 출력 필드는 세 가지 익명 GPO 제한 설정의 결과 제한에 대한 정보를 제공합니다. 가능한 결과 제한은 다음과 같습니다.

- "접근 불가"

  익명 사용자는 지정된 공유 및 명명된 파이프에 대한 액세스가 거부되며 SAM 계정과 공유의 열거를 사용할 수 없습니다. 네트워크 액세스: 명명된 파이프 및 공유에 대한 익명 액세스 제한 GPO가 설정된 경우 이러한 제한이 나타납니다.

- 번호 매기기

  익명 사용자는 지정된 공유 및 명명된 파이프에 액세스할 수 있지만 SAM 계정과 공유의 열거를 사용할 수는 없습니다. 이 결과 제한은 다음 두 조건이 모두 충족되는 경우에 나타납니다.

  - 네트워크 액세스 : 명명된 파이프와 공유에 대한 익명 액세스 제한 GPO가 비활성화됩니다.
  - Network access: do not allow anonymous enumeration of SAM accounts(SAM 계정의 익명 열거 허용 안 함) 또는 Network access: do not allow anonymous enumeration of SAM accounts and 공유 GPO(SAM 계정과 공유의 익명 열거 허용 안 함) 중 하나가 활성화됩니다.

- 무제한입니다

  익명 사용자는 모든 액세스 권한이 있으며 열거형을 사용할 수 있습니다. 이 결과 제한은 다음 두 조건이 모두 충족되는 경우에 나타납니다.

  - 네트워크 액세스 : 명명된 파이프와 공유에 대한 익명 액세스 제한 GPO가 비활성화됩니다.
  - Network access: do not allow anonymous enumeration of SAM accounts(SAM 계정의 익명 열거 허용 안 함) 및 Network access: do not allow anonymous enumeration of SAM accounts and ses(SAM 계정과 공유의 익명 열거 허용 안 함) GPO가 모두 비활성화됩니다.
    - 제한된 그룹

      제한된 그룹을 구성하여 기본 제공 그룹 또는 사용자 정의 그룹의 구성원을 중앙에서 관리할 수 있습니다. 그룹 정책을 통해 제한된 그룹을 적용하면 CIFS 서버 로컬 그룹의 구성원은 적용된 그룹 정책에 정의된 멤버 자격 목록 설정과 일치하도록 자동으로 설정됩니다.

  제한 그룹 GPO를 사용하여 설정합니다.

- 중앙 액세스 정책 설정

  중앙 액세스 정책 목록을 지정합니다. 중앙 액세스 정책과 관련 중앙 액세스 정책 규칙에 따라 SVM의 여러 파일에 대한 액세스 권한이 결정됩니다.

관련 정보

- 서버에서 GPO 지원 활성화 또는 비활성화
- 서버의 파일 액세스 보안에 대해 알아보세요
- "SMB 및 NFS 감사 및 보안 추적"
- 서버 보안 설정 수정
- 지점 사무실에서 공유 콘텐츠를 캐시하기 위해 BranchCache를 사용하는 방법에 대해 알아보세요.
- ONTAP 서명을 사용하여 네트워크 보안을 강화하는 방법에 대해 알아보세요.

- 바이패스 트래버스 검사 구성에 대해 알아보세요
- 익명 사용자의 액세스 제한을 구성합니다

GPO에 대한 **ONTAP SMB** 서버 요구 사항

SMB 서버에서 GPO(그룹 정책 개체)를 사용하려면 시스템이 여러 요구 사항을 충족해야 합니다.

- SMB는 클러스터에서 라이센스가 있어야 합니다. SMB 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오 "있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.
- SMB 서버는 Windows Active Directory 도메인에 구성 및 가입해야 합니다.
- SMB 서버 관리자 상태는 켜져야 합니다.
- GPO를 구성하고 SMB 서버 컴퓨터 개체가 포함된 Windows Active Directory OU(조직 단위)에 적용해야 합니다.
- SMB 서버에서 GPO 지원을 활성화해야 합니다.

ONTAP SMB 서버에서 **GPO** 지원을 설정하거나 해제합니다

CIFS 서버에서 GPO(그룹 정책 개체) 지원을 설정하거나 해제할 수 있습니다. CIFS 서버에서 GPO 지원을 설정하면 CIFS 서버 컴퓨터 개체가 포함된 OU(조직 구성 단위)에 적용되는 그룹 정책에 정의된 적용 가능한 GPO가 CIFS 서버에 적용됩니다.

이 작업에 대해

워크그룹 모드에서는 CIFS 서버에서 GPO를 설정할 수 없습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
GPO를 활성화합니다	'vserver cifs group-policy modify -vserver_vserver_name_-status enabled'
GPO를 비활성화합니다	'vserver cifs group-policy modify -vserver_vserver_name_-status disabled'

2. GPO 지원이 'vserver cifs group-policy show-vserver+vserver_name_'(SVM CIFS 그룹 정책 표시) 상태로 설정되어 있는지 확인합니다

   워크그룹 모드의 CIFS 서버에 대한 그룹 정책 상태는 "사용 안 함"으로 표시됩니다.

예

다음 예에서는 SVM(Storage Virtual Machine) VS1 에 대한 GPO 지원을 설정합니다.

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

관련 정보

지원되는 GPO에 대해 알아보세요

GPO에 대한 서버 요구 사항

SMB 서버에서 GPO 업데이트에 대해 알아보세요

SMB 서버에서 GPO 설정을 수동으로 업데이트합니다.

GPO 구성에 대한 정보를 표시합니다

SMB 서버에서 GPO를 업데이트하는 방법

ONTAP SMB 서버에서 **GPO**를 업데이트하는 방법에 대해 알아봅니다

기본적으로 ONTAP는 90분마다 GPO(그룹 정책 개체) 변경 내용을 검색하고 적용합니다. 보안 설정은 16시간마다 새로 고쳐집니다. ONTAP에서 GPO를 자동으로 업데이트하기 전에 GPO를 업데이트하여 새 GPO 정책 설정을 적용하려면 ONTAP 명령을 사용하여 CIFS 서버에서 수동 업데이트를 트리거하면 됩니다.

- 기본적으로 모든 GPO는 90분마다 확인 및 업데이트됩니다.

  이 간격은 구성 가능하며 '새로 고침 간격' 및 '임의 오프셋' GPO 설정을 사용하여 설정할 수 있습니다.

  ONTAP는 Active Directory에 GPO 변경 사항을 쿼리합니다. Active Directory에 기록된 GPO 버전 번호가 CIFS 서버의 GPO 버전 번호보다 높을 경우 ONTAP는 새 GPO를 검색하고 적용합니다. 버전 번호가 같으면 CIFS 서버의 GPO가 업데이트되지 않습니다.

- 보안 설정 GPO는 16시간마다 새로 고쳐집니다.

  ONTAP는 이러한 GPO의 변경 여부에 관계없이 보안 설정 GPO를 16시간마다 검색하고 적용합니다.

  > ⓘ 현재 ONTAP 버전에서는 16시간 기본값을 변경할 수 없습니다. Windows 클라이언트 기본 설정입니다.

- 모든 GPO는 ONTAP 명령을 사용하여 수동으로 업데이트할 수 있습니다.

  이 명령은 Windows 'gpupdate.exe' /force' 명령을 시뮬레이션합니다.

관련 정보

SMB 서버에서 GPO 설정을 수동으로 업데이트합니다.

ONTAP SMB 서버에서 **GPO** 설정을 수동으로 업데이트합니다

CIFS 서버에서 GPO(그룹 정책 개체) 설정을 즉시 업데이트하려면 설정을 수동으로 업데이트할 수 있습니다. 변경된 설정만 업데이트하거나 이전에 적용되었지만 변경되지 않은 설정을 포함하여 모든 설정에 대해 업데이트를 적용할 수 있습니다.

단계

1. 적절한 작업을 수행합니다.

업데이트하려면...	명령 입력...
GPO 설정이 변경되었습니다	'vserver cifs group-policy update-vserver_vserver_name_'
모든 GPO 설정	'vserver cifs group-policy update-vserver_vserver_name_-force-re애플리케이션-all -settings true'

관련 정보

SMB 서버에서 GPO 업데이트에 대해 알아보세요

ONTAP SMB GPO 구성에 대한 정보를 표시합니다

Active Directory에 정의된 GPO(그룹 정책 개체) 구성과 CIFS 서버에 적용된 GPO 구성에 대한 정보를 표시할 수 있습니다.

이 작업에 대해

CIFS 서버가 속한 도메인의 Active Directory에 정의된 모든 GPO 구성에 대한 정보를 표시하거나 CIFS 서버에 적용된 GPO 구성에 대한 정보만 표시할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행하여 GPO 구성에 대한 정보를 표시합니다.

모든 그룹 정책 구성에 대한 정보를 표시하려면...	명령 입력...
Active Directory에 정의되어 있습니다	'vserver cifs group-policy show-defined-vserver vserver_name'
CIFS 지원 스토리지 가상 시스템(SVM)에 적용	'vserver cifs group-policy show-applied-vserver vserver_name'

예

다음 예에서는 VS1 이라는 CIFS 지원 SVM이 속한 Active Directory에 정의된 GPO 구성을 보여 줍니다.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
-----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2

    GPO Name: Resultant Set of Policy
      Status: enabled
```

```
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

다음 예에서는 CIFS 지원 SVM VS1 V1에 적용된 GPO 구성을 보여 줍니다.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
```

```
   GPO Name: Default Domain Policy
     Level: Domain
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
```

```
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

관련 정보

서버에서 GPO 지원 활성화 또는 비활성화

ONTAP SMB의 제한된 그룹 **GPO**에 대한 정보를 표시합니다

Active Directory에서 GPO(그룹 정책 개체)로 정의되고 CIFS 서버에 적용되는 제한된 그룹에 대한 자세한 정보를 표시할 수 있습니다.

이 작업에 대해

기본적으로 다음 정보가 표시됩니다.

- 그룹 정책 이름입니다
- 그룹 정책 버전입니다
- 링크

  그룹 정책이 구성되는 수준을 지정합니다. 가능한 출력 값은 다음과 같습니다.

  - ONTAP에서 그룹 정책이 구성되면 Local이 됩니다
  - 도메인 컨트롤러의 사이트 수준에서 그룹 정책이 구성되면 '사이트'입니다
  - 도메인 컨트롤러의 도메인 수준에서 그룹 정책이 구성되면 "domain"입니다
  - 조직 단위(OrganizationalUnit) - 도메인 컨트롤러의 조직 단위(OU) 수준에서 그룹 정책이 구성된 경우
  - 다양한 수준에서 정의된 모든 그룹 정책에서 파생된 정책의 결과 집합에 대한 RSoP
- 제한된 그룹 이름입니다
- 제한된 그룹에 속하고 속하지 않는 사용자 및 그룹
- 제한된 그룹이 추가되는 그룹의 목록입니다

  그룹은 여기에 나열된 그룹 이외의 그룹의 구성원이 될 수 있습니다.

단계

1. 다음 작업 중 하나를 수행하여 모든 제한된 그룹 GPO에 대한 정보를 표시합니다.

모든 제한된 그룹 **GPO**에 대한 정보를 표시하려면…	명령 입력…
Active Directory에 정의되어 있습니다	'vserver cifs group-policy restricted-group show-defined-vserver vserver_name'
CIFS 서버에 적용됩니다	'vserver cifs group-policy restricted-group show-applied-vserver vserver_name'

예

다음 예에서는 VS1 이라는 CIFS 지원 SVM이 속한 Active Directory 도메인에 정의된 제한된 그룹 GPO에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9
```

다음 예에서는 CIFS 지원 SVM VS1 에 적용된 제한된 그룹 GPO에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9
```

관련 정보

GPO 구성에 대한 정보를 표시합니다

Active Directory에 정의된 중앙 액세스 정책에 대한 자세한 정보를 표시할 수 있습니다. GPO(그룹 정책 개체)를 통해 CIFS 서버에 적용되는 중앙 액세스 정책에 대한 정보를 표시할 수도 있습니다.

이 작업에 대해

기본적으로 다음 정보가 표시됩니다.

- SVM 이름
- 중앙 액세스 정책의 이름입니다
- SID
- 설명
- 생성 시간
- 수정 시간
- 구성원 규칙

CIFS 서버는 GPO를 지원하지 않으므로 워크그룹 모드의 CIFS 서버는 표시되지 않습니다.

단계

1. 다음 작업 중 하나를 수행하여 중앙 액세스 정책에 대한 정보를 표시합니다.

모든 중앙 액세스 정책에 대한 정보를 표시하려면...	명령 입력...
Active Directory에 정의되어 있습니다	'vserver cifs group-policy central-access-policy show-defined-vserver_vserver_name_'
CIFS 서버에 적용됩니다	'vserver cifs group-policy central-access-policy show-applied-vserver_vserver_name_'

예

다음 예에서는 Active Directory에 정의된 모든 중앙 액세스 정책에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
-----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

다음 예에서는 클러스터의 SVM(스토리지 가상 머신)에 적용되는 모든 중앙 액세스 정책에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                   SID
-------- --------------------
-----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

관련 정보

- 서버의 파일 액세스 보안에 대해 알아보세요

- GPO 구성에 대한 정보를 표시합니다
- 중앙 액세스 정책 규칙에 대한 정보를 표시합니다

ONTAP SMB 중앙 액세스 정책 규칙에 대한 정보를 표시합니다

Active Directory에 정의된 중앙 액세스 정책과 연결된 중앙 액세스 정책 규칙에 대한 자세한 정보를 표시할 수 있습니다. 중앙 액세스 정책 GPO(그룹 정책 개체)를 통해 CIFS 서버에 적용되는 중앙 액세스 정책 규칙에 대한 정보를 표시할 수도 있습니다.

이 작업에 대해

정의되고 적용된 중앙 액세스 정책 규칙에 대한 자세한 정보를 표시할 수 있습니다. 기본적으로 다음 정보가 표시됩니다.

- SVM 이름
- 중앙 액세스 규칙의 이름입니다
- 설명
- 생성 시간
- 수정 시간
- 현재 권한
- 제안된 권한
- 타겟 리소스

중앙 액세스 정책과 관련된 모든 중앙 액세스 정책 규칙에 대한 정보를 표시하려면...	명령 입력...
Active Directory에 정의되어 있습니다	'vserver cifs group-policy central-access-rule show-defined-vserver vserver_name'
CIFS 서버에 적용됩니다	'vserver cifs group-policy central-access-rule show-applied-vserver vserver_name'

예

다음 예에서는 Active Directory에 정의된 중앙 액세스 정책과 관련된 모든 중앙 액세스 정책 규칙에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver     Name
----------- --------------------
vs1         r1
            Description: rule #1
          Creation Time: Tue Oct 22 09:33:48 2013
      Modification Time: Tue Oct 22 09:33:48 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
            Description: rule #2
          Creation Time: Tue Oct 22 10:27:57 2013
      Modification Time: Tue Oct 22 10:27:57 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

다음 예에서는 클러스터의 SVM(스토리지 가상 머신)에 적용되는 중앙 액세스 정책과 연결된 모든 중앙 액세스 정책 규칙에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver     Name
----------- --------------------
vs1         r1
            Description: rule #1
          Creation Time: Tue Oct 22 09:33:48 2013
      Modification Time: Tue Oct 22 09:33:48 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
            Description: rule #2
          Creation Time: Tue Oct 22 10:27:57 2013
      Modification Time: Tue Oct 22 10:27:57 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

관련 정보

- 서버의 파일 액세스 보안에 대해 알아보세요
- GPO 구성에 대한 정보를 표시합니다
- 중앙 액세스 정책에 대한 정보를 표시합니다

SMB 서버 컴퓨터 계정 암호를 관리하기 위한 **ONTAP** 명령입니다

암호를 변경, 재설정 및 비활성화하고 자동 업데이트 일정을 구성하기 위한 명령을 알아야 합니다. SMB 서버에서 자동으로 업데이트되도록 스케줄을 구성할 수도 있습니다.

원하는 작업	이 명령 사용...
ONTAP가 AD 서비스와 동기화될 때 도메인 계정 암호를 변경합니다	'vserver cifs domain password change'를 선택합니다
ONTAP가 AD 서비스와 동기화되지 않은 경우 도메인 계정 암호를 다시 설정합니다	'vserver cifs domain password reset'
자동 컴퓨터 계정 암호 변경을 위해 SMB 서버를 구성합니다	'vserver cifs domain password schedule modify -vserver vserver_name -is-schedule -enabled true'
SMB 서버에서 자동 컴퓨터 계정 암호 변경을 비활성화합니다	'vserver cifs domain password schedule modify -vserver vs1-is-schedule -enabled false'

에 대한 자세한 내용은 `vserver cifs domain password` "ONTAP 명령 참조입니다"을 참조하십시오.

도메인 컨트롤러 연결을 관리합니다

ONTAP SMB에서 검색된 서버에 대한 정보를 표시합니다

CIFS 서버에서 검색된 LDAP 서버 및 도메인 컨트롤러와 관련된 정보를 표시할 수 있습니다.

단계

1. 검색된 서버와 관련된 정보를 표시하려면 'vserver cifs domain discovered-servers show' 명령을 입력합니다

예

다음 예에서는 SVM VS1 에서 검색된 서버를 보여 줍니다.

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address     Status
--------------- -------- ---------- ----------- -------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4        OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5        OK
example.com     MS-DC    adequate   DC-1        1.1.3.4        OK
example.com     MS-DC    adequate   DC-2        1.1.3.5        OK
```

관련 정보

- 서버를 재설정하고 재검색합니다
- 서버 중지 또는 시작

ONTAP SMB 서버를 재설정하고 재검색합니다

CIFS 서버에서 서버를 재설정하고 재검색하면 CIFS 서버가 LDAP 서버 및 도메인 컨트롤러에 대한 저장된 정보를 삭제할 수 있습니다. 서버 정보를 폐기한 후 CIFS 서버는 이러한 외부 서버에 대한 현재 정보를 다시 가져옵니다. 이 기능은 연결된 서버가 적절하게 응답하지 않는 경우에 유용할 수 있습니다.

단계

1. 'vserver cifs domain discovered - servers reset -servers -vserver_vserver_name_' 명령을 입력합니다
2. 새로 재검색된 서버에 대한 정보를 표시합니다. 'vserver cifs domain discovered-servers show -vserver_vserver_name_'

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver)의 VS1 용 서버를 재설정하고 다시 검색합니다.

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

관련 정보

- 검색된 서버에 대한 정보를 표시합니다
- 서버 중지 또는 시작

ONTAP SMB 도메인 컨트롤러 검색을 관리합니다

ONTAP 9.3부터는 DC(도메인 컨트롤러)가 검색되는 기본 프로세스를 수정할 수 있습니다. 이렇게 하면 사이트 또는 기본 DC 풀로 검색을 제한할 수 있으며, 이는 환경에 따라 성능 개선을 초래할 수 있습니다.

이 작업에 대해

기본적으로 동적 검색 프로세스는 기본 DC, 로컬 사이트의 모든 DC 및 모든 원격 DC를 포함하여 사용 가능한 모든

DC를 검색합니다. 이 구성을 사용하면 특정 환경에서 인증 및 공유 액세스에 지연 시간이 발생할 수 있습니다. 사용하려는 DC 풀을 이미 결정했거나 원격 DC가 부적절하거나 액세스할 수 없는 경우 검색 방법을 변경할 수 있습니다.

ONTAP 9.3 이상 릴리즈에서는 "cifs domain discovered-servers" 명령의 discovery-mode 매개 변수를 사용하여 다음 검색 옵션 중 하나를 선택할 수 있습니다.

- 도메인의 모든 DC가 검색됩니다.
- 로컬 사이트의 DC만 검색됩니다.

  를 클릭합니다 `default-site` 사이트 및 서비스의 사이트에 할당되지 않은 LIF와 함께 이 모드를 사용하도록 SMB 서버에 대한 매개 변수를 정의할 수 있습니다.

- 서버 검색은 수행되지 않으며, SMB 서버 구성은 기본 DC에만 의존합니다.

  이 모드를 사용하려면 먼저 SMB 서버의 기본 DC를 정의해야 합니다.

시작하기 전에

advanced 권한 수준이어야 합니다.

단계

1. 원하는 검색 옵션을 지정합니다. 'vserver cifs domain discovered-servers discovery-mode modify -vserver_vserver_name_-mode{all|site|none}'

   '모드' 파라미터 옵션:

   - 모두

     사용 가능한 모든 DC를 검색합니다(기본값).

   - '사이트'입니다

     사이트에 대한 DC 검색을 제한합니다.

   - "없음"

     검색을 수행하지 않고 기본 DC만 사용하십시오.

기본 **ONTAP SMB** 도메인 컨트롤러를 추가합니다

ONTAP는 DNS를 통해 도메인 컨트롤러를 자동으로 검색합니다. 필요에 따라 특정 도메인의 기본 도메인 컨트롤러 목록에 하나 이상의 도메인 컨트롤러를 추가할 수 있습니다.

이 작업에 대해

지정된 도메인에 대한 기본 도메인 컨트롤러 목록이 이미 있는 경우 새 목록이 기존 목록과 병합됩니다.

단계

1. 기본 도메인 컨트롤러 목록에 추가하려면 + "vserver cifs domain preferred-dc add-vserver_vserver_name_-domain_domain_name_-preferred-dc ip_address,…+" 명령을 입력합니다

   '-vserver_vserver_name_'은 SVM(Storage Virtual Machine) 이름을 지정합니다.

'-domain_domain_name_'은 지정된 도메인 컨트롤러가 속한 도메인의 정규화된 Active Directory 이름을 지정합니다.

'-preferred-dc_ip_address_',… 기본 설정 도메인 컨트롤러의 IP 주소를 쉼표로 구분된 목록으로 지정합니다.

예

다음 명령을 실행하면 cifs.lab.example.com 도메인에 대한 외부 액세스를 관리하기 위해 SVM VS1의 SMB 서버가 사용하는 기본 도메인 컨트롤러 목록에 도메인 컨트롤러 172.17.102.25 및 172.17.102.24가 추가됩니다.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

관련 정보

기본 도메인 컨트롤러를 관리하는 명령입니다

기본 **SMB** 도메인 컨트롤러를 관리하기 위한 **ONTAP** 명령입니다

기본 도메인 컨트롤러를 추가, 표시 및 제거하는 명령을 알아야 합니다.

원하는 작업	이 명령 사용...
기본 도메인 컨트롤러를 추가합니다	'vserver cifs domain preferred-dc add'
기본 도메인 컨트롤러를 표시합니다	'vserver cifs domain preferred-dc show'
기본 도메인 컨트롤러를 제거합니다	'vserver cifs domain preferred-dc remove'

에 대한 자세한 내용은 `vserver cifs domain preferred-dc` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

기본 도메인 컨트롤러를 추가합니다

ONTAP SMB 도메인 컨트롤러에 대한 암호화된 연결을 활성화합니다

ONTAP 9.8부터 도메인 컨트롤러에 대한 연결이 암호화되도록 지정할 수 있습니다.

이 작업에 대해

ONTAP는 `-encryption-required-for-dc-connection' 옵션이 true로 설정되어 있을 때 도메인 컨트롤러(DC) 통신을 암호화해야 하며 기본값은 false입니다. SMB3에서만 암호화가 지원되므로 이 옵션을 설정하면 SMB3 프로토콜만 ONTAP-DC 연결에 사용됩니다.

암호화된 DC 통신이 필요한 경우 ONTAP는 SMB3 연결만 협상하므로 '-SMB2-enabled-for-DC-connections' 옵션이 무시됩니다. DC가 SMB3 및 암호화를 지원하지 않는 경우 ONTAP가 이를 통해 연결되지 않습니다.

단계

1. DC와의 암호화된 통신을 활성화합니다. 'vserver cifs security modify -vserver_svm_name_-encryption -required-for-dc-connection true'

null 세션을 사용하여 Kerberos가 아닌 환경의 스토리지에 액세스합니다

ONTAP SMB null 세션을 사용하여 Kerberos가 아닌 환경의 스토리지에 액세스합니다

null 세션 액세스는 스토리지 시스템 데이터와 같은 네트워크 리소스 및 로컬 시스템에서 실행되는 클라이언트 기반 서비스에 대한 권한을 제공합니다. 클라이언트 프로세스가 "시스템" 계정을 사용하여 네트워크 리소스에 액세스할 때 Null 세션이 발생합니다. Null 세션 구성은 비 Kerberos 인증에만 적용됩니다.

ONTAP SMB 스토리지 시스템이 null 세션 액세스를 제공하는 방법에 대해 알아보십시오

null 세션 공유는 인증이 필요하지 않으므로 null 세션 액세스가 필요한 클라이언트의 IP 주소가 스토리지 시스템에 매핑되어야 합니다.

기본적으로 매핑되지 않은 null 세션 클라이언트는 공유 열거형과 같은 특정 ONTAP 시스템 서비스에 액세스할 수 있지만 스토리지 시스템 데이터에 액세스하지 못하도록 제한됩니다.

> ONTAP에서는 옵션을 사용하여 Windows RestrictAnonymous 레지스트리 설정 값을 `-restrict-anonymous` 지원합니다. 이렇게 하면 매핑되지 않은 null 사용자가 시스템 리소스를 보거나 액세스할 수 있는 범위를 제어할 수 있습니다. 예를 들어 공유 열거를 사용하지 않도록 설정하고 IPC$ 공유(숨겨진 명명된 파이프 공유)에 액세스할 수 있습니다. 및 `vserver cifs options show -restrict-anonymous` 의 옵션에 대해 자세히 `vserver cifs options modify`"ONTAP 명령 참조입니다" 알아봅니다.

달리 구성하지 않는 한 null 세션을 통해 스토리지 시스템 액세스를 요청하는 로컬 프로세스를 실행하는 클라이언트는 ""Everyone""과 같은 제한적이지 않은 그룹의 구성원입니다. 선택한 스토리지 시스템 리소스에 대해 null 세션 액세스를 제한하려면 모든 null 세션 클라이언트가 속한 그룹을 생성해야 합니다. 이 그룹을 생성하면 스토리지 시스템 액세스를 제한하고 null 세션 클라이언트에 적용되는 스토리지 시스템 리소스 권한을 설정할 수 있습니다.

ONTAP는 'vserver name-mapping' 명령 세트에서 null 사용자 세션을 사용하여 스토리지 시스템 리소스에 액세스할 수 있는 클라이언트의 IP 주소를 지정하는 매핑 구문을 제공합니다. Null 사용자에 대한 그룹을 생성한 후에는 null 세션에만 적용되는 스토리지 시스템 리소스 및 리소스 권한에 대한 액세스 제한을 지정할 수 있습니다. Null 사용자는 익명 로그온으로 식별됩니다. Null 사용자는 홈 디렉토리에 액세스할 수 없습니다.

매핑된 IP 주소에서 스토리지 시스템을 액세스하는 모든 null 사용자에게 매핑된 사용자 권한이 부여됩니다. null 사용자로 매핑된 스토리지 시스템에 대한 무단 액세스를 방지하려면 적절한 예방 조치를 고려하십시오. 최대한의 보호를 위해, IP 주소 "스포크"의 가능성을 제거하기 위해, 별도의 네트워크에 null 사용자 스토리지 시스템 액세스를 필요로 하는 모든 클라이언트와 스토리지 시스템을 배치하십시오.

관련 정보

익명 사용자의 액세스 제한을 구성합니다

ONTAP SMB 파일 시스템 공유에 null 사용자에게 액세스 권한을 부여합니다

null 세션 클라이언트가 사용할 그룹을 할당하고 null 세션 클라이언트의 IP 주소를 기록하여 null 세션을 사용하여 데이터를 액세스할 수 있는 스토리지 시스템의 클라이언트 목록에 추가하는 방식으로 null 세션 클라이언트를 통해 스토리지 시스템 리소스에 대한 액세스를 허용할 수 있습니다.

단계

1. "vserver name-mapping create" 명령을 사용하여 Null 사용자를 IP 한정자를 사용하여 유효한 Windows 사용자에게 매핑합니다.

   다음 명령을 실행하면 유효한 호스트 이름이 google.com 인 user1에 null 사용자가 매핑됩니다.

   ```
   vserver name-mapping create -direction win-unix  -position 1 -pattern
   "ANONYMOUS LOGON" -replacement user1 - hostname google.com
   ```

   다음 명령을 실행하면 유효한 IP 주소가 10.238.2.54/32인 user1에 null 사용자가 매핑됩니다.

   ```
   vserver name-mapping create -direction win-unix  -position 2 -pattern
   "ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
   ```

2. 이름 매핑을 확인하려면 'vserver name-mapping show' 명령을 사용하십시오.

   ```
   vserver name-mapping show

   Vserver:   vs1
   Direction: win-unix
   Position Hostname         IP Address/Mask
   -------- --------         ----------------
   1        -                10.72.40.83/32      Pattern: anonymous logon
                                              Replacement: user1
   ```

3. "vserver cifs options modify –win-name -for-null-user" 명령을 사용하여 null 사용자에게 Windows 구성원을 할당합니다.

   이 옵션은 Null 사용자에 대해 유효한 이름 매핑이 있는 경우에만 적용할 수 있습니다.

   ```
   vserver cifs options modify -win-name-for-null-user user1
   ```

4. "vserver cifs options show" 명령을 사용하여 null 사용자가 Windows 사용자 또는 그룹에 매핑되었는지 확인합니다.

   ```
   vserver cifs options show

   Vserver :vs1

   Map Null User to Windows User of Group: user1
   ```

SMB 서버의 NetBIOS 별칭을 관리합니다

ONTAP SMB 서버의 NetBIOS 별칭 관리에 대해 자세히 알아보십시오

NetBIOS 별칭은 SMB 클라이언트가 SMB 서버에 연결할 때 사용할 수 있는 SMB 서버의 대체 이름입니다. SMB 서버에 대한 NetBIOS 별칭을 구성하면 다른 파일 서버의 데이터를 SMB 서버로 통합할 때 SMB 서버가 원래 파일 서버의 이름에 응답하도록 할 때 유용할 수 있습니다.

SMB 서버를 생성할 때 또는 SMB 서버를 생성한 후 언제든지 NetBIOS 별칭 목록을 지정할 수 있습니다. 목록에서 NetBIOS 별칭을 언제든지 추가하거나 제거할 수 있습니다. NetBIOS 별칭 목록에 있는 이름을 사용하여 SMB 서버에 연결할 수 있습니다.

관련 정보

NetBIOS over TCP 연결에 대한 정보를 표시합니다

ONTAP SMB 서버에 NetBIOS 별칭 목록을 추가합니다

SMB 클라이언트가 별칭을 사용하여 SMB 서버에 접속하도록 하려면 NetBIOS 별칭 목록을 만들거나 NetBIOS 별칭의 기존 목록에 NetBIOS 별칭을 추가할 수 있습니다.

이 작업에 대해

- NetBIOS 별칭 이름은 최대 15자까지 지정할 수 있습니다.
- SMB 서버에서 최대 200개의 NetBIOS 별칭을 구성할 수 있습니다.
- 다음 문자는 허용되지 않습니다.

  @# * ()=+[]|;:",<>\/?

단계

1. NetBIOS 별칭: + 'vserver cifs add-netbios-alias-vserver_vserver_name_-NetBIOS-alias_netbios_alias_,… '를 추가합니다

   'vserver cifs add-netbios-alias-vserver vs1-netbios-alias alias_1, alias_2, alias_3'

   - 쉼표로 구분된 목록을 사용하여 하나 이상의 NetBIOS 별칭을 지정할 수 있습니다.
   - 지정된 NetBIOS 별칭이 기존 목록에 추가됩니다.
   - 목록이 현재 비어 있는 경우 새 NetBIOS 별칭 목록이 생성됩니다.
2. NetBIOS 별칭이 올바르게 추가되었는지 확인합니다. 'vserver cifs show -vserver vserver_name -display -netbios -aliases'

   'vserver cifs show-vserver vs1-display-netbios-aliases'

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

관련 정보

- SMB 서버 목록에서 NetBIOS 별칭 제거
- SMB 서버에 대한 NetBIOS 별칭 목록 표시

ONTAP SMB 서버 목록에서 **NetBIOS** 별칭을 제거합니다

CIFS 서버에 대한 특정 NetBIOS 별칭이 필요하지 않은 경우 목록에서 해당 NetBIOS 별칭을 제거할 수 있습니다. 목록에서 모든 NetBIOS 별칭을 제거할 수도 있습니다.

이 작업에 대해

쉼표로 구분된 목록을 사용하여 둘 이상의 NetBIOS 별칭을 제거할 수 있습니다. '-NetBIOS-aliases' 매개 변수의 값으로 '-'를 지정하여 CIFS 서버에서 모든 NetBIOS 별칭을 제거할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

을(를) 제거하려면...	입력...
목록에서 특정 NetBIOS 별칭	'vserver cifs remove-netbios-alias-vserver_name_-netbios-alias_netbios_alias_,...'
목록에서 모든 NetBIOS 별칭	'vserver cifs remove-netbios-aliases-vserver_vserver_name_-netbios-aliases-'

'vserver cifs remove-netbios-alias-vserver vs1-netbios-alias_1'

2. 지정된 NetBIOS 별칭이 제거되었는지 확인합니다. 'vserver cifs show -vserver_vserver_name_-display -netbios-aliases'

'vserver cifs show-vserver vs1-display-netbios-aliases'

```
Vserver: vs1

          Server Name: CIFS_SERVER
          NetBIOS Aliases: ALIAS_2, ALIAS_3
```

ONTAP SMB 서버에 대한 **NetBIOS** 별칭 목록을 표시합니다

NetBIOS 별칭 목록을 표시할 수 있습니다. 이 기능은 SMB 클라이언트가 CIFS 서버에 접속할 수 있는 이름 목록을 확인하려는 경우에 유용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

다음에 대한 정보를 표시하려면...	입력...
CIFS 서버의 NetBIOS 별칭입니다	'vserver cifs show-display-netbios-aliases'
자세한 CIFS 서버 정보의 일부로 NetBIOS 별칭 목록입니다	'vserver cifs show-instance'

다음 예에서는 CIFS 서버의 NetBIOS 별칭에 대한 정보를 표시합니다.

'vserver cifs show-display-netbios-aliases'

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

다음 예에서는 자세한 CIFS 서버 정보의 일부로 NetBIOS 별칭 목록을 표시합니다.

'vserver cifs show-instance'

```
                                    Vserver: vs1
                  CIFS Server NetBIOS Name: CIFS_SERVER
                NetBIOS Domain/Workgroup Name: EXAMPLE
                  Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                       Authentication Style: domain
            CIFS Server Administrative Status: up
                      CIFS Server Description:
                      List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

에 대한 자세한 내용은 `vserver cifs show` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- 서버에 NetBIOS 별칭 목록 추가
- 서버 관리를 위한 명령어

ONTAP SMB 클라이언트가 **NetBIOS** 별칭을 사용하여 연결되어 있는지 확인합니다

SMB 클라이언트가 NetBIOS 별칭을 사용하여 연결되어 있는지 여부와 연결된 경우 연결에 사용되는 NetBIOS 별칭을 확인할 수 있습니다. 이 기능은 연결 문제를 해결할 때 유용할 수 있습니다.

이 작업에 대해

SMB 연결에 연결된 NetBIOS 별칭(있는 경우)을 표시하려면 '-instance' 매개 변수를 사용해야 합니다. CIFS 서버 이름 또는 IP 주소를 사용하여 SMB 연결을 수행하는 경우 NetBIOS 이름 필드의 출력은 "-"(하이픈)입니다.

단계

1. 원하는 작업을 수행합니다.

다음에 대한 **NetBIOS** 정보를 표시하려면…	입력…
SMB 연결	'vserver cifs session show-instance'
지정된 NetBIOS 별칭을 사용하는 연결:	'vserver cifs session show-instance-netbios-name_netbios_name_'

다음 예에서는 세션 ID 1과 SMB 연결을 설정하는 데 사용되는 NetBIOS 별칭에 대한 정보를 표시합니다.

'vserver cifs session show-session-id 1-instance'

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
                Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                 Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                 Open Shares: 2
                  Open Files: 2
                  Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

기타 **SMB** 서버 작업을 관리합니다

ONTAP SMB 서버를 중지 또는 시작합니다

사용자가 SMB 공유를 통해 데이터에 액세스하지 않는 상태에서 작업을 수행할 때 유용할 수 있는 SVM에서 CIFS 서버를 중지할 수 있습니다. CIFS 서버를 시작하여 SMB 액세스를 재시작할 수 있습니다. CIFS 서버를 중지하면 스토리지 가상 시스템(SVM)에서 허용되는 프로토콜도 수정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
CIFS 서버를 중지합니다	'vserver cifs stop-vserver_vserver_name_[-foreground{true
false}]'	CIFS 서버를 시작합니다
'vserver cifs start -vserver_vserver_name_[-foreground{true	false}]'

'-foreground'는 포그라운드와 배경에서 명령을 실행할지 여부를 지정합니다. 이 매개 변수를 입력하지 않으면 true로 설정되고 포그라운드에서 명령이 실행됩니다.

2. 'vserver cifs show' 명령을 사용하여 CIFS 서버 관리 상태가 올바른지 확인합니다.

예

다음 명령은 SVM VS1 에서 CIFS 서버를 시작합니다.

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

관련 정보

- 검색된 서버에 대한 정보를 표시합니다
- 서버를 재설정하고 재검색합니다

ONTAP SMB 서버를 다른 **OU**로 이동합니다

CIFS 서버 생성 프로세스는 다른 OU를 지정하지 않는 한 설정 중에 기본 OU(조직 구성 단위) CN=컴퓨터를 사용합니다. 설정 후 CIFS 서버를 다른 OU로 이동할 수 있습니다.

단계

1. Windows 서버에서 * Active Directory 사용자 및 컴퓨터 * 트리를 엽니다.
2. SVM(스토리지 가상 머신)에 대한 Active Directory 개체를 찾습니다.

3. 개체를 마우스 오른쪽 단추로 클릭하고 * 이동 * 을 선택합니다.
4. SVM과 연결할 OU를 선택합니다

결과

SVM 객체가 선택한 OU에 배치됩니다.

ONTAP SMB 서버를 이동하기 전에 동적 **DNS** 도메인을 수정하십시오

SMB 서버를 다른 도메인으로 이동할 때 Active Directory 통합 DNS 서버가 DNS에 SMB 서버의 DNS 레코드를 동적으로 등록하도록 하려면 SMB 서버를 이동하기 전에 SVM(스토리지 가상 시스템)에서 DDNS(동적 DNS)를 수정해야 합니다.

시작하기 전에

SMB 서버 컴퓨터 계정이 포함될 새 도메인의 서비스 위치 레코드가 포함된 DNS 도메인을 사용하려면 SVM에서 DNS 이름 서비스를 수정해야 합니다. 보안 DDNS를 사용하는 경우 Active Directory 통합 DNS 이름 서버를 사용해야 합니다.

이 작업에 대해

DDNS(SVM에서 구성된 경우)는 데이터 LIF의 DNS 레코드를 자동으로 새 도메인에 추가하지만 원래 도메인의 DNS 레코드는 원래 DNS 서버에서 자동으로 삭제되지 않습니다. 수동으로 삭제해야 합니다.

SMB 서버를 이동하기 전에 DDNS 수정을 완료하려면 다음 항목을 참조하십시오.

"동적 DNS 서비스를 구성합니다"

ONTAP SMB SVM을 **Active Directory** 도메인에 가입합니다

"vserver cifs modify" 명령을 사용하여 도메인을 수정하여 기존 SMB 서버를 삭제하지 않고 SVM(스토리지 가상 시스템)을 Active Directory 도메인에 연결할 수 있습니다. 현재 도메인에 다시 참가하거나 새 도메인에 가입할 수 있습니다.

시작하기 전에

- SVM에는 이미 DNS 구성이 있어야 합니다.
- SVM을 위한 DNS 구성은 타겟 도메인을 지원할 수 있어야 합니다.

  DNS 서버에는 도메인 LDAP 및 도메인 컨트롤러 서버에 대한 SRV(서비스 위치 레코드)가 포함되어 있어야 합니다.

이 작업에 대해

- Active Directory 도메인 수정을 계속하려면 CIFS 서버의 관리 상태를 로 설정해야 `down` 합니다.
- 명령이 성공적으로 완료되면 관리 상태가 자동으로 로 `up`설정됩니다. 에 대한 자세한 내용은 `up` "ONTAP 명령 참조입니다"을 참조하십시오.
- 도메인에 가입할 때 이 명령을 완료하는 데 몇 분 정도 걸릴 수 있습니다.

단계

1. SVM을 CIFS 서버 도메인에 가입합니다. 'vserver cifs modify -vserver_vserver_name_ -domain_domain_name_-status -admin down'

에 대한 자세한 내용은 `vserver cifs modify` "ONTAP 명령 참조입니다"을 참조하십시오. 새 도메인에 대해 DNS를 다시 구성해야 하는 경우 에 대한 자세한 `vserver dns modify` 내용은 를 "ONTAP 명령 참조입니다 "참조하십시오.

SMB 서버에 대한 Active Directory 컴퓨터 계정을 만들려면 '*example*'.com 도메인 내의 'ou=_example_ou' 컨테이너에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름과 암호를 제공해야 합니다.

ONTAP 9.7부터 AD 관리자는 권한이 있는 Windows 계정에 이름과 암호를 제공하는 대신 keytab 파일에 대한 URI를 제공할 수 있습니다. URI를 받으면 '-keytab-Uri' 매개 변수에 vserver cifs' 명령을 포함하여 포함시키십시오.

2. CIFS 서버가 원하는 Active Directory 도메인에 있는지 확인합니다. 'vserver cifs show'

예

다음 예에서는 SVM VS1 의 SMB 서버 ""CIFSSERVER1""이 keytab 인증을 사용하여 example.com 도메인에 연결됩니다.

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE           domain
```

TCP 연결을 통한 **ONTAP SMB NetBIOS**에 대한 정보를 표시합니다

NBT(NetBIOS over TCP) 연결에 대한 정보를 표시할 수 있습니다. 이는 NetBIOS 관련 문제를 해결할 때 유용할 수 있습니다.

단계

1. 'vserver cifs nbtstat' 명령을 사용하여 NetBIOS over TCP 연결에 대한 정보를 표시합니다.

IPv6를 통한 NBNS(NetBIOS 이름 서비스)는 지원되지 않습니다.

예

다음 예제에서는 ""cluster1""에 대해 표시되는 NetBIOS 이름 서비스 정보를 보여 줍니다.

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

SMB 서버를 관리하기 위한 **ONTAP** 명령입니다

생성, 표시, 수정, 중지, 시작 명령을 알아야 합니다. 및 SMB 서버 삭제. 또한 서버를 재설정 및 재검색, 컴퓨터 계정 암호 변경 또는 재설정, 컴퓨터 계정 암호 변경 예약, NetBIOS 별칭 추가 또는 제거 등의 명령도 있습니다.

원하는 작업	이 명령 사용…
SMB 서버를 생성합니다	'vserver cifs create
SMB 서버에 대한 정보를 표시합니다	'vserver cifs show'
SMB 서버를 수정합니다	'vserver cifs modify(가상 CIFS 수정)
SMB 서버를 다른 도메인으로 이동합니다	'vserver cifs modify(가상 CIFS 수정)

SMB 서버를 중지합니다	'vserver cifs stop'
SMB 서버를 시작합니다	'vserver cifs start'를 선택합니다
SMB 서버를 삭제합니다	'vserver cifs delete
SMB 서버의 서버를 재설정하고 다시 검색합니다	'vserver cifs domain discovered - servers reset-servers'
SMB 서버의 컴퓨터 계정 암호를 변경합니다	'vserver cifs domain password change'를 선택합니다
SMB 서버의 컴퓨터 계정 암호를 재설정합니다	'vserver cifs domain password change'를 선택합니다
SMB 서버의 컴퓨터 계정에 대한 자동 암호 변경을 예약합니다	'vserver cifs domain password schedule modify'를 참조하십시오
SMB 서버에 대한 NetBIOS 별칭을 추가합니다	'vserver cifs add-netbios-aliases'
SMB 서버의 NetBIOS 별칭을 제거합니다	'vserver cifs remove-netbios-aliases'

에 대한 자세한 내용은 `vserver cifs` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

"SMB 서버를 삭제할 때 로컬 사용자 및 그룹이 어떻게 됩니까"

ONTAP SMB NetBIOS 이름 서비스를 활성화합니다

ONTAP 9부터는 NetBIOS 이름 서비스(NBNS, Windows 인터넷 이름 서비스 또는 WINS라고도 함)가 기본적으로 사용되지 않습니다. 이전에는 CIFS 지원 SVM(스토리지 가상 머신)이 네트워크에서 WINS가 활성화되었는지 여부에 관계없이 이름 등록 브로드캐스트를 전송했습니다. NBNS가 필요한 구성으로 이러한 브로드캐스트를 제한하려면 새 CIFS 서버에 대해 NBNS를 명시적으로 설정해야 합니다.

시작하기 전에

- 이미 NBNS를 사용하고 있으며 ONTAP 9로 업그레이드하는 경우 이 작업을 완료할 필요가 없습니다. NBNS는 이전과 마찬가지로 계속 작동합니다.
- NBNS는 UDP(포트 137)를 통해 활성화됩니다.
- IPv6을 통한 NBNS는 지원되지 않습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. CIFS 서버에서 NBNS를 설정합니다.

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. 관리자 권한 수준으로 돌아갑니다.

```
set -privilege admin
```

SMB 액세스 및 **SMB** 서비스에 **IPv6**를 사용합니다

IPv6에 대한 **ONTAP SMB** 요구 사항에 대해 알아보십시오

SMB 서버에서 IPv6를 사용하려면 먼저 IPv6를 지원하는 ONTAP 및 SMB 버전과 라이센스 요구 사항이 무엇인지 알아야 합니다.

ONTAP 라이센스 요구 사항

SMB 라이센스가 있는 경우 IPv6에 대한 특수 라이센스가 필요하지 않습니다. SMB 라이센스는 에 포함되어 "ONTAP 1을 참조하십시오"있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

SMB 프로토콜 버전 요구 사항

- SVM의 경우 ONTAP는 모든 버전의 SMB 프로토콜에서 IPv6를 지원합니다.

ⓘ IPv6를 통한 NBNS(NetBIOS 이름 서비스)는 지원되지 않습니다.

ONTAP SMB 액세스 및 **CIFS** 서비스를 통한 **IPv6** 지원에 대해 자세히 알아보십시오

CIFS 서버에서 IPv6를 사용하려면 ONTAP가 CIFS 서비스에 대한 SMB 액세스 및 네트워크 통신을 위해 IPv6를 지원하는 방법을 알고 있어야 합니다.

Windows 클라이언트 및 서버 지원

ONTAP는 IPv6를 지원하는 Windows 서버 및 클라이언트를 지원합니다. 다음은 Microsoft Windows 클라이언트 및 서버 IPv6 지원에 대한 설명입니다.

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 이상에서는 DNS, LDAP, CLDAP 및 Kerberos 서비스를 포함한 SMB 파일 공유 및 Active Directory 서비스에 대해 IPv6를 지원합니다.

  IPv6 주소가 구성된 경우 Windows 7 및 Windows Server 2008 이상 릴리즈에서는 Active Directory 서비스에 대해 기본적으로 IPv6을 사용합니다. IPv6 연결을 통한 NTLM 및 Kerberos 인증이 모두 지원됩니다.

  ONTAP에서 지원하는 모든 Windows 클라이언트는 IPv6 주소를 사용하여 SMB 공유에 연결할 수 있습니다.

ONTAP가 지원하는 Windows 클라이언트에 대한 최신 정보는 를 참조하십시오 "상호 운용성 매트릭스".

NT 도메인은 IPv6에서 지원되지 않습니다.

추가 **CIFS** 서비스 지원

ONTAP는 SMB 파일 공유 및 Active Directory 서비스에 대한 IPv6 지원 외에도 다음에 대한 IPv6 지원을 제공합니다.

- 오프라인 폴더, 로밍 프로필, 폴더 리디렉션 및 이전 버전을 포함한 클라이언트측 서비스입니다
- 동적 홈 디렉토리(홈 디렉토리 기능), symlink 및 Widelink, BranchCache, ODX 복사 오프로드, 자동 노드 추천 등의 서버 측 서비스 및 이전 버전
- Windows 로컬 사용자 및 그룹을 사용하여 액세스 제어 및 권한 관리, CLI를 사용한 파일 권한 및 감사 정책 설정, 보안 추적, 파일 잠금 관리, SMB 작업 모니터링 등의 파일 액세스 관리 서비스입니다
- NAS 멀티 프로토콜 감사
- FPolicy를 참조하십시오
- 지속적으로 사용 가능한 공유, Witness 프로토콜 및 원격 VSS(SMB 구성 기반 Hyper-V에 사용)

네임 서비스 및 인증 서비스 지원

IPv6에서는 다음 이름 서비스와의 통신이 지원됩니다.

- 도메인 컨트롤러
- DNS 서버
- LDAP 서버
- KDC 서버
- NIS 서버

ONTAP SMB 서버가 **IPv6**를 사용하여 외부 서버에 연결하는 방법에 대해 알아봅니다

요구 사항을 충족하는 구성을 생성하려면 CIFS 서버가 외부 서버에 연결할 때 IPv6을 사용하는 방법을 알고 있어야 합니다.

- 원본 주소 선택

  외부 서버에 연결하려고 시도하면 선택한 소스 주소는 대상 주소와 같은 유형이어야 합니다. 예를 들어, IPv6 주소에 연결하는 경우 CIFS 서버를 호스팅하는 SVM(스토리지 가상 머신)에는 소스 주소로 사용할 IPv6 주소가 있는 데이터 LIF 또는 관리 LIF가 있어야 합니다. 마찬가지로, SVM을 IPv4 주소에 연결할 경우 소스 주소로 사용할 IPv4 주소가 있는 데이터 LIF 또는 관리 LIF가 있어야 합니다.

- DNS를 사용하여 동적으로 검색된 서버의 경우 서버 검색은 다음과 같이 수행됩니다.
  - 클러스터에서 IPv6이 비활성화되어 있으면 IPv4 서버 주소만 검색됩니다.
  - 클러스터에서 IPv6이 활성화되어 있으면 IPv4 및 IPv6 서버 주소가 모두 검색됩니다. 주소가 속한 서버의 적합성과 IPv6 또는 IPv4 데이터 또는 관리 LIF의 가용성에 따라 두 유형 중 하나를 사용할 수 있습니다. 동적 서버 검색은 도메인 컨트롤러 및 LSA, NETLOGON, Kerberos 및 LDAP와 같은 관련 서비스를 검색하는 데 사용됩니다.
- DNS 서버 연결

DNS 서버에 연결할 때 SVM이 IPv6을 사용하는지 여부는 DNS 이름 서비스 구성에 따라 달라집니다. DNS 서비스가 IPv6 주소를 사용하도록 구성된 경우 IPv6를 사용하여 연결합니다. 필요한 경우 DNS 이름 서비스 구성에서 IPv4 주소를 사용하여 DNS 서버에 대한 연결이 계속 IPv4 주소를 사용하도록 할 수 있습니다. DNS 이름 서비스를 구성할 때 IPv4 및 IPv6 주소의 조합을 지정할 수 있습니다.

- LDAP 서버 접속 구성

  LDAP 서버에 연결할 때 SVM이 IPv6을 사용하는지 여부는 LDAP 클라이언트 구성에 따라 달라집니다. LDAP 클라이언트가 IPv6 주소를 사용하도록 구성된 경우 IPv6를 사용하여 연결됩니다. 필요한 경우 LDAP 클라이언트 구성에서 IPv4 주소를 사용하여 LDAP 서버에 대한 연결이 계속 IPv4 주소를 사용하도록 할 수 있습니다. LDAP 클라이언트 구성을 구성할 때 IPv4 및 IPv6 주소의 조합을 지정할 수 있습니다.

  LDAP 클라이언트 구성은 UNIX 사용자, 그룹 및 넷그룹 이름 서비스에 대해 LDAP를 구성할 때 사용됩니다.

- NIS 서버 접속

  NIS 서버에 연결할 때 SVM이 IPv6을 사용하는지 여부는 NIS 이름 서비스 구성에 따라 달라집니다. NIS 서비스가 IPv6 주소를 사용하도록 구성된 경우 IPv6를 사용하여 연결합니다. 필요한 경우 NIS 이름 서비스 구성에서 IPv4 주소를 사용하여 NIS 서버에 대한 연결이 계속 IPv4 주소를 사용하도록 할 수 있습니다. NIS 이름 서비스를 구성할 때 IPv4 및 IPv6 주소의 조합을 지정할 수 있습니다.

  NIS 이름 서비스는 UNIX 사용자, 그룹, 넷그룹 및 호스트 이름 객체를 저장하고 관리하는 데 사용됩니다.

관련 정보

- 서버에 IPv6 활성화
- IPv6 세션에 대한 정보를 모니터링하고 표시합니다.

ONTAP SMB 서버에 **IPv6**를 사용하도록 설정합니다

클러스터 설정 중에 IPv6 네트워크가 활성화되지 않습니다. SMB용 IPv6를 사용하려면 클러스터 설정이 완료된 후 클러스터 관리자가 IPv6을 사용하도록 설정해야 합니다. 클러스터 관리자가 IPv6을 사용하도록 설정하면 전체 클러스터에 대해 설정됩니다.

단계

1. IPv6 사용:'네트워크 옵션 IPv6 수정 사용 참'을 선택합니다

   IPv6이 활성화되었습니다. SMB 액세스를 위한 IPv6 데이터 LIF를 구성할 수 있습니다.

관련 정보

- IPv6 세션에 대한 정보를 모니터링하고 표시합니다.
- "System Manager를 사용하여 네트워크를 시각화합니다"
- "클러스터에서 IPv6 활성화"
- "네트워크 옵션 IPv6 수정"

ONTAP SMB 서버에 대해 **IPv6**를 사용하지 않도록 설정하는 방법에 대해 자세히 알아보십시오

네트워크 옵션을 사용하여 클러스터에 IPv6이 설정되어 있어도 동일한 명령을 사용하여 SMB용 IPv6를 해제할 수 없습니다. 대신 ONTAP는 클러스터 관리자가 클러스터에서 마지막 IPv6 사용 인터페이스를 비활성화할 때 IPv6를 비활성화합니다. IPv6 지원 인터페이스 관리에 대해서는 클러스터 관리자와 통신해야 합니다.

관련 정보

- "System Manager를 사용하여 ONTAP 네트워크를 시각화합니다"

IPv6 ONTAP SMB 세션에 대한 정보를 모니터링하고 표시합니다

IPv6 네트워크를 사용하여 연결된 SMB 세션에 대한 정보를 모니터링하고 표시할 수 있습니다. 이 정보는 IPv6 SMB 세션에 대한 기타 유용한 정보와 함께 IPv6를 사용하여 연결 중인 클라이언트를 확인하는 데 유용합니다.

단계

1. 원하는 작업을 수행합니다.

다음 사항을 확인할 수 있습니다.	명령 입력...
SVM(스토리지 가상 시스템)에 대한 SMB 세션은 IPv6를 사용하여 연결됩니다	'vserver cifs session show -vserver_vserver_name_ -instance'
IPv6은 지정된 LIF 주소를 통해 SMB 세션에 사용됩니다	'vserver cifs session show -vserver_vserver_name_ -lif-address_LIF_ip_address_-instance' '*LIF_IP_address*'는 데이터 LIF의 IPv6 주소입니다.

SMB를 사용하여 파일 액세스를 설정합니다

보안 스타일을 구성합니다

보안 스타일이 데이터 액세스에 미치는 영향

ONTAP SMB 보안 스타일과 그 영향에 대해 알아보십시오

UNIX, NTFS, 혼합 및 통합 등 네 가지 보안 유형이 있습니다. 각 보안 스타일은 데이터에 대한 사용 권한이 처리되는 방식에 다른 영향을 줍니다. 용도에 맞는 적절한 보안 스타일을 선택할 수 있도록 다양한 효과를 이해해야 합니다.

보안 스타일은 클라이언트 유형이 데이터에 액세스할 수 있거나 액세스할 수 없는 형식을 결정하지 않는다는 점을 이해하는 것이 중요합니다. 보안 스타일은 ONTAP에서 데이터 액세스를 제어하는 데 사용하는 권한 유형과 이러한 권한을 수정할 수 있는 클라이언트 유형만 결정합니다.

예를 들어, 볼륨이 UNIX 보안 스타일을 사용하는 경우에도 SMB 클라이언트는 ONTAP의 멀티 프로토콜 특성으로 인해 데이터에 액세스(적절하게 인증 및 승인)할 수 있습니다. 그러나 ONTAP에서는 UNIX 클라이언트만 기본 툴을 사용하여 수정할 수 있는 UNIX 권한을 사용합니다.

보안 스타일	사용 권한을 수정할 수 있는 클라이언트입니다	클라이언트가 사용할 수 있는 권한	결과적으로 효율적인 보안 스타일을 제공합니다	파일에 액세스할 수 있는 클라이언트입니다
Unix	NFS 를 참조하십시오	NFSv3 모드 비트	Unix	NFS 및 SMB
		NFSv4.x ACL		
NTFS입니다	중소기업	NTFS ACL	NTFS입니다	
혼합	NFS 또는 SMB	NFSv3 모드 비트	Unix	
		NFSv4.ACL		
		NTFS ACL	NTFS입니다	
통합(ONTAP 9.4 및 이전 릴리즈에서 무한 확장 볼륨에만 해당)	NFS 또는 SMB	NFSv3 모드 비트	Unix	
		NFSv4.1 ACL		
		NTFS ACL	NTFS입니다	

FlexVol 볼륨은 UNIX, NTFS 및 혼합 보안 스타일을 지원합니다. 보안 스타일이 혼합 또는 통합된 경우 사용자가 보안 스타일을 개별적으로 설정하므로 사용자가 마지막으로 권한을 수정한 클라이언트 유형에 따라 유효 사용 권한이 달라집니다. 권한을 수정한 마지막 클라이언트가 NFSv3 클라이언트인 경우 사용 권한은 UNIX NFSv3 모드 비트입니다. 마지막 클라이언트가 NFSv4 클라이언트인 경우 사용 권한은 NFSv4 ACL입니다. 마지막 클라이언트가 SMB 클라이언트인 경우 사용 권한은 Windows NTFS ACL입니다.

통합 보안 스타일은 ONTAP 9.5 이상 릴리스에서 더 이상 지원되지 않는 무한 볼륨에서만 사용할 수 있습니다. 자세한 내용은 을 참조하십시오 FlexGroup 볼륨 관리 개요.

그만큼 `show-effective-permissions` 매개변수를 사용하여 `vserver security file-directory` 명령을 사용하면 지정된 파일이나 폴더 경로에 대해 Windows 또는 UNIX 사용자에게 부여된 유효 권한을 표시할 수 있습니다. 또한 선택적 매개 변수를 `-share-name` 사용하면 효과적인 공유 권한을 표시할 수 있습니다. 에 대한 자세한 내용은 `vserver security file-directory show-effective-permissions` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP는 처음에 일부 기본 파일 권한을 설정합니다. 기본적으로 UNIX, 혼합 및 통합 보안 스타일 볼륨의 모든 데이터에 대한 효과적인 보안 스타일은 UNIX이고, 기본 보안 스타일에 의해 허용되는 대로 클라이언트에 의해 구성될 때까지 유효 사용 권한 유형은 UNIX 모드 비트(별도로 지정하지 않는 경우 0755)입니다. 기본적으로 NTFS 보안 스타일 볼륨의 모든 데이터에 대한 효과적인 보안 스타일은 NTFS이며 ACL을 통해 모든 사람에게 모든 권한을 제공할 수 있습니다.

관련 정보

- "ONTAP 명령 참조입니다"

ONTAP SMB 보안 스타일을 설정할 위치 및 시기에 대해 알아보십시오

보안 스타일은 FlexVol 볼륨(루트 또는 데이터 볼륨) 및 qtree에서 설정할 수 있습니다. 보안 스타일은 생성 시 수동으로 설정하거나 자동으로 상속하거나 나중에 변경할 수 있습니다.

ONTAP SVM에서 사용할 **SMB** 보안 유형을 결정합니다

볼륨에 사용할 보안 스타일을 결정하는 데 도움이 되도록 두 가지 요소를 고려해야 합니다. 기본 요소는 파일 시스템을 관리하는 관리자 유형입니다. 2차 요소는 볼륨의 데이터에 액세스하는

사용자 또는 서비스의 유형입니다.

볼륨에 보안 스타일을 구성할 때는 최상의 보안 스타일을 선택하고 사용 권한 관리 문제를 피하기 위해 환경의 요구 사항을 고려해야 합니다. 다음 고려 사항을 통해 결정을 내릴 수 있습니다.

보안 스타일	다음 경우에 선택...
Unix	• 파일 시스템은 UNIX 관리자가 관리합니다. • 대부분의 사용자는 NFS 클라이언트입니다. • 데이터에 액세스하는 애플리케이션은 UNIX 사용자를 서비스 계정으로 사용합니다.
NTFS입니다	• 파일 시스템은 Windows 관리자가 관리합니다. • 대부분의 사용자는 SMB 클라이언트입니다. • 데이터에 액세스하는 응용 프로그램은 Windows 사용자를 서비스 계정으로 사용합니다.
혼합	파일 시스템은 UNIX 관리자와 Windows 관리자 모두에서 관리되며 사용자는 NFS 클라이언트와 SMB 클라이언트로 구성됩니다.

ONTAP SMB 보안 스타일 상속에 대해 알아보십시오

새 FlexVol 볼륨 또는 qtree를 생성할 때 보안 스타일을 지정하지 않으면 보안 스타일이 다른 방식으로 상속됩니다.

보안 스타일은 다음과 같은 방식으로 상속됩니다.

- FlexVol 볼륨은 SVM이 포함된 루트 볼륨의 보안 스타일을 상속합니다.
- qtree는 포함된 FlexVol 볼륨의 보안 스타일을 상속합니다.
- 파일 또는 디렉토리는 포함된 FlexVol 볼륨 또는 qtree의 보안 스타일을 상속합니다.

ONTAP SMB FlexVol 볼륨에 대한 **UNIX** 사용 권한을 유지하는 방법에 대해 알아봅니다

현재 UNIX 사용 권한이 있는 FlexVol 볼륨의 파일을 Windows 응용 프로그램에서 편집하고 저장하면 ONTAP에서 UNIX 사용 권한을 보존할 수 있습니다.

Windows 클라이언트의 응용 프로그램이 파일을 편집하고 저장할 때 파일의 보안 속성을 읽고, 새 임시 파일을 만들고, 해당 속성을 임시 파일에 적용한 다음 임시 파일에 원래 파일 이름을 지정합니다.

Windows 클라이언트가 보안 속성에 대한 쿼리를 수행할 때 UNIX 권한을 정확하게 나타내는 생성된 ACL을 받습니다. 이 생성된 ACL의 유일한 목적은 파일이 Windows 애플리케이션에 의해 업데이트되므로 파일의 UNIX 사용 권한을 보존하여 결과 파일이 동일한 UNIX 사용 권한을 갖도록 하는 것입니다. ONTAP는 생성된 ACL을 사용하여 NTFS ACL을 설정하지 않습니다.

ONTAP SMB 서버의 Windows 보안 탭을 사용하여 UNIX 권한을 관리하는 방법에 대해 알아봅니다

SVM에서 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 대한 UNIX 권한을 조작하려는 경우 Windows 클라이언트의 보안 탭을 사용할 수 있습니다. 또는 Windows ACL을 쿼리하고 설정할 수 있는 응용 프로그램을 사용할 수도 있습니다.

- UNIX 사용 권한 수정

  Windows 보안 탭을 사용하여 혼합 보안 스타일 볼륨 또는 qtree에 대한 UNIX 권한을 보고 변경할 수 있습니다. 기본 Windows 보안 탭을 사용하여 UNIX 권한을 변경하는 경우 변경하기 전에 먼저 편집할 기존 ACE(모드 비트를 0으로 설정)를 제거해야 합니다. 또는 고급 편집기를 사용하여 권한을 변경할 수도 있습니다.

  모드 권한을 사용하는 경우 나열된 UID, GID 및 기타(컴퓨터에 계정이 있는 다른 모든 사용자)에 대한 모드 권한을 직접 변경할 수 있습니다. 예를 들어, 표시된 UID에 r-x 권한이 있는 경우 UID 권한을 rwx로 변경할 수 있습니다.

- UNIX 권한을 NTFS 권한으로 변경합니다

  Windows 보안 탭을 사용하면 파일 및 폴더에 UNIX 유효 보안 스타일이 있는 혼합 보안 스타일 볼륨 또는 qtree의 UNIX 보안 개체를 Windows 보안 개체로 대체할 수 있습니다.

  원하는 Windows 사용자 및 그룹 개체로 대체하려면 먼저 나열된 모든 UNIX 권한 항목을 제거해야 합니다. 그런 다음 Windows 사용자 및 그룹 개체에서 NTFS 기반 ACL을 구성할 수 있습니다. 모든 UNIX 보안 개체를 제거하고 혼합 보안 스타일 볼륨 또는 qtree의 파일 또는 폴더에 Windows 사용자 및 그룹만 추가하면 파일 또는 폴더의 효과적인 보안 스타일이 UNIX에서 NTFS로 변경됩니다.

  폴더에 대한 권한을 변경할 때 기본 Windows 동작은 이러한 변경 내용을 모든 하위 폴더 및 파일에 전파하는 것입니다. 따라서 보안 스타일의 변경 사항을 모든 하위 폴더, 하위 폴더 및 파일에 전파하지 않으려면 전파 선택 사항을 원하는 설정으로 변경해야 합니다.

ONTAP SVM 루트 볼륨에 SMB 보안 형식을 구성합니다

SVM(Storage Virtual Machine) 루트 볼륨 보안 스타일을 구성하여 SVM의 루트 볼륨에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 보안 스타일을 정의하려면 '-rootvolume-security-style' 매개 변수와 함께 'vserver create' 명령을 사용하십시오.

   루트 볼륨 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS 또는 혼합 입니다.

2. 생성한 SVM의 루트 볼륨 보안 스타일('vserver show -vserver_vserver_name_')을 포함하여 구성을 표시하고 확인합니다

ONTAP FlexVol 볼륨에 SMB 보안 스타일을 구성합니다

FlexVol 볼륨 보안 스타일을 구성하여 SVM(스토리지 가상 머신)의 FlexVol 볼륨에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

FlexVol 볼륨이	명령 사용…
아직 없습니다	보안 스타일을 지정하기 위해 볼륨 생성 및 '-security-style' 매개 변수를 포함합니다.
이미 있습니다	볼륨 수정, -security-style 매개 변수를 포함해서 보안 스타일을 지정합니다.

FlexVol 볼륨 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS 또는 혼합 입니다.

FlexVol 볼륨을 만들 때 보안 스타일을 지정하지 않으면 볼륨은 루트 볼륨의 보안 스타일을 상속합니다.

볼륨 생성 또는 볼륨 수정 명령에 대한 자세한 내용은 을 참조하십시오 "논리적 스토리지 관리".

2. 생성한 FlexVol 볼륨의 보안 스타일을 포함하여 구성을 표시하려면 다음 명령을 입력합니다.

   'volume show-volume volume_name-instance'

ONTAP qtree에서 **SMB** 보안 스타일을 구성합니다

Qtree 볼륨 보안 스타일을 구성하여 Qtree에서 데이터에 사용되는 권한의 유형을 결정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

qtree가…	명령 사용…
아직 없습니다	볼륨 qtree create를 수행하고 보안 스타일을 지정하는 -security-style 매개 변수를 포함합니다.
이미 있습니다	볼륨 qtree 수정과 보안 유형을 지정하는 -security-style 매개 변수를 포함합니다.

qtree 보안 스타일에 사용할 수 있는 옵션은 UNIX, NTFS, 혼합 입니다.

Qtree를 만들 때 보안 스타일을 지정하지 않으면 기본 보안 스타일이 '혼합'으로 설정됩니다.

'볼륨 qtree 생성' 또는 '볼륨 qtree 수정' 명령에 대한 자세한 내용은 을 참조하십시오 "논리적 스토리지 관리".

2. 생성한 qtree의 보안 스타일을 포함하여 구성을 표시하려면 ' volume qtree show-qtree qtree qtree_name-instance ' 명령을 입력합니다

NAS 네임스페이스에서 데이터 볼륨을 생성하고 관리합니다

NAS 네임스페이스에서 **ONTAP SMB** 데이터 볼륨을 생성하고 관리하는 방법에 대해 알아보십시오

NAS 환경에서 파일 액세스를 관리하려면 SVM(스토리지 가상 머신)에서 데이터 볼륨과 접합

지점을 관리해야 합니다. 여기에는 네임스페이스 아키텍처 계획, 접합 지점을 사용하거나 사용하지 않는 볼륨 생성, 볼륨 마운트 또는 마운트 해제, 데이터 볼륨 및 NFS 서버 또는 CIFS 서버 네임스페이스에 대한 정보 표시 등이 포함됩니다.

지정된 접합 지점으로 **ONTAP SMB** 데이터 볼륨을 생성합니다

데이터 볼륨을 생성할 때 교차점을 지정할 수 있습니다. 결과 볼륨은 교차점에 자동으로 마운트되며 NAS 액세스를 위해 즉시 구성할 수 있습니다.

시작하기 전에

볼륨을 생성할 애그리게이트가 이미 존재해야 합니다.

> 다음 문자는 접합 경로에 사용할 수 없습니다. *#"><|? \
>
> 또한 접합 경로 길이는 255자를 초과할 수 없습니다.

단계

1. "volume create-vserver_name_-volume_volume_name_-aggregate_aggregate_name_-size{integer[KB|MB|GB|TB|PB]}-security-style{NTFS|UNIX|MIXED}-junction-path_junction_path_"를 사용하여 볼륨을 생성합니다

   접합 경로는 루트(/)로 시작해야 하며 디렉터리와 접합된 볼륨을 모두 포함할 수 있습니다. 접합 경로에는 볼륨의 이름을 포함할 필요가 없습니다. 접합 경로는 볼륨 이름과 무관합니다.

   볼륨 보안 스타일을 지정하는 것은 선택 사항입니다. 보안 스타일을 지정하지 않으면 ONTAP에서 SVM(스토리지 가상 머신)의 루트 볼륨에 적용되는 것과 동일한 보안 스타일로 볼륨을 생성합니다. 그러나 루트 볼륨의 보안 스타일이 만드는 데이터 볼륨에 적용할 보안 스타일이 아닐 수 있습니다. 문제 해결이 어려운 파일 액세스 문제를 최소화하기 위해 볼륨을 생성할 때 보안 스타일을 지정하는 것이 좋습니다.

   교차경로는 대/소문자를 구분하지 않고 /eng은 /eng과 같습니다. CIFS 공유를 생성하는 경우 Windows는 연결 경로를 대/소문자를 구분하는 것처럼 처리합니다. 예를 들어, junction이 /eng인 경우 CIFS 공유의 경로는 /eng가 아니라 /eng로 시작해야 합니다.

   데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 여러 가지 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 볼륨이 원하는 접합 지점 'volume show-vserver_vserver_name_-volume_volume_name_-junction'을 사용하여 생성되었는지 확인합니다

예

다음 예에서는 junction path "/eng/home"이 있는 SVM VS1 상에 ""home4""라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

접합 지점을 지정하지 않고 **ONTAP SMB** 데이터 볼륨을 생성합니다

교차점을 지정하지 않고 데이터 볼륨을 생성할 수 있습니다. 결과 볼륨은 자동으로 마운트되지 않으며 NAS 액세스에 대해 구성할 수 없습니다. 해당 볼륨에 대해 SMB 공유 또는 NFS 내보내기를 구성하려면 먼저 볼륨을 마운트해야 합니다.

시작하기 전에

볼륨을 생성할 애그리게이트가 이미 존재해야 합니다.

단계

1. 다음 명령을 사용하여 접합 지점 없이 볼륨을 생성합니다. 'volume create-vserver_name_-volume_volume_name_-aggregate_aggregate_name_-size{integer[KB|MB|GB|TB|PB]} - security-style{NTFS|UNIX|MIXED}'

   볼륨 보안 스타일을 지정하는 것은 선택 사항입니다. 보안 스타일을 지정하지 않으면 ONTAP에서 SVM(스토리지 가상 머신)의 루트 볼륨에 적용되는 것과 동일한 보안 스타일로 볼륨을 생성합니다. 그러나 루트 볼륨의 보안 스타일이 데이터 볼륨에 적용할 보안 스타일이 아닐 수 있습니다. 문제 해결이 어려운 파일 액세스 문제를 최소화하기 위해 볼륨을 생성할 때 보안 스타일을 지정하는 것이 좋습니다.

   데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 여러 가지 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 볼륨이 "volume show-vserver_name_-volume_volume_name_-junction" 접합 지점 없이 생성되었는지 확인합니다

예

다음 예에서는 교차점에 마운트되지 않은 SVM VS1 상에 "sales"라는 이름의 볼륨을 생성합니다.

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

NAS 네임스페이스에서 기존 **ONTAP SMB** 볼륨을 마운트하거나 마운트 해제합니다

SVM(스토리지 가상 시스템) 볼륨에 포함된 데이터에 대한 NAS 클라이언트 액세스를 구성하려면 먼저 NAS 네임스페이스에 볼륨을 마운트해야 합니다. 볼륨이 현재 마운트되지 않은 경우 볼륨을 연결 지점에 마운트할 수 있습니다. 볼륨을 마운트 해제할 수도 있습니다.

이 작업에 대해

볼륨을 마운트 해제하고 오프라인으로 전환하면 마운트 해제된 볼륨의 네임스페이스 내에 포함된 접합 지점의 볼륨 데이터를 비롯하여 연결 지점 내의 모든 데이터를 NAS 클라이언트에서 액세스할 수 없습니다.

> 볼륨에 대한 NAS 클라이언트 액세스를 중단하려면 볼륨을 마운트 해제하는 것만으로는 충분하지 않습니다. 볼륨을 오프라인으로 전환하거나 클라이언트 측 파일 핸들 캐시가 무효화되도록 다른 단계를 수행해야 합니다. 자세한 내용은 다음 기술 자료 문서를 참조하십시오. "ONTAP의 네임스페이스에서 제거후에도 NFSv3 클라이언트가 볼륨에 계속 액세스할 수 있습니다"

볼륨을 마운트 해제하고 오프라인으로 전환하면 볼륨 내의 데이터가 손실되지 않습니다. 또한 마운트 해제된 볼륨 내의 볼륨이나 디렉토리 및 연결 지점에 생성된 기존 볼륨 내보내기 정책 및 SMB 공유가 보존됩니다. 마운트 해제된 볼륨을 다시 마운트하면 NAS 클라이언트가 기존 엑스포트 정책과 SMB 공유를 사용하여 볼륨 내에 포함된 데이터에 액세스할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

원하는 작업	명령 입력...
볼륨을 마운트합니다	'volume mount-vserver_svm_name_-volume_volume_name_-junction-path_junction_path_'

원하는 작업	명령 입력...

볼륨을 마운트 해제합니다	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. 볼륨이 원하는 마운트 상태에 있는지 확인합니다.

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

예

다음 예에서는 SVM ""VS1""에 있는 ""판매""라는 볼륨을 접합 지점 """/판매""에 마운트합니다.

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

다음 예에서는 SVM ""VS1""에 있는 ""데이터""라는 이름의 볼륨을 마운트 해제하고 오프라인으로 전환합니다.

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

ONTAP SMB 볼륨 마운트 및 접합 지점 정보를 표시합니다

스토리지 가상 시스템(SVM)에 대해 마운트된 볼륨 및 볼륨이 마운트된 접합 지점에 대한 정보를 표시할 수 있습니다. 또한 어느 볼륨이 분기점에 마운트되지 않는지 확인할 수 있습니다. 이

정보를 사용하여 SVM 네임스페이스를 이해하고 관리할 수 있습니다.

단계

1. 원하는 작업을 수행합니다.

를 표시하려면...	명령 입력...
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 요약 정보	'volume show-vserver vserver_name-junction'
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 자세한 정보	'volume show -vserver vserver_name -volume volume_name -instance'
SVM에서 마운트 및 마운트 해제된 볼륨에 대한 특정 정보	a. 필요한 경우 볼륨 표시 필드? 명령을 사용하여 '-fields' 매개 변수에 대한 유효한 필드를 표시할 수 있습니다 b. '-fields' 매개 변수를 사용하여 원하는 정보를 표시합니다. volume show -vserver vserver_name -fields fieldname,…

예

다음 예는 SVM VS1 에서 마운트 및 마운트 해제된 볼륨에 대한 요약을 표시합니다.

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

다음 예는 SVM VS2 에 있는 볼륨의 지정된 필드에 대한 정보를 표시합니다.

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

이름 매핑을 구성합니다

ONTAP SMB 이름 매핑 구성에 대해 자세히 알아보십시오

ONTAP는 이름 매핑을 사용하여 CIFS ID를 UNIX ID에 매핑하고, Kerberos ID를 UNIX ID에 매핑하며, UNIX ID를 CIFS ID에 매핑합니다. 사용자 자격 증명을 얻고 NFS 클라이언트나 CIFS 클라이언트에서 연결 중인지에 관계없이 적절한 파일 액세스를 제공하려면 이 정보가 필요합니다.

이름 매핑을 사용할 필요가 없는 두 가지 예외가 있습니다.

- 순수 UNIX 환경을 구성하고 볼륨에 CIFS 액세스 또는 NTFS 보안 스타일을 사용하지 않을 계획입니다.
- 대신 사용할 기본 사용자를 구성합니다.

  이 시나리오에서는 모든 개별 클라이언트 자격 증명을 매핑하지 않고 모든 클라이언트 자격 증명이 동일한 기본 사용자에게 매핑되기 때문에 이름 매핑이 필요하지 않습니다.

사용자 이름 매핑만 사용할 수 있으며 그룹에서는 사용할 수 없습니다.

그러나 개별 사용자 그룹을 특정 사용자에게 매핑할 수 있습니다. 예를 들어, 영업이라는 단어가 있는 모든 AD 사용자를 특정 UNIX 사용자 및 사용자의 UID에 매핑할 수 있습니다.

ONTAP SMB 이름 매핑에 대해 자세히 알아보십시오

ONTAP에서 사용자에 대한 자격 증명을 매핑해야 하는 경우 먼저 로컬 이름 매핑 데이터베이스와 LDAP 서버에서 기존 매핑을 확인합니다. SVM의 네임 서비스 구성에 따라 1개 또는 2개 모두를 검사할지 여부를 결정합니다.

- Windows에서 UNIX로의 매핑의 경우

  매핑을 찾을 수 없는 경우 ONTAP는 소문자 Windows 사용자 이름이 UNIX 도메인의 유효한 사용자 이름인지 확인합니다. 이렇게 해도 문제가 해결되지 않으면 기본 UNIX 사용자를 사용합니다(구성된 경우). 기본 UNIX 사용자가 구성되어 있지 않고 ONTAP가 이러한 방식으로 매핑을 얻을 수 없는 경우 매핑이 실패하고 오류가 반환됩니다.

- UNIX에서 Windows로의 매핑의 경우

  매핑을 찾을 수 없는 경우 ONTAP는 SMB 도메인의 UNIX 이름과 일치하는 Windows 계정을 찾으려고 시도합니다. 이 기능이 작동하지 않으면 기본 SMB 사용자를 사용합니다(구성된 경우). 기본 CIFS 사용자가 구성되어 있지 않고 ONTAP가 이러한 방식으로 매핑을 가져올 수 없는 경우 매핑이 실패하고 오류가 반환됩니다.

컴퓨터 계정은 기본적으로 지정된 기본 UNIX 사용자에게 매핑됩니다. 기본 UNIX 사용자를 지정하지 않으면 컴퓨터 계정 매핑이 실패합니다.

- ONTAP 9.5부터 기본 UNIX 사용자가 아닌 다른 사용자에게 시스템 계정을 매핑할 수 있습니다.
- ONTAP 9.4 이하 버전에서는 시스템 계정을 다른 사용자에게 매핑할 수 없습니다.

  컴퓨터 계정에 대한 이름 매핑이 정의되어 있더라도 매핑은 무시됩니다.

UNIX 사용자와 **Windows** 사용자 이름 간 매핑에 대한 **ONTAP SMB** 다중 도메인 검색에 대해 알아봅니다

ONTAP는 UNIX 사용자를 Windows 사용자에게 매핑할 때 다중 도메인 검색을 지원합니다. 일치하는 결과가 반환될 때까지 검색된 모든 신뢰할 수 있는 도메인이 대체 패턴과 일치하는 항목을 검색합니다. 또는 검색된 신뢰할 수 있는 도메인 목록 대신 사용되는 기본 신뢰할 수 있는 도메인 목록을 구성할 수 있으며 일치하는 결과가 반환될 때까지 순서대로 검색됩니다.

도메인 트러스트가 **UNIX** 사용자에게 **Windows** 사용자 이름 매핑 검색에 미치는 영향

다중 도메인 사용자 이름 매핑의 작동 방식을 이해하려면 ONTAP에서 도메인 트러스트가 작동하는 방식을 이해해야 합니다. CIFS 서버의 홈 도메인과의 Active Directory 트러스트 관계는 양방향 신뢰일 수도 있고 인바운드 트러스트 또는 아웃바운드 트러스트를 포함한 두 가지 단방향 트러스트 유형 중 하나일 수도 있습니다. 홈 도메인은 SVM의 CIFS 서버가 속하는 도메인입니다.

- _양방향 트러스트 _

  양방향 트러스트를 사용하면 두 도메인이 서로 신뢰합니다. CIFS 서버의 홈 도메인에 다른 도메인과의 양방향 트러스트가 있는 경우 홈 도메인이 신뢰할 수 있는 도메인에 속한 사용자를 인증하고 권한을 부여할 수 있으며 그 반대의 경우도 마찬가지입니다.

  UNIX 사용자 대 Windows 사용자 이름 매핑 검색은 홈 도메인과 다른 도메인 간의 양방향 트러스트가 있는 도메인에서만 수행할 수 있습니다.

- _아웃바운드 트러스트 _

  아웃바운드 트러스트를 사용하면 홈 도메인이 다른 도메인을 신뢰합니다. 이 경우 홈 도메인이 아웃바운드 신뢰할 수 있는 도메인에 속하는 사용자를 인증하고 권한을 부여할 수 있습니다.

  UNIX 사용자 대 Windows 사용자 이름 매핑 검색을 수행할 때 홈 도메인의 아웃바운드 트러스트가 _not_sunfre검색되었습니다.

- _ 인바운드 신뢰 _

  인바운드 트러스트를 사용하면 다른 도메인이 CIFS 서버의 홈 도메인을 신뢰합니다. 이 경우 홈 도메인은 인바운드 신뢰할 수 있는 도메인에 속하는 사용자를 인증하거나 승인할 수 없습니다.

  UNIX 사용자 대 Windows 사용자 이름 매핑 검색을 수행할 때 홈 도메인의 인바운드 트러스트가 _not_sound입니다.

이름 매핑에 대한 다중 도메인 검색을 구성하는 데 와일드카드**(*)**를 사용하는 방법

다중 도메인 이름 매핑 검색은 Windows 사용자 이름의 도메인 섹션에서 와일드카드를 사용하여 쉽게 수행할 수 있습니다. 다음 표에서는 이름 매핑 항목의 도메인 부분에서 와일드카드를 사용하여 다중 도메인 검색을 사용하는 방법을 보여 줍니다.

패턴	교체	결과
루트	• \\ 관리자	UNIX 사용자 "root"는 "administrator"라는 사용자에게 매핑됩니다. "administrator"라는 이름의 첫 번째 일치하는 사용자를 찾을 때까지 모든 신뢰할 수 있는 도메인을 순서대로 검색합니다.
*	\ * \\ *	유효한 UNIX 사용자는 해당 Windows 사용자에게 매핑됩니다. 모든 신뢰할 수 있는 도메인은 해당 이름을 가진 첫 번째 일치하는 사용자를 찾을 때까지 순서대로 검색됩니다. 패턴 \ * \\ * 은 UNIX에서 Windows로의 이름 매핑에만 유효하며 다른 방법은 사용할 수 없습니다.

다중 도메인 이름 검색 수행 방법

다음 두 가지 방법 중 하나를 선택하여 다중 도메인 이름 검색에 사용되는 신뢰할 수 있는 도메인 목록을 확인할 수 있습니다.

- ONTAP에서 컴파일한 자동으로 검색된 양방향 트러스트 목록을 사용합니다

- 컴파일하는 신뢰할 수 있는 기본 도메인 목록을 사용합니다

UNIX 사용자가 사용자 이름의 도메인 섹션에 와일드카드를 사용하여 Windows 사용자에게 매핑된 경우 Windows 사용자는 다음과 같이 모든 신뢰할 수 있는 도메인에서 찾을 수 있습니다.

- 선호하는 트러스트된 도메인 목록이 구성되어 있으면 매핑된 Windows 사용자는 이 검색 목록에서만 순서대로 검색됩니다.
- 신뢰할 수 있는 도메인의 기본 설정 목록이 구성되어 있지 않으면 홈 도메인의 모든 양방향 신뢰할 수 있는 도메인에서 Windows 사용자가 표시됩니다.
- 홈 도메인에 대해 양방향으로 신뢰할 수 있는 도메인이 없는 경우 사용자는 홈 도메인에서 표시됩니다.

UNIX 사용자가 사용자 이름의 도메인 섹션이 없는 Windows 사용자에게 매핑된 경우 Windows 사용자는 홈 도메인에서 찾을 수 있습니다.

ONTAP SMB 이름 매핑 변환 규칙에 대해 알아보십시오

ONTAP 시스템은 각 SVM에 대해 일련의 전환 규칙을 유지합니다. 각 규칙은 A_pattern_과 A_replacement_의 두 부분으로 구성됩니다. 변환은 적절한 목록의 시작 부분에서 시작하여 첫 번째 일치 규칙을 기반으로 대체를 수행합니다. 이 패턴은 UNIX 형식의 정규식입니다. 대체는 UNIX 'ed' 프로그램과 마찬가지로 패턴에서 부분식을 나타내는 이스케이프 시퀀스를 포함하는 문자열입니다.

ONTAP SMB 이름 매핑을 생성합니다

'vserver name-mapping create' 명령을 사용하여 이름 매핑을 생성할 수 있습니다. 이름 매핑을 사용하여 Windows 사용자가 UNIX 보안 스타일 볼륨에 액세스하고 그 반대로 액세스할 수 있습니다.

이 작업에 대해

각 SVM에서 ONTAP은 각 방향에 대해 최대 12,500개의 이름 매핑을 지원합니다.

단계

1. 이름 매핑을 작성하십시오. 'vserver name-mapping create-vserver_vserver_name_-direction{KRB-UNIX|win-unix|unix-win}-position_integer_-pattern text-replacement_text_'

> ⓘ `-pattern`및 `-replacement` 문은 정규식으로 공식화할 수 있습니다. 또한 이 문을 사용하여 `null` 대체 문자열(공백 문자)을 사용하여 사용자에 대한 매핑을 명시적으로 거부할 `" "` 수도 `-replacement` 있습니다. 에 대한 자세한 내용은 `vserver name-mapping create` link:https://docs.netapp.com/us-en/ontap-cli/vserver-name-mapping-create.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

   Windows와 UNIX 간 매핑이 생성될 때 새 매핑이 생성될 때 ONTAP 시스템에 대한 열린 연결이 있는 모든 SMB 클라이언트는 로그아웃했다가 다시 로그인하여 새 매핑을 확인해야 합니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM에 이름 매핑이 생성됩니다. 매핑은 우선 순위 목록의 위치 1에서 UNIX에서 Windows로의 매핑입니다. 매핑은 UNIX 사용자 johnd를 Windows 사용자 ENG\JohnnDoe에 매핑합니다.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

다음 명령을 실행하면 이름이 VS1 인 SVM에 또 다른 이름 매핑이 생성됩니다. 매핑은 우선 순위 목록의 위치 1에서 Windows에서 UNIX로의 매핑입니다. 여기에는 정규식이 포함됩니다. 매핑은 SVM과 연결된 LDAP 도메인의 사용자에게 도메인 ENG의 모든 CIFS 사용자를 매핑합니다.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

다음 명령을 실행하면 이름이 VS1 인 SVM에 또 다른 이름 매핑이 생성됩니다. 이 패턴에는 이스케이프해야 하는 Windows 사용자 이름의 요소로 ""$"가 포함됩니다. 매핑은 Windows 사용자 ENG\John$ops를 UNIX 사용자 John_ops에 매핑합니다.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

기본 **ONTAP SMB** 사용자를 구성합니다

사용자의 다른 모든 매핑 시도가 실패하거나 UNIX와 Windows 간에 개별 사용자를 매핑하지 않으려는 경우 사용할 기본 사용자를 구성할 수 있습니다. 또는 매핑되지 않은 사용자의 인증에 실패하도록 하려면 기본 사용자를 구성하지 않아야 합니다.

이 작업에 대해

CIFS 인증의 경우 각 Windows 사용자를 개별 UNIX 사용자에게 매핑하지 않으려면 대신 기본 UNIX 사용자를 지정할 수 있습니다.

NFS 인증의 경우 각 UNIX 사용자를 개별 Windows 사용자에게 매핑하지 않으려면 대신 기본 Windows 사용자를 지정할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	다음 명령을 입력합니다...
기본 UNIX 사용자를 구성합니다	'vserver cifs options modify-default-unix-user_user_name_'
기본 Windows 사용자를 구성합니다	'vserver nfs modify -default-win-user_user_name_'

SMB 이름 매핑을 관리하기 위한 **ONTAP** 명령

이름 매핑을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용…
이름 매핑을 생성합니다	`vserver name-mapping create`
특정 위치에 이름 매핑을 삽입합니다	`vserver name-mapping insert`
이름 매핑을 표시합니다	`vserver name-mapping show`
두 이름 매핑의 위치를 교환합니다. 참고: 이름 매핑이 IP 한정자 항목으로 구성된 경우에는 스왑이 허용되지 않습니다.	`vserver name-mapping swap`
이름 매핑을 수정합니다	`vserver name-mapping modify`
이름 매핑을 삭제합니다	`vserver name-mapping delete`
올바른 이름 매핑을 확인합니다	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

에 대한 자세한 내용은 `vserver name-mapping` "ONTAP 명령 참조입니다"을 참조하십시오.

다중 도메인 이름 매핑 검색을 구성합니다

ONTAP SMB 다중 도메인 이름 매핑 검색을 사용하거나 사용하지 않도록 설정합니다

다중 도메인 이름 매핑 검색을 사용하면 UNIX 사용자를 Windows 사용자 이름 매핑에 구성할 때 Windows 이름의 도메인 부분에서 와일드 카드(\ )를 사용할 수 있습니다. 이름의 도메인 부분에서 와일드카드()를 사용하면 ONTAP에서 CIFS 서버의 컴퓨터 계정이 포함된 도메인과 양방향 트러스트가 있는 모든 도메인을 검색할 수 있습니다.

이 작업에 대해

양방향으로 신뢰할 수 있는 모든 도메인을 검색하는 대신 선호하는 신뢰할 수 있는 도메인 목록을 구성할 수 있습니다. 선호하는 신뢰할 수 있는 도메인 목록이 구성되면 ONTAP는 검색된 양방향으로 신뢰할 수 있는 도메인 대신 선호하는 신뢰할 수 있는 도메인 목록을 사용하여 다중 도메인 이름 매핑 검색을 수행합니다.

- 다중 도메인 이름 매핑 검색은 기본적으로 사용하도록 설정됩니다.
- 이 옵션은 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다

2. 다음 작업 중 하나를 수행합니다.

다중 도메인 이름 매핑 검색을 사용하려는 경우...	명령 입력...
활성화됨	'vserver cifs options modify -vserver_vserver_name_-is-trusted-domain-enum -search-enabled true'
사용 안 함	'vserver cifs options modify -vserver_vserver_name_-is-trusted-domain-enum -search-enabled false'

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

관련 정보

사용 가능한 서버 옵션

신뢰할 수 있는 **ONTAP SMB** 도메인을 재설정하고 재검색합니다

신뢰할 수 있는 모든 도메인을 강제로 다시 검색할 수 있습니다. 이 기능은 신뢰할 수 있는 도메인 서버가 제대로 응답하지 않거나 트러스트 관계가 변경된 경우에 유용할 수 있습니다. CIFS 서버의 컴퓨터 계정이 포함된 도메인인 홈 도메인과의 양방향 트러스트가 있는 도메인만 검색됩니다.

단계

1. 'vserver cifs domain trusts retrover' 명령을 사용하여 신뢰할 수 있는 도메인을 재설정하고 다시 검색합니다.

   'vserver cifs domain r트러스트 reDiscover - vserver vs1'

관련 정보

검색된 신뢰할 수 있는 도메인에 대한 정보를 표시합니다

검색된 신뢰할 수 있는 **ONTAP SMB** 도메인에 대한 정보를 표시합니다

CIFS 서버의 컴퓨터 계정이 포함된 도메인인 CIFS 서버의 홈 도메인에 대해 검색된 신뢰할 수 있는 도메인에 대한 정보를 표시할 수 있습니다. 이 기능은 검색된 신뢰할 수 있는 도메인과 검색된 신뢰할 수 있는 도메인 목록 내에서 해당 도메인의 순서가 어떻게 정렬되는지 알고 싶을 때 유용합니다.

이 작업에 대해

홈 도메인과 양방향 트러스트가 있는 도메인만 검색됩니다. 홈 도메인의 DC(도메인 컨트롤러)가 DC에서 결정한 순서대로 신뢰할 수 있는 도메인 목록을 반환하므로 목록 내의 도메인 순서를 예측할 수 없습니다. 신뢰할 수 있는 도메인 목록을 표시하여 다중 도메인 이름 매핑 검색에 대한 검색 순서를 결정할 수 있습니다.

표시된 신뢰할 수 있는 도메인 정보는 노드 및 SVM(스토리지 가상 머신)별로 그룹화됩니다.

단계

1. 'vserver cifs domain trusts show' 명령을 사용하여 검색된 신뢰할 수 있는 도메인에 대한 정보를 표시합니다.

'vserver cifs domain ships ships ships vs1'이 표시됩니다

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

관련 정보

신뢰할 수 있는 도메인을 다시 설정하고 다시 검색합니다

기본 설정 목록에서 신뢰할 수 있는 **ONTAP SMB** 도메인을 추가, 제거 또는 교체합니다

SMB 서버의 기본 설정 신뢰할 수 있는 도메인 목록에서 신뢰할 수 있는 도메인을 추가하거나 제거하거나 현재 목록을 수정할 수 있습니다. 기본 설정 신뢰할 수 있는 도메인 목록을 구성하는 경우 다중 도메인 이름 매핑 검색을 수행할 때 검색된 양방향 신뢰할 수 있는 도메인 대신 이 목록이 사용됩니다.

이 작업에 대해

- 기존 목록에 신뢰할 수 있는 도메인을 추가하는 경우 새 목록이 기존 목록과 병합되고 끝에 새 항목이 추가됩니다 신뢰할 수 있는 도메인은 신뢰할 수 있는 도메인 목록에 나타나는 순서대로 검색됩니다.
- 기존 목록에서 신뢰할 수 있는 도메인을 제거하고 목록을 지정하지 않는 경우 지정된 SVM(스토리지 가상 머신)에 대한 신뢰할 수 있는 전체 도메인 목록이 제거됩니다.
- 신뢰할 수 있는 도메인의 기존 목록을 수정하면 새 목록이 기존 목록을 덮어씁니다.

> ⓘ 선호하는 트러스트된 도메인 목록에 양방향 트러스트된 도메인만 입력해야 합니다. 기본 도메인 목록에 아웃바운드 또는 인바운드 트러스트 도메인을 입력할 수 있지만 다중 도메인 이름 매핑 검색을 수행할 때는 사용되지 않습니다. ONTAP는 단방향 도메인의 항목을 건너뛰고 목록에서 다음 양방향 신뢰할 수 있는 도메인으로 이동합니다.

단계

1. 다음 작업 중 하나를 수행합니다.

기본 설정 신뢰할 수 있는 도메인 목록을 사용하여 다음을 수행하려면...	명령 사용...
신뢰할 수 있는 도메인을 목록에 추가합니다	'vserver cifs domain name-mapping-search add-vserver_vserver_name_-trusted-domain FQDN,...'
목록에서 신뢰할 수 있는 도메인을 제거합니다	'vserver cifs domain name-mapping-search remove-vserver_vserver_name_[-trusted-domain FQDN,...]'
기존 목록을 수정합니다	'vserver cifs domain name-mapping-search modify -vserver_vserver_name_-trusted-domain FQDN,...'

예

다음 명령을 실행하면 SVM VS1 에서 사용하는 신뢰할 수 있는 도메인 2개(cifs1.example.com 및 cifs2.example.com 추가할 수 있습니다.

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

다음 명령을 실행하면 SVM VS1 에서 사용되는 목록에서 신뢰할 수 있는 도메인 2개가 제거됩니다.

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

다음 명령을 실행하면 SVM VS1 에서 사용하는 신뢰할 수 있는 도메인 목록이 수정됩니다. 새 목록이 원본 목록을 대체합니다.

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

관련 정보

기본 설정 신뢰할 수 있는 도메인 목록에 대한 정보를 표시합니다

기본 설정 신뢰할 수 있는 **ONTAP SMB** 도메인 목록에 대한 정보를 표시합니다

신뢰할 수 있는 도메인이 기본 설정된 신뢰할 수 있는 도메인 목록에 있는지, 다중 도메인 이름 매핑 검색이 설정된 경우 검색 순서에 대한 정보를 표시할 수 있습니다. 자동으로 검색된 신뢰할 수 있는 도메인 목록을 사용하는 대신 기본 설정 신뢰할 수 있는 도메인 목록을 구성할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

다음에 대한 정보를 표시하려면...	명령 사용...
SVM(스토리지 가상 머신)별로 그룹화된 클러스터의 모든 기본 신뢰할 수 있는 도메인	'vserver cifs domain name-mapping-search show'
지정된 SVM에서 선호 트러스트된 도메인 모두	'vserver cifs domain name-mapping-search show -vserver_vserver_name_'

다음 명령을 실행하면 클러스터의 모든 기본 설정 신뢰할 수 있는 도메인에 대한 정보가 표시됩니다.

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ----------------------------------
vs1             CIFS1.EXAMPLE.COM
```

관련 정보

선호하는 목록에서 신뢰할 수 있는 도메인을 추가, 제거 또는 교체합니다.

SMB 공유를 생성하고 구성합니다

ONTAP SMB 공유 생성 및 구성에 대해 자세히 알아보십시오

사용자와 애플리케이션이 SMB를 통해 CIFS 서버의 데이터를 액세스하려면 먼저 볼륨의 명명된 액세스 지점인 SMB 공유를 생성하고 구성해야 합니다. 공유 매개 변수를 지정하고 속성을 공유하여 공유를 사용자 지정할 수 있습니다. 언제든지 기존 공유를 수정할 수 있습니다.

SMB 공유를 생성할 때 ONTAP는 모든 사용자에 대한 모든 권한 권한이 있는 공유에 대한 기본 ACL을 생성합니다.

SMB 공유는 스토리지 가상 머신(SVM)의 CIFS 서버에 연결됩니다. SVM이 삭제되거나 SMB 공유가 연결된 CIFS 서버가 SVM에서 삭제된 경우 SMB 공유가 삭제됩니다. SVM에서 CIFS 서버를 다시 생성하는 경우 SMB 공유를 다시 생성해야 합니다.

관련 정보

- 로컬 사용자 및 그룹에 대해 알아보세요
- "Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성"
- 볼륨에서 파일 이름 번역을 위한 문자 매핑 구성

기본 관리 ONTAP SMB 공유에 대해 알아봅니다

SVM(스토리지 가상 시스템)에서 CIFS 서버를 생성하면 기본 관리 공유가 자동으로 생성됩니다. 이러한 기본 공유가 무엇이고 어떻게 사용되는지 이해해야 합니다.

ONTAP는 CIFS 서버를 생성할 때 다음과 같은 기본 관리 공유를 생성합니다.

ONTAP 9.8부터 관리자$ 공유는 기본적으로 더 이상 생성되지 않습니다.

- IPC$
- 관리 비용(ONTAP 9.7 이하 버전에만 해당)
- c$

$ 문자로 끝나는 공유는 숨겨진 공유이므로 기본 관리 공유는 내 컴퓨터에서 표시되지 않지만 공유 폴더를 사용하여 볼 수 있습니다.

IPC$** 및 **admin$ 기본 공유가 사용되는 방법입니다

IPC$ 및 admin$ 공유는 ONTAP에서 사용되며 Windows 관리자가 SVM에 상주하는 데이터에 액세스하는 데 사용할 수 없습니다.

- IPC$ 공유입니다

  IPC$ 공유는 프로그램 간 통신에 필수적인 명명된 파이프를 공유하는 리소스입니다. IPC$ 공유는 컴퓨터의 원격 관리 및 컴퓨터의 공유 리소스를 볼 때 사용됩니다. IPC$ 공유의 공유 설정, 공유 속성 또는 ACL은 변경할 수 없습니다. IPC$ 공유의 이름을 바꾸거나 삭제할 수도 없습니다.

- 관리 비용 공유(ONTAP 9.7 이하만 해당)

  ⓘ ONTAP 9.8부터 관리자$ 공유는 기본적으로 더 이상 생성되지 않습니다.

  SVM의 원격 관리 중에 admin$ 공유가 사용됩니다. 이 리소스의 경로는 항상 SVM 루트로 연결되는 경로입니다. admin$ 공유에 대한 공유 설정, 공유 속성 또는 ACL은 변경할 수 없습니다. admin$ 공유의 이름을 바꾸거나 삭제할 수도 없습니다.

c$ 기본 공유가 사용되는 방식

c$ 공유는 클러스터 또는 SVM 관리자가 SVM 루트 볼륨에 액세스하고 관리하는 데 사용할 수 있는 관리 공유입니다.

c$ 공유의 특징은 다음과 같습니다.

- 이 공유의 경로는 항상 SVM 루트 볼륨의 경로이며 수정할 수 없습니다.
- c$ 공유의 기본 ACL은 Administrator/Full Control입니다.

  이 사용자는 BUILTIN\administrator입니다. 기본적으로 BUILTIN\ 관리자는 공유에 매핑하고 매핑된 루트 디렉토리에서 파일 및 폴더를 보거나, 만들거나, 수정하거나, 삭제할 수 있습니다. 이 디렉터리의 파일과 폴더를 관리할 때는 주의해야 합니다.

- c$ 공유의 ACL을 변경할 수 있습니다.
- c$ 공유 설정을 변경하고 속성을 공유할 수 있습니다.
- c$ 공유를 삭제할 수 없습니다.
- SVM 관리자는 네임스페이스 접합을 교차하여 매핑된 c$ 공유에서 나머지 SVM 네임스페이스에 액세스할 수 있습니다.
- c$ 공유는 Microsoft 관리 콘솔을 사용하여 액세스할 수 있습니다.

관련 정보

Windows 보안 탭을 사용하여 고급 파일 권한 구성

SMB 서버에서 SMB 공유를 생성할 때는 ONTAP 공유 이름 지정 요구 사항을 염두에 두어야 합니다.

ONTAP의 공유 명명 규칙은 Windows의 명명 규칙과 동일하며 다음과 같은 요구 사항을 포함합니다.

- 각 공유의 이름은 SMB 서버에 대해 고유해야 합니다.
- 공유 이름은 대/소문자를 구분하지 않습니다.
- 최대 공유 이름 길이는 80자입니다.
- 유니코드 공유 이름이 지원됩니다.
- $ 문자로 끝나는 공유 이름은 숨겨진 공유입니다.
- ONTAP 9.7 이전 버전의 경우 admin$, ipc$ 및 c$ 관리 공유가 모든 CIFS 서버에서 자동으로 생성되며 예약된 공유 이름이 됩니다. ONTAP 9.8부터는 관리자$ 공유가 더 이상 자동으로 생성되지 않습니다.
- 공유를 생성할 때 공유 이름 ONTAP_admin$을(를) 사용할 수 없습니다.
- 공백이 포함된 공유 이름이 지원됩니다.
  - 공유 이름의 첫 문자 또는 마지막 문자로 공백을 사용할 수 없습니다.
  - 공백이 포함된 공유 이름은 따옴표로 묶어야 합니다.

    작은따옴표는 공유 이름의 일부로 간주되며 따옴표 대신 사용할 수 없습니다.

- SMB 공유의 이름을 지정할 경우 다음과 같은 특수 문자가 지원됩니다.

```
! @ # $ % & ' _ - . ~ ( ) { }
```

- SMB 공유의 이름을 지정할 때 다음 특수 문자는 지원되지 않습니다.

```
** [ ] " / \ : ; | < > , ? * =
```

멀티 프로토콜 환경에서 공유를 생성할 때의 **ONTAP SMB** 디렉토리 대소문자 구분 요구사항에 대해 알아보십시오

8.3 명명 체계가 사용되는 SVM에서 공유를 생성하여 이름 간 사례만 차이가 나는 디렉토리 이름을 구별할 경우, 클라이언트가 원하는 디렉토리 경로에 연결되도록 공유 경로에 8.3 이름을 사용해야 합니다.

다음 예에서는 Linux 클라이언트에 ""testdir"" 및 ""testdir""이라는 이름의 디렉토리 두 개가 생성되었습니다. 디렉토리가 포함된 볼륨의 연결 경로는 `/home'입니다. 첫 번째 출력은 Linux 클라이언트에서 출력되고 두 번째 출력은 SMB 클라이언트에서 출력됩니다.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

두 번째 디렉토리에 공유를 생성할 때 공유 경로에 8.3 이름을 사용해야 합니다. 이 예에서 첫 번째 디렉토리의 공유 경로는 "/home/testdir"이고 두 번째 디렉토리의 공유 경로는 "/home/TESTDI~1"입니다.

SMB 공유 속성을 사용합니다

ONTAP SMB 공유 속성 사용에 대해 자세히 알아보십시오

SMB 공유의 속성을 사용자 지정할 수 있습니다.

사용 가능한 공유 속성은 다음과 같습니다.

공유 속성	설명
oplocks	이 속성은 공유에서 클라이언트 측 캐시라고도 하는 편의적 잠금을 사용하도록 지정합니다.
"탐색 가능"	이 속성을 사용하면 Windows 클라이언트가 공유를 탐색할 수 있습니다.
'하울스냅샷'	이 속성은 클라이언트가 스냅샷을 보고 탐색할 수 있도록 지정합니다.
'변상강화하는'	이 속성은 공유에서 변경 통지 요청을 지원하도록 지정합니다. SVM에서 공유하면 기본 초기 속성이 됩니다.
'attributecache	이 속성을 사용하면 SMB 공유의 파일 속성 캐싱을 통해 속성에 더 빠르게 액세스할 수 있습니다. 기본값은 특성 캐싱을 사용하지 않는 것입니다. 이 속성은 SMB 1.0을 통해 공유에 연결하는 클라이언트가 있는 경우에만 사용해야 합니다. 클라이언트가 SMB 2.x 또는 SMB 3.0을 통해 공유에 연결하는 경우에는 이 공유 속성을 사용할 수 없습니다.

공유 속성	설명
"계속 사용할 수 있습니다.	이 속성을 사용하면 SMB 클라이언트가 지속적으로 파일을 열 수 있습니다. 이렇게 열린 파일은 페일오버 및 반환과 같은 운영 중단 이벤트로부터 보호됩니다.
브랜치캐시	이 속성은 클라이언트가 이 공유 내의 파일에 대해 BranchCache 해시를 요청할 수 있도록 공유를 지정합니다. 이 옵션은 CIFS BranchCache 구성에서 ""공유당""을 운영 모드로 지정한 경우에만 유용합니다.
'액세스 기반 열거'	이 속성은 이 공유에서 *Access* 기반 열거(ABE)를 사용하도록 지정합니다. 개별 사용자의 액세스 권한에 따라 사용자가 ABE로 필터링된 공유 폴더를 볼 수 있으므로 사용자에게 액세스 권한이 없는 폴더 또는 기타 공유 리소스를 표시할 수 없습니다.
네임스페이스-캐싱	이 속성은 이 공유에 연결하는 SMB 클라이언트가 CIFS 서버가 반환하는 디렉터리 열거 결과를 캐시할 수 있도록 지정함으로써 성능을 향상시킬 수 있습니다. 기본적으로 SMB 1 클라이언트는 디렉터리 열거 결과를 캐시하지 않습니다. SMB 2 및 SMB 3 클라이언트는 기본적으로 캐시 디렉토리 열거 결과를 제공하므로 이 공유 속성을 지정하면 SMB 1 클라이언트 연결에만 성능 이점이 있습니다.
'암호화-데이터'	이 속성은 이 공유에 액세스할 때 SMB 암호화를 사용하도록 지정합니다. SMB 데이터에 액세스할 때 암호화를 지원하지 않는 SMB 클라이언트는 이 공유에 액세스할 수 없습니다.

기존 **ONTAP SMB** 공유에서 공유 속성을 추가하거나 제거합니다

공유 속성을 추가하거나 제거하여 기존 SMB 공유를 사용자 지정할 수 있습니다. 이 기능은 환경의 변화하는 요구 사항에 맞게 공유 구성을 변경하려는 경우에 유용합니다.

시작하기 전에

수정할 속성이 있는 공유가 있어야 합니다.

이 작업에 대해

공유 속성 추가 지침:

- 쉼표로 구분된 목록을 사용하여 하나 이상의 공유 속성을 추가할 수 있습니다.
- 이전에 지정한 공유 속성은 그대로 유지됩니다.

  새로 추가된 속성은 기존 공유 속성 목록에 추가됩니다.

- 공유에 이미 적용된 공유 속성에 새 값을 지정하면 새로 지정한 값이 원래 값을 대체합니다.

- 'vserver cifs share properties add' 명령을 사용하여 공유 속성을 제거할 수 없습니다.

  'vserver cifs share properties remove' 명령을 사용하여 공유 속성을 제거할 수 있습니다.

공유 속성 제거 지침:

- 쉼표로 구분된 목록을 사용하여 하나 이상의 공유 속성을 제거할 수 있습니다.
- 이전에 지정했지만 제거하지 않은 공유 속성은 그대로 유지됩니다.

단계

1. 적절한 명령을 입력합니다.

원하는 작업	명령 입력...
공유 속성 추가	'vserver cifs 공유 속성 add-vserver_vserver_name_-share-name_share_name_-share-properties_,...'
공유 속성을 제거합니다	'vserver CIFS 공유 속성 remove-vserver_vserver_name_-share-name_share_name_-share-properties_properties_,...'

2. 공유 속성 설정을 확인합니다. 'vserver cifs share show -vserver vserver_name -share-name share_name'

예

다음 명령을 실행하면 SVM VS1 에서 "shhowsnapshot" 공유 속성이 "share1"이라는 공유에 추가됩니다.

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

다음 명령을 실행하면 SVM VS1 의 "shay2"라는 공유에서 탐색 가능한 공유 속성이 제거됩니다.

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share    Path       Properties   Comment    ACL
---------  ------   --------   ----------   --------   -----------
vs1        share2   /share2    oplocks      -          Everyone / Full
Control
                               changenotify
```

관련 정보

공유 관리를 위한 명령

force-group 공유 설정을 사용하여 **ONTAP SMB** 사용자 액세스를 최적화합니다

ONTAP 명령줄에서 UNIX 효과적인 보안이 설정된 데이터에 대한 공유를 생성할 때 해당 공유의 SMB 사용자가 생성한 모든 파일이 UNIX 그룹 데이터베이스에서 미리 정의된 그룹이어야 하는 _force-group_이라는 동일한 그룹에 속하도록 지정할 수 있습니다. force-group을 사용하면 다양한 그룹에 속한 SMB 사용자가 파일에 쉽게 액세스할 수 있습니다.

강제 그룹 지정은 공유가 UNIX 또는 혼합 qtree에 있는 경우에만 의미가 있습니다. 이러한 공유의 파일에 대한 액세스는 UNIX GID가 아닌 Windows 권한에 의해 결정되므로 NTFS 볼륨이나 qtree의 공유에 대해 강제 그룹을 설정할 필요가 없습니다.

공유에 대해 force-group이 지정된 경우 공유의 다음 내용이 적용됩니다.

- 이 공유에 액세스하는 force-group의 SMB 사용자는 force-group의 GID로 일시적으로 변경됩니다.

  이 GID를 사용하면 주 GID 또는 UID로 정상적으로 액세스할 수 없는 이 공유의 파일에 액세스할 수 있습니다.

- SMB 사용자가 생성한 이 공유의 모든 파일은 파일 소유자의 기본 GID에 관계없이 동일한 강제 그룹에 속합니다.

SMB 사용자가 NFS에서 생성된 파일에 액세스하려고 하면 SMB 사용자의 기본 GID가 액세스 권한을 결정합니다.

force-group은 NFS 사용자가 이 공유의 파일에 액세스하는 방법에 영향을 주지 않습니다. NFS에서 생성된 파일은 파일 소유자로부터 GID를 가져옵니다. 액세스 권한 결정은 파일에 액세스하려는 NFS 사용자의 UID 및 기본 GID를 기반으로 합니다.

force-group을 사용하면 다양한 그룹에 속한 SMB 사용자가 파일에 쉽게 액세스할 수 있습니다. 예를 들어 회사 웹 페이지를 저장하고 엔지니어링 및 마케팅 부서의 사용자에게 쓰기 권한을 부여하기 위해 공유를 만들고 ""webgroup1"" 그룹에 쓰기 권한을 부여할 수 있습니다. 강제 그룹 때문에 이 공유에 있는 SMB 사용자가 만든 모든 파일은 ""webgroup1"" 그룹의 소유입니다. 또한 공유에 액세스할 때 ""webgroup1"" 그룹의 GID가 자동으로 할당됩니다. 따라서 엔지니어링 및 마케팅 부서에서 사용자의 액세스 권한을 관리할 필요 없이 모든 사용자가 이 공유에 쓸 수 있습니다.

관련 정보

강제 그룹 공유 설정으로 공유 만들기

UNIX 파일 보안이 설정된 볼륨 또는 Qtree에서 데이터에 액세스하는 SMB 사용자가 ONTAP 동일한 UNIX 그룹에 속한 것으로 간주하도록 하려면 force-group 공유 설정을 사용하여 SMB 공유를 생성할 수 있습니다.

단계

1. SMB 공유:'vserver cifs share create-vserver_name_-share-name_share_name_-path path path -force -group-for-create_unix_group_name_'을 생성합니다

   공유의 UNC 경로('\\servername\sharename\filepath')에 256자 이상(UNC 경로의 초기 ""\"" 제외)이 포함되어 있으면 Windows 속성 상자의 * 보안 * 탭을 사용할 수 없습니다. 이것은 ONTAP 문제가 아니라 Windows 클라이언트 문제입니다. 이 문제를 방지하려면 256자를 초과하는 UNC 경로를 사용하여 공유를 생성하지 마십시오.

   공유가 생성된 후 force 그룹을 제거하려면 언제든지 공유를 수정하고 빈 문자열(""")을 "-force-group-for-create" 매개 변수의 값으로 지정할 수 있습니다. 공유를 수정하여 강제 그룹을 제거하는 경우 이 공유에 대한 모든 기존 연결은 이전에 설정된 강제 그룹을 기본 GID로 계속 설정합니다.

예

다음 명령을 실행하면 "/Corp/CompanyInfo" 디렉토리에 웹에서 액세스할 수 있는 ""웹 페이지" 공유가 생성되며, 이 디렉토리에서 SMB 사용자가 생성한 모든 파일이 webgroup1 그룹에 할당됩니다.

'vserver cifs share create-vserver vs1-share-name povp-path/corp/CompanyInfo-force-group-for-create webgroup1'

관련 정보

강제 그룹 공유 설정을 사용하여 사용자 액세스 최적화

MMC를 사용하여 **ONTAP SMB** 공유에 대한 정보를 봅니다

SVM에서 SMB 공유에 대한 정보를 확인하고 MMC(Microsoft Management Console)를 사용하여 일부 관리 작업을 수행할 수 있습니다. 공유를 보려면 먼저 MMC를 SVM에 연결해야 합니다.

이 작업에 대해

MMC를 사용하여 SVM에 포함된 공유에 대해 다음 작업을 수행할 수 있습니다.

- 공유 보기
- 활성 세션을 봅니다
- 열린 파일을 봅니다
- 시스템의 세션, 파일 및 트리 연결 목록을 열거합니다
- 시스템에서 열려 있는 파일을 닫습니다
- 열려 있는 세션을 닫습니다
- 공유 생성/관리

이전 기능에 의해 표시되는 뷰는 특정 노드에 한정되며 클러스터에는 해당되지 않습니다. 따라서 MMC를 사용하여 SMB 서버 호스트 이름(즉, cifs01.domain.local)에 연결하면 클러스터 내의 단일 LIF로 DNS를 설정한 방법에 따라 라우팅됩니다.

ONTAP용 MMC에서는 다음 기능이 지원되지 않습니다.

- 새 로컬 사용자/그룹을 생성합니다
- 기존 로컬 사용자/그룹 관리/보기
- 이벤트 또는 성능 로그 보기
- 스토리지
- 서비스 및 애플리케이션

작업이 지원되지 않는 경우, remote procedure call failed' 오류가 발생할 수 있습니다.

"FAQ: ONTAP에서 Windows MMC 사용"

단계

1. Windows 서버에서 컴퓨터 관리 MMC를 열려면 * 제어판 * 에서 * 관리 도구 * > * 컴퓨터 관리 * 를 선택합니다.
2. 작업 * > * 다른 컴퓨터에 연결 * 을 선택합니다.

   컴퓨터 선택 대화 상자가 나타납니다.

3. 스토리지 시스템의 이름을 입력하거나 * Browse * 를 클릭하여 스토리지 시스템을 찾습니다.
4. 확인 * 을 클릭합니다.

   MMC를 SVM에 연결합니다.

5. 탐색 창에서 * 공유 폴더 * > * 공유 * 를 클릭합니다.

   SVM의 공유 목록이 오른쪽 표시 창에 표시됩니다.

6. 공유의 공유 속성을 표시하려면 공유를 두 번 클릭하여 * 속성 * 대화 상자를 엽니다.
7. MMC를 사용하여 스토리지 시스템에 접속할 수 없는 경우 스토리지 시스템에서 다음 명령 중 하나를 사용하여 BUILTIN\Administrators 그룹 또는 BUILTIN\Power Users 그룹에 사용자를 추가할 수 있습니다.

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

SMB 공유를 관리하기 위한 **ONTAP** 명령

'vserver cifs share' 및 'vserver cifs share properties' 명령을 사용하여 SMB 공유를 관리할 수 있습니다.

원하는 작업	이 명령 사용...
SMB 공유를 생성합니다	'vserver cifs share create
SMB 공유를 표시합니다	'vserver cifs share show'를 선택합니다
SMB 공유를 수정합니다	'vserver cifs share modify'를 선택합니다
SMB 공유를 삭제합니다	'vserver cifs share delete
기존 공유에 공유 속성을 추가합니다	'vserver cifs share properties add'를 선택합니다
기존 공유에서 공유 속성을 제거합니다	'vserver cifs share properties remove(가상 CIFS 공유 속성 제거
공유 속성에 대한 정보를 표시합니다	'vserver cifs share properties show'를 선택합니다

에 대한 자세한 내용은 `vserver cifs` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 공유 ACL을 사용하여 파일 액세스 보호

ONTAP SMB 공유 레벨 ACL 관리에 대해 자세히 알아보십시오

공유 수준 ACL을 변경하여 사용자에게 공유에 대한 액세스 권한을 더 많이 또는 덜 부여할 수 있습니다. Windows 사용자 및 그룹 또는 UNIX 사용자 및 그룹을 사용하여 공유 수준 ACL을 구성할 수 있습니다.

기본적으로 공유 수준 ACL은 Everyone이라는 표준 그룹에 모든 권한을 부여합니다. ACL에 대한 모든 제어 기능은 도메인 및 모든 신뢰할 수 있는 도메인의 모든 사용자가 공유에 대한 모든 액세스 권한을 갖는다는 것을 의미합니다. Windows 클라이언트의 Microsoft Management Console(MMC)이나 ONTAP 명령줄을 사용하여 공유 수준 ACL에 대한 액세스 수준을 제어할 수 있습니다. "공유 액세스 제어 목록 만들기"..

MMC를 사용할 때 다음 지침이 적용됩니다.

- 지정된 사용자 및 그룹 이름은 Windows 이름이어야 합니다.
- Windows 권한만 지정할 수 있습니다.

ONTAP 명령줄을 사용할 때 다음 지침이 적용됩니다.

- 지정된 사용자 및 그룹 이름은 Windows 이름 또는 UNIX 이름일 수 있습니다.

  ACL을 생성하거나 수정할 때 사용자 및 그룹 유형을 지정하지 않으면 기본 유형은 Windows 사용자 및 그룹입니다.

- Windows 권한만 지정할 수 있습니다.

ONTAP SMB 공유 액세스 제어 목록을 생성합니다

SMB 공유에 대한 ACL(액세스 제어 목록)을 생성하여 공유 권한을 구성하면 사용자 및 그룹의

공유에 대한 액세스 수준을 제어할 수 있습니다.

이 작업에 대해

로컬 또는 도메인 Windows 사용자 또는 그룹 이름 또는 UNIX 사용자 또는 그룹 이름을 사용하여 공유 수준 ACL을 구성할 수 있습니다.

새 ACL을 생성하기 전에 보안 위험을 야기시키는 기본 공유 ACL 'Everyone/Full Control'을 삭제해야 합니다.

워크그룹 모드에서 로컬 도메인 이름은 SMB 서버 이름입니다.

단계

1. 기본 공유 ACL인 'vserver cifs share access-control delete-vserver <vserver_name>-share <share_name>-user-or-group everyone'을 삭제하십시오
2. 새 ACL 구성:

을 사용하여 **ACL**을 구성하려면…	명령 입력…
Windows 사용자	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`
Windows 그룹	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`
Unix 사용자입니다	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
Unix 그룹	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. 'vserver cifs share access-control show' 명령을 사용하여 공유에 적용된 ACL이 올바른지 확인하십시오.

예

다음 명령을 실행하면 이 표시됩니다 `Change` "vs1.example.com" SVM에서 "Sales" 공유를 위한 "Sales Team" Windows 그룹에 대한 권한:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

다음 명령을 실행하면 `Read` "vs2.example.com" SVM의 "eng" 공유에 대한 "engineering" UNIX 그룹에 대한 권한이 부여됩니다.

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering              unix-group  Read
```

다음 명령은 `Change` "Tiger Team"이라는 로컬 Windows 그룹에 `Full_Control` 대한 권한을 부여하고 "VS1" SVM에서 "datavol5" 공유에 대해 "Sue Chang"이라는 로컬 Windows 사용자에게 권한을 부여합니다.

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

SMB 공유 액세스 제어 목록을 관리하기 위한 **ONTAP** 명령

SMB ACL(액세스 제어 목록)을 관리하기 위한 명령을 알아야 합니다. 여기에는 ACL 생성, 표시, 수정 및 삭제가 포함됩니다.

원하는 작업	이 명령 사용...
새 ACL을 생성합니다	'vserver cifs share access-control create'
ACL을 표시합니다	'vserver cifs share access-control show'를 참조하십시오
ACL을 수정합니다	'vserver cifs share access-control modify'를 참조하십시오
ACL을 삭제한다	'vserver cifs share access-control delete'

파일 권한을 사용하여 파일 액세스를 보호합니다

ONTAP SMB SVM에 대한 **Windows** 보안 탭을 사용하여 고급 **NTFS** 파일 권한 구성

Windows 속성 창의 * Windows 보안 * 탭을 사용하여 파일 및 폴더에 대한 표준 NTFS 파일 권한을 구성할 수 있습니다.

시작하기 전에

이 작업을 수행하는 관리자는 선택한 개체에 대한 권한을 변경할 수 있는 충분한 NTFS 권한이 있어야 합니다.

이 작업에 대해

NTFS 파일 사용 권한 구성은 NTFS 보안 설명자와 연결된 NTFS DACL(임의 액세스 제어 목록)에 항목을 추가하여 Windows 호스트에서 수행됩니다. 그런 다음 보안 설명자가 NTFS 파일 및 디렉터리에 적용됩니다. 이러한 작업은 Windows GUI에서 자동으로 처리됩니다.

단계

1. Windows 탐색기의 * Tools * 메뉴에서 * Map network drive * 를 선택합니다.
2. 네트워크 드라이브 연결 * 대화 상자를 완료합니다.

   a. 드라이브 * 문자를 선택합니다.

   b. 폴더 * 상자에 사용 권한을 적용할 데이터와 공유 이름을 포함하는 공유가 포함된 CIFS 서버 이름을 입력합니다.

      CIFS 서버 이름이 ""cifs_server""이고 공유 이름이 "share1"인 경우 "\\cifs_server\share1"을 입력해야 합니다.

      CIFS 서버 이름 대신 CIFS 서버에 대한 데이터 인터페이스의 IP 주소를 지정할 수 있습니다.

   c. 마침 * 을 클릭합니다.

   선택한 드라이브가 마운트되고 공유 내에 포함된 파일 및 폴더를 표시하는 Windows 탐색기 창이 준비됩니다.

3. NTFS 파일 권한을 설정할 파일 또는 디렉터리를 선택합니다.
4. 파일 또는 디렉터리를 마우스 오른쪽 단추로 클릭한 다음 * 속성 * 을 선택합니다.
5. 보안 * 탭을 선택합니다.

   보안* 탭에는 NTFS 권한이 설정된 사용자 및 그룹 목록이 표시됩니다. [사용 권한] 상자에 선택한 각 사용자 또는 그룹에 대해 적용되는 허용 및 거부 권한 목록이 표시됩니다.

6. 고급 * 을 클릭합니다.

   Windows 속성 창에는 사용자 및 그룹에 할당된 기존 파일 권한에 대한 정보가 표시됩니다.

7. 권한 변경 * 을 클릭합니다.

   사용 권한 창이 열립니다.

8. 원하는 작업을 수행합니다.

원하는 작업	다음을 수행합니다.
새 사용자 또는 그룹에 대한 고급 NTFS 권한을 설정합니다	a. 추가 * 를 클릭합니다. b. 선택할 개체 이름 입력 * 상자에 추가할 사용자 또는 그룹의 이름을 입력합니다. c. 확인 * 을 클릭합니다.

원하는 작업	다음을 수행합니다.
사용자 또는 그룹의 고급 NTFS 권한을 변경합니다	a. 사용 권한 항목: * 상자에서 고급 사용 권한을 변경할 사용자 또는 그룹을 선택합니다. b. 편집 * 을 클릭합니다.
사용자 또는 그룹에 대한 고급 NTFS 권한을 제거합니다	a. 사용 권한 항목: * 상자에서 제거할 사용자 또는 그룹을 선택합니다. b. 제거 * 를 클릭합니다. c. 13단계로 건너뜁니다.

새 사용자 또는 그룹에 고급 NTFS 권한을 추가하거나 기존 사용자 또는 그룹에 대한 NTFS 고급 권한을 변경하는 경우 <Object>의 권한 항목 상자가 열립니다.

9. 적용 대상 * 상자에서 이 NTFS 파일 권한 항목을 적용할 방법을 선택합니다.

   단일 파일에 NTFS 파일 권한을 설정하는 경우 * 적용 대상 * 상자가 활성화되지 않습니다. 적용 대상 * 설정은 기본적으로 * 이 개체만 * 으로 설정됩니다.

10. 사용 권한 * 상자에서 이 개체에 설정할 고급 권한에 대해 * 허용 * 또는 * 거부 * 상자를 선택합니다.

    - 지정된 액세스를 허용하려면 * 허용 * 상자를 선택합니다.
    - 지정된 액세스를 허용하지 않으려면 * Deny * 상자를 선택합니다. 다음과 같은 고급 권한에 대한 권한을 설정할 수 있습니다.
    - * 완전 제어 *

      이 고급 권한을 선택하면 다른 모든 고급 권한이 자동으로 선택됩니다(권한 허용 또는 거부).

    - * 폴더 트래버스/파일 실행 *
    - * 폴더 나열/데이터 읽기 *
    - * 읽기 속성 *
    - * 확장 속성 읽기 *
    - * 파일 생성/데이터 쓰기 *
    - * 폴더 생성/데이터 추가 *
    - * 속성 쓰기 *
    - * 확장 속성 쓰기 *
    - * 하위 폴더 및 파일 삭제 *
    - * 삭제 *
    - * 읽기 권한 *
    - * 권한 변경 *
    - * 소유권 가져오기 *

고급 사용 권한 상자 중 하나를 선택할 수 없는 경우 상위 개체에서 사용 권한이 상속되기 때문입니다.

11. 이 개체의 하위 폴더와 파일이 이러한 권한을 상속하도록 하려면 * 이 컨테이너 내의 개체 및/또는 컨테이너에 이 권한을 적용합니다 * 상자를 선택합니다.
12. 확인 * 을 클릭합니다.
13. NTFS 사용 권한 추가, 제거 또는 편집을 마친 후 이 개체에 대한 상속 설정을 지정합니다.
    - 이 개체의 부모 * 상자에서 상속 가능한 사용 권한 포함 을 선택합니다.

      이것이 기본값입니다.
    - 모든 자식 개체 권한을 이 개체의 상속 가능한 권한으로 바꾸기 * 상자를 선택합니다.

      단일 파일에 NTFS 파일 권한을 설정하는 경우 사용 권한 상자에 이 설정이 없습니다.

      이 설정을 선택할 때는 주의하십시오. 이 설정은 모든 자식 개체에 대한 기존 사용 권한을 모두 제거하고 이 개체의 사용 권한 설정으로 바꿉니다. 제거하지 않으려는 사용 권한을 실수로 제거할 수 있습니다. 혼합 보안 형식 볼륨 또는 qtree에서 사용 권한을 설정할 때는 특히 중요합니다. 자식 개체에 UNIX 효과적인 보안 스타일이 있는 경우 이러한 자식 개체에 NTFS 권한을 전파하면 ONTAP에서 이러한 개체를 UNIX 보안 스타일에서 NTFS 보안 스타일로 변경하고 해당 자식 개체에 대한 모든 UNIX 권한이 NTFS 권한으로 대체됩니다.
    - 두 상자를 모두 선택합니다.
    - 어느 상자도 선택하지 않습니다.
14. 확인 * 을 클릭하여 * 권한 * 상자를 닫습니다.
15. [확인]을 클릭하여 <개체>* 상자의 * 고급 보안 설정을 닫습니다.

    고급 NTFS 권한을 설정하는 방법에 대한 자세한 내용은 Windows 설명서를 참조하십시오.

관련 정보

- 서버에 NTFS 보안 설명자 만들기
- NTFS 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다
- 혼합 보안 형식 볼륨의 파일 보안에 대한 정보를 표시합니다
- UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다

SMB NTFS 파일 권한에 대한 **ONTAP** 명령

ONTAP CLI를 사용하여 파일 및 디렉토리에 대한 NTFS 파일 권한을 구성할 수 있습니다. 따라서 Windows 클라이언트에서 SMB 공유를 사용하여 데이터에 연결할 필요 없이 NTFS 파일 권한을 구성할 수 있습니다.

NTFS 보안 설명자와 연결된 NTFS DACL(임의 액세스 제어 목록)에 항목을 추가하여 NTFS 파일 권한을 구성할 수 있습니다. 그런 다음 보안 설명자가 NTFS 파일 및 디렉터리에 적용됩니다.

명령줄을 사용해서만 NTFS 파일 권한을 구성할 수 있습니다. CLI를 사용하여 NFSv4 ACL을 구성할 수 없습니다.

단계

1. NTFS 보안 설명자를 만듭니다.

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. NTFS 보안 설명자에 DACL을 추가합니다.

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. 파일/디렉토리 보안 정책을 생성합니다.

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

ONTAP SMB 서버를 통해 파일에 액세스할 때 액세스 제어를 제공하는 **UNIX** 파일 권한에 대해 알아보세요.

FlexVol 볼륨은 NTFS, UNIX 또는 MIXED의 세 가지 보안 유형 중 하나를 가질 수 있습니다. 보안 스타일에 관계없이 SMB를 통해 데이터에 액세스할 수 있지만 UNIX의 효율적인 보안을 통해 데이터에 액세스하려면 적절한 UNIX 파일 권한이 필요합니다.

SMB를 통해 데이터에 액세스할 때 사용자가 요청된 작업을 수행할 수 있는 권한이 있는지 여부를 결정할 때 여러 액세스 제어가 사용됩니다.

- 권한 내보내기

  SMB 액세스에 대한 내보내기 권한 구성은 선택 사항입니다.

- 공유 권한
- 파일 권한

  사용자가 작업을 수행하려는 데이터에 다음 유형의 파일 권한이 적용될 수 있습니다.

  - NTFS입니다
  - Unix NFSv4 ACL
  - UNIX 모드 비트

NFSv4 ACL 또는 UNIX 모드 비트 세트가 있는 데이터의 경우 데이터에 대한 파일 액세스 권한을 결정하는 데 UNIX 스타일 권한이 사용됩니다. SVM 관리자는 사용자가 원하는 작업을 수행할 권한을 갖도록 적절한 파일 권한을 설정해야 합니다.

혼합 보안 형식 볼륨의 데이터는 NTFS 또는 UNIX의 효과적인 보안 스타일을 가질 수 있습니다. 데이터에 UNIX 유효 보안 스타일이 있는 경우 데이터에 대한 파일 액세스 권한을 결정할 때 NFSv4 사용 권한 또는 UNIX 모드 비트가 사용됩니다.

DAC(Dynamic Access Control)를 사용하여 파일 액세스 보안

ONTAP SMB 서버에 대한 DAC 파일 액세스 보안에 대해 알아보세요

동적 액세스 제어를 사용하고 Active Directory에서 중앙 액세스 정책을 생성한 후 적용된 GPO(그룹 정책 개체)를 통해 SVM의 파일 및 폴더에 적용하여 액세스를 보호할 수 있습니다. 중앙 액세스 정책 스테이징 이벤트를 사용하여 변경 내용을 적용하기 전에 중앙 액세스 정책에 대한 영향을 확인할 수 있도록 감사를 구성할 수 있습니다.

CIFS 자격 증명에 추가

동적 액세스 제어 전에 CIFS 자격 증명에는 보안 주체(사용자의) ID와 Windows 그룹 구성원이 포함되어 있습니다. 동적 액세스 제어를 사용하면 디바이스 ID, 디바이스 클레임 및 사용자 클레임을 비롯한 세 가지 유형의 정보가 자격 증명에 추가됩니다.

- 장치 ID

  사용자가 로그인하는 장치의 ID 및 그룹 멤버쉽은 제외하고 사용자의 ID 정보의 아날로그.

- 장치 요청

  장치 보안 주체에 대한 어설션. 예를 들어 장치 클레임은 특정 OU의 구성원일 수 있습니다.

- 사용자 클레임

  사용자 보안 주체에 대한 어설션. 예를 들어 사용자 클레임은 AD 계정이 특정 OU의 구성원일 수 있습니다.

중앙 액세스 정책

파일에 대한 중앙 액세스 정책을 사용하면 조직에서 사용자 그룹, 사용자 클레임, 장치 클레임 및 리소스 속성을 사용하는 조건부 식을 포함하는 인증 정책을 중앙에서 배포하고 관리할 수 있습니다.

예를 들어, 비즈니스에 큰 영향을 미치는 데이터에 액세스하려면 정규직 직원이어야 하며 관리되는 장치의 데이터만 액세스할 수 있어야 합니다. 중앙 액세스 정책은 Active Directory에서 정의되고 GPO 메커니즘을 통해 파일 서버로 배포됩니다.

고급 감사를 통한 중앙 액세스 정책 스테이징

중앙 액세스 정책은 '성질'일 수 있으며, 이 경우 파일 액세스 검사 중에 "what-if" 방식으로 평가됩니다. 정책이 적용된 경우 어떤 결과가 발생했는지, 현재 구성된 것과 어떻게 다른 결과가 감사 이벤트로 기록됩니다. 이렇게 하면 관리자가 감사 이벤트 로그를 사용하여 실제로 정책을 적용하기 전에 액세스 정책 변경의 영향을 확인할 수 있습니다. 액세스 정책 변경의 영향을 평가한 후 GPO를 통해 원하는 SVM에 정책을 배포할 수 있습니다.

관련 정보

- 지원되는 GPO에 대해 알아보세요
- SMB 서버에 그룹 정책 개체를 적용하는 방법에 대해 알아보세요.
- 서버에서 GPO 지원 활성화 또는 비활성화
- GPO 구성에 대한 정보를 표시합니다
- 중앙 액세스 정책에 대한 정보를 표시합니다

- 중앙 액세스 정책 규칙에 대한 정보를 표시합니다
- 서버의 데이터를 보호하기 위해 중앙 액세스 정책을 구성합니다.
- 서버 보안에 대한 정보 표시
- "SMB 및 NFS 감사 및 보안 추적"

ONTAP SMB 서버에 지원되는 **DAC** 기능

CIFS 서버에서 DAC(동적 액세스 제어)를 사용하려면 ONTAP가 Active Directory 환경에서 동적 액세스 제어 기능을 지원하는 방법을 이해해야 합니다.

동적 액세스 제어에 지원됩니다

ONTAP는 CIFS 서버에서 동적 액세스 제어가 설정된 경우 다음 기능을 지원합니다.

기능	설명
파일 시스템에 대한 클레임입니다	청구는 사용자에 대한 일부 진실을 나타내는 간단한 이름 및 값 쌍입니다. 사용자 자격 증명에는 클레임 정보가 포함되며 파일의 보안 설명자는 클레임 검사가 포함된 액세스 검사를 수행할 수 있습니다. 따라서 관리자는 파일에 액세스할 수 있는 사용자를 보다 세밀하게 제어할 수 있습니다.
파일 액세스 검사에 대한 조건식입니다	파일의 보안 매개 변수를 수정할 때 사용자는 임의로 복잡한 조건식을 파일의 보안 설명자에 추가할 수 있습니다. 조건부 표현식에는 클레임 확인이 포함될 수 있습니다.
중앙 액세스 정책을 통해 파일 액세스를 중앙 집중식으로 제어	중앙 액세스 정책은 파일에 태그를 지정할 수 있는 Active Directory에 저장된 일종의 ACL입니다. 디스크에 있는 보안 설명자와 태그가 지정된 중앙 액세스 정책 모두의 액세스 검사가 액세스를 허용하는 경우에만 파일에 대한 액세스가 부여됩니다. 따라서 관리자는 디스크의 보안 설명자를 수정하지 않고도 중앙 위치(AD)에서 파일에 대한 액세스를 제어할 수 있습니다.
중앙 액세스 정책 스테이징	중앙 액세스 정책의 "변경"을 통해 실제 파일 액세스에 영향을 주지 않고 보안 변경 사항을 시도하는 기능을 추가하고 감사 보고서에서 변경 효과를 확인할 수 있습니다.
ONTAP CLI를 사용하여 중앙 액세스 정책 보안에 대한 정보 표시 지원	'vserver security file-directory show' 명령을 확장하여 적용된 중앙 액세스 정책에 대한 정보를 표시합니다.
중앙 액세스 정책을 포함하는 보안 추적	적용된 중앙 액세스 정책에 대한 정보가 포함된 결과를 표시하도록 'vserver security trace' 명령 제품군을 확장합니다.

동적 액세스 제어에 지원되지 않습니다

CIFS 서버에서 동적 액세스 제어가 설정된 경우 ONTAP는 다음 기능을 지원하지 않습니다.

기능	설명
NTFS 파일 시스템 객체의 자동 분류	이 확장명은 ONTAP에서 지원되지 않는 Windows 파일 분류 인프라스트럭처의 확장입니다.
중앙 액세스 정책 스테이징 이외의 고급 감사	고급 감사를 위해 중앙 액세스 정책 스테이징만 지원됩니다.

ONTAP SMB 서버에서 **DAC** 및 중앙 액세스 정책을 사용하는 방법에 대해 알아보세요.

DAC(Dynamic Access Control) 및 중앙 액세스 정책을 사용하여 CIFS 서버의 파일과 폴더를 보호할 때 고려해야 할 몇 가지 사항이 있습니다.

정책 규칙이 **DOMAIN\administrator** 사용자에게 적용되는 경우 **NFS** 액세스가 루트에 대해 거부될 수 있습니다

특정 상황에서는 루트 사용자가 액세스하려는 데이터에 중앙 액세스 정책 보안이 적용될 때 루트에 대한 NFS 액세스가 거부될 수 있습니다. 이 문제는 중앙 액세스 정책에 도메인\관리자에게 적용되는 규칙이 포함되어 있고 루트 계정이 도메인\관리자 계정에 매핑된 경우에 발생합니다.

도메인\관리자 사용자에게 규칙을 적용하는 대신 도메인\관리자 그룹과 같은 관리 권한이 있는 그룹에 규칙을 적용해야 합니다. 이렇게 하면 이 문제의 근본 영향을 받지 않고 root를 domain\administrator 계정에 매핑할 수 있습니다.

Active Directory에서 적용된 중앙 액세스 정책을 찾을 수 없는 경우 **CIFS** 서버의 **BUILTIN\Administrators** 그룹에 리소스에 대한 액세스 권한이 있습니다

CIFS 서버에 포함된 리소스에 중앙 액세스 정책이 적용될 수 있지만 CIFS 서버가 중앙 액세스 정책의 SID를 사용하여 Active Directory에서 정보를 검색하려고 하면 SID가 Active Directory의 기존 중앙 액세스 정책 SID와 일치하지 않습니다. 이러한 경우 CIFS 서버는 해당 리소스에 대한 로컬 기본 복구 정책을 적용합니다.

로컬 기본 복구 정책을 사용하면 CIFS 서버의 BUILTIN\Administrators 그룹이 해당 리소스에 액세스할 수 있습니다.

ONTAP SMB 서버에 대한 **DAC** 활성화 또는 비활성화

DAC(Dynamic Access Control)를 사용하여 CIFS 서버의 객체를 보호할 수 있는 옵션은 기본적으로 해제되어 있습니다. CIFS 서버에서 동적 액세스 제어를 사용하려면 이 옵션을 설정해야 합니다. 나중에 동적 액세스 제어를 사용하여 CIFS 서버에 저장된 객체를 보호하지 않으려는 경우 이 옵션을 해제할 수 있습니다.

Active Directory에서 동적 액세스 제어를 구성하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리 를 참조하십시오.

"Microsoft TechNet: 동적 액세스 제어 시나리오 개요"

이 작업에 대해

동적 액세스 제어가 설정되면 파일 시스템에 동적 액세스 제어 관련 항목이 있는 ACL이 포함될 수 있습니다. 동적 액세스 제어를 사용하지 않으면 현재 동적 액세스 제어 항목은 무시되고 새 항목은 허용되지 않습니다.

이 옵션은 고급 권한 수준에서만 사용할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

동적 액세스 제어를 원하는 경우…	명령 입력…
활성화됨	'vserver cifs options modify -vserver_vserver_name_-is-dac-enabled true'
사용 안 함	'vserver cifs options modify -vserver_vserver_name_-is-dac-enabled false'

3. 관리자 권한 수준으로 복귀: 'Set-Privilege admin

관련 정보

서버의 데이터를 보호하기 위해 중앙 액세스 정책을 구성합니다.

ONTAP SMB 서버에서 **DAC**가 비활성화된 경우 **DAC ACE**가 포함된 **ACL** 관리

동적 액세스 제어 ACE로 ACL이 적용된 리소스가 있고 SVM(스토리지 가상 시스템)에서 동적 액세스 제어를 사용하지 않도록 설정한 경우 해당 리소스에서 비 동적 액세스 제어 ACE를 관리하기 전에 동적 액세스 제어 ACE를 제거해야 합니다.

이 작업에 대해

동적 액세스 제어를 사용하지 않도록 설정한 후에는 기존 동적 액세스 제어 ACE를 제거하거나 기존 동적 액세스 제어 ACE를 제거해야 새로운 비 동적 액세스 제어 ACE를 추가할 수 있습니다.

일반적으로 ACL을 관리하는 데 사용하는 툴을 사용하여 이러한 단계를 수행할 수 있습니다.

단계

1. 리소스에 적용되는 동적 액세스 제어 ACE를 결정합니다.
2. 리소스에서 동적 액세스 제어 ACE를 제거합니다.
3. 리소스에서 원하는 대로 비 동적 액세스 제어 ACE를 추가하거나 제거합니다.

ONTAP SMB 서버의 데이터를 보호하기 위한 중앙 액세스 정책 구성

CIFS 서버에서 DAC(Dynamic Access Control) 활성화, Active Directory에서 중앙 액세스 정책 구성, GPO를 사용하여 Active Directory 컨테이너에 중앙 액세스 정책 적용 등 중앙 액세스 정책을 사용하여 CIFS 서버의 데이터에 안전하게 액세스하기 위해 수행해야 하는 몇 가지 단계가 있습니다. 그리고 CIFS 서버에서 GPO를 사용하도록 설정합니다.

시작하기 전에

- 중앙 액세스 정책을 사용하도록 Active Directory를 구성해야 합니다.
- 중앙 액세스 정책을 만들고 CIFS 서버가 포함된 컨테이너에 GPO를 만들고 적용하려면 Active Directory 도메인

컨트롤러에 대한 충분한 액세스 권한이 있어야 합니다.

- 필요한 명령을 실행하려면 SVM(스토리지 가상 머신)에 대한 충분한 관리 액세스 권한이 있어야 합니다.

이 작업에 대해

중앙 액세스 정책은 Active Directory의 GPO(그룹 정책 개체)에 정의되고 적용됩니다. Active Directory의 중앙 액세스 정책을 구성하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리 를 참조하십시오.

"Microsoft TechNet: 중앙 액세스 정책 시나리오"

단계

1. "vserver cifs options modify" 명령을 사용하여 아직 활성화되지 않은 SVM에서 동적 액세스 제어를 활성화하십시오.

   'vserver cifs options modify -vserver vs1-is-dac-enabled true'

2. "vserver cifs group-policy modify" 명령을 사용하여 CIFS 서버가 아직 설정되지 않은 경우 CIFS 서버에서 GPO(그룹 정책 개체)를 사용하도록 설정합니다.

   'vserver cifs group-policy modify - vserver vs1-status enabled'

3. Active Directory에 중앙 액세스 규칙 및 중앙 액세스 정책을 생성합니다.
4. GPO(그룹 정책 개체)를 만들어 Active Directory에 중앙 액세스 정책을 배포합니다.
5. CIFS 서버 컴퓨터 계정이 있는 컨테이너에 GPO를 적용합니다.
6. 'vserver cifs group-policy update' 명령을 사용하여 CIFS 서버에 적용된 GPO를 수동으로 업데이트합니다.

   'vserver cifs group-policy update-vserver vs1'을 선택합니다

7. "vserver cifs group-policy show-applied" 명령을 사용하여 GPO 중앙 액세스 정책이 CIFS 서버의 리소스에 적용되는지 확인합니다.

   다음 예에서는 기본 도메인 정책에 CIFS 서버에 적용되는 두 가지 중앙 액세스 정책이 있음을 보여 줍니다.

   'vserver cifs group-policy show-applied'

```
Vserver: vs1
-----------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
```

```
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
```

```
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

관련 정보

- SMB 서버에 그룹 정책 개체를 적용하는 방법에 대해 알아보세요.
- GPO 구성에 대한 정보를 표시합니다
- 중앙 액세스 정책에 대한 정보를 표시합니다
- 중앙 액세스 정책 규칙에 대한 정보를 표시합니다
- 서버에 대한 DAC 활성화 또는 비활성화

ONTAP SMB 서버의 DAC 보안에 대한 정보 표시

DAC(Dynamic Access Control) 보안에 대한 정보를 NTFS 볼륨과 NTFS 유효 보안 데이터가 혼합된 보안 스타일 볼륨에서 표시할 수 있습니다. 여기에는 조건부 ACE, 리소스 ACE 및 중앙 액세스 정책 ACE에 대한 정보가 포함됩니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 폴더 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver vserver_name -path path path'
세부 정보가 확장됩니다	'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true'
여기서 출력은 그룹 및 사용자 SID와 함께 표시됩니다	'vserver security file-directory show -vserver vserver_name -path path -lookup-names false'
16진수 비트 마스크가 텍스트 형식으로 변환되는 파일과 디렉토리의 파일 및 디렉토리 보안에 대해 설명합니다	'vserver security file-directory show -vserver vserver_name -path path path -텍스트 마스크 true'

예

다음 예제는 SVM VS1 경로의 동적 액세스 제어 보안 정보 /vol1 을 보여줍니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                            Vserver: vs1
                          File Path: /vol1
                File Inode Number: 112
                   Security Style: mixed
                  Effective Style: ntfs
                   DOS Attributes: 10
           DOS Attributes in Text: ----D---
           Expanded Dos Attribute: -
                     Unix User Id: 0
                    Unix Group Id: 1
                   Unix Mode Bits: 777
           Unix Mode Bits in Text: rwxrwxrwx
                             ACLs: NTFS Security Descriptor
                                   Control:0xbf14
                                   Owner:CIFS1\Administrator
                                   Group:CIFS1\Domain Admins
                                   SACL - ACEs
                                      ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                      RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                      POLICY ID-All resources - No Write-
0x0-OI|CI
                                   DACL - ACEs
                                      ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                      ALLOW-Everyone-0x1f01ff-OI|CI
                                      ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

관련 정보

- GPO 구성에 대한 정보를 표시합니다
- 중앙 액세스 정책에 대한 정보를 표시합니다
- 중앙 액세스 정책 규칙에 대한 정보를 표시합니다

ONTAP SMB 서버의 **DAC**에 대한 고려 사항 되돌리기

DAC(동적 액세스 제어)를 지원하지 않는 ONTAP 버전으로 되돌릴 경우 어떤 일이 발생할지, 되돌리기 전과 후에 무엇을 해야 하는지 알고 있어야 합니다.

하나 이상의 SVM(스토리지 가상 머신)에서 동적 액세스 제어와 동적 액세스 제어를 지원하지 않는 ONTAP 버전으로

클러스터를 되돌리려면 되돌리기 전에 다음을 수행해야 합니다.

- 클러스터에서 활성화된 모든 SVM에서 동적 액세스 제어를 해제해야 합니다.
- "file-op" 이벤트 유형만 사용하려면 "cap-staging" 이벤트 유형이 포함된 클러스터의 감사 구성을 수정해야 합니다.

동적 액세스 제어 ACE가 있는 파일 및 폴더에 대한 몇 가지 중요한 복원 고려 사항을 이해하고 이에 대한 조치를 취해야 합니다.

- 클러스터를 되돌린 경우 기존 동적 액세스 제어 ACE는 제거되지 않지만 파일 액세스 검사에서는 무시됩니다.
- 동적 액세스 제어 ACE는 재버전 후에 무시되므로 동적 액세스 제어 ACE가 있는 파일에서 파일에 대한 액세스가 변경됩니다.

  이렇게 하면 사용자가 이전에는 액세스할 수 없었던 파일에 액세스하거나 이전에 액세스할 수 없었던 파일에 액세스할 수 있습니다.

- 영향을 받는 파일에 비동적 액세스 제어 ACE를 적용하여 이전 보안 수준을 복원해야 합니다.

  되돌리기 전에 또는 다시 버전이 완료된 직후 작업을 수행할 수 있습니다.

> 동적 액세스 제어 ACE는 다시 버전 변경 후 무시되므로 영향을 받는 파일에 비동적 액세스 제어 ACE를 적용할 때 제거할 필요가 없습니다. 그러나 필요한 경우 수동으로 제거할 수 있습니다.

내보내기 정책을 사용하여 **SMB** 액세스를 보호합니다

ONTAP SMB 액세스를 통한 내보내기 정책 사용에 대해 알아보세요

SMB 서버에서 SMB 액세스에 대한 엑스포트 정책을 사용하는 경우, SMB 클라이언트에서 SVM 볼륨에 대한 액세스를 제어할 때 엑스포트 정책이 사용됩니다. 데이터에 액세스하려면 SMB 액세스를 허용하는 엑스포트 정책을 생성한 다음, SMB 공유를 포함하는 볼륨과 정책을 연결할 수 있습니다.

내보내기 정책에는 데이터에 대한 액세스가 허용되는 클라이언트와 읽기 전용 및 읽기-쓰기 액세스에 지원되는 인증 프로토콜을 지정하는 하나 이상의 규칙이 적용됩니다. 모든 클라이언트, 클라이언트 서브넷 또는 특정 클라이언트에 대한 SMB 액세스를 허용하고 Kerberos 인증, NTLM 인증 또는 데이터에 대한 읽기 전용 및 읽기-쓰기 액세스를 결정할 때 Kerberos 및 NTLM 인증을 사용하여 인증을 허용하도록 내보내기 정책을 구성할 수 있습니다.

내보내기 정책에 적용된 모든 내보내기 규칙을 처리한 후 ONTAP는 클라이언트에 액세스 권한이 부여되었는지 여부와 허용되는 액세스 수준을 결정할 수 있습니다. 내보내기 규칙은 Windows 사용자 및 그룹이 아니라 클라이언트 컴퓨터에 적용됩니다. 내보내기 규칙은 Windows 사용자 및 그룹 기반 인증 및 권한 부여를 대체하지 않습니다. 내보내기 규칙은 공유 및 파일 액세스 권한 외에도 액세스 보안의 또 다른 계층을 제공합니다.

볼륨에 대한 클라이언트 액세스를 구성하기 위해 각 볼륨에 정확히 하나의 엑스포트 정책을 연결합니다. 각 SVM에는 여러 엑스포트 정책이 포함될 수 있습니다. 따라서 여러 볼륨이 있는 SVM에 대해 다음을 수행할 수 있습니다.

- SVM의 각 볼륨에 서로 다른 엑스포트 정책을 지정하여 개별 클라이언트 액세스 제어를 SVM의 각 볼륨에 할당
- 각 볼륨에 대해 새로운 엑스포트 정책을 생성할 필요 없이 동일한 클라이언트 액세스 제어를 위해 SVM의 여러 볼륨에 동일한 엑스포트 정책을 할당합니다.

각 SVM에는 규칙이 없는 "기본값"이라는 엑스포트 정책이 하나 이상 있습니다. 이 엑스포트 정책을 삭제할 수는 없지만 이름을 바꾸거나 수정할 수는 있습니다. 기본적으로 SVM의 각 볼륨은 기본 엑스포트 정책과 연결됩니다. SVM에서

SMB 액세스에 대한 엑스포트 정책을 사용하지 않도록 설정한 경우, "기본값" 엑스포트 정책은 SMB 액세스에 영향을 미치지 않습니다.

NFS 및 SMB 호스트 모두에 대한 액세스를 제공하는 규칙을 구성하고 이 규칙을 엑스포트 정책에 연결할 수 있습니다. 그런 다음, NFS 및 SMB 호스트 모두에 액세스해야 하는 데이터가 포함된 볼륨에 연결할 수 있습니다. 또는 SMB 클라이언트만 액세스해야 하는 일부 볼륨이 있는 경우, SMB 프로토콜을 사용해서만 액세스를 허용하고 읽기 전용 및 쓰기 액세스에 Kerberos 또는 NTLM(또는 둘 다)만 사용하는 규칙을 사용하여 엑스포트 정책을 구성할 수 있습니다. 그러면 엑스포트 정책이 SMB 액세스만 원하는 볼륨에 연결됩니다.

SMB에 대한 엑스포트 정책이 설정되어 있고 클라이언트가 해당 엑스포트 정책에서 허용하지 않는 액세스 요청을 하는 경우, 요청이 실패하고 권한 거부 메시지가 표시됩니다. 클라이언트가 볼륨의 엑스포트 정책에 있는 규칙과 일치하지 않으면 액세스가 거부됩니다. 내보내기 정책이 비어 있으면 모든 액세스가 암시적으로 거부됩니다. 공유 및 파일 권한이 액세스를 허용하는 경우에도 마찬가지입니다. 즉, SMB 공유가 포함된 볼륨에서 다음을 최소한으로 허용하도록 엑스포트 정책을 구성해야 합니다.

- 모든 클라이언트 또는 적절한 클라이언트 하위 집합에 대한 액세스를 허용합니다
- SMB를 통한 액세스를 허용합니다
- Kerberos 또는 NTLM 인증(또는 둘 다)을 사용하여 적절한 읽기 전용 및 쓰기 액세스 허용

에 대해 자세히 알아보십시오 "엑스포트 정책 구성 및 관리".

ONTAP SMB 수출 규칙에 대해 알아보세요

내보내기 규칙은 엑스포트 정책의 기능 요소입니다. 내보내기 규칙은 클라이언트 액세스 요청을 처리하는 방법을 결정하기 위해 구성한 특정 매개 변수와 볼륨에 대한 클라이언트 액세스 요청을 일치시킵니다.

클라이언트에 대한 액세스를 허용하려면 내보내기 정책에 하나 이상의 내보내기 규칙이 있어야 합니다. 엑스포트 정책에 둘 이상의 규칙이 포함된 경우 규칙은 엑스포트 정책에 표시되는 순서대로 처리됩니다. 규칙 순서는 규칙 인덱스 번호로 지정됩니다. 규칙이 클라이언트와 일치하면 해당 규칙의 권한이 사용되며 추가 규칙은 처리되지 않습니다. 일치하는 규칙이 없으면 클라이언트가 액세스가 거부됩니다.

다음 조건을 사용하여 내보내기 규칙을 구성하여 클라이언트 액세스 권한을 결정할 수 있습니다.

- NFSv4 또는 SMB와 같이 요청을 보내는 클라이언트에서 사용하는 파일 액세스 프로토콜입니다.
- 호스트 이름 또는 IP 주소와 같은 클라이언트 식별자입니다.

  '-clientmatch' 필드의 최대 크기는 4096자입니다.

- Kerberos v5, NTLM 또는 AUTH_SYS와 같이 클라이언트에서 인증하는 데 사용되는 보안 유형입니다.

규칙이 여러 조건을 지정하는 경우 클라이언트는 규칙을 적용하기 위해 모든 조건을 충족해야 합니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것

- '어다나'

클라이언트 액세스 요청은 NFSv3 프로토콜을 사용하여 전송되고 클라이언트의 IP 주소는 10.1.17.37입니다.

클라이언트 액세스 프로토콜이 일치하더라도 클라이언트의 IP 주소는 내보내기 규칙에 지정된 IP 주소와 다른 서브넷에 있습니다. 따라서 클라이언트 일치가 실패하고 이 규칙은 이 클라이언트에 적용되지 않습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '어다나'

클라이언트 액세스 요청은 NFSv4 프로토콜을 사용하여 전송되고 클라이언트의 IP 주소는 10.1.16.54입니다.

클라이언트 액세스 프로토콜이 일치하고 클라이언트의 IP 주소가 지정된 서브넷에 있습니다. 따라서 클라이언트 일치가 성공하고 이 규칙이 이 클라이언트에 적용됩니다. 클라이언트는 보안 유형에 관계없이 읽기-쓰기 액세스를 받습니다.

예

엑스포트 정책에는 다음 매개 변수가 있는 엑스포트 규칙이 포함되어 있습니다.

- 프로토콜 NFS3
- '-clientmatch "10.1.16.0/255.255.255.0'
- 모든 것
- '-rwrule' krb5, NTLM

클라이언트 #1의 IP 주소는 10.1.16.207이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고 Kerberos v5로 인증됩니다.

클라이언트 #2에는 IP 주소가 10.1.16.211이고, NFSv3 프로토콜을 사용하여 액세스 요청을 보내고, AUTH_SYS로 인증됩니다.

클라이언트 액세스 프로토콜과 IP 주소는 두 클라이언트 모두에 대해 일치합니다. 읽기 전용 매개 변수를 사용하면 인증된 보안 유형에 관계없이 모든 클라이언트에 읽기 전용 액세스를 사용할 수 있습니다. 따라서 두 클라이언트 모두 읽기 전용 액세스 권한이 부여됩니다. 그러나 인증된 보안 유형 Kerberos v5를 사용하여 인증되었기 때문에 클라이언트 #1만 읽기-쓰기 액세스를 받습니다. 클라이언트 #2에서 읽기-쓰기 권한이 없습니다.

SMB를 통한 액세스를 제한하거나 허용하는 **ONTAP** 내보내기 정책 규칙의 예

이 예에서는 SMB 액세스에 대한 엑스포트 정책이 설정된 SVM에서 SMB를 통한 액세스를 제한 또는 허용하는 엑스포트 정책 규칙을 생성하는 방법을 보여줍니다.

SMB 액세스에 대한 엑스포트 정책은 기본적으로 비활성화되어 있습니다. SMB 액세스에 대한 엑스포트 정책을 설정한 경우에만 SMB 액세스를 제한하거나 허용하는 엑스포트 정책 규칙을 구성해야 합니다.

SMB 액세스에 대한 엑스포트 규칙입니다

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 엑스포트 규칙이 생성됩니다.

- 정책 이름: cifs1
- 색인 번호: 1
- 클라이언트 일치: 192.168.1.0/24 네트워크의 클라이언트만 일치시킵니다
- 프로토콜: SMB 액세스만 지원합니다
- 읽기 전용 액세스: NTLM 또는 Kerberos 인증을 사용하는 클라이언트에 대한 액세스
- 읽기-쓰기 액세스: Kerberos 인증을 사용하는 클라이언트에 대한 액세스

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

SMB 및 **NFS** 액세스에 대한 엑스포트 규칙

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 엑스포트 규칙이 생성됩니다.

- 정책 이름: cifsnfs1
- 색인 번호: 2
- 클라이언트 일치: 모든 클라이언트를 일치시킵니다
- 프로토콜: SMB 및 NFS 액세스
- 읽기 전용 액세스: 모든 클라이언트에 대해
- 읽기-쓰기 액세스: Kerberos(NFS 및 SMB) 또는 NTLM 인증(SMB)을 사용하는 클라이언트에 대한 액세스
- UNIX 사용자 ID 0(영)에 대한 매핑: 사용자 ID 65534에 매핑됨(일반적으로 사용자 이름에 매핑되지 않음)
- SUID 및 SGID 액세스: 허용

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

NTLM을 사용한 **SMB** 액세스에 대한 내보내기 규칙입니다

다음 명령을 실행하면 다음 구성을 가진 ""VS1"" SVM에 대한 엑스포트 규칙이 생성됩니다.

- 정책 이름: ntlm1
- 색인 번호: 1
- 클라이언트 일치: 모든 클라이언트를 일치시킵니다
- 프로토콜: SMB 액세스만 지원합니다

- 읽기 전용 액세스: NTLM을 사용하는 클라이언트에만 해당됩니다
- 읽기-쓰기 액세스: NTLM을 사용하는 클라이언트에만 해당됩니다

NTLM 전용 액세스에 대해 읽기 전용 옵션 또는 읽기/쓰기 옵션을 구성하는 경우 클라이언트 일치 옵션에서 IP 주소 기반 항목을 사용해야 합니다. 그렇지 않으면 "액세스 거부" 오류가 발생합니다. 이는 ONTAP가 호스트 이름을 사용하여 클라이언트의 액세스 권한을 확인할 때 Kerberos SPN(서비스 사용자 이름)을 사용하기 때문입니다. NTLM 인증은 SPN 이름을 지원하지 않습니다.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

SMB 액세스를 위한 **ONTAP** 내보내기 정책 활성화 또는 비활성화

SVM(스토리지 가상 머신)에서 SMB 액세스에 대한 엑스포트 정책을 설정하거나 해제할 수 있습니다. 내보내기 정책을 사용하여 리소스에 대한 SMB 액세스를 제어하는 것은 선택 사항입니다.

시작하기 전에

다음은 SMB에 대한 엑스포트 정책을 설정하기 위한 요구 사항입니다.

- 클라이언트에 대한 내보내기 규칙을 만들기 전에 DNS에 "PTR" 레코드가 있어야 합니다.
- SVM에서 NFS 클라이언트에 대한 액세스를 제공하고 NFS 액세스에 사용할 호스트 이름이 CIFS 서버 이름과 다른 경우 호스트 이름에 대한 추가 "A" 및 "PTR" 레코드 세트가 필요합니다.

이 작업에 대해

SVM에서 새 CIFS 서버를 설정할 때 SMB 액세스에 대한 엑스포트 정책을 사용하는 것은 기본적으로 해제되어 있습니다. 인증 프로토콜 또는 클라이언트 IP 주소 또는 호스트 이름을 기반으로 액세스를 제어하려는 경우 SMB 액세스에 대한 엑스포트 정책을 설정할 수 있습니다. 언제든지 SMB 액세스에 대한 엑스포트 정책을 설정하거나 해제할 수 있습니다.

NFS 지원 SVM에서 CIFS/SMB에 대한 엑스포트 정책을 활성화하면 Linux 클라이언트가 SVM에서 명령을 사용하여 연결된 엑스포트 정책 규칙을 통해 모든 SMB 볼륨의 접합 경로를 볼 수 있습니다 `showmount -e`.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 엑스포트 정책 활성화 또는 비활성화:
   - 내보내기 정책 활성화: 'vserver cifs options modify -vserver_vserver_name_-is-exportpolicy -enabled true'
   - 엑스포트 정책 비활성화: 'vserver cifs options modify -vserver_vserver_name_-is-exportpolicy -enabled false
3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 엑스포트 정책을 사용하여 SVM VS1 기반 리소스에 대한 SMB 클라이언트 액세스를 제어할 수 있습니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다

Storage-Level Access Guard를 사용하여 안전한 ONTAP SMB 파일 액세스에 대해 알아보세요.

기본 파일 수준 및 내보내기/공유 보안을 사용하여 액세스를 보호하는 것 외에도 ONTAP가 볼륨 수준에서 적용한 세 번째 보안 계층인 스토리지 수준 액세스 가드를 구성할 수 있습니다. Storage-Level Access Guard는 모든 NAS 프로토콜에서 해당 프로토콜이 적용된 스토리지 객체에 액세스하는 데 적용됩니다.

NTFS 액세스 권한만 지원됩니다. ONTAP에서 UNIX 사용자에 대한 보안 검사를 수행하여 스토리지 수준 액세스 가드가 적용된 볼륨의 데이터에 액세스하려면 UNIX 사용자는 볼륨을 소유한 SVM에서 Windows 사용자에게 매핑해야 합니다.

Storage-Level Access Guard 동작

- Storage-Level Access Guard는 스토리지 개체의 모든 파일 또는 모든 디렉토리에 적용됩니다.

  볼륨의 모든 파일 또는 디렉토리에는 Storage-Level Access Guard 설정이 적용되기 때문에 전파를 통한 상속은 필요하지 않습니다.

- 저장소 수준 액세스 가드를 구성하여 파일에만 적용하거나 디렉터리에만 적용하거나 볼륨 내의 파일과 디렉터리에 모두 적용할 수 있습니다.
  - 파일 및 디렉터리 보안

    스토리지 객체 내의 모든 디렉토리 및 파일에 적용됩니다. 기본 설정입니다.

  - 파일 보안

    스토리지 객체 내의 모든 파일에 적용됩니다. 이 보안을 적용해도 디렉터리에 대한 액세스 또는 감사에는 영향을 주지 않습니다.

  - 디렉터리 보안

    스토리지 객체 내의 모든 디렉토리에 적용됩니다. 이 보안을 적용해도 파일에 대한 액세스 또는 감사에는 영향을 주지 않습니다.

- Storage-Level Access Guard는 사용 권한을 제한하는 데 사용됩니다.

  추가 액세스 권한은 제공하지 않습니다.

- NFS 또는 SMB 클라이언트의 파일 또는 디렉토리에 대한 보안 설정을 볼 경우 Storage-Level Access Guard 보안이 표시되지 않습니다.

  스토리지 객체 레벨에서 적용되고 유효 사용 권한을 결정하는 데 사용되는 메타데이터에 저장됩니다.

- 시스템(Windows 또는 UNIX) 관리자도 클라이언트에서 스토리지 수준 보안을 취소할 수 없습니다.

  스토리지 관리자만 수정할 수 있습니다.

- NTFS 또는 혼합 보안 스타일을 사용하는 볼륨에 스토리지 수준 액세스 가드를 적용할 수 있습니다.
- 볼륨이 포함된 SVM에 CIFS 서버가 구성되어 있는 경우 UNIX 보안 스타일을 사용하는 볼륨에 Storage-Level Access Guard를 적용할 수 있습니다.
- 볼륨이 볼륨 접합 경로 아래에 마운트되고 해당 경로에 Storage-Level Access Guard가 있는 경우 그 아래에 마운트된 볼륨으로 전파되지 않습니다.
- Storage-Level Access Guard 보안 설명자는 SnapMirror 데이터 복제 및 SVM 복제를 통해 복제됩니다.
- 바이러스 스캐너용 특별한 디스펜션이 있습니다.

  저장소 수준 액세스 가드가 개체에 대한 액세스를 거부하더라도 이러한 서버에서 파일과 디렉토리를 선별하기 위해 예외적인 액세스가 허용됩니다.

- 스토리지 레벨 액세스 가드로 인해 액세스가 거부되면 FPolicy 알림이 전송되지 않습니다.

액세스 확인 순서

파일 또는 디렉토리에 대한 액세스는 내보내기 또는 공유 권한, 볼륨에 설정된 Storage-Level Access Guard 권한, 파일 및/또는 디렉토리에 적용되는 기본 파일 권한의 합집합에 의해 결정됩니다. 모든 보안 수준을 평가하여 파일 또는 디렉터리에 있는 유효한 권한을 결정합니다. 보안 액세스 검사는 다음 순서로 수행됩니다.

1. SMB 공유 또는 NFS 엑스포트 레벨 사용 권한
2. 스토리지 레벨 액세스 가드
3. NTFS 파일/폴더 ACL(액세스 제어 목록), NFSv4 ACL 또는 UNIX 모드 비트

Storage-Level Access Guard 사용 사례

Storage-Level Access Guard는 클라이언트 측에서 볼 수 없는 스토리지 수준에서 추가 보안을 제공하므로 사용자 또는 관리자가 데스크톱에서 해당 보안을 취소할 수 없습니다. 스토리지 레벨에서 액세스를 제어하는 기능이 유용하다고 볼 수 있는 특정 사용 사례가 있습니다.

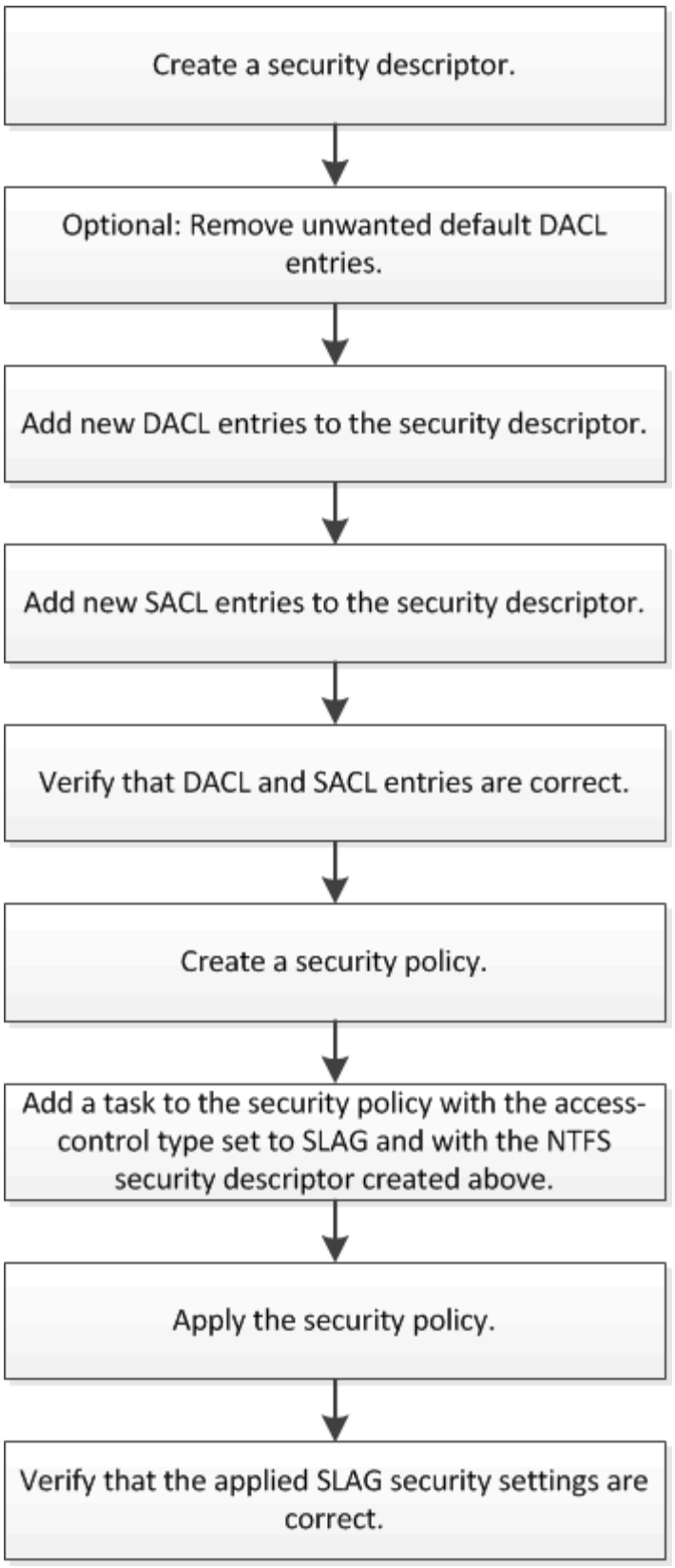
이 기능의 일반적인 사용 사례는 다음과 같습니다.

- 스토리지 수준에서 모든 사용자의 액세스를 감사 및 제어하여 지적 재산권을 보호합니다
- 은행 및 거래 그룹을 비롯한 금융 서비스 기업을 위한 스토리지
- 정부 서비스 및 개별 부서용 개별 파일 스토리지

- 모든 학생 파일을 보호하는 대학

ONTAP SMB 서버에서 **Storage-Level Access Guard**에 대한 구성 워크플로

스토리지 레벨 액세스 가드(slag)를 구성하는 워크플로에서는 NTFS 파일 권한 및 감사 정책을 구성하는 데 사용하는 것과 동일한 ONTAP CLI 명령을 사용합니다. 지정된 대상에서 파일 및 디렉토리 액세스를 구성하는 대신 지정된 SVM(스토리지 가상 머신) 볼륨의 슬래그를 구성합니다.



관련 정보

서버에서 스토리지 수준 액세스 보호 구성

볼륨 또는 qtree에 스토리지 레벨 액세스 가드를 구성하려면 여러 단계를 수행해야 합니다. Storage-Level Access Guard는 스토리지 레벨에서 설정된 액세스 보안 수준을 제공합니다. 모든 NAS 프로토콜에서 적용된 스토리지 객체에 대한 모든 액세스에 적용되는 보안을 제공합니다.

단계

1. 'vserver security file-directory NTFS create' 명령을 사용하여 보안 설명자를 생성합니다.

   'vserver security file-directory NTFS create-vserver vs1-ntfs-sd sd1"vserver security file-directory NTFS show-vserver vs1'

```
Vserver: vs1

   NTFS Security    Owner Name
   Descriptor Name
   ------------     --------------
   sd1              -
```

   보안 설명자는 다음 네 가지 기본 ACE(DACL 액세스 제어 항목)를 사용하여 만들어집니다.

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    BUILTIN\Administrators
                     allow    full-control   this-folder, sub-folders,
files
    BUILTIN\Users    allow    full-control   this-folder, sub-folders,
files
    CREATOR OWNER    allow    full-control   this-folder, sub-folders,
files
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

   Storage-Level Access Guard를 구성할 때 기본 항목을 사용하지 않으려면 보안 설명자에 고유한 ACE를 만들고 추가하기 전에 해당 항목을 제거할 수 있습니다.

2. Storage-Level Access Guard 보안으로 구성하지 않으려는 보안 설명자에서 기본 DACL ACE 중 하나를 제거합니다.

   a. 'vserver security file-directory NTFS DACL remove' 명령을 사용하여 불필요한 DACL ACE를 제거합니다.

이 예제에서는 세 개의 기본 DACL ACE가 보안 설명자인 BUILTIN\Administrators, BUILTIN\Users 및 Creator Owner에서 제거됩니다.

'vserver security file-directory NTFS DACL remove-vserver vs1-ntfs-sd SD1-access-type allow-account builtin\users"vserver security file-directory NTFS DACL remove-vserver vs1-directory vs1-access-directs builtl-creator' vserver security file-directs -directs -ntfs -directs -ntfs -directs -directs -creator

b. 'vserver security file-directory NTFS DACL show' 명령을 사용하여 스토리지 수준 액세스 가드 보안에 사용하지 않을 DACL ACE가 보안 설명자에서 제거되었는지 확인합니다.

이 예제에서 명령의 출력은 NT AUTHORITY\SYSTEM DEFAULT DACL ACE 항목만 남겨 두고 세 개의 기본 DACL ACE가 보안 설명자에서 제거되었는지 확인합니다.

'vserver security file-directory NTFS DACL show -vserver vs1'

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. 'vserver security file-directory NTFS DACL add' 명령을 사용하여 하나 이상의 DACL 항목을 보안 설명자에 추가합니다.

이 예제에서는 보안 설명자에 두 개의 DACL ACE가 추가됩니다.

'vserver security file-directory NTFS DACL add-vserver vs1-ntfs-sd SD1-access-type allow-account example\engineering-rights full-control-apply-to this-folder, sub-folders, files"vserver security file-directory ntfs DACL add-vserver vs1-ntfs-access-type allow-account" example\Domain Users"-read-folders 폴더에 대한 읽기 권한

4. 'vserver security file-directory NTFS SACL add' 명령을 사용하여 하나 이상의 SACL 항목을 보안 설명자에 추가합니다.

이 예제에서는 두 개의 SACL ACE가 보안 설명자에 추가됩니다.

'vserver security file-directory NTFS SACL add-vserver vs1-ntfs-sd SD1-access-type failure-account' example\Domain Users"-rights read-apply-to this-folder, sub-folders, files"vserver security file-directory NTFS SACL add-vserver vs1-ntfs-sd-access-type success-account example\engineering-folders full-control-folders

5. 'vserver security file-directory NTFS DACL show' 및 'vserver security file-directory NTFS SACL show' 명령을 각각 사용하여 DACL 및 SACL ACE가 올바르게 구성되었는지 확인합니다.

이 예제에서 다음 명령은 보안 설명자 "'Sd1'"의 DACL 항목에 대한 정보를 표시합니다.

'vserver security file-directory NTFS DACL show -vserver vs1-NTFS-SD SD1'

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     allow    read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     allow    full-control   this-folder, sub-folders,
files
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

이 예제에서 다음 명령은 보안 설명자 "'sd1'"에 대한 SACL 항목에 대한 정보를 표시합니다.

'vserver security file-directory NTFS SACL show -vserver vs1-NTFS-SD SD1'

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. 'vserver security file-directory policy create' 명령을 사용하여 보안 정책을 생성합니다.

   다음 예제에서는 ""정책1""이라는 정책을 만듭니다.

   'vserver security file-directory policy create-vserver vs1-policy-name policy1'

7. 'vserver security file-directory policy show' 명령을 사용하여 정책이 올바르게 구성되었는지 확인합니다.

   'vserver security file-directory policy show'를 선택합니다

```
Vserver          Policy Name
------------     --------------
vs1              policy1
```

8. 을 사용하여 연결된 보안 설명자가 있는 작업을 보안 정책에 추가합니다 `vserver security file-directory policy task add` 명령과 함께 `-access-control` 매개 변수를 로 설정합니다 `slag`.

   정책에 둘 이상의 Storage-Level Access Guard 작업이 포함될 수 있지만 파일 디렉터리 및 Storage-Level Access Guard 작업을 모두 포함하도록 정책을 구성할 수는 없습니다. 정책에는 모든 스토리지 레벨 액세스 가드 작업 또는 모든 파일 디렉토리 작업이 포함되어야 합니다.

   이 예제에서는 보안 설명자 'Sd1'에 할당된 "정책1"이라는 정책에 작업이 추가됩니다. 액세스 제어 유형이 '슬래그'로 설정된 '/datavol1' 경로에 할당됩니다.

   'vserver security file-directory policy task add-vserver vs1-policy-name policy1-path/datavol1-access-control slag-security-type ntfs-ntfs-mode propagate-ntfs-sd SD1'

9. 'vserver security file-directory policy task show' 명령을 사용하여 작업이 올바르게 구성되었는지 확인합니다.

   'vserver security file-directory policy task show -vserver vs1-policy-name policy1'

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. 'vserver security file-directory apply' 명령을 사용하여 Storage-Level Access Guard 보안 정책을 적용합니다.

    'vserver security file-directory apply-vserver vs1-policy-name policy1'

    보안 정책을 적용할 작업이 예약됩니다.

11. 'vserver security file-directory show' 명령을 사용하여 적용된 Storage-Level Access Guard 보안 설정이 올바른지 확인합니다.

    이 예제에서 명령의 출력은 스토리지 레벨 액세스 가드 보안이 NTFS 볼륨 '/datavol1'에 적용되었음을 보여 줍니다. 모든 사용자에게 모든 권한을 허용하는 기본 DACL이 그대로 유지되더라도 Storage-Level Access Guard 보안은 Storage-Level Access Guard 설정에 정의된 그룹에 대한 액세스를 제한(및 감사)합니다.

    'vserver security file-directory show -vserver vs1-path/datavol1'

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

관련 정보

- NTFS 파일 보안, NTFS 감사 정책 및 스토리지 수준 액세스 보호 관리를 위한 명령
- 서버의 Storage-Level Access Guard에 대한 구성 워크플로
- 서버의 Storage-Level Access Guard에 대한 정보 표시
- 서버에서 스토리지 수준 액세스 보호 제거

ONTAP SMB 서버의 효과적인 **SLAG** 매트릭스

볼륨 또는 qtree 또는 둘 다에서 슬래그를 구성할 수 있습니다. 슬래그 매트릭스는 표에 나열된 다양한 시나리오에서 적용 가능한 슬래그 구성인 볼륨 또는 qtree를 정의합니다.

	AFS에서 볼륨 슬래그	스냅샷의 볼륨 슬래그	**AFS**에서 **qtree** 슬래그	스냅샷에서 **Qtree** 슬래그
AFS(Access File System)에서 볼륨 액세스	예	아니요	해당 없음	해당 없음
스냅샷의 볼륨 액세스	예	아니요	해당 없음	해당 없음
AFS에서 qtree 액세스(qtree에 슬래그가 있는 경우)	아니요	아니요	예	아니요
AFS에서 qtree 액세스(qtree에 슬래그가 없는 경우)	예	아니요	아니요	아니요
스냅샷에서 qtree 액세스(qtree AFS에 슬래그가 있는 경우)	아니요	아니요	예	아니요
스냅샷에서 qtree 액세스(qtree AFS에 슬래그가 없는 경우)	예	아니요	아니요	아니요

ONTAP SMB 서버에서 **Storage-Level Access Guard**에 대한 정보 표시

Storage-Level Access Guard는 볼륨 또는 qtree에 적용되는 세 번째 보안 계층입니다. Windows 속성 창을 사용하면 저장소 수준 액세스 가드 설정을 볼 수 없습니다. ONTAP CLI를 사용하여 스토리지 레벨 액세스 가드 보안에 대한 정보를 확인해야 합니다. 이 정보는 구성을 확인하거나 파일 액세스 문제를 해결하는 데 사용할 수 있습니다.

이 작업에 대해

SVM(Storage Virtual Machine)의 이름과 스토리지 레벨 액세스 가드 보안 정보를 표시할 볼륨 또는 qtree의 경로를 입력해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

단계

1. Storage-Level Access Guard 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver_vserver_name_-path_path_'

정보를 표시하려면...	다음 명령을 입력합니다...
세부 정보가 확장됩니다	'vserver security file-directory show -vserver_vserver_name_-path_path_-expand-mask true'

예

다음 예에서는 SVM VS1 에서 경로 '/datavol1’을 사용하여 NTFS 보안 스타일 볼륨에 대한 Storage-Level Access Guard 보안 정보를 표시합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

다음 예에서는 SVM VS1 경로의 '/datavol5' 경로에서 혼합 보안 형식 볼륨에 대한 Storage-Level Access Guard 정보를 표시합니다. 이 볼륨의 최상위 수준에는 UNIX의 효과적인 보안이 있습니다. 이 볼륨에는 Storage-Level Access Guard 보안이 있습니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

ONTAP SMB 서버에서 스토리지 수준 액세스 보호 제거

저장소 수준에서 액세스 보안을 더 이상 설정하지 않으려면 볼륨 또는 qtree에서 저장소 수준 액세스 가드를 제거할 수 있습니다. Storage-Level Access Guard를 제거해도 일반 NTFS 파일 및 디렉터리 보안은 수정하거나 제거되지 않습니다.

단계

1. 'vserver security file-directory show' 명령을 사용하여 볼륨 또는 qtree에 Storage-Level Access Guard가 구성되어 있는지 확인합니다.

   'vserver security file-directory show -vserver vs1-path/datavol2'

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. 'vserver security file-directory remove-slag' 명령을 사용하여 Storage-Level Access Guard를 제거합니다.

   'vserver security file-directory remove-slag-vserver vs1-path/datavol2'

3. 'vserver security file-directory show' 명령을 사용하여 볼륨 또는 qtree에서 Storage-Level Access Guard가 제거되었는지 확인합니다.

   'vserver security file-directory show -vserver vs1-path/datavol2'

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

SMB를 사용하여 파일 액세스를 관리합니다

로컬 사용자 및 그룹을 인증 및 인증에 사용합니다

ONTAP에서 로컬 사용자 및 그룹을 사용하는 방법

로컬 **ONTAP SMB** 사용자 및 그룹에 대해 알아보세요

사용자 환경에서 로컬 사용자 및 그룹을 구성하고 사용할지 여부를 결정하기 전에 로컬 사용자 및 그룹의 정의 및 이에 대한 몇 가지 기본 정보를 알아야 합니다.

- * 로컬 사용자 *

  생성된 SVM(스토리지 가상 머신)만 볼 수 있는 고유한 SID(보안 식별자)를 가진 사용자 계정 로컬 사용자 계정에는 사용자 이름 및 SID를 비롯한 일련의 속성이 있습니다. 로컬 사용자 계정은 NTLM 인증을 사용하여 CIFS 서버에서 로컬로 인증됩니다.

  사용자 계정에는 여러 가지 용도가 있습니다.

  - 사용자에게 *User Rights Management* 권한을 부여하는 데 사용됩니다.
  - SVM이 소유한 파일 및 폴더 리소스에 대한 공유 레벨 및 파일 레벨 액세스를 제어하는 데 사용됩니다.
- * 로컬 그룹 *

고유한 SID가 있는 그룹은 해당 SID가 생성된 SVM에서만 볼 수 있습니다. 그룹에는 구성원 집합이 포함됩니다. 구성원은 로컬 사용자, 도메인 사용자, 도메인 그룹 및 도메인 컴퓨터 계정일 수 있습니다. 그룹을 생성, 수정 또는 삭제할 수 있습니다.

그룹은 여러 가지 용도로 사용됩니다.

- 해당 구성원에게 *User Rights Management* 권한을 부여하는 데 사용됩니다.
- SVM이 소유한 파일 및 폴더 리소스에 대한 공유 레벨 및 파일 레벨 액세스를 제어하는 데 사용됩니다.

- * 로컬 도메인 *

  SVM에서 범위가 지정된 로컬 영역 로컬 도메인의 이름은 CIFS 서버 이름입니다. 로컬 사용자 및 그룹은 로컬 도메인 내에 포함됩니다.

- * SID(보안 식별자) *

  SID는 Windows 스타일의 보안 주체를 식별하는 가변 길이 숫자 값입니다. 예를 들어 일반적인 SID는 S-1-5-21-3139654847-1303905135-2517279418-123456의 형태를 사용합니다.

- * NTLM 인증 *

  CIFS 서버에서 사용자를 인증하는 데 사용되는 Microsoft Windows 보안 방법입니다.

- * 클러스터 복제 데이터베이스(RDB) *

  클러스터의 각 노드에 인스턴스가 있는 복제된 데이터베이스입니다. 로컬 사용자 및 그룹 객체가 RDB에 저장됩니다.

로컬 **ONTAP SMB** 사용자 및 로컬 그룹을 생성하는 이유

SVM(스토리지 가상 시스템)에서 로컬 사용자 및 로컬 그룹을 생성하는 데는 여러 가지 이유가 있습니다. 예를 들어 DC(도메인 컨트롤러)를 사용할 수 없거나, 로컬 그룹을 사용하여 권한을 할당하거나, SMB 서버가 작업 그룹에 있는 경우 로컬 사용자 계정을 사용하여 SMB 서버에 액세스할 수 있습니다.

다음과 같은 이유로 하나 이상의 로컬 사용자 계정을 만들 수 있습니다.

- SMB 서버가 작업 그룹에 있고 도메인 사용자를 사용할 수 없습니다.

  로컬 사용자는 작업 그룹 구성에 필요합니다.

- 도메인 컨트롤러를 사용할 수 없는 경우 SMB 서버를 인증하고 로그인할 수 있어야 합니다.

  로컬 사용자는 도메인 컨트롤러가 다운되었을 때 NTLM 인증을 사용하여 SMB 서버를 인증할 수 있으며, 네트워크 문제로 인해 SMB 서버가 도메인 컨트롤러에 접속할 수 없게 되는 경우

- 로컬 사용자에게 사용자 권한 관리 권한을 할당하려고 합니다.

  User Rights Management 는 SMB 서버 관리자가 SVM에 대한 사용자 및 그룹의 권한을 제어할 수 있는 기능입니다. 사용자 계정에 권한을 할당하거나 해당 권한이 있는 로컬 그룹의 구성원으로 만들어 사용자에게 권한을 할당할 수 있습니다.

다음과 같은 이유로 하나 이상의 로컬 그룹을 만들 수 있습니다.

- SMB 서버가 작업 그룹에 있고 도메인 그룹을 사용할 수 없습니다.

  로컬 그룹은 작업 그룹 구성에 필요하지 않지만 로컬 작업 그룹 사용자에 대한 액세스 권한을 관리하는 데 유용할 수 있습니다.

- 공유 및 파일 액세스 제어를 위해 로컬 그룹을 사용하여 파일 및 폴더 리소스에 대한 액세스를 제어하려는 경우
- Customized_User Rights Management_Privileges를 사용하여 로컬 그룹을 생성하려고 합니다.

  일부 기본 제공 사용자 그룹에는 사전 정의된 권한이 있습니다. 사용자 지정된 권한 집합을 할당하려면 로컬 그룹을 생성하고 해당 그룹에 필요한 권한을 할당할 수 있습니다. 그런 다음 로컬 사용자, 도메인 사용자 및 도메인 그룹을 로컬 그룹에 추가할 수 있습니다.

관련 정보

- 로컬 사용자 인증에 대해 알아보세요
- 지원되는 권한 목록입니다

로컬 **ONTAP SMB** 사용자 인증에 대해 알아보세요

로컬 사용자가 CIFS 서버의 데이터를 액세스하려면 먼저 인증된 세션을 생성해야 합니다.

SMB는 세션 기반이므로 세션이 처음 설정될 때 사용자 ID를 한 번만 결정할 수 있습니다. CIFS 서버는 로컬 사용자를 인증할 때 NTLM 기반 인증을 사용합니다. NTLMv1과 NTLMv2가 모두 지원됩니다.

ONTAP는 세 가지 사용 사례에서 로컬 인증을 사용합니다. 각 활용 사례는 사용자 이름의 도메인 부분(domain\user 형식)이 CIFS 서버의 로컬 도메인 이름(CIFS 서버 이름)과 일치하는지 여부에 따라 달라집니다.

- 도메인 부분이 일치합니다

  데이터에 대한 액세스를 요청할 때 로컬 사용자 자격 증명을 제공하는 사용자는 CIFS 서버에서 로컬로 인증됩니다.

- 도메인 부분이 일치하지 않습니다

  ONTAP는 CIFS 서버가 속한 도메인의 도메인 컨트롤러에서 NTLM 인증을 사용하려고 합니다. 인증에 성공하면 로그인이 완료된 것입니다. 성공하지 못하면 다음 단계는 인증이 성공하지 못한 이유에 따라 달라집니다.

  예를 들어 사용자가 Active Directory에 있지만 암호가 잘못되었거나 만료된 경우 ONTAP는 CIFS 서버에서 해당 로컬 사용자 계정을 사용하지 않습니다. 대신 인증에 실패합니다. ONTAP가 CIFS 서버에 있는 경우 NetBIOS 도메인 이름이 일치하지 않아도 인증을 위해 해당 로컬 계정을 사용하는 경우도 있습니다. 예를 들어 일치하는 도메인 계정이 있지만 비활성화된 경우 ONTAP는 CIFS 서버에서 해당 로컬 계정을 사용하여 인증합니다.

- 도메인 부분이 지정되지 않았습니다

  ONTAP는 먼저 로컬 사용자로 인증을 시도합니다. 로컬 사용자로 인증에 실패하면 ONTAP는 CIFS 서버가 속한 도메인의 도메인 컨트롤러를 사용하여 사용자를 인증합니다.

로컬 또는 도메인 사용자 인증이 성공적으로 완료되면 ONTAP는 로컬 그룹 구성원 자격 및 권한을 고려하여 전체 사용자 액세스 토큰을 생성합니다.

로컬 사용자의 NTLM 인증에 대한 자세한 내용은 Microsoft Windows 설명서를 참조하십시오.

관련 정보

서버에서 로컬 사용자 인증을 활성화하거나 비활성화합니다.

ONTAP SMB 사용자 액세스 토큰에 대해 알아보세요

사용자가 공유를 매핑하면 인증된 SMB 세션이 설정되고 사용자, 사용자의 그룹 구성원 자격 및 누적 권한, 매핑된 UNIX 사용자에 대한 정보가 포함된 사용자 액세스 토큰이 생성됩니다.

이 기능을 사용하지 않는 한 로컬 사용자 및 그룹 정보도 사용자 액세스 토큰에 추가됩니다. 액세스 토큰이 구성되는 방식은 로컬 사용자에 대한 로그인인지 Active Directory 도메인 사용자에 대한 로그인인지에 따라 달라집니다.

- 로컬 사용자 로그인입니다

  로컬 사용자는 다른 로컬 그룹의 구성원이 될 수 있지만 로컬 그룹은 다른 로컬 그룹의 구성원이 될 수 없습니다. 로컬 사용자 액세스 토큰은 특정 로컬 사용자가 구성원인 그룹에 할당된 모든 권한의 합집합으로 구성됩니다.

- 도메인 사용자 로그인

  도메인 사용자가 로그인하면 ONTAP는 사용자가 구성원인 모든 도메인 그룹의 사용자 SID 및 SID가 포함된 사용자 액세스 토큰을 얻습니다. ONTAP는 도메인 사용자 액세스 토큰의 조합과 사용자의 도메인 그룹(있는 경우)의 로컬 멤버십에서 제공하는 액세스 토큰, 도메인 사용자 또는 해당 도메인 그룹 구성원에 할당된 모든 직접 권한을 사용합니다.

로컬 및 도메인 사용자 로그인의 경우 사용자 액세스 토큰에 대해 기본 그룹 제거도 설정됩니다. 기본 RID는 Domain Users(RID 513)입니다. 기본값을 변경할 수 없습니다.

Windows-to-UNIX 및 UNIX-to-Windows 이름 매핑 프로세스는 로컬 및 도메인 계정에 대해 동일한 규칙을 따릅니다.

UNIX 사용자에서 로컬 계정으로 자동 매핑은 암시적으로 수행되지 않습니다. 이 작업이 필요한 경우 기존 이름 매핑 명령을 사용하여 명시적 매핑 규칙을 지정해야 합니다.

로컬 그룹이 포함된 **ONTAP SMB SVM**에서 **SnapMirror**를 사용하는 방법에 대해 알아보세요**.**

로컬 그룹이 포함된 SVM이 소유한 볼륨에 SnapMirror를 구성할 때는 지침을 숙지해야 합니다.

SnapMirror에서 다른 SVM으로 복제된 파일, 디렉토리 또는 공유에 적용된 ACE의 로컬 그룹은 사용할 수 없습니다. SnapMirror 기능을 사용하여 다른 SVM의 볼륨에 DR 미러를 생성하고 볼륨에 로컬 그룹에 ACE가 있는 경우 ACE는 미러에서 유효하지 않습니다. 데이터를 다른 SVM으로 복제하면 데이터가 다른 로컬 도메인에 효과적으로 교차합니다. 로컬 사용자 및 그룹에 부여되는 사용 권한은 원래 생성된 SVM의 범위 내에서만 유효합니다.

ONTAP SMB 서버를 삭제하면 사용자와 그룹에 어떤 영향이 있는지 알아보세요**.**

CIFS 서버가 생성될 때 로컬 사용자 및 그룹의 기본 세트가 생성되고 CIFS 서버를 호스팅하는 SVM(스토리지 가상 머신)과 연결됩니다. SVM 관리자는 언제든지 로컬 사용자 및 그룹을 생성할 수 있습니다. CIFS 서버를 삭제할 때 로컬 사용자 및 그룹에 어떤 일이 발생하는지 알고 있어야 합니다.

로컬 사용자 및 그룹은 SVM에 연결되어 있으므로 보안 고려 사항으로 인해 CIFS 서버를 삭제할 때 삭제되지 않습니다.

CIFS 서버가 삭제되어도 로컬 사용자 및 그룹은 삭제되지 않지만 숨겨집니다. SVM에서 CIFS 서버를 다시 생성할 때까지 로컬 사용자 및 그룹을 보거나 관리할 수 없습니다.

CIFS 서버 관리 상태는 로컬 사용자 또는 그룹의 표시에는 영향을 주지 않습니다.

로컬 **ONTAP SMB** 사용자 및 그룹과 함께 **Microsoft Management Console**을 사용하는 방법을 알아보세요**.**

Microsoft 관리 콘솔에서 로컬 사용자 및 그룹에 대한 정보를 볼 수 있습니다. 이 ONTAP 릴리스에서는 Microsoft 관리 콘솔에서 로컬 사용자 및 그룹에 대한 다른 관리 작업을 수행할 수 없습니다.

ONTAP SMB 클러스터 되돌리기에 대해 알아보세요

로컬 사용자 및 그룹을 지원하지 않는 ONTAP 릴리즈로 클러스터를 되돌리려는 경우 로컬 사용자 및 그룹을 사용하여 파일 액세스 또는 사용자 권한을 관리하려면 특정 고려 사항을 알고 있어야 합니다.

- 보안상의 이유로 ONTAP가 로컬 사용자 및 그룹 기능을 지원하지 않는 버전으로 되돌려지면 구성된 로컬 사용자, 그룹 및 권한에 대한 정보가 삭제되지 않습니다.
- ONTAP의 이전 주요 버전으로 되돌릴 때 ONTAP는 인증 및 자격 증명 생성 중에 로컬 사용자 및 그룹을 사용하지 않습니다.
- 로컬 사용자 및 그룹은 파일 및 폴더 ACL에서 제거되지 않습니다.
- 로컬 사용자 또는 그룹에 부여된 권한으로 인해 부여되는 액세스에 의존하는 파일 액세스 요청이 거부됩니다.

  액세스를 허용하려면 로컬 사용자 및 그룹 개체 대신 도메인 개체를 기반으로 액세스를 허용하도록 파일 권한을 다시 구성해야 합니다.

어떤 로컬 권한이 있는지 확인합니다

지원되는 **ONTAP SMB** 권한 목록

ONTAP에는 지원되는 권한이 미리 정의되어 있습니다. 미리 정의된 특정 로컬 그룹에는 이러한 권한 중 일부가 기본적으로 추가됩니다. 또한 미리 정의된 그룹에서 권한을 추가하거나 제거하거나 새 로컬 사용자 또는 그룹을 만들고 만든 그룹 또는 기존 도메인 사용자 및 그룹에 권한을 추가할 수도 있습니다.

다음 표에는 SVM(스토리지 가상 시스템)에서 지원되는 권한이 나열되어 있으며 할당된 권한이 있는 BUILTIN 그룹 목록이 제공됩니다.

권한 이름입니다	기본 보안 설정입니다	설명
'SeTcbPrivilege'입니다	없음	운영 체제의 일부로 작동합니다
'BackupPrivilege'입니다	'BUILTIN\Administrators', 'BUILTIN\Backup Operators'	파일 및 디렉토리를 백업하고 모든 ACL을 재정의합니다

권한 이름입니다	기본 보안 설정입니다	설명
스저장창고특권	'BUILTIN\Administrators', 'BUILTIN\Backup Operators'	파일 및 디렉토리를 복원하고 모든 ACL을 재정의하면 유효한 사용자 또는 그룹 SID가 파일 소유자로 설정됩니다
'새테이크오너선프리빌리지'	'BUILTIN\Administrators'	파일 또는 기타 개체의 소유권을 가져옵니다
'보안 권한'	'BUILTIN\Administrators'	감사 관리 여기에는 보안 로그 보기, 덤프 및 지우기가 포함됩니다.
'스변경NotifyPrivilege'입니다	'BUILTIN\Administrators', 'BUILTIN\Backup Operators', 'BUILTIN\Power Users', 'BUILTIN\Users', 'Everyone'	횡단 검사를 무시합니다 이 권한이 있는 사용자는 폴더, 교집합 또는 교차로를 횡단(x) 권한이 필요하지 않습니다.

관련 정보

- 권한 할당에 대해 알아보세요
- 바이패스 트래버스 검사 구성에 대해 알아보세요

ONTAP SMB 권한 할당에 대해 알아보세요

로컬 사용자 또는 도메인 사용자에게 직접 권한을 할당할 수 있습니다. 또는 할당된 권한이 해당 사용자에게 부여할 기능과 일치하는 로컬 그룹에 사용자를 할당할 수 있습니다.

- 생성한 그룹에 권한 집합을 할당할 수 있습니다.

  그런 다음 해당 사용자에게 부여할 권한이 있는 사용자를 그룹에 추가합니다.

- 기본 권한이 해당 사용자에게 부여할 권한과 일치하는 미리 정의된 그룹에 로컬 사용자 및 도메인 사용자를 할당할 수도 있습니다.

관련 정보

- 로컬 또는 도메인 사용자 또는 그룹에 권한을 추가합니다
- 로컬 또는 도메인 사용자 또는 그룹에서 권한을 제거합니다
- 로컬 또는 도메인 사용자 및 그룹에 대한 권한을 재설정합니다
- 바이패스 트래버스 검사 구성에 대해 알아보세요

ONTAP SMB 서버의 **BUILTIN** 그룹 및 로컬 관리자 계정에 대해 알아보세요.

BUILTIN 그룹 및 로컬 관리자 계정을 사용할 때 유의해야 할 몇 가지 지침이 있습니다. 예를 들어 로컬 관리자 계정의 이름을 바꿀 수는 있지만 이 계정은 삭제할 수 없습니다.

- Administrator 계정의 이름을 바꿀 수는 있지만 삭제할 수는 없습니다.
- 관리자 계정은 BUILTIN\Administrators 그룹에서 제거할 수 없습니다.
- BUILTIN 그룹은 이름을 바꿀 수 있지만 삭제할 수 없습니다.

  BUILTIN 그룹의 이름을 바꾼 후 잘 알려진 이름으로 다른 로컬 개체를 만들 수 있지만 개체에 새 RID가 할당됩니다.

- 로컬 게스트 계정이 없습니다.

관련 정보

사전 정의된 BUILTIN 그룹 및 기본 권한

로컬 **ONTAP SMB** 사용자 암호에 대한 요구 사항

기본적으로 로컬 사용자 암호는 복잡성 요구 사항을 충족해야 합니다. 암호 복잡성 요구 사항은 Microsoft Windows_Local 보안 정책 _ 에 정의된 요구 사항과 비슷합니다.

암호는 다음 기준을 충족해야 합니다.

- 6자 이상이어야 합니다
- 사용자 계정 이름을 포함해서는 안 됩니다
- 다음 4개 범주 중 3개 이상의 문자를 포함해야 합니다.
  - 영어 대문자(A ~ Z)
  - 영어 소문자(a ~ z)
  - 기본 10자리(0 ~ 9)
  - 특수 문자:

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

관련 정보

- 로컬 사용자에 대한 암호 복잡성 구성
- 서버 보안 설정에 대한 정보 표시
- 로컬 사용자 계정 암호를 변경합니다

미리 정의된 **BUILTIN** 그룹 및 기본 **ONTAP SMB** 권한

ONTAP에서 제공하는 미리 정의된 BUILTIN 그룹 집합에 로컬 사용자 또는 도메인 사용자의 구성원을 할당할 수 있습니다. 사전 정의된 그룹에는 사전 정의된 권한이 할당됩니다.

다음 표에는 미리 정의된 그룹이 설명되어 있습니다.

미리 정의된 **BUILTIN** 그룹	기본 권한
"BUILTIN\Administrators" RID 544 처음 만들어지면 500여 개 계정을 없앤다고 하면 자동으로 이 그룹의 회원이 됩니다. SVM(Storage Virtual Machine)이 도메인에 가입되면 domain\Domain Admins 그룹이 그룹에 추가됩니다. SVM이 도메인을 벗어나면 domain\Domain Admins 그룹이 그룹에서 제거됩니다.	• 'BackupPrivilege'입니다 • 스저장창고특권 • '보안 권한' • '새테이크오너선프리빌리지' • '스변경NotifyPrivilege'입니다
"BUILTIN\Power Users" RID 547 이 그룹을 처음 만들 때 구성원이 없습니다. 이 그룹의 구성원은 다음과 같은 특성을 갖습니다. • 로컬 사용자 및 그룹을 생성하고 관리할 수 있습니다. • 자체 또는 다른 개체를 'BUILTIN\Administrators' 그룹에 추가할 수 없습니다.	'스변경NotifyPrivilege'입니다
``BUILTIN\Backup Operators' RID 551 이 그룹을 처음 만들 때 구성원이 없습니다. 이 그룹의 구성원은 백업 의도로 열린 파일 또는 폴더에 대한 읽기 및 쓰기 권한을 재정의할 수 있습니다.	• 'BackupPrivilege'입니다 • 스저장창고특권 • '스변경NotifyPrivilege'입니다
"BUILTIN\Users" RID 545 처음 만들어도 이 그룹에는 인증된 사용자 특별 그룹 외에 구성원이 없습니다. SVM이 도메인에 가입되면 이 그룹에 domain\Domain Users" 그룹이 추가됩니다. SVM이 도메인을 벗어나면 이 그룹에서 "도메인 사용자" 그룹이 제거됩니다.	'스변경NotifyPrivilege'입니다
모든 사람의 ID S-1-0입니다 이 그룹에는 게스트(익명 사용자 제외)를 포함한 모든 사용자가 포함됩니다. 이 그룹은 묵시적 멤버십을 가진 암시적 그룹입니다.	'스변경NotifyPrivilege'입니다

관련 정보

- 서버의 BUILTIN 그룹 및 로컬 관리자 계정에 대해 알아보세요.
- 지원되는 권한 목록입니다
- 바이패스 트래버스 검사 구성에 대해 알아보세요

로컬 사용자 및 그룹 기능을 설정하거나 해제합니다

로컬 **ONTAP SMB** 사용자 및 그룹 기능에 대해 알아보세요

NTFS 보안 스타일 데이터의 액세스 제어에 로컬 사용자 및 그룹을 사용하려면 먼저 로컬 사용자 및 그룹 기능을 활성화해야 합니다. 또한 SMB 인증에 로컬 사용자를 사용하려면 로컬 사용자 인증 기능을 활성화해야 합니다.

로컬 사용자 및 그룹 기능 및 로컬 사용자 인증은 기본적으로 사용됩니다. 이 옵션이 설정되어 있지 않으면 로컬 사용자 및 그룹을 구성하고 사용할 수 있도록 설정하기 전에 설정해야 합니다. 언제든지 로컬 사용자 및 그룹 기능을 사용하지 않도록 설정할 수 있습니다.

로컬 사용자 및 그룹 기능을 명시적으로 해제하는 것 외에도, 클러스터의 노드가 해당 기능을 지원하지 않는 ONTAP 릴리즈로 되돌려지는 경우 ONTAP는 로컬 사용자 및 그룹 기능을 비활성화합니다. 클러스터의 모든 노드에서 지원하는 ONTAP 버전이 실행될 때까지 로컬 사용자 및 그룹 기능이 활성화되지 않습니다.

관련 정보

- 로컬 사용자 계정을 수정합니다
- 로컬 그룹을 수정합니다
- 로컬 또는 도메인 사용자 또는 그룹에 권한을 추가합니다

ONTAP SMB 서버에서 로컬 사용자 및 그룹 활성화 또는 비활성화

SVM(스토리지 가상 머신)에서 SMB 액세스를 위해 로컬 사용자 및 그룹을 설정하거나 해제할 수 있습니다. 로컬 사용자 및 그룹 기능은 기본적으로 활성화되어 있습니다.

이 작업에 대해

SMB 공유 및 NTFS 파일 권한을 구성할 때 로컬 사용자 및 그룹을 사용할 수 있으며 SMB 연결을 생성할 때 로컬 사용자를 인증에 사용할 수도 있습니다. 로컬 사용자를 인증에 사용하려면 로컬 사용자 및 그룹 인증 옵션도 활성화해야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

로컬 사용자 및 그룹을 사용하려는 경우...	명령 입력...
활성화됨	'vserver cifs options modify -vserver_vserver_name_-is-local-users-and-groups -enabled true'
사용 안 함	'vserver cifs options modify -vserver_vserver_name_-is-local-users-and-groups -enabled false'

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 SVM VS1 에서 로컬 사용자 및 그룹 기능을 사용하도록 설정합니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

관련 정보

- 서버에서 로컬 사용자 인증을 활성화하거나 비활성화합니다.
- 로컬 사용자 계정을 설정하거나 해제합니다

ONTAP SMB 서버에서 로컬 사용자 인증을 활성화하거나 비활성화합니다**.**

SVM(스토리지 가상 머신)에서 SMB 액세스에 대한 로컬 사용자 인증을 설정하거나 해제할 수 있습니다. 기본값은 로컬 사용자 인증을 허용하는 것입니다. 이는 SVM이 도메인 컨트롤러에 연결할 수 없거나 도메인 레벨 액세스 제어를 사용하지 않도록 선택하는 경우에 유용합니다.

시작하기 전에

CIFS 서버에서 로컬 사용자 및 그룹 기능을 설정해야 합니다.

이 작업에 대해

언제든지 로컬 사용자 인증을 활성화 또는 비활성화할 수 있습니다. SMB 연결을 생성할 때 인증에 로컬 사용자를 사용하려면 CIFS 서버의 로컬 사용자 및 그룹 옵션도 설정해야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

로컬 인증을 사용하려는 경우...	명령 입력...
활성화됨	'vserver cifs options modify -vserver_vserver_name_-is-local-auth-enabled true'
사용 안 함	'vserver cifs options modify -vserver_vserver_name_-is-local-auth-enabled false'

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 SVM VS1 에서 로컬 사용자 인증을 사용합니다.

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

관련 정보

- 로컬 사용자 인증에 대해 알아보세요
- 서버에서 로컬 사용자 및 그룹 활성화 또는 비활성화

로컬 사용자 계정을 관리합니다

로컬 **ONTAP SMB** 사용자 계정 수정

기존 사용자의 전체 이름 또는 설명을 변경하고 사용자 계정을 활성화하거나 비활성화하려면 로컬 사용자 계정을 수정할 수 있습니다. 사용자 이름이 손상되었거나 관리를 위해 이름 변경이 필요한 경우 로컬 사용자 계정의 이름을 바꿀 수도 있습니다.

원하는 작업	명령 입력...
로컬 사용자의 전체 이름을 수정합니다	'vserver cifs users-and-groups local-user modify -vserver_vserver_name_-user-name_user_name_ -full-name text' 전체 이름에 공백이 포함되어 있으면 큰따옴표로 묶어야 합니다.
로컬 사용자의 설명을 수정합니다	'vserver cifs users-and-groups local-user modify -vserver_vserver_name_-user-name_user_name_ -description text' 설명에 공백이 포함된 경우 큰따옴표로 묶어야 합니다.
로컬 사용자 계정을 활성화하거나 비활성화합니다	'vserver cifs users-and-groups local-user modify -vserver_vserver_name_-user-name_user_name_-is -account-disabled{true
false}'	로컬 사용자 계정의 이름을 바꿉니다

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver)의 로컬 사용자 "'cifs_server\sue""를 "'cifs_server\sue_new""로 바꿉니다.1

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

로컬 **ONTAP SMB** 사용자 계정 활성화 또는 비활성화

사용자가 SMB 연결을 통해 SVM(스토리지 가상 머신)에 포함된 데이터에 액세스할 수 있도록 하려면 로컬 사용자 계정을 활성화합니다. 사용자가 SMB를 통해 SVM 데이터에 액세스하지 못하도록 하려면 로컬 사용자 계정을 사용하지 않도록 설정할 수도 있습니다.

이 작업에 대해

사용자 계정을 수정하여 로컬 사용자를 활성화할 수 있습니다.

단계

1. 적절한 작업을 수행합니다.

원하는 작업	명령 입력...
사용자 계정을 활성화합니다	'vserver cifs users-and-groups local-user modify -vserver_vserver_name_-user-name_user_name_ -is-account-disabled false'
사용자 계정을 비활성화합니다	'vserver cifs users-and-groups local-user modify -vserver_vserver_name_-user-name_user_name_ -is-account-disabled true'

로컬 **ONTAP SMB** 사용자 계정 비밀번호 변경

로컬 사용자의 계정 암호를 변경할 수 있습니다. 이 방법은 사용자의 암호가 손상되었거나 사용자가 암호를 잊어버린 경우에 유용합니다.

단계

1. 'vserver cifs users-and-groups local-user set-password-vserver_vserver_name_-user-name_user_name_' 작업을 수행하여 암호를 변경하십시오

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver) VS1 과 연관된 로컬 사용자 ""cifs_server\sue""의 암호를 설정합니다.

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

관련 정보

로컬 사용자에 대한 암호 복잡성 구성

서버 보안 설정에 대한 정보 표시

ONTAP SMB 로컬 사용자에 대한 정보 표시

모든 로컬 사용자의 목록을 요약 양식에 표시할 수 있습니다. 특정 사용자에 대해 구성된 계정 설정을 확인하려면 해당 사용자에 대한 자세한 계정 정보와 여러 사용자에 대한 계정 정보를 표시할 수 있습니다. 이 정보를 통해 사용자 설정을 수정해야 하는지 여부를 확인하고 인증 또는 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

사용자 암호에 대한 정보는 표시되지 않습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
SVM(스토리지 가상 시스템)의 모든 사용자에 대한 정보 표시	'vserver cifs users-and-groups local-user show -vserver_vserver_name_'
사용자에 대한 자세한 계정 정보를 표시합니다	'vserver cifs users-and-groups local-user show-instance-vserver_vserver_name_-user-name_user_name_'

명령을 실행할 때 선택할 수 있는 다른 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `vserver cifs` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 예제는 SVM VS1 의 모든 로컬 사용자에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- ---------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones
```

로컬 사용자의 **ONTAP SMB** 그룹 멤버십에 대한 정보를 표시합니다.

로컬 사용자가 속한 로컬 그룹에 대한 정보를 표시할 수 있습니다. 이 정보를 사용하여 파일 및 폴더에 대한 사용자의 액세스 권한을 결정할 수 있습니다. 이 정보는 사용자가 파일 및 폴더에 대해 가질 액세스 권한을 결정하거나 파일 액세스 문제를 해결할 때 유용할 수 있습니다.

이 작업에 대해

명령을 사용자 지정하여 표시할 정보만 표시할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
지정된 로컬 사용자의 로컬 사용자 구성원 정보를 표시합니다	'vserver cifs users-and-groups local-user show-membership-user-name_user_name_'
이 로컬 사용자가 구성원인 로컬 그룹의 로컬 사용자 구성원 정보를 표시합니다	'vserver cifs users-and-groups local-user show-membership_group_name_'
지정된 SVM(스토리지 가상 머신)과 연결된 로컬 사용자의 사용자 구성원 정보를 표시합니다.	'vserver cifs users-and-groups local-user show-membership-vserver_vserver_name_'
지정된 SVM의 모든 로컬 사용자에 대한 세부 정보를 표시합니다	'vserver cifs users-and-groups local-user show-membership-instance-vserver_vserver_name_'

예

다음 예에서는 SVM VS1 상의 모든 로컬 사용자에 대한 구성원 정보를 표시합니다. 사용자 "'cifs_server\Administrator'"는 "'BUILTIN\Administrators'" 그룹의 구성원이고 "'cifs_server\sue'"는 "'cifs_server\G1'" 그룹의 구성원입니다.

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

로컬 **ONTAP SMB** 사용자 계정 삭제

CIFS 서버에 대한 로컬 SMB 인증이 더 이상 필요하지 않거나 SVM에 포함된 데이터에 대한 액세스 권한을 결정하기 위해 SVM(스토리지 가상 시스템)에서 로컬 사용자 계정을 삭제할 수 있습니다.

이 작업에 대해

로컬 사용자를 삭제할 때 다음 사항에 유의하십시오.

- 파일 시스템이 변경되지 않았습니다.

  이 사용자를 참조하는 파일 및 디렉토리의 Windows 보안 설명자는 조정되지 않습니다.

- 로컬 사용자에 대한 모든 참조는 멤버 자격 및 권한 데이터베이스에서 제거됩니다.
- Administrator와 같이 잘 알려진 표준 사용자는 삭제할 수 없습니다.

단계

1. 삭제할 로컬 사용자 계정의 이름을 확인합니다. 'vserver cifs users-and-groups local-user show -vserver_vserver_name_'
2. 로컬 사용자 'vserver cifs users-and-groups local-user delete -vserver_vserver_name_-user-name_username_name_'을 삭제합니다
3. 사용자 계정이 삭제되었는지 확인합니다. 'vserver cifs users-and-groups local-user show -vserver_vserver_name_'

예

다음 예에서는 SVM VS1 관련 로컬 사용자 ""cifs_server\sue""를 삭제합니다.

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name      Description
-------- ---------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                    Full Name      Description
-------- ---------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
```

로컬 그룹을 관리합니다

로컬 **ONTAP SMB** 그룹 수정

기존 로컬 그룹에 대한 설명을 변경하거나 그룹의 이름을 변경하여 기존 로컬 그룹을 수정할 수 있습니다.

원하는 작업	명령 사용...
로컬 그룹 설명을 수정합니다	'vserver cifs users-and-groups local-group modify -vserver_vserver_name_-group-name_group_name_-description text' 설명에 공백이 포함되어 있으면 큰따옴표로 묶어야 합니다.
로컬 그룹의 이름을 바꿉니다	'vserver cifs users-and-groups local-group rename -vserver_vserver_name_-group-name_group_name_-new-group-name_new_group_name_'

예

다음 예에서는 로컬 그룹 ""cifs_server\engineering""의 이름을 ""cifs_server\engineering_new""로 바꿉니다.

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

다음 예에서는 로컬 그룹 ""cifs_server\engineering""의 설명을 수정합니다.

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

ONTAP SMB 로컬 그룹에 대한 정보 표시

클러스터 또는 지정된 SVM(스토리지 가상 머신)에 구성된 모든 로컬 그룹 목록을 표시할 수 있습니다. 이 정보는 SVM에 포함된 데이터에 대한 파일 액세스 문제 또는 SVM의 사용자 권한(권한) 문제를 해결할 때 유용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

에 대한 정보를 원할 경우...	명령 입력...
클러스터의 모든 로컬 그룹입니다	'vserver cifs users-and-groups local-group show'를 참조하십시오
SVM의 모든 로컬 그룹	'vserver cifs users-and-groups local-group show -vserver_vserver_name_'

이 명령을 실행할 때 선택할 수 있는 다른 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `vserver cifs` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 예제는 SVM VS1 의 모든 로컬 그룹에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                    Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

로컬 **ONTAP SMB** 그룹 구성원 자격을 관리합니다

로컬 또는 도메인 사용자를 추가 및 제거하거나 도메인 그룹을 추가 및 제거하여 로컬 그룹 구성원 자격을 관리할 수 있습니다. 이 기능은 그룹에 배치된 액세스 제어를 기반으로 데이터에 대한 액세스를 제어하려는 경우 또는 사용자에게 해당 그룹에 연결된 권한을 부여하려는 경우에 유용합니다.

이 작업에 대해

로컬 그룹에 구성원을 추가하기 위한 지침:

- special_everyone_group에 사용자를 추가할 수 없습니다.
- 사용자를 추가하려면 로컬 그룹이 있어야 합니다.
- 사용자를 로컬 그룹에 추가하려면 사용자가 있어야 합니다.
- 로컬 그룹을 다른 로컬 그룹에 추가할 수 없습니다.
- 도메인 사용자 또는 그룹을 로컬 그룹에 추가하려면 Data ONTAP에서 SID에 대한 이름을 확인할 수 있어야 합니다.

로컬 그룹에서 구성원을 제거하는 지침:

- special_everyone_group에서 구성원을 제거할 수 없습니다.
- 구성원을 제거할 그룹이 있어야 합니다.
- ONTAP는 그룹에서 제거하려는 구성원 이름을 해당 SID로 확인할 수 있어야 합니다.

단계

1. 그룹에서 구성원을 추가 또는 제거합니다.

원하는 작업	그런 다음 명령을 사용합니다...
그룹에 구성원을 추가합니다	'vserver cifs users-and-groups local-group add-member-vserver_name_-group-name_group_name_-member-names name[,...]'지정된 로컬 그룹에 추가할 쉼표로 구분된 로컬 사용자, 도메인 사용자 또는 도메인 그룹의 목록을 지정할 수 있습니다.

원하는 작업	그런 다음 명령을 사용합니다...
그룹에서 구성원을 제거합니다	'vserver cifs users-and-groups local-group remove-memers-vserver_name_-group-name_group_name_-member-names name[,...]'지정된 로컬 그룹에서 제거할 로컬 사용자, 도메인 사용자 또는 도메인 그룹의 쉼표로 구분된 목록을 지정할 수 있습니다.

다음 예에서는 SVM VS1 상의 로컬 그룹 "sMB_server\sue"와 도메인 그룹 "AD_DOM\DOM_ENG"를 로컬 그룹 "sMB_server\engineering"에 추가합니다.

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

다음 예에서는 SVM VS1 로컬 그룹 "sMB_server\sue"와 "sMB_server\james"를 SVM VS1 로컬 그룹 "sMB_server\engineering"에서 제거합니다.

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

관련 정보

로컬 그룹 구성원에 대한 정보를 표시합니다

로컬 그룹 구성원에 대한 **ONTAP SMB** 정보 표시

클러스터 또는 지정된 SVM(스토리지 가상 머신)에 구성된 로컬 그룹의 모든 구성원 목록을 표시할 수 있습니다. 이 정보는 파일 액세스 문제 또는 사용자 권한(권한) 문제를 해결할 때 유용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

다음에 대한 정보를 표시하려면...	명령 입력...
클러스터의 모든 로컬 그룹의 구성원입니다	'vserver cifs users-and-groups local-group show-ups'
SVM에 있는 모든 로컬 그룹의 구성원	'vserver cifs users-and-groups local-group show-ners-vserver_vserver_name_'

예

다음 예는 SVM VS1 로컬 그룹의 모든 구성원에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

로컬 **ONTAP SMB** 그룹 삭제

SVM(스토리지 가상 시스템)에서 로컬 그룹을 삭제하여 해당 SVM과 관련된 데이터에 대한 액세스 권한을 결정하거나 SVM 사용자 권한(권한)을 그룹 멤버에 할당할 필요가 없는 경우 해당 로컬 그룹을 삭제할 수 있습니다.

이 작업에 대해

로컬 그룹을 삭제할 때 다음 사항에 유의하십시오.

- 파일 시스템이 변경되지 않았습니다.

  이 그룹을 참조하는 파일 및 디렉토리의 Windows 보안 설명자는 조정되지 않습니다.

- 그룹이 없으면 오류가 반환됩니다.
- special_everyone_group은 삭제할 수 없습니다.
- BUILTIN\Administrators__BUILTIN\Users_와 같은 기본 제공 그룹은 삭제할 수 없습니다.

단계

1. SVM에 로컬 그룹 목록을 표시하여 삭제할 로컬 그룹의 이름을 확인합니다. 'vserver cifs users-and-groups local-group show -vserver vserver_name'
2. 로컬 그룹 'vserver cifs users-and-groups local-group delete -vserver_vserver_name_-group-name_group_name_'을 삭제합니다
3. 그룹이 삭제되었는지 확인합니다. 'vserver cifs users-and-groups local-user show -vserver_vserver_name_'

예

다음 예에서는 SVM VS1 관련 로컬 그룹 ""cifs_server\sales""를 삭제합니다.

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

로컬 데이터베이스에서 **ONTAP SMB** 도메인 사용자 및 그룹 이름 업데이트

CIFS 서버의 로컬 그룹에 도메인 사용자 및 그룹을 추가할 수 있습니다. 이러한 도메인 개체는 클러스터의 로컬 데이터베이스에 등록됩니다. 도메인 개체의 이름이 변경된 경우 로컬 데이터베이스를 수동으로 업데이트해야 합니다.

이 작업에 대해

도메인 이름을 업데이트할 SVM(스토리지 가상 시스템)의 이름을 지정해야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 적절한 작업을 수행합니다.

도메인 사용자 및 그룹을 업데이트하려면 다음을 수행합니다.	이 명령 사용...
성공적으로 업데이트되었지만 업데이트에 실패한 도메인 사용자 및 그룹을 표시합니다	'vserver cifs users-and-groups update-names-vserver_vserver_name_'
성공적으로 업데이트된 도메인 사용자 및 그룹을 표시합니다	'vserver cifs users-and-groups update-names-vserver_vserver_name_-display-failed-only false'

도메인 사용자 및 그룹을 업데이트하려면 다음을 수행합니다.	이 명령 사용...
업데이트에 실패한 도메인 사용자 및 그룹만 표시합니다	'vserver cifs users-and-groups update-names-vserver_vserver_name_-display-failed-only true'
업데이트에 대한 모든 상태 정보를 표시하지 않습니다	'vserver cifs users-and-groups update-names-vserver_vserver_name_-suppress-all-output TRUE'

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 스토리지 가상 머신(SVM, 이전의 Vserver) VS1 과 관련된 도메인 사용자 및 그룹의 이름을 업데이트합니다. 마지막 업데이트 시 업데이트해야 할 종속 이름 체인이 있습니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

로컬 권한을 관리합니다

ONTAP SMB 로컬 또는 도메인 사용자나 그룹에 권한 추가

권한을 추가하여 로컬 또는 도메인 사용자 또는 그룹의 사용자 권한을 관리할 수 있습니다. 추가된 권한은 이러한 개체에 할당된 기본 권한을 재정의합니다. 사용자 또는 그룹에 있는 권한을 사용자 지정할 수 있으므로 보안이 강화됩니다.

시작하기 전에

권한을 추가할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

이 작업에 대해

객체에 권한을 추가하면 해당 사용자 또는 그룹에 대한 기본 권한이 재정의됩니다. 권한을 추가해도 이전에 추가한 권한은 제거되지 않습니다.

로컬 또는 도메인 사용자 또는 그룹에 권한을 추가할 때는 다음 사항을 염두에 두어야 합니다.

- 하나 이상의 권한을 추가할 수 있습니다.
- 도메인 사용자 또는 그룹에 권한을 추가할 때 ONTAP는 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다.

  ONTAP가 도메인 컨트롤러에 연결할 수 없는 경우 명령이 실패할 수 있습니다.

단계

1. 로컬 또는 도메인 사용자 또는 그룹에 하나 이상의 권한을 추가합니다. 'vserver cifs users-and-groups privilege add-privilege-vserver_name_-user-or-group-name name name-Privileges_Privilege_[,...]'
2. 원하는 권한이 객체에 적용되었는지 확인합니다. 'vserver cifs users-and-groups privilege show-vserver_name_-user-or-group-name_name_'

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver)의 사용자 " cifs_server\sue ""에 "'seTcbPrivilege'" 및 "'setTakeOwnershipPrivilege"" 권한을 추가합니다1.

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

ONTAP SMB 로컬 또는 도메인 사용자나 그룹의 권한 제거

권한을 제거하여 로컬 또는 도메인 사용자 또는 그룹에 대한 사용자 권한을 관리할 수 있습니다. 이렇게 하면 사용자와 그룹이 보유한 최대 권한을 사용자 지정할 수 있으므로 보안이 강화됩니다.

시작하기 전에

권한을 제거할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

이 작업에 대해

로컬 또는 도메인 사용자 또는 그룹에서 권한을 제거할 때는 다음 사항을 염두에 두어야 합니다.

- 하나 이상의 권한을 제거할 수 있습니다.
- 도메인 사용자 또는 그룹에서 권한을 제거할 때 ONTAP는 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다.

  ONTAP가 도메인 컨트롤러에 연결할 수 없는 경우 명령이 실패할 수 있습니다.

단계

1. 로컬 또는 도메인 사용자 또는 그룹에서 하나 이상의 권한을 제거합니다. 'vserver cifs users-and-groups privilege remove-privilege-vserver_name_-user-or-group-name_name_-Privileges_Privilege_[,...]'
2. 원하는 권한이 'vserver cifs users-and-groups privilege show-vserver_name_-user-or-group-name_name_' 객체에서 제거되었는지 확인합니다

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver)의 사용자 " cifs_server\sue "(cifs_server\sue ")에서 "'seTcbPrivilege' 및 "'setegenershipPrivilege'" 권한을 제거합니다1.

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

ONTAP SMB 로컬 또는 도메인 사용자 및 그룹에 대한 권한 재설정

로컬 또는 도메인 사용자 및 그룹에 대한 권한을 재설정할 수 있습니다. 이 기능은 로컬 또는 도메인 사용자 또는 그룹에 대한 권한을 수정한 후 해당 수정 사항이 더 이상 필요 또는 필요하지 않을 때 유용합니다.

이 작업에 대해

로컬 또는 도메인 사용자 또는 그룹에 대한 권한을 재설정하면 해당 개체에 대한 권한 항목이 제거됩니다.

단계

1. 로컬 또는 도메인 사용자 또는 그룹에 대한 권한을 재설정합니다. 'vserver cifs users-and-groups privilege reset-privilege-vserver_name_-user-or-group-name_name_'
2. 객체에 대한 권한이 재설정되었는지 확인합니다. 'vserver cifs users-and-groups privilege show -vserver_vserver_name_-user-or-group-name_name_'

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver) VS1 에서 사용자 "'cifs_server\sue'"에 대한 권한을 재설정합니다. 기본적으로 일반 사용자는 자신의 계정과 연결된 권한이 없습니다.

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

다음 예제에서는 ""BUILTIN\Administrators" 그룹에 대한 권한을 다시 설정하여 권한 항목을 효과적으로 제거합니다.

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ -------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

ONTAP SMB 권한 재정의에 대한 정보 표시

도메인 또는 로컬 사용자 계정 또는 그룹에 할당된 사용자 지정 권한에 대한 정보를 표시할 수 있습니다. 이 정보를 통해 원하는 사용자 권한이 적용되는지 여부를 확인할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

다음에 대한 정보를 표시하려면...	이 명령을 입력하십시오...
SVM(스토리지 가상 시스템)의 모든 도메인 및 로컬 사용자 및 그룹에 대한 사용자 지정 권한	'vserver cifs users-and-groups privilege show -vserver_vserver_name_'
SVM에서 특정 도메인 또는 로컬 사용자 및 그룹에 대한 사용자 지정 권한	'vserver cifs users-and-groups 권한 표시 -vserver_vserver_name_-user-or-group-name_name_'

이 명령을 실행할 때 선택할 수 있는 다른 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `vserver cifs users-and-groups privilege show` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 명령을 실행하면 SVM VS1 에 대한 로컬 또는 도메인 사용자 및 그룹과 명시적으로 연결된 모든 권한이 표시됩니다.

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------- ---------------------  ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

우회 통과 검사를 구성합니다

ONTAP SMB 바이패스 트래버스 검사 구성에 대해 알아보세요.

통과 확인 무시 사용자 권한(_privilege_라고도 함)은 사용자가 이동 중인 디렉터리에 대한 권한이 없더라도 경로 내의 모든 디렉터리를 파일로 이동할 수 있는지 여부를 결정합니다. 통과 확인을 허용 또는 허용하지 않을 경우 어떤 일이 발생하는지, 그리고 SVM(스토리지 가상 시스템)에서 사용자에 대한 통과 확인을 건너뛰도록 구성하는 방법을 이해해야 합니다.

우회 통과 확인을 허용 또는 허용하지 않을 때 발생하는 현상

- 허용되는 경우 사용자가 파일에 액세스하려고 할 때 ONTAP는 파일에 대한 액세스 허용 또는 거부 여부를 결정할 때 중간 디렉토리에 대한 통과 권한을 확인하지 않습니다.
- 허용되지 않는 경우 ONTAP는 파일 경로에 있는 모든 디렉토리에 대해 트래버스(실행) 권한을 확인합니다.

  중간 디렉토리에 ""X""(통과 권한)이 없으면 ONTAP는 해당 파일에 대한 액세스를 거부합니다.

우회 통과 검사를 구성합니다

ONTAP CLI를 사용하거나 이 사용자 권한으로 Active Directory 그룹 정책을 구성하여 통과 통과 확인 바이패스를 구성할 수 있습니다.

'eChangeNotifyPrivilege' 권한은 사용자가 횡단 확인을 우회할 수 있는지 여부를 제어합니다.

- SVM의 로컬 SMB 사용자 또는 그룹 또는 도메인 사용자 또는 그룹에 추가하면 통과 확인을 건너뛸 수 있습니다.
- SVM의 로컬 SMB 사용자 또는 그룹 또는 도메인 사용자 또는 그룹에서 제거하면 통과 확인을 건너뛸 수 없습니다.

기본적으로 SVM의 다음 BUILTIN 그룹에는 횡단 확인을 건너뛸 수 있는 권한이 있습니다.

- 'BUILTIN\Administrators'
- 'BUILTIN\Power Users'
- 'BUILTIN\Backup Operators'
- 'BUILTIN\Users'
- '모든 사람'

이러한 그룹 중 하나의 구성원이 통과 확인을 건너뛰도록 허용하지 않으려면 그룹에서 이 권한을 제거해야 합니다.

CLI를 사용하여 SVM에서 로컬 SMB 사용자 및 그룹에 대한 통과 검사를 구성할 때 다음 사항을 염두에 두어야 합니다.

- 사용자 지정 로컬 또는 도메인 그룹의 구성원이 통과 확인을 건너뛰도록 하려면 해당 그룹에 'eChangeNotifyPrivilege' 권한을 추가해야 합니다.
- 개별 로컬 또는 도메인 사용자가 횡단 검사를 무시하도록 허용하고 해당 권한이 있는 그룹의 구성원이 아닌 경우 해당 사용자 계정에 'eChangeNotifyPrivilege' 권한을 추가할 수 있습니다.
- 언제든지 'ChangeNotifyPrivilege' 권한을 제거하여 로컬 또는 도메인 사용자 또는 그룹에 대한 통과 확인을 사용하지 않도록 설정할 수 있습니다.

> ⓘ 지정된 로컬 또는 도메인 사용자 또는 그룹에 대한 우회 트래버스 검사를 비활성화하려면 "Everyone" 그룹에서 'ChangeNotifyPrivilege' 권한도 제거해야 합니다.

관련 정보

- 사용자 또는 그룹이 디렉토리 통과 확인을 건너뛰도록 허용합니다
- 디렉토리 통과 확인을 거치지 않고 사용자 또는 그룹을 허용하지 않습니다
- 볼륨에서 파일 이름 번역을 위한 문자 매핑 구성
- 공유 액세스 제어 목록 만들기
- Storage-Level Access Guard를 사용하여 파일 액세스를 보호합니다
- 지원되는 권한 목록입니다
- 로컬 또는 도메인 사용자 또는 그룹에 권한을 추가합니다

사용자 또는 그룹이 **ONTAP SMB** 디렉터리 트래버스 검사를 우회하도록 허용

사용자가 이동 중인 디렉토리에 대한 사용 권한이 없더라도 경로 내의 모든 디렉토리를 통과할 수 있도록 하려면 SVM(Storage Virtual Machine)의 로컬 SMB 사용자 또는 그룹에 'seChangeNotifyPrivilege' 권한을 추가하면 됩니다. 기본적으로 사용자는 디렉터리 통과 확인을 건너뛸 수 있습니다.

시작하기 전에

- SVM에 SMB 서버가 있어야 합니다.
- 로컬 사용자 및 그룹 SMB 서버 옵션을 활성화해야 합니다.
- 'eChangeNotifyPrivilege' 권한을 추가할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

이 작업에 대해

도메인 사용자 또는 그룹에 권한을 추가할 때 ONTAP는 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다. ONTAP가 도메인 컨트롤러에 연결할 수 없으면 명령이 실패할 수 있습니다.

단계

1. 로컬 또는 도메인 사용자 또는 그룹에 'seChangeNotifyPrivilege' 권한을 추가하여 통과 확인을 사용하지 않도록 설정합니다. 'vserver cifs users-and-groups privilege add-privilege_vserver_name_-user-or-group-name_name_-Privileges SeChangeNotifyPrivilege'

   '-user-or-group-name' 매개 변수의 값은 로컬 사용자 또는 그룹 또는 도메인 사용자 또는 그룹입니다.

2. 지정된 사용자 또는 그룹이 통과 확인 생략 기능을 사용하도록 설정했는지 확인합니다. 'vserver cifs users-and-groups privilege show-vserver_name_-user-or-group-name_name_'

예

다음 명령을 사용하면 "'Example\eng'" 그룹에 속한 사용자가 'seChangeNotifyPrivilege' 권한을 그룹에 추가하여 디렉터리 통과 확인을 건너뛸 수 있습니다.

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege
```

관련 정보

디렉토리 통과 확인을 거치지 않고 사용자 또는 그룹을 허용하지 않습니다

사용자 또는 그룹이 **ONTAP SMB** 디렉터리 트래버스 검사를 우회하는 것을 허용하지 않음

사용자가 이동 중인 디렉토리에 대한 권한이 없기 때문에 경로 내의 모든 디렉토리를 이동하지 않으려면 SVM(Storage Virtual Machine)의 로컬 SMB 사용자 또는 그룹에서 'seChangeNotifyPrivilege' 권한을 제거할 수 있습니다.

시작하기 전에

권한을 제거할 로컬 또는 도메인 사용자 또는 그룹이 이미 있어야 합니다.

이 작업에 대해

도메인 사용자 또는 그룹에서 권한을 제거할 때 ONTAP는 도메인 컨트롤러에 문의하여 도메인 사용자 또는 그룹의 유효성을 검사할 수 있습니다. ONTAP가 도메인 컨트롤러에 연결할 수 없으면 명령이 실패할 수 있습니다.

단계

1. 통과 확인 무시 허용 안 함: 'vserver cifs users-and-groups privilege remove-privilege-vserver_vserver_name_-user-or-group-name_name_-Privileges SeChangeNotifyPrivilege'

   이 명령은 '-user-or-group-name_name_' 매개 변수 값으로 지정한 로컬 또는 도메인 사용자 또는 그룹에서 'seChangeNotifyPrivilege' 권한을 제거합니다.

2. 지정된 사용자 또는 그룹이 통과 확인을 사용하지 않도록 설정했는지 확인합니다. 'vserver cifs users-and-groups privilege show-vserver_name_-user-or-group-name_name_'

예

다음 명령을 실행하면 디렉토리 트래버스 검사를 거치지 않고 "'example\eng'" 그룹에 속한 사용자가 사용할 수 없습니다.

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           -
```

관련 정보

사용자 또는 그룹이 디렉토리 통과 확인을 건너뛰도록 허용합니다

파일 보안 및 감사 정책에 대한 정보를 표시합니다

ONTAP SMB 파일 보안 및 감사 정책 보기에 대해 알아보세요

SVM(스토리지 가상 머신)의 볼륨 내에 포함된 파일 및 디렉토리의 파일 보안에 대한 정보를 표시할 수 있습니다. FlexVol 볼륨의 감사 정책에 대한 정보를 표시할 수 있습니다. 구성된 경우 FlexVol 볼륨의 저장소 수준 액세스 가드 및 동적 액세스 제어 보안 설정에 대한 정보를 표시할 수 있습니다.

파일 보안에 대한 정보 표시

다음 보안 스타일을 사용하여 볼륨 및 Qtree(FlexVol 볼륨의 경우) 내에 포함된 데이터에 적용되는 파일 보안에 대한 정보를 표시할 수 있습니다.

- NTFS입니다
- Unix
- 혼합

감사 정책에 대한 정보 표시

다음 NAS 프로토콜을 통해 FlexVol 볼륨의 액세스 이벤트를 감사하기 위한 감사 정책에 대한 정보를 표시할 수 있습니다.

- SMB(모든 버전)
- NFSv4.x

스토리지 레벨 액세스 가드(슬래그) 보안에 대한 정보 표시

스토리지 레벨 액세스 가드 보안은 FlexVol 볼륨 및 qtree 개체에 다음 보안 스타일로 적용할 수 있습니다.

- NTFS입니다
- 혼합
- UNIX(볼륨을 포함하는 SVM에서 CIFS 서버가 구성된 경우)

DAC(Dynamic Access Control) 보안에 대한 정보 표시

동적 액세스 제어 보안은 다음 보안 스타일을 사용하여 FlexVol 볼륨 내의 개체에 적용할 수 있습니다.

- NTFS입니다
- 혼합(오브젝트에 NTFS 유효 보안이 있는 경우)

관련 정보

- Storage-Level Access Guard를 사용하여 안전한 파일 액세스에 대해 알아보세요
- 서버의 Storage-Level Access Guard에 대한 정보 표시

NTFS 보안 스타일 볼륨에서 **ONTAP SMB** 파일 보안에 대한 정보 표시

NTFS 보안 스타일 볼륨의 파일 및 디렉터리 보안에 대한 정보(보안 스타일 및 효과적인 보안 스타일, 적용되는 권한, DOS 속성 정보 등)를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 폴더 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- NTFS 보안 스타일 볼륨 및 qtree는 파일 액세스 권한을 결정할 때 NTFS 파일 권한과 Windows 사용자 및 그룹만 사용하므로 UNIX 관련 출력 필드에는 표시 전용 UNIX 파일 권한 정보가 포함됩니다.
- ACL 출력은 NTFS 보안이 설정된 파일 및 폴더에 대해 표시됩니다.
- 볼륨 루트 또는 qtree에서 Storage-Level Access Guard 보안을 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 파일 ACL과 Storage-Level Access Guard ACL이 모두 표시될 수 있습니다.
- 또한 동적 액세스 제어가 지정된 파일 또는 디렉터리 경로에 대해 구성된 경우 이 출력에는 동적 액세스 제어 ACE에 대한 정보도 표시됩니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver_vserver_name_-path_path_'
세부 정보가 확장됩니다	'vserver security file-directory show -vserver_vserver_name_-path_path_-expand-mask true'

예

다음 예제는 SVM VS1 경로의 /vol4" 보안 정보를 보여줍니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                          Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

다음 예에서는 SVM VS1 경로의 /data/engineering에 대한 확장된 마스크와 함께 보안 정보를 표시합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

               Vserver: vs1
             File Path: /data/engineering
     File Inode Number: 5544
```

```
          Security Style: ntfs
         Effective Style: ntfs
          DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
```

```
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
```

```
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

다음 예에서는 SVM VS1 에서 경로 '/datavol1’이 있는 볼륨에 대한 Storage-Level Access Guard 보안 정보를 비롯한 보안 정보를 표시합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

관련 정보

- 혼합 보안 형식 볼륨의 파일 보안에 대한 정보를 표시합니다
- UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다

보안 스타일 및 효과적인 보안 스타일, 적용되는 사용 권한, UNIX 소유자 및 그룹에 대한 정보 등 혼합 보안 스타일 볼륨에 대한 파일 및 디렉터리 보안에 대한 정보를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 폴더 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- 혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉토리 등 UNIX 파일 권한을 사용하는 일부 파일 및 폴더가 포함될 수 있습니다.
- 혼합 보안 형식 볼륨의 최상위 수준에는 UNIX 또는 NTFS의 효과적인 보안이 있을 수 있습니다.
- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

  모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 디렉토리의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 UNIX 파일 사용 권한과 Storage-Level Access Guard ACL이 모두 표시될 수 있습니다.
- 명령에 입력한 경로가 NTFS 유효 보안을 사용하는 데이터인 경우 해당 파일 또는 디렉토리 경로에 동적 액세스 제어가 구성되어 있으면 동적 액세스 제어 ACE에 대한 정보도 출력에 표시됩니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver vserver_name -path path path'
세부 정보가 확장됩니다	'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true'

예

다음 예에서는 SVM VS1 경로 '/projects'에 대한 보안 정보를 확장된 마스크 형식으로 표시합니다. 이 혼합 보안 방식 경로에는 UNIX의 효과적인 보안이 있습니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

다음 예제는 SVM VS1 경로 '/data'에 대한 보안 정보를 보여줍니다. 이 혼합 보안 방식 경로에는 NTFS의 효과적인 보안이 있습니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

다음 예에서는 SVM VS1 경로의 '/datavol5' 경로에 있는 볼륨에 대한 보안 정보를 표시합니다. 이러한 혼합 보안 유형의 최상위 수준에는 UNIX의 효과적인 보안이 있습니다. 이 볼륨에는 Storage-Level Access Guard 보안이 있습니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

관련 정보

- NTFS 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다
- UNIX 보안 스타일 볼륨의 파일 보안에 대한 정보를 표시합니다

UNIX 보안 스타일 볼륨에서 **ONTAP SMB** 파일 보안에 대한 정보 표시

UNIX 보안 스타일 볼륨의 파일 및 디렉터리 보안에 대한 정보(보안 스타일 및 효과적인 보안 스타일, 적용되는 사용 권한, UNIX 소유자 및 그룹에 대한 정보 등)를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 파일 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 파일 또는 디렉토리 보안 정보를 표시할 데이터의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- UNIX 보안 스타일 볼륨 및 qtree는 파일 액세스 권한을 결정할 때 모드 비트 또는 NFSv4 ACL 중 하나의 UNIX 파일 권한만 사용합니다.
- NFSv4 보안이 설정된 파일 및 폴더에 대해서만 ACL 출력이 표시됩니다.

  모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 디렉토리의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- NFSv4 보안 설명자의 경우 ACL 출력의 소유자 및 그룹 출력 필드는 적용되지 않습니다.

  NTFS 보안 설명자에만 의미가 있습니다.

- SVM에 CIFS 서버가 구성된 경우 UNIX 볼륨 또는 qtree에서 Storage-Level Access Guard 보안이 지원되므로 '-path' 매개 변수에 지정된 볼륨 또는 qtree에 적용된 Storage-Level Access Guard 보안에 대한 정보가 출력에 포함될 수 있습니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver_vserver_name_-path_path_'
세부 정보가 확장됩니다	'vserver security file-directory show -vserver_vserver_name_-path_path_-expand-mask true'

예

다음 예제는 SVM VS1 경로의 / home 경로에 대한 보안 정보를 표시합니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                          Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

다음 예에서는 SVM VS1 경로의 / home 경로에 대한 보안 정보를 확장된 마스크 형식으로 표시합니다.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                          Unix User Id: 0
                         Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

관련 정보

- 보안 스타일 볼륨의 파일 보안에 대한 정보 표시
- 혼합 보안 형식 볼륨의 파일 보안에 대한 정보를 표시합니다

SMB FlexVol 볼륨의 **NTFS** 감사 정책에 대한 정보를 표시하는 **ONTAP** 명령

FlexVol 볼륨에서 보안 스타일 및 효과적인 보안 스타일의 정의, 적용되는 권한 및 시스템 액세스 제어 목록에 대한 정보를 포함하여 NTFS 감사 정책에 대한 정보를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 감사 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 감사 정보를 표시할 파일 또는 폴더의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- NTFS 보안 스타일 볼륨 및 qtree는 감사 정책에 NTFS SACL(시스템 액세스 제어 목록)만 사용합니다.
- NTFS 효과적인 보안이 적용된 혼합 보안 스타일 볼륨의 파일과 폴더에 NTFS 감사 정책이 적용될 수 있습니다.

  혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉토리 등 UNIX 파일 권한을 사용하는 일부 파일과 디렉토리가 포함될 수 있습니다.

- 혼합 보안 형식 볼륨의 최상위 수준에는 UNIX 또는 NTFS의 효과적인 보안이 포함될 수 있으며 NTFS SACL이 포함될 수도 있고 포함되지 않을 수도 있습니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 파일 및 폴더 NFSv4 SACL 및 Storage-Level Access Guard NTFS SACL이 모두 표시될 수 있습니다.
- 명령에 입력한 경로가 NTFS 유효 보안을 사용하는 데이터인 경우 해당 파일 또는 디렉토리 경로에 동적 액세스 제어가 구성되어 있으면 동적 액세스 제어 ACE에 대한 정보도 출력에 표시됩니다.
- NTFS 유효 보안이 있는 파일 및 폴더에 대한 보안 정보를 표시할 때 UNIX 관련 출력 필드에는 표시 전용 UNIX 파일 권한 정보가 포함됩니다.

  NTFS 보안 스타일 파일 및 폴더는 파일 액세스 권한을 결정할 때 NTFS 파일 권한과 Windows 사용자 및 그룹만 사용합니다.

- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

  모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 폴더의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.

단계

1. 파일 및 디렉터리 감사 정책 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver vserver_name -path path path'

정보를 표시하려면...	다음 명령을 입력합니다...
를 참조하십시오	'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true'

예

다음 예에서는 SVM VS1 경로의 /Corp 경로에 대한 감사 정책 정보를 표시합니다. 경로에 NTFS 유효 보안이 있습니다. NTFS 보안 설명자는 성공 및 성공/실패 SACL 항목을 모두 포함합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

다음 예제는 SVM VS1 경로의 /datavol1 경로에 대한 감사 정책 정보를 표시합니다. 이 경로에는 일반 파일 및 폴더 SACL과 Storage-Level Access Guard SACL이 모두 포함됩니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

SMB FlexVol 볼륨의 **NFSv4** 감사 정책에 대한 정보를 표시하는 **ONTAP** 명령

보안 스타일 및 효과적인 보안 스타일의 정의, 적용되는 권한 및 SACL(시스템 액세스 제어 목록)에 대한 정보를 포함하여 ONTAP CLI를 사용하여 FlexVol 볼륨에서 NFSv4 감사 정책에 대한

정보를 표시할 수 있습니다. 결과를 사용하여 보안 구성을 확인하거나 감사 문제를 해결할 수 있습니다.

이 작업에 대해

SVM(스토리지 가상 시스템)의 이름과 감사 정보를 표시할 파일 또는 디렉토리의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- UNIX 보안 스타일 볼륨 및 qtree는 감사 정책에 NFSv4 SACL만 사용합니다.
- UNIX 보안 스타일의 혼합 보안 스타일 볼륨에 있는 파일과 디렉토리에는 NFSv4 감사 정책이 적용될 수 있습니다.

  혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉토리 등 UNIX 파일 권한을 사용하는 일부 파일과 디렉토리가 포함될 수 있습니다.

- 혼합 보안 형식 볼륨의 최상위 수준은 UNIX 또는 NTFS의 유효 보안을 가질 수 있으며 NFSv4 SACL을 포함하거나 포함하지 않을 수 있습니다.
- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

  모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 폴더의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 NFSv4 파일 및 디렉터리 SACL과 Storage-Level Access Guard NTFS SACL이 모두 표시될 수 있습니다.
- SVM에 CIFS 서버가 구성된 경우 UNIX 볼륨 또는 qtree에서 Storage-Level Access Guard 보안이 지원되므로 '-path' 매개 변수에 지정된 볼륨 또는 qtree에 적용된 Storage-Level Access Guard 보안에 대한 정보가 출력에 포함될 수 있습니다.

단계

1. 파일 및 디렉터리 보안 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면...	다음 명령을 입력합니다...
요약 양식	'vserver security file-directory show -vserver vserver_name -path path path'
세부 정보가 확장됩니다	'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true'

예

다음 예제는 SVM VS1 경로 /lab에 대한 보안 정보를 보여 줍니다. 이 UNIX 보안 스타일 경로에는 NFSv4 SACL이 있습니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

ONTAP SMB 파일 보안 및 감사 정책 정보를 표시하는 방법을 알아보세요.

와일드카드 문자(*)를 사용하여 지정된 경로 또는 루트 볼륨 아래에 있는 모든 파일 및 디렉토리의 파일 보안 및 감사 정책에 대한 정보를 표시할 수 있습니다.

와일드카드 문자(*)는 모든 파일 및 디렉터리의 정보를 표시할 아래의 지정된 디렉터리 경로의 마지막 하위 구성 요소로 사용할 수 있습니다. "" * ""로 명명된 특정 파일이나 디렉터리의 정보를 표시하려면 큰따옴표("""") 안에 전체 경로를 제공해야 합니다.

예

와일드카드 문자를 사용하여 다음 명령을 실행하면 SVM VS1 경로의 '/1/' 아래에 있는 모든 파일 및 디렉토리에 대한 정보가 표시됩니다.

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

다음 명령을 실행하면 SVM VS1 의 path '/vol1/a' 아래에 " * "로 명명된 파일의 정보가 표시됩니다. 경로는 큰따옴표(" ")로 묶습니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
         Unix User Id: 1002
        Unix Group Id: 65533
       Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                  ACLs: NFSV4 Security Descriptor
                        Control:0x8014
                        SACL - ACEs
                          AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                        DACL - ACEs
                          ALLOW-EVERYONE@-0x1f00a9-FI|DI
                          ALLOW-OWNER@-0x1f01ff-FI|DI
                          ALLOW-GROUP@-0x1200a9-IG
```

CLI를 사용하여 **SVM**에서 **NTFS** 파일 보안**, NTFS** 감사 정책 및 **Storage-Level Access Guard**를 관리합니다

SMB NTFS 파일 보안**, NTFS** 감사 정책 및 스토리지 수준 액세스 보호 관리를 위한 **ONTAP** 명령

CLI를 사용하여 스토리지 가상 시스템(SVM)에서 NTFS 파일 보안, NTFS 감사 정책 및 스토리지 레벨 액세스 가드를 관리할 수 있습니다.

SMB 클라이언트 또는 CLI를 사용하여 NTFS 파일 보안 및 감사 정책을 관리할 수 있습니다. 그러나 CLI를 사용하여 파일 보안 및 감사 정책을 구성하면 원격 클라이언트를 사용하여 파일 보안을 관리할 필요가 없습니다. CLI를 사용하면 단일 명령을 사용하여 여러 파일과 폴더에 보안을 적용하는 데 걸리는 시간을 크게 줄일 수 있습니다.

ONTAP에서 SVM 볼륨에 적용한 또 다른 보안 계층인 스토리지 레벨 액세스 가드를 구성할 수 있습니다. Storage-Level Access Guard는 모든 NAS 프로토콜에서 Storage-Level Access Guard가 적용되는 스토리지 객체에 대한 액세스에 적용됩니다.

스토리지 레벨 액세스 가드는 ONTAP CLI에서만 구성 및 관리할 수 있습니다. SMB 클라이언트에서 스토리지 수준 액세스 가드 설정을 관리할 수 없습니다. 또한 NFS 또는 SMB 클라이언트의 파일 또는 디렉토리에 대한 보안 설정을 볼 경우 Storage-Level Access Guard 보안이 표시되지 않습니다. 시스템(Windows 또는 UNIX) 관리자도 클라이언트에서 스토리지 수준 액세스 가드 보안을 취소할 수 없습니다. 따라서 Storage-Level Access Guard는 스토리지 관리자가 독립적으로 설정하고 관리하는 데이터 액세스를 위한 추가 보안 계층을 제공합니다.

스토리지 레벨 액세스 가드에 대해 NTFS 액세스 권한만 지원되지만, ONTAP는 UNIX 사용자가 볼륨을 소유하는 SVM에서 Windows 사용자에게 매핑될 경우 스토리지 레벨 액세스 가드가 적용되는 볼륨의 데이터에 대해 NFS에 대한 액세스를 위한 보안 검사를 수행할 수 있습니다.

NTFS 보안 스타일 볼륨

NTFS 보안 스타일 볼륨 및 Qtree에 포함된 모든 파일 및 폴더는 NTFS의 효율적인 보안을 사용합니다. "vserver security file-directory" 명령 제품군을 사용하여 NTFS 보안 스타일 볼륨에 다음 유형의 보안을 구현할 수 있습니다.

- 볼륨에 포함된 파일 및 폴더에 대한 파일 권한 및 감사 정책
- 볼륨에 대한 스토리지 레벨 액세스 가드 보안

혼합 보안 형식 볼륨

혼합 보안 스타일 볼륨 및 qtree에는 UNIX의 효과적인 보안이 있는 일부 파일과 폴더가 포함될 수 있으며, 모드 비트 또는 NFSv4.x ACL 및 NFSv4.x 감사 정책, NTFS 효과적인 보안이 설정된 일부 파일 및 폴더, NTFS 파일 권한 및 감사 정책을 사용하는 일부 파일 및 폴더가 포함될 수 있습니다. 'vserver security file-directory' 명령 제품군을 사용하여 혼합 보안 스타일 데이터에 다음 유형의 보안을 적용할 수 있습니다.

- 혼합 볼륨 또는 qtree에서 NTFS 유효 보안 유형을 사용하는 파일 및 폴더에 대한 파일 권한 및 감사 정책
- 스토리지 레벨 액세스 NTFS 및 UNIX의 효율적인 보안 방식으로 볼륨에 대한 보호

Unix 보안 스타일 볼륨

UNIX 보안 스타일 볼륨 및 qtree에는 UNIX 유효 보안(모드 비트 또는 NFSv4.x ACL)이 있는 파일 및 폴더가 포함되어 있습니다. UNIX 보안 스타일 볼륨에 보안을 구현하기 위해 'vserver security file-directory' 명령 제품군을 사용하려면 다음 사항을 염두에 두어야 합니다.

- "vserver security file-directory" 명령 제품군은 UNIX 보안 스타일 볼륨 및 qtree에서 UNIX 파일 보안 및 감사 정책을 관리하는 데 사용할 수 없습니다.
- SVM과 타겟 볼륨에 CIFS 서버가 포함된 경우 "vserver security file-directory" 명령 제품군을 사용하여 UNIX 보안 스타일 볼륨에서 Storage-Level Access Guard를 구성할 수 있습니다.

관련 정보

- 파일 보안 및 감사 정책 보기에 대해 알아보세요
- 서버에 NTFS 보안 설명자 만들기
- 파일 및 폴더에 감사 정책을 구성하고 적용하는 명령
- Storage-Level Access Guard를 사용하여 안전한 파일 액세스에 대해 알아보세요

SMB 파일 및 폴더 보안을 설정하기 위한 ONTAP 명령

원격 클라이언트의 개입 없이 로컬로 파일 및 폴더 보안을 적용 및 관리할 수 있으므로 많은 수의 파일 또는 폴더에 대해 대량 보안을 설정하는 데 걸리는 시간을 크게 줄일 수 있습니다.

CLI를 사용하여 다음과 같은 사용 사례에서 파일 및 폴더 보안을 설정할 수 있습니다.

- 홈 디렉토리의 파일 스토리지와 같은 대규모 엔터프라이즈 환경에 있는 파일의 스토리지
- 데이터 마이그레이션
- Windows 도메인 변경
- NTFS 파일 시스템 전반에 걸쳐 파일 보안 및 감사 정책 표준화

ONTAP 명령을 사용하여 **SMB** 파일 및 폴더 보안을 설정할 때의 제한 사항에 대해 알아보세요**.**

CLI를 사용하여 파일 및 폴더 보안을 설정할 때 특정 제한 사항을 알고 있어야 합니다.

- 'vserver security file-directory' 명령 제품군은 NFSv4 ACL 설정을 지원하지 않습니다.

  NTFS 보안 설명자는 NTFS 파일 및 폴더에만 적용할 수 있습니다.

보안 설명자를 사용하여 **ONTAP SMB** 파일 및 폴더 보안을 적용합니다**.**

보안 설명자는 사용자가 파일 및 폴더에 대해 수행할 수 있는 작업과 사용자가 파일 및 폴더에 액세스할 때 감사할 작업을 결정하는 액세스 제어 목록을 포함합니다.

- * 권한 *

  권한은 개체의 소유자가 허용하거나 거부하고 개체(사용자, 그룹 또는 컴퓨터 개체)가 지정된 파일이나 폴더에서 수행할 수 있는 작업을 결정합니다.

- * 보안 설명자 *

  보안 설명자는 파일 또는 폴더와 관련된 권한을 정의하는 보안 정보가 포함된 데이터 구조입니다.

- * ACL(액세스 제어 목록) *

  액세스 제어 목록은 보안 설명자가 적용된 파일 또는 폴더에서 사용자, 그룹 또는 컴퓨터 개체가 수행할 수 있는 작업에 대한 정보를 포함하는 보안 설명자에 포함된 목록입니다. 보안 설명자는 다음 두 가지 유형의 ACL을 포함할 수 있습니다.

  ◦ DACL(임의 액세스 제어 목록)

  ◦ 시스템 액세스 제어 목록(SACL)

- * DACL(임의 액세스 제어 목록) *

  DACL에는 파일 또는 폴더에 대한 작업을 수행할 수 있는 액세스가 허용 또는 거부된 사용자, 그룹 및 컴퓨터 개체에 대한 SIDS 목록이 포함되어 있습니다. DACL에는 ACE(액세스 제어 항목)가 0개 이상 포함되어 있습니다.

- * 시스템 액세스 제어 목록(SACL) *

  SACL에는 성공 또는 실패 감사 이벤트가 기록되는 사용자, 그룹 및 컴퓨터 개체에 대한 SIDS 목록이 포함되어 있습니다. SACL에는 ACE(액세스 제어 항목)가 0개 이상 포함되어 있습니다.

- * ACE(액세스 제어 항목) *

  ACE는 DACL 또는 SACL의 개별 항목입니다.

  ◦ DACL 액세스 제어 항목은 특정 사용자, 그룹 또는 컴퓨터 개체에 대해 허용 또는 거부된 액세스 권한을 지정합니다.

  ◦ SACL 액세스 제어 항목은 특정 사용자, 그룹 또는 컴퓨터 개체에서 수행하는 지정된 작업을 감사할 때 기록할 성공 또는 실패 이벤트를 지정합니다.

- * 사용 권한 상속 *

권한 상속에서는 보안 설명자에 정의된 권한이 부모 개체에서 개체로 전파되는 방법을 설명합니다. 상속 가능한 권한만 자식 개체에서 상속합니다. 상위 객체에 대한 권한을 설정할 때 폴더, 하위 폴더, 파일이 이 폴더에 적용, 하위 폴더, 파일 등을 통해 해당 항목을 상속할 수 있는지 여부를 결정할 수 있습니다.

관련 정보

- "SMB 및 NFS 감사 및 보안 추적"
- 파일 및 폴더에 감사 정책을 구성하고 적용하는 명령

ONTAP SVM 재해 복구 대상에서 로컬 **SMB** 사용자 또는 그룹을 사용하는 파일 디렉토리 정책을 적용하는 방법에 대해 알아보세요**.**

파일 디렉토리 정책 구성에서 보안 설명자나 DACL 또는 SACL 항목의 로컬 사용자 또는 그룹을 사용하는 경우 ID 폐기 구성의 SVM(Storage Virtual Machine) 재해 복구 대상에 파일 디렉토리 정책을 적용하기 전에 염두에 두어야 할 몇 가지 지침이 있습니다.

소스 클러스터의 소스 SVM이 소스 SVM에서 데이터 및 구성을 소스 SVM에서 타겟 클러스터의 대상 SVM으로 복제하는 SVM을 위한 재해 복구 구성을 구성할 수 있습니다.

SVM 재해 복구의 두 가지 유형 중 하나를 설정할 수 있습니다.

- ID가 보존됩니다

  이 구성에서는 SVM과 CIFS 서버의 ID가 보존됩니다.

- ID가 삭제되었습니다

  이 구성에서는 SVM과 CIFS 서버의 ID가 유지되지 않습니다. 이 시나리오에서는 대상 SVM의 SVM 및 CIFS 서버의 이름이 소스 SVM의 SVM 및 CIFS 서버 이름과 다릅니다.

ID 폐기 구성에 대한 지침

로컬 사용자, 그룹 및 권한 구성이 포함된 SVM 소스의 경우 ID가 폐기된 구성에서 SVM 대상의 CIFS 서버 이름과 일치하도록 로컬 도메인(로컬 CIFS 서버 이름)의 이름을 변경해야 합니다. 예를 들어, 소스 SVM 이름이 ""VS1""이고 CIFS 서버 이름이 ""CIFS1""이고 대상 SVM 이름이 ""VS1_DST""이고 CIFS 서버 이름이 ""CIFS1_DST""인 경우 로컬 사용자 ""CIFS1\user1""의 로컬 도메인 이름이 ""FS1""""로 자동 변경됩니다.

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

로컬 사용자 및 그룹 데이터베이스에서 로컬 사용자 및 그룹 이름이 자동으로 변경되더라도 파일 디렉토리 정책 구성('vserver security file-directory' 명령 제품군을 사용하여 CLI에 구성된 정책)에서 로컬 사용자 또는 그룹 이름이 자동으로 변경되지 않습니다.

예를 들어, ""vs1""의 경우 "-account" 매개 변수가 ""CIFS1\user1""로 설정된 DACL 항목을 구성한 경우 대상의 CIFS 서버 이름을 반영하도록 대상 SVM에서 설정이 자동으로 변경되지 않습니다.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

CIFS 서버 이름을 대상 CIFS 서버 이름으로 수동으로 변경하려면 'vserver security file-directory modify' 명령을 사용해야 합니다.

계정 매개 변수가 포함된 파일 디렉토리 정책 구성 구성 요소입니다

로컬 사용자 또는 그룹을 포함할 수 있는 매개 변수 설정을 사용할 수 있는 세 가지 파일 디렉토리 정책 구성 구성 요소가 있습니다.

- 보안 설명자

  필요에 따라 보안 설명자의 소유자와 보안 설명자의 소유자의 기본 그룹을 지정할 수 있습니다. 보안 설명자가 소유자 및 기본 그룹 항목에 대해 로컬 사용자 또는 그룹을 사용하는 경우, 계정 이름에 대상 SVM을 사용하도록 보안 설명자를 수정해야 합니다. 'vserver security file-directory NTFS modify' 명령을 사용하여 계정 이름을 필요에 따라 변경할 수 있습니다.

- DACL 항목

  각 DACL 항목은 계정과 연결되어 있어야 합니다. 대상 SVM 이름을 사용하려면 로컬 사용자 또는 그룹 계정을 사용하는 모든 DACL을 수정해야 합니다. 기존 DACL 항목에 대한 계정 이름을 수정할 수 없으므로 보안 설명자에서 로컬 사용자 또는 그룹의 DACL 항목을 제거하고 수정된 대상 계정 이름으로 새 DACL 항목을 만든 다음 이러한 새 DACL 항목을 적절한 보안 설명자와 연결해야 합니다.

- SACL 항목

  각 SACL 항목은 계정과 연결되어 있어야 합니다. 대상 SVM 이름을 사용하려면 로컬 사용자 또는 그룹 계정을 사용하는 SACL을 수정해야 합니다. 기존 SACL 항목에 대한 계정 이름을 수정할 수 없으므로 보안 설명자에서 로컬 사용자 또는 그룹을 가진 SACL 항목을 제거하고 수정된 대상 계정 이름으로 새 SACL 항목을 만든 다음 이러한 새 SACL 항목을 적절한 보안 설명자와 연결해야 합니다.

정책을 적용하기 전에 파일 디렉토리 정책 구성에 사용되는 로컬 사용자 또는 그룹을 변경해야 합니다. 그렇지 않으면 적용 작업이 실패합니다.

CLI를 사용하여 **NTFS** 파일 및 폴더에 파일 보안을 구성하고 적용합니다

ONTAP SMB 서버에서 **NTFS** 보안 설명자 생성

NTFS 보안 설명자(파일 보안 정책)를 생성하는 것은 NTFS ACL(액세스 제어 목록)을 구성하여 SVM(스토리지 가상 머신) 내에 있는 파일 및 폴더에 적용하는 첫 번째 단계입니다. 보안 설명자를 정책 작업의 파일 또는 폴더 경로에 연결할 수 있습니다.

이 작업에 대해

NTFS 보안 스타일 볼륨 내에 있는 파일 및 폴더 또는 혼합 보안 스타일 볼륨에 상주하는 파일 및 폴더에 대한 NTFS 보안 설명자를 만들 수 있습니다.

기본적으로 보안 설명자가 만들어지면 네 개의 DACL(임의 액세스 제어 목록) ACE(액세스 제어 항목)가 해당 보안 설명자에 추가됩니다. 네 가지 기본 ACE는 다음과 같습니다.

오브젝트	액세스 유형입니다	액세스 권한	사용 권한을 적용할 위치입니다
BUILTIN\Administrators입니다	허용	모든 권한	폴더, 하위 폴더, 파일
BUILTIN\사용자	허용	모든 권한	폴더, 하위 폴더, 파일
작성자 소유자	허용	모든 권한	폴더, 하위 폴더, 파일
NT AUTHORITY\SYSTEM	허용	모든 권한	폴더, 하위 폴더, 파일

다음 선택적 매개 변수를 사용하여 보안 설명자 구성을 사용자 지정할 수 있습니다.

- 보안 설명자의 소유자입니다
- 소유자의 기본 그룹입니다
- 원시 제어 플래그

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 자세한 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

ONTAP SMB 서버의 **NTFS** 보안 설명자에 **NTFS DACL** 액세스 제어 항목 추가

NTFS 보안 설명자에 DACL(임의 액세스 제어 목록) ACE(액세스 제어 항목)를 추가하는 것은 파일이나 폴더에 NTFS ACL을 구성하고 적용하는 두 번째 단계입니다. 각 항목은 액세스가 허용되거나 거부된 개체를 식별하고 ACE에 정의된 파일 또는 폴더에 대해 개체가 수행할 수 있거나 수행할 수 없는 작업을 정의합니다.

이 작업에 대해

보안 설명자의 DACL에 하나 이상의 ACE를 추가할 수 있습니다.

보안 설명자에 기존 ACE가 있는 DACL이 포함된 경우 명령은 새 ACE를 DACL에 추가합니다. 보안 설명자에 DACL이 포함되어 있지 않으면 명령에서 DACL을 생성하고 새 ACE를 추가합니다.

'-account' 매개 변수에 지정된 계정에 대해 허용 또는 거부할 권한을 지정하여 DACL 항목을 선택적으로 사용자 지정할 수 있습니다. 권한을 지정할 수 있는 세 가지 상호 배타적인 방법이 있습니다.

- 권한
- 고급 권한
- 원시 권한(고급 권한)

DACL 항목에 대한 권한을 지정하지 않으면 기본값은 "모든 권한"으로 설정됩니다.

선택적으로 상속 적용 방법을 지정하여 DACL 항목을 사용자 지정할 수 있습니다.

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 이 절차에서 설명하는 명령에 대한 자세한

내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

단계

1. 보안 설명자에 DACL 항목을 추가합니다. 'vserver security file -directory NTFS DACL add -vserver vserver_name -ntfs -sd sd sd_name -access -type {allow | deny} -account name_or_SIDoptional_parameters'

   'vserver security file-directory NTFS DACL add-NTFS-SD SD1-access-type deny-account domain\joe-rights full-control-apply-to this-folder-vserver-vs1'

2. DACL 항목이 올바른지 확인합니다. 'vserver security file-directory NTFS DACL show -vserver vserver_name -ntfs -sd sd sd_name -access-type{allow|deny} -account name_or_SID'

   'vserver security file-directory NTFS DACL show -vserver vs1-ntfs-sd SD1-access-type deny-account domain\joe'

```
                Vserver: vs1
Security Descriptor Name: sd1
             Allow or Deny: deny
      Account Name or SID: DOMAIN\joe
             Access Rights: full-control
  Advanced Access Rights: -
                  Apply To: this-folder
             Access Rights: full-control
```

에 대한 자세한 내용은 `vserver security file-directory ntfs dacl` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SMB 보안 정책 생성

SVM에 대한 파일 보안 정책을 생성하는 것은 파일이나 폴더에 ACL을 구성 및 적용하는 세 번째 단계입니다. 정책은 다양한 작업을 위한 컨테이너 역할을 하며, 여기서 각 작업은 파일이나 폴더에 적용할 수 있는 단일 항목입니다. 나중에 보안 정책에 작업을 추가할 수 있습니다.

이 작업에 대해

보안 정책에 추가하는 작업에는 NTFS 보안 설명자와 파일 또는 폴더 경로 간의 연결이 포함됩니다. 따라서 보안 정책을 각 SVM(NTFS 보안 스타일 볼륨 또는 혼합 보안 스타일 볼륨 포함)과 연결해야 합니다.

단계

1. 'vserver security file-directory policy create-vserver vserver_name-policy-name policy_name' 보안 정책을 생성합니다

   'vserver security file-directory policy create-policy-name policy1-vserver vs1'

2. 보안 정책 'vserver security file-directory policy show'를 확인합니다

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

ONTAP SMB 보안 정책에 작업 추가

보안 정책에 정책 작업을 생성하고 추가하는 것은 SVM의 파일 또는 폴더에 ACL을 구성 및 적용하는 네 번째 단계입니다. 정책 작업을 생성할 때 작업을 보안 정책에 연결합니다. 하나 이상의 작업 항목을 보안 정책에 추가할 수 있습니다.

이 작업에 대해

보안 정책은 작업의 컨테이너입니다. 작업은 보안 정책이 NTFS 또는 혼합 보안이 있는 파일 또는 폴더(또는 Storage-Level Access Guard를 구성하는 경우 볼륨 개체)에 대해 수행할 수 있는 단일 작업을 말합니다.

다음과 같은 두 가지 유형의 작업이 있습니다.

- 파일 및 디렉터리 작업

  지정된 파일 및 폴더에 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 파일 및 디렉토리 작업을 통해 적용된 ACL은 SMB 클라이언트 또는 ONTAP CLI를 통해 관리할 수 있습니다.

- 스토리지 레벨 액세스 가드 작업

  지정된 볼륨에 Storage-Level Access Guard 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 스토리지 레벨 액세스 가드 작업을 통해 적용된 ACL은 ONTAP CLI를 통해서만 관리할 수 있습니다.

작업에는 파일(또는 폴더) 또는 파일 집합(또는 폴더)의 보안 구성에 대한 정의가 포함됩니다. 정책의 모든 작업은 경로로 고유하게 식별됩니다. 단일 정책 내에서 경로당 하나의 작업만 있을 수 있습니다. 정책에 중복된 작업 항목이 있을 수 없습니다.

정책에 작업 추가 지침:

- 정책당 최대 10,000개의 작업 항목이 있을 수 있습니다.
- 정책에는 하나 이상의 작업이 포함될 수 있습니다.

  정책에 둘 이상의 작업이 포함될 수 있지만 파일 디렉터리 및 저장소 수준 액세스 가드 작업을 모두 포함하도록 정책을 구성할 수는 없습니다. 정책에는 모든 스토리지 레벨 액세스 가드 작업 또는 모든 파일 디렉토리 작업이 포함되어야 합니다.

- Storage-Level Access Guard는 사용 권한을 제한하는 데 사용됩니다.

  추가 액세스 권한은 제공하지 않습니다.

보안 정책에 작업을 추가할 때 다음 네 가지 필수 매개 변수를 지정해야 합니다.

- SVM 이름

- 정책 이름입니다
- 경로
- 경로와 연결할 보안 설명자입니다

다음 선택적 매개 변수를 사용하여 보안 설명자 구성을 사용자 지정할 수 있습니다.

- 보안 유형입니다
- 전파 모드
- 인덱스 위치
- 액세스 제어 유형입니다

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

단계

1. 보안 정책에 관련 보안 설명자가 포함된 작업을 추가합니다. 'vserver 보안 파일 - 디렉토리 정책 작업 추가 - vserver vserver_name -policy -name policy_name -path path -NTFS-SD_nameoptional_parameters'

   파일 디렉토리는 '-access-control' 파라미터의 기본값입니다. 파일 및 디렉터리 액세스 작업을 구성할 때 액세스 제어 유형을 지정하는 것은 선택 사항입니다.

   'vserver security file-directory policy task add-vserver vs1-policy-name policy1-path/home/dir1-security-type NTFS-NTFS-MODE propagate-NTFS-SD SD2-index-num 1-access-control file-directory'를 선택합니다

2. 정책 작업 구성을 확인합니다. 'vserver security file-directory policy task show -vserver vserver_name -policy -name policy_name -path path path'

   'vserver security file-directory policy task show'를 선택합니다

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

에 대한 자세한 내용은 `vserver security file-directory policy task` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SMB 보안 정책 적용

파일 또는 폴더에 NTFS ACL을 생성하고 적용하는 마지막 단계는 SVM에 파일 보안 정책을

적용하는 것입니다.

이 작업에 대해

보안 정책에 정의된 보안 설정을 FlexVol 볼륨(NTFS 또는 혼합 보안 스타일) 내에 있는 NTFS 파일 및 폴더에 적용할 수 있습니다.

> 감사 정책 및 관련 SACL이 적용되면 기존의 모든 DACL을 덮어씁니다. 보안 정책과 관련 DACL을 적용하면 기존 DACL을 덮어씁니다. 새 보안 정책을 만들고 적용하기 전에 기존 보안 정책을 검토해야 합니다.

단계

1. 보안 정책('vserver security file-directory apply-vserver vserver_name -policy -name policy_name')을 적용합니다

   'vserver security file-directory apply-vserver vs1-policy-name policy1'

   정책 적용 작업이 예약되고 작업 ID가 반환됩니다.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

ONTAP SMB 보안 정책 작업 모니터링

보안 정책을 SVM(스토리지 가상 머신)에 적용할 때 보안 정책 작업을 모니터링하여 작업 진행률을 모니터링할 수 있습니다. 이 기능은 보안 정책의 응용 프로그램이 성공했는지 확인하려는 경우에 유용합니다. 이 기능은 많은 수의 파일과 폴더에 대량 보안을 적용하는 장기 실행 작업이 있는 경우에도 유용합니다.

이 작업에 대해

보안 정책 작업에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 사용해야 합니다.

단계

1. 보안 정책 작업 'vserver security file-directory job show -vserver vserver_name'을 모니터링합니다

   'vserver security file-directory job show -vserver vs1'

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

ONTAP SMB 파일 보안 확인

파일 보안 설정을 확인하여 보안 정책을 적용한 SVM(스토리지 가상 머신)의 파일 또는 폴더에 원하는 설정이 있는지 확인할 수 있습니다.

이 작업에 대해

보안 설정을 확인할 파일과 폴더의 경로와 데이터가 포함된 SVM의 이름을 제공해야 합니다. 옵션 '-Expand-mask' 매개 변수를 사용하여 보안 설정에 대한 자세한 정보를 표시할 수 있습니다.

단계

1. 파일 및 폴더 보안 설정 표시: 'vserver security file-directory show -vserver vserver_name -path path path[-expand-mask true]'

   'vserver security file-directory show -vserver vs1-path/data/engineering-expand-mask true'

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
```

```
                            .... .... .... ...0 = Owner Defaulted

                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          DACL - ACEs
                            ALLOW-Everyone-0x1f01ff
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
```

```
                            0... .... .... .... .... .... .... .... =
Generic Read
                            .0.. .... .... .... .... .... .... .... =
Generic Write
                            ..0. .... .... .... .... .... .... .... =
Generic Execute
                            ...1 .... .... .... .... .... .... .... =
Generic All
                            .... ...0 .... .... .... .... .... .... =
System Security
                            .... .... ...0 .... .... .... .... .... =
Synchronize
                            .... .... .... 0... .... .... .... .... =
Write Owner
                            .... .... .... .0.. .... .... .... .... =
Write DAC
                            .... .... .... ..0. .... .... .... .... =
Read Control
                            .... .... .... ...0 .... .... .... .... =
Delete
                            .... .... .... .... .... ...0 .... .... =
Write Attributes
                            .... .... .... .... .... .... 0... .... =
Read Attributes
                            .... .... .... .... .... .... .0.. .... =
Delete Child
                            .... .... .... .... .... .... ..0. .... =
Execute
                            .... .... .... .... .... .... ...0 .... =
Write EA
                            .... .... .... .... .... .... .... 0... =
Read EA
                            .... .... .... .... .... .... .... .0.. =
Append
                            .... .... .... .... .... .... .... ..0. =
Write
                            .... .... .... .... .... .... .... ...0 =
Read
```

CLI를 사용하여 **NTFS** 파일 및 폴더에 감사 정책을 구성하고 적용합니다

NTFS 파일 및 폴더에 **SMB** 감사 정책을 구성하고 적용하기 위한 **ONTAP** 명령

ONTAP CLI를 사용할 때 NTFS 파일 및 폴더에 감사 정책을 적용하려면 몇 가지 단계를 수행해야 합니다. 먼저 NTFS 보안 설명자를 만들고 보안 설명자에 SACL을 추가합니다. 그런

다음 보안 정책을 만들고 정책 작업을 추가합니다. 그런 다음 SVM(스토리지 가상 시스템)에 보안 정책을 적용합니다.

이 작업에 대해

보안 정책을 적용한 후 보안 정책 작업을 모니터링하고 적용된 감사 정책의 설정을 확인할 수 있습니다.

> 감사 정책 및 관련 SACL이 적용되면 기존의 모든 DACL을 덮어씁니다. 새 보안 정책을 만들고 적용하기 전에 기존 보안 정책을 검토해야 합니다.

관련 정보

- Storage-Level Access Guard를 사용하여 안전한 파일 액세스에 대해 알아보세요
- SMB 파일 및 폴더 보안을 설정하기 위해 명령을 사용할 때의 제한 사항에 대해 알아보세요.
- 보안 설명자를 사용하여 파일 및 폴더 보안을 적용합니다.
- "SMB 및 NFS 감사 및 보안 추적"
- 서버에 NTFS 보안 설명자 만들기

ONTAP SMB 서버에서 **NTFS** 보안 설명자 생성

NTFS 보안 설명자 감사 정책을 생성하는 것은 SVM에 상주하는 파일 및 폴더에 NTFS ACL(액세스 제어 목록)을 구성 및 적용하는 첫 번째 단계입니다. 보안 설명자를 정책 작업의 파일 또는 폴더 경로에 연결합니다.

이 작업에 대해

NTFS 보안 스타일 볼륨 내에 있는 파일 및 폴더 또는 혼합 보안 스타일 볼륨에 상주하는 파일 및 폴더에 대한 NTFS 보안 설명자를 만들 수 있습니다.

기본적으로 보안 설명자가 만들어지면 네 개의 DACL(임의 액세스 제어 목록) ACE(액세스 제어 항목)가 해당 보안 설명자에 추가됩니다. 네 가지 기본 ACE는 다음과 같습니다.

오브젝트	액세스 유형입니다	액세스 권한	사용 권한을 적용할 위치입니다
BUILTIN\Administrators입니다	허용	모든 권한	폴더, 하위 폴더, 파일
BUILTIN\사용자	허용	모든 권한	폴더, 하위 폴더, 파일
작성자 소유자	허용	모든 권한	폴더, 하위 폴더, 파일
NT AUTHORITY\SYSTEM	허용	모든 권한	폴더, 하위 폴더, 파일

다음 선택적 매개 변수를 사용하여 보안 설명자 구성을 사용자 지정할 수 있습니다.

- 보안 설명자의 소유자입니다
- 소유자의 기본 그룹입니다

- 원시 제어 플래그

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

단계

1. 고급 매개 변수를 사용하려면 권한 수준을 고급:'Set-Privilege Advanced'로 설정합니다
2. 보안 설명자:'vserver security file-directory NTFS create-vserver vserver_name-NTFS-SD sd_nameoptional_parameters'를 생성합니다

   'vserver security file-directory NTFS create-NTFS-SD SD1-vserver vs1-owner domain\joe'

3. 보안 설명자 구성이 올바른지 확인합니다. 'vserver security file-directory NTFS show -vserver vserver_name -NTFS-SD sd_name'

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                  Security Descriptor Name: sd1
            Owner of the Security Descriptor: DOMAIN\joe
   ```

4. 고급 권한 수준인 경우 'Set-Privilege admin'으로 돌아갑니다

ONTAP SMB 서버의 **NTFS** 보안 설명자에 **NTFS SACL** 액세스 제어 항목 추가

SACL(시스템 액세스 제어 목록) ACE(액세스 제어 항목)를 NTFS 보안 설명자에 추가하는 것은 SVM의 파일 또는 폴더에 대한 NTFS 감사 정책을 생성하는 두 번째 단계입니다. 각 항목은 감사하려는 사용자 또는 그룹을 식별합니다. SACL 항목은 성공한 액세스 시도 또는 실패한 액세스 시도를 감사할지 여부를 정의합니다.

이 작업에 대해

보안 설명자의 SACL에 하나 이상의 ACE를 추가할 수 있습니다.

보안 설명자에 기존 ACE가 있는 SACL이 포함된 경우 이 명령은 새 ACE를 SACL에 추가합니다. 보안 설명자에 SACL이 포함되어 있지 않으면 명령에서 SACL을 만들고 새 ACE를 추가합니다.

'-account' 매개 변수에 지정된 계정의 성공 또는 실패 이벤트에 대해 감사할 권한을 지정하여 SACL 항목을 구성할 수 있습니다. 권한을 지정할 수 있는 세 가지 상호 배타적인 방법이 있습니다.

- 권한
- 고급 권한
- 원시 권한(고급 권한)

SACL 항목에 대한 권한을 지정하지 않으면 기본 설정은 "모든 권한"입니다.

"apply to" 매개 변수를 사용하여 상속을 적용하는 방법을 지정하여 SACL 항목을 선택적으로 사용자 지정할 수 있습니다. 이 매개 변수를 지정하지 않으면 기본적으로 이 SACL 항목을 이 폴더, 하위 폴더 및 파일에 적용합니다.

단계

1. 보안 설명자에 SACL 항목을 추가합니다. 'vserver security file-directory NTFS SACL add -vserver vserver_name -ntfs -sd sd sd_name -access -type {failure | success} -account name_or_SIDoptional_parameters'

   'vserver security file-directory NTFS SACL add-NTFS-SD SD1-access-type failure-account domain\joe-rights full-control-apply-to this-folder-vserver-vs1'

2. SACL 항목이 올바른지 확인합니다. 'vserver security file-directory NTFS SACL show -vserver vserver_name -ntfs -sd sd sd_name -access -type {failure | success} -account name_or_SID'

   'vserver security file-directory NTFS SACL show -vserver vs1-NTFS-SD SD1-access-type deny-account domain\joe'

```
                                Vserver: vs1
                  Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
                      Account Name or SID: DOMAIN\joe
                             Access Rights: full-control
                   Advanced Access Rights: -
                                 Apply To: this-folder
                             Access Rights: full-control
```

ONTAP SMB 보안 정책 생성

SVM(스토리지 가상 머신)에 대한 감사 정책을 생성하는 것은 ACL을 구성하여 파일 또는 폴더에 적용하는 세 번째 단계입니다. 정책은 다양한 작업을 위한 컨테이너 역할을 하며, 여기서 각 작업은 파일이나 폴더에 적용할 수 있는 단일 항목입니다. 나중에 보안 정책에 작업을 추가할 수 있습니다.

이 작업에 대해

보안 정책에 추가하는 작업에는 NTFS 보안 설명자와 파일 또는 폴더 경로 간의 연결이 포함됩니다. 따라서 보안 정책을 각 SVM(스토리지 가상 머신)(NTFS 보안 스타일 볼륨 또는 혼합 보안 스타일 볼륨 포함)과 연결해야 합니다.

단계

1. 'vserver security file-directory policy create-vserver vserver_name-policy-name policy_name' 보안 정책을 생성합니다

   'vserver security file-directory policy create-policy-name policy1-vserver vs1'

2. 보안 정책 'vserver security file-directory policy show'를 확인합니다

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

ONTAP SMB 보안 정책에 작업 추가

보안 정책에 정책 작업을 생성하고 추가하는 것은 SVM의 파일 또는 폴더에 ACL을 구성 및 적용하는 네 번째 단계입니다. 정책 작업을 생성할 때 작업을 보안 정책에 연결합니다. 하나 이상의 작업 항목을 보안 정책에 추가할 수 있습니다.

이 작업에 대해

보안 정책은 작업의 컨테이너입니다. 작업은 보안 정책이 NTFS 또는 혼합 보안이 있는 파일 또는 폴더(또는 Storage-Level Access Guard를 구성하는 경우 볼륨 개체)에 대해 수행할 수 있는 단일 작업을 말합니다.

다음과 같은 두 가지 유형의 작업이 있습니다.

- 파일 및 디렉터리 작업

  지정된 파일 및 폴더에 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 파일 및 디렉토리 작업을 통해 적용된 ACL은 SMB 클라이언트 또는 ONTAP CLI를 통해 관리할 수 있습니다.

- 스토리지 레벨 액세스 가드 작업

  지정된 볼륨에 Storage-Level Access Guard 보안 설명자를 적용하는 작업을 지정하는 데 사용됩니다. 스토리지 레벨 액세스 가드 작업을 통해 적용된 ACL은 ONTAP CLI를 통해서만 관리할 수 있습니다.

작업에는 파일(또는 폴더) 또는 파일 집합(또는 폴더)의 보안 구성에 대한 정의가 포함됩니다. 정책의 모든 작업은 경로로 고유하게 식별됩니다. 단일 정책 내에서 경로당 하나의 작업만 있을 수 있습니다. 정책에 중복된 작업 항목이 있을 수 없습니다.

정책에 작업 추가 지침:

- 정책당 최대 10,000개의 작업 항목이 있을 수 있습니다.
- 정책에는 하나 이상의 작업이 포함될 수 있습니다.

  정책에 둘 이상의 작업이 포함될 수 있지만 파일 디렉터리 및 저장소 수준 액세스 가드 작업을 모두 포함하도록 정책을 구성할 수는 없습니다. 정책에는 모든 스토리지 레벨 액세스 가드 작업 또는 모든 파일 디렉토리 작업이 포함되어야 합니다.

- Storage-Level Access Guard는 사용 권한을 제한하는 데 사용됩니다.

  추가 액세스 권한은 제공하지 않습니다.

다음 선택적 매개 변수를 사용하여 보안 설명자 구성을 사용자 지정할 수 있습니다.

- 보안 유형입니다

- 전파 모드
- 인덱스 위치
- 액세스 제어 유형입니다

선택적 매개 변수의 값은 Storage-Level Access Guard에서 무시됩니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

단계

1. 보안 정책에 관련 보안 설명자가 포함된 작업을 추가합니다. 'vserver 보안 파일 - 디렉토리 정책 작업 추가 - vserver vserver_name -policy -name policy_name -path path -NTFS-SD_nameoptional_parameters'

   파일 디렉토리는 '-access-control' 파라미터의 기본값입니다. 파일 및 디렉터리 액세스 작업을 구성할 때 액세스 제어 유형을 지정하는 것은 선택 사항입니다.

   'vserver security file-directory policy task add-vserver vs1-policy-name policy1-path/home/dir1-security-type NTFS-NTFS-MODE propagate-NTFS-SD SD2-index-num 1-access-control file-directory'를 선택합니다

2. 정책 작업 구성을 확인합니다. 'vserver security file-directory policy task show -vserver vserver_name -policy -name policy_name -path path path'

   'vserver security file-directory policy task show'를 선택합니다

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS        NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate   sd2
```

에 대한 자세한 내용은 `vserver security file-directory policy task` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SMB 보안 정책 적용

파일 또는 폴더에 NTFS ACL을 생성하고 적용하는 마지막 단계는 SVM에 감사 정책을 적용하는 것입니다.

이 작업에 대해

보안 정책에 정의된 보안 설정을 FlexVol 볼륨(NTFS 또는 혼합 보안 스타일) 내에 있는 NTFS 파일 및 폴더에 적용할 수 있습니다.

감사 정책 및 관련 SACL이 적용되면 기존의 모든 DACL을 덮어씁니다. 보안 정책과 관련 DACL을 적용하면 기존 DACL을 덮어씁니다. 새 보안 정책을 만들고 적용하기 전에 기존 보안 정책을 검토해야 합니다.

단계

1. 'vserver security file-directory apply-vserver vserver_name-policy-name policy_name' 보안 정책을 적용합니다

   'vserver security file-directory apply-vserver vs1-policy-name policy1'

   정책 적용 작업이 예약되고 작업 ID가 반환됩니다.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

ONTAP SMB 보안 정책 작업 모니터링

보안 정책을 SVM(스토리지 가상 머신)에 적용할 때 보안 정책 작업을 모니터링하여 작업 진행률을 모니터링할 수 있습니다. 이 기능은 보안 정책의 응용 프로그램이 성공했는지 확인하려는 경우에 유용합니다. 이 기능은 많은 수의 파일과 폴더에 대량 보안을 적용하는 장기 실행 작업이 있는 경우에도 유용합니다.

이 작업에 대해

보안 정책 작업에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 사용해야 합니다.

단계

1. 보안 정책 작업 'vserver security file-directory job show -vserver vserver_name'을 모니터링합니다

   'vserver security file-directory job show -vserver vs1'

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

ONTAP SMB 감사 정책 확인

감사 정책을 확인하여 보안 정책을 적용한 SVM(스토리지 가상 시스템)의 파일 또는 폴더에 원하는 감사 보안 설정이 있는지 확인할 수 있습니다.

이 작업에 대해

'vserver security file-directory show' 명령을 사용하여 감사 정책 정보를 표시합니다. 표시할 파일 또는 폴더 감사 정책 정보를 가진 데이터의 경로와 데이터가 들어 있는 SVM의 이름을 제공해야 합니다.

단계

1. 감사 정책 설정 표시: 'vserver security file-directory show -vserver_vserver_name_-path_path_'

예

다음 명령을 실행하면 SVM VS1 경로의 ""/Corp" 경로에 적용된 감사 정책 정보가 표시됩니다. 경로에 성공 및 성공/실패 SACL 항목이 모두 적용됩니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
      Security Style: ntfs
     Effective Style: ntfs
      DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
       Unix Group Id: 0
      Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                ACLs: NTFS Security Descriptor
                      Control:0x8014
                      Owner:DOMAIN\Administrator
                      Group:BUILTIN\Administrators
                      SACL - ACEs
                        ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                        SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                      DACL - ACEs
                        ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                        ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                        ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

ONTAP SMB 보안 정책 작업 관리에 대해 알아보세요

특정 상황에서 보안 정책 작업이 있는 경우 해당 보안 정책 또는 해당 정책에 할당된 작업을 수정할 수 없습니다. 정책을 수정할 수 있는 조건이나 수정할 수 없는 조건을 이해해야 정책을 수정할 수 있습니다. 정책 수정에는 정책에 할당된 작업을 추가, 제거 또는 수정하고 정책을 삭제 또는 수정하는 작업이 포함됩니다.

해당 정책에 대한 작업이 있고 해당 작업이 다음 상태인 경우 해당 정책에 할당된 보안 정책 또는 작업을 수정할 수 없습니다.

- 작업이 실행 중이거나 진행 중입니다.
- 작업이 일시 중지되었습니다.
- 작업이 재개되고 실행 중 상태입니다.

- 작업이 다른 노드로 장애 조치를 기다리는 경우

다음 상황에서 보안 정책에 대한 작업이 있는 경우 해당 보안 정책 또는 해당 정책에 할당된 작업을 성공적으로 수정할 수 있습니다.

- 정책 작업이 중지되었습니다.
- 정책 작업이 성공적으로 완료되었습니다.

SMB 서버에서 NTFS 보안 설명자를 관리하기 위한 ONTAP 명령

보안 설명자를 관리하기 위한 특정 ONTAP 명령이 있습니다. 보안 설명자에 대한 정보를 생성, 수정, 삭제 및 표시할 수 있습니다.

원하는 작업	이 명령 사용...
NTFS 보안 설명자를 만듭니다	'vserver security file-directory NTFS create'
기존 NTFS 보안 설명자를 수정합니다	'vserver security file-directory NTFS modify'를 참조하십시오
기존 NTFS 보안 설명자에 대한 정보를 표시합니다	'vserver security file-directory NTFS show'
NTFS 보안 설명자를 삭제합니다	'vserver security file-directory NTFS delete

에 대한 자세한 내용은 `vserver security file-directory ntfs` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 서버에서 NTFS DACL 액세스 제어 항목을 관리하기 위한 ONTAP 명령

DACL ACE(액세스 제어 항목)를 관리하기 위한 특정 ONTAP 명령이 있습니다. 언제든지 ACE를 NTFS DACL에 추가할 수 있습니다. DACL의 ACE에 대한 정보를 수정, 삭제 및 표시하여 기존 NTFS DACL을 관리할 수도 있습니다.

원하는 작업	이 명령 사용...
ACE를 만들어 NTFS DACL에 추가합니다	'vserver security file-directory NTFS DACL add'
NTFS DACL에서 기존 ACE를 수정합니다	'vserver security file-directory NTFS DACL modify'를 선택합니다
NTFS DACL의 기존 ACE에 대한 정보를 표시합니다	'vserver security file-directory NTFS DACL show'
NTFS DACL에서 기존 ACE를 제거합니다	'vserver security file-directory NTFS DACL remove'

에 대한 자세한 내용은 `vserver security file-directory ntfs dacl` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 서버에서 NTFS SACL 액세스 제어 항목을 관리하기 위한 ONTAP 명령

SACL ACE(액세스 제어 항목)를 관리하기 위한 특정 ONTAP 명령이 있습니다. 언제든지 ACE를 NTFS SACL에 추가할 수 있습니다. SACL의 ACE에 대한 정보를 수정, 삭제 및 표시하여 기존 NTFS SACL을 관리할 수도 있습니다.

원하는 작업	이 명령 사용...
ACE를 만들어 NTFS SACL에 추가합니다	'vserver security file-directory NTFS SACL add'
NTFS SACL에서 기존 ACE를 수정합니다	'vserver security file-directory NTFS SACL modify'를 참조하십시오
NTFS SACL의 기존 ACE에 대한 정보를 표시합니다	'vserver security file-directory NTFS SACL show'
NTFS SACL에서 기존 ACE를 제거합니다	'vserver security file-directory NTFS SACL remove'

에 대한 자세한 내용은 `vserver security file-directory ntfs sacl` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 보안 정책을 관리하기 위한 ONTAP 명령

보안 정책을 관리하기 위한 특정 ONTAP 명령이 있습니다. 정책에 대한 정보를 표시하고 정책을 삭제할 수 있습니다. 보안 정책을 수정할 수 없습니다.

원하는 작업	이 명령 사용...
보안 정책을 생성합니다	'vserver security file-directory policy create'를 참조하십시오
보안 정책에 대한 정보를 표시합니다	'vserver security file-directory policy show'를 선택합니다
보안 정책을 삭제합니다	'vserver security file-directory policy delete

에 대한 자세한 내용은 `vserver security file-directory policy` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 보안 정책 작업을 관리하기 위한 ONTAP 명령

보안 정책 작업에 대한 정보를 추가, 수정, 제거 및 표시하는 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
보안 정책 작업을 추가합니다	'vserver security file-directory policy task add'

원하는 작업	이 명령 사용...
보안 정책 작업을 수정합니다	'vserver security file-directory policy task modify'를 선택합니다
보안 정책 작업에 대한 정보를 표시합니다	'vserver security file-directory policy task show'를 선택합니다
보안 정책 작업을 제거합니다	'vserver security file-directory policy task remove'

에 대한 자세한 내용은 `vserver security file-directory policy task` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 보안 정책 작업을 관리하기 위한 ONTAP 명령

보안 정책 작업에 대한 정보를 일시 중지, 다시 시작, 중지 및 표시하는 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
보안 정책 작업을 일시 중지합니다	'vserver security file-directory job pause -vserver vserver_name -id integer'
보안 정책 작업을 다시 시작합니다	'vserver security file-directory job resume - vserver vserver_name -id integer'
보안 정책 작업에 대한 정보를 표시합니다	'vserver security file-directory job show -vserver_name' 이 명령을 사용하여 작업의 작업 ID를 확인할 수 있습니다.
보안 정책 작업을 중지합니다	'vserver security file-directory job stop -vserver vserver_name -id integer'

에 대한 자세한 내용은 `vserver security file-directory job` "ONTAP 명령 참조입니다"을 참조하십시오.

SMB 공유에 대한 메타데이터 캐시를 구성합니다

ONTAP SMB 메타데이터 캐싱에 대해 알아보세요

메타데이터 캐싱을 사용하면 SMB 1.0 클라이언트에서 파일 속성 캐싱을 통해 파일 및 폴더 특성에 더 빠르게 액세스할 수 있습니다. 공유별로 특성 캐싱을 설정하거나 해제할 수 있습니다. 메타데이터 캐시가 설정된 경우 캐시된 항목에 대한 라이브 시간 을 구성할 수도 있습니다. 클라이언트가 SMB 2.x 또는 SMB 3.0을 통해 공유에 접속하는 경우에는 메타데이터 캐싱을 구성할 필요가 없습니다.

SMB 메타데이터 캐시가 설정되면 제한된 시간 동안 경로 및 파일 속성 데이터를 저장합니다. 따라서 공통 워크로드를 사용하는 SMB 1.0 클라이언트의 SMB 성능이 향상될 수 있습니다.

특정 작업의 경우 SMB는 경로 및 파일 메타데이터에 대한 여러 개의 동일한 쿼리를 포함할 수 있는 상당한 양의

트래픽을 생성합니다. SMB 메타데이터 캐싱을 사용하여 캐시에서 정보를 가져오는 방식으로 SMB 1.0 클라이언트의 중복 쿼리 수를 줄이고 성능을 향상할 수 있습니다.

가능성은 낮지만 메타데이터 캐시가 오래된 정보를 SMB 1.0 클라이언트에 제공할 수도 있습니다. 귀사의 환경에서 이러한 위험을 감당할 수 없는 경우 이 기능을 활성화하지 마십시오.

ONTAP SMB 메타데이터 캐시 활성화

SMB 메타데이터 캐시를 설정하여 SMB 1.0 클라이언트의 SMB 성능을 향상할 수 있습니다. 기본적으로 SMB 메타데이터 캐싱은 해제되어 있습니다.

단계

1. 원하는 작업을 수행합니다.

원하는 작업	명령 입력...
공유를 생성할 때 SMB 메타데이터 캐싱을 설정합니다	'vserver cifs share create -vserver_vserver_name_ -share-name_share_name_-path_path_-share -properties attributecache'
기존 공유에서 SMB 메타데이터 캐싱을 설정합니다	"vserver cifs 공유 속성 add -vserver_vserver_name_ -share-name_share_name_-share-properties attributecache

관련 정보

- 메타데이터 캐시 항목의 수명 구성
- 기존 주식에 주식 속성 추가 또는 제거

ONTAP SMB 메타데이터 캐시 항목의 수명 구성

SMB 메타데이터 캐시 항목의 수명을 구성하여 사용자 환경에서 SMB 메타데이터 캐시 성능을 최적화할 수 있습니다. 기본값은 10초입니다.

시작하기 전에

SMB 메타데이터 캐시 기능을 활성화해야 합니다. SMB 메타데이터 캐싱이 설정되어 있지 않으면 SMB 캐시 TTL 설정이 사용되지 않습니다.

단계

1. 원하는 작업을 수행합니다.

다음과 같은 경우 **SMB** 메타데이터 캐시 항목의 수명을 구성하려는 경우	명령 입력...
공유를 생성합니다	'vserver cifs share-create-vserver_vserver_name_-share-name_share_name_-path_path_-attribute-cache-tl[integer][integerm]'

다음과 같은 경우 **SMB** 메타데이터 캐시 항목의 수명을 구성하려는 경우	명령 입력…
기존 공유를 수정합니다	'vserver cifs share-modify-vserver_vserver_name_-share-name_share_name_-attribute-cache-tl[integerh][integerm][integer]'

공유를 생성하거나 수정할 때 추가 공유 구성 옵션과 속성을 지정할 수 있습니다. 에 대한 자세한 내용은 `vserver cifs share` "ONTAP 명령 참조입니다"을 참조하십시오.

파일 잠금 관리

프로토콜 간 **ONTAP SMB** 파일 잠금에 대해 알아보세요

파일 잠금은 사용자가 이전에 다른 사용자가 연 파일에 액세스하지 못하도록 클라이언트 응용 프로그램에서 사용하는 방법입니다. ONTAP가 파일을 잠그는 방법은 클라이언트의 프로토콜에 따라 다릅니다.

클라이언트가 NFS 클라이언트인 경우 잠금이 권고사항이고, 클라이언트가 SMB 클라이언트인 경우 잠금이 필수입니다.

NFS와 SMB 파일 잠금의 차이로 인해 NFS 클라이언트가 SMB 애플리케이션에서 이전에 연 파일에 액세스하지 못할 수 있습니다.

NFS 클라이언트가 SMB 애플리케이션에 의해 잠긴 파일에 액세스하려고 할 때 다음이 발생합니다.

- 혼합 볼륨 또는 NTFS 볼륨에서 rm, rmdir, mv 등의 파일 조작 작업으로 인해 NFS 응용 프로그램이 실패할 수 있습니다.
- NFS 읽기 및 쓰기 작업은 SMB 거부-읽기 및 거부-쓰기 열기 모드에 의해 각각 거부됩니다.
- 배타적 SMB bytelock로 파일의 쓰기 범위가 잠기면 NFS 쓰기 작업이 실패합니다.
- 연결을 끊습니다
  - NTFS 파일 시스템의 경우 SMB 및 CIFS 삭제 작업이 지원됩니다.

    마지막으로 닫은 후에 파일이 제거됩니다.
  - NFS 연결 해제 작업은 지원되지 않습니다.

    NTFS 및 SMB 의미가 필요하고 NFS에 대해 마지막 Delete-On-Close 작업이 지원되지 않기 때문에 지원되지 않습니다.
  - UNIX 파일 시스템의 경우 연결 해제 작업이 지원됩니다.

    NFS 및 UNIX 시맨틱이 필요하기 때문에 지원됩니다.
- 이름 바꾸기
  - NTFS 파일 시스템의 경우 SMB 또는 CIFS에서 대상 파일을 열면 대상 파일의 이름을 바꿀 수 있습니다.
  - NFS 이름 변경은 지원되지 않습니다.

NTFS 및 SMB 의미가 필요하므로 지원되지 않습니다.

UNIX 보안 스타일 볼륨에서 NFS 링크 해제 및 이름 바꾸기 작업은 SMB 잠금 상태를 무시하고 파일에 대한 액세스를 허용합니다. UNIX 보안 스타일 볼륨에서 다른 모든 NFS 작업은 SMB 잠금 상태를 존중합니다.

ONTAP SMB 읽기 전용 비트에 대해 알아보세요

읽기 전용 비트는 파일을 쓰기 가능(사용 안 함)인지 읽기 전용(사용 가능)인지를 나타내기 위해 파일별로 설정됩니다.

Windows를 사용하는 SMB 클라이언트는 파일당 읽기 전용 비트를 설정할 수 있습니다. NFS 클라이언트는 파일당 읽기 전용 비트를 사용하는 프로토콜 작업이 없으므로 파일당 읽기 전용 비트를 설정하지 않습니다.

ONTAP는 Windows를 사용하는 SMB 클라이언트가 해당 파일을 생성할 때 파일에 읽기 전용 비트를 설정할 수 있습니다. 또한 ONTAP는 NFS 클라이언트와 SMB 클라이언트 간에 파일이 공유될 때 읽기 전용 비트를 설정할 수 있습니다. 일부 소프트웨어는 NFS 클라이언트 및 SMB 클라이언트에서 사용할 때 읽기 전용 비트를 사용하도록 설정해야 합니다.

ONTAP가 NFS 클라이언트와 SMB 클라이언트 간에 공유되는 파일에 대해 적절한 읽기 및 쓰기 권한을 유지하려면 다음 규칙에 따라 읽기 전용 비트를 처리합니다.

- NFS는 읽기 전용 비트가 설정된 파일을 쓰기 권한 비트가 설정되지 않은 것처럼 처리합니다.
- NFS 클라이언트가 모든 쓰기 권한 비트를 사용하지 않도록 설정하고 이전에 해당 비트 중 하나 이상이 활성화된 경우 ONTAP는 해당 파일에 대해 읽기 전용 비트를 설정합니다.
- NFS 클라이언트가 쓰기 권한 비트를 설정하면 ONTAP는 해당 파일에 대해 읽기 전용 비트를 해제합니다.
- 파일에 대한 읽기 전용 비트가 설정되어 있고 NFS 클라이언트가 해당 파일에 대한 권한을 검색하려고 하면 파일에 대한 권한 비트가 NFS 클라이언트로 전송되지 않고 ONTAP는 쓰기 권한 비트가 마스킹된 상태로 NFS 클라이언트에 사용 권한 비트를 전송합니다.
- 파일에 대한 읽기 전용 비트가 설정되어 있고 SMB 클라이언트가 읽기 전용 비트를 사용하지 않도록 설정한 경우 ONTAP는 해당 파일에 대한 소유자의 쓰기 권한 비트를 설정합니다.
- 읽기 전용 비트가 설정된 파일은 루트에서만 쓸 수 있습니다.

읽기 전용 비트는 다음과 같은 방식으로 ACL 및 Unix 모드 비트와 상호 작용합니다.

파일에 읽기 전용 비트가 설정된 경우:

- 해당 파일의 ACL에는 변경 사항이 없습니다. NFS 클라이언트는 읽기 전용 비트가 설정되기 전과 동일한 ACL을 보게 됩니다.
- 파일에 대한 쓰기 접근을 허용하는 모든 Unix 모드 비트는 무시됩니다.
- NFS와 SMB 클라이언트는 모두 파일을 읽을 수 있지만, 수정할 수는 없습니다.
- ACL 및 UNIX 모드 비트는 읽기 전용 비트 때문에 무시됩니다. 즉, ACL이 쓰기 액세스를 허용하더라도 읽기 전용 비트는 수정을 방지합니다.

파일에 읽기 전용 비트가 설정되지 않은 경우:

- ONTAP ACL 및 UNIX 모드 비트를 기반으로 액세스를 결정합니다.
  - ACL 또는 UNIX 모드 비트가 쓰기 액세스를 거부하는 경우 NFS 및 SMB 클라이언트는 파일을 수정할 수 없습니다.

◦ ACL이나 UNIX 모드 비트가 쓰기 액세스를 거부하지 않으면 NFS 및 SMB 클라이언트가 파일을 수정할 수 있습니다.

> 파일 권한 변경은 SMB 클라이언트에 즉시 적용되지만 NFS 클라이언트가 특성 캐싱을 사용하는 경우 NFS 클라이언트에 즉시 적용되지 않을 수 있습니다.

공유 경로 구성 요소에 대한 잠금 처리에서 **ONTAP**가 **Windows**와 어떻게 다른지 설명합니다

Windows와 달리 ONTAP는 파일이 열려 있는 동안 열려 있는 파일에 대한 경로의 각 구성 요소를 잠그지 않습니다. 이 동작은 SMB 공유 경로에도 영향을 줍니다.

ONTAP는 경로의 각 구성 요소를 잠그지 않으므로 열려 있는 파일 또는 공유 위에 있는 경로 구성 요소의 이름을 바꿀 수 있습니다. 이렇게 하면 특정 응용 프로그램에 문제가 발생하거나 SMB 구성의 공유 경로가 잘못될 수 있습니다. 이로 인해 공유에 액세스할 수 없게 될 수 있습니다.

경로 구성 요소의 이름을 변경하여 발생하는 문제를 방지하려면 사용자나 응용 프로그램이 중요한 디렉터리의 이름을 바꾸지 못하도록 보안 설정을 적용할 수 있습니다.

ONTAP SMB 잠금에 대한 정보 표시

현재 파일 잠금에 대한 정보를 표시할 수 있습니다. 여기에는 보유한 잠금의 유형 및 잠금 상태, 바이트 범위 잠금에 대한 세부 정보, 공유 잠금 모드, 위임 잠금 및 편의적 잠금, 잠금이 내구성 또는 지속 핸들로 열렸는지 여부 등이 포함됩니다.

이 작업에 대해

NFSv4 또는 NFSv4.1을 통해 설정된 잠금에 대해 클라이언트 IP 주소를 표시할 수 없습니다.

기본적으로 명령은 모든 잠금에 대한 정보를 표시합니다. 명령 매개 변수를 사용하여 특정 SVM(스토리지 가상 머신)의 잠금에 대한 정보를 표시하거나 명령의 출력을 다른 기준으로 필터링할 수 있습니다.

'vserver lock show' 명령은 네 가지 유형의 잠금에 대한 정보를 표시합니다.

- 바이트 범위 잠금 - 파일의 일부만 잠급니다.
- 공유 잠금 - 열린 파일을 잠급니다.
- SMB를 통한 클라이언트 측 캐싱을 제어하는 편의적 잠금 기능
- 위임 - NFSv4.x에서 클라이언트 측 캐싱을 제어합니다

선택적 매개 변수를 지정하면 각 잠금 유형에 대한 중요한 정보를 확인할 수 있습니다. 에 대한 자세한 내용은 `vserver locks show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 'vserver lock show' 명령을 사용하여 잠금에 대한 정보를 표시합니다.

예

다음 예에서는 '/vol1/file1' 경로가 있는 파일의 NFSv4 잠금에 대한 요약 정보를 표시합니다. sharelock 액세스 모드는 write-deny_none 이며, 잠금이 쓰기 위임과 함께 부여되었습니다.

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
              Sharelock Mode: write-deny_none
                                                        delegation  -
              Delegation Type: write
```

다음 예에서는 경로 '/data2/data2_2/intro.pptx'를 사용하여 파일의 SMB 잠금에 대한 자세한 oplock 및 sharelock 정보를 표시합니다. IP 주소가 10.3.1.3인 클라이언트에 write-deny_none의 공유 잠금 액세스 모드를 가진 파일에 내구성 있는 핸들이 부여됩니다. 배치 oplock 레벨이 있는 리스 oplock이 부여됩니다.

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                  Vserver: vs1
                   Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                  Vserver: vs1
                   Volume: data2_2
```

```
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

ONTAP SMB 잠금 해제

파일 잠금으로 인해 클라이언트가 파일에 액세스하지 못하는 경우 현재 보류된 잠금에 대한 정보를 표시한 다음 특정 잠금을 중단할 수 있습니다. 잠금을 해제해야 하는 시나리오의 예로는 응용 프로그램 디버깅이 있습니다.

이 작업에 대해

`vserver locks break`명령은 advanced 권한 수준 이상에서만 사용할 수 있습니다. 에 대한 자세한 내용은 `vserver locks break` link:https://docs.netapp.com/us-en/ontap-cli/vserver-locks-break.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

단계

1. 잠금을 해제해야 하는 정보를 찾으려면 'vserver lock show' 명령을 사용합니다.

   에 대한 자세한 내용은 `vserver locks show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
3. 다음 작업 중 하나를 수행합니다.

다음을 지정하여 잠금을 해제하려면...	명령 입력...
SVM 이름, 볼륨 이름, LIF 이름 및 파일 경로	'vserver lock break - vserver vserver_name - volume volume_name - path path path -lif lif'
잠금 ID입니다	'vserver lock break-lockid UUID

4. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

SMB 작업을 모니터링합니다

ONTAP SMB 세션 정보 표시

SMB 연결 및 세션 ID와 세션을 사용하는 워크스테이션의 IP 주소를 포함하여 설정된 SMB 세션에 대한 정보를 표시할 수 있습니다. 세션의 SMB 프로토콜 버전 및 지속적으로 사용 가능한 보호 수준에 대한 정보를 표시하여 세션이 무중단 운영을 지원하는지 여부를 확인할 수 있습니다.

이 작업에 대해

SVM의 모든 세션에 대한 정보를 요약 형식으로 표시할 수 있습니다. 그러나 대부분의 경우 반환되는 출력량이 큽니다. 옵션 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다.

- 옵션 '-fields' 매개변수를 사용하여 선택한 필드에 대한 출력을 표시할 수 있습니다.

  필드를 입력할 수 있습니다 사용할 수 있는 필드를 결정합니다.

- '-instance' 매개 변수를 사용하면 설정된 SMB 세션에 대한 자세한 정보를 표시할 수 있습니다.
- '-fields' 매개 변수 또는 '-instance' 매개 변수를 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

SMB 세션 정보를 표시하려면...	다음 명령을 입력합니다...
SVM의 모든 세션에 대해 요약 양식을 작성합니다	'vserver cifs session show -vserver vserver_name'을 선택합니다
지정된 연결 ID에 있습니다	'vserver cifs session show -vserver vserver_name -connection -id integer'를 선택합니다
지정된 워크스테이션 IP 주소에서	'vserver cifs session show -vserver vserver_name -address workstation_ip_address'
지정된 LIF IP 주소입니다	'vserver cifs session show -vserver vserver_name -lif-address LIF_ip_address'

SMB 세션 정보를 표시하려면…	다음 명령을 입력합니다…
지정된 노드에서	'vserver cifs session show -vserver vserver_name -node{node_name
local}'	지정된 Windows 사용자로부터
'vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name'	지정된 인증 메커니즘을 사용합니다
'vserver cifs session show -vserver vserver_name -auth-mechanism{NTLMv1	NTLMv2
Kerberos	Anonymous}'
지정된 프로토콜 버전을 사용하여	'vserver cifs session show -vserver vserver_name -protocol -version{SMB1
SMB2	SMB2_1
SMB3	SMB3_1}'을 선택합니다 [NOTE] ==== 지속적으로 사용 가능한 보호 기능과 SMB 멀티 채널은 SMB 3.0 이상 세션에서만 사용할 수 있습니다. 모든 적격 세션에서 해당 상태를 보려면 이 매개 변수를 'MB3' 이상으로 설정한 값으로 지정해야 합니다. ====
지속적으로 사용 가능한 보호 수준을 지정합니다	'vserver cifs session show -vserver vserver_name -Continuously-available{No
Yes	Partial}' [NOTE] ==== 계속 사용 가능한 상태가 "부분"인 경우 세션에 하나 이상의 열려 있는 연속 사용 가능한 파일이 포함되어 있지만 세션에 계속 사용 가능한 보호 기능이 있는 일부 파일이 열려 있지 않은 것입니다. 'vserver cifs sessions file show' 명령을 사용하여 설정된 세션에서 계속 사용 가능한 보호 기능을 사용하여 열려 있지 않은 파일을 확인할 수 있습니다. ====
지정된 SMB 서명 세션 상태	'vserver cifs session show -vserver vserver_name -is-session -signed{true

예

다음 명령을 실행하면 IP 주소가 10.1.1.1인 워크스테이션에서 설정된 SVM VS1 세션의 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                      Open          Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

다음 명령을 실행하면 SVM VS1 에서 지속적으로 사용 가능한 보호 기능을 지원하는 세션에 대한 자세한 세션 정보가 표시됩니다. 도메인 계정을 사용하여 연결을 만들었습니다.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

다음 명령을 실행하면 SVM VS1 기반 SMB 3.0 및 SMB 멀티 채널을 사용하는 세션에 대한 세션 정보가 표시됩니다. 이 예에서 사용자는 LIF IP 주소를 사용하여 SMB 3.0 지원 클라이언트에서 이 공유에 연결했습니다. 따라서 인증 메커니즘은 NTLMv2로 기본값입니다. 지속적으로 사용 가능한 보호 기능을 사용하여 연결하려면 Kerberos 인증을 사용하여 연결해야 합니다.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

관련 정보

열려 있는 SMB 파일에 대한 정보 표시

열려 있는 **ONTAP SMB** 파일에 대한 정보 표시

SMB 연결 및 세션 ID, 호스팅 볼륨, 공유 이름 및 공유 경로를 포함하여 열려 있는 SMB 파일에 대한 정보를 표시할 수 있습니다. 파일의 지속적인 사용 가능한 보호 수준에 대한 정보를 표시할 수 있습니다. 이 정보는 열려 있는 파일이 무중단 작업을 지원하는 상태에 있는지 여부를 확인하는 데 유용합니다.

이 작업에 대해

설정된 SMB 세션에서 열린 파일에 대한 정보를 표시할 수 있습니다. 표시된 정보는 SMB 세션 내의 특정 파일에 대한 SMB 세션 정보를 확인해야 할 때 유용합니다.

예를 들어, 열린 파일 중 일부가 지속적으로 사용 가능한 보호 기능을 통해 열려 있고 일부는 지속적으로 사용 가능한 보호 기능을 통해 열려 있지 않은 SMB 세션이 있는 경우(vserver cifs session show 명령의 출력 값이 부분(Partial)인 경우), 이 명령을 사용하여 계속 사용할 수 없는 파일을 확인할 수 있습니다.

선택적 매개 변수 없이 'vserver cifs session file show' 명령을 사용하면 SVM(스토리지 가상 시스템)에서 설정된 SMB 세션의 모든 열려 있는 파일에 대한 정보를 요약 형식으로 표시할 수 있습니다.

그러나 대부분의 경우 반환되는 출력량이 큽니다. 선택적 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할

수 있습니다. 이 기능은 열려 있는 파일의 작은 하위 집합에 대한 정보만 보려는 경우에 유용합니다.

- 옵션 '-fields' 매개변수를 사용하여 선택한 필드에 출력을 표시할 수 있습니다.

  이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

- '-instance' 매개 변수를 사용하여 열려 있는 SMB 파일에 대한 자세한 정보를 표시할 수 있습니다.

  이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

열려 있는 **SMB** 파일을 표시하려면...	다음 명령을 입력합니다...
SVM에 대해 요약 형식으로 표시됩니다	'vserver cifs session file show -vserver vserver_name'을 선택합니다
지정된 노드에서	'vserver cifs session file show -vserver vserver_name -node{node_name
local}'를 선택합니다	지정된 파일 ID에 있습니다
'vserver cifs session file show -vserver vserver_name -file-id integer'를 선택합니다	지정된 SMB 연결 ID에서
'vserver cifs session file show -vserver vserver_name -connection -id integer'를 선택합니다	지정된 SMB 세션 ID에서
'vserver cifs session file show -vserver vserver_name -session-id integer'를 선택합니다	지정된 호스팅 집계에서
'vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name'	지정된 볼륨에서
'vserver cifs session file show -vserver vserver_name -hosting -volume volume volume_name'	지정된 SMB 공유에서
'vserver cifs session file show -vserver vserver_name -share share_name'	지정된 SMB 경로에 있어야 합니다
'vserver cifs session file show -vserver vserver_name -path path path'	지속적으로 사용 가능한 보호 수준을 지정합니다

열려 있는 **SMB** 파일을 표시하려면…	다음 명령을 입력합니다…
'vserver cifs session file show -vserver vserver_name -Continuously-available{No	Yes}' [NOTE] ==== 계속 사용 가능한 상태가 '아니요'인 경우 열려 있는 파일은 Takeover와 Giveback에서 중단 없이 복구할 수 없습니다. 또한, 고가용성 관계에 있는 파트너 간의 일반 애그리게이트 재배치에서 복구할 수 없습니다. ====
지정된 다시 연결된 상태에서	'vserver cifs session file show -vserver vserver_name -re연결됨{No

출력 결과를 구체화하는 데 사용할 수 있는 추가 선택적 매개 변수가 있습니다. 에 대한 자세한 내용은 `vserver cifs session file show` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 예에서는 SVM VS1 에서 열린 파일에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

다음 예에서는 SVM VS1에서 파일 ID 82가 있는 개방형 SMB 파일에 대한 자세한 정보를 표시합니다.

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

관련 정보

세션 정보 표시

ONTAP SMB 서버에서 사용 가능한 통계, 개체 및 카운터를 확인합니다.

CIFS, SMB, 감사 및 BranchCache 해시 통계에 대한 정보를 얻고 성능을 모니터링하려면 데이터를 가져올 수 있는 개체와 카운터를 알고 있어야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

다음 사항을 확인하고자 하는 경우:	입력...
사용할 수 있는 개체	'통계 카탈로그 개체 쇼'
사용할 수 있는 특정 개체입니다	`statistics catalog object show -object object_name`
사용할 수 있는 카운터	`statistics catalog counter show -object object_name`

   사용 가능한 개체 및 카운터를 비롯한 에 대한 자세한 `statistics catalog object show` 내용은 에서 "ONTAP 명령 참조입니다"알아보십시오.

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 명령을 실행하면 고급 권한 수준에 표시된 대로 클러스터에서 CIFS 및 SMB 액세스와 관련된 선택한 통계 개체에 대한 설명이 표시됩니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

다음 명령을 실행하면 고급 권한 수준에서 표시되는 "CIFS" 개체의 일부 카운터에 대한 정보가 표시됩니다.

이 예제에서는 "CIFS" 객체에 대해 사용 가능한 카운터를 모두 표시하지 않고 출력이 잘립니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
---------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- ----------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

관련 정보

- 통계를 표시합니다
- "통계 카탈로그 카운터 개체 표시"
- "통계 시작"

ONTAP SMB 통계 표시

CIFS 및 SMB, 감사 및 BranchCache 해시에 대한 통계를 비롯한 다양한 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

시작하기 전에

객체에 대한 정보를 표시하려면 먼저 '통계 시작' 및 '통계 중지' 명령을 사용하여 데이터 샘플을 수집해야 합니다.

자세히 알아보세요 `statistics start` 그리고 `statistics stop` 에서 "ONTAP 명령 참조입니다" .

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

에 대한 통계를 표시하려면...	입력...
모든 SMB 버전	'통계 표시 - 객체 CIFS'
SMB 1.0	'스타티틱스 쇼-객체 SMB1'
SMB 2.x 및 SMB 3.0	'스타티틱스 쇼 오브젝트 SMB2'
노드의 CIFS 하위 시스템입니다	'스타티틱스 쇼-객체 nblade_cifs'
멀티프로토콜 감사	'스타티틱스 쇼-객체 감사_ng'
BranchCache 해시 서비스입니다	'스타티틱스 쇼-객체 해시드'
다이나믹 DNS	'통계 표시 - 오브젝트 DDNS_UPDATE'

   에 대한 자세한 내용은 `statistics show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

관련 정보

- 서버에서 사용 가능한 통계, 개체 및 카운터를 확인합니다.
- SMB 서명 세션 통계 모니터링
- BranchCache 통계를 표시합니다
- 통계를 사용하여 자동 노드 조회 활동을 모니터링합니다
- "Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성"

- "성능 모니터링 설정"

SMB 클라이언트 기반 서비스 구축

오프라인 파일을 사용하여 오프라인 사용을 위해 파일 캐싱을 허용합니다

오프라인 파일을 사용하여 **ONTAP SMB** 파일을 오프라인에서 사용할 수 있도록 캐싱하는 방법에 대해 알아보세요.

ONTAP는 오프라인 사용을 위해 파일을 로컬 호스트에 캐시할 수 있는 Microsoft 오프라인 파일 기능 또는 _클라이언트측 캐싱_을 지원합니다. 사용자는 오프라인 파일 기능을 사용하여 네트워크에서 연결이 끊어진 경우에도 파일 작업을 계속할 수 있습니다.

Windows 사용자 문서 및 프로그램이 자동으로 공유에서 캐시되는지 아니면 파일을 수동으로 캐시하도록 선택해야 하는지 여부를 지정할 수 있습니다. 수동 캐싱은 새 공유에 대해 기본적으로 설정됩니다. 오프라인으로 사용할 수 있는 파일은 Windows 클라이언트의 로컬 디스크와 동기화됩니다. 동기화는 특정 스토리지 시스템 공유에 대한 네트워크 접속이 복구되는 경우에 발생합니다.

오프라인 파일 및 폴더는 CIFS 서버에 저장된 파일 및 폴더의 버전과 동일한 액세스 권한을 유지하므로 오프라인 파일 및 폴더에 대한 작업을 수행하려면 CIFS 서버에 저장된 파일 및 폴더에 대한 충분한 권한이 있어야 합니다.

사용자 및 네트워크의 다른 사용자가 동일한 파일을 변경한 경우 사용자는 파일의 로컬 버전을 네트워크에 저장하거나 다른 버전을 유지하거나 둘 다 저장할 수 있습니다. 사용자가 두 버전을 모두 유지할 경우 로컬 사용자의 변경 내용이 있는 새 파일이 로컬에 저장되고 캐시된 파일은 CIFS 서버에 저장된 파일 버전의 변경 내용으로 덮어쓰입니다.

공유 구성 설정을 사용하여 공유 단위로 오프라인 파일을 구성할 수 있습니다. 공유를 만들거나 수정할 때 네 개의 오프라인 폴더 구성 중 하나를 선택할 수 있습니다.

- 캐싱이 없습니다

  공유에 대한 클라이언트 측 캐시를 해제합니다. 파일과 폴더는 클라이언트에 로컬로 자동으로 캐시되지 않으며 사용자는 파일 또는 폴더를 로컬로 캐시하도록 선택할 수 없습니다.

- 수동 캐싱

  공유에 캐시할 파일을 수동으로 선택할 수 있습니다. 기본 설정입니다. 기본적으로 파일 또는 폴더는 로컬 클라이언트에 캐시되지 않습니다. 사용자는 오프라인 사용을 위해 로컬로 캐시할 파일과 폴더를 선택할 수 있습니다.

- 자동 문서 캐싱

  사용자 문서를 공유에 자동으로 캐시할 수 있습니다. 액세스한 파일 및 폴더만 로컬로 캐시됩니다.

- 자동 프로그램 캐싱

  프로그램 및 사용자 문서를 자동으로 공유에 캐시할 수 있습니다. 액세스한 파일, 폴더 및 프로그램만 로컬로 캐시됩니다. 또한 이 설정을 사용하면 클라이언트가 네트워크에 연결되어 있는 경우에도 로컬로 캐시된 실행 파일을 실행할 수 있습니다.

Windows 서버 및 클라이언트에서 오프라인 파일을 구성하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

관련 정보

- 로밍 프로필을 사용하여 SVM과 연결된 CIFS 서버에 사용자 프로필을 중앙에서 저장합니다
- 폴더 리디렉션을 사용하여 서버에 데이터를 저장하는 방법에 대해 알아보세요.
- 지점 사무실에서 공유 콘텐츠를 캐시하기 위해 BranchCache를 사용하는 방법에 대해 알아보세요.
- "Microsoft TechNet 라이브러리: technet.microsoft.com/en-us/library/"

오프라인 **ONTAP SMB** 파일 사용에 대한 요구 사항에 대해 알아보세요.

CIFS 서버에서 Microsoft 오프라인 파일 기능을 사용하려면 먼저 ONTAP 및 SMB의 버전과 이 기능을 지원하는 Windows 클라이언트를 알아야 합니다.

ONTAP 버전 요구 사항

ONTAP 릴리스는 오프라인 파일을 지원합니다.

SMB 프로토콜 버전 요구 사항

SVM(스토리지 가상 시스템)의 경우 ONTAP은 모든 버전의 SMB에서 오프라인 파일을 지원합니다.

Windows 클라이언트 요구 사항

Windows 클라이언트는 오프라인 파일을 지원해야 합니다.

오프라인 파일 기능을 지원하는 Windows 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

"mysupport.netapp.com/matrix"

오프라인 **ONTAP SMB** 파일 배포를 위한 지침

홈 디렉토리에 'showsnapshot' 공유 속성이 설정된 홈 디렉토리 공유에 오프라인 파일을 배포할 때 이해해야 하는 몇 가지 중요한 지침이 있습니다.

공유 속성이 오프라인 파일이 구성된 홈 디렉토리 공유에 설정된 경우 `showsnapshot` Windows 클라이언트는 사용자의 홈 디렉토리에 있는 폴더 아래에 모든 스냅샷을 캐싱합니다. `~snapshot`

다음 중 하나에 해당하면 Windows 클라이언트가 홈 디렉토리 아래에 있는 모든 스냅샷을 캐시합니다.

- 사용자가 클라이언트에서 홈 디렉토리를 오프라인으로 사용할 수 있도록 합니다.

  홈 디렉토리에 있는 '~snapshot' 폴더의 내용이 포함되어 오프라인으로 사용할 수 있습니다.

- 사용자는 '내 문서'와 같은 폴더를 CIFS 서버 공유에 있는 홈 디렉토리의 루트로 리디렉션하도록 폴더 리디렉션을 구성합니다.

  일부 Windows 클라이언트는 리디렉션된 폴더를 자동으로 오프라인으로 사용할 수 있도록 만들 수 있습니다. 폴더가 홈 디렉토리의 루트로 리디렉션되면 "~snapshot" 폴더가 캐시된 오프라인 콘텐츠에 포함됩니다.

오프라인 파일에 폴더가 포함된 오프라인 파일 배포는 `~snapshot` 피해야 합니다. 폴더의 스냅샷에는 `~snapshot` ONTAP가 스냅샷을 생성한 시점의 볼륨에 있는 모든 데이터가 포함됩니다. 따라서 폴더의 오프라인 복사본을 만들면 `~snapshot` 클라이언트에서 많은 로컬 스토리지가 사용되고, 오프라인 파일 동기화 중에 네트워크 대역폭이 소모되며, 오프라인 파일을 동기화하는 데 걸리는 시간이 늘어납니다.

오프라인 **SMB** 파일 지원을 구성하기 위한 **ONTAP** 명령

SMB 공유를 생성할 때 또는 언제든지 기존 SMB 공유를 수정하여 오프라인 파일 4개 설정 중 하나를 지정하여 ONTAP CLI를 사용하여 오프라인 파일 지원을 구성할 수 있습니다. 수동 오프라인 파일 지원은 기본 설정입니다.

이 작업에 대해

오프라인 파일 지원을 구성할 때 다음 네 가지 오프라인 파일 설정 중 하나를 선택할 수 있습니다.

설정	설명
"없음"	Windows 클라이언트가 이 공유의 모든 파일을 캐싱하지 않습니다.
수동	Windows 클라이언트의 사용자가 캐시할 파일을 수동으로 선택할 수 있습니다.
문서	Windows 클라이언트가 오프라인 액세스를 위해 사용자가 사용하는 사용자 문서를 캐시할 수 있도록 합니다.
프로그램	Windows 클라이언트가 오프라인 액세스를 위해 사용자가 사용하는 프로그램을 캐시에 저장하도록 허용합니다. 클라이언트는 공유를 사용할 수 있는 경우에도 오프라인 모드에서 캐시된 프로그램 파일을 사용할 수 있습니다.

오프라인 파일 설정은 하나만 선택할 수 있습니다. 기존 SMB 공유에서 오프라인 파일 설정을 수정하면 새 오프라인 파일 설정이 원래 설정으로 대체됩니다. 기존의 다른 SMB 공유 구성 설정 및 공유 속성은 제거 또는 교체되지 않습니다. 이러한 구성 작업은 명시적으로 제거 또는 변경될 때까지 유효합니다.

단계

1. 적절한 작업을 수행합니다.

에서 오프라인 파일을 구성하려면...	명령 입력...
새로운 SMB 공유	'vserver cifs share create - vserver vserver_name -share-name share_name -path path -offline -files{none
manual	documents
programs}'	기존 SMB 공유입니다

에서 오프라인 파일을 구성하려면...	명령 입력...
'vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files{none	manual
documents	programs}'

2. SMB 공유 구성이 올바른지 확인합니다. 'vserver cifs share show -vserver vserver_name -share-name share_name -instance'

예

다음 명령을 실행하면 오프라인 파일이 "문서"로 설정된 "data1"이라는 SMB 공유가 생성됩니다.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

다음 명령을 실행하면 오프라인 파일 설정을 '수동'으로 변경하고 파일 및 디렉토리 모드 생성 마스크에 대한 값을 추가하여 "data1"이라는 기존 SMB 공유가 수정됩니다.

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
           File Mode Creation Mask: 644
      Directory Mode Creation Mask: 777
                    Share Comment: Offline files
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

관련 정보

기존 주식에 주식 속성 추가 또는 제거

컴퓨터 관리 **MMC**를 사용하여 **ONTAP SMB** 공유에서 오프라인 파일 지원 구성

사용자가 오프라인에서 사용할 수 있도록 로컬로 파일을 캐시하도록 허용하려면 컴퓨터 관리 MMC(Microsoft Management Console)를 사용하여 오프라인 파일 지원을 구성할 수 있습니다.

단계

1. Windows 서버에서 MMC를 열려면 Windows 탐색기에서 로컬 컴퓨터 아이콘을 마우스 오른쪽 단추로 클릭한 다음 * 관리 * 를 선택합니다.
2. 왼쪽 패널에서 * 컴퓨터 관리 * 를 선택합니다.
3. 작업 * > * 다른 컴퓨터에 연결 * 을 선택합니다.

   컴퓨터 선택 대화 상자가 나타납니다.
4. CIFS 서버의 이름을 입력하거나 * Browse * 를 클릭하여 CIFS 서버를 찾습니다.

   CIFS 서버의 이름이 SVM(Storage Virtual Machine) 호스트 이름과 같으면 SVM 이름을 입력합니다. CIFS 서버 이름이 SVM 호스트 이름과 다른 경우 CIFS 서버의 이름을 입력합니다.

5. 확인 * 을 클릭합니다.
6. 콘솔 트리에서 * 시스템 도구 * > * 공유 폴더 * 를 클릭합니다.
7. 공유 * 를 클릭합니다.
8. 결과 창에서 공유를 마우스 오른쪽 버튼으로 클릭합니다.
9. 속성 * 을 클릭합니다.

   선택한 공유의 속성이 표시됩니다.

10. 일반 * 탭에서 * 오프라인 설정 * 을 클릭합니다.

    오프라인 설정 대화 상자가 나타납니다.

11. 필요에 따라 오프라인 사용 가능성 옵션을 구성합니다.
12. 확인 * 을 클릭합니다.

로밍 프로필을 사용하여 **SVM**과 연결된 **SMB** 서버에 사용자 프로필을 중앙에서 저장합니다

로밍 프로필을 사용하여 **ONTAP SMB** 사용자 프로필을 중앙에서 저장하는 방법에 대해 알아보세요.

ONTAP는 SVM(스토리지 가상 머신)과 연결된 CIFS 서버에 Windows 로밍 프로필을 저장할 수 있도록 지원합니다. 사용자 로밍 프로파일을 구성하면 사용자가 로그인하는 위치에 관계없이 자동 리소스 사용 가능 여부 등의 이점이 제공됩니다. 또한 로밍 프로필은 사용자 프로필의 관리 및 관리를 간소화합니다.

로밍 사용자 프로필에는 다음과 같은 이점이 있습니다.

- 자동 리소스 가용성

  사용자가 Windows 8, Windows 7, Windows 2000 또는 Windows XP를 실행하는 네트워크의 컴퓨터에 로그인하면 사용자의 고유한 프로필을 자동으로 사용할 수 있습니다. 사용자는 네트워크에서 사용하는 각 컴퓨터에 프로파일을 만들 필요가 없습니다.

- 간편한 컴퓨터 교체

  사용자 프로파일 정보는 모두 네트워크에서 별도로 유지되므로 사용자의 프로파일을 새 대체 컴퓨터에 쉽게 다운로드할 수 있습니다. 사용자가 새 컴퓨터에 처음 로그인하면 사용자 프로필의 서버 복사본이 새 컴퓨터에 복사됩니다.

관련 정보

- 오프라인 사용을 위해 파일을 캐싱하는 오프라인 파일 사용에 대해 알아보세요.
- 폴더 리디렉션을 사용하여 서버에 데이터를 저장하는 방법에 대해 알아보세요.

로밍 **ONTAP SMB** 프로필 사용에 대한 요구 사항에 대해 알아보세요.

CIFS 서버에서 Microsoft의 로밍 프로필을 사용하려면 먼저 ONTAP 및 SMB의 버전과 이 기능을 지원하는 Windows 클라이언트를 알아야 합니다.

ONTAP 버전 요구 사항

ONTAP는 로밍 프로필을 지원합니다.

SMB 프로토콜 버전 요구 사항

SVM(스토리지 가상 시스템)의 경우 ONTAP은 모든 버전의 SMB에서 로밍 프로필을 지원합니다.

Windows 클라이언트 요구 사항

사용자가 로밍 프로필을 사용하려면 Windows 클라이언트가 이 기능을 지원해야 합니다.

로밍 프로필을 지원하는 Windows 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

"NetApp 상호 운용성 매트릭스 툴"

Active Directory 사용자 및 컴퓨터 MMC를 통해 로밍 ONTAP SMB 프로필 구성

사용자가 네트워크의 컴퓨터에 로그온할 때 자동으로 사용자 프로필을 사용할 수 있도록 하려면 Active Directory 사용자 및 컴퓨터 MMC 스냅인을 통해 로밍 프로필을 구성할 수 있습니다. Windows Server에서 로밍 프로필을 구성하는 경우 Active Directory 관리 센터를 사용할 수 있습니다.

단계

1. Windows 서버에서 Active Directory 사용자 및 컴퓨터 MMC(또는 Windows 서버의 Active Directory 관리 센터)를 엽니다.
2. 로밍 프로필을 구성할 사용자를 찾습니다.
3. 사용자를 마우스 오른쪽 단추로 클릭하고 * 속성 * 을 클릭합니다.
4. 프로필 * 탭에서 사용자의 로밍 프로필을 저장할 공유의 프로파일 경로를 입력한 다음 '%username%'을(를) 입력합니다.

   예를 들어, 프로파일 경로는 다음과 같습니다: '\\vs1.example.com\profiles\%username%`. 사용자가 처음 로그인하면 '%username%'이(가) 사용자 이름으로 대체됩니다.

   > '\\vs1.example.com\profiles\%username%` 경로에서 'profiles'는 SVM(Storage Virtual Machine) VS1 공유에 대한 공유 이름이며 모든 사람에게 모든 권한이 부여됩니다.

5. 확인 * 을 클릭합니다.

SMB 서버에 데이터를 저장하려면 폴더 리디렉션을 사용합니다

ONTAP SMB 서버에 데이터를 저장하기 위해 폴더 리디렉션을 사용하는 방법에 대해 알아보세요.

ONTAP는 사용자 또는 관리자가 로컬 폴더의 경로를 CIFS 서버의 위치로 리디렉션할 수 있도록 Microsoft 폴더 리디렉션을 지원합니다. SMB 공유에 데이터가 저장되어 있더라도 리디렉션된 폴더가 로컬 Windows 클라이언트에 저장된 것처럼 나타납니다.

폴더 리디렉션은 주로 홈 디렉터리를 이미 배포했으며 기존 홈 디렉터리 환경과의 호환성을 유지하고자 하는 조직을 위한 것입니다.

- 문서, 바탕 화면, 시작 메뉴 등을 리디렉션할 수 있는 폴더의 예로 들 수 있습니다.
- 사용자는 Windows 클라이언트에서 폴더를 리디렉션할 수 있습니다.
- 관리자는 Active Directory에서 GPO를 구성하여 폴더 리디렉션을 중앙 집중식으로 구성 및 관리할 수 있습니다.
- 관리자가 로밍 프로필을 구성한 경우 폴더 리디렉션을 통해 관리자가 사용자 데이터를 프로필 데이터에서 나눌 수 있습니다.
- 관리자는 폴더 리디렉션 및 오프라인 파일을 함께 사용하여 로컬 폴더의 데이터 스토리지를 CIFS 서버로 리디렉션하는 동시에 사용자가 콘텐츠를 로컬로 캐시할 수 있습니다.

관련 정보

- 오프라인 사용을 위해 파일을 캐싱하는 오프라인 파일 사용에 대해 알아보세요.
- 로밍 프로필을 사용하여 SVM과 연결된 CIFS 서버에 사용자 프로필을 중앙에서 저장합니다

ONTAP SMB 폴더 리디렉션 사용에 대한 요구 사항에 대해 알아보세요**.**

CIFS 서버에서 Microsoft의 폴더 리디렉션을 사용하려면 먼저 ONTAP 및 SMB의 버전과 이 기능을 지원하는 Windows 클라이언트를 알아야 합니다.

ONTAP 버전 요구 사항

ONTAP는 Microsoft 폴더 리디렉션을 지원합니다.

SMB 프로토콜 버전 요구 사항

SVM(스토리지 가상 시스템)의 경우 ONTAP는 모든 버전의 SMB에서 Microsoft의 폴더 리디렉션을 지원합니다.

Windows 클라이언트 요구 사항

사용자가 Microsoft의 폴더 리디렉션을 사용하려면 Windows 클라이언트가 이 기능을 지원해야 합니다.

폴더 리디렉션을 지원하는 Windows 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

"mysupport.netapp.com/matrix"

Windows 속성을 사용하여 **ONTAP SMB** 폴더 리디렉션 구성

Windows 속성 창을 사용하여 폴더 리디렉션을 구성할 수 있습니다. 이 방법을 사용하면 Windows 사용자가 SVM 관리자의 도움 없이 폴더 리디렉션을 구성할 수 있다는 이점이 있습니다.

단계

1. Windows 탐색기에서 네트워크 공유로 리디렉션할 폴더를 마우스 오른쪽 단추로 클릭합니다.
2. 속성 * 을 클릭합니다.

   선택한 공유의 속성이 표시됩니다.

3. 바로 가기 * 탭에서 * 대상 * 을 클릭하고 선택한 폴더를 리디렉션할 네트워크 위치의 경로를 지정합니다.

예를 들어, 폴더를 "Q:\"에 매핑된 홈 디렉토리의 "ata" 폴더로 리디렉션하려면 "Q:\data"를 대상으로 지정합니다.

4. 확인 * 을 클릭합니다.

   오프라인 폴더 구성에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

관련 정보

"Microsoft TechNet 라이브러리: technet.microsoft.com/en-us/library/"

SMB 2.x를 사용하여 **Windows** 클라이언트에서 **ONTAP ~snapshot** 디렉토리에 액세스하는 방법에 대해 알아보세요.

SMB 2.x를 사용하여 Windows 클라이언트에서 디렉토리에 액세스하는 방법은 `~snapshot` SMB 1.0에 사용되는 방법과 다릅니다. SMB 2.x 연결을 사용하여 스냅샷에 저장된 데이터에 성공적으로 액세스할 때 디렉토리에 액세스하는 방법을 이해해야 `~snapshot` 합니다.

SVM 관리자는 가상 서버 CIFS 공유 속성 제품군의 명령을 사용하여 'showsnapshot' 공유 속성을 활성화하거나 비활성화하여 Windows 클라이언트의 사용자가 공유의 '~snapshot' 디렉토리를 보고 액세스할 수 있는지 여부를 제어합니다.

> `showsnapshot`공유 속성을 비활성화하면 `SMB 2.x`를 사용하는 `Windows` 클라이언트의 사용자는 디렉토리를 볼 수 `~snapshot` 없으며 디렉토리 내의 특정 스냅샷이나 디렉토리에 대한 경로를 수동으로 입력하는 경우에도 디렉토리 `~snapshot` 내의 스냅샷에 액세스할 수 `~snapshot` 없습니다.

'showsnapshot' 공유 속성이 활성화되면 SMB 2.x를 사용하는 Windows 클라이언트의 사용자는 공유 루트 또는 공유 루트 아래의 연결 지점 또는 디렉토리 내에서 '~snapshot' 디렉토리를 볼 수 없습니다. 그러나 공유에 접속한 후에는 공유 경로의 끝에 수동으로 \~snapshot을 추가하여 숨겨진 `~snapshot' 디렉토리에 액세스할 수 있습니다. 숨겨진 '~snapshot' 디렉토리는 두 개의 진입점에서 액세스할 수 있습니다.

- 공유 루트에 있습니다
- 공유 공간의 모든 접합 지점에서

공유 내의 비접속 하위 디렉토리에서는 숨겨진 '~snapshot' 디렉토리에 액세스할 수 없습니다.

예

다음 예제에서 보여 주는 구성을 사용하면 "eng" 공유에 SMB 2.x가 연결되어 있는 Windows 클라이언트의 사용자가 공유 경로 및 경로의 모든 연결 지점에서 공유 경로에 "\~snapshot"을 수동으로 추가하여 '~snapshot" 디렉토리에 액세스할 수 있습니다. 숨겨진 '~snapshot' 디렉토리는 다음 세 가지 경로에서 액세스할 수 있습니다.

- '\\VS1\ENG\~스냅샷'
- '\\VS1\ENG\projects1\~스냅샷'
- '\\VS1\ENG\projects2\~스냅샷'

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

이전 버전을 사용하여 파일 및 폴더를 복구합니다

이전 버전을 사용하여 **ONTAP SMB** 파일 및 폴더 복구에 대해 알아보세요

Microsoft 이전 버전을 사용하는 기능은 특정 형태의 스냅샷을 지원하고 이를 사용하도록 설정한 파일 시스템에 적용할 수 있습니다. 스냅샷 기술은 ONTAP의 핵심 요소입니다. 사용자는 Microsoft 이전 버전 기능을 사용하여 Windows 클라이언트에서 스냅샷의 파일과 폴더를 복구할 수 있습니다.

이전 버전 기능을 사용하면 스토리지 관리자의 개입 없이 스냅샷을 탐색하거나 스냅샷에서 데이터를 복구할 수 있습니다. 이전 버전은 구성할 수 없습니다. 항상 활성화되어 있습니다. 스토리지 관리자가 공유에서 스냅샷을 사용할 수 있도록 설정한 경우 사용자는 이전 버전을 사용하여 다음 작업을 수행할 수 있습니다.

- 실수로 삭제된 파일을 복구합니다.
- 실수로 파일을 덮어쓴 경우 복구
- 작업 중 파일 버전을 비교합니다.

스냅샷에 저장된 데이터는 읽기 전용입니다. 파일을 변경하려면 파일 복사본을 다른 위치에 저장해야 합니다. 스냅샷은 주기적으로 삭제되므로 이전 버전의 파일을 영구적으로 보존하려면 이전 버전에 포함된 파일의 복사본을 만들어야 합니다.

Microsoft 이전 버전을 사용하기 위한 **ONTAP SMB** 요구 사항

CIFS 서버에서 이전 버전을 사용하려면 먼저 ONTAP 및 SMB의 버전과 지원 대상 Windows 클라이언트를 알아야 합니다. 또한 스냅샷 설정 요구 사항에 대해서도 알아야 합니다.

ONTAP 버전 요구 사항

이전 버전을 지원합니다.

SMB 프로토콜 버전 요구 사항

SVM(스토리지 가상 시스템)의 경우 ONTAP은 모든 버전의 SMB에서 이전 버전을 지원합니다.

Windows 클라이언트 요구 사항

사용자가 이전 버전을 사용하여 스냅샷의 데이터에 액세스하려면 Windows 클라이언트가 해당 기능을 지원해야 합니다.

이전 버전을 지원하는 Windows 클라이언트에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

"NetApp 상호 운용성 매트릭스 툴"

스냅샷 설정에 대한 요구 사항

이전 버전을 사용하여 스냅샷의 데이터에 액세스하려면 활성화된 스냅샷 정책이 데이터를 포함하는 볼륨에 연결되어 있어야 하고, 클라이언트가 스냅샷 데이터에 액세스할 수 있어야 하며, 스냅샷이 있어야 합니다.

Windows 이전 버전 탭을 사용하여 **ONTAP SMB** 스냅샷 데이터를 보고 관리합니다**.**

Windows 클라이언트 시스템의 사용자는 Windows 속성 창의 이전 버전 탭을 사용하여 SVM(스토리지 가상 시스템) 관리자의 개입 없이 스냅샷에 저장된 데이터를 복원할 수 있습니다.

이 작업에 대해

관리자가 공유를 포함하는 볼륨에 스냅샷을 설정하고 관리자가 스냅샷을 표시하도록 공유를 구성한 경우에는 이전 버전 탭을 사용하여 SVM에 저장된 데이터의 스냅샷에서 데이터를 보고 관리할 수 있습니다.

단계

1. Windows 탐색기에서 CIFS 서버에 저장된 데이터의 매핑된 드라이브 컨텐츠를 표시합니다.
2. 스냅샷을 보거나 관리할 매핑된 네트워크 드라이브에서 파일 또는 폴더를 마우스 오른쪽 단추로 클릭합니다.
3. 속성 * 을 클릭합니다.

   선택한 파일 또는 폴더의 속성이 표시됩니다.

4. 이전 버전 * 탭을 클릭합니다.

   선택한 파일 또는 폴더의 사용 가능한 스냅샷 목록이 폴더 버전: 상자에 표시됩니다. 나열된 스냅샷은 스냅샷 이름 접두사 및 생성 타임스탬프로 식별됩니다.

5. 폴더 버전: * 상자에서 관리할 파일 또는 폴더의 복사본을 마우스 오른쪽 단추로 클릭합니다.
6. 적절한 작업을 수행합니다.

원하는 작업	다음을 수행합니다**.**
해당 스냅샷의 데이터를 봅니다	열기 * 를 클릭합니다.
해당 스냅샷에서 데이터 복제본을 생성합니다	복사 * 를 클릭합니다.

스냅샷의 데이터는 읽기 전용입니다. 이전 버전 탭에 나열된 파일과 폴더를 수정하려면 쓰기 가능한 위치에 수정할 파일 및 폴더의 복사본을 저장하고 복사본을 수정해야 합니다.

7. 스냅샷 데이터 관리를 마친 후 * 확인 * 을 클릭하여 * 속성 * 대화 상자를 닫습니다.

   이전 버전 탭을 사용하여 스냅샷 데이터를 보고 관리하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

관련 정보

"Microsoft TechNet 라이브러리: technet.microsoft.com/en-us/library/"

ONTAP SMB 스냅샷을 이전 버전에서 사용할 수 있는지 확인하세요**.**

활성화된 스냅샷 정책이 공유를 포함하는 볼륨에 적용되고 볼륨 구성에서 스냅샷에 대한 액세스를 허용하는 경우에만 이전 버전 탭에서 스냅샷을 볼 수 있습니다. 스냅샷 가용성을 확인하는 것은 이전 버전 액세스 권한을 가진 사용자를 지원할 때 유용합니다.

단계

1. 공유 데이터가 있는 볼륨에 자동 스냅샷이 설정되어 있는지 여부와 클라이언트가 스냅샷 디렉토리에 액세스할 수 있는지 여부를 확인합니다. `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   이 출력에는 볼륨과 연결된 스냅샷 정책, 클라이언트 스냅샷 디렉토리 액세스 사용 여부 및 사용 가능한 스냅샷 수가 표시됩니다.

2. 연결된 스냅샷 정책이 설정되었는지 확인합니다. `volume snapshot policy show -policy policy-name`
3. 사용 가능한 스냅샷 나열: `volume snapshot show -volume volume_name`

   스냅샷 정책 및 스냅샷 스케줄을 구성하고 관리하는 방법에 대한 자세한 내용은 을 참조하십시오."데이터 보호"

예

다음 예에서는 "'data1""의 공유 데이터 및 사용 가능한 스냅숏을 포함하는 "'data1" 볼륨과 연관된 스냅숏 정책에 대한 정보를 표시합니다.

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                   3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                  SnapMirror Label
    ---------------- -----     ----------------------- -------------------
    hourly               6     hourly                  -
    daily                2     daily                   daily
    weekly               2     weekly                  weekly

cluster1::> volume snapshot show -volume data1
                                                                 ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

관련 정보

- 이전 버전 액세스를 활성화하기 위한 스냅샷 구성 생성
- "데이터 보호"

이전 버전 액세스를 활성화하기 위해 **ONTAP SMB** 스냅샷 구성을 만듭니다.

스냅샷에 대한 클라이언트 액세스가 설정되어 있고 스냅샷이 있는 경우 이전 버전 기능을 항상 사용할 수 있습니다. 스냅샷 구성이 이러한 요구 사항을 충족하지 않는 경우 를 충족하는 스냅샷 구성을 생성할 수 있습니다.

단계

1. 이전 버전 액세스를 허용하려는 공유가 포함된 볼륨에 연결된 스냅샷 정책이 없는 경우 스냅샷 정책을 볼륨에 연결하고 명령을 사용하여 활성화합니다. `volume modify`

   에 대한 자세한 내용은 `volume modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 명령을 사용하여 옵션을 로 `true` 설정하여 `-snap-dir` 스냅샷에 대한 액세스를 `volume modify` 설정합니다.

   에 대한 자세한 내용은 `volume modify` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 및 `volume snapshot policy show` 명령을 사용하여 스냅샷 정책이 설정되어 있고 스냅샷 디렉토리에 대한 액세스가 설정되어 있는지 `volume show` 확인합니다.

   및 `volume snapshot policy show` 에 대한 자세한 `volume show` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

   스냅샷 정책 및 스냅샷 스케줄을 구성하고 관리하는 방법에 대한 자세한 내용은 을 참조하십시오."데이터 보호"

관련 정보

"데이터 보호"

ONTAP SMB 접합을 포함하는 이전 버전 디렉토리 복원에 대해 알아보세요.

이전 버전을 사용하여 교차점이 포함된 폴더를 복원할 때 유의해야 할 몇 가지 지침이 있습니다.

이전 버전을 사용하여 정션 포인트인 하위 폴더가 있는 폴더를 복원할 때 "액세스 거부" 오류로 인해 복구가 실패할 수 있습니다.

복원하려는 폴더에 '-parent' 옵션과 함께 'vol show' 명령을 사용하여 교차점이 있는지 여부를 확인할 수 있습니다. 또한 'vserver security trace' 명령을 사용하여 파일 및 폴더 액세스 문제에 대한 자세한 로그를 생성할 수 있습니다.

관련 정보

NAS 네임스페이스에서 데이터 볼륨 생성 및 관리

SMB 서버 기반 서비스 구축

홈 디렉터리를 관리합니다

ONTAP SMB 서버에서 동적 홈 디렉토리를 활성화하는 방법에 대해 알아보세요.

ONTAP 홈 디렉터리를 사용하면 연결된 사용자와 변수 집합을 기반으로 서로 다른 디렉터리에 매핑되는 SMB 공유를 구성할 수 있습니다. 각 사용자에 대해 별도의 공유를 생성하는 대신 몇 가지 홈 디렉토리 매개 변수를 사용하여 하나의 공유를 구성하여 진입점(공유)과 홈 디렉토리(SVM의 디렉토리) 간의 사용자 관계를 정의할 수 있습니다.

게스트 사용자로 로그인한 사용자는 홈 디렉토리가 없으며 다른 사용자의 홈 디렉토리에 액세스할 수 없습니다. 사용자가 디렉토리에 매핑되는 방식을 결정하는 변수는 네 가지입니다.

- * 공유 이름 *

사용자가 연결하는 공유의 이름입니다. 이 공유에 대한 홈 디렉토리 속성을 설정해야 합니다.

공유 이름에는 다음 동적 이름을 사용할 수 있습니다.

- '%w'(사용자의 Windows 사용자 이름)
- '%d'(사용자의 Windows 도메인 이름)
- '%u'(사용자가 매핑한 UNIX 사용자 이름)공유 이름을 모든 홈 디렉토리에 고유하도록 하려면 공유 이름에 '%w' 또는 '%u' 변수가 포함되어야 합니다. 공유 이름에는 "%d"와 "%w" 변수(예: "%d"/"%w")가 모두 포함될 수 있으며, 공유 이름에는 정적 부분과 변수 부분(예: home_""%w")이 포함될 수 있습니다.

- * 공유 경로 *

  이 경로는 공유에 의해 정의되고 공유 이름 중 하나와 연관되며, SVM의 루트에서 사용자의 전체 홈 디렉토리 경로를 생성하기 위해 각 검색 경로에 추가됩니다. 정적(예: "home"), 동적(예: "%w") 또는 두 가지 조합(예: "eng/%w")일 수 있습니다.

- * 검색 경로 *

  ONTAP에서 홈 디렉토리를 검색하도록 지정하는 SVM 루트의 절대 경로 세트입니다. 명령을 사용하여 검색 경로를 하나 이상 지정할 수 `vserver cifs home-directory search-path add` 있습니다. 여러 개의 검색 경로를 지정하면 ONTAP는 유효한 경로를 찾을 때까지 지정된 순서대로 경로를 시도합니다. 에 대한 자세한 내용은 `vserver cifs home-directory search-path add` "ONTAP 명령 참조입니다"을 참조하십시오.

- * 디렉토리 *

  사용자를 위해 생성한 사용자의 홈 디렉토리입니다. 디렉터리 이름은 일반적으로 사용자의 이름입니다. 검색 경로로 정의된 디렉토리 중 하나에 홈 디렉토리를 생성해야 합니다.

예를 들어, 다음 설정을 고려합니다.

- 사용자: John Smith
- 사용자 도메인: Acme
- 사용자 이름: jsmith
- SVM 이름: vs1
- 홈 디렉토리 공유 이름 #1: home_"%w" - 공유 경로: "%w"
- 홈 디렉토리 공유 이름 #2:"%w" - 공유 경로: "%d/%w"
- 검색 경로 #1:'/vol0home/home'
- 검색 경로 #2:'/vol1home/home'
- 검색 경로 #3:'/vol2home/home'
- 홈 디렉토리: `/vol1home/home/jsmith'

시나리오 1: 사용자가 '\\VS1\home_jsmith'에 연결합니다. 첫 번째 홈 디렉토리 공유 이름과 일치하고 상대 경로 jsmith를 생성합니다. ONTAP는 이제 각 검색 경로를 순서대로 확인하여 jsmith라는 디렉토리를 검색합니다.

- '/vol0home/home/jsmith'가 존재하지 않아 2번 검색경로로 이동함.
- '/vol1home/home/jsmith'가 존재하므로 검색 경로 #3이 확인되지 않고 사용자가 홈 디렉토리에 연결되어 있습니다.

시나리오 2: 사용자가 '\\VS1\jsmith'에 연결합니다. 두 번째 홈 디렉토리 공유 이름과 일치하고 상대 경로 Acme/jsmith를 생성합니다. ONTAP는 이제 각 검색 경로를 순서대로 확인하여 "Acme/jsmith"라는 디렉토리를 검색합니다.

- '/vol0home/home/acme/jsmith'가 존재하지 않고 검색 경로 #2로 이동합니다.
- '/vol1home/home/acme/jsmith'가 존재하지 않고 검색 경로 #3으로 이동합니다.
- '/vol2home/home/acme/jsmith'가 존재하지 않아 홈 디렉토리가 존재하지 않아 연결이 실패합니다.

홈 디렉토리 공유

ONTAP SMB 홈 디렉토리 공유 추가

SMB 홈 디렉토리 기능을 사용하려면 공유 속성에 포함된 홈 디렉토리 속성에 공유를 하나 이상 추가해야 합니다.

이 작업에 대해

'vserver cifs share create' 명령을 사용하여 공유를 생성할 때 홈 디렉토리 공유를 생성하거나 'vserver cifs share modify' 명령을 사용하여 언제든지 기존 공유를 홈 디렉토리 공유로 변경할 수 있습니다.

홈 디렉토리 공유를 생성하려면 공유를 생성하거나 수정할 때 '-share-properties' 옵션에 homeddirectory 값을 포함해야 합니다. 사용자가 홈 디렉토리에 연결할 때 동적으로 확장되는 변수를 사용하여 공유 이름을 지정하고 경로를 공유할 수 있습니다. 경로에서 사용할 수 있는 변수는 각각 Windows 사용자 이름, 도메인 및 매핑된 UNIX 사용자 이름에 해당하는 "%w", "%d" 및 "%u"입니다.

단계

1. 홈 디렉토리 공유 추가: + 'vserver cifs share create -vserver_vserver_name_-share-name_share_name_ -path_path_-share-properties homed디렉토리 [,…]'

   '-vserver"vserver'는 검색 경로를 추가할 SVM(CIFS 지원 스토리지 가상 머신)을 지정합니다.

   '-share-name_share-name_'은 홈 디렉토리 공유 이름을 지정합니다.

   공유 이름에 리터럴 문자열 '%w', '%u' 또는 '%d' 중 하나가 포함된 경우 필수 변수 중 하나가 포함된 것 외에도 ONTAP가 리터럴 문자열을 변수(예: "%%w")로 취급하지 않도록 리터럴 문자열 앞에 %(percent) 문자를 입력해야 합니다.

   - 공유 이름에는 '%w' 또는 '%u' 변수가 포함되어야 합니다.
   - 공유 이름에는 "%d" 변수(예: "%d"/"%w") 또는 공유 이름의 정적 부분(예: home1_""%w")이 추가로 포함될 수 있습니다.
   - 관리자가 공유를 사용하여 다른 사용자의 홈 디렉토리에 연결하거나 사용자가 다른 사용자의 홈 디렉토리에 연결할 수 있도록 허용하는 경우 동적 공유 이름 패턴 앞에는 물결표(~)가 와야 합니다.

     vserver cifs home-directory modify는 '-is-home-dirs-access-for-admin-enabled' 옵션을 true로 설정하거나 고급 옵션 '-is-home-dirs-access-for-public-enabled'를 true로 설정하여 이 액세스를 활성화하는 데 사용됩니다.

   path는 홈 디렉토리의 상대 경로를 지정합니다.

'-share-properties homed디렉토리[,…]'는 해당 공유의 공유 속성을 지정합니다. homedir 값을 지정해야 합니다.

쉼표로 구분된 목록을 사용하여 추가 공유 속성을 지정할 수 있습니다.

1. 'vserver cifs share show' 명령을 사용하여 홈 디렉토리 공유를 성공적으로 추가했는지 확인하십시오.

예

다음 명령을 실행하면 "%w"라는 홈 디렉토리 공유가 생성됩니다. oplocks, browable, changenotify 공유 속성은 homedir 공유 속성을 설정하는 것 외에도 설정됩니다.

이 예에서는 SVM의 모든 공유에 대한 출력을 표시하지 않습니다. 출력이 잘립니다.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver     Share     Path          Properties      Comment  ACL
----------- -------- ------------ -------------- -------- -----------
vs1         %w        %w            oplocks         -        Everyone / Full
Control
                                  browsable
                                  changenotify
                                  homedirectory
```

관련 정보

- 홈 디렉토리 검색 경로 추가
- 서버에서 자동 노드 참조를 사용하기 위한 요구 사항 및 지침
- 사용자 홈 디렉토리에 대한 접근성 관리

홈 디렉토리 공유에 대한 고유한 **ONTAP SMB** 사용자 이름 요구 사항에 대해 알아보세요.

공유를 동적으로 생성하려면 "%w"(Windows 사용자 이름) 또는 "%u"(UNIX 사용자 이름) 변수를 사용하여 홈 디렉토리 공유를 생성할 때 고유한 사용자 이름을 지정해야 합니다. 공유 이름이 사용자 이름에 매핑됩니다.

정적 공유 이름과 사용자 이름이 같을 때 다음 두 가지 문제가 발생할 수 있습니다.

- 사용자가 net view 명령을 사용하여 클러스터의 공유를 나열하면 동일한 사용자 이름의 공유 두 개가 표시됩니다.
- 사용자가 해당 공유 이름에 연결하면 사용자는 항상 정적 공유에 연결되어 있으며 동일한 이름으로 홈 디렉토리 공유에 액세스할 수 없습니다.

예를 들어 "administrator"라는 이름의 공유가 있고 "administrator" Windows 사용자 이름이 있습니다. 홈 디렉토리 공유를 만들고 해당 공유에 연결하면 ""administrator"" 홈 디렉토리 공유가 아니라 ""administrator"" 정적 공유에 연결됩니다.

다음 단계를 수행하여 중복된 공유 이름으로 문제를 해결할 수 있습니다.

- 사용자의 홈 디렉토리 공유와 더 이상 충돌하지 않도록 정적 공유의 이름을 바꿉니다.

- 사용자에게 더 이상 정적 공유 이름과 충돌하지 않도록 새 사용자 이름을 제공합니다.
- '%w' 매개 변수를 사용하는 대신 ""home""과 같은 정적 이름으로 CIFS 홈 디렉토리 공유를 생성하여 공유 이름과 충돌하지 않도록 합니다.

업그레이드 후 정적 **ONTAP SMB** 홈 디렉토리 공유 이름에 어떤 일이 발생하는지 알아보세요**.**

홈 디렉토리 공유 이름에는 "%w" 또는 "%u" 동적 변수가 포함되어야 합니다. 새로운 요구 사항으로 ONTAP 버전으로 업그레이드한 후 기존 정적 홈 디렉토리 공유 이름에 어떤 일이 발생할지 알고 있어야 합니다.

홈 디렉토리 구성에 정적 공유 이름이 포함되어 있고 ONTAP로 업그레이드하면 정적 홈 디렉토리 공유 이름이 변경되지 않으며 여전히 유효합니다. 그러나 "%w" 또는 "%u" 변수를 포함하지 않는 새 홈 디렉토리 공유는 생성할 수 없습니다.

이러한 변수 중 하나를 사용자의 홈 디렉토리 공유 이름에 포함하도록 요구하면 모든 공유 이름이 홈 디렉토리 구성에서 고유하도록 할 수 있습니다. 필요한 경우 정적 홈 디렉토리 공유 이름을 "%w" 또는 "%u" 변수가 포함된 이름으로 변경할 수 있습니다.

ONTAP SMB 홈 디렉토리 검색 경로 추가

ONTAP SMB 홈 디렉토리를 사용하려면 하나 이상의 홈 디렉토리 검색 경로를 추가해야 합니다.

이 작업에 대해

'vserver cifs home-directory search-path add' 명령을 사용하여 홈 디렉토리 검색 경로를 추가할 수 있습니다.

'vserver cifs home-directory search-path add' 명령은 명령 실행 중에 '-path' 옵션에 지정된 경로를 확인합니다. 지정한 경로가 없으면 명령을 실행하면 계속할 것인지 여부를 묻는 메시지가 생성됩니다. 당신은 'y'나 'n'을 선택합니다. 계속하려면 y를 선택하면 ONTAP가 검색 경로를 생성합니다. 그러나 홈 디렉토리 구성에서 검색 경로를 사용하려면 먼저 디렉토리 구조를 만들어야 합니다. 계속하지 않도록 선택하면 명령이 실패하고 검색 경로가 생성되지 않습니다. 그런 다음 경로 디렉토리 구조를 생성하고 'vserver cifs home-directory search-path add' 명령을 다시 실행할 수 있습니다.

단계

1. 홈 디렉토리 검색 경로 'vserver cifs home-directory search-path add-vserver vserver-path path path' 추가
2. 'vserver cifs home-directory search-path show' 명령을 사용하여 검색 경로를 성공적으로 추가했는지 확인합니다.

예

다음 예에서는 SVM VS1 홈 디렉토리 구성에 경로 '/home1'을 추가합니다.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

다음 예에서는 SVM VS1 홈 디렉토리 구성에 경로 '/home2'를 추가하려고 합니다. 경로가 존재하지 않습니다. 계속하지 않도록 선택할 수 있습니다.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

관련 정보

홈 디렉토리 공유 추가

%w 및 **%d** 변수를 사용하여 **ONTAP SMB** 홈 디렉토리 구성을 만듭니다.

"%w" 및 "%d" 변수를 사용하여 홈 디렉토리 설정을 작성할 수 있습니다. 사용자는 동적으로 생성된 공유를 사용하여 홈 공유에 연결할 수 있습니다.

단계

1. 사용자의 홈 디렉토리를 포함할 qtree를 생성합니다: 'volume qtree create-vserver vserver_name-qtree-path qtree_path'
2. qtree가 올바른 보안 유형인 'volume qtree show'를 사용하는지 확인합니다
3. Qtree에서 원하는 보안 스타일을 사용하지 않는 경우 'volume qtree security' 명령을 사용하여 보안 스타일을 변경하십시오.
4. 홈 디렉토리 공유 추가: "vserver cifs share create-vserver vserver-share-name %w-path %d/%w-share-properties homed디렉토리\[,...\]"

   '-vserver"vserver'는 검색 경로를 추가할 SVM(CIFS 지원 스토리지 가상 머신)을 지정합니다.

   '-share-name '%w'는 홈 디렉토리 공유 이름을 지정합니다. ONTAP는 각 사용자가 홈 디렉토리에 접속할 때 동적으로 공유 이름을 생성합니다. 공유 이름은 *WINDOWS_USER_NAME* 형식입니다.

   '-path '%d/%w'는 홈 디렉토리의 상대 경로를 지정합니다. 상대 경로는 각 사용자가 자신의 홈 디렉토리에 접속할 때 동적으로 생성되며 *domain/windows_user_name* 형식이 됩니다.

   '-share-properties homed디렉토리 [,…]+'는 해당 공유의 공유 속성을 지정합니다. homedir 값을 지정해야 합니다. 쉼표로 구분된 목록을 사용하여 추가 공유 속성을 지정할 수 있습니다.
5. 'vserver cifs share show' 명령을 사용하여 공유에 원하는 구성이 있는지 확인합니다.
6. 홈 디렉토리 검색 경로 'vserver cifs home-directory search-path add-vserver vserver-path path path' 추가

   '-vserver_vserver-name_'은 검색 경로를 추가할 CIFS 지원 SVM을 지정합니다.

   '-path_path_'는 검색 경로에 대한 절대 디렉토리 경로를 지정합니다.
7. 'vserver cifs home-directory search-path show' 명령을 사용하여 검색 경로를 성공적으로 추가했는지 확인합니다.
8. 홈 디렉토리가 있는 사용자의 경우 홈 디렉토리를 포함하도록 지정된 qtree 또는 볼륨에 해당 디렉토리를

생성합니다.

예를 들어, '/vol/vol1/users' 경로와 생성할 디렉토리가 mydomain\user1인 사용자 이름으로 qtree를 생성한 경우 '/vol/vol1/users/mydomain/user1' 경로를 사용하여 디렉토리를 생성합니다.

/home1 에 마운트된 ""home1" 볼륨을 생성한 경우 "/home1/mydomain/user1" 경로를 사용하여 디렉토리를 생성합니다.

9. 드라이브를 매핑하거나 UNC 경로를 사용하여 연결하여 사용자가 홈 공유에 성공적으로 연결할 수 있는지 확인합니다.

   예를 들어, mydomain\user1 사용자가 SVM VS1 에 있는 8단계에서 생성한 디렉토리에 연결하려는 경우 user1은 UNC 경로 "\\VS1\user1"을 사용하여 연결됩니다.

예

다음 예제의 명령은 다음과 같은 설정으로 홈 디렉토리 구성을 만듭니다.

- 공유 이름은 %W입니다
- 상대 홈 디렉토리 경로는 %d/%W입니다
- 홈 디렉토리 /home1 을 포함하는 데 사용되는 검색 경로는 NTFS 보안 스타일로 구성된 볼륨입니다.
- SVM VS1 에서 구성이 생성됩니다.

사용자가 Windows 호스트에서 홈 디렉토리에 액세스할 때 이 유형의 홈 디렉토리 구성을 사용할 수 있습니다. 또한 사용자가 Windows 및 UNIX 호스트에서 홈 디렉토리를 액세스할 때 이 유형의 구성을 사용할 수 있으며 파일 시스템 관리자는 Windows 기반 사용자 및 그룹을 사용하여 파일 시스템에 대한 액세스를 제어할 수 있습니다.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

관련 정보

- %u 변수를 사용하여 홈 디렉토리를 구성하십시오
- 추가 홈 디렉토리 구성에 대해 알아보세요
- 사용자 홈 디렉토리 경로에 대한 정보 표시

%u 변수를 사용하여 **ONTAP SMB** 홈 디렉토리 구성

'%w' 변수를 사용하여 공유 이름을 지정하는 홈 디렉토리 구성을 만들 수 있지만 '%u' 변수를 사용하여 홈 디렉토리 공유의 상대 경로를 지정할 수 있습니다. 그런 다음 사용자는 홈 디렉토리의 실제 이름 또는 경로를 인식하지 않고 Windows 사용자 이름을 사용하여 생성된 동적 공유를 사용하여 홈 공유에 연결할 수 있습니다.

단계

1. 사용자의 홈 디렉토리를 포함할 qtree를 생성합니다: 'volume qtree create-vserver vserver_name-qtree-path qtree_path'
2. qtree가 올바른 보안 유형인 'volume qtree show'를 사용하는지 확인합니다
3. Qtree에서 원하는 보안 스타일을 사용하지 않는 경우 'volume qtree security' 명령을 사용하여 보안 스타일을 변경하십시오.
4. 홈 디렉토리 공유 추가: "vserver cifs share create-vserver vserver-share-name%w-path%u-share-properties homed디렉토리,...]"

   '-vserver"vserver'는 검색 경로를 추가할 SVM(CIFS 지원 스토리지 가상 머신)을 지정합니다.

   '-share-name '%w'는 홈 디렉토리 공유 이름을 지정합니다. 공유 이름은 각 사용자가 홈 디렉토리에 접속하고 *windows_user_name* 형식으로 작성될 때 동적으로 생성됩니다.

   ⓘ '-share-name' 옵션에도 '%u' 변수를 사용할 수 있습니다. 이렇게 하면 매핑된 UNIX 사용자 이름을 사용하는 상대 공유 경로가 생성됩니다.

   '-path '%u'는 홈 디렉토리의 상대 경로를 지정합니다. 상대 경로는 각 사용자가 홈 디렉토리에 접속하고 *Mapped_UNIX_USER_NAME* 형식으로 작성될 때 동적으로 생성됩니다.

   ⓘ 이 옵션의 값에는 정적 요소도 포함될 수 있습니다. 예: 'ENG/%u'.

   '-share-properties' + homed디렉토리 \[,…\]+'는 해당 공유의 공유 속성을 지정합니다. homedir 값을 지정해야 합니다. 쉼표로 구분된 목록을 사용하여 추가 공유 속성을 지정할 수 있습니다.

5. 'vserver cifs share show' 명령을 사용하여 공유에 원하는 구성이 있는지 확인합니다.
6. 홈 디렉토리 검색 경로 'vserver cifs home-directory search-path add-vserver vserver-path path path' 추가

   '-vserver"vserver'는 검색 경로를 추가할 CIFS 지원 SVM을 지정합니다.

   path는 검색경로에 대한 절대 디렉토리 경로를 지정합니다.

7. 'vserver cifs home-directory search-path show' 명령을 사용하여 검색 경로를 성공적으로 추가했는지 확인합니다.
8. UNIX 사용자가 없으면 'vserver services UNIX -user create' 명령을 사용하여 UNIX 사용자를 생성합니다.

   ⓘ 사용자를 매핑하기 전에 Windows 사용자 이름을 매핑할 UNIX 사용자 이름이 있어야 합니다.

9. "vserver name-mapping create -vserver vserver_name -direction win -unix -priority integer -pattern windows_user_name -replacement unix_user_name" 명령을 사용하여 UNIX 사용자에 대한 Windows 사용자의 이름 매핑을 생성합니다

   ⓘ Windows 사용자를 UNIX 사용자에게 매핑하는 이름 매핑이 이미 있는 경우 매핑 단계를 수행할 필요가 없습니다.

   Windows 사용자 이름이 해당 UNIX 사용자 이름으로 매핑됩니다. Windows 사용자가 홈 디렉토리 공유에 접속하면 디렉토리 이름이 UNIX 사용자 이름과 일치한다는 것을 인식하지 않고 동적으로 생성된 홈 디렉토리에 Windows 사용자 이름에 해당하는 공유 이름을 연결합니다.

10. 홈 디렉토리가 있는 사용자의 경우 홈 디렉토리를 포함하도록 지정된 qtree 또는 볼륨에 해당 디렉토리를 생성합니다.

    예를 들어, 생성하려는 디렉토리가 ""unixuser1""인 사용자의 매핑된 UNIX 사용자 이름과 함께 "/vol/vol1/users" 경로를 사용하여 qtree를 생성한 경우 "/vol/vol1/users/unixuser1" 경로를 사용하여 디렉토리를 생성할 수 있습니다.

    /home1 에 마운트된 ""home1" 볼륨을 생성한 경우 "/home1/unixuser1" 경로를 사용하여 디렉토리를 생성합니다.

11. 드라이브를 매핑하거나 UNC 경로를 사용하여 연결하여 사용자가 홈 공유에 성공적으로 연결할 수 있는지 확인합니다.

    예를 들어, 사용자 mydomain\user1이 UNIX 사용자 unixuser1에 매핑되고 SVM VS1에 있는 10단계에서 생성한 디렉토리에 연결하려는 경우 user1은 UNC 경로 "\\VS1\user1"을 사용하여 연결됩니다.

예

다음 예제의 명령은 다음과 같은 설정으로 홈 디렉토리 구성을 만듭니다.

- 공유 이름은 %W입니다
- 상대 홈 디렉토리 경로는 %u입니다
- 홈 디렉토리 /home1 을 포함하는 데 사용되는 검색 경로는 UNIX 보안 스타일로 구성된 볼륨입니다.
- SVM VS1 에서 구성이 생성됩니다.

사용자가 Windows 호스트 또는 Windows 및 UNIX 호스트 모두에서 홈 디렉토리에 액세스할 때 이 유형의 홈 디렉토리 구성을 사용할 수 있으며 파일 시스템 관리자는 UNIX 기반 사용자 및 그룹을 사용하여 파일 시스템에 대한 액세스를 제어할 수 있습니다.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
              Share Properties: oplocks
                                browsable
                                changenotify
                                homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                                Replacement: unixuser1
```

관련 정보

- %w 및 %d 변수를 사용하여 홈 디렉토리 구성을 만듭니다.
- 추가 홈 디렉토리 구성에 대해 알아보세요
- 사용자 홈 디렉토리 경로에 대한 정보 표시

추가 **ONTAP SMB** 홈 디렉토리 구성에 대해 알아보세요

"%w", "%d", "%u" 변수를 사용하여 홈 디렉토리 설정을 추가로 생성할 수 있습니다. 이 변수를 사용하여 필요에 맞게 홈 디렉토리 구성을 사용자 정의할 수 있습니다.

공유 이름과 검색 경로에서 변수와 정적 문자열을 조합하여 여러 홈 디렉토리 구성을 만들 수 있습니다. 다음 표에는 여러 가지 홈 디렉토리 구성을 만드는 방법을 보여 주는 몇 가지 예가 나와 있습니다.

'/vol1/user'가 홈 디렉토리를 포함할 때 생성되는 경로...	공유 명령...
사용자를 '/vol1/user/win_username'으로 안내하는 공유 경로 '\\vs1\~win_username'을 만듭니다	'vserver cifs share create-share-name~%w-path%w-share-properties oplocks, browable, changenotify, homedir'
사용자를 '/vol1/user/domain/win_username'으로 안내하는 공유 경로 '\\vs1\win_username'을 만듭니다	'vserver cifs share create-share-name %w-path %d/%w-share-properties oplocks, browable, changenotify, homedir'
사용자를 '/vol1/user/unix_username'으로 안내하는 공유 경로 '\\vs1\win_username'을 만듭니다	'vserver cifs share create-share-name %w-path %u-share-properties oplocks, browable, changenotify, homedir'
사용자를 '/vol1/user/unix_username'으로 안내하는 공유 경로 '\\vs1\unix_username'을 생성합니다	'vserver cifs share create-share-name %u-path %u-share-properties oplocks, browable, changenotify, homedir'

SMB 검색 경로를 관리하기 위한 **ONTAP** 명령

SMB 홈 디렉토리 구성을 위한 검색 경로를 관리하기 위한 특정 ONTAP 명령이 있습니다. 예를 들어, 검색 경로에 대한 정보를 추가, 제거 및 표시하는 명령이 있습니다. 검색 경로 순서를 변경하는 명령도 있습니다.

원하는 작업	이 명령 사용...
검색 경로를 추가합니다	'vserver cifs home-directory search-path add'
검색 경로를 표시합니다	'vserver cifs home-directory search-path show'
검색 경로 순서를 변경합니다	'vserver cifs home-directory search-path reorder'
검색 경로를 제거합니다	'vserver cifs home-directory search-path remove'

에 대한 자세한 내용은 `vserver cifs home-directory search-path` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SMB 사용자 홈 디렉토리 경로에 대한 정보 표시

스토리지 가상 시스템(SVM)에 SMB 사용자의 홈 디렉토리 경로를 표시할 수 있습니다. SVM은

CIFS 홈 디렉토리 경로가 여러 개 구성되어 있고 사용자의 홈 디렉토리가 있는 경로를 확인하려는 경우에 사용할 수 있습니다.

단계

1. 'vserver cifs home-directory show-user' 명령을 사용하여 홈 디렉토리 경로를 표시합니다.

   'vserver cifs home-directory show-user-vserver vs1-username user1'

```
Vserver      User                 Home Dir Path
-----------  -------------------  ----------------------
vs1          user1                /home/user1
```

관련 정보

사용자 홈 디렉토리에 대한 접근성 관리

ONTAP SMB 사용자 홈 디렉토리에 대한 접근성 관리

기본적으로 사용자의 홈 디렉토리는 해당 사용자만 액세스할 수 있습니다. 공유의 동적 이름 앞에 물결표(~)가 있는 공유의 경우 Windows 관리자 또는 다른 사용자(공용 액세스)가 사용자의 홈 디렉토리에 대한 액세스를 설정하거나 해제할 수 있습니다.

시작하기 전에

SVM(스토리지 가상 머신)의 홈 디렉토리 공유는 앞에 물결표(~)가 오는 동적 공유 이름으로 구성해야 합니다. 다음 사례는 공유 명명 요구 사항을 보여 줍니다.

홈 디렉토리 공유 이름입니다	공유에 연결하는 명령의 예
~ %d~ %w	'net use * {백슬래시} {백슬래시}IPaddress{백슬래시} ~domain~user/u:credentials'을 사용하십시오
~ %w	'net use * {백슬래시} {백슬래시}IPaddress{백슬래시} ~user/u:credentials'를 사용하십시오
~abc~ %w	'net use * {백슬래시} {백슬래시}IPaddress{ 백슬래시}abc~user/u:credentials'를 사용하십시오

단계

1. 적절한 작업을 수행합니다.

사용자의 홈 디렉토리에 대한 액세스를 설정하거나 해제하려면...	다음을 입력하십시오.
Windows 관리자	'vserver cifs home-directory modify -vserver_vserver_name_-is-home-dirs-access-for -admin-enabled{true|false}' 기본값은 'true'입니다.

사용자의 홈 디렉토리에 대한 액세스를 설정하거나 해제하려면...	다음을 입력하십시오.
모든 사용자(공용 액세스)	a. 권한 수준을 advanced:+'et-Privilege advanced로 설정합니다 b. 액세스 설정 또는 해제:'vserver cifs home-directory modify -vserver_vserver_name_-is -home-dirs-access-for-public-enabled{true

다음 예에서는 사용자의 홈 디렉토리에 대한 공용 액세스를 활성화합니다. + 'Set-Privilege advanced' + 'vserver cifs home-directory modify -vserver vs1-is-home-dirs-access-for-public-enabled true' + 'Set-Privilege admin'

관련 정보

사용자 홈 디렉토리 경로에 대한 정보 표시

UNIX 심볼 링크에 대한 SMB 클라이언트 액세스를 구성합니다

ONTAP SMB 클라이언트가 UNIX 심볼릭 링크에 액세스할 수 있도록 하는 방법에 대해 알아보세요.

심볼 링크는 다른 파일 또는 디렉토리에 대한 참조가 포함된 UNIX 환경에서 생성되는 파일입니다. 클라이언트가 심볼 링크에 액세스하는 경우 클라이언트는 심볼 링크가 참조하는 타겟 파일 또는 디렉토리로 리디렉션됩니다. ONTAP는 Wwidelink(로컬 파일 시스템 외부의 타겟을 포함한 절대 링크)를 포함하여 상대 및 절대 심볼 링크를 지원합니다.

ONTAP는 SMB 클라이언트가 SVM에 구성된 UNIX 심볼 링크를 따라갈 수 있도록 지원합니다. 이 기능은 선택 사항이며 다음 설정 중 하나로 'vserver cifs share create' 명령의 '-symlink-properties' 옵션을 사용하여 공유별로 구성할 수 있습니다.

- 읽기/쓰기 권한으로 설정됩니다
- 읽기 전용 액세스를 사용하도록 설정되었습니다
- SMB 클라이언트에서 심볼 링크를 숨겨 사용할 수 없습니다
- SMB 클라이언트의 심볼 링크에 대한 액세스 없이 비활성화됩니다

공유에 대한 심볼 링크를 설정하면 추가 구성 없이 상대 심볼 링크가 작동합니다.

공유에 대한 심볼 링크를 설정하면 절대 심볼 링크가 즉시 작동하지 않습니다. 먼저 대상 SMB 경로에 대한 심볼 링크의 UNIX 경로 간에 매핑을 생성해야 합니다. 절대 심볼 링크 매핑을 생성할 때 로컬 링크인지 또는 _wwidelink_인지를 지정할 수 있습니다. widelink는 다른 스토리지 디바이스의 파일 시스템에 대한 링크이거나 동일한 ONTAP 시스템에서 별도의 SVM에 호스팅된 파일 시스템에 대한 링크일 수 있습니다. widelink를 만들 때는 클라이언트가 따라야 하는 정보를 포함해야 합니다. 즉, 클라이언트가 디렉터리 연결 지점을 검색할 재분석 지점을 만들어야 합니다. 로컬 공유 외부에 있는 파일 또는 디렉토리에 대한 절대 심볼 링크를 생성하지만 인접성을 로컬로 설정하면 ONTAP는 타겟에 대한 액세스를 허용하지 않습니다.

> 클라이언트가 로컬 심볼 링크(절대 또는 상대 링크)를 삭제하려고 하면 타겟 파일이나 디렉토리가 아닌 심볼 링크만 삭제됩니다. 그러나 클라이언트가 widelink를 삭제하려고 하면 wwidelink가 참조하는 실제 타겟 파일이나 디렉토리가 삭제될 수 있습니다. 클라이언트가 SVM 외부에서 타겟 파일 또는 디렉토리를 명시적으로 열고 삭제할 수 있기 때문에 ONTAP에서는 이 기능을 제어할 수 없습니다.

- * 재분석 지점 및 ONTAP 파일 시스템 서비스 *

  reparse point_는 파일과 함께 볼륨에 선택적으로 저장할 수 있는 NTFS 파일 시스템 객체입니다. 재분석 지점은 SMB 클라이언트가 NTFS 스타일 볼륨으로 작업할 때 향상된 파일 시스템 서비스 또는 확장된 파일 시스템 서비스를 받을 수 있는 기능을 제공합니다. 재분석 지점은 재분석 지점의 유형을 식별하는 표준 태그 및 클라이언트가 추가 처리를 위해 SMB 클라이언트에서 검색할 수 있는 재분석 지점의 콘텐츠로 구성됩니다. 확장된 파일 시스템 기능에 사용할 수 있는 개체 유형 중 ONTAP는 재분석 포인트 태그를 사용하여 NTFS 심볼 링크 및 디렉터리 연결 지점에 대한 지원을 구현합니다. 재분석 지점의 내용을 이해할 수 없는 SMB 클라이언트는 단순히 무시하며 재분석 지점에서 활성화할 수 있는 확장 파일 시스템 서비스를 제공하지 않습니다.

- * 심볼 링크에 대한 디렉터리 교차점 및 ONTAP 지원 *

  디렉토리 교차점은 파일이 저장된 대체 위치를 다른 경로(심볼 링크) 또는 별도의 스토리지 디바이스(widelinks)에 참조할 수 있는 파일 시스템 디렉토리 구조 내의 위치입니다. ONTAP SMB 서버는 디렉터리 연결 지점을 재분석 지점으로 Windows 클라이언트에 노출하므로, 디렉토리 연결 지점을 이동할 때 사용 가능한 클라이언트가 ONTAP에서 재분석 지점 내용을 가져올 수 있습니다. 따라서 동일한 파일 시스템에 포함된 것처럼 다른 경로 또는 스토리지 디바이스를 탐색하고 연결할 수 있습니다.

- * 재분석 포인트 옵션을 사용하여 widelink 지원 활성화 *

  이 `-is-use-junctions-as-reparse-points-enabled` 옵션은 ONTAP 9에서 기본적으로 활성화되어 있습니다. 모든 SMB 클라이언트가 와이드링크를 지원하지는 않으므로, 정보 활성화 옵션은 프로토콜 버전별로 구성 가능합니다. 이를 통해 관리자는 지원되는 SMB 클라이언트와 지원되지 않는 SMB 클라이언트를 모두 지원할 수 있습니다. 이 옵션을 활성화해야 합니다. `-widelink-as-reparse-point-versions` 와이드링크를 사용하여 공유에 액세스하는 각 클라이언트 프로토콜의 경우 기본값은 SMB1입니다.

관련 정보

- "Windows 백업 애플리케이션 및 Unix 스타일 symlink"
- "Microsoft 설명서: 지점 재분석"

ONTAP SMB 액세스를 위한 **UNIX** 심볼릭 링크 구성 시 제한 사항

SMB 액세스를 위해 UNIX 심볼 링크를 구성할 때 특정 제한 사항을 알고 있어야 합니다.

제한	설명
45	CIFS 서버 이름에 FQDN을 사용할 때 지정할 수 있는 CIFS 서버 이름의 최대 길이입니다. 또는 CIFS 서버 이름을 NetBIOS 이름으로 지정할 수 있습니다. 이 이름은 15자로 제한됩니다.
80	공유 이름의 최대 길이입니다.

제한	설명
256	심볼 링크를 생성할 때 또는 기존 심볼 링크의 UNIX 경로를 수정할 때 지정할 수 있는 UNIX 경로의 최대 길이입니다. UNIX 경로는 ""/"(슬래시)로 시작하고 ""/""로 끝나야 합니다. 시작 및 끝 슬래시는 모두 256자 제한의 일부로 계산됩니다.
256	심볼 링크를 생성하거나 기존 심볼 링크의 CIFS 경로를 수정할 때 지정할 수 있는 CIFS 경로의 최대 길이입니다. CIFS 경로는 ""/"(슬래시)로 시작하고 ""/""로 끝나야 합니다. 시작 및 끝 슬래시는 모두 256자 제한의 일부로 계산됩니다.

관련 정보

공유에 대한 심볼릭 링크 매핑 만들기

ONTAP SMB 서버에서 자동 **DFS** 광고 제어

CIFS 서버 옵션은 공유에 연결할 때 SMB 클라이언트에 DFS 기능을 알리는 방법을 제어합니다. ONTAP는 클라이언트가 SMB를 통해 심볼 링크에 액세스할 때 DFS 조회를 사용하므로 이 옵션을 비활성화하거나 활성화할 때 어떤 영향이 있는지 알고 있어야 합니다.

CIFS 서버 옵션은 CIFS 서버가 SMB 클라이언트에 DFS를 사용할 수 있음을 자동으로 알리는지 여부를 결정합니다. 기본적으로 이 옵션은 설정되어 있으며 CIFS 서버는 심볼 링크에 대한 액세스가 비활성화된 공유에 연결할 때도 SMB 클라이언트에 DFS를 사용할 수 있다고 항상 알립니다. CIFS 서버가 심볼 링크에 대한 액세스가 설정된 공유에 연결할 때만 DFS를 클라이언트에 제공할 수 있음을 알리려면 이 옵션을 사용하지 않도록 설정할 수 있습니다.

이 옵션을 비활성화하면 어떻게 되는지 알고 있어야 합니다.

- 심볼 링크에 대한 공유 구성은 변경되지 않습니다.
- 공유 매개 변수가 심볼 링크 액세스를 허용하도록 설정된 경우(읽기-쓰기 액세스 또는 읽기 전용 액세스) CIFS 서버는 해당 공유에 접속하는 클라이언트에 DFS 기능을 알립니다.

  클라이언트 연결 및 심볼 링크에 대한 액세스는 중단 없이 계속됩니다.

- 공유 매개 변수가 액세스를 비활성화하거나 공유 매개 변수의 값이 null인 경우 심볼 링크 액세스를 허용하지 않도록 설정된 경우 CIFS 서버는 해당 공유에 접속하는 클라이언트에 DFS 기능을 알리지 않습니다.

  클라이언트는 CIFS 서버가 DFS를 사용할 수 있고 더 이상 DFS를 광고하지 않기 때문에 심볼 링크 액세스가 비활성화된 공유에 접속된 클라이언트는 CIFS 서버 옵션을 비활성화한 후 이러한 공유에 액세스하지 못할 수 있습니다. 이 옵션을 사용하지 않도록 설정한 후 이러한 공유에 연결된 클라이언트를 재부팅해야 캐시된 정보가 지워질 수 있습니다.

이러한 변경 사항은 SMB 1.0 연결에는 적용되지 않습니다.

ONTAP SMB 공유에서 **UNIX** 심볼릭 링크 지원 구성

SMB 공유를 생성할 때 또는 언제든지 기존 SMB 공유를 수정하여 심볼 링크 공유 속성 설정을

지정하여 SMB 공유에 대한 UNIX 심볼 링크 지원을 구성할 수 있습니다. UNIX 심볼 링크 지원은 기본적으로 활성화되어 있습니다. 공유에서 UNIX 심볼 링크 지원을 해제할 수도 있습니다.

이 작업에 대해

SMB 공유에 대한 UNIX 심볼 링크 지원을 구성할 때 다음 설정 중 하나를 선택할 수 있습니다.

설정	설명
'enable'(사용되지 않음 *)	심볼 링크가 읽기-쓰기 액세스를 사용하도록 설정되도록 지정합니다.
READ_OVERY'(사용되지 않음 *)	읽기 전용 액세스를 위해 symlink를 사용하도록 지정합니다. 이 설정은 Wodelink에는 적용되지 않습니다. Widelink 액세스는 항상 읽기-쓰기입니다.
'hide'(사용되지 않음 *)	SMB 클라이언트가 symlink를 볼 수 없도록 지정합니다.
엄정한 보안 없음	클라이언트가 공유 경계 외부의 symlink를 따르도록 지정합니다.
'체조'입니다	symlink가 읽기-쓰기 액세스를 위해 로컬로 설정되도록 지정합니다. CIFS 옵션 is-advertise-DFS-enabled가 true로 설정되어 있어도 DFS 광고는 생성되지 않습니다. 기본 설정입니다.
'체임링크', '와이델링크'	읽기-쓰기 액세스를 위해 로컬 symlink와 wizelink를 모두 지정합니다. CIFS 옵션 is-advertise-DFS-enabled가 false로 설정되어 있어도 로컬 symlink와 Wipelink 모두에 대해 DFS 광고가 생성됩니다.
"할 수 없습니다	symlinks 및 widelinks를 사용하지 않도록 지정합니다. CIFS 옵션 is-advertise-DFS-enabled가 true로 설정되어 있어도 DFS 광고는 생성되지 않습니다.
""(null, 설정되지 않음)	공유의 심볼 링크를 해제합니다.
'-'(설정되지 않음)	공유의 심볼 링크를 해제합니다.

- enable_, *hide* 및 _read-only_parameters는 더 이상 사용되지 않으며 ONTAP의 향후 릴리스에서 제거될 수 있습니다.

단계

1. 심볼 링크 지원을 구성하거나 사용하지 않도록 설정:

만약...	입력...
새로운 SMB 공유	'+vserver cifs share create-vserver vserver_name-share-name share-path-path-symlink-properties{enable
hide	read-only
""	-
symlinks	symlinks-and-wdelink
disable},…]+'	기존 SMB 공유입니다
'+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink -properties{enable	hide
read-only	"
-	symlinks
symlinks-and-wifelink	disable},…]+'

2. SMB 공유 구성이 올바른지 확인합니다. 'vserver cifs share show -vserver vserver_name -share-name share_name -instance'

예

다음 명령을 실행하면 UNIX 심볼 링크 구성이 "enable"로 설정된 "data1"이라는 SMB 공유가 생성됩니다.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: -
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

관련 정보

공유에 대한 심볼릭 링크 매핑 만들기

ONTAP SMB 공유에 대한 심볼릭 링크 매핑 만들기

SMB 공유에 대한 UNIX 심볼 링크 매핑을 생성할 수 있습니다. 상위 폴더에 상대적인 파일이나 폴더를 참조하는 상대 심볼 링크를 만들거나 절대 경로를 사용하여 파일 또는 폴더를 참조하는 절대 심볼 링크를 만들 수 있습니다.

이 작업에 대해

SMB 2.x를 사용하는 경우 Mac OS X 클라이언트에서 Widelink에 액세스할 수 없습니다 사용자가 Mac OS X 클라이언트의 widelink를 사용하여 공유에 연결하려고 하면 시도가 실패합니다. 그러나 SMB 1을 사용하는 경우 Mac OS X 클라이언트에서 Wistelink를 사용할 수 있습니다.

단계

1. SMB 공유에 대한 심볼 링크 매핑을 생성하려면 다음을 수행합니다. "vserver cifs symlink create -vserver virtual_server_name -unix-path path path path -share-name share_name -cifs-path path path path[-cifs-server server_name][-locality{local|free|wdelink}][-home-directory{true|false}]"

   '-vserver"virtual_server_name'은 SVM(Storage Virtual Machine) 이름을 지정합니다.

'-unix-path' path는 UNIX 경로를 지정합니다. UNIX 경로는 슬래시("/")로 시작해야 하며 슬래시("/")로 끝나야 합니다.

'-share-name"share_name'은 매핑할 SMB 공유의 이름을 지정합니다.

'-cifs-path' path는 CIFS 경로를 지정합니다. CIFS 경로는 슬래시("/")로 시작해야 하며 슬래시("/")로 끝나야 합니다.

'-cifs-server "server_name'은 CIFS 서버 이름을 지정합니다. CIFS 서버 이름은 DNS 이름(예: mynetwork.cifs.server.com), IP 주소 또는 NetBIOS 이름으로 지정할 수 있습니다. NetBIOS 이름은 'vserver cifs show' 명령을 사용하여 확인할 수 있습니다. 이 선택적 매개 변수를 지정하지 않으면 로컬 CIFS 서버의 NetBIOS 이름이 기본값이 됩니다.

``지역성'{'local'|'free'|'wdelink'}은 로컬 링크, 무료 링크 또는 넓은 심볼 링크 생성 여부를 지정합니다. 로컬 심볼 링크는 로컬 SMB 공유에 매핑됩니다. 무료 심볼 링크는 로컬 SMB 서버의 어느 위치에나 매핑할 수 있습니다. 넓은 심볼 링크는 네트워크의 모든 SMB 공유에 매핑됩니다. 이 선택적 매개 변수를 지정하지 않으면 기본값은 "local"입니다.

'-home-directory'{'true'|'false'}는 타겟 공유가 홈 디렉토리인지 여부를 지정합니다. 이 매개 변수는 선택 사항이지만 타겟 공유가 홈 디렉토리로 구성될 때 이 매개 변수를 "true"로 설정해야 합니다. 기본값은 false 입니다.

예

다음 명령을 실행하면 이름이 VS1 인 SVM에 심볼 링크 매핑이 생성됩니다. UNIX 경로인 /src/, SMB 공유 이름 "소스", CIFS 경로, /mycompany/source/", CIFS 서버 IP 주소 123.123.123.123 등이 있으며, 이는 wizelink입니다.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

관련 정보

공유에서 UNIX 심볼릭 링크 지원 구성

SMB 심볼릭 링크 매핑을 관리하기 위한 **ONTAP** 명령

심볼 링크 매핑을 관리하기 위한 특정 ONTAP 명령이 있습니다.

원하는 작업	이 명령 사용...
심볼 링크 매핑을 생성합니다	'vserver cifs symlink create
심볼 링크 매핑에 대한 정보를 표시합니다	'vserver cifs symlink show'
심볼 링크 매핑을 수정합니다	'vserver cifs symlink modify'
심볼 링크 매핑을 삭제합니다	'vserver cifs symlink delete

에 대한 자세한 내용은 `vserver cifs symlink` "ONTAP 명령 참조입니다"을 참조하십시오.

Windows에서 실행 중인 백업 응용 프로그램이 Unix 스타일의 심볼 링크(symlink)를 발견하면 링크가 팔로우되고 데이터가 백업됩니다. ONTAP 9.15.1부터 데이터 대신 symlink를 백업할 수 있습니다. 이 기능은 ONTAP FlexGroup 볼륨과 FlexVols에서 완벽하게 지원됩니다.

개요

Windows 백업 작업 중에 ONTAP가 symlink를 처리하는 방식을 변경하기 전에 이점, 주요 개념 및 구성 옵션을 숙지해야 합니다.

이점

이 기능을 비활성화하거나 사용할 수 없는 경우 각 symlink가 통과하고 링크되는 데이터가 백업됩니다. 이로 인해 불필요한 데이터가 백업될 수 있으며 특정 상황에서는 응용 프로그램이 루프로 끝날 수 있습니다. 대신 symlink를 백업하면 이러한 문제가 발생하지 않습니다. 또한 대부분의 경우 symlink 파일은 데이터에 비해 매우 작기 때문에 백업을 완료하는 데 걸리는 시간이 줄어듭니다. IO 작업이 감소하여 클러스터의 전반적인 성능도 향상됩니다.

Windows 서버 환경

이 기능은 Windows에서 실행되는 백업 응용 프로그램에 대해 지원됩니다. 환경을 사용하기 전에 환경의 기술적 측면을 이해해야 합니다.

확장 속성

Windows는 파일과 선택적으로 연결되는 추가 메타데이터를 집합적으로 형성하는 EA(확장 특성)를 지원합니다. 이러한 속성은 에 설명된 대로 Linux용 Windows 하위 시스템과 같은 다양한 응용 프로그램에서 "WSL에 대한 파일 권한 "사용됩니다. 응용 프로그램은 ONTAP에서 데이터를 읽을 때 각 파일에 대해 확장 속성을 요청할 수 있습니다.

이 기능이 설정되면 symlink가 확장 속성에서 반환됩니다. 따라서 백업 애플리케이션은 메타데이터를 저장하는 데 사용되는 표준 EA 지원을 제공해야 합니다. 일부 Windows 유틸리티는 확장 속성을 지원하고 유지합니다. 그러나 백업 소프트웨어가 확장 속성의 백업 및 복구를 지원하지 않는 경우 각 파일과 연결된 메타데이터가 보존되지 않으며 symlink를 제대로 처리하지 못합니다.

Windows 구성

Microsoft Windows 서버에서 실행되는 백업 응용 프로그램에는 일반 파일 보안을 우회할 수 있는 특별한 권한이 부여될 수 있습니다. 이 작업은 일반적으로 Backup Operators 그룹에 응용 프로그램을 추가하여 수행합니다. 그런 다음 앱은 필요에 따라 파일을 백업 및 복원할 수 있을 뿐만 아니라 다른 관련 시스템 작업을 수행할 수 있습니다. 백업 애플리케이션에서 사용하는 SMB 프로토콜은 ONTAP에서 데이터를 읽고 쓸 때 감지할 수 있는 것처럼 약간만 변경되었습니다.

요구 사항

symlink 백업 기능에는 다음과 같은 몇 가지 요구 사항이 있습니다.

- 클러스터에서 ONTAP 9.15.1 이상이 실행되고 있습니다.
- 특수 백업 권한이 부여된 Windows 백업 응용 프로그램입니다.
- 또한 백업 애플리케이션은 확장 속성을 지원하고 백업 작업 중에 이를 요청해야 합니다.
- ONTAP symlink 백업 기능은 해당 데이터 SVM에 대해 활성화됩니다.

구성 옵션

ONTAP CLI 외에도 REST API를 사용하여 이 기능을 관리할 수 있습니다. 자세한 내용은 을 "ONTAP REST API 및 자동화의 새로운 기능" 참조하십시오. ONTAP가 Unix 스타일 심링크를 처리하는 방식을 결정하는 구성은 SVM별로 별도로 수행해야 합니다.

ONTAP에서 symlink 백업 기능을 활성화합니다

ONTAP 9.15.1을 사용하는 기존 CLI 명령에 구성 옵션이 도입되었습니다. 이 옵션을 사용하여 Unix 스타일의 symlink 처리를 활성화하거나 비활성화할 수 있습니다.

시작하기 전에

기본을 요구 사항검토합니다. 추가 사항:

- CLI 권한을 고급 수준으로 높일 수 있습니다.
- 수정할 데이터 SVM을 결정합니다. SVM `vs1` 은 예 명령에 사용됩니다.

단계

1. advanced 권한 수준을 설정합니다.

```
set privilege advanced
```

2. symlink 파일 백업을 활성화합니다.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

BranchCache를 사용하여 지사에 SMB 공유 콘텐츠를 캐싱합니다

지점 사무실에서 **ONTAP SMB** 공유 콘텐츠를 캐싱하기 위해 **BranchCache**를 사용하는 방법에 대해 알아보세요**.**

BranchCache는 요청 클라이언트에 대한 로컬 컴퓨터의 콘텐츠를 캐싱할 수 있도록 Microsoft에서 개발했습니다. ONTAP의 BranchCache를 구현하면 WAN(Wide Area Network) 사용률을 줄이고, 지사의 사용자가 SMB를 사용하여 SVM(Storage Virtual Machine)에 저장된 콘텐츠에 액세스할 때 액세스 응답 시간을 향상시킬 수 있습니다.

BranchCache를 구성하는 경우 Windows BranchCache 클라이언트는 먼저 SVM에서 콘텐츠를 검색한 다음 지사 내의 컴퓨터에 콘텐츠를 캐시합니다. 지사의 다른 BranchCache 지원 클라이언트가 동일한 컨텐츠를 요청하는 경우 SVM은 먼저 요청된 사용자를 인증하고 권한을 부여합니다. 그런 다음, SVM이 캐시된 콘텐츠가 아직 최신 상태인지 확인하고 최신 상태인 경우 캐시된 콘텐츠에 대한 클라이언트 메타데이터를 보냅니다. 그런 다음 클라이언트는 메타데이터를 사용하여 로컬 기반 캐시에서 콘텐츠를 직접 검색합니다.

관련 정보

오프라인 사용을 위해 파일을 캐싱하는 오프라인 파일 사용에 대해 알아보세요.

ONTAP SMB BranchCache 버전 지원에 대해 알아보세요

ONTAP가 지원하는 BranchCache 버전은 무엇인지 알고 있어야 합니다.

ONTAP는 BranchCache 1 및 향상된 BranchCache 2 를 지원합니다.

- SVM(스토리지 가상 시스템)에 대해 SMB 서버의 BranchCache를 구성할 때 BranchCache 1, BranchCache 2 또는 모든 버전을 사용하도록 설정할 수 있습니다.

  기본적으로 모든 버전이 활성화됩니다.

- BranchCache 2만 사용하도록 설정한 경우 원격 사무소 Windows 클라이언트 시스템은 BranchCache 2를 지원해야 합니다.

  SMB 3.0 이상 클라이언트만 BranchCache 2를 지원합니다.

BranchCache 버전에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

관련 정보

"Microsoft TechNet 라이브러리: technet.microsoft.com/en-us/library/"

ONTAP SMB 네트워크 프로토콜 지원 요구 사항에 대해 알아보세요**.**

ONTAP BranchCache를 구축하기 위한 네트워크 프로토콜 요구 사항을 알고 있어야 합니다.

SMB 2.1 이상을 사용하여 IPv4 및 IPv6 네트워크에서 ONTAP BranchCache 기능을 구현할 수 있습니다.

BranchCache 구축에 사용되는 모든 CIFS 서버 및 지사 시스템에는 SMB 2.1 이상 프로토콜이 설정되어 있어야 합니다. SMB 2.1에는 클라이언트가 BranchCache 환경에 참여할 수 있도록 하는 프로토콜 확장이 있습니다. BranchCache 지원을 제공하는 최소 SMB 프로토콜 버전입니다. SMB 2.1은 BranchCache 버전 1을 지원합니다.

BranchCache 버전 2를 사용하려면 SMB 3.0이 지원되는 최소 버전입니다. BranchCache 2 구축에 사용되는 모든 CIFS 서버 및 지사 시스템에는 SMB 3.0 이상이 활성화되어 있어야 합니다.

일부 클라이언트가 SMB 2.1만 지원하고 일부 클라이언트가 SMB 3.0을 지원하는 원격 사무소가 있는 경우 CIFS 서버에 BranchCache 1과 BranchCache 2를 모두 지원하는 BranchCache 구성을 구현할 수 있습니다.

Microsoft BranchCache 기능은 HTTP/HTTPS 및 SMB 프로토콜을 파일 액세스 프로토콜로 사용하는 것을 지원하지만 ONTAP BranchCache는 SMB의 사용만 지원합니다.

ONTAP SMB 및 **Windows** 호스트 버전 요구 사항에 대해 알아보세요**.**

BranchCache를 구성하려면 ONTAP 및 지점 Windows 호스트가 특정 버전 요구 사항을 충족해야 합니다.

BranchCache를 구성하기 전에 클러스터 및 참여하는 지사 클라이언트의 ONTAP 버전이 SMB 2.1 이상을 지원하고 BranchCache 기능을 지원해야 합니다. Hosted Cache 모드를 구성하는 경우 캐시 서버에 지원되는 호스트를 사용해야 합니다.

BranchCache 1은 다음 ONTAP 버전 및 Windows 호스트에서 지원됩니다.

- 콘텐츠 서버: ONTAP 기반의 SVM(스토리지 가상 시스템
- 캐시 서버: Windows Server 2008 R2 또는 Windows Server 2012 이상
- 피어 또는 클라이언트: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 또는 Windows Server 2012 이상

BranchCache 2는 다음 ONTAP 버전 및 Windows 호스트에서 지원됩니다.

- 콘텐츠 서버: ONTAP 기반의 SVM
- 캐시 서버: Windows Server 2012 이상
- 피어 또는 클라이언트: Windows 8 또는 Windows Server 2012 이상

ONTAP SMB가 **BranchCache** 해시를 무효화하는 이유에 대해 알아보세요**.**

BranchCache 구성을 계획할 때 ONTAP에서 해시를 무효화하는 이유를 이해하는 것이 도움이 될 수 있습니다. 구성할 운영 모드를 결정하는 데 도움이 되며 BranchCache를 활성화할 공유를 선택하는 데 도움이 될 수 있습니다.

ONTAP는 해시가 유효한지 확인하기 위해 BranchCache 해시를 관리해야 합니다. 해시가 유효하지 않은 경우 ONTAP는 해시를 무효화하고 다음에 해당 콘텐츠가 요청될 때 BranchCache가 여전히 활성화되어 있다고 가정하고 새 해시를 계산합니다.

ONTAP는 다음과 같은 이유로 해시를 무효화합니다.

- 서버 키가 수정되었습니다.

  서버 키가 수정되면 ONTAP는 해시 저장소의 모든 해시를 무효화합니다.

- BranchCache 해시 저장소의 최대 크기에 도달했기 때문에 캐시에서 해시가 플러시됩니다.

  이 매개 변수는 조정 가능하며 비즈니스 요구 사항에 맞게 수정할 수 있습니다.

- 파일은 SMB 또는 NFS 액세스를 통해 수정됩니다.
- 해시가 계산된 파일은 'Snap restore' 명령어를 이용하여 복구한다.
- BranchCache를 사용하는 SMB 공유가 포함된 볼륨은 'Snap restore' 명령을 사용하여 복구됩니다.

ONTAP SMB 해시 저장소 위치 선택에 대해 알아보세요

BranchCache를 구성할 때는 해시를 저장할 위치와 해시 저장소의 크기를 선택합니다. 해시 저장소 위치 및 크기를 선택할 때 지침을 이해하면 CIFS 지원 SVM에서 BranchCache 구성을 계획하는 데 도움이 됩니다.

- atime 업데이트가 허용되는 볼륨에서 해시 저장소를 찾아야 합니다.

  해시 파일의 액세스 시간은 자주 액세스하는 파일을 해시 저장소에 유지하는 데 사용됩니다. atime 업데이트가 비활성화된 경우 생성 시간이 이 용도로 사용됩니다. 자주 사용하는 파일을 추적하기 위해 atime을 사용하는 것이 좋습니다.

- SnapMirror 대상 및 SnapLock 볼륨과 같은 읽기 전용 파일 시스템에서는 해시를 저장할 수 없습니다.
- 해시 저장소의 최대 크기에 도달하면 새 해시를 위한 공간을 확보하기 위해 이전 해시가 플러시됩니다.

  해시 저장소의 최대 크기를 늘려 캐시에서 플러시되는 해시의 양을 줄일 수 있습니다.

- 해시를 저장하는 볼륨을 사용할 수 없거나 꽉 찼거나 BranchCache 서비스에서 해시 정보를 검색할 수 없는 클러스터 내 통신에 문제가 있는 경우 BranchCache 서비스를 사용할 수 없습니다.

  볼륨이 오프라인 상태이거나 스토리지 관리자가 해시 저장소에 대한 새 위치를 지정했기 때문에 볼륨을 사용할 수 없습니다.

  이 경우 파일 액세스에 문제가 발생하지 않습니다. 해시 저장소에 대한 액세스가 방해를 받으면 ONTAP는 클라이언트에 Microsoft 정의 오류를 반환하여 클라이언트가 일반 SMB 읽기 요청을 사용하여 파일을 요청하게 합니다.

관련 정보

- 서버에서 BranchCache 구성
- 공유에서 BranchCache 구성 수정

ONTAP SMB BranchCache 권장 사항에 대해 알아보세요

BranchCache를 구성하기 전에 BranchCache 캐싱을 활성화할 SMB 공유를 결정할 때 유의해야 할 몇 가지 권장 사항이 있습니다.

사용할 운영 모드와 BranchCache를 활성화할 SMB 공유를 결정할 때 다음 권장 사항을 염두에 두어야 합니다.

- BranchCache의 이점은 원격으로 캐시되는 데이터의 변경 사항이 자주 변경되는 경우 감소합니다.
- BranchCache 서비스는 여러 원격 사무소 클라이언트에서 다시 사용하거나 단일 원격 사용자가 반복적으로 액세스하는 파일 콘텐츠에 의해 다시 사용되는 파일 콘텐츠를 포함하는 공유에 유용합니다.
- 스냅샷 및 SnapMirror 대상의 데이터와 같은 읽기 전용 콘텐츠에 대해 캐싱을 사용하도록 설정하는 것이 좋습니다.

BranchCache를 구성합니다

ONTAP SMB BranchCache 구성에 대해 알아보세요

ONTAP 명령을 사용하여 SMB 서버에서 BranchCache를 구성합니다. BranchCache를 구현하려면 클라이언트도 구성해야 하며, 콘텐츠를 캐시하려는 지사의 호스팅된 캐시 서버도 선택적으로 구성해야 합니다.

공유 단위로 캐싱을 사용하도록 BranchCache를 구성하는 경우 BranchCache 캐싱 서비스를 제공할 SMB 공유에서 BranchCache를 사용하도록 설정해야 합니다.

ONTAP SMB BranchCache 구성을 위한 요구 사항

몇 가지 필수 구성 요소를 충족한 후 BranchCache를 설정할 수 있습니다.

SVM용 CIFS 서버에서 BranchCache를 구성하기 전에 다음 요구 사항이 충족되어야 합니다.

- ONTAP는 클러스터의 모든 노드에 설치해야 합니다.
- CIFS에 대한 라이센스가 있어야 하며 SMB 서버를 구성해야 합니다. SMB 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오"있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.
- IPv4 또는 IPv6 네트워크 연결을 구성해야 합니다.
- BranchCache 1의 경우 SMB 2.1 이상이 활성화되어 있어야 합니다.
- BranchCache 2의 경우 SMB 3.0을 사용하도록 설정해야 하며 원격 Windows 클라이언트가 BranchCache 2를 지원해야 합니다.

ONTAP SMB 서버에서 **BranchCache** 구성

BranchCache를 구성하여 공유별로 BranchCache 서비스를 제공할 수 있습니다. 또는 BranchCache를 구성하여 모든 SMB 공유에서 캐싱을 자동으로 설정할 수 있습니다.

이 작업에 대해

SVM에서 BranchCache를 구성할 수 있습니다.

- CIFS 서버의 모든 SMB 공유 내에 포함된 모든 콘텐츠에 대해 캐싱 서비스를 제공하려는 경우 모든 공유 BranchCache 구성을 생성할 수 있습니다.
- CIFS 서버에서 선택한 SMB 공유 내에 포함된 콘텐츠에 대해 캐싱 서비스를 제공하려는 경우 공유당 BranchCache 구성을 생성할 수 있습니다.

BranchCache를 구성할 때는 다음 매개 변수를 지정해야 합니다.

필수 매개변수	설명
_SVM 이름 _	BranchCache는 SVM별로 구성됩니다. BranchCache 서비스를 구성할 CIFS 지원 SVM을 지정해야 합니다.
해시 스토어에 대한 경로 _	BranchCache 해시는 SVM 볼륨의 일반 파일에 저장됩니다. ONTAP에서 해시 데이터를 저장할 기존 디렉터리의 경로를 지정해야 합니다. BranchCache 해시 경로는 읽기/쓰기가 가능해야 합니다. 스냅샷 디렉토리와 같은 읽기 전용 경로는 허용되지 않습니다. 해시 데이터는 다른 데이터가 포함된 볼륨에 저장하거나 해시 데이터를 저장하기 위한 별도의 볼륨을 생성할 수 있습니다. SVM이 SVM 재해 복구 소스인 경우 해시 경로가 루트 볼륨에 있을 수 없습니다. 루트 볼륨이 재해 복구 대상에 복제되지 않기 때문입니다. 해시 경로에는 공백과 유효한 파일 이름 문자가 포함될 수 있습니다.

필요에 따라 다음 매개 변수를 지정할 수 있습니다.

선택적 매개 변수입니다	설명
_지원되는 버전 _	ONTAP는 BranchCache 1 및 2를 지원합니다. 버전 1, 버전 2 또는 두 버전을 모두 사용할 수 있습니다. 기본값은 두 버전을 모두 사용하는 것입니다.
_ 해시 저장소의 최대 크기 _	해시 데이터 저장소에 사용할 크기를 지정할 수 있습니다. 해시 데이터가 이 값을 초과하면 ONTAP는 이전 해시를 삭제하여 새 해시를 위한 공간을 만듭니다. 해시 저장소의 기본 크기는 1GB입니다. BranchCache는 해시가 지나치게 공격적인 방식으로 폐기되지 않을 경우 보다 효율적으로 성능을 발휘합니다. 해시 저장소가 꽉 찼기 때문에 해시가 자주 삭제되는 경우 BranchCache 구성을 수정하여 해시 저장소 크기를 늘릴 수 있습니다.
_서버 키 _	BranchCache 서비스가 클라이언트가 BranchCache 서버를 가장하지 못하도록 하는 데 사용하는 서버 키를 지정할 수 있습니다. 서버 키를 지정하지 않으면 BranchCache 구성을 만들 때 서버 키가 임의로 생성됩니다. 여러 서버가 동일한 파일에 BranchCache 데이터를 제공하는 경우 클라이언트는 동일한 서버 키를 사용하는 모든 서버의 해시를 사용할 수 있도록 서버 키를 특정 값으로 설정할 수 있습니다. 서버 키에 공백이 있으면 서버 키를 따옴표로 묶어야 합니다.
_작동 모드 _	기본 설정은 공유별로 BranchCache를 사용하는 것입니다. • BranchCache 구성을 생성하여 공유별로 BranchCache를 사용하도록 설정하려면 이 선택적 매개 변수를 지정하지 않거나 "공유당"을 지정할 수 있습니다. • 모든 공유에서 BranchCache를 자동으로 활성화하려면 운영 모드를 '모든 공유’로 설정해야 합니다.

단계

1. 필요에 따라 SMB 2.1 및 3.0 활성화:
   a. 권한 수준을 Advanced:'Set-Privilege advanced’로 설정합니다
   b. 구성된 SVM SMB 설정을 확인하여 필요한 모든 SMB 버전이 활성화되었는지 확인합니다. 'vserver cifs options show -vserver_vserver_name_'
   c. 필요한 경우 SMB 2.1:'vserver cifs options modify -vserver_vserver_name_-SMB2-enabled true’를 설정합니다

      이 명령을 사용하면 SMB 2.0 및 SMB 2.1이 모두 설정됩니다.

   d. 필요한 경우 SMB 3.0:'vserver cifs options modify -vserver_vserver_name_-SMB3-enabled true’를 설정합니다

e. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

2. BranchCache 구성:'vserver cifs BranchCache create-vserver_name_-hash-store-path path path [-hash-store-max-size{integer[KB|MB|GB|TB|PB]} [-versions{v1-enable|v2-enable|enable-all][-server-key text] -operating-mode{per-share|all-share}}

   지정된 해시 스토리지 경로가 있어야 하며 SVM에서 관리하는 볼륨에 상주해야 합니다. 경로는 읽기 쓰기 가능 볼륨에도 있어야 합니다. 경로가 읽기 전용이거나 존재하지 않으면 명령이 실패합니다.

   SVM BranchCache 구성을 추가할 때 동일한 서버 키를 사용하려면 서버 키에 대해 입력한 값을 기록합니다. BranchCache 구성에 대한 정보를 표시할 때는 서버 키가 나타나지 않습니다.

3. BranchCache 구성이 올바른지 확인합니다. 'vserver cifs BranchCache show -vserver_vserver_name_'

예

다음 명령을 실행하면 SMB 2.1과 3.0이 모두 활성화되어 있고 SVM VS1의 모든 SMB 공유에서 캐싱이 자동으로 활성화되도록 BranchCache가 구성됩니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

다음 명령은 SMB 2.1과 3.0이 모두 활성화되어 있는지 확인하고, SVM VS1 기반 공유별로 캐싱이 가능하도록 BranchCache를 구성하고, BranchCache 구성을 확인합니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

관련 정보

- BranchCache 버전 지원에 대해 알아보세요
- 원격 사무실에서 BranchCache를 구성하는 방법에 대해 알아보세요.
- BranchCache 지원 SMB 공유를 생성합니다
- 기존 공유에서 BranchCache 활성화
- 공유에서 BranchCache 구성 수정
- 공유에서 BranchCache 비활성화에 대해 알아보세요
- 공유에서 BranchCache 구성을 삭제합니다.

ONTAP SMB에서 원격 사무실에서 **BranchCache**를 구성하는 방법에 대해 알아보세요**.**

SMB 서버에서 BranchCache를 구성한 후에는 클라이언트 컴퓨터에 BranchCache를 설치하고 구성해야 하며, 필요에 따라 원격 사무실의 캐싱 서버에 BranchCache를 설치하고 구성해야 합니다. Microsoft는 원격 사무소에서 BranchCache를 구성하는 지침을 제공합니다.

지점 클라이언트 구성 지침 및 BranchCache를 사용할 캐싱 서버(선택 사항)는 Microsoft BranchCache 웹 사이트에 있습니다.

"Microsoft BranchCache 문서: 새로운 기능"

BranchCache 지원 **SMB** 공유를 구성합니다

BranchCache 지원 **ONTAP SMB** 공유 구성에 대해 알아보세요**.**

SMB 서버 및 지사에 BranchCache를 구성한 후에는 지점의 클라이언트가 캐시할 콘텐츠를 포함하는 SMB 공유에서 BranchCache를 사용하도록 설정할 수 있습니다.

BranchCache 캐싱은 SMB 서버의 모든 SMB 공유 또는 공유별로 설정할 수 있습니다.

- 공유별로 BranchCache를 사용하도록 설정한 경우 공유를 생성하거나 기존 공유를 수정하여 BranchCache를 사용하도록 설정할 수 있습니다.

  기존 SMB 공유에서 캐싱을 사용하는 경우 ONTAP는 해당 공유에서 BranchCache를 사용하도록 설정하는 즉시 해시 컴퓨팅을 시작하고 콘텐츠를 요청하는 클라이언트로 메타데이터를 전송합니다.

- 이전에 SMB로 공유에 접속한 클라이언트는 이후에 BranchCache가 해당 공유에 설정된 경우 BranchCache 지원을 받지 못합니다.

  ONTAP는 SMB 세션이 설정된 시간에 공유에 대한 BranchCache 지원을 알립니다. BranchCache를 사용하도록 설정할 때 이미 세션을 설정한 클라이언트는 연결을 끊고 다시 연결하여 이 공유에 캐시된 콘텐츠를 사용해야 합니다.

> ⓘ 이후에 SMB 공유의 BranchCache가 비활성화되면 ONTAP는 요청 클라이언트로 메타데이터 전송을 중지합니다. 데이터가 필요한 클라이언트는 콘텐츠 서버(SMB 서버)에서 직접 검색합니다.

BranchCache 지원 **ONTAP SMB** 공유 생성

공유를 생성할 때 "BranchCache" 공유 속성을 설정하여 SMB 공유에서 BranchCache를 사용하도록 설정할 수 있습니다.

이 작업에 대해

- SMB 공유에 BranchCache가 설정되어 있으면 공유에 수동 캐싱으로 설정된 오프라인 파일 구성이 있어야 합니다.

  공유를 생성할 때 기본 설정입니다.

- BranchCache 사용 공유를 생성할 때 추가 선택적 공유 매개 변수를 지정할 수도 있습니다.
- BranchCache가 SVM(스토리지 가상 시스템)에서 구성 및 설정되지 않은 경우에도 공유에 "BranchCache" 속성을 설정할 수 있습니다.

  그러나 공유 폴더에 캐시된 콘텐츠가 제공되도록 하려면 SVM에서 BranchCache를 구성하고 사용하도록 설정해야 합니다.

- '-share-properties' 매개 변수를 사용할 때 공유에 적용되는 기본 공유 속성이 없으므로 쉼표로 구분된 목록을 사용하여 "BranchCache" 공유 속성 외에도 공유에 적용할 다른 모든 공유 속성을 지정해야 합니다.
- 에 대한 자세한 내용은 `vserver cifs share create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. BranchCache 지원 SMB 공유 생성: + 'vserver CIFS share create -vserver_vserver_name_-share -name_share_name_-path_path_-share-properties BranchCache[,…]'
2. 'vserver cifs share show' 명령을 사용하여 SMB 공유에 BranchCache 공유 속성이 설정되어 있는지 확인합니다.

예

다음 명령을 실행하면 SVM VS1 에서 "/data " 경로를 사용하여 " data " 라는 BranchCache 지원 SMB 공유가 생성됩니다. 기본적으로 오프라인 파일 설정은 '수동'으로 설정됩니다.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
            Share Properties: branchcache
                              oplocks
                              browsable
                              changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

관련 정보

단일 공유에서 BranchCache 비활성화

기존 **ONTAP SMB** 공유에서 **BranchCache** 활성화

기존 공유 속성 목록에 'BranchCache' 공유 속성을 추가하여 기존 SMB 공유에서 BranchCache를 사용하도록 설정할 수 있습니다.

이 작업에 대해

- SMB 공유에 BranchCache가 설정되어 있으면 공유에 수동 캐싱으로 설정된 오프라인 파일 구성이 있어야 합니다.

  기존 공유의 오프라인 파일 설정이 수동 캐싱으로 설정되어 있지 않으면 공유를 수정하여 구성해야 합니다.

- BranchCache가 SVM(스토리지 가상 시스템)에서 구성 및 설정되지 않은 경우에도 공유에 "BranchCache" 속성을 설정할 수 있습니다.

그러나 공유 폴더에 캐시된 콘텐츠가 제공되도록 하려면 SVM에서 BranchCache를 구성하고 사용하도록 설정해야 합니다.

- 공유에 "BranchCache" 공유 속성을 추가하면 기존 공유 설정과 공유 속성이 유지됩니다.

  BranchCache 공유 속성이 기존 공유 속성 목록에 추가됩니다. 에 대한 자세한 내용은 `vserver cifs share properties add` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 필요한 경우 수동 캐싱에 대한 오프라인 파일 공유 설정을 구성합니다.
   a. 'vserver cifs share show' 명령을 사용하여 오프라인 파일 공유 설정을 확인합니다.
   b. 오프라인 파일 공유 설정이 manual로 설정되어 있지 않으면 필요한 값('vserver cifs share modify -vserver vserver_name -share-name share-name share_name -offline-files manual')으로 변경합니다
2. 기존 SMB 공유에서 BranchCache를 사용하도록 설정합니다. 'vserver cifs share properties add-vserver vserver_name -share-name share_name-share-properties BranchCache'
3. SMB 공유에서 BranchCache 공유 속성이 설정되어 있는지 확인합니다. 'vserver cifs share show -vserver vserver_name -share-name share_name'

예

다음 명령을 실행하면 SVM VS1 에서 " data2 " 라는 기존 SMB 공유에서 "/data2 " 경로를 사용하여 BranchCache를 사용할 수 있습니다.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              showsnapshot
                              changenotify
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

관련 정보

- 기존 주식에 주식 속성 추가 또는 제거
- 단일 공유에서 BranchCache 비활성화

BranchCache 구성을 관리하고 모니터링합니다

ONTAP SMB 공유에서 **BranchCache** 구성 수정

해시 저장소 디렉토리 경로 변경, 해시 저장소 최대 디렉토리 크기, 운영 모드 및 지원되는 BranchCache 버전을 포함하여 SVM에서 BranchCache 서비스의 구성을 수정할 수 있습니다. 해시 저장소가 포함된 볼륨의 크기를 늘릴 수도 있습니다.

단계

1. 적절한 작업을 수행합니다.

원하는 작업	다음을 입력하십시오.
해시 저장소 디렉터리 크기를 수정합니다	'vserver cifs BranchCache modify -vserver vserver_name -hash-store -max-size{integer[KB
MB	GB
TB	PB]}'
해시 저장소가 포함된 볼륨의 크기를 늘립니다	``볼륨 크기 - vserver vserver_name - volume volume_name - new-size new_size [k
m	g
t]' 해시 저장소가 포함된 볼륨이 가득 차면 볼륨의 크기를 늘릴 수 있습니다. 새 볼륨 크기를 숫자로 지정한 다음 단위를 지정할 수 있습니다. 에 대해 자세히 알아보십시오 "FlexVol 볼륨 관리"	해시 저장소 디렉터리 경로를 수정합니다

원하는 작업	다음을 입력하십시오.
'vserver cifs BranchCache modify -vserver vserver_name -hash-store-path path -flush -hash{true	false}' SVM이 SVM 재해 복구 소스인 경우 해시 경로가 루트 볼륨에 있을 수 없습니다. 루트 볼륨이 재해 복구 대상에 복제되지 않기 때문입니다. BranchCache 해시 경로에는 공백과 유효한 파일 이름 문자가 포함될 수 있습니다. 해시 경로를 수정할 경우 ONTAP가 원래 해시 저장 위치에서 해시를 플러시할지 여부를 지정하는 필수 매개 변수입니다. '-flush-hash' 파라미터에 대해 다음 값을 설정할 수 있습니다. **"true"**를 지정하면 **ONTAP**는 원래 위치에서 해시를 삭제하고 **BranchCache** 사용 클라이언트가 새 요청을 수행할 때 새 위치에 새 해시를 만듭니다. false를 지정하면 해시가 플러시되지 않습니다. + 이 경우 해시 저장소 경로를 원래 위치로 다시 변경하여 나중에 기존 해시를 다시 사용하도록 선택할 수 있습니다.
작동 모드를 변경합니다	'vserver cifs BranchCache modify -vserver vserver_name -operating-mode{per-share
all-share	disable}' 작동 모드를 수정할 때 다음 사항에 유의해야 합니다. **ONTAP**는 **SMB** 세션이 설정되어 있을 때 공유에 대한 **BranchCache** 지원을 알립니다. BranchCache를 사용하도록 설정할 때 이미 세션을 설정한 클라이언트는 연결을 끊고 다시 연결하여 이 공유에 캐시된 콘텐츠를 사용해야 합니다.
BranchCache 버전 지원을 변경합니다	'vserver cifs BranchCache modify -vserver vserver vserver_name -versions{v1-enable
v2-enable	enable-all}'

2. 'vserver cifs BranchCache show' 명령을 사용하여 구성 변경 사항을 확인합니다.

ONTAP SMB 공유에서 **BranchCache** 구성에 대한 정보 표시

구성을 확인하거나 구성을 수정하기 전에 현재 설정을 확인할 때 사용할 수 있는 SVM(스토리지 가상 머신)에 BranchCache 구성에 대한 정보를 표시할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

를 표시하려면...	이 명령을 입력하십시오...
모든 SVM의 BranchCache 구성에 대한 요약 정보	'vserver cifs BranchCache show'를 선택합니다
특정 SVM의 구성에 대한 자세한 정보	'vserver cifs BranchCache show -vserver_vserver_name_'

예

다음 예에서는 SVM VS1 BranchCache 구성에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
            Supported BranchCache Versions: enable_all
                        Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
          CIFS BranchCache Operating Modes: per_share
```

ONTAP SMB BranchCache 서버 키 변경

SVM(스토리지 가상 시스템)에서 BranchCache 구성을 수정하고 다른 서버 키를 지정하여 BranchCache 서버 키를 변경할 수 있습니다.

이 작업에 대해

여러 서버가 동일한 파일에 BranchCache 데이터를 제공하는 경우 클라이언트는 동일한 서버 키를 사용하는 모든 서버의 해시를 사용할 수 있도록 서버 키를 특정 값으로 설정할 수 있습니다.

서버 키를 변경할 때는 해시 캐시도 플러시해야 합니다. 해시를 플러싱한 후 ONTAP는 BranchCache 사용 클라이언트가 새 요청을 할 때 새 해시를 생성합니다.

단계

1. 'vserver cifs BranchCache modify -vserver vserver_name -server -key text -flush -hash true' 명령을 사용하여 서버 키를 변경합니다

   새 서버 키를 구성할 때는 -flush-hash를 지정하고 값을 true로 설정해야 합니다.

2. 'vserver cifs BranchCache show' 명령을 사용하여 BranchCache 구성이 올바른지 확인합니다.

예

다음 예에서는 공백이 포함된 새 서버 키를 설정하고 SVM VS1 의 해시 캐시를 플러시합니다.

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

관련 정보

ONTAP가 BranchCache 해시를 무효화하는 이유에 대해 알아보세요.

지정된 **ONTAP SMB** 경로에서 **BranchCache** 해시를 미리 계산합니다**.**

BranchCache 서비스를 구성하여 단일 파일, 디렉토리 또는 디렉토리 구조의 모든 파일에 대한 해시를 사전 계산할 수 있습니다. 이 방법은 사용량이 많지 않은 시간 동안 BranchCache 사용 공유의 데이터에 대한 해시를 계산할 때 유용합니다.

이 작업에 대해

해시 통계를 표시하기 전에 데이터 샘플을 수집하려면 '통계 시작' 및 '통계 중지' 옵션 명령을 사용해야 합니다.

- 사전 컴퓨팅 해시를 계산할 스토리지 가상 시스템(SVM)과 경로를 지정해야 합니다.
- 또한 해시를 재귀적으로 계산할 것인지 여부를 지정해야 합니다.
- 해시를 재귀적으로 계산하려는 경우 BranchCache 서비스는 지정된 경로 아래의 전체 디렉토리 트리를 탐색한 다음 각 대상 객체에 대한 해시를 계산합니다.

  자세히 알아보세요 `statistics start` 그리고 `statistics stop` 에서 "ONTAP 명령 참조입니다" .

단계

1. 원하는 대로 사전 계산 해시:

에서 해시를 사전 계산하려는 경우...	명령 입력...
단일 파일 또는 디렉토리입니다	'vserver cifs BranchCache hash-create-vserver vserver_name-path path-recurse false
디렉토리 구조의 모든 파일에 반복적으로 존재합니다	'vserver cifs BranchCache hash-create-vserver vserver_name-path absolute_path-recurse true'

2. '통계' 명령을 사용하여 해시가 계산되는지 확인합니다.

   a. 원하는 SVM 인스턴스에 대한 'hashd' 객체 통계 표시: 'stattisics show-object hashd-instance

vserver_name'

b. 명령을 반복하여 생성된 해시 수가 증가하는지 확인합니다.

에 대한 자세한 내용은 `statistics show` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 예에서는 경로 '/data'와 SVM VS1 의 모든 포함된 파일 및 하위 디렉토리에 해시를 생성합니다.

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

관련 정보

- "성능 모니터링 설정"

ONTAP SMB SVM BranchCache 해시 저장소에서 해시 플러시

SVM(스토리지 가상 머신)의 BranchCache 해시 저장소에서 캐시된 모든 해시를 플러시할 수 있습니다. 지사 BranchCache 구성을 변경한 경우 이 기능이 유용할 수 있습니다. 예를 들어 최근에 분산 캐싱에서 호스팅된 캐싱 모드로 캐싱 모드를 재구성한 경우 해시 저장소를 플러시해야 합니다.

이 작업에 대해

해시를 플러싱한 후 ONTAP는 BranchCache 사용 클라이언트가 새 요청을 할 때 새 해시를 생성합니다.

단계

1. BranchCache 해시 저장소에서 해시를 플러시합니다. 'vserver cifs BranchCache hash-flush-vserver_vserver_name_'

   'vserver cifs BranchCache hash-flush-vserver vs1'

ONTAP SMB BranchCache 통계 표시

BranchCache 통계를 에 표시할 수도 있습니다. 그 중에서도 캐싱을 얼마나 잘 수행하고 있는지 식별하고, 구성이 클라이언트에 캐시된 콘텐츠를 제공하고 있는지 여부를 확인하고, 해시 파일을 삭제하여 최신 해시 데이터를 저장할 공간을 확보할 수 있는지 확인할 수 있습니다.

이 작업에 대해

"hashd" 통계 객체에는 BranchCache 해시에 대한 통계 정보를 제공하는 카운터가 포함되어 있습니다. CIFS 통계 객체에는 BranchCache 관련 작업에 대한 통계 정보를 제공하는 카운터가 포함되어 있습니다. 고급 권한 수준에서 이러한 개체에 대한 정보를 수집하고 표시할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

2. 'tistics catalog counter show' 명령을 사용하여 BranchCache 관련 카운터를 출력한다.

```
cluster1::*> statistics catalog counter show -object hashd

Object: hashd
    Counter                     Description
    --------------------------
-----------------------------------------------
    branchcache_hash_created    Number of times a request to generate
                                BranchCache hash for a file succeeded.
```

```
    branchcache_hash_files_replaced
                                Number of times a BranchCache hash file
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    avg_junction_depth          Average number of junctions crossed by
SMB
                                and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
                                data failed. These are failures when
                                attempting to read existing hash data.
It
                                does not include attempts to fetch hash
data
                                that has not yet been generated.
```

```
    branchcache_hash_fetch_ok   Total number of times a request to fetch
hash
                                data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                requesting hashes.
    branchcache_missing_hash_bytes
                                Total number of bytes of data that had
to be
                                read by the client because the hash for
that
                                content was not available on the server.
   ....Output truncated....
```

에 대한 자세한 내용은 `statistics catalog counter show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. '스타티틱스 스타트', '스타티틱스 스톱' 명령어를 사용해 BranchCache 관련 통계를 수집한다.

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

자세히 알아보세요 `statistics start` 그리고 `statistics stop` 에서 "ONTAP 명령 참조입니다" .

4. 통계 표시 명령을 사용하여 수집된 BranchCache 통계를 표시합니다.

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

에 대한 자세한 내용은 `statistics show` "ONTAP 명령 참조입니다"을 참조하십시오.

5. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

```
cluster1::*> set -privilege admin
```

관련 정보

- 통계를 표시합니다
- "성능 모니터링 설정"
- "통계 시작"
- "통계 중지"

BranchCache 그룹 정책 개체에 대한 **ONTAP SMB** 지원에 대해 알아보세요.

ONTAP BranchCache는 특정 BranchCache 구성 매개 변수에 대한 중앙 집중식 관리를 허용하는 BranchCache GPO(그룹 정책 개체)를 지원합니다. BranchCache에는 두 가지 GPO, 즉 BranchCache GPO의 해시 게시 GPO와 BranchCache GPO의 해시 버전 지원 GPO가 사용됩니다.

- * BranchCache GPO * 용 해시 게시

  BranchCache GPO의 해시 게시는 '-operating-mode' 매개 변수에 해당합니다. GPO 업데이트가 발생하면 이 값은 그룹 정책이 적용되는 OU(조직 구성 단위) 내에 포함된 SVM(스토리지 가상 시스템) 개체에 적용됩니다.

- * BranchCache GPO * 에 대한 해시 버전 지원

  BranchCache GPO의 해시 버전 지원은 '-versions' 매개 변수에 해당합니다. GPO 업데이트가 발생하면 이 값은 그룹 정책이 적용되는 조직 구성 단위 내에 포함된 SVM 개체에 적용됩니다.

관련 정보

SMB 서버에 그룹 정책 개체를 적용하는 방법에 대해 알아보세요.

ONTAP SMB BranchCache 그룹 정책 개체에 대한 정보 표시

CIFS 서버의 GPO(그룹 정책 개체) 구성에 대한 정보를 표시하여 BranchCache GPO가 CIFS 서버가 속한 도메인에 대해 정의되었는지 그리고 그러한 경우 허용되는 설정이 무엇인지 확인할 수 있습니다. 또한 BranchCache GPO 설정이 CIFS 서버에 적용되는지 여부를 확인할 수 있습니다.

이 작업에 대해

CIFS 서버가 속한 도메인 내에서 GPO 설정이 정의되더라도 CIFS 지원 SVM(스토리지 가상 머신)이 포함된 OU(조직 구성 단위)에는 적용되지 않을 수도 있습니다. 적용된 GPO 설정은 CIFS 지원 SVM에 적용되는 정의된 모든 GPO의 하위 집합입니다. GPO를 통해 적용된 BranchCache 설정은 CLI를 통해 적용된 설정을 재정의합니다.

단계

1. 'vserver cifs group-policy show-defined' 명령을 사용하여 Active Directory 도메인에 대해 정의된 BranchCache GPO 설정을 표시합니다.

   이 예제에는 명령에 사용할 수 있는 출력 필드가 모두 표시되지 않습니다. 출력이 잘립니다.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. 'vserver cifs group-policy show-applied' 명령을 사용하여 CIFS 서버에 적용된 BranchCache GPO 설정을 표시합니다. ``이

이 예제에는 명령에 사용할 수 있는 출력 필드가 모두 표시되지 않습니다. 출력이 잘립니다.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

관련 정보

- 서버에서 GPO 지원 활성화 또는 비활성화
- "SVM CIFS 그룹 - policy show-defined"
- "SVM CIFS 그룹 - policy show-applied"

SMB 공유에서 BranchCache를 해제합니다

ONTAP SMB 공유에서 BranchCache 비활성화에 대해 알아보세요

특정 SMB 공유에서 BranchCache 캐싱 서비스를 제공하지 않고 나중에 이러한 공유에 캐싱 서비스를 제공하려는 경우 공유별로 BranchCache를 사용하지 않도록 설정할 수 있습니다. BranchCache가 모든 공유에서 캐싱을 제공하도록 구성되었지만 모든 캐싱 서비스를 일시적으로 해제하려면 BranchCache 구성을 수정하여 모든 공유에서 자동 캐싱을 중지할 수 있습니다.

SMB 공유의 BranchCache가 이후에 처음 설정된 후 비활성화되면 ONTAP는 요청된 클라이언트로 메타데이터 전송을 중지합니다. 데이터가 필요한 클라이언트는 콘텐츠 서버(SVM(Storage Virtual Machine)의 CIFS 서버)에서 직접 데이터를 검색합니다.

관련 정보

BranchCache 지원 공유 구성에 대해 알아보세요

단일 **ONTAP SMB** 공유에서 **BranchCache** 비활성화

이전에 캐시된 콘텐츠를 제공한 특정 공유에 캐싱 서비스를 제공하지 않으려면 기존 SMB 공유에서 BranchCache를 사용하지 않도록 설정할 수 있습니다.

단계

1. 'vserver cifs share properties remove-vserver vserver_name -share-name share_name-share-properties BranchCache' 명령을 입력합니다

   BranchCache 공유 속성이 제거됩니다. 다른 적용된 공유 속성은 그대로 유지됩니다.

예

다음 명령을 실행하면 이름이 "data2"인 기존 SMB 공유에서 BranchCache가 비활성화됩니다.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

모든 **ONTAP SMB** 공유에서 자동 캐싱 중지

BranchCache 구성에서 각 SVM(스토리지 가상 머신)의 모든 SMB 공유에 대한 캐싱을 자동으로 설정하는 경우 BranchCache 구성을 수정하여 모든 SMB 공유의 컨텐츠를 자동으로 캐싱하지 않도록 할 수 있습니다.

이 작업에 대해

모든 SMB 공유에서 자동 캐싱을 중지하려면 BranchCache 운영 모드를 공유 기준 캐싱으로 변경합니다.

단계

1. 모든 SMB 공유에서 자동 캐싱을 중지하도록 BranchCache를 구성합니다. 'vserver cifs BranchCache modify -vserver vserver_name -operating-mode per-share'
2. BranchCache 구성이 올바른지 확인합니다. 'vserver cifs BranchCache show -vserver vserver_name'

예

다음 명령을 실행하면 스토리지 가상 머신(SVM, 이전의 Vserver)의 BranchCache 구성이 변경되어 모든 SMB 공유에서 자동 캐싱을 중지합니다.

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

SVM에서 **BranchCache**를 비활성화하거나 활성화합니다

ONTAP SMB 서버에서 **BranchCache**를 비활성화하거나 다시 활성화하면 어떤 일이 발생하는지 알아보세요.

이전에 BranchCache를 구성했지만 지사 클라이언트가 캐시된 콘텐츠를 사용하지 않도록 하려면 CIFS 서버에서 캐싱을 해제할 수 있습니다. BranchCache를 사용하지 않도록 설정하면 어떤 일이 발생하는지 알고 있어야 합니다.

BranchCache를 사용하지 않도록 설정하면 ONTAP는 더 이상 해시를 계산하지 않고 요청 클라이언트로 메타데이터를 보내지 않습니다. 그러나 파일 액세스는 중단되지 않습니다. 그 후 BranchCache를 사용하는 클라이언트가 액세스할 콘텐츠에 대한 메타데이터 정보를 요청하면 ONTAP는 Microsoft 정의 오류로 응답하여 클라이언트가 실제 콘텐츠를 요청하는 두 번째 요청을 보냅니다. CIFS 서버는 콘텐츠 요청에 따라 SVM(스토리지 가상 머신)에 저장된 실제 콘텐츠를 전송합니다.

CIFS 서버에서 BranchCache를 사용하지 않도록 설정한 후 SMB 공유는 BranchCache 기능을 알리지 않습니다. 새 SMB 연결에서 데이터에 액세스하기 위해 클라이언트는 SMB 읽기 요청을 정상적으로 처리합니다.

언제든지 CIFS 서버에서 BranchCache를 다시 설정할 수 있습니다.

- BranchCache를 비활성화하면 해시 저장소가 삭제되지 않으므로 요청된 해시가 여전히 유효하다면 ONTAP는 해시 요청을 다시 활성화한 후 해시 요청에 응답할 때 저장된 해시를 사용할 수 있습니다.
- BranchCache를 사용하지 않는 동안 BranchCache 사용 공유에 SMB 연결을 설정한 클라이언트는 BranchCache를 나중에 다시 사용하도록 설정한 경우 BranchCache 지원을 받지 않습니다.

  이는 ONTAP가 SMB 세션을 설정할 때 공유에 대한 BranchCache 지원을 광고하기 때문입니다. BranchCache를 사용하지 않는 동안 BranchCache 사용 공유에 세션을 설정한 클라이언트는 이 공유에 대해 캐시된 콘텐츠를 사용하려면 연결을 끊고 다시 연결해야 합니다.

CIFS 서버에서 BranchCache를 해제한 후에 해시 저장소를 저장하지 않으려면 수동으로 삭제할 수 있습니다. BranchCache를 다시 사용하도록 설정하는 경우 해시 저장소 디렉터리가 있는지 확인해야 합니다. BranchCache를 다시 사용하도록 설정한 후 BranchCache 사용 공유는 BranchCache 기능을 광고합니다. ONTAP는 BranchCache 사용 클라이언트가 새 요청을 할 때 새 해시를 생성합니다.

ONTAP SMB 공유에서 **BranchCache** 비활성화 또는 활성화

BranchCache 운영 모드를 사용 안 함으로 변경하여 SVM(스토리지 가상 시스템)에서 BranchCache를 사용하지 않도록 설정할 수 있습니다. 운영 모드를 변경하여 BranchCache 서비스를 공유당 제공하거나 모든 공유에 자동으로 제공하여 언제든지 BranchCache를 활성화할 수 있습니다.

단계

1. 적절한 명령을 실행합니다.

원하는 작업	그런 다음 다음을 입력합니다.
BranchCache를 비활성화합니다	'vserver cifs BranchCache modify -vserver vserver_name -operating-mode disable'
공유당 BranchCache를 설정합니다	'vserver cifs BranchCache modify -vserver vserver_name -operating-mode per-share'
모든 공유에 대해 BranchCache를 사용하도록 설정합니다	'vserver cifs BranchCache modify -vserver vserver_name -operating-mode all-공유'

2. BranchCache 작동 모드가 'vserver cifs BranchCache show -vserver vserver vserver_name' 설정으로 구성되어 있는지 확인합니다

예

다음 예에서는 SVM VS1 에서 BranchCache를 사용하지 않도록 설정합니다.

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

SVM에서 **BranchCache** 구성을 삭제합니다

ONTAP SMB 공유에서 **BranchCache** 구성을 삭제하면 어떤 일이 발생하는지 알아보세요**.**

이전에 BranchCache를 구성했지만 SVM(스토리지 가상 시스템)이 캐시된 콘텐츠를 계속 제공하지 않도록 하려면 CIFS 서버에서 BranchCache 구성을 삭제할 수 있습니다. 구성을 삭제할 때 어떤 일이 발생하는지 알고 있어야 합니다.

구성을 삭제하면 ONTAP에서 해당 SVM에 대한 구성 정보를 클러스터에서 제거하고 BranchCache 서비스를 중지합니다. ONTAP에서 SVM의 해시 저장소를 삭제할 것인지 여부를 선택할 수 있습니다.

BranchCache 구성을 삭제해도 BranchCache 사용 클라이언트의 액세스가 중단되지 않습니다. 그 후 BranchCache를 사용하는 클라이언트가 이미 캐시된 콘텐츠에 대한 기존 SMB 연결에 대한 메타데이터 정보를 요청하면 ONTAP는 Microsoft 정의 오류로 응답하여 클라이언트가 실제 콘텐츠를 요청하는 두 번째 요청을 보냅니다. CIFS 서버는 콘텐츠 요청에 응답하여 SVM에 저장된 실제 콘텐츠를 전송합니다

BranchCache 구성이 삭제된 후 SMB 공유는 BranchCache 기능을 알리지 않습니다. 새 SMB 연결을 사용하여 이전에 캐시되지 않은 콘텐츠에 액세스하려면 클라이언트는 SMB 읽기 요청을 정상적으로 처리합니다.

ONTAP SMB 공유에서 **BranchCache** 구성을 삭제합니다**.**

SVM(스토리지 가상 시스템)에서 BranchCache 서비스를 삭제하는 데 사용하는 명령은 기존 해시를 삭제하거나 유지할지 여부에 따라 달라집니다.

단계

1. 적절한 명령을 실행합니다.

원하는 작업	그런 다음 다음을 입력합니다**.**
BranchCache 구성을 삭제하고 기존 해시를 삭제합니다	'vserver cifs BranchCache delete -vserver_vserver_name_-flush-hash true
BranchCache 구성을 삭제하지만 기존 해시는 그대로 둡니다	'vserver cifs BranchCache delete -vserver_vserver_name_-flush-hash false

예

다음 예에서는 SVM VS1 상의 BranchCache 구성을 삭제하고 기존 해시를 모두 삭제합니다.

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

ONTAP SMB BranchCache를 되돌릴 때 발생하는 일을 알아보세요.

ONTAP를 BranchCache를 지원하지 않는 릴리즈로 되돌릴 경우 어떤 일이 발생하는지 이해하는 것이 중요합니다.

- BranchCache를 지원하지 않는 ONTAP 버전으로 되돌릴 경우 SMB 공유는 BranchCache를 사용하는 클라이언트에 BranchCache 기능을 알리지 않으므로 클라이언트는 해시 정보를 요청하지 않습니다.

  대신 일반 SMB 읽기 요청을 사용하여 실제 콘텐츠를 요청합니다. 콘텐츠 요청에 따라 SMB 서버는 SVM(스토리지 가상 머신)에 저장된 실제 콘텐츠를 전송합니다.

- 해시 저장소를 호스팅하는 노드가 BranchCache를 지원하지 않는 릴리즈로 되돌려지면 스토리지 관리자는 복원 중에 인쇄되는 명령을 사용하여 BranchCache 구성을 수동으로 되돌려야 합니다.

  이 명령을 실행하면 BranchCache 구성 및 해시가 삭제됩니다.

  복원이 완료된 후 스토리지 관리자는 원하는 경우 해시 저장소가 포함된 디렉토리를 수동으로 삭제할 수 있습니다.

관련 정보

공유에서 BranchCache 구성을 삭제합니다.

Microsoft 원격 복제 성능 향상

ONTAP SMB 서버에서 **Microsoft** 원격 복사 성능 개선에 대해 알아보세요.

Microsoft ODX(Offloaded Data Transfer)는 _copy offload_라고도 하며 호스트 컴퓨터를 통해 데이터를 전송하지 않고도 호환되는 스토리지 장치 내부 또는 간에 데이터를 직접 전송할 수 있습니다.

ONTAP은 SMB 및 SAN 프로토콜을 모두 지원하는 ODX를 지원합니다. 소스는 CIFS 서버 또는 LUN일 수 있으며 대상은 CIFS 서버 또는 LUN일 수 있습니다.

ODX가 아닌 파일을 전송하면 소스에서 데이터를 읽어 네트워크를 통해 클라이언트 컴퓨터로 전송합니다. 클라이언트 컴퓨터는 네트워크를 통해 데이터를 대상으로 다시 전송합니다. 요약하면 클라이언트 컴퓨터는 소스에서 데이터를 읽고 대상에 씁니다. ODX 파일 전송을 사용하면 데이터가 소스에서 타겟으로 직접 복사됩니다.

오프로드 복사본은 소스 및 타겟 스토리지 간에 직접 수행되므로 성능이 크게 향상됩니다. 소스 및 대상 간의 복제 시간 단축, 클라이언트의 리소스 활용률(CPU, 메모리) 감소, 네트워크 I/O 대역폭 사용률 감소 등의 성능 이점을 얻을 수 있습니다.

SMB 환경의 경우 이 기능은 클라이언트와 스토리지 서버가 모두 SMB 3.0 및 ODX 기능을 지원하는 경우에만 사용할 수 있습니다. SAN 환경의 경우 이 기능은 클라이언트와 스토리지 서버가 ODX 기능을 모두 지원하는 경우에만 사용할 수 있습니다. ODX를 지원하고 ODX를 사용하는 클라이언트 컴퓨터는 파일을 이동하거나 복사할 때 오프로드된 파일

전송을 자동으로 투명하게 사용합니다. ODX는 Windows 탐색기를 통해 파일을 끌어서 놓을지, 명령줄 파일 복사 명령을 사용하는지, 클라이언트 애플리케이션이 파일 복사 요청을 시작하는지 여부와 관계없이 사용됩니다.

관련 정보

- 자동 위치 지정을 통해 자동 노드 참조를 제공하여 클라이언트 응답 시간을 개선하는 방법에 대해 알아보세요.
- "Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성"

ONTAP SMB 서버에서 **ODX**에 대해 알아보세요

ODX 복사 오프로드는 토큰 기반 메커니즘을 사용하여 ODX 지원 CIFS 서버 내부 또는 간에 데이터를 읽고 씁니다. CIFS 서버는 데이터를 호스트를 통해 라우팅하는 대신 데이터를 나타내는 작은 토큰을 클라이언트에 보냅니다. ODX 클라이언트는 해당 토큰을 대상 서버에 제공하고, 이 토큰을 통해 표시되는 데이터를 소스에서 타겟으로 전송할 수 있습니다.

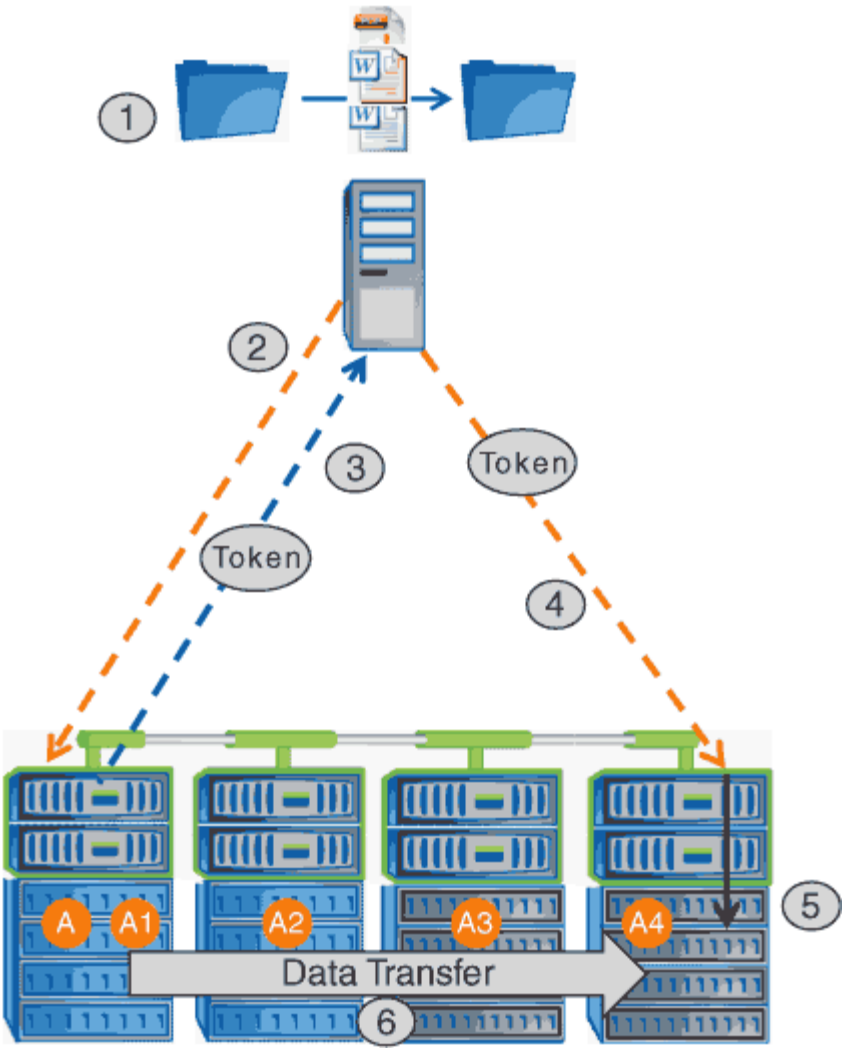
ODX 클라이언트는 CIFS 서버가 ODX를 지원하는 서버임을 인식하면 소스 파일을 열고 CIFS 서버에서 토큰을 요청합니다. 대상 파일을 연 후 클라이언트는 토큰을 사용하여 서버에서 데이터를 소스에서 대상으로 직접 복사하도록 지시합니다.

복사 작업의 범위에 따라 소스 및 대상이 동일한 SVM(스토리지 가상 머신) 또는 다른 SVM에 있을 수 있습니다.

토큰은 데이터의 시점 표현의 역할을 합니다. 예를 들어, 스토리지 위치 간에 데이터를 복사할 때 데이터 세그먼트를 나타내는 토큰이 요청 클라이언트로 반환되고, 이 클라이언트는 대상에 복사되므로 클라이언트를 통해 기본 데이터를 복사할 필요가 없습니다.

ONTAP는 8MB의 데이터를 나타내는 토큰을 지원합니다. 8MB를 초과하는 ODX 복제본은 8MB의 데이터를 나타내는 각 토큰과 함께 여러 토큰을 사용하여 수행됩니다.

다음 그림에서는 ODX 복사 작업과 관련된 단계를 설명합니다.



1. 사용자가 Windows 탐색기, 명령줄 인터페이스 또는 가상 시스템 마이그레이션의 일부로 파일을 복사 또는 이동하거나 응용 프로그램이 파일 복사 또는 이동을 시작합니다.
2. ODX 지원 클라이언트는 이 전송 요청을 ODX 요청으로 자동 변환합니다.

   CIFS 서버로 전송되는 ODX 요청에 토큰에 대한 요청이 있습니다.

3. CIFS 서버에서 ODX가 설정되어 있고 연결이 SMB 3.0을 통해 설정되어 있으면 CIFS 서버가 토큰을 생성합니다. 이는 소스에서 데이터를 논리적으로 표현한 것입니다.
4. 클라이언트는 데이터를 나타내는 토큰을 받아 쓰기 요청과 함께 대상 CIFS 서버로 전송합니다.

   이 데이터는 네트워크를 통해 소스에서 클라이언트로 복사한 다음 클라이언트에서 대상으로 복사하는 유일한 데이터입니다.

5. 토큰이 스토리지 서브시스템에 제공됩니다.
6. SVM은 내부적으로 복사 또는 이동을 수행합니다.

   복사 또는 이동된 파일이 8MB보다 큰 경우 복제를 수행하려면 여러 토큰이 필요합니다. 필요에 따라 복사를 완료하기 위해 2-6단계를 수행합니다.

ODX 복사 작업을 오프로드하는 데 장애가 발생하면 복사 또는 이동 작업이 복사 또는 이동 작업에 대한 기존 읽기 및 쓰기로 다시 이동됩니다. 마찬가지로, 대상 CIFS 서버가 ODX 또는 ODX를 지원하지 않을 경우 복사 또는 이동 작업이 복사 또는 이동 작업에 대한 기존 읽기 및 쓰기로 다시 돌아갑니다.

ONTAP SMB 서버에서 **ODX**를 사용하기 위한 요구 사항

복사 오프로드를 SVM(스토리지 가상 머신)과 함께 사용하려면 먼저 특정 요구사항을 알고 있어야 합니다.

ONTAP 버전 요구 사항

ONTAP는 복사 오프로드를 위한 ODX를 지원합니다.

SMB 버전 요구 사항

- ONTAP는 SMB 3.0 이상을 지원하는 ODX를 지원합니다.
- ODX를 사용하려면 CIFS 서버에서 SMB 3.0을 설정해야 함:
  - ODX를 사용하도록 설정하면 SMB 3.0도 사용할 수 없습니다.
  - SMB 3.0을 비활성화하면 ODX도 비활성화됩니다.

Windows 서버 및 클라이언트 요구 사항

복사 오프로드를 위해 ODX를 사용하려면 Windows 클라이언트에서 이 기능을 지원해야 합니다.

를 클릭합니다 "NetApp 상호 운용성 매트릭스"지원되는 Windows 클라이언트에 대한 최신 정보를 제공합니다.

볼륨 요구 사항

- 소스 볼륨은 최소 1.25GB여야 합니다.
- 압축 볼륨을 사용하는 경우 압축 유형은 적응 가능해야 하며 압축 그룹 크기 8K만 지원됩니다.

  보조 압축 유형은 지원되지 않습니다.

ONTAP SMB 서버에서 **ODX**를 사용하기 위한 지침

복사 오프로드에 ODX를 사용하려면 먼저 지침을 숙지하고 있어야 합니다. 예를 들어, ODX를 사용할 수 있는 볼륨 유형을 파악하고 클러스터 내부 및 클러스터 간 ODX 고려 사항을 파악해야 합니다.

볼륨 지침

- 다음과 같은 볼륨 구성에서는 복사 오프로드에 ODX를 사용할 수 없습니다.
  - 소스 볼륨 크기가 1.25GB 미만입니다

    ODX를 사용하려면 볼륨 크기가 1.25GB 이상이어야 합니다.

  - 읽기 전용 볼륨입니다

ODX는 로드 공유 미러 또는 SnapMirror 또는 SnapVault 대상 볼륨에 상주하는 파일 및 폴더에 사용되지 않습니다.

- 소스 볼륨 중복 제거가 수행되지 않은 경우

- ODX 복사본은 클러스터 내 복사본에만 지원됩니다.

  ODX를 사용하여 파일 또는 폴더를 다른 클러스터의 볼륨으로 복사할 수는 없습니다.

기타 지침

- SMB 환경에서 복사 오프로드에 ODX를 사용하려면 파일이 256KB 이상이어야 합니다.

  작은 파일은 기존 복사 작업을 사용하여 전송됩니다.

- ODX 복사 오프로드는 복제 프로세스의 일부로 중복 제거를 사용합니다.

  데이터를 복사하거나 이동할 때 SVM 볼륨에서 중복 제거를 수행하지 않으려면 해당 SVM에서 ODX 복사 오프로드를 해제해야 합니다.

- ODX를 지원하려면 데이터 전송을 수행하는 애플리케이션에 데이터를 기록해야 합니다.

  ODX를 지원하는 애플리케이션 작업은 다음과 같습니다.

  - 가상 하드 디스크(VHD) 생성 및 변환, 스냅샷 관리, 가상 컴퓨터 간 파일 복사 등의 Hyper-V 관리 작업
  - Windows 탐색기 작업
  - Windows PowerShell 복사 명령
  - Windows 명령 프롬프트 복사 명령

    Windows 명령 프롬프트의 Robocopy는 ODX를 지원합니다.

    ODX를 지원하는 Windows 서버 또는 클라이언트에서 애플리케이션이 실행되고 있어야 합니다.

+
Windows 서버 및 클라이언트에서 지원되는 ODX 애플리케이션에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

관련 정보

"Microsoft TechNet 라이브러리: technet.microsoft.com/en-us/library/"

ONTAP SMB 서버에서 **ODX** 사용 사례

ODX가 성능 이점을 제공하는 상황을 파악할 수 있도록 SVM에서 ODX를 사용하는 사용 사례를 알고 있어야 합니다.

ODX를 지원하는 Windows 서버 및 클라이언트는 원격 서버 간에 데이터를 복사하는 기본 방법으로 복사 오프로드를 사용합니다. Windows 서버 또는 클라이언트가 ODX를 지원하지 않거나 ODX 복사 오프로드가 어느 시점에서든 장애가 발생하면 복사 또는 이동 작업이 복사 또는 이동 작업에 대한 기존 읽기/쓰기로 다시 돌아갑니다.

ODX 복사 및 이동 사용을 지원하는 사용 사례는 다음과 같습니다.

- 체내

  소스 및 대상 파일 또는 LUN이 동일한 볼륨 내에 있습니다.

- 볼륨 간, 동일한 노드, 동일한 SVM

  소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- 볼륨 간, 다른 노드, 동일한 SVM

  소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- SVM 간, 동일한 노드

  소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

- SVM 간, 다른 노드

  소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

- 클러스터 간

  소스 및 타겟 LUN은 클러스터 전반의 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 이 기능은 SAN에만 지원되며 CIFS에는 사용할 수 없습니다.

다음과 같은 몇 가지 특별한 사용 사례가 있습니다.

- ONTAP ODX를 구현하면 ODX를 사용하여 SMB 공유와 FC 또는 iSCSI 연결 가상 드라이브 간에 파일을 복사할 수 있습니다.

  SMB 공유와 LUN이 동일한 클러스터에 존재하는 경우, ODX를 지원하는 Windows 탐색기, Windows CLI 또는 PowerShell, Hyper-V 또는 기타 애플리케이션을 사용하여 SMB 공유와 연결된 LUN 간에 ODX 복사 오프로드를 사용하여 파일을 원활하게 복사 또는 이동할 수 있습니다.

- Hyper-V는 ODX 복사 오프로드를 위한 몇 가지 추가 사용 사례를 제공합니다.

  - Hyper-V에서 ODX 복사 오프로드 패스스스루 를 사용하여 VHD(가상 하드 디스크) 파일 내부 또는 VHD 파일 간에 데이터를 복사하거나, 매핑된 SMB 공유와 동일한 클러스터 내에서 연결된 iSCSI LUN 간에 데이터를 복사할 수 있습니다.

    이렇게 하면 게스트 운영 체제에서 복제본을 기본 스토리지로 전달할 수 있습니다.

  - 고정 크기의 VHD를 생성할 때 ODX는 잘 알려진 제로화 토큰을 사용하여 0으로 디스크를 초기화하는 데 사용됩니다.
  - 소스 및 타겟 스토리지가 동일한 클러스터에 있는 경우 ODX 복사 오프로드가 가상 머신 스토리지 마이그레이션에 사용됩니다.

Hyper-V를 사용한 ODX 복사 오프로드 패스쓰루 사용 사례를 활용하려면 게스트 운영 체제가 ODX를 지원하고, 게스트 운영 체제 디스크는 ODX를 지원하는 스토리지(SMB 또는 SAN)를 통해 지원되는 SCSI 디스크여야 합니다. 게스트 운영 체제의 IDE 디스크는 ODX 패스스스루 를 지원하지 않습니다.

ONTAP SMB 서버에서 **ODX** 활성화 또는 비활성화

스토리지 가상 시스템(SVM)에서 ODX를 사용하거나 사용하지 않도록 설정할 수 있습니다. 기본적으로 SMB 3.0도 사용하도록 설정된 경우 ODX 복사 오프로드를 지원합니다.

시작하기 전에

SMB 3.0을 활성화해야 합니다.

이 작업에 대해

SMB 3.0을 비활성화하면 ONTAP도 SMB ODX를 비활성화합니다. SMB 3.0을 다시 설정하는 경우 SMB ODX를 수동으로 다시 설정해야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 다음 작업 중 하나를 수행합니다.

ODX 복사 오프로드 기능을 사용하려면...	명령 입력...
활성화됨	'vserver cifs options modify -vserver vserver_name -copy -offload -enabled true'
사용 안 함	'vserver cifs options modify -vserver vserver_name -copy -offload -enabled false'

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

예

다음 예에서는 SVM VS1 에서 ODX 복사 오프로드를 활성화합니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

관련 정보

사용 가능한 서버 옵션

자동 위치로 **SMB** 자동 노드 조회를 제공하여 클라이언트 응답 시간을 단축합니다

자동 위치 지정을 통해 **ONTAP SMB** 자동 노드 참조를 제공하여 클라이언트 응답 시간을 개선하는 방법에 대해 알아보세요.

자동 위치에서는 SMB 자동 노드 조회를 사용하여 스토리지 가상 시스템(SVM)에서 SMB 클라이언트 성능을 높입니다. 자동 노드 조수는 요청 클라이언트를 데이터가 상주하는 볼륨을 호스팅하는 노드 SVM의 LIF로 자동으로 리디렉션하여 클라이언트 응답 시간을 향상할 수 있습니다.

SMB 클라이언트가 SVM에서 호스팅된 SMB 공유에 연결할 경우, 요청된 데이터를 소유하지 않은 노드에 있는 LIF를 사용하여 연결할 수 있습니다. 클라이언트가 연결된 노드는 클러스터 네트워크를 사용하여 다른 노드가 소유한 데이터에 액세스합니다. SMB 연결이 요청된 데이터를 포함하고 있는 노드에 있는 LIF를 사용하면 클라이언트에서 더 빠른 응답 시간을 경험할 수 있습니다.

- ONTAP는 Microsoft DFS 조회를 사용하여 SMB 클라이언트에 네임스페이스에서 요청된 파일 또는 폴더가 다른 곳에 호스팅된다는 사실을 알리는 이 기능을 제공합니다.

  노드가 데이터를 포함하는 노드에 SVM LIF가 있다고 판단하면 노드를 전문의에게 의뢰합니다.

- IPv4 및 IPv6 LIF IP 주소에 대해 자동 노드 조회가 지원됩니다.
- 조인은 클라이언트가 연결되는 공유 루트의 위치를 기반으로 합니다.
- SMB 협상 중에 불합격입니다.

  연결이 설정되기 전에 의뢰합니다. ONTAP가 SMB 클라이언트를 타겟 노드로 참조하면 연결이 연결되고 클라이언트는 해당 시점부터 참조된 LIF 경로를 통해 데이터에 액세스합니다. 이렇게 하면 클라이언트가 데이터에 더 빠르게 액세스할 수 있고 추가 클러스터 통신을 피할 수 있습니다.

> 공유가 여러 연결 지점을 거치는 경우 일부 접합부가 다른 노드에 포함된 볼륨에 연결되는 경우 공유 내의 데이터가 여러 노드로 분산됩니다. ONTAP는 공유의 루트에 대해 로컬인 조회를 제공하므로 ONTAP는 이러한 비 로컬 볼륨에 포함된 데이터를 검색하기 위해 클러스터 네트워크를 사용해야 합니다. 이러한 유형의 네임스페이스 아키텍처를 사용하면 자동 노드 조회가 성능에 큰 이점을 제공하지 않을 수 있습니다.

데이터를 호스팅하는 노드에 사용 가능한 LIF가 없는 경우 ONTAP은 클라이언트가 선택한 LIF를 사용하여 연결을 설정합니다. SMB 클라이언트가 파일을 연 후에는 동일한 참조 연결을 통해 계속 파일에 액세스합니다.

어떤 이유로든 CIFS 서버가 조회를 수행할 수 없는 경우 SMB 서비스가 중단되지 않습니다. SMB 연결은 자동 노드 조회가 활성화되지 않은 것처럼 설정됩니다.

관련 정보

Microsoft 원격 복제 성능 향상

ONTAP SMB 서버에서 자동 노드 참조를 사용하기 위한 요구 사항 및 지침

SMB 자동 노드 조회를 사용하려면 _ autolocation _ 이라고도 하며, 이 기능을 지원하는 ONTAP 버전을 비롯한 특정 요구 사항을 알고 있어야 합니다. 또한 지원되는 SMB 프로토콜 버전 및 기타 특정 특별 지침에 대해서도 알아야 합니다.

ONTAP 버전 및 라이센스 요구 사항

- 클러스터의 모든 노드는 자동 노드 조회를 지원하는 ONTAP 버전을 실행하고 있어야 합니다.
- 자동 위치 정보를 사용하려면 SMB 공유에서 Widelink를 활성화해야 합니다.
- CIFS에 대한 라이센스가 있어야 하며 SMB 서버가 SVM에 있어야 합니다. SMB 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오"있습니다. ONTAP One이 없고 라이선스가 설치되지 않은 경우 영업 담당자에게 문의하십시오.

SMB 프로토콜 버전 요구 사항

- SVM의 경우 ONTAP는 모든 SMB 버전에서 자동 노드 조회를 지원합니다.

SMB 클라이언트 요구 사항

ONTAP에서 지원하는 모든 Microsoft 클라이언트는 SMB 자동 노드 조회를 지원합니다.

상호 운용성 매트릭스에는 ONTAP에서 지원하는 Windows 클라이언트에 대한 최신 정보가 포함되어 있습니다.

"NetApp 상호 운용성 매트릭스 툴"

데이터 **LIF** 요구사항

데이터 LIF를 SMB 클라이언트를 위한 잠재 고객으로 사용하려면 NFS와 CIFS를 모두 사용하도록 설정된 데이터 LIF를 생성해야 합니다.

타겟 노드에 NFS 프로토콜에만 사용하도록 설정된 데이터 LIF가 있거나 SMB 프로토콜에 대해서만 사용하도록 설정된 데이터 LIF가 있는 경우 자동 노드 조회가 작동하지 않을 수 있습니다.

이 요구 사항이 충족되지 않으면 데이터 액세스가 영향을 받지 않습니다. SMB 클라이언트는 클라이언트가 SVM에 연결할 때 사용한 원래 LIF를 사용하여 공유를 매핑합니다.

참조된 **SMB** 연결을 만들 때 **NTLM** 인증 요구 사항

NTLM 인증은 CIFS 서버가 포함된 도메인 및 자동 노드 조회를 사용하려는 클라이언트가 포함된 도메인에서 허용되어야 합니다.

SMB 서버는 조회를 수행할 때 Windows 클라이언트에 대한 IP 주소를 참조합니다. NTLM 인증은 IP 주소를 사용하여 연결할 때 사용되므로 Kerberos 인증은 참조된 연결에 대해 수행되지 않습니다.

이는 Kerberos(service/netbios name, service/FQDN) 형태의 서비스 주체 이름을 Windows 클라이언트가 생성할 수 없기 때문에 클라이언트가 Kerberos 티켓을 서비스에 요청할 수 없다는 뜻입니다.

홈 디렉토리 기능과 함께 자동 노드 조회를 사용하는 지침

공유가 홈 디렉토리 공유 속성을 사용하여 구성된 경우 홈 디렉토리 구성에 대해 하나 이상의 홈 디렉토리 검색 경로가 구성될 수 있습니다. 검색 경로는 SVM 볼륨을 포함하는 각 노드에 포함된 볼륨을 가리킬 수 있습니다. 클라이언트는 추천을 받으며 액티브 로컬 데이터 LIF가 사용 가능한 경우 홈 사용자의 홈 디렉토리에 로컬로 연결된 참조된 LIF를 통해 연결됩니다.

SMB 1.0 클라이언트가 자동 노드 조회가 설정된 동적 홈 디렉토리에 액세스하는 경우 지침이 있습니다. 이는 SMB 1.0 클라이언트가 인증을 받기 전에 자동 노드 조회를 필요로 하기 때문입니다. 이는 SMB 서버가 사용자 이름을 가지기 전입니다. 그러나 SMB 1.0 클라이언트에서 SMB 홈 디렉토리 액세스가 올바르게 작동하는 경우는 다음과 같습니다.

- SMB 홈 디렉토리는 ""%w"(Windows 사용자 이름) 또는 ""%u"(매핑된 UNIX 사용자 이름)와 같은 단순 이름을 사용하도록 구성되어 있으며 ""%d\%w"(domain-name\user-name)와 같은 도메인 이름 스타일 이름은 사용하지 않습니다.
- 홈 디렉토리 공유를 생성할 때 CIFS 홈 디렉토리 공유 이름은 ""home""과 같은 정적 이름이 아니라 변수(""%w" 또는 ""%u")로 구성됩니다.

SMB 2.x 및 SMB 3.0 클라이언트의 경우 자동 노드 조회를 사용하여 홈 디렉토리에 액세스할 때 특별한 지침이 없습니다.

기존에 연결된 연결이 있는 **CIFS** 서버에서 자동 노드 조회를 해제하는 지침입니다

이 옵션이 설정된 후 자동 노드 조회를 사용하지 않도록 설정하면 현재 참조된 LIF에 연결된 클라이언트가 계속 연결된 상태로 유지됩니다. ONTAP는 DFS 조회를 SMB 자동 노드 조정의 메커니즘으로 사용하므로, 클라이언트의 캐시된 DFS 참조 시간이 초과될 때까지 이 옵션을 비활성화한 후에 클라이언트가 참조된 LIF에 다시 연결할 수도 있습니다. 자동 노드 조회를 지원하지 않는 ONTAP 버전으로 되돌리는 경우에도 마찬가지입니다. 클라이언트는 클라이언트의 캐시에서 DFS 참조 시간이 초과될 때까지 계속 조회를 사용합니다.

Autolocation은 SMB 자동 노드 조회를 사용하여 SVM의 데이터 볼륨을 소유하는 노드의 LIF에 클라이언트를 위탁하여 SMB 클라이언트의 성능을 높입니다. SMB 클라이언트가 SVM에서 호스팅되는 SMB 공유에 연결할 경우, 요청된 데이터를 소유하지 않고 클러스터 인터커넥트 네트워크를 사용하여 데이터를 검색하는 노드에서 LIF를 사용하여 연결할 수 있습니다. SMB 연결이 요청된 데이터를 포함하고 있는 노드에 있는 LIF를 사용하는 경우 클라이언트는 더 빠른 응답 시간을 경험할 수 있습니다.

ONTAP는 Microsoft DFS(분산 파일 시스템) 조회를 사용하여 SMB 클라이언트에 네임스페이스에서 요청된 파일 또는 폴더가 다른 곳에 호스팅된다는 사실을 알려 주는 이 기능을 제공합니다. 노드가 데이터를 포함하는 노드에 SVM LIF가 있다고 판단하면 노드를 전문의에게 의뢰합니다. 조인은 클라이언트가 연결되는 공유 루트의 위치를 기반으로 합니다.

SMB 협상 중에 불합격입니다. 연결이 설정되기 전에 의뢰합니다. ONTAP가 SMB 클라이언트를 타겟 노드로 참조하면 연결이 연결되고 클라이언트는 해당 시점부터 참조된 LIF 경로를 통해 데이터에 액세스합니다. 이렇게 하면 클라이언트가 데이터에 더 빠르게 액세스할 수 있고 추가 클러스터 통신을 피할 수 있습니다.

Mac OS 클라이언트에서 자동 노드 조회를 사용하는 방법에 대한 지침입니다

Mac OS X 클라이언트는 Microsoft의 DFS(Distributed File System)를 지원하지만 SMB 자동 노드 조회를 지원하지 않습니다. Windows 클라이언트는 SMB 공유에 연결하기 전에 DFS 참조 요청을 합니다. ONTAP는 요청된 데이터를 호스팅하는 동일한 노드에 있는 데이터 LIF를 지칭하여 클라이언트 응답 시간을 개선합니다. Mac OS는 DFS를 지원하지만 Mac OS 클라이언트는 이 영역의 Windows 클라이언트와 정확히 작동하지 않습니다.

관련 정보

- 서버에서 동적 홈 디렉토리를 활성화하는 방법에 대해 알아보세요.
- "네트워크 관리"
- "NetApp 상호 운용성 매트릭스 툴"

ONTAP SMB 자동 노드 참조 지원

SMB 자동 노드 조회를 활성화하기 전에 특정 ONTAP 기능이 조회를 지원하지 않는다는 점을 알아야 합니다.

- 다음 유형의 볼륨은 SMB 자동 노드 조회를 지원하지 않습니다.
  - 로드 공유 미러의 읽기 전용 구성원입니다

◦ 데이터 보호 미러의 타겟 볼륨입니다

- 노드 조회가 LIF 이동 옆에서 이동하지 않습니다.

  클라이언트가 SMB 2.x 또는 SMB 3.0 연결을 통해 위탁된 연결을 사용 중이고 데이터 LIF가 중단 없이 이동되는 경우, LIF가 더 이상 데이터에 로컬이 아니어도 클라이언트는 계속 동일한 연결 연결을 사용합니다.

- 노드 조회가 볼륨 이동 옆에서 이동하지 않습니다.

  클라이언트가 SMB 연결을 통해 참조된 연결을 사용하고 있고 볼륨 이동이 발생하는 경우, 클라이언트는 볼륨이 데이터 LIF와 같은 노드에 더 이상 존재하지 않더라도 계속해서 동일한 연결 연결을 사용합니다.

ONTAP SMB 자동 노드 참조 활성화 또는 비활성화

SMB 자동 노드 조회를 활성화하여 SMB 클라이언트 액세스 성능을 높일 수 있습니다. ONTAP가 SMB 클라이언트에 조회를 하지 않도록 하려면 자동 노드 조회를 사용하지 않도록 설정할 수 있습니다.

시작하기 전에

CIFS 서버는 SVM(스토리지 가상 머신)에서 구성 및 실행해야 합니다.

이 작업에 대해

SMB 자동 노드 조회 기능은 기본적으로 비활성화되어 있습니다. 필요에 따라 각 SVM에서 이 기능을 활성화 또는 비활성화할 수 있습니다.

이 옵션은 고급 권한 수준에서 사용할 수 있습니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. 필요에 따라 SMB 자동 노드 조회를 설정하거나 해제합니다.

SMB 자동 노드 조회를 원하는 경우…	다음 명령을 입력합니다…
활성화됨	'vserver cifs options modify -vserver vserver_name -is-referral-enabled true'
사용 안 함	'vserver cifs options modify -vserver vserver_name -is-referral-enabled false'

   옵션 설정은 새 SMB 세션에 적용됩니다. 기존 연결이 있는 클라이언트는 기존 캐시 시간 제한이 만료될 때만 노드 조회를 사용할 수 있습니다.

3. 'Set-Privilege admin'으로 설정

관련 정보

사용 가능한 서버 옵션

SMB 연결 조회 수를 확인하려면 '통계' 명령어를 사용해 자동 노드 조회 활동을 모니터링할 수 있다. 조회를 모니터링하면 공유를 호스팅하는 노드에서 자동 조회가 접속을 찾는 범위와 CIFS 서버의 공유에 대한 로컬 액세스를 더 잘 제공할 수 있도록 데이터 LIF를 재분산해야 하는지 여부를 확인할 수 있습니다.

이 작업에 대해

"CIFS" 객체는 SMB 자동 노드 조회를 모니터링할 때 유용한 고급 권한 수준의 여러 카운터를 제공합니다.

- 'node_referral_발급'

  공유 루트의 노드와 다른 노드에서 호스팅되는 LIF를 사용하여 클라이언트가 연결된 후 공유 루트 노드에 대한 조회를 실행한 클라이언트 수입니다.

- 'node_referral_local

  공유 루트를 호스팅하는 동일한 노드에서 호스팅되는 LIF를 사용하여 연결된 클라이언트의 수입니다. 로컬 액세스는 일반적으로 최적의 성능을 제공합니다.

- 'node_referral_not_possible'

  공유 루트의 노드와 다른 노드에서 호스팅되는 LIF를 사용하여 연결한 후 공유 루트를 호스팅하는 노드에 아직 위탁하지 않은 클라이언트 수입니다. 이는 공유 루트의 노드에 대한 활성 데이터 LIF를 찾을 수 없기 때문입니다.

- 'node_referral_remote

  공유 루트를 호스팅하는 노드와 다른 노드에서 호스팅되는 LIF를 사용하여 연결된 클라이언트 수입니다. 원격 액세스로 인해 성능이 저하될 수 있습니다.

특정 기간(샘플)에 대한 데이터를 수집 및 확인하여 스토리지 가상 시스템(SVM)에 대한 자동 노드 참조 통계를 모니터링할 수 있습니다. 데이터 수집을 중지하지 않으면 샘플의 데이터를 볼 수 있습니다. 데이터 수집을 중지하면 고정된 샘플이 제공됩니다. 데이터 수집을 중지하지 않으면 이전 쿼리와 비교하는 데 사용할 수 있는 업데이트된 데이터를 가져올 수 있습니다. 비교를 통해 성능 추세를 파악할 수 있습니다.

'통계' 명령을 통해 수집한 정보를 평가하고 사용하려면 사용자 환경에서 클라이언트의 분포를 이해해야 합니다.

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
2. '통계' 명령어를 이용하여 자동 노드 조회 통계를 볼 수 있다.

   이 예제에서는 샘플링된 기간에 대한 데이터를 수집하고 확인하여 자동 노드 참조 통계를 보여 줍니다.

   a. 'stantics start-object cifs-instance vs1-sample-id sample1' 컬렉션을 시작합니다

      ```
      Statistics collection is being started for Sample-id: sample1
      ```

   b. 원하는 수집 시간이 경과할 때까지 기다립니다.

c. '스타티틱스 스톱-시료-ID 삼ple1' 컬렉션을 중단한다

```
Statistics collection is being stopped for Sample-id: sample1
```

자세히 알아보세요 `statistics start` 그리고 `statistics stop` 에서 "ONTAP 명령 참조입니다" .

d. 자동 노드 참조 통계: 'stattics show -sample-id sample1-counter * node *'를 봅니다

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                     Value
    --------------------------- ----------------------------
    node_name                                   node1
    node_referral_issued                            0
    node_referral_local                             1
    node_referral_not_possible                      2
    node_referral_remote                            2
    ...

    node_name                                   node2
    node_referral_issued                            2
    node_referral_local                             1
    node_referral_not_possible                      0
    node_referral_remote                            2
    ...
```

SVM VS1에 참여하는 모든 노드의 카운터를 출력합니다. 이 예에서는 자동 노드 조회 통계와 관련된 출력 필드만 제공합니다.

에 대한 자세한 내용은 `statistics show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. admin 권한 수준으로 복귀:'et-Privilege admin'입니다

관련 정보

- 통계를 표시합니다
- "성능 모니터링 설정"

Windows 클라이언트를 사용하여 클라이언트 측 **ONTAP SMB** 자동 노드 참조 정보 모니터링

클라이언트의 관점에서 어떤 조회를 수행할지 결정하려면 Windows dutil.exe를 사용할 수 있습니다.

Windows 7 이상의 클라이언트에서 사용할 수 있는 RSAT(원격 서버 관리 도구) 키트에는 Dsutil.exe가 포함되어 있습니다. 이 유틸리티를 사용하면 추천 캐시의 내용에 대한 정보를 표시하고 클라이언트가 현재 사용하고 있는 각 추천 정보에 대한 정보를 볼 수 있습니다. 이 유틸리티를 사용하여 클라이언트의 조회 캐시를 지울 수도 있습니다. 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

관련 정보

"Microsoft TechNet 라이브러리: technet.microsoft.com/en-us/library/"

액세스 기반 열거를 사용하여 공유에 대한 폴더 보안을 제공합니다

액세스 기반 열거를 통해 공유에 **ONTAP SMB** 폴더 보안 제공

SMB 공유에서 ABE(Access-Based Enumeration)를 사용하면 공유 내에 포함된 폴더나 파일에 액세스할 수 있는 권한이 없는 사용자(개인 또는 그룹 권한 제한 사용 여부)는 공유 자체가 표시되더라도 공유 리소스가 해당 환경에 표시되지 않습니다.

일반 공유 속성을 사용하면 공유에 포함된 파일 또는 폴더를 보거나 수정할 수 있는 권한이 있는 사용자(개별 또는 그룹)를 지정할 수 있습니다. 그러나 공유 내의 폴더나 파일이 액세스 권한이 없는 사용자에게 표시되는지 여부를 제어할 수는 없습니다. 이러한 폴더 또는 공유 내의 파일 이름이 개발 중인 고객 또는 제품 이름과 같은 중요한 정보를 설명하는 경우 문제가 발생할 수 있습니다.

ABE(Access-Based Enumeration)는 공유 속성을 확장하여 공유 내의 파일 및 폴더 열거를 포함합니다. 따라서 ABE를 사용하면 사용자 액세스 권한에 따라 공유 내의 파일 및 폴더 표시를 필터링할 수 있습니다. 즉, 공유 자체는 모든 사용자에게 표시되지만 공유 내의 파일과 폴더는 지정된 사용자에게 표시되거나 숨겨집니다. 업무 공간의 중요한 정보를 보호하는 것 외에도, ABE를 사용하면 전체 컨텐츠 범위에 액세스할 필요가 없는 사용자에게 혜택을 제공하기 위해 대규모 디렉터리 구조의 표시를 단순화할 수 있습니다. 예를 들어 공유 자체는 모든 사용자에게 표시되지만 공유 내의 파일과 폴더는 표시하거나 숨길 수 있습니다.

에 대해 자세히 알아보십시오 "SMB/CIFS 액세스 기반 열거 사용 시 성능에 미치는 영향".

ONTAP SMB 공유에서 액세스 기반 열거 활성화 또는 비활성화

SMB 공유에서 ABE(Access-Based Enumeration)를 설정하거나 해제하여 사용자가 액세스 권한이 없는 공유 리소스를 볼 수 없도록 하거나 허용할 수 있습니다.

이 작업에 대해

기본적으로 ABE는 비활성화되어 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

원하는 작업	명령 입력...
새 공유에서 ABE를 활성화합니다	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` SMB 공유를 생성할 때 추가 공유 설정 및 추가 공유 속성을 지정할 수 있습니다. 에 대한 자세한 내용은 `vserver cifs share create` "ONTAP 명령 참조입니다"을 참조하십시오.

원하는 작업	명령 입력...
기존 공유에서 ABE를 활성화합니다	'vserver cifs 공유 속성 add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration' 기존 공유 속성은 보존됩니다. ABE 공유 속성은 기존 공유 속성 목록에 추가됩니다.
기존 공유에서 ABE를 비활성화합니다	'vserver cifs share properties remove - vserver vserver_name -share-name share_name -share -properties access-based-enumeration' 다른 공유 속성은 보존됩니다. 공유 속성 목록에서 ABE 공유 속성만 제거됩니다.

2. 'vserver cifs share show' 명령을 사용하여 공유 구성이 올바른지 확인합니다.

예

다음 예에서는 SVM VS1 에서 /sales 경로를 사용하여 "sale"이라는 이름의 ABE SMB 공유를 생성합니다. 공유는 공유 속성으로 '액세스 기반 열거'로 만들어집니다.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                     Vserver: vs1
                       Share: sales
     CIFS Server NetBIOS Name: VS1
                        Path: /sales
             Share Properties: access-based-enumeration
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                 Offline Files: manual
Vscan File-Operations Profile: standard
```

다음 예제에서는 "data2"라는 SMB 공유에 "액세스 기반 열거" 공유 속성을 추가합니다.

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ------------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

관련 정보

기존 주식에 주식 속성 추가 또는 제거

ONTAP SMB 공유에서 **Windows** 클라이언트의 액세스 기반 열거 활성화 또는 비활성화

Windows 클라이언트에서 SMB 공유에 대해 ABE(액세스 기반 열거)를 설정하거나 해제할 수 있습니다. 그러면 CIFS 서버에 연결하지 않고도 이 공유 설정을 구성할 수 있습니다.

새 버전의 Windows Server 및 Windows 클라이언트에서는 abecmd 유틸리티를 사용할 수 없습니다. 이 제품은 Windows Server 2008의 일부로 출시되었습니다. 2020년 1월 14일에 Windows Server 2008에 대한 지원이 종료되었습니다.

단계

1. ABE를 지원하는 Windows 클라이언트에서 'abecmd[/enable|/disable][/server cifs_server_name]{/all|share_name}' 명령을 입력합니다

   "abecmd" 명령에 대한 자세한 내용은 Windows 클라이언트 설명서를 참조하십시오.

NFS 및 SMB 파일 및 디렉토리 명명 종속성

ONTAP NFS 및 **SMB** 파일 및 디렉토리 명명 종속성에 대해 알아보세요.

파일 및 디렉토리 명명 규칙은 ONTAP 클러스터 및 클라이언트의 언어 설정과 함께 네트워크 클라이언트의 운영 체제 및 파일 공유 프로토콜에 따라 다릅니다.

운영 체제 및 파일 공유 프로토콜에는 다음이 결정됩니다.

- 문자 파일 이름에 사용할 수 있습니다
- 파일 이름의 대/소문자 구분

ONTAP는 ONTAP 릴리즈별 파일, 디렉토리 및 qtree 이름에서 멀티바이트 문자를 지원합니다.

ONTAP SMB 파일 또는 디렉토리 이름에 유효한 문자에 대해 알아보세요.

다른 운영 체제를 사용하는 클라이언트에서 파일 또는 디렉토리에 액세스하는 경우 두 운영 체제 모두에서 유효한 문자를 사용해야 합니다.

예를 들어 UNIX를 사용하여 파일 또는 디렉토리를 생성하는 경우 MS-DOS 파일 또는 디렉토리 이름에 콜론이 허용되지 않으므로 이름에 콜론(:)을 사용하지 마십시오. 유효한 문자의 제한 사항은 운영 체제마다 다르므로 금지된 문자에 대한 자세한 내용은 클라이언트 운영 체제 설명서를 참조하십시오.

다중 프로토콜 환경에서 **ONTAP SMB** 파일 및 디렉토리 이름의 대소문자 구분

파일 및 디렉토리 이름은 NFS 클라이언트의 경우 대/소문자를 구분하며, SMB 클라이언트의 경우 대/소문자를 구분하지 않지만 대/소문자를 구분합니다. SMB 공유를 생성하는 동안 그리고 공유 내의 데이터에 액세스할 때 경로를 지정할 때 취해야 할 조치와 멀티 프로토콜 환경에 미치는 영향을 이해해야 합니다.

SMB 클라이언트가 testdir라는 디렉토리를 만들면 SMB 클라이언트와 NFS 클라이언트 모두 파일 이름을 testdir로 표시합니다. 그러나 SMB 사용자가 나중에 디렉터리 이름 testdir을 만들려고 하면 해당 이름이 SMB 클라이언트에 현재 있기 때문에 이 이름은 허용되지 않습니다. NFS 사용자가 나중에 "testdir"이라는 디렉토리를 생성할 경우 NFS 및 SMB 클라이언트는 다음과 같이 디렉토리 이름을 다르게 표시합니다.

- NFS 클라이언트에서는 디렉토리 이름이 대/소문자를 구분하기 때문에 디렉토리 이름이 생성될 때 testdir와 testdir 같은 두 디렉토리 이름을 모두 볼 수 있습니다.
- SMB 클라이언트는 8.3 이름을 사용하여 두 디렉토리를 구분합니다. 한 디렉토리에 기본 파일 이름이 있습니다. 추가 디렉토리에는 8.3 파일 이름이 할당됩니다.
  - SMB 클라이언트에서는 testdir과 testDI~1이 표시됩니다.
  - ONTAP는 두 디렉토리를 구분하기 위해 'TESTDI~1' 디렉토리 이름을 생성한다.

    이 경우 SVM(스토리지 가상 머신)에서 공유를 생성하거나 수정하는 동안 공유 경로를 지정할 때 8.3 이름을 사용해야 합니다.

마찬가지로 SMB 클라이언트가 test.txt를 만들면 SMB 클라이언트와 NFS 클라이언트 모두 파일 이름을 text.txt로 표시합니다. 그러나 SMB 사용자가 나중에 Test.txt를 생성하려고 하면 SMB 클라이언트에 해당 이름이 현재 있기 때문에 이 이름은 허용되지 않습니다. NFS 사용자가 나중에 Test.txt라는 파일을 만들면 NFS 및 SMB 클라이언트는 다음과 같이 파일 이름을 다르게 표시합니다.

- NFS 클라이언트에서는 파일 이름이 대/소문자를 구분하기 때문에 이름이 test.txt와 Test.txt로 만들어지면 두 파일 이름이 모두 표시됩니다.
- SMB 클라이언트는 8.3 이름을 사용하여 두 파일을 구분합니다. 한 파일에 기본 파일 이름이 있습니다. 8.3 파일 이름이 추가로 할당됩니다.
  - SMB 클라이언트의 경우 test.txt와 test~1.TXT가 표시됩니다.
  - ONTAP는 두 파일을 구별하기 위해 'test~1.TXT' 파일 이름을 만듭니다.

> SVM CIFS 문자 매핑 명령을 사용하여 문자 매핑을 설정하거나 수정한 경우 일반적으로 대/소문자를 구분하지 않는 Windows 조회가 대/소문자를 구분합니다.

ONTAP SMB 파일 및 디렉토리 이름 생성에 대해 알아보세요

ONTAP는 SMB 클라이언트에서 액세스할 수 있는 디렉토리인 원래 긴 이름과 8.3 형식의 이름을 사용하여 파일 또는 디렉토리의 이름을 두 개 생성하고 유지합니다.

파일 또는 디렉토리 이름이 8자 이름 또는 3자 확장자 제한(파일의 경우)을 초과하는 경우, ONTAP는 다음과 같이 8.3

형식 이름을 생성합니다.

- 이름이 6자를 초과하면 원본 파일 또는 디렉터리 이름이 6자로 잘립니다.
- 잘려서 더 이상 고유하지 않은 파일 또는 디렉토리 이름에 물결표(~)와 숫자(1 - 5)를 추가합니다.

  비슷한 이름이 5개 이상 있어 숫자가 부족하면 원래 이름과 아무런 관계가 없는 고유한 이름이 만들어집니다.

- 파일의 경우 파일 확장명이 3자로 잘립니다.

예를 들어, NFS 클라이언트가 'specifications.html'이라는 파일을 생성할 경우 ONTAP에서 생성한 8.3 형식 파일 이름은 'specif~1.htm'입니다. 이 이름이 이미 있는 경우 ONTAP에서는 파일 이름 끝에 다른 번호를 사용합니다. 예를 들어, NFS 클라이언트가 'specifications_new.html'이라는 다른 파일을 만들 경우 'specifications_new.html'의 8.3 형식은 'specif~2.htm'입니다.

ONTAP SMB 다중 바이트 파일**,** 디렉토리 및 **qtree** 이름에 대해 알아보세요

ONTAP 9.5부터 4바이트 UTF-8 인코딩 이름을 지원하므로 BMP(기본 다국어 플레인) 외부의 유니코드 보조 문자를 포함하는 파일, 디렉터리 및 트리 이름을 만들고 표시할 수 있습니다. 이전 릴리스에서는 이러한 보조 문자가 멀티 프로토콜 환경에서 올바르게 표시되지 않았습니다.

4바이트 UTF-8 인코딩된 이름을 지원하기 위해 새 _utf8mb4_language 코드를 "vserver" 및 "volume" 명령 제품군에 사용할 수 있습니다.

다음 방법 중 하나로 새 볼륨을 만들어야 합니다.

- 볼륨 '-language' 옵션을 명시적으로 설정하는 것은 'volume create-language utf8mb4{…}'입니다
- 옵션을 위해 생성되거나 수정된 SVM에서 볼륨 '-language' 옵션을 상속합니다: 'vserver[create|modify] -language utf8mb4{…}"volume create{…}'
- ONTAP 9.6 이하 버전에서는 utf8mb4 지원을 위한 기존 볼륨을 수정할 수 없습니다. 새로운 utf8mb4 지원 볼륨을 생성한 다음 클라이언트 기반 복사 툴을 사용하여 데이터를 마이그레이션해야 합니다.

  utf8mb4 지원을 위해 SVM을 업데이트할 수 있지만 기존 볼륨에 원래 언어 코드가 유지됩니다.

  ONTAP 9.7P1 이상을 사용 중인 경우 지원 요청을 통해 utf8mb4에 대한 기존 볼륨을 수정할 수 있습니다. 자세한 내용은 을 참조하십시오 "ONTAP에서 생성한 후 볼륨 언어를 변경할 수 있습니까?".

- ONTAP 9.8부터 를 사용할 수 있습니다 `[-language <Language code>]` 볼륨 언어를 *.utf-8에서 utf8mb4로 변경하는 매개 변수입니다. 볼륨의 언어를 변경하려면 에 문의하십시오 "NetApp 지원".

> 4바이트 UTF-8 문자를 사용하는 LUN 이름은 현재 지원되지 않습니다.

- 유니코드 문자 데이터는 일반적으로 16비트 UTF-16(Unicode Transformation Format)을 사용하는 Windows 파일 시스템 응용 프로그램과 8비트 UTF-8(Unicode Transformation Format)을 사용하는 NFS 파일 시스템에 표시됩니다.

  ONTAP 9.5 이전 버전에서는 Windows 클라이언트에서 생성한 UTF-16 보조 문자를 포함한 이름이 다른 Windows 클라이언트에 올바르게 표시되었지만 NFS 클라이언트용 UTF-8로 올바르게 변환되지 않았습니다. 마찬가지로, 생성된 NFS 클라이언트에서 UTF-8 보완 문자를 사용하는 이름은 Windows 클라이언트의 UTF-16으로 올바르게 변환되지 않았습니다.

- ONTAP 9.4 이하를 실행하는 시스템에서 유효하거나 잘못된 보조 문자가 포함된 파일 이름을 만들면 ONTAP가 파일 이름을 거부하고 잘못된 파일 이름 오류를 반환합니다.

  이 문제를 방지하려면 파일 이름에 BMP 문자만 사용하고 보조 문자는 사용하지 마십시오. 또는 ONTAP 9.5 이상으로 업그레이드하십시오.

ONTAP 9부터는 qtree 이름에 유니코드 문자가 허용됩니다.

- 'volume qtree' 명령군 또는 System Manager를 사용하여 qtree 이름을 설정하거나 수정할 수 있습니다.
- Qtree 이름에는 일본어 및 중국어 문자와 같은 유니코드 형식의 멀티바이트 문자가 포함될 수 있습니다.
- ONTAP 9.5 이전 버전에서는 BMP 문자(즉, 3바이트로 표현될 수 있는 문자)만 지원되었습니다.

> ONTAP 9.5 이전의 릴리즈에서는 qtree 상위 볼륨의 연결 경로에 유니코드 문자가 있는 qtree 및 디렉토리 이름이 포함될 수 있습니다. 볼륨 표시 명령은 상위 볼륨에 UTF-8 언어 설정이 있는 경우 이러한 이름을 올바르게 표시합니다. 그러나 상위 볼륨 언어가 UTF-8 언어 설정 중 하나가 아닌 경우 junction-path의 일부 부분은 숫자 NFS 대체 이름을 사용하여 표시됩니다.

- 9.5 이상 릴리즈에서는 qtree 이름이 qtree 이름으로 지원되지만 qtree가 utf8mb4에 대해 활성화된 볼륨에 있습니다.

볼륨에서 **ONTAP SMB** 파일 이름 변환을 위한 문자 매핑 구성

NFS 클라이언트는 SMB 클라이언트 및 특정 Windows 애플리케이션에 유효하지 않은 문자를 포함하는 파일 이름을 생성할 수 있습니다. SMB 클라이언트가 유효하지 않은 NFS 이름의 파일에 액세스할 수 있도록 볼륨의 파일 이름 변환에 대한 문자 매핑을 구성할 수 있습니다.

이 작업에 대해

NFS 클라이언트가 생성한 파일을 SMB 클라이언트가 액세스할 때 ONTAP는 파일 이름을 찾습니다. 이름이 유효한 SMB 파일 이름이 아닌 경우(예: 포함된 콜론 "":" 문자가 있는 경우) ONTAP는 각 파일에 대해 유지되는 8.3 파일 이름을 반환합니다. 그러나 이로 인해 중요한 정보를 긴 파일 이름으로 인코딩하는 응용 프로그램에 문제가 발생합니다.

따라서 다른 운영 체제의 클라이언트 간에 파일을 공유하는 경우 두 운영 체제 모두에서 유효한 파일 이름에 문자를 사용해야 합니다.

그러나 SMB 클라이언트에 대해 유효한 파일 이름이 아닌 문자를 포함하는 파일 이름을 생성하는 NFS 클라이언트가 있는 경우, 잘못된 NFS 문자를 SMB 및 특정 Windows 애플리케이션이 허용하는 유니코드 문자로 변환하는 맵을 정의할 수 있습니다. 예를 들어, 이 기능은 CATIA MCAD 및 Mathematica 응용 프로그램과 이 요구 사항이 있는 다른 응용 프로그램을 지원합니다.

볼륨별로 문자 매핑을 구성할 수 있습니다.

볼륨에 문자 매핑을 구성할 때 다음 사항을 염두에 두어야 합니다.

- 문자 매핑이 교차점에 적용되지 않습니다.

  각 접합 볼륨에 대해 문자 매핑을 명시적으로 구성해야 합니다.

- 올바르지 않거나 잘못된 문자를 나타내는 데 사용되는 유니코드 문자가 파일 이름에 일반적으로 나타나지 않는 문자인지 확인해야 합니다. 그렇지 않으면 원치 않는 매핑이 발생합니다.

예를 들어 콜론(:)을 하이픈(-)에 매핑하려고 하지만 파일 이름에 하이픈(-)이 올바르게 사용된 경우 ""a-b""라는 파일에 액세스하려는 Windows 클라이언트의 요청이 ""a:b""(원하는 결과가 아님)의 NFS 이름에 매핑됩니다.

- 문자 매핑을 적용한 후에도 매핑에 여전히 잘못된 Windows 문자가 포함되어 있으면 ONTAP는 Windows 8.3 파일 이름으로 다시 돌아갑니다.
- FPolicy 알림, NAS 감사 로그, 보안 추적 메시지에 매핑된 파일 이름이 표시됩니다.
- DP 유형의 SnapMirror 관계가 생성될 때 소스 볼륨의 문자 매핑이 대상 DP 볼륨에 복제되지 않습니다.
- 대소문자 구분: 매핑된 Windows 이름이 NFS 이름으로 전환되기 때문에 이름 조회는 NFS 의미를 따릅니다. 여기에는 NFS 조회가 대/소문자를 구분한다는 사실도 포함됩니다. 즉, 매핑된 공유에 액세스하는 응용 프로그램이 대/소문자를 구분하지 않는 Windows 동작에 의존해서는 안 됩니다. 그러나 8.3 이름은 사용할 수 있으며 대/소문자를 구분하지 않습니다.
- 부분 매핑 또는 잘못된 매핑: 이름을 매핑하여 디렉터리 열거("dir")를 수행하는 클라이언트로 반환하면 결과 유니코드 이름이 Windows 유효성을 검사합니다. 이름에 여전히 잘못된 문자가 있거나 Windows에 유효하지 않은 경우(예: "." 또는 공백으로 끝나는 경우) 잘못된 이름 대신 8.3 이름이 반환됩니다.

단계

1. 문자 매핑 구성: +

"vserver cifs character-mapping create -vserver_vserver_name_-volume_volume_name_ -mapping_mapping_text_,… 를 누릅니다

매핑은 "":"로 구분된 소스-타겟 문자 쌍 목록으로 구성됩니다. 문자는 16진수를 사용하여 입력한 유니코드 문자입니다. 예: 3C:E03C. 를 누릅니다

콜론으로 구분된 각 mapping_text 쌍의 첫 번째 값은 번역할 NFS 문자의 16진수 값이고 두 번째 값은 SMB가 사용하는 유니코드 값입니다. 매핑 쌍은 고유해야 합니다(일대일 매핑이 있어야 함).

- 소스 매핑+

다음 표에서는 소스 매핑에 사용할 수 있는 유니코드 문자 집합을 보여 줍니다.

를 누릅니다

유니코드 문자입니다	인쇄된 문자	설명
0x01-0x19	해당 없음	인쇄할 수 없는 제어 문자입니다
0x5C		백슬래시
0x3A	:	결장
0x2A	*	별표
0x3F	?	물음표
0x22	"	인용 부호가 있습니다

유니코드 문자입니다	인쇄된 문자	설명
0x3C	를 누릅니다	보다 작음
0x3E	를 누릅니다	보다 큼
0x7C		
세로선	0xB1	±

- 타겟 매핑

  U+E0000…U+F8FF 범위의 유니코드 "전용 용도 영역"에서 대상 문자를 지정할 수 있습니다.

예

다음 명령을 실행하면 SVM(스토리지 가상 시스템) VS1 에서 "data"라는 이름의 볼륨에 대한 문자 매핑이 생성됩니다.

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

관련 정보

네임스페이스에서 데이터 볼륨을 만들고 관리하는 방법에 대해 알아보세요.

SMB 파일 이름 변환을 위한 문자 매핑을 관리하기 위한 **ONTAP** 명령

FlexVol 볼륨에서 SMB 파일 이름 변환에 사용되는 파일 문자 매핑을 생성, 수정, 정보 표시 또는 삭제하여 문자 매핑을 관리할 수 있습니다.

원하는 작업	이 명령 사용…
새 파일 문자 매핑을 만듭니다	'vserver cifs character-mapping create'
파일 문자 매핑에 대한 정보를 표시합니다	'vserver cifs character-mapping show'
기존 파일 문자 매핑을 수정합니다	'vserver cifs character-mapping modify'를 참조하십시오
파일 문자 매핑을 삭제합니다	'vserver cifs character-mapping delete

에 대한 자세한 내용은 `vserver cifs character-mapping` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

볼륨에서 파일 이름 번역을 위한 문자 매핑 구성

NAS 데이터에 S3 클라이언트 액세스 제공

ONTAP S3 멀티프로토콜 지원에 대해 알아보세요

ONTAP 9.12.1부터는 S3 프로토콜을 실행하는 클라이언트가 다시 포맷하지 않고 NFS 및 SMB 프로토콜을 사용하는 클라이언트에 제공되는 동일한 데이터에 액세스할 수 있도록 설정할 수 있습니다. 이 기능을 사용하면 NAS 클라이언트에서 NAS 데이터를 계속 처리하는 동시에 S3 애플리케이션(예: 데이터 마이닝 및 인공 지능)을 실행하는 S3 클라이언트에 오브젝트 데이터를 제공할 수 있습니다.

S3 멀티 프로토콜 기능은 다음과 같은 두 가지 사용 사례를 해결합니다.

1. S3 클라이언트를 사용하여 기존 NAS 데이터에 액세스

   기존 데이터가 기존 NAS 클라이언트(NFS 또는 SMB)를 사용하여 생성되었고 NAS 볼륨(FlexVol 또는 FlexGroup 볼륨)에 있는 경우 S3 클라이언트의 분석 도구를 사용하여 이 데이터에 액세스할 수 있습니다.

2. NAS 및 S3 프로토콜을 모두 사용하여 I/O를 수행할 수 있는 최신 클라이언트를 위한 백엔드 스토리지

   NAS와 S3 프로토콜을 모두 사용하여 동일한 데이터를 읽고 쓸 수 있는 Spark 및 Kafka와 같은 애플리케이션에 통합 액세스를 제공할 수 있습니다.

S3 멀티프로토콜 지원 작동 방식

ONTAP 멀티프로토콜 지원을 통해 동일한 데이터 세트를 파일 계층 구조나 버킷의 객체로 표현할 수 있습니다. 이를 위해 ONTAP S3 클라이언트가 S3 객체 요청을 사용하여 NAS 스토리지에서 파일을 생성, 읽기, 삭제 및 열거할 수 있도록 하는 "S3 NAS 버킷"을 생성합니다. 이 매핑은 NAS 보안 구성을 준수하며, 파일 및 디렉터리 액세스 권한을 관찰하고 필요에 따라 보안 감사 추적에 기록합니다.

이 매핑은 지정된 NAS 디렉토리 계층을 S3 버킷으로 제공하여 수행됩니다. 디렉토리 계층의 각 파일은 이름이 매핑된 디렉토리에서 상대적으로 아래로 내려가는 S3 오브젝트로 표시되며 디렉토리 경계는 슬래시 문자('/')로 표시됩니다.

ONTAP 정의 S3 사용자는 NAS 디렉토리에 매핑되는 버킷에 정의된 버킷 정책에 따라 제어되는 이 스토리지에 액세스할 수 있습니다. 이를 위해서는 S3 사용자와 SMB/NFS 사용자 간에 매핑을 정의해야 합니다. SMB/NFS 사용자의 자격 증명은 NAS 권한 확인에 사용되며 이러한 액세스로 인해 발생하는 모든 감사 레코드에 포함됩니다.

SMB 또는 NFS 클라이언트가 파일을 생성하면 파일이 디렉토리에 즉시 배치되므로 데이터가 쓰기 전에 클라이언트에 표시됩니다. S3 클라이언트는 모든 데이터가 기록될 때까지 새 오브젝트가 네임스페이스에 표시되지 않는 다른 의미를 기대합니다. S3를 NAS 스토리지에 매핑하는 방식은 S3 의미를 사용하여 파일을 생성하므로 S3 생성 명령이 완료될 때까지 파일을 외부적으로 볼 수 없습니다.

S3 NAS 버킷 용 데이터 보호

S3 NAS "버킷"은 단순히 S3 클라이언트를 위한 NAS 데이터의 매핑일 뿐이며, 표준 S3 버킷이 아닙니다. 따라서 NetApp SnapMirror S3 기능을 사용하여 S3 NAS 버킷을 보호할 필요가 없습니다. 대신 SnapMirror 비동기 볼륨

복제를 사용하여 S3 NAS 버킷이 포함된 볼륨을 보호할 수 있습니다. SnapMirror 동기 및 SVM 재해 복구는 지원되지 않습니다.

ONTAP 9.14.1부터, MetroCluster IP 및 FC 구성을 위한 미러링된 애그리게이트 및 미러링되지 않은 애그리게이트에서 S3 NAS 버킷이 지원됩니다.

에 대해 자세히 "SnapMirror 비동기"알아보십시오.

S3 NAS 버킷에 대한 감사

S3 NAS 버킷은 기존의 S3 버킷이 아니므로 액세스 감사를 위해 S3 감사를 구성할 수 없습니다. 에 대해 자세히 알아보십시오 "S3 감사".

그럼에도 불구하고 S3 NAS 버킷에 매핑된 NAS 파일 및 디렉토리는 기존의 ONTAP 감사 절차를 사용하여 액세스 이벤트에 대한 감사를 수행할 수 있습니다. 따라서 S3 작업은 다음과 같은 예외를 제외하고 NAS 감사 이벤트를 트리거할 수 있습니다.

- S3 정책 구성(그룹 또는 버킷 정책)에 의해 S3 클라이언트 액세스가 거부되면 이벤트에 대한 NAS 감사가 시작되지 않습니다. 이는 SVM 감사 점검을 수행하기 전에 S3 권한을 확인하기 때문입니다.
- S3 GET 요청의 타겟 파일이 0 크기인 경우 0개의 콘텐츠가 GET 요청으로 반환되고 읽기 액세스가 기록되지 않습니다.
- S3 GET 요청의 타겟 파일이 사용자에게 통과 권한이 없는 폴더에 있는 경우 액세스 시도가 실패하고 이벤트가 기록되지 않습니다.

에 대해 자세히 알아보십시오 "SVM에서 NAS 이벤트 감사".

개체 다중 파트 업로드

ONTAP 9.16.1부터 기본 FlexGroup 볼륨에서 을 사용하도록 설정한 경우 S3 NAS 버킷에서 오브젝트 다중 부분 업로드가 "고급 용량 밸런싱"지원됩니다.

NAS 파일 스토리지에서 오브젝트 다중 부분 업로드를 사용하면 S3 프로토콜 클라이언트가 큰 오브젝트를 더 작은 부분으로 업로드할 수 있습니다. 개체 다중 파트 업로드에는 다음과 같은 이점이 있습니다.

- 객체를 병렬로 업로드할 수 있습니다.
- 업로드가 실패하거나 일시 중지되는 경우 아직 업로드되지 않은 부분만 업로드해야 합니다. 전체 개체의 업로드를 다시 시작할 필요가 없습니다.
- 개체 크기를 미리 알 수 없는 경우(예: 큰 개체가 아직 작성되는 경우), 클라이언트는 개체의 일부를 즉시 업로드하고 전체 개체가 생성된 후 업로드를 완료할 수 있습니다.

S3 NAS 버킷의 멀티파트 객체는 부분 크기가 아닌 정수 크기로 정렬되어야 합니다. 예를 들어, 파트는 4MB 또는 4GB 또는 이와 유사한 크기일 수 있습니다. 파트는 4.5MB 또는 4000.5MB와 같이 부분 크기 또는 MB 미만의 크기를 사용할 수 없습니다.

멀티파트 업로드는 다음 S3 작업을 지원합니다.

- AbortMultipartUpload 를 클릭합니다
- CompleteMultipartUpload를 클릭합니다
- CopyObject(ONTAP 9.17.1부터)

- CreateMultptUpload 를 클릭합니다

  ONTAP 9.17.1부터 CreateMultipartUpload는 태그 지정과 사용자 메타데이터 키/값 쌍을 지원합니다.

- ListMultipartUpload 를 클릭합니다
- 업로드 파트

> 부품 번호로 가져오기("PARTNUMBER=xx")는 S3 NAS 버킷에서 지원되지 않습니다. 대신 전체 개체가 반환됩니다.

S3 및 **NAS** 상호 운용성

ONTAP S3 NAS 버킷은 여기에 나열된 기능을 제외한 표준 NAS 및 S3 기능을 지원합니다.

NAS 기능은 현재 **S3 NAS** 버킷에서 지원되지 않습니다

FabricPool 용량 계층입니다

S3 NAS 버킷을 FabricPool의 용량 계층으로 구성할 수 없습니다.

현재 **S3 NAS** 버킷에서 지원되지 않는 **S3** 작업 및 기능

작업

- ByPassGovernanceRetention 을 참조하십시오
- DeleteBucketLifecycleConfiguration을 참조하십시오
- GetBuckLifecycleConfiguration 을 참조하십시오
- GetBucketObjectLockConfiguration 을 참조하십시오
- GetBuckketVersioning 을 참조하십시오
- GetObjectRetention을 참조하십시오
- ListBuckketVersioning을 참조하십시오
- ListObjectVersions 를 선택합니다
- PutBucketLifecycleConfiguration을 참조하십시오
- PutBucketVersioning을 참조하십시오
- PutObjectLockConfiguration 을 참조하십시오
- PutObjectRetention

> 이러한 S3 작업은 S3 NAS 버킷에서 S3를 사용하는 경우 특별히 지원되지 않습니다. 네이티브 S3 버킷을 사용할 때 이러한 작업은 다음과 "정상적으로 지원됩니다"같습니다.

AWS 사용자 메타데이터

- ONTAP 9.17.1부터 다중 파트 객체가 포함된 메타데이터가 지원됩니다.
- ONTAP 9.16.1 버전부터 단일 파트 객체의 메타데이터를 지원합니다.
- ONTAP 9.15.1 이하 버전의 경우 S3 사용자 메타데이터의 일부로 수신된 키 값 쌍이 오브젝트 데이터와 함께 디스크에 저장되지 않습니다.

- ONTAP 9.15.1 이하 버전의 경우 접두사가 "x-amz-meta"인 요청 헤더는 무시됩니다.

AWS 태그

- ONTAP 9.17.1부터 다중 파트 객체가 있는 태그가 지원됩니다.
- ONTAP 9.16.1 버전부터 단일 파트 객체를 포함하는 태그를 지원합니다.
- ONTAP 9.15.1 이하 버전의 PUT 객체 및 Multipart Initiate 요청에서는 접두사 "x-amz-tagging"이 있는 헤더가 무시됩니다.
- ONTAP 9.15.1 이하 버전의 경우 기존 파일에 대한 태그 업데이트 요청(?태깅 쿼리 문자열을 사용한 PUT, GET 및 삭제 요청)이 오류로 거부됩니다.

버전 관리

버킷 매핑 구성에서는 버전 관리를 지정할 수 없습니다.

- null이 아닌 버전 사양(versionId=xyz 쿼리 문자열)이 포함된 요청은 오류 응답을 받습니다.
- 버킷의 버전 관리 상태에 영향을 주는 요청은 오류와 함께 거부됩니다.

ONTAP S3 클라이언트 액세스를 위한 NAS 데이터 요구 사항에 대해 알아보세요.

S3 액세스를 위해 NAS 파일 및 디렉토리를 매핑할 때 몇 가지 고유한 비호환성이 있다는 것을 이해하는 것이 중요합니다. S3 NAS 버킷을 사용하여 NAS 파일 계층을 서비스하기 전에 NAS 파일 계층을 조정해야 할 수 있습니다.

S3 NAS 버킷은 S3 버킷 구문을 사용하여 해당 디렉토리를 매핑함으로써 NAS 디렉토리에 대한 S3 액세스를 제공하며 디렉토리 트리의 파일은 오브젝트로 표시됩니다. 오브젝트 이름은 S3 버킷 구성에 지정된 디렉토리를 기준으로 파일의 슬래시로 구분된 경로 이름입니다.

이 매핑에서는 S3 NAS 버킷을 사용하여 파일 및 디렉토리를 제공할 경우 다음과 같은 몇 가지 요구사항이 발생합니다.

- S3 이름은 1024바이트로 제한되므로 S3를 사용하면 경로 이름이 더 긴 파일에 액세스할 수 없습니다.
- 파일 및 디렉터리 이름은 255자로 제한되므로 개체 이름은 255자 이하의 연속된 비슬래시('/') 문자를 사용할 수 없습니다
- 백슬래시('\') 문자로 구분된 SMB 경로 이름은 S3에 슬래시('/') 문자를 포함하는 객체 이름으로 표시됩니다.
- 일부 합법적인 S3 객체 이름 쌍은 매핑된 NAS 디렉토리 트리에서 공존할 수 없습니다. 예를 들어, 합법적인 S3 객체 이름인 "part1/part2"와 "part1/part2/part3"은 NAS 디렉토리 트리에 동시에 존재할 수 없는 파일에 매핑됩니다. "part1/part2"는 첫 번째 이름에서는 파일이고 다른 이름에서는 디렉토리이기 때문입니다.
  - "part1/part2"가 기존 파일인 경우 S3에서 "part1/part2/part3"을 생성하는 데 실패합니다.
  - "part1/part2/part3"이 기존 파일인 경우 S3에서 "part1/part2"를 생성하거나 삭제하면 실패합니다.
  - 기존 오브젝트의 이름과 일치하는 S3 오브젝트 생성은 NAS에 있지만 정확히 일치해야 하는 기존 오브젝트(버전이 지정되지 않은 버킷)를 대체합니다. 위의 예제에서는 이름이 충돌하는 동안 이름이 일치하지 않으므로 기존 개체를 제거하지 않습니다.

객체 저장소는 매우 많은 수의 임의의 이름을 지원하도록 설계되었지만, NAS 디렉토리 구조는 매우 많은 수의 이름이 하나의 디렉토리에 저장되면 성능 문제가 발생할 수 있습니다. 특히, 슬래시('/') 문자가 없는 이름은 모두 NAS 매핑의 루트 디렉토리에 배치됩니다. "NAS 친화적"이지 않은 이름을 광범위하게 사용하는 애플리케이션은 NAS 매핑보다는 실제 객체 저장소 버킷에 호스팅하는 것이 더 좋습니다.

ONTAP SVM에서 NAS 데이터에 대한 S3 프로토콜 액세스 활성화

S3 프로토콜 액세스를 활성화하려면 NAS 지원 SVM이 오브젝트 저장소 서버 추가, 네트워킹 및 인증 요구사항 확인을 포함하여 S3 지원 서버와 동일한 요구사항을 충족하는지 확인해야 합니다.

새로운 ONTAP 설치의 경우 NAS 데이터를 클라이언트에 제공하도록 구성한 후 SVM에 대한 S3 프로토콜 액세스를 지원하는 것이 좋습니다. NAS 프로토콜 구성에 대한 자세한 내용은 다음을 참조하십시오.

- "NFS 구성"
- "SMB 구성"

시작하기 전에

S3 프로토콜을 활성화하기 전에 다음을 구성해야 합니다.

- S3 프로토콜과 NFS, SMB 또는 둘 다에 대한 라이센스가 필요합니다.
- SVM은 원하는 NAS 프로토콜을 위해 구성됩니다.
- NFS 및/또는 SMB 서버가 존재합니다.
- DNS 및 기타 필요한 서비스가 구성됩니다.
- NAS 데이터를 클라이언트 시스템으로 내보내거나 공유 중입니다.

이 작업에 대해

S3 클라이언트에서 S3 기반 SVM으로 HTTPS 트래픽을 활성화하려면 CA(인증 기관) 인증서가 필요합니다. 다음 세 소스의 CA 인증서를 사용할 수 있습니다.

- SVM에서 자체 서명된 새로운 ONTAP 인증서
- SVM에 자체 서명된 기존 ONTAP 인증서
- 타사 인증서입니다.

NAS 데이터 제공에 사용하는 S3/NAS 버킷에 동일한 데이터 LIF를 사용할 수 있습니다. 특정 IP 주소가 필요한 경우 를 참조하십시오 "데이터 LIF 생성". LIF에서 S3 데이터 트래픽을 활성화하려면 S3 서비스 데이터 정책이 필요합니다. S3를 포함하도록 SVM의 기존 서비스 정책을 수정할 수 있습니다.

S3 오브젝트 서버를 생성할 때 S3 서버 이름을 클라이언트가 S3 액세스에 사용할 FQDN(정규화된 도메인 이름)으로 입력할 준비를 해야 합니다. S3 서버 FQDN은 버킷 이름으로 시작하지 않아야 합니다.

시스템 관리자

1. NAS 프로토콜이 구성된 스토리지 VM에서 S3를 설정합니다.
   a. 스토리지 > 스토리지 VM * 을 클릭하고 NAS 지원 스토리지 VM을 선택한 다음 설정 을 클릭하고 S3 아래를 클릭합니다 .
   b. 인증서 유형을 선택합니다. 시스템에서 생성한 인증서 또는 사용자 인증서 중 하나를 선택하든 클라이언트 액세스에 필요합니다.
   c. 네트워크 인터페이스를 입력합니다.
2. 시스템에서 생성한 인증서를 선택한 경우 새 스토리지 VM 생성이 확인되면 인증서 정보가 표시됩니다. 다운로드 * 를 클릭하고 클라이언트 액세스를 위해 저장합니다.
   ◦ 비밀 키는 다시 표시되지 않습니다.
   ◦ 인증서 정보가 다시 필요한 경우 * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭합니다.

CLI를 참조하십시오

1. SVM에서 S3 프로토콜이 허용되는지 확인합니다.
   `vserver show -fields allowed-protocols`
2. 이 SVM에 대한 공개 키 인증서를 기록합니다. + 새로운 ONTAP 자체 서명 인증서가 필요한 경우 를 참조하십시오 "SVM에서 CA 인증서를 생성하고 설치합니다".
3. 서비스 데이터 정책을 업데이트합니다
   a. SVM+에 대한 서비스 데이터 정책을 표시합니다
      `network interface service-policy show -vserver svm_name`

      에 대한 자세한 내용은 `network interface service-policy show` "ONTAP 명령 참조입니다 "을 참조하십시오.

   b. 및 가 없는 경우 를 `data-core` `data-s3-server services` 추가합니다.
      `network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server`
4. SVM에 있는 데이터 LIF가 귀사의 요구사항을 충족하는지 확인하십시오.
   `network interface show -vserver svm_name`

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

5. S3 서버 생성:
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

S3 서버를 생성할 때 또는 나중에 언제든지 추가 옵션을 지정할 수 있습니다.

- HTTPS는 기본적으로 포트 443에서 활성화됩니다. secure-listener-port 옵션을 사용하여 포트 번호를 변경할 수 있습니다. 를 누릅니다
  HTTPS가 활성화된 경우 SSL/TLS와의 올바른 통합을 위해 CA 인증서가 필요합니다. ONTAP 9.15.1부터 TLS 1.3은 S3 오브젝트 스토리지에서 지원됩니다.
- HTTP는 기본적으로 사용되지 않으며, 이 옵션을 설정하면 서버가 포트 80에서 수신 대기합니다. is-http-

enabled 옵션을 사용하여 설정하거나 -listener-port 옵션을 사용하여 포트 번호를 변경할 수 있습니다. + HTTP가 활성화되면 모든 요청과 응답이 일반 텍스트로 네트워크를 통해 전송됩니다.

1. S3이 원하는 대로 구성되었는지 확인합니다
   `vserver object-store-server show`

- example * + 다음 명령은 모든 오브젝트 스토리지 서버의 구성 값을 확인합니다.
  `cluster1::> vserver object-store-server show`

```
Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                 Secure Listener Port For HTTPS: 443
                                   HTTP Enabled: false
                                  HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

관련 정보

- "네트워크 인터페이스 서비스 정책 추가 서비스"

ONTAP S3 NAS 버킷 생성

S3 NAS 버킷은 S3 버킷 이름과 NAS 경로를 매핑한 것입니다. S3 NAS 버킷을 사용하면 기존 볼륨과 디렉터리 구조를 가진 SVM 네임스페이스의 모든 부분에 대한 S3 액세스를 제공할 수 있습니다.

시작하기 전에

- S3 오브젝트 서버는 NAS 데이터를 포함하는 SVM으로 구성됩니다.
- NAS 데이터는 에 부합합니다 "S3 클라이언트 액세스에 대한 요구 사항".

이 작업에 대해

SVM의 루트 디렉토리 내에 모든 파일 및 디렉토리 세트를 지정하도록 S3 NAS 버킷을 구성할 수 있습니다.

다음 매개 변수의 조합을 기반으로 NAS 데이터에 대한 액세스를 허용하거나 허용하지 않는 버킷 정책을 설정할 수도 있습니다.

- 파일 및 디렉터리
- 사용자 및 그룹 권한
- S3 작업

예를 들어, 많은 사용자에게 읽기 전용 데이터 액세스 권한을 부여하는 버킷 정책과, 제한된 사용자 그룹이 해당 데이터의 일부에 대해 작업을 수행할 수 있도록 허용하는 또 다른 버킷 정책을 설정할 수 있습니다.

ONTAP 9.18.1부터 애플리케이션이 S3 프로토콜을 사용하여 FlexCache 볼륨의 데이터에 액세스할 수 있도록 하는 NAS 버킷을 생성할 수 있습니다. 클러스터의 모든 노드는 ONTAP 9.18.1 이상을 실행해야 합니다. S3 프로토콜을 사용하여 FlexCache 볼륨에 액세스하려면 먼저 `-is-s3-enabled` 옵션을 `true` "FlexCache 볼륨에서"로 설정해야 합니다. 이 매개변수는 기본적으로 `false`로 설정되어 있습니다.

ONTAP 9.17.1부터 S3 NAS 버킷을 연결 경로가 아닌 볼륨에 직접 연결할 수 있습니다. 기본적으로 NAS 볼륨의 S3 버킷은 연결 경로와 연결되며, ONTAP 관리자는 언제든지 이 경로를 변경할 수 있습니다. 이러한 변경으로 인해 S3 버킷 작업이 중단될 수 있습니다. ONTAP 9.17.1부터는 `-is-nas-path-mutable false` 옵션과 함께 `vserver object-store-server bucket create` ONTAP CLI에서 명령을 사용하여 S3 NAS 버킷을 볼륨에 연결할 수 있습니다. 기본적으로 `-is-nas-path-mutable` 로 설정됩니다 `true` .

S3 NAS "버킷"은 매핑이지 S3 버킷이 아니므로 표준 S3 버킷의 다음 속성은 S3 NAS 버킷에 적용되지 않습니다.

- * aggr-list\aggr-list-multiplier\storage-service-level\volume\size\exclude-aggr-list\QoS-policy-group * + S3 NAS 버킷을 구성할 때 볼륨 또는 qtree가 생성되지 않습니다.
- 역할 \은 **-protected**입니다 \은 **-protected-on-ontap**입니다 \은 **-protected-on-cloud**입니다 + S3 NAS 버킷은 SnapMirror S3를 사용하여 보호되거나 미러링되지 않고 대신 볼륨 세분성에서 사용 가능한 일반 SnapMirror 보호 기능을 사용합니다.
- **versioning-state**+ NAS 볼륨에는 일반적으로 다른 버전을 저장할 수 있는 스냅샷 기술이 있습니다. 그러나 버전 관리는 현재 S3 NAS 버킷에서 사용할 수 없습니다.
- 볼륨 명령을 통해 NAS 볼륨에 대해 * logical-used\object-count * + 등가 통계를 사용할 수 있습니다.
- **multipart** 객체 + ONTAP 9.16.1부터 S3 NAS 버킷에서 multipart 객체가 지원됩니다. "고급 용량 밸런싱" 기본 FlexGroup 볼륨에서 활성화되어 있습니다. 고급 용량 분산은 FlexGroup 볼륨에서만 활성화할 수 있습니다. FlexVol 볼륨에서는 활성화할 수 없습니다.

단계

시스템 관리자나 ONTAP CLI를 사용하여 NAS 버킷을 생성할 수 있습니다.

시스템 관리자

NAS가 활성화된 스토리지 VM에 새 S3 NAS 버킷을 추가합니다.

1. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
2. S3 NAS 버킷의 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력하지 말고 * More Options * 를 클릭합니다.
3. 유효한 경로 이름을 입력하거나 찾아보기를 클릭하여 유효한 경로 이름 목록에서 선택합니다. + 올바른 경로 이름을 입력하면 S3 NAS 구성과 관련이 없는 옵션이 숨겨집니다.
4. S3 사용자를 NAS 사용자 및 생성된 그룹에 이미 매핑한 경우 해당 사용 권한을 구성한 다음 * 저장 * 을 클릭합니다. +이 단계에서 사용 권한을 구성하기 전에 S3 사용자를 NAS 사용자에게 이미 매핑해야 합니다.

그렇지 않으면 * 저장 * 을 클릭하여 S3 NAS 버킷 구성을 완료합니다.

CLI를 참조하십시오

1. NAS 파일 시스템이 포함된 SVM에 S3 NAS 버킷을 만듭니다.
   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> -type nas -nas-path <junction_path> -is-nas-path-mutable
   true|false [-comment <text>]
   ```

   예제 1: S3 NAS 버킷 만들기

   ```
   cluster1::> vserver object-store-server bucket create -bucket testbucket
   -type nas -path /vol1
   ```

   예제 2: S3 NAS 버킷을 생성하고 버킷을 볼륨에 연결

   ```
   vserver object-store-server bucket create -vserver vs1 -bucket nasbucket1
   -type nas -nas-path /pathA/dir1 -is-nas-path-mutable false
   ```

ONTAP S3 클라이언트 사용자 활성화

S3 클라이언트 사용자가 NAS 데이터에 액세스할 수 있도록 하려면 S3 사용자 이름을 해당 NAS 사용자에 매핑한 다음 버킷 서비스 정책을 사용하여 NAS 데이터에 대한 액세스 권한을 부여해야 합니다.

시작하기 전에

클라이언트 액세스를 위한 사용자 이름(LINUX/UNIX, Windows 및 S3 클라이언트 사용자)이 이미 존재해야 합니다.

일부 S3 기능은 에 대해 알고 "S3 NAS 버킷에서 지원되지 않음"있어야 합니다.

이 작업에 대해

S3 사용자 이름을 해당 Linux/UNIX 또는 Windows 사용자에게 매핑하면 S3 클라이언트가 NAS 파일에 액세스할 때 NAS 파일에 대한 권한 부여 검사를 수행할 수 있습니다. S3-NAS 매핑은 단일 이름 또는 POSIX 정규식으로 표현될 수 있는 S3 사용자 이름_Pattern_과 Linux/UNIX 또는 Windows 사용자 이름_Replacement_를 제공하여 지정합니다.

이름 매핑이 없는 경우 기본 이름 매핑이 사용됩니다. 여기서 S3 사용자 이름 자체는 UNIX 사용자 이름 및 Windows

사용자 이름으로 사용됩니다. 를 사용하여 UNIX 및 Windows 기본 사용자 이름 매핑을 수정할 수 있습니다 `vserver object-store-server modify` 명령.

로컬 이름 매핑 구성만 지원되며 LDAP는 지원되지 않습니다.

S3 사용자를 NAS 사용자에게 매핑한 후에는 액세스 권한이 있는 리소스(디렉토리 및 파일)와 해당 사용자가 액세스할 수 있거나 수행할 수 없는 작업을 지정하는 권한을 사용자에게 부여할 수 있습니다.

시스템 관리자

1. UNIX 또는 Windows 클라이언트(또는 둘 다)에 대한 로컬 이름 매핑을 생성합니다.
   a. 스토리지 > 버킷 * 을 클릭한 다음 S3/NAS 지원 스토리지 VM을 선택합니다.
   b. Settings * 를 선택한 다음 * Name Mapping * (* Host Users and Groups * 아래)을 클릭합니다 → .
   c. S3 to Windows * 또는 * S3 to UNIX * 타일(또는 둘 다)에서 * 추가 * 를 클릭한 다음 원하는 * 패턴 * (S3) 및 * 교체 * (NAS) 사용자 이름을 입력합니다.
2. 버킷 정책을 생성하여 클라이언트 액세스를 제공합니다.
   a. 스토리지 > Bucket * 을 클릭하고 원하는 S3 버킷 옆에 있는 을 ⋮ 클릭한 다음 * Edit * 를 클릭합니다.
   b. 추가 * 를 클릭하고 원하는 값을 입력합니다.
      - * Principal * - S3 사용자 이름을 제공하거나 기본값(모든 사용자)을 사용합니다.
      - * 효과 * - * 허용 * 또는 * 거부 * 를 선택합니다.
      - * 조치 * - 이러한 사용자 및 리소스에 대한 조치를 입력합니다. 현재 오브젝트 저장소 서버가 S3 NAS 버킷에 대해 지원하는 리소스 작업 집합은 GetObject , PutObject , DeleteObject , ListBucket , GetBuckketAcl 입니다. GetObjectAcl, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBucketLocation, GetBuckketVersioning, PutBucketVersioning 및 ListBuckketVersions. 이 매개 변수에는 와일드카드를 사용할 수 있습니다.
      - * 리소스 * - 작업이 허용 또는 거부된 폴더나 파일 경로를 입력하거나 기본(버킷의 루트 디렉터리)을 사용합니다.

CLI를 참조하십시오

1. UNIX 또는 Windows 클라이언트(또는 둘 다)에 대한 로컬 이름 매핑을 생성합니다. 를 누릅니다
   `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position integer -pattern s3_user_name -replacement nas_user_name`
   - `-position` 매핑 평가의 우선 순위 번호입니다. 1 또는 2를 입력합니다.
   - `-pattern` - S3 사용자 이름 또는 정규식입니다
   - `-replacement` - Windows 또는 UNIX 사용자 이름입니다

예

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

1. 버킷 정책을 생성하여 클라이언트 액세스를 제공합니다. 를 누릅니다
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` - 사용자가 작업을 요청할 때 액세스를 허용할지 또는 거부할지 여부를 지정합니다.
   - `-action <Action>, …` - 허용되거나 거부되는 리소스 작업을 지정합니다. 개체 저장소 서버에서 S3 NAS 버킷에 대해 현재 지원하는 리소스 작업 집합은 GetObject, PutObject, DeleteObject, ListBucketAcl, GetObjectAcl 및 GetBucketLocation입니다. 이 매개 변수에는 와일드카드를 사용할 수 있습니다.

- `-principal <Objectstore Principal>, …` - 이 매개 변수에 지정된 개체 저장소 서버 사용자 또는 그룹에 대해 액세스를 요청하는 사용자의 유효성을 검사합니다.
  - 개체 저장소 서버 그룹은 그룹 이름에 접두사 그룹 / 을 추가하여 지정합니다.
  - `-principal` -(하이픈 문자)는 모든 사용자에게 액세스 권한을 부여합니다.
- `-resource <text>, …` - 허용/거부 권한이 설정된 버킷, 폴더 또는 개체를 지정합니다. 이 매개 변수에는 와일드카드를 사용할 수 있습니다.
- `[-sid <SID>]` - 오브젝트 저장소 서버 버킷 정책 문에 대한 선택적 텍스트 설명을 지정합니다.

예

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성

Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성 개요

ONTAP 기능을 사용하면 Microsoft Hyper-V와 Microsoft SQL Server라는 SMB 프로토콜을 통해 두 Microsoft 애플리케이션의 무중단 운영을 실현할 수 있습니다.

다음과 같은 상황에서 SMB 무중단 운영을 구현하려는 경우 다음 절차를 따라야 합니다.

- 기본 SMB 프로토콜 파일 액세스가 구성되었습니다.
- SVM에 상주하는 SMB 3.0 이상 파일 공유를 활성화하여 다음 오브젝트를 저장하려고 합니다.
  - Hyper-V 가상 머신 파일
  - SQL Server 시스템 데이터베이스

관련 정보

ONTAP 기술 및 외부 서비스와의 상호 작용에 대한 자세한 내용은 다음 기술 보고서(TR)를 참조하십시오 "NetApp 기술 보고서 4172: ONTAP 모범 사례를 사용한 SMB 3.0 기반 Microsoft Hyper-V".** "NetApp 기술 보고서 4369: clustered Data ONTAP을 사용한 Microsoft SQL Server의 모범 사례 및 SQL Server의 SnapManager 7.2"

SMB 솔루션을 통해 Microsoft Hyper-V 및 SQL Server용 ONTAP를 구성합니다

지속적으로 사용 가능한 SMB 3.0 이상 파일 공유를 사용하여 Hyper-V 가상 머신 파일 또는 SQL Server 시스템 데이터베이스와 사용자 데이터베이스를 SVM에 상주하는 볼륨에 저장하는 동시에 계획된 이벤트와 계획되지 않은 이벤트 모두에 무중단 운영(NDO)을 제공할 수 있습니다.

SMB를 통한 Microsoft Hyper-V

SMB를 통한 Hyper-V 솔루션을 생성하려면 먼저 ONTAP를 구성하여 Microsoft Hyper-V 서버에 스토리지 서비스를 제공해야 합니다. 또한 Microsoft 클러스터(클러스터 구성을 사용하는 경우), Hyper-V 서버, CIFS 서버에서 호스팅하는 공유에 대한 지속적인 SMB 3.0 연결, SVM 볼륨에 저장된 가상 시스템 파일을 보호하기 위한 백업 서비스도 구성해야 합니다.

Hyper-V 서버는 Windows 2012 Server 이상에서 구성해야 합니다. 독립 실행형 및 클러스터링된 Hyper-V 서버 구성이 모두 지원됩니다.

- Microsoft 클러스터 및 Hyper-V 서버 생성에 대한 자세한 내용은 Microsoft 웹 사이트를 참조하십시오.
- SnapManager for Hyper-V는 SMB 구성을 통한 Hyper-V와 통합되도록 설계된 신속한 스냅샷 기반 백업 서비스를 지원하는 호스트 기반 애플리케이션입니다.

  SMB 구성을 통한 Hyper-V에서 SnapManager를 사용하는 방법에 대한 자세한 내용은 _SnapManager for Hyper-V 설치 및 관리 가이드 _ 를 참조하십시오.

SMB를 통한 Microsoft SQL Server

SMB를 통한 SQL Server 솔루션을 생성하려면 먼저 Microsoft SQL Server 애플리케이션에 스토리지 서비스를 제공하도록 ONTAP를 구성해야 합니다. 또한 클러스터된 구성을 사용하는 경우 Microsoft 클러스터도 구성해야 합니다. 그런 다음 Windows 서버에 SQL Server를 설치 및 구성하고 CIFS 서버에서 호스팅하는 공유에 대해 지속적으로 사용 가능한 SMB 3.0 연결을 생성합니다. 필요에 따라 SVM 볼륨에 저장된 데이터베이스 파일을 보호하도록 백업 서비스를 구성할 수 있습니다.

SQL Server는 Windows 2012 Server 이상에서 설치 및 구성해야 합니다. 독립 실행형 구성과 클러스터 구성이 모두 지원됩니다.

- Microsoft 클러스터 만들기 및 SQL Server 설치 및 구성에 대한 자세한 내용은 Microsoft 웹 사이트를 참조하십시오.
- Microsoft SQL Server용 SnapCenter 플러그인은 SMB 구성을 통해 SQL Server와 통합하도록 설계된 호스트 기반 애플리케이션으로, 신속한 스냅샷 기반 백업 서비스를 지원합니다.

  Microsoft SQL Server용 SnapCenter 플러그인 사용에 대한 자세한 내용은 를 참조하십시오 "Microsoft SQL Server용 SnapCenter 플러그인" 문서화:

SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영

Hyper-V 및 SQL Server over SMB의 무중단 운영은 무엇을 의미하는지

SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영은 애플리케이션 서버와 포함된 가상 머신 또는 데이터베이스를 온라인 상태로 유지하고 다양한 관리 작업 중에 지속적인 가용성을 제공할 수 있는 기능의 조합을 의미합니다. 여기에는 스토리지 인프라의 계획된 다운타임과 계획되지 않은 다운타임이 모두 포함됩니다.

SMB를 통해 애플리케이션 서버에서 지원되는 무중단 운영은 다음과 같습니다.

- 계획된 테이크오버 및 반환

- 계획되지 않은 테이크오버
- 업그레이드
- 계획된 애그리게이트 재배치(ARL)
- LIF 마이그레이션 및 페일오버
- 계획된 볼륨 이동

프로토콜을 지원하여 **SMB**를 통해 무중단 운영을 실현합니다

Microsoft는 SMB 3.0 릴리스와 함께 SMB를 통해 Hyper-V 및 SQL Server의 무중단 운영을 지원하는 데 필요한 기능을 제공하는 새로운 프로토콜을 출시했습니다.

ONTAP은 SMB를 통해 애플리케이션 서버에 무중단 운영을 제공할 때 다음과 같은 프로토콜을 사용합니다.

- SMB 3.0
- 증인

SMB를 통한 **Hyper-V** 및 **SQL Server**의 무중단 운영에 대한 주요 개념입니다

SMB 솔루션을 통해 Hyper-V 또는 SQL Server를 구성하기 전에 알아야 하는 무중단 운영(NDO)에 대한 몇 가지 개념이 있습니다.

- * 지속적으로 사용 가능한 공유 *

  지속적으로 사용 가능한 공유 속성이 설정된 SMB 3.0 공유입니다. 지속적으로 사용 가능한 공유를 통해 연결하는 클라이언트는 테이크오버, 반환 및 애그리게이트 재배치와 같은 운영 중단 이벤트를 견딜 수 있습니다.

- * 노드 *

  클러스터의 구성원인 단일 컨트롤러입니다. SFO 쌍의 두 노드를 구별하기 위해 한 노드는 _ local node _ 라고도 하며 다른 노드는 _ partner node _ 또는 _ remote node _ 라고도 합니다. 스토리지의 기본 소유자는 로컬 노드입니다. 기본 소유자가 실패하는 경우 스토리지를 제어하는 보조 소유자가 파트너 노드입니다. 각 노드는 해당 스토리지의 기본 소유자이며 파트너의 스토리지를 위한 2차 소유자입니다.

- * 무중단 애그리게이트 재배치 *

  클라이언트 애플리케이션을 중단하지 않고 클러스터에서 SFO 쌍 내의 파트너 노드 간에 애그리게이트를 이동할 수 있습니다.

- 무중단 페일오버 * 를 지원합니다

  테이크오버를 참조하십시오.

- * 무중단 LIF 마이그레이션 *

  LIF를 통해 클러스터에 연결된 클라이언트 애플리케이션을 중단하지 않고 LIF 마이그레이션을 수행할 수 있습니다. SMB 연결의 경우 SMB 2.0 이상을 사용하여 연결하는 클라이언트에만 가능합니다.

- 무중단 운영 *

주요 ONTAP 관리 및 업그레이드 작업을 수행할 뿐만 아니라 클라이언트 애플리케이션을 중단하지 않고 노드 장애를 견딜 수 있는 기능 이때 무중단 테이크오버, 무중단 업그레이드, 무중단 마이그레이션 기능이 전반적으로 사용됩니다.

- 무중단 업그레이드 *

  애플리케이션 중단 없이 노드 하드웨어 또는 소프트웨어를 업그레이드할 수 있는 기능

- * 무중단 볼륨 이동 *

  볼륨을 사용하는 애플리케이션을 중단하지 않고 클러스터 전체에서 볼륨을 자유롭게 이동할 수 있습니다. SMB 연결의 경우, 모든 버전의 SMB가 무중단 볼륨 이동을 지원합니다.

- * 영구 핸들 *

  연결이 끊길 경우 지속적으로 사용 가능한 연결을 통해 CIFS 서버에 투명하게 다시 연결할 수 있도록 하는 SMB 3.0의 속성입니다. 내구성이 뛰어난 핸들과 마찬가지로 연결 클라이언트와의 통신이 끊긴 후 CIFS 서버가 일정 시간 동안 영구 핸들을 유지합니다. 그러나 지속적인 핸들은 내구성 있는 핸들보다 뛰어난 복원력을 제공합니다. 다시 연결한 후 60초 이내에 클라이언트에서 핸들을 다시 확보할 수 있는 기회를 제공할 뿐 아니라 CIFS 서버는 60초 동안 파일에 대한 액세스를 요청하는 다른 클라이언트에 대한 액세스를 거부합니다.

  영구 핸들에 대한 정보는 SFO 파트너의 영구 스토리지에 미러링되므로, 영구 핸들이 분리된 클라이언트는 SFO 파트너가 노드 스토리지에 대한 소유권을 갖게 된 후 내구성 있는 핸들을 다시 확보할 수 있습니다. 지속적인 핸들은 LIF 이동 시 무중단 운영(내구성이 뛰어난 핸들 지원)을 제공할 뿐만 아니라 테이크오버, 반환 및 애그리게이트 재배치를 위한 무중단 운영을 제공합니다.

- SFO 반환 *

  테이크오버 이벤트에서 복구할 때 애그리게이트를 홈 위치로 반환

- SFO 쌍 *

  두 노드 중 하나가 작동을 중지할 경우 컨트롤러가 상호 데이터를 제공하도록 구성된 노드 쌍입니다. 시스템 모델에 따라 두 컨트롤러 모두 단일 섀시 내에 있거나 컨트롤러가 별도 섀시에 있을 수 있습니다. 2노드 클러스터에서 HA 쌍이라고 합니다.

- * 테이크오버 *

  해당 스토리지의 기본 소유자가 실패한 경우 파트너가 스토리지를 제어하는 프로세스입니다. SFO 맥락에서 페일오버 및 테이크오버는 동의어입니다.

SMB 3.0 기능이 **SMB** 공유에서 무중단 운영을 지원하는 방법

SMB 3.0은 SMB 공유를 통해 Hyper-V 및 SQL Server의 무중단 운영을 지원하는 중요한 기능을 제공합니다. 여기에는 SMB 클라이언트가 파일 열기 상태를 재확보하고 SMB 연결을 투명하게 다시 설정할 수 있도록 하는 '연속 사용 가능' 공유 속성과 '영구 핸들’이라는 파일 핸들 유형이 포함됩니다.

지속적으로 사용 가능한 공유 속성 집합을 사용하여 공유에 연결하는 SMB 3.0 지원 클라이언트에 영구 핸들을 부여할 수 있습니다. SMB 세션의 연결이 끊기면 CIFS 서버는 영구 처리 상태에 대한 정보를 유지합니다. CIFS 서버는 클라이언트가 다시 연결될 수 있는 60초 동안 다른 클라이언트 요청을 차단하여, 영구 핸들이 있는 클라이언트가 네트워크 연결 해제 후 핸들을 다시 확보할 수 있도록 합니다. 핸들을 지속적으로 사용하는 클라이언트는 SVM(스토리지

가상 머신)의 데이터 LIF 중 하나를 사용하여 다시 연결할 수 있습니다. 즉, 동일한 LIF를 통해 다시 연결하거나 다른 LIF를 통해 다시 연결할 수 있습니다.

애그리게이트 재배치, 테이크오버 및 반환은 모두 SFO 쌍 간에 발생합니다. 영구 핸들이 있는 파일을 사용하여 세션의 분리 및 재연결을 원활하게 관리하기 위해 파트너 노드는 모든 영구 핸들 잠금 정보의 복사본을 유지 관리합니다. SFO 파트너는 이벤트의 계획인지 계획되지 않는지에 관계없이 영구 핸들 연결을 중단 없이 관리할 수 있습니다. 이 새로운 기능을 통해 CIFS 서버에 대한 SMB 3.0 연결이 예전부터 운영 중단 없이 할당된 SVM에 할당된 다른 데이터 LIF로 투명하게 페일오버할 수 있습니다.

영구 핸들을 사용하면 CIFS 서버가 SMB 3.0 연결을 투명하게 페일오버할 수 있지만 장애가 발생하여 Hyper-V 애플리케이션이 Windows Server 클러스터의 다른 노드로 페일오버될 경우 클라이언트는 연결이 끊어진 핸들의 파일 핸들을 다시 확보할 수 없습니다. 이 시나리오에서는 연결이 끊긴 상태의 파일 핸들이 다른 노드에서 다시 시작될 경우 Hyper-V 응용 프로그램의 액세스를 차단할 수 있습니다. ""장애 조치 클러스터링""은 SMB 3.0의 일부이며, 이러한 시나리오를 해결하기 위해 오래되고 충돌하는 핸들을 무효화하는 메커니즘을 제공합니다. 이 메커니즘을 사용하면 Hyper-V 클러스터 노드에 장애가 발생할 경우 Hyper-V 클러스터가 신속하게 복구될 수 있습니다.

Witness 프로토콜이 투명한 장애 조치를 강화하기 위해 수행하는 조치

Witness 프로토콜은 SMB 3.0에서 지속적으로 사용 가능한 공유(CA 공유)를 위한 향상된 클라이언트 페일오버 기능을 제공합니다. 입회자는 LIF 페일오버 복구 기간을 거치지 않으므로 더 빠른 페일오버를 촉진합니다. SMB 3.0 연결이 시간 초과될 때까지 기다리지 않고 노드를 사용할 수 없을 때 애플리케이션 서버에 알립니다.

클라이언트에서 실행 중인 애플리케이션이 페일오버가 발생했는지 알지 못하면서 페일오버가 원활하게 이루어집니다. Witness를 사용할 수 없는 경우에도 페일오버 작업은 성공적으로 수행되지만 Witness를 사용하지 않는 페일오버는 효율성이 떨어집니다.

다음 요구 사항이 충족되면 감시 강화 장애 조치가 가능합니다.

- SMB 3.0이 활성화된 SMB 3.0 지원 CIFS 서버에서만 사용할 수 있습니다.
- 공유는 지속적인 가용성 공유 속성 세트와 함께 SMB 3.0을 사용해야 합니다.
- 애플리케이션 서버가 연결되는 노드의 SFO 파트너는 애플리케이션 서버의 데이터를 호스팅하는 SVM(스토리지 가상 머신)에 적어도 하나의 운영 데이터 LIF가 할당되어 있어야 합니다.

> ⓘ Witness 프로토콜은 SFO 쌍 사이에서 작동합니다. LIF가 클러스터 내의 노드로 마이그레이션할 수 있으므로 모든 노드가 SFO 파트너의 증인이 될 수 있습니다. 애플리케이션 서버용 데이터를 호스팅하는 SVM이 파트너 노드에 활성 데이터 LIF가 없는 경우 Witness 프로토콜은 특정 노드에서 SMB 연결을 빠르게 페일오버할 수 없습니다. 따라서 클러스터의 모든 노드는 이러한 구성 중 하나를 호스팅하는 각 SVM에 대해 적어도 하나의 데이터 LIF를 가져야 합니다.

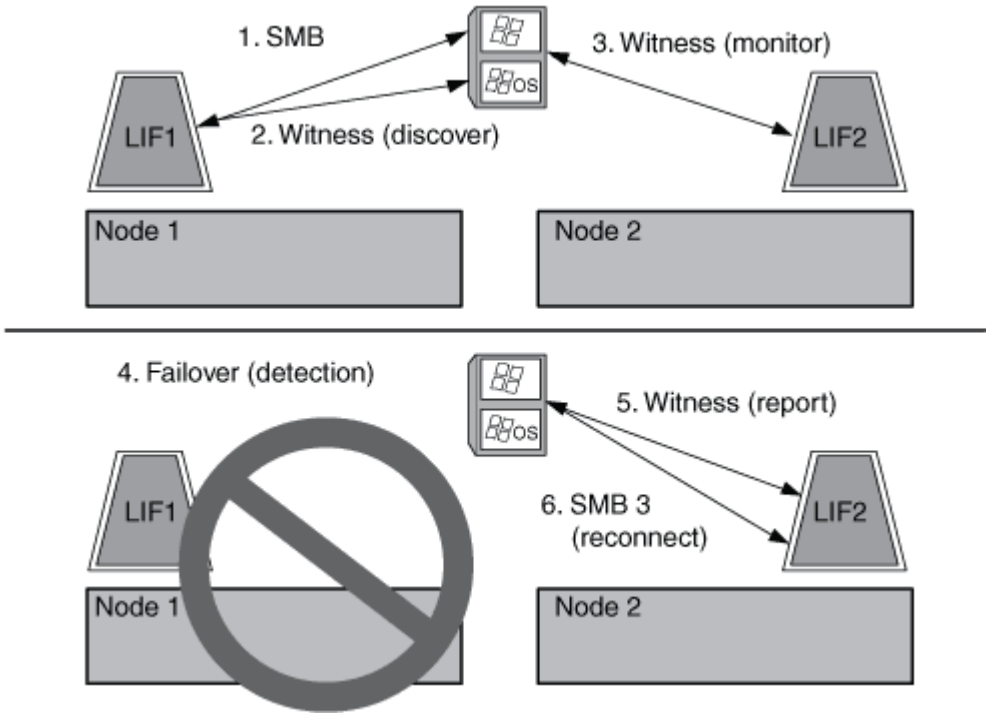
- 애플리케이션 서버는 개별 LIF IP 주소를 사용하는 대신 DNS에 저장된 CIFS 서버 이름을 사용하여 CIFS 서버에 연결해야 합니다.

Witness 프로토콜 작동 방식

ONTAP는 노드의 SFO 파트너를 증인으로 사용하여 Witness 프로토콜을 구현합니다. 장애가 발생할 경우 파트너는 빠르게 장애를 감지하고 SMB 클라이언트에 알립니다.

Witness 프로토콜은 다음 프로세스를 사용하여 향상된 장애 조치를 제공합니다.

1. 애플리케이션 서버가 Node1에 대한 지속적으로 사용 가능한 SMB 연결을 설정하면 CIFS 서버가 애플리케이션 서버에 Witness를 사용할 수 있음을 알립니다.
2. 애플리케이션 서버는 Node1에서 Witness 서버의 IP 주소를 요청하고, 스토리지 가상 시스템(SVM)에 할당된 Node2(SFO 파트너) 데이터 LIF IP 주소 목록을 수신합니다.
3. 애플리케이션 서버는 IP 주소 중 하나를 선택하고 Node2에 대한 Witness 연결을 생성하며, Node1에서 계속 사용 가능한 연결이 이동해야 하는 경우 알림을 받을 레지스터를 생성합니다.
4. Node1에서 페일오버 이벤트가 발생할 경우 Witness는 페일오버 이벤트를 발생하지만 반환과 관련이 없습니다.
5. 감시 기능은 장애 조치 이벤트를 감지하고 Witness 연결을 통해 애플리케이션 서버에 SMB 연결이 Node2로 이동해야 함을 알립니다.
6. 애플리케이션 서버는 SMB 세션을 Node2로 이동하고 클라이언트 액세스를 중단하지 않고 연결을 복구합니다.



원격 **VSS**와 공유 기반 백업

원격 **VSS**를 사용한 공유 기반 백업 개요

원격 VSS를 사용하여 CIFS 서버에 저장된 Hyper-V 가상 머신 파일의 공유 기반 백업을 수행할 수 있습니다.

Microsoft 원격 VSS(Volume Shadow Copy Services)는 기존 Microsoft VSS 인프라의 확장입니다. Microsoft는 원격 VSS를 통해 VSS 인프라스트럭처를 확장하여 SMB 공유의 섀도우 복제를 지원하고 있습니다. 또한 Hyper-V와 같은 서버 애플리케이션에서 SMB 파일 공유에 VHD 파일을 저장할 수 있습니다. 이러한 확장을 사용하면 데이터 및 구성 파일을 공유에 저장하는 가상 시스템에 대해 애플리케이션 정합성이 보장되는 섀도우 복제본을 가져올 수 있습니다.

원격 **VSS** 개념

SMB를 통한 Hyper-V 구성의 백업 서비스에서 원격 VSS(Volume Shadow Copy Service)를 사용하는 방법을 이해하는 데 필요한 특정 개념을 이해해야 합니다.

- * VSS(Volume Shadow Copy Service) *

  특정 시점에 특정 볼륨에 있는 데이터의 백업 복사본 또는 스냅샷을 생성하는 데 사용되는 Microsoft 기술입니다. VSS는 데이터 서버, 백업 애플리케이션 및 스토리지 관리 소프트웨어 사이에서 조정을 수행하여 일관된 백업의 생성 및 관리를 지원합니다.

- * 원격 VSS(원격 볼륨 섀도 복사본 서비스) *

  SMB 3.0 공유를 통해 데이터에 액세스할 수 있는 특정 시점의 데이터 정합성 보장 상태에 있는 데이터의 공유 기반 백업 복사본을 생성하는 데 사용되는 Microsoft 기술입니다. 볼륨 섀도 복사본 서비스 _ 라고도 합니다.

- * 섀도 복사본 *

  공유에 포함된 중복 데이터 집합을 적절하게 정의된 즉시 사용합니다. 섀도우 복제본은 데이터의 일관된 시점 백업을 생성하는 데 사용되므로 시스템이나 애플리케이션에서 원래 볼륨의 데이터를 계속 업데이트할 수 있습니다.

- * 섀도 복사본 세트 *

  한 공유에 해당하는 각 섀도 복사본을 포함하는 하나 이상의 섀도 복사본 모음입니다. 섀도우 복제본 세트 내의 섀도우 복제본은 동일한 작업에서 백업해야 하는 모든 공유를 나타냅니다. VSS 지원 애플리케이션의 VSS 클라이언트는 세트에 포함할 섀도우 복제본을 식별합니다.

- * 섀도우 복제본 세트 자동 복구 *

  섀도우 복제본이 포함된 복제본 디렉토리가 시점 정합성이 보장되는 원격 VSS 지원 백업 애플리케이션에 대한 백업 프로세스의 일부입니다. 백업을 시작할 때 애플리케이션의 VSS 클라이언트는 백업 예약된 데이터(Hyper-V의 경우 가상 머신 파일)에서 소프트웨어 체크포인트를 생성하도록 애플리케이션을 트리거합니다. 그러면 VSS 클라이언트가 응용 프로그램을 계속할 수 있습니다. 섀도우 복제본 세트가 생성된 후 원격 VSS는 섀도우 복제본 세트를 쓰기 가능하게 만들고 쓰기 가능한 복제본을 애플리케이션에 노출합니다. 애플리케이션은 앞서 생성한 소프트웨어 체크포인트를 사용하여 자동 복구를 수행하여 섀도우 복제본 세트를 백업할 준비를 합니다. 자동 복구는 체크포인트가 생성된 이후 파일 및 디렉토리의 변경 사항을 언롤링함으로써 섀도우 복제본을 정합성 보장 상태로 만듭니다. 자동 복구는 VSS 지원 백업을 위한 선택적 단계입니다.

- * 섀도 복사본 ID *

  섀도우 복제본을 고유하게 식별하는 GUID입니다.

- * 섀도 복사본 세트 ID *

  동일한 서버에 대한 섀도우 복제본 ID의 컬렉션을 고유하게 식별하는 GUID입니다.

- * Hyper-V * 용 SnapManager

  Microsoft Windows Server 2012 Hyper-V의 백업 및 복원 작업을 자동화하고 단순화하는 소프트웨어입니다 SnapManager for Hyper-V는 원격 VSS와 자동 복구를 사용하여 SMB 공유를 통해 Hyper-V 파일을 백업합니다.

관련 정보

SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영에 대한 주요 개념입니다

원격 VSS와 공유 기반 백업

원격 **VSS**에서 사용하는 디렉토리 구조의 예

원격 VSS는 섀도우 복제본을 생성할 때 Hyper-V 가상 머신 파일을 저장하는 디렉토리 구조를 통과합니다. 가상 머신 파일의 백업을 성공적으로 생성할 수 있도록 적절한 디렉토리 구조가 무엇인지 이해하는 것이 중요합니다.

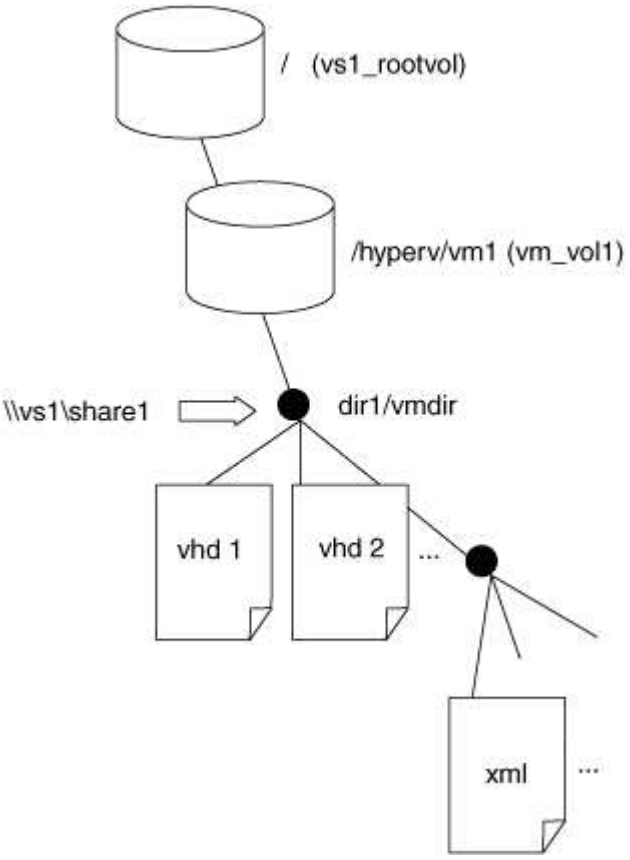
섀도우 복제본을 성공적으로 생성하기 위해 지원되는 디렉토리 구조는 다음 요구 사항을 따릅니다.

- 가상 머신 파일을 저장하는 데 사용되는 디렉토리 구조 내에는 디렉토리와 일반 파일만 있습니다.

  디렉터리 구조에는 연결 지점, 링크 또는 비정규 파일이 포함되어 있지 않습니다.

- 가상 머신의 모든 파일은 단일 공유 내에 있습니다.
- 가상 머신 파일을 저장하는 데 사용되는 디렉토리 구조가 섀도 복사본 디렉토리의 구성된 깊이를 초과하지 않습니다.
- 공유의 루트 디렉토리에는 가상 머신 파일 또는 디렉토리만 포함됩니다.

다음 그림에서는 vm_vol1이라는 이름의 볼륨이 SVM(Storage Virtual Machine) VS1 의 '/hyperv/vm1'에 있는 접합 지점으로 생성됩니다. 가상 머신 파일을 포함하는 하위 디렉토리는 교차점 아래에 생성됩니다. Hyper-V 서버의 가상 머신 파일은 "/hyperv/vm1/dir1/vmdir" 경로가 있는 share1을 통해 액세스합니다. 섀도 복사본 서비스는 share1 아래의 디렉토리 구조 내에 포함된 모든 가상 머신 파일의 섀도 복사본을 만듭니다(섀도우 복제본 디렉토리의 구성된 깊이까지).



SnapManager for Hyper-V가 **SMB**를 통해 **Hyper-V**에 대한 원격 **VSS** 기반 백업을 관리하는 방법

SnapManager for Hyper-V를 사용하여 원격 VSS 기반 백업 서비스를 관리할 수 있습니다. SnapManager for Hyper-V 관리 백업 서비스를 사용하면 공간 효율적인 백업 세트를 생성할 수

있다는 이점이 있습니다.

Hyper-V 관리 백업을 위한 SnapManager 최적화 기능은 다음과 같습니다.

- ONTAP와 SnapDrive의 통합은 SMB 공유 위치를 검색할 때 성능을 최적화합니다.

  ONTAP는 공유가 상주하는 볼륨의 이름을 SnapDrive에 제공합니다.

- SnapManager for Hyper-V는 섀도우 복제본 서비스를 복제해야 하는 SMB 공유의 가상 머신 파일 목록을 지정합니다.

  가상 머신 파일의 타겟 목록을 제공함으로써 섀도우 복제본 서비스는 공유에 있는 모든 파일의 섀도우 복제본을 생성할 필요가 없습니다.

- 스토리지 가상 머신(SVM)에 복원에 사용할 SnapManager for Hyper-V의 스냅샷이 보존됩니다.

  백업 단계가 없습니다. 백업은 공간 효율성이 뛰어난 스냅샷입니다.

SnapManager for Hyper-V는 다음 프로세스를 사용하여 SMB를 통한 Hyper-V의 백업 및 복원 기능을 제공합니다.

1. 섀도 복사본 작업을 준비하는 중입니다

   SnapManager for Hyper-V 애플리케이션의 VSS 클라이언트는 섀도우 복제본 세트를 설정합니다. VSS 클라이언트는 섀도 복사본 세트에 포함할 공유에 대한 정보를 수집하고 이 정보를 ONTAP에 제공합니다. 세트에는 하나 이상의 섀도 복사본이 포함될 수 있으며 하나의 섀도 복사본은 하나의 공유에 해당합니다.

2. 섀도 복사본 세트 생성(자동 복구가 사용되는 경우)

   섀도 복사본 세트에 포함된 모든 공유에서 ONTAP는 섀도 복사본을 만들고 섀도 복사본을 쓰기 가능하게 만듭니다.

3. 섀도우 복제본 세트를 노출합니다

   ONTAP에서 섀도우 복제본을 생성한 후 SnapManager for Hyper-V에 노출되므로 애플리케이션의 VSS 작성기가 자동 복구를 수행할 수 있습니다.

4. 섀도우 복제본 세트를 자동으로 복구합니다

   섀도우 복제본 세트를 생성하는 동안 백업 세트에 포함된 파일에 대한 활성 변경이 발생하는 기간이 있습니다. 애플리케이션의 VSS 작성자는 섀도우 복제본을 업데이트하여 백업 전에 정합성이 완벽하게 보장되는 상태인지 확인해야 합니다.

   자동 복구를 수행하는 방법은 애플리케이션에 따라 다릅니다. 원격 VSS가 이 단계에 없습니다.

5. 섀도 복사본 세트 완료 및 정리

   VSS 클라이언트는 자동 복구를 완료한 후 ONTAP에 알립니다. 섀도 복사본 세트는 읽기 전용으로 만들어져 백업할 준비가 된 상태입니다. 백업에 SnapManager for Hyper-V를 사용하면 스냅샷의 파일이 백업이 되므로 백업 단계의 경우 백업 세트의 공유를 포함하는 모든 볼륨에 대해 스냅샷이 생성됩니다. 백업이 완료되면 CIFS 서버에서 섀도우 복제본 세트가 제거됩니다.

SMB 공유를 통해 Hyper-V 및 SQL Server에서 ODX 복사 오프로드를 사용하는 방법

ODX(Offloaded Data Transfer)는 _copy offload_라고도 하며 호스트 컴퓨터를 통해 데이터를 전송하지 않고도 호환되는 스토리지 장치 내부 또는 간에 직접 데이터를 전송할 수 있습니다. ONTAP ODX 복사 오프로드를 사용하면 SMB 설치를 통해 애플리케이션 서버에서 복사 작업을 수행할 때 성능 이점을 얻을 수 있습니다.

ODX가 아닌 파일 전송에서는 소스 CIFS 서버에서 데이터를 읽고 네트워크를 통해 클라이언트 컴퓨터로 전송합니다. 클라이언트 컴퓨터는 네트워크를 통해 대상 CIFS 서버로 데이터를 다시 전송합니다. 요약하면 클라이언트 컴퓨터는 소스에서 데이터를 읽고 대상에 씁니다. ODX 파일 전송을 사용하면 데이터가 소스에서 타겟으로 직접 복사됩니다.

오프로드 복사본은 소스 및 타겟 스토리지 간에 직접 수행되므로 성능이 크게 향상됩니다. 소스 및 대상 간의 복제 시간 단축, 클라이언트의 리소스 활용률(CPU, 메모리) 감소, 네트워크 I/O 대역폭 사용률 감소 등의 성능 이점을 얻을 수 있습니다.

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
ODX 복사 및 이동 사용을 지원하는 사용 사례는 다음과 같습니다.
```

- 체내

  소스 및 대상 파일 또는 LUN이 동일한 볼륨 내에 있습니다.

- 볼륨 간, 동일한 노드, 동일한 SVM(스토리지 가상 머신)

  소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- 볼륨 간, 다른 노드, 동일한 SVM

  소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- SVM 간, 동일한 노드

  소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

- SVM 간, 다른 노드

  소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

Hyper-V 솔루션을 사용한 ODX 복사 오프로드의 구체적인 사용 사례는 다음과 같습니다.

- Hyper-V에서 ODX 복사 오프로드 패스스스루 를 사용하여 VHD(가상 하드 디스크) 파일 내부 또는 VHD 파일 간에 데이터를 복사하거나, 매핑된 SMB 공유와 동일한 클러스터 내에서 연결된 iSCSI LUN 간에 데이터를 복사할 수 있습니다.

  이렇게 하면 게스트 운영 체제에서 복제본을 기본 스토리지로 전달할 수 있습니다.

- 고정 크기의 VHD를 생성할 때 ODX는 잘 알려진 제로화 토큰을 사용하여 0으로 디스크를 초기화하는 데 사용됩니다.
- 소스 및 타겟 스토리지가 동일한 클러스터에 있는 경우 ODX 복사 오프로드가 가상 머신 스토리지 마이그레이션에 사용됩니다.

> Hyper-V를 사용한 ODX 복사 오프로드 패스쓰루 사용 사례를 활용하려면 게스트 운영 체제가 ODX를 지원하고, 게스트 운영 체제 디스크는 ODX를 지원하는 스토리지(SMB 또는 SAN)를 통해 지원되는 SCSI 디스크여야 합니다. 게스트 운영 체제의 IDE 디스크는 ODX 패스스스루 를 지원하지 않습니다.

SQL Server 솔루션을 사용한 ODX 복사 오프로드의 구체적인 사용 사례는 다음과 같습니다.

- ODX 복사 오프로드 를 사용하여 매핑된 SMB 공유 간에 또는 동일한 클러스터 내에서 SMB 공유와 연결된 iSCSI LUN 간에 SQL Server 데이터베이스를 내보내고 가져올 수 있습니다.
- 소스 및 타겟 스토리지가 동일한 클러스터에 있는 경우 ODX 복사 오프로드를 사용하여 데이터베이스를 내보내고 가져올 수 있습니다.

구성 요구 사항 및 고려 사항

ONTAP 및 라이센스 요구 사항

SVM에서 무중단 운영을 위해 SQL Server 또는 Hyper-V over SMB 솔루션을 생성할 때 특정 ONTAP 및 라이센스 요구사항을 알아야 합니다.

ONTAP 버전 요구 사항

- SMB를 통한 Hyper-V

  ONTAP는 Windows 2012 이상에서 실행되는 Hyper-V에 대해 SMB 공유를 통한 무중단 운영을 지원합니다.

- SMB를 통한 SQL Server

  ONTAP는 Windows 2012 이상에서 실행되는 SQL Server 2012 이상에 대해 SMB 공유를 통한 무중단 운영을 지원합니다.

SMB 공유에서 무중단 운영을 지원하는 ONTAP, Windows Server 및 SQL Server의 지원되는 버전에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

"NetApp 상호 운용성 매트릭스 툴"

라이센스 요구 사항

다음 라이센스가 필요합니다.

- CIFS를 선택합니다
- FlexClone(SMB를 통한 Hyper-V만 해당)

  원격 VSS를 백업에 사용하는 경우 이 라이센스가 필요합니다. 섀도 복사본 서비스는 FlexClone을 사용하여 백업을 만들 때 사용되는 파일의 시점 복사본을 만듭니다.

FlexClone 라이센스는 원격 VSS를 사용하지 않는 백업 방법을 사용하는 경우 선택 사항입니다.

FlexClone 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오"있습니다. ONTAP One이 없는 경우, "필요한 라이센스가 설치되어 있는지 확인합니다"그리고 필요한 경우, 를 수행해야 "설치합니다"합니다.

네트워크 및 데이터 **LIF** 요구사항

무중단 운영을 위해 SQL Server 또는 SMB를 통한 Hyper-V 구성을 생성할 때 특정 네트워크 및 데이터 LIF 요구사항을 알고 있어야 합니다.

네트워크 프로토콜 요구 사항

- IPv4 및 IPv6 네트워크가 지원됩니다.
- SMB 3.0 이상이 필요합니다.

  SMB 3.0은 무중단 운영을 제공하는 데 필요한 지속적으로 사용 가능한 SMB 연결을 생성하는 데 필요한 기능을 제공합니다.

- DNS 서버에는 SVM(Storage Virtual Machine)의 데이터 LIF에 할당된 IP 주소에 CIFS 서버 이름을 매핑하는 항목이 포함되어 있어야 합니다.

  Hyper-V 또는 SQL Server 애플리케이션 서버는 일반적으로 가상 머신 또는 데이터베이스 파일에 액세스할 때 여러 데이터 LIF를 통해 여러 개의 연결을 생성합니다. 적절한 기능을 위해 애플리케이션 서버는 여러 고유 IP 주소에 여러 번 연결하는 대신 CIFS 서버 이름을 사용하여 이러한 여러 SMB 연결을 설정해야 합니다.

  또한 감시 기능을 사용하려면 개별 LIF IP 주소 대신 CIFS 서버의 DNS 이름을 사용해야 합니다.

  ONTAP 9.4부터 SMB 멀티 채널을 활성화하여 SMB 구성에서 Hyper-V 및 SQL Server의 처리량과 내결함성을 향상시킬 수 있습니다. 이렇게 하려면 클러스터 및 클라이언트에 1G, 10G 또는 더 큰 NIC가 여러 개 설치되어 있어야 합니다.

데이터 **LIF** 요구사항

- SMB 솔루션을 통해 애플리케이션 서버를 호스팅하는 SVM은 클러스터의 모든 노드에 운영 데이터 LIF가 하나 이상 있어야 합니다.

  SVM 데이터 LIF는 애플리케이션 서버에서 액세스하는 데이터를 현재 호스팅하지 않는 노드를 비롯하여 클러스터 내의 다른 데이터 포트로 페일오버할 수 있습니다. 또한 Witness 노드는 항상 애플리케이션 서버가 접속된 노드의 SFO 파트너이므로 클러스터의 모든 노드가 잠재적인 Witness 노드입니다.

- 데이터 LIF가 자동으로 복구되도록 구성하지 않아야 합니다.

  테이크오버 또는 반환 이벤트가 발생한 후에는 데이터 LIF를 홈 포트로 수동으로 되돌려야 합니다.

- 모든 데이터 LIF IP 주소에는 DNS에 항목이 있어야 하며 모든 항목이 CIFS 서버 이름으로 확인되어야 합니다.

  애플리케이션 서버는 CIFS 서버 이름을 사용하여 SMB 공유에 접속해야 합니다. LIF IP 주소를 사용하여 연결되도록 애플리케이션 서버를 구성하지 마십시오.

- CIFS 서버 이름이 SVM 이름과 다른 경우 DNS 항목이 CIFS 서버 이름으로 확인되어야 합니다.

SMB를 통한 **Hyper-V**의 **SMB** 서버 및 볼륨 요구 사항

무중단 운영을 위해 SMB를 통한 Hyper-V 구성을 생성할 때 특정 SMB 서버 및 볼륨 요구사항을 알고 있어야 합니다.

SMB 서버 요구 사항

- SMB 3.0을 활성화해야 합니다.

  이 기능은 기본적으로 활성화되어 있습니다.

- 기본 UNIX 사용자 CIFS 서버 옵션은 유효한 UNIX 사용자 계정으로 구성해야 합니다.

  애플리케이션 서버는 SMB 연결을 생성할 때 컴퓨터 계정을 사용합니다. 모든 SMB 액세스를 위해서는 Windows 사용자가 UNIX 사용자 계정 또는 기본 UNIX 사용자 계정에 성공적으로 매핑되어야 하므로 ONTAP는 애플리케이션 서버의 컴퓨터 계정을 기본 UNIX 사용자 계정에 매핑할 수 있어야 합니다.

- 자동 노드 조회를 비활성화해야 합니다(이 기능은 기본적으로 비활성화되어 있습니다).

  Hyper-V 시스템 파일 이외의 데이터에 액세스하기 위해 자동 노드 조회를 사용하려면 해당 데이터에 대해 별도의 SVM을 생성해야 합니다.

- Kerberos 및 NTLM 인증은 SMB 서버가 속한 도메인에서 모두 허용되어야 합니다.

  ONTAP는 원격 VSS에 대한 Kerberos 서비스를 광고하지 않으므로 NTLM을 허용하도록 도메인을 설정해야 합니다.

- 섀도 복사본 기능이 활성화되어 있어야 합니다.

  이 기능은 기본적으로 활성화되어 있습니다.

- 섀도 복사본을 만들 때 섀도 복사본 서비스가 사용하는 Windows 도메인 계정은 SMB 서버 로컬 BUILTIN\Administrators 또는 BUILTIN\Backup Operators 그룹의 구성원이어야 합니다.

볼륨 요구 사항

- 가상 머신 파일을 저장하는 데 사용되는 볼륨은 NTFS 보안 스타일 볼륨으로 만들어야 합니다.

  지속적으로 사용 가능한 SMB 연결을 사용하여 애플리케이션 서버에 NDO를 제공하려면 공유가 포함된 볼륨이 NTFS 볼륨이어야 합니다. 또한 항상 NTFS 볼륨이어야 합니다. 혼합 보안 스타일 볼륨 또는 UNIX 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통해 NDO에 직접 사용할 수는 없습니다. 혼합 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통해 NDO에 사용하려면 ACL을 볼륨 상단에 수동으로 배치하고 해당 ACL을 포함된 모든 파일 및 폴더에 전파해야 합니다. 그렇지 않으면 소스 또는 대상 볼륨이 처음에 혼합 또는 UNIX 보안 스타일 볼륨으로 생성된 후 나중에 NTFS 보안 스타일로 변경된 경우 가상 머신 마이그레이션 또는 데이터베이스 파일 내보내기 및 가져오기가 다른 볼륨으로 이동될 수 있습니다.

- 섀도 복사본 작업이 성공하려면 볼륨에 충분한 공간이 있어야 합니다.

  사용 가능한 공간은 섀도 복사본 백업 세트에 포함된 공유 내에 포함된 모든 파일, 디렉토리 및 하위 디렉토리에 사용되는 결합된 공간보다 최소한 크거나 같아야 합니다. 이 요구 사항은 자동 복구를 사용하는 섀도우 복제본에만 적용됩니다.

관련 정보

"Microsoft TechNet 라이브러리: technet.microsoft.com/en-us/library/"

SMB를 통한 **SQL Server**의 **SMB** 서버 및 볼륨 요구 사항

무중단 운영을 위해 SMB를 통한 SQL Server 구성을 생성할 때 특정 SMB 서버 및 볼륨 요구사항을 알고 있어야 합니다.

SMB 서버 요구 사항

- SMB 3.0을 활성화해야 합니다.

  이 기능은 기본적으로 활성화되어 있습니다.

- 기본 UNIX 사용자 CIFS 서버 옵션은 유효한 UNIX 사용자 계정으로 구성해야 합니다.

  애플리케이션 서버는 SMB 연결을 생성할 때 컴퓨터 계정을 사용합니다. 모든 SMB 액세스를 위해서는 Windows 사용자가 UNIX 사용자 계정 또는 기본 UNIX 사용자 계정에 성공적으로 매핑되어야 하므로 ONTAP는 애플리케이션 서버의 컴퓨터 계정을 기본 UNIX 사용자 계정에 매핑할 수 있어야 합니다.

  또한 SQL Server에서는 도메인 사용자를 SQL Server 서비스 계정으로 사용합니다. 서비스 계정도 기본 UNIX 사용자에게 매핑되어야 합니다.

- 자동 노드 조회를 비활성화해야 합니다(이 기능은 기본적으로 비활성화되어 있습니다).

  SQL Server 데이터베이스 파일 이외의 데이터에 액세스하기 위해 자동 노드 조회를 사용하려면 해당 데이터에 대해 별도의 SVM을 생성해야 합니다.

- ONTAP에 SQL Server를 설치하는 데 사용되는 Windows 사용자 계정에 SeSecurityPrivilege 권한이 할당되어야 합니다.

  이 권한은 SMB 서버 로컬 BUILTIN\Administrators 그룹에 할당됩니다.

볼륨 요구 사항

- 가상 머신 파일을 저장하는 데 사용되는 볼륨은 NTFS 보안 스타일 볼륨으로 만들어야 합니다.

  지속적으로 사용 가능한 SMB 연결을 사용하여 애플리케이션 서버에 NDO를 제공하려면 공유가 포함된 볼륨이 NTFS 볼륨이어야 합니다. 또한 항상 NTFS 볼륨이어야 합니다. 혼합 보안 스타일 볼륨 또는 UNIX 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통해 NDO에 직접 사용할 수는 없습니다. 혼합 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통해 NDO에 사용하려면 ACL을 볼륨 상단에 수동으로 배치하고 해당 ACL을 포함된 모든 파일 및 폴더에 전파해야 합니다. 그렇지 않으면 소스 또는 대상 볼륨이 처음에 혼합 또는 UNIX 보안 스타일 볼륨으로 생성된 후 나중에 NTFS 보안 스타일로 변경된 경우 가상 머신 마이그레이션 또는 데이터베이스 파일 내보내기 및 가져오기가 다른 볼륨으로 이동될 수 있습니다.

- 데이터베이스 파일이 포함된 볼륨에는 접합부가 포함될 수 있지만 SQL Server는 데이터베이스 디렉토리 구조를 생성할 때 접합을 교차하지 않습니다.
- Microsoft SQL Server용 SnapCenter 플러그인 백업 작업이 성공하려면 볼륨에 충분한 공간이 있어야 합니다.

  SQL Server 데이터베이스 파일이 있는 볼륨은 데이터베이스 디렉토리 구조와 공유 내에 있는 모든 포함된 파일을 저장할 수 있을 만큼 커야 합니다.

관련 정보

"Microsoft TechNet 라이브러리: technet.microsoft.com/en-us/library/"

SMB를 통한 **Hyper-V**의 지속적인 가용성 공유 요구 사항 및 고려 사항

무중단 운영을 지원하는 SMB 구성을 통해 Hyper-V에서 지속적으로 사용 가능한 공유를 구성할 때 특정 요구사항과 고려 사항을 알고 있어야 합니다.

공유 요구 사항

- 응용 프로그램 서버에서 사용하는 공유는 지속적으로 사용 가능한 속성 집합을 사용하여 구성해야 합니다.

  지속적으로 사용 가능한 공유에 연결되는 애플리케이션 서버에는 SMB 공유에 중단 없이 다시 연결할 수 있는 영구 핸들이 제공되며, 테이크오버, 반환, 애그리게이트 재배치와 같은 운영 중단 이벤트가 발생한 후 파일 잠금을 재확보할 수 있습니다.

- 원격 VSS 지원 백업 서비스를 사용하려는 경우 접합을 포함하는 공유에 Hyper-V 파일을 넣을 수 없습니다.

  자동 복구 사례에서는 공유를 이동하는 동안 분기점이 발생하면 섀도우 복제본 생성이 실패합니다. 자동 복구가 아닌 경우 섀도우 복제본 생성이 실패하지는 않지만 교차점은 아무 것도 가리키지 않습니다.

- 자동 복구와 함께 원격 VSS 지원 백업 서비스를 사용하려는 경우 다음을 포함하는 공유에 Hyper-V 파일을 넣을 수 없습니다.
  - symlinks, hardlinks 또는 wdelink
  - 일반 파일이 아닙니다

    공유에 섀도우 복제본으로 연결되는 링크나 비정규 파일이 있는 경우 섀도우 복제본 생성이 실패합니다. 이 요구 사항은 자동 복구를 사용하는 섀도우 복제본에만 적용됩니다.

  - 섀도 복사본 작업이 성공하려면 볼륨에 충분한 공간이 있어야 합니다(SMB를 통한 Hyper-V만 해당).

    사용 가능한 공간은 섀도 복사본 백업 세트에 포함된 공유 내에 포함된 모든 파일, 디렉토리 및 하위 디렉토리에 사용되는 결합된 공간보다 최소한 크거나 같아야 합니다. 이 요구 사항은 자동 복구를 사용하는 섀도우 복제본에만 적용됩니다.

- 애플리케이션 서버에서 계속 사용 가능한 공유에 대해 다음 공유 속성을 설정하지 않아야 합니다.
  - 더 높여 줍니다
  - 특성 캐싱
  - BranchCache입니다

고려 사항

- 할당량은 지속적으로 사용 가능한 공유에서 지원됩니다.
- SMB를 통한 Hyper-V 구성에서는 다음 기능이 지원되지 않습니다.
  - 감사
  - FPolicy를 참조하십시오
- '연속 가용성' 매개변수가 '예'로 설정된 SMB 공유에서는 바이러스 검사가 수행되지 않습니다.

SMB를 통한 **SQL Server**의 지속적인 가용성 공유 요구 사항 및 고려 사항

무중단 운영을 지원하는 SMB 구성을 통해 SQL Server에 대해 지속적으로 사용 가능한 공유를 구성할 때 특정 요구사항과 고려 사항을 알고 있어야 합니다.

공유 요구 사항

- 가상 머신 파일을 저장하는 데 사용되는 볼륨은 NTFS 보안 스타일 볼륨으로 만들어야 합니다.

  지속적으로 사용 가능한 SMB 연결을 통해 애플리케이션 서버에 무중단 운영을 제공하려면 공유를 포함하는 볼륨이 NTFS 볼륨이어야 합니다. 또한 항상 NTFS 볼륨이어야 합니다. 혼합 보안 스타일 볼륨 또는 UNIX 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통한 무중단 운영에 직접 사용할 수는 없습니다. 혼합 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통한 무중단 작업에 사용하려면 ACL을 볼륨 상단에 수동으로 배치하고 해당 ACL을 포함된 모든 파일 및 폴더에 전파해야 합니다. 그렇지 않으면 소스 또는 대상 볼륨이 처음에 혼합 또는 UNIX 보안 스타일 볼륨으로 생성된 후 나중에 NTFS 보안 스타일로 변경된 경우 가상 머신 마이그레이션 또는 데이터베이스 파일 내보내기 및 가져오기가 다른 볼륨으로 이동될 수 있습니다.

- 응용 프로그램 서버에서 사용하는 공유는 지속적으로 사용 가능한 속성 집합을 사용하여 구성해야 합니다.

  지속적으로 사용 가능한 공유에 연결되는 애플리케이션 서버에는 SMB 공유에 중단 없이 다시 연결할 수 있는 영구 핸들이 제공되며, 테이크오버, 반환, 애그리게이트 재배치와 같은 운영 중단 이벤트가 발생한 후 파일 잠금을 재확보할 수 있습니다.

- 데이터베이스 파일이 포함된 볼륨에는 접합부가 포함될 수 있지만 SQL Server는 데이터베이스 디렉토리 구조를 생성할 때 접합을 교차하지 않습니다.
- Microsoft SQL Server용 SnapCenter 플러그인을 성공적으로 사용하려면 볼륨에 충분한 공간이 있어야 합니다.

  SQL Server 데이터베이스 파일이 있는 볼륨은 데이터베이스 디렉토리 구조와 공유 내에 있는 모든 포함된 파일을 저장할 수 있을 만큼 커야 합니다.

- 애플리케이션 서버에서 계속 사용 가능한 공유에 대해 다음 공유 속성을 설정하지 않아야 합니다.
  - 더 높여 줍니다
  - 특성 캐싱
  - BranchCache입니다

공유 고려 사항

- 할당량은 지속적으로 사용 가능한 공유에서 지원됩니다.
- SMB를 통한 SQL Server 구성에서는 다음 기능이 지원되지 않습니다.
  - 감사
  - FPolicy를 참조하십시오
- 지속적으로 사용 가능한 공유 자산이 설정된 SMB 공유에서는 바이러스 검사가 수행되지 않습니다.

SMB 구성을 통한 **Hyper-V**에 대한 원격 **VSS** 고려 사항

SMB를 통한 Hyper-V 구성에 대해 원격 VSS 지원 백업 솔루션을 사용할 때는 특정 고려 사항을 염두에 두어야 합니다.

일반 원격 **VSS** 고려 사항

- Microsoft 애플리케이션 서버당 최대 64개의 공유를 구성할 수 있습니다.

  섀도우 복제본 세트에 64개 이상의 공유가 있는 경우 섀도우 복제본 작업이 실패합니다. 이는 Microsoft의 요구 사항입니다.

- CIFS 서버당 하나의 활성 섀도 복사본 세트만 허용됩니다.

  동일한 CIFS 서버에 섀도우 복제본 작업이 진행 중인 경우 섀도우 복제본 작업이 실패합니다. 이는 Microsoft의 요구 사항입니다.

- 원격 VSS가 섀도우 복제본을 생성하는 디렉토리 구조 내에서는 접합을 수행할 수 없습니다.
  - 자동 복구 사례에서는 공유를 이동하는 동안 분기점이 발생하면 섀도우 복제본 생성이 실패합니다.
  - 비자동 복구 사례에서는 섀도우 복제본 생성이 실패하지 않지만 접합은 아무 것도 가리키지 않습니다.

자동 복구를 사용하는 섀도우 복제본에만 적용되는 원격 **VSS** 고려 사항

자동 복구를 사용하는 섀도 복사본에만 특정 제한사항이 적용됩니다.

- 섀도우 복제본 생성에는 하위 디렉토리 5개의 최대 디렉토리 수준이 허용됩니다.

  섀도우 복제본 서비스가 섀도우 복제본 백업 세트를 생성하는 디렉토리 깊이입니다. 가상 머신 파일이 포함된 디렉토리가 5개 수준 이상 중첩되면 섀도우 복제본 생성이 실패합니다. 이는 공유를 복제할 때 디렉토리 트래버설을 제한하기 위한 것입니다. 최대 디렉토리 깊이는 CIFS 서버 옵션을 사용하여 변경할 수 있습니다.

- 볼륨의 사용 가능한 공간이 적절해야 합니다.

  사용 가능한 공간은 섀도 복사본 백업 세트에 포함된 공유 내에 포함된 모든 파일, 디렉토리 및 하위 디렉토리에 사용되는 결합된 공간보다 최소한 크거나 같아야 합니다.

- 원격 VSS가 섀도우 복제본을 생성하는 디렉토리 구조 내에서 링크나 일반 파일이 허용되지 않습니다.

  공유에 섀도 복사본에 대한 링크 또는 비정규 파일이 있는 경우 섀도 복사본 생성이 실패합니다. 클론 프로세스에서 이를 지원하지 않습니다.

- 디렉토리에는 NFSv4 ACL이 허용되지 않습니다.

  섀도우 복제본 생성이 파일에 NFSv4 ACL을 유지하지만 디렉토리의 NFSv4 ACL이 손실됩니다.

- 섀도 복사본 세트를 생성할 수 있는 시간은 최대 60초입니다.

  Microsoft 사양은 섀도 복사본 세트를 생성하는 데 최대 60초를 허용합니다. VSS 클라이언트가 이 시간 내에 섀도우 복제본 세트를 생성할 수 없는 경우 섀도우 복제본 작업이 실패하므로 섀도우 복제본 세트의 파일 수가 제한됩니다. 백업 세트에 포함될 수 있는 실제 파일 또는 가상 머신 수는 서로 다르며, 이 수는 여러 요인에 따라 달라지며 각 고객 환경에 따라 결정되어야 합니다.

ODX SMB를 통한 **SQL Server** 및 **Hyper-V**의 복사 오프로드 요구 사항

가상 머신 파일을 마이그레이션하거나 애플리케이션 서버를 통해 데이터를 전송하지 않고 데이터베이스 파일을 소스에서 대상 스토리지 위치로 직접 내보내고 가져오려면 ODX 복사

오프로드를 활성화해야 합니다. SQL Server에서 ODX 복사 오프로드를 사용하고 SMB 솔루션을 통해 Hyper-V를 사용하는 것에 대해 이해해야 하는 특정 요구사항이 있습니다.

ODX 복사 오프로드를 사용하면 성능을 대폭 향상할 수 있습니다. 이 CIFS 서버 옵션은 기본적으로 설정되어 있습니다.

- ODX 복사 오프로드를 사용하려면 SMB 3.0을 설정해야 합니다.
- 소스 볼륨은 최소 1.25GB여야 합니다.
- 복사본 오프로드와 함께 사용되는 볼륨에 대해 중복제거를 활성화해야 합니다.
- 압축 볼륨을 사용하는 경우 압축 유형은 적응 가능해야 하며 압축 그룹 크기 8K만 지원됩니다.

  보조 압축 유형은 지원되지 않습니다

- ODX 복사 오프로드를 사용하여 디스크 내부 및 디스크 간에 Hyper-V 게스트를 마이그레이션하려면 SCSI 디스크를 사용하도록 Hyper-V 서버를 구성해야 합니다.

  기본값은 IDE 디스크를 구성하는 것이지만, 디스크가 IDE 디스크를 사용하여 생성된 경우 게스트가 마이그레이션될 때 ODX 복사 오프로드가 작동하지 않습니다.

SMB 구성을 통한 **SQL Server** 및 **Hyper-V** 권장 사항

SQL Server 및 Hyper-V over SMB 구성이 강력하고 작동 가능한지 확인하려면 솔루션 구성 시 권장 모범 사례를 숙지해야 합니다.

일반 권장 사항

- 일반 사용자 데이터와 애플리케이션 서버 파일을 분리합니다.

  가능하면 전체 SVM(스토리지 가상 시스템)과 해당 스토리지를 애플리케이션 서버의 데이터에 사용합니다.

- 최상의 성능을 위해 SVM에서 애플리케이션 서버의 데이터를 저장하는 데 사용되는 SMB 서명을 활성화하지 마십시오.
- 최상의 성능과 향상된 내결함성을 위해 SMB 멀티 채널을 통해 단일 SMB 세션에서 ONTAP와 클라이언트 간에 여러 개의 연결을 제공할 수 있습니다.
- Hyper-V 또는 SQL Server over SMB 구성에서 사용되는 공유 이외의 공유에 대해 지속적으로 사용 가능한 공유를 생성하지 마십시오.
- 지속적인 가용성에 사용되는 공유에 대한 변경 알림을 해제합니다.
- ARL에는 일부 작업을 일시 중지하는 단계가 있으므로 ARL(Aggregate relocation)과 동시에 볼륨 이동을 수행하지 마십시오.
- SMB를 통한 Hyper-V 솔루션의 경우 클러스터 가상 머신을 생성할 때 게스트 내 iSCSI 드라이브를 사용합니다. 공유 '.vHDX' 파일은 ONTAP SMB 공유에서 SMB를 통한 Hyper-V에 지원되지 않습니다.

SMB를 통한 **Hyper-V** 또는 **SQL Server** 구성 계획

볼륨 구성 워크시트를 작성합니다

이 워크시트는 SMB 구성을 통해 SQL Server 및 Hyper-V용 볼륨을 생성할 때 필요한 값을 쉽게

기록할 수 있는 방법을 제공합니다.

각 볼륨에 대해 다음 정보를 지정해야 합니다.

- 스토리지 가상 시스템(SVM) 이름

  SVM 이름은 모든 볼륨에서 동일합니다.

- 볼륨 이름입니다
- 애그리게이트 이름입니다

  클러스터의 노드에 있는 애그리게이트에 볼륨을 생성할 수 있습니다.

- 크기
- 접합 경로

애플리케이션 서버 데이터를 저장하는 데 사용되는 볼륨을 생성할 때 다음 사항을 염두에 두어야 합니다.

- 루트 볼륨에 NTFS 보안 스타일이 없는 경우 볼륨을 생성할 때 보안 스타일을 NTFS로 지정해야 합니다.

  기본적으로 볼륨은 SVM 루트 볼륨의 보안 스타일을 상속합니다.

- 볼륨은 기본 볼륨 공간 보장으로 구성해야 합니다.
- 필요에 따라 공간 자동 크기 조정 관리 설정을 구성할 수 있습니다.
- 스냅숏 공간 예비 공간을 결정하는 옵션을 로 `0`설정해야 합니다.
- 볼륨에 적용된 스냅샷 정책을 해제해야 합니다.

  SVM 스냅샷 정책이 해제되어 있으면 볼륨에 대한 스냅샷 정책을 지정할 필요가 없습니다. 볼륨은 SVM에 대한 스냅샷 정책을 상속합니다. SVM에 대한 스냅샷 정책이 해제되지 않고 스냅샷을 생성하도록 구성된 경우 볼륨 레벨에서 스냅샷 정책을 지정해야 하며 해당 정책을 비활성화해야 합니다. 섀도 복사본 서비스 가능 백업 및 SQL Server 백업은 스냅샷 생성 및 삭제를 관리합니다.

- 볼륨에 대한 로드 공유 미러는 구성할 수 없습니다.

공유 진입점 아래에 접합된 볼륨이 없도록 애플리케이션 서버가 사용하는 공유를 생성하려는 연결 경로를 선택해야 합니다.

예를 들어, 가상 시스템 파일을 ""vol1"", ""vol2"", ""vol3"" 및 ""vol4""라는 네 개의 볼륨에 저장하려면 예제에 표시된 네임스페이스를 생성할 수 있습니다. 그런 다음 '/data1/vol1', '/data1/vol2', '/data2/vol3', '/data2/vol4' 경로에서 애플리케이션 서버에 대한 공유를 생성할 수 있습니다.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

정보 유형	값
_Volume 1: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	
_Volume 2: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	
_Volume 3: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	
_Volume 4: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	
_Volume 5: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	
_Volume 6: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	
_추가 볼륨: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	

SMB 공유 구성 워크시트를 작성합니다

이 워크시트를 사용하여 SMB 구성에서 SQL Server 및 Hyper-V에 대해 지속적으로 사용 가능한 SMB 공유를 생성할 때 필요한 값을 기록하십시오.

SMB 공유 속성 및 구성 설정에 대한 정보입니다

각 공유에 대해 다음 정보를 지정해야 합니다.

- 스토리지 가상 시스템(SVM) 이름

  SVM 이름은 모든 공유에서 동일합니다

- 공유 이름
- 경로
- 공유 속성

  다음 두 공유 속성을 구성해야 합니다.

- oplocks
- "계속 사용할 수 있습니다.

다음 공유 속성을 설정하지 않아야 합니다.

- 홈디렉토리 attributecache
- 브랜치캐시
- '액세스 기반 열거'
  - symlinks를 비활성화해야 합니다('-symlink-properties' 매개 변수의 값은 null ['] 이어야 함).

공유 경로에 대한 정보입니다

원격 VSS를 사용하여 Hyper-V 파일을 백업하는 경우 Hyper-V 서버에서 가상 머신 파일이 저장된 스토리지 위치로 SMB 연결을 설정할 때 사용할 공유 경로를 선택해야 합니다. 네임스페이스에서 어느 지점에서나 공유를 생성할 수 있지만 Hyper-V 서버가 사용하는 공유의 경로에 접합된 볼륨이 포함되어서는 안 됩니다. 교차점이 포함된 공유 경로에서는 섀도 복사본 작업을 수행할 수 없습니다.

SQL Server는 데이터베이스 디렉토리 구조를 생성할 때 교차점을 교차할 수 없습니다. 교차점이 포함된 SQL Server에 대한 공유 경로를 생성할 수 없습니다.

예를 들어, 표시된 네임스페이스를 사용할 경우 가상 머신 파일 또는 데이터베이스 파일을 볼륨 ""vol1"", ""vol2"", ""vol3"", ""vol4""에 저장하려면 "/data1/vol1", "/data1/vol2", "/data2/data4" 경로에 애플리케이션 서버의 공유를 생성해야 합니다.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

관리 관리를 위해 및 `/data2` 경로에 공유를 만들 수 있지만 `/data1`, 애플리케이션 서버가 이러한 공유를 사용하여 데이터를 저장하도록 구성하지 마십시오.

계획 워크시트

정보 유형	값
_볼륨 1: SMB 공유 이름 및 경로 _	
_Volume 2: SMB 공유 이름 및 경로 _	
_Volume 3: SMB 공유 이름 및 경로 _	

정보 유형	값
_Volume 4: SMB 공유 이름 및 경로 _	
_Volume 5: SMB 공유 이름 및 경로 _	
_Volume 6: SMB 공유 이름 및 경로 _	
_Volume 7: SMB 공유 이름 및 경로 _	
_추가 볼륨: SMB 공유 이름 및 경로 _	

SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영을 위한 ONTAP 구성 생성

SMB를 통한 **Hyper-V** 및 **SQL Server**의 무중단 운영을 위한 **ONTAP** 구성 개요를 제공합니다

SMB를 통한 무중단 운영을 제공하는 Hyper-V 및 SQL Server 설치를 준비하기 위해 수행해야 하는 몇 가지 ONTAP 구성 단계가 있습니다.

SMB를 통해 Hyper-V 및 SQL Server의 무중단 운영을 위한 ONTAP 구성을 생성하기 전에 다음 작업을 완료해야 합니다.

- 클러스터에서 시간 서비스를 설정해야 합니다.
- SVM에 대해 네트워킹을 설정해야 합니다.
- SVM을 생성해야 합니다.
- 데이터 LIF 인터페이스는 SVM에서 구성해야 합니다.
- SVM에서 DNS를 구성해야 합니다.
- SVM에 대해 원하는 이름 서비스를 설정해야 합니다.
- SMB 서버를 생성해야 합니다.

관련 정보

SMB를 통한 Hyper-V 또는 SQL Server 구성 계획

구성 요구 사항 및 고려 사항

Kerberos 및 **NTLMv2** 인증이 모두 허용되는지 확인**(SMB** 공유를 통한 **Hyper-V)**

SMB를 통한 Hyper-V의 무중단 운영에서는 데이터 SVM 및 Hyper-V 서버의 CIFS 서버가 Kerberos 및 NTLMv2 인증을 모두 허용해야 합니다. 허용되는 인증 방법을 제어하는 CIFS 서버와 Hyper-V 서버 모두에서 설정을 확인해야 합니다.

이 작업에 대해

지속적으로 사용 가능한 공유 연결을 만들 때는 Kerberos 인증이 필요합니다. 원격 VSS 프로세스의 일부는 NTLMv2 인증을 사용합니다. 따라서 SMB를 통한 Hyper-V 구성에서는 두 인증 방법을 모두 사용하는 연결이 지원되어야 합니다.

Kerberos 및 NTLMv2 인증을 모두 허용하도록 다음 설정을 구성해야 합니다.

- 스토리지 가상 시스템(SVM)에서 SMB를 위한 엑스포트 정책을 사용하지 않도록 설정해야 합니다.

Kerberos 및 NTLMv2 인증은 항상 SVM에서 활성화되지만, 엑스포트 정책을 사용하여 인증 방법에 따라 액세스를 제한할 수 있습니다.

SMB에 대한 엑스포트 정책은 선택 사항이며 기본적으로 비활성화되어 있습니다. 내보내기 정책을 사용하지 않도록 설정하면 기본적으로 CIFS 서버에서 Kerberos 및 NTLMv2 인증이 모두 허용됩니다.

- CIFS 서버 및 Hyper-V 서버가 속하는 도메인은 Kerberos 및 NTLMv2 인증을 모두 허용해야 합니다.

Kerberos 인증은 Active Directory 도메인에서 기본적으로 활성화됩니다. 그러나 보안 정책 설정 또는 그룹 정책을 사용하여 NTLMv2 인증을 허용하지 않을 수 있습니다.

단계

1. SVM에서 엑스포트 정책이 비활성화되어 있는지 확인하려면 다음을 수행하십시오.
   a. 권한 수준을 고급으로 설정합니다.

      ' * set-Privilege advanced * '

   b. '-is-exportpolicy-enabled' CIFS server 옵션이 'false'로 설정되어 있는지 확인합니다.

      '* vserver cifs options show -vserver_vserver_name_-fields vserver, is-exportpolicy-enabled *

   c. 관리자 권한 레벨로 돌아갑니다.

      ' * set-privilege admin * '

2. SMB에 대한 엑스포트 정책이 비활성화되어 있지 않으면 다음을 비활성화하십시오.

   '* vserver cifs options modify -vserver_vserver_name_-is-exportpolicy -enabled false *

3. 도메인에서 NTLMv2 및 Kerberos 인증이 모두 허용되는지 확인합니다.

   도메인에서 허용되는 인증 방법을 결정하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

4. 도메인이 NTMLv2 인증을 허용하지 않는 경우 Microsoft 설명서에 설명된 방법 중 하나를 사용하여 NTLMv2 인증을 사용하도록 설정합니다.

예

다음 명령을 실행하면 SVM VS1 에서 SMB용 엑스포트 정책이 비활성화되어 있는지 확인할 수 있습니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

cluster1::*> set -privilege admin
```

도메인 계정이 **ONTAP**의 기본 **UNIX** 사용자에게 매핑되는지 확인합니다

Hyper-V 및 SQL Server는 도메인 계정을 사용하여 지속적으로 사용 가능한 공유에 대한 SMB 연결을 생성합니다. 연결을 성공적으로 생성하려면 컴퓨터 계정이 UNIX 사용자에게 성공적으로 매핑되어야 합니다. 이 작업을 수행하는 가장 편리한 방법은 컴퓨터 계정을 기본 UNIX 사용자에게 매핑하는 것입니다.

이 작업에 대해

Hyper-V 및 SQL Server는 도메인 컴퓨터 계정을 사용하여 SMB 연결을 만듭니다. 또한 SQL Server는 도메인 사용자 계정을 서비스 계정으로 사용하여 SMB 연결을 만듭니다.

스토리지 가상 머신(SVM)을 생성하면 ONTAP에서 자동으로 기본 사용자 이름을 생성합니다. `pcuser` (UID가 있는 `65534`) 및 그룹 이름 `pcuser` (GID가 있는 `65534`), 그리고 기본 사용자를 추가합니다. `pcuser` 그룹. 클러스터를 Data ONTAP 8.2로 업그레이드하기 전에 존재했던 SVM에서 SMB를 통한 Hyper-V 솔루션을 구성하는 경우 기본 사용자 및 그룹이 없을 수 있습니다. 그렇지 않으면 CIFS 서버의 기본 UNIX 사용자를 구성하기 전에 생성해야 합니다.

단계

1. 기본 UNIX 사용자가 있는지 확인합니다.

   ```
   vserver cifs options show -vserver <vserver_name>
   ```

2. 기본 사용자 옵션이 설정되지 않은 경우 기본 UNIX 사용자로 지정할 수 있는 UNIX 사용자가 있는지 확인합니다.

   ```
   vserver services unix-user show -vserver <vserver_name>
   ```

3. 기본 사용자 옵션이 설정되어 있지 않고 기본 UNIX 사용자로 지정할 수 있는 UNIX 사용자가 없는 경우, 기본 그룹과 기본 UNIX 사용자를 만들고, 기본 사용자를 그룹에 추가합니다.
4. 기본 그룹에는 일반적으로 "pcuser"라는 그룹 이름이 지정됩니다 그룹에 할당된 GID는 `65534` 이어야 합니다.
   a. 기본 그룹을 만듭니다.

```
vserver services unix-group create -vserver <vserver_name> -name
pcuser -id 65534
```

b. 기본 사용자를 만들고 기본 그룹에 기본 사용자를 추가합니다.

```
vserver services unix-user create -vserver <vserver_name> -user
pcuser -id 65534 -primary-gid 65534
```

c. 기본 사용자와 기본 그룹이 올바르게 구성되었는지 확인하세요.

```
vserver services unix-user show -vserver <vserver_name>
```

```
vserver services unix-group show -vserver <vserver_name> -members
```

5. CIFS 서버의 기본 사용자가 구성되지 않은 경우 다음을 수행합니다.

a. 기본 사용자를 구성합니다.

```
vserver cifs options modify -vserver <vserver_name> -default-unix
-user pcuser
```

b. 기본 UNIX 사용자가 올바르게 구성되었는지 확인합니다.

```
vserver cifs options show -vserver <vserver_name>
```

6. 애플리케이션 서버의 컴퓨터 계정이 기본 사용자에게 올바르게 매핑되었는지 확인하려면 SVM에 상주하는 공유에 드라이브를 매핑하고 "vserver cifs session show" 명령을 사용하여 Windows 사용자를 UNIX 사용자 매핑으로 확인합니다.

에 대한 자세한 내용은 `vserver cifs options` "ONTAP 명령 참조입니다"을 참조하십시오.

예

존재합니다. `pcuser` 사용자는 SVM vs1에서 CIFS 서버의 기본 사용자로 지정됩니다.

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
```

```
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

SVM 루트 볼륨의 보안 스타일이 **NTFS**로 설정되어 있는지 확인합니다

Hyper-V 및 SQL Server over SMB의 무중단 운영이 성공하려면 NTFS 보안 스타일로 볼륨을 만들어야 합니다. 루트 볼륨의 보안 스타일은 SVM(스토리지 가상 머신)에서 생성된 볼륨에

기본적으로 적용되므로 루트 볼륨의 보안 스타일을 NTFS로 설정해야 합니다.

이 작업에 대해

- SVM을 생성할 때 루트 볼륨 보안 스타일을 지정할 수 있습니다.
- 루트 볼륨이 NTFS 보안 스타일로 설정되어 있는 SVM이 생성되지 않으면 나중에 'volume modify' 명령을 사용하여 보안 스타일을 변경할 수 있습니다.

단계

1. SVM 루트 볼륨의 현재 보안 유형을 확인합니다.

   '* volume show -vserver_vserver_name_- 필드 vserver, 볼륨, 보안 스타일 *

2. 루트 볼륨이 NTFS 보안 스타일 볼륨이 아닌 경우 보안 스타일을 NTFS로 변경합니다.

   '* volume modify -vserver_vserver_name_-volume root_volume_name -security-style NTFS * '

3. SVM 루트 볼륨이 NTFS 보안 스타일로 설정되었는지 확인합니다.

   '* volume show -vserver_vserver_name_- 필드 vserver, 볼륨, 보안 스타일 *

예

다음 명령은 SVM VS1 에서 루트 볼륨 보안 스타일이 NTFS인지 확인합니다.

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

필요한 **CIFS** 서버 옵션이 구성되었는지 확인합니다

필요한 CIFS 서버 옵션이 Hyper-V 및 SQL Server over SMB의 무중단 운영 요구 사항에 따라 설정 및 구성되었는지 확인해야 합니다.

이 작업에 대해

- SMB 2.x 및 SMB 3.0을 활성화해야 합니다.
- ODX 복사 오프로드를 사용하여 성능을 향상시키려면 ODX 복사 오프로드를 활성화해야 합니다.
- Hyper-V over SMB 솔루션에서 원격 VSS 지원 백업 서비스를 사용하는 경우 VSS Shadow Copy 서비스를 활성화해야 합니다(Hyper-V만 해당).

단계

1. 필요한 CIFS 서버 옵션이 SVM(스토리지 가상 시스템)에서 설정되었는지 확인합니다.
   a. 권한 수준을 고급으로 설정합니다.

      ' * set-Privilege advanced * '

   b. 다음 명령을 입력합니다.

      '* vserver CIFS options show -vserver_vserver_name_ *'

      다음 옵션은 "참"으로 설정해야 합니다.

      - '-SMB2-ENABLED'입니다
      - '-SMB3-enabled'입니다
      - '-copy-offload-enabled'
      - '-shadowcopy -enabled'(Hyper-V만 해당)
2. "참"으로 설정되어 있지 않은 옵션이 있는 경우 다음을 수행하십시오.
   a. vserver cifs options modify 명령을 사용하여 "true"로 설정합니다.
   b. vserver cifs options show 명령을 사용하여 옵션이 "true"로 설정되어 있는지 확인합니다.
3. 관리자 권한 레벨로 돌아갑니다.

   ' * set-privilege admin * '

예

다음 명령은 SVM VS1 기반 Hyper-V 구성에 필요한 옵션이 설정되어 있는지 확인합니다. 이 예에서는 옵션 요구 사항을 충족하도록 ODX 복사 오프로드를 활성화해야 합니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

성능 및 이중화를 위해 **SMB** 멀티 채널을 구성합니다

ONTAP 9.4부터 SMB 다중 채널을 구성하여 단일 SMB 세션에서 ONTAP와 클라이언트 간에 여러 연결을 제공할 수 있습니다. 이렇게 하면 SMB 구성에서 Hyper-V 및 SQL Server의 처리량과 내결함성을 향상시킬 수 있습니다.

시작하기 전에

SMB 3.0 이상 버전에서 클라이언트가 협상하는 경우에만 SMB 멀티 채널 기능을 사용할 수 있습니다. SMB 3.0 이상은 기본적으로 ONTAP SMB 서버에서 사용하도록 설정됩니다.

이 작업에 대해

ONTAP 클러스터에서 적절한 구성이 식별되는 경우 SMB 클라이언트가 자동으로 여러 네트워크 연결을 감지하고 사용합니다.

SMB 세션의 동시 연결 수는 구축한 NIC에 따라 달라집니다.

- * 클라이언트와 ONTAP 클러스터의 1G NIC *

  클라이언트는 NIC당 하나의 연결을 설정하고 모든 연결에 세션을 바인딩합니다.

- * 클라이언트 및 ONTAP 클러스터에 10G 이상의 대용량 NIC *

  클라이언트는 NIC당 최대 4개의 연결을 설정하고 모든 연결에 세션을 바인딩합니다. 클라이언트는 여러 개의 10G 및 대용량 NIC에 연결을 설정할 수 있습니다.

다음 매개 변수(고급 권한)도 수정할 수 있습니다.

- `-max-connections-per-session`

  다중 채널 세션당 허용되는 최대 연결 수입니다. 기본값은 32개 연결입니다.

  기본값보다 더 많은 연결을 설정하려면 기본값인 32개의 연결을 사용하는 클라이언트 구성을 동일하게 조정해야 합니다.

- `-max-lifs-per-session`

  Multichannel 세션당 공고되는 최대 네트워크 인터페이스 수입니다. 기본값은 256개의 네트워크 인터페이스입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. SMB 서버에서 SMB 멀티 채널 활성화:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. ONTAP가 SMB 멀티 채널 세션을 보고하는지 확인합니다.

```
vserver cifs session show
```

4. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

예

다음 예에서는 모든 SMB 세션에 대한 정보를 표시하며 단일 세션에 대해 여러 개의 연결을 표시합니다.

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

다음 예에서는 세션 ID 1이 있는 SMB 세션에 대한 자세한 정보를 표시합니다.

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
                Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

NTFS 데이터 볼륨을 생성합니다

Hyper-V 또는 SQL Server over SMB 애플리케이션 서버에서 사용할 수 있도록 지속적으로 사용 가능한 공유를 구성하려면 먼저 SVM(스토리지 가상 머신)에 NTFS 데이터 볼륨을

생성해야 합니다. 볼륨 구성 워크시트를 사용하여 데이터 볼륨을 생성합니다.

이 작업에 대해

데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 선택적 매개 변수가 있습니다. 볼륨 사용자 지정에 대한 자세한 내용은 를 참조하십시오 "논리적 스토리지 관리".

데이터 볼륨을 생성할 때 다음을 포함하는 볼륨 내에 교차점을 생성해서는 안 됩니다.

- ONTAP에서 섀도 복사본을 만드는 Hyper-V 파일입니다
- SQL Server를 사용하여 백업되는 SQL Server 데이터베이스 파일입니다

> 혼합 또는 UNIX 보안 스타일을 사용하는 볼륨을 실수로 만든 경우 볼륨을 NTFS 보안 스타일 볼륨으로 변경한 다음 이 볼륨을 직접 사용하여 무중단 운영을 위해 지속적으로 사용 가능한 공유를 생성할 수 없습니다. Hyper-V 및 SQL Server over SMB의 무중단 운영은 구성에 사용된 볼륨이 NTFS 보안 스타일 볼륨으로 만들어지지 않는 한 제대로 작동하지 않습니다. 볼륨을 삭제하고 NTFS 보안 스타일로 볼륨을 다시 생성해야 합니다. 또는 Windows 호스트에서 볼륨을 매핑하고 볼륨 상단에 ACL을 적용하고 볼륨의 모든 파일 및 폴더에 ACL을 전파할 수 있습니다.

단계

1. 적절한 명령을 입력하여 데이터 볼륨을 생성합니다.

SVM에서 루트 볼륨 보안 유형이 인 볼륨을 생성하려는 경우...	명령 입력...
NTFS입니다	'* volume create-vserver_vserver_name_-volume_volume_name_-aggregate_aggregate_name_-size 정수 [KB|MB|GB|TB|PB]-junction-path_path_ *'
NTFS가 아닙니다	'* volume create-vserver_vserver_name_-volume_volume_name_-aggregate_aggregate_name_-size integer [KB|MB|GB|TB|PB]-security-style NTFS-junction-path *'

2. 볼륨 구성이 올바른지 확인합니다.

   '* volume show -vserver_vserver_name_-volume_volume_name_*'

지속적으로 사용 가능한 **SMB** 공유를 생성합니다

데이터 볼륨을 생성한 후 애플리케이션 서버가 Hyper-V 가상 머신 및 구성 파일, SQL Server 데이터베이스 파일에 액세스하는 데 사용하는 연속 사용 가능한 공유를 생성할 수 있습니다. SMB 공유를 생성할 때 공유 구성 워크시트를 사용해야 합니다.

단계

1. 기존 데이터 볼륨 및 연결 경로에 대한 정보를 표시합니다.

   '* volume show -vserver_vserver_name_-junction *'

2. 지속적으로 사용 가능한 SMB 공유 생성:

'* vserver CIFS 공유 create-vserver_vserver_name_-share-name_share_name_-path_path_-share-properties oplocks, Continuously-available-symlink""[-comment text] *'

- 필요에 따라 공유 구성에 주석을 추가할 수 있습니다.
- 기본적으로 오프라인 파일 공유 속성은 공유에서 구성되며 '수동'으로 설정됩니다.
- ONTAP는 Everyone/Full Control의 Windows 기본 공유 권한으로 공유를 생성합니다.

3. 공유 구성 워크시트의 모든 공유에 대해 이전 단계를 반복합니다.
4. 'vserver cifs share show' 명령을 사용하여 구성이 올바른지 확인하십시오.
5. 드라이브를 각 공유에 매핑하고 * Windows 속성 * 창을 사용하여 파일 권한을 구성하여 지속적으로 사용 가능한 공유에서 NTFS 파일 권한을 구성합니다.

예

다음 명령을 실행하면 스토리지 가상 머신(SVM, 이전 명칭 Vserver) VS1 에 "data2"라는 이름의 연속 사용 가능한 공유가 생성됩니다. '-symlink' 매개변수를 ""로 설정하면 Symlink가 비활성화됩니다.

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                  Junction
Vserver   Volume     Active   Junction Path    Path Source
--------- ---------- -------- ---------------- ------------
vs1       data       true     /data            RW_volume
vs1       data1      true     /data/data1      RW_volume
vs1       data2      true     /data/data2      RW_volume
vs1       vs1_root   -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
            Share Properties: oplocks
                              continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

sSecurityPrivilege 권한을 사용자 계정에 추가합니다**(SMB** 공유의 **SQL Server**에 해당**).**

SQL Server 설치에 사용되는 도메인 사용자 계정에는 "'seSecurityPrivilege'" 권한이 할당되어 있어야 도메인 사용자에게 기본적으로 할당되지 않은 권한이 필요한 CIFS 서버에서 특정 작업을 수행할 수 있습니다.

시작하기 전에

SQL Server 설치에 사용되는 도메인 계정이 이미 있어야 합니다.

이 작업에 대해

SQL Server 설치 관리자의 계정에 권한을 추가할 때 ONTAP는 도메인 컨트롤러에 연락하여 계정의 유효성을 검사할 수 있습니다. ONTAP가 도메인 컨트롤러에 연결할 수 없으면 명령이 실패할 수 있습니다.

단계

1. "seSecurityPrivilege" 권한 추가:

   '* vserver cifs users-and-groups 권한 add-privilege-vserver_vserver_name_-user-or-group-name_account_name_-Privileges SeSecurityPrivilege*'

   '-user-or-group-name' 매개 변수의 값은 SQL Server 설치에 사용되는 도메인 사용자 계정의 이름입니다.

2. 계정에 권한이 적용되는지 확인합니다.

   '* vserver cifs users-and-groups 권한 show -vserver_vserver_name_-user-or-group -name_account_name_*'

예

다음 명령을 실행하면 SVM(Storage Virtual Machine) VS1 예제 도메인의 SQL Server 설치 관리자 계정에 "seSecurityPrivilege" 권한이 추가됩니다.

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name           Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

VSS 섀도우 복제본 디렉토리 깊이 구성**(SMB** 공유를 통한 **Hyper-V**의 경우**)**

필요에 따라 SMB 공유 내에서 섀도우 복제본을 생성할 디렉토리의 최대 깊이를 구성할 수 있습니다. 이 매개 변수는 ONTAP에서 섀도 복사본을 만들어야 하는 하위 디렉터리의 최대 수준을 수동으로 제어하려는 경우에 유용합니다.

시작하기 전에

VSS 섀도우 복제본 기능을 활성화해야 합니다.

이 작업에 대해

기본값은 최대 5개의 하위 디렉토리에 대한 섀도우 복제본을 생성하는 것입니다. 이 값이 '0'으로 설정되면 ONTAP는 모든 하위 디렉토리에 대한 섀도우 복제본을 만듭니다.

> 섀도우 복제본 세트 디렉토리 깊이에 5개 이상의 하위 디렉토리나 모든 하위 디렉토리가 포함되도록 지정할 수 있지만 섀도우 복제본 세트 생성이 60초 이내에 완료되어야 한다는 Microsoft 요구 사항이 있습니다. 이 시간 내에 완료할 수 없는 경우 섀도우 복제본 세트 생성이 실패합니다. 선택한 섀도 복사본 디렉토리 깊이로 인해 생성 시간이 시간 제한을 초과하지 않아야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   ' * set-Privilege advanced * '

2. VSS 섀도우 복제본 디렉토리 깊이를 원하는 레벨로 설정합니다.

   ``vserver cifs options modify -vserver_vserver_name_-shadowcopy -dir -depth integer*'

   ``vserver cifs options modify -vserver vs1-shadowcopy -dir-depth 6 *'

3. 관리자 권한 레벨로 돌아갑니다.

   ' * set-privilege admin * '

SMB 구성을 통해 Hyper-V 및 SQL Server 관리

지속적인 가용성을 위해 기존 공유를 구성합니다

Hyper-V 및 SQL Server 애플리케이션 서버에서 Hyper-V 가상 머신 및 구성 파일, SQL Server 데이터베이스 파일에 중단 없이 액세스하는 데 사용하는 공유를 계속 사용할 수 있도록 기존 공유를 수정할 수 있습니다.

이 작업에 대해

공유에 다음과 같은 특성이 있는 경우 SMB를 통해 애플리케이션 서버와 무중단 운영을 위해 기존 공유를 지속적으로 사용할 수 있는 공유로 사용할 수 없습니다.

- 이 공유에 homedory 공유 속성이 설정되어 있으면
- 공유에 활성화된 symlink 또는 widelink가 포함된 경우
- 공유에 공유의 루트 아래에 접합된 볼륨이 포함되어 있는 경우

다음 두 공유 매개 변수가 올바르게 설정되었는지 확인해야 합니다.

- '-offline-files' 매개변수는 수동(기본값) 또는 없음(없음)으로 설정됩니다.
- Symlink를 비활성화해야 합니다.

다음 공유 속성을 구성해야 합니다.

- "계속 사용할 수 있습니다.

- oplocks

다음 공유 속성을 설정하지 않아야 합니다. 현재 공유 속성 목록에 있는 경우 지속적으로 사용 가능한 공유에서 제거해야 합니다.

- 'attributecache
- 브랜치캐시

단계

1. 현재 공유 매개 변수 설정 및 구성된 공유 속성의 현재 목록을 표시합니다.

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. 필요한 경우 명령을 사용하여 공유 매개 변수를 수정하여 symlink를 비활성화하고 오프라인 파일을 manual로 `vserver cifs share modify` 설정합니다.
   - '-symlink' 매개 변수의 값을 ""로 설정하여 symlink를 비활성화할 수 있습니다.
   - '-offline-files' 파라미터는 'Manual'을 지정하여 올바른 설정으로 설정할 수 있습니다.
3. 공유 속성을 추가하고 필요한 경우 공유 속성을 추가합니다 `continuously-available` `oplocks` .

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

   oplocks 공유 속성이 아직 설정되지 않은 경우 계속 사용 가능한 공유 속성과 함께 추가해야 합니다.

4. 지속적으로 사용 가능한 공유에서 지원되지 않는 공유 속성을 제거합니다.

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

   쉼표로 구분된 목록으로 공유 속성을 지정하여 하나 이상의 공유 속성을 제거할 수 있습니다.

5. '-symlink' 및 '-offline-files' 매개 변수가 올바르게 설정되었는지 확인합니다.

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. 구성된 공유 속성 목록이 올바른지 확인합니다.

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

예

다음 예에서는 SMB를 통해 애플리케이션 서버가 있는 NDOs에 대해 SVM(스토리지 가상 머신) "VS1"이라는 기존 공유를 구성하는 방법을 보여 줍니다.

- 매개 변수를 로 설정하면 공유에서 symlink가 `-symlink ""`비활성화됩니다.
- '-offline-file' 파라미터가 수정되어 'manual'로 설정됩니다.
- 이 공유에 계속 이용 가능한 공유자산이 추가됩니다.
- oplocks 공유 속성은 이미 공유 속성 목록에 있으므로 추가할 필요가 없습니다.
- 이 지분에서는 attributecache 공유재산을 빼내기도 합니다.
- "탐색 가능" 공유 속성은 SMB를 통해 애플리케이션 서버와 NDO에 사용되는 지속적인 사용 가능 공유에 대한 선택 사항이며 공유 속성 중 하나로 유지됩니다.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

SMB 백업을 통해 **Hyper-V**에 대한 **VSS** 섀도우 복제본을 설정하거나 해제합니다

VSS 인식 백업 애플리케이션을 사용하여 SMB 공유에 저장된 Hyper-V 가상 머신 파일을 백업하는 경우 VSS 섀도우 복제본을 설정해야 합니다. VSS 인식 백업 애플리케이션을 사용하지 않는 경우 VSS 섀도우 복제본을 비활성화할 수 있습니다. 기본값은 VSS 섀도우 복제본을 설정하는 것입니다.

이 작업에 대해

언제든지 VSS 섀도우 복제본을 설정하거나 해제할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   ' * set-Privilege advanced * '

2. 다음 작업 중 하나를 수행합니다.

VSS 섀도우 복제본을 만들려는 경우...	명령 입력...
활성화됨	``vserver cifs options modify -vserver_vserver_name_-shadowcopy -enabled true *'
사용 안 함	'* vserver cifs options modify -vserver_vserver_name_-shadowcopy -enabled false *

3. 관리자 권한 레벨로 돌아갑니다.

   ' * set-privilege admin * '

예

다음 명령을 실행하면 SVM VS1 에서 VSS 섀도우 복제본이 활성화됩니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

통계를 사용하여 **SMB** 작업을 통해 **Hyper-V** 및 **SQL Server**를 모니터링합니다

ONTAP에서 사용할 수 있는 통계 개체 및 카운터를 확인합니다

CIFS, SMB, 감사 및 BranchCache 해시 통계에 대한 정보를 얻고 성능을 모니터링하려면 데이터를 가져올 수 있는 개체와 카운터를 알고 있어야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

다음 사항을 확인하고자 하는 경우:	입력...
사용할 수 있는 개체	'통계 카탈로그 개체 쇼'
사용할 수 있는 특정 개체입니다	`statistics catalog object show -object` *`object_name`*
사용할 수 있는 카운터	`statistics catalog counter show -object` *`object_name`*

   자세히 알아보세요 `statistics catalog object show` 그리고 `statistics catalog counter show` 에서 "ONTAP 명령 참조입니다" .

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

예

다음 명령을 실행하면 고급 권한 수준에 표시된 대로 클러스터에서 CIFS 및 SMB 액세스와 관련된 선택한 통계 개체에 대한 설명이 표시됩니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

다음 명령을 실행하면 고급 권한 수준에서 표시되는 "CIFS" 개체의 일부 카운터에 대한 정보가 표시됩니다.

ⓘ 이 예제에서는 "CIFS" 객체에 대해 사용 가능한 카운터를 모두 표시하지 않고 출력이 잘립니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

에 대한 자세한 내용은 `statistics start` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP에서 **SMB** 통계를 표시합니다

다양한 SMB 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

단계

1. '통계 시작' 및 '통계 중지' 옵션 명령을 사용하여 데이터 샘플을 수집합니다.
2. 다음 작업 중 하나를 수행합니다.

에 대한 통계를 표시하려면...	다음 명령을 입력합니다...
모든 SMB 버전	' * statistics show-object cifs *'
SMB 1.0	' * statistics show-object SMB1 * '
SMB 2.x 및 SMB 3.0	' * statistics show-object SMB2 * '
노드의 SMB 하위 시스템입니다	'* statistics show -object nblade_cifs * '

관련 정보

- "통계에 따르면"
- "통계 시작"
- "통계 중지"

구성이 무중단 운영이 가능한지 확인합니다

상태 모니터링을 사용하여 무중단 운영 상태가 정상인지 확인하십시오

상태 모니터링 에서는 클러스터 전체의 시스템 상태에 대한 정보를 제공합니다. 상태 모니터는 SMB 구성을 통해 Hyper-V 및 SQL Server를 모니터링하여 애플리케이션 서버에 대한 무중단 운영(NDO)을 보장합니다. 상태가 성능 저하인 경우 가능한 원인 및 권장 복구 조치를 포함하여 문제에 대한 세부 정보를 볼 수 있습니다.

여러 개의 상태 모니터가 있습니다. ONTAP는 개별 상태 모니터의 전체 시스템 상태와 상태를 모두 모니터링합니다. 노드 연결 상태 모니터에는 CIFS-NDO 서브시스템이 포함되어 있습니다. 모니터에는 특정 물리적 조건으로 인해 운영 중단이 발생할 수 있는 경우 알림을 트리거하는 상태 정책이 있으며, 중단 상태가 있을 경우 알림을 생성하고 수정 조치에 대한 정보를 제공합니다. SMB 구성을 통한 NDO의 경우 다음 두 가지 조건에 대한 경고가 생성됩니다.

경고 **ID**	심각도입니다	조건
``HaNotReadyCifsNdo_Alert*’	전공	노드에서 애그리게이트에서 볼륨에 호스팅되는 하나 이상의 파일이 장애 발생 시 지속성을 약속하는 지속적으로 사용 가능한 SMB 공유를 통해 열렸습니다. 파트너와의 HA 관계는 구성되지 않았거나 상태가 아닙니다.

경고 **ID**	심각도입니다	조건
'* NoStandbyLifcifsNdo_Alert * '	경미합니다	SVM(스토리지 가상 머신)은 노드를 통해 SMB를 통해 데이터를 능동적으로 제공하고, 지속적으로 사용 가능한 공유를 통해 지속적으로 열려 있는 SMB 파일이 있지만, 해당 파트너 노드가 SVM을 위한 활성 데이터 LIF를 노출하지 않습니다.

시스템 상태 모니터링을 사용하여 무중단 운영 상태를 표시합니다

'시스템 상태' 명령을 사용하면 클러스터의 전체 시스템 상태 및 CIFS-NDO 하위 시스템의 상태에 대한 정보를 표시하고, 알림에 응답하고, 향후 알림을 구성하고, 상태 모니터링 구성 방법에 대한 정보를 표시할 수 있습니다.

단계

1. 적절한 작업을 수행하여 상태 모니터링:

를 표시하려면...	명령 입력...
개별 상태 모니터의 전체 상태를 반영하는 시스템의 상태입니다	'* 시스템 상태 표시 *'
CIFS-NDO 서브시스템의 상태에 대한 정보입니다	'* 시스템 상태 하위 시스템 표시 - 하위 시스템 cifs-NDO-instance*'

2. 적절한 작업을 수행하여 CIFS-NDO 알림 모니터링을 구성하는 방법에 대한 정보를 표시합니다.

다음에 대한 정보를 표시하려면...	명령 입력...
모니터링되는 노드, 초기화 상태 및 상태와 같은 CIFS-NDO 서브시스템에 대한 상태 모니터의 구성 및 상태입니다	'* 시스템 상태 구성 show-subsystem cifs-NDO *'
상태 모니터에서 잠재적으로 생성할 수 있는 CIFS-NDO 알림을 나타냅니다	'* 시스템 상태 경고 정의 show-subsystem cifs-NDO *'
CIFS-NDO 상태 모니터링 정책으로 알림이 발생하는 시기를 결정합니다	'* 시스템 상태 정책 정의 표시 - 모니터 노드 연결 * '

자세한 정보를 표시하려면 '-instance' 매개 변수를 사용합니다.

예

다음 출력에는 클러스터 및 CIFS-NDO 서브시스템의 전체 상태에 대한 정보가 표시됩니다.

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                    Subsystem: CIFS-NDO
                       Health: ok
         Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                         Node: node2
  Subsystem Refresh Interval: 5m
```

다음 출력에는 CIFS-NDO 서브시스템의 상태 모니터 구성 및 상태에 대한 자세한 정보가 나와 있습니다.

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                           Node: node1
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                           Node: node2
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

지속적으로 사용 가능한 **SMB** 공유 구성을 확인합니다

무중단 운영을 지원하려면 Hyper-V 및 SQL Server SMB 공유를 지속적으로 사용 가능한 공유로 구성해야 합니다. 또한 확인해야 할 다른 공유 설정도 있습니다. 계획된 또는 계획되지 않은 중단 이벤트가 있는 경우 공유가 애플리케이션 서버에 무중단 운영을 원활하게 제공하도록 올바르게 구성되었는지 확인해야 합니다.

이 작업에 대해

다음 두 공유 매개 변수가 올바르게 설정되었는지 확인해야 합니다.

- '-offline-files' 매개변수는 수동(기본값) 또는 없음(없음)으로 설정됩니다.

- Symlink를 비활성화해야 합니다.

적절한 무중단 운영을 위해서는 다음 공유 속성을 설정해야 합니다.

- "계속 사용할 수 있습니다.
- oplocks

다음 공유 속성을 설정하지 않아야 합니다.

- 홈디렉토리
- 'attributecache
- 브랜치캐시
- '액세스 기반 열거'

단계

1. 오프라인 파일이 '수동' 또는 '사용 안 함'으로 설정되어 있고 symlink가 비활성화되어 있는지 확인합니다.

   '* vserver CIFS 공유 show -vserver_vserver_name_*'

2. SMB 공유가 무중단 가용성을 위해 구성되었는지 확인합니다.

   '* vserver cifs 공유 속성 표시 - vserver_vserver_name_*'

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver) VS1 의 "shay1"이라는 공유 설정을 표시합니다. 오프라인 파일은 '수동'으로 설정되고 symlink는 비활성화됩니다('대칭 링크 속성' 필드 출력에서 하이픈으로 지정됨).

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: VS1
                         Path: /data/share1
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

다음 예에서는 SVM VS1 에서 "shay1"이라는 이름의 공유에 대한 공유 속성을 표시합니다.

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

LIF 상태를 확인합니다

Hyper-V와 SQL Server over SMB 구성을 통해 SVM(스토리지 가상 시스템)을 구성하여 클러스터의 각 노드에 LIF를 갖는 일상적인 작업을 수행하는 경우에도 일부 LIF는 다른 노드의 포트로 이동할 수 있습니다. LIF 상태를 확인하고 필요한 수정 조치를 취해야 합니다.

이 작업에 대해

원활한 무중단 운영 지원을 제공하려면 클러스터의 각 노드에 SVM을 위한 LIF가 하나 이상 있어야 하며 모든 LIF가 홈 포트와 연결되어야 합니다. 구성된 LIF 중 일부가 현재 홈 포트에 연결되어 있지 않으면 포트 문제를 해결한 다음 LIF를 홈 포트로 되돌려야 합니다.

단계

1. SVM을 위해 구성된 LIF 정보 표시:

   '* 네트워크 인터페이스 show -vserver_vserver_name_*'

   이 예에서 ""lif1"은 홈 포트에 없습니다.

   네트워크 인터페이스 show-vserver vs1

   ```
               Logical    Status     Network           Current    Current Is
   Vserver     Interface  Admin/Oper Address/Mask      Node       Port
   Home
   ----------- ---------- ---------- ----------------- ---------- -------
   ----
   vs1
               lif1         up/up    10.0.0.128/24     node2      e0d
   false
               lif2         up/up    10.0.0.129/24     node2      e0d
   true
   ```

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 일부 LIF가 홈 포트에 없는 경우 다음 단계를 수행하십시오.

   a. 각 LIF에서 LIF의 홈 포트가 무엇인지 확인합니다.

      '* 네트워크 인터페이스 show -vserver_vserver_name_-lif_lif_name_-fields home-node, home-port *

'* network interface show -vserver vs1-lif lif lif1-fields home-node, home-port * '

```
vserver lif  home-node  home-port
------- ---- ---------- ---------
vs1     lif1 node1      e0d
```

b. 각 LIF에서 LIF의 홈 포트가 작동하는지 확인합니다.

'* 네트워크 포트 show-node_node_name_-port_port_- 필드 포트, 링크 *

'network port show-node node1-port e0d-fields port, link

```
node       port link
---------- ---- ----
node1      e0d  up
```

이 예에서는 "lif1"을 홈 포트인 node1:e0d로 다시 마이그레이션해야 합니다.

에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. LIF와 연결되어야 하는 홈 포트 네트워크 인터페이스 중 하나가 상태에 있지 않은 경우 `up`, 이러한 인터페이스가 작동되도록 문제를 해결하십시오. 에 대한 자세한 내용은 `up` "ONTAP 명령 참조입니다"을 참조하십시오.
4. 필요한 경우 LIF를 홈 포트로 되돌립니다.

'* 네트워크 인터페이스 되돌리기 - vserver_vserver_name_-lif_lif_name_*'

'* 네트워크 인터페이스 되돌리기 - vserver vs1-lif lif liff li1*'

에 대한 자세한 내용은 `network interface revert` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 클러스터의 각 노드에 SVM을 위한 액티브 LIF가 있는지 확인합니다.

'* 네트워크 인터페이스 show -vserver_vserver_name_*'

'* 네트워크 인터페이스 show-vserver vs1*'

```
            Logical    Status     Network           Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask      Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node1      e0d
true
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

SMB 세션을 지속적으로 사용할 수 있는지 확인합니다

SMB 세션 정보를 표시합니다

SMB 연결 및 세션 ID와 세션을 사용하는 워크스테이션의 IP 주소를 포함하여 설정된 SMB 세션에 대한 정보를 표시할 수 있습니다. 세션의 SMB 프로토콜 버전 및 지속적으로 사용 가능한 보호 수준에 대한 정보를 표시하여 세션이 무중단 운영을 지원하는지 여부를 확인할 수 있습니다.

이 작업에 대해

SVM의 모든 세션에 대한 정보를 요약 형식으로 표시할 수 있습니다. 그러나 대부분의 경우 반환되는 출력량이 큽니다. 옵션 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다.

- 옵션 '-fields' 매개변수를 사용하여 선택한 필드에 대한 출력을 표시할 수 있습니다.

  필드를 입력할 수 있습니다 사용할 수 있는 필드를 결정합니다.

- '-instance' 매개 변수를 사용하면 설정된 SMB 세션에 대한 자세한 정보를 표시할 수 있습니다.
- '-fields' 매개 변수 또는 '-instance' 매개 변수를 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

SMB 세션 정보를 표시하려면...	다음 명령을 입력합니다...
SVM의 모든 세션에 대해 요약 양식을 작성합니다	'* vserver cifs session show -vserver_vserver_name_*'
지정된 연결 ID에 있습니다	'* vserver cifs session show -vserver_vserver_name_-connection-id integer *'
지정된 워크스테이션 IP 주소에서	'* vserver cifs session show -vserver_vserver_name_ -address_workstation_ip_address_ *'

SMB 세션 정보를 표시하려면...	다음 명령을 입력합니다...
지정된 LIF IP 주소입니다	'* vserver cifs session show -vserver_vserver_name_-lif -address_LIF_ip_address_ *'
지정된 노드에서	'* vserver cifs session show -vserver_vserver_name_-node{node_name
local} *'	지정된 Windows 사용자로부터
'* vserver cifs session show -vserver_vserver_name_ -windows -user_user_name_*' user_name 형식은 '[domain]\user'입니다.	지정된 인증 메커니즘을 사용합니다
'* vserver cifs session show -vserver_vserver_name_ -auth-mechanism authentication_mechanism *' '-auth-mechanism'의 값은 다음 중 하나일 수 있습니다. • "NTLMv1"입니다 • NTLMv2 • Kerberos • '익명'	지정된 프로토콜 버전을 사용하여

SMB 세션 정보를 표시하려면...	다음 명령을 입력합니다...
'* vserver cifs session show -vserver_vserver_name_ -protocol-version protocol_version *' '-protocol-version'의 값은 다음 중 하나일 수 있습니다. • 'MB1'입니다 • MB2 • MB2_1 • MB3 • 'MB3_1' 지속적으로 사용 가능한 보호 기능과 SMB 멀티 채널은 SMB 3.0 이상 세션에서만 사용할 수 있습니다. 모든 적격 세션에서 해당 상태를 보려면 이 매개 변수를 'MB3' 이상으로 설정한 값으로 지정해야 합니다.	지속적으로 사용 가능한 보호 수준을 지정합니다

SMB 세션 정보를 표시하려면...	다음 명령을 입력합니다...
'* vserver cifs session show -vserver_vserver_name_ -Continuously -available_Continuously_available_protection_level_*' '-연속 사용 가능'의 값은 다음 중 하나일 수 있습니다. • 아니 • 네 • 부분	지정된 SMB 서명 세션 상태

예

다음 명령을 실행하면 IP 주소가 10.1.1.1인 워크스테이션에서 설정된 SVM VS1 세션의 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

다음 명령을 실행하면 SVM VS1 에서 지속적으로 사용 가능한 보호 기능을 지원하는 세션에 대한 자세한 세션 정보가 표시됩니다. 도메인 계정을 사용하여 연결을 만들었습니다.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

다음 명령을 실행하면 SVM VS1 기반 SMB 3.0 및 SMB 멀티 채널을 사용하는 세션에 대한 세션 정보가 표시됩니다. 이 예에서 사용자는 LIF IP 주소를 사용하여 SMB 3.0 지원 클라이언트에서 이 공유에 연결했습니다. 따라서 인증 메커니즘은 NTLMv2로 기본값입니다. 지속적으로 사용 가능한 보호 기능을 사용하여 연결하려면 Kerberos 인증을 사용하여 연결해야 합니다.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

ONTAP에서 열린 **SMB** 파일에 대한 정보를 표시합니다

SMB 연결 및 세션 ID, 호스팅 볼륨, 공유 이름 및 공유 경로를 포함하여 열려 있는 SMB 파일에 대한 정보를 표시할 수 있습니다. 또한 파일의 지속적으로 사용 가능한 보호 수준에 대한 정보를 표시할 수도 있습니다. 이 정보는 열려 있는 파일이 무중단 작업을 지원하는 상태에 있는지 여부를 확인하는 데 유용합니다.

이 작업에 대해

설정된 SMB 세션에서 열린 파일에 대한 정보를 표시할 수 있습니다. 표시된 정보는 SMB 세션 내의 특정 파일에 대한 SMB 세션 정보를 확인해야 할 때 유용합니다.

예를 들어, 열린 파일 중 일부가 지속적으로 사용 가능한 보호 기능을 통해 열려 있고 일부는 지속적으로 사용 가능한 보호 기능을 통해 열려 있지 않은 SMB 세션이 있는 경우(vserver cifs session show 명령의 출력 값이 부분(Partial)인 경우), 이 명령을 사용하여 계속 사용할 수 없는 파일을 확인할 수 있습니다.

선택적 매개 변수 없이 'vserver cifs session file show' 명령을 사용하면 SVM(스토리지 가상 시스템)에서 설정된 SMB 세션의 모든 열려 있는 파일에 대한 정보를 요약 형식으로 표시할 수 있습니다.

그러나 대부분의 경우 반환되는 출력량이 큽니다. 선택적 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다. 이 기능은 열려 있는 파일의 작은 하위 집합에 대한 정보만 보려는 경우에 유용합니다.

- 옵션 '-fields' 매개변수를 사용하여 선택한 필드에 출력을 표시할 수 있습니다.

이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

- '-instance' 매개 변수를 사용하여 열려 있는 SMB 파일에 대한 자세한 정보를 표시할 수 있습니다.

  이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

열려 있는 **SMB** 파일을 표시하려면...	다음 명령을 입력합니다...
SVM에 대해 요약 형식으로 표시됩니다	'* vserver cifs 세션 파일 표시 -vserver_vserver_name_*'
지정된 노드에서	'* vserver CIFS 세션 파일 show -vserver_vserver_name_-node{node_name
local} *	지정된 파일 ID에 있습니다
'* vserver cifs 세션 파일 표시 -vserver_vserver_name_-file-id integer*'	지정된 SMB 연결 ID에서
'* vserver cifs 세션 파일 표시 -vserver_vserver_name_-connection-id integer*'	지정된 SMB 세션 ID에서
'* vserver cifs 세션 파일 표시 -vserver_vserver_name_-session-id integer*'	지정된 호스팅 집계에서
'* vserver cifs 세션 파일 표시 -vserver_vserver_name_-hosting-aggregate_aggregate_name_*'	지정된 볼륨에서
'* vserver cifs 세션 파일 표시 -vserver_vserver_name_-hosting-volume_volume_name_*'	지정된 SMB 공유에서
'* vserver CIFS 세션 파일 표시 -vserver_vserver_name_-share_share_name_*'	지정된 SMB 경로에 있어야 합니다
'* vserver CIFS 세션 파일 표시 -vserver_vserver_name_-path_path_*'	지속적으로 사용 가능한 보호 수준을 지정합니다

열려 있는 **SMB** 파일을 표시하려면…	다음 명령을 입력합니다…
'* vserver cifs 세션 파일 표시 -vserver_vserver_name_-Continuously-available_Continuously_available_status_ * '-연속 사용 가능'의 값은 다음 중 하나일 수 있습니다. • 아니 • 네 계속 사용 가능한 상태가 '아니요'인 경우 열려 있는 파일은 Takeover와 Giveback에서 중단 없이 복구할 수 없습니다. 또한, 고가용성 관계에 있는 파트너 간의 일반 애그리게이트 재배치에서 복구할 수 없습니다.	지정된 다시 연결된 상태에서

출력 결과를 구체화하는 데 사용할 수 있는 추가 선택적 매개 변수가 있습니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

예

다음 예에서는 SVM VS1 에서 열린 파일에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

다음 예에서는 SVM VS1에서 파일 ID 82가 있는 개방형 SMB 파일에 대한 자세한 정보를 표시합니다.

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

SAN 스토리지 관리

SAN 개념

iSCSI를 사용한 SAN 프로비저닝

SAN 환경에서 스토리지 시스템은 스토리지 대상 디바이스가 있는 타겟입니다. iSCSI 및 FC의 경우 스토리지 타겟 디바이스를 LUN(논리 유닛)이라고 합니다. Fibre Channel을 통한 NVMe(Non-Volatile Memory Express)의 경우 스토리지 타겟 디바이스를 네임스페이스라고 합니다.

iSCSI 및 FC용 LUN을 생성하거나 NVMe용 네임스페이스를 생성하여 스토리지를 구성합니다. 그런 다음 iSCSI(Internet Small Computer Systems Interface) 또는 FC(Fibre Channel) 프로토콜 네트워크를 사용하여 호스트에서 LUN 또는 네임스페이스에 액세스합니다.

iSCSI 네트워크에 연결하기 위해 호스트는 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 통합 네트워크 어댑터(CNA) 또는 전용 iSCSI 호스트 버스 어댑터(HBA)를 사용할 수 있습니다.

FC 네트워크에 접속하려면 호스트에 FC HBA 또는 CNA가 필요합니다.

지원되는 FC 프로토콜은 다음과 같습니다.

- FC
- FCoE 를 참조하십시오
- NVMe를 참조하십시오

iSCSI 타겟 노드 네트워크 연결 및 이름

iSCSI 타겟 노드는 다음과 같은 여러 가지 방법으로 네트워크에 연결할 수 있습니다.

- ONTAP에 통합된 소프트웨어를 사용하는 이더넷 인터페이스를 통해.
- 다중 시스템 인터페이스, iSCSI에 사용되는 인터페이스로 SMB 및 NFS와 같은 다른 프로토콜의 트래픽을 전송할 수 있습니다.
- UTA(통합 타겟 어댑터) 또는 CNA(통합 네트워크 어댑터) 사용

모든 iSCSI 노드에는 노드 이름이 있어야 합니다.

iSCSI 노드 이름에 대한 두 형식 또는 형식 지정자는 _iqn_과 _eui_입니다. SVM iSCSI 타겟은 항상 iqn형 지정자를 사용합니다. 이니시에이터는 iqn 유형 또는 eui 유형 지정자를 사용할 수 있습니다.

스토리지 시스템 노드 이름입니다

iSCSI를 실행하는 각 SVM에는 역방향 도메인 이름과 고유한 인코딩 번호를 기반으로 하는 기본 노드 이름이 있습니다.

노드 이름은 다음 형식으로 표시됩니다.

iqn.1992-08.com.netapp:sn.*unique-encoding-number*

다음 예에서는 고유한 인코딩 번호가 있는 스토리지 시스템의 기본 노드 이름을 보여 줍니다.

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

iSCSI용 TCP 포트

iSCSI 프로토콜은 ONTAP에서 TCP 포트 번호 3260을 사용하도록 구성되어 있습니다.

ONTAP는 iSCSI의 포트 번호 변경을 지원하지 않습니다. 포트 번호 3260은 iSCSI 사양의 일부로 등록되었으며 다른 애플리케이션이나 서비스에서 사용할 수 없습니다.

관련 정보

"NetApp 설명서: ONTAP SAN 호스트 구성"

iSCSI 서비스 관리

iSCSI 서비스 관리

"vserver iSCSI interface enable" 또는 "vserver iscsi interface disable" 명령을 사용하여 SVM(스토리지 가상 시스템)의 iSCSI 논리 인터페이스에서 iSCSI 서비스의 가용성을 관리할 수 있습니다.

기본적으로 iSCSI 서비스는 모든 iSCSI 논리 인터페이스에서 활성화됩니다.

호스트에서 iSCSI를 구현하는 방법

iSCSI는 하드웨어 또는 소프트웨어를 사용하여 호스트에서 구현할 수 있습니다.

다음 방법 중 하나로 iSCSI를 구현할 수 있습니다.

- 호스트의 표준 이더넷 인터페이스를 사용하는 이니시에이터 소프트웨어 사용
- iSCSI HBA(호스트 버스 어댑터)를 통해: iSCSI HBA가 호스트 운영 체제에 로컬 디스크가 있는 SCSI 디스크 어댑터로 나타납니다.
- TCP/IP 처리를 오프로드하는 TOE(TCP Offload Engine) 어댑터 사용

  iSCSI 프로토콜 처리는 호스트 소프트웨어에 의해 계속 수행됩니다.

iSCSI 인증의 작동 방식

iSCSI 세션의 초기 단계 중에 이니시에이터는 iSCSI 세션을 시작하기 위해 스토리지 시스템에 로그인 요청을 보냅니다. 그러면 스토리지 시스템에서 로그인 요청을 허용하거나 거부하거나 로그인이 필요하지 않음을 확인합니다.

iSCSI 인증 방법은 다음과 같습니다.

- CHAP(Challenge Handshake Authentication Protocol) — 초기자는 CHAP 사용자 이름 및 암호를 사용하여 로그인합니다.

CHAP 암호를 지정하거나 16진수 암호 암호를 생성할 수 있습니다. CHAP 사용자 이름과 암호는 두 가지 유형이 있습니다.

  - 인바운드 — 스토리지 시스템이 이니시에이터를 인증합니다.

    CHAP 인증을 사용하는 경우 인바운드 설정이 필요합니다.

  - 아웃바운드 — 초기자가 스토리지 시스템을 인증할 수 있도록 하는 선택적 설정입니다.

    스토리지 시스템에서 인바운드 사용자 이름과 암호를 정의한 경우에만 아웃바운드 설정을 사용할 수 있습니다.

- deny — 스토리지 시스템에 대한 액세스가 거부됩니다.
- 없음 — 스토리지 시스템은 이니시에이터에 대한 인증을 요구하지 않습니다.

이니시에이터 목록과 해당 인증 방법을 정의할 수 있습니다. 이 목록에 없는 이니시에이터에 적용되는 기본 인증 방법을 정의할 수도 있습니다.

관련 정보

"Data ONTAP를 사용하는 Windows 다중 경로 옵션: Fibre Channel 및 iSCSI"

iSCSI 초기자 보안 관리

ONTAP는 iSCSI 초기자에 대한 보안을 관리하는 다양한 기능을 제공합니다. iSCSI 초기자 목록과 각각에 대한 인증 방법을 정의하고, 인증 목록에 초기자 및 관련 인증 방법을 표시하고, 인증 목록에서 이니시에이터를 추가 및 제거하고, 목록에 없는 이니시에이터에 대한 기본 iSCSI 초기자 인증 방법을 정의할 수 있습니다.

iSCSI 엔드포인트 격리

기존 iSCSI 보안 명령에서는 IP 주소 범위 또는 여러 IP 주소를 사용할 수 있습니다.

모든 iSCSI 초기자는 세션 또는 대상과의 연결을 설정할 때 발신 IP 주소를 제공해야 합니다. 이 새로운 기능은 원본 IP 주소가 지원되지 않거나 알려지지 않은 경우 이니시에이터가 클러스터에 로그인하지 못하도록 하여 고유한 식별 체계를 제공합니다. 지원되지 않거나 알 수 없는 IP 주소에서 시작된 모든 이니시에이터는 iSCSI 세션 계층에서 로그인이 거부되어 이니시에이터가 클러스터 내의 LUN 또는 볼륨에 액세스하지 못하게 됩니다.

두 개의 새로운 명령으로 이 새로운 기능을 구현하여 기존 항목을 관리할 수 있습니다.

이니시에이터 주소 범위를 추가합니다

"vserver iscsi security add-initiator-address-range" 명령을 사용하여 IP 주소 범위 또는 여러 IP 주소를 추가하여 iSCSI 초기자 보안 관리를 향상시킵니다.

'cluster1::> vserver iscsi security add-initiator-address-range'

이니시에이터 주소 범위를 제거합니다

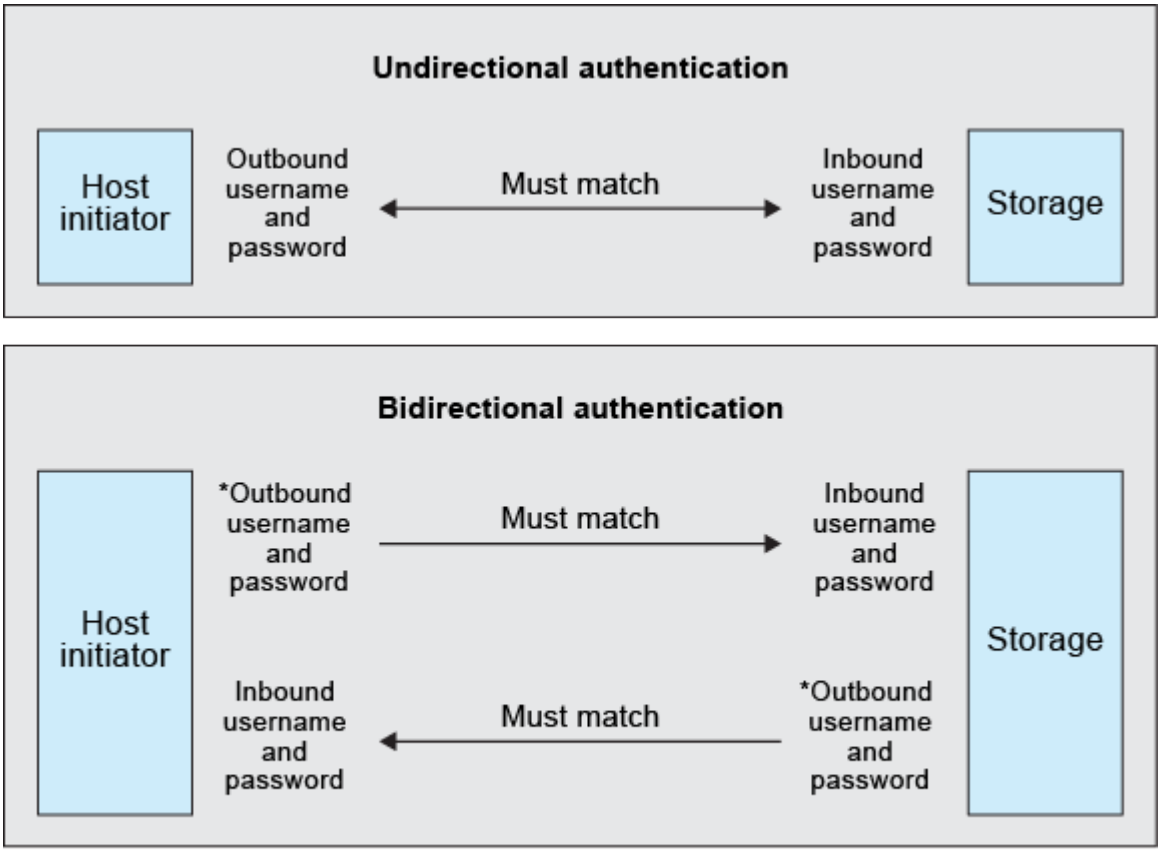
vserver iscsi security remove-initiator-address-range 명령으로 IP 주소 범위 또는 여러 IP 주소를 제거합니다.

'cluster1::> vserver iscsi security remove-initiator-address-range'

ONTAP 에서 **iSCSI** 이니시에이터에 대한 **CHAP** 인증에 대해 알아보세요**.**

CHAP(Challenge Handshake Authentication Protocol)는 iSCSI 이니시에이터와 타겟 간의 인증된 통신을 활성화합니다. CHAP 인증을 사용하는 경우 이니시에이터와 스토리지 시스템 모두에서 CHAP 사용자 이름 및 암호를 정의합니다.

iSCSI 세션의 초기 단계 중에 이니시에이터는 스토리지 시스템에 로그인 요청을 보내 세션을 시작합니다. 로그인 요청에는 이니시에이터의 CHAP 사용자 이름 및 CHAP 알고리즘이 포함됩니다. 스토리지 시스템이 CHAP 챌린지에 응답합니다. 이니시에이터는 CHAP 응답을 제공합니다. 스토리지 시스템에서 응답을 확인하고 이니시에이터를 인증합니다. CHAP 암호는 응답을 계산하는 데 사용됩니다.



인증	아웃바운드	인바운드	성냥?
단방향	호스트 개시자 사용자 이름 및 비밀번호	저장소 사용자 이름 및 비밀번호	반드시 일치해야 함
양방향	호스트 개시자 사용자 이름 및 비밀번호	저장소 사용자 이름 및 비밀번호	반드시 일치해야 함
양방향	저장소 사용자 이름 및 비밀번호	호스트 개시자 사용자 이름 및 비밀번호	반드시 일치해야 함

호스트 이니시에이터의 아웃바운드 사용자 이름과 비밀번호는 스토리지 시스템의 아웃바운드 사용자 이름과 비밀번호와 달라야 합니다.

CHAP 인증 사용에 대한 지침입니다

CHAP 인증을 사용할 때 다음 지침을 따르세요.

- 스토리지 시스템에서 인바운드 사용자 이름과 암호를 정의하는 경우 이니시에이터에서 아웃바운드 CHAP 설정에 동일한 사용자 이름과 암호를 사용해야 합니다. 양방향 인증을 사용하도록 스토리지 시스템에 아웃바운드 사용자 이름과 암호도 정의한 경우, 이니시에이터에서 인바운드 CHAP 설정에 동일한 사용자 이름과 암호를 사용해야 합니다.
- 스토리지 시스템의 인바운드 및 아웃바운드 설정에 동일한 사용자 이름과 암호를 사용할 수 없습니다.
- CHAP 사용자 이름은 1 ~ 128바이트일 수 있습니다.

  시스템에서는 null 사용자 이름을 허용하지 않습니다.

- CHAP 암호(암호)는 1 ~ 512바이트입니다.

  비밀번호는 16진수 값이나 문자열이 될 수 있습니다. 16진수 값의 경우 “0x” 또는 “0X” 접두사를 붙여 값을 입력해야 합니다.

  이 시스템은 널 비밀번호를 허용하지 않습니다.

> ONTAP에서는 CHAP 암호(암호)에 영어가 아닌 특수 문자, 숫자 및 공백을 사용할 수 있습니다. 그러나 호스트 제한에 따라 다릅니다. 이러한 호스트 중 특정 호스트에서 허용되지 않는 호스트는 사용할 수 없습니다.
>
> 예를 들어, Microsoft iSCSI 소프트웨어 초기자는 IPsec 암호화가 사용되지 않는 경우 초기자 및 대상 CHAP 암호를 모두 12바이트 이상 필요로 합니다. 최대 암호 길이는 IPsec의 사용 여부에 관계없이 16바이트입니다.
>
> 추가적인 제한 사항에 대해서는 개시자의 문서를 참조하세요.

iSCSI 인터페이스 액세스 목록을 사용하여 이니시에이터 인터페이스를 제한하는 방법은 성능과 보안을 향상시킬 수 있습니다

iSCSI 인터페이스 액세스 목록을 사용하면 이니시에이터가 액세스할 수 있는 SVM의 LIF 수를 제한하여 성능과 보안을 강화할 수 있습니다.

초기자가 iSCSI 'endTargets' 명령을 사용하여 검색 세션을 시작하면 액세스 목록에 있는 LIF(네트워크 인터페이스)와 연결된 IP 주소를 수신합니다. 기본적으로 모든 이니시에이터는 SVM의 모든 iSCSI LIF에 액세스할 수 있습니다. 액세스 목록을 사용하여 이니시에이터가 액세스할 수 있는 SVM의 LIF 수를 제한할 수 있습니다.

ONTAP의 **iSNS(**인터넷 저장소 이름 서비스)입니다

iSNS(Internet Storage Name Service)는 TCP/IP 스토리지 네트워크에서 iSCSI 디바이스를 자동으로 검색하고 관리할 수 있도록 하는 프로토콜입니다. iSNS 서버는 IP 주소, iSCSI 노드 이름 IQN 및 포털 그룹을 포함하여 네트워크의 활성 iSCSI 장치에 대한 정보를 유지합니다.

타사 공급업체에서 iSNS 서버를 가져올 수 있습니다. 네트워크에 iSNS 서버가 구성되어 이니시에이터 및 타겟에 사용하도록 설정되어 있는 경우 SVM(스토리지 가상 머신)에 관리 LIF를 사용하여 iSNS 서버에 해당 SVM에 대한 모든 iSCSI LIF를 등록할 수 있습니다. 등록이 완료되면 iSCSI 이니시에이터가 iSNS 서버를 쿼리하여 해당 SVM에 대한 모든 LIF를 검색할 수 있습니다.

iSNS 서비스를 사용하려는 경우 iSNS(Internet Storage Name Service) 서버에 스토리지 가상 시스템(SVM)이 올바르게 등록되어 있는지 확인해야 합니다.

네트워크에 iSNS 서버가 없는 경우 호스트에 표시되도록 각 타겟을 수동으로 구성해야 합니다.

iSNS 서버의 기능

iSNS 서버는 iSNS(Internet Storage Name Service) 프로토콜을 사용하여 IP 주소, iSCSI 노드 이름(IQN) 및 포털 그룹을 포함하여 네트워크의 활성 iSCSI 장치에 대한 정보를 유지합니다.

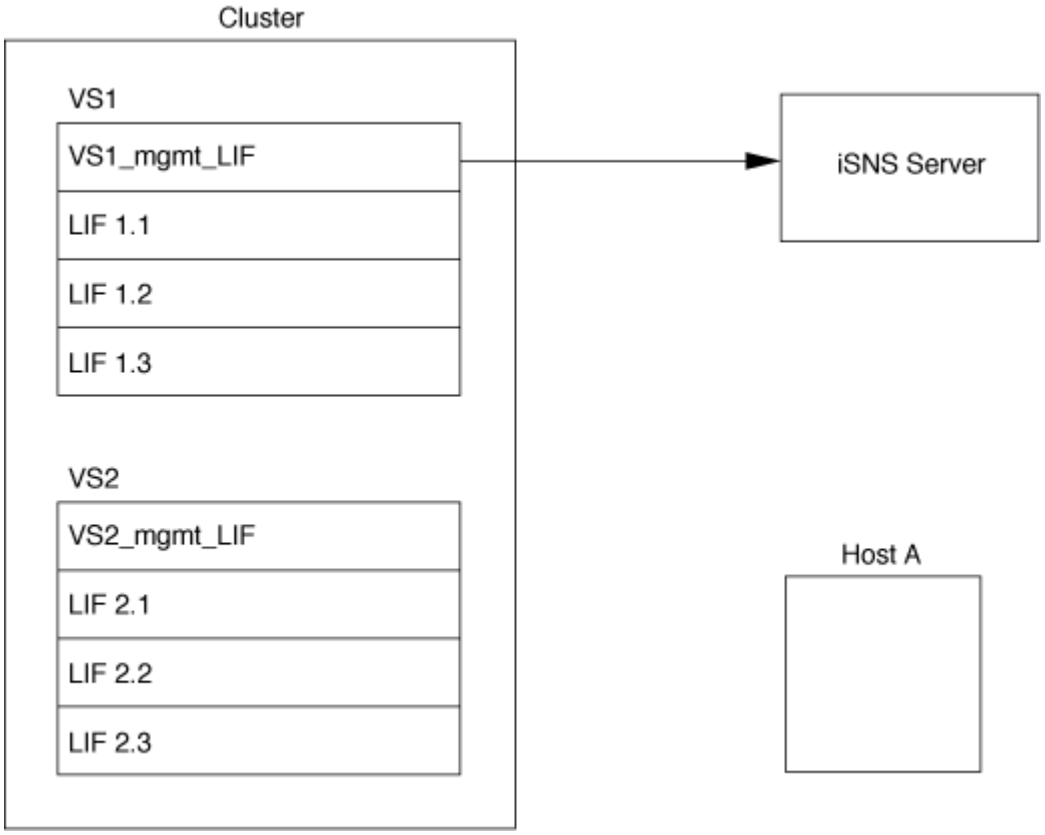
iSNS 프로토콜을 사용하면 IP 스토리지 네트워크에서 iSCSI 디바이스를 자동으로 검색하고 관리할 수 있습니다. iSCSI 이니시에이터는 iSNS 서버를 쿼리하여 iSCSI 타겟 디바이스를 검색할 수 있습니다.

NetApp은 iSNS 서버를 제공하거나 재판매하지 않습니다. NetApp에서 지원하는 공급업체로부터 이러한 서버를 받을 수 있습니다.

SVM이 iSNS 서버와 상호 작용하는 방식

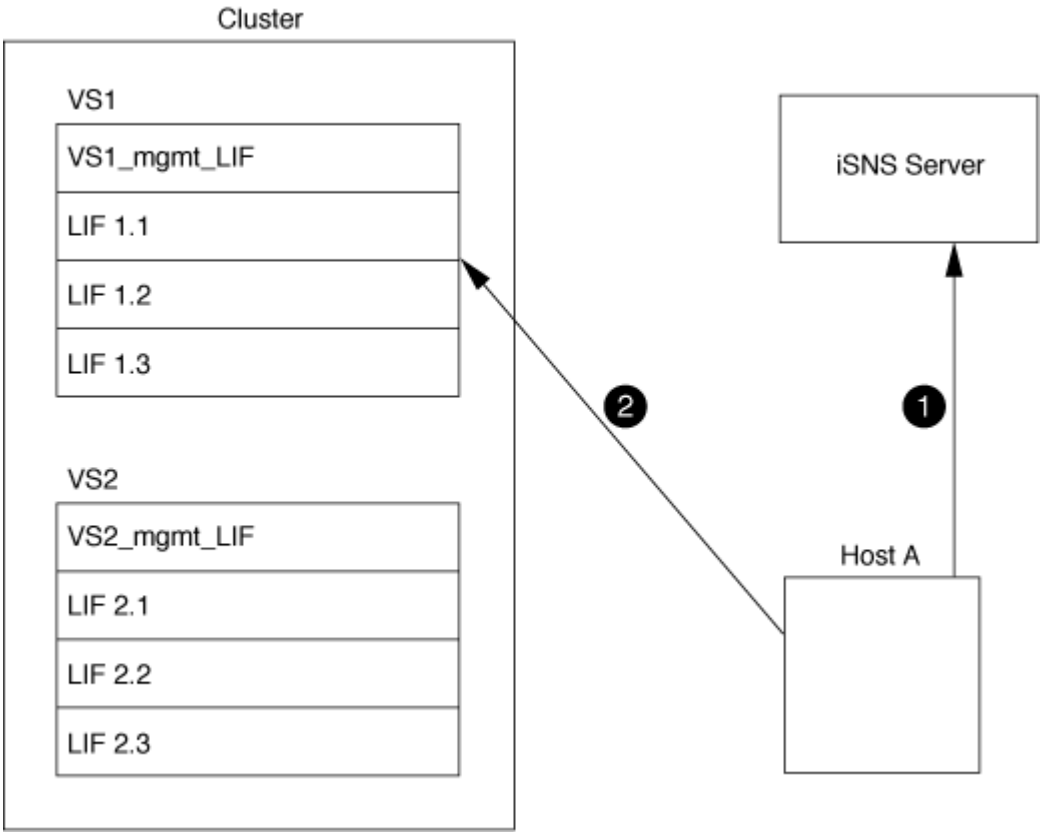
iSNS 서버는 SVM 관리 LIF를 통해 각 SVM(스토리지 가상 시스템)과 통신합니다. 관리 LIF는 특정 SVM을 위한 iSNS 서비스를 사용하여 모든 iSCSI 대상 노드 이름, 별칭 및 포털 정보를 등록합니다.

다음 예에서는 SVM ""VS1""이 SVM 관리 LIF ""VS1_mgmt_lif""를 사용하여 iSNS 서버에 등록합니다. iSNS 등록 중에 SVM은 SVM 관리 LIF를 통해 모든 iSCSI LIF를 iSNS 서버에 보냅니다. iSNS 등록이 완료되면 iSNS 서버에 ""VS1""에서 iSCSI를 지원하는 모든 LIF 목록이 있습니다. 클러스터에 SVM이 여러 개 포함된 경우 각 SVM은 iSNS 서버에 개별적으로 등록하여 iSNS 서비스를 사용해야 합니다.



다음 예에서는 iSNS 서버가 타겟과의 등록을 완료한 후 호스트 A가 1단계에서 설명한 대로 iSNS 서버를 통해 ""VS1""에 대한 모든 LIF를 검색할 수 있습니다. 호스트 A가 ""VS1""에 대한 LIF 검색을 완료한 후 호스트 A는 2단계에 표시된 ""VS1""에 있는 LIF와 연결을 설정할 수 있습니다. 호스트 A는 관리 LIF가 ""VS2"에 ""VS2""에 ""VS2""에

등록될 때까지 ""VS2""에 있는 LIF를 인식하지 못합니다.



그러나 인터페이스 액세스 목록을 정의하는 경우 호스트는 인터페이스 액세스 목록에 정의된 LIF만 사용하여 타겟에 액세스할 수 있습니다.

iSNS를 처음 구성한 후 SVM 구성 설정이 변경되면 ONTAP에서 iSNS 서버를 자동으로 업데이트합니다.

구성을 변경하는 시간과 ONTAP가 iSNS 서버에 업데이트를 보내는 시간 사이에 몇 분 정도 지연될 수 있습니다. iSNS 서버에서 iSNS 정보를 즉시 업데이트합니다 `vserver iscsi isns update`. 에 대한 자세한 내용은 `vserver iscsi isns update` "ONTAP 명령 참조입니다"을 참조하십시오.

iSNS 관리 명령입니다

ONTAP는 iSNS 서비스를 관리하는 명령을 제공합니다.

원하는 작업	이 명령 사용…
iSNS 서비스를 구성합니다	'SVM iSCSI iSNS create'
iSNS 서비스를 시작합니다	가상 iSCSI iSNS 시작
iSNS 서비스를 수정합니다	'SVM iSCSI iSNS modify(iSCSI iSNS 수정)'
iSNS 서비스 구성을 표시합니다	SVM iSCSI iSNS show

등록된 iSNS 정보를 강제로 업데이트합니다	가상 iSCSI iSNS 업데이트
iSNS 서비스를 중지합니다	가상 iSCSI iSNS 중지
iSNS 서비스를 제거합니다	가상 iSCSI iSNS 삭제
명령에 대한 man 페이지를 봅니다	man_command name _

에 대한 자세한 내용은 `vserver iscsi isns` "ONTAP 명령 참조입니다"을 참조하십시오.

FC를 통한 SAN 프로비저닝

ONTAP에서 FC SAN을 구축하는 방법을 이해하는 데 필요한 중요한 개념을 알아야 합니다.

FC 타겟 노드가 네트워크에 연결되는 방법

스토리지 시스템과 호스트에는 케이블이 있는 FC 스위치에 연결할 수 있는 어댑터가 있습니다.

노드가 FC SAN에 연결되면 각 SVM은 스위치 패브릭 이름 서비스에 LIF의 WWPN(World Wide Port Name)을 등록합니다. SVM의 WWNN과 각 LIF의 WWPN은 ONTAP에서 자동으로 할당됩니다.

FC를 사용하는 호스트의 노드에 대한 직접 연결은 지원되지 않습니다. NPIV가 필요하며 이 경우 스위치를 사용해야 합니다. iSCSI 세션을 사용하면 네트워크 라우팅 또는 직접 연결 중 하나의 연결에서 통신할 수 있습니다. 그러나 이러한 두 가지 방법은 모두 ONTAP에서 지원됩니다.

FC 노드의 식별 방법

FC로 구성된 각 SVM은 WWNN(Worldwide Node Name)으로 식별됩니다.

WWPN 사용 방법

WWPN은 FC를 지원하도록 구성된 SVM에서 각 LIF를 식별합니다. 이러한 LIF는 클러스터 내 각 노드에서 물리적 FC 포트를 사용합니다. 이 포트는 노드에서 FC 또는 FCoE로 구성된 FC 타겟 카드, UTA 또는 UTA2 포트일 수 있습니다.

- 이니시에이터 그룹 생성

  호스트 HBA의 WWPN은 이니시에이터 그룹(igroup)을 생성하는 데 사용됩니다. igroup은 특정 LUN에 대한 호스트 액세스를 제어하는 데 사용됩니다. FC 네트워크에서 이니시에이터의 WWPN 컬렉션을 지정하여 igroup을 생성할 수 있습니다. 스토리지 시스템의 LUN을 igroup에 매핑할 때 해당 그룹의 모든 이니시에이터가 해당 LUN에 액세스할 수 있도록 허용할 수 있습니다. 호스트의 WWPN이 LUN에 매핑된 igroup에 없는 경우 해당 호스트는 LUN에 액세스할 수 없습니다. 즉, LUN이 해당 호스트의 디스크로 표시되지 않습니다.

  또한 포트 세트를 생성하여 특정 타겟 포트에만 LUN을 표시할 수 있습니다. 포트 세트는 FC 타겟 포트 그룹으로 구성됩니다. igroup을 포트 세트에 바인딩할 수 있습니다. igroup 내의 모든 호스트는 포트 세트의 타겟 포트에 연결하여 LUN에 액세스할 수 있습니다.

- FC LIF의 고유 식별

  WWPN은 각 FC 논리 인터페이스를 고유하게 식별합니다. 호스트 운영 체제는 WWNN과 WWPN을 함께 사용하여

SVM 및 FC LIF를 식별합니다. 일부 운영 체제에서는 LUN이 호스트에서 동일한 타겟 ID에 표시되도록 영구 바인딩이 필요합니다.

전세계적인 이름 지정 작동 방식

전 세계 이름은 ONTAP에서 순차적으로 생성됩니다. 그러나 ONTAP에서 할당한 방식 때문에 비순차적 순서로 할당된 것처럼 보일 수 있습니다.

각 어댑터에는 사전 구성된 WWPN 및 WWNN이 있지만 ONTAP는 이러한 사전 구성된 값을 사용하지 않습니다. 대신, ONTAP는 온보드 이더넷 포트의 MAC 주소를 기반으로 자체 WWPN 또는 WWNs를 할당합니다.

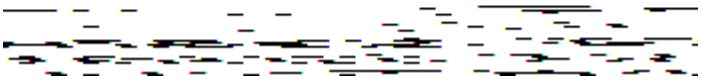
다음과 같은 이유로 전 세계 이름이 지정되면 비순차적인 것으로 보일 수 있습니다.

- 전 세계 이름은 클러스터의 모든 노드 및 SVM(스토리지 가상 머신)에 할당됩니다.
- 전 세계적으로 확보된 이름은 재활용되고 사용 가능한 이름 풀에 다시 추가됩니다.

FC 스위치의 식별 방법

파이버 채널 스위치에는 장치 자체를 위한 WWNN(Worldwide Node Name)과 각 포트에 대한 WWPN(Worldwide Port Name)이 하나씩 있습니다.

예를 들어, 다음 다이어그램에서는 16포트 Brocade 스위치의 각 포트에 WWPN을 할당하는 방법을 보여 줍니다. 특정 스위치에 대한 포트 번호 지정 방법에 대한 자세한 내용은 해당 스위치에 대해 공급업체에서 제공한 설명서를 참조하십시오.



포트 * 0 *, WWPN 20: **00**:00:60:69:51:06:B4

포트 * 1 *, WWPN 20: **01**:00:60:69:51:06:B4

포트 * 14 *, WWPN 20: **0E**:00:60:69:51:06:B4

포트 * 15 *, WWPN 20: **0f**:00:60:69:51:06:B4

NVMe를 이용한 **SAN** 프로비저닝

ONTAP 9.4부터는 SAN 환경에서 NVMe/FC가 지원됩니다. 스토리지 관리자는 NVMe/FC를 사용하여 네임스페이스와 서브시스템을 프로비저닝한 다음 네임스페이스를 하위 시스템에 매핑할 수 있습니다. 이는 LUN이 FC 및 iSCSI의 igroup에 용량 할당 및 매핑된 방식과 비슷합니다.

NVMe 네임스페이스는 논리 블록으로 포맷될 수 있는 비휘발성 메모리의 양입니다. 네임스페이스는 FC 및 iSCSI 프로토콜을 위한 LUN과 동일하며 NVMe 서브시스템은 igroup과 유사합니다. NVMe 하위 시스템을 이니시에이터와 연결할 수 있으므로 연결된 이니시에이터가 하위 시스템 내의 네임스페이스에 액세스할 수 있습니다.

기능에서도 유사하지만, NVMe 네임스페이스는 LUN에서 지원되는 모든 기능을 지원하지 않습니다.

ONTAP 9.5부터 NVMe를 사용한 호스트 데이터 액세스를 지원하려면 라이센스가 필요합니다. ONTAP 9.4에서 NVMe를 사용하는 경우 ONTAP 9.5로 업그레이드한 후 라이센스를 취득하기 위한 90일 유예 기간이 제공됩니다. 이 있는 "ONTAP 1 을 참조하십시오"경우 NVMe 라이센스가 포함됩니다. 다음 명령을 사용하여 라이센스를 설정할 수 있습니다.

'System license add-license-code_NVMe_license_key_'

관련 정보

"NetApp 기술 보고서 4684: NVMe/FC를 사용하여 최신 SAN 구현 및 구성"

SAN 볼륨

SAN 볼륨 개요 정보

ONTAP는 일반 프로비저닝, 씬 프로비저닝 및 반일반 프로비저닝의 세 가지 기본 볼륨 프로비저닝 옵션을 제공합니다. 각 옵션은 볼륨 공간과 ONTAP 블록 공유 기술의 공간 요구 사항을 관리하는 다양한 방법을 사용합니다. 옵션의 작동 방식을 이해하면 환경에 가장 적합한 옵션을 선택할 수 있습니다.

SAN LUN과 NAS 공유를 동일한 FlexVol 볼륨에 배치하는 것은 권장되지 않습니다. SAN LUN을 위해 특별히 별도의 FlexVol 볼륨을 프로비저닝해야 하며 NAS 공유에 별도의 FlexVol 볼륨을 프로비저닝해야 합니다. 이렇게 하면 관리 및 복제 구축이 간소화되고 FlexVol 볼륨이 Active IQ Unified Manager(이전의 OnCommand Unified Manager)에서 지원되는 방식과 유사점이 있습니다.

볼륨에 대한 씬 프로비저닝

씬 프로비저닝된 볼륨이 생성된 경우 ONTAP는 볼륨이 생성될 때 추가 공간을 예약하지 않습니다. 볼륨에 데이터가 기록될 때 볼륨은 쓰기 작업을 수용하기 위해 Aggregate에서 필요한 스토리지를 요청합니다. 씬 프로비저닝된 볼륨을 사용하면 애그리게이트를 오버 커밋할 수 있으므로 애그리게이트에 여유 공간이 부족할 때 볼륨이 필요한 공간을 확보할 수 없게 됩니다.

'-space-보증' 옵션을 '없음'으로 설정하여 씬 프로비저닝된 FlexVol 볼륨을 만듭니다.

볼륨에 대한 일반 프로비저닝입니다

씩 프로비저닝된 볼륨이 생성되면 ONTAP는 언제든지 볼륨의 블록을 쓸 수 있도록 애그리게이트에 충분한 스토리지를 남겨 둡니다. 일반 프로비저닝을 사용하도록 볼륨을 구성할 경우 압축 및 중복제거와 같은 ONTAP 스토리지 효율성 기능을 사용하여 대규모 초기 스토리지 요구사항을 상쇄할 수 있습니다.

'-space-slo'(서비스 수준 목표) 옵션을 'thick'으로 설정하여 씩 프로비저닝된 FlexVol 볼륨을 만듭니다.

볼륨에 반씩 프로비저닝

반씩 프로비저닝을 사용하는 볼륨이 생성된 경우 ONTAP에서는 애그리게이트에서 볼륨 크기를 고려하여 스토리지 공간을 별도로 설정합니다. 블록 공유 기술에서 블록을 사용하고 있기 때문에 볼륨에 여유 공간이 부족해지면 ONTAP이 보호 데이터 오브젝트(스냅샷 및 FlexClone 파일 및 LUN)를 삭제하여 보유 중인 공간을 확보하도록 시도합니다. ONTAP가 덮어쓰기 작업에 필요한 공간과 보조를 맞출 수 있을 만큼 보호 데이터 객체를 빠르게 삭제할 수 있는 한 쓰기 작업은 계속 성공합니다. 이를 '최선 노력'이라고 합니다.

- 참고: * 다음 기능은 반씩 프로비저닝을 사용하는 볼륨에서 지원되지 않습니다.
- 중복제거, 압축, 컴팩션과 같은 스토리지 효율성 기술
- Microsoft ODX(Offloaded Data Transfer)

semi-thick-provisioned FlexVol 볼륨은 '-space-slo'(서비스 수준 목표) 옵션을 'sEMI-thick'으로 설정하여 생성합니다.

공간 예약 파일 및 **LUN**과 함께 사용

공간 예약 파일 또는 LUN은 생성 시 스토리지가 할당되는 파일입니다. 역사적으로 NetApp은 공간 예약이 사용되지 않는 LUN(비공간 예약 LUN)을 지칭하기 위해 ""씬 프로비저닝된 LUN"이라는 용어를 사용했습니다.

- 참고: * 비공간 예약 파일은 일반적으로 ""씬 프로비저닝 파일""이라고 하지 않습니다.

다음 표에는 세 가지 볼륨 프로비저닝 옵션을 공간 예약 파일 및 LUN과 함께 사용하는 방법의 주요 차이점이 요약되어 있습니다.

볼륨 프로비저닝	**LUN**/파일 공간 예약	덮어쓰기	보호 데이터 [2]	스토리지 효율성 [3]
두껍게	지원	[1]을(를) 보장합니다	NetApp이 보장합니다	지원
얇음	효과 없음	없음	NetApp이 보장합니다	지원
약간 두껍습니다	지원	최선의 노력 [1]	최선을 다하세요	지원되지 않습니다

- 참고 *
  1. 덮어쓰기 보장 또는 최선의 덮어쓰기 보장을 제공하려면 LUN 또는 파일에 공간 예약을 설정해야 합니다.
  2. 보호 데이터에는 스냅샷, 자동 삭제로 표시된 FlexClone 파일 및 LUN(백업 클론)이 포함됩니다.
  3. 스토리지 효율성에는 중복제거, 압축, 자동 삭제로 표시되지 않은 모든 FlexClone 파일 및 LUN(활성 클론), FlexClone 하위 파일(복사본 오프로드로 사용)이 포함됩니다.

SCSI 씬 프로비저닝된 **LUN** 지원

ONTAP는 T10 SCSI 씬 프로비저닝 LUN과 NetApp 씬 프로비저닝 LUN을 지원합니다. T10 SCSI 씬 프로비저닝을 사용하면 호스트 애플리케이션에서 LUN 공간 재확보, 블록 환경의 LUN 공간 모니터링 기능 등 SCSI 기능을 지원할 수 있습니다. T10 SCSI 씬 프로비저닝은 SCSI 호스트 소프트웨어에서 지원해야 합니다.

ONTAP의 pace-allocation 설정을 사용하면 LUN에서 T10 씬 프로비저닝 지원을 활성화/비활성화할 수 있습니다. ONTAP의 pace-allocation enable 설정을 사용하여 LUN에 T10 SCSI 씬 프로비저닝을 활성화합니다.

그만큼 `[-space-allocation {enabled|disabled}]` 에서 명령 "ONTAP 명령 참조입니다" T10 씬 프로비저닝에 대한 지원을 활성화/비활성화하고 LUN에서 T10 SCSI 씬 프로비저닝을 활성화하는 방법에 대한 자세한 정보가 있습니다.

볼륨 프로비저닝 옵션을 구성합니다

씬 프로비저닝, 일반 프로비저닝 또는 반씩 프로비저닝을 위해 볼륨을 구성할 수 있습니다.

이 작업에 대해

'-space-slo' 옵션을 'thick'으로 설정하면 다음과 같은 이점이 있습니다.

- 전체 볼륨이 Aggregate에 사전 할당됩니다. 볼륨의 '-space-보증' 옵션을 구성하려면 'volume create' 또는 'volume modify' 명령을 사용할 수 없습니다.
- 덮어쓰기에 필요한 공간의 100%가 예약됩니다. 볼륨의 '-fractional-reserve' 옵션을 구성하려면 'volume modify' 명령을 사용할 수 없습니다

'-space-slo' 옵션을 'EMI-thick'으로 설정하면 다음과 같은 이점이 있습니다.

- 전체 볼륨이 Aggregate에 사전 할당됩니다. 볼륨의 '-space-보증' 옵션을 구성하려면 'volume create' 또는 'volume modify' 명령을 사용할 수 없습니다.
- 덮어쓰기용으로 예약된 공간이 없습니다. 'volume modify' 명령을 사용하여 볼륨의 '-fractional-reserve' 옵션을 구성할 수 있습니다.
- 스냅샷 자동 삭제가 설정되었습니다.

단계

1. 볼륨 프로비저닝 옵션 구성:

   'volume create-vserver_vserver_name_-volume_volume_name_-aggregate_aggregate_name_-space-slo none|thick|semi-thick-space-보증 없음|볼륨'

   '-space-보증' 옵션은 AFF 시스템과 비 AFF DP 볼륨에 대해 기본적으로 '없음'으로 설정됩니다. 그렇지 않으면 볼륨(volume)으로 기본 설정됩니다. 기존 FlexVol 볼륨의 경우 'volume modify' 명령을 사용하여 프로비저닝 옵션을 구성합니다.

   다음 명령은 씬 프로비저닝을 위해 SVM VS1 에서 vol1을 구성합니다.

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-guarantee
   none
   ```

   다음 명령을 실행하면 일반 프로비저닝을 위해 SVM VS1 vol1에 대해 vol1이 구성됩니다.

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo thick
   ```

   다음 명령을 실행하면 반씩 프로비저닝을 위해 SVM VS1 vol1에 대해 vol1이 구성됩니다.

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo semi-
   thick
   ```

SAN 볼륨 구성 옵션

LUN을 포함하는 볼륨에서 다양한 옵션을 설정해야 합니다. 볼륨 옵션을 설정하는 방법에 따라 볼륨의 LUN에서 사용할 수 있는 공간이 결정됩니다.

자동 확장

자동 행을 활성화 또는 비활성화할 수 있습니다. 이 기능을 사용하도록 설정하면 ONTAP에서 볼륨 크기를 미리 결정한 최대 크기까지 자동으로 늘릴 수 있습니다. 볼륨의 자동 증가를 지원하려면 포함된 애그리게이트에 사용 가능한 공간이 있어야 합니다. 따라서 자동 확장 기능을 사용하도록 설정한 경우 포함된 애그리게이트의 여유 공간을 모니터링하고 필요 시 더 많은 공간을 추가해야 합니다.

스냅샷 생성을 지원하기 위해 자동 확장을 트리거할 수 없습니다. 스냅샷을 생성하려고 하는데 볼륨에 공간이 부족하면 자동 증가가 설정된 경우에도 스냅샷 생성이 실패합니다.

자동 확장 기능을 비활성화하면 볼륨 크기는 동일하게 유지됩니다.

자동 축소

자동 축소를 사용하거나 사용하지 않도록 설정할 수 있습니다. 자동 축소를 사용하도록 설정하면 ONTAP에서 볼륨에서 사용된 공간 양이 미리 정해진 임계값을 줄일 때 볼륨의 전체 크기를 자동으로 줄일 수 있습니다. 따라서 볼륨을 트리거하여 사용되지 않는 여유 공간을 자동으로 릴리즈하여 스토리지 효율성이 향상됩니다.

스냅샷 자동 삭제

스냅샷 자동 삭제는 다음 중 하나가 발생하면 스냅샷을 자동으로 삭제합니다.

- 볼륨이 거의 꽉 찼습니다.
- 스냅샷 예약 공간이 거의 가득 찼습니다.
- 덮어쓰기 예약 공간이 가득 찼습니다.

스냅샷을 오래된 스냅샷에서 최신 스냅샷으로 또는 최신 스냅샷에서 오래된 스냅샷으로 삭제하도록 스냅샷 자동 삭제를 구성할 수 있습니다. 스냅샷 자동 삭제는 클론 복제된 볼륨 또는 LUN의 스냅샷에 연결된 스냅샷은 삭제하지 않습니다.

볼륨에 추가 공간이 필요하고 자동 확장 및 스냅샷 자동 삭제를 모두 사용하도록 설정한 경우, 기본적으로 ONTAP은 먼저 자동 확장을 트리거하여 필요한 공간을 확보하려고 시도합니다. 자동 확장을 통해 충분한 공간을 확보하지 못하면 스냅샷 자동 삭제가 트리거됩니다.

스냅숏 예비 공간입니다

스냅숏 예비 공간은 스냅숏용으로 예약된 볼륨의 공간 크기를 정의합니다. 스냅숏 예비 공간에 할당된 공간은 다른 용도로 사용할 수 없습니다. 스냅숏 예비 공간에 할당된 모든 공간이 사용되는 경우 스냅숏에서 볼륨의 추가 공간을 사용하기 시작합니다.

SAN 환경에서 볼륨을 이동하기 위한 요구사항

LUN 또는 네임스페이스가 포함된 볼륨을 이동하기 전에 특정 요구 사항을 충족해야 합니다.

- 하나 이상의 LUN이 포함된 볼륨의 경우 클러스터의 각 노드에 연결되는 LUN(LIF)당 경로가 2개 이상 있어야 합니다.

  따라서 단일 장애 지점이 발생하지 않으며 시스템에서 구성 요소 장애를 극복할 수 있습니다.

- 네임스페이스가 포함된 볼륨의 경우 클러스터는 ONTAP 9.6 이상을 실행해야 합니다.

  ONTAP 9.5를 실행하는 NVMe 구성에는 볼륨 이동이 지원되지 않습니다.

lun 덮어쓰기 예약 _ 이라고도 하는 분할 예약을 통해 FlexVol 볼륨의 공간 예약 LUN 및 파일에 대한 덮어쓰기 예약 기능을 해제할 수 있습니다. 이렇게 하면 스토리지 활용률을 최대화하는 데 도움이 될 수 있지만 공간 부족으로 인한 쓰기 작업 실패로 인해 환경이 부정적인 영향을 받는 경우 이러한 구성에서 부과하는 요구사항을 이해해야 합니다.

분획 예약 설정은 백분율로 표현되며 유효한 값은 0, 100%입니다. 분할 예약 설정은 볼륨의 속성입니다.

부분 예약 공간을 '0'으로 설정하면 스토리지 활용률이 증가합니다. 그러나 볼륨 보장이 "볼륨"으로 설정되어 있어도 볼륨에 있는 데이터에 액세스하는 응용 프로그램은 사용 가능한 공간이 부족할 경우 데이터 중단을 경험할 수 있습니다. 그러나 적절한 볼륨 구성 및 사용을 통해 쓰기 실패 가능성을 최소화할 수 있습니다. ONTAP는 다음 요구 사항 중 _ALL_이 충족되면 부분 예약 공간이 '0'으로 설정된 볼륨에 대해 "'최선 노력'" 쓰기 보장을 제공합니다.

- 중복 제거가 사용되지 않습니다
- 압축이 사용되지 않습니다
- FlexClone 하위 파일을 사용하지 않습니다
- 모든 FlexClone 파일과 FlexClone LUN이 자동으로 삭제됩니다

  이 설정은 기본 설정이 아닙니다. 생성 시 또는 FlexClone 파일 또는 FlexClone LUN을 생성한 후에 이를 수정하여 자동 삭제를 명시적으로 설정해야 합니다.

- ODX 및 FlexClone 복사 오프로드가 사용되지 않습니다
- 볼륨 보장이 '볼륨'으로 설정되어 있습니다
- 파일 또는 LUN 공간 예약이 '사용'되었습니다
- 볼륨 스냅숏 예비 공간이 '0'으로 설정되어 있습니다
- 볼륨 스냅샷 자동 삭제는 의 약정 수준 `destroy`, 제거 목록 `lun_clone,vol_clone,cifs_share,file_clone,sfsr` 및 트리거로 `volume` 이루어집니다 `enabled`

  이 설정은 필요한 경우 FlexClone 파일 및 FlexClone LUN도 삭제되도록 합니다.

변경률이 높은 경우 드물지만 스냅샷 자동 삭제가 지연되어 위에서 요구하는 모든 구성 설정을 사용 중이더라도 볼륨의 공간이 부족해질 수 있습니다.

또한 필요에 따라 볼륨 자동 확장 기능을 사용하여 볼륨 스냅샷이 자동으로 삭제될 가능성을 줄일 수 있습니다. 자동 확장 기능을 사용하도록 설정한 경우 연결된 애그리게이트의 여유 공간을 모니터링해야 합니다. Aggregate가 가득 차서 볼륨 증가를 막을 수 없을 경우, 볼륨의 여유 공간이 고갈되면 더 많은 스냅샷이 삭제될 수 있습니다.

위 구성 요구사항을 모두 충족하지 못할 경우 볼륨에서 공간이 부족하지 않도록 해야 하는 경우 볼륨의 분할 예약 설정을 '100'으로 설정해야 합니다. 이를 위해서는 공간을 미리 확보해야 하지만, 위에 나열된 기술이 사용 중일 때도 데이터 수정 작업이 성공하도록 보장합니다.

분할 예약 설정의 기본값 및 허용되는 값은 볼륨의 보장에 따라 다릅니다.

볼륨 보장	기본 분할 예약	허용되는 값
볼륨	100	0, 100

볼륨 보장	기본 분할 예약	허용되는 값
없음	0	0, 100

SAN 호스트측 공간 관리

씬 프로비저닝된 환경에서 호스트 측 공간 관리는 호스트 파일 시스템에서 확보된 스토리지 시스템의 공간 관리 프로세스를 완료합니다.

호스트 파일 시스템에는 새 데이터를 저장하는 데 사용할 수 있는 블록과 덮어쓰지 않아야 하는 유효한 데이터가 들어 있는 블록을 추적하는 메타데이터가 포함되어 있습니다. 이 메타데이터는 LUN 또는 네임스페이스 내에 저장됩니다. 호스트 파일 시스템에서 파일이 삭제되면 파일 시스템 메타데이터가 업데이트되어 해당 파일의 블록을 여유 공간으로 표시합니다. 그런 다음 새로 확보된 블록을 포함하도록 총 파일 시스템 여유 공간이 다시 계산됩니다. 스토리지 시스템에서 이러한 메타데이터 업데이트는 호스트에서 수행하는 다른 쓰기와 다르지 않습니다. 따라서 스토리지 시스템에서 삭제된 내용이 있는지 인식하지 못합니다.

이렇게 하면 호스트에서 보고된 사용 가능한 공간의 양과 기본 스토리지 시스템에서 보고하는 사용 가능한 공간의 양이 서로 일치하지 않습니다. 예를 들어, 스토리지 시스템에서 호스트에 할당된 새로 프로비저닝된 200GB LUN이 있다고 가정합니다. 호스트와 스토리지 시스템 모두 200GB의 사용 가능한 공간을 보고합니다. 그런 다음 호스트는 100GB 데이터를 씁니다. 이때 호스트 및 스토리지 시스템 모두 100GB 사용 공간과 100GB 사용 안 된 공간을 보고합니다.

그런 다음 호스트에서 50GB의 데이터를 삭제합니다. 이때 호스트는 50GB의 사용된 공간과 150GB의 사용되지 않은 공간을 보고합니다. 그러나 스토리지 시스템은 100GB 사용 공간과 100GB의 미사용 공간을 보고합니다.

호스트 측 공간 관리는 다양한 방법을 사용하여 호스트와 스토리지 시스템 간의 공간 차이를 조정합니다.

SnapCenter를 통한 호스트 관리 단순화

SnapCenter 소프트웨어를 사용하면 iSCSI 및 FC 스토리지와 관련된 일부 관리 및 데이터 보호 작업을 단순화할 수 있습니다. SnapCenter는 Windows 및 UNIX 호스트용 선택적 관리 패키지입니다.

SnapCenter 소프트웨어를 사용하면 여러 스토리지 시스템에 분산될 수 있는 스토리지 풀에서 가상 디스크를 손쉽게 생성하고 스토리지 프로비저닝 작업을 자동화하고 호스트 데이터와 일치하는 스냅샷에서 스냅샷 및 클론을 생성하는 프로세스를 단순화할 수 있습니다.

에 대한 자세한 내용은 NetApp 제품 설명서를 참조하십시오 "SnapCenter".

관련 링크

"SAN 프로토콜에 ONTAP 공간 할당을 사용합니다"

Igroup 정보

이니시에이터 그룹(igroup)은 FC 프로토콜 호스트 WWPN 또는 iSCSI 호스트 노드 이름의 테이블입니다. igroup을 정의하고 LUN에 매핑하여 LUN에 액세스할 수 있는 이니시에이터를 제어할 수 있습니다.

일반적으로 호스트의 모든 이니시에이터 포트 또는 소프트웨어 이니시에이터가 LUN에 액세스할 수 있도록 합니다. 다중 경로 소프트웨어를 사용하거나 클러스터 호스트를 사용하는 경우, 각 클러스터 호스트의 각 이니시에이터 포트 또는 소프트웨어 이니시에이터는 동일한 LUN에 대한 이중 경로를 필요로 합니다.

LUN을 생성하기 전이나 후에 LUN에 액세스할 수 있는 이니시에이터를 지정하는 igroup을 생성할 수 있지만 LUN을 igroup에 매핑하기 전에 igroup을 생성해야 합니다.

이니시에이터 그룹에 여러 이니시에이터가 있을 수 있으며, 여러 igroup이 동일한 이니시에이터를 포함할 수 있습니다. 그러나 동일한 이니시에이터가 있는 여러 igroup에 LUN을 매핑할 수 없습니다. 이니시에이터는 서로 다른 상치성 igroup의 구성원일 수 없습니다.

igroup에서 **LUN** 액세스를 제공하는 방법의 예

여러 igroup을 생성하여 호스트에 사용할 수 있는 LUN을 정의할 수 있습니다. 예를 들어, 호스트 클러스터가 있는 경우 igroup을 사용하여 특정 LUN이 클러스터의 한 호스트에만 또는 클러스터의 모든 호스트에 표시되는지 확인할 수 있습니다.

다음 표에서는 4개의 igroup이 스토리지 시스템에 액세스하는 4개의 서로 다른 호스트에 대한 LUN에 액세스하는 방법을 보여 줍니다. 클러스터 호스트(Host3 및 Host4)는 모두 동일한 igroup(Group3)의 구성원이며 이 igroup에 매핑된 LUN에 액세스할 수 있습니다. group4라는 igroup에는 파트너가 볼 수 없는 로컬 정보를 저장하기 위한 Host4의 WWPN이 포함되어 있습니다.

HBA WWPN, IQN 또는 **EUI**가 포함된 호스트	**Igroup**	**WWPN, IQN, EUI**가 **igroup**에 추가되었습니다	**LUN**이 **igroup**에 매핑되어 있습니다
호스트1, 단일 경로(iSCSI 소프트웨어 이니시에이터) iqn.1991-05.com.microsoft:host1	그룹1	iqn.1991-05.com.microsoft:host1	'/vol/vol2/lun1'
Host2, 다중 경로(HBA 2개) 10:00:00:00:C9:2b:6b:3c 10:00:00:00:C9:2b:02:3c	그룹2	10:00:00:00:C9:2b:6b:3c 10:00:00:00:C9:2b:02:3c	'/vol/vol2/lun2'
호스트 3, 다중 경로, 호스트 4로 클러스터링되었습니다 10:00:00:00:C9:2b:32:1b 10:00:00:00:C9:2b:41:02	그룹3	10:00:00:00:C9:2b:32:1b 10:00:00:00:C9:2b:41:02 10:00:00:00:C9:2b:51:2c 10:00:00:00:C9:2b:47:A2	'/vol/vol2/qtree1/lun3'
Host4, multipath, 클러스터링됨(Host3에는 표시되지 않음) 10:00:00:00:C9:2b:51:2c 10:00:00:00:C9:2b:47:A2	그룹4	10:00:00:00:C9:2b:51:2c 10:00:00:00:C9:2b:47:A2	'/vol/vol2/qtree2/lun4"/vol/vol2/qtree1/lun5'

igroup에 대해 이니시에이터 WWPN 및 iSCSI 노드 이름을 지정합니다

igroup을 생성할 때 이니시에이터의 iSCSI 노드 이름 및 WWPN을 지정하거나 나중에 추가할 수 있습니다. LUN을 생성할 때 이니시에이터 iSCSI 노드 이름과 WWPN을 지정하도록 선택한 경우 나중에 필요에 따라 제거할 수 있습니다.

Host Utilities 설명서의 지침에 따라 WWPN을 얻고 특정 호스트와 연결된 iSCSI 노드 이름을 찾습니다. ESX 소프트웨어를 실행하는 호스트의 경우 Virtual Storage Console을 사용합니다.

가상화된 SAN 환경을 사용할 때의 이점

SVM(Storage Virtual Machine)과 LIF를 사용하여 가상화 환경을 구축하면 클러스터의 모든 노드로 SAN 환경을 확장할 수 있습니다.

- 분산 관리

  SVM의 모든 노드에 로그인하여 클러스터의 모든 노드를 관리할 수 있습니다.

- 데이터 액세스 증가

  MPIO 및 ALUA를 사용하면 SVM을 위한 모든 활성 iSCSI 또는 FC LIF를 통해 데이터에 액세스할 수 있습니다.

- LUN 액세스를 제어합니다

  SLM 및 포트 세트를 사용하는 경우 이니시에이터가 LUN에 액세스하는 데 사용할 수 있는 LIF를 제한할 수 있습니다.

ESX 호스트의 VMware VAAI 성능을 향상시킵니다

ONTAP는 ESX 호스트가 ESX 4.1 이상을 실행하는 경우 특정 VMware VAAI(vStorage APIs for Array Integration) 기능을 지원합니다. 이러한 기능은 ESX 호스트에서 스토리지 시스템으로 작업을 오프로드하고 네트워크 처리량을 늘리는 데 도움이 됩니다. ESX 호스트는 올바른 환경에서 자동으로 기능을 활성화합니다.

VAAI 기능은 다음 SCSI 명령을 지원합니다.

- "extended_copy"

  이 기능을 사용하면 호스트가 데이터 전송에 참여하지 않고도 LUN 간 또는 LUN 내에서 데이터 전송을 시작할 수 있습니다. 따라서 ESX CPU 주기가 단축되고 네트워크 처리량이 증가합니다. "복사 오프로드"라고도 하는 확장된 복사 기능은 가상 머신의 클론 생성과 같은 시나리오에서 사용됩니다. ESX 호스트에서 호출하면 복제 오프로드 기능은 호스트 네트워크를 통해 이동하는 대신 스토리지 시스템 내의 데이터를 복제합니다. Copy Offload는 다음과 같은 방법으로 데이터를 전송합니다.

  - 하나의 LUN 내에서
  - 볼륨 내의 LUN 간
  - 스토리지 가상 시스템(SVM) 내의 서로 다른 볼륨에 있는 LUN 간
  - 클러스터 내의 서로 다른 SVM에 있는 LUN 간에 이 기능을 호출할 수 없는 경우 ESX 호스트는 복사 작업에

표준 읽기 및 쓰기 명령을 자동으로 사용합니다.

- 같은 글씨를 쓰십시오

  이 기능은 0과 같은 반복된 패턴을 스토리지 배열에 쓰는 작업을 오프로드합니다. ESX 호스트는 파일 채우기 0과 같은 작업에서 이 기능을 사용합니다.

- 비교 및 쓰기

  이 기능은 특정 파일 액세스 동시 접속 제한을 우회하여 가상 머신 부팅 등의 작업을 가속화합니다.

VAAI 환경 사용에 대한 요구 사항

VAAI 기능은 ESX 운영 체제의 일부이며 올바른 환경을 설정한 경우 ESX 호스트에서 자동으로 호출됩니다.

환경 요구 사항은 다음과 같습니다.

- ESX 호스트는 ESX 4.1 이상을 실행해야 합니다.
- VMware 데이터 저장소를 호스팅하는 NetApp 스토리지 시스템은 ONTAP를 실행 중이어야 합니다.
- (복제 오프로딩만 해당) VMware 복제 작업의 소스 및 대상은 동일한 클러스터 내의 동일한 스토리지 시스템에서 호스팅되어야 합니다.

> 현재 복제 오프로드 기능은 다른 스토리지 시스템에서 호스팅되는 VMware 데이터 저장소 간에 데이터 복제를 지원하지 않습니다.

VAAI 기능이 **ESX**에서 지원되는지 확인합니다

ESX 운영 체제에서 VAAI 기능을 지원하는지 확인하려면 vSphere Client를 확인하거나 호스트에 액세스하는 다른 방법을 사용할 수 있습니다. ONTAP는 기본적으로 SCSI 명령을 지원합니다.

ESX 호스트 고급 설정을 확인하여 VAAI 기능이 설정되었는지 여부를 확인할 수 있습니다. 표에는 ESX 제어 이름에 해당하는 SCSI 명령이 나와 있습니다.

scsi 명령	**ESX** 제어 이름**(VAAI** 기능**)**
Extended_copy(확장 복사)	하드하드웨어가속한이동
같은 쓰기	하드wareAcceleratedInit
Compare_and_write(비교 및 쓰기)	하드wareAcceleratedLocking

SAN 복사 오프로드

Microsoft ODX(Offloaded Data Transfer)

Microsoft ODX(Offloaded Data Transfer)는 _copy offload_라고도 하며 호스트 컴퓨터를 통해 데이터를 전송하지 않고 스토리지 장치 내에서 또는 호환되는 스토리지 장치 간에 직접 데이터를 전송할 수 있습니다.

VMware와 Microsoft는 복제 오프로드 작업을 지원하여 성능과 네트워크 처리량을 높여줍니다. 개별 복제 오프로드 기능을 사용하려면 VMware 및 Windows 운영 체제 환경의 요구 사항을 충족하도록 시스템을 구성해야 합니다.

가상화된 환경에서 VMware와 Microsoft 복사 오프로드를 사용하는 경우 LUN을 정렬해야 합니다. 정렬되지 않은 LUN은 성능을 저하시킬 수 있습니다. "정렬되지 않은 LUN에 대해 자세히 알아보세요".

ONTAP은 SMB 및 SAN 프로토콜을 모두 지원하는 ODX를 지원합니다.

ODX가 아닌 파일을 전송하면 소스에서 데이터를 읽고 네트워크를 통해 호스트로 전송합니다. 호스트는 네트워크를 통해 데이터를 대상으로 다시 전송합니다. ODX 파일 전송에서는 호스트를 거치지 않고 데이터를 소스에서 대상으로 직접 복사합니다.

ODX는 오프로드된 복사본이 소스와 대상 간에 직접 수행되므로, 동일한 볼륨 내에서 복사본을 수행할 경우 동일한 볼륨 복사본의 복사 시간 단축, 클라이언트의 CPU 및 메모리 사용률 감소, 네트워크 I/O 대역폭 사용률 감소 등 상당한 성능 이점을 실현할 수 있습니다. 여러 볼륨에 걸쳐 있는 복사본에서는 호스트 기반 복사본에 비해 성능이 크게 향상되지 않을 수 있습니다.

SAN 환경의 경우 ODX는 호스트와 스토리지 시스템 모두에서 지원되는 경우에만 사용할 수 있습니다. ODX를 지원하고 ODX를 사용하는 클라이언트 컴퓨터는 파일을 이동하거나 복사할 때 오프로드된 파일 전송을 자동으로 투명하게 사용합니다. ODX는 Windows 탐색기를 통해 파일을 끌어서 놓을지, 명령줄 파일 복사 명령을 사용하는지, 클라이언트 애플리케이션이 파일 복사 요청을 시작하는지 여부와 관계없이 사용됩니다.

ODX 사용을 위한 요구사항

복사 오프로드를 위해 ODX를 사용할 계획이라면 볼륨 지원 고려 사항, 시스템 요구 사항 및 소프트웨어 기능 요구 사항을 잘 알고 있어야 합니다.

ODX를 사용하려면 시스템에 다음이 있어야 합니다.

- ONTAP

  ODX는 지원되는 ONTAP 버전에서 자동으로 활성화됩니다.

- 최소 소스 볼륨 2GB

  최적의 성능을 위해 소스 볼륨은 260GB보다 커야 합니다.

- Windows 클라이언트에서 ODX를 지원합니다

  ODX는 Windows Server 2012 이상 및 Windows 8 이상에서 지원됩니다. 상호 운용성 매트릭스에는 지원되는 Windows 클라이언트에 대한 최신 정보가 포함되어 있습니다.

  "NetApp 상호 운용성 매트릭스 툴"

- ODX에 대한 복사 애플리케이션 지원

  데이터 전송을 수행하는 애플리케이션은 ODX를 지원해야 합니다. ODX를 지원하는 애플리케이션 작업은 다음과 같습니다.

  - 가상 하드 디스크(VHD) 생성 및 변환, 스냅샷 관리, 가상 컴퓨터 간 파일 복사 등의 Hyper-V 관리 작업
  - Windows 탐색기 작업
  - Windows PowerShell 복사 명령

◦ Windows 명령 프롬프트 복사 명령 Microsoft TechNet 라이브러리에는 Windows 서버 및 클라이언트에서 지원되는 ODX 응용 프로그램에 대한 자세한 정보가 나와 있습니다.

- 압축된 볼륨을 사용하는 경우 압축 그룹 크기는 8K여야 합니다.

  32K 압축 그룹 크기가 지원되지 않습니다.

ODX는 다음 볼륨 유형과 함께 작동하지 않습니다.

- 용량이 2GB 미만인 소스 볼륨
- 읽기 전용 볼륨입니다
- "FlexCache 볼륨"

  ⓘ ODX는 FlexCache 원본 볼륨에서 지원됩니다.

- "반씩 프로비저닝된 볼륨"

특수 시스템 파일 요구 사항

qtree에 있는 ODX 파일을 삭제할 수 있습니다. 기술 지원 부서의 지시가 없는 한 다른 ODX 시스템 파일을 제거하거나 수정하지 마십시오.

ODX 기능을 사용하면 시스템의 모든 볼륨에 ODX 시스템 파일이 존재합니다. 이러한 파일을 사용하면 ODX 전송 중에 사용된 데이터를 특정 시점으로 표시할 수 있습니다. 다음 시스템 파일은 데이터가 오프로드된 LUN 또는 파일을 포함하는 각 볼륨의 루트 레벨에 있습니다.

- '.copy-offload'(숨겨진 디렉토리)
- '.tokens'(숨겨진 파일.copy-offload' 디렉토리)

"copy-offload delete-tokens-path dir_path-node_node_name_" 명령을 사용하여 ODX 파일이 포함된 qtree를 삭제할 수 있습니다.

ODX의 사용 사례

ODX가 성능 이점을 제공하는 상황을 파악할 수 있도록 SVM에서 ODX를 사용하는 사용 사례를 알고 있어야 합니다.

ODX를 지원하는 Windows 서버 및 클라이언트는 원격 서버 간에 데이터를 복사하는 기본 방법으로 복사 오프로드를 사용합니다. Windows 서버 또는 클라이언트가 ODX를 지원하지 않거나 ODX 복사 오프로드가 어느 시점에서든 장애가 발생하면 복사 또는 이동 작업이 복사 또는 이동 작업에 대한 기존 읽기/쓰기로 다시 돌아갑니다.

ODX 복사 및 이동 사용을 지원하는 사용 사례는 다음과 같습니다.

- 체내

  소스 및 대상 파일 또는 LUN이 동일한 볼륨 내에 있습니다.

- 볼륨 간, 동일한 노드, 동일한 SVM

  소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- 볼륨 간, 다른 노드, 동일한 SVM

소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- SVM 간, 동일한 노드

  소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

- SVM 간, 다른 노드

  소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

- 클러스터 간

  소스 및 타겟 LUN은 클러스터 전반의 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 이 기능은 SAN에만 지원되며 SMB에는 적용되지 않습니다.

다음과 같은 몇 가지 특별한 사용 사례가 있습니다.

- ONTAP ODX를 구현하면 ODX를 사용하여 SMB 공유와 FC 또는 iSCSI 연결 가상 드라이브 간에 파일을 복사할 수 있습니다.

  SMB 공유와 LUN이 동일한 클러스터에 존재하는 경우, ODX를 지원하는 Windows 탐색기, Windows CLI 또는 PowerShell, Hyper-V 또는 기타 애플리케이션을 사용하여 SMB 공유와 연결된 LUN 간에 ODX 복사 오프로드를 사용하여 파일을 원활하게 복사 또는 이동할 수 있습니다.

- Hyper-V는 ODX 복사 오프로드를 위한 몇 가지 추가 사용 사례를 제공합니다.

  - Hyper-V에서 ODX 복사 오프로드 패스스스루 를 사용하여 VHD(가상 하드 디스크) 파일 내부 또는 VHD 파일 간에 데이터를 복사하거나, 매핑된 SMB 공유와 동일한 클러스터 내에서 연결된 iSCSI LUN 간에 데이터를 복사할 수 있습니다.

    이렇게 하면 게스트 운영 체제에서 복제본을 기본 스토리지로 전달할 수 있습니다.

  - 고정 크기의 VHD를 생성할 때 ODX는 잘 알려진 제로화 토큰을 사용하여 0으로 디스크를 초기화하는 데 사용됩니다.
  - 소스 및 타겟 스토리지가 동일한 클러스터에 있는 경우 ODX 복사 오프로드가 가상 머신 스토리지 마이그레이션에 사용됩니다.

> Hyper-V를 사용한 ODX 복사 오프로드 패스쓰루 사용 사례를 활용하려면 게스트 운영 체제가 ODX를 지원하고, 게스트 운영 체제 디스크는 ODX를 지원하는 스토리지(SMB 또는 SAN)를 통해 지원되는 SCSI 디스크여야 합니다. 게스트 운영 체제의 IDE 디스크는 ODX 패스스스루 를 지원하지 않습니다.

NVMe 복사 오프로드에 대해 알아보세요

NVMe 복사 오프로드를 사용하면 NVMe 호스트가 CPU에서 ONTAP 스토리지 컨트롤러의 CPU로 복사 작업을 오프로드할 수 있습니다. 호스트는 애플리케이션 워크로드를 위해 CPU 리소스를 예약하는 동시에 한 NVMe 네임스페이스에서 다른 네임스페이스로 데이터를 복사할 수 있습니다.

예를 들어, 성능 분포를 개선하기 위해 스토리지 작업 부하를 재조정해야 한다고 가정해 보겠습니다. 이를 위해서는 각각 평균 크기가 500GB인 45개의 NVMe 네임스페이스를 포함하는 10개의 가상 머신(VM)을 마이그레이션해야 합니다. 즉, 약 22.5TB의 데이터를 복사해야 한다는 의미입니다. 호스트는 데이터 마이그레이션에 자체 CPU를 사용하는 대신 NVMe 복사 오프로드를 사용하여 데이터가 복사되는 동안 애플리케이션 워크로드에 대한 CPU 리소스가 감소하지 않도록 할 수 있습니다.

NVMe 복사 오프로드 지원 및 제한 사항

NVMe 복사 오프로드는 ONTAP 9.18.1부터 지원됩니다. ONTAP NVMe 복사 오프로드를 시작할 수 없습니다. 호스트에서 지원하고 시작해야 합니다.

ONTAP 사용한 NVMe 복사 오프로드 작업에는 다음과 같은 제한 사항이 적용됩니다.

- 지원되는 최대 복사 작업 크기는 16MB입니다.
- 데이터는 동일한 하위 시스템 내의 NVMe 네임스페이스 간에만 마이그레이션될 수 있습니다.
- 데이터는 동일한 HA 쌍의 노드 간에만 마이그레이션될 수 있습니다.

SAN 관리

SAN 프로비저닝

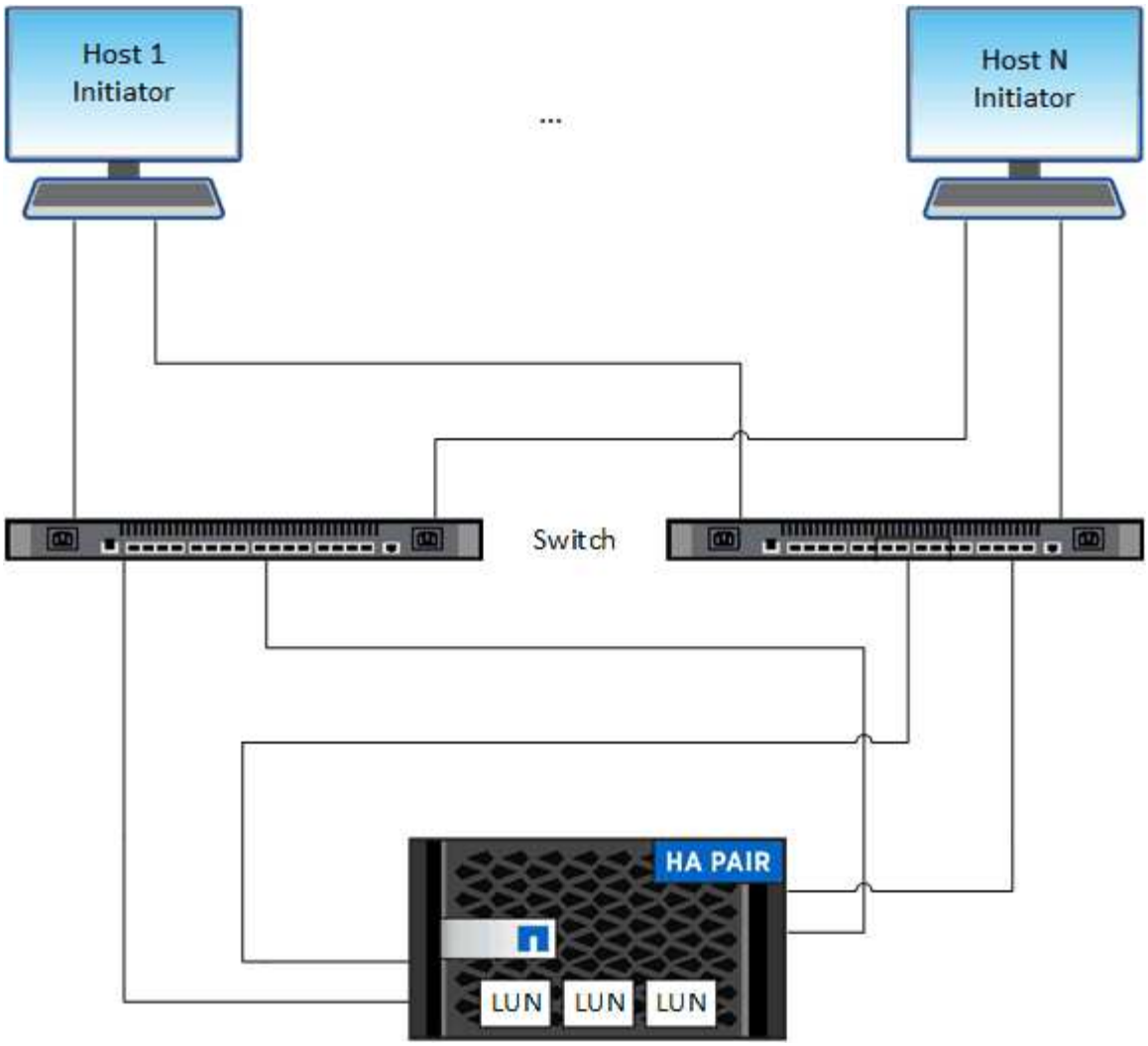
SAN 관리 개요

이 섹션의 내용은 ONTAP 9.7 이상 릴리즈에서 ONTAP CLI(Command Line Interface) 및 System Manager를 사용하여 SAN 환경을 구성하고 관리하는 방법을 보여줍니다.

클래식 시스템 관리자(ONTAP 9.7 이전에서만 사용 가능)를 사용하는 경우 다음 항목을 참조하십시오.

- "iSCSI 프로토콜"
- "FC/FCoE 프로토콜"

iSCSI 및 FC 프로토콜을 사용하여 SAN 환경에 스토리지를 제공할 수 있습니다.



iSCSI 및 FC에서는 스토리지 타겟을 LUN(논리 유닛)이라고 하며 호스트에 표준 블록 디바이스로 제공됩니다. LUN을 생성한 다음 이를 이니시에이터 그룹(igroup)에 매핑합니다. 이니시에이터 그룹은 FC 호스트 WWP 및 iSCSI 호스트 노드 이름의 테이블이며 어떤 이니시에이터가 LUN을 액세스할 수 있는지 제어합니다.

FC 대상은 FC 스위치 및 호스트 측 어댑터를 통해 네트워크에 연결되며 WWPN(World Wide Port Name)으로 식별됩니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 통합 네트워크 어댑터(CNA) 또는 전용 호스트 파스트 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 공인 이름(IQN)으로 식별됩니다.

를 참조하십시오

ASA R2 스토리지 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 또는 ASA A20)을 사용하는 경우 을 참조하십시오"ASA R2 스토리지 시스템 설명서".

All-Flash SAN 어레이 구성에 대해 자세히 알아보십시오

NetApp ASA(All-Flash SAN 어레이)는 ONTAP 9.7부터 사용할 수 있습니다. ASA는 검증된 AFF NetApp 플랫폼을 기반으로 하는 All-Flash SAN 전용 솔루션입니다.

ASA 플랫폼에는 다음이 포함됩니다.

- ASA A150

- ASA A250
- ASA A400
- ASA A800
- ASA A900
- ASA C250 을 참조하십시오
- ASA C400 을 참조하십시오
- ASA C800을 참조하십시오

ONTAP 9.16.0부터 ASA R2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 또는 ASA A20)에서 SAN 전용 고객을 위한 단순화된 ONTAP 환경을 이용할 수 있습니다. ASA R2 시스템을 사용하는 경우 를 "ASA R2 시스템 설명서"참조하십시오.

ASA 플랫폼은 다중 경로를 위해 대칭 액티브-액티브 를 사용합니다. 모든 경로가 액티브/최적화되어 있으므로 스토리지 페일오버 시 호스트는 I/O를 재개하기 위해 페일오버 경로의 ALUA 전환을 기다릴 필요가 없습니다 그러면 페일오버 시간이 단축됩니다.

ASA를 설정합니다

ASA(All-Flash SAN Array)는 비 ASA 시스템과 동일한 설정 절차를 따릅니다.

System Manager는 클러스터를 초기화하고, 로컬 계층을 생성하고, 프로토콜을 구성하고, ASA에 대한 스토리지를 프로비저닝하는 데 필요한 절차를 안내합니다.

ONTAP 클러스터 설정을 시작합니다.

ASA 호스트 설정 및 유틸리티

All-Flash SAN 어레이(ASA)를 설정하기 위한 호스트 설정은 다른 모든 SAN 호스트의 호스트 설정과 동일합니다.

를 다운로드할 수 있습니다 "NetApp 호스트 유틸리티 소프트웨어" 지원 사이트의 특정 호스트에 대해.

ASA 시스템을 식별하는 방법

ASA 시스템은 System Manager를 사용하거나 CLI(ONTAP Command Line Interface)를 사용하여 식별할 수 있습니다.

- * System Manager 대시보드에서 *: * 클러스터 > 개요 * 를 클릭한 다음 시스템 노드를 선택합니다.

  Personality * 는 * All-Flash SAN Array * 로 표시됩니다.

- * CLI * 에서: 를 입력합니다 `san config show` 명령.

  ASA 시스템에 대해 "All-Flash SAN 어레이" 값이 true로 반환됩니다.

  에 대한 자세한 내용은 `san config show` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "기술 보고서 4968: NetApp All-SAN 어레이 데이터 가용성 및 무결성"

- "NetApp 기술 보고서 4080: 최신 SAN에 대한 모범 사례"

FCoE에 대한 스위치를 구성합니다

FC 서비스를 기존 이더넷 인프라에서 실행하려면 먼저 FCoE에 대한 스위치를 구성해야 합니다.

시작하기 전에

- SAN 구성이 지원되어야 합니다.

  지원되는 구성에 대한 자세한 내용은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

- UTA(Unified Target Adapter)를 스토리지 시스템에 설치해야 합니다.

  UTA2를 사용하는 경우 "CNA" 모드로 설정해야 합니다.

- 통합 네트워크 어댑터(CNA)가 호스트에 설치되어 있어야 합니다.

단계

1. 스위치 설명서를 참조하여 FCoE에 맞게 스위치를 구성하십시오.
2. 클러스터의 각 노드에 대한 DCB 설정이 올바르게 구성되었는지 확인합니다.

   ```
   run -node node1 -command dcb show
   ```

   DCB 설정이 스위치에 구성되어 있습니다. 설정이 잘못된 경우 스위치 설명서를 참조하십시오.

3. FC 타겟 포트의 온라인 상태가 일 때 FCoE 로그인이 작동하는지 확인합니다 `true`.

   ```
   fcp adapter show -fields node,adapter,status,state,speed,fabric-
   established,physical-protocol
   ```

   FC 대상 포트의 온라인 상태가 "거짓"인 경우 스위치 설명서를 참조하십시오.

관련 정보

- "NetApp 상호 운용성 매트릭스 툴"
- "NetApp 기술 보고서 3800: FCoE(Fibre Channel over Ethernet) 엔드 투 엔드 구축 가이드"
- "Cisco MDS 9000 NX-OS 및 SAN-OS 소프트웨어 구성 가이드"
- "Brocade 제품"

시스템 요구 사항

LUN을 설정하려면 LUN을 생성하고, igroup을 생성하고, LUN을 igroup에 매핑해야 합니다. LUN을 설정하기 전에 시스템이 특정 사전 요구 사항을 충족해야 합니다.

- 상호 운용성 매트릭스에는 지원되는 SAN 구성이 나와 있어야 합니다.

- SAN 환경은 에 지정된 SAN 호스트 및 컨트롤러 구성 제한을 충족해야 합니다 "NetApp Hardware Universe를 참조하십시오" ONTAP 소프트웨어 버전에 적용됩니다.
- 지원되는 버전의 Host Utilities가 설치되어 있어야 합니다.

  자세한 내용은 Host Utilities 설명서를 참조하십시오.

- LUN 소유 노드와 소유 노드의 HA 파트너에 SAN LIF가 있어야 합니다.

관련 정보

- "NetApp 상호 운용성 매트릭스 툴"
- "ONTAP SAN 호스트 구성"
- "NetApp 기술 보고서 4017: 파이버 채널 SAN 모범 사례"

LUN을 생성하기 전에 알아야 할 사항

클러스터에서 LUN 설정을 시작하기 전에 이러한 LUN 지침을 검토해야 합니다.

실제 **LUN** 크기가 약간 다른 이유

LUN의 크기와 관련하여 다음 사항에 유의하십시오.

- LUN을 생성할 때 LUN의 실제 크기는 LUN의 OS 유형에 따라 약간 다를 수 있습니다. LUN을 생성한 후에는 LUN OS 유형을 수정할 수 없습니다.
- 최대 LUN 크기로 LUN을 생성하는 경우 LUN의 실제 크기가 약간 더 작을 수 있습니다. ONTAP는 한계치를 약간 낮추어 줍니다.
- 각 LUN의 메타데이터는 포함하는 애그리게이트에서 약 64KB의 공간을 필요로 합니다. LUN을 생성할 때 포함하는 애그리게이트에 LUN의 메타데이터를 위한 충분한 공간이 있는지 확인해야 합니다. Aggregate에 LUN의 메타데이터를 위한 충분한 공간이 없을 경우 일부 호스트에서 LUN에 액세스하지 못할 수 있습니다.

LUN ID 할당 지침

일반적으로 기본 LUN ID는 0으로 시작하고 각 추가 매핑된 LUN에 대해 1씩 증분식으로 할당됩니다. 호스트는 LUN ID를 LUN의 위치 및 경로 이름과 연결합니다. 유효한 LUN ID 번호의 범위는 호스트에 따라 다릅니다. 자세한 내용은 Host Utilities와 함께 제공된 설명서를 참조하십시오.

LUN을 **igroup**에 매핑하기 위한 지침

- LUN을 igroup에 한 번만 매핑할 수 있습니다.
- 모범 사례로서, igroup을 통해 하나의 특정 이니시에이터에 LUN을 매핑해야 합니다.
- 한 개의 이니시에이터를 여러 igroup에 추가할 수 있지만 이니시에이터는 하나의 LUN에만 매핑할 수 있습니다.
- 동일한 igroup에 매핑된 두 LUN에 대해 동일한 LUN ID를 사용할 수 없습니다.
- Igroup 및 포트 세트에 동일한 프로토콜 유형을 사용해야 합니다.

프로토콜 **FC** 또는 **iSCSI** 라이센스를 확인하고 추가합니다

FC 또는 iSCSI를 사용하여 SVM(스토리지 가상 시스템)에 대한 블록 액세스를 활성화하려면 먼저 라이센스가 있어야 합니다. FC 및 iSCSI 라이센스는 에 포함되어 "ONTAP 1 을

참조하십시오"있습니다.

예 **14.** 단계

시스템 관리자

ONTAP One이 없는 경우 ONTAP System Manager(9.7 이상)를 사용하여 FC 또는 iSCSI 라이센스를 확인하고 추가합니다.

1. System Manager에서 * Cluster > Settings > Licenses * 를 선택합니다
2. 라이센스가 목록에 없으면 를 선택하고 라이센스 키를 입력합니다

.
3. 추가 * 를 선택합니다.

CLI를 참조하십시오

ONTAP One이 없는 경우 ONTAP CLI를 사용하여 FC 또는 iSCSI 라이센스를 확인하고 추가합니다.

1. FC 또는 iSCSI에 대한 활성 라이센스가 있는지 확인합니다.

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. FC 또는 iSCSI에 대한 활성 라이센스가 없는 경우 라이센스 코드를 추가합니다.

```
license add -license-code <your_license_code>
```

SAN 스토리지 용량 할당

이 절차를 수행하면 FC 또는 iSCSI 프로토콜이 이미 구성된 기존 스토리지 VM에 새 LUN이 생성됩니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 저장소를 프로비저닝합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

새 스토리지 VM을 생성하고 FC 또는 iSCSI 프로토콜을 구성해야 하는 경우 를 참조하십시오 "FC용 SVM 구성" 또는 "iSCSI용 SVM을 구성합니다".

FC 라이센스가 활성화되어 있지 않으면 LIF 및 SVM이 온라인 상태로 나타나지만 운영 상태는 다운입니다.

LUN은 호스트에 디스크 디바이스로 나타납니다.

ALUA(Asymmetric Logical Unit Access)는 LUN 생성 중에 항상 사용하도록 설정됩니다. ALUA 설정은 변경할 수 없습니다.

SVM의 모든 FC LIF에서 이니시에이터를 호스팅하려면 단일 이니시에이터 조닝을 사용해야 합니다.

ONTAP 9.8부터는 스토리지 용량 할당 시 QoS가 기본적으로 사용하도록 설정됩니다. 프로비저닝 프로세스 도중 또는 나중에 QoS를 사용하지 않도록 설정하거나 사용자 지정 QoS 정책을 선택할 수 있습니다.

예 **15.** 단계

시스템 관리자

ONTAP System Manager(9.7 이상)와 함께 FC 또는 iSCSI 프로토콜을 사용하여 SAN 호스트에 스토리지를 제공할 LUN을 생성합니다.

System Manager Classic(9.7 이하 버전에서 사용 가능)을 사용하여 이 작업을 완료하려면 을 참조하십시오 "Red Hat Enterprise Linux용 iSCSI 구성"

단계

1. 호스트에 적절한 를 "SAN 호스트 유틸리티"설치합니다.
2. System Manager에서 * 스토리지 > LUN * 을 클릭한 다음 * 추가 * 를 클릭합니다.
3. LUN을 생성하는 데 필요한 정보를 입력합니다.
4. ONTAP 버전에 따라 * 추가 옵션 * 을 클릭하여 다음 중 하나를 수행할 수 있습니다.

옵션을 선택합니다	부터 사용할 수 있습니다
• 상위 볼륨 대신 LUN에 QoS 정책을 할당합니다 ◦ * 추가 옵션 > 스토리지 및 최적화 * 를 선택합니다 ◦ 성능 서비스 수준 * 을 선택합니다. ◦ 전체 볼륨 대신 개별 LUN에 QoS 정책을 적용하려면 * Apply these performance limits enforcement to each LUN * 을 선택합니다. 기본적으로 성능 제한은 볼륨 레벨에 적용됩니다.	ONTAP 9.10.1
• 기존 이니시에이터 그룹을 사용하여 새 이니시에이터 그룹을 생성합니다 ◦ 추가 옵션 > 호스트 정보 * ◦ 기존 이니시에이터 그룹을 사용하여 새 이니시에이터 그룹 * 을 선택합니다. ⓘ 다른 igroup이 포함된 igroup의 OS 유형은 생성된 후에는 변경할 수 없습니다.	ONTAP 9.9.1
• igroup 또는 호스트 이니시에이터에 설명을 추가합니다 이 설명은 igroup 또는 호스트 이니시에이터의 별칭으로 사용됩니다. ◦ 추가 옵션 > 호스트 정보 *	ONTAP 9.9.1

• 기존 볼륨에 LUN을 생성합니다 기본적으로 새 LUN은 새 볼륨에 생성됩니다. ◦ 추가 옵션 > LUN 추가 * 를 선택합니다 ◦ Group related LUNs * 를 선택합니다.	ONTAP 9.9.1
• QoS를 비활성화하거나 사용자 지정 QoS 정책을 선택합니다 ◦ * 추가 옵션 > 스토리지 및 최적화 * 를 선택합니다 ◦ 성능 서비스 수준 * 을 선택합니다. ⓘ ONTAP 9.9.1 이상에서 사용자 지정 QoS 정책을 선택하면 지정된 로컬 계층에 수동 배치를 선택할 수도 있습니다.	ONTAP 9.8

5. FC의 경우 WWPN으로 FC 스위치를 조닝(Zoning)하십시오. 이니시에이터당 하나의 존을 사용하고 각 존에 모든 타겟 포트를 포함합니다.
6. 호스트에서 LUN을 검색합니다.

   VMware vSphere의 경우 VSC(가상 스토리지 콘솔)를 사용하여 LUN을 검색하고 초기화할 수 있습니다.
7. LUN을 초기화하고 필요에 따라 파일 시스템을 생성합니다.
8. 호스트가 LUN에 데이터를 쓰고 읽을 수 있는지 확인합니다.

CLI를 참조하십시오

ONTAP CLI에서 FC 또는 iSCSI 프로토콜을 사용하여 SAN 호스트에 스토리지를 제공할 LUN을 생성합니다.

1. FC 또는 iSCSI에 대한 라이센스가 있는지 확인합니다.

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. FC 또는 iSCSI 라이센스가 없는 경우 'license add' 명령을 사용합니다.

```
license add -license-code <your_license_code>
```

3. SVM에서 프로토콜 서비스 지원:

   ◦ iSCSI의 경우: *

   ```
   vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
   ```

   ◦ FC: *

   ```
   vserver fcp create -vserver <svm_name> -status-admin up
   ```

4. 각 노드에서 SVM에 대해 2개의 LIF를 생성합니다.

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -role
   data -data-protocol <iscsi|fc> -home-node <node_name> -home-port
   <port_name> -address <ip_address> -netmask <netmask>
   ```

   NetApp은 각 SVM에서 데이터를 제공할 수 있도록 노드당 최소 하나의 iSCSI 또는 FC LIF를 지원합니다. 그러나 이중화를 위해서는 노드당 두 개의 LIF가 필요합니다. iSCSI의 경우 노드당 최소 두 개의 LIF를 별도의 이더넷 네트워크에 구성하는 것이 좋습니다.

5. LIF가 생성되었으며 운영 상태가 '온라인'인지 확인합니다.

   ```
   network interface show -vserver <svm_name> <lif_name>
   ```

6. LUN 생성:

   ```
   lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>
   -size <lun_size> -ostype linux -space-reserve <enabled|disabled>
   ```

   LUN 이름은 255자를 초과할 수 없으며 공백을 포함할 수 없습니다.

   NVFAIL 옵션은 볼륨에 LUN이 생성될 때 자동으로 활성화됩니다.

7. Igroup 생성:

   ```
   igroup create -vserver <svm_name> -igroup <igroup_name> -protocol
   <fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
   ```

8. LUN을 igroup에 매핑:

```
lun mapping create -vserver <svm_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. LUN이 올바르게 구성되었는지 확인합니다.

```
lun show -vserver <svm_name>
```

10. 필요한 경우 "포트 세트를 생성하고 igroup에 바인딩합니다".
11. 호스트 설명서의 단계를 따라 특정 호스트에서 블록 액세스를 설정합니다.
12. Host Utilities를 사용하여 FC 또는 iSCSI 매핑을 완료하고 호스트에서 LUN을 검색할 수 있습니다.

관련 정보

- "SAN 관리 개요"
- "ONTAP SAN 호스트 구성"
- "System Manager에서 SAN 이니시에이터 그룹을 보고 관리합니다"
- "NetApp 기술 보고서 4017: 파이버 채널 SAN 모범 사례"

NVMe 프로비저닝

NVMe 개요

NVMe(Non-Volatile Memory Express) 프로토콜을 사용하여 SAN 환경에 스토리지를 제공할 수 있습니다. NVMe 프로토콜은 솔리드 스테이트 스토리지의 성능을 위해 최적화되어 있습니다.

NVMe의 경우 스토리지 타겟을 네임스페이스라고 합니다. NVMe 네임스페이스는 많은 비휘발성 스토리지로, 논리 블록으로 포맷되고 호스트에 표준 블록 장치로 제공될 수 있습니다. 네임스페이스와 서브시스템을 생성한 다음, 네임스페이스를 서브시스템에 매핑합니다. 이는 LUN이 FC 및 iSCSI용 igroup에 프로비저닝 및 매핑된 방식과 유사합니다.

NVMe 대상은 이더넷 스위치 및 호스트 측 어댑터를 사용하여 FC 스위치 또는 표준 TCP 인프라를 사용하여 표준 FC 인프라를 통해 네트워크에 연결됩니다.

NVMe에 대한 지원은 ONTAP 버전에 따라 다릅니다. 을 참조하십시오 "NVMe 지원 및 제한 사항" 를 참조하십시오.

NVMe란 무엇입니까

NVMe(Nonvolatile Memory Express) 프로토콜은 비휘발성 스토리지 미디어에 액세스하는 데 사용되는 전송 프로토콜입니다.

NVMe over Fabrics (NVMeoF)는 PCIe 이외의 연결을 통해 NVMe 기반 통신을 가능하게 하는 NVMe에 대한 사양 정의 확장입니다. 이 인터페이스를 통해 외부 스토리지 인클로저를 서버에 연결할 수 있습니다.

NVMe는 플래시 기술에서 고성능 영구 메모리 기술에 이르기까지 비휘발성 메모리로 구축된 스토리지 장치에 효율적으로 액세스할 수 있도록 설계되었습니다. 따라서 하드 디스크 드라이브용으로 설계된 스토리지 프로토콜과 동일한 제한이 없습니다. 플래시 및 SSD(Solid State Device)는 일종의 비휘발성 메모리(NVM)입니다. NVM은 정전 시 콘텐츠를 보관하는 메모리의 한 유형입니다. NVMe는 해당 메모리에 액세스할 수 있는 방법입니다.

NVMe의 이점으로는 데이터 전송을 위한 속도, 생산성, 처리량 및 용량이 증가합니다. 구체적인 특징은 다음과 같습니다.

- NVMe는 최대 64,000개의 대기열을 지원하도록 설계되었습니다.

  또한 각 대기열에는 최대 64,000개의 동시 명령이 있을 수 있습니다.

- NVMe는 여러 하드웨어 및 소프트웨어 공급업체에서 지원합니다
- NMVe는 빠른 응답 시간을 지원하는 플래시 기술을 통해 생산성이 더 높습니다
- NVMe를 사용하면 SSD로 전송되는 각 "요청"에 대해 여러 데이터 요청을 처리할 수 있습니다.

  NVMe는 "재퀘스트"를 디코딩하는 데 시간이 더 적게 걸리며 다중 스레드 프로그램에서 스레드 잠금을 요구하지 않습니다.

- NVMe는 CPU 레벨에서 병목 현상을 방지하고 시스템이 확장됨에 따라 대규모 확장성을 지원하는 기능을 지원합니다.

NVMe 네임스페이스 정보

NVMe 네임스페이스는 논리 블록으로 포맷될 수 있는 비휘발성 메모리(NVM)의 양입니다. 네임스페이스는 스토리지 가상 머신이 NVMe 프로토콜을 통해 구성되고 FC 및 iSCSI 프로토콜에 대한 LUN과 동등한 경우에 사용됩니다.

하나 이상의 네임스페이스가 프로비저닝되고 NVMe 호스트에 연결됩니다. 각 네임스페이스는 다양한 블록 크기를 지원할 수 있습니다.

NVMe 프로토콜은 여러 컨트롤러를 통해 네임스페이스에 대한 액세스를 제공합니다. 대부분의 운영 체제에서 지원되는 NVMe 드라이버를 사용하면 SSD(Solid State Drive) 네임스페이스가 수정 없이 파일 시스템과 애플리케이션을 구축할 수 있는 표준 블록 장치로 표시됩니다.

네임스페이스 ID(NSID)는 네임스페이스에서 액세스를 제공하기 위해 컨트롤러에서 사용하는 식별자입니다. 호스트 또는 호스트 그룹에 대한 NSID를 설정할 때 호스트가 볼륨에 액세스할 수 있도록 구성할 수도 있습니다. 논리적 블록은 한 번에 하나의 호스트 그룹에만 매핑할 수 있으며, 지정된 호스트 그룹에는 중복된 NSID가 없습니다.

NVMe 하위 시스템 정보

NVMe 하위 시스템에는 하나 이상의 NVMe 컨트롤러, 네임스페이스, NVM 하위 시스템 포트, NVM 스토리지 미디어 및 컨트롤러와 NVM 스토리지 미디어 간의 인터페이스가 포함되어 있습니다. NVMe 네임스페이스를 생성할 때 기본적으로 이 네임스페이스는 서브시스템에 매핑되지 않습니다. 새 하위 시스템이나 기존 하위 시스템을 매핑하도록 선택할 수도 있습니다.

관련 정보

- "NVMe 스토리지 프로비저닝"ASA, AFF 및 FAS 시스템에 대해 알아보십시오
- "NVMe 네임스페이스를 서브시스템에 매핑합니다"ASA AFF 및 FAS 시스템에 대해 알아보십시오.
- "SAN 호스트 및 클라우드 클라이언트를 구성합니다"
- ASA R2(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 또는 ASA A20) 스토리지 시스템에 대해

알아보십시오."SAN 스토리지 프로비저닝"

NVMe 라이센스 요구 사항

ONTAP 9.5부터 NVMe를 지원하려면 라이센스가 필요합니다. ONTAP 9.4에서 NVMe를 사용하는 경우 ONTAP 9.5로 업그레이드한 후 라이센스를 취득하기 위한 90일 유예 기간이 제공됩니다.

다음 명령을 사용하여 라이센스를 설정할 수 있습니다.

'System license add-license-code_NVMe_license_key_'

NVMe 구성**,** 지원 및 제한 사항

ONTAP 9.4부터 "비휘발성 메모리 익스프레스(NVMe)" SAN 환경에서 프로토콜을 사용할 수 있습니다. FC-NVMe는 기존 FC 네트워크와 동일한 물리적 설정 및 조닝(zoning)을 사용하지만 FC-SCSI보다 더 큰 대역폭과 향상된 IOPS를 제공하며 지연 시간을 줄일 수 있습니다.

NVMe 지원 및 제한 사항은 사용 중인 ONTAP 버전, 플랫폼 및 구성에 따라 다릅니다. 특정 구성에 대한 자세한 내용은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴". 지원되는 제한 사항은 을 참조하십시오 "Hardware Universe".

클러스터당 최대 노드는 * 지원되는 플랫폼 혼합 * 에서 Hardware Universe에서 사용할 수 있습니다.

구성

- 단일 패브릭 또는 멀티 패브릭을 사용하여 NVMe 구성을 설정할 수 있습니다.
- SAN을 지원하는 모든 SVM에 하나의 관리 LIF를 구성해야 합니다.
- 임베디드 블레이드 스위치의 경우를 제외하고 이기종 FC 스위치 패브릭을 사용할 수 없습니다.

  특정 예외는 에 나열되어 있습니다 "NetApp 상호 운용성 매트릭스 툴".

- 캐스케이드, 부분 메시, 풀 메시, 코어 에지 및 디렉터 패브릭은 모두 FC 스위치를 패브릭에 연결하는 업계 표준 방법이며 모두 지원됩니다.

  패브릭은 하나 또는 여러 개의 스위치로 구성될 수 있으며, 스토리지 컨트롤러를 여러 스위치에 연결할 수 있습니다.

피처

사용 중인 ONTAP 버전에 따라 다음 NVMe 기능이 지원됩니다.

ONTAP로 시작하는 중…	NVMe를 지원합니다
9.17.1	• VMware 워크로드를 위한 SnapMirror 액티브 싱크 NVMe/FC 및 NVMe/TCP 호스트 액세스.
9.15.1	• NVMe/TCP에서 4노드 MetroCluster IP 구성

9.14.1	• 서브시스템에서 호스트 우선 순위 설정(호스트 레벨 QoS)
9.12.1	• NVMe/FC에서 4노드 MetroCluster IP 구성 • ONTAP 9.12.1 이전의 프런트 엔드 NVMe 네트워크에서는 MetroCluster 구성이 지원되지 않습니다. • MetroCluster 구성은 NVMe/TCP에서 지원되지 않습니다.
9.10.1	네임스페이스 크기 조정
9.9.1	• 네임스페이스와 LUN이 동일한 볼륨에 공존합니다
9.8	• 프로토콜 공존 SCSI, NAS 및 NVMe 프로토콜은 동일한 스토리지 가상 머신(SVM)에 존재할 수 있습니다. ONTAP 9.8 이전에는 SVM에서 NVMe가 유일한 프로토콜이 될 수 있습니다.
9.6	• 네임스페이스의 경우 512바이트 블록 및 4096바이트 블록입니다 기본값은 4096입니다. 512는 호스트 운영 체제가 4096바이트 블록을 지원하지 않는 경우에만 사용해야 합니다. • 매핑된 네임스페이스를 사용하여 볼륨 이동
9.5	• 다중 경로 HA 쌍 페일오버/반환

프로토콜

다음 NVMe 프로토콜이 지원됩니다.

프로토콜	ONTAP로 시작하는 중…	허용된 사용자…
TCP	9.10.1	기본값
FC	9.4	기본값

ONTAP 9.8부터 동일한 SVM(스토리지 가상 머신)에서 SCSI, NAS 및 NVMe 프로토콜을 구성할 수 있습니다. ONTAP 9.7 이하 버전에서는 NVMe가 SVM에서 유일한 프로토콜이 될 수 있습니다.

네임스페이스

NVMe 네임스페이스를 사용하여 작업할 때 다음을 숙지해야 합니다.

- ONTAP 9.15.1 이하 버전의 경우 ONTAP는 공간 재확보를 위해 NVMe와 함께 NVMe 데이터 집합 관리(할당 해제) 명령을 지원하지 않습니다.
- SnapRestore를 사용하여 LUN에서 네임스페이스를 복원하거나 그 반대로 복원할 수 없습니다.
- 네임스페이스에 대한 공간 보장은 포함하는 볼륨의 공간 보장과 동일합니다.
- 7-Mode에서 운영되는 Data ONTAP의 볼륨 전환에서는 네임스페이스를 생성할 수 없습니다.
- 네임스페이스는 다음을 지원하지 않습니다.
  - 이름 바꾸기
  - 볼륨 간 이동
  - 볼륨 간 복사
  - 온 디맨드 복사

추가 제한 사항

다음 **ONTAP** 기능은 **NVMe** 구성에서 지원되지 않습니다**.**

- 가상 스토리지 콘솔
- 영구 예약

다음은 **ONTAP 9.4**를 실행하는 노드에만 적용됩니다**.**

- NVMe LIF 및 네임스페이스는 동일한 노드에서 호스팅되어야 합니다.
- NVMe LIF가 생성되기 전에 NVMe 서비스를 생성해야 합니다.

관련 정보

"최신 SAN의 모범 사례"

NVMe용 스토리지 **VM**을 구성합니다

노드에서 NVMe 프로토콜을 사용하려면 NVMe용으로 특수 SVM을 구성해야 합니다.

시작하기 전에

FC 또는 이더넷 어댑터는 NVMe를 지원해야 합니다. 지원되는 어댑터가 에 나열되어 있습니다 "NetApp Hardware Universe를 참조하십시오".

예 **16.** 단계

시스템 관리자

ONTAP System Manager(9.7 이상)를 사용하여 NVMe용 스토리지 VM을 구성합니다.

새 스토리지 **VM**에서 **NVMe**를 구성합니다	기존 스토리지 **VM**에서 **NVMe**를 구성합니다
1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭한 다음 * 추가 * 를 클릭합니다. 2. 스토리지 VM의 이름을 입력합니다. 3. 액세스 프로토콜 * 에 대해 * NVMe * 를 선택합니다. 4. NVMe/FC * 활성화 또는 * NVMe/TCP * 활성화 및 * 저장 * 을 선택합니다.	1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭합니다. 2. 구성할 스토리지 VM을 클릭합니다. 3. 설정 * 탭을 클릭한 다음 NVMe 프로토콜 옆에 있는 을 클릭합니다. 4. NVMe/FC * 활성화 또는 * NVMe/TCP * 활성화 및 * 저장 * 을 선택합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 NVMe용 스토리지 VM을 구성합니다.

1. 기존 SVM을 사용하지 않으려면 다음을 생성합니다.

```
vserver create -vserver <SVM_name>
```

   a. SVM이 생성되었는지 확인:

```
vserver show
```

2. 클러스터에 NVMe 또는 TCP 가능 어댑터가 설치되어 있는지 확인합니다.

   NVMe의 경우:

```
network fcp adapter show -data-protocols-supported fc-nvme
```

   TCP의 경우:

```
network port show
```

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. ONTAP 9.7 이하를 실행 중인 경우 SVM에서 프로토콜을 모두 제거하십시오.

```
vserver remove-protocols -vserver <SVM_name> -protocols
iscsi,fcp,nfs,cifs,ndmp
```

ONTAP 9.8부터는 NVMe를 추가할 때 다른 프로토콜을 제거할 필요가 없습니다.

4. SVM에 NVMe 프로토콜을 추가합니다.

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. ONTAP 9.7 이하를 실행 중인 경우, NVMe가 SVM에서 허용되는 유일한 프로토콜인지 확인하십시오.

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

NVMe는 허용된 프로토콜 칼럼 아래에 표시되는 유일한 프로토콜이어야 합니다.

6. NVMe 서비스를 생성합니다.

```
vserver nvme create -vserver <SVM_name>
```

7. NVMe 서비스가 생성되었는지 확인하십시오.

```
vserver nvme show -vserver <SVM_name>
```

`Administrative Status`SVM은 으로 나열되어야 합니다 `up`. 에 대한 자세한 내용은 `up` link:https://docs.netapp.com/us-en/ontap-cli/up.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

8. NVMe/FC LIF 생성:
   - ONTAP 9.9.1 이하, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

   - ONTAP 9.10.1 이상의 경우 FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fc-nvme> -home-node <home_node> -home-port
<home_port> -status-admin up -failover-policy disabled -firewall
-policy data -auto-revert false -failover-group <failover_group>
-is-dns-update-enabled false
```

- ONTAP 9.10.1 이상의 경우 TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

9. HA 파트너 노드에 NVMe/FC LIF 생성:
   - ONTAP 9.9.1 이하, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

   - ONTAP 9.10.1 이상의 경우 FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-fc> -data-protocol <fc-nvme>
-home-node <home_node> -home-port <home_port> -status-admin up
-failover-policy disabled -firewall-policy data -auto-revert
false -failover-group <failover_group> -is-dns-update-enabled
false
```

   - ONTAP 9.10.1 이상의 경우 TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

10. NVMe/FC LIF가 생성되었는지 확인:

```
network interface show -vserver <SVM_name>
```

11. LIF와 동일한 노드에서 볼륨 생성:

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate
<aggregate_name> -size <volume_size>
```

자동 효율성 정책에 대한 경고 메시지가 표시되면 무시해도 됩니다.

NVMe 스토리지 프로비저닝

다음 단계를 사용하여 기존 스토리지 VM에서 NVMe 지원 호스트에 대한 네임스페이스를 생성하고 스토리지를 프로비저닝할 수 있습니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 저장소를 프로비저닝합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

ONTAP 9.8부터는 스토리지 용량 할당 시 QoS가 기본적으로 사용하도록 설정됩니다. 프로비저닝 프로세스 중에 또는 나중에 QoS를 비활성화하거나 사용자 지정 QoS 정책을 선택할 수 있습니다.

시작하기 전에

스토리지 VM은 NVMe에 맞게 구성해야 하며 FC 또는 TCP 전송은 이미 설정되어 있어야 합니다.

시스템 관리자

ONTAP System Manager(9.7 이상)를 사용하여 NVMe 프로토콜을 사용하여 스토리지를 제공하기 위한 네임스페이스를 생성합니다.

단계

1. System Manager에서 * 스토리지 > NVMe 네임스페이스 * 를 클릭한 다음 * 추가 * 를 클릭합니다.

   새 하위 시스템을 만들어야 하는 경우 * 추가 옵션 * 을 클릭합니다.

2. ONTAP 9.8 이상을 실행하고 있고 QoS를 비활성화하거나 사용자 지정 QoS 정책을 선택하려면 * 추가 옵션 * 을 클릭한 다음 * 스토리지 및 최적화 * 에서 * 성능 서비스 수준 * 을 선택합니다.
3. WWPN을 기준으로 FC 스위치를 조닝(Zoning)하십시오. 이니시에이터당 하나의 존을 사용하고 각 존에 모든 타겟 포트를 포함합니다.
4. 호스트에서 새 네임스페이스를 검색합니다.
5. 네임스페이스를 초기화하고 파일 시스템으로 포맷합니다.
6. 호스트에서 네임스페이스에서 데이터를 쓰고 읽을 수 있는지 확인합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 NVMe 프로토콜을 사용하여 스토리지를 제공하기 위한 네임스페이스를 생성합니다.

이 절차에서는 NVMe 프로토콜용으로 이미 구성된 기존 스토리지 VM에 NVMe 네임스페이스 및 서브시스템을 생성한 다음, 네임스페이스를 서브시스템에 매핑하여 호스트 시스템에서 데이터에 액세스할 수 있도록 합니다.

NVMe용 스토리지 VM을 구성해야 하는 경우 를 참조하십시오 "NVMe를 위한 SVM 구성".

단계

1. SVM이 NVMe용으로 구성되었는지 확인합니다.

   ```
   vserver show -vserver <svm_name> -fields allowed-protocols
   ```

   "NVMe"는 "허용된 프로토콜" 열 아래에 표시되어야 합니다.

2. NVMe 네임스페이스를 생성합니다.

   매개 변수로 참조하는 볼륨이 이미 존재해야 하며, 그렇지 않으면 이 명령을 실행하기 전에 볼륨을 `-path` 생성해야 합니다.

   ```
   vserver nvme namespace create -vserver <svm_name> -path <path> -size
   <size_of_namespace> -ostype <OS_type>
   ```

3. NVMe 하위 시스템을 생성합니다.

```
vserver nvme subsystem create -vserver <svm_name> -subsystem
<name_of_subsystem> -ostype <OS_type>
```

NVMe 하위 시스템 이름은 대/소문자를 구분합니다. 1 ~ 96자를 포함해야 합니다. 특수 문자를 사용할 수 있습니다.

4. 하위 시스템이 생성되었는지 확인합니다.

```
vserver nvme subsystem show -vserver <svm_name>
```

NVMe 서브시스템은 Subsystem 열에 표시되어야 한다.

5. 호스트에서 NQN을 가져옵니다.
6. 호스트 NQN을 하위 시스템에 추가합니다.

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN>
```

7. 네임스페이스를 하위 시스템에 매핑합니다.

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem
<subsystem_name> -path <path>
```

네임스페이스는 단일 하위 시스템에만 매핑할 수 있습니다.

8. 네임스페이스가 하위 시스템에 매핑되어 있는지 확인합니다.

```
vserver nvme namespace show -vserver <svm_name> -instance
```

하위 시스템은 연결된 하위 시스템으로 나열되어야 합니다.

NVMe 네임스페이스를 하위 시스템에 매핑합니다

NVMe 네임스페이스를 하위 시스템에 매핑하면 호스트에서 데이터에 액세스할 수 있습니다. 스토리지를 프로비저닝할 때 NVMe 네임스페이스를 하위 시스템에 매핑하거나 스토리지를 프로비저닝한 후 연결할 수 있습니다.

ONTAP 9.17.1부터 SnapMirror 액티브 동기화 구성을 사용하는 경우, 호스트를 NVMe 서브시스템에 추가하는 동시에 호스트에 SVM을 근접 가상 서버로 추가할 수 있습니다. NVMe 서브시스템의 네임스페이스에 대한 액티브 최적화 경로는 근접 가상 서버로 구성된 SVM에서만 호스트에 게시됩니다.

ONTAP 9.14.1부터 특정 호스트에 대한 리소스 할당의 우선 순위를 지정할 수 있습니다. 기본적으로 호스트가 NVMe 서브시스템에 추가되면 보통 우선 순위가 부여됩니다. ONTAP CLI(명령줄 인터페이스)를 사용하여 기본 우선 순위를 보통에서 높음으로 수동으로 변경할 수 있습니다. 높은 우선 순위가 할당된 호스트에는 더 큰 입출력 대기열 수와 대기열 깊이가 할당됩니다.

ONTAP 9.13.1 이하 버전에서 하위 시스템에 추가된 호스트에 높은 우선 순위를 부여하려는 경우 다음을 수행할 수 있습니다 호스트 우선 순위를 변경합니다.

시작하기 전에

네임스페이스와 하위 시스템이 이미 만들어져 있어야 합니다. 네임스페이스와 하위 시스템을 만들어야 하는 경우 를 참조하십시오 "NVMe 스토리지 프로비저닝".

NVMe 네임스페이스 매핑

단계

1. 호스트에서 NQN을 가져옵니다.
2. 호스트 NQN을 하위 시스템에 추가합니다.

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

호스트의 기본 우선 순위를 보통에서 높음으로 변경하려면 `-priority high` 옵션을 사용합니다. 이 옵션은 ONTAP 9.14.1부터 사용할 수 있습니다. 에 대한 자세한 내용은 `vserver nvme subsystem host add` "ONTAP 명령 참조입니다"을 참조하십시오.

SVM을 추가하려면 `proximal-vserver` SnapMirror 활성 동기화 구성에서 NVMe 하위 시스템에 호스트를 추가하는 동안 호스트에 다음을 사용할 수 있습니다. `-proximal-vservers` 옵션입니다. 이 옵션은 ONTAP 9.17.1부터 사용할 수 있습니다. 소스 SVM이나 대상 SVM, 또는 둘 다를 추가할 수 있습니다. 이 명령을 실행 중인 SVM이 기본값입니다.

3. 네임스페이스를 하위 시스템에 매핑합니다.

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem
<subsystem_name> -path <path>
```

네임스페이스는 단일 하위 시스템에만 매핑할 수 있습니다. 에 대한 자세한 내용은 `vserver nvme subsystem map add` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 네임스페이스가 하위 시스템에 매핑되어 있는지 확인합니다.

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

하위 시스템이 로 나열되어야 `Attached subsystem` 합니다. 에 대한 자세한 내용은 `vserver nvme namespace show` "ONTAP 명령 참조입니다"을 참조하십시오.

LUN 관리

LUN QoS 정책 그룹을 편집합니다

ONTAP 9.10.1부터 System Manager를 사용하여 여러 LUN에 동시에 QoS(서비스 품질) 정책을 할당하거나 제거할 수 있습니다.

볼륨 레벨에서 QoS 정책이 할당된 경우 볼륨 레벨에서 QoS 정책을 변경해야 합니다. LUN 레벨에서 원래 할당된 LUN 레벨에서만 QoS 정책을 편집할 수 있습니다.

단계

1. System Manager에서 * 스토리지 > LUN * 을 클릭합니다.
2. 편집할 LUN을 선택합니다.

   한 번에 둘 이상의 LUN을 편집하는 경우 LUN은 동일한 SVM(Storage Virtual Machine)에 속해야 합니다. 동일한 SVM에 속하지 않는 LUN을 선택하면 QoS 정책 그룹을 편집하는 옵션이 표시되지 않습니다.

3. More * 를 클릭하고 * Edit QoS Policy Group * 을 선택합니다.

LUN을 네임스페이스로 변환

ONTAP 9.11.1부터 ONTAP CLI를 사용하여 현재 위치에서 기존 LUN을 NVMe 네임스페이스로 변환할 수 있습니다.

시작하기 전에

- 지정한 LUN에 igroup에 대한 기존 맵이 없어야 합니다.
- LUN은 MetroCluster로 구성된 SVM이나 SnapMirror 활성 동기화 관계에 있어서는 안 됩니다.
- LUN은 프로토콜 엔드포인트이거나 프로토콜 엔드포인트에 바인딩되지 않아야 합니다.
- LUN에 0이 아닌 접두사 및/또는 접미사 스트림이 있어서는 안 됩니다.
- LUN은 스냅샷의 일부이거나 SnapMirror 관계의 대상 측에서 읽기 전용 LUN일 수 없습니다.

단계

1. LUN을 NVMe 네임스페이스로 변환:

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```

LUN을 오프라인 상태로 전환합니다

ONTAP 9.10.1부터 System Manager를 사용하여 LUN을 오프라인 상태로 전환할 수 있습니다. ONTAP 9.10.1 이전에는 ONTAP CLI를 사용하여 LUN을 오프라인 상태로 전환해야 합니다.

시스템 관리자

단계

1. System Manager에서 * 스토리지 > LUN * 을 클릭합니다.
2. 단일 LUN 또는 여러 LUN을 오프라인 상태로 전환합니다

원하는 사항	이렇게 하십시오.
단일 LUN을 오프라인 상태로 전환합니다	LUN 이름 옆에 있는 을 ⋮ 클릭하고 * 오프라인 상태로 전환 * 을 선택합니다.
여러 LUN을 오프라인 상태로 전환	1. 오프라인 상태로 전환할 LUN을 선택합니다. 2. More * 를 클릭하고 * Take Offline * 을 선택합니다.

CLI를 참조하십시오

CLI를 사용할 때는 한 번에 하나의 LUN만 오프라인 상태로 전환할 수 있습니다.

단계

1. LUN을 오프라인 상태로 전환:

```
lun offline <lun_name> -vserver <SVM_name>
```

ONTAP에서 **LUN** 크기를 조정합니다

LUN 크기를 늘리거나 줄일 수 있습니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 저장 장치의 크기를 늘리려면. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

ⓘ Solaris LUN의 크기는 조정할 수 없습니다.

LUN의 크기를 늘립니다

LUN을 늘릴 수 있는 크기는 ONTAP 버전에 따라 다릅니다.

ONTAP 버전입니다	최대 LUN 크기입니다
ONTAP 9.12.1P2 이상	AFF, FAS 및 ASA 플랫폼의 경우 128TB

ONTAP 9.8 이상	• ASA(All-Flash SAN 어레이) 플랫폼의 경우 128TB • 비 ASA 플랫폼의 경우 16TB
ONTAP 9.5, 9.6, 9.7	16TB
ONTAP 9.4 이하	원래 LUN 크기의 10배이지만 최대 LUN 크기인 16TB를 넘지 않습니다. 예를 들어 100GB LUN을 생성하는 경우 1,000GB로만 확장할 수 있습니다. LUN의 실제 최대 크기는 정확히 16TB가 아닐 수 있습니다. ONTAP는 한계치를 약간 낮추어 줍니다.

크기를 늘리기 위해 LUN을 오프라인 상태로 전환하지 않아도 됩니다. 그러나 크기를 늘린 후에는 호스트에서 LUN을 재검색하여 크기 변경을 인식해야 합니다.

예 **17.** 단계

시스템 관리자

ONTAP 시스템 관리자(9.7 이상)를 사용하여 LUN의 크기를 늘립니다.

1. System Manager에서 * 스토리지 > LUN * 을 클릭합니다.
2. 을 ⋮ 클릭하고 * 편집 * 을 선택합니다.
3. 스토리지 및 최적화 * 에서 LUN의 크기를 늘리고 * 저장 * 을 클릭합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 LUN의 크기를 늘립니다.

1. LUN 크기를 늘립니다.

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

   에 대한 자세한 내용은 `lun resize` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 늘어난 LUN 크기 확인:

```
lun show -vserver <SVM_name>
```

ONTAP 작업은 LUN의 실제 최대 크기를 반올림하여 예상 값보다 약간 작습니다. 또한 실제 LUN 크기는 LUN의 OS 유형에 따라 약간 다를 수 있습니다. 정확한 크기 조정 값을 얻으려면 고급 모드에서 다음 명령을 실행합니다.

```
set -unit B

lun show -fields max-resize-size -volume volume_name -lun lun_name
```

+
에 대한 자세한 내용은 `lun show` "ONTAP 명령 참조입니다"을 참조하십시오.

1. 호스트에서 LUN을 다시 검색합니다.
2. 호스트 문서에 따라 새로 생성된 LUN 크기를 호스트 파일 시스템에 표시합니다.

LUN 크기를 줄입니다

LUN 크기를 줄이기 전에 호스트는 LUN 데이터가 포함된 블록을 더 작은 LUN 크기의 바운더리로 마이그레이션해야 합니다. SnapCenter와 같은 툴을 사용하면 LUN 데이터가 포함된 블록을 잘라내지 않고도 LUN이 제대로 감소하는지 확인할 수 있습니다. LUN 크기를 수동으로 줄이는 것은 권장되지 않습니다.

LUN 크기를 줄이면 ONTAP에서 자동으로 LUN 크기가 줄어들었음을 이니시에이터에 알립니다. 그러나 호스트에서 새 LUN 크기를 인식하려면 추가 단계가 필요할 수 있습니다. 호스트 파일 구조의 크기 감소에 대한 자세한 내용은 호스트 설명서를 참조하십시오.

LUN을 이동합니다

SVM(스토리지 가상 시스템) 내의 볼륨 간에 LUN을 이동할 수 있지만 SVM 간에 LUN을 이동할 수는 없습니다. SVM 내에서 볼륨 간에 이동하는 LUN은 연결 끊김 없이 즉시 이동됩니다.

시작하기 전에

LUN이 SLM(선택적 LUN 맵)을 사용하는 경우 다음을 수행해야 합니다 "SLM reporting-nodes 목록을 수정합니다" LUN을 이동하기 전에 대상 노드 및 해당 HA 파트너를 포함해야 합니다.

이 작업에 대해

LUN 이동 중에는 중복제거, 압축, 컴팩션과 같은 스토리지 효율성 기능이 유지되지 않습니다. LUN 이동이 완료된 후 다시 적용해야 합니다.

스냅샷을 통한 데이터 보호는 볼륨 레벨에서 발생합니다. 따라서 LUN을 이동하면 대상 볼륨의 데이터 보호 체계에 따라 이동됩니다. 대상 볼륨에 대해 설정된 스냅샷이 없으면 LUN의 스냅샷이 생성되지 않습니다. 또한 LUN의 모든 스냅샷은 해당 스냅샷이 삭제될 때까지 원래 볼륨에 유지됩니다.

LUN을 다음 볼륨으로 이동할 수 없습니다.

- SnapMirror 타겟 볼륨
- SVM 루트 볼륨

다음 유형의 LUN을 이동할 수 없습니다.

- 파일에서 생성된 LUN입니다
- NVFail 상태인 LUN
- 로드 공유 관계에 있는 LUN입니다
- 프로토콜 엔드포인트 클래스 LUN

클러스터의 노드가 서로 다른 ONTAP 버전을 사용하는 경우, 소스 볼륨이 대상 볼륨보다 최신 버전인 경우에만 서로 다른 노드의 볼륨 간에 LUN을 이동할 수 있습니다. 예를 들어, 소스 볼륨의 노드가 ONTAP 9.15.1이고 대상 볼륨의

노드가 ONTAP 9.16.1인 경우 LUN을 이동할 수 없습니다. 동일한 ONTAP 버전을 사용하는 노드의 볼륨 간에는 LUN을 이동할 수 있습니다.

1TB 이상인 Solaris OS_TYPE LUN의 경우 LUN 이동 중에 호스트에서 시간 초과가 발생할 수 있습니다. 이 LUN 유형의 경우 이동을 시작하기 전에 LUN을 마운트 해제해야 합니다.

예 **18.** 단계

시스템 관리자

ONTAP System Manager(9.7 이상)를 사용하여 LUN을 이동합니다.

ONTAP 9.10.1부터 단일 LUN을 이동할 때 시스템 관리자를 사용하여 새 볼륨을 생성할 수 있습니다. ONTAP 9.8 및 9.9.1에서는 LUN 이동을 시작하기 전에 LUN을 이동할 볼륨이 있어야 합니다.

단계

1. System Manager에서 * 스토리지 > LUN * 을 클릭합니다.
2. 이동할 LUN을 마우스 오른쪽 버튼으로 ⋮ 클릭한 다음 * Move LUN * 을 선택합니다.

   ONTAP 9.10.1에서 LUN을 * 기존 볼륨 * 또는 * 새 볼륨 * 으로 이동하려면 선택합니다.

   새 볼륨을 생성하도록 선택한 경우 볼륨 사양을 제공합니다.
3. 이동 * 을 클릭합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 LUN을 이동합니다.

1. LUN 이동:

   ```
   lun move start
   ```

   매우 짧은 기간 동안 원본 볼륨과 대상 볼륨 모두에 LUN이 표시됩니다. 이는 예상되며 이동이 완료되면 해결됩니다.
2. 이동 상태를 추적하고 성공적으로 완료되었는지 확인합니다.

   ```
   lun move show
   ```

관련 정보

- "선택적 LUN 맵입니다"

LUN을 삭제합니다

LUN이 더 이상 필요하지 않은 경우 SVM(스토리지 가상 시스템)에서 LUN을 삭제할 수

있습니다.

시작하기 전에

LUN을 삭제하기 전에 해당 igroup에서 매핑 해제해야 합니다.

단계

1. 애플리케이션 또는 호스트에서 LUN을 사용하고 있지 않은지 확인합니다.
2. igroup에서 LUN 매핑을 해제합니다.

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<LUN_name> -igroup <igroup_name>
```

3. LUN을 삭제합니다.

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. LUN을 삭제했는지 확인합니다.

```
lun show -vserver <SVM_name>
```

```
Vserver   Path              State    Mapped  Type     Size
--------- ----------------- -------- ------- -------- ------
vs5       /vol/vol16/lun8   online   mapped  windows  10.00GB
```

LUN을 복제하기 전에 알아야 할 사항

LUN을 복제하기 전에 몇 가지 사항을 숙지해야 합니다.

클러스터 관리자는 'lun copy' 명령을 사용하여 클러스터 내의 SVM(스토리지 가상 머신)에서 LUN을 복제할 수 있습니다. 클러스터 관리자는 SVM 간 LUN 복사 작업을 수행하기 전에 'vserver peer create' 명령을 사용하여 SVM(스토리지 가상 시스템) 피어링 관계를 설정해야 합니다. 소스 볼륨에 SIS 클론에 대한 충분한 공간이 있어야 합니다.

스냅샷의 LUN은 명령의 소스 LUN으로 사용할 수 `lun copy` 있습니다. 명령을 사용하여 LUN을 복제하면 `lun copy` LUN 복사본을 읽기 및 쓰기 액세스에 즉시 사용할 수 있습니다. LUN 복제본을 생성해도 소스 LUN은 변경되지 않습니다. 소스 LUN과 LUN 복제본은 모두 LUN 일련 번호가 서로 다른 고유한 LUN으로 존재합니다. 소스 LUN에 대한 변경 내용은 LUN 복제본에 반영되지 않으며 LUN 복제본에 대한 변경 내용은 소스 LUN에 반영되지 않습니다. 소스 LUN의 LUN 매핑은 새 LUN에 복제되지 않으므로 LUN 복제본을 매핑해야 합니다.

스냅샷을 통한 데이터 보호는 볼륨 레벨에서 발생합니다. 따라서 LUN을 소스 LUN의 볼륨과 다른 볼륨으로 복제하는 경우 대상 LUN은 대상 볼륨의 데이터 보호 체계에 따라 달라집니다. 대상 볼륨에 대해 설정된 스냅샷이 없는 경우 LUN 복제본의 스냅샷이 생성되지 않습니다.

LUN을 복사하는 것은 무중단 운영입니다.

다음 유형의 LUN은 복제할 수 없습니다.

- 파일에서 생성된 LUN입니다
- NVFAIL 상태에 있는 LUN
- 로드 공유 관계에 있는 LUN입니다
- 프로토콜 엔드포인트 클래스 LUN

에 대한 자세한 내용은 `lun copy` "ONTAP 명령 참조입니다"을 참조하십시오.

LUN의 구성 및 사용 공간을 검사합니다

LUN에 사용된 구성된 공간과 실제 공간을 알면 공간 재확보, 데이터가 포함된 예약된 공간의 양, LUN에 사용된 실제 크기와 비교하여 재확보된 공간을 확인할 수 있습니다.

단계

1. 구성된 공간과 LUN에 사용된 실제 공간을 비교하여 확인합니다.

   LUN show

   다음 예에서는 vs3 스토리지 가상 시스템(SVM)에서 LUN이 사용하는 실제 공간과 구성된 공간을 비교하여 보여줍니다.

   'lun show -vserver vs3 - 필드 경로, 크기, 사용된 크기, 공간 예약

```
vserver path                    size    space-reserve size-used
------- ------------------      ------- ------------- ---------
vs3     /vol/vol0/lun1          50.01GB disabled      25.00GB
vs3     /vol/vol0/lun1_backup   50.01GB disabled      32.15GB
vs3     /vol/vol0/lun2          75.00GB disabled      0B
vs3     /vol/volspace/lun0      5.00GB  enabled       4.50GB
4 entries were displayed.
```

   에 대한 자세한 내용은 `lun show` "ONTAP 명령 참조입니다"을 참조하십시오.

스토리지 QoS를 사용하여 LUN에 대한 I/O 성능을 제어 및 모니터링합니다

스토리지 QoS 정책 그룹에 LUN을 할당하여 LUN에 대한 입출력 성능을 제어할 수 있습니다. 입출력 성능을 제어하여 워크로드가 특정 성능 목표를 달성하도록 보장하고, 다른 워크로드에 부정적인 영향을 주는 워크로드를 조절할 수 있습니다.

이 작업에 대해

정책 그룹은 최대 처리량 제한(예: 100MB/s)을 적용합니다. 최대 처리량을 지정하지 않고 정책 그룹을 생성하면 워크로드를 제어하기 전에 성능을 모니터링할 수 있습니다.

FlexVol 볼륨 및 LUN이 있는 SVM(스토리지 가상 시스템)을 정책 그룹에 할당할 수도 있습니다.

LUN을 정책 그룹에 할당하는 것에 대한 다음 요구 사항을 참고하십시오.

- LUN은 정책 그룹이 속한 SVM에 의해 포함되어야 합니다.

  정책 그룹을 생성할 때 SVM을 지정합니다.

- LUN을 정책 그룹에 할당할 경우 LUN에 포함된 볼륨 또는 SVM을 정책 그룹에 할당할 수 없습니다.

스토리지 QoS를 사용하는 방법에 대한 자세한 내용은 를 참조하십시오 "시스템 관리 참조".

단계

1. QoS policy-group create 명령을 사용하여 정책 그룹을 생성합니다.

   에 대한 자세한 내용은 `qos policy-group create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 정책 그룹에 LUN을 할당하려면 "lun create" 명령 또는 "lun modify" 명령과 함께 -qos-policy-group" 매개 변수를 사용합니다.

   에 대한 자세한 내용은 `lun` "ONTAP 명령 참조입니다"을 참조하십시오.

3. QoS 통계 명령어를 이용하여 성능 데이터를 확인할 수 있다.
4. 필요한 경우 QoS policy-group modify 명령을 사용하여 정책 그룹의 최대 처리량 한도를 조정합니다.

   에 대한 자세한 내용은 `qos policy-group modify` "ONTAP 명령 참조입니다"을 참조하십시오.

LUN을 효과적으로 모니터링하는 데 사용할 수 있는 툴입니다

툴을 사용하면 LUN을 효과적으로 모니터링하고 공간 부족 현상을 방지할 수 있습니다.

- Active IQ Unified Manager은 환경의 모든 클러스터에서 모든 스토리지를 관리할 수 있는 무료 툴입니다.
- System Manager는 ONTAP에 내장된 그래픽 사용자 인터페이스로, 클러스터 레벨에서 스토리지 요구사항을 수동으로 관리할 수 있습니다.
- OnCommand Insight은 스토리지 인프라에 대한 단일 뷰를 제공하며 LUN, 볼륨 및 애그리게이트에 스토리지 공간이 부족할 때 자동 모니터링, 경고 및 보고를 설정할 수 있습니다.

전환된 **LUN**의 기능 및 제한

SAN 환경에서는 7-Mode 볼륨을 ONTAP로 전환하는 동안 서비스 중단이 필요합니다. 전환을 완료하려면 호스트를 종료해야 합니다. 전환 후에는 ONTAP에서 데이터 제공을 시작하기 전에 호스트 구성을 업데이트해야 합니다

호스트를 종료하고 전환을 완료할 수 있는 유지 관리 기간을 예약해야 합니다.

7-Mode에서 운영되는 Data ONTAP에서 ONTAP로 전환된 LUN에는 LUN 관리 방식에 영향을 주는 특정 기능과 제한 사항이 있습니다.

전환된 LUN에서 다음을 수행할 수 있습니다.

- 'lun show' 명령을 사용하여 LUN을 확인합니다

- 'transition 7-mode show' 명령을 사용하여 7-Mode 볼륨에서 전환된 LUN의 인벤토리를 확인합니다
- 7-Mode 스냅샷에서 볼륨을 복원합니다

  볼륨을 복원하면 스냅샷에 캡처된 모든 LUN이 전환됩니다

- 명령을 사용하여 7-Mode 스냅샷에서 단일 LUN을 복원합니다 `snapshot restore-file`
- 7-Mode 스냅샷에서 LUN 클론을 생성합니다
- 7-Mode 스냅샷에서 캡처된 LUN의 블록 범위를 복원합니다
- 7-Mode 스냅샷을 사용하여 볼륨의 FlexClone을 생성합니다

전환된 LUN에서는 다음을 수행할 수 없습니다.

- 볼륨에서 캡처된 스냅샷 지원 LUN 클론에 액세스합니다

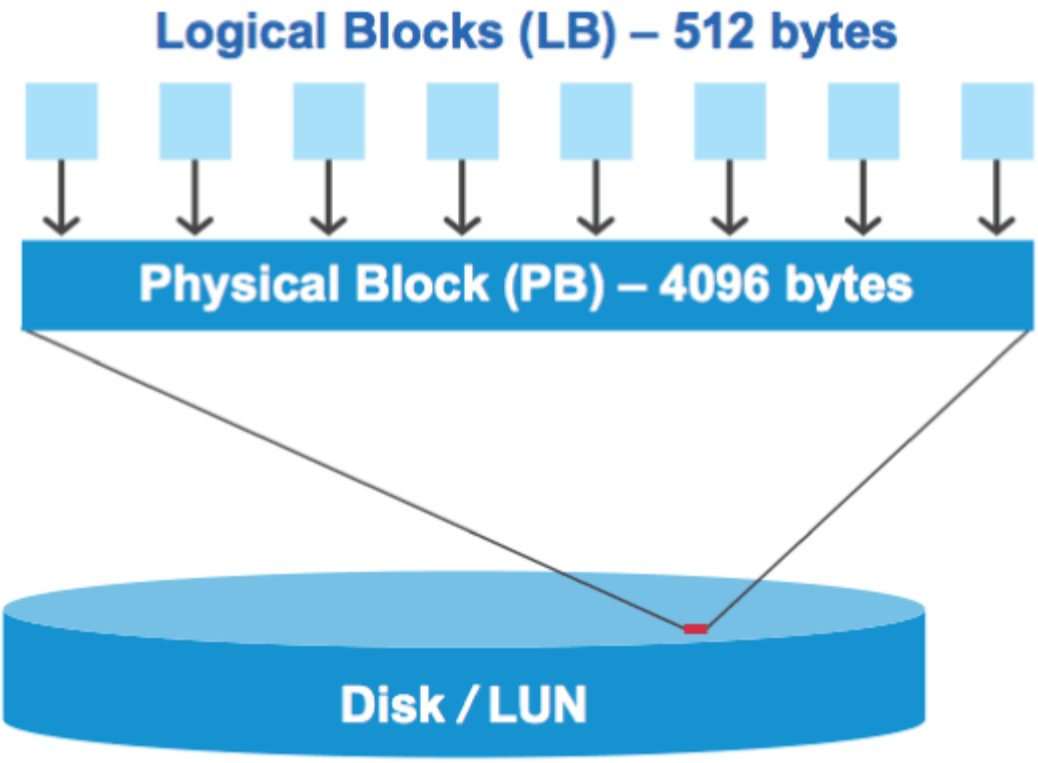
관련 정보

- "복사 기반 전환"
- "LUN 표시"

올바르게 정렬된 **LUN**의 입출력 정렬 불량 개요

ONTAP는 올바르게 정렬된 LUN에 대한 I/O 정렬 불량을 보고할 수 있습니다. 일반적으로 이 정렬 불량 경고는 LUN이 제대로 프로비저닝되고 파티셔닝 테이블이 올바른 경우에 무시할 수 있습니다.

LUN과 하드 디스크는 모두 스토리지를 블록으로 제공합니다. 호스트의 디스크에 대한 블록 크기가 512바이트이므로 LUN은 호스트에 해당 크기의 블록을 제공하는 동시에 실제로 더 큰 4KB 블록을 사용하여 데이터를 저장합니다. 호스트에서 사용되는 512바이트 데이터 블록을 논리적 블록이라고 합니다. LUN에서 데이터를 저장하는 데 사용하는 4KB 데이터 블록을 물리적 블록이라고 합니다. 즉, 각 4KB 물리적 블록에는 8개의 512바이트 논리적 블록이 있습니다.



호스트 운영 체제는 모든 논리 블록에서 읽기 또는 쓰기 I/O 작업을 시작할 수 있습니다. I/O 작업은 물리적 블록의 첫 번째 논리적 블록에서 시작될 때만 정렬되는 것으로 간주됩니다. 물리적 블록의 시작이 아닌 논리적 블록에서 I/O 작업이 시작되면 I/O가 잘못 정렬된 것으로 간주됩니다. ONTAP는 자동으로 정렬 불량을 감지하여 LUN에 보고합니다. 하지만 잘못 정렬된 I/O가 있다고 해서 LUN도 제대로 정렬되지 않은 것은 아닙니다. 잘못 정렬된 I/O가 제대로 정렬된 LUN에 보고될 수 있습니다.

추가 조사가 필요한 경우 다음을 참조하세요."NetApp 지식 기반: LUN에서 정렬되지 않은 IO를 식별하는 방법은 무엇입니까?"

정렬 문제 해결을 위한 도구에 대한 자세한 내용은 다음 설명서를 참조하십시오: +

- "Windows Unified Host Utilities 7.1"
- "SAN 스토리지 설명서를 프로비저닝합니다"

LUN OS 유형을 사용하여 **I/O**를 조정할 수 있습니다

ONTAP 9.7 이하 버전의 경우 권장 ONTAP LUN을 사용해야 합니다 `ostype` OS 파티셔닝 스키마에 I/O를 정렬하기 위해 운영 체제에 가장 일치하는 값

호스트 운영 체제에서 사용되는 파티션 구조는 I/O 정렬 불량을 크게 유발하는 요소입니다. 일부 ONTAP LUN "OSType" 값에는 호스트 운영 체제에서 사용하는 기본 파티셔닝 구조를 정렬할 수 있도록 "접두사"라고 하는 특수 오프셋을 사용합니다.

> ⓘ 경우에 따라 I/O를 정렬하기 위해 사용자 지정 파티셔닝 테이블이 필요할 수 있습니다. 그러나 접두사 값이 0보다 큰 OSType 값에서는 사용자 지정 파티션이 잘못 정렬된 I/O를 생성할 수 있습니다

ONTAP 9.7 또는 이전 버전에서 프로비저닝된 LUN에 대한 자세한 내용은 다음을 참조하세요."NetApp 기술 자료: LUN에서 정렬되지 않은 IO를 식별하는 방법" .

기본적으로 ONTAP 9.8 이상에서 프로비저닝된 새 LUN은 모든 LUN OS 유형에 대한 접두사 및 접미사 크기가 0입니다. I/O는 기본적으로 지원되는 호스트 운영 체제에 맞춰 정렬되어야 합니다.

Linux에 대한 특수 I/O 정렬 고려 사항

Linux 배포판은 데이터베이스, 다양한 볼륨 관리자 및 파일 시스템을 위한 원시 디바이스로 LUN을 사용하는 다양한 방법을 제공합니다. 원시 디바이스로 사용하거나 논리적 볼륨에서 물리적 볼륨으로 사용할 경우 LUN에 파티션을 생성할 필요가 없습니다.

RHEL 5 이전 및 SLES 10 이전 버전의 경우, 볼륨 관리자 없이 LUN을 사용할 경우, 정렬된 오프셋에서 시작하는 하나의 파티션을 LUN에 분할해야 합니다. 이 파티션은 8개의 논리적 블록의 짝수 배수로 이루어진 섹터입니다.

Solaris LUN에 대한 특수 I/O 정렬 고려 사항

'솔리스' OSType을 사용할지, '솔리스_EFI' OSType을 사용할지 결정할 때는 다양한 요소를 고려해야 합니다.

를 참조하십시오 "Solaris 호스트 유틸리티 설치 및 관리 가이드" 을 참조하십시오.

ESX 부팅 LUN이 잘못 정렬되었습니다

ESX 부팅 LUN으로 사용되는 LUN은 일반적으로 ONTAP에서 정렬 불량이 있다고 보고합니다. ESX는 부팅 LUN에 여러 파티션을 생성하므로 정렬하기가 매우 어렵습니다. 잘못 정렬된 ESX 부팅 LUN은 일반적으로 성능 문제가 되지 않습니다. 잘못 정렬된 입출력의 총량이 작기 때문입니다. LUN이 VMware "OSType"으로 올바르게 프로비저닝되었다고 가정할 경우 별도의 작업이 필요하지 않습니다.

관련 정보

"VMware vSphere, 기타 가상 환경 및 NetApp 스토리지 시스템에 대한 게스트 VM 파일 시스템 파티션/디스크 정렬"

LUN이 오프라인 상태가 될 때 발생하는 문제를 해결하는 방법

쓰기에 사용할 수 있는 공간이 없으면 LUN이 오프라인 상태가 되어 데이터 무결성을 유지합니다. LUN의 공간이 부족하고 다양한 이유로 인해 오프라인 상태가 될 수 있으며 문제를 해결할 수 있는 몇 가지 방법이 있습니다.

만약...	할 수 있는 일...
Aggregate가 가득 찼습니다	• 디스크를 더 추가합니다. • 'volume modify' 명령을 사용하여 사용 가능한 공간이 있는 볼륨을 축소합니다. • 사용 가능한 공간이 있는 공간 보장 볼륨이 있는 경우 볼륨 수정 명령을 사용하여 볼륨 공간 보장을 "없음"으로 변경합니다.

만약...	할 수 있는 일...
볼륨이 가득 찼지만 포함된 애그리게이트에 사용 가능한 공간이 있습니다	• 공간 보장 볼륨의 경우 볼륨 크기를 늘리려면 'volume modify' 명령을 사용하십시오. • 씬 프로비저닝된 볼륨의 경우 'volume modify' 명령을 사용하여 볼륨의 최대 크기를 늘리십시오. 볼륨 자동 증가를 사용하지 않는 경우 'volume modify-en자동 확장 모드'를 사용하여 활성화하십시오. • 명령을 사용하여 스냅샷을 수동으로 `volume snapshot delete` 삭제하거나 명령을 사용하여 `volume snapshot autodelete modify` 스냅샷을 자동으로 삭제합니다.

관련 정보

"디스크 및 로컬 계층(애그리게이트) 관리"

"논리적 스토리지 관리"

호스트에 표시되지 않는 **iSCSI LUN** 문제를 해결합니다

iSCSI LUN은 호스트에 로컬 디스크로 표시됩니다. 스토리지 시스템 LUN을 호스트에서 디스크로 사용할 수 없는 경우 구성 설정을 확인해야 합니다.

구성 설정	할 일
케이블 연결	호스트와 스토리지 시스템 사이의 케이블이 올바르게 연결되었는지 확인합니다.
네트워크 연결	호스트와 스토리지 시스템 간에 TCP/IP 접속이 설정되어 있는지 확인합니다. • 스토리지 시스템 명령줄에서 iSCSI에 사용 중인 호스트 인터페이스를 ping합니다. "ping –node_node_name_-destination_host_ip_address_for_iscsi_" • 호스트 명령줄에서 iSCSI에 사용 중인 스토리지 시스템 인터페이스를 ping합니다. "ping –node_node_name_-destination_host_ip_address_for_iscsi_"
시스템 요구 사항	구성 요소의 자격 여부를 확인합니다. 또한 호스트 운영 체제(OS) 서비스 팩 수준, 이니시에이터 버전, ONTAP 버전 및 기타 시스템 요구 사항이 올바른지 확인합니다. 상호 운용성 매트릭스에는 최신 시스템 요구 사항이 포함되어 있습니다.
점보 프레임	구성에서 점보 프레임을 사용하는 경우 네트워크 경로의 모든 장치(호스트 이더넷 NIC, 스토리지 시스템 및 모든 스위치)에서 점보 프레임이 활성화되어 있는지 확인합니다.
iSCSI 서비스 상태입니다	iSCSI 서비스에 라이센스가 부여되어 스토리지 시스템에서 시작되었는지 확인합니다.

구성 설정	할 일
초기자 로그인	이니시에이터가 스토리지 시스템에 로그인되어 있는지 확인합니다. "iscsi initiator show" 명령 출력에 로그인한 이니시에이터가 없는 경우 호스트에서 이니시에이터 구성을 확인하십시오. 스토리지 시스템이 이니시에이터의 타겟으로 구성되어 있는지도 확인합니다.
iSCSI 노드 이름(IQN)	igroup 구성에서 올바른 이니시에이터 노드 이름을 사용하고 있는지 확인합니다. 호스트에서 이니시에이터 툴 및 명령을 사용하여 이니시에이터 노드 이름을 표시할 수 있습니다. igroup 및 호스트에 구성된 이니시에이터 노드 이름이 일치해야 합니다.
LUN 매핑	LUN이 igroup에 매핑되어 있는지 확인합니다. 스토리지 시스템 콘솔에서 다음 명령 중 하나를 사용할 수 있습니다. • LUN mapping show는 모든 LUN과 매핑된 igroup을 표시합니다. • 'lun mapping show -igroup'은 특정 igroup에 매핑된 LUN을 표시합니다.
iSCSI LIF가 사용하도록 설정합니다	iSCSI 논리 인터페이스가 활성화되었는지 확인합니다.

관련 정보

- "NetApp 상호 운용성 매트릭스 툴"
- "LUN 매핑이 표시됩니다"

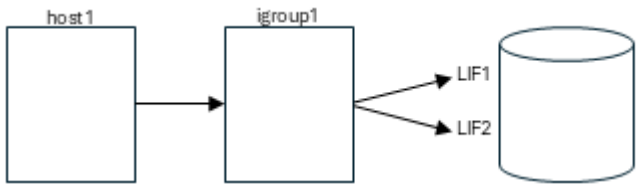
Igroup 및 portset 관리

포트 세트 및 **igroup**을 사용하여 **LUN** 액세스를 제한하는 방법

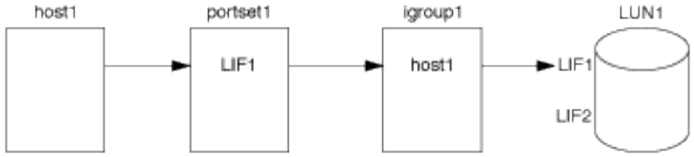
SLM(Selective LUN Map)을 사용하는 것 외에도 igroup 및 포트 세트를 통해 LUN에 대한 액세스를 제한할 수 있습니다.

Portset을 SLM과 함께 사용하여 특정 타겟에 대한 액세스를 특정 이니시에이터에 추가로 제한할 수 있습니다. 포트 세트와 함께 SLM을 사용하는 경우 LUN을 소유한 노드의 HA 파트너와 해당 노드의 포트셋 LIF 세트에서 LUN에 액세스할 수 있습니다.

다음 예에서 host1에는 포트셋이 없습니다. 포트셋이 없으면 host1은 LIF1과 LIF2를 통해 LUN1에 액세스할 수 있습니다.



포트셋을 사용하여 LUN1에 대한 액세스를 제한할 수 있습니다. 다음 예에서 host1은 LIF1을 통해서만 LUN1에 액세스할 수 있습니다. 하지만 LIF2가 portset1에 없기 때문에 host1은 LIF2를 통해 LUN1에 액세스할 수 없습니다.



관련 정보

- 선택적 LUN 맵입니다
- 포트셋 및 igroup에 바인딩

SAN 이니시에이터 및 **igroup**을 보고 관리합니다

System Manager를 사용하여 이니시에이터 그룹(igroup)과 이니시에이터를 보고 관리할 수 있습니다.

이 작업에 대해

- 이니시에이터 그룹은 스토리지 시스템의 특정 LUN에 액세스할 수 있는 호스트를 식별합니다.
- 이니시에이터 및 이니시에이터 그룹을 생성한 후 편집하거나 삭제할 수 있습니다.
- SAN 이니시에이터 그룹 및 이니시에이터를 관리하려면 다음 작업을 수행할 수 있습니다.
  - [view-manage-san-igroups]
  - [view-manage-san-inits]

SAN 이니시에이터 그룹을 보고 관리합니다

System Manager를 사용하여 이니시에이터 그룹(igroup) 목록을 볼 수 있습니다. 목록에서 추가 작업을 수행할 수 있습니다.

단계

1. System Manager에서 * 호스트 > SAN 이니시에이터 그룹 * 을 클릭합니다.

   페이지에 이니시에이터 그룹(igroup) 목록이 표시됩니다. 목록이 큰 경우 페이지의 오른쪽 아래 모서리에 있는 페이지 번호를 클릭하여 목록의 추가 페이지를 볼 수 있습니다.

   열에는 igroup에 대한 다양한 정보가 표시됩니다. 9.11.1부터 igroup의 연결 상태도 표시됩니다. 상태 알림 위로 마우스를 가져가면 세부 정보가 표시됩니다.

2. (선택 사항): 목록의 오른쪽 위에 있는 아이콘을 클릭하여 다음 작업을 수행할 수 있습니다.
   - * 검색 *
   - * 목록을 다운로드 * 합니다.
   - 목록에서 * 표시 * 또는 * 숨기기 * 열을 표시합니다.
   - * 필터 * 목록의 데이터.
3. 목록에서 작업을 수행할 수 있습니다.
   - + Add igroup을 추가하려면 클릭합니다.
   - igroup 이름을 클릭하여 igroup에 대한 세부 정보를 보여주는 * Overview * 페이지를 표시합니다.

개요 * 페이지에서 igroup과 연결된 LUN을 볼 수 있으며 작업을 시작하여 LUN을 생성하고 LUN을 매핑할 수 있습니다. 기본 목록으로 돌아가려면 * 모든 SAN 이니시에이터 * 를 클릭합니다.

- igroup에 마우스를 올려놓고 igroup 이름 옆에 있는 을 클릭하여 ⋮ igroup을 편집하거나 삭제합니다.
- igroup 이름 왼쪽에 있는 영역 위로 마우스를 가져간 다음 확인란을 선택합니다. 이니시에이터 그룹에 * + 추가를 클릭하면 해당 igroup을 다른 igroup에 추가할 수 있습니다.
- 스토리지 VM * 열에서 스토리지 VM의 이름을 클릭하여 해당 VM에 대한 세부 정보를 봅니다.

SAN 이니시에이터를 보고 관리합니다

System Manager를 사용하여 이니시에이터 목록을 볼 수 있습니다. 목록에서 추가 작업을 수행할 수 있습니다.

단계

1. System Manager에서 * 호스트 > SAN 이니시에이터 그룹 * 을 클릭합니다.

   페이지에 이니시에이터 그룹(igroup) 목록이 표시됩니다.

2. 이니시에이터를 보려면 다음을 수행하십시오.

   - FC 이니시에이터 * 탭을 클릭하여 FC 이니시에이터 목록을 표시합니다.
   - iSCSI 초기자 목록을 보려면 * iSCSI 초기자 * 탭을 클릭합니다.

     열에는 이니시에이터에 대한 다양한 정보가 표시됩니다.

   9.11.1부터 초기자의 연결 상태도 표시됩니다. 상태 알림 위로 마우스를 가져가면 세부 정보가 표시됩니다.

3. (선택 사항): 목록의 오른쪽 위에 있는 아이콘을 클릭하여 다음 작업을 수행할 수 있습니다.
   - * 검색 * 특정 이니시에이터 목록입니다.
   - * 목록을 다운로드 * 합니다.
   - 목록에서 * 표시 * 또는 * 숨기기 * 열을 표시합니다.
   - * 필터 * 목록의 데이터.

중첩된 **igroup**을 생성합니다

ONTAP 9.9.1부터 다른 기존 igroup으로 구성된 igroup을 생성할 수 있습니다.

1. System Manager에서 * 호스트 > SAN 이니시에이터 그룹 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
2. igroup * 이름 * 및 * 설명 * 을 입력합니다.

   설명은 igroup 별칭으로 사용됩니다.

3. 스토리지 VM * 및 * 호스트 운영 체제 * 를 선택합니다.

   ⓘ igroup이 생성된 후 중첩된 igroup의 OS 유형을 변경할 수 없습니다.

4. 이니시에이터 그룹 구성원 * 에서 * 기존 이니시에이터 그룹 * 을 선택합니다.

검색 * 을 사용하여 추가할 이니시에이터 그룹을 찾아서 선택할 수 있습니다.

여러 **LUN**에 **igroup** 매핑

ONTAP 9.9.1부터 igroup을 2개 이상의 LUN에 동시에 매핑할 수 있습니다.

1. System Manager에서 * 스토리지 > LUN * 을 클릭합니다.
2. 매핑할 LUN을 선택합니다.
3. More * 를 클릭한 다음 * Map to Initiator Groups * 를 클릭합니다.

선택한 igroup이 선택한 LUN에 추가됩니다. 기존 매핑은 덮어쓰지 않습니다.

포트셋 및 **igroup**에 바인딩

또한 를 사용할 수 있습니다 "선택적 LUN 맵(SLM)"포트셋 를 생성하고 포트셋 를 igroup에 바인딩하여 이니시에이터에서 LUN에 액세스하는 데 사용할 수 있는 LIF를 더 제한할 수 있습니다.

포트셋 를 igroup에 바인딩하지 않으면 igroup의 모든 이니시에이터가 LUN과 소유 노드의 HA 파트너가 소유하는 노드의 모든 LIF를 통해 매핑된 LUN에 액세스할 수 있습니다.

시작하기 전에

LIF가 하나 이상, igroup 하나가 있어야 합니다.

인터페이스 그룹을 사용하지 않는 경우 iSCSI와 FC 모두에서 중복성을 위해 두 개의 LIF가 권장됩니다. 인터페이스 그룹에서는 LIF가 하나만 권장됩니다.

이 작업에 대해

노드에 LIF가 2개 이상 있고 특정 이니시에이터를 LIF의 하위 집합으로 제한하려는 경우 SLM에 Portset을 사용하는 것이 좋습니다. 포트 세트가 없으면 LUN 및 소유 노드의 HA 파트너를 소유하는 노드를 통해 LUN에 액세스할 수 있는 모든 이니시에이터가 노드의 모든 타겟에 액세스할 수 있습니다.

예 **19.** 단계

시스템 관리자

ONTAP 9.10.1부터 System Manager를 사용하여 포트 세트를 생성하고 igroup에 바인딩할 수 있습니다.

9.10.1 이전의 ONTAP 릴리즈에서 포트셋 및 igroup을 바인딩해야 하는 경우 ONTAP CLI 절차를 사용해야 합니다.

ONTAP 9.12.1부터 기존 포트셋이 없으면 ONTAP CLI 프로시저를 사용하여 첫 번째 포트셋을 만들어야 합니다.

1. System Manager에서 * Network > Overview > Portsets * 를 클릭하고 * Add * 를 클릭합니다.
2. 새 포트셋 정보를 입력하고 * 추가 * 를 클릭합니다.
3. 호스트 > SAN 이니시에이터 그룹 * 을 클릭합니다.
4. 포트셋 를 새 igroup에 바인딩하려면 * 추가 * 를 클릭합니다.

   포트셋 을 기존 igroup에 바인딩하려면 igroup을 선택하고 를 ⋮클릭한 다음 * 이니시에이터 그룹 편집 * 을 클릭합니다.

관련 정보

"이니시에이터 및 igroup을 보고 관리합니다"

CLI를 참조하십시오

1. 적절한 LIF가 포함된 포트 세트를 생성합니다.

   ' create-vserver_vserver_name_-포트셋_이름_-protocol_protocol_-port-name_port_name_'

   FC를 사용하는 경우 프로토콜 매개변수를 FCP로 지정합니다. iSCSI를 사용하는 경우 프로토콜 매개변수를 iSCSI로 지정합니다.

2. igroup을 포트 세트에 바인드합니다.

   'lun igroup bind -vserver_vserver_name_-igroup_igroup_name_-포트셋_포트셋_이름_

   에 대한 자세한 내용은 `lun igroup bind` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 포트 세트와 LIF가 올바른지 확인합니다.

   ' show-vserver_vserver_name_'

```
Vserver   Portset   Protocol Port Names    Igroups
--------- --------- -------- ------------- --------
vs3       portset0  iscsi    lif0,lif1     igroup1
```

포틀세트를 관리합니다

또한 "선택적 LUN 맵(SLM)"포트 세트를 사용하여 이니시에이터에서 LUN에 액세스하는 데

사용할 수 있는 LIF를 추가로 제한할 수 있습니다.

ONTAP 9.10.1부터 System Manager를 사용하여 포트 세트와 관련된 네트워크 인터페이스를 변경하고 포트 세트를 삭제할 수 있습니다.

포트셋 관련 네트워크 인터페이스를 변경합니다

1. System Manager에서 * Network > Overview > Portsets * 를 선택합니다.
2. 편집할 포트셋 을 선택한 ⋮ 다음 * 포트세트 편집 * 을 선택합니다.

포트셋 삭제

1. System Manager에서 * Network > Overview > Portsets * 를 클릭합니다.
2. 포트셋 하나를 삭제하려면 포트셋, 선택 후 * 포트세트 삭제 * 를 ⋮ 선택합니다.

   여러 개의 포트 세트를 삭제하려면 포트 세트를 선택하고 * Delete * (삭제 *)를 클릭합니다.

선택적 **LUN** 맵 개요

SLM(Selective LUN Map)은 호스트에서 LUN으로의 경로 수를 줄입니다. SLM 기능을 통해 새 LUN 맵이 생성되면 LUN 및 해당 HA 파트너를 소유하는 노드의 경로를 통해서만 LUN에 액세스할 수 있습니다.

SLM은 호스트당 단일 igroup을 관리할 수 있도록 하며, 포트셋 조작 또는 LUN 재매핑이 필요하지 않은 무중단 LUN 이동 작업도 지원합니다.

"포트 세트" SLM과 함께 사용하여 특정 타겟에 대한 액세스를 특정 이니시에이터에 더 제한할 수 있습니다. 포트 세트와 함께 SLM을 사용하는 경우 LUN을 소유한 노드의 HA 파트너와 해당 노드의 포트셋 LIF 세트에서 LUN에 액세스할 수 있습니다.

SLM은 모든 새로운 LUN 맵에서 기본적으로 활성화됩니다.

LUN 맵에서 **SLM**이 설정되었는지 여부를 확인합니다

환경에 ONTAP 9 릴리즈에서 생성된 LUN과 이전 버전에서 전환된 LUN의 조합이 있는 경우, 특정 LUN에 SLM(선택적 LUN 맵)이 활성화되어 있는지 여부를 확인해야 할 수 있습니다.

의 출력에 표시된 정보를 사용할 수 있습니다 `lun mapping show -fields reporting-nodes, node` 명령을 사용하여 LUN 맵에서 SLM이 활성화되어 있는지 여부를 확인합니다. SLM이 활성화되지 않은 경우 명령 출력의 "노드 재이식" 열 아래의 셀에 "-"가 표시됩니다. SLM이 활성화된 경우 ""노드" 열 아래에 표시되는 노드 목록이 "노드 재이식" 열에 복제됩니다.

에 대한 자세한 내용은 `lun mapping show` "ONTAP 명령 참조입니다"을 참조하십시오.

SLM 보고 노드 목록을 수정합니다

LUN이 포함된 LUN 또는 볼륨을 동일한 클러스터 내의 다른 고가용성(HA) 쌍으로 이동하는 경우, 이동을 시작하기 전에 선택 LUN 맵(SLM: Selective LUN Map) 보고 노드 목록을 수정하여 최적화된 활성 LUN 경로가 유지되도록 해야 합니다.

단계

1. 대상 노드와 해당 파트너 노드를 애그리게이트 또는 볼륨의 보고 노드 목록에 추가합니다.

```
lun mapping add-reporting-nodes -vserver <vserver_name> -path <lun_path>
-igroup <igroup_name> [-destination-aggregate <aggregate_name>|-
destination-volume <volume_name>]
```

일관된 명명 규칙이 있는 경우 대신 를 사용하여 여러 LUN 매핑을 동시에 수정할 수 있습니다 `igroup_prefix*` `igroup_name`.

2. 호스트를 재검색하여 새로 추가된 경로를 검색합니다.
3. OS에 필요한 경우 다중 경로 네트워크 I/O(MPIO) 구성에 새 경로를 추가합니다.
4. 필요한 이동 작업에 대해 명령을 실행하고 작업이 완료될 때까지 기다립니다.
5. Active/Optimized 경로를 통해 입출력이 서비스되고 있는지 확인합니다.

```
lun mapping show -fields reporting-nodes
```

6. 보고 노드 목록에서 이전 LUN 소유자 및 해당 파트너 노드를 제거합니다.

```
lun mapping remove-reporting-nodes -vserver <vserver_name> -path
<lun_path> -igroup <igroup_name> -remote-nodes
```

7. LUN이 기존 LUN 맵에서 제거되었는지 확인합니다.

```
lun mapping show -fields reporting-nodes
```

8. 호스트 OS의 오래된 디바이스 항목을 제거합니다.
9. 필요한 경우 경로 다중화 구성 파일을 변경합니다.
10. 호스트를 재검색하여 이전 경로가 제거되었는지 확인합니다. + 호스트를 재검색하는 특정 단계는 호스트 설명서를 참조하십시오.

iSCSI 프로토콜을 관리합니다

최상의 성능을 위해 네트워크를 구성합니다

이더넷 네트워크의 성능은 매우 다양합니다. 특정 구성 값을 선택하여 iSCSI에 사용되는 네트워크의 성능을 최대화할 수 있습니다.

단계

1. 호스트 및 스토리지 포트를 동일한 네트워크에 연결합니다.

   동일한 스위치에 연결하는 것이 가장 좋습니다. 라우팅은 절대 사용해서는 안 됩니다.

2. 사용 가능한 최고 속도 포트를 선택하고 iSCSI에 전용으로 지정합니다.

   10GbE 포트가 가장 적합합니다. 1GbE 포트는 최소 포트입니다.

3. 모든 포트에 대해 이더넷 흐름 제어를 사용하지 않도록 설정합니다.

   이 표시됩니다 "네트워크 관리" CLI를 사용하여 이더넷 포트 흐름 제어를 구성하는 데 사용됩니다.

4. 점보 프레임(일반적으로 MTU 9000)을 사용하도록 설정합니다.

   이니시에이터, 타겟 및 스위치를 비롯한 데이터 경로의 모든 디바이스가 점보 프레임을 지원해야 합니다. 그렇지 않으면 점보 프레임이 실제로 네트워크 성능을 크게 줄입니다.

iSCSI용 **SVM**을 구성합니다

iSCSI를 위한 SVM(Storage Virtual Machine)을 구성하려면 SVM용 LIF를 생성하고 이러한 LIF에 iSCSI 프로토콜을 할당해야 합니다.

이 작업에 대해

iSCSI 프로토콜로 데이터를 제공하는 SVM은 노드당 최소 하나의 iSCSI LIF가 필요합니다. 이중화를 위해서는 노드당 LIF를 2개 이상 생성해야 합니다.

예 **20.** 단계

시스템 관리자

ONTAP System Manager(9.7 이상)를 사용하여 iSCSI용 스토리지 VM을 구성합니다.

새 스토리지 **VM**에서 **iSCSI**를 구성합니다	기존 스토리지 **VM**에서 **iSCSI**를 구성합니다
1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭한 다음 * 추가 * 를 클릭합니다. 2. 스토리지 VM의 이름을 입력합니다. 3. 액세스 프로토콜 * 에 대해 * iSCSI * 를 선택합니다. 4. iSCSI 활성화 * 를 클릭하고 네트워크 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. + 각 노드에는 최소 2개의 네트워크 인터페이스가 있어야 합니다. 5. 저장 * 을 클릭합니다.	1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭합니다. 2. 구성할 스토리지 VM을 클릭합니다. 3. 설정 * 탭을 클릭한 다음 iSCSI 프로토콜 옆에 있는 을 클릭합니다. 4. iSCSI 활성화 * 를 클릭하고 네트워크 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. + 각 노드에는 최소 2개의 네트워크 인터페이스가 있어야 합니다. 5. 저장 * 을 클릭합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 iSCSI용 스토리지 VM을 구성합니다.

1. SVM이 iSCSI 트래픽을 수신하도록 설정:

   'vserver iscsi create-vserver_vserver_name_-target-alias_vserver_name_'

2. iSCSI에 사용할 SVM을 위한 LIF를 각 노드에서 생성합니다.
   - ONTAP 9.6 이상:

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol iscsi -service-policy default-data-iscsi -home-node node_name
     -home-port port_name -address ip_address -netmask netmask
     ```

   - ONTAP 9.5 이하:

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol iscsi -home-node node_name -home-port port_name -address
     ip_address -netmask netmask
     ```

3. LIF를 올바르게 설정했는지 확인하십시오.

   'network interface show -vserver_vserver_name_'

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

4. iSCSI가 작동 중이고 해당 SVM의 타겟 IQN이 실행 중인지 확인합니다.

   'vserver iscsi show –vserver_vserver_name_'

5. 호스트에서 LIF에 iSCSI 세션을 생성합니다.

관련 정보

- "NetApp 기술 보고서 4080: 최신 SAN에 대한 모범 사례"

이니시에이터에 대한 보안 정책 방법을 정의합니다

이니시에이터 목록과 해당 인증 방법을 정의할 수 있습니다. 사용자 정의 인증 방법이 없는 이니시에이터에 적용되는 기본 인증 방법을 수정할 수도 있습니다.

이 작업에 대해

제품의 보안 정책 알고리즘을 사용하여 고유한 암호를 생성하거나 사용하려는 암호를 수동으로 지정할 수 있습니다.

일부 이니시에이터는 16진수 CHAP 암호 암호를 지원하지 않습니다.

단계

1. "vserver iSCSI security create" 명령을 사용하여 이니시에이터에 대한 보안 정책 방법을 생성합니다.

   'vserver iscsi security create-vserver vS2-initiator iqn.1991-05.com.microsoft:host1 -auth-type CHAP-user-name byby1-outbound-user-name byby2'

2. 화면 명령에 따라 암호를 추가합니다.

   인바운드 및 아웃바운드 CHAP 사용자 이름 및 암호를 사용하여 초기자 iqn.1991-05.com.microsoft:host1 에 대한 보안 정책 방법을 만듭니다.

관련 정보

- iSCSI 인증의 작동 방식
- CHAP 인증입니다

SVM을 위한 **iSCSI** 서비스를 삭제합니다

더 이상 필요하지 않은 경우 SVM(스토리지 가상 머신)에 대한 iSCSI 서비스를 삭제할 수 있습니다.

시작하기 전에

iSCSI 서비스를 삭제하려면 먼저 iSCSI 서비스의 관리 상태가 "down" 상태여야 합니다. 'vserver iscsi modify' 명령을 사용하여 관리 상태를 아래로 이동할 수 있습니다.

단계

1. 'vserver iscsi modify' 명령을 사용하여 LUN에 대한 입출력을 중지합니다.

   'vserver iscsi modify -vserver vs1-status-admin down'

2. SVM에서 iSCSI 서비스를 제거하려면 "vserver iSCSI delete" 명령을 사용하십시오.

   'vserver iscsi delete - vserver vs_1'

3. SVM에서 iSCSI 서비스를 삭제했는지 확인하려면 'vserver iscsi show 명령'을 사용하십시오.

   'vserver iscsi show -vserver vs1'

iSCSI 세션 오류 복구에 대한 자세한 내용을 확인하십시오

iSCSI 세션 오류 복구 수준을 높이면 iSCSI 오류 복구에 대한 자세한 정보를 얻을 수 있습니다. 높은 오류 복구 레벨을 사용하면 iSCSI 세션 성능이 약간 저하될 수 있습니다.

이 작업에 대해

기본적으로 ONTAP는 iSCSI 세션에 대해 오류 복구 레벨 0을 사용하도록 구성됩니다. 오류 복구 레벨 1 또는 2에 대해 검증된 이니시에이터를 사용하는 경우 오류 복구 레벨을 증가하도록 선택할 수 있습니다. 수정된 세션 오류 복구 수준은 새로 생성된 세션에만 영향을 미치며 기존 세션에는 영향을 미치지 않습니다.

ONTAP 9.4부터 iSCSI show와 iSCSI modify 명령에서는 max-error-recovery-level 옵션이 지원되지 않습니다.

단계

1. 고급 모드 진입:

   세트 프리빌리지 고급

2. "iscsi show" 명령을 사용하여 현재 설정을 확인합니다.

   'iscsi show -vserver vs3 -fields max-error-recovery-level'

```
vserver max-error-recovery-level
------- ------------------------
vs3     0
```

3. iSCSI modify 명령을 사용하여 오류 복구 수준을 변경합니다.

   'iscsi modify -vserver vs3 -max-error-recovery-level 2'

iSNS 서버를 사용하여 **SVM**을 등록합니다

"vserver iSCSI iSNS" 명령을 사용하여 iSNS 서버에 등록할 SVM(스토리지 가상 시스템)을 구성할 수 있습니다.

이 작업에 대해

'vserver iscsi iSNS create' 명령은 iSNS 서버에 등록할 SVM을 구성합니다. SVM은 iSNS 서버를 구성하거나 관리할 수 있는 명령을 제공하지 않습니다. iSNS 서버를 관리하려면 공급업체에서 제공하는 iSNS 서버 관리 도구 또는 인터페이스를 사용할 수 있습니다.

단계

1. iSNS 서버에서 iSNS 서비스가 작동 가능하고 서비스를 사용할 수 있는지 확인합니다.
2. 데이터 포트에 SVM 관리 LIF를 생성합니다.

'network interface create -vserver_SVM_name_-lif_lif_name_-role data-protocol none-home-node_home_node_name_-home-port_home_home_home_port_-address_-netmask_network_mask_'

에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. SVM에 iSCSI 서비스가 없는 경우 생성합니다.

   'vserver iscsi create-vserver_SVM_name_'

4. iSCSI 서비스가 성공적으로 생성되었는지 확인합니다.

   'iscsi show -vserver_SVM_name _'

5. SVM에 대한 기본 경로가 있는지 확인합니다.

   'network route show -vserver_SVM_name _'

6. SVM에 대한 기본 경로가 없는 경우 기본 경로를 생성합니다.

   'network route create-vserver_SVM_name_-destination_destination_-gateway_gateway_'

   에 대한 자세한 내용은 `network route create` "ONTAP 명령 참조입니다"을 참조하십시오.

7. iSNS 서비스에 등록할 SVM을 구성합니다.

   'vserver iSCSI iSNS create -vserver_SVM_name_-address_ip_address_'

   IPv4 및 IPv6 주소 제품군이 모두 지원됩니다. iSNS 서버의 주소 제품군은 SVM 관리 LIF의 주소 제품군과 같아야 합니다.

   예를 들어, IPv6 주소를 사용하여 anSVM 관리 LIF를 IPv4 주소와 함께 iSNS 서버에 연결할 수 없습니다.

8. iSNS 서비스가 실행 중인지 확인합니다.

   'vserver iscsi iSNS show -vserver_SVM_name _'

9. iSNS 서비스가 실행되고 있지 않으면 다음을 시작합니다.

   'vserver iscsi iSNS start -vserver_SVM_name_'

스토리지 시스템의 **iSCSI** 오류 메시지를 해결합니다

'event log show' 명령을 사용하여 볼 수 있는 일반적인 iSCSI 관련 오류 메시지가 많이 있습니다. 이러한 메시지의 의미와 해당 메시지가 파악한 문제를 해결하기 위해 수행할 수 있는 작업을 알고 있어야 합니다.

다음 표에는 가장 일반적인 오류 메시지와 해결 지침이 나와 있습니다.

메시지	설명	할 일
'iSCSI: 네트워크 인터페이스 식별자 사용 안 함, 들어오는 연결이 삭제됨'	인터페이스에서 iSCSI 서비스가 활성화되어 있지 않습니다.	"iSCSI interface enable" 명령을 사용하여 인터페이스에서 iSCSI 서비스를 활성화할 수 있습니다. 예를 들면 다음과 같습니다. 'iSCSI interface enable - vserver vs1-lif lif liff li1'
"iSCSI: 이니시에이터 노데이름 인증에 실패했습니다.	지정된 이니시에이터에 대해 CHAP가 올바르게 구성되지 않았습니다.	CHAP 설정을 확인해야 합니다. 스토리지 시스템의 인바운드 및 아웃바운드 설정에 동일한 사용자 이름과 암호를 사용할 수 없습니다. • 스토리지 시스템의 인바운드 자격 증명은 이니시에이터의 아웃바운드 자격 증명과 일치해야 합니다. • 스토리지 시스템의 아웃바운드 자격 증명은 이니시에이터의 인바운드 자격 증명과 일치해야 합니다.

에 대한 자세한 내용은 `event log show` "ONTAP 명령 참조입니다"을 참조하십시오.

자동 **iSCSI LIF** 페일오버를 사용 또는 사용하지 않도록 설정합니다

ONTAP 9.11.1 이상으로 업그레이드한 후에는 ONTAP 9.10.1 이전 버전에서 생성된 모든 iSCSI LIF에서 자동 LIF 페일오버를 수동으로 사용하도록 설정해야 합니다.

ONTAP 9.11.1부터 All-Flash SAN 어레이 플랫폼에서 iSCSI LIF에 대한 자동 LIF 페일오버를 활성화할 수 있습니다. 스토리지 페일오버가 발생하는 경우 iSCSI LIF가 홈 노드나 포트에서 HA 파트너 노드 또는 포트로 자동으로 마이그레이션된 다음, 페일오버가 완료되면 다시 뒤로 마이그레이션됩니다. 또는 iSCSI LIF의 포트가 정상 상태가 아닐 경우 LIF는 자동으로 현재 홈 노드의 정상 포트로 마이그레이션된 다음, 포트가 다시 정상 상태가 되면 원래 포트로 다시 돌아갑니다. 를 사용하면 iSCSI에서 실행되는 SAN 워크로드가 페일오버가 발생한 후 I/O 서비스를 더 빠르게 재개할 수 있습니다.

ONTAP 9.11.1 이상에서는 기본적으로 새로 생성된 iSCSI LIF가 다음 조건 중 하나에 해당할 경우 자동 LIF 페일오버에 사용하도록 설정됩니다.

- SVM에 iSCSI LIF가 없습니다
- SVM의 모든 iSCSI LIF는 자동 LIF 페일오버에 사용할 수 있습니다

자동 **iSCSI LIF** 페일오버를 사용합니다

기본적으로 ONTAP 9.10.1 이전 버전에서 생성된 iSCSI LIF는 자동 LIF 페일오버에 사용되지 않습니다. 자동 LIF 페일오버에 사용되지 않는 SVM에 iSCSI LIF가 있으면 새로 생성한 LIF가 자동 LIF 페일오버 중에 사용할 수 없습니다. 자동 LIF 페일오버가 사용되도록 설정되어 있지 않고 페일오버 이벤트가 발생하면 iSCSI LIF가 마이그레이션되지 않습니다.

에 대해 자세히 "LIF 페일오버 및 반환"알아보십시오.

단계

1. iSCSI LIF에 대해 자동 페일오버 활성화:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy sfo-partner-only -auto-revert true
```

SVM에서 모든 iSCSI LIF를 업데이트하려면 를 사용하십시오 `-lif*` 대신 `lif`.

자동 **iSCSI LIF** 페일오버를 해제합니다

이전에 ONTAP 9.10.1 이하 버전에서 생성된 iSCSI LIF에서 자동 iSCSI LIF 페일오버를 사용하도록 설정한 경우 이 기능을 사용하지 않도록 설정할 수 있습니다.

단계

1. iSCSI LIF에 대한 자동 페일오버 비활성화:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy disabled -auto-revert false
```

SVM에서 모든 iSCSI LIF를 업데이트하려면 를 사용하십시오 `-lif*` 대신 `lif`.

관련 정보

- "LIF를 생성합니다"
- 수동 "LIF를 마이그레이션합니다"
- 수동 "LIF를 홈 포트로 되돌립니다"
- "LIF에서 페일오버 설정을 구성합니다"

FC 프로토콜을 관리합니다

FC용 SVM 구성

FC용 SVM(Storage Virtual Machine)을 구성하려면 SVM용 LIF를 생성하고 이러한 LIF에 FC 프로토콜을 할당해야 합니다.

시작하기 전에

FC 라이센스("ONTAP One에 포함되어 있습니다")가 있어야 하며 활성화해야 합니다. FC 라이센스가 활성화되지 않으면 LIF 및 SVM이 온라인 상태로 표시되지만 운영 상태는 입니다. `down` LIF 및 SVM이 작동할 수 있도록 FC 서비스를 설정해야 합니다. SVM의 모든 FC LIF에서 이니시에이터를 호스팅하려면 단일 이니시에이터 조닝을 사용해야 합니다.

이 작업에 대해

NetApp은 각 SVM에서 FC 프로토콜을 통해 데이터를 제공하는 FC LIF를 노드당 1개 이상 지원합니다. 노드당 LIF

2개와 Fabric 2개를 사용해야 하며, 연결된 노드당 LIF 1개가 있어야 합니다. 이는 노드 계층과 패브릭에서 이중화를 제공합니다.

예 **21.** 단계

시스템 관리자

ONTAP System Manager(9.7 이상)를 사용하여 iSCSI용 스토리지 VM을 구성합니다.

새 스토리지 **VM**에서 **FC**를 구성합니다	기존 스토리지 **VM**에서 **FC**를 구성합니다
1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭한 다음 * 추가 * 를 클릭합니다. 2. 스토리지 VM의 이름을 입력합니다. 3. 액세스 프로토콜 * 으로 * FC * 를 선택합니다. 4. FC * 활성화 를 클릭합니다. + FC 포트가 자동으로 할당됩니다. 5. 저장 * 을 클릭합니다.	1. System Manager에서 * 스토리지 > 스토리지 VM * 을 클릭합니다. 2. 구성할 스토리지 VM을 클릭합니다. 3. 설정 * 탭을 클릭한 다음 FC 프로토콜 옆에 있는 을 클릭합니다 . 4. FC * 활성화 를 클릭하고 네트워크 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. + FC 포트가 자동으로 할당됩니다. 5. 저장 * 을 클릭합니다.

CLI를 참조하십시오

1. SVM에서 FC 서비스 활성화:

   'vserver fcp create-vserver_vserver_name_-status-admin up'

2. FC를 지원하는 각 노드에서 SVM에 대해 2개의 LIF를 생성합니다.
   - ONTAP 9.6 이상:

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol fcp -service-policy default-data-fcp -home-node node_name
     -home-port port_name -address ip_address -netmask netmask -status-admin
     up
     ```

   - ONTAP 9.5 이하:

     'network interface create-vserver_vserver_name_-lif_lif_name_-role data-protocol fcp-home-node_node_name_-home-port_port_'

3. LIF가 생성되었으며 운영 상태가 '온라인'인지 확인합니다.

   'network interface show -vserver_vserver_name__lif_name_'

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "NetApp 지원"

- "NetApp 상호 운용성 매트릭스 툴"
- 클러스터 SAN 환경의 LIF 고려 사항

SVM을 위한 FC 서비스를 삭제합니다

더 이상 필요하지 않은 경우 SVM(스토리지 가상 머신)에 대한 FC 서비스를 삭제할 수 있습니다.

시작하기 전에

SVM에 대한 FC 서비스를 삭제하려면 관리 상태가 "자체"여야 합니다. 'vserver fcp modify' 명령 또는 'vserver fcp stop' 명령을 사용하여 관리 상태를 down으로 설정할 수 있습니다.

단계

1. 'vserver FCP stop' 명령을 사용하여 LUN에 대한 입출력을 중지합니다.

   'vserver fcp stop-vserver vs_1'

2. SVM에서 서비스를 제거하려면 'vserver FCP delete' 명령을 사용하십시오.

   'vserver fcp delete-vserver vs_1'

3. SVM에서 FC 서비스를 삭제했는지 확인하려면 'vserver FCP show'를 사용하십시오.

   'vserver fcp show -vserver vs_1'

FCoE 점보 프레임에 대한 권장 MTU 구성

FCoE(Fibre Channel over Ethernet)의 경우 CNA의 이더넷 어댑터 부분에 대한 점보 프레임을 9000 MTU로 구성해야 합니다. CNA의 FCoE 어댑터 부분에 대한 점보 프레임은 1500 MTU 이상으로 구성해야 합니다. 이니시에이터, 타겟 및 모든 중재 스위치가 점보 프레임을 지원하고 점보 프레임에 맞게 구성된 경우에만 점보 프레임을 구성합니다.

NVMe 프로토콜 관리

SVM을 위한 NVMe 서비스를 시작합니다

스토리지 가상 시스템(SVM)에서 NVMe 프로토콜을 사용하려면 먼저 SVM에서 NVMe 서비스를 시작해야 합니다.

시작하기 전에

NVMe는 시스템에서 프로토콜로 허용되어야 합니다.

지원되는 NVMe 프로토콜은 다음과 같습니다.

프로토콜	다음으로 시작…	허용된 사용자…
TCP	ONTAP 9.10.1	기본값
FCP	ONTAP 9.4	기본값

단계

1. 권한 설정을 고급으로 변경합니다.

   세트 프리빌리지 고급

2. NVMe가 프로토콜로 허용되는지 확인합니다.

   'vserver NVMe show'

3. NVMe 프로토콜 서비스를 생성합니다.

   'vserver NVMe create

4. SVM에서 NVMe 프로토콜 서비스를 시작합니다.

   'vserver NVMe modify-status-admin up'을 선택합니다

SVM에서 **NVMe** 서비스를 삭제합니다

필요한 경우 스토리지 가상 시스템(SVM)에서 NVMe 서비스를 삭제할 수 있습니다.

단계

1. 권한 설정을 고급으로 변경합니다.

   세트 프리빌리지 고급

2. SVM에서 NVMe 서비스를 중지합니다.

   'vserver NVMe modify-status-admin down'

3. NVMe 서비스를 삭제합니다.

   'vserver NVMe delete

네임스페이스 크기 조정

ONTAP 9.10.1부터 ONTAP CLI를 사용하여 NVMe 네임스페이스의 크기를 늘리거나 줄일 수 있습니다. System Manager를 사용하여 NVMe 네임스페이스의 크기를 늘릴 수 있습니다.

네임스페이스의 크기를 늘립니다

시스템 관리자

1. 스토리지 > NVMe 네임스페이스 * 를 클릭합니다.
2. 늘릴 네임스페이스를 마우스 오른쪽 단추로 클릭한 다음 * 편집 * 을 클릭합니다.
3. capacity * 에서 네임스페이스의 크기를 변경합니다.

CLI를 참조하십시오

1. 'vserver NVMe namespace modify -vserver_SVM_name_-path_path_ –size_new_size_of_namespace_' 명령을 입력합니다

네임스페이스의 크기를 줄입니다

ONTAP CLI를 사용하여 NVMe 네임스페이스의 크기를 줄여야 합니다.

1. 권한 설정을 고급으로 변경합니다.

   '세트-프리빌리지 어드밴스드'

2. 네임스페이스 크기 축소:

   'vserver NVMe namespace modify -vserver_SVM_name_-path_namespace_path_ -size_new_size_of_namespace_'

네임스페이스를 **LUN**으로 변환합니다

ONTAP 9.11.1부터는 ONTAP CLI를 사용하여 데이터 이동 없이 기존 NVMe 네임스페이스를 LUN으로 변환할 수 있습니다.

시작하기 전에

- 지정된 NVMe 네임스페이스에는 하위 시스템에 대한 기존 맵이 없어야 합니다.
- 네임스페이스가 스냅샷의 일부이거나 SnapMirror 관계의 대상 측에 읽기 전용 네임스페이스로 있어서는 안 됩니다.
- NVMe 네임스페이스는 특정 플랫폼 및 네트워크 카드에서만 지원되므로 이 기능은 특정 하드웨어에서만 작동합니다.

단계

1. 다음 명령을 입력하여 NVMe 네임스페이스를 LUN으로 변환합니다.

   'LUN convert-from-namespace-vserver-namespace-path'

   에 대한 자세한 내용은 `lun convert-from-namespace` "ONTAP 명령 참조입니다"을 참조하십시오.

NVMe를 통해 대역 내 인증을 설정합니다

ONTAP 9.12.1부터 ONTAP CLI(명령줄 인터페이스)를 사용하여 DH-HMAC-CHAP 인증을 사용하여 NVMe/TCP 및 NVMe/FC 프로토콜을 통해 NVMe 호스트와 컨트롤러 간에 대역 내(보안), 양방향 및 단방향 인증을 구성할 수 있습니다. ONTAP 9.14.1부터 System

Manager에서 대역 내 인증을 구성할 수 있습니다.

대역내 인증을 설정하려면 각 호스트 또는 컨트롤러가 NVMe 호스트 또는 컨트롤러의 NQN 및 관리자가 구성한 인증 비밀의 조합인 DH-HMAC-CHAP 키와 연결되어야 합니다. NVMe 호스트 또는 컨트롤러가 해당 피어를 인증하려면 피어와 연결된 키를 알고 있어야 합니다.

단방향 인증에서는 호스트에 대해 암호 키가 구성되지만 컨트롤러는 구성되지 않습니다. 양방향 인증에서 비밀 키는 호스트와 컨트롤러 모두에 대해 구성됩니다.

SHA-256은 기본 해시 함수이고 2048비트는 기본 DH 그룹입니다.

시스템 관리자

ONTAP 9.14.1부터는 System Manager를 사용하여 NVMe 서브시스템을 생성 또는 업데이트하고, NVMe 네임스페이스를 생성 또는 클론 복제하며, 새로운 NVMe 네임스페이스로 일관성 그룹을 추가하는 동안 대역 내 인증을 구성할 수 있습니다.

단계

1. System Manager에서 * Hosts > NVMe Subsystem * 을 클릭하고 * Add * 를 클릭합니다.
2. NVMe 서브시스템 이름을 추가하고 스토리지 VM 및 호스트 운영 체제를 선택합니다.
3. 호스트 NQN을 입력합니다.
4. 호스트 NQN 옆에 있는 * Use in-band authentication * 을 선택합니다.
5. 호스트 암호 및 컨트롤러 암호를 제공합니다.

   DH-HMAC-CHAP 키는 NVMe 호스트 또는 컨트롤러의 NQN과 관리자가 구성한 인증 비밀의 조합입니다.
6. 각 호스트에 대해 선호하는 해시 기능과 DH 그룹을 선택합니다.

   해시 함수와 DH 그룹을 선택하지 않으면 SHA-256이 기본 해시 함수로 할당되고 2048비트가 기본 DH 그룹으로 할당됩니다.
7. 선택적으로 * Add * 를 클릭하고 필요에 따라 단계를 반복하여 호스트를 추가합니다.
8. 저장 * 을 클릭합니다.
9. 대역 내 인증이 활성화되어 있는지 확인하려면 * System Manager > Hosts > NVMe Subsystem > Grid > Peek view * 를 클릭합니다.

   호스트 이름 옆에 투명한 키 아이콘은 단방향 모드가 설정되어 있음을 나타냅니다. 호스트 이름 옆의 불투명 키는 양방향 모드가 활성화되었음을 나타냅니다.

CLI를 참조하십시오

단계

1. DH-HMAC-CHAP 인증을 NVMe 하위 시스템에 추가합니다.

   ```
   vserver nvme subsystem host add -vserver <svm_name> -subsystem
   <subsystem> -host-nqn <host_nqn> -dhchap-host-secret
   <authentication_host_secret> -dhchap-controller-secret
   <authentication_controller_secret> -dhchap-hash-function <sha-
   256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
   bit|8192-bit>
   ```

   에 대한 자세한 내용은 `vserver nvme subsystem host add` "ONTAP 명령 참조입니다"을 참조하십시오.
2. DH-HMAC CHAP 인증 프로토콜이 호스트에 추가되었는지 확인합니다.

```
vserver nvme subsystem host show
```

```
  [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
  [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
  [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

에 대한 자세한 내용은 `vserver nvme subsystem host show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. NVMe 컨트롤러 생성 중에 DH-HMAC CHAP 인증이 수행되었는지 확인합니다.

```
vserver nvme subsystem controller show
```

```
 [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
 [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
 [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

관련 정보

- "vserver nvme 서브시스템 컨트롤러 표시"

NVMe를 통한 대역 내 인증을 비활성화합니다

DH-HMAC-CHAP를 사용하여 NVMe를 통해 대역 내 인증을 구성한 경우 언제든지 비활성화할 수 있습니다.

ONTAP 9.12.1 이상에서 ONTAP 9.12.0 이하로 되돌리는 경우 되돌리기 전에 대역내 인증을 비활성화해야 합니다. DH-HMAC-CHAP를 사용한 대역내 인증이 해제되지 않은 경우 되돌리기가 실패합니다.

단계

1. DH-HMAC-CHAP 인증을 비활성화하려면 서브시스템에서 호스트를 제거합니다.

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. DH-HMAC-CHAP 인증 프로토콜이 호스트에서 제거되었는지 확인합니다.

```
vserver nvme subsystem host show
```

3. 인증 없이 호스트를 하위 시스템에 다시 추가합니다.

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

NVMe/TCP에 대한 **TLS** 보안 채널을 설정합니다

ONTAP 9.16.1 버전부터 NVMe/TCP 연결에 대해 TLS 보안 채널을 구성할 수 있습니다. 시스템 관리자 또는 ONTAP CLI를 사용하여 TLS가 활성화된 새 NVMe 서브시스템을 추가하거나 기존 NVMe 서브시스템에 대해 TLS를 활성화할 수 있습니다. ONTAP TLS 하드웨어 오프로드를 지원하지 않습니다.

시스템 관리자

ONTAP 9.16.1부터는 System Manager를 사용하여 NVMe 서브시스템을 생성 또는 업데이트하거나, NVMe 네임스페이스를 생성 또는 복제하거나, 새로운 NVMe 네임스페이스로 일관성 그룹을 추가하는 동안 NVMe/TCP 연결용 TLS를 구성할 수 있습니다.

단계

1. System Manager에서 * Hosts > NVMe Subsystem * 을 클릭하고 * Add * 를 클릭합니다.
2. NVMe 서브시스템 이름을 추가하고 스토리지 VM 및 호스트 운영 체제를 선택합니다.
3. 호스트 NQN을 입력합니다.
4. 호스트 NQN 옆에 있는 * 전송 계층 보안(TLS) 필요 * 를 선택합니다.
5. 사전 공유 키(PSK)를 제공합니다.
6. 저장 * 을 클릭합니다.
7. TLS 보안 채널이 활성화되어 있는지 확인하려면 * System Manager > 호스트 > NVMe 하위 시스템 > 그리드 > Peek view * 를 선택합니다.

CLI를 참조하십시오

단계

1. TLS 보안 채널을 지원하는 NVMe 서브시스템 호스트를 추가합니다. 다음을 사용하여 사전 공유 키(PSK)를 제공할 수 있습니다. `tls-configured-psk` 논쟁:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-configured-psk <key_text>
```

2. NVMe 서브시스템 호스트가 TLS 보안 채널에 대해 구성되어 있는지 확인합니다. 선택적으로 인수를 사용하여 해당 키 유형을 사용하는 호스트만 표시할 수 `tls-key-type` 있습니다.

```
vserver nvme subsystem host show -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-key-type {none|configured}
```

3. NVMe 서브시스템 호스트 컨트롤러가 TLS 보안 채널에 대해 구성되어 있는지 확인합니다. 선택적으로, `tls-identity` 또는 `tls-cipher` 인수를 사용하여 해당 TLS 특성이 있는 컨트롤러만 표시할 수 있습니다 `tls-key-type`.

```
vserver nvme subsystem controller show -vserver <svm_name>
-subsystem <subsystem> -host-nqn <host_nqn> -tls-key-type
{none|configured} -tls-identity <text> -tls-cipher
{none|TLS_AES_128_GCM_SHA256|TLS_AES_256_GCM_SHA384}
```

관련 정보

- "SVM NVMe 서브시스템"

NVMe/TCP에 대한 **TLS** 보안 채널을 비활성화합니다

ONTAP 9.16.1부터, NVMe/TCP 연결을 위해 TLS 보안 채널을 구성할 수 있습니다. NVMe/TCP 연결을 위해 TLS 보안 채널을 구성한 경우 언제든지 사용하지 않도록 설정할 수 있습니다.

단계

1. TLS 보안 채널을 비활성화하려면 서브시스템에서 호스트를 제거합니다.

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. TLS 보안 채널이 호스트에서 제거되었는지 확인합니다.

```
vserver nvme subsystem host show
```

3. TLS 보안 채널이 없는 서브시스템에 호스트를 다시 추가합니다.

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

관련 정보

- "SVM NVMe 서브시스템 호스트"

NVMe 호스트 우선순위를 변경합니다

ONTAP 9.14.1부터 특정 호스트에 대한 리소스 할당의 우선순위를 지정하도록 NVMe 서브시스템을 구성할 수 있습니다. 기본적으로 호스트가 서브시스템에 추가되면 보통 우선순위가 할당됩니다. 높은 우선 순위가 할당된 호스트에는 더 큰 입출력 대기열 수와 대기열 깊이가 할당됩니다.

ONTAP CLI(명령줄 인터페이스)를 사용하여 기본 우선 순위를 보통에서 높음으로 수동으로 변경할 수 있습니다. 호스트에 할당된 우선 순위를 변경하려면 하위 시스템에서 호스트를 제거한 다음 다시 추가해야 합니다.

단계

1. 호스트 우선 순위가 Regular로 설정되어 있는지 확인합니다.

```
vserver nvme show-host-priority
```

에 대한 자세한 내용은 `vserver nvme show-host-priority` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 서브시스템에서 호스트 제거:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

에 대한 자세한 내용은 `vserver nvme subsystem host remove` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 호스트가 서브시스템에서 제거되었는지 확인합니다.

```
vserver nvme subsystem host show
```

에 대한 자세한 내용은 `vserver nvme subsystem host show` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 우선 순위가 높은 하위 시스템에 호스트를 다시 추가합니다.

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
-priority high
```

에 대한 자세한 내용은 `vserver nvme subsystem host add` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP에서 NVMe/TCP 컨트롤러의 자동화된 호스트 검색을 관리합니다

ONTAP 9.14.1부터는 IP 기반 패브릭에서 NVMe/TCP 프로토콜을 사용하여 컨트롤러의 호스트 검색이 기본적으로 자동화됩니다.

NVMe/TCP 컨트롤러의 자동화된 호스트 검색 지원

이전에 자동 호스트 검색을 사용하지 않도록 설정했지만 필요한 사항이 변경된 경우 다시 사용하도록 설정할 수 있습니다.

단계

1. 고급 권한 모드 시작:

```
set -privilege advanced
```

2. 자동 검색 사용:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled true
```

3. NVMe/TCP 컨트롤러의 자동화된 검색이 활성화되었는지 확인합니다.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

NVMe/TCP 컨트롤러의 자동화된 호스트 검색을 사용하지 않도록 설정합니다

호스트에서 NVMe/TCP 컨트롤러를 자동으로 검색할 필요가 없고 네트워크에서 원치 않는 멀티캐스트 트래픽을 감지한 경우 이 기능을 비활성화해야 합니다.

단계

1. 고급 권한 모드 시작:

```
set -privilege advanced
```

2. 자동 검색 사용 안 함:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled false
```

3. NVMe/TCP 컨트롤러의 자동 검색이 비활성화되었는지 확인합니다.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

ONTAP에서 **NVMe** 호스트 가상 머신 식별자를 비활성화합니다

ONTAP 9.14.1부터 기본적으로 ONTAP는 NVMe/FC 호스트의 기능을 지원하여 고유 식별자로 가상 머신을 식별하고 NVMe/FC 호스트에서 가상 머신 리소스 활용률을 모니터링할 수 있도록 합니다. 또한 호스트측 보고 및 문제 해결이 향상됩니다.

bootarg를 사용하여 이 기능을 비활성화할 수 있습니다. 를 참조하십시오"NetApp 기술 자료: ONTAP 에서 NVMe 호스트 가상 머신 식별자를 비활성화하는 방법" .

FC 어댑터를 사용하여 시스템을 관리합니다

FC 어댑터를 사용하여 시스템을 관리합니다

온보드 FC 어댑터 및 FC 어댑터 카드를 관리하는 데 사용할 수 있는 명령입니다. 이러한 명령을 사용하여 어댑터 모드를 구성하고 어댑터 정보를 표시하며 속도를 변경할 수 있습니다.

대부분의 스토리지 시스템에는 이니시에이터 또는 타겟으로 구성할 수 있는 온보드 FC 어댑터가 있습니다. 또한, 이니시에이터 또는 타겟으로 구성된 FC 어댑터 카드를 사용할 수도 있습니다. 개시자는 백엔드 디스크 셸프와 연결되고, 외부 스토리지 어레이에도 연결될 수 있습니다. 타겟은 FC 스위치에만 연결됩니다. FC 대상 HBA 포트와 스위치 포트 속도는 모두 동일한 값으로 설정해야 하며 자동으로 설정하면 안 됩니다.

관련 정보

"SAN 구성"

FC 어댑터를 관리하는 명령입니다

FC 명령을 사용하여 스토리지 컨트롤러에 대한 FC 타겟 어댑터, FC 이니시에이터 어댑터 및 온보드 FC 어댑터를 관리할 수 있습니다. FC 프로토콜과 FC-NVMe 프로토콜을 위해 FC 어댑터를 관리하는 데 동일한 명령이 사용됩니다.

FC 이니시에이터 어댑터 명령은 노드 레벨에서만 작동합니다. FC Initiator Adapter 명령을 사용하려면 먼저 'run-node_node_name_' 명령을 사용해야 합니다.

FC 타겟 어댑터를 관리하는 명령입니다

원하는 작업	이 명령 사용...
노드에 FC 어댑터 정보를 표시합니다	네트워크 FCP 어댑터가 표시됩니다
FC 타겟 어댑터 매개 변수를 수정합니다	네트워크 FCP 어댑터 수정
FC 프로토콜 트래픽 정보를 표시합니다	'run-node_node_name_sysstat -f'
FC 프로토콜이 실행된 시간을 표시합니다	'run-node_node_name_uptime'
어댑터 구성 및 상태를 표시합니다	'run-node_node_name_sysconfig-v_adapter_'
설치된 확장 카드와 구성 오류가 있는지 확인합니다	'run-node_node_name_sysconfig-ac'
명령에 대한 man 페이지를 봅니다	`man <command_name>`

FC 이니시에이터 어댑터를 관리하는 명령입니다

원하는 작업	이 명령 사용...
노드의 모든 이니시에이터 및 해당 어댑터에 대한 정보를 표시합니다	'run-node_node_name_storage show adapter'입니다
어댑터 구성 및 상태를 표시합니다	'run-node_node_name_sysconfig-v_adapter_'
설치된 확장 카드와 구성 오류가 있는지 확인합니다	'run-node_node_name_sysconfig-ac'

온보드 **FC** 어댑터를 관리하는 명령입니다

원하는 작업	이 명령 사용...
온보드 FC 포트의 상태를 표시합니다	'run-node_node_name_system hardware unified-connect show

관련 정보

- "네트워크 FCP 어댑터"

FC 어댑터를 구성합니다

각 온보드 FC 포트는 이니시에이터 또는 타겟으로 개별적으로 구성할 수 있습니다. 특정 FC 어댑터의 포트는 온보드 FC 포트와 마찬가지로 타겟 포트 또는 이니시에이터 포트로 개별적으로 구성할 수도 있습니다. 대상 모드에 대해 구성할 수 있는 어댑터 목록은 에서 확인할 수 있습니다 "NetApp Hardware Universe를 참조하십시오".

타겟 모드는 포트를 FC 이니시에이터에 연결하는 데 사용됩니다. 이니시에이터 모드는 외부 LUN 가져오기(FLI)를 통해 포트를 테이프 드라이브, 테이프 라이브러리 또는 타사 스토리지에 연결하는 데 사용됩니다.

FC 프로토콜과 FC-NVMe 프로토콜을 위해 FC 어댑터를 구성할 때도 동일한 단계가 사용됩니다. 하지만 특정 FC 어댑터만 FC-NVMe를 지원합니다. 를 참조하십시오 "NetApp Hardware Universe를 참조하십시오" FC-NVMe 프로토콜을 지원하는 어댑터 목록을 확인하십시오.

FC 어댑터를 타겟 모드로 구성합니다

단계

1. 어댑터를 오프라인 상태로 전환:

   'node run-node_node_name_storage disable adapter_adapter_name_'

   어댑터가 오프라인 상태가 되지 않으면 시스템의 해당 어댑터 포트에서 케이블을 분리할 수도 있습니다.

2. 어댑터를 이니시에이터에서 타겟으로 변경합니다.

   'system hardware unified-connect modify -t target-node_node_name_adapter_adapter_name_'

3. 변경한 어댑터를 호스팅하는 노드를 재부팅합니다.
4. 타겟 포트의 구성이 올바른지 확인합니다.

   'network fcp adapter show-node_name _'

   에 대한 자세한 내용은 `network fcp adapter show` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 어댑터를 온라인으로 전환합니다.

   'network fcp adapter modify -node_node_name_-adapter_adapter_port_-state up

이니시에이터 모드에 맞게 **FC** 어댑터를 구성합니다

시작하기 전에

- 어댑터에 있는 LIF는 해당 LIF가 구성원인 포트 세트에서 제거해야 합니다.
- 물리적 포트의 속성을 타겟에서 이니시에이터로 변경하기 전에 수정할 물리적 포트를 사용하는 모든 SVM(스토리지 가상 머신)의 모든 LIF를 마이그레이션 또는 제거해야 합니다.

NVMe/FC는 이니시에이터 모드를 지원합니다.

단계

1. 어댑터에서 모든 LIF를 제거합니다.

   '네트워크 인터페이스 삭제 - vserver_SVM_name_-lif_LIF_name, LIF_name_'

   에 대한 자세한 내용은 `network interface delete` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 어댑터를 오프라인 상태로 전환:

   'network fcp adapter modify -node_node_name_-adapter_adapter_port_-status-admin down'

   어댑터가 오프라인 상태가 되지 않으면 시스템의 해당 어댑터 포트에서 케이블을 분리할 수도 있습니다.

3. 어댑터를 타겟에서 이니시에이터로 변경합니다.

   'System hardware unified-connect modify -t initiator_adapter_port_

4. 변경한 어댑터를 호스팅하는 노드를 재부팅합니다.
5. FC 포트가 구성에 맞는 올바른 상태로 구성되었는지 확인합니다.

   '시스템 하드웨어 통합 접속 쇼

6. 어댑터를 다시 온라인으로 전환합니다.

   'node run-node_node_name_storage enable adapter_adapter_port_'

어댑터 설정을 봅니다

특정 명령을 사용하여 FC/UTA 어댑터에 대한 정보를 볼 수 있습니다.

FC 타겟 어댑터

단계

1. 네트워크 FCP 어댑터 show 명령을 사용하여 어댑터 정보를 표시합니다. 네트워크 FCP 어댑터 show-instance-node node1-adapter 0a

   출력에는 사용되는 각 슬롯의 시스템 구성 정보와 어댑터 정보가 표시됩니다.

   에 대한 자세한 내용은 `network fcp adapter show` "ONTAP 명령 참조입니다"을 참조하십시오.

UTA(Unified Target Adapter) X1143A-R6

단계

1. 케이블을 연결하지 않고 컨트롤러를 부팅합니다.
2. 'system hardware unified-connect show' 명령어를 실행하여 포트 구성 및 모듈을 확인할 수 있다.
3. CNA 및 포트를 구성하기 전에 포트 정보를 확인합니다.

UTA2 포트를 **CNA** 모드에서 **FC** 모드로 변경합니다

UTA2 포트를 CNA(Converged Network Adapter) 모드에서 FC(Fibre Channel) 모드로 변경하여 FC 이니시에이터 및 FC 타겟 모드를 지원해야 합니다. 포트를 네트워크에 연결하는 물리적 미디어를 변경해야 하는 경우 CNA 모드에서 FC 모드로 속성을 변경해야 합니다.

단계

1. 어댑터를 오프라인 상태로 전환:

   'network fcp adapter modify -node_node_name_-adapter_adapter_name_-status-admin down'

2. 포트 모드를 변경합니다.

   'ucadmin modify -node_node_name_-adapter_adapter_name_-mode fcp'

3. 노드를 재부팅한 다음 어댑터를 온라인 상태로 전환합니다.

   'network fcp adapter modify -node_node_name_-adapter_adapter_name_-status-admin up

4. 필요에 따라 관리자 또는 VIF 관리자에게 포트를 삭제하거나 제거하도록 알립니다.

   - 포트가 LIF의 홈 포트로 사용되고, 인터페이스 그룹(ifgrp) 또는 호스트 VLAN의 구성원인 경우 관리자는 다음을 수행해야 합니다.

     i. LIF를 이동하거나, ifgrp에서 포트를 제거하거나, VLAN을 각각 삭제합니다.

     ii. 'network port delete' 명령어를 실행해 포트를 수동으로 삭제한다.

     'network port delete' 명령이 실패하면 관리자가 오류를 해결한 다음 명령을 다시 실행해야 합니다.

     에 대한 자세한 내용은 `network port delete` "ONTAP 명령 참조입니다"을 참조하십시오.

   - 포트가 LIF의 홈 포트로 사용되지 않고, ifgrp의 구성원이 아니며 VLAN을 호스팅하지 않는 경우, VIF 관리자는 재부팅 시 기록에서 포트를 제거해야 합니다.

     VIF 관리자가 포트를 제거하지 않는 경우, 관리자는 재부팅 후 'network port delete' 명령을 사용하여 수동으로 제거해야 합니다.

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                                  Speed(Mbps)
Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
    --------- ------------ ---------------- ---- ---- -----------
```

```
--------
    ...
    e0i       Default      Default          down 1500  auto/10    -
    e0f       Default      Default          down 1500  auto/10    -
    ...

    net-f8040-34::> ucadmin show
                               Current  Current    Pending  Pending
Admin
    Node            Adapter   Mode     Type       Mode     Type
Status
    ------------    -------   -------  ---------  -------  ---------
-----------
    net-f8040-34-01   0e       cna      target     -        -
offline
    net-f8040-34-01   0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0


    net-f8040-34::> network interface show -fields home-port, curr-
port

    vserver lif                     home-port curr-port
    ------- --------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt          e0M       e0M
    net-f8040-34
            m                     e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed
to fc.
```

```
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y
```

에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 올바른 SFP+가 설치되었는지 확인합니다.

   네트워크 FCP 어댑터 show-instance-node-adapter입니다

   CNA의 경우 10Gb 이더넷 SFP를 사용해야 합니다. FC의 경우 노드에서 구성을 변경하기 전에 8Gb SFP 또는 16Gb SFP를 사용해야 합니다.

   에 대한 자세한 내용은 `network fcp adapter show` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "네트워크 인터페이스"

CNA/UTA2 타겟 어댑터 광 모듈을 변경합니다

어댑터에 대해 선택한 퍼스낼리티 모드를 지원하도록 유니파이드 타겟 어댑터(CNA/UTA2)의 광 모듈을 변경해야 합니다.

단계

1. 카드에 사용된 현재 SFP+를 확인합니다. 그런 다음 기본 설정 특성(FC 또는 CNA)에 대해 현재 SFP+를 적절한 SFP+로 교체합니다.
2. X1143A-R6 어댑터에서 현재 광 모듈을 제거합니다.
3. 기본 퍼스낼리티 모드(FC 또는 CNA) 광학장치에 맞는 모듈을 삽입합니다.
4. 올바른 SFP+가 설치되었는지 확인합니다.

   네트워크 FCP 어댑터 show-instance-node-adapter입니다

   지원되는 SFP+ 모듈 및 Cisco Twinax(Copper) 케이블은 _Hardware Universe_에 나열되어 있습니다.

관련 정보

- "NetApp Hardware Universe를 참조하십시오"
- "네트워크 FCP 어댑터가 표시됩니다"

X1143A-R6 어댑터에 대해 지원되는 포트 구성

FC 타겟 모드는 X1143A-R6 어댑터 포트의 기본 구성입니다. 하지만 이 어댑터의 포트는 10Gb 이더넷 및 FCoE 포트 또는 16Gb FC 포트로 구성할 수 있습니다.

이더넷 및 FCoE용으로 구성된 경우 X1143A-R6 어댑터는 동일한 10GbE 포트에서 동시 NIC 및 FCoE 타겟 트래픽을 지원합니다. FC용으로 구성한 경우 동일한 ASIC를 공유하는 각 2포트 쌍은 FC 타겟 또는 FC 이니시에이터 모드에 대해 개별적으로 구성할 수 있습니다. 즉, 단일 X1143A-R6 어댑터는 하나의 2포트 쌍에서 FC 타겟 모드를, 다른 2포트 쌍에서 FC 이니시에이터 모드를 지원할 수 있습니다.

관련 정보

"NetApp Hardware Universe를 참조하십시오"

"SAN 구성"

포트를 구성합니다

통합 타겟 어댑터(X1143A-R6)를 구성하려면 동일한 퍼스낼리티 모드에서 동일한 칩에 두 개의 인접 포트를 구성해야 합니다.

단계

1. 'system node hardware unified-connect modify' 명령을 사용하여 FC(Fibre Channel) 또는 CNA(Converged Network Adapter)에 필요한 포트를 구성합니다.
2. FC 또는 10Gb 이더넷에 적합한 케이블을 연결합니다.
3. 올바른 SFP+가 설치되었는지 확인합니다.

   네트워크 FCP 어댑터 show-instance-node-adapter입니다

   CNA의 경우 10Gb 이더넷 SFP를 사용해야 합니다. FC의 경우 연결 중인 FC 패브릭을 기반으로 8Gb SFP 또는 16Gb SFP를 사용해야 합니다.

   에 대한 자세한 내용은 `network fcp adapter show` "ONTAP 명령 참조입니다"을 참조하십시오.

X1133A-R6 어댑터를 사용할 경우 연결 끊김 방지

별도의 X1133A-R6 HBA에 대한 중복 경로를 사용하여 시스템을 구성하면 포트 장애 시 연결이 끊어지지 않습니다.

X1133A-R6 HBA는 2개의 2포트 쌍으로 구성된 4포트, 16Gb FC 어댑터입니다. X1133A-R6 어댑터는 타겟 모드 또는 이니시에이터 모드로 구성할 수 있습니다. 각 2포트 쌍은 단일 ASIC에서 지원됩니다(예: ASIC 1의 포트 1과 포트 2, ASIC 2의 포트 3과 포트 4). 단일 ASIC의 두 포트는 타겟 모드나 이니시에이터 모드에서 동일한 모드로 작동하도록 구성해야 합니다. ASIC에서 쌍을 지원하는 데 오류가 발생하면 페어의 두 포트가 모두 오프라인 상태가 됩니다.

이러한 접속 구성 손실을 방지하려면 X1133A-R6 HBA를 분리하는 이중 경로 또는 HBA의 다른 ASIC에서 지원되는 포트에 대한 이중 경로를 사용하여 시스템을 구성합니다.

모든 **SAN** 프로토콜에 대한 **LIF** 관리

모든 **SAN** 프로토콜에 대한 **LIF** 관리

이니시에이터는 SAN 환경의 클러스터에 대한 페일오버 기능에 MPIO(다중 경로 I/O) 및 ALUA(Asymmetric Logical Unit Access)를 사용해야 합니다. 노드에 장애가 발생할 경우 LIF는 장애가 발생한 파트너 노드의 IP 주소를 마이그레이션하거나 가정하지 않습니다. 대신, 호스트에서 ALUA를 사용하여 LIF를 통해 LUN 액세스를 위한 적절한 경로를 선택해야 합니다.

HA 쌍에서 처리하는 LUN에 대한 액세스를 허용하려면 논리 인터페이스(LIF)를 사용하여 HA 쌍의 각 노드에서 하나 이상의 iSCSI 경로를 생성해야 합니다. SAN을 지원하는 모든 SVM(스토리지 가상 머신)마다 하나의 관리 LIF를 구성해야 합니다.

직접 연결 또는 이더넷 스위치 사용이 연결에 지원됩니다. 두 가지 연결 유형에 대해 LIF를 생성해야 합니다.

- SAN을 지원하는 모든 SVM(스토리지 가상 머신)마다 하나의 관리 LIF를 구성해야 합니다.
  노드당 두 개의 LIF를 구성할 수 있으며, FC와 함께 사용되는 각 패브릭과 iSCSI용 이더넷 네트워크를 각각 하나씩 구성할 수 있습니다.

LIF를 생성한 후 포트 세트에서 제거하고 SVM(스토리지 가상 머신) 내의 다른 노드로 이동한 후 삭제할 수 있습니다.

관련 정보

- "LIF 개요 구성"
- "LIF를 생성합니다"

ONTAP에서 **NVMe LIF**를 구성합니다

NVMe LIF를 구성할 때 특정 요구사항을 충족해야 합니다.

시작하기 전에

NVMe는 LIF를 생성하는 FC 어댑터에서 지원되어야 합니다. 지원되는 어댑터는 에 나와 있습니다 "Hardware Universe".

이 작업에 대해

ONTAP 9.12.1 이상부터 최대 12개 노드에서 노드당 두 개의 NVMe LIF를 구성할 수 있다. ONTAP 9.11.1 이하 버전에서는 최대 2개 노드에서 노드당 두 개의 NVMe LIF를 구성할 수 있다.

NVMe LIF를 생성할 때 다음 규칙이 적용됩니다.

- NVMe는 데이터 LIF에서 유일한 데이터 프로토콜일 수 있습니다.
- SAN을 지원하는 모든 SVM에 대해 하나의 관리 LIF를 구성해야 합니다.
- ONTAP 9.5 이상의 경우 네임스페이스가 포함된 노드와 노드의 HA 파트너에 NVMe LIF를 구성해야 합니다.
- ONTAP 9.4만 해당:
  - NVMe LIF 및 네임스페이스는 동일한 노드에서 호스팅되어야 합니다.
  - SVM당 하나의 NVMe 데이터 LIF만 구성할 수 있습니다.

단계

1. LIF를 생성합니다.

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>
-home-port <home_port>
```

NVMe/TCP는 ONTAP 9.10.1 이상부터 사용할 수 있습니다.

2. LIF가 생성되었는지 확인합니다.

```
network interface show -vserver <SVM_name>
```

NVMe/TCP LIF 생성 후 포트 8009에서 검색을 수신합니다.

관련 정보

- "네트워크 인터페이스"

SAN LIF를 이동하기 전에 알아야 할 사항

클러스터에 노드 추가, 클러스터에서 노드 삭제 등과 같이 클러스터의 콘텐츠를 변경하는 경우에는 LIF 이동만 수행해야 합니다. LIF 이동을 수행할 경우 FC 패브릭을 재존치하거나 클러스터의 연결된 호스트와 새로운 타겟 인터페이스 간에 새 iSCSI 세션을 생성할 필요가 없습니다.

네트워크 인터페이스 이동 명령을 사용하면 SAN LIF를 이동할 수 없습니다. SAN LIF는 LIF를 오프라인 상태로 전환하고 LIF를 다른 홈 노드 또는 포트로 이동한 다음, 새로운 위치에서 온라인 상태로 다시 전환하여 수행해야 합니다. ALUA(Asymmetric Logical Unit Access)는 모든 ONTAP SAN 솔루션의 일부로 이중 경로 및 자동 경로 선택을 제공합니다. 따라서 LIF가 이동을 위해 오프라인 상태로 전환되면 I/O 중단이 발생하지 않습니다. 호스트는 간단히 재시도하여 I/O를 다른 LIF로 이동합니다.

LIF 이동을 사용하면 다음을 중단 없이 수행할 수 있습니다.

- LUN 데이터에 액세스하는 호스트에 전혀 영향을 주지 않는 방식으로 클러스터의 HA 쌍 중 하나를 업그레이드된 HA 쌍으로 교체합니다
- 대상 인터페이스 카드를 업그레이드합니다
- SVM(스토리지 가상 시스템)의 리소스를 클러스터의 한 노드 세트에서 클러스터의 다른 노드 세트로 이동합니다

포트 세트에서 **SAN LIF**를 제거합니다

삭제하거나 이동하려는 LIF가 포트 세트에 있는 경우 LIF를 삭제하거나 이동하기 전에 포트 세트에서 LIF를 제거해야 합니다.

이 작업에 대해

다음 절차의 1단계는 하나의 LIF가 포트 세트에 있는 경우에만 수행해야 합니다. 포트 세트가 이니시에이터 그룹에 바인딩되어 있는 경우 포트 세트의 마지막 LIF를 제거할 수 없습니다. 그렇지 않으면 포트 세트에 여러 LIF가 있는 경우 2단계부터 시작할 수 있습니다.

단계

1. 포트 세트에 하나의 LIF만 있는 경우 'lun igroup unbind' 명령을 사용하여 이니시에이터 그룹에서 포트 세트를 바인딩 해제합니다.

   > 이니시에이터 그룹을 포트 세트에서 바인딩 해제하면 이니시에이터 그룹의 모든 이니시에이터가 모든 네트워크 인터페이스의 이니시에이터 그룹에 매핑된 모든 타겟 LUN에 액세스할 수 있습니다.

   'cluster1::> lun igroup unbind-vserver vs1-igroup ig1'

   에 대한 자세한 내용은 `lun igroup unbind` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 'lun 포트셋 제거' 명령을 사용하여 포트 세트에서 LIF를 제거합니다.

   'cluster1::> port set remove-vserver vs1-포트셋 PS1-port-name liff 1'

   에 대한 자세한 내용은 `lun portset remove` "ONTAP 명령 참조입니다"을 참조하십시오.

SAN LIF를 이동합니다

노드를 오프라인 상태로 전환해야 하는 경우 SAN LIF를 이동하여 WWPN과 같은 구성 정보를 유지하고 스위치 패브릭의 재조닝(zoning)을 방지할 수 있습니다. SAN LIF가 이동되기 전에 먼저 오프라인으로 전환되어야 하므로 호스트 트래픽은 호스트 다중 경로 소프트웨어를 통해 LUN에 대한 무중단 액세스를 제공해야 합니다. SAN LIF를 클러스터의 아무 노드로 이동할 수 있지만 SVM(스토리지 가상 머신) 간에 SAN LIF를 이동할 수 없습니다.

시작하기 전에

LIF가 포트 세트의 구성원인 경우 LIF를 다른 노드로 이동하기 전에 포트 세트에서 LIF를 제거해야 합니다.

이 작업에 대해

이동하려는 LIF의 대상 노드 및 물리적 포트는 동일한 FC 패브릭 또는 이더넷 네트워크에 있어야 합니다. LIF를 적절하게 구역이 되어 있지 않은 다른 패브릭으로 이동하거나 iSCSI 이니시에이터와 타겟 간의 연결이 없는 이더넷 네트워크로 LIF를 이동할 경우 LUN을 다시 온라인 상태로 전환할 때 LUN에 액세스할 수 없습니다.

단계

1. LIF의 관리 및 운영 상태를 봅니다.

   'network interface show -vserver_vserver_name_'

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. LIF의 상태를 '자체'(오프라인)로 변경합니다.

   'network interface modify -vserver_vserver_name_-lif_LIF_name_-status-admin down'

   에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

3. LIF를 새 노드 및 포트에 할당합니다.

   'network interface modify -vserver_vserver_name_-lif_LIF_name_-home-node_node_name_-home -port_port_name_'

4. LIF의 상태를 '위쪽'(온라인)으로 변경합니다.

   'network interface modify -vserver_vserver_name_-lif_LIF_name_-status-admin up

   에 대한 자세한 내용은 `up` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 변경 사항 확인:

   'network interface show -vserver_vserver_name_'

SAN 환경에서 **LIF**를 삭제합니다

LIF를 삭제하기 전에 LIF에 연결된 호스트가 다른 경로를 통해 LUN에 액세스할 수 있는지 확인해야 합니다.

시작하기 전에

삭제하려는 LIF가 포트 세트의 구성원인 경우 LIF를 삭제하려면 먼저 포트 세트에서 LIF를 제거해야 합니다.

시스템 관리자

ONTAP 시스템 관리자(9.7 이상)가 설치된 LIF를 삭제합니다.

단계

1. System Manager에서 * Network > Overview * 를 클릭한 다음 * Network Interfaces * 를 선택합니다.
2. LIF를 삭제할 스토리지 VM을 선택합니다.
3. 을 ⋮ 클릭하고 * 삭제 * 를 선택합니다.

CLI를 참조하십시오

ONTAP CLI에서 LIF를 삭제합니다.

단계

1. 삭제할 LIF와 현재 포트의 이름을 확인합니다.

   'network interface show – vserver_vserver_name _'

2. LIF를 삭제합니다.

   네트워크 인터페이스 삭제

   'network interface delete-vserver vs1-lif lif liff li1'

   에 대한 자세한 내용은 `network interface delete` "ONTAP 명령 참조입니다"을 참조하십시오.

3. LIF를 삭제했는지 확인합니다.

   네트워크 인터페이스 쇼

   네트워크 인터페이스 show-vserver vs1

   ```
   Logical  Status     Network                       Current   Current Is
   Vserver  Interface  Admin/Oper Address/Mask       Node      Port
   Home
   -------  ---------- ---------- ----------------- --------- -------
   ----
   vs1
            lif2       up/up      192.168.2.72/24   node-01   e0b
   true
            lif3       up/up      192.168.2.73/24   node-01   e0b
   true
   ```

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

SAN LIF 요구사항에서 클러스터에 노드를 추가해야 합니다

클러스터에 노드를 추가할 때는 특정 고려 사항을 염두에 두어야 합니다.

- 새 노드에서 LUN을 생성하기 전에 필요에 따라 새 노드에 LIF를 생성해야 합니다.
- 호스트에서 호스트 스택 및 프로토콜에 따라 이러한 LIF를 검색해야 합니다.
- 클러스터 인터커넥트 네트워크를 사용하지 않고 LUN 및 볼륨 이동을 수행할 수 있도록 새 노드에 LIF를 생성해야 합니다.

호스트 **iSCSI SendTargets** 검색 작업에 **FQDN**을 반환하도록 **iSCSI LIF**를 구성합니다

ONTAP 9부터 호스트 OS가 iSCSI SendTargets 검색 작업을 전송할 때 FQDN(정규화된 도메인 이름)을 반환하도록 iSCSI LIF를 구성할 수 있습니다. FQDN은 호스트 OS와 스토리지 서비스 사이에 NAT(Network Address Translation) 디바이스가 있는 경우에 유용합니다.

이 작업에 대해

NAT 장치의 한 쪽에 있는 IP 주소는 다른 쪽에는 의미가 없지만 FQDN은 양쪽에서 의미를 가질 수 있습니다.

FQDN 값 상호 운용성 제한은 모든 호스트 OS에서 128자입니다.

단계

1. 권한 설정을 고급으로 변경합니다.

   세트 프리빌리지 고급

2. FQDN을 반환하도록 iSCSI LIF 구성:

   "vserver iSCSI interface modify -vserver_SVM_name_-lif_iscsi_LIF_name_-SendTargets_FQDN"

   다음 예에서는 iSCSI LIF가 storagehost-005.example.com 를 FQDN으로 반환하도록 구성되어 있습니다.

   'vserver iscsi interface modify -vserver vs1 -lif vs1_iSCSI1-SendTargets-FQDN storagehost-005.example.com'

3. SendTargets가 FQDN인지 확인합니다.

   'vserver iscsi interface show -vserver_SVM_name_-fields SendTargets-FQDN'

   이 예제에서 storagehost-005.example.com 은 SendTargets-FQDN 출력 필드에 표시됩니다.

```
cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
sendtargets-fqdn
vserver lif        sendtargets-fqdn
------- ---------- --------------------------
vs1     vs1_iscsi1 storagehost-005.example.com
vs1     vs1_iscsi2 storagehost-006.example.com
```

관련 정보

"ONTAP 명령 참조입니다"

SAN 프로토콜에 ONTAP 공간 할당을 사용합니다

ONTAP 공간을 할당하면 LUN 또는 NVMe 네임스페이스가 공간이 부족할 때 오프라인 상태로 전환되지 않도록 방지하고 SAN 호스트에서 공간을 재확보할 수 있습니다.

ONTAP는 SAN 프로토콜과 ONTAP 버전에 따라 공간 할당을 지원합니다. ONTAP 9.16.1부터 새로 생성된 LUN 및 모든 네임스페이스에 대해 iSCSI, FC, NVMe 프로토콜에 대해 공간 할당이 기본적으로 활성화됩니다.

ONTAP 버전입니다	프로토콜	공간 할당은...
9.16.1 이상	• iSCSI • FC • NVMe를 참조하십시오	새로 생성된 LUN 및 모든 네임스페이스에 대해 기본적으로 설정됩니다
9.15.1	• iSCSI • FC	새로 생성된 LUN에 대해 기본적으로 설정됩니다
	NVMe를 참조하십시오	지원되지 않습니다
9.14.1 이하	• iSCSI • FC	새로 생성된 LUN에 대해 기본적으로 해제되어 있습니다
	NVMe를 참조하십시오	지원되지 않습니다

공간 할당이 설정된 경우:

- LUN 또는 네임스페이스에 공간이 부족할 경우 ONTAP는 쓰기 작업에 사용할 수 있는 여유 공간이 없음을 호스트에 알립니다. 그 결과 LUN 또는 네임스페이스가 온라인 상태로 유지되고 읽기 작업이 계속 서비스됩니다. 호스트 구성에 따라 호스트가 성공할 때까지 쓰기 작업을 다시 시도하거나 호스트 파일 시스템이 오프라인이 될 때까지 재시도합니다. LUN 또는 네임스페이스에서 추가 여유 공간을 사용할 수 있게 되면 쓰기 작업이 재개됩니다.

  공간 할당이 사용하도록 설정되어 있지 않은 경우 LUN 또는 네임스페이스에 공간이 부족할 때 모든 I/O 작업이 실패하고 LUN 또는 네임스페이스가 오프라인 상태가 됩니다. 정상 작업을 재개하려면 공간 문제를 해결해야 합니다. 호스트에서 LUN 디바이스를 다시 검색해야 경로 및 디바이스를 운영 상태로 복구할 수 있습니다.

- 호스트는 SCSI 또는 NVMe(일명 `TRIM`) 작업을 수행할 수 `UNMAP` 있습니다. 매핑 해제 작업을 사용하면 호스트에서 더 이상 유효한 데이터를 포함하지 않으므로 더 이상 필요하지 않은 데이터 블록을 식별할 수 있습니다. 일반적으로 파일 삭제 후 식별이 이루어집니다. 그런 다음 스토리지 시스템에서 해당 데이터 블록을 할당 해제하여 다른 곳에서 공간을 사용할 수 있도록 합니다. 이러한 할당 해제는 특히 데이터 회전율이 높은 파일 시스템에서 전반적인 스토리지 효율성을 크게 향상시킵니다.

시작하기 전에

공간 할당을 설정하려면 쓰기를 완료할 수 없는 경우 공간 할당 오류를 올바르게 처리할 수 있는 호스트 구성이 필요합니다. SCSI 또는 NVMe를 `UNMAP` 활용하려면 SCSI SBC-3 표준에 정의된 논리적 블록 프로비저닝을 사용할 수 있는 구성이 필요합니다.

공간 할당을 설정할 때 다음 호스트는 현재 씬 프로비저닝을 지원합니다.

- Citrix XenServer 6.5 이상
- VMware ESXi 5.0 이상
- Oracle Linux 6.2 UEK 커널 이상
- Red Hat Enterprise Linux 6.2 이상
- SUSE Linux Enterprise Server 11 이상
- Solaris 11.1 이상
- Windows

이 작업에 대해

클러스터를 ONTAP 9.15.1 이상으로 업그레이드하면 소프트웨어 업그레이드 전에 생성된 모든 LUN에 대한 공간 할당 설정은 호스트 유형에 관계없이 업그레이드 후에도 동일하게 유지됩니다. 예를 들어 공간 할당이 해제된 VMware 호스트에 대해 ONTAP 9.13.1에서 LUN을 생성한 경우 ONTAP 9.15.1로 업그레이드한 후 해당 LUN에 대한 공간 할당이 해제된 상태로 유지됩니다.

단계

1. 공간 할당 활성화:

```
lun modify -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-space-allocation enabled
```

2. 공간 할당이 설정되었는지 확인합니다.

```
lun show -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-fields space-allocation
```

3. 호스트 운영 체제에서 공간 할당이 활성화되어 있는지 확인합니다.

> 일부 버전의 VMware ESXi를 포함한 일부 호스트 구성은 설정 변경을 자동으로 인식할 수 있으며 사용자 개입이 필요하지 않습니다. 다른 구성에서는 장치를 다시 검색해야 할 수 있습니다. 일부 파일 시스템 및 볼륨 관리자는 를 사용하여 공간을 재확보하기 위해 추가적인 특정 설정이 필요할 수 `SCSI UNMAP` 있습니다. 파일 시스템을 다시 마운트하거나 전체 운영 체제를 재부팅해야 할 수 있습니다. 해당 호스트의 설명서를 참조하여 지침을 확인하십시오.

VMware ESXi 8.x 이상 **NVMe** 호스트에 대한 호스트 구성

NVMe 프로토콜을 사용하여 ESXi 8.x 이상을 실행하는 VMware 호스트가 있는 경우 ONTAP에서 공간 할당을 설정한 후 호스트에서 다음 단계를 수행해야 합니다.

단계

1. ESXi 호스트에서 DSM이 비활성화되었는지 확인합니다.

```
esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
```

예상 값은 0입니다.

2. NVMe DSM 활성화:

```
esxcfg-advcfg -s 1 /Scsi/NvmeUseDsmTp4040
```

3. DSM이 활성화되어 있는지 확인합니다.

```
esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
```

예상 값은 1입니다.

관련 링크

에 대해 자세히 "ONTAP를 사용하는 ESXi 8.x에 대한 NVMe-oF 호스트 구성"알아보십시오.

권장되는 볼륨 및 파일 또는 **LUN** 구성 조합

권장되는 볼륨 및 파일 또는 **LUN** 구성 조합 개요

애플리케이션 및 관리 요구사항에 따라 FlexVol 볼륨과 파일 또는 LUN 구성의 특정 조합이 사용할 수 있습니다. 이러한 조합을 통해 얻을 수 있는 이점과 비용을 이해하면 환경에 적합한 볼륨 및 LUN 구성의 조합을 결정하는 데 도움이 됩니다.

권장되는 볼륨 및 LUN 구성 조합은 다음과 같습니다.

- 일반 볼륨 프로비저닝이 있는 공간 예약 파일 또는 LUN
- 씬 볼륨 프로비저닝이 있는 공간 예약 파일이 아닌 LUN
- 반씩 볼륨 프로비저닝을 사용하는 공간 예약 파일 또는 LUN

이러한 구성 조합과 함께 LUN에서 SCSI 씬 프로비저닝을 사용할 수 있습니다.

일반 볼륨 프로비저닝이 있는 공간 예약 파일 또는 **LUN**

- 이점: *
- 공간 예약 파일 내의 모든 쓰기 작업이 보장되며 공간 부족으로 인해 작업이 실패하지 않습니다.
- 볼륨의 스토리지 효율성 및 데이터 보호 기술에는 제한이 없습니다.
- 비용 및 제한: *
- 전체적으로 프로비저닝된 볼륨을 지원할 수 있도록 충분한 공간을 집합체로부터 충분히 미리 설정해야 합니다.
- LUN 생성 시 볼륨에서 LUN의 2배에 해당하는 공간이 할당됩니다.

씬 볼륨 프로비저닝이 있는 공간 예약 파일이 아닌 **LUN**

- 이점: *
- 볼륨의 스토리지 효율성 및 데이터 보호 기술에는 제한이 없습니다.
- 공간은 사용되는 경우에만 할당됩니다.

- 비용 및 제한: *
- 쓰기 작업은 보장되지 않으며, 볼륨에 여유 공간이 없을 경우 실패할 수 있습니다.
- Aggregate에 여유 공간이 부족하지 않도록 하려면 Aggregate의 여유 공간을 효과적으로 관리해야 합니다.

반씩 볼륨 프로비저닝을 사용하는 공간 예약 파일 또는 **LUN**

- 이점: *

공간을 일반 볼륨 프로비저닝보다 미리 예약하므로 최선의 쓰기 보장이 제공됩니다.

- 비용 및 제한: *
- 이 옵션을 사용하면 쓰기 작업이 실패할 수 있습니다.

  볼륨의 여유 공간과 데이터 휘발성의 균형을 적절하게 유지하여 이 위험을 완화할 수 있습니다.

- 스냅샷, FlexClone 파일 및 LUN과 같은 데이터 보호 객체의 보존에 의존할 수는 없습니다.
- 중복제거, 압축, ODX/복사 오프로드 등 자동으로 삭제할 수 없는 ONTAP 블록 공유 스토리지 효율성 기능은 사용할 수 없습니다.

환경에 맞는 올바른 볼륨 및 **LUN** 구성 조합을 결정합니다

환경에 대한 몇 가지 기본적인 질문에 답변하면 환경에 가장 적합한 FlexVol 볼륨 및 LUN 구성을 파악하는 데 도움이 됩니다.

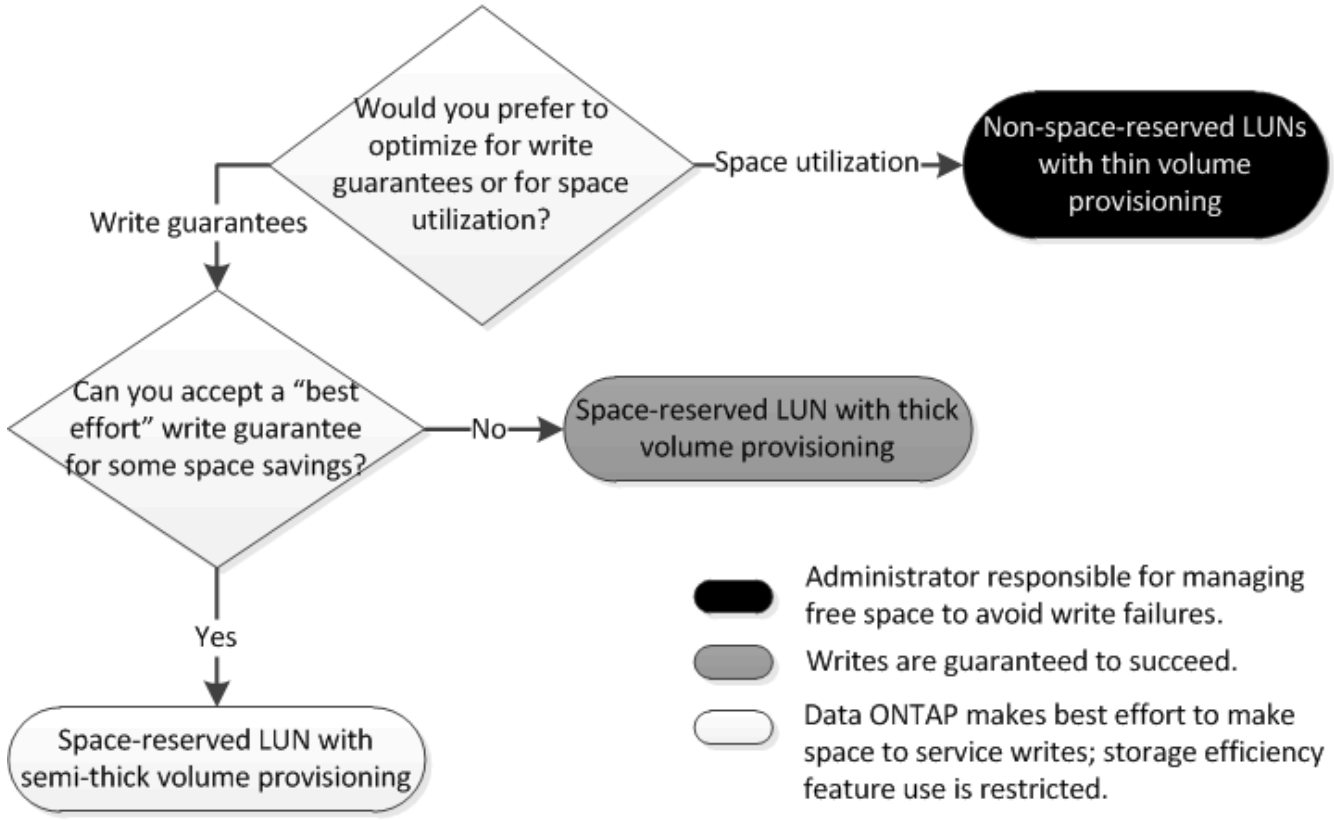
이 작업에 대해

LUN 및 볼륨 구성을 최적화하여 스토리지 활용률을 극대화하거나 쓰기 보장을 극대화할 수 있습니다. 스토리지 활용률의 요구사항과 여유 공간을 신속하게 모니터링 및 보충하는 기능을 기준으로 설치에 적합한 FlexVol 볼륨 및 LUN 볼륨을 결정해야 합니다.

각 LUN에 대해 별도의 볼륨이 필요하지 않습니다.

단계

1. 다음 진단트리를 사용하여 환경에 가장 적합한 볼륨 및 LUN 구성 조합을 결정합니다.



LUN의 데이터 증가율 계산

시간이 경과하면서 LUN 데이터가 증가하는 속도를 알고 있어야 공간 예약 LUN 또는 비공간 예약 LUN을 사용해야 하는지 여부를 확인할 수 있습니다.

이 작업에 대해

지속적으로 높은 데이터 증가율을 사용하면 공간 예약 LUN이 더 나은 옵션이 될 수 있습니다. 데이터 증가율이 낮은 경우 공간이 예약되지 않은 LUN을 고려해야 합니다.

OnCommand Insight와 같은 도구를 사용하여 데이터 증가율을 계산하거나 수동으로 계산할 수 있습니다. 다음은 수동 계산에 대한 단계입니다.

단계

1. 공간 예약 LUN을 설정합니다.
2. LUN의 데이터를 1주일 등의 지정된 기간 동안 모니터링합니다.

   모니터링 기간이 충분히 길어 데이터 증가 시 정기적으로 발생하는 대표적인 샘플을 형성해야 합니다. 예를 들어, 매달 말에 지속적으로 증가하는 데이터의 양이 상당히 많을 것입니다.

3. 매일 증가하는 데이터의 양을 GB 단위로 기록합니다.
4. 모니터링 기간이 끝나면 각 날짜의 합계를 더한 다음 모니터링 기간의 일 수로 나눕니다.

   이 계산으로 평균 성장률을 얻을 수 있습니다.

예

이 예에서는 200GB LUN이 필요합니다. LUN을 1주일 동안 모니터링하고 다음과 같은 일일 데이터 변경 사항을 기록하기로 결정합니다.

- 일요일: 20GB
- 월요일: 18GB
- 화요일: 17GB
- 수요일: 20GB
- 목요일: 20GB
- 금요일: 23GB
- 토요일: 22GB

이 예에서 성장률(20+18+17+20+20+23+22)/7=20GB입니다.

일반 프로비저닝된 볼륨이 있는 공간 예약 파일 또는 **LUN**에 대한 구성 설정입니다

이 FlexVol 볼륨 및 파일 또는 LUN 구성 조합을 사용하면 스토리지 효율성 기술을 사용할 수 있으며 공간이 사전에 충분히 할당되므로 여유 공간을 능동적으로 모니터링할 필요가 없습니다.

일반 프로비저닝을 사용하여 볼륨에서 공간 예약 파일 또는 LUN을 구성하려면 다음 설정이 필요합니다.

볼륨 설정	값
보장	볼륨
부분 예약	100
스냅숏 예비 공간입니다	모두
스냅샷 자동 삭제	선택 사항
자동 확장	선택 사항: 사용하도록 설정한 경우 애그리게이트 가용 공간을 능동적으로 모니터링해야 합니다.

파일 또는 **LUN** 설정	값
공간 예약	활성화됨

공간이 예약되지 않은 파일 또는 씬 프로비저닝된 볼륨이 있는 **LUN**에 대한 구성 설정입니다

이 FlexVol 볼륨 및 파일 또는 LUN 구성 조합을 사용하려면 가장 적은 양의 스토리지를 미리 할당해야 하지만 공간 부족으로 인한 오류를 방지하기 위해 활성 여유 공간 관리가 필요합니다.

씬 프로비저닝된 볼륨에서 공간이 예약되지 않은 파일 또는 LUN을 구성하려면 다음 설정이 필요합니다.

볼륨 설정	값
보장	없음
부분 예약	0
스냅숏 예비 공간입니다	모두
스냅샷 자동 삭제	선택 사항
자동 확장	선택 사항

파일 또는 **LUN** 설정	값
공간 예약	사용 안 함

추가 고려 사항

볼륨 또는 애그리게이트의 공간이 부족해지면 파일 또는 LUN에 대한 쓰기 작업이 실패할 수 있습니다.

볼륨과 애그리게이트의 여유 공간을 적극적으로 모니터링하지 않으려면 볼륨에 대해 Autogrow를 활성화하고 볼륨의 최대 크기를 애그리게이트 크기로 설정해야 합니다. 이 구성에서는 aggregate 여유 공간을 적극적으로 모니터링해야 하지만, 볼륨의 여유 공간을 모니터링할 필요는 없습니다.

반씩 볼륨 프로비저닝을 사용하는 공간 예약 파일 또는 **LUN**에 대한 구성 설정입니다

이 FlexVol 볼륨 및 파일 또는 LUN 구성 조합을 사용하면 완전히 프로비저닝된 조합보다 더 적은 양의 스토리지를 미리 할당할 수 있지만 볼륨에 사용할 수 있는 효율성 기술에 제한이 있습니다. 이러한 구성 조합의 경우 덮어쓰기의 작업이 가장 효율적으로 처리됩니다.

반씩 프로비저닝을 사용하여 볼륨에서 공간 예약 LUN을 구성하려면 다음 설정이 필요합니다.

볼륨 설정	값
보장	볼륨
부분 예약	0
스냅숏 예비 공간입니다	0
스냅샷 자동 삭제	제거 약속 수준에서는 모든 오브젝트, 볼륨으로 설정된 트리거, 자동 삭제를 위해 활성화된 모든 FlexClone LUN 및 FlexClone 파일이 포함된 제거 목록이 있습니다.
자동 확장	선택 사항: 사용하도록 설정한 경우 애그리게이트 가용 공간을 능동적으로 모니터링해야 합니다.

파일 또는 **LUN** 설정	값
공간 예약	활성화됨

기술 제한

이 구성 조합에는 다음 볼륨 스토리지 효율성 기술을 사용할 수 없습니다.

- 압축
- 중복 제거
- ODX 및 FlexClone 복사 오프로드
- FlexClone LUN 및 FlexClone 파일이 자동 삭제용으로 표시되지 않음(활성 클론)
- FlexClone 하위 파일
- ODX/복사 오프로드

추가 고려 사항

이 구성 조합을 사용할 때는 다음 사항을 고려해야 합니다.

- 해당 LUN을 지원하는 볼륨의 공간이 부족하면 보호 데이터(FlexClone LUN 및 파일, 스냅샷)가 삭제됩니다.
- 볼륨에 여유 공간이 부족하면 쓰기 작업이 시간 초과되어 실패할 수 있습니다.

압축은 AFF 플랫폼에 대해 기본적으로 사용하도록 설정되어 있습니다. AFF 플랫폼에서 반씩 프로비저닝을 사용하려는 모든 볼륨에 대해 압축을 명시적으로 해제해야 합니다.

SAN 데이터 보호

SAN 환경을 위한 ONTAP 데이터 보호 방법에 대해 알아보십시오

실수로 인한 삭제, 애플리케이션 충돌, 데이터 손상 또는 재해가 발생할 경우 복원에 사용할 수 있도록 데이터의 복사본을 만들어 데이터를 보호할 수 있습니다. ONTAP는 데이터 보호 및 백업 요구에 따라 데이터를 보호할 수 있는 다양한 방법을 제공합니다.

SnapMirror 활성 동기화

ONTAP 9.9.1의 일반 가용성부터 SAN 환경에서 비즈니스 크리티컬 애플리케이션의 자동 페일오버를 지원하기 위해 제로 복구 시간 목표(제로 RTO) 또는 투명 애플리케이션 페일오버(TAF)를 제공합니다. SnapMirror 액티브 동기화를 사용하려면 2개의 AFF 클러스터 또는 2개의 ASA(All Flash SAN Array) 클러스터가 있는 구성으로 ONTAP Mediator 1.2를 설치해야 합니다.

"SnapMirror 활성 동기화"

스냅샷

LUN의 여러 백업을 수동 또는 자동으로 생성, 예약 및 유지 관리할 수 있습니다. 스냅샷은 최소한의 추가 볼륨 공간만 사용하며 성능 비용이 들지 않습니다. LUN 데이터가 실수로 수정되거나 삭제된 경우 최신 스냅샷 중 하나에서 해당 데이터를 쉽고 빠르게 복원할 수 있습니다.

FlexClone LUN(FlexClone 라이센스 필요)

활성 볼륨 또는 스냅샷에 있는 다른 LUN의 쓰기 가능한 특정 시점 복사본을 제공합니다. 클론 및 상위 항목은 서로 영향을 주지 않고 독립적으로 수정할 수 있습니다.

SnapRestore(라이센스 필요)

전체 볼륨의 스냅샷에서 요청 시 데이터를 빠르고 공간 효율적으로 복구할 수 있습니다. SnapRestore를 사용하면 스토리지 시스템을 재부팅하지 않고도 LUN을 이전에 보존된 상태로 복원할 수 있습니다.

데이터 보호 미러 복사본**(SnapMirror** 라이센스 필요)

볼륨에 있는 데이터의 스냅샷을 주기적으로 생성하고, 로컬 또는 광역 네트워크를 통해 해당 스냅샷을 다른 클러스터에 있는 파트너 볼륨에 복사하고, 이러한 스냅샷을 보존할 수 있도록 함으로써 비동기식 재해 복구를 제공합니다. 소스 볼륨의 데이터가 손상되었거나 손실된 경우 파트너 볼륨의 미러 복사본을 사용하여 마지막 스냅샷 시점의 데이터를 빠르게 복구하고 복구할 수 있습니다.

SnapVault 백업**(SnapMirror** 라이센스 필요)

스토리지를 효율적으로 장기 백업 보존 SnapVault 관계를 사용하면 선택한 볼륨 스냅샷을 대상 볼륨에 백업하고 백업을 유지할 수 있습니다.

테이프 백업 및 아카이브 작업을 수행하는 경우 SnapVault 보조 볼륨에 이미 백업된 데이터에 대해 수행할 수 있습니다.

Windows 또는 **UNIX**용 **SnapDrive(SnapDrive** 라이센스 필요)

Windows 또는 UNIX 호스트에서 직접 LUN에 대한 액세스를 구성하고, LUN을 관리하고, 스토리지 시스템 스냅샷을 관리합니다.

기본 테이프 백업 및 복구

대부분의 기존 테이프 드라이브 지원은 ONTAP에 포함되어 있으며 테이프 공급업체가 새 디바이스에 대한 지원을 동적으로 추가하는 방법도 포함되어 있습니다. 또한 ONTAP는 RMT(Remote Magnetic Tape) 프로토콜을 지원하여 모든 가능 시스템에 백업 및 복구를 수행할 수 있습니다.

관련 정보

"NetApp 설명서: UNIX용 SnapDrive" "NetApp 설명서:SnapDrive for Windows(최신 릴리스)" "테이프 백업을 사용한 데이터 보호"

ONTAP 스냅샷에서 단일 LUN을 복구합니다

단일 LUN이 포함된 전체 볼륨을 복원하지 않고 스냅샷에서 단일 LUN을 복구할 수 있습니다. LUN을 제자리에서 또는 볼륨의 새 경로로 복원할 수 있습니다. 이 작업은 볼륨의 다른 파일 또는 LUN에 영향을 주지 않고 단일 LUN만 복구합니다. 스트림을 사용하여 파일을 복원할 수도 있습니다.

시작하기 전에

- 복원 작업을 완료하려면 볼륨에 충분한 공간이 있어야 합니다.
  - 부분 예약 공간이 0%인 공간 예약 LUN을 복원하는 경우 복원된 LUN 크기의 1배가 필요합니다.

- 부분 예약 공간이 100%인 공간 예약 LUN을 복원하는 경우 복원된 LUN의 크기의 2배가 필요합니다.
- 공간이 예약되지 않은 LUN을 복원하는 경우 복원된 LUN에 사용된 실제 공간만 필요합니다.

- 대상 LUN의 스냅샷이 생성되어야 합니다.

  복구 작업이 실패하면 대상 LUN이 잘릴 수 있습니다. 이러한 경우 스냅샷을 사용하여 데이터 손실을 방지할 수 있습니다.

- 소스 LUN의 스냅샷이 생성되어야 합니다.

  드물지만 LUN 복구가 실패하여 소스 LUN을 사용할 수 없게 되는 경우가 있습니다. 이 경우 스냅샷을 사용하여 LUN을 복구 시도 바로 전 상태로 되돌릴 수 있습니다.

- 대상 LUN과 소스 LUN의 OS 유형이 같아야 합니다.

  대상 LUN의 OS 유형이 소스 LUN과 다른 경우 복구 작업 후 호스트가 대상 LUN에 대한 데이터 액세스를 잃을 수 있습니다.

단계

1. 호스트에서 LUN에 대한 모든 호스트 액세스를 중지합니다.
2. 호스트에서 LUN을 액세스할 수 없도록 해당 호스트에서 LUN을 마운트 해제합니다.
3. LUN 매핑을 해제합니다.

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

4. LUN을 복구할 스냅샷을 결정합니다.

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. LUN을 복구하기 전에 LUN의 스냅샷을 생성합니다.

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name>
```

6. 볼륨에 지정된 LUN을 복구합니다.

```
volume snapshot restore-file -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name> -path <lun_path>
```

7. 화면의 단계를 따릅니다.
8. 필요한 경우 LUN을 온라인 상태로 전환합니다.

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

9. 필요한 경우 LUN을 다시 매핑합니다.

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

10. 호스트에서 LUN을 다시 마운트합니다.
11. 호스트에서 LUN에 대한 액세스를 다시 시작합니다.

ONTAP 스냅샷에서 볼륨의 모든 LUN을 복구합니다

명령을 사용하여 스냅샷에서 지정된 볼륨의 모든 LUN을 복원할 수 `volume snapshot restore` 있습니다.

단계

1. 호스트에서 LUN에 대한 모든 호스트 액세스를 중지합니다.

   볼륨에 있는 LUN에 대한 모든 호스트 액세스를 중지하지 않고 SnapRestore를 사용하면 데이터 손상 및 시스템 오류가 발생할 수 있습니다.

2. 호스트에서 LUN을 액세스할 수 없도록 해당 호스트에서 LUN을 마운트 해제합니다.
3. LUN 매핑 해제:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

4. 볼륨을 복원할 스냅샷을 결정합니다.

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. 권한 설정을 고급으로 변경합니다.

```
set -privilege advanced
```

6. 데이터 복원:

```
volume snapshot restore -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name>
```

7. 화면의 지침을 따릅니다.
8. LUN을 다시 매핑합니다.

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. LUN이 온라인 상태인지 확인합니다.

```
lun show -vserver <SVM_name> -path <lun_path> -fields state
```

10. LUN이 온라인 상태가 아닌 경우 온라인 상태로 전환합니다.

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

11. 권한 설정을 admin으로 변경합니다.

```
set -privilege admin
```

12. 호스트에서 LUN을 다시 마운트합니다.
13. 호스트에서 LUN에 대한 액세스를 다시 시작합니다.

ONTAP FlexClone LUN으로 데이터를 보호합니다

FlexClone LUN은 활성 볼륨 또는 스냅샷에 있는 다른 LUN의 쓰기 가능한 시점 복제본입니다. 클론 및 상위 항목은 서로 영향을 주지 않고 독립적으로 수정할 수 있습니다.

FlexClone LUN을 사용하여 LUN의 읽기/쓰기 복사본을 여러 개 생성할 수 있습니다.

FlexClone LUN을 생성하는 이유

- 테스트를 위해 LUN의 임시 복사본을 생성해야 합니다.
- 운영 데이터에 대한 액세스 권한을 부여하지 않고 추가 사용자가 데이터 복사본을 사용할 수 있도록 해야 합니다.
- 원본 데이터는 변경되지 않은 형식으로 유지하면서 조작 및 예상 작업에 사용할 데이터베이스 복제본을 만들려는 경우
- LUN 데이터의 특정 부분 집합(볼륨 그룹의 특정 논리적 볼륨 또는 파일 시스템, 또는 파일 시스템의 특정 파일 또는 파일 세트)를 원래 LUN의 나머지 데이터를 복원하지 않고 원래 LUN에 복사합니다. 이 작업은 LUN과 LUN 클론의 마운트를 동시에 지원하는 운영 체제에서 가능합니다. SnapDrive for UNIX는 'Snap connect' 명령을 통해 이를 지원합니다.
- 동일한 운영 체제를 사용하는 여러 SAN 부팅 호스트가 필요합니다.

FlexClone LUN은 처음에 부모 LUN과 공간을 공유합니다. 기본적으로 FlexClone LUN은 상위 LUN의 공간 예약 속성을 상속합니다. 예를 들어, 상위 LUN이 공간이 예약되지 않은 경우 FlexClone LUN도 기본적으로 공간이 예약되지 않습니다. 그러나 공간 예약 LUN인 상위에서 공간 예약 FlexClone LUN을 생성할 수 있습니다.

LUN을 클론 복제하면 블록 공유가 백그라운드에서 수행되며 블록 공유가 완료될 때까지 볼륨 스냅샷을 생성할 수 없습니다.

'볼륨 스냅샷 자동 삭제 수정' 명령을 사용하여 FlexClone LUN 자동 삭제 기능을 사용하도록 볼륨을 구성해야 합니다. 그렇지 않으면 FlexClone LUN이 자동으로 삭제되지만 FlexClone 자동 삭제에 대해 볼륨이 구성되지 않은 경우 FlexClone LUN이 삭제되지 않습니다.

FlexClone LUN을 생성할 때 FlexClone LUN 자동 삭제 기능은 기본적으로 해제되어 있습니다. FlexClone LUN을 자동으로 삭제하려면 먼저 모든 FlexClone LUN에서 수동으로 활성화해야 합니다. 반씩 볼륨 프로비저닝을 사용하고 이 옵션으로 제공되는 "'최선 노력" 쓰기 보장을 원하는 경우, _ALL_FlexClone LUN을 자동 삭제할 수 있도록 해야 합니다.

> 스냅샷에서 FlexClone LUN을 생성할 때 LUN은 공간 효율적인 백그라운드 프로세스를 사용하여 스냅샷에서 자동으로 분할되므로 LUN이 계속해서 스냅샷에 의존하거나 추가 공간을 소비하지 않습니다. 이 백그라운드 분할이 완료되지 않고 이 스냅샷이 자동으로 삭제되면 해당 FlexClone LUN에 대한 FlexClone 자동 삭제 기능을 해제했더라도 해당 FlexClone LUN이 삭제됩니다. 백그라운드 분할이 완료된 후 해당 스냅샷이 삭제되더라도 FlexClone LUN은 삭제되지 않습니다.

관련 정보

- "FlexClone LUN을 생성합니다"
- "FlexClone LUN을 자동으로 삭제하도록 FlexVol volume을 구성합니다"
- "FlexClone LUN이 자동으로 삭제되지 않도록 방지합니다"

SAN 환경에서 SnapVault 백업을 구성하고 사용합니다

SAN 환경에서의 **ONTAP SnapVault** 백업에 대해 알아보십시오

SAN 환경에서 SnapVault 구성 및 사용은 NAS 환경에서 구성 및 사용과 매우 유사하지만, SAN 환경에서 LUN을 복원하려면 몇 가지 특별한 절차가 필요합니다.

SnapVault 백업에는 소스 볼륨의 읽기 전용 복제본 세트가 포함됩니다. SAN 환경에서는 개별 LUN이 아닌 전체 볼륨을 SnapVault 2차 볼륨에 항상 백업합니다.

LUN이 포함된 운영 볼륨과 SnapVault 백업 역할을 하는 보조 볼륨 간의 SnapVault 관계를 생성하고 초기화하는 절차는 파일 프로토콜에 사용되는 FlexVol 볼륨에서 사용되는 절차와 동일합니다. 이 절차는 에 자세히 설명되어 있습니다 "데이터 보호".

스냅샷이 생성되고 SnapVault 보조 볼륨에 복제되기 전에 백업되는 LUN이 정합성 보장 상태로 유지되도록 하는 것이 중요합니다. SnapCenter를 사용하여 스냅샷 생성을 자동화하면 백업된 LUN이 완료되어 원래 애플리케이션에서 사용할 수 있습니다.

SnapVault 2차 볼륨에서 LUN을 복구하는 기본적인 세 가지 선택 사항은 다음과 같습니다.

- SnapVault 2차 볼륨에서 LUN을 직접 매핑하고 호스트를 LUN에 연결하여 LUN의 컨텐츠를 액세스할 수 있습니다.

  LUN은 읽기 전용이며 SnapVault 백업의 최신 스냅샷에서만 매핑할 수 있습니다. 영구 예약 및 기타 LUN 메타데이터가 손실됩니다. 필요한 경우 호스트에서 복제 프로그램을 사용하여 LUN 컨텐츠를 원래 LUN에 다시 복제할 수 있습니다(액세스할 수 있는 경우).

  LUN의 일련 번호가 소스 LUN과 다릅니다.

- SnapVault 보조 볼륨의 모든 스냅샷을 새로운 읽기-쓰기 볼륨에 복제할 수 있습니다.

  그런 다음 볼륨에 있는 LUN을 매핑하고 호스트를 LUN에 연결하여 LUN의 컨텐츠를 액세스할 수 있습니다. 필요한 경우 호스트에서 복제 프로그램을 사용하여 LUN 컨텐츠를 원래 LUN에 다시 복제할 수 있습니다(액세스할 수 있는 경우).

- SnapVault 2차 볼륨의 모든 스냅샷에서 LUN이 포함된 전체 볼륨을 복원할 수 있습니다.

  전체 볼륨을 복원하면 볼륨에 있는 모든 LUN과 파일이 교체됩니다. 스냅샷이 생성된 이후에 생성된 모든 새 LUN은 손실됩니다.

  LUN은 매핑, 일련 번호, UUID 및 영구 예약을 보유합니다.

ONTAP SnapVault 백업에서 읽기 전용 **LUN** 복사본에 액세스합니다

SnapVault 백업의 최신 스냅샷에서 LUN의 읽기 전용 복제본에 액세스할 수 있습니다. LUN ID, 경로 및 일련 번호는 소스 LUN과 다르며 먼저 매핑해야 합니다. 영구 예약, LUN 매핑 및 igroup은 SnapVault 2차 볼륨에 복제되지 않습니다.

시작하기 전에

- SnapVault 관계를 초기화해야 하며 SnapVault 2차 볼륨의 최신 스냅샷에 원하는 LUN이 포함되어 있어야 합니다.
- SnapVault 백업을 포함하는 SVM(스토리지 가상 머신)에는 LUN 복사본에 액세스하는 데 사용되는 호스트에서 액세스할 수 있는 원하는 SAN 프로토콜을 갖춘 하나 이상의 LIF가 있어야 합니다.
- SnapVault 2차 볼륨에서 LUN 복사본에 직접 액세스할 계획이라면 미리 SnapVault SVM에 igroup을 생성해야 합니다.

  먼저 LUN이 포함된 볼륨을 복원하거나 클론 복제하지 않고도 SnapVault 2차 볼륨에서 LUN에 직접 액세스할 수 있습니다.

이 작업에 대해

이전 스냅샷에서 매핑된 LUN이 있는 동안 새 스냅샷이 SnapVault 보조 볼륨에 추가되면 매핑된 LUN의 컨텐츠가 변경됩니다. LUN은 여전히 동일한 식별자로 매핑되지만 데이터는 새 스냅샷에서 가져옵니다. LUN 크기가 변경되면 일부 호스트는 자동으로 크기 변경을 감지합니다. 크기 변경을 확인하려면 Windows 호스트에서 디스크를 재검색해야 합니다.

단계

1. SnapVault 2차 볼륨에서 사용 가능한 LUN을 나열합니다.

   ```
   lun show
   ```

   이 예에서는 운영 볼륨의 원래 LUN과 SnapVault 보조 볼륨 dstvolB의 복제본을 모두 볼 수 있습니다.

```
cluster::> lun show

Vserver   Path                  State   Mapped   Type          Size
--------  ------------------    ------  -------  --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

에 대한 자세한 내용은 `lun show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 원하는 호스트의 igroup이 SnapVault 2차 볼륨이 포함된 SVM에 이미 없으면 igroup을 생성합니다.

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <ostype> -initiator <initiator_name>
```

이 명령은 iSCSI 프로토콜을 사용하는 Windows 호스트에 대한 igroup을 생성합니다.

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

3. 원하는 LUN 복사본을 igroup에 매핑합니다.

```
lun mapping create -vserver <SVM_name> -path <LUN_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
  -igroup temp_igroup
```

에 대한 자세한 내용은 `lun mapping create` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 호스트를 LUN에 연결하고 필요에 따라 LUN의 컨텐츠를 액세스합니다.

ONTAP SnapVault 백업에서 단일 **LUN**을 복원합니다

단일 LUN을 새 위치 또는 원래 위치로 복구할 수 있습니다. SnapVault 2차 볼륨의 모든

스냅샷에서 복원할 수 있습니다. LUN을 원래 위치로 복구하려면 먼저 LUN을 새 위치로 복원한 다음 복사합니다.

시작하기 전에

- SnapVault 관계를 초기화해야 하며 SnapVault 보조 볼륨에 복구할 적절한 스냅샷이 포함되어 있어야 합니다.
- SnapVault 2차 볼륨을 포함하는 SVM(스토리지 가상 머신)에는 LUN 복사본에 액세스하는 데 사용되는 호스트에서 액세스할 수 있는 원하는 SAN 프로토콜을 갖춘 하나 이상의 LIF가 있어야 합니다.
- SnapVault SVM에 igroup이 이미 있어야 합니다.

이 작업에 대해

이 프로세스에는 SnapVault 2차 볼륨의 스냅샷에서 읽기-쓰기 볼륨 클론 생성이 포함됩니다. 클론에서 LUN을 직접 사용하거나 필요에 따라 LUN 콘텐츠를 원래 LUN 위치로 다시 복제할 수 있습니다.

클론의 LUN의 경로와 일련 번호가 원래 LUN과 다릅니다. 영구 예약은 유지되지 않습니다.

단계

1. SnapVault 백업이 포함된 보조 볼륨을 확인합니다.

```
snapmirror show
```

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                         Snapmirrored
                                 Idle       -         true    -
```

2. LUN을 복구할 스냅샷을 식별합니다.

```
volume snapshot show
```

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

3. 원하는 스냅샷에서 읽기-쓰기 클론을 생성합니다

```
volume clone create -vserver <SVM_name> -flexclone <flexclone_name>
-type <type> -parent-volume <parent_volume_name> -parent-snapshot
<snapshot_name>
```

볼륨 클론은 SnapVault 백업과 동일한 애그리게이트에 생성됩니다. 클론을 저장할 공간이 Aggregate에 있어야 합니다.

```
cluster::> volume clone create -vserver vserverB
  -flexclone dstvolB_clone -type RW -parent-volume dstvolB
  -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. 볼륨 클론의 LUN을 나열합니다.

```
lun show -vserver <SVM_name> -volume <flexclone_volume_name>
```

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone

Vserver   Path                      State   Mapped   Type
--------- ------------------------  ------- -------- --------
vserverB  /vol/dstvolB_clone/lun_A  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_B  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_C  online  unmapped windows

3 entries were displayed.
```

에 대한 자세한 내용은 `lun show` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 원하는 호스트의 igroup이 SnapVault 백업이 포함된 SVM에 이미 없으면 igroup을 생성합니다.

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <os_type> -initiator <initiator_name>
```

이 예는 iSCSI 프로토콜을 사용하는 Windows 호스트에 대한 igroup을 생성합니다.

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

6. 원하는 LUN 복사본을 igroup에 매핑합니다.

```
lun mapping create -vserver <SVM_name> -path <lun_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB
  -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

에 대한 자세한 내용은 `lun mapping create` "ONTAP 명령 참조입니다"을 참조하십시오.

7. 호스트를 LUN에 연결하고 필요에 따라 LUN의 컨텐츠를 액세스합니다.

   LUN은 읽기/쓰기이며 원래 LUN 대신 사용할 수 있습니다. LUN 일련 번호가 다르므로 호스트는 이 일련 번호를 원본과 다른 LUN으로 해석합니다.

8. 호스트에서 복제 프로그램을 사용하여 LUN 컨텐츠를 원래 LUN에 다시 복제합니다.

관련 정보

- "스냅미러 쇼"

ONTAP SnapVault 백업에서 볼륨의 모든 **LUN**을 복원합니다

SnapVault 백업에서 볼륨에 있는 하나 이상의 LUN을 복원해야 하는 경우 전체 볼륨을 복원할 수 있습니다. 볼륨을 복원하면 볼륨의 모든 LUN에 영향을 줍니다.

시작하기 전에

SnapVault 관계를 초기화해야 하며 SnapVault 보조 볼륨에 복구할 적절한 스냅샷이 포함되어 있어야 합니다.

이 작업에 대해

전체 볼륨을 복원하면 볼륨이 스냅샷이 생성된 시점의 상태로 돌아갑니다. 스냅샷 후에 LUN이 볼륨에 추가된 경우 복구 프로세스 중에 해당 LUN이 제거됩니다.

볼륨을 복원한 후 LUN은 복원 직전에 매핑된 igroup에 계속 매핑됩니다. LUN 매핑은 스냅샷 시점의 매핑과 다를 수 있습니다. 호스트 클러스터의 LUN에 대한 영구 예약이 유지됩니다.

단계

1. 볼륨에 있는 모든 LUN에 대한 입출력을 중지합니다.
2. SnapVault 2차 볼륨이 포함된 2차 볼륨을 확인합니다.

```
snapmirror show
```

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                        Snapmirrored
                                Idle       -         true    -
```

3. 복원할 스냅샷을 식별합니다.

```
volume snapshot show
```

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

4. 사용할 스냅샷을 지정합니다.

```
snapmirror restore -destination-path <destination_path> -source-path
<source_path> -source-snapshot <snapshot_name>
```

복원을 위해 지정하는 대상은 복원 중인 원본 볼륨입니다.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. 호스트 클러스터에서 LUN을 공유하는 경우 영향을 받는 호스트에서 LUN의 영구 예약을 복원합니다.

SnapVault 백업에서 볼륨 복원

다음 예에서는 스냅샷이 생성된 후에 LUN_D라는 LUN이 볼륨에 추가되었습니다. 스냅샷에서 전체 볼륨을 복구한 후 LUN_D가 더 이상 나타나지 않습니다.

'lun show' 명령 출력에서 운영 볼륨의 srcvolA 및 SnapVault 보조 볼륨 dstvolB에서 해당 LUN의 읽기 전용 복제본을 확인할 수 있습니다. SnapVault 백업에는 LUN_D의 복제본이 없습니다.

```
cluster::> lun show
Vserver   Path                  State   Mapped   Type          Size
--------- ------------------    ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_D  online  mapped   windows  250.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

7 entries were displayed.

cluster::>snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB
  -source-snapshot daily.2013-02-10_0010

Warning: All data newer than snapshot hourly.2013-02-11_1205
on volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

cluster::> lun show
Vserver   Path                  State   Mapped   Type          Size
--------- ------------------    ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

SnapVault 보조 볼륨에서 볼륨을 복구한 후에는 소스 볼륨에 LUN_D가 더 이상 포함되지 않습니다 복구 후 소스 볼륨의 LUN은 여전히 매핑되므로 LUN을 다시 매핑할 필요가 없습니다.

관련 정보

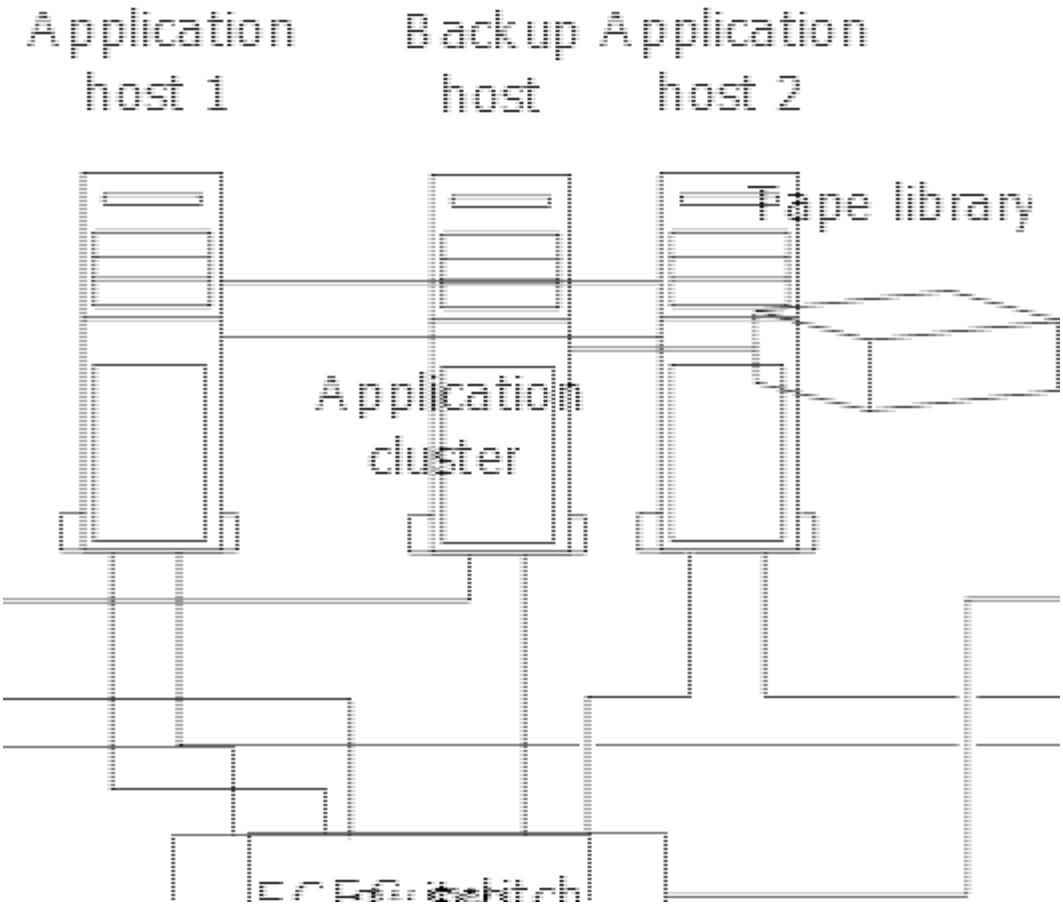
- "SnapMirror 복원"
- "스냅미러 쇼"

호스트 백업 시스템을 **ONTAP**에 연결하기 위한 권장 구성입니다

별도의 백업 호스트를 통해 SAN 시스템을 테이프로 백업하여 애플리케이션 호스트의 성능

저하를 방지할 수 있습니다.

백업을 위해 SAN 및 NAS 데이터를 별도로 유지해야 합니다. 아래 그림은 운영 스토리지 시스템에 대한 호스트 백업 시스템의 권장 물리적 구성을 보여 줍니다. 볼륨을 SAN 전용으로 구성해야 합니다. LUN은 단일 볼륨으로 제한하거나 여러 볼륨 또는 스토리지 시스템에 분산할 수 있습니다.



호스트의 볼륨은 스토리지 시스템에서 매핑된 단일 LUN 또는 HP-UX 시스템의 VxVM과 같은 볼륨 관리자를 사용하여 여러 LUN으로 구성될 수 있습니다.

호스트 백업 시스템을 사용하여 **ONTAP** 스토리지 시스템의 **LUN**을 보호합니다

스냅샷에서 클론 생성된 LUN을 호스트 백업 시스템의 소스 데이터로 사용할 수 있습니다.

시작하기 전에

운영 LUN이 존재하고 애플리케이션 서버의 WWPN 또는 이니시에이터 노드 이름을 포함하는 igroup에 매핑되어야 합니다. LUN도 포맷되고 호스트에서 액세스할 수 있어야 합니다

단계

1. 호스트 파일 시스템 버퍼의 내용을 디스크에 저장합니다.

   호스트 운영 체제에서 제공하는 명령을 사용하거나 SnapDrive for Windows 또는 SnapDrive for UNIX를 사용할 수 있습니다. 이 단계를 SAN 백업 사전 처리 스크립트의 일부로 지정할 수도 있습니다.

2. 운영 LUN의 스냅샷을 생성합니다.

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot> -comment <comment> -foreground false
```

3. 운영 LUN의 클론을 생성합니다.

```
volume file clone create -vserver <SMV_name> -volume <volume> -source
-path <path> -snapshot-name <snapshot> -destination-path
<destination_path>
```

4. 백업 서버의 WWPN을 포함하는 igroup을 생성합니다.

```
lun igroup create -vserver <SVM_name> -igroup <igroup> -protocol
<protocol> -ostype <os_type> -initiator <initiator>
```

5. 3단계에서 생성한 LUN 클론을 백업 호스트에 매핑합니다.

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup>
```

   이 단계를 SAN 백업 애플리케이션의 사후 처리 스크립트에 포함하도록 선택할 수 있습니다.

6. 호스트에서 새 LUN을 검색하고 호스트에서 파일 시스템을 사용할 수 있도록 설정합니다.

   이 단계를 SAN 백업 애플리케이션의 사후 처리 스크립트에 포함하도록 선택할 수 있습니다.

7. SAN 백업 애플리케이션을 사용하여 백업 호스트에서 테이프로 LUN 클론의 데이터를 백업합니다.
8. LUN 클론을 오프라인 상태로 전환합니다.

```
lun modify -vserver <SVM_name> -path <path> -state offline
```

9. LUN 클론을 제거합니다.

```
lun delete -vserver <SVM_name> -volume <volume> -lun <lun_name>
```

10. 스냅샷을 제거합니다.

```
volume snapshot delete -vserver <SVM_name> -volume <volume> -snapshot
<snapshot>
```

SAN 구성 참조

ONTAP SAN 구성에 대해 자세히 알아보십시오

SAN(Storage Area Network)은 iSCSI 또는 FC와 같은 SAN 전송 프로토콜을 통해 호스트에 연결된 스토리지 솔루션으로 구성됩니다. 스토리지 솔루션이 하나 이상의 스위치를 통해 호스트에 연결되도록 SAN을 구성할 수 있습니다. iSCSI를 사용하는 경우 스위치를 사용하지 않고 스토리지 솔루션을 호스트에 직접 연결하도록 SAN을 구성할 수도 있습니다.

SAN에서는 Windows, Linux 또는 UNIX와 같은 서로 다른 운영 체제를 사용하는 여러 호스트가 동시에 스토리지 솔루션에 액세스할 수 있습니다. 을 사용할 수 있습니다 "선택적 LUN 매핑" 및 "포트 세트" 호스트와 스토리지 간의 데이터 액세스를 제한합니다.

iSCSI의 경우 스토리지 솔루션과 호스트 간의 네트워크 토폴로지를 네트워크라고 합니다. FC, FC/NVMe 및 FCoE의 경우 스토리지 솔루션과 호스트 사이의 네트워크 토폴로지를 패브릭이라고 합니다. 데이터 액세스 손실로부터 시스템을 보호하는 이중화를 생성하려면 다중 네트워크 또는 다중 패브릭 구성에서 HA 쌍으로 SAN을 설정해야 합니다. 단일 노드 또는 단일 네트워크/패브릭을 사용하는 구성은 완전히 중복되지 않으므로 권장되지 않습니다.

SAN을 구성한 후 수행할 수 있습니다 "iSCSI 또는 FC용 스토리지를 프로비저닝합니다"또는 직접 할 수 있습니다 "FC/NVMe용 스토리지를 프로비저닝합니다". 그런 다음 호스트에 연결하여 데이터 서비스를 시작할 수 있습니다.

SAN 프로토콜 지원은 ONTAP 버전, 플랫폼 및 구성에 따라 다릅니다. 특정 구성에 대한 자세한 내용은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

관련 정보

- "SAN 관리 개요"
- "NVMe 구성, 지원 및 제한 사항"

iSCSI 구성

ONTAP 시스템으로 iSCSI 네트워크를 구성합니다

iSCSI SAN 호스트에 직접 연결하거나 하나 이상의 IP 스위치를 통해 호스트에 연결하는 고가용성(HA) 쌍을 사용하여 iSCSI 구성을 설정해야 합니다.

"HA 쌍" 는 호스트가 LUN을 액세스하는 데 사용할 Active/Optimized 및 Active/Unoptimized 경로에 대한 보고 노드로 정의됩니다. Windows, Linux 또는 UNIX와 같은 서로 다른 운영 체제를 사용하는 여러 호스트가 스토리지를 동시에 액세스할 수 있습니다. 호스트는 ALUA를 지원하는 지원되는 다중 경로 솔루션을 설치 및 구성해야 합니다. 지원되는 운영 체제 및 다중 경로 솔루션은 에서 확인할 수 있습니다 "NetApp 상호 운용성 매트릭스 툴".

다중 네트워크 구성에서는 호스트를 스토리지 시스템에 연결하는 스위치가 두 개 이상 있습니다. 다중 네트워크 구성은 완전히 중복되므로 권장됩니다. 단일 네트워크 구성에는 호스트를 스토리지 시스템에 연결하는 스위치 하나가 있습니다. 단일 네트워크 구성은 완전히 중복되지 않습니다.

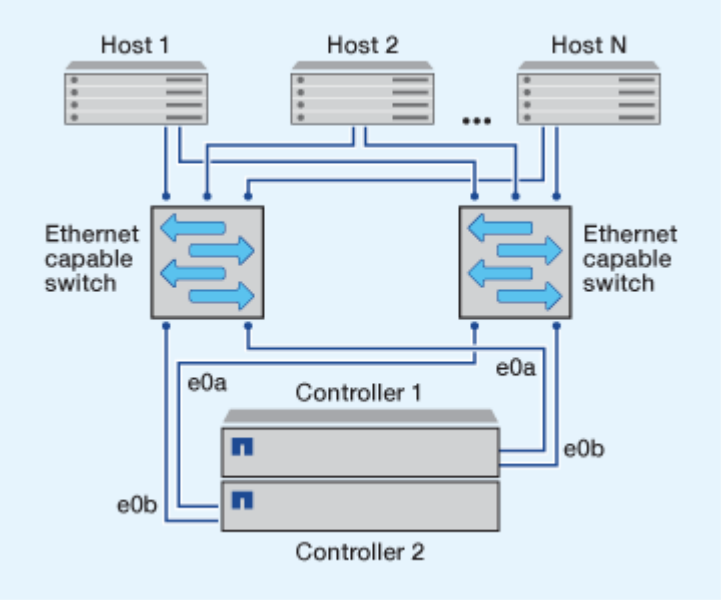
"단일 노드 구성" 내결함성 및 무중단 운영을 지원하는 데 필요한 이중화를 제공하지 않기 때문에 권장되지 않습니다.

관련 정보

- HA Pair 소유의 LUN에 액세스하는 데 사용되는 경로를 제한하는 방법에 대해 "선택적 LUN 매핑(SLM)"알아보십시오.
- 에 대해 자세히 알아보십시오 "SAN LIF".
- 에 대해 자세히 알아보십시오 "iSCSI에서 VLAN의 이점".

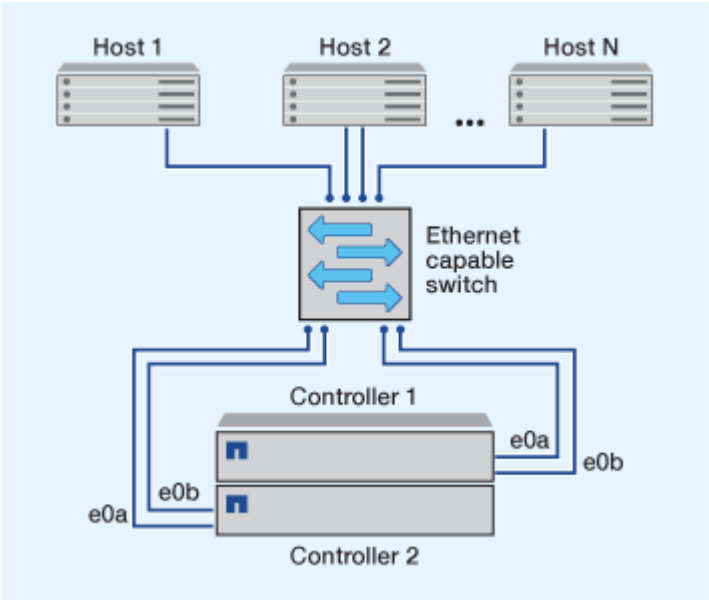
다중 네트워크 **iSCSI** 구성

다중 네트워크 HA 쌍 구성에서는 2개 이상의 스위치가 하나 이상의 호스트에 HA 쌍을 연결합니다. 스위치가 여러 개 있으므로 이 구성은 완전히 중복됩니다.



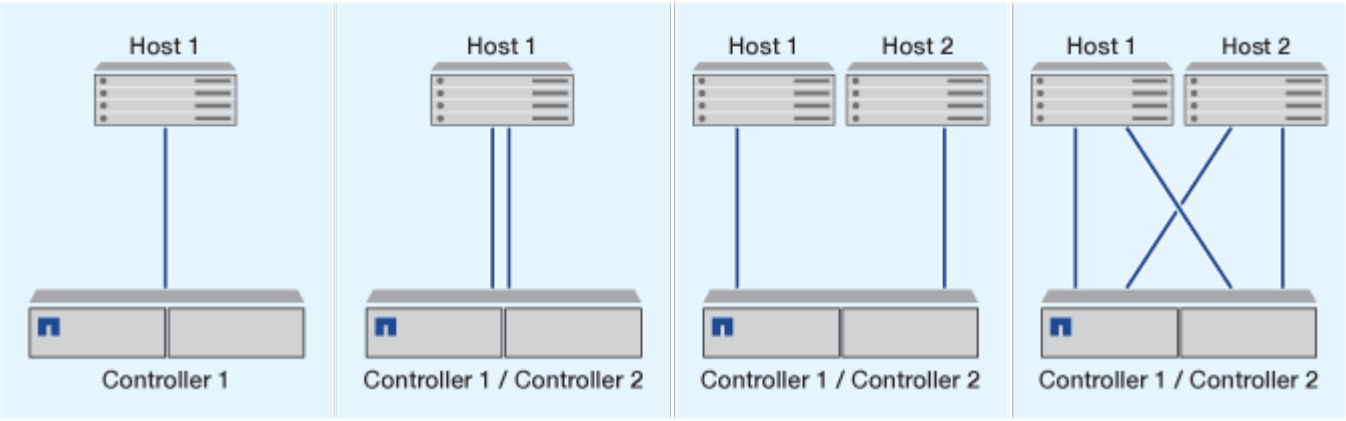
단일 네트워크 **iSCSI** 구성

단일 네트워크 HA Pair 구성에서 1개의 스위치는 HA 쌍을 하나 이상의 호스트에 연결합니다. 단일 스위치가 있으므로 이 구성은 완전히 중복되지 않습니다.



직접 연결 **iSCSI** 구성

직접 연결 구성에서는 하나 이상의 호스트가 컨트롤러에 직접 연결됩니다.



iSCSI 구성에서 **ONTAP** 시스템과 함께 **VLAN**을 사용할 때의 이점

VLAN은 브로드캐스트 도메인으로 그룹화된 스위치 포트 그룹으로 구성됩니다. VLAN은 단일 스위치에 있거나 여러 스위치 섀시에 걸쳐 있을 수 있습니다. 정적 및 동적 VLAN을 사용하면 IP 네트워크 인프라 내에서 보안을 강화하고, 문제를 격리하고, 사용 가능한 경로를 제한할 수 있습니다.

대규모 IP 네트워크 인프라에서 VLAN을 구현할 경우 다음과 같은 이점을 얻을 수 있습니다.

- 보안 강화:

  VLAN을 사용하면 이더넷 네트워크 또는 IP SAN의 여러 노드 간 액세스를 제한하므로 기존 인프라를 활용하는 동시에 보안을 강화할 수 있습니다.

- 문제를 격리하여 이더넷 네트워크 및 IP SAN 안정성 향상
- 문제 공간을 제한하여 문제 해결 시간 단축
- 특정 iSCSI 타겟 포트에 대한 사용 가능한 경로 수 감소
- 호스트에서 사용하는 최대 경로 수 감소

  경로가 너무 많으면 재연결 시간이 느려집니다. 호스트에 다중 경로 솔루션이 없는 경우 VLAN을 사용하여 하나의 경로만 허용할 수 있습니다.

동적 **VLAN**

동적 VLAN은 MAC 주소를 기반으로 합니다. 포함할 멤버의 MAC 주소를 지정하여 VLAN을 정의할 수 있습니다.

동적 VLAN은 유연성을 제공하며 장치가 물리적으로 스위치에 연결되어 있는 물리적 포트에 매핑하지 않아도 됩니다. VLAN을 재구성하지 않고도 한 포트에서 다른 포트로 케이블을 이동할 수 있습니다.

정적 **VLAN**

정적 VLAN은 포트 기반입니다. 스위치 및 스위치 포트는 VLAN 및 해당 구성원을 정의하는 데 사용됩니다.

정적 VLAN은 MAC(Media Access Control) 스푸핑을 사용하여 VLAN을 위반할 수 없기 때문에 보안이 향상됩니다. 그러나 다른 사람이 스위치에 물리적으로 액세스할 수 있는 경우 케이블을 교체하고 네트워크 주소를 다시 구성하면 액세스가 허용됩니다.

일부 환경에서는 동적 VLAN보다 정적 VLAN을 쉽게 생성하고 관리할 수 있습니다. 정적 VLAN은 48비트 MAC 주소 대신 스위치 및 포트 식별자만 지정할 수 있기 때문입니다. 또한 스위치 포트 범위에 VLAN 식별자를 사용하여 레이블을 지정할 수 있습니다.

FC 구성

ONTAP 시스템으로 FC 또는 FC-NVMe 패브릭을 구성합니다

HA 쌍과 최소 2개의 스위치를 사용하여 FC 및 FC-NVMe SAN 호스트를 구성하는 것이 좋습니다. 따라서 패브릭 및 스토리지 시스템 계층에서 이중화를 제공하여 내결함성과 무중단 운영을 지원합니다. 스위치를 사용하지 않고 FC 또는 FC-NVMe SAN 호스트를 HA 쌍에 직접 연결할 수 없습니다.

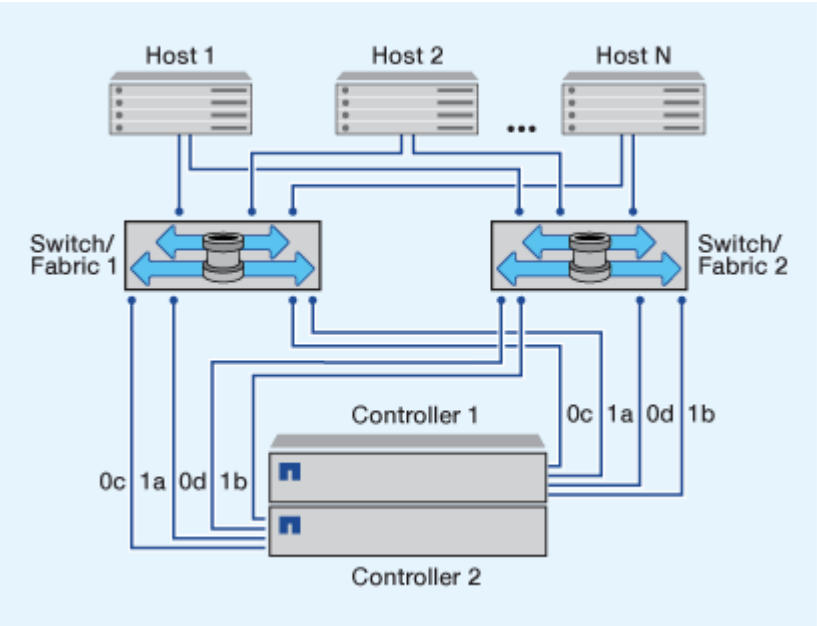
캐스케이드, 부분 메시, 풀 메시, 코어 에지 및 디렉터 패브릭은 모두 FC 스위치를 패브릭에 연결하는 업계 표준 방법이며 모두 지원됩니다. 임베디드 블레이드 스위치의 경우를 제외하고 이기종 FC 스위치 패브릭을 사용할 수 없습니다. 특정 예외는 에 나열되어 있습니다 "상호 운용성 매트릭스 툴". 패브릭은 하나 또는 여러 개의 스위치로 구성될 수 있으며, 스토리지 컨트롤러를 여러 스위치에 연결할 수 있습니다.

Windows, Linux 또는 UNIX와 같은 서로 다른 운영 체제를 사용하는 여러 호스트가 스토리지 컨트롤러에 동시에 액세스할 수 있습니다. 호스트에서는 지원되는 다중 경로 솔루션을 설치하고 구성해야 합니다. 지원되는 운영 체제 및 다중 경로 솔루션은 상호 운용성 매트릭스 툴에서 확인할 수 있습니다.

Multifabric FC 및 FC-NVMe 구성

멀티패브릭 HA 쌍 구성에서는 HA 쌍을 하나 이상의 호스트에 연결하는 스위치가 2개 이상 있습니다. 다음 멀티 패브릭 HA 쌍 그림은 2개의 패브릭만 보여주지만, 모든 멀티 패브릭 구성에 2개 이상의 패브릭을 사용할 수 있습니다.

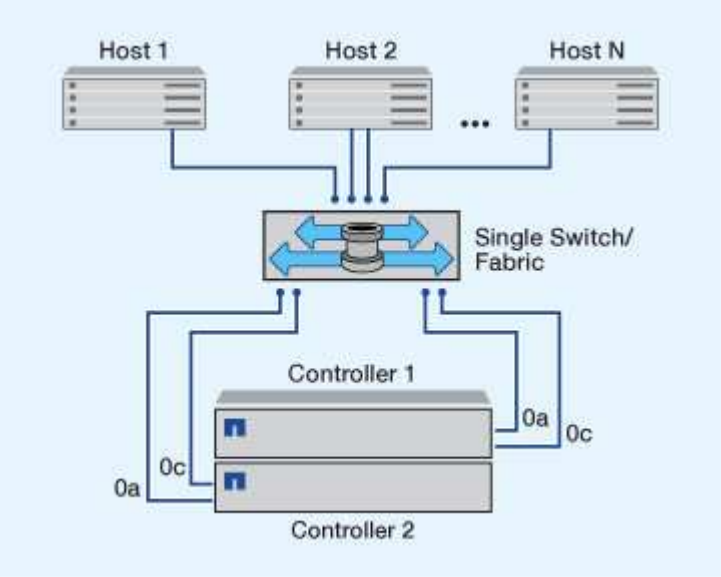
그림에 표시된 FC 대상 포트 번호(0c, 0d, 1a, 1b)가 예시입니다. 실제 포트 번호는 스토리지 노드의 모델 및 확장 어댑터를 사용하고 있는지에 따라 다릅니다.



단일 패브릭 HA 쌍 구성에서는 HA 쌍의 두 컨트롤러를 하나 이상의 호스트에 연결하는 하나의 패브릭이 있습니다. 호스트와 컨트롤러가 단일 스위치를 통해 연결되므로 단일 패브릭 HA 쌍 구성은 완전히 이중화되지 않습니다.

그림에 표시된 FC 타겟 포트 번호(0a, 0c)가 예입니다. 실제 포트 번호는 스토리지 노드의 모델 및 확장 어댑터를 사용하고 있는지에 따라 다릅니다.

FC 구성을 지원하는 모든 플랫폼은 단일 패브릭 HA 쌍 구성을 지원합니다.



"단일 노드 구성" 내결함성 및 무중단 운영을 지원하는 데 필요한 이중화를 제공하지 않기 때문에 권장되지 않습니다.

관련 정보

- HA Pair 소유의 LUN에 액세스하는 데 사용되는 경로를 제한하는 방법에 대해 "선택적 LUN 매핑(SLM)"알아보십시오.
- 에 대해 자세히 알아보십시오 "SAN LIF".

ONTAP 시스템으로 **FC** 스위치를 구성하는 모범 사례

최상의 성능을 얻으려면 FC 스위치를 구성할 때 특정 모범 사례를 고려해야 합니다.

고정 링크 속도 설정은 FC 스위치 구성의 모범 사례이며, 특히 대규모 패브릭의 경우 패브릭 리빌드에 최고의 성능을 제공하고 시간을 크게 단축할 수 있기 때문에 그렇습니다. 자동 협상은 유연성이 높지만 FC 스위치 구성이 예전처럼 수행하지 않기 때문에 전체적인 패브릭 구성 시퀀스의 시간이 길어집니다.

Fabric에 연결된 모든 스위치는 NPIV(N_Port ID Virtualization)를 지원해야 하며 NPIV를 설정해야 합니다. ONTAP는 NPIV를 사용하여 패브릭에 FC 대상을 제공합니다.

지원되는 환경에 대한 자세한 내용은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

FC 및 iSCSI 모범 사례는 를 참조하십시오 "NetApp 기술 보고서 4080: 최신 SAN에 대한 모범 사례".

ONTAP 시스템에 권장되는 FC 타겟 포트 구성 및 속도

FC 타겟 포트는 FC 프로토콜에 대해 구성 및 사용되는 것과 정확히 동일한 방법으로 FC-NVMe 프로토콜에 대해 구성하고 사용할 수 있습니다. FC-NVMe 프로토콜에 대한 지원은 사용하는 플랫폼과 ONTAP 버전에 따라 다릅니다. NetApp Hardware Universe를 사용하여 지원을 확인합니다.

최상의 성능과 가용성을 얻으려면 특정 플랫폼에 대해 에 나와 있는 권장 대상 포트 구성을 사용해야 "NetApp Hardware Universe를 참조하십시오" 합니다.

공유 ASIC를 통한 FC 타겟 포트 구성

다음 플랫폼에는 공유 ASIC(Application-Specific Integrated Circuits)와 포트 쌍이 있습니다. 확장 어댑터를 이러한 플랫폼에 사용할 경우 연결에 동일한 ASIC를 사용하지 않도록 FC 포트를 구성해야 합니다.

컨트롤러	공유 ASIC가 있는 포트 쌍	대상 포트 수: 권장 포트 수
• FAS8200를 참조하십시오 • AFF A300	0g + 0h	1:0g 2:0g, 0h
• FAS2720 • FAS2750 • AFF A220	0C+0d 0e+0f	1:0c 2:0c, 0e 3:0c, 0e, 0d 4:0c, 0e, 0d, 0f

FC 타겟 포트의 지원 속도입니다

FC 타겟 포트는 다른 속도로 실행되도록 구성할 수 있습니다. 지정된 호스트에서 사용하는 모든 타겟 포트는 동일한 속도로 설정되어야 합니다. 대상 포트 속도를 연결할 장치의 속도와 일치하도록 설정해야 합니다. 포트 속도에 자동 협상을 사용하지 마십시오. autonegotiation으로 설정된 포트는 Takeover/Giveback 또는 기타 중단 후 다시 연결하는 데 더 오래 걸릴 수 있습니다.

다음과 같은 속도로 실행되도록 온보드 포트 및 확장 어댑터를 구성할 수 있습니다. 필요에 따라 각 컨트롤러 및 확장 어댑터 포트를 각기 다른 속도로 구성할 수 있습니다.

4Gb 포트	8Gb 포트	16Gb 포트	32 Gb 포트
• 4Gb • 2Gb • 1Gb	• 8Gb • 4Gb • 2Gb	• 16Gb • 8Gb • 4Gb	• 32Gb • 16Gb • 8Gb

지원되는 어댑터 및 지원되는 속도의 전체 목록은 를 참조하십시오 "NetApp Hardware Universe를 참조하십시오".

ONTAP FC 어댑터 포트를 구성합니다

온보드 FC 어댑터 및 일부 FC 확장 어댑터 카드는 이니시에이터 또는 대상 포트로 개별적으로 구성할 수 있습니다. 다른 FC 확장 어댑터는 출고 시 이니시에이터 또는 대상으로 구성되므로 변경할 수 없습니다. FC SFP+ 어댑터로 구성된 지원 UTA2 카드를 통해서도 추가 FC 포트를

사용할 수 있습니다.

이니시에이터 포트를 사용하여 백엔드 디스크 쉘프 및 외부 스토리지 어레이에 직접 연결할 수 있습니다. 타겟 포트는 FC 스위치에만 연결할 수 있습니다.

FC용으로 구성된 온보드 포트 및 CNA/UTA2 포트의 수는 컨트롤러의 모델에 따라 다릅니다. 지원되는 타겟 확장 어댑터도 컨트롤러 모델에 따라 다릅니다. 컨트롤러 모델에 지원되는 온보드 FC 포트 및 타겟 확장 어댑터의 전체 목록은 를 참조하십시오"NetApp Hardware Universe를 참조하십시오".

이니시에이터 모드에 맞게 **FC** 어댑터를 구성합니다

이니시에이터 모드는 외부 LUN 가져오기(FLI)를 통해 포트를 테이프 드라이브, 테이프 라이브러리 또는 타사 스토리지에 연결하는 데 사용됩니다.

시작하기 전에

- 어댑터에 있는 LIF는 해당 LIF가 구성원인 포트 세트에서 제거해야 합니다.
- 물리적 포트의 속성을 타겟에서 이니시에이터로 변경하기 전에 수정할 물리적 포트를 사용하는 모든 SVM(스토리지 가상 머신)의 모든 LIF를 마이그레이션 또는 제거해야 합니다.

NVMe/FC는 이니시에이터 모드를 지원합니다.

단계

1. 어댑터에서 모든 LIF를 제거합니다.

```
network interface delete -vserver _SVM_name_ -lif _lif_name_,_lif_name_
```

2. 어댑터를 오프라인 상태로 전환:

```
network fcp adapter modify -node _node_name_ -adapter _adapter_port_
-status-admin down
```

어댑터가 오프라인 상태가 되지 않으면 시스템의 해당 어댑터 포트에서 케이블을 분리할 수도 있습니다.

3. 어댑터를 타겟에서 이니시에이터로 변경합니다.

```
system hardware unified-connect modify -t initiator _adapter_port_
```

4. 변경한 어댑터를 호스팅하는 노드를 재부팅합니다.
5. FC 포트가 구성에 맞는 올바른 상태로 구성되었는지 확인합니다.

```
system hardware unified-connect show
```

6. 어댑터를 다시 온라인으로 전환합니다.

```
node run -node _node_name_ storage enable adapter _adapter_port_
```

FC 어댑터를 타겟 모드로 구성합니다

타겟 모드는 포트를 FC 이니시에이터에 연결하는 데 사용됩니다.

FC 프로토콜 및 FC-NVMe 프로토콜에 사용할 FC 어댑터를 구성하는 데 동일한 단계가 사용됩니다. 하지만 특정 FC 어댑터만 FC-NVMe를 지원합니다. FC-NVMe 프로토콜을 지원하는 어댑터 목록은 를 참조하십시오"NetApp Hardware Universe를 참조하십시오".

단계

1. 어댑터를 오프라인 상태로 전환:

```
node run -node _node_name_ storage disable adapter _adapter_name_
```

   어댑터가 오프라인 상태가 되지 않으면 시스템의 해당 어댑터 포트에서 케이블을 분리할 수도 있습니다.

2. 어댑터를 이니시에이터에서 타겟으로 변경합니다.

```
system node hardware unified-connect modify -t target -node _node_name_
adapter _adapter_name_
```

3. 변경한 어댑터를 호스팅하는 노드를 재부팅합니다.
4. 타겟 포트의 구성이 올바른지 확인합니다.

```
network fcp adapter show -node _node_name_
```

5. 어댑터를 온라인으로 전환합니다.

```
network fcp adapter modify -node _node_name_ -adapter _adapter_port_
-state up
```

FC 어댑터 속도를 구성합니다

자동 협상을 사용하는 대신 어댑터 대상 포트 속도를 연결할 장치의 속도와 일치하도록 구성해야 합니다. autonegotiation으로 설정된 포트는 Takeover/Giveback 또는 기타 중단 후 다시 연결하는 데 더 오랜 시간이 걸릴 수 있습니다.

이 작업에 대해

이 작업에는 클러스터의 모든 SVM(Storage Virtual Machine)과 모든 LIF가 포함되므로 이 작업의 범위를 제한하려면 '-home-port' 및 '-home-lif' 매개 변수를 사용해야 합니다. 이러한 매개 변수를 사용하지 않으면 클러스터에 있는 모든 LIF에 작업이 적용되며, 이는 바람직하지 않을 수 있습니다.

시작하기 전에

이 어댑터를 홈 포트로 사용하는 모든 LIF는 오프라인 상태여야 합니다.

단계

1. 이 어댑터의 모든 LIF를 오프라인 상태로 전환:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin down
```

2. 어댑터를 오프라인 상태로 전환:

```
network fcp adapter modify -node node1 -adapter 0c -state down
```

어댑터가 오프라인 상태가 되지 않으면 시스템의 해당 어댑터 포트에서 케이블을 분리할 수도 있습니다.

3. 포트 어댑터의 최대 속도를 확인합니다.

```
fcp adapter show -instance
```

어댑터 속도를 최대 속도 이상으로 수정할 수 없습니다.

4. 어댑터 속도를 변경합니다.

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```

5. 어댑터를 온라인으로 전환합니다.

```
network fcp adapter modify -node node1 -adapter 0c -state up
```

6. 어댑터에 있는 모든 LIF를 온라인으로 전환합니다.

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin up
```

FC 어댑터를 관리하기 위한 **ONTAP** 명령입니다

FC 명령을 사용하여 스토리지 컨트롤러에 대한 FC 타겟 어댑터, FC 이니시에이터 어댑터 및 온보드 FC 어댑터를 관리할 수 있습니다. FC 프로토콜과 FC-NVMe 프로토콜을 위해 FC 어댑터를 관리하는 데 동일한 명령이 사용됩니다.

FC 이니시에이터 어댑터 명령은 노드 레벨에서만 작동합니다. FC Initiator Adapter 명령을 사용하려면 먼저 'run-node_node_name_' 명령을 사용해야 합니다.

FC 타겟 어댑터를 관리하는 명령입니다

원하는 작업	이 명령 사용...
노드에 FC 어댑터 정보를 표시합니다	네트워크 FCP 어댑터가 표시됩니다
FC 타겟 어댑터 매개 변수를 수정합니다	네트워크 FCP 어댑터 수정
FC 프로토콜 트래픽 정보를 표시합니다	'run-node_node_name_sysstat -f'
FC 프로토콜이 실행된 시간을 표시합니다	'run-node_node_name_uptime'
어댑터 구성 및 상태를 표시합니다	'run-node_node_name_sysconfig-v_adapter_'
설치된 확장 카드와 구성 오류가 있는지 확인합니다	'run-node_node_name_sysconfig-ac'
명령에 대한 man 페이지를 봅니다	man command_name'입니다

FC 이니시에이터 어댑터를 관리하는 명령입니다

원하는 작업	이 명령 사용...
노드의 모든 이니시에이터 및 해당 어댑터에 대한 정보를 표시합니다	'run-node_node_name_storage show adapter'입니다
어댑터 구성 및 상태를 표시합니다	'run-node_node_name_sysconfig-v_adapter_'
설치된 확장 카드와 구성 오류가 있는지 확인합니다	'run-node_node_name_sysconfig-ac'

온보드 **FC** 어댑터를 관리하는 명령입니다

원하는 작업	이 명령 사용...
온보드 FC 포트의 상태를 표시합니다	'시스템 노드 하드웨어 통합 접속 쇼

관련 정보

- "네트워크 FCP 어댑터"

X1133A-R6 어댑터를 사용하는 **ONTAP** 시스템에 대한 연결 손실을 방지합니다

별도의 X1133A-R6 HBA에 대한 중복 경로를 사용하여 시스템을 구성하면 포트 장애 시 연결이 끊어지지 않습니다.

X1133A-R6 HBA는 2개의 2포트 쌍으로 구성된 4포트, 16Gb FC 어댑터입니다. X1133A-R6 어댑터는 타겟 모드 또는 이니시에이터 모드로 구성할 수 있습니다. 각 2포트 쌍은 단일 ASIC에서 지원됩니다(예: ASIC 1의 포트 1과 포트 2, ASIC 2의 포트 3과 포트 4). 단일 ASIC의 두 포트는 타겟 모드나 이니시에이터 모드에서 동일한 모드로 작동하도록 구성해야 합니다. ASIC에서 쌍을 지원하는 데 오류가 발생하면 페어의 두 포트가 모두 오프라인 상태가 됩니다.

이러한 접속 구성 손실을 방지하려면 X1133A-R6 HBA를 분리하는 이중 경로 또는 HBA의 다른 ASIC에서 지원되는 포트에 대한 이중 경로를 사용하여 시스템을 구성합니다.

FCoE 구성

ONTAP 시스템으로 FCoE 패브릭을 구성합니다

FCoE는 다양한 방법으로 FCoE 스위치를 사용하여 구성할 수 있습니다. 직접 연결 구성은 FCoE에서 지원되지 않습니다.

모든 FCoE 구성은 이중 패브릭이며 완전히 이중화되며 호스트측 다중 경로 소프트웨어가 필요합니다. 모든 FCoE 구성에서는 이니시에이터와 타겟 사이의 경로에 최대 홉 수 제한까지 여러 FCoE 및 FC 스위치를 포함할 수 있습니다. 스위치를 서로 연결하려면 스위치가 이더넷 ISL을 지원하는 펌웨어 버전을 실행해야 합니다. 모든 FCoE 구성의 각 호스트는 다른 운영 체제로 구성할 수 있습니다.

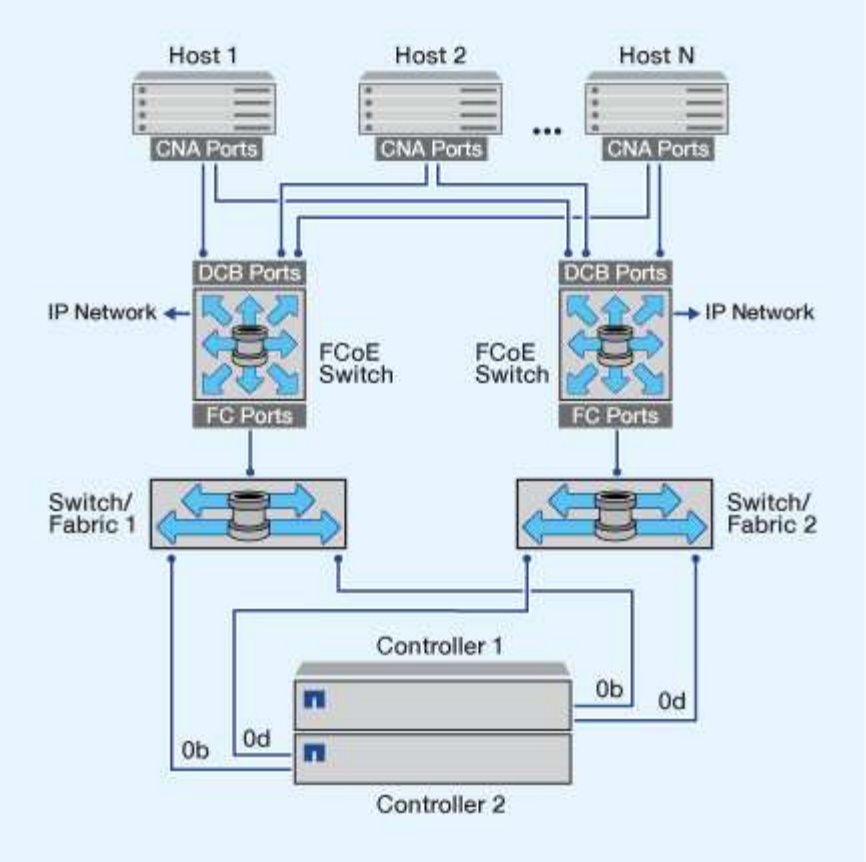
FCoE 구성에는 FCoE 기능을 명시적으로 지원하는 이더넷 스위치가 필요합니다. FCoE 구성은 FC 스위치와 동일한 상호 운용성 및 품질 보증 프로세스를 통해 검증되었습니다. 지원되는 구성은 상호 운용성 매트릭스 에 나와 있습니다. 이러한 지원되는 구성에 포함된 매개 변수 중 일부는 스위치 모델, 단일 Fabric에 구축할 수 있는 스위치 수 및 지원되는 스위치 펌웨어 버전입니다.

그림에 나와 있는 FC 타겟 확장 어댑터 포트 번호의 예가 나와 있습니다. 실제 포트 번호는 FCoE 대상 확장 어댑터가 설치된 확장 슬롯에 따라 다를 수 있습니다.

FCoE 이니시에이터에서 FC 타겟으로

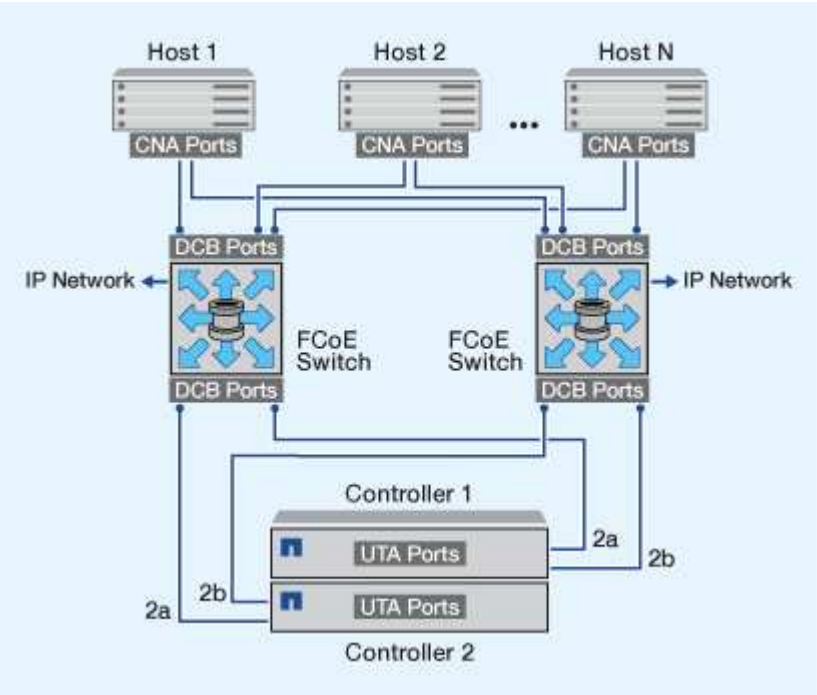
CNA(FCoE 이니시에이터)를 사용하면 FCoE 스위치를 FC 타겟 포트에 연결하여 HA 쌍의 두 컨트롤러에 호스트를 연결할 수 있습니다. FCoE 스위치에도 FC 포트가 있어야 합니다. 호스트 FCoE 이니시에이터는 항상 FCoE 스위치에 연결됩니다. FCoE 스위치는 FC 타겟에 직접 연결하거나 FC 스위치를 통해 FC 타겟에 연결할 수 있습니다.

다음 그림에서는 FCoE 스위치에 연결된 호스트 CNA와 HA 쌍에 연결하기 전에 FC 스위치에 연결하는 방법을 보여 줍니다.



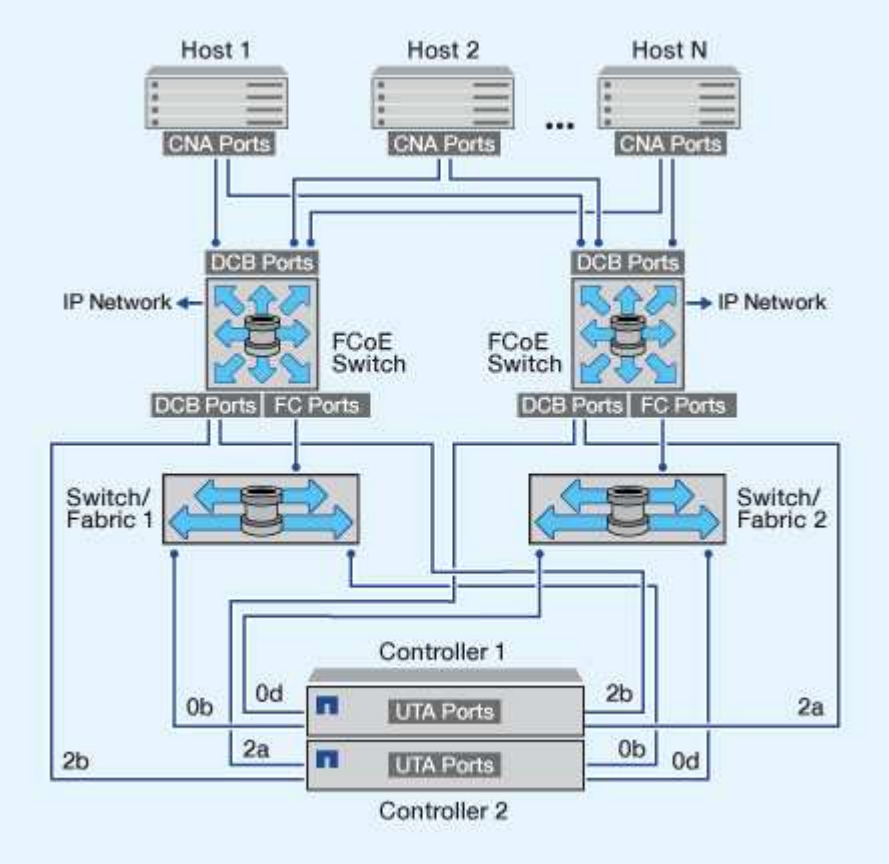
FCoE 이니시에이터에서 **FCoE** 타겟으로

CNA(호스트 FCoE 이니시에이터)를 사용하면 HA 쌍의 두 컨트롤러에 호스트를 FCoE 스위치를 통해 FCoE 타겟 포트(UTA 또는 UTA2)에 연결할 수 있습니다.



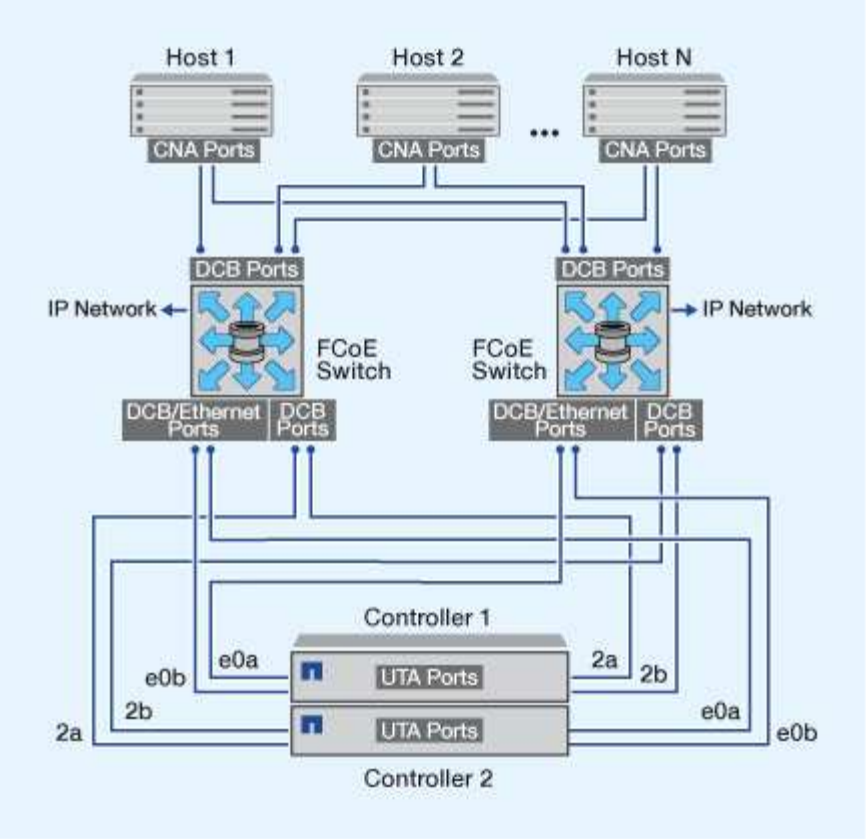
FCoE 이니시에이터에서 **FCoE** 및 **FC** 타겟으로

CNA(호스트 FCoE 이니시에이터)를 사용하면 HA 쌍의 두 컨트롤러에 호스트를 FCoE 스위치를 통해 FCoE 및 FC 타겟 포트(UTA 또는 UTA2)에 연결할 수 있습니다.



IP 스토리지 프로토콜과 혼합된 **FCoE**

CNA(호스트 FCoE 이니시에이터)를 사용하면 HA 쌍의 두 컨트롤러에 호스트를 FCoE 스위치를 통해 FCoE 타겟 포트(UTA 또는 UTA2)에 연결할 수 있습니다. FCoE 포트는 단일 스위치에 대한 기존 링크 집계를 사용할 수 없습니다. Cisco 스위치는 FCoE를 지원하는 특수한 유형의 Link Aggregation(가상 포트 채널)을 지원합니다. 가상 포트 채널은 두 스위치에 대한 개별 링크를 집계합니다. 다른 이더넷 트래픽에 가상 포트 채널을 사용할 수도 있습니다. NFS, SMB, iSCSI 및 기타 이더넷 트래픽을 포함하여 FCoE 이외의 트래픽에 사용되는 포트는 FCoE 스위치에서 일반 이더넷 포트를 사용할 수 있습니다.



ONTAP는 **FCoE** 이니시에이터 및 타겟 포트 조합을 지원합니다

FCoE와 기존 FC Initiator와 타겟의 특정 조합이 지원됩니다.

FCoE 이니시에이터

호스트 컴퓨터에서 FCoE 이니시에이터와 스토리지 컨트롤러의 기존 FC 타겟을 모두 사용할 수 있습니다. 호스트 FCoE 초기자는 FCoE DCB(데이터 센터 브리징) 스위치에 연결해야 합니다. 대상에 대한 직접 연결은 지원되지 않습니다.

다음 표에는 지원되는 조합이 나와 있습니다.

이니시에이터	타겟	지원 여부
FC	FC	예
FC	FCoE 를 참조하십시오	예
FCoE 를 참조하십시오	FC	예
FCoE 를 참조하십시오	FCoE 를 참조하십시오	예

FCoE 타겟

FC 포트가 추가 대상 어댑터인지 온보드 포트인지에 관계없이 스토리지 컨트롤러의 4Gb, 8Gb 또는 16Gb FC 포트와 FCoE 타겟 포트를 혼합할 수 있습니다. 동일한 스토리지 컨트롤러에 FCoE 및 FC 타겟 어댑터를 둘 다 사용할 수

있습니다.

온보드 및 확장 FC 포트의 결합에 대한 규칙이 계속 적용됩니다.

FC 및 FCoE 조닝

ONTAP 시스템을 통한 **FC** 및 **FCoE** 조닝에 대해 알아보십시오

FC, FC-NVMe 또는 FCoE 존은 패브릭 내 하나 이상의 포트를 논리적으로 그룹화한 것입니다. 장치가 서로 보고, 연결하고, 세션을 만들고, 통신할 수 있으려면 두 포트가 모두 같은 존의 구성원이어야 합니다.

조닝을 사용하면 공통 영역을 공유하는 엔드 포인트에 대한 액세스 및 연결을 제한하여 보안을 강화할 수 있습니다. 같은 존에 없는 포트는 서로 통신할 수 없습니다. 이렇게 하면 이니시에이터 HBA 간의 _crosstalk_가 감소되거나 제거됩니다. 연결 문제가 발생할 경우 조닝(zoning)을 통해 문제를 특정 포트 세트로 격리하여 해결 시간을 단축할 수 있습니다.

조닝으로 인해 특정 포트에 대해 사용 가능한 경로 수가 감소하고 호스트와 스토리지 시스템 사이의 경로 수가 감소합니다. 예를 들어, 일부 호스트 OS 다중 경로 솔루션에는 관리 가능한 경로 수에 제한이 있습니다. 조닝을 통해 호스트에 표시되는 경로 수를 줄일 수 있으므로 호스트에 대한 경로가 호스트 운영 체제에서 허용하는 최대 경로를 초과하지 않도록 할 수 있습니다.

World Wide Name 기반 조닝

WWN(World Wide Name)을 기반으로 하는 조닝은 영역 내에 포함할 구성원의 WWN을 지정합니다. 일부 스위치 공급업체에서는 WWNN(World Wide Node Name) 조닝을 사용할 수 있지만, ONTAP에서 조닝(Zoning)을 사용하면 WWPN(World Wide Port Name) 조닝을 사용해야 합니다.

특정 포트를 올바르게 정의하고 NPIV를 효과적으로 사용하려면 WWPN 조닝이 필요합니다. FC 스위치는 노드에 있는 물리적 포트의 WWPN이 아니라 대상 LIF(논리 인터페이스)의 WWPN을 사용하여 조닝되어야 합니다. 물리적 포트의 WWPN은 ""50"으로 시작하고 LIF의 WWPN은 ""20"으로 시작합니다.

WWPN 조닝을 사용하면 디바이스가 Fabric에 물리적으로 연결된 위치에 따라 액세스가 결정되지 않으므로 유연성이 제공됩니다. 영역을 재구성하지 않고도 한 포트에서 다른 포트로 케이블을 이동할 수 있습니다.

ONTAP 시스템에 권장되는 **FC** 및 **FCoE** 조닝 구성

호스트에 경로 다중화 솔루션이 설치되어 있지 않거나, 네 개 이상의 호스트가 SAN에 연결되어 있거나, 선택적 LUN 매핑이 클러스터의 노드에 구현되지 않은 경우 조닝 구성을 생성해야 합니다.

권장 FC 및 FCoE 조닝 구성에서 각 존에는 이니시에이터 포트와 하나 이상의 타겟 LIF가 포함됩니다. 이렇게 구성하면 각 호스트 이니시에이터가 모든 노드에 액세스할 수 있고 동일한 노드에 액세스하는 호스트가 서로의 포트를 볼 수 없습니다

호스트 이니시에이터가 있는 존에 스토리지 가상 머신(SVM)의 모든 LIF를 추가합니다. 따라서 기존 영역을 편집하거나 새 영역을 생성하지 않고 볼륨 또는 LUN을 이동할 수 있습니다.

이중 패브릭 조닝 구성

이중 패브릭 조닝 구성은 단일 구성 요소 장애로 인한 데이터 손실을 방지하기 위해 권장됩니다. 이중 패브릭 구성에서

각 호스트 이니시에이터는 다양한 스위치를 사용하여 클러스터의 각 노드에 연결됩니다. 하나의 스위치를 사용할 수 없게 되더라도 나머지 스위치를 통해 데이터 액세스가 유지됩니다. 다중 경로를 관리하려면 호스트에 다중 경로 소프트웨어가 필요합니다.

다음 그림에서는 두 개의 이니시에이터가 있고 다중 경로 소프트웨어가 실행 중인 호스트를 보여 줍니다. 두 개의 구역이 있습니다. "선택적 LUN 매핑(SLM)" 모든 노드가 보고 노드로 간주되도록 구성됩니다.

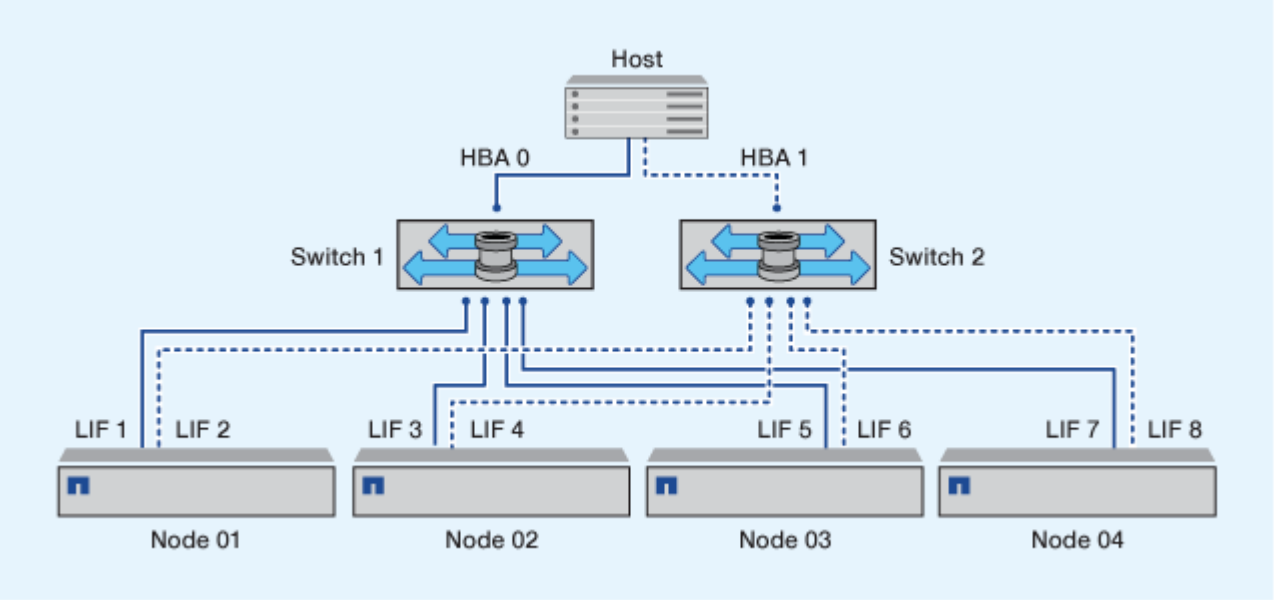
이 그림에 사용된 명명 규칙은 ONTAP 솔루션에 사용할 수 있는 명명 규칙 중 하나에 불과합니다.

- 존 1: HBA 0, LIF_1, LIF_3, LIF_5 및 LIF_7
- 구역 2: HBA 1, LIF_2, LIF_4, LIF_6 및 LIF_8

각 호스트 이니시에이터는 다른 스위치를 통해 조닝됩니다. 구역 1은 스위치 1을 통해 액세스합니다. 구역 2는 스위치 2를 통해 액세스합니다.

각 호스트는 모든 노드의 LIF에 액세스할 수 있습니다. 따라서 노드에 장애가 발생하더라도 호스트가 LUN에 액세스할 수 있습니다. SVM은 SLM 보고 노드 구성을 기반으로 클러스터의 모든 노드에서 모든 iSCSI 및 FC LIF에 액세스할 수 있습니다. SLM, 포트 세트 또는 FC 스위치 조닝을 사용하여 SVM에서 호스트로의 경로 수와 SVM에서 LUN으로의 경로 수를 줄일 수 있습니다.

구성에 더 많은 노드가 포함된 경우, 추가 노드의 LIF가 이 영역에 포함됩니다.



호스트 운영 체제 및 다중 경로 소프트웨어는 노드의 LUN에 액세스하는 데 사용되는 경로 수를 지원해야 합니다.

단일 패브릭 조닝

단일 패브릭 구성에서는 단일 스위치를 통해 각 호스트 이니시에이터를 각 스토리지 노드에 연결합니다. 단일 패브릭 조닝 구성은 단일 구성 요소 장애로 인한 데이터 손실에 대한 보호를 제공하지 않으므로 권장하지 않습니다. 단일 패브릭 조닝을 구성하는 경우 솔루션에서 복원력을 제공하려면 각 호스트에 두 개의 이니시에이터를 구성하여 다중 경로를 구현해야 합니다. 다중 경로를 관리하려면 호스트에 다중 경로 소프트웨어가 필요합니다.

각 호스트 이니시에이터에는 이니시에이터가 액세스할 수 있는 각 노드에서 LIF가 하나 이상 있어야 합니다. 조닝을

사용하면 호스트 이니시에이터에서 클러스터의 HA 노드 쌍에 대한 경로를 하나 이상 허용하여 LUN 접속 경로를 제공할 수 있어야 합니다. 즉, 호스트의 각 이니시에이터에는 자신의 존 구성 내 노드당 하나의 대상 LIF만 있을 수 있음을 의미합니다. 클러스터에서 동일한 노드 또는 여러 노드에 대한 다중 경로가 필요한 경우 각 노드의 존 구성에 노드당 여러 개의 LIF가 존재하게 됩니다. 따라서 노드에 장애가 발생하거나 LUN이 포함된 볼륨이 다른 노드로 이동되는 경우에도 호스트는 계속 LUN에 액세스할 수 있습니다. 또한 보고 노드를 적절하게 설정해야 합니다.

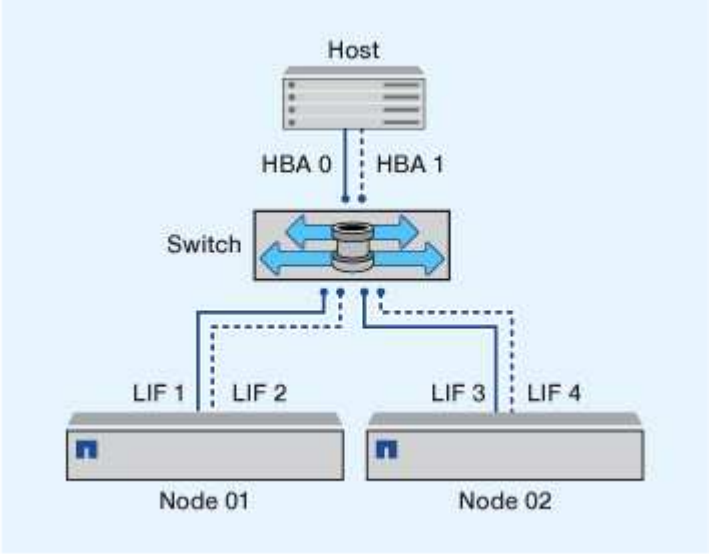
Cisco FC 및 FCoE 스위치를 사용할 때 단일 패브릭 영역에는 동일한 물리적 포트에 대해 둘 이상의 대상 LIF가 포함될 수 없습니다. 같은 포트에 여러 LIF가 있는 경우 LIF 포트가 연결 손실로부터 복구되지 못할 수 있습니다.

다음 그림에서는 두 개의 이니시에이터가 있고 다중 경로 소프트웨어가 실행 중인 호스트를 보여 줍니다. 두 개의 영역이 있습니다.

이 그림에 사용된 명명 규칙은 ONTAP 솔루션에 사용할 수 있는 명명 규칙 중 하나에 불과합니다.

- 구역 1: HBA 0, LIF_1 및 LIF_3
- 구역 2: HBA 1, LIF_2 및 LIF_4

구성에 더 많은 노드가 포함된 경우, 추가 노드의 LIF가 이 존에 포함됩니다



이 예제에서는 각 영역에 4개의 LIF를 모두 가질 수도 있습니다. 이 경우 영역은 다음과 같습니다.

- 존 1: HBA 0, LIF_1, LIF_2, LIF_3 및 LIF_4
- 존 2: HBA 1, LIF_1, LIF_2, LIF_3 및 LIF_4

호스트 운영 체제 및 다중 경로 소프트웨어는 노드의 LUN에 액세스하는 데 사용되는 지원되는 경로 수를 지원해야 합니다. 노드의 LUN에 액세스하는 데 사용되는 경로 수를 확인하려면 SAN 구성 제한 섹션을 참조하십시오.

Cisco FC 및 **FCoE** 스위치에 대한 조닝 제한 사항

Cisco FC 및 FCoE 스위치를 사용할 경우 영역의 물리적 포트 및 논리 인터페이스(LIF) 사용에 특정 제한이 적용됩니다.

물리적 포트

- FC-NVMe 및 FC는 동일한 32Gb 물리적 포트를 공유할 수 있습니다

- FC-NVMe 및 FCoE는 동일한 물리적 포트를 공유할 수 없습니다
- FC와 FCoE는 같은 물리적 포트를 공유할 수 있지만 프로토콜 LIF는 별도의 영역에 있어야 합니다.

논리 인터페이스**(LIF)**

- 존에는 클러스터의 모든 타겟 포트의 LIF가 포함될 수 있습니다.

  호스트에 허용되는 최대 경로 수를 초과하지 않도록 SLM 구성을 확인하십시오.

- 특정 포트의 각 LIF는 해당 포트의 다른 LIF와 다른 영역에 있어야 합니다
- 다른 물리적 포트에 있는 LIF는 동일한 존에 있을 수 있습니다.

ONTAP 시스템 및 비 **NetApp** 시스템에 연결된 **SAN** 호스트의 요구 사항

공유 SAN 구성은 ONTAP 스토리지 시스템과 다른 공급업체의 스토리지 시스템에 모두 연결되는 호스트로 정의됩니다. 여러 요구사항을 충족할 경우, 단일 호스트에서 ONTAP 스토리지 시스템 및 다른 공급업체의 스토리지 시스템에 액세스할 수 있습니다.

모든 호스트 운영 체제에서 별도의 어댑터를 사용하여 각 공급업체의 스토리지 시스템에 연결하는 것이 좋습니다. 별도의 어댑터를 사용하면 드라이버와 설정이 충돌할 가능성이 줄어듭니다. ONTAP 스토리지 시스템에 연결하려면 어댑터 모델, BIOS, 펌웨어 및 드라이버가 NetApp 상호 운용성 매트릭스 툴에 지원되는 것으로 표시되어야 합니다.

호스트에 대해 필수 또는 권장 시간 초과 값과 기타 스토리지 매개 변수를 설정해야 합니다. 항상 NetApp 소프트웨어를 설치하거나 NetApp 설정을 마지막에 적용해야 합니다.

- AIX의 경우 구성의 상호 운용성 매트릭스 툴에 나열된 AIX Host Utilities 버전의 값을 적용해야 합니다.
- ESX의 경우 VMware vSphere용 Virtual Storage Console을 사용하여 호스트 설정을 적용해야 합니다.
- HP-UX의 경우 HP-UX 기본 스토리지 설정을 사용해야 합니다.
- Linux의 경우 구성의 상호 운용성 매트릭스 툴에 나열된 Linux Host Utilities 버전의 값을 적용해야 합니다.
- Solaris의 경우, 구성의 상호 운용성 매트릭스 툴에 나열된 Solaris Host Utilities 버전의 값을 적용해야 합니다.
- Windows의 경우 구성의 상호 운용성 매트릭스 툴에 나열된 Windows Host Utilities 버전을 설치해야 합니다.

관련 정보

"NetApp 상호 운용성 매트릭스 툴"

MetroCluster 환경의 **SAN** 구성입니다

ONTAP MetroCluster 환경에서 지원되는 **SAN** 구성

MetroCluster 환경에서 SAN 구성을 사용할 때는 몇 가지 고려 사항을 염두에 두어야 합니다.

- MetroCluster 구성은 프런트엔드 FC 패브릭 ""라우팅된" vSAN 구성을 지원하지 않습니다.
- ONTAP 9.15.1부터 NVMe/TCP에서 4노드 MetroCluster IP 구성이 지원됩니다.
- ONTAP 9.12.1부터 4노드 MetroCluster IP 구성이 NVMe/FC에서 지원됩니다. ONTAP 9.12.1 이전의 프런트엔드 NVMe 네트워크에서는 MetroCluster 구성이 지원되지 않습니다.
- iSCSI, FC, FCoE 등의 다른 SAN 프로토콜은 MetroCluster 구성에서 지원됩니다.

- SAN 클라이언트 구성을 사용할 때는 에 제공된 노트에 MetroCluster 구성에 대한 특별한 고려 사항이 포함되어 있는지 확인해야 합니다 "NetApp 상호 운용성 매트릭스 툴" (IMT).
- 운영 체제 및 애플리케이션은 MetroCluster의 자동 계획되지 않은 전환 및 Tiebreaker 또는 중재자 시작 전환을 지원하기 위해 120초의 I/O 복원력을 제공해야 합니다.
- MetroCluster 구성은 프런트 엔드 FC 패브릭의 양쪽에서 동일한 WWNN 및 WWPN을 사용합니다.

관련 정보

- "MetroCluster 데이터 보호 및 재해 복구 이해"
- "NetApp 지식 기반: MetroCluster 구성에서 AIX 호스트 지원에 대한 고려 사항은 무엇입니까?"
- "NetApp 지식 기반: MetroCluster 구성에서 Solaris 호스트 지원 고려 사항"

ONTAP MetroCluster 스위치오버 및 스위치백 중에는 포트 중첩을 방지합니다

SAN 환경에서는 이전 포트가 오프라인이 되고 새 포트가 온라인 상태가 될 때 겹치지 않도록 프런트엔드 스위치를 구성할 수 있습니다.

스위치오버 중에 정상적인 사이트의 FC 포트가 패브릭에 로그인한 후 패브릭에서 재해 사이트의 FC 포트가 오프라인이며 이름 및 디렉토리 서비스에서 이 포트를 제거했습니다.

재해의 FC 포트가 아직 제거되지 않은 경우 중복 WWPN으로 인해 정상적인 사이트에서 FC 포트의 패브릭 로그인 시도가 거부될 수 있습니다. FC 스위치의 이러한 동작은 기존 디바이스가 아닌 이전 디바이스의 로그인을 사용하도록 변경할 수 있습니다. 이 동작이 다른 패브릭 디바이스에 미치는 영향을 확인해야 합니다. 자세한 내용은 스위치 공급업체에 문의하십시오.

스위치 유형에 따라 올바른 절차를 선택하십시오.

예 **22.** 단계

Cisco 스위치

1. 스위치에 연결하고 로그인합니다.
2. 구성 모드 시작:

```
switch# config t
switch(config)#
```

3. 이름 서버 데이터베이스의 첫 번째 장치 항목을 새 장치로 덮어씁니다.

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. NX-OS 8.x를 실행 중인 스위치에서 flogi 일시 중지 시간 초과가 0으로 설정되었는지 확인합니다.

   a. 일시 중지 시간 표시:

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. 이전 단계의 출력이 시간 간격이 0임을 나타내지 않으면 0으로 설정합니다.

   'Switch (config)#flogi scale enable'

   '스위치(config)$flogi 시간 제한 0'

Brocade 스위치

1. 스위치에 연결하고 로그인합니다.
2. 'witchDisable' 명령어를 입력한다.
3. configure 명령을 입력하고 프롬프트에 y를 누릅니다.

```
 F-Port login parameters (yes, y, no, n): [no] y
```

4. 설정 1 선택:

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. 나머지 프롬프트에 응답하거나 * Ctrl+D * 를 누릅니다.
6. 'witchEnable' 명령어를 입력한다.

관련 정보

"테스트 또는 유지 관리를 위한 전환 수행"

SAN 호스트 다중 경로에 대한 ONTAP 지원

ONTAP는 FC와 iSCSI 호스트의 다중 경로에 대해 ALUA(Asymmetric Logical Unit Access) 소프트웨어를 사용합니다.

ONTAP 9.5부터 ANA(Asynchronous Namespace Access)를 사용하는 NVMe 호스트에 대해 다중 경로 HA(고가용성) 쌍 페일오버/반환이 지원됩니다. ONTAP 9.4에서 NVMe는 호스트에서 타겟으로의 경로를 하나만 지원하므로 애플리케이션 호스트는 HA 파트너에 대한 경로 페일오버를 관리해야 합니다.

SAN 호스트가 둘 이상의 경로를 통해 LUN 또는 NVMe 네임스페이스에 액세스할 수 있는 경우 다중 경로 소프트웨어가 필요합니다. LUN 또는 NVMe 네임스페이스에 대한 모든 경로에 대해 운영 체제에 단일 디스크를 제공합니다. 이 기능이 없으면 운영 체제는 각 경로를 별도의 디스크로 처리하여 데이터 손상이 발생할 수 있습니다.

다음 중 하나가 있는 경우 솔루션은 여러 경로를 포함하는 것으로 간주됩니다.

- 호스트의 단일 이니시에이터 포트에서 SVM의 여러 SAN LIF에 연결됩니다
- 여러 이니시에이터 포트를 SVM의 단일 SAN LIF에 연결합니다
- 여러 이니시에이터 포트를 SVM의 여러 SAN LIF에 연결합니다

MPIO(다중 경로 I/O) 소프트웨어라고도 하는 다중 경로 소프트웨어가 HA 구성에 권장됩니다. 선택적 LUN 맵 이외에도 LUN에 액세스하는 데 사용되는 경로를 제한하기 위해 FC 스위치 조닝 또는 포트 세트를 사용하는 것이 좋습니다.

ALUA 또는 ANA를 지원하는 특정 호스트 구성에 대한 자세한 내용은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴" 및 "ONTAP SAN 호스트 구성" 호스트 운영 체제를 위한 것입니다.

클러스터의 호스트에서 노드까지 권장되는 경로 수입니다

호스트에서 클러스터의 각 노드로 이어지는 경로가 8개를 초과할 수 없습니다. 또한 호스트 OS 및 호스트에서 사용되는 다중 경로에 대해 지원할 수 있는 총 경로 수를 초과하지 않아야 합니다.

클러스터의 SVM(스토리지 가상 머신)에서 사용하는 동안 각 보고 노드에 연결되는 LUN당 최소 2개의 경로를 보유해야 "선택적 LUN 맵(SLM)"합니다. 따라서 단일 장애 지점이 발생하지 않으며 시스템에서 구성 요소 장애를 극복할 수 있습니다.

클러스터에 4개 이상의 노드가 있거나 모든 노드에서 SVM이 사용하는 4개 이상의 타겟 포트가 있는 경우 다음 방법을 사용하여 노드의 LUN에 액세스하는 데 사용할 수 있는 경로 수를 제한하여 권장되는 최대 8개 경로를 초과하지 않도록 할 수 있습니다.

- SLM

  SLM은 호스트에서 LUN으로의 경로 수를 LUN과 소유 노드의 HA 파트너가 있는 노드의 경로로만 줄여줍니다. SLM은 기본적으로 활성화되어 있습니다.

- "iSCSI에 대한 Portset입니다"
- 호스트에서 FC igroup 매핑
- FC 스위치 조닝

구성 제한

ONTAP 클러스터당 지원되는 최대 노드 및 **SAN** 호스트를 결정합니다

클러스터당 지원되는 노드 수는 ONTAP 버전, 컨트롤러 모델 및 클러스터 노드의 프로토콜에 따라 다릅니다. 클러스터에 연결할 수 있는 최대 SAN 호스트 수도 사용자의 특정 구성에 따라 다릅니다.

클러스터당 지원되는 최대 노드를 확인합니다

클러스터의 노드가 FC, FC-NVMe, FCoE 또는 iSCSI에 대해 구성된 경우 해당 클러스터는 SAN 노드 제한으로 제한됩니다. 클러스터의 컨트롤러에 기반한 노드 제한은 _Hardware Universe_에 나열되어 있습니다.

단계

1. 로 이동합니다 "NetApp Hardware Universe를 참조하십시오".
2. 왼쪽 위에서 * 홈 * 옆에 있는 * 플랫폼 * 을 선택한 다음 플랫폼 유형을 선택합니다.
3. 사용 중인 ONTAP 버전을 선택합니다.

   플랫폼을 선택할 수 있는 새 열이 표시됩니다.

4. 솔루션에 사용되는 플랫폼을 선택하십시오.
5. Choose your Specifications(사양 선택) * 에서 * Select All(모두 선택) * 을 선택 취소합니다.
6. Max Nodes per Cluster(NAS/SAN) * 를 선택합니다.
7. 결과 표시 * 를 클릭합니다.

결과

선택한 플랫폼에 대한 클러스터당 최대 노드가 표시됩니다.

클러스터에서 더 많은 **FC** 호스트를 지원할 수 있는지 확인합니다

FC 및 FC-NVMe 구성의 경우 시스템에서 이니시에이터-타겟 nexuse(ITN) 수를 사용하여 클러스터에 호스트를 더 추가할 수 있는지 확인해야 합니다.

ITN은 호스트의 이니시에이터에서 스토리지 시스템의 타겟으로 연결되는 하나의 경로를 나타냅니다. FC 및 FC-NVMe 구성의 노드당 최대 ITN 수는 2,048개입니다. 최대 ITN 수 미만이면 계속해서 클러스터에 호스트를 추가할 수 있습니다.

클러스터에서 사용되는 ITN 수를 확인하려면 클러스터의 각 노드에 대해 다음 단계를 수행하십시오.

단계

1. 특정 노드에서 모든 LIF를 식별합니다.
2. 노드의 모든 LIF에 대해 다음 명령을 실행합니다.

```
fcp initiator show -fields wwpn, lif
```

명령 출력의 하단에 표시되는 항목 수는 해당 LIF의 ITN 수를 나타냅니다.

3. 각 LIF에 대해 표시되는 ITN 수를 기록합니다.
4. 클러스터의 모든 노드에 있는 각 LIF의 ITN 수를 추가합니다.

   이 합계는 클러스터의 ITN 수를 나타냅니다.

클러스터에서 더 많은 **iSCSI** 호스트를 지원할 수 있는지 확인합니다

노드에 직접 연결할 수 있거나 하나 이상의 스위치를 통해 연결할 수 있는 호스트의 수는 사용 가능한 이더넷 포트의 수에 따라 달라집니다. 사용 가능한 이더넷 포트 수는 컨트롤러의 모델 및 컨트롤러에 설치된 어댑터의 수와 유형에 따라 결정됩니다. 컨트롤러 및 어댑터에 지원되는 이더넷 포트 수는 _Hardware Universe_에서 확인할 수 있습니다.

모든 다중 노드 클러스터 구성의 경우, 클러스터에 호스트를 더 추가할 수 있는지 여부를 알 수 있도록 노드당 iSCSI 세션 수를 결정해야 합니다. 클러스터가 노드당 최대 iSCSI 세션 수보다 많은 경우 계속해서 클러스터에 호스트를 추가할 수 있습니다. 노드당 최대 iSCSI 세션 수는 클러스터의 컨트롤러 유형에 따라 달라집니다.

단계

1. 노드에서 모든 타겟 포털 그룹을 식별합니다.
2. 노드의 모든 타겟 포털 그룹에 대한 iSCSI 세션 수를 확인합니다.

```
iscsi session show -tpgroup _tpgroup_
```

명령 출력 하단에 표시되는 항목 수는 해당 타겟 포털 그룹에 대한 iSCSI 세션 수를 나타냅니다.

3. 각 타겟 포털 그룹에 대해 표시되는 iSCSI 세션 수를 기록합니다.
4. 노드의 각 타겟 포털 그룹에 대한 iSCSI 세션 수를 추가합니다.

   총계 는 노드의 iSCSI 세션 수를 나타냅니다.

All-Flash SAN 어레이 구성 제한 및 지원

ASA(All-Flash SAN 어레이)의 구성 제한 및 지원은 ONTAP 버전에 따라 다릅니다.

지원되는 구성 제한에 대한 최신 정보는 에서 확인할 수 있습니다 "NetApp Hardware Universe를 참조하십시오".

> 이러한 제한은 ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 참조하세요. "ASA R2 시스템 스토리지 제한" .

SAN 프로토콜 및 클러스터당 지원되는 노드 수

지원되는 SAN 프로토콜과 클러스터당 최대 노드 수는 MetroCluster가 아닌 구성인지 MetroCluster 구성이 있는지에 따라 달라집니다.

MetroCluster 구성이 아닌 경우

다음 표는 MetroCluster가 아닌 구성에서 SAN 프로토콜에 대한 ASA 지원 과 클러스터당 지원되는 노드 수를 보여줍니다.

ONTAP로 시작하는 중…	프로토콜 지원	클러스터당 최대 노드 수
9.11.1	• NVMe/TCP • NVMe/FC	12
9.10.1	• NVMe/TCP	2
9.9.1	• NVMe/FC	2
	• FC • iSCSI	12
9.7	• FC • iSCSI	2

MetroCluster IP 구성

다음 표는 MetroCluster IP 구성에서 SAN 프로토콜에 대한 ASA 지원과 클러스터당 지원되는 노드 수를 보여줍니다.

ONTAP로 시작하는 중…	프로토콜 지원	클러스터당 최대 노드 수
9.15.1	• NVMe/TCP	4노드 MetroCluster IP 구성에서 클러스터당 2개 노드
9.12.1	• NVMe/FC	4노드 MetroCluster IP 구성에서 클러스터당 2개 노드
9.9.1	• FC • iSCSI	8노드 MetroCluster IP 구성으로 클러스터당 4개 노드
9.7	• FC • iSCSI	4노드 MetroCluster IP 구성에서 클러스터당 2개 노드

영구 포트 지원

ONTAP 9.8부터는 FC 프로토콜을 사용하도록 구성된 ASA(All-Flash SAN Array)에서 영구 포트가 기본적으로 활성화됩니다. 영구 포트는 FC에만 사용할 수 있으며 WWPN(World Wide Port Name)으로 식별되는 영역 구성원이 필요합니다.

영구 포트는 고가용성(HA) 파트너의 해당 물리적 포트에 섀도 LIF를 생성하여 테이크오버의 영향을 줄입니다. 노드가 되면 파트너 노드의 섀도 LIF는 WWPNe를 포함하여 원래 LIF의 ID를 가정합니다. 가져온 오버 노드의 경로 상태가

장애 발생으로 변경되기 전에 섀도우 LIF는 호스트 MPIO 스택에 대한 Active/Optimized 경로로 표시되고 I/O가 이동됩니다. 따라서 스토리지 페일오버 작업 중에도 호스트가 항상 동일한 수의 경로를 타겟으로 인식하기 때문에 I/O 중단이 줄어듭니다.

영구 포트의 경우 HA 쌍 내에서 다음과 같은 FCP 포트 특성이 동일해야 합니다.

- FCP 포트의 개수
- FCP 포트 이름
- FCP 포트의 속도입니다
- FCP LIF WWPN 기반 조닝

HA Pair 내에서 동일 특성이 아닌 경우, 다음과 같은 EMS 메시지가 발생한다.

"EMS: scsiblade.lif.persistent.ports.fcp.init.error`

영구 포트에 대한 자세한 내용은 을 참조하십시오"NetApp 기술 보고서 4080: 최신 SAN에 대한 모범 사례".

ONTAP 시스템에서 사용되는 **FC** 스위치의 구성 제한

파이버 채널 스위치에는 포트, 포트 그룹, 블레이드 및 스위치별로 지원되는 로그인 수를 포함한 최대 구성 제한이 있습니다. 지원되는 제한은 스위치 벤더에서 문서로 제공합니다.

각 FC 논리 인터페이스(LIF)는 FC 스위치 포트에 로그인합니다. 노드에서 단일 타겟의 총 로그인 수는 LIF 수에 기본 물리적 포트의 로그인 수 1을 더한 값과 같습니다. 로그인 또는 기타 구성 값에 대한 스위치 공급업체의 구성 제한을 초과하지 마십시오. 또한 NPIV가 활성화된 가상화 환경에서 호스트 측에서 사용되는 초기자에 대해서도 마찬가지입니다. 솔루션에서 사용 중인 타겟 또는 이니시에이터에 대한 스위치 공급업체의 로그인 구성 제한을 초과하지 마십시오.

Brocade 스위치 제한

Brocade 스위치에 대한 구성 제한은 _ Brocade 확장성 지침 _ 에서 확인할 수 있습니다.

Cisco Systems 스위치 제한

에서 Cisco 스위치에 대한 구성 제한을 찾을 수 있습니다 "Cisco 구성 제한" 사용 중인 Cisco 스위치 소프트웨어 버전에 대한 안내서입니다.

ONTAP에서 지원되는 최대 **FC** 및 **FCoE** 홉 수

홉 수는 이니시에이터(호스트)와 타겟(스토리지 시스템) 사이의 경로에 있는 스위치의 수로 정의됩니다. 호스트와 스토리지 시스템 간에 지원되는 최대 FC 홉 수는 스위치 공급업체에 따라 다릅니다.

Cisco Systems의 설명서에서는 이 값을 SAN fabric_의 _diameter로 참조합니다.

FCoE의 경우 FC 스위치에 FCoE 스위치를 연결할 수 있습니다. 엔드 투 엔드 FCoE 연결의 경우 FCoE 스위치는 이더넷 ISL(Inter-Switch Link)을 지원하는 펌웨어 버전을 실행해야 합니다.

공급업체를 전환합니다	지원되는 홉 수입니다
모든 정보를 제공합니다	• FC의 경우 7 • FCoE의 경우 5입니다
Cisco의	• FC의 경우 7 • 최대 3개의 스위치가 FCoE 스위치일 수 있습니다.

ONTAP FC 호스트의 큐 길이를 계산합니다

노드별 및 FC 포트 팬인 당 ITNs의 최대 값을 얻으려면 호스트에서 FC 큐 길이를 조정해야 할 수 있습니다. FC 포트에 연결할 수 있는 HBA의 수와 LUN의 최대 수는 FC 타겟 포트에서 사용 가능한 큐 깊이로 제한됩니다.

이 작업에 대해

큐 깊이는 스토리지 컨트롤러에서 한 번에 대기열에 넣을 수 있는 입출력 요청(SCSI 명령)의 수입니다. 호스트의 이니시에이터 HBA에서 스토리지 컨트롤러의 타겟 어댑터로 연결되는 각 입출력 요청은 대기열 항목을 사용합니다. 일반적으로 큐 길이가 클수록 성능이 향상됩니다. 그러나 스토리지 컨트롤러의 최대 큐 수준에 도달하면 해당 스토리지 컨트롤러는 QFULL 응답을 반환하여 들어오는 명령을 거부합니다. 많은 수의 호스트가 스토리지 컨트롤러에 액세스하고 있는 경우, 시스템 성능이 크게 저하되어 일부 시스템에서 오류가 발생할 수 있는 QFULL 조건을 피할 수 있도록 신중하게 계획해야 합니다.

여러 이니시에이터(호스트)가 있는 구성에서는 모든 호스트에 유사한 대기열 깊이가 있어야 합니다. 동일한 타겟 포트를 통해 스토리지 컨트롤러에 접속된 호스트 간의 큐 크기가 서로 다르기 때문에 큐 크기가 작은 호스트는 큐 크기가 큰 호스트에 의해 리소스에 액세스할 수 없습니다.

다음과 같은 일반적인 권장 사항은 ""조정"" 대기열 깊이에 대해 만들 수 있습니다.

- 중소 규모 시스템의 경우 HBA 대기열 길이가 32인 HBA를 사용합니다.
- 대규모 시스템의 경우 HBA 대기열 길이가 128인 HBA를 사용합니다.
- 예외 케이스 또는 성능 테스트의 경우 큐 처리 문제가 발생하지 않도록 256개의 큐 길이를 사용하십시오.
- 모든 호스트는 모든 호스트에 동일한 액세스를 제공하기 위해 유사한 값으로 설정된 대기열 깊이를 가져야 합니다.
- 성능 패널이나 오류를 방지하려면 스토리지 컨트롤러 타겟 FC 포트 큐 길이를 초과하지 않아야 합니다.

단계

1. 하나의 FC 타겟 포트에 연결되는 모든 호스트의 총 FC 이니시에이터 수를 계산합니다.
2. 128을 곱합니다.
   - 결과가 2,048보다 작으면 모든 이니시에이터에 대한 대기열 길이를 128로 설정합니다. 스토리지 컨트롤러의 각 타겟 포트 2개에 하나의 이니시에이터가 접속된 호스트 15개가 있습니다. 15 × 128 = 1,920. 1,920은 총 대기열 길이 제한인 2,048보다 작기 때문에 모든 이니시에이터에 대한 대기열 길이를 128로 설정할 수 있습니다.
   - 결과가 2,048보다 크면 3단계로 이동합니다. 스토리지 컨트롤러의 각 타겟 포트 2개에 하나의 이니시에이터가 연결된 30개의 호스트가 있습니다. 30 × 128 = 3,840. 3,840이 총 대기열 길이 제한인 2,048보다 크기 때문에 3단계에서 해결 방법 중 하나를 선택해야 합니다.
3. 다음 옵션 중 하나를 선택하여 스토리지 컨트롤러에 호스트를 더 추가합니다.

- 옵션 1:
  i. FC 타겟 포트를 추가합니다.
  ii. FC 이니시에이터를 재배포합니다.
  iii. 1단계와 2단계를 반복합니다. + 원하는 큐 길이 3,840이 포트당 사용 가능한 큐 길이를 초과합니다. 이를 해결하기 위해 각 컨트롤러에 2포트 FC 타겟 어댑터를 추가한 다음, 30개 호스트 중 15개가 1개의 포트 세트에 연결되고 나머지 15개 호스트는 2번째 포트 세트에 연결되도록 FC 스위치를 재존할 수 있습니다. 그런 다음 포트당 큐 깊이가 15 × 128 = 1,920으로 줄어듭니다.
- 옵션 2:
  i. 예상되는 I/O 요구 사항에 따라 각 호스트를 "대형" 또는 "소형"으로 지정합니다.
  ii. 큰 이니시에이터 수에 128을 곱합니다.
  iii. 작은 이니시에이터 수에 32를 곱합니다.
  iv. 두 결과를 함께 추가합니다.
  v. 결과가 2,048보다 작으면 큰 호스트의 대기열 길이를 128로, 작은 호스트의 대기열 길이를 32로 설정합니다.
  vi. 결과가 포트당 2,048보다 크면 총 대기열 길이가 2,048보다 작거나 같을 때까지 이니시에이터당 대기열 길이를 줄입니다.

> ⓘ 초당 특정 I/O 처리량을 달성하는 데 필요한 큐 길이를 예측하려면 다음 수식을 사용합니다.
>
> 필요한 대기열 길이 = (초당 I/O 수) × (응답 시간)
>
> 예를 들어, 응답 시간이 3밀리초인 초당 40,000회의 I/O가 필요한 경우 필요한 큐 깊이는 40,000 × (.003) = 120입니다.

대기열 길이를 기본 권장 사항 32로 제한하려면 대상 포트에 연결할 수 있는 최대 호스트 수는 64개입니다. 그러나 큐 크기가 128로 결정되면 최대 16개의 호스트를 하나의 타겟 포트에 연결할 수 있습니다. 대기열 길이가 클수록 단일 타겟 포트에서 지원할 수 있는 호스트 수가 줄어듭니다. 대기열 길이를 손상시키지 않는 요구 사항이 있는 경우 더 많은 대상 포트를 얻을 수 있습니다.

원하는 큐 길이 3,840이 포트당 사용 가능한 큐 길이를 초과합니다. 스토리지 I/O 요구 사항이 높은 10개의 "대용량" 호스트와 I/O 요구 사항이 낮은 20개의 "소규모" 호스트가 있습니다. 큰 호스트의 이니시에이터 큐 길이를 128로, 작은 호스트의 이니시에이터 큐 길이를 32로 설정합니다.

총 큐 깊이는 (10×128) + (20×32) = 1,920입니다.

사용 가능한 대기열 길이를 각 이니시에이터에 균등하게 분산시킬 수 있습니다.

결과적인 이니시에이터당 대기열 길이는 2,048 ÷ 30 = 68입니다.

ONTAP SAN 호스트의 큐 길이를 수정합니다

노드별 ITN 및 FC 포트 팬인에 대한 최대 값을 달성하려면 호스트의 대기열 길이를 변경해야 할 수 있습니다. 환경에 맞게 가능합니다."최적의 대기열 길이를 계산합니다"

AIX 호스트

"chdev" 명령을 사용하여 AIX 호스트의 대기열 길이를 변경할 수 있습니다. "chdev" 명령을 사용하여 변경한 사항은 재부팅 후에도 유지됩니다.

예:

- hdisk7 디바이스의 대기열 길이를 변경하려면 다음 명령을 사용합니다.

  chdev -l hdisk7 -a queue_depth=32

- fcs0 HBA의 대기열 길이를 변경하려면 다음 명령을 사용하십시오.

  "chdev -l fcs0 -a num_cmd_elems=128"

  num_cmd_elems의 기본값은 200입니다. 최대값은 2,048입니다.

  num_cmd_elems를 변경하려면 HBA를 오프라인 상태로 전환한 다음 rmdev-l fcs0-R 및 makdev-l fcs0-P 명령을 사용하여 다시 온라인 상태로 전환해야 할 수도 있습니다.

HP-UX 호스트

커널 매개 변수 'scsi_max_qdepth'를 사용하여 HP-UX 호스트에서 LUN 또는 디바이스 대기열 길이를 변경할 수 있습니다. 커널 매개 변수 max_fcp_reqs를 사용하여 HBA 대기열 길이를 변경할 수 있습니다.

- 'scsi_max_qdepth'의 기본값은 8입니다. 최대값은 255입니다.

  'kmtune' 명령의 '-u' 옵션을 사용하면 실행 중인 시스템에서 'scsi_max_qdepth'를 동적으로 변경할 수 있습니다. 이 변경 사항은 시스템의 모든 장치에 적용됩니다. 예를 들어, 다음 명령을 사용하여 LUN 대기열 길이를 64로 늘릴 수 있습니다.

  "kmtune -u -s scsi_max_qdepth=64"

  'csictl' 명령어를 이용하여 개별 장치 파일의 대기열 길이를 변경할 수 있다. 'csictl' 명령을 사용한 변경 사항은 시스템 재부팅 시에도 지속되지 않습니다. 특정 장치 파일의 대기열 길이를 보고 변경하려면 다음 명령을 실행합니다.

  'csictl -a /dev/rdsk/c2t2d0'

  'csictl -m queue_depth=16/dev/rdsk/c2t2d0'

- max_fcp_reqs의 기본값은 512입니다. 최대값은 1024입니다.

  'max_fcp_reqs'의 변경 사항을 적용하려면 커널을 재구축하고 시스템을 재부팅해야 합니다. 예를 들어 HBA 대기열 길이를 256으로 변경하려면 다음 명령을 사용합니다.

  "kmtune -u -s max_fcp_reqs=256"

Solaris 호스트

Solaris 호스트에 대한 LUN 및 HBA 대기열 길이를 설정할 수 있습니다.

- LUN 큐 깊이의 경우: 호스트에서 사용 중인 LUN 수에 LUN당 스로틀(LUN-대기열-깊이)을 곱한 값은 호스트의 tgt-queue-depth 값보다 작거나 같아야 합니다.
- Sun 스택의 대기열 깊이의 경우: 기본 드라이버는 HBA 레벨에서 LUN 단위 또는 대상 max_throttle에 대한 설정을 허용하지 않습니다. 기본 드라이버에 대해 max_throttle 값을 설정하는 데 권장되는 방법은 '/kernel/drv/sd.conf' 및 '/kernel/drv/ssd.conf' 파일의 장치별 유형(VID_PID) 수준에 있습니다. 호스트 유틸리티는 MPxIO 구성의 경우 이 값을 64로, Veritas DMP 구성의 경우 8로 설정합니다.

단계

1. '#cd/kernel/drv'
2. `#vi lpfc.conf'
3. '/TFT-queue(/tgt-queue)'를 검색합니다

   tgt-queue-depth=32

   기본값은 설치 시 32로 설정됩니다.

4. 환경 구성에 따라 원하는 값을 설정합니다.
5. 파일을 저장합니다.
6. 'sync;sync;sync;reboot---r' 명령을 사용하여 호스트를 재부팅합니다.

QLogic HBA의 VMware 호스트입니다

'esxcfg-module' 명령을 사용하여 HBA 시간 제한 설정을 변경합니다. ESX.conf 파일을 수동으로 업데이트하는 것은 권장되지 않습니다.

단계

1. 서비스 콘솔에 루트 사용자로 로그온합니다.
2. 현재 로드된 Qlogic HBA 모듈을 확인하려면 '#vmkload_mod -l' 명령을 사용합니다.
3. Qlogic HBA의 단일 인스턴스의 경우 다음 명령을 실행합니다.

   '#esxcfg-module-s ql2xmaxqdepth=64 qla2300_707'

   이 예에서는 qla2300_707 모듈을 사용합니다. "vmkload_mod -l"의 출력에 따라 적절한 모듈을 사용합니다.

4. 다음 명령을 사용하여 변경 내용을 저장합니다.

   '#/usr/sbin/esxcfg-boot -b'

5. 다음 명령을 사용하여 서버를 재부팅합니다.

   '#reboot'

6. 다음 명령을 사용하여 변경 사항을 확인합니다.
   a. '#esxcfg-module-g qla2300_707'
   b. ``qla2300_707 활성화됨 = 1 옵션 = 'ql2xmaxqdepth=64''

Emulex HBA용 VMware 호스트

'esxcfg-module' 명령을 사용하여 HBA 시간 제한 설정을 변경합니다. ESX.conf 파일을 수동으로 업데이트하는 것은 권장되지 않습니다.

단계

1. 서비스 콘솔에 루트 사용자로 로그온합니다.
2. 현재 어떤 Emulex HBA가 로드되었는지 확인하려면 '#vmkload_mod -l grep lpfc' 명령을 사용합니다.
3. Emulex HBA의 단일 인스턴스의 경우 다음 명령을 입력합니다.

   '#esxcfg-module-s lpfc0_lun_queue_depth=16 lpfcdd_7xx'

   HBA 모델에 따라 모듈은 lpfcdd_7xx 또는 lpfcdd_732일 수 있습니다. 위 명령은 lpfcdd_7xx 모듈을 사용합니다. vmkload_mod-l의 결과에 따라 적절한 모듈을 사용해야 합니다.

   이 명령을 실행하면 LUN 대기열 길이가 lpfc0으로 표시된 HBA에 대해 16으로 설정됩니다.

4. Emulex HBA의 여러 인스턴스의 경우 다음 명령을 실행합니다.

   "a esxcfg-module-s" lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"lpfcdd_7xx"

   lpfc0에 대한 LUN 큐 길이 및 lpfc1에 대한 LUN 큐 크기는 16으로 설정됩니다.

5. 다음 명령을 입력합니다.

   '#esxcfg-boot-b'

6. reboot를 사용하여 재부팅합니다.

Emulex HBA용 Windows 호스트

Windows 호스트에서는 "LPUTILNT" 유틸리티를 사용하여 Emulex HBA의 대기열 길이를 업데이트할 수 있습니다.

단계

1. C:\WINNT\system32 디렉토리에 있는 LPUTILNT 유틸리티를 실행합니다.
2. 오른쪽의 메뉴에서 * Drive Parameters * 를 선택합니다.
3. 아래로 스크롤하여 * QueueDepth * 를 두 번 클릭합니다.

   QueueDepth * 를 150보다 크게 설정하는 경우 다음 Windows 레지스트리 값도 적절하게 늘려야 합니다.

   'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests'를 선택합니다

Qlogic HBA에 대한 Windows 호스트입니다

Windows 호스트에서는 및 'sansurfer' HBA 관리자 유틸리티를 사용하여 Qlogic HBA의 대기열 깊이를 업데이트할 수 있습니다.

단계

1. '서퍼' HBA 매니저 유틸리티를 실행합니다.
2. HBA 포트 * > * 설정 * 을 클릭합니다.
3. 목록 상자에서 * 고급 HBA 포트 설정 * 을 클릭합니다.
4. Execution Throttle 파라미터를 업데이트한다.

Emulex HBA용 Linux 호스트

Linux 호스트에서 Emulex HBA의 대기열 깊이를 업데이트할 수 있습니다. 재부팅 후에도 업데이트가 지속되도록 하려면 새 RAM 디스크 이미지를 생성하고 호스트를 재부팅해야 합니다.

단계

1. 수정할 대기열 길이 매개 변수를 식별합니다.

   Modinfo lpfc | grep queue_depth(Modinfo lpfc | grep queue_depth

   설명이 포함된 대기열 길이 매개 변수 목록이 표시됩니다. 운영 체제 버전에 따라 다음 대기열 길이 매개 변수 중 하나 이상을 수정할 수 있습니다.

   - 'lpfc_lun_queue_depth': 특정 LUN에 대기할 수 있는 최대 FC 명령어 수(uint)
   - 'lpfc_hba_queue_depth': lpfc HBA(uint)에 대기할 수 있는 최대 FC 명령어 수
   - 'lpfc_tgt_queue_depth': 특정 대상 포트에 대기할 수 있는 최대 FC 명령어 수(uint)

     "lpfc_tgt_queue_depth" 매개변수는 Red Hat Enterprise Linux 7.x 시스템, SUSE Linux Enterprise Server 11 SP4 시스템 및 12.x 시스템에만 적용됩니다.

2. Red Hat Enterprise Linux 5.x 시스템에 대한 '/etc/modprobe.conf' 파일과 Red Hat Enterprise Linux 6.x 또는 7.x 시스템에 대한 '/etc/modprobe.d/scsi.conf' 파일 또는 SUSE Linux Enterprise Server 11.x 또는 12.x 시스템에 대기열 길이 매개 변수를 추가하여 대기열 깊이를 업데이트합니다.

   운영 체제 버전에 따라 다음 명령 중 하나 이상을 추가할 수 있습니다.

   - 'options lpfc lpfc_hba_queue_depth=new_queue_depth'
   - 'options lpfc lpfc_lun_queue_depth=new_queue_depth'
   - 'options lpfc_tgt_queue_depth=new_queue_depth'
3. 새 RAM 디스크 이미지를 만든 다음 호스트를 재부팅하여 재부팅 후에도 업데이트가 지속되도록 합니다.

   자세한 내용은 를 참조하십시오 "시스템 관리" Linux 운영 체제 버전용.

4. 수정한 각 대기열 길이 매개 변수에 대해 대기열 길이 값이 업데이트되었는지 확인합니다.

   'cat/sys/class/scsi_host/host_number/lpfc_lun_queue_depth"cat/sys/class/scsi_host/host_number/lpfc_tgt_queue_depth"cat/sys/class/scsi_host/host_number/lpfc_hba_queue_depth'

```
root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
      30
```

대기열 깊이의 현재 값이 표시됩니다.

QLogic HBA용 Linux 호스트

Linux 호스트에서 QLogic 드라이버의 장치 대기열 길이를 업데이트할 수 있습니다. 재부팅 후에도 업데이트가 지속되도록 하려면 새 RAM 디스크 이미지를 생성하고 호스트를 재부팅해야 합니다. QLogic HBA 관리 GUI 또는 CLI(명령줄 인터페이스)를 사용하여 QLogic HBA 대기열 길이를 수정할 수 있습니다.

이 작업은 QLogic HBA CLI를 사용하여 QLogic HBA 대기열 길이를 수정하는 방법을 보여줍니다

단계

1. 수정할 장치 대기열 길이 매개 변수를 식별합니다.

   'modinfo qla2xxx | grep ql2xmaxqdepth'

   각 LUN에 대해 설정할 수 있는 최대 대기열 길이를 나타내는 "ql2xmaxqdepth" 대기열 길이 매개변수만 수정할 수 있습니다. RHEL 7.5 이상의 경우 기본값은 64입니다. 기본값은 RHEL 7.4 이전 버전의 경우 32입니다.

   ```
   root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
   parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
   Default is 64. (int)
   ```

2. 장치 대기열 깊이 값 업데이트:

   - 수정 사항을 영구적으로 만들려면 다음 단계를 수행하십시오.
     i. Red Hat Enterprise Linux 5.x 시스템에 대한 '/etc/modprobe.conf' 파일과 Red Hat Enterprise Linux 6.x 또는 7.x 시스템에 대한 '/etc/modprobe.d/scsi.conf' 파일에 대기열 깊이 매개 변수를 추가하거나 SUSE Linux Enterprise Server 11.x 또는 12.x 시스템에 대한 '/etc/modprobe.conf' 파일에 대기열 길이를 업데이트합니다. laq2xxx.options
     ii. 새 RAM 디스크 이미지를 만든 다음 호스트를 재부팅하여 재부팅 후에도 업데이트가 지속되도록 합니다.

     자세한 내용은 를 참조하십시오 "시스템 관리" Linux 운영 체제 버전용.
   - 현재 세션에 대해서만 매개 변수를 수정하려면 다음 명령을 실행합니다.

     'echo new_queue_depth>/sys/module/qla2xxx/parameters/ql2xmaxqdepth'

     다음 예제에서 대기열 길이는 128로 설정됩니다.

   ```
   echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

3. 대기열 길이 값이 업데이트되었는지 확인합니다.

   'cat/sys/module/qla2xxx/parameters/ql2xmaxqdepth'

   대기열 깊이의 현재 값이 표시됩니다.

4. QLogic HBA BIOS에서 펌웨어 매개변수 "실행 스로틀"을 업데이트하여 QLogic HBA 대기열 길이를 수정합니다.

a. QLogic HBA 관리 CLI에 로그인합니다.

   '/opt/QLogic_Corporation/QConvergConsoleCLI/qaucli'

b. 주 메뉴에서 "어댑터 구성" 옵션을 선택합니다.

```
[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

        CLI - Version 2.2.0 (Build 15)

    Main Menu

    1:  Adapter Information
    **2:  Adapter Configuration**
    3:  Adapter Updates
    4:  Adapter Diagnostics
    5:  Monitoring
    6:  FabricCache CLI
    7:  Refresh
    8:  Help
    9:  Exit


        Please Enter Selection: 2
```

c. 어댑터 구성 매개 변수 목록에서 'HBA Parameters' 옵션을 선택합니다.

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. HBA 포트 목록에서 필요한 HBA 포트를 선택합니다.

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

HBA 포트의 세부 정보가 표시됩니다.

e. HBA Parameters(HBA 매개변수) 메뉴에서 Display HBA Parameters(HBA 매개변수 표시) 옵션을 선택하여 "Execution Throttle(실행 스로틀)" 옵션의 현재 값을 확인합니다.

실행 스로틀 옵션의 기본값은 65535입니다.

```
HBA Parameters Menu

======================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
```

```
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
-------------------------------------------------------------------------
--------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
-------------------------------------------------------------------------
--------
Connection Options             : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                      : Auto
Frame Size                     : 2048
Hard Loop ID                   : 0
Loop Reset Delay (seconds)     : 5
Enable Host HBA BIOS           : Enabled
Enable Hard Loop ID            : Disabled
Enable FC Tape Support         : Enabled
Operation Mode                 : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us)  : 0
**Execution Throttle             : 65535**
Login Retry Count              : 8
Port Down Retry Count          : 30
Enable LIP Full Login          : Enabled
Link Down Timeout (seconds)    : 30
Enable Target Reset            : Enabled
LUNs Per Target                : 128
Out Of Order Frame Assembly    : Disabled
Enable LR Ext. Credits         : Disabled
Enable Fabric Assigned WWN     : N/A

Press <Enter> to continue:
```

a. 계속하려면 * Enter * 를 누르십시오.

b. HBA Parameters(HBA 매개변수) 메뉴에서 Configure HBA Parameters(HBA 매개변수 구성) 옵션을 선택하여 HBA 매개변수를 수정합니다.

c. Configure Parameters 메뉴에서 'Execute Throttle' 옵션을 선택하고 이 매개 변수의 값을 업데이트합니다.

```
Configure Parameters Menu

=====================================================
HBA            : 2 Port: 1
SN             : BFD1524C78510
HBA Model      : QLE2562
HBA Desc.      : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version     : 8.01.02
WWPN           : 21-00-00-24-FF-8D-98-E0
WWNN           : 20-00-00-24-FF-8D-98-E0
Link           : Online
=====================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. 계속하려면 * Enter * 를 누르십시오.

e. Configure Parameters 메뉴에서 'Commit Changes' 옵션을 선택하여 변경 사항을 저장합니다.

f. 메뉴를 종료합니다.

S3 오브젝트 스토리지 관리

ONTAP 9의 S3 지원에 대해 알아보십시오

ONTAP S3 구성에 대해 자세히 알아보십시오

ONTAP 9.8부터는 ONTAP System Manager와 같은 친숙한 관리 효율성 툴을 사용하여 ONTAP 클러스터에서 ONTAP S3(Simple Storage Service) 오브젝트 스토리지 서버를 사용하여 ONTAP에서 개발 및 운영을 위한 고성능 오브젝트 스토리지를 신속하게 프로비저닝하고 ONTAP의 스토리지 효율성 및 보안을 활용할 수 있습니다.

2024년 7월부터 이전에 PDF로 게시된 기술 보고서의 콘텐츠가 ONTAP 제품 설명서와 통합되었습니다. 이제 ONTAP S3 문서에 ONTAP 모범 사례 _ TR-4814:S3의 콘텐츠가 포함되어 있습니다.

System Manager 및 ONTAP CLI를 사용하는 S3 구성

System Manager 및 ONTAP CLI를 사용하여 ONTAP S3를 구성 및 관리할 수 있습니다. System Manager를 사용하여 S3를 활성화하고 버킷을 생성할 때 ONTAP은 단순한 구성을 위한 모범 사례 기본값을 선택합니다. 구성 매개 변수를 지정해야 하는 경우 ONTAP CLI를 사용할 수도 있습니다. CLI에서 S3 서버 및 버킷을 구성할 경우에도 원하는 경우 System Manager로 관리하거나 그 반대로 구성할 수 있습니다.

System Manager를 사용하여 S3 버킷을 생성하는 경우, ONTAP은 시스템에서 가장 가용성이 높은 기본 성능 서비스 수준을 구성합니다. 예를 들어, AFF 시스템에서 기본 설정은 * Extreme * 입니다. 성능 서비스 수준은 사전 정의된 QoS(Quality of Service) 정책 그룹입니다. 기본 서비스 수준 대신 사용자 지정 QoS 정책 그룹 또는 정책 그룹을 지정할 수 있습니다.

사전 정의된 적응형 QoS 정책 그룹은 다음과 같습니다.

- * Extreme *: 가장 낮은 지연 시간과 최고의 성능을 기대하는 애플리케이션에 사용됩니다.
- * 성능 *: 성능 요구사항 및 지연 시간이 중간 정도인 애플리케이션에 사용됩니다.
- * 가치 *: 처리량과 용량이 지연 시간보다 더 중요한 애플리케이션에 사용됩니다.
- * 사용자 정의 *: 사용자 정의 QoS 정책을 지정하거나 QoS 정책을 지정하지 않습니다.

계층화에 * 사용을 선택하면 성능 서비스 수준이 선택되지 않으며 시스템은 계층형 데이터에 대해 최적의 성능을 갖춘 저비용 미디어를 선택합니다.

참고 항목: "적응형 QoS 정책 그룹을 사용합니다".

ONTAP는 가장 적합한 디스크가 있는 로컬 계층에서 이 버킷을 프로비저닝하려고 시도하여 선택한 서비스 수준을 충족시킵니다. 그러나 버킷에 포함할 디스크를 지정해야 하는 경우 로컬 계층(애그리게이트)을 지정하여 CLI에서 S3 오브젝트 스토리지를 구성하는 것이 좋습니다. CLI에서 S3 서버를 구성할 경우에도 원할 경우 System Manager로 관리할 수 있습니다.

버킷에 사용할 애그리게이트를 지정할 수 있는 기능은 CLI를 통해서만 지정할 수 있습니다.

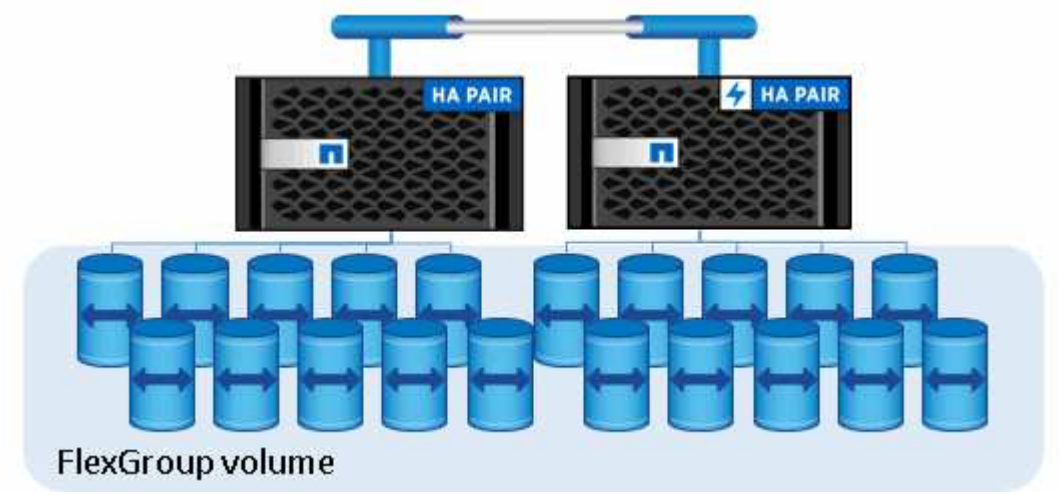
Cloud Volumes ONTAP에서 **S3** 버킷 구성

Cloud Volumes ONTAP에서 버킷 서비스를 제공하려면 기본 애그리게이트를 수동으로 선택하여 해당 애그리게이트가 하나의 노드만 사용하는지 확인하는 것이 좋습니다. 두 노드의 애그리게이트를 사용하면 지리적으로 서로 분리되어 있는 가용성 영역에 노드가 있기 때문에 지연 시간 문제가 발생하기 때문에 성능에 영향을 미칠 수 있습니다. 따라서 Cloud Volumes ONTAP 환경에서는 이 작업을 수행해야 합니다 CLI에서 S3 버킷을 구성합니다.

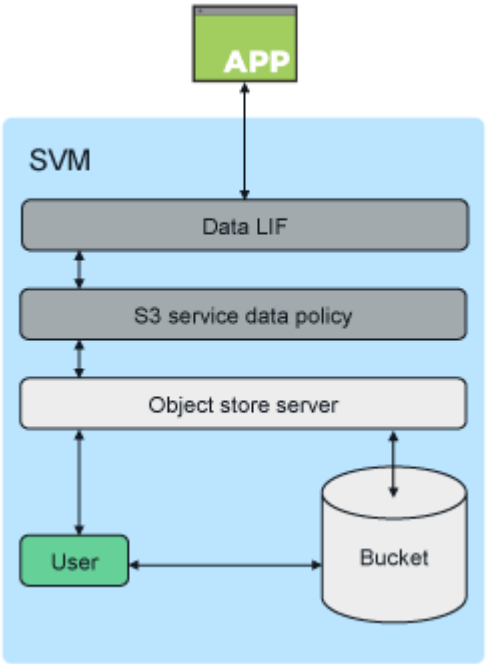
그렇지 않으면 Cloud Volumes ONTAP의 S3 서버가 사내 환경과 Cloud Volumes ONTAP에서 동일하게 구성 및 관리됩니다.

FlexGroup 볼륨을 사용하는 ONTAP S3 아키텍처

ONTAP에서 버킷의 기본 아키텍처는 여러 개의 구성 멤버 볼륨으로 구성되지만 단일 볼륨으로 관리되는 단일 네임스페이스인 A "FlexGroup 볼륨"입니다.



버킷에 대한 액세스는 승인된 사용자 및 클라이언트 애플리케이션을 통해 제공됩니다.



버킷을 FabricPool 엔드포인트로 사용하는 것을 포함하여 S3 애플리케이션에만 사용할 경우 기본 FlexGroup 볼륨은 S3 프로토콜만 지원합니다.

ONTAP 9.12.1부터 NAS 프로토콜을 사용하도록 미리 구성된 에서도 S3 프로토콜을 활성화할 수 "멀티프로토콜 NAS 볼륨"있습니다. 멀티프로토콜 NAS 볼륨에서 S3 프로토콜이 활성화된 경우 클라이언트 애플리케이션은 NFS, SMB 및 S3를 사용하여 데이터를 읽고 쓸 수 있습니다.

버킷 제한

최소 용량

최소 버킷 용량은 ONTAP 플랫폼에 의해 결정됩니다.

- 온프레미스 플랫폼의 경우 95GB입니다.
- Lab on Demand 이용 시 1.6GB의 용량이 필요합니다.
- ONTAP Select 의 경우 200MB가 필요합니다.

최대 크기

최대 버킷 용량은 FlexGroup 의 최대 크기인 60PB로 제한됩니다.

최대 버킷 수

FlexGroup 볼륨당 최대 버킷 수는 1,000개이며, 클러스터당 최대 12,000개(FlexGroup 볼륨 12개 사용 시)입니다.

ONTAP 9.14.1 이상을 사용한 자동 **FlexGroup** 사이징

ONTAP 9.14.1부터 기본 FlexGroup 크기는 포함된 버킷 크기를 기반으로 합니다. 버킷을 추가하거나 제거하면 FlexGroup 볼륨이 자동으로 증가 또는 감소합니다.

예를 들어 초기 Bucket_A가 100GB로 프로비저닝되면 FlexGroup는 100GB로 씬 프로비저닝됩니다. 300GB의 Bucket_B, 500GB의 Bucket_C라는 두 개의 추가 버킷을 생성하면 FlexGroup 볼륨이 900GB로 증가합니다.

(100GB의 Bucket_A + 300GB의 Bucket_B + 500GB의 Bucket_C = 900GB)

Bucket_A를 삭제하면 기본 FlexGroup 볼륨이 800GB로 줄어듭니다.

ONTAP 9.13.1 이하 버전에서 기본 **FlexGroup** 크기가 수정되었습니다

버킷 확장을 위한 용량을 제공하려면 FlexGroup 볼륨에 있는 모든 버킷의 총 사용 용량이 클러스터의 사용 가능한 스토리지 애그리게이트 기준 최대 FlexGroup 볼륨 용량의 33% 미만이어야 합니다. 이 조건을 충족할 수 없으면 새로 생성되는 자동으로 생성된 FlexGroup 볼륨에 새 버킷이 프로비저닝됩니다.

ONTAP 9.14.1 이전 버전에서는 FlexGroup 크기가 환경에 따라 기본 크기로 고정되어 있습니다.

- 1.6PB(ONTAP
- ONTAP Select은 100TB

클러스터의 용량이 기본 크기로 FlexGroup 볼륨을 프로비저닝할 수 없을 경우 ONTAP는 기존 환경에서 프로비저닝할 수 있을 때까지 기본 크기를 절반으로 줄입니다.

예를 들어, 300TB 환경에서 FlexGroup 볼륨은 200TB(1.6PB, 800TB, 400TB FlexGroup 볼륨 크기가 너무 커서 환경에 맞지 않는 경우)로 자동으로 프로비저닝됩니다.

ONTAP S3 주요 사용 사례

다음은 ONTAP S3 서비스에 대한 클라이언트 액세스의 주요 사용 사례입니다.

- FabricPool을 사용하여 비활성 데이터를 ONTAP의 버킷에 계층화하여 ONTAP to ONTAP 계층화를 지원합니다. 내의 버킷으로 계층화하거나 "로컬 클러스터"의 버킷으로의 계층화가 "원격 클러스터"모두 지원됩니다. ONTAP S3에 계층화하면 추가 FabricPool 라이센스나 새로운 기술을 관리할 필요 없이 비활성 데이터에 저렴한 ONTAP 시스템을 사용하고 새로운 플래시 용량에 대한 비용을 절감할 수 있습니다.
- ONTAP 9.12.1부터 NAS 프로토콜을 사용하도록 미리 구성된 에서도 S3 프로토콜을 활성화할 수 "멀티프로토콜 NAS 볼륨"있습니다. 멀티프로토콜 NAS 볼륨에서 S3 프로토콜이 사용되면 클라이언트 애플리케이션은 S3, NFS, SMB를 사용하여 데이터를 읽고 쓸 수 있으므로 다양한 추가 사용 사례가 열립니다. 가장 일반적인 사용 사례 중 하나는 볼륨에 데이터를 쓰는 NAS 클라이언트와 S3 클라이언트가 동일한 데이터를 읽고 분석, 비즈니스 인텔리전스, 머신 러닝, 광학 문자 인식 등과 같은 특수 작업을 수행하는 것입니다.

> ONTAP S3는 추가 하드웨어 및 관리 없이 기존 ONTAP 클러스터에서 S3 기능을 사용하려는 경우에 적합합니다. NetApp StorageGRID은 오브젝트 스토리지에 대한 NetApp의 대표적인 솔루션입니다. StorageGRID는 광범위한 S3 작업, 고급 ILM 기능 또는 ONTAP 기반 시스템에서 얻을 수 없는 용량을 활용해야 하는 네이티브 S3 애플리케이션에 권장됩니다. 자세한 내용은 를 "StorageGRID 설명서 "참조하십시오.

관련 정보

"FlexGroup 볼륨 관리"

계획

S3 오브젝트 스토리지를 위한 ONTAP 버전 및 플랫폼 지원

S3 오브젝트 스토리지는 ONTAP 9.8 이상을 사용하는 모든 AFF, FAS 및 ONTAP Select 플랫폼에서 지원됩니다.

FC, iSCSI, NFS, NVMe_oF 및 SMB 등의 다른 프로토콜과 마찬가지로, S3을 사용하려면 먼저 라이센스를 설치해야 ONTAP에서 사용할 수 있습니다. S3 라이센스는 비용이 들지 않는 라이센스이지만 ONTAP 9.8로 업그레이드하는 시스템에 설치해야 합니다. S3 라이센스는 NetApp 지원 사이트의 에서 다운로드할 수 "마스터 라이센스 키 페이지" 있습니다.

새로운 ONTAP 9.8 이상 시스템에는 S3 라이센스가 사전 설치되어 있습니다.

Cloud Volumes ONTAP

ONTAP S3는 Cloud Volumes ONTAP에서 사내 환경과 동일하게 구성 및 작동합니다. 단 한 가지 예외가 있습니다.

- Cloud Volumes ONTAP에서 버킷을 생성할 때는 CLI 절차를 사용하여 기본 FlexGroup 볼륨이 단일 노드의 애그리게이트만 사용하도록 해야 합니다. 노드가 지리적으로 서로 분리되어 있는 가용성 영역에 있고 지연 시간 문제가 발생하기 쉽기 때문에 여러 노드에서 애그리게이트를 사용하는 것은 성능에 영향을 미칩니다.

클라우드 공급자	**ONTAP** 버전
Google 클라우드	ONTAP 9.12.1 이상
설치하고	ONTAP 9.11.0 이상
Azure를 지원합니다	ONTAP 9.9.1 이상

NetApp ONTAP용 **Amazon FSx**

S3 오브젝트 스토리지는 ONTAP 9.11 이상을 사용하는 Amazon FSx for NetApp 서비스에서 지원됩니다.

MetroCluster를 통해 **S3** 지원

ONTAP 9.14.1부터 MetroCluster IP 및 FC 구성의 미러링된 애그리게이트에서 SVM에 S3 오브젝트 스토리지 서버를 사용하도록 설정할 수 있습니다.

ONTAP 9.12.1부터 MetroCluster IP 구성의 미러링되지 않은 Aggregate에서 SVM에서 S3 오브젝트 스토리지 서버를 활성화할 수 있습니다. MetroCluster IP 구성에서 미러링되지 않은 애그리게이트의 제한에 대한 자세한 내용은 를 참조하십시오. "미러링되지 않은 애그리게이트의 고려 사항"

SnapMirror S3는 MetroCluster 구성에서 지원되지 않습니다.

S3 ONTAP 9.7의 공용 미리 보기

ONTAP 9.7에서는 S3 오브젝트 스토리지가 공용 미리 보기로 도입되었습니다. 이 버전은 프로덕션 환경을 위해 제작되지 않았으며 ONTAP 9.8부터 더 이상 업데이트되지 않습니다. ONTAP 9.8 이상 릴리즈에서만 운영 환경에서 S3 오브젝트 스토리지를 지원합니다.

9.7 공용 미리 보기로 생성된 S3 버킷은 ONTAP 9.8 이상에서 사용할 수 있지만 향상된 기능을 활용할 수는 없습니다. 9.7 공용 미리 보기로 만든 버킷이 있는 경우 이러한 버킷의 내용을 9.8 버킷으로 마이그레이션하여 기능 지원, 보안 및 성능 향상을 지원해야 합니다.

ONTAP S3가 지원되는 작업

ONTAP S3 작업은 아래 명시된 경우를 제외하고 표준 S3 REST API에서 지원됩니다. 자세한 내용은 를 참조하십시오 "Amazon S3 API 참조".

> 이러한 S3 작업은 ONTAP에서 네이티브 S3 버킷을 사용할 때 특히 지원됩니다. 버전 관리, 개체 잠금 및 기타 기능과 관련된 작업과 같은 이러한 작업 중 일부는 을 사용할 때 지원되지 "S3 NAS 버킷(멀티프로토콜 NAS 볼륨의 S3)"않습니다.

특정 작업에 대해 별도로 언급하지 않는 한, ONTAP 9.8부터 다음과 같은 일반적인 요청 헤더가 지원됩니다.

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`

- `Date`
- `Expect`
- `Host`
- `x-amz-date`

버킷 작업

ONTAP에서 AWS S3 API를 사용하여 다음 작업이 지원됩니다.

버킷 작동	로 시작하는 **ONTAP** 지원
CreateBucket ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음 추가 헤더도 지원합니다. • `x-amz-bucket-object-lock-enabled`	ONTAP 9.11.1
삭제 버킷 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.11.1
DeleteBucketCors ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
DeleteBucketLifecycle ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
DeleteBuckketPolicy를 참조하십시오 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.12.1
GetBucketAcl ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
GetBucketCors ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
GetBuckLifecycleConfiguration 을 참조하십시오 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.13.1 *만료 작업만 지원됩니다.
GetBucketLocation ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.10.1
GetBucketPolicy ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.12.1

버킷 작동	로 시작하는 **ONTAP** 지원
GetBucketVersioning ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.11.1
HeadBucket ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
ListAllMyBuckets ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
ListBuckets ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
ListBucketVersions ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.11.1
퍼트버킷	• ONTAP 9.11.1 • ONTAP 9.8 - ONTAP REST API에서만 지원됩니다
PutBucketCors ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
PutBucketLifecycleConfiguration ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.13.1 * 만료 작업만 지원됩니다.
PutBucketPolicy ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.12.1
PutBucketVersioning ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.11.1

오브젝트 작업

ONTAP 9.9.1부터 ONTAP S3는 오브젝트 메타데이터 및 태그 지정을 지원합니다.

- PutObject 및 CreateMultipartUpload 를 사용하여 키-값 쌍을 포함합니다 `x-amz-meta-<key>.`

  예: ' x-amz-meta-project: ONTAP_S3'.

- GetObject 및 HeadObject 는 사용자 정의 메타데이터를 반환합니다.
- 메타데이터와 달리 태그는 다음을 사용하여 오브젝트와 독립적으로 읽을 수 있습니다.
  - PutObjectTagging
  - GetObjectTagging
  - DeleteObjectTagging 을 선택합니다

ONTAP 9.11.1부터 ONTAP S3는 다음과 같은 ONTAP API와 함께 개체 버전 관리 및 관련 작업을 지원합니다.

- GetBuckketVersioning 을 참조하십시오
- 목록 BuckketVersions
- PutBucketVersioning을 참조하십시오

특정 작업에 대해 별도로 언급하지 않는 한 다음 URI 쿼리 매개변수가 지원됩니다.

- `versionId`(ONTAP 9.12.1부터 시작되는 개체 작업에 필요함)

개체 작업입니다	로 시작하는 **ONTAP** 지원
AbortMultipartUpload 를 클릭합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 쿼리 매개변수도 지원합니다. `uploadId`	ONTAP 9.8
CompleteMultipartUpload를 클릭합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 쿼리 매개변수도 지원합니다. `uploadId`	ONTAP 9.8
CopyObject 를 선택합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 헤더도 지원합니다. • `x-amz-copy-source` • `x-amz-copy-source-if-match` • `x-amz-copy-source-if-modified-since` • `x-amz-copy-source-if-none-match` • `x-amz-copy-source-if-unmodified-since` • `x-amz-metadata-directive` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-tagging` • `x-amz-tagging-directive` • `x-amz-meta-<metadata-name>`	ONTAP 9.12.1

개체 작업입니다	로 시작하는 **ONTAP** 지원
CreateMultptUpload 를 클릭합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 헤더도 지원합니다. • `Cache-Control` • `Content-Disposition` • `Content-Encoding` • `Content-Language` • `Expires` • `x-amz-tagging` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-meta-<metadata-name>`	ONTAP 9.8
DeleteObject 를 클릭합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음 추가 헤더도 지원합니다. • `x-amz-bypass-governance-retention`	ONTAP 9.8
DeleteObjects ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음 추가 헤더도 지원합니다.* `x-amz-bypass-governance-retention`	ONTAP 9.11.1
DeleteObjectTagging 을 선택합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.9.1

개체 작업입니다	로 시작하는 **ONTAP** 지원
GetObject 를 참조하십시오 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 쿼리 매개변수도 지원합니다. • `partNumber` • `response-cache-control` • `response-content-disposition` • `response-content-encoding` • `response-content-language` • `response-content-type` • `response-expires` 그리고 이 추가 요청 헤더는 다음과 같습니다. • 범위	ONTAP 9.8
GetObjectAcl ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8
GetObjectAttributes ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음 추가 헤더도 지원합니다. • `x-amz-object-attributes`	ONTAP 9.17.1
GetObjectRetention ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.14.1
GetObjectTagging ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.9.1
HeadObject ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.8

개체 작업입니다	로 시작하는 **ONTAP** 지원
ListMultipartUpload 를 클릭합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 매개변수도 지원합니다. • `delimiter` • `key-marker` • `max-uploads` • `prefix` • `upload-id-marker`	ONTAP 9.8
ListObjects 를 선택합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 매개변수도 지원합니다. • `delimiter` • `encoding-type` • `marker` • `max-keys` • `prefix`	ONTAP 9.8
ListObjectsV2 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 매개변수도 지원합니다. • `continuation-token` • `delimiter` • `encoding-type` • `fetch-owner` • `max-keys` • `prefix` • `start-after`	ONTAP 9.8

개체 작업입니다	로 시작하는 **ONTAP** 지원
ListObjectVersions 를 선택합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 매개변수도 지원합니다. • `delimiter` • `encoding-type` • `key-marker` • `max-keys` • `prefix` • `version-id-marker`	ONTAP 9.11.1
목록 파트 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 매개변수도 지원합니다. • `max-parts` • `part-number-marker` • `uploadId`	ONTAP 9.8
PutObject 를 선택합니다 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 헤더도 지원합니다. • `Cache-Control` • `Content-Disposition` • `Content-Encoding` • `Content-Language` • `Expires` • `x-amz-tagging` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-meta-<metadata-name>`	ONTAP 9.8
PutObjectLockConfiguration ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.14.1

개체 작업입니다	로 시작하는 **ONTAP** 지원
PutObjectRetention ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음 추가 헤더도 지원합니다. • `x-amz-bypass-governance-retention`	ONTAP 9.14.1
PutObjectTagging ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원합니다.	ONTAP 9.9.1
업로드 파트	ONTAP 9.8
업로드파트 복사 ONTAP S3는 이 요청에 대한 모든 일반 매개변수와 헤더를 지원하며, 다음과 같은 추가 URI 매개변수도 지원합니다. • `partNumber` • `uploadId` 그리고 다음과 같은 추가 요청 헤더가 있습니다. • `x-amz-copy-source` • `x-amz-copy-source-if-match` • `x-amz-copy-source-if-modified-since` • `x-amz-copy-source-if-none-match` • `x-amz-copy-source-if-unmodified-since` • `x-amz-copy-source-range`	ONTAP 9.12.1

그룹 정책

이러한 작업은 S3에 한정되지 않으며 일반적으로 IAM(Identity and Management) 프로세스와 연결됩니다. ONTAP는 이러한 명령을 지원하지만 IAM REST API는 사용하지 않습니다.

- 정책을 생성합니다
- AttachGroup 정책

사용자 관리

이러한 작업은 S3에 한정되지 않으며 일반적으로 IAM 프로세스와 연관됩니다.

- CreateUser 를 선택합니다
- DeleteUser 를 클릭합니다
- 그룹 생성

- 삭제 그룹

릴리즈별 **S3** 작업

ONTAP 9.14.1

ONTAP 9.14.1에는 S3 오브젝트 잠금 지원이 추가되었습니다.

> 법적 증거 자료 보관 작업(정의된 보존 시간이 없는 잠금)은 지원되지 않습니다.

- GetObjectLockConfiguration 을 참조하십시오
- GetObjectRetention을 참조하십시오
- PutObjectLockConfiguration 을 참조하십시오
- PutObjectRetention

ONTAP 9.13.1

ONTAP 9.13.1에는 버킷 라이프사이클 관리 지원이 추가되었습니다.

- DeleteBucketLifecycleConfiguration을 참조하십시오
- GetBuckLifecycleConfiguration 을 참조하십시오
- PutBucketLifecycleConfiguration을 참조하십시오

ONTAP 9.12.1

ONTAP 9.12.1에는 버킷 정책 및 오브젝트 복사 기능이 추가되었습니다.

- DeleteBuckketPolicy를 참조하십시오
- GetBuckketPolicy를 참조하십시오
- BucketPolicy를 참조하십시오
- CopyObject 를 선택합니다
- 업로드파트 복사

ONTAP 9.11.1

ONTAP 9.11.1에는 버전 관리, 미리 지정된 URL, 청크 업로드 지원, S3 API를 사용한 버킷 생성 및 삭제와 같은 일반적인 S3 작업 지원이 추가되었습니다.

- ONTAP S3는 이제 청크 업로드 서명 요청을 지원합니다. `x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD`
- ONTAP S3는 이제 미리 설정된 URL을 사용하여 개체를 공유하거나 다른 사용자가 사용자 자격 증명 없이도 개체를 업로드할 수 있도록 클라이언트 응용 프로그램을 지원합니다.
- CreateBucket
- 삭제 버킷
- GetBuckketVersioning 을 참조하십시오
- 목록 BuckketVersions
- 퍼트버킷

- PutBucketVersioning을 참조하십시오
- DeleteObjects 를 클릭합니다
- ListObjectVersions 를 선택합니다

첫 번째 버킷이 될 때까지 기본 FlexGroup이 생성되지 않으므로 외부 클라이언트가 CreateBucket을 사용하여 버킷을 생성하려면 먼저 ONTAP에서 버킷을 생성해야 합니다.

ONTAP 9.10.1

ONTAP 9.10.1에는 SnapMirror S3 및 GetBucketLocation에 대한 지원이 추가되었습니다.

- GetBucketLocation 을 참조하십시오

ONTAP 9.9.1

ONTAP 9.9.1에서는 ONTAP S3에 개체 메타데이터 및 태그 지정 지원에 대한 지원을 추가합니다.

- PutObject 및 CreateMultipartUpload 는 이제 를 사용하여 키-값 쌍을 `x-amz-meta-<key>` 포함합니다. 예를 들면 다음과 `x-amz-meta-project: ontap_s3`같습니다.
- GetObject 및 HeadObject 는 이제 사용자 정의 메타데이터를 반환합니다.

태그는 버킷과 함께 사용할 수도 있습니다. 메타데이터와 달리 태그는 다음을 사용하여 오브젝트와 독립적으로 읽을 수 있습니다.

- PutObjectTagging
- GetObjectTagging
- DeleteObjectTagging 을 선택합니다

ONTAP S3 상호 운용성

ONTAP S3 서버는 일반적으로 이 표에 명시된 경우를 제외하고 다른 ONTAP 기능과 상호 작용합니다.

피처 영역	지원	지원되지 않습니다
Cloud Volumes ONTAP	• ONTAP 9.9.1 이상 릴리즈의 Azure 클라이언트 • ONTAP 9.11.0 이상 릴리즈의 AWS 클라이언트 • ONTAP 9.12.1 이상 릴리스의 Google Cloud 클라이언트	• ONTAP 9.8 및 이전 릴리스의 모든 클라이언트용 Cloud Volumes ONTAP

피처 영역	지원	지원되지 않습니다
데이터 보호	• Cloud Sync • 오브젝트 잠금, 거버넌스 및 규정 준수(ONTAP 9.14.1부터) • "개체 버전 관리" (ONTAP 9.11.1부터) • 미러링되지 않은 MetroCluster 애그리게이트(ONTAP 9.12.1부터) • 미러링된 MetroCluster 애그리게이트(ONTAP 9.14.1부터) • "SnapMirror S3" (ONTAP 9.10.1부터) • SnapMirror(NAS 볼륨만 해당, ONTAP 9.12.1부터) • SnapLock(NAS 볼륨 전용, ONTAP 9.14.1부터)	• 삭제 코딩 • NDMP • SMTape • SnapMirror (동기 및 비동기) • SnapMirror 클라우드 • SVM 재해 복구 • SyncMirror (SyncMirror 미러링된 집계는 ONTAP 9.14.1부터 MetroCluster 구성에서 지원됩니다. SyncMirror MetroCluster 구성 외부에서는 지원되지 않습니다.)
암호화	• NetApp 애그리게이트 암호화(NAE) • NetApp 볼륨 암호화(NVE) • NSE(NetApp 스토리지 암호화) • TLS/SSL	• 슬래그
MetroCluster 환경	-	SnapMirror S3
스토리지 효율성	• 중복 제거 • 압축 • 컴팩션	• 집계 수준 효율성(동일한 집계에 있는 멤버는 교차 볼륨 중복 제거를 활용할 수 있지만 다른 집계에 있는 멤버는 활용할 수 없음) • ONTAP S3 버킷을 포함하는 FlexGroup 볼륨의 볼륨 클론 • FlexClone 기술(볼륨, 파일 및 LUN)
서비스 품질(QoS)	• QoS 최대(천장) • 최소 QoS(층)	-

피처 영역	지원	지원되지 않습니다
추가 기능	• "S3 이벤트를 감사합니다" (ONTAP 9.10.1부터) • "버킷 수명 주기 관리" (ONTAP 9.13.1부터) • FabricPool 클라우드 계층(네이티브 S3만 해당) • FabricPool 로컬 계층(NAS 볼륨만 해당) • FlexCache 볼륨(ONTAP 9.18.1부터 지원)	• FPolicy를 참조하십시오 • Qtree • 할당량 • FabricPool 클라우드 계층(NAS 볼륨만 해당) • FabricPool 로컬 계층(네이티브 S3 전용)

ONTAP에서 S3를 사용한 검증된 타사 솔루션

S3는 보편적인 표준이며, 이는 지원되는 애플리케이션의 포괄적인 목록이 아닙니다. 단지 해당 파트너와 협력하여 검증된 솔루션 목록일 뿐입니다. 찾고 있는 솔루션이 목록에 없으면 NetApp 계정 담당자에게 문의하십시오.

네이티브 **S3** 버킷을 사용하여 검증된 타사 솔루션

- 아마존 SageMaker
- Apache Hadoop S3A 클라이언트
- 아파치 카프카
- 아파치 스파크
- Commvault(V11)
- Confluent Kafka
- NetBackup을 선택합니다
- 레드햇 키
- Rubrik으로 이동합니다
- 스노우플레이크
- 트리노
- Veeam(V12)

이러한 솔루션은 ONTAP에서 네이티브 S3 버킷을 사용할 때 특별히 검증됩니다. 버전 관리, 객체 잠금 및 기타 기능과 관련된 솔루션 등 일부 솔루션은 ONTAP을 사용할 때 지원되지 않습니다. "S3 NAS 버킷(멀티프로토콜 NAS 볼륨의 S3)" .

구성

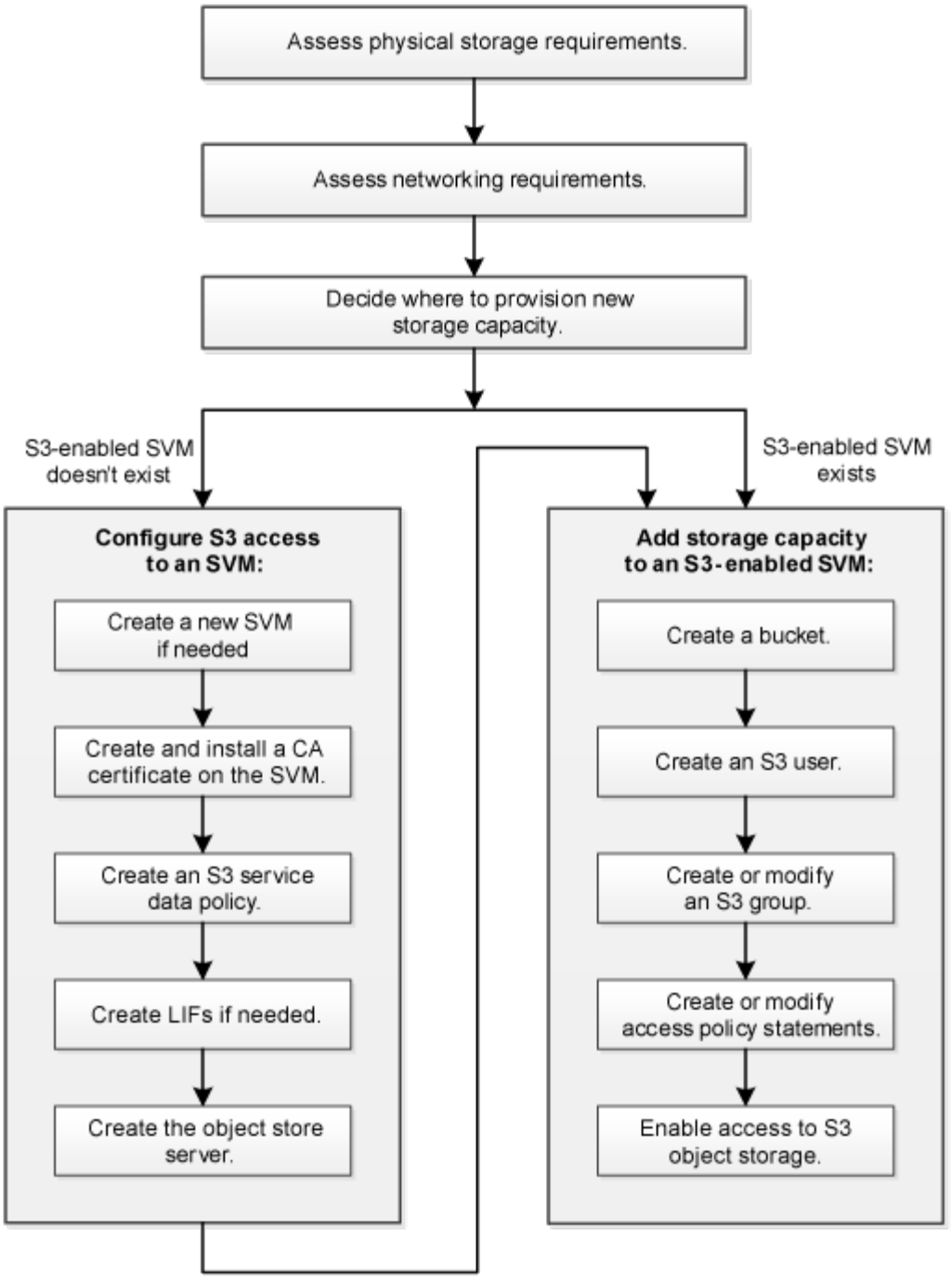
S3 구성 프로세스 정보

ONTAP S3 구성 워크플로우

S3 구성에는 물리적 스토리지 및 네트워킹 요구사항을 평가한 다음, 특정 목적에 맞는 워크플로우 선택, 즉 새 SVM 또는 기존 SVM에 대한 S3 액세스 구성, 또는 이미 S3 액세스용으로 완전히 구성된 기존 SVM에 버킷 및 사용자 추가 등이 포함됩니다.

클러스터와 클라이언트 간의 시간을 동기화하려면 NTP(네트워크 시간 프로토콜) 구성이 필요합니다. 클라이언트 액세스를 위해서는 ONTAP S3 객체 저장소와 클라이언트 간에 최소 15분 이상의 유효한 타임스탬프가 필요합니다. "NTP 구성 방법에 대해 알아보세요" .

System Manager를 사용하여 새 스토리지 VM에 대한 S3 액세스를 구성하면 인증서 및 네트워킹 정보를 입력하라는 메시지가 표시되고 스토리지 VM 및 S3 오브젝트 스토리지 서버가 단일 작업으로 생성됩니다.



ONTAP S3의 물리적 스토리지 요구사항을 평가합니다

클라이언트용 S3 스토리지를 프로비저닝하기 전에 새 오브젝트 저장소를 위한 기존 Aggregate의 공간이 충분한지 확인해야 합니다. 존재하지 않는 경우, 디스크를 기존 Aggregate에 추가하거나 원하는 유형 및 위치의 새 Aggregate를 생성할 수 있습니다.

이 작업에 대해

S3 지원 SVM에서 S3 버킷을 생성하면 FlexGroup 볼륨이 "자동으로 생성됩니다" 해당 버킷을 지원합니다. ONTAP Select에서 기본 애그리게이트와 FlexGroup 구성요소를 자동으로(기본값) 선택할 수도 있고, 기본 애그리게이트와 FlexGroup 구성요소를 직접 선택할 수도 있습니다.

Aggregate 및 FlexGroup 구성 요소(예: 기본 디스크에 특정한 성능 요구 사항이 있는 경우)를 지정하려는 경우, 애그리게이트 구성이 FlexGroup 볼륨 프로비저닝을 위한 모범 사례 지침을 준수해야 합니다. 자세한 내용:

- "FlexGroup 볼륨 관리"
- "NetApp 기술 보고서 4571-A: NetApp ONTAP FlexGroup 볼륨 모범 사례"

Cloud Volumes ONTAP에서 버킷을 제공하는 경우 기본 애그리게이트를 수동으로 선택하여 하나의 노드만 사용하도록 하는 것이 좋습니다. 두 노드의 애그리게이트를 사용하면 지리적으로 서로 분리되어 있는 가용성 영역에 노드가 있기 때문에 지연 시간 문제가 발생하기 때문에 성능에 영향을 미칠 수 있습니다. 에 대해 자세히 알아보십시오 "Cloud Volumes ONTAP용 버킷 생성".

ONTAP S3 서버를 사용하여 성능 계층과 동일한 클러스터에 로컬 FabricPool 용량 계층을 생성할 수 있습니다. 예를 들어, SSD 디스크가 한 HA 쌍에 연결되어 있고 _cold_data를 다른 HA 쌍의 HDD 디스크에 계층화하려는 경우 이 방법이 유용할 수 있습니다. 이 사용 사례에서 로컬 용량 계층이 포함된 S3 서버와 버킷은 성능 계층과 다른 HA 쌍이어야 합니다. 1노드 및 2노드 클러스터에서는 로컬 계층화가 지원되지 않습니다.

단계

1. 기존 애그리게이트에서 사용 가능한 공간 표시:

   '스토리지 집계 쇼'

   충분한 공간 또는 필수 노드 위치가 있는 Aggregate가 있는 경우 S3 구성의 이름을 기록합니다.

```
cluster-1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                         normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                         normal
6 entries were displayed.
```

2. 충분한 공간 또는 필수 노드 위치가 있는 애그리게이트가 없는 경우 'storage aggregate add-disks' 명령을 사용하여 기존 애그리게이트에 디스크를 추가하거나 'storage aggregate create' 명령을 사용하여 새 애그리게이트를 생성합니다.

관련 정보

- "스토리지 집계 추가 디스크"
- "저장소 집계 생성"

S3 스토리지를 클라이언트에 제공하기 전에 네트워킹이 S3 프로비저닝 요구사항을 충족하도록 올바르게 구성되었는지 확인해야 합니다.

시작하기 전에

다음과 같은 클러스터 네트워킹 객체를 구성해야 합니다.

- 물리적 및 논리적 포트
- 브로드캐스트 도메인
- 서브넷(필요한 경우)
- IPspace(기본 IPspace 외에 필요 시)
- 페일오버 그룹(필요에 따라 각 브로드캐스트 도메인의 기본 페일오버 그룹 추가)
- 외부 방화벽

이 작업에 대해

원격 FabricPool 용량(클라우드) 계층 및 원격 S3 클라이언트의 경우 데이터 SVM을 사용하고 데이터 LIF를 구성해야 합니다. FabricPool 클라우드 계층의 경우 클러스터 피어링이 필요하지 않으므로 인터클러스터 LIF도 구성해야 합니다.

로컬 FabricPool 용량 계층의 경우 시스템 SVM("클러스터")을 사용해야 하지만 LIF 구성을 위한 두 가지 옵션이 있습니다.

- 클러스터 LIF를 사용할 수 있습니다.

  이 옵션을 선택하면 더 이상 LIF 구성이 필요하지 않지만 클러스터 LIF의 트래픽이 증가합니다. 또한 로컬 계층은 다른 클러스터에서 액세스할 수 없습니다.

- 데이터 및 인터클러스터 LIF를 사용할 수 있습니다.

  이 옵션을 사용하려면 S3 프로토콜에 LIF를 설정하는 등 추가 구성이 필요합니다. 하지만 로컬 계층도 다른 클러스터에 대한 원격 FabricPool 클라우드 계층으로 액세스할 수 있습니다.

단계

1. 사용 가능한 물리적 포트 및 가상 포트를 표시합니다.

   네트워크 포트 쇼

   - 가능하면 데이터 네트워크에 대해 최고 속도의 포트를 사용해야 합니다.
   - 최상의 성능을 얻으려면 데이터 네트워크의 모든 구성 요소에 동일한 MTU 설정이 있어야 합니다.

2. 서브넷 이름을 사용하여 LIF에 대한 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 존재하고 사용 가능한 충분한 주소가 있는지 확인합니다.

   네트워크 서브넷 쇼

   서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 서브넷은 network subnet create 명령을 사용하여 생성된다.

에 대한 자세한 내용은 `network subnet show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 사용 가능한 IPspace 표시:

   네트워크 IPspace 쇼

   기본 IPspace 또는 사용자 지정 IPspace를 사용할 수 있습니다.

4. IPv6 주소를 사용하려면 클러스터에서 IPv6이 활성화되어 있는지 확인합니다.

   네트워크 옵션 IPv6 쇼

   필요한 경우 'network options ipv6 modify' 명령을 사용하여 IPv6을 사용하도록 설정할 수 있습니다.

관련 정보

- "네트워크 포트가 표시됩니다"
- "네트워크 옵션 IPv6"
- "네트워크 IPspace가 표시됩니다"
- "네트워크 서브넷 생성"

새로운 **ONTAP S3** 스토리지 용량을 프로비저닝할 위치를 결정합니다

새 S3 버킷을 생성하기 전에 새 SVM이나 기존 SVM에 배치할 것인지 결정해야 합니다. 이 결정에 따라 워크플로가 결정됩니다.

선택

- S3에 대해 활성화되지 않은 새 SVM 또는 SVM에서 버킷을 프로비저닝하려면 다음 항목의 단계를 완료하십시오.

  "S3를 위해 SVM을 생성합니다"

  "S3에 대한 버킷을 생성합니다"

  S3는 NFS 및 SMB와 SVM에서 공존할 수 있지만, 다음 중 하나가 참인 경우 새 SVM을 생성하도록 선택할 수 있습니다.

  - 클러스터에서 S3를 처음으로 사용하도록 설정하고 있습니다.
  - S3 지원을 활성화하지 않으려는 클러스터에 기존 SVM이 있습니다.
  - 클러스터에 하나 이상의 S3 기반 SVM이 있고 성능 특성이 다른 또 다른 S3 서버를 원합니다. SVM에서 S3를 활성화한 후 버킷 프로비저닝을 진행합니다.

- 기존 S3 기반 SVM에서 초기 버킷 또는 추가 버킷을 프로비저닝하려면 다음 항목의 단계를 완료하십시오.

  "S3에 대한 버킷을 생성합니다"

SVM에 대한 S3 액세스를 구성합니다

ONTAP S3용 **SVM**을 생성합니다

S3는 SVM의 다른 프로토콜과 공존할 수 있지만, 네임스페이스와 워크로드를 격리하기 위해 새 SVM을 생성할 수 있습니다.

이 작업에 대해

SVM에서 S3 오브젝트 스토리지만 제공하는 경우 S3 서버는 DNS 구성이 필요하지 않습니다. 그러나 다른 프로토콜을 사용하는 경우 SVM에서 DNS를 구성할 수 있습니다.

System Manager를 사용하여 새 스토리지 VM에 대한 S3 액세스를 구성하면 인증서 및 네트워킹 정보를 입력하라는 메시지가 표시되고 스토리지 VM 및 S3 오브젝트 스토리지 서버가 단일 작업으로 생성됩니다.

예 **23.** 단계

시스템 관리자

S3 서버 이름을 클라이언트가 S3 액세스에 사용할 FQDN(정규화된 도메인 이름)으로 입력할 준비가 되어 있어야 합니다. S3 서버 FQDN은 버킷 이름으로 시작하지 않아야 합니다.

인터페이스 역할 데이터에 대한 IP 주소를 입력할 준비가 되어 있어야 합니다.

외부 CA 서명 인증서를 사용하는 경우 이 절차를 수행하는 동안 해당 인증서를 입력하라는 메시지가 표시됩니다. 또한 시스템에서 생성한 인증서를 사용할 수도 있습니다.

1. 스토리지 VM에서 S3를 설정합니다.

   a. 새 스토리지 VM 추가: * 스토리지 > 스토리지 VM * 을 클릭한 다음 * 추가 * 를 클릭합니다.

      기존 스토리지 VM이 없는 새 시스템인 경우 * 대시보드 > 프로토콜 구성 * 을 클릭합니다.

   S3 서버를 기존 스토리지 VM에 추가하려면 * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭하고 * S3 * 아래를 클릭합니다.

   a. S3 * 활성화 를 클릭한 다음 S3 서버 이름 을 입력합니다.

   b. 인증서 유형을 선택합니다.

      시스템에서 생성한 인증서 또는 사용자 인증서 중 하나를 선택하든 클라이언트 액세스에 필요합니다.

   c. 네트워크 인터페이스를 입력합니다.

2. 시스템에서 생성한 인증서를 선택한 경우 새 스토리지 VM 생성이 확인되면 인증서 정보가 표시됩니다. 다운로드 * 를 클릭하고 클라이언트 액세스를 위해 저장합니다.

   ◦ 비밀 키는 다시 표시되지 않습니다.

   ◦ 인증서 정보가 다시 필요한 경우 * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭합니다.

CLI를 참조하십시오

1. S3 라이센스가 클러스터에서 라이센스되었는지 확인합니다.

```
system license show -package s3
```

   그렇지 않은 경우 영업 담당자에게 문의하십시오.

2. SVM 생성:

```
vserver create -vserver <svm_name> -subtype default -rootvolume
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security
-style unix -language C.UTF-8 -data-services <data-s3-server>
-ipspace <ipspace_name>
```

- '-rootvolume-security-style' 옵션에 UNIX 설정을 사용합니다.
- 기본 C. UTF-8 '-language' 옵션을 사용합니다.
- IPSpace 설정은 선택 사항입니다.

3. 새로 생성한 SVM의 구성 및 상태 확인:

```
vserver show -vserver <svm_name>
```

'Vserver 작동 상태' 필드에는 '실행 중' 상태가 표시되어야 합니다. 초기화 중 상태가 표시되는 경우 루트 볼륨 생성 등 일부 중간 작업이 실패한 것으로, SVM을 삭제하고 다시 생성해야 합니다.

예

다음 명령은 IPspace에서 데이터 액세스를 위한 SVM을 생성합니다. spaceba:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services data-s3-server -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

다음 명령을 실행하면 루트 볼륨 1GB 단위로 SVM이 생성되고 자동으로 시작되어 '실행 중' 상태에 있음을 알 수 있습니다. 루트 볼륨에는 규칙을 포함하지 않는 기본 엑스포트 정책이 있으므로 생성 시 루트 볼륨을 내보내지 않습니다. 기본적으로 vsadmin 사용자 계정은 생성되고 '잠김' 상태입니다. vsadmin 역할이 기본 vsadmin 사용자 계정에 할당됩니다.

```
cluster-1::> vserver show -vserver svm1.example.com
                                    Vserver: svm1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_svm1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                  List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

ONTAP S3 지원 **SVM**에 **CA** 인증서를 생성하고 설치합니다

S3 클라이언트는 S3 지원 SVM에 HTTPS 트래픽을 전송하기 위해 인증 기관(CA) 인증서가 필요합니다. CA 인증서는 클라이언트 애플리케이션과 ONTAP 개체 저장소 서버 간에 신뢰 관계를 만듭니다. 원격 클라이언트가 액세스할 수 있는 개체 저장소로 사용하기 전에 ONTAP 에 CA 인증서를 설치해야 합니다.

이 작업에 대해

S3 서버가 HTTP만 사용하도록 구성할 수 있고 CA 인증서 요구 사항 없이 클라이언트를 구성할 수는 있지만 HTTPS 트래픽을 CA 인증서가 있는 ONTAP S3 서버로 보호하는 것이 가장 좋습니다.

IP 트래픽이 클러스터 LIF만 통과하는 로컬 계층화 사용 사례에는 CA 인증서가 필요하지 않습니다.

이 절차의 지침은 ONTAP 자체 서명 인증서를 만들고 설치합니다. ONTAP에서 자체 서명된 인증서를 생성할 수 있지만 타사 인증 기관에서 서명한 인증서를 사용하는 것이 좋습니다. 자세한 내용은 관리자 인증 설명서를 참조하십시오.

"관리자 인증 및 RBAC"

및 추가 구성 옵션에 대한 자세한 `security certificate` 내용은 "ONTAP 명령 참조입니다"를 참조하십시오.

단계

1. 자체 서명된 디지털 인증서 생성:

   'Security certificate create - vserver_svm_name _ -type root-ca-common-name_ca_cert_name _'

   '-type root-ca' 옵션은 자체 서명된 디지털 인증서를 만들어 설치하여 CA(인증 기관)를 사용하여 다른 인증서에 서명합니다.

   '-common-name' 옵션은 SVM의 CA(인증 기관) 이름을 생성하며 인증서의 전체 이름을 생성할 때 사용됩니다.

   기본 인증서 크기는 2048비트입니다.

   예

   ```
   cluster-1::> security certificate create -vserver svm1.example.com -type
   root-ca -common-name svm1_ca

   The certificate's generated name for reference:
   svm1_ca_159D1587CE21E9D4_svm1_ca
   ```

   인증서의 생성된 이름이 표시되면 이 절차의 이후 단계를 위해 저장해야 합니다.

   에 대한 자세한 내용은 `security certificate create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 인증서 서명 요청 생성:

   'Security certificate generate - csr-common-name_s3_server_name_[additional_options]'

   서명 요청의 '-common-name' 매개변수는 S3 서버 이름(FQDN)이어야 합니다.

   필요한 경우 SVM에 대한 위치 및 기타 세부 정보를 제공할 수 있습니다.

   그만큼 `-dns-name` 매개변수는 클라이언트가 DNS 이름 목록을 제공하는 주체 대체 이름 확장을 지정하기 위해 종종 필요합니다.

   그만큼 `-ipaddr` 클라이언트는 IP 주소 목록을 제공하는 주체 대체 이름 확장을 지정하기 위해 종종 매개변수가 필요합니다.

   나중에 참조할 수 있도록 인증서 요청과 개인 키의 복사본을 보관하라는 메시지가 표시됩니다.

   에 대한 자세한 내용은 `security certificate generate-csr` "ONTAP 명령 참조입니다"을 참조하십시오.

3. SVM_CA를 사용하여 CSR에 서명하여 S3 서버의 인증서를 생성합니다.

   '보안 인증서 서명 - vserver_svm_name_-ca_ca_cert_name_-ca-serial_ca_cert_serial_number_[additional_options]'

   이전 단계에서 사용한 명령 옵션을 입력합니다.

- '-ca' — 1단계에서 입력한 CA의 공통 이름입니다.
- '-ca-serial' — 1단계의 CA 일련 번호입니다. 예를 들어 CA 인증서 이름이 svm1_ca_159D1587CE21E9D4_svm1_ca인 경우 일련 번호는 159D1587CE21E9D4입니다.

  기본적으로 서명된 인증서는 365일 후에 만료됩니다. 다른 값을 선택하고 다른 서명 세부 정보를 지정할 수 있습니다.

  메시지가 표시되면 2단계에서 저장한 인증서 요청 문자열을 복사하여 입력합니다.

서명된 인증서가 표시되면 나중에 사용할 수 있도록 저장합니다.

4. S3 기반 SVM에 서명된 인증서 설치:

   'Security certificate install-type server-vserver_svm_name_'

   메시지가 표시되면 인증서와 개인 키를 입력합니다.

   인증서 체인이 필요한 경우 중간 인증서를 입력할 수 있습니다.

   개인 키와 CA 서명 디지털 인증서가 표시되면 나중에 참조할 수 있도록 저장합니다.

5. 공개 키 인증서 받기:

   'Security certificate show -vserver_svm_name_-common-name_ca_cert_name_-type root-ca-instance'

   나중에 클라이언트 측 구성을 위해 공개 키 인증서를 저장합니다.

   예

```
cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca  -instance

                      Name of Vserver: svm1.example.com
           FQDN or Custom Common Name: svm1_ca
          Serial Number of Certificate: 159D1587CE21E9D4
                Certificate Authority: svm1_ca
                  Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
              Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
               Certificate Start Date: Thu May 09 10:58:39 2020
          Certificate Expiration Date: Fri May 08 10:58:39 2021
               Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                         Country Name: US
               State or Province Name:
                        Locality Name:
                    Organization Name:
                    Organization Unit:
Contact Administrator's Email Address:
                             Protocol: SSL
                      Hashing Function: SHA256
              Self-Signed Certificate: true
       Is System Internal Certificate: false
```

관련 정보

- "보안 인증서 설치"
- "보안 인증서가 표시됩니다"
- "보안 인증서 서명"

ONTAP S3 서비스 데이터 정책을 생성합니다

S3 데이터 및 관리 서비스에 대한 서비스 정책을 생성할 수 있습니다. LIF에서 S3 데이터 트래픽을 활성화하려면 S3 서비스 데이터 정책이 필요합니다.

이 작업에 대해

데이터 LIF 및 인터클러스터 LIF를 사용하는 경우 S3 서비스 데이터 정책이 필요합니다. 로컬 계층화 사용 사례에서 클러스터 LIF를 사용하는 경우에는 필요하지 않습니다.

LIF에 서비스 정책을 지정한 경우, 이 정책을 사용하여 LIF에 대한 기본 역할, 페일오버 정책 및 데이터 프로토콜 목록을 구성합니다.

SVM 및 LIF에 여러 프로토콜을 구성할 수 있지만 오브젝트 데이터를 제공할 때 S3가 유일한 프로토콜이 되도록 하는

것이 좋습니다.

단계

1. 권한 설정을 고급으로 변경합니다.

   세트 프리빌리지 고급

2. 서비스 데이터 정책 생성:

   'network interface service-policy create-vserver_svm_name_-policy_policy_name_-services data-core, data-s3-server'

   ONTAP S3을 활성화하는 데 필요한 서비스는 데이터 코어(Data-Core) 및 데이터-S3-서버(Data-S3-Server) 서비스뿐입니다. 단, 다른 서비스는 필요에 따라 포함할 수 있습니다.

   에 대한 자세한 내용은 `network interface service-policy create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP S3에 대한 데이터 **LIF**를 생성합니다

새 SVM을 생성한 경우 S3 액세스를 위해 생성하는 전용 LIF는 데이터 LIF가 되어야 합니다.

시작하기 전에

- 기본 물리적 또는 논리적 네트워크 포트가 관리 `up` 상태로 구성되어야 합니다. 에 대한 자세한 내용은 `up` "ONTAP 명령 참조입니다"을 참조하십시오.
- 서브넷 이름을 사용하여 LIF에 대한 IP 주소 및 네트워크 마스크 값을 할당하려는 경우, 서브넷이 이미 존재해야 합니다.

  서브넷에는 동일한 계층 3 서브넷에 속하는 IP 주소 풀이 포함되어 있습니다. 네트워크 서브넷 만들기 명령을 사용하여 만듭니다.

  에 대한 자세한 내용은 `network subnet create` "ONTAP 명령 참조입니다"을 참조하십시오.

- LIF 서비스 정책이 이미 존재해야 합니다.
- 모범 사례로서, 데이터 액세스에 사용되는 LIF(Data-S3-서버)와 관리 작업(관리-https)에 사용되는 LIF는 별도로 두어야 합니다. 두 서비스 모두 같은 LIF에서 활성화해서는 안 됩니다.
- DNS 레코드에는 Data-S3-서버가 연결된 LIF의 IP 주소만 있어야 합니다. 다른 LIF의 IP 주소가 DNS 레코드에 지정된 경우 다른 서버에서 ONTAP S3 요청을 처리할 수 있으므로 예기치 않은 응답이나 데이터 손실이 발생할 수 있습니다.

이 작업에 대해

- 동일한 네트워크 포트에서 IPv4 및 IPv6 LIF를 모두 생성할 수 있습니다.
- 클러스터에 LIF가 많은 경우 'network interface capacity show' 명령을 사용하여 클러스터에서 지원되는 LIF 용량과 각 노드에서 지원되는 LIF 용량을 확인할 수 있습니다 (고급 권한 수준에서).

  및 `network interface capacity details show` 에 대한 자세한 `network interface capacity show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

- 원격 FabricPool 용량(클라우드) 계층화를 사용하는 경우 인터클러스터 LIF도 구성해야 합니다.

단계

1. LIF 생성:

   'network interface create-vserver_svm_name_-lif_lif_name_-service-policy_service_policy_names_-home-node_node_name_-home-port_port_name_{-address_netmask_ip_address_|-subnet-name_subnet_subnet_name_} - firewall-policy data-auto-revert_revert_revert_false

   - 홈 노드는 LIF에서 네트워크 인터페이스 되돌리기 명령을 실행할 때 LIF가 반환하는 노드입니다.

     에 대한 자세한 내용은 `network interface revert` "ONTAP 명령 참조입니다"을 참조하십시오.

     또한 LIF가 '-auto-revert' 옵션을 사용하여 홈 노드 및 홈 포트로 자동으로 되돌아가는지 여부를 지정할 수도 있습니다.

   - '-home-port'는 LIF에서 '네트워크 인터페이스 되돌리기' 명령을 실행하면 LIF가 반환되는 물리적 또는 논리적 포트입니다.
   - IP 주소는 '-address' 및 '-netmask' 옵션을 사용하여 지정하거나 '-subnet_name' 옵션을 사용하여 서브넷에서 할당을 활성화할 수 있습니다.
   - 서브넷을 사용하여 IP 주소와 네트워크 마스크를 제공하면, 서브넷에 정의된 서브넷이 해당 서브넷을 사용하여 LIF를 생성할 때 해당 게이트웨이에 대한 기본 경로가 SVM에 자동으로 추가됩니다.
   - 서브넷을 사용하지 않고 수동으로 IP 주소를 할당하는 경우 다른 IP 서브넷에 클라이언트 또는 도메인 컨트롤러가 있는 경우 게이트웨이에 대한 기본 라우트를 구성해야 할 수 있습니다. SVM 내에서 정적 라우트를 생성하는 방법에 대한 자세한 `network route create` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.
   - '-firewall-policy' 옵션의 경우 LIF 역할과 동일한 기본 data를 사용합니다.

     필요에 따라 나중에 사용자 지정 방화벽 정책을 만들고 추가할 수 있습니다.

     ⓘ ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 참조하십시오 "LIF의 방화벽 정책을 구성합니다".

   - '-자동 되돌리기'를 사용하면 시작, 관리 데이터베이스의 상태 변경 또는 네트워크 연결이 이루어지는 시기에 데이터 LIF가 홈 노드로 자동 복구되는지 여부를 지정할 수 있습니다. 기본 설정은 false로 설정되어 있지만 사용자 환경의 네트워크 관리 정책에 따라 false로 설정할 수 있습니다.
   - '-service-policy' 옵션은 사용자가 만든 데이터 및 관리 서비스 정책과 필요한 기타 정책을 지정합니다.

2. '-address' 옵션에서 IPv6 주소를 할당하려면 다음과 같이 하십시오.

   a. network NDP prefix show 명령을 사용하여 다양한 인터페이스에서 습득한 RA prefix 목록을 볼 수 있다.

      고급 권한 수준에서 network NDP prefix show 명령을 사용할 수 있다.

   b. IPv6 주소를 수동으로 구성하려면 접두사:id 형식을 사용합니다.

      접두사는 다양한 인터페이스에서 습득한 접두사입니다.

   ID를 도출하려면 임의의 64비트 16진수 숫자를 선택합니다.

3. 'network interface show' 명령을 사용하여 LIF가 성공적으로 생성되었는지 확인합니다.
4. 구성된 IP 주소에 연결할 수 있는지 확인합니다.

다음을 확인하려면...	사용...
IPv4 주소입니다	네트워크 핑
IPv6 주소입니다	네트워크 핑6

예

다음 명령을 실행하면 'y-s3-policy' 서비스 정책에 할당된 S3 데이터 LIF를 생성하는 방법이 표시됩니다.

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

다음 명령을 실행하면 cluster-1의 모든 LIF가 표시됩니다. 데이터 LIF datalif1 및 datalif3은 IPv4 주소로 구성되고 datalif4는 IPv6 주소로 구성됩니다.

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

관련 정보

- "네트워크 Ping"
- "네트워크 인터페이스"
- "네트워크 NDP 접두사가 표시됩니다"

ONTAP S3를 사용하여 원격 **FabricPool** 계층화를 위한 인터클러스터 **LIF**를 생성합니다

ONTAP S3를 사용하여 원격 FabricPool 용량(클라우드) 계층화를 활성화하는 경우 인터클러스터 LIF를 구성해야 합니다. 데이터 네트워크와 공유하는 포트에 대한 인터클러스터 LIF를 구성할 수 있습니다. 이렇게 하면 인터클러스터 네트워킹에 필요한 포트 수가 줄어듭니다.

시작하기 전에

- 기본 물리적 또는 논리적 네트워크 포트가 관리 `up` 상태로 구성되어야 합니다. 에 대한 자세한 내용은 `up` "ONTAP 명령 참조입니다"을 참조하십시오.
- LIF 서비스 정책이 이미 존재해야 합니다.

이 작업에 대해

인터클러스터 LIF는 로컬 Fabric 풀 계층화나 외부 S3 애플리케이션을 제공하기 위해 필요하지 않습니다.

단계

1. 클러스터의 포트 나열:

   네트워크 포트 쇼

   다음 예에서는 "cluster01"의 네트워크 포트를 보여줍니다.

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 시스템 SVM에 대한 인터클러스터 LIF 생성:

   'network interface create-vserver cluster-lif_LIF_name_-service-policy default-인터클러스터-home -node_node_-home-port_port_-address_port_ip_-netmask_mask_'

   다음 예에서는 인터클러스터 LIF 'cluster01_icl01'과 'cluster01_icl02'를 생성합니다.

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 인터클러스터 LIF가 생성되었는지 확인합니다.

   네트워크 인터페이스 show-service-policy default-인터클러스터

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0c
true
```

4. 인터클러스터 LIF가 중복되는지 확인합니다.

   네트워크 인터페이스 show-service-policy default-인터클러스터-failover를 선택합니다

   다음 예에서는 e0c 포트의 인터클러스터 LIF 'cluster01_icl01'과 cluster01_icl02가 e0d 포트로 페일오버된다는 것을 보여 줍니다.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP S3 오브젝트 저장소 서버를 생성합니다

ONTAP 오브젝트 저장소 서버는 ONTAP NAS 및 SAN 서버에서 제공하는 파일 또는 블록 스토리지가 아니라 데이터를 S3 오브젝트로 관리합니다.

시작하기 전에

S3 서버 이름을 클라이언트가 S3 액세스에 사용할 FQDN(정규화된 도메인 이름)으로 입력할 준비가 되어 있어야 합니다. FQDN은 버킷 이름으로 시작할 수 없습니다. 가상 호스팅 스타일을 사용하여 버킷에 액세스하는 경우 서버 이름이 로 `mydomain.com`사용됩니다. `bucketname.mydomain.com`예를 들어,

자체 서명된 CA 인증서(이전 단계에서 만든 인증서) 또는 외부 CA 공급업체에서 서명한 인증서가 있어야 합니다. IP 트래픽이 클러스터 LIF만 통과하는 로컬 계층화 사용 사례에는 CA 인증서가 필요하지 않습니다.

이 작업에 대해

오브젝트 저장소 서버가 생성되면 UID 0의 루트 사용자가 생성됩니다. 이 루트 사용자에 대해 액세스 키 또는 암호 키가 생성되지 않았습니다. ONTAP 관리자는 'object-store-server users Regenerate-keys' 명령을 실행하여 이 사용자의 액세스 키와 비밀 키를 설정해야 합니다.

> NetApp 모범 사례로서 이 루트 사용자를 사용하지 마십시오. 루트 사용자의 액세스 키 또는 암호 키를 사용하는 모든 클라이언트 애플리케이션은 오브젝트 저장소의 모든 버킷과 개체에 대한 모든 액세스 권한을 가집니다.

에 대한 자세한 내용은 `vserver object-store-server` "ONTAP 명령 참조입니다"을 참조하십시오.

예 **24.** 단계

시스템 관리자

기존 스토리지 VM에 S3 서버를 추가하는 경우 이 절차를 사용합니다. S3 서버를 새 스토리지 VM에 추가하려면 을 참조하십시오 "S3를 위한 스토리지 SVM 생성".

인터페이스 역할 데이터에 대한 IP 주소를 입력할 준비가 되어 있어야 합니다.

1. 기존 스토리지 VM에서 S3를 설정합니다.
   a. 스토리지 VM을 선택합니다. * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭하고 * S3 * 아래를 클릭합니다.
   b. S3 * 활성화 를 클릭한 다음 S3 서버 이름 을 입력합니다.
   c. 인증서 유형을 선택합니다.

      시스템에서 생성한 인증서 또는 사용자 인증서 중 하나를 선택하든 클라이언트 액세스에 필요합니다.

   d. 네트워크 인터페이스를 입력합니다.
2. 시스템에서 생성한 인증서를 선택한 경우 새 스토리지 VM 생성이 확인되면 인증서 정보가 표시됩니다. 다운로드 * 를 클릭하고 클라이언트 액세스를 위해 저장합니다.
   - 비밀 키는 다시 표시되지 않습니다.
   - 인증서 정보가 다시 필요한 경우 * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 선택한 다음 * 설정 * 을 클릭합니다.

CLI를 참조하십시오

1. S3 서버 생성:

   ```
   vserver object-store-server create -vserver svm_name -object-store-server
   s3_server_fqdn -certificate-name server_certificate_name -comment text
   [additional_options]
   ```

   S3 서버를 생성할 때 또는 나중에 언제든지 추가 옵션을 지정할 수 있습니다.

   - 로컬 계층화를 구성하는 경우 SVM 이름은 데이터 SVM 또는 시스템 SVM(클러스터) 이름일 수 있습니다.
   - 인증서 이름은 서버 CA 인증서(중간 또는 루트 CA 인증서)가 아니라 서버 인증서(최종 사용자 또는 리프 인증서)의 이름이어야 합니다.
   - HTTPS는 기본적으로 포트 443에서 활성화됩니다. '-secure-listener-port' 옵션을 사용하여 포트 번호를 변경할 수 있습니다.

     HTTPS가 활성화된 경우 SSL/TLS와의 올바른 통합을 위해 CA 인증서가 필요합니다. ONTAP 9.15.1부터 TLS 1.3은 S3 오브젝트 스토리지에서 지원됩니다.

   - HTTP는 기본적으로 해제되어 있습니다. 활성화되면 서버는 포트 80에서 수신 대기합니다. 를 사용하여 활성화할 수 있습니다 `-is-http-enabled` 옵션을 선택하거나 를 사용하여 포트 번호를 변경합니다 `-listener-port` 옵션을 선택합니다.

     HTTP가 활성화되면 요청과 응답이 네트워크를 통해 일반 텍스트로 전송됩니다.

2. S3이 구성되었는지 확인:

   'vserver object-store-server show'를 선택합니다

예

이 명령은 모든 객체 스토리지 서버의 구성 값을 확인합니다.

```
cluster1::> vserver object-store-server show

            Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                   Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

S3 지원 SVM에 스토리지 용량 추가

ONTAP S3 버킷을 생성합니다

S3 오브젝트는 _ bucket _ 에 유지됩니다. 다른 디렉터리 내의 디렉터리 안에 파일로 중첩되지 않습니다.

시작하기 전에

S3 서버가 포함된 스토리지 VM이 이미 존재해야 합니다.

이 작업에 대해

- ONTAP 9.14.1부터는 S3 FlexGroup 볼륨에 버킷이 생성되면 자동 크기 조정이 활성화되었습니다. 따라서 기존 및 새 FlexGroup 볼륨에서 버킷 생성 중에 과도한 용량 할당이 필요 없습니다. FlexGroup 볼륨의 크기는 다음 지침에 따라 최소 필요한 크기로 조정됩니다. 필요한 최소 크기는 FlexGroup 볼륨에 있는 모든 S3 버킷의 총 크기입니다.
  - ONTAP 9.14.1부터 새 버킷 생성 시 S3 FlexGroup 볼륨이 생성되는 경우 필요한 최소 크기로 FlexGroup 볼륨이 생성됩니다.
  - ONTAP 9.14.1 전에 S3 FlexGroup 볼륨을 생성한 경우, ONTAP 9.14.1 이후 생성되거나 삭제된 첫 번째 버킷이 FlexGroup 볼륨의 크기를 필요한 최소 크기로 조정합니다.
  - ONTAP 9.14.1 전에 S3 FlexGroup 볼륨이 생성되었고 이미 필요한 최소 크기가 있는 경우, ONTAP 9.14.1 이후 버킷 생성 또는 삭제에 의해 S3 FlexGroup 볼륨의 크기가 유지됩니다.
- 스토리지 서비스 수준은 *value*, *performance* 및 _extreme_default 수준으로 사전 정의된 QoS(Adaptive Quality of Service) 정책 그룹입니다. 기본 스토리지 서비스 수준 대신 맞춤형 QoS 정책 그룹을 정의하여 버킷에 적용할 수도 있습니다. 스토리지 서비스 정의에 대한 자세한 내용은 을 "스토리지 서비스 정의"참조하십시오. 성능 관리에 대한 자세한 내용은 을 "성능 관리"참조하십시오. ONTAP 9.8부터는 스토리지 용량 할당 시 QoS가 기본적으로

사용하도록 설정됩니다. 프로비저닝 프로세스 도중 또는 나중에 QoS를 사용하지 않도록 설정하거나 사용자 지정 QoS 정책을 선택할 수 있습니다.

- 로컬 용량 계층화를 구성하는 경우, S3 서버가 있는 시스템 스토리지 VM이 아닌 데이터 스토리지 VM에 버킷 및 사용자를 생성합니다.
- 원격 클라이언트 액세스의 경우 S3 지원 스토리지 VM에서 버킷을 구성해야 합니다. S3이 활성화되지 않은 스토리지 VM에서 버킷을 생성하는 경우 로컬 계층화에만 사용할 수 있습니다.
- ONTAP 9.14.1부터 가능합니다 "MetroCluster 구성의 경우 미러링된 또는 미러링되지 않은 애그리게이트에 버킷을 생성합니다".
- CLI의 경우 버킷을 생성할 때 두 가지 프로비저닝 옵션이 있습니다.
  - ONTAP Select에서 기본 애그리게이트와 FlexGroup 구성 요소 사용(기본값)
    - ONTAP는 애그리게이트를 자동으로 선택하여 첫 번째 버킷에 대한 FlexGroup 볼륨을 생성 및 구성합니다. 플랫폼에 사용할 수 있는 가장 높은 서비스 수준이 자동으로 선택되거나 스토리지 서비스 수준을 지정할 수 있습니다. 스토리지 VM에서 나중에 추가하는 모든 추가 버킷은 동일한 기본 FlexGroup 볼륨을 갖게 됩니다.
    - 또는 버킷이 계층화에 사용되는지 여부를 지정할 수 있습니다. 이 경우 ONTAP는 계층형 데이터에 대해 최적의 성능을 제공하는 경제적인 미디어를 선택하려고 합니다.
  - 기본 애그리게이트 및 FlexGroup 구성요소 선택(고급 권한 명령 옵션 필요): 버킷과 FlexGroup 볼륨을 생성해야 하는 애그리게이트를 수동으로 선택한 다음, 각 애그리게이트에서 구성요소 수를 지정할 수 있습니다. 추가 버킷 추가 시:
    - 새 버킷에 대해 Aggregate 및 구성요소를 지정하는 경우 새 FlexGroup가 새 버킷에 대해 생성됩니다.
    - 새 버킷의 Aggregate 및 구성요소를 지정하지 않을 경우 새 버킷이 기존 FlexGroup에 추가됩니다. 을 참조하십시오 FlexGroup 볼륨 관리 를 참조하십시오.

      버킷을 생성할 때 Aggregate 및 구성요소를 지정하면 QoS 정책 그룹, 기본값 또는 사용자 지정이 적용되지 않습니다. 나중에 'vserver object-store-server bucket modify' 명령을 사용하여 이 작업을 수행할 수 있습니다.

    에 대한 자세한 내용은 `vserver object-store-server bucket modify` "ONTAP 명령 참조입니다"을 참조하십시오.
- 참고: * Cloud Volumes ONTAP에서 버킷을 제공하는 경우 CLI 절차를 사용해야 합니다. 기본 애그리게이트는 한 노드만 사용하는지 확인하기 위해 수동으로 선택하는 것이 좋습니다. 두 노드의 애그리게이트를 사용하면 지리적으로 서로 분리되어 있는 가용성 영역에 노드가 있기 때문에 지연 시간 문제가 발생하기 때문에 성능에 영향을 미칠 수 있습니다.

ONTAP CLI로 **S3** 버킷을 생성합니다

1. Aggregate 및 FlexGroup 구성 요소를 직접 선택하려면 권한 수준을 Advanced(고급)로 설정하십시오. 그렇지 않으면 admin 권한 수준이 Advanced(고급)로 설정됩니다
2. 버킷 생성:

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> -size [integer{KB|MB|GB|TB|PB}] [-comment text]
   [additional_options]
   ```

   스토리지 VM 이름은 데이터 스토리지 VM 또는 일 수 있습니다 `Cluster` 로컬 계층화를 구성하는 경우 (시스템 스토리지 VM 이름)

ONTAP에서 성능 또는 사용량을 기준으로 버킷을 생성하려면 다음 옵션 중 하나를 사용하십시오.

- 서비스 레벨

  가치, 성능, 익스트림 등의 가치 중 하나로 스토리지 서비스 수준 옵션을 포함시키십시오.

- 계층화

  사용된 용량 계층 TRUE 옵션을 포함합니다.

  기본 FlexGroup 볼륨을 생성할 애그리게이트를 지정하려면 다음 옵션을 사용하십시오.

- '-aggr-list' 매개 변수는 FlexGroup 볼륨 구성요소에 사용할 애그리게이트 목록을 지정합니다.

  목록의 각 항목은 지정된 애그리게이트에 구성요소를 생성합니다. Aggregate를 여러 번 지정하여 Aggregate에 여러 구성요소를 생성할 수 있습니다.

FlexGroup 볼륨 전체에서 일관된 성능을 위해서는 모든 애그리게이트에서 동일한 디스크 유형과 RAID 그룹 구성을 사용해야 합니다.

- '-aggr-list-multiplier' 매개 변수는 FlexGroup 볼륨을 생성할 때 '-aggr-list' 매개 변수로 나열된 애그리게이트를 반복하는 횟수를 지정합니다.

  '-aggr-list-multiplier' 파라미터의 기본값은 4이다.

3. 필요한 경우 QoS 정책 그룹을 추가합니다.

   'vserver object-store-server bucket modify -bucket_bucket_name_-qos-policy-group_qos_policy_group_'

4. 버킷 생성 확인:

   'vserver object-store-server bucket show[-instance]'

예

다음 예에서는 스토리지 VM용 버킷을 생성합니다 `vs1` 있습니다 `1TB` 집계 지정:

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

System Manager로 S3 버킷을 생성합니다

1. S3 지원 스토리지 VM에 새 버킷을 추가합니다.
   a. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력합니다.
      - 이 지점에서 * Save * (저장 *)를 클릭하면 다음 기본 설정으로 버킷이 생성됩니다.
        - 그룹 정책이 이미 적용되어 있지 않으면 버킷에 대한 액세스 권한이 사용자에게 부여되지 않습니다.

오브젝트 저장소에 대한 무제한 액세스 권한이 있으므로 S3 루트 사용자를 사용하여 ONTAP 오브젝트 스토리지를 관리하고 권한을 공유해서는 안 됩니다. 대신 할당한 관리 권한이 있는 사용자 또는 그룹을 만듭니다.

- 시스템에서 가장 높은 수준의 서비스 품질(성능) 수준입니다.
- 이 기본값으로 버킷을 만들려면 * 저장 * 을 클릭합니다.

추가 권한 및 제한 사항을 구성합니다

버킷을 구성할 때 * 추가 옵션 * 을 클릭하여 오브젝트 잠금, 사용자 권한 및 성능 수준에 대한 설정을 구성하거나 나중에 이 설정을 수정할 수 있습니다.

FabricPool 계층화에 S3 오브젝트 저장소를 사용하려는 경우 성능 서비스 수준이 아닌 * 계층화에 사용 * (계층 데이터에 최적의 성능을 제공하는 저비용 미디어 사용)을 선택하는 것이 좋습니다.

버킷에서 버전 관리를 사용하도록 설정한 경우, S3 클라이언트를 사용하여 오브젝트의 특정 버전에 오브젝트 잠금 보존 시간을 배치할 수 있습니다. 개체의 특정 버전을 잠그더라도 개체의 다른 버전이 삭제되는 것을 막을 수는 없습니다. 나중에 복구할 수 있도록 개체의 버전 관리를 활성화하려면 * 버전 관리 활성화 * 를 선택합니다. 버킷에서 오브젝트 잠금을 사용하도록 설정하는 경우 버전 관리가 기본적으로 활성화됩니다. 개체 버전 관리에 대한 자세한 내용은 를 "Amazon용 S3 버킷에서 버전 관리 사용"참조하십시오.

9.14.1부터 S3 버킷에서 오브젝트 잠금이 지원됩니다. 버킷이 생성될 때 S3 오브젝트 잠금을 활성화해야 합니다. 기존 버킷에서는 오브젝트 잠금을 활성화할 수 없습니다. 오브젝트 잠금은 네이티브 S3 사용 사례에서만 사용할 수 있습니다. S3 프로토콜을 사용하도록 구성된 멀티프로토콜 NAS 볼륨은 SnapLock를 사용하여 WORM 스토리지에 데이터를 커밋해야 합니다. S3 오브젝트 잠금에는 표준 SnapLock 라이센스가 필요합니다. 이 라이센스는 에 "ONTAP 1 을 참조하십시오"포함되어 있습니다.

ONTAP One 이전에는 SnapLock 라이센스가 보안 및 규정 준수 번들에 포함되어 있었습니다. 보안 및 규정 준수 번들은 더 이상 제공되지 않지만 여전히 유효합니다. 현재는 필요하지 않지만 기존 고객은 선택할 수 "ONTAP One으로 업그레이드하십시오"있습니다. . "설치합니다" 객체 잠금을 활성화하기 전에 먼저 이 작업을 수행해야 합니다.

SnapLock 라이센스가 설치되어 있음을 확인한 후 버킷의 객체가 삭제되거나 덮어쓰지 않도록 보호하려면 * 개체 잠금 활성화 * 를 선택합니다. 잠금은 모든 오브젝트 또는 특정 버전에서 활성화될 수 있으며 클러스터 노드에 대해 SnapLock 컴플라이언스 클록이 초기화된 경우에만 활성화됩니다. 다음 단계를 수행하십시오.

1. 클러스터의 어떤 노드에서도 SnapLock 컴플라이언스 클록이 초기화되지 않으면 * SnapLock 규정 준수 클록 초기화 * 버튼이 나타납니다. Initialize SnapLock Compliance Clock * 을 클릭하여 클러스터 노드에서 SnapLock 컴플라이언스 클록을 초기화합니다.
2. 오브젝트에 대해 *WORM(Write Once, Read Many)* 권한을 허용하는 시간 기반 잠금을 활성화하려면 * Governance * mode를 선택하십시오. _Governance_mode에서도 특정 권한을 가진 관리자 사용자가 객체를 삭제할 수 있습니다.
3. 객체에 대해 보다 엄격한 삭제 규칙을 지정하고 업데이트하려면 * 규정 준수 * 모드를 선택하십시오. 이 오브젝트 잠금 모드에서는 지정된 보존 기간이 완료된 후에만 오브젝트를 만료시킬 수 있습니다. 보존 기간을 지정하지 않으면 객체는 무기한으로 잠긴 상태로 유지됩니다.
4. 특정 기간 동안 잠금을 적용하려면 잠금 보존 기간을 일 또는 년 단위로 지정합니다.

잠금은 버전 및 비버전 S3 버킷에 적용할 수 있습니다. NAS 객체에는 객체 잠금을 적용할 수 없습니다.

버킷에 대한 보호 및 권한 설정 및 성능 서비스 수준을 구성할 수 있습니다.

사용 권한을 구성하기 전에 사용자 및 그룹을 이미 만들어야 합니다.

자세한 내용은 을 "새 버킷을 위한 거울을 작성합니다"참조하십시오.

버킷에 대한 접근을 확인합니다

S3 클라이언트 애플리케이션(ONTAP S3 또는 외부 타사 애플리케이션)에서 다음을 입력하여 새로 생성된 버킷에 대한 액세스를 확인할 수 있습니다.

- S3 서버 CA 인증서입니다.
- 사용자의 액세스 키와 비밀 키입니다.
- S3 서버 FQDN 이름 및 버킷 이름입니다.

ONTAP S3 버킷 크기를 늘리거나 줄입니다

필요한 경우 기존 버킷의 크기를 늘리거나 줄일 수 있습니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 버킷 크기를 관리할 수 있습니다.

시스템 관리자

1. 스토리지 > 버킷 * 을 선택하고 수정할 버킷을 찾습니다.
2. 버킷 이름 옆에 있는 을 ⋮ 클릭하고 * 편집 * 을 선택합니다.
3. Edit bucket * 창에서 버킷 용량을 변경합니다.
4. * 저장 *.

CLI를 참조하십시오

1. 버킷 용량 변경:

```
vserver object-store-server bucket modify -vserver <SVM_name>
-bucket <bucket_name> -size {<integer>[KB|MB|GB|TB|PB]}
```

MetroCluster 구성의 경우 미러링된 또는 미러링되지 않은 애그리게이트에 **ONTAP S3** 버킷을 생성합니다

ONTAP 9.14.1부터 MetroCluster FC 및 IP 구성의 미러링 또는 미러링되지 않은 애그리게이트에 버킷을 프로비저닝할 수 있습니다.

이 작업에 대해

- 기본적으로 버킷은 미러링된 애그리게이트에서 프로비저닝됩니다.
- 에 설명된 것과 동일한 프로비저닝 지침을 따릅니다 "버킷을 만듭니다" MetroCluster 환경에서 버킷 생성에 적용됩니다.

- 다음 S3 오브젝트 스토리지 기능은 MetroCluster 환경에서 * 지원되지 않음 *.
  - SnapMirror S3
  - S3 버킷 라이프사이클 관리
  - Compliance * 모드에서 S3 오브젝트 잠금

    거버넌스 * 모드에서 S3 오브젝트 잠금이 지원됩니다.
  - 로컬 FabricPool 계층화

시작하기 전에

S3 서버를 포함하는 SVM이 이미 존재해야 합니다.

버킷을 생성하는 프로세스

CLI를 참조하십시오

1. Aggregate 및 FlexGroup 구성 요소를 직접 선택하려면 권한 수준을 Advanced(고급)로 설정하십시오. 그렇지 않으면 admin 권한 수준이 Advanced(고급)로 설정됩니다
2. 버킷 생성:

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates
   true/false]
   ```

   를 설정합니다 `-use-mirrored-aggregates` 옵션을 로 설정합니다 `true` 또는 `false` 미러링된 애그리게이트를 사용할지, 아니면 미러링되지 않은 애그리게이트를 사용할지에 따라 다릅니다.

   > 기본적으로 은(는) 입니다 `-use-mirrored-aggregates` 옵션이 로 설정되어 있습니다 `true`.

   - SVM 이름은 데이터 SVM이어야 합니다.
   - 옵션을 지정하지 않을 경우 ONTAP는 800GB 버킷을 생성하고 서비스 레벨이 시스템에서 사용 가능한 최대 레벨로 설정합니다.
   - ONTAP에서 성능 또는 사용량을 기준으로 버킷을 생성하려면 다음 옵션 중 하나를 사용하십시오.
     - 서비스 레벨

       가치, 성능, 익스트림 등의 가치 중 하나로 스토리지 서비스 수준 옵션을 포함시키십시오.

     - 계층화

       사용된 용량 계층 TRUE 옵션을 포함합니다.

   - 기본 FlexGroup 볼륨을 생성할 애그리게이트를 지정하려면 다음 옵션을 사용하십시오.
     - '-aggr-list' 매개 변수는 FlexGroup 볼륨 구성요소에 사용할 애그리게이트 목록을 지정합니다.

       목록의 각 항목은 지정된 애그리게이트에 구성요소를 생성합니다. Aggregate를 여러 번 지정하여 Aggregate에 여러 구성요소를 생성할 수 있습니다.

   FlexGroup 볼륨 전체에서 일관된 성능을 위해서는 모든 애그리게이트에서 동일한 디스크 유형과 RAID 그룹 구성을 사용해야 합니다.

   - '-aggr-list-multiplier' 매개 변수는 FlexGroup 볼륨을 생성할 때 '-aggr-list' 매개 변수로 나열된 애그리게이트를 반복하는 횟수를 지정합니다.

     '-aggr-list-multiplier' 파라미터의 기본값은 4이다.

3. 필요한 경우 QoS 정책 그룹을 추가합니다.

   'vserver object-store-server bucket modify -bucket_bucket_name_-qos-policy -group_qos_policy_group_'

4. 버킷 생성 확인:

   'vserver object-store-server bucket show[-instance]'

예

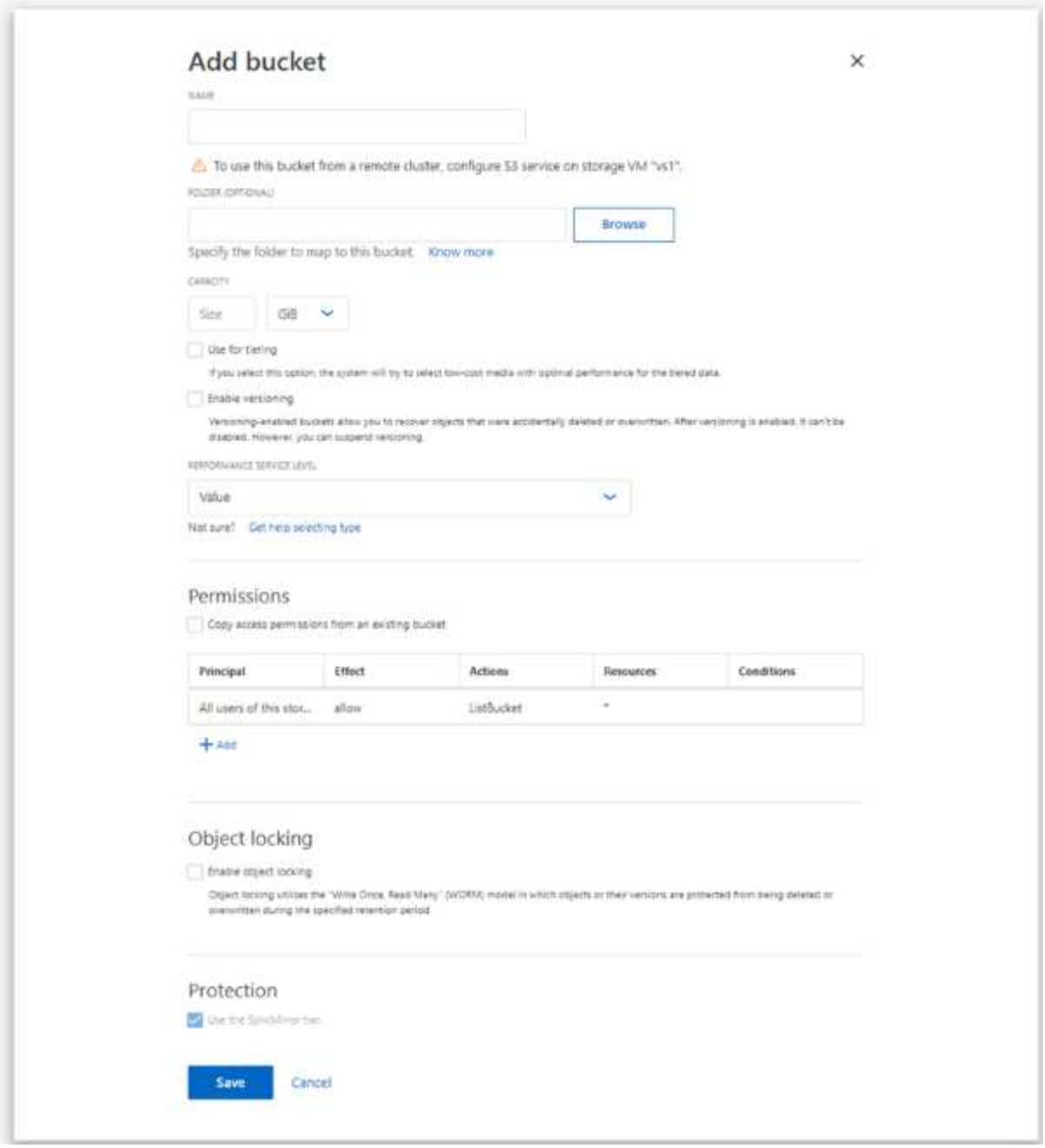
다음 예에서는 미러링된 애그리게이트에 1TB 크기의 SVM VS1에 대한 버킷을 생성합니다.

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

시스템 관리자

1. S3 지원 스토리지 VM에 새 버킷을 추가합니다.
   a. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력합니다.

      기본적으로 버킷은 미러링된 애그리게이트에서 프로비저닝됩니다. 미러링되지 않은 Aggregate에 버킷을 생성하려면 * More Options * 를 선택하고 다음 이미지와 같이 * Protection * 아래에서 * Use the SyncMirror tier * 확인란의 선택을 취소합니다.



- 이 지점에서 * Save * (저장 *)를 클릭하면 다음 기본 설정으로 버킷이 생성됩니다.
  - 그룹 정책이 이미 적용되어 있지 않으면 버킷에 대한 액세스 권한이 사용자에게 부여되지 않습니다.

> 오브젝트 저장소에 대한 무제한 액세스 권한이 있으므로 S3 루트 사용자를 사용하여 ONTAP 오브젝트 스토리지를 관리하고 권한을 공유해서는 안 됩니다. 대신 할당한 관리 권한이 있는 사용자 또는 그룹을 만듭니다.

  - 시스템에서 가장 높은 수준의 서비스 품질(성능) 수준입니다.
- bucket을 구성할 때 * 추가 옵션 * 을 클릭하여 사용자 권한 및 성능 수준을 구성하거나 나중에 이러한 설정을 수정할 수 있습니다.
  - 권한을 구성하려면 * 추가 옵션 * 을 사용하기 전에 사용자 및 그룹을 이미 만들어야 합니다.

- FabricPool 계층화에 S3 오브젝트 저장소를 사용하려는 경우 성능 서비스 수준이 아닌 * 계층화에 사용 * (계층 데이터에 최적의 성능을 제공하는 저비용 미디어 사용)을 선택하는 것이 좋습니다.

2. S3 클라이언트 앱(다른 ONTAP 시스템 또는 외부 타사 앱)에서 다음을 입력하여 새 버킷에 대한 액세스를 확인합니다.
   - S3 서버 CA 인증서입니다.
   - 사용자의 액세스 키와 비밀 키입니다.
   - S3 서버 FQDN 이름 및 버킷 이름입니다.

ONTAP S3 버킷 라이프사이클 관리 규칙을 생성합니다

ONTAP 9.13.1부터 S3 버킷에서 오브젝트 라이프사이클을 관리하는 라이프사이클 관리 규칙을 생성할 수 있습니다. 버킷의 특정 오브젝트에 대한 삭제 규칙을 정의하고 이 규칙을 통해 버킷 오브젝트를 만료시킬 수 있습니다. 따라서 보존 요구사항을 충족하고 전체 S3 오브젝트 스토리지를 효율적으로 관리할 수 있습니다.

버킷 오브젝트에 대해 오브젝트 잠금이 설정되어 있으면 잠긴 오브젝트에 오브젝트 만료에 대한 라이프사이클 관리 규칙이 적용되지 않습니다. 개체 잠금에 대한 자세한 내용은 을 참조하십시오 "버킷을 만듭니다".

시작하기 전에

- S3 서버와 버킷을 포함하는 S3 기반 SVM이 이미 존재해야 합니다. 을 참조하십시오 "S3를 위해 SVM을 생성합니다" 를 참조하십시오.
- 멀티프로토콜 NAS 볼륨에서 S3를 사용하거나 MetroCluster 구성에서 S3를 사용하는 경우에는 버킷 라이프사이클 관리 규칙이 지원되지 않습니다.

이 작업에 대해

수명 주기 관리 규칙을 생성할 때 버킷 객체에 다음 삭제 작업을 적용할 수 있습니다.

- 현재 버전 삭제 - 이 작업은 규칙에 의해 식별된 개체를 만료시킵니다. 버킷에 버전 관리가 활성화되어 있는 경우 S3는 만료된 개체를 모두 사용할 수 없게 합니다. 버전 관리를 사용하지 않으면 이 규칙은 개체를 영구적으로 삭제합니다. CLI 작업은 입니다 `Expiration`.
- 현재 버전이 아닌 버전 삭제 - 이 작업은 S3에서 현재 개체가 아닌 개체를 영구적으로 제거할 수 있는 시기를 지정합니다. CLI 작업은 입니다 `NoncurrentVersionExpiration`.

현재 버전이 아닌 버전은 현재 버전의 생성 또는 수정 시간을 기반으로 합니다. 현재 개체가 아닌 개체의 지연된 제거는 실수로 개체를 삭제하거나 덮어쓸 때 유용할 수 있습니다. 예를 들어, 최신 버전이 아닌 버전이 5일 후에 삭제되도록 만료 규칙을 구성할 수 있습니다. 예를 들어 2014년 1월 1일 오전 10시 30분 UTC에 (버전 ID `111111`)라는 개체를 만든다고 가정해 `photo.gif` 보겠습니다. 2014년 1월 2일 오전 11시 30분에 실수로 (버전 ID)를 삭제했는데 `photo.gif`, 이 경우 새 버전 ID(예: 버전 ID `111111`)가 포함된 삭제 마커가 `4857693` 만들어집니다. 삭제가 영구화되기 전에 원래 버전(버전 ID `111111`)을 복구할 수 있는 기간이 5 `photo.gif`일입니다. `2014년 1월 8일 00:00 UTC`에 만료에 대한 수명 주기 규칙은 최신 버전이 아닌 `5`일 후에 실행되고 영구적으로 삭제됩니다 `photo.gif`(버전 ID `111111`).

- 만료된 삭제 표식 삭제 - 이 작업은 만료된 개체 삭제 표식을 삭제합니다.

버전 관리를 사용하는 버킷에서 삭제 표식이 있는 오브젝트는 개체의 현재 버전이 됩니다. 객체는 삭제되지 않으며, 객체에 대해 작업을 수행할 수 없습니다. 이러한 개체는 연결된 현재 버전이 없으면 만료됩니다. CLI 작업은 입니다 `Expiration`.

- 불완전한 다중 파트 업로드 삭제 - 이 작업은 다중 파트 업로드가 계속 진행되도록 허용할 최대 시간(일)을 설정합니다. 다음 중 삭제됩니다. CLI 작업은 입니다 `AbortIncompleteMultipartUpload`.

수행하는 절차는 사용하는 인터페이스에 따라 다릅니다. ONTAP 9.13,1에서는 CLI를 사용해야 합니다. ONTAP 9.14.1부터 System Manager를 사용할 수도 있습니다.

CLI를 사용하여 수명 주기 관리 규칙을 관리합니다

ONTAP 9.13.1부터는 ONTAP CLI를 사용하여 라이프사이클 관리 규칙을 생성하여 S3 버킷에서 오브젝트를 만료할 수 있습니다.

시작하기 전에

CLI의 경우 버킷 수명 주기 관리 규칙을 생성할 때 각 만료 작업 유형에 대한 필수 필드를 정의해야 합니다. 이러한 필드는 초기 생성 후 수정할 수 있습니다. 다음 표에는 각 작업 유형에 대한 고유 필드가 표시됩니다.

작업 유형	고유 필드
NonCurrentVersionExpiration 을 참조하십시오	• `-non-curr-days` - 현재 버전이 아닌 버전이 삭제될 때까지 남은 일 수입니다 • `-new-non-curr-versions` - 유지할 최신 버전이 아닌 버전 수입니다
만료	• `-obj-age-days` - 생성 후 현재 버전의 오브젝트를 삭제할 수 있는 일 수입니다 • `-obj-exp-date` 객체가 만료되는 특정 날짜입니다 • `-expired-obj-del-markers` - 객체를 정리해 마커를 삭제합니다
AbortIncompleteMultipartUpload를 중단합니다	• `-after-initiation-days` - 시작 일수입니다. 이후 업로드가 중단될 수 있습니다

버킷 수명주기 관리 규칙을 특정 객체 하위 집합에만 적용하려면 관리자는 규칙을 생성할 때 각 필터를 설정해야 합니다. 규칙을 생성할 때 이러한 필터를 설정하지 않으면 버킷 내의 모든 오브젝트에 규칙이 적용됩니다.

다음을 제외한 _ 을(를) 처음 생성한 후 모든 필터를 수정할 수 있습니다. +

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

단계

1. 를 사용합니다 `vserver object-store-server bucket lifecycle-management-rule create` 버킷 수명 주기 관리 규칙을 생성하기 위해 만료 작업 유형에 필요한 필드가 있는 명령입니다.

예

다음 명령을 실행하면 NonCurrentVersionExpiration 버킷 수명주기 관리 규칙이 생성됩니다.

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

예

다음 명령을 실행하면 만료 버킷 수명주기 관리 규칙이 생성됩니다.

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

예

다음 명령을 실행하면 AbortIncompleteMultipartUpload 버킷 수명주기 관리 규칙이 생성됩니다.

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

System Manager를 사용하여 라이프사이클 관리 규칙을 관리합니다

ONTAP 9.14.1부터 System Manager를 사용하여 S3 오브젝트를 만료할 수 있습니다. S3 오브젝트에 대한 라이프사이클 관리 규칙을 추가, 편집, 삭제할 수 있습니다. 또한 한 버킷에 대해 생성된 수명주기 규칙을 가져와 다른 버킷의 오브젝트에 사용할 수 있습니다. 활성 규칙을 사용하지 않도록 설정하고 나중에 활성화할 수 있습니다.

문서 수정 상태 관리 규칙을 추가합니다

1. 스토리지 > Bucket * 을 클릭합니다.
2. 만료 규칙을 지정할 버킷을 선택합니다.
3. ⋮아이콘을 클릭하고 * 문서 수정 상태 규칙 관리 * 를 선택합니다.
4. 추가 > 라이프사이클 규칙 * 을 클릭합니다.

5. 문서 수정 상태 규칙 추가 페이지에서 규칙 이름을 추가합니다.
6. 규칙의 범위를 정의하여 버킷의 모든 오브젝트에 적용할지 또는 특정 오브젝트에 적용할지 여부를 지정합니다. 오브젝트를 지정하려면 다음 필터 조건 중 하나 이상을 추가합니다.
   a. 접두사: 규칙을 적용할 개체 키 이름의 접두사를 지정합니다. 일반적으로 개체의 경로 또는 폴더입니다. 규칙마다 접두사를 하나씩 입력할 수 있습니다. 유효한 접두사가 제공되지 않는 한 규칙은 버킷의 모든 오브젝트에 적용됩니다.
   b. 태그: 규칙을 적용할 개체에 대해 최대 3개의 키 및 값 쌍(태그)을 지정합니다. 필터링에는 유효한 키만 사용됩니다. 값은 선택 사항입니다. 그러나 값을 추가하는 경우에는 해당 키에 대해 유효한 값만 추가해야 합니다.
   c. 크기: 오브젝트의 최소 크기와 최대 크기 사이에서 범위를 제한할 수 있습니다. 두 값 중 하나 또는 모두를 입력할 수 있습니다. 기본 단위는 MiB입니다.
7. 작업을 지정합니다.
   a. * 객체의 현재 버전 만료 *: 생성 후 특정 일 수 또는 특정 날짜에 모든 현재 객체를 영구적으로 사용할 수 없도록 규칙을 설정합니다. 만료된 개체 삭제 표식 삭제 * 옵션을 선택한 경우에는 이 옵션을 사용할 수 없습니다.
   b. * 현재 버전이 아닌 버전을 영구적으로 삭제 *: 현재 버전이 아닌 버전을 삭제할 일 수와 보관할 버전 수를 지정합니다.
   c. 만료된 개체 삭제 표식 삭제: 만료된 삭제 표식이 있는 개체를 삭제하려면 이 작업을 선택합니다. 만료된 삭제 표식은 연결된 현재 개체가 없는 삭제 표식입니다.

      이 옵션은 보존 기간 이후 모든 오브젝트를 자동으로 삭제하는 * 현재 버전의 오브젝트 만료 * 옵션을 선택하면 사용할 수 없습니다. 이 옵션은 개체 태그가 필터링에 사용되는 경우에도 사용할 수 없습니다.

   d. * 불완전한 다중 파트 업로드 삭제 *: 불완전한 다중 파트 업로드가 삭제되는 일 수를 설정합니다. 진행 중인 다중 파트 업로드가 지정된 보존 기간 내에 실패할 경우 불완전한 다중 파트 업로드를 삭제할 수 있습니다. 이 옵션은 개체 태그가 필터링에 사용되는 경우 사용할 수 없습니다.
   e. 저장 * 을 클릭합니다.

문서 수정 상태 규칙 불러오기

1. 스토리지 > Bucket * 을 클릭합니다.
2. 만료 규칙을 가져올 버킷을 선택합니다.
3. ⋮ 아이콘을 클릭하고 * 문서 수정 상태 규칙 관리 * 를 선택합니다.
4. 추가 > 규칙 가져오기 * 를 클릭합니다.
5. 규칙을 가져올 버킷을 선택합니다. 선택한 버킷에 대해 정의된 수명 주기 관리 규칙이 나타납니다.
6. 가져올 규칙을 선택합니다. 한 번에 하나의 규칙을 선택할 수 있으며 기본 선택 항목이 첫 번째 규칙입니다.
7. 가져오기 * 를 클릭합니다.

규칙을 편집, 삭제 또는 비활성화합니다

규칙과 연결된 문서 수정 상태 관리 작업만 편집할 수 있습니다. 규칙이 객체 태그로 필터링된 경우 * 만료된 객체 삭제 마커 삭제 * 및 * 불완전한 다중 파트 업로드 삭제 * 옵션을 사용할 수 없습니다.

규칙을 삭제하면 해당 규칙이 이전에 연결된 개체에 더 이상 적용되지 않습니다.

1. 스토리지 > Bucket * 을 클릭합니다.
2. 수명주기 관리 규칙을 편집, 삭제 또는 비활성화할 버킷을 선택합니다.
3. ⋮ 아이콘을 클릭하고 * 문서 수정 상태 규칙 관리 * 를 선택합니다.
4. 필요한 규칙을 선택합니다. 한 번에 하나의 규칙을 편집하고 사용하지 않도록 설정할 수 있습니다. 한 번에 여러 규칙을 삭제할 수 있습니다.
5. 편집 *, * 삭제 * 또는 * 비활성화 * 를 선택하고 절차를 완료합니다.

ONTAP S3 사용자를 생성합니다

특정 권한을 가진 S3 사용자를 생성합니다. 모든 ONTAP 개체 저장소에서 인증된 클라이언트로의 연결을 제한하려면 사용자 인증이 필요합니다.

시작하기 전에.

S3 지원 스토리지 VM이 이미 존재해야 합니다.

이 작업에 대해

S3 사용자에게 스토리지 VM의 모든 버킷에 대한 액세스 권한을 부여할 수 있습니다. S3 사용자를 생성할 때 사용자에 대한 액세스 키와 비밀 키도 생성됩니다. 객체 저장소 및 버킷 이름의 FQDN과 함께 사용자와 공유해야 합니다.

보안 강화를 위해 ONTAP 9.15.1부터 S3 사용자가 생성된 시점에만 액세스 키와 비밀 키가 표시되며 다시 표시할 수 없습니다. 키를 분실한 경우"새 키를 다시 생성해야 합니다".

버킷 정책 또는 오브젝트 서버 정책에서 S3 사용자에게 특정 액세스 권한을 부여할 수 있습니다.

> ⓘ 새 오브젝트 저장소 서버를 만들면 ONTAP에서 루트 사용자(UID 0)를 생성합니다. 이 사용자는 모든 버킷에 액세스할 수 있는 권한이 있는 사용자입니다. NetApp에서는 ONTAP S3를 루트 사용자로 관리하는 대신 특정 권한으로 관리자 역할을 생성하는 것이 좋습니다.

CLI를 참조하십시오

1. S3 사용자 생성:
   `vserver object-store-server user create -vserver svm_name -user user_name -comment [-comment text] -key-time-to-live time`

   - 코멘트 추가는 선택 사항입니다.
   - ONTAP 9.14.1부터 에서 키가 유효한 기간을 정의할 수 있습니다 `-key-time-to-live` 매개 변수. 이 형식으로 보존 기간을 추가하여 액세스 키가 만료되는 기간을 표시할 수 있습니다.
     `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
     예를 들어 1일, 2시간, 3분, 4초의 보존 기간을 입력하려면 값을 로 입력합니다 `P1DT2H3M4S`. 지정하지 않으면 이 키는 무기한 동안 유효합니다.

     아래 예는 이름을 가진 사용자를 생성합니다 `sm_user1` 있습니다 `vs0`키 보존 기간이 1주일로 설정되어 있습니다.

```
vserver object-store-server user create -vserver vs0 -user sm_user1
-key-time-to-live P1W
```

2. 액세스 키와 비밀 키를 저장해야 합니다. S3 클라이언트에서 액세스하는 데 필요합니다.

시스템 관리자

1. 스토리지 > 스토리지 VM * 을 클릭합니다. 사용자를 추가해야 하는 스토리지 VM을 선택하고 * Settings * 를 선택한 다음 S3 아래에서 를 클릭합니다 .
2. 사용자를 추가하려면 * 사용자 > 추가 * 를 클릭합니다.
3. 사용자의 이름을 입력합니다.
4. ONTAP 9.14.1부터 사용자에 대해 생성된 액세스 키의 보존 기간을 지정할 수 있습니다. 키가 자동으로 만료되는 일, 시간, 분 또는 초 단위로 보존 기간을 지정할 수 있습니다. 기본적으로 이 값은 로 설정됩니다 `0` 이는 키가 무기한 유효함을 나타냅니다.
5. 저장 * 을 클릭합니다. 사용자가 만들어지고 해당 사용자에 대한 액세스 키와 비밀 키가 생성됩니다.
6. 액세스 키와 비밀 키를 다운로드하거나 저장합니다. S3 클라이언트에서 액세스하는 데 필요합니다.

다음 단계

- S3 그룹을 생성하거나 수정합니다

ONTAP S3 사용자 그룹을 생성하거나 수정하여 버킷에 대한 액세스를 제어합니다

적절한 액세스 권한을 가진 사용자 그룹을 생성하여 버킷 액세스를 간소화할 수 있습니다.

시작하기 전에

S3 지원 SVM의 S3 사용자가 이미 존재해야 합니다.

이 작업에 대해

S3 그룹의 사용자는 SVM의 모든 버킷에 대한 액세스 권한을 부여할 수 있지만 여러 SVM에는 액세스할 수 없습니다. 그룹 액세스 권한은 다음 두 가지 방법으로 구성할 수 있습니다.

- 버킷 레벨에서

  S3 사용자 그룹을 생성한 후 버킷 정책 문에 그룹 권한을 지정하며 해당 버킷에만 적용됩니다.

- SVM 레벨에서

  S3 사용자 그룹을 생성한 후 그룹 정의에 오브젝트 서버 정책 이름을 지정합니다. 이러한 정책은 그룹 구성원에 대한 버킷 및 액세스를 결정합니다.

시스템 관리자

1. 스토리지 VM 편집: * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 클릭한 다음 * 설정 * 을 클릭하고 S3 아래를 클릭합니다 .
2. 그룹 추가: * 그룹 * 을 선택한 다음 * 추가 * 를 선택합니다.
3. 그룹 이름을 입력하고 사용자 목록에서 선택합니다.
4. 기존 그룹 정책을 선택하거나 지금 추가하거나 나중에 정책을 추가할 수 있습니다.

CLI를 참조하십시오

1. S3 그룹 생성: 'vserver object-store-server group create-vserver_svm_name_-name_group_name_-users_user_name\(s\)*[-policies_policy_names*][-comment_text_\]' 객체 저장소에 하나의 버킷만 있는 구성에서는 '-policies' 옵션을 생략할 수 있으며 그룹 이름은 버킷 정책에 추가할 수 있습니다. '-policies' 옵션은 나중에 객체 스토리지 서버 정책을 생성한 후 'vserver object-store-server group modify' 명령을 사용하여 추가할 수 있습니다.

ONTAP S3 키를 재생성하고 보존 기간을 수정합니다

S3 클라이언트 액세스를 사용하도록 사용자를 생성하는 동안 액세스 키와 비밀 키가 자동으로 생성됩니다. 키가 만료되거나 손상된 경우 사용자의 키를 다시 생성할 수 있습니다.

선택키 생성에 대한 자세한 내용은 을 참조하십시오 "S3 사용자를 생성합니다".

시스템 관리자

1. 스토리지 > 스토리지 VM * 을 클릭한 다음 스토리지 VM을 선택합니다.
2. 설정 * 탭에서 * S3 * 타일을 클릭합니다 .
3. 사용자 * 탭에서 액세스 키가 없거나 사용자의 키가 만료되었는지 확인합니다.
4. 키를 다시 생성해야 하는 경우 사용자 옆에 있는 을 클릭한 다음 * 키 재생성 * 을 클릭합니다.
5. 기본적으로 생성된 키는 무기한으로 유효합니다. 9.14.1부터 키가 자동으로 만료되는 보존 기간을 수정할 수 있습니다. 보존 기간을 일, 시간, 분 또는 초로 입력합니다.
6. 저장 * 을 클릭합니다. 키가 재생성됩니다. 키 보존 기간의 변경 사항은 즉시 적용됩니다.
7. 액세스 키와 비밀 키를 다운로드하거나 저장합니다. S3 클라이언트에서 액세스하는 데 필요합니다.

CLI를 참조하십시오

1. 를 실행하여 사용자의 액세스 및 비밀 키를 다시 생성합니다 `vserver object-store-server user regenerate-keys` 명령.
2. 기본적으로 생성된 키는 무기한으로 유효합니다. 9.14.1부터 키가 자동으로 만료되는 보존 기간을 수정할 수 있습니다. 다음 형식으로 보존 기간을 추가할 수 있습니다.
   `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
   예를 들어 1일, 2시간, 3분, 4초의 보존 기간을 입력하려면 값을 로 입력합니다 `P1DT2H3M4S`.

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name
   -user user -key-time-to-live 0
   ```

3. 액세스 키와 비밀 키를 저장합니다. S3 클라이언트에서 액세스하는 데 필요합니다.

액세스 정책 문을 만들거나 수정합니다

ONTAP S3 버킷 및 오브젝트 저장소 서버 정책에 대해 알아보십시오

S3 리소스에 대한 사용자 및 그룹 액세스는 버킷 및 오브젝트 저장소 서버 정책에 의해 제어됩니다. 사용자 또는 그룹이 적은 경우 버킷 수준에서 액세스를 제어하는 것이 충분하지만 사용자 및 그룹이 많은 경우에는 오브젝트 저장소 서버 수준에서 액세스를 제어하는 것이 더 쉽습니다.

기본 **ONTAP S3** 버킷 정책에 액세스 규칙을 추가합니다

기본 버킷 정책에 액세스 규칙을 추가할 수 있습니다. 접근 제어의 범위는 포함된 버킷이므로 하나의 버킷이 있을 때 가장 적합합니다.

시작하기 전에

S3 서버와 버킷이 포함된 S3 지원 스토리지 VM이 이미 존재해야 합니다.

권한을 부여하기 전에 사용자 또는 그룹을 이미 만들어야 합니다.

이 작업에 대해

새 사용자와 그룹에 대한 새 문을 추가하거나 기존 문의 특성을 수정할 수 있습니다. 에 대한 자세한 내용은 `vserver object-store-server bucket policy` "ONTAP 명령 참조입니다"을 참조하십시오.

사용자 및 그룹 권한은 버킷이 생성될 때 또는 나중에 필요할 때 부여할 수 있습니다. 버킷 용량과 QoS 정책 그룹 할당을 수정할 수도 있습니다.

ONTAP 9.9.1부터 ONTAP S3 서버에서 AWS 클라이언트 개체 태그 지정 기능을 지원하려는 경우 해당 작업이 수행됩니다 `GetObjectTagging`, `PutObjectTagging`, 및 `DeleteObjectTagging` 버킷 또는 그룹 정책을 사용하여 허용되어야 합니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

단계

1. 버킷 편집: * 저장소 > 버킷 * 을 클릭하고 원하는 버킷을 클릭한 다음 * 편집 * 을 클릭합니다. 사용 권한을 추가하거나 수정할 때 다음 매개 변수를 지정할 수 있습니다.
   - * Principal *: 액세스 권한이 부여된 사용자 또는 그룹입니다.
   - * 효과 *: 사용자 또는 그룹에 대한 액세스를 허용하거나 거부합니다.
   - * 조치 *: 주어진 사용자 또는 그룹에 대해 버킷에서 허용되는 작업.
   - * 리소스 *: 액세스가 부여되거나 거부되는 버킷 내의 객체 경로 및 이름입니다.

     기본값은 ***bucketname** * 및 ***bucketname/** * * 이며 버킷의 모든 개체에 대한 액세스를 허용합니다**.** 단일 개체에 대한 액세스 권한을 부여할 수도 있습니다**(**예**: ***bucketname/*_readme.txt**).

   - * 조건 * (선택 사항): 액세스를 시도할 때 계산되는 식입니다. 예를 들어, 액세스가 허용되거나 거부될 IP 주소 목록을 지정할 수 있습니다.

> ONTAP 9.14.1부터 * 리소스 * 필드에서 버킷 정책의 변수를 지정할 수 있습니다. 이러한 변수는 정책을 평가할 때 상황별 값으로 대체되는 자리 표시자입니다. 예를 들어, IF를 입력합니다 `${aws:username}` 이 정책에 대한 변수로 지정되면 이 변수가 요청 컨텍스트 사용자 이름으로 대체되고 해당 사용자에 대해 구성된 대로 정책 작업을 수행할 수 있습니다.

CLI를 참조하십시오

단계

1. 버킷 정책에 구문 추가:

   'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_store_resources_[-sid text][-index integer]'

   다음 매개 변수는 액세스 권한을 정의합니다.

효과	이 문은 액세스를 허용하거나 거부할 수 있습니다
액션	모든 작업을 의미하는 ' * '를 지정하거나, GetObject, PutObject, DeleteObject, ListBucket, GetBuckketAcl, GetObjectAcl 중 하나 이상의 목록을 지정할 수 있습니다. ListBuckketMultpartUploads, ListMultipartUploadParts를 참조하십시오.

``원자''	하나 이상의 S3 사용자 또는 그룹 목록 • 최대 10명의 사용자 또는 그룹을 지정할 수 있습니다. • S3 Group을 지정한 경우 Group/group_name 형태의 그룹이어야 한다 • '*'는 공개 액세스를 의미하도록 지정할 수 있습니다. 즉, 액세스 키와 비밀 키 없이 액세스할 수 있습니다. • 보안 주체를 지정하지 않으면 스토리지 VM의 모든 S3 사용자에게 액세스 권한이 부여됩니다.
'-resource'	버킷과 버킷에 포함된 모든 물체 와일드카드 문자입니다 `*` 및 `?` 리소스를 지정하기 위한 정규식을 만드는 데 사용할 수 있습니다. 리소스의 경우 정책에 변수를 지정할 수 있습니다. 정책 변수는 정책을 평가할 때 컨텍스트 값으로 대체되는 자리 표시자입니다.

선택적으로 '-sid' 옵션을 사용하여 텍스트 문자열을 주석으로 지정할 수 있습니다.

예

다음 예에서는 객체 저장소 서버 사용자 user1의 readme 폴더에 대한 액세스를 허용하는 스토리지 VM svm1.example.com 및 bucket1에 대한 객체 저장소 서버 버킷 정책 문을 생성합니다.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

다음 예에서는 객체 저장소 서버 그룹 group1의 모든 객체에 대한 액세스를 허용하는 스토리지 VM svm1.example.com 및 bucket1에 대한 객체 저장소 서버 버킷 정책 문을 생성합니다.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

ONTAP 9.14.1부터 버킷 정책에 대한 변수를 지정할 수 있습니다. 다음 예에서는 스토리지 VM에 대한 서버 버킷 정책 설명을 생성합니다 `svm1` 및 `bucket1`, 및 은 지정합니다 `${aws:username}` 정책 리소스에 대한 변수로 사용됩니다. 정책이 평가되면 정책 변수가 요청 컨텍스트 사용자 이름으로 대체되고 해당 사용자에 대해 구성된 대로 정책 작업을 수행할 수 있습니다. 예를 들어, 다음 정책 문을 평가할 때 `${aws:username}` S3 작업을 수행하는 사용자로 대체됩니다. 사용자인 경우 `user1` 사용자에게 액세스 권한이 부여된 작업을 수행합니다 `bucket1` 현재 `bucket1/user1/*`.

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

ONTAP S3 오브젝트 저장소 서버 정책을 생성하거나 수정합니다

오브젝트 저장소의 하나 이상의 버킷에 적용할 수 있는 정책을 생성할 수 있습니다. 오브젝트 저장소 서버 정책을 사용자 그룹에 연결할 수 있으므로 여러 버킷에서 리소스 액세스 관리를 간소화할 수 있습니다.

시작하기 전에

S3 서버와 버킷을 포함하는 S3 기반 SVM이 이미 존재해야 합니다.

이 작업에 대해

오브젝트 스토리지 서버 그룹에서 기본 정책 또는 사용자 지정 정책을 지정하여 SVM 레벨에서 액세스 정책을 활성화할 수 있습니다. 정책은 그룹 정의에 지정될 때까지 적용되지 않습니다.

> 개체 스토리지 서버 정책을 사용할 때는 정책 자체가 아니라 그룹 정의에서 보안 주체(사용자 및 그룹)를 지정합니다.

ONTAP S3 리소스에 액세스하기 위한 세 가지 읽기 전용 기본 정책이 있습니다.

- 전체 액세스
- NoS3액세스
- ReadOnlyAccess 를 참조하십시오

또한 새 사용자 지정 정책을 만든 다음 새 사용자 및 그룹에 대한 새 문을 추가하거나 기존 문의 특성을 수정할 수도 있습니다. 에 대한 자세한 내용은 `vserver object-store-server policy` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 9.9.1부터 ONTAP S3 서버에서 AWS 클라이언트 개체 태그 지정 기능을 지원하려는 경우 해당 작업이 수행됩니다 `GetObjectTagging`, `PutObjectTagging`, 및 `DeleteObjectTagging` 버킷 또는 그룹 정책을 사용하여 허용되어야 합니다.

다음 절차는 사용하는 인터페이스에 따라 다릅니다. — System Manager 또는 CLI:

시스템 관리자

- System Manager를 사용하여 오브젝트 저장소 서버 정책을 생성하거나 수정합니다 *

단계

1. 스토리지 VM 편집: * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 클릭한 다음 * 설정 * 을 클릭하고 S3 아래를 클릭합니다 .
2. 사용자 추가: * Policies * 를 클릭한 다음 * Add * 를 클릭합니다.
   a. 정책 이름을 입력하고 그룹 목록에서 선택합니다.
   b. 기존 기본 정책을 선택하거나 새 정책을 추가합니다.

      그룹 정책을 추가하거나 수정할 때 다음 매개 변수를 지정할 수 있습니다.

      - Group(그룹): 액세스 권한이 부여된 그룹입니다.
      - 효과: 하나 이상의 그룹에 대한 액세스를 허용하거나 거부합니다.
      - 조치: 주어진 그룹에 대해 하나 이상의 버킷에서 허용되는 조치.
      - 리소스: 액세스가 부여되거나 거부되는 하나 이상의 버킷 내에 있는 오브젝트의 경로 및 이름입니다. 예를 들면 다음과 같습니다.
        - * 스토리지 VM의 모든 버킷에 대한 액세스 권한을 부여합니다.
        - * bucketname * 및 * bucketname/** 특정 버킷의 모든 물체에 대한 액세스 권한을 부여합니다.
        - * bucketname/readme.txt * 특정 버킷의 개체에 대한 액세스 권한을 부여합니다.
   c. 필요한 경우 기존 정책에 구문을 추가합니다.

CLI를 참조하십시오

- CLI를 사용하여 오브젝트 저장소 서버 정책을 생성하거나 수정합니다 *

단계

1. 오브젝트 스토리지 서버 정책 생성:

   'vserver object-store-server policy create-vserver_svm_name_-policy_policy_name_[-comment_text_]'

2. 정책에 대한 문을 생성합니다.

   'vserver object-store-server policy statement create-vserver_svm_name_-policy_policy_name_-effect{allow|deny}-action_object_store_actions_-resource_object_store_resources_[sid text]'입니다

   다음 매개 변수는 액세스 권한을 정의합니다.

효과	이 문은 액세스를 허용하거나 거부할 수 있습니다

액션	모든 작업을 의미하는 ' * '를 지정하거나, GetObject, PutObject, DeleteObject, ListBucket, GetBuckketAcl, GetObjectAcl 중 하나 이상의 목록을 지정할 수 있습니다. ListAllMyBucket, ListBuckketMultpartUploads, ListMultipartUploadParts를 포함합니다.
'-resource'	버킷과 버킷에 포함된 모든 물체 와일드카드 문자 ' * '와 '?'입니다 리소스를 지정하기 위한 정규식을 구성하는 데 사용할 수 있습니다.

선택적으로 '-sid' 옵션을 사용하여 텍스트 문자열을 주석으로 지정할 수 있습니다.

기본적으로 새 문은 순서대로 처리되는 문 목록의 끝에 추가됩니다. 나중에 문을 추가하거나 수정할 때 문장의 '-index' 설정을 수정하여 처리 순서를 변경할 수 있습니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP S3 액세스를 위한 외부 디렉토리 서비스를 구성합니다

ONTAP 9.14.1부터 외부 디렉토리용 서비스가 ONTAP S3 오브젝트 스토리지와 통합되었습니다. 이러한 통합은 외부 디렉터리 서비스를 통한 사용자 및 액세스 관리를 단순화합니다.

ONTAP 오브젝트 스토리지 환경에 대한 액세스 권한을 통해 외부 디렉토리 서비스에 속하는 사용자 그룹을 제공할 수 있습니다. LDAP(Lightweight Directory Access Protocol)는 ID 및 액세스 관리(IAM)를 위한 데이터베이스와 서비스를 제공하는 Active Directory와 같은 디렉터리 서비스와 통신하는 인터페이스입니다. 액세스를 제공하려면 ONTAP S3 환경에서 LDAP 그룹을 구성해야 합니다. 액세스를 구성하면 그룹 구성원에게 ONTAP S3 버킷에 대한 권한이 부여됩니다. LDAP에 대한 자세한 내용은 를 "ONTAP NFS SVM에서 LDAP 이름 서비스 사용에 대해 알아보세요 "참조하십시오.

또한 빠른 바인딩 모드에 맞게 Active Directory 사용자 그룹을 구성하여 사용자 자격 증명을 검증하고 LDAP 연결을 통해 타사 및 오픈 소스 S3 응용 프로그램을 인증할 수 있습니다.

시작하기 전에

LDAP 그룹을 구성하고 그룹 액세스를 위해 빠른 바인딩 모드를 활성화하기 전에 다음 사항을 확인하십시오.

1. S3 서버가 포함된 S3 사용 스토리지 VM이 생성되었습니다. 을 참조하십시오 "S3를 위해 SVM을 생성합니다".
2. 해당 스토리지 VM에 버킷이 생성되었습니다. 을 참조하십시오 "버킷을 만듭니다".
3. 스토리지 VM에 DNS가 구성되어 있다. 을 "DNS 서비스를 구성합니다"참조하십시오.
4. LDAP 서버의 자체 서명된 루트 CA(인증 기관) 인증서가 스토리지 VM에 설치되어 있습니다. 을 "SVM에 자체 서명된 루트 CA 인증서 설치"참조하십시오.
5. LDAP 클라이언트는 SVM에서 TLS를 사용하도록 구성했습니다. "ONTAP NFS 액세스를 위한 LDAP 클라이언트 구성 생성"및 을 "정보를 위해 ONTAP NFS SVM과 LDAP 클라이언트 구성을 연결합니다."참조하십시오.

LDAP에 대한 **S3** 액세스를 구성합니다

1. 그룹에 대한 SVM의 _NAME 서비스 데이터베이스_로 LDAP를 지정하고 LDAP에 대한 암호를 지정합니다.

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

ONTAP 명령 참조에서 https://docs .NetApp.com/us-en/ONTAP-cli/vserver-services-name-service-ns-switch-modify.html 명령 링크에 대해 자세히[`vserver services name-service ns-switch modify` 알아보십시오.

2. 를 사용하여 오브젝트 저장소 버킷 정책 문을 생성합니다 `principal` 액세스 권한을 부여할 LDAP 그룹으로 설정합니다.

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

예: 다음 예제에서는 에 대한 버킷 정책 문을 만듭니다 `buck1`. 이 정책은 LDAP 그룹에 대한 액세스를 허용합니다 `group1` 리소스(버킷 및 해당 객체)에 `buck1`.

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. LDAP 그룹의 사용자를 확인합니다 `group1` 는 S3 클라이언트에서 S3 작업을 수행할 수 있습니다.

인증에 **LDAP** 빠른 바인드 모드를 사용합니다

1. 그룹에 대한 SVM의 _NAME 서비스 데이터베이스_로 LDAP를 지정하고 LDAP에 대한 암호를 지정합니다.

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

ONTAP 명령 참조에서 https://docs .NetApp.com/us-en/ONTAP-cli/vserver-services-name-service-ns-switch-modify.html 명령 링크에 대해 자세히[`vserver services name-service ns-switch modify`

알아보십시오.

2. S3 버킷에 액세스하는 LDAP 사용자에게 버킷 정책에 정의된 권한이 있는지 확인합니다. 자세한 내용은 을 참조하십시오 "버킷 정책을 수정합니다".
3. LDAP 그룹의 사용자가 다음 작업을 수행할 수 있는지 확인합니다.
   a. S3 클라이언트의 액세스 키를 다음 형식으로 구성합니다 `"NTAPFASTBIND" + base64-encode(user-name:password)`. 예 `"NTAPFASTBIND"`: +base64-encode(ldapuser:password)
   `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

      S3 클라이언트에서 비밀 키를 입력하라는 메시지가 표시될 수 있습니다. 비밀 키가 없으면 16자 이상의 암호를 입력할 수 있습니다.

   b. 사용자에게 권한이 있는 S3 클라이언트에서 기본 S3 작업을 수행합니다.

Base64 자격 증명

ONTAP S3의 기본 구성은 HTTP를 제외하며 HTTPS 및 TLS(전송 계층 보안) 연결만 사용합니다. ONTAP는 자체 서명된 인증서를 생성할 수 있지만 타사 CA(인증 기관)의 인증서를 사용하는 것이 좋습니다. CA 인증서를 사용할 때는 클라이언트 응용 프로그램과 ONTAP 개체 저장소 서버 간에 신뢰할 수 있는 관계를 만듭니다.

Base64로 인코딩된 자격 증명은 쉽게 디코딩됩니다. HTTPS를 사용하면 인코딩된 자격 증명이 중간자 패킷 스니퍼에 의해 캡처되지 않습니다.

사전 서명된 URL을 생성할 때 인증에 LDAP Fast-bind 모드를 사용하지 마십시오. 인증은 사전 서명된 URL에 포함된 Base64 액세스 키만을 기반으로 합니다. Base64 액세스 키를 디코딩하는 모든 사용자에게 사용자 이름과 암호가 표시됩니다.

인증 방법은 **nsswitch**이고 **LDAP**가 설정된 예입니다

```
$curl -siku <user>:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>", "name":<user>,"key_time_to_live":"PT6H3M"}
```

API를 SVM의 데이터 LIF가 아니라 클러스터 관리 LIF로 지정합니다. 사용자가 자신의 키를 생성하도록 허용하려면 해당 역할에 HTTP 권한을 추가하여 curl을 사용해야 합니다. 이 권한은 S3 API 권한에 추가됩니다.

Active Directory 또는 **SMB** 서버에 대한 **S3** 액세스 구성

버킷 정책 문에 지정된 nasgroup 또는 nasgroup에 속한 사용자에게 UID 및 GID가 설정되지 않은 경우 이러한 특성을 찾을 수 없으면 조회가 실패합니다. Active Directory는 UID가 아닌 SID를 사용합니다. SID 항목을 UID에 매핑할 수 없는 경우 필요한 데이터를 ONTAP로 가져와야 합니다.

그렇게 하려면 SVM이 Active Directory로 인증되고 필요한 사용자 및 그룹 정보를 가져올 수 있도록 을 "SVM active-directory create 를 참조하십시오"사용하십시오.

또는 를 사용하여 "SVM CIFS 생성"Active Directory 도메인에 SMB 서버를 생성합니다.

네임 서버와 개체 저장소에 서로 다른 도메인 이름을 사용하는 경우 조회 실패가 발생할 수 있습니다. 조회 실패를 방지하기 위해 NetApp UPN 형식의 리소스 권한 부여에 신뢰할 수 있는 도메인을 사용할 것을 권장합니다. `nasgroup/group@trusted_domain.com` 신뢰할 수 있는 도메인은 SMB 서버의 신뢰할 수 있는 도메인 목록에 추가된 도메인입니다. 방법을 알아보세요. "선호하는 신뢰할 수 있는 도메인을 추가, 제거 및 수정합니다." SMB 서버 목록에서.

인증 방법이 도메인이고 신뢰할 수 있는 도메인이 **Active Directory**에 구성된 경우 키를 생성합니다

`s3/services/<svm_uuid>/users`UPN 형식으로 지정된 사용자가 있는 끝점을 사용합니다. 예:

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user@fqdn>,"key_time_to_live":"PT6H3M"}
```

API를 SVM의 데이터 LIF가 아니라 클러스터 관리 LIF로 지정합니다. 사용자가 자신의 키를 생성하도록 허용하려면 해당 역할에 HTTP 권한을 추가하여 curl을 사용해야 합니다. 이 권한은 S3 API 권한에 추가됩니다.

인증 방법이 도메인이고 신뢰할 수 있는 도메인이 없는 경우 키를 생성합니다

이 작업은 LDAP가 비활성화되어 있거나 POSIX 사용자가 UID 및 GID를 구성하지 않은 경우에 가능합니다. 예:

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn]>,"key_time_to_live":"PT6H3M"}
```

API를 SVM의 데이터 LIF가 아니라 클러스터 관리 LIF로 지정합니다. 사용자가 자신의 키를 생성하도록 허용하려면 해당 역할에 HTTP 권한을 추가하여 curl을 사용해야 합니다. 이 권한은 S3 API 권한에 추가됩니다. 신뢰할 수 있는 도메인이 없는 경우 사용자 이름에 선택적 도메인 값(@FQDN)만 추가하면 됩니다.

LDAP 또는 도메인 사용자가 자신의 **ONTAP S3** 액세스 키를 생성할 수 있습니다

ONTAP 9.14.1부터 ONTAP 관리자는 사용자 지정 역할을 만들고 로컬 또는 도메인 그룹이나 LDAP(Lightweight Directory Access Protocol) 그룹에 부여하여 해당 그룹에 속한 사용자가 S3 클라이언트 액세스에 대한 자체 액세스 및 비밀 키를 생성할 수 있습니다.

액세스 키 생성을 위해 API를 호출하는 사용자에게 사용자 지정 역할을 생성하고 할당할 수 있도록 스토리지 VM에서 몇 가지 구성 단계를 수행해야 합니다.

LDAP가 비활성화된 경우 다음을 수행할 수 있습니다. "ONTAP S3 액세스를 위한 외부 디렉토리 서비스 구성" 사용자가 액세스 키를 생성할 수 있도록 합니다.

시작하기 전에

다음을 확인합니다.

1. S3 서버가 포함된 S3 사용 스토리지 VM이 생성되었습니다. 을 참조하십시오 "S3를 위해 SVM을 생성합니다".
2. 해당 스토리지 VM에 버킷이 생성되었습니다. 을 참조하십시오 "버킷을 만듭니다".
3. 스토리지 VM에 DNS가 구성되어 있다. 을 "DNS 서비스를 구성합니다"참조하십시오.
4. LDAP 서버의 자체 서명된 루트 CA(인증 기관) 인증서가 스토리지 VM에 설치되어 있습니다. 을 "SVM에 자체 서명된 루트 CA 인증서 설치"참조하십시오.
5. LDAP 클라이언트는 스토리지 VM에서 TLS를 사용하도록 구성했습니다. 을 "ONTAP NFS 액세스를 위한 LDAP 클라이언트 구성 생성"참조하십시오.
6. 클라이언트 구성을 SVM에 연결합니다. 을 "ONTAP NFS SVM과 LDAP 클라이언트 구성 연결"참조하십시오. 에 대한 자세한 내용은 `vserver services name-service ldap create` "ONTAP 명령 참조입니다"을 참조하십시오.
7. 데이터 스토리지 VM을 사용하는 경우 관리 네트워크 인터페이스(LIF) 및 VM에 그리고 LIF에 대한 서비스 정책을 생성합니다. 및 `network interface service-policy create` 에 대한 자세한 `network interface create` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

액세스 키 생성을 위한 사용자를 구성합니다

예 **25.** 단계

LDAP 사용자

1. LDAP를 스토리지 VM의 _NAME 서비스 데이터베이스_로 지정하고 LDAP에 대한 암호를 지정합니다.

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

에 대한 자세한 내용은 `vserver services name-service ns-switch modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. S3 사용자 REST API 끝점에 액세스하여 사용자 지정 역할 생성:
`security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
이 예에서 는 입니다 `s3-role` 스토리지 VM의 사용자에 대해 역할이 생성됩니다 `svm-1`, 모든 액세스 권한, 읽기, 만들기 및 업데이트가 부여되는 대상.

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

에 대한 자세한 내용은 `security login rest-role create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. LDAP 사용자 그룹을 만듭니다. `security login` 명령을 실행하고 S3 사용자 REST API 엔드포인트에 액세스하기 위한 새로운 사용자 지정 역할을 추가합니다. 자세히 알아보세요 `security login create` 에서 "ONTAP 명령 참조입니다" .

```
security login create -user-or-group-name <ldap-group-name>
-application http -authentication-method nsswitch -role <custom-
role-name> -is-ns-switch-group yes
```

이 예에서는 LDAP 그룹입니다 `ldap-group-1` 이(가) 에 생성됩니다 `svm-1`및 사용자 지정 역할 `s3role` API 끝점에 액세스할 수 있도록 이 API에 추가되고, 빠른 바인드 모드에서 LDAP 액세스가 활성화됩니다.

```
security login create -user-or-group-name ldap-group-1 -application
http -authentication-method nsswitch -role s3role -is-ns-switch
-group yes -second-authentication-method none -vserver svm-1 -is
-ldap-fastbind yes
```

자세한 내용은 을 "ONTAP NFS SVM에 대한 nsswitch 인증을 위해 LDAP 빠른 바인딩을 사용합니다 ."참조하십시오.

에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

LDAP 그룹에 사용자 정의 역할을 추가하면 해당 그룹의 사용자는 ONTAP 에 제한된 액세스 권한을 가질 수 있습니다. `/api/protocols/s3/services/{svm.uuid}/users` 엔드포인트. API를 호출하면 LDAP 그룹 사용자는 S3 클라이언트에 액세스하기 위한 액세스 키와 비밀 키를 직접 생성할 수 있습니다. 키는 본인만 생성할 수 있으며 다른 사용자는 생성할 수 없습니다.

도메인 사용자

1. S3 사용자 REST API 엔드포인트에 액세스할 수 있는 사용자 지정 역할을 만듭니다.

```
security login rest-role create -vserver <vserver-name> -role <custom-
role-name> -api "/api/protocols/s3/services/*/users" -access <access-
type>
```

이 예에서는 `s3-role` 스토리지 VM의 사용자에 대한 역할이 생성됩니다. `svm-1` 모든 접근 권한(읽기, 만들기, 업데이트)이 부여됩니다.

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

에 대한 자세한 내용은 `security login rest-role create` "ONTAP 명령 참조입니다"을 참조하십시오.

1. 도메인 사용자 그룹을 만듭니다. `security login` 명령을 실행하고 S3 사용자 REST API 엔드포인트에 액세스하기 위한 새로운 사용자 지정 역할을 추가합니다. 자세히 알아보세요 `security login create` 에서 "ONTAP 명령 참조입니다" .

   ```
   security login create -vserver <vserver-name> -user-or-group-name
   domain\<group-name> -application http -authentication-method domain
   -role <custom-role-name>
   ```

   이 예에서 도메인 그룹은 `domain\group1` 에서 생성됩니다 `svm-1` , 그리고 사용자 정의 역할 `s3role` API 엔드포인트에 액세스하기 위해 추가되었습니다.

   ```
   security login create -user-or-group-name domain\group1 -application
   http -authentication-method domain -role s3role -vserver svm-1
   ```

   에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

도메인 그룹에 사용자 정의 역할을 추가하면 해당 그룹의 사용자가 ONTAP 에 제한적으로 액세스할 수 있습니다. `/api/protocols/s3/services/{svm.uuid}/users` 엔드포인트. API를 호출하면 도메인 그룹 사용자는 S3 클라이언트에 액세스하기 위한 액세스 키와 비밀 키를 직접 생성할 수 있습니다. 해당 키는 본인만 생성할 수 있으며 다른 사용자는 생성할 수 없습니다.

S3 또는 LDAP 사용자로 자체 액세스 키를 생성합니다

ONTAP 9.14.1부터 관리자가 사용자 고유의 키를 생성하는 역할을 부여한 경우, S3 클라이언트에 액세스하기 위한 고유한 액세스 및 비밀 키를 생성할 수 있습니다. 다음 ONTAP REST API 끝점을 사용하여 자신에 대해서만 키를 생성할 수 있습니다.

S3 사용자를 생성하고 키를 생성합니다**.**

이 REST API 호출은 다음 메서드와 엔드포인트를 사용합니다. 이 엔드포인트에 대한 자세한 내용은 참조를 참조하세요. "API 설명서" .

HTTP 메소드	경로
게시	/api/protocols/s3/services/{svm.uuid}/사용자

도메인 사용자의 경우 S3 사용자 이름에 다음 형식을 사용하세요. `user@fqdn` , 어디 `fqdn` 도메인의 정규화된 도메인 이름입니다.

컬의 예

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"user1@example.com"}'
```

JSON 출력 예

```
{
  "records": [
    {
      "access_key": "4KX07KF7ML8YNWY01JWG",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

S3 사용자에 대한 키 재생성

S3 사용자가 이미 있는 경우 해당 사용자의 액세스 키와 비밀 키를 다시 생성할 수 있습니다. 이 REST API 호출은 다음 메서드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
반점	/api/프로토콜/s3/서비스/{svm.uuid}/사용자/{이름}

컬의 예

```
curl
--request PATCH \
--location "https://$FQDN_IP
/api/protocols/s3/services/{svm.uuid}/users/{name} " \
--include \
--header "Authorization: Basic $BASIC_AUTH" \
--data '{"regenerate_keys":"True"}'
```

JSON 출력 예

```
{
  "records": [
    {
      "access_key": "DX12U609DMRVD8U30Z1M",
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

S3 오브젝트 스토리지에 대한 클라이언트 액세스 지원

원격 **FabricPool** 계층화에 대해 **ONTAP S3** 액세스를 설정합니다

ONTAP S3를 원격 FabricPool 용량(클라우드) 계층으로 사용하려면 ONTAP S3 관리자가 원격 ONTAP 클러스터 관리자에게 S3 서버 구성에 대한 정보를 제공해야 합니다.

이 작업에 대해

FabricPool 클라우드 계층을 구성하려면 다음 S3 서버 정보가 필요합니다.

- 서버 이름(FQDN)
- 버킷 이름
- CA 인증서
- 액세스 키
- 암호(암호 액세스 키)

또한 다음과 같은 네트워킹 구성이 필요합니다.

- DNS 서버에 S3 서버의 FQDN 이름과 LIF의 IP 주소를 포함하여 admin SVM용으로 구성된 원격 ONTAP S3 서버의 호스트 이름에 대한 항목이 있어야 합니다.
- 클러스터 피어링이 필요하지 않더라도 로컬 클러스터에 인터클러스터 LIF를 구성해야 합니다.

ONTAP S3를 클라우드 계층으로 구성하는 방법에 대한 FabricPool 설명서를 참조하십시오.

"FabricPool를 사용하여 스토리지 계층 관리"

ONTAP S3를 로컬 FabricPool 용량 계층으로 사용하려면 생성한 버킷을 기반으로 오브젝트 저장소를 정의한 다음 오브젝트 저장소를 성능 계층 애그리게이트에 연결하여 FabricPool를 생성해야 합니다.

시작하기 전에

ONTAP S3 서버 이름과 버킷 이름이 있어야 하며, 클러스터 LIF("-vserver Cluster" 매개 변수)를 사용하여 S3 서버를 생성해야 합니다.

이 작업에 대해

오브젝트 저장소 구성에는 S3 서버, 버킷 이름 및 인증 요구사항을 비롯한 로컬 용량 계층에 대한 정보가 포함됩니다.

생성한 오브젝트 저장소 구성은 다른 오브젝트 저장소 또는 버킷과 다시 연관해서는 안 됩니다. 로컬 계층에 대해 여러 개의 버킷을 생성할 수 있지만, 단일 버킷에 여러 오브젝트 저장소를 생성할 수는 없습니다.

로컬 용량 계층에는 FabricPool 라이센스가 필요하지 않습니다.

단계

1. 로컬 용량 계층에 대한 객체 저장소 생성:

   '스토리지 집계 객체 저장 구성 create-object-store-name_store_name_-IPSpace 클러스터 공급자 유형 ONTAP_S3-server_name_-container-name_bucket_name_-access-key_access-secret-password password"

   - container-name은 사용자가 만든 S3 버킷입니다.
   - '-access-key' 파라미터는 ONTAP S3 서버에 대한 요청을 승인한다.
   - secret-password 매개 변수(secret access key)는 ONTAP S3 서버에 대한 요청을 인증합니다.
   - '-is-certificate-validation-enabled' 매개 변수를 'false'로 설정하여 ONTAP S3에 대한 인증서 확인을 비활성화할 수 있습니다.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyLocalObjStore -ipspace Cluster -provider-type
   ONTAP_S3 -server s3.example.com
   -container-name bucket1 -access-key myS3key -secret-password myS3pass
   ```

2. 오브젝트 저장소 구성 정보를 표시하고 확인합니다.

   'Storage aggregate object-store config show'를 선택합니다

3. 선택 사항 "비활성 데이터 보고를 사용하여 볼륨의 비활성 데이터 양을 결정합니다":.

   볼륨의 비활성 데이터 양을 보면 FabricPool 로컬 계층화에 사용할 애그리게이트를 결정할 수 있습니다.

4. 오브젝트 저장소를 Aggregate에 연결합니다.

   'STORAGE 집계 객체-STORE ATTACH-AGGATE_AGGr_NAME_-OBJECT-STORE-NAME_STORE_NAME_'

'allow-flexgroup * true *' 옵션을 사용하면 FlexGroup 볼륨 구성요소를 포함하는 애그리게이트를 연결할 수 있습니다.

```
cluster1::> storage aggregate object-store attach
-aggregate aggr1 -object-store-name MyLocalObjStore
```

5. 오브젝트 저장소 정보를 표시하고 첨부된 오브젝트 저장소를 사용할 수 있는지 확인합니다.

'스토리지 골재 오브젝트 저장소 쇼'

```
cluster1::> storage aggregate object-store show

Aggregate    Object Store Name    Availability State
---------    -----------------    ------------------
aggr1        MyLocalObjStore      available
```

관련 정보

- "저장소 집계 객체-저장소 연결"
- "저장소 집계 객체-저장소 구성 생성"
- "저장소 집계 객체-저장소 구성 표시"
- "저장소 집계 객체-저장소 표시"

S3 클라이언트 애플리케이션이 **ONTAP S3** 서버에 액세스하도록 설정

S3 클라이언트 애플리케이션에서 ONTAP S3 서버에 액세스하려면 ONTAP S3 관리자가 S3 사용자에게 구성 정보를 제공해야 합니다.

시작하기 전에

S3 클라이언트 앱은 다음 AWS 서명 버전을 사용하여 ONTAP S3 서버를 인증할 수 있어야 합니다.

- 서명 버전 4, ONTAP 9.8 이상
- 서명 버전 2, ONTAP 9.11.1 이상

다른 서명 버전은 ONTAP S3에서 지원되지 않습니다.

ONTAP S3 관리자는 버킷 정책 또는 오브젝트 스토리지 서버 정책에서 S3 사용자를 생성하고 개별 사용자 또는 그룹 구성원으로 액세스 권한을 부여해야 합니다.

S3 클라이언트 앱은 ONTAP S3 서버 이름을 확인할 수 있어야 합니다. 이 경우 ONTAP S3 관리자가 S3 서버 LIF의 S3 서버 이름(FQDN) 및 IP 주소를 제공해야 합니다.

이 작업에 대해

ONTAP S3 버킷에 액세스하려면 S3 클라이언트 애플리케이션의 사용자가 ONTAP S3 관리자가 제공하는 정보를 입력합니다.

ONTAP 9.9.1부터 ONTAP S3 서버는 다음 AWS 클라이언트 기능을 지원합니다.

- 사용자 정의 개체 메타데이터

  PUT(또는 POST)를 사용하여 개체를 만들 때 키 값 쌍 집합을 메타데이터로 할당할 수 있습니다. 개체에 대해 가져오기/헤드 작업을 수행하면 사용자 정의 메타데이터가 시스템 메타데이터와 함께 반환됩니다.

- 개체 태그 지정

  객체 분류에 대한 태그로 별도의 키 값 쌍 세트를 할당할 수 있습니다. 메타데이터와 달리 태그는 오브젝트와 독립적으로 REST API를 사용하여 생성되고 읽혀지며, 오브젝트가 만들어지거나 그 이후에 언제든지 구현됩니다.

> ⓘ 클라이언트가 태그 정보를 가져오고 넣을 수 있도록 하려면 버킷 또는 그룹 정책을 사용하여 GetObjectTagging, PutObjectTagging, DeleteObjectTagging 등의 작업을 허용해야 합니다.

자세한 내용은 AWS S3 설명서를 참조하십시오.

단계

1. S3 서버 이름과 CA 인증서를 입력하여 ONTAP S3 서버로 S3 클라이언트 앱을 인증합니다.
2. 다음 정보를 입력하여 S3 클라이언트 앱에서 사용자를 인증합니다.
   - S3 서버 이름(FQDN) 및 버킷 이름입니다
   - 사용자의 액세스 키 및 암호 키입니다

ONTAP S3 스토리지 서비스 레벨

ONTAP에는 해당 최소 성능 요소에 매핑된 사전 정의된 스토리지 서비스가 포함되어 있습니다.

클러스터 또는 SVM에서 사용 가능한 실제 스토리지 서비스 세트는 SVM에서 애그리게이트를 구성하는 스토리지 유형에 따라 결정됩니다.

다음 표에는 최소 성능 요소가 사전 정의된 스토리지 서비스에 매핑되는 방식이 나와 있습니다.

스토리지 서비스	예상 **IOPS(SLA)**	최대 **IOPS(SLO)**	최소 볼륨 **IOPS**	예상 지연 시간	예상 **IOPS**가 적용됩니까**?**
값	TB당 128개	TB당 512개	75를	17ms	AFF: 예 그렇지 않으면 아니오
성능	TB당 2048개	TB당 4096	500입니다	2ms	예
익스트림	TB당 6144	12288/TB	1000입니다	1ms	예

다음 표에는 각 미디어 또는 노드 유형에 대해 사용 가능한 스토리지 서비스 수준이 정의되어 있습니다.

미디어 또는 노드	사용 가능한 스토리지 서비스 수준입니다
디스크	값
가상 머신 디스크	값
하이브리드	값
최적의 용량을 제공하는 플래시	값
솔리드 스테이트 드라이브(SSD) - 비 AFF	값
최적의 성능을 발휘하는 플래시-SSD(AFF)	최고의 성능, 가치

ONTAP S3 버킷을 위한 CORS(Cross-Origin Resource Sharing)를 구성합니다

ONTAP 9.16.1부터 CORS(Cross-Origin Resource Sharing)를 구성하여 다른 도메인의 클라이언트 웹 애플리케이션이 ONTAP 버킷을 액세스할 수 있도록 할 수 있습니다. 이렇게 하면 웹 브라우저를 사용하여 버킷 객체에 안전하게 액세스할 수 있습니다.

CORS는 HTTP를 기반으로 하는 프레임워크로, 한 웹 페이지에 정의된 스크립트가 다른 도메인의 서버에 있는 리소스에 액세스할 수 있도록 합니다. 프레임워크는 웹 보안의 초기 기반인 _same-origin policy_를 안전하게 우회하는 데 사용됩니다. 주요 개념 및 용어에 대한 설명은 아래에 나와 있습니다.

원점

오리진은 리소스의 위치와 ID를 정확하게 정의합니다. 이 값은 다음 값의 조합으로 표시됩니다.

- URI 체계(프로토콜)
- 호스트 이름(도메인 이름 또는 IP 주소)
- 포트 번호입니다

원점의 간단한 예는 다음과 같습니다 `https://www.mycompany.com:8001`. 오리진이 CORS와 함께 사용될 때 요청을 하는 클라이언트를 식별합니다.

동일한 원본 정책입니다

SOP(동일 원본 정책)는 브라우저 기반 스크립트에 적용되는 보안 개념 및 제한 사항입니다. 이 정책은 두 페이지가 동일한 원본에 있는 경우 웹 페이지에서 처음 로드된 스크립트가 다른 페이지의 데이터에 액세스할 수 있도록 합니다. 이 제한 사항은 악성 스크립트가 다른 오리진 페이지의 데이터에 액세스하는 것을 방지합니다.

일반적인 **CORS** 사용 사례

CORS에는 몇 가지 일반적인 사용 사례가 있습니다. 대부분의 경우 도메인 간 인증뿐만 아니라 AJAX 요청, 글꼴 로드, 스타일시트 및 스크립트와 같이 도메인 간 액세스의 잘 정의된 인스턴스가 포함됩니다. CORS는 단일 페이지 애플리케이션(SPA)의 일부로 구현할 수도 있습니다.

HTTP 헤더

CORS는 HTTP 요청 및 응답에 삽입된 헤더를 사용하여 구현됩니다. 예를 들어, 액세스 제어를 구현하고 메서드와 헤더를 포함하여 허용되는 작업을 나타내는 몇 가지 응답 헤더가 있습니다. HTTP 요청에 _Origin_header가 있으면

도메인 간 요청으로 정의됩니다. 오리진 값은 CORS 서버에서 유효한 CORS 구성을 찾는 데 사용됩니다.

HTTP 사전 전송 요청

서버가 특정 메서드 및 헤더를 포함하여 CORS를 지원하는지 여부를 초기에 확인하기 위한 선택적 요청입니다. 응답에 따라 CORS 요청을 완료할 수도 있고 완료할 수도 없습니다.

ONTAP 버킷

버킷은 잘 정의된 네임스페이스를 기반으로 저장 및 액세스하는 오브젝트의 컨테이너입니다. ONTAP 버킷에는 두 가지 유형이 있습니다.

- NAS 및 S3 프로토콜을 통해 액세스할 수 있는 NAS 버킷입니다
- S3 프로토콜을 통해서만 액세스할 수 있는 S3 버킷

ONTAP에서의 **CORS** 구현

CORS는 ONTAP 9.16.1 이상 릴리즈에서 기본적으로 사용됩니다. 활성화할 각 SVM에서 CORS를 구성해야 합니다.

ONTAP 클러스터에 대해 CORS를 사용하지 않도록 설정하는 관리 옵션은 없습니다. 그러나 규칙을 정의하지 않거나 기존 규칙을 모두 삭제하여 이 규칙을 효과적으로 비활성화할 수 있습니다.

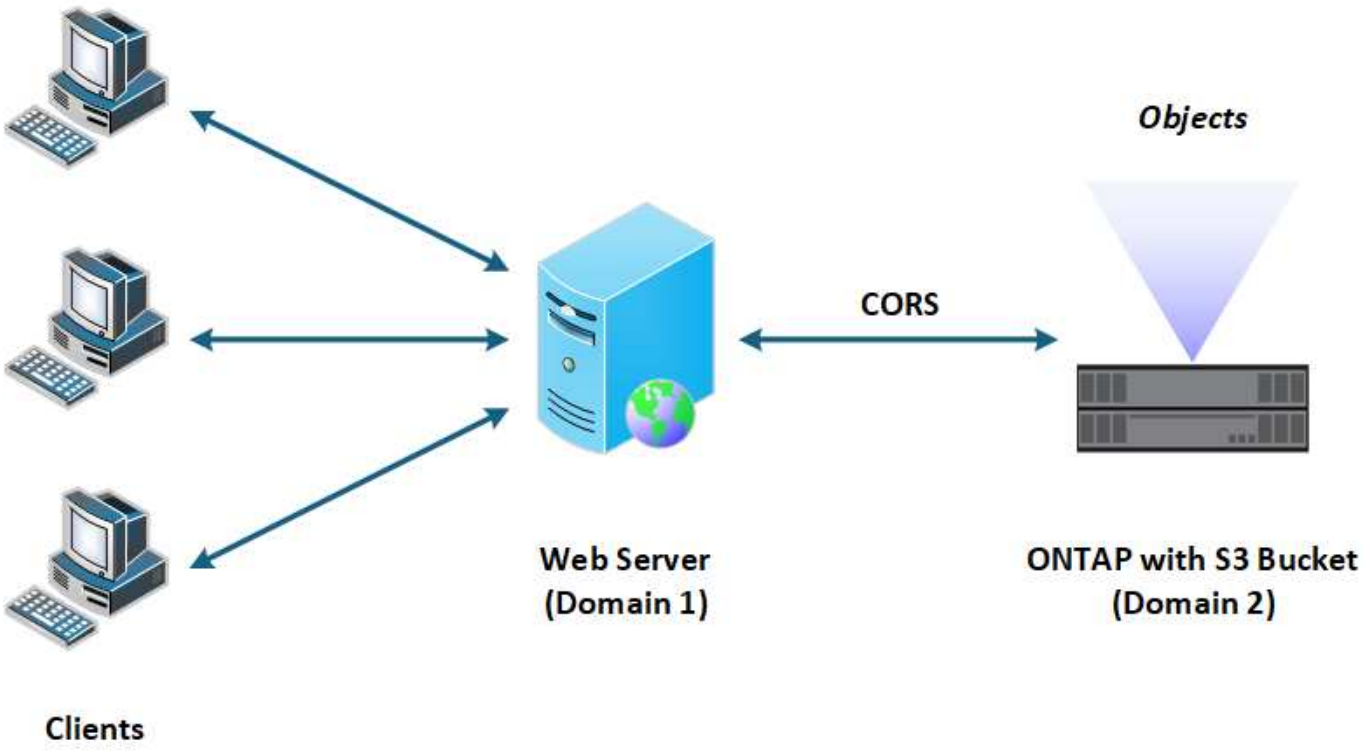
가능한 사용 사례

ONTAP CORS 구현은 도메인 간 리소스 액세스를 위한 다음과 같은 몇 가지 가능한 토폴로지를 지원합니다.

- ONTAP S3 버킷(동일하거나 다른 SVM 또는 클러스터 내부)
- ONTAP NAS 버킷(동일하거나 다른 SVM 또는 클러스터 내)
- ONTAP S3 및 NAS 버킷(동일하거나 다른 SVM 또는 클러스터 내)
- ONTAP 버킷 및 외부 공급업체 버킷
- 다양한 시간대의 버킷

개략적인 보기

다음은 CORS에서 ONTAP S3 버킷에 대한 액세스를 지원하는 방법을 개략적으로 보여 줍니다.



CORS 규칙 정의

이 기능을 활성화하고 사용하려면 ONTAP에서 CORS 규칙을 정의해야 합니다.

구성 작업

ONTAP에서 지원되는 세 가지 기본 구성 규칙 동작은 다음과 같습니다.

- 표시
- 생성
- 삭제

ONTAP에 정의된 CORS 규칙에는 SVM과 버킷은 물론 허용된 오리진, 메서드 및 헤더를 포함한 여러 속성이 있습니다.

관리 옵션

ONTAP 클러스터에서 CORS를 관리할 때 사용할 수 있는 몇 가지 옵션이 있습니다.

ONTAP 명령줄 인터페이스입니다

명령줄 인터페이스를 사용하여 CORS를 구성할 수 있습니다. 자세한 내용은 을 CLI를 사용하여 CORS 관리 참조하십시오.

ONTAP REST API를 참조하십시오

ONTAP REST API를 사용하여 CORS를 구성할 수 있습니다. CORS 기능을 지원하기 위해 추가된 새 끝점이 없습니다. 대신 다음과 같은 기존 끝점을 사용할 수 있습니다.

```
/api/protocols/s3/services/{svm.uuid}/buckets/{bucket.uuid}
```

자세한 내용은 을 "ONTAP 자동화 설명서"참조하십시오.

S3 API를 사용합니다

S3 API를 사용하여 ONTAP 버킷에서 CORS 구성을 생성하고 삭제할 수 있습니다. S3 클라이언트 관리자는 다음을 비롯하여 충분한 Privileges가 필요합니다.

- 액세스 또는 비밀 키 자격 증명
- s3api를 통한 액세스를 허용하도록 버킷에 구성된 정책입니다

업그레이드 및 되돌리기

CORS를 사용하여 ONTAP S3 버킷을 액세스하려는 경우 몇 가지 관리 문제를 알고 있어야 합니다.

업그레이드 중

모든 노드가 9.16.1로 업그레이드되면 CORS 기능이 지원됩니다. 혼합 모드 클러스터에서 이 기능은 유효 클러스터 버전(ECV)이 9.16.1 이상일 때만 사용할 수 있습니다.

되돌리기

사용자 관점에서 클러스터 복원을 진행하기 전에 모든 CORS 구성을 제거해야 합니다. 내부적으로 이 작업은 모든 CORS 데이터베이스를 삭제합니다. 이러한 데이터 구조를 지우고 되돌리는 명령을 실행하라는 메시지가 표시됩니다.

CLI를 사용하여 **CORS** 관리

ONTAP CLI를 사용하여 CORS 규칙을 관리할 수 있습니다. 주요 작업은 아래에 설명되어 있습니다. CORS 명령을 실행하려면 ONTAP * admin * 권한 수준이어야 합니다.

생성

명령을 사용하여 CORS 규칙을 정의할 수 `vserver object-store-server bucket cors-rule create` 있습니다. 에 대한 자세한 내용은 `vserver object-store-server bucket cors-rule create` "ONTAP 명령 참조입니다"을 참조하십시오.

매개 변수

규칙을 만드는 데 사용되는 매개 변수는 아래에 설명되어 있습니다.

매개 변수	설명
`vserver`	규칙이 생성되는 오브젝트 저장소 서버 버킷을 호스팅하는 SVM(SVM)의 이름을 지정합니다.

매개 변수	설명
`bucket`	규칙이 생성되는 오브젝트 저장소 서버의 버킷 이름입니다.
`index`	규칙이 생성되는 개체 저장소 서버 버킷의 인덱스를 나타내는 선택적 매개 변수입니다.
`rule id`	오브젝트 저장소 서버 버킷 규칙의 고유 식별자입니다.
`allowed-origins`	오리진 간 요청이 출발할 수 있는 오리진 목록입니다.
`allowed-methods`	오리진 간 요청에서 허용되는 HTTP 메서드 목록입니다.
`allowed-headers`	크로스 오리진 요청에서 허용되는 HTTP 헤더 목록입니다.
`expose-headers`	고객이 애플리케이션에서 액세스할 수 있는 CORS 응답에 보내는 추가 헤더 목록입니다.
`max-age-in-seconds`	브라우저가 특정 리소스에 대해 비행 전 응답을 캐시해야 하는 시간을 지정하는 선택적 매개 변수입니다.

예

```
vserver object-store-server bucket cors-rule create -vserver vs1 -bucket
bucket1 -allowed-origins www.myexample.com -allowed-methods GET,DELETE
```

표시

명령을 사용하여 현재 규칙 및 해당 내용의 목록을 표시할 수 `vserver object-store-server bucket cors-rule show` 있습니다. 에 대한 자세한 내용은 `vserver object-store-server bucket cors-rule show` "ONTAP 명령 참조입니다"을 참조하십시오.

매개 변수를 포함하면 `-instance` 각 규칙에 대해 제공되는 데이터가 확장됩니다. 원하는 필드를 지정할 수도 있습니다.

예

```
server object-store-server bucket cors-rule show -instance
```

삭제

delete 명령을 사용하여 CORS 규칙의 인스턴스를 제거할 수 있습니다. `index`규칙 값이 필요하므로 이 작업은 다음 두 단계로 수행됩니다.

1. `show`명령을 실행하여 규칙을 표시하고 해당 인덱스를 검색합니다.

2. 인덱스 값을 사용하여 삭제를 실행합니다.

예

```
vserver object-store-server bucket cors-rule delete -vserver vs1 -bucket
bucket1 -index 1
```

수정

기존 CORS 규칙을 수정하는 데 사용할 수 있는 CLI 명령이 없습니다. 규칙을 수정하려면 다음을 수행해야 합니다.

1. 기존 규칙을 삭제합니다.
2. 원하는 옵션을 사용하여 새 규칙을 만듭니다.

SnapMirror S3로 버킷 보호

ONTAP SnapMirror S3에 대해 알아보십시오

ONTAP 9.10.1부터 SnapMirror 미러링 및 백업 기능을 사용하여 ONTAP S3 오브젝트 저장소의 버킷을 보호할 수 있습니다. 표준 SnapMirror와 달리 SnapMirror S3를 통해 AWS S3와 같은 비 NetApp 대상에 대한 미러링 및 백업을 수행할 수 있습니다.

SnapMirror S3는 ONTAP S3 버킷에서 다음 대상에 이르는 액티브 미러 및 백업 계층을 지원합니다.

타겟	액티브 미러 및 테이크오버 지원	백업 및 복원을 지원합니까?
ONTAP S3 • 버킷이 동일한 SVM에 포함됩니다 • 동일한 클러스터에서 서로 다른 SVM의 버킷 • SVM의 다양한 클러스터에서 버킷	예	예
StorageGRID	아니요	예
설치하고	아니요	예
Azure용 Cloud Volumes ONTAP	예	예
AWS 환경을 위한 Cloud Volumes ONTAP	예	예
Google Cloud용 Cloud Volumes ONTAP	예	예

ONTAP S3 서버에서 기존 버킷을 보호하거나 데이터 보호를 즉시 활성화할 수 있는 새로운 버킷을 생성할 수 있습니다.

SnapMirror S3 요구사항

- ONTAP 버전입니다

  소스 및 대상 클러스터에서 ONTAP 9.10.1 이상이 실행되고 있어야 합니다.

SnapMirror S3는 MetroCluster 구성에서 지원되지 않습니다.

- 라이센싱

  에서 사용할 수 있는 라이센스는 다음과 같습니다 "ONTAP 1 을 참조하십시오" ONTAP 소스 및 대상 시스템에서 다음 항목에 대한 액세스를 제공하려면 소프트웨어 제품군이 필요합니다.

  - ONTAP S3 프로토콜 및 스토리지
  - SnapMirror S3에서 다른 NetApp 오브젝트 저장소 타겟(ONTAP S3, StorageGRID, Cloud Volumes ONTAP) 공략
  - SnapMirror S3에서 AWS S3(에서 사용 가능"ONTAP One 호환성 번들")를 비롯한 타사 오브젝트 저장소 공략
  - 클러스터에서 ONTAP 9.10.1을 실행 중인 "FabricPool 라이센스"경우 가 필요합니다.
- ONTAP S3
  - ONTAP S3 서버에서 소스 및 타겟 SVM을 실행해야 합니다.
  - TLS 액세스를 위한 CA 인증서를 S3 서버를 호스팅하는 시스템에 설치하는 것이 좋지만 반드시 필요한 것은 아닙니다.
    - S3 서버의 인증서를 서명하는 데 사용되는 CA 인증서는 S3 서버를 호스팅하는 클러스터의 관리 스토리지 VM에 설치해야 합니다.
    - 자체 서명된 CA 인증서 또는 외부 CA 공급업체에서 서명한 인증서를 사용할 수 있습니다.
    - 소스 또는 대상 스토리지 VM이 HTTPS에서 수신 대기 중이 아닌 경우 CA 인증서를 설치할 필요가 없습니다.
- 피어링(ONTAP S3 타겟용)
  - 인터클러스터 LIF를 구성해야 하며(원격 ONTAP 대상용), 소스 및 대상 클러스터의 인터클러스터 LIF가 소스 및 대상 S3 서버 데이터 LIF에 연결할 수 있습니다.
  - 소스 및 타겟 클러스터를 피어링했습니다(원격 ONTAP 타겟의 경우).
  - 소스 및 타겟 스토리지 VM을 모든 ONTAP 타겟에 대해 피어링했습니다.
- SnapMirror 정책
  - 모든 SnapMirror S3 관계에 S3별 SnapMirror 정책이 필요하지만 여러 관계에 동일한 정책을 사용할 수 있습니다.
  - 사용자 고유의 정책을 만들거나 다음 값을 포함하는 기본 * 연속 * 정책을 사용할 수 있습니다.
    - 스로틀(처리량/대역폭의 상한) - 무제한
    - 복구 지점 목표 시간: 1시간(3600초)

SnapMirror 관계에 있는 두 개의 S3 버킷이 있을 때 개체의 현재 버전이 만료(삭제됨)되도록 라이프사이클 정책이 구성된 경우 동일한 작업이 파트너 버킷에 복제된다는 것을 알아야 합니다. 파트너 버킷이 읽기 전용 또는 패시브 인 경우에도 마찬가지입니다.

- 루트 사용자 키 SnapMirror S3 관계에 필요한 스토리지 VM 루트 사용자 액세스 키는 ONTAP에서 기본적으로 할당하지 않습니다. SnapMirror S3 관계를 처음 생성할 때 소스 및 대상 스토리지 VM에 키가 있는지 확인해야 하며, 키가 없으면 키를 다시 생성해야 합니다. 다시 생성해야 하는 경우 액세스 및 암호 키 쌍을 사용하는 모든 클라이언트 및 모든 SnapMirror 오브젝트 저장소 구성을 새 키로 업데이트해야 합니다.

S3 서버 구성에 대한 자세한 내용은 다음 항목을 참조하십시오.

- "스토리지 VM에서 S3 서버를 활성화합니다"
- "ONTAP S3 구성 프로세스 정보"

클러스터 및 스토리지 VM 피어링에 대한 자세한 내용은 다음 항목을 참조하십시오.

- "미러링 및 보관 준비(System Manager, 1-6단계)"
- "클러스터 및 SVM 피어링(CLI)"

지원되는 **SnapMirror** 관계

SnapMirror S3는 팬아웃 및 캐스케이드 관계를 지원합니다. 개요는 다음을 참조하세요. "팬아웃 및 캐스케이드 데이터 보호 구축" .

SnapMirror S3는 팬인 구축(여러 소스 버킷과 단일 대상 버킷 간의 데이터 보호 관계)을 지원하지 않습니다. SnapMirror S3는 여러 클러스터에서 단일 보조 클러스터로 여러 버킷 미러를 지원할 수 있지만 각 소스 버킷에는 보조 클러스터에 자체 대상 버킷이 있어야 합니다.

SnapMirror S3는 MetroCluster 환경에서 지원되지 않습니다.

S3 버킷에 대한 액세스 제어

새 버킷을 생성할 때 사용자 및 그룹을 생성하여 액세스를 제어할 수 있습니다.

SnapMirror S3는 소스 버킷에서 타겟 버킷으로 오브젝트를 복제하지만 소스 오브젝트 저장소의 사용자, 그룹 및 정책을 타겟 오브젝트 저장소로 복제하지 않습니다.

페일오버 이벤트 중에 클라이언트가 대상 버킷에 액세스할 수 있도록 대상 오브젝트 저장소에서 사용자, 그룹 정책, 권한 및 유사한 구성 요소를 구성해야 합니다.

대상 클러스터에서 사용자가 생성될 때 소스 키를 수동으로 제공하는 경우 소스 및 대상 사용자가 동일한 액세스 및 암호 키를 사용할 수 있습니다. 예를 들면 다음과 같습니다.

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

자세한 내용은 다음 항목을 참조하십시오.

- "S3 사용자 및 그룹 추가(System Manager)"
- "S3 사용자 생성(CLI)"
- "S3 그룹 생성 또는 수정(CLI)"

SnapMirror S3에서 **S3** 오브젝트 잠금 및 버전 관리를 사용합니다

오브젝트 잠금 및 버전 관리가 활성화된 ONTAP 버킷에서 SnapMirror S3를 사용할 수 있으며 다음과 같은 몇 가지 사항을 고려해야 합니다.

- 오브젝트 잠금이 설정된 상태로 소스 버킷을 복제하려면 대상 버킷에도 오브젝트 잠금이 설정되어 있어야 합니다.

또한 소스와 대상 모두에 버전 관리가 활성화되어 있어야 합니다. 이렇게 하면 두 버킷의 기본 보존 정책이 서로 다른 경우 삭제 내용을 대상 버킷에 미러링할 필요가 없습니다.

- S3 SnapMirror는 오브젝트의 기간별 버전을 복제하지 않습니다. 개체의 현재 버전만 복제됩니다.

Object Locked 객체가 대상 버킷으로 미러링되면 원래 보존 시간이 유지됩니다. 잠금 해제된 객체가 복제되면 대상 버킷의 기본 보존 기간이 적용됩니다. 예를 들면 다음과 같습니다.

- 버킷 A의 기본 보존 기간은 30일이고 버킷 B의 기본 보존 기간은 60일입니다. Bucket A에서 Bucket B로 복제된 객체는 Bucket B의 기본 보존 기간보다 작더라도 30일 보존 기간을 유지합니다
- 버킷 A에는 기본 보존 기간이 없고 버킷 B에는 기본 보존 기간이 60일입니다. 잠금 해제된 객체가 버킷 A에서 버킷 B로 복제되면 60일의 보존 기간이 적용됩니다. 객체가 Bucket A에서 수동으로 잠길 경우 Bucket B로 복제될 때 원래 보존 기간이 유지됩니다
- 버킷 A의 기본 보존 기간은 30일이고 버킷 B의 기본 보존 기간은 없습니다. 버킷 A에서 버킷 B로 복제된 객체는 30일의 보존 기간을 유지합니다.

원격 클러스터의 미러링 및 백업 보호

원격 클러스터에서 새로운 **ONTAP S3** 버킷에 대한 미러 관계를 생성합니다

새로운 S3 버킷을 생성하면 원격 클러스터의 SnapMirror S3 대상으로 즉시 보호할 수 있습니다.

이 작업에 대해

소스 시스템과 대상 시스템 모두에서 작업을 수행해야 합니다.

시작하기 전에

- ONTAP 버전, 라이센스 및 S3 서버 구성에 대한 요구사항이 완료되었습니다.
- 소스 클러스터와 대상 클러스터 간에 피어링 관계가 있으며, 소스 및 대상 스토리지 VM 간에 피어링 관계가 있습니다.
- 소스 및 대상 VM에 CA 인증서가 필요합니다. 자체 서명된 CA 인증서 또는 외부 CA 공급업체에서 서명한 인증서를 사용할 수 있습니다.

시스템 관리자

1. 이 스토리지 VM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 대상 스토리지 VM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 다시 생성하십시오.
   a. 스토리지 > 스토리지 VM * 을 클릭한 다음 스토리지 VM을 선택합니다.
   b. 설정 * 탭에서 * S3 * 타일을 클릭합니다 .
   c. 사용자 * 탭에서 루트 사용자에 대한 액세스 키가 있는지 확인합니다.
   d. 없으면 * root * 옆에 있는 을 클릭한 다음 * 키 재생성 * 을 클릭합니다. 키가 이미 있는 경우 키를 다시 생성하지 마십시오.
2. 스토리지 VM을 편집하여 사용자를 추가하고 소스 및 대상 스토리지 VM 모두에서 사용자를 그룹에 추가하려면 다음을 수행합니다.

   스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM, * 설정 * 을 차례로 클릭한 다음 S3를 클릭합니다.

   을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.
3. 소스 클러스터에서 기존 SnapMirror S3 정책이 없고 기본 정책을 사용하지 않으려는 경우 새 정책을 만듭니다.
   a. 보호 > 개요 * 를 클릭한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. 보호 정책 * 옆에 있는 * 추가 * 를 클릭합니다.
      - 정책 이름과 설명을 입력합니다.
      - 정책 범위, 클러스터 또는 SVM을 선택합니다
      - SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
      - 스로틀 * 및 * 복구 지점 목표 * 값을 입력합니다.
4. SnapMirror 보호를 통해 버킷 생성:
   a. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다. 사용 권한 확인은 선택 사항이지만 사용하는 것이 좋습니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력한 다음 * 추가 옵션 * 을 클릭합니다.
   c. 사용 권한 * 에서 * 추가 * 를 클릭합니다.
      - * Principal * 및 * Effect * - 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
      - * 조치 * - 다음 값이 표시되는지 확인합니다.

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - * 리소스 * - 기본값(*bucketname, bucketname/* *) 또는 필요한 기타 값을 사용합니다.

        을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.

d. 보호 * 에서 * SnapMirror(ONTAP 또는 클라우드) 활성화 * 를 선택합니다. 그런 다음 다음 다음 값을 입력합니다.

- 목적지
  - * 대상: ONTAP 시스템 *
  - * 클러스터 *: 원격 클러스터를 선택합니다.
  - * 스토리지 VM *: 원격 클러스터에서 스토리지 VM을 선택합니다.
  - * S3 서버 CA 인증서 *: _source_certificate의 내용을 복사하여 붙여 넣습니다.
- 출처
  - * S3 서버 CA 인증서: * destination_certificate의 내용을 복사하여 붙여 넣습니다.

5. 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우 * 대상에서 동일한 인증서 사용 * 을 선택합니다.
6. Destination Settings * 를 클릭하면 버킷 이름, 용량 및 성능 서비스 레벨의 기본값 대신 사용자 정의 값을 입력할 수도 있습니다.
7. 저장 * 을 클릭합니다. 소스 스토리지 VM에 새 버킷이 생성되면 대상 스토리지 VM을 생성한 새 버킷에 미러링됩니다.

잠긴 버킷을 백업합니다

ONTAP 9.14.1부터는 잠긴 S3 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

새 버킷이나 기존 버킷에 대한 보호 설정을 정의할 때 소스 및 타겟 클러스터가 ONTAP 9.14.1 이상을 실행하고 소스 버킷에서 오브젝트 잠금이 설정된 경우 대상 버킷에서 오브젝트 잠금을 설정할 수 있다. 소스 버킷의 객체 잠금 모드 및 잠금 보존 기간이 대상 버킷의 복제된 객체에 적용됩니다. 또한 * Destination Settings * 섹션에서 대상 버킷에 대해 다른 잠금 보존 기간을 정의할 수 있습니다. 이 보존 기간은 소스 버킷 및 S3 인터페이스에서 복제되는 잠기지 않은 오브젝트에도 적용됩니다.

버킷에서 오브젝트 잠금을 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 "버킷을 만듭니다".

CLI를 참조하십시오

1. 이 SVM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 타겟 SVM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 재생성

   'vserver object-store-server user show'를 선택합니다

   루트 사용자에 대한 액세스 키가 있는지 확인합니다. 없는 경우 다음을 입력합니다.

   'vserver object-store-server user reenate-keys-vserver svm_name-user_root_'

   키가 이미 있는 경우 키를 다시 생성하지 마십시오.

2. 소스 및 타겟 SVM 모두에 버킷 생성:

   'vserver object-store-server bucket create-vserver svm_name-bucket bucket_name[-size_integer_[KB|MB|GB|TB|PB][-comment_text_][*additional_options*]'

3. 소스 및 타겟 SVM의 기본 버킷 정책에 액세스 규칙을 추가합니다.

   'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-

principal_user_and_group_names_-resource_object_store_resources_[-sid_text_][-index_integer_][-index_integer_

예

```
src_cluster::> vserver object-store-server bucket policy add-statement -bucket test-bucket -effect allow -action GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts -principal --resource test-bucket, test-bucket /*
```

4. 소스 SVM에서 기존 정책이 없고 기본 정책을 사용하지 않으려는 경우 SnapMirror S3 정책을 만듭니다. `snapmirror policy create -vserver` *`svm_name`* `-policy policy_name -type continuous [-rpo` *`integer`*`] [-throttle` *`throttle_type`*`] [-comment` *`text`*`] [`*`additional_options`*`]`

   매개 변수:

   - 유형 `continuous` - SnapMirror S3 관계에 대한 유일한 정책 유형입니다(필수).
   - `-rpo` - 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항).
   - `-throttle` - 처리량/대역폭에 대한 상한을 킬로바이트/초 단위로 지정합니다(선택 사항).

     예

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type continuous -rpo 0 -policy test-policy
     ```

5. 소스 및 타겟 클러스터의 관리 SVM에 CA 서버 인증서 설치:

   a. 소스 클러스터에서 *destination_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_src_admin_svm*-cert-name_dest_server_certificate_'

   b. 대상 클러스터에서 *source_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_dest_admin_svm*-cert-name_src_server_certificate_'

      외부 CA 공급업체에서 서명한 인증서를 사용하는 경우, 소스 및 대상 관리 SVM에 동일한 인증서를 설치합니다.

   에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 소스 SVM에서 SnapMirror S3 관계를 만듭니다.

   '스냅미러 create-source-path_src_svm_name_:/bucket/*bucket_name*-destination -path_dest_peer_svm_name_:/bucket/*bucket_name*,…} [-policy policy_name]'입니다

   생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

예

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy
test-policy
```

7. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"
- "스냅미러 쇼"

원격 클러스터에서 기존 **ONTAP S3** 버킷에 대한 미러 관계를 생성합니다

ONTAP 9.10.1 이전 릴리즈에서 S3 구성을 업그레이드한 경우와 같이 언제든지 기존 S3 버킷을 보호할 수 있습니다.

이 작업에 대해

소스 및 대상 클러스터 모두에서 작업을 수행해야 합니다.

시작하기 전에

- ONTAP 버전, 라이센스 및 S3 서버 구성에 대한 요구사항이 완료되었습니다.
- 소스 클러스터와 대상 클러스터 간에 피어링 관계가 있으며, 소스 및 대상 스토리지 VM 간에 피어링 관계가 있습니다.
- 소스 및 대상 VM에 CA 인증서가 필요합니다. 자체 서명된 CA 인증서 또는 외부 CA 공급업체에서 서명한 인증서를 사용할 수 있습니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 미러 관계를 생성할 수 있습니다.

시스템 관리자

1. 이 스토리지 VM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 대상 스토리지 VM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 다시 생성하십시오.
   a. 스토리지 > 스토리지 VM * 을 선택한 다음 스토리지 VM을 선택합니다.
   b. 설정 * 탭에서 * S3 * 타일을 클릭합니다 .
   c. 사용자 * 탭에서 루트 사용자에 대한 액세스 키가 있는지 확인합니다.
   d. 없으면 * root * 옆에 있는 을 클릭한 다음 * 키 재생성 * 을 클릭합니다 키가 이미 있는 경우 키를 다시 생성하지 마십시오.
2. 기존 사용자 및 그룹이 존재하고 소스 및 대상 스토리지 VM 모두에서 올바른 액세스 권한이 있는지 확인합니다. * 스토리지 > 스토리지 VM을 선택한 다음 * 설정 * 탭을 선택합니다. 마지막으로 * S3 * 타일을 찾아 를 선택하고 * 사용자 * 탭을 선택한 다음 * 그룹 * 탭을 선택하여 사용자 및 그룹 액세스 설정을 확인합니다.

   을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.
3. 소스 클러스터에서 기존 SnapMirror S3 정책이 없고 기본 정책을 사용하지 않으려는 경우 새 정책을 만듭니다.
   a. 보호 > 개요 * 를 선택한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. 보호 정책 * 옆에 있는 을 선택한 다음 * 추가 * 를 클릭합니다.
   c. 정책 이름과 설명을 입력합니다.
   d. 클러스터 또는 SVM에서 정책 범위를 선택합니다.
   e. SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
   f. 스로틀 * 및 * 복구 지점 목표 * 값을 입력합니다.
4. 기존 버킷의 버킷 접근 정책이 여전히 요구 사항을 충족하는지 확인합니다.
   a. 스토리지 > 버킷 * 을 클릭한 다음 보호할 버킷을 선택합니다.
   b. 사용 권한 * 탭에서 * 편집 * 을 클릭한 다음 * 사용 권한 * 아래에서 * 추가 * 를 클릭합니다.
      - * Principal and Effect *: 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
      - * 조치 *: 다음 값이 표시되는지 확인하십시오.

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - * 리소스 *: 기본값(*bucketname, bucketname/* *) 또는 필요한 기타 값을 사용합니다.

        을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.
5. SnapMirror S3 보호로 기존 버킷 보호:
   a. 스토리지 * > * 버킷 * 을 클릭한 다음 보호할 버킷을 선택합니다.
   b. 보호 * 를 클릭하고 다음 값을 입력합니다.

- 목적지
  - * 대상 *: ONTAP 시스템
  - * 클러스터 *: 원격 클러스터를 선택합니다.
  - * 스토리지 VM *: 원격 클러스터에서 스토리지 VM을 선택합니다.
  - * S3 서버 CA 인증서 *: _source_certificate의 내용을 복사하여 붙여 넣습니다.
- 출처
  - * S3 서버 CA 인증서 *: _destination_certificate의 내용을 복사하여 붙여 넣습니다.

6. 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우 * 대상에서 동일한 인증서 사용 * 을 선택합니다.
7. Destination Settings * 를 클릭하면 버킷 이름, 용량 및 성능 서비스 레벨의 기본값 대신 사용자 정의 값을 입력할 수도 있습니다.
8. 저장 * 을 클릭합니다. 기존 버킷은 대상 스토리지 VM의 새 버킷으로 미러링됩니다.

잠긴 버킷을 백업합니다

ONTAP 9.14.1부터는 잠긴 S3 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

새 버킷이나 기존 버킷에 대한 보호 설정을 정의할 때 소스 및 타겟 클러스터가 ONTAP 9.14.1 이상을 실행하고 소스 버킷에서 오브젝트 잠금이 설정된 경우 대상 버킷에서 오브젝트 잠금을 설정할 수 있다. 소스 버킷의 객체 잠금 모드 및 잠금 보존 기간이 대상 버킷의 복제된 객체에 적용됩니다. 또한 * Destination Settings * 섹션에서 대상 버킷에 대해 다른 잠금 보존 기간을 정의할 수 있습니다. 이 보존 기간은 소스 버킷 및 S3 인터페이스에서 복제되는 잠기지 않은 오브젝트에도 적용됩니다.

버킷에서 오브젝트 잠금을 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 "버킷을 만듭니다".

CLI를 참조하십시오

1. 이 SVM에 대한 첫 번째 SnapMirror S3 관계인 경우, 소스 및 타겟 SVM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우
   `vserver object-store-server user show` 루트 사용자 키를 다시 생성하십시오. + 루트 사용자에 대한 액세스 키가 있는지 확인하십시오. 이 없으면 다음을 입력합니다
   `vserver object-store-server user regenerate-keys -vserver` *`svm_name`* `-user` *`root`*. + 키가 이미 있는 경우 키를 다시 생성하지 마십시오.
2. 대상 SVM에서 미러 타겟으로 사용할 버킷을 생성합니다.

   'vserver object-store-server bucket create-vserver_svm_name_-bucket_dest_bucket_name_[-size_integer_[KB|MB|GB|TB|PB][-comment_text_][*additional_options*]'

3. 기본 버킷 정책의 액세스 규칙이 소스 및 타겟 SVM에서 모두 올바른지 확인합니다.

   'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_object_store_resources_[-sid_text_][-index_integer_][-index_integer_

예

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 소스 SVM에서 기존 정책이 없고 기본 정책을 사용하지 않으려는 경우 SnapMirror S3 정책을 만듭니다.

   '스냅샷 정책 생성 - vserver svm_name - policy policy_name - type continuous [-RPO_integer_] [-throttle_throttle_type_] [-comment_text_] [*additional_options*]'

   매개 변수:

   - `continuous` – SnapMirror S3 관계에 대한 유일한 정책 유형(필수).
   - '-RPO' – 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항).
   - '-throttle' – 처리량/대역폭의 상한값을 킬로바이트/초 단위로 지정합니다(선택 사항).

     예

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. 소스 및 타겟 클러스터의 관리 SVM에 CA 인증서 설치:

   a. 소스 클러스터에서 *destination_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_src_admin_svm*-cert-name_dest_server_certificate_'

   b. 대상 클러스터에서 *SOURCE_S3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_dest_admin_svm*-cert-name_src_server_certificate_'+ 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우 소스 및 대상 SVM 관리자에 동일한 인증서를 설치합니다.

      에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 소스 SVM에서 SnapMirror S3 관계를 만듭니다.

   '스냅미러 create-source-path_src_svm_name_:/bucket/*bucket_name*-destination-path dest_peer_svm_name:/bucket/*bucket_name*,…} [-policy policy_name]'입니다

   생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

   예

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/test-
   bucket -destination-path vs1:/bucket/test-bucket-mirror -policy
   test-policy
   ```

7. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"
- "스냅미러 쇼"

원격 클러스터의 대상 **ONTAP S3** 버킷에서 테이크오버합니다

소스 버킷의 데이터를 사용할 수 없는 경우 SnapMirror 관계를 중단하여 대상 버킷에 대한 쓰기 가능 및 데이터 제공을 시작할 수 있습니다.

이 작업에 대해

테이크오버 작업이 수행되면 소스 버킷이 읽기 전용으로 전환되고 원래 타겟 버킷은 읽기-쓰기로 변환되어 SnapMirror S3 관계를 반대로 전환합니다.

비활성화된 소스 버킷을 다시 사용할 수 있게 되면 SnapMirror S3는 두 버킷의 컨텐츠를 자동으로 다시 동기화합니다. 볼륨 SnapMirror 구축에 필요한 것처럼 관계를 명시적으로 재동기화할 필요는 없습니다.

테이크오버 작업은 원격 클러스터에서 시작되어야 합니다.

SnapMirror S3는 소스 버킷에서 타겟 버킷으로 오브젝트를 복제하지만 소스 오브젝트 저장소의 사용자, 그룹 및 정책을 타겟 오브젝트 저장소로 복제하지 않습니다.

페일오버 이벤트 중에 클라이언트가 대상 버킷에 액세스할 수 있도록 대상 오브젝트 저장소에서 사용자, 그룹 정책, 권한 및 유사한 구성 요소를 구성해야 합니다.

대상 클러스터에서 사용자가 생성될 때 소스 키를 수동으로 제공하는 경우 소스 및 대상 사용자가 동일한 액세스 및 암호 키를 사용할 수 있습니다. 예를 들면 다음과 같습니다.

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

시스템 관리자

사용할 수 없는 버킷에서 페일오버 및 데이터 서비스 시작:

1. 보호 > 관계 * 를 클릭한 다음 * SnapMirror S3 * 를 선택합니다.
2. 을 클릭하고 * 페일오버 * 를 선택한 다음 * 페일오버 * 를 클릭합니다.

CLI를 참조하십시오

1. '스냅미러 페일오버 시작-목적지-PATH_svm_name_:/bucket/*bucket_name*' 대상 버킷에 대한 페일오버 작업을 시작합니다
2. 페일오버 작업의 상태 '스냅샷 표시 - 필드 상태'를 확인합니다

   예

```
dest_cluster::> snapmirror failover start -destination-path
dest_svm1:/bucket/test-bucket-mirror
```

관련 정보

- "S3 사용자 및 그룹 추가(System Manager)"
- "S3 사용자 생성(CLI)"
- "S3 그룹 생성 또는 수정(CLI)"
- "스냅미러 페일오버 시작"
- "스냅미러 쇼"

원격 클러스터의 타겟 **SVM**에서 **ONTAP S3** 버킷을 복원합니다

소스 버킷의 데이터가 손실되거나 손상된 경우 대상 버킷에서 오브젝트를 복원하여 데이터를 다시 채울 수 있습니다.

이 작업에 대해

대상 버킷을 기존 버킷 또는 새 버킷으로 복원할 수 있습니다. 복구 작업의 타겟 버킷은 대상 버킷의 논리적 사용된 공간보다 커야 합니다.

기존 버킷을 사용하는 경우 복원 작업을 시작할 때 비어 있어야 합니다. 복구는 시간 내에 버킷을 "롤백"하지 않고 빈 버킷을 이전 컨텐츠로 채웁니다.

복구 작업은 원격 클러스터에서 시작해야 합니다.

시스템 관리자

백업된 데이터 복원:

1. 보호 > 관계 * 를 클릭한 다음 * SnapMirror S3 * 를 선택합니다.
2. 을 ⋮ 클릭한 다음 * 복원 * 을 선택합니다.
3. 소스 * 에서 * 기존 버킷 * (기본값) 또는 * 새 버킷 * 을 선택합니다.
   - 기존 버킷 * (기본값)으로 복원하려면 다음 작업을 완료하십시오.
     - 기존 버킷을 검색할 클러스터와 스토리지 VM을 선택합니다.
     - 기존 버킷을 선택합니다.
     - destination_s3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
   - 새 버킷 * 으로 복원하려면 다음 값을 입력합니다.
     - 새로운 버킷을 호스팅할 클러스터 및 스토리지 VM
     - 새로운 버킷의 이름, 용량 및 성능 서비스 수준.
       을 참조하십시오 "스토리지 서비스 레벨" 를 참조하십시오.
     - destination_s3 서버 CA 인증서의 내용.
4. 대상 * 에서 _source_S3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
5. 보호 > 관계 * 를 클릭하여 복구 진행률을 모니터링합니다.

잠긴 버킷을 복원합니다

ONTAP 9.14.1부터 잠긴 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

오브젝트 잠김 버킷은 새 버킷이나 기존 버킷으로 복원할 수 있습니다. 다음과 같은 시나리오에서 오브젝트 잠금 버킷을 대상으로 선택할 수 있습니다.

- * 새 버킷으로 복원 * : 오브젝트 잠금이 활성화된 경우, 버킷을 생성하여 오브젝트 잠금이 활성화된 버킷을 복원할 수 있습니다. 잠긴 버킷을 복원하면 원래 버킷의 오브젝트 잠금 모드와 보존 기간이 복제됩니다. 새 버킷에 대해 다른 잠금 보존 기간을 정의할 수도 있습니다. 이 보존 기간은 다른 소스의 잠기지 않은 개체에 적용됩니다.
- * 기존 버킷으로 복원 *: 기존 버킷에서 버전 관리 및 유사한 오브젝트 잠금 모드가 활성화되어 있는 한 오브젝트 잠금 버킷을 기존 버킷으로 복원할 수 있습니다. 원래 버킷의 보존 기간이 유지됩니다.
- * 비잠금 버킷 복원 * : 버킷에서 오브젝트 잠금이 활성화되지 않은 경우에도 오브젝트 잠금이 활성화되어 있고 소스 클러스터에 있는 버킷으로 복원할 수 있습니다. 버킷을 복원하면 잠기지 않은 모든 객체가 잠기며 대상 버킷의 보존 모드 및 기간을 적용할 수 있습니다.

CLI를 참조하십시오

1. 복원할 새 대상 버킷을 생성합니다. 자세한 내용은 을 "새 ONTAP S3 버킷에 대한 클라우드 백업 관계를 생성한다"참조하십시오.
2. 대상 버킷에 대한 복원 작업을 시작합니다. '스냅미러 복구 - 소스 - path_svm_name_:/bucket/*bucket_name* - destination-path_svm_name_:/bucket/*bucket_name*'

예

```
dest_cluster::> snapmirror restore -source-path
src_vs1:/bucket/test-bucket -destination-path dest_vs1:/bucket/test-
bucket-mirror
```

에 대한 자세한 내용은 `snapmirror restore` "ONTAP 명령 참조입니다"을 참조하십시오.

로컬 클러스터의 미러링 및 백업 보호

로컬 클러스터에서 새로운 **ONTAP S3** 버킷에 대한 미러 관계를 생성합니다

새로운 S3 버킷을 생성하면 동일한 클러스터의 SnapMirror S3 대상으로 즉시 보호할 수 있습니다. 다른 스토리지 VM의 버킷이나 소스와 동일한 스토리지 VM의 버킷에 데이터를 미러링할 수 있습니다.

시작하기 전에

- ONTAP 버전, 라이센스 및 S3 서버 구성에 대한 요구사항이 완료되었습니다.
- 소스 및 대상 스토리지 VM 사이에 피어링 관계가 있습니다.
- 소스 및 대상 VM에 CA 인증서가 필요합니다. 자체 서명된 CA 인증서 또는 외부 CA 공급업체에서 서명한 인증서를 사용할 수 있습니다.

시스템 관리자

1. 이 스토리지 VM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 대상 스토리지 VM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 다시 생성하십시오.
   a. 스토리지 > 스토리지 VM * 을 클릭한 다음 스토리지 VM을 선택합니다.
   b. 설정 * 탭에서 S3 타일을 클릭합니다 .
   c. 사용자 * 탭에서 루트 사용자에 대한 액세스 키가 있는지 확인합니다
   d. 없으면 * root * 옆에 있는 을 클릭한 다음 * 키 재생성 * 을 클릭합니다. 키가 이미 있는 경우 키를 다시 생성하지 마십시오.
2. 스토리지 VM을 편집하여 사용자를 추가하고 사용자를 그룹에 추가하려면 * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 클릭한 다음 * 설정 * 을 클릭하고 S3 아래를 클릭합니다.

   을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.
3. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
   a. 보호 > 개요 * 를 클릭한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. 보호 정책 * 옆에 있는 * 추가 * 를 클릭합니다.
      - 정책 이름과 설명을 입력합니다.
      - 정책 범위, 클러스터 또는 SVM을 선택합니다
      - SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
      - 스로틀 * 및 * 복구 지점 목표 * 값을 입력합니다.
4. SnapMirror 보호를 통해 버킷 생성:
   a. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력한 다음 * 추가 옵션 * 을 클릭합니다.
   c. 사용 권한 * 에서 * 추가 * 를 클릭합니다. 사용 권한 확인은 선택 사항이지만 사용하는 것이 좋습니다.
      - * Principal * 및 * Effect * - 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
      - * 조치 * - 다음 값이 표시되는지 확인합니다.

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - * 리소스 * - 기본값 '(버켓 이름, 버켓 이름/ *)' 또는 필요한 기타 값을 사용합니다

        을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.
   d. 보호 * 에서 * SnapMirror(ONTAP 또는 클라우드) 활성화 * 를 선택합니다. 그런 다음 다음 다음 값을 입력합니다.
      - 목적지

        - * 대상 *: ONTAP 시스템
        - * 클러스터 *: 로컬 클러스터를 선택합니다.
        - * 스토리지 VM *: 로컬 클러스터에서 스토리지 VM을 선택합니다.
        - * S3 서버 CA 인증서 *: 소스 인증서의 내용을 복사하여 붙여 넣습니다.
    - 출처
        - * S3 서버 CA 인증서 *: 대상 인증서의 내용을 복사하여 붙여 넣습니다.
5. 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우 * 대상에서 동일한 인증서 사용 * 을 선택합니다.
6. Destination Settings * 를 클릭하면 버킷 이름, 용량 및 성능 서비스 레벨의 기본값 대신 사용자 정의 값을 입력할 수도 있습니다.
7. 저장 * 을 클릭합니다. 소스 스토리지 VM에 새 버킷이 생성되면 대상 스토리지 VM을 생성한 새 버킷에 미러링됩니다.

잠긴 버킷을 백업합니다

ONTAP 9.14.1부터는 잠긴 S3 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

새 버킷이나 기존 버킷에 대한 보호 설정을 정의할 때 소스 및 타겟 클러스터가 ONTAP 9.14.1 이상을 실행하고 소스 버킷에서 오브젝트 잠금이 설정된 경우 대상 버킷에서 오브젝트 잠금을 설정할 수 있다. 소스 버킷의 객체 잠금 모드 및 잠금 보존 기간이 대상 버킷의 복제된 객체에 적용됩니다. 또한 * Destination Settings * 섹션에서 대상 버킷에 대해 다른 잠금 보존 기간을 정의할 수 있습니다. 이 보존 기간은 소스 버킷 및 S3 인터페이스에서 복제되는 잠기지 않은 오브젝트에도 적용됩니다.

버킷에서 오브젝트 잠금을 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 "버킷을 만듭니다".

CLI를 참조하십시오

1. 이 SVM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 타겟 SVM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 재생성
   `vserver object-store-server user show`

   루트 사용자에 대한 액세스 키가 있는지 확인합니다. 없는 경우 'vserver object-store-server user reenate-keys-vserver_svm_name_-user_root_'를 입력합니다

   키가 이미 있는 경우 키를 다시 생성하지 마십시오.

2. 소스 및 타겟 SVM 모두에 버킷 생성:

   'vserver object-store-server bucket create-vserver svm_name-bucket bucket_name[-size_integer_[KB|MB|GB|TB|PB][-comment_text_][*additional_options*]'

3. 소스 및 타겟 SVM의 기본 버킷 정책에 액세스 규칙을 추가합니다.

   'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_object_store_resources_[-sid_text_][-index_integer_][-index_integer_

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   매개 변수:

   - `continuous` – SnapMirror S3 관계에 대한 유일한 정책 유형(필수).
   - '-RPO' – 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항).
   - '-throttle' – 처리량/대역폭의 상한값을 킬로바이트/초 단위로 지정합니다(선택 사항).

   예

   ```
   src_cluster::> snapmirror policy create -vserver vs0 -type
   continuous -rpo 0 -policy test-policy
   ```

5. 관리 SVM에 CA 서버 인증서 설치:
   a. 관리 SVM에 *source_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_admin_svm*-cert-name_src_server_certificate_'
   b. 관리 SVM에 *destination_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_admin_svm*-cert-name_dest_server_certificate_'+ 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우에는 관리 SVM에 이 인증서를 설치해야 합니다.

      에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

6. SnapMirror S3 관계 생성:
`snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
   bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror
   -policy test-policy
   ```

7. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"
- "스냅미러 쇼"

로컬 클러스터에서 기존 **ONTAP S3** 버킷에 대한 미러 관계를 생성합니다

ONTAP 9.10.1 이전 릴리즈에서 S3 구성을 업그레이드한 경우와 같이 언제든지 동일한 클러스터에서 기존 S3 버킷을 보호할 수 있습니다. 다른 스토리지 VM의 버킷이나 소스와 동일한 스토리지 VM의 버킷에 데이터를 미러링할 수 있습니다.

시작하기 전에

- ONTAP 버전, 라이센스 및 S3 서버 구성에 대한 요구사항이 완료되었습니다.
- 소스 및 대상 스토리지 VM 사이에 피어링 관계가 있습니다.
- 소스 및 대상 VM에 CA 인증서가 필요합니다. 자체 서명된 CA 인증서 또는 외부 CA 공급업체에서 서명한 인증서를 사용할 수 있습니다.

시스템 관리자

1. 이 스토리지 VM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 대상 스토리지 VM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 다시 생성하십시오.
   a. 스토리지 > 스토리지 VM * 을 클릭한 다음 스토리지 VM을 선택합니다.
   b. 설정 * 탭에서 * S3 * 타일을 클릭합니다 .
   c. 사용자 * 탭에서 루트 사용자에 대한 액세스 키가 있는지 확인합니다.
   d. 없으면 * root * 옆에 있는 을 클릭한 다음 * 키 재생성 * 을 클릭합니다. 키가 이미 있는 경우 키를 다시 생성하지 마십시오
2. 기존 사용자 및 그룹이 존재하고 소스 및 대상 스토리지 VM 모두에서 올바른 액세스 권한이 있는지 확인합니다. * 스토리지 > 스토리지 VM을 선택하고 * 스토리지 VM을 선택한 다음 * 설정 * 탭을 선택합니다. 마지막으로 * S3 * 타일을 찾아 를 선택하고 * 사용자 * 탭을 선택한 다음 * 그룹 * 탭을 선택하여 사용자 및 그룹 액세스 설정을 확인합니다.

   을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.
3. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
   a. 보호 > 개요 * 를 클릭한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. 보호 정책 * 옆에 있는 * 추가 * 를 클릭합니다.
      - 정책 이름과 설명을 입력합니다.
      - 정책 범위, 클러스터 또는 SVM을 선택합니다
      - SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
      - 스로틀 * 및 * 복구 지점 목표 * 값을 입력합니다.
4. 기존 버킷의 버킷 접근 정책이 고객의 요구를 지속적으로 충족하는지 확인합니다.
   a. 스토리지 > 버킷 * 을 클릭한 다음 보호할 버킷을 선택합니다.
   b. 사용 권한 * 탭에서 * 편집 * 을 클릭한 다음 * 사용 권한 * 아래에서 * 추가 * 를 클릭합니다.
      - * Principal * 및 * Effect * - 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
      - * 조치 * - 다음 값이 표시되는지 확인합니다.

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - * 리소스 * - 기본값(버켓 이름, 버켓 이름/ *) 또는 필요한 기타 값을 사용합니다.

        을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.
5. SnapMirror S3로 기존 버킷 보호:
   a. 스토리지 * > * 버킷 * 을 클릭한 다음 보호할 버킷을 선택합니다.
   b. 보호 * 를 클릭하고 다음 값을 입력합니다.

- 목적지
  - * 대상 *: ONTAP 시스템
  - * 클러스터 *: 로컬 클러스터를 선택합니다.
  - * 스토리지 VM *: 동일하거나 다른 스토리지 VM을 선택하십시오.
  - * S3 서버 CA 인증서 *: _source_certificate의 내용을 복사하여 붙여 넣습니다.
- 출처
  - * S3 서버 CA 인증서 *: _destination_certificate의 내용을 복사하여 붙여 넣습니다.

6. 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우 * 대상에서 동일한 인증서 사용 * 을 선택합니다.
7. Destination Settings * 를 클릭하면 버킷 이름, 용량 및 성능 서비스 레벨의 기본값 대신 사용자 정의 값을 입력할 수도 있습니다.
8. 저장 * 을 클릭합니다. 기존 버킷은 대상 스토리지 VM의 새 버킷으로 미러링됩니다.

잠긴 버킷을 백업합니다

ONTAP 9.14.1부터는 잠긴 S3 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

새 버킷이나 기존 버킷에 대한 보호 설정을 정의할 때 소스 및 타겟 클러스터가 ONTAP 9.14.1 이상을 실행하고 소스 버킷에서 오브젝트 잠금이 설정된 경우 대상 버킷에서 오브젝트 잠금을 설정할 수 있다. 소스 버킷의 객체 잠금 모드 및 잠금 보존 기간이 대상 버킷의 복제된 객체에 적용됩니다. 또한 * Destination Settings * 섹션에서 대상 버킷에 대해 다른 잠금 보존 기간을 정의할 수 있습니다. 이 보존 기간은 소스 버킷 및 S3 인터페이스에서 복제되는 잠기지 않은 오브젝트에도 적용됩니다.

버킷에서 오브젝트 잠금을 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 "버킷을 만듭니다".

CLI를 참조하십시오

1. 이 SVM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 타겟 SVM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우 재생성
   `vserver object-store-server user show`

   루트 사용자에 대한 액세스 키가 있는지 확인합니다. 없는 경우 'vserver object-store-server user reenate-keys-vserver_svm_name_-user_root_'를 입력합니다

   키가 이미 있는 경우 키를 다시 생성하지 마십시오.

2. 대상 SVM에서 미러 타겟으로 사용할 버킷을 생성합니다.

   'vserver object-store-server bucket create-vserver_svm_name_-bucket_dest_bucket_name_[-size_integer_[KB|MB|GB|TB|PB][-comment_text_][*additional_options*]'

3. 기본 버킷 정책에 대한 액세스 규칙이 소스 및 타겟 SVM에서 모두 올바른지 확인합니다.

   'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_object_store_resources_[-sid_text_][-index_integer_][-index_integer_

예

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.

   '스냅샷 정책 생성 - vserver_svm_name_-policy_policy_name - type continuous [-RPO_integer_] [-throttle_throttle_type_] [-comment text] [*additional_options*]'

   매개 변수:

   - `continuous` – SnapMirror S3 관계에 대한 유일한 정책 유형(필수).
   - '-RPO' – 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항).
   - '-throttle' – 처리량/대역폭의 상한값을 킬로바이트/초 단위로 지정합니다(선택 사항).

     예

     ```
     clusterA::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. 관리 SVM에 CA 서버 인증서 설치:

   a. 관리 SVM에 *source_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_admin_svm*-cert-name_src_server_certificate_'

   b. 관리 SVM에 *destination_s3* 서버 인증서에 서명한 *CA* 인증서를 설치합니다. '보안 인증서 설치 유형 *server-ca-vserver_admin_svm*-cert-name_dest_server_certificate_'+ 외부 CA 공급업체에서 서명한 인증서를 사용하는 경우에는 관리 SVM에 이 인증서를 설치해야 합니다.

      에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

6. SnapMirror S3 관계 생성:
   `snapmirror create -source-path` *`src_svm_name`*`:/bucket/`*`bucket_name`* `-destination-path` *`dest_peer_svm_name`*`:/bucket/`*`bucket_name`*`, …} [-policy policy_name]`

   생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

   예

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
   bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy
   test-policy
   ```

7. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"
- "스냅미러 쇼"

로컬 클러스터의 타겟 **ONTAP S3** 버킷에서 테이크오버합니다

소스 버킷의 데이터를 사용할 수 없는 경우 SnapMirror 관계를 중단하여 대상 버킷에 대한 쓰기 가능 및 데이터 제공을 시작할 수 있습니다.

이 작업에 대해

테이크오버 작업이 수행되면 소스 버킷이 읽기 전용으로 전환되고 원래 타겟 버킷은 읽기-쓰기로 변환되어 SnapMirror S3 관계를 반대로 전환합니다.

비활성화된 소스 버킷을 다시 사용할 수 있게 되면 SnapMirror S3는 두 버킷의 컨텐츠를 자동으로 다시 동기화합니다. 표준 볼륨 SnapMirror 배포에 필요하므로 관계를 명시적으로 다시 동기화할 필요는 없습니다.

대상 버킷이 원격 클러스터에 있는 경우 원격 클러스터에서 테이크오버 작업을 시작해야 합니다.

시스템 관리자

사용할 수 없는 버킷에서 페일오버 및 데이터 서비스 시작:

1. 보호 > 관계 * 를 클릭한 다음 * SnapMirror S3 * 를 선택합니다.
2. 을 클릭하고 * 페일오버 * 를 선택한 다음 * 페일오버 * 를 클릭합니다.

CLI를 참조하십시오

1. '스냅미러 페일오버 시작-목적지-PATH_svm_name_:/bucket/*bucket_name*' 대상 버킷에 대한 페일오버 작업을 시작합니다
2. 페일오버 작업의 상태 '스냅샷 표시 - 필드 상태'를 확인합니다

예

'clusterA:::> SnapMirror 페일오버 start-destination-path vs1:/bucket/test-bucket-mirror'

관련 정보

- "스냅미러 페일오버 시작"
- "스냅미러 쇼"

로컬 클러스터의 타겟 **SVM**에서 **ONTAP S3** 버킷을 복원합니다

소스 버킷의 데이터가 손실되거나 손상된 경우 대상 버킷에서 오브젝트를 복원하여 데이터를 다시 채울 수 있습니다.

이 작업에 대해

대상 버킷을 기존 버킷 또는 새 버킷으로 복원할 수 있습니다. 복구 작업의 타겟 버킷은 대상 버킷의 논리적 사용된 공간보다 커야 합니다.

기존 버킷을 사용하는 경우 복원 작업을 시작할 때 비어 있어야 합니다. 복구는 시간 내에 버킷을 "롤백"하지 않고 빈 버킷을 이전 컨텐츠로 채웁니다.

복구 작업은 로컬 클러스터에서 시작해야 합니다.

시스템 관리자

백업 데이터 복원:

1. 보호 > 관계 * 를 클릭한 다음 버킷을 선택합니다.
2. 을 ⋮ 클릭한 다음 * 복원 * 을 선택합니다.
3. 소스 * 에서 * 기존 버킷 * (기본값) 또는 * 새 버킷 * 을 선택합니다.
   - 기존 버킷 * (기본값)으로 복원하려면 다음 작업을 완료하십시오.
     - 기존 버킷을 검색할 클러스터와 스토리지 VM을 선택합니다.
     - 기존 버킷을 선택합니다.
4. 대상 S3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
   - 새 버킷 * 으로 복원하려면 다음 값을 입력합니다.
     - 새로운 버킷을 호스팅할 클러스터 및 스토리지 VM
     - 새로운 버킷의 이름, 용량 및 성능 서비스 수준.
       을 참조하십시오 "스토리지 서비스 레벨" 를 참조하십시오.
     - 대상 S3 서버 CA 인증서의 내용.
5. 대상 * 에서 소스 S3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
6. 보호 * > 관계 를 클릭하여 복원 진행률을 모니터링합니다.

잠긴 버킷을 복원합니다

ONTAP 9.14.1부터 잠긴 버킷을 백업하고 필요에 따라 복원할 수 있습니다.

오브젝트 잠김 버킷은 새 버킷이나 기존 버킷으로 복원할 수 있습니다. 다음과 같은 시나리오에서 오브젝트 잠금 버킷을 대상으로 선택할 수 있습니다.

- * 새 버킷으로 복원 * : 오브젝트 잠금이 활성화된 경우, 버킷을 생성하여 오브젝트 잠금이 활성화된 버킷을 복원할 수 있습니다. 잠긴 버킷을 복원하면 원래 버킷의 오브젝트 잠금 모드와 보존 기간이 복제됩니다. 새 버킷에 대해 다른 잠금 보존 기간을 정의할 수도 있습니다. 이 보존 기간은 다른 소스의 잠기지 않은 개체에 적용됩니다.
- * 기존 버킷으로 복원 *: 기존 버킷에서 버전 관리 및 유사한 오브젝트 잠금 모드가 활성화되어 있는 한 오브젝트 잠금 버킷을 기존 버킷으로 복원할 수 있습니다. 원래 버킷의 보존 기간이 유지됩니다.
- * 비잠금 버킷 복원 * : 버킷에서 오브젝트 잠금이 활성화되지 않은 경우에도 오브젝트 잠금이 활성화되어 있고 소스 클러스터에 있는 버킷으로 복원할 수 있습니다. 버킷을 복원하면 잠기지 않은 모든 객체가 잠기며 대상 버킷의 보존 모드 및 기간을 적용할 수 있습니다.

CLI를 참조하십시오

1. 오브젝트를 새 버킷으로 복원하는 경우 새 버킷을 생성합니다. 자세한 내용은 을 "새 ONTAP S3 버킷에 대한 클라우드 백업 관계를 생성한다"참조하십시오.
2. 대상 버킷에 대한 복원 작업을 시작합니다. '스냅미러 복구 - 소스 - path_svm_name_:/bucket/*bucket_name* - destination-path_svm_name_:/bucket/*bucket_name*'

예

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket
-destination-path vs1:/bucket/test-bucket-mirror
```

에 대한 자세한 내용은 `snapmirror restore` "ONTAP 명령 참조입니다"을 참조하십시오.

클라우드 타겟을 통한 백업 보호

ONTAP SnapMirror S3 클라우드 타겟 관계 요구사항

소스 및 타겟 환경이 클라우드 타겟에 대한 SnapMirror S3 백업 보호 요구사항을 충족하는지 확인하십시오.

데이터 버킷에 액세스하려면 오브젝트 저장소 공급자의 유효한 계정 자격 증명이 있어야 합니다.

클러스터를 클라우드 오브젝트 저장소에 연결하려면 먼저 클러스터에서 인터클러스터 LIF 및 IPspace를 구성해야 합니다. 로컬 스토리지의 데이터를 클라우드 오브젝트 저장소로 원활하게 전송하려면 각 노드에 대한 인터클러스터 LIF를 생성해야 합니다.

StorageGRID 대상의 경우 다음 정보를 알아야 합니다.

- FQDN(정규화된 도메인 이름) 또는 IP 주소로 표시되는 서버 이름입니다
- 버킷 이름. 버킷이 이미 있어야 합니다
- 액세스 키
- 비밀 키

또한 StorageGRID 서버 인증서에 서명하는 데 사용되는 CA 인증서는 ONTAP S3 클러스터의 관리 스토리지 VM에 다음을 사용하여 설치해야 합니다. `security certificate install` 명령. 자세한 내용은 "CA 인증서를 설치하는 중입니다"StorageGRID 사용 여부 를 참조하십시오.

AWS S3 타겟의 경우 다음 정보를 알아야 합니다.

- FQDN(정규화된 도메인 이름) 또는 IP 주소로 표시되는 서버 이름입니다
- 버킷 이름. 버킷이 이미 있어야 합니다
- 액세스 키
- 비밀 키

ONTAP 클러스터의 관리 스토리지 VM용 DNS 서버는 FQDN(사용되는 경우)을 IP 주소로 확인할 수 있어야 합니다.

관련 정보

- "보안 인증서 설치"

새 **ONTAP S3** 버킷에 대한 클라우드 백업 관계를 생성한다

새로운 S3 버킷을 생성하면 객체 저장소 공급자(StorageGRID 시스템 또는 Amazon S3 배포)의 SnapMirror S3 대상 버킷에 즉시 백업할 수 있습니다.

시작하기 전에

- 객체 저장소 공급자에 대한 유효한 계정 자격 증명 및 구성 정보가 있습니다.
- 소스 시스템에 인터클러스터 네트워크 인터페이스 및 IPspace가 구성되었습니다.
- • 소스 스토리지 VM의 DNS 구성은 타겟의 FQDN을 확인할 수 있어야 합니다.

시스템 관리자

1. 스토리지 VM을 편집하여 사용자를 추가하고 사용자를 그룹에 추가합니다.
   a. 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM, * 설정 * 을 차례로 클릭한 다음 * S3 * 아래를 클릭합니다 .

      을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.

2. 소스 시스템에 Cloud Object Store 추가:
   a. 보호 > 개요 * 를 클릭한 다음 * 클라우드 오브젝트 저장소 * 를 선택합니다.
   b. 추가 * 를 클릭한 다음 * Amazon S3 * 또는 * StorageGRID * 를 선택합니다.
   c. 다음 값을 입력합니다.
      - 클라우드 오브젝트 저장소 이름
      - URL 스타일(경로 또는 가상 호스팅)
      - 스토리지 VM(S3에 대해 활성화됨)
      - 개체 저장소 서버 이름(FQDN)
      - 오브젝트 저장소 인증서
      - 액세스 키
      - 비밀 키
      - 컨테이너(버킷) 이름입니다
3. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
   a. 보호 > 개요 * 를 클릭한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. →보호 정책 * 옆에 있는 * 추가 * 를 클릭합니다.
      - 정책 이름과 설명을 입력합니다.
      - 정책 범위, 클러스터 또는 SVM을 선택합니다
      - SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
      - 스로틀 * 및 * 복구 지점 목표 * 값을 입력합니다.
4. SnapMirror 보호를 통해 버킷 생성:
   a. 스토리지 > 버킷 * 을 클릭한 다음 * 추가 * 를 클릭합니다.
   b. 이름을 입력하고 스토리지 VM을 선택한 다음 크기를 입력한 다음 * 추가 옵션 * 을 클릭합니다.
   c. 사용 권한 * 에서 * 추가 * 를 클릭합니다. 사용 권한 확인은 선택 사항이지만 사용하는 것이 좋습니다.
      - * Principal * and * Effect *: 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 적용합니다.
      - * 조치 *: 다음 값이 표시되는지 확인하십시오.

```
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
```

- * 리소스 : 필요한 기본값 **_(bucketname, bucketname/)** 또는 기타 값을 사용합니다.

  을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.

d. 보호 * 에서 * SnapMirror(ONTAP 또는 클라우드) * 를 선택하고 * 클라우드 스토리지 * 를 선택한 다음 * 클라우드 오브젝트 저장소 * 를 선택합니다.

Save * 를 클릭하면 소스 스토리지 VM에 새 버킷이 생성되고 클라우드 오브젝트 저장소에 백업됩니다.

CLI를 참조하십시오

1. 이 SVM에 대한 첫 번째 SnapMirror S3 관계인 경우 소스 및 타겟 SVM에 대한 루트 사용자 키가 있는지 확인하고 그렇지 않은 경우
   `vserver object-store-server user show` 루트 사용자 키를 재생성합니다. + 루트 사용자에 대한 액세스 키가 있는지 확인하십시오. 이 없으면 다음을 입력합니다
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`. + 키가 이미 있는 경우 키를 다시 생성하지 마십시오.
2. 소스 SVM에서 버킷을 생성합니다. 'vserver object-store-server bucket create-vserver_svm_name_-bucket_bucket_name_[-size_integer_[KB|MB|GB|TB|PB][-comment_text_][*additional_options*]'
3. 기본 버킷 정책에 액세스 규칙을 추가합니다. 'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_store_resources_[-sid_text_][-index_integer_integer

   예

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   매개 변수: * `type continuous` – SnapMirror S3 관계에 대한 유일한 정책 유형(필수). * `-rpo` – 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항). `-throttle`* – 처리량/대역폭에 대한 상한을 킬로바이트/초 단위로 지정합니다(선택 사항).

   예

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

5. 타겟이 StorageGRID 시스템인 경우 소스 클러스터의 관리 SVM에 StorageGRID CA 서버 인증서를 설치합니다. '보안 인증서 설치 유형 server-ca-vserver_src_admin_svm_-cert-name_storage_grid_server_certificate_'

에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

6. SnapMirror S3 대상 오브젝트 저장소 정의:
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

   매개 변수: * `-object-store-name` – 로컬 ONTAP 시스템에 있는 개체 저장소 대상의 이름입니다. `-usage*` – `data` 이 워크플로에 사용합니다. * `-provider-type` – `AWS_S3` 및 `SGWS` (StorageGRID) 타겟이 지원됩니다. `-server*` – 대상 서버의 FQDN 또는 IP 주소입니다. `-is-ssl-enabled*` – SSL 활성화는 선택 사항이지만 권장됩니다. + 에서 에 대해 자세히 `snapmirror object-store config create` "ONTAP 명령 참조입니다"알아보십시오.

   예

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

7. SnapMirror S3 관계 생성:
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

   매개 변수:
   * `-destination-path` - 이전 단계에서 만든 개체 저장소 이름과 고정 값입니다 `objstore`.
   를 누릅니다
   생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

   예

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"
- "스냅미러 쇼"

기존 **ONTAP S3** 버킷에 대한 클라우드 백업 관계를 생성한다

ONTAP 9.10.1 이전 릴리즈에서 S3 구성을 업그레이드한 경우와 같이 언제든지 기존 S3 버킷 백업을 시작할 수 있습니다.

시작하기 전에

- 객체 저장소 공급자에 대한 유효한 계정 자격 증명 및 구성 정보가 있습니다.
- 소스 시스템에 인터클러스터 네트워크 인터페이스 및 IPspace가 구성되었습니다.
- 소스 스토리지 VM의 DNS 구성은 타겟의 FQDN을 확인할 수 있어야 합니다.

시스템 관리자

1. 사용자 및 그룹이 올바르게 정의되었는지 확인합니다. * 스토리지 > 스토리지 VM * 을 클릭하고 스토리지 VM을 클릭한 다음 * 설정 * 을 클릭하고 S3를 클릭합니다 .

   을 참조하십시오 "S3 사용자 및 그룹 추가" 를 참조하십시오.

2. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
   a. 보호 > 개요 * 를 클릭한 다음 * 로컬 정책 설정 * 을 클릭합니다.
   b. →보호 정책 * 옆에 있는 * 추가 * 를 클릭합니다.
   c. 정책 이름과 설명을 입력합니다.
   d. 정책 범위, 클러스터 또는 SVM을 선택합니다
   e. SnapMirror S3 관계에 대해 * 지속적 * 을 선택합니다.
   f. 스로틀 * 및 * 복구 지점 목표 값 * 을 입력합니다.
3. 소스 시스템에 Cloud Object Store 추가:
   a. 보호 > 개요 * 를 클릭한 다음 * 클라우드 오브젝트 저장소 * 를 선택합니다.
   b. 추가 * 를 클릭한 다음, StorageGRID Webscale * 용 * Amazon S3 * 또는 * 기타 * 를 선택합니다.
   c. 다음 값을 입력합니다.
      - 클라우드 오브젝트 저장소 이름
      - URL 스타일(경로 또는 가상 호스팅)
      - 스토리지 VM(S3에 대해 활성화됨)
      - 개체 저장소 서버 이름(FQDN)
      - 오브젝트 저장소 인증서
      - 액세스 키
      - 비밀 키
      - 컨테이너(버킷) 이름입니다
4. 기존 버킷의 버킷 접근 정책이 여전히 요구 사항을 충족하는지 확인합니다.
   a. 스토리지 * > * 버킷 * 을 클릭한 다음 보호할 버킷을 선택합니다.
   b. 사용 권한 * 탭에서 * 편집 * 을 클릭한 다음 * 사용 권한 * 아래에서 * 추가 * 를 클릭합니다.
      - * Principal * 및 * Effect * - 사용자 그룹 설정에 해당하는 값을 선택하거나 기본값을 그대로 사용합니다.
      - * Actions * - GetObject, PutObject, DeleteObject, ListBucket, GetBuckketAcl, GetObjectAcl, ListBuckketMultipartUploads, ListMultiPartUploadParts 등의 값이 표시되는지 확인합니다
      - * 리소스 * - 기본값(*(버켓 이름, 버켓 이름/ *)* 또는 필요한 기타 값을 사용합니다.

        을 참조하십시오 "버킷에 대한 사용자 액세스를 관리합니다" 이 필드에 대한 자세한 내용은 를 참조하십시오.
5. SnapMirror S3를 사용하여 버킷 백업:

a. 스토리지 * > * 버킷 * 을 클릭한 다음 백업할 버킷을 선택합니다.

b. 보호 * 를 클릭하고 * 대상 * 에서 * 클라우드 스토리지 * 를 선택한 다음 * 클라우드 오브젝트 저장소 * 를 선택합니다.

Save * 를 클릭하면 기존 버킷이 클라우드 오브젝트 저장소로 백업됩니다.

CLI를 참조하십시오

1. 기본 버킷 정책의 액세스 규칙이 올바른지 확인합니다. 'vserver object-store-server bucket policy add-statement-vserver_svm_name_-bucket_bucket_name_-effect{allow|deny}-action_object_store_actions_-principal_user_and_group_names_-resource_store_resources_[-sid_text_integer']

   예

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

2. 기존 정책이 없고 기본 정책을 사용하지 않으려면 SnapMirror S3 정책을 만드세요.
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   매개 변수: * `type continuous` – SnapMirror S3 관계에 대한 유일한 정책 유형(필수). * `-rpo` – 복구 시점 목표의 시간을 초 단위로 지정합니다(선택 사항). `-throttle`* – 처리량/대역폭에 대한 상한을 킬로바이트/초 단위로 지정합니다(선택 사항).

   예

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

3. 타겟이 StorageGRID 시스템인 경우 소스 클러스터의 관리 SVM에 StorageGRID CA 인증서를 설치합니다. '보안 인증서 설치 유형 server-ca-vserver_src_admin_svm_-cert-name_storage_grid_server_certificate_'

   에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

4. SnapMirror S3 대상 오브젝트 저장소 정의:
   `snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

   매개 변수: * `-object-store-name` – 로컬 ONTAP 시스템에 있는 개체 저장소 대상의 이름입니다. `-usage`* – `data` 이 워크플로에 사용합니다. * `-provider-type` – `AWS_S3` 및 `SGWS` (StorageGRID)

타겟이 지원됩니다. `-server`* – 대상 서버의 FQDN 또는 IP 주소입니다. `-is-ssl-enabled`* – SSL 활성화는 선택 사항이지만 권장됩니다. + 에서 에 대해 자세히 `snapmirror object-store config create` "ONTAP 명령 참조입니다"알아보십시오.

예

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

5. SnapMirror S3 관계 생성:
`snapmirror create -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`object_store_name`*`:/objstore -policy` *`policy_name`*

매개 변수:
* `-destination-path` - 이전 단계에서 만든 개체 저장소 이름과 고정 값입니다 `objstore`.
를 누릅니다
생성한 정책을 사용하거나 기본값을 사용할 수 있습니다.

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

6. 미러링이 활성 상태인지 확인합니다. '스냅샷 표시 - 정책 유형 연속 필드 상태'

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"
- "스냅미러 쇼"

클라우드 타겟에서 **ONTAP S3** 버킷 복원

소스 버킷의 데이터가 손실되거나 손상된 경우 대상 버킷에서 복구하여 데이터를 다시 채울 수 있습니다.

이 작업에 대해

대상 버킷을 기존 버킷 또는 새 버킷으로 복원할 수 있습니다. 복구 작업의 타겟 버킷은 대상 버킷의 논리적 사용 공간보다 커야 합니다.

기존 버킷을 사용하는 경우 복원 작업을 시작할 때 비어 있어야 합니다. 복구는 시간 내에 버킷을 "롤백"하지 않고 빈 버킷을 이전 컨텐츠로 채웁니다.

시스템 관리자

백업 데이터 복원:

1. 보호 > 관계 * 를 클릭한 다음 * SnapMirror S3 * 를 선택합니다.
2. 을 ⋮ 클릭한 다음 * 복원 * 을 선택합니다.
3. 소스 * 에서 * 기존 버킷 * (기본값) 또는 * 새 버킷 * 을 선택합니다.
   - 기존 버킷 * (기본값)으로 복원하려면 다음 작업을 완료하십시오.
     - 기존 버킷을 검색할 클러스터와 스토리지 VM을 선택합니다.
     - 기존 버킷을 선택합니다.
     - destination_s3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
   - 새 버킷 * 으로 복원하려면 다음 값을 입력합니다.
     - 새로운 버킷을 호스팅할 클러스터 및 스토리지 VM
     - 새로운 버킷의 이름, 용량 및 성능 서비스 수준. 을 참조하십시오 "스토리지 서비스 레벨" 를 참조하십시오.
     - 대상 S3 서버 CA 인증서의 내용.
4. 대상 * 에서 _source_S3 서버 CA 인증서의 내용을 복사하여 붙여 넣습니다.
5. 보호 > 관계 * 를 클릭하여 복구 진행률을 모니터링합니다.

CLI 절차

1. 복원할 새 대상 버킷을 생성합니다. 자세한 내용은 을 참조하십시오 "버킷에 대한 백업 관계 생성(클라우드 타겟)".
2. 대상 버킷에 대한 복구 작업을 시작합니다.
   `snapmirror restore -source-path` *`object_store_name`*`:/objstore -destination -path` *`svm_name`*`:/bucket/`*`bucket_name`*

   예

   다음 예에서는 대상 버킷을 기존 버킷으로 복원합니다.

```
clusterA::> snapmirror restore -source-path sgws.store:/objstore
-destination-path vs0:/bucket/test-bucket
```

   에 대한 자세한 내용은 `snapmirror restore` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror S3 정책을 수정합니다

RPO 및 스로틀 값을 조정하려는 경우 S3 SnapMirror 정책을 수정할 수 있습니다.

시스템 관리자

1. 보호 > 관계 * 를 클릭한 다음 수정할 관계에 대한 보호 정책을 선택합니다.
2. 정책 이름 옆에 있는 을 ⋮ 클릭한 다음 * 편집 * 을 클릭합니다.

CLI를 참조하십시오

SnapMirror S3 정책 수정:

```
snapmirror policy modify -vserver <svm_name> -policy <policy_name> [-rpo
<integer>] [-throttle <throttle_type>] [-comment <text>]
```

매개 변수:

- `-rpo`: 복구 지점 목표의 시간을 초 단위로 지정합니다.
- `-throttle`: 처리량/대역폭에 대한 상한을 킬로바이트/초 단위로 지정합니다.

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

관련 정보

- "스냅미러 정책 수정"

스냅샷으로 **S3** 데이터를 보호합니다

ONTAP S3 스냅샷에 대해 자세히 알아보십시오

ONTAP 9.16.1부터 ONTAP 스냅샷 기술을 사용하여 ONTAP S3 버킷의 읽기 전용 시점 이미지를 생성할 수 있습니다.

S3 스냅샷 기능을 사용하면 스냅샷을 수동으로 생성하거나 스냅샷 정책을 통해 스냅샷을 자동으로 생성할 수 있습니다. S3 스냅샷은 S3 클라이언트에 S3 버킷으로 제공됩니다. S3 클라이언트를 통해 스냅샷에서 콘텐츠를 찾아보고 복원할 수 있습니다.

ONTAP 9.16.1에서 S3 스냅샷은 S3 버킷의 현재 버전만 캡처합니다. 최신 버전이 아닌 버킷을 S3 스냅샷에서 캡처하지 않습니다. 또한 스냅샷 생성 후 객체 태그가 수정되면 시점 객체 태그가 스냅샷에 캡처되지 않습니다.

S3 스냅샷은 클러스터 시간을 기준으로 합니다. 시간을 동기화하려면 클러스터에서 NTP 서버를 구성해야 합니다. 자세한 내용은 을 "클러스터 시간을 관리합니다"참조하십시오.

할당량 및 공간 사용량

할당량은 S3 버킷에 사용되는 오브젝트 수와 논리적 크기를 추적합니다. S3 스냅샷이 생성될 때 스냅샷이 파일 시스템에서 삭제될 때까지 S3 스냅샷에서 캡처된 오브젝트는 사용된 버킷 오브젝트 수 및 크기에 계산됩니다.

다중 파트 개체

멀티 파트 객체의 경우 최종 객체만 스냅샷에 캡처됩니다. 다중 부분 객체의 부분 업로드는 스냅샷에 캡처되지 않습니다.

버전 및 비버전 버킷의 스냅샷

버전 및 비버전 버킷 모두에서 스냅샷을 생성할 수 있습니다. 스냅숏은 스냅숏이 캡처될 때 현재 개체 버전만 포함합니다.

버전 관리된 버킷 및 스냅샷

오브젝트 버전 관리가 활성화된 버킷에서 스냅샷은 스냅샷이 생성된 후 가장 최근의 오브젝트 버전의 콘텐츠를 유지합니다. 버킷에서 비최신 버전은 제외됩니다.

이 예에서는 오브젝트 버전 관리가 활성화된 버킷에서 오브젝트에 `obj1` v1, v2, v3, v4, v5가 있습니다. v3(캡처 시점에 가장 최근 버전)에서 `obj1` 스냅샷을 `snap1` 생성했습니다. 브라우징 시 `snap1` `obj1` v3에 생성된 컨텐츠가 있는 객체로 표시됩니다. 이전 버전의 콘텐츠는 반환되지 않습니다.

> ⓘ 스냅샷이 삭제될 때까지 현재 버전이 아닌 버전은 파일 시스템에 유지됩니다.

비버전 버킷 및 스냅샷

버전이 지정되지 않은 버킷에서 S3 스냅샷은 스냅샷 생성 전에 최신 커밋의 내용을 유지합니다.

다음 예를 들어 개체 버전 관리를 사용할 수 없는 버킷에서 (T1, T2, T3, T4 및 T5)에서 개체를 `obj1` 여러 번 덮어썼습니다. T3와 T4 사이에 S3 스냅샷을 `snap1` 생성했습니다. 브라우징 시 `snap1` `obj1` T3에서 생성된 컨텐츠와 함께 가 나타납니다.

개체 만료 및 스냅샷

ONTAP S3 오브젝트 만료 및 S3 스냅샷 기능은 서로 독립적으로 작동합니다. ONTAP 오브젝트 만료 기능은 S3 버킷에 정의된 라이프사이클 관리 규칙에 따라 오브젝트 버전을 만료한다. S3 스냅샷은 스냅샷이 생성된 시점의 버킷 객체의 정적 복사본입니다.

버킷에서 오브젝트 버전 관리를 사용하는 경우, 해당 버킷에 정의된 만료 규칙으로 인해 특정 버전의 오브젝트가 삭제되면 만료된 오브젝트 버전의 콘텐츠가 하나 이상의 S3 스냅샷에서 현재 버전으로 캡처된 경우 파일 시스템에 계속 남아 있습니다. 해당 객체 버전은 해당 스냅샷이 삭제될 때만 파일 시스템에 더 이상 존재하지 않습니다.

마찬가지로, 버전 관리가 비활성화된 버킷에서 만료 규칙에 따라 오브젝트가 삭제되지만 일부 기존 S3 스냅샷에서 오브젝트가 캡처된 경우 해당 오브젝트는 파일 시스템에 유지됩니다. 객체를 캡처하는 스냅샷이 삭제되면 객체가 파일 시스템에서 영구적으로 제거됩니다.

S3 오브젝트 만료 및 라이프사이클 관리에 대한 자세한 내용은 을 참조하십시오"버킷 수명 주기 관리 규칙을 생성합니다".

S3 스냅샷의 제한 사항

ONTAP 9.16.1에서 다음 기능 제외 및 시나리오를 참고하십시오.

- S3 버킷에 대해 최대 1023개의 스냅샷을 생성할 수 있습니다.
- 클러스터를 ONTAP 9.16.1 이전 버전의 ONTAP로 되돌리려면 먼저 클러스터의 모든 버킷에서 모든 S3 스냅샷과 메타데이터를 삭제해야 합니다.
- 스냅샷이 있는 오브젝트가 포함된 S3 버킷을 삭제해야 하는 경우 해당 버킷에 있는 모든 오브젝트의 해당 스냅샷을 모두 삭제했는지 확인하십시오.
- S3 스냅샷은 다음 구성에서 지원되지 않습니다.

- 완전히 새로운 차원의 제휴가 이루어질 수 있습니다 SnapMirror
- 물체 잠금이 활성화된 버킷
- NetApp 콘솔에서
- On System Manager 를 참조하십시오
- ONTAP MetroCluster 구성에서

- 로컬 또는 원격 FabricPool 용량 계층으로 사용되는 버킷에서는 S3 스냅샷을 사용하지 않는 것이 좋습니다.

ONTAP S3 스냅샷을 생성합니다

S3 스냅샷을 수동으로 생성하거나 스냅샷 정책을 설정하여 S3 스냅샷을 자동으로 생성할 수 있습니다. 스냅샷은 데이터 백업 및 복구에 사용하는 개체의 정적 복사본 역할을 합니다. 스냅샷 보존 기간을 결정하기 위해 지정된 간격으로 자동 스냅샷 생성을 지원하는 스냅샷 정책을 생성할 수 있습니다.

S3 스냅샷은 오브젝트 버전 관리를 사용 또는 사용하지 않고 S3 버킷에서 오브젝트 데이터를 보호하는 데 도움이 됩니다.

스냅샷은 S3 버킷에서 오브젝트 버전 관리를 사용하지 않는 경우, 이전 오브젝트 버전을 사용할 수 없는 경우 복원 작업에 사용할 수 있는 시점 레코드의 역할을 하기 때문에 데이터 보호를 설정하는 데 특히 유용합니다.

이 작업에 대해

- 다음 명명 규칙이 스냅샷에 적용됩니다(수동 및 자동 스냅샷 모두).
  - S3 스냅샷 이름은 최대 30자까지 지정할 수 있습니다
  - S3 스냅샷 이름은 소문자, 숫자, 점(.) 및 하이픈(-)만 구성할 수 있습니다.
  - S3 스냅샷 이름은 문자 또는 숫자로 끝나야 합니다
  - S3 스냅샷 이름에는 하위 문자열이 포함될 수 없습니다 `s3snap`
- S3 프로토콜의 컨텍스트에서 버킷 명명 제한으로 인해 버킷 이름이 63자로 제한됩니다. ONTAP S3 스냅샷은 S3 프로토콜을 통해 버킷으로 표시되므로 스냅샷 버킷 이름에 유사한 제한이 적용됩니다. 기본적으로 원래 버킷 이름이 기본 버킷 이름으로 사용됩니다.
- 어떤 버킷에 속하는 스냅샷을 보다 쉽게 식별할 수 있도록 스냅샷 버킷 이름은 기본 버킷 이름과 스냅샷 이름 앞에 붙는 특수 문자열로 `-s3snap-` 구성됩니다. 스냅샷 버킷 이름의 형식은 로 `<base_bucket_name>-s3snap-<snapshot_name>`지정됩니다.

  예를 들어, 다음 명령을 실행하여 `snap1` 에서 을 `bucket-a` 생성하면 기본 버킷에 액세스 권한이 있는 경우, S3 클라이언트를 통해 액세스할 수 있는 이름으로 스냅샷 버킷이 `bucket-a-s3snap-snap1` 생성됩니다.

  ```
  vserver object-store-server bucket snapshot create -bucket bucket-a
  -snapshot snap1
  ```

- 63자를 초과하는 스냅샷 버킷 이름을 생성하는 스냅샷을 생성할 수 없습니다.
- 자동 스냅샷 이름에는 기존 볼륨 스냅샷의 명명 규칙과 유사한 정책 일정 이름과 타임스탬프가 포함됩니다. 예를

들어 예약된 스냅샷 이름은 및 `hourly-2024-05-22-1105` 일 수 `daily-2024-01-01-0015` 있습니다.

S3 스냅샷을 수동으로 생성합니다

ONTAP CLI를 사용하여 S3 스냅샷을 수동으로 생성할 수 있습니다. 이 절차는 로컬 클러스터에만 스냅샷을 생성합니다.

단계

1. S3 스냅샷 생성:

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

다음 예에서는 `vs0` 스토리지 VM 및 `website-data` 버킷에 이라는 스냅샷을 `pre-update` 생성합니다.

```
vserver object-store-server bucket snapshot create -vserver vs0 -bucket
website-data -snapshot pre-update
```

버킷에 S3 스냅샷 정책을 할당합니다

S3 버킷 수준에서 스냅샷 정책을 구성하면 ONTAP가 예약된 S3 스냅샷을 자동으로 생성합니다. 기존 스냅샷 정책과 마찬가지로 S3 스냅샷에 대해 최대 5개의 일정을 구성할 수 있습니다.

스냅샷 정책은 일반적으로 스냅샷을 생성할 스케줄, 각 스케줄에 대해 보존할 복제본 수 및 스케줄 접두사를 지정합니다. 예를 들어 정책은 매일 오전 12시 10분에 S3 스냅샷 하나를 생성하고 가장 최근의 복제본 두 개를 보존하고 이름을 지정할 수 `daily-<timestamp>` 있습니다.

기본 스냅샷 정책은 다음을 보존합니다.

- 시간별 스냅샷 6개
- 일일 스냅샷 2개
- 주간 스냅샷 2개

시작하기 전에

- S3 버킷에 할당하기 전에 스냅샷 정책을 생성해야 합니다.

> S3 스냅샷에 대한 정책은 다른 ONTAP 스냅샷 정책과 동일한 규칙을 따릅니다. 하지만 스냅샷 스케줄에 보존 기간이 구성된 스냅샷 정책은 S3 버킷에 할당할 수 없습니다.

스냅샷 자동 생성을 위한 스냅샷 정책 생성에 대한 자세한 내용은 을 참조하십시오"사용자 지정 스냅샷 정책 구성 개요".

단계

1. 버킷에 스냅샷 정책을 할당합니다.

```
vserver object-store-server bucket create -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

또는

```
vserver object-store-server bucket modify -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

클러스터를 ONTAP 9.16.1 이전 버전의 ONTAP로 되돌려야 하는 경우 모든 버킷의 값이 (또는 -)로 설정되어 `none` 있는지 확인하십시오 `snapshot-policy`.

관련 정보

"ONTAP S3 스냅샷에 대해 자세히 알아보십시오"

ONTAP S3 스냅샷을 보고 복원합니다

ONTAP 9.16.1부터 S3 클라이언트의 버킷에 대한 S3 스냅샷 데이터를 보고 찾아볼 수 있습니다. ONTAP 9.18.1부터 ONTAP CLI를 사용하여 S3 스냅샷 버킷에 기본적으로 액세스할 수 있습니다. 또한 S3 스냅샷에서 S3 클라이언트의 단일 객체, 객체 세트 또는 전체 버킷을 복원할 수 있습니다.

시작하기 전에

- ONTAP CLI에서 버킷 스냅샷 복원 작업을 기본적으로 수행하려면 클러스터의 모든 노드에서 ONTAP 9.18.1 이상이 실행되어야 합니다. ONTAP 9.18.1부터 S3 브라우저는 더 이상 필요하지 않지만 작업은 계속 지원됩니다.
- 주어진 버킷에 대해 한 번에 하나의 스냅샷 복원 작업만 허용됩니다.

이 작업에 대해

ONTAP 9.16.1부터 ONTAP S3 스냅샷 기능은 수동 및 예약된 스냅샷 생성 및 삭제, S3 버킷에 대한 스냅샷 정책, S3 클라이언트 기반 스냅샷 검색을 포함하여 ONTAP S3 버킷에 대한 기본 스냅샷 기능을 제공합니다.

ONTAP 9.18.1부터 네이티브 ONTAP 스냅샷 복원에 대한 지원이 추가되어 ONTAP 관리자가 S3 브라우저를 사용하지 않고도 특정 시점 복원 기능을 사용할 수 있습니다. 스냅샷에는 현재 버킷 버전만 캡처됩니다. 버전 기록은 캡처되지 않으며 S3 스냅샷 복원 작업으로 복원되지 않습니다.

S3 스냅샷 나열 및 보기

S3 스냅샷 세부 정보를 보고, 비교하고, 오류를 식별할 수 있습니다. ONTAP CLI를 사용하면 S3 버킷에서 생성된 모든 스냅샷을 나열할 수 있습니다.

단계

1. S3 스냅샷 목록:

```
vserver object-store-server bucket snapshot show
```

클러스터의 모든 버킷에 대해 생성된 S3 스냅샷의 스냅샷 이름, 스토리지 VM, 버킷, 생성 시간 및 인스턴스 UUID를 볼 수 있습니다.

2. 버킷 이름을 지정하여 해당 버킷에 대해 생성된 모든 S3 스냅샷의 이름, 생성 시간, 인스턴스 UUID를 볼 수도 있습니다.

```
vserver object-store-server bucket snapshot show -vserver <svm_name>
-bucket <bucket_name>
```

S3 스냅샷 콘텐츠를 찾아봅니다

환경에서 장애나 문제가 발견되면 S3 버킷 스냅샷의 콘텐츠를 탐색하여 오류를 식별할 수 있습니다. 또한 S3 스냅샷을 탐색하여 오류 없는 콘텐츠를 복원할 수도 있습니다.

S3 스냅샷은 S3 클라이언트에 스냅샷 버킷으로 제공됩니다. 스냅샷 버킷 이름은 다음과 같이 형식화됩니다. `<base_bucket_name>-s3snap-<snapshot_name>` . 다음을 사용하여 스토리지 VM의 모든 스냅샷 버킷을 볼 수 있습니다. `ListBuckets` S3 API 작업.

S3 스냅샷 버킷은 기본 버킷의 액세스 정책을 상속받으며 읽기 전용 작업만 지원합니다. 삭제 및 쓰기 기반 작업은 금지됩니다. 기본 버킷에 액세스할 수 있는 권한이 있는 경우 S3 스냅샷 버킷에서 다음과 같은 읽기 전용 S3 API 작업을 수행할 수도 있습니다. `HeadObject` , `GetObject` , `GetObjectTagging` , `ListObjects` , `ListObjectVersions` , `GetObjectAcl` , 그리고 `CopyObject` .

> 이 `CopyObject` 작업은 S3 스냅샷 버킷이 소스 버킷의 스냅샷인 경우에만 지원되며, 스냅샷의 스토리지 타겟인 경우에는 지원되지 않습니다.

이러한 작업에 대한 자세한 내용은 을 "ONTAP S3가 지원되는 작업"참조하십시오.

ONTAP 사용하여 **S3** 스냅샷에서 버킷 복원

ONTAP 9.18.1부터 ONTAP CLI를 사용하여 ONTAP S3 스냅샷을 사용하여 전체 버킷을 복원할 수 있습니다. 선택한 스냅샷이 생성된 시점에 존재했던 버킷 버전만 복원할 수 있습니다.

단계

1. 버킷을 복원하는 데 사용할 스냅샷을 식별하세요.

```
vserver object-store-server bucket snapshot show
```

2. 버킷을 복원합니다.

```
vserver object-store-server bucket snapshot restore start -vserver
<storage VM name> -bucket <bucket name> -snapshot <snapshot name>
```

S3 클라이언트를 사용하여 S3 버킷 스냅샷에서 데이터 복원

ONTAP 에서 전체 버킷을 복원하는 것 외에도 S3cmd나 S3 Browser와 같은 S3 클라이언트를 사용하여 S3 스냅샷에서 단일 개체, 개체 세트 또는 전체 버킷을 복원할 수도 있습니다.

"버전이 지정된 스냅샷과 버전이 지정되지 않은 스냅샷에 대해 자세히 알아보세요."

다음을 사용하여 전체 버킷, 특정 접두사가 있는 개체 또는 단일 개체를 복원할 수 있습니다. `aws s3 cp` 명령.

단계

1. 기본 S3 버킷의 스냅샷을 생성합니다.

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <base_bucket_name> -snapshot <snapshot_name>
```

2. 스냅샷을 사용하여 기본 버킷을 복원합니다.
   - 전체 버킷을 복원합니다. 스냅샷 버킷 이름을 형식으로 `<base_bucket_name>-s3snap-<snapshot_name>` 사용합니다.

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>
s3://<base-bucket>  --recursive
```

   - 다음 접두사를 사용하여 디렉터리의 개체를 `dir1` 복원합니다.

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>/dir1
s3://<base_bucket_name>/dir1 --recursive
```

   - 이름이 인 단일 개체 복원 `web.py`:

```
aws --endpoint http://<IP> s3 cp s3:// <snapshot-bucket-name>/web.py
s3://<base_bucket_name>/web.py
```

ONTAP S3 스냅샷을 삭제합니다

더 이상 필요하지 않은 S3 스냅샷을 삭제하고 버킷의 스토리지 공간을 확보할 수 있습니다. S3 스냅샷을 수동으로 제거하거나 S3 버킷에 연결된 스냅샷 정책을 수정하여 일정에 대해 보존할 스냅샷 수를 변경할 수 있습니다.

S3 버킷에 대한 스냅샷 정책은 기존 ONTAP 스냅샷 정책과 동일한 삭제 규칙을 따릅니다. 스냅샷 정책 생성에 대한 자세한 내용은 을 "스냅샷 정책을 생성합니다"참조하십시오.

이 작업에 대해

- 여러 스냅숏에서 객체 버전(버전 버킷의 경우) 또는 객체(버전이 지정되지 않은 버킷의 경우)가 캡처된 경우 마지막으로 보호된 스냅샷이 삭제된 후에만 파일 시스템에서 객체가 제거됩니다.
- 스냅샷이 있는 오브젝트가 포함된 S3 버킷을 삭제해야 하는 경우 해당 버킷에 있는 모든 오브젝트의 모든 스냅샷을 삭제했는지 확인하십시오.
- 클러스터를 ONTAP 9.16.1 이전 버전의 ONTAP로 되돌려야 하는 경우 모든 버킷에 대해 모든 S3 스냅샷을 삭제했는지 확인하십시오. S3 버킷의 스냅샷 메타데이터를 제거하기 위해 명령을 실행해야 할 수도 `vserver object-store-server bucket clear-snapshot-metadata` 있습니다. 자세한 내용은 을 "S3 스냅샷 메타데이터를 지웁니다"참조하십시오.
- 스냅샷을 일괄적으로 삭제할 때 여러 스냅샷에 캡처된 많은 수의 개체를 제거하여 개별 스냅샷을 삭제할 때보다 더 많은 공간을 효율적으로 확보할 수 있습니다. 따라서 스토리지 오브젝트를 위해 더 많은 공간을 재확보할 수 있습니다.

단계

1. 특정 S3 스냅샷을 삭제하려면 다음 명령을 실행합니다.

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

2. 버킷에서 모든 S3 스냅샷을 제거하려면 다음 명령을 실행합니다.

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot *
```

S3 스냅샷 메타데이터를 지웁니다

S3 스냅샷을 사용하면 스냅샷 메타데이터도 버킷에서 생성됩니다. 스냅샷 메타데이터는 모든 스냅샷이 해당 스냅샷에서 제거되더라도 계속해서 버킷에 있게 됩니다. 스냅샷 메타데이터가 있으면 다음 작업이 차단됩니다.

- 클러스터를 ONTAP 9.16.1 이전 버전의 ONTAP로 되돌립니다
- 버킷에 SnapMirror S3 구성

이러한 작업을 수행하기 전에 버킷에서 모든 스냅샷 메타데이터를 지워야 합니다.

시작하기 전에

메타데이터 지우기를 시작하기 전에 버킷에서 모든 S3 스냅샷을 제거했는지 확인합니다.

단계

1. 버킷에서 스냅샷 메타데이터를 지우려면 다음 명령을 실행합니다.

```
vserver object-store-server bucket clear-snapshot-metadata -vserver
<svm_name> -bucket <bucket_name>
```

S3 이벤트를 감사합니다

ONTAP S3 이벤트 감사에 대해 자세히 알아보십시오

ONTAP 9.10.1부터 ONTAP S3 환경에서 데이터 및 관리 이벤트를 감사할 수 있습니다. S3 감사 기능은 기존의 NAS 감사 기능과 유사하며, S3 및 NAS 감사가 클러스터에 공존할 수 있습니다.

SVM에서 S3 감사 구성을 생성하고 활성화하면 S3 이벤트가 로그 파일에 기록됩니다. 기록할 다음 이벤트를 지정할 수 있습니다.

릴리즈별 오브젝트 액세스(데이터) 이벤트

9.11.1:

- 목록 BuckketVersions
- ListBucket(ListObjects 9.10.1의 이름이 이것으로 변경됨)
- ListAllMyBucket(9.10.1의 ListBucket 이름이 이것으로 변경됨)

9.10.1:

- HeadObject 를 선택합니다
- GetObject 를 참조하십시오
- PutObject 를 선택합니다
- DeleteObject 를 클릭합니다
- ListBucket
- ListObjects 를 선택합니다
- MPUpload 를 클릭합니다
- MPUploadPart 를 참조하십시오
- MPComplete(MPComplete)
- MPAbort(MP중단)
- GetObjectTagging
- DeleteObjectTagging 을 선택합니다
- PutObjectTagging
- 업로드 목록
- 목록 파트

릴리스별 관리 이벤트

9.15.1:

- GetBucketCORS 를 참조하십시오

- PutBucketCORS/퍼트버케토르스
- DeleteBucketCORS를 클릭합니다

9.14.1:

- GetObjectRetention을 참조하십시오
- PutObjectRetention
- PutBucketObjectLockConfiguration 을 참조하십시오
- GetBucketObjectLockConfiguration 을 참조하십시오

9.13.1:

- PutBucketLifecycle 을 참조하십시오
- DeleteBucketLifecycle
- GetBucketLifecycle 을 참조하십시오

9.12.1:

- GetBuckketPolicy를 참조하십시오
- CopyObject 를 선택합니다
- 업로드파트 복사
- BucketPolicy를 참조하십시오
- DeleteBuckketPolicy를 참조하십시오

9.11.1:

- GetBuckketVersioning 을 참조하십시오
- PutBucketVersioning을 참조하십시오

9.10.1:

- 머리버킷
- GetBuckketAcl
- GetObjectAcl
- 퍼트버킷
- 삭제 버킷
- ModifyObject태그 지정
- GetBucketLocation 을 참조하십시오

로그 형식은 JSON(JavaScript Object Notation)입니다.

S3 및 NFS 감사 구성의 경우 결합된 제한은 클러스터당 400개의 SVM입니다.

다음 라이센스가 필요합니다.

- ONTAP S3 프로토콜 및 스토리지를 위한 ONTAP One, 이전의 코어 번들에 포함됨

자세한 내용은 을 참조하십시오 "ONTAP 감사 프로세스의 작동 방식".

감사 보장

기본적으로 S3 및 NAS 감사가 보장됩니다. ONTAP는 노드를 사용할 수 없는 경우에도 감사 가능한 모든 버킷 액세스 이벤트를 기록할 수 있도록 보장합니다. 해당 작업에 대한 감사 레코드가 영구 스토리지의 스테이징 볼륨에 저장될 때까지 요청된 버킷 작업을 완료할 수 없습니다. 공간이 부족하거나 다른 문제로 인해 스테이징 파일에 감사 레코드를 커밋할 수 없는 경우 클라이언트 작업이 거부됩니다.

감사를 위한 공간 요구 사항

ONTAP 감사 시스템에서는 감사 레코드가 처음에는 개별 노드의 이진 스테이징 파일에 저장됩니다. 주기적으로 이러한 로그는 통합되어 사용자가 읽을 수 있는 이벤트 로그로 변환되며, SVM의 감사 이벤트 로그 디렉토리에 저장됩니다.

스테이징 파일은 감사 구성이 생성될 때 ONTAP에서 생성하는 전용 스테이징 볼륨에 저장됩니다. 애그리게이트당 하나의 스테이징 볼륨이 있습니다.

감사 구성에서 사용 가능한 충분한 공간을 계획해야 합니다.

- 감사된 버킷을 포함하는 애그리게이트에서 스테이징 볼륨의 경우
- 변환된 이벤트 로그가 저장되는 디렉토리가 포함된 볼륨입니다.

S3 감사 구성을 생성할 때 다음 두 가지 방법 중 하나를 사용하여 이벤트 로그 수와 볼륨의 사용 가능한 공간을 제어할 수 있습니다.

- 숫자 제한, '-rotate-limit' 매개변수는 보존되어야 하는 최소 감사 파일 수를 제어합니다.
- 시간 제한: '-retention-duration' 매개변수는 파일을 보존할 수 있는 최대 기간을 제어합니다.

두 매개 변수 모두에서 구성된 값을 초과하면 오래된 감사 파일을 삭제하여 새 감사 파일을 저장할 공간을 만들 수 있습니다. 두 매개 변수 모두 값이 0이면 모든 파일이 유지되어야 함을 나타냅니다. 따라서 충분한 공간을 확보하기 위해 매개 변수 중 하나를 0이 아닌 값으로 설정하는 것이 좋습니다.

감사 보장 때문에 감사 데이터에 사용할 수 있는 공간이 회전 제한 전에 초과되면 최신 감사 데이터를 생성할 수 없으므로 클라이언트가 데이터에 액세스하지 못합니다. 따라서 이 값과 감사에 할당된 공간을 신중하게 선택해야 하며 감사 시스템의 사용 가능한 공간에 대한 경고에 응답해야 합니다.

자세한 내용은 을 참조하십시오 "기본 감사 개념".

ONTAP S3 감사 구성 계획

S3 감사 구성에 대해 여러 매개 변수를 지정하거나 기본값을 그대로 사용해야 합니다. 특히 적절한 여유 공간을 확보하는 데 도움이 되는 로그 회전 매개 변수를 고려해야 합니다.

에 대한 자세한 내용은 `vserver object-store-server audit create` "ONTAP 명령 참조입니다"을 참조하십시오.

일반 매개변수

감사 구성을 만들 때 지정해야 하는 필수 매개 변수는 두 가지입니다. 지정할 수 있는 세 가지 선택적 매개 변수도 있습니다.

정보 유형입니다	옵션을 선택합니다	필수 요소입니다
_SVM 이름 _ 감사 구성을 생성할 SVM의 이름입니다. S3에 대해 SVM이 이미 존재하고 사용하도록 설정해야 합니다.	`-vserver svm_name`	예
_로그 대상 경로 _ 변환된 감사 로그를 저장할 위치를 지정합니다. SVM에 경로가 이미 있어야 합니다. 경로는 최대 864자까지 가능하며 읽기-쓰기 권한이 있어야 합니다. 경로가 유효하지 않으면 감사 구성 명령이 실패합니다.	'-destination_text_'	예
_ 감사할 이벤트의 범주 _ 다음 이벤트 범주를 감사할 수 있습니다. • Data GetObject , PutObject 및 DeleteObject 이벤트 • 관리 PutBucket 및 DeleteBucket 이벤트 기본값은 데이터 이벤트만 감사하는 것입니다.	'-events{data|management},…'	아니요

다음 매개 변수 중 하나를 입력하여 감사 로그 파일 수를 제어할 수 있습니다. 값을 입력하지 않으면 모든 로그 파일이 유지됩니다.

정보 유형입니다	옵션을 선택합니다	필수 요소입니다
_ 로그 파일 회전 제한 _ 가장 오래된 로그 파일을 회전하기 전에 유지할 감사 로그 파일 수를 결정합니다. 예를 들어 값을 5로 입력하면 마지막 5개의 로그 파일이 유지됩니다. 값 0은 모든 로그 파일이 보존됨을 나타냅니다. 기본값은 0입니다.	'-rotate-limit_integer _'	아니요

_로그 파일 지속 시간 제한 _ 로그 파일을 삭제하기 전에 보존할 수 있는 기간을 결정합니다. 예를 들어 5d0h0m 값을 입력하면 5일 이상 지난 로그가 삭제됩니다. 값 0은 모든 로그 파일이 보존됨을 나타냅니다. 기본값은 0입니다.	'-retention duration_integer_time_'	아니요

감사 로그 회전을 위한 매개 변수입니다

크기 또는 일정에 따라 감사 로그를 회전할 수 있습니다. 기본값은 크기에 따라 감사 로그를 회전하는 것입니다.

로그 크기에 따라 로그를 회전합니다

기본 로그 회전 방법과 기본 로그 크기를 사용하려면 로그 회전을 위한 특정 매개 변수를 구성할 필요가 없습니다. 기본 로그 크기는 100MB입니다.

기본 로그 크기를 사용하지 않으려면 '-rotate-size' 매개변수를 구성하여 사용자 정의 로그 크기를 지정할 수 있습니다.

로그 크기만을 기준으로 회전을 재설정하려면 다음 명령을 사용하여 '-rotate-schedule-minute' 매개 변수를 설정 해제합니다.

'vserver audit modify -vserver_svm_name_-destination/-rotate-schedule-minute -'

일정에 따라 로그를 회전합니다

일정에 따라 감사 로그를 회전하도록 선택한 경우 시간 기반 회전 매개 변수를 조합하여 로그 회전을 예약할 수 있습니다.

- 시간 기반 회전을 사용하는 경우 '-rotate-schedule-minute' 매개변수는 필수입니다.
- 다른 모든 시간 기반 회전 매개변수는 옵션입니다.
  - '-rotate-schedule-month’입니다
  - '-rotate-schedule-DayOfWeek'
  - '-rotate-schedule-day'
  - '-rotate-schedule-hour'
- 회전 일정은 모든 시간 관련 값을 사용하여 계산됩니다. 예를 들어, '-rotate-schedule-minute' 매개 변수만 지정하면 감사 로그 파일은 모든 연도의 모든 월에 지정된 모든 요일에 지정된 분을 기준으로 회전합니다.
- 시간 기반 회전 매개 변수(예: '-rotate-schedule-month' 및 '-rotate-schedule-minutes')를 하나 또는 두 개만 지정하는 경우 모든 시간 동안 모든 요일에 지정한 분 값을 기준으로 로그 파일이 회전되며 지정된 개월 동안에만 회전됩니다.

  예를 들어 월요일, 수요일 및 토요일은 오전 10시 30분에 월, 3월, 8월 중 감사 로그를 회전하도록 지정할 수 있습니다

- '-rotate-schedule-dayOfWeek' 및 '-rotate-schedule-day' 값을 모두 지정하면 독립적으로 간주됩니다.

  예를 들어, `-rotate-schedule-dayOfWeek’를 금요일로 지정하고 '-rotate-schedule-day’를 13일로 지정하면 13일에 금요일이 아니라 지정한 달의 13일에 감사 로그가 회전합니다.

- 일정만 기준으로 회전을 재설정하려면 다음 명령을 사용하여 '-rotate-size 매개 변수'를 해제합니다.

  'vserver audit modify -vserver_svm_name_-destination/-rotate-size-'

로그 크기 및 일정에 따라 로그를 회전합니다

모든 조합의 -rotate-size 매개 변수와 시간 기반 회전 매개 변수를 모두 설정하여 로그 크기와 일정에 따라 로그 파일을 회전하도록 선택할 수 있습니다. 예를 들어, '-rotate-size'를 10MB로 설정하고 '-rotate-schedule-minute'를 15로 설정하면 로그 파일 크기가 10MB에 도달하거나 매 시간 15분(둘 중 먼저 발생하는 이벤트)에 도달할 때 로그 파일이 회전합니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP S3 감사 구성을 생성하고 사용합니다

S3 감사를 구현하려면 먼저 S3 기반 SVM에서 영구 오브젝트 저장소 감사 구성을 생성한 다음 구성을 활성화합니다.

시작하기 전에

- S3 지원 SVM이 있습니다.
- 로컬 계층에 볼륨을 스테이징할 공간이 충분한지 확인합니다.

이 작업에 대해

감사 구성은 감사하려는 S3 버킷을 포함하는 각 SVM에 필요합니다. 신규 또는 기존 S3 서버에서 S3 감사를 활성화할 수 있습니다. 감사 구성은 * vserver object-store-server audit delete * 명령을 통해 제거될 때까지 S3 환경에서 지속됩니다.

S3 감사 구성은 감사를 위해 선택한 SVM의 모든 버킷에 적용됩니다. 감사 가능 SVM에는 감사되고 감사되지 않은 버킷이 포함될 수 있습니다.

로그 크기 또는 일정에 따라 자동 로그 회전에 대해 S3 감사를 구성하는 것이 좋습니다. 자동 로그 회전을 구성하지 않으면 기본적으로 모든 로그 파일이 유지됩니다. vserver object-store-server audit rotate -log * 명령을 사용하여 S3 로그 파일을 수동으로 회전할 수도 있습니다.

SVM이 SVM 재해 복구 소스인 경우 타겟 경로가 루트 볼륨에 있을 수 없습니다.

단계

1. 감사 구성을 생성하여 로그 크기 또는 일정에 따라 감사 로그를 회전합니다.

감사 로그를 회전하려면...	입력...
로그 크기	'vserver object-store-server audit create-vserver_svm_name_-destination_path_[[- events]{data| management},…] {[-rotate-limit_integer_]|[-retention-duration[*integer_d][_integer_h][_integer_m]]}[-rotate-size{_integer*[KB|MB|GB|TB|PB]}]']

감사 로그를 회전하려면...	입력...
일정	'vserver object-store-server audit create-vserver_svm_name_-destination path[[- events]{data| management},…] {[-rotate-limit_integer_]|[-retention-duration[*integerd*][*integerh*][*integerm*]}[-rotate-schedule -month_chron_month_][-rotate_schedule -DayOfWeek_chron_dayOfWeek_] [-rotate_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_month 시간 기반 감사 로그 회전을 구성하려면 '-rotate-schedule-minute' 매개 변수가 필요합니다.

2. S3 감사 활성화:

   'vserver object-store-server audit enable-vserver_svm_name_'

예

다음 예제에서는 크기 기반 회전을 사용하여 모든 S3 이벤트(기본값)를 감사하는 감사 구성을 만듭니다. 로그는 /audit_log 디렉토리에 저장됩니다. 로그 파일 크기 제한은 200MB입니다. 로그 크기가 200MB에 도달하면 로그가 회전합니다.

'cluster1::> vserver audit create - vserver vs1-destination/audit_log-rotate-size 200MB'

다음 예제에서는 크기 기반 회전을 사용하여 모든 S3 이벤트(기본값)를 감사하는 감사 구성을 만듭니다. 로그 파일 크기 제한은 100MB(기본값)이며, 로그 삭제 전 5일 동안 보존됩니다.

'cluster1::> vserver audit create - vserver vs1-destination/audit_log-retention-duration 5d0h0m'

다음 예제에서는 시간 기반 회전을 사용하여 S3 관리 이벤트와 중앙 액세스 정책 스테이징 이벤트를 감사하는 감사 구성을 만듭니다. 감사 로그는 매월 오후 12시 30분에 순환됩니다 일주일 내내. 로그 회전 제한은 5입니다.

'cluster1:> vserver audit create - vserver vs1-destination/audit_log-events management-rotate-schedule -month all-rotate-schedule -dayOfWeek all-rotate-schedule-hour 12-rotate-schedule-minute 30-rotate-limit 5'

ONTAP S3 감사를 위한 버킷 선택

감사 가능 SVM에서 감사할 버킷은 지정해야 합니다.

시작하기 전에

- S3 감사를 위해 SVM을 사용하도록 설정했습니다.

이 작업에 대해

S3 감사 구성은 SVM별로 활성화되지만 감사를 위해 SVM에서 버킷을 선택해야 합니다. SVM에 버킷을 추가하고 새 버킷을 감사하려면 이 절차를 사용하여 해당 버킷을 선택해야 합니다. S3 감사를 위해 SVM에서 감사하지 않은 버킷을 포함할 수도 있습니다.

감사 구성은 명령에 의해 제거될 때까지 버킷에 대해 `vserver object-store-server audit event-selector delete` 유지됩니다.

단계

1. S3 감사에 사용할 버킷 선택:

```
vserver object-store-server audit event-selector create -vserver
<svm_name> -bucket <bucket_name> [[-access] {read-only|write-only|all}]
[[-permission] {allow-only|deny-only|all}]
```

   - `-access`: 감사할 이벤트 액세스 형식을 지정합니다 `read-only`. , `write-only` 또는 `all` (기본값은 입니다. `all`)
   - `-permission`: 감사할 이벤트 권한의 유형을 지정합니다 `allow-only`. , `deny-only` 또는 `all` (기본값은 입니다. `all`)

예

다음 예제에서는 읽기 전용 액세스로 허용된 이벤트만 기록하는 버킷 감사 구성을 만듭니다.

'cluster1::> vserver object-store-server audit event-selector create-vserver vs1-bucket test-bucket-access read-only-permission allow-only'

ONTAP S3 감사 구성을 수정합니다

개별 버킷의 감사 매개 변수 또는 SVM에서 감사를 위해 선택한 모든 버킷의 감사 구성을 수정할 수 있습니다.

에 대한 감사 구성을 수정하려면...	입력...
개별 버킷	'vserver object-store-server audit event-selector modify -vserver_svm_name_[-bucket_bucket_name_][_parameters to modify _]'
SVM의 모든 버킷	'vserver object-store-server audit modify -vserver_svm_name_[_parameters to modify _]'

예

다음 예에서는 쓰기 전용 액세스 이벤트만 감사하도록 개별 버킷 감사 구성을 수정합니다.

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

다음 예에서는 SVM의 모든 버킷에 대한 감사 구성을 수정하여 로그 크기 제한을 10MB로 변경하고 회전 전에 로그 파일 3개를 보존합니다.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

ONTAP S3 감사 구성을 표시합니다

감사 구성을 완료한 후 감사가 올바르게 구성되어 있고 활성화되어 있는지 확인할 수 있습니다. 또한 클러스터의 모든 오브젝트 저장소 감사 구성에 대한 정보를 표시할 수도 있습니다.

이 작업에 대해

버킷 및 SVM 감사 구성에 대한 정보를 표시할 수 있습니다.

- 버킷: `vserver object-store-server audit event-selector show` 명령을 사용합니다

  매개 변수 없이 명령을 실행하면 오브젝트 저장소 감사 구성이 포함된 클러스터의 모든 SVM에 있는 버킷에 대한 다음 정보가 표시됩니다.

  - SVM 이름
  - 버킷 이름
  - 액세스 및 권한 값
- SVM: 명령을 사용합니다 `vserver object-store-server audit show`

  매개 변수 없이 명령을 실행하면 오브젝트 저장소 감사 구성이 포함된 클러스터의 모든 SVM에 대한 다음 정보가 표시됩니다.

  - SVM 이름
  - 감사 상태
  - 대상 디렉토리

'-fields' 파라미터를 지정하여 표시할 감사 구성 정보를 지정할 수 있습니다.

단계

S3 감사 구성에 대한 정보 표시:

에 대한 구성을 수정하려면...	입력...
버킷	'vserver object-store-server audit event-selector show[-vserver_svm_name_][*parameters*]'
SVM	'vserver object-store-server audit show[-vserver_svm_name_][*parameters*]'

예

다음 예는 단일 버킷에 대한 정보를 표시합니다.

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

다음 예는 SVM의 모든 버킷에 대한 정보를 표시합니다.

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver            :vs1
     Bucket             :test-bucket
     Access             :all
     Permission         :all
```

다음 예에서는 모든 SVM에 대한 이름, 감사 상태, 이벤트 유형, 로그 형식, 타겟 디렉토리를 표시합니다.

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

다음 예에서는 SVM 이름과 모든 SVM의 감사 로그에 대한 세부 정보를 표시합니다.

```
cluster1::> vserver object-store-server audit show -log-save-details

                 Rotation                            Rotation
      Vserver    File Size Rotation Schedule         Limit
      ---------- --------- ------------------------- --------
      vs1        100MB     -                         0
```

다음 예제는 모든 SVM에 대한 모든 감사 구성 정보를 목록 형식으로 표시합니다.

```
cluster1::> vserver object-store-server audit show -instance

                              Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: data
                          Log Format: json
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
                  Log Retention Time: 0s
```

인증 및 액세스 제어

인증 및 액세스 제어 개요

ONTAP 클러스터 인증과 ONTAP 웹 서비스에 대한 액세스 제어를 관리할 수 있습니다.

System Manager 또는 CLI를 사용하여 클러스터 및 스토리지에 대한 클라이언트 및 관리자 액세스를 제어하고 보호할 수 있습니다.

기존 System Manager(ONTAP 9.7 이하 버전에서만 사용 가능)를 사용하는 경우 을 참조하십시오 "System Manager Classic(ONTAP 9.0 ~ 9.7)"

클라이언트 인증 및 권한 부여

ONTAP는 신뢰할 수 있는 소스로 ID를 확인하여 클라이언트 시스템과 사용자를 인증합니다. ONTAP는 사용자의 자격 증명을 파일 또는 디렉터리에 구성된 권한과 비교하여 사용자가 파일 또는 디렉터리에 액세스할 수 있도록 승인합니다.

관리자 인증 및 **RBAC**

관리자는 로컬 또는 원격 로그인 계정을 사용하여 클러스터 및 스토리지 VM에 대한 자체 인증을 수행합니다. 역할 기반 액세스 제어(RBAC)는 관리자가 액세스할 수 있는 명령을 결정합니다.

관리자 인증 및 **RBAC** 관리

ONTAP의 관리자 인증 및 **RBAC**에 대해 알아봅니다

ONTAP 클러스터 관리자 및 SVM(스토리지 가상 시스템) 관리자의 로그인 계정을 활성화할 수 있습니다. 역할 기반 액세스 제어(RBAC)를 사용하여 관리자의 기능을 정의할 수도 있습니다.

로컬 관리자 계정이 다음 유형의 인증을 통해 SVM(관리 스토리지 가상 시스템) 또는 데이터 SVM에 액세스할 수 있도록 설정할 수 있습니다.

- "암호"
- "SSH 공개 키"
- "SSL 인증서"
- "SSH 다단계 인증(MFA)"

  ONTAP 9.3부터 암호 및 공개 키로 인증이 지원됩니다.

원격 관리자 계정에서 다음 인증 유형을 사용하여 관리 SVM 또는 데이터 SVM에 액세스할 수 있습니다.

- "Active Directory를 클릭합니다"

  ONTAP 9.13.1부터 Active Directory 사용자에 대한 기본 또는 보조 인증 방법으로 SSH 공개 키를 사용할 수 있습니다.

- "SAML 인증(관리 SVM에만 해당)"

  ONTAP 9.3부터 SAML(Security Assertion Markup Language) 인증은 서비스 프로세서 인프라, ONTAP API 또는 System Manager 웹 서비스를 사용하여 관리 SVM에 액세스하는 데 사용할 수 있습니다.

- "LDAP 또는 NIS"

  ONTAP 9.4부터 SSH MFA를 LDAP 또는 NIS 서버의 원격 사용자에게 사용할 수 있습니다. nsswitch 및 공개 키를 사용한 인증이 지원됩니다.

ONTAP 관리자 인증 및 RBAC 워크플로

로컬 관리자 계정 또는 원격 관리자 계정에 대해 인증을 설정할 수 있습니다. 로컬 계정의 계정 정보는 스토리지 시스템에 있으며 원격 계정의 계정 정보는 다른 위치에 있습니다. 각 계정에는 미리 정의된 역할 또는 사용자 지정 역할이 있을 수 있습니다.

구성 워크시트를 작성합니다

로그인 계정을 만들고 RBAC(역할 기반 액세스 제어)를 설정하기 전에 의 각 항목에 대한 정보를 수집해야 "구성 워크시트"합니다.

관리자 계정이 로컬 계정인지 원격 계정인지 확인합니다

- 로컬인 경우**:** "암호" "SSH를 클릭합니다", , "SSH MFA"또는 "SSL" 액세스를 활성화합니다.
- * If remote: * 원격 액세스 유형을 결정합니다. 액세스 유형에 따라,"Active Directory 액세스를 설정합니다", "LDAP 또는 NIS 액세스 설정"또는"SAML 인증 구성(관리자 SVM에만 해당)".

역할 기반 액세스 설정

관리자에게 할당된 역할에 따라 관리자가 액세스할 수 있는 명령이 결정됩니다. 역할은 관리자 계정을 만들 때 할당되며 나중에 지정할 수 "수정됨"있습니다. 및 "SVM" 관리자에 대해 또는 "사용자 지정 역할을 정의합니다"필요에 따라 미리 정의된 역할을 사용할 수 "클러스터"있습니다.

관리자 계정을 관리합니다

계정 액세스를 활성화한 방법에 따라 다음을 연결해야 할 수 있습니다. "로컬 계정이 있는 공개 키입니다" , 관리하다 "공개 키 및 X.509 인증서" , 구성 "SSH 로그인용 Cisco Duo 2FA" , 설치하다 "CA 서명 서버 디지털 인증서" 또는 구성 "Active Directory를 클릭합니다" , "LDAP, 즉 NIS입니다" 액세스. 계정 액세스를 활성화하기 전이나 후에 다음 작업을 수행할 수 있습니다.

추가 보안 기능을 구성합니다

- "여러 관리자 검증 관리" 지정된 관리자의 승인이 필요한 특정 작업을 확인하려면
- "동적 권한 부여 관리" 사용자의 신뢰 수준에 따라 추가 권한 부여 검사를 동적으로 적용하려는 경우
- "JIT(Just-In-Time) 권한 상승 구성" 특정 작업을 수행하기 위해 사용자에게 일시적으로 상승된 권한을 허용하려는

경우.

ONTAP 관리자 인증 및 RBAC 설정을 위한 워크시트

로그인 계정을 생성하고 역할 기반 액세스 제어(RBAC)를 설정하기 전에 구성 워크시트의 각 항목에 대한 정보를 수집해야 합니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

로그인 계정을 만들거나 수정합니다

로그인 계정을 사용하여 스토리지 VM에 액세스할 수 있도록 설정할 때 이러한 값을 명령과 함께 `security login create` 제공합니다. 에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

계정이 스토리지 VM에 액세스하는 방식을 수정할 때 명령에 동일한 값을 `security login modify` 제공합니다. 에 대한 자세한 내용은 `security login modify` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	계정이 액세스하는 스토리지 VM의 이름입니다. 기본값은 클러스터에 대한 admin 스토리지 VM의 이름입니다.	
'-user-or-group-name’입니다	계정의 사용자 이름 또는 그룹 이름입니다. 그룹 이름을 지정하면 그룹의 각 사용자에 액세스할 수 있습니다. 사용자 이름 또는 그룹 이름을 여러 응용 프로그램과 연결할 수 있습니다.	
'-응용 프로그램'	스토리지 VM에 액세스하는 데 사용되는 애플리케이션: • http입니다 • ontapi • 'NMP’입니다 • "쉬"	

'-AuthMethod’입니다	계정을 인증하는 데 사용되는 메소드: • SSL 인증서 인증용 인증서 • Active Directory 인증을 위한 "domain"입니다 • LDAP 또는 NIS 인증을 위한 nsswitch입니다 • 사용자 비밀번호 인증용 비밀번호 • 공개 키 인증을 위한 공개 키 • SNMP 커뮤니티 문자열을 위한 커뮤니티 • SNMP 사용자 보안 모델을 위한 USM • SAML(Security Assertion Markup Language) 인증 시 'AML	
'-remote-switch-ipaddress'	원격 스위치의 IP 주소입니다. 원격 스위치는 CSMM(Cluster Switch Health Monitor)에서 모니터링하는 클러스터 스위치이거나 MCC-HM(MetroCluster Health Monitor)에서 모니터링하는 FC(Fibre Channel) 스위치일 수 있습니다. 이 옵션은 애플리케이션이 NMP에 있고 인증 방법이 USM 일 때만 적용됩니다.	
'-역할'	계정에 할당된 액세스 제어 역할: • 클러스터(관리자 스토리지 VM)의 경우 기본값은 입니다 `admin`. • 데이터 스토리지 VM의 경우 기본값은 입니다 `vsadmin`.	
``논평’	(선택 사항) 계정에 대한 설명 텍스트입니다. 텍스트는 큰따옴표(")로 묶어야 합니다.	
'-is-ns-switch-group'	계정이 LDAP 그룹 계정인지 NIS 그룹 계정인지 여부('예' 또는 '아니요')	

두 번째 인증 방법	다단계 인증의 경우 두 번째 인증 방법: • "없음" 다단계 인증을 사용하지 않으면 기본값이 됩니다 • AuthMethod가 password 또는 nsswitch 일 때 공개 키 인증을 위한 공개 키 • 'AuthMethod'가 공개 키일 때 사용자 암호 인증을 위한 'password'입니다 • AuthMethod가 publickey 일 때 사용자 암호 인증을 위한 nsswitch 인증 순서는 항상 공개 키와 암호 순서로 표시됩니다.	
'-is-ldap-fastbind'	ONTAP 9.11.1부터 true로 설정하면 nsswitch 인증에 대한 LDAP 고속 바인딩이 설정됩니다. 기본값은 false 입니다. LDAP 빠른 바인딩을 사용하려면 `-authentication -method` 값을 로 설정해야 `nsswitch` 합니다. "ONTAP NFS SVM에 대한 nsswitch 인증을 위해 LDAP 빠른 바인딩을 사용합니다."..	

Cisco Duo 보안 정보를 구성합니다

스토리지 VM에 대해 SSH 로그인으로 Cisco Duo 2단계 인증을 사용하도록 설정할 때 이 값을 `security login duo create` 명령에 입력합니다. 에 대한 자세한 내용은 `security login duo create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	Duo 인증 설정이 적용되는 스토리지 VM(ONTAP CLI에서 가상 서버라고도 함)	
`-integration-key`	Duo에 SSH 애플리케이션을 등록할 때 얻은 통합 키입니다.	
`-secret-key`	Duo에 SSH 애플리케이션을 등록할 때 얻은 비밀 키입니다.	

`-api-host`	Duo에 SSH 애플리케이션을 등록할 때 얻은 API 호스트 이름입니다. 예를 들면 다음과 같습니다. `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	Duo 인증을 방해하는 서비스 또는 구성 오류 발생 시 실패합니다 `safe` (액세스 허용) 또는 `secure` (액세스 거부). 기본값은 입니다 `safe`즉, Duo API 서버에 액세스할 수 없는 등의 오류로 인해 Duo 인증이 실패할 경우 Duo 인증이 무시됩니다.	
`-http-proxy`	지정된 HTTP 프록시를 사용합니다. HTTP 프록시에 인증이 필요한 경우 프록시 URL에 자격 증명을 포함합니다. 예를 들면 다음과 같습니다. `http-proxy=http://username:password@proxy.example.org:8080`	
`-autopush`	둘 다 가능합니다 `true` 또는 `false`. 기본값은 입니다 `false`. If(경우 `true`, Duo는 푸시 로그인 요청을 사용자의 전화기로 자동으로 전송하여 푸시 기능을 사용할 수 없는 경우 전화 통화로 되돌립니다. 이렇게 하면 암호 인증이 효과적으로 비활성화됩니다. If(경우 `false`인증 방법을 선택하라는 메시지가 표시됩니다. 를 사용하여 구성 시 `autopush = true`, 설정하는 것이 좋습니다 `max-prompts = 1`.	

`-max-prompts`	사용자가 두 번째 요소로 인증하지 못하면 Duo는 사용자에게 다시 인증하라는 메시지를 표시합니다. 이 옵션은 액세스를 거부하기 전에 Duo가 표시하는 최대 프롬프트 수를 설정합니다. 이어야 합니다 `1`, `2`, 또는 `3`. 기본값은 입니다 `1`. 예를 들어, When `max-prompts = 1`, 사용자가 첫 번째 프롬프트에서 성공적으로 인증해야 하는 반면 IF `max-prompts = 2`초기 프롬프트에서 잘못된 정보를 입력하면 다시 인증하라는 메시지가 표시됩니다. 를 사용하여 구성 시 `autopush = true`, 설정하는 것이 좋습니다 `max-prompts = 1`. 최상의 경험을 위해 공개 키 인증만 있는 사용자는 항상 을(를) 가질 수 있습니다 `max-prompts` 를 로 설정합니다 `1`.	
`-enabled`	Duo 이중 인증을 활성화합니다. 를 로 설정합니다 `true` 기본적으로 사용됩니다. 활성화되면 구성된 매개 변수에 따라 SSH 로그인 중에 Duo 이중 인증이 적용됩니다. Duo가 비활성화된 경우(로 설정 `false`), Duo 인증은 무시됩니다.	
`-pushinfo`	이 옵션은 액세스 중인 응용 프로그램 또는 서비스의 이름과 같은 추가 정보를 푸시 알림에 제공합니다. 이렇게 하면 사용자가 올바른 서비스에 로그인하는지 확인할 수 있으며 추가적인 보안 계층을 제공합니다.	

사용자 지정 역할을 정의합니다

사용자 지정 역할을 정의할 때 이러한 값을 명령과 함께 `security login role create` 제공합니다. 에 대한 자세한 내용은 `security login role create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치

'-vserver'	(선택 사항) 역할과 연결된 스토리지 VM(ONTAP CLI에서 가상 서버라고 함)의 이름입니다.	
'-역할'	역할의 이름입니다.	
'-cmddirname’입니다	역할이 액세스를 제공하는 명령 또는 명령 디렉토리입니다. 명령 하위 디렉터리 이름은 큰따옴표(")로 묶어야 합니다. 예를 들어 ""볼륨 스냅샷""을 입력합니다. 모든 명령 디렉토리를 지정하려면 'default’를 입력해야 합니다.	
'-액세스'	(선택 사항) 역할에 대한 액세스 수준입니다. 명령 디렉토리의 경우: • "없음"(사용자 지정 역할의 기본값)은 명령 디렉토리의 명령에 대한 액세스를 거부합니다 • '재만’은 명령 디렉토리와 하위 디렉토리에 있는 'show' 명령에 대한 액세스 권한을 부여합니다 • ALL은 명령 디렉토리와 하위 디렉토리에 있는 모든 명령에 대한 액세스 권한을 부여합니다 비내장 명령어 _ (create, modify, delete, sHow로 끝내지 않는 명령어): • "없음"(사용자 지정 역할의 기본값)은 명령에 대한 액세스를 거부합니다 • "재담만"은 적용할 수 없습니다 • 모두 명령을 사용할 수 있는 권한을 부여합니다 내장 명령에 대한 액세스를 부여하거나 거부하려면 명령 디렉터리를 지정해야 합니다.	

'-query'	(선택 사항) 명령 또는 명령 디렉터리의 명령에 대해 유효한 옵션 형식으로 지정된 액세스 수준을 필터링하는 데 사용되는 쿼리 개체입니다. 쿼리 개체는 큰따옴표 (")로 묶어야 합니다. 예를 들어, 명령 디렉토리가 "volume"이면 쿼리 객체 "-aggr0"은 "aggr0" 집합에만 액세스를 활성화합니다.	

공개 키를 사용자 계정에 연결합니다

SSH 공개 키를 사용자 계정에 연결할 때 이러한 값을 `security login publickey create` 명령에 제공합니다. 에 대한 자세한 내용은 `security login publickey create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	(선택 사항) 계정이 액세스하는 스토리지 VM의 이름입니다.	
'-사용자 이름'	계정의 사용자 이름입니다. 기본값인 admin은 클러스터 관리자의 기본 이름입니다.	
``인덱스’	공개 키의 인덱스 번호입니다. 이 키가 계정에 대해 만들어진 첫 번째 키인 경우 기본값은 0이고, 그렇지 않은 경우 기본값은 해당 계정의 기존 인덱스 번호가 가장 높은 값보다 하나 더 큽니다.	
'-공개 키'	OpenSSH 공개 키입니다. 키를 큰따옴표(")로 묶어야 합니다.	
'-역할'	계정에 할당된 액세스 제어 역할입니다.	
``논평’	(선택 사항) 공개 키에 대한 설명 텍스트입니다. 텍스트는 큰따옴표(")로 묶어야 합니다.	

`-x509-certificate`	(선택 사항) ONTAP 9.13.1 부터는 SSH 공개 키와 X.509 인증서 연결을 관리할 수 있습니다. X.509 인증서를 SSH 공개 키와 연결하면 ONTAP는 SSH 로그인 시 이 인증서가 유효한지 확인합니다. 만료되었거나 해지된 경우 로그인이 허용되지 않고 연결된 SSH 공개 키가 비활성화됩니다. 가능한 값: • `install`: 지정된 PEM 인코딩된 X.509 인증서를 설치하고 SSH 공개 키와 연결합니다. 설치할 인증서의 전체 텍스트를 포함합니다. • `modify`: 기존 PEM 인코딩된 X.509 인증서를 지정된 인증서와 업데이트하고 SSH 공개 키에 연결합니다. 새 인증서의 전체 텍스트를 포함합니다. • `delete`: SSH 공개 키와 기존 X.509 인증서 연결을 제거합니다.	

동적 권한 부여 전역 설정을 구성합니다

ONTAP 9.15.1부터 명령에 이러한 값을 `security dynamic-authorization modify` 제공합니다. 에 대한 자세한 내용은 `security dynamic-authorization modify` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	신뢰 점수 설정을 수정해야 하는 스토리지 VM의 이름입니다. 이 매개 변수를 생략하면 클러스터 수준의 설정이 사용됩니다.	

``상태''	동적 인증 모드입니다. 가능한 값: • `disabled`: (기본값) 동적 인증이 비활성화되었습니다. • `visibility`: 이 모드는 동적 권한 부여를 테스트하는 데 유용합니다. 이 모드에서는 모든 제한된 작업에서 신뢰 점수가 확인되지만 적용되지는 않습니다. 그러나 거부되거나 추가 인증 문제가 발생했을 수 있는 모든 작업이 기록됩니다. • `enforced`: 로 테스트를 완료한 후 사용합니다 `visibility` 모드를 선택합니다. 이 모드에서는 모든 제한된 작업에서 신뢰 점수를 확인하고 제한 조건이 충족되면 활동 제한이 적용됩니다. 또한 억제 간격이 적용되어 지정된 간격 내에 추가적인 인증 문제가 발생하지 않습니다.	
`-suppression-interval`	지정된 간격 내에 추가적인 인증 문제를 방지합니다. 간격은 ISO-8601 형식으로 1분에서 1시간 사이의 값을 허용합니다. 0으로 설정하면 억제 간격이 비활성화되고 필요한 경우 사용자에게 항상 인증 확인 메시지가 표시됩니다.	
`-lower-challenge-boundary`	하위 MFA(다중 요소 인증) 본인 확인 백분율 경계입니다. 유효한 범위는 0에서 99 사이입니다. 값 100은 모든 요청이 거부되기 때문에 유효하지 않습니다. 기본값은 0입니다.	
`-upper-challenge-boundary`	상위 MFA 챌린지 백분율 경계입니다. 유효한 범위는 0에서 100 사이입니다. 이 값은 하위 경계 값보다 크거나 같아야 합니다. 값이 100이면 모든 요청이 거부되거나 추가 인증 챌린지가 적용됩니다. 본인 확인 없이 허용되는 요청은 없습니다. 기본값은 90입니다.	

CA 서명 서버 디지털 인증서를 설치합니다

저장소 VM을 SSL 서버로 인증하는 데 사용할 CSR(디지털 인증서 서명 요청)을 생성할 때 이러한 값을 명령과 함께 `security certificate generate-csr` 제공합니다. 에 대한 자세한 내용은 `security certificate generate-csr` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-common-name'입니다	정규화된 도메인 이름(FQDN) 또는 사용자 지정 일반 이름인 인증서의 이름입니다.	
'-size'	개인 키의 비트 수입니다. 값이 클수록 키가 더 안전합니다. 기본값은 2048입니다. 가능한 값은 512, 1024, 1536, 2048입니다.	
``국가'	스토리지 VM의 국가로, 2자로 된 코드입니다. 기본값은 입니다 `US`. 코드 목록은 를 참조하십시오"ONTAP 명령 참조입니다".	
``상태''	스토리지 VM의 시/도입니다.	
``지역성''	스토리지 VM의 인접성	
``조직''	스토리지 VM의 조직입니다.	
``단위''	스토리지 VM 조직의 단위입니다.	
'-email-addr'	스토리지 VM에 대한 담당자 관리자의 e-메일 주소입니다.	
``해쉬-함수''	인증서 서명을 위한 암호화 해싱 기능 기본값은 'HA256'입니다. 가능한 값은 'HA1', 'HA256', 'MD5'입니다.	

클러스터 또는 스토리지 VM을 SSL 서버로 인증하는 데 사용할 CA 서명 디지털 인증서를 설치할 때 이러한 값을 명령과 함께 `security certificate install` 제공합니다. 다음 표에는 계정 구성과 관련된 옵션만 나와 있습니다. 에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	인증서를 설치할 스토리지 VM의 이름입니다.	

``유형''	인증서 유형: • 서버 인증서 및 중간 인증서에 대한 서버 • SSL 클라이언트의 루트 CA의 공개 키 인증서에 대한 client-ca • ONTAP가 클라이언트인 SSL 서버의 루트 CA의 공개 키 인증서에 대한 서버-카 • SSL 클라이언트로서 ONTAP의 자체 서명 또는 CA 서명 디지털 인증서 및 개인 키용 '클라이언트'	

Active Directory 도메인 컨트롤러 액세스를 구성합니다

데이터 스토리지 VM에 대해 SMB 서버를 이미 구성한 경우 스토리지 VM을 게이트웨이로 구성하거나 클러스터에 대한 Active Directory 도메인 컨트롤러 액세스를 위해 _tunnel_로 구성하려는 경우 이 값을 명령과 함께 `security login domain-tunnel create` 제공합니다. 에 대한 자세한 내용은 `security login domain-tunnel create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	SMB 서버가 구성된 스토리지 VM의 이름입니다.	

SMB 서버를 구성하지 않은 상태에서 Active Directory 도메인에 스토리지 VM 컴퓨터 계정을 생성하려는 경우 이 값을 명령과 함께 `vserver active-directory create` 제공합니다. 에 대한 자세한 내용은 `vserver active-directory create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	Active Directory 컴퓨터 계정을 생성할 스토리지 VM의 이름입니다.	
'-계정-이름'	컴퓨터 계정의 NetBIOS 이름입니다.	
``도메인'	FQDN(정규화된 도메인 이름)입니다.	
'-ou'	도메인의 조직 단위입니다. 기본값은 CN=Computers입니다. ONTAP는 이 값을 도메인 이름에 더하여 Active Directory 고유 이름을 생성합니다.	

LDAP 또는 **NIS** 서버 액세스를 구성합니다

스토리지 VM에 대한 LDAP 클라이언트 구성을 생성할 때 이러한 값을 명령과 함께 `vserver services name-`

`service ldap client create` 제공합니다. 에 대한 자세한 내용은 `vserver services name-service ldap client create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 표에는 계정 구성과 관련된 옵션만 나와 있습니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	클라이언트 구성에 대한 스토리지 VM의 이름입니다.	
'-client-config'입니다	클라이언트 구성의 이름입니다.	
'-LDAP-서버'	클라이언트가 연결되는 LDAP 서버의 IP 주소 및 호스트 이름을 쉼표로 구분하여 나열합니다.	
'-스키마'	클라이언트가 LDAP 쿼리를 만드는 데 사용하는 스키마입니다.	
'-use-start-tls'	클라이언트가 Start TLS를 사용하여 LDAP 서버와의 통신을 암호화하는지 여부("true" 또는 "false") TLS 시작은 데이터 스토리지 VM에 대한 액세스에만 지원됩니다. 관리자 스토리지 VM에 대한 액세스는 지원되지 않습니다.	

LDAP 클라이언트 구성을 스토리지 VM에 연결할 때 이러한 값을 명령과 함께 `vserver services name-service ldap create` 제공합니다. 에 대한 자세한 내용은 `vserver services name-service ldap create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	클라이언트 구성을 연결할 스토리지 VM의 이름입니다.	
'-client-config'입니다	클라이언트 구성의 이름입니다.	
'-client-enabled'	스토리지 VM이 LDAP 클라이언트 구성을 사용할 수 있는지 여부를 나타냅니다 (`true` 또는 `false`)를 클릭합니다.	

스토리지 VM에서 NIS 도메인 구성을 생성할 때 명령과 함께 이러한 값을 `vserver services name-service`

`nis-domain create` 제공합니다. 에 대한 자세한 내용은 `vserver services name-service nis-domain create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	도메인 구성을 생성할 스토리지 VM의 이름입니다.	
``도메인’	도메인의 이름입니다.	
'-NIS-서버'	도메인 구성에 사용되는 NIS 서버의 IP 주소 및 호스트 이름을 쉼표로 구분된 목록입니다.	

이름 서비스 소스의 조회 순서를 지정할 때 이러한 값을 명령과 함께 `vserver services name-service ns-switch create` 제공합니다. 에 대한 자세한 내용은 `vserver services name-service ns-switch create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	이름 서비스 조회 순서를 구성할 스토리지 VM의 이름입니다.	
'-데이터베이스'	네임 서비스 데이터베이스: • 파일 및 DNS 이름 서비스를 위한 호스트 • 파일, LDAP, NIS 이름 서비스에 대한 그룹 • 파일, LDAP 및 NIS 이름 서비스의 'passwd' • 파일, LDAP 및 NIS 이름 서비스에 대한 넷그룹 • 파일 및 LDAP 이름 서비스에 대한 이름 맵	
``근원''	쉼표로 구분된 목록에서 이름 서비스 소스를 조회하는 순서: • '파일' • 드문들 • "LDAP" • 국정원	

SAML 액세스를 구성합니다

ONTAP 9.3부터 SAML 인증을 구성하는 명령과 함께 이러한 값을 `security saml-sp create` 제공합니다. 에 대한 자세한 내용은 `security saml-sp create` "ONTAP 명령 참조입니다"을 참조하십시오.

필드에 입력합니다	설명	귀사의 가치
'-IDP-Uri'	IDP 메타데이터를 다운로드할 수 있는 IDP(Identity Provider) 호스트의 FTP 주소 또는 HTTP 주소입니다.	
``SP-HOST''	SAML 서비스 공급자 호스트(ONTAP 시스템)의 호스트 이름 또는 IP 주소입니다. 기본적으로 클러스터 관리 LIF의 IP 주소가 사용됩니다.	
`-cert-ca` 및 `-cert-serial`, 또는 `-cert-common-name`	서비스 공급자 호스트(ONTAP 시스템)의 서버 인증서 세부 정보입니다. 서비스 공급자의 CA(인증 기관)와 인증서의 일련 번호 또는 서버 인증서 공통 이름을 입력할 수 있습니다.	
'-verify-metadata-server'	IDP 메타데이터 서버의 ID를 검증해야 하는지 여부('true' 또는 'false'). 가장 좋은 방법은 이 값을 항상 TRUE로 설정하는 것입니다.	

로그인 계정을 만듭니다

ONTAP 로그인 계정 생성에 대해 자세히 알아봅니다

로컬 또는 원격 클러스터 및 SVM 관리자 계정을 활성화할 수 있습니다. 로컬 계정은 계정 정보, 공개 키 또는 보안 인증서가 스토리지 시스템에 상주하는 계정입니다. AD 계정 정보는 도메인 컨트롤러에 저장됩니다. LDAP 및 NIS 계정은 LDAP 및 NIS 서버에 상주합니다.

클러스터 및 **SVM** 관리자

클러스터 관리자는 _ 클러스터에 대한 admin SVM에 액세스합니다. 클러스터 설정 시 admin이라는 예약 이름의 클러스터 관리자와 SVM 관리자가 자동으로 생성됩니다.

기본 'admin' 역할을 가진 클러스터 관리자는 전체 클러스터와 리소스를 관리할 수 있습니다. 클러스터 관리자는 필요에 따라 서로 다른 역할을 가진 추가 클러스터 관리자를 생성할 수 있습니다.

SVM 관리자는 _ 데이터 SVM에 액세스합니다. 클러스터 관리자가 필요에 따라 데이터 SVM 및 SVM 관리자를 생성합니다.

SVM 관리자는 기본적으로 'vsadmin' 역할이 할당됩니다. 클러스터 관리자는 필요에 따라 SVM 관리자에게 다양한 역할을 할당할 수 있습니다.

명명 규칙

다음 일반 이름은 원격 클러스터 및 SVM 관리자 계정에 사용할 수 없습니다.

- "아담"
- "출력함"
- "CLI"
- "데몬"
- "FTP"
- "게임"
- "중지"
- "lp"
- "메일"
- "남자"
- "나루트"
- "NetApp"
- "뉴스"
- "없음"
- "연산자"
- "루트"
- "종료"
- "sshd"
- "동기화"
- "시스템"
- "우프"
- "www"

병합된 역할

동일한 사용자에 대해 여러 원격 계정을 사용하도록 설정하면 계정에 지정된 모든 역할의 조합이 사용자에게 할당됩니다. 즉, LDAP 또는 NIS 계정에 vsadmin 역할이 할당되고 같은 사용자의 AD 그룹 계정에 vsadmin-volume 역할이 할당되면 AD 사용자는 보다 포괄적인 vsadmin 기능으로 로그인합니다. 역할은 _ 병합 _ 이라고 합니다.

로컬 계정 액세스를 설정합니다

로컬 **ONTAP** 계정 액세스 설정 에 대해 자세히 알아보십시오

로컬 계정은 계정 정보, 공개 키 또는 보안 인증서가 스토리지 시스템에 상주하는 계정입니다. 명령을 사용하여 로컬 계정에서 관리자 또는 데이터 SVM에 액세스할 수 있도록 설정할 수 있습니다 `security login create`.

관련 정보

- "보안 로그인 생성"

ONTAP 계정 암호 액세스를 활성화합니다

명령을 사용하여 관리자 계정이 암호로 관리자 또는 데이터 SVM에 액세스하도록 설정할 수 있습니다 `security login create`. 명령을 입력하면 암호를 묻는 메시지가 표시됩니다.

이 작업에 대해

로그인 계정에 할당하려는 액세스 제어 역할이 확실하지 않은 경우 명령을 사용하여 나중에 역할을 추가할 수 `security login modify` 있습니다.

에 대한 자세한 내용은 `security login modify` "ONTAP 명령 참조입니다"을 참조하십시오.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 로컬 관리자 계정에서 암호를 사용하여 SVM에 액세스:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   다음 명령을 사용하면 미리 정의된 백업 역할을 가진 클러스터 관리자 계정 admin1이 암호를 사용하여 SVM "engCluster"에 액세스할 수 있습니다. 명령을 입력하면 암호를 묻는 메시지가 표시됩니다.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

   에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 계정 **SSH** 공개 키 액세스를 설정합니다

명령을 사용하여 관리자 계정이 SSH 공개 키로 admin 또는 데이터 SVM에 액세스하도록 설정할 수 있습니다 `security login create`.

이 작업에 대해

- 계정이 SVM에 액세스하려면 먼저 공개 키를 계정에 연결해야 합니다.

  공개 키를 사용자 계정과 연결

  계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- 로그인 계정에 할당하려는 액세스 제어 역할이 확실하지 않은 경우 명령을 사용하여 나중에 역할을 추가할 수 `security login modify` 있습니다.

에 대한 자세한 내용은 `security login modify` "ONTAP 명령 참조입니다"을 참조하십시오.

클러스터에서 FIPS 모드를 활성화하려면 지원되는 키 알고리즘이 없는 기존 SSH 공개 키 계정을 지원되는 키 유형으로 재구성해야 합니다. FIPS를 사용하도록 설정하기 전에 계정을 다시 구성해야 하며 그렇지 않으면 관리자 인증이 실패합니다.

다음 표에는 ONTAP SSH 연결에 지원되는 호스트 키 유형 알고리즘이 나와 있습니다. 이러한 키 유형은 SSH 공개 인증 구성에 적용되지 않습니다.

ONTAP 릴리즈	FIPS 모드에서 지원되는 키 유형입니다	FIPS 이외의 모드에서 지원되는 키 유형입니다
9.11.1 이상	ECDSA-SHA2-nistp256	ECDSA-SHA2-nistp256+RSA-SHA2-512+RSA-SHA2-256+ssh-ed25519+ssh-dss+ssh-ssh-rsa
9.10.1 이하	ECDSA-SHA2-nistp256+ssh-ed25519	ECDSA-SHA2-nistp256+ssh-ed25519+ssh-dss+ssh-rsa

ONTAP 9.11.1부터 ssh-ed25519 호스트 키 알고리즘에 대한 지원이 제거되었습니다.

자세한 내용은 을 "FIPS를 사용하여 네트워크 보안을 구성합니다"참조하십시오.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 로컬 관리자 계정이 SSH 공개 키를 사용하여 SVM에 액세스할 수 있도록 합니다.

   '보안 로그인 생성 - vserver_SVM_name_-user-or-group-name user_or_group_name-application_application_-AuthMethod_authentication_method_-role_role_-comment_comment_'

   다음 명령을 실행하면 SSH 공개 키를 사용하여 SVM "engData1"에 액세스할 수 있도록 사전 정의된 "vsadmin-volume" 역할이 있는 SVM 관리자 계정의 vmadmin1이 활성화됩니다.

   ```
   cluster1::>security login create -vserver engData1 -user-or-group-name
   svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
   ```

   에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

공개 키를 관리자 계정에 연결하지 않은 경우, 계정이 SVM에 액세스하려면 먼저 연결해야 합니다.

공개 키를 사용자 계정과 연결

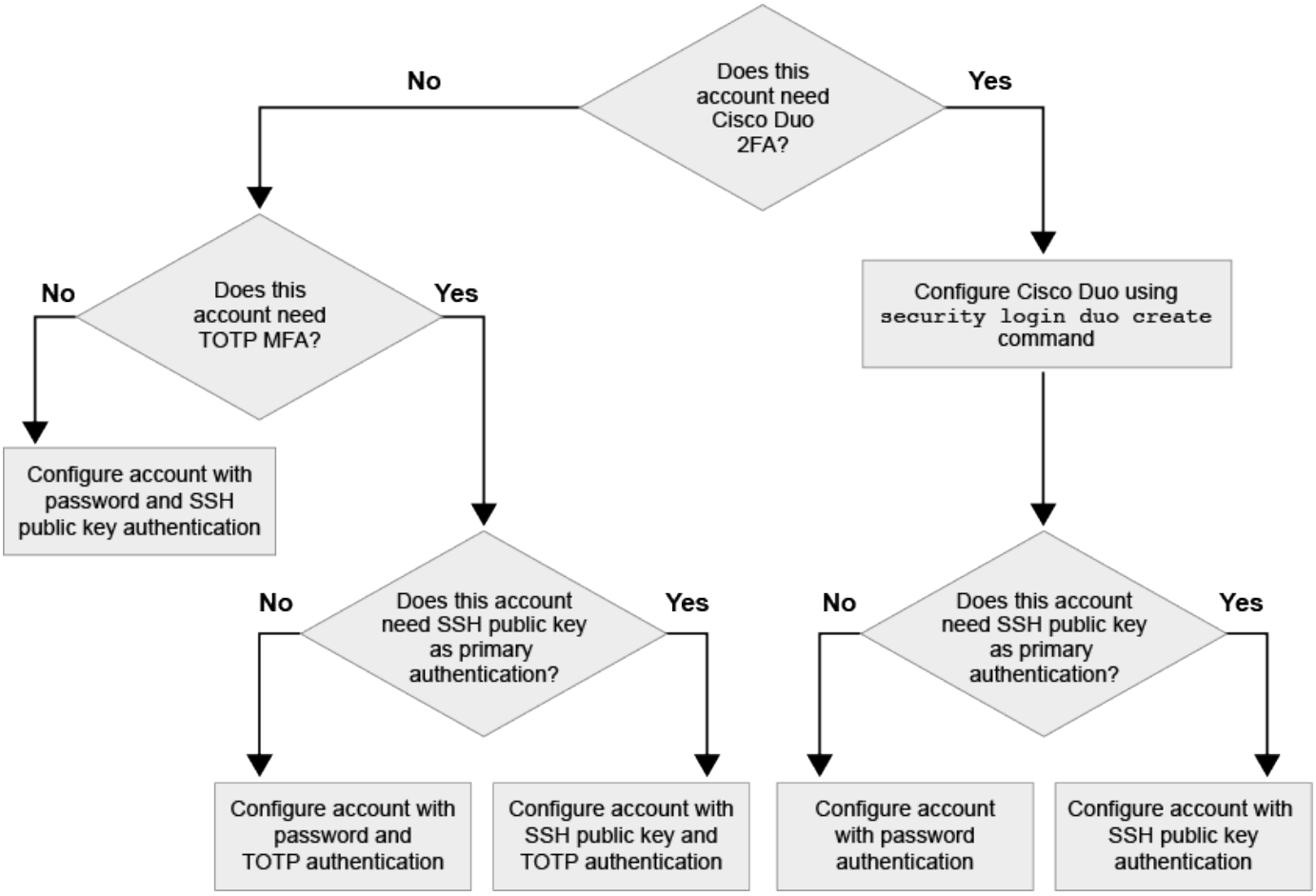
ONTAP 다단계 인증에 대해 알아보십시오

다단계 인증(MFA)을 사용하면 사용자에게 관리자 또는 데이터 스토리지 VM에 로그인하기 위한 두 가지 인증 방법을 제공하도록 요구하여 보안을 강화할 수 있습니다.

ONTAP 버전에 따라 다단계 인증을 위해 SSH 공개 키, 사용자 암호 및 시간 기반 TOTP(일회성 암호)를 함께 사용할 수 있습니다. Cisco Duo(ONTAP 9.14.1 이상)를 활성화 및 구성하면 모든 사용자에 대한 기존 방법을 보완하는 추가 인증 방법으로 사용됩니다.

다음으로 시작...	첫 번째 인증 방법입니다	두 번째 인증 방법입니다
ONTAP 9.14.1	SSH 공개 키	토TP
	사용자 암호	토TP
	SSH 공개 키	Cisco 듀오
	사용자 암호입니다	Cisco 듀오
ONTAP 9.13.1	SSH 공개 키	토TP
	사용자 암호입니다	토TP
ONTAP 9.3	SSH 공개 키	사용자 암호입니다

MFA가 구성된 경우 클러스터 관리자가 먼저 로컬 사용자 계정을 사용하도록 설정한 다음 로컬 사용자가 계정을 구성해야 합니다.



SSH 및 **TOTP**를 통해 **ONTAP** 다단계 인증을 활성화합니다

다단계 인증(MFA)을 사용하면 사용자가 admin 또는 data SVM에 로그인하기 위한 두 가지 인증 방법을 제공하도록 요구하여 보안을 강화할 수 있습니다.

이 작업에 대해

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 로그인 계정에 할당하려는 액세스 제어 역할이 확실하지 않은 경우 명령을 사용하여 나중에 역할을 추가할 수 `security login modify` 있습니다.

  에 대한 자세한 내용은 `security login modify` "ONTAP 명령 참조입니다"을 참조하십시오.

  "관리자에게 할당된 역할 수정"

- 인증을 위해 공개 키를 사용하는 경우, 계정이 SVM에 액세스하려면 먼저 공개 키를 계정에 연결해야 합니다.

  "공개 키를 사용자 계정에 연결합니다"

  계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- ONTAP 9.12.1부터 FIDO2(Fast Identity Online) 또는 PIV(Personal Identity Verification) 인증 표준을 사용하여 SSH 클라이언트 MFA에 Yubikey 하드웨어 인증 장치를 사용할 수 있습니다.

SSH 공개 키 및 사용자 암호로 MFA를 사용하도록 설정합니다

ONTAP 9.3부터 클러스터 관리자는 SSH 공개 키 및 사용자 암호를 사용하여 MFA로 로그인하도록 로컬 사용자 계정을 설정할 수 있습니다.

1. SSH 공개 키 및 사용자 암호를 사용하여 로컬 사용자 계정에서 MFA를 사용하도록 설정합니다.

```
security login create -vserver <svm_name> -user-or-group-name
<user_name> -application ssh -authentication-method <password|publickey>
-role admin -second-authentication-method <password|publickey>
```

다음 명령을 수행하려면 미리 정의된 "admin" 역할을 가진 SVM 관리자 계정 "admin2"가 SSH 공개 키와 사용자 암호를 사용하여 SVM "engData1"에 로그인해야 합니다.

```
cluster-1::> security login create -vserver engData1 -user-or-group-name
admin2 -application ssh -authentication-method publickey -role admin
-second-authentication-method password

Please enter a password for user 'admin2':
Please enter it again:
Warning: To use public-key authentication, you must create a public key
for user "admin2".
```

에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

TOTP로 MFA를 활성화합니다

ONTAP 9.13.1 부터는 로컬 사용자가 SSH 공개 키 또는 사용자 암호와 TOTP(Time-Based One-Time Password)를 사용하여 admin 또는 data SVM에 로그인하도록 하여 보안을 강화할 수 있습니다. TOTP로 MFA에 대해 계정을 활성화한 후 로컬 사용자는 에 로그인해야 합니다 "구성을 완료합니다".

TOTP는 현재 시간을 사용하여 1회 암호를 생성하는 컴퓨터 알고리즘입니다. TOTP를 사용하는 경우 SSH 공개 키 또는 사용자 암호 뒤에 항상 두 번째 인증 형태입니다.

시작하기 전에

이러한 작업을 수행하려면 스토리지 관리자여야 합니다.

단계

사용자 암호 또는 SSH 공개 키를 사용하여 MFA를 에 설정하고 TOTP를 두 번째 인증 방법으로 설정할 수 있습니다.

사용자 암호 및 **TOTP**로 **MFA**를 활성화합니다

1. 사용자 암호 및 TOTP를 사용하여 다단계 인증을 위한 사용자 계정을 활성화합니다.

   ◦ 신규 사용자 계정의 경우 *

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   ◦ 기존 사용자 계정의 경우 *

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. TOTP로 MFA가 활성화되었는지 확인합니다.

   ```
   security login show
   ```

SSH 공개 키 및 **TOTP**로 **MFA**를 활성화합니다

1. SSH 공개 키 및 TOTP를 사용하여 다단계 인증을 위한 사용자 계정을 활성화합니다.

   ◦ 신규 사용자 계정의 경우 *

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role>
   -comment <comment>
   ```

   ◦ 기존 사용자 계정의 경우 *

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   +
   에 대한 자세한 내용은 `security login modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. TOTP로 MFA가 활성화되었는지 확인합니다.

```
security login show
```

에 대한 자세한 내용은 `security login show` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

- 공개 키를 관리자 계정에 연결하지 않은 경우, 계정이 SVM에 액세스하려면 먼저 연결해야 합니다.

  "공개 키를 사용자 계정과 연결"

- TOTP로 MFA 구성을 완료하려면 로컬 사용자가 로그인해야 합니다.

  "TOTP로 MFA에 대한 로컬 사용자 계정을 구성합니다"

관련 정보

- "ONTAP 9의 다단계 인증(TR-4647)"
- "ONTAP 명령 참조입니다"

TOTP를 사용하여 **MFA**에 대한 로컬 **ONTAP** 사용자 계정을 구성합니다

ONTAP 9.13.1부터 TOTP(시간 기반 일회성 암호)를 사용하여 다단계 인증(MFA)으로 사용자 계정을 구성할 수 있습니다.

시작하기 전에

- 스토리지 관리자는 을(를) 사용해야 합니다 "TOTP로 MFA를 활성화합니다" 사용자 계정에 대한 두 번째 인증 방법입니다.
- 기본 사용자 계정 인증 방법은 사용자 암호 또는 공용 SSH 키여야 합니다.
- TOTP 앱이 스마트폰과 연동되도록 구성하고 TOTP 비밀 키를 만들어야 합니다.

  Microsoft Authenticator, Google Authenticator, Authy 및 기타 TOTP 호환 인증기가 지원됩니다.

단계

1. 현재 인증 방법으로 사용자 계정에 로그인합니다.

   현재 인증 방법은 사용자 암호 또는 SSH 공개 키여야 합니다.

2. 계정에 TOTP 구성을 생성합니다.

```
security login totp create -vserver "<svm_name>" -username
"<account_username >"
```

3. TOTP 구성이 계정에서 활성화되어 있는지 확인합니다.

```
security login totp show -vserver "<svm_name>" -username
"<account_username>"
```

관련 정보

- "보안 로그인 totp create"
- "보안 로그인 totp show"

ONTAP 사용자 계정에 대한 **TOTP** 비밀 키를 재설정합니다

계정 보안을 보호하려면 TOTP 비밀 키가 손상되었거나 손실된 경우 이를 비활성화하고 새 키를 만들어야 합니다.

키가 손상된 경우 **TOTP**를 재설정합니다

TOTP 비밀 키가 손상되었지만 여전히 액세스할 수 있는 경우 손상된 키를 제거하고 새 키를 만들 수 있습니다.

1. 사용자 암호 또는 SSH 공개 키 및 손상된 TOTP 비밀 키를 사용하여 사용자 계정에 로그인합니다.
2. 손상된 TOTP 암호 키를 제거합니다.

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. 새 TOTP 암호 키 생성:

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. TOTP 구성이 계정에서 활성화되어 있는지 확인합니다.

```
security login totp show -vserver <svm_name> -username
<account_username>
```

키를 분실한 경우 **TOTP**를 재설정합니다

TOTP 암호 키가 분실된 경우 스토리지 관리자에게 문의하십시오 "키를 사용하지 않도록 설정합니다". 키를 비활성화한 후 첫 번째 인증 방법을 사용하여 새 TOTP에 로그인하고 구성할 수 있습니다.

시작하기 전에

TOTP 암호 키는 스토리지 관리자가 해제해야 합니다. 저장소 관리자 계정이 없는 경우 저장소 관리자에게 문의하여 키를 사용하지 않도록 설정합니다.

단계

1. 스토리지 관리자가 TOTP 암호를 비활성화한 후 기본 인증 방법을 사용하여 로컬 계정에 로그인합니다.
2. 새 TOTP 암호 키 생성:

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. TOTP 구성이 계정에서 활성화되어 있는지 확인합니다.

```
security login totp show -vserver <svm_name> -username
<account_username>
```

관련 정보

- "보안 로그인 totp create"
- "보안 로그인 totp 삭제"
- "보안 로그인 totp show"

ONTAP 사용자 계정에 대해 **TOTP** 비밀 키를 비활성화합니다

로컬 사용자의 TOTP(Time-based One-Time Password) 비밀 키를 분실한 경우 저장소 관리자가 손실된 키를 비활성화해야 새 TOTP 비밀 키를 생성할 수 있습니다.

이 작업에 대해

이 작업은 클러스터 관리자 계정에서만 수행할 수 있습니다.

단계

1. TOTP 암호 키 비활성화:

```
security login totp modify -vserver <svm_name> -username
<account_username> -enabled false
```

에 대한 자세한 내용은 `security login totp modify` "ONTAP 명령 참조입니다"을 참조하십시오.

SSL 인증서 **ONTAP** 계정 액세스를 활성화합니다

명령을 사용하여 관리자 계정이 SSL 인증서를 통해 관리자 또는 데이터 SVM에 액세스하도록 설정할 수 있습니다 `security login create`.

이 작업에 대해

- 계정이 SVM에 액세스하려면 CA 서명 서버 디지털 인증서를 설치해야 합니다.

  CA 서명 서버 인증서 생성 및 설치

계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- 로그인 계정에 할당할 액세스 제어 역할을 잘 모르는 경우 나중에 '보안 로그인 수정' 명령을 사용하여 역할을 추가할 수 있습니다.

  관리자에게 할당된 역할 수정

> 클러스터 관리자 계정의 경우 에서 인증서 인증이 지원됩니다 `http`, `ontapi`, 및 `rest` 응용 프로그램. SVM 관리자 계정의 경우 인증서 인증은 을 통해서만 지원됩니다 `ontapi` 및 `rest` 응용 프로그램.

단계

1. 로컬 관리자 계정이 SSL 인증서를 사용하여 SVM에 액세스할 수 있도록 지원:

   '보안 로그인 생성 - vserver SVM_name -user -or -group -name user_or_group_name -application application application -AuthMethod authentication_method -role role role-comment'

   다음 명령을 실행하면 SSL 디지털 인증서를 사용하여 SVM "engData2"에 액세스할 수 있는 기본 "vsadmin" 역할을 가진 SVM 관리자 계정 'vmadmin2'가 활성화됩니다.

   ```
   cluster1::>security login create -vserver engData2 -user-or-group-name
   svmadmin2 -application ontapi -authmethod cert
   ```

   에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

CA 서명 서버 디지털 인증서를 설치하지 않은 경우 계정이 SVM에 액세스하려면 먼저 인증서를 설치해야 합니다.

CA 서명 서버 인증서 생성 및 설치

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

Active Directory ONTAP 계정 액세스를 설정합니다

명령을 사용하여 AD(Active Directory) 사용자 또는 그룹 계정을 활성화하여 관리자 또는 데이터 SVM에 액세스할 수 있습니다 `security login create`. AD 그룹의 모든 사용자는 그룹에 할당된 역할을 통해 SVM에 액세스할 수 있습니다.

이 작업에 대해

- 계정이 SVM에 액세스하려면 먼저 클러스터 또는 SVM에 대한 AD 도메인 컨트롤러 액세스를 구성해야 합니다.

  Active Directory 도메인 컨트롤러 액세스 구성

  계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- ONTAP 9.13.1 부터는 SSH 공개 키를 AD 사용자 암호와 함께 기본 또는 보조 인증 방법으로 사용할 수 있습니다.

  SSH 공개 키를 기본 인증으로 사용하도록 선택하면 AD 인증이 수행되지 않습니다.

- ONTAP 9.11.1부터 AD LDAP 서버에서 지원되는 경우 를 사용할 수 "ONTAP NFS SVM에 대한 nsswitch 인증을 위해 LDAP 빠른 바인딩을 사용합니다."있습니다.
- 로그인 계정에 할당하려는 액세스 제어 역할이 확실하지 않은 경우 명령을 사용하여 나중에 역할을 추가할 수 `security login modify` 있습니다.

  에 대한 자세한 내용은 `security login modify` "ONTAP 명령 참조입니다"을 참조하십시오.

  관리자에게 할당된 역할 수정

AD 그룹 계정 액세스는 에서만 지원됩니다 `SSH`, `ontapi`, 및 `rest` 응용 프로그램. 다단계 인증에는 일반적으로 사용되는 SSH 공개 키 인증에서는 AD 그룹이 지원되지 않습니다.

시작하기 전에

- 클러스터 시간은 AD 도메인 컨트롤러에서 5분 이내에 에 동기화되어야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. AD 사용자 또는 그룹 관리자 계정을 사용하여 SVM에 액세스:
   - AD 사용자용: *

ONTAP 버전	기본 인증	보조 인증	명령
9.13.1 이상	공개 키	없음	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

ONTAP 버전	기본 인증	보조 인증	명령

9.13.1 이상	도메인	공개 키	• 신규 사용자용 *
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			• 기존 사용자의 경우 *
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

9.0 이상	도메인	없음	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

AD 그룹의 경우 *

ONTAP 버전입니다	기본 인증	보조 인증	명령
9.0 이상	도메인	없음	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

작업을 마친 후

AD 도메인 컨트롤러를 클러스터 또는 SVM에 액세스하도록 구성하지 않은 경우 계정이 SVM에 액세스하려면 먼저 액세스 권한을 구성해야 합니다.

Active Directory 도메인 컨트롤러 액세스 구성

관련 정보

- "보안 로그인 생성"

LDAP 또는 **NIS ONTAP** 계정 액세스를 설정합니다

명령을 사용하여 LDAP 또는 NIS 사용자 계정을 사용하여 관리자 또는 데이터 SVM에 액세스할 수 있도록 설정할 수 있습니다 `security login create`. SVM에 대한 LDAP 또는 NIS 서버 액세스를 구성하지 않은 경우, 계정이 SVM에 액세스하려면 먼저 액세스 권한을 구성해야 합니다.

이 작업에 대해

- 그룹 계정은 지원되지 않습니다.
- 계정이 SVM에 액세스하려면 먼저 SVM에 대한 LDAP 또는 NIS 서버 액세스를 구성해야 합니다.

  LDAP 또는 NIS 서버 액세스를 구성합니다

  계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- 로그인 계정에 할당하려는 액세스 제어 역할이 확실하지 않은 경우 명령을 사용하여 나중에 역할을 추가할 수 `security login modify` 있습니다.

  에 대한 자세한 내용은 `security login modify` "ONTAP 명령 참조입니다"을 참조하십시오.

  관리자에게 할당된 역할 수정

- ONTAP 9.4부터 LDAP 또는 NIS 서버를 통한 원격 사용자에 대해 MFA(Multifactor Authentication)가 지원됩니다.
- ONTAP 9.11.1부터 LDAP 서버에서 지원되는 경우 를 사용할 수 "ONTAP NFS SVM에 대한 nsswitch 인증을 위해 LDAP 빠른 바인딩을 사용합니다."있습니다.
- 알려진 LDAP 문제로 인해 LDAP 사용자 계정 정보 필드(예: "gecos", "userPassword" 등)에 ":"(콜론) 문자를 사용해서는 안 됩니다. 그렇지 않으면 해당 사용자에 대한 조회 작업이 실패합니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. LDAP 또는 NIS 사용자 또는 그룹 계정을 사용하여 SVM에 액세스:

   'security login create - vserver SVM_name -user -or -group -name user_name -application application -AuthMethod nsswitch -role role -comment comment comment -is -ns -switch -group yes | no [-is -ldap -fastbind true]'를 참조하십시오

   "로그인 계정 생성 또는 수정"

다음 명령을 실행하면 미리 정의된 백업 역할을 사용하여 LDAP 또는 NIS 클러스터 관리자 계정 guest2가 SVM "engCluster"에 액세스할 수 있습니다.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
guest2 -application ssh -authmethod nsswitch -role backup
```

에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. LDAP 또는 NIS 사용자에 대해 MFA 로그인 활성화:

```
security login modify -user-or-group-name rem_usr1 -application ssh
-authentication-method nsswitch -role admin -is-ns-switch-group no -second
-authentication-method publickey
```

인증 방법은 홍보 키로, 두 번째 인증 방식은 nsswitch로 지정할 수 있습니다.

다음 예에서는 MFA 인증이 활성화되어 있는 것을 보여 줍니다.

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

작업을 마친 후

SVM에 대한 LDAP 또는 NIS 서버 액세스를 구성하지 않은 경우, 계정이 SVM에 액세스하려면 먼저 액세스 권한을 구성해야 합니다.

LDAP 또는 NIS 서버 액세스를 구성합니다

관련 정보

- "보안 로그인"

액세스 제어 역할을 관리합니다

ONTAP 액세스 제어 역할 관리에 대해 알아봅니다

관리자에게 할당된 역할에 따라 관리자가 액세스할 수 있는 명령이 결정됩니다. 관리자 계정을 만들 때 역할을 할당합니다. 필요에 따라 다른 역할을 할당하거나 사용자 지정 역할을 정의할 수 있습니다.

ONTAP 관리자에게 할당된 역할을 수정합니다

명령을 사용하여 클러스터 또는 SVM 관리자 계정의 역할을 변경할 수 있습니다 `security login modify`. 미리 정의된 역할 또는 사용자 지정 역할을 할당할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 클러스터 또는 SVM 관리자의 역할 변경:

   '보안 로그인 수정 - vserver SVM_name -user -or -group -name user_or_group_name -application application application -AuthMethod authentication_method -role role role-comment

   "로그인 계정 생성 또는 수정"

   다음 명령을 실행하면 AD 클러스터 관리자 계정 DOMAIN1\guest1 의 역할이 미리 정의된 "재만" 역할로 변경됩니다.

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   다음 명령을 실행하면 AD 그룹 계정 DOMAIN1\adgroup의 SVM 관리자 계정 역할이 사용자 지정 "vol_role" 역할로 변경됩니다.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

   에 대한 자세한 내용은 `security login modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 관리자를 위한 사용자 지정 역할 정의

명령을 사용하여 사용자 지정 역할을 정의할 수 `security login role create` 있습니다. 역할에 연결할 기능을 정확하게 조합하기 위해 필요한 만큼 명령을 실행할 수 있습니다.

이 작업에 대해

- 사전 정의되거나 사용자 지정되거나 관계 없이 역할은 ONTAP 명령 또는 명령 디렉터리에 대한 액세스를 허용하거나 거부합니다.

  명령 디렉토리(예: 볼륨)는 관련 명령 및 명령 하위 디렉토리 그룹입니다. 이 절차에서 설명한 경우를 제외하고 명령 디렉터리에 대한 액세스 권한을 부여하거나 거부하면 디렉터리 및 해당 하위 디렉터리의 각 명령에 대한 액세스 권한이 부여되거나 거부됩니다.

- 특정 명령 액세스 또는 하위 디렉토리 액세스는 상위 디렉토리 액세스보다 우선합니다.

  역할이 명령 디렉토리로 정의된 후 특정 명령이나 상위 디렉토리의 하위 디렉토리에 대해 다른 액세스 수준으로 다시 정의된 경우 명령 또는 하위 디렉토리에 지정된 액세스 수준이 상위 명령의 액세스 수준을 재정의합니다.

> ⓘ "admin" 클러스터 관리자만 사용할 수 있는 명령 또는 명령 디렉토리에 대한 액세스를 제공하는 SVM 관리자 역할을 할당할 수 없습니다. 예를 들어, 'security' 명령 디렉토리입니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 사용자 지정 역할 정의:

   'Security login role create -vserver SVM_name -role role -cmddirname command_or_directory_name -access access_level -query'

   다음 명령을 실행하면 'volume' 명령 디렉토리의 명령에 대한 'vol_role' 역할이 전체 액세스되고 'volume snapshot' 하위 디렉토리의 명령에 대한 읽기 전용 액세스가 부여됩니다.

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   다음 명령어를 통해 'storage' 명령 디렉토리의 명령에 대한 'vm_storage' 역할 읽기 전용 액세스, 'storage encryption' 하위 디렉토리의 명령에 대한 액세스 권한 없음, 'storage aggregate offline' 비내장 명령에 대한 전체 액세스 권한을 부여한다.

   ```
   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage" -access readonly

   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage encryption" -access none

   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage aggregate plex offline" -access all
   ```

   에 대한 자세한 내용은 `security login role create` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "보안 로그인 역할이 생성됩니다"
- "스토리지 애그리게이트 플렉스를 오프라인 상태로 설정합니다"
- "스토리지 암호화"

ONTAP 클러스터 관리자를 위한 사전 정의된 역할입니다

클러스터 관리자를 위한 사전 정의된 역할은 대부분의 요구사항을 충족해야 합니다. 필요에 따라 사용자 지정 역할을 만들 수 있습니다. 기본적으로 클러스터 관리자에게는 미리 정의된 "admin" 역할이 할당됩니다.

다음 표에는 클러스터 관리자를 위한 사전 정의된 역할이 나와 있습니다.

이 역할은…	이 수준의 액세스 권한…	명령 또는 명령 디렉토리로 이동합니다

관리자	모두	모든 명령 디렉토리(기본값)
Admin-NO-FSA(ONTAP 9.12.1부터 사용 가능)	읽기/쓰기	• 모든 명령 디렉토리(기본값) • `security login rest-role` • `security login role`
읽기 전용	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	없음
`volume file show-disk-usage`	AutoSupport	모두
• '세트' • '시스템 노드 AutoSupport	없음	기타 모든 명령 디렉토리(기본값)
백업	모두	'vserver services ndmp'
읽기 전용	'볼륨'	없음
기타 모든 명령 디렉토리(기본값)	읽기 전용	모두

• '보안 로그인 비밀번호 사용자 계정 로컬 암호 및 키 정보 관리에만 사용됩니다 • '세트'	• ONTAP 9.8부터 읽기 전용입니다 • ONTAP 9.8 이전 버전에서는 없음	'보안'
읽기 전용	기타 모든 명령 디렉토리(기본값)	SnapLock
모두	• '세트' • '볼륨 생성' • 볼륨 수정 • `volume move` • '볼륨 쇼'	없음
• `volume move governor` • `volume move recommend`	없음	기타 모든 명령 디렉토리(기본값)
없음	없음	모든 명령 디렉토리(기본값)

AutoSupport 역할은 AutoSupport OnDemand가 사용하는 미리 정의된 AutoSupport 계정에 할당됩니다. ONTAP에서는 AutoSupport 계정을 수정하거나 삭제할 수 없습니다. 또한 ONTAP에서는 다른 사용자 계정에 'AutoSupport' 역할을 할당할 수 없습니다.

관련 정보

- "보안 로그인"
- "설정"
- "볼륨"
- "SVM 서비스 NDMP"

ONTAP SVM 관리자를 위한 사전 정의된 역할

SVM 관리자를 위한 사전 정의된 역할은 대부분의 요구사항을 충족해야 합니다. 필요에 따라 사용자 지정 역할을 만들 수 있습니다. 기본적으로 SVM 관리자는 사전 정의된 "vsadmin" 역할이 할당됩니다.

다음 표에는 SVM 관리자를 위한 사전 정의된 역할이 나와 있습니다.

역할 이름	제공합니다

vsadmin을 선택합니다	• 사용자 계정 로컬 암호 및 키 정보 관리 • 볼륨 이동을 제외한 볼륨 관리 • 할당량, qtree, 스냅샷 및 파일 관리 • LUN 관리 • 권한 있는 삭제를 제외한 SnapLock 작업 수행 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • 서비스 구성: DNS, LDAP 및 NIS • 작업 모니터링 • 네트워크 연결 및 네트워크 인터페이스 모니터링 • SVM 상태 모니터링
vsadmin - 볼륨	• 사용자 계정 로컬 암호 및 키 정보 관리 • 볼륨 이동을 제외한 볼륨 관리 • 할당량, qtree, 스냅샷 및 파일 관리 • LUN 관리 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • 서비스 구성: DNS, LDAP 및 NIS • 네트워크 인터페이스 모니터링 • SVM 상태 모니터링
vsadmin - 프로토콜	• 사용자 계정 로컬 암호 및 키 정보 관리 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • 서비스 구성: DNS, LDAP 및 NIS • LUN 관리 • 네트워크 인터페이스 모니터링 • SVM 상태 모니터링
vsadmin - 백업	• 사용자 계정 로컬 암호 및 키 정보 관리 • NDMP 작업 관리 • 복구된 볼륨을 읽기/쓰기로 만듭니다 • SnapMirror 관계 및 스냅샷 관리 • 볼륨 및 네트워크 정보 보기

vsadmin - SnapLock	• 사용자 계정 로컬 암호 및 키 정보 관리 • 볼륨 이동을 제외한 볼륨 관리 • 할당량, qtree, 스냅샷 및 파일 관리 • 권한 있는 삭제를 포함한 SnapLock 작업 수행 • 프로토콜 구성: NFS 및 SMB • 서비스 구성: DNS, LDAP 및 NIS • 작업 모니터링 • 네트워크 연결 및 네트워크 인터페이스 모니터링
vsadmin - 읽기 전용입니다	• 사용자 계정 로컬 암호 및 키 정보 관리 • SVM 상태 모니터링 • 네트워크 인터페이스 모니터링 • 볼륨 및 LUN 보기 • 서비스 및 프로토콜 보기

System Manager를 사용하여 **ONTAP** 관리자 액세스 관리

관리자에게 할당된 역할에 따라 관리자가 System Manager에서 수행할 수 있는 기능이 결정됩니다. 클러스터 관리자 및 스토리지 VM 관리자를 위한 사전 정의된 역할은 System Manager에서 제공합니다. 관리자 계정을 만들 때 역할을 할당하거나 나중에 다른 역할을 할당할 수 있습니다.

계정 액세스를 설정한 방법에 따라 다음 중 하나를 수행해야 할 수 있습니다.

- 공개 키를 로컬 계정에 연결합니다.
- CA 서명 서버 디지털 인증서를 설치합니다.
- AD, LDAP 또는 NIS 액세스를 구성합니다.

계정 액세스를 활성화하기 전이나 후에 이러한 작업을 수행할 수 있습니다.

관리자에게 역할 할당

다음과 같이 관리자에게 역할을 할당합니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. 사용자 및 역할 * 옆에 있는 을 → 선택합니다.
3. 사용자 * 아래에서 를 선택합니다 + Add .
4. 사용자 이름을 지정하고 * 역할 * 의 드롭다운 메뉴에서 역할을 선택합니다.
5. 사용자의 로그인 방법 및 암호를 지정합니다.

관리자 역할 변경

다음과 같이 관리자의 역할을 변경합니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 역할을 변경할 사용자의 이름을 선택한 다음 사용자 이름 옆에 나타나는 을 클릭합니다 ⋮ .
3. 편집 * 을 클릭합니다.
4. 드롭다운 메뉴에서 * 역할 * 의 역할을 선택합니다.

ONTAP 에서 **JIT** 권한 상승에 액세스

ONTAP 9.17.1부터 클러스터 관리자는 다음을 수행할 수 있습니다. "JIT(Just-In-Time) 권한 상승 구성" ONTAP 사용자가 특정 작업을 수행할 수 있도록 일시적으로 권한을 상승시킬 수 있도록 합니다. JIT가 사용자에 대해 구성된 경우, 사용자는 작업을 수행하는 데 필요한 권한이 있는 역할로 일시적으로 권한을 상승시킬 수 있습니다. 세션이 만료되면 사용자는 원래 액세스 수준으로 돌아갑니다.

클러스터 관리자는 사용자가 JIT 권한 상승에 액세스할 수 있는 기간을 구성할 수 있습니다. 예를 들어, 클러스터 관리자는 사용자 권한 상승에 대한 액세스를 세션당 30분(세션 유효 기간)으로 설정하고 30일(JIT 유효 기간) 동안 사용할 수 있도록 구성할 수 있습니다. 30일 동안 사용자는 필요한 만큼 권한을 상승시킬 수 있지만, 각 세션은 30분으로 제한됩니다.

이 작업에 대해

- JIT 권한 승격은 SSH를 통해 ONTAP 에 액세스하는 사용자에게만 제공됩니다. 승격된 권한은 현재 SSH 세션 내에서만 사용할 수 있지만, 필요한 만큼의 동시 SSH 세션 내에서 권한을 승격할 수 있습니다.
- JIT 권한 승격은 비밀번호, nsswitch 또는 도메인 인증을 사용하여 로그인하는 사용자에게만 지원됩니다. 다중 요소 인증(MFA)은 JIT 권한 승격에 지원되지 않습니다.
- 구성된 세션 또는 JIT 유효 기간이 만료되거나 클러스터 관리자가 사용자의 JIT 액세스 권한을 취소하면 사용자의 JIT 세션이 종료됩니다.

시작하기 전에

- JIT 권한 승격에 액세스하려면 클러스터 관리자가 사용자 계정에 대한 JIT 액세스를 구성해야 합니다. 클러스터 관리자는 권한을 승격할 수 있는 역할과 승격된 권한에 액세스할 수 있는 기간을 결정합니다.

단계

1. 구성된 역할에 대한 권한을 일시적으로 상승시킵니다.

```
security jit-privilege elevate
```

   이 명령을 입력하면 로그인 비밀번호를 입력하라는 메시지가 표시됩니다. 계정에 JIT 액세스가 구성된 경우, 설정된 세션 기간 동안 권한이 상승됩니다. 세션 기간이 만료되면 원래 액세스 수준으로 돌아갑니다. 설정된 JIT 유효 기간 내에 필요한 만큼 권한을 상승시킬 수 있습니다.

2. JIT 세션의 남은 시간을 확인하세요.

```
security jit-privilege show-remaining-time
```

현재 JIT 세션에 있는 경우 이 명령은 남은 시간을 표시합니다.

3. 필요한 경우 JIT 세션을 일찍 종료하세요.

```
security jit-privilege reset
```

현재 JIT 세션에 있는 경우 이 명령을 실행하면 JIT 세션이 종료되고 원래 액세스 수준이 복원됩니다.

ONTAP 에서 JIT 권한 상승 구성

ONTAP 9.17.1부터 클러스터 관리자는 JIT(Just-In-Time) 권한 상승을 구성하여 ONTAP 사용자가 특정 작업을 수행할 수 있도록 일시적으로 권한을 상승시킬 수 있습니다. JIT가 사용자에 대해 구성된 경우, "그들의 특권을 높이다" 작업을 수행하는 데 필요한 권한이 있는 역할로 전환됩니다. 세션 기간이 만료되면 사용자는 원래 액세스 수준으로 돌아갑니다.

클러스터 관리자는 사용자가 JIT 권한 상승에 액세스할 수 있는 기간을 구성할 수 있습니다. 예를 들어, 사용자 JIT 권한 상승 액세스를 세션당 30분(세션 유효 기간)으로 설정하고 30일(JIT 유효 기간) 동안 사용할 수 있도록 구성할 수 있습니다. 30일 동안 사용자는 필요한 만큼 권한을 상승시킬 수 있지만, 각 세션은 30분으로 제한됩니다.

JIT 권한 승격은 최소 권한 원칙을 지원하여 사용자가 승격된 권한이 필요한 작업을 수행할 때 해당 권한을 영구적으로 부여하지 않아도 되도록 합니다. 이를 통해 무단 접근이나 실수로 인한 시스템 변경 위험을 줄일 수 있습니다. 다음 예시에서는 JIT 권한 승격의 일반적인 사용 사례를 설명합니다.

- 임시 액세스를 허용합니다. `security login create` 그리고 `security login delete` 사용자의 온보딩 및 오프보딩을 가능하게 하는 명령입니다.
- 임시 액세스 허용 `system node image update` 그리고 `system node upgrade-revert` 업데이트 기간 동안. 업데이트가 완료되면 명령 액세스가 취소됩니다.
- 임시 액세스 허용 `cluster add-node` , `cluster remove-node` , 그리고 `cluster modify` 클러스터 확장 또는 재구성을 활성화합니다. 클러스터 변경이 완료되면 명령 액세스가 취소됩니다.
- 임시 액세스 허용 `volume snapshot restore` 복원 작업 및 백업 대상 관리를 활성화합니다. 복원 또는 구성이 완료되면 명령 액세스 권한이 취소됩니다.
- 임시 액세스 허용 `security audit log show` 규정 준수 검사 중에 감사 로그 검토 및 내보내기를 활성화합니다.

일반적인 JIT 사용 사례에 대한 더 자세한 목록은 다음을 참조하세요. 일반적인 JIT 사용 사례 .

클러스터 관리자는 ONTAP 사용자에 대한 JIT 액세스를 설정하고, 클러스터 전체 또는 특정 SVM에 대해 기본 JIT 유효 기간을 구성할 수 있습니다.

이 작업에 대해

- JIT 권한 승격은 SSH를 통해 ONTAP 에 액세스하는 사용자에게만 제공됩니다. 승격된 권한은 사용자의 현재 SSH 세션 내에서만 사용할 수 있지만, 필요한 만큼의 동시 SSH 세션 내에서 권한을 승격할 수 있습니다.
- JIT 권한 승격은 비밀번호, nsswitch 또는 도메인 인증을 사용하여 로그인하는 사용자에게만 지원됩니다. 다중 요소

인증(MFA)은 JIT 권한 승격에 지원되지 않습니다.

시작하기 전에

- ONTAP 클러스터 관리자여야 합니다. `admin` 다음 작업을 수행하기 위한 권한 수준입니다.

글로벌 JIT 설정 수정

ONTAP 클러스터 전체 또는 특정 SVM에 대해 기본 JIT 설정을 수정할 수 있습니다. 이러한 설정은 JIT 액세스 권한이 구성된 사용자의 기본 세션 유효 기간과 최대 JIT 유효 기간을 결정합니다.

이 작업에 대해

- 기본값 `default-session-validity-period` 값은 1시간입니다. 이 설정은 사용자가 JIT 세션에서 상승된 권한에 액세스할 수 있는 시간을 결정합니다. 이 시간이 지나면 다시 상승해야 합니다.
- 기본값 `max-jit-validity-period` 값은 90일입니다. 이 설정은 구성된 시작일 이후 사용자가 JIT 권한 상승에 액세스할 수 있는 최대 기간을 결정합니다. 개별 사용자별로 JIT 유효 기간을 설정할 수 있지만, 최대 JIT 유효 기간을 초과할 수 없습니다.

단계

1. 현재 JIT 설정을 확인하세요.

```
security jit-privilege show -vserver <svm_name>
```

`-vserver` 는 선택 사항입니다. SVM을 지정하지 않으면 명령은 전역 JIT 설정을 표시합니다.

2. JIT 설정을 전역적으로 또는 SVM에 대해 수정합니다.

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

SVM을 지정하지 않으면 명령이 전역 JIT 설정을 수정합니다. 다음 예제는 SVM의 기본 JIT 세션 기간을 45분으로, 최대 JIT 기간을 30일로 설정합니다. `svm1` :

```
security jit-privilege modify -vserver svm1 -default-session-validity-period
45m -max-jit-validity-period 30d
```

이 예에서 사용자는 한 번에 45분 동안 JIT 권한 상승에 액세스할 수 있으며 구성된 시작 날짜로부터 최대 30일 동안 JIT 세션을 시작할 수 있습니다.

사용자에 대한 JIT 권한 승격 액세스 구성

ONTAP 사용자에게 JIT 권한 상승 액세스를 할당할 수 있습니다.

단계

1. 사용자의 현재 JIT 액세스를 확인하세요.

```
security jit-privilege user show -username <username>
```

`-username` 는 선택 사항입니다. 사용자 이름을 지정하지 않으면 모든 사용자의 JIT 액세스 권한이 표시됩니다.

2. 사용자에게 새로운 JIT 액세스 권한 할당:

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

   - 만약에 `-vserver` 지정되지 않으면 JIT 액세스는 클러스터 수준에서 할당됩니다.
   - `-role` 사용자가 승격될 RBAC 역할입니다. 지정하지 않으면 `-role` 기본값으로 설정됨 `admin` .
   - `-session-validity-period` 사용자가 새 JIT 세션을 시작하기 전에 승격된 역할에 액세스할 수 있는 기간입니다. 지정하지 않으면 전역 또는 SVM `default-session-validity-period` 사용됩니다.
   - `-jit-validity-period` 구성된 시작 날짜 이후 사용자가 JIT 세션을 시작할 수 있는 최대 기간입니다. 지정하지 않으면 `session-validity-period` 사용됩니다. 이 매개변수는 전역 또는 SVM을 초과할 수 없습니다. `max-jit-validity-period` .
   - `-start-time` 사용자가 JIT 세션을 시작할 수 있는 날짜와 시간입니다. 지정하지 않으면 현재 날짜와 시간이 사용됩니다.

     다음 예제에서는 다음을 허용합니다. `ontap_user` 에 접근하려면 `admin` 새로운 JIT 세션을 시작하기 전에 1시간 동안 역할을 수행해야 합니다. `ontap_user` 2025년 7월 1일 오후 1시부터 60일 동안 JIT 세션을 시작할 수 있습니다.
     `security jit-privilege user create -username ontap_user -role admin -session -validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"`

3. 필요한 경우 사용자의 JIT 액세스를 취소합니다.

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

사용자의 JIT 액세스를 취소합니다. `-vserver` 지정되지 않으면 JIT 액세스가 클러스터 수준에서 취소됩니다. 사용자가 활성 JIT 세션에 있는 경우 세션이 종료됩니다.

일반적인 **JIT** 사용 사례

다음 표에는 JIT 권한 승격의 일반적인 사용 사례가 나와 있습니다. 각 사용 사례에 대해 관련 명령에 대한 액세스를 제공하도록 RBAC 역할을 구성해야 합니다. 각 명령은 ONTAP 명령 참조에 연결되어 있으며, 해당 명령 및 매개변수에 대한 자세한 정보를 제공합니다.

사용 사례	명령	세부
사용자 및 역할 관리	• '보안 로그인 생성' • '보안 로그인 삭제	온보딩 또는 오프보딩 중에 사용자를 추가/제거하거나 역할을 변경하기 위해 일시적으로 권한을 상승시킵니다.

사용 사례	명령	세부
인증서 관리	• `security certificate create` • `security certificate install`	인증서 설치 또는 갱신을 위해 단기 액세스 권한을 부여합니다.
SSH/CLI 액세스 제어	• `security login create -application ssh`	문제 해결이나 공급업체 지원을 위해 일시적으로 SSH 액세스를 허용합니다.
라이센스 관리	• `system license add` • `system license delete`	기능 활성화 또는 비활성화 중에 라이선스를 추가하거나 제거할 수 있는 권한을 부여합니다.
시스템 업그레이드 및 패치	• `system node image update` • `system node upgrade-revert`	업그레이드 창에 대한 권한을 높인 다음 취소합니다.
네트워크 보안 설정	• `security login role create` • `security login role modify`	네트워크 관련 보안 역할에 대한 임시 변경을 허용합니다.
클러스터 관리	• `cluster add-node` • `cluster remove-node` • `cluster modify`	클러스터 확장이나 재구성을 위해 Elevate를 사용합니다.
SVM 관리	• `vserver create` • `vserver delete` • `vserver modify`	SVM에 프로비저닝 또는 서비스 해제를 위한 관리자 권한을 일시적으로 부여합니다.
볼륨 관리	• '볼륨 생성' • '볼륨 삭제' • 볼륨 수정	볼륨 프로비저닝, 크기 조정 또는 제거를 위해 높이십시오.
스냅샷 관리	• '볼륨 스냅샷 생성' • '볼륨 스냅샷 삭제' • '볼륨 스냅샷 복원'	복구 중에 스냅샷을 삭제하거나 복원하려면 Elevate를 사용합니다.

사용 사례	명령	세부
네트워크 구성	• `network interface create` • `network port vlan create`	유지 관리 기간 동안 네트워크 변경에 대한 권한을 부여합니다.
디스크/집계 관리	• `storage disk assign` • `storage aggregate create` • '스토리지 집계 추가 디스크'	디스크를 추가, 제거하거나 집계를 관리하기 위해 Elevate를 사용합니다.
데이터 보호	• 스냅미러 생성 • `snapmirror modify` • `snapmirror restore`	SnapMirror 관계를 구성하거나 복원하기 위해 일시적으로 상승합니다.
성능 튜닝	• `qos policy-group create` • `qos policy-group modify`	성능 문제 해결이나 튜닝을 위해 Elevate를 활용하세요.
감사 로그 액세스	• 보안 감사 로그 쇼	규정 준수 검사 중에 감사 로그 검토 또는 내보내기를 위해 일시적으로 상승합니다.
이벤트 및 알림 관리	• `event notification create` • `event notification modify`	이벤트 알림이나 SNMP 트랩을 구성하거나 테스트하기 위해 Elevate를 사용합니다.
규정 준수 기반 데이터 액세스	• '볼륨 쇼' • 보안 감사 로그 쇼	감사자가 민감한 데이터나 로그를 검토할 수 있도록 일시적으로 읽기 전용 액세스 권한을 부여합니다.
특권 액세스 검토	• '보안 로그인 쇼' • `security login role show`	일시적으로 권한을 승격하여 권한 있는 접근 권한을 검토하고 보고합니다. 제한된 시간 동안 읽기 전용의 권한 승격된 접근 권한을 부여합니다.

관련 정보

- "클러스터"
- "이벤트 알림"
- "회로망"
- "qos 정책 그룹"
- "보안"

- "SnapMirror를 참조하십시오"
- "내부"
- "시스템"
- "볼륨"
- "SVM"

관리자 계정을 관리합니다

ONTAP 관리자 계정 관리에 대해 자세히 알아봅니다

계정 액세스를 설정한 방법에 따라 공개 키를 로컬 계정에 연결하거나, CA 서명 서버 디지털 인증서를 설치하거나, AD, LDAP 또는 NIS 액세스를 구성해야 할 수 있습니다. 계정 액세스를 활성화하기 전이나 후에 이러한 모든 작업을 수행할 수 있습니다.

공개 키를 ONTAP 관리자 계정에 연결합니다

SSH 공개 키 인증의 경우 계정에서 SVM에 액세스할 수 있으려면 먼저 공개 키를 관리자 계정과 연결해야 합니다. 명령을 사용하여 키를 관리자 계정에 연결할 수 `security login publickey create` 있습니다.

이 작업에 대해

암호 및 SSH 공개 키로 SSH를 통해 계정을 인증하면 먼저 공개 키로 계정이 인증됩니다.

시작하기 전에

- SSH 키를 생성해야 합니다.
- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. 공개 키를 관리자 계정에 연결:

   '보안 로그인 공개 키 생성 - vserver_SVM_name_-username_user_name_-index_index_-publickey_certificate_-comment_comment_'

   에 대한 자세한 내용은 `security login publickey create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 공개 키를 확인하여 변경 사항을 확인합니다.

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

   에 대한 자세한 내용은 `security login publickey show` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 명령을 실행하면 공용 키가 SVM 관리자 계정에 연결됩니다 `svmadmin1` SVM을 위해 `engData1`. 공개 키에는 인덱스 번호 5가 할당됩니다.

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

ONTAP 관리자를 위한 **SSH** 공개 키 및 **X.509** 인증서를 관리합니다

관리자 계정으로 SSH 인증 보안을 강화하기 위해 명령 집합을 사용하여 SSH 공개 키 및 X.509 인증서와의 연결을 관리할 수 `security login publickey` 있습니다.

공개 키와 **X.509** 인증서를 관리자 계정에 연결합니다

ONTAP 9.13.1 부터는 X.509 인증서를 관리자 계정과 연결된 공개 키와 연결할 수 있습니다. 이렇게 하면 해당 계정에 대한 SSH 로그인 시 인증서 만료 또는 해지 확인을 추가로 보호할 수 있습니다.

이 작업에 대해

SSH 공개 키와 X.509 인증서를 모두 사용하여 SSH를 통해 계정을 인증하는 경우 ONTAP는 SSH 공개 키로 인증하기 전에 X.509 인증서의 유효성을 검사합니다. 인증서가 만료되거나 해지되면 SSH 로그인이 거부되고 공개 키는 자동으로 비활성화됩니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.
- SSH 키를 생성해야 합니다.
- X.509 인증서만 만료 여부를 확인해야 하는 경우 자체 서명된 인증서를 사용할 수 있습니다.
- X.509 인증서의 만료 및 해지 여부를 확인해야 하는 경우:
  - CA(인증 기관)로부터 인증서를 받아야 합니다.
  - 명령을 사용하여 인증서 체인(중간 및 루트 CA 인증서)을 `security certificate install` 설치해야 합니다. 에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.
  - SSH용 OCSP를 활성화해야 합니다. 을 참조하십시오 "디지털 인증서가 OCSP를 사용하여 유효한지 확인합니다" 를 참조하십시오.

단계

1. 공개 키와 X.509 인증서를 관리자 계정에 연결합니다.

   ```
   security login publickey create -vserver SVM_name -username user_name -index
   index -publickey certificate -x509-certificate install
   ```

   에 대한 자세한 내용은 `security login publickey create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 공개 키를 확인하여 변경 사항을 확인합니다.

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

   에 대한 자세한 내용은 `security login publickey show` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 명령을 실행하면 공용 키와 X.509 인증서가 SVM 관리자 계정에 연결됩니다 `svmadmin2` SVM을 위해 `engData2`. 공개 키에는 인덱스 번호 6이 할당됩니다.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

관리자 계정의 SSH 공개 키에서 인증서 연결을 제거합니다

공개 키를 유지하면서 계정의 SSH 공개 키에서 현재 인증서 연결을 제거할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. 관리자 계정에서 X.509 인증서 연결을 제거하고 기존 SSH 공개 키를 유지합니다.

   ```
   security login publickey modify -vserver SVM_name -username user_name -index
   index -x509-certificate delete
   ```

   에 대한 자세한 내용은 `security login publickey modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 공개 키를 확인하여 변경 사항을 확인합니다.

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

예

다음 명령을 실행하면 SVM 관리자 계정에서 X.509 인증서 연결이 제거됩니다 `svmadmin2` SVM을 위해 `engData2` 인덱스 번호 6.

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

관리자 계정에서 공개 키 및 인증서 연결을 제거합니다

계정에서 현재 공개 키 및 인증서 구성을 제거할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. 관리자 계정에서 공개 키와 X.509 인증서 연결을 제거합니다.

```
security login publickey delete -vserver SVM_name -username user_name -index
index
```

에 대한 자세한 내용은 `security login publickey delete` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 공개 키를 확인하여 변경 사항을 확인합니다.

```
security login publickey show -vserver SVM_name -username user_name -index
index
```

예

다음 명령을 실행하면 SVM 관리자 계정에서 공개 키와 X.509 인증서가 제거됩니다 `svmadmin3` SVM을 위해 `engData3` 인덱스 번호 7.

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

관련 정보

- "보안 로그인 공개키"

ONTAP SSH 로그인에 대해 **Cisco Duo 2FA**를 구성합니다

ONTAP 9.14.1부터 SSH 로그인 시 2FA(2단계 인증)에 Cisco Duo를 사용하도록 ONTAP를 구성할 수 있습니다. 클러스터 수준에서 Duo를 구성하면 기본적으로 모든 사용자 계정에 적용됩니다. 또는 스토리지 VM(이전에는 가상 머신이라고 함) 레벨에서 Duo를 구성할 수 있습니다. 이 경우 스토리지 VM의 사용자에게만 적용됩니다. Duo를 활성화하고 구성하면 모든 사용자에 대한 기존 방법을 보완하는 추가 인증 방법으로 사용됩니다.

SSH 로그인에 대해 Duo 인증을 사용하는 경우 사용자는 다음에 SSH를 사용하여 로그인할 때 장치를 등록해야 합니다. 등록 정보는 Cisco Duo를 참조하십시오 "등록 문서".

ONTAP 명령줄 인터페이스를 사용하여 Cisco Duo에서 다음 작업을 수행할 수 있습니다.

- Cisco Duo를 구성합니다
- Cisco Duo 구성을 변경합니다
- Cisco Duo 구성을 제거합니다
- Cisco Duo 구성을 봅니다
- Duo 그룹을 제거합니다
- Duo 그룹 보기
- 사용자를 위한 Duo 인증 우회

Cisco Duo를 구성합니다

명령을 사용하여 전체 클러스터 또는 특정 스토리지 VM(ONTAP CLI에서 가상 서버라고 함)에 대한 Cisco Duo 구성을 생성할 수 있습니다 `security login duo create`. 이렇게 하면 이 클러스터 또는 스토리지 VM에 대한 SSH

로그인에 Cisco Duo가 활성화됩니다. 에 대한 자세한 내용은 `security login duo create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. Cisco Duo Admin Panel에 로그인합니다.
2. 애플리케이션 > UNIX 애플리케이션 * 으로 이동합니다.
3. 통합 키, 비밀 키 및 API 호스트 이름을 기록합니다.
4. SSH를 사용하여 ONTAP 계정에 로그인합니다.
5. 이 스토리지 VM에 대해 Cisco Duo 인증을 사용하도록 설정하고, 환경 정보를 괄호 안의 값으로 대체합니다.

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

Cisco Duo 구성을 변경합니다

Cisco Duo가 사용자를 인증하는 방법(예: 받은 인증 프롬프트 수 또는 사용된 HTTP 프록시)을 변경할 수 있습니다. 스토리지 VM(ONTAP CLI에서 가상 서버로 지칭)에 대한 Cisco Duo 구성을 변경해야 하는 경우 명령을 사용할 수 있습니다 `security login duo modify`. 에 대한 자세한 내용은 `security login duo modify` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. Cisco Duo Admin Panel에 로그인합니다.
2. 애플리케이션 > UNIX 애플리케이션 * 으로 이동합니다.
3. 통합 키, 비밀 키 및 API 호스트 이름을 기록합니다.
4. SSH를 사용하여 ONTAP 계정에 로그인합니다.
5. 이 스토리지 VM에 대한 Cisco Duo 구성을 변경하여 환경의 업데이트된 정보를 괄호 안의 값으로 대체합니다.

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-max-prompts 1|2|3 \
-is-enabled true|false \
-fail-mode safe|secure
```

Cisco Duo 구성을 제거합니다

Cisco Duo 구성을 제거하면 SSH 사용자가 로그인할 때 Duo를 사용하여 인증할 필요가 없습니다. 스토리지 VM(ONTAP CLI에서 가상 서버로 지칭)에 대한 Cisco Duo 구성을 제거하려면 명령을 사용합니다 `security login duo delete`. 에 대한 자세한 내용은 `security login duo delete` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 스토리지 VM 이름을 로 대체하여 이 스토리지 VM에 대한 Cisco Duo 구성을 제거합니다 `<STORAGE_VM_NAME>`:

```
security login duo delete  -vserver <STORAGE_VM_NAME>
```

이렇게 하면 이 스토리지 VM에 대한 Cisco Duo 구성이 영구적으로 삭제됩니다.

Cisco Duo 구성을 봅니다

명령을 사용하여 스토리지 VM(ONTAP CLI에서 가상 서버로 지칭)에 대한 기존 Cisco Duo 구성을 볼 수 있습니다 `security login duo show`. 에 대한 자세한 내용은 `security login duo show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 이 스토리지 VM에 대한 Cisco Duo 구성을 표시합니다. 필요한 경우 를 사용할 수 있습니다 `vserver` 스토리지 VM 이름을 로 대체하는 스토리지 VM을 지정하는 매개 변수입니다 `<STORAGE_VM_NAME>`:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

다음과 유사한 출력이 표시됩니다.

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

Duo 그룹을 생성합니다

Cisco Duo에 특정 Active Directory, LDAP 또는 로컬 사용자 그룹의 사용자만 Duo 인증 프로세스에 포함하도록 지시할 수 있습니다. Duo 그룹을 생성하는 경우 해당 그룹의 사용자만 Duo 인증을 요구합니다. 명령을 사용하여 Duo 그룹을 생성할 수 `security login duo group create` 있습니다. 그룹을 생성할 때 필요에 따라 해당 그룹의 특정 사용자를 Duo 인증 프로세스에서 제외할 수 있습니다. 에 대한 자세한 내용은 `security login duo group create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 환경의 정보를 대괄호로 묶은 값으로 대체하여 Duo 그룹을 만듭니다. 를 생략할 경우 `-vserver` 매개 변수로, 그룹이 클러스터 레벨에서 생성됩니다.

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

Duo 그룹의 이름은 Active Directory, LDAP 또는 로컬 그룹과 일치해야 합니다. 선택적 매개 변수로 지정한 사용자는 `-excluded-users` Duo 인증 프로세스에 포함되지 않습니다.

Duo 그룹 보기

명령을 사용하여 기존 Cisco Duo 그룹 항목을 볼 수 `security login duo group show` 있습니다. 에 대한 자세한 내용은 `security login duo group show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 환경의 정보를 대괄호로 묶은 값으로 대체하여 Duo 그룹 항목을 표시합니다. 를 생략할 경우 `-vserver` 매개 변수로, 그룹이 클러스터 레벨에 표시됩니다.

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

Duo 그룹의 이름은 Active Directory, LDAP 또는 로컬 그룹과 일치해야 합니다. 선택적 매개 변수로 지정한 사용자는 `-excluded-users` 표시되지 않습니다.

Duo 그룹을 제거합니다

명령을 사용하여 Duo 그룹 항목을 제거할 수 `security login duo group delete` 있습니다. 그룹을 제거하면 해당 그룹의 사용자가 Duo 인증 프로세스에 더 이상 포함되지 않습니다. 에 대한 자세한 내용은 `security login duo group delete` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. Duo 그룹 항목을 제거하여 환경의 정보를 대괄호 안의 값으로 대체합니다. 를 생략할 경우 `-vserver` 매개 변수로, 그룹이 클러스터 레벨에서 제거됩니다.

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME>
```

Duo 그룹의 이름은 Active Directory, LDAP 또는 로컬 그룹과 일치해야 합니다.

사용자를 위한 **Duo** 인증 우회

Duo SSH 인증 프로세스에서 모든 사용자 또는 특정 사용자를 제외할 수 있습니다.

모든 **Duo** 사용자를 제외합니다

모든 사용자에 대해 Cisco Duo SSH 인증을 비활성화할 수 있습니다.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. SSH 사용자에 대해 Cisco Duo 인증을 사용하지 않도록 설정하고 SVM 이름을 로 바꿉니다 `<STORAGE_VM_NAME>`:

```
security login duo modify -vserver <STORAGE_VM_NAME> -is-enabled false
```

Duo 그룹 사용자를 제외합니다

Duo 그룹에 속한 특정 사용자를 Duo SSH 인증 프로세스에서 제외할 수 있습니다.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 그룹의 특정 사용자에 대해 Cisco Duo 인증을 비활성화합니다. 제외할 그룹 이름 및 사용자 목록을 대괄호 안의 값으로 대체합니다.

```
security login duo group modify -group-name <GROUP_NAME> -excluded-users
<USER1, USER2>
```

Duo 그룹의 이름은 Active Directory, LDAP 또는 로컬 그룹과 일치해야 합니다. 매개 변수로 지정한 사용자는 `-excluded-users` Duo 인증 프로세스에 포함되지 않습니다.

에 대한 자세한 내용은 `security login duo group modify` "ONTAP 명령 참조입니다"을 참조하십시오.

로컬 **Duo** 사용자를 제외합니다

Cisco Duo Admin Panel을 사용하여 특정 로컬 사용자를 Duo 인증을 사용하지 않도록 제외할 수 있습니다. 자세한 내용은 를 참조하십시오 "Cisco Duo 설명서".

ONTAP에서 CA 서명 서버 인증서를 생성하고 설치합니다

운영 시스템에서 클러스터 또는 SVM을 SSL 서버로 인증하는 데 사용할 CA 서명 디지털 인증서를 설치하는 것이 좋습니다. 명령을 사용하여 인증서 서명 요청(CSR)을 생성하고, `security certificate install` 명령을 사용하여 인증 기관으로부터 받은 인증서를 설치할 수 `security certificate generate-csr` 있습니다. 및 `security certificate install` 에 대한 자세한 `security certificate generate-csr` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

인증서 서명 요청을 생성합니다

'Security certificate generate -csr' 명령을 사용하여 CSR(인증서 서명 요청)을 생성할 수 있습니다. 요청을 처리한 후 CA(인증 기관)에서 서명된 디지털 인증서를 보냅니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. CSR 생성:

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

다음 명령을 실행하면 미국 캘리포니아주 서니베일에 위치한 회사 부서의 `server1.companyname.com` 그룹에서 `IT` 사용할 수 있도록 해시 기능에서 `Software` 생성된 2048비트 개인 키가 포함된 CSR이 `SHA256` 생성됩니다. SVM 담당자 관리자의 이메일 주소는 입니다 `web@example.com`. 출력에 CSR과 개인 키가 표시됩니다.

CSR 생성 예

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

NOTE: Keep a copy of your certificate request and private key for
future reference.
```

2. CSR 출력에서 인증서 요청을 복사한 다음 전자 양식(예: 전자 메일)으로 신뢰할 수 있는 타사 CA로 보내 서명합니다.

   요청을 처리한 후 CA는 서명된 디지털 인증서를 보냅니다. 개인 키와 CA 서명 디지털 인증서의 복사본을 유지해야 합니다.

CA 서명 서버 인증서를 설치합니다

명령을 사용하여 SVM에 CA 서명 서버 인증서를 설치할 수 있습니다 `security certificate install`. ONTAP는 서버 인증서의 인증서 체인을 형성하는 CA(인증 기관) 루트 및 중간 인증서를 입력하라는 메시지를 표시합니다. 에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. CA 서명 서버 인증서 설치:

```
security certificate install -vserver SVM_name -type certificate_type
```

ONTAP 서버 인증서의 인증서 체인을 형성하는 CA 루트 및 중간 인증서를 입력하라는 메시지가 표시됩니다. 체인은 서버 인증서를 발급한 CA의 인증서로 시작되며 CA의 루트 인증서까지 범위가 될 수 있습니다. 누락된 중간 인증서는 서버 인증서 설치에 실패합니다.

다음 명령을 실행하면 SVM에 CA 서명 서버 인증서 및 중간 인증서를 설치합니다 `engData2`.

CA 서명 서버 인증서 중간 인증서 설치 예

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

관련 정보

- "보안 인증서 생성 - CSR"

System Manager를 사용하여 **ONTAP** 인증서를 관리합니다

ONTAP 9.10.1부터 시스템 관리자를 사용하여 신뢰할 수 있는 인증서 기관, 클라이언트/서버 인증서 및 로컬(온보드) 인증서 기관을 관리할 수 있습니다.

System Manager를 사용하면 다른 응용 프로그램에서 받은 인증서를 관리할 수 있으므로 해당 응용 프로그램의 통신을 인증할 수 있습니다. 시스템을 다른 응용 프로그램에 식별하는 고유한 인증서를 관리할 수도 있습니다.

인증서 정보를 봅니다

System Manager를 사용하면 클러스터에 저장된 신뢰할 수 있는 인증서 기관, 클라이언트/서버 인증서 및 로컬 인증서 기관을 볼 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 영역으로 스크롤합니다. 인증서 * 섹션에 다음 세부 정보가 표시됩니다.
   - 저장된 신뢰할 수 있는 인증 기관의 수입니다.
   - 저장된 클라이언트/서버 인증서 수
   - 저장된 로컬 인증 기관의 수입니다.
3. 인증서 범주에 대한 세부 정보를 보려면 숫자를 선택하고, 모든 범주에 대한 정보가 포함된 * 인증서 * 페이지를 열려면 선택합니다 → . 이 목록에는 전체 클러스터에 대한 정보가 표시됩니다. 특정 스토리지 VM에 대한 정보만 표시하려면 다음 단계를 수행하십시오.
   a. 스토리지 > 스토리지 VM * 을 선택합니다.
   b. 스토리지 VM을 선택합니다.
   c. 설정 * 탭으로 전환합니다.
   d. 인증서 * 섹션에 표시된 번호를 선택합니다.

다음 단계

- 인증서 * 페이지에서 을(를) 사용할 수 있습니다 인증서 서명 요청을 생성합니다.
- 인증서 정보는 세 개의 탭으로 구분됩니다. 각 범주마다 하나씩 있습니다. 각 탭에서 다음 작업을 수행할 수 있습니다.

이 탭에서…	다음 절차를 수행할 수 있습니다…
• 신뢰할 수 있는 인증 기관 *	• [install-trusted-cert] • 신뢰할 수 있는 인증 기관을 삭제합니다 • 신뢰할 수 있는 인증 기관을 갱신합니다

• 클라이언트/서버 인증서 *	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
• 로컬 인증 기관 *	• 새 로컬 인증 기관을 생성합니다 • 로컬 인증 기관을 사용하여 인증서에 서명합니다 • 로컬 인증 기관을 삭제합니다 • 로컬 인증 기관을 갱신합니다

인증서 서명 요청을 생성합니다

인증서 * 페이지의 아무 탭에서나 System Manager를 사용하여 CSR(인증서 서명 요청)을 생성할 수 있습니다. 개인 키와 해당하는 CSR이 생성되며, 이 키는 인증 기관을 통해 서명하여 공용 인증서를 생성할 수 있습니다.

단계

1. 인증서 * 페이지를 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. CSR 생성 * 을 선택합니다.
3. 주체 이름에 대한 정보를 입력합니다.
   a. 일반 이름 * 을 입력합니다.
   b. 국가 * 를 선택합니다.
   c. 조직 * 을 입력합니다.
   d. 조직 단위 * 를 입력합니다.
4. 기본값을 무시하려면 * 추가 옵션 * 을 선택하고 추가 정보를 제공합니다.

신뢰할 수 있는 인증 기관을 설치(추가)합니다

신뢰할 수 있는 인증 기관을 System Manager에 추가로 설치할 수 있습니다.

단계

1. 신뢰할 수 있는 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 을 + Add 선택합니다.
3. 신뢰할 수 있는 인증 기관 추가* 패널에서 다음을 수행하십시오.
   ◦ 이름 * 을 입력합니다.
   ◦ 범위 * 에서 스토리지 VM을 선택합니다.
   ◦ 일반 이름 * 을 입력합니다.
   ◦ 유형 * 을 선택합니다.
   ◦ 인증서 세부 정보 * 를 입력하거나 가져옵니다.

신뢰할 수 있는 인증 기관을 삭제합니다

System Manager를 사용하면 신뢰할 수 있는 인증 기관을 삭제할 수 있습니다.

ONTAP에 사전 설치된 신뢰할 수 있는 인증 기관은 삭제할 수 없습니다.

단계

1. 신뢰할 수 있는 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 신뢰할 수 있는 인증 기관의 이름을 선택합니다.
3. 이름 옆에 있는 을 선택한 다음 * 삭제 * 를 선택합니다.

신뢰할 수 있는 인증 기관을 갱신합니다

System Manager를 사용하면 만료되었거나 곧 만료될 신뢰할 수 있는 인증 기관을 갱신할 수 있습니다.

단계

1. 신뢰할 수 있는 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 신뢰할 수 있는 인증 기관의 이름을 선택합니다.
3. 인증서 이름 옆에 있는 * 갱신 * 을 선택합니다 .

클라이언트/서버 인증서를 설치(추가)합니다

System Manager를 사용하면 추가 클라이언트/서버 인증서를 설치할 수 있습니다.

단계

1. 클라이언트/서버 인증서 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 을 + Add 선택합니다.
3. 클라이언트/서버 인증서 추가 * 패널에서 다음을 수행하십시오.
   - 인증서 이름 * 을 입력합니다.
   - 범위 * 에서 스토리지 VM을 선택합니다.
   - 일반 이름 * 을 입력합니다.
   - 유형 * 을 선택합니다.
   - 인증서 세부 정보 * 를 입력하거나 가져옵니다. 텍스트 파일에서 인증서 세부 정보를 작성하거나 복사하여 붙여 넣거나 * Import *(가져오기 *)를 클릭하여 인증서 파일에서 텍스트를 가져올 수 있습니다.
   - 개인 키 * 를 입력합니다.
     텍스트 파일에서 개인 키를 작성하거나 복사하여 붙여 넣거나 * Import *(가져오기 *)를 클릭하여 개인 키 파일에서 텍스트를 가져올 수 있습니다.

자체 서명된 클라이언트/서버 인증서를 생성(추가)합니다

System Manager를 사용하면 자체 서명된 클라이언트/서버 인증서를 추가로 생성할 수 있습니다.

단계

1. 클라이언트/서버 인증서 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.

2. 선택 * + 자체 서명 인증서 생성 *.
3. 자체 서명된 인증서 생성 * 패널에서 다음을 수행합니다.
    - 인증서 이름 * 을 입력합니다.
    - 범위 * 에서 스토리지 VM을 선택합니다.
    - 일반 이름 * 을 입력합니다.
    - 유형 * 을 선택합니다.
    - 해시 함수 * 를 선택합니다.
    - 키 크기 * 를 선택합니다.
    - 스토리지 VM * 을 선택합니다.

클라이언트/서버 인증서를 삭제합니다

System Manager를 사용하면 클라이언트/서버 인증서를 삭제할 수 있습니다.

단계

1. 클라이언트/서버 인증서 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 클라이언트/서버 인증서의 이름을 선택합니다.
3. 이름 옆에 있는 을 선택한 ⋮ 다음 * 삭제 * 를 클릭합니다.

클라이언트/서버 인증서를 갱신합니다

System Manager를 사용하면 만료되었거나 곧 만료될 클라이언트/서버 인증서를 갱신할 수 있습니다.

단계

1. 클라이언트/서버 인증서 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 클라이언트/서버 인증서의 이름을 선택합니다.
3. 이름 옆에 있는 을 ⋮ 선택한 다음 * 갱신 * 을 클릭합니다.

새 로컬 인증 기관을 생성합니다

System Manager를 사용하여 새 로컬 인증 기관을 만들 수 있습니다.

단계

1. 로컬 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 을 + Add 선택합니다.
3. [로컬 인증 기관 추가]* 패널에서 다음 작업을 수행하십시오.
    - 이름 * 을 입력합니다.
    - 범위 * 에서 스토리지 VM을 선택합니다.
    - 일반 이름 * 을 입력합니다.
4. 기본값을 무시하려면 * 추가 옵션 * 을 선택하고 추가 정보를 제공합니다.

로컬 인증 기관을 사용하여 인증서에 서명합니다

System Manager에서 로컬 인증 기관을 사용하여 인증서에 서명할 수 있습니다.

단계

1. 로컬 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 로컬 인증 기관의 이름을 선택합니다.
3. 이름 옆에 있는 * 인증서 서명 * 을 선택합니다 ⋮ .
4. 인증서 서명 요청 * 양식 을 작성합니다.
   - 인증서 서명 콘텐츠를 붙여 넣거나 * 가져오기 * 를 클릭하여 인증서 서명 요청 파일을 가져올 수 있습니다.
   - 인증서가 유효한 일 수를 지정합니다.

로컬 인증 기관을 삭제합니다

System Manager를 사용하면 로컬 인증 기관을 삭제할 수 있습니다.

단계

1. 로컬 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 로컬 인증 기관의 이름을 선택합니다.
3. 이름 옆에 있는 을 ⋮ 선택한 다음 * Delete * 를 선택합니다.

로컬 인증 기관을 갱신합니다

System Manager를 사용하면 만료되었거나 곧 만료될 로컬 인증 기관을 갱신할 수 있습니다.

단계

1. 로컬 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 로컬 인증 기관의 이름을 선택합니다.
3. 이름 옆에 있는 을 ⋮ 선택한 다음 * 갱신 * 을 클릭합니다.

ONTAP에서 **Active Directory** 도메인 컨트롤러 액세스를 구성합니다

AD 계정이 SVM에 액세스하려면 먼저 클러스터 또는 SVM에 대한 AD 도메인 컨트롤러 액세스를 구성해야 합니다. 데이터 SVM을 위해 SMB 서버를 이미 구성한 경우, SVM을 클러스터에 대한 AD 액세스를 위한 게이트웨이 또는 _tunnel_로 구성할 수 있습니다. SMB 서버를 구성하지 않은 경우 AD 도메인에서 SVM에 대한 컴퓨터 계정을 생성할 수 있습니다.

ONTAP는 다음과 같은 도메인 컨트롤러 인증 서비스를 지원합니다.

- Kerberos
- LDAP를 지원합니다
- Netlogon
- 로컬 보안 기관(LSA)

ONTAP는 보안 Netlogon 연결을 위해 다음 세션 키 알고리즘을 지원합니다.

세션 키 알고리즘입니다	다음으로 시작…
HMAC-SHA256, AES(Advanced Encryption Standard) 기반 클러스터에서 ONTAP 9.9.1 이하를 실행하고 도메인 컨트롤러가 보안 Netlogon 서비스를 위해 AES를 적용하는 경우 연결이 실패합니다. 이 경우 ONTAP와의 강력한 키 연결을 허용하도록 도메인 컨트롤러를 다시 구성해야 합니다.	ONTAP 9.10.1
Des 및 HMAC-MD5(강력한 키가 설정된 경우)	모든 ONTAP 9 릴리스

Netlogon 보안 채널을 설정하는 동안 AES 세션 키를 사용하려면 SVM에서 AES가 활성화되어 있는지 확인해야 합니다.

- ONTAP 9.14.1부터 AES는 SVM을 생성할 때 기본적으로 사용하도록 설정되며, Netlogon 보안 채널 설정 중에 AES 세션 키를 사용하도록 SVM의 보안 설정을 수정할 필요가 없습니다.
- ONTAP 9.10.1~9.13.1에서는 SVM을 생성할 때 AES가 기본적으로 사용하지 않도록 설정됩니다. 다음 명령을 사용하여 AES를 사용하도록 설정해야 합니다.

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

ONTAP 9.14.1 이상으로 업그레이드할 때 이전 ONTAP 릴리즈와 함께 생성된 기존 SVM에 대한 AES 설정이 자동으로 변경되지 않습니다. 하지만 이러한 SVM에서 AES를 사용하도록 설정하려면 이 설정의 값을 업데이트해야 합니다.

인증 터널을 구성합니다

데이터 SVM을 위해 SMB 서버를 이미 구성한 경우 'security login domain-tunnel create' 명령을 사용하여 SVM을 게이트웨이로 구성하거나, AD에서 클러스터에 액세스하도록 _tunnel_을 사용할 수 있습니다.

ONTAP 9.16.1 이전에는 인증 터널을 사용하여 AD로 클러스터 관리자 계정을 관리해야 합니다.

시작하기 전에

- 데이터 SVM을 위해 SMB 서버를 구성해야 합니다.
- 클러스터의 admin SVM에 액세스하려면 AD 도메인 사용자 계정을 활성화해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

ONTAP 9.10.1부터 AD 액세스를 위한 SVM 게이트웨이(도메인 터널)가 있는 경우 AD 도메인에서 NTLM을 비활성화한 경우 관리자 인증에 Kerberos를 사용할 수 있습니다. 이전 릴리즈에서는 SVM 게이트웨이에 대한 관리자 인증을 사용하여 Kerberos를 지원하지 않았습니다. 이 기능은 기본적으로 사용할 수 있으며 구성이 필요하지 않습니다.

Kerberos 인증은 항상 먼저 시도됩니다. 오류가 발생하면 NTLM 인증이 시도됩니다.

단계

1. 클러스터에 대한 AD 도메인 컨트롤러 액세스를 위한 인증 터널로 SMB 지원 데이터 SVM 구성:

```
security login domain-tunnel create -vserver <svm_name>
```

에 대한 자세한 내용은 `security login domain-tunnel create` "ONTAP 명령 참조입니다"을 참조하십시오.

사용자가 인증을 받으려면 SVM이 실행 중이어야 합니다.

다음 명령은 SMB 지원 데이터 SVM `engData`을 인증 터널로 구성합니다.

```
cluster1::>security login domain-tunnel create -vserver engData
```

도메인에서 **SVM** 컴퓨터 계정을 생성합니다

데이터 SVM용으로 SMB 서버를 구성하지 않은 경우 'vserver active-directory create' 명령을 사용하여 도메인의 SVM에 대한 컴퓨터 계정을 생성할 수 있습니다.

이 작업에 대해

'vserver active-directory create' 명령을 입력하면 도메인의 지정된 조직 단위에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 AD 사용자 계정에 대한 자격 증명을 제공하라는 메시지가 표시됩니다. 계정의 암호는 비워둘 수 없습니다.

ONTAP 9.16.1부터 이 절차를 사용하여 AD로 클러스터 관리자 계정을 관리할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. AD 도메인에서 SVM을 위한 컴퓨터 계정을 생성합니다.

```
vserver active-directory create -vserver <SVM_name> -account-name
<NetBIOS_account_name> -domain <domain> -ou <organizational_unit>
```

ONTAP 9.16.1부터 `-vserver` 매개 변수에는 관리 SVM을 사용할 수 있습니다. 에 대한 자세한 내용은 `vserver active-directory create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 SVM용 `engData` 도메인에 `example.com` 이라는 컴퓨터 계정이 생성됩니다 `ADSERVER1`. 명령을 입력한 후 AD 사용자 계정 자격 증명을 입력하라는 메시지가 표시됩니다.

```
cluster1::>vserver active-directory create -vserver engData -account
-name ADSERVER1 -domain example.com

In order to create an Active Directory machine account, you must supply
the name and password of a Windows account with sufficient privileges to
add computers to the "CN=Computers" container within the "example.com"
domain.

Enter the user name: Administrator

Enter the password:
```

ONTAP에서 **LDAP** 또는 **NIS** 서버 액세스를 구성합니다

LDAP 또는 NIS 계정이 SVM에 액세스하려면 먼저 SVM에 대한 LDAP 또는 NIS 서버 액세스를 구성해야 합니다. 스위치 기능을 사용하면 LDAP 또는 NIS를 대체 이름 서비스 소스로 사용할 수 있습니다.

LDAP 서버 액세스를 구성합니다

LDAP 계정이 SVM에 액세스하려면 SVM에 대한 LDAP 서버 액세스를 구성해야 합니다. SVM에서 'vserver services name-service ldap client create' 명령을 사용하여 LDAP 클라이언트 구성을 생성할 수 있습니다. 그런 다음 "vserver services name-service ldap create" 명령을 사용하여 LDAP 클라이언트 구성을 SVM과 연결할 수 있습니다.

이 작업에 대해

대부분의 LDAP 서버는 ONTAP에서 제공하는 기본 스키마를 사용할 수 있습니다.

- MS-AD-BIS(대부분의 Windows 2012 이상 AD 서버에 대한 기본 스키마)
- AD-IDMU(Windows 2008, Windows 2016 이상 AD 서버)
- AD-SFU(Windows 2003 및 이전 AD 서버)
- RFC-2307(UNIX LDAP 서버)

그렇지 않으면 기본 스키마를 사용하는 것이 가장 좋습니다. 이 경우 기본 스키마를 복사하고 복사본을 수정하여 고유한 스키마를 만들 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- "NFS 구성"
- "NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법"

시작하기 전에

- 를 설치해야 "CA 서명 서버 디지털 인증서"SVM에합니다.
- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. SVM에서 LDAP 클라이언트 구성을 생성합니다.

```
vserver services name-service ldap client create -vserver <SVM_name> -client
-config <client_configuration> -servers <LDAP_server_IPs> -schema <schema>
-use-start-tls <true|false>
```

시작 TLS는 데이터 SVM에 대한 액세스에만 지원됩니다. 관리 SVM에 대한 액세스는 지원되지 않습니다.

에 대한 자세한 내용은 `vserver services name-service ldap client create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 SVM에 `engData` 이라는 LDAP 클라이언트 구성이 `corp` 생성됩니다. 클라이언트는 IP 주소 172.160.0.100 및 172.16.0.101을 사용하여 LDAP 서버에 익명 바인딩합니다. 클라이언트는 RFC-2307 스키마를 사용하여 LDAP 쿼리를 만듭니다. 클라이언트와 서버 간의 통신은 시작 TLS를 사용하여 암호화됩니다.

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```

그만큼 `-ldap-servers` 필드는 다음을 대체합니다. `-servers` 필드입니다. 다음을 사용할 수 있습니다. `-ldap-servers` LDAP 서버의 호스트 이름이나 IP 주소를 지정하는 필드입니다.

2. LDAP 클라이언트 구성을 SVM에 연결: `vserver services name-service ldap create -vserver <SVM_name> -client-config <client_configuration> -client-enabled <true|false>`

   에 대한 자세한 내용은 `vserver services name-service ldap create` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령은 LDAP 클라이언트 구성을 연결합니다 `corp` SVM을 사용합니다 `engData`및 는 SVM에서 LDAP 클라이언트를 활성화합니다.

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```

그만큼 `vserver services name-service ldap create` 명령은 자동 구성 검증을 수행하고 ONTAP 이름 서버에 접속할 수 없는 경우 오류 메시지를 보고합니다.

3. vserver services name-service ldap check 명령을 사용하여 이름 서버의 상태를 확인합니다.

   다음 명령을 실행하면 SVM vs0에서 LDAP 서버를 검증합니다.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                    |
```

당신은 사용할 수 있습니다 `name service check` 네임 서버의 상태를 검증하는 명령입니다.

NIS 서버 액세스를 구성합니다

NIS 계정이 SVM에 액세스하려면 먼저 SVM에 대한 NIS 서버 액세스를 구성해야 합니다. SVM에 NIS 도메인 구성을 생성하려면 'vserver services name-service nis-domain create' 명령을 사용할 수 있습니다.

시작하기 전에

- SVM에서 NIS 도메인을 구성하기 전에 구성된 모든 서버를 사용할 수 있고 액세스할 수 있어야 합니다.
- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. SVM에서 NIS 도메인 구성 생성:

   ```
   vserver services name-service nis-domain create -vserver <SVM_name> -domain
   <client_configuration> -nis-servers <NIS_server_IPs>
   ```

   에 대한 자세한 내용은 `vserver services name-service nis-domain create` "ONTAP 명령 참조입니다"을 참조하십시오.

   > 그만큼 `-nis-servers` 필드는 다음을 대체합니다. `-servers` 필드입니다. 다음을 사용할 수 있습니다. `-nis-servers` NIS 서버의 호스트 이름이나 IP 주소를 지정하는 필드입니다.

   다음 명령을 실행하면 SVM에 대한 NIS 도메인 구성을 `engData` 생성합니다. NIS 도메인은 `nisdomain` IP 주소를 사용하여 NIS 서버와 통신합니다. `192.0.2.180`

   ```
   cluster1::>vserver services name-service nis-domain create
   -vserver engData -domain nisdomain -nis-servers 192.0.2.180
   ```

네임 서비스 스위치를 생성합니다

이름 서비스 스위치 기능을 사용하면 LDAP 또는 NIS를 대체 이름 서비스 소스로 사용할 수 있습니다. 'vserver services name-service ns-switch modify' 명령을 사용하여 이름 서비스 소스의 조회 순서를 지정할 수 있습니다.

시작하기 전에

- LDAP 및 NIS 서버 액세스를 구성해야 합니다.

- 이 작업을 수행하려면 클러스터 관리자 또는 SVM 관리자여야 합니다.

단계

1. 이름 서비스 원본에 대한 조회 순서를 지정합니다.

   ```
   vserver services name-service ns-switch modify -vserver <SVM_name> -database
   <name_service_switch_database> -sources <name_service_source_order>
   ```

   에 대한 자세한 내용은 `vserver services name-service ns-switch modify` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령은 SVM에서 데이터베이스에 `engData` 대한 LDAP 및 NIS 이름 서비스 소스의 조회 순서를 `passwd` 지정합니다.

   ```
   cluster1::>vserver services name-service ns-switch
   modify -vserver engData -database passwd -source files ldap,nis
   ```

ONTAP 관리자 암호를 변경합니다

처음 시스템에 로그인한 후 즉시 초기 암호를 변경해야 합니다. SVM 관리자는 '보안 로그인 비밀번호' 명령을 사용하여 비밀번호를 변경할 수 있습니다. 클러스터 관리자인 경우 '보안 로그인 암호' 명령을 사용하여 관리자 암호를 변경할 수 있습니다.

이 작업에 대해

새 암호는 다음 규칙을 준수해야 합니다.

- 사용자 이름은 포함할 수 없습니다
- 8자 이상이어야 합니다
- 하나 이상의 문자와 숫자를 포함해야 합니다
- 마지막 여섯 개의 암호와 같을 수 없습니다

> 명령을 사용하여 지정된 역할과 연결된 계정의 암호 규칙을 수정할 수 `security login role config modify` 있습니다.

시작하기 전에

- 암호를 변경하려면 클러스터 또는 SVM 관리자여야 합니다.
- 다른 관리자의 암호를 변경하려면 클러스터 관리자여야 합니다.

단계

1. 관리자 암호 변경: `security login password -vserver` *`svm_name`* `-username` *`user_name`*

   다음 명령을 실행하면 SVM에 대한 관리자 admin의 암호(vs1.example.com``)가 변경됩니다. 현재 암호를 입력하라는 메시지가 표시되면 새 암호를 입력하고 다시 입력합니다.

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

관련 정보

- "보안 로그인 역할 구성 수정"
- "보안 로그인 암호"

ONTAP 관리자 계정을 잠그고 잠금 해제합니다

'Security login lock' 명령어를 이용하여 관리자 계정을 잠그고, 'Security login unlock' 명령어를 이용하여 계정 잠금을 해제할 수 있다.

시작하기 전에

이러한 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 관리자 계정 잠금:

   'Security login lock - vserver SVM_name - username user_name

   다음 명령을 실행하면 SVM에 대한 관리자 계정 admin1이 잠깁니다. vs1.example.com``:

   ```
   cluster1::>security login lock -vserver engData -username admin1
   ```

   에 대한 자세한 내용은 `security login lock` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 관리자 계정 잠금 해제:

   'Security login unlock - vserver SVM_name - username user_name'

   다음 명령을 실행하면 SVM에 대한 관리자 계정 admin1의 잠금이 해제됩니다. vs1.example.com``:

   ```
   cluster1::>security login unlock -vserver engData -username admin1
   ```

   에 대한 자세한 내용은 `security login unlock` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "보안 로그인"

ONTAP에서 실패한 로그인 시도를 관리합니다

로그인 시도가 반복적으로 실패하면 침입자가 스토리지 시스템을 액세스하려고 시도하는 것을 나타내는 경우가 있습니다. 침입이 발생하지 않도록 여러 단계를 수행할 수 있습니다.

로그인 시도가 실패했음을 어떻게 알 수 있습니다

이벤트 관리 시스템(EMS)은 매 시간마다 로그인 실패 사실을 알립니다. 'audit.log' 파일에서 실패한 로그인 시도 기록을 찾을 수 있습니다.

반복 로그인 시도가 실패하면 어떻게 해야 합니까

단기적으로는 침입 방지를 위한 여러 단계를 수행할 수 있습니다.

- 암호는 최소 대문자, 소문자, 특수 문자 및/또는 숫자로 구성되어야 합니다
- 로그인 시도 실패 후 지연을 적용합니다
- 허용되는 로그인 시도 실패 횟수를 제한하고 지정된 시도 실패 횟수 이후에 사용자를 잠급니다
- 지정된 일 수 동안 비활성 상태인 계정을 만료 및 잠급니다

명령을 사용하여 이러한 작업을 수행할 수 `security login role config modify` 있습니다. 에 대한 자세한 내용은 `security login role config modify` "ONTAP 명령 참조입니다"을 참조하십시오.

장기적으로 다음과 같은 추가 단계를 수행할 수 있습니다.

- 명령을 사용하여 `security ssh modify` 새로 생성된 모든 SVM에 대해 실패한 로그인 시도 횟수를 제한할 수 있습니다. 에 대한 자세한 내용은 `security ssh modify` "ONTAP 명령 참조입니다"을 참조하십시오.
- 사용자에게 암호를 변경하도록 요구하여 기존 MD5 알고리즘 계정을 보다 안전한 SHA-512 알고리즘으로 마이그레이션합니다.

ONTAP 관리자 계정 암호에 SHA-2를 적용합니다

ONTAP 9.0 이전에 만든 관리자 계정은 암호를 수동으로 변경할 때까지 업그레이드 후 MD5 암호를 계속 사용합니다. MD5는 SHA-2보다 안전하지 않습니다. 따라서 업그레이드 후 MD5 계정 사용자에게 암호를 변경하여 기본 SHA-512 해시 기능을 사용하도록 해야 합니다.

이 작업에 대해

암호 해시 기능을 사용하면 다음을 수행할 수 있습니다.

- 지정된 해시 함수와 일치하는 사용자 계정을 표시합니다.
- 지정된 해시 기능(예: MD5)을 사용하는 계정을 만료하여 사용자가 다음 로그인 시 암호를 변경하도록 합니다.
- 암호가 지정된 해시 기능을 사용하는 계정을 잠급니다.
- ONTAP 9 이전 릴리즈로 되돌릴 때 이전 릴리즈에서 지원하는 MD5(해시 기능)와 호환되도록 클러스터 관리자의 자체 암호를 재설정합니다.

ONTAP는 NetApp Manageability SDK를 사용하여 해시된 SHA-2 암호만 허용합니다 (`security-login-create` 및 `security-login-modify-password`)를 클릭합니다.

단계

1. MD5 관리자 계정을 SHA-512 암호 해시 기능으로 마이그레이션합니다.
   a. MD5 관리자 계정 모두 만료: '보안 로그인 만료 - 암호 - vserver* - 사용자 이름* - 해시 - 기능 MD5'

      이렇게 하면 MD5 계정 사용자는 다음 로그인 시 암호를 변경해야 합니다.

   b. MD5 계정 사용자에게 콘솔 또는 SSH 세션을 통해 로그인하도록 요청합니다.

      계정이 만료되었음을 감지하고 사용자에게 암호를 변경하라는 메시지를 표시합니다. SHA-512는 변경된 암호에 기본적으로 사용됩니다.

2. 사용자가 로그인하지 않은 MD5 계정의 경우 일정 시간 내에 암호를 변경하려면 다음과 같이 계정 마이그레이션을 강제로 수행합니다.
   a. MD5 해시 기능(고급 권한 수준)을 계속 사용하는 계정 잠금: '보안 로그인 만료 - 암호 - vserver* - 사용자 이름 * - 해시 - 기능 md5 - 정수 후 잠금

      록애프터(lock-After)로 지정된 일 수가 지나면 MD5 계정에 액세스할 수 없습니다.

   b. 사용자가 암호를 변경할 준비가 되면 계정의 잠금을 해제합니다. `security login unlock -vserver` *`svm_name`* `-username` *`user_name`*
   c. 사용자가 콘솔 또는 SSH 세션을 통해 계정에 로그인하고 시스템에서 암호를 변경하도록 요청하는 경우 암호를 변경하도록 요청합니다.

관련 정보

- "보안 로그인 만료 - 암호"
- "보안 로그인 잠금 해제"

System Manager에서 발생하는 **ONTAP** 파일 액세스 문제 진단 및 해결

ONTAP 9.8부터 파일 액세스 문제를 추적하고 볼 수 있습니다.

단계

1. System Manager에서 * 스토리지 > 스토리지 VM * 을 선택합니다.
2. 추적을 수행할 스토리지 VM을 선택합니다.
3. ⋮ More * 를 클릭합니다.
4. 추적 파일 액세스 * 를 클릭합니다.
5. 사용자 이름과 클라이언트 IP 주소를 입력한 다음 * 추적 시작 * 을 클릭합니다.

   추적 결과가 테이블에 표시됩니다. 이유 * 열은 파일에 액세스할 수 없는 이유를 제공합니다.

6. ⌄ 파일 액세스 권한을 보려면 결과 테이블의 왼쪽 열을 클릭합니다.

여러 관리자 검증 관리

ONTAP 다중 관리자 인증에 대해 알아봅니다

ONTAP 9.11.1부터 MAV(다중 관리자 확인)를 사용하여 지정된 관리자의 승인 후에만 볼륨 또는 스냅샷 삭제와 같은 특정 작업을 실행할 수 있습니다. 따라서 손상되거나 악의적이거나 경험이 부족한 관리자가 원치 않는 변경 또는 데이터 삭제를 방지할 수 있습니다.

다중 관리자 검증 구성은 다음과 같이 구성됩니다.

- "하나 이상의 관리자 승인 그룹을 생성합니다."
- "다중 관리 확인 기능 활성화."
- "규칙 추가 또는 수정"

초기 구성 후에는 MAV 승인 그룹(MAV 관리자)의 관리자만 이러한 요소를 수정할 수 있습니다.

다중 관리자 확인이 활성화된 경우 모든 보호된 작업을 완료하려면 다음 단계를 수행해야 합니다.

1. 사용자가 작업을 시작하면, 가 표시됩니다 "요청이 생성되었습니다."
2. 작업을 실행하기 전에 하나 이상의 작업을 수행합니다 "MAV 관리자가 승인해야 합니다."
3. 승인되면 사용자에게 메시지가 표시되고 작업이 완료됩니다.

MAV 관리자 승인 없이 다중 관리자 확인 기능을 비활성화해야 하는 경우 NetApp 지원팀에 문의하여 다음 사항을 언급하십시오."NetApp 기술 자료: MAV 관리자가 사용 불가능한 경우 다중 관리자 검증을 비활성화하는 방법" .

멀티 관리 검증은 작업이 완료되기 전에 각 자동화 작업이 승인을 받아야 하기 때문에 대량 자동화가 필요한 볼륨 또는 워크플로우에서 사용할 수 없습니다. 자동화와 MAV를 함께 사용하려면 특정 MAV 작업에 대한 쿼리를 사용하는 것이 좋습니다. 예를 들어, 자동화가 관련되지 않은 볼륨에만 MAV 규칙을 적용할 수 `volume delete` 있으며 특정 명명 체계를 사용하여 해당 볼륨을 지정할 수 있습니다.

Cloud Volumes ONTAP에서는 다중 관리자 인증을 사용할 수 없습니다.

다중 관리 확인 작동 방식

다중 관리 검증의 구성:

- 승인 및 거부권을 가진 하나 이상의 관리자 그룹.
- _rules table_의 보호된 작업 또는 명령 집합.
- 보호된 작업의 실행을 식별하고 제어하기 위한 _ 규칙 엔진 _.

역할 기반 액세스 제어(RBAC) 규칙 이후에 MAV 규칙을 평가합니다. 따라서 보호된 작업을 실행하거나 승인하는 관리자는 해당 작업에 대한 최소 RBAC 권한을 이미 가지고 있어야 합니다. "RBAC에 대해 자세히 알아보십시오".

시스템 정의 규칙

다중 관리 검증이 활성화된 경우 시스템 정의 규칙(_guard-rail_rules라고도 함)은 MAV 프로세스 자체를 회피하는 위험을 포함할 수 있는 일련의 MAV 작업을 설정합니다. 이러한 작업은 규칙 테이블에서 제거할 수 없습니다. MAV가 활성화되면 별표(*)로 지정된 작업은 실행 전에 하나 이상의 관리자가 승인해야 합니다. 단, * show * 명령은 예외입니다.

- `security multi-admin-verify modify` 작동 *

  다중 관리 검증 기능의 구성을 제어합니다.

- `security multi-admin-verify approval-group` 운영 *

  여러 관리자 확인 자격 증명을 사용하여 관리자 집합에서 구성원 자격을 제어합니다.

- `security multi-admin-verify rule` 운영 *

  admin이 여러 개인 검증이 필요한 명령 세트 제어

- '보안 멀티-관리-검증 요청' 작업

  승인 프로세스를 제어합니다.

규칙으로 보호된 명령

시스템에서 정의한 작업 외에도 다음 명령은 다중 관리자 검증이 활성화된 경우 기본적으로 보호되지만, 규칙을 수정하여 이러한 명령에 대한 보호를 제거할 수 있습니다.

- "보안 로그인 암호"
- "보안 로그인 잠금 해제"
- "설정"

각 ONTAP 버전은 다중 관리자 확인 규칙으로 보호할 수 있는 더 많은 명령을 제공합니다. 보호에 사용할 수 있는 명령의 전체 목록을 보려면 ONTAP 릴리스를 선택하십시오.

9.17.1

- `cluster date modify` (영어
- `cluster log-forwarding create` (영어
- `cluster log-forwarding delete` (영어
- `cluster log-forwarding modify` (영어
- '클러스터 피어 삭제'
- `cluster time-service ntp server create` (영어
- `cluster time-service ntp server delete` (영어
- `cluster time-service ntp key create` (영어
- `cluster time-service ntp key delete` (영어
- `cluster time-service ntp key modify` (영어
- `cluster time-service ntp server modify` (영어
- 이벤트 구성 수정
- `event config set-mail-server-password` [3]
- `lun delete` (영어
- `security anti-ransomware volume attack clear-suspect` [1]
- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume event-log modify` (영어
- `security anti-ransomware volume pause` [1]
- `security anti-ransomware vserver event-log modify` (영어
- `security audit modify` (영어
- `security ipsec config modify` (영어
- `security ipsec policy create` (영어
- `security ipsec policy delete` (영어
- `security ipsec policy modify` (영어
- '보안 로그인 생성'
- '보안 로그인 삭제
- 보안 로그인 수정
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase` (영어
- `security saml-sp create` (영어

- `security saml-sp delete` (영어
- `security saml-sp modify` (영어
- `security webauthn credentials delete` (영어
- `snaplock legal-hold end` (영어
- `storage aggregate delete` (영어
- `storage aggregate offline` (영어
- `storage encryption disk destroy` (영어
- `storage encryption disk modify` (영어
- `storage encryption disk revert-to-original-state` (영어
- `storage encryption disk sanitize` (영어
- `system bridge run-cli` (영어
- `system controller flash-cache secure-erase run` (영어
- `system controller service-event delete` (영어
- `system health alert delete` (영어
- `system health alert modify` (영어
- `system health policy definition modify` (영어
- `system node autosupport modify` (영어
- `system node autosupport trigger modify` (영어
- `system node coredump delete` (영어
- `system node coredump delete-all` (영어
- `system node hardware nvram-encryption modify` (영어
- '시스템 노드 실행
- '시스템 노드 시스템 쉘'
- `system script delete` (영어
- `system service-processor ssh add-allowed-addresses` (영어
- `system service-processor ssh remove-allowed-addresses` (영어
- `system smtape restore` (영어
- `system switch ethernet log disable-collection` (영어
- `system switch ethernet log modify` (영어
- `timezone` (영어
- `volume create` (영어
- '볼륨 삭제'
- `volume encryption conversion start` (영어

- `volume encryption rekey start` (영어
- `volume file privileged-delete` (영어
- 볼륨 FlexCache 삭제
- `volume modify` (영어
- `volume rename` [5]
- `volume recovery-queue modify` [2]
- `volume recovery-queue purge` [2]
- `volume recovery-queue purge-all` [2]
- `volume snaplock modify` [1]
- '볼륨 스냅샷 자동 삭제 수정'
- `volume snapshot create` (영어
- '볼륨 스냅샷 삭제'
- `volume snapshot modify` (영어
- 볼륨 스냅샷 정책 추가 스케줄
- 볼륨 스냅샷 정책 생성
- 볼륨 스냅샷 정책 삭제
- 볼륨 스냅샷 정책 수정
- 볼륨 스냅샷 정책 수정 스케줄
- 볼륨 스냅샷 정책 제거 스케줄
- `volume snapshot rename` (영어
- '볼륨 스냅샷 복원'
- `vserver audit create` (영어
- `vserver audit delete` (영어
- `vserver audit disable` (영어
- `vserver audit modify` (영어
- `vserver audit rotate-log` (영어
- `vserver create` (영어
- `vserver consistency-group create` (영어
- `vserver consistency-group delete` (영어
- `vserver consistency-group modify` (영어
- `vserver consistency-group snapshot create` (영어
- `vserver consistency-group snapshot delete` (영어
- `vserver delete` (영어

- `vserver modify` [2]
- `vserver object-store-server audit create` (영어
- `vserver object-store-server audit delete` (영어
- `vserver object-store-server audit disable` (영어
- `vserver object-store-server audit modify` (영어
- `vserver object-store-server audit rotate-log` (영어
- `vserver object-store-server bucket cors-rule create` (영어
- `vserver object-store-server bucket cors-rule delete` (영어
- `vserver options` (영어
- 'vserver peer delete
- `vserver security file-directory apply` (영어
- `vserver security file-directory remove-slag` (영어
- `vserver stop` (영어
- `vserver vscan disable` (영어
- `vserver vscan on-access-policy create` (영어
- `vserver vscan on-access-policy delete` (영어
- `vserver vscan on-access-policy disable` (영어
- `vserver vscan on-access-policy modify` (영어
- `vserver vscan scanner-pool create` (영어
- `vserver vscan scanner-pool delete` (영어
- `vserver vscan scanner-pool modify` (영어

9.16.1

- `cluster date modify` (영어
- `cluster log-forwarding create` (영어
- `cluster log-forwarding delete` (영어
- `cluster log-forwarding modify` (영어
- '클러스터 피어 삭제'
- `cluster time-service ntp server create` (영어
- `cluster time-service ntp server delete` (영어
- `cluster time-service ntp key create` (영어
- `cluster time-service ntp key delete` (영어
- `cluster time-service ntp key modify` (영어
- `cluster time-service ntp server modify` (영어

- 이벤트 구성 수정
- `event config set-mail-server-password` [3]
- `lun delete` (영어
- `security anti-ransomware volume attack clear-suspect` [1]
- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume event-log modify` (영어
- `security anti-ransomware volume pause` [1]
- `security anti-ransomware vserver event-log modify` (영어
- `security audit modify` (영어
- `security ipsec config modify` (영어
- `security ipsec policy create` (영어
- `security ipsec policy delete` (영어
- `security ipsec policy modify` (영어
- '보안 로그인 생성'
- '보안 로그인 삭제
- 보안 로그인 수정
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase` (영어
- `security saml-sp create` (영어
- `security saml-sp delete` (영어
- `security saml-sp modify` (영어
- `security webauthn credentials delete` (영어
- `snaplock legal-hold end` (영어
- `storage aggregate delete` (영어
- `storage aggregate offline` (영어
- `storage encryption disk destroy` (영어
- `storage encryption disk modify` (영어
- `storage encryption disk revert-to-original-state` (영어
- `storage encryption disk sanitize` (영어
- `system bridge run-cli` (영어
- `system controller flash-cache secure-erase run` (영어

- `system controller service-event delete` (영어
- `system health alert delete` (영어
- `system health alert modify` (영어
- `system health policy definition modify` (영어
- `system node autosupport modify` (영어
- `system node autosupport trigger modify` (영어
- `system node coredump delete` (영어
- `system node coredump delete-all` (영어
- `system node hardware nvram-encryption modify` (영어
- '시스템 노드 실행
- '시스템 노드 시스템 쉘'
- `system script delete` (영어
- `system service-processor ssh add-allowed-addresses` (영어
- `system service-processor ssh remove-allowed-addresses` (영어
- `system smtape restore` (영어
- `system switch ethernet log disable-collection` (영어
- `system switch ethernet log modify` (영어
- `timezone` (영어
- `volume create` (영어
- '볼륨 삭제'
- `volume encryption conversion start` (영어
- `volume encryption rekey start` (영어
- `volume file privileged-delete` (영어
- 볼륨 FlexCache 삭제
- `volume modify` (영어
- `volume recovery-queue modify` [2]
- `volume recovery-queue purge` [2]
- `volume recovery-queue purge-all` [2]
- `volume snaplock modify` [1]
- '볼륨 스냅샷 자동 삭제 수정'
- `volume snapshot create` (영어
- '볼륨 스냅샷 삭제'
- `volume snapshot modify` (영어

- 볼륨 스냅샷 정책 추가 스케줄
- 볼륨 스냅샷 정책 생성
- 볼륨 스냅샷 정책 삭제
- 볼륨 스냅샷 정책 수정
- 볼륨 스냅샷 정책 수정 스케줄
- 볼륨 스냅샷 정책 제거 스케줄
- `volume snapshot rename` (영어
- '볼륨 스냅샷 복원'
- `vserver audit create` (영어
- `vserver audit delete` (영어
- `vserver audit disable` (영어
- `vserver audit modify` (영어
- `vserver audit rotate-log` (영어
- `vserver create` (영어
- `vserver consistency-group create` (영어
- `vserver consistency-group delete` (영어
- `vserver consistency-group modify` (영어
- `vserver consistency-group snapshot create` (영어
- `vserver consistency-group snapshot delete` (영어
- `vserver delete` (영어
- `vserver modify` [2]
- `vserver object-store-server audit create` (영어
- `vserver object-store-server audit delete` (영어
- `vserver object-store-server audit disable` (영어
- `vserver object-store-server audit modify` (영어
- `vserver object-store-server audit rotate-log` (영어
- `vserver object-store-server bucket cors-rule create` (영어
- `vserver object-store-server bucket cors-rule delete` (영어
- `vserver options` (영어
- 'vserver peer delete
- `vserver security file-directory apply` (영어
- `vserver security file-directory remove-slag` (영어
- `vserver stop` (영어

- `vserver vscan disable`(영어
- `vserver vscan on-access-policy create`(영어
- `vserver vscan on-access-policy delete`(영어
- `vserver vscan on-access-policy disable`(영어
- `vserver vscan on-access-policy modify`(영어
- `vserver vscan scanner-pool create`(영어
- `vserver vscan scanner-pool delete`(영어
- `vserver vscan scanner-pool modify`(영어

9.15.1

- `cluster date modify`(영어
- `cluster log-forwarding create`(영어
- `cluster log-forwarding delete`(영어
- `cluster log-forwarding modify`(영어
- '클러스터 피어 삭제'
- `cluster time-service ntp server create`(영어
- `cluster time-service ntp server delete`(영어
- `cluster time-service ntp key create`(영어
- `cluster time-service ntp key delete`(영어
- `cluster time-service ntp key modify`(영어
- `cluster time-service ntp server modify`(영어
- 이벤트 구성 수정
- `event config set-mail-server-password`[3]
- `lun delete`(영어
- `security anti-ransomware volume attack clear-suspect`[1]
- `security anti-ransomware volume disable`[1]
- `security anti-ransomware volume event-log modify`(영어
- `security anti-ransomware volume pause`[1]
- `security anti-ransomware vserver event-log modify`(영어
- `security audit modify`(영어
- `security ipsec config modify`(영어
- `security ipsec policy create`(영어
- `security ipsec policy delete`(영어
- `security ipsec policy modify`(영어

- '보안 로그인 생성'
- '보안 로그인 삭제
- 보안 로그인 수정
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase` (영어
- `security saml-sp create` (영어
- `security saml-sp delete` (영어
- `security saml-sp modify` (영어
- `snaplock legal-hold end` (영어
- `storage aggregate delete` (영어
- `storage encryption disk destroy` (영어
- `storage encryption disk modify` (영어
- `storage encryption disk revert-to-original-state` (영어
- `storage encryption disk sanitize` (영어
- `system bridge run-cli` (영어
- `system controller flash-cache secure-erase run` (영어
- `system controller service-event delete` (영어
- `system health alert delete` (영어
- `system health alert modify` (영어
- `system health policy definition modify` (영어
- `system node autosupport modify` (영어
- `system node autosupport trigger modify` (영어
- `system node coredump delete` (영어
- `system node coredump delete-all` (영어
- `system node hardware nvram-encryption modify` (영어
- '시스템 노드 실행
- '시스템 노드 시스템 쉘'
- `system script delete` (영어
- `system service-processor ssh add-allowed-addresses` (영어
- `system service-processor ssh remove-allowed-addresses` (영어
- `system smtape restore` (영어

- `system switch ethernet log disable-collection` (영어
- `system switch ethernet log modify` (영어
- `timezone` (영어
- `volume create` (영어
- '볼륨 삭제'
- `volume file privileged-delete` (영어
- 볼륨 FlexCache 삭제
- `volume modify` (영어
- `volume recovery-queue modify` [2]
- `volume recovery-queue purge` [2]
- `volume recovery-queue purge-all` [2]
- `volume snaplock modify` [1]
- '볼륨 스냅샷 자동 삭제 수정'
- `volume snapshot create` (영어
- '볼륨 스냅샷 삭제'
- `volume snapshot modify` (영어
- 볼륨 스냅샷 정책 추가 스케줄
- 볼륨 스냅샷 정책 생성
- 볼륨 스냅샷 정책 삭제
- 볼륨 스냅샷 정책 수정
- 볼륨 스냅샷 정책 수정 스케줄
- 볼륨 스냅샷 정책 제거 스케줄
- `volume snapshot rename` (영어
- '볼륨 스냅샷 복원'
- `vserver audit create` (영어
- `vserver audit delete` (영어
- `vserver audit disable` (영어
- `vserver audit modify` (영어
- `vserver audit rotate-log` (영어
- `vserver create` (영어
- `vserver delete` (영어
- `vserver modify` [2]
- `vserver object-store-server audit create` (영어

- `vserver object-store-server audit delete` (영어
- `vserver object-store-server audit disable` (영어
- `vserver object-store-server audit modify` (영어
- `vserver object-store-server audit rotate-log` (영어
- `vserver options` (영어
- 'vserver peer delete
- `vserver security file-directory apply` (영어
- `vserver security file-directory remove-slag` (영어
- `vserver vscan disable` (영어
- `vserver vscan on-access-policy create` (영어
- `vserver vscan on-access-policy delete` (영어
- `vserver vscan on-access-policy disable` (영어
- `vserver vscan on-access-policy modify` (영어
- `vserver vscan scanner-pool create` (영어
- `vserver vscan scanner-pool delete` (영어
- `vserver vscan scanner-pool modify` (영어

9.14.1

- '클러스터 피어 삭제'
- 이벤트 구성 수정
- `security anti-ransomware volume attack clear-suspect` [1]
- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume event-log modify` (영어
- `security anti-ransomware volume pause` [1]
- `security anti-ransomware vserver event-log modify` (영어
- '보안 로그인 생성'
- '보안 로그인 삭제
- 보안 로그인 수정
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- '시스템 노드 실행
- '시스템 노드 시스템 쉘'
- '볼륨 삭제'

- 볼륨 FlexCache 삭제
- `volume recovery-queue modify` [2]
- `volume recovery-queue purge` [2]
- `volume recovery-queue purge-all` [2]
- `volume snaplock modify` [1]
- '볼륨 스냅샷 자동 삭제 수정'
- '볼륨 스냅샷 삭제'
- 볼륨 스냅샷 정책 추가 스케줄
- 볼륨 스냅샷 정책 생성
- `volume snapshot policy delete` *
- 볼륨 스냅샷 정책 수정
- 볼륨 스냅샷 정책 수정 스케줄
- 볼륨 스냅샷 정책 제거 스케줄
- '볼륨 스냅샷 복원'
- `vserver create` (영어
- `vserver modify` [2]
- 'vserver peer delete

9.13.1

- '클러스터 피어 삭제'
- 이벤트 구성 수정
- `security anti-ransomware volume attack clear-suspect` [1]
- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume pause` [1]
- '보안 로그인 생성'
- '보안 로그인 삭제
- 보안 로그인 수정
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- '시스템 노드 실행
- '시스템 노드 시스템 쉘'
- '볼륨 삭제'
- 볼륨 FlexCache 삭제
- `volume snaplock modify` [1]

- '볼륨 스냅샷 자동 삭제 수정'
- '볼륨 스냅샷 삭제'
- 볼륨 스냅샷 정책 추가 스케줄
- 볼륨 스냅샷 정책 생성
- `volume snapshot policy delete *`
- 볼륨 스냅샷 정책 수정
- 볼륨 스냅샷 정책 수정 스케줄
- 볼륨 스냅샷 정책 제거 스케줄
- '볼륨 스냅샷 복원'
- 'vserver peer delete

9.12.1 / 9.11.1

- '클러스터 피어 삭제'
- 이벤트 구성 수정
- '보안 로그인 생성'
- '보안 로그인 삭제
- 보안 로그인 수정
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- '시스템 노드 실행
- '시스템 노드 시스템 쉘'
- '볼륨 삭제'
- 볼륨 FlexCache 삭제
- '볼륨 스냅샷 자동 삭제 수정'
- '볼륨 스냅샷 삭제'
- 볼륨 스냅샷 정책 추가 스케줄
- 볼륨 스냅샷 정책 생성
- `volume snapshot policy delete *`
- 볼륨 스냅샷 정책 수정
- 볼륨 스냅샷 정책 수정 스케줄
- 볼륨 스냅샷 정책 제거 스케줄
- '볼륨 스냅샷 복원'
- 'vserver peer delete

1. 9.13.1에 대한 새로운 규칙 보호 명령입니다
2. 9.14.1에 대한 새로운 규칙 보호 명령입니다
3. 9.15.1에 대한 새로운 규칙 보호 명령입니다
4. 9.16.1에 대한 새로운 규칙 보호 명령입니다
5. 9.17.1에 대한 새로운 규칙 보호 명령

*이 명령은 CLI에서만 사용할 수 있으며 일부 릴리즈에서는 System Manager에서 사용할 수 없습니다.

여러 관리자의 승인 방식

보호된 작업이 MAV 보호 클러스터에 입력될 때마다 작업 실행 요청이 지정된 MAV 관리자 그룹으로 전송됩니다.

다음을 구성할 수 있습니다.

- MAV 그룹의 이름, 연락처 정보 및 관리자 수

  MAV 관리자는 클러스터 관리자 권한이 있는 RBAC 역할을 가지고 있어야 합니다.

- MAV 관리자 그룹 수
  - 각 보호된 작업 규칙에 대해 MAV 그룹이 할당됩니다.
  - 여러 MAV 그룹의 경우 지정된 규칙을 승인하는 MAV 그룹을 구성할 수 있습니다.
- 보호된 작업을 실행하는 데 필요한 MAV 승인 수입니다.
- MAV 관리자가 승인 요청에 응답해야 하는 _ 승인 만료 _ 기간.
- 요청 관리자가 작업을 완료해야 하는 _ 실행 expiry_period입니다.

이러한 매개 변수가 구성되면 이를 수정하려면 MAV 승인이 필요합니다.

MAV 관리자는 보호된 작업을 실행하기 위한 자체 요청을 승인할 수 없습니다. 즉,

- 관리자가 한 명 있는 클러스터에서는 MAV를 사용하지 않아야 합니다.
- MAV 그룹에 한 명만 있는 경우 MAV 관리자는 보호된 작업을 시작할 수 없습니다. 정규 관리자는 보호된 작업을 시작해야 하며 MAV 관리자는 승인만 할 수 있습니다.
- MAV 관리자가 보호된 작업을 실행할 수 있도록 하려면 MAV 관리자 수가 필요한 승인 수보다 1개 이상 커야 합니다. 예를 들어 보호된 작업에 대해 두 번의 승인이 필요하고 MAV 관리자가 이를 실행하도록 하려면 MAV administrators 그룹에 세 명의 사용자가 있어야 합니다.

MAV 관리자는 전자 메일 알림(EMS 사용)으로 승인 요청을 받거나 요청 대기열을 쿼리할 수 있습니다. 요청을 받으면 다음 세 가지 작업 중 하나를 수행할 수 있습니다.

- 승인
- 거부(거부권)
- 무시(동작 없음)

다음과 같은 경우 전자 메일 알림이 MAV 규칙과 연결된 모든 승인자에게 전송됩니다.

- 요청이 생성됩니다.

- 요청이 승인되거나 거부되었습니다.
- 승인된 요청이 실행됩니다.

요청자가 작업에 대해 동일한 승인 그룹에 있는 경우 요청이 승인되면 이메일을 받게 됩니다.

> 요청자는 승인 그룹에 있는 경우에도 자신의 요청을 승인할 수 없습니다(자신의 요청에 대한 전자 메일 알림을 받을 수는 있음). 승인 그룹에 없는 요청자(즉, MAV 관리자가 아닌)는 이메일 알림을 받지 않습니다.

보호된 작업 실행의 작동 방식

보호된 작업에 대해 실행이 승인되면 요청 사용자는 메시지가 표시될 때 작업을 계속합니다. 작업이 거부되면 요청 사용자는 계속하기 전에 요청을 삭제해야 합니다.

MAV 규칙은 RBAC 권한 이후에 평가됩니다. 따라서 작업 실행에 대한 충분한 RBAC 권한이 없는 사용자는 MAV 요청 프로세스를 시작할 수 없습니다.

MAV 규칙은 보호된 작업이 실행되기 전에 평가됩니다. 즉, 규칙은 시스템의 현재 상태를 기반으로 적용됩니다. 예를 들어, MAV 규칙이 다음과 같이 생성되는 경우 `volume modify` 의 질문으로 `-size 5GB` , 사용하여 `volume modify` 5GB 볼륨의 크기를 2GB로 조정하려면 MAV 승인이 필요하지만, 2GB 볼륨의 크기를 5GB로 조정하는 경우에는 승인이 필요하지 않습니다.

관련 정보

- "클러스터"
- "LUN을 클릭합니다"
- "보안"
- "SnapLock 법적 증거 자료 보관 종료"
- "저장 집계"
- "스토리지 암호화"
- "시스템"

MAV에 대한 **ONTAP** 관리자 승인 그룹을 관리합니다

MAV(Multi-admin verification)를 활성화하기 전에 승인 또는 거부권을 부여할 관리자가 하나 이상 포함된 관리자 승인 그룹을 만들어야 합니다. 다중 관리자 확인을 활성화한 경우 승인 그룹 구성원을 수정하려면 기존의 검증된 관리자 중 한 명의 승인이 필요합니다.

이 작업에 대해

기존 관리자를 MAV 그룹에 추가하거나 새 관리자를 만들 수 있습니다.

MAV 기능은 기존의 역할 기반 액세스 제어(RBAC) 설정을 그대로 사용합니다. 잠재적인 MAV 관리자는 MAV 관리자 그룹에 추가하기 전에 보호 작업을 실행할 수 있는 충분한 권한이 있어야 합니다. "RBAC에 대해 자세히 알아보십시오."

승인 요청이 보류 중이라는 것을 MAV 관리자에게 알리도록 MAV를 구성할 수 있습니다. 이렇게 하려면 이메일 알림(특히, 'Mail From' 및 'Mail Server' 매개 변수)을 구성하거나 이러한 매개 변수를 지워 알림을 비활성화해야 합니다. 이메일 알림이 없으면 MAV 관리자는 승인 대기열을 수동으로 확인해야 합니다.

ONTAP 9.15.1부터 Active Directory(AD) 사용자를 MAV 관리자로 구성할 수 있습니다. AD 사용자는 다음과 같아야 합니다."ONTAP 관리자로 구성됨" .

System Manager 절차

처음으로 MAV 승인 그룹을 만들려면 System Manager 절차 - 를 참조하십시오 "다중 관리 검증을 활성화합니다."

기존 승인 그룹을 수정하거나 추가 승인 그룹을 만들려면:

1. 여러 관리자 검증을 받을 관리자 식별
   a. 클러스터 > 설정 * 을 클릭합니다
   b. 사용자 및 역할 * 옆에 있는 을 클릭합니다 →
   c. 사용자 * 아래에서 를 클릭합니다 + Add
   d. 필요에 따라 명단을 수정합니다.

      자세한 내용은 을 참조하십시오 "관리자 액세스 제어."

2. MAV 승인 그룹 생성 또는 수정:
   a. 클러스터 > 설정 * 을 클릭합니다
   b. 보안 * 섹션에서 * 다중 관리자 승인 * 옆에 있는 을 클릭합니다 → . (⚙ MAV가 아직 구성되지 않은 경우 아이콘이 표시됩니다.)
      - 이름: 그룹 이름을 입력합니다.
      - 승인자: 사용자 목록에서 승인자를 선택합니다.
      - 이메일 주소: 이메일 주소를 입력합니다.
      - Default group(기본 그룹): 그룹을 선택합니다.

MAV가 활성화되면 기존 구성을 편집하려면 MAV 승인이 필요합니다.

CLI 절차

1. 'Mail From' 및 'Mail Server' 매개 변수에 값이 설정되어 있는지 확인합니다. 입력:

   이벤트 구성 쇼

   디스플레이는 다음과 비슷해야 합니다.

```
cluster01::> event config show
                            Mail From:  admin@localhost
                          Mail Server:  localhost
                            Proxy URL:  -
                           Proxy User:  -
 Publish/Subscribe Messaging Enabled:  true
```

   이러한 매개 변수를 구성하려면 다음을 입력합니다.

"이벤트 구성 수정-메일-보낸 사람_이메일_주소_-메일-서버_서버_이름_'

및 `event config modify` 에 대한 자세한 `event config show` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

2. 여러 관리자 검증을 받을 관리자 식별

원하는 사항	이 명령을 입력합니다
현재 관리자를 표시합니다	'보안 로그인 쇼'
현재 관리자의 자격 증명을 수정합니다	'Security login modify_<parameters>_'
새 관리자 계정을 만듭니다	'Security login create-user-or-group-name_admin_name_-application ssh-authentication-method password

에 대한 자세한 `security login show` `security login modify` 내용은, 및 `security login create`"ONTAP 명령 참조입니다" 을 참조하십시오.

3. MAV 승인 그룹 생성:

`security multi-admin-verify approval-group create [ -vserver` *`svm_name`*`] -name` *`group_name`* `-approvers` *`approver1`*`[,`*`approver2`*`…] [[-email` *`address1`*`], `*`address1`*`…]`

- '-vserver' - 이번 릴리즈에서는 관리 SVM만 지원됩니다.
- '-name' - 최대 64자의 MAV 그룹 이름입니다.
- `-approvers`- 한 명 이상의 승인자 목록. AD 사용자의 경우 다음 형식을 사용하세요. `domain\user` . 예를 들어, `mydomain\pavan` .
- '-email' - 요청을 작성, 승인, 거부하거나 실행할 때 통지되는 하나 이상의 이메일 주소입니다.
  - 예: * 다음 명령을 실행하면 멤버 2개와 관련 이메일 주소가 있는 MAV 그룹이 생성됩니다.

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. 그룹 생성 및 구성원 자격 확인:

`security multi-admin-verify approval-group show`

- 예: *

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name          Approvers         Email
-------  ---------------- ------------------
------------------------------------------------------------
svm-1    mav-grp1    pavan,julia       email
pavan@myfirm.com,julia@myfirm.com
```

이 명령을 사용하여 초기 MAV 그룹 구성을 수정합니다.

- 참고: * 모두 실행 전에 MAV 관리자의 승인이 필요합니다.

원하는 사항	이 명령을 입력합니다
그룹 특성을 수정하거나 기존 구성원 정보를 수정합니다	'Security multi-admin - Verify approval-group modify[*parameters*]'
구성원을 추가 또는 제거합니다	'보안 다중 관리자 - 승인 확인 - 그룹 바꾸기[-vserver_svm_name_] - name_group_name_[-approver-to-add_approver1_[,*approver2*…]] [-approver-to-remove_approver1_[,*approver2*…]'
그룹을 삭제합니다	'보안 multi-admin-verify approval-group delete[-vserver_svm_name_]-name_group_name_'

관련 정보

- "보안 다중 관리자 확인"

ONTAP에서 다중 관리자 확인을 활성화 또는 비활성화합니다

MAV(Multi-admin verification)를 명시적으로 활성화해야 합니다. 다중 관리 확인을 사용하도록 설정한 후에는 MAV 승인 그룹(MAV 관리자)의 관리자가 이를 삭제해야 합니다.

이 작업에 대해

MAV가 활성화되면 MAV를 수정하거나 사용하지 않도록 하려면 MAV 관리자의 승인이 필요합니다.

MAV 관리자 승인 없이 다중 관리자 확인 기능을 비활성화해야 하는 경우 NetApp 지원팀에 문의하여 다음 사항을 언급하십시오."NetApp 기술 자료: MAV 관리자가 사용 불가능한 경우 다중 관리자 검증을 비활성화하는 방법" .

MAV를 사용하도록 설정하면 다음 매개 변수를 전역적으로 지정할 수 있습니다.

승인 그룹

글로벌 승인 그룹 목록 MAV 기능을 사용하려면 하나 이상의 그룹이 필요합니다.

ARP(Autonomous 랜섬웨어Protection)와 함께 MAV를 사용하는 경우 ARP 일시 중지, 비활성화 및 의심되는 요청을 승인하는 신규 또는 기존 승인 그룹을 정의하십시오.

필수 승인자

보호된 작업을 실행하는 데 필요한 승인자 수입니다. 기본 및 최소 숫자는 1입니다.

필요한 승인자 수는 기본 승인 그룹의 총 고유 승인자 수보다 적어야 합니다.

승인 만료(시간, 분, 초)

MAV 관리자가 승인 요청에 응답해야 하는 기간. 기본값은 1시간(1시간)이고, 지원되는 최소 값은 1초(1초)이며, 지원되는 최대 값은 14일(14D)입니다.

실행 만료(시간, 분, 초)

요청 관리자가 완료해야 하는 기간:: 작업. 기본값은 1시간(1시간)이고, 지원되는 최소 값은 1초(1초)이며, 지원되는 최대 값은 14일(14D)입니다.

또한 특정 매개 변수에 대해 이러한 매개 변수를 재정의할 수도 있습니다 "작업 규칙."

System Manager 절차

1. 여러 관리자 검증을 받을 관리자 식별
   a. 클러스터 > 설정 * 을 클릭합니다
   b. 사용자 및 역할 * 옆에 있는 을 클릭합니다 →
   c. 사용자 * 아래에서 를 클릭합니다 + Add
   d. 필요에 따라 명단을 수정합니다.

      자세한 내용은 을 참조하십시오 "관리자 액세스 제어."

2. 하나 이상의 승인 그룹을 생성하고 하나 이상의 규칙을 추가하여 다중 관리 검증을 활성화합니다.
   a. 클러스터 > 설정 * 을 클릭합니다
   b. 보안 * 섹션에서 * 다중 관리자 승인 * 옆에 있는 을 클릭합니다 ⚙ .
   c. + Add 하나 이상의 승인 그룹을 추가하려면 클릭하십시오.
      - 이름 - 그룹 이름을 입력합니다.
      - 승인자 - 사용자 목록에서 승인자를 선택합니다.
      - 이메일 주소 – 이메일 주소를 입력합니다.
      - Default group(기본 그룹) – 그룹을 선택합니다.
   d. 하나 이상의 규칙을 추가합니다.
      - 작업 - 목록에서 지원되는 명령을 선택합니다.
      - 쿼리 - 원하는 명령 옵션 및 값을 입력합니다.
      - 선택적 매개 변수입니다. 글로벌 설정을 적용하려면 비워 두거나 글로벌 설정을 재정의하기 위해 특정 규칙에 다른 값을 할당합니다.
        - 승인자 수가 필요합니다
        - 승인 그룹
   e. 기본값을 보거나 수정하려면 * 고급 설정 * 을 클릭합니다.

- 필요한 승인자 수(기본값: 1)
- 실행 요청 만료(기본값: 1시간)
- 승인 요청 만료(기본값: 1시간)
- 메일 서버 *
- 발신 이메일 주소 *
  - 이렇게 하면 "알림 관리"에서 관리되는 이메일 설정이 업데이트됩니다. 아직 구성되지 않은 경우 설정하라는 메시지가 표시됩니다.

f. MAV 초기 구성을 완료하려면 * 활성화 * 를 클릭합니다.

초기 구성 후 현재 MAV 상태가 * Multi-Admin Approval * (다중 관리자 승인 *) 타일에 표시됩니다.

- 상태(활성화됨 또는 아님)
- 승인이 필요한 활성 작업
- 보류 중인 미결 요청 수입니다

을 클릭하여 기존 구성을 표시할 수 →있습니다. 기존 구성을 편집하려면 MAV 승인이 필요합니다.

다중 관리 확인을 비활성화하려면:

1. 클러스터 > 설정 * 을 클릭합니다
2. 보안 * 섹션에서 * 다중 관리자 승인 * 옆에 있는 을 클릭합니다 .
3. 사용 전환 단추를 클릭합니다.

   이 작업을 완료하려면 MAV 승인이 필요합니다.

CLI 절차

CLI에서 MAV 기능을 활성화하기 전에 하나 이상의 기능이 있어야 합니다 "MAV 관리자 그룹" 이(가) 생성되어야 합니다.

원하는 사항	이 명령을 입력합니다
MAV 기능을 활성화합니다	'보안 multi-admin-verify modify-approval-group1_[,*group2*…] [-필수-승인자_nn_] - 활성화된 참 [-실행-만료 [*nn*h] [*nn*m] [*nn*s] [- 승인-만료 [*nn*h] [*nn*s] [*nn*s]] • 예 *: 다음 명령을 실행하면 1개의 승인 그룹, 2개의 필수 승인자 및 기본 만료 기간이 포함된 MAV가 활성화됩니다. `cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true` 최소 1개를 추가하여 초기 구성을 완료합니다 "작업 규칙."
MAV 구성 수정(MAV 승인 필요)	'보안 Multi-admin-Verify approval-group modify [-approval-group1_[,*group2*…] [-필수-승인자_nn_] [-실행-만료 [*nn*h] [*nn*m] [*nn*s] [- 승인-만료 [*nn*h] [*nn*s]]

MAV 기능을 확인합니다	'보안 멀티-관리-검증 쇼'
	
	• 예: *
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution`
	`Approval Approval`
	`Enabled Approvers Expiry Expiry`
	`Groups`
	`------- --------- ---------`
	`-------- ----------`
	`true 2 1h 1h`
	`mav-grp1`

MAV 기능 비활성화(MAV 승인 필요)	'보안 멀티-관리-검증 수정-사용 안 함

관련 정보

- "보안 다중 관리자 확인"

ONTAP에서 보호된 작업에 대한 다중 관리자 인증 규칙을 관리합니다

MAV(Multi-admin verification) 규칙을 만들어 승인이 필요한 작업을 지정합니다. 작업이 시작될

때마다 보호된 작업이 차단되고 승인 요청이 생성됩니다.

적절한 RBAC 기능이 있는 관리자가 MAV를 활성화하기 전에 규칙을 만들 수 있지만, M5V가 활성화되면 규칙 집합을 수정하려면 MAV 승인이 필요합니다.

작업당 하나의 MAV 규칙만 만들 수 있습니다. 예를 들어 여러 개를 만들 수 없습니다 `volume-snapshot-delete` 규칙. 원하는 규칙 제약 조건은 하나의 규칙 내에 포함되어야 합니다.

보호할 규칙을 만들 수 있습니다 "알려 드립니다". 명령에 대한 보호 기능이 처음 제공되는 ONTAP 버전부터 각 명령을 보호할 수 있습니다.

MAV 시스템 기본 명령에 대한 규칙인 입니다 `security multi-admin-verify` "명령"변경할 수 없습니다.

시스템에서 정의한 작업 외에도 다음 명령은 다중 관리자 검증이 활성화된 경우 기본적으로 보호되지만, 규칙을 수정하여 이러한 명령에 대한 보호를 제거할 수 있습니다.

- "보안 로그인 암호"
- "보안 로그인 잠금 해제"
- "설정"

규칙 제약 조건

규칙을 만들 때 필요한 경우 명령 기능의 하위 집합으로 요청을 제한하는 옵션을 지정할 수 `-query` 있습니다. 이 `-query` 옵션을 사용하여 SVM, 볼륨, 스냅샷 이름과 같은 구성 요소를 제한할 수도 있습니다.

예를 들어 `volume snapshot delete` 명령에서 를 `-query` 로 설정할 수 있습니다 `-snapshot !hourly*,!daily*,!weekly*`. 즉, 매시간, 일별 또는 주별 속성으로 접두사가 지정된 볼륨 스냅샷이 MAV 보호에서 제외됩니다.

```
smci-vsim20::> security multi-admin-verify rule show
                                                 Required  Approval
Vserver Operation                                Approvers Groups
------- ---------------------------------------- --------- -------------
vs01    volume snapshot delete                   -         -
          Query: -snapshot !hourly*,!daily*,!weekly*
```

제외된 구성 요소는 MAV로 보호되지 않으므로 관리자가 삭제하거나 이름을 바꿀 수 있습니다.

기본적으로 규칙은 보호된 작업이 입력될 때 해당 명령이 자동으로 생성되도록 `security multi-admin-verify request create "protected_operation"` 지정합니다. 명령을 별도로 입력하도록 이 기본값을 수정할 수 `request create` 있습니다.

기본적으로 규칙별 예외를 지정할 수 있지만 규칙은 다음과 같은 전역 MAV 설정을 상속합니다.

- 필요한 승인자 수
- 승인 그룹
- 승인 만료 기간

- 실행 만료 기간

System Manager 절차

보호된 작업 규칙을 처음으로 추가하려면 에 System Manager 절차를 참조하십시오 "다중 관리 검증을 활성화합니다."

기존 규칙 집합을 수정하려면 다음을 수행합니다.

1. 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 섹션에서 * 다중 관리자 승인 * 옆에 있는 을 선택합니다 .
3. 규칙을 하나 이상 추가하려면 선택합니다 Add . 기존 규칙을 수정하거나 삭제할 수도 있습니다.
   - 작업 - 목록에서 지원되는 명령을 선택합니다.
   - 쿼리 - 원하는 명령 옵션 및 값을 입력합니다.
   - 선택적 매개 변수 – 글로벌 설정을 적용하려면 비워 두거나 글로벌 설정을 재정의하기 위해 특정 규칙에 다른 값을 할당합니다.
     - 승인자 수가 필요합니다
     - 승인 그룹

CLI 절차

모든 '보안 멀티 관리-검증 규칙' 명령은 '보안 멀티-관리-검증 규칙 표시'를 제외하고 실행 전에 MAV 관리자의 승인이 필요합니다.

원하는 사항	이 명령을 입력합니다
규칙을 만듭니다	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

현재 관리자의 자격 증명을 수정합니다	`security login modify <parameters>`
	
	• 예 *: 다음 규칙에 따라 루트 볼륨을 삭제해야 합니다.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

규칙을 수정합니다	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
규칙을 삭제합니다	`security multi-admin-verify rule delete -operation "protected_operation"`
규칙 표시	'보안 멀티-관리-검증 규칙 표시'

관련 정보

- "보안 다중 관리자 확인 규칙"
- "보안 로그인 수정"

ONTAP에서 **MAV** 보호 작업의 실행을 요청합니다

MAV(Multi-admin verification)를 사용하도록 설정된 클러스터에서 보호 작업 또는 명령을 시작하면 ONTAP가 자동으로 작업을 인터셉트하여 MAV 승인 그룹(MAV 관리자)의 한 명 이상의 관리자가 승인해야 하는 요청을 생성하도록 요청합니다. 또는 대화 상자 없이 MAV 요청을 만들 수 있습니다.

요청이 승인되면 쿼리에 응답하여 요청 만료 기간 내에 작업을 완료해야 합니다. 거부되거나 요청 또는 만료 기간이 초과된 경우 요청을 삭제하고 다시 제출해야 합니다.

MAV 기능은 기존 RBAC 설정을 그대로 사용합니다. 즉, 관리자 역할에 MAV 설정과 관계없이 보호된 작업을 실행할 수 있는 충분한 권한이 있어야 합니다. "RBAC에 대해 자세히 알아보십시오"..

MAV 관리자인 경우 보호된 작업을 실행하기 위한 요청도 MAV 관리자의 승인을 받아야 합니다.

System Manager 절차

사용자가 메뉴 항목을 클릭하여 작업을 시작하고 작업을 보호하는 경우 승인 요청이 생성되고 다음과 유사한 알림이 사용자에게 표시됩니다.

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

MAV가 활성화된 경우 사용자의 로그인 ID 및 MAV 역할(승인자 여부)에 따라 보류 중인 요청을 표시하는 * 다중 관리자 요청 * 창을 사용할 수 있습니다. 보류 중인 각 요청에 대해 다음 필드가 표시됩니다.

- 작동
- 색인(숫자)
- 상태(보류, 승인됨, 거부됨, 실행됨 또는 만료됨)

  한 승인자가 요청을 거부하면 추가 작업이 불가능합니다.

- 쿼리(요청된 작업의 매개 변수 또는 값)
- 사용자를 요청하는 중입니다
- 요청이 에 만료됩니다
- (수) 보류 중인 승인자
- (수) 잠재적 승인자

요청이 승인되면 요청 사용자는 만료 기간 내에 작업을 다시 시도할 수 있습니다.

사용자가 승인 없이 작업을 재시도하면 다음과 유사한 알림이 표시됩니다.

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

CLI 절차

1. 보호된 작업을 직접 입력하거나 MAV 요청 명령을 사용합니다.
   - 예제 – 볼륨을 삭제하려면 다음 명령 중 하나를 입력합니다. *
     - '볼륨 삭제'

```
cluster-1::*> volume delete -volume vol1 -vserver vs0

Warning: This operation requires multi-admin verification. To
create a
         verification request use "security multi-admin-verify
request
         create".

         Would you like to create a request for this operation?
          {y|n}: y

Error: command failed: The security multi-admin-verify request
(index 3) is
       auto-generated and requires approval.
```

     - `security multi-admin-verify request create "volume delete"`

```
Error: command failed: The security multi-admin-verify request
(index 3)
       requires approval.
```

2. 요청의 상태를 확인하고 MAV 통지에 응답합니다.
   a. 요청이 승인되면 CLI 메시지에 응답하여 작업을 완료합니다.
      - 예: *

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: approved
Required Approvers: 1
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Info: Volume "vol1" in Vserver "vs0" will be marked as deleted and
placed in the volume recovery queue. The space used by the volume
will be recovered only after the retention period of 12 hours has
completed. To recover the space immediately, get the volume name
using (privilege:advanced) "volume recovery-queue show vol1_*" and
then "volume recovery-queue purge -vserver vs0 -volume <volume_name>"
command. To recover the volume use the (privilege:advanced) "volume
recovery-queue recover -vserver vs0       -volume <volume_name>"
command.

Warning: Are you sure you want to delete volume "vol1" in Vserver
"vs0" ?
{y|n}: y
```

b. 요청이 거부되거나 만료 기간이 지난 경우 요청을 삭제하고 다시 제출하거나 MAV 관리자에게 문의하십시오.

   - 예: *

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: vetoed
Required Approvers: 1
 Pending Approvers: 1
   Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
         Approvals: -
       User Vetoed: admin2
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:38:47
     Time Approved: -
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

관련 정보

- "보안 다중 관리자 확인"

ONTAP에서 **MAV** 보호 작업 요청을 관리합니다

MAV 승인 그룹의 관리자(MAV 관리자)가 보류 중인 작업 실행 요청에 대해 알림을 받으면, 정해진 시간(승인 만료) 내에 승인 또는 거부 메시지로 응답해야 합니다. 충분한 수의 승인을 받지 못하면 요청자는 해당 요청을 삭제하고 다시 요청해야 합니다.

이 작업에 대해

승인 요청은 인덱스 번호로 식별되며, 이 번호는 이메일 메시지와 요청 대기열의 디스플레이에 포함됩니다.

> `multi-admin-verify`종료 상태의 요청은 자동으로 덮어쓰이거나 제거될 수 있습니다. 사용하세요"감사 로그" 이전 요청을 검토합니다.

요청 대기열의 다음 정보를 표시할 수 있습니다.

작동

요청이 생성되는 보호된 작업입니다.

쿼리

사용자가 작업을 적용하려는 개체(또는 개체)입니다.

상태

요청의 현재 상태, 보류, 승인, 거부, 만료됨, 실행됨. 한 승인자가 요청을 거부하면 추가 작업이 불가능합니다.

필수 승인자

요청을 승인하는 데 필요한 MAV 관리자 수 사용자는 작업 규칙에 필요한 승인자 매개 변수를 설정할 수 있습니다. 사용자가 필수 승인자를 규칙에 설정하지 않으면 전역 설정의 필수 승인자가 적용됩니다.

보류 중인 승인자

요청을 승인하기 위해 승인 요청을 승인해야 하는 MAV 관리자 수.

승인 만료

MAV 관리자가 승인 요청에 응답해야 하는 기간. 권한이 있는 사용자는 작업 규칙에 대한 승인 만료 기간을 설정할 수 있습니다. 규칙에 대해 승인-만료가 설정되어 있지 않으면 전역 설정의 승인-만료가 적용됩니다.

실행 만료

요청 관리자가 작업을 완료해야 하는 기간. 권한이 있는 사용자는 작업 규칙에 대해 실행 만료 기간을 설정할 수 있습니다. 규칙에 대해 execution-expiry를 설정하지 않으면 전역 설정에서의 execution-expiry가 적용됩니다.

사용자가 승인했습니다

요청을 승인한 MAV 관리자

사용자가 거부했습니다

요청에 거부권을 행사한 MAV 관리자

스토리지 **VM(SVM)**

요청이 연결된 SVM 이 릴리즈에서는 admin SVM만 지원합니다.

사용자가 요청되었습니다

요청을 생성한 사용자의 사용자 이름입니다.

생성 시간

요청이 생성된 시간입니다.

시간이 승인되었습니다

요청 상태가 승인으로 변경된 시간입니다.

설명

요청과 관련된 모든 메모.

사용자 허용

요청이 승인된 보호된 작업을 수행하도록 허용된 사용자 목록입니다. '사용자 허용'이 비어 있으면 적절한 권한을 가진 모든 사용자가 작업을 수행할 수 있습니다.

시스템 관리자

MAV 관리자는 승인 요청 세부 정보, 요청 만료 기간, 요청을 승인하거나 거부할 수 있는 링크가 포함된 이메일 메시지를 받습니다. 이메일의 링크를 클릭하여 승인 대화 상자에 접근하거나 시스템 관리자에서 *이벤트 및 작업 > 요청*으로 이동할 수 있습니다.

요청 창은 다중 관리자 검증이 활성화된 경우에 사용할 수 있으며, 사용자의 로그인 ID와 MAV 역할(승인자 여부)에 따라 보류 중인 요청을 표시합니다.

- 작동
- 색인(숫자)
- 상태(보류, 승인됨, 거부됨, 실행됨 또는 만료됨)

  한 승인자가 요청을 거부하면 추가 작업이 불가능합니다.

- 쿼리(요청된 작업의 매개 변수 또는 값)
- 사용자를 요청하는 중입니다
- 요청이 에 만료됩니다
- (수) 보류 중인 승인자
- (수) 잠재적 승인자

MAV 관리자는 이 창에 개별 작업 또는 선택한 작업 그룹을 승인, 거부 또는 삭제할 수 있는 추가 컨트롤이 있습니다. 그러나 MAV 관리자가 요청 사용자인 경우 자신의 요청을 승인, 거부 또는 삭제할 수 없습니다.

CLI를 참조하십시오

1. 보류 중인 요청에 대한 알림을 이메일로 받으면 요청의 색인 번호와 승인 만료 기간을 기록해 두세요. 인덱스 번호는 아래에 언급된 **show** 또는 **show-pending** 옵션을 사용하여 표시할 수도 있습니다.
2. 요청을 승인 또는 거부하십시오.

원하는 사항	이 명령을 입력합니다
요청을 승인합니다	'security multi-admin-verify request approve_nn_'
요청을 거부하십시오	'security multi-admin-verify request reject_nn_'
모든 요청, 보류 중인 요청 또는 단일 요청을 표시합니다	'security multi-admin-verify request{show	show-pending}[*nn*] {-fields_field1_[,*field2*…] [-instance]}' 대기열에 있는 모든 요청 또는 보류 중인 요청만 표시할 수 있습니다. 인덱스 번호를 입력하면 해당 에 대한 정보만 표시됩니다. 특정 필드('-fields' 매개 변수 사용) 또는 모든 필드('-instance' 매개 변수 사용)에 대한 정보를 표시할 수 있습니다.
요청을 삭제합니다	

예:

다음 시퀀스는 MAV 관리자가 이미 하나의 승인이 있는 색인 번호 3의 요청 이메일을 받은 후에 요청을 승인합니다.

```
          cluster1::> security multi-admin-verify request show-pending
                                      Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         julia


cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: approved
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: julia
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

예:

다음 시퀀스는 MAV 관리자가 이미 하나의 승인이 있는 색인 번호 3의 요청 이메일을 받은 후에 요청을 거부한다.

```
      cluster1::> security multi-admin-verify request show-pending
                                     Pending
Index Operation      Query State    Approvers Requestor
----- -------------- ----- -------- --------- ---------
    3 volume delete  -     pending 1         pavan


cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: vetoed
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin1
       User Vetoed: mav-admin2
           Vserver: cluster-1
    User Requested: pavan
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

관련 정보

- "보안 다중 관리자 확인"

동적 권한 부여 관리

ONTAP 동적 인증에 대해 알아보십시오

ONTAP 9.15.1부터 관리자는 동적 권한 부여를 구성 및 활성화하여 ONTAP에 대한 원격 액세스의 보안을 강화하는 한편 악의적인 행위자로 인해 발생할 수 있는 잠재적인 손상을 완화할 수 있습니다. ONTAP 9.15.1에서는 동적 권한 부여가 사용자에게 보안 점수를 할당하는 초기 프레임워크를 제공하며, 사용자의 활동이 의심스러운 경우 추가 권한 검사를 통해 사용자에게 문제를 주거나 작업을 완전히 거부할 수 있습니다. 관리자는 규칙을 만들고 신뢰 점수를 할당하며 제한 명령을 사용하여 특정 작업이 허용되거나 거부되는 시기를 결정할 수 있습니다. 관리자는 클러스터 전체 또는 개별 스토리지 VM에 대해 동적 권한 부여를 활성화할 수 있습니다.

동적 권한 부여 작동 방식

동적 권한 부여는 신뢰 점수 부여 시스템을 사용하여 권한 부여 정책에 따라 사용자에게 다른 신뢰 수준을 할당합니다. 사용자의 신뢰 수준에 따라 사용자가 수행하는 작업을 허용 또는 거부하거나 추가 인증을 요구하는 메시지가 표시될 수 있습니다.

"동적 권한 부여를 사용자 지정합니다"기준 점수 가중치 및 기타 동적 권한 부여 속성을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오.

신뢰할 수 있는 장치

동적 권한 부여가 사용 중인 경우 신뢰할 수 있는 장치의 정의는 사용자가 인증 방법 중 하나로 공개 키 인증을 사용하여 ONTAP에 로그인하는 데 사용하는 장치입니다. 해당 사용자만 해당 개인 키를 소유하므로 장치를 신뢰할 수 있습니다.

동적 권한 부여의 예입니다

볼륨을 삭제하려고 하는 세 명의 다른 사용자의 예를 들어 보십시오. 작업을 수행하려고 하면 각 사용자에 대한 위험 등급이 검사됩니다.

- 첫 번째 사용자는 이전 인증 실패가 거의 없는 신뢰할 수 있는 장치에서 로그인하므로 위험 등급이 낮아지며 추가 인증 없이 작업이 허용됩니다.
- 두 번째 사용자는 이전 인증 실패의 비율이 보통인 신뢰할 수 있는 장치에서 로그인하므로 위험 등급이 보통입니다. 작업을 허용하기 전에 추가 인증을 요청하는 메시지가 표시됩니다.
- 세 번째 사용자는 이전 인증 실패의 비율이 높은 신뢰할 수 없는 장치에서 로그인하므로 위험 등급이 높으므로 작업이 허용되지 않습니다.

다음 단계

- "동적 권한 부여를 사용하거나 사용하지 않습니다"
- "동적 권한 부여를 사용자 지정합니다"

ONTAP에서 동적 인증을 사용하거나 사용하지 않도록 설정합니다

ONTAP 9.15.1부터 관리자는 에서 동적 권한 부여를 구성하고 활성화할 수 있습니다 `visibility` 모드 를 눌러 구성을 테스트하거나 에서 를 누릅니다 `enforced` SSH를 통해 접속하는 CLI 사용자에 대한 구성을 활성화하는 모드입니다. 동적 인증이 더 이상 필요하지 않으면 비활성화할 수 있습니다. 동적 권한 부여를 비활성화해도 구성 설정을 계속 사용할 수 있으며 나중에 다시 사용하도록 설정하려는 경우 해당 설정을 사용할 수 있습니다.

에 대한 자세한 내용은 `security dynamic-authorization modify` "ONTAP 명령 참조입니다"을 참조하십시오.

테스트에 대한 동적 인증을 활성화합니다

표시 모드에서 동적 권한 부여를 활성화하면 기능을 테스트하고 사용자가 실수로 잠기지 않도록 할 수 있습니다. 이 모드에서는 모든 제한된 작업에서 신뢰 점수가 확인되지만 적용되지는 않습니다. 그러나 거부되거나 추가 인증 문제가 발생했을 수 있는 모든 작업이 기록됩니다. 가장 좋은 방법은 의도한 설정을 적용하기 전에 이 모드에서 테스트해야 합니다.

다른 동적 권한 부여 설정을 아직 구성하지 않은 경우에도 이 단계에 따라 처음으로 동적 권한 부여를 활성화할 수 있습니다. "동적 권한 부여를 사용자 지정합니다"사용자 환경에 맞게 사용자 지정할 수 있도록 다른 동적 권한 부여 설정을 구성하는 단계는 을 참조하십시오.

단계

1. 전역 설정을 구성하고 기능 상태를 로 변경하여 가시성 모드에서 동적 권한 부여를 활성화합니다 `visibility`. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. 를 사용하여 결과를 확인합니다 `show` 전역 설정을 표시하는 명령:

```
security dynamic-authorization show
```

강제 모드에서 동적 권한 부여를 활성화합니다

강제 적용 모드에서 동적 권한 부여를 활성화할 수 있습니다. 일반적으로 이 모드는 가시성 모드로 테스트를 완료한 후에 사용합니다. 이 모드에서는 모든 제한된 작업에서 신뢰 점수를 확인하고 제한 조건이 충족되면 활동 제한이 적용됩니다. 또한 억제 간격이 적용되어 지정된 간격 내에 추가적인 인증 문제가 발생하지 않습니다.

이 단계에서는 에서 동적 권한 부여를 이전에 구성하고 사용하도록 설정했다고 가정합니다 `visibility` 모드를 사용하는 것이 좋습니다.

단계

1. 에서 동적 권한 부여를 활성화합니다 `enforced` 모드로 변경합니다 `enforced`. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage_VM_name>
```

2. 를 사용하여 결과를 확인합니다 `show` 전역 설정을 표시하는 명령:

```
security dynamic-authorization show
```

동적 권한 부여를 비활성화합니다

추가 인증 보안이 더 이상 필요하지 않은 경우 동적 권한 부여를 비활성화할 수 있습니다.

단계

1. 상태를 로 변경하여 동적 권한 부여를 비활성화합니다 `disabled`. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. 를 사용하여 결과를 확인합니다 `show` 전역 설정을 표시하는 명령:

```
security dynamic-authorization show
```

에 대한 자세한 내용은 `security dynamic-authorization show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 단계

(선택 사항) 환경에 따라 "동적 권한 부여를 사용자 지정합니다"다른 동적 권한 부여 설정을 구성하려면 을 참조하십시오.

ONTAP에서 동적 권한 부여를 사용자 지정합니다

관리자는 동적 인증 구성의 다양한 측면을 사용자 지정하여 ONTAP 클러스터에 대한 원격 관리자 SSH 연결의 보안을 강화할 수 있습니다.

보안 요구에 따라 다음과 같은 동적 권한 부여 설정을 사용자 지정할 수 있습니다.

- 동적 권한 부여 전역 설정을 구성합니다
- 동적 권한 부여 신뢰 점수 구성 요소를 구성합니다
- 사용자 지정 신뢰 점수 공급자를 구성합니다
- 제한된 명령을 구성합니다
- 동적 권한 부여 그룹을 구성합니다

동적 권한 부여 전역 설정을 구성합니다

보호할 스토리지 VM, 인증 문제에 대한 억제 간격 및 신뢰 점수 설정을 비롯한 동적 권한 부여에 대한 글로벌 설정을 구성할 수 있습니다.

에 대한 자세한 내용은 `security login domain-tunnel create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 동적 권한 부여에 대한 글로벌 설정을 구성합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다.

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. 결과 구성을 봅니다.

```
security dynamic-authorization show
```

제한된 명령을 구성합니다

동적 권한 부여를 사용하면 제한된 기본 명령 집합이 기능에 포함됩니다. 이 목록은 필요에 맞게 수정할 수 있습니다. 을 참조하십시오 "MAV(Multi-admin Verification) 문서" 제한된 명령의 기본 목록에 대한 자세한 내용은

제한된 명령을 추가합니다

동적 권한 부여로 제한된 명령 목록에 명령을 추가할 수 있습니다.

에 대한 자세한 내용은 `security dynamic-authorization rule create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 명령을 추가합니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage_VM_name>
```

2. 제한된 명령의 결과 목록을 봅니다.

```
security dynamic-authorization rule show
```

제한된 명령을 제거합니다

동적 권한 부여로 제한된 명령 목록에서 명령을 제거할 수 있습니다.

에 대한 자세한 내용은 `security dynamic-authorization rule delete` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 명령을 제거합니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage_VM_name>
```

2. 제한된 명령의 결과 목록을 봅니다.

```
security dynamic-authorization rule show
```

동적 권한 부여 그룹을 구성합니다

기본적으로 동적 권한 부여는 모든 사용자 및 그룹을 활성화하는 즉시 적용됩니다. 그러나 을 사용하여 그룹을 생성할 수 있습니다 `security dynamic-authorization group create` 명령을 사용하여 동적 권한이 특정 사용자에게만 적용되도록 합니다.

동적 권한 부여 그룹을 추가합니다

동적 권한 부여 그룹을 추가할 수 있습니다.

에 대한 자세한 내용은 `security dynamic-authorization group create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 그룹을 만듭니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

```
security dynamic-authorization group create \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name> \
-excluded-usernames <user1,user2,user3...>
```

2. 결과 동적 권한 부여 그룹을 봅니다.

```
security dynamic-authorization group show
```

동적 권한 부여 그룹을 제거합니다

동적 권한 부여 그룹을 제거할 수 있습니다.

에 대한 자세한 내용은 `security dynamic-authorization group delete` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 그룹을 삭제합니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

```
security dynamic-authorization group delete \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. 결과 동적 권한 부여 그룹을 봅니다.

```
security dynamic-authorization group show
```

동적 권한 부여 신뢰 점수 구성 요소를 구성합니다

점수 매기기 기준의 우선 순위를 변경하거나 위험 점수에서 특정 기준을 제거하도록 최대 점수 가중치를 구성할 수 있습니다.

ⓘ 가장 좋은 방법은 기본 점수 가중치를 그대로 두고 필요한 경우에만 조정해야 합니다.

에 대한 자세한 내용은 `security dynamic-authorization trust-score-component modify` "ONTAP 명령 참조입니다"을 참조하십시오.

다음은 기본 점수 및 백분율 가중치와 함께 수정할 수 있는 구성 요소입니다.

기준	부품 이름	기본 원시 점수 가중치	기본 백분율 가중치
신뢰할 수 있는 장치	`trusted-device`	20	50
사용자 로그인 인증 기록	`authentication-history`	20	50

단계

1. 신뢰 점수 구성 요소를 수정합니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. 결과 신뢰 점수 구성 요소 설정을 봅니다.

```
security dynamic-authorization trust-score-component show
```

사용자의 신뢰 점수를 재설정합니다

시스템 정책으로 인해 사용자의 액세스가 거부되고 ID를 입증할 수 있는 경우 관리자는 사용자의 신뢰 점수를 재설정할 수 있습니다.

에 대한 자세한 내용은 `security dynamic-authorization user-trust-score reset` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 명령을 추가합니다. 을 참조하십시오 동적 권한 부여 신뢰 점수 구성 요소를 구성합니다 재설정할 수 있는 신뢰 점수 구성 요소 목록 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

신뢰 점수를 표시합니다

사용자는 로그인 세션에 대해 자신의 신뢰 점수를 표시할 수 있습니다.

단계

1. 신뢰 점수 표시:

```
security login whoami
```

다음과 유사한 출력이 표시됩니다.

```
User: admin
Role: admin
Trust Score: 50
```

에 대한 자세한 내용은 `security login whoami` "ONTAP 명령 참조입니다"을 참조하십시오.

사용자 지정 신뢰 점수 공급자를 구성합니다

외부 신뢰 점수 공급자로부터 채점 방법을 이미 받은 경우 사용자 지정 공급자를 동적 권한 부여 구성에 추가할 수 있습니다.

시작하기 전에

- 사용자 지정 신뢰 점수 공급자는 JSON 응답을 반환해야 합니다. 다음 구문 요구 사항을 충족해야 합니다.
  - 신뢰 점수를 반환하는 필드는 스칼라 필드여야 하며 배열 요소가 아닙니다.
  - 신뢰 점수를 반환하는 필드는 과 같이 중첩된 필드가 될 수 있습니다 `trust_score.value`.
  - JSON 응답 내에 숫자 신뢰 점수를 반환하는 필드가 있어야 합니다. 이 값을 기본적으로 사용할 수 없는 경우 래퍼 스크립트를 작성하여 이 값을 반환할 수 있습니다.
- 제공된 값은 신뢰 점수 또는 위험 점수일 수 있습니다. 신뢰 점수는 오름차순이고 신뢰 수준이 높을수록 높은 반면 위험 점수는 내림차순이라는 차이가 있습니다. 예를 들어 0에서 100 사이의 점수 범위에 대해 신뢰 점수가 90이면 점수가 매우 신뢰할 수 있고 추가 도전 없이 "허용"이 될 가능성이 높다는 것을 나타냅니다. 점수 범위가 0 ~ 100인 경우 위험 점수가 90이면 고위험이며 추가 도전 없이 "거부"가 발생할 가능성이 높습니다.
- ONTAP REST API를 통해 사용자 지정 신뢰 점수 공급자에 액세스할 수 있어야 합니다.
- 사용자 지정 신뢰 점수 공급자는 지원되는 매개 변수 중 하나를 사용하여 구성할 수 있어야 합니다. 지원되는 매개 변수 목록에 없는 구성이 필요한 사용자 지정 신뢰 점수 공급자는 지원되지 않습니다.

  에 대한 자세한 내용은 `security dynamic-authorization trust-score-component create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 사용자 지정 신뢰 점수 공급자를 추가합니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. 결과 신뢰 점수 공급자 설정을 봅니다.

```
security dynamic-authorization trust-score-component show
```

사용자 지정 신뢰 점수 공급자 태그를 구성합니다

태그를 사용하여 외부 신뢰 점수 공급자와 통신할 수 있습니다. 이렇게 하면 중요한 정보를 노출하지 않고 URL의 정보를 신뢰 점수 공급자로 보낼 수 있습니다.

에 대한 자세한 내용은 `security dynamic-authorization trust-score-component create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 신뢰 점수 공급자 태그를 활성화합니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

예를 들면 다음과 같습니다.

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

OAuth 2.0을 사용한 인증 및 권한 부여

ONTAP OAuth 2.0 구축 개요

ONTAP 9.14부터 OAuth 2.0(Open Authorization 2.0) 프레임워크를 사용하여 ONTAP 클러스터에 대한 액세스를 제어할 수 있습니다. 이 기능은 ONTAP CLI, System Manager, REST API를 포함한 모든 ONTAP 관리 인터페이스를 사용하여 구성할 수 있습니다. 그러나 OAuth 2.0 권한 부여 및 액세스 제어 결정은 클라이언트가 REST API를 사용하여 ONTAP에 액세스할 때만 적용할 수 있습니다.

OAuth 2.0 지원은 ONTAP 9.14.0에서 처음 도입되었으며 사용 중인 ONTAP 릴리스에 따라 가용성이 달라집니다. 를 참조하십시오 "ONTAP 릴리즈 노트" 를 참조하십시오.

기능 및 이점

ONTAP와 함께 OAuth 2.0을 사용할 때의 주요 기능과 이점은 다음과 같습니다.

OAuth 2.0 표준을 지원합니다

OAuth 2.0은 업계 표준 인증 프레임워크입니다. 서명된 액세스 토큰을 사용하여 보호된 리소스에 대한 액세스를 제한하고 제어하는 데 사용됩니다. OAuth 2.0을 사용하면 다음과 같은 여러 이점이 있습니다.

- 권한 부여 구성에 대한 다양한 옵션
- 암호를 포함한 클라이언트 자격 증명을 공개하지 마십시오
- 토큰은 구성에 따라 만료되도록 설정할 수 있습니다

- REST API와 함께 사용하는 데 가장 적합합니다

널리 사용되는 인증 서버에서 테스트했습니다

ONTAP OAuth 2.0 구현은 다음과 같이 ONTAP 릴리스를 기반으로 하는 몇 가지 일반적인 서버 또는 서비스에서 테스트되었습니다.

- ONTAP 9.16.1(이름 매핑 및 외부 역할에 대한 그룹 UUID 지원):
  - Microsoft Entra ID입니다
- ONTAP 9.14.1(표준 OAuth 2.0 기능 지원)
  - Auth0
  - ADFS(Active Directory Federation Service)
  - 키클로크

각 ONTAP 릴리즈에서 사용할 수 있는 기능에 대한 자세한 내용은 을 "인증 서버 및 액세스 토큰"참조하십시오.

여러 개의 동시 인증 서버 지원

단일 ONTAP 클러스터에 대해 최대 8개의 인증 서버를 정의할 수 있습니다. 따라서 다양한 보안 환경의 요구 사항을 충족할 수 있는 유연성을 제공합니다.

나머지 역할과의 통합

ONTAP 권한 부여 결정은 궁극적으로 사용자 또는 그룹에 할당된 REST 역할을 기반으로 합니다. 이러한 역할은 액세스 토큰에서 자체 포함된 범위 또는 Active Directory 또는 LDAP 그룹과 함께 로컬 ONTAP 정의를 기반으로 수행됩니다.

보낸 사람 제한 액세스 토큰을 사용하는 옵션입니다

클라이언트 인증을 강화하는 MTL(상호 전송 계층 보안)을 사용하도록 ONTAP 및 인증 서버를 구성할 수 있습니다. OAuth 2.0 액세스 토큰은 원래 발급된 클라이언트에서만 사용됩니다. 이 기능은 FAPI 및 MITRE에서 수립한 보안 권장 사항을 포함하여 몇 가지 일반적인 보안 권장 사항을 지원하고 그에 맞게 조정됩니다.

구현 및 구성

OAuth 2.0 구현 및 구성의 여러 측면을 개괄적으로 살펴보면 시작할 때 고려해야 할 사항이 있습니다.

ONTAP 내의 **OAuth 2.0** 엔티티

OAuth 2.0 권한 부여 프레임워크는 데이터 센터 또는 네트워크 내의 실제 요소 또는 가상 요소에 매핑할 수 있는 여러 엔터티를 정의합니다. OAuth 2.0 엔터티 및 ONTAP에 대한 적응은 아래 표에 나와 있습니다.

OAuth 2.0 엔티티	설명
리소스	내부 ONTAP 명령을 통해 ONTAP 리소스에 액세스하는 REST API 엔드포인트입니다.
리소스 소유자	보호된 리소스를 생성했거나 기본적으로 소유한 ONTAP 클러스터 사용자입니다.
리소스 서버	ONTAP 클러스터인 보호된 리소스의 호스트입니다.
클라이언트	리소스 소유자를 대신하거나 리소스 소유자의 권한이 있는 REST API 끝점에 대한 액세스를 요청하는 응용 프로그램입니다.
인증 서버	일반적으로 액세스 토큰 발급 및 관리 정책 적용을 담당하는 전용 서버입니다.

핵심 **ONTAP** 구성

OAuth 2.0을 활성화하고 사용하려면 ONTAP 클러스터를 구성해야 합니다. 여기에는 인증 서버에 대한 연결 설정 및 필요한 ONTAP 인증 구성 정의가 포함됩니다. 다음과 같은 관리 인터페이스를 사용하여 이 구성을 수행할 수 있습니다.

- ONTAP 명령줄 인터페이스입니다
- 시스템 관리자
- ONTAP REST API를 참조하십시오

환경 및 지원 서비스

ONTAP 정의 외에 인증 서버도 구성해야 합니다. 그룹-역할 매핑을 사용하는 경우 Active Directory 그룹 또는 이에 상응하는 LDAP도 구성해야 합니다.

지원되는 **ONTAP** 클라이언트

ONTAP 9.14부터 REST API 클라이언트는 OAuth 2.0을 사용하여 ONTAP에 액세스할 수 있습니다. REST API 호출을 실행하기 전에 인증 서버에서 액세스 토큰을 얻어야 합니다. 그런 다음 클라이언트는 HTTP 승인 요청 헤더를 사용하여 이 토큰을 _bearer token_으로 ONTAP 클러스터에 전달합니다. 필요한 보안 수준에 따라 클라이언트에서 인증서를 만들고 설치하여 MTL을 기반으로 보낸 사람 제한 토큰을 사용할 수도 있습니다.

선택된 용어

ONTAP를 사용하여 OAuth 2.0 배포를 살펴보기 시작하면 몇 가지 용어를 익히는 것이 좋습니다. 을 참조하십시오 "추가 리소스" OAuth 2.0에 대한 자세한 내용을 보려면 링크를 클릭하십시오.

액세스 토큰

인증 서버에서 발급되고 OAuth 2.0 클라이언트 응용 프로그램에서 보호된 리소스에 대한 액세스를 요청하는 데 사용하는 토큰입니다.

JSON 웹 토큰

액세스 토큰을 포맷하는 데 사용되는 표준입니다. JSON은 OAuth 2.0 클레임을 세 개의 주요 섹션으로 정렬한 작은 형식으로 표현하는 데 사용됩니다.

보낸 사람 제한 액세스 토큰

MTL(상호 전송 계층 보안) 프로토콜을 기반으로 하는 선택적 기능입니다. 토큰에 추가 확인 클레임을 사용하면 액세스 토큰이 원래 발급된 클라이언트에서만 액세스 토큰을 사용할 수 있습니다.

JSON 웹 키 집합입니다

JWKS는 ONTAP에서 클라이언트가 제시한 JWT 토큰을 확인하기 위해 사용하는 공개 키 모음입니다. 키 세트는 일반적으로 전용 URI를 통해 인증 서버에서 사용할 수 있습니다.

범위

범위를 사용하면 ONTAP REST API와 같은 보호된 리소스에 대한 응용 프로그램의 액세스를 제한하거나 제어할 수 있습니다. 액세스 토큰은 문자열로 표시됩니다.

ONTAP REST 역할입니다

ONTAP 9.6에 도입된 REST 역할은 ONTAP RBAC 프레임워크의 핵심 부분입니다. 이러한 역할은 ONTAP에서 여전히 지원하는 이전의 기존 역할과 다릅니다. ONTAP의 OAuth 2.0 구현은 REST 역할만 지원합니다.

HTTP 권한 부여 헤더

REST API 호출의 일부로 클라이언트 및 관련 권한을 식별하기 위한 HTTP 요청에 포함된 헤더 인증 및 권한 부여가 수행되는 방법에 따라 몇 가지 기능 또는 구현이 가능합니다. ONTAP에 OAuth 2.0 액세스 토큰을 제시할 때 토큰은 *bearer token* 으로 식별됩니다.

HTTP 기본 인증

초기 HTTP 인증 기법은 여전히 ONTAP에서 지원됩니다. 일반 텍스트 자격 증명(사용자 이름 및 암호)은 콜론으로 연결되고 base64로 인코딩됩니다. 이 문자열은 승인 요청 헤더에 배치되고 서버로 전송됩니다.

파피

금융 업계를 위한 프로토콜, 데이터 스키마 및 보안 권장 사항을 제공하는 OpenID Foundation의 작업 그룹입니다. 이 API는 원래 금융 등급 API로 알려져 있었습니다.

마이터

미국 공군과 미국 정부에 기술 및 보안 지침을 제공하는 비영리 민간 회사입니다.

추가 리소스

몇 가지 추가 리소스가 아래에 제공됩니다. OAuth 2.0 및 관련 표준에 대한 자세한 내용을 보려면 이러한 사이트를 검토해야 합니다.

프로토콜 및 표준

- "RFC 6749: OAuth 2.0 인증 프레임워크"
- "RFC 7519: JSON 웹 토큰(JWT)"
- "RFC 7523: OAuth 2.0 클라이언트 인증 및 권한 부여에 대한 JSON 웹 토큰(JWT) 프로파일"
- "RFC 7662: OAuth 2.0 토큰 소개"
- "RFC 7800: JWT에 대한 소유 증명 키"
- "RFC 8705: OAuth 2.0 상호 TLS 클라이언트 인증 및 인증서 바인딩된 액세스 토큰"

조직

- "OpenID 파운데이션"
- "FAPI 작업 그룹"
- "마이터"
- "IANA-JWT의 약어입니다"

제품 및 서비스

- "Auth0"
- "내부 ID"
- "ADFS 개요"
- "키클로크"

추가 도구 및 유틸리티

- "Auth0에 의한 JWT"
- "OpenSSL 을 참조하십시오"

NetApp 설명서 및 리소스

- "ONTAP 자동화 설명서"

개념

ONTAP 의 **OAuth 2.0** 권한 부여 서버 및 액세스 토큰

인증 서버는 OAuth 2.0 권한 부여 프레임워크 내에서 중앙 구성 요소로 몇 가지 중요한 기능을 수행합니다.

OAuth 2.0 인증 서버

권한 부여 서버는 주로 액세스 토큰을 만들고 서명합니다. 이러한 토큰에는 클라이언트 응용 프로그램이 보호된 리소스에 선택적으로 액세스할 수 있도록 하는 ID 및 권한 부여 정보가 포함되어 있습니다. 서버는 일반적으로 서로 격리되며 독립 실행형 전용 서버나 대규모 ID 및 액세스 관리 제품의 일부로 구현하는 등 여러 가지 방법으로 구현할 수 있습니다.

인증 서버에는 다른 용어를 사용할 수 있습니다. 특히 OAuth 2.0 기능이 보다 큰 ID 및 액세스 관리 제품 또는 솔루션 내에 패키지되어 있는 경우 더욱 그렇습니다. 예를 들어, * ID 공급자(IDP) * 라는 용어는 * 인증 서버 * 와 같은 의미로 사용되는 경우가 많습니다.

관리

권한 부여 서버는 액세스 토큰을 발급하는 것 외에도 일반적으로 웹 사용자 인터페이스를 통해 관련 관리 서비스를 제공합니다. 예를 들어 다음을 정의하고 관리할 수 있습니다.

- 사용자 및 사용자 인증
- 범위
- 테넌트 및 영역을 통한 관리 분리
- 정책 적용
- 다양한 외부 서비스에 연결
- 기타 ID 프로토콜(예: SAML) 지원

ONTAP는 OAuth 2.0 표준과 호환되는 인증 서버와 호환됩니다.

ONTAP로 정의

ONTAP에 하나 이상의 인증 서버를 정의해야 합니다. ONTAP는 각 서버와 안전하게 통신하여 토큰을 확인하고 클라이언트 응용 프로그램을 지원하는 기타 관련 작업을 수행합니다.

ONTAP 구성의 주요 측면은 다음과 같습니다. 도 참조하십시오 "OAuth 2.0 배포 시나리오" 를 참조하십시오.

액세스 토큰의 유효성 검사 방법 및 위치

액세스 토큰의 유효성을 검사하는 방법에는 두 가지가 있습니다.

- 로컬 검증

  ONTAP는 토큰을 발급한 인증 서버에서 제공한 정보를 기반으로 액세스 토큰의 유효성을 로컬로 검사할 수

있습니다. 인증 서버에서 검색된 정보는 ONTAP에 의해 캐시되고 정기적으로 새로 고쳐집니다.

- 원격 자기 주도

  또한 인증 서버에서 토큰의 유효성을 검사하기 위해 원격 검사를 사용할 수도 있습니다. introspection은 권한이 있는 사용자가 인증 서버에 액세스 토큰을 쿼리할 수 있도록 하는 프로토콜입니다. ONTAP는 액세스 토큰에서 특정 메타데이터를 추출하고 토큰의 유효성을 검사하는 방법을 제공합니다. ONTAP은 성능상의 이유로 일부 데이터를 캐싱합니다.

네트워크 위치

ONTAP가 방화벽 뒤에 있을 수 있습니다. 이 경우 프록시를 구성의 일부로 식별해야 합니다.

권한 부여 서버가 정의되는 방법

CLI, System Manager 또는 REST API를 포함한 관리 인터페이스를 사용하여 ONTAP에 권한 부여 서버를 정의할 수 있습니다. 예를 들어, CLI에서는 명령을 사용합니다 `security oauth2 client create`.

에 대한 자세한 내용은 `security oauth2 client create` "ONTAP 명령 참조입니다"을 참조하십시오.

인증 서버 수입니다

단일 ONTAP 클러스터에 대해 최대 8개의 인증 서버를 정의할 수 있습니다. 발급사 또는 발급사/대상 그룹 클레임이 고유하면 동일한 인증 서버를 동일한 ONTAP 클러스터에 두 번 이상 정의할 수 있습니다. 예를 들어 Keycloak를 사용하면 다른 영역을 사용할 때 항상 이 경우가 발생합니다.

OAuth 2.0 기능은 ONTAP에서 지원됩니다

OAuth 2.0에 대한 지원은 처음에 ONTAP 9.14.1에서 제공되었으며 이후 릴리스에서도 계속 향상되었습니다. ONTAP에서 지원하는 OAuth 2.0 기능은 아래에 설명되어 있습니다.

> ⓘ 특정 ONTAP 릴리스에서 도입된 기능은 향후 릴리스로 이전됩니다.

ONTAP 9.16.1

ONTAP 9.16.1은 기본 Entra ID 그룹에 대한 Entra ID별 확장을 포함하도록 표준 OAuth 2.0 기능을 확장합니다. 여기에는 이름 대신 액세스 토큰에 GUID를 사용하는 작업이 포함됩니다. 또한 릴리스는 액세스 토큰의 "역할" 필드를 사용하여 기본 ID 공급자 역할을 ONTAP 역할에 매핑하기 위해 외부 역할 매핑에 대한 지원을 추가합니다.

ONTAP 9.14.1

ONTAP 9.14.1부터 인증 서버는 다음을 사용하는 응용 프로그램에 대해 다음 표준 OAuth 2.0 기능을 통해 지원됩니다.

- 및 "RFC 7519: JSON 웹 토큰(JWT)" 에 설명된 대로 "ISS", "AUD" 및 "exp"와 같은 표준 필드가 있는 OAuth 2.0 "RFC6749: OAuth 2.0 인증 프레임워크" 여기에는 "UPN", "AppID", "sub", "username" 또는 "preferred_username"과 같은 액세스 토큰의 필드를 통해 사용자를 고유하게 식별하는 기능도 포함됩니다.
- "그룹" 필드가 있는 그룹 이름에 대한 ADFS 공급업체별 확장명입니다.
- "그룹" 필드가 있는 그룹 UUID에 대한 Azure 공급업체별 확장입니다.
- OAuth 2.0 액세스 토큰 범위 내에서 자체 포함 및 명명된 역할을 사용하는 인증 지원을 위한 ONTAP 확장 여기에는 범위 내의 그룹 이름뿐만 아니라 "범위" 및 "SCP" 필드가 포함됩니다.

OAuth 2.0 액세스 토큰 사용

인증 서버에서 발급한 OAuth 2.0 액세스 토큰은 ONTAP에서 검증하고 REST API 클라이언트 요청에 대한 역할 기반 액세스 결정을 내리는 데 사용됩니다.

액세스 토큰을 가져오는 중입니다

REST API를 사용하는 ONTAP 클러스터에 정의된 인증 서버에서 액세스 토큰을 얻어야 합니다. 토큰을 얻으려면 인증 서버에 직접 연결해야 합니다.

ONTAP는 액세스 토큰을 발급하거나 클라이언트에서 인증 서버로 요청을 리디렉션하지 않습니다.

토큰을 요청하는 방법은 다음과 같은 여러 요인에 따라 달라집니다.

- 인증 서버 및 구성 옵션
- OAuth 2.0 보조금 유형
- 요청을 발급하는 데 사용되는 클라이언트 또는 소프트웨어 도구입니다

허가 유형

A_GRANT_는 OAuth 2.0 액세스 토큰을 요청하고 수신하는 데 사용되는 네트워크 흐름 집합을 포함한 잘 정의된 프로세스입니다. 클라이언트, 환경 및 보안 요구 사항에 따라 여러 가지 다른 부여 형식을 사용할 수 있습니다. 인기 있는 보조금 유형 목록은 아래 표에 나와 있습니다.

허가 유형	설명
클라이언트 자격 증명입니다	ID 및 공유 암호 등 자격 증명만 사용하는 일반적인 부여 유형입니다. 클라이언트는 리소스 소유자와 밀접한 트러스트 관계를 갖는 것으로 간주됩니다.
암호	리소스 소유자 암호 자격 증명 부여 유형은 리소스 소유자가 클라이언트와 신뢰 관계가 설정된 경우에 사용할 수 있습니다. 레거시 HTTP 클라이언트를 OAuth 2.0으로 마이그레이션할 때도 유용합니다.
인증 코드	이는 기밀 클라이언트에 이상적인 보조금 유형이며 리디렉션 기반 흐름을 기반으로 합니다. 액세스 토큰을 가져오고 토큰을 새로 고치는 데 사용할 수 있습니다.

JWT 콘텐츠

OAuth 2.0 액세스 토큰은 JWT로 포맷됩니다. 콘텐츠는 사용자의 구성에 따라 인증 서버에서 만들어집니다. 그러나 토큰은 클라이언트 응용 프로그램에서 불투명합니다. 클라이언트는 토큰을 검사하거나 내용을 인식할 이유가 없습니다.

각 JWT 액세스 토큰에는 클레임 집합이 포함됩니다. 클레임은 권한 부여 서버의 관리 정의에 따라 발급자의 특성과 권한 부여를 설명합니다. 표준에 등록된 청구의 일부는 아래 표에 설명되어 있습니다. 모든 문자열은 대/소문자를 구분합니다.

청구	키워드	설명
발급사	아이에스에스주식회사	토큰을 발급한 보안 주체를 식별합니다. 신청 처리는 응용 프로그램에 따라 다릅니다.
제목	하위	토큰의 제목 또는 사용자입니다. 이름은 전역적으로 또는 로컬에서 고유하도록 범위가 지정됩니다.
대상	호주 달러	토큰을 받을 수신자입니다. 문자열 배열로 구현됩니다.

청구	키워드	설명
만료	만료	토큰이 만료되어 거부되어야 하는 시간입니다.

을 참조하십시오 "RFC 7519: JSON 웹 토큰" 를 참조하십시오.

클라이언트 인증

ONTAP 클라이언트 인증에 대한 개요 및 옵션

ONTAP OAuth 2.0 구현은 유연하고 강력하도록 설계되어 ONTAP 환경을 보호하는 데 필요한 기능을 제공합니다. 상호 배타적인 구성 옵션은 여러 가지가 있습니다. 권한 부여 결정은 궁극적으로 OAuth 2.0 액세스 토큰에 포함되어 있거나 OAuth 2.0 액세스 토큰에서 파생된 ONTAP REST 역할을 기반으로 합니다.

만 사용할 수 있습니다 "ONTAP REST 역할" OAuth 2.0에 대한 권한 부여를 구성하는 경우. 이전 ONTAP의 기존 역할은 지원되지 않습니다.

ONTAP는 사용자의 구성에 따라 가장 적합한 하나의 인증 옵션을 적용합니다. ONTAP에서 클라이언트 액세스 결정을 내리는 방법에 대한 자세한 내용은 을 "ONTAP에서 액세스를 결정하는 방법"참조하십시오.

OAuth 2.0 독립형 범위

이러한 범위에는 액세스 토큰의 단일 문자열 내에 캡슐화된 하나 이상의 사용자 지정 REST 역할이 포함됩니다. ONTAP 역할 정의와는 독립적입니다. 권한 부여 서버에서 범위 문자열을 구성해야 합니다. 자세한 내용은 을 "자체 포함된 OAuth 2.0 범위" 참조하십시오.

로컬 **ONTAP REST** 역할

builtin 또는 custom 중 하나의 명명된 REST 역할을 사용할 수 있습니다. 명명된 역할의 범위 구문은 * ontap-role - * <URL-encoded-ONTAP-role-name>입니다. 예를 들어, ONTAP 역할이 인 경우 `admin` 범위 문자열은 입니다 `ontap-role-admin`.

사용자

"http" 응용 프로그램에 대한 액세스 권한으로 정의된 액세스 토큰의 사용자 이름을 사용할 수 있습니다. 사용자는 정의된 인증 방법인 암호, 도메인(Active Directory), nsswitch(LDAP)에 따라 다음 순서로 테스트됩니다.

그룹

권한 부여 서버는 인증에 ONTAP 그룹을 사용하도록 구성할 수 있습니다. 로컬 ONTAP 정의를 검사했지만 액세스를 결정할 수 없는 경우 Active Directory("도메인") 또는 LDAP("nsswitch") 그룹이 사용됩니다. 그룹 정보는 다음 두 가지 방법 중 하나로 지정할 수 있습니다.

- OAuth 2.0 범위 문자열

  그룹 멤버십을 가진 사용자가 없는 경우 클라이언트 자격 증명 흐름을 사용하여 기밀 응용 프로그램을 지원합니다. 범위의 이름은 * ontap-group - * <URL-encoded-ONTAP-group-name>여야 합니다. 예를 들어 그룹이 "development"인 경우 범위 문자열은 "ontap-group-development"가 됩니다.

- "그룹" 요구 사항

  리소스 소유자(암호 부여) 흐름을 사용하여 ADFS에서 발급한 액세스 토큰에 사용됩니다.

보다 "ONTAP 에서 OAuth 2.0 또는 SAML IdP 그룹 작업" 자세한 내용은.

ONTAP 의 독립형 OAuth 2.0 범위

자체 포함 범위는 액세스 토큰으로 전달되는 문자열입니다. 각각은 완전한 사용자 지정 역할 정의이며 ONTAP에서 액세스 결정을 내리는 데 필요한 모든 것을 포함합니다. 범위는 ONTAP 자체 내에 정의된 모든 REST 역할과 별개입니다.

범위 문자열의 형식입니다

기본 수준에서 범위는 연속된 문자열로 표시되며 콜론으로 구분된 6개의 값으로 구성됩니다. 범위 문자열에 사용되는 매개 변수는 아래에 설명되어 있습니다.

ONTAP 리터럴

범위는 리터럴 값으로 시작해야 합니다 `ontap` 소문자로 입력합니다. ONTAP에만 해당하는 범위를 식별합니다.

클러스터

범위가 적용되는 ONTAP 클러스터를 정의합니다. 값은 다음과 같습니다.

- 클러스터 UUID

  단일 클러스터를 식별합니다.

- 별표(*)

  범위가 모든 클러스터에 적용됨을 나타냅니다.

ONTAP CLI 명령을 사용하여 클러스터의 UUID를 표시할 수 있습니다 `cluster identity show`. 지정하지 않으면 범위가 모든 클러스터에 적용됩니다. 에 대한 자세한 내용은 `cluster identity show` "ONTAP 명령 참조입니다 "을 참조하십시오.

역할

자체 포함된 범위에 포함된 REST 역할의 이름입니다. 이 값은 ONTAP에서 검사하거나 ONTAP에 정의된 기존 REST 역할과 일치하지 않습니다. 이 이름은 로깅에 사용됩니다.

액세스 수준

이 값은 범위에서 API 끝점을 사용할 때 클라이언트 응용 프로그램에 적용되는 액세스 수준을 나타냅니다. 아래 표에 설명된 대로 6개의 값이 있습니다.

액세스 수준	설명
없음	지정된 끝점에 대한 모든 액세스를 거부합니다.
읽기 전용	GET를 사용하여 읽기 액세스만 허용합니다.
read_create 를 참조하십시오	POST를 사용하여 새 리소스 인스턴스를 만들고 읽기 액세스를 허용합니다.

액세스 수준	설명
read_modify 를 참조하십시오	패치를 사용하여 기존 리소스를 업데이트할 수 있을 뿐 아니라 읽기 액세스를 허용합니다.
READ_CREATE_MODIFY 을 참조하십시오	삭제를 제외한 모든 액세스를 허용합니다. 허용되는 작업에는 GET(읽기), POST(작성) 및 패치(업데이트)가 포함됩니다.
모두	전체 액세스를 허용합니다.

SVM

클러스터 내 SVM의 이름이 범위에 적용됩니다. * 값(별표)을 사용하여 모든 SVM을 나타냅니다.

이 기능은 ONTAP 9.14.1에서 완벽하게 지원되지 않습니다. SVM 매개 변수를 무시하고 별표를 자리 표시자로 사용할 수 있습니다. 를 검토합니다 "ONTAP 릴리즈 노트" 향후 SVM 지원 확인

REST API URI입니다

리소스 또는 관련 리소스 집합에 대한 전체 또는 부분 경로입니다. 문자열은 로 시작해야 합니다 `/api`. 값을 지정하지 않으면 범위가 ONTAP 클러스터의 모든 API 끝점에 적용됩니다.

범위 예

다음은 자급식 범위의 몇 가지 예입니다.

ONTAP: *:joes-역할: read_create_modify: *:/api/cluster

이 역할에 할당된 사용자에게 에 대한 읽기, 생성 및 수정 액세스 권한을 제공합니다 `/cluster` 엔드포인트.

CLI 관리 도구

ONTAP는 자체 포함된 범위를 보다 쉽게 관리할 수 있도록 CLI 명령을 제공합니다 `security oauth2 scope` 입력 매개 변수를 기반으로 범위 문자열을 생성합니다.

명령을 입력합니다 `security oauth2 scope` 은 고객 입력에 따라 두 가지 사용 사례를 가지고 있습니다.

- 문자열 범위를 지정하는 CLI 매개 변수입니다

  이 버전의 명령을 사용하여 입력 매개 변수를 기반으로 범위 문자열을 생성할 수 있습니다.

- 문자열을 CLI 매개 변수로 지정합니다

  이 버전의 명령을 사용하여 입력 범위 문자열을 기반으로 명령 매개 변수를 생성할 수 있습니다.

예

다음 예제에서는 아래 명령 예제 다음에 포함된 출력으로 범위 문자열을 생성합니다. 이 정의는 모든 클러스터에 적용됩니다.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

`ontap:*:joes-role:readonly:*:/api/cluster`

에 대한 자세한 내용은 `security oauth2 scope` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 의 OAuth 2.0 외부 역할 매핑

외부 역할은 ONTAP에서 사용하도록 구성된 식별 공급자에서 정의됩니다. ONTAP CLI를 사용하여 이러한 외부 역할과 ONTAP 역할 간의 매핑 관계를 만들고 관리할 수 있습니다.

ONTAP REST API를 사용하여 외부 역할 매핑 기능을 구성할 수도 있습니다. 자세한 내용은 을 "ONTAP 자동화 설명서"참조하십시오.

액세스 토큰의 외부 역할

다음은 두 개의 외부 역할이 포함된 JSON 액세스 토큰의 일부입니다.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

구성

ONTAP 명령줄 인터페이스를 사용하여 외부 역할 매핑 기능을 관리할 수 있습니다.

생성

명령을 사용하여 역할 매핑 구성을 정의할 수 `security login external-role-mapping create` 있습니다. 이 명령과 관련 옵션을 실행하려면 ONTAP * admin * 권한 수준이어야 합니다.

매개 변수

그룹 매핑을 생성하는 데 사용되는 매개 변수는 아래에 설명되어 있습니다.

매개 변수	설명
`external-role`	외부 ID 공급자에 정의된 역할의 이름입니다.
`provider`	ID 공급자의 이름입니다. 시스템의 식별자여야 합니다.
`ontap-role`	외부 역할이 매핑되는 기존 ONTAP 역할을 나타냅니다.

예

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

에 대한 자세한 내용은 `security login external-role-mapping create` "ONTAP 명령 참조입니다"을 참조하십시오.

추가 **CLI** 작업

이 명령을 실행하면 다음과 같은 몇 가지 추가 작업이 지원됩니다.

- 표시
- 수정
- 삭제

관련 정보

- "ONTAP 명령 참조입니다"

ONTAP가 클라이언트 액세스를 결정하는 방법

OAuth 2.0을 올바르게 설계하고 구현하려면 ONTAP에서 클라이언트의 액세스 결정을 내리기 위해 인증 구성이 사용되는 방법을 이해해야 합니다. 액세스를 결정하는 데 사용되는 주요 단계는 ONTAP 릴리스에 따라 아래에 나와 있습니다.

ONTAP 9.15.1에서 중요한 OAuth 2.0 업데이트가 없었습니다. 9.15.1 릴리스를 사용하는 경우 ONTAP 9.14.1에 대한 설명을 참조하십시오.

관련 정보

- "OAuth 2.0 기능은 ONTAP에서 지원됩니다"

ONTAP 9.16.1

ONTAP 9.16.1은 표준 OAuth 2.0 지원을 확장하여 기본 Entra ID 그룹에 대한 Microsoft Entra ID별 확장 및 외부 역할 매핑을 포함합니다.

ONTAP 9.16.1에 대한 클라이언트 액세스를 확인합니다

1단계**:** 자체 포함 범위

액세스 토큰에 자체 포함된 범위가 포함되어 있는 경우 ONTAP는 먼저 이러한 범위를 검사합니다. 자체 포함된 범위가 없는 경우 2단계로 이동합니다.

하나 이상의 자체 포함 범위가 있는 경우 ONTAP는 명시적 * allow * 또는 * deny * 결정을 내릴 수 있을 때까지 각 범위를 적용합니다. 명시적인 결정이 내려지면 처리가 종료됩니다.

ONTAP에서 명시적인 액세스 결정을 내릴 수 없는 경우 2단계를 계속 진행합니다.

2단계**:** 로컬 역할 플래그를 확인합니다

ONTAP는 부울 매개 변수를 `use-local-roles-if-present`검사합니다. 이 플래그의 값은 ONTAP로 정의된 각 인증 서버에 대해 별도로 설정됩니다.

- 값이 이면 `true` 3단계를 계속 진행합니다.
- 값이 이면 `false` 처리가 종료되고 액세스가 거부됩니다.

3단계**:** 이름이 지정된 **ONTAP REST** 역할입니다

액세스 토큰에 OR `scp` 필드에 이름이 지정된 REST 역할이 포함되어 있거나 클레임으로 포함되어 있는 경우 `scope` ONTAP는 해당 역할을 사용하여 액세스 결정을 내립니다. 이렇게 하면 항상 * allow * 또는 * deny * 결정이 되고 처리가 종료됩니다.

이름이 지정된 REST 역할이 없거나 역할을 찾을 수 없는 경우 4단계를 계속 진행하십시오.

4단계**:** 사용자

액세스 토큰에서 사용자 이름을 추출하고 "http" 응용 프로그램에 액세스할 수 있는 사용자와 일치시키려고 시도합니다. 사용자는 다음과 같은 순서로 인증 방법에 따라 검사됩니다.

- 암호
- 도메인(Active Directory)
- Nsswitch(LDAP)

일치하는 사용자가 발견되면 ONTAP는 사용자에게 정의된 역할을 사용하여 액세스 결정을 내립니다. 이로 인해 항상 * allow * 또는 * deny * 결정이 내려지고 처리가 종료됩니다.

사용자가 일치하지 않거나 액세스 토큰에 사용자 이름이 없는 경우 5단계를 계속 진행합니다.

5단계**:** 그룹

하나 이상의 그룹이 포함된 경우 형식이 검사됩니다. 그룹이 UUID로 표현된 경우 내부 그룹 매핑 테이블이 검색됩니다. 그룹과 일치하는 역할이 있고 연관된 역할이 있는 경우, ONTAP 해당 그룹에 정의된 역할을 사용하여 액세스 결정을 내립니다. 이는 항상 **ALLOW** 또는 **DENY** 결정으로 이어지고 처리가 종료됩니다. 자세한 내용은 다음을 참조하십시오. "ONTAP 에서 OAuth 2.0 또는 SAML IdP 그룹 작업" .

그룹이 이름으로 표시되고 도메인 또는 nsswitch 인증을 사용하여 구성된 경우 ONTAP는 각 그룹을 Active Directory 또는 LDAP 그룹과 일치시키려고 시도합니다. 그룹 일치 항목이 있는 경우 ONTAP는 그룹에 대해 정의된 역할을 사용하여 액세스 결정을 내립니다. 이로 인해 항상 * allow * 또는 * deny * 결정이 내려지고 처리가 종료됩니다.

일치하는 그룹이 없거나 액세스 토큰에 그룹이 없으면 액세스가 거부되고 처리가 종료됩니다.

ONTAP 9.14.1

지원되는 초기 OAuth 2.0은 표준 OAuth 2.0 기능을 기반으로 하는 ONTAP 9.14.1에 도입되었습니다.

ONTAP 9.14.1에 대한 클라이언트 액세스를 확인합니다

1단계**:** 자체 포함 범위

액세스 토큰에 자체 포함된 범위가 포함되어 있는 경우 ONTAP는 먼저 이러한 범위를 검사합니다. 자체 포함된 범위가 없는 경우 2단계로 이동합니다.

하나 이상의 자체 포함 범위가 있는 경우 ONTAP는 명시적 * allow * 또는 * deny * 결정을 내릴 수 있을 때까지 각 범위를 적용합니다. 명시적인 결정이 내려지면 처리가 종료됩니다.

ONTAP에서 명시적인 액세스 결정을 내릴 수 없는 경우 2단계를 계속 진행합니다.

2단계**:** 로컬 역할 플래그를 확인합니다

ONTAP는 부울 매개 변수를 `use-local-roles-if-present`검사합니다. 이 플래그의 값은 ONTAP로 정의된 각 인증 서버에 대해 별도로 설정됩니다.

- 값이 이면 `true` 3단계를 계속 진행합니다.
- 값이 이면 `false` 처리가 종료되고 액세스가 거부됩니다.

3단계**:** 이름이 지정된 **ONTAP REST** 역할입니다

액세스 토큰에 OR `scp` 필드에 이름이 지정된 REST 역할이 포함된 경우 `scope` ONTAP는 해당 역할을 사용하여 액세스 결정을 내립니다. 이렇게 하면 항상 * allow * 또는 * deny * 결정이 되고 처리가 종료됩니다.

이름이 지정된 REST 역할이 없거나 역할을 찾을 수 없는 경우 4단계를 계속 진행하십시오.

4단계**:** 사용자

액세스 토큰에서 사용자 이름을 추출하고 "http" 응용 프로그램에 액세스할 수 있는 사용자와 일치시키려고 시도합니다. 사용자는 다음과 같은 순서로 인증 방법에 따라 검사됩니다.

- 암호
- 도메인(Active Directory)
- Nsswitch(LDAP)

일치하는 사용자가 발견되면 ONTAP는 사용자에게 정의된 역할을 사용하여 액세스 결정을 내립니다. 이로 인해 항상 * allow * 또는 * deny * 결정이 내려지고 처리가 종료됩니다.

사용자가 일치하지 않거나 액세스 토큰에 사용자 이름이 없는 경우 5단계를 계속 진행합니다.

5단계**:** 그룹

하나 이상의 그룹이 도메인 또는 nsswitch 인증을 사용하여 포함되어 구성된 경우 ONTAP는 이러한 그룹을 각각 Active Directory 또는 LDAP 그룹과 일치시키려고 시도합니다.

그룹 일치 항목이 있는 경우 ONTAP는 그룹에 대해 정의된 역할을 사용하여 액세스 결정을 내립니다. 이로 인해 항상 * allow * 또는 * deny * 결정이 내려지고 처리가 종료됩니다.

일치하는 그룹이 없거나 액세스 토큰에 그룹이 없으면 액세스가 거부되고 처리가 종료됩니다.

ONTAP 사용한 OAuth 2.0 배포 시나리오

ONTAP에 대한 인증 서버를 정의할 때 사용할 수 있는 몇 가지 구성 옵션이 있습니다. 이러한 옵션에 따라 몇 가지 배포 시나리오 중 하나를 사용하여 사용자 환경에 적합한 인증 서버를 정의할 수 있습니다.

구성 매개 변수 요약

ONTAP에 대한 인증 서버를 정의할 때 사용할 수 있는 몇 가지 구성 매개 변수가 있습니다. 이러한 매개 변수는 일반적으로 모든 관리 인터페이스에서 지원됩니다.

> 개별 매개 변수 또는 필드에 사용되는 이름은 ONTAP 관리 인터페이스에 따라 다를 수 있습니다. 관리 인터페이스의 차이를 수용하기 위해 테이블의 각 매개 변수에 하나의 일반 이름이 사용됩니다. 특정 인터페이스에 사용되는 정확한 이름은 컨텍스트에 따라 명확해야 합니다.

매개 변수	설명
이름	ONTAP에 알려진 인증 서버의 이름입니다.
응용 프로그램	정의가 적용되는 ONTAP 내부 응용 프로그램입니다. 이 값은 * http * 여야 합니다.
발급자 URI입니다	토큰을 발급하는 사이트 또는 조직을 식별하는 경로가 있는 FQDN입니다.
공급자 JWKS URI입니다	ONTAP가 액세스 토큰의 유효성을 검사하는 데 사용되는 JSON 웹 키 세트를 가져오는 경로 및 파일 이름의 FQDN입니다.
JWKS 새로 고침 간격입니다	ONTAP가 공급자 JWKS URI에서 인증서 정보를 새로 고치는 빈도를 결정하는 시간 간격입니다. 값은 ISO-8601 형식으로 지정됩니다.
성찰의 끝점입니다	ONTAP에서 자체 조사를 통해 원격 토큰 유효성 검사를 수행하는 데 사용하는 경로가 있는 FQDN입니다.
클라이언트 ID입니다	인증 서버에 정의된 클라이언트의 이름입니다. 이 값이 포함된 경우 인터페이스를 기반으로 연결된 클라이언트 암호도 제공해야 합니다.
발신 프록시	이는 ONTAP가 방화벽 뒤에 있을 때 인증 서버에 대한 액세스를 제공하기 위한 것입니다. URI는 curl 형식이어야 합니다.
있는 경우 로컬 역할을 사용합니다	로컬 ONTAP 정의가 사용되는지 여부를 결정하는 부울 플래그(명명된 REST 역할 및 로컬 사용자 포함)
원격 사용자 클레임	ONTAP에서 로컬 사용자와 일치시키기 위해 사용하는 대체 이름입니다. 를 사용합니다 `sub` 로컬 사용자 이름과 일치하는 액세스 토큰의 필드입니다.
대상	이 필드는 액세스 토큰을 사용할 수 있는 끝점을 정의합니다.

배포 시나리오

다음은 몇 가지 일반적인 배포 시나리오입니다. 토큰 유효성 검사는 ONTAP에서 로컬로 수행되는지 아니면 인증 서버에서 원격으로 수행되는지를 기준으로 구성됩니다. 각 시나리오에는 필요한 구성 옵션 목록이 포함되어 있습니다. 을 참조하십시오 "ONTAP에 OAuth 2.0 배포" 구성 명령의 예를 참조하십시오.

> 인증 서버를 정의한 후 ONTAP 관리 인터페이스를 통해 구성을 표시할 수 있습니다. 예를 들어, 명령을 사용합니다 `security oauth2 client show` ONTAP CLI 사용.

로컬 검증

다음 배포 시나리오는 토큰 유효성 검사를 로컬로 수행하는 ONTAP를 기반으로 합니다.

프록시 없이 자체 포함된 범위를 사용합니다

이것은 OAuth 2.0 자체 포함 범위만 사용하는 가장 간단한 배포입니다. 로컬 ONTAP ID 정의는 사용되지 않습니다. 다음 매개 변수를 포함해야 합니다.

- 이름
- 응용 프로그램(http)
- 공급자 JWKS URI입니다
- 발급자 URI입니다

또한 인증 서버에 범위를 추가해야 합니다.

프록시에 자체 포함된 범위를 사용합니다

이 배포 시나리오에서는 OAuth 2.0 자체 포함 범위를 사용합니다. 로컬 ONTAP ID 정의는 사용되지 않습니다. 하지만 인증 서버는 방화벽 뒤에 있으므로 프록시를 구성해야 합니다. 다음 매개 변수를 포함해야 합니다.

- 이름
- 응용 프로그램(http)
- 공급자 JWKS URI입니다
- 발신 프록시
- 발급자 URI입니다
- 대상

또한 인증 서버에 범위를 추가해야 합니다.

프록시에 로컬 사용자 역할 및 기본 사용자 이름 매핑을 사용합니다

이 배포 시나리오에서는 기본 이름 매핑과 함께 로컬 사용자 역할을 사용합니다. 원격 사용자 클레임은 기본값인 을 사용합니다 `sub` 액세스 토큰의 이 필드는 로컬 사용자 이름과 일치시키는 데 사용됩니다. 사용자 이름은 40자 이하여야 합니다. 인증 서버는 방화벽 뒤에 있으므로 프록시를 구성해야 합니다. 다음 매개 변수를 포함해야 합니다.

- 이름
- 응용 프로그램(http)
- 공급자 JWKS URI입니다
- 있는 경우 로컬 역할을 사용합니다 (`true`)
- 발신 프록시
- 발급사

로컬 사용자가 ONTAP로 정의되었는지 확인해야 합니다.

프록시를 사용하여 로컬 사용자 역할 및 대체 사용자 이름 매핑을 사용합니다

이 배포 시나리오에서는 로컬 ONTAP 사용자와 일치시키는 데 사용되는 대체 사용자 이름과 함께 로컬 사용자 역할을 사용합니다. 인증 서버는 방화벽 뒤에 있으므로 프록시를 구성해야 합니다. 다음 매개 변수를 포함해야 합니다.

- 이름
- 응용 프로그램(http)
- 공급자 JWKS URI입니다
- 있는 경우 로컬 역할을 사용합니다 (`true`)
- 원격 사용자 클레임
- 발신 프록시
- 발급자 URI입니다
- 대상

로컬 사용자가 ONTAP로 정의되었는지 확인해야 합니다.

원격 자기 주도

다음 배포 구성은 ONTAP를 기반으로 합니다. 이 구성은 자체 조사를 통해 토큰 유효성 검사를 원격으로 수행합니다.

프록시 없이 자체 포함된 범위를 사용합니다

OAuth 2.0 독립형 범위를 사용하여 간단하게 배포할 수 있습니다. ONTAP ID 정의는 사용되지 않습니다. 다음 매개 변수를 포함해야 합니다.

- 이름
- 응용 프로그램(http)
- 성찰의 끝점입니다
- 클라이언트 ID입니다
- 발급자 URI입니다

인증 서버에서 클라이언트 및 클라이언트 비밀은 물론 범위를 정의해야 합니다.

관련 정보

- "보안 oauth2 클라이언트 표시"

OAuth 2.0 Mutual TLS를 사용한 **ONTAP** 클라이언트 인증

보안 요구에 따라 강력한 클라이언트 인증을 구현하도록 MTL(Mutual TLS)을 선택적으로 구성할 수 있습니다. OAuth 2.0 배포의 일부로 ONTAP와 함께 사용할 경우 MTL은 액세스 토큰이 원래 발급된 클라이언트에서만 사용되도록 보장합니다.

상호 **TLS**와 **OAuth 2.0**

TLS(Transport Layer Security)는 두 애플리케이션(일반적으로 클라이언트 브라우저와 웹 서버)간에 보안 통신 채널을 설정하는 데 사용됩니다. 상호 TLS는 클라이언트 인증서를 통해 클라이언트를 강력하게 식별함으로써 이 기능을 확장합니다. OAuth 2.0이 있는 ONTAP 클러스터에서 사용할 경우 기본 MTL 기능은 보낸 사람 제한 액세스 토큰을 생성하고 사용하여 확장됩니다.

보낸 사람 제한 액세스 토큰은 원래 발급된 클라이언트에서만 사용할 수 있습니다. 이 기능을 지원하기 위해 새로운 확인 요청이 있습니다 (`cnf`)이 토큰에 삽입됩니다. 필드에 속성이 포함되어 있습니다 `x5t#S256` 액세스 토큰을 요청할 때

사용되는 클라이언트 인증서의 다이제스트가 들어 있습니다. 이 값은 토큰 유효성 검사의 일부로 ONTAP에서 확인합니다. 보낸 사람 제한이 없는 인증 서버에서 발급한 액세스 토큰에는 추가 확인 클레임이 포함되지 않습니다.

각 인증 서버에 대해 MTL을 별도로 사용하도록 ONTAP를 구성해야 합니다. 예를 들어, CLI 명령을 사용할 수 있습니다 `security oauth2 client` 매개 변수를 포함합니다 `use-mutual-tls` 아래 표와 같이 세 가지 값을 기반으로 MTL 처리를 제어합니다.

> 각 구성에서 ONTAP가 수행한 결과 및 작업은 구성 매개 변수 값과 액세스 토큰 및 클라이언트 인증서의 내용에 따라 달라집니다. 표의 매개 변수는 최소 값부터 최대 제한값까지 구성됩니다.

매개 변수	설명
없음	인증 서버에 대해 OAuth 2.0 상호 TLS 인증이 완전히 비활성화되었습니다. 토큰에 확인 클레임이 있거나 TLS 연결과 함께 클라이언트 인증서가 제공된 경우에도 ONTAP는 MTL 클라이언트 인증서 인증을 수행하지 않습니다.
요청	OAuth 2.0 상호 TLS 인증은 클라이언트가 보낸 사람 제한 액세스 토큰을 제공하는 경우 적용됩니다. 즉, MTL은 확인 요청(속성 포함)이 있는 경우에만 적용됩니다 `x5t#S256`)이 액세스 토큰에 있습니다. 기본 설정입니다.
필수 요소입니다	OAuth 2.0 상호 TLS 인증은 인증 서버에서 발급한 모든 액세스 토큰에 대해 적용됩니다. 따라서 모든 액세스 토큰은 sender-constraint여야 합니다. 액세스 토큰에 확인 클레임이 없거나 잘못된 클라이언트 인증서가 있는 경우 인증 및 REST API 요청이 실패합니다.

높은 수준의 구현 흐름

ONTAP 환경에서 OAuth 2.0과 함께 MTL을 사용할 때 적용되는 일반적인 단계는 다음과 같습니다. 을 참조하십시오 "RFC 8705: OAuth 2.0 상호 TLS 클라이언트 인증 및 인증서 바인딩된 액세스 토큰" 를 참조하십시오.

1단계**:** 클라이언트 인증서를 생성하고 설치합니다

클라이언트 ID 설정은 클라이언트 개인 키에 대한 지식을 입증하기 위한 것입니다. 해당 공개 키는 클라이언트에서 제공하는 서명된 X.509 인증서에 저장됩니다. 클라이언트 인증서 만들기와 관련된 단계는 다음과 같습니다.

1. 공개 및 개인 키 쌍을 생성합니다
2. 인증서 서명 요청을 만듭니다
3. CSR 파일을 잘 알려진 CA로 보냅니다
4. CA에서 요청을 확인하고 서명된 인증서를 발급합니다

일반적으로 클라이언트 인증서를 로컬 운영 체제에 설치하거나 curl과 같은 공통 유틸리티를 사용하여 직접 사용할 수 있습니다.

2단계**: MTL**을 사용하도록 **ONTAP**를 구성합니다

MTL을 사용하도록 ONTAP을 구성해야 합니다. 이 구성은 각 인증 서버에 대해 별도로 수행됩니다. 예를 들어, CLI를 사용하면 명령을 사용할 수 있습니다 `security oauth2 client` 선택적 매개 변수와 함께 사용됩니다 `use-mutual-tls`. 을 참조하십시오 "ONTAP에 OAuth 2.0 배포" 를 참조하십시오.

3단계**:** 클라이언트가 액세스 토큰을 요청합니다

클라이언트는 ONTAP로 구성된 인증 서버에서 액세스 토큰을 요청해야 합니다. 클라이언트 응용 프로그램은 1단계에서 생성하고 설치한 인증서가 있는 MTL을 사용해야 합니다.

4단계**:** 인증 서버가 액세스 토큰을 생성합니다

인증 서버는 클라이언트 요청을 확인하고 액세스 토큰을 생성합니다. 이 과정에서 클라이언트 인증서의 메시지 다이제스트가 생성되며, 이 다이제스트는 토큰에 확인 클레임(필드)으로 포함됩니다 `cnf`)를 클릭합니다.

5단계**:** 클라이언트 애플리케이션이 **ONTAP**에 액세스 토큰을 제공합니다

클라이언트 응용 프로그램은 ONTAP 클러스터에 REST API 호출을 수행하고 권한 부여 요청 헤더에 액세스 토큰을 * 베어러 토큰 * 으로 포함합니다. 클라이언트는 액세스 토큰을 요청하는 데 사용된 것과 동일한 인증서를 가진 MTL을 사용해야 합니다.

6단계**: ONTAP**는 클라이언트와 토큰을 확인합니다**.**

ONTAP는 MTL 처리의 일부로 사용되는 클라이언트 인증서뿐만 아니라 HTTP 요청으로 액세스 토큰을 받습니다. ONTAP는 먼저 액세스 토큰의 서명을 확인합니다. 구성에 따라 ONTAP는 클라이언트 인증서의 메시지 다이제스트를 생성하고 토큰의 확인 클레임 * CNF * 와 비교합니다. 두 값이 일치하면 ONTAP는 API 요청을 하는 클라이언트가 액세스 토큰이 원래 발급된 클라이언트와 동일하다는 것을 확인했습니다.

관련 정보

- "보안 oauth2 클라이언트"

구성 및 배포

ONTAP와 함께 **OAuth 2.0**을 배포할 준비를 하십시오

ONTAP 환경에서 OAuth 2.0을 구성하기 전에 배포를 준비해야 합니다. 주요 작업과 결정에 대한 요약이 아래에 나와 있습니다. 섹션의 정렬은 일반적으로 따라야 할 순서에 맞춰집니다. 그러나 대부분의 배포에는 적용되지만 필요에 따라 환경에 맞게 조정해야 합니다. 공식 배포 계획을 작성하는 것도 고려해야 합니다.

사용자 환경에 따라 ONTAP에 정의된 인증 서버에 대한 구성을 선택할 수 있습니다. 여기에는 각 배포 유형에 대해 구체화해야 하는 매개 변수 값이 포함됩니다. 을 참조하십시오 "OAuth 2.0 배포 시나리오" 를 참조하십시오.

보호된 리소스 및 클라이언트 응용 프로그램

OAuth 2.0은 보호된 리소스에 대한 액세스를 제어하기 위한 권한 부여 프레임워크입니다. 이 점을 감안하면 모든 배포에서 중요한 첫 단계는 사용 가능한 리소스가 무엇이고 어떤 클라이언트가 액세스할 필요가 있는지 확인하는 것입니다.

클라이언트 애플리케이션을 식별합니다

REST API 호출을 실행할 때 OAuth 2.0을 사용할 클라이언트와 이들이 액세스해야 하는 API 엔드포인트를 결정해야 합니다.

기존 **ONTAP REST** 역할 및 로컬 사용자를 검토합니다

REST 역할 및 로컬 사용자를 포함하여 기존 ONTAP ID 정의를 검토해야 합니다. OAuth 2.0을 구성하는 방법에 따라 이러한 정의를 액세스 결정에 사용할 수 있습니다.

OAuth 2.0으로의 글로벌 전환

OAuth 2.0 인증을 점진적으로 구현할 수도 있지만 각 인증 서버에 대한 글로벌 플래그를 설정하여 모든 REST API 클라이언트를 OAuth 2.0으로 즉시 이동할 수도 있습니다. 따라서 자체 포함된 범위를 만들 필요 없이 기존 ONTAP 구성을 기반으로 액세스 결정을 내릴 수 있습니다.

인증 서버

권한 부여 서버는 액세스 토큰을 발행하고 관리 정책을 시행함으로써 OAuth 2.0 배포에서 중요한 역할을 수행합니다.

인증 서버를 선택하여 설치합니다

하나 이상의 인증 서버를 선택하여 설치해야 합니다. 범위를 정의하는 방법을 비롯하여 ID 공급자의 구성 옵션 및 절차를 숙지하는 것이 중요합니다. Microsoft Entra ID를 비롯한 일부 인증 서버는 이름 대신 UUID를 사용하여 그룹을 나타냅니다.

인증 루트 **CA** 인증서를 설치해야 하는지 확인합니다

ONTAP는 인증 서버의 인증서를 사용하여 클라이언트가 제공하는 서명된 액세스 토큰의 유효성을 검사합니다. 이렇게 하려면 ONTAP에서 루트 CA 인증서와 모든 중간 인증서가 필요합니다. ONTAP와 함께 사전 설치되어 있을 수 있습니다. 그렇지 않은 경우 설치해야 합니다.

네트워크 위치 및 구성을 평가합니다

인증 서버가 방화벽 뒤에 있는 경우 프록시 서버를 사용하도록 ONTAP를 구성해야 합니다.

클라이언트 인증 및 권한 부여

클라이언트 인증 및 권한 부여에는 몇 가지 측면을 고려해야 합니다.

자체 포함된 범위 또는 로컬 **ONTAP ID** 정의

상위 수준에서는 권한 부여 서버에서 정의된 자체 포함 범위를 정의하거나 역할 및 사용자를 비롯한 기존 로컬 ONTAP ID 정의를 사용할 수 있습니다.

로컬 **ONTAP** 처리 옵션

ONTAP ID 정의를 사용하는 경우 다음을 포함하여 적용할 항목을 결정해야 합니다.

- 이름이 지정된 REST 역할입니다
- 로컬 사용자와 일치합니다
- Active Directory 또는 LDAP 그룹

로컬 검증 또는 원격 검사

액세스 토큰의 유효성을 ONTAP에서 로컬로 검사할지, 아니면 자체 검사를 통해 인증 서버에서 검사할지 결정해야 합니다. 또한 새로 고침 간격과 같이 고려해야 할 여러 관련 값도 있습니다.

보낸 사람 제한 액세스 토큰

높은 수준의 보안이 필요한 환경에서는 MTL을 기반으로 보내기 제한 액세스 토큰을 사용할 수 있습니다. 이렇게 하려면 각 클라이언트에 대한 인증서가 필요합니다.

UUID 및 **ID** 매핑으로 그룹화합니다

UUID를 사용하여 그룹을 나타내는 인증 서버를 사용하는 경우 그룹 이름 및 연결된 역할에 매핑하는 방법을 계획해야 합니다.

관리 인터페이스

다음을 비롯한 모든 ONTAP 인터페이스를 통해 OAuth 2.0을 관리할 수 있습니다.

- 명령줄 인터페이스입니다
- 시스템 관리자

- REST API

클라이언트가 액세스 토큰을 요청하는 방법

클라이언트 응용 프로그램은 권한 부여 서버에서 직접 액세스 토큰을 요청해야 합니다. 허가 유형을 포함하여 이 작업을 수행하는 방법을 결정해야 합니다.

ONTAP를 구성합니다

몇 가지 ONTAP 구성 작업을 수행해야 합니다.

REST 역할 및 로컬 사용자를 정의합니다

인증 구성에 따라 로컬 ONTAP 식별 처리를 사용할 수 있습니다. 이 경우 REST 역할 및 사용자 정의를 검토하고 정의해야 합니다. 또한 인증 서버에 따라 UUID 값을 기반으로 하는 관리 그룹이 포함될 수도 있습니다.

코어 구성

핵심 ONTAP 구성을 수행하는 데 필요한 주요 단계는 다음과 같습니다.

- 선택적으로 인증 서버의 인증서를 서명한 CA에 대한 루트 인증서(및 모든 중간 인증서)를 설치합니다.
- 인증 서버를 정의합니다.
- 클러스터에 대해 OAuth 2.0 처리를 활성화합니다.

ONTAP에 OAuth 2.0 배포

핵심 OAuth 2.0 기능을 배포하려면 세 가지 기본 단계가 필요합니다.

시작하기 전에

ONTAP를 구성하기 전에 OAuth 2.0 배포를 준비해야 합니다. 예를 들어 인증서의 서명 방법 및 방화벽 뒤에 있는지 등 인증 서버를 평가해야 합니다. 을 참조하십시오 "ONTAP와 함께 OAuth 2.0을 배포할 준비를 하십시오" 를 참조하십시오.

1단계: 인증 서버 루트 CA 인증서를 설치합니다

ONTAP에는 미리 설치된 루트 CA 인증서가 다수 포함되어 있습니다. 따라서 대부분의 경우 추가 구성 없이 ONTAP에서 인증 서버의 인증서를 즉시 인식합니다. 그러나 인증 서버 인증서 서명 방법에 따라 루트 CA 인증서와 중간 인증서를 설치해야 할 수도 있습니다.

필요한 경우 아래 제공된 지침에 따라 인증서를 설치합니다. 필요한 모든 인증서를 클러스터 수준에서 설치해야 합니다.

ONTAP 액세스 방법에 따라 올바른 절차를 선택합니다.

예 **26.** 단계

시스템 관리자

1. System Manager에서 * 클러스터 * > * 설정 * 을 선택합니다.
2. 아래로 스크롤하여 * 보안 * 섹션으로 이동합니다.
3. Certificates * 옆에 있는 * → * 를 클릭합니다.
4. 신뢰할 수 있는 인증 기관 * 탭에서 * 추가 * 를 클릭합니다.
5. 가져오기 * 를 클릭하고 인증서 파일을 선택합니다.
6. 사용자 환경에 대한 구성 매개 변수를 입력합니다.
7. 추가 * 를 클릭합니다.

CLI를 참조하십시오

1. 설치를 시작합니다.

   보안 인증서설치형 server-ca

2. 다음 콘솔 메시지를 찾습니다.

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. 텍스트 편집기로 인증서 파일을 엽니다.
4. 다음 행을 포함하여 전체 인증서를 복사합니다.

   ```
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

5. 명령 프롬프트 후 터미널에 인증서를 붙여 넣습니다.
6. Enter * 키를 눌러 설치를 완료합니다.
7. 다음 중 하나를 사용하여 인증서가 설치되었는지 확인합니다.

   ```
   security certificate show-user-installed
   ```

   ```
   security certificate show
   ```

2단계**:** 인증 서버를 구성합니다

ONTAP에 하나 이상의 인증 서버를 정의해야 합니다. 구성 및 배포 계획에 따라 매개 변수 값을 선택해야 합니다. 검토 "OAuth2 배포 시나리오" 구성에 필요한 정확한 매개 변수를 결정합니다.

권한 부여 서버 정의를 수정하려면 기존 정의를 삭제하고 새 정의를 만듭니다.

아래에 제공된 예는 의 첫 번째 간단한 배포 시나리오를 기반으로 합니다 "로컬 검증". 독립 실행형 범위는 프록시 없이

사용됩니다.

ONTAP 액세스 방법에 따라 올바른 절차를 선택합니다. CLI 절차에서는 명령을 실행하기 전에 교체해야 하는 기호 변수를 사용합니다.

예 **27.** 단계

시스템 관리자

1. System Manager에서 * 클러스터 * > * 설정 * 을 선택합니다.
2. 아래로 스크롤하여 * 보안 * 섹션으로 이동합니다.
3. OAuth 2.0 권한 부여 * 옆에 있는 * + * 를 클릭합니다.
4. 추가 옵션 * 을 선택합니다.
5. 다음과 같이 배포에 필요한 값을 제공합니다.
   - 이름
   - 응용 프로그램(http)
   - 공급자 JWKS URI입니다
   - 발급자 URI입니다
6. 추가 * 를 클릭합니다.

CLI를 참조하십시오

1. 정의를 다시 만듭니다.

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

예를 들면 다음과 같습니다.

```
security oauth2 client create \
-config-name auth0 \
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
realm/protocol/openid-connect/certs \
-application http \
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

에 대한 자세한 내용은 `security oauth2 client create` "ONTAP 명령 참조입니다"을 참조하십시오.

3단계**: OAuth 2.0**을 활성화합니다

마지막 단계는 OAuth 2.0을 활성화하는 것입니다. ONTAP 클러스터에 대한 전역 설정입니다.

ONTAP, 인증 서버 및 지원 서비스가 모두 올바르게 구성되었는지 확인하기 전까지는 OAuth 2.0 처리를 활성화하지 마십시오.

ONTAP 액세스 방법에 따라 올바른 절차를 선택합니다.

예 **28.** 단계

시스템 관리자

1. System Manager에서 * 클러스터 * > * 설정 * 을 선택합니다.
2. 아래로 스크롤하여 * 보안 섹션 * 을 찾습니다.
3. OAuth 2.0 권한 부여 * 옆에 있는 * → * 를 클릭합니다.
4. OAuth 2.0 권한 부여 * 를 활성화합니다.

CLI를 참조하십시오

1. OAuth 2.0 활성화:

```
security oauth2 modify -enabled true
```

2. OAuth 2.0이 활성화되어 있는지 확인합니다.

```
security oauth2 show
Is OAuth 2.0 Enabled: true
```

관련 정보

- "보안 인증서 설치"
- "보안 인증서가 표시됩니다"
- "보안 oauth2 수정"
- "보안 oauth2 표시"

OAuth 2.0을 사용하여 **ONTAP REST API** 호출을 발행합니다**.**

ONTAP의 OAuth 2.0 구현은 REST API 클라이언트 애플리케이션을 지원합니다. curl을 사용하여 간단한 REST API 호출을 실행하여 OAuth 2.0을 사용할 수 있습니다. 아래 예에서는 ONTAP 클러스터 버전을 검색합니다.

시작하기 전에

ONTAP 클러스터에 대해 OAuth 2.0 기능을 구성하고 사용하도록 설정해야 합니다. 여기에는 인증 서버 정의가 포함됩니다.

1단계**:** 액세스 토큰을 획득합니다

REST API 호출에 사용할 액세스 토큰을 얻어야 합니다. 토큰 요청은 ONTAP 외부에서 수행되며 정확한 절차는 인증 서버 및 해당 구성에 따라 다릅니다. 웹 브라우저, curl 명령 또는 프로그래밍 언어를 사용하여 토큰을 요청할 수

있습니다.

설명 목적으로 curl을 사용하여 Keycloak에서 액세스 토큰을 요청하는 방법에 대한 예가 아래에 나와 있습니다.

Keycloak 예

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

반환된 토큰을 복사하여 저장해야 합니다.

2단계**: REST API** 호출을 실행합니다

유효한 액세스 토큰이 있으면 액세스 토큰과 함께 curl 명령을 사용하여 REST API 호출을 실행할 수 있습니다.

매개 변수 및 변수

컬링 예제의 두 변수는 아래 표에 설명되어 있습니다.

변수	설명
$FQDN_IP입니다	ONTAP 관리 LIF의 정규화된 도메인 이름 또는 IP 주소
$access_token입니다	인증 서버에서 발급한 OAuth 2.0 액세스 토큰

curl 예제를 실행하기 전에 먼저 Bash 셸 환경에서 이러한 변수를 설정해야 합니다. 예를 들어, Linux CLI에서 다음 명령을 입력하여 FQDN 변수를 설정하고 표시합니다.

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

두 변수가 모두 로컬 Bash 셸에 정의되면 curl 명령을 복사하여 CLI에 붙여 넣을 수 있습니다. Enter * 키를 눌러 변수를 대체하고 명령을 실행합니다.

컬의 예

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

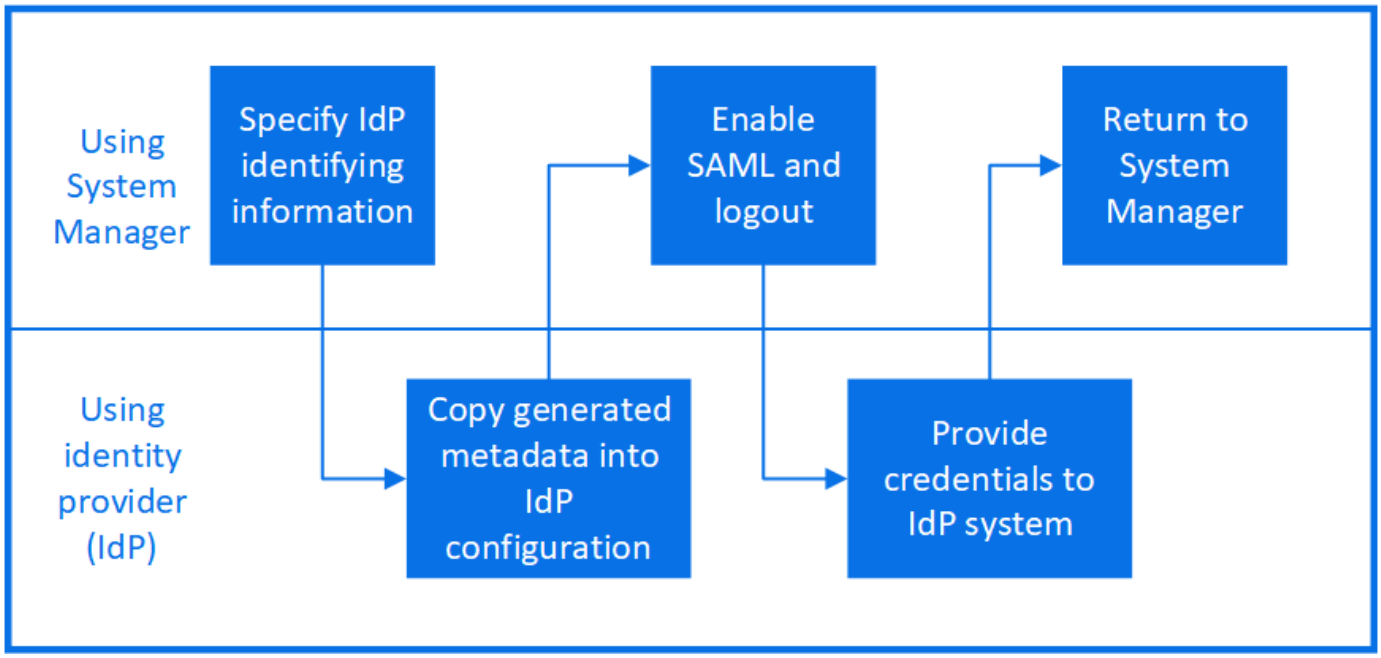
원격 ONTAP 사용자에 대한 SAML 인증 구성

ONTAP 9.3부터 웹 서비스에 대한 SAML(Security Assertion Markup Language) 인증을 구성할 수 있습니다. SAML 인증을 구성하고 활성화하면 사용자는 Active Directory 및 LDAP와 같은 디렉터리 서비스 공급자 대신 외부 ID 공급자(IdP)를 통해 인증됩니다. SAML 인증을 비활성화하면 Active Directory 및 LDAP와 같이 구성된 디렉터리 서비스 공급자가 인증에 사용됩니다.

SAML 인증을 활성화합니다

System Manager 또는 CLI를 사용하여 SAML 인증을 활성화하려면 다음 단계를 수행하십시오. 클러스터에서 ONTAP 9.7 이하를 실행 중인 경우에는 System Manager에서 따라야 하는 단계가 다릅니다. 시스템에서 사용할 수 있는 System Manager 온라인 도움말을 참조하십시오.

SAML 인증을 활성화하면 SAML 인증이 구성된 원격 사용자만 System Manager GUI에 액세스할 수 있습니다. SAML 인증이 활성화된 후에는 로컬 사용자가 System Manager GUI에 액세스할 수 없습니다.



이 작업에 대해

- SAML 인증은 ONTAP 에만 적용됩니다. `http` 그리고 `ontapi` 응용 프로그램.

  그만큼 `http` 그리고 `ontapi` 애플리케이션은 다음 웹 서비스에서 사용됩니다: 서비스 프로세서 인프라, ONTAP API, 시스템 관리자.

- SAML 인증은 관리 SVM에 액세스하는 경우에만 적용됩니다.
- ONTAP 9.17.1부터 IdP에서 제공하는 그룹 정보를 ONTAP 역할에 매핑할 수 있습니다. 이를 통해 IdP에 정의된 그룹을 기반으로 사용자에게 역할을 할당할 수 있습니다. 자세한 내용은 다음을 참조하세요. "ONTAP 에서 OAuth 2.0 또는 SAML IdP 그룹 작업" .

다음 IdP는 System Manager에서 검증되었습니다.

- Microsoft Entra ID(ONTAP 9.17.1 이상에서 검증됨)
- Active Directory 페더레이션 서비스
- Cisco Duo(다음 ONTAP 버전으로 검증됨)
  - 9.7P21 이상 9.7 릴리스(참조 "System Manager Classic 설명서")
  - 9.8P17 및 이후 9.8 패치 릴리스
  - 9.9.1P13 및 이후 9.9.1 패치 릴리스
  - 9.10.1P9 및 이후 9.10.1 패치 릴리스
  - 9.11.1P4 및 이후 9.11.1 패치 릴리스
  - 9.12.1 이상 릴리즈
- 시바볼레스

시작하기 전에

- 원격 인증에 사용할 IdP는 다음과 같아야 합니다구성됨. IdP의 URI가 있어야 합니다. URI는 ONTAP 인증 요청을 보내고 응답을 받는 웹 주소입니다.
- ONTAP 클러스터와 IdP 사이에서 포트 443이 열려 있어야 합니다.
- ONTAP 클러스터와 IdP는 각각 상대방의 정규화된 도메인 이름에 ping을 보낼 수 있어야 합니다. DNS가 올바르게 구성되었고 클러스터 인증서가 만료되지 않았는지 확인하십시오.
- 필요한 경우 IdP의 신뢰할 수 있는 인증 기관(CA)을 ONTAP 에 추가하세요 당신은 할 수 있어요 "System Manager를 사용하여 ONTAP 인증서 관리". IdP에서 ONTAP 클러스터 인증서를 구성해야 할 수도 있습니다
- ONTAP 클러스터에 액세스할 수 있어야 합니다. "서비스 프로세서(SP)" 콘솔. SAML이 잘못 구성된 경우 SP 콘솔에서 비활성화해야 합니다.
- Entra ID(ONTAP 9.17.1부터 검증됨)를 사용하는 경우, ONTAP SAML 구성을 생성하기 전에 ONTAP 메타데이터로 Entra ID를 구성해야 합니다. Entra ID는 ONTAP 메타데이터로 구성될 때까지 IdP URI를 제공하지 않습니다. IdP URI는 ONTAP SAML 구성을 생성하는 데 필수적입니다.
  - System Manager를 사용하여 SAML을 구성하는 경우, System Manager에서 ONTAP 메타데이터를 제공할 때까지 IdP URI 필드를 비워 두십시오. ONTAP 메타 ONTAP 로 Entra ID를 구성한 후, SAML 구성을 활성화하기 전에 IdP URI를 System Manager에 복사하십시오.
  - ONTAP CLI를 사용하여 SAML을 구성하는 경우, ONTAP SAML 구성을 활성화하기 전에 ONTAP 메타데이터를 생성해야 합니다. 다음 명령을 사용하여 ONTAP 메타데이터 파일을 생성할 수 있습니다.

    ```
    security saml-sp default-metadata create -sp-host <ontap_host_name>
    ```

    `ontap_host_name` SAML 서비스 공급자 호스트의 호스트 이름 또는 IP 주소이며, 이 경우 ONTAP 시스템입니다. 기본적으로 클러스터 관리 IP 주소가 사용됩니다. 선택적으로 ONTAP 서버 인증서 정보를 제공할 수 있습니다. 기본적으로 ONTAP 웹 서버 인증서 정보가 사용됩니다.

  제공된 메타데이터를 사용하여 Entra ID를 구성하세요. ONTAP SAML 구성을 생성하기 전에 Entra ID를 구성해야 합니다. Entra가 구성된 후 아래 CLI 절차를 진행하세요.

  - 클러스터의 모든 노드가 버전 9.17.1이 될 때까지 Entra ID에 대한 ONTAP 메타데이터를 생성할 수 없습니다.

단계

환경에 따라 다음 단계를 수행하십시오.

시스템 관리자

1. 클러스터 > 설정 * 을 클릭합니다.
2. SAML 인증 * 옆에 있는 을 클릭합니다.
3. SAML 인증 활성화 * 확인란이 선택되어 있는지 확인합니다.
4. IdP URI의 URL을 입력하세요(다음 포함) "https://"). Entra ID를 사용하는 경우 이 단계를 건너뛰세요.
5. 필요한 경우 호스트 시스템 주소를 수정하세요. 이 주소는 인증 후 IdP가 연결할 주소입니다. 기본값은 클러스터 관리 IP 주소입니다.
6. 올바른 인증서가 사용되고 있는지 확인합니다.
   - 시스템이 "서버" 유형의 인증서를 하나만 사용하여 매핑된 경우 해당 인증서는 기본값으로 간주되어 표시되지 않습니다.
   - 시스템이 여러 인증서를 "서버" 유형으로 매핑한 경우 인증서 중 하나가 표시됩니다. 다른 인증서를 선택하려면 * 변경 * 을 클릭합니다.
7. 저장 * 을 클릭합니다. 확인 창에 메타데이터 정보가 표시되며, 이 정보는 클립보드에 자동으로 복사됩니다.
8. 지정한 IdP 시스템으로 이동하여 클립보드에서 메타데이터를 복사하여 시스템 메타데이터를 업데이트하세요. Entra ID를 사용하는 경우, 시스템 메타데이터로 Entra ID를 구성한 후 IdP URI를 ONTAP 에 복사하세요.
9. System Manager의 확인 창으로 돌아가서 * 호스트 URI 또는 메타데이터 * 를 사용하여 IDP를 구성했는지 * 확인란을 선택합니다.
10. SAML 기반 인증을 활성화하려면 * 로그아웃 * 을 클릭합니다. IDP 시스템에 인증 화면이 표시됩니다.
11. IdP 로그인 페이지에서 SAML 기반 자격 증명을 입력하세요. 자격 증명이 확인되면 시스템 관리자 홈페이지로 이동합니다.

CLI를 참조하십시오

1. SAML 구성을 생성하여 ONTAP가 IDP 메타데이터에 액세스할 수 있도록 합니다.

   ```
   security saml-sp create -idp-uri <idp_uri> -sp-host <ontap_host_name>
   ```

   IDP_Uri는 IDP 메타데이터를 다운로드할 수 있는 IDP 호스트의 FTP 또는 HTTP 주소입니다.

   > 일부 URL에는 물음표(?) 문자가 포함되어 있습니다. 물음표는 ONTAP 명령줄의 활성 도움말을 활성화합니다. 물음표가 있는 URL을 입력하려면 먼저 다음 명령을 사용하여 활성 도움말을 비활성화해야 합니다. `set -active-help false` . 활성 도움말은 나중에 다음 명령을 사용하여 다시 활성화할 수 있습니다. `set -active-help true` . 자세한 내용은 "ONTAP 명령 참조입니다" .

   'ontap_host_name'은 SAML 서비스 공급자 호스트의 호스트 이름 또는 IP 주소이며, 이 경우 ONTAP 시스템입니다. 기본적으로 클러스터 관리 LIF의 IP 주소가 사용됩니다.

   ONTAP 서버 인증서 정보를 선택적으로 제공할 수 있습니다. 기본적으로 ONTAP 웹 서버 인증서 정보가 사용됩니다.

```
cluster_12::> security saml-sp create -idp-uri
https://example.url.net/idp/shibboleth

Warning: This restarts the web server. Any HTTP/S connections that
are active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and ONTAP users for the same directory server
domain to ensure that users are the same for different
authentication methods. See the "security login show" command for
the ONTAP user configuration.
```

ONTAP 호스트 메타데이터에 액세스할 수 있는 URL이 표시됩니다.

2. IdP 호스트에서 IdP 구성 ONTAP 호스트 메타데이터를 사용합니다. Entra ID를 사용하는 경우 이 단계는 이미 완료되었습니다.
3. IdP가 구성되면 SAML 구성을 활성화합니다.

   ```
   security saml-sp modify -is-enabled true
   ```

   'http' 또는 'ontapi' 애플리케이션에 액세스하는 기존 사용자는 자동으로 SAML 인증을 위해 구성됩니다.

4. 사용자를 생성하려면 `http` 또는 `ontapi` SAML이 구성된 후 애플리케이션에서 새 사용자에 대한 인증 방법으로 SAML을 지정하십시오. ONTAP 9.17.1 이전에는 기존 사용자에 대해 SAML 로그인이 자동으로 생성됩니다. `http` 또는 `ontapi` SAML이 활성화된 경우 사용자. 새 사용자는 SAML에 맞게 구성해야 합니다. ONTAP 9.17.1부터 SAML을 사용하여 생성된 모든 사용자는 `password` , `domain` , 또는 `nsswitch` SAML이 활성화되면 인증 방법은 IdP에 대해 자동으로 인증됩니다.

   a. 인증을 사용하여 새 사용자를 위한 로그인 방법을 만듭니다. `user_name` IdP에 구성된 사용자 이름과 일치해야 합니다.

      > `user_name` 값은 대소문자를 구분합니다. Entra ID를 사용하지 않는 경우 사용자 이름만 포함하고 도메인 부분은 포함하지 마십시오. Entra ID를 사용하는 경우 _user_name@domain.com_과 같이 도메인을 포함하여 사용자 이름을 생성할 수 있습니다.

      ```
      security login create -user-or-group-name <user_name> -application [http
      | ontapi] -authentication-method saml -vserver <svm_name>
      ```

      예:

      ```
      cluster_12::> security login create -user-or-group-name admin1
      -application http -authentication-method saml -vserver cluster_12
      ```

b. 사용자 항목이 생성되었는지 확인합니다.

'보안 로그인 쇼'

예:

```
cluster_12::> security login show

Vserver: cluster_12

Second
User/Group                  Authentication                 Acct
Authentication
Name            Application Method        Role Name        Locked
Method
--------------- ----------- ------------- ---------------- ------
--------------
admin           console     password      admin            no
none
admin           http        password      admin            no
none
admin           http        saml          admin            -
none
admin           ontapi      password      admin            no
none
admin           ontapi      saml          admin            -
none
admin           service-processor
                            password      admin            no
none
admin           ssh         password      admin            no
none
admin1          http        password      backup           no
none
admin1          http        saml          backup           -
none
```

+
에 대한 자세한 내용은 `security login show` "ONTAP 명령 참조입니다"을 참조하십시오.

SAML 인증을 비활성화합니다

외부 ID 공급자(IdP)를 통한 원격 System Manager 사용자 인증을 중지하려면 SAML 인증을 비활성화할 수 있습니다. SAML 인증을 비활성화하면 로컬 사용자 인증 또는 Active Directory 및 LDAP와 같은 구성된 디렉터리 서비스 공급자가 사용자를 인증하는 데 사용됩니다.

환경에 따라 다음 단계를 수행하십시오.

예 **29.** 단계

시스템 관리자

1. 클러스터 > 설정 * 을 클릭합니다.
2. SAML Authentication * 에서 * Enabled * 토글 버튼을 클릭합니다.
3. 선택 사항: * SAML 인증 * 옆에 있는 을 클릭한 다음 * SAML 인증 사용 * 확인란의 선택을 취소할 수도 있습니다.

CLI를 참조하십시오

1. SAML 인증 비활성화:

```
security saml-sp modify -is-enabled false
```

2. SAML 인증을 더 이상 사용하지 않거나 IDP를 수정하려는 경우 SAML 구성을 삭제합니다.

```
security saml-sp delete
```

타사 **IdP** 구성

이 작업에 대해

ONTAP 으로 인증하려면 IdP 설정을 변경해야 할 수 있습니다. 다음 섹션에서는 지원되는 IdP에 대한 구성 정보를 제공합니다.

내부 **ID**

Entra ID를 구성할 때 새 애플리케이션을 생성하고 ONTAP 에서 제공하는 메타데이터를 사용하여 SAML 로그인을 구성하세요. 애플리케이션 생성 후 애플리케이션 SAML 설정의 "속성 및 클레임" 섹션을 다음과 같이 편집하세요.

설정	값
이름	항아리:oid:0.9.2342.19200300.100.1.1
네임스페이스	비워두세요
이름 형식	URI
출처	기인하다
소스 속성	사용자.사용자 주체 이름

Entra ID로 그룹을 사용하려면 다음 설정으로 그룹 클레임을 추가하세요.

설정	값
이름	항아리:oid:1.3.6.1.4.1.5923.1.5.1.1
네임스페이스	비워두세요
소스 속성	그룹 ID입니다

Entra ID는 UUID 형식으로 그룹 정보를 제공합니다. Entra ID를 사용하여 그룹을 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요. "UUID를 사용하여 그룹을 관리합니다" .

애플리케이션 SAML 설정의 "SAML 인증서" 섹션에 제공된 _앱 페더레이션 메타데이터 URL_은 ONTAP 에 입력할 IdP URI입니다.

Entra ID 다중 인증 구성에 대한 정보는 다음을 참조하세요. "Microsoft Entra 다중 인증 배포 계획" .

자세한 내용은 다음을 참조하세요. "Entra ID 문서" .

Active Directory 페더레이션 서비스

AD FS(Active Directory Federation Services)를 구성할 때는 ONTAP 에서 제공하는 서비스 공급자 메타데이터를 사용하여 새로운 클레임 인식 신뢰 당사자 트러스트를 추가해야 합니다. 신뢰 당사자 트러스트가 생성되면 "LDAP 특성을 클레임으로 보내기" 템플릿을 사용하여 신뢰 당사자 트러스트의 클레임 발급 정책에 다음 클레임 규칙을 추가합니다.

속성 저장소	**LDAP** 속성	발신 청구 유형
Active Directory를 클릭합니다	SAM 계정 이름	이름 ID
Active Directory를 클릭합니다	SAM 계정 이름	항아리:oid:0.9.2342.19200300.100.1.1
Active Directory를 클릭합니다	이름 형식	urn:oasis:names:tc:SAML:2.0:attrname-format:uri
Active Directory를 클릭합니다	토큰 그룹 - 도메인 이름으로 적격화됨	항아리:oid:1.3.6.1.4.1.5923.1.5.1.1

속성 저장소	**LDAP** 속성	발신 청구 유형
Active Directory를 클릭합니다	sAMAccountName	항아리:oid:1.2.840.113556.1.4.221

AD FS는 이름 형식으로 그룹 정보를 제공합니다. AD FS에서 그룹을 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요. "이름으로 그룹을 관리합니다" .

자세한 내용은 다음을 참조하세요. "AD FS 설명서" .

Cisco 듀오

를 참조하세요 "Cisco Duo 설명서" 구성 정보.

시바볼레스

Shibboleth IdP를 구성하기 전에 LDAP 서버를 구성해야 합니다.

ONTAP 에서 SAML을 활성화할 때 제공된 호스트 메타데이터 XML을 저장하세요. Shibboleth가 설치된 호스트에서 다음 내용을 `metadata/sp-metadata.xml` Shibboleth IdP 홈 디렉토리 내의 호스트 메타데이터 XML을 사용합니다.

자세한 내용은 다음을 참조하세요. "시바볼레스" .

SAML 구성 관련 문제를 해결합니다

SAML(Security Assertion Markup Language) 인증을 구성하지 못한 경우 SAML 구성이 실패한 각 노드를 수동으로 복구하고 장애를 복구할 수 있습니다. 복구 프로세스 중에 웹 서버가 다시 시작되고 활성 HTTP 연결 또는 HTTPS 연결이 중단됩니다.

이 작업에 대해

SAML 인증을 구성할 경우 ONTAP는 노드별로 SAML 구성을 적용합니다. SAML 인증을 설정하면 구성 문제가 있는 경우 ONTAP에서 자동으로 각 노드를 복구하려고 시도합니다. 노드에서 SAML 구성에 문제가 있는 경우 SAML 인증을 비활성화한 다음 SAML 인증을 다시 활성화할 수 있습니다. SAML 인증을 다시 설정한 후에도 하나 이상의 노드에 SAML 구성이 적용되지 않는 경우가 있을 수 있습니다. SAML 구성이 실패한 노드를 확인한 다음 해당 노드를 수동으로 복구할 수 있습니다.

단계

1. 고급 권한 레벨에 로그인합니다.

   세트 프리빌리지 고급

2. SAML 구성이 실패한 노드 식별:

   ```
   security saml-sp status show -instance
   ```

   예:

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                Update Status: config-failed
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

에 대한 자세한 내용은 `security saml-sp status show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 장애가 발생한 노드에서 SAML 구성을 복구합니다.

   `security saml-sp repair -node <node_name>`

   예:

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

   웹 서버가 다시 시작되고 활성화된 HTTP 연결 또는 HTTPS 연결이 모두 중단됩니다.

   에 대한 자세한 내용은 `security saml-sp repair` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 모든 노드에서 SAML이 구성되었는지 확인합니다.

   `security saml-sp status show -instance`

   예:

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                 Update Status: config-success
                Database Epoch: 9
    Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
         ID of SAML Config Job: 179

                          Node: node2
                 Update Status: config-success
                Database Epoch: 9
    Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
         ID of SAML Config Job: 180
2 entries were displayed.
```

에 대한 자세한 내용은 `security saml-sp status show` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "ONTAP 명령 참조입니다"
- "보안 SAML - SP"
- "보안 로그인 생성"

ONTAP 에서 OAuth 2.0 또는 SAML IdP 그룹 작업

ONTAP OAuth 2.0 권한 부여 서버 또는 SAML ID 공급자(IdP)를 기반으로 그룹을 구성하는 여러 옵션을 제공합니다. 이렇게 구성된 그룹은 ONTAP 에서 액세스 권한을 결정하는 데 사용되는 역할에 매핑될 수 있습니다.

ONTAP 9.17.1부터 SAML IdP에서 제공하는 그룹 정보를 ONTAP 역할에 매핑할 수 있습니다. 이를 통해 IdP에 정의된 그룹을 기반으로 사용자에게 역할을 할당할 수 있습니다. 자세한 내용은 "SAML 인증을 구성합니다". ONTAP 9.14.1부터 ONTAP OAuth 2.0에 대한 그룹 이름 인증을 지원합니다. ONTAP 9.16.1부터 ONTAP OAuth 2.0 그룹 UUID 인증 및 역할 매핑을 지원합니다. "ONTAP OAuth 2.0 구축 개요" .

그룹을 식별하는 방법

권한 부여 서버 또는 SAML IdP에서 그룹을 구성하면 해당 그룹은 이름이나 UUID를 사용하여 OAuth 2.0 액세스 토큰 또는 SAML 어설션을 통해 식별되고 전달됩니다. ONTAP 구성하기 전에 권한 부여 서버 또는 SAML IdP가 그룹을 처리하는 방식을 알고 있어야 합니다.

액세스 토큰에 여러 그룹이 포함된 경우 ONTAP는 일치하는 항목이 있을 때까지 각 그룹을 사용하려고 시도합니다.

그룹 이름

많은 권한 부여 서버와 SAML IdP(Active Directory Federation Service(ADFS) 등)는 이름을 사용하여 그룹을 식별하고 나타냅니다. 은 ADFS에서 생성된 여러 그룹을 포함하는 JSON OAuth 2.0 액세스 토큰의 일부입니다. 이름으로 그룹을 관리합니다 자세한 내용은.

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

UUID를 그룹화합니다

일부 권한 부여 서버와 Microsoft Entra ID와 같은 SAML IdP는 UUID를 사용하여 그룹을 식별하고 나타냅니다. 다음은 Entra ID에서 생성된 여러 그룹을 포함하는 OAuth 2.0 액세스 토큰의 일부입니다. UUID를 사용하여 그룹을 관리합니다 자세한 내용은.

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

이름으로 그룹을 관리합니다

권한 부여 서버 또는 SAML IdP가 그룹을 식별하기 위해 이름을 사용하는 경우, ONTAP 클러스터에 각 그룹이 정의되어 있는지 확인해야 합니다. 보안 환경에 따라 그룹이 이미 정의되어 있을 수도 있습니다.

다음은 ONTAP 그룹을 정의하는 CLI 명령의 예입니다. 샘플 액세스 토큰의 명명된 그룹을 사용합니다. 명령을 실행하려면 ONTAP **admin** 권한 수준이 필요합니다.

예

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

사용 `-authentication-method domain` 또는 `nsswitch` SAML IdP 및 OAuth 2.0 권한 부여 서버 그룹의 경우.

ONTAP REST API를 사용하여 이 기능을 구성할 수도 있습니다. 자세한 내용은 "ONTAP 자동화 설명서" .

UUID를 사용하여 그룹을 관리합니다

권한 부여 서버 또는 SAML IdP가 UUID 값을 사용하여 그룹을 나타내는 경우, 그룹을 사용하기 전에 두 단계 구성을 수행해야 합니다. ONTAP 9.16.1부터 두 가지 매핑 기능을 사용할 수 있으며 Entra ID를 통해 테스트되었습니다. OAuth 2.0용 Entra ID는 ONTAP 9.16.1부터 지원되고, SAML용 Entra ID는 ONTAP 9.17.1부터 지원됩니다. CLI 명령을 실행하려면 ONTAP **admin** 권한 수준이 필요합니다.

ONTAP REST API를 사용하여 이러한 기능을 구성할 수도 있습니다. 자세한 내용은 을 "ONTAP 자동화 설명서"참조하십시오.

그룹 UUID를 그룹 이름에 매핑합니다

UUID 값을 사용하여 그룹을 나타내는 권한 부여 서버 또는 SAML IdP를 사용하는 경우, 그룹 UUID를 그룹 이름에 매핑해야 합니다. 주요 ONTAP CLI 작업은 다음과 같습니다.

생성

다음을 사용하여 새 그룹 매핑 구성을 정의할 수 있습니다. `security login group create` 명령. 그룹 UUID와 이름은 권한 부여 서버 또는 SAML IdP의 구성과 일치해야 합니다. 자세히 알아보기 `security login group create` 에서 "ONTAP 명령 참조입니다" .

매개 변수

그룹 매핑을 생성하는 데 사용되는 매개 변수는 아래에 설명되어 있습니다.

매개 변수	설명
`vserver`	선택적으로 그룹이 연결된 SVM(SVM)의 이름을 지정합니다. 생략하면 그룹이 ONTAP 클러스터와 연결됩니다.
`name`	ONTAP에서 사용할 그룹의 고유 이름입니다.
`type`	이 값은 그룹의 출처가 되는 ID 공급자를 나타냅니다.
`uuid`	권한 부여 서버나 SAML IdP에서 제공하는 그룹의 범용 고유 식별자를 지정합니다.

다음은 ONTAP 그룹을 정의하는 CLI 명령의 예입니다. 샘플 액세스 토큰의 UUID 그룹을 사용합니다.

예

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

그룹을 생성한 후 그룹에 대해 고유한 읽기 전용 정수 식별자가 생성됩니다.

추가 **CLI** 작업

이 명령을 실행하면 다음과 같은 몇 가지 추가 작업이 지원됩니다.

- 표시
- 수정
- 삭제

옵션을 사용하여 그룹에 대해 생성된 고유한 그룹 ID를 검색할 수 `show` 있습니다. 에 대한 자세한 내용은 `show` "ONTAP 명령 참조입니다"을 참조하십시오.

그룹 **UUID**를 역할에 매핑합니다

UUID 값을 사용하여 그룹을 나타내는 권한 부여 서버 또는 SAML IdP를 사용하는 경우, 그룹을 역할에 매핑할 수 있습니다. ONTAP 의 역할 기반 액세스 제어에 대한 자세한 내용은 다음을 참조하십시오. "ONTAP 액세스 제어 역할 관리에 대해 알아봅니다" . 주요 ONTAP CLI 작업은 아래와 같습니다. 명령을 실행하려면 ONTAP **admin** 권한 수준이 필요합니다.

먼저 해야 할 일은 그룹 UUID를 그룹 이름에 매핑 그룹에 대해 생성된 고유 정수 ID를 검색합니다. 그룹을 역할에 매핑하려면 이 ID가 필요합니다.

생성

다음을 사용하여 새 역할 매핑을 정의할 수 있습니다. `security login group role-mapping create` 명령. 자세히 알아보기 `security login group role-mapping create` 에서 "ONTAP 명령 참조입니다" .

매개 변수

그룹을 역할에 매핑하는 데 사용되는 매개 변수는 아래에 설명되어 있습니다.

매개 변수	설명
`group-id`	명령을 사용하여 그룹에 대해 생성된 고유 ID를 `security login group create` 지정합니다.
`role`	그룹이 매핑되는 ONTAP 역할의 이름입니다.

예

```
security login group role-mapping create -group-id 1 -role admin
```

추가 **CLI** 작업

이 명령을 실행하면 다음과 같은 몇 가지 추가 작업이 지원됩니다.

- 표시
- 수정
- 삭제

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

관련 정보

- "외부 역할 매핑"

WebAuthn MFA를 사용한 인증 및 권한 부여

ONTAP System Manager 사용자를 위한 WebAuthn 다중 요소 인증에 대해 알아보세요.

관리자는 ONTAP 9.16.1부터 System Manager에 로그인하는 사용자에 대해 WebAuthn MFA(다중 요소 인증)를 활성화할 수 있습니다. 이렇게 하면 FIDO2 키(예: YubiKey)를 두 번째 인증 형태로 사용하여 System Manager 로그인을 사용할 수 있습니다. 기본적으로 WebAuthn MFA는 신규 및 기존 ONTAP 사용자에 대해 사용되지 않습니다.

WebAuthn MFA는 첫 번째 인증 방법에 대해 다음 유형의 인증을 사용하는 사용자 및 그룹에 대해 지원됩니다.

- 사용자: 암호, 도메인 또는 nsswitch
- 그룹: domain 또는 nsswitch

WebAuthn MFA를 사용자에 대한 두 번째 인증 방법으로 설정한 후 System Manager에 로그인할 때 사용자에게 하드웨어 인증자를 등록하라는 메시지가 표시됩니다. 등록 후 개인 키는 인증자에 저장되고 공개 키는 ONTAP에 저장됩니다.

ONTAP는 사용자당 하나의 WebAuthn 자격 증명을 지원합니다. 사용자가 인증 프로그램을 분실하여 교체해야 하는 경우 ONTAP 관리자는 다음에 로그인할 때 새 인증 프로그램을 등록할 수 있도록 해당 사용자의 WebAuthn 자격 증명을 삭제해야 합니다.

> ⓘ 두 번째 인증 방법으로 WebAuthn MFA를 사용하도록 설정한 사용자는 "https://myontap.example.com"IP 주소(예:"https://192.168.100.200") 대신 FQDN(예:)을 사용하여 System Manager에 액세스해야 합니다. WebAuthn MFA가 활성화된 사용자의 경우 IP 주소를 사용하여 System Manager 로그인 시도가 거부됩니다.

ONTAP 시스템 관리자 사용자 또는 그룹에 대해 WebAuthn MFA를 활성화합니다

ONTAP 관리자는 WebAuthn MFA 옵션이 활성화된 새 사용자 또는 그룹을 추가하거나 기존 사용자 또는 그룹에 대한 옵션을 활성화하여 시스템 관리자 사용자 또는 그룹에 대해 WebAuthn MFA를 활성화할 수 있습니다.

WebAuthn MFA를 사용자 또는 그룹에 대한 두 번째 인증 방법으로 활성화하면 사용자(또는 해당 그룹의 모든 사용자)는 다음에 System Manager에 로그인할 때 하드웨어 FIDO2 장치를 등록하라는 메시지가 표시됩니다. 이 등록은 사용자의 로컬 운영 체제에 의해 처리되며, 일반적으로 보안 키 삽입, 암호 작성 및 보안 키(지원되는 경우)로 구성됩니다.

새 사용자 또는 그룹을 만들 때 **WebAuthn MFA**를 활성화합니다

System Manager 또는 ONTAP CLI를 사용하여 WebAuthn MFA가 설정된 새 사용자 또는 그룹을 생성할 수 있습니다.

시스템 관리자

1. 클러스터 > 설정 * 을 선택합니다.
2. 사용자 및 역할 * 옆에 있는 화살표 아이콘을 선택합니다.
3. 사용자 * 아래에서 * 추가 * 를 선택합니다.
4. 사용자 또는 그룹 이름을 지정하고 * Role * 의 드롭다운 메뉴에서 역할을 선택합니다.
5. 사용자 또는 그룹의 로그인 방법과 암호를 지정합니다.

   WebAuthn MFA는 사용자를 위한 "password", "domain" 또는 "nsswitch", 그룹에 대한 "domain" 또는 "nsswitch"의 로그인 방법을 지원합니다.
6. HTTP * 용 MFA 열에서 * 사용 * 을 선택합니다.
7. 저장 * 을 선택합니다.

CLI를 참조하십시오

1. WebAuthn MFA를 사용하도록 설정한 새 사용자 또는 그룹을 만듭니다.

   다음 예제에서 WebAuthn MFA는 두 번째 인증 방법으로 "publickey"를 선택하여 사용할 수 있습니다.

```
security login create -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

   에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

기존 사용자 또는 그룹에 대해 **WebAuthn MFA**를 활성화합니다

기존 사용자 또는 그룹에 대해 WebAuthn MFA를 활성화할 수 있습니다.

시스템 관리자

1. 클러스터 > 설정 * 을 선택합니다.
2. 사용자 및 역할 * 옆에 있는 화살표 아이콘을 선택합니다.
3. 사용자 및 그룹 목록에서 편집할 사용자 또는 그룹의 옵션 메뉴를 선택합니다.

   WebAuthn MFA는 사용자를 위한 "password", "domain" 또는 "nsswitch", 그룹에 대한 "domain" 또는 "nsswitch"의 로그인 방법을 지원합니다.
4. 해당 사용자의 * MFA for HTTP * 열에서 * Enabled * 를 선택합니다.
5. 저장 * 을 선택합니다.

CLI를 참조하십시오

1. 기존 사용자 또는 그룹을 수정하여 해당 사용자 또는 그룹에 대해 WebAuthn MFA를 활성화합니다.

   다음 예제에서 WebAuthn MFA는 두 번째 인증 방법으로 "publickey"를 선택하여 사용할 수 있습니다.

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

   에 대한 자세한 내용은 `security login modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 시스템 관리자 사용자를 위한 WebAuthn MFA를 비활성화합니다

ONTAP 관리자는 System Manager 또는 ONTAP CLI를 사용하여 사용자 또는 그룹을 편집하여 사용자 또는 그룹에 대해 WebAuthn MFA를 사용하지 않도록 설정할 수 있습니다.

기존 사용자 또는 그룹에 대해 WebAuthn MFA를 비활성화합니다

언제든지 기존 사용자 또는 그룹에 대해 WebAuthn MFA를 비활성화할 수 있습니다.

등록된 자격 증명을 사용하지 않도록 설정하면 자격 증명이 유지됩니다. 나중에 자격 증명을 다시 활성화하면 동일한 자격 증명이 사용되므로 사용자가 로그인할 때 다시 등록할 필요가 없습니다.

시스템 관리자

1. 클러스터 > 설정 * 을 선택합니다.
2. 사용자 및 역할 * 옆에 있는 화살표 아이콘을 선택합니다.
3. 사용자 및 그룹 목록에서 편집할 사용자 또는 그룹을 선택합니다.
4. 해당 사용자의 * MFA for HTTP * 열에서 * Disabled * 를 선택합니다.
5. 저장 * 을 선택합니다.

CLI를 참조하십시오

1. 기존 사용자 또는 그룹을 수정하여 해당 사용자 또는 그룹에 대해 WebAuthn MFA를 비활성화합니다.

   다음 예에서는 두 번째 인증 방법으로 "none"을 선택하여 WebAuthn MFA를 사용할 수 없습니다.

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method none \
                         -application http \
                         -role admin
   ```

   에 대한 자세한 내용은 `security login modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP WebAuthn MFA 설정을 보고 자격 증명을 관리합니다

ONTAP 관리자는 클러스터 전체의 WebAuthn MFA 설정을 보고 WebAuthn MFA에 대한 사용자 및 그룹 자격 증명을 관리할 수 있습니다.

WebAuthn MFA에 대한 클러스터 설정을 봅니다

ONTAP CLI를 사용하여 WebAuthn MFA에 대한 클러스터 설정을 볼 수 있습니다.

단계

1. WebAuthn MFA에 대한 클러스터 설정을 봅니다. 선택적으로 인수를 사용하여 스토리지 VM을 지정할 수 `vserver` 있습니다.

   ```
   security webauthn show -vserver <storage_vm_name>
   ```

   에 대한 자세한 내용은 `security webauthn show` "ONTAP 명령 참조입니다"을 참조하십시오.

지원되는 공개 키 **WebAuthn MFA** 알고리즘을 봅니다

스토리지 VM 또는 클러스터에 대해 WebAuthn MFA에 대해 지원되는 공개 키 알고리즘을 볼 수 있습니다.

단계

1. 지원되는 공개 키 WebAuthn MFA 알고리즘을 나열합니다. 선택적으로 인수를 사용하여 스토리지 VM을 지정할 수 `vserver` 있습니다.

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

에 대한 자세한 내용은 `security webauthn supported-algorithms show` "ONTAP 명령 참조입니다"을 참조하십시오.

등록된 **WebAuthn MFA** 자격 증명을 봅니다

ONTAP 관리자는 모든 사용자에 대해 등록된 WebAuthn 자격 증명을 볼 수 있습니다. 이 절차를 사용하는 관리자가 아닌 사용자는 자신의 등록된 WebAuthn 자격 증명만 볼 수 있습니다.

단계

1. 등록된 WebAuthn MFA 자격 증명을 봅니다.

```
security webauthn credentials show
```

에 대한 자세한 내용은 `security webauthn credentials show` "ONTAP 명령 참조입니다"을 참조하십시오.

등록된 **WebAuthn MFA** 자격 증명을 제거합니다

등록된 WebAuthn MFA 자격 증명을 제거할 수 있습니다. 이 기능은 사용자의 하드웨어 키를 분실하거나 도난당했거나 더 이상 사용하지 않는 경우에 유용합니다. 사용자가 원래 하드웨어 인증기를 가지고 있지만 새 인증기로 교체하려는 경우 등록된 자격 증명을 제거할 수도 있습니다. 자격 증명을 제거하면 사용자에게 대체 인증자를 등록하라는 메시지가 표시됩니다.

> ⓘ 사용자에 대해 등록된 자격 증명을 제거해도 해당 사용자에 대해 WebAuthn MFA가 해제되지 않습니다. 사용자가 하드웨어 인증 프로그램을 분실하여 교체하기 전에 로그인해야 하는 경우, 다음 단계를 사용하여 자격 증명을 제거해야 "WebAuthn MFA를 비활성화합니다"합니다.

시스템 관리자

1. 클러스터 > 설정 * 을 선택합니다.
2. 사용자 및 역할 * 옆에 있는 화살표 아이콘을 선택합니다.
3. 사용자 및 그룹 목록에서 자격 증명을 제거하려는 사용자 또는 그룹의 옵션 메뉴를 선택합니다.
4. Remove MFA for HTTP credentials * 를 선택합니다.
5. 제거 * 를 선택합니다.

CLI를 참조하십시오

1. 등록된 자격 증명을 삭제합니다. 다음 사항에 유의하십시오.
   - 선택적으로 사용자의 스토리지 VM을 지정할 수 있습니다. 이 인수를 생략하면 클러스터 레벨에서 자격 증명이 제거됩니다.
   - 필요한 경우 자격 증명을 삭제할 사용자의 사용자 이름을 지정할 수 있습니다. 생략하면 현재 사용자에 대한 자격 증명이 제거됩니다.

   ```
   security webauthn credentials delete -vserver <storage_vm_name>
   -username <username>
   ```

   에 대한 자세한 내용은 `security webauthn credentials delete` "ONTAP 명령 참조입니다"을 참조하십시오.

웹 서비스 관리

웹 서비스 관리 개요

클러스터 또는 SVM(Storage Virtual Machine)에 대한 웹 서비스를 설정 또는 해제하고, 웹 서비스 설정을 표시하고, 역할 사용자가 웹 서비스에 액세스할 수 있는지 여부를 제어할 수 있습니다.

다음과 같은 방법으로 클러스터 또는 SVM을 위한 웹 서비스를 관리할 수 있습니다.

- 특정 웹 서비스 활성화 또는 비활성화
- 웹 서비스에 대한 액세스가 암호화된 HTTP(SSL)로만 제한되는지 여부 지정
- 웹 서비스의 사용 가능 여부를 표시합니다
- 역할의 사용자가 웹 서비스에 액세스할 수 있도록 허용 또는 허용하지 않습니다
- 웹 서비스에 액세스할 수 있는 역할을 표시합니다

사용자가 웹 서비스에 액세스하려면 다음 조건을 모두 충족해야 합니다.

- 사용자를 인증해야 합니다.

  예를 들어 웹 서비스에서 사용자 이름과 암호를 묻는 메시지가 표시될 수 있습니다. 사용자의 응답은 유효한 계정과

일치해야 합니다.

- 사용자는 올바른 액세스 방법을 사용하여 설정해야 합니다.

  지정된 웹 서비스에 대해 올바른 액세스 방법을 사용하는 사용자에게만 인증이 성공합니다. ONTAP API 웹 서비스('ontapi')의 경우 사용자에게 "ontapi" 액세스 방법이 있어야 합니다. 다른 모든 웹 서비스의 경우 사용자는 http 액세스 방법을 가지고 있어야 합니다.

  를 사용합니다 `security login` 사용자의 액세스 방법 및 인증 방법을 관리하는 명령입니다.

- 사용자의 액세스 제어 역할을 허용하도록 웹 서비스를 구성해야 합니다.

  'vserver services web access' 명령을 사용하여 웹 서비스에 대한 역할의 액세스를 제어합니다.

방화벽이 설정된 경우 웹 서비스에 사용할 LIF의 방화벽 정책을 HTTP 또는 HTTPS를 허용하도록 설정해야 합니다.

웹 서비스 액세스에 HTTPS를 사용하는 경우, 웹 서비스를 제공하는 클러스터 또는 SVM에 SSL도 사용하도록 설정해야 하며 클러스터 또는 SVM에 대한 디지털 인증서를 제공해야 합니다.

ONTAP 웹 서비스에 대한 액세스 관리

웹 서비스는 사용자가 HTTP 또는 HTTPS를 사용하여 액세스할 수 있는 응용 프로그램입니다. 클러스터 관리자는 웹 프로토콜 엔진을 설정하고, SSL을 구성하고, 웹 서비스를 활성화하고, 역할의 사용자가 웹 서비스에 액세스할 수 있도록 할 수 있습니다.

ONTAP 9.6부터는 다음과 같은 웹 서비스가 지원됩니다.

- 서비스 프로세서 인프라('pi')

  이 서비스에서는 클러스터 관리 LIF 또는 노드 관리 LIF를 통해 노드의 로그, 코어 덤프 및 MIB 파일을 HTTP 또는 HTTPS 액세스에 사용할 수 있습니다. 기본 설정은 "사용"입니다.

  노드의 로그 파일이나 코어 덤프 파일에 액세스하라는 요청이 있을 경우 `spi` 웹 서비스는 파일이 있는 노드에서 다른 노드의 루트 볼륨으로의 마운트 지점을 자동으로 생성합니다. 마운트 지점을 수동으로 생성할 필요는 없습니다.

- ONTAP API('ontapi')

  이 서비스를 사용하면 ONTAP API를 실행하여 원격 프로그램으로 관리 기능을 실행할 수 있습니다. 기본 설정은 "사용"입니다.

  일부 외부 관리 도구에 이 서비스가 필요할 수 있습니다. 예를 들어, System Manager를 사용하는 경우 이 서비스를 활성 상태로 유지해야 합니다.

- Data ONTAP 디스커버리(disco)

  이 서비스를 사용하면 오프 박스 관리 애플리케이션이 네트워크에서 클러스터를 검색할 수 있습니다. 기본 설정은 "사용"입니다.

- 지원 진단('Support')

이 서비스는 시스템의 특별 권한 환경에 대한 액세스를 제어하여 문제 분석 및 해결을 지원합니다. 기본 설정은 사용 안 함 입니다. 기술 지원 부서의 지시가 있을 때만 이 서비스를 활성화해야 합니다.

- System Manager('smmgr')

  이 서비스는 ONTAP에 포함된 System Manager의 가용성을 제어합니다. 기본 설정은 "사용"입니다. 이 서비스는 클러스터에서만 지원됩니다.

- 펌웨어 베이스보드 관리 컨트롤러(BMC) 업데이트('FW_BMC')

  이 서비스를 사용하여 BMC 펌웨어 파일을 다운로드할 수 있습니다. 기본 설정은 "사용"입니다.

- ONTAP 문서(dOCS)

  이 서비스를 통해 ONTAP 설명서에 액세스할 수 있습니다. 기본 설정은 "사용"입니다.

- ONTAP RESTful API(DOCS_API)

  이 서비스를 통해 ONTAP RESTful API 설명서에 액세스할 수 있습니다. 기본 설정은 "사용"입니다.

- 파일 업로드 및 다운로드('FUD')

  이 서비스는 파일 업로드 및 다운로드를 제공합니다. 기본 설정은 "사용"입니다.

- ONTAP 메시징('ontapmsg')

  이 서비스는 이벤트에 등록할 수 있는 게시 및 구독 인터페이스를 지원합니다. 기본 설정은 "사용"입니다.

- ONTAP 포털('포털')

  이 서비스는 게이트웨이를 가상 서버에 구현합니다. 기본 설정은 "사용"입니다.

- ONTAP Restful Interface(재차)

  이 서비스는 클러스터 인프라의 모든 요소를 원격으로 관리하는 데 사용되는 RESTful 인터페이스를 지원합니다. 기본 설정은 "사용"입니다.

- SAML(Security Assertion Markup Language) 서비스 공급자 지원(SAML)

  이 서비스는 SAML 서비스 공급자를 지원하는 리소스를 제공합니다. 기본 설정은 "사용"입니다.

- SAML 서비스 공급자(SML-SP)

  이 서비스는 SP 메타데이터 및 어설션 소비자 서비스와 같은 서비스를 서비스 공급자에게 제공합니다. 기본 설정은 "사용"입니다.

ONTAP 9.7부터는 다음과 같은 추가 서비스가 지원됩니다.

- 구성 백업 파일('백업')

  이 서비스를 사용하면 구성 백업 파일을 다운로드할 수 있습니다. 기본 설정은 "사용"입니다.

- ONTAP 보안('보안')

이 서비스는 향상된 인증을 위해 CSRF 토큰 관리를 지원합니다. 기본 설정은 "사용"입니다.

ONTAP에서 웹 프로토콜 엔진을 관리합니다

웹 액세스가 허용되는지 여부와 사용할 수 있는 SSL 버전을 제어하도록 클러스터의 웹 프로토콜 엔진을 구성할 수 있습니다. 웹 프로토콜 엔진에 대한 구성 설정을 표시할 수도 있습니다.

다음과 같은 방법으로 클러스터 수준에서 웹 프로토콜 엔진을 관리할 수 있습니다.

- '-external' 파라미터를 가진 'system services web modify' 명령어를 이용하여 원격 클라이언트가 HTTP나 HTTPS를 이용하여 웹 서비스 컨텐츠에 액세스할 수 있는지 여부를 지정할 수 있다.
- '-supported-protocol' 파라미터를 가진 '보안 설정 수정' 명령어를 이용하여 SSLv3을 안전한 웹 액세스에 사용할지 여부를 지정할 수 있다. 기본적으로 SSLv3은 비활성화되어 있습니다. 전송 계층 보안 1.0(TLSv1.0)이 활성화되어 있으며 필요한 경우 비활성화할 수 있습니다.

  에 대한 자세한 내용은 `security config modify` "ONTAP 명령 참조입니다"을 참조하십시오.

- FIPS(Federal Information Processing Standard) 140-2 규정 준수 모드를 사용하여 클러스터 전체의 컨트롤 플레인 웹 서비스 인터페이스를 구현할 수 있습니다.

  기본적으로 FIPS 140-2 규정 준수 모드는 비활성화되어 있습니다.

  - * FIPS 140-2 compliance mode 비활성화 시 * '보안 구성 수정' 명령에 대해 'is-FIPS-enabled' 매개 변수를 'true'로 설정한 다음 'security config show' 명령을 사용하여 온라인 상태를 확인하면 FIPS 140-2 compliance 모드를 사용할 수 있습니다.
  - * FIPS 140-2 규정 준수 모드가 활성화된 경우 *
    - ONTAP 9.11.1부터 TLSv1, TLSv1.1 및 SSLv3이 비활성화되고 TSLv1.2 및 TSLv1.3만 활성화됩니다. ONTAP 9 내부와 외부의 다른 시스템 및 통신에 영향을 줍니다. FIPS 140-2 규정 준수 모드를 활성화한 후 이후에 사용하지 않도록 설정하는 경우 TLSv1, TLSv1.1 및 SSLv3은 비활성화 상태로 유지됩니다. TLSv1.2 또는 TLSv1.3은 이전 구성에 따라 활성화된 상태로 유지됩니다.
    - 9.11.1 이전의 ONTAP 버전에서는 TLSv1 및 SSLv3이 모두 사용되지 않고 TLSv1.1 및 TLSv1.2만 활성화됩니다. ONTAP를 사용하면 FIPS 140-2 규정 준수 모드가 활성화된 경우 TLSv1 및 SSLv3을 모두 사용할 수 없습니다. FIPS 140-2 규정 준수 모드를 활성화한 후 나중에 비활성화하면 TLSv1 및 SSLv3은 비활성화 상태로 유지되지만 TLSv1.2 또는 TLSv1.1 및 TLSv1.2는 이전 구성에 따라 모두 활성화됩니다.
- 'system security config show' 명령을 사용하여 클러스터 차원의 보안 구성을 표시할 수 있습니다.

  에 대한 자세한 내용은 `security config show` "ONTAP 명령 참조입니다"을 참조하십시오.

방화벽이 설정된 경우 웹 서비스에 사용할 논리 인터페이스(LIF)의 방화벽 정책을 HTTP 또는 HTTPS 액세스를 허용하도록 설정해야 합니다.

웹 서비스 액세스에 HTTPS를 사용하는 경우, 웹 서비스를 제공하는 클러스터 또는 SVM(스토리지 가상 머신)에 SSL도 사용하도록 설정해야 하며 클러스터 또는 SVM에 디지털 인증서를 제공해야 합니다.

MetroCluster 구성에서는 클러스터의 웹 프로토콜 엔진에 대해 변경한 설정이 파트너 클러스터에 복제되지 않습니다.

웹 프로토콜 엔진을 관리하기 위한 **ONTAP** 명령

'system services web' 명령어를 이용하여 웹 프로토콜 엔진을 관리한다. '시스템 서비스 방화벽 정책 생성' 및 '네트워크 인터페이스 수정' 명령을 사용하여 웹 액세스 요청이 방화벽을 통과할 수 있도록 합니다.

원하는 작업	이 명령 사용...
클러스터 수준에서 웹 프로토콜 엔진을 구성합니다. • 클러스터에 대한 웹 프로토콜 엔진을 설정하거나 해제합니다 • 클러스터에 대해 SSLv3을 사용하거나 사용하지 않도록 설정합니다 • 보안 웹 서비스(HTTPS)를 위해 FIPS 140-2 규정 준수 활성화 또는 비활성화	'시스템 서비스 웹 수정
클러스터 수준에서 웹 프로토콜 엔진의 구성을 표시하고, 클러스터 전체에서 웹 프로토콜이 작동하는지 여부를 확인하고, FIPS 140-2 규정 준수를 활성화 및 온라인 상태로 표시합니다	'시스템 서비스 웹 쇼'
노드의 웹 프로토콜 엔진 구성 및 클러스터의 노드에 대한 웹 서비스 처리 작업을 표시합니다	'시스템 서비스 웹 노드 쇼'
방화벽 정책을 생성하거나 기존 방화벽 정책에 HTTP 또는 HTTPS 프로토콜 서비스를 추가하여 웹 액세스 요청이 방화벽을 통과할 수 있도록 합니다	'시스템 서비스 방화벽 정책 생성 service 매개 변수를 http 또는 https로 설정하면 웹 액세스 요청이 방화벽을 통과할 수 있습니다.
방화벽 정책을 LIF와 연결합니다	네트워크 인터페이스 수정 '-firewall-policy' 매개 변수를 사용하여 LIF의 방화벽 정책을 수정할 수 있습니다.

관련 정보

- "네트워크 인터페이스 수정"

ONTAP 웹 서비스에 대한 액세스 구성

웹 서비스에 대한 액세스를 구성하면 권한 있는 사용자가 HTTP 또는 HTTPS를 사용하여 클러스터의 서비스 콘텐츠 또는 SVM(스토리지 가상 머신)에 액세스할 수 있습니다.

단계

1. 방화벽이 설정된 경우 웹 서비스에 사용될 LIF의 방화벽 정책에 HTTP 또는 HTTPS 액세스가 설정되어 있는지 확인합니다.

'system services firewall show' 명령을 사용하여 방화벽이 활성화되어 있는지 확인할 수 있습니다.

a. 방화벽 정책에 HTTP 또는 HTTPS가 설정되어 있는지 확인하려면 'system services firewall policy show' 명령을 사용합니다.

   시스템 서비스 방화벽 정책의 '-service' 매개 변수를 'http' 또는 'https'로 설정하여 해당 정책이 웹 액세스를 지원할 수 있도록 합니다.

b. HTTP 또는 HTTPS를 지원하는 방화벽 정책이 웹 서비스를 제공하는 LIF와 연결되어 있는지 확인하려면 '-firewall-policy' 매개 변수와 함께 'network interface show' 명령을 사용하십시오.

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

   'network interface modify' 명령을 '-firewall-policy' 매개 변수와 함께 사용하여 LIF에 방화벽 정책을 적용합니다.

에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 클러스터 수준 웹 프로토콜 엔진을 구성하고 웹 서비스 콘텐츠를 액세스할 수 있도록 하려면 'system services web modify' 명령을 사용합니다.
3. 보안 웹 서비스(HTTPS)를 사용하려는 경우 '보안 SSL 수정' 명령을 사용하여 SSL을 활성화하고 클러스터 또는 SVM에 대한 디지털 인증서 정보를 제공합니다.

   에 대한 자세한 내용은 `security ssl modify` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 클러스터 또는 SVM에 대한 웹 서비스를 활성화하려면 'vserver services web modify' 명령을 사용하십시오.

   클러스터 또는 SVM에 대해 활성화할 각 서비스에 대해 이 단계를 반복해야 합니다.

5. 클러스터 또는 SVM에서 웹 서비스에 액세스하는 역할을 승인하려면 'vserver services web access create' 명령을 사용하십시오.

   액세스 권한을 부여하는 역할이 이미 있어야 합니다. 'Security login role show' 명령어를 사용해 기존 역할을 표시하거나, 'ecurity login role create' 명령어를 사용해 새로운 역할을 생성할 수 있다.

   및 `security login role create` 에 대한 자세한 `security login role show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

6. 웹 서비스에 액세스할 수 있는 권한을 가진 역할의 경우, '보안 로그인 표시' 명령의 출력을 확인하여 사용자가 올바른 액세스 방법을 사용하도록 구성해야 합니다.

   ONTAP API 웹 서비스('ontapi')에 액세스하려면 사용자가 "ontapi" 액세스 방법으로 구성해야 합니다. 다른 모든 웹 서비스에 액세스하려면 사용자가 http 액세스 방법으로 구성되어야 합니다.

   에 대한 자세한 내용은 `security login show` "ONTAP 명령 참조입니다"을 참조하십시오.

명령을 사용하여 `security login create` 사용자에 대한 액세스 방법을 추가합니다. 에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

웹 서비스 관리를 위한 **ONTAP** 명령

'vserver services web' 명령을 사용하여 클러스터나 SVM(스토리지 가상 머신)의 웹 서비스 가용성을 관리할 수 있습니다. 'vserver services web access' 명령을 사용하여 웹 서비스에 대한 역할의 액세스를 제어합니다.

원하는 작업	이 명령 사용...
클러스터 또는 SVM을 위한 웹 서비스 구성: • 웹 서비스를 활성화 또는 비활성화합니다 • 웹 서비스에 액세스하는 데 HTTPS만 사용할 수 있는지 여부를 지정합니다	가상 서버 서비스 웹 수정
클러스터 또는 anSVM을 위한 웹 서비스의 구성 및 가용성을 표시합니다	가상 서버 서비스 웹 쇼
클러스터 또는 SVM에서 웹 서비스에 액세스하는 역할을 승인합니다	'vserver services web access create'
클러스터 또는 anSVM에서 웹 서비스에 액세스하도록 승인된 역할을 표시합니다	'vserver services web access show'
클러스터 또는 SVM에서 웹 서비스에 대한 역할 액세스 방지	'vserver services web access delete'(가상 서버 서비스 웹 액세스 삭제)

관련 정보

"ONTAP 명령 참조입니다"

ONTAP 노드의 마운트 포인트를 관리하기 위한 명령

'pi' 웹 서비스는 노드의 로그 파일 또는 코어 파일에 대한 액세스 요청이 있을 경우 한 노드에서 다른 노드의 루트 볼륨으로 마운트 지점을 자동으로 생성합니다. 마운트 지점을 수동으로 관리할 필요는 없지만 'system node root-mount' 명령을 사용하면 됩니다.

원하는 작업	이 명령 사용...
한 노드에서 다른 노드의 루트 볼륨으로 마운트 지점을 수동으로 생성합니다	'시스템 노드 root-mount create' 하나의 노드만 다른 노드로 존재할 수 있다.
마운트 지점이 생성된 시간과 현재 상태를 포함하여 클러스터의 노드에 기존 마운트 지점을 표시합니다	'system node root-mount show'
한 노드에서 다른 노드의 루트 볼륨으로 마운트 지점을 삭제하고 마운트 지점에 대한 연결을 강제로 닫습니다	'시스템 노드 root-mount delete

관련 정보

"ONTAP 명령 참조입니다"

ONTAP 에서 SSL 관리

를 사용합니다 `security ssl` 클러스터 또는 SVM(스토리지 가상 머신)에 대한 SSL 프로토콜을 관리하는 명령입니다. SSL 프로토콜은 디지털 인증서를 사용하여 웹 서버와 브라우저 간에 암호화된 연결을 설정함으로써 웹 액세스의 보안을 향상시킵니다.

다음과 같은 방법으로 클러스터 또는 SVM(스토리지 가상 머신)의 SSL을 관리할 수 있습니다.

- SSL 활성화
- 디지털 인증서를 생성 및 설치하고 이를 클러스터 또는 SVM과 연계합니다
- SSL이 활성화되었는지 여부를 확인하기 위해 SSL 구성을 표시하고, 사용 가능한 경우 SSL 인증서 이름을 표시합니다
- 웹 액세스 요청을 통과할 수 있도록 클러스터 또는 SVM에 대한 방화벽 정책 설정
- 사용할 수 있는 SSL 버전을 정의합니다
- 웹 서비스에 대한 HTTPS 요청에만 액세스를 제한합니다

SSL 관리를 위한 명령입니다

를 사용합니다 `security ssl` 클러스터 또는 SVM(스토리지 가상 머신)에 대한 SSL 프로토콜을 관리하는 명령입니다.

원하는 작업	이 명령 사용...
클러스터 또는 SVM에 SSL을 활성화하고 디지털 인증서를 연결합니다	보안 SSL 수정
클러스터 또는 SVM의 SSL 구성과 인증서 이름을 표시합니다	보안 SSL 쇼

및 `security ssl show` 에 대한 자세한 `security ssl modify` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

ONTAP 웹 서비스에 HSTS 사용

HTTP Strict Transport Security(HSTS)는 프로토콜 다운그레이드 공격 및 쿠키 하이재킹과 같은 중간자 공격으로부터 웹사이트를 보호하는 웹 보안 정책 메커니즘입니다. HSTS는 HTTPS 사용을 강제함으로써 사용자 브라우저와 서버 간의 모든 통신이 암호화되도록 보장합니다. ONTAP 9.17.1부터 ONTAP ONTAP 웹 서비스에 HTTPS 연결을 강제할 수 있습니다.

HSTS는 ONTAP 과 초기 보안 HTTPS 연결이 설정된 후에만 웹 브라우저에 의해 적용됩니다. 브라우저가 초기 보안 연결을 설정하지 않으면 HSTS가 적용되지 않습니다. HSTS 관리에 대한 자세한 내용은 브라우저 설명서를 참조하십시오.

이 작업에 대해

- 9.17.1 이상에서는 새로 설치된 ONTAP 클러스터에 대해 HSTS가 기본적으로 활성화되어 있습니다. 9.17.1로 업그레이드하면 HSTS가 기본적으로 활성화되지 않습니다. 업그레이드 후 HSTS를 활성화해야 합니다.
- HSTS는 모든 지원됩니다 "ONTAP 웹 서비스" .

시작하기 전에

- 다음 작업에는 고급 권한이 필요합니다.

HSTS 구성 표시

현재 HSTS 구성을 표시하여 활성화되어 있는지 확인하고 최대 연령 설정을 볼 수 있습니다.

단계

1. 사용하세요 `system services web show` HSTS 설정을 포함한 현재 웹 서비스 구성을 표시하는 명령:

```
cluster-1::system services web*> show

                    External Web Services: true
                                HTTP Port: 80
                               HTTPS Port: 443
                          Protocol Status: online
                        Per Address Limit: 80
                      Wait Queue Capacity: 192
                             HTTP Enabled: true
                  CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                            HSTS Enabled: true
                   HSTS max age (Seconds): 63072000
```

HSTS를 활성화하고 최대 연령을 설정하세요

ONTAP 9.17.1부터 새 ONTAP 클러스터에서 HSTS가 기본적으로 활성화됩니다. 기존 클러스터를 9.17.1 이상으로 업그레이드하는 경우, HTTPS 사용을 강제하려면 클러스터에서 HSTS를 수동으로 활성화해야 합니다. HSTS를 활성화하고 최대 사용 기간을 설정할 수 있습니다. HSTS가 활성화된 경우 언제든지 최대 사용 기간을 변경할 수 있습니다. HSTS가 활성화되면 브라우저는 초기 보안 연결이 설정된 후에만 보안 연결을 적용하기 시작합니다.

단계

1. 사용하세요 `system services web modify` HSTS를 활성화하거나 최대 연령을 수정하는 명령:

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age` 브라우저가 HTTPS를 강제 적용하는 기간을 초 단위로 지정합니다. 기본값은 63072000초(2년)입니다.

HSTS 비활성화

브라우저는 각 연결마다 HSTS 최대 사용 기간 설정을 저장하며, ONTAP 에서 HSTS가 비활성화된 경우에도 전체 기간 동안 HSTS를 계속 적용합니다. HSTS가 비활성화된 후 브라우저가 HSTS 적용을 중단하는 데는 설정된 최대 사용 기간까지 걸립니다. 이 기간 동안 보안 연결이 불가능해지면 HSTS를 적용하는 브라우저는 문제가 해결되거나 브라우저의 최대 사용 기간이 만료될 때까지 ONTAP 웹 서비스에 대한 액세스를 허용하지 않습니다.

단계

1. HSTS를 비활성화하려면 다음을 사용하세요. `system services web modify` 명령:

```
system services web modify -hsts-enabled false
```

관련 정보

"RFC 6797 - HTTP 엄격한 전송 보안(HSTS)"

ONTAP 웹 서비스 액세스 문제 해결

구성 오류로 인해 웹 서비스 액세스 문제가 발생합니다. LIF, 방화벽 정책, 웹 프로토콜 엔진, 웹 서비스, 디지털 인증서를 확인하여 오류를 해결할 수 있습니다. 사용자 액세스 권한이 모두 올바르게 구성되어 있습니다.

다음 표는 웹 서비스 구성 오류를 식별하고 해결하는 데 도움이 됩니다.

이 액세스 문제는...	이 구성 오류로 인해 발생합니다.	오류를 해결하려면...
웹 서비스에 액세스하려고 하면 웹 브라우저에서 "연결할 수 없음" 또는 "연결 실패" 오류가 반환됩니다.	LIF가 잘못 구성될 수 있습니다.	웹 서비스를 제공하는 LIF를 ping할 수 있는지 확인합니다. 명령을 사용하여 `network ping` LIF를 ping할 수 있습니다.

이 액세스 문제는...	이 구성 오류로 인해 발생합니다.	오류를 해결하려면...
방화벽이 잘못 구성되었을 수 있습니다.	HTTP 또는 HTTPS를 지원하도록 방화벽 정책을 설정하고 웹 서비스를 제공하는 LIF에 정책이 할당되도록 합니다. '시스템 서비스 방화벽 정책' 명령을 사용하여 방화벽 정책을 관리합니다. 'network interface modify' 명령을 '-firewall-policy' 매개 변수와 함께 사용하여 정책을 LIF와 연결합니다.	웹 프로토콜 엔진이 비활성화되었을 수 있습니다.
웹 서비스에 액세스할 수 있도록 웹 프로토콜 엔진이 활성화되어 있는지 확인합니다. '시스템 서비스 웹' 명령을 사용하여 클러스터의 웹 프로토콜 엔진을 관리합니다.	웹 서비스에 액세스하려고 하면 웹 브라우저에서 "찾을 수 없음" 오류가 반환됩니다.	웹 서비스가 비활성화되었을 수 있습니다.
액세스를 허용할 각 웹 서비스가 개별적으로 설정되어 있는지 확인합니다. 'vserver services web modify' 명령을 사용하여 액세스를 위한 웹 서비스를 활성화할 수 있습니다.	웹 브라우저가 사용자의 계정 이름 및 암호를 사용하여 웹 서비스에 로그인하지 못합니다.	사용자를 인증할 수 없거나, 액세스 방법이 올바르지 않거나, 사용자가 웹 서비스에 액세스할 수 있는 권한이 없습니다.

이 액세스 문제는...	이 구성 오류로 인해 발생합니다.	오류를 해결하려면...
사용자 계정이 존재하고 올바른 액세스 방법 및 인증 방법으로 구성되었는지 확인합니다. 또한 사용자의 역할이 웹 서비스에 액세스할 수 있는 권한이 있는지 확인합니다. '보안 로그인' 명령어를 이용하여 사용자 계정과 접속 방법 및 인증 방식을 관리할 수 있다. ONTAP API 웹 서비스에 액세스하려면 "ontapi" 액세스 방법이 필요합니다. 다른 모든 웹 서비스에 액세스하려면 http 접근 방식이 필요합니다. 'vserver services web access' 명령을 사용하여 웹 서비스에 대한 역할의 액세스를 관리합니다.	HTTPS를 사용하여 웹 서비스에 연결하면 웹 브라우저에서 연결이 중단되었음을 나타냅니다.	웹 서비스를 제공하는 클러스터 또는 SVM(스토리지 가상 머신)에서 SSL을 사용하지 못할 수 있습니다.
클러스터 또는 SVM에 SSL이 활성화되어 있고 디지털 인증서가 유효한지 확인합니다. 'Security SSL' 명령어를 이용하여 HTTP 서버의 SSL 설정을 관리하고 'Security certificate show' 명령어를 이용하여 디지털 인증서 정보를 출력한다.	HTTPS를 사용하여 웹 서비스에 연결하면 웹 브라우저에서 연결을 신뢰할 수 없음을 나타냅니다.	자체 서명된 디지털 인증서를 사용 중일 수 있습니다.

관련 정보

- "ONTAP 의 네트워크 구성에 대한 모범 사례는 무엇입니까?"
- "네트워크 Ping"
- "네트워크 인터페이스 수정"
- "보안 인증서 생성 - CSR"
- "보안 인증서 설치"

- "보안 인증서가 표시됩니다"
- "보안 SSL"

인증서를 사용하여 원격 서버의 ID를 확인합니다

ONTAP 에서 인증서를 사용하여 원격 서버의 신원을 확인하는 방법에 대해 알아보세요.

ONTAP는 보안 인증서 기능을 지원하여 원격 서버의 ID를 확인합니다.

ONTAP 소프트웨어는 다음과 같은 디지털 인증서 기능 및 프로토콜을 사용하여 보안 연결을 지원합니다.

- OCSP(온라인 인증서 상태 프로토콜)는 SSL 및 TLS(전송 계층 보안) 연결을 사용하여 ONTAP 서비스에서 디지털 인증서 요청 상태를 검증합니다. 이 기능은 기본적으로 비활성화되어 있습니다.
- 신뢰할 수 있는 루트 인증서의 기본 집합은 ONTAP 소프트웨어에 포함되어 있습니다.
- KMIP(Key Management Interoperability Protocol) 인증서를 통해 클러스터 및 KMIP 서버를 상호 인증할 수 있습니다.

ONTAP 에서 OCSP를 사용하여 디지털 인증서가 유효한지 확인합니다.

OCSP(온라인 인증서 상태 프로토콜)는 OCSP가 활성화된 경우 TLS(전송 계층 보안) 통신을 사용하는 ONTAP 애플리케이션이 디지털 인증서 상태를 수신할 수 있도록 합니다. 특정 애플리케이션에 대한 OCSP 인증서 상태 확인을 언제든지 활성화 또는 비활성화할 수 있습니다. 기본적으로 OCSP 인증서 상태 확인은 사용되지 않습니다.

시작하기 전에

이 작업을 수행하려면 고급 권한 수준 액세스 권한이 필요합니다.

이 작업에 대해

OCSP는 다음 애플리케이션을 지원합니다.

- AutoSupport
- EMS(이벤트 관리 시스템)
- TLS를 통한 LDAP
- 키 관리 상호 운용성 프로토콜(KMIP)
- 로깅 감사
- FabricPool
- SSH(ONTAP 9.13.1 로 시작)

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다.
2. 특정 ONTAP 응용 프로그램에 대한 OCSP 인증서 상태 검사를 사용하거나 사용하지 않도록 설정하려면 적절한 명령을 사용합니다.

OCSP 인증서 상태를 통해 일부 응용 프로그램을 확인하려는 경우...	명령 사용...
활성화됨	`security config ocsp enable -app app name`
사용 안 함	`security config ocsp disable -app app name`

다음 명령을 실행하면 AutoSupport 및 EMS에 대한 OCSP 지원이 활성화됩니다.

```
cluster::*> security config ocsp enable -app asup,ems
```

OCSP가 활성화되면 애플리케이션은 다음 응답 중 하나를 수신합니다.

- 양호 - 인증서가 유효하며 통신이 진행됩니다.
- 해지 - 인증서는 발급 인증 기관에서 영구적으로 신뢰할 수 없는 것으로 간주되어 통신이 진행되지 않습니다.
- 알 수 없음 - 서버에 인증서에 대한 상태 정보가 없으며 통신이 진행되지 않습니다.
- OCSP 서버 정보가 인증서에 없습니다. 서버는 OCSP가 비활성화되어 TLS 통신을 계속하는 것처럼 작동하지만 상태 검사는 발생하지 않습니다.
- OCSP 서버의 응답이 없습니다. 응용 프로그램을 계속할 수 없습니다.

3. TLS 통신을 사용하는 모든 응용 프로그램에 대해 OCSP 인증서 상태 검사를 사용하거나 사용하지 않도록 설정하려면 적절한 명령을 사용합니다.

OCSP 인증서 상태가 모든 응용 프로그램의 상태를 확인하려는 경우...	명령 사용...
활성화됨	'보안 구성 OCSP 활성화 '-APP ALL'
사용 안 함	보안 구성 OCSP 비활성화 '-APP ALL'

이 옵션을 활성화하면 모든 응용 프로그램은 지정된 인증서가 양호, 취소 또는 알 수 없다는 서명된 응답을 받습니다. 인증서가 해지된 경우 응용 프로그램을 계속 진행할 수 없습니다. 애플리케이션이 OCSP 서버로부터 응답을 수신하지 못하거나 서버에 연결할 수 없는 경우 응용 프로그램을 계속 진행할 수 없습니다.

4. 'Security config OCSP show' 명령어를 사용하면 OCSP를 지원하는 모든 애플리케이션과 지원 상태를 확인할 수 있다.

```
cluster::*> security config ocsp show
         Application                         OCSP Enabled?
         --------------------                ---------------------
         autosupport                         false
         audit_log                           false
         fabricpool                          false
         ems                                 false
         kmip                                false
         ldap_ad                             true
         ldap_nis_namemap                    true
         ssh                                 true

         8 entries were displayed.
```

관련 정보

- "보안 구성 OCSP를 사용할 수 있습니다"
- "보안 구성 OCSP 비활성화"
- "보안 구성 OCSP 쇼"

ONTAP 에서 TLS 기반 애플리케이션의 기본 인증서 보기

ONTAP TLS(전송 계층 보안)를 사용하여 ONTAP 애플리케이션에 대한 기본 신뢰할 수 있는 루트 인증서 세트를 제공합니다.

시작하기 전에

기본 인증서는 관리자 SVM을 생성하는 동안 또는 업그레이드하는 동안에만 설치됩니다.

이 작업에 대해

현재 클라이언트 역할을 하고 인증서 검증이 필요한 애플리케이션은 AutoSupport, EMS, LDAP, 감사 로깅, FabricPool입니다. 및 KMIP

인증서가 만료되면 사용자에게 인증서 삭제를 요청하는 EMS 메시지가 호출됩니다. 기본 인증서는 고급 권한 수준에서만 삭제할 수 있습니다.

> 기본 인증서를 삭제하면 일부 ONTAP 응용 프로그램이 예상대로 작동하지 않을 수 있습니다(예: AutoSupport 및 감사 로깅).

단계

1. security certificate show 명령을 사용하여 admin SVM에 설치된 기본 인증서를 볼 수 있습니다.

   '* security certificate show -vserver –type server-ca*'

```
cluster1::> security certificate show

Vserver    Serial Number   Certificate Name
Type
---------- -------------- ----------------------------------------
---------
vs0        4F4E4D7B         www.example.com
server
    Certificate Authority:  www.example.com
          Expiration Date: Thu Feb 28 16:08:28 2013
```

에 대한 자세한 내용은 `security certificate show` "ONTAP 명령 참조입니다"을 참조하십시오.

클러스터와 KMIP 서버를 상호 인증합니다

ONTAP 클러스터와 KMIP 서버 개요 상호 인증

KMIP(Key Management Interoperability Protocol) 서버와 같은 외부 키 관리자를 함께 사용하면 키 관리자가 SSL을 통해 KMIP를 사용하여 클러스터와 통신할 수 있습니다. 애플리케이션 또는 특정 기능(예: 스토리지 암호화 기능)에서 보안 데이터 액세스를 제공하기 위해 보안 키가 필요한 경우 이 작업을 수행합니다.

ONTAP에서 클러스터에 대한 인증서 서명 요청을 생성합니다

보안 인증서 'generate-csr' 명령을 사용하여 인증서 서명 요청(CSR)을 생성할 수 있습니다. 요청을 처리한 후 CA(인증 기관)에서 서명된 디지털 인증서를 보냅니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자 또는 SVM 관리자여야 합니다.

단계

1. CSR 생성:

```
security certificate generate-csr -common-name <FQDN_or_common_name>
-size 512|1024|1536|2048 -country <country> -state <state> -locality
<locality> -organization <organization> -unit <unit> -email-addr
<email_of_contact> -hash-function SHA1|SHA256|MD5
```

에 대한 자세한 내용은 `security certificate generate-csr` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령은 SHA256 해싱 기능에 의해 생성된 2,048비트 개인 키를 가진 CSR을 생성하고, 사용자 정의 공통 이름이 server1.companyname.com 인 회사의 IT 부서에서 사용하는 사용자 정의 공용 키가 미국 캘리포니아주 서니베일에 있습니다. SVM 연락처 관리자의 이메일 주소는 web@example.com 입니다. 출력에 CSR과 개인 키가

표시됩니다.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. CSR 출력에서 인증서 요청을 복사한 다음 전자 양식(예: 전자 메일)으로 신뢰할 수 있는 타사 CA로 보내 서명합니다.

   요청을 처리한 후 CA는 서명된 디지털 인증서를 보냅니다. 개인 키와 CA 서명 디지털 인증서의 복사본을 유지해야 합니다.

ONTAP 클러스터에 대한 CA 서명 서버 인증서 설치

SSL 서버에서 클러스터 또는 SVM(Storage Virtual Machine)을 SSL 클라이언트로 인증할 수 있도록 하려면 클러스터 또는 SVM에 클라이언트 유형과 함께 디지털 인증서를 설치합니다. 그런 다음 서버에 설치하기 위해 SSL 서버 관리자에게 클라이언트-CA 인증서를 제공합니다.

시작하기 전에

SSL 서버의 루트 인증서를 이미 클러스터 또는 SVM에 'server-ca' 인증서 유형으로 설치해야 합니다.

단계

1. 클라이언트 인증에 자체 서명된 디지털 인증서를 사용하려면 type client 매개 변수를 사용하여 Security certificate create 명령을 사용합니다.

   에 대한 자세한 내용은 `security certificate create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 클라이언트 인증에 CA 서명 디지털 인증서를 사용하려면 다음 단계를 수행하십시오.

   a. 보안 인증서 'generate-csr' 명령을 사용하여 디지털 인증서 서명 요청(CSR)을 생성합니다.

      ONTAP는 인증서 요청과 개인 키가 포함된 CSR 출력을 표시하고 나중에 참조할 수 있도록 출력을 파일로 복사하도록 알려 줍니다.

   b. 전자 양식(예: 전자 메일)으로 CSR 출력에서 인증서 요청을 신뢰할 수 있는 CA로 보내 서명합니다.

나중에 참조할 수 있도록 개인 키와 CA 서명 인증서의 복사본을 유지해야 합니다.

요청을 처리한 후 CA는 서명된 디지털 인증서를 보냅니다.

a. '-type client' 매개 변수와 함께 보안 인증서 설치 명령을 사용하여 CA 서명 인증서를 설치합니다.
b. 메시지가 표시되면 인증서와 개인 키를 입력한 다음 * Enter * 키를 누릅니다.
c. 메시지가 표시되면 추가 루트 또는 중간 인증서를 입력하고 * Enter * 를 누릅니다.

   신뢰할 수 있는 루트 CA에서 시작하고 사용자에게 발급된 SSL 인증서로 끝나는 인증서 체인이 중간 인증서를 누락하는 경우 클러스터나 SVM에 중간 인증서를 설치합니다. 중간 인증서는 최종 엔터티 서버 인증서를 발급하기 위해 신뢰할 수 있는 루트에서 발급하는 하위 인증서입니다. 그 결과 신뢰할 수 있는 루트 CA에서 시작하여 중간 인증서를 거쳐 사용자에게 발급된 SSL 인증서로 끝나는 인증서 체인이 만들어집니다.

3. 서버에 설치하기 위해 SSL 서버 관리자에게 클러스터 또는 SVM의 '클라이언트-CA' 인증서를 제공합니다.

   인스턴스, 클라이언트-CA 형식의 매개 변수를 가진 보안 인증서 표시 명령은 클라이언트-CA 인증서 정보를 표시합니다.

관련 정보

- "보안 인증서 설치"
- "보안 인증서가 표시됩니다"

ONTAP 의 KMIP 서버에 대한 CA 서명 클라이언트 인증서 설치

클라이언트 및 서버 CA 유형과 함께 KMIP(Key Management Interoperability Protocol)(-subtype KMIP-cert 매개 변수)의 인증서 하위 유형은 클러스터 및 KMIP 서버와 같은 외부 키 관리자를 상호 인증하는 데 인증서가 사용됨을 나타냅니다.

이 작업에 대해

KMIP 인증서를 설치하여 KMIP 서버를 클러스터에 대한 SSL 서버로 인증합니다.

단계

1. KMIP 서버용 KMIP 인증서를 설치하려면 '-type server-ca' 및 '-subtype KMIP-cert' 매개 변수와 함께 'Security certificate install' 명령을 사용하십시오.
2. 메시지가 표시되면 인증서를 입력한 다음 Enter 키를 누릅니다.

   ONTAP는 나중에 참조할 수 있도록 인증서 복사본을 보관하도록 알려 줍니다.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```

관련 정보

- "보안 인증서 설치"

보안 및 데이터 암호화

자율 랜섬웨어 보호

ONTAP 자율적 랜섬웨어 방어에 대해 알아보십시오

ONTAP 9.10.1부터 ONTAP 관리자는 NAS(NFS 및 SMB) 환경에서 워크로드 분석을 수행하는 ARP(자율 랜섬웨어 보호)를 활성화하여 랜섬웨어 공격을 나타낼 수 있는 비정상 활동을 사전에 감지하고 경고할 수 있습니다. ONTAP 9.17.1부터 ARP는 LUN이나 NVMe 네임스페이스를 포함하는 SAN 볼륨이나 VMware와 같은 하이퍼바이저의 가상 디스크를 포함하는 NAS 볼륨을 비롯한 블록 장치 볼륨도 지원합니다.

ARP는 ONTAP에 직접 내장되어 ONTAP의 다른 기능들과의 통합 제어 및 조정을 보장합니다. ARP는 실시간으로 작동하여 파일 시스템에 데이터를 쓰거나 읽는 동시에 처리하고, 잠재적인 랜섬웨어 공격을 신속하게 탐지하고 대응합니다.

ARP는 추가적인 보호를 위해 정기적인 간격과 예약된 간격으로 잠금 스냅샷을 생성합니다. 스냅샷 보존 기간을 스마트하게 관리합니다. 특이한 활동이 감지되지 않으면 스냅샷은 빠르게 재사용됩니다. 하지만 공격이 감지되면 공격 시작 전에 생성된 스냅샷이 장기간 보관됩니다. ONTAP 버전에 따른 변경 사항을 포함한 자세한 내용은 다음을 참조하십시오. ARP 스냅샷.

라이센스 및 지원

ARP를 사용하려면 라이센스가 필요합니다. 새 볼륨에서 ARP를 기본적으로 활성화할지, 아니면 볼륨별로 수동으로 활성화할지 결정하십시오.

ARP 라이선스 옵션

ARP 지원이 포함되어 있습니다."ONTAP One 라이센스" . ONTAP One 라이선스가 없는 경우 ONTAP 버전에 따라 ARP 사용을 위한 다른 라이선스를 사용할 수 있습니다

ONTAP 릴리스	라이센스
ONTAP 9.11.1 이상	`Anti_ransomware`
ONTAP 9.10.1	`MT_EK_MGMT` (멀티 테넌트 키 관리)

- ONTAP 9.10.1에서 ONTAP 9.11.1 이상으로 업그레이드하고 시스템에 ARP가 이미 구성되어 있는 경우 새 버전을 설치할 필요가 없습니다. `Anti-ransomware` 라이센스. 새로운 ARP 구성에는 새 라이센스가 필요합니다.
- ONTAP 9.11.1 이상에서 ONTAP 9.10.1로 되돌리고 Anti_ransomware 라이선스로 ARP를 활성화한 경우 경고 메시지가 표시되고 ARP를 재구성해야 할 수 있습니다. "ARP를 되돌리는 방법에 대해 알아보십시오" .

ARP 활성화 옵션

ARP는 클러스터, SVM 및 볼륨 수준에서 유연한 활성화 옵션을 제공하므로 새 볼륨에 대해 자동 기본 활성화를 구성하거나 필요에 따라 기존 볼륨에서 ARP를 수동으로 활성화할 수 있습니다.

새 볼륨에서 자동 기본 활성화

ONTAP 9.18.1부터 AFF A 시리즈 및 AFF C 시리즈, ASA 및 ASA r2 시스템의 모든 새 볼륨에서 ARP가 기본적으로 자동으로 활성화됩니다. 이 자동 기본 ARP 활성화는 "지원되지 않는 볼륨 또는 구성"에는 적용되지 않습니다.

새 볼륨에 대한 ARP 기본 활성화는 업그레이드 후 12시간의 유예 기간이 지난 후에 적용되거나, ONTAP 9.18.1을 새로 설치하는 경우에는 ARP 라이센스가 설치되어 있으면 즉시 적용됩니다. 기존 볼륨에는 ARP를 수동으로 활성화합니다해야 합니다.

유예 기간 동안 "시스템 관리자 또는 ONTAP CLI를 사용하여 클러스터 수준에서 새 볼륨에 대한 기본 활성화를 해제할 수 있습니다.". 옵트아웃하지 않으면 유예 기간이 끝난 후 생성된 모든 새 볼륨에 대해 ARP가 자동으로 활성화됩니다. 유예 기간 후에 필요 사항이 변경되면 언제든지 기본 활성화 기능을 켜거나 끌 수 있습니다.

새 볼륨에서 수동 기본 활성화

클러스터 수준에서 ARP의 자동 기본 활성화를 비활성화한 경우 SVM 수준에서 "모든 새 볼륨에서 기본적으로 ARP를 수동으로 활성화합니다"를 선택할 수도 있습니다. ONTAP 9.17.1 이하 버전에서는 새 볼륨에서 ARP를 기본적으로 활성화하도록 구성하는 유일한 방법입니다.

기존 볼륨 전체 또는 특정 볼륨에 대한 **ARP** 활성화

9.18.1부터 클러스터 레벨에서 기존의 모든 볼륨에 대해 ARP를 수동으로 활성화할 수 있습니다(**Cluster > Security***를 선택하고 ***Anti-ransomware** 섹션에서 ⋮를 선택한 다음 *Enable on all existing volumes*를 선택).

특정 볼륨에 대해서만 ARP 활성화를 제한하려면 "볼륨별로 ARP를 활성화합니다"할 수 있습니다.

ONTAP 랜섬웨어 보호 전략

효과적인 랜섬웨어 보호를 위해서는 여러 보호 계층이 함께 작동해야 합니다.

ONTAP에는 랜섬웨어로부터 보호하기 위한 FPolicy, 스냅샷, SnapLock 및 Active IQ Digital Advisor(Digital Advisor라고도 함)와 같은 기능이 포함되어 있지만, ARP는 추가적인 방어 계층을 제공합니다.

랜섬웨어로부터 보호하는 NetApp 포트폴리오의 다른 기능에 대한 자세한 내용은 다음을 참조하십시오.

- "Ransomware 및 NetApp의 보호 포트폴리오"
- "PowerShell을 사용한 ONTAP 사이버 볼트 강화"

ARP가 감지하는 것

ONTAP ARP는 공격자가 몸값을 지불할 때까지 데이터를 은닉하는 서비스 거부(DoS) 공격으로부터 보호하도록 설계되었습니다. ARP는 다음을 기반으로 실시간 랜섬웨어 탐지 기능을 제공합니다.

- 수신 데이터를 암호화된 텍스트 또는 일반 텍스트로 식별합니다.
- 다음을 감지하는 분석:
  - 엔트로피: (NAS 및 SAN에서 사용됨) 파일 내 데이터의 무작위성 평가
  - 파일 확장자 유형: (NAS에서만 사용됨) 예상되는 확장자 유형에 맞지 않는 파일 확장자
  - 파일 **IOPS**: (ONTAP 9.11.1부터 NAS에서만 사용됨) 데이터 암호화로 인한 비정상적인 볼륨 활동 급증

ARP는 소수의 파일만 암호화된 후 대부분의 랜섬웨어 공격이 확산되는 것을 감지하고, 자동으로 대응하여 데이터를 보호하며, 의심되는 공격이 발생했을 때 경고합니다.

어떠한 랜섬웨어 탐지 시스템도 완전한 안전을 보장할 수 없습니다. ARP는 바이러스 백신 소프트웨어가 침입을 감지하지 못할 경우 추가적인 방어 계층을 제공합니다.

ARP 모드에 대해 알아보세요

볼륨에 대해 ARP가 활성화되면 기준선을 설정하기 위한 학습 기간에 들어갑니다. ARP는 활성 감지 모드로 전환하기 전에 시스템 메트릭을 분석하여 경고 프로필을 개발합니다. 활성 모드에서 ARP는 비정상적인 활동을 모니터링하고, 보호 조치를 취하고, 비정상적인 동작이 감지되면 경고를 생성합니다.

ARP의 경우 학습 모드와 활성 모드 동작은 ONTAP 버전, 볼륨 유형, 프로토콜(NAS 또는 SAN)에 따라 다릅니다.

NAS 환경 및 모드 유형

다음 표는 NAS 환경에서 ONTAP 9.10.1과 이후 버전 간의 차이점을 요약한 것입니다.

이전 ARP 모델이 적용된 버전에서는 활성 모니터링을 시작하기 전에 학습 기간을 두는 것이 좋습니다. 지원하는 NAS 환경의 경우ARP/AI 학습 기간이 없으며, 적극적인 모니터링이 즉시 시작됩니다.

방법	설명	볼륨 유형 및 버전
학습	ONTAP 의 특정 버전과 특정 볼륨 유형의 경우 ARP를 활성화하면 ARP가 자동으로 학습 모드로 설정됩니다. 학습 모드에서 ONTAP 시스템은 엔트로피, 파일 확장자 유형, 파일 IOPS 등의 분석 영역을 기반으로 경고 프로필을 개발합니다. ARP를 30일 동안 학습 모드로 유지하는 것이 좋습니다. ONTAP 9.13.1부터 ARP는 최적의 학습 간격을 자동으로 결정하고 전환을 자동화하며, 이는 30일 전에 실행될 수 있습니다. ONTAP 9.13.1 이전 버전에서는 수동으로 전환할 수 있습니다. FlexVol 볼륨의 ONTAP 9.16.1부터는 활성 모드만 존재하며, 이 버전 이상으로 업그레이드된 모든 FlexVol 볼륨의 경우 학습 모드가 자동으로 활성 모드로 전환됩니다. ONTAP 9.16.1~9.17.1의 경우 FlexGroup 볼륨은 아직 ARP/AI에서 지원되지 않으며 이전 ARP 모델을 계속 실행합니다. 이러한 이유로 FlexGroup 볼륨이 포함된 이러한 버전에는 여전히 학습 기간이 권장됩니다. ONTAP 9.18.1부터 FlexVol 및 FlexGroup 볼륨 모두에 대해 활성 모드만 존재합니다. 업그레이드된 볼륨은 자동으로 활성 모드로 전환됩니다. "학습 모드에서 활성 모드로 전환하는 방법에 대해 자세히 알아보세요." . 이 명령은 `security anti-ransomware volume workload-behavior show` 볼륨에서 감지된 파일 확장명을 표시합니다. 이 명령을 학습 모드 초기에 실행하면 파일 유형이 정확하게 표시되는 경우 ONTAP가 다른 메트릭을 수집하고 있으므로 해당 데이터를 활성 모드로 전환하기 위한 기준으로 사용해서는 안 됩니다. 에 대한 자세한 내용은 `security anti-ransomware volume workload-behavior show` "ONTAP 명령 참조입니다"을 참조하십시오.	• ONTAP 9.10.1~9.15.1을 사용한 FlexVol 볼륨 • ONTAP 9.13.1에서 ONTAP 9.17.1로의 FlexGroup 볼륨

방법	설명	볼륨 유형 및 버전
활동적인	활성 모드에서 파일 확장자가 비정상으로 표시되면 알림을 평가해야 합니다. 알림에 따라 조치를 취하여 데이터를 보호하거나, 알림을 오탐지로 표시할 수 있습니다. 알림을 오탐지로 표시하면 알림 프로필이 업데이트됩니다. 예를 들어, 새로운 파일 확장자로 인해 알림이 발생하고 해당 알림을 오탐지로 표시하면 다음에 해당 파일 확장자가 발견될 때 알림을 받지 않습니다.	지원되는 모든 ONTAP 버전과 FlexVol 및 FlexGroup 볼륨

SAN 환경 및 모드 유형

SAN 환경은 활성 감지 모드로 자동 전환되기 전에 평가 기간(NAS 환경의 학습 모드와 유사)을 사용합니다. 다음 표는 평가 모드와 활성 모드를 요약한 것입니다.

방법	설명	볼륨 유형 및 버전
평가	ARP/AI는 평가 기간 동안 SAN 볼륨에 대한 즉각적인 활성 보호 기능을 제공하는 반면, 기준 암호화 동작을 확인하기 위해 2~4주간의 평가 기간이 수행됩니다. 기준 임계값이 설정되는 동안에도 감지 및 경고가 발생할 수 있습니다. 평가 기간이 완료되었는지 확인하려면 다음을 실행하세요. `security anti-ransomware volume show` 명령 및 확인 `Block device detection status` . "SAN 볼륨 및 엔트로피 평가 기간에 대해 자세히 알아보세요." .	• ONTAP 9.17.1 이상을 사용한 FlexVol 볼륨
활동적인	평가 기간 후에 ARP SAN 보호가 활성화되었는지 확인하려면 다음을 실행하세요. `security anti-ransomware volume show` 명령 및 확인 `Block device detection status` . 상태 `Active_suitable_workload` 평가된 엔트로피 양을 성공적으로 모니터링할 수 있음을 나타냅니다. ARP는 평가 중에 검토된 데이터에 따라 적응 임계값을 자동으로 조정합니다.	• ONTAP 9.17.1 이상을 사용한 FlexVol 볼륨

위협 평가 및 ARP 스냅샷

ARP는 학습된 분석 데이터를 기반으로 수신되는 데이터를 측정하여 위협 발생 확률을 평가합니다. ARP는 이상 징후를 감지하면 측정값을 할당합니다. ARP는 감지 시점 또는 정기적인 간격으로 스냅샷을 할당할 수 있습니다.

ARP 임계값

- * Low * (낮음) *: 볼륨에서 비정상 상태를 가장 먼저 감지합니다(예: 볼륨에서 새 파일 확장자가 관찰됨). 이 감지 수준은 ARP/AI가 없는 ONTAP 9.16.1 이전 버전에서만 사용할 수 있습니다.
  - ONTAP 9.11.1부터 다음을 수행할 수 있습니다. "ARP에 대한 탐지 매개변수 사용자 정의" .
  - ONTAP 9.10.1에서 Moderate로 에스컬레이션하기 위한 임계값은 100개 이상의 파일입니다.
- 보통: 높은 엔트로피가 감지되거나 이전에는 발견되지 않았던 동일한 파일 확장자를 가진 파일이 여러 개 관찰됩니다. 이는 ARP/AI가 적용된 ONTAP 9.16.1 이상의 기본 감지 수준입니다.

ONTAP 에서 분석 보고서를 실행하여 이상 징후가 랜섬웨어 프로필과 일치하는지 확인한 후 위협 수준이 중간 수준으로 상승합니다. 공격 가능성이 중간 수준인 경우, ONTAP EMS 알림을 생성하여 위협을 평가하도록 안내합니다. ONTAP는 낮은 위협에 대한 경고를 전송하지 않지만 ONTAP 9.14.1부터는 다음을 수행할 수 있습니다"기본 알림 설정 수정". "비정상적인 활동에 응답합니다" .

System Manager의 * Events * 섹션 또는 명령을 사용하여 보통 수준의 위협에 대한 정보를 볼 수 `security anti-ransomware volume show` 있습니다. ARP/AI가 없는 ONTAP 9.16.1 이전 버전의 명령을 사용하여 낮은 위협 이벤트를 볼 수도 `security anti-ransomware volume show` 있습니다. 에 대한 자세한 내용은 `security anti-ransomware volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

ARP 스냅샷

ARP는 공격의 조기 징후가 감지되면 스냅샷을 만듭니다. 그런 다음 상세 분석을 수행하여 잠재적 공격을 확인하거나 차단합니다. ARP 스냅샷은 공격이 완전히 확인되기 전에도 사전에 생성되므로 특정 합법적인 애플리케이션의 경우 정기적으로 생성될 수도 있습니다. 이러한 스냅샷의 존재를 이상 현상으로 간주해서는 안 됩니다. 공격이 확인되면 공격 확률이 증가합니다. `Moderate` 공격 알림이 생성됩니다.

ONTAP 9.17.1부터 NAS 및 SAN 볼륨 모두에 대해 정기적으로 ARP 스냅샷이 생성되며 감지된 이상에 대한 대응으로도 ARP 스냅샷이 생성됩니다. ONTAP ARP 스냅샷에 이름을 추가하여 쉽게 식별할 수 있도록 합니다.

ONTAP 9.11.1부터 보존 설정을 수정할 수 있습니다. 자세한 내용은 다음을 참조하세요. "스냅샷 옵션을 수정합니다" .

다음 표는 버전별 ARP 스냅샷 차이점을 요약한 것입니다.

피처	**ONTAP 9.17.1** 이상	**ONTAP 9.16.1** 및 이전 버전
창조 트리거	• 스냅샷은 특정 트리거와 관계없이 고정된 4시간 간격으로 생성됩니다. • 공격 확인 트리거 유형에 따라 "주기적" 또는 "공격" 스냅샷이 생성됩니다.	• 높은 엔트로피가 감지되었습니다 • 새로운 파일 확장자가 감지되었습니다(9.15.1 및 이전 버전) • 파일 작업 급증이 감지되었습니다(9.15.1 및 이전 버전) 스냅샷 생성 간격은 트리거 유형에 따라 달라집니다.
접두사 이름 규칙	"안티랜섬웨어 정기 백업" "안티랜섬웨어 공격 백업"	"랜섬웨어 방지 백업"
삭제 동작	ARP 스냅샷이 잠겨 있어 관리자가 삭제할 수 없습니다.	ARP 스냅샷이 잠겨 있어 관리자가 삭제할 수 없습니다.
최대 스냅샷 수	"6개의 스냅샷 구성 가능 한도"	"6개의 스냅샷 구성 가능 한도"
보존 기간	스냅샷은 일반적으로 12시간 동안 보관됩니다. • NAS 볼륨: 파일 분석을 통해 공격이 확인되면 공격 전에 생성된 스냅샷은 관리자가 공격을 참으로 표시하거나 거짓 긍정(명확한 의심)으로 표시할 때까지 보관됩니다. • SAN 볼륨 또는 VM 데이터 저장소: 블록 엔트로피 분석을 통해 공격이 확인되면 공격 전에 생성된 스냅샷은 10일 동안 보관됩니다(구성 가능).	• 트리거 조건에 따라 결정됨(고정되지 않음) • 공격이 발생하기 전에 생성된 스냅샷은 관리자가 공격을 참으로 표시하거나 거짓 양성(명확한 의심)으로 표시할 때까지 보관됩니다.

피처	**ONTAP 9.17.1** 이상	**ONTAP 9.16.1** 및 이전 버전
명백한 의심 행위	관리자는 확인을 기준으로 보존 기간을 설정하는 명백한 의심 작업을 수행할 수 있습니다. • 24시간 동안 거짓 양성 보존 • 7일간의 True Positive 유지 기간	관리자는 확인을 기준으로 보존 기간을 설정하는 명백한 의심 작업을 수행할 수 있습니다. • 24시간 동안 거짓 양성 보존 • 7일간의 True Positive 유지 기간 이 예방적 보존 동작은 ONTAP 9.16.1 이전에는 존재하지 않았습니다.
만료 시간	모든 스냅샷에 만료 시간이 설정됩니다.	없음

랜섬웨어 공격 후 **ONTAP**에서 데이터를 복구하는 방법

ARP는 검증된 ONTAP 데이터 보호 및 재해 복구 기술을 기반으로 랜섬웨어 공격에 대응합니다. ARP는 공격의 조기 징후가 감지되면 잠긴 스냅샷을 생성합니다. 먼저 공격이 실제 공격인지 오탐지인지 확인해야 합니다. 공격이 확인되면 ARP 스냅샷을 사용하여 볼륨을 복원할 수 있습니다.

잠긴 스냅샷은 일반적인 방법으로는 삭제할 수 없습니다. 그러나 나중에 해당 공격을 오탐지로 표시하기로 결정하면 ONTAP 잠긴 사본을 삭제합니다.

전체 볼륨을 되돌리는 대신, 선택한 스냅샷에서 영향을 받은 파일을 복구할 수 있습니다.

공격에 대응하고 데이터를 복구하는 방법에 대한 자세한 내용은 다음 항목을 참조하세요.

- "비정상적인 활동에 응답합니다"
- "ARP 스냅샷에서 데이터 복구"
- "ONTAP 스냅샷에서 복구"
- "스마트 랜섬웨어 복구"

ARP에 대한 다중 관리자 인증 보호

ONTAP 9.13.1부터 ARP(자율 랜섬웨어 차단) 구성을 위해 인증된 사용자 관리자 2명 이상이 필요할 수 있도록 MAV(다중 관리자 검증)를 활성화하는 것이 좋습니다. 자세한 내용은 을 "다중 관리 검증을 활성화합니다"참조하십시오.

인공 지능**(ARP/AI)**을 이용한 자율적 랜섬웨어 방어

ONTAP 9.16.1부터 ARP는 NAS 환경에서 끊임없이 진화하는 랜섬웨어를 99% 정확도로 탐지하는 랜섬웨어 방지 분석용 머신 러닝 모델을 채택하여 사이버 복원력을 향상시킵니다. ARP의 머신 러닝 모델은 시뮬레이션된 랜섬웨어 공격 전후의 대용량 파일 데이터 세트를 기반으로 사전 학습됩니다. 이러한 리소스 집약적인 학습은 ONTAP 외부에서 오픈 소스 포렌식 연구 데이터 세트를 사용하여 모델을 학습시킵니다. 고객 데이터는 전체 모델링 파이프라인에 사용되지 않으며 개인정보 보호 문제는 발생하지 않습니다. 이 학습을 통해 생성된 사전 학습된 모델은 ONTAP 에 기본 제공됩니다. 이 모델은 ONTAP CLI 또는 ONTAP API를 통해 접근하거나 수정할 수 없습니다.

ARP/AI에 대한 능동적 보호로의 즉각적인 전환

ARP/AI를 사용하면학습 기간 . ARP/AI는 다음 지원되는 볼륨 유형에 대해 설치 또는 업그레이드 직후에 활성화됩니다.

- ONTAP 9.16.1 이상을 사용한 NAS FlexVol 볼륨

- ONTAP 9.18.1 이상을 사용한 NAS FlexGroup 볼륨
- ONTAP 9.17.1 이상을 사용하는 SAN 볼륨(즉시 활성화됨,"평가 기간")

ARP 기능이 이미 활성화된 기존 볼륨과 새 볼륨의 경우, 클러스터를 ARP/AI 지원 ONTAP 버전으로 업그레이드하면 ARP/AI 보호가 자동으로 활성화됩니다.

ARP/AI 자동 업데이트

최신 보안을 유지하기 위해 ARP/AI는 정기적인 ONTAP 업그레이드 및 릴리스 주기 외에도 빈번하게 자동 업데이트를 제공합니다. "자동 업데이트를 활성화했습니다" 보안 파일에 대한 자동 업데이트를 선택하면 ARP/AI에 대한 자동 보안 업데이트를 받을 수 있습니다. 또한 다음 을 선택할 수도 있습니다. "이 업데이트를 수동으로 만드세요" 업데이트가 발생하는 시기를 제어합니다.

ONTAP 9.16.1부터 시스템 및 펌웨어 업데이트 외에 ARP/AI용 보안 업데이트를 System Manager를 사용하여 사용할 수 있습니다.

"ARP/AI 업데이트에 대해 자세히 알아보십시오"

ARP/AI 모델과 **ARP** 모델의 차이점 개요

피처	아프	**ARP/AI**
ONTAP 버전	ONTAP 9.10.1-9.15.1	ONTAP 9.16.1 이상, 9.15.1(기술 미리 보기)
감지 방법	파일 활동, 데이터 엔트로피 및 파일 확장자 유형을 분석합니다	대규모 포렌식 데이터 세트로 학습된 AI/머신 러닝 모델, 엔트로피 및 파일 동작 분석
학습 기간	NAS FlexVol 볼륨의 경우 30일 학습 모드가 필요합니다(자동 전환 기능은 9.13.1 이상 버전에서 사용 가능)	학습 기간 없음, 활성화 즉시 활성화됩니다.
볼륨 유형 지원	• FlexVol: 9.10.1 이상 • FlexGroup: 9.13.1 이상 • SAN: 지원되지 않음	• FlexVol: 9.16.1 이상 • FlexGroup: 9.18.1 이상 • SAN: 9.17.1 이상(평가 기간 포함)
스냅샷 생성	높은 엔트로피, 새로운 파일 확장자 또는 파일 작업 급증으로 인해 트리거됩니다.	고정된 4시간 간격으로 생성되며 공격 확인 시에도 생성됩니다
스냅샷 보존	관리자가 의심스러운 활동을 지울 때까지 보관됩니다.	기본값은 12시간이며, 공격 확인 여부에 따라 연장됩니다(오탐의 경우 24시간, 확인된 공격의 경우 7일)
업데이트	정적 감지 로직(ONTAP 업그레이드에 한해서만 업데이트됨)	ONTAP 릴리스와 관계없이 자동 보안 업데이트가 제공됩니다.
구축	볼륨별 수동 활성화 또는 SVM 레벨 기본 설정	볼륨별 수동 활성화 또는 SVM 수준의 기본 설정, 9.18.1 이상에서 지원되는 시스템의 경우 클러스터 수준에서 모든 새 볼륨에 대한 기본 활성화

피처	아프	**ARP/AI**
평가 기간	해당 없음	기준 암호화 임계값을 설정하기 위해 SAN 볼륨에 필요(2~4주)

관련 정보

- "ONTAP 명령 참조입니다"

ONTAP 자율적 랜섬웨어 방어 사용 사례 및 고려사항

자율형 랜섬웨어 보호(ARP)는 ONTAP 9.10.1부터 NAS 워크로드와 ONTAP 9.17.1부터 SAN 워크로드에 사용할 수 있습니다. ARP를 구축하기 전에 권장되는 용도와 지원되는 구성, 그리고 성능에 미치는 영향을 파악해야 합니다.

지원 구성 및 지원되지 않는 구성

ARP를 사용하도록 결정할 때 볼륨의 워크로드가 ARP에 적합하고 필요한 시스템 구성을 충족하는지 확인하는 것이 중요합니다.

적합한 워크로드

ARP는 다음 유형의 작업 부하에 적합합니다.

- NFS 또는 SAN 스토리지의 데이터베이스
- Windows 또는 Linux 홈 디렉토리

  ARP/AI가 없는 환경에서는 사용자가 학습 기간 동안 감지되지 않은 확장자를 가진 파일을 생성할 수 있습니다. 이로 인해 이 워크로드에서 오탐지(false positive)가 발생할 가능성이 더 높습니다.

- 이미지 및 비디오

  예: 의료 기록 및 전자 설계 자동화(EDA) 데이터

부적합한 워크로드

ARP는 다음 유형의 작업 부하에 적합하지 않습니다.

- 파일 생성 또는 삭제 작업 빈도가 높은 작업(몇 초 안에 수십만 개의 파일 생성, 예: 테스트/개발 작업)
- ARP의 위협 탐지는 파일 생성, 이름 변경 또는 삭제 작업의 비정상적인 급증을 인식하는 능력에 달려 있습니다. 애플리케이션 자체가 파일 활동의 근원인 경우, 랜섬웨어 활동과 효과적으로 구별할 수 없습니다.
- 애플리케이션이나 호스트가 데이터를 암호화하는 작업 부하.

  ARP는 수신 데이터를 암호화된 데이터와 암호화되지 않은 데이터로 구분하는 데 의존합니다. 애플리케이션 자체에서 데이터를 암호화하는 경우 이 기능의 효과가 감소합니다. 그러나 ARP는 파일 활동(삭제, 덮어쓰기, 생성 또는 새 파일 확장자로 생성 또는 이름 변경) 및 파일 유형에 따라 여전히 작동할 수 있습니다.

지원되는 구성

ONTAP 9.10.1부터 NAS, NFS 및 SMB FlexVol 볼륨에 ARP를 사용할 수 있습니다. 9.17.1부터 SAN 스토리지를

사용하는 iSCSI, FC 및 NVMe용 SAN FlexVol 볼륨에 ARP를 사용할 수 있습니다.

ARP는 ONTAP 9.10.1부터 MetroCluster 구성에서 지원됩니다.

다른 구성 및 볼륨 유형에 대한 지원은 다음 ONTAP 버전에서 제공됩니다.

	ONTAP 9.18.1	ONTAP 9.17.1	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
SnapMirror 비동기로 보호되는 볼륨	✓	✓	✓	✓	✓	✓	✓		
SnapMirror 비동기(SVM 재해 복구)를 통해 SVM 보호	✓	✓	✓	✓	✓	✓	✓		
SVM 데이터 이동성(`vserver migrate`)	✓	✓	✓	✓	✓	✓	✓		
FlexGroup 볼륨[1]	✓	✓	✓	✓	✓	✓			
다중 관리 검증	✓	✓	✓	✓	✓				
ARP/AI 및 자동 업데이트	✓	✓							
ARP/AI 기본 활성화[2]	✓								

[1] ONTAP 9.16.1 및 9.17.1은 FlexGroup 볼륨에 대한 ARP/AI 지원을 제공하지 않습니다. 이러한 버전으로 업그레이드한 후에도 ARP에 대해 활성화된 FlexGroup 볼륨은 ARP/AI 이전에 사용된 것과 동일한 ARP 모델로 계속 작동합니다. ONTAP 9.18.1부터 FlexGroup 볼륨은 ARP/AI 모델을 사용합니다.

[2] ONTAP 9.18.1부터 AFF A 시리즈 및 AFF C 시리즈, ASA 및 ASA r2 시스템에 대해 ARP/AI 기본 활성화 동작이 제공됩니다. 이 동작은 업그레이드 후 12시간의 유예 기간이 지난 후 또는 ONTAP 9.18.1을 새로 설치하는 경우 즉시 모든 새 볼륨에서 ARP/AI를 자동으로 활성화합니다. "기존 볼륨"에서 ARP를 수동으로 활성화해야 합니다.

SnapMirror 및 **ARP** 상호 운용성

ONTAP 9.12.1부터 SnapMirror 비동기 대상 볼륨에서 ARP가 지원됩니다. SnapMirror 동기식 또는 SnapMirror 활성 동기화에서는 ARP가 지원되지 않습니다.

SnapMirror 소스 볼륨이 ARP를 지원하는 경우 SnapMirror 대상 볼륨은 자동으로 ARP 구성 상태(예: `dry-run` 또는 `enabled`), ARP 교육 데이터 및 ARP에서 생성한 소스 볼륨의 스냅샷. 명시적인 활성화는 필요하지 않습니다.

대상 볼륨은 읽기 전용(RO) 스냅샷으로 구성되지만, 해당 데이터에 대한 ARP 처리는 수행되지 않습니다. 그러나 SnapMirror 대상 볼륨이 읽기-쓰기(RW)로 변환되면 RW로 변환된 대상 볼륨에서 ARP가 자동으로 활성화됩니다. 대상 볼륨은 소스 볼륨에 이미 기록된 내용 외에 추가적인 학습 절차를 필요로 하지 않습니다.

ONTAP 9.10.1 및 9.11.1에서 SnapMirror ARP 구성 상태, 학습 데이터 및 스냅샷을 소스 볼륨에서 대상 볼륨으로 전송하지 않습니다. 따라서 SnapMirror 대상 볼륨을 RW로 변환할 때, 변환 후 학습 모드에서 대상 볼륨의 ARP를 명시적으로 활성화해야 합니다.

ARP 및 가상 머신

ARP는 VMware의 가상 머신(VM)에서 지원됩니다. ARP 감지는 VM 내부와 외부의 변경 사항에 대해 다르게 작동합니다. VM 내에서 많은 양의 고압축 파일(예: 7z 및 ZIP)이나 암호화된 파일(예: 암호로 보호된 PDF, DOC 또는 ZIP)이 포함된 작업에는 ARP를 권장하지 않습니다.

VM 외부의 변경 사항

ARP는 암호화된 상태로 볼륨에 새로운 확장자가 들어오거나 파일 확장자가 변경되는 경우 VM 외부의 NFS 볼륨에서 파일 확장자 변경을 감지할 수 있습니다.

VM 내부의 변경 사항

랜섬웨어 공격으로 VM 외부는 변경하지 않고 VM 내부의 파일만 변경되는 경우, ARP는 VM의 기본 엔트로피가 낮을 경우(예: .txt, .docx 또는 .mp4 파일) 위협을 감지합니다. ONTAP 9.16.1 이하 버전에서는 ARP가 이 시나리오에서 보호 스냅샷을 생성하지만 VM 외부의 파일 확장자가 변경되지 않았으므로 위협 경고를 생성하지 않습니다. ONTAP 9.17.1의 SAN 지원 버전부터 ARP는 VM 내부에서 엔트로피 이상을 감지할 경우 위협 경고를 추가로 생성합니다.

기본적으로 파일이 높은 엔트로피(예: .gzip 또는 암호로 보호된 파일)인 경우 ARP의 탐지 기능이 제한됩니다. 이 경우에도 ARP는 사전 스냅샷을 생성할 수 있습니다. 단, 파일 확장자가 외부에서 변경되지 않은 경우 경고는 발생하지 않습니다.

SAN의 경우 ARP는 볼륨 수준에서 엔트로피 통계를 분석하고 엔트로피 이상이 발견되면 감지를 트리거합니다.

> VM 내에서 발생하는 공격을 감지하는 기능은 FlexVol 볼륨에서만 사용할 수 있으며 ONTAP 9.18.1 이상에서 FlexGroup 볼륨에 VM 데이터 저장소가 구성된 경우에는 사용할 수 없습니다.

지원되지 않는 구성입니다

ONTAP S3 환경에서는 ARP가 지원되지 않습니다.

ARP는 다음 볼륨 구성을 지원하지 않습니다.

- FlexGroup 볼륨(ONTAP 9.10.1~9.12.1).

> ONTAP 9.13.1부터 ONTAP 9.17.1까지 FlexGroup 볼륨이 지원되지만 ARP/AI 이전에 사용된 ARP 모델로 제한됩니다. FlexGroup 볼륨은 ONTAP 9.18.1부터 ARP/AI에서 지원됩니다.

- FlexCache 볼륨(ARP는 오리진 FlexVol 볼륨에서 지원되지만 캐시 볼륨에서는 지원되지 않음)
- 오프라인 볼륨
- SnapLock 볼륨

- SnapMirror 활성 동기화
- SnapMirror 동기식
- SnapMirror 비동기식(ONTAP 9.10.1 및 9.11.1). SnapMirror 비동기식은 ONTAP 9.12.1부터 지원됩니다. 자세한 내용은 다음을 참조하세요. SnapMirror를 참조하십시오 .
- 제한된 볼륨
- 스토리지 VM의 루트 볼륨입니다
- 중지된 스토리지 VM의 볼륨입니다

ARP 성능 및 주파수 고려 사항

ARP는 처리량과 최대 IOPS로 측정했을 때 시스템 성능에 미치는 영향이 미미할 수 있습니다. ARP 기능의 영향은 특정 볼륨 워크로드에 따라 다릅니다. 일반적인 워크로드의 경우 다음과 같은 구성 제한을 권장합니다.

워크로드 특성	노드당 권장 볼륨 제한입니다	노드당 볼륨 제한을 초과하면 성능이 저하됩니다 [1]
읽기 집약적이거나 데이터를 압축할 수 있습니다.	150	최대 IOPS의 4%
쓰기 집약적이며 데이터를 압축할 수 없습니다.	60	• NAS: ONTAP 9.15.1 및 이전 버전의 경우 최대 IOPS의 10% • NAS: ONTAP 9.16.1 이상 버전의 경우 최대 IOPS의 5% • SAN: ONTAP 9.17.1 이상의 경우 최대 IOPS의 5%

[1] 권장 한도를 초과하여 볼륨을 추가하더라도 이러한 백분율을 넘으면 시스템 성능이 저하되지 않습니다.

ARP 분석은 우선순위에 따라 실행되므로 보호된 볼륨 수가 늘어날수록 각 볼륨에서 분석이 실행되는 빈도가 줄어듭니다.

대량의 새 볼륨에 대해 ARP를 기본적으로 활성화하면 시스템 리소스 사용량이 증가할 수 있습니다. 볼륨에서 ARP를 활성화할 때는 스냅샷과 같은 경쟁 프로세스의 공간 요구 사항을 고려하십시오.

플랫폼별 **ARP**의 볼륨 제한

ONTAP 9.18.1부터 ARP는 플랫폼 유형 및 CPU 코어 개수를 기반으로 증가된 볼륨 제한을 지원합니다.

플랫폼 유형	노드당 최대 **ARP** 지원 볼륨
로우엔드(CPU 코어 수가 최대 20개인 시스템)	250
중급(최대 64개의 CPU 코어가 있는 시스템)	500입니다
고급형(CPU 코어 개수가 64개 이상인 시스템)	1000입니다

CPU 코어 개수는 2노드 HA 쌍의 각 개별 노드에 적용됩니다.

ARP로 보호되는 볼륨을 사용한 다중 관리자 검증

ONTAP 9.13.1 부터는 ARP를 통한 추가 보안을 위해 MAV(Multi-admin verification)를 활성화할 수 있습니다. MAV를 사용하면 최소한 두 명 이상의 인증된 관리자가 ARP를 끄거나 ARP를 일시 중지하거나 의심스러운 공격을 보호된 볼륨에서 위양성(false positive)으로 표시해야 합니다. 의 방법을 "ARP 보호 볼륨에 대해 MAV를 활성화합니다 "알아보십시오.

MAV 그룹에 대한 관리자를 정의하고, `security anti-ransomware volume pause`, 및 `security anti-ransomware volume attack clear-suspect` 보호할 ARP 명령에 대한 MAV 규칙을 `security anti-ransomware volume disable` 만들어야 합니다. MAV 그룹의 각 관리자는 MAV 설정 내에서 각각의 새 규칙 요청을 승인해야 "MAV 규칙을 다시 추가합니다"합니다.

에 대한 자세한 `security anti-ransomware volume disable` `security anti-ransomware volume pause` 내용은, 및 `security anti-ransomware volume attack clear-suspect`"ONTAP 명령 참조입니다" 을 참조하십시오.

ONTAP 9.14.1부터 ARP는 ARP 스냅샷 생성 및 새 파일 확장자 관찰에 대한 알림을 제공합니다. 이러한 이벤트에 대한 알림은 기본적으로 비활성화되어 있습니다. 알림은 볼륨 또는 SVM 수준에서 설정할 수 있습니다. 사용하여 알림을 활성화할 수 있습니다. `security anti-ransomware vserver event-log modify` 또는 볼륨 수준에서 `security anti-ransomware volume event-log modify` .

및 `security anti-ransomware volume event-log modify` 에 대한 자세한 `security anti-ransomware vserver event-log modify` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

다음 단계

- "자율주행 랜섬웨어 보호 활성화"
- "ARP로 보호되는 볼륨에 대해 MAV를 활성화합니다"

ARP 활성화

볼륨에서 **ONTAP** 자율형 랜섬웨어 보호 기능을 활성화합니다

ONTAP 9.10.1부터 기존 볼륨에서 ARP(자율적 랜섬웨어 방어)를 활성화하거나 새 볼륨을 생성한 후 처음부터 ARP를 활성화할 수 있습니다.

이 작업에 대해

ARP를 활성화하려면 환경에 맞는 절차를 따르십시오.귀하의 환경이 특정 요구 사항을 충족하는지 확인하십시오. :

- FlexVol 볼륨이 있는 NAS
- FlexGroup 볼륨이 있는 NAS
- SAN 볼륨

ARP를 활성화한 후 환경과 ONTAP 버전에 따라 ARP가 전환 기간에 들어갈 수 있습니다.

볼륨 유형입니다	**ONTAP** 버전입니다	활성화 후의 동작
NAS FlexGroup	ONTAP 9.18.1 이상	ARP/AI는 학습 기간 없이 즉시 활성화됩니다.
	ONTAP 9.13.1부터 9.17.1까지	ARP는 30일 동안 학습 모드로 시작됩니다.

볼륨 유형입니다	**ONTAP** 버전입니다	활성화 후의 동작
NAS FlexVol	ONTAP 9.16.1 이상	ARP/AI는 학습 기간 없이 즉시 활성화됩니다.
	ONTAP 9.10.1부터 9.15.1까지	ARP는 30일 동안 학습 모드로 시작됩니다.
SAN 볼륨	ONTAP 9.17.1 이상	ARP/AI는 즉시 활성화되어 초기 보수적 임계값에서 전환하기 전에 적절한 경고 임계값을 설정하기 위한 평가 기간을 시작합니다.

시작하기 전에

ARP를 활성화하기 전에 환경에 다음 사항이 있는지 확인하세요.

NAS 특정 요구 사항

- NFS 또는 SMB(또는 둘 다) 프로토콜이 활성화된 스토리지 VM(SVM)입니다.
- 클라이언트가 구성된 NAS 작업 부하.
- 활동적인"접합 경로" 볼륨을 위해서.

SAN 특정 요구 사항

- iSCSI, FC 또는 NVMe 프로토콜이 활성화된 스토리지 VM(SVM).
- 클라이언트가 구성된 SAN 워크로드.

일반 요구 사항

- 그만큼"올바른 라이센스입니다" ONTAP 버전용입니다.
- (권장) 다중 관리자 검증(MAV)이 활성화되어 있습니다(ONTAP 9.13.1 이상). 보다"다중 관리 검증을 활성화합니다" .

NAS FlexVol 볼륨에서 **ARP** 활성화

System Manager나 ONTAP CLI를 사용하여 NAS FlexVol 볼륨에서 ARP를 활성화할 수 있습니다. 해당 프로세스는 ONTAP 버전에 따라 다릅니다.

ONTAP 9.16.1 이상

ONTAP 9.16.1부터 ARP/AI는 학습 기간 없이 즉시 활성화됩니다.

시스템 관리자

1. 스토리지 > 볼륨 * 을 선택한 다음 보호할 볼륨을 선택합니다.
2. 볼륨 * 개요의 * 보안 * 탭에서 * 상태 * 를 선택하여 비활성화에서 활성화로 전환합니다.
3. 랜섬웨어 방지 상자에서 볼륨의 ARP 상태를 확인하세요.

   모든 볼륨에 대한 ARP 상태를 표시하려면 * Volumes * 창에서 * Show/Hide * 를 선택한 다음 * Anti-Ransomware * 상태가 선택되어 있는지 확인합니다.

CLI를 참조하십시오

기존 볼륨에서 **ARP** 활성화**:**

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

ARP가 활성화된 새 볼륨을 만듭니다**.**

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state enabled -junction-path
</path_name>
```

ARP 상태 확인**:**

```
security anti-ransomware volume show
```

에 대한 자세한 내용은 `security anti-ransomware volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 9.10.1부터 **9.15.1**까지

ONTAP 9.10.1~9.15.1의 경우 처음에 ARP를 활성화해야 합니다."학습 모드" (또는 "테스트 실행" 상태). 시스템은 작업 부하를 분석하여 정상적인 동작을 특성화합니다. 활성 모드에서 시작하면 과도한 오탐지 보고가 발생할 수 있습니다.

ARP를 최소 30일 동안 학습 모드로 실행하는 것이 좋습니다. ONTAP 9.13.1부터 ARP는 최적의 학습 기간 간격을 자동으로 결정하고 전환을 자동화하며, 이는 30일 전에 실행될 수 있습니다.

시스템 관리자

1. 스토리지 > 볼륨 * 을 선택한 다음 보호할 볼륨을 선택합니다.
2. 볼륨 * 개요의 * 보안 * 탭에서 * 상태 * 를 선택하여 비활성화에서 활성화로 전환합니다.
3. 랜섬웨어 방지 상자에서 *학습 모드에서 활성화*를 선택합니다.

당신은 할 수 있습니다"연관된 스토리지 VM에서 자동 학습을 활성 모드로 전환하는 것을 비활성화합니다." 학습 모드에서 활성 모드로의 전환을 수동으로 제어하려는 경우.

기존 볼륨에서 학습 및 활성 모드는 볼륨의 기존 데이터가 아닌 새로 기록된 데이터에만 적용됩니다. ARP에 대해 볼륨이 활성화된 후 새 데이터를 기반으로 이전 일반 데이터 트래픽의 특성이 가정되기 때문에 기존 데이터는 스캔되고 분석되지 않습니다.

4. 랜섬웨어 방지 상자에서 볼륨의 ARP 상태를 확인하세요.

   모든 볼륨에 대한 ARP 상태를 표시하려면 * Volumes * 창에서 * Show/Hide * 를 선택한 다음 * Anti-Ransomware * 상태가 선택되어 있는지 확인합니다.

CLI를 참조하십시오

기존 볼륨에서 **ARP** 활성화**:**

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver
<svm_name>
```

에 대한 자세한 내용은 `security anti-ransomware volume dry-run` "ONTAP 명령 참조입니다"을 참조하십시오.

ARP가 활성화된 새 볼륨을 만듭니다**.**

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state dry-run -junction-path
</path_name>
```

자동 전환 비활성화**(**선택 사항**):**

ONTAP 9.13.1부터 ONTAP 9.15.1까지 업그레이드하고 연관된 모든 볼륨에 대해 학습 모드에서 활성 모드로의 전환을 수동으로 제어하려는 경우 SVM에서 다음 작업을 수행할 수 있습니다.

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

ARP 상태 확인**:**

```
security anti-ransomware volume show
```

NAS FlexGroup 볼륨에서 ARP 활성화

System Manager나 ONTAP CLI를 사용하여 NAS FlexGroup 볼륨에서 ARP를 활성화할 수 있습니다. 해당 프로세스는 ONTAP 버전에 따라 다릅니다.

ONTAP 9.18.1 이상

ONTAP 9.18.1부터 ARP/AI는 학습 기간이 필요 없이 FlexGroup 볼륨에 대해 즉시 활성화됩니다.

시스템 관리자

1. *저장소 > 볼륨*을 선택한 다음 보호하려는 FlexGroup 볼륨을 선택합니다.
2. 볼륨 * 개요의 * 보안 * 탭에서 * 상태 * 를 선택하여 비활성화에서 활성화로 전환합니다.
3. 랜섬웨어 방지 상자에서 볼륨의 ARP 상태를 확인하세요.

   모든 볼륨에 대한 ARP 상태를 표시하려면 * Volumes * 창에서 * Show/Hide * 를 선택한 다음 * Anti-Ransomware * 상태가 선택되어 있는지 확인합니다.

CLI를 참조하십시오

기존 **FlexGroup** 볼륨에서 **ARP** 활성화**:**

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

ARP가 활성화된 새로운 **FlexGroup** 볼륨을 만듭니다**.**

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti
-ransomware-state enabled -junction-path </path_name>
```

ARP 상태 확인**:**

```
security anti-ransomware volume show
```

ONTAP 9.13.1부터 **9.17.1**까지

ONTAP 9.13.1~9.17.1의 경우 FlexGroup 볼륨은 다음에서 시작됩니다."학습 모드" . 시스템은 작업 부하를 분석하여 정상적인 동작을 특성화합니다.

ARP를 최소 30일 동안 학습 모드로 실행하는 것이 좋습니다. ARP는 최적의 학습 기간 간격을 자동으로 결정하고 30일 전에 전환이 자동화될 수 있습니다.

시스템 관리자

1. *저장소 > 볼륨*을 선택한 다음 보호하려는 FlexGroup 볼륨을 선택합니다.
2. 볼륨 * 개요의 * 보안 * 탭에서 * 상태 * 를 선택하여 비활성화에서 활성화로 전환합니다.
3. 랜섬웨어 방지 상자에서 *학습 모드에서 활성화*를 선택합니다.

당신은 할 수 있습니다"자동 학습에서 활성 모드로의 전환 비활성화" 학습 모드에서 활성 모드로의 전환을 수동으로 제어하려는 경우.

4. 랜섬웨어 방지 상자에서 볼륨의 ARP 상태를 확인하세요.

CLI를 참조하십시오

기존 **FlexGroup** 볼륨에서 **ARP** 활성화**:**

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver
<svm_name>
```

ARP가 활성화된 새로운 **FlexGroup** 볼륨을 만듭니다**.**

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti
-ransomware-state dry-run -junction-path </path_name>
```

자동 전환 비활성화(선택 사항)**:**

학습 모드에서 활성 모드로의 전환을 수동으로 제어하려면 다음을 수행하세요.

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

ARP 상태 확인**:**

```
security anti-ransomware volume show
```

SAN 볼륨에서 ARP 활성화

ONTAP 9.17.1부터 SAN 볼륨에서 ARP를 활성화할 수 있습니다. ARP/AI 기능은 자동으로 활성화되며 SAN 볼륨을 적극적으로 모니터링하고 보호하기 시작합니다."평가 기간" 동시에 워크로드가 ARP에 적합한지 확인하고 감지를 위한 최적의 암호화 임계값을 설정합니다.

System Manager나 ONTAP CLI를 사용하여 SAN 볼륨에서 ARP를 활성화할 수 있습니다.

시스템 관리자

단계

1. *저장소 > 볼륨*을 선택한 다음 보호하려는 SAN 볼륨을 선택합니다.
2. 볼륨 * 개요의 * 보안 * 탭에서 * 상태 * 를 선택하여 비활성화에서 활성화로 전환합니다.
3. ARP/AI는 자동으로 평가 기간에 들어갑니다.
4. 랜섬웨어 방지 상자에서 ARP 상태와 평가 상태를 확인하세요.

   모든 볼륨에 대한 ARP 상태를 표시하려면 * Volumes * 창에서 * Show/Hide * 를 선택한 다음 * Anti-Ransomware * 상태가 선택되어 있는지 확인합니다.

CLI를 참조하십시오

기존 **SAN** 볼륨에서 **ARP** 활성화**:**

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

ARP가 활성화된 새 **SAN** 볼륨을 만듭니다**.**

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state enabled
```

ARP 상태 및 평가 상태 확인**:**

```
security anti-ransomware volume show
```

확인하다 `Block device detection status` 평가 기간 진행 상황을 모니터링하는 필드입니다.

에 대한 자세한 내용은 `security anti-ransomware volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "학습 기간 후 활성 모드로 전환합니다"

새 볼륨에서 **ONTAP** 자율적 랜섬웨어 방어 기능을 기본적으로 활성화합니다

ONTAP 9.10.1부터 스토리지 VM(SVM)을 구성하여 새 볼륨이 Autonomous Ransomware Protection(ARP)으로 기본적으로 설정되도록 할 수 있습니다. System Manager 또는 ONTAP CLI를 사용하여 이 설정을 수정할 수 있습니다.

ONTAP 9.18.1부터 클러스터 업그레이드 또는 새 설치 후 12시간의 유예 기간이 지나면 "지원되는 시스템"에 대해 클러스터 수준에서 모든 새 볼륨에 대해 ARP가 기본적으로 활성화됩니다. 클러스터 수준에서 ARP의 자동 기본

활성화를 비활성화하더라도 SVM 수준에서 모든 새 볼륨에 대해 ARP를 수동으로 기본적으로 활성화하도록 선택할 수 있습니다.

ONTAP 9.17.1 이하 버전에서는 SVM 수준에서 구성하는 것이 새 볼륨에서 ARP를 기본적으로 활성화하는 유일한 방법입니다.

이 작업에 대해

기본적으로 새 볼륨은 ARP 기능이 비활성화된 상태로 생성됩니다. SVM에서 생성된 새 볼륨에서 기본적으로 ARP 기능을 활성화하고 활성화되도록 설정해야 합니다.

ARP가 활성화되지 않은 기존 볼륨은 SVM의 기본값을 변경해도 ARP 활성화 상태가 자동으로 변경되지 않습니다. 이 절차에 설명된 SVM 설정 변경 사항은 새 볼륨에만 영향을 미칩니다. 방법을 배우십시오"기존 볼륨에 대해 ARP를 활성화합니다" .

ARP를 활성화한 후 환경과 ONTAP 버전에 따라 ARP가 전환 기간에 들어갈 수 있습니다.

볼륨 유형입니다	**ONTAP** 버전입니다	활성화 후의 동작
NAS FlexGroup	ONTAP 9.18.1 이상	ARP/AI는 학습 기간 없이 즉시 활성화됩니다.
	ONTAP 9.13.1부터 9.17.1까지	ARP는 30일 동안 학습 모드로 시작됩니다.
NAS FlexVol	ONTAP 9.16.1 이상	ARP/AI는 학습 기간 없이 즉시 활성화됩니다.
	ONTAP 9.10.1부터 9.15.1까지	ARP는 30일 동안 학습 모드로 시작됩니다.
SAN 볼륨	ONTAP 9.17.1 이상	ARP/AI는 즉시 활성화되어 초기 보수적 임계값에서 전환하기 전에 적절한 경고 임계값을 설정하기 위한 평가 기간을 시작합니다.

시작하기 전에

ARP를 활성화하기 전에 환경에 다음 사항이 있는지 확인하세요.

NAS 특정 요구 사항

- NFS 또는 SMB(또는 둘 다) 프로토콜이 활성화된 스토리지 VM(SVM)입니다.
- 활동적인"접합 경로" 볼륨을 위해서.

SAN 특정 요구 사항

- iSCSI, FC 또는 NVMe 프로토콜이 활성화된 스토리지 VM(SVM).

일반 요구 사항

- 그만큼"올바른 라이센스입니다" ONTAP 버전용입니다.
- (권장) 다중 관리자 검증(MAV)이 활성화되었습니다(ONTAP 9.13.1+). 보다"다중 관리 검증을 활성화합니다" .

단계

시스템 관리자 또는 ONTAP CLI를 사용하여 새 볼륨에 대해 기본적으로 ARP를 활성화할 수 있습니다.

시스템 관리자

1. 환경에 따라 저장소 또는 *클러스터*를 선택하고, *저장소 VM*을 선택한 다음 ARP로 보호하려는 볼륨이 포함된 저장소 VM을 선택합니다.
2. 설정 탭으로 이동합니다. 보안*에서 *랜섬웨어 방지 타일을 찾아 선택합니다. .
3. 랜섬웨어 방지(ARP)를 활성화하려면 확인란을 선택하세요. 스토리지 VM의 모든 적격 볼륨에서 ARP를 활성화하려면 추가 확인란을 선택하세요.
4. 권장 학습 기간이 있는 ONTAP 버전의 경우, *충분한 학습 후 학습 모드에서 활성 모드로 자동 전환*을 선택하세요. 이를 통해 ARP가 최적의 학습 기간 간격을 결정하고 활성 모드로 자동 전환할 수 있습니다.

CLI를 참조하십시오

새 볼륨에서 기본적으로 **ARP**를 활성화하도록 기존 **SVM** 수정

선택하다 `dry-run` ARP 버전에 다음이 필요한 경우학습 기간 . 그렇지 않으면 선택하십시오 `enabled` .

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume
-state <dry-run|enabled>
```

새 볼륨에 대해 기본적으로 **ARP**가 활성화된 새 **SVM**을 만듭니다.

선택하다 `dry-run` ARP 버전에 다음이 필요한 경우학습 기간 . 그렇지 않으면 선택하십시오 `enabled` .

```
vserver create -vserver <svm_name> -anti-ransomware-default-volume
-state <dry-run|enabled>
```

기존 **SVM**을 수정하여 자동 학습을 활성 모드로 전환하지 않도록 합니다.

ONTAP 9.15.1을 통해 ONTAP 9.13.1로 업그레이드했고 기본 상태가 다음과 같은 경우 `dry-run` (학습모드)에서는 적응학습이 활성화되어 변경이 가능합니다. `enabled` 상태(활성 모드)는 자동으로 수행됩니다. 이 자동 스위치를 비활성화하면 연관된 모든 볼륨에 대해 학습 모드에서 활성 모드로의 전환을 수동으로 제어할 수 있습니다.

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

ARP 상태 확인

```
security anti-ransomware volume show
```

관련 정보

- "학습 기간 후 활성 모드로 전환합니다"
- "보안 랜섬웨어 볼륨 보기"

ONTAP 9.18.1부터 ARP 라이센스가 설치되어 있는 경우 업그레이드 또는 새로 설치한 후 12시간의 워밍업 기간이 지나면 AFF A-series 및 AFF C-series, ASA, ASA r2 시스템의 모든 새 볼륨에서 ARP(Autonomous Ransomware Protection)가 기본적으로 자동으로 활성화됩니다. System Manager 또는 ONTAP CLI를 사용하여 12시간 유예 기간 중 또는 이후에 이 기본 활성화를 해제할 수 있습니다.

기존 볼륨은 ARP용 "수동으로 활성화됨"이어야 합니다.

이 작업에 대해

이 절차에 대해 선택한 설정은 나중에 변경할 수 있습니다. 유예 기간 이후에는 언제든지 기본 활성화 기능을 켜거나 끌 수 있습니다.

```
security anti-ransomware auto-enable modify -new-volume-auto-enable
false|true
```

단계

System Manager 또는 ONTAP CLI를 사용하여 ARP 기본 활성화 옵션을 관리할 수 있습니다.

시스템 관리자

1. 클러스터 > 설정 * 을 선택합니다.
2. 다음 중 하나를 수행합니다.
   - 활성 유예 기간 동안 비활성화:
     i. 랜섬웨어 방지 섹션에서 ARP가 활성화되기까지 남은 시간을 나타내는 메시지가 표시됩니다. *활성화 안 함*을 선택합니다.
     ii. 다음 대화 상자에서 *Disable*을 선택하여 새 볼륨에 대한 기본 ARP 활성화가 해제되었는지 확인하십시오.
   - 유예 기간 후 비활성화:
     i. 랜섬웨어 방지 섹션에서 를 선택하세요.
     ii. 확인란을 선택한 다음 *저장*을 클릭하여 새 볼륨에 대한 기본 ARP 활성화를 비활성화합니다.

CLI를 참조하십시오

1. 기본 활성화 상태를 확인합니다.

```
security anti-ransomware auto-enable show
```

2. 새 볼륨에 대한 기본 활성화 비활성화:

```
security anti-ransomware auto-enable modify -new-volume-auto-enable
false
```

관련 정보

- "개별 볼륨에서 ONTAP 자율형 랜섬웨어 보호 기능을 활성화합니다"

학습 기간 후에 **ONTAP ARP**에서 활성 모드로 전환합니다

NAS 환경의 경우, ARP 지원 볼륨을 학습 모드에서 활성 모드로 수동 또는 자동으로 전환할 수 있습니다. ONTAP 9.15.1 및 이전 버전에서 ARP를 사용하거나 ONTAP 9.17.1 및 이전 버전에서 FlexGroup 볼륨에서 ARP를 실행하는 경우 모드를 전환해야 합니다.

ARP가 권장 최소 30일의 학습 모드 실행을 완료하면 수동으로 액티브 모드로 전환할 수 있습니다. ONTAP 9.13.1부터 ARP는 최적의 학습 기간 간격을 자동으로 결정하고 전환을 자동화하며, 이는 30일 전에 발생할 수 있습니다.

ARP/AI 보호 기능과 함께 ARP를 사용하는 경우 ARP가 자동으로 활성화됩니다. 학습 기간이 필요하지 않습니다.

기존 볼륨에서 학습 및 활성 모드는 볼륨의 기존 데이터가 아닌 새로 기록된 데이터에만 적용됩니다. ARP에 대해 볼륨이 활성화된 후 새 데이터를 기반으로 이전 일반 데이터 트래픽의 특성이 가정되기 때문에 기존 데이터는 스캔되고 분석되지 않습니다.

학습 기간 후 수동으로 활성 모드로 전환합니다

ONTAP 9.10.1~9.15.1(FlexGroup 볼륨이 있는 ONTAP 9.17.1 이하)의 경우 학습 기간이 완료된 후 시스템 관리자나 ONTAP CLI를 사용하여 ARP 학습 모드에서 활성 모드로 수동으로 전환할 수 있습니다.

이 작업에 대해

이 절차에 설명된 학습 기간 후 활성 모드로 수동 전환하는 작업은 NAS 환경에만 해당됩니다.

단계

시스템 관리자나 ONTAP CLI를 사용하여 학습 모드에서 활성 모드로 전환할 수 있습니다.

시스템 관리자

1. 스토리지 > 볼륨 * 을 선택한 다음 활성 모드에 사용할 준비가 된 볼륨을 선택합니다.
2. 볼륨 * 개요의 * 보안 * 탭에서 안티 랜섬웨어 상자에서 * 활성 모드로 전환 * 을 선택합니다.
3. Anti-랜섬웨어 * 상자에서 볼륨의 ARP 상태를 확인할 수 있습니다.

CLI를 참조하십시오

1. 보호된 볼륨을 자동으로 활성 모드로 전환하지 않은 경우 이를 수정하여 활성 모드로 전환합니다.

   ```
   security anti-ransomware volume enable -volume <vol_name> -vserver
   <svm_name>
   ```

   볼륨 수정 명령을 사용하여 활성 모드로 전환할 수도 있습니다.

   ```
   volume modify -volume <vol_name> -vserver <svm_name> -anti
   -ransomware-state enabled
   ```

2. 볼륨의 ARP 상태를 확인합니다.

   ```
   security anti-ransomware volume show
   ```

학습 모드에서 활성 모드로 자동 전환

ONTAP 9.13.1부터 ARP 분석에 적응형 학습 기능이 추가되었으며, 학습 모드에서 활성 모드로의 전환은 자동으로 이루어집니다. ARP가 학습 모드에서 활성 모드로 자동 전환하는 자율적인 결정은 다음 옵션의 구성 설정을 기반으로 합니다.

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

자동 전환을 활성화하면 모든 조건이 충족되지 않더라도 최대 30일 후에 볼륨이 자동으로 활성 모드로 전환됩니다. 이 30일 제한은 고정되어 있으며 변경할 수 없습니다.

기본값을 포함한 ARP 구성 옵션에 대한 자세한 내용은 를 참조하십시오 "ONTAP 명령 참조입니다".

관련 정보

- "보안 랜섬웨어 볼륨"

SAN 볼륨에 대한 ONTAP ARP 평가 기간에 대해 알아보세요.

ONTAP 9.17.1부터 ARP는 SAN 볼륨 워크로드의 엔트로피 수준이 랜섬웨어 보호에 적합한지 확인하기 위한 평가 기간을 요구합니다. SAN 볼륨에서 ARP가 활성화되면 ARP/AI는 평가 기간 동안 볼륨을 적극적으로 모니터링하고 보호하는 동시에 최적의 암호화 임계값을 결정합니다. 평가 기간 동안 기준 임계값이 설정되는 동안 보수적인 임계값을 사용하여 감지 및 경고가 발생할 수 있습니다. ARP는 평가 대상 SAN 볼륨에서 적합한 워크로드와 적합하지 않은 워크로드를 구분하고, 워크로드가 보호에 적합하다고 판단되면 평가 기간 통계를 기반으로 암호화 임계값을 자동으로 설정합니다.

엔트로피 평가 이해

시스템은 10분 간격으로 지속적인 암호화 통계를 수집합니다. 평가 중에 ARP 주기적 스냅샷도 4시간마다 지속적으로 생성됩니다. 간격 내 암호화 비율이 이 볼륨에 대해 식별된 최적 암호화 임계값을 초과하면 경고가 트리거됩니다. `Anti_ransomware_attack_backup` 스냅샷이 생성되고, 주기적 ARP 스냅샷에서 스냅샷 보존 시간이 늘어납니다.

평가 기간이 활성화되어 있는지 확인하세요

다음 명령을 실행하고 상태를 확인하여 평가가 활성 상태인지 확인할 수 있습니다 `evaluation_period`. 평가 대상이 아닌 볼륨의 경우 평가 상태가 표시되지 않습니다.

```
security anti-ransomware volume show -vserver <svm_name> -volume
<volume_name>
```

응답 예시:

```
Vserver Name                                    : vs1
Volume Name                                     : v1
State                                           : enabled
Attack Probability                              : none
Attack Timeline                                 : -
Number of Attacks                               : -
Attack Detected By                              : -
Block device detection status                   : evaluation_period
```

평가 기간 데이터 수집 모니터링

다음 명령을 실행하면 암호화 탐지를 실시간으로 모니터링할 수 있습니다. 이 명령은 각 암호화 비율 범위에 포함된 데이터 양을 보여주는 히스토그램을 반환합니다. 히스토그램은 10분마다 업데이트됩니다.

```
security anti-ransomware volume entropy-stat show-encryption-percentage-
histogram -vserver <svm_name> -name <lun_name> -duration real_time
```

응답 예시:

```
Vserver     Name              Entropy Range   Seen N Time     Data Written
----------  ----------------  --------------- --------------
-------------
vs0         lun1              0-5%            4               100MB
vs0         lun1              6-10%           10              900MB
vs0         lun1              11-15%          20              40MB
vs0         lun1              16-20%          10              70MB
vs0         lun1              21-25%          60              450MB
vs0         lun1              26-30%          4               100MB
vs0         lun1              31-35%          10              900MB
vs0         lun1              36-40%          20              40MB
vs0         lun1              41-45%          0               0
vs0         lun1              46-50%          0               0
vs0         lun1              51-55%          0               0
vs0         lun1              56-60%          0               0
vs0         lun1              61-65%          0               0
vs0         lun1              66-70%          0               0
vs0         lun1              71-75%          0               0
vs0         lun1              76-80%          0               0
vs0         lun1              81-85%          0               0
vs0         lun1              86-90%          0               0
vs0         lun1              91-95%          0               0
vs0         lun1              96-100%         0               0

20 entries were displayed.
```

적절한 작업 부하 및 적응 임계값

평가는 다음 결과 중 하나로 종료됩니다.

- 해당 워크로드는 **ARP**에 적합합니다. ARP는 평가 기간 동안 확인된 최대 암호화 비율의 10% 이상으로 적응형 임계값을 자동 설정합니다. 또한 ARP는 통계 수집을 계속하고 주기적인 ARP 스냅샷을 생성합니다.
- 작업 부하가 **ARP**에 적합하지 않습니다. ARP는 평가 기간 동안 확인된 최대 암호화 비율로 적응형 임계값을 자동 설정합니다. ARP는 또한 통계 수집을 계속하고 주기적인 ARP 스냅샷을 생성하지만, 궁극적으로 시스템은 해당 볼륨에서 ARP를 비활성화할 것을 권장합니다.

평가 결과 확인

평가 기간이 종료되면 ARP는 평가 결과에 따라 자동으로 적응 임계값을 설정합니다.

다음 명령을 실행하여 평가 결과를 확인할 수 있습니다. 볼륨 적합성은 `Block device detection status` 필드:

```
security anti-ransomware volume show  -vserver <svm_name> -volume
<volume_name>
```

응답 예시:

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : Active_suitable_workload

Block device evaluation start time :  5/16/2025 01:49:01
```

평가 결과에 따라 채택된 값 임계값을 표시할 수도 있습니다.

```
security anti-ransomware volume attack-detection-parameters show -vserver
<svm_name> -volume <volume_name>
```

응답 예시:

```
                                    Vserver Name : vs_1

                                     Volume Name : vm_2

Block Device Auto Learned Encryption Threshold : 10
...
```

ONTAP 자율적 랜섬웨어 보호를 일시 중지하여 워크로드 이벤트를 분석에서 제외합니다

비정상적인 워크로드 이벤트가 발생할 것으로 예상되는 경우 언제든지 ARP(Autonomous 랜섬웨어 보호) 분석을 일시 중지 및 재개할 수 있습니다.

ONTAP 9.13.1부터 ARP를 일시 중지하기 위해 2명 이상의 인증된 사용자 관리자가 필요하도록 MAV(Multi-admin Verification)를 활성화할 수 있습니다.

"MAV에 대해 자세히 알아보십시오"..

이 작업에 대해

ARP 일시 중지 동안 ONTAP 새로운 쓰기에 대한 이벤트나 작업을 기록하지 않습니다. 그러나 이전 로그에 대한 분석은 백그라운드에서 계속됩니다.

> ARP 비활성화 기능을 사용하여 분석을 일시 중지하지 마십시오. 이렇게 하면 볼륨에서 ARP가 비활성화되고 학습된 워크로드 동작에 대한 기존 정보가 모두 손실됩니다. 이 경우 학습 기간을 다시 시작해야 합니다.

단계

시스템 관리자 또는 ONTAP CLI를 사용하여 ARP를 일시 중지할 수 있습니다.

시스템 관리자

1. 스토리지 > 볼륨 * 을 선택한 다음 ARP를 일시 중지할 볼륨을 선택합니다.
2. 볼륨 개요의 보안 탭에서 랜섬웨어 방지 상자에서 *랜섬웨어 방지 일시 중지*를 선택합니다.

   ONTAP 9.13.1부터 MAV를 사용하여 ARP 설정을 보호하는 경우 일시 중지 작업 시 한 명 이상의 추가 관리자의 승인을 얻도록 요청합니다. "모든 관리자로부터 승인을 받아야 합니다" MAV 승인 그룹과 연관되지 않으면 작업이 실패합니다.

3. 모니터링을 재개하려면 *랜섬웨어 방지 재개*를 선택하세요.

CLI를 참조하십시오

1. 볼륨에서 ARP 일시 중지:

   ```
   security anti-ransomware volume pause -vserver <svm_name> -volume
   <vol_name>
   ```

2. 처리를 재개하려면 를 사용합니다 `resume` 명령:

   ```
   security anti-ransomware volume resume -vserver <svm_name> -volume
   <vol_name>
   ```

   에 대한 자세한 내용은 `security anti-ransomware volume` "ONTAP 명령 참조입니다"을 참조하십시오.

3. ONTAP 9.13.1부터 ARP와 함께 사용 가능한 MAV를 사용하여 ARP 설정을 보호하는 경우 일시 중지 작업을 수행하면 한 명 이상의 추가 관리자의 승인을 얻도록 요청합니다. MAV 승인 그룹에 속한 모든 관리자의 승인을 받아야 하며, 그렇지 않으면 작업이 실패합니다.

   MAV를 사용 중이고 예상 일시 중지 작업에 추가 승인이 필요한 경우 각 MAV 그룹 승인자는 다음을 수행합니다.

   a. 요청 표시:

      ```
      security multi-admin-verify request show
      ```

   b. 요청 승인:

      ```
      security multi-admin-verify request approve -index[<number
      returned from show request>]
      ```

      마지막 그룹 승인자에 대한 응답은 볼륨이 수정되었고 ARP 상태가 일시 중지되었음을 나타냅니다.

      MAV를 사용하고 있고 MAV 그룹 승인자인 경우 일시 중지 작업 요청을 거부할 수 있습니다.

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

+
에 대한 자세한 내용은 `security multi-admin-verify request` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 자율적 랜섬웨어 방어 공격 감지 매개 변수를 관리합니다

ONTAP 9.11.1부터 자율적 랜섬웨어 방어를 활성화하여 특정 볼륨에서 랜섬웨어 감지 매개 변수를 수정하고 알려진 서지(surge)를 일반 파일 활동으로 보고할 수 있습니다. 감지 매개 변수를 조정하면 특정 볼륨 작업량에 따라 보고의 정확도를 높일 수 있습니다.

공격 탐지 작동 방식

자율 랜섬웨어 보호(ARP)가 학습 또는 평가 모드에 있을 때 볼륨 동작에 대한 기준값을 개발합니다. 여기에는 엔트로피, 파일 확장자, 그리고 ONTAP 9.11.1부터는 IOPS가 포함됩니다. 이러한 기준값은 랜섬웨어 위협을 평가하는 데 사용됩니다. "ARP가 감지하는 것" .

특정 볼륨과 작업 부하에는 다른 감지 매개변수가 필요합니다. 예를 들어, ARP가 활성화된 볼륨은 다양한 유형의 파일 확장자를 호스팅할 수 있으며, 이 경우 이전에 본 적이 없는 파일 확장자에 대한 임계값 수를 기본값인 20보다 큰 수로 수정하거나 이전에 본 적이 없는 파일 확장자에 따른 경고를 비활성화할 수 있습니다. ONTAP 9.11.1부터 공격 탐지 매개변수를 수정하여 특정 작업 부하에 더 잘 맞출 수 있습니다.

ONTAP 9.14.1부터 ARP가 새 파일 확장자를 관찰하고 ARP가 스냅샷을 생성할 때 경고를 구성할 수 있습니다. 자세한 내용은 을 [modify-alerts]참조하십시오.

NAS 환경에서의 공격 탐지

ONTAP 9.10.1에서 ARP는 다음 조건을 모두 감지하면 경고를 발생시킵니다.

- 이전에 볼륨에서 관찰되지 않은 파일 확장명을 가진 20개 이상의 파일
- 높은 엔트로피 데이터

ONTAP 9.11.1부터 ARP는 _ONLY_ONLY_ONE 조건이 충족되면 위협 경고를 발생시킨다. 예를 들어, 이전에 볼륨에서 관찰되지 않은 파일 확장자를 가진 20개 이상의 파일이 24시간 내에 관찰되는 경우 ARP는 이를 관찰된 엔트로피의 위협_상관 없이_으로 분류합니다. 24시간 및 20파일 값은 기본값이며 수정할 수 있습니다.

> 오탐지 발생률을 줄이려면 *스토리지 > 볼륨 > 보안 > 워크로드 특성 구성*으로 이동하여 *새 파일 형식 모니터링*을 비활성화하세요. 이 설정은 ONTAP 9.14.1 P7, 9.15.1 P1, 9.16.1 이상 버전에서 기본적으로 비활성화되어 있습니다.

SAN 환경에서의 공격 탐지

ONTAP 9.17.1부터 ARP는 자동으로 학습된 임계값을 초과하는 높은 암호화율을 감지하면 경고를 표시합니다. 이 임계값은 "평가 기간" 하지만 수정이 가능합니다.

공격 탐지 매개 변수를 수정합니다

ARP 지원 볼륨의 예상 동작에 따라 공격 탐지 매개변수를 수정해야 할 수도 있습니다.

단계

1. 기존 공격 탐지 매개 변수 보기:

```
security anti-ransomware volume attack-detection-parameters show
-vserver <svm_name> -volume <volume_name>
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
                                              Vserver Name : vs1
                                               Volume Name : vol1
           Block Device Auto Learned Encryption Threshold : 10
            Is Detection Based on High Entropy Data Rate? : true
  Is Detection Based on Never Seen before File Extension? : true
                 Is Detection Based on File Create Rate? : true
                 Is Detection Based on File Rename Rate? : true
                 Is Detection Based on File Delete Rate? : true
          Is Detection Relaxing Popular File Extensions? : true
               High Entropy Data Surge Notify Percentage : 100
                File Create Rate Surge Notify Percentage : 100
                File Rename Rate Surge Notify Percentage : 100
                File Delete Rate Surge Notify Percentage : 100
 Never Seen before File Extensions Count Notify Threshold : 5
       Never Seen before File Extensions Duration in Hour : 48
```

2. 표시된 모든 필드는 부울 또는 정수 값으로 수정할 수 있습니다. 필드를 수정하려면 다음을 사용하세요. `security anti-ransomware volume attack-detection-parameters modify` 명령.

   에 대한 자세한 내용은 `security anti-ransomware volume attack-detection-parameters modify` "ONTAP 명령 참조입니다"을 참조하십시오.

알려진 서지를 보고합니다

ARP는 활성 상태에서도 감지 매개변수에 대한 기준값을 계속 수정합니다. 부피 활동, 1회 서지 또는 새로운 정상의 특징인 서지 중 한 가지를 알고 있는 경우, 안전한 것으로 보고해야 합니다. 수동으로 이러한 서지를 안전한 것으로 보고하면 ARP의 위협 평가의 정확도를 높이는 데 도움이 됩니다.

일회성 급지를 보고합니다

1. 알려진 상황에서 일회성 서지가 발생하고 향후 상황에서 ARP가 비슷한 서지를 보고하려면 워크로드 동작에서 서지를 지웁니다.

```
security anti-ransomware volume workload-behavior clear-surge -vserver
<svm_name> -volume <volume_name>
```

에 대한 자세한 내용은 `security anti-ransomware volume workload-behavior clear-surge` "ONTAP 명령 참조입니다"을 참조하십시오.

기준선 서지 수정

1. 보고된 서지가 정상적인 응용 프로그램 동작으로 간주되어야 하는 경우 서지를 보고하여 기준 서지 값을 수정합니다.

```
security anti-ransomware volume workload-behavior update-baseline-from-
surge -vserver <svm_name> -volume <volume_name>
```

자세히 알아보세요 `security anti-ransomware volume workload-behavior update-baseline-from-surge` 에서 "ONTAP 명령 참조입니다" .

ARP 경고를 구성합니다

ONTAP 9.14.1부터 ARP를 사용하면 두 ARP 이벤트에 대한 경고를 지정할 수 있습니다.

- 볼륨에서 새 파일 확장명을 관찰합니다
- ARP 스냅샷 생성

이러한 두 이벤트에 대한 경고는 개별 볼륨 또는 전체 SVM에 설정할 수 있습니다. SVM에 대해 경고를 활성화하면 알림을 사용하도록 설정한 후 생성된 볼륨에서만 경고 설정이 상속됩니다. 기본적으로 알림은 모든 볼륨에 대해 활성화되지 않습니다.

이벤트 알림은 여러 관리자의 확인을 통해 제어할 수 있습니다. 자세한 내용은 다음을 참조하세요. "ARP로 보호되는 볼륨을 사용한 다중 관리자 검증" .

단계

시스템 관리자나 ONTAP CLI를 사용하여 ARP 이벤트에 대한 알림을 설정할 수 있습니다.

시스템 관리자

볼륨에 대한 알림을 설정합니다

1. *볼륨*으로 이동합니다. 설정을 수정할 개별 볼륨을 선택합니다.
2. 보안 탭을 선택한 다음 *이벤트 심각도 설정*을 선택합니다.
3. 새로운 파일 확장자 감지됨 및 랜섬웨어 스냅샷 생성됨 알림을 받으려면 심각도 제목 아래의 드롭다운 메뉴를 선택하세요. 설정을 *이벤트 생성 안 함*에서 *알림*으로 변경하세요.
4. 저장 * 을 선택합니다.

SVM에 대한 알림 설정

1. *저장소 VM*으로 이동한 다음 설정을 활성화하려는 SVM을 선택합니다.
2. 보안 항목 아래에서 랜섬웨어 방지 카드를 찾으세요 . ⋮ 그런 다음 *랜섬웨어 이벤트 심각도 편집*을 클릭합니다.
3. 새로운 파일 확장자 감지됨 및 랜섬웨어 스냅샷 생성됨 알림을 받으려면 심각도 제목 아래의 드롭다운 메뉴를 선택하세요. 설정을 *이벤트 생성 안 함*에서 *알림*으로 변경하세요.
4. 저장 * 을 선택합니다.

CLI를 참조하십시오

볼륨에 대한 알림을 설정합니다

- 새 파일 확장자에 대한 알림을 설정하려면 다음을 수행합니다.

```
security anti-ransomware volume event-log modify -vserver <svm_name>
-volume <volume_name> -is-enabled-on-new-file-extension-seen true`
```

- ARP 스냅샷 생성을 위한 경고를 설정하려면:

```
security anti-ransomware volume event-log modify -vserver <svm_name>
-volume <volume_name> -is-enabled-on-snapshot-copy-creation true
```

- 를 사용하여 설정을 확인합니다 `anti-ransomware volume event-log show` 명령.

SVM에 대한 알림 설정

- 새 파일 확장자에 대한 알림을 설정하려면 다음을 수행합니다.

```
security anti-ransomware vserver event-log modify -vserver
<svm_name> -is-enabled-on-new-file-extension-seen true
```

- ARP 스냅샷 생성을 위한 경고를 설정하려면:

```
security anti-ransomware vserver event-log modify -vserver
<svm_name> -is-enabled-on-snapshot-copy-creation true
```

- 를 사용하여 설정을 확인합니다 `security anti-ransomware vserver event-log show` 명령.

자세히 알아보세요 `security anti-ransomware vserver event-log` 의 명령 "ONTAP 명령 참조입니다" .

관련 정보

- "자율적 랜섬웨어 방어 공격 및 자율적 랜섬웨어 방어 스냅샷을 이해합니다"..
- "ONTAP 명령 참조입니다"

ONTAP ARP가 감지한 비정상적인 활동에 응답합니다

ARP(Autonomous 랜섬웨어 Protection)가 보호 볼륨에서 비정상적인 활동을 감지하면 경고를 표시합니다. 알림을 평가하여 활동이 허용 가능한지(가양성) 또는 공격이 악의적으로 보이는지 여부를 결정해야 합니다. 공격을 범주화한 후 의심스러운 파일에 대한 경고 및 알림을 지울 수 있습니다.

공격을 분류하면 ARP 스냅샷은 분류 작업(ONTAP 9.16.1 이상)에 의해 시작된 단축 기간 동안 보관되거나 즉시 삭제됩니다(ONTAP 9.15.1 이하).

ONTAP 9.11.1부터 다음을 수정할 수 있습니다. "보존 설정" ARP 스냅샷의 경우.

이 작업에 대해

ARP는 높은 데이터 엔트로피, 데이터 암호화를 사용하는 비정상적인 볼륨 활동, 그리고 비정상적인 파일 확장자 등의 조합을 감지할 경우 의심 파일 목록을 표시합니다. ONTAP 9.17.1부터 NAS 및 SAN 환경 모두에서 엔트로피 급증에 대한 자세한 정보가 System Manager의 랜섬웨어 방지 페이지에도 보고됩니다.

ARP 경고 알림이 발행되면 다음 두 가지 방법 중 하나로 활동을 지정하여 응답합니다.

- 긍정 오류

  식별된 파일 유형 또는 엔트로피 스파이크는 작업 부하에서 예상된 것이므로 무시할 수 있습니다.

- * 잠재적 랜섬웨어 공격 *

  식별된 파일 유형이나 엔트로피 스파이크는 작업 부하에서 예상치 못한 것이며 잠재적인 공격으로 간주해야 합니다.

결정을 업데이트하고 ARP 알림을 지우면 정상적인 모니터링이 재개됩니다. ARP는 위협 평가 프로필에 평가를 기록하고, 선택 사항을 기반으로 후속 파일 활동을 모니터링합니다.

공격이 의심되는 경우에는 알림을 지우기 전에 공격이 공격인지 여부를 확인하고, 공격에 대한 대응 및 보호된 데이터를 복원해야 합니다. "랜섬웨어 공격에서 복구하는 방법에 대해 자세히 알아보십시오".

전체 볼륨을 복원하는 경우 지울 알림이 없습니다.

시작하기 전에

ARP는 볼륨을 적극적으로 보호해야 하며 학습이나 평가 모드에 있어서는 안 됩니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 비정상적인 활동에 대응할 수 있습니다.

시스템 관리자

1. "비정상적인 활동" 알림을 받으면 링크를 따라가세요. 또는 볼륨 개요의 보안 탭으로 이동하세요.

   경고는 * Events * 메뉴의 * Overview * 창에 표시됩니다.

2. 보안 탭에서 의심되는 파일 유형이나 엔트로피 스파이크 보고서를 검토합니다.
   - 의심되는 파일의 경우, 의심되는 파일 유형 대화 상자에서 각 파일 유형을 검사하고 각각을 개별적으로 표시하세요.
   - 엔트로피 스파이크에 대해서는 엔트로피 보고서를 살펴보세요.

3. 귀하의 응답을 기록하세요:

이 값을 선택하면…	이 작업 수행…
거짓 양성	a. 다음 중 하나를 수행합니다. ◦ 파일 유형 경고를 보려면 *의심스러운 파일 유형 업데이트 및 지우기*를 선택하세요. ◦ 엔트로피 스파이크의 경우 *거짓 양성으로 표시*를 선택합니다. 이러한 작업은 의심되는 파일 또는 활동에 대한 경고 알림을 지웁니다. 그런 다음 ARP가 볼륨에 대한 정상적인 모니터링을 재개합니다. ONTAP 9.16.1 이상의 ARP/AI의 경우, 분류 작업으로 트리거된 단축 보존 기간이 지나면 ARP 스냅샷이 자동으로 삭제됩니다. ONTAP 9.15.1 이하 버전의 경우, 의심되는 파일 유형을 지우면 관련 ARP 스냅샷이 자동으로 삭제됩니다. ⓘ ONTAP 9.13.1부터 MAV를 사용하여 ARP 설정을 보호하는 경우, 명백한 의심 작업에서는 한 명 이상의 추가 관리자의 승인을 얻도록 요청합니다. "모든 관리자로부터 승인을 받아야 합니다" MAV 승인 그룹과 연관되지 않으면 작업이 실패합니다.

잠재적인 랜섬웨어 공격	a. 공격에 대응하세요: ◦ 파일 유형 경고의 경우 선택한 파일을 *잠재적 랜섬웨어 공격*으로 표시하고 "보호된 데이터를 복원합니다" . ◦ 공격을 나타내는 엔트로피 스파이크의 경우 *잠재적 랜섬웨어 공격으로 표시*를 선택합니다. "보호된 데이터를 복원합니다" . b. 데이터 복구가 완료되면 결정을 기록하고 정상적인 ARP 모니터링을 재개하세요. ◦ 파일 유형 경고를 보려면 *의심스러운 파일 유형 업데이트 및 지우기*를 선택하세요. ◦ 엔트로피 스파이크의 경우 *잠재적 랜섬웨어 공격으로 표시*를 선택하고 *저장 및 해제*를 선택합니다. ⓘ 전체 볼륨을 복원한 경우 지워야 할 의심되는 파일 유형 알림이 없습니다. 결정을 기록하면 공격 보고서가 삭제됩니다. ONTAP 9.16.1 이상의 ARP/AI의 경우, 분류 작업으로 트리거된 단축 보존 기간이 지나면 ARP 스냅샷이 자동으로 삭제됩니다. ONTAP 9.15.1 이하 버전의 경우 볼륨을 복원하면 ARP 스냅샷이 자동으로 삭제됩니다.

CLI를 참조하십시오

공격을 확인하세요

1. 랜섬웨어 공격이 의심되는 경우 다음 사항을 통지하여 공격의 시간 및 심각도를 확인하십시오.

```
security anti-ransomware volume show -vserver <svm_name> -volume
<vol_name>
```

샘플 출력:

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 5/12/2025 01:03:23
Number of Attacks: 1
Attack Detected By: encryption_percentage_analysis
```

EMS 메시지를 확인할 수도 있습니다.

```
event log show -message-name callhome.arw.activity.seen
```

2. 공격 보고서를 생성하고 저장할 위치를 지정합니다.

```
security anti-ransomware volume attack generate-report -vserver
<svm_name> -volume <vol_name> -dest-path
<[svm_name]:[junction_path/sub_dir_name]>
```

명령 예:

```
security anti-ransomware volume attack generate-report -vserver vs0
-volume vol1 -dest-path vs0:vol1
```

샘플 출력:

```
Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
"vs0:vol1/"
```

3. 관리 클라이언트 시스템에서 보고서를 봅니다. 예를 들면 다음과 같습니다.

```
cat report_file_vs0_vol1_14-09-2021_01-21-08
```

조치를 취하다

1. 파일 확장자나 엔트로피 스파이크에 대한 평가에 따라 다음 작업 중 하나를 수행하세요.

   ◦ 거짓 양성

   다음 명령 중 하나를 실행하여 결정을 기록하고 정상적인 Autonomous Ransomware Protection 모니터링을 재개하세요.

   - 파일 확장자의 경우:

     ```
     anti-ransomware volume attack clear-suspect -vserver
     <svm_name> -volume <vol_name> [<extension_identifiers>] -false
     -positive true
     ```

     다음 선택적 매개 변수를 사용하여 특정 확장만 위양성으로 식별합니다.

     - `[-extension <text>, … ]`: 파일 확장자

   - 엔트로피 스파이크의 경우:

```
security anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive true
```

◦ 잠재적인 랜섬웨어 공격

공격에 대응하고 "ARP 생성 백업 스냅샷으로부터 데이터를 복구합니다". 데이터가 복구되면 다음 명령 중 하나를 실행하여 결정을 기록하고 정상적인 ARP 모니터링을 재개하세요

- 파일 확장자의 경우:

```
anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> [<extension identifiers>] -false
-positive false
```

다음 선택적 매개 변수를 사용하여 특정 확장만 잠재적 랜섬웨어로 식별하십시오.

- `[-extension <text>, … ]`: 파일 확장자

- 엔트로피 스파이크의 경우:

```
security anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive
false
```

이것 `clear-suspect` 작업은 공격 보고서를 지웁니다. 전체 볼륨을 복원한 경우 지울 의심 파일 유형 알림은 없습니다. ONTAP 9.16.1 이상의 ARP/AI의 경우, 분류 작업으로 트리거된 단축 보존 기간이 지나면 ARP 스냅샷이 자동으로 삭제됩니다. ONTAP 9.15.1 이하 버전의 경우, 볼륨을 복원하거나 의심 이벤트를 삭제하면 ARP 스냅샷이 자동으로 삭제됩니다.

2. 9.18.1부터 다음 상태를 확인할 수 있습니다. `clear-suspect` 작업:

```
security anti-ransomware volume show -clear-suspect-status -volume
<vol_name> -vserver <svm_name>
```

MAV 옵션

1. MAV를 사용하고 있고 예상되는 경우 `clear-suspect` 작업에 추가 승인이 필요합니다. 각 MAV 그룹 승인자는 다음을 수행해야 합니다.

a. 요청 표시:

```
security multi-admin-verify request show
```

b. 정상적인 랜섬웨어 방지 모니터링 재개 요청을 승인합니다.

```
security multi-admin-verify request approve -index[<number
returned from show request>]
```

마지막 그룹 승인자에 대한 응답은 볼륨이 수정되었고 가양성이 기록되었음을 나타냅니다.

2. MAV를 사용하고 있고 MAV 그룹 승인자인 경우 의심스러운 요청을 거부할 수도 있습니다.

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

관련 정보

- "NetApp 지식 기반: 자율 랜섬웨어 보호 공격 및 자율 랜섬웨어 보호 스냅샷 이해"
- "자동 스냅샷 옵션을 수정합니다"
- "보안 랜섬웨어 볼륨"
- "보안 다중 관리자 확인 요청"

랜섬웨어 공격 후 **ONTAP ARP** 스냅샷에서 데이터를 복원합니다

자율 랜섬웨어 보호(ARP)는 잠재적인 랜섬웨어 위협으로부터 보호하기 위해 스냅샷을 생성합니다. 이러한 ARP 스냅샷 중 하나 또는 볼륨의 다른 스냅샷을 사용하여 데이터를 복원할 수 있습니다.

이 작업에 대해

ARP는 다음 이름 중 하나를 접두사로 사용하여 스냅샷을 생성합니다.

- `Anti_ransomware_periodic_backup` : ONTAP 9.17.1 이상에서 정기적으로 생성되는 스냅샷에 사용됩니다. 예를 들어, `Anti_ransomware_periodic_backup.2025-06-01_1248` .
- `Anti_ransomware_attack_backup`: ONTAP 9.17.1 이상에서 비정상 상황에 대응하여 생성된 스냅샷에 사용됩니다. 예를 들어, `Anti_ransomware_attack_backup.2025-08-25_1248` .
- `Anti_ransomware_backup` : ONTAP 9.16.1 이하 버전에서 비정상 상황에 대응하여 생성되는 스냅샷과 함께 사용됩니다. 예를 들어, `Anti_ransomware_backup.2022-12-20_1248` .

스냅샷 이외의 스냅샷에서 복원하려면 `Anti_ransomware` 시스템 공격이 식별된 후 스냅샷을 먼저 공개해야 합니다.

시스템 공격이 보고되지 않으면 먼저 다음에서 복원해야 합니다. `Anti_ransomware` 스냅샷을 만든 다음 선택한 스냅샷에서 볼륨의 후속 복원을 완료합니다.

ARP 보호 볼륨이 SnapMirror 관계에 속한 경우, 스냅샷에서 볼륨을 복원한 후 해당 볼륨의 모든 미러 사본을 수동으로 업데이트해야 합니다. 이 단계를 건너뛰면 미러 사본을 사용할 수 없게 되어 삭제했다가 다시 만들어야 할 수 있습니다.

시작하기 전에

"해당 공격을 잠재적인 랜섬웨어 공격으로 표시해야 합니다." 스냅샷에서 데이터를 복원하기 전에.

단계

System Manager 또는 ONTAP CLI를 사용하여 데이터를 복원할 수 있습니다.

시스템 관리자

시스템 공격 후 복원

1. ARP 스냅샷에서 복원하려면 2단계로 건너뜁니다. 이전 스냅샷에서 복원하려면 먼저 ARP 스냅샷의 잠금을 해제해야 합니다.
   a. 스토리지 > 볼륨 * 을 선택합니다.
   b. 보안 * 을 선택한 다음 * 의심되는 파일 형식 보기 * 를 선택합니다.
   c. 파일을 "잠재적 랜섬웨어 공격"으로 표시합니다.
   d. Update * 및 * Clear Suspect File Types * 를 선택합니다.
2. 볼륨에 스냅샷을 표시합니다.

   스토리지 > 볼륨 * 을 선택한 다음 볼륨 및 * Snapshot 복사본 * 을 선택합니다.
3. 복원하려는 스냅샷 옆에 있는 을 선택한 다음 * Restore * 를 선택합니다.

시스템 공격이 확인되지 않은 경우 복원합니다

1. 볼륨에 스냅샷을 표시합니다.

   스토리지 > 볼륨 * 을 선택한 다음 볼륨 및 * Snapshot 복사본 * 을 선택합니다.
2. 선택하다 그런 다음 선택하세요 `Anti_ransomware` 스냅 사진.
3. Restore * 를 선택합니다.
4. Snapshot Copies * 메뉴로 돌아간 다음 사용할 스냅샷을 선택합니다. Restore * 를 선택합니다.

CLI를 참조하십시오

시스템 공격 후 복원

ARP 스냅샷에서 복원하려면 2단계로 건너뜁니다. 이전 스냅샷에서 데이터를 복원하려면 ARP 스냅샷의 잠금을 해제해야 합니다.

> 아래에 설명된 명령을 사용하는 경우 이전 스냅샷에서 복원하기 전에 랜섬웨어 방지 SnapLock를 해제하면 `volume snapshot restore` 됩니다. FlexClone, 단일 파일 스냅 복원 또는 다른 방법을 사용하여 데이터를 복원하는 경우에는 이 작업이 필요하지 않습니다.

1. 공격을 잠재적인 랜섬웨어 공격으로 표시 (`-false-positive false`) 및 의심스러운 파일 삭제 (`clear-suspect`):

```
anti-ransomware volume attack clear-suspect -vserver <svm_name>
-volume <vol_name> [<extension identifiers>] -false-positive false
```

   다음 매개변수 중 하나를 사용하여 확장자를 식별하세요.

   - `[-seq-no integer]` : 의심 목록에 있는 파일의 일련 번호입니다.
   - `[-extension text, … ]` : 파일 확장자

° `[-start-time date_time -end-time date_time]` : 지울 파일 범위의 시작 및 종료 시간(형식: "MM/DD/YYYY HH:MM:SS")입니다.

2. 볼륨의 스냅샷을 나열합니다.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

다음 예에서는 의 스냅샷을 `vol1` 보여 줍니다.

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

3. 스냅숏에서 볼륨의 내용 복원:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

다음 예에서는 vol1의 내용을 복원합니다.

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

시스템 공격이 확인되지 않은 경우 복원합니다

1. 볼륨의 스냅샷을 나열합니다.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

다음 예에서는 의 스냅샷을 `vol1` 보여 줍니다.

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. 스냅숏에서 볼륨의 내용 복원:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

다음 예에서는 vol1의 내용을 복원합니다.

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

에 대한 자세한 내용은 `volume snapshot` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "NetApp 지식 기반: ONTAP 에서의 랜섬웨어 예방 및 복구"
- "ONTAP 명령 참조입니다"

자동 생성된 **ARP** 스냅샷에 대한 설정 조정

ONTAP 9.11.1부터 CLI를 사용하여 의심되는 랜섬웨어 공격에 대응하여 자동으로 생성되는 ARP(자율적 랜섬웨어 방어) 스냅샷의 보존 설정을 제어할 수 있습니다.

시작하기 전에

ARP 스냅샷 옵션은 다음에서만 수정할 수 있습니다. "노드 SVM" 다른 SVM 유형에서는 그렇지 않습니다.

단계

1. 모든 현재 ARP 스냅샷 설정 표시:

```
options -option-name arw*
```

2. 선택한 현재 ARP 스냅샷 설정 표시:

```
options -option-name <arw_setting_name>
```

3. ARP 스냅샷 설정 수정:

```
options -option-name <arw_setting_name> -option-value
<arw_setting_value>
```

다음 설정을 수정할 수 있습니다.

설명된 명령 중 일부는 ONTAP 9.17.1부터 더 이상 지원되지 않습니다. ONTAP 9.17.1에 추가된 명령은 NAS 및 SAN 환경을 모두 지원합니다.

설정	설명	지원되는 버전
`arw.snap.max.count`	볼륨에 동시에 존재할 수 있는 최대 ARP 스냅샷 수를 지정합니다. 총 ARP 스냅샷 수가 이 제한을 넘지 않도록 이전 사본은 삭제됩니다.	ONTAP 9.11.1 이상
`arw.snap.create.interval.hours`	ARP 스냅샷 생성 간격(시간)을 지정합니다. 데이터 엔트로피 기반 공격이 의심되고 가장 최근에 생성된 ARP 스냅샷이 지정된 간격보다 오래된 경우 새로운 ARP 스냅샷이 생성됩니다.	ONTAP 9.11.1 이상
`arw.snap.normal.retain.interval.hours`	ARP 스냅샷이 보존되는 기간(시간)을 지정합니다. ARP 스냅샷이 보존 임계값에 도달하면 삭제됩니다.	• ONTAP 9.11.1에서 ONTAP 9.16.1로 • ONTAP 9.17.1 이상에서 더 이상 사용되지 않습니다.

설정	설명	지원되는 버전
`arw.snap.max.retain.interval.days`	ARP 스냅샷을 보존할 수 있는 최대 지속 시간을 days_로 지정합니다. 이 기간보다 오래된 ARP 스냅샷은 볼륨에 보고된 공격이 없으면 삭제됩니다. ARP 스냅샷의 최대 보존 간격은 보통 위협이 감지된 경우 무시됩니다. 위협에 대한 응답으로 생성된 ARP 스냅샷은 사용자가 위협에 응답할 때까지 유지됩니다. 위협을 false positive로 표시하면 ONTAP는 볼륨에 대한 ARP 스냅샷을 삭제합니다.	• ONTAP 9.11.1에서 ONTAP 9.16.1로 • ONTAP 9.17.1 이상에서 더 이상 사용되지 않습니다.
`arw.snap.create.interval.hours.post.max.count`	볼륨에 이미 최대 개수의 ARP 스냅샷이 있는 경우 ARP 스냅샷 생성 간격(시간)을 지정합니다. 최대 개수에 도달하면 새 복사본을 위한 공간을 확보하기 위해 ARP 스냅샷이 삭제됩니다. 이 옵션을 사용하면 새 ARP 스냅샷 생성 속도를 줄여 이전 복사본을 유지할 수 있습니다. 볼륨에 이미 최대 개수의 ARP 스냅샷이 있는 경우, 다음 ARP 스냅샷 생성에는 이 옵션에 지정된 간격이 사용됩니다. `arw.snap.create.interval.hours` .	• ONTAP 9.11.1부터 9.16.1까지 • ONTAP 9.17.1 이상에서 더 이상 사용되지 않습니다.
`arw.snap.low.encryption.retain.duration.hours`	암호화 활동이 낮은 기간 동안 생성된 ARP 스냅샷의 보존 기간을 시간 단위로 지정합니다.	• ONTAP 9.17.1 이상
`arw.snap.new.extns.interval.hours`	새 파일 확장자가 감지될 때 생성되는 ARP 스냅샷 사이의 간격(시간)을 지정합니다. 새 파일 확장자가 감지되면 새 ARP 스냅샷이 생성됩니다. 새 파일 확장자가 감지되어 생성된 이전 스냅샷은 이 지정된 간격보다 이전 스냅샷입니다. 새 파일 확장자 를 자주 생성하는 작업 부하에서 이 간격은 ARP 스냅샷의 빈도를 제어하는 데 도움이 됩니다. 이 옵션은 다음과는 별개로 존재합니다. `arw.snap.create.interval.hours` 데이터 엔트로피 기반 ARP 스냅샷의 간격을 지정합니다.	• ONTAP 9.11.1에서 ONTAP 9.16.1로 • ONTAP 9.17.1 이상에서 더 이상 사용되지 않습니다.
`arw.snap.retain.hours.after.clear.suspect.false.alert`	관리자가 공격 사고를 오탐지로 표시한 후 예방 조치로 ARP 스냅샷을 보관하는 간격(시간)을 지정합니다. 이 예방 보관 기간이 만료되면 옵션에 정의된 표준 보관 기간에 따라 스냅샷이 삭제될 수 있습니다. `arw.snap.normal.retain.interval.hours` 그리고 `arw.snap.max.retain.interval.days` .	• ONTAP 9.16.1 이상
`arw.snap.retain.hours.after.clear.suspect.real.attack`	관리자가 공격 사고를 실제 공격으로 표시한 후 예방 조치로 ARP 스냅샷을 보관하는 간격(시간)을 지정합니다. 이 예방 보관 기간이 만료되면 옵션에 정의된 표준 보관 기간에 따라 스냅샷이 삭제될 수 있습니다. `arw.snap.normal.retain.interval.hours` 그리고 `arw.snap.max.retain.interval.days` .	• ONTAP 9.16.1 이상

설정	설명	지원되는 버전
`arw.snap.surge.interval.days`	IO 서지에 대한 응답으로 생성된 ARP 스냅샷 사이의 간격 _(일)을 지정합니다. ONTAP는 IO 트래픽에 과부하가 있고 마지막으로 생성된 ARP 스냅샷이 지정된 간격보다 오래된 경우 ARP 스냅샷 서지 복제본을 생성합니다. 또한 이 옵션은 ARP 서지 스냅숏에 대한 보존 기간을 day_로 지정합니다.	ONTAP 9.11.1 이상
`arw.high.encryption.alert.enabled`	높은 수준의 암호화에 대한 알림을 활성화합니다. 이 옵션이 설정된 경우 `on` (기본값), ONTAP 암호화 비율이 지정된 임계값을 초과하면 경고를 보냅니다. `arw.high.encryption.percentage.threshold` .	ONTAP 9.17.1 이상
`arw.high.encryption.percentage.threshold`	볼륨의 최대 암호화 비율을 지정합니다. 암호화 비율이 이 임계값을 초과하면 ONTAP 증가를 공격으로 간주하고 ARP 스냅샷을 생성합니다. `arw.high.encryption.alert.enabled` 설정해야 합니다 `on` 이 옵션을 적용하려면 다음을 수행하세요.	ONTAP 9.17.1 이상
`arw.snap.high.encryption.retain.duration.hours`	높은 암호화 임계값 이벤트 중에 생성된 스냅샷의 보존 기간 간격을 시간 단위로 지정합니다.	ONTAP 9.17.1 이상

4. SAN 환경에서 ARP를 사용하는 경우 다음 평가 기간 설정도 수정할 수 있습니다.

설정	설명	지원되는 버전
`arw.block_device.auto.learn.threshold.min_value`	블록 장치에 대한 평가의 자동 학습 단계 동안 최소 암호화 임계값 백분율 값을 지정합니다.	ONTAP 9.17.1 이상
`arw.block_device.auto.learn.threshold.max_value`	블록 장치에 대한 평가의 자동 학습 단계 동안 최대 암호화 임계값 백분율 값을 지정합니다.	ONTAP 9.17.1 이상
`arw.block_device.evaluation.phase.min_hours`	암호화 임계값이 설정되기 전에 평가 단계가 실행되어야 하는 최소 간격(시간)을 지정합니다.	ONTAP 9.17.1 이상
`arw.block_device.evaluation.phase.max_hours`	암호화 임계값이 설정되기 전에 평가 단계가 실행되어야 하는 최대 간격(시간)을 지정합니다.	ONTAP 9.17.1 이상
`arw.block_device.evaluation.phase.min_data_ingest_size_GB`	암호화 임계값이 설정되기 전에 평가 단계에서 수집해야 하는 최소 데이터 양(GB)을 지정합니다.	ONTAP 9.17.1 이상

설정	설명	지원되는 버전
`arw.block_device.evaluation.phase.alert.enabled`	블록 장치에서 ARP 평가 단계에 대한 경고를 활성화할지 여부를 지정합니다. 기본값은 다음과 같습니다. `True` .	ONTAP 9.17.1 이상
`arw.block_device.evaluation.phase.alert.threshold`	블록 장치에서 ARP 평가 단계의 임계값 비율을 지정합니다. 암호화 비율이 이 임계값을 초과하면 경고가 발생합니다.	ONTAP 9.17.1 이상

관련 정보

- "위협 평가 및 ARP 스냅샷"
- "SAN 엔트로피 평가 기간"

AI(ARP/AI)로 ONTAP 자율적 랜섬웨어 방어 업데이트

최신 랜섬웨어 위협에 대한 보호를 최신 상태로 유지하기 위해 ARP/AI는 일반 ONTAP 릴리스 정보 외부에서 발생하는 자동 업데이트를 제공합니다.

ONTAP 9.16.1부터 시스템 및 펌웨어 업데이트 외에도 System Manager 소프트웨어 다운로드를 통해 ARP/AI 보안 업데이트를 이용할 수 있습니다. ONTAP 클러스터가 이미 등록된 경우 "시스템 및 펌웨어 자동 업데이트" ARP/AI 보안 업데이트가 있을 때 자동으로 알림을 받게 됩니다. 또한 업데이트 기본 설정 ONTAP 보안 업데이트를 자동으로 설치하도록 합니다.

원하는 경우 ARP/AI를 수동으로 업데이트합니다NetApp 지원 사이트에서 업데이트를 다운로드하여 System Manager를 사용하여 설치할 수 있습니다.

이 작업에 대해

ARP/AI는 시스템 관리자를 사용해서만 업데이트할 수 있습니다.

ARP/AI에 대한 업데이트 기본 설정을 선택합니다

시스템 관리자에서 보안 파일에 대한 자동 업데이트 사용 페이지의 설정이 다음과 같이 설정됩니다. `Show notifications` 이미 자동 펌웨어 및 시스템 업데이트에 등록되어 있는 경우 `Automatically update` ONTAP 최신 업데이트를 자동으로 적용하도록 설정하려면 다음을 수행하세요. 다크 사이트를 사용하거나 수동으로 업데이트를 수행하는 경우, 알림을 표시하거나 보안 업데이트를 자동으로 해제하도록 선택할 수 있습니다.

시작하기 전에

자동 보안 업데이트의 "AutoSupport 및 AutoSupport OnDemand가 활성화되고 전송 프로토콜이 HTTPS로 설정되어야 합니다"경우.

단계

1. System Manager에서 * 클러스터 > 설정 > 소프트웨어 업데이트 * 를 클릭합니다.
2. 소프트웨어 업데이트 * 섹션에서 를 선택합니다 → .
3. 소프트웨어 업데이트 * 페이지에서 * 기타 모든 업데이트 * 탭을 선택합니다.
4. 기타 모든 업데이트 * 탭을 선택하고 * 자세히 * 를 클릭합니다.

5. 자동 업데이트 설정 편집 * 을 선택합니다.
6. 자동 업데이트 설정 페이지에서 * 보안 파일 * 을 선택합니다.
7. 보안 파일에 대해 수행할 작업을 지정합니다(ARP/AI 업데이트).

   자동으로 업데이트하거나 알림을 표시하거나 업데이트를 자동으로 해제하도록 선택할 수 있습니다.

   보안 업데이트가 자동으로 업데이트되도록 하려면 AutoSupport 및 AutoSupport OnDemand를 사용하도록 설정하고 전송 프로토콜을 HTTPS로 설정해야 합니다.

8. 이용 약관에 동의하고 * 저장 * 을 선택합니다.

최신 보안 패키지로 **ARP/AI**를 수동으로 업데이트합니다

Active IQ Unified Manager에 등록되었는지 여부에 따라 적절한 절차를 따릅니다.

의도하지 않은 ARP 다운그레이드를 방지하려면 현재 버전보다 최신 ARP 업데이트만 설치하십시오.

Digital Advisor를 사용하는 **ONTAP 9.16.1** 이상

1. System Manager에서 * 대시보드 * 로 이동합니다.

   Health * 섹션에 클러스터에 대해 권장되는 보안 업데이트가 있는지 여부에 대한 메시지가 표시됩니다.

2. 경고 메시지를 클릭합니다.
3. 권장 업데이트 목록에서 보안 업데이트 옆에 있는 * 작업 * 을 선택합니다.
4. 업데이트를 즉시 설치하려면 * 업데이트 * 를 클릭하고, 나중에 업데이트 일정을 예약하려면 * 일정 * 을 클릭합니다.

   업데이트가 이미 예약된 경우 * 편집 * 또는 * 취소 * 할 수 있습니다.

ONTAP 9.16.1 이상(디지털 어드바이저 제외)

1. 로 "NetApp Support 사이트"이동하여 로그인합니다.
2. 프롬프트를 완료하고 클러스터 ARP/AI를 업데이트하는 데 사용할 보안 패키지를 다운로드합니다.
3. 파일을 네트워크의 HTTP 또는 FTP 서버 또는 ARP/AI로 클러스터에서 액세스할 수 있는 로컬 폴더에 복사합니다.
4. System Manager에서 * 클러스터 > 설정 > 소프트웨어 업데이트 * 를 클릭합니다.
5. 소프트웨어 업데이트 * 에서 * 기타 모든 업데이트 * 탭을 선택합니다.
6. 수동 업데이트 * 창에서 * 보안 파일 추가 * 를 클릭하고 다음 기본 설정 중 하나를 사용하여 파일을 추가합니다.
   - * 서버에서 다운로드 *: 보안 파일 패키지의 URL을 입력합니다.
   - * 로컬 클라이언트에서 업로드 *: 다운로드한 TGZ 파일로 이동합니다.

   파일 이름이 로 `ontap_security_file_arpai_` 시작하고 파일 확장명으로 지정되었는지 확인합니다. `.tgz`

7. 업데이트를 적용하려면 * 추가 * 를 클릭하십시오.

ARP/AI 업데이트를 확인합니다

해제되었거나 설치에 실패한 자동 업데이트 기록을 보려면 다음을 실행합니다.

1. System Manager에서 * 클러스터 > 설정 > 소프트웨어 업데이트 * 를 클릭합니다.
2. 소프트웨어 업데이트 * 섹션에서 를 선택합니다 →.
3. 소프트웨어 업데이트 * 페이지에서 * 기타 모든 업데이트 * 탭을 선택하고 * 자세히 * 를 클릭합니다.
4. 모든 자동 업데이트 보기 * 를 선택합니다.

관련 정보

- "ARP/AI에 대해 알아보세요"
- "소프트웨어 업데이트를 위한 이메일 구독"

Vscan을 통한 바이러스 보호

ONTAP Vscan을 사용한 바이러스 백신 구성에 대해 알아보세요

Vscan은 NetApp에서 개발한 바이러스 백신 검사 솔루션으로, 고객이 바이러스나 기타 악성 코드에 의해 데이터가 손상되는 것을 방지할 수 있습니다.

Vscan은 클라이언트가 SMB를 통해 파일에 액세스할 때 바이러스 검사를 수행합니다. 주문형 또는 일정에 따라 스캔을 수행하도록 Vscan을 구성할 수 있습니다. ONTAP CLI(명령줄 인터페이스) 또는 ONTAP API(응용 프로그래밍 인터페이스)를 사용하여 Vscan과 상호 작용할 수 있습니다.

관련 정보

"Vscan 파트너 솔루션"

NetApp 바이러스 백신 보호 정보

ONTAP Vscan을 사용한 NetApp 바이러스 검사에 대해 알아보세요

Vscan은 NetApp에서 개발한 바이러스 백신 검사 솔루션으로, 고객이 바이러스나 기타 악성 코드에 의해 데이터가 손상되는 것을 방지할 수 있습니다. 파트너가 제공하는 바이러스 백신 소프트웨어와 ONTAP 기능을 결합하여 고객이 파일 검사를 관리하는 데 필요한 유연성을 제공합니다.

바이러스 검사 작동 방식

스토리지 시스템은 타사 공급업체의 안티바이러스 소프트웨어를 호스팅하는 외부 서버로 검사 작업을 오프로드합니다.

활성 스캐닝 모드에 따라 ONTAP는 클라이언트가 SMB(온액세스)를 통해 파일에 액세스하거나 특정 위치, 스케줄 또는 즉시(온디맨드)에 있는 파일에 액세스할 때 스캔 요청을 전송합니다.

- 액세스 시 검사 _ 를 사용하여 클라이언트가 SMB를 통해 파일을 열거나 읽거나 이름을 바꾸거나 닫을 때 바이러스를 검사할 수 있습니다. 외부 서버가 파일의 스캔 상태를 보고할 때까지 파일 작업이 일시 중단됩니다. 파일이 이미 스캔되면 ONTAP에서 파일 작업을 허용합니다. 그렇지 않으면 서버에서 스캔을 요청합니다.

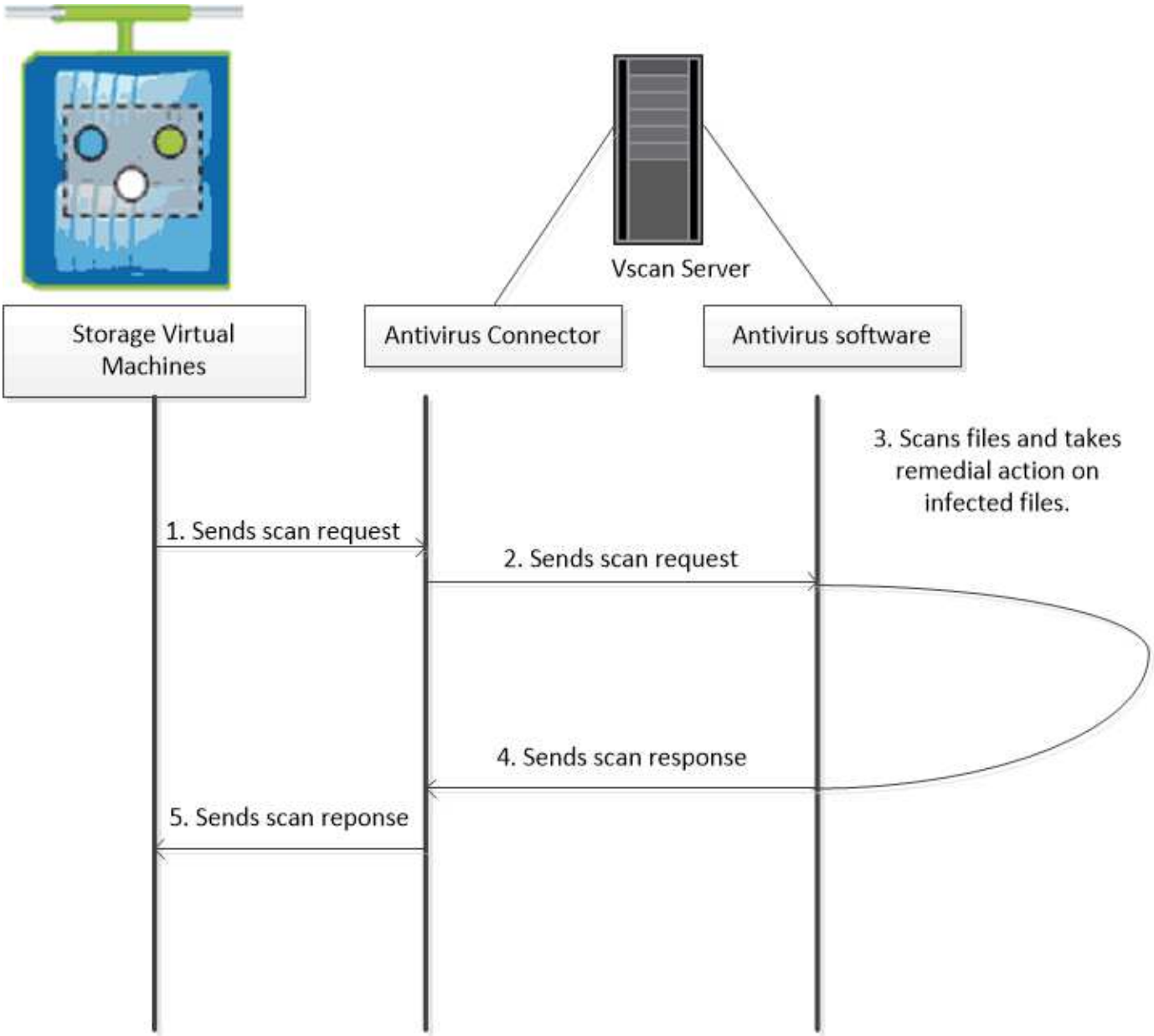
액세스 시 스캐닝은 NFS에서 지원되지 않습니다.

- 주문형 검사 _ 을(를) 사용하여 파일에 바이러스가 있는지 즉시 또는 일정에 따라 확인할 수 있습니다. 일반적으로 온액세스 스캐닝에 적합한 크기인 기존 AV 인프라가 과부하되지 않도록 사용량이 적은 시간에만 온디맨드 검사를 실행하는 것이 좋습니다. 외부 서버는 선택한 파일의 스캔 상태를 업데이트하므로 SMB에 비해 파일 액세스 지연 시간이 줄어듭니다. 파일 수정이나 소프트웨어 버전 업데이트가 있는 경우 외부 서버에서 새 파일 검사를 요청합니다.

  NFS를 통해서만 내보낸 볼륨에서도 SVM 네임스페이스에서 모든 경로에 대해 온디맨드 스캐닝을 사용할 수 있습니다.

일반적으로 SVM에서 액세스 시 스캐닝 모드와 온디맨드 스캐닝 모드를 모두 사용할 수 있습니다. 어느 모드에서든 바이러스 백신 소프트웨어는 소프트웨어 설정에 따라 감염된 파일에 대한 치료 조치를 취합니다.

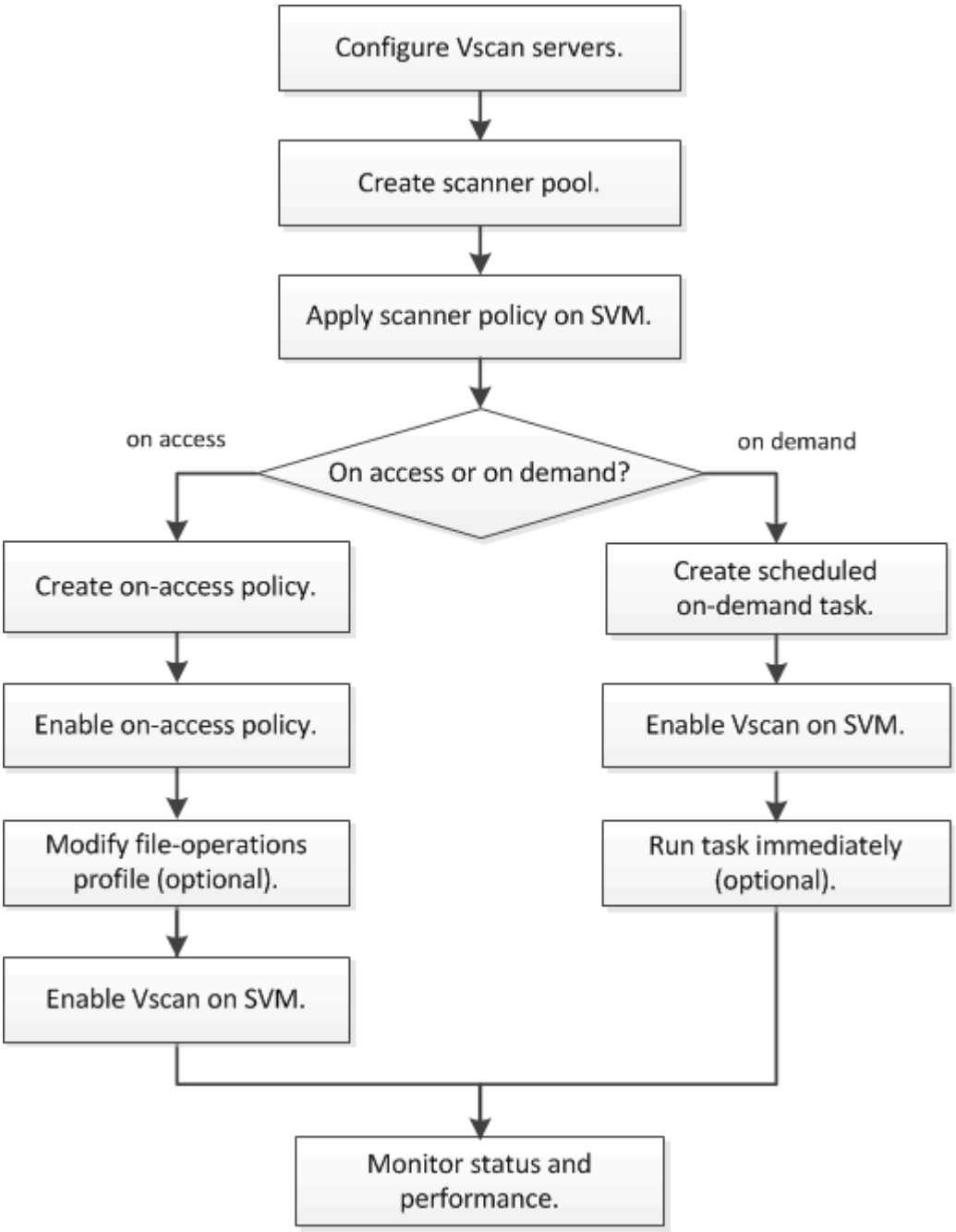
NetApp에서 제공하고 외부 서버에 설치된 ONTAP 바이러스 백신 커넥터는 스토리지 시스템과 바이러스 백신 소프트웨어 간의 통신을 처리합니다.



ONTAP Vscan을 사용한 바이러스 검사 워크플로

스캔을 활성화하기 전에 스캐너 풀을 생성하고 스캐너 정책을 적용해야 합니다. 일반적으로 SVM에서 액세스 시 스캐닝 모드와 온디맨드 스캐닝 모드를 모두 사용할 수 있습니다.

CIFS 구성을 완료해야 합니다.



필요 시 작업을 생성하려면 액세스 시 정책을 하나 이상 활성화해야 합니다. 기본 정책이거나 사용자가 만든 액세스 시 정책일 수 있습니다.

다음 단계

- 단일 클러스터에 스캐너 풀을 생성합니다

- 단일 클러스터에 스캐너 정책을 적용합니다
- 액세스 시 정책을 생성합니다

ONTAP Vscan을 활용한 안티바이러스 아키텍처

NetApp 바이러스 백신 아키텍처는 Vscan 서버 소프트웨어와 관련 설정으로 구성됩니다.

Vscan 서버 소프트웨어

Vscan 서버에 이 소프트웨어를 설치해야 합니다.

- * ONTAP 안티바이러스 커넥터 *

  이 소프트웨어는 NetApp에서 제공하며 SVM과 바이러스 백신 소프트웨어 간의 스캔 요청 및 응답 통신을 처리합니다. 가상 시스템에서 실행할 수 있지만 최상의 성능을 위해서는 물리적 시스템을 사용해야 합니다. NetApp Support 사이트에서 이 소프트웨어를 다운로드할 수 있습니다(로그인 필요).

- * 안티바이러스 소프트웨어 *

  이 소프트웨어는 바이러스 또는 기타 악성 코드가 있는 파일을 검사하는 파트너 제공 소프트웨어입니다. 소프트웨어를 구성할 때 감염된 파일에 대해 수행할 치료 조치를 지정합니다.

Vscan 소프트웨어 설정

Vscan 서버에서 이러한 소프트웨어 설정을 구성해야 합니다.

- * 스캐너 풀 *

  이 설정은 SVM에 연결할 수 있는 Vscan 서버 및 특별 권한 사용자를 정의합니다. 또한 스캔 요청 시간 초과 기간을 정의하며, 이 기간이 지나면 스캔 요청이 다른 Vscan 서버로 전송됩니다(사용 가능한 경우).

  > Vscan 서버의 바이러스 백신 소프트웨어에서 시간 초과 기간을 scanner-pool scan-request 시간 초과 기간보다 5초 이내로 설정해야 합니다. 따라서 소프트웨어의 시간 제한 기간이 스캔 요청의 시간 초과 기간보다 크기 때문에 파일 액세스가 모두 지연되거나 거부되는 상황을 피할 수 있습니다.

- * 특별 권한 사용자 *

  이 설정은 Vscan 서버에서 SVM에 연결하는 데 사용하는 도메인 사용자 계정입니다. 계정은 스캐너 풀의 권한이 있는 사용자 목록에 있어야 합니다.

- * 스캐너 정책 *

  이 설정은 스캐너 풀의 활성 여부를 결정합니다. 스캐너 정책은 시스템 정의이므로 사용자 정의 스캐너 정책을 만들 수 없습니다. 다음 세 가지 정책만 사용할 수 있습니다.

  - "기본"은 스캐너 풀이 활성화되도록 지정합니다.
  - `Secondary` 기본 스캐너 풀에 있는 Vscan 서버가 연결되어 있지 않을 때만 스캐너 풀이 활성화되도록 지정합니다.
  - "유휴"는 스캐너 풀이 비활성 상태라고 지정합니다.

- * 액세스 시 정책 *

  이 설정은 액세스 시 스캔의 범위를 정의합니다. 스캔할 최대 파일 크기, 스캔에 포함할 파일 확장명 및 경로, 스캔에서 제외할 파일 확장명 및 경로를 지정할 수 있습니다.

  기본적으로 읽기-쓰기 볼륨만 스캔됩니다. 읽기 전용 볼륨을 스캔할 수 있도록 하거나 실행 액세스 권한으로 연 파일로 스캔을 제한하는 필터를 지정할 수 있습니다.

  - '스캔-볼륨'은 읽기 전용 볼륨을 스캔할 수 있게 해줍니다.
  - '스캔 실행 액세스'는 실행 권한으로 연 파일로 스캔을 제한합니다.

    "접속 실행"은 "실행 권한"과 다릅니다. 특정 클라이언트는 파일이 "실행 의도"로 열린 경우에만 실행 파일에 "실행 액세스"를 가집니다.

  를 설정할 수 있습니다 `scan-mandatory` 바이러스 검사에 사용할 수 있는 Vscan 서버가 없을 때 파일 액세스가 허용되도록 지정하는 옵션. 온액세스 모드에서는 다음 두 가지 상호 배타적인 옵션 중에서 선택할 수 있습니다.

  - 필수: Vscan은 이 옵션을 사용하여 제한 시간이 만료될 때까지 서버에 스캔 요청을 전송하려고 합니다. 서버에서 스캔 요청을 수락하지 않으면 클라이언트 액세스 요청이 거부됩니다.
  - 비필수: Vscan은 이 옵션을 통해 바이러스 스캔에 Vscan 서버를 사용할 수 있는지 여부에 관계없이 항상 클라이언트 액세스를 허용합니다.

- * 온디맨드 작업 *

  이 설정은 온디맨드 스캔의 범위를 정의합니다. 스캔할 최대 파일 크기, 스캔에 포함할 파일 확장명 및 경로, 스캔에서 제외할 파일 확장명 및 경로를 지정할 수 있습니다. 하위 디렉터리의 파일은 기본적으로 스캔됩니다.

  cron 일정을 사용하여 작업 실행 시간을 지정합니다. 명령을 사용하여 작업을 즉시 실행할 수 `vserver vscan on-demand-task run` 있습니다. 에 대한 자세한 내용은 `vserver vscan on-demand-task run` "ONTAP 명령 참조입니다"을 참조하십시오.

- * Vscan 파일 작업 프로필(액세스 시 스캔에만 해당) *

  를 클릭합니다 `vscan-fileop-profile` 에 대한 매개 변수입니다 `vserver cifs share create` 명령은 바이러스 검사를 트리거하는 SMB 파일 작업을 정의합니다. 기본적으로 매개 변수는 로 설정됩니다 `standard`NetApp 모범 사례입니다. SMB 공유를 생성하거나 수정할 때 필요에 따라 이 매개 변수를 조정할 수 있습니다.

  - NO-SCAN은 공유에 대해 바이러스 검사가 트리거되지 않도록 지정합니다.
  - `standard` 열기, 닫기 및 이름 바꾸기 작업을 통해 바이러스 검사가 트리거되도록 지정합니다.
  - `strict` 열기, 읽기, 닫기 및 이름 바꾸기 작업을 통해 바이러스 검사가 트리거되도록 지정합니다.

    이 '사전' 프로필은 여러 클라이언트가 동시에 파일에 액세스하는 상황에 대해 향상된 보안을 제공합니다. 한 클라이언트에서 바이러스를 작성한 후 파일을 닫고 두 번째 클라이언트에서 동일한 파일을 열어 둘 경우 두 번째 클라이언트에서 읽기 작업을 수행하면 파일이 닫히기 전에 검사가 트리거됩니다.

    `strict`동시에 액세스할 것으로 예상되는 파일이 포함된 공유로 프로필을 제한해야 합니다. 이 프로필은 더 많은 스캔 요청을 생성하므로 성능에 영향을 미칠 수 있습니다.

◦ `writes-only` 수정된 파일이 닫힐 때만 바이러스 검사가 트리거되도록 지정합니다.

그 이후로 `writes-only` 스캔 요청을 적게 생성하여 일반적으로 성능을 향상시킵니다.

이 프로필을 사용하는 경우, 감염되지 않은 감염된 파일을 삭제하거나 격리하도록 스캐너를 구성해야 합니다. 예를 들어, 클라이언트가 바이러스에 감염된 후 파일을 닫고 파일이 복구, 삭제 또는 격리되지 않은 경우 파일에 액세스하는 모든 클라이언트가 파일을 닫습니다 `without` 쓰기 작업을 하면 감염됩니다.

ⓘ 클라이언트 응용 프로그램에서 이름 바꾸기 작업을 수행하면 파일이 새 이름으로 닫히고 스캔되지 않습니다. 이러한 작업이 환경에 보안 문제가 될 경우 '표준' 또는 '중독' 프로필을 사용해야 합니다.

에 대한 자세한 내용은 `vserver cifs share create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP Vscan 파트너 솔루션에 대해 알아보세요

NetApp는 Trellix, Symantec, Trend Micro, Sentinel One, Deep 본능 및 OPSWAT와 협력하여 ONTAP Vscan 기술을 기반으로 하는 업계 최고의 맬웨어 방지 및 바이러스 방지 솔루션을 제공합니다. 이러한 솔루션을 통해 맬웨어에 대한 파일을 검사하고 영향을 받는 파일을 수정할 수 있습니다.

아래 표에 나와 있는 것처럼 Trellix, Symantec 및 Trend Micro의 상호 운용성 세부 정보는 NetApp 상호 운용성 매트릭스에 보관되어 있습니다. Trellix, Symantec, Deep 본능 및 OPSWAT에 대한 상호 운용성 세부 정보는 파트너 웹 사이트에서도 확인할 수 있습니다. Sentinel One, Deep 본능, OPSWAT 및 기타 신규 파트너에 대한 상호 운용성 세부 정보는 해당 웹 사이트에서 파트너가 관리합니다.

파트너	솔루션 설명서	상호 운용성 세부 정보
Trelix(이전 명칭 McAfee)	"Trelix 제품 설명서"	• "NetApp 상호 운용성 매트릭스 툴" • "엔드포인트 보안 스토리지 보호에 지원되는 플랫폼(trellix.com)"
시만텍	"Symantec Protection Engine 9.0.0"	• "NetApp 상호 운용성 매트릭스 툴" • "NAS(Network Attached Storage) 9.x.x용 Symantec Protection Engine(SPE)으로 인증된 파트너 장치 지원 매트릭스"
Trend Micro	"Trend Micro ServerProtect for Storage 6.0 시작 가이드"	"NetApp 상호 운용성 매트릭스 툴"

파트너	솔루션 설명서	상호 운용성 세부 정보
센티넬 원	• "SentinelOne 특이성 클라우드 데이터 보안" • "SentinelOne 지원" 이 링크를 사용하려면 사용자 로그인이 필요합니다. Sentinel One에서 액세스를 요청할 수 있습니다.	해당 없음
깊은 본능	NAS용 DSX • "문서 및 상호 운용성" 이 링크를 사용하려면 사용자 로그인이 필요합니다. 당신은 깊은 본능에서 액세스를 요청할 수 있습니다. • "데이터 시트"	해당 없음
OPSWAT	OPSWAT MetaDefender 스토리지 보안 • "MetaDefender 스토리지 보안과 NetApp의 통합" • "OPSWAT 파트너 페이지 를 참조하십시오" • "통합 솔루션 개요"	해당 없음

Vscan 서버 설치 및 구성

ONTAP Vscan 서버 설치 및 구성

하나 이상의 Vscan 서버를 설정하여 시스템의 파일에 바이러스가 있는지 검사합니다. 공급업체에서 제공한 지침에 따라 서버에 바이러스 백신 소프트웨어를 설치하고 구성합니다.

NetApp에서 제공하는 README 파일의 지침에 따라 ONTAP 안티바이러스 커넥터를 설치하고 구성합니다. 또는 의 지침을 따릅니다 "ONTAP 안티바이러스 커넥터 설치 페이지를 참조하십시오".

재해 복구 및 MetroCluster 구성의 경우 기본/로컬 및 보조/파트너 ONTAP 클러스터에 대해 별도의 Vscan 서버를 설정 및 구성해야 합니다.

안티바이러스 소프트웨어 요구 사항

- 안티바이러스 소프트웨어 요구 사항에 대한 자세한 내용은 공급업체 설명서를 참조하십시오.

- Vscan에서 지원하는 공급업체, 소프트웨어 및 버전에 대한 자세한 내용은 "Vscan 파트너 솔루션"페이지를 참조하십시오.

ONTAP 안티바이러스 커넥터 요구 사항

- ONTAP 안티바이러스 커넥터는 NetApp Support 사이트의 * 소프트웨어 다운로드 * 페이지에서 다운로드할 수 있습니다. "NetApp 다운로드: 소프트웨어"
- ONTAP 안티바이러스 커넥터에서 지원되는 Windows 버전 및 상호 운용성 요구 사항에 대한 자세한 내용은 을 참조하십시오"Vscan 파트너 솔루션".

> 하나의 클러스터에 다른 Vscan 서버용으로 다양한 버전의 Windows 서버를 설치할 수 있습니다.

- Windows 서버에 .NET 3.0 이상이 설치되어 있어야 합니다.
- Windows 서버에서 SMB 2.0을 활성화해야 합니다.

ONTAP Vscan Antivirus 커넥터 설치

Vscan 서버에 ONTAP 안티바이러스 커넥터를 설치하여 ONTAP를 실행하는 시스템과 Vscan 서버 간의 통신을 활성화합니다. ONTAP 안티바이러스 커넥터가 설치되면 안티바이러스 소프트웨어는 하나 이상의 SVM(스토리지 가상 머신)과 통신할 수 있습니다.

이 작업에 대해

- "Vscan 파트너 솔루션"지원되는 프로토콜, 안티바이러스 공급업체 소프트웨어 버전, ONTAP 버전, 상호 운용성 요구 사항 및 Windows 서버에 대한 자세한 내용은 페이지를 참조하십시오.
- NET 4.5.1 이상이 설치되어 있어야 합니다.
- ONTAP 안티바이러스 커넥터는 가상 머신에서 실행할 수 있습니다. 그러나 최상의 성능을 위해 NetApp에서는 바이러스 백신 검사에 전용 물리적 시스템을 사용할 것을 권장합니다.
- ONTAP 안티바이러스 커넥터를 설치하고 실행하는 Windows 서버에서 SMB 2.0을 활성화해야 합니다.

시작하기 전에

- 지원 사이트에서 ONTAP 안티바이러스 커넥터 설치 파일을 다운로드하여 하드 드라이브의 디렉터리에 저장합니다.
- ONTAP 안티바이러스 커넥터를 설치하기 위한 요구 사항을 충족하는지 확인합니다.
- Antivirus Connector를 설치할 수 있는 관리자 권한이 있는지 확인합니다.

단계

1. 적절한 설치 파일을 실행하여 Antivirus Connector 설치 마법사를 시작합니다.
2. 다음 _ 을(를) 선택합니다. 대상 폴더 대화 상자가 열립니다.
3. 목록에 있는 폴더에 Antivirus Connector를 설치하려면 _Next_를 선택하고 다른 폴더에 설치하려면 _Change_를 선택하십시오.
4. ONTAP AV 커넥터 Windows 서비스 자격 증명 대화 상자가 열립니다.
5. Windows 서비스 자격 증명을 입력하거나 * 추가 * 를 선택하여 사용자를 선택합니다. ONTAP 시스템의 경우 이 사용자는 유효한 도메인 사용자여야 하며 SVM의 스캐너 풀 구성에 있어야 합니다.
6. 다음 * 을 선택합니다. 프로그램 설치 준비 완료 대화 상자가 열립니다.

7. 설치를 시작하려면 * 설치 * 를 선택하고 설정을 변경하려면 * 뒤로 * 를 선택하십시오.
상태 상자가 열리고 설치 진행률을 차트로 표시한 다음 InstallShield 마법사 완료 대화 상자가 나타납니다.
8. ONTAP 관리 또는 데이터 LIF 구성을 계속하려면 ONTAP LIF 구성 확인란을 선택합니다.
이 Vscan 서버를 사용하려면 먼저 하나 이상의 ONTAP 관리 또는 데이터 LIF를 구성해야 합니다.
9. 설치 로그를 보려면 * Windows Installer 로그 표시 * 확인란을 선택합니다.
10. 설치를 종료하고 InstallShield 마법사를 닫으려면 * 마침 * 을 선택하십시오.
ONTAP LIF 구성 * 아이콘이 바탕 화면에 저장되어 ONTAP LIF를 구성합니다.
11. 바이러스 백신 커넥터에 SVM을 추가합니다.
데이터 LIF 목록을 검색하기 위해 폴링되는 ONTAP 관리 LIF를 추가하거나 데이터 LIF 또는 LIF를 직접 구성하여 SVM을 바이러스 백신 커넥터에 추가할 수 있습니다.
ONTAP 관리 LIF가 구성된 경우 폴링 정보와 ONTAP 관리자 계정 자격 증명도 제공해야 합니다.
    - 에 대해 관리 LIF 또는 SVM의 IP 주소가 활성화되었는지 확인합니다 `management-https`. 데이터 LIF만 구성하는 경우에는 이러한 변경이 필요하지 않습니다.
    - HTTP 응용 프로그램에 대한 사용자 계정을 만들고 REST API에 대한 액세스(읽기 전용) 권한이 있는 역할을 할당했는지 확인합니다 `/api/network/ip/interfaces`.
    - 및 `security login create` 에 대한 자세한 `security login role create` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

> 관리 SVM에 대한 인증 터널 SVM을 추가하여 도메인 사용자를 계정으로 사용할 수도 있습니다. 에 대한 자세한 내용은 `security login domain-tunnel create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 안티바이러스 커넥터 설치를 완료하면 바탕 화면에 저장된 * ONTAP LIF 구성 * 아이콘을 마우스 오른쪽 단추로 클릭한 다음 * 관리자 권한으로 실행 * 을 선택합니다.
2. ONTAP LIF 구성 대화 상자에서 기본 구성 유형을 선택하고 다음 작업을 수행합니다.

이 유형의 LIF를 생성하려면…	다음 단계를 수행합니다.
데이터 LIF	a. "역할"을 "데이터"로 설정 b. "데이터 프로토콜"을 "CIFS"로 설정합니다. c. "방화벽 정책"을 "데이터"로 설정합니다. d. "서비스 정책"을 "default-data-files"로 설정합니다.
관리 LIF	a. "역할 * 을 "데이터"로 설정 b. "데이터 프로토콜"을 "없음"으로 설정합니다. c. "방화벽 정책"을 "관리"로 설정 d. "서비스 정책"을 "default-management"로 설정합니다.

에 대해 자세히 "LIF 생성"알아보세요.

LIF를 생성한 후 추가하려는 SVM의 데이터 또는 관리 LIF 또는 IP 주소를 입력합니다. 클러스터 관리 LIF를 입력할 수도 있습니다. 클러스터 관리 LIF를 지정하면 SMB를 제공하는 클러스터 내의 모든 SVM이 Vscan 서버를 사용할

수 있습니다.

> Vscan 서버에 Kerberos 인증이 필요한 경우 각 SVM 데이터 LIF는 고유한 DNS 이름을 가져야 하며, Windows Active Directory에 SPN(Server Principal Name)으로 등록해야 합니다. 각 데이터 LIF에 대해 고유한 DNS 이름을 사용할 수 없거나 SPN으로 등록된 경우 Vscan 서버는 NT LAN Manager 메커니즘을 사용하여 인증을 수행합니다. Vscan 서버가 연결된 후 DNS 이름 및 SPN을 추가하거나 수정하는 경우 변경 사항을 적용하려면 Vscan 서버에서 Antivirus Connector 서비스를 다시 시작해야 합니다.

3. 관리 LIF를 구성하려면 폴링 기간을 초 단위로 입력합니다. 폴링 기간은 Antivirus Connector가 SVM 또는 클러스터의 LIF 구성의 변경 사항을 확인하는 빈도입니다. 기본 폴링 간격은 60초입니다.
4. 관리 LIF를 구성하려면 ONTAP admin 계정 이름 및 암호를 입력합니다.
5. Test * 를 클릭하여 연결을 확인하고 인증을 확인합니다. 관리 LIF 구성에 대해서만 인증이 검증됩니다.
6. 업데이트 * 를 클릭하여 폴링하거나 연결할 LIF 목록에 LIF를 추가합니다.
7. 저장 * 을 클릭하여 레지스트리에 대한 연결을 저장합니다.
8. 연결 목록을 레지스트리 가져오기 또는 레지스트리 내보내기 파일로 내보내려면 * 내보내기 * 를 클릭합니다. 여러 Vscan 서버가 동일한 관리 또는 데이터 LIF 세트를 사용하는 경우 이 기능이 유용합니다.

를 참조하십시오 "ONTAP 안티바이러스 커넥터 페이지를 구성합니다" 를 클릭합니다.

ONTAP Vscan Antivirus 커넥터 구성

ONTAP 관리 LIF, 폴링 정보 및 ONTAP 관리자 계정 자격 증명을 입력하거나 데이터 LIF만 입력하여 연결하려는 하나 이상의 SVM(스토리지 가상 머신)을 지정하도록 ONTAP 바이러스 백신 커넥터를 구성합니다. SVM 연결의 세부 정보를 수정하거나 SVM 연결을 제거할 수도 있습니다. 기본적으로 ONTAP 바이러스 백신 커넥터는 ONTAP 관리 LIF가 구성된 경우 REST API를 사용하여 데이터 LIF 목록을 검색합니다.

SVM 연결의 세부 정보를 수정합니다

ONTAP 관리 LIF 및 폴링 정보를 수정하여 안티바이러스 커넥터에 추가된 SVM(스토리지 가상 머신) 연결의 세부 정보를 업데이트할 수 있습니다. 데이터 LIF를 추가한 후에는 업데이트할 수 없습니다. 데이터 LIF를 업데이트하려면 먼저 이러한 LIF를 제거한 다음 새 LIF 또는 IP 주소를 사용하여 다시 추가해야 합니다.

시작하기 전에

HTTP 응용 프로그램에 대한 사용자 계정을 만들고 REST API에 대한 액세스(읽기 전용) 권한이 있는 역할을 할당했는지 확인합니다 `/api/network/ip/interfaces`.

및 `security login create` 에 대한 자세한 `security login role create` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

관리 SVM에 대한 인증 터널 SVM을 추가하여 도메인 사용자를 계정으로 사용할 수도 있습니다. 에 대한 자세한 내용은 `security login domain-tunnel create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 안티바이러스 커넥터 설치를 완료하면 바탕 화면에 저장된 * ONTAP LIF 구성 * 아이콘을 마우스 오른쪽 단추로 클릭한 다음 * 관리자 권한으로 실행 * 을 선택합니다. ONTAP LIF 구성 대화 상자가 열립니다.

2. SVM IP 주소를 선택한 다음 * Update * 를 클릭합니다.
3. 필요에 따라 정보를 업데이트합니다.
4. 저장 * 을 클릭하여 레지스트리에서 연결 세부 정보를 업데이트합니다.
5. 연결 목록을 레지스트리 가져오기 또는 레지스트리 내보내기 파일로 내보내려면 * 내보내기 * 를 클릭합니다. 여러 Vscan 서버가 동일한 관리 또는 데이터 LIF 세트를 사용하는 경우 이 기능이 유용합니다.

안티바이러스 커넥터에서 **SVM** 연결을 제거합니다

더 이상 SVM 연결이 필요하지 않은 경우 제거할 수 있습니다.

단계

1. 안티바이러스 커넥터 설치를 완료하면 바탕 화면에 저장된 * ONTAP LIF 구성 * 아이콘을 마우스 오른쪽 단추로 클릭한 다음 * 관리자 권한으로 실행 * 을 선택합니다. ONTAP LIF 구성 대화 상자가 열립니다.
2. 하나 이상의 SVM IP 주소를 선택한 다음 * 제거 * 를 클릭합니다.
3. 저장 * 을 클릭하여 레지스트리에서 연결 세부 정보를 업데이트합니다.
4. 연결 목록을 레지스트리 가져오기 또는 레지스트리 내보내기 파일로 내보내려면 * 내보내기 * 를 클릭합니다. 여러 Vscan 서버가 동일한 관리 또는 데이터 LIF 세트를 사용하는 경우 이 기능이 유용합니다.

문제 해결

시작하기 전에

이 절차에서 레지스트리 값을 만들 때는 오른쪽 창을 사용합니다.

진단 목적으로 바이러스 백신 커넥터 로그를 활성화하거나 비활성화할 수 있습니다. 기본적으로 이러한 로그는 비활성화되어 있습니다. 성능을 향상시키려면 Antivirus Connector 로그를 사용하지 않도록 설정하고 중요 이벤트에 대해서만 활성화해야 합니다.

단계

1. 시작 * 을 선택하고 검색 상자에 "regedit"를 입력한 다음 를 선택합니다 `regedit.exe` 를 선택합니다.
2. 레지스트리 편집기 * 에서 ONTAP 안티바이러스 커넥터의 다음 하위 키를 찾습니다. `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 다음 표에 나와 있는 형식, 이름 및 값을 제공하여 레지스트리 값을 만듭니다.

유형	이름	값
문자열	Tracepath(추적 경로)	C:\avshim.log 으로 문의하십시오

   이 레지스트리 값은 다른 유효한 경로일 수 있습니다.

4. 다음 표에 나와 있는 형식, 이름, 값 및 로깅 정보를 제공하여 다른 레지스트리 값을 만듭니다.

유형	이름	중요한 로깅	중간 로깅	자세한 로깅
DWORD를 클릭합니다	TraceLevel 을 선택합니다	1	2 또는 3	4

이렇게 하면 3단계의 TracePath에 제공된 경로 값으로 저장되는 Antivirus Connector 로그가 활성화됩니다.

5. 3단계와 4단계에서 만든 레지스트리 값을 삭제하여 Antivirus Connector 로그를 비활성화합니다.
6. 이름이 "LogRotation"(따옴표 제외)인 "multi_sz" 유형의 다른 레지스트리 값을 만듭니다. "LogRotation"에서 회전 크기 항목으로 "logFileSize:1"을 제공하고(1은 1MB를 나타냄) 다음 줄에서는 로 "logFileCount:5"를 제공합니다
   회전 한계 입력(5가 한계)

   이러한 값은 선택 사항입니다. 이 옵션이 제공되지 않으면 회전 크기 및 회전 제한에 각각 20MB와 10개의 파일이 사용됩니다. 제공된 정수 값은 10진수 또는 분수 값을 제공하지 않습니다. 기본값보다 높은 값을 제공하면 기본값이 대신 사용됩니다.

7. 사용자 구성 로그 회전을 사용하지 않으려면 6단계에서 만든 레지스트리 값을 삭제합니다.

사용자 지정 가능한 배너

사용자 지정 배너를 사용하면 _ Configure ONTAP LIF api_ 창에 법적 구속력 있는 문구와 시스템 액세스 고지 사항을 배치할 수 있습니다.

단계

1. 의 내용을 업데이트하여 기본 배너를 수정합니다 `banner.txt` 파일을 설치 디렉토리에 저장한 다음 변경 내용을 저장합니다.
   배너에 반영된 변경 사항을 보려면 Configure ONTAP LIF API 창을 다시 열어야 합니다.

확장 조례**(EO)** 모드를 활성화합니다

보안 작동을 위해 EO(Extended Ordinance) 모드를 활성화하거나 비활성화할 수 있습니다.

단계

1. 시작 * 을 선택하고 검색 상자에 "regedit"를 입력한 다음 를 선택합니다 `regedit.exe` 를 선택합니다.
2. 레지스트리 편집기 * 에서 ONTAP 안티바이러스 커넥터의 다음 하위 키를 찾습니다.
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 오른쪽 창에서 "DWORD" 유형의 새 레지스트리 값을 만들어 EO 모드를 사용하지 않도록 설정하려면 "EO_Mode"(따옴표 제외) 및 값 "1"(따옴표 제외)을 사용합니다.

   기본적으로 이 인 경우 `EO_Mode` 레지스트리 항목이 없습니다. EO 모드가 비활성화됩니다. EO 모드를 활성화할 때 외부 syslog 서버와 상호 인증서 인증을 모두 구성해야 합니다.

외부 **syslog** 서버를 구성합니다

시작하기 전에

이 절차에서 레지스트리 값을 만들 때는 오른쪽 창을 사용합니다.

단계

1. 시작 * 을 선택하고 검색 상자에 "regedit"를 입력한 다음 를 선택합니다 `regedit.exe` 를 선택합니다.
2. 레지스트리 편집기 * 에서 syslog 구성에 대한 ONTAP 안티바이러스 커넥터 하위 키를 생성합니다.
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP`

```
Antivirus Connector\v1.0\syslog
```

3. 다음 표와 같이 유형, 이름 및 값을 제공하여 레지스트리 값을 만듭니다.

유형	이름	값
DWORD를 클릭합니다	syslog_enabled	1 또는 0

"1" 값은 syslog를 활성화하고 "0" 값은 syslog를 비활성화합니다.

4. 다음 표에 표시된 정보를 제공하여 다른 레지스트리 값을 만듭니다.

유형	이름
등록_SZ	syslog_host입니다

값 필드에 syslog 호스트 IP 주소 또는 도메인 이름을 입력합니다.

5. 다음 표에 표시된 정보를 제공하여 다른 레지스트리 값을 만듭니다.

유형	이름
등록_SZ	syslog_port

값 필드에 syslog 서버가 실행 중인 포트 번호를 제공합니다.

6. 다음 표에 표시된 정보를 제공하여 다른 레지스트리 값을 만듭니다.

유형	이름
등록_SZ	Syslog_프로토콜

syslog 서버에서 사용 중인 프로토콜을 값 필드에 "TCP" 또는 "UDP"로 입력합니다.

7. 다음 표에 표시된 정보를 제공하여 다른 레지스트리 값을 만듭니다.

유형	이름	로그_CRIT	로그_통지	Log_Info(로그 정보)	log_debug 를 참조하십시오
DWORD를 클릭합니다	syslog_레벨	2	5	6	7

8. 다음 표에 표시된 정보를 제공하여 다른 레지스트리 값을 만듭니다.

유형	이름	값
DWORD를 클릭합니다	Syslog_TLS	1 또는 0

"1" 값은 TLS(Transport Layer Security)를 사용하여 syslog를 활성화하고 "0" 값은 TLS를 사용하는 syslog를 비활성화합니다.

구성된 외부 **syslog** 서버가 원활하게 실행되는지 확인합니다

- 키가 없거나 null 값이 있는 경우:
  - 프로토콜은 기본적으로 "TCP"로 설정됩니다.
  - 일반 "TCP/UDP"의 경우 기본적으로 "514"이고 TLS의 경우 기본적으로 "6514"입니다.
  - syslog 레벨의 기본값은 5(log_notice)입니다.
- syslog가 활성화되어 있는지 확인하려면 를 확인하십시오 `syslog_enabled` 값은 "1"입니다. 를 누릅니다 `syslog_enabled` 값은 "1"입니다. EO 모드의 활성화 여부에 관계없이 구성된 원격 서버에 로그인할 수 있어야 합니다.
- EO 모드가 "1"로 설정된 경우 를 변경합니다 `syslog_enabled` "1"에서 "0"까지의 값은 다음과 같습니다.
  - EO 모드에서 syslog가 활성화되지 않은 경우 서비스를 시작할 수 없습니다.
  - 시스템이 안정 상태에서 실행 중인 경우, EO 모드에서 syslog를 비활성화할 수 없으며 syslog가 강제로 "1"로 설정된다는 경고가 나타납니다. 이 경고는 레지스트리에서 확인할 수 있습니다. 이 경우 먼저 EO 모드를 비활성화한 다음 syslog를 비활성화해야 합니다.
- EO 모드 및 syslog를 사용할 때 syslog 서버가 성공적으로 실행되지 않으면 서비스 실행이 중지됩니다. 이 문제는 다음과 같은 이유 중 하나로 인해 발생할 수 있습니다.
  - 유효하지 않거나 syslog_host가 구성되지 않았습니다.
  - UDP 또는 TCP와 별도로 잘못된 프로토콜이 구성되었습니다.
  - 포트 번호가 잘못되었습니다.
- TCP 또는 TLS over TCP 구성의 경우 서버가 IP 포트에서 수신 대기하지 않으면 연결이 실패하고 서비스가 종료됩니다.

X.509 상호 인증서 인증을 구성합니다

X.509 인증서 기반 상호 인증은 관리 경로에서 바이러스 백신 커넥터와 ONTAP 간의 SSL(Secure Sockets Layer) 통신에 사용할 수 있습니다. EO 모드가 활성화되어 있고 인증서를 찾을 수 없는 경우 AV 커넥터가 종료됩니다. 안티바이러스 커넥터에 대해 다음 절차를 수행하십시오.

단계

1. 안티바이러스 커넥터는 안티바이러스 커넥터가 설치 디렉토리를 실행하는 디렉토리 경로에서 NetApp 서버의 안티바이러스 커넥터 클라이언트 인증서 및 CA(인증 기관) 인증서를 검색합니다. 인증서를 이 고정 디렉토리 경로에 복사합니다.
2. 클라이언트 인증서와 개인 키를 PKCS12 형식으로 포함하고 이름을 "AV_CLIENT.P12"로 지정합니다.
3. NetApp 서버의 인증서에 서명하는 데 사용된 CA 인증서(루트 CA까지의 모든 중간 서명 기관 포함)가 PEM(Privacy Enhanced Mail) 형식이고 "Ontap_CA.pem"이라는 이름을 가지고 있는지 확인하세요. Antivirus Connector 설치 디렉토리에 넣으세요. ONTAP 시스템에서 "ONTAP"의 Antivirus Connector에 대한 클라이언트 인증서에 서명하는 데 사용되는 CA 인증서(루트 CA까지의 모든 중간 서명 기관 포함)를 "client-ca" 유형 인증서로 설치합니다.

스캐너 풀을 구성합니다

ONTAP Vscan 스캐너 풀 구성에 대해 알아보세요

스캐너 풀은 SVM에 연결할 수 있는 Vscan 서버 및 특별 권한 사용자를 정의합니다. 스캐너 정책은 스캐너 풀이 활성 상태인지 여부를 결정합니다.

SMB 서버에서 내보내기 정책을 사용하는 경우 각 Vscan 서버를 엑스포트 정책에 추가해야 합니다.

단일 클러스터에 **ONTAP Vscan** 스캐너 풀을 만듭니다**.**

스캐너 풀은 SVM에 연결할 수 있는 Vscan 서버 및 특별 권한 사용자를 정의합니다.

시작하기 전에

- SVM과 Vscan 서버는 동일한 도메인 또는 신뢰할 수 있는 도메인에 있어야 합니다.
- 클러스터 관리 LIF를 사용하여 ONTAP 바이러스 백신 커넥터를 구성합니다.
- 권한이 있는 사용자 목록에는 Vscan 서버가 SVM에 연결하는 데 사용하는 도메인 및 사용자 이름이 포함되어야 합니다.
- 스캐너 풀이 구성되면 서버에 대한 연결 상태를 확인합니다.

단계

1. 스캐너 풀 생성:

   ```
   vserver vscan scanner-pool create -vserver cluster_admin_SVM -scanner-pool
   scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - 클러스터 관리자 SVM을 지정합니다.
   - 각 Vscan 서버 호스트 이름에 대한 IP 주소 또는 FQDN을 지정합니다.
   - 권한이 있는 각 사용자의 도메인 및 사용자 이름을 지정합니다.

   에 대한 자세한 내용은 `vserver vscan scanner-pool create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 스캐너 풀이 생성되었는지 확인합니다.

   ```
   vserver vscan scanner-pool show -vserver cluster_admin_SVM -scanner-pool
   scanner_pool
   ```

   다음 명령을 실행하면 'S' 스캐너 풀에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan scanner-pool show -vserver cluster_admin_SVM
-scanner-pool SP

                                    Vserver: cluster_admin_SVM
                                Scanner Pool: SP
                              Applied Policy: idle
                              Current Status: off
          Cluster on Which Policy Is Applied: -
                   Scanner Pool Config Owner: cluster
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                    List of Privileged Users: cifs\u1, cifs\u2
```

명령을 사용하여 클러스터의 모든 스캐너 풀을 볼 수도 `vserver vscan scanner-pool show` 있습니다. 에 대한 자세한 내용은 `vserver vscan scanner-pool show` "ONTAP 명령 참조입니다"을 참조하십시오.

MetroCluster 구성에서 **ONTAP Vscan** 스캐너 풀 생성

클러스터의 운영 및 2차 SVM에 해당하는 MetroCluster 구성의 각 클러스터에 기본 및 2차 스캐너 풀을 생성해야 합니다.

시작하기 전에

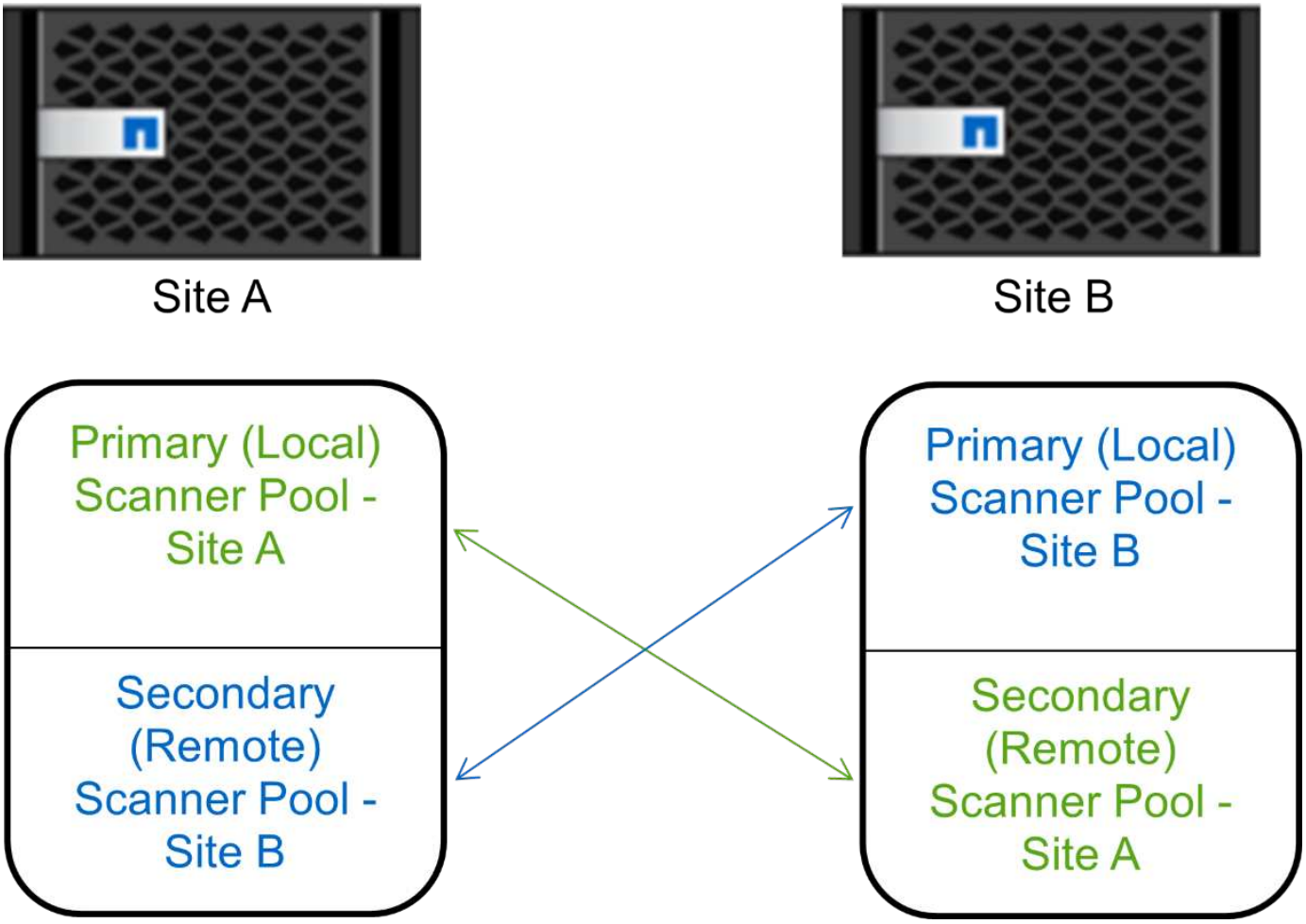
- SVM과 Vscan 서버는 동일한 도메인 또는 신뢰할 수 있는 도메인에 있어야 합니다.
- 개별 SVM용으로 정의된 스캐너 풀의 경우 ONTAP 바이러스 백신 커넥터를 SVM 관리 LIF 또는 SVM 데이터 LIF와 함께 구성해야 합니다.
- 클러스터의 모든 SVM에 대해 정의된 스캐너 풀의 경우 클러스터 관리 LIF에서 ONTAP 바이러스 백신 커넥터를 구성해야 합니다.
- 권한이 있는 사용자 목록에는 Vscan 서버가 SVM에 연결하는 데 사용하는 도메인 사용자 계정이 포함되어야 합니다.
- 스캐너 풀이 구성되면 서버에 대한 연결 상태를 확인합니다.

이 작업에 대해

MetroCluster 구성은 물리적으로 분리된 2개의 미러링된 클러스터를 구현하여 데이터를 보호합니다. 각 클러스터는 다른 클러스터의 데이터와 SVM 구성을 동기식으로 복제합니다. 로컬 클러스터의 1차 SVM은 클러스터가 온라인 상태일 때 데이터를 제공합니다. 로컬 클러스터의 2차 SVM은 원격 클러스터가 오프라인일 때 데이터를 제공합니다.

즉, MetroCluster 구성에서 각 클러스터에 기본 및 보조 스캐너 풀을 생성해야 하며, 클러스터가 2차 SVM에서 데이터 제공을 시작하면 2차 풀이 활성화됩니다. DR(재해 복구)의 경우 구성은 MetroCluster와 비슷합니다.

이 그림은 일반적인 MetroCluster/DR 구성을 보여 줍니다.



단계

1. 스캐너 풀 생성:

   'vserver vscan scanner -pool create -vserver_data_SVM|cluster_admin_SVM_-scanner -pool_scanner_pool_-hostname_vscan_server_hostname_-privileged-users_privileged_users_'

   - 개별 SVM용으로 정의된 풀에 대해 데이터 SVM을 지정하고, 클러스터의 모든 SVM에 대해 정의된 풀에 대해 클러스터 관리 SVM을 지정합니다.
   - 각 Vscan 서버 호스트 이름에 대한 IP 주소 또는 FQDN을 지정합니다.
   - 권한이 있는 각 사용자의 도메인 및 사용자 이름을 지정합니다.

   운영 SVM이 포함된 클러스터에서 모든 스캐너 풀을 생성해야 합니다.

   에 대한 자세한 내용은 `vserver vscan scanner-pool create` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 MetroCluster 구성의 각 클러스터에 운영 및 2차 스캐너 풀이 생성됩니다.

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. 스캐너 풀이 생성되었는지 확인합니다.

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   다음 명령을 실행하면 스캐너 풀 'pool1'에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: idle
                              Current Status: off
         Cluster on Which Policy Is Applied: -
                   Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

   또한 명령을 사용하여 SVM에 있는 모든 스캐너 풀을 볼 수도 있습니다 `vserver vscan scanner-pool show`. 에 대한 자세한 내용은 `vserver vscan scanner-pool show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP Vscan을 사용하여 단일 클러스터에 스캐너 정책 적용

스캐너 정책은 스캐너 풀이 활성 상태인지 여부를 결정합니다. 정의된 Vscan 서버가 SVM에 연결할 수 있으려면 먼저 스캐너 풀을 활성화해야 합니다.

이 작업에 대해

- 스캐너 풀에는 하나의 스캐너 정책만 적용할 수 있습니다.
- 클러스터에서 모든 SVM에 대해 스캐너 풀을 생성한 경우 각 SVM에 개별적으로 스캐너 정책을 적용해야 합니다.

단계

1. 스캐너 정책 적용:

   'vserver vscan scanner -pool apply -policy -vserver data_SVM -scanner -pool scanner_pool -scanner -policy primary | secondary|idle -cluster cluster_to_apply_policy_on'

   스캐너 정책은 다음 값 중 하나를 가질 수 있습니다.

   - "기본"은 스캐너 풀이 활성화되도록 지정합니다.
   - '2차'는 기본 스캐너 풀에 Vscan 서버가 연결되어 있지 않은 경우에만 스캐너 풀이 활성화되도록 지정합니다.
   - "유휴"는 스캐너 풀이 비활성 상태라고 지정합니다.

     다음 예제는 이름이 인 스캐너 풀을 보여 줍니다 `SP` 를 누릅니다 `vs1` SVM 활성화:

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP  -scanner-policy primary
```

2. 스캐너 풀이 활성화되었는지 확인합니다.

   'vserver vscan scanner -pool show -vserver data_SVM|cluster_admin_SVM-scanner -pool scanner_pool'

   이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

   다음 명령을 실행하면 'S' 스캐너 풀에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                               Scanner Pool: SP
                             Applied Policy: primary
                             Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                     List of Privileged Users: cifs\u1, cifs\u2
```

   명령을 사용하여 SVM에서 활성 스캐너 풀을 볼 수 있습니다 `vserver vscan scanner-pool show-active`. 에 대한 자세한 내용은 `vserver vscan scanner-pool show-active` "ONTAP 명령 참조입니다"을 참조하십시오.

MetroCluster ONTAP Vscan 구성에 스캐너 정책 적용

스캐너 정책은 스캐너 풀이 활성 상태인지 여부를 결정합니다. MetroCluster 구성에서 각 클러스터의 기본 및 보조 스캐너 풀에 스캐너 정책을 적용해야 합니다.

이 작업에 대해

- 스캐너 풀에는 하나의 스캐너 정책만 적용할 수 있습니다.
- 클러스터에서 모든 SVM에 대해 스캐너 풀을 생성한 경우 각 SVM에 개별적으로 스캐너 정책을 적용해야 합니다.
- 재해 복구 및 MetroCluster 구성의 경우 로컬 클러스터 및 원격 클러스터의 모든 스캐너 풀에 스캐너 정책을 적용해야 합니다.
- 로컬 클러스터에 대해 생성하는 정책에서 에서 로컬 클러스터를 지정해야 합니다 `cluster` 매개 변수. 원격 클러스터에 대해 생성한 정책에서 에서 원격 클러스터를 지정해야 합니다 `cluster` 매개 변수. 그런 다음 재해 발생 시 원격 클러스터가 바이러스 검사 작업을 대신 수행할 수 있습니다.

단계

1. 스캐너 정책 적용:

   'vserver vscan scanner -pool apply -policy -vserver_data_SVM_ -scanner -pool_scanner_pool_ -scanner -policy primary|secondary|idle -cluster_cluster_to_apply_policy_on_'

   에 대한 자세한 내용은 `vserver vscan scanner-pool apply-policy` "ONTAP 명령 참조입니다"을 참조하십시오.

   스캐너 정책은 다음 값 중 하나를 가질 수 있습니다.

   - "기본"은 스캐너 풀이 활성화되도록 지정합니다.
   - '2차'는 기본 스캐너 풀에 Vscan 서버가 연결되어 있지 않은 경우에만 스캐너 풀이 활성화되도록 지정합니다.
   - "유휴"는 스캐너 풀이 비활성 상태라고 지정합니다.

   > ⓘ 운영 SVM이 포함된 클러스터에서 모든 스캐너 정책을 적용해야 합니다.

   다음 명령은 MetroCluster 구성에서 각 클러스터의 기본 및 보조 스캐너 풀에 스캐너 정책을 적용합니다.

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. 스캐너 풀이 활성화되었는지 확인합니다.

   'vserver vscan scanner -pool show -vserver data_SVM|cluster_admin_SVM-scanner -pool scanner_pool'

   에 대한 자세한 내용은 `vserver vscan scanner-pool show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 스캐너 풀 'pool1'에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: primary
                              Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

   명령을 사용하여 SVM에서 활성 스캐너 풀을 볼 수 있습니다 `vserver vscan scanner-pool show-active`. 에 대한 자세한 내용은 `vserver vscan scanner-pool show-active` "ONTAP 명령 참조입니다"을 참조하십시오.

Vscan에서 스캐너 풀을 관리하기 위한 **ONTAP** 명령

스캐너 풀을 수정 및 삭제하고, 스캐너 풀의 권한이 있는 사용자와 Vscan 서버를 관리할 수 있습니다. 스캐너 풀에 대한 요약 정보도 볼 수 있습니다.

원하는 작업	다음 명령을 입력합니다...

스캐너 풀을 수정합니다	'vserver vscan scanner-pool modify(가상 Vscan 스캐너 풀 수정)
스캐너 풀을 삭제합니다	'vserver vscan scanner -pool delete'(Vscan scanner -pool 삭제
스캐너 풀에 권한이 있는 사용자를 추가합니다	'vserver vscan scanner-pool privileged-users add'
스캐너 풀에서 권한이 있는 사용자를 삭제합니다	'vserver vscan scanner-pool privileged-users remove'(Vscan scanner-
Vscan 서버를 스캐너 풀에 추가합니다	'vserver vscan scanner-pool servers add'
스캐너 풀에서 Vscan 서버를 삭제합니다	'vserver vscan scanner-pool servers remove(Vscan scanner-pool 서버
스캐너 풀에 대한 요약 및 세부 정보를 봅니다	'vserver vscan scanner-pool show'
스캐너 풀에 대한 권한이 있는 사용자를 봅니다	'vserver vscan scanner-pool privileged-users show'(Vscan scanner-pool
모든 스캐너 풀에 대한 Vscan 서버를 봅니다	'vserver vscan scanner-pool servers show'

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

액세스 시 스캔을 구성합니다

ONTAP Vscan 온액세스 정책 생성

액세스 시 정책은 액세스 시 검사의 범위를 정의합니다. 개별 SVM 또는 클러스터의 모든 SVM에 대해 액세스 시 정책을 생성할 수 있습니다. 클러스터에서 모든 SVM에 대해 액세스 시 정책을 생성한 경우 각 SVM에 대해 개별적으로 정책을 활성화해야 합니다.

이 작업에 대해

- 스캔할 최대 파일 크기, 스캔에 포함할 파일 확장명 및 경로, 스캔에서 제외할 파일 확장명 및 경로를 지정할 수 있습니다.
- 바이러스 검사를 위해 Vscan 서버를 사용할 수 없는 경우 파일 액세스가 허용되도록 '스캔 필수' 옵션을 꺼짐으로 설정할 수 있습니다.
- 기본적으로 ONTAP는 "default_cifs"라는 액세스 시 정책을 생성하고 클러스터에 있는 모든 SVM에 대해 활성화합니다.
- 에 따라 스캔 제외 대상이 되는 모든 파일 `paths-to-exclude`, `file-ext-to-exclude`, 또는 `max-file-size` 매개 변수는 에도 스캔 대상으로 고려되지 않습니다 `scan-mandatory` 옵션이 켜짐으로 설정되어 있습니다. (이것을 확인하십시오 "문제 해결" 과 관련된 연결 문제에 대한 섹션입니다 `scan-mandatory` 옵션)
- 기본적으로 읽기-쓰기 볼륨만 스캔됩니다. 읽기 전용 볼륨을 스캔할 수 있도록 하거나 실행 권한으로 연 파일로 스캔을 제한하는 필터를 지정할 수 있습니다.

- 지속적으로 사용 가능한 매개 변수가 Yes로 설정된 SMB 공유에서는 바이러스 검사가 수행되지 않습니다.
- 를 참조하십시오 "안티바이러스 아키텍처" Vscan 파일 - 작업 프로필 _ 에 대한 자세한 내용은 섹션을 참조하십시오.
- SVM당 최대 10개의 액세스 정책을 생성할 수 있습니다. 그러나 한 번에 하나의 온액세스 정책만 활성화할 수 있습니다.
  - 액세스 시 정책에서 바이러스 검사에서 최대 100개의 경로 및 파일 확장명을 제외할 수 있습니다.
- 일부 파일 제외 권장 사항:
  - CIFS 사용자에 대한 응답 속도가 느려지거나 스캔 요청 시간 초과가 발생할 수 있으므로 바이러스 검사에서 큰 파일(파일 크기를 지정할 수 있음)을 제외하는 것이 좋습니다. 제외의 기본 파일 크기는 2GB입니다.
  - 과 같은 파일 확장명을 제외하는 것이 좋습니다 `.vhd` 및 `.tmp` 이러한 확장자가 있는 파일은 스캔에 적합하지 않을 수 있기 때문입니다.
  - 격리 디렉터리나 가상 하드 드라이브 또는 데이터베이스만 저장되는 경로와 같은 파일 경로를 제외하는 것이 좋습니다.
  - 한 번에 하나의 정책만 활성화할 수 있으므로 모든 제외가 동일한 정책에 지정되어 있는지 확인합니다. NetApp는 바이러스 백신 엔진에 지정된 것과 동일한 제외 세트를 사용할 것을 적극 권장합니다.
  - ONTAP 9.14.1부터 와일드카드를 사용하여 제외할 액세스 시 경로 및 파일 확장자를 지정할 수 있습니다.
- 의 경우 액세스 시 정책이 필요합니다 온디맨드 검사. 에 대한 액세스 시 스캔을 방지하려면 을 설정해야 합니다 `-scan-files-with-no-ext` 버튼을 눌러 false로 이동하고 `-file-ext-to-exclude` 모든 확장자를 제외하려면 * 를 선택합니다.

단계

1. 액세스 시 정책 생성:

   'vserver vscan on-access-policy create -vserver_data_SVM|cluster_admin_SVM_-policy -name_policy_name_-protocol cifs-max-file-size_max_size_of_files_to_scan_ – filters [scan-ro-volume,] [scan-execute-access] -file-ext-to -include_ext_ext_ext_ext_exclude_ext_ext_exclude_ext_ext_ext_ext_exclude_exclude_ext_ext_exclude_file_exclude_file_file_scan_exclude_exclude_exclude_file_file_file_file_file_file_max-max_max-max-max-max-max_

   - 개별 SVM에 정의된 정책에 따라 데이터 SVM을 지정하고, 클러스터의 모든 SVM에 정의된 정책에 따라 클러스터 관리 SVM을 지정합니다.
   - '-file-ext-to-exclude' 설정은 '-file-ext-to-include' 설정보다 우선합니다.
   - 설정 `-scan-files-with-no-ext` 를 true로 설정하면 확장자가 없는 파일을 스캔할 수 있습니다. 다음 명령을 실행하면 이라는 온액세스 정책이 생성됩니다 `Policy1` 를 누릅니다 `vs1` SVM:

   ```
   cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
   -name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
   -file-ext-to-include "mp*","tx*" -file-ext-to-exclude "mp3","txt" -scan
   -files-with-no-ext false -paths-to-exclude "\vol\a b\","\vol\a,b\"
   ```

2. 다음과 같이 on-access 정책이 생성되었는지 확인합니다. `vserver vscan on-access-policy show -instance` *`data_SVM|cluster_admin_SVM`* `-policy-name` *`name`*

에 대한 자세한 내용은 `vserver vscan on-access-policy` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 Policy1 정책에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                            Vserver: vs1
                             Policy: Policy1
                      Policy Status: off
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
             File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

ONTAP Vscan 온액세스 정책 활성화

액세스 시 정책은 액세스 시 검사의 범위를 정의합니다. SVM의 파일을 스캔하려면 먼저 SVM에서 액세스 시 정책을 활성화해야 합니다.

클러스터에서 모든 SVM에 대해 액세스 시 정책을 생성한 경우 각 SVM에 대해 개별적으로 정책을 활성화해야 합니다. 한 번에 하나의 SVM에 대해 액세스 시 정책만 활성화할 수 있습니다.

단계

1. 액세스 시 정책 활성화:

   'vserver vscan on-access-policy enable-vserver data_SVM-policy-name policy_name'

   다음 명령을 실행하면 이라는 온액세스 정책이 설정됩니다 `Policy1` 를 누릅니다 `vs1` SVM:

   ```
   cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
   -name Policy1
   ```

2. 액세스 시 정책이 활성화되어 있는지 확인합니다.

   `vserver vscan on-access-policy show -instance` *`data_SVM`* `-policy-name` *`policy_name`*

   에 대한 자세한 내용은 `vserver vscan on-access-policy show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 "Policy1" 액세스 시 정책에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                            Vserver: vs1
                             Policy: Policy1
                      Policy Status: on
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
             File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

SMB 공유에 대한 **ONTAP Vscan** 파일 작업 프로필 수정

SMB 공유의 _ Vscan 파일 작업 프로필 _ 은(는) 스캔을 트리거할 수 있는 공유 작업을 정의합니다. 기본적으로 매개 변수는 로 설정됩니다 `standard`. SMB 공유를 생성하거나 수정할 때 필요에 따라 매개 변수를 조정할 수 있습니다.

를 참조하십시오 "안티바이러스 아키텍처" Vscan 파일 - 작업 프로필 _ 에 대한 자세한 내용은 섹션을 참조하십시오.

> 가 있는 SMB 공유에서는 바이러스 검사가 수행되지 않습니다 `continuously-available` 매개 변수를 로 설정합니다 `Yes`.

단계

1. SMB 공유에 대한 Vscan 파일 작업 프로필의 값을 수정합니다.

   `vserver cifs share modify -vserver` *`data_SVM`* `-share-name` *`share`* `-path` *`share_path`* `-vscan-fileop-profile no-scan|standard|strict|writes-only`

   에 대한 자세한 내용은 `vserver cifs share modify` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 SMB 공유에 대한 Vscan 파일 작업 프로필이 로 변경됩니다 `strict`:

   ```
   cluster1::> vserver cifs share modify -vserver vs1 -share-name
   SALES_SHARE -path /sales -vscan-fileop-profile strict
   ```

액세스 시 정책을 수정, 비활성화 또는 삭제할 수 있습니다. 정책의 요약 및 세부 정보를 볼 수 있습니다.

원하는 작업	다음 명령을 입력합니다…
액세스 시 정책을 생성합니다	`vserver vscan on-access-policy create`
액세스 시 정책을 수정합니다	'vserver Vscan on-access-policy modify'를 참조하십시오
액세스 시 정책을 설정합니다	`vserver vscan on-access-policy enable`
액세스 시 정책을 사용하지 않도록 설정합니다	'vserver Vscan on-access-policy disable'
액세스 시 정책을 삭제합니다	'vserver Vscan on-access-policy delete
액세스 시 정책에 대한 요약 및 세부 정보를 봅니다	'vserver vscan on-access-policy show'를 참조하십시오
제외할 경로 목록에 추가합니다	`vserver vscan on-access-policy paths-to-exclude add`
제외할 경로 목록에서 삭제합니다	`vserver vscan on-access-policy paths-to-exclude remove`
제외할 경로 목록을 봅니다	`vserver vscan on-access-policy paths-to-exclude show`
제외할 파일 확장명 목록에 추가합니다	`vserver vscan on-access-policy file-ext-to-exclude add`
제외할 파일 확장명 목록에서 삭제합니다	`vserver vscan on-access-policy file-ext-to-exclude remove`
제외할 파일 확장명 목록을 봅니다	`vserver vscan on-access-policy file-ext-to-exclude show`
포함할 파일 확장명 목록에 추가합니다	`vserver vscan on-access-policy file-ext-to-include add`
포함할 파일 확장명 목록에서 삭제합니다	`vserver vscan on-access-policy file-ext-to-include remove`

포함할 파일 확장명 목록을 봅니다	`vserver vscan on-access-policy file-ext-to-include show`

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

온디맨드 스캐닝 구성

ONTAP Vscan 온디맨드 스캐닝 구성에 대해 알아보세요

주문형 검사를 사용하여 파일에 바이러스가 있는지 즉시 또는 일정에 따라 확인할 수 있습니다.

예를 들어, 사용량이 적은 시간에만 스캔을 실행하거나 액세스 시 스캔에서 제외되었던 매우 큰 파일을 스캔할 수 있습니다. cron 일정을 사용하여 작업 실행 시간을 지정할 수 있습니다.

필요 시 작업을 생성하려면 액세스 시 정책을 하나 이상 활성화해야 합니다. 기본 정책이거나 사용자가 만든 액세스 시 정책일 수 있습니다.

을 참조하십시오

- 작업을 만들 때 일정을 할당할 수 있습니다.
- SVM에서 한 번에 하나의 작업만 예약할 수 있습니다.
- 필요 시 스캐닝은 심볼 링크 또는 스트림 파일의 스캔을 지원하지 않습니다.

필요 시 스캐닝은 심볼 링크 또는 스트림 파일의 스캔을 지원하지 않습니다.

필요 시 작업을 생성하려면 액세스 시 정책을 하나 이상 활성화해야 합니다. 기본 정책이거나 사용자가 만든 액세스 시 정책일 수 있습니다.

ONTAP Vscan으로 주문형 작업 만들기

주문형 작업은 주문형 바이러스 검사의 범위를 정의합니다. 스캔할 파일의 최대 크기, 스캔에 포함할 파일의 확장명 및 경로, 스캔에서 제외할 파일의 확장명 및 경로를 지정할 수 있습니다. 하위 디렉터리의 파일은 기본적으로 스캔됩니다.

이 작업에 대해

- 각 SVM에 대해 최대 10개의 온디맨드 작업이 존재할 수 있지만, 하나의 SVM만 활성화할 수 있습니다.
- 필요 시 작업에서는 스캔과 관련된 통계와 관련된 정보가 포함된 보고서를 생성합니다. 이 보고서는 명령을 사용하거나 정의된 위치에서 작업에 의해 생성된 보고서 파일을 다운로드하여 액세스할 수 있습니다.
- ONTAP 9.14.1부터 와일드카드를 사용하여 제외할 온디맨드 경로와 파일 확장자를 지정할 수 있습니다.

시작하기 전에

- 이(가) 있어야 합니다 액세스 시 정책을 생성했습니다. 정책은 기본 정책이거나 사용자가 만든 정책일 수 있습니다. On-access 정책이 없으면 검사를 활성화할 수 없습니다.

단계

1. 필요 시 작업 만들기:

   `vserver vscan on-demand-task create -vserver data_SVM -task-name task_name -scan-paths paths_of_files_to_scan -report-directory report_directory_path -report-expiry-time expiration_time_for_report -schedule cron_schedule -max -file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to -exclude file_extensions -file-ext-to-include file_extensions -scan-files-with -no-ext true|false -directory-recursion true|false`

   - '-file-ext-to-exclude' 설정은 '-file-ext-to-include' 설정보다 우선합니다.
   - 설정 `-scan-files-with-no-ext` 를 true로 설정하면 확장자가 없는 파일을 스캔할 수 있습니다.

     에 대한 자세한 내용은 `vserver vscan on-demand-task create` "ONTAP 명령 참조입니다"을 참조하십시오.

     다음 명령을 실행하면 이라는 On-Demand 작업이 생성됩니다 `Task1` VS1의 VM에서:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

+

> 명령을 사용하여 작업의 상태를 볼 수 `job show` 있습니다. 및 `job resume` 명령을 사용하여 작업을 일시 중지하고 다시 시작하거나 `job stop` 명령을 사용하여 작업을 종료할 수 `job pause` 있습니다. 에 대한 자세한 내용은 `job` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 주문형 작업이 생성되었는지 확인합니다.

   `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

   에 대한 자세한 내용은 `vserver vscan on-demand-task show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 'Task1' 작업에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                            Vserver: vs1
                          Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: info
        Expiration Time for Report: -
```

작업을 마친 후

작업을 실행하도록 예약하기 전에 SVM에서 스캔을 활성화해야 합니다.

ONTAP Vscan을 사용하여 주문형 작업 일정을 예약하세요

일정을 할당하지 않고 작업을 만들고 를 사용할 수 있습니다 `vserver vscan on-demand-task schedule` 스케줄을 할당하거나 작업을 생성하는 동안 스케줄을 추가하는 명령입니다.

이 작업에 대해

'vserver vscan on-demand-task schedule' 명령으로 할당된 스케줄은 'vserver vscan on-demand-task create' 명령으로 이미 할당된 스케줄보다 우선합니다.

단계

1. 필요 시 작업 예약:

   `vserver vscan on-demand-task schedule -vserver` *`data_SVM`* `-task-name` *`task_name`* `-schedule cron_schedule`

   다음 명령을 실행하면 이라는 액세스 시 작업이 예약됩니다 `Task2` 를 누릅니다 `vs2` SVM:

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

에 대한 자세한 내용은 `vserver vscan on-demand-task schedule` "ONTAP 명령 참조입니다"을 참조하십시오.

> 작업 상태를 보려면 `job show` 명령을 사용하십시오. `job pause`및 `job resume` 명령은 각각 작업을 일시 중지하고 다시 시작합니다. 명령은 작업을 종료합니다. `job stop` 에 대한 자세한 내용은 `job` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 필요 시 작업이 예약되었는지 확인합니다.

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

   에 대한 자세한 내용은 `vserver vscan on-demand-task show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 '작업 2' 작업에 대한 세부 정보가 표시됩니다.

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                            Vserver: vs2
                          Task Name: Task2
                 List of Scan Paths: /vol1/, /vol2/cifs/
               Report Directory Path: /report
                        Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
              File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: info
```

작업을 마친 후

작업을 실행하도록 예약하기 전에 SVM에서 스캔을 활성화해야 합니다.

ONTAP Vscan 온디맨드 작업을 즉시 실행하세요

일정을 할당했는지 여부에 관계없이 필요 시 작업을 즉시 실행할 수 있습니다.

시작하기 전에

SVM에서 스캔을 활성화해야 합니다.

단계

1. 필요 시 작업을 즉시 실행합니다.

   `vserver vscan on-demand-task run -vserver data_SVM -task-name task_name`

   다음 명령을 실행하면 이라는 온액세스 작업이 실행됩니다 `Task1` 를 누릅니다 `vs1` SVM:

   ```
   cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
   Task1
   [Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
   command to view the status.
   ```

   에 대한 자세한 내용은 `vserver vscan on-demand-task run` "ONTAP 명령 참조입니다"을 참조하십시오.

   명령을 사용하여 작업의 상태를 볼 수 `job show` 있습니다. 및 `job resume` 명령을 사용하여 작업을 일시 중지하고 다시 시작하거나 `job stop` 명령을 사용하여 작업을 종료할 수 `job pause` 있습니다. 에 대한 자세한 내용은 `job` "ONTAP 명령 참조입니다"을 참조하십시오.

주문형 작업 관리를 위한 **ONTAP Vscan** 명령

필요 시 작업을 수정, 삭제 또는 예약 취소할 수 있습니다. 작업에 대한 요약 및 세부 정보를 보고 작업에 대한 보고서를 관리할 수 있습니다.

원하는 작업	다음 명령을 입력합니다…
주문형 작업을 만듭니다	`vserver vscan on-demand-task create`
필요 시 작업을 수정합니다	'vserver vscan on-demand-task modify(가상 Vscan 주문형 작업 수정)
필요 시 작업을 삭제합니다	'vserver vscan on-demand-task delete'(가상 Vscan 주문형 작업 삭제
주문형 작업을 실행합니다	`vserver vscan on-demand-task run`
필요 시 작업을 예약합니다	`vserver vscan on-demand-task schedule`
필요 시 작업 일정을 취소합니다	'vserver vscan on-demand-task unschedule'
필요 시 작업에 대한 요약 및 세부 정보를 봅니다	'vserver vscan on-demand-task show'
주문형 보고서 보기	'vserver vscan on-demand-task report show'(가상 Vscan 주문형 작업 보고서 표시
필요 시 보고서를 삭제합니다	'vserver Vscan 주문형 작업 보고서 삭제

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP Vscan에서 오프박스 바이러스 백신 기능을 구성하기 위한 모범 사례

ONTAP에서 오프 박스 기능을 구성할 때는 다음 권장 사항을 고려하십시오.

- 권한이 있는 사용자를 바이러스 검사 작업으로 제한합니다. 일반 사용자는 권한이 있는 사용자 자격 증명을 사용하지 않도록 해야 합니다. 이러한 제한은 Active Directory에서 권한이 있는 사용자에 대한 로그인 권한을 해제하면 얻을 수 있습니다.
- 권한이 있는 사용자는 administrators 그룹 또는 backup operators 그룹과 같이 도메인에서 많은 권한이 있는 사용자 그룹에 속할 필요가 없습니다. 권한이 있는 사용자는 Vscan 서버 접속을 생성하고 바이러스 검사를 위한 파일에 액세스할 수 있도록 스토리지 시스템에서만 유효성을 검사해야 합니다.
- Vscan 서버를 실행하는 컴퓨터는 바이러스 검사 목적으로만 사용하십시오. 일반적인 사용을 방지하려면 이러한 컴퓨터에서 Windows 터미널 서비스 및 기타 원격 액세스 조항을 비활성화하고 관리자에게만 새 소프트웨어를 설치할 권한을 부여하십시오.
- Vscan 서버를 바이러스 검사 전용으로 사용하고 백업 등의 다른 작업에 사용하지 마십시오. Vscan 서버를 가상 머신(VM)으로 실행하기로 결정할 수 있습니다. Vscan 서버를 VM으로 실행하는 경우 VM에 할당된 리소스가 공유되지 않고 바이러스 검사를 수행하기에 충분한지 확인합니다.
- 리소스의 초과 할당을 방지하기 위해 Vscan 서버에 적절한 CPU, 메모리 및 디스크 용량을 제공합니다. 대부분의 Vscan 서버는 여러 CPU 코어 서버를 사용하고 CPU 전반에 로드를 분산하도록 설계되었습니다.
- NetApp는 다른 클라이언트 네트워크 트래픽의 영향을 받지 않도록 SVM에서 Vscan 서버로의 연결에 전용 VLAN을 사용하는 것이 좋습니다. Vscan 서버의 안티바이러스 VLAN 및 SVM의 데이터 LIF 전용 NIC(네트워크 인터페이스 카드)를 생성합니다. 이 단계는 네트워크 문제가 발생할 경우 관리 및 문제 해결을 간소화합니다. 바이러스 백신 트래픽은 개인 네트워크를 사용하여 분리해야 합니다. 다음 방법 중 하나를 사용하여 DC(도메인 컨트롤러) 및 ONTAP와 통신하도록 바이러스 백신 서버를 구성해야 합니다.
  - DC는 트래픽을 분리하는 데 사용되는 개인 네트워크를 통해 바이러스 백신 서버와 통신해야 합니다.
  - DC 및 안티바이러스 서버는 CIFS 클라이언트 네트워크와 동일하지 않은 다른 네트워크(앞에서 언급한 전용 네트워크가 아님)를 통해 통신해야 합니다.
  - 바이러스 백신 통신에 Kerberos 인증을 사용하려면 프라이빗 LIF에 대한 DNS 항목과 프라이빗 LIF에 대해 생성된 DNS 항목에 해당하는 DC에 서비스 사용자 이름을 생성해야 합니다. 바이러스 백신 커넥터에 LIF를 추가할 때 이 이름을 사용하십시오. DNS는 안티바이러스 커넥터에 연결된 각 전용 LIF에 대해 고유한 이름을 반환할 수 있어야 합니다.

> Vscan 트래픽용 LIF가 클라이언트 트래픽에 대한 LIF가 아닌 다른 포트에 구성되어 있는 경우, 포트 장애가 발생하면 Vscan LIF가 다른 노드로 페일오버될 수 있습니다. 변경 사항으로 인해 새 노드에서 Vscan 서버에 연결할 수 없으며 노드의 파일 작업에 대한 검색 알림이 실패합니다. Vscan 서버가 노드에서 수행된 파일 작업에 대한 스캔 요청을 처리할 수 있도록 노드에 있는 하나 이상의 LIF를 통해 연결할 수 있는지 확인합니다.

- 1GbE 네트워크 이상을 사용하여 NetApp 스토리지 시스템과 Vscan 서버를 연결합니다.
- 여러 Vscan 서버가 있는 환경의 경우 비슷한 고성능 네트워크 연결이 있는 모든 서버를 연결합니다. Vscan 서버를 연결하면 부하 공유를 허용하여 성능이 향상됩니다.
- 원격 사이트 및 지사의 경우 NetApp는 원격 Vscan 서버 대신 로컬 Vscan 서버를 사용할 것을 권장합니다. 이는 지연 시간이 길기 때문입니다. 비용이 중요한 경우 보통 수준의 바이러스 보호를 위해 노트북 또는 PC를 사용하십시오. 볼륨 또는 qtree를 공유하고 원격 사이트의 모든 시스템에서 스캔하여 전체 파일 시스템 검사를 주기적으로 예약할 수 있습니다.

- 여러 Vscan 서버를 사용하여 로드 밸런싱 및 이중화를 위해 SVM의 데이터를 스캔합니다. CIFS 워크로드 양과 그에 따른 바이러스 백신 트래픽은 SVM당 다릅니다. 스토리지 컨트롤러에서 CIFS 및 바이러스 검사 지연 시간을 모니터링합니다. 시간에 따른 결과 추세를 모니터링합니다. 추세 임계값을 초과하는 Vscan 서버의 CPU 또는 애플리케이션 큐로 인해 CIFS 지연 시간 및 바이러스 검사 지연 시간이 증가하면 CIFS 클라이언트가 대기 시간이 길어질 수 있습니다. Vscan 서버를 추가합니다
하중을 분산시킵니다.
- 최신 버전의 ONTAP 안티바이러스 커넥터를 설치합니다.
- 바이러스 백신 엔진과 정의를 최신 상태로 유지합니다. 업데이트 빈도에 대한 권장 사항은 파트너에게 문의하십시오.
- 멀티 테넌시 환경에서는 Vscan 서버와 SVM이 동일한 도메인 또는 신뢰할 수 있는 도메인에 속해 있는 경우 여러 SVM과 스캐너 풀(Vscan 서버 풀)을 공유할 수 있습니다.
- 감염된 파일에 대한 바이러스 백신 소프트웨어 정책은 대부분의 바이러스 백신 공급업체에서 설정한 기본값인 " 삭제" 또는 "격리"로 설정되어야 합니다. "vscan-fileop-profile"이 "write_only"로 설정되어 있고 감염된 파일이 발견되면 파일이 공유에 남아 있고 파일을 열면 검사가 트리거되지 않으므로 열 수 있습니다. 바이러스 백신 검사는 파일을 닫은 후에만 트리거됩니다.
- 를 클릭합니다 `scan-engine timeout` 값은 보다 작아야 합니다 `scanner-pool request-timeout` 값. 더 높은 값으로 설정하면 파일 액세스가 지연되고 결국 시간 초과될 수 있습니다.
이를 방지하려면 를 구성하십시오 `scan-engine timeout` 보다 5초 더 짧습니다 `scanner-pool request-timeout` 값. 를 변경하는 방법에 대한 지침은 스캔 엔진 공급업체의 설명서를 참조하십시오 `scan-engine timeout` 설정. 를 클릭합니다 `scanner-pool timeout` 고급 모드에서 다음 명령을 사용하고 에 적절한 값을 입력하여 변경할 수 있습니다 `request-timeout` 매개 변수:
`vserver vscan scanner-pool modify`.
- 온-액세스 검사 워크로드에 적합한 크기로 주문형 검사를 사용해야 하는 환경의 경우, NetApp 기존 바이러스 백신 인프라에 추가 로드가 발생하지 않도록 사용량이 적은 시간에 온디맨드 검사 작업을 예약하는 것이 좋습니다.

파트너 관련 모범 사례에 대한 자세한 내용은 을 "Vscan 파트너 솔루션"참조하십시오.

SVM ONTAP Vscan에서 바이러스 검사 활성화

액세스 또는 온디맨드 검사를 실행하려면 SVM에서 바이러스 검사를 활성화해야 합니다.

단계

1. SVM에서 바이러스 검사 활성화:

   'vserver Vscan enable - vserver data_SVM'

   에 대한 자세한 내용은 `vserver vscan enable` "ONTAP 명령 참조입니다"을 참조하십시오.

   > 필요한 경우 명령을 사용하여 바이러스 검사를 비활성화할 수 `vserver vscan disable` 있습니다. 에 대한 자세한 내용은 `vserver vscan disable` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 에서 바이러스 검사가 활성화됩니다 `vs1` SVM:

   ```
   cluster1::> vserver vscan enable -vserver vs1
   ```

2. SVM에서 바이러스 검사가 활성화되었는지 확인합니다.

   'vserver vscan show -vserver data_SVM'

   에 대한 자세한 내용은 `vserver vscan show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 의 Vscan 상태가 표시됩니다 `vs1` SVM:

```
cluster1::> vserver vscan show -vserver vs1

                              Vserver: vs1
                        Vscan Status: on
```

ONTAP Vscan 스캔 파일 상태 재설정

경우에 따라 명령을 사용하여 파일에 대해 캐시된 정보를 삭제하여 SVM에서 성공적으로 스캔된 파일의 스캔 상태를 재설정해야 할 수 있습니다 `vserver vscan reset`. 예를 들어, 잘못 구성된 검사가 있는 경우 이 명령을 사용하여 바이러스 검사 처리를 다시 시작할 수 있습니다. 에 대한 자세한 내용은 `vserver vscan reset` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

'vserver Vscan reset' 명령을 실행하면 다음에 액세스할 때 모든 유효한 파일이 스캔됩니다.

> 이 명령은 다시 스캔 대상 파일의 수와 크기에 따라 성능에 부정적인 영향을 미칠 수 있습니다.

시작하기 전에

이 작업에는 고급 권한이 필요합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

   에 대한 자세한 내용은 `set -privilege advanced` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 스캔한 파일의 상태 재설정:

   'vserver Vscan reset - vserver data_SVM'

   다음 명령을 실행하면 에서 스캔한 파일의 상태가 재설정됩니다 `vs1` SVM:

```
cluster1::> vserver vscan reset -vserver vs1
```

ONTAP를 사용하여 Vscan 이벤트 로그 정보를 봅니다

'vserver Vscan show-events' 명령을 사용하여 감염된 파일에 대한 이벤트 로그 정보, Vscan 서버에 대한 업데이트 등을 확인할 수 있습니다. 클러스터에 대한 이벤트 정보 또는 지정된 노드, SVM 또는 Vscan 서버에 대한 이벤트 정보를 볼 수 있습니다.

시작하기 전에

Vscan 이벤트 로그를 보려면 고급 권한이 필요합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

   에 대한 자세한 내용은 `set` "ONTAP 명령 참조입니다"을 참조하십시오.

2. Vscan 이벤트 로그 정보 보기:

   'vserver vscan show-events'

   에 대한 자세한 내용은 `vserver vscan show-events` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 클러스터 'cluster1'에 대한 이벤트 로그 정보가 표시됩니다.

```
cluster1::*> vserver vscan show-events

Vserver     Node              Server           Event Type         Event Time
----------- ---------------- ---------------- -----------------
-----------------
vs1         Cluster-01       192.168.1.1      file-infected      9/5/2014
11:37:38
vs1         Cluster-01       192.168.1.1      scanner-updated    9/5/2014
11:37:08
vs1         Cluster-01       192.168.1.1      scanner-connected 9/5/2014
11:34:55
3 entries were displayed.
```

연결 문제를 모니터링하고 해결합니다

스캔 필수 옵션과 관련된 잠재적인 **ONTAP Vscan** 연결 문제

"vserver vscan connection-status show" 명령을 사용하면 연결 문제 해결에 도움이 될 수 있는 Vscan 서버 연결에 대한 정보를 볼 수 있습니다.

기본적으로, 액세스 시 스캔에 대한 '스캔 필수' 옵션은 Vscan 서버 연결을 스캐닝에 사용할 수 없을 때 파일 액세스를 거부합니다. 이 옵션은 중요한 안전 기능을 제공하지만 몇 가지 상황에서 문제가 발생할 수 있습니다.

- 클라이언트 액세스를 활성화하기 전에 LIF가 있는 각 노드의 SVM에 하나 이상의 Vscan 서버가 연결되어 있는지 확인해야 합니다. 클라이언트 액세스를 활성화한 후 서버를 SVM에 연결해야 하는 경우 Vscan 서버 연결을 사용할 수 없기 때문에 파일 액세스가 거부되지 않도록 SVM에서 '필수' 옵션을 해제해야 합니다. 서버를 연결한 후 옵션을 다시 켤 수 있습니다.
- 대상 LIF가 SVM을 위한 모든 Vscan 서버 연결을 호스팅하는 경우 LIF가 마이그레이션되면 서버와 SVM 간 연결이 끊어집니다. Vscan 서버 연결을 사용할 수 없어 파일 액세스가 거부되지 않도록 하려면 LIF를 마이그레이션하기 전에 '필수' 옵션을 해제해야 합니다. LIF가 마이그레이션된 후 옵션을 다시 설정할 수 있습니다.

각 SVM에는 최소한 2개의 Vscan 서버가 할당되어 있어야 합니다. Vscan 서버를 클라이언트 액세스에 사용되는 네트워크와 다른 네트워크를 통해 스토리지 시스템에 연결하는 것이 가장 좋습니다.

에 대한 자세한 내용은 `vserver vscan connection-status show` "ONTAP 명령 참조입니다"을 참조하십시오.

Vscan 서버 연결 상태를 보기 위한 **ONTAP** 명령

'vserver vscan connection-status show' 명령을 사용하여 Vscan 서버 연결 상태에 대한 요약 및 세부 정보를 볼 수 있습니다.

원하는 작업	다음 명령을 입력합니다...
Vscan 서버 연결 요약 보기	'vserver vscan connection-status show'
Vscan 서버 연결에 대한 세부 정보를 봅니다	'vserver vscan connection-status show-all'을 선택합니다
연결된 Vscan 서버에 대한 세부 정보를 봅니다	'vserver Vscan connection-status show-connected'(가상 Vscan 연결 상태 표시 - 연결됨
연결되지 않은 사용 가능한 Vscan 서버에 대한 세부 정보를 봅니다	'vserver Vscan connection-status show-not-connected'(가상 Vscan 연결 상태 표시 - 연결되지 않음)

에 대한 자세한 내용은 `vserver vscan connection-status show` "ONTAP 명령 참조입니다"을 참조하십시오.

바이러스 **ONTAP Vscan** 스캐닝 문제 해결

일반적인 바이러스 검사 문제의 경우 가능한 원인과 해결 방법이 있습니다. 바이러스 검사는 Vscan이라고도 합니다.

문제	해결 방법

Vscan 서버는 에 연결할 수 없습니다 clustered ONTAP 스토리지 시스템을 활용할 수 있습니다.	스캐너 풀 구성에서 Vscan 서버 IP 주소를 지정하는지 확인합니다. 스캐너 풀 목록에서 허용된 권한이 있는 사용자가 활성 상태인지 확인합니다. 스캐너 풀을 확인하려면 를 실행합니다 `vserver vscan scanner-pool show` 스토리지 시스템 명령 프롬프트에서 명령을 입력합니다. 그래도 Vscan 서버에 연결할 수 없는 경우 네트워크에 문제가 있을 수 있습니다.
클라이언트에서 높은 지연 시간을 관찰합니다.	스캐너 풀에 Vscan 서버를 더 추가해야 할 때가 되었을 것입니다.
너무 많은 스캔이 트리거되었습니다.	의 값을 수정합니다 `vscan-fileop-profile` 바이러스 검사를 위해 모니터링되는 파일 작업의 수를 제한하는 매개 변수입니다.
일부 파일이 스캔되지 않습니다.	온액세스 정책을 확인합니다. 이러한 파일의 경로가 경로 제외 목록에 추가되었거나 파일 크기가 제외에 대해 구성된 값을 초과할 수 있습니다. On-access 정책을 확인하려면 를 실행합니다 `vserver vscan on-access-policy show` 스토리지 시스템 명령 프롬프트에서 명령을 입력합니다.
파일 액세스가 거부되었습니다.	정책 구성에 _scan-mandatory_setting이 지정되어 있는지 확인한다. 이 설정은 연결된 Vscan 서버가 없는 경우 데이터 액세스를 거부합니다. 필요에 따라 설정을 수정합니다.

관련 정보

- "Vscan vscan scanner -pool show를 선택합니다"
- "vserver Vscan on-access-policy show 를 참조하십시오"

ONTAP Vscan 상태 및 성능 활동 모니터링

Vscan 서버 연결 상태와 같은 Vscan 모듈의 중요한 측면을 모니터링할 수 있습니다. Vscan 서버의 상태 및 스캔된 파일 수 이 정보는 도움이 됩니다 Vscan 서버와 관련된 문제를 진단합니다.

Vscan 서버 연결 정보를 봅니다

Vscan 서버의 연결 상태를 보고 이미 사용 중인 연결을 관리할 수 있습니다 및 사용 가능한 연결입니다. 다양한 명령이 정보를 표시합니다 Vscan 서버의 연결 상태 정보

명령…	표시된 정보…
'vserver vscan connection-status show'	연결 상태 요약

'vserver vscan connection-status show-all'을 선택합니다	연결 상태에 대한 자세한 정보입니다
'vserver Vscan connection-status show-not-connected'(가상 Vscan 연결 상태 표시 - 연결되지 않음)	사용할 수 있지만 연결되지 않은 연결의 상태입니다
'vserver Vscan connection-status show-connected'(가상 Vscan 연결 상태 표시 - 연결됨	연결된 Vscan 서버에 대한 정보입니다

에 대한 자세한 내용은 `vserver vscan connection-status show` "ONTAP 명령 참조입니다"을 참조하십시오.

Vscan 서버 통계를 봅니다

Vscan 서버별 통계를 확인하여 성능을 모니터링하고 바이러스 검사 관련 문제를 진단할 수 있습니다. Vscan을 사용하려면 먼저 데이터 샘플을 수집해야 합니다. `statistics show` Vscan 서버 통계를 표시하는 명령입니다.

에 대한 자세한 내용은 `statistics show` "ONTAP 명령 참조입니다"을 참조하십시오.

데이터 샘플을 완료하려면 다음 단계를 완료하십시오.

단계

1. `statistics start`명령 및 선택적 `statistics stop` 명령을 실행합니다.

   자세히 알아보세요 `statistics start` 그리고 `statistics stop` 에서 "ONTAP 명령 참조입니다" .

Vscan 서버 요청 및 대기 시간에 대한 통계를 봅니다

ONTAP를 사용할 수 있습니다 `offbox_vscan` Vscan의 속도를 모니터링하기 위해 SVM 단위로 카운터를 사용합니다
모든 Vscan에 대해 1초에 발송 및 수신된 서버 요청 및 서버 지연 시간
서버. 이러한 통계를 보려면 다음 단계를 완료하십시오.

단계

1. 다음 카운터로 명령을 실행합니다 `statistics show -object offbox_vscan -instance SVM`.

카운터...	표시된 정보...
`scan_request_dispatched_rate`	ONTAP에서 초당 Vscan 서버로 보낸 바이러스 검사 요청 수입니다
`scan_noti_received_rate`	ONTAP가 초당 Vscan 서버로부터 받은 바이러스 검사 요청 수입니다
`dispatch_latency`	ONTAP 내의 대기 시간으로 사용 가능한 Vscan 서버를 식별하고 해당 Vscan 서버로 요청을 전송합니다

scan_latency	ONTAP에서 Vscan 서버로의 왕복 지연 시간(스캔 실행 시간 포함)

ONTAP 오프박스 **Vscan** 카운터에서 생성된 통계의 예

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-------------------------------------------------------------------
```

개별 **Vscan** 서버 요청 및 대기 시간에 대한 통계를 봅니다

ONTAP를 사용할 수 있습니다 `offbox_vscan_server` Vscan 서버당, SVM당, 오프박스 Vscan 서버의 카운터, 및 노드별 기준으로 파견된 Vscan 서버 요청 비율 및 에 대한 서버 지연 시간을 모니터링합니다
각 Vscan 서버를 개별적으로 사용할 수 있습니다. 이 정보를 수집하려면 다음 단계를 완료하십시오.

단계

1. 를 실행합니다 `statistics show –object offbox_vscan –instance SVM:servername:nodename` 다음 카운터를 사용하여 명령을 실행합니다.

카운터…	표시된 정보…
scan_request_dispatched_rate	ONTAP에서 보낸 바이러스 검사 요청 수입니다
scan_latency	ONTAP에서 Vscan 서버로의 왕복 지연 시간(스캔 실행 시간 포함) 초당 Vscan 서버로

ONTAP offbox_Vscan_server 카운터에서 생성된 통계의 예

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-------------------------------------------------------------------
```

Vscan 서버 활용도에 대한 통계를 봅니다

ONTAP를 사용할 수도 있습니다 `offbox_vscan_server` Vscan 서버 – 측면 활용 수집 카운터 통계. 이러한 통계는 SVM, Box가 없는 Vscan 서버별, 노드 단위로 추적됩니다. 있습니다 Vscan 서버의 CPU 사용률, Vscan 서버의 스캔 작업에 대한 대기열 깊이를 포함합니다 (현재 및 최대), 사용된 메모리 및 사용된 네트워크.
이러한 통계는 ONTAP 내의 통계 카운터로 Antivirus Connector에 의해 전달됩니다. 있습니다 20초마다 폴링되는 데이터를 기반으로 하며 정확성을 위해 여러 번 수집해야 합니다.
그렇지 않으면 통계에 표시되는 값은 마지막 폴링만 반영합니다. CPU 사용률 및 큐는 입니다 특히 모니터링 및 분석에 중요합니다. 평균 대기열의 값이 높으면 가 표시됩니다 Vscan 서버에 병목 현상이 있습니다.
Vscan 서버에 대한 사용률을 SVM 단위, 오프박스 Vscan 서버 단위 및 노드별로 수집합니다 다음 단계를 완료합니다.

단계

1. Vscan 서버에 대한 활용도 통계를 수집합니다

   를 실행합니다 `statistics show –object offbox_vscan_server –instance SVM:servername:nodename` 명령을 입력합니다 `offbox_vscan_server` 카운터:

카운터…	표시된 정보…
`scanner_stats_pct_cpu_used`	Vscan 서버의 CPU 활용도입니다
`scanner_stats_pct_input_queue_avg`	Vscan 서버에 대한 스캔 요청의 평균 대기열
`scanner_stats_pct_input_queue_hiwaterma rk`	Vscan 서버에서 스캔 요청 최대 대기열
`scanner_stats_pct_mem_used`	Vscan 서버에서 사용되는 메모리입니다
`scanner_stats_pct_network_used`	Vscan 서버에서 사용되는 네트워크

Vscan 서버에 대한 사용률 통계의 예

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
---------------------------------------------------------------
```

관련 정보

- "ONTAP 명령 참조입니다"

SVM에서 NAS 이벤트를 감사합니다

SMB 및 NFS 프로토콜 모두에 대해 ONTAP를 사용하여 파일 액세스를 감사하는 방법에 대해 알아보십시오

FPolicy를 사용하여 기본 감사 및 파일 정책 관리와 같은 ONTAP에서 SMB 및 NFS 프로토콜에 사용할 수 있는 파일 액세스 감사 기능을 사용할 수 있습니다.

다음과 같은 상황에서 SMB 및 NFS 파일 액세스 이벤트에 대한 감사를 설계하고 구현해야 합니다.

- 기본 SMB 및 NFS 프로토콜 파일 액세스가 구성되었습니다.
- 다음 방법 중 하나를 사용하여 감사 구성을 만들고 유지 관리하려고 합니다.
  - 기본 ONTAP 기능
  - 외부 FPolicy 서버

SVM에서 NAS 이벤트를 감사합니다

NAS 이벤트에 대한 감사는 스토리지 가상 시스템(SVM)에서 특정 SMB 및 NFS 이벤트를 추적하고 기록할 수 있는 보안 측정값입니다. 이를 통해 잠재적인 보안 문제를 추적하고 보안 위반의 증거를 제공할 수 있습니다. 또한 Active Directory 중앙 액세스 정책을 스테이징하고 감사하여 이러한 정책을 구현하면 어떤 결과가 초래되는지 확인할 수 있습니다.

SMB 이벤트

다음 이벤트를 감사할 수 있습니다.

- SMB 파일 및 폴더 액세스 이벤트입니다

  감사 기능이 활성화된 SVM에 속한 FlexVol 볼륨에 저장된 개체에 대해 SMB 파일 및 폴더 액세스 이벤트를 감사할 수 있습니다.

- SMB 로그온 및 로그오프 이벤트

  SVM에서 SMB 서버의 SMB 로그온 및 로그오프 이벤트를 감사할 수 있습니다.

- 중앙 액세스 정책 스테이징 이벤트입니다

  제안된 중앙 액세스 정책을 통해 적용된 권한을 사용하여 SMB 서버의 개체에 대한 효과적인 액세스를 감사할 수 있습니다. 중앙 액세스 정책의 스테이징을 통해 감사를 수행하여 중앙 액세스 정책이 구축되기 전에 어떤 영향이 있는지 확인할 수 있습니다.

  중앙 액세스 정책 스테이징에 대한 감사는 Active Directory GPO를 사용하여 설정되지만 SVM 감사 구성은 중앙 액세스 정책 스테이징 이벤트를 감사하도록 구성해야 합니다.

  SMB 서버에서 동적 액세스 제어를 사용하지 않고 감사 구성에서 중앙 액세스 정책 스테이징을 설정할 수 있지만, 동적 액세스 제어를 설정한 경우에만 중앙 액세스 정책 스테이징 이벤트가 생성됩니다. 동적 액세스 제어는 SMB 서버 옵션을 통해 활성화됩니다. 기본적으로 활성화되어 있지 않습니다.

NFS 이벤트입니다

SVM에 저장된 객체에 NFSv4 ACL을 활용하여 파일 및 디렉토리 이벤트를 감사할 수 있습니다.

감사 작동 방식

기본적인 ONTAP 감사 개념에 대해 알아봅니다

ONTAP의 감사를 이해하려면 몇 가지 기본적인 감사 개념을 알고 있어야 합니다.

- * 스테이징 파일 *

  통합 및 변환 전에 감사 레코드가 저장되는 개별 노드의 중간 바이너리 파일입니다. 스테이징 파일은 스테이징 볼륨에 포함되어 있습니다.

- * 스테이징 볼륨 *

  ONTAP에서 스테이징 파일을 저장하기 위해 생성한 전용 볼륨입니다. 애그리게이트당 하나의 스테이징 볼륨이 있습니다. 스테이징 볼륨은 모든 감사 가능 스토리지 가상 시스템(SVM)에서 공유되며, 해당 애그리게이트 내 데이터 볼륨의 데이터 액세스 감사 레코드를 저장합니다. 각 SVM의 감사 레코드는 스테이징 볼륨 내의 개별 디렉토리에 저장됩니다.

  클러스터 관리자는 스테이징 볼륨에 대한 정보를 볼 수 있지만 다른 대부분의 볼륨 작업은 허용되지 않습니다. ONTAP만 스테이징 볼륨을 생성할 수 있습니다. ONTAP는 스테이징 볼륨에 이름을 자동으로 할당합니다. 모든 스테이징 볼륨 이름은 mdv_AUD_ 로 시작하고 그 스테이징 볼륨을 포함하는 애그리게이트의 UUID로 시작합니다(예: mdv_AUD_1d0131843d4811e296fc123478563412).

- * 시스템 볼륨 *

  파일 서비스 감사 로그의 메타데이터와 같은 특수 메타데이터가 포함된 FlexVol 볼륨입니다. admin SVM은 시스템 볼륨을 소유하며 클러스터 전체에서 볼 수 있습니다. 스테이징 볼륨은 시스템 볼륨의 유형입니다.

- * 통합 작업 *

  감사가 설정되어 있을 때 생성되는 작업입니다. 각 SVM에서 장기적으로 실행되는 이 작업은 SVM 구성원 노드 전체의 스테이징 파일에서 감사 레코드를 가져갑니다. 이 작업은 감사 레코드를 날짜순으로 정렬하여 병합한 다음, evtx 또는 XML 파일 형식으로 감사 구성에 지정된 사용자 판독 가능한 이벤트 로그 형식으로 변환합니다. 변환된 이벤트 로그는 SVM 감사 구성에 지정된 감사 이벤트 로그 디렉토리에 저장됩니다.

ONTAP 감사 프로세스의 기능에 대해 알아봅니다

ONTAP 감사 프로세스는 Microsoft 감사 프로세스와 다릅니다. 감사를 구성하기 전에 ONTAP 감사 프로세스의 작동 방식을 이해해야 합니다.

감사 레코드는 처음에 개별 노드의 이진 스테이징 파일에 저장됩니다. SVM에서 감사를 사용하면 모든 구성원 노드가 해당 SVM에 대한 스테이징 파일을 유지합니다. 주기적으로 이러한 로그는 통합되어 사용자가 읽을 수 있는 이벤트 로그로 변환되며, SVM의 감사 이벤트 로그 디렉토리에 저장됩니다.

SVM에서 감사를 활성화할 때의 프로세스입니다

감사는 SVM에서만 활성화할 수 있습니다. 스토리지 관리자가 SVM에 대한 감사를 활성화할 때 감사 하위 시스템은 스테이징 볼륨이 있는지 여부를 확인합니다. SVM이 소유한 데이터 볼륨이 포함된 각 애그리게이트의 스테이징 볼륨이 있어야 합니다. 감사 하위 시스템은 필요한 스테이징 볼륨이 없는 경우 이를 생성합니다.

감사 하위 시스템은 감사를 사용하기 전에 다른 필수 구성 요소 작업도 완료합니다.

- 감사 서브시스템은 로그 디렉토리 경로를 사용할 수 있고 symlink를 포함하지 않는지 확인합니다.

  로그 디렉토리는 SVM 네임스페이스 내의 경로로 이미 존재해야 합니다. 감사 로그 파일을 보관할 새 볼륨 또는 qtree를 생성하는 것이 좋습니다. 감사 하위 시스템은 기본 로그 파일 위치를 할당하지 않습니다. 감사 구성에 지정된 로그 디렉토리 경로가 올바른 경로가 아닌 경우 "지정한 경로"/path"가 SVM "Vserver_NAME" 오류가 있는 네임스페이스에 없으므로 구성 생성을 감사하지 못합니다.

  디렉토리가 있지만 symlink가 포함된 경우 구성을 생성할 수 없습니다.

- 감사 기능은 통합 작업을 예약합니다.

  이 작업이 예약되면 감사가 활성화됩니다. SVM 감사 구성 및 로그 파일은 재부팅 후에도 또는 NFS 또는 SMB 서버가 중지 또는 재시작되어도 유지됩니다.

이벤트 로그 통합

로그 통합은 감사가 비활성화될 때까지 정기적으로 실행되는 예약된 작업입니다. 감사를 사용하지 않도록 설정하면 통합 작업에서 나머지 모든 로그가 통합되었는지 확인합니다.

감사 보장

기본적으로 감사는 보장됩니다. ONTAP는 노드를 사용할 수 없는 경우에도 감사 가능한 모든 파일 액세스 이벤트(구성된 감사 정책 ACL에 의해 지정됨)를 기록합니다. 해당 작업에 대한 감사 레코드가 영구 저장소의 스테이징 볼륨에

저장될 때까지 요청된 파일 작업을 완료할 수 없습니다. 공간이 부족하거나 다른 문제로 인해 스테이징 파일의 디스크에 감사 레코드를 커밋할 수 없는 경우 클라이언트 작업이 거부됩니다.

관리자 또는 권한 수준 액세스 권한이 있는 계정 사용자는 NetApp Manageability SDK 또는 REST API를 사용하여 파일 감사 로깅 작업을 건너뛸 수 있습니다. Audit.LOG 파일에 저장된 Command History 로그를 검토하여 NetApp Manageability SDK 또는 REST API를 사용하여 파일 작업이 수행되었는지 확인할 수 있습니다.

명령 기록 감사 로그에 대한 자세한 내용은 의 "관리 활동에 대한 감사 로깅 관리" 섹션을 참조하십시오 "시스템 관리".

노드를 사용할 수 없는 경우의 통합 프로세스

감사가 설정된 SVM에 속하는 볼륨을 포함하는 노드를 사용할 수 없는 경우 통합 감사 작업의 동작은 노드의 스토리지 페일오버(SFO) 파트너(또는 2노드 클러스터의 경우 HA 파트너)를 사용할 수 있는지 여부에 따라 달라집니다.

- SFO 파트너를 통해 스테이징 볼륨을 사용할 수 있는 경우 노드에서 마지막으로 보고된 스테이징 볼륨이 스캔되고 통합이 정상적으로 진행됩니다.
- SFO 파트너를 사용할 수 없는 경우 작업에 부분 로그 파일이 생성됩니다.

  노드에 연결할 수 없는 경우 통합 작업은 해당 SVM의 사용 가능한 다른 노드의 감사 레코드를 통합합니다. 작업이 완료되지 않은 것을 확인하기 위해 통합 파일 이름에 접미사 .partial이 추가됩니다.

- 사용할 수 없는 노드를 사용할 수 있게 되면 해당 노드의 감사 레코드가 해당 시점에 다른 노드의 감사 레코드와 통합됩니다.
- 모든 감사 레코드가 보존됩니다.

이벤트 로그 회전

감사 이벤트 로그 파일은 구성된 임계값 로그 크기에 도달하거나 구성된 일정에 도달하면 회전합니다. 이벤트 로그 파일이 순환되면 예약된 통합 작업에서 먼저 활성 변환된 파일의 이름을 타임 스탬프 아카이브 파일로 바꾼 다음 새 활성 변환 이벤트 로그 파일을 만듭니다.

SVM에서 감사를 사용하지 않도록 설정할 때의 프로세스입니다

SVM에서 감사를 사용하지 않도록 설정하면 통합 작업이 마지막으로 한 번 트리거됩니다. 모든 미해결, 기록된 감사 레코드는 사용자가 읽을 수 있는 형식으로 기록됩니다. SVM에서 감사를 사용하지 않도록 설정하고 확인할 수 있으면 이벤트 로그 디렉토리에 저장된 기존 이벤트 로그가 삭제되지 않습니다.

해당 SVM에 대한 기존 스테이징 파일이 모두 통합된 후에는 통합 작업이 일정에서 제거됩니다. SVM에 대한 감사 구성을 비활성화해도 감사 구성은 제거되지 않습니다. 스토리지 관리자는 언제든지 감사를 다시 활성화할 수 있습니다.

감사를 사용할 때 생성되는 감사 통합 작업은 통합 작업을 모니터링하고 오류로 인해 통합 작업이 종료되는 경우 다시 만듭니다. 사용자가 감사 통합 작업을 삭제할 수 없습니다.

ONTAP 감사를 위한 사전 요구 사항

SVM(스토리지 가상 시스템)에 대한 감사를 구성 및 설정하기 전에 특정 요구사항과 고려 사항을 숙지해야 합니다.

- NFS 및 S3 감사 사용 SVM에 대한 결합 제한은 ONTAP 버전에 따라 다릅니다.

ONTAP 버전입니다	최대
9.8 이하	50
9.9.1 이상	400

- 감사는 SMB 또는 NFS 라이센스와 관련이 없습니다.

  클러스터에 SMB 및 NFS 라이센스가 설치되어 있지 않은 경우에도 감사를 구성 및 활성화할 수 있습니다.

- NFS 감사는 보안 ACE(U형)를 지원합니다.
- NFS 감사의 경우 모드 비트와 감사 ACE 사이에 매핑이 없습니다.

  ACL을 모드 비트로 변환할 때 감사 ACE는 건너뜁니다. 모드 비트를 ACL로 변환할 때 감사 ACE가 생성되지 않습니다.

- 감사 구성에 지정된 디렉토리가 있어야 합니다.

  이 명령이 없으면 감사 구성을 만드는 명령이 실패합니다.

- 감사 구성에 지정된 디렉토리는 다음 요구 사항을 충족해야 합니다.
  - 디렉토리에는 심볼 링크가 포함되어 있지 않아야 합니다.

    감사 구성에 지정된 디렉터리에 심볼 링크가 포함된 경우 감사 구성을 생성하는 명령이 실패합니다.

  - 절대 경로를 사용하여 디렉토리를 지정해야 합니다.

    예를 들어, '/vs1/…/'와 같은 상대 경로를 지정하면 안 됩니다.

- 감사는 스테이징 볼륨에 사용 가능한 공간이 있는 경우에 따라 달라집니다.

  감사된 볼륨이 포함된 애그리게이트에서 스테이징 볼륨에 충분한 공간이 있는지 확인하고 계획을 세워야 합니다.

- 감사는 변환된 이벤트 로그가 저장되는 디렉토리가 포함된 볼륨에 사용 가능한 공간이 있는지 여부에 따라 달라집니다.

  이벤트 로그를 저장하는 데 사용되는 볼륨에 충분한 공간이 있는지 확인하고 계획을 세워야 합니다. 감사 구성을 생성할 때 '-rotate-limit' 매개 변수를 사용하여 감사 디렉토리에 유지할 이벤트 로그 수를 지정할 수 있습니다. 감사 구성은 볼륨에 이벤트 로그에 사용할 수 있는 충분한 공간이 있는지 확인하는 데 도움이 됩니다.

- SMB 서버에서 동적 액세스 제어를 설정하지 않고 감사 구성에서 중앙 액세스 정책 스테이징을 설정할 수 있지만 동적 액세스 제어를 활성화하여 중앙 액세스 정책 스테이징 이벤트를 생성해야 합니다.

  동적 액세스 제어는 기본적으로 사용되지 않습니다.

감사를 설정할 때 애그리게이트 공간 고려 사항

감사 구성이 생성되고 클러스터에서 하나 이상의 SVM(스토리지 가상 머신)에 감사가 활성화되어 있으면 감사 서브시스템이 모든 기존 애그리게이트 및 생성되는 모든 새 애그리게이트에 스테이징 볼륨을 생성합니다. 클러스터에서 감사를 활성화할 때는 애그리게이트 공간의 특정 고려 사항을 알아야 합니다.

애그리게이트에서 사용할 수 없는 공간으로 인해 스테이징 볼륨 생성이 실패할 수 있습니다. 감사 구성을 생성할 때 기존

애그리게이트에 스테이징 볼륨을 포함할 충분한 공간이 없는 경우 이러한 문제가 발생할 수 있습니다.

SVM에 대한 감사를 활성화하기 전에 스테이징 볼륨에 대한 기존 애그리게이트에 충분한 공간이 있는지 확인해야 합니다.

ONTAP 감사 레코드의 스테이징 파일 크기에 대한 제한 사항

스테이징 파일의 감사 레코드 크기는 32KB를 초과할 수 없습니다.

대규모 감사 레코드가 발생할 수 있는 경우

다음 시나리오 중 하나에서 관리 감사 중에 대규모 감사 레코드가 발생할 수 있습니다.

- 많은 수의 사용자가 있는 그룹에 사용자를 추가 또는 삭제합니다.
- 많은 수의 파일 공유 사용자와 파일 공유에서 파일 공유 ACL(액세스 제어 목록)을 추가 또는 삭제합니다.
- 기타 시나리오.

이 문제를 방지하려면 관리 감사를 사용하지 않도록 설정합니다. 이렇게 하려면 감사 구성을 수정하고 감사 이벤트 유형 목록에서 다음을 제거합니다.

- 파일 공유
- 사용자 계정
- 보안 그룹
- authorization-policy-change를 참조하십시오

  제거 후에는 파일 서비스 감사 하위 시스템에 의해 감사되지 않습니다.

너무 큰 감사 기록의 영향

- 감사 레코드 크기가 너무 크면(32KB 이상) 감사 레코드가 생성되지 않고 감사 하위 시스템에서 다음과 유사한 EMS(이벤트 관리 시스템) 메시지가 생성됩니다.

  "파일 서비스 감사 하위 시스템이 max_audit_record_size 값보다 크기 때문에 작업에 실패했거나 감사 레코드를 잘라냅니다. SVM UUID=%s, event_id=%u, size=%u

  감사가 보장된 경우 감사 레코드를 생성할 수 없기 때문에 파일 작업이 실패합니다.

- Audit Record의 크기가 9,999바이트보다 큰 경우 위와 동일한 EMS 메시지가 출력된다. 키 값이 더 큰 부분 감사 레코드가 누락되었습니다.
- 감사 레코드가 2,000자를 초과하면 실제 값 대신 다음 오류 메시지가 표시됩니다.

  이 필드의 값이 너무 길어 표시할 수 없습니다

ONTAP 감사 이벤트 로그에 지원되는 형식에 대해 알아봅니다

변환된 감사 이벤트 로그에 지원되는 파일 형식은 evtx 및 XML 파일 형식입니다.

감사 구성을 만들 때 파일 형식의 유형을 지정할 수 있습니다. 기본적으로 ONTAP는 바이너리 로그를 'evtx' 파일 형식으로 변환합니다.

ONTAP 감사 이벤트 로그를 보고 처리합니다

감사 이벤트 로그를 사용하여 적절한 파일 보안이 있는지 여부와 잘못된 파일 및 폴더 액세스 시도가 있는지 여부를 확인할 수 있습니다. evtx 또는 XML 파일 형식으로 저장된 감사 이벤트 로그를 보고 처리할 수 있습니다.

- evtx 파일 형식

  Microsoft 이벤트 뷰어를 사용하여 변환된 'evtx' 감사 이벤트 로그를 저장된 파일로 열 수 있습니다.

  이벤트 뷰어를 사용하여 이벤트 로그를 볼 때 사용할 수 있는 두 가지 옵션이 있습니다.

  - 일반 보기

    모든 이벤트에 공통되는 정보는 이벤트 레코드에 대해 표시됩니다. 이 버전의 ONTAP에서는 이벤트 레코드에 대한 이벤트 관련 데이터가 표시되지 않습니다. 상세도를 사용하여 이벤트 관련 데이터를 표시할 수 있습니다.

  - 상세보기

    친숙한 뷰와 XML 뷰를 사용할 수 있습니다. 보기 및 XML 보기에는 모든 이벤트에 공통되는 정보와 이벤트 레코드에 대한 이벤트 관련 데이터가 모두 표시됩니다.

- 'xml' 파일 형식

  XML 파일 형식을 지원하는 타사 응용 프로그램에서 XML 감사 이벤트 로그를 보고 처리할 수 있습니다. XML 스키마와 XML 필드 정의에 대한 정보가 있는 경우 XML 보기 도구를 사용하여 감사 로그를 볼 수 있습니다. XML 스키마 및 정의에 대한 자세한 내용은 을 참조하십시오 "ONTAP 감사 스키마 참조".

이벤트 뷰어를 사용하여 활성 감사 로그를 보는 방법

클러스터에서 감사 통합 프로세스가 실행 중인 경우 통합 프로세스에서 감사 사용 스토리지 가상 시스템(SVM)에 대한 새 레코드를 활성 감사 로그 파일에 추가합니다. 이 활성 감사 로그는 Microsoft 이벤트 뷰어에서 SMB 공유를 통해 액세스하고 열 수 있습니다.

이벤트 뷰어에는 기존 감사 레코드를 보는 것 외에도 콘솔 창에서 콘텐츠를 새로 고칠 수 있는 새로 고침 옵션이 있습니다. 새로 추가된 로그를 이벤트 뷰어에서 볼 수 있는지 여부는 활성 감사 로그에 액세스하는 데 사용된 공유에 oplocks가 설정되어 있는지 여부에 따라 달라집니다.

공유에 oplocks 설정을 지정합니다	동작
활성화됨	이벤트 뷰어는 해당 시점까지 기록된 이벤트가 포함된 로그를 엽니다. 새로 고침 작업은 통합 프로세스에 추가된 새 이벤트로 로그를 새로 고치지 않습니다.
사용 안 함	이벤트 뷰어는 해당 시점까지 기록된 이벤트가 포함된 로그를 엽니다. 새로 고침 작업은 통합 프로세스에 추가된 새 이벤트로 로그를 새로 고칩니다.

이 정보는 evtx 이벤트 로그에만 적용됩니다. XML 이벤트 로그는 브라우저에서 SMB를 통해 보거나 XML 편집기나 뷰어를 사용하여 NFS를 통해 볼 수 있습니다.

감사할 수 있는 **SMB** 이벤트입니다

ONTAP에서 결과를 해석하기 위해 감사할 수 있는 **SMB** 이벤트에 대해 알아보십시오

ONTAP는 특정 파일 및 폴더 액세스 이벤트, 특정 로그온 및 로그오프 이벤트, 중앙 액세스 정책 스테이징 이벤트를 비롯한 특정 SMB 이벤트를 감사할 수 있습니다. 감사할 수 있는 액세스 이벤트를 알면 이벤트 로그의 결과를 해석할 때 도움이 됩니다.

다음과 같은 추가 SMB 이벤트를 감사할 수 있습니다.

이벤트 ID(EVT/evtx)	이벤트	설명	범주
4670)을 참조하십시오	개체 권한이 변경되었습니다	객체 액세스: 권한이 변경되었습니다.	파일 액세스
4907	개체 감사 설정이 변경되었습니다	개체 액세스: 감사 설정이 변경되었습니다.	파일 액세스
4913	객체 중앙 액세스 정책이 변경되었습니다	개체 액세스: 캡이 변경되었습니다.	파일 액세스

다음 SMB 이벤트는 ONTAP 9.0 이상에서 감사할 수 있습니다.

이벤트 ID(EVT/evtx)	이벤트	설명	범주
540/4624	계정이 성공적으로 로그온되었습니다	로그온/로그오프: 네트워크(SMB) 로그온.	로그온 및 로그오프
529/4625	계정 로그온에 실패했습니다	로그온/로그오프: 알 수 없는 사용자 이름 또는 잘못된 암호입니다.	로그온 및 로그오프
530/4625	계정 로그온에 실패했습니다	로그온/로그오프: 계정 로그온 시간 제한.	로그온 및 로그오프
531/4625	계정 로그온에 실패했습니다	로그온/로그오프: 계정이 현재 비활성화되었습니다.	로그온 및 로그오프
532/4625	계정 로그온에 실패했습니다	로그온/로그오프: 사용자 계정이 만료되었습니다.	로그온 및 로그오프
533/4625	계정 로그온에 실패했습니다	로그온/로그오프: 사용자가 이 컴퓨터에 로그온할 수 없습니다.	로그온 및 로그오프

534/4625	계정 로그온에 실패했습니다	로그온/로그오프: 여기에 로그온 유형이 부여되지 않았습니다.	로그온 및 로그오프
535/4625	계정 로그온에 실패했습니다	로그온/로그오프: 사용자 암호가 만료되었습니다.	로그온 및 로그오프
537/4625	계정 로그온에 실패했습니다	로그온/로그오프: 위의 이유 이외의 이유로 로그온하지 못했습니다.	로그온 및 로그오프
539/4625	계정 로그온에 실패했습니다	로그온/로그오프: 계정이 잠겼습니다.	로그온 및 로그오프
538/4634	계정이 로그오프되었습니다	로그온/로그오프: 로컬 또는 네트워크 사용자 로그오프.	로그온 및 로그오프
560/4656)을 참조하십시오	객체 열기/객체 생성	오브젝트 액세스: 오브젝트(파일 또는 디렉토리)가 열려 있습니다.	파일 액세스
563/4659	삭제 의도에 따라 개체를 엽니다	오브젝트 액세스: 오브젝트(파일 또는 디렉토리)에 대한 핸들이 삭제 의향과 함께 요청되었습니다.	파일 액세스
564/4660	개체 삭제	오브젝트 액세스: 오브젝트 삭제(파일 또는 디렉토리). ONTAP는 Windows 클라이언트가 개체(파일 또는 디렉터리)를 삭제하려고 할 때 이 이벤트를 생성합니다.	파일 액세스
567/4663	개체 읽기/개체 쓰기/개체 속성 가져오기/개체 특성 설정	오브젝트 액세스: 오브젝트 액세스 시도(읽기, 쓰기, get 속성, set 속성) • 참고: * 이 이벤트의 경우 ONTAP는 개체에 대한 첫 번째 SMB 읽기 및 첫 번째 SMB 쓰기 작업(성공 또는 실패)만 감사합니다. 이렇게 하면 단일 클라이언트가 개체를 열고 동일한 개체에 대해 여러 번의 연속 읽기 또는 쓰기 작업을 수행할 때 ONTAP에서 과도한 로그 항목을 만들지 못하게 됩니다.	파일 액세스
해당 없음/4664	하드 링크	개체 액세스: 하드 링크를 만들려고 했습니다.	파일 액세스
해당 없음/4818	제안된 중앙 액세스 정책은 현재 중앙 액세스 정책과 동일한 액세스 권한을 부여하지 않습니다	객체 액세스: 중앙 액세스 정책 스테이징.	파일 액세스

NA/NA Data ONTAP 이벤트 ID 9999	개체 이름 바꾸기	오브젝트 액세스: 오브젝트 이름 바꾸기. ONTAP 이벤트입니다. 현재 Windows에서 단일 이벤트로 지원되지 않습니다.	파일 액세스
NA/NA Data ONTAP 이벤트 ID 9998	개체 연결 끊기	개체 액세스: 개체 연결 해제됨. ONTAP 이벤트입니다. 현재 Windows에서 단일 이벤트로 지원되지 않습니다.	파일 액세스

이벤트 **4656**에 대한 추가 정보

감사 XML 이벤트의 HandleID 태그에는 액세스한 개체(파일 또는 디렉터리)의 핸들이 들어 있습니다. evtx 4656 이벤트에 대한 "HandleID" 태그는 open 이벤트가 새 개체를 만들거나 기존 개체를 여는 데 사용되는지 여부에 따라 다른 정보를 포함합니다.

- Open event가 Open request로 새로운 object(file or directory)를 생성하려는 경우 Audit XML event의 HandleID 태그는 빈 HandleID를 표시합니다(예: "<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>").

  실제 개체 생성이 발생하기 전과 핸들이 있기 전에 열려 있는(새 개체 만들기) 요청을 감사하기 때문에 "HandleID"가 비어 있습니다. 같은 개체에 대한 후속 감사 이벤트에는 'HandleID' 태그에 올바른 객체 핸들이 있습니다.

- open event가 기존 object를 열기 위한 open 요청인 경우 audit event는 'HandleID' 태그(예: "<Data Name="HandleID">0000000401;00;000000ea;00123ed4</Data>")에서 해당 object의 할당된 handle을 갖게 됩니다.

ONTAP 감사 객체에 대한 전체 경로를 결정합니다

감사 레코드에 대한 "<ObjectName>" 태그에 인쇄된 객체 경로에는 볼륨의 이름(괄호 안에 표시)과 포함하는 볼륨의 루트에서의 상대 경로가 포함됩니다. 연결 경로를 포함하여 감사된 개체의 전체 경로를 결정하려면 특정 단계를 수행해야 합니다.

단계

1. 감사 이벤트의 "<ObjectName>" 태그를 확인하여 감사된 개체에 대한 볼륨 이름 및 상대 경로를 확인합니다.

   이 예에서 볼륨 이름은 "data1"이고 파일의 상대 경로는 "/dir1/file.txt"입니다.

   '<Data Name="ObjectName">"(data1); /dir1/file.txt'</Data>'

2. 이전 단계에서 확인한 볼륨 이름을 사용하여 감사된 개체가 포함된 볼륨의 연결 경로를 결정합니다.

   이 예에서 볼륨 이름은 "data1"이고 감사 대상 객체가 포함된 볼륨의 연결 경로는 "/data/data1"입니다.

   '볼륨 표시-접합-볼륨 데이터1'

```
                                 Junction                       Junction
Vserver   Volume       Language Active    Junction Path     Path Source
--------- ------------ -------- --------  ----------------- -----------
vs1       data1        en_US.UTF-8
                                 true      /data/data1       RW_volume
```

3. 볼륨의 접합 경로에 "<ObjectName>" 태그에 있는 상대 경로를 추가하여 감사된 개체의 전체 경로를 확인합니다.

   이 예에서 볼륨의 접합 경로는 다음과 같습니다.

   '/data/data1/dir1/file.text'

교집합 및 하드 링크에 대한 **ONTAP** 감사에 대해 알아봅니다

symlink 및 hard link를 감사할 때는 몇 가지 고려 사항을 염두에 두어야 합니다.

감사 레코드에는 "ObjectName" 태그에서 식별되는 감사 객체의 경로를 비롯하여 감사 중인 객체에 대한 정보가 포함되어 있습니다. symlink와 hard link의 path가 ObjectName 태그에 기록되는 방식을 알고 있어야 합니다.

Symlink

Symlink는 대상 오브젝트의 위치에 대한 포인터가 포함된 별도의 inode가 있는 파일이며, 대상이라고 합니다. symlink를 통해 개체에 액세스할 때 ONTAP는 자동으로 symlink를 해석하고 볼륨의 대상 개체에 대한 실제 정규 프로토콜 무관 경로를 따릅니다.

다음 예제 출력에는 둘 다 target.txt라는 파일을 가리키는 두 개의 symlink가 있습니다. 심볼 링크 중 하나는 상대 symlink로, 다른 하나는 절대 symlink입니다. symlink 중 하나가 감사되는 경우 audit event의 ObjectName 태그에 "target.txt" 파일의 경로가 포함됩니다.

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

하드 링크

하드 링크는 파일 시스템의 기존 파일과 이름을 연결하는 디렉토리 항목입니다. 하드 링크는 원본 파일의 inode 위치를 가리킵니다. ONTAP에서 symlink를 해석하는 방법과 마찬가지로 ONTAP는 하드 링크를 해석하고 볼륨의 대상 개체에 대한 실제 정규 경로를 따릅니다. 하드 링크 개체에 대한 액세스가 감사되면 감사 이벤트는 하드 링크 경로가 아닌 ObjectName 태그에 이 절대 정규 경로를 기록합니다.

대체 **NTFS** 데이터 스트림의 **ONTAP** 감사에 대해 알아봅니다

NTFS 대체 데이터 스트림을 사용하여 파일을 감사할 때 고려해야 할 몇 가지 사항이 있습니다.

감사대상 개체의 위치는 이벤트 레코드에 ObjectName 태그(경로)와 HandleID 태그(핸들)라는 두 개의 태그를 사용하여 기록됩니다. 기록되는 스트림 요청을 제대로 식별하려면 NTFS 대체 데이터 스트림에 대한 다음 필드의 ONTAP 레코드를 알고 있어야 합니다.

- evtx ID: 4656 이벤트(감사 이벤트 열기 및 만들기)
  - 대체 데이터 스트림의 경로는 ObjectName 태그에 기록됩니다.
  - 대체 데이터 스트림의 핸들은 HandleID 태그에 기록됩니다.
- evtx ID: 4663 이벤트(읽기, 쓰기, GetAttr 등과 같은 기타 모든 감사 이벤트)
  - 대체 데이터 스트림이 아닌 기본 파일의 경로는 ObjectName 태그에 기록됩니다.
  - 대체 데이터 스트림의 핸들은 HandleID 태그에 기록됩니다.

예

다음 예제에서는 "HandleID" 태그를 사용하여 대체 데이터 스트림에 대한 evtx ID: 4663 이벤트를 식별하는 방법을 보여 줍니다. READ AUDIT 이벤트에 기록된 ObjectName 태그(경로)가 기본 파일 경로에 있더라도 HandleID 태그를 사용하여 대체 데이터 스트림에 대한 감사 레코드로 이벤트를 식별할 수 있습니다.

스트림 파일 이름은 base_file_name:stream_name 형식으로 지정됩니다. 이 예제에서 dIR1 디렉토리에는 다음 경로를 가진 대체 데이터 스트림이 있는 기본 파일이 포함되어 있습니다.

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

다음 이벤트 예제의 출력은 표시된 대로 잘립니다. 출력에 해당 이벤트에 사용할 수 있는 출력 태그가 모두 표시되지 않습니다.

evtx ID 4656(열린 감사 이벤트)의 경우 대체 데이터 스트림에 대한 감사 레코드 출력은 "ObjectName" 태그에 대체 데이터 스트림 이름을 기록합니다.

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

evtx ID 4663(감사 이벤트 읽기)의 경우 동일한 대체 데이터 스트림에 대한 감사 레코드 출력은 "ObjectName" 태그에 기본 파일 이름을 기록합니다. 그러나 "HandleID" 태그의 핸들은 대체 데이터 스트림의 핸들로, 이 이벤트를 대체 데이터 스트림과 연관시키는 데 사용할 수 있습니다.

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

NFS 파일 및 디렉토리 액세스 이벤트에 대한 ONTAP 감사 에 대해 자세히 알아보십시오

ONTAP는 특정 NFS 파일 및 디렉토리 액세스 이벤트를 감사할 수 있습니다. 감사할 수 있는 액세스 이벤트를 알면 변환된 감사 이벤트 로그의 결과를 해석할 때 도움이 됩니다.

다음 NFS 파일 및 디렉토리 액세스 이벤트를 감사할 수 있습니다.

- 읽기
- 개방형
- 를 닫습니다
- readdir
- 쓰기
- SetAttr
- 생성
- 링크
- 운영
- 제거
- GetAttr
- 확인합니다
- nVerify(확인)
- 이름 바꾸기

NFS 이름 바꾸기 이벤트를 안정적으로 감사하려면 디렉터리 권한이 충분한 경우 파일 권한이 이름 바꾸기 작업에 대해 검사되지 않으므로 파일 대신 디렉터리에 감사 ACE를 설정해야 합니다.

ONTAP SVM에 대한 감사 구성 계획

SVM(스토리지 가상 시스템)에 대한 감사를 구성하기 전에 사용 가능한 구성 옵션을 파악하고 각 옵션에 설정할 값을 계획해야 합니다. 이 정보는 비즈니스 요구 사항에 맞는 감사 구성을 구성하는 데 도움이 됩니다.

모든 감사 구성에 공통적으로 적용되는 특정 구성 매개 변수가 있습니다.

또한 통합 및 변환된 감사 로그를 회전할 때 사용할 메서드를 지정하는 데 사용할 수 있는 특정 매개 변수가 있습니다. 감사를 구성할 때 다음 세 가지 방법 중 하나를 지정할 수 있습니다.

- 로그 크기에 따라 로그를 회전합니다

  로그를 회전시키는 데 사용되는 기본 방법입니다.

- 일정에 따라 로그를 회전합니다
- 로그 크기 및 일정에 따라 로그 회전(먼저 발생하는 이벤트)

로그 회전 방법 중 하나 이상이 항상 설정되어야 합니다.

모든 감사 구성에 공통으로 사용되는 매개 변수입니다

감사 구성을 만들 때 지정해야 하는 필수 매개 변수는 두 가지입니다. 다음 세 가지 옵션 매개 변수도 지정할 수 있습니다.

정보 유형입니다	옵션을 선택합니다	필수 요소입니다	포함	당신의 가치
_SVM 이름 _ 감사 구성을 생성할 SVM의 이름입니다. SVM이 이미 존재해야 합니다.	'-vserver"vserver_name'	예	예	
_로그 대상 경로 _ 변환된 감사 로그가 저장되는 디렉토리, 일반적으로 전용 볼륨 또는 qtree를 지정합니다. 경로는 SVM 네임스페이스에 이미 존재해야 합니다. 경로는 최대 864자까지 가능하며 읽기-쓰기 권한이 있어야 합니다. 경로가 유효하지 않으면 감사 구성 명령이 실패합니다. SVM이 SVM 재해 복구 소스인 경우 로그 타겟 경로가 루트 볼륨에 있을 수 없습니다. 루트 볼륨 컨텐츠가 재해 복구 대상에 복제되지 않기 때문입니다. FlexCache 볼륨은 로그 대상(ONTAP 9.7 이상)으로 사용할 수 없습니다.	목적지 텍스트	예	예	

_ 감사할 이벤트의 범주 _ 감사할 이벤트의 범주를 지정합니다. 다음 이벤트 범주를 감사할 수 있습니다. • 파일 액세스 이벤트(SMB 및 NFSv4 모두) • SMB 로그온 및 로그오프 이벤트 • 중앙 액세스 정책 스테이징 이벤트입니다 중앙 액세스 정책 스테이징 이벤트는 Windows 2012 Active Directory 도메인부터 사용할 수 있습니다. • 비동기식 - 삭제 • 파일 공유 범주 이벤트입니다 • 정책 변경 이벤트를 감사합니다 • 로컬 사용자 계정 관리 이벤트입니다 • 보안 그룹 관리 이벤트입니다 • 인증 정책 변경 이벤트입니다 기본값은 파일 액세스 및 SMB 로그온 및 로그오프 이벤트를 감사하는 것입니다. • 참고: * "cap-staging"을 이벤트 범주로 지정하려면 SVM에 SMB 서버가 있어야 합니다. SMB 서버에서 동적 액세스 제어를 사용하지 않고 감사 구성에서 중앙 액세스 정책 스테이징을 설정할 수 있지만, 동적 액세스 제어를 설정한 경우에만 중앙 액세스 정책 스테이징 이벤트가 생성됩니다. 동적 액세스 제어는 SMB 서버 옵션을 통해 활성화됩니다. 기본적으로 활성화되어 있지 않습니다.	`-events {file-ops`	`cifs-logon-logoff`	`cap-staging`	`file-share`
`audit-policy-change`	`user-account`	`security-group`	`authorization-policy-change`	`async-delete}`

아니요			_로그 파일 출력 형식 _ 감사 로그의 출력 형식을 결정합니다. 출력 형식은 ONTAP 관련 'XML' 또는 Microsoft Windows 'evtx' 로그 형식일 수 있습니다. 기본적으로 출력 형식은 evtx입니다.	'-format '{'xml'

'evtx'}	아니요			_ 로그 파일 회전 제한 _ 가장 오래된 로그 파일을 회전하기 전에 유지할 감사 로그 파일 수를 결정합니다. 예를 들어 5를 입력하면 마지막 5개의 로그 파일이 유지됩니다. 0 값은 모든 로그 파일이 보존됨을 나타냅니다. 기본값은 0입니다.

감사 이벤트 로그를 회전할 시기를 결정하는 데 사용되는 매개 변수입니다

- 로그 크기에 따라 로그를 회전합니다 *

기본값은 크기에 따라 감사 로그를 회전하는 것입니다.

- 기본 로그 크기는 100MB입니다
- 기본 로그 회전 방법과 기본 로그 크기를 사용하려면 로그 회전을 위한 특정 매개 변수를 구성할 필요가 없습니다.
- 로그 크기만을 기준으로 감사 로그를 회전하려면 다음 명령을 사용하여 '-rotate-schedule-minute' 매개 변수를 'vserver audit modify -vs0 -destination/-rotate-schedule -minute-'로 설정하십시오

기본 로그 크기를 사용하지 않으려면 '-rotate-size' 매개 변수를 구성하여 사용자 지정 로그 크기를 지정할 수 있습니다.

정보 유형입니다	옵션을 선택합니다	필수 요소입니다	포함	당신의 가치

_로그 파일 크기 제한 _ 감사 로그 파일 크기 제한을 결정합니다.	'-rotate-size'{'integer'[KB	MB	GB	TB

- 일정에 따라 로그를 회전합니다 *

일정에 따라 감사 로그를 회전하도록 선택한 경우 시간 기반 회전 매개 변수를 조합하여 로그 회전을 예약할 수 있습니다.

- 시간 기반 회전을 사용하는 경우 '-rotate-schedule-minute' 매개변수는 필수입니다.
- 다른 모든 시간 기반 회전 매개변수는 옵션입니다.
- 회전 일정은 모든 시간 관련 값을 사용하여 계산됩니다.

  예를 들어, '-rotate-schedule-minute' 매개 변수만 지정하면 감사 로그 파일은 모든 연도의 모든 월에 지정된 모든 요일에 지정된 분을 기준으로 회전합니다.

- 시간 기반 회전 매개 변수(예: '-rotate-schedule-month' 및 '-rotate-schedule-minutes')를 하나 또는 두 개만 지정하는 경우 모든 시간 동안 모든 요일에 지정한 분 값을 기준으로 로그 파일이 회전되며 지정된 개월 동안에만 회전됩니다.

  예를 들어 월요일, 수요일 및 토요일은 오전 10시 30분에 월, 3월, 8월 중 감사 로그를 회전하도록 지정할 수 있습니다

- '-rotate-schedule-dayOfWeek' 및 '-rotate-schedule-day' 값을 모두 지정하면 독립적으로 간주됩니다.

  예를 들어, `-rotate-schedule-dayOfWeek’를 금요일로 지정하고 '-rotate-schedule-day’를 13일로 지정하면 13일에 금요일이 아니라 지정한 달의 13일에 감사 로그가 회전합니다.

- 일정에 따라 감사 로그를 회전하려면 다음 명령을 사용하여 '-rotate-size' 매개 변수를 unset한다. 'vserver audit modify -vs0 -destination/-rotate -size-

다음 사용 가능한 감사 매개 변수 목록을 사용하여 감사 이벤트 로그 순환에 대한 일정을 구성하는 데 사용할 값을 결정할 수 있습니다.

정보 유형입니다	옵션을 선택합니다	필수 요소입니다	포함	당신의 가치
_로그 순환 스케줄: 월 _ 감사 로그 순환에 대한 월별 일정을 결정합니다. 유효한 값은 '1월’과 '모두’를 통해 '1월’입니다. 예를 들어 월 1월, 3월 및 8월 동안 감사 로그를 회전하도록 지정할 수 있습니다.	'-rotate-schedule-month' chron_month’입니다	아니요		

_Log 순환 스케줄: 요일 _ 감사 로그 회전에 대한 일별(요일) 일정을 결정합니다. 유효한 값은 '어타데이', '올데이'입니다. 예를 들어 감사 로그를 화요일과 금요일 또는 모든 요일에 회전하도록 지정할 수 있습니다.	'-rotate-schedule-dayOfWeek"chron_DayOfWeek'	아니요		
_ 로그 순환 스케줄: 일 _ 감사 로그 회전에 대한 월 일정 날짜를 결정합니다. 유효한 값은 1부터 31까지입니다. 예를 들어 감사 로그가 한 달의 10일과 20일 또는 한 달의 모든 일에 회전되도록 지정할 수 있습니다.	'-rotate-schedule-day"chron_dayofmonth'	아니요		
_ 로그 순환 스케줄: 시간 _ 감사 로그를 회전하기 위한 시간별 스케줄을 결정합니다. 유효한 값의 범위는 0(자정)에서 23(오후 11:00)까지입니다. All을 지정하면 감사 로그가 1시간마다 회전합니다. 예를 들어 감사 로그를 6(오전 6) 및 18(오후 6:00)에 회전하도록 지정할 수 있습니다.	'-rotate-schedule-hour"chron_hour'	아니요		
_ 로그 회전 스케줄: 분 _ 감사 로그를 회전하기 위한 분 일정을 결정합니다. 유효한 값의 범위는 0에서 59까지입니다. 예를 들어 30분에 감사 로그를 회전하도록 지정할 수 있습니다.	'-rotate-schedule-minute"chron_minute'	예, 스케줄 기반 로그 회전을 구성하는 경우, 그렇지 않으면 아니요		

- 로그 크기 및 일정에 따라 로그 회전 *

'-rotate-size' 매개변수와 시간 기반 회전 매개변수를 조합하여 로그 크기와 일정에 따라 로그 파일을 회전하도록 선택할 수 있습니다. 예를 들어, '-rotate-size'를 10MB로 설정하고 '-rotate-schedule-minute'를 15로 설정하면 로그 파일 크기가 10MB에 도달하거나 매 시간 15분(둘 중 먼저 발생하는 이벤트)에 도달할 때 로그 파일이 회전합니다.

SVM에 파일 및 디렉토리 감사 구성을 생성합니다

ONTAP SVM에 파일 및 디렉토리 감사 구성을 생성합니다

SVM(Storage Virtual Machine)에서 파일 및 디렉토리 감사 구성을 생성하는 작업에는 사용

가능한 구성 옵션 이해, 구성 계획 수립, 구성 구성 및 활성화 등이 포함됩니다. 그런 다음 감사 구성에 대한 정보를 표시하여 결과 구성이 원하는 구성인지 확인할 수 있습니다.

파일 및 디렉토리 이벤트 감사를 시작하려면 먼저 SVM(스토리지 가상 머신)에 감사 구성을 생성해야 합니다.

시작하기 전에

중앙 액세스 정책 스테이징에 대한 감사 구성을 생성하려는 경우 SVM에 SMB 서버가 있어야 합니다.

- SMB 서버에서 동적 액세스 제어를 사용하지 않고 감사 구성에서 중앙 액세스 정책 스테이징을 설정할 수 있지만, 동적 액세스 제어를 설정한 경우에만 중앙 액세스 정책 스테이징 이벤트가 생성됩니다.

  동적 액세스 제어는 SMB 서버 옵션을 통해 활성화됩니다. 기본적으로 활성화되어 있지 않습니다.

- 필드, 중복 항목 및 존재하지 않는 항목에 대한 잘못된 입력 등 명령에서 필드의 인수가 잘못된 경우 감사 단계 전에 명령이 실패합니다.

  이러한 실패는 감사 기록을 생성하지 않습니다.

이 작업에 대해

SVM이 SVM 재해 복구 소스인 경우 타겟 경로가 루트 볼륨에 있을 수 없습니다.

단계

1. 계획 워크시트의 정보를 사용하여 감사 구성을 만들어 로그 크기 또는 일정에 따라 감사 로그를 회전합니다.

감사 로그를 회전하려면…	입력…
로그 크기	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
일정	``vserver audit create-vserver_name-destination path-events[{file-ops
cifs-logon-logoff	cap-staging}][-format{xml

예

다음 예제에서는 크기 기반 회전을 사용하여 파일 작업 및 SMB 로그온 및 로그오프 이벤트(기본값)를 감사하는 감사 구성을 만듭니다. 로그 형식은 evtx(기본값)입니다. 로그는 '/audit_log' 디렉토리에 저장됩니다. 로그 파일 크기 제한은 200MB입니다. 로그 크기는 200MB에 도달하면 회전됩니다.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

다음 예에서는 크기 기반 회전을 사용하여 파일 작업 및 SMB 로그온 및 로그오프 이벤트(기본값)를 감사하는 감사 구성을 만듭니다. 로그 형식은 입니다 `EVTX` (기본값). 로그는 에 저장됩니다 `/cifs_event_logs` 디렉토리. 로그 파일 크기 제한은 입니다 `100 MB` (기본값), 로그 회전 제한은 입니다 `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

다음 예에서는 파일 작업, CIFS 로그온 및 로그오프 이벤트 및 시간 기반 회전을 사용하여 중앙 액세스 정책 스테이징 이벤트를 감사하는 감사 구성을 생성합니다. 로그 형식은 evtx(기본값)입니다. 감사 로그는 매월 오후 12시 30분에 순환됩니다 일주일 내내. 로그 회전 제한은 "5"입니다.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

관련 정보

- "SVM에 대한 감사를 설정합니다"
- "감사 구성을 확인합니다"

감사 구성을 설정한 후 **ONTAP SVM**에 대한 감사 기능이 활성화됩니다

감사 구성 설정을 마쳤으면 SVM(스토리지 가상 머신)에 대한 감사를 활성화해야 합니다.

시작하기 전에

SVM 감사 구성이 이미 존재해야 합니다.

이 작업에 대해

SVM 재해 복구 ID 폐기 구성이 SnapMirror 초기화가 완료된 후 먼저 시작되고 SVM에 감사 구성이 있으면 ONTAP에서 감사 구성을 자동으로 비활성화합니다. 스테이징 볼륨이 가득 차는 것을 방지하기 위해 읽기 전용 SVM에서 감사가 비활성화됩니다. SnapMirror 관계가 부러지고 SVM이 읽기-쓰기 상태가 된 후에만 감사를 활성화할 수 있습니다.

단계

1. SVM에 대한 감사 활성화:

   'vserver audit enable - vserver vserver_name'

   'vserver audit enable - vserver vs1'

관련 정보

- "감사 구성을 만듭니다"
- "감사 구성을 확인합니다"

ONTAP 감사 구성을 확인합니다

감사 구성을 완료한 후에는 감사가 올바르게 구성되어 있고 활성화되어 있는지 확인해야 합니다.

단계

1. 감사 구성을 확인합니다.

   'vserver audit show-instance-vserver vserver_name'

   다음 명령은 SVM(Storage Virtual Machine) VS1 에 대한 모든 감사 구성 정보를 목록으로 표시합니다.

   'vserver audit show-instance-vserver vs1'

```
                            Vserver: vs1
                  Auditing state: true
            Log Destination Path: /audit_log
     Categories of Events to Audit: file-ops
                         Log Format: evtx
              Log File Size Limit: 200MB
      Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
       Log Rotation Schedule: Hour: -
     Log Rotation Schedule: Minute: -
                Rotation Schedules: -
          Log Files Rotation Limit: 0
```

관련 정보

- "감사 구성을 만듭니다"
- "SVM에 대한 감사를 설정합니다"

파일 및 폴더 감사 정책을 구성합니다

ONTAP SVM에 대한 감사 구성을 활성화하고 파일 및 폴더 감사 정책을 구성합니다

파일 및 폴더 액세스 이벤트에 대한 감사를 구현하는 과정은 두 단계로 구성됩니다. 먼저 SVM(스토리지 가상 시스템)에서 감사 구성을 생성하고 활성화해야 합니다. 둘째, 모니터링할 파일과 폴더에 대해 감사 정책을 구성해야 합니다. 성공한 액세스 시도와 실패한 액세스 시도를 모두 모니터링하도록 감사 정책을 구성할 수 있습니다.

SMB 및 NFS 감사 정책을 모두 구성할 수 있습니다. SMB 및 NFS 감사 정책은 다양한 구성 요구사항 및 감사 기능을

갖습니다.

적절한 감사 정책이 구성된 경우 ONTAP는 SMB 또는 NFS 서버가 실행 중인 경우에만 감사 정책에 지정된 SMB 및 NFS 액세스 이벤트를 모니터링합니다.

NTFS 보안 스타일 파일 및 디렉터리에 대한 ONTAP 감사 정책을 구성합니다

파일 및 디렉터리 작업을 감사하려면 감사 정보를 수집할 파일 및 디렉터리에 대한 감사 정책을 구성해야 합니다. 감사 구성을 설정 및 활성화하는 것 외에 다른 기능도 있습니다. Windows 보안 탭을 사용하거나 ONTAP CLI를 사용하여 NTFS 감사 정책을 구성할 수 있습니다.

Windows 보안 탭을 사용하여 NTFS 감사 정책 구성

Windows 속성 창의 * Windows 보안 * 탭을 사용하여 파일 및 디렉터리에 대한 NTFS 감사 정책을 구성할 수 있습니다. 이는 Windows 클라이언트에 있는 데이터에 대한 감사 정책을 구성할 때 사용되는 것과 동일한 방법으로, 익숙한 GUI 인터페이스를 사용할 수 있습니다.

시작하기 전에

감사는 SACL(시스템 액세스 제어 목록)을 적용하는 데이터가 포함된 SVM(스토리지 가상 시스템)에서 구성해야 합니다.

이 작업에 대해

NTFS 감사 정책 구성은 NTFS 보안 설명자와 연결된 NTFS SACL에 항목을 추가하여 수행됩니다. 그런 다음 보안 설명자가 NTFS 파일 및 디렉터리에 적용됩니다. 이러한 작업은 Windows GUI에서 자동으로 처리됩니다. 보안 설명자는 파일 및 폴더 액세스 권한을 적용하기 위한 DACL(임의 액세스 제어 목록), 파일 및 폴더 감사를 위한 SACL 또는 SACL 및 DACL을 모두 포함할 수 있습니다.

Windows 보안 탭을 사용하여 NTFS 감사 정책을 설정하려면 Windows 호스트에서 다음 단계를 수행하십시오.

단계

1. Windows 탐색기의 * Tools * 메뉴에서 * Map network drive * 를 선택합니다.
2. 네트워크 드라이브 매핑 * 상자를 완료합니다.

   a. 드라이브 * 문자를 선택합니다.

   b. 폴더 * 상자에 감사할 데이터와 공유 이름을 가지고 있는 공유가 포함된 SMB 서버 이름을 입력합니다.

      SMB 서버 이름 대신 SMB 서버에 대한 데이터 인터페이스의 IP 주소를 지정할 수 있습니다.

      SMB 서버 이름이 "smb_server"이고 공유 이름이 "hay1"인 경우 \\smb_server\share1"을 입력해야 합니다.

   c. 마침 * 을 클릭합니다.

   선택한 드라이브가 마운트되고 공유 내에 포함된 파일 및 폴더를 표시하는 Windows 탐색기 창이 준비됩니다.

3. 감사 액세스를 설정할 파일 또는 디렉토리를 선택합니다.
4. 파일 또는 디렉터리를 마우스 오른쪽 단추로 클릭한 다음 * 속성 * 을 선택합니다.
5. 보안 * 탭을 선택합니다.
6. 고급 * 을 클릭합니다.

7. 감사 * 탭을 선택합니다.
8. 원하는 작업을 수행합니다.

원하는 경우	다음을 수행합니다
새 사용자 또는 그룹에 대한 감사를 설정합니다	a. 추가 * 를 클릭합니다. b. 선택할 개체 이름을 입력하십시오. 상자에 추가할 사용자 또는 그룹의 이름을 입력합니다. c. 확인 * 을 클릭합니다.
사용자 또는 그룹에서 감사를 제거합니다	a. 선택할 개체 이름을 입력하십시오. 상자에서 제거할 사용자 또는 그룹을 선택합니다. b. 제거 * 를 클릭합니다. c. 확인 * 을 클릭합니다. d. 이 절차의 나머지 부분을 건너뜁니다.
사용자 또는 그룹에 대한 감사 변경	a. 선택할 개체 이름을 입력하십시오. 상자에서 변경할 사용자 또는 그룹을 선택합니다. b. 편집 * 을 클릭합니다. c. 확인 * 을 클릭합니다.

사용자 또는 그룹에 대한 감사를 설정하거나 기존 사용자 또는 그룹에 대한 감사를 변경하는 경우 <object>에 대한 감사 항목 상자가 열립니다.

9. 적용 대상 * 상자에서 이 감사 항목을 적용할 방법을 선택합니다.

   다음 중 하나를 선택할 수 있습니다.

   - * 이 폴더, 하위 폴더 및 파일 *
   - * 이 폴더 및 하위 폴더 *
   - * 이 폴더만 *
   - * 이 폴더 및 파일 *
   - * 하위 폴더 및 파일만 *
   - * 하위 폴더만 *
   - * 파일만 * 단일 파일에 대한 감사를 설정하는 경우 * 적용 대상 * 상자가 활성화되지 않습니다. 적용 대상 * 상자 설정은 기본적으로 * 이 개체만 * 으로 설정됩니다.

   > 감사는 SVM 리소스를 사용하기 때문에 보안 요구사항을 충족하는 감사 이벤트를 제공하는 최소 수준만 선택하십시오.

10. Access* 상자에서 감사할 내용과 성공한 이벤트, 실패 이벤트 또는 둘 모두를 감사할지 여부를 선택합니다.
    - 성공한 이벤트를 감사하려면 성공 상자를 선택합니다.

- 실패 이벤트를 감사하려면 실패 상자를 선택합니다.

  보안 요구 사항을 충족하기 위해 모니터링해야 하는 작업만 선택합니다. 이러한 감사 가능한 이벤트에 대한 자세한 내용은 Windows 설명서를 참조하십시오. 다음 이벤트를 감사할 수 있습니다.

- * 완전 제어 *
- * 폴더 트래버스/파일 실행 *
- * 폴더 나열/데이터 읽기 *
- * 읽기 속성 *
- * 확장 속성 읽기 *
- * 파일 생성/데이터 쓰기 *
- * 폴더 생성/데이터 추가 *
- * 속성 쓰기 *
- * 확장 속성 쓰기 *
- * 하위 폴더 및 파일 삭제 *
- * 삭제 *
- * 읽기 권한 *
- * 권한 변경 *
- * 소유권 가져오기 *

11. 감사 설정이 원본 컨테이너의 후속 파일 및 폴더에 전파되지 않도록 하려면 * 이 감사 항목을 이 컨테이너 내의 개체 및/또는 컨테이너에 적용 * 상자를 선택합니다.
12. 적용 * 을 클릭합니다.
13. 감사 항목 추가, 제거 또는 편집을 마친 후 * 확인 * 을 클릭합니다.

    object>에 대한 감사 항목 상자가 닫힙니다.

14. 감사 * 상자에서 이 폴더의 상속 설정을 선택합니다.

    보안 요구 사항을 충족하는 감사 이벤트를 제공하는 최소 수준만 선택합니다. 다음 중 하나를 선택할 수 있습니다.

    - 이 개체의 부모 상자에서 상속 가능한 감사 항목 포함 을 선택합니다.
    - 모든 하위 항목의 기존 상속 가능한 감사 항목을 이 개체의 상속 가능한 감사 항목으로 바꾸기 상자를 선택합니다.
    - 두 상자를 모두 선택합니다.
    - 어느 상자도 선택하지 않습니다. 단일 파일에 대해 SACL을 설정하는 경우 모든 하위 항목에 대해 상속 가능한 기존 감사 항목을 이 개체의 상속 가능한 감사 항목으로 바꾸기 상자는 감사 상자에 없습니다.

15. 확인 * 을 클릭합니다.

    감사 상자가 닫힙니다.

ONTAP CLI를 사용하여 **NTFS** 감사 정책을 구성합니다

ONTAP CLI를 사용하여 파일 및 폴더에 대한 감사 정책을 구성할 수 있습니다. 따라서 Windows 클라이언트에서 SMB 공유를 사용하여 데이터에 연결할 필요 없이 NTFS 감사 정책을 구성할 수 있습니다.

'vserver security file-directory' 명령 제품군을 사용하여 NTFS 감사 정책을 구성할 수 있습니다.

CLI를 사용하는 NTFS SACL만 구성할 수 있습니다. 이 ONTAP 명령 제품군에는 NFSv4 SACL 구성이 지원되지 않습니다. 이러한 명령을 사용하여 의 파일 및 폴더에 NTFS SACL을 구성하고 추가하는 방법에 대해 자세히 "ONTAP 명령 참조입니다"알아보십시오.

UNIX 보안 스타일 파일 및 디렉터리에 대한 **ONTAP** 감사를 구성합니다

NFSv4.x ACL에 감사 ACE를 추가하여 UNIX 보안 스타일 파일 및 디렉토리에 대한 감사를 구성합니다. 이를 통해 보안을 위해 특정 NFS 파일 및 디렉토리 액세스 이벤트를 모니터링할 수 있습니다.

이 작업에 대해

NFSv4.x의 경우 임의 ACE와 시스템 ACE가 모두 동일한 ACL에 저장됩니다. 이 파일은 별도의 DACL 및 SACL에 저장되지 않습니다. 따라서 기존 ACL을 덮어쓰거나 잃지 않도록 기존 ACL에 감사 ACE를 추가할 때는 주의해야 합니다. 감사 ACE를 기존 ACL에 추가하는 순서는 중요하지 않습니다.

단계

1. nfs4_getfacl 또는 이와 동등한 명령을 사용하여 파일 또는 디렉토리의 기존 ACL을 검색합니다.

   에서 ACL 조작에 대해 자세히 "ONTAP 명령 참조입니다"알아보십시오.

2. 원하는 감사 ACE를 추가합니다.
3. nfs4_setfacl 또는 이와 동등한 명령을 사용하여 파일 또는 디렉토리에 업데이트된 ACL을 적용합니다.

파일 및 디렉토리에 적용된 감사 정책에 대한 정보를 표시합니다

Windows 보안 탭에 액세스하여 **ONTAP** 감사 정책 정보를 봅니다

Windows 속성 창의 보안 탭을 사용하여 파일 및 디렉터리에 적용된 감사 정책에 대한 정보를 표시할 수 있습니다. 이는 Windows 서버에 있는 데이터에 사용되는 것과 동일한 방법으로, 고객이 익숙한 GUI 인터페이스를 사용할 수 있습니다.

이 작업에 대해

파일 및 디렉터리에 적용된 감사 정책에 대한 정보를 표시하면 지정된 파일 및 폴더에 적절한 SACL(시스템 액세스 제어 목록)이 설정되어 있는지 확인할 수 있습니다.

NTFS 파일 및 폴더에 적용된 SACL에 대한 정보를 표시하려면 Windows 호스트에서 다음 단계를 수행하십시오.

단계

1. Windows 탐색기의 * Tools * 메뉴에서 * Map network drive * 를 선택합니다.
2. 네트워크 드라이브 연결 * 대화 상자를 완료합니다.

   a. 드라이브 * 문자를 선택합니다.

b. 폴더 * 상자에 감사할 데이터와 공유 이름을 둘 다 포함하는 공유가 포함된 SVM(스토리지 가상 시스템)의 IP 주소 또는 SMB 서버 이름을 입력합니다.

   SMB 서버 이름이 "smb_server"이고 공유 이름이 "hay1"인 경우 \\smb_server\share1"을 입력해야 합니다.

   SMB 서버 이름 대신 SMB 서버에 대한 데이터 인터페이스의 IP 주소를 지정할 수 있습니다.

c. 마침 * 을 클릭합니다.

선택한 드라이브가 마운트되고 공유 내에 포함된 파일 및 폴더를 표시하는 Windows 탐색기 창이 준비됩니다.

3. 감사 정보를 표시할 파일 또는 디렉터리를 선택합니다.
4. 파일 또는 디렉토리를 마우스 오른쪽 버튼으로 클릭하고 * 속성 * 을 선택합니다.
5. 보안 * 탭을 선택합니다.
6. 고급 * 을 클릭합니다.
7. 감사 * 탭을 선택합니다.
8. 계속 * 을 클릭합니다.

   감사 상자가 열립니다. 감사 항목 * 상자에는 SACL이 적용된 사용자 및 그룹의 요약이 표시됩니다.

9. 감사 항목 * 상자에서 SACL 항목을 표시할 사용자 또는 그룹을 선택합니다.
10. 편집 * 을 클릭합니다.

    object>에 대한 감사 항목이 열립니다.

11. Access* 상자에서 선택한 개체에 적용된 현재 SACL을 확인합니다.
12. 객체> * 에 대한 * 감사 항목을 닫으려면 * 취소 * 를 클릭합니다.
13. 취소 * 를 클릭하여 * 감사 * 상자를 닫습니다.

ONTAP FlexVol 볼륨의 **NTFS** 감사 정책에 대한 정보를 표시합니다

FlexVol 볼륨에서 보안 스타일 및 효과적인 보안 스타일의 정의, 적용되는 권한 및 시스템 액세스 제어 목록에 대한 정보를 포함하여 NTFS 감사 정책에 대한 정보를 표시할 수 있습니다. 이 정보를 사용하여 보안 구성을 확인하거나 감사 문제를 해결할 수 있습니다.

이 작업에 대해

파일 및 디렉터리에 적용된 감사 정책에 대한 정보를 표시하면 지정된 파일 및 폴더에 적절한 SACL(시스템 액세스 제어 목록)이 설정되어 있는지 확인할 수 있습니다.

SVM(스토리지 가상 시스템)의 이름과 감사 정보를 표시할 파일 또는 폴더의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- NTFS 보안 스타일 볼륨 및 qtree는 감사 정책에 NTFS SACL(시스템 액세스 제어 목록)만 사용합니다.
- NTFS 효과적인 보안이 적용된 혼합 보안 스타일 볼륨의 파일과 폴더에 NTFS 감사 정책이 적용될 수 있습니다.

  혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉토리 등 UNIX 파일 권한을 사용하는 일부 파일과 디렉토리가 포함될 수 있습니다.

- 혼합 보안 형식 볼륨의 최상위 수준에는 UNIX 또는 NTFS의 효과적인 보안이 포함될 수 있으며 NTFS SACL이 포함될 수도 있고 포함되지 않을 수도 있습니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 파일 및 폴더 NFSv4 SACL 및 Storage-Level Access Guard NTFS SACL이 모두 표시될 수 있습니다.
- 명령에 입력한 경로가 NTFS 유효 보안을 사용하는 데이터인 경우 해당 파일 또는 디렉토리 경로에 동적 액세스 제어가 구성되어 있으면 동적 액세스 제어 ACE에 대한 정보도 출력에 표시됩니다.
- NTFS 유효 보안이 있는 파일 및 폴더에 대한 보안 정보를 표시할 때 UNIX 관련 출력 필드에는 표시 전용 UNIX 파일 권한 정보가 포함됩니다.

  NTFS 보안 스타일 파일 및 폴더는 파일 액세스 권한을 결정할 때 NTFS 파일 권한과 Windows 사용자 및 그룹만 사용합니다.

- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

  모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 폴더의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.

단계

1. 파일 및 디렉터리 감사 정책 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면…	다음 명령을 입력합니다…
요약 양식	'vserver security file-directory show -vserver vserver_name -path path path'
를 참조하십시오	'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true'

예

다음 예에서는 SVM VS1 경로의 /Corp 경로에 대한 감사 정책 정보를 표시합니다. 경로에 NTFS 유효 보안이 있습니다. NTFS 보안 설명자는 성공 및 성공/실패 SACL 항목을 모두 포함합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

다음 예제는 SVM VS1 경로의 /datavol1 경로에 대한 감사 정책 정보를 표시합니다. 이 경로에는 일반 파일 및 폴더 SACL과 Storage-Level Access Guard SACL이 모두 포함됩니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

와일드카드 문자를 사용하여 **ONTAP** 파일 보안 및 감사 정책에 대한 정보를 표시합니다

와일드카드 문자(*)를 사용하여 지정된 경로 또는 루트 볼륨 아래에 있는 모든 파일 및 디렉토리의 파일 보안 및 감사 정책에 대한 정보를 표시할 수 있습니다.

와일드카드 문자(*)는 모든 파일 및 디렉터리의 정보를 표시할 아래의 지정된 디렉터리 경로의 마지막 하위 구성 요소로 사용할 수 있습니다.

"*"로 명명된 특정 파일 또는 디렉토리의 정보를 표시하려면 큰따옴표("") 안에 전체 경로를 제공해야 합니다.

예

와일드카드 문자를 사용하여 다음 명령을 실행하면 SVM VS1 경로의 '/1/' 아래에 있는 모든 파일 및 디렉토리에 대한 정보가 표시됩니다.

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
          Security Style: mixed
         Effective Style: ntfs
          DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
          Security Style: mixed
         Effective Style: ntfs
          DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

다음 명령을 실행하면 SVM VS1 의 path '/vol1/a' 아래에 " * "로 명명된 파일의 정보가 표시됩니다. 경로는 큰따옴표(" ")로 묶습니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                  Vserver: vs1
                File Path: "/vol1/a/*"
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

감사할 수 있는 **CLI** 변경 이벤트입니다

감사 가능한 **ONTAP CLI** 변경 이벤트에 대해 알아보십시오

ONTAP는 특정 SMB 공유 이벤트, 특정 감사 정책 이벤트, 특정 로컬 보안 그룹 이벤트, 로컬 사용자 그룹 이벤트 및 인증 정책 이벤트를 비롯한 특정 CLI 변경 이벤트를 감사할 수 있습니다. 감사할 수 있는 변경 이벤트를 이해하면 이벤트 로그의 결과를 해석할 때 도움이 됩니다.

감사 로그를 수동으로 회전하고, 감사를 설정 또는 비활성화하고, 변경 이벤트 감사 정보를 표시하고, 변경 이벤트 감사 및 감사 변경 이벤트를 수정하여, CLI 변경 이벤트를 감사하여 스토리지 가상 시스템(SVM) 감사 CLI 변경 이벤트를 관리할 수 있습니다.

관리자 권한으로 SMB-share, 로컬 사용자 그룹, 로컬 보안 그룹, 인증 정책 및 감사 정책 이벤트와 관련된 구성을 변경하기 위해 명령을 실행하는 경우 레코드가 생성되고 해당 이벤트가 감사됩니다.

감사 범주	이벤트	이벤트 ID입니다	이 명령 실행…
Mhost 감사	정책 변경	[4719] 감사 구성이 변경되었습니다	'vserver audit disable

enable	modify'	파일 공유	[5142] 네트워크 공유가 추가되었습니다
'vserver cifs share create	[5143] 네트워크 공유가 수정되었습니다	'vserver cifs share modify"vserver cifs share create	modify
delete"vserver cifs share add	remove'	[5144] 네트워크 공유가 삭제되었습니다	'vserver cifs share delete
감사	사용자 계정	[4720] 로컬 사용자가 생성되었습니다	'vserver cifs users-and-groups local-user create"vserver services name-service unix-user create'를 참조하십시오
[4722] 로컬 사용자가 활성화되었습니다	'vserver cifs users-and-groups local-user create	modify'를 참조하십시오	[4724] 로컬 사용자 암호 재설정
'vserver cifs users-and-groups local-user set-password	[4725] 로컬 사용자가 비활성화되었습니다	'vserver cifs users-and-groups local-user create	modify'를 참조하십시오
[4726] 로컬 사용자가 삭제되었습니다	'vserver cifs users-and-groups local-user delete"vserver services name-service unix-user delete"를 선택합니다	[4738] 로컬 사용자 변경	'vserver cifs users-and-groups local-user modify"vserver services name-service unix-user modify"를 선택합니다
[4781] 로컬 사용자 이름 바꾸기	'vserver cifs users-and-groups local-user rename'을 선택합니다	보안 그룹	[4731] 로컬 보안 그룹이 생성되었습니다
'vserver cifs users-and-groups local-group create"vserver services name-service unix-group create'를 참조하십시오	[4734] 로컬 보안 그룹이 삭제되었습니다	SVM CIFS 사용자-그룹 로컬-그룹 삭제 SVM 서비스 이름-서비스 UNIX-그룹 삭제	[4735] 로컬 보안 그룹이 수정되었습니다
vserver cifs users-and-groups local-group rename	modify ``vserver services name-service unix-group modify''라는 이름의 가상 서버 사용자 및 그룹 로컬 그룹 이름 변경	[4732] 사용자가 로컬 그룹에 추가되었습니다	가상 CIFS 사용자 및 그룹 로컬 그룹 추가 멤버 가상 서버 서비스 이름 서비스 unix 그룹 추가 사용자
[4733] 사용자가 로컬 그룹에서 제거되었습니다	SVM CIFS 사용자-그룹 local-group remove-멤버들 vserver services name-service unix-group deluser	authorization-policy-change를 참조하십시오	[4704] 사용자 권한이 할당되었습니다

'vserver cifs users-and-groups Privilege add-privilege'	[4705] 사용자 권한이 제거되었습니다	'vserver cifs users-and-groups Privilege remove-Privilege	reset-Privilege

관련 정보

- "SVM"

파일 공유 **ONTAP** 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 파일 공유 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다. 파일 공유 이벤트는 SMB 네트워크 공유가 'vserver cifs share' 관련 명령을 사용하여 수정될 때 생성됩니다.

이벤트 ID 5142, 5143 및 5144와 파일 공유 이벤트는 SVM에 대해 SMB 네트워크 공유를 추가, 수정 또는 삭제할 때 생성됩니다. SMB 네트워크 공유 구성은 'CIFS share access control create | modify | delete' 명령을 사용하여 수정합니다.

다음 예에서는 'audit_dest'라는 공유 객체가 생성될 때 ID 5143이 생성된 파일 공유 이벤트를 표시합니다.

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

감사 정책 변경 **ONTAP** 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 감사 정책 변경 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다. Audit-policy-change 이벤트는 'vserver audit' 관련 명령어를 이용하여 Audit 정책을 수정할 때 발생한다.

이벤트 ID 4719를 사용하는 감사 정책 변경 이벤트는 감사 정책이 사용 안 함, 사용 또는 수정될 때마다 생성되며 사용자가 트랙을 커버하기 위해 감사를 비활성화하려고 시도하는 시점을 식별하는 데 도움이 됩니다. 기본적으로 구성되어 있으며 비활성화하려면 진단 권한이 필요합니다.

다음 예제에서는 감사가 비활성화된 경우 ID 4719가 생성된 감사 정책 변경 이벤트를 표시합니다.

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

사용자 계정 **ONTAP** 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 사용자 계정 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다.

이벤트 ID 4720, 4722, 4724, 4725, 4726, 4738 및 4781은 로컬 SMB 또는 NFS 사용자가 시스템에서 생성 또는 삭제되거나, 로컬 사용자 계정이 활성화, 비활성화 또는 수정되고, 로컬 SMB 사용자 암호가 재설정 또는 변경될 때 생성됩니다. 사용자 계정 이벤트는 사용자 계정이 'vserver cifs users-and-groups_<local user>_' 및 'vserver services name-service_<unix user>_' 명령을 사용하여 수정될 때 생성됩니다.

다음 예에서는 로컬 SMB 사용자가 생성될 때 ID 4720이 생성된 사용자 계정 이벤트를 표시합니다.

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

다음 예제에서는 앞의 예제에서 만든 로컬 SMB 사용자의 이름이 변경된 경우 ID 4781이 생성된 사용자 계정 이벤트를 표시합니다.

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

보안 그룹 **ONTAP** 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 보안 그룹 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다.

이벤트 ID 4731, 4732, 4733, 4734 및 4735가 포함된 보안 그룹 이벤트는 로컬 SMB 또는 NFS 그룹이 시스템에서 생성 또는 삭제되고 로컬 사용자가 그룹에서 추가 또는 제거될 때 생성됩니다. 사용자 계정이 'vserver cifs users-and-groups_<local-group>_' 및 'vserver services name-service_<unix-group>_' 명령을 사용하여 수정될 때 security-group-events가 생성됩니다.

다음 예에서는 로컬 UNIX 보안 그룹이 생성될 때 ID 4731이 생성된 보안 그룹 이벤트를 표시합니다.

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

authorization-policy-change ONTAP 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 인증 정책 변경 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다.

이벤트 ID 4704 및 4705의 권한 부여 정책 변경 이벤트는 SMB 사용자 및 SMB 그룹에 대해 권한 부여 권한이 부여되거나 취소될 때마다 생성됩니다. authorization-policy-change 이벤트는 vserver cifs users-and-groups 권한 관련 명령을 사용하여 권한 부여 권한이 할당되거나 취소될 때 생성됩니다.

다음 예에서는 SMB 사용자 그룹에 대한 인증 권한이 할당된 경우 ID 4704가 생성된 인증 정책 이벤트를 표시합니다.

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

감사 구성을 관리합니다

감사 이벤트 로그를 수동으로 회전하여 특정 **ONTAP SVM** 이벤트 로그를 확인합니다

감사 이벤트 로그를 보려면 먼저 로그를 사용자가 읽을 수 있는 형식으로 변환해야 합니다. ONTAP이 로그를 자동으로 회전하기 전에 특정 SVM(스토리지 가상 시스템)의 이벤트 로그를 보려는 경우 SVM에서 감사 이벤트 로그를 수동으로 회전할 수 있습니다.

단계

1. vserver audit rotate -log 명령을 사용하여 감사 이벤트 로그를 회전합니다.

   'vserver audit rotate-log-vserver vs1'

   감사 이벤트 로그는 SVM 감사 이벤트 로그 디렉토리에 감사 구성('XML' 또는 'evtx')에 지정된 형식으로 저장되며, 적절한 애플리케이션을 사용하여 볼 수 있습니다.

ONTAP SVM에 대한 감사 기능 사용 또는 사용 안 함

SVM(스토리지 가상 머신)에 대한 감사를 설정하거나 해제할 수 있습니다. 감사를 비활성화하여 파일 및 디렉터리 감사를 일시적으로 중지할 수 있습니다. 감사 구성이 있는 경우 언제든지 감사를 활성화할 수 있습니다.

시작하기 전에

SVM에 대한 감사를 활성화하려면 먼저 SVM의 감사 구성이 이미 존재해야 합니다.

"감사 구성을 만듭니다"

이 작업에 대해

감사를 사용하지 않도록 설정해도 감사 구성은 삭제되지 않습니다.

단계

1. 적절한 명령을 수행합니다.

감사를 원하는 경우…	명령 입력…
활성화됨	'vserver audit enable - vserver vserver_name'
사용 안 함	'vserver audit disable-vserver vserver_name'

2. 감사가 원하는 상태인지 확인합니다.

   'vserver audit show -vserver vserver_name'

예

다음 예에서는 SVM VS1 에 대한 감사를 설정합니다.

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                               Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

다음 예에서는 SVM VS1 에 대한 감사를 해제합니다.

```
cluster1::> vserver audit disable -vserver vs1

                                Vserver: vs1
                      Auditing state: false
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

ONTAP 감사 구성에 대한 정보를 표시합니다

감사 구성에 대한 정보를 표시할 수 있습니다. 이 정보를 통해 각 SVM에 대해 구성이 현재 위치에서 원하는 것인지 확인할 수 있습니다. 표시된 정보를 사용하여 감사 구성이 설정되었는지 여부를 확인할 수도 있습니다.

이 작업에 대해

모든 SVM의 감사 구성에 대한 자세한 정보를 표시하거나 선택적 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다. 선택적 매개 변수를 지정하지 않으면 다음 항목이 표시됩니다.

- 감사 구성이 적용되는 SVM 이름입니다
- 진실 허위일 수 있는 감사 상태

  감사 상태가 true이면 감사가 활성화됩니다. 감사 상태가 false이면 감사가 비활성화됩니다.

- 감사할 이벤트의 범주입니다
- 감사 로그 형식입니다
- 감사 하위 시스템이 통합 및 변환된 감사 로그를 저장하는 대상 디렉토리입니다

단계

1. vserver audit show 명령을 사용하여 감사 구성에 대한 정보를 표시합니다.

   에 대한 자세한 내용은 `vserver audit show` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 예에서는 모든 SVM에 대한 감사 구성을 요약하여 표시합니다.

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

다음 예에서는 모든 SVM에 대한 모든 감사 구성 정보를 목록 형식으로 표시합니다.

```
cluster1::> vserver audit show -instance

                              Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
```

감사 구성을 수정하기 위한 **ONTAP** 명령

감사 설정을 변경하려면 로그 경로 대상 및 로그 형식 수정, 감사할 이벤트 범주 수정, 로그 파일을 자동으로 저장하는 방법, 저장할 최대 로그 파일 수 지정 등 언제든지 현재 구성을 수정할 수 있습니다.

원하는 작업	이 명령 사용…
로그 대상 경로를 수정합니다	'-destination' 매개 변수를 사용하여 vserver audit modify를 수행합니다
감사할 이벤트 범주를 수정합니다	'-events' 매개 변수를 사용하여 vserver audit modify를 수행합니다 중앙 액세스 정책 스테이징 이벤트를 감사하려면 스토리지 가상 머신(SVM)에서 DAC(Dynamic Access Control) SMB 서버 옵션을 활성화해야 합니다.
로그 형식을 수정합니다	vserver audit modify는 -format 매개 변수를 사용합니다

내부 로그 파일 크기에 따라 자동 저장을 사용하도록 설정합니다	'-rotate-size' 파라미터를 사용한 vserver audit modify
시간 간격에 따라 자동 저장을 사용하도록 설정합니다	vserver audit modify with the '-rotate-schedule-month', '-rotate-schedule-dayOfWeek', '-rotate-schedule-day', '-rotate-schedule-hour', '-rotate-schedule-minute' 매개 변수를 사용합니다
저장된 로그 파일의 최대 개수를 지정합니다	'-rotate-limit' 파라미터를 사용한 vserver audit modify

ONTAP SVM에서 감사 구성을 삭제합니다

더 이상 SVM(스토리지 가상 시스템)의 파일 및 디렉토리 이벤트를 감사하지 않고 SVM에 대한 감사 구성을 유지하고 싶지 않으면 감사 구성을 삭제할 수 있습니다.

단계

1. 감사 구성을 사용하지 않도록 설정합니다.

   'vserver audit disable-vserver vserver_name'

   'vserver audit disable - vserver vs1'

2. 감사 구성을 삭제합니다.

   'vserver audit delete - vserver vserver_name'

   'vserver audit delete - vserver vs1'

감사된 **ONTAP** 클러스터를 되돌리는 것의 영향을 이해합니다

클러스터를 되돌리려는 경우 클러스터에 감사 기능이 설정된 SVM(스토리지 가상 머신)이 있을 때 ONTAP에서 따르는 복원 프로세스에 대해 알고 있어야 합니다. 되돌리기 전에 특정 조치를 취해야 합니다.

SMB 로그온 및 로그오프 이벤트 및 중앙 액세스 정책 스테이징 이벤트에 대한 감사를 지원하지 않는 **ONTAP** 버전으로 되돌립니다

SMB 로그온 및 로그오프 이벤트 감사 및 중앙 액세스 정책 스테이징 이벤트는 clustered Data ONTAP 8.3에서 시작됩니다. 이러한 이벤트 유형을 지원하지 않는 ONTAP 버전으로 되돌리려고 하고 이러한 이벤트 유형을 모니터링하는 감사 구성이 있는 경우, 되돌리기 전에 감사 기능이 설정된 SVM에 대한 감사 구성을 변경해야 합니다. 파일 작업 이벤트만 감사되도록 구성을 수정해야 합니다.

ONTAP 감사 및 스테이징 볼륨 공간 문제 해결

스테이징 볼륨 또는 감사 이벤트 로그가 포함된 볼륨에 공간이 부족할 때 문제가 발생할 수 있습니다. 공간이 부족하면 새 감사 레코드를 생성할 수 없으므로 클라이언트가 데이터에 액세스하지 못하게 되고 액세스 요청이 실패합니다. 이러한 볼륨 공간 문제를 해결하고 해결하는 방법을 알아야 합니다.

이벤트 로그 볼륨과 관련된 공간 문제를 해결합니다

이벤트 로그 파일이 포함된 볼륨의 공간이 부족한 경우 감사 기능은 로그 레코드를 로그 파일로 변환할 수 없습니다. 이로 인해 클라이언트 액세스 장애가 발생합니다. 이벤트 로그 볼륨과 관련된 공간 문제를 해결하는 방법을 알고 있어야 합니다.

- 스토리지 가상 머신(SVM) 및 클러스터 관리자는 볼륨 및 애그리게이트의 사용 및 구성에 대한 정보를 표시하여 볼륨 공간이 부족한지 여부를 확인할 수 있습니다.
- 이벤트 로그가 포함된 볼륨에 공간이 부족하면 SVM 및 클러스터 관리자가 이벤트 로그 파일 중 일부를 제거하거나 볼륨 크기를 늘려 공간 문제를 해결할 수 있습니다.

> ⓘ 이벤트 로그 볼륨이 포함된 애그리게이트는 가득 찬 경우, 볼륨의 크기를 늘리려면 애그리게이트의 크기를 늘려야 합니다. 클러스터 관리자만 집계 크기를 늘릴 수 있습니다.

- 감사 구성을 수정하여 이벤트 로그 파일의 대상 경로를 다른 볼륨의 디렉토리로 변경할 수 있습니다.

> ⓘ 다음과 같은 경우 데이터 액세스가 거부됩니다.
>
> - 대상 디렉토리가 삭제됩니다.
> - 대상 디렉토리를 호스팅하는 볼륨에 대한 파일 제한이 최대 레벨에 도달합니다.

자세히 알아보기:

- "볼륨에 대한 정보를 보고 볼륨 크기를 늘리는 방법".
- "Aggregate에 대한 정보를 보고 애그리게이트를 관리하는 방법".

스테이징 볼륨과 관련된 공간 문제를 해결합니다

SVM(Storage Virtual Machine)에 대한 스테이징 파일이 포함된 볼륨 중 공간이 부족한 경우 감사를 통해 로그 레코드를 스테이징 파일에 쓸 수 없습니다. 이로 인해 클라이언트 액세스 장애가 발생합니다. 이 문제를 해결하려면 SVM에 사용된 스테이징 볼륨이 볼륨 사용에 대한 정보를 표시하여 가득 찼는지 여부를 확인해야 합니다.

통합된 이벤트 로그 파일이 포함된 볼륨에 충분한 공간이 있지만 공간 부족으로 인해 여전히 클라이언트 액세스 장애가 발생하는 경우 스테이징 볼륨의 공간이 부족할 수 있습니다. SVM 관리자는 SVM을 위한 스테이징 파일이 포함된 스테이징 볼륨의 공간이 부족한지 여부를 확인하기 위해 여러분에게 연락해야 합니다. 감사 하위 시스템은 스테이징 볼륨의 공간이 부족하여 감사 이벤트를 생성할 수 없는 경우 EMS 이벤트를 생성합니다. 장치에 남은 공간이 없습니다라는 메시지가 표시됩니다. 스테이징 볼륨에 대한 정보는 사용자만 볼 수 있으며 SVM 관리자는 볼 수 없습니다.

모든 스테이징 볼륨 이름은 mdv_AUD_ 로 시작하고 그 스테이징 볼륨을 포함하는 애그리게이트의 UUID로 시작합니다. 다음 예에서는 클러스터 내의 데이터 SVM에 대한 파일 서비스 감사 구성을 생성할 때 자동으로 생성되는 admin SVM의 시스템 볼륨 4개를 보여 줍니다.

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          5GB     4.75GB
5%
4 entries were displayed.
```

스테이징 볼륨에 공간이 부족하면 볼륨 크기를 늘려 공간 문제를 해결할 수 있습니다.

> ⓘ 스테이징 볼륨이 포함된 aggregate가 가득 찬 경우 볼륨의 크기를 늘리려면 애그리게이트의 크기를 늘려야 합니다. 애그리게이트의 크기를 늘릴 수 있는 것은 없으며 SVM 관리자는 불가능합니다.

하나 이상의 애그리게이트에서 사용 가능한 공간이 2GB 미만(ONTAP 9.14.1 이하) 또는 5GB(ONTAP 9.15.1부터 시작)인 경우 SVM 감사 생성이 실패합니다. SVM 감사 생성에 실패하면 생성된 스테이징 볼륨이 삭제됩니다.

SVM에서 파일 모니터링 및 관리를 위해 FPolicy를 사용합니다

FPolicy 이해

ONTAP FPolicy 솔루션에 대해 알아보세요

FPolicy는 파트너 솔루션을 통해 SVM(스토리지 가상 머신)의 파일 액세스 이벤트를 모니터링 및 관리하는 데 사용되는 파일 액세스 알림 프레임워크입니다. 파트너 솔루션을 사용하면 데이터 거버넌스 및 규정 준수, 랜섬웨어 보호 및 데이터 이동성과 같은 다양한 사용 사례를 해결할 수 있습니다.

파트너 솔루션에는 NetApp 지원 타사 솔루션과 NetApp 제품 워크로드 보안과 Cloud Data Sense가 모두 포함됩니다.

FPolicy 솔루션에는 두 가지 부품이 있습니다. ONTAP FPolicy 프레임워크는 클러스터의 활동을 관리하고 파트너 애플리케이션(일명 외부 FPolicy 서버)에 알림을 보냅니다. 외부 FPolicy 서버는 ONTAP FPolicy에서 보낸 알림을 처리하여 고객 사용 사례를 이행합니다.

ONTAP 프레임워크는 FPolicy 구성을 생성하고 유지하며 파일 이벤트를 모니터링하고 외부 FPolicy 서버에 알림을 보냅니다. ONTAP FPolicy는 외부 FPolicy 서버와 SVM(스토리지 가상 머신) 노드 간의 통신을 허용하는 인프라를

제공합니다.

FPolicy 프레임워크는 외부 FPolicy 서버에 연결되며, 클라이언트 액세스의 결과로 특정 파일 시스템 이벤트에 대한 알림을 FPolicy 서버로 보냅니다. 외부 FPolicy 서버에서 알림을 처리하고 응답을 노드로 다시 보냅니다. 알림 처리 결과로 발생하는 작업은 응용 프로그램과 노드와 외부 서버 간의 통신이 비동기 또는 동기인지 여부에 따라 달라집니다.

ONTAP FPolicy 동기 및 비동기 알림

FPolicy는 FPolicy 인터페이스를 통해 외부 FPolicy 서버에 알림을 보냅니다. 알림은 동기 또는 비동기 모드로 전송됩니다. 알림 모드는 FPolicy 서버에 알림을 보낸 후 ONTAP에서 수행하는 작업을 결정합니다.

- * 비동기 알림 *

  비동기 알림을 사용할 경우 노드는 FPolicy 서버의 응답을 기다리지 않으므로 시스템의 전반적인 처리량이 향상됩니다. 이 유형의 알림은 FPolicy 서버에서 알림 평가의 결과로 어떤 작업도 수행할 필요가 없는 애플리케이션에 적합합니다. 예를 들어, 스토리지 가상 시스템(SVM) 관리자가 파일 액세스 활동을 모니터링하고 감사하려고 할 때 비동기 알림이 사용됩니다.

  비동기 모드에서 작동하는 FPolicy 서버에서 네트워크 중단이 발생하는 경우, 정전 중에 생성된 FPolicy 알림은 스토리지 노드에 저장됩니다. FPolicy 서버가 온라인 상태로 돌아오면 저장된 알림에 대한 알림이 표시되고 스토리지 노드에서 가져올 수 있습니다. 정전 중에 알림을 저장할 수 있는 시간은 최대 10분까지 구성할 수 있습니다.

  ONTAP 9.14.1부터 FPolicy를 사용하면 SVM의 비동기적 정책에 대한 파일 액세스 이벤트를 캡처하는 영구 저장소를 설정할 수 있습니다. 영구 저장소는 클라이언트 I/O 처리를 FPolicy 알림 처리와 분리하여 클라이언트 지연 시간을 줄여 줍니다. 동기(필수 또는 비필수) 및 비동기 필수 구성은 지원되지 않습니다.

- * 동기식 알림 *

  동기식 모드에서 실행하도록 구성된 경우 FPolicy 서버는 클라이언트 작업을 계속하기 전에 모든 알림을 확인해야 합니다. 이 유형의 알림은 알림 평가 결과에 따라 조치가 필요한 경우에 사용됩니다. 예를 들어, SVM 관리자가 외부 FPolicy 서버에 지정된 기준에 따라 요청을 허용하거나 거부하려는 경우 동기식 알림이 사용됩니다.

동기 및 비동기 애플리케이션

FPolicy 애플리케이션은 비동기식 및 동기식 모두에서 사용할 수 있습니다.

비동기식 애플리케이션은 외부 FPolicy 서버가 파일 또는 디렉토리에 대한 액세스를 변경하거나 SVM(스토리지 가상 머신)의 데이터를 수정하지 않는 애플리케이션입니다. 예를 들면 다음과 같습니다.

- 파일 액세스 및 감사 로깅
- 스토리지 리소스 관리

동기식 애플리케이션은 데이터 액세스가 변경되거나 외부 FPolicy 서버에 의해 데이터가 수정된 애플리케이션입니다. 예를 들면 다음과 같습니다.

- 할당량 관리
- 파일 액세스 차단
- 파일 아카이빙 및 계층적 스토리지 관리

- 암호화 및 암호 해독 서비스
- 압축 및 압축 해제 서비스

ONTAP FPolicy 영구 저장소

영구 저장소는 클라이언트 I/O 처리를 FPolicy 알림 처리와 분리하여 클라이언트 지연 시간을 줄여 줍니다. ONTAP 9.14.1부터 SVM의 비동기적 정책에 대한 파일 액세스 이벤트를 캡처하는 FPolicy 영구 저장소를 설정할 수 있습니다. 동기(필수 또는 비필수) 및 비동기 필수 구성은 지원되지 않습니다.

이 기능은 FPolicy 외부 모드에서만 사용할 수 있습니다. 사용하는 파트너 응용 프로그램이 이 기능을 지원해야 합니다. 파트너와 협력하여 이 FPolicy 구성이 지원되도록 해야 합니다.

ONTAP 9.15.1부터 FPolicy 영구 저장소 구성이 단순화됩니다. 를 클릭합니다 `persistent-store create` 명령은 SVM에 대한 볼륨 생성을 자동화하고 영구 저장소 모범 사례에 따라 볼륨을 구성합니다.

영구 저장소 모범 사례에 대한 자세한 내용은 을 참조하십시오 "FPolicy를 구성하기 위한 요구사항, 고려 사항 및 모범 사례".

영구 저장소 추가에 대한 자세한 내용은 을 참조하십시오 "영구 저장소를 만듭니다".

ONTAP FPolicy 구성 유형

기본 FPolicy 구성 유형은 두 가지입니다. 하나의 구성에서는 외부 FPolicy 서버를 사용하여 알림을 처리하고 처리합니다. 다른 구성에서는 외부 FPolicy 서버를 사용하지 않습니다. 대신 ONTAP 내부 기본 FPolicy 서버를 사용하여 확장자에 따라 간단한 파일 차단을 수행합니다.

- * 외부 FPolicy 서버 구성 *

  이 알림은 FPolicy 서버로 전송됩니다. FPolicy 서버는 요청을 심사하고 규칙을 적용하여 노드에서 요청된 파일 작업을 허용할 것인지 결정합니다. 그런 다음 동기식 정책의 경우 FPolicy 서버가 노드에 응답을 보내 요청된 파일 작업을 허용하거나 차단합니다.

- * 기본 FPolicy 서버 구성 *

  알림은 내부적으로 스크리닝됩니다. FPolicy 범위에 구성된 파일 확장명 설정에 따라 요청이 허용되거나 거부됩니다.

- 참고 *: 거부된 파일 확장 요청은 기록되지 않습니다.

기본 FPolicy 구성을 생성하는 경우

기본 FPolicy 구성에서는 ONTAP 내부 FPolicy 엔진을 사용하여 파일의 확장명에 따라 파일 작업을 모니터링하고 차단합니다. 이 솔루션에는 외부 FPolicy 서버(FPolicy 서버)가 필요하지 않습니다. 이 간단한 솔루션이 필요한 경우 기본 파일 차단 구성을 사용하는 것이 좋습니다.

기본 파일 차단을 사용하면 구성된 작업 및 필터링 이벤트와 일치하는 모든 파일 작업을 모니터링한 다음 특정 확장명을 가진 파일에 대한 액세스를 거부할 수 있습니다. 기본 구성입니다.

이 구성은 파일 확장자만을 기준으로 파일 액세스를 차단하는 방법을 제공합니다. 예를 들어, 'P3' 확장자가 포함된 파일을 차단하려면 'P3'의 대상 파일 확장자를 가진 특정 작업에 대한 알림을 제공하는 정책을 구성합니다. 이 정책은

알림을 생성하는 작업에 대한 mP3 파일 요청을 거부하도록 구성되어 있습니다.

다음은 기본 FPolicy 구성에 적용됩니다.

- FPolicy 서버 기반 파일 검사에서 지원되는 것과 동일한 필터 및 프로토콜 세트도 기본 파일 차단에 대해 지원됩니다.
- 기본 파일 차단 및 FPolicy 서버 기반 파일 검사 애플리케이션을 동시에 구성할 수 있습니다.

  이렇게 하려면 기본 파일 차단용으로 구성된 정책 하나와 FPolicy 서버 기반 파일 검사용으로 구성된 정책 하나를 사용하여 SVM(스토리지 가상 머신)에 대해 두 개의 개별 FPolicy 정책을 구성할 수 있습니다.

- 기본 파일 차단 기능은 파일 내용이 아닌 확장자에 따라 파일을 심사합니다.
- 심볼 링크의 경우 네이티브 파일 차단은 루트 파일의 파일 확장명을 사용합니다.

에 대해 자세히 알아보십시오 "FPolicy: 기본 파일 차단".

외부 **FPolicy** 서버를 사용하는 구성을 생성하는 시기

외부 FPolicy 서버를 사용하여 알림을 처리 및 관리하는 FPolicy 구성은 파일 확장자에 따라 단순한 파일 차단이 필요한 사용 사례에 적합한 강력한 솔루션을 제공합니다.

파일 액세스 이벤트를 모니터링 및 기록하고, 할당량 서비스를 제공하고, 단순 파일 확장자 이외의 기준에 따라 파일 차단을 수행하고, 계층적 스토리지 관리 애플리케이션을 사용하여 데이터 마이그레이션 서비스를 제공하려는 경우에 외부 FPolicy 서버를 사용하는 구성을 생성해야 합니다. 스토리지 가상 시스템(SVM)의 데이터 서브셋만 모니터링하는 세부적인 정책 세트를 제공할 수도 있습니다.

ONTAP FPolicy 구현에서의 클러스터 구성 요소 역할

클러스터와 포함된 SVM(스토리지 가상 머신) 및 데이터 LIF는 모두 FPolicy 구현에서 역할을 합니다.

- * 클러스터 *

  클러스터는 FPolicy 관리 프레임워크를 포함하고 클러스터의 모든 FPolicy 구성에 대한 정보를 유지 관리하고 관리합니다.

- * SVM *

  FPolicy 구성은 SVM 레벨에서 정의됩니다. 구성 범위는 SVM 이며 SVM 리소스에서만 작동합니다. 한 SVM 구성은 다른 SVM에 상주하는 데이터에 대한 파일 액세스 요청을 모니터링하고 알림을 전송할 수 없습니다.

  FPolicy 구성은 관리 SVM에서 정의할 수 있습니다. 관리 SVM에서 구성을 정의하면 모든 SVM에서 구성을 확인하고 사용할 수 있습니다.

- 데이터 LIF *

  FPolicy 서버에 대한 연결은 FPolicy 구성을 사용하여 SVM에 속하는 데이터 LIF를 통해 이루어집니다. 이러한 연결에 사용되는 데이터 LIF는 일반 클라이언트 액세스에 사용되는 데이터 LIF와 같은 방법으로 페일오버할 수 있습니다.

ONTAP FPolicy가 외부 FPolicy 서버와 작동하는 방식

스토리지 가상 시스템(SVM)에서 FPolicy를 구성하고 사용하도록 설정한 후에는 SVM이 참여하는 모든 노드에서 FPolicy가 실행됩니다. FPolicy는 알림 처리를 위해 외부 FPolicy 서버(FPolicy 서버)와의 연결을 설정하고 유지하는 동시에 FPolicy 서버와 주고받는 알림 메시지를 관리하는 역할을 합니다.

또한 연결 관리의 일환으로 FPolicy는 다음과 같은 책임을 수행합니다.

- 파일 알림이 올바른 LIF를 통해 FPolicy 서버로 흐르도록 합니다.
- 여러 FPolicy 서버가 정책에 연결될 때 FPolicy 서버로 알림을 보낼 때 로드 밸런싱이 수행됩니다.
- FPolicy 서버에 대한 연결이 끊어지면 연결을 다시 설정하려고 시도합니다.
- 인증된 세션을 통해 FPolicy 서버에 알림을 보냅니다.
- 패스스루 읽기가 활성화된 경우 FPolicy 서버에서 클라이언트 요청을 처리하기 위해 설정하는 패스스루 읽기 데이터 연결을 관리합니다.

FPolicy 통신에는 제어 채널이 어떻게 사용됩니다

FPolicy는 스토리지 가상 머신(SVM)에 참여하는 각 노드의 데이터 LIF에서 외부 FPolicy 서버에 대한 제어 채널 연결을 시작합니다. FPolicy는 제어 채널을 사용하여 파일 알림을 전송합니다. 따라서 FPolicy 서버는 SVM 토폴로지를 기준으로 여러 개의 제어 채널 연결을 볼 수 있습니다.

동기 통신에 권한 있는 데이터 액세스 채널이 사용되는 방식

동기식 사용 사례에서 FPolicy 서버는 권한이 있는 데이터 액세스 경로를 통해 SVM(스토리지 가상 머신)에 있는 데이터에 액세스합니다. 권한 있는 경로를 통해 액세스하면 전체 파일 시스템이 FPolicy 서버에 노출됩니다. IT 부서는 데이터 파일에 액세스하여 정보를 수집하고, 파일을 스캔하거나, 파일을 읽거나, 파일에 쓸 수 있습니다.

외부 FPolicy 서버가 권한 있는 데이터 채널을 통해 SVM 루트에서 전체 파일 시스템에 액세스할 수 있으므로 권한이 있는 데이터 채널 연결이 보안되어야 합니다.

권한 있는 데이터 액세스 채널에서 FPolicy 연결 자격 증명을 사용하는 방법

FPolicy 서버는 FPolicy 구성과 함께 저장된 특정 Windows 사용자 자격 증명을 사용하여 클러스터 노드에 대한 권한 있는 데이터 액세스 연결을 만듭니다. SMB는 권한이 있는 데이터 액세스 채널 연결을 만들기 위해 지원되는 유일한 프로토콜입니다.

FPolicy 서버에 권한이 있는 데이터 액세스가 필요한 경우 다음 조건을 충족해야 합니다.

- 클러스터에서 SMB 라이센스를 활성화해야 합니다.
- FPolicy 서버는 FPolicy 구성에 구성된 자격 증명에서 실행해야 합니다.

데이터 채널을 연결할 때 FPolicy는 지정된 Windows 사용자 이름에 대한 자격 증명을 사용합니다. admin 공유 ONTAP_admin$에서 데이터 액세스가 가능합니다.

권한 있는 데이터 액세스를 위해 수퍼 사용자 자격 증명을 부여하는 것은 무엇을 의미하는지

ONTAP는 FPolicy 구성에 구성된 IP 주소와 사용자 자격 증명의 조합을 사용하여 수퍼 사용자 자격 증명을 FPolicy 서버에 부여합니다.

수퍼 사용자 상태는 FPolicy 서버가 데이터에 액세스할 때 다음 권한을 부여합니다.

- 권한 검사를 피하십시오

  사용자는 파일 및 디렉터리 액세스에 대한 검사를 피할 수 있습니다.

- 특수 잠금 권한

  ONTAP는 기존 잠금과 관계없이 모든 파일에 대한 읽기, 쓰기 또는 수정 액세스를 허용합니다. FPolicy 서버가 파일에서 바이트 범위 잠금을 사용하면 파일에서 기존 잠금을 즉시 제거할 수 있습니다.

- FPolicy 검사를 생략합니다

  FPolicy 알림을 생성하지 않습니다.

FPolicy가 정책 처리를 관리하는 방법입니다

스토리지 가상 시스템(SVM)에 여러 FPolicy 정책이 할당될 수 있으며 각 정책은 서로 다른 우선순위를 갖습니다. SVM에 적절한 FPolicy 구성을 생성하려면 FPolicy에서 정책 처리를 관리하는 방법을 이해하는 것이 중요합니다.

각 파일 액세스 요청은 처음에 평가하여 이 이벤트를 모니터링하는 정책을 결정합니다. 모니터링되는 이벤트인 경우 관심 있는 정책과 함께 모니터링되는 이벤트에 대한 정보가 FPolicy로 전달되어 FPolicy가 평가됩니다. 각 정책은 할당된 우선 순위에 따라 평가됩니다.

정책을 구성할 때는 다음 권장 사항을 고려해야 합니다.

- 다른 정책보다 먼저 정책을 항상 평가하려면 우선 순위가 더 높은 정책을 구성합니다.
- 모니터링되는 이벤트에 대해 요청된 파일 액세스 작업의 성공이 다른 정책에 대해 평가된 파일 요청에 대한 사전 요구 사항이면 첫 번째 파일 작업의 성공 또는 실패를 보다 높은 우선 순위로 제어하는 정책을 지정합니다.

  예를 들어, 하나의 정책이 FPolicy 파일 아카이빙 및 복원 기능을 관리하고 두 번째 정책이 온라인 파일의 파일 액세스 작업을 관리하는 경우, 파일 복원을 관리하는 정책은 우선 순위가 더 높아야 두 번째 정책에 의해 관리되는 작업을 허용하기 전에 파일을 복원할 수 있습니다.

- 파일 액세스 작업에 적용할 수 있는 모든 정책을 평가하려면 동기 정책을 낮은 우선 순위로 지정합니다.

정책 시퀀스 번호를 수정하여 기존 정책에 대한 정책 우선 순위를 다시 정렬할 수 있습니다. 하지만 FPolicy에서 수정된 우선 순위 순서에 따라 정책을 평가하도록 하려면 수정된 시퀀스 번호를 사용하여 정책을 사용하지 않도록 설정하고 다시 활성화해야 합니다.

노드-외부 ONTAP FPolicy 서버 통신 프로세스

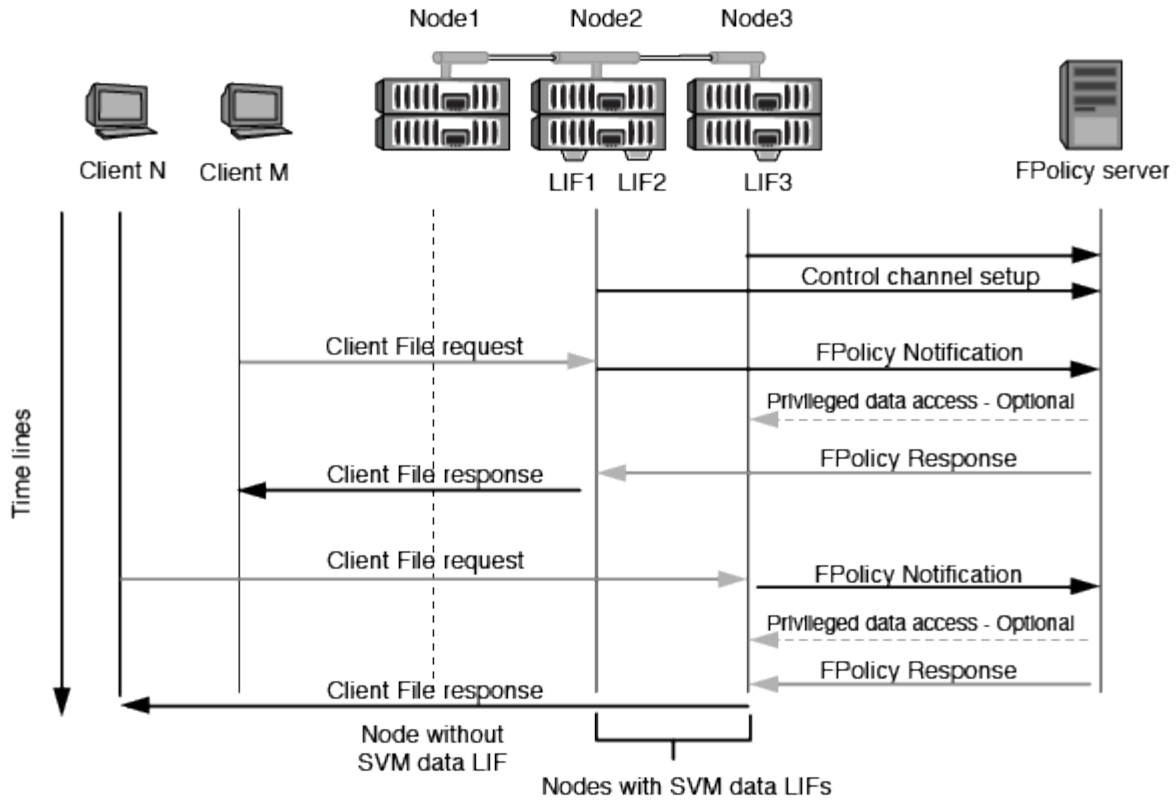
FPolicy 구성을 올바르게 계획하려면 노드-외부 FPolicy 서버 통신 프로세스가 무엇인지 이해해야 합니다.

각 스토리지 가상 머신(SVM)에 참여하는 모든 노드는 TCP/IP를 사용하여 외부 FPolicy 서버(FPolicy 서버)에 연결을 시작합니다. FPolicy 서버에 대한 연결은 노드 데이터 LIF를 사용하여 설정됩니다. 따라서 노드에 SVM을 위한 운영 데이터 LIF가 있는 경우에만 참여 노드가 연결을 설정할 수 있습니다.

참여 노드의 각 FPolicy 프로세스는 정책이 사용되도록 설정된 경우 FPolicy 서버에 연결을 설정하려고 시도합니다. 정책 구성에 지정된 FPolicy 외부 엔진의 IP 주소와 포트를 사용합니다.

이 연결을 통해 데이터 LIF를 통해 각 SVM에 참여하는 각 노드에서 FPolicy 서버로 제어 채널을 설정합니다. 또한 IPv4 및 IPv6 데이터 LIF 주소가 동일한 참여 노드에 있는 경우 FPolicy는 IPv4와 IPv6 모두에 대한 연결을 시도합니다. 따라서 SVM이 여러 노드로 확장되거나 IPv4 및 IPv6 주소가 둘 다 있는 경우 SVM에서 FPolicy 정책을 활성화한 후 FPolicy 서버에서 클러스터의 여러 제어 채널 설정 요청을 준비할 수 있어야 합니다.

예를 들어, 클러스터에 Node1, Node2, Node3와 같은 3개의 노드가 있고, SVM 데이터 LIF가 Node2와 Node3에만 분산되는 경우, 데이터 볼륨의 분산에 관계없이 제어 채널은 Node2와 Node3에서만 시작됩니다. Node2에는 SVM에 속하는 두 개의 데이터 LIF(LIF1 및 LIF2)가 있으며, 초기 접속은 LIF1입니다. LIF1에 장애가 발생하면 FPolicy는 LIF2에서 제어 채널을 설정하려고 시도합니다.



FPolicy가 **LIF** 마이그레이션 또는 페일오버 중에 외부 통신을 관리하는 방법입니다

데이터 LIF는 동일한 노드의 데이터 포트 또는 원격 노드의 데이터 포트로 마이그레이션할 수 있습니다.

데이터 LIF가 페일오버되거나 마이그레이션되면 FPolicy 서버에 새 제어 채널 연결이 만들어집니다. 그런 다음 FPolicy는 시간이 초과된 SMB 및 NFS 클라이언트 요청을 다시 시도할 수 있습니다. 그 결과 새 알림이 외부 FPolicy 서버로 전송됩니다. 이 노드는 FPolicy 서버 응답을 원래의 제한 시간이 초과된 SMB 및 NFS 요청에 대해 거부합니다.

노드 페일오버 중에 **FPolicy**가 외부 통신을 관리하는 방법

FPolicy 통신에 사용되는 데이터 포트를 호스팅하는 클러스터 노드에 장애가 발생하면 ONTAP는 FPolicy 서버와 노드 간의 연결을 끊습니다.

FPolicy 통신에 사용되는 데이터 포트를 다른 활성 노드로 마이그레이션하도록 페일오버 정책을 구성하여 FPolicy 서버로 클러스터 페일오버가 미치는 영향을 완화할 수 있습니다. 마이그레이션이 완료되면 새 데이터 포트를 사용하여 새 연결이 설정됩니다.

데이터 포트를 마이그레이션하도록 페일오버 정책이 구성되지 않은 경우 FPolicy 서버가 장애가 발생한 노드가 시작될 때까지 기다려야 합니다. 노드가 가동되면 새 세션 ID가 있는 해당 노드에서 새 연결이 시작됩니다.

FPolicy 서버에서 Keep-alive 프로토콜 메시지의 끊어진 연결을 감지합니다. FPolicy를 구성할 때 세션 ID를 제거하는 시간이 초과되었습니다. 기본 연결 유지 시간 초과는 2분입니다.

SVM 네임스페이스 전반의 **ONTAP FPolicy** 서비스에 대해 알아보세요**.**

ONTAP은 유니파이드 스토리지 가상 시스템(SVM) 네임스페이스를 제공합니다. 접합을 통해 클러스터 전체의 볼륨을 연결하여 하나의 논리적 파일 시스템을 제공합니다. FPolicy 서버는 네임스페이스 토폴로지를 인식하고 네임스페이스에서 FPolicy 서비스를 제공합니다.

네임스페이스는 SVM 내에서만 고유하며 SVM 내부에 포함되어 있습니다. 따라서 SVM 컨텍스트에서만 네임스페이스를 볼 수 있습니다. 네임스페이스에는 다음과 같은 특성이 있습니다.

- 각 SVM에는 네임스페이스 루트의 루트가 루트 볼륨으로, 네임스페이스에서 슬래시(/)로 표시되는 단일 네임스페이스가 있습니다.
- 다른 모든 볼륨에는 루트(/) 아래에 접합점이 있습니다.
- 볼륨 접합은 클라이언트에 영향을 미치지 않습니다.
- 단일 NFS 내보내기로 전체 네임스페이스에 대한 액세스를 제공할 수 있습니다. 그렇지 않으면 엑스포트 정책으로 특정 볼륨을 내보낼 수 있습니다.
- SMB 공유는 볼륨 내의 qtree 또는 네임스페이스 내의 모든 디렉토리에 생성할 수 있습니다.
- 네임스페이스 아키텍처는 유연합니다.

  일반적인 네임스페이스 아키텍처의 예는 다음과 같습니다.

  - 루트에서 단일 분기가 있는 네임스페이스
  - 루트에서 여러 개의 분기가 있는 네임스페이스입니다
  - 여러 개의 분기되지 않은 볼륨을 루트에서 벗어난 네임스페이스입니다

ONTAP FPolicy passthrough-read가 계층적 저장소 관리의 사용성을 향상시키는 방법

패스스루 읽기를 통해 FPolicy 서버(계층적 스토리지 관리(HSM) 서버로 작동)가 보조 스토리지 시스템에서 기본 스토리지 시스템으로 파일을 리콜하지 않고 오프라인 파일에 대한 읽기 액세스를 제공할 수 있습니다.

FPolicy 서버가 SMB 서버에 상주하는 파일에 HSM을 제공하도록 구성된 경우, 파일이 보조 스토리지에 오프라인으로 저장되고 스텁 파일만 운영 스토리지에 남아 있는 경우 정책 기반 파일 마이그레이션이 발생합니다. 스텁 파일이 클라이언트에 일반 파일로 나타나지만 실제로는 원본 파일의 크기가 같은 스파스 파일입니다. 스파스 파일에는 SMB 오프라인 비트 세트가 있고 보조 스토리지로 마이그레이션된 실제 파일을 가리킵니다.

일반적으로 오프라인 파일에 대한 읽기 요청이 수신되면 요청된 콘텐츠를 운영 스토리지로 다시 리콜한 다음 운영 스토리지를 통해 액세스해야 합니다. 데이터를 기본 스토리지로 다시 불러내야 할 경우 좋지 않은 영향을 몇 가지 일으킬 수 있습니다. 원치 않는 결과 중 하나는 요청에 응답하기 전에 콘텐츠를 다시 불러와야 하는 필요성과 기본 스토리지의 리콜 대상 파일에 필요한 공간 소비가 증가했기 때문에 발생하는 클라이언트 요청에 대한 지연 시간이 늘어난 것입니다.

FPolicy 패스스루 읽기를 사용하면 HSM 서버(FPolicy 서버)에서 2차 스토리지 시스템에서 1차 스토리지 시스템으로 파일을 리콜하지 않고 마이그레이션된 오프라인 파일에 대한 읽기 액세스를 제공할 수 있습니다. 파일을 운영 스토리지로 다시 호출하는 대신 읽기 요청을 보조 스토리지에서 직접 처리할 수 있습니다.

ODX(복사 오프로드)는 FPolicy 패스스루 읽기 작업에서 지원되지 않습니다.

PassThrough-read는 다음과 같은 이점을 제공하여 유용성을 향상시킵니다.

- 운영 스토리지에 요청된 데이터를 운영 스토리지로 다시 불러올 공간이 충분하지 않은 경우에도 읽기 요청을 처리할 수 있습니다.
- 스크립트 또는 백업 솔루션에서 많은 오프라인 파일에 액세스해야 하는 경우와 같이 데이터 리콜이 급증할 수 있는 경우 용량과 성능을 더욱 효과적으로 관리할 수 있습니다.
- 스냅샷의 오프라인 파일에 대한 읽기 요청을 처리할 수 있습니다.

  스냅샷은 읽기 전용이므로 스텁 파일이 스냅샷에 있는 경우 FPolicy 서버가 원본 파일을 복원할 수 없습니다. 패스스루 읽기를 사용하면 이 문제가 해결됩니다.

- 보조 스토리지의 파일에 대한 액세스를 통해 읽기 요청을 처리하고 오프라인 파일을 운영 스토리지로 리콜해야 하는 시기를 제어하는 정책을 설정할 수 있습니다.

  예를 들어, HSM 서버에서 파일을 운영 스토리지로 다시 마이그레이션하기 전에 지정된 시간 내에 오프라인 파일에 액세스할 수 있는 횟수를 지정하는 정책을 생성할 수 있습니다. 이 유형의 정책은 거의 액세스하지 않는 파일을 리콜하지 않습니다.

FPolicy 패스스루 읽기가 활성화된 경우 읽기 요청이 관리되는 방법입니다

FPolicy 패스스루 읽기를 사용하도록 설정한 경우 스토리지 가상 시스템(SVM)과 FPolicy 서버 간의 연결을 최적으로 구성할 수 있도록 읽기 요청이 관리되는 방식을 이해해야 합니다.

FPolicy 패스스루 읽기를 사용하고 SVM이 오프라인 파일에 대한 요청을 받으면 FPolicy가 표준 연결 채널을 통해 FPolicy 서버(HSM 서버)에 알림을 보냅니다.

알림을 수신한 FPolicy 서버는 알림에 전송된 파일 경로에서 데이터를 읽고, SVM과 FPolicy 서버 사이에 설정된 패스스루 읽기 전용 데이터 연결을 통해 SVM으로 요청된 데이터를 보냅니다.

데이터가 전송된 후 FPolicy 서버는 읽기 요청에 대해 허용 또는 거부로 응답합니다. 읽기 요청의 허용 또는 거부 여부에 따라 ONTAP는 요청된 정보를 보내거나 클라이언트에 오류 메시지를 보냅니다.

FPolicy 구성을 계획합니다

ONTAP FPolicy 구성을 위한 요구 사항, 고려 사항 및 모범 사례

스토리지 가상 시스템(SVM)에서 FPolicy 구성을 생성하고 구성하기 전에 FPolicy를 구성하기 위한 특정 요구사항, 고려 사항 및 모범 사례를 알고 있어야 합니다.

FPolicy 기능은 CLI(Command Line Interface) 또는 REST API를 통해 구성됩니다.

FPolicy 설정 요구 사항

SVM(스토리지 가상 머신)에서 FPolicy를 구성하고 사용하기 전에 특정 요구사항을 알고 있어야 합니다.

- 클러스터의 모든 노드는 FPolicy를 지원하는 ONTAP 버전을 실행하고 있어야 합니다.
- ONTAP 기본 FPolicy 엔진을 사용하지 않는 경우 외부 FPolicy 서버(FPolicy 서버)가 설치되어 있어야 합니다.

- FPolicy 정책은 사용되는 SVM의 데이터 LIF에서 액세스할 수 있는 서버에 FPolicy 서버를 설치해야 합니다.

> ONTAP 9.8부터 ONTAP는 `data-fpolicy-client` 서비스가 추가된 아웃바운드 FPolicy 연결에 대한 클라이언트 LIF 서비스를 제공합니다. "LIF 및 서비스 정책에 대해 자세히 알아보십시오"..

- FPolicy 서버의 IP 주소는 FPolicy 정책 외부 엔진 구성에서 1차 또는 2차 서버로 구성해야 합니다.
- FPolicy 서버가 권한 있는 데이터 채널을 통해 데이터에 액세스하는 경우 다음과 같은 추가 요구사항이 충족되어야 합니다.
  - SMB는 클러스터에서 라이센스가 있어야 합니다.

    권한 있는 데이터 액세스는 SMB 연결을 사용하여 수행됩니다.
  - 권한이 있는 데이터 채널을 통해 파일에 액세스하기 위한 사용자 자격 증명을 구성해야 합니다.
  - FPolicy 서버는 FPolicy 구성에 구성된 자격 증명에서 실행해야 합니다.
  - FPolicy 서버와 통신하는 데 사용되는 모든 데이터 LIF는 허용되는 프로토콜 중 하나로 'CIFS'를 사용하도록 구성해야 합니다.

    패스스루 읽기 연결에 사용되는 LIF가 포함됩니다.

FPolicy를 설정할 때의 모범 사례와 권장 사항입니다

SVM(스토리지 가상 머신)에서 FPolicy를 설정할 때 일반 구성 모범 사례와 권장 사항을 잘 활용하여 FPolicy 구성이 고객의 요구사항을 충족하는 강력한 모니터링 성능 및 결과를 제공하도록 하십시오.

성능, 사이징 및 구성과 관련된 특정 지침은 FPolicy 파트너 애플리케이션을 사용하십시오.

영구 저장소

ONTAP 9.14.1부터 FPolicy를 사용하면 SVM의 비동기적 정책에 대한 파일 액세스 이벤트를 캡처하는 영구 저장소를 설정할 수 있습니다. 영구 저장소는 클라이언트 I/O 처리를 FPolicy 알림 처리와 분리하여 클라이언트 지연 시간을 줄여 줍니다. 동기(필수 또는 비필수) 및 비동기 필수 구성은 지원되지 않습니다.

- 영구 저장소 기능을 사용하기 전에 파트너 응용 프로그램에서 이 구성을 지원하는지 확인하십시오.
- FPolicy가 활성화된 각 SVM에 대해 하나의 영구 저장소가 필요합니다.
  - 각 SVM에 하나의 영구 저장소만 설정할 수 있습니다. 서로 다른 파트너의 정책이 있는 경우에도 이 단일 영구 저장소를 해당 SVM의 모든 FPolicy 구성에 사용해야 합니다.
- ONTAP 9.15.1 이상:
  - 영구 저장소를 만들 때 영구 저장소, 볼륨 및 해당 볼륨 구성이 자동으로 처리됩니다.
- ONTAP 9.14.1:
  - 영구 저장소, 볼륨 및 해당 볼륨 구성은 수동으로 처리됩니다.
- FPolicy로 최대 트래픽을 모니터링할 것으로 예상되는 LIF가 포함된 노드에 영구 저장소 볼륨을 생성합니다.
  - ONTAP 9.15.1 이상: 영구 저장소 생성 중에 볼륨이 자동으로 생성되고 구성됩니다.
  - ONTAP 9.14.1: 클러스터 관리자는 FPolicy가 활성화된 각 SVM에서 영구 저장소의 볼륨을 생성하고 구성해야 합니다.

- 영구 저장소에 누적된 알림이 프로비저닝된 볼륨 크기를 초과하면 FPolicy가 적절한 EMS 메시지와 함께 수신 알림을 삭제하기 시작합니다.
  - ONTAP 9.15.1 이상: 추가 `size` 매개 변수, 입니다 `autosize-mode` 매개 변수는 사용된 공간에 대한 응답으로 볼륨을 확장하거나 축소하는 데 도움이 될 수 있습니다.
  - ONTAP 9.14.1: 입니다 `size` 최대 한도를 제공하기 위해 볼륨 생성 중에 매개 변수를 구성합니다.
- 스냅샷 정책을 로 설정합니다 `none` 를 대신 영구 저장소 볼륨에 사용합니다 `default`. 이는 스냅샷을 실수로 복구하여 현재 이벤트가 손실되지 않도록 하고 중복 이벤트 처리를 방지하기 위한 것입니다.
  - ONTAP 9.15.1 이상 `snapshot-policy` 영구 저장소 생성 중에는 매개 변수가 자동으로 없음으로 구성됩니다.
  - ONTAP 9.14.1: 입니다 `snapshot-policy` 매개 변수가 로 구성됩니다 `none` 볼륨 생성 중.
- 영구 저장소 볼륨을 외부 사용자 프로토콜 액세스(CIFS/NFS)에 액세스할 수 없도록 하여 영구 이벤트 레코드가 실수로 손상되거나 삭제되지 않도록 합니다.
  - ONTAP 9.15.1 이상: 영구 저장소를 생성하는 동안 ONTAP는 외부 사용자 프로토콜 액세스(CIFS/NFS)에서 볼륨을 자동으로 차단합니다.
  - ONTAP 9.14.1: FPolicy를 활성화한 후 ONTAP에서 볼륨을 마운트 해제하여 접합 경로를 제거합니다. 따라서 외부 사용자 프로토콜 액세스(CIFS/NFS)에 액세스할 수 없습니다.

자세한 내용은 을 참조하십시오 "FPolicy 영구 저장소" 및 "영구 저장소를 만듭니다".

영구 저장소 페일오버 및 반환

영구 저장소는 마지막 이벤트가 수신되었을 때와 마찬가지로 예상치 못한 재부팅이 발생하거나 FPolicy가 비활성화되었다가 다시 사용되도록 설정됩니다. 테이크오버 작업 후 새 이벤트는 파트너 노드에서 저장하고 처리합니다. 반환 작업 후 영구 저장소는 노드 테이크오버 발생 시 계속 처리될 수 있는 처리되지 않은 이벤트의 처리를 다시 시작합니다. 라이브 이벤트는 처리되지 않은 이벤트보다 우선 순위가 부여됩니다.

동일한 SVM 내에서 영구 저장소 볼륨이 한 노드에서 다른 노드로 이동하는 경우 아직 처리되지 않은 알림도 새 노드로 이동됩니다. 다시 실행해야 합니다. `fpolicy persistent-store create` 볼륨이 이동된 후 두 노드 중 하나에서 명령을 실행하여 보류 중인 알림이 외부 서버로 전달되도록 합니다.

자세히 알아보세요 `fpolicy persistent-store create` 에서 "ONTAP 명령 참조입니다" .

정책 구성

SVM에 대한 FPolicy 외부 엔진, 이벤트 및 범위를 구성하여 전반적인 경험과 보안을 향상할 수 있습니다.

- SVM용 FPolicy 외부 엔진 구성:
  - 추가 보안 제공에는 성능 비용이 발생합니다. SSL(Secure Sockets Layer) 통신을 활성화하면 공유 액세스에 성능 영향이 있습니다.
  - FPolicy 외부 엔진은 FPolicy 서버 알림 처리의 복원력과 고가용성을 제공하도록 FPolicy 서버를 두 개 이상 구성해야 합니다.
- SVM에 대한 FPolicy 이벤트 구성:

  파일 작업 모니터링은 전반적인 환경에 영향을 미칩니다. 예를 들어, 스토리지 측에서 원치 않는 파일 작업을 필터링하면 작업 환경이 개선됩니다. NetApp에서는 다음 구성을 설정할 것을 권장합니다.
  - 최소 파일 작업 유형을 모니터링하고 사용 사례를 위반하지 않고 최대 필터 수를 설정합니다.

- GetAttr , 읽기, 쓰기, 열기 및 닫기 작업에 필터를 사용합니다. SMB 및 NFS 홈 디렉토리 환경에서는 이러한 작업의 비율이 높습니다.

- SVM에 대한 FPolicy 범위 구성:

  전체 SVM에서 정책 범위를 설정하는 대신 공유, 볼륨, 엑스포트 등의 관련 스토리지 오브젝트로 정책 범위를 제한합니다. NetApp에서는 디렉터리 확장명을 확인하는 것이 좋습니다. 를 누릅니다 `is-file-extension-check-on-directories-enabled` 매개 변수가 로 설정되었습니다 `true`디렉터리 개체는 일반 파일과 동일한 확장 검사를 받습니다.

네트워크 구성

FPolicy 서버와 컨트롤러 간 네트워크 연결 지연 시간이 짧아야 합니다. NetApp은 개인 네트워크를 사용하여 FPolicy 트래픽을 클라이언트 트래픽과 분리하는 것을 권장합니다.

또한 대기 시간과 고대역폭 연결을 최소화하기 위해 외부 FPolicy 서버(FPolicy 서버)를 고대역폭 연결을 통해 클러스터 근처에 배치해야 합니다.

> FPolicy 트래픽용 LIF가 클라이언트 트래픽을 위해 LIF와 다른 포트에서 구성된 시나리오의 경우 포트 장애로 인해 FPolicy LIF가 다른 노드로 페일오버될 수 있습니다. 따라서 FPolicy 서버에 노드에 연결할 수 없게 되어 노드의 파일 작업에 대한 FPolicy 알림이 실패합니다. 이 문제를 방지하려면 FPolicy 서버가 노드의 하나 이상의 LIF를 통해 도달하여 해당 노드에서 수행된 파일 작업에 대한 FPolicy 요청을 처리할 수 있는지 확인하십시오.

하드웨어 구성

FPolicy 서버를 물리적 서버 또는 가상 서버에 사용할 수 있습니다. FPolicy 서버가 가상 환경에 있는 경우 전용 리소스(CPU, 네트워크 및 메모리)를 가상 서버에 할당해야 합니다.

클러스터 노드-FPolicy 서버 비율은 FPolicy 서버가 과부하되지 않도록 최적화되어야 하며, 이는 SVM이 클라이언트 요청에 응답할 때 지연 시간을 유발할 수 있습니다. 최적의 비율은 FPolicy 서버를 사용하는 파트너 애플리케이션에 따라 다릅니다. NetApp은 파트너와 협력하여 적절한 가치를 결정할 것을 권장합니다.

다중 정책 구성

시퀀스 번호와 관계없이 기본 차단에 대한 FPolicy 정책이 가장 높은 우선순위를 가지며, 결정 변경 정책은 다른 정책보다 더 높은 우선순위를 갖습니다. 정책 우선 순위는 사용 사례에 따라 다릅니다. NetApp은 파트너와 협력하여 적절한 우선 순위를 결정할 것을 권장합니다.

크기 고려 사항

FPolicy는 SMB 및 NFS 작업의 인라인 모니터링을 수행하고, 외부 서버로 알림을 전송하고, 외부 엔진 통신 모드(동기식 또는 비동기식)에 따라 응답을 기다립니다. 이 프로세스는 SMB 및 NFS 액세스 및 CPU 리소스의 성능에 영향을 줍니다.

문제를 완화하기 위해 NetApp은 파트너와 협력하여 FPolicy를 사용하기 전에 환경을 평가하고 크기를 조정하는 것이 좋습니다. 사용자 수, 작업량 특성(사용자 및 데이터 크기별 작업, 네트워크 지연 시간, 장애 또는 서버 속도 등) 등 여러 요소의 성능이 영향을 받습니다.

성능을 모니터링합니다

FPolicy는 알림 기반 시스템입니다. 알림은 처리를 위해 외부 서버로 전송되고 ONTAP에 대한 응답을 다시 생성합니다.

이 라운드 트립 프로세스는 클라이언트 액세스의 지연 시간을 늘립니다.

FPolicy 서버와 ONTAP에서 성능 카운터를 모니터링하면 솔루션에서 병목 현상을 식별하고 최적의 솔루션을 위해 필요에 따라 매개 변수를 조정할 수 있습니다. 예를 들어 FPolicy 지연 시간이 증가하면 SMB 및 NFS 액세스 지연 시간에 계단식 효과가 나타납니다. 따라서 워크로드(SMB 및 NFS)와 FPolicy 지연 시간을 모두 모니터링해야 합니다. 또한 ONTAP의 서비스 품질 정책을 사용하여 FPolicy에 사용되는 각 볼륨 또는 SVM에 대한 워크로드를 설정할 수 있습니다.

NetApp에서는 을 실행할 것을 권장합니다 `statistics show -object workload` 명령을 사용하여 워크로드 통계를 표시합니다. 또한 다음 매개 변수를 모니터링해야 합니다.

- 평균, 읽기 및 쓰기 지연 시간
- 총 작업 수입니다
- 카운터 읽기 및 쓰기

다음 FPolicy 카운터를 사용하여 FPolicy 하위 시스템의 성능을 모니터링할 수 있습니다.

FPolicy와 관련된 통계를 수집하려면 진단 모드에 있어야 합니다.

단계

1. FPolicy 카운터 수집:
   a. `statistics start -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics start -object fpolicy_policy -instance <instance_name> -sample-id <ID>`
2. FPolicy 카운터 표시:
   a. `statistics show -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics show -object fpolicy_server -instance <instance_name> -sample-id <ID>`

   를 클릭합니다 `fpolicy` 및 `fpolicy_server` 카운터는 다음 표에 설명된 여러 성능 매개 변수에 대한 정보를 제공합니다.

카운터	설명
• FPolicy 카운터 *	중단_요청
SVM에서 처리가 중단된 화면 요청 수입니다	event_count입니다
알림을 발생시키는 이벤트 목록입니다	max_request_latency를 입력합니다
최대 화면 요청 대기 시간	미결_요청
처리 중인 총 화면 요청 수입니다	처리된_요청
SVM에서 FPolicy 처리를 통해 수행된 총 화면 요청 수입니다	request_latency_hist 를 참조하십시오

카운터	설명
화면 요청에 대한 지연 시간의 히스토그램입니다	Requests_Dispatched_rate(요청_발송
초당 디스패치된 화면 요청 수입니다	request_Received_rate를 입력합니다
초당 수신된 화면 요청 수입니다	• FPolicy_server 카운터 *
max_request_latency를 입력합니다	화면 요청에 대한 최대 대기 시간입니다
미결_요청	응답을 기다리는 총 화면 요청 수입니다
request_latency를 입력합니다	화면 요청에 대한 평균 대기 시간입니다
request_latency_hist 를 참조하십시오	화면 요청에 대한 지연 시간의 히스토그램입니다
request_sent_rate입니다	초당 FPolicy 서버로 전송된 화면 요청 수입니다
응답_수신_속도	FPolicy 서버에서 초당 수신한 화면 응답 수입니다

및 `statistics show` 에 대한 자세한 `statistics start` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

FPolicy 워크플로우 및 다른 기술에 대한 의존성을 관리합니다

구성을 변경하기 전에 FPolicy 정책을 사용하지 않는 것이 좋습니다. NetApp 예를 들어 활성화된 정책에 대해 구성된 외부 엔진에서 IP 주소를 추가하거나 수정하려면 먼저 정책을 사용하지 않도록 설정합니다.

NetApp FlexCache 볼륨을 모니터링하도록 FPolicy를 구성하는 경우 NetApp는 FPolicy를 구성하여 읽기 및 GetAttr 파일 작업을 모니터링하지 않는 것이 좋습니다. ONTAP에서 이러한 작업을 모니터링하려면 inode-to-path(I2P) 데이터를 검색할 필요가 있습니다. I2P 데이터는 FlexCache 볼륨에서 검색할 수 없으므로 원본 볼륨에서 가져와야 합니다. 따라서 이러한 작업을 모니터링하면 FlexCache가 제공할 수 있는 성능 이점이 없어집니다.

FPolicy와 오프박스 바이러스 백신 솔루션을 모두 구축하면 바이러스 백신 솔루션에서 먼저 알림을 받습니다. FPolicy 처리는 바이러스 백신 검사가 완료된 후에만 시작됩니다. 바이러스 백신 검사 속도가 느리면 전체 성능이 저하될 수 있으므로 바이러스 백신 솔루션의 크기를 올바르게 조정하는 것이 중요합니다.

통과 연결 - 읽기 업그레이드 및 되돌리기 고려 사항

패스스루 읽기를 지원하는 ONTAP 릴리즈로 업그레이드하기 전에 또는 패스스루 읽기를 지원하지 않는 릴리즈로 되돌리기 전에 반드시 알아야 하는 특정 업그레이드 및 되돌리기 고려 사항이 있습니다.

업그레이드 중

모든 노드가 FPolicy 패스스루 읽기를 지원하는 ONTAP 버전으로 업그레이드된 후 클러스터는 패스스루 읽기 기능을 사용할 수 있습니다. 하지만 기존 FPolicy 구성에서는 패스스루 읽기가 기본적으로 비활성화됩니다. 기존 FPolicy 구성에서 패스스루 읽기를 사용하려면 FPolicy 정책을 비활성화하고 구성을 수정한 다음 구성을 다시 활성화해야 합니다.

되돌리기

FPolicy 패스스루 읽기를 지원하지 않는 ONTAP 버전으로 되돌리기 전에 다음 조건을 충족해야 합니다.

- 패스스루 읽기를 사용하여 모든 정책을 비활성화한 다음 패스스루 읽기를 사용하지 않도록 영향을 받는 구성을 수정합니다.
- 클러스터에서 모든 FPolicy 정책을 사용하지 않도록 설정하여 클러스터에서 FPolicy 기능을 사용하지 않도록 설정합니다.

영구 저장소를 지원하지 않는 ONTAP 버전으로 되돌리기 전에 FPolicy 정책에 영구 저장소가 구성되어 있지 않은지 확인하십시오. 영구 저장소가 구성되어 있으면 되돌리기가 실패합니다.

관련 정보

- "통계에 따르면"
- "통계 시작"

ONTAP FPolicy 구성 설정

FPolicy가 파일 액세스를 모니터링하기 전에 FPolicy 서비스가 필요한 스토리지 가상 시스템(SVM)에서 FPolicy 구성을 생성하고 사용하도록 설정해야 합니다.

SVM에서 FPolicy 구성을 설정하고 활성화하는 단계는 다음과 같습니다.

1. FPolicy 외부 엔진을 생성합니다.

   FPolicy 외부 엔진은 특정 FPolicy 구성과 관련된 외부 FPolicy 서버(FPolicy 서버)를 식별합니다. 내부 ""기본"" FPolicy 엔진을 사용하여 기본 파일 차단 구성을 생성하는 경우 FPolicy 외부 엔진을 생성할 필요가 없습니다.

   ONTAP 9.15.1부터 를 사용할 수 있습니다 `protobuf` 엔진 형식 를 로 설정한 경우 `protobuf`, 알림 메시지는 Google Protupf를 사용하여 바이너리 형태로 인코딩됩니다. 엔진 포맷을 로 설정하기 전에 `protobuf`, FPolicy 서버도 지원해야 합니다 `protobuf` 역직렬화. 자세한 내용은 을 참조하십시오 "FPolicy 외부 엔진 구성을 계획하십시오"

2. FPolicy 이벤트를 생성합니다.

   FPolicy 이벤트는 FPolicy 정책이 모니터링해야 하는 사항을 설명합니다. 이벤트는 모니터링할 프로토콜과 파일 작업으로 구성되며 필터 목록을 포함할 수 있습니다. 이벤트는 FPolicy 외부 엔진이 알림을 보내야 하는 모니터링되는 이벤트 목록의 범위를 좁히기 위해 필터를 사용합니다. 이벤트는 정책이 볼륨 작업을 모니터링하는지 여부도 지정합니다.

3. FPolicy 영구 저장소를 생성합니다(선택 사항).

   ONTAP 9.14.1부터 FPolicy를 설정할 수 있습니다 "영구 저장소" SVM에서 비동기적 정책에 대한 파일 액세스 이벤트를 캡처합니다. 동기(필수 또는 비필수) 및 비동기 필수 구성은 지원되지 않습니다.

   영구 저장소는 클라이언트 I/O 처리를 FPolicy 알림 처리와 분리하여 클라이언트 지연 시간을 줄여 줍니다.

   ONTAP 9.15.1부터 FPolicy 영구 저장소 구성이 단순화됩니다. 를 클릭합니다 `persistent-store-create` 명령은 SVM에 대한 볼륨 생성을 자동화하고 영구 저장소에 대한 볼륨을 구성합니다.

4. FPolicy 정책을 생성합니다.

FPolicy 정책은 적합한 범위와 함께 모니터링해야 하는 이벤트 세트를 지정하고 모니터링되는 이벤트 중 어떤 알림을 지정된 FPolicy 서버(또는 FPolicy 서버가 구성되지 않은 경우 기본 엔진)로 보내야 하는 것을 연결해야 합니다. 또한 FPolicy 서버에서 알림을 받는 데이터에 대한 권한이 부여되는지 여부를 정의합니다. 서버에서 데이터에 액세스해야 하는 경우 FPolicy 서버에 권한이 있는 액세스가 필요합니다. 액세스 권한이 필요한 일반적인 사용 사례로는 파일 차단, 할당량 관리 및 계층적 스토리지 관리가 있습니다. 이 정책은 이 정책 구성이 FPolicy 서버를 사용하는지 또는 내부 ""기본"" FPolicy 서버를 사용하는지 여부를 지정하는 것입니다.

정책은 스크리닝이 필수인지 여부를 지정합니다. 스크리닝이 필수이고 모든 FPolicy 서버가 다운되었거나 정의된 제한 시간 내에 FPolicy 서버로부터 응답이 없는 경우, 파일 액세스가 거부됩니다.

정책의 경계는 SVM입니다. 정책은 여러 SVM에 적용할 수 없습니다. 하지만 특정 SVM에는 범위, 이벤트, 외부 서버 구성이 같거나 다른 여러 FPolicy 정책이 있을 수 있습니다.

5. 정책 범위를 구성합니다.

   FPolicy 범위는 정책에서 모니터링에서 활동하거나 제외하는 볼륨, 공유 또는 엑스포트 정책을 결정합니다. 또한 FPolicy 모니터링에서 포함하거나 제외할 파일 확장명을 결정합니다.

   ⓘ 제외 목록이 포함 목록보다 우선합니다.

6. FPolicy 정책을 사용합니다.

   정책이 활성화되면 제어 채널 및 옵션으로 권한이 있는 데이터 채널이 연결됩니다. SVM이 참여하는 노드의 FPolicy 프로세스에서 모니터링 파일 및 폴더 액세스를 시작하고, 구성된 조건과 일치하는 이벤트의 경우 FPolicy 서버에 알림을 보내거나, FPolicy 서버가 구성되지 않은 경우 기본 엔진에 알림을 보냅니다.

ⓘ 정책에서 네이티브 파일 차단을 사용하는 경우 외부 엔진이 구성되어 있지 않거나 정책과 연결되지 않습니다.

FPolicy 외부 엔진 구성을 계획하십시오

ONTAP FPolicy 외부 엔진 구성 계획

FPolicy 외부 엔진을 구성하기 전에 외부 엔진을 생성하는 것이 무엇을 의미하고 사용 가능한 구성 매개 변수를 이해해야 합니다. 이 정보는 각 매개변수에 대해 설정할 값을 결정하는 데 도움이 됩니다.

FPolicy 외부 엔진을 생성할 때 정의되는 정보입니다

외부 엔진 구성에서는 FPolicy가 외부 FPolicy 서버에 대한 연결을 만들고 관리하는 데 필요한 정보를 정의합니다. 여기에는 다음과 같은 정보가 포함됩니다.

- SVM 이름
- 엔진 이름입니다
- 기본 및 보조 FPolicy 서버의 IP 주소와 FPolicy 서버에 연결할 때 사용할 TCP 포트 번호입니다
- 엔진 유형이 비동기식인지 동기식인지 여부
- 엔진 포맷인지 여부 `xml` 또는 `protobuf`

ONTAP 9.15.1부터 를 사용할 수 있습니다 `protobuf` 엔진 형식 를 로 설정한 경우 `protobuf`, 알림 메시지는 Google Protupf를 사용하여 바이너리 형태로 인코딩됩니다. 엔진 포맷을 로 설정하기 전에 `protobuf`, FPolicy 서버도 지원해야 합니다 `protobuf` 역직렬화.

ONTAP 9.15.1부터 프로토타입이 지원되므로 이전 릴리즈의 ONTAP로 되돌리기 전에 외부 엔진 형식을 고려해야 합니다. ONTAP 9.15.1 이전 릴리즈로 되돌리는 경우 FPolicy 파트너와 함께 다음 중 하나를 수행합니다.

- 에서 각 엔진 형식을 변경합니다 `protobuf` 를 선택합니다 `xml`
- 엔진 형식이 인 엔진을 삭제하십시오 `protobuf`

- 노드와 FPolicy 서버 간의 연결을 인증하는 방법

  상호 SSL 인증을 구성하도록 선택한 경우 SSL 인증서 정보를 제공하는 매개 변수도 구성해야 합니다.

- 다양한 고급 권한 설정을 사용하여 연결을 관리하는 방법

  여기에는 시간 초과 값, 재시도 값, 연결 유지 값, 최대 요청 값, 전송 및 수신 버퍼 크기 값, 세션 시간 초과 값 등을 정의하는 매개 변수가 포함됩니다.

'vserver FPolicy policy external-engine create' 명령은 FPolicy 외부 엔진을 생성하는 데 사용됩니다.

기본 외부 엔진 매개 변수는 무엇입니까

다음 기본 FPolicy 구성 매개 변수 표를 사용하여 구성을 계획할 수 있습니다.

정보 유형입니다	옵션을 선택합니다
SVM _ 이 외부 엔진과 연결할 SVM 이름을 지정합니다. 각 FPolicy 구성은 단일 SVM 내에서 정의됩니다. FPolicy 정책 구성을 생성하기 위해 함께 조합되는 외부 엔진, 정책 이벤트, 정책 범위 및 정책은 모두 동일한 SVM과 연결되어야 합니다.	'-vserver"vserver_name'

_ 엔진 이름 _ 외부 엔진 구성에 할당할 이름을 지정합니다. 나중에 FPolicy 정책을 생성할 때 외부 엔진 이름을 지정해야 합니다. 이렇게 하면 외부 엔진이 정책에 연결됩니다. 이름은 최대 256자까지 입력할 수 있습니다. MetroCluster 또는 SVM 재해 복구 구성에서 외부 엔진 이름을 구성하는 경우 최대 200자의 이름을 입력해야 합니다. 이름에는 다음 ASCII 범위 문자의 조합을 사용할 수 있습니다. • "A" ~ "z" • A부터 Z까지 • 0에서 9까지 • ""_","-",".""	엔진-이름 엔진_이름
_1차 FPolicy 서버 _ 노드가 특정 FPolicy 정책에 대한 알림을 보내는 기본 FPolicy 서버를 지정합니다. 값은 쉼표로 구분된 IP 주소 목록으로 지정됩니다. 둘 이상의 기본 서버 IP 주소가 지정된 경우 SVM이 참여하는 모든 노드에서 정책이 활성화된 시점에 지정된 모든 기본 FPolicy 서버에 대한 제어 연결을 생성합니다. 여러 기본 FPolicy 서버를 구성하는 경우 라운드 로빈 방식으로 FPolicy 서버에 알림이 전송됩니다. 외부 엔진이 MetroCluster 또는 SVM 재해 복구 구성에 사용되는 경우 소스 사이트에 있는 FPolicy 서버의 IP 주소를 1차 서버로 지정해야 합니다. 대상 사이트에 있는 FPolicy 서버의 IP 주소를 2차 서버로 지정해야 합니다.	'-primary-servers"ip_address',…
_ 포트 번호 _ FPolicy 서비스의 포트 번호를 지정합니다.	'-port' 정수
_보조 FPolicy 서버 _ 지정된 FPolicy 정책에 대해 파일 액세스 이벤트를 보낼 보조 FPolicy 서버를 지정합니다. 값은 쉼표로 구분된 IP 주소 목록으로 지정됩니다. 보조 서버는 운영 서버에 연결할 수 없는 경우에만 사용됩니다. 정책이 활성화되면 보조 서버에 대한 연결이 설정되지만, 운영 서버에 연결할 수 있는 서버가 없는 경우에만 보조 서버로 알림이 전송됩니다. 여러 2차 서버를 구성하는 경우 통지는 라운드 로빈 방식으로 FPolicy 서버로 전송됩니다.	'-secondary-servers"ip_address',…

_외부 엔진 유형 _ 외부 엔진이 동기식 또는 비동기식 모드로 작동할지 여부를 지정합니다. 기본적으로 FPolicy는 동기식 모드에서 작동합니다. '동기식'으로 설정하면 파일 요청 처리가 FPolicy 서버에 알림을 전송하고 FPolicy 서버로부터 응답을 받을 때까지 계속되지 않습니다. 이 시점에서 FPolicy 서버의 응답이 요청된 작업을 허용하는지 여부에 따라 요청 흐름이 계속 진행되거나 처리 결과가 거부됩니다. '비동기'로 설정하면 파일 요청 처리가 FPolicy 서버에 알림을 보낸 다음 계속됩니다.	'-extern-engine-type "external_engine_type' 이 파라미터의 값은 다음 중 하나일 수 있습니다. • '동기식' • 비동기식
_외부 엔진 형식 _ 외부 엔진 형식이 XML인지 protubuf인지 지정합니다. ONTAP 9.15.1부터 protubuf 엔진 포맷을 사용할 수 있습니다. protobuf로 설정하면 Google Protobuf를 사용하여 알림 메시지가 바이너리 형태로 인코딩됩니다. 엔진 형식을 protobuf로 설정하기 전에 FPolicy 서버가 prototebuf deserialization도 지원하는지 확인하십시오.	`- extern-engine-format {protobuf 또는 xml}`
_FPolicy 서버와 통신하기 위한 _SSL 옵션 _ FPolicy 서버와의 통신에 사용되는 SSL 옵션을 지정합니다. 필수 매개 변수입니다. 다음 정보를 기반으로 옵션 중 하나를 선택할 수 있습니다. • no-auth로 설정하면 인증이 발생하지 않습니다. 통신 링크는 TCP를 통해 설정됩니다. • 'server-auth'로 설정하면 SVM은 SSL 서버 인증을 사용하여 FPolicy 서버를 인증합니다. • '이중 인증'으로 설정하면 SVM과 FPolicy 서버 간에 상호 인증이 수행됩니다. SVM은 FPolicy 서버를 인증하고 FPolicy 서버는 SVM을 인증합니다. 상호 SSL 인증을 구성하려면 '-certificate-common-name', '-certificate-serial', '-certificate-ca' 매개 변수도 구성해야 합니다.	'-ssl-option'{'no-auth'
'server-auth'	'mutual-auth'}
_인증서 FQDN 또는 사용자 정의 일반 이름 _ SVM과 FPolicy 서버 간의 SSL 인증이 구성된 경우 사용되는 인증서 이름을 지정합니다. 인증서 이름을 FQDN 또는 사용자 지정 일반 이름으로 지정할 수 있습니다. '-ssl-option' 파라미터에 대해 'mutual-auth'를 지정하면 '-certificate-common-name' 파라미터에 대한 값을 지정해야 합니다.	'-certificate-common-name' text'입니다

_인증서 일련 번호 _ SVM과 FPolicy 서버 간의 SSL 인증이 구성된 경우 인증에 사용되는 인증서의 일련 번호를 지정합니다. '-ssl-option' 파라미터에 대해 'mutual-auth’를 지정하면 '-certificate-serial' 파라미터에 대한 값을 지정해야 합니다.	'-certificate-serial' text’입니다
_인증 기관 _ SVM과 FPolicy 서버 간의 SSL 인증이 구성된 경우 인증에 사용되는 인증서의 CA 이름을 지정합니다. '-ssl-option' 파라미터에 대해 'mutual-auth’를 지정하면 '-certificate-ca' 파라미터에 대한 값을 지정해야 합니다.	``인증서-카’’ 텍스트

고급 외부 엔진 옵션은 무엇입니까

고급 매개 변수를 사용하여 구성을 사용자 지정할지 여부를 계획할 때 다음 고급 FPolicy 구성 매개 변수 테이블을 사용할 수 있습니다. 다음 매개 변수를 사용하여 클러스터 노드와 FPolicy 서버 간의 통신 동작을 수정합니다.

정보 유형입니다	옵션을 선택합니다
요청 취소에 대한 시간 초과 _ FPolicy 서버에서 응답을 대기하는 시간 간격(시, 분, 초)을 지정합니다. 시간 초과 간격이 경과하면 노드가 FPolicy 서버로 취소 요청을 보냅니다. 그런 다음 노드가 대체 FPolicy 서버로 알림을 보냅니다. 이 시간 초과는 응답하지 않는 FPolicy 서버를 처리하는 데 도움이 되며 SMB/NFS 클라이언트 응답을 개선할 수 있습니다. 또한, 알림 요청이 다운/불량 FPolicy 서버에서 대체 FPolicy 서버로 이동되었기 때문에 시간 초과 후 요청을 취소하면 시스템 리소스를 해제하는 데 도움이 됩니다. 이 값의 범위는 0에서 100까지입니다. 값이 '0’으로 설정되어 있으면 이 옵션이 비활성화되고 요청 취소 메시지가 FPolicy 서버로 전송되지 않습니다. 기본값은 20입니다.	'-reqs-cancel-timeout"integer'[h
m	s]
_요청 중단을 위한 시간 초과 _ 요청 중단 시 시간 제한(시), 분(분) 또는 초(초)을 지정합니다. 이 값의 범위는 0에서 200까지입니다.	``reqs-abort-timeout""integer'[h
m	s]

_ 상태 요청 전송 간격 _ 상태 요청을 FPolicy 서버로 전송한 후 시간('h'), 분(') 또는 초(") 단위로 간격을 지정합니다. 이 값의 범위는 0에서 50까지입니다. 이 값이 '0'으로 설정되어 있으면 옵션이 비활성화되고 상태 요청 메시지가 FPolicy 서버로 전송되지 않습니다. 기본값은 10입니다.	'-status-req-interval"integer'[h
m	s]
_FPolicy 서버의 최대 대기 요청 수 _ FPolicy 서버에서 대기할 수 있는 최대 대기 요청 수를 지정합니다. 이 값의 범위는 입니다 `1` 부터 까지 `10000`. 기본값은 입니다 `500`.	'-max-server-reqs' 정수
_응답하지 않는 FPolicy 서버 연결을 끊는 데 시간이 초과되었습니다 FPolicy 서버와의 연결이 종료된 후 시간 간격(시, 분, 초)을 지정합니다. FPolicy 서버의 대기열에 허용되는 최대 요청이 포함되어 있고 제한 시간 내에 응답이 수신되지 않는 경우에만 제한 시간 이후에 연결이 종료됩니다. 허용되는 최대 요청 수는 '50'(기본값) 또는 'max-server-reqs-' 매개 변수에 지정된 숫자입니다. 이 값의 범위는 1에서 100까지입니다. 기본값은 60입니다.	'-server-progress-timeout"integer'[h
m	s]
_FPolicy server_에 연결 유지 메시지를 보내는 간격 FPolicy 서버에 연결 유지 메시지가 전송되는 시간 간격(시), 분(분) 또는 초(초)을 지정합니다. 연결 유지 메시지는 반개방 연결을 감지합니다. 이 값의 범위는 10에서 600까지입니다. 이 값이 '0'으로 설정되어 있으면 이 옵션이 비활성화되고 Keep-alive 메시지가 FPolicy 서버로 전송되지 않습니다. 기본값은 120입니다.	'-keep-alive-interval -"integer'[h
m	s]
_최대 재연결 시도 횟수 _ 연결이 끊어진 후 SVM이 FPolicy 서버에 다시 연결하려고 시도하는 최대 횟수를 지정합니다. 이 값의 범위는 0에서 20까지입니다. 기본값은 5입니다.	'-max-connection-retries' 정수

수신 버퍼 크기 _ FPolicy 서버에 대해 연결된 소켓의 수신 버퍼 크기를 지정합니다. 기본값은 256KB(킬로바이트)로 설정됩니다. 이 값을 0으로 설정하면 수신 버퍼의 크기가 시스템에서 정의한 값으로 설정됩니다. 예를 들어, 소켓의 기본 수신 버퍼 크기가 65536바이트인 경우 조정 가능한 값을 0으로 설정하면 소켓 버퍼 크기는 65536바이트로 설정됩니다. 기본값이 아닌 값을 사용하여 수신 버퍼의 크기(바이트)를 설정할 수 있습니다.	'-recv-buffer-size' 정수
_ 버퍼 크기 전송 _ FPolicy 서버에 대해 연결된 소켓의 전송 버퍼 크기를 지정합니다. 기본값은 256KB(킬로바이트)로 설정됩니다. 이 값을 0으로 설정하면 전송 버퍼의 크기가 시스템에서 정의한 값으로 설정됩니다. 예를 들어, 조정 가능한 값을 0으로 설정하여 소켓의 기본 전송 버퍼 크기가 65536바이트로 설정된 경우 소켓 버퍼 크기는 65536바이트로 설정됩니다. 기본값이 아닌 값을 사용하여 전송 버퍼의 크기(바이트)를 설정할 수 있습니다.	send-buffer-size 정수
_재연결 중 세션 ID를 제거하는 데 시간이 초과되었습니다 재연결 시도 중에 새 세션 ID가 FPolicy 서버로 전송되는 시간(시), 분(분) 또는 초(초) 단위로 지정합니다. 스토리지 컨트롤러와 FPolicy 서버 간의 연결이 종료되고 '-session-timeout' 간격 내에 다시 연결되면 이전 세션 ID가 FPolicy 서버로 전송되어 이전 알림에 대한 응답을 보낼 수 있습니다. 기본값은 10초로 설정됩니다.	'- session-timeout['integer' h]['integer' m.]['integer''seger']

SSL 인증 연결을 사용하도록 **ONTAP FPolicy** 외부 엔진을 구성하는 방법에 대한 추가 정보

FPolicy 서버에 연결할 때 SSL을 사용하도록 FPolicy 외부 엔진을 구성하려면 몇 가지 추가 정보를 알고 있어야 합니다.

SSL 서버 인증

SSL 서버 인증에 FPolicy 외부 엔진을 구성하도록 선택한 경우 외부 엔진을 생성하기 전에 FPolicy 서버 인증서에 서명한 CA(인증 기관)의 공개 인증서를 설치해야 합니다.

상호 인증

SVM(스토리지 가상 머신) 데이터 LIF를 외부 FPolicy 서버에 연결할 때 SSL 상호 인증을 사용하도록 FPolicy 외부 엔진을 구성한 경우, 외부 엔진을 생성합니다. FPolicy 서버 인증서에 서명한 CA의 공용 인증서를 SVM 인증을 위한 공용 인증서 및 키 파일과 함께 설치해야 합니다. FPolicy 정책이 설치된 인증서를 사용하는 동안에는 이 인증서를 삭제하지 마십시오.

FPolicy가 외부 FPolicy 서버에 연결할 때 상호 인증에 인증서를 사용하는 동안 인증서를 삭제하면 해당 인증서를 사용하는 비활성화된 FPolicy 정책을 다시 활성화할 수 없습니다. 같은 설정의 새 인증서가 SVM에 생성되고 설치된 경우에도 이 상황에서는 FPolicy 정책을 다시 활성화할 수 없습니다.

인증서가 삭제된 경우 새 인증서를 설치하고, 새 인증서를 사용하는 FPolicy 외부 엔진을 새로 생성한 다음, FPolicy 정책을 수정하여 다시 사용할 FPolicy 정책에 새 외부 엔진을 연결해야 합니다.

SSL용 인증서를 설치합니다

FPolicy 서버 인증서에 서명하는 데 사용되는 CA의 공개 인증서는 을 사용하여 설치됩니다 `security certificate install` 명령과 함께 `-type` 매개 변수를 로 설정합니다 `client-ca`. SVM 인증에 필요한 개인 키와 공개 인증서는 을 사용하여 설치합니다 `security certificate install` 명령과 함께 `-type` 매개 변수를 로 설정합니다 `server`.

관련 정보

- "보안 인증서 설치"

ONTAP FPolicy 인증서는 **ID** 보존 구성이 아닌 **SVM** 재해 복구 관계에서 복제되지 않습니다**.**

FPolicy 서버에 연결할 때 SSL 인증에 사용되는 보안 인증서는 ID가 아닌 구성을 사용하여 SVM 재해 복구 대상에 복제하지 않습니다. SVM의 FPolicy 외부 엔진 구성이 복제되지만 보안 인증서는 복제되지 않습니다. 대상에 보안 인증서를 수동으로 설치해야 합니다.

SVM 재해 복구 관계를 설정할 때 'napMirror create' 명령의 '-identity-preserve' 옵션에 선택한 값에 따라 타겟 SVM에 복제된 구성 세부 정보가 결정됩니다.

'-identity-preserve' 옵션을 'true'(ID-preserve)로 설정하면 보안 인증서 정보를 비롯한 모든 FPolicy 구성 세부 정보가 복제됩니다. 이 옵션을 "false"(non-ID-preserve)로 설정한 경우에만 대상에 보안 인증서를 설치해야 합니다.

관련 정보

- "SnapMirror 생성"

MetroCluster 및 **SVM** 재해 복구 구성을 사용하는 클러스터 범위 **ONTAP FPolicy** 외부 엔진에 대한 제한 사항

클러스터 스토리지 가상 시스템(SVM)을 외부 엔진에 할당하여 클러스터 범위 FPolicy 외부 엔진을 생성할 수 있습니다. 하지만 MetroCluster 또는 SVM 재해 복구 구성에서 클러스터 범위 외부 엔진을 만들 때는 SVM이 FPolicy 서버와의 외부 통신에 사용하는 인증 방법을 선택할 때 특정 제한이 있습니다.

외부 FPolicy 서버를 생성할 때 인증 없음, SSL 서버 인증 및 SSL 상호 인증이라는 세 가지 인증 옵션을 선택할 수 있습니다. 외부 FPolicy 서버가 데이터 SVM에 할당되는 인증 옵션을 선택할 때는 제한이 없지만 클러스터 범위 FPolicy 외부 엔진을 생성할 때는 제한이 있습니다.

구성	허용됩니까?
인증 없이 MetroCluster 또는 SVM 재해 복구 및 클러스터 범위 FPolicy 외부 엔진(SSL이 구성되지 않음)	예

MetroCluster 또는 SVM 재해 복구, SSL 서버 또는 SSL 상호 인증을 사용하는 클러스터 범위 FPolicy 외부 엔진	아니요

- SSL 인증을 사용하는 클러스터 범위 FPolicy 외부 엔진이 있고 MetroCluster 또는 SVM 재해 복구 구성을 생성하려는 경우, MetroCluster 또는 SVM 재해 복구 구성을 생성하기 전에 이 외부 엔진을 수정하거나 외부 엔진을 제거하지 않아야 합니다.
- MetroCluster 또는 SVM 재해 복구 구성이 이미 있는 경우 ONTAP는 클러스터 범위 FPolicy 외부 엔진을 SSL 인증으로 생성하지 못합니다.

ONTAP FPolicy 외부 엔진 구성 워크시트 완료

이 워크시트를 사용하여 FPolicy 외부 엔진 구성 프로세스 중에 필요한 값을 기록할 수 있습니다. 매개 변수 값이 필요한 경우 외부 엔진을 구성하기 전에 해당 매개 변수에 사용할 값을 결정해야 합니다.

기본 외부 엔진 구성에 대한 정보

각 매개 변수 설정을 외부 엔진 구성에 포함할지 여부를 기록한 다음 포함하려는 매개 변수의 값을 기록해야 합니다.

정보 유형입니다	필수 요소입니다	포함	당신의 가치
스토리지 가상 시스템(SVM) 이름	예	예	
엔진 이름입니다	예	예	
기본 FPolicy 서버	예	예	
포트 번호입니다	예	예	
2차 FPolicy 서버	아니요		
외부 엔진 유형	아니요		
외부 FPolicy 서버와의 통신에 사용되는 SSL 옵션입니다	예	예	
인증서 FQDN 또는 사용자 지정 일반 이름입니다	아니요		
인증서 일련 번호입니다	아니요		
인증 기관	아니요		

고급 외부 엔진 매개 변수에 대한 정보입니다

고급 매개 변수를 사용하여 외부 엔진을 구성하려면 고급 권한 모드에서 구성 명령을 입력해야 합니다.

정보 유형입니다	필수 요소입니다	포함	당신의 가치
요청 취소 시간이 초과되었습니다	아니요		
요청 중단 시간 초과	아니요		
상태 요청 전송 간격입니다	아니요		
FPolicy 서버에서 최대 미해결 요청을 사용합니다	아니요		
응답하지 않는 FPolicy 서버의 연결을 끊는 데 시간이 초과되었습니다	아니요		
FPolicy 서버에 연결 유지 메시지를 보내는 간격	아니요		
최대 재연결 시도 횟수	아니요		
수신 버퍼 크기입니다	아니요		
전송 버퍼 크기입니다	아니요		
다시 연결하는 동안 세션 ID를 제거하는 데 시간이 초과되었습니다	아니요		

FPolicy 이벤트 구성을 계획합니다

ONTAP FPolicy 이벤트 구성에 대해 알아봅니다

FPolicy 이벤트를 구성하기 전에 FPolicy 이벤트가 생성하는 것이 무엇을 의미하는지 이해해야 합니다. 이벤트를 모니터링할 프로토콜, 모니터링할 이벤트 및 사용할 이벤트 필터를 결정해야 합니다. 이 정보는 설정할 값을 계획하는 데 도움이 됩니다.

FPolicy 이벤트를 생성하는 것은 의미입니다

FPolicy 이벤트를 생성한다는 것은 FPolicy 프로세스에서 모니터링할 파일 액세스 작업과 모니터링되는 이벤트 알림 중 외부 FPolicy 서버로 보내야 하는 정보를 정의하는 것입니다. FPolicy 이벤트 구성은 다음 구성 정보를 정의합니다.

- 스토리지 가상 시스템(SVM) 이름
- 이벤트 이름입니다
- 모니터링할 프로토콜

FPolicy는 SMB, NFSv3, NFSv4 및 ONTAP 9.15.1부터 NFSv4.1 파일 액세스 작업을 모니터링할 수 있습니다.

- 모니터링할 파일 작업

  모든 파일 작업이 각 프로토콜에 유효한 것은 아닙니다.

- 구성할 파일 필터

  특정 파일 작업 및 필터 조합만 유효합니다. 각 프로토콜에는 지원되는 고유한 조합 세트가 있습니다.

- 볼륨 마운트 및 마운트 해제 작업을 모니터링할지 여부

> ⓘ 세 가지 매개 변수(-protocol, -file-operations, -filters)에 대한 종속성이 있습니다. 다음 조합은 세 가지 매개 변수에 대해 유효합니다.
>
> - '-protocol' 및 '-file-operations' 매개변수를 지정할 수 있습니다.
> - 세 가지 매개 변수를 모두 지정할 수 있습니다.
> - 매개 변수를 지정할 수 없습니다.

FPolicy 이벤트 구성에 포함되는 내용

다음 가용 FPolicy 이벤트 구성 매개 변수 목록을 사용하여 구성을 계획할 수 있습니다.

정보 유형입니다	옵션을 선택합니다
SVM _ 이 FPolicy 이벤트와 연결할 SVM 이름을 지정합니다. 각 FPolicy 구성은 단일 SVM 내에서 정의됩니다. FPolicy 정책 구성을 생성하기 위해 함께 조합되는 외부 엔진, 정책 이벤트, 정책 범위 및 정책은 모두 동일한 SVM과 연결되어야 합니다.	'-vserver''vserver_name'

_ 이벤트 이름 _ FPolicy 이벤트에 할당할 이름을 지정합니다. FPolicy 정책을 생성할 때 FPolicy 이벤트를 이벤트 이름을 사용하여 정책에 연결합니다. 이름은 최대 256자까지 입력할 수 있습니다. MetroCluster 또는 SVM 재해 복구 구성에서 이벤트를 구성하는 경우 최대 200자의 이름을 입력해야 합니다. 이름에는 다음 ASCII 범위 문자의 조합을 사용할 수 있습니다. • "A" ~ "z" • A부터 Z까지 • 0에서 9까지 • ""_","-",".""	이벤트-이름 이벤트_이름
프로토콜 _ FPolicy 이벤트에 구성할 프로토콜을 지정합니다. '-protocol' 목록은 다음 값 중 하나를 포함할 수 있습니다. • 'CIFS'입니다 • 'NFSv3' • 'NFSv4 '-protocol'을 지정하면 '-file-operations' 파라미터에 유효한 값을 지정해야 합니다. 프로토콜 버전이 변경되면 유효한 값이 변경될 수 있습니다. ONTAP 9.15.1부터 NFSv4를 사용하면 NFSv4.0 및 NFSv4.1 이벤트를 캡처할 수 있습니다.	프로토콜

_ 파일 작업 _ FPolicy 이벤트에 대한 파일 작업 목록을 지정합니다. 이 이벤트는 '-protocol' 매개 변수에 지정된 프로토콜을 사용하여 모든 클라이언트 요청에서 이 목록에 지정된 작업을 확인합니다. 쉼표로 구분된 목록을 사용하여 하나 이상의 파일 작업을 나열할 수 있습니다. '-file-operations' 목록에는 다음 값 중 하나 이상이 포함될 수 있습니다. • 파일 닫기 작업을 위해 '닫기'를 선택합니다 • 파일 작성 작업을 위한 '작성'입니다 • 디렉토리 생성 작업을 위한 'create-dir' • 파일 삭제 작업의 경우 '삭제'를 선택합니다 • 디렉토리 삭제 작업의 경우 'Delete_dir' • Get 특성 연산에 대한 GetAttr 입니다 • 링크 작동을 위한 링크 • 조회 연산에 대한 조회 • 파일 열기 작업을 위해 '열기'를 선택합니다 • 파일 읽기 작업에 대한 READ • 파일 쓰기 작업에 대한 '쓰기' • 파일 이름 바꾸기 작업에 대한 이름'입니다 • 디렉터리 이름 바꾸기 작업의 경우 RENAME_DIR입니다 • 셋트 특성 연산에 대한 '셋트'입니다 • 심볼 링크 작업을 위한 '대칭 링크'입니다 '-file-operations'를 지정하면 '-protocol' 파라미터에 유효한 프로토콜을 지정해야 합니다.	'-파일-작업"파일_작업',…

필터 _ 지정된 프로토콜에 대해 지정된 파일 작업에 대한 필터 목록을 지정합니다. '-filters' 매개 변수의 값은 클라이언트 요청을 필터링하는 데 사용됩니다. 목록에는 다음 중 하나 이상이 포함될 수 있습니다. ⓘ '-filters' 파라미터를 지정할 경우 '-file-operations' 및 '-protocol' 파라미터에 대한 유효한 값을 지정해야 합니다. • 대체 데이터 스트림에 대한 클라이언트 요청을 필터링하는 모니터 광고 옵션 • 수정과 함께 닫기 위해 클라이언트 요청을 필터링하는 '수정 종료' 옵션. • 수정하지 않고 클라이언트 요청을 필터링하는 '수정 없이 종료' 옵션. • 첫 번째 읽기에 대한 클라이언트 요청을 필터링하는 '첫 번째 읽기' 옵션. • 첫 번째 쓰기를 위해 클라이언트 요청을 필터링하는 '첫 번째 쓰기' 옵션. • 오프라인 비트 세트에 대한 클라이언트 요청을 필터링하는 오프라인 비트 옵션입니다. 이 필터를 설정하면 FPolicy 서버에서 오프라인 파일에 액세스할 때만 알림을 받습니다. • 삭제 의도로 개설된 클라이언트 요청을 필터링하는 'open-with-delete-intent' 옵션. 이 필터를 설정하면 FPolicy 서버에서 파일을 삭제하려고 할 때만 FPolicy 서버가 알림을 받게 됩니다. 'file_delete_on_close' 플래그가 지정된 경우 파일 시스템에서 사용됩니다. • 클라이언트 요청을 쓰기 의도로 필터링하기 위한 "쓰기 의도로 열기" 옵션. 이 필터를 설정하면 FPolicy 서버에서 파일을 열려고 할 때만 알림을 받습니다. • 크기 변경으로 클라이언트 쓰기 요청을 필터링하기 위한 Write-with-size-change 옵션. • 'SetAttr-with-owner-change' 옵션을 사용하여 파일 또는 디렉터리의 소유자 변경을 위한 클라이언트 SetAttr 요청을 필터링합니다. • 파일 또는 디렉토리의 그룹을 변경하기 위한 클라이언트 SetAttr 요청을 필터링하는 'Setattr-with-group-change' 옵션 • 파일 또는 디렉터리에서 SACL을 변경하기 위한 클라이언트 SetAttr 요청을 필터링하는 'Setattr-with-SACL-change' 옵션입니다. 이 필터는 SMB 및 NFSv4 프로토콜에만 사용할 수 있습니다. • 파일 또는 디렉토리의 DACL 변경을 위한 클라이언트 SetAttr 요청을 필터링하는 'Setattr-with-DACL-change' 옵션. 이 필터는 SMB 및 NFSv4 프로토콜에만 사용할 수 있습니다. 파일 또는 디렉토리의 수정 시간을 변경하기 위해 클라이언트 SetAttr 요청을 필터링하는 'Setattr-with-modify-time-change' 옵션. 파일 또는 디렉터리의 액세스 시간 변경을 위한 클라이언트 SetAttr 요청을	'-filters' 필터,…

_ 은(는) 볼륨 작업이 필요합니다. _ 볼륨 마운트 및 마운트 해제 작업에 모니터링이 필요한지 여부를 지정합니다. 기본값은 false 입니다.	'-볼륨-작동'{'참'
'거짓'} '-filters' 필터,…	_FPolicy 액세스가 거부된 알림 _ ONTAP 9.13.1 부터는 권한이 없어 실패한 파일 작업에 대한 알림을 받을 수 있습니다. 이러한 알림은 보안, 랜섬웨어 보호 및 거버넌스에 유용합니다. 권한 부족으로 인해 파일 작업에 대한 알림이 생성되지 않습니다. 여기에는 다음이 포함됩니다. • NTFS 권한으로 인해 오류가 발생했습니다. • Unix 모드 비트로 인한 실패. • NFSv4 ACL로 인한 실패
`-monitor-fileop-failure` {`true`	`false`}

SMB용 **ONTAP FPolicy** 모니터에서 지원되는 파일 작업 및 필터 조합

FPolicy 이벤트를 구성할 때는 특정 조합의 파일 작업 및 필터만 SMB 파일 액세스 작업을 모니터링하는 데 지원됩니다.

SMB 파일 액세스 이벤트의 FPolicy 모니터링을 위해 지원되는 파일 작업 및 필터 조합 목록은 다음 표에 나와 있습니다.

지원되는 파일 작업	지원되는 필터
를 닫습니다	모니터 광고, 오프라인 비트, 수정 사항이 있는 닫기, 수정 없이 종료, 읽기 작업이 거의 없는 exclude-directory 를 선택합니다
생성	모니터 광고, 오프라인 비트
디렉토리 작성	현재 이 파일 작업에 대해 지원되는 필터가 없습니다.
삭제	모니터 광고, 오프라인 비트
Delete_dir	현재 이 파일 작업에 대해 지원되는 필터가 없습니다.
GetAttr	offline-bit, exclude-dir

개방형	monitor-ads, offline-bit, open-with-delete-intent, open-with-write-intent, exclude-dir
읽기	모니터 광고, 오프라인 비트, 첫 번째 읽기
쓰기	모니터 광고, 오프라인 비트, 처음 쓰기, 크기 변경 포함 쓰기
이름 바꾸기	모니터 광고, 오프라인 비트
이름 바꾸기_디렉토리	현재 이 파일 작업에 대해 지원되는 필터가 없습니다.
SetAttr	monitor-ads, offline-bit, SetAttr_with_owner_change, SetAttr_with_group_change, SetAttr_with_mode_change, SetAttr_with_SACL_change, SetAttr_with_DACL_change, SetAttr_with_modify_time_change, SetAttr_with_access_time_change, SetAttr_with_creation_time_change, SetAttr_with_size_change, SetAttr_with_allocation_size_change, exclude_directory

ONTAP 9.13.1 부터는 권한이 없어 실패한 파일 작업에 대한 알림을 받을 수 있습니다. SMB 파일 액세스 이벤트의 FPolicy 모니터링을 위한 지원되는 액세스 거부 파일 작업 및 필터 조합 목록은 다음 표에 나와 있습니다.

지원되는 액세스 거부 파일 작업입니다	지원되는 필터
개방형	해당 없음

ONTAP FPolicy가 **NFSv3**에 대해 모니터링하는 지원되는 파일 작업 및 필터 조합

FPolicy 이벤트를 구성할 때는 NFSv3 파일 액세스 작업을 모니터링하기 위해 특정 파일 작업 및 필터 조합만 지원된다는 점에 유의해야 합니다.

NFSv3 파일 액세스 이벤트의 FPolicy 모니터링을 위해 지원되는 파일 작업 및 필터 조합 목록은 다음 표에 나와 있습니다.

지원되는 파일 작업	지원되는 필터
생성	오프라인 비트
디렉토리 작성	현재 이 파일 작업에 대해 지원되는 필터가 없습니다.
삭제	오프라인 비트
Delete_dir	현재 이 파일 작업에 대해 지원되는 필터가 없습니다.
링크	오프라인 비트

조회	offline-bit, exclude-dir
읽기	오프라인-비트, 첫 번째-읽기
쓰기	오프라인-비트, 첫 번째-쓰기, 크기 변경 쓰기
이름 바꾸기	오프라인 비트
이름 바꾸기_디렉토리	현재 이 파일 작업에 대해 지원되는 필터가 없습니다.
SetAttr	offline-bit, SetAttr_with_owner_change, SetAttr_with_group_change, SetAttr_with_mode_change, SetAttr_with_modify_time_change, SetAttr_with_access_time_change, SetAttr_with_size_change, exclude_directory
symlink	오프라인 비트

ONTAP 9.13.1 부터는 권한이 없어 실패한 파일 작업에 대한 알림을 받을 수 있습니다. NFSv3 파일 액세스 이벤트의 FPolicy 모니터링을 위한 지원되는 액세스 거부 파일 작업 및 필터 조합 목록은 다음 표에 나와 있습니다.

지원되는 액세스 거부 파일 작업입니다	지원되는 필터
액세스	해당 없음
생성	해당 없음
디렉토리 작성	해당 없음
삭제	해당 없음
Delete_dir	해당 없음
링크	해당 없음
읽기	해당 없음
이름 바꾸기	해당 없음
이름 바꾸기_디렉토리	해당 없음
SetAttr	해당 없음
쓰기	해당 없음

FPolicy 이벤트를 구성할 때는 NFSv4 파일 액세스 작업을 모니터링하기 위해 특정 파일 작업 및 필터 조합만 지원된다는 점에 유의해야 합니다.

ONTAP 9.15.1부터 FPolicy는 NFSv4.1 프로토콜을 지원합니다.

NFSv4 또는 NFSv4.1 파일 액세스 이벤트에 대한 FPolicy 모니터링에 대해 지원되는 파일 작업 및 필터 조합의 목록이 다음 표에 나와 있습니다.

지원되는 파일 작업	지원되는 필터
를 닫습니다	offline-bit, exclude-directory
생성	오프라인 비트
디렉토리 작성	현재 이 파일 작업에 대해 지원되는 필터가 없습니다.
삭제	오프라인 비트
Delete_dir	현재 이 파일 작업에 대해 지원되는 필터가 없습니다.
GetAttr	offline-bit, exclude-directory
링크	오프라인 비트
조회	offline-bit, exclude-directory
개방형	offline-bit, exclude-directory
읽기	오프라인-비트, 첫 번째-읽기
쓰기	오프라인-비트, 첫 번째-쓰기, 크기 변경 쓰기
이름 바꾸기	오프라인 비트
이름 바꾸기_디렉토리	현재 이 파일 작업에 대해 지원되는 필터가 없습니다.
SetAttr	offline-bit, SetAttr_with_owner_change, SetAttr_with_group_change, SetAttr_with_mode_change, SetAttr_with_SACL_change, SetAttr_with_DACL_change, SetAttr_with_modify_time_change, SetAttr_with_access_time_change, SetAttr_with_size_change, exclude_directory
symlink	오프라인 비트

ONTAP 9.13.1 부터는 권한이 없어 실패한 파일 작업에 대한 알림을 받을 수 있습니다. NFSv4 또는 NFSv4.1 파일 액세스 이벤트에 대한 FPolicy 모니터링에 대해 지원되는 액세스 거부 파일 작업 및 필터 조합의 목록이 다음 표에 나와 있습니다.

지원되는 액세스 거부 파일 작업입니다	지원되는 필터
액세스	해당 없음
생성	해당 없음
디렉토리 작성	해당 없음
삭제	해당 없음
Delete_dir	해당 없음
링크	해당 없음
개방형	해당 없음
읽기	해당 없음
이름 바꾸기	해당 없음
이름 바꾸기_디렉토리	해당 없음
SetAttr	해당 없음
쓰기	해당 없음

ONTAP FPolicy 이벤트 구성 워크시트 완료

이 워크시트를 사용하여 FPolicy 이벤트 구성 프로세스 중에 필요한 값을 기록할 수 있습니다. 매개 변수 값이 필요한 경우 FPolicy 이벤트를 구성하기 전에 매개 변수에 사용할 값을 결정해야 합니다.

각 매개 변수 설정을 FPolicy 이벤트 구성에 포함할지 여부를 기록한 다음 포함하려는 매개 변수의 값을 기록해야 합니다.

정보 유형입니다	필수 요소입니다	포함	당신의 가치
스토리지 가상 시스템(SVM) 이름	예	예	
이벤트 이름입니다	예	예	

프로토콜	아니요		
파일 작업	아니요		
필터	아니요		
볼륨 작업입니다	아니요		
거부된 이벤트 액세스 + (ONTAP 9.13부터 지원)	아니요		

FPolicy 정책 구성을 계획합니다

ONTAP FPolicy 정책 구성에 대해 알아보세요

FPolicy 정책을 구성하기 전에 정책을 생성할 때 어떤 매개 변수가 필요한지, 그리고 특정 선택적 매개 변수를 구성해야 하는 이유를 이해해야 합니다. 이 정보는 각 매개변수에 대해 설정할 값을 결정하는 데 도움이 됩니다.

FPolicy 정책을 생성할 때 정책을 다음과 연계합니다.

- 스토리지 가상 시스템(SVM)
- 하나 이상의 FPolicy 이벤트입니다
- FPolicy 외부 엔진

또한 몇 가지 선택적 정책 설정을 구성할 수도 있습니다.

FPolicy 정책 구성에 포함되는 내용

다음 사용 가능한 FPolicy 정책 목록과 선택적 매개 변수를 사용하여 구성을 계획할 수 있습니다.

정보 유형입니다	옵션을 선택합니다	필수 요소입니다	기본값
_SVM 이름 _ FPolicy 정책을 생성할 SVM의 이름을 지정합니다.	'-vserver"vserver_name'	예	없음

_정책 이름 _ FPolicy 정책의 이름을 지정합니다. 이름은 최대 256자까지 입력할 수 있습니다. MetroCluster 또는 SVM 재해 복구 구성에서 정책을 구성하는 경우 이름은 최대 200자가 되어야 합니다. 이름에는 다음 ASCII 범위 문자의 조합을 사용할 수 있습니다. • "A" ~ "z" • A부터 Z까지 • 0에서 9까지 • ""_","-",".""	정책-이름 정책_이름	예	없음
_ 이벤트 이름 _ FPolicy 정책에 연결할 쉼표로 구분된 이벤트 목록을 지정합니다. • 둘 이상의 이벤트를 정책에 연결할 수 있습니다. • 이벤트는 프로토콜에 따라 다릅니다. • 단일 정책을 사용하여 정책이 모니터링할 각 프로토콜에 대한 이벤트를 생성한 다음 이벤트를 정책에 연결하여 둘 이상의 프로토콜에 대한 파일 액세스 이벤트를 모니터링할 수 있습니다. • 이벤트가 이미 있어야 합니다.	'-events"event_name',…	예	없음
_영구 저장소 _ ONTAP 9.14.1부터 이 매개 변수는 SVM의 비동기적 정책에 대한 파일 액세스 이벤트를 캡처할 영구 저장소를 지정합니다.	`-persistent -store persistent_store_name`	아니요	없음

_외부 엔진 이름 _ FPolicy 정책에 연결할 외부 엔진의 이름을 지정합니다. • 외부 엔진에는 FPolicy 서버로 알림을 보내는 데 필요한 정보가 노드에 포함되어 있습니다. • FPolicy를 구성하여 단순한 파일 차단에 ONTAP 기본 외부 엔진을 사용하거나 외부 FPolicy 서버(FPolicy 서버)를 사용하여 보다 정교한 파일 차단 및 파일 관리를 위해 구성된 외부 엔진을 사용할 수 있습니다. • 네이티브 외부 엔진을 사용하려면 이 매개 변수의 값을 지정하지 않거나 값으로 'native'를 지정할 수 있습니다. • FPolicy 서버를 사용하려면 외부 엔진에 대한 구성이 이미 있어야 합니다.	엔진 엔진 엔진 이름	예(정책에서 내부 ONTAP 기본 엔진을 사용하지 않는 경우)	네이티브입니다
_ 은(는) 필수 스크리닝 필수 항목입니다. _ 필수 파일 액세스 스크리닝이 필요한지 여부를 지정합니다. • 필수 선별 설정은 기본 및 보조 서버가 모두 중단되거나 지정된 시간 제한 시간 내에 FPolicy 서버로부터 응답이 없을 경우 파일 액세스 이벤트에 대해 수행되는 작업을 결정합니다. • true로 설정하면 파일 액세스 이벤트가 거부됩니다. • false로 설정하면 파일 액세스 이벤트가 허용됩니다.	'-is-mandatory'{'true'	'false'}	아니요

"참"입니다	권한 있는 액세스 허용 _ FPolicy 서버에서 권한이 있는 데이터 연결을 사용하여 모니터링되는 파일 및 폴더에 대한 액세스 권한을 부여할지 여부를 지정합니다. 구성된 경우 FPolicy 서버는 권한 있는 데이터 연결을 사용하여 모니터링되는 데이터가 포함된 SVM의 루트에서 파일에 액세스할 수 있습니다. 특별 권한 데이터 액세스의 경우 SMB는 클러스터에서 라이센스를 받아야 하며 FPolicy 서버에 연결하는 데 사용되는 모든 데이터 LIF는 허용되는 프로토콜 중 하나로 'CIFS'를 사용하도록 구성해야 합니다. 특별 권한 액세스를 허용하도록 정책을 구성하려면 FPolicy 서버가 권한 액세스에 사용할 계정의 사용자 이름도 지정해야 합니다.	'-allow-privileged-access' {'yes'	'no'}

아니요(패스스루 읽기가 활성화되지 않은 경우)	아니	_특별 권한 사용자 이름 _ FPolicy 서버가 권한 있는 데이터 액세스에 사용하는 계정의 사용자 이름을 지정합니다. • 이 매개 변수의 값은 "domain\user name" 형식을 사용해야 합니다. • '-allow-privileged-access'가 no로 설정되어 있으면 이 파라미터에 설정된 값이 무시됩니다.	'-privileged-user-name' user_name

아니요(권한 있는 액세스가 활성화되지 않은 경우)	없음	통과 허용 - 읽기 _ FPolicy 서버가 FPolicy 서버에서 2차 스토리지(오프라인 파일)에 아카이빙된 파일에 대해 패스스루 읽기 서비스를 제공할 수 있는지 여부를 지정합니다. • 패스스루 읽기는 데이터를 운영 스토리지로 복원하지 않고 오프라인 파일의 데이터를 읽는 방법입니다. PassThrough-read는 읽기 요청에 응답하기 전에 파일을 운영 스토리지에 다시 호출할 필요가 없기 때문에 응답 대기 시간을 줄입니다. 또한 패스스루 읽기를 통해 읽기 요청을 충족하기 위해 리콜된 파일에만 운영 스토리지 공간을 사용할 필요가 없으므로 스토리지 효율성을 최적화합니다. • 이 기능을 사용하도록 설정하면 FPolicy 서버에서 통과 읽기를 위해 특별히 연 별도의 권한 데이터 채널을 통해 파일에 대한 데이터를 제공합니다. • 패스스루 읽기를 구성하려면 권한 있는 액세스를 허용하도록 정책도 구성해야 합니다.	'-is-passstrough-read-enabled'{'true'

기본 엔진을 사용하도록 FPolicy 정책을 구성하는 경우 정책에 구성된 FPolicy 범위를 정의하는 방법에 대한 특정 요구사항이 있습니다.

FPolicy 범위는 FPolicy 정책이 적용되는 경계(예: FPolicy가 지정된 볼륨 또는 공유에 적용되는지 여부)를 정의합니다. FPolicy 정책이 적용되는 범위를 더욱 제한하는 다양한 매개 변수가 있습니다. 이 매개 변수 중 하나인 '-is-file-extension-check-on-directories-enabled'는 디렉터리에서 파일 확장명을 검사할지 여부를 지정합니다. 기본값은 false로, 디렉토리의 파일 확장자가 선택되지 않았음을 의미합니다.

기본 엔진을 사용하는 FPolicy 정책이 공유 또는 볼륨에서 활성화되고 정책 범위에 대한 '-is-file-extension-check-on-directories-enabled' 매개 변수가 'false'로 설정된 경우 디렉토리 액세스가 거부됩니다. 이 구성에서는 파일 확장자가 디렉토리에 대해 검사되지 않으므로 정책 범위에 속하는 경우 모든 디렉토리 작업이 거부됩니다.

네이티브 엔진을 사용할 때 디렉터리 액세스가 성공하도록 하려면 범위를 만들 때 '-is-file-extension-check-on-directories-enabled 매개 변수'를 'true'로 설정해야 합니다.

이 매개 변수를 'true'로 설정하면 디렉터리 작업에 대한 확장 검사가 수행되어 FPolicy 범위 구성에 포함되거나 제외된 확장명을 기준으로 액세스를 허용할지 또는 거부할지 여부를 결정합니다.

이 워크시트를 사용하여 FPolicy 정책 구성 프로세스 중에 필요한 값을 기록할 수 있습니다. 각 매개 변수 설정을 FPolicy 정책 구성에 포함할지 여부를 기록한 다음 포함하려는 매개 변수의 값을 기록해야 합니다.

정보 유형입니다	포함	당신의 가치
스토리지 가상 시스템(SVM) 이름	예	
정책 이름입니다	예	
이벤트 이름	예	
영구 저장소		
외부 엔진 이름입니다		
필수 스크리닝이 필요합니까?		
권한 있는 액세스를 허용합니다		
권한이 있는 사용자 이름입니다		
통과 읽기가 활성화되어 있습니까?		

FPolicy 범위 구성을 계획합니다

ONTAP FPolicy 범위 구성에 대해 알아보세요

FPolicy 범위를 구성하기 전에 범위를 생성하는 것이 무엇을 의미하는지 이해해야 합니다. 범위 구성에 포함된 내용을 이해해야 합니다. 또한 우선 순위 범위 규칙이 무엇인지 이해해야 합니다. 이 정보는 설정할 값을 계획하는 데 도움이 될 수 있습니다.

FPolicy 범위를 생성하는 것은 의미입니다

FPolicy 범위를 만들려면 FPolicy 정책이 적용되는 경계를 정의해야 합니다. SVM(스토리지 가상 시스템)은 기본 경계입니다. FPolicy 정책의 범위를 생성할 때 적용되는 FPolicy 정책을 정의해야 하며 범위를 적용할 SVM을 지정해야 합니다.

지정된 SVM 내에서 범위를 더욱 제한하는 다양한 매개 변수가 있습니다. 범위에 포함할 항목을 지정하거나 범위에서 제외할 항목을 지정하여 범위를 제한할 수 있습니다. 설정된 정책에 범위를 적용하면 이 명령에 의해 정의된 범위에 정책 이벤트 검사가 적용됩니다.

""포함" 옵션에서 일치하는 파일 액세스 이벤트에 대한 알림이 생성됩니다. ""제외" 옵션에서 일치하는 파일 액세스 이벤트에 대한 알림이 생성되지 않습니다.

FPolicy 범위 구성은 다음 구성 정보를 정의합니다.

- SVM 이름
- 정책 이름입니다
- 모니터링되는 항목을 포함하거나 제외할 공유입니다
- 모니터링할 항목을 포함하거나 제외할 내보내기 정책입니다
- 모니터링되는 항목을 포함하거나 제외할 볼륨입니다
- 모니터링되는 항목을 포함하거나 제외할 파일 확장입니다
- 디렉토리 객체에 대한 파일 확장자 검사 수행 여부

> 클러스터 FPolicy 정책 범위에는 특별히 고려해야 할 사항이 있습니다. 클러스터 FPolicy 정책은 클러스터 관리자가 admin SVM에 대해 생성하는 정책입니다. 클러스터 관리자가 해당 클러스터 FPolicy 정책의 범위도 생성한 경우 SVM 관리자는 동일한 정책의 범위를 생성할 수 없습니다. 그러나 클러스터 관리자가 클러스터 FPolicy 정책의 범위를 생성하지 않는 경우 SVM 관리자는 해당 클러스터 정책의 범위를 생성할 수 있습니다. SVM 관리자가 해당 클러스터 FPolicy 정책의 범위를 생성하는 경우, 클러스터 관리자가 이후에 동일한 클러스터 정책에 대한 클러스터 범위를 생성할 수 없습니다. 이는 클러스터 관리자가 동일한 클러스터 정책의 범위를 재정의할 수 없기 때문입니다.

우선 순위 범위 규칙은 무엇입니까

범위 구성에 적용되는 우선 순위 규칙은 다음과 같습니다.

- 공유가 '-공유-포함' 매개 변수에 포함되어 있고 공유의 상위 볼륨이 '-볼륨-제외' 매개 변수에 포함된 경우 '-볼륨-제외가 '-공유-포함'보다 우선합니다.
- 수출 정책이 '-export-policies-to-include' 매개 변수에 포함되어 있고 수출 정책의 상위 볼륨이 '-volumes-to-exclude' 매개 변수에 포함된 경우 '-volumes-to-exclude'가 '-export-policies-to-include'보다 우선합니다.

- 관리자는 '-file-extensions-to-include' 및 '-file-extensions-to-exclude' 목록을 모두 지정할 수 있습니다.

  '-file-extensions-to-exclude' 매개 변수가 검사되기 전에 '-file-extensions-to-include' 매개 변수가 선택됩니다.

FPolicy 범위 구성에 포함되는 내용

다음 가용 FPolicy 범위 구성 매개 변수 목록을 사용하여 구성을 계획할 수 있습니다.

> 범위에 포함되거나 범위에서 제외될 공유, 내보내기 정책, 볼륨 및 파일 확장명을 구성할 때 포함 및 제외 매개 변수에는 ""와 같은 메타문자도 포함될 수 있습니다?`" and "`"". 정규식의 사용은 지원되지 않습니다.

정보 유형입니다	옵션을 선택합니다
SVM _ FPolicy 범위를 생성할 SVM 이름을 지정합니다. 각 FPolicy 구성은 단일 SVM 내에서 정의됩니다. FPolicy 정책 구성을 생성하기 위해 함께 조합되는 외부 엔진, 정책 이벤트, 정책 범위 및 정책은 모두 동일한 SVM과 연결되어야 합니다.	'-vserver"vserver_name'
_정책 이름 _ 범위를 연결할 FPolicy 정책의 이름을 지정합니다. FPolicy 정책이 이미 존재해야 합니다.	정책-이름 정책_이름
_ 을(를) 포함할 공유 _ 범위가 적용되는 FPolicy 정책을 모니터링할 쉼표로 구분된 공유 목록을 지정합니다.	'-공유-포함"사어_이름',…
제외할 공유 _ 범위가 적용되는 FPolicy 정책에 대해 모니터링에서 제외할 쉼표로 구분된 공유 목록을 지정합니다.	'-공유-제외"사어_이름',…
_Volumes to Include_범위가 적용되는 FPolicy 정책을 모니터링할 쉼표로 구분된 볼륨 목록을 지정합니다.	'-볼륨-포함"볼륨_이름',…
제외할 볼륨 _ 범위가 적용되는 FPolicy 정책에 대해 모니터링에서 제외할 쉼표로 구분된 볼륨 목록을 지정합니다.	'-볼륨-제외"볼륨_이름',…

_ 포함할 정책 내보내기 _ 범위가 적용되는 FPolicy 정책을 모니터링할 쉼표로 구분된 엑스포트 정책 목록을 지정합니다.	'-export-policies-to-include' export_policy_name',…
_ 제외할 정책 내보내기 _ 범위가 적용되는 FPolicy 정책에 대해 모니터링에서 제외할 내보내기 정책의 쉼표로 구분된 목록을 지정합니다.	'-export-policies-to-exclude' export_policy_name',…
_ 포함할 파일 확장자 _ 범위가 적용되는 FPolicy 정책을 모니터링할 쉼표로 구분된 파일 확장자 목록을 지정합니다.	'-file-extensions-to-include"file_extensions',…
_ 제외할 파일 확장자 _ 범위가 적용되는 FPolicy 정책에 대해 모니터링에서 제외할 파일 확장명 목록을 쉼표로 구분하여 지정합니다.	'-file-extensions-to-exclude"file_extensions',…
_ 디렉토리에 대한 파일 확장자 확인이 활성화되었습니까? _ 파일 이름 확장명 검사를 디렉터리 개체에도 적용할지 여부를 지정합니다. 이 매개 변수를 "true"로 설정하면 디렉터리 개체는 일반 파일과 동일한 확장 검사를 받습니다. 이 매개 변수가 false로 설정되어 있으면 이름 확장명이 일치하지 않아도 디렉터리 이름이 확장명에 일치하지 않고 디렉터리에 대한 알림이 전송됩니다. 범위가 할당된 FPolicy 정책이 기본 엔진을 사용하도록 구성된 경우 이 매개 변수를 'true'로 설정해야 합니다.	'-is-file-extension-check-on-directories-enabled'{'true'
'false'	}

ONTAP FPolicy 범위 워크시트 완료

이 워크시트를 사용하여 FPolicy 범위 구성 프로세스에서 필요한 값을 기록할 수 있습니다. 매개 변수 값이 필요한 경우 FPolicy 범위를 구성하기 전에 매개 변수에 사용할 값을 결정해야 합니다.

FPolicy 범위 구성에 각 매개 변수 설정을 포함할지 여부를 기록한 다음 포함하려는 매개 변수의 값을 기록해야 합니다.

정보 유형입니다	필수 요소입니다	포함	당신의 가치
스토리지 가상 시스템(SVM) 이름	예	예	
정책 이름입니다	예	예	
포함할 공유입니다	아니요		
제외할 공유입니다	아니요		

포함할 볼륨	아니요		
제외할 볼륨입니다	아니요		
포함할 엑스포트 정책	아니요		
제외할 정책을 내보냅니다	아니요		
포함할 파일 확장자	아니요		
제외할 파일 확장자입니다	아니요		
디렉토리의 파일 확장자 확인이 활성화되었습니까?	아니요		

FPolicy 구성을 생성합니다

ONTAP FPolicy 외부 엔진 생성

FPolicy 구성을 생성하려면 외부 엔진을 생성해야 합니다. 외부 엔진은 FPolicy가 외부 FPolicy 서버에 대한 연결을 만들고 관리하는 방법을 정의합니다. 구성에서 내부 ONTAP 엔진(기본 외부 엔진)을 간단한 파일 차단에 사용하는 경우 별도의 FPolicy 외부 엔진을 구성하지 않아도 되며 이 단계를 수행할 필요가 없습니다.

시작하기 전에

를 클릭합니다 "외부 엔진" 워크시트를 작성해야 합니다.

이 작업에 대해

외부 엔진이 MetroCluster 구성에 사용되는 경우 소스 사이트에 있는 FPolicy 서버의 IP 주소를 1차 서버로 지정해야 합니다. 대상 사이트에 있는 FPolicy 서버의 IP 주소를 2차 서버로 지정해야 합니다.

단계

1. 'vserver FPolicy external-engine create' 명령을 사용하여 FPolicy 외부 엔진을 생성합니다.

   다음 명령을 실행하면 SVM(스토리지 가상 시스템)vs1.example.com 에서 외부 엔진이 생성됩니다. FPolicy 서버와의 외부 통신에는 인증이 필요하지 않습니다.

   'vserver FPolicy external-engine create-vserver-name vs1.example.com -engine-name engine.1-primary-servers 10.1.1.2, 10.1.1.3-port 6789-SSL-option no-auth'

2. 'vserver FPolicy external-engine show' 명령을 사용하여 FPolicy 외부 엔진 구성을 확인하십시오.

   다음 명령을 실행하면 SVM vs1.example.com 에 구성된 모든 외부 엔진에 대한 정보가 표시됩니다.

   'vserver FPolicy policy external-engine show -vserver vs1.example.com'을 참조하십시오

```
                                Primary        Secondary
External
Vserver             Engine      Servers        Servers       Port Engine
Type
---------------     ----------  -------------- ----------- ------
----------
vs1.example.com     engine1     10.1.1.2,      -             6789
synchronous
                                10.1.1.3
```

다음 명령을 실행하면 SVM vs1.example.com 의 ""엔진1" 외부 엔진에 대한 자세한 정보가 표시됩니다.

'vserver FPolicy policy external-engine show -vserver vs1.example.com -engine-name engine11'을 참조하십시오

```
                             Vserver: vs1.example.com
                              Engine: engine1
             Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
       Port Number of FPolicy Service: 6789
            Secondary FPolicy Servers: -
                 External Engine Type: synchronous
SSL Option for External Communication: no-auth
           FQDN or Custom Common Name: -
         Serial Number of Certificate: -
               Certificate Authority: -
```

ONTAP FPolicy 이벤트 생성

FPolicy 정책 구성을 생성하는 과정에서 FPolicy 이벤트를 생성해야 합니다. 이벤트가 생성될 때 FPolicy 정책에 이벤트를 연결합니다. 이벤트는 모니터링하고 필터링할 파일 액세스 이벤트와 모니터링할 프로토콜을 정의합니다.

시작하기 전에

FPolicy 이벤트를 완료해야 "워크시트"합니다.

FPolicy 이벤트를 생성합니다

1. 'vserver FPolicy event create' 명령을 사용하여 FPolicy 이벤트를 생성합니다.

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -file-operations open,close,read,write
   ```

2. 'vserver FPolicy event show' 명령을 사용하여 FPolicy 이벤트 구성을 확인하십시오.

   'vserver FPolicy policy event show - vserver vs1.example.com'을 참조하십시오

```
                  Event                File                        Is Volume
Vserver           Name      Protocols  Operations    Filters       Operation
---------------   --------- ---------  ------------- ---------
------------
vs1.example.com   event1    cifs       open, close,  -             false
                                      read, write
```

FPolicy 액세스 거부 이벤트를 생성합니다

ONTAP 9.13.1 부터는 권한이 없어 실패한 파일 작업에 대한 알림을 받을 수 있습니다. 이러한 알림은 보안, 랜섬웨어 보호 및 거버넌스에 유용합니다.

1. 'vserver FPolicy event create' 명령을 사용하여 FPolicy 이벤트를 생성합니다.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name
event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

ONTAP FPolicy 영구 저장소 생성

영구 저장소는 클라이언트 I/O 처리를 FPolicy 알림 처리와 분리하여 클라이언트 지연 시간을 줄여 줍니다. ONTAP 9.14.1부터 FPolicy를 설정할 수 있습니다 "영구 저장소" SVM에서 비동기적 정책에 대한 파일 액세스 이벤트를 캡처합니다. 동기(필수 또는 비필수) 및 비동기 필수 구성은 지원되지 않습니다.

ONTAP 9.15.1부터 FPolicy 영구 저장소 구성이 단순화됩니다. 를 클릭합니다 `persistent-store create` 명령은 SVM에 대한 볼륨 생성을 자동화하고 영구 저장소에 대한 볼륨을 구성합니다.

ONTAP 릴리즈에 따라 영구 저장소를 만드는 방법에는 두 가지가 있습니다.

- ONTAP 9.15.1 이상: 영구 저장소를 만들면 ONTAP에서 자동으로 볼륨을 만들고 동시에 구성합니다. FPolicy 영구 저장소 구성을 간소화하고 모든 모범 사례를 구현합니다.
- ONTAP 9.14.1: 볼륨을 수동으로 생성 및 구성한 다음 새로 생성된 볼륨에 대한 영구 저장소를 생성합니다.

각 SVM에 하나의 영구 저장소만 설정할 수 있습니다. 서로 다른 파트너의 정책이 있는 경우에도 이 단일 영구 저장소를 해당 SVM의 모든 FPolicy 구성에 사용해야 합니다.

영구 저장소 만들기(ONTAP 9.15.1 이상)

ONTAP 9.15.1부터 를 사용합니다 `fpolicy persistent-store create` 인라인 볼륨 생성 및 구성으로 FPolicy 영구 저장소를 생성하는 명령 ONTAP는 외부 사용자 프로토콜 액세스(CIFS/NFS)에서 볼륨을 자동으로 차단합니다.

시작하기 전에

- 영구 저장소를 생성하려는 SVM에 애그리게이트가 하나 이상 있어야 합니다.
- SVM에서 사용할 수 있는 애그리게이트에 액세스할 수 있어야 하고, 볼륨을 생성할 수 있는 충분한 권한이 있어야 합니다.

단계

1. 볼륨을 자동으로 생성 및 구성하는 영구 저장소를 생성합니다.

```
vserver fpolicy persistent-store create -vserver <vserver> -persistent-store
<name> -volume <volume_name> -size <size> -autosize-mode
<off|grow|grow_shrink>
```

   - 를 클릭합니다 `vserver` 매개 변수는 SVM의 이름입니다.
   - 를 클릭합니다 `persistent-store` 매개 변수는 영구 저장소의 이름입니다.
   - 를 클릭합니다 `volume` 매개 변수는 영구 저장소 볼륨의 이름입니다.

     기존의 빈 볼륨을 사용하려면 를 사용합니다 `volume show` 명령을 사용하여 찾아서 volume 매개 변수에 지정합니다.

   - 를 클릭합니다 `size` 매개 변수는 외부 서버(파트너 응용 프로그램)에 전달되지 않은 이벤트를 유지할 기간을 기반으로 합니다.

     예를 들어, 초당 30,000개의 알림이 있는 클러스터에서 30분 이벤트를 지속하려는 경우:

     필요한 볼륨 크기 = 30000 x 30 x 60 x 0.6KB(평균 알림 레코드 크기) = 32400000KB = ~32GB

     대략적인 알림 비율을 확인하려면 FPolicy 파트너 애플리케이션에 연결하거나 FPolicy 카운터를 사용하십시오 `requests_dispatched_rate`.

     기존 볼륨을 사용하는 경우 size 매개 변수는 선택 사항입니다. size 매개 변수에 값을 입력하면 지정한 크기로 볼륨이 수정됩니다.

   - 를 클릭합니다 `autosize-mode` 매개 변수는 볼륨의 자동 크기 조정 모드를 지정합니다. 지원되는 자동 크기 조정 모드는 다음과 같습니다.
     - 꺼짐 - 사용된 공간의 양에 대응하여 볼륨이 증가하거나 축소되지 않습니다.
     - 확장 - 볼륨의 사용된 공간이 확장 임계값을 초과할 때 볼륨이 자동으로 증가합니다.
     - grow_shrink - 사용된 공간의 양에 따라 볼륨이 증가하거나 축소됩니다.

2. FPolicy 정책을 생성하고 영구 저장소 이름을 해당 정책에 추가합니다. 자세한 내용은 을 참조하십시오 "FPolicy 정책을 생성합니다".

영구 저장소 생성**(ONTAP 9.14.1)**

볼륨을 생성한 다음 해당 볼륨을 사용할 영구 저장소를 만들 수 있습니다. 그런 다음 외부 사용자 프로토콜 액세스(CIFS/NFS)에서 새로 생성된 볼륨을 차단할 수 있습니다.

단계

1. 영구 저장소용으로 프로비저닝할 수 있는 SVM에 빈 볼륨을 생성합니다.

```
volume create -vserver <SVM Name> -volume <volume> -state <online> -policy
<default> -unix-permissions <777> -size <value> -aggregate <aggregate name>
-snapshot-policy <none>
```

   볼륨을 생성할 충분한 RBAC 권한을 가진 관리자 사용자가 volume CLI 명령 또는 REST API를 사용하여 원하는

크기의 볼륨을 생성하고 해당 볼륨의 이름을 로 제공해야 합니다 `-volume` 영구 저장소에서 CLI 명령 또는 REST API를 생성합니다.

- 를 클릭합니다 `vserver` 매개 변수는 SVM의 이름입니다.
- 를 클릭합니다 `volume` 매개 변수는 영구 저장소 볼륨의 이름입니다.
- 를 클릭합니다 `state` 볼륨을 사용할 수 있도록 매개 변수를 온라인으로 설정해야 합니다.
- 를 클릭합니다 `policy` 이미 구성된 경우 매개 변수는 FPolicy 서비스 정책으로 설정됩니다. 그렇지 않은 경우 를 사용할 수 있습니다 `volume modify` 나중에 명령을 사용하여 정책을 추가합니다.
- 를 클릭합니다 `unix-permissions` 매개 변수는 선택 사항입니다.
- 를 클릭합니다 `size` 매개 변수는 외부 서버(파트너 응용 프로그램)에 전달되지 않은 이벤트를 유지할 기간을 기반으로 합니다.

  예를 들어, 초당 30,000개의 알림이 있는 클러스터에서 30분 이벤트를 지속하려는 경우:

  필요한 볼륨 크기 = 30000 x 30 x 60 x 0.6KB(평균 알림 레코드 크기) = 32400000KB = ~32GB

대략적인 알림 비율을 확인하려면 FPolicy 파트너 애플리케이션에 연결하거나 FPolicy 카운터를 사용하십시오 `requests_dispatched_rate`.

- FlexVol 볼륨에 애그리게이트 매개 변수가 필요하며, 그렇지 않으면 필요하지 않습니다.
- 를 클릭합니다 `snapshot-policy` 매개 변수는 none으로 설정해야 합니다. 이렇게 하면 스냅샷이 실수로 복구되지 않아 현재 이벤트가 손실되고 중복 이벤트 처리가 방지됩니다.

  기존의 빈 볼륨을 사용하려면 를 사용합니다 `volume show` 명령을 사용하여 찾을 수 있으며 `volume modify` 명령을 사용하여 필요한 사항을 변경합니다. 정책, 크기 및 를 확인합니다 `snapshot-policy` 영구 저장소에 대한 매개 변수가 올바르게 설정되어 있습니다.

2. 영구 저장소 만들기:

   ```
   vserver fpolicy persistent store create -vserver <SVM> -persistent-store
   <PS_name> -volume <volume>
   ```

   - 를 클릭합니다 `vserver` 매개 변수는 SVM의 이름입니다.
   - 를 클릭합니다 `persistent-store` 매개 변수는 영구 저장소의 이름입니다.
   - 를 클릭합니다 `volume` 매개 변수는 영구 저장소 볼륨의 이름입니다.

3. FPolicy 정책을 생성하고 영구 저장소 이름을 해당 정책에 추가합니다. 자세한 내용은 을 참조하십시오 "FPolicy 정책을 생성합니다".

ONTAP FPolicy 정책 생성

FPolicy 정책을 생성할 때 외부 엔진과 하나 이상의 이벤트를 정책에 연결합니다. 또한 이 정책은 필수 선별 작업이 필요한지 여부, FPolicy 서버가 SVM(스토리지 가상 머신)의 데이터에 액세스할 수 있는 권한이 있는지 여부 및 오프라인 파일에 대한 패스스루 읽기를 사용할 수 있는지 여부도 지정합니다.

시작하기 전에

- FPolicy 정책 워크시트를 작성해야 합니다.
- FPolicy 서버를 사용하도록 정책을 구성하려는 경우 외부 엔진이 존재해야 합니다.
- FPolicy 정책과 연관하려는 FPolicy 이벤트가 하나 이상 있어야 합니다.
- 특별 권한 데이터 액세스를 구성하려면 SVM에 SMB 서버가 있어야 합니다.
- 정책에 대한 영구 저장소를 구성하려면 엔진 유형이 * 비동기 * 여야 하고 정책이 * 비필수 * 여야 합니다.

  자세한 내용은 을 참조하십시오 "영구 저장소를 만듭니다".

단계

1. FPolicy 정책을 생성합니다.

   ```
   vserver fpolicy policy create -vserver-name vserver_name -policy-name
   policy_name -engine engine_name -events event_name, [-persistent-store
   PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
   privileged-user-name domain\user_name] [-is-passthrough-read-enabled
   {true|false}]
   ```

   - FPolicy 정책에 하나 이상의 이벤트를 추가할 수 있습니다.
   - 기본적으로 필수 스크리닝이 활성화됩니다.
   - '-allow-privileged-access' 파라미터를 'yes'로 설정하여 권한 있는 액세스를 허용하려면 권한 있는 액세스에 대한 권한 있는 사용자 이름도 구성해야 합니다.
   - '-is-passthrough-read-enabled' 매개 변수를 'true'로 설정하여 패스스루 읽기를 구성하려면 권한이 있는 데이터 액세스도 구성해야 합니다.

     다음 명령을 실행하면 이벤트1, 외부 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진 엔진1 등의 정책1이 생성됩니다. 이 정책은 정책 구성에서 'vserver FPolicy policy create - vserver vs1.example.com -policy -name policy1 -events event1 - engine engine 1'이라는 기본값을 사용합니다

     다음 명령을 실행하면 이벤트2, 외부 엔진 등의 정책2가 생성됩니다. 이 정책은 지정된 사용자 이름을 사용하여 권한 있는 액세스를 사용하도록 구성됩니다. 패스스루 읽기가 활성화된 경우:

     'vserver FPolicy policy create - vserver vs1.example.com - policy -name policy2 - event2 - event2 - engine engine 2 - allow-privileged-access yes-privileged-user-name example\archive_acct-is-passthrough-read-enabled true'

     다음 명령은 ""event3""이라는 이벤트가 연결된 ""네이티브e1""이라는 정책을 만듭니다. 이 정책은 네이티브 엔진을 사용하며 정책 구성에서 기본값을 사용합니다.

   'vserver FPolicy policy create-vserver vs1.example.com -policy-name naive1-event3-engine native'

2. 'vserver FPolicy show' 명령을 사용하여 FPolicy 정책 구성을 확인하십시오.

   다음 명령을 실행하면 다음 정보를 비롯하여 세 가지 구성된 FPolicy 정책에 대한 정보가 표시됩니다.

   - 정책과 연결된 SVM
   - 정책과 연결된 외부 엔진입니다

- 정책과 관련된 이벤트입니다
- 필수 스크리닝이 필요한지 여부
- 특별 권한 액세스가 'vserver FPolicy show'인지 여부

```
   Vserver       Policy     Events    Engine    Is Mandatory  Privileged
                 Name                                         Access
--------------   ---------  --------- --------- ------------
-----------
vs1.example.com  policy1    event1    engine1   true          no
vs1.example.com  policy2    event2    engine2   true          yes
vs1.example.com  native1    event3    native    true          no
```

ONTAP FPolicy 범위 생성

FPolicy 정책을 생성한 후에는 FPolicy 범위를 생성해야 합니다. 범위를 생성할 때 범위를 FPolicy 정책과 연계합니다. 범위는 FPolicy 정책이 적용되는 경계를 정의합니다. 범위에는 공유, 엑스포트 정책, 볼륨, 파일 확장명을 기준으로 파일을 포함하거나 제외할 수 있습니다.

시작하기 전에

FPolicy 범위 워크시트를 작성해야 합니다. FPolicy 정책은 연결된 외부 엔진과 함께 있어야 하며(정책이 외부 FPolicy 서버를 사용하도록 구성된 경우) 하나 이상의 관련 FPolicy 이벤트가 있어야 합니다.

단계

1. 'vserver FPolicy scope create' 명령을 사용하여 FPolicy 범위를 생성합니다.

   'vserver FPolicy policy scope create-vserver-name vs1.example.com -policy-name policy1-volumes-to-include datavol1, datavol2'

2. 'vserver FPolicy scope show' 명령을 사용하여 FPolicy 범위 구성을 확인하십시오.

   'vserver FPolicy scope show -vserver vs1.example.com -instance'

```
                    Vserver: vs1.example.com
                     Policy: policy1
          Shares to Include: -
          Shares to Exclude: -
         Volumes to Include: datavol1, datavol2
         Volumes to Exclude: -
Export Policies to Include: -
Export Policies to Exclude: -
File Extensions to Include: -
File Extensions to Exclude: -
```

ONTAP FPolicy 정책 활성화

FPolicy 정책 구성을 수행한 후 FPolicy 정책을 사용하도록 설정합니다. 정책을 설정하면 우선 순위가 설정되고 정책에 대한 파일 액세스 모니터링이 시작됩니다.

시작하기 전에

FPolicy 정책은 연결된 외부 엔진과 함께 있어야 하며(정책이 외부 FPolicy 서버를 사용하도록 구성된 경우) 하나 이상의 관련 FPolicy 이벤트가 있어야 합니다. FPolicy 정책 범위가 존재하며 FPolicy 정책에 할당해야 합니다.

이 작업에 대해

우선 순위는 SVM(스토리지 가상 시스템)에서 여러 정책이 활성화되어 있고 둘 이상의 정책이 동일한 파일 액세스 이벤트에 가입되어 있는 경우에 사용됩니다. 네이티브 엔진 구성을 사용하는 정책은 정책을 설정할 때 할당된 시퀀스 번호에 관계없이 다른 엔진에 대한 정책보다 우선 순위가 높습니다.

관리 SVM에서 정책을 활성화할 수 없습니다.

단계

1. 'vserver FPolicy enable' 명령을 사용하여 FPolicy 정책을 활성화하십시오.

   'vserver FPolicy enable-vserver-name vs1.example.com - policy-name policy1-sequence-number 1'

2. 'vserver FPolicy show' 명령을 사용하여 FPolicy 정책이 활성화되어 있는지 확인하십시오.

   'vserver FPolicy show -vserver vs1.example.com'을 참조하십시오

```
                                  Sequence
Vserver           Policy Name       Number  Status   Engine
---------------  ----------------- --------  -------- ---------
vs1.example.com  policy1                 1  on       engine1
```

FPolicy 구성을 관리합니다

FPolicy 구성을 수정합니다

ONTAP에서 FPolicy 구성을 수정하는 명령

FPolicy 구성은 구성을 구성하는 요소를 수정하여 수정할 수 있습니다. 외부 엔진, FPolicy 이벤트, FPolicy 범위, FPolicy 영구 저장소 및 FPolicy 정책을 수정할 수 있습니다. FPolicy 정책을 사용하거나 사용하지 않도록 설정할 수도 있습니다. FPolicy 정책을 사용하지 않도록 설정하면 해당 정책에 대한 파일 모니터링이 중단됩니다.

구성을 수정하기 전에 FPolicy 정책을 사용하지 않도록 설정해야 합니다.

수정하려는 경우…	이 명령 사용…
외부 엔진	'가상 FPolicy 정책 외부 - 엔진 수정'

이벤트	'SVM FPolicy 정책 이벤트 수정
범위	'SVM FPolicy 정책 범위 수정'
영구 저장소	`vserver fpolicy persistent-store modify`
정책	'가상 서버 FPolicy 정책 수정'

에 대한 자세한 내용은 `vserver fpolicy policy` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP FPolicy 정책 활성화 또는 비활성화

구성이 완료된 후 FPolicy 정책을 활성화할 수 있습니다. 정책을 설정하면 우선 순위가 설정되고 정책에 대한 파일 액세스 모니터링이 시작됩니다. 정책에 대한 파일 액세스 모니터링을 중지하려면 FPolicy 정책을 사용하지 않도록 설정할 수 있습니다.

시작하기 전에

FPolicy 정책을 활성화하기 전에 FPolicy 구성을 완료해야 합니다.

이 작업에 대해

- 우선 순위는 SVM(스토리지 가상 시스템)에서 여러 정책이 활성화되어 있고 둘 이상의 정책이 동일한 파일 액세스 이벤트에 가입되어 있는 경우에 사용됩니다.
- 네이티브 엔진 구성을 사용하는 정책은 정책을 설정할 때 할당된 시퀀스 번호에 관계없이 다른 엔진에 대한 정책보다 우선 순위가 높습니다.
- FPolicy 정책의 우선순위를 변경하려면 정책을 사용하지 않도록 설정한 다음 새 시퀀스 번호를 사용하여 다시 사용하도록 설정해야 합니다.

단계

1. 적절한 작업을 수행합니다.

원하는 작업	다음 명령을 입력합니다…
FPolicy 정책을 사용하십시오	'vserver FPolicy enable-vserver-name vserver_name-policy-name policy_name-sequence-number integer'
FPolicy 정책을 사용하지 않도록 설정합니다	'vserver FPolicy disable-vserver-name vserver_name-policy-name policy_name'

FPolicy 구성에 대한 정보를 표시합니다

ONTAP FPolicy show 명령에 대해 알아보세요

FPolicy 구성에 대한 정보를 표시하여 '방법' 명령의 작동 방식을 이해하는 것이 좋습니다.

추가 매개 변수 없이 'show' 명령을 실행하면 요약 형식으로 정보가 표시됩니다. 또한 모든 'show' 명령은 'instance', '-

fields'라는 상호 배타적인 두 개의 선택적 매개 변수를 갖습니다.

'-instance' 매개 변수를 'show' 명령과 함께 사용하면 명령 출력에 자세한 정보가 목록 형식으로 표시됩니다. 경우에 따라 상세 출력 시간이 오래 걸리고 필요한 것보다 많은 정보를 포함할 수 있습니다. '-fields"fieldname[,fieldname…]' 파라미터를 사용하면 지정한 필드에 대한 정보만 표시하도록 출력을 사용자 정의할 수 있습니다. '?'를 입력하여 지정할 수 있는 필드를 식별할 수 있습니다 '-fields' 파라미터 뒤에

> 필드 매개 변수가 있는 'show' 명령의 출력에는 요청된 필드와 관련된 다른 관련 필드와 필수 필드가 표시될 수 있습니다.

모든 'show' 명령에는 출력을 필터링하고 명령 출력에 표시되는 정보의 범위를 좁힐 수 있도록 하는 하나 이상의 선택적 매개 변수가 있습니다. '?'를 입력하여 명령에 사용할 수 있는 선택적 매개 변수를 식별할 수 있습니다 'show' 명령 뒤에.

'show' 명령은 UNIX 스타일 패턴과 와일드카드를 지원하여 명령 매개 변수 인수의 여러 값을 일치시킬 수 있습니다. 예를 들어 값을 지정할 때 와일드카드 연산자(*), NOT 연산자(!), OR 연산자(|), 범위 연산자(integer…integer), 보다 작음 연산자(<), 보다 큼 연산자(>), 보다 작거나 같음 연산자(<=) 및 보다 크거나 같음 연산자(>=)를 사용할 수 있습니다.

UNIX 스타일 패턴 및 와일드카드 사용에 대한 자세한 내용은 을 참조하십시오 ONTAP 명령줄 인터페이스 사용.

ONTAP의 **FPolicy** 구성에 대한 정보를 표시하기 위한 명령입니다

FPolicy show 명령을 사용하면 외부 엔진, 이벤트, 범위, 정책에 대한 정보를 비롯하여 FPolicy 구성에 대한 정보를 표시할 수 있습니다.

FPolicy에 대한 정보를 표시하려면…	이 명령 사용…
외부 엔진	'vserver FPolicy external-engine show'
이벤트	'vserver FPolicy event show'
범위	'SVM FPolicy 정책 범위 표시
정책	'vserver FPolicy show'

에 대한 자세한 내용은 `vserver fpolicy policy` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP FPolicy 정책 상태에 대한 정보 표시

FPolicy 정책 상태에 대한 정보를 표시하여 정책이 사용되는지 여부, 외부 엔진이 사용하도록 구성되었는지, 정책의 시퀀스 번호가 무엇인지, FPolicy 정책이 어떤 스토리지 가상 머신(SVM)과 연결되어 있는지 확인할 수 있습니다.

이 작업에 대해

매개 변수를 지정하지 않으면 다음 정보가 표시됩니다.

- SVM 이름
- 정책 이름입니다

- 정책 시퀀스 번호입니다
- 정책 상태입니다

클러스터 또는 특정 SVM에 구성된 FPolicy 정책의 정책 상태에 대한 정보를 표시할 뿐만 아니라 명령 매개 변수를 사용하여 명령 출력을 다른 기준으로 필터링할 수 있습니다.

나열된 정책에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 지정할 수 있습니다. 또는 '-fields' 매개 변수를 사용하여 명령 출력 또는 '-fields?'에 표시된 필드만 표시할 수 있습니다 사용할 수 있는 필드를 결정합니다.

단계

1. 적절한 명령을 사용하여 FPolicy 정책 상태에 대한 필터링된 정보를 표시합니다.

정책에 대한 상태 정보를 표시하려면…	명령 입력…
클러스터에서	'vserver FPolicy show'
지정한 상태를 가진 사용자	'vserver FPolicy show -status{on
off}'	SVM을 지정합니다
'vserver FPolicy show -vserver vserver_name'을 선택합니다	지정된 정책 이름을 가진
'vserver FPolicy show-policy-name policy_name'입니다	지정된 외부 엔진을 사용합니다

예

다음 예는 클러스터의 FPolicy 정책에 대한 정보를 표시합니다.

```
cluster1::> vserver fpolicy show
                                        Sequence
Vserver              Policy Name          Number  Status      Engine
-------------------- -------------------- --------  ---------   ---------
FPolicy              cserver_policy       -         off         eng1
vs1.example.com      v1p1                 -         off         eng2
vs1.example.com      v1p2                 -         off         native
vs1.example.com      v1p3                 -         off         native
vs1.example.com      cserver_policy       -         off         eng1
vs2.example.com      v1p1                 3         on          native
vs2.example.com      v1p2                 1         on          eng3
vs2.example.com      cserver_policy       2         on          eng1
```

활성화된 **ONTAP FPolicy** 정책에 대한 정보 표시

활성화된 FPolicy 정책에 대한 정보를 표시하여 사용자가 사용하도록 구성된 FPolicy 외부 엔진,

정책의 우선순위 및 FPolicy 정책이 연결된 스토리지 가상 시스템(SVM)을 결정할 수 있습니다.

이 작업에 대해

매개 변수를 지정하지 않으면 다음 정보가 표시됩니다.

- SVM 이름
- 정책 이름입니다
- 정책 우선 순위

명령 매개 변수를 사용하여 지정된 기준에 따라 명령의 출력을 필터링할 수 있습니다.

단계

1. 적절한 명령을 사용하여 활성화된 FPolicy 정책에 대한 정보를 표시합니다.

활성화된 정책에 대한 정보를 표시하려면…	명령 입력…
클러스터에서	'vserver FPolicy show-enabled'를 선택합니다
SVM을 지정합니다	'vserver FPolicy show-enabled-vserver vserver_name'을 선택합니다
지정된 정책 이름을 가진	'vserver FPolicy show-enabled-policy-name policy_name'
지정된 시퀀스 번호를 사용하여	'vserver FPolicy show-enabled-priority integer'

예

다음 예는 클러스터에서 활성화된 FPolicy 정책에 대한 정보를 표시합니다.

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

FPolicy 서버 연결을 관리합니다

ONTAP의 외부 **FPolicy** 서버에 연결합니다

파일 처리를 활성화하려면 이전에 연결이 종료된 경우 외부 FPolicy 서버에 수동으로 연결해야 할 수 있습니다. 서버 시간 초과에 도달하거나 일부 오류로 인해 연결이 종료됩니다. 또는 관리자가 수동으로 연결을 종료할 수도 있습니다.

이 작업에 대해

치명적인 오류가 발생하면 FPolicy 서버에 대한 연결을 종료할 수 있습니다. 치명적인 오류를 일으키는 문제를 해결한 후에는 FPolicy 서버에 수동으로 다시 연결해야 합니다.

단계

1. 'vserver FPolicy engine-connect' 명령을 사용하여 외부 FPolicy 서버에 연결하십시오.

   에 대한 자세한 내용은 `vserver fpolicy engine-connect` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 'vserver FPolicy show -engine' 명령을 사용하여 외부 FPolicy 서버가 연결되어 있는지 확인하십시오.

   에 대한 자세한 내용은 `vserver fpolicy show-engine` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP의 외부 FPolicy 서버와 연결 끊기

외부 FPolicy 서버에서 수동으로 연결을 끊어야 할 수도 있습니다. FPolicy 서버에 알림 요청 처리에 문제가 있거나 FPolicy 서버에서 유지 관리를 수행해야 하는 경우 이 방법이 바람직할 수 있습니다.

단계

1. 'vserver FPolicy engine-disconnect' 명령을 사용하여 외부 FPolicy 서버에서 분리하십시오.

   에 대한 자세한 내용은 `vserver fpolicy engine-disconnect` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 'vserver FPolicy show -engine' 명령을 사용하여 외부 FPolicy 서버의 연결이 끊겼는지 확인하십시오.

   에 대한 자세한 내용은 `vserver fpolicy show-engine` "ONTAP 명령 참조입니다"을 참조하십시오.

외부 ONTAP FPolicy 서버에 대한 연결에 대한 정보 표시

클러스터의 외부 FPolicy 서버(FPolicy 서버) 또는 지정된 SVM(스토리지 가상 머신)에 대한 연결에 대한 상태 정보를 표시할 수 있습니다. 이 정보는 어떤 FPolicy 서버가 연결되어 있는지 확인하는 데 도움이 될 수 있습니다.

이 작업에 대해

매개 변수를 지정하지 않으면 다음 정보가 표시됩니다.

- SVM 이름
- 노드 이름
- FPolicy 정책 이름입니다
- FPolicy 서버 IP 주소입니다
- FPolicy 서버 상태입니다
- FPolicy 서버 유형입니다

클러스터 또는 특정 SVM에서 FPolicy 연결에 대한 정보를 표시하는 것 외에도 명령 매개 변수를 사용하여 명령 출력을

다른 기준으로 필터링할 수 있습니다.

나열된 정책에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 지정할 수 있습니다. 또는 '-fields' 매개 변수를 사용하여 명령 출력에 표시된 필드만 표시할 수 있습니다. 당신은 `?'를 입력할 수 있습니다 '-fields' 매개 변수 뒤에 사용할 수 있는 필드를 찾습니다.

단계

1. 적절한 명령을 사용하여 노드와 FPolicy 서버 사이의 연결 상태에 대한 필터링된 정보를 표시합니다.

FPolicy 서버에 대한 연결 상태 정보를 표시하려면…	입력…
지정할 수 있습니다	'vserver FPolicy show -engine-server ip_address'
특정 SVM용	'vserver FPolicy show -engine -vserver vserver_name'
지정된 정책에 첨부되어 있습니다	'vserver FPolicy show-engine-policy-name policy_name'입니다
지정한 서버 상태를 사용합니다	'vserver FPolicy show-engine-server-status' 서버 상태는 다음 중 하나일 수 있습니다. • '연결됨' • "연결 안 됨" • 연결 중 • 연결 중
지정된 유형의 경우	'vserver FPolicy show-engine-server-type type' FPolicy 서버 유형은 다음 중 하나일 수 있습니다. • 1차 • 2차

지정된 이유로 연결이 끊어졌습니다	'vserver FPolicy show-engine-disconnect-reason text'를 참조하십시오 연결 해제는 여러 가지 이유로 인해 발생할 수 있습니다. 연결을 끊는 일반적인 이유는 다음과 같습니다. • CLI로부터 dissconnect 명령을 받았습니다 • FPolicy 서버에서 알림 응답을 구문 분석하는 동안 오류가 발생했습니다 • FPolicy 핸드셰이크를 실패했습니다 • SL 핸드셰이크가 실패했습니다 • FPolicy 서버에 대한 TCP 연결이 실패했습니다 • FPolicy 서버로부터 받은 화면 응답 메시지가 유효하지 않습니다

예

이 예는 SVM의 FPolicy 서버에 대한 외부 엔진 연결 정보를 표시합니다. vs1.example.com:

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                              Server-       Server-
Vserver          Policy    Node          Server      status        type
---------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1   node1        10.1.1.2      connected     primary
vs1.example.com policy1   node1        10.1.1.3      disconnected  primary
vs1.example.com policy1   node2        10.1.1.2      connected     primary
vs1.example.com policy1   node2        10.1.1.3      disconnected  primary
```

이 예는 연결된 FPolicy 서버에 대한 정보만 표시합니다.

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver          policy-name server
---------- ---------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2
```

ONTAP FPolicy 패스스루-읽기 연결 상태에 대한 정보 표시

클러스터에서 FPolicy 패스스루 읽기 연결 상태에 대한 정보를 외부 FPolicy 서버(FPolicy 서버)에 표시하거나 지정된 SVM(스토리지 가상 머신)에 대한 정보를 표시할 수 있습니다. 이 정보를 통해 패스스루 읽기 데이터 연결이 있는 FPolicy 서버와 패스스루 읽기 연결이 끊어진 FPolicy 서버를 확인할 수 있습니다.

이 작업에 대해

매개 변수를 지정하지 않으면 다음 정보가 표시됩니다.

- SVM 이름
- FPolicy 정책 이름입니다
- 노드 이름
- FPolicy 서버 IP 주소입니다
- FPolicy 패스스루 - 읽기 연결 상태입니다

클러스터 또는 특정 SVM에서 FPolicy 연결에 대한 정보를 표시하는 것 외에도 명령 매개 변수를 사용하여 명령 출력을 다른 기준으로 필터링할 수 있습니다.

나열된 정책에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 지정할 수 있습니다. 또는 '-fields' 매개 변수를 사용하여 명령 출력에 표시된 필드만 표시할 수 있습니다. 당신은 `?'를 입력할 수 있습니다 '-fields' 매개 변수 뒤에 사용할 수 있는 필드를 찾습니다.

단계

1. 적절한 명령을 사용하여 노드와 FPolicy 서버 사이의 연결 상태에 대한 필터링된 정보를 표시합니다.

연결 상태 정보를 표시하려면…	명령 입력…
FPolicy 패스스루 - 클러스터에 대한 읽기 연결 상태입니다	'vserver FPolicy show-passthrough-read-connection’을 선택합니다
FPolicy 패스스루 - 지정된 SVM에 대한 연결 상태를 읽습니다	'vserver FPolicy show -passthrough -read-connection -vserver vserver vserver_name’을 선택합니다
FPolicy 패스스루 - 지정된 정책에 대한 연결 상태를 읽습니다	'vserver FPolicy show-passthrough-read-connection-policy-name policy_name’을 선택합니다
지정된 정책에 대한 FPolicy 패스쓰루 세부 연결 상태입니다	'vserver FPolicy show-passthrough-read-connection-policy-name policy_name-instance'
FPolicy 패스스루 - 지정한 상태에 대한 연결 상태를 읽습니다	'vserver FPolicy show-passthrough-read-connection-policy-name policy_name-server-status' 서버 상태는 다음 중 하나일 수 있습니다. • '연결됨' • "연결 안 됨"

예

다음 명령을 실행하면 클러스터의 모든 FPolicy 서버에서 패스스루 읽기 연결에 대한 정보가 표시됩니다.

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                          FPolicy           Server
Vserver          Policy Name   Node       Server            Status
---------------  ------------ ---------- -----------------
--------------
vs2.example.com  pol_cifs_2    FPolicy-01   2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
```

다음 명령을 실행하면 ""pol_cifs_1" 정책에 구성된 FPolicy 서버의 패스스루 읽기 연결에 대한 자세한 정보가 표시됩니다.

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                        Node: FPolicy-01
                                     Vserver: vs1.example.com
                                      Policy: pol_cifs_1
                                      Server: 1.1.1.1
                Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

보안 추적을 사용하여 액세스를 확인합니다

ONTAP 보안 추적에 대해 알아보세요

ONTAP에 SVM(스토리지 가상 머신)의 SMB 및 NFS 서버가 작업 수행을 위한 클라이언트 또는 사용자의 요청을 허용하거나 거부하는 이유에 대한 정보를 기록하도록 권한 추적 필터를 추가할 수 있습니다. 이 기능은 파일 액세스 보안 체계가 적절한지 확인하거나 파일 액세스 문제를 해결하려는 경우에 유용합니다.

보안 추적을 사용하면 SVM에서 SMB 및 NFS를 통해 클라이언트 작업을 감지하는 필터를 구성하고 해당 필터와 일치하는 모든 액세스 검사를 추적할 수 있습니다. 그런 다음 액세스가 허용되거나 거부된 이유를 간단히 요약할 수 있는 추적 결과를 볼 수 있습니다.

SVM의 파일 및 폴더에서 SMB 또는 NFS 액세스에 대한 보안 설정을 확인하거나 액세스 문제가 발생한 경우 필터를 빠르게 추가하여 권한 추적을 설정할 수 있습니다.

다음 목록에서는 보안 추적 작동 방식에 대한 중요한 사실을 간략하게 설명합니다.

- ONTAP는 SVM 레벨에서 보안 추적을 적용합니다.

- 각 수신 요청이 활성화된 보안 추적의 필터링 기준과 일치하는지 확인합니다.
- 추적은 파일 및 폴더 액세스 요청 모두에 대해 수행됩니다.
- 트레이스는 다음 기준에 따라 필터링할 수 있습니다.
  - 클라이언트 IP입니다
  - SMB 또는 NFS 경로입니다
  - Windows 이름입니다
  - Unix 이름입니다
- 요청은 _allowed_and_Denied_access 응답 결과에 대해 스크리닝됩니다.
- 활성화된 추적의 필터링 기준과 일치하는 각 요청은 추적 결과 로그에 기록됩니다.
- 스토리지 관리자는 필터의 시간 초과를 구성하여 필터를 자동으로 해제할 수 있습니다.
- 요청이 여러 필터와 일치하면 가장 높은 인덱스 번호를 가진 필터의 결과가 기록됩니다.
- 스토리지 관리자는 추적 결과 로그의 결과를 인쇄하여 액세스 요청이 허용 또는 거부된 이유를 확인할 수 있습니다.

ONTAP SVM에서 보안 추적 모니터링을 위한 액세스 검사 유형

파일 또는 폴더에 대한 액세스 검사는 여러 기준에 따라 수행됩니다. Security Trace는 이러한 모든 기준에 대한 작업을 모니터링합니다.

보안 추적 모니터가 사용하는 액세스 검사의 유형은 다음과 같습니다.

- 볼륨 및 qtree 보안 스타일
- 작업이 요청된 파일 및 폴더가 포함된 파일 시스템의 효과적인 보안
- 사용자 매핑
- 공유 수준 권한
- 내보내기 수준 권한
- 파일 수준 권한
- 스토리지 레벨 액세스 가드 보안

ONTAP SVM에서 보안 추적을 생성할 때의 고려 사항

SVM(스토리지 가상 머신)에 보안 추적을 생성할 때는 몇 가지 사항을 염두에 두어야 합니다. 예를 들어 추적을 만들 수 있는 프로토콜, 지원되는 보안 스타일 및 최대 활성 트레이스 수를 알아야 합니다.

- SVM에서는 보안 추적만 생성할 수 있습니다.
- 각 보안 추적 필터 항목은 SVM에 따라 다릅니다.

  트레이스를 실행할 SVM을 지정해야 합니다.

- SMB 및 NFS 요청에 대한 권한 추적 필터를 추가할 수 있습니다.

- 추적 필터를 생성할 SVM에서 SMB 또는 NFS 서버를 설정해야 합니다.
- NTFS, UNIX, 혼합 보안 스타일 볼륨 및 Qtree에 상주하는 파일 및 폴더에 대한 보안 추적을 만들 수 있습니다.
- SVM당 최대 10개의 권한 추적 필터를 추가할 수 있습니다.
- 필터를 만들거나 수정할 때는 필터 인덱스 번호를 지정해야 합니다.

  필터는 인덱스 번호 순으로 간주됩니다. 인덱스 번호가 더 높은 필터의 조건은 인덱스 번호가 더 낮은 기준 앞에 고려됩니다. 추적 중인 요청이 활성화된 여러 필터의 조건과 일치하면 인덱스 번호가 가장 높은 필터만 트리거됩니다.

- 보안 추적 필터를 만들고 활성화한 후에는 클라이언트 시스템에서 일부 파일 또는 폴더 요청을 수행하여 추적 필터가 추적 결과 로그를 캡처하고 기록할 수 있는 활동을 생성해야 합니다.
- 파일 액세스 확인 또는 문제 해결 목적으로만 권한 추적 필터를 추가해야 합니다.

  권한 추적 필터를 추가하면 컨트롤러 성능에 약간의 영향을 줄 수 있습니다.

  확인 또는 문제 해결 작업을 완료하면 모든 권한 추적 필터를 비활성화하거나 제거해야 합니다. 또한 ONTAP에서 로그에 많은 수의 추적 결과를 전송하지 않도록 선택한 필터링 조건은 가능한 한 구체해야 합니다.

보안 추적을 수행합니다

ONTAP 보안 추적을 수행하는 방법을 알아보세요

보안 추적을 수행하려면 보안 추적 필터를 만들고, 필터 기준을 확인하고, 필터 기준과 일치하는 SMB 또는 NFS 클라이언트에 액세스 요청을 생성하고, 결과를 확인해야 합니다.

보안 필터를 사용하여 추적 정보를 캡처한 후 필터를 수정하고 다시 사용하거나 더 이상 필요하지 않은 경우 비활성화할 수 있습니다. 필터 추적 결과를 보고 분석한 후 더 이상 필요하지 않은 경우 삭제할 수 있습니다.

ONTAP SVM에서 보안 추적 필터 생성

SVM(스토리지 가상 머신)에서 SMB 및 NFS 클라이언트 작업을 감지하고 필터와 일치하는 모든 액세스 검사를 추적하는 보안 추적 필터를 생성할 수 있습니다. 보안 추적의 결과를 사용하여 구성을 확인하거나 액세스 문제를 해결할 수 있습니다.

이 작업에 대해

vserver security trace filter create 명령에는 두 가지 필수 매개 변수가 있습니다.

필수 매개변수	설명
'-vserver"vserver_name'	_SVM 이름 _ 보안 추적 필터를 적용할 파일 또는 폴더가 포함된 SVM의 이름입니다.
인덱스 인덱스 인덱스 인덱스 번호	_필터 인덱스 번호 _ 필터에 적용할 인덱스 번호입니다. SVM당 최대 10개의 추적 필터로 제한됩니다. 이 매개 변수에 허용되는 값은 1 ~ 10입니다.

여러 선택적 필터 매개 변수를 사용하여 보안 추적 필터를 사용자 지정하여 보안 추적에서 생성된 결과를 좁힐 수 있습니다.

필터 매개 변수	설명
'-client-ip"ip_Address'	이 필터는 사용자가 SVM에 액세스하는 데 사용할 IP 주소를 지정합니다.
길의 길	이 필터는 권한 추적 필터를 적용할 경로를 지정합니다. '-path'의 값은 다음 형식 중 하나를 사용할 수 있습니다. • 공유 또는 내보내기의 루트에서 시작하는 전체 경로입니다 • 공유의 루트에 상대적인 부분 경로입니다 경로 값에 NFS 스타일 디렉토리 UNIX 스타일 디렉토리 구분 기호를 사용해야 합니다.
'-windows-name"win_user_name' 또는 '-unix-name"unix_user_name'	추적할 액세스 요청의 Windows 사용자 이름 또는 UNIX 사용자 이름을 지정할 수 있습니다. 사용자 이름 변수는 대/소문자를 구분하지 않습니다. 동일한 필터에 Windows 사용자 이름과 UNIX 사용자 이름을 모두 지정할 수는 없습니다. SMB 및 NFS 액세스 이벤트를 추적할 수 있더라도 UNIX 보안 스타일 데이터가 혼합된 데이터에 대한 액세스 검사를 수행할 때 매핑된 UNIX 사용자 및 매핑된 UNIX 사용자 그룹이 사용될 수 있습니다.
'-trace-allow'{'yes'	'no'}
거부 이벤트 추적은 항상 보안 추적 필터에 대해 활성화됩니다. 선택적으로 허용 이벤트를 추적할 수 있습니다. 허용 이벤트를 추적하려면 이 매개변수를 "예"로 설정합니다.	``사용'{'사용'
'사용 안 함'}	보안 추적 필터를 사용하거나 사용하지 않도록 설정할 수 있습니다. 기본적으로 보안 추적 필터는 활성화되어 있습니다.
시간 사용 정수	필터 시간 초과를 지정하면 필터 시간 초과가 해제됩니다.

단계

1. 보안 추적 필터 만들기:

   'vserver security trace filter create-vserver vserver_name-index index_numberfilter_parameters'

   filter_parameters는 선택 필터 매개변수 목록입니다.

   에 대한 자세한 내용은 `vserver security trace filter create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 보안 추적 필터 항목을 확인합니다.

   'vserver security trace filter show -vserver vserver_name -index index index_number'

예

다음 명령을 실행하면 IP 주소 10.10.7에서 공유 경로 '\\server\share1\dir1\dir2\file.txt'를 사용하여 파일에 액세스하는 모든 사용자에 대한 보안 추적 필터가 생성됩니다. 이 필터는 '-path' 옵션을 위한 전체 경로를 사용합니다. 데이터에 액세스하는 데 사용되는 클라이언트의 IP 주소는 10.10.7입니다. 필터는 30분 후에 시간 초과됩니다.

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
```

다음 명령을 실행하면 '-path' 옵션에 대한 상대 경로를 사용하여 보안 추적 필터를 만듭니다. 이 필터는 ""Joe""라는 이름의 Windows 사용자에 대한 액세스를 추적합니다. Joe가 공유 경로 '\\server\share1\dir1\dir2\file.txt'를 사용하여 파일에 액세스하고 있습니다. 필터 추적은 이벤트를 허용 및 거부합니다.

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                              Vserver: vs1
                         Filter Index: 2
             Client IP Address to Match: -
                                 Path: /dir1/dir2/file.txt
                   Windows User Name: mydomain\joe
                      UNIX User Name: -
                   Trace Allow Events: yes
                      Filter Enabled: enabled
              Minutes Filter is Enabled: 60
```

ONTAP SVM의 보안 추적 필터에 대한 정보 표시

SVM(스토리지 가상 시스템)에 구성된 보안 추적 필터에 대한 정보를 표시할 수 있습니다. 이를 통해 각 필터 추적의 액세스 이벤트 유형을 확인할 수 있습니다.

단계

1. 'vserver security trace filter show' 명령을 사용하여 보안 추적 필터 항목에 대한 정보를 출력한다.

   에 대한 자세한 내용은 `vserver security trace filter show` "ONTAP 명령 참조입니다"을

참조하십시오.

예

다음 명령을 실행하면 SVM VS1 의 모든 보안 추적 필터에 대한 정보가 표시됩니다.

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

ONTAP SVM에서 보안 추적 결과 표시

보안 추적 필터와 일치하는 파일 작업에 대해 생성된 보안 추적 결과를 표시할 수 있습니다. 이 결과를 사용하여 파일 액세스 보안 구성을 검증하거나 SMB 및 NFS 파일 액세스 문제를 해결할 수 있습니다.

시작하기 전에

활성화된 보안 추적 필터가 있어야 하며 보안 추적 결과를 생성하려면 보안 추적 필터와 일치하는 SMB 또는 NFS 클라이언트에서 작업을 수행해야 합니다.

이 작업에 대해

모든 보안 추적 결과의 요약을 표시하거나 선택적 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다. 이 기능은 보안 추적 결과에 많은 수의 레코드가 포함된 경우에 유용합니다.

선택적 매개 변수를 지정하지 않으면 다음 항목이 표시됩니다.

- 스토리지 가상 시스템(SVM) 이름
- 노드 이름
- Security Trace Index Number이다
- 보안 스타일
- 경로
- 이유
- 사용자 이름입니다

  추적 필터 구성 방법에 따라 사용자 이름이 표시됩니다.

필터가 구성된 경우…	그러면…
UNIX 사용자 이름을 사용합니다	보안 추적 결과에 UNIX 사용자 이름이 표시됩니다.

Windows 사용자 이름을 사용합니다	보안 추적 결과에 Windows 사용자 이름이 표시됩니다.
사용자 이름이 없습니다	보안 추적 결과에 Windows 사용자 이름이 표시됩니다.

선택적 매개 변수를 사용하여 출력을 사용자 지정할 수 있습니다. 명령 출력에 반환되는 결과의 범위를 좁히는 데 사용할 수 있는 선택적 매개 변수 중 몇 가지는 다음과 같습니다.

선택적 매개 변수입니다	설명
``필드''필드_이름, …	선택한 필드에 출력을 표시합니다. 이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.
'-인스턴스'	보안 추적 이벤트에 대한 자세한 정보를 표시합니다. 이 매개 변수를 다른 선택적 매개 변수와 함께 사용하면 특정 필터 결과에 대한 자세한 정보를 표시할 수 있습니다.
'-node' node_name'입니다	지정된 노드의 이벤트에 대한 정보만 표시합니다.
'-vserver"vserver_name'	지정된 SVM의 이벤트에 대한 정보만 표시합니다.
인덱스 정수	지정된 인덱스 번호에 해당하는 필터의 결과로 발생한 이벤트에 대한 정보를 표시합니다.
'-client-ip"ip_address'	지정된 클라이언트 IP 주소에서 파일 액세스로 인해 발생한 이벤트에 대한 정보를 표시합니다.
길의 길	지정된 경로에 대한 파일 액세스 결과로 발생한 이벤트에 대한 정보를 표시합니다.
'-user-name"user_name'입니다	지정된 Windows 또는 UNIX 사용자가 파일에 액세스한 결과로 발생한 이벤트에 대한 정보를 표시합니다.
'-security-style"security_style'	지정된 보안 스타일이 있는 파일 시스템에서 발생한 이벤트에 대한 정보를 표시합니다.

기타 선택적 매개 변수에 대한 자세한 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

단계

1. 'vserver security trace trace trace -result show' 명령어를 사용해 보안추적 필터 결과를 출력한다.

   'vserver security trace trace-result show-user-name domain\user'를 선택합니다

```
Vserver: vs1

Node     Index   Filter Details          Reason
-------- ------- ---------------------  ----------------------------
node1    3       User:domain\user       Access denied by explicit ACE
                 Security Style:mixed
                 Path:/dir1/dir2/

node1    5       User:domain\user       Access denied by explicit ACE
                 Security Style:unix
                 Path:/dir1/
```

ONTAP SVM에서 보안 추적 필터 수정

추적할 액세스 이벤트를 결정하는 데 사용되는 선택적 필터 매개 변수를 변경하려면 기존 보안 추적 필터를 수정할 수 있습니다.

이 작업에 대해

필터가 적용되는 SVM(Storage Virtual Machine) 이름과 필터의 인덱스 번호를 지정하여 수정할 보안 추적 필터를 식별해야 합니다. 모든 선택적 필터 매개 변수를 수정할 수 있습니다.

단계

1. 보안 추적 필터 수정:

   'vserver security trace filter modify -vserver vserver_name -index index_numberfilter_parameters'

   - vserver_name은 보안 추적 필터를 적용할 SVM의 이름입니다.
   - index_number는 필터에 적용할 인덱스 번호입니다. 이 매개 변수에 허용되는 값은 1 ~ 10입니다.
   - filter_parameters는 선택 필터 매개변수 목록입니다.
2. 보안 추적 필터 항목을 확인합니다.

   'vserver security trace filter show -vserver vserver_name -index index index_number'

예

다음 명령을 실행하면 인덱스 번호 1로 보안 추적 필터가 수정됩니다. 이 필터는 IP 주소에서 공유 경로 '\\server\share1\dir1\dir2\file.txt'를 사용하여 파일에 액세스하는 모든 사용자에 대한 이벤트를 추적합니다. 이 필터는 '-path' 옵션을 위한 전체 경로를 사용합니다. 필터 추적은 이벤트를 허용 및 거부합니다.

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                                Vserver: vs1
                           Filter Index: 1
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                     Windows User Name: -
                        UNIX User Name: -
                    Trace Allow Events: yes
                        Filter Enabled: enabled
                 Minutes Filter is Enabled: 60
```

ONTAP SVM에서 보안 추적 필터 삭제

보안 추적 필터 항목이 더 이상 필요하지 않으면 삭제할 수 있습니다. SVM(스토리지 가상 시스템)당 최대 10개의 보안 추적 필터를 사용할 수 있으므로 불필요한 필터를 삭제하면 최대 한도까지 도달했을 때 새 필터를 생성할 수 있습니다.

이 작업에 대해

삭제할 보안 추적 필터를 고유하게 식별하려면 다음을 지정해야 합니다.

- 트레이스 필터가 적용된 SVM의 이름입니다
- 추적 필터의 필터 인덱스 번호입니다

단계

1. 삭제할 보안 추적 필터 항목의 필터 인덱스 번호를 식별합니다.

   'vserver security trace filter show -vserver vserver_name'

   'vserver security trace filter show -vserver vs1'이 표시됩니다

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        1    -            /dir1/dir2/file.txt          yes      -
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

2. 이전 단계의 필터 인덱스 번호 정보를 사용하여 필터 항목을 삭제합니다.

   'vserver security trace filter delete -vserver vserver_name -index index index_number'

'vserver security trace filter delete - vserver vs1-index 1'

3. 보안 추적 필터 항목이 삭제되었는지 확인합니다.

   'vserver security trace filter show -vserver vserver_name'

   'vserver security trace filter show -vserver vs1'이 표시됩니다

```
Vserver   Index   Client-IP            Path             Trace-Allow
Windows-Name
--------- -----  -----------  ----------------------   -----------
-------------
vs1         2    -            /dir3/dir4/                  no
mydomain\joe
```

ONTAP SVM에서 보안 추적 레코드 삭제

필터 추적 레코드를 사용하여 파일 액세스 보안을 확인하거나 SMB 또는 NFS 클라이언트 액세스 문제를 해결하면 보안 추적 로그에서 보안 추적 레코드를 삭제할 수 있습니다.

이 작업에 대해

보안 추적 레코드를 삭제하려면 먼저 레코드의 시퀀스 번호를 알아야 합니다.

> 각 SVM(스토리지 가상 머신)에는 최대 128개의 추적 레코드를 저장할 수 있습니다. SVM에서 최대값을 선택하면 새 트레이스 레코드가 추가될 때 가장 오래된 트레이스 레코드가 자동으로 삭제됩니다. 이 SVM에서 트레이스 레코드를 수동으로 삭제하지 않을 경우 최대 한도에 도달한 후 ONTAP에서 가장 오래된 트레이스 결과를 자동으로 삭제하여 새 결과를 얻을 수 있는 공간을 만들 수 있습니다.

단계

1. 삭제할 레코드의 시퀀스 번호를 식별합니다.

   'vserver security trace trace -result show -vserver vserver_name -instance'

2. 보안 추적 레코드를 삭제합니다.

   'vserver security trace trace -result delete -node node_name -vserver vserver_name -seqnum integer'

   'vserver security trace trace-result delete-vserver vs1-node node1-seqnum 999'

   - '-node "node_name'은 삭제하려는 권한 추적 이벤트가 발생한 클러스터 노드의 이름입니다.

     필수 매개 변수입니다.

   - '-vserver"vserver_name'은 삭제할 권한 추적 이벤트가 발생한 SVM의 이름입니다.

     필수 매개 변수입니다.

   - '-seqnum' 정수 는 삭제하려는 로그 이벤트의 시퀀스 번호입니다.

필수 매개 변수입니다.

ONTAP SVM의 모든 보안 추적 레코드 삭제

기존 보안 추적 레코드를 유지하지 않으려면 한 번의 명령으로 노드의 모든 레코드를 삭제할 수 있습니다.

단계

1. 모든 보안 추적 레코드 삭제:

   'vserver security trace trace -result delete -node node_name -vserver vserver_name *'

   - '-node "node_name'은 삭제하려는 권한 추적 이벤트가 발생한 클러스터 노드의 이름입니다.
   - '-vserver"vserver_name'은 삭제할 권한 추적 이벤트가 발생한 SVM(스토리지 가상 시스템)의 이름입니다.

ONTAP 보안 추적 결과 해석

보안 추적 결과는 요청이 허용 또는 거부된 이유를 제공합니다. 출력 액세스 허용 또는 거부 이유와 액세스가 허용되거나 거부된 액세스 확인 경로 내의 위치를 조합하여 결과를 표시합니다. 결과를 사용하여 작업을 격리하고 작업이 허용되지 않는 이유를 식별할 수 있습니다.

결과 유형 및 필터 세부 정보 목록에 대한 정보 찾기

명령에서 보안 추적 결과에 포함될 수 있는 결과 형식 및 필터 세부 정보 목록을 찾을 수 `vserver security trace trace-result show` 있습니다. 에 대한 자세한 내용은 `vserver security trace trace-result show` "ONTAP 명령 참조입니다"을 참조하십시오.

의 출력 예 `Reason` 의 필드 `Allow` 결과 유형

다음은 추적 결과 로그에 나타나는 "Reason" 필드의 출력 예입니다. 결과 유형은 "Allow"입니다.

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

의 출력 예 `Reason` 의 필드 `Allow` 결과 유형

다음은 추적 결과 로그에 나타나는 "Reason" 필드의 출력 예입니다. 결과 유형은 "eny"입니다.

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

의 출력 예 `Filter details` 필드에 입력합니다

다음은 필터 기준과 일치하는 파일 및 폴더를 포함하는 파일 시스템의 효과적인 보안 스타일을 나열하는 추적 결과 로그의 "필터 세부 정보" 필드의 출력 예입니다.

```
Security Style: MIXED and ACL
```

ONTAP SVM에 대한 추가 정보를 찾을 수 있는 곳

SMB 클라이언트 액세스를 성공적으로 테스트한 후에는 고급 SMB 구성을 수행하거나 SAN 액세스를 추가할 수 있습니다. NFS 클라이언트 액세스를 성공적으로 테스트한 후 고급 NFS 구성을 수행하거나 SAN 액세스를 추가할 수 있습니다. 프로토콜 액세스가 완료되면 SVM의 루트 볼륨을 보호해야 합니다.

SMB 구성

다음을 사용하여 SMB 액세스를 추가로 구성할 수 있습니다.

- "SMB 관리"

  SMB 프로토콜을 사용하여 파일 액세스를 구성 및 관리하는 방법에 대해 설명합니다.

- "NetApp 기술 보고서 4191: clustered Data ONTAP 8.2 Windows 파일 서비스에 대한 모범 사례 가이드를 참조하십시오"

  SMB 구현 및 기타 Windows 파일 서비스 기능에 대한 간략한 개요와 ONTAP의 권장 사항 및 기본 문제 해결 정보를 제공합니다.

- "NetApp 기술 보고서 3740: Data ONTAP의 SMB 2 차세대 CIFS 프로토콜"

  SMB 2 기능, 구성 세부 정보 및 ONTAP에서의 구축에 대해 설명합니다.

NFS 구성

다음을 사용하여 NFS 액세스를 추가로 구성할 수 있습니다.

- "NFS 관리"

  NFS 프로토콜을 사용하여 파일 액세스를 구성 및 관리하는 방법에 대한 설명은 에 나와 있습니다.

- "NetApp 기술 보고서 4067: NFS 모범 사례 및 구축 가이드"

  NFSv3 및 NFSv4 운영 가이드 역할을 하며 NFSv4를 중심으로 ONTAP 운영 체제에 대한 개요를 제공합니다.

- "NetApp 기술 보고서 4668: 이름 서비스 모범 사례 가이드"

  인증을 위해 LDAP, NIS, DNS 및 로컬 사용자 및 그룹 파일을 구성할 때 고려해야 할 사항과 제한 사항, 권장 사항 및 사항에 대한 포괄적인 목록을 제공합니다.

- "NetApp 기술 보고서 4616: ONTAP에서 Microsoft Active Directory와 NFS Kerberos"
- "NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법"

- "NetApp 기술 보고서 3580: NFSv4 향상 및 모범 사례 가이드 Data ONTAP 구축"

  에서는 ONTAP를 실행하는 시스템에 접속된 AIX, Linux 또는 Solaris 클라이언트에서 NFSv4 구성 요소를 구축하는 동안 따라야 하는 Best Practice를 설명합니다.

루트 볼륨 보호

SVM에서 프로토콜을 구성한 후에는 루트 볼륨이 보호되는지 확인해야 합니다.

- "데이터 보호"

  NAS 지원 SVM에 대한 NetApp의 모범 사례인 SVM 루트 볼륨을 보호하기 위해 로드 공유 미러를 생성하는 방법에 대해 설명합니다. 또한, 로드 공유 미러에서 SVM 루트 볼륨을 프로모션하여 볼륨 장애 또는 손실로부터 빠르게 복구하는 방법을 설명합니다.

System Manager로 암호화를 관리합니다

소프트웨어 기반 암호화를 사용하여 **ONTAP** 클러스터에 저장된 데이터를 암호화합니다**.**

볼륨 암호화를 사용하여 기본 장치를 용도 변경, 반환, 위치 변경 또는 도난 당한 경우 볼륨 데이터를 읽을 수 없도록 합니다. 볼륨 암호화는 특수 디스크가 필요하지 않으며 모든 HDD 및 SSD와 함께 작동합니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 소프트웨어 수준 암호화를 활성화합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

볼륨 암호화에는 키 관리자가 필요합니다. System Manager를 사용하여 Onboard Key Manager를 구성할 수 있습니다. 외부 키 관리자를 사용할 수도 있지만 먼저 ONTAP CLI를 사용하여 설정해야 합니다.

키 관리자를 구성한 후에는 새 볼륨이 기본적으로 암호화됩니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. Encryption * 아래에서 Onboard Key Manager를 처음으로 구성하려면 클릭합니다 .
3. 기존 볼륨을 암호화하려면 * 스토리지 > 볼륨 * 을 클릭합니다.
4. 원하는 볼륨에서 를 클릭한 다음 * 편집 * 을 클릭합니다.
5. 암호화 사용 * 을 선택합니다.

자체 암호화 드라이브를 사용하여 **ONTAP** 클러스터에 저장된 데이터를 암호화합니다**.**

기본 장치를 용도 변경, 반환, 위치 변경 또는 도난 당한 경우 로컬 계층의 모든 데이터를 읽을 수 없도록 디스크 암호화를 사용합니다. 디스크 암호화에는 특수한 자체 암호화 HDD 또는 SSD가 필요합니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 하드웨어 수준 암호화를 활성화합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

디스크 암호화에는 키 관리자가 필요합니다. System Manager를 사용하여 온보드 키 관리자를 구성할 수 있습니다. 외부 키 관리자를 사용할 수도 있지만 먼저 ONTAP CLI를 사용하여 설정해야 합니다.

ONTAP에서 자체 암호화 디스크를 감지하면 로컬 계층을 생성할 때 온보드 키 관리자를 구성하라는 메시지가 표시됩니다.

단계

1. Encryption * 아래에서 온보드 키 관리자를 클릭하여 구성합니다.
2. 디스크를 다시 입력해야 한다는 메시지가 나타나면 을 클릭한 다음 * Rekey Disks * 를 클릭합니다.

CLI를 사용하여 암호화를 관리합니다

ONTAP 저장 데이터 암호화에 대해 알아보세요

NetApp은 스토리지 미디어가 용도 변경, 반환, 잘못된 위치 또는 도난된 경우 유휴 데이터를 읽을 수 없도록 소프트웨어 및 하드웨어 기반 암호화 기술을 모두 제공합니다.

- NVE(NetApp Volume Encryption)를 사용하는 소프트웨어 기반 암호화는 한 번에 하나의 볼륨 데이터 암호화를 지원합니다
- NSE(NetApp Storage Encryption)를 사용하는 하드웨어 기반 암호화는 데이터의 쓰기 시 전체 디스크 암호화(FDE)를 지원합니다.

NetApp 볼륨 및 집계 암호화 구성

ONTAP NetApp 볼륨 및 집계 암호화에 대해 알아보세요

NetApp Volume Encryption(NVE)은 유휴 데이터를 한 번에 하나의 볼륨으로 암호화하는 소프트웨어 기반 기술입니다. 스토리지 시스템에서만 액세스할 수 있는 암호화 키를 사용하면 기본 장치를 용도 변경, 반환, 잘못된 위치 변경 또는 도난 당한 경우 볼륨 데이터를 읽을 수 없습니다.

NVE 이해

NVE를 사용하면 메타데이터와 데이터(스냅샷 포함)가 모두 암호화됩니다. 데이터에 대한 액세스는 볼륨별로 고유한 XTS-AES-256 키를 통해 제공됩니다. 외부 키 관리 서버 또는 온보드 키 관리자(OKM)는 노드에 키를 제공합니다.

- 외부 키 관리 서버는 KMIP(Key Management Interoperability Protocol)를 사용하여 노드에 키를 제공하는 스토리지 환경의 타사 시스템입니다. 데이터와 다른 스토리지 시스템에 있는 외부 키 관리 서버를 구성하는 것이 가장 좋습니다.
- Onboard Key Manager는 데이터와 동일한 스토리지 시스템의 노드에 키를 제공하는 기본 제공 툴입니다.

ONTAP 9.7부터 볼륨 암호화(VE) 라이센스가 있고 온보드 키 관리자 또는 외부 키 관리자를 사용하는 경우 애그리게이트 및 볼륨 암호화가 기본적으로 활성화됩니다. VE 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오

"있습니다. 외부 또는 온보드 키 관리자를 구성할 때마다 새로운 애그리게이트 및 완전히 새로운 볼륨에 대해 유휴 데이터 암호화를 구성하는 방식이 변경됩니다. 새로운 애그리게이트에 NetApp NAE(Aggregate Encryption)가 기본적으로 사용되도록 설정됩니다. NAE 애그리게이트에 포함되지 않은 새로운 볼륨의 경우 기본적으로 NVE(NetApp Volume Encryption)가 활성화됩니다. 멀티 테넌트(multi-tenant) 키 관리를 사용하여 데이터 스토리지 가상 시스템(SVM)을 자체 키 관리자로 구성한 경우, SVM용으로 생성된 볼륨은 NVE로 자동으로 구성됩니다.

새 볼륨이나 기존 볼륨에서 암호화를 활성화할 수 있습니다. NVE는 중복제거, 압축을 비롯한 광범위한 스토리지 효율성 기능을 지원합니다. ONTAP 9.14.1부터 가능합니다 기존 SVM 루트 볼륨에서 NVE를 활성화합니다.

SnapLock를 사용하는 경우 비어 있는 새 SnapLock 볼륨에서만 암호화를 활성화할 수 있습니다. 기존 SnapLock 볼륨에서는 암호화를 활성화할 수 없습니다.

NVE는 모든 유형의 애그리게이트(HDD, SSD, 하이브리드, 어레이 LUN), RAID 유형, ONTAP Select를 비롯한 지원되는 모든 ONTAP 구현에서 사용할 수 있습니다. 또한 하드웨어 기반 암호화와 NVE를 사용하여 자체 암호화 드라이브에서 데이터를 "이중 암호화"할 수 있습니다.

NVE가 활성화되면 코어 덤프도 암호화됩니다.

애그리게이트 레벨 암호화

일반적으로 암호화된 모든 볼륨에 고유한 키가 할당됩니다. 볼륨이 삭제되면 키와 함께 삭제됩니다.

ONTAP 9.6부터는 _NetApp 애그리게이트 암호화(NAE)_를 사용하여 암호화할 볼륨의 포함된 애그리게이트에 키를 할당할 수 있습니다. 암호화된 볼륨이 삭제되면 애그리게이트의 키가 유지됩니다. 키가 전체 Aggregate가 삭제된 경우 삭제됩니다.

인라인 또는 백그라운드 애그리게이트 레벨 중복제거를 수행하려는 경우 애그리게이트 레벨 암호화를 사용해야 합니다. 그 외에는 NVE에서 애그리게이트 레벨의 중복제거가 지원되지 않습니다.

ONTAP 9.7부터 볼륨 암호화(VE) 라이센스가 있고 온보드 키 관리자 또는 외부 키 관리자를 사용하는 경우 애그리게이트 및 볼륨 암호화가 기본적으로 활성화됩니다.

NVE 볼륨과 NAE 볼륨이 동일한 애그리게이트에 공존할 수 있습니다. 애그리게이트 레벨 암호화로 암호화된 볼륨은 기본적으로 NAE 볼륨입니다. 볼륨을 암호화할 때 기본값을 재정의할 수 있습니다.

'volume move' 명령을 사용하여 NVE 볼륨을 NAE 볼륨으로 변환하거나 그 반대로 변환할 수 있습니다. NAE 볼륨을 NVE 볼륨으로 복제할 수 있습니다.

NAE 볼륨에서는 'Secure purge' 명령어를 사용할 수 없다.

외부 키 관리 서버를 사용하는 경우

일반적으로 온보드 키 관리자를 사용하는 것이 더 저렴하고 더 편리하긴 하지만, 다음 중 하나라도 해당하는 경우 KMIP 서버를 설치해야 합니다.

- 암호화 키 관리 솔루션은 FIPS(Federal Information Processing Standards) 140-2 또는 KMIP OASIS KMIP 표준을 준수해야 합니다.
- 암호화 키를 중앙 집중식으로 관리하는 다중 클러스터 솔루션이 필요합니다.
- 기업은 인증 키를 시스템 또는 데이터와 다른 위치에 저장하는 추가적인 보안을 필요로 합니다.

외부 키 관리의 범위

외부 키 관리 범위에 따라 주요 관리 서버가 클러스터의 모든 SVM을 보호할지 또는 선택한 SVM에만 안전할지 여부가 결정됩니다.

- 클러스터 범위 _ 를 사용하여 클러스터의 모든 SVM에 대한 외부 키 관리를 구성할 수 있습니다. 클러스터 관리자는 서버에 저장된 모든 키에 액세스할 수 있습니다.
- ONTAP 9.6부터는 _SVM SCOPE_를 사용하여 클러스터의 명명된 SVM에 대한 외부 키 관리를 구성할 수 있습니다. 이는 각 테넌트가 서로 다른 SVM(또는 SVM 세트)을 사용하여 데이터를 제공하는 멀티테넌트 환경에 가장 적합합니다. 지정된 테넌트의 SVM 관리자만 해당 테넌트의 키에 액세스할 수 있습니다.
  - ONTAP 9.17.1부터 다음을 사용할 수 있습니다. 바비칸 KMS 데이터 SVM에 대해서만 NVE 키를 보호합니다.
  - ONTAP 9.10.1부터 를 사용할 수 있습니다 Azure Key Vault 및 Google Cloud KMS 데이터 SVM에 대해서만 NVE 키를 보호합니다. 이 기능은 9.12.0부터 AWS의 KMS에 사용할 수 있습니다.

동일한 클러스터에서 두 범위를 모두 사용할 수 있습니다. SVM용으로 키 관리 서버를 구성한 경우 ONTAP에서는 이러한 서버만 사용하여 키를 보호합니다. 그렇지 않으면 ONTAP는 클러스터에 구성된 키 관리 서버로 키를 보호합니다.

검증된 외부 키 관리자 목록은 에서 확인할 수 있습니다 "NetApp 상호 운용성 매트릭스 툴(IMT)". IMT의 검색 기능에 "Key Manager"라는 용어를 입력하면 이 목록을 확인할 수 있습니다.

> Azure Key Vault 및 AWS KMS와 같은 클라우드 KMS 공급자는 KMIP를 지원하지 않습니다. 따라서 IMT에 나열되지 않습니다.

지원 세부 정보

다음 표에는 NVE 지원 세부사항이 나와 있습니다.

리소스 또는 기능	지원 세부 정보
플랫폼	AES-NI 오프로드 기능이 필요합니다. 해당 플랫폼에서 NVE와 NAE가 지원되는지 확인하려면 HWU(Hardware Universe)를 참조하십시오.

암호화	ONTAP 9.7부터 볼륨 암호화(VE) 라이센스를 추가하고 온보드 또는 외부 키 관리자를 구성한 경우 새로 생성된 애그리게이트 및 볼륨이 기본적으로 암호화됩니다. 암호화되지 않은 Aggregate를 생성해야 하는 경우 다음 명령을 사용합니다. '스토리지 집계 생성-암호화-집계-키 거짓'을 사용합니다 일반 텍스트 볼륨을 만들어야 하는 경우 다음 명령을 사용합니다. 볼륨 만들기-암호화 거짓 다음과 같은 경우 암호화가 기본적으로 활성화되지 않습니다. • VE 라이센스가 설치되지 않았습니다. • 키 관리자가 구성되지 않았습니다. • 플랫폼 또는 소프트웨어는 암호화를 지원하지 않습니다. • 하드웨어 암호화가 활성화됩니다.
ONTAP	모든 ONTAP 구현. Cloud Volumes ONTAP 지원은 ONTAP 9.5 이상에서 제공됩니다.
장치	HDD, SSD, 하이브리드, 어레이 LUN
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
볼륨	데이터 볼륨 및 기존 SVM 루트 볼륨. MetroCluster 메타데이터 볼륨의 데이터는 암호화할 수 없습니다. 9.14.1 이전 버전의 ONTAP에서는 NVE를 통해 SVM 루트 볼륨의 데이터를 암호화할 수 없습니다. ONTAP 9.14.1부터 ONTAP는 를 지원합니다 SVM 루트 볼륨에 NVE.
애그리게이트 레벨 암호화	ONTAP 9.6부터 NVE는 Aggregate 레벨의 암호화(NAE)를 지원합니다. • 인라인 또는 백그라운드 애그리게이트 레벨 중복제거를 수행하려는 경우 애그리게이트 레벨 암호화를 사용해야 합니다. • 집계 수준 암호화 볼륨을 다시 설정할 수 없습니다. • 애그리게이트 레벨 암호화 볼륨에서는 보안 제거가 지원되지 않습니다. • NAE는 데이터 볼륨 외에 SVM 루트 볼륨 및 MetroCluster 메타데이터 볼륨의 암호화를 지원합니다. NAE는 루트 볼륨 암호화를 지원하지 않습니다.
SVM 범위	MetroCluster 는 ONTAP 9.8부터 지원됩니다. ONTAP 9.6부터 NVE는 Onboard Key Manager가 아닌 외부 키 관리에 대해서만 SVM 범위를 지원합니다.

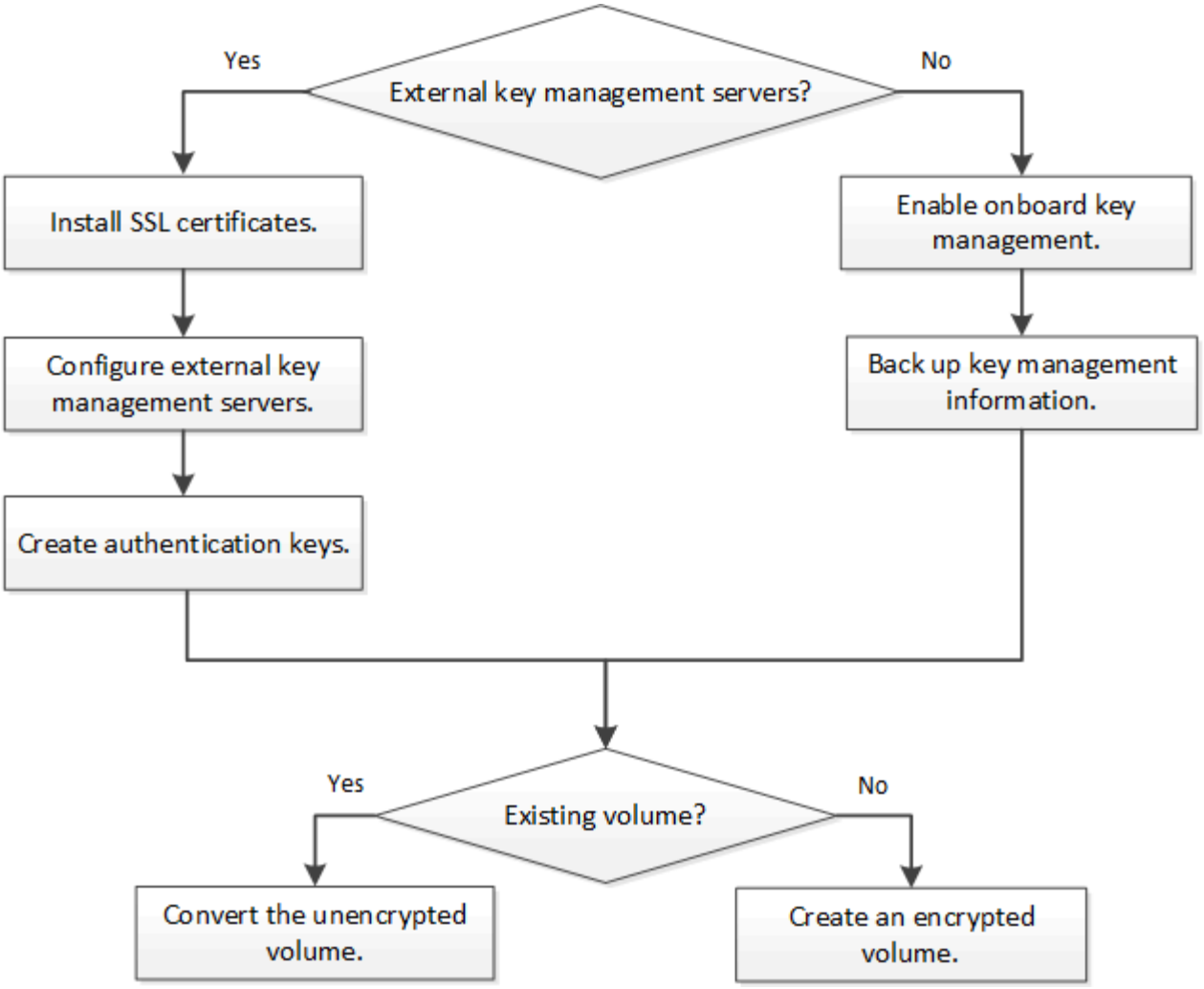
스토리지 효율성	중복제거, 압축, 컴팩션, FlexClone: 클론은 상위 클론에서 클론을 분할한 후에도 상위 클론과 동일한 키를 사용합니다. 를 수행해야 합니다 `volume move` 분할된 클론에서 분할된 클론에는 다른 키가 있습니다.
복제	• 볼륨 복제의 경우 소스 볼륨과 대상 볼륨의 암호화 설정이 다를 수 있습니다. 소스에 대해 암호화를 구성할 수 있고 대상에 대해 구성되지 않을 수도 있습니다. 소스에 구성된 암호화는 대상에 복제되지 않습니다. 소스 및 대상에서 암호화를 수동으로 구성해야 합니다. NVE를 구성합니다및 NVE를 사용하여 볼륨 데이터 암호화을 참조하십시오. • SVM 복제의 경우, 볼륨 암호화를 지원하는 노드가 타겟에 포함되지 않은 경우, 복제가 성공하지만 타겟 볼륨이 암호화되지 않은 한 타겟 볼륨이 자동으로 암호화됩니다. • MetroCluster 구성의 경우 각 클러스터는 구성된 키 서버에서 외부 키 관리 키를 가져옵니다. OKM 키는 구성 복제 서비스에 의해 파트너 사이트에 복제됩니다.
규정 준수	SnapLock 은 새로운 볼륨에 대해서만 규정 준수 및 엔터프라이즈 모드에서 모두 지원됩니다. 기존 SnapLock 볼륨에서는 암호화를 활성화할 수 없습니다.
FlexGroup 볼륨	FlexGroup 볼륨이 지원됩니다. 대상 애그리게이트는 소스 애그리게이트와 볼륨 레벨 또는 애그리게이트 레벨에서 동일한 유형이어야 합니다. ONTAP 9.5부터 FlexGroup 볼륨을 제자리에서 다시 입력하다
7-Mode 전환	7-Mode 전환 툴 3.3부터는 7-Mode 전환 툴 CLI를 사용하여, 클러스터링된 시스템의 NVE 지원 대상 볼륨으로의 복사본 기반 전환을 수행할 수 있습니다.

관련 정보

- "FAQ - NetApp 볼륨 암호화 및 NetApp 애그리게이트 암호화"
- "저장소 집계 생성"

ONTAP NetApp 볼륨 암호화 워크플로

볼륨 암호화를 활성화하려면 키 관리 서비스를 구성해야 합니다. 새 볼륨이나 기존 볼륨에서 암호화를 활성화할 수 있습니다.



"VE 라이센스를 설치해야 합니다" 그리고 NVE로 데이터를 암호화하기 전에 키 관리 서비스를 구성합니다. 라이센스를 설치하기 전에 다음을 수행해야 "ONTAP 버전이 NVE를 지원하는지 확인합니다"합니다.

NVE를 구성합니다

ONTAP 클러스터 버전이 **NVE**를 지원하는지 확인하세요.

라이센스를 설치하기 전에 클러스터 버전이 NVE를 지원하는지 확인해야 합니다. sion 명령을 사용하여 클러스터 버전을 확인할 수 있습니다.

이 작업에 대해

클러스터 버전은 클러스터의 모든 노드에서 실행되는 ONTAP의 가장 낮은 버전입니다.

단계

1. 클러스터 버전이 NVE를 지원하는지 확인

   안절부절부절부절도

   명령 출력에 "no Data at Rest Encryption" 텍스트가 표시되는 경우 또는 에 나와 있지 않은 플랫폼을 사용하는 경우에는 NVE가 지원되지 않습니다 `1Ono-DARE`"지원 세부 정보".

VE 라이센스를 사용하면 클러스터의 모든 노드에서 이 기능을 사용할 수 있습니다. 이 라이센스는 NVE로 데이터를 암호화하기 전에 필요합니다. 에 포함되어 "ONTAP 1 을 참조하십시오"있습니다.

ONTAP One 이전에는 VE 라이센스가 암호화 번들에 포함되어 있었습니다. 암호화 번들이 더 이상 제공되지 않지만 여전히 유효합니다. 현재는 필요하지 않지만 기존 고객은 선택할 수 "ONTAP One으로 업그레이드하십시오"있습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 영업 담당자로부터 VE 라이센스 키를 받았거나 ONTAP One이 설치되어 있어야 합니다.

단계

1. "VE 라이센스가 설치되어 있는지 확인합니다"..

   VE 라이센스 패키지 이름은 입니다 `VE`.

2. 라이센스가 설치되지 않은 경우"System Manager 또는 ONTAP CLI를 사용하여 설치합니다".

외부 키 관리를 구성합니다

ONTAP NetApp Volume Encryption을 사용하여 외부 키 관리 구성에 대해 알아보세요**.**

하나 이상의 외부 키 관리 서버를 사용하여 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 외부 키 관리 서버는 키 관리 상호 운용성 프로토콜(KMIP)을 사용하여 노드에 키를 제공하는 스토리지 환경의 타사 시스템입니다. ONTAP Onboard Key Manager 외에도 여러 외부 키 관리 서버를 지원합니다.

ONTAP 9.10.1부터 다음을 사용할 수 있습니다. Azure Key Vault 또는 Google Cloud Key Manager 서비스 데이터 SVM에 대한 NVE 키를 보호합니다. ONTAP 9.11.1부터 클러스터에서 여러 개의 외부 키 관리자를 구성할 수 있습니다. 보다클러스터형 키 서버 구성 . ONTAP 9.12.0부터 다음을 사용할 수 있습니다. "AWS의 KMS" 데이터 SVM에 대한 NVE 키를 보호합니다. ONTAP 9.17.1부터 OpenStack을 사용할 수 있습니다. 바비칸 KMS 데이터 SVM에 대한 NVE 키를 보호합니다.

ONTAP System Manager를 사용하여 외부 키 관리자를 관리하세요

ONTAP 9.7부터 온보드 키 관리자를 사용하여 인증 및 암호화 키를 저장하고 관리할 수 있습니다. ONTAP 9.13.1부터는 외부 키 관리자를 사용하여 이러한 키를 저장하고 관리할 수도 있습니다.

Onboard Key Manager는 클러스터 내부의 보안 데이터베이스에 키를 저장하고 관리합니다. 범위는 클러스터입니다. 외부 키 관리자는 클러스터 외부에 키를 저장하고 관리합니다. 범위는 클러스터 또는 스토리지 VM일 수 있습니다. 하나 이상의 외부 키 관리자를 사용할 수 있습니다. 다음 조건이 적용됩니다.

- Onboard Key Manager가 활성화된 경우 클러스터 수준에서 외부 키 관리자를 활성화할 수 없지만 스토리지 VM 수준에서 설정할 수 있습니다.
- 외부 키 관리자가 클러스터 레벨에서 활성화된 경우 Onboard Key Manager를 활성화할 수 없습니다.

외부 키 관리자를 사용하는 경우 스토리지 VM 및 클러스터당 최대 4개의 기본 키 서버를 등록할 수 있습니다. 각 기본 키 서버는 최대 3개의 보조 키 서버로 클러스터링할 수 있습니다.

외부 키 관리자를 구성합니다

스토리지 VM에 대한 외부 키 관리자를 추가하려면 스토리지 VM에 대한 네트워크 인터페이스를 구성할 때 선택적 게이트웨이를 추가해야 합니다. 스토리지 VM이 네트워크 경로 없이 생성된 경우 외부 키 관리자에 대한 라우트를 명시적으로 생성해야 합니다. 을 참조하십시오 "LIF(네트워크 인터페이스) 생성".

단계

System Manager의 다양한 위치에서 외부 키 관리자를 구성할 수 있습니다.

1. 외부 키 관리자를 구성하려면 다음 시작 단계 중 하나를 수행합니다.

워크플로우	내비게이션	시작 단계
키 관리자를 구성합니다	• 클러스터 * > * 설정 * 을 선택합니다	보안 * 섹션으로 스크롤합니다. Encryption * 에서 을 선택합니다 . 외부 키 관리자 * 를 선택합니다.
로컬 계층을 추가합니다	• 스토리지 * > * 계층 *	Add Local Tier * 를 선택합니다. "키 관리자 구성" 확인란을 선택합니다. 외부 키 관리자 * 를 선택합니다.
스토리지를 준비합니다	• 대시보드 *	Capacity * 섹션에서 * Prepare Storage * 를 선택합니다. 그런 다음 "키 관리자 구성"을 선택합니다. 외부 키 관리자 * 를 선택합니다.
암호화 구성(스토리지 VM 범위의 키 관리자만 해당)	스토리지 * > * 스토리지 VM *	스토리지 VM을 선택합니다. 설정 * 탭을 선택합니다. 보안 * 아래의 * 암호화 * 섹션에서 을 선택합니다 .

2. 기본 키 서버를 추가하려면 + Add * IP 주소 또는 호스트 이름 * 및 * 포트 * 필드를 선택하고 입력합니다.
3. 기존에 설치된 인증서가 * KMIP Server CA Certificates * 및 * KMIP Client Certificate * 필드에 나열됩니다. 다음 작업 중 하나를 수행할 수 있습니다.
   - 키 관리자에 매핑할 설치된 인증서를 선택하려면 선택합니다 . (여러 서비스 CA 인증서를 선택할 수 있지만 하나의 클라이언트 인증서만 선택할 수 있습니다.)
   - 아직 설치되지 않은 인증서를 추가하고 외부 키 관리자에 매핑하려면 * 새 인증서 추가 * 를 선택합니다.
   - 외부 키 관리자에 매핑하지 않을 설치된 인증서를 삭제하려면 인증서 이름 옆에 있는 을 선택합니다 × .
4. 보조 키 서버를 추가하려면 * 보조 키 서버 * 열에서 * 추가 * 를 선택하고 세부 정보를 제공합니다.
5. 구성을 완료하려면 * 저장 * 을 선택하십시오.

기존 외부 키 관리자를 편집합니다

외부 키 관리자를 이미 구성한 경우 해당 설정을 수정할 수 있습니다.

단계

1. 외부 키 관리자 구성을 편집하려면 다음 시작 단계 중 하나를 수행합니다.

범위	내비게이션	시작 단계
클러스터 범위 외부 키 관리자	• 클러스터 * > * 설정 * 을 선택합니다	보안 * 섹션으로 스크롤합니다. Encryption * 에서 를 ⋮선택한 다음 * Edit External Key Manager * 를 선택합니다.
스토리지 VM 범위 외부 키 관리자	스토리지 * > * 스토리지 VM *	스토리지 VM을 선택합니다. 설정 * 탭을 선택합니다. 보안 * 아래의 * 암호화 * 섹션에서 * 외부 키 관리자 편집 * 을 ⋮선택합니다.

2. 기존 키 서버가 * Key Servers * 표에 나열되어 있습니다. 다음 작업을 수행할 수 있습니다.
   - 를 선택하여 새 키 서버를 추가합니다 + Add .
   - 키 서버의 이름이 들어 있는 표 셀의 끝에서 를 선택하여 키 서버를 ⋮ 삭제합니다. 해당 기본 키 서버와 연결된 보조 키 서버도 구성에서 제거됩니다.

외부 키 관리자를 삭제합니다

볼륨이 암호화되지 않은 경우 외부 키 관리자를 삭제할 수 있습니다.

단계

1. 외부 키 관리자를 삭제하려면 다음 단계 중 하나를 수행합니다.

범위	내비게이션	시작 단계
클러스터 범위 외부 키 관리자	• 클러스터 * > * 설정 * 을 선택합니다	보안 * 섹션으로 스크롤합니다. Encryption * 에서 select를 ⋮선택한 다음 * Delete External Key Manager * 를 선택합니다.
스토리지 VM 범위 외부 키 관리자	스토리지 * > * 스토리지 VM *	스토리지 VM을 선택합니다. 설정 * 탭을 선택합니다. 보안 * 아래의 * 암호화 * 섹션에서 를 ⋮선택한 다음 * 외부 키 관리자 삭제 * 를 선택합니다.

키 관리자 간에 키를 마이그레이션합니다

클러스터에서 여러 키 관리자가 활성화된 경우 키를 한 키 관리자에서 다른 키 관리자로 마이그레이션해야 합니다. 이 프로세스는 System Manager에서 자동으로 완료됩니다.

- Onboard Key Manager 또는 외부 키 관리자가 클러스터 수준에서 활성화되어 있고 일부 볼륨이 암호화된 경우 그런 다음 스토리지 VM 수준에서 외부 키 관리자를 구성할 때 클러스터 수준에서 Onboard Key Manager 또는 외부 키 관리자에서 스토리지 VM 수준의 외부 키 관리자로 키를 마이그레이션해야 합니다. 이 프로세스는 System Manager에서 자동으로 완료됩니다.
- 스토리지 VM에서 암호화 없이 볼륨을 생성한 경우 키를 마이그레이션할 필요가 없습니다.

ONTAP 클러스터에 **SSL** 인증서 설치

클러스터와 KMIP 서버는 KMIP SSL 인증서를 사용하여 서로의 ID를 확인하고 SSL 연결을 설정합니다. KMIP 서버와의 SSL 연결을 구성하기 전에, 클러스터에 대한 KMIP 클라이언트

SSL 인증서와 KMIP 서버의 루트 인증 기관(CA)에 대한 SSL 공용 인증서를 설치해야 합니다.

이 작업에 대해

HA 쌍에서는 두 노드가 동일한 퍼블릭 및 프라이빗 KMIP SSL 인증서를 사용해야 합니다. 동일한 KMIP 서버에 여러 HA 쌍을 연결하는 경우, HA 쌍의 모든 노드는 동일한 공용 및 전용 KMIP SSL 인증서를 사용해야 합니다.

시작하기 전에

- 서버에서 시간을 동기화하여 인증서, KMIP 서버 및 클러스터를 생성해야 합니다.
- 클러스터를 위한 공용 SSL KMIP 클라이언트 인증서를 얻어야 합니다.
- 클러스터를 위한 SSL KMIP 클라이언트 인증서와 관련된 개인 키를 얻어야 합니다.
- SSL KMIP 클라이언트 인증서는 암호로 보호되어 있지 않아야 합니다.
- KMIP 서버의 루트 CA(인증 기관)에 대한 SSL 공용 인증서를 얻어야 합니다.
- MetroCluster 환경에서는 두 클러스터 모두에 동일한 KMIP SSL 인증서를 설치해야 합니다.

> ⓘ 클러스터에 인증서를 설치하기 전이나 후에 KMIP 서버에 클라이언트 및 서버 인증서를 설치할 수 있습니다.

단계

1. 클러스터에 SSL KMIP 클라이언트 인증서를 설치합니다.

   'Security certificate install - vserver admin_svm_name -type client'

   SSL KMIP 공용 및 개인 인증서를 입력하라는 메시지가 표시됩니다.

   'cluster1::> security certificate install -vserver cluster1-type client'

2. KMIP 서버의 루트 CA(인증 기관)에 대한 SSL 공용 인증서를 설치합니다.

   'Security certificate install - vserver admin_svm_name -type server-ca'

   'cluster1::> security certificate install -vserver cluster1-type server-ca'를 입력합니다

관련 정보

- "보안 인증서 설치"

ONTAP 9.6 이상에서 **NVE**에 대한 외부 키 관리 활성화

KMIP 서버를 사용하여 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호합니다. ONTAP 9.6부터 데이터 SVM이 암호화된 데이터에 액세스하는 데 사용하는 키를 보호하기 위해 별도의 외부 키 관리자를 구성하는 옵션이 제공됩니다.

ONTAP 9.11.1부터 기본 키 서버당 최대 3개의 보조 키 서버를 추가하여 클러스터된 키 서버를 생성할 수 있습니다. 자세한 내용은 을 참조하십시오 클러스터링된 외부 키 서버를 구성합니다.

이 작업에 대해

최대 4개의 KMIP 서버를 클러스터나 SVM에 연결할 수 있습니다. 중복성과 재해 복구를 위해 최소 두 개의 서버를 사용하세요.

외부 키 관리 범위에 따라 주요 관리 서버가 클러스터의 모든 SVM을 보호할지 또는 선택한 SVM에만 안전할지 여부가 결정됩니다.

- 클러스터 범위 _ 를 사용하여 클러스터의 모든 SVM에 대한 외부 키 관리를 구성할 수 있습니다. 클러스터 관리자는 서버에 저장된 모든 키에 액세스할 수 있습니다.
- ONTAP 9.6부터는 _SVM SCOPE_를 사용하여 클러스터의 데이터 SVM을 위한 외부 키 관리를 구성할 수 있습니다. 이는 각 테넌트가 서로 다른 SVM(또는 SVM 세트)을 사용하여 데이터를 제공하는 멀티테넌트 환경에 가장 적합합니다. 지정된 테넌트의 SVM 관리자만 해당 테넌트의 키에 액세스할 수 있습니다.
- 멀티테넌트 환경의 경우 다음 명령을 사용하여 _MT_EK_MGMT_에 대한 라이센스를 설치합니다.

  'System license add-license-code <MT_EK_MGMT license code>'

  에 대한 자세한 내용은 `system license add` "ONTAP 명령 참조입니다"을 참조하십시오.

동일한 클러스터에서 두 범위를 모두 사용할 수 있습니다. SVM용으로 키 관리 서버를 구성한 경우 ONTAP에서는 이러한 서버만 사용하여 키를 보호합니다. 그렇지 않으면 ONTAP는 클러스터에 구성된 키 관리 서버로 키를 보호합니다.

클러스터 범위에서 온보드 키 관리를 구성하고 SVM 범위에서 외부 키 관리를 구성할 수 있습니다. 'Security key-manager key migrate' 명령을 사용하여 클러스터 범위의 온보드 키 관리에서 SVM 범위의 외부 키 관리자로 키를 마이그레이션할 수 있습니다.

에 대한 자세한 내용은 `security key-manager key migrate` "ONTAP 명령 참조입니다"을 참조하십시오.

시작하기 전에

- KMIP SSL 클라이언트 및 서버 인증서를 설치해야 합니다.
- KMIP 서버는 각 노드의 노드 관리 LIF에서 접근 가능해야 합니다.
- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.
- MetroCluster 환경에서:
  - 외부 키 관리를 활성화하기 전에 MetroCluster 완전히 구성해야 합니다.
  - 두 클러스터에 동일한 KMIP SSL 인증서를 설치해야 합니다.
  - 두 클러스터 모두에 외부 키 관리자를 구성해야 합니다.

단계

1. 클러스터의 Key Manager 접속 구성:

   'Security key-manager external enable - vserver admin_SVM-key-servers host_name | ip_address: port,… -client-cert client_certificate-server-ca-cert server_CA_certificates'를 참조하십시오

   > 그만큼 `security key-manager external enable` 명령은 다음을 대체합니다. `security key-manager setup` 명령. 클러스터 로그인 프롬프트에서 명령을 실행하면, *`admin_SVM`* 현재 클러스터의 관리 SVM으로 기본 설정됩니다. 당신은 실행할 수 있습니다 `security key-manager external modify` 외부 키 관리 구성을 변경하는 명령입니다.

   다음 명령을 실행하면 외부 키 서버가 3개인 'cluster1'에 대한 외부 키 관리가 활성화됩니다. 첫 번째 키 서버는 호스트 이름과 포트를 사용하여 지정되고, 두 번째 키는 IP 주소와 기본 포트를 사용하여 지정되며, 세 번째 키는 IPv6 주소와 포트를 사용하여 지정됩니다.

```
cluster1::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. SVM을 위한 키 관리자 구성:

'Security key-manager external enable - vserver SVM-key-servers host_name | ip_address: port,… -client -cert client_certificate-server-ca-cert server_CA_certificates'를 참조하십시오

- SVM 로그인 프롬프트에서 명령을 실행하면, `SVM` 현재 SVM을 기본값으로 사용합니다. 당신은 실행할 수 있습니다 `security key-manager external modify` 외부 키 관리 구성을 변경하는 명령입니다.
- MetroCluster 환경에서 데이터 SVM을 위한 외부 키 관리를 구성하는 경우 를 반복할 필요가 없습니다 `security key-manager external enable` 명령을 파트너 클러스터에 표시합니다.

다음 명령을 실행하면 기본 포트 5696에서 단일 키 서버가 수신 대기하는 'vm1'에 대한 외부 키 관리가 활성화됩니다.

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. 추가 SVM에 대해 마지막 단계를 반복합니다.

명령을 사용하여 추가 SVM을 구성할 수도 있습니다 `security key-manager external add-servers`. `security key-manager external add-servers`명령이 `security key-manager add` 명령을 대체합니다. 에 대한 자세한 내용은 `security key-manager external add-servers` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 구성된 모든 KMIP 서버가 연결되어 있는지 확인합니다.

'Security key-manager external show-status-node node_name'입니다

`security key-manager external show-status`명령이 `security key-manager show -status` 명령을 대체합니다. 에 대한 자세한 내용은 `security key-manager external show-status` link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-external-show-status.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  -----------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available
node2
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available

8 entries were displayed.
```

5. 필요한 경우 일반 텍스트 볼륨을 암호화된 볼륨으로 변환합니다.

   `volume encryption conversion start`

   볼륨을 변환하기 전에 외부 키 관리자를 완전히 구성해야 합니다.

관련 정보

- 클러스터링된 외부 키 서버를 구성합니다
- "시스템 라이센스 추가"
- "보안 키 관리자 키 마이그레이션"
- "보안 키 관리자 외부 추가 서버"
- "보안 키 관리자 외부 상태 표시"

ONTAP 9.5 및 이전 버전에서 **NVE**에 대한 외부 키 관리 활성화

하나 이상의 KMIP 서버를 사용하여 클러스터에서 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 하나의 노드에 KMIP 서버를 최대 4개까지 연결할 수 있습니다. 이중화 및 재해 복구를 위해 최소 2대의 서버를 사용하는 것이 좋습니다.

이 작업에 대해

ONTAP는 클러스터의 모든 노드에 대해 KMIP 서버 연결을 구성합니다.

시작하기 전에

- KMIP SSL 클라이언트 및 서버 인증서를 설치해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 외부 키 관리자를 구성하기 전에 MetroCluster 환경을 구성해야 합니다.
- MetroCluster 환경에서는 두 클러스터에 동일한 KMIP SSL 인증서를 설치해야 합니다.

단계

1. 클러스터 노드에 대한 Key Manager 접속 구성:

   보안 키 관리자 설정

   키 관리자 설정이 시작됩니다.

   > MetroCluster 환경에서는 두 클러스터에서 모두 이 명령을 실행해야 합니다. 자세히 알아보세요 `security key-manager setup` 에서"ONTAP 명령 참조입니다" .

2. 각 프롬프트에 적절한 응답을 입력합니다.
3. KMIP 서버 추가:

   'Security key-manager add-address key_management_server_ipaddress

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   > MetroCluster 환경에서는 두 클러스터 모두에서 이 명령을 실행해야 합니다.

4. 이중화를 위해 KMIP 서버를 추가로 추가합니다.

   'Security key-manager add-address key_management_server_ipaddress

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   > MetroCluster 환경에서는 두 클러스터 모두에서 이 명령을 실행해야 합니다.

5. 구성된 모든 KMIP 서버가 연결되어 있는지 확인합니다.

   보안 키 관리자 표시 상태

   이 절차에 설명된 명령에 대해 자세히 알아보세요."ONTAP 명령 참조입니다" .

```
cluster1::> security key-manager show -status

Node            Port      Registered Key Manager  Status
--------------  ----      ----------------------  ---------------
cluster1-01     5696      20.1.1.1                available
cluster1-01     5696      20.1.1.2                available
cluster1-02     5696      20.1.1.1                available
cluster1-02     5696      20.1.1.2                available
```

6. 필요한 경우 일반 텍스트 볼륨을 암호화된 볼륨으로 변환합니다.

   `volume encryption conversion start`

   볼륨을 변환하기 전에 외부 키 관리자를 완전히 구성해야 합니다. MetroCluster 환경에서는 외부 키 관리자를 두 사이트에 모두 구성해야 합니다.

클라우드 공급자와 함께 **ONTAP** 데이터 **SVM**에 대한 **NVE** 키 관리

ONTAP 9.10.1부터 클라우드 호스팅 응용 프로그램에서 및 를 "Google Cloud Platform의 키 관리 서비스(Cloud KMS)"사용하여 ONTAP 암호화 키를 보호할 수 "Azure 키 저장소(AKV)"있습니다. ONTAP 9.12.0부터, 로 NVE 키를 보호할 수도 "AWS의 KMS"있습니다.

AWS KMS, AKV 및 Cloud KMS를 사용하여 보호할 수 있습니다 "NVE(NetApp Volume Encryption) 키" 데이터 SVM에만 해당.

이 작업에 대해

클라우드 공급자를 사용한 키 관리는 CLI 또는 ONTAP REST API를 사용하여 설정할 수 있습니다.

클라우드 공급자를 사용하여 키를 보호할 때는 기본적으로 데이터 SVM LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용됩니다. 노드 관리 네트워크는 클라우드 공급자의 인증 서비스(Azure의 경우 login.microsoftonline.com, Cloud KMS의 경우 oauth2.googleapis.com)와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않은 경우 클러스터에서 키 관리 서비스를 제대로 사용할 수 없습니다.

클라우드 공급자 키 관리 서비스를 사용할 때는 다음과 같은 제한 사항을 숙지해야 합니다.

- NSE(NetApp 스토리지 암호화) 및 NAE(NetApp 애그리게이트 암호화)에 클라우드 공급자 키 관리를 사용할 수 없습니다. "외부 KMIP" 대신 사용할 수 있습니다.
- MetroCluster 구성에서는 클라우드 공급자 키 관리를 사용할 수 없습니다.
- 클라우드 공급자 키 관리는 데이터 SVM에서만 구성할 수 있습니다.

시작하기 전에

- 해당 클라우드 공급자에 KMS를 구성해야 합니다.
- ONTAP 클러스터 노드는 NVE를 지원해야 합니다.
- "VE(Volume Encryption) 및 MTEKM(Multi-tenant Encryption Key Management) 라이센스를 설치해야 합니다".. 이 라이선스는 에 "ONTAP 1 을 참조하십시오"포함되어 있습니다.

- 클러스터 또는 SVM 관리자여야 합니다.
- 데이터 SVM에는 암호화된 볼륨이 포함되어 있지 않아야 하며 키 관리자를 사용해야 합니다. 데이터 SVM에 암호화된 볼륨이 포함된 경우 KMS를 구성하기 전에 해당 볼륨을 마이그레이션해야 합니다.

외부 키 관리를 활성화합니다

외부 키 관리를 사용하는 방법은 사용하는 특정 키 관리자에 따라 다릅니다. 해당 키 관리자 및 환경의 탭을 선택합니다.

설치하고

시작하기 전에

- 암호화를 관리하는 IAM 역할이 사용할 AWS KMS 키에 대한 권한을 만들어야 합니다. IAM 역할에는 다음 작업을 허용하는 정책이 포함되어야 합니다.
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`
    를 누릅니다
    자세한 내용은 의 AWS 설명서를 참조하십시오 "보조금".

ONTAP SVM에서 **AWS KMV**를 활성화합니다

1. 시작하기 전에 AWS KMS에서 액세스 키 ID와 비밀 키를 모두 받으십시오.
2. 권한 수준을 고급으로 설정합니다.
   `set -priv advanced`
3. AWS KMS 활성화:
   `security key-manager external aws enable -vserver svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. 메시지가 표시되면 비밀 키를 입력합니다.
5. AWS KMS가 올바르게 구성되었는지 확인합니다.
   `security key-manager external aws show -vserver svm_name`

   에 대한 자세한 내용은 `security key-manager external aws` "ONTAP 명령 참조입니다"을 참조하십시오.

Azure를 지원합니다

ONTAP SVM에서 **Azure Key Vault**를 활성화합니다

1. 시작하기 전에 Azure 계정에서 클라이언트 암호 또는 인증서로 적절한 인증 자격 증명을 얻어야 합니다. 또한 클러스터의 모든 노드가 정상 상태인지 확인해야 합니다. 명령을 사용하여 확인할 수 `cluster show` 있습니다. 에 대한 자세한 내용은 `cluster show` "ONTAP 명령 참조입니다"을 참조하십시오.
2. 권한 수준을 Advanced'et-priv advanced로 설정합니다
3. SVM의 보안 키 관리자 외부 Azure ENABLE - CLIENT-id_client_id_-tenant-id_tenant_id_-name-key-id_id_-authentication-method {certificate|client-secret} 에서 AKV를 활성화합니다. 메시지가 나타나면 Azure 계정에서 클라이언트 인증서 또는 클라이언트 암호를 입력합니다.
4. AKV가 올바르게 활성화되었는지 확인합니다.
   `security key-manager external azure show vserver svm_name`
   서비스 상태가 양호하지 않은 경우 데이터 SVM LIF를 통해 AKV 키 관리 서비스에 대한 연결을 설정합니다.

   에 대한 자세한 내용은 `security key-manager external azure` "ONTAP 명령 참조입니다"을 참조하십시오.

Google 클라우드

ONTAP SVM에서 클라우드 **KMS** 지원

1. 시작하기 전에 JSON 형식으로 Google Cloud KMS 계정 키 파일의 개인 키를 받으십시오. GCP 계정에서

찾을 수 있습니다. 또한 클러스터의 모든 노드가 정상 상태인지 확인해야 합니다. 명령을 사용하여 확인할 수 `cluster show` 있습니다. 에 대한 자세한 내용은 `cluster show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 권한 수준을 고급으로 설정:
`set -priv advanced`
3. SVM에서 Cloud KMS 사용
`security key-manager external gcp enable -vserver` *`svm_name`* `-project-id` *`project_id`*`-key-ring-name` *`key_ring_name`* `-key-ring-location` *`key_ring_location`* `-key-name` *`key_name`*
메시지가 표시되면 서비스 계정 개인 키로 JSON 파일의 내용을 입력합니다
4. Cloud KMS가 올바른 매개변수로 구성되었는지 확인하세요.
`security key-manager external gcp show vserver` *`svm_name`* 의 상태 `kms_wrapped_key_status` 될 것이다 "`UNKNOWN`" 암호화된 볼륨이 생성되지 않은 경우. 서비스 도달성이 적절하지 않은 경우 데이터 SVM LIF를 통해 GCP 키 관리 서비스에 대한 연결을 설정합니다.

   에 대한 자세한 내용은 `security key-manager external gcp` "ONTAP 명령 참조입니다"을 참조하십시오.

하나 이상의 암호화된 볼륨이 데이터 SVM용으로 이미 구성되어 있고 admin SVM 온보드 키 관리자가 해당 NVE 키를 관리하는 경우 이러한 키를 외부 키 관리 서비스로 마이그레이션해야 합니다. CLI에서 이 작업을 수행하려면 다음 명령을 실행합니다.
`security key-manager key migrate -from-Vserver *admin_SVM* -to-Vserver *data_SVM*`데이터 SVM의 모든 NVE 키가 성공적으로 마이그레이션될 때까지 테넌트의 데이터 SVM에 대해 암호화된 새 볼륨을 생성할 수 없습니다.

관련 정보

- "Cloud Volumes ONTAP용 NetApp 암호화 솔루션으로 볼륨 암호화"
- "보안 키 관리자 외부"

Barbican KMS로 **ONTAP** 키 관리

ONTAP 9.17.1부터 OpenStack을 사용할 수 있습니다. "바비칸 KMS" ONTAP 암호화 키를 보호하기 위해. Barbican KMS는 키를 안전하게 저장하고 액세스하는 서비스입니다. Barbican KMS는 데이터 SVM의 NetApp 볼륨 암호화(NVE) 키를 보호하는 데 사용할 수 있습니다. Barbican은 다음을 사용합니다. "오픈스택 Keystone" 인증을 위한 OpenStack의 ID 서비스입니다.

이 작업에 대해

CLI 또는 ONTAP REST API를 사용하여 Barbican KMS에서 키 관리를 구성할 수 있습니다. 9.17.1 릴리스에서는 Barbican KMS 지원에 다음과 같은 제한 사항이 있습니다.

- Barbican KMS는 NetApp Storage Encryption(NSE) 및 NetApp Aggregate Encryption(NAE)을 지원하지 않습니다. 대신 다음을 사용할 수 있습니다. "외부 KMIP" 또는 "온보드 키 관리자(OKM)" NSE 및 NVE 키의 경우.
- Barbican KMS는 MetroCluster 구성에서 지원되지 않습니다.
- Barbican KMS는 데이터 SVM에 대해서만 구성할 수 있습니다. 관리자 SVM에서는 사용할 수 없습니다.

달리 명시되지 않는 한, 관리자는 `admin` 권한 수준은 다음 절차를 수행할 수 있습니다.

시작하기 전에

- Barbican KMS와 OpenStack Keystone 구성해야 합니다. Barbican과 함께 사용하는 SVM은 Barbican 및 OpenStack Keystone 서버에 대한 네트워크 액세스 권한이 있어야 합니다.
- Barbican 및 OpenStack Keystone 서버에 사용자 지정 인증 기관(CA)을 사용하는 경우 CA 인증서를 설치해야 합니다. `security certificate install -type server-ca -vserver <admin_svm>` .

Barbican KMS 구성을 만들고 활성화합니다**.**

SVM에 대한 새로운 Barbican KMS 구성을 생성하고 활성화할 수 있습니다. SVM에는 비활성화된 Barbican KMS 구성이 여러 개 있을 수 있지만, 한 번에 하나만 활성화할 수 있습니다.

단계

1. SVM에 대한 새로운 비활성 Barbican KMS 구성을 만듭니다.

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id` Barbican 키 암호화 키(KEK)의 키 식별자입니다. 다음을 포함한 전체 URL을 입력하세요. `https://` .

> 일부 URL에는 물음표(?) 문자가 포함되어 있습니다. 물음표는 ONTAP 명령줄의 활성 도움말을 활성화합니다. 물음표가 있는 URL을 입력하려면 먼저 다음 명령을 사용하여 활성 도움말을 비활성화해야 합니다. `set -active-help false` . 활성 도움말은 나중에 다음 명령을 사용하여 다시 활성화할 수 있습니다. `set -active-help true` . 자세한 내용은 "ONTAP 명령 참조입니다" .

   - `-keystone-url` OpenStack Keystone 인증 호스트의 URL입니다. 다음을 포함한 전체 URL을 입력하세요. `https://` .
   - `-application-cred-id` 는 애플리케이션 자격 증명 ID입니다.

     이 명령을 입력하면 애플리케이션 자격 증명 비밀 키를 입력하라는 메시지가 표시됩니다. 이 명령은 비활성 Barbican KMS 구성을 생성합니다.

     다음 예제에서는 이름이 지정된 새 비활성 Barbican KMS 구성을 만듭니다. `config1` SVM의 경우 `svm1` :

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. 새로운 Barbican KMS 구성을 활성화하세요:

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

이 명령을 사용하여 Barbican KMS 구성 간에 전환할 수 있습니다. SVM에 이미 활성화된 Barbican KMS 구성이 있는 경우, 해당 구성은 비활성화되고 새 구성이 활성화됩니다.

3. 새로운 Barbican KMS 구성이 활성화되었는지 확인하세요.

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

이 명령은 SVM 또는 노드에서 활성 Barbican KMS 구성의 상태를 제공합니다. 예를 들어, SVM이 `svm1` 노드에서 `node1` 활성화된 Barbican KMS 구성이 있는 경우 다음 명령을 실행하면 해당 구성의 상태가 반환됩니다.

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

Barbican KMS 구성의 자격 증명 및 설정 업데이트

활성 또는 비활성 Barbican KMS 구성의 현재 설정을 보고 업데이트할 수 있습니다.

단계

1. SVM에 대한 현재 Barbican KMS 구성을 확인하세요.

```
security key-manager external barbican show -vserver <svm_name>
```

각 Barbican KMS 구성에 대한 키 ID, OpenStack Keystone URL 및 애플리케이션 자격 증명 ID가 SVM에 표시됩니다.

2. Barbican KMS 구성 설정을 업데이트합니다.

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

이 명령은 지정된 Barbican KMS 구성의 시간 초과 및 확인 설정을 업데이트합니다. `timeout` ONTAP Barbican의 응답을 기다리는 시간(초)을 결정합니다. 기본값은 `timeout` 10초입니다. `verify` 그리고 `verify-host` 연결하기 전에 Barbican 호스트의 ID와 호스트 이름을 각각 확인해야 하는지 여부를 결정합니다. 기본적으로 이러한 매개변수는 다음과 같이 설정됩니다. `true` . 그 `vserver` 그리고 `config-name` 매개변수는 필수입니다. 다른 매개변수는 선택 사항입니다.

3. 필요한 경우 활성 또는 비활성 Barbican KMS 구성의 자격 증명을 업데이트합니다.

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

이 명령을 입력하면 새로운 애플리케이션 자격 증명 비밀 키를 입력하라는 메시지가 표시됩니다.

4. 필요한 경우 활성 Barbican KMS 구성에 대해 누락된 SVM 키 암호화 키(KEK)를 복원합니다.
   a. 누락된 SVM KEK를 복원합니다. `security key-manager external barbican restore` :

```
security key-manager external barbican restore -vserver <svm_name>
```

이 명령은 Barbican 서버와 통신하여 활성 Barbican KMS 구성에 대한 SVM KEK를 복원합니다.

5. 필요한 경우 Barbican KMS 구성에 맞게 SVM KEK를 다시 키로 지정하세요.
   a. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

   b. SVM KEK를 다시 키로 지정 `security key-manager external barbican rekey-internal` :

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

이 명령은 지정된 SVM에 대한 새로운 SVM KEK를 생성하고 볼륨 암호화 키를 새로운 SVM KEK로 다시 래핑합니다. 새로운 SVM KEK는 활성 Barbican KMS 구성으로 보호됩니다.

Barbican KMS와 **Onboard Key Manager** 간 키 마이그레이션

Barbican KMS에서 Onboard Key Manager(OKM)로 키를 마이그레이션할 수 있으며, 그 반대의 경우도 가능합니다. OKM에 대한 자세한 내용은 다음을 참조하세요. "ONTAP 9.6 이상에서 온보드 키 관리를 활성화합니다" .

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 필요한 경우 Barbican KMS에서 OKM으로 키를 마이그레이션합니다.

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<admin_svm_name>
```

`svm_name` Barbican KMS 구성을 사용한 SVM의 이름입니다.

3. 필요한 경우 OKM에서 Barbican KMS로 키를 마이그레이션합니다.

```
security key-manager key migrate -from-vserver <admin_svm_name> -to
-vserver <svm_name>
```

Barbican KMS 구성 비활성화 및 삭제

암호화된 볼륨이 없는 활성 Barbican KMS 구성을 비활성화할 수 있으며, 비활성 Barbican KMS 구성을 삭제할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. 활성 Barbican KMS 구성을 비활성화합니다.

```
security key-manager keystore disable -vserver <svm_name>
```

SVM에 NVE 암호화 볼륨이 있는 경우 해당 볼륨을 암호 해독해야 합니다. 키를 마이그레이션하다 Barbican KMS 구성을 비활성화하기 전에. 새로운 Barbican KMS 구성을 활성화할 때 NVE 볼륨을 복호화하거나 키를 마이그레이션할 필요는 없으며, 현재 활성화된 Barbican KMS 구성은 비활성화됩니다.

3. 비활성 Barbican KMS 구성을 삭제합니다.

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```

Onboard Key Manager를 사용하여 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 암호화된 볼륨 또는 자체 암호화 디스크에 액세스하는 각 클러스터에서 Onboard Key Manager를 활성화해야 합니다.

이 작업에 대해

클러스터에 노드를 추가할 때마다 보안 키 관리자 온보드 동기화 명령을 실행해야 합니다.

MetroCluster 구성이 있는 경우 을 실행해야 합니다 `security key-manager onboard enable` 먼저 로컬 클러스터에서 명령을 실행한 다음 를 실행합니다 `security key-manager onboard sync` 원격 클러스터에 대해 동일한 암호를 사용하여 명령을 실행합니다. 를 실행할 때 `security key-manager onboard enable` 로컬 클러스터에서 명령을 실행한 다음 원격 클러스터에서 동기화하면 를 실행할 필요가 없습니다 `enable` 명령을 원격 클러스터에서 다시 수행합니다.

자세히 알아보세요 `security key-manager onboard enable` 그리고 `security key-manager onboard sync` 에서"ONTAP 명령 참조입니다" .

기본적으로 노드를 재부팅할 때는 키 관리자 암호를 입력할 필요가 없습니다. 재부팅 후 사용자가 암호를 입력하도록 요구하려면 'cc-mode-enabled=yes' 옵션을 사용할 수 있습니다.

NVE의 경우 cc-mode-enabled=yes를 설정하면 볼륨 생성, 볼륨 이동 시작 명령을 사용하여 생성한 볼륨이 자동으로 암호화됩니다. 볼륨 만들기에는 -encrypt true를 지정할 필요가 없습니다. 볼륨 이동 시작의 경우 -encrypt-destination true를 지정하지 않아도 됩니다.

CSfC(Commercial Solutions for Classified) 요구 사항을 충족하기 위해 ONTAP 저장 데이터 암호화를 구성할 때 NSE와 NVE를 함께 사용해야 하며, Common Criteria 모드에서 Onboard Key Manager가 활성화되어 있는지 확인해야 합니다. 보다"CSDC 솔루션 요약" .

Common Criteria 모드('cc-mode-enabled=yes')에서 Onboard Key Manager를 활성화하면 다음과 같은 방식으로 시스템 동작이 변경됩니다.

- 시스템은 Common Criteria 모드에서 작동 중일 때 연속 실패한 클러스터 암호 시도를 모니터링합니다.

  클러스터 암호를 5번 입력하지 못하면 24시간을 기다리거나 노드를 재부팅하여 제한을 재설정하세요.

- 시스템 이미지 업데이트는 NetApp RSA-3072 코드 서명 인증서와 SHA-384 코드 서명 다이제스트를 함께 사용하여 일반적인 NetApp RSA-2048 코드 서명 인증서와 SHA-256 코드 서명 다이제스트 대신 이미지 무결성을 확인합니다.

  업그레이드 명령은 다양한 디지털 서명을 검사하여 이미지 내용이 변경되거나 손상되지 않았는지 확인합니다. 검증에 성공하면 시스템은 이미지 업데이트 프로세스의 다음 단계로 진행합니다. 그렇지 않으면 이미지 업데이트에 실패합니다. 자세히 알아보세요 `cluster image` 에서"ONTAP 명령 참조입니다" .

온보드 키 관리자는 키를 휘발성 메모리에 저장합니다. 휘발성 메모리 내용은 시스템이 재부팅되거나 중단되면 지워집니다. 시스템은 중단되면 30초 이내에 휘발성 메모리를 지웁니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- Onboard Key Manager를 구성하기 전에 MetroCluster 환경을 구성해야 합니다.

단계

1. 키 관리자 설정을 시작합니다.

   '보안 키 관리자 온보드 활성화-cc-모드 사용 예|아니오'

   재부팅 후 키 관리자 암호를 입력하도록 하려면 'cc-mode-enabled=yes'를 설정합니다. NVE의 경우 cc-mode-enabled=yes를 설정하면 볼륨 생성, 볼륨 이동 시작 명령을 사용하여 생성한 볼륨이 자동으로 암호화됩니다. MetroCluster 구성에서는 '-cc-mode-enabled' 옵션이 지원되지 않습니다. 보안 키매니저 온보드 활성화 명령은 보안 키매니저 설정 명령을 대체합니다.

2. 32~256자 사이의 암호를 입력하세요. "`cc-mode`"의 경우 64~256자 사이의 암호를 입력하세요.

   지정된 ""cc-mode"" 암호가 64자 미만이면 키 관리자 설정 작업에 암호 프롬프트가 다시 표시되기 전에 5초의 지연이 발생합니다.

3. 암호 확인 프롬프트에서 암호를 다시 입력합니다.
4. 인증 키가 생성되었는지 확인합니다.

   '보안 키 관리자 키 쿼리 - 키 유형 NSE-AK'

   `security key-manager key query`명령이 `security key-manager query key` 명령을 대체합니다.

   에 대한 자세한 내용은 `security key-manager key query` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 선택적으로 일반 텍스트 볼륨을 암호화된 볼륨으로 변환할 수 있습니다.

   ```
   volume encryption conversion start
   ```

   볼륨을 변환하기 전에 Onboard Key Manager를 완전히 구성해야 합니다. MetroCluster 환경에서는 두 사이트 모두에서 Onboard Key Manager를 구성해야 합니다.

작업을 마친 후

나중에 사용할 수 있도록 암호를 스토리지 시스템 외부의 안전한 위치에 복사합니다.

온보드 키 관리자 암호를 구성한 후, 저장 시스템 외부의 안전한 위치에 정보를 수동으로 백업하세요. 보다"온보드 키 관리 정보를 수동으로 백업합니다" .

관련 정보

- "클러스터 이미지 명령"
- "보안 키 관리자 외부 활성화"
- "보안 키 관리자 키 쿼리"

- "보안 키 관리자 온보드 활성화"

ONTAP 9.5 및 이전 버전에서 **NVE**에 대한 온보드 키 관리 활성화

Onboard Key Manager를 사용하여 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 암호화된 볼륨 또는 자체 암호화 디스크에 액세스하는 각 클러스터에서 Onboard Key Manager를 활성화해야 합니다.

이 작업에 대해

클러스터에 노드를 추가할 때마다 보안 키 관리자 설정 명령을 실행해야 합니다.

MetroCluster 구성이 있는 경우 다음 지침을 검토하십시오.

- ONTAP 9.5에서는 로컬 클러스터에서 보안 키 관리자 설정, 원격 클러스터에서 보안 키 관리자 설정 -동기화 -MetroCluster -구성 예 를 각각 동일한 암호를 사용하여 실행해야 합니다.
- ONTAP 9.5 이전에는 로컬 클러스터에서 보안 키 관리자 설정을 실행하고 약 20초 정도 기다린 다음 원격 클러스터에서 동일한 암호를 사용하여 보안 키 관리자 설정을 실행해야 합니다.

기본적으로 노드를 재부팅할 때는 키 관리자 암호를 입력할 필요가 없습니다. ONTAP 9.4부터 '-enable-cc-mode yes' 옵션을 사용하여 재부팅 후 사용자가 암호를 입력하도록 할 수 있습니다.

NVE의 경우 '-enable-cc-mode yes'를 설정하면 볼륨 생성 및 볼륨 이동 시작 명령으로 생성한 볼륨이 자동으로 암호화됩니다. 볼륨 만들기에는 -encrypt true를 지정할 필요가 없습니다. 볼륨 이동 시작의 경우 -encrypt-destination true를 지정하지 않아도 됩니다.

실패한 암호 구문을 시도한 후에는 노드를 다시 재부팅해야 합니다.

시작하기 전에

- 외부 키 관리(KMIP) 서버와 함께 NSE 또는 NVE를 사용하는 경우 외부 키 관리자 데이터베이스를 삭제하세요.

  "외부 키 관리에서 온보드 키 관리로 전환"

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- Onboard Key Manager를 구성하기 전에 MetroCluster 환경을 구성하세요.

단계

1. 키 관리자 설정을 시작합니다.

   '보안 키 관리자 설정-활성화-cc-모드 예|아니오'

   ONTAP 9.4부터는 사용자가 재부팅 후 키 관리자 암호를 입력하도록 하는 '-enable-cc-mode yes' 옵션을 사용할 수 있습니다. NVE의 경우 '-enable-cc-mode yes'를 설정하면 볼륨 생성 및 볼륨 이동 시작 명령으로 생성한 볼륨이 자동으로 암호화됩니다.

   다음 예제에서는 재부팅할 때마다 암호를 입력할 필요 없이 키 관리자를 cluster1에서 설정하기 시작합니다.

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. 온보드 키 관리를 구성하라는 메시지가 나타나면 "예"를 입력합니다.
3. 암호문 프롬프트에서 32자에서 256자 사이의 암호문을 입력하거나 64에서 256자 사이의 암호문을 "cc-mode"로 입력합니다.

> 지정된 ""cc-mode"" 암호가 64자 미만이면 키 관리자 설정 작업에 암호 프롬프트가 다시 표시되기 전에 5초의 지연이 발생합니다.

4. 암호 확인 프롬프트에서 암호를 다시 입력합니다.
5. 모든 노드에 대해 키가 구성되었는지 확인합니다.

`security key-manager show-key-store`

```
cluster1::> security key-manager show-key-store

Node: node1
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

자세히 알아보세요 `security key-manager show-key-store` 에서"ONTAP 명령 참조입니다" .

6. 필요한 경우 일반 텍스트 볼륨을 암호화된 볼륨으로 변환합니다.

   ```
   volume encryption conversion start
   ```

   볼륨을 변환하기 전에 Onboard Key Manager를 구성하세요. MetroCluster 환경에서는 두 사이트 모두에 구성합니다.

작업을 마친 후

나중에 사용할 수 있도록 암호를 스토리지 시스템 외부의 안전한 위치에 복사합니다.

온보드 키 관리자 암호를 구성할 때 재해 발생에 대비해 저장 시스템 외부의 안전한 위치에 정보를 백업하세요. 보다 "온보드 키 관리 정보를 수동으로 백업합니다" .

관련 정보

- "온보드 키 관리 정보를 수동으로 백업합니다"
- "외부 키 관리에서 온보드 키 관리로 전환"
- "보안 키 관리자 show-key-store"

새로 추가된 **ONTAP** 노드에서 온보드 키 관리 활성화

Onboard Key Manager를 사용하여 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 암호화된 볼륨 또는 자체 암호화 디스크에 액세스하는 각 클러스터에서 Onboard Key Manager를 활성화해야 합니다.

ONTAP 9.6 이상의 경우 다음을 실행해야 합니다. `security key-manager onboard sync` 클러스터에 노드를 추가할 때마다 명령을 실행합니다.

ONTAP 9.5 이전 버전의 경우, 클러스터에 노드를 추가할 때마다 '보안 키 관리자 설정' 명령을 실행해야 합니다.

온보드 키 관리 기능을 사용하여 클러스터에 노드를 추가하는 경우 이 명령을 실행하여 누락된 키를 새로 고칩니다.

MetroCluster 구성이 있는 경우 다음 지침을 검토하십시오.

- ONTAP 9.6부터 로컬 클러스터에서 보안 키 관리자 온보드 활성화를 먼저 실행한 다음 원격 클러스터에서 동일한 암호를 사용하여 보안 키 관리자 온보드 동기화를 실행해야 합니다.

  및 `security key-manager onboard sync` 에 대한 자세한 `security key-manager onboard enable` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

- ONTAP 9.5에서는 로컬 클러스터에서 보안 키 관리자 설정, 원격 클러스터에서 보안 키 관리자 설정 -동기화 -MetroCluster -구성 예 를 각각 동일한 암호를 사용하여 실행해야 합니다.
- ONTAP 9.5 이전에는 로컬 클러스터에서 보안 키 관리자 설정을 실행하고 약 20초 정도 기다린 다음 원격 클러스터에서 동일한 암호를 사용하여 보안 키 관리자 설정을 실행해야 합니다.

기본적으로 노드를 재부팅할 때는 키 관리자 암호를 입력할 필요가 없습니다. ONTAP 9.4부터 '-enable-cc-mode yes' 옵션을 사용하여 재부팅 후 사용자가 암호를 입력하도록 할 수 있습니다.

NVE의 경우 '-enable-cc-mode yes'를 설정하면 볼륨 생성 및 볼륨 이동 시작 명령으로 생성한 볼륨이 자동으로 암호화됩니다. 볼륨 만들기에는 -encrypt true를 지정할 필요가 없습니다. 볼륨 이동 시작의 경우 -encrypt-destination true를 지정하지 않아도 됩니다.

암호 입력에 실패하면 노드를 재부팅하세요. 재부팅 후 암호를 다시 입력해보세요.

관련 정보

- "클러스터 이미지 명령"
- "보안 키 관리자 외부 활성화"
- "보안 키 관리자 온보드 활성화"

NVE 또는 NAE를 사용하여 볼륨 데이터 암호화

NVE를 사용하여 ONTAP 볼륨 데이터를 암호화하는 방법에 대해 알아보세요.

ONTAP 9.7부터는 VE 라이센스 및 온보드 키 또는 외부 키 관리 기능이 있는 경우 기본적으로 애그리게이트 및 볼륨 암호화가 활성화됩니다. ONTAP 9.6 이하 버전의 경우 새 볼륨 또는 기존 볼륨에서 암호화를 활성화할 수 있습니다. 볼륨 암호화를 활성화하려면 VE 라이센스를 설치하고 키 관리를 활성화해야 합니다. NVE는 FIPS-140-2 레벨 1을 준수합니다.

ONTAP에서 VE 라이센스를 사용하여 애그리게이트 수준 암호화를 활성화합니다

ONTAP 9.7부터"VE 라이센스", 온보드 키 또는 외부 키 관리가 있는 경우 새로 생성된 애그리게이트와 볼륨은 기본적으로 암호화됩니다. ONTAP 9.6부터 애그리게이트 레벨 암호화를 사용하여 암호화할 볼륨에 포함된 애그리게이트에 키를 할당할 수 있습니다.

이 작업에 대해

인라인 또는 백그라운드 애그리게이트 레벨 중복제거를 수행하려는 경우 애그리게이트 레벨 암호화를 사용해야 합니다. 그 외에는 NVE에서 애그리게이트 레벨의 중복제거가 지원되지 않습니다.

애그리게이트 레벨 암호화를 위해 활성화된 애그리게이트를 *NAE aggregate*(NetApp 애그리게이트 암호화의 경우)라고 합니다. NAE 애그리게이트의 모든 볼륨은 NAE 또는 NVE 암호화로 암호화되어야 합니다. Aggregate 레벨의 암호화를 사용하면 Aggregate에서 생성한 볼륨이 NAE 암호화로 기본적으로 암호화됩니다. 대신 NVE 암호화를 사용하도록 기본값을 재정의할 수 있습니다.

NAE 애그리게이트에서는 일반 텍스트 볼륨이 지원되지 않습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 애그리게이트 레벨 암호화 활성화 또는 비활성화:

대상…	이 명령 사용…
ONTAP 9.7 이상을 사용하여 NAE 애그리게이트를 생성합니다	`storage aggregate create -aggregate aggregate_name -node node_name`

ONTAP 9.6으로 NAE 애그리게이트를 생성합니다	`storage aggregate create -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true`
NAE가 아닌 집계를 NAE 집계로 변환합니다	`storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true`
NAE 집계를 NAE가 아닌 집집합으로 변환합니다	`storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key false`

자세히 알아보세요 `storage aggregate modify` 에서 "ONTAP 명령 참조입니다" .

다음 명령을 실행하면 "aggr1"에서 집계 수준 암호화가 활성화됩니다.

- ONTAP 9.7 이상:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 이하:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

에 대한 자세한 내용은 `storage aggregate create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. Aggregate가 암호화를 사용하도록 설정되어 있는지 확인합니다.

'스토리지 집계 표시 필드 암호화 - 집계 키 사용'

다음 명령을 실행하면 "aggr1"이 암호화에 대해 활성화되어 있는지 확인합니다.

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

에 대한 자세한 내용은 `storage aggregate show` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

'volume create' 명령을 실행하여 암호화된 볼륨을 생성합니다.

KMIP 서버를 사용하여 노드의 암호화 키를 저장하는 경우, ONTAP는 볼륨을 암호화할 때 암호화 키를 서버에 자동으로 "푸시"(푸시)"합니다.

ONTAP에서 새 볼륨에 대해 암호화를 활성화합니다

'volume create' 명령을 사용하여 새 볼륨에서 암호화를 활성화할 수 있습니다.

이 작업에 대해

NVE(NetApp Volume Encryption)를 사용하여 볼륨을 암호화하고 ONTAP 9.6, NetApp Aggregate Encryption(NAE)로 시작할 수 있습니다. NAE와 NVE에 대한 자세한 내용은 를 참조하십시오 볼륨 암호화 개요.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP에서 새 볼륨에 대한 암호화를 활성화하는 절차는 사용 중인 ONTAP 버전과 특정 구성에 따라 다릅니다.

- ONTAP 9.4부터 시작합니다(사용하는 경우) `cc-mode` Onboard Key Manager(온보드 키 관리자)를 설정할 때 로 생성한 볼륨입니다 `volume create` 명령은 사용자가 지정하든 관계없이 자동으로 암호화됩니다 `-encrypt true`.
- ONTAP 9.6 및 이전 버전에서는 을 사용해야 합니다 `-encrypt true` 와 함께 `volume create` 암호화를 활성화하는 명령(사용하지 않은 경우 `cc-mode`)를 클릭합니다.
- ONTAP 9.6에서 NAE 볼륨을 작성하려면 집계 수준에서 NAE를 활성화해야 합니다. 을 참조하십시오 VE 라이센스로 애그리게이트 레벨 암호화를 설정합니다 를 참조하십시오.
- ONTAP 9.7부터, "VE 라이센스"온보드 키 또는 외부 키 관리가 있는 경우 새로 생성된 볼륨이 기본적으로 암호화됩니다. 기본적으로 NAE 애그리게이트에서 생성된 새 볼륨은 NVE가 아닌 NAE 유형이 됩니다.
  - ONTAP 9.7 이상 릴리즈에서 추가하는 경우 `-encrypt true` 를 누릅니다 `volume create` NAE 애그리게이트에서 볼륨을 생성하는 명령은 볼륨에 NAE 대신 NVE 암호화가 있습니다. NAE 애그리게이트의 모든 볼륨은 NVE 또는 NAE로 암호화되어야 합니다.

NAE 애그리게이트에서는 일반 텍스트 볼륨이 지원되지 않습니다.

단계

1. 새 볼륨을 생성하고 볼륨에 암호화가 활성화되어 있는지 여부를 지정합니다. 새 볼륨이 NAE 애그리게이트에 있는 경우 기본적으로 볼륨은 다음 NAE 볼륨이 됩니다.

생성 방법…	이 명령 사용…
NAE 볼륨	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*

NVE 볼륨	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` 를 누릅니다 NAE가 지원되지 않는 ONTAP 9.6 및 이전 버전에서는 `-encrypt true` NVE를 사용하여 볼륨을 암호화하도록 지정합니다. NAE 애그리게이트에서 볼륨이 생성되는 ONTAP 9.7 이상에서는 `-encrypt true` 대신 NAE의 기본 암호화 유형을 재정의하여 NVE 볼륨을 생성합니다.
일반 텍스트 볼륨입니다	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 볼륨에 암호화가 설정되어 있는지 확인합니다.

   볼륨 쇼는 암호화된 사실이다

   에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

결과

KMIP 서버를 사용하여 노드의 암호화 키를 저장하는 경우, ONTAP는 볼륨을 암호화할 때 암호화 키를 서버에 자동으로 "푸시" 합니다.

기존 **ONTAP** 볼륨에서 **NAE** 또는 **NVE** 활성화

둘 중 하나를 사용할 수 있습니다 `volume move start` 또는 을 누릅니다 `volume encryption conversion start` 기존 볼륨에서 암호화를 활성화하는 명령입니다.

이 작업에 대해

당신은 사용할 수 있습니다 `volume encryption conversion start` 볼륨을 다른 위치로 이동하지 않고도 기존 볼륨의 암호화를 "현재 위치"에서 활성화하는 명령입니다. 또는 다음을 사용할 수 있습니다. `volume move start` 명령.

볼륨 암호화 변환 시작 명령을 사용하여 기존 볼륨에서 암호화를 활성화합니다

당신은 사용할 수 있습니다 `volume encryption conversion start` 볼륨을 다른 위치로 옮기지 않고도 기존 볼륨의 암호화를 "그대로" 활성화하는 명령입니다.

변환 작업을 시작한 후에는 작업을 완료해야 합니다. 작업 중에 성능 문제가 발생하면 를 실행할 수 있습니다 `volume encryption conversion pause` 명령을 사용하여 작업을 일시 중지하고, 를 클릭합니다 `volume encryption conversion resume` 명령을 사용하여 작업을 재개합니다.

를 사용할 수 없습니다 `volume encryption conversion start` SnapLock 볼륨을 변환합니다.

단계

1. 기존 볼륨에서 암호화 활성화:

   '볼륨 암호화 변환 시작 - SVM_NAME - volume volume volume_name'

   에 대한 자세한 내용은 `volume encryption conversion start` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 기존 볼륨의 암호화가 설정됩니다 `vol1`:

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   시스템에서 볼륨에 대한 암호화 키를 생성합니다. 볼륨의 데이터가 암호화됩니다.

2. 변환 작업의 상태를 확인합니다.

   볼륨 암호화 변환 표시

   에 대한 자세한 내용은 `volume encryption conversion show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 변환 작업의 상태가 표시됩니다.

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ----------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. 변환 작업이 완료되면 볼륨이 암호화에 활성화되어 있는지 확인합니다.

   볼륨 쇼는 암호화된 사실이다

   에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 암호화된 볼륨이 'cluster1'에 표시됩니다.

   ```
   cluster1::> volume show -is-encrypted true

   Vserver  Volume  Aggregate  State   Type  Size  Available  Used
   -------  ------  ---------  -----   ----  -----  ---------  ----
   vs1      vol1    aggr2      online    RW  200GB    160.0GB  20%
   ```

결과

KMIP 서버를 사용하여 노드의 암호화 키를 저장하는 경우, ONTAP는 볼륨을 암호화할 때 암호화 키를 서버에 자동으로 "푸시"(푸시)"합니다.

볼륨 이동 시작 명령을 사용하여 기존 볼륨에서 암호화를 활성화합니다

명령을 사용하여 기존 볼륨을 이동하여 암호화를 활성화할 수 `volume move start` 있습니다. 동일한 애그리게이트 또는 다른 애그리게이트를 사용할 수 있습니다.

이 작업에 대해

- ONTAP 9.8부터 볼륨 이동 시작을 사용하여 SnapLock 또는 FlexGroup 볼륨에서 암호화를 활성화할 수 있습니다.
- ONTAP 9.4부터 Onboard Key Manager를 설정할 때 ""cc-mode""를 활성화하면 "volume move start" 명령으로 생성한 볼륨이 자동으로 암호화됩니다. `-encrypt-destination true'는 지정하지 않아도 됩니다.
- ONTAP 9.6부터는 Aggregate 수준의 암호화를 사용하여 이동할 볼륨의 포함된 Aggregate에 키를 할당할 수 있습니다. 고유 키로 암호화된 볼륨을 _ NVE 볼륨 _ 이라고 합니다(NetApp 볼륨 암호화를 사용한다는 의미). 애그리게이트 레벨 키로 암호화된 볼륨을 _NAE 볼륨 _ (NetApp 애그리게이트 암호화의 경우)이라고 합니다. NAE 애그리게이트에서는 일반 텍스트 볼륨이 지원되지 않습니다.
- ONTAP 9.14.1부터 NVE로 SVM 루트 볼륨을 암호화할 수 있습니다. 자세한 내용은 을 참조하십시오 SVM 루트 볼륨에 NetApp 볼륨 암호화를 구성합니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자이거나 클러스터 관리자가 권한을 위임한 SVM 관리자여야 합니다.

"볼륨 이동 명령을 실행하는 위임 권한"

단계

1. 기존 볼륨을 이동하고 볼륨에 암호화가 활성화되어 있는지 여부를 지정합니다.

변환…	이 명령 사용…
NVE 볼륨에 대한 일반 텍스트 볼륨입니다	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true`
NAE 볼륨에 대한 NVE 또는 일반 텍스트 볼륨(대상에 애그리게이트 레벨 암호화가 사용되는 것으로 가정)	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true`
NVE 볼륨에 대한 NAE 볼륨	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false`
Nae 볼륨을 일반 텍스트 볼륨으로	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`
NVE 볼륨을 일반 텍스트 볼륨으로	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

에 대한 자세한 내용은 `volume move start` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 이름이 vol1인 일반 텍스트 볼륨이 NVE 볼륨으로 변환됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

대상에서 애그리게이트 레벨 암호화를 사용하도록 설정한 경우 다음 명령을 실행하면 NVE 볼륨이나 일반 텍스트 볼륨 vol1이 NAE 볼륨으로 변환됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

다음 명령을 실행하면 이름이 vol2인 NAE 볼륨이 NVE 볼륨으로 변환됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

다음 명령을 실행하면 이름이 vol2인 NAE 볼륨이 일반 텍스트 볼륨으로 변환됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

다음 명령을 실행하면 이름이 vol2인 NVE 볼륨이 일반 텍스트 볼륨으로 변환됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. 클러스터 볼륨의 암호화 유형을 확인합니다.

   '볼륨 표시 필드 암호화 - 없음|볼륨|집계'를 입력합니다

   암호화 유형 필드는 ONTAP 9.6 이상에서 사용할 수 있습니다.

   에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 'cluster2'의 볼륨 암호화 유형이 표시됩니다.

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. 볼륨에 암호화가 설정되어 있는지 확인합니다.

   볼륨 쇼는 암호화된 사실이다

   에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 암호화된 볼륨이 'cluster2'에 표시됩니다.

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

결과

KMIP 서버를 사용하여 노드의 암호화 키를 저장하는 경우, 볼륨을 암호화할 때 ONTAP는 서버에 암호화 키를 자동으로 푸시합니다.

ONTAP SVM 루트 볼륨에 NVE 구성

ONTAP 9.14.1부터 스토리지 VM(SVM) 루트 볼륨에서 NetApp 볼륨 암호화(NVE)를 활성화할 수 있습니다. NVE에서는 루트 볼륨을 고유 키로 암호화하여 SVM의 보안을 강화합니다.

이 작업에 대해

SVM 루트 볼륨의 NVE는 SVM이 생성된 후에만 활성화할 수 있습니다.

시작하기 전에

- SVM 루트 볼륨은 NetApp 애그리게이트 암호화(NAE)로 암호화된 애그리게이트에 있어서는 안 됩니다.
- Onboard Key Manager 또는 외부 키 관리자를 사용하여 암호화를 활성화해야 합니다.
- ONTAP 9.14.1 이상을 실행해야 합니다.
- NVE로 암호화된 루트 볼륨이 포함된 SVM을 마이그레이션하려면 마이그레이션이 완료된 후 SVM 루트 볼륨을 일반 텍스트 볼륨으로 변환한 다음 SVM 루트 볼륨을 다시 암호화해야 합니다.
  - SVM 마이그레이션의 타겟 Aggregate에서 NAE를 사용하는 경우 루트 볼륨은 기본적으로 NAE를 상속합니다.
- SVM이 SVM 재해 복구 관계에 있는 경우:
  - 미러링된 SVM의 암호화 설정은 대상에 복사되지 않습니다. 소스 또는 대상에서 NVE를 활성화한 경우

미러링된 SVM 루트 볼륨에서 NVE를 별도로 활성화해야 합니다.

- 타겟 클러스터의 모든 애그리게이트가 NAE를 사용하는 경우 SVM 루트 볼륨은 NAE를 사용합니다.

단계

ONTAP CLI 또는 System Manager를 사용하여 SVM 루트 볼륨에서 NVE를 활성화할 수 있습니다.

CLI를 참조하십시오

제자리에서 SVM 루트 볼륨에서 NVE를 사용하거나 애그리게이트 간에 볼륨을 이동하여 활성화할 수 있습니다.

루트 볼륨을 제자리에서 암호화합니다

1. 루트 볼륨을 암호화된 볼륨으로 변환:

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. 암호화가 성공했는지 확인합니다. 를 클릭합니다 `volume show -encryption-type volume` NVE를 사용하는 모든 볼륨의 목록을 표시합니다.

SVM 루트 볼륨을 이동하여 암호화

1. 볼륨 이동 시작:

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

   에 대한 자세한 내용은 `volume move` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 를 확인합니다 `volume move` 에서 작업이 성공했습니다 `volume move show` 명령. 를 클릭합니다 `volume show -encryption-type volume` NVE를 사용하는 모든 볼륨의 목록을 표시합니다.

시스템 관리자

1. 스토리지> 볼륨 으로 이동합니다.
2. 암호화할 SVM 루트 볼륨의 이름 옆에 있는 **Edit** 를 선택합니다 ⋮ .
3. 저장소 및 최적화 제목 아래에서 암호화 활성화 를 선택합니다.
4. 저장을 선택합니다.

ONTAP 노드 루트 볼륨에 **NVE** 구성

ONTAP 9.8부터 NetApp 볼륨 암호화를 사용하여 노드의 루트 볼륨을 보호할 수 있습니다.

이 작업에 대해

이 절차는 노드 루트 볼륨에 적용됩니다. SVM 루트 볼륨에는 적용되지 않습니다. SVM 루트 볼륨은 애그리게이트 레벨 암호화 및 ONTAP 9.14.1부터 NVE.

루트 볼륨 암호화가 시작되면 완료해야 합니다. 작업을 일시 중지할 수 없습니다. 암호화가 완료되면 루트 볼륨에 새 키를 할당할 수 없으며 보안 제거 작업을 수행할 수 없습니다.

시작하기 전에

- 시스템에서 HA 구성을 사용해야 합니다.
- 노드 루트 볼륨이 이미 생성되어 있어야 합니다.
- KMIP(Key Management Interoperability Protocol)를 사용하여 시스템에 온보드 키 관리자 또는 외부 키 관리 서버가 있어야 합니다.

단계

1. 루트 볼륨 암호화:

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. 변환 작업의 상태를 확인합니다.

   볼륨 암호화 변환 표시

3. 변환 작업이 완료되면 볼륨이 암호화되었는지 확인합니다.

   '볼륨 표시 필드'

   다음은 암호화된 볼륨에 대한 출력 예입니다.

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```

NetApp 하드웨어 기반 암호화를 구성합니다

ONTAP 하드웨어 기반 암호화에 대해 알아보세요

NetApp 하드웨어 기반 암호화는 FDE(전체 디스크 암호화)가 쓰일 때 데이터를 지원합니다. 펌웨어에 저장된 암호화 키가 없으면 데이터를 읽을 수 없습니다. 암호화 키는 인증된 노드에서만 액세스할 수 있습니다.

NetApp 하드웨어 기반 암호화 이해

노드는 외부 키 관리 서버 또는 Onboard Key Manager에서 검색된 인증 키를 사용하여 자체 암호화 드라이브에 대해 자신을 인증합니다.

- 외부 키 관리 서버는 KMIP(Key Management Interoperability Protocol)를 사용하여 노드에 키를 제공하는 스토리지 환경의 타사 시스템입니다. 데이터와 다른 스토리지 시스템에 있는 외부 키 관리 서버를 구성하는 것이 가장 좋습니다.
- Onboard Key Manager는 데이터와 동일한 스토리지 시스템의 노드에 인증 키를 제공하는 기본 제공 도구입니다.

하드웨어 기반 암호화와 NetApp 볼륨 암호화를 사용하여 자체 암호화 드라이브에서 데이터를 "이중 암호화"할 수 있습니다.

자체 암호화 드라이브가 사용되면 코어 덤프도 암호화됩니다.

HA 쌍이 암호화 SAS 또는 NVMe 드라이브(SED, NSE, FIPS)를 사용 중인 경우 항목의 지침을 따라야 합니다 FIPS 드라이브 또는 SED를 보호되지 않는 모드로 되돌리는 중입니다 시스템을 초기화하기 전에 HA 쌍 내의 모든 드라이브(부팅 옵션 4 또는 9) 이렇게 하지 않을 경우 드라이브를 용도 변경할 경우 향후의 데이터 손실이 발생할 수 있습니다.

지원되는 자체 암호화 드라이브 유형입니다

다음과 같은 두 가지 유형의 자체 암호화 드라이브가 지원됩니다.

- 자체 암호화 FIPS 인증 SAS 또는 NVMe 드라이브가 모든 FAS 및 AFF 시스템에서 지원됩니다. FIPS 드라이브라고 하는 이러한 드라이브는 Federal Information Processing Standard Publication 140-2, 레벨 2의 요구 사항을 준수합니다. 인증된 기능을 통해 드라이브에 대한 서비스 거부 공격을 방지하는 것과 같은 암호화 외에도 보호 기능을 사용할 수 있습니다. FIPS 드라이브를 동일한 노드 또는 HA 쌍의 다른 유형의 드라이브와 혼합할 수 없습니다.
- ONTAP 9.6부터 FIPS 테스트를 거치지 않은 자체 암호화 NVMe 드라이브가 AFF A800, A320 이상 시스템에서 지원됩니다. SED_라고 하는 이러한 드라이브는 FIPS 드라이브와 동일한 암호화 기능을 제공하지만 동일한 노드 또는 HA 쌍의 비암호화 드라이브와 혼합될 수 있습니다.
- FIPS 검증을 거친 모든 드라이브는 FIPS 검증을 거친 펌웨어 암호화 모듈을 사용합니다. FIPS 드라이브 암호화 모듈은 드라이브 외부에서 생성된 키를 사용하지 않습니다(드라이브에 입력된 인증 암호는 드라이브의 펌웨어 암호화 모듈에서 키 암호화 키를 얻는 데 사용됩니다).

비암호화 드라이브는 SED 또는 FIPS 드라이브가 아닌 드라이브입니다.

Flash Cache 모듈이 있는 시스템에서 NSE를 사용하는 경우, NVE 또는 NAE도 활성화해야 합니다. NSE는 Flash Cache 모듈에 상주하는 데이터를 암호화하지 않습니다.

외부 키 관리 사용 시기

일반적으로 온보드 키 관리자를 사용하는 것이 더 저렴하고 더 편리하긴 하지만 다음 중 하나라도 해당하는 경우 외부 키 관리를 사용해야 합니다.

- 조직의 정책에는 FIPS 140-2 레벨 2(또는 그 이상) 암호화 모듈을 사용하는 키 관리 솔루션이 필요합니다.
- 암호화 키를 중앙 집중식으로 관리하는 다중 클러스터 솔루션이 필요합니다.
- 기업은 인증 키를 시스템 또는 데이터와 다른 위치에 저장하는 추가적인 보안을 필요로 합니다.

지원 세부 정보

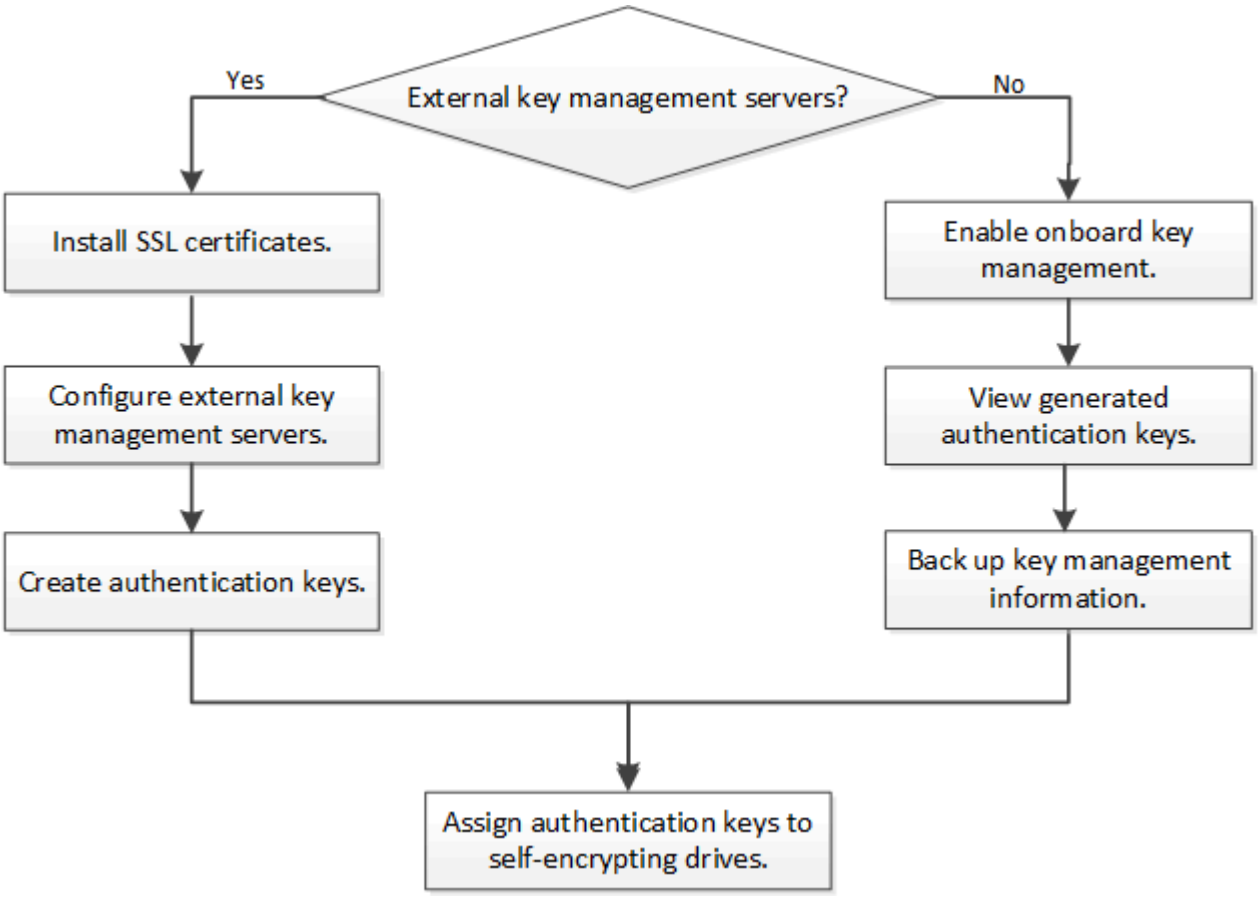
다음 표에는 중요한 하드웨어 암호화 지원 세부 정보가 나와 있습니다. 지원되는 KMIP 서버, 스토리지 시스템 및 디스크 쉘프에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

리소스 또는 기능	지원 세부 정보
비동종 디스크 세트	• FIPS 드라이브를 동일한 노드 또는 HA 쌍의 다른 유형의 드라이브와 혼합할 수 없습니다. HA 쌍을 준수하는 것은 동일한 클러스터에서 규정을 준수하지 않는 HA 쌍과 공존할 수 있습니다. • SED는 동일한 노드 또는 HA 쌍에서 비암호화 드라이브와 혼합될 수 있습니다.

드라이브 유형입니다	• FIPS 드라이브는 SAS 또는 NVMe 드라이브가 될 수 있습니다. • SED는 NVMe 드라이브여야 합니다.
10Gb 네트워크 인터페이스	ONTAP 9.3부터 KMIP 키 관리 구성은 외부 키 관리 서버와의 통신을 위한 10Gb 네트워크 인터페이스를 지원합니다.
키 관리 서버와의 통신을 위한 포트	ONTAP 9.3부터는 모든 스토리지 컨트롤러 포트를 사용하여 키 관리 서버와 통신할 수 있습니다. 그렇지 않으면 키 관리 서버와 통신하기 위해 e0M 포트를 사용해야 합니다. 스토리지 컨트롤러 모델에 따라 부팅 프로세스 중에 키 관리 서버와 통신하기 위해 특정 네트워크 인터페이스를 사용하지 못할 수 있습니다.
MetroCluster(MCC)	• NVMe 드라이브는 MCC를 지원합니다. • SAS 드라이브는 MCC를 지원하지 않습니다.

하드웨어 기반 암호화 워크플로우

클러스터가 자체 암호화 드라이브에 인증하려면 키 관리 서비스를 구성해야 합니다. 외부 키 관리 서버 또는 온보드 키 관리자를 사용할 수 있습니다.



관련 정보

- "NetApp Hardware Universe를 참조하십시오"
- "NetApp 볼륨 암호화 및 NetApp 애그리게이트 암호화"

외부 키 관리를 구성합니다

ONTAP 외부 키 관리 구성에 대해 알아보세요

하나 이상의 외부 키 관리 서버를 사용하여 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 외부 키 관리 서버는 KMIP(Key Management Interoperability Protocol)를 사용하여 노드에 키를 제공하는 스토리지 환경의 타사 시스템입니다.

온보드 키 관리자를 사용하여 NVE(NetApp Volume Encryption)를 구현할 수 있습니다. ONTAP 9.3 이상에서는 외부 키 관리(KMIP)와 온보드 키 관리자를 사용하여 NVE를 구현할 수 있습니다. ONTAP 9.11.1부터 클러스터에 여러 외부 키 관리자를 구성할 수 있습니다. 을 참조하십시오 클러스터링된 키 서버를 구성합니다.

ONTAP 클러스터에 **SSL** 인증서 설치

클러스터와 KMIP 서버는 KMIP SSL 인증서를 사용하여 서로의 ID를 확인하고 SSL 연결을 설정합니다. KMIP 서버와의 SSL 연결을 구성하기 전에, 클러스터에 대한 KMIP 클라이언트 SSL 인증서와 KMIP 서버의 루트 인증 기관(CA)에 대한 SSL 공용 인증서를 설치해야 합니다.

이 작업에 대해

HA 쌍에서는 두 노드가 동일한 퍼블릭 및 프라이빗 KMIP SSL 인증서를 사용해야 합니다. 동일한 KMIP 서버에 여러 HA 쌍을 연결하는 경우, HA 쌍의 모든 노드는 동일한 공용 및 전용 KMIP SSL 인증서를 사용해야 합니다.

시작하기 전에

- 서버에서 시간을 동기화하여 인증서, KMIP 서버 및 클러스터를 생성해야 합니다.
- 클러스터를 위한 공용 SSL KMIP 클라이언트 인증서를 얻어야 합니다.
- 클러스터를 위한 SSL KMIP 클라이언트 인증서와 관련된 개인 키를 얻어야 합니다.
- SSL KMIP 클라이언트 인증서는 암호로 보호되어 있지 않아야 합니다.
- KMIP 서버의 루트 CA(인증 기관)에 대한 SSL 공용 인증서를 얻어야 합니다.
- MetroCluster 환경에서는 두 클러스터 모두에 동일한 KMIP SSL 인증서를 설치해야 합니다.

클러스터에 인증서를 설치하기 전이나 후에 KMIP 서버에 클라이언트 및 서버 인증서를 설치할 수 있습니다.

단계

1. 클러스터에 SSL KMIP 클라이언트 인증서를 설치합니다.

   'Security certificate install - vserver admin_svm_name -type client'

   SSL KMIP 공용 및 개인 인증서를 입력하라는 메시지가 표시됩니다.

   'cluster1::> security certificate install -vserver cluster1-type client'

2. KMIP 서버의 루트 CA(인증 기관)에 대한 SSL 공용 인증서를 설치합니다.

   'Security certificate install - vserver admin_svm_name -type server-ca'

   'cluster1::> security certificate install -vserver cluster1-type server-ca'를 입력합니다

관련 정보

- "보안 인증서 설치"

ONTAP 9.6 이상에서 하드웨어 기반 암호화를 위한 외부 키 관리 활성화

하나 이상의 KMIP 서버를 사용하여 클러스터에서 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 하나의 노드에 KMIP 서버를 최대 4개까지 연결할 수 있습니다. 이중화 및 재해 복구를 위해 최소 2대의 서버를 사용하는 것이 좋습니다.

ONTAP 9.11.1부터 기본 키 서버당 최대 3개의 보조 키 서버를 추가하여 클러스터된 키 서버를 생성할 수 있습니다. 자세한 내용은 을 참조하십시오 클러스터링된 외부 키 서버를 구성합니다.

시작하기 전에

- KMIP SSL 클라이언트 및 서버 인증서를 설치해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- MetroCluster 환경에서:
  - 외부 키 관리자를 구성하기 전에 MetroCluster 환경을 구성해야 합니다.
  - 두 클러스터에 동일한 KMIP SSL 인증서를 설치해야 합니다.

단계

1. 클러스터의 Key Manager 접속 구성:

   "+ 보안 키 관리자 외부 활성화 - vserver admin_SVM-key-servers host_name | ip_address:port,… -client-cert client_certificate-server-ca-cert server_CA_certificates+'

   - `security key-manager external enable`명령이 `security key-manager setup` 명령을 대체합니다. 명령을 실행하여 외부 키 관리 구성을 변경할 수 `security key-manager external modify` 있습니다. 에 대한 자세한 내용은 `security key-manager external enable` "ONTAP 명령 참조입니다"을 참조하십시오.
   - MetroCluster 환경에서 관리 SVM에 대한 외부 키 관리를 구성하는 경우 를 반복해야 합니다 `security key-manager external enable` 명령을 파트너 클러스터에 표시합니다.

   다음 명령을 실행하면 외부 키 서버가 3개인 'cluster1'에 대한 외부 키 관리가 활성화됩니다. 첫 번째 키 서버는 호스트 이름과 포트를 사용하여 지정되고, 두 번째 키는 IP 주소와 기본 포트를 사용하여 지정되며, 세 번째 키는 IPv6 주소와 포트를 사용하여 지정됩니다.

   ```
   clusterl::> security key-manager external enable -key-servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. 구성된 모든 KMIP 서버가 연결되어 있는지 확인합니다.

   'Security key-manager external show-status-node_name-vserver SVM-key-server host_name|ip_address:port-key-server-status available|not-responding|unknown'

`security key-manager external show-status`명령이 `security key-manager show -status` 명령을 대체합니다. 에 대한 자세한 내용은 `security key-manager external show-status` link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-external-show-status.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ---------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

관련 정보

- 클러스터링된 외부 키 서버를 구성합니다
- "보안 키 관리자 외부 활성화"
- "보안 키 관리자 외부 상태 표시"

ONTAP 9.5 및 이전 버전에서 하드웨어 기반 암호화를 위한 외부 키 관리 활성화

하나 이상의 KMIP 서버를 사용하여 클러스터에서 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 하나의 노드에 KMIP 서버를 최대 4개까지 연결할 수 있습니다. 이중화 및 재해 복구를 위해 최소 2대의 서버를 사용하는 것이 좋습니다.

이 작업에 대해

ONTAP는 클러스터의 모든 노드에 대해 KMIP 서버 연결을 구성합니다.

시작하기 전에

- KMIP SSL 클라이언트 및 서버 인증서를 설치해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

- 외부 키 관리자를 구성하기 전에 MetroCluster 환경을 구성해야 합니다.
- MetroCluster 환경에서는 두 클러스터에 동일한 KMIP SSL 인증서를 설치해야 합니다.

단계

1. 클러스터 노드에 대한 Key Manager 접속 구성:

   보안 키 관리자 설정

   키 관리자 설정이 시작됩니다.

   > MetroCluster 환경에서는 두 클러스터에서 모두 이 명령을 실행해야 합니다. 자세히 알아보세요 `security key-manager setup` 에서"ONTAP 명령 참조입니다" .

2. 각 프롬프트에 적절한 응답을 입력합니다.
3. KMIP 서버 추가:

   'Security key-manager add-address key_management_server_ipaddress

   ```
   cluster1::> security key-manager add -address 20.1.1.1
   ```

   > MetroCluster 환경에서는 두 클러스터 모두에서 이 명령을 실행해야 합니다.

4. 이중화를 위해 KMIP 서버를 추가로 추가합니다.

   'Security key-manager add-address key_management_server_ipaddress

   ```
   cluster1::> security key-manager add -address 20.1.1.2
   ```

   > MetroCluster 환경에서는 두 클러스터 모두에서 이 명령을 실행해야 합니다.

5. 구성된 모든 KMIP 서버가 연결되어 있는지 확인합니다.

   보안 키 관리자 표시 상태

   이 절차에 설명된 명령에 대해 자세히 알아보세요."ONTAP 명령 참조입니다" .

   ```
   cluster1::> security key-manager show -status

   Node             Port      Registered Key Manager  Status
   ---------------  ----      ----------------------  ---------------
   cluster1-01      5696      20.1.1.1                available
   cluster1-01      5696      20.1.1.2                available
   cluster1-02      5696      20.1.1.1                available
   cluster1-02      5696      20.1.1.2                available
   ```

6. 필요한 경우 일반 텍스트 볼륨을 암호화된 볼륨으로 변환합니다.

   ```
   volume encryption conversion start
   ```

   볼륨을 변환하기 전에 외부 키 관리자를 완전히 구성해야 합니다. MetroCluster 환경에서는 외부 키 관리자를 두 사이트에 모두 구성해야 합니다.

ONTAP에서 클러스터된 외부 키 서버를 구성합니다

ONTAP 9.11.1부터 SVM에서 클러스터링된 외부 키 관리 서버에 대한 연결을 구성할 수 있습니다. 클러스터형 키 서버를 사용하면 SVM에서 기본 키 서버와 보조 키 서버를 지정할 수 있습니다. ONTAP 키를 등록하거나 검색할 때 먼저 기본 키 서버에 액세스를 시도한 후 작업이 성공적으로 완료될 때까지 순차적으로 보조 서버에 액세스를 시도합니다.

NetApp Storage Encryption(NSE), NetApp Volume Encryption(NVE), NetApp Aggregate Encryption(NAE) 키에 외부 키 서버를 사용할 수 있습니다. SVM은 최대 4개의 기본 외부 KMIP 서버를 지원할 수 있습니다. 각 기본 서버는 최대 3개의 보조 키 서버를 지원할 수 있습니다.

이 작업에 대해

- 이 프로세스는 KMIP를 사용하는 주요 서버만 지원합니다. 지원되는 키 서버 목록을 보려면 를 확인하십시오 "NetApp 상호 운용성 매트릭스 툴".

시작하기 전에

- "SVM에 대해 KMIP 키 관리를 활성화해야 합니다".
- 클러스터의 모든 노드에서 ONTAP 9.11.1 이상이 실행되고 있어야 합니다.
- 서버 목록의 순서는 다음과 같습니다. `-secondary-key-servers` 매개변수는 외부 키 관리(KMIP) 서버의 액세스 순서를 반영합니다.

클러스터링된 키 서버를 생성합니다

구성 절차는 기본 키 서버를 구성했는지 여부에 따라 달라집니다.

SVM에 **1**차 및 **2**차 키 서버를 추가합니다

단계

1. 클러스터(관리 SVM)에 대해 키 관리가 활성화되지 않았는지 확인하세요.

   ```
   security key-manager external show -vserver <svm_name>
   ```

   SVM에 이미 최대 4개의 기본 키 서버가 활성화되어 있는 경우 새 기본 키 서버를 추가하기 전에 기존 기본 키 서버 중 하나를 제거해야 합니다.

2. 기본 키 관리자를 활성화합니다.

   ```
   security key-manager external enable -vserver <svm_name> -key-servers
   <primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs
   <server_ca_cert_names>
   ```

   - 포트를 지정하지 않으면 `-key-servers` 매개변수의 경우 기본 포트 5696이 사용됩니다.

   > 실행 중이라면 `security key-manager external enable` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다. NetApp 두 클러스터 모두에서 동일한 키 서버를 사용할 것을 강력히 권장합니다.

3. 기본 키 서버를 수정하여 보조 키 서버를 추가합니다. 그만큼 `-secondary-key-servers` 매개변수는 최대 3개의 주요 서버를 쉼표로 구분하여 나열할 수 있습니다.

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - 보조 키 서버에 대한 포트 번호를 포함하지 마십시오. `-secondary-key-servers` 매개변수. 기본 키 서버와 동일한 포트 번호를 사용합니다.

   > 실행 중이라면 `security key-manager external` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다. NetApp 두 클러스터 모두에서 동일한 키 서버를 사용할 것을 강력히 권장합니다.

기존 기본 키 서버에 보조 키 서버를 추가합니다

단계

1. 기본 키 서버를 수정하여 보조 키 서버를 추가합니다. 그만큼 `-secondary-key-servers` 매개변수는 최대 3개의 주요 서버를 쉼표로 구분하여 나열할 수 있습니다.

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - 보조 키 서버에 대한 포트 번호를 포함하지 마십시오. `-secondary-key-servers` 매개변수. 기본 키 서버와 동일한 포트 번호를 사용합니다.

실행 중이라면 `security key-manager external modify-server` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다. NetApp 두 클러스터 모두에서 동일한 키 서버를 사용할 것을 강력히 권장합니다.

보조 키 서버에 대한 자세한 내용은 다음을 참조하세요. [mod-secondary].

클러스터링된 키 서버를 수정합니다

보조 키 서버를 추가 및 제거하고, 보조 키 서버의 액세스 순서를 변경하거나, 특정 키 서버의 지정(기본 또는 보조)을 변경하여 클러스터형 외부 키 서버를 수정할 수 있습니다. MetroCluster 구성에서 클러스터된 외부 키 서버를 수정하는 경우 NetApp 두 클러스터에서 동일한 키 서버를 사용할 것을 강력히 권장합니다.

보조 키 서버를 수정합니다

`security key-manager external modify-server`명령의 `-secondary-key-servers` 매개변수를 사용하여 보조 키 서버를 관리합니다. 그만큼 `-secondary-key-servers` 매개변수는 쉼표로 구분된 목록을 허용합니다. 목록에서 보조 키 서버의 지정된 순서는 보조 키 서버의 액세스 순서를 결정합니다. 보조 키 서버가 다른 순서로 입력된 상태에서 `security key-manager external modify-server` 명령을 실행하여 액세스 순서를 수정할 수 있습니다. 보조 키 서버에 대한 포트 번호를 포함하지 마세요.

실행 중이라면 `security key-manager external modify-server` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다.

보조 키 서버를 제거하려면 유지하려는 키 서버를 포함하세요. `-secondary-key-servers` 매개변수를 선택하고 제거하려는 매개변수는 생략합니다. 모든 보조 키 서버를 제거하려면 인수를 사용하세요. `-` , 없음을 의미합니다.

기본 및 보조 키 서버를 변환합니다

다음 단계에 따라 특정 키 서버의 지정(기본 또는 보조)을 변경할 수 있습니다.

기본 키 서버를 보조 키 서버로 변환

단계

1. SVM에서 기본 키 서버를 제거합니다.

```
security key-manager external remove-servers
```

> 실행 중이라면 `security key-manager external remove-servers` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다.

2. 수행하다클러스터링된 키 서버를 생성합니다 이전 기본 키 서버를 보조 키 서버로 사용하는 절차입니다.

보조 키 서버를 기본 키 서버로 변환

단계

1. 기존 기본 키 서버에서 보조 키 서버를 제거합니다.

```
security key-manager external modify-server -secondary-key-servers
```

- 실행 중이라면 `security key-manager external modify-server -secondary-key-servers` MetroCluster 구성에서 관리 SVM에 대한 명령을 실행하려면 두 클러스터에서 모두 명령을 실행해야 합니다. 개별 데이터 SVM에 대해 명령을 실행하는 경우 두 클러스터 모두에서 명령을 실행할 필요는 없습니다.
- 기존 키 서버를 제거하는 동안 보조 키 서버를 기본 키 서버로 변환하는 경우, 제거 및 변환을 완료하기 전에 새 키 서버를 추가하려고 하면 키 중복이 발생할 수 있습니다.

1. 수행하다클러스터링된 키 서버를 생성합니다 이전 보조 키 서버를 새로운 클러스터형 키 서버의 기본 키 서버로 사용하는 절차입니다.

참조하다[mod-secondary] 자세한 내용은.

관련 정보

- 자세히 알아보세요 `security key-manager external` 에서"ONTAP 명령 참조입니다"

ONTAP 9.6 이상에서 인증 키를 생성합니다

'Security key-manager key create' 명령을 사용하여 노드의 인증 키를 생성한 후 구성된 KMIP 서버에 저장할 수 있습니다.

이 작업에 대해

보안 설정에서 데이터 인증과 FIPS 140-2 인증을 위해 다른 키를 사용해야 하는 경우 각각에 대해 별도의 키를 만들어야 합니다. 그렇지 않은 경우 데이터 액세스에 사용하는 것과 동일한 인증 키를 FIPS 규정 준수에 사용할 수 있습니다.

ONTAP은 클러스터의 모든 노드에 대해 인증 키를 생성합니다.

- Onboard Key Manager가 활성화된 경우 이 명령은 지원되지 않습니다. 그러나 Onboard Key Manager가

활성화되면 두 개의 인증 키가 자동으로 생성됩니다. 키는 다음 명령을 사용하여 볼 수 있습니다.

```
security key-manager key query -key-type NSE-AK
```

- 구성된 키 관리 서버가 이미 128개 이상의 인증 키를 저장하고 있으면 경고가 표시됩니다.
- 사용하여명령을 수 `security key-manager key delete` 사용하지 않는 키를 삭제할 있습니다. `security key-manager key delete`지정된 키가 현재 ONTAP에서 사용 중인 경우 명령이 실패합니다. (이 명령을 사용하려면 보다 큰 `Privileges`가 있어야 `admin` 합니다.)

> MetroCluster 환경에서 키를 삭제하기 전에 키가 파트너 클러스터에서 사용되고 있지 않은지 확인해야 합니다. 파트너 클러스터에서 다음 명령을 사용하여 키가 사용되고 있지 않은지 확인할 수 있습니다.
>
> - `storage encryption disk show -data-key-id <key-id>`
> - `storage encryption disk show -fips-key-id <key-id>`

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 클러스터 노드의 인증 키를 생성합니다.

```
security key-manager key create -key-tag <passphrase_label> -prompt-for
-key true|false
```

> 설정을 `prompt-for-key=true` 사용하면 클러스터 관리자에게 암호화된 드라이브를 인증할 때 사용할 암호를 묻는 메시지가 표시됩니다. 그렇지 않으면 시스템이 자동으로 32바이트 암호를 생성합니다. `security key-manager key create`명령이 `security key-manager create-key` 명령을 대체합니다. 에 대한 자세한 내용은 `security key-manager key create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예제에서는 32바이트 암호를 자동으로 생성하는 "cluster1"에 대한 인증 키를 만듭니다.

```
cluster1::> security key-manager key create
Key ID: <id_value>
```

2. 인증 키가 생성되었는지 확인합니다.

```
security key-manager key query -node node
```

`security key-manager key query`명령이 `security key-manager query key` 명령을 대체합니다.

출력에 표시되는 키 ID는 인증 키를 참조하는 데 사용되는 식별자입니다. 실제 인증 키 또는 데이터 암호화 키가 아닙니다.

다음 예제에서는 "cluster1"에 대해 인증 키가 생성되었는지 확인합니다.

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID: <id_value>
node1                                    NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID: <id_value>
node2                                    NSE-AK    yes
    Key ID: <id_value>
```

에 대한 자세한 내용은 `security key-manager key query` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "저장 암호화 디스크 표시"

ONTAP 9.5 이전 버전에서 인증 키를 만듭니다

'Security key-manager create-key' 명령을 사용하여 노드의 인증 키를 생성한 후 구성된 KMIP 서버에 저장할 수 있습니다.

이 작업에 대해

보안 설정에서 데이터 인증과 FIPS 140-2 인증을 위해 다른 키를 사용해야 하는 경우 각각에 대해 별도의 키를 만들어야 합니다. 그렇지 않은 경우 데이터 액세스에 사용하는 FIPS 준수에 동일한 인증 키를 사용할 수 있습니다.

ONTAP은 클러스터의 모든 노드에 대해 인증 키를 생성합니다.

- 온보드 키 관리가 활성화된 경우 이 명령은 지원되지 않습니다.
- 구성된 키 관리 서버가 이미 128개 이상의 인증 키를 저장하고 있으면 경고가 표시됩니다.

  키 관리 서버 소프트웨어를 사용하여 사용하지 않는 키를 삭제한 다음 명령을 다시 실행할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 클러스터 노드의 인증 키를 생성합니다.

   보안 키 관리자 만들기 키

   에 대한 자세한 내용은 `security key-manager create-key` "ONTAP 명령 참조입니다"을 참조하십시오.

   > 출력에 표시되는 키 ID는 인증 키를 참조하는 데 사용되는 식별자입니다. 실제 인증 키 또는 데이터 암호화 키가 아닙니다.

   다음 예제에서는 "cluster1"에 대한 인증 키를 만듭니다.

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: <id_value>

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. 인증 키가 생성되었는지 확인합니다.

   보안 키 관리자 쿼리

   에 대한 자세한 내용은 `security key-manager query` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예제에서는 "cluster1"에 대해 인증 키가 생성되었는지 확인합니다.

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-01     NSE-AK    yes
       Key ID: <id_value>


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID: <id_value>
```

ONTAP 외부 키 관리를 사용하여 **FIPS** 드라이브 또는 **SED**에 데이터 인증 키 할당

'스토리지 암호화 디스크 수정' 명령을 사용하여 데이터 인증 키를 FIPS 드라이브 또는 SED에 할당할 수 있습니다. 클러스터 노드는 이 키를 사용하여 드라이브에서 암호화된 데이터를 잠그거나 잠금 해제합니다.

이 작업에 대해

자체 암호화 드라이브는 인증 키 ID가 기본값이 아닌 값으로 설정된 경우에만 무단 액세스로부터 보호됩니다. 키 ID 0x0이 있는 제조업체 보안 ID(MSID)는 SAS 드라이브의 표준 기본값입니다. NVMe 드라이브의 경우 표준 기본값은 빈 키 ID로 표시되는 null 키입니다. 키 ID를 자체 암호화 드라이브에 할당하면 시스템은 해당 인증 키 ID를 기본값이 아닌 값으로 변경합니다.

이 절차는 중단되지 않습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. FIPS 드라이브 또는 SED에 데이터 인증 키 할당:

   'Storage encryption disk modify -disk_disk_ID_-data-key-id_key_ID_'

   에 대한 자세한 내용은 `storage encryption disk modify` "ONTAP 명령 참조입니다"을 참조하십시오.

'Security key-manager query-key-type NSE-AK' 명령어를 이용하여 키 ID를 확인할 수 있다.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
<id_value>

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. 인증 키가 할당되었는지 확인합니다.

   스토리지 암호화 디스크 표시

   에 대한 자세한 내용은 `storage encryption disk show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
[...]
```

관련 정보

- "저장 암호화 디스크 표시"
- "저장 암호화 디스크 표시 상태"

온보드 키 관리를 구성합니다

ONTAP 9.6 이상에서 온보드 키 관리를 활성화합니다

Onboard Key Manager를 사용하여 FIPS 드라이브 또는 SED에 대한 클러스터 노드를 인증할 수 있습니다. Onboard Key Manager는 데이터와 동일한 스토리지 시스템의 노드에 인증 키를 제공하는 기본 제공 도구입니다. Onboard Key Manager는 FIPS-140-2 레벨 1을 준수합니다.

Onboard Key Manager를 사용하여 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 암호화된 볼륨 또는 자체 암호화 디스크에 액세스하는 각 클러스터에서 Onboard Key Manager를 활성화해야 합니다.

이 작업에 대해

클러스터에 노드를 추가할 때마다 보안 키 관리자 온보드 활성화 명령을 실행해야 합니다. MetroCluster 구성에서는 먼저 로컬 클러스터에서 보안 키 관리자 온보드 활성화를 실행한 다음 원격 클러스터에서 동일한 암호를 사용하여 보안 키 관리자 온보드 동기화를 실행해야 합니다.

자세히 알아보세요 `security key-manager onboard enable` 그리고 `security key-manager onboard sync` 에서"ONTAP 명령 참조입니다" .

기본적으로 노드를 재부팅할 때는 키 관리자 암호를 입력할 필요가 없습니다. MetroCluster를 제외하고, 사용자가 재부팅 후 암호문을 입력하도록 'cc-mode-enabled=yes' 옵션을 사용할 수 있습니다.

Common Criteria 모드('cc-mode-enabled=yes')에서 Onboard Key Manager를 활성화하면 다음과 같은 방식으로 시스템 동작이 변경됩니다.

- 시스템은 Common Criteria 모드에서 작동 중일 때 연속 실패한 클러스터 암호 시도를 모니터링합니다.

  NSE(NetApp 스토리지 암호화)가 활성화되어 있고 부팅 시 올바른 클러스터 암호를 입력하지 않으면 시스템이 드라이브를 인증할 수 없고 자동으로 재부팅됩니다. 이 문제를 해결하려면 부팅 프롬프트에서 올바른 클러스터 암호를 입력해야 합니다. 시스템이 부팅되면 24시간 동안 클러스터 암호를 매개 변수로 요구하는 명령에 대해 최대 5회 연속 클러스터 암호를 올바르게 입력할 수 있습니다. 제한에 도달한 경우(예: 클러스터 암호를 5회 연속으로 올바르게 입력하지 않은 경우) 24시간 제한 시간이 경과할 때까지 기다리거나 노드를 재부팅하여 제한을 재설정해야 합니다.

- 시스템 이미지 업데이트는 NetApp RSA-3072 코드 서명 인증서와 SHA-384 코드 서명 다이제스트를 함께 사용하여 일반적인 NetApp RSA-2048 코드 서명 인증서와 SHA-256 코드 서명 다이제스트 대신 이미지 무결성을 확인합니다.

  업그레이드 명령은 다양한 디지털 서명을 검사하여 이미지 내용이 변경되거나 손상되지 않았는지 확인합니다. 검증이 성공하면 이미지 업데이트는 다음 단계로 진행됩니다. 검증이 실패하면 이미지 업데이트가 실패합니다. 자세히 알아보세요 `cluster image` 에서"ONTAP 명령 참조입니다" .

Onboard Key Manager는 휘발성 메모리에 키를 저장합니다. 시스템을 재부팅하거나 정지하면 휘발성 메모리 내용이 지워집니다. 정상적인 작동 조건에서는 시스템을 정지하면 30초 이내에 휘발성 메모리 콘텐츠가 지워집니다.

시작하기 전에

- NSE를 외부 키 관리(KMIP) 서버와 함께 사용할 경우 외부 키 관리자 데이터베이스를 삭제해야 합니다.

  "외부 키 관리에서 온보드 키 관리로 전환"

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- Onboard Key Manager를 구성하기 전에 MetroCluster 환경을 구성해야 합니다.

단계

1. 키 관리자 설정 명령을 시작합니다.

   '보안 키 관리자 온보드 활성화-cc-모드 사용 예|아니오'

   `cc-mode-enabled=yes`재부팅 후 사용자가 키 관리자 암호를 입력하도록 요구하도록 설정합니다. `- cc-mode-enabled`MetroCluster 구성에서는 옵션이 지원되지 않습니다. `security key-manager onboard enable`명령이 `security key-manager setup` 명령을 대체합니다.

   다음 예제에서는 재부팅할 때마다 암호를 입력할 필요 없이 키 관리자 설치 명령을 cluster1에서 시작합니다.

2. 32~256자 사이의 암호를 입력하세요. "`cc-mode`"의 경우 64~256자 사이의 암호를 입력하세요.

지정된 ""cc-mode"" 암호가 64자 미만이면 키 관리자 설정 작업에 암호 프롬프트가 다시 표시되기 전에 5초의 지연이 발생합니다.

3. 암호 확인 프롬프트에서 암호를 다시 입력합니다.
4. 시스템이 인증 키를 생성하는지 확인하세요.

   '보안 키 관리자 키 쿼리 노드

   `security key-manager key query`명령이 `security key-manager query key` 명령을 대체합니다.

   에 대한 자세한 내용은 `security key-manager key query` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

나중에 사용할 수 있도록 암호를 스토리지 시스템 외부의 안전한 위치에 복사합니다.

시스템은 클러스터의 복제된 데이터베이스(RDB)에 주요 관리 정보를 자동으로 백업합니다. 재해 복구를 위해 이 정보를 수동으로 백업해야 합니다.

관련 정보

- "클러스터 이미지 명령"
- "보안 키 관리자 외부 활성화"
- "보안 키 관리자 키 쿼리"
- "보안 키 관리자 온보드 활성화"
- "외부 키 관리에서 온보드 키 관리로 전환"

ONTAP 9.5 이전 버전에서 온보드 키 관리를 활성화합니다

Onboard Key Manager를 사용하여 FIPS 드라이브 또는 SED에 대한 클러스터 노드를 인증할 수 있습니다. Onboard Key Manager는 데이터와 동일한 스토리지 시스템의 노드에 인증 키를 제공하는 기본 제공 도구입니다. Onboard Key Manager는 FIPS-140-2 레벨 1을 준수합니다.

온보드 키 관리자를 사용하면 클러스터가 암호화된 데이터에 액세스하는 데 사용하는 키를 보호할 수 있습니다. 암호화된 볼륨이나 자체 암호화 디스크에 액세스하는 각 클러스터에서 Onboard Key Manager를 활성화합니다.

이 작업에 대해

클러스터에 노드를 추가할 때마다 보안 키 관리자 설정 명령을 실행해야 합니다.

MetroCluster 구성이 있는 경우 다음 지침을 검토하십시오.

- ONTAP 9.5에서는 로컬 클러스터에서 보안 키 관리자 설정, 원격 클러스터에서 보안 키 관리자 설정 -동기화 -MetroCluster -구성 예 를 각각 동일한 암호를 사용하여 실행해야 합니다.
- ONTAP 9.5 이전에는 로컬 클러스터에서 보안 키 관리자 설정을 실행하고 약 20초 정도 기다린 다음 원격 클러스터에서 동일한 암호를 사용하여 보안 키 관리자 설정을 실행해야 합니다.

기본적으로 노드를 재부팅할 때는 키 관리자 암호를 입력할 필요가 없습니다. ONTAP 9.4부터 '-enable-cc-mode yes'

옵션을 사용하여 재부팅 후 사용자가 암호를 입력하도록 할 수 있습니다.

NVE의 경우 '-enable-cc-mode yes'를 설정하면 볼륨 생성 및 볼륨 이동 시작 명령으로 생성한 볼륨이 자동으로 암호화됩니다. 볼륨 만들기에는 -encrypt true를 지정할 필요가 없습니다. 볼륨 이동 시작의 경우 -encrypt-destination true를 지정하지 않아도 됩니다.

실패한 암호 구문을 시도한 후에는 노드를 다시 재부팅해야 합니다.

시작하기 전에

- 외부 키 관리(KMIP) 서버와 함께 NSE를 사용하는 경우 외부 키 관리자 데이터베이스를 삭제하세요.

  "외부 키 관리에서 온보드 키 관리로 전환"

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- Onboard Key Manager를 구성하기 전에 MetroCluster 환경을 구성하세요.

단계

1. 키 관리자 설정을 시작합니다.

   '보안 키 관리자 설정-활성화-cc-모드 예|아니오'

   ONTAP 9.4부터는 사용자가 재부팅 후 키 관리자 암호를 입력하도록 하는 '-enable-cc-mode yes' 옵션을 사용할 수 있습니다. NVE의 경우 '-enable-cc-mode yes'를 설정하면 볼륨 생성 및 볼륨 이동 시작 명령으로 생성한 볼륨이 자동으로 암호화됩니다.

   다음 예제에서는 재부팅할 때마다 암호를 입력할 필요 없이 키 관리자를 cluster1에서 설정하기 시작합니다.

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. 온보드 키 관리를 구성하라는 메시지가 나타나면 "예"를 입력합니다.
3. 암호문 프롬프트에서 32자에서 256자 사이의 암호문을 입력하거나 64에서 256자 사이의 암호문을 "cc-mode"로 입력합니다.

   지정된 ""cc-mode"" 암호가 64자 미만이면 키 관리자 설정 작업에 암호 프롬프트가 다시 표시되기 전에 5초의 지연이 발생합니다.

4. 암호 확인 프롬프트에서 암호를 다시 입력합니다.
5. 모든 노드에 대해 키가 구성되었는지 확인합니다.

   `security key-manager show-key-store`

   자세히 알아보세요 `security key-manager show-key-store` 에서"ONTAP 명령 참조입니다" .

```
cluster1::> security key-manager show-key-store

Node: node1
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

작업을 마친 후

ONTAP 클러스터의 복제된 데이터베이스(RDB)에 주요 관리 정보를 자동으로 백업합니다.

온보드 키 관리자 암호를 구성한 후에는 해당 정보를 저장 시스템 외부의 안전한 위치에 수동으로 백업하세요. 보다 "온보드 키 관리 정보를 수동으로 백업합니다" .

관련 정보

- "온보드 키 관리 정보를 수동으로 백업합니다"
- "보안 키 관리자 설정"
- "보안 키 관리자 show-key-store"
- "외부 키 관리에서 온보드 키 관리로 전환"

ONTAP 온보드 키 관리를 사용하여 **FIPS** 드라이브 또는 **SED**에 데이터 인증 키 할당

'스토리지 암호화 디스크 수정' 명령을 사용하여 데이터 인증 키를 FIPS 드라이브 또는 SED에 할당할 수 있습니다. 클러스터 노드는 이 키를 사용하여 드라이브의 데이터에 액세스합니다.

이 작업에 대해

자체 암호화 드라이브는 인증 키 ID가 기본값이 아닌 값으로 설정된 경우에만 무단 액세스로부터 보호됩니다. 키 ID 0x0이 있는 제조업체 보안 ID(MSID)는 SAS 드라이브의 표준 기본값입니다. NVMe 드라이브의 경우 표준 기본값은 빈

키 ID로 표시되는 null 키입니다. 키 ID를 자체 암호화 드라이브에 할당하면 시스템은 해당 인증 키 ID를 기본값이 아닌 값으로 변경합니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. FIPS 드라이브 또는 SED에 데이터 인증 키 할당:

   'Storage encryption disk modify -disk_disk_ID_-data-key-id_key_ID_'

   에 대한 자세한 내용은 `storage encryption disk modify` "ONTAP 명령 참조입니다"을 참조하십시오.

   'Security key-manager key query-key-type NSE-AK' 명령어를 이용하여 키 ID를 확인할 수 있다.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   에 대한 자세한 내용은 `security key-manager key query` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 인증 키가 할당되었는지 확인합니다.

   스토리지 암호화 디스크 표시

   에 대한 자세한 내용은 `storage encryption disk show` "ONTAP 명령 참조입니다"을 참조하십시오.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   [...]
   ```

관련 정보

- "저장 암호화 디스크 표시"
- "저장 암호화 디스크 표시 상태"

ONTAP FIPS 드라이브에 **FIPS 140-2** 인증 키 할당

'-FIPS-key-id' 옵션과 함께 'storage encryption disk modify' 명령을 사용하여 FIPS 140-2

인증 키를 FIPS 드라이브에 할당할 수 있습니다. 클러스터 노드는 드라이브에 대한 서비스 거부 공격을 방지하는 것과 같이 데이터 액세스 이외의 드라이브 작업에 이 키를 사용합니다.

이 작업에 대해

보안 설정에서 데이터 인증과 FIPS 140-2 인증을 위해 다른 키를 사용해야 할 수 있습니다. 그렇지 않은 경우 데이터 액세스에 사용하는 FIPS 준수에 동일한 인증 키를 사용할 수 있습니다.

이 절차는 중단되지 않습니다.

시작하기 전에

드라이브 펌웨어는 FIPS 140-2 규정 준수를 지원해야 합니다. 를 클릭합니다 "NetApp 상호 운용성 매트릭스 툴" 지원되는 드라이브 펌웨어 버전에 대한 정보를 제공합니다.

단계

1. 먼저 데이터 인증 키를 할당했는지 확인해야 합니다. 이 작업은 를 사용하여 수행할 수 있습니다 외부 키 관리자 또는 을 누릅니다 Onboard Key Manager(온보드 키 관리자. 'storage encryption disk show' 명령을 사용하여 키가 할당되었는지 확인합니다.
2. SED에 FIPS 140-2 인증 키 할당:

   'Storage encryption disk modify -disk_disk_id_-FIPS-key-id_FIPS_authentication_key_id_'

   '보안 키 관리자 쿼리' 명령을 사용하여 키 ID를 볼 수 있습니다.

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

3. 인증 키가 할당되었는지 확인합니다.

   스토리지 암호화 디스크 show-FIPS

   에 대한 자세한 내용은 `storage encryption disk show` "ONTAP 명령 참조입니다"을 참조하십시오.

   ```
   cluster1::> storage encryption disk show -fips
   Disk    Mode FIPS-Compliance Key ID
   ------  ----
   ------------------------------------------------------------------
   2.10.0  full <id_value>
   2.10.1  full <id_value>
   [...]
   ```

관련 정보

- "저장 암호화 디스크 수정"
- "저장 암호화 디스크 표시"
- "저장 암호화 디스크 표시 상태"

ONTAP에서 **KMIP** 서버 연결을 위해 클러스터 차원의 **FIPS** 호환 모드를 사용하도록 설정합니다

'보안 구성 수정' 명령을 -FIPS 사용' 옵션과 함께 사용하면 전송 중인 데이터에 대해 클러스터 차원의 FIPS 호환 모드를 사용할 수 있습니다. 이렇게 하면 클러스터가 KMIP 서버에 연결할 때 FIPS 모드에서 OpenSSL을 사용하게 됩니다.

이 작업에 대해

클러스터 전반의 FIPS 호환 모드를 사용하도록 설정하면 클러스터에서 TLS1.2 및 FIPS 인증 암호 그룹만 자동으로 사용됩니다. 클러스터 차원의 FIPS 호환 모드는 기본적으로 해제되어 있습니다.

클러스터 전체 보안 구성을 수정한 후에는 클러스터 노드를 수동으로 재부팅해야 합니다.

시작하기 전에

- 스토리지 컨트롤러는 FIPS 호환 모드로 구성해야 합니다.
- 모든 KMIP 서버는 TLSv1.2를 지원해야 합니다. TLSv1.2는 클러스터 차원의 FIPS 호환 모드가 활성화된 경우 KMIP 서버에 대한 연결을 완료해야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. TLSv1.2가 지원되는지 확인합니다.

   '보안 설정 표시 - 지원 - 프로토콜'

   에 대한 자세한 내용은 `security config show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. 클러스터 전체 FIPS 호환 모드 사용:

   보안 설정 수정 - FIPS 활성화 True-Interface SSL

에 대한 자세한 내용은 `security config modify` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 클러스터 노드를 수동으로 재부팅합니다.
5. 클러스터 차원에서 FIPS 호환 모드가 활성화되어 있는지 확인합니다.

   '보안 구성 쇼'

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                              !aNULL:!EXP:
                                              !eNULL:!RC4
```

NetApp 암호화 관리

ONTAP에서 볼륨 데이터의 암호화를 해제합니다

볼륨 이동 시작 명령을 사용하여 볼륨 데이터를 이동하거나 암호화 해제할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 암호화된 기존 볼륨을 이동하고 볼륨의 데이터를 암호화 해제합니다.

   `volume move start -vserver` *`SVM_name`* `-volume volume_name -destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

   에 대한 자세한 내용은 `volume move start` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 이름이 "vol1"인 기존 볼륨이 대상 애그리게이트 "aggr3"으로 이동하고 볼륨의 데이터 암호화를 해제합니다.

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr3 -encrypt-destination false
```

   볼륨에 대한 암호화 키가 삭제됩니다. 볼륨의 데이터가 암호화되지 않습니다.

2. 볼륨에 암호화가 비활성화되어 있는지 확인합니다.

볼륨 표시 암호화

에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 'cluster1'의 볼륨이 암호화되는지 여부가 표시됩니다.

```
cluster1::> volume show -encryption

Vserver  Volume    Aggregate    State     Encryption State
-------  ------    ---------    -----     ----------------
vs1      vol1      aggr1        online    none
```

ONTAP에서 암호화된 볼륨을 이동합니다

'volume move start' 명령을 사용하여 암호화된 볼륨을 이동할 수 있습니다. 이동된 볼륨은 동일한 애그리게이트 또는 다른 애그리게이트에 있을 수 있습니다.

이 작업에 대해

대상 노드 또는 대상 볼륨이 볼륨 암호화를 지원하지 않으면 이동이 실패합니다.

를 클릭합니다 `-encrypt-destination` 의 옵션입니다 `volume move start` 암호화된 볼륨의 경우 기본적으로 true입니다. 대상 볼륨을 암호화하지 않도록 지정해야 하는 요구 사항은 볼륨의 데이터를 실수로 암호화 해제하지 않도록 합니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 암호화된 기존 볼륨을 이동하고 볼륨의 데이터를 암호화된 상태로 유지:

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`*

   에 대한 자세한 내용은 `volume move start` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 이름이 "vol1"인 기존 볼륨이 대상 애그리게이트 "aggr3"으로 이동하고 볼륨의 데이터가 암호화된 상태로 유지됩니다.

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. 볼륨에 암호화가 활성화되어 있는지 확인합니다.

   볼륨 쇼는 암호화된 사실이다

   에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 암호화된 볼륨이 'cluster1'에 표시됩니다.

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
```

ONTAP에서 **volume encryption key start** 명령을 사용하여 볼륨의 암호화 키를 변경합니다

볼륨의 암호화 키를 정기적으로 변경하는 것이 가장 좋은 방법입니다. ONTAP 9.3부터는 '볼륨 암호화 키 다시 시작' 명령을 사용하여 암호화 키를 변경할 수 있습니다.

이 작업에 대해

키를 다시 입력하다 이전 키로 되돌릴 수 없습니다. 작업 중에 성능 문제가 발생하면 '볼륨 암호화 일시 중지' 명령을 실행하여 작업을 일시 중지하고 '볼륨 암호화 다시 시작' 명령을 실행하여 작업을 다시 시작할 수 있습니다.

키를 다시 입력하다 새 쓰기 및 해당 읽기에서 새 키가 사용됩니다. 그렇지 않으면 읽기에서 이전 키를 사용합니다.

ⓘ SnapLock 볼륨을 다시 입력하다

단계

1. 암호화 키 변경:

   '볼륨 암호화 키 다시 시작 - SVM_NAME - volume volume volume_name'

   다음 명령을 실행하면 SVM의 vol1에 대한 암호화 키가 VS1 로 변경됩니다.

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. 키를 다시 입력하다

   볼륨 암호화 키를 다시 입력하다

   에 대한 자세한 내용은 `volume encryption rekey show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 키를 다시 입력하다

   ```
   cluster1::> volume encryption rekey show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ---------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. 키를 다시 입력하다

   볼륨 쇼는 암호화된 사실이다

   에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 암호화된 볼륨이 'cluster1'에 표시됩니다.

```
cluster1::> volume show -is-encrypted true

Vserver   Volume   Aggregate   State   Type   Size   Available   Used
-------   ------   ---------   -----   ----   -----   ---------  ----
vs1       vol1     aggr2      online     RW   200GB     160.0GB   20%
```

ONTAP 볼륨 이동 시작 명령을 사용하여 볼륨의 암호화 키를 변경합니다.

볼륨의 암호화 키를 정기적으로 변경하는 것이 가장 좋은 방법입니다. 명령을 사용하여 암호화 키를 변경할 수 `volume move start` 있습니다. 이동된 볼륨은 동일한 애그리게이트 또는 다른 애그리게이트에 있을 수 있습니다.

이 작업에 대해

SnapLock 또는 FlexGroup 볼륨을 다시 입력하다

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 기존 볼륨을 이동하고 암호화 키를 변경합니다.

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

   에 대한 자세한 내용은 `volume move start` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 이름이 ' * vol1 * '인 기존 볼륨이 대상 집합 ' * aggr2 * '로 이동하고 암호화 키가 변경됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -generate-destination-key true
```

   볼륨에 대한 새 암호화 키가 생성됩니다. 볼륨의 데이터는 암호화된 상태로 유지됩니다.

2. 볼륨에 암호화가 활성화되어 있는지 확인합니다.

   볼륨 쇼는 암호화된 사실이다

   에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 암호화된 볼륨이 'cluster1'에 표시됩니다.

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2      online   RW  200GB    160.0GB  20%
```

ONTAP NetApp 스토리지 암호화를 위한 인증 키 순환

NSE(NetApp Storage Encryption)를 사용할 때 인증 키를 회전할 수 있습니다.

이 작업에 대해

NSE 환경에서 인증 키를 회전하면 외부 키 관리자(KMIP)를 사용할 수 있습니다.

NSE 환경에서 인증 키를 회전하면 온보드 키 관리자(OKM)가 지원되지 않습니다.

단계

1. Security key-manager create-key 명령을 사용하여 새 인증 키를 생성합니다.

   인증 키를 변경하려면 먼저 새 인증 키를 생성해야 합니다.

2. 'storage encryption disk modify -disk * -data-key-id' 명령어를 이용하여 인증 키를 변경한다.

관련 정보

- "저장 암호화 디스크 수정"

ONTAP에서 암호화된 볼륨을 삭제합니다

'volume delete' 명령을 사용하여 암호화된 볼륨을 삭제할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 볼륨이 오프라인 상태여야 합니다.

단계

1. 암호화된 볼륨 삭제:

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

   에 대한 자세한 내용은 `volume delete` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 이름이 "vol1"인 암호화된 볼륨이 삭제됩니다.

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

삭제를 확인하는 메시지가 나타나면 '예'를 입력합니다.

24시간 후 볼륨에 대한 암호화 키가 삭제됩니다.

`-force true`옵션을 사용하여 `volume delete` 볼륨을 삭제하고 해당 암호화 키를 즉시 제거합니다. 이 명령을 사용하려면 고급 권한이 필요합니다. 에 대한 자세한 내용은 `volume delete` link:https://docs.netapp.com/us-en/ontap-cli/volume-delete.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

작업을 마친 후

'volume recovery-queue' 명령을 사용하여 'volume delete' 명령을 실행한 후 보존 기간 동안 삭제된 볼륨을 복구할 수 있습니다.

`volume recovery-queue` *`SVM_name`* `-volume` *`volume_name`*

"볼륨 복구 기능 사용 방법"

암호화된 볼륨에서 데이터를 안전하게 제거합니다

암호화된 **ONTAP** 볼륨에서 데이터를 안전하게 제거하는 방법에 대해 알아보세요.

ONTAP 9.4부터 보안 제거를 사용하여 NVE 지원 볼륨에서 데이터를 중단 없이 스크럽할 수 있습니다. 암호화된 볼륨에 데이터를 스크러빙하면 물리적 미디어에서 데이터를 복구할 수 없습니다. 예를 들어, 블록 덮어쓰기 시 데이터 추적이 남아 있거나 비어 있는 테넌트의 데이터를 안전하게 삭제하기 위해 "스필지"가 남아 있을 수 있습니다.

Secure Purge는 NVE 지원 볼륨에서 이전에 삭제된 파일에 대해서만 작동합니다. 암호화되지 않은 볼륨은 스크럽 할 수 없습니다. 온보드 키 관리자가 아닌 KMIP 서버를 사용하여 키를 제공해야 합니다.

보안 제거 사용에 대한 고려 사항

- NetApp Aggregate Encryption(NAE)이 활성화된 Aggregate에서 생성된 볼륨은 보안 제거를 지원하지 않습니다.
- Secure Purge는 NVE 지원 볼륨에서 이전에 삭제된 파일에 대해서만 작동합니다.
- 암호화되지 않은 볼륨은 스크럽 할 수 없습니다.
- 온보드 키 관리자가 아닌 KMIP 서버를 사용하여 키를 제공해야 합니다.

ONTAP 버전에 따라 퍼지 기능을 다르게 보호합니다.

ONTAP 9.8 이상

- 보안 삭제는 MetroCluster 및 FlexGroup에서 지원됩니다.
- 제거할 볼륨이 SnapMirror 관계의 소스인 경우 보안 제거를 수행하기 위해 SnapMirror 관계를 중단할 필요가 없습니다.
- 재암호화 방법은 SnapMirror 데이터 보호를 사용하는 볼륨과 SnapMirror 데이터 보호(DP)를 사용하지 않는 볼륨 또는 SnapMirror 확장 데이터 보호를 사용하는 볼륨의 경우에 다릅니다.
  - 기본적으로 SnapMirror 데이터 보호(DP) 모드를 사용하는 볼륨은 볼륨 이동 다시 암호화 방법을 사용하여 데이터를 다시 암호화합니다.
  - 기본적으로 SnapMirror 데이터 보호 또는 XDP(SnapMirror Extended Data Protection) 모드를 사용하는 볼륨을 사용하지 않는 볼륨은 데이터 이동 없이 재암호화 방법을 사용합니다.
  - 이러한 기본값은 'secure purge re-encryption-method[volume-move|in-place-키를 다시 입력하다]' 명령을 사용하여 변경할 수 있습니다.
- 기본적으로 FlexVol 볼륨의 모든 스냅샷은 보안 제거 작업 중에 자동으로 삭제됩니다. 기본적으로 FlexGroup 볼륨 및 SnapMirror 데이터 보호를 사용하는 볼륨의 스냅샷은 안전한 삭제 작업 중에 자동으로 삭제되지 않습니다. 이러한 기본값은 명령을 사용하여 변경할 수 `secure purge delete-all-snapshots [true|false]` 있습니다.

ONTAP 9.7 이하**:**

- 보안 퍼지는 다음을 지원하지 않습니다.
  - 플랙스클론
  - SnapVault
  - FabricPool
- 제거할 볼륨이 SnapMirror 관계의 소스인 경우 볼륨을 제거하려면 SnapMirror 관계를 해제해야 합니다.

  볼륨에 사용 중인 스냅샷이 있는 경우 볼륨을 비우기 전에 스냅샷을 해제해야 합니다. 예를 들어, FlexClone 볼륨을 상위 볼륨에서 분할해야 할 수 있습니다.
- 보안 제거 기능을 성공적으로 호출하면 새 키를 사용하여 남아 있는 비퍼지된 데이터를 다시 암호화하는 볼륨 이동이 트리거됩니다.

  이동된 볼륨은 현재 애그리게이트에 있습니다. 이전 키는 자동으로 삭제되므로 삭제된 데이터를 스토리지 미디어에서 복구할 수 없습니다.

SnapMirror 관계 없이 암호화된 **ONTAP** 볼륨에서 데이터 스크럽

ONTAP 9.4부터 안전한 제거를 사용하여 NVE 지원 볼륨에서 중단 없이 "하위" 데이터를 사용할 수 있습니다.

이 작업에 대해

Secure-Purge는 삭제된 파일의 데이터 양에 따라 완료하는 데 몇 분에서 몇 시간까지 걸릴 수 있습니다. 'volume encryption secure-purge show' 명령을 사용하여 작업 상태를 볼 수 있습니다. 'volume encryption secure-purge abort' 명령을 사용하여 작업을 종료할 수 있습니다.

SAN 호스트에서 보안 제거를 수행하려면 제거할 파일이 포함된 전체 LUN을 삭제하거나 제거할 파일에 속한 블록에 대해 LUN에서 구멍을 뚫을 수 있어야 합니다. LUN을 삭제할 수 없거나 호스트 운영 체제에서 LUN의 구멍을 뚫을 수 없는 경우 보안 제거를 수행할 수 없습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 이 작업에는 고급 권한이 필요합니다.

단계

1. 안전하게 제거할 파일 또는 LUN을 삭제합니다.
   - NAS 클라이언트에서 안전하게 제거할 파일을 삭제합니다.
   - SAN 호스트에서 제거할 파일에 속한 블록에 대해 LUN에서 안전하게 지우거나 구멍을 뚫을 LUN을 삭제합니다.
2. 스토리지 시스템에서 고급 권한 레벨로 변경합니다.

   세트 프리빌리지 고급

3. 안전하게 제거할 파일이 스냅샷에 있는 경우 스냅샷을 삭제합니다.

   `snapshot delete -vserver SVM_name -volume volume_name -snapshot`

4. 삭제된 파일을 안전하게 삭제:

   `volume encryption secure-purge start -vserver SVM_name -volume volume_name`

   다음 명령을 실행하면 삭제된 파일이 SVM의 vol1에서 VS1 형식으로 안전하게 삭제됩니다.

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. 보안 제거 작업의 상태를 확인합니다.

   볼륨 암호화 보안 제거 쇼

SnapMirror 비동기 관계를 사용하여 암호화된 **ONTAP** 볼륨에서 데이터 스크럽

ONTAP 9.8부터는 SnapMirror 비동기식 관계를 통해 NVE 지원 볼륨에서 중단 없이 데이터를 "스크럽" 데이터로 안전하게 제거할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 이 작업에는 고급 권한이 필요합니다.

이 작업에 대해

Secure-Purge는 삭제된 파일의 데이터 양에 따라 완료하는 데 몇 분에서 몇 시간까지 걸릴 수 있습니다. 'volume

encryption secure-purge show' 명령을 사용하여 작업 상태를 볼 수 있습니다. 'volume encryption secure-purge abort' 명령을 사용하여 작업을 종료할 수 있습니다.

> SAN 호스트에서 보안 제거를 수행하려면 제거할 파일이 포함된 전체 LUN을 삭제하거나 제거할 파일에 속한 블록에 대해 LUN에서 구멍을 뚫을 수 있어야 합니다. LUN을 삭제할 수 없거나 호스트 운영 체제에서 LUN의 구멍을 뚫을 수 없는 경우 보안 제거를 수행할 수 없습니다.

단계

1. 스토리지 시스템에서 advanced 권한 수준으로 전환합니다.

   세트 프리빌리지 고급

2. 안전하게 제거할 파일 또는 LUN을 삭제합니다.
   - NAS 클라이언트에서 안전하게 제거할 파일을 삭제합니다.
   - SAN 호스트에서 제거할 파일에 속한 블록에 대해 LUN에서 안전하게 지우거나 구멍을 뚫을 LUN을 삭제합니다.
3. 안전하게 제거할 비동기 관계의 대상 볼륨을 준비합니다.

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   SnapMirror 비동기식 관계의 각 볼륨에 대해 이 단계를 반복합니다.

4. 안전하게 제거할 파일이 스냅샷에 있는 경우 스냅샷을 삭제합니다.

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. 안전하게 제거할 파일이 기본 스냅샷에 있는 경우 다음을 수행합니다.

   a. SnapMirror 비동기식 관계에서 대상 볼륨에 스냅샷을 생성합니다.

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. SnapMirror를 업데이트하여 기본 스냅샷을 앞으로 이동합니다.

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   SnapMirror 비동기식 관계의 각 볼륨에 대해 이 단계를 반복합니다.

   a. 기본 스냅샷 수에 1을 더한 것과 같은 (a) 및 (b)단계를 반복합니다.

      예를 들어 기본 스냅샷이 두 개 있는 경우 (a) 및 (b) 단계를 세 번 반복해야 합니다.

   b. 기본 스냅샷이 있는지 확인합니다.
      `snapshot show -vserver SVM_name -volume volume_name`
   c. 기본 스냅샷 삭제:
      `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. 삭제된 파일을 안전하게 삭제:

   `volume encryption secure-purge start -vserver svm_name -volume volume_name`

   SnapMirror 비동기식 관계의 각 볼륨에서 이 단계를 반복합니다.

   다음 명령을 실행하면 삭제된 파일이 SVM의 ""vol1""에서 "vs1""으로 안전하게 삭제됩니다.

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

7. 안전한 퍼지 작업의 상태를 확인합니다.

   볼륨 암호화 보안 제거 쇼

관련 정보

- "스냅미러 업데이트"

SnapMirror 동기 관계를 사용하여 암호화된 **ONTAP** 볼륨에서 데이터 스크럽

ONTAP 9.8부터 SnapMirror 동기식 관계를 통해 NVE 지원 볼륨에서 보안 삭제를 사용하여 중단 없이 데이터를 "스크럽"할 수 있습니다.

이 작업에 대해

삭제된 파일의 데이터 양에 따라 보안 제거를 완료하는 데 몇 분에서 몇 시간까지 걸릴 수 있습니다. 'volume encryption secure-purge show' 명령을 사용하여 작업 상태를 볼 수 있습니다. 'volume encryption secure-purge abort' 명령을 사용하여 작업을 종료할 수 있습니다.

> SAN 호스트에서 보안 제거를 수행하려면 제거할 파일이 포함된 전체 LUN을 삭제하거나 제거할 파일에 속한 블록에 대해 LUN에서 구멍을 뚫을 수 있어야 합니다. LUN을 삭제할 수 없거나 호스트 운영 체제에서 LUN의 구멍을 뚫을 수 없는 경우 보안 제거를 수행할 수 없습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 이 작업에는 고급 권한이 필요합니다.

단계

1. 스토리지 시스템에서 고급 권한 레벨로 변경합니다.

   세트 프리빌리지 고급

2. 안전하게 제거할 파일 또는 LUN을 삭제합니다.
   - NAS 클라이언트에서 안전하게 제거할 파일을 삭제합니다.
   - SAN 호스트에서 제거할 파일에 속한 블록에 대해 LUN에서 안전하게 지우거나 구멍을 뚫을 LUN을 삭제합니다.
3. 안전하게 제거할 비동기 관계의 대상 볼륨을 준비합니다.

```
volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
-prepare true
```

SnapMirror 동기식 관계의 다른 볼륨에 대해 이 단계를 반복합니다.

4. 안전하게 제거할 파일이 스냅샷에 있는 경우 스냅샷을 삭제합니다.

```
snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
```

5. 보안 제거 파일이 기본 스냅샷 또는 공통 스냅샷에 있는 경우 SnapMirror를 업데이트하여 공통 스냅샷을 앞으로 이동합니다.

```
snapmirror update -source-snapshot <snapshot_name> -destination-path
<destination_path>
```

두 개의 일반적인 스냅샷이 있으므로 이 명령을 두 번 실행해야 합니다.

6. 보안 제거 파일이 애플리케이션 정합성 보장 스냅샷에 있는 경우 SnapMirror 동기식 관계에서 두 볼륨의 스냅샷을 삭제합니다.

```
snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
```

두 볼륨에서 이 단계를 수행합니다.

7. 삭제된 파일을 안전하게 삭제:

```
volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
```

SnapMirror 동기식 관계의 각 볼륨에 대해 이 단계를 반복합니다.

다음 명령을 실행하면 삭제된 파일이 SVM ""VS1""의 ""vol1""에서 안전하게 삭제됩니다.

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

8. 안전한 퍼지 작업의 상태를 확인합니다.

볼륨 암호화 보안 제거 쇼

관련 정보

- "스냅미러 업데이트"

ONTAP 온보드 키 관리 암호문구 변경

NetApp 온보드 키 관리 암호를 정기적으로 변경할 것을 권장합니다. 새로운 암호문구는 저장 시스템 외부의 안전한 장소에 저장해야 합니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

- 이 작업에는 고급 권한이 필요합니다.
- MetroCluster 환경에서 로컬 클러스터에서 암호를 업데이트한 후 파트너 클러스터에서 암호 업데이트를 동기화합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 온보드 키 관리 암호를 변경합니다. 사용하는 명령은 실행 중인 ONTAP 버전에 따라 달라집니다.

   ONTAP 9.6 이상

   보안 키 관리자 온보드 업데이트 암호문

   ONTAP 9.5 이하

   보안 키 관리자 업데이트 암호문

3. 32~256자 사이의 암호를 입력하세요. "`cc-mode`"의 경우 64~256자 사이의 암호를 입력하세요.

   지정된 ""cc-mode"" 암호가 64자 미만이면 키 관리자 설정 작업에 암호 프롬프트가 다시 표시되기 전에 5초의 지연이 발생합니다.

4. 암호 확인 프롬프트에서 암호를 다시 입력합니다.
5. MetroCluster 구성을 사용하는 경우 파트너 클러스터에서 업데이트된 암호를 동기화하세요.
   a. ONTAP 버전에 맞는 올바른 명령을 선택하여 파트너 클러스터에서 암호를 동기화하세요.

      ONTAP 9.6 이상

      ```
      security key-manager onboard sync
      ```

      ONTAP 9.5 이하

      - ONTAP 9.5에서 다음을 실행합니다.

        ```
        security key-manager setup -sync-metrocluster-config
        ```

      - ONTAP 9.4 및 이전 버전에서는 로컬 클러스터에서 암호를 업데이트한 후 20초간 기다린 후 파트너 클러스터에서 다음 명령을 실행합니다.

        보안 키 관리자 설정

   b. 메시지가 나타나면 새로운 암호를 입력하세요.

      두 클러스터 모두에서 동일한 암호를 사용해야 합니다.

작업을 마친 후

나중에 사용할 수 있도록 온보드 키 관리 암호를 저장 시스템 외부의 안전한 위치에 복사합니다.

온보드 키 관리 암호를 변경할 때마다 키 관리 정보를 수동으로 백업하세요.

관련 정보

- "온보드 키 관리 정보를 수동으로 백업합니다"
- "보안 키 관리자 온보드 업데이트 암호 구문"

ONTAP 온보드 키 관리 정보를 수동으로 백업하세요**.**

Onboard Key Manager 암호를 구성할 때마다 온보드 키 관리 정보를 스토리지 시스템 외부의 안전한 위치에 복사해야 합니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 이 작업에는 고급 권한이 필요합니다.

이 작업에 대해

모든 키 관리 정보는 클러스터의 복제된 데이터베이스(RDB)에 자동으로 백업됩니다. 또한 재해 발생 시 사용할 수 있도록 키 관리 정보를 수동으로 백업해야 합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 클러스터의 키 관리 백업 정보를 표시합니다.

이 ONTAP 버전의 경우…	이 명령 사용…
ONTAP 9.6 이상	보안 키 관리자 온보드 쇼 백업
ONTAP 9.5 이하	보안 키 관리자 백업 쇼

   다음 9.6 명령은 키 관리 백업 정보를 표시합니다. `cluster1` :

```
cluster1::> security key-manager onboard show-backup

     -------------------------BEGIN BACKUP-------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
     IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

시작하기 전에

- 외부 KMIP 서버와 함께 NSE를 사용하는 경우 외부 키 관리자 데이터베이스를 삭제합니다. 자세한 내용은 다음을 참조하세요."외부 키 관리에서 ONTAP 온보드 키 관리로 전환" .
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

Flash Cache 모듈이 있는 시스템에서 NSE를 사용하는 경우, NVE 또는 NAE도 활성화해야 합니다. NSE는 Flash Cache 모듈에 상주하는 데이터를 암호화하지 않습니다.

ONTAP 9.6 이상

ONTAP 9.8 이상을 실행 중이고 루트 볼륨이 암호화된 경우 에 대한 절차를 따릅니다 [ontap-9-8].

1. 키를 복원해야 하는지 확인합니다. +'보안 키 관리자 키 쿼리 - node_node_'

   에 대한 자세한 내용은 `security key-manager key query` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 키 복원: + '보안 키 관리자 온보드 동기화

   에 대한 자세한 내용은 `security key-manager onboard sync` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 암호 프롬프트에서 클러스터의 온보드 키 관리 암호를 입력합니다.

암호화된 루트 볼륨이 있는 **ONTAP 9.8** 이상

ONTAP 9.8 이상을 실행 중이고 루트 볼륨이 암호화된 경우 부팅 메뉴를 사용하여 온보드 키 관리 복구 암호를 설정해야 합니다. 부팅 미디어를 교체하는 경우에도 이 프로세스가 필요합니다.

1. 노드를 부팅 메뉴로 부팅하고 '(10) 온보드 키 관리 복구 비밀 설정' 옵션을 선택합니다.
2. 이 옵션을 사용하려면 'y'를 입력합니다.
3. 프롬프트에서 클러스터의 온보드 키 관리 암호를 입력합니다.
4. 프롬프트에서 백업 키 데이터를 입력합니다.

   백업 키 데이터를 입력한 후 노드는 부팅 메뉴로 돌아갑니다.

5. 부팅 메뉴에서 '(1) Normal Boot' 옵션을 선택합니다.

ONTAP 9.5 이하

1. 키를 복원해야 하는지 확인합니다. + '보안 키 관리자 키 쇼'
2. 키 복원: + S/S Security Key-manager setup -node_node_

   자세히 알아보세요 `security key-manager setup` 에서"ONTAP 명령 참조입니다" .

3. 암호 프롬프트에서 클러스터의 온보드 키 관리 암호를 입력합니다.

외부 키 관리 암호화 키를 수동으로 복원하고 다른 노드에 푸시할 수 있습니다. 클러스터 키를 생성할 때 일시적으로 중단했던 노드를 다시 시작하는 경우 이 작업을 수행할 수 있습니다.

이 작업에 대해

ONTAP 9.6 이상에서는 '보안 키 관리자 키 쿼리 노드_이름' 명령을 사용하여 키를 복원해야 하는지 확인할 수 있습니다.

ONTAP 9.5 이전 버전에서는 '보안 키 관리자 키 표시' 명령을 사용하여 키를 복원해야 하는지 확인할 수 있습니다.

> Flash Cache 모듈이 있는 시스템에서 NSE를 사용하는 경우, NVE 또는 NAE도 활성화해야 합니다. NSE는 Flash Cache 모듈에 상주하는 데이터를 암호화하지 않습니다.

에 대한 자세한 내용은 `security key-manager key query` "ONTAP 명령 참조입니다"을 참조하십시오.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. ONTAP 9.8 이상을 실행 중이고 루트 볼륨이 암호화된 경우 다음을 수행합니다.

   ONTAP 9.7 이하를 실행 중이거나 ONTAP 9.8 이상을 실행 중이고 루트 볼륨이 암호화되지 않은 경우 이 단계를 건너뜁니다.

   a. bootargs:+'setenv kmip.init.ipaddr <ip-address>"etenv kmip.init.netmask <netmask>"etenv kmip.init.gateway <gateway>"setenv kmip.init.interface e0M"boot_ONTAP'을 설정합니다
   b. 노드를 부팅 메뉴로 부팅하고 '(11) Configure node for external key management' 옵션을 선택합니다.
   c. 프롬프트에 따라 관리 인증서를 입력합니다.

      모든 관리 인증서 정보를 입력하면 시스템이 부팅 메뉴로 돌아갑니다.

   d. 부팅 메뉴에서 '(1) Normal Boot' 옵션을 선택합니다.

2. 키 복원:

이 ONTAP 버전의 경우…	이 명령 사용…
ONTAP 9.6 이상	'Security key-manager external restore-vserver SVM-node-key-server host_name
ip_address:port-key-id key_id-key-tag key_tag'	ONTAP 9.5 이하

> `node` 기본값은 모든 노드입니다.
>
> 온보드 키 관리가 활성화된 경우 이 명령은 지원되지 않습니다.

다음 ONTAP 9.6 명령은 외부 키 관리 인증 키를 "cluster1"의 모든 노드에 복원합니다.

```
clusterl::> security key-manager external restore
```

관련 정보

- "보안 키 관리자 외부 복원"

ONTAP 클러스터에서 KMIP SSL 인증서 교체

모든 SSL 인증서의 만료 날짜가 있습니다. 인증서가 만료되기 전에 인증서를 업데이트해야 인증 키에 대한 액세스 권한을 상실할 수 있습니다.

시작하기 전에

- 클러스터를 위한 대체 공용 인증서 및 개인 키를 확보해야 합니다(KMIP 클라이언트 인증서).
- KMIP 서버용 대체 공용 인증서(KMIP 서버-CA 인증서)를 받아야 합니다.
- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.
- MetroCluster 환경에서 KMIP SSL 인증서를 교체하는 경우 두 클러스터 모두에 동일한 대체 KMIP SSL 인증서를 설치해야 합니다.

> 클러스터에 인증서를 설치하기 전이나 후에 KMIP 서버에 대체 클라이언트 및 서버 인증서를 설치할 수 있습니다.

단계

1. 새 KMIP 서버-CA 인증서를 설치합니다.

   'Security certificate install-type server-ca-vserver<>'를 선택합니다

2. 새 KMIP 클라이언트 인증서 설치:

   'Security certificate install-type client-vserver<>'

3. 키 관리자 구성을 업데이트하여 새로 설치된 인증서를 사용합니다.

   '보안 키 관리자 외부 수정 - vserver <>-client-cert <>-server-ca-certs <>'

   MetroCluster 환경에서 ONTAP 9.6 이상을 실행하고 있고 admin SVM에서 key manager 구성을 수정하려는 경우 구성의 두 클러스터 모두에서 명령을 실행해야 합니다.

> 새로 설치된 인증서를 사용하도록 키 관리자 구성을 업데이트하면 새 클라이언트 인증서의 공개/개인 키가 이전에 설치된 키와 다르면 오류가 반환됩니다. 를 참조하십시오"NetApp 지식 기반: 새 클라이언트 인증서 공개 키 또는 개인 키가 기존 클라이언트 인증서와 다릅니다." 이 오류를 무시하는 방법에 대한 지침은 다음을 참조하세요.

관련 정보

- "보안 인증서 설치"
- "보안 키 관리자 외부 수정"

ONTAP에서 FIPS 드라이브 또는 SED를 교체합니다

일반 디스크를 교체하는 것과 동일한 방법으로 FIPS 드라이브 또는 SED를 교체할 수 있습니다. 새 데이터 인증 키를 교체 드라이브에 할당하십시오. FIPS 드라이브의 경우 새 FIPS 140-2 인증 키를 할당할 수도 있습니다.

> HA 쌍이 를 사용 중인 경우 "SAS 또는 NVMe 드라이브(SED, NSE, FIPS) 암호화", 항목의 지침을 따라야 합니다 "FIPS 드라이브 또는 SED를 보호되지 않는 모드로 되돌리는 중입니다" 시스템을 초기화하기 전에 HA 쌍 내의 모든 드라이브(부팅 옵션 4 또는 9) 이렇게 하지 않을 경우 드라이브를 용도 변경할 경우 향후의 데이터 손실이 발생할 수 있습니다.

시작하기 전에

- 드라이브에서 사용하는 인증 키의 키 ID를 알아야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 디스크가 실패로 표시되어 있는지 확인합니다.

   스토리지 디스크 고장

   에 대한 자세한 내용은 `storage disk show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                    Usable
Physical
    Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
Size
    ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
-------
    0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
133.9GB
    0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
134.2GB
[...]
```

2. 디스크 쉘프 모델의 하드웨어 가이드에 나와 있는 지침에 따라 장애가 발생한 디스크를 제거하고 새 FIPS 드라이브 또는 SED로 교체합니다.
3. 새로 교체한 디스크의 소유권을 할당합니다.

   'Storage disk assign-disk disk_name-owner node'

   에 대한 자세한 내용은 `storage disk assign` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. 새 디스크가 할당되었는지 확인합니다.

   스토리지 암호화 디스크 표시

   에 대한 자세한 내용은 `storage encryption disk show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.0  data <id_value>
1.10.1  data <id_value>
2.1.1   open 0x0
[...]
```

5. 데이터 인증 키를 FIPS 드라이브 또는 SED에 할당합니다.

   "FIPS 드라이브 또는 SED(외부 키 관리)에 데이터 인증 키 할당"

6. 필요한 경우 FIPS 140-2 인증 키를 FIPS 드라이브에 할당합니다.

   "FIPS 140-2 인증 키를 FIPS 드라이브에 할당"

관련 정보

- "저장 디스크 할당"
- "저장 디스크 표시"
- "저장 암호화 디스크 표시"

FIPS 드라이브 또는 SED에 액세스할 수 없도록 설정합니다

FIPS 드라이브 또는 SED에서 ONTAP 데이터에 액세스할 수 없게 만드는 방법에 대해 알아보세요.

FIPS 드라이브 또는 SED에 있는 데이터를 영구적으로 액세스할 수 없지만 드라이브의 사용되지 않는 공간을 새 데이터에 계속 사용하려면 디스크를 삭제할 수 있습니다. 데이터를 영구적으로 액세스할 수 없도록 만들고 드라이브를 다시 사용하지 않으려면 해당 드라이브를 제거할 수 있습니다.

- 디스크 삭제

  자체 암호화 드라이브를 삭제할 때 시스템은 디스크 암호화 키를 새 임의 값으로 변경하고, 전원 켜짐 잠금 상태를 false로 재설정하고, 키 ID를 기본값으로 설정합니다(제조업체 보안 ID 0x0(SAS 드라이브) 또는 null 키(NVMe

드라이브)). 이렇게 하면 디스크의 데이터에 액세스할 수 없게 되고 데이터를 검색할 수 없게 됩니다. 삭제된 디스크를 제로화되지 않은 스페어 디스크로 다시 사용할 수 있습니다.

- 디스크 폐기

  FIPS 드라이브 또는 SED를 제거할 때 시스템은 디스크 암호화 키를 알 수 없는 임의 값으로 설정하고 디스크를 복구할 수 없도록 잠급니다. 이렇게 하면 디스크를 영구적으로 사용할 수 없게 되고 디스크에 있는 데이터에 영구적으로 액세스할 수 없게 됩니다.

개별 자체 암호화 드라이브 또는 노드의 모든 자체 암호화 드라이브를 삭제하고 제거할 수 있습니다.

ONTAP에서 **FIPS** 드라이브 또는 **SED**를 삭제합니다

FIPS 드라이브 또는 SED에 있는 데이터를 영구적으로 액세스할 수 없도록 만들고 새 데이터에 드라이브를 사용하려면 'Storage encryption disk sanitize' 명령을 사용하여 드라이브를 삭제할 수 있습니다.

이 작업에 대해

자체 암호화 드라이브를 삭제할 때 시스템은 디스크 암호화 키를 새 임의 값으로 변경하고, 전원 켜짐 잠금 상태를 false로 재설정하고, 키 ID를 기본값으로 설정합니다(제조업체 보안 ID 0x0(SAS 드라이브) 또는 null 키(NVMe 드라이브)). 이렇게 하면 디스크의 데이터에 액세스할 수 없게 되고 데이터를 검색할 수 없게 됩니다. 삭제된 디스크를 제로화되지 않은 스페어 디스크로 다시 사용할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 보존해야 하는 데이터를 다른 디스크의 Aggregate로 마이그레이션합니다.
2. FIPS 드라이브 또는 SED에서 삭제되는 애그리게이트를 삭제합니다.

   'Storage aggregate delete-aggregate_aggregate_name_'

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

   에 대한 자세한 내용은 `storage aggregate delete` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 삭제할 FIPS 드라이브 또는 SED의 디스크 ID 식별:

   스토리지 암호화 디스크 데이터 필드 데이터 키 ID, FIPS 키 ID, 소유자

   에 대한 자세한 내용은 `storage encryption disk show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.2  data <id_value>
[...]
```

4. FIPS 드라이브가 FIPS 준수 모드에서 실행 중인 경우 노드에 대한 FIPS 인증 키 ID를 기본 MSID 0x0으로 다시 설정합니다.

   'Storage encryption disk modify -disk_disk_id_-FIPS-key-id 0x0'

   '보안 키 관리자 쿼리' 명령을 사용하여 키 ID를 볼 수 있습니다.

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. 드라이브 완전 삭제:

   'Storage encryption disk sanitize -disk_disk_id_'

   이 명령을 사용하여 핫 스페어 또는 파손된 디스크만 삭제할 수 있습니다. 유형에 관계없이 모든 디스크를 필터링하려면 `-force-all-state` 옵션을 사용합니다. 에 대한 자세한 내용은 `storage encryption disk sanitize` "ONTAP 명령 참조입니다"을 참조하십시오.

   ⓘ ONTAP에서 계속하기 전에 확인 문구를 입력하라는 메시지를 표시합니다. 화면에 표시된 대로 정확하게 구문을 입력합니다.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

6. 삭제된 디스크:'storage disk unfail-spare true-disk_disk_id_'의 장애를 해제합니다

7. 디스크에 소유자가 있는지 확인합니다.
   `storage disk show -disk disk_id`
   를 누릅니다
   디스크에 소유자가 없는 경우 하나를 할당합니다.
   `storage disk assign -owner node -disk disk_id`
8. 삭제할 디스크를 소유하는 노드에 대한 노드 선택을 입력합니다.

   'system node run-node_node_name_'

   를 실행합니다 `disk sanitize release` 명령.
9. 노드 쉘을 종료합니다. 디스크 장애 복구 다시 취소:
   `storage disk unfail -spare true -disk disk_id`
10. 디스크가 이제 스페어이고 'storage disk show -disk_disk_id_'라는 Aggregate에서 재사용할 준비가 되었는지 확인합니다

관련 정보

- "저장 디스크 할당"
- "저장 디스크 표시"
- "저장 디스크가 고장나지 않음"
- "저장 암호화 디스크 수정"
- "스토리지 암호화 디스크 정리"
- "저장 암호화 디스크 표시 상태"

ONTAP에서 **FIPS** 드라이브 또는 **SED**를 제거합니다

FIPS 드라이브 또는 SED에 있는 데이터를 영구적으로 액세스할 수 없게 하고 드라이브를 다시 사용할 필요가 없는 경우 '저장소 암호화 디스크 폐기' 명령을 사용하여 디스크를 폐기할 수 있습니다.

이 작업에 대해

FIPS 드라이브 또는 SED를 제거할 때 시스템은 디스크 암호화 키를 알 수 없는 임의 값으로 설정하고 드라이브를 복구할 수 없도록 잠급니다. 이렇게 하면 디스크가 사실상 사용할 수 없게 되고 디스크에 있는 데이터에 영구적으로 액세스할 수 없게 됩니다. 그러나 디스크 레이블에 인쇄된 PSID(Physical Secure ID)를 사용하여 디스크를 공장 출하시 구성된 설정으로 재설정할 수 있습니다. 자세한 내용은 을 참조하십시오 "인증 키가 손실된 경우 FIPS 드라이브 또는 SED를 서비스에 반환합니다".

> Non-Returnable Disk Plus 서비스(NRD Plus)가 없는 경우 FIPS 드라이브 또는 SED를 폐기해서는 안 됩니다. 디스크를 폐기하면 보증이 무효화됩니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 보존해야 하는 데이터를 다른 디스크의 aggregate에 마이그레이션합니다.
2. 제거할 FIPS 드라이브 또는 SED의 Aggregate 삭제:

'Storage aggregate delete-aggregate aggregate_name'을 선택합니다

```
cluster1::> storage aggregate delete -aggregate aggr1
```

에 대한 자세한 내용은 `storage aggregate delete` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 제거할 FIPS 드라이브 또는 SED의 디스크 ID 식별:

   스토리지 암호화 디스크 표시

   에 대한 자세한 내용은 `storage encryption disk show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
-------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.2  data <id_value>
[...]
```

4. 디스크 폐기:

   'Storage encryption disk destroy - disk disk_id'

   에 대한 자세한 내용은 `storage encryption disk destroy` "ONTAP 명령 참조입니다"을 참조하십시오.

   계속하기 전에 확인 문구를 입력하라는 메시지가 표시됩니다. 화면에 표시된 대로 정확하게 구문을 입력합니다.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

관련 정보

- "저장 암호화 디스크 파괴"
- "저장 암호화 디스크 표시"
- "저장 암호화 디스크 표시 상태"

ONTAP의 **FIPS** 드라이브 또는 **SED**에서 긴급 데이터 삭제

보안 비상 시에 스토리지 시스템이나 KMIP 서버에서 전원을 사용할 수 없는 경우에도 FIPS 드라이브 또는 SED에 대한 액세스를 즉시 차단할 수 있습니다.

시작하기 전에

- KMIP 서버를 사용할 때 전원이 공급되지 않는 경우, 쉽게 파괴되는 인증 항목(예: 스마트 카드 또는 USB 드라이브)으로 KMIP 서버를 구성해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. FIPS 드라이브 또는 SED에서 긴급 데이터 파쇄 수행:

만약…	그러면…

스토리지 시스템에서 전원을 사용할 수 있으며 스토리지 시스템을 오프라인으로 전환할 수 있는 시간이 있습니다	a. 스토리지 시스템이 HA 쌍으로 구성된 경우 Takeover를 해제합니다. b. 모든 애그리게이트를 오프라인 상태로 전환하고 삭제합니다. c. 권한 수준을 advanced:+'et-Privilege advanced로 설정합니다 d. 드라이브가 FIPS 준수 모드에 있는 경우 노드에 대한 FIPS 인증 키 ID를 기본 MSID(+'STorage encryption disk modify -disk * -FIPS-key -id 0x0'로 다시 설정합니다 e. 스토리지 시스템을 중단합니다. f. 유지보수 모드로 부팅합니다. g. 디스크를 완전 삭제 또는 폐기: ◦ 디스크의 데이터에 액세스할 수 없도록 하고 디스크를 다시 사용할 수 있도록 하려면 + 디스크 암호화 sanitize-all을 선택합니다 ◦ 디스크에 있는 데이터에 액세스할 수 없도록 하고 디스크를 저장할 필요가 없으면 + 디스크 암호화 destroy disk_id1 disk_id2…"를 삭제합니다 ⓘ 디스크 암호화 삭제 및 디스크 암호화 삭제 명령은 유지 보수 모드에만 사용됩니다. 이러한 명령은 각 HA 노드에서 실행해야 하며 깨진 디스크에는 사용할 수 없습니다. h. 파트너 노드에 대해 이 단계를 반복합니다. 이렇게 하면 스토리지 시스템이 영구적으로 비활성화되며 모든 데이터가 지워집니다. 시스템을 다시 사용하려면 다시 구성해야 합니다.	스토리지 시스템에서 전원을 사용할 수 있으며 데이터를 즉시 제거해야 합니다

a. * 디스크에 있는 데이터에 액세스할 수 없도록 만들고 디스크를 다시 사용하려면 디스크를 삭제해야 합니다. * b. 스토리지 시스템이 HA 쌍으로 구성된 경우 Takeover를 해제합니다. c. 권한 수준을 고급으로 설정합니다. 세트 프리빌리지 고급 d. 드라이브가 FIPS 준수 모드인 경우 노드의 FIPS 인증 키 ID를 다시 기본 MSID로 설정합니다. 'Storage encryption disk modify -disk * -FIPS-key-id 0x0' e. 디스크 완전 삭제: 스토리지 암호화 디스크 완전 삭제 -disk * -force -all -states true	a. * 디스크에 있는 데이터에 액세스할 수 없도록 하고 디스크를 저장할 필요가 없는 경우, 다음 디스크를 파기하십시오: * b. 스토리지 시스템이 HA 쌍으로 구성된 경우 Takeover를 해제합니다. c. 권한 수준을 고급으로 설정합니다. 세트 프리빌리지 고급 d. 디스크 폐기: 스토리지 암호화 디스크 destroy-disk * -force-all -states true	스토리지 시스템에서 패닉이 발생하고 모든 데이터가 지워져 시스템이 영구적으로 비활성화된 상태로 유지됩니다. 시스템을 다시 사용하려면 다시 구성해야 합니다.
KMIP 서버에서 전원을 사용할 수 있지만 스토리지 시스템은 사용할 수 없습니다	a. KMIP 서버에 로그인합니다. b. 액세스를 방지하려는 데이터가 포함된 FIPS 드라이브 또는 SED와 연결된 모든 키를 제거합니다. 이렇게 하면 스토리지 시스템에서 디스크 암호화 키에 액세스할 수 없습니다.	KMIP 서버 또는 스토리지 시스템에서 전원을 사용할 수 없습니다

관련 정보

- "저장 암호화 디스크 파괴"
- "저장 암호화 디스크 수정"
- "스토리지 암호화 디스크 정리"

ONTAP 에서 인증 키가 손실된 경우 **FIPS** 드라이브 또는 **SED**를 서비스에 반환

FIPS 드라이브 또는 SED가 영구적으로 인증 키를 분실하여 KMIP 서버에서 검색할 수 없는 경우, 시스템은 FIPS 드라이브 또는 SED를 파손된 것으로 처리합니다. 디스크의 데이터에 액세스하거나 복구할 수 없지만 SED의 미사용 공간을 데이터에 다시 사용할 수 있도록 하는 단계를 수행할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

이 작업에 대해

FIPS 드라이브 또는 SED의 인증 키가 영구적으로 손실되어 복구할 수 없는 경우에만 이 프로세스를 사용해야 합니다.

디스크가 분할되어 있는 경우 이 프로세스를 시작하기 전에 먼저 분할되지 않아야 합니다.

> 디스크 파티션을 해제하는 명령은 진단 수준에서만 사용할 수 있으며 NetApp 지원팀의 감독 하에 수행해야 합니다. 계속 진행하기 전에 **NetApp** 지원팀에 문의하는 것이 좋습니다**.** 또한 다음을 참조할 수도 있습니다."NetApp 지식 기반: ONTAP 에서 스페어 드라이브의 파티션을 해제하는 방법" .

단계

1. FIPS 드라이브 또는 SED를 서비스 상태로 되돌리기:

SED가 다음과 같은 경우	다음 단계 사용…

FIPS 호환 모드가 아니거나 FIPS 호환 모드에서는 FIPS 키를 사용할 수 없습니다	a. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
	b. FIPS 키를 기본 제조 보안 ID 0x0:'스토리지 암호화 디스크 수정 - FIPS-key-id 0x0-DISK_DISK_id_'로 재설정합니다
	c. 작업이 성공했는지 확인합니다. '스토리지 암호화 디스크 표시 상태' 작업이 실패하면 이 항목의 PSID 프로세스를 사용합니다.
	d. 깨진 디스크 정리:'storage encryption disk sanitize -disk_disk_id_' 다음 단계로 진행하기 전에 'storage encryption disk show-status' 명령으로 작업이 성공했는지 확인합니다.
	e. 삭제된 디스크:'storage disk unfail-spare true-disk_disk_id_'의 장애를 해제합니다
	f. 디스크에 소유자가 있는지 확인합니다.
	`storage disk show -disk disk_id`
	를 누릅니다
	디스크에 소유자가 없는 경우 하나를 할당합니다.
	`storage disk assign -owner node -disk disk_id`
	i. 삭제할 디스크를 소유하는 노드에 대한 노드 선택을 입력합니다.
	'system node run-node_node_name_'
	를 실행합니다 `disk sanitize release` 명령.
	g. 노드 쉘을 종료합니다. 디스크 장애 복구 다시 취소:
	`storage disk unfail -spare true -disk disk_id`
	h. 디스크가 이제 스페어이고 'storage disk show -disk_disk_id_'라는 Aggregate에서 재사용할 준비가 되었는지 확인합니다

FIPS 준수 모드에서는 FIPS 키를 사용할 수 없으며 SED에는 레이블에 인쇄된 PSID가 있습니다	a. 디스크 레이블에서 디스크의 PSID를 가져옵니다.
	b. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다
	c. 디스크를 출고 시 구성된 설정으로 재설정합니다. '스토리지 암호화 디스크 복원 -원본-디스크_디스크_id_-psid_disk_physical_secure_id_' 다음 단계로 진행하기 전에 '저장소 암호화 디스크 표시-상태' 명령으로 작업이 성공했는지 확인합니다.
	d. ONTAP 9.8P5 이하를 실행 중인 경우 다음 단계로 건너뜁니다. ONTAP 9.8P6 이상을 실행 중인 경우 살균된 디스크의 오류를 해제하십시오.
	`storage disk unfail -disk disk_id`
	e. 디스크에 소유자가 있는지 확인합니다.
	`storage disk show -disk disk_id`
	를 누릅니다
	디스크에 소유자가 없는 경우 하나를 할당합니다.
	`storage disk assign -owner node -disk disk_id`
	i. 삭제할 디스크를 소유하는 노드에 대한 노드 선택을 입력합니다.
	'system node run-node_node_name_'
	를 실행합니다 `disk sanitize release` 명령.
	f. 노드 쉘을 종료합니다. 디스크 장애 복구 다시 취소:
	`storage disk unfail -spare true -disk disk_id`
	g. 디스크가 이제 스페어이고 'storage disk show -disk_disk_id_'라는 Aggregate에서 재사용할 준비가 되었는지 확인합니다

관련 정보

- "저장 암호화 디스크 수정"
- "저장 암호화 디스크를 원래 상태로 되돌리기"
- "스토리지 암호화 디스크 정리"
- "저장 암호화 디스크 표시 상태"

ONTAP 에서 **FIPS** 드라이브 또는 **SED**를 보호되지 않은 모드로 되돌리기

노드에 대한 인증 키 ID가 기본값이 아닌 값으로 설정된 경우에만 FIPS 드라이브 또는 SED가 무단 액세스로부터 보호됩니다. 명령을 사용하여 키 ID를 기본값으로 설정하면 FIPS 드라이브 또는 SED를 보호되지 않는 모드로 되돌릴 수 `storage encryption disk modify` 있습니다. 보호되지 않은 모드의 FIPS 드라이브 또는 SED는 기본 암호화 키를 사용하는 반면 보호 모드의 FIPS 드라이브 또는 SED는 제공된 보안 암호화 키를 사용합니다. 드라이브에 암호화된 데이터가 있고 드라이브가 보호되지 않는 모드로 재설정되더라도 데이터는 여전히 암호화되어 노출되지 않습니다.

FIPS 드라이브나 SED가 보호되지 않은 모드로 돌아간 후 암호화된 데이터에 액세스할 수 없도록 하려면 다음 절차를 따르세요. FIPS와 데이터 키 ID가 재설정되면 기존 데이터는 해독할 수 없으며 원래 키를 복원하지 않는 한 액세스할 수 없습니다.

HA 쌍이 암호화 SAS 또는 NVMe 드라이브(SED, NSE, FIPS)를 사용 중인 경우 시스템을 초기화하기 전에 HA 쌍 내의 모든 드라이브에 대해 이 프로세스를 따라야 합니다(부팅 옵션 4 또는 9). 이렇게 하지 않을 경우 드라이브를 용도 변경할 경우 향후의 데이터 손실이 발생할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. FIPS 드라이브가 FIPS 준수 모드에서 실행 중인 경우 노드에 대한 FIPS 인증 키 ID를 기본 MSID 0x0으로 다시 설정합니다.

   'Storage encryption disk modify -disk_disk_id_-FIPS-key-id 0x0'

   '보안 키 관리자 쿼리' 명령을 사용하여 키 ID를 볼 수 있습니다.

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   다음 명령을 사용하여 작업이 성공했는지 확인합니다.

   '스토리지 암호화 디스크 표시 상태'입니다

   "Disks Begun"과 "Disks Done"의 숫자가 같아질 때까지 show-status 명령을 반복합니다.

```
cluster1:: storage encryption disk show-status

            FIPS    Latest   Start               Execution   Disks
Disks Disks
Node        Support Request  Timestamp           Time (sec)  Begun
Done  Successful
-------     ------- -------- ------------------  ---------- ------
------  ----------
cluster1    true    modify   1/18/2022 15:29:38    3           14     5
5
1 entry was displayed.
```

3. 노드의 데이터 인증 키 ID를 기본 MSID 0x0으로 다시 설정합니다.

   'Storage encryption disk modify -disk_disk_id_-data-key-id 0x0

   SAS 또는 NVMe 드라이브를 보호되지 않는 모드로 반환하든 관계없이 '-data-key-id' 값은 0x0으로 설정되어야 합니다.

   '보안 키 관리자 쿼리' 명령을 사용하여 키 ID를 볼 수 있습니다.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

   다음 명령을 사용하여 작업이 성공했는지 확인합니다.

   '스토리지 암호화 디스크 표시 상태'입니다

   숫자가 같아질 때까지 show-status 명령을 반복합니다. "disks began"과 "disks done"의 숫자가 같으면 작업이 완료됩니다.

유지보수 모드

ONTAP 9.7부터 유지 관리 모드에서 FIPS 드라이브를 다시 입력하다 이전 섹션에서 ONTAP CLI 지침을 사용할 수 없는 경우에만 유지보수 모드를 사용해야 합니다.

단계

1. 노드에 대한 FIPS 인증 키 ID를 기본 MSID 0x0으로 다시 설정합니다.

   '디스크 암호화 키를 다시 입력하다 0x0_FIPS 0x0_disklist_'

2. 노드의 데이터 인증 키 ID를 기본 MSID 0x0으로 다시 설정합니다.

"디스크 암호화 0x0_disklist_"

3. FIPS 인증 키를 성공적으로 다시 입력했는지 확인합니다.

   디스크 암호화 show_FIPS

4. 데이터 인증 키가 다음 키로 성공적으로 다시 입력되었는지 확인합니다.

   디스크 암호화 쇼

   출력에는 기본 MSID 0x0 키 ID 또는 키 서버가 보유한 64자 값이 표시될 수 있습니다. 를 클릭합니다 `Locked?` 필드는 데이터 잠금을 의미합니다.

```
Disk       FIPS Key ID                  Locked?
---------- ---------------------------- -------
0a.01.0    0x0                           Yes
```

관련 정보

- "저장 암호화 디스크 수정"
- "저장 암호화 디스크 표시 상태"

ONTAP에서 외부 키 관리자 연결을 제거합니다

서버가 더 이상 필요하지 않은 경우 노드에서 KMIP 서버를 분리할 수 있습니다. 예를 들어, 볼륨 암호화로 전환할 때 KMIP 서버를 분리할 수 있습니다.

이 작업에 대해

HA 쌍의 한 노드에서 KMIP 서버를 분리하면 시스템이 모든 클러스터 노드에서 서버의 연결을 자동으로 끊습니다.

KMIP 서버를 분리한 후 외부 키 관리를 계속 사용하려면 다른 KMIP 서버를 사용하여 인증 키를 제공할 수 있어야 합니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. 현재 노드에서 KMIP 서버를 분리합니다.

이 ONTAP 버전의 경우…	이 명령 사용…
ONTAP 9.6 이상	'Security key-manager external remove-servers-vserver SVM-key-servers host_name
ip_address:port,…	ONTAP 9.5 이하

   MetroCluster 환경에서는 admin SVM에 대해 두 클러스터 모두에서 이러한 명령을 반복해야 합니다.

다음 ONTAP 9.6 명령은 첫 번째 이름이 k1인 'cluster1'의 외부 키 관리 서버 2대에 대한 연결을 비활성화하며, 두 번째 주소는 IP 주소가 10.0.0.20인 기본 포트 5696에서 수신, 포트 24482에서 수신 대기 중입니다.

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

및 `security key-manager delete` 에 대한 자세한 `security key-manager external remove-servers` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP 외부 키 관리 서버 속성 수정

ONTAP 9.6부터, 외부 키 관리 서버의 I/O 제한 시간 및 사용자 이름을 변경하기 위해 'Security key-manager external modify-server' 명령어를 사용할 수 있다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.
- 이 작업에는 고급 권한이 필요합니다.
- MetroCluster 환경에서는 관리 SVM을 위해 두 클러스터 모두에서 이러한 단계를 반복해야 합니다.

단계

1. 스토리지 시스템에서 고급 권한 레벨로 변경합니다.

   세트 프리빌리지 고급

2. 클러스터의 외부 키 관리자 서버 속성 수정:

   'Security key-manager external modify-server-vserver admin_SVM-key-server host_name|ip_address:port,… -timeout 1…60 - username user_name'입니다

   > 시간 초과 값은 초 단위로 표시됩니다. 사용자 이름을 수정하면 새 암호를 입력하라는 메시지가 표시됩니다. 클러스터 로그인 프롬프트에서 명령을 실행하면 '*admin_SVM*'이(가) 현재 클러스터의 admin SVM으로 기본 설정됩니다. 외부 키 관리자 서버 속성을 수정하려면 클러스터 관리자여야 합니다.

   다음 명령을 실행하면 기본 포트 5696에서 수신 대기하는 'cluster1' 외부 키 관리 서버의 시간 초과 값이 45초로 변경됩니다.

   ```
   clusterl::> security key-manager external modify-server -vserver
   cluster1 -key-server ks1.local -timeout 45
   ```

3. SVM에 대한 외부 키 관리자 서버 속성 수정(NVE만 해당):

   'Security key-manager external modify-server-vserver SVM-key-server host_name|ip_address:port,… -timeout 1…60 - username user_name'입니다

시간 초과 값은 초 단위로 표시됩니다. 사용자 이름을 수정하면 새 암호를 입력하라는 메시지가 표시됩니다. SVM 로그인 프롬프트에서 명령을 실행하면 '*SVM*'이(가) 현재 SVM으로 기본 설정됩니다. 외부 키 관리자 서버 속성을 수정하려면 클러스터 또는 SVM 관리자여야 합니다.

다음 명령을 실행하면 기본 포트 5696에서 수신 대기 중인 'vm1' 외부 키 관리 서버의 사용자 이름과 암호가 변경됩니다.

```
svm1::> security key-manager external modify-server -vserver svm11 -key
-server ks1.local -username svm1user
Enter the password:
Reenter the password:
```

4. 추가 SVM에 대해 마지막 단계를 반복합니다.

관련 정보

- "보안 키 관리자 외부 수정 서버"

ONTAP의 온보드 키 관리에서 외부 키 관리로 전환합니다

온보드 키 관리에서 외부 키 관리로 전환하려면 온보드 키 관리 구성을 삭제해야 외부 키 관리를 활성화할 수 있습니다.

시작하기 전에

- 하드웨어 기반 암호화의 경우 모든 FIPS 드라이브 또는 SED의 데이터 키를 기본값으로 재설정해야 합니다.

  "FIPS 드라이브 또는 SED를 보호되지 않는 모드로 되돌리는 중입니다"

- 소프트웨어 기반 암호화의 경우 모든 볼륨의 암호화를 해제해야 합니다.

  "볼륨 데이터 암호화를 해제합니다"

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 클러스터의 온보드 키 관리 구성을 삭제합니다.

이 ONTAP 버전의 경우…	이 명령 사용…
ONTAP 9.6 이상	'Security key-manager 온보드 disable-vserver SVM
ONTAP 9.5 이하	보안 키 관리자 삭제 키 데이터베이스

및 `security key-manager delete-key-database` 에 대한 자세한 `security key-manager onboard disable` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

외부 키 관리에서 **ONTAP** 온보드 키 관리로 전환

온보드 키 관리로 전환하려면 온보드 키 관리를 활성화하기 전에 외부 키 관리 구성을 삭제하세요.

시작하기 전에

- 하드웨어 기반 암호화의 경우 모든 FIPS 드라이브 또는 SED의 데이터 키를 기본값으로 재설정해야 합니다.

  "FIPS 드라이브 또는 SED를 보호되지 않는 모드로 되돌리는 중입니다"

- 모든 외부 키 관리자 연결을 삭제해야 합니다.

  "외부 키 관리자 연결을 삭제하는 중입니다"

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

키 관리를 전환하는 단계는 사용 중인 ONTAP 버전에 따라 다릅니다.

ONTAP 9.6 이상

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 다음 명령을 사용합니다.

   'Security key-manager external disable-vserver_admin_SVM_'

   MetroCluster 환경에서는 admin SVM에 대해 두 클러스터 모두에서 명령을 반복해야 합니다.

자세히 알아보세요 `security key-manager external disable` 에서"ONTAP 명령 참조입니다" .

ONTAP 9.5 이하

'Security key-manager delete-KMIP-config' 명령어를 사용한다

자세히 알아보세요 `security key-manager delete-kmip-config` 에서"ONTAP 명령 참조입니다" .

관련 정보

- "보안 키 관리자 외부 비활성화"

ONTAP 부팅 프로세스 중에 키 관리 서버에 접속할 수 없는 경우 어떻게 됩니까**?**

ONTAP는 NSE에 구성된 스토리지 시스템이 부팅 프로세스 중 지정된 키 관리 서버에 연결할 수 없는 경우 원치 않는 동작을 방지하기 위해 특정 예방 조치를 취합니다.

스토리지 시스템이 NSE에 맞게 구성되고 SED가 리키 입력 및 잠겨 있고 SED의 전원이 켜져 있는 경우, 스토리지 시스템은 SED에 액세스하기 전에 키 관리 서버에서 필요한 인증 키를 검색하여 SED에 대한 자체 인증을 해야 합니다.

스토리지 시스템은 지정된 키 관리 서버에 최대 3시간 동안 접속을 시도합니다. 이 시간 이후에 스토리지 시스템이 해당 시스템에 연결할 수 없는 경우 부팅 프로세스가 중지되고 스토리지 시스템이 중지됩니다.

스토리지 시스템이 지정된 키 관리 서버에 성공적으로 접속하면 최대 15분 동안 SSL 연결을 시도합니다. 스토리지 시스템이 지정된 키 관리 서버와 SSL 연결을 설정할 수 없는 경우 부팅 프로세스가 중지되고 스토리지 시스템이 중지됩니다.

스토리지 시스템이 키 관리 서버에 연결하여 연결을 시도하는 동안 CLI에서 실패한 연결 시도에 대한 자세한 정보가 표시됩니다. Ctrl+C를 누르면 언제든지 연결 시도를 중단할 수 있습니다

보안 조치로서 SED는 제한된 수의 무단 액세스 시도만 허용하며, 그 이후에는 기존 데이터에 대한 액세스를 차단합니다. 스토리지 시스템이 지정된 키 관리 서버에 연결할 수 없어 적절한 인증 키를 얻을 수 없는 경우 기본 키로만 인증을 시도하여 시도 실패 및 패닉이 발생할 수 있습니다. 패닉이 발생할 경우 스토리지 시스템이 자동으로 재부팅되도록 구성된 경우 부팅 루프로 진입하여 SED에서 지속적인 인증 실패를 초래하게 됩니다.

이러한 시나리오에서 스토리지 시스템을 중단하는 것은 스토리지 시스템이 부팅 루프에 진입하지 못하도록 하는 것으로, SED가 영구적으로 잠기면 특정 횟수의 연속 인증 실패 횟수를 초과하여 의도하지 않은 데이터가 손실될 수 있습니다. 잠금 보호의 제한 및 유형은 제조 사양 및 SED 유형에 따라 다릅니다.

SED 유형	연속 실패한 인증 시도 횟수로 인해 잠금이 발생합니다	안전 한도에 도달하면 잠금 보호 유형입니다
HDD	1024	영구. 적절한 인증 키를 다시 사용할 수 있는 경우에도 데이터를 복구할 수 없습니다.
펌웨어 버전 NA00 또는 NA01이 있는 X440_PHM2800MCTO 800GB NSE SSD	5	임시. 잠금 기능은 디스크 전원을 껐다가 다시 켤 때까지만 적용됩니다.
펌웨어 버전 NA00 또는 NA01이 있는 X577_PHM2800MCTO 800GB NSE SSD	5	임시. 잠금 기능은 디스크 전원을 껐다가 다시 켤 때까지만 적용됩니다.
더 높은 펌웨어 버전의 X440_PHM2800MCTO 800GB NSE SSD	1024	영구. 적절한 인증 키를 다시 사용할 수 있는 경우에도 데이터를 복구할 수 없습니다.
펌웨어 버전이 더 높은 X577_PHM2800MCTO 800GB NSE SSD	1024	영구. 적절한 인증 키를 다시 사용할 수 있는 경우에도 데이터를 복구할 수 없습니다.
그 외 모든 SSD 모델	1024	영구. 적절한 인증 키를 다시 사용할 수 있는 경우에도 데이터를 복구할 수 없습니다.

모든 SED 유형의 경우 인증에 성공하면 시도 횟수가 0으로 재설정됩니다.

지정된 키 관리 서버에 도달하지 못해 스토리지 시스템이 중단된 경우 스토리지 시스템 부팅을 계속 시도하기 전에 먼저

통신 장애의 원인을 파악하고 수정해야 합니다.

기본적으로 **ONTAP** 암호화 비활성화

ONTAP 9.7부터 볼륨 암호화(VE) 라이센스가 있고 온보드 키 관리자 또는 외부 키 관리자를 사용하는 경우 애그리게이트 및 볼륨 암호화가 기본적으로 활성화됩니다. 필요한 경우 전체 클러스터에 대해 암호화를 기본적으로 사용하지 않도록 설정할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자이거나 클러스터 관리자가 권한을 위임한 SVM 관리자여야 합니다.

단계

1. ONTAP 9.7 이상에서 전체 클러스터에 대해 기본적으로 암호화를 사용하지 않도록 설정하려면 다음 명령을 실행합니다.

   'options-option-name encryption.data_at_rest_encryption.disable_by_default-option-value on’입니다

데이터 보호 및 재해 복구

클러스터 및 **SVM** 피어링

ONTAP 클러스터 및 **SVM** 피어링에 대해 알아보십시오

소스 및 타겟 클러스터와 소스 및 타겟 스토리지 가상 머신(SVM) 간에 피어 관계를 생성할 수 있습니다. SnapMirror를 사용하여 스냅샷을 복제하려면 먼저 이러한 엔터티 간에 피어 관계를 생성해야 합니다.

ONTAP 9.3은 클러스터와 SVM 간의 피어 관계를 간편하게 구성할 수 있도록 향상된 기능을 제공합니다. 모든 ONTAP 9 버전에서 클러스터 및 SVM 피어링 절차를 사용할 수 있습니다. 해당 버전의 ONTAP에 적합한 절차를 사용해야 합니다.

System Manager나 자동화된 스크립팅 도구가 아니라 CLI(Command-Line Interface)를 사용하여 절차를 수행합니다.

클러스터 및 **SVM** 피어링을 준비합니다

ONTAP 피어링 기초

SnapMirror를 사용하여 스냅샷을 복제하려면 소스 및 대상 클러스터 간, 소스 및 대상 SVM 간에 _peer 관계_를 생성해야 합니다. 피어 관계는 클러스터와 SVM이 데이터를 안전하게 교환할 수 있도록 네트워크 연결을 정의합니다.

피어 관계의 클러스터와 SVM은 _인터클러스터 논리 인터페이스(LIF)를 사용하여 인터클러스터 네트워크를 통해 통신합니다. _ 인터클러스터 LIF는 일반적으로 "기본 인터클러스터 코어" 네트워크 인터페이스 서비스 정책을 사용하여 생성되는 LIF입니다. 피어링된 클러스터의 모든 노드에 대한 인터클러스터 LIF를 생성해야 합니다.

인터클러스터 LIF는 해당 LIF가 할당된 시스템 SVM에 속하는 경로를 사용합니다. ONTAP에서 IPspace 내에서 클러스터 레벨 통신을 위한 시스템 SVM을 자동으로 생성합니다.

팬아웃 및 캐스케이드 토폴로지가 모두 지원됩니다. 계단식 토폴로지에서는 1차 클러스터와 2차 클러스터 간에 그리고 2차 클러스터와 3차 클러스터 간에 인터클러스터 네트워크만 만들어야 합니다. 1차 클러스터와 3차 클러스터 간에 인터클러스터 네트워크를 생성할 필요가 없습니다.

> 관리자가 기본 인터클러스터 서비스 정책에서 인터클러스터 코어 서비스를 제거할 수 있지만 권장하지는 않습니다. 이 경우 "default-인터클러스터"를 사용하여 만든 LIF는 실제로 인터클러스터 LIF가 아닙니다. 기본 인터클러스터 서비스 정책에 인터클러스터 코어 서비스가 포함되어 있는지 확인하려면 다음 명령을 사용합니다.
>
> 네트워크 인터페이스 서비스 정책 표시 정책 기본값 - 인터클러스터
>
> 에 대한 자세한 내용은 `network interface service-policy show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 피어링 사전 요구사항

클러스터 피어링을 설정하기 전에 연결, 포트, IP 주소, 서브넷, 방화벽, 클러스터 명명

요구사항이 충족됩니다.

> ONTAP 9.6부터 클러스터 피어링은 데이터 복제를 위한 TLS 1.2 AES-256 GCM 암호화 지원을 기본적으로 제공합니다. 암호화를 사용하지 않는 경우에도 클러스터 피어링이 작동하려면 기본 보안 암호("PSK-AES256-GCM-SHA384")가 필요합니다.
>
> ONTAP 9.11.1부터 DHE-PSK 보안 사이퍼를 기본적으로 사용할 수 있습니다.
>
> ONTAP 9.15.1부터 클러스터 피어링은 기본적으로 데이터 복제를 위한 TLS 1.3 암호화 지원을 제공합니다.

연결 요구 사항

로컬 클러스터의 모든 인터클러스터 LIF는 원격 클러스터의 모든 인터클러스터 LIF와 통신할 수 있어야 합니다.

반드시 필요한 것은 아니지만 일반적으로 동일한 서브넷에 있는 인터클러스터 LIF에 사용되는 IP 주소를 구성하는 것이 더 간단합니다. IP 주소는 데이터 LIF와 동일한 서브넷 또는 다른 서브넷에 상주할 수 있습니다. 각 클러스터에 사용되는 서브넷은 다음 요구사항을 충족해야 합니다.

- 서브넷은 인터클러스터 통신에 사용되는 포트를 포함하는 브로드캐스트 도메인에 속해야 합니다.
- 서브넷에는 노드당 하나의 인터클러스터 LIF에 할당할 수 있는 충분한 IP 주소가 있어야 합니다.

  예를 들어, 4노드 클러스터에서 인터클러스터 통신에 사용되는 서브넷에는 사용 가능한 IP 주소 4개가 있어야 합니다.

각 노드에는 인터클러스터 네트워크의 IP 주소를 사용하는 인터클러스터 LIF가 있어야 합니다.

인터클러스터 LIF는 IPv4 주소 또는 IPv6 주소를 가질 수 있습니다.

> ONTAP를 사용하면 필요에 따라 두 프로토콜을 인터클러스터 LIF에 동시에 표시할 수 있으므로 피어링 네트워크를 IPv4에서 IPv6로 마이그레이션할 수 있습니다. 이전 릴리즈에서는 전체 클러스터에 대한 모든 인터클러스터 관계가 IPv4 또는 IPv6였습니다. 이는 프로토콜 변경이 잠재적으로 운영 중단이 발생할 수 있음을 의미합니다.

포트 요구 사항

인터클러스터 통신에 전용 포트를 사용하거나 데이터 네트워크에서 사용하는 포트를 공유할 수 있습니다. 포트는 다음 요구 사항을 충족해야 합니다.

- 지정된 원격 클러스터와 통신하는 데 사용되는 모든 포트는 동일한 IPspace에 있어야 합니다.

  여러 클러스터를 사용하여 다른 IPspace를 사용할 수 있습니다. IPspace 내에서만 쌍방향 전체 메시 연결이 필요합니다.

- 인터클러스터 통신에 사용되는 브로드캐스트 도메인에는 한 포트에서 다른 포트로 인터클러스터 통신이 페일오버할 수 있도록 노드당 두 개 이상의 포트가 포함되어야 합니다.

  브로드캐스트 도메인에 추가된 포트는 물리적 네트워크 포트, VLAN 또는 인터페이스 그룹(ifgrp)일 수 있습니다.

- 모든 포트는 케이블로 연결되어야 합니다.

- 모든 포트가 정상 상태여야 합니다.
- 포트의 MTU 설정이 일치해야 합니다.

방화벽 요구 사항

ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 참조하십시오 "LIF의 방화벽 정책을 구성합니다".

방화벽과 인터클러스터 방화벽 정책은 다음 프로토콜을 허용해야 합니다.

- 양방향 ICMP 트래픽
- 포트 11104 및 11105를 통해 모든 인터클러스터 LIF의 IP 주소로 양방향으로 시작된 TCP 트래픽입니다
- 인터클러스터 LIF 간 양방향 HTTPS

  CLI를 사용하여 클러스터 피어링을 설정할 때는 HTTPS가 필요하지 않지만 나중에 System Manager를 사용하여 데이터 보호를 구성하면 HTTPS가 필요합니다.

기본 '인터클러스터' 방화벽 정책은 HTTPS 프로토콜을 통해 모든 IP 주소(0.0.0.0/0)에서 액세스할 수 있도록 합니다. 필요한 경우 정책을 수정하거나 대체할 수 있습니다.

클러스터 요구사항

클러스터는 다음 요구사항을 충족해야 합니다.

- 클러스터는 255개 이상의 클러스터와 피어 관계에 있을 수 없습니다.

공유 또는 전용 **ONTAP** 포트를 사용합니다

인터클러스터 통신에 전용 포트를 사용하거나 데이터 네트워크에서 사용하는 포트를 공유할 수 있습니다. 포트 공유 여부를 결정할 때는 네트워크 대역폭, 복제 간격 및 포트 가용성을 고려해야 합니다.

다른 피어링된 클러스터 중 전용 포트를 사용하여 포트 하나를 공유할 수 있습니다.

네트워크 대역폭

10GbE 같은 고속 네트워크가 있는 경우 데이터 액세스에 사용되는 것과 동일한 10GbE 포트를 사용하여 복제를 수행할 수 있는 충분한 로컬 LAN 대역폭이 있을 수 있습니다.

또한 사용 가능한 WAN 대역폭을 LAN 대역폭과 비교해야 합니다. 사용 가능한 WAN 대역폭이 10GbE보다 훨씬 작은 경우 전용 포트를 사용해야 할 수 있습니다.

이 규칙의 한 가지 예외는 클러스터의 전체 또는 여러 노드에서 데이터를 복제하는 경우입니다. 이 경우 대역폭 사용률을 일반적으로 노드 전체에 분산합니다.

전용 포트를 사용하지 않는 경우 복제 네트워크의 MTU(Maximum Transmission Unit) 크기는 일반적으로 데이터 네트워크의 MTU 크기와 같아야 합니다.

복제 간격입니다

사용량이 적은 시간에 복제가 수행되면 10GbE LAN 연결이 없어도 복제에 데이터 포트를 사용할 수 있습니다.

정상 업무 시간 중에 복제가 수행되는 경우 복제할 데이터의 양과 데이터 프로토콜 경합을 유발할 수 있는 대역폭이 너무 많이 필요한지 여부를 고려해야 합니다. 데이터 프로토콜(SMB, NFS, iSCSI)의 네트워크 활용률이 50%를 넘는 경우, 노드 페일오버가 발생할 경우 성능이 저하되지 않도록 인터클러스터 통신에 전용 포트를 사용해야 합니다.

포트 가용성

복제 트래픽이 데이터 트래픽을 방해한다고 판단할 경우 인터클러스터 LIF를 동일한 노드의 다른 인터클러스터 지원 공유 포트로 마이그레이션할 수 있습니다.

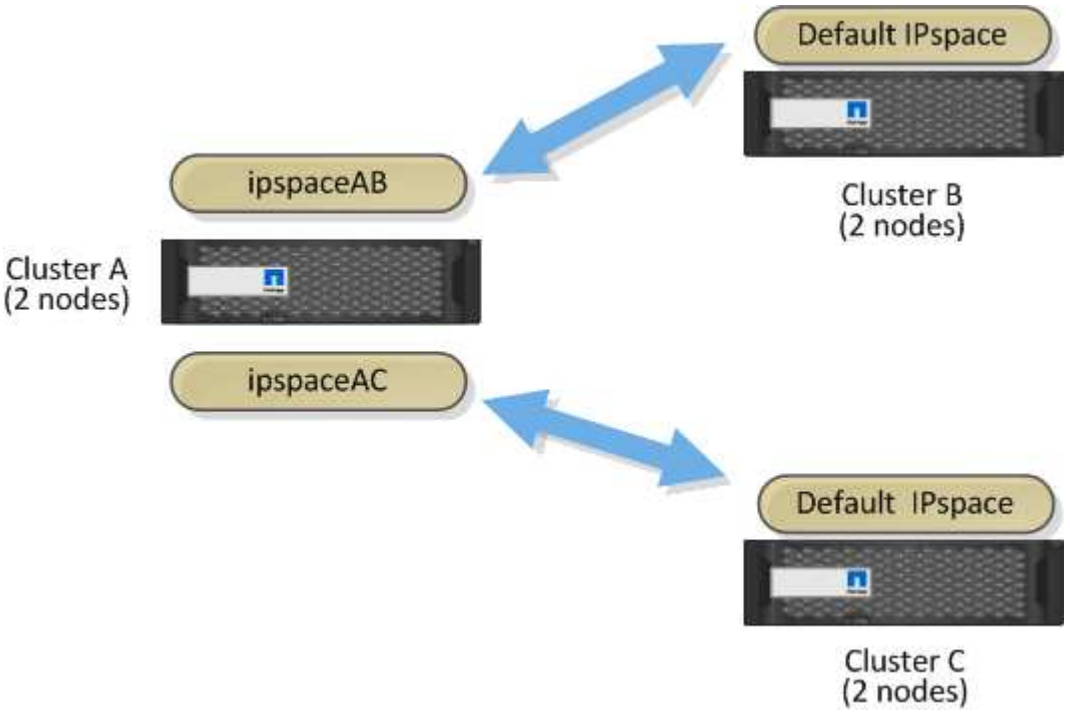
복제에 VLAN 포트를 전용으로 지정할 수도 있습니다. 포트의 대역폭은 모든 VLAN과 기본 포트 간에 공유됩니다.

사용자 지정 **ONTAP IPspace**를 사용하여 복제 트래픽을 격리합니다

맞춤형 IPspace를 사용하여 클러스터에서 다른 동료들과 상호 작용을 분리할 수 있습니다. _Designated 인터클러스터 연결 _ 이라고 하는 이 구성을 통해 서비스 공급자는 멀티 테넌트 환경에서 복제 트래픽을 격리할 수 있습니다.

예를 들어 클러스터 A와 클러스터 B 사이의 복제 트래픽을 클러스터 A와 클러스터 C 사이의 복제 트래픽과 분리하려고 한다고 가정합니다 이렇게 하려면 클러스터 A에서 2개의 IPspace를 생성할 수 있습니다

IPspace에는 클러스터 B와 통신하는 데 사용하는 인터클러스터 LIF가 포함되어 있습니다 다른 에는 다음 그림과 같이 클러스터 C와 통신하는 데 사용하는 인터클러스터 LIF가 포함되어 있습니다.



관련 정보

- "ONTAP IPspace 구성에 대해 자세히 알아보십시오"

인터클러스터 LIF를 구성합니다

공유 데이터 포트에 대한 ONTAP 인터클러스터 LIF를 구성합니다

데이터 네트워크와 공유하는 포트에 대한 인터클러스터 LIF를 구성할 수 있습니다. 이렇게 하면 인터클러스터 네트워킹에 필요한 포트 수가 줄어듭니다.

단계

1. 클러스터의 포트 나열:

   네트워크 포트 쇼

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 "cluster01"의 네트워크 포트를 보여줍니다.

```
cluster01::> network port show
                                                                 Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. 관리자 SVM(기본 IPspace) 또는 시스템 SVM(사용자 지정 IPspace)에 대한 인터클러스터 LIF를 생성합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	'network interface create-vserver_system_SVM_-lif_LIF_name_-service-policy default-인터클러스터 -home-node_node_-home-port port-address_port_ip_-netmask_mask_'
• ONTAP 9.5 및 이전 버전의 경우: *	'network interface create-vserver_system_SVM_-lif_LIF_name_-role l인터클러스터-home-node_node_ -home-port_port_-address_port_ip_ -netmask_mask_'

에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 인터클러스터 LIF 'cluster01_icl01'과 'cluster01_icl02'를 생성합니다.

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. 인터클러스터 LIF가 생성되었는지 확인합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	네트워크 인터페이스 show-service-policy default-인터클러스터
• ONTAP 9.5 및 이전 버전의 경우: *	네트워크 인터페이스 show-role 인터클러스터(network interface show-role 인터클러스터)

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0c
true
```

4. 인터클러스터 LIF가 중복되는지 확인합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	'network interface show – service-policy default-인터클러스터-failover'
• ONTAP 9.5 및 이전 버전의 경우: *	네트워크 인터페이스 show-role 인터클러스터-failover를 참조하십시오

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 e0c 포트의 인터클러스터 LIF 'cluster01_icl01'과 cluster01_icl02가 e0d 포트로 페일오버된다는 것을 보여 줍니다.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

전용 포트에 대한 **ONTAP** 인터클러스터 **LIF**를 구성합니다

전용 포트에 대한 인터클러스터 LIF를 구성할 수 있습니다. 이렇게 하면 일반적으로 복제 트래픽에 사용할 수 있는 대역폭이 증가합니다.

단계

1. 클러스터의 포트 나열:

   네트워크 포트 쇼

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 "cluster01"의 네트워크 포트를 보여줍니다.

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. 인터클러스터 통신 전용으로 사용할 수 있는 포트를 확인합니다.

   네트워크 인터페이스 보기 필드 홈 포트, 통화 포트

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예제는 포트 e0e 및 e0f에 LIF가 할당되지 않음을 보여줍니다.

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. 전용 포트에 대한 페일오버 그룹을 생성합니다.

'network interface failover-groups create-vserver_system_SVM_-failover-group_failover_group_-targets_physical_or_logical_ports_'

다음 예에서는 시스템 SVM 'cluster01'의 페일오버 그룹 intercluster01에 포트 e0e와 e0f를 할당합니다.

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. 페일오버 그룹이 생성되었는지 확인합니다.

   네트워크 인터페이스 페일오버 그룹들이 보여줌

   에 대한 자세한 내용은 `network interface failover-groups show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. 시스템 SVM에 대한 인터클러스터 LIF를 생성한 다음 이를 페일오버 그룹에 할당합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	"네트워크 인터페이스 create-vserver_system_SVM_-lif_LIF_name_-service-policy default-인터클러스터 -home-node_node_-home-port_port_ -address_port_ip_-netmask_mask_-failover -group_group_"

옵션을 선택합니다	설명
• ONTAP 9.5 및 이전 버전의 경우: *	'network interface create -vserver_system_SVM_ -lif_LIF_name_-role 인터클러스터 -home -node_node_-home-port_port_-address_port_ip_ -netmask_mask_-failover -group_failover_group_'

에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 페일오버 그룹 intercluster01에 인터클러스터 LIF 'cluster01_icl01'과 'cluster01_icl02'를 생성합니다.

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. 인터클러스터 LIF가 생성되었는지 확인합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	네트워크 인터페이스 show-service-policy default-인터클러스터
• ONTAP 9.5 및 이전 버전의 경우: *	네트워크 인터페이스 show-role 인터클러스터(network interface show-role 인터클러스터)

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0f
true
```

7. 인터클러스터 LIF가 중복되는지 확인합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	네트워크 인터페이스 show-service-policy default-인터클러스터-failover를 선택합니다
• ONTAP 9.5 및 이전 버전의 경우: *	네트워크 인터페이스 show-role 인터클러스터-failover를 참조하십시오

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 SVM e0e 포트의 인터클러스터 LIF 'cluster01_icl01'과 cluster01_icl02가 e0f 포트로 페일오버된다는 것을 보여 줍니다.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

사용자 지정 IPspace에서 인터클러스터 LIF를 구성할 수 있습니다. 멀티 테넌트 환경에서 복제 트래픽을 분리할 수 있습니다.

사용자 지정 IPspace를 생성하는 경우 시스템은 시스템 SVM(스토리지 가상 머신)을 해당 IPspace의 시스템 개체에 대한 컨테이너 역할을 합니다. 새 SVM을 새 IPspace의 모든 인터클러스터 LIF의 컨테이너로 사용할 수 있습니다. 새 SVM은 사용자 지정 IPspace와 동일한 이름을 갖습니다.

단계

1. 클러스터의 포트 나열:

   네트워크 포트 쇼

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 "cluster01"의 네트워크 포트를 보여줍니다.

```
cluster01::> network port show
                                                                 Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. 클러스터에서 맞춤형 IPspace 생성:

   네트워크 IPspace 생성 - IPSpace_IPSpace_

   다음 예에서는 사용자 지정 IPspace "IPSpace-IC1"을 생성합니다.

```
cluster01::> network ipspace create -ipspace ipspace-IC1
```

에 대한 자세한 내용은 `network ipspace create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 인터클러스터 통신 전용으로 사용할 수 있는 포트를 확인합니다.

   네트워크 인터페이스 보기 필드 홈 포트, 통화 포트

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예제는 포트 e0e 및 e0f에 LIF가 할당되지 않음을 보여줍니다.

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01_clus1   e0a       e0a
Cluster cluster01_clus2   e0b       e0b
Cluster cluster02_clus1   e0a       e0a
Cluster cluster02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

4. 기본 브로드캐스트 도메인에서 사용 가능한 포트를 제거합니다.

   네트워크 포트 브로드캐스트-도메인 제거-포트-브로드캐스트-도메인 기본 포트 포트

   포트는 한 번에 둘 이상의 브로드캐스트 도메인에 있을 수 없습니다. 에 대한 자세한 내용은 `network port broadcast-domain remove-ports` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 기본 브로드캐스트 도메인에서 포트 "e0e" 및 "e0f"를 제거합니다.

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

5. 포트가 기본 브로드캐스트 도메인에서 제거되었는지 확인합니다.

   네트워크 포트 쇼

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 기본 브로드캐스트 도메인에서 포트 "e0e"와 "e0f"가 제거되었음을 보여 줍니다.

```
cluster01::> network port show
                                                          Speed (Mbps)
Node   Port    IPspace   Broadcast Domain Link   MTU     Admin/Oper
------ ------- --------- --------------- ----- ------- ------------
cluster01-01
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
cluster01-02
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
```

6. 사용자 지정 IPspace에서 브로드캐스트 도메인 생성:

   'network port broadcast-domain create-IPSpace_IPSpace_-broadcast-domain_broadcast_domain_-mtu_mtu_-ports_ports_'

   다음 예에서는 IPspace 'IPSpace-IC1'에 브로드캐스트 도메인 'IPSpace-IC1-BD'를 생성합니다.

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

7. 브로드캐스트 도메인이 생성되었는지 확인합니다.

   네트워크 포트 브로드캐스트 도메인 쇼

   에 대한 자세한 내용은 `network port broadcast-domain show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster01::> network port broadcast-domain show
IPspace Broadcast                                       Update
Name    Domain Name    MTU  Port List                   Status Details
------- ----------- ------  --------------------------- --------------
Cluster Cluster       9000
                            cluster01-01:e0a            complete
                            cluster01-01:e0b            complete
                            cluster01-02:e0a            complete
                            cluster01-02:e0b            complete
Default Default       1500
                            cluster01-01:e0c            complete
                            cluster01-01:e0d            complete
                            cluster01-01:e0f            complete
                            cluster01-01:e0g            complete
                            cluster01-02:e0c            complete
                            cluster01-02:e0d            complete
                            cluster01-02:e0f            complete
                            cluster01-02:e0g            complete
ipspace-IC1
        ipspace-IC1-bd
                      1500
                            cluster01-01:e0e            complete
                            cluster01-01:e0f            complete
                            cluster01-02:e0e            complete
                            cluster01-02:e0f            complete
```

8. 시스템 SVM에 대한 인터클러스터 LIF를 생성한 후 이를 브로드캐스트 도메인에 할당합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	'network interface create-vserver_system_SVM_-lif_LIF_name_-service-policy default-인터클러스터 -home-node_node_-home-port_port_ -address_port_ip_-netmask_mask_'
• ONTAP 9.5 및 이전 버전의 경우: *	'network interface create-vserver_system_SVM_-lif_LIF_name_-role l인터클러스터-home-node_node_ -home-port_port_-address_port_ip_ -netmask_mask_'

LIF는 홈 포트가 할당된 브로드캐스트 도메인에서 생성됩니다. 브로드캐스트 도메인에는 브로드캐스트 도메인과 동일한 이름의 기본 페일오버 그룹이 있습니다. 에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 브로드캐스트 도메인 IPSpace-IC1-BD에 인터클러스터 LIF 'cluster01_icl01' 및 'cluster01_icl02'를 생성합니다.

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. 인터클러스터 LIF가 생성되었는지 확인합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	네트워크 인터페이스 show-service-policy default-인터클러스터
• ONTAP 9.5 및 이전 버전의 경우: *	네트워크 인터페이스 show-role 인터클러스터(network interface show-role 인터클러스터)

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
ipspace-IC1
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0f
true
```

10. 인터클러스터 LIF가 중복되는지 확인합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	네트워크 인터페이스 show-service-policy default-인터클러스터-failover를 선택합니다
• ONTAP 9.5 및 이전 버전의 경우: *	네트워크 인터페이스 show-role 인터클러스터-failover를 참조하십시오

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 SVM e0e 포트의 인터클러스터 LIF 'cluster01_icl01' 및 'cluster01_icl02'가 e0f 포트로 페일오버된 것을 보여줍니다.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
ipspace-IC1
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

피어 관계를 구성합니다

ONTAP 클러스터 피어 관계를 생성합니다

데이터 백업 및 재해 복구를 위해 데이터를 원격 클러스터에 복제하여 데이터를 보호하려면 로컬 및 원격 클러스터 간에 클러스터 피어 관계를 생성해야 합니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 스냅샷 복제를 설정하려면. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

몇 가지 기본 보호 정책을 사용할 수 있습니다. 사용자 지정 정책을 사용하려면 보호 정책을 만들어야 합니다.

시작하기 전에

ONTAP CLI를 사용하는 경우 다음 방법 중 하나를 사용하여 피어링할 클러스터의 모든 노드에 인터클러스터 LIF를 생성해야 합니다.

- "공유 데이터 포트에 대한 인터클러스터 LIF를 구성합니다"
- "전용 데이터 포트에 대한 인터클러스터 LIF를 구성합니다"
- "사용자 지정 IPspace에서 인터클러스터 LIF를 구성합니다"

단계

ONTAP 시스템 관리자 또는 ONTAP CLI를 사용하여 이 작업을 수행합니다.

시스템 관리자

1. 로컬 클러스터에서 * 클러스터 > 설정 * 을 클릭합니다.
2. Intercluster Settings * 섹션에서 * Add Network Interfaces * 를 클릭하고 IP 주소와 서브넷 마스크를 입력하여 클러스터에 대한 클러스터 간 네트워크 인터페이스를 추가합니다.

   원격 클러스터에서 이 단계를 반복합니다.
3. 원격 클러스터에서 * 클러스터 > 설정 * 을 클릭합니다.
4. Cluster Peers * 섹션을 클릭하고 * Generate Passphrase * 를 선택합니다.
5. 원격 ONTAP 클러스터 버전을 선택합니다.
6. 생성된 암호를 복사합니다.
7. 로컬 클러스터의 * 클러스터 피어 * 에서 * 피어 클러스터 * 를 클릭하고 * 피어 클러스터 * 를 선택합니다.
8. 피어 클러스터 * 창에서 암호를 붙여 넣고 * 클러스터 피어링 초기화 * 를 클릭합니다.

CLI를 참조하십시오

1. 대상 클러스터에서 소스 클러스터와의 피어 관계를 생성합니다.

```
cluster peer create -generate-passphrase -offer-expiration
<MM/DD/YYYY HH:MM:SS|1...7days|1...168hours> -peer-addrs
<peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name|*> -ipspace
<ipspace>
```

   '-generate-passphrase와 '-peer-addrs'를 모두 지정하면 '-peer-addrs'에 지정된 인터클러스터 LIF가 있는 클러스터만 생성된 암호를 사용할 수 있습니다.

   사용자 지정 IPspace를 사용하지 않는 경우에는 이 옵션을 무시할 `-ipspace` 수 있습니다. 에 대한 자세한 내용은 `cluster peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

   ONTAP 9.6 이상에서 피어링 관계를 생성하고 클러스터 간 피어링 통신을 암호화하지 않으려면, 암호화를 비활성화하려면 '-encryption-protocol-proposed none' 옵션을 사용해야 합니다.

   다음 예에서는 지정되지 않은 원격 클러스터와 클러스터 피어 관계를 생성하고 로컬 클러스터에서 SVM "VS1" 및 "VS2"와 피어 관계를 사전 승인합니다.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

다음 예에서는 인터클러스터 LIF IP 주소 192.140.112.103 및 192.140.112.104에서 원격 클러스터와 클러스터 피어 관계를 생성하고 로컬 클러스터의 SVM과의 피어 관계를 사전 승인합니다.

```
cluster02::> cluster peer create -generate-passphrase -peer-addrs
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101,192.140.112.102
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

다음 예에서는 지정되지 않은 원격 클러스터와 클러스터 피어 관계를 생성하고 로컬 클러스터에서 SVM `vs1' 및 VS2"와 피어 관계를 사전 승인합니다.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. 소스 클러스터에서 소스 클러스터를 대상 클러스터에 인증합니다.

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

에 대한 자세한 내용은 `cluster peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 인터클러스터 LIF IP 주소 192.140.112.101 및 192.140.112.102에서 원격 클러스터에 대한 로컬 클러스터를 인증합니다.

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship, use
a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

메시지가 나타나면 피어 관계에 대한 암호를 입력합니다.

3. 클러스터 피어 관계가 생성되었는지 확인합니다.

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance

                                 Peer Cluster Name: cluster02
                     Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
                Availability of the Remote Cluster: Available
                               Remote Cluster Name: cluster2
                               Active IP Addresses: 192.140.112.101,
192.140.112.102
                             Cluster Serial Number: 1-80-123456
                    Address Family of Relationship: ipv4
              Authentication Status Administrative: no-authentication
                 Authentication Status Operational: absent
                                 Last Update Time: 02/05 21:05:41
                     IPspace for the Relationship: Default
```

4. 피어 관계에서 노드의 접속 상태와 상태를 확인합니다.

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health
Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
```

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	"볼륨 재해 복구 준비 개요"

ONTAP 인터클러스터 **SVM** 피어 관계를 생성합니다

'vserver peer create' 명령을 사용하여 로컬 및 원격 클러스터의 SVM 간에 피어 관계를 생성할 수 있습니다.

시작하기 전에

- 소스 및 타겟 클러스터를 내다봐야 합니다.
- 원격 클러스터의 SVM에 대해 "사전 승인된" 피어 관계가 있어야 합니다.

  자세한 내용은 을 참조하십시오 "클러스터 피어 관계 생성".

이 작업에 대해

여러 SVM에 대한 피어 관계를 "사전 승인"하려면 SVM을 나열하세요. `-initial-allowed-vserver` 클러스터 피어 관계를 생성할 때의 옵션입니다. 자세한 내용은 을 "클러스터 피어 관계 생성"참조하십시오.

단계

1. 데이터 보호 대상 클러스터에서 피어링을 위해 사전 승인된 SVM을 표시합니다.

   'vserver peer permission show'

```
cluster02::> vserver peer permission show
Peer Cluster         Vserver               Applications
-------------------  --------------------  --------------------
cluster02            vs1,vs2               snapmirror
```

2. 데이터 보호 소스 클러스터에서 데이터 보호 대상 클러스터의 사전 승인된 SVM과 피어 관계를 생성합니다.

   'vserver peer create-vserver_local_SVM_-peer-vserver_remote_SVM_'

   에 대한 자세한 내용은 `vserver peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 로컬 SVM 'pvs1'과 사전 승인된 원격 SVM 'VS1' 간에 피어 관계를 생성합니다.

```
cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
```

3. SVM 피어 관계 확인:

   'vserver peer show'

```
cluster01::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

ONTAP 인터클러스터 **SVM** 피어 관계를 추가합니다

클러스터 피어 관계를 구성한 후 SVM을 생성할 경우 SVM에 대한 피어 관계를 수동으로 추가해야 합니다. 'vserver peer create' 명령을 사용하여 SVM 간에 피어 관계를 생성할 수 있습니다. 피어 관계가 생성된 후 원격 클러스터에서 'vserver peer accept'를 실행하여 피어 관계를 승인할 수 있습니다.

시작하기 전에

소스 및 타겟 클러스터를 내다봐야 합니다.

이 작업에 대해

로컬 데이터 백업을 위해 동일한 클러스터에서 SVM 간에 피어 관계를 생성할 수 있습니다. 에 대한 자세한 내용은 `vserver peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

관리자가 명령을 사용하여 제안된 SVM 피어 관계를 거부하는 경우가 `vserver peer reject` 있습니다. SVM 간 관계가 상태인 경우 `rejected` 관계를 삭제해야 새 관계를 생성할 수 있습니다. 에 대한 자세한 내용은 `vserver peer reject` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 데이터 보호 소스 클러스터에서 데이터 보호 타겟 클러스터의 SVM과 피어 관계를 생성합니다.

   'vserver peer create -vserver_local_SVM_-peer-vserver_remote_SVM_-applications SnapMirror|file-copy|lun-copy -peer -cluster_remote_cluster_'

   다음 예에서는 로컬 SVM `pvs1''과 원격 SVM` vs1" 간에 피어 관계를 생성합니다

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   -applications snapmirror -peer-cluster cluster02
   ```

   로컬 및 원격 SVM의 이름이 동일한 경우 _ local name _ 을(를) 사용하여 SVM 피어 관계를 생성해야 합니다.

   ```
   cluster01::> vserver peer create -vserver vs1 -peer-vserver
   vs1 -applications snapmirror -peer-cluster cluster01
   -local-name cluster1vs1LocallyUniqueName
   ```

2. 데이터 보호 소스 클러스터에서 피어 관계가 시작되었는지 확인합니다.

   'vserver peer show-all'

   에 대한 자세한 내용은 `vserver peer show-all` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 SVM `pvs1''과 SVM` vs1" 간의 피어 관계가 시작된 것을 보여 줍니다.

   ```
   cluster01::> vserver peer show-all
               Peer        Peer                        Peering
   Vserver     Vserver     State      Peer Cluster     Applications
   --------    --------    ---------  -------------    ------------
   pvs1        vs1         initiated   Cluster02         snapmirror
   ```

3. 데이터 보호 대상 클러스터에서 보류 중인 SVM 피어 관계를 표시합니다.

   'vserver peer show'

   에 대한 자세한 내용은 `vserver peer show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 'cluster02'에 대해 보류 중인 피어 관계를 나열합니다.

```
cluster02::> vserver peer show

                    Peer                Peer
Vserver             Vserver             State
-----------         -----------         ------------
vs1                 pvs1                pending
```

4. 데이터 보호 대상 클러스터에서 보류 중인 피어 관계를 승인합니다.

   'vserver peer accept -vserver_local_SVM_-peer-vserver_remote_SVM_'

   에 대한 자세한 내용은 `vserver peer accept` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 로컬 SVM 'VS1'과 원격 SVM 'pvs1' 간의 피어 관계를 승인합니다.

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. SVM 피어 관계 확인:

   'vserver peer show'

```
cluster01::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

피어 관계에서 **ONTAP** 클러스터 피어링 암호화를 활성화합니다

ONTAP 9.6부터 클러스터 피어링 암호화는 새로 생성한 모든 클러스터 피어링 관계에서 기본적으로 활성화됩니다. 클러스터 피어링 암호화는 미리 공유된 키(PSK) 및 전송 보안 계층(TLS)을 사용하여 클러스터 간 피어링 통신을 보호합니다. 그러면 피어링된 클러스터 사이에 보안 계층이 추가됩니다.

이 작업에 대해

피어링된 클러스터를 ONTAP 9.6 이상으로 업그레이드하고 ONTAP 9.5 이전 버전에서 피어링 관계가 생성된 경우, 업그레이드 후 클러스터 피어링 암호화를 수동으로 활성화해야 합니다. 클러스터 피어링 암호화를 활성화하려면 피어링 관계의 두 클러스터가 ONTAP 9.6 이상을 실행해야 합니다.

단계

1. 대상 클러스터에서 소스 클러스터와의 통신에 대해 암호화를 설정합니다.

   'cluster peer modify_source_cluster_-auth-status-admin use-authentication-encryption-protocol-proposed TLS-PSK

2. 메시지가 나타나면 암호를 입력합니다.
3. 데이터 보호 소스 클러스터에서 데이터 보호 대상 클러스터와의 통신을 위해 암호화를 설정합니다.

   'cluster peer modify_data_protection_destination_cluster_-auth-status-admin use-authentication-encryption-protocol-proposed TLS-PSK

4. 메시지가 표시되면 대상 클러스터에 입력한 것과 동일한 암호를 입력합니다.

에 대한 자세한 내용은 `cluster peer modify` "ONTAP 명령 참조입니다"을 참조하십시오.

피어 관계에서 **ONTAP** 클러스터 피어링 암호화를 제거합니다

기본적으로 클러스터 피어링 암호화는 ONTAP 9.6 이상에서 생성된 모든 피어 관계에서 활성화됩니다. 클러스터 간 피어링 통신에 암호화를 사용하지 않으려면 비활성화할 수 있습니다.

단계

1. 타겟 클러스터에서 소스 클러스터와의 통신을 수정하여 클러스터 피어링 암호화 사용을 중지합니다.
   - 암호화를 제거하고 인증을 유지하려면 다음을 입력합니다.

     ```
     cluster peer modify <source_cluster> -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - 암호화 및 인증 제거하기:
     i. 인증되지 않은 액세스를 허용하도록 클러스터 피어링 정책을 수정합니다.

     ```
     cluster peer policy modify -is-unauthenticated-access-permitted
     true
     ```

     ii. 암호화 및 인증 액세스 수정:

     ```
     cluster peer modify <source_cluster> -auth-status no-
     authentication
     ```

2. 메시지가 표시되면 암호를 입력합니다.
3. 암호를 다시 입력하여 확인합니다.
4. 소스 클러스터에서 대상 클러스터와의 통신에 대한 암호화를 해제합니다.
   - 암호화를 제거하고 인증을 유지하려면 다음을 입력합니다.

```
cluster peer modify <destination_cluster> -auth-status-admin use-
authentication -encryption-protocol-proposed none
```

◦ 암호화 및 인증 제거하기:

i. 인증되지 않은 액세스를 허용하도록 클러스터 피어링 정책을 수정합니다.

```
cluster peer policy modify -is-unauthenticated-access-permitted
true
```

ii. 암호화 및 인증 액세스 수정:

```
cluster peer modify <destination_cluster> -auth-status no-
authentication
```

5. 메시지가 표시되면 대상 클러스터에서 사용한 것과 동일한 암호 구문을 입력하고 다시 입력합니다.

로컬 스냅샷을 관리합니다

로컬 **ONTAP** 스냅샷 관리에 대해 자세히 알아보십시오

스냅샷 _ 은(는) 볼륨의 읽기 전용 시점 이미지입니다. 이미지는 마지막 스냅샷 이후 파일의 변경 사항만 기록하기 때문에 최소한의 저장 공간을 사용하고 성능 오버헤드를 거의 일으키지 않습니다.

스냅샷을 사용하여 볼륨의 전체 내용을 복원하거나 개별 파일 또는 LUN을 복구할 수 있습니다. 스냅샷은 볼륨의 디렉토리에 저장됩니다. `.snapshot`

ONTAP 9.4 이상에서는 FlexVol volume 최대 1023개의 스냅샷을 포함할 수 있습니다. ONTAP 9.3 이하 버전에서는 볼륨에 최대 255개의 스냅샷을 포함할 수 있습니다.

ONTAP 9.8부터 FlexGroup 볼륨에는 1023개의 스냅샷이 포함될 수 있습니다. 자세한 내용은 을 "스냅샷을 사용하여 FlexGroup 볼륨을 보호합니다"참조하십시오.

ONTAP 장기 보존 스냅샷에 대해 알아보세요

정책 유형이 "vault" 또는 "mirror-vault"인 SnapMirror 관계를 사용하면 SnapMirror 관계의 보조 볼륨에 직접 스냅샷을 생성할 수 있습니다. 이러한 스냅샷은 대상 위치에 백업으로 보관됩니다. 이러한 스냅샷은 장기간 보존을 위해 생성되는 경우가 많으며, 장기 보존 스냅샷이라고 합니다.

SnapMirror 정책 규칙에서 스냅샷 생성 일정, 스냅샷 이름 접두사, SnapMirror 레이블 및 보존 횟수를 지정하여 장기 보존 스냅샷을 만듭니다. 이 스냅샷은 소스의 보존 규칙에 관계없이 SnapMirror 대상 볼륨에 보존됩니다.

장기 보존 스냅샷은 FlexVol SnapMirror 구성에서만 사용할 수 있습니다. FlexGroup SnapMirror 구성에 대해서는

장기 보존 스냅샷을 생성할 수 없습니다.

SnapMirror 캐스케이드 관계에서는 장기 보존 스냅샷을 캐스케이드의 마지막 볼륨에만 만들 수 있습니다.

관련 정보

- "캐스케이드 배포가 작동하는 방식에 대해 알아보세요"
- "ONTAP SnapMirror 스케줄을 정의하여 대상에 로컬 복제본을 생성합니다"

사용자 지정 스냅샷 정책을 구성합니다

사용자 지정 **ONTAP** 스냅샷 정책을 구성하는 방법에 대해 자세히 알아보십시오

스냅샷 정책 _ 은(는) 시스템에서 스냅샷을 생성하는 방법을 정의합니다. 정책은 스냅샷을 생성할 시기, 보존할 복제본 수 및 스냅샷 이름을 지정하는 방법을 지정합니다. 예를 들어 시스템은 매일 오전 12시 10분에 스냅샷 하나를 생성하고 가장 최근의 복제본 두 개를 보존하며 복제본 이름을 "`daily""로 지정할 수 있습니다.*timestamp*.

볼륨에 대한 기본 정책은 다음 일정에 따라 스냅샷을 자동으로 생성하며 가장 오래된 스냅샷은 삭제되어 새 복제본을 위한 공간을 확보합니다.

- 시간당 최대 6개의 스냅샷이 해당 시간 이후 5분 동안 촬영되었습니다.
- 월요일부터 토요일까지 자정 이후 10분에 최대 2개의 일일 스냅샷을 촬영합니다.
- 매주 일요일 자정 이후 15분에 최대 2개의 주간 스냅샷이 촬영됩니다.

볼륨을 생성할 때 스냅샷 정책을 지정하지 않으면 해당 볼륨이 포함된 SVM(스토리지 가상 머신)과 연결된 스냅샷 정책을 상속합니다.

사용자 지정 **ONTAP** 스냅샷 정책을 구성하는 경우

기본 스냅샷 정책이 볼륨에 적합하지 않은 경우 스냅샷의 빈도, 보존 및 이름을 수정하는 사용자 지정 정책을 구성할 수 있습니다. 스케줄은 주로 활성 파일 시스템의 변경 속도에 따라 결정됩니다.

자주 사용하지 않는 파일을 하루에 한 번 백업하면서 자주 사용하는 파일 시스템을 데이터베이스와 같이 백업할 수 있습니다. 데이터베이스의 경우에도 일반적으로 전체 백업을 하루에 한 번 또는 두 번 실행하는 동시에 트랜잭션 로그를 매시간 백업합니다.

그 밖의 요인은 귀사에 파일이 중요한 이유, SLA(서비스 수준 계약), RPO(복구 시점 목표) 및 RTO(복구 시간 목표)입니다. 일반적으로 필요한 만큼의 스냅샷만 보존해야 합니다.

ONTAP 스냅샷 작업 일정을 생성합니다

스냅샷 정책에는 스냅샷 작업 스케줄이 하나 이상 필요합니다. System Manager 또는 명령을 사용하여 작업 일정을 생성할 수 있습니다 `job schedule cron create`. 에 대한 자세한 내용은 `job schedule cron create` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 스냅샷 작업 일정을 생성합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

기본적으로 ONTAP는 작업 일정 이름에 타임스탬프를 추가하여 스냅샷의 이름을 구성합니다.

해당 월의 요일 및 요일에 대한 값을 모두 지정하면 값은 독립적으로 간주됩니다. 예를 들어, 일 사양 금요일과 월 사양 13일이 포함된 cron 일정은 금요일이 아니라 매달 13일에 각각 금요일과 13일에 실행됩니다.

예 **30.** 단계

시스템 관리자

1. Protection > Overview * 로 이동하고 * Local policy settings * 를 확장합니다.
2. Schedules * 창에서 를 →클릭합니다.
3. Schedules * 창에서 를 + Add 클릭합니다.
4. 일정 추가 * 창에서 일정 이름을 입력하고 컨텍스트 및 일정 유형을 선택합니다.
5. 저장 * 을 클릭합니다.

CLI를 참조하십시오

1. 작업 일정 생성:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

월-일-일-주-시-시간의 경우 월, 일, 시 순으로 모두 작업을 실행하도록 지정할 수 있습니다.

ONTAP 9.10.1.1부터는 작업 일정에 SVM을 포함할 수 있습니다.

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

다음 예에서는 토요일 오전 3시에 실행되는 'myweekly'라는 작업 일정을 생성합니다.

```
cluster1::> job schedule cron create -name myweekly -dayofweek
"Saturday" -hour 3 -minute 0
```

다음 예제에서는 여러 일, 시간 및 분을 지정하는 mywelymulti라는 일정을 만듭니다.

```
job schedule cron create -name myweeklymulti -dayofweek
"Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
```

ONTAP 스냅샷 정책을 생성합니다

스냅샷 정책은 스냅샷을 생성할 시기, 보존할 복제본 수 및 스냅샷 이름을 지정하는 방법을 지정합니다. 예를 들어 시스템은 매일 오전 12시 10분에 스냅샷 하나를 생성하고 가장 최근의 복제본 두 개를 보존하고 이름을 ""매일""로 지정할 수.*timestamp* 있습니다. 스냅샷 정책에는 최대 5개의 작업 일정을 포함할 수 있습니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 스냅샷 정책을 생성합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

기본적으로 ONTAP는 작업 일정 이름에 타임스탬프를 추가하여 스냅샷의 이름을 구성합니다.

```
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

원하는 경우 작업 스케줄 이름의 접두사를 대체할 수 있습니다.

'스냅샷 레이블' 옵션은 SnapMirror 복제용 옵션입니다. 자세한 내용은 을 참조하십시오 "정책 규칙 정의".

단계

System Manager 또는 ONTAP CLI를 사용하여 스냅샷 정책을 생성할 수 있습니다. 이 절차에서는 로컬 클러스터에만 스냅샷 정책을 생성합니다.

시스템 관리자

1. Protection > Overview * 로 이동하고 * Local policy settings * 를 확장합니다.
2. Snapshot policies * 창에서 를 →클릭합니다.
3. Snapshot policies * 탭에서 를 + Add 클릭합니다.
4. Add snapshot policy * 창에서 정책 이름을 입력하고 범위를 선택합니다.
5. 을 클릭합니다 + Add .
6. 일정을 선택하려면 현재 표시된 일정 이름을 클릭하고 를 ⌄클릭한 다음 다른 일정을 선택합니다.
7. 보존할 최대 스냅샷을 입력하고 필요한 경우 SnapMirror 레이블 및 SnapLock 보존 기간을 입력합니다.
8. 저장 * 을 클릭합니다.

CLI를 참조하십시오

1. 스냅샷 정책 생성:

```
volume snapshot policy create -vserver <SVM> -policy <policy_name>
-enabled true|false -schedule1 <schedule1_name> -count1
<copies_to_retain> -prefix1 <snapshot_prefix> -snapmirror-label1
<snapshot_label> ... -schedule5 <schedule5_name> -count5
<copies_to_retain> -prefix5 <snapshot_prefix> -snapmirror-label5
<snapshot_label>
```

다음 예에서는 일정에 따라 실행되는 `daily` 라는 스냅샷 정책을 `snap_policy_daily` 생성합니다. 정책에는 최대 5개의 스냅샷이 있으며 각 스냅샷에는 `daily.timestamp` 이름과 SnapMirror 레이블이 `daily`있습니다.

```
cluster1::> volume snapshot policy create -vserver vs0 -policy
snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1
daily
```

스냅샷을 수동으로 관리합니다

스냅샷을 수동으로 생성하고 삭제합니다

예약된 스냅샷이 생성될 때까지 기다릴 수 없는 경우 스냅샷을 수동으로 생성할 수 있으며 더 이상 필요하지 않은 경우 스냅샷을 삭제할 수 있습니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 주문형 스냅샷을 생성합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

스냅샷을 수동으로 생성합니다

System Manager 또는 ONTAP CLI를 사용하여 스냅샷을 수동으로 생성할 수 있습니다.

시스템 관리자

단계

1. 저장소 **>** 볼륨*으로 이동하여 *스냅샷 탭을 선택합니다.
2. 을 클릭합니다 + Add .
3. Add a snapshot * 창에서 기본 스냅샷 이름을 그대로 사용하거나 원하는 경우 편집합니다.
4. * 선택 사항 *: SnapMirror 레이블 추가
5. 추가 * 를 클릭합니다.

CLI를 참조하십시오

1. 스냅샷 생성:

```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

스냅샷을 수동으로 삭제합니다

System Manager 또는 ONTAP CLI를 사용하여 스냅샷을 수동으로 삭제할 수 있습니다.

시스템 관리자

단계

1. 스토리지 > 볼륨 * 으로 이동하고 * Snapshot 복사본 * 탭을 선택합니다.
2. 삭제하려는 스냅샷을 찾아 를 클릭하고 * Delete * 를 선택합니다.
3. 스냅샷 삭제 * 창에서 * 스냅샷 삭제 * 를 선택합니다.
4. 삭제 * 를 클릭합니다.

CLI를 참조하십시오

1. 명령을 사용하여 `volume snapshot show` 삭제할 스냅샷을 확인합니다.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

이 예에서 명령은 SVM vs3의 볼륨 vol3에 대한 스냅샷을 표시합니다.

```
cluster::> volume snapshot show -vserver vs3 -volume vol3

                                                  ---Blocks---
Vserver  Volume  Snapshot                  Size   Total% Used%
-------- ------- ------------------------ -----  ------ -----
vs3      vol3
                 snap1.2013-05-01_0015   100KB   0%    38%
                 snap1.2013-05-08_0015   76KB    0%    32%
                 snap2.2013-05-09_0010   76KB    0%    32%
                 snap2.2013-05-10_0010   76KB    0%    32%
                 snap3.2013-05-10_1005   72KB    0%    31%
                 snap3.2013-05-10_1105   72KB    0%    31%
                 snap3.2013-05-10_1205   72KB    0%    31%
                 snap3.2013-05-10_1305   72KB    0%    31%
                 snap3.2013-05-10_1405   72KB    0%    31%
                 snap3.2013-05-10_1505   72KB    0%    31%
10 entries were displayed.
```

2. 스냅샷 삭제:

원하는 작업	이 명령을 입력하십시오...
단일 스냅샷을 삭제합니다	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name_`

원하는 작업	이 명령을 입력하십시오...
여러 스냅샷을 삭제합니다	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name1_[,_snapshot_name2_,...]`
모든 스냅샷을 삭제합니다	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot *`

스냅샷을 삭제하기 전에 재확보 가능한 공간을 계산합니다

ONTAP 9.10.1부터 System Manager를 사용하여 삭제할 스냅샷을 선택하고 삭제하기 전에 재확보 가능한 공간을 계산할 수 있습니다.

단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 스냅샷을 삭제할 볼륨을 선택합니다.
3. *스냅샷*을 클릭하세요.
4. 스냅샷을 하나 이상 선택합니다.
5. 회수 가능 공간 계산 * 을 클릭합니다.

스냅숏 예비 공간을 관리합니다

ONTAP 스냅숏 예비 공간 관리에 대해 자세히 알아봅니다

snapshot reserve_는 스냅샷을 위한 디스크 공간의 비율을 기본값으로 5%로 설정합니다. 스냅숏 예비 공간이 소진된 경우 스냅숏은 활성 파일 시스템의 공간을 사용하므로 필요에 따라 스냅숏 예비 공간을 늘릴 수 있습니다. 또는 예약이 꽉 차면 스냅샷을 자동으로 삭제할 수 있습니다.

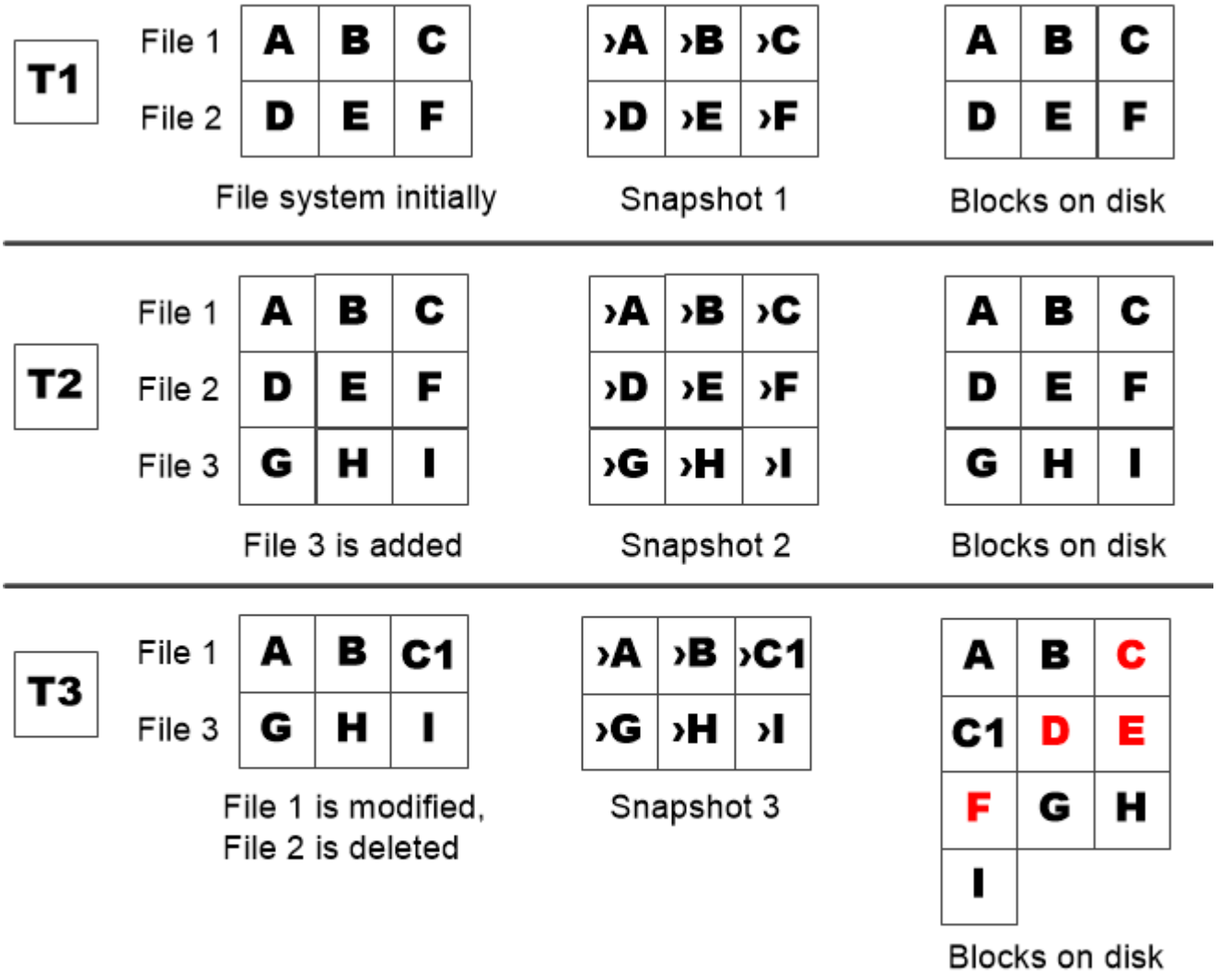
스냅숏 예비 공간을 늘릴 시기

스냅숏 예비 공간을 증가할지 여부를 결정할 때 스냅숏은 마지막 스냅숏이 만들어진 이후 파일의 변경 내용만 기록한다는 점을 기억해야 합니다. 활성 파일 시스템의 블록이 수정되거나 삭제될 때만 디스크 공간을 사용합니다.

즉, 파일 시스템의 변경률이 스냅샷에서 사용되는 디스크 공간의 양을 결정하는 데 중요한 요소가 됩니다. 생성한 스냅샷 수에 관계없이 활성 파일 시스템이 변경되지 않은 경우 디스크 공간을 소비하지 않습니다.

예를 들어 데이터베이스 트랜잭션 로그를 포함하는 FlexVol volume의 경우 변경 속도를 높이기 위해 20%의 스냅숏 예비 공간이 있을 수 있습니다. 더 자주 업데이트되는 데이터베이스를 캡처하기 위해 더 많은 스냅샷을 생성할 수 있을 뿐만 아니라 스냅샷이 사용하는 추가 디스크 공간을 처리할 수 있도록 더 큰 스냅숏 예비 공간이 필요합니다.

스냅샷은 블록 복제본이 아닌 블록에 대한 포인터로 구성됩니다. 포인터는 블록의 "클레임"이라고 생각할 수 있습니다. ONTAP는 스냅샷이 삭제될 때까지 블록을 "보류"합니다.



A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.

보호된 파일을 삭제하면 예상보다 파일 공간이 줄어들 수 있습니다

스냅샷은 해당 블록을 사용한 파일을 삭제한 후에도 해당 블록을 가리킵니다. 따라서 스냅숏 예비 공간이 소진되면 전체 파일 시스템을 삭제하면 사용 중인 파일 시스템보다 사용 가능한 공간이 줄어드는 직관적인 결과가 발생할 수 있습니다.

다음 예제를 고려해 보십시오. 파일을 삭제하기 전에 'df' 명령 출력은 다음과 같습니다.

```
Filesystem           kbytes  used    avail  capacity
/vol/vol0/           3000000 3000000 0       100%
/vol/vol0/.snapshot 1000000 500000  500000   50%
```

전체 파일 시스템을 삭제하고 볼륨의 스냅샷을 생성한 후 `df` 명령은 다음 출력을 생성합니다.

```
Filesystem           kbytes  used    avail  capacity
/vol/vol0/           3000000 2500000 500000   83%
/vol/vol0/.snapshot 1000000 3500000 0       350%
```

출력에서 알 수 있듯이, 이전에 활성 파일 시스템에서 사용했던 3GB의 전체 용량이 삭제되기 전에 사용된 0.5GB와 함께 스냅샷에 사용되고 있습니다.

스냅샷이 사용하는 디스크 공간이 스냅샷 예비 공간을 초과하기 때문에 활성 파일용으로 예약된 공간에 2.5GB의 "스필" 오버플로우가 발생하여 3GB가 예상될 수 있는 파일용으로 0.5GB의 여유 공간이 남습니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP 스냅샷 디스크 사용량 모니터링

명령을 사용하여 스냅샷 디스크 사용량을 모니터링할 수 `df` 있습니다. 이 명령은 활성 파일 시스템의 사용 가능한 공간과 스냅숏 예비 공간을 표시합니다.

단계

1. 스냅샷 디스크 사용량 표시: `df`

   다음 예에서는 스냅샷 디스크 사용량을 보여 줍니다.

   ```
   cluster1::> df
   Filesystem           kbytes  used    avail  capacity
   /vol/vol0/           3000000 3000000 0       100%
   /vol/vol0/.snapshot 1000000 500000  500000   50%
   ```

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

볼륨에서 사용 가능한 **ONTAP** 스냅숏 예비 공간을 확인합니다

매개 변수를 명령과 함께 `volume show` 사용하여 볼륨에서 사용 가능한 스냅숏 예비 공간의 양을 확인할 수 `snapshot-reserve-available` 있습니다. 에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 볼륨에서 사용 가능한 스냅숏 예비 공간을 확인합니다.

'vol show -vserver_SVM_-volume_volume_-fields snapshot-reserve-available'

다음 예는 에 대해 사용 가능한 스냅숏 예비 공간을 `vol1` 표시합니다.

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available
------- ------ --------------------------
vs0     vol1   4.84GB
```

ONTAP 스냅숏 예비 공간을 수정합니다

스냅샷이 활성 파일 시스템에 예약된 공간을 사용하지 않도록 더 큰 스냅숏 예비 공간을 구성할 수 있습니다. 스냅샷을 위한 공간이 더 이상 필요하지 않으면 스냅숏 예비 공간을 줄일 수 있습니다.

단계

1. 스냅숏 예비 공간을 수정합니다.

   'volume modify -vserver_SVM_-volume_volume_- percent-snapshot-space_snap_reserve_'

   에 대한 자세한 내용은 `volume modify` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 에 대한 스냅숏 예비 공간을 `vol1` 10%로 설정합니다.

   ```
   cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
   -space 10
   ```

자동 삭제 ONTAP 스냅샷

명령을 사용하여 스냅숏 예비 공간이 초과되었을 때 스냅숏의 자동 삭제를 트리거할 수 `volume snapshot autodelete modify` 있습니다. 기본적으로 가장 오래된 스냅샷이 먼저 삭제됩니다. 에 대한 자세한 내용은 `volume snapshot autodelete modify` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

LUN 및 파일 클론은 삭제할 스냅샷이 더 이상 없으면 삭제됩니다.

단계

1. 자동 삭제 스냅샷:

   '볼륨 스냅샷 자동 삭제 수정 - vserver_SVM_-volume_volume_-enabled true|false-trigger volume|snap_reserve'

다음 예에서는 스냅숏 예비 공간이 소진된 경우 스냅샷을 자동으로 `vol1` 삭제합니다.

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1
-enabled true -trigger snap_reserve
```

스냅샷에서 파일을 복원합니다

NFS 또는 **SMB** 클라이언트의 **ONTAP** 스냅샷에서 파일을 복구합니다

NFS 또는 SMB 클라이언트의 사용자는 스토리지 시스템 관리자의 개입 없이 스냅샷에서 직접 파일을 복구할 수 있습니다.

파일 시스템의 모든 디렉토리에는 NFS 및 SMB 사용자가 액세스할 수 있는 하위 디렉토리가 포함되어 `.snapshot` 있습니다. `.snapshot`하위 디렉토리에는 볼륨의 스냅샷에 해당하는 하위 디렉토리가 포함되어 있습니다.

```
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

각 하위 디렉토리에는 스냅샷이 참조하는 파일이 포함됩니다. 사용자가 실수로 파일을 삭제하거나 덮어쓸 경우 파일을 스냅샷 하위 디렉토리에서 읽기-쓰기 디렉토리로 복사하여 상위 읽기-쓰기 디렉토리로 복원할 수 있습니다.

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

ONTAP 스냅샷 디렉토리에 대한 **NFS** 및 **SMB** 클라이언트 액세스를 설정 및 해제합니다

명령의 ONTAP CLI 옵션을 `volume modify` 사용하여 스냅샷 디렉토리에 대한 액세스를 사용하거나 사용하지 않도록 설정할 수 `-snapdir-access` 있으며, ONTAP 9.10.1부터 System Manager를 사용하여 클라이언트 시스템이 볼륨의 스냅샷 디렉토리에 액세스하도록 설정하거나 해제할 수 있습니다. 액세스를 활성화하면 스냅샷 디렉토리가 클라이언트에 표시되고 Windows 클라이언트가 스냅샷 디렉토리에 드라이브를 매핑하여 해당 컨텐츠를 보고 액세스할 수 있습니다. 그러면 NFS 및 SMB 클라이언트가 스냅샷에서 파일 또는 LUN을 복구할 수

있습니다.

볼륨 설정을 편집하거나 볼륨의 공유 설정을 편집하여 볼륨의 스냅샷 디렉터리에 대한 액세스를 활성화하거나 비활성화할 수 있습니다.

볼륨을 편집하여 스냅샷 디렉토리에 대한 클라이언트 액세스를 설정 또는 해제합니다

단계

ONTAP System Manager 또는 ONTAP CLI를 사용하여 클라이언트 스냅샷 디렉토리 액세스를 사용하거나 사용하지 않도록 설정할 수 있습니다. 볼륨의 스냅샷 디렉토리는 기본적으로 클라이언트가 액세스할 수 있습니다.

시스템 관리자

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 표시하거나 숨길 스냅샷 디렉토리가 포함된 볼륨을 선택합니다.
3. 을 ⋮ 클릭하고 * 편집 * 을 선택합니다.
4. 스냅샷(로컬) 설정 섹션에서 *클라이언트에 스냅샷 디렉터리 표시*를 선택하거나 선택 해제합니다.
5. 저장 * 을 클릭합니다.

CLI를 참조하십시오

1. 스냅샷 디렉토리 액세스 상태를 확인합니다.

```
volume show -vserver <SVM_name> -volume <vol_name> -fields snapdir-
access
```

예:

```
clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-
access
vserver volume snapdir-access
------- ------ --------------
vs0     vol1   false
```

에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 스냅샷 디렉토리 액세스를 설정하거나 해제합니다.

```
volume modify -vserver <SVM_name> -volume <vol_name> -snapdir-access
<true|false>
```

다음 예에서는 vol1에서 스냅샷 디렉토리 액세스를 설정합니다.

```
clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access
true
Volume modify successful on volume vol1 of Vserver vs0.
```

에 대한 자세한 내용은 `volume modify` "ONTAP 명령 참조입니다"을 참조하십시오.

공유를 편집하여 스냅샷 디렉토리에 대한 클라이언트 액세스를 설정하거나 해제합니다

볼륨의 스냅샷 디렉토리는 기본적으로 클라이언트가 액세스할 수 있습니다.

단계

1. 스토리지 > 공유 * 를 클릭합니다.
2. 표시하거나 숨길 스냅샷 디렉토리가 포함된 볼륨을 선택합니다.
3. 을 ⋮ 클릭하고 * 편집 * 을 선택합니다.
4. Share Properties * 섹션에서 * Allow clients to access snapshots directory * 를 선택하거나 선택 취소합니다.
5. 저장 * 을 클릭합니다.

ONTAP 스냅샷에서 단일 파일을 복구합니다

명령을 사용하여 스냅샷에서 단일 파일 또는 LUN을 복원할 수 `volume snapshot restore-file` 있습니다. 기존 파일을 바꾸지 않으려는 경우 상위 읽기-쓰기 볼륨의 다른 위치로 파일을 복원할 수 있습니다.

이 작업에 대해

기존 LUN을 복구하는 경우 LUN 클론이 생성되고 스냅샷 형태로 백업됩니다. 복원 작업 중에 LUN에서 읽거나 LUN에 쓸 수 있습니다.

스트림이 있는 파일은 기본적으로 복원됩니다.

단계

1. 볼륨의 스냅샷을 나열합니다.

   'volume snapshot show -vserver_SVM_-volume_volume_'

   에 대한 자세한 내용은 `volume snapshot show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예는 의 스냅샷을 `vol1` 보여 줍니다.

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. 스냅샷에서 파일 복구:

   '볼륨 스냅샷 복원 - 파일 - vserver_SVM_-volume_volume_-snapshot_snapshot_-path_file_path_-restore-path_destination_path_'

에 대한 자세한 내용은 `volume snapshot restore-file` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 myfile.txt 파일을 복구합니다.

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

ONTAP 스냅샷에서 파일의 일부를 복원합니다

데이터의 시작 바이트 오프셋과 바이트 수를 알고 있다고 가정하면 명령을 사용하여 스냅샷에서 LUN으로 데이터 범위를 복원할 수 있습니다 `volume snapshot partial-restore-file`. 이 명령을 사용하여 여러 데이터베이스를 동일한 LUN에 저장하는 호스트에서 데이터베이스 중 하나를 복원할 수 있습니다.

ONTAP 9.12.1부터 를 사용하는 볼륨에 대해 부분 복원을 사용할 수 SnapMirror 활성 동기화있습니다.

단계

1. 볼륨의 스냅샷을 나열합니다.

   'volume snapshot show -vserver_SVM_-volume_volume_'

   에 대한 자세한 내용은 `volume snapshot show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예는 의 스냅샷을 `vol1` 보여 줍니다.

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. 스냅샷에서 파일의 일부를 복원합니다.

   '볼륨 스냅샷 부분 복구 파일 - vserver_SVM_-volume_volume_-snapshot_snapshot_-path_file_path_-start-byte_starting_byte_-byte-count_byte_count_'

   시작 바이트 오프셋 및 바이트 수는 4,096의 배수여야 합니다.

다음 예에서는 myfile.txt 파일의 첫 4,096바이트를 복원합니다.

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0
-byte-count 4096
```

ONTAP 스냅숏에서 볼륨의 내용을 복원합니다

스냅숏에서 복원하면 볼륨을 이전 시점으로 복구할 수 있습니다. System Manager 또는 명령을 사용하여 스냅샷에서 볼륨의 내용을 복원할 수 `volume snapshot restore` 있습니다. 에 대한 자세한 내용은 `volume snapshot restore` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

볼륨에 SnapMirror 관계가 있는 경우 스냅샷에서 복구한 직후 볼륨의 모든 미러 복사본을 수동으로 복제합니다. 그렇지 않으면 미러 복사본을 사용할 수 없게 되므로 복사본을 삭제하고 다시 생성해야 합니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 이전 스냅샷에서 복원할 수 있습니다.

시스템 관리자

1. Storage * 를 클릭하고 볼륨을 선택합니다.
2. Snapshot 복사본 * 에서 복원할 스냅샷 옆의 를 클릭하고 * 복원 * 을 선택합니다.

CLI를 참조하십시오

1. 볼륨의 스냅샷을 나열합니다.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

다음 예에서는 의 스냅샷을 `vol1` 보여 줍니다.

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. 스냅숏에서 볼륨의 내용 복원:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

다음 예에서는 vol1의 내용을 복원합니다.

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

SnapMirror 볼륨 복제

SnapMirror 볼륨 복제에 대해 알아보십시오

ONTAP SnapMirror 비동기식 재해 복구에 대해 알아보십시오

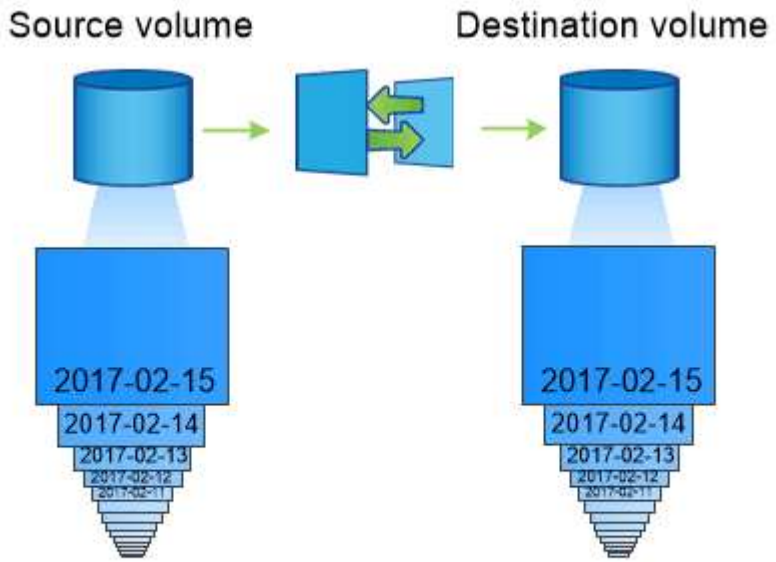
_SnapMirror_는 지리적으로 원격 사이트의 운영 스토리지에서 보조 스토리지로 페일오버하도록 설계된 재해 복구 기술입니다. 그 이름이 시사하듯이 SnapMirror는 운영 사이트에서 재해가 발생한 경우에도 데이터를 계속 제공할 수 있는 보조 스토리지에 작업 데이터의 복제본 또는 _MIRROR_를 생성합니다.

운영 사이트에서 데이터를 계속 제공할 수 있는 경우 필요한 데이터를 다시 전송하여 미러에서 클라이언트를 전혀 제공하지 않고 그대로 제공할 수 있습니다. 페일오버 사용 사례에서 알 수 있듯이, 2차 시스템의 컨트롤러는 미러링된 스토리지의 데이터를 효율적으로 지원하기 위해 운영 시스템의 컨트롤러와 동등하거나 거의 동등해야 합니다.

데이터 보호 관계

데이터가 볼륨 레벨에서 미러링됩니다. 운영 스토리지의 소스 볼륨과 2차 스토리지의 타겟 볼륨 간의 관계를 _ 데이터 보호 관계라고 합니다. _ 볼륨이 상주하는 클러스터와 볼륨의 데이터를 제공하는 SVM이 되어야 합니다."자세히 들여다보았습니다" 피어 관계를 통해 클러스터와 SVM이 데이터를 안전하게 교환할 수 있습니다.

다음 그림에서는 SnapMirror 데이터 보호 관계를 보여 줍니다.



A SnapMirror data protection relationship typically mirrors the Snapshot copies available on the source volume.

데이터 보호 관계의 범위

볼륨 간 또는 볼륨을 소유한 SVM 간에 직접 데이터 보호 관계를 생성할 수 있습니다. SVM 데이터 보호 관계에서는 NFS 엑스포트 및 SMB 공유에서 RBAC에 이르는 SVM 구성의 전체 또는 일부를 복제할 뿐만 아니라 SVM이 소유한 볼륨의 데이터도 복제됩니다.

또한 다음과 같은 특수 데이터 보호 애플리케이션용 SnapMirror를 사용할 수도 있습니다.

- SVM 루트 볼륨의 _load 공유 mirror_copy를 사용하면 노드 운영 중단 또는 페일오버 발생 시에도 데이터에 액세스할 수 있습니다.

- SnapLock 볼륨 _ 간의 데이터 보호 관계를 통해 WORM 파일을 보조 스토리지로 복제할 수 있습니다.

  "SnapLock 기술을 사용한 아카이브 및 규정 준수"

- ONTAP 9.13.1부터 SnapMirror 비동기식을 사용하여 보호할 수 정합성 보장 그룹있습니다. ONTAP 9.14.1부터 SnapMirror 비동기식을 사용하여 일관성 그룹 관계를 사용하여 볼륨 세분화 스냅샷을 타겟 클러스터에 복제할 수 있습니다. 자세한 내용은 을 SnapMirror 비동기식 보호를 구성합니다참조하십시오.

SnapMirror 데이터 보호 관계가 초기화된 방식

SnapMirror를 처음 호출하면 소스 볼륨에서 대상 볼륨으로 _baseline transfer_를 수행합니다. 관계에 대한 _SnapMirror 정책_은 기준 및 모든 업데이트의 내용을 정의합니다.

기본 SnapMirror 정책 'MirorAllSnapshots'에 따른 기본 전송에는 다음 단계가 포함됩니다.

- 소스 볼륨의 스냅샷을 생성합니다.
- 스냅샷과 해당 스냅샷이 참조하는 모든 데이터 블록을 대상 볼륨으로 전송합니다.
- ""활성"" 미러가 손상된 경우 사용할 수 있도록 소스 볼륨의 나머지 덜 최근의 스냅샷을 대상 볼륨으로 전송합니다.

SnapMirror 데이터 보호 관계가 업데이트되는 방법

업데이트는 구성한 일정에 따라 비동기식입니다. 보존은 소스의 스냅샷 정책을 미러링합니다.

정책에 따라 업데이트될 때마다 `MirrorAllSnapshots` SnapMirror는 소스 볼륨의 스냅샷을 생성하고 해당 스냅샷과 마지막 업데이트 이후에 생성된 모든 스냅샷을 전송합니다. 정책의 다음 출력에서 다음 `snapmirror policy show` 사항에 `MirrorAllSnapshots` 유의하십시오.

- `Create Snapshot` 는 SnapMirror에서 관계를 업데이트할 때 스냅샷을 생성함을 나타내는 ""true"" `MirrorAllSnapshots`입니다.
- `MirrorAllSnapshots` 에는 SnapMirror가 관계를 업데이트할 때 SnapMirror에서 생성한 스냅샷과 마지막 업데이트 이후에 생성된 모든 스냅샷이 모두 전송됨을 나타내는 "'sm_created'" 및 "'all_source_snapshots'" 규칙이 있습니다.

```
cluster_dst::> snapmirror policy show -policy MirrorAllSnapshots -instance

                     Vserver: vs0
      SnapMirror Policy Name: MirrorAllSnapshots
      SnapMirror Policy Type: async-mirror
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: SnapMirror asynchronous policy for mirroring
all snapshots
                              and the latest active file system.
       Total Number of Rules: 2
                  Total Keep: 2
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              all_source_snapshots    1  false       0 -
-
```

대칭 복사 정책

사전 구성된 `MirrorLatest` 정책은 SnapMirror에서 생성된 스냅샷만 초기화 및 업데이트 시 전송된다는 점을 제외하고 와 동일하게 `MirrorAllSnapshots` 작동합니다.

```
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
```

관련 정보

- "스냅미러 정책 보기"

ONTAP SnapMirror 동기식 재해 복구 에 대해 알아보십시오

ONTAP 9.5부터, SnapMirror 동기(SM-S) 기술은 최소 16GB의 메모리가 있는 모든 FAS 및

AFF 플랫폼 및 모든 ONTAP Select 플랫폼에서 지원됩니다. SnapMirror 동기식 기술은 볼륨 레벨에서 동기식 데이터 복제를 제공하는 라이센스된 노드별 기능입니다.

이 기능은 데이터 손실이 전혀 필요하지 않는 금융, 의료 및 기타 규제 대상 산업에서 동기식 복제에 대한 규제 및 국가 차원의 요구를 해결합니다.

SnapMirror 동기식 작업이 허용됩니다

HA 쌍당 SnapMirror 동기식 복제 작업 수의 제한은 컨트롤러 모델에 따라 다릅니다.

다음 표에는 플랫폼 유형 및 ONTAP 릴리즈에 따라 HA 쌍당 허용되는 SnapMirror 동기식 작업의 수가 나와 있습니다.

플랫폼	ONTAP 9.14.1부터 ONTAP 9.11.1까지	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.9.1 이전 릴리즈
AFF	400	200	160	80
ASA	400	200	160	80
FAS	80	80	80	40
ONTAP Select	40	40	40	20

지원되는 기능

다음 표에는 SnapMirror Synchronous 및 지원이 제공되는 ONTAP 릴리스에서 지원되는 기능이 나와 있습니다.

피처	첫 번째 릴리스가 지원됩니다	추가 정보
SnapMirror 동기식 관계의 운영 볼륨에 대한 바이러스 백신	ONTAP 9.6	
애플리케이션이 생성한 스냅샷 복제입니다	ONTAP 9.7	스냅샷이 해당 시점에 적절한 레이블로 태그된 경우 `snapshot create` SnapMirror CLI나 ONTAP API를 사용하여 애플리케이션을 정지시킨 후 사용자가 생성한 스냅샷이나 외부 스크립트로 생성한 스냅샷을 동기식으로 복제합니다. 스냅샷 정책을 사용하여 생성된 예약된 스냅샷은 복제되지 않습니다. 애플리케이션에서 생성된 스냅샷 복제에 대한 자세한 내용은 다음을 참조하세요 ."NetApp 지식 기반: SnapMirror 동기를 사용하여 애플리케이션에서 생성된 스냅샷을 복제하는 방법" .
클론 자동 삭제	ONTAP 9.6	
없음, 스냅샷 또는 자동의 계층화 정책이 있는 FabricPool 애그리게이트는 SnapMirror 동기식 소스 및 대상에서 지원됩니다.	ONTAP 9.5	FabricPool 애그리게이트의 타겟 볼륨을 모든 계층화 정책으로 설정할 수 없습니다.
FC	ONTAP 9.5	지연 시간이 10ms를 초과하지 않는 모든 네트워크
FC-NVMe를 참조하십시오	ONTAP 9.7	

파일 클론	ONTAP 9.7	
SnapMirror 동기식 관계의 운영 볼륨에 대한 FPolicy	ONTAP 9.6	
SnapMirror 동기식 관계의 운영 볼륨에 대한 하드 및 소프트 할당량	ONTAP 9.6	할당량 규칙은 대상에 복제되지 않으므로 할당량 데이터베이스가 대상에 복제되지 않습니다.
클러스터 내 동기식 관계	ONTAP 9.14.1	소스 볼륨과 타겟 볼륨이 서로 다른 HA 쌍에 배치된 경우 고가용성이 제공됩니다. 전체 클러스터가 다운되면 클러스터가 복구될 때까지 볼륨에 액세스할 수 없습니다. 클러스터 내 SnapMirror 동기식 관계는 동시 작업의 전체 제한에 기여합니다.HA 쌍당 관계
iSCSI	ONTAP 9.5	
LUN 클론 및 NVMe 네임스페이스 클론	ONTAP 9.7	
애플리케이션 생성 스냅샷을 통해 백업되는 LUN 클론입니다	ONTAP 9.7	
혼합 프로토콜 액세스(NFS v3 및 SMB)	ONTAP 9.6	
NDMP/NDMP 복구	ONTAP 9.13.1	SnapMirror Synchronous에 NDMP를 사용하려면 소스 클러스터와 대상 클러스터 모두 ONTAP 9.13.1 이상을 실행해야 합니다. 자세한 내용은 을 참조하십시오 NDMP 복제본을 사용하여 데이터를 전송합니다.
AFF/ASA 플랫폼에서만 무중단 SnapMirror 동기식 운영(NDO)이 가능합니다.	ONTAP 9.12.1	무중단 운영을 지원하므로 업무 중단 시간을 예약하지 않고 일반적인 여러 유지보수 작업을 수행할 수 있습니다. 지원되는 운영에는 2개의 클러스터 각각에서 단일 노드가 정상 작동하는 경우 테이크오버 및 반환, 볼륨 이동이 포함됩니다.
NFS v4.2	ONTAP 9.10.1	
NFS v4.0	ONTAP 9.6	
NFS v4.1	ONTAP 9.6	
NVMe/TCP	9.10.1	
높은 메타데이터 작업 빈도 제한을 제거합니다	ONTAP 9.6	
TLS 1.2 암호화를 사용하여 전송 중인 중요한 데이터에 대한 보안	ONTAP 9.6	
단일 파일 및 부분 파일 복구	ONTAP 9.13.1	
SMB 2.0 이상	ONTAP 9.6	
SnapMirror 동기식 미러 계단식 배열	ONTAP 9.6	SnapMirror 동기식 관계의 타겟 볼륨으로부터의 관계는 SnapMirror 비동기식 관계여야 합니다.

SVM 재해 복구	ONTAP 9.6	* SnapMirror 동기식 소스는 SVM 재해 복구 소스로도 될 수 있습니다. 예를 들어, 한 구간으로는 SnapMirror 동기식, 다른 구간으로는 SVM 재해 복구를 사용하는 팬아웃 구성이 될 수 있습니다. * SnapMirror 동기식 소스는 SnapMirror 동기식 소스는 데이터 보호 소스를 연속적으로 지원하지 않으므로 SVM 재해 복구 대상이 될 수 없습니다. 타겟 클러스터에서 SVM 재해 복구 플립 재동기화를 수행하기 전에 동기식 관계를 해제해야 합니다. * SnapMirror 동기식 대상은 SVM 재해 복구에서 DP 볼륨의 복제를 지원하지 않으므로 SVM 재해 복구 소스가 될 수 없습니다. 동기식 소스를 플립 재동기화하면 타겟 클러스터의 DP 볼륨을 제외하고 SVM 재해 복구가 수행됩니다.
소스 볼륨에 테이프 기반 복구	ONTAP 9.13.1	
NAS에 대한 소스 볼륨과 대상 볼륨 간의 타임 스탬프 패리티입니다	ONTAP 9.6	ONTAP 9.5에서 ONTAP 9.6으로 업그레이드한 경우 소스 볼륨의 새 파일 및 수정된 파일에 대해서만 타임스탬프가 복제됩니다. 소스 볼륨의 기존 파일 타임스탬프가 동기화되지 않습니다.

지원되지 않는 기능입니다

다음 기능은 SnapMirror 동기식 관계에서 지원되지 않습니다.

- 자율 랜섬웨어 보호
- 정합성 보장 그룹
- DP_Optimized(DPO) 시스템
- FlexGroup 볼륨
- FlexCache 볼륨
- 글로벌 제한
- 팬아웃 구성에서는 하나의 관계만 SnapMirror 동기식 관계가 될 수 있고 소스 볼륨의 다른 모든 관계는 SnapMirror 비동기식 관계여야 합니다.
- LUN 이동
- MetroCluster 구성
- 혼합 SAN 및 NVMe 액세스 LUN과 NVMe 네임스페이스는 동일한 볼륨 또는 SVM에서 지원되지 않습니다.
- SnapCenter
- SnapLock 볼륨
- 변조 방지 스냅샷
- 대상 볼륨에서 dump 및 SMTape를 사용하여 테이프 백업 또는 복구를 수행합니다
- 소스 볼륨의 처리량(QoS Min
- Volume SnapRestore를 참조하십시오
- VVOL

작동 모드

SnapMirror Synchronous에는 사용되는 SnapMirror 정책 유형에 따라 두 가지 작동 모드가 있습니다.

- * 동기화 모드 * 동기화 모드에서는 애플리케이션 I/O 작업이 운영 및 보조 스토리지 시스템과 병렬로 전송됩니다. 어떤 이유로든 보조 스토리지에 대한 쓰기가 완료되지 않으면 애플리케이션이 운영 스토리지에 계속 쓸 수 있습니다. 오류 상태가 수정되면 SnapMirror 동기식 기술은 자동으로 보조 스토리지와 재동기화되고 동기식 모드에서 운영 스토리지에서 보조 스토리지로 복제를 재개합니다. 동기화 모드에서 RPO=0과 RTO는 2차 복제 장애가 발생할 때까지 매우 낮지만 RPO 및 RTO가 결정되지 않습니다. 그러나 2차 복제가 실패하고 재동기화가 완료된 문제를 복구하는 데 걸리는 시간과 동일합니다.
- * StrictSync 모드 * SnapMirror Synchronous는 선택적으로 StrictSync 모드로 작동할 수 있습니다. 어떤 이유로든 보조 스토리지에 대한 쓰기가 완료되지 않으면 애플리케이션 입출력이 실패하여 운영 스토리지와 보조 스토리지가 동일한지 확인합니다. SnapMirror 관계가 `InSync` 상태로 돌아간 후에만 운영 시스템에 대한 애플리케이션 입출력이 재개됩니다. 운영 스토리지에 장애가 발생할 경우 페일오버 후 데이터 손실 없이 보조 스토리지에서 애플리케이션 입출력을 재개할 수 있습니다. StrictSync 모드에서는 RPO가 항상 0이고 RTO는 매우 낮습니다.

관계 상태

SnapMirror 동기식 관계의 상태는 `InSync` 정상 작동 중에 항상 상태입니다. 어떤 이유로든 SnapMirror 전송이 실패하면 대상이 소스와 동기화되지 않으므로 `OutofSync` 상태로 이동할 수 있습니다.

SnapMirror 동기식 관계의 경우 시스템이 `InSync` `OutofSync`고정된 간격으로 관계 상태 또는)를 자동으로 확인합니다. 관계 상태가 인 `OutofSync` 경우 ONTAP는 자동으로 자동 재동기화 프로세스를 트리거하여 관계를 `InSync` 상태로 되돌립니다. 소스 또는 대상에서 계획되지 않은 스토리지 페일오버 또는 네트워크 중단과 같은 작업으로 인해 전송이 실패한 경우에만 자동 재동기화가 트리거됩니다. `snapmirror quiesce`및 과 같은 사용자 시작 작업은 `snapmirror break` 자동 재동기화를 트리거하지 않습니다.

관계 상태가 `OutofSync` StrictSync 모드에서 SnapMirror 동기 관계에 대한 상태가 되면 운영 볼륨에 대한 모든 I/O 작업이 중지됩니다. `OutofSync`동기화 모드에서 SnapMirror 동기식 관계의 상태는 운영 볼륨에 영향을 주지 않으며 운영 볼륨에 입출력 작업이 허용됩니다.

관련 정보

- "NetApp 기술 보고서 4733: SnapMirror 동기식 구성 및 모범 사례"
- "SnapMirror가 깨졌습니다"
- "SnapMirror 중지"

기본 **ONTAP** 데이터 보호 정책

ONTAP에는 데이터 보호 관계에 사용할 수 있는 몇 가지 기본 보호 정책이 포함되어 있습니다. 사용하는 정책은 보호 관계 유형에 따라 다릅니다.

기본 정책이 데이터 보호 관계 요구 사항을 충족하지 못하는 경우 다음을 수행할 수 "사용자 지정 정책을 만듭니다 "있습니다.

기본 보호 정책 및 설명 목록입니다

기본 보호 정책 및 관련 정책 유형은 아래에 설명되어 있습니다.

이름	설명	정책 유형입니다
비동기식	최신 활성 파일 시스템과 일별 및 주별 스냅샷을 시간별 전송 일정으로 미러링하기 위한 통합된 SnapMirror 비동기식 및 볼트 정책	비동기식
자동화된 장애 조치	복제 실패 시 클라이언트 입출력이 중단되지 않는 제로 RTO 보장의 SnapMirror 동기식 정책입니다.	동기식이다
자동화된 장애 이중 모드	제로 RTO 보장 및 양방향 동기화 복제를 제공하는 SnapMirror Synchronous 정책입니다.	동기식이다
CloudBackupDefault를 선택합니다	일일 규칙을 포함한 볼트 정책.	비동기식
연속	S3 버킷 미러링 정책	연속
DailyBackup을 선택합니다	일일 규칙 및 일일 전송 일정이 포함된 볼트 정책	비동기식
DPDefault(기본값)	모든 스냅샷과 최신 액티브 파일 시스템을 미러링하기 위한 SnapMirror 비동기식 정책	비동기식
MirrorAllSnapshots을 선택합니다	모든 스냅샷과 최신 액티브 파일 시스템을 미러링하기 위한 SnapMirror 비동기식 정책	비동기식
MirrorAllSnapshotsDiscardNetwork 를 참조하십시오	네트워크 구성을 제외한 모든 스냅샷과 최신 활성 파일 시스템을 미러링하기 위한 SnapMirror 비동기식 정책	비동기식
MirrorAndVault를 선택합니다	최신 활성 파일 시스템과 일별 및 주별 스냅샷을 미러링하기 위한 통합된 SnapMirror 비동기식 및 볼트 정책입니다.	비동기식
MirrorAndVaultDiscardNetwork 를 참조하십시오	네트워크 구성을 제외한 최신 활성 파일 시스템과 일별 및 주별 스냅샷을 미러링하기 위한 통합된 SnapMirror 비동기식 및 볼트 정책.	비동기식
대칭 복사	최신 액티브 파일 시스템을 미러링하기 위한 SnapMirror 비동기식 정책입니다.	비동기식
SnapCenterSync 를 참조하십시오	SnapCenter with Application 생성 스냅샷 구성에 대한 SnapMirror Synchronous for Application에 대한 정책	동기식이다
StrictSync를 선택합니다	복제 실패 시 클라이언트 액세스가 중단되는 SnapMirror Synchronous에 대한 정책입니다.	동기식이다
동기식이다	복제 실패 시 클라이언트 액세스가 중단되지 않는 SnapMirror Synchronous에 대한 정책입니다.	동기식이다
Unified7년	7년 보존이 있는 Unified SnapMirror 정책	비동기식
XDPDefault	일별 및 주별 규칙을 포함한 볼트 정책.	비동기식

ONTAP StrictSync 및 동기화 정책에서 지원하는 워크로드에 대해 알아보십시오

StrictSync 및 동기화 정책은 FC, iSCSI 및 FC-NVMe 프로토콜을 사용하는 모든 LUN 기반 애플리케이션뿐만 아니라 데이터베이스, VMware, 할당량, SMB 등과 같은 엔터프라이즈 애플리케이션용 NFSv3 및 NFSv4 프로토콜을 지원합니다. ONTAP 9.6부터 SnapMirror 동기식 은 EDA(전자 설계 자동화), 홈 디렉토리, 소프트웨어 구축 워크로드와 같은 엔터프라이즈 파일 서비스에 사용할 수 있습니다.

ONTAP 9.5에서 동기화 정책의 경우 NFSv3 또는 NFSv4 워크로드를 선택하는 동안 몇 가지 중요한 측면을 고려해야 합니다. 동기화 정책은 높은 읽기 또는 쓰기 입출력 워크로드를 처리할 수 있으므로 워크로드별로 데이터 읽기 또는 쓰기 작업의 양은 고려하지 않습니다. ONTAP 9.5에서는 과도한 파일 생성, 디렉토리 생성, 파일 권한 변경 또는 디렉토리 권한 변경이 있는 워크로드가 적합하지 않을 수 있습니다(이러한 작업을 메타데이터 워크로드가 높은 워크로드라고 함). 메타데이터가 많은 워크로드의 전형적인 예로는 여러 개의 테스트 파일을 만들고, 자동화를 실행하고, 파일을 삭제하는 DevOps 워크로드가 있습니다. 또 다른 예로는 컴파일 중에 여러 임시 파일을 생성하는 병렬 빌드 워크로드가 있습니다. 쓰기 메타데이터 작업이 높으면 미러 간의 동기화가 일시적으로 중단되어 클라이언트의 읽기 및 쓰기 입출력이 중단될 수 있습니다.

ONTAP 9.6부터는 이러한 제한이 제거되며 SnapMirror Synchronous는 홈 디렉토리 및 소프트웨어 빌드 워크로드 등과 같은 다중 사용자 환경이 포함된 엔터프라이즈 파일 서비스 워크로드에 사용할 수 있습니다.

관련 정보

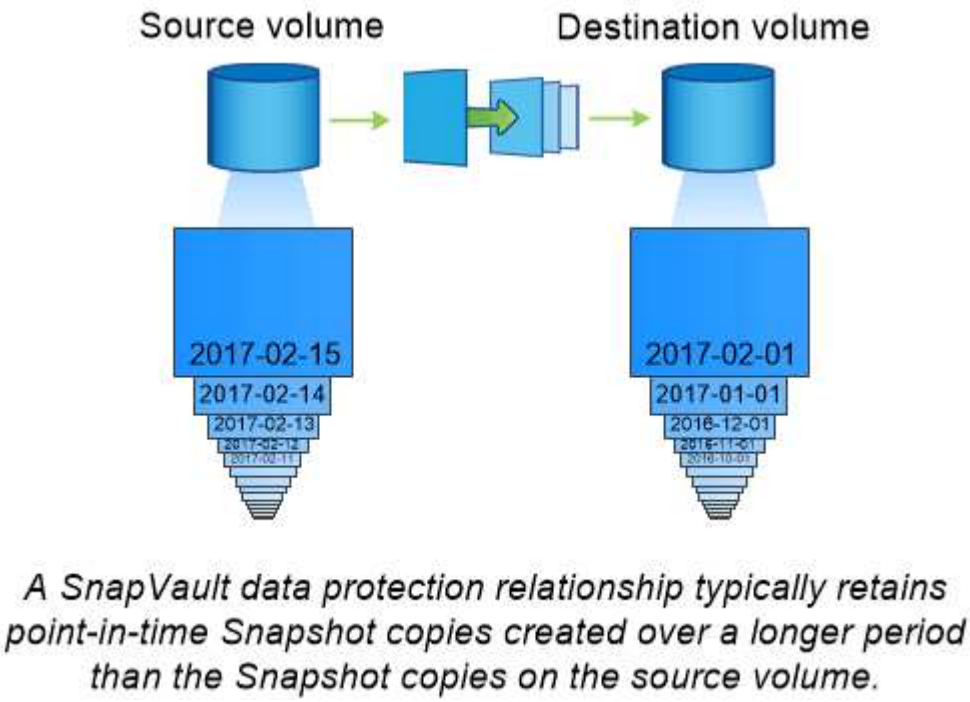
"SnapMirror 동기식 구성 및 모범 사례"

ONTAP SnapMirror 기술을 사용한 볼트 보관에 대해 알아봅니다

SnapMirror 볼트 정책은 ONTAP 9.3 이상에서 SnapVault 기술을 대체합니다. 표준 준수 및 기타 거버넌스 관련 목적을 위해 D2D 스냅샷 복제에는 SnapMirror 소산 정책을 사용합니다. 일반적으로 대상에 현재 소스 볼륨에 있는 스냅샷만 포함되는 SnapMirror 관계와는 달리, 볼트 대상은 훨씬 더 긴 기간 동안 생성된 시점 스냅샷을 보존합니다.

예를 들어, 비즈니스의 정부 회계 규정을 준수하기 위해 데이터의 월별 스냅샷을 20년 동안 보관할 수 있습니다. 볼트 스토리지에서 데이터를 제공할 필요가 없으므로 대상 시스템에서 느리고 저렴한 디스크를 사용할 수 있습니다.

아래 그림은 SnapMirror 볼트 데이터 보호 관계를 보여줍니다.



볼트 데이터 보호 관계가 초기화되는 방법

관계에 대한 SnapMirror 정책에서는 기본 내용과 모든 업데이트를 정의합니다.

기본 볼트 정책에 따른 기본 전송은 `XDPDefault` 소스 볼륨의 스냅샷을 만든 다음 해당 복사본과 해당 복사본이 참조하는 데이터 블록을 대상 볼륨에 전송합니다. SnapMirror 관계와 달리 볼트 백업에는 기준선에 이전 스냅샷이 포함되지 않습니다.

볼트 데이터 보호 관계를 업데이트하는 방법

업데이트는 구성한 일정에 따라 비동기식입니다. 관계 정책에 정의된 규칙은 업데이트에 포함할 새 스냅샷과 보존할 복제본 수를 식별합니다. 정책에 정의된 레이블(예: ""월")은 소스의 스냅샷 정책에 정의된 하나 이상의 레이블과 일치해야 합니다. 그렇지 않으면 복제가 실패합니다.

정책에 따라 업데이트될 때마다 `XDPDefault` SnapMirror는 정책 규칙에 정의된 레이블과 일치하는 레이블이 있는 경우 마지막 업데이트 이후 생성된 스냅샷을 전송합니다. 정책의 다음 출력에서 다음 `snapmirror policy show` 사항에 `XDPDefault` 유의하십시오.

- `Create Snapshot` 는 SnapMirror에서 관계를 업데이트할 때 스냅샷을 생성하지 않음을 나타내는 "'false"' `XDPDefault`입니다.
- `XDPDefault` 에는 ""daily"" 및 ""weekly"" 규칙이 있습니다. 이는 SnapMirror에서 관계를 업데이트할 때 소스에 레이블이 일치하는 모든 스냅샷이 전송됨을 나타냅니다.

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

                     Vserver: vs0
      SnapMirror Policy Name: XDPDefault
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Default policy for XDP relationships with
daily and weekly
                              rules.
       Total Number of Rules: 2
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

관련 정보

- "스냅미러 정책 보기"

ONTAP SnapMirror 통합 복제에 대해 알아보십시오

SnapMirror_Unified replication_을 사용하면 동일한 대상 볼륨에 재해 복구 및 아카이빙을 구성할 수 있습니다. 통합 복제가 적절한 경우 필요한 보조 스토리지의 양을 줄이고 기본 전송 수를 제한하며 네트워크 트래픽을 줄일 수 있습니다.

통합 데이터 보호 관계의 초기화 방법

SnapMirror와 마찬가지로 통합 데이터 보호는 처음 호출할 때 기본 전송을 수행합니다. 관계에 대한 SnapMirror 정책에서는 기본 내용과 모든 업데이트를 정의합니다.

기본 통합 데이터 보호 정책에 따른 기본 전송은 `MirrorAndVault` 소스 볼륨의 스냅샷을 생성한 다음 해당 복사본과 이 복사본이 타겟 볼륨에 참조하는 데이터 블록을 전송합니다. 볼트 보관과 마찬가지로, 통합 데이터 보호에는 기준선에 이전 스냅샷이 포함되지 않습니다.

통합 데이터 보호 관계를 업데이트하는 방법

정책에 따라 업데이트될 때마다 `MirrorAndVault` SnapMirror는 소스 볼륨의 스냅샷을 생성하고 해당 스냅샷과 마지막 업데이트 이후 생성된 모든 스냅샷을 스냅샷 정책 규칙에 정의된 레이블과 일치하는 레이블이 있는 경우 전송합니다. 정책의 다음 출력에서 다음 `snapmirror policy show` 사항에 `MirrorAndVault` 유의하십시오.

- `Create Snapshot` 는 SnapMirror에서 관계를 업데이트할 때 스냅샷을 생성함을 나타내는 ""true"" `MirrorAndVault`입니다.
- `MirrorAndVault` 에는 SnapMirror가 관계를 업데이트할 때 SnapMirror에 의해 생성된 스냅샷과 소스에 일치하는 레이블이 있는 스냅샷이 모두 전송됨을 나타내는 "'sm_created'", "'daily'" 및 "'weekly" 규칙이 있습니다.

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance

                    Vserver: vs0
      SnapMirror Policy Name: MirrorAndVault
      SnapMirror Policy Type: mirror-vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: A unified SnapMirror synchronous and
SnapVault policy for
                              mirroring the latest file system and daily
and weekly snapshots.
       Total Number of Rules: 3
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Unified7년 정책입니다

사전 구성된 `Unified7year` 정책은 과 정확히 동일하게 `MirrorAndVault` 작동합니다. 단, 네 번째 규칙은 월별 스냅샷을 전송하고 7년 동안 보존한다는 점이 다릅니다.

```
                          Rules: SnapMirror Label     Keep   Preserve Warn
Schedule Prefix
                                 ----------------     ----   -------- ----
--------- ------
                                 sm_created              1   false       0 -
-
                                 daily                   7   false       0 -
-
                                 weekly                 52   false       0 -
-
                                 monthly                84   false       0 -
-
```

데이터 손상을 방지합니다

통합 복제는 초기화할 때 SnapMirror에서 생성한 스냅샷으로 기본 전송 내용을 제한합니다. 업데이트할 때마다 SnapMirror는 소스의 다른 스냅샷을 생성하고 스냅샷 정책 규칙에 정의된 레이블과 일치하는 레이블이 있는 새 스냅샷과 해당 스냅샷을 전송합니다.

대상에 마지막으로 전송된 스냅샷의 복사본을 생성하여 업데이트된 스냅샷이 손상되는 것을 방지할 수 있습니다. 이 ""로컬 복사본""은 소스의 보존 규칙에 관계없이 보존되므로 SnapMirror에 의해 원래 전송된 스냅샷을 소스에서 더 이상 사용할 수 없는 경우에도 대상에서 해당 복제본을 사용할 수 있습니다.

통합 데이터 복제를 사용하는 경우

전체 미러 유지 관리의 이점을 통합 복제가 2차 스토리지의 양을 줄이고 기본 전송 수를 제한하며 네트워크 트래픽을 감소시켜 주는 이점과 비교하여 평가해야 합니다.

통합 복제의 적절성을 결정하는 주요 요인은 활성 파일 시스템의 변경률입니다. 예를 들어, 기존 미러는 데이터베이스 트랜잭션 로그의 시간별 스냅샷을 저장하는 볼륨에 더 적합합니다.

관련 정보

- "스냅미러 정책 보기"

ONTAP 데이터 보호 대상 볼륨이 자동으로 증가하는 경우

볼륨에 포함된 가용 공간이 애그리게이트에 있는 경우 데이터 보호 미러 전송 중에 소스 볼륨이 증가하면 타겟 볼륨의 크기가 자동으로 커집니다.

이 동작은 대상의 자동 증가 설정에 관계없이 발생합니다. 볼륨의 증가를 제한하거나 ONTAP가 볼륨을 증가하도록 할 수는 없습니다.

기본적으로 데이터 보호 볼륨은 'grow_shrink' 자동 크기 조정 모드로 설정되어 있으며, 이 모드에서는 사용된 공간의 양에 따라 볼륨이 커지거나 축소됩니다. 데이터 보호 볼륨의 최대 자동 크기 조정 크기는 최대 FlexVol 크기와 동일하며 플랫폼에 따라 다릅니다. 예를 들면 다음과 같습니다.

- FAS8200, 기본 DP 볼륨 최대 크기 조정 = 100TB

자세한 내용은 을 참조하십시오 "NetApp Hardware Universe를 참조하십시오".

fan-out_deployment 를 사용하여 데이터 보호를 여러 보조 시스템으로 확장할 수 있습니다. cascade_deployment를 사용하여 데이터 보호를 3차 시스템으로 확장할 수 있습니다.

팬아웃 및 계단식 구축 모두 SnapMirror DR, SnapVault 또는 통합 복제의 모든 조합을 지원합니다. ONTAP 9.5부터 SnapMirror 동기식 관계는 하나 이상의 SnapMirror 비동기식 관계를 통해 팬아웃 구축을 지원합니다. 팬아웃 구성에서는 하나의 관계만 SnapMirror 동기식 관계가 될 수 있으며 소스 볼륨의 다른 모든 관계는 SnapMirror 비동기식 관계여야 합니다. SnapMirror 동기식 관계는 ONTAP 9.6부터 계단식 배포를 지원하지만 SnapMirror 동기식 관계의 타겟 볼륨과의 관계는 SnapMirror 비동기식 관계여야 합니다. SnapMirror 활성 동기화 (ONTAP 9.13.1부터 지원됨) 팬아웃 구성도 지원합니다.

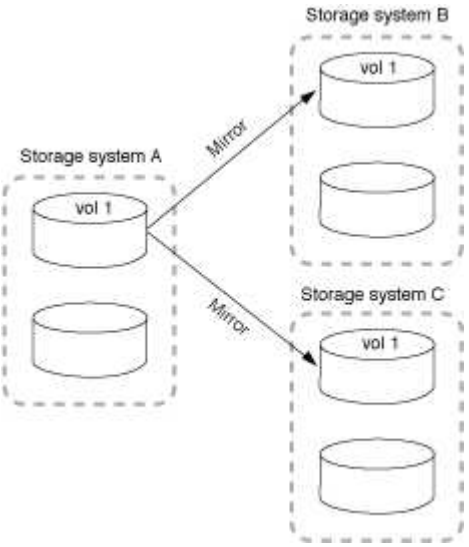
fan-in_deployment를 사용하여 여러 운영 시스템과 단일 보조 시스템 간에 데이터 보호 관계를 생성할 수 있습니다. 각 관계는 2차 시스템에서 다른 볼륨을 사용해야 합니다.

팬아웃 또는 캐스케이드 구성의 일부인 볼륨은 재동기화에 시간이 오래 걸릴 수 있습니다. SnapMirror 관계가 오랫동안 "준비 중" 상태를 보고하는 것을 보면 흔히 볼 수 있습니다.

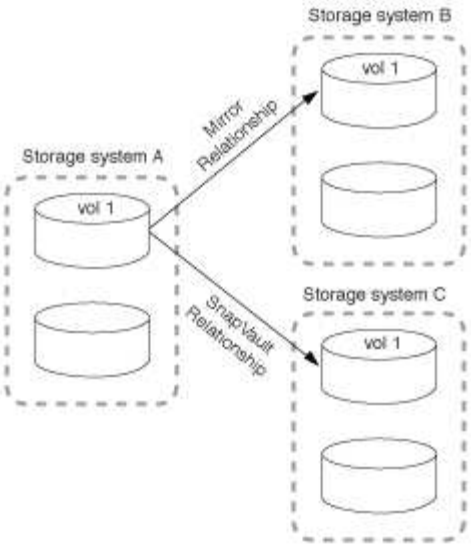
팬아웃**(fan-out)** 배포의 작동 방식

SnapMirror는 _multiple-mirror_and_mirror-vault_fan-out 배포를 지원합니다.

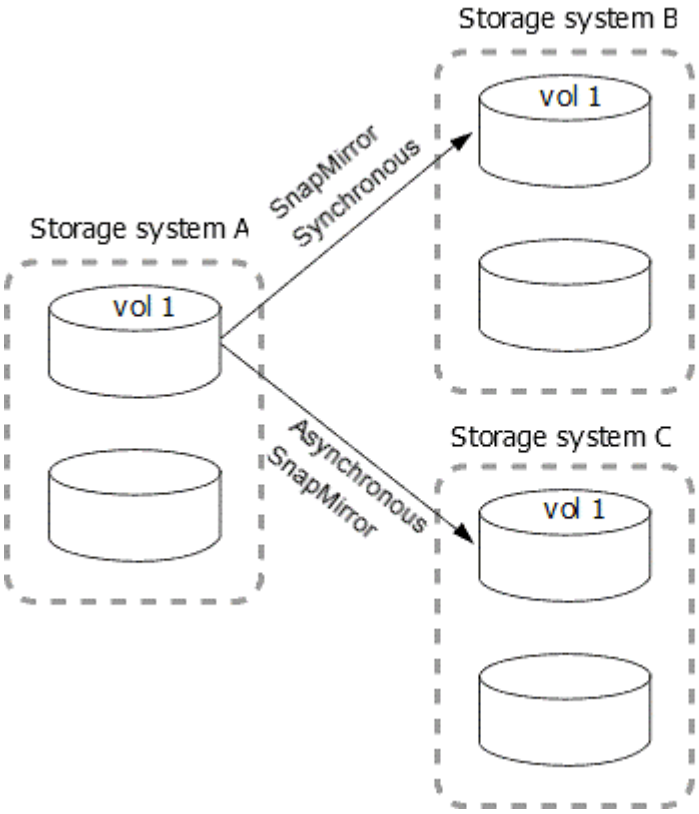
다중 미러 팬아웃 구축은 여러 보조 볼륨에 대한 미러 관계가 있는 소스 볼륨으로 구성됩니다.



미러 볼트(mirror-vault) 팬아웃 구축은 2차 볼륨에 대한 미러 관계와 다른 2차 볼륨에 대한 SnapVault 관계를 가진 소스 볼륨으로 구성됩니다.



ONTAP 9.5부터는 SnapMirror 동기식 관계를 통해 팬아웃 환경을 구축할 수 있지만, 팬아웃 구성에서 하나의 관계만 SnapMirror 동기식 관계가 될 수 있으며 소스 볼륨의 다른 모든 관계는 SnapMirror 비동기식 관계여야 합니다.



다중 구간 배포의 작동 방식

SnapMirror는 *mirror-mirror_mirror-vault*,_vault-mirror_and_vault-vault_cascade 배포를 지원합니다.

미러 계단식 배열 구축은 소스 볼륨이 2차 볼륨으로 미러링되고 2차 볼륨이 3차 볼륨으로 미러링되는 관계 체인으로 구성됩니다. 2차 볼륨을 사용할 수 없게 되면 새로운 기준 전송을 수행하지 않고도 1차 볼륨과 3차 볼륨 간의 관계를 동기화할 수 있습니다.

계층형 볼륨 관계에서 장기 보존 스냅샷은 모든 ONTAP 9 버전에서 계층 구조의 최종 SnapMirror 대상 볼륨에서만 지원됩니다. 캐스케이드 구조의 중간 볼륨에서 장기 보존 스냅샷을 활성화하면 백업 및 스냅샷이 누락될 수 있습니다.

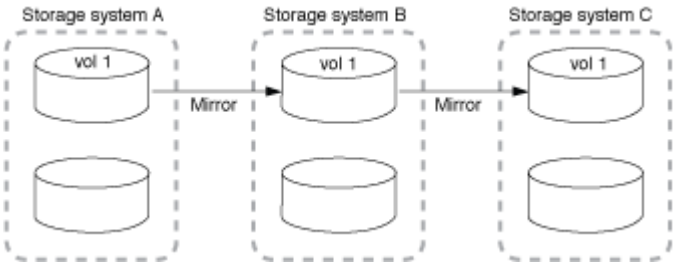
캐스케이드 구성에서 중간 볼륨 중 하나라도 장기 보존 스냅샷이 활성화된 지원되지 않는 구성인 경우 기술 지원팀에 문의하여 다음 내용을 참조하십시오. "NetApp 기술 자료: 장기 보존(LTR) 스냅샷이 활성화된 볼륨을 계단식으로 배열하는 것은 지원되지 않습니다." 도움이 필요합니다.

다음 ONTAP 버전에서는 최종 SnapMirror 대상 볼륨을 제외한 캐스케이드의 모든 볼륨에서 장기 보존 스냅샷을 활성화할 수 없습니다.

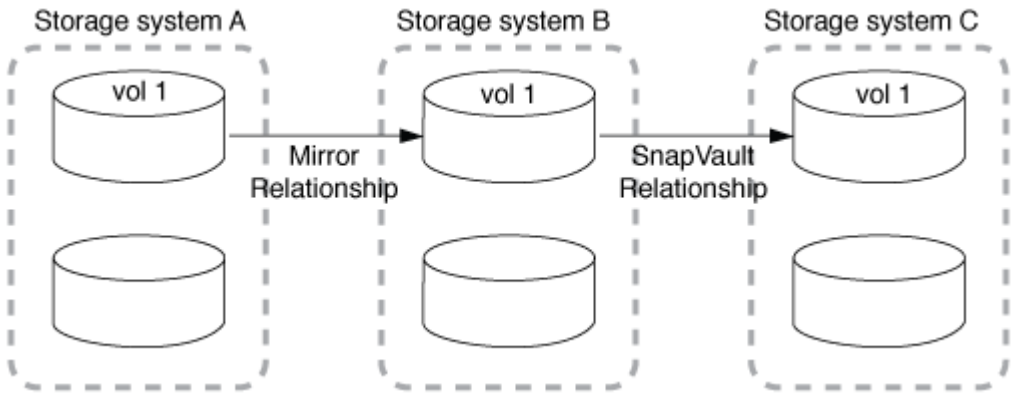
- 9.15.1 이상
- 9.14.1P2 및 P4부터 P14까지
- 9.13.1P9부터 P17까지
- 9.12.1 P12부터 P19까지
- 9.11.1P15부터 P20까지
- 9.10.1P18부터 P20까지
- 9.9.1P20

자세히 알아보세요"장기 보존 스냅샷" .

ONTAP 9.6부터 미러 계단식 구축 환경에서 SnapMirror 동기식 관계가 지원됩니다. 운영 볼륨 및 2차 볼륨만 SnapMirror 동기식 관계에 있을 수 있습니다. 2차 볼륨과 3차 볼륨 간의 관계는 비동기식이어야 합니다.



미러 소산 다중 구간 구축은 소스 볼륨이 보조 볼륨으로 미러링되고 2차 볼륨이 3차 볼륨으로 저장되는 관계 체인으로 구성됩니다.



Vault-mirror 및 Vault-Vault Cascade 배포도 지원됩니다.

- 볼트 미러 계단식 배열 구축은 소스 볼륨을 보조 볼륨으로 보관하고 2차 볼륨을 3차 볼륨으로 미러링하는 관계 체인으로 구성됩니다.
- 볼트-볼트 캐스케이드 배포는 소스 볼륨이 보조 볼륨으로 볼트되고 보조 볼륨이 3차 볼륨으로 볼트되는 관계 체인으로 구성됩니다.

관련 정보

- SnapMirror 활성 동기화를 사용하여 팬아웃 구성에서 보호를 다시 시작합니다

ONTAP SnapMirror 라이센스에 대해 알아보십시오

ONTAP 9.3부터 ONTAP 인스턴스 간 복제를 위한 라이센스가 간소화되었습니다. ONTAP 9 릴리즈에서는 SnapMirror 라이센스가 볼트와 미러 관계를 모두 지원합니다. SnapMirror 라이센스를 사용하여 백업 및 재해 복구 사용 사례 모두에 대해 ONTAP 복제를 지원할 수 있습니다.

ONTAP 9.3 릴리즈 이전에는 ONTAP ONTAP 인스턴스 간의 _vault_관계를 구성하기 위해 별도의 SnapVault 라이센스가 필요했습니다. DP 인스턴스는 보존 시간이 더 긴 백업 사용 사례를 지원하기 위해 더 많은 스냅샷을 보존할 수 있고, ONTAP 인스턴스 간의 _mirror_관계를 구성하기 위해 SnapMirror 라이센스가 필요했습니다. SnapMirror 및 SnapVault 라이센스는 모두 ONTAP 8.x 및 9.x 릴리즈에 대해 계속 사용 및 지원됩니다.

SnapVault 사용권은 계속 작동하고 ONTAP 8.x 및 9.x 릴리즈 모두에서 지원되지만, SnapVault 사용권 대신 SnapMirror 사용권을 사용할 수 있으며 미러 및 볼트 구성에 모두 사용할 수 있습니다.

ONTAP 비동기식 복제의 경우 ONTAP 9.3부터 단일 통합 복제 엔진을 사용하여 확장된 데이터 보호 모드(XDP) 정책을 구성합니다. 이때 미러 정책, 볼트(Vault) 정책 또는 미러 볼트(Mirror-Vault) 정책에 대해 SnapMirror 라이센스를 구성할 수 있습니다. 소스 및 타겟 클러스터 모두에 SnapMirror 라이센스가 필요합니다. SnapMirror 라이센스가 이미 설치되어 있는 경우에는 SnapVault 라이센스가 필요하지 않습니다. SnapMirror 비동기 영구 라이센스는 새로운 AFF 및 FAS 시스템에 설치된 ONTAP One 소프트웨어 제품군에 포함됩니다.

데이터 보호 구성 제한은 ONTAP 버전, 하드웨어 플랫폼 및 설치된 라이센스를 비롯한 여러 요소를 사용하여 결정됩니다. 자세한 내용은 을 참조하십시오 "Hardware Universe".

SnapMirror 동기식 라이센스

ONTAP 9.5부터 SnapMirror 동기식 관계가 지원됩니다. SnapMirror 동기식 관계를 생성하려면 다음 라이센스가 필요합니다.

- 소스 클러스터와 대상 클러스터 모두에 SnapMirror 동기식 라이센스가 필요합니다.

  SnapMirror 동기식 라이센스는 의 "ONTAP One 라이센스 제품군"일부입니다.

  2019년 6월 이전에 프리미엄 또는 플래시 번들과 함께 시스템을 구매하신 경우, NetApp 마스터 키를 다운로드하여 NetApp 지원 사이트 에서 필요한 SnapMirror 동기식 라이센스를 얻을 수 있습니다 "마스터 라이센스 키".

- 소스 클러스터와 대상 클러스터 모두에 SnapMirror 라이센스가 필요합니다.

SnapMirror 클라우드 라이센스

ONTAP 9.8부터 SnapMirror 클라우드 라이센스는 ONTAP 인스턴스에서 오브젝트 스토리지 엔드포인트로 스냅샷의 비동기 복제를 제공합니다. 복제 대상은 사내 오브젝트 저장소뿐만 아니라 S3 및 S3 호환 퍼블릭 클라우드 오브젝트 스토리지 서비스를 사용하여 구성할 수 있습니다. SnapMirror 클라우드 관계는 ONTAP 시스템에서 사전 검증된 오브젝트 스토리지 대상까지 지원됩니다.

SnapMirror 클라우드는 독립 실행형 라이센스로 사용할 수 없습니다. ONTAP 클러스터당 하나의 라이센스만 필요합니다. SnapMirror 클라우드 라이센스 외에 SnapMirror 비동기식 라이센스도 필요합니다.

SnapMirror 클라우드 관계를 생성하려면 다음 라이센스가 필요합니다.

- 오브젝트 저장소 엔드포인트로 직접 복제하기 위한 SnapMirror 라이센스와 SnapMirror 클라우드 라이센스 모두
- 다중 정책 복제 워크플로우(예: 디스크-디스크-클라우드)를 구성할 경우 모든 ONTAP 인스턴스에 SnapMirror 라이센스가 필요하며, SnapMirror 클라우드 라이센스는 오브젝트 스토리지 엔드포인트로 직접 복제되는 소스 클러스터에 대해서만 필요합니다.

ONTAP 9.9.1부터 "SnapMirror 클라우드 복제에 System Manager를 사용하십시오"가능합니다.

공인 SnapMirror 클라우드 타사 애플리케이션 목록이 NetApp 웹 사이트에 게시됩니다.

데이터 보호 최적화 라이센스

DPO(Data Protection Optimized) 라이센스는 더 이상 판매되지 않으며 DPO는 현재 플랫폼에서 지원되지 않습니다. 그러나 지원되는 플랫폼에 DPO 라이센스가 설치되어 있는 경우 NetApp은 해당 플랫폼의 가용성이 끝날 때까지 계속해서 지원을 제공합니다.

DPO는 ONTAP One 라이센스 번들에 포함되지 않으며, DPO 라이센스가 시스템에 설치되어 있는 경우 ONTAP One 라이센스 번들로 업그레이드할 수 없습니다.

지원되는 플랫폼에 대한 자세한 내용은 을 참조하십시오 "Hardware Universe".

ONTAP DPO 시스템은 향상된 기능을 제공합니다

ONTAP 9.6부터는 DP_Optimized(DPO) 라이센스가 설치될 때 지원되는 최대 FlexVol 볼륨 수가 증가합니다. ONTAP 9.4부터 DPO 라이센스가 있는 시스템은 SnapMirror 백오프, 볼륨 간 백그라운드 중복제거, 스냅샷 블록을 도너로 사용 및 컴팩션을 지원합니다.

ONTAP 9.6부터 보조 또는 데이터 보호 시스템에서 지원되는 최대 FlexVol 볼륨 수가 증가하여 노드당 최대 2,500개의 FlexVol 볼륨 또는 페일오버 모드에서 최대 5,000개까지 확장할 수 있습니다. 에서 FlexVol 볼륨 증가를 활성화할 수 "DP_Optimized(DPO) 라이센스"있습니다. 소스 노드와 대상 노드 모두에서 A가 "SnapMirror 라이센스"필요합니다.

ONTAP 9.4부터는 DPO 시스템에 다음과 같은 기능이 향상되었습니다.

- SnapMirror 백 오프: DPO 시스템에서 복제 트래픽은 클라이언트 워크로드가 제공하는 것과 동일한 우선순위를 갖습니다.

  DPO 시스템에서는 SnapMirror 백오프가 기본적으로 사용되지 않습니다.

- 볼륨 백그라운드 중복제거 및 볼륨 간 백그라운드 중복제거: DPO 시스템에서 볼륨 백그라운드 중복제거 및 볼륨 간 백그라운드 중복제거가 활성화됩니다.

  'Storage aggregate Efficiency cross-volume-dedupe start-aggregate_aggregate_name_-scan-old-data true' 명령을 실행하여 기존 데이터를 중복 제거할 수 있습니다. 가장 좋은 방법은 사용량이 적은 시간에 명령을 실행하여 성능에 미치는 영향을 줄이는 것입니다.

  에 대한 자세한 내용은 `storage aggregate efficiency cross-volume-dedupe start` "ONTAP 명령 참조입니다"을 참조하십시오.

- 스냅샷 블록을 기부자로 사용하여 공간 절감 증가: 액티브 파일 시스템에서 사용할 수 없지만 스냅샷에 트래핑된 데이터 블록은 볼륨 중복제거의 기부자로 사용됩니다.

  또한 새 데이터는 스냅샷에 트래핑된 데이터로 중복 제거할 수 있어 스냅샷 블록을 효과적으로 공유할 수 있습니다. 도너 공간이 늘어나면 특히 볼륨에 많은 수의 스냅샷이 있을 때 더 많은 절감 효과를 얻을 수 있습니다.

- 컴팩션: DPO 볼륨에서는 데이터 컴팩션이 기본적으로 사용됩니다.

ONTAP SnapMirror 명령의 경로 이름 패턴 일치에 대해 알아봅니다

패턴 일치를 사용하여 '스냅샷 미러' 명령에서 소스 및 대상 경로를 지정할 수 있습니다.

'스냅미러' 명령은 'vserver:volume' 형식으로 정규화된 경로 이름을 사용합니다. SVM 이름을 입력하지 않고 경로 이름을 약어로 입력할 수 있습니다. 이 경우 '스냅샷 미러' 명령은 사용자의 로컬 SVM 컨텍스트를 가정합니다.

SVM이 "vserver1"이라고 하고 볼륨이 "vol1"이라고 가정하면 정규화된 경로 이름은 vserver1:vol1입니다.

경로에서 별표(*)를 와일드카드로 사용하여 일치하는 정규화된 경로 이름을 선택할 수 있습니다. 다음 표에서는 와일드카드를 사용하여 볼륨 범위를 선택하는 예를 보여 줍니다.

'*'	모든 경로를 일치시킵니다.
' vs * '	모든 SVM과 볼륨을 "V"로 시작하는 SVM 이름으로 일치시킵니다.
'*: * src * '	모든 SVM을 'rc' 텍스트가 포함된 볼륨 이름과 일치시킵니다.
' *:vol *'	모든 SVM을 볼륨 이름부터 찾습니다.

```
vs1::> snapmirror show -destination-path *:*dest*

Progress
Source              Destination  Mirror        Relationship  Total
Last
Path          Type  Path         State         Status        Progress
Healthy Updated
------------- ---- ------------ ------------- -------------- ----------
------- --------
vs1:sm_src2
              DP   vs2:sm_dest1
                                 Snapmirrored  Idle           -
true    -
```

에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror 관계 작업의 확장 쿼리에 대해 알아봅니다

_extended query_를 사용하여 여러 SnapMirror 관계에 대해 한 번에 SnapMirror 작업을 수행할 수 있습니다. 예를 들어, 하나의 명령을 사용하여 초기화하려는 초기화되지 않은 SnapMirror 관계가 여러 개 있을 수 있습니다.

이 작업에 대해

다음 SnapMirror 작업에 확장 쿼리를 적용할 수 있습니다.

- 초기화되지 않은 관계를 초기화하는 중입니다
- 중단된 관계를 재개하는 중입니다
- 끊어진 관계를 재동기화합니다
- 유휴 관계를 업데이트하는 중입니다
- 관계 데이터 전송을 중단합니다

단계

1. 다양한 관계에서 SnapMirror 작업 수행:

   '*SnapMirror* 명령{-state 상태} *'

   다음 명령을 실행하면 '초기화되지 않음' 상태인 SnapMirror 관계가 초기화됩니다.

   ```
   vs1::> snapmirror initialize {-state Uninitialized} *
   ```

   에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

SnapMirror 관계에 대한 호환 **ONTAP** 버전

소스 및 타겟 볼륨에서 SnapMirror 데이터 보호 관계를 생성하기 전에 호환되는 ONTAP 버전을 실행해야 합니다. ONTAP를 업그레이드하기 전에 현재 ONTAP 버전이 SnapMirror 관계에 대한 대상 ONTAP 버전과 호환되는지 확인해야 합니다.

통합 복제 관계

사내 또는 Cloud Volumes ONTAP 릴리즈를 사용하여 "XDP" 유형의 SnapMirror 관계 구축:

ONTAP 9.9.0부터:

- ONTAP 9.x.0 릴리즈는 클라우드 전용 릴리즈이며 Cloud Volumes ONTAP 시스템을 지원합니다. 릴리스 버전 뒤의 별표(*)는 클라우드 전용 릴리스를 나타냅니다.

  ⓘ ONTAP 9.16.0은 클라우드 전용 규칙에 대한 예외입니다."ASA r2 시스템" . 릴리스 버전 뒤에 있는 더하기 기호(+)는 ASA r2와 클라우드 지원 릴리스를 모두 나타냅니다. ASA r2 시스템은 다른 ASA r2 시스템에 대해서만 SnapMirror 관계를 지원합니다.

- ONTAP 9.x.1 릴리스는 일반 릴리스이며 온-프레미스 및 Cloud Volumes ONTAP 시스템을 모두 지원합니다.

ⓘ 경우 "고급 용량 밸런싱"ONTAP 9.16.1 이상을 실행하는 클러스터의 볼륨에서 이 설정된SnapMirror 전송이 ONTAP ONTAP 9.16.1 이전 버전을 실행하는 클러스터에 지원되지 않습니다.

ⓘ 상호 운용성은 양방향입니다.

• ONTAP 버전 9.4 이상에 대한 상호 운용성*

ONTAP 버전…	이러한 이전 ONTAP 버전과의 상호 작용…																				
	9.18.1	9.17.1	9.16.1	9.16.0 이상	9.15.1	9.15.0 *	9.14.1	9.14.0 *	9.13.1	9.13.0 *	9.12.1	9.12.0 *	9.11.1	9.11.0 *	9.10.1	9.10.0 *	9.9.1	9.9.0 *	9.8	9.7	9.6	9.5
9.18.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.17.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.16.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.16.0 이상	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.15.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요
9.15.0 *	아니요	* 예 *	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	아니요	아니요	아니요	아니요
9.14.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요
9.14.0 *	아니요	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	아니요	아니요	아니요	아니요
9.13.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요
9.13.0 *	아니요	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	아니요	아니요
9.12.1	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요

9.12.0*	아니요	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	아니요	아니요
9.11.1	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요
9.11.0*	아니요	아니요	아니요	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요
9.10.1	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.10.0*	아니요	아니요	아니요	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	* 예 *	* 예 *	* 예 *
9.9.1	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.9.0 *	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.8	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.7	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.6	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.5	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *

SnapMirror 동기식 관계

SnapMirror 동기식은 ONTAP 클라우드 인스턴스에 지원되지 않습니다.

ONTAP 버전 …	이러한 이전 ONTAP 버전과의 상호 작용…													
	9.18.1	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.18.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.17.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.16.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요

9.15.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요
9.14.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요
9.13.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요
9.12.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요
9.11.1	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요
9.10.1	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요
9.9.1	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요
9.8	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요
9.7	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.6	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *
9.5	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *

SnapMirror SVM 재해 복구 관계

- 이 매트릭스는 ONTAP 9.10.1부터 시작되는 SVM 데이터 이동성 마이그레이션 기능에 적용됩니다.
- SVM DR을 사용하면 표시된 제한 사항을 충족하지 않는 SVM을 마이그레이션할 수 있습니다. "SVM 마이그레이션(SVM 데이터 이동성)".
- 두 경우 모두 최대 2개의 주요 최신 ONTAP 버전으로 소스 클러스터와 대상 클러스터를 분리할 수 있으며, 대상 버전은 소스 ONTAP 버전과 동일하거나 더 최신 버전이어야 합니다.

SVM 재해 복구 데이터 및 **SVM** 보호**:**

SVM 재해 복구는 동일한 버전의 ONTAP를 실행하는 클러스터 간에만 지원됩니다. * SVM 복제에 대해 버전 독립성이 지원되지 않습니다 *.

SVM 마이그레이션을 위한 **SVM** 재해 복구**:**

- 복제는 소스의 이전 ONTAP 버전에서 대상에 있는 동일한 버전 또는 이후 버전의 ONTAP로 단일 방향으로 지원됩니다.
- 타겟 클러스터의 ONTAP 버전은 아래 표와 같이 최신 주요 온프레미스 버전 2개 또는 최신 주요 클라우드 버전 2개(ONTAP 9.9.0부터 시작)를 초과할 수 없습니다.
  - 장기 데이터 보호 사용 사례에는 복제가 지원되지 않습니다.

릴리스 버전 뒤의 별표(*)는 클라우드 전용 릴리스를 나타냅니다.

지원을 확인하려면 왼쪽 표 열에서 소스 버전을 찾은 다음 맨 위 행에서 대상 버전을 찾습니다(같은 버전에 대한 DR/마이그레이션 및 최신 버전에 대한 마이그레이션만).

ONTAP 9.10.1 이상을 사용하는 경우 다음을 사용할 수 있습니다. "SVM 데이터 이동성" SVM DR 대신 SVM을 한 클러스터에서 다른 클러스터로 마이그레이션하는 기능을 제공합니다.

출처	목적지

	9.5	9.6	9.7	9.8	9.9.0 *	9.9.1	9.10.0 *	9.10.1	9.11.0 *	9.11.1	9.12.0 *	9.12.1	9.13.0 *	9.13.1	9.14.0 *	9.14.1	9.15.0 *	9.15.1	9.16.0	9.16.1	9.17.1	9.18.1
9.5	DR/마이그레이션	마이그레이션	마이그레이션																			
9.6		DR/마이그레이션	마이그레이션	마이그레이션																		
9.7			DR/마이그레이션	마이그레이션	마이그레이션																	
9.8				DR/마이그레이션	마이그레이션	마이그레이션		마이그레이션														
9.9.0 *					DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션												
9.9.1						DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션												
9.10.0 *							DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션										

9.10.1								DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션								
9.11.0*									DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션						
9.11.1										DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션						
9.12.0*											DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션				
9.12.1												DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션				
9.13.0*													DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션			
9.13.1														DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션			

9.14.0*															DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	
9.14.1																DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	
9.15.0*																	DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	
9.15.1																		DR/마이그레이션	마이그레이션	마이그레이션	
9.16.0																			DR/마이그레이션	마이그레이션	마이그레이션
9.16.1																				DR/마이그레이션	마이그레이션
9.17.1																					DR/마이그레이션

9.1 8.1																					DR /마 이 그 레 이 션

SnapMirror 재해 복구 관계

"DP" 유형의 SnapMirror 관계 및 정책 유형 ""비동기 미러""의 경우:

DP 유형 미러는 ONTAP 9.11.1부터 초기화할 수 없으며 ONTAP 9.12.1에서 완전히 사용되지 않습니다. 자세한 내용은 을 참조하십시오 "데이터 보호 SnapMirror 관계의 사용 중단".

다음 표에서 왼쪽에 있는 열은 소스 볼륨의 ONTAP 버전을 나타내고, 맨 위 행은 대상 볼륨에 있을 수 있는 ONTAP 버전을 나타냅니다.

출처	목적지								
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3
9.11.1	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.10.1	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.9.1	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요
9.8	아니요	예	예	예	아니요	아니요	아니요	아니요	아니요
9.7	아니요	아니요	예	예	예	아니요	아니요	아니요	아니요
9.6	아니요	아니요	아니요	예	예	예	아니요	아니요	아니요
9.5	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요
9.4	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요
9.3	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예

상호 운용성은 양방향성이 아닙니다.

ONTAP SnapMirror 제한 사항에 대해 알아보십시오

데이터 보호 관계를 생성하기 전에 기본적인 SnapMirror 제한을 숙지해야 합니다.

- 타겟 볼륨에는 소스 볼륨이 하나만 있을 수 있습니다.

  소스 볼륨에는 여러 개의 대상 볼륨이 있을 수 있습니다. 타겟 볼륨은 모든 유형의 SnapMirror 복제 관계의 소스 볼륨이 될 수 있습니다.

- 스토리지 모델에 따라 단일 소스 볼륨에서 최대 8개 또는 16개의 대상 볼륨을 팬아웃할 수 있습니다. 를 참조하십시오 "Hardware Universe" 를 참조하십시오.
- SnapMirror DR 관계의 대상에 파일을 복원할 수 없습니다.

- 소스 또는 대상 SnapVault 볼륨은 32비트일 수 없습니다.
- SnapVault 관계의 소스 볼륨은 FlexClone 볼륨이 아니어야 합니다.

> 관계는 작동하지만 FlexClone 볼륨에서 제공하는 효율성은 유지되지 않습니다.

SnapMirror 볼륨 복제를 구성합니다

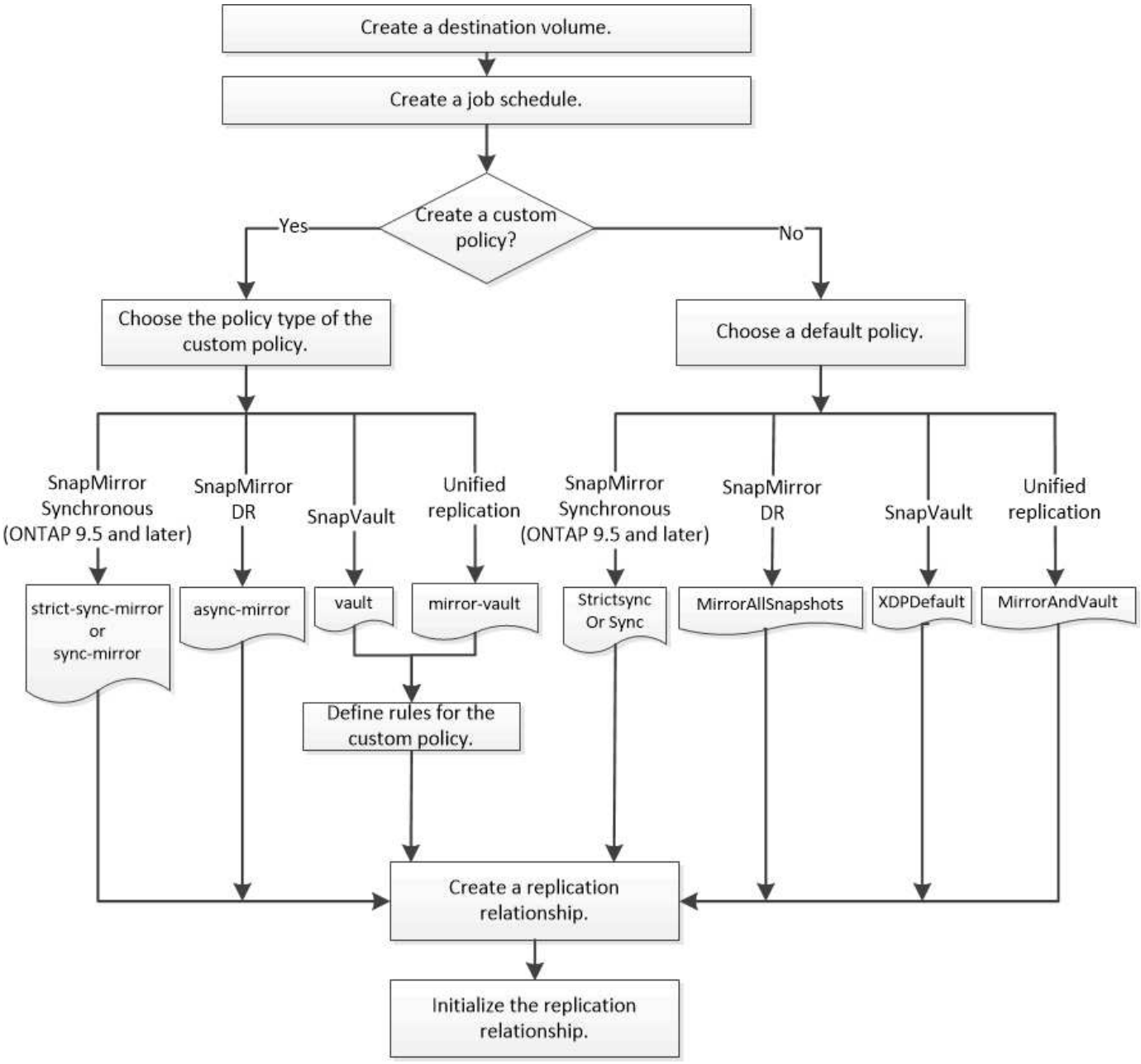
ONTAP SnapMirror 복제 워크플로우

SnapMirror는 SnapMirror DR, 아카이브(이전의 SnapVault) 및 통합 복제라는 세 가지 유형의 데이터 보호 관계를 제공합니다. 동일한 기본 워크플로를 따라 각 관계 유형을 구성할 수 있습니다.

ONTAP 9.9.1부터는 GA될 수 있습니다. "SnapMirror 활성 동기화" 제로 RTO(Zero Recovery Time Objective) 또는 TAF(Transparent Application Failover)를 제공하여 SAN 환경에서 업무상 중요한 애플리케이션의 자동 페일오버를 지원합니다.

SnapMirror 데이터 보호 관계의 각 유형에 대해 워크플로는 동일합니다. 대상 볼륨 생성, 작업 일정 생성, 정책 지정, 관계 생성 및 초기화

ONTAP 9.3부터는 '스냅샷 보호' 명령을 사용하여 한 번에 데이터 보호 관계를 구성할 수 있습니다. 스냅샷 보호 기능을 사용하더라도 워크플로우의 각 단계를 이해해야 합니다.



관련 정보

- "SnapMirror 보호"

한 번에 **ONTAP SnapMirror** 복제 관계를 구성합니다

ONTAP 9.3부터 다음을 사용할 수 있습니다. `snapmirror protect` 단일 단계로 데이터 보호 관계를 구성하는 명령입니다. 복제할 볼륨 목록, 대상 클러스터의 SVM, 작업 일정 및 SnapMirror 정책을 지정합니다. `snapmirror protect` 나머지는 다 해줍니다.

시작하기 전에

- 소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

  "클러스터 및 SVM 피어링"

- 대상 볼륨의 언어는 소스 볼륨의 언어와 동일해야 합니다.

이 작업에 대해

'스냅샷 보호' 명령은 지정된 SVM과 연결된 애그리게이트를 선택합니다. SVM과 연결된 애그리게이트가 없으면 클러스터의 모든 애그리게이트 중에서 선택합니다. Aggregate는 여유 공간의 양과 애그리게이트의 볼륨 수를 기준으로 합니다.

그런 다음 'napmirror protect' 명령은 다음 단계를 수행합니다.

- 복제할 볼륨 목록에서 각 볼륨에 대해 적절한 유형과 예약된 공간을 사용하여 대상 볼륨을 생성합니다.
- 지정한 정책에 적합한 복제 관계를 구성합니다.
- 관계를 초기화합니다.

대상 볼륨의 이름은 '*source_volume_name_dst*' 형식입니다. 기존 이름과 충돌하는 경우 명령이 볼륨 이름에 번호를 추가합니다. 명령 옵션에서 접두사 및/또는 접미사를 지정할 수 있습니다. 접미사는 시스템 제공 st 접미사를 대체합니다.

ONTAP 9.4 이상에서는 대상 볼륨에 최대 1019개의 스냅샷을 포함할 수 있습니다. ONTAP 9.3 및 이전 버전에서는 대상 볼륨에 최대 251개의 스냅샷을 포함할 수 있습니다.

> ⓘ 초기화에는 시간이 오래 걸릴 수 있습니다. 스냅미러 보호 기능은 작업이 완료되기 전에 초기화가 완료될 때까지 기다리지 않습니다. 따라서 초기화가 완료되는 시점을 결정하려면 job show 명령 대신 sapmirror show 명령을 사용해야 합니다.

ONTAP 9.5부터 `snapmirror protect` 명령을 사용하여 SnapMirror 동기식 관계를 만들 수 있습니다.

자세히 알아보세요 `snapmirror protect` 에서 "ONTAP 명령 참조입니다" .

단계

1. 한 단계로 복제 관계를 생성하고 초기화합니다.

   이 명령을 실행하기 전에 꺾쇠 괄호 안의 변수를 필수 값으로 바꾸어야 합니다.

   ```
   snapmirror protect -path-list <SVM:volume> -destination-vserver
   <destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
   <true|false> -destination-volume-prefix <prefix> -destination-volume
   -suffix <suffix>
   ```

   > ⓘ 이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다. '-auto-initialize' 옵션은 기본적으로 ""true""로 설정됩니다.

   다음 예에서는 기본 'MirorAllSnapshots' 정책을 사용하여 SnapMirror DR 관계를 생성하고 초기화합니다.

   ```
   cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
   -destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
   replication_daily
   ```

원하는 경우 사용자 지정 정책을 사용할 수 있습니다. 자세한 내용은 을 참조하십시오 "사용자 지정 복제 정책 생성".

다음 예에서는 기본 "XDPDefault" 정책을 사용하여 SnapVault 관계를 만들고 초기화합니다.

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

다음 예제에서는 기본 MirorAndVault 정책을 사용하여 통합 복제 관계를 만들고 초기화합니다.

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

다음 예에서는 기본 `Sync` 정책을 사용하여 SnapMirror 동기식 관계를 만들고 초기화합니다.

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

SnapVault 및 통합 복제 정책의 경우 대상에서 마지막으로 전송된 스냅샷의 복제본을 생성하기 위한 일정을 정의하는 것이 유용할 수 있습니다. 자세한 내용은 을 "대상에 로컬 복제본을 생성하기 위한 스케줄 정의"참조하십시오.

작업을 마친 후

를 사용합니다 `snapmirror show` 명령을 사용하여 SnapMirror 관계가 생성되었는지 확인합니다.

에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "작업 표시"

한 번에 한 단계씩 복제 관계를 구성합니다

ONTAP SnapMirror 대상 볼륨을 생성합니다

타겟에서 명령을 사용하여 대상 볼륨을 생성할 수 `volume create` 있습니다. 대상 볼륨의 크기는 소스 볼륨보다 크거나 같아야 합니다. 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 대상 볼륨 생성:

   'volume create-vserver_SVM_-volume volume-aggregate_aggregate_-type DP-size_size_'

다음 예에서는 이름이 "VolA_DST"인 2GB 대상 볼륨을 생성합니다.

```
cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
-aggregate node01_aggr -type DP -size 2GB
```

ONTAP SnapMirror 복제 작업 일정을 생성합니다

작업 일정은 SnapMirror에서 일정이 할당된 데이터 보호 관계를 자동으로 업데이트할지 여부를 결정합니다. System Manager 또는 명령을 사용하여 복제 작업 일정을 생성할 수 `job schedule cron create` 있습니다. 에 대한 자세한 내용은 `job schedule cron create` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

데이터 보호 관계를 생성할 때 작업 일정을 할당합니다. 작업 일정을 할당하지 않으면 관계를 수동으로 업데이트해야 합니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 복제 작업 일정을 생성할 수 있습니다.

시스템 관리자

1. Protection > Overview * 로 이동한 후 * Local policy settings * 를 확장합니다.
2. Schedules * 창에서 를 →클릭합니다.
3. Schedules * 창에서 를 + Add 클릭합니다.
4. 일정 추가 * 창에서 일정 이름을 입력하고 컨텍스트 및 일정 유형을 선택합니다.
5. 저장 * 을 클릭합니다.

CLI를 참조하십시오

1. 작업 일정 생성:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

월-일-일-주-시-시간의 경우 월, 일, 시 순으로 모두 작업을 실행하도록 지정할 수 있습니다.

ONTAP 9.10.1.1부터는 작업 일정에 SVM을 포함할 수 있습니다.

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

볼륨 SnapMirror 관계에서 FlexVol 볼륨의 최소 지원 일정(RPO)은 5분입니다. 볼륨 SnapMirror 관계에서 FlexGroup 볼륨의 최소 지원 일정(RPO)은 30분입니다.

다음 예에서는 토요일 오전 3시에 실행되는 my_weekly라는 작업 일정을 생성합니다.

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

SnapMirror 복제 정책을 사용자 지정합니다

사용자 지정 **ONTAP SnapMirror** 복제 정책을 생성합니다

관계의 기본 정책이 적합하지 않은 경우 사용자 지정 복제 정책을 생성할 수 있습니다. 예를 들어 네트워크 전송에서 데이터를 압축하거나 SnapMirror에서 스냅샷을 전송하는 시도 횟수를 수정할 수 있습니다.

복제 관계를 생성할 때 기본 또는 사용자 지정 정책을 사용할 수 있습니다. 사용자 지정 아카이브(이전 SnapVault) 또는 통합 복제 정책의 경우 초기화 및 업데이트 중에 전송되는 스냅샷을 결정하는 _rules_를 하나 이상 정의해야 합니다. 대상에 로컬 스냅샷을 생성하기 위한 스케줄을 정의할 수도 있습니다.

복제 정책의 _policy type_은 이 정책이 지원하는 관계 유형을 결정합니다. 아래 표에는 사용 가능한 정책 유형이 나와 있습니다.

정책 유형입니다	관계 유형
비동기식 - 미러	SnapMirror DR
볼트	SnapVault
대칭 복사 - 볼트	통합 복제
엄격한 동기식 미러링	StrictSync 모드의 SnapMirror 동기(ONTAP 9.5부터 지원됨)
동기식-미러	동기화 모드의 SnapMirror 동기(ONTAP 9.5부터 지원됨)

사용자 지정 복제 정책을 생성할 때는 기본 정책 다음에 정책을 모델링하는 것이 좋습니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 맞춤형 데이터 보호 정책을 생성할 수 있습니다. ONTAP 9.11.1부터 System Manager를 사용하여 사용자 정의 미러 및 볼트 정책을 생성하고 레거시 정책을 표시 및 선택할 수 있습니다. 이 기능은 ONTAP 9.8P12 이상의 ONTAP 9.8 패치에서도 사용할 수 있습니다.

소스 클러스터와 대상 클러스터 모두에 사용자 지정 보호 정책을 생성합니다.

시스템 관리자

1. 보호 > 개요 > 로컬 정책 설정 * 을 클릭합니다.
2. 보호 정책 * 에서 을 →클릭합니다.
3. 보호 정책 * 창에서 을 + Add 클릭합니다.
4. 새 정책 이름을 입력하고 정책 범위를 선택합니다.
5. 정책 유형을 선택합니다. 볼트 전용 또는 미러 전용 정책을 추가하려면 * Asynchronous * 를 선택하고 * 기존 정책 유형 사용 * 을 클릭합니다.
6. 필수 필드에 내용을 입력합니다.
7. 저장 * 을 클릭합니다.
8. 다른 클러스터에서 이 단계를 반복합니다.

CLI를 참조하십시오

1. 사용자 지정 복제 정책 생성:

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type
<async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror>
-comment <comment> -tries <transfer_tries> -transfer-priority
<low|normal> -is-network-compression-enabled <true|false>
```

ONTAP 9.5부터 매개 변수를 사용하여 SnapMirror 동기식 관계에 대한 일반 스냅샷 스케줄을 생성하기 위한 스케줄을 지정할 수 `-common-snapshot-schedule` 있습니다. 기본적으로 SnapMirror 동기식 관계에 대한 일반적인 스냅샷 일정은 1시간입니다. SnapMirror 동기식 관계의 스냅샷 스케줄에 대해 30분에서 2시간 사이의 값을 지정할 수 있습니다.

다음 예에서는 데이터 전송에 대해 네트워크 압축을 활성화하는 SnapMirror DR에 대한 사용자 지정 복제 정책을 생성합니다.

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network
compression enabled" -is-network-compression-enabled true
```

다음 예에서는 SnapVault에 대한 사용자 지정 복제 정책을 생성합니다.

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

다음 예에서는 통합 복제에 대한 사용자 지정 복제 정책을 생성합니다.

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_unified -type mirror-vault
```

다음 예에서는 StrictSync 모드에서 SnapMirror 동기식 관계에 대한 사용자 지정 복제 정책을 생성합니다.

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

에 대한 자세한 내용은 `snapmirror policy create` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

"'볼트' 및 "미러 볼트" 정책 유형의 경우 초기화 및 업데이트 중에 전송되는 스냅샷을 결정하는 규칙을 정의해야 합니다.

사용하세요 `snapmirror policy show` SnapMirror 정책이 생성되었는지 확인하는 명령입니다.

자세히 알아보세요 `snapmirror policy show` 에서 "ONTAP 명령 참조입니다" .

ONTAP SnapMirror 정책에 대한 규칙을 정의합니다

또는 `mirror-vault` 정책 유형을 사용하는 사용자 지정 정책의 경우 `vault` 초기화 및 업데이트 중에 전송되는 스냅샷을 결정하는 규칙을 하나 이상 정의해야 합니다. 또는 `mirror-vault` 정책 유형을 사용하여 기본 정책에 대한 규칙을 정의할 수도 `vault` 있습니다.

이 작업에 대해

또는 `mirror-vault` 정책 유형을 사용하는 모든 정책에는 `vault` 복제할 스냅샷을 지정하는 규칙이 있어야 합니다. 예를 들어 이 규칙은 `bi-monthly` SnapMirror 레이블이 할당된 스냅샷만 복제해야 함을 `bi-monthly` 나타냅니다. 소스에서 스냅샷 정책을 구성할 때 SnapMirror 레이블을 지정합니다.

각 정책 유형은 하나 이상의 시스템 정의 규칙과 연결됩니다. 이러한 규칙은 정책 유형을 지정할 때 정책에 자동으로 할당됩니다. 아래 표에는 시스템 정의 규칙이 나와 있습니다.

시스템 정의 규칙	정책 유형에 사용됩니다	결과
SM_생성됨	비동기 미러, 미러 볼트, 동기화, StrictSync	SnapMirror에 의해 생성된 스냅샷은 초기화 및 업데이트 시 전송됩니다.
ALL_SOURCE_SNAPSHOTS 를 선택합니다	비동기식 - 미러	초기화 및 업데이트 시 소스의 새 스냅샷이 전송됩니다.
매일	볼트, 미러 볼트	초기화 및 업데이트 시 SnapMirror 레이블이 있는 소스의 새 스냅샷이 `daily` 전송됩니다.
매주	볼트, 미러 볼트	초기화 및 업데이트 시 SnapMirror 레이블이 있는 소스의 새 스냅샷이 `weekly` 전송됩니다.

매월	대칭 복사 - 볼트	초기화 및 업데이트 시 SnapMirror 레이블이 있는 소스의 새 스냅샷이 `monthly` 전송됩니다.
app_consistent	동기화, StrictSync	소스에 SnapMirror 레이블이 있는 스냅샷은 `app_consistent` 동기식으로 대상에 복제됩니다. ONTAP 9.7부터 지원됩니다.

""비동기 미러" 정책 유형을 제외하고 필요에 따라 기본 또는 사용자 지정 정책에 대한 추가 규칙을 지정할 수 있습니다. 예를 들면 다음과 같습니다.

- 기본 정책의 경우 `MirrorAndVault` 소스의 스냅샷을 SnapMirror 레이블과 일치시키기 위해 `bi-monthly` 이라는 규칙을 생성할 수 `bi-monthly` 있습니다.
- 정책 유형이 지정된 사용자 지정 정책의 경우 `mirror-vault` 소스의 스냅숏을 SnapMirror 레이블과 일치시키기 위해 `bi-weekly` 이라는 규칙을 만들 수 `bi-weekly` 있습니다.

단계

1. 정책의 규칙 정의:

   '스냅샷 정책 추가 규칙 -vserver_SVM_-policy_policy_for_rule_-snapmirror-label_snapmirror-label_ -keep_retention_count_'

   다음 예제에서는 기본 MirorAndVault 정책에 SnapMirror 레이블 '격월'이 있는 규칙을 추가합니다.

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   다음 예에서는 사용자 지정 my_SnapVault 정책에 SnapMirror 레이블 "격주"가 포함된 규칙을 추가합니다.

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_snapvault -snapmirror-label bi-weekly -keep 26
   ```

   다음 예에서는 사용자 지정 'Sync' 정책에 SnapMirror 레이블 'app_consistent'가 포함된 규칙을 추가합니다.

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
   -snapmirror-label app_consistent -keep 1
   ```

   에 대한 자세한 내용은 `snapmirror policy add-rule` "ONTAP 명령 참조입니다"을 참조하십시오.

   그런 다음 이 SnapMirror 레이블과 일치하는 소스 클러스터에서 스냅샷을 복제할 수 있습니다.

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

ONTAP SnapMirror 스케줄을 정의하여 대상에 로컬 복제본을 생성합니다

SnapVault 및 통합 복제 관계의 경우 마지막으로 전송된 스냅샷의 복사본을 대상에 생성하여 업데이트된 스냅샷이 손상되는 것을 방지할 수 있습니다. 이 "로컬 복사본"은 소스의 보존 규칙에 관계없이 보존되므로 SnapMirror에서 원래 전송한 스냅샷을 소스에서 더 이상 사용할 수 없는 경우에도 대상에서 해당 복제본을 사용할 수 있습니다.

이 작업에 대해

로컬 복사본을 만드는 일정을 지정합니다. `-schedule` 옵션 `snapmirror policy add-rule` 명령.

단계

1. 대상에 로컬 복제본을 생성하기 위한 스케줄을 정의합니다.

   '스냅샷 정책 추가-규칙-vserver_SVM_-policy_policy_for_rule_-snapmirror-label_snapmirror-label_ -schedule_schedule_'

   작업 일정을 작성하는 방법에 대한 예는 을 참조하십시오"복제 작업 스케줄 생성".

   다음 예제에서는 기본 MirorAndVault 정책에 로컬 복사본을 만들기 위한 일정을 추가합니다.

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
   ```

   다음 예에서는 사용자 지정 my_unified" 정책에 로컬 복사본을 만들기 위한 일정을 추가합니다.

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_unified -snapmirror-label my_monthly -schedule my_monthly
   ```

   에 대한 자세한 내용은 `snapmirror policy add-rule` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror 복제 관계를 생성합니다

운영 스토리지의 소스 볼륨과 보조 스토리지의 대상 볼륨 간의 관계를 _ 데이터 보호 관계라고 합니다. _ 명령을 사용하여 SnapMirror DR, SnapVault 또는 통합 복제 데이터 보호 관계를 생성할 수 있습니다. `snapmirror create`

> 이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 복제 관계를 생성합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

ONTAP 9.11.1부터 시스템 관리자를 사용하여 미리 작성된 사용자 정의 미러 및 볼트 정책을 선택하고, 레거시 정책을 표시 및 선택하고, 볼륨 및 스토리지 VM을 보호할 때 보호 정책에 정의된 전송 일정을 재정의할 수 있습니다. 이 기능은 ONTAP 9.8P12 이상의 ONTAP 9.8 패치에서도 사용할 수 있습니다.

ONTAP 9.8P12 이상 ONTAP 9.8 패치 릴리즈를 사용하고 시스템 관리자를 사용하여 SnapMirror를 구성한 경우, ONTAP 9.9.1 또는 ONTAP 9.10.1 릴리즈로 업그레이드할 계획이면 ONTAP 9.9.1.1P13 이상 및 ONTAP 9.10.1P10 이상 패치 릴리즈를 사용해야 합니다.

시작하기 전에

- 소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

  "클러스터 및 SVM 피어링"

- 대상 볼륨의 언어는 소스 볼륨의 언어와 동일해야 합니다.

이 작업에 대해

ONTAP 9.3까지 SnapMirror는 DP 모드에서 호출되고 SnapMirror는 XDP 모드에서 호출될 때까지 서로 다른 복제 엔진을 사용했으며, 버전 의존성에 대한 접근법도 다릅니다.

- DP 모드에서 호출된 SnapMirror는 ONTAP 버전이 운영 스토리지와 2차 스토리지에서 동일해야 하는 _version-dependent_replication 엔진을 사용합니다.

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- XDP 모드에서 호출된 SnapMirror는 운영 스토리지와 보조 스토리지에서 서로 다른 ONTAP 버전을 지원하는 _version-flexible_replication 엔진을 사용했습니다.

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

성능이 향상됨에 따라 버전에 상관없이 유연한 SnapMirror의 주요 이점이 버전에 따라 달라지는 복제 처리량의 약간 이점보다 훨씬 큽니다. 이러한 이유로 ONTAP 9.3부터 XDP 모드가 새로운 기본값이 되었으며 명령줄이나 신규 또는 기존 스크립트에서 DP 모드를 호출하는 경우 XDP 모드가 자동으로 XDP 모드로 변환됩니다.

기존 관계는 영향을 받지 않습니다. 관계가 이미 DP 유형인 경우 DP 유형이 됩니다. 아래 표에는 예상되는 동작이 나와 있습니다.

지정하는 경우…	유형은…	기본 정책(정책을 지정하지 않은 경우)은…
DP	XDP	MirrorAllSnapshots(SnapMirror DR)
아무것도 없습니다	XDP	MirrorAllSnapshots(SnapMirror DR)
XDP	XDP	XDPDefault(SnapVault)

아래 절차의 예를 참조하십시오.

변환 예외 사항은 다음과 같습니다.

- SVM 데이터 보호 관계는 DP 모드로 계속 기본이 됩니다.

  XDP를 명시적으로 지정하여 기본 MirorAllSnapshots 정책으로 XDP 모드를 가져옵니다.

- 로드 공유 데이터 보호 관계는 기본적으로 DP 모드로 유지됩니다.
- SnapLock 데이터 보호 관계는 기본적으로 DP 모드로 유지됩니다.
- DP의 명시적 호출은 다음 클러스터 전체 옵션을 설정한 경우 계속해서 DP 모드로 설정됩니다.

  ```
  options replication.create_data_protection_rels.enable on
  ```

  DP를 명시적으로 호출하지 않으면 이 옵션은 무시됩니다.

ONTAP 9.14.1부터, `-backoff-level` 및 명령에 옵션이 추가되어 `snapmirror create` `snapmirror modify` `snapmirror restore` 관계별 백오프 레벨을 지정할 수 있습니다. 이 옵션은 FlexVol SnapMirror 관계에서만 지원됩니다. 선택적 명령은 클라이언트 작업에 따른 SnapMirror 백 오프 레벨을 지정합니다. Backoff 값은 high, medium 또는 none일 수 있습니다. 기본값은 high 입니다.

ONTAP 9.5부터 SnapMirror 동기식 관계가 지원됩니다.

ONTAP 9.4 이상에서는 대상 볼륨에 최대 1019개의 스냅샷을 포함할 수 있습니다. ONTAP 9.3 및 이전 버전에서는 대상 볼륨에 최대 251개의 스냅샷을 포함할 수 있습니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 복제 관계를 생성할 수 있습니다.

시스템 관리자

1. 보호할 볼륨 또는 LUN을 선택합니다. * 스토리지 > 볼륨 * 또는 * 스토리지 > LUN * 을 클릭한 다음 원하는 볼륨 또는 LUN 이름을 클릭합니다.
2. 을 Protect 클릭합니다.
3. 대상 클러스터와 스토리지 VM을 선택합니다.
4. 비동기식 정책이 기본적으로 선택됩니다. 동기식 정책을 선택하려면 * 추가 옵션 * 을 클릭합니다.
5. 보호 * 를 클릭합니다.
6. 선택한 볼륨 또는 LUN의 * SnapMirror(로컬 또는 원격) * 탭을 클릭하여 보호가 올바르게 설정되었는지 확인합니다.

CLI를 참조하십시오

1. 대상 클러스터에서 복제 관계를 생성합니다.

   이 명령을 실행하기 전에 꺾쇠 괄호 안의 변수를 필수 값으로 바꾸어야 합니다.

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
```

   `schedule`매개 변수는 SnapMirror 동기식 관계를 생성할 때 적용할 수 없습니다.

   다음 예에서는 기본 'MirorLatest' 정책을 사용하여 SnapMirror DR 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
MirrorLatest
```

   다음 예에서는 기본 "XDPDefault" 정책을 사용하여 SnapVault 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
XDPDefault
```

   다음 예에서는 기본 MirorAndVault 정책을 사용하여 통합 복제 관계를 생성합니다.

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
MirrorAndVault
```

   다음 예에서는 사용자 지정 my_unified" 정책을 사용하여 통합 복제 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

다음 예에서는 기본 `Sync` 정책을 사용하여 SnapMirror 동기식 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

다음 예에서는 기본 `StrictSync` 정책을 사용하여 SnapMirror 동기식 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

다음 예에서는 SnapMirror DR 관계를 생성합니다. DP 유형이 자동으로 XDP로 변환되고 정책이 지정되지 않은 경우 정책은 기본적으로 'MirorAllSnapshots' 정책으로 설정됩니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

다음 예에서는 SnapMirror DR 관계를 생성합니다. 유형이나 정책이 지정되지 않은 경우 정책은 기본적으로 'MirorAllSnapshots' 정책으로 설정됩니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

다음 예에서는 SnapMirror DR 관계를 생성합니다. 정책이 지정되지 않은 경우 정책은 기본적으로 'XDPDefault' 정책으로 설정됩니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

다음 예에서는 사전 정의된 정책과 SnapMirror 동기식 관계를 `SnapCenterSync` 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

미리 정의된 정책의 `SnapCenterSync` 유형이 `Sync`입니다. 이 정책은 "`app_consistent`"로 생성된 모든 스냅샷을 `snapmirror-label` 복제합니다.

작업을 마친 후

를 사용합니다 `snapmirror show` 명령을 사용하여 SnapMirror 관계가 생성되었는지 확인합니다.

에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "SnapMirror 페일오버 테스트 볼륨을 생성하고 삭제합니다"..

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	"SnapVault를 사용한 볼륨 백업 개요"

관련 정보

- "SnapMirror 생성"

ONTAP SnapMirror 복제 관계를 초기화합니다

모든 관계 유형에 대해 초기화는 a_baseline transfer_:를 수행합니다. 즉, 소스 볼륨의 스냅샷을 생성한 다음 해당 복사본과 해당 복제본이 참조하는 모든 데이터 블록을 대상 볼륨에 전송합니다. 그렇지 않으면 전송 내용이 정책에 따라 달라집니다.

시작하기 전에

소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

"클러스터 및 SVM 피어링"

이 작업에 대해

초기화에는 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 기준 전송을 실행할 수 있습니다.

ONTAP 9.5부터 SnapMirror 동기식 관계가 지원됩니다.

노드 재부팅, 인수/반환 또는 패닉 등의 이유로 파일 시스템이 재부팅되는 경우 초기화가 자동으로 재개되지 않으므로 수동으로 다시 시작해야 합니다.

단계

1. 복제 관계 초기화:

```
snapmirror initialize -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 초기화합니다.

```
cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 미러 볼트 배포에서 공통 스냅샷을 보장합니다

당신은 사용할 수 있습니다 `snapmirror snapshot-owner create` 미러-볼트 배포 환경에서 보조 노드에 레이블이 지정된 스냅샷을 보존하는 명령입니다. 이렇게 하면 볼트 관계 업데이트를 위한 공통 스냅샷이 생성됩니다.

이 작업에 대해

미러 볼트 팬 아웃 또는 캐스케이드 배포를 함께 사용하는 경우 소스 및 대상 볼륨에 공통 스냅샷이 없으면 업데이트가 실패한다는 점에 유의해야 합니다.

SnapMirror는 업데이트를 수행하기 전에 항상 소스 볼륨의 스냅샷을 생성하므로 미러 볼트 팬아웃 또는 캐스케이드 배포에서는 미러 관계에 문제가 되지 않습니다.

그러나 SnapMirror는 볼트 관계를 업데이트할 때 원본 볼륨의 스냅샷을 생성하지 않기 때문에 볼트 관계의 문제일 수 있습니다. 볼트 관계의 원본과 대상 모두에 공통 스냅샷이 하나 이상 있는지 확인하려면 을 사용해야 `snapmirror snapshot-owner create` 합니다. "데이터 보호 팬아웃 및 캐스케이드 구축에 대해 자세히 알아보십시오"..

단계

1. 소스 볼륨에서 보존하려는 레이블이 지정된 스냅샷에 소유자를 할당합니다.

   ```
   snapmirror snapshot-owner create -vserver <SVM> -volume <volume> -snapshot
   <snapshot> -owner <owner>
   ```

   다음 예에서는 `ApplicationA` 스냅샷의 소유자로 `snap1` 할당합니다.

   ```
   clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

   자세히 알아보세요 `snapmirror snapshot-owner create` 에서 "ONTAP 명령 참조입니다" .

2. 에 설명된 대로 미러 관계를 업데이트합니다 "복제 관계를 수동으로 업데이트합니다".

   또는 미러 관계의 예약된 업데이트를 기다릴 수 있습니다.

3. 레이블이 지정된 스냅샷을 볼트 대상으로 전송:

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
   snapshot
   ```

다음 예에서는 **snap1** 스냅샷을 전송합니다

```
clust1::> snapmirror update -vserver vs1 -volume vol1
-source-snapshot snap1
```

볼트 관계가 업데이트될 때 레이블이 지정된 스냅샷이 보존됩니다.

에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 소스 볼륨에서 레이블이 지정된 스냅샷에서 소유자를 제거합니다.

'스냅샷-소유자 삭제 - vserver_SVM_-volume_volume_-snapshot_snapshot_-owner_owner_'

다음 예에서는 스냅샷 소유자로서 `snap1` 를 제거합니다 `ApplicationA`.

```
clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
-snapshot snap1 -owner ApplicationA
```

에 대한 자세한 내용은 `snapmirror snapshot-owner delete` "ONTAP 명령 참조입니다"을 참조하십시오.

예: ONTAP SnapMirror 볼트-볼트 캐스케이드를 구성합니다

한 번에 한 단계씩 복제 관계를 구성하는 방법을 구체적으로 보여 주는 예가 나와 있습니다. 이 예제에서 구성한 볼트-볼트 캐스케이드 배포를 사용하여 라벨이 붙은 251개 이상의 스냅샷을 보존할 수 `my-weekly` 있습니다.

시작하기 전에

소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

이 작업에 대해

이 예제에서는 다음을 가정합니다.

- 소스 클러스터에 SnapMirror 레이블, `my-weekly` 및 `my-monthly` 을 사용하여 스냅샷을 구성했습니다. `my-daily`
- 2차 및 3차 대상 클러스터에 이라는 대상 볼륨을 구성했습니다. `volA`
- 2차 및 3차 대상 클러스터에서 이름이 지정된 복제 작업 일정을 구성했습니다. `my_snapvault`

이 예에서는 두 개의 사용자 지정 정책을 기반으로 복제 관계를 생성하는 방법을 보여 줍니다.

- 이 `snapvault_secondary` 정책은 2차 대상 클러스터에 매일 7개, 주별 52개 및 월별 180개의 스냅샷을 보존합니다.
- 는 `snapvault_tertiary policy` 3차 대상 클러스터에 매주 250개의 스냅샷을 보존합니다.

단계

1. 보조 대상 클러스터에서 정책을 생성합니다 `snapvault_secondary`.

```
cluster_secondary::> snapmirror policy create -policy snapvault_secondary
-type vault -comment "Policy on secondary for vault to vault cascade" -vserver
svm_secondary
```

2. 보조 대상 클러스터에서 정책에 대한 규칙을 정의합니다 `my-daily`.

   'cluster_secondary::> snapmirror policy add-rule-policy snapvault_secondary-snapmirror-label my-daily-keep 7-vserver svm_secondary'

3. 보조 대상 클러스터에서 정책에 대한 규칙을 정의합니다 `my-weekly`.

   'cluster_secondary::> snapmirror policy add-rule-policy snapvault_secondary-snapmirror-label my-weekly-keep 52-vserver svm_secondary'

4. 보조 대상 클러스터에서 정책에 대한 규칙을 정의합니다 `my-monthly`.

   'cluster_secondary::> SnapMirror 정책 add-rule-policy snapvault_secondary-snapmirror-label my-monthly-keep 180-vserver svm_secondary'

5. 보조 대상 클러스터에서 정책을 확인합니다.

   'cluster_secondary:::> snapmirror policy show snapvault_secondary-instance'

```
                    Vserver: svm_secondary
      SnapMirror Policy Name: snapvault_secondary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on secondary for vault to vault
cascade
       Total Number of Rules: 3
                  Total Keep: 239
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-daily               7  false       0 -
-
                              my-weekly             52  false       0 -
-
                              my-monthly           180  false       0 -
-
```

6. 보조 대상 클러스터에서 소스 클러스터와의 관계를 생성합니다.

   'cluster_secondary::> snapmirror create-source-path svm_primary: VolA-destination-path svm_secondary: VolA-type XDP - schedule my_SnapVault-policy SnapVault_secondary'

7. 보조 대상 클러스터에서 소스 클러스터와의 관계를 초기화합니다.

   'cluster_secondary::> snapmirror initialize-source-path svm_primary: VolA-destination-path svm_secondary: VolA'

8. 3차 대상 클러스터에서 `snapvault_tertiary` 정책을 생성합니다.

   ```
   cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type vault -comment "Policy on tertiary for vault to vault cascade" -vserver svm_tertiary
   ```

9. 3차 대상 클러스터에서 정책에 대한 규칙을 정의합니다 `my-weekly`.

   'cluster_tertiary::> SnapMirror 정책 add-rule-policy snapvault_tertiary-snapmirror-label my-weekly-keep 250-vserver svm_tertiary'

10. 3차 대상 클러스터에서 정책을 확인합니다.

    'cluster_tertiary:::> snapmirror policy show snapvault_tertiary-instance'

    ```
                         Vserver: svm_tertiary
          SnapMirror Policy Name: snapvault_tertiary
          SnapMirror Policy Type: vault
                    Policy Owner: cluster-admin
                     Tries Limit: 8
                Transfer Priority: normal
       Ignore accesstime Enabled: false
         Transfer Restartability: always
     Network Compression Enabled: false
                 Create Snapshot: false
                         Comment: Policy on tertiary for vault to vault
    cascade
           Total Number of Rules: 1
                      Total Keep: 250
                           Rules: SnapMirror Label     Keep  Preserve Warn
    Schedule Prefix
                                  ----------------     ----  -------- ----
    -------- ------
                                  my-weekly             250  false       0 -
    -
    ```

11. 3차 대상 클러스터에서 2차 클러스터와의 관계를 생성합니다.

    'cluster_tertiary::> snapmirror create-source-path svm_secondary: VolA-destination-path svm_tertiary:

VolA-type XDP - schedule my_SnapVault-policy SnapVault_tertiary'

12. 3차 대상 클러스터에서 2차 클러스터와의 관계를 초기화합니다.

    'cluster_tertiary::> snapmirror initialize-source-path svm_secondary: VolA-destination-path svm_tertertiary: VolA'

관련 정보

- "SnapMirror 생성"
- "SnapMirror 초기화"
- "스냅미러 정책 추가 규칙"
- "스냅미러 정책 생성"
- "스냅미러 정책 보기"

SnapMirror 볼륨 복제를 관리합니다

기존 ONTAP SnapMirror DP 유형 관계를 XDP로 변환합니다

ONTAP 9.12.1 이상으로 업그레이드하는 경우 업그레이드하기 전에 DP 유형 관계를 XDP로 변환해야 합니다. ONTAP 9.12.1 이상은 DP 유형 관계를 지원하지 않습니다. 기존 DP 유형 관계를 XDP로 쉽게 변환하여 버전에 상관없이 유연한 SnapMirror를 활용할 수 있습니다.

ONTAP 9.12.1로 업그레이드하기 전에 기존 DP 유형 관계를 XDP로 변환해야 ONTAP 9.12.1 이상 릴리즈로 업그레이드할 수 있습니다.

이 작업에 대해

- SnapMirror는 기존 DP 유형 관계를 XDP로 자동 변환하지 않습니다. 관계를 변환하려면 기존 관계를 분리 및 삭제하고 새로운 XDP 관계를 생성한 다음 관계를 다시 동기화해야 합니다.
- 전환을 계획할 때는 XDP SnapMirror 관계의 백그라운드 준비 및 데이터 웨어하우징 단계에 시간이 오래 걸릴 수 있습니다. SnapMirror 관계가 오랫동안 "준비 중" 상태를 보고하는 것을 보면 흔히 볼 수 있습니다.

> SnapMirror 관계 유형을 DP에서 XDP로 변환한 후에는 자동 크기 조정 및 공간 보장과 같은 공간 관련 설정이 더 이상 대상에 복제되지 않습니다.

단계

1. 대상 클러스터에서 SnapMirror 관계가 DP 유형이고, 미러 상태가 SnapMired 상태이고, 관계 상태가 Idle 상태이고, 관계가 정상 상태인지 확인합니다.

   ```
   snapmirror show -destination-path <SVM:volume>
   ```

   다음 예제는 'napmirror show' 명령의 출력을 보여줍니다.

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

명령 출력의 복사본을 유지하여 기존 관계 설정을 추적하는 것이 유용할 수 있습니다 `snapmirror show`. 에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 소스 볼륨과 대상 볼륨에서 두 볼륨에 모두 공통 스냅샷이 있는지 확인합니다.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

다음 예에서는 를 보여 줍니다 `volume snapshot show` 소스 및 대상 볼륨의 출력:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. 변환 중에 예약된 업데이트가 실행되지 않도록 하려면 기존 DP 유형 관계를 중지합니다.

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 설정합니다.

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror quiesce` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 기존 DP 유형 관계 끊기:

```
snapmirror break -destination-path <SVM:volume>
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst의 관계를 나눕니다.

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 대상 볼륨에 스냅샷 자동 삭제가 설정되어 있는 경우 비활성화합니다.

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

다음 예에서는 대상 볼륨에서 스냅샷 자동 삭제를 `volA_dst` 비활성화합니다.

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. 기존 DP 유형 관계 삭제:

```
snapmirror delete -destination-path <SVM:volume>
```

에 대한 자세한 내용은 `snapmirror-delete` "ONTAP 명령 참조입니다"을 참조하십시오.

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 삭제합니다.

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. 소스에서 원본 SVM 재해 복구 관계 해제:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

다음 예에서는 SVM 재해 복구 관계를 해제합니다.

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

에 대한 자세한 내용은 `snapmirror release` "ONTAP 명령 참조입니다"을 참조하십시오.

8. 'napmirror show' 명령에서 보존한 출력을 사용하여 새로운 XDP 유형 관계를 생성할 수 있습니다.

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

새 관계는 동일한 소스 볼륨과 타겟 볼륨을 사용해야 합니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 소스 볼륨 간에 SnapMirror 재해 복구 관계를 생성합니다 `volA` 켜짐 `svm1` 및 타겟 볼륨입니다 `volA_dst` 켜짐 `svm_backup` 기본값 사용 `MirrorAllSnapshots` 정책:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. 소스 및 대상 볼륨 재동기화:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

재동기화 시간을 개선하려면 다음을 사용할 수 있습니다. `-quick-resync` 옵션은 있지만 저장 효율성으로 인한 절감 효과가 사라질 수 있다는 점을 알아야 합니다.

> ⓘ 이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다. 재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 재동기화한다.

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

자세히 알아보세요 `snapmirror resync` 에서 "ONTAP 명령 참조입니다" .

10. 스냅샷의 자동 삭제를 해제한 경우 다시 설정합니다.

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

작업을 마친 후

1. 를 사용합니다 `snapmirror show` 명령을 사용하여 SnapMirror 관계가 생성되었는지 확인합니다.

   에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. SnapMirror XDP 대상 볼륨이 SnapMirror 정책에 정의된 대로 스냅샷 업데이트를 시작하면 소스 클러스터의 명령 출력을 사용하여 `snapmirror list-destinations` 새 SnapMirror XDP 관계를 표시합니다.

DP 유형 관계에 대한 추가 정보

ONTAP 9.3부터 XDP 모드가 기본값이며 명령줄이나 새 스크립트 또는 기존 스크립트에서 DP 모드를 호출하면 자동으로 XDP 모드로 변환됩니다.

기존 관계는 영향을 받지 않습니다. 관계가 이미 DP 유형인 경우 DP 유형이 됩니다. ONTAP 9.5부터 MirrorAndVault는 데이터 보호 모드가 지정되지 않았거나 XDP 모드가 관계 유형으로 지정된 경우 기본 정책입니다. 아래 표는 예상되는 동작을 보여줍니다.

지정하는 경우…	유형은…	기본 정책(정책을 지정하지 않은 경우)은…
DP	XDP	MirrorAllSnapshots(SnapMirror DR)
아무것도 없습니다	XDP	MirrorAndVault(통합 복제)
XDP	XDP	MirrorAndVault(통합 복제)

표에서 볼 수 있듯이 다른 상황에서 XDP에 할당된 기본 정책은 변환이 이전 유형과 동일한 기능을 유지하도록 합니다. 물론 필요에 따라 통합 복제에 대한 정책을 비롯한 다양한 정책을 사용할 수 있습니다.

지정하는 경우…	정책은…	그 결과…
DP	MirrorAllSnapshots을 선택합니다	SnapMirror DR
XDPDefault	SnapVault	MirrorAndVault를 선택합니다
통합 복제	XDP	MirrorAllSnapshots을 선택합니다
SnapMirror DR	XDPDefault	SnapVault

변환 예외 사항은 다음과 같습니다.

- SVM 데이터 보호 관계는 ONTAP 9.3 및 이전 버전에서 DP 모드로 계속 기본값입니다.

  ONTAP 9.4부터 SVM 데이터 보호 관계는 기본적으로 XDP 모드로 설정됩니다.

- 루트 볼륨 로드 공유 데이터 보호 관계는 기본적으로 DP 모드로 유지됩니다.
- SnapLock 데이터 보호 관계는 ONTAP 9.4 이하 버전에서 DP 모드로 계속 기본값입니다.

  ONTAP 9.5부터 SnapLock 데이터 보호 관계는 XDP 모드로 기본 설정됩니다.

- DP의 명시적 호출은 다음 클러스터 전체 옵션을 설정한 경우 계속해서 DP 모드로 설정됩니다.

  ```
  options replication.create_data_protection_rels.enable on
  ```

  DP를 명시적으로 호출하지 않으면 이 옵션은 무시됩니다.

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 중지"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"

ONTAP SnapMirror 관계의 유형을 변환합니다

ONTAP 9.5부터 SnapMirror Synchronous가 지원됩니다. 기본 전송을 수행하지 않고도 SnapMirror 비동기식 관계를 SnapMirror 동기식 관계로 변환하거나 그 반대로 전환할 수 있습니다.

이 작업에 대해

SnapMirror 정책을 변경하여 SnapMirror 비동기식 관계를 SnapMirror 동기식 관계로 변환하거나 그 반대로 변환할 수 없습니다.

단계

- * SnapMirror 비동기 관계를 SnapMirror 동기 관계로 변환 *

  a. 대상 클러스터에서 SnapMirror 비동기식 관계를 삭제합니다.

  ```
  snapmirror delete -destination-path <SVM:volume>
  ```

  ```
  cluster2::>snapmirror delete -destination-path vs1_dr:vol1
  ```

  b. 소스 클러스터에서 일반 스냅샷을 삭제하지 않고 SnapMirror 관계를 해제합니다.

  ```
  snapmirror release -relationship-info-only true -destination-path
  <destination_SVM>:<destination_volume>
  ```

  ```
  cluster1::>snapmirror release -relationship-info-only true
  -destination-path vs1_dr:vol1
  ```

  c. 대상 클러스터에서 SnapMirror 동기식 관계를 생성합니다.

  ```
  snapmirror create -source-path src_SVM:src_volume -destination-path
  <destination_SVM>:<destination_volume> -policy sync-mirror
  ```

  ```
  cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
  vs1_dr:vol1 -policy sync
  ```

  d. SnapMirror 동기식 관계 재동기화:

  ```
  snapmirror resync -destination-path <destination_SVM:destination_volume>
  ```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

- * SnapMirror 동기식 관계를 SnapMirror 비동기식 관계로 변환 *

  a. 대상 클러스터에서 기존 SnapMirror 동기식 관계를 중지합니다.

  ```
  snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
  ```

  ```
  cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
  ```

  b. 대상 클러스터에서 SnapMirror 비동기식 관계를 삭제합니다.

  ```
  snapmirror delete -destination-path <SVM:volume>
  ```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

c. 소스 클러스터에서 일반 스냅샷을 삭제하지 않고 SnapMirror 관계를 해제합니다.

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM:destination_volume>
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

d. 대상 클러스터에서 SnapMirror 비동기식 관계를 생성합니다.

```
snapmirror create -source-path src_SVM:src_volume -destination-path
<destination_SVM:destination_volume> -policy MirrorAllSnapshots
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

e. SnapMirror 동기식 관계 재동기화:

```
snapmirror resync -destination-path <destination_SVM:destination_volume>
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 중지"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"

ONTAP SnapMirror 동기식 관계의 모드를 변환합니다

ONTAP 9.5부터 SnapMirror 동기식 관계가 지원됩니다. SnapMirror 동기식 관계의 모드를 StrictSync에서 Sync로 또는 그 반대로 변환할 수 있습니다.

이 작업에 대해

SnapMirror 동기식 관계의 정책을 수정하여 모드를 변환할 수는 없습니다.

단계

1. 대상 클러스터에서 기존 SnapMirror 동기식 관계를 중지합니다.

```
snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

2. 대상 클러스터에서 기존 SnapMirror 동기식 관계를 삭제합니다.

```
snapmirror delete -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror delete -destination-path vs1_dr:vol1
```

3. 소스 클러스터에서 일반 스냅샷을 삭제하지 않고 SnapMirror 관계를 해제합니다.

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM>:<destination_volume>
```

```
cluster1::> snapmirror release -relationship-info-only true -destination
-path vs1_dr:vol1
```

4. 대상 클러스터에서 SnapMirror 동기식 관계를 변환할 모드를 지정하여 SnapMirror 동기식 관계를 생성합니다.

```
snapmirror create -source-path vs1:vol1 -destination-path
<destination_SVM>:<destination_volume> -policy Sync|StrictSync
```

```
cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy Sync
```

5. 대상 클러스터에서 SnapMirror 관계를 다시 동기화합니다.

```
snapmirror resync -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 중지"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"

ONTAP SnapMirror 페일오버 테스트 볼륨을 생성하고 삭제합니다

ONTAP 9.14.1부터 System Manager를 사용하여 활성 SnapMirror 관계를 중단하지 않고 SnapMirror 페일오버 및 재해 복구를 테스트하는 볼륨 클론을 생성할 수 있습니다. 테스트를 마치면 연결된 데이터를 정리하고 테스트 볼륨을 삭제할 수 있습니다.

SnapMirror 페일오버 테스트 볼륨을 생성합니다

이 작업에 대해

- 동기식 및 SnapMirror 비동기식 관계에 대해 페일오버 테스트를 수행할 수 있습니다.
- 재해 복구 테스트를 수행하기 위한 볼륨 클론이 생성됩니다.
- 클론 볼륨은 SnapMirror 대상과 동일한 스토리지 VM에 생성됩니다.
- FlexVol 및 FlexGroup SnapMirror 관계를 사용할 수 있습니다.
- 선택한 관계에 대한 테스트 클론이 이미 있으면 해당 관계에 대해 다른 클론을 생성할 수 없습니다.
- SnapLock 볼트 관계는 지원되지 않습니다.

시작하기 전에

- 클러스터 관리자여야 합니다.
- SnapMirror 라이센스를 소스 및 대상 클러스터에 설치해야 합니다.

단계

1. 대상 클러스터에서 * 보호 > 관계 * 를 선택합니다.
2. 관계 소스 옆에 있는 을 ⋮ 선택하고 * Test Failover * 를 선택합니다.
3. Test Failover * 창에서 * Test Failover * 를 선택합니다.
4. 스토리지 > 볼륨 * 을 선택하고 테스트 페일오버 볼륨이 표시되는지 확인합니다.
5. 스토리지 > 공유 * 를 선택합니다.
6. 을 + Add 선택하고 * 공유 * 를 선택합니다.
7. 공유 추가 * 창의 * 공유 이름 * 필드에 공유 이름을 입력합니다.
8. 폴더 * 필드에서 * 찾아보기 * 를 선택하고 테스트 클론 볼륨을 선택한 다음 * 저장 * 을 선택합니다.
9. 공유 추가 * 창 아래쪽에서 * 저장 * 을 선택합니다.
10. 스토리지 > 공유 * 창에서 생성한 공유를 찾은 후 를 선택하여 ⌄ 공유 정보를 봅니다.
11. SMB/CIFS 액세스 * 에서 공유에 대한 액세스 경로를 복사하거나 기록해 둡니다(예 `\\123.456.7.890\failover_test`:).
12. SMB 액세스 경로를 사용하여 클라이언트에서 공유를 열고 테스트 볼륨에 읽기 및 쓰기 기능이 있는지 확인합니다.

장애 조치 데이터를 정리하고 테스트 볼륨을 삭제합니다

장애 조치 테스트를 완료한 후 테스트 볼륨과 연결된 모든 데이터를 정리하고 삭제할 수 있습니다.

단계

1. 대상 클러스터에서 * 보호 > 관계 * 를 선택합니다.

2. 관계 소스 옆에 있는 을 ⋮ 선택하고 * Clean Up Test Failover * 를 선택합니다.
3. Clean Up Test Failover * 창에서 * Clean Up * 을 선택합니다.
4. 스토리지 > 볼륨 * 을 선택하고 테스트 볼륨이 삭제되었는지 확인합니다.

SnapMirror DR 대상 볼륨의 데이터를 제공합니다

ONTAP SnapMirror 대상 볼륨을 쓰기 가능하게 만듭니다

볼륨에서 클라이언트로 데이터를 제공하려면 먼저 대상 볼륨을 쓰기 가능하게 만들어야 합니다. 소스를 사용할 수 없게 될 때 미러 대상에서 데이터를 제공하려면 대상에 대한 예약된 전송을 중지한 다음 SnapMirror 관계를 끊어 대상을 쓰기 가능으로 만듭니다.

이 작업에 대해

이 작업은 대상 SVM 또는 타겟 클러스터에서 수행해야 합니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 대상 볼륨을 쓰기 가능하게 만들 수 있습니다.

시스템 관리자

1. 보호 관계를 선택합니다. * 보호 > 관계 * 를 클릭한 후 원하는 볼륨 이름을 클릭합니다.
2. 을 클릭합니다.
3. 예약된 전송 중지: * 일시 중지 * 를 클릭합니다.
4. 대상을 쓰기 가능 상태로 만듭니다. * Break * (중단 *)를 클릭합니다.
5. 기본 * 관계 * 페이지로 이동하여 관계 상태가 "연결 해제"로 표시되는지 확인합니다.

다음 단계

대상 볼륨을 쓰기 가능한 볼륨으로 만든 후에 이 "복제 관계를 역방향으로 재동기화합니다" 작업을 수행해야 합니다.

비활성화된 소스 볼륨을 다시 사용할 수 있게 되면 관계를 다시 역동기화하여 현재 데이터를 원래 소스 볼륨에 복제해야 합니다.

CLI를 참조하십시오

1. 목적지로의 예약된 전송 중지:

```
snapmirror quiesce -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 예약된 전송을 중지합니다.

```
cluster_dst::> snapmirror quiesce -source-path svm1:volA
-destination-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror quiesce` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 목적지로의 진행 중인 전송을 중지합니다.

```
snapmirror abort -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

SnapMirror 동기식 관계에는 이 단계가 필요하지 않습니다(ONTAP 9.5부터 지원됨).

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 지속적인 전송을 중지합니다.

```
cluster_dst::> snapmirror abort -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror abort` "ONTAP 명령 참조입니다"을 참조하십시오.

3. SnapMirror DR 관계 끊기:

```
snapmirror break -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst의 관계를 나눕니다.

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 단계

대상 볼륨을 쓰기 가능한 볼륨으로 만든 후에 이 "복제 관계를 다시 동기화합니다" 작업을 수행해야 합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	"볼륨 재해 복구 개요"

데이터 액세스를 위한 **ONTAP SnapMirror** 대상 볼륨을 구성합니다

대상 볼륨을 쓰기 가능한 상태로 만든 후 데이터 액세스를 위해 볼륨을 구성해야 합니다. 소스 볼륨이 다시 활성화될 때까지 NAS 클라이언트, NVMe 하위 시스템 및 SAN 호스트가 대상 볼륨의 데이터에 액세스할 수 있습니다.

NAS 환경:

1. 소스 볼륨이 소스 SVM에 마운트된 것과 동일한 접합 경로를 사용하여 NAS 볼륨을 네임스페이스에 마운트합니다.
2. 대상 볼륨의 SMB 공유에 적절한 ACL을 적용합니다.
3. 대상 볼륨에 NFS 내보내기 정책을 할당합니다.
4. 대상 볼륨에 할당량 규칙을 적용합니다.
5. 대상 볼륨으로 클라이언트를 리디렉션합니다.
6. 클라이언트에서 NFS 및 SMB 공유를 다시 마운트합니다.

SAN 환경:

1. 볼륨의 LUN을 적절한 이니시에이터 그룹에 매핑합니다.
2. iSCSI의 경우 SAN 호스트 이니시에이터에서 SAN LIF로 iSCSI 세션을 생성합니다.
3. SAN 클라이언트에서 스토리지 재검색을 수행하여 연결된 LUN을 검색합니다.

NVMe 환경에 대한 자세한 내용은 을 참조하십시오 "SAN 관리".

원래 **ONTAP SnapMirror** 소스 볼륨을 다시 활성화합니다

대상에서 데이터를 더 이상 제공할 필요가 없을 때 소스 볼륨과 타겟 볼륨 간에 원래 데이터 보호 관계를 다시 설정할 수 있습니다.

이 작업에 대해

- 아래 절차에서는 원본 소스 볼륨의 기준선이 온전한 것으로 가정합니다. 기준선이 변경되지 않은 경우 절차를 수행하기 전에 데이터를 제공하는 볼륨과 원본 소스 볼륨 간의 관계를 생성하고 초기화해야 합니다.
- XDP SnapMirror 관계의 백그라운드 준비 및 데이터 웨어하우징 단계는 시간이 오래 걸릴 수 있습니다. SnapMirror 관계가 오랫동안 "준비 중" 상태를 보고하는 것을 보면 흔히 볼 수 있습니다.

단계

1. 원래 데이터 보호 관계를 반대로 전환합니다.

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   에 대한 자세한 내용은 `snapmirror resync` "ONTAP 명령 참조입니다"을 참조하십시오.

   > ⓘ 이 명령은 원래 소스 SVM 또는 원래 소스 클러스터에서 실행해야 합니다. 재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다. 소스와 대상에 공통 스냅샷이 없는 경우 명령이 실패합니다. `snapmirror initialize`관계를 다시 초기화하는 데 사용합니다. 에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 svm1의 원본 소스 볼륨 VolA와 SVM_BACKUP의 데이터 제공 볼륨 VolA_DST 사이의 관계를 반전시킵니다.

   ```
   cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

2. 원래 소스에 대한 데이터 액세스를 다시 설정할 준비가 되면 원래 타겟 볼륨에 대한 액세스를 중지하십시오. 한 가지 방법은 원래 대상 SVM을 중지하는 것입니다.

   'vserver stop-vserver_SVM_'

   > ⓘ 이 명령은 원래 대상 SVM 또는 원래 대상 클러스터에서 실행해야 합니다. 이 명령을 사용하면 사용자가 전체 원래 대상 SVM에 액세스할 수 없습니다. 다른 방법을 사용하여 원래 대상 볼륨에 대한 액세스를 중지할 수 있습니다.

   다음 예에서는 원래 대상 SVM을 중지합니다.

   ```
   cluster_dst::> vserver stop svm_backup
   ```

   에 대한 자세한 내용은 `vserver stop` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 반대 관계 업데이트:

   `snapmirror update -source-path SVM:volume -destination-path SVM:volume`

   이 명령은 원래 소스 SVM 또는 원래 소스 클러스터에서 실행해야 합니다.

   다음 예에서는 데이터를 제공하고 있는 볼륨, VM_BACKUP의 VolA_DST, Svm1의 원본 소스 볼륨 VolA의 관계를 업데이트합니다.

   ```
   cluster_src::> snapmirror update -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 원래 소스 SVM 또는 원래 소스 클러스터에서 역방향 관계에 대한 예약된 전송을 중지합니다.

   `snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume`

   이 명령은 원래 소스 SVM 또는 원래 소스 클러스터에서 실행해야 합니다.

   다음 예에서는 원래 대상 볼륨 간의 예약된 전송을 중지합니다. `volA_dst` 켜짐 `svm_backup`및 원본 소스 볼륨, `volA` 켜짐 `svm1`:

   ```
   cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   에 대한 자세한 내용은 `snapmirror quiesce` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 최종 업데이트가 완료되고 관계가 관계 상태에 "중지됨"으로 표시되면 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계를 분리합니다.

   `snapmirror break -source-path SVM:volume -destination-path SVM:volume`

   이 명령은 원래 소스 SVM 또는 소스 클러스터에서 실행해야 합니다.

   다음 예에서는 원래 대상 볼륨 간의 관계를 끊는 경우를 보여 줍니다. `volA_dst` 켜짐 `svm_backup`및 원본 소스 볼륨, `volA` 켜짐 `svm1`:

   ```
   cluster_scr::> snapmirror break -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 원래 소스 SVM 또는 원래 소스 클러스터에서 역방향 데이터 보호 관계를 삭제합니다.

`snapmirror delete -source-path SVM:volume -destination-path SVM:volume`

이 명령은 원래 소스 SVM 또는 원래 소스 클러스터에서 실행해야 합니다.

다음 예에서는 svm1의 원래 소스 볼륨 VolA와 SVM_BACKUP의 VolA_DST에서 데이터를 제공하고 있는 볼륨 간의 역방향 관계를 삭제합니다.

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

에 대한 자세한 내용은 `snapmirror delete` "ONTAP 명령 참조입니다"을 참조하십시오.

7. 원래 대상 SVM 또는 원래 대상 클러스터에서 역방향 관계를 해제합니다.

`snapmirror release -source-path SVM:volume -destination-path SVM:volume`

이 명령은 원래 대상 SVM 또는 원래 대상 클러스터에서 실행해야 합니다.

다음 예에서는 원래 타겟 볼륨 간의 역방향 관계를 해제하며 `volA_dst` 켜짐 `svm_backup`및 원본 소스 볼륨, `volA` 켜짐 `svm1`:

```
cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

에 대한 자세한 내용은 `snapmirror release` "ONTAP 명령 참조입니다"을 참조하십시오.

8. 원래 대상에서 원래 데이터 보호 관계를 다시 설정합니다.

`snapmirror resync -source-path SVM:volume -destination-path SVM:volume`

다음 예에서는 svm1의 원본 소스 볼륨 VolA와 sm_backup의 원래 대상 볼륨 VolA_dst 간의 관계를 다시 설정합니다.

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror resync` "ONTAP 명령 참조입니다"을 참조하십시오.

9. 필요한 경우 원래 대상 SVM을 시작합니다.

'vserver start-vserver_SVM_'

다음 예에서는 원래 대상 SVM을 시작합니다.

```
cluster_dst::> vserver start svm_backup
```

에 대한 자세한 내용은 `vserver start` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

를 사용합니다 `snapmirror show` 명령을 사용하여 SnapMirror 관계가 생성되었는지 확인합니다.

에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

SnapMirror 대상 볼륨에서 파일을 복원합니다

ONTAP SnapMirror 대상에서 파일, LUN 또는 NVMe 네임스페이스를 복원합니다

단일 파일, LUN, 스냅샷에서 파일 또는 LUN 세트를 복원하거나 SnapMirror 대상 볼륨에서 NVMe 네임스페이스를 복원할 수 있습니다. ONTAP 9.7부터는 SnapMirror 동기식 대상에서 NVMe 네임스페이스를 복원할 수도 있습니다. 파일을 원래 소스 볼륨이나 다른 볼륨으로 복원할 수 있습니다.

시작하기 전에

SnapMirror 동기 대상(ONTAP 9.5부터 지원됨)에서 파일 또는 LUN을 복구하려면 먼저 관계를 삭제하고 해제해야 합니다.

이 작업에 대해

파일 또는 LUN(대상 볼륨)을 복원하는 볼륨은 읽기-쓰기 볼륨이어야 합니다.

- SnapMirror는 소스 및 대상 볼륨에 공통 스냅샷이 있는 경우 _ 증가분 복구 _ 를 수행합니다(일반적으로 원래 소스 볼륨으로 복구할 때와 마찬가지로).
- 그렇지 않으면 SnapMirror가 _baseline restore_를 수행하여 지정된 스냅샷과 해당 스냅샷이 참조하는 모든 데이터 블록이 대상 볼륨으로 전송됩니다.

단계

1. 대상 볼륨의 스냅샷을 나열합니다.

   ```
   volume snapshot show -vserver <SVM> -volume volume
   ```

   에 대한 자세한 내용은 `volume snapshot show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예는 대상의 스냅샷을 보여 `vserverB:secondary1` 줍니다.

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. SnapMirror 대상 볼륨의 스냅샷에서 단일 파일 또는 LUN 또는 파일 또는 LUN 집합 복구:

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
snapshot -file-list <source_file_path,@destination_file_path>
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 명령을 실행하면 `daily.2013-01-25_0010` 원래 대상 볼륨의 스냅샷과 `file2` 파일이 원래 소스 볼륨의 `secondary1` 활성 파일 시스템의 동일한 위치로 `primary1` 복원됩니다. `file1`

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

다음 명령을 실행하면 `daily.2013-01-25_0010` 원래 대상 볼륨의 `secondary1` 스냅샷과 `file2` 파일이 원래 소스 볼륨의 활성 파일 시스템의 다른 위치로 `primary1` 복원됩니다. `file1`

대상 파일 경로는 @ 기호와 원본 소스 볼륨의 루트에서 파일 경로로 시작합니다. 이 예에서는 file1 이 /dir1/file1로

복구되고 file2 가 기본 y1의 /dir2.new/file2 로 복원됩니다.

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

다음 명령을 실행하면 `file3` 원래 대상 볼륨의 `secondary1` 스냅샷과 `daily.2013-01-25_0010` 파일이 원래 소스 볼륨의 활성 파일 시스템의 다른 위치로 복원되고 `file1` 에서 `snap1` 의 활성 파일 시스템의 `primary1` 동일한 위치로 `primary1` 복원됩니다. `file2`

이 예에서는 파일 'file1'이 '/dir1/file1'로 복원되고 새 파일3이 '/dir3.new/file3'로 복원됩니다.

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

관련 정보

- "SnapMirror 복원"

ONTAP SnapMirror 대상에서 볼륨 내용을 복원합니다

SnapMirror 대상 볼륨의 스냅숏에서 전체 볼륨의 내용을 복원할 수 있습니다. 볼륨의 내용을 원래 소스 볼륨 또는 다른 볼륨으로 복원할 수 있습니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 데이터를 복구하려면. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

복원 작업의 대상 볼륨은 다음 중 하나여야 합니다.

- 소스 및 대상 볼륨에 공통 스냅샷이 있는 경우(일반적으로 원래 소스 볼륨으로 복구할 때와 마찬가지로) 읽기-쓰기 볼륨인 경우 SnapMirror가 _증분 복구_를 수행합니다.

  공통 스냅샷이 없는 경우 명령이 실패합니다. 볼륨의 내용을 빈 읽기-쓰기 볼륨으로 복원할 수 없습니다.

- 빈 데이터 보호 볼륨으로서, 이 경우 SnapMirror가 _baseline restore_를 수행하고, 지정된 스냅샷과 해당

스냅샷이 참조하는 모든 데이터 블록이 소스 볼륨으로 전송됩니다.

볼륨의 내용을 복원하는 것은 운영 중단이 발생합니다. 복원 작업이 실행 중일 때는 SnapVault 운영 볼륨에서 SMB 트래픽이 실행되고 있지 않아야 합니다.

복원 작업의 타겟 볼륨에 압축이 활성화되어 있고 소스 볼륨에 압축이 활성화되어 있지 않은 경우 타겟 볼륨에서 압축을 비활성화합니다. 복원 작업이 완료된 후 압축을 다시 활성화해야 합니다.

대상 볼륨에 대해 정의된 할당량 규칙은 복구를 수행하기 전에 비활성화됩니다. 복원 작업이 완료된 후 "volume quota modify" 명령을 사용하여 할당량 규칙을 다시 활성화할 수 있습니다.

볼륨의 데이터가 손실되거나 손상된 경우 이전 스냅샷에서 복원하여 데이터를 롤백할 수 있습니다.

이 절차는 소스 볼륨의 현재 데이터를 이전 스냅샷 버전의 데이터로 대체합니다. 대상 클러스터에서 이 작업을 수행해야 합니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 볼륨의 콘텐츠를 복원할 수 있습니다.

시스템 관리자

1. 보호 > 관계 * 를 클릭한 다음 소스 볼륨 이름을 클릭합니다.
2. 을 ⋮ 클릭한 다음 * 복원 * 을 선택합니다.
3. 소스 * 에서 소스 볼륨은 기본적으로 선택됩니다. 소스 이외의 볼륨을 선택하려면 * 기타 볼륨 * 을 클릭합니다.
4. 대상 * 에서 복원할 스냅샷을 선택합니다.
5. 소스와 대상이 서로 다른 클러스터에 있는 경우 원격 클러스터에서 * 보호 > 관계 * 를 클릭하여 복구 진행률을 모니터링합니다.

CLI를 참조하십시오

1. 대상 볼륨의 스냅샷을 나열합니다.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

다음 예는 대상의 스냅샷을 보여 `vserverB:secondary1` 줍니다.

```
cluster_dst::> volume snapshot show -vserver vserverB -volume
secondary1

Vserver     Volume      Snapshot                State    Size
Total% Used%
-------     ------      ---------- ----------- ------   -----
------ -----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. SnapMirror 대상 볼륨에 있는 스냅샷에서 볼륨의 내용 복원:

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
```

-destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot <snapshot>

> 이 명령은 원래 소스 SVM 또는 원래 소스 클러스터에서 실행해야 합니다.

다음 명령을 실행하면 원래 대상 볼륨에 있는 `secondary1` 스냅샷에서 `daily.2013-01-25_0010` 원본 소스 볼륨의 콘텐츠가 복원됩니다. `primary1`

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010

Warning: All data newer than snapshot daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. 복원된 볼륨을 다시 마운트하고 볼륨을 사용하는 모든 애플리케이션을 다시 시작합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	"SnapVault를 사용한 볼륨 복원 개요"

관련 정보

- "SnapMirror 복원"
- "볼륨 스냅샷 표시"

ONTAP SnapMirror 복제 관계를 수동으로 업데이트합니다

소스 볼륨이 이동되었기 때문에 업데이트에 실패하면 복제 관계를 수동으로 업데이트해야 할 수 있습니다.

이 작업에 대해

SnapMirror는 복제 관계를 수동으로 업데이트할 때까지 이동된 소스 볼륨에서 전송을 중단합니다.

ONTAP 9.5부터 SnapMirror 동기식 관계가 지원됩니다. 소스 볼륨과 타겟 볼륨이 항상 이 관계에서 동기화되지만, 보조 클러스터의 뷰는 매시간 기준으로 운영 클러스터와 동기화됩니다. 대상에서 시점 데이터를 보려면 `snapmirror update` 명령을 실행하여 수동 업데이트를 수행해야 합니다.

단계

1. 복제 관계를 수동으로 업데이트합니다.

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

> 이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다. 소스와 대상에 공통 스냅샷이 없는 경우 명령이 실패합니다. `snapmirror initialize`관계를 다시 초기화하는 데 사용합니다. 에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 업데이트합니다.

```
cluster_src::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror 복제 관계를 다시 동기화합니다

대상 볼륨을 쓰기 가능하게 만든 후, 소스 및 대상 볼륨에 공통 스냅샷이 없기 때문에 업데이트가 실패한 후 또는 관계에 대한 복제 정책을 변경하려는 경우 복제 관계를 다시 동기화해야 합니다.

ONTAP 9.8부터 System Manager를 사용하여 역방향 재동기화 작업을 수행하여 기존 보호 관계를 삭제하고 소스 볼륨과 대상 볼륨의 기능을 반대로 되돌릴 수 있습니다. 그런 다음, 소스를 복구 또는 교체하고 소스를 업데이트하고 시스템의 원래 구성을 다시 설정하는 동안 대상 볼륨을 사용하여 데이터를 제공합니다.

> System Manager는 클러스터 내 관계와의 역방향 재동기화를 지원하지 않습니다. ONTAP CLI를 사용하여 클러스터 내 관계와 역방향 재동기화 작업을 수행할 수 있습니다.

이 작업에 대해

- 재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다.
- 팬아웃 또는 캐스케이드 구성의 일부인 볼륨은 재동기화에 시간이 오래 걸릴 수 있습니다. SnapMirror 관계가 오랫동안 "준비 중" 상태를 보고하는 것을 보면 흔히 볼 수 있습니다.
- ONTAP 9.13.1부터 ONTAP 기본적으로 빠른 재동기화를 사용하여 재동기화 시간을 줄이려고 합니다. 기본적으로 빠른 재동기화를 사용하려면 다음 조건이 충족되어야 합니다.
  - FlexVol 볼륨에는 볼륨에 복제본이 없습니다.
  - MirrorAllSnapshots 정책을 사용하는 경우

> 사용 중 `-quick-resync` 전송된 데이터 블록의 저장 효율성이 제거되어 재동기화 대상 볼륨에서 추가 공간을 소모할 수 있습니다. 이러한 추가 공간 소비는 재동기화 대상에서 인라인 또는 복제 후 스토리지 효율성 적용의 일부로 복구됩니다.

그만큼 `-quick-resync` 매개변수는 선택 사항입니다. 다음을 사용하여 빠른 재동기화를 활성화하거나 비활성화할 수 있습니다. `-quick-resync true|false` 매개변수와 함께 `snapmirror resync` 명령.

더 많은 정보를 원하시면 `-quick-resync`, 참조 "ONTAP 명령 참조입니다".

단계

System Manager 또는 ONTAP CLI를 사용하여 이 작업을 수행할 수 있습니다. ONTAP CLI를 사용하는 경우 대상 볼륨을 쓰기 가능하게 만들지, 복제 관계를 업데이트하는지에 관계없이 절차는 동일합니다.

System Manager 역방향 재동기화

"관계를 끊습니다"대상을 쓰기 가능하게 만들려면 관계를 역순으로 다시 동기화합니다.

1. 대상 클러스터에서 * 보호 > 관계 * 를 클릭합니다.
2. 되돌릴 분리된 관계 위로 마우스를 가져가 를 클릭하고 * Reverse Resync * 를 선택합니다.
3. Reverse resync relationship * 창에서 * Reverse resync * 를 클릭합니다.
4. 관계 * 에서 관계에 대한 * 전송 상태 * 를 확인하여 역방향 재동기화 진행률을 모니터링합니다.

다음 단계

원래 원본을 다시 사용할 수 있게 되면 역방향 관계를 해제하고 다른 역방향 재동기화 작업을 수행하여 원래 관계를 다시 설정할 수 있습니다. 역방향 재동기화 프로세스는 데이터를 제공하는 사이트의 모든 변경 사항을 원래 소스로 복사하고 원래 소스를 다시 읽기-쓰기 가능하게 만듭니다.

System Manager가 다시 동기화됩니다

1. 보호 > 관계 * 를 클릭합니다.
2. 재동기화할 관계 위로 마우스를 가져간 후 를 클릭하고 * Break * 를 선택합니다.
3. 관계 상태가 "해제"로 표시되면 를 클릭한 다음 * 재동기화 * 를 선택합니다.
4. 관계 * 에서 관계 상태를 확인하여 재동기화 진행률을 모니터링합니다. 재동기화가 완료되면 상태가 "미러링 "으로 변경됩니다.

CLI를 참조하십시오

1. 소스 및 대상 볼륨 재동기화:

```
snapmirror resync -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume> -type DP|XDP
-policy <policy>
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 의 소스 볼륨과 의 대상 볼륨 간의 관계를 다시 `volA svm1 volA_dst` `svm_backup`동기화합니다.

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror resync` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "ONTAP SnapMirror 대상 SVM에서 데이터를 다시 동기화합니다"

ONTAP SnapMirror 볼륨 복제 관계를 삭제합니다

및 `snapmirror release` 명령을 사용하여 볼륨 복제 관계를 삭제할 수 `snapmirror delete` 있습니다. 그런 다음 불필요한 대상 볼륨을 수동으로 삭제할 수 있습니다.

이 작업에 대해

이 `snapmirror release` 명령은 SnapMirror에서 생성된 스냅샷을 소스에서 삭제합니다. 옵션을 사용하여 스냅샷을 보존할 수 `-relationship-info-only` 있습니다.

단계

1. 복제 관계를 중지합니다.

   `snapmirror quiesce -destination-path <SVM:volume>|<cluster://SVM/volume>`

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

   에 대한 자세한 내용은 `snapmirror quiesce` "ONTAP 명령 참조입니다"을 참조하십시오.

2. (선택 사항) 대상 볼륨이 읽기/쓰기 볼륨이어야 하는 경우 복제 관계를 끊으십시오. 대상 볼륨을 삭제할 계획이거나 읽기/쓰기가 필요한 볼륨이 없는 경우 이 단계를 건너뛸 수 있습니다.

   `snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume>, … -destination-path <SVM:volume>|<cluster://SVM/volume>, …`

   ```
   cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
   svm_backup:volA_dst
   ```

   에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 복제 관계를 삭제합니다.

   `snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>, … -destination-path <SVM:volume>|<cluster://SVM/volume>, …`

   ⓘ 대상 클러스터 또는 대상 SVM에서 이 명령을 실행해야 합니다.

   다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 삭제합니다.

   ```
   cluster_dst::> snapmirror delete -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

   에 대한 자세한 내용은 `snapmirror delete` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 소스 SVM에서 복제 관계 정보 해제:

```
snapmirror release -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

소스 클러스터 또는 소스 SVM에서 이 명령을 실행해야 합니다.

다음 예에서는 소스 SVM의 vm1에서 지정된 복제 관계에 대한 정보를 해제합니다.

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror release` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror 볼륨에서 스토리지 효율성 관리

SnapMirror는 타겟 볼륨에 사후 처리 데이터 압축이 활성화되어 있는 경우를 제외하고 소스 및 타겟 볼륨에서 스토리지 효율성을 유지합니다. 이 경우 타겟 볼륨에서 스토리지 효율성이 모두 손실됩니다. 이 문제를 해결하려면 타겟 볼륨에서 사후 처리 압축을 비활성화하고 관계를 수동으로 업데이트하며 스토리지 효율성을 다시 활성화해야 합니다.

이 작업에 대해

명령을 사용하여 볼륨에 효율성이 활성화되어 있는지 여부를 확인할 수 `volume efficiency show` 있습니다. 에 대한 자세한 내용은 `volume efficiency show` "ONTAP 명령 참조입니다"을 참조하십시오.

SnapMirror 감사 로그를 보고 전송 설명을 찾아 SnapMirror에서 스토리지 효율성이 유지되는지 확인할 수 있습니다. 전송 설명이 `transfer_desc=Logical Transfer with Storage Efficiency`표시되면 SnapMirror는 스토리지 효율성을 유지하는 것입니다. 전송 설명이 `transfer_desc=Logical Transfer`표시되면 SnapMirror는 스토리지 효율성을 유지하는 것이 아닙니다. 예를 들면 다음과 같습니다.

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uuid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

시작하기 전에

- 소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

  "클러스터 및 SVM 피어링"

- 타겟 볼륨에서 사후 처리 압축을 비활성화해야 합니다.
- 스토리지를 사용한 논리적 전송: ONTAP 9.3부터 스토리지 효율성을 다시 활성화하기 위해 더 이상 수동 업데이트가 필요하지 않습니다. SnapMirror에서 사후 처리 압축이 비활성화되었다고 감지하면 다음 예약 업데이트에서 스토리지 효율성을 자동으로 다시 활성화합니다. 소스와 대상 모두 ONTAP 9.3을 실행해야 합니다.
- ONTAP 9.3부터 AFF 시스템은 타겟 볼륨을 쓰기 가능한 상태로 만든 후 FAS 시스템과 다른 방식으로 스토리지

효율성 설정을 관리합니다.

- 다음을 사용하여 대상 볼륨을 쓰기 가능하게 만든 후 `snapmirror break` 명령을 실행하면 볼륨의 캐싱 정책이 자동으로 설정됩니다. `auto` (기본값).

  이 동작은 FlexVol 볼륨에만 적용되며 FlexGroup 볼륨에는 적용되지 않습니다.

  에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

- 재동기화 시 캐싱 정책이 자동으로 설정됩니다. `none` 원래 설정과 관계없이 중복 제거 및 인라인 압축은 자동으로 비활성화됩니다. 필요에 따라 설정을 수동으로 수정해야 합니다.

스토리지 효율성을 활성화한 수동 업데이트는 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 작업을 실행할 수 있습니다.

단계

1. 복제 관계를 업데이트하고 스토리지 효율성을 다시 설정합니다.

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -enable
-storage-efficiency true
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다. 소스와 대상에 공통 스냅샷이 없는 경우 명령이 실패합니다. `snapmirror initialize`관계를 다시 초기화하는 데 사용합니다. 에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 업데이트하고 스토리지 효율성을 다시 활성화합니다.

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror 전역 제한을 사용합니다

글로벌 네트워크 스로틀링은 모든 SnapMirror 및 SnapVault 전송에 대해 노드 단위로 사용할 수 있습니다.

이 작업에 대해

SnapMirror 글로벌 제한 때문에 들어오고/또는 나가는 SnapMirror 및 SnapVault 전송에 사용되는 대역폭이 제한됩니다. 이 제한은 클러스터의 모든 노드에서 클러스터 전체에 적용됩니다.

예를 들어, 발신 스로틀이 100Mbps로 설정된 경우 클러스터의 각 노드는 발신 대역폭을 100Mbps로 설정합니다. 글로벌 임계치 조절이 비활성화된 경우 모든 노드에서 비활성화됩니다.

데이터 전송 속도는 대개 초당 비트 수(bps)로 표현되지만 스로틀 값은 초당 킬로바이트(kbps)로 입력해야 합니다.

ONTAP 9.9.1 이하 릴리스에서는 스로틀이 전송 또는 로드 공유 미러 전송에 영향을 미치지 `volume move` 않습니다. ONTAP 9.10.0부터 볼륨 이동 작업을 제한하는 옵션을 지정할 수 있습니다. 자세한 내용은 을 참조하십시오 "ONTAP 9.10 이상에서 볼륨 이동을 제한하는 방법".

글로벌 제한은 SnapMirror 및 SnapVault 전송을 위한 관계별 스로틀 기능과 함께 작동합니다. 관계별 전송의 결합된 대역폭이 글로벌 스로틀의 값을 초과할 때까지, 즉 글로벌 스로틀이 적용될 때까지 관계별 스로틀이 적용됩니다. 스로틀 값 0은 글로벌 스로틀링이 비활성화됨을 의미합니다.

SnapMirror 글로벌 제한은 동기화 상태에서의 SnapMirror 동기식 관계에는 영향을 미치지 않습니다. 그러나 초기화 작업과 같은 비동기 전송 단계를 수행하거나 동기화 중단 이벤트 후에 스로틀이 SnapMirror 동기식 관계에 영향을 줍니다. 따라서 SnapMirror 동기식 관계에서 글로벌 제한을 설정하지 않는 것이 좋습니다.

단계

1. 글로벌 제한 활성화:

   'options-option-name replication.throttle.enable on|off'

   다음 예에서는 "cluster_dst"에서 SnapMirror 글로벌 제한을 활성화하는 방법을 보여 줍니다.

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. 대상 클러스터에서 들어오는 전송에 사용되는 최대 총 대역폭을 지정합니다.

   `options -option-name replication.throttle.incoming.max_kbs <KBps>`

   권장되는 최소 스로틀 대역폭은 4kbps(초당 킬로바이트)이며 최대 초당 최대 2TB입니다(Tbps). 이 옵션의 기본값은 입니다 `unlimited`. 즉, 사용된 총 대역폭에 대한 제한이 없습니다.

   다음 예는 들어오는 전송에 사용되는 최대 총 대역폭을 100Mbps(초당 메가비트)로 설정하는 방법을 보여줍니다.

   ```
   cluster_dst::> options -option-name
   replication.throttle.incoming.max_kbs 12500
   ```

   초당 100메가비트(Mbps) = 12500KB/초(kbps)

3. 소스 클러스터에서 보내는 전송에 사용되는 최대 총 대역폭을 지정합니다.

   `options -option-name replication.throttle.outgoing.max_kbs <KBps>`

   권장되는 최소 스로틀 대역폭은 4kbps이고 최대 스로틀 대역폭은 2Tbps입니다. 이 옵션의 기본값은 입니다 `unlimited`. 즉, 사용된 총 대역폭에 대한 제한이 없습니다. 매개 변수 값은 초당 킬로바이트(kbps)입니다.

   다음 예에서는 송신 전송에 사용되는 최대 총 대역폭을 100Mbps로 설정하는 방법을 보여 줍니다.

```
cluster_src::> options -option-name
replication.throttle.outgoing.max_kbs 12500
```

SnapMirror SVM 복제 관리

ONTAP SnapMirror SVM 복제에 대해 알아보십시오

SnapMirror를 사용하여 SVM 간에 데이터 보호 관계를 생성할 수 있습니다. 이러한 유형의 데이터 보호 관계에서 NFS 엑스포트, SMB 공유에서 RBAC에 이르는 SVM 구성의 전체 또는 일부를 복제할 뿐만 아니라 SVM이 소유한 볼륨의 데이터도 복제됩니다.

지원되는 관계 유형

데이터를 지원하는 SVM만 복제할 수 있습니다. 지원되는 데이터 보호 관계 유형은 다음과 같습니다.

- _SnapMirror DR, _ 이 경우 일반적으로 대상에 현재 소스에 있는 스냅샷만 포함됩니다.

  ONTAP 9.9.1부터 이 동작은 미러 볼트 정책을 사용할 때 변경됩니다. ONTAP 9.9.1부터 소스와 대상에 다른 스냅샷 정책을 생성할 수 있으며, 소스의 스냅샷이 대상의 스냅샷을 덮어쓰지 않습니다.

  - 정상적인 예약 작업, 업데이트 및 재동기화 중에 소스에서 타겟으로 덮어써지지 않습니다
  - 분리 작업 중에는 삭제되지 않습니다.
  - 플립 재동기화 작업 중에는 삭제되지 않습니다.
    ONTAP 9.9.1 이상을 사용하여 미러 소산 정책을 사용하여 SVM 재해 관계를 구성하면 정책은 다음과 같이 작동합니다.
  - 소스의 사용자 정의 스냅샷 정책은 대상에 복제되지 않습니다.
  - 시스템 정의 스냅샷 정책은 대상에 복제되지 않습니다.
  - 사용자 및 시스템 정의 스냅샷 정책과의 볼륨 연결은 대상에 복제되지 않습니다. SVM.
- _SnapMirror 통합 복제_는 대상이 DR과 장기 보존을 위해 구성됩니다.

SnapMirror 통합 복제에 대한 자세한 내용은 을 참조하십시오 "SnapMirror 통합 복제 기본 사항".

복제 정책의 _policy type_은 이 정책이 지원하는 관계 유형을 결정합니다. 다음 표에는 사용 가능한 정책 유형이 나와 있습니다.

정책 유형입니다	관계 유형
비동기식 - 미러	SnapMirror DR
대칭 복사 - 볼트	통합 복제

XDP는 ONTAP 9.4에서 SVM 복제 기본값으로 DP를 대체합니다

ONTAP 9.4부터 SVM 데이터 보호 관계는 기본적으로 XDP 모드로 설정됩니다. SVM 데이터 보호 관계는 ONTAP 9.3 및 이전 버전에서 DP 모드로 계속 기본값입니다.

기존 관계는 XDP 기본값의 영향을 받지 않습니다. 관계가 이미 DP 유형인 경우 DP 유형이 됩니다. 다음 표에서는 예상할 수 있는 동작을 보여 줍니다.

지정하는 경우…	유형은…	기본 정책(정책을 지정하지 않은 경우)은…
DP	XDP	MirrorAllSnapshots(SnapMirror DR)
아무것도 없습니다	XDP	MirrorAllSnapshots(SnapMirror DR)
XDP	XDP	MirrorAndVault(통합 복제)

DP 관계를 XDP 관계로 변환하는 방법과 기타 세부 정보는 다음에서 확인할 수 있습니다"기존 ONTAP DP 유형 관계를 XDP로 변환합니다".

> SVM 복제에서는 버전에 상관없이 지원되지 않습니다. SVM 재해 복구 구성에서 페일오버 및 페일백 작업을 지원하려면 타겟 SVM이 소스 SVM 클러스터와 동일한 ONTAP 버전을 실행 중인 클러스터에 있어야 합니다.

"SnapMirror 관계에 대한 호환 ONTAP 버전"

SVM 구성을 복제하는 방법

SVM 복제 관계의 내용은 다음 필드의 상호 작용에 의해 결정됩니다.

- 'napMirror create' 명령의 '-identity-preserve true' 옵션은 전체 SVM 구성을 복제합니다.

  를 클릭합니다 `-identity-preserve false` 옵션은 SVM의 볼륨, 인증 및 권한 부여 구성과 에 나와 있는 프로토콜 및 이름 서비스 설정만 복제합니다 "SVM 재해 복구 관계에 복제된 구성".

- 'napMirror policy create' 명령의 '-discard-configs network' 옵션은 소스 및 대상 SVM이 서로 다른 서브넷에 있는 경우에 사용하기 위해 SVM 복제에서 LIF 및 관련 네트워크 설정을 제외합니다.
- 볼륨 수정 명령의 '-vserver-dr-protection protected' 옵션은 SVM 복제에서 지정된 볼륨을 제외합니다.

그렇지 않으면 SVM 복제가 볼륨 복제와 거의 동일합니다. 볼륨 복제에 사용하는 것과 동일한 워크플로우를 SVM 복제에 사용할 수 있습니다.

지원 세부 정보

다음 표에서는 SnapMirror SVM 복제에 대한 지원 정보를 보여 줍니다.

리소스 또는 기능	지원 세부 정보

배포 유형	• 단일 소스에서 단일 대상으로 • ONTAP 9.4, 팬아웃. 두 개의 대상으로만 팬아웃할 수 있습니다. 기본적으로 소스 SVM당 하나의 ID만 보존되며 진정한 관계는 유지됩니다.
관계 유형	• SnapMirror 재해 복구 • SnapMirror 통합 복제
복제 범위	인터클러스터 전용 동일한 클러스터에서 SVM을 복제할 수 없습니다.
자율 랜섬웨어 보호	• ONTAP 9.12.1부터 지원됩니다. 자세한 내용은 을 "자율 랜섬웨어 보호"참조하십시오.
정합성 보장 그룹 비동기식 지원	ONTAP 9.14.1부터 일관성 그룹이 있을 경우 최대 32개의 SVM 재해 복구 관계가 지원됩니다. 을 참조하십시오 "일관성 그룹 보호" 및 "정합성 보장 그룹 제한" 를 참조하십시오.
FabricPool	ONTAP 9.6부터 FabricPool에서 SnapMirror SVM 복제가 지원됩니다. SVM DR 관계인 경우 소스 및 타겟 볼륨에서 FabricPool 애그리게이트를 사용할 필요가 없지만 동일한 계층화 정책을 사용해야 합니다. ONTAP 9.12.1부터 SnapMirror SVM 복제는 FabricPool 및 FlexGroup 볼륨이 함께 작동하는 경우에 지원됩니다. 9.12.1 이전에는 이러한 기능 중 두 가지가 함께 작동했지만 세 가지 기능이 모두 함께 작동되지는 않았습니다.

MetroCluster	ONTAP 9.11.1부터 MetroCluster 구성 내 SVM 재해 복구 관계의 양측이 추가 SVM 재해 복구 구성의 소스 역할을 할 수 있습니다. ONTAP 9.5부터 MetroCluster 구성에서 SnapMirror SVM 복제가 지원됩니다. • ONTAP 9.10.X 이전 릴리즈에서는 MetroCluster 구성이 SVM 재해 복구 관계의 대상이 될 수 없습니다. • ONTAP 9.10.1 이상 릴리즈에서 MetroCluster 구성은 마이그레이션 목적으로만 SVM 재해 복구 관계의 대상이 될 수 있으며 에 설명된 모든 필수 요구사항을 충족해야 합니다 "TR-4966: SVM을 MetroCluster 솔루션으로 마이그레이션". • MetroCluster 구성 내의 활성 SVM만 SVM 재해 복구 관계의 소스가 될 수 있습니다. 전환 전 동기화 소스 SVM이나 전환 후 동기화 대상 SVM이 소스가 될 수 있습니다. • MetroCluster 구성이 안정적인 상태인 경우 볼륨이 온라인 상태가 아니기 때문에 MetroCluster 동기화 대상 SVM이 SVM 재해 복구 관계의 소스가 될 수 없습니다. • 동기식 소스 SVM이 SVM 재해 복구 관계의 소스인 경우 소스 SVM 재해 복구 관계 정보가 MetroCluster 파트너에게 복제됩니다. • 스위치오버 및 스위치백 프로세스 중에 SVM 재해 복구 대상으로의 복제가 실패할 수 있습니다. 그러나 스위치오버 또는 스위치백 프로세스가 완료된 후에는 다음 SVM 재해 복구 예정된 업데이트가 성공적으로 수행됩니다.
일관성 그룹	ONTAP 9.14.1부터 지원됩니다. 자세한 내용은 을 참조하십시오 일관성 그룹 보호.
ONTAP S3	SVM 재해 복구는 지원되지 않습니다.
SnapMirror Synchronous	SVM 재해 복구는 지원되지 않습니다.
버전 독립적	지원되지 않습니다.

볼륨 암호화	• 소스의 암호화된 볼륨은 대상에서 암호화됩니다. • 온보드 키 관리자 또는 KMIP 서버를 타겟에 구성해야 합니다. • 대상에서 새 암호화 키가 생성됩니다. • 대상에 volume.encryption을 지원하는 노드가 없으면 복제가 성공하지만 대상 볼륨은 암호화되지 않습니다.

SVM 재해 복구 관계에 복제된 구성

다음 표에서는 의 상호 작용을 보여 줍니다 `snapmirror create -identity-preserve` 옵션과 `snapmirror policy create -discard-configs network` 옵션:

구성이 복제되었습니다		'-**identity**-**preserve true**'		'-**identity**-**preserve false**'
		'-discard-configs 네트워크'가 설정되지 않은 정책 *	* '-discard-configs 네트워크'가 설정된 정책 *	
네트워크	NAS LIF	예	아니요	아니요
LIF Kerberos 구성	예	아니요	아니요	SAN LIF
아니요	아니요	아니요	방화벽 정책	예
예	아니요	서비스 정책	예	예
아니요	루트	예	아니요	아니요
브로드캐스트 도메인	아니요	아니요	아니요	서브넷
아니요	아니요	아니요	IPspace	아니요
아니요	아니요	중소기업	SMB 서버	예
예	아니요	로컬 그룹 및 로컬 사용자	예	예
예	권한	예	예	예
섀도 복사본	예	예	예	BranchCache입니다
예	예	예	서버 옵션	예

예	예	서버 보안	예	예
아니요	더 높여 줍니다	예	예	예
symlink	예	예	예	FPolicy 정책, Fsecurity 정책 및 Fsecurity NTFS입니다
예	예	예	이름 매핑 및 그룹 매핑	예
예	예	감사 정보	예	예
예	NFS 를 참조하십시오	엑스포트 정책	예	예
아니요	엑스포트 정책 규칙	예	예	아니요
NFS 서버	예	예	아니요	RBAC
보안 인증서	예	예	아니요	로그인 사용자, 공개 키, 역할 및 역할 구성
예	예	예	SSL	예
예	아니요	네임 서비스	DNS 및 DNS 호스트	예
예	아니요	Unix 사용자 및 UNIX 그룹	예	예
예	Kerberos 영역 및 Kerberos 키 블록	예	예	아니요
LDAP 및 LDAP 클라이언트	예	예	아니요	넷그룹
예	예	아니요	NIS를 선택합니다	예
예	아니요	웹 및 웹 액세스	예	예
아니요	볼륨	오브젝트	예	예
예	스냅샷 및 스냅샷 정책	예	예	예

자동 삭제 정책	아니요	아니요	아니요	효율성 정책
예	예	예	할당량 정책 및 할당량 정책 규칙입니다	예
예	예	복구 대기열	예	예
예	루트 볼륨	네임스페이스	예	예
예	사용자 데이터	아니요	아니요	아니요
Qtree	아니요	아니요	아니요	할당량
아니요	아니요	아니요	파일 레벨 QoS	아니요
아니요	아니요	속성: 루트 볼륨 상태, 공간 보장, 크기, 크기 조정 및 총 파일 수입니다	아니요	아니요
아니요	스토리지 QoS	QoS 정책 그룹	예	예
예	파이버 채널(FC)	아니요	아니요	아니요
iSCSI	아니요	아니요	아니요	LUN을 클릭합니다
오브젝트	예	예	예	Igroup
아니요	아니요	아니요	포트 세트	아니요
아니요	아니요	일련 번호	아니요	아니요
아니요	SNMP를 선택합니다	V3 사용자	예	예

SVM 재해 복구 스토리지 제한

다음 표는 스토리지 오브젝트당 지원되는 최대 볼륨 수 및 SVM 재해 복구 관계의 권장 최대 수를 보여줍니다. 제한 사항은 플랫폼에 따라 다를 수 있습니다. 을 참조하십시오 "Hardware Universe" 특정 구성에 대한 제한 사항을 알아봅니다.

스토리지 객체	제한
SVM	300개의 유연한 볼륨

HA 쌍	1,000개의 유연한 볼륨
클러스터	128개의 SVM 재해 관계

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"

SVM 구성 복제

ONTAP SnapMirror SVM 복제 워크플로우

SnapMirror SVM 복제에는 대상 SVM 생성, 복제 작업 일정 생성, SnapMirror 관계 생성 및 초기화가 포함됩니다.

요구 사항에 가장 적합한 복제 워크플로우를 결정해야 합니다.

- "전체 SVM 구성을 복제합니다"
- "SVM 복제에서 LIF 및 관련 네트워크 설정을 제외합니다"
- "SVM 구성의 Exlude 네트워크, 네임 서비스 및 기타 설정"

볼륨을 **ONTAP SnapMirror** 대상 **SVM**에 배치하는 기준입니다

소스 SVM에서 타겟 SVM으로 볼륨을 복제할 때 애그리게이트 선택 기준을 파악하는 것이 중요합니다.

애그리게이트는 다음 기준에 따라 선택됩니다.

- 볼륨은 항상 비루트 애그리게이트에 배치되어 있습니다.
- 사용 가능한 여유 공간과 애그리게이트에 이미 호스팅되는 볼륨의 수를 기준으로 비 루트 애그리게이트를 선택합니다.

  여유 공간이 더 많은 애그리게이트를 사용하고 더 적은 볼륨을 우선 순위로 지정합니다. 가장 높은 우선순위를 가진 애그리게이트는 선택됩니다.

- FabricPool 애그리게이트에서 소스 볼륨은 동일한 계층화-정책을 사용하여 대상의 FabricPool 애그리게이트에 배치됩니다.
- 소스 SVM의 볼륨이 Flash Pool 애그리게이트에 있는 경우, 그러한 애그리게이트와 사용 가능한 공간이 충분할 경우, 타겟 SVM의 Flash Pool 애그리게이트에 볼륨을 배치하면 됩니다.
- 복제된 볼륨의 '-space-보증' 옵션이 'volume'으로 설정된 경우 사용 가능한 공간이 볼륨 크기보다 큰 애그리게이트만 고려됩니다.
- 소스 볼륨 크기에 따라 복제 중에 타겟 SVM에서 볼륨 크기가 자동으로 커집니다.

  대상 SVM에서 크기를 사전 예약하려면 볼륨 크기를 조정해야 합니다. 소스 SVM을 기반으로 하는 타겟 SVM에서 볼륨 크기가 자동으로 축소되지 않습니다.

한 Aggregate에서 다른 Aggregate로 볼륨을 이동할 경우, 대상 SVM에서 'volume move' 명령을 사용할 수 있습니다.

전체 **ONTAP SVM** 구성을 복제합니다

SVM DR(재해 복구) 관계를 생성하여 하나의 SVM 구성을 다른 SVM 구성으로 복제할 수 있습니다. 운영 사이트에 재해가 발생하면 대상 SVM을 빠르게 활성화할 수 있습니다.

시작하기 전에

소스 및 타겟 클러스터와 SVM을 피어링해야 합니다. 자세한 내용은 을 참조하십시오 "클러스터 피어 관계를 생성합니다" 및 "SVM 인터클러스터 피어 관계를 생성합니다".

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

이 작업에 대해

이 워크플로우에서는 이미 기본 정책 또는 사용자 지정 복제 정책을 사용하고 있다고 가정합니다.

ONTAP 9.9.1부터 미러 소산 정책을 사용할 때 소스 및 대상 SVM에 다른 스냅샷 정책을 생성할 수 있으며 대상의 스냅샷은 소스의 스냅샷으로 덮어쓰지 않습니다. 자세한 내용은 을 "SnapMirror SVM 복제 이해"참조하십시오.

대상에서 이 절차를 완료합니다. 예를 들어 소스 스토리지 VM에 SMB가 구성된 경우 새 보호 정책을 생성해야 하는 경우 정책을 생성하고 * Identity preserve * 옵션을 사용해야 합니다. 자세한 내용은 을 "사용자 지정 데이터 보호 정책을 생성합니다"참조하십시오.

단계

이 작업은 System Manager 또는 ONTAP CLI에서 수행할 수 있습니다.

시스템 관리자

1. 대상 클러스터에서 * 보호 > 관계 * 를 클릭합니다.
2. 관계 * 에서 * 보호 * 를 클릭하고 * 스토리지 VM(DR) * 를 선택합니다.
3. 보호 정책을 선택합니다. 맞춤형 보호 정책을 생성한 경우 해당 정책을 선택한 다음 복제할 소스 클러스터와 스토리지 VM을 선택합니다. 새 스토리지 VM 이름을 입력하여 새 대상 스토리지 VM을 생성할 수도 있습니다.
4. 필요한 경우 대상 설정을 변경하여 ID 보존을 재정의하고 네트워크 인터페이스 및 프로토콜을 포함하거나 제외합니다.
5. 저장 * 을 클릭합니다.

CLI를 참조하십시오

1. 대상 SVM 생성:

```
vserver create -vserver <SVM_name> -subtype dp-destination
```

SVM 이름은 소스 및 타겟 클러스터 전체에서 고유해야 합니다.

다음 예에서는 sm_backup이라는 대상 SVM을 생성합니다.

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-
destination
```

에 대한 자세한 내용은 `vserver create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 대상 클러스터에서 'vserver peer create' 명령을 사용하여 SVM 피어 관계를 생성합니다.

자세한 내용은 을 참조하십시오 "SVM 인터클러스터 피어 관계를 생성합니다".

에 대한 자세한 내용은 `vserver peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 복제 작업 스케줄 생성:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

월-일-일-주-시-시간의 경우 월, 일, 시 순으로 모두 작업을 실행하도록 지정할 수 있습니다.

> SVM SnapMirror 관계에서 FlexVol 볼륨의 최소 지원 일정(RPO)은 15분입니다. SVM SnapMirror 관계에서 FlexGroup 볼륨의 최소 지원 일정(RPO)은 30분입니다.

다음 예에서는 토요일 오전 3시에 실행되는 my_weekly라는 작업 일정을 생성합니다.

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
saturday -hour 3 -minute 0
```

에 대한 자세한 내용은 `job schedule cron create` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 타겟 SVM 또는 타겟 클러스터에서 복제 관계를 생성합니다.

```
snapmirror create -source-path <SVM_name>: -destination-path
<SVM_name>: -type <DP|XDP> -schedule <schedule> -policy <policy>
-identity-preserve true
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다.

다음 예에서는 기본 'MirorAllSnapshots' 정책을 사용하여 SnapMirror DR 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy
MirrorAllSnapshots -identity-preserve true
```

다음 예에서는 기본 MirorAndVault 정책을 사용하여 통합 복제 관계를 생성합니다.

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

정책 유형인 '비동기 미러'를 사용하여 사용자 지정 정책을 생성했다고 가정하면 다음 예에서는 SnapMirror DR 관계가 생성됩니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_mirrored
-identity-preserve true
```

정책 유형 'Mirror-vault'로 사용자 지정 정책을 생성했다고 가정하면 다음 예에서는 통합 복제 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_unified
-identity-preserve true
```

에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 대상 SVM 중지:

```
vserver stop -vserver <SVM_name>
```

다음 예에서는 svm_backup이라는 대상 SVM을 중지합니다.

```
cluster_dst::> vserver stop -vserver svm_backup
```

에 대한 자세한 내용은 `vserver stop` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 대상 SVM 또는 대상 클러스터에서 SVM 복제 관계를 초기화합니다.

```
snapmirror initialize -source-path <SVM_name>: -destination-path
<SVM_name>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다.

다음 예에서는 소스 SVM, svm1, 대상 SVM, svm_backup 간의 관계를 초기화합니다.

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror SVM 복제에서 **LIF** 및 관련 네트워크 설정을 제외합니다

소스 및 타겟 SVM이 서로 다른 서브넷에 있는 경우 '스냅샷 정책 생성' 명령의 '-discard-configs network' 옵션을 사용하여 SVM 복제에서 LIF 및 관련 네트워크 설정을 제외할 수 있습니다.

시작하기 전에

소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

자세한 내용은 을 참조하십시오 "클러스터 피어 관계를 생성합니다" 및 "SVM 인터클러스터 피어 관계를 생성합니다".

이 작업에 대해

SVM 복제 관계를 생성할 때 'napmirror create' 명령의 '-identity-preserve' 옵션을 'true'로 설정해야 합니다.

단계

1. 대상 SVM 생성:

'vserver create-vserver_SVM_-subtype DP-destination'

SVM 이름은 소스 및 타겟 클러스터 전체에서 고유해야 합니다.

다음 예에서는 sm_backup이라는 대상 SVM을 생성합니다.

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. 대상 클러스터에서 'vserver peer create' 명령을 사용하여 SVM 피어 관계를 생성합니다.

   자세한 내용은 을 참조하십시오 "SVM 인터클러스터 피어 관계를 생성합니다".

   에 대한 자세한 내용은 `vserver peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 작업 일정 생성:

   "작업 일정 cron create-name_job_name_-month_month_-DayOfWeek_day_of_week_-day_day_of_month_-hour_hour_-minute_minute_"

   월-일-일-주-시-시간의 경우 월, 일, 시 순으로 모두 작업을 실행하도록 지정할 수 있습니다.

   > SVM SnapMirror 관계에서 FlexVol 볼륨의 최소 지원 일정(RPO)은 15분입니다. SVM SnapMirror 관계에서 FlexGroup 볼륨의 최소 지원 일정(RPO)은 30분입니다.

   다음 예에서는 토요일 오전 3시에 실행되는 my_weekly라는 작업 일정을 생성합니다.

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. 사용자 지정 복제 정책 생성:

   '스냅샷 정책 생성 - vserver_SVM_-policy_policy_-type async-mirror|vault|mirror-vault-comment_comment_-transfer_rs-priority low|normal-is-network-compression-enabled true|false-discard-configs network'

   다음 예제에서는 LIF를 제외한 SnapMirror DR에 대한 사용자 지정 복제 정책을 생성합니다.

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_exclude_LIFs -type async-mirror -discard-configs network
```

   다음 예에서는 LIF를 제외한 유니파이드 복제에 대한 맞춤형 복제 정책을 생성합니다.

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

   > 향후 페일오버 및 페일백 시나리오를 지원하기 위해 소스 클러스터에 동일한 맞춤형 SnapMirror 정책을 생성하는 것을 고려해 보십시오.

에 대한 자세한 내용은 `snapmirror policy create` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 대상 SVM 또는 대상 클러스터에서 다음 명령을 실행하여 복제 관계를 생성합니다.

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve true|false -discard
-configs true|false
```

> '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예제에서는 LIF를 제외한 SnapMirror DR 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_weekly -policy DR_exclude_LIFs
-identity-preserve true
```

다음 예제에서는 LIF를 제외한 SnapMirror 통합 복제 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_weekly -policy unified_exclude_LIFs
-identity-preserve true -discard-configs true
```

에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 대상 SVM 중지:

'vserver stop'

'_SVM 이름 _'

다음 예에서는 svm_backup이라는 대상 SVM을 중지합니다.

```
cluster_dst::> vserver stop -vserver svm_backup
```

7. 대상 SVM 또는 대상 클러스터에서 복제 관계를 초기화합니다.

'스냅샷 초기화-소스-경로_SVM_:-대상-경로_SVM_:'

다음 예에서는 소스 'svm1'과 대상 'svm_backup' 간의 관계를 초기화합니다.

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

재해가 발생할 경우 데이터 액세스를 위해 대상 SVM에서 네트워크 및 프로토콜을 구성해야 합니다.

관련 정보

- "SnapMirror 생성"
- "SnapMirror 초기화"
- "스냅미러 정책 생성"

ONTAP를 통한 **SVM** 복제에서 네트워크, 네임 서비스 및 기타 설정을 제외합니다

타겟 SVM과의 충돌 또는 구성 차이를 방지하기 위해 SVM 복제 관계에서 네트워크, 네임 서비스 및 기타 설정을 제외할 수 있습니다.

스냅샷 생성 명령의 '-identity-preserve false' 옵션을 사용하여 SVM의 볼륨 및 보안 구성만 복제할 수 있습니다. 일부 프로토콜 및 이름 서비스 설정도 보존됩니다.

이 작업에 대해

보존된 프로토콜 및 이름 서비스 설정 목록은 를 참조하십시오 "SVM DR 관계에 복제된 구성".

시작하기 전에

소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

자세한 내용은 을 참조하십시오 "클러스터 피어 관계를 생성합니다" 및 "SVM 인터클러스터 피어 관계를 생성합니다".

단계

1. 대상 SVM 생성:

   'vserver create-vserver_SVM_-subtype DP-destination'

   SVM 이름은 소스 및 타겟 클러스터 전체에서 고유해야 합니다.

   다음 예에서는 sm_backup이라는 대상 SVM을 생성합니다.

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. 대상 클러스터에서 'vserver peer create' 명령을 사용하여 SVM 피어 관계를 생성합니다.

   자세한 내용은 을 참조하십시오 "SVM 인터클러스터 피어 관계를 생성합니다".

   에 대한 자세한 내용은 `vserver peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 복제 작업 스케줄 생성:

   "작업 일정 cron create-name_job_name_-month_month_-DayOfWeek_day_of_week_-day_day_of_month_-hour_hour_-minute_minute_"

   월-일-일-주-시-시간의 경우 월, 일, 시 순으로 모두 작업을 실행하도록 지정할 수 있습니다.

SVM SnapMirror 관계에서 FlexVol 볼륨의 최소 지원 일정(RPO)은 15분입니다. SVM SnapMirror 관계에서 FlexGroup 볼륨의 최소 지원 일정(RPO)은 30분입니다.

다음 예에서는 토요일 오전 3시에 실행되는 my_weekly라는 작업 일정을 생성합니다.

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. 네트워크, 이름 서비스 및 기타 구성 설정을 제외한 복제 관계를 생성합니다.

'sapmirror create-source-path_SVM_:-destination-path_SVM_:-type DP|XDP-schedule schedule -policy -identity -preserve false'

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오. 이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 기본 'MirorAllSnapshots' 정책을 사용하여 SnapMirror DR 관계를 생성합니다. 네트워크, 네임 서비스 및 기타 구성 설정은 SVM 복제에서 제외됩니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve false
```

다음 예제에서는 기본 MirorAndVault 정책을 사용하여 통합 복제 관계를 만듭니다. 네트워크, 이름 서비스 및 기타 구성 설정은 관계가 제외됩니다.

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

정책 유형인 '비동기 미러'를 사용하여 사용자 지정 정책을 생성했다고 가정하면 다음 예에서는 SnapMirror DR 관계가 생성됩니다. 네트워크, 네임 서비스 및 기타 구성 설정은 SVM 복제에서 제외됩니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

정책 유형 'Mirror-vault'로 사용자 지정 정책을 생성했다고 가정하면 다음 예에서는 통합 복제 관계를 생성합니다. 네트워크, 네임 서비스 및 기타 구성 설정은 SVM 복제에서 제외됩니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 대상 SVM 중지:

   'vserver stop'

   '_SVM 이름 _'

   다음 예는 dv1이라는 대상 SVM을 중지합니다.

   ```
   destination_cluster::> vserver stop -vserver dvs1
   ```

6. SMB를 사용하는 경우 SMB 서버도 구성해야 합니다.

   을 참조하십시오 "SMB 전용: SMB 서버 생성".

7. 대상 SVM 또는 대상 클러스터에서 SVM 복제 관계를 초기화합니다.

   '스냅샷 초기화-소스-경로_SVM_이름_:-대상-경로_SVM_이름_:'

   에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

재해가 발생할 경우 데이터 액세스를 위해 대상 SVM에서 네트워크 및 프로토콜을 구성해야 합니다.

ONTAP SnapMirror SVM DR 관계에 사용할 로컬 계층 지정

재해 복구 SVM이 생성된 후 명령과 함께 옵션을 `vserver modify` 사용하여 SVM DR 타겟 볼륨을 호스팅하는 데 사용되는 로컬 계층을 제한할 수 `aggr-list` 있습니다.

단계

1. 대상 SVM 생성:

   'vserver create-vserver_SVM_-subtype DP-destination'

2. 재해 복구 SVM의 집계 목록을 수정하여 재해 복구 SVM 볼륨을 호스팅하는 데 사용되는 로컬 계층을 제한합니다.

   'cluster_dest::> vserver modify -vserver_SVM_-aggr-list <comma-separated-list>'

DR 관계에서 **ONTAP SnapMirror** 대상 **SVM**에 대한 **SMB** 서버를 생성합니다

소스 SVM에 SMB 구성이 있으며 을 로 `false` 설정하도록 선택한 경우 `identity-`

preserve, 대상 SVM에 대한 SMB 서버를 생성해야 합니다. SnapMirror 관계를 초기화할 때 공유와 같은 일부 SMB 구성에는 SMB 서버가 필요합니다.

단계

1. 명령을 사용하여 타겟 SVM을 vserver start 시작합니다.

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

에 대한 자세한 내용은 vserver start "ONTAP 명령 참조입니다"을 참조하십시오.

2. vserver show 명령을 사용하여 대상 SVM이 "Running" 상태이고 하위 유형이 dp-destination인지 확인하십시오.

```
destination_cluster::> vserver show
                                  Admin      Operational Root
Vserver  Type    Subtype          State      State       Volume
Aggregate
-------- ------- ----------       ---------- ----------- ----------
----------
dvs1     data    dp-destination   running    running       -         -
```

에 대한 자세한 내용은 vserver show "ONTAP 명령 참조입니다"을 참조하십시오.

3. 네트워크 인터페이스 생성 명령을 사용하여 LIF를 생성합니다.

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101  -address 192.0.2.128 -netmask 255.255.255.128
```

에 대한 자세한 내용은 network interface create "ONTAP 명령 참조입니다"을 참조하십시오.

4. network route create 명령을 사용하여 route를 생성한다.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"네트워크 관리"

에 대한 자세한 내용은 network route create "ONTAP 명령 참조입니다"을 참조하십시오.

5. 'vserver services dns create' 명령을 사용하여 DNS를 구성합니다.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

에 대한 자세한 내용은 `vserver services dns create` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 'vserver cifs domain preferred-dc add' 명령을 사용하여 기본 도메인 컨트롤러를 추가합니다.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

에 대한 자세한 내용은 `vserver cifs domain preferred-dc add` "ONTAP 명령 참조입니다"을 참조하십시오.

7. 'vserver cifs create' 명령을 사용하여 SMB 서버를 생성합니다.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

에 대한 자세한 내용은 `vserver cifs create` "ONTAP 명령 참조입니다"을 참조하십시오.

8. 'vserver stop' 명령을 사용하여 대상 SVM을 중지합니다.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

에 대한 자세한 내용은 `vserver stop` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror SVM DR 관계에서 볼륨을 제외합니다

기본적으로 소스 SVM의 모든 RW 데이터 볼륨이 복제됩니다. 소스 SVM의 모든 볼륨을 보호하지 않으려는 경우 '볼륨 수정' 명령의 '-vserver-dr-protection protected' 옵션을 사용하여 SVM 복제에서 볼륨을 제외할 수 있습니다.

단계

1. SVM 복제에서 볼륨 제외:

   'volume modify -vserver_SVM_-volume_volume_-vserver-dr-protection protected'

   에 대한 자세한 내용은 `volume modify` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 SVM 복제에서 볼륨 'VolA_src'를 제외합니다.

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection unprotected
```

나중에 원래 제외된 SVM 복제에 볼륨을 포함하려면 다음 명령을 실행합니다.

'볼륨 수정 - vserver_SVM_-volume_volume_-vserver-dr-protection protected

다음 예에서는 SVM 복제의 볼륨 VolA_src를 포함합니다.

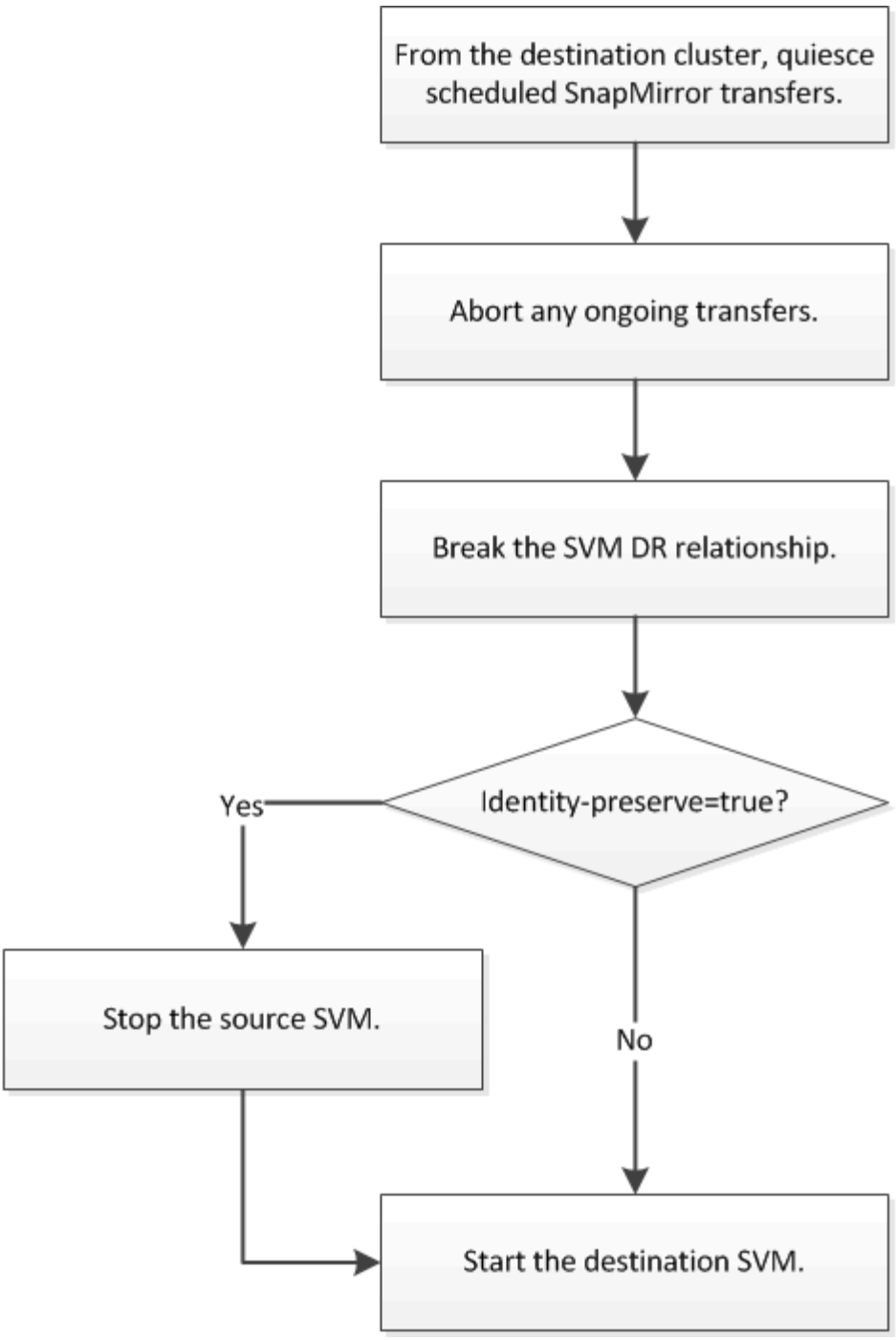
```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection protected
```

2. 에 설명된 대로 SVM 복제 관계를 생성하고 초기화합니다 "전체 SVM 구성 복제".

SnapMirror SVM DR 대상에서 데이터 제공

ONTAP SnapMirror SVM 재해 복구 워크플로우

재해를 복구하고 타겟 SVM에서 데이터를 제공하려면 타겟 SVM을 활성화해야 합니다. 타겟 SVM을 활성화하려면 예약된 SnapMirror 전송을 중지하고, 지속적인 SnapMirror 전송을 중단하고, 복제 관계를 중단하고, 소스 SVM을 중지하고, 타겟 SVM을 시작해야 합니다.



ONTAP SnapMirror SVM 대상 볼륨을 쓰기 가능으로 구성합니다

클라이언트에 데이터를 제공하려면 SVM 대상 볼륨을 쓰기 가능하게 해야 합니다.

이 절차는 볼륨 복제 절차와 크게 동일하지만 한 가지 예외가 있습니다. SVM 복제 관계를 생성할 때 를 설정한 `-identity-preserve true` 경우, 대상 SVM을 활성화하기 전에 소스 SVM을 중지해야 합니다.

이 작업에 대해

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

재해 복구 시나리오에서는 소스 SVM과 해당 데이터에 액세스할 수 없고 마지막 재동기화 이후의 업데이트가 불량하거나 손상되었을 수 있으므로 소스 SVM에서 재해 복구 대상 SVM으로 SnapMirror 업데이트를 수행할 수 없습니다.

ONTAP 9.8부터 System Manager를 사용하여 재해 발생 후 대상 스토리지 VM을 활성화할 수 있습니다. 대상 스토리지 VM을 활성화하면 SVM 대상 볼륨을 쓸 수 있고 데이터를 클라이언트에 제공할 수 있습니다.

단계

이 작업은 System Manager 또는 ONTAP CLI에서 수행할 수 있습니다.

시스템 관리자

1. 소스 클러스터에 액세스할 수 있는 경우 SVM이 중지되었는지 확인합니다. * 스토리지 > 스토리지 VM * 으로 이동하고 SVM을 위한 * 상태 * 열을 확인합니다.
2. 소스 SVM 상태가 "실행 중"인 경우 중지하십시오. 를 선택하고 ⋮ * 중지 * 를 선택하십시오.
3. 대상 클러스터에서 원하는 보호 관계를 찾습니다. * 보호 > 관계 * 로 이동합니다.
4. 원하는 소스 스토리지 VM 이름 위로 마우스를 가져가 를 클릭하고 ⋮* 대상 스토리지 VM 활성화 * 를 선택합니다.
5. 대상 스토리지 VM 활성화 * 창에서 * 대상 스토리지 VM 활성화 및 관계 해제 * 를 선택합니다.
6. Activate * 를 클릭합니다.

CLI를 참조하십시오

1. 대상 SVM 또는 대상 클러스터에서 SVM을 중지하여 대상으로 예약된 전송을 중지합니다.

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

ⓘ '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 소스 SVM의 vm1과 대상 SVM의 vm_backup 간의 예약된 전송을 중지합니다.

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination
-path svm_backup:
```

에 대한 자세한 내용은 `snapmirror quiesce` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 대상 SVM 또는 대상 클러스터에서 목적지로의 진행 중인 전송을 중지합니다.

```
snapmirror abort -source-path <SVM>: -destination-path <SVM>:
```

ⓘ '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 소스 SVM의 vm1과 대상 SVM의 vm_backup 간의 지속적인 전송을 중지합니다.

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path
svm_backup:
```

에 대한 자세한 내용은 `snapmirror abort` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 타겟 SVM 또는 타겟 클러스터에서 복제 관계를 중단하십시오.

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 소스 SVM의 vm1과 대상 SVM의 vm_backup 간의 관계를 나눕니다.

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

4. SVM 복제 관계를 생성할 때 '-identity-preserve true'를 설정하면 소스 SVM을 중지합니다.

```
vserver stop -vserver <SVM>
```

다음 예에서는 소스 SVM의 vm1'를 중지합니다.

```
cluster_src::> vserver stop svm1
```

5. 대상 SVM 시작:

```
vserver start -vserver <SVM>
```

다음 예에서는 대상 SVM의 VM_BACKUP을 시작합니다.

```
cluster_dst::> vserver start svm_backup
```

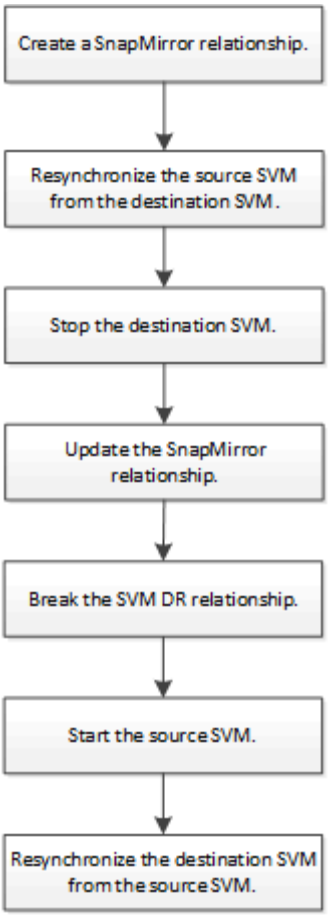
작업을 마친 후

에 설명된 대로 데이터 액세스를 위해 SVM 대상 볼륨을 구성합니다 "데이터 액세스를 위한 대상 볼륨을 구성합니다".

SnapMirror 소스 SVM을 재활성화합니다

ONTAP SnapMirror 소스 **SVM** 재활성화 워크플로우

재해 발생 후 소스 SVM이 있으면 SVM 재해 복구 관계를 재생성하여 재활성화하고 보호할 수 있습니다.



원래 **ONTAP SnapMirror** 소스 **SVM**을 다시 활성화합니다

대상에서 데이터를 더 이상 사용할 필요가 없을 경우 소스 및 타겟 SVM 간에 원래 데이터 보호 관계를 다시 설정할 수 있습니다. 이 절차는 볼륨 복제 절차와 크게 동일하지만 한 가지 예외가 있습니다. 소스 SVM을 다시 활성화하기 전에 타겟 SVM을 중지해야 합니다.

시작하기 전에

- 데이터를 제공하는 동안 대상 볼륨의 크기를 늘인 경우 소스 볼륨을 다시 활성화하기 전에 원본 소스 볼륨의 최대 크기 자동 크기 조정을 수동으로 늘려 충분히 성장할 수 있도록 해야 합니다.

"타겟 볼륨이 자동으로 증가하는 경우"

클러스터 관리자는 데이터 손실을 방지하기 위해 원래 소스 SVM을 다시 활성화하기 전에 클라이언트의 쓰기 작업을 일시 중지해야 합니다.

이 작업에 대해

ONTAP 9.11.1부터 `-quick-resync true` `snapmirror resync`SVM DR 관계의 역재동기화를 수행하는 동안 명령의 `CLI` 옵션을 사용하여 재해 복구 예행 연습 중에 재동기화 시간을 줄일 수 있습니다. 빠른 재동기화를 통해 데이터 웨어하우스 재구축 및 복원 작업을 바이패스하여 운영 상태로 돌아가는 데 걸리는 시간을 줄일 수 있습니다. 에 대한 자세한 내용은 `snapmirror resync` "ONTAP 명령 참조입니다"을 참조하십시오.

빠른 재동기화는 타겟 볼륨의 스토리지 효율성을 유지하지 않습니다. 빠른 재동기화를 설정하면 대상 볼륨에서 사용하는 볼륨 공간이 증가할 수 있습니다.

이 절차에서는 원본 소스 볼륨의 기준선이 온전한 것으로 가정합니다. 기준선이 변경되지 않은 경우 절차를 수행하기 전에 데이터를 제공하는 볼륨과 원본 소스 볼륨 간의 관계를 생성하고 초기화해야 합니다.

ONTAP 9.8부터 시스템 관리자를 사용하여 재해 발생 후 소스 스토리지 VM을 다시 활성화할 수 있습니다.

단계

이 작업은 시스템 관리자 또는 ONTAP CLI를 사용하여 수행할 수 있습니다.

시스템 관리자 **ONTAP 9.17.1** 이상

1. 대상 클러스터에서 원하는 보호 관계를 선택하려면 *보호 > 복제*를 클릭하십시오.
2. 소스 이름 위에 마우스 커서를 올려놓고 클릭하세요. ⋮그리고 *역방향 동기화*를 클릭하세요.
3. Reverse resync relationship * 창에서 * Reverse resync * 를 클릭합니다.

   해당 관계는 복제 테이블에서 사라지고 이제 원래 소스 클러스터에서 관리됩니다.

4. 원본 소스 클러스터에서 *보호 > 복제*를 클릭하고 상태가 *미러링됨*으로 표시되는지 확인하여 역방향 재동기화가 완료되었는지 확인합니다.
5. 원래 대상 클러스터에서 *클러스터 > 스토리지 VM*으로 이동합니다.
6. 스토리지 VM을 찾고, 스토리지 VM 이름 위에 마우스 커서를 올린 다음 클릭합니다. ⋮그리고 *정지*를 클릭하세요.
7. 저장소 **VM** 중지 창에서 *중지*를 클릭합니다.
8. 원본 클러스터에서 *보호 > 복제*로 이동하여 다시 활성화할 스토리지 VM을 찾고, 스토리지 VM 이름 위에 마우스 커서를 올려놓은 다음 클릭합니다. ⋮그런 다음 *대상 스토리지 VM 활성화*를 클릭합니다.
9. 대상 스토리지 **VM** 활성화 창에서 *대상 스토리지 VM을 활성화하고 연결을 해제*를 선택한 다음 *활성화*를 클릭합니다.
10. 복제 페이지로 돌아가면 스토리지 VM 이름 위에 마우스 커서를 다시 올려놓고 클릭하세요. ⋮그리고 *역방향 동기화*를 클릭하세요.

시스템 관리자 **ONTAP 9.16.1** 및 이전 버전

1. 대상 클러스터에서 원하는 보호 관계를 선택하려면 *보호 > 관계*를 클릭하십시오.
2. 소스 이름 위에 마우스 커서를 올려놓고 클릭하세요. ⋮그리고 *역방향 동기화*를 클릭하세요.
3. Reverse resync relationship * 창에서 * Reverse resync * 를 클릭합니다.

   해당 관계는 이제 원래 소스 클러스터에서 관리되므로 관계 테이블에서 사라집니다.

4. 원본 소스 클러스터에서 *보호 > 관계*를 클릭하고 상태가 *미러링됨*으로 표시되는지 확인하여 역방향 재동기화가 완료되었는지 확인합니다.
5. 원래 대상 클러스터에서 *스토리지 > 스토리지 VM*으로 이동합니다.
6. 스토리지 VM을 찾고, 스토리지 VM 이름 위에 마우스 커서를 올린 다음 클릭합니다. ⋮그리고 *정지*를 클릭하세요.
7. 저장소 **VM** 중지 창에서 *중지*를 클릭합니다.
8. 원본 클러스터에서 스토리지 VM(이제 역관계의 원본 SVM)을 찾고, SVM 이름 위에 마우스 커서를 올려놓은 다음 클릭합니다. ⋮그런 다음 *대상 스토리지 VM 활성화*를 클릭합니다.
9. 대상 스토리지 **VM** 활성화 창에서 *대상 스토리지 VM 활성화 및 연결 해제*를 선택하고 *활성화*를 클릭합니다.
10. 관계 페이지로 돌아가서 스토리지 VM 이름 위에 마우스 커서를 다시 올려놓고 클릭하세요. ⋮그리고 *역방향 동기화*를 클릭하세요.

CLI를 참조하십시오

1. 원본 소스 SVM 또는 원본 소스 클러스터에서 동일한 구성, 정책 및 ID 보존 설정을 원본 SVM DR 관계로

사용하여 역방향 SVM DR 관계를 생성합니다.

```
snapmirror create -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 데이터를 제공하는 SVM과 SVM_BACKUP, 그리고 원래 소스 SVM, Svm1 간의 관계를 생성합니다.

```
cluster_src::> snapmirror create -source-path svm_backup:
-destination-path svm1:
```

에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 데이터 보호 관계를 반대로 전환합니다.

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다.

소스와 대상에 공통 스냅샷이 없는 경우 명령이 실패합니다. `snapmirror initialize`관계를 다시 초기화하는 데 사용합니다.

다음 예에서는 원래 소스 SVM, svm1, 데이터를 제공하는 SVM, svm_backup의 관계를 반전시킵니다.

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1:
```

사용 예 - 빠른 재동기화 옵션:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1: -quick-resync true
```

3. 원래 소스 SVM에 대한 데이터 액세스를 다시 설정할 준비가 되면 원래 타겟 SVM을 중지하고 원래 타겟 SVM에 현재 연결된 모든 클라이언트의 연결을 끊습니다.

```
vserver stop -vserver <SVM>
```

다음 예에서는 현재 데이터를 제공하고 있는 원래 대상 SVM을 중지합니다.

```
cluster_dst::> vserver stop svm_backup
```

4. 'vserver show' 명령을 사용하여 원래 대상 SVM이 중지됨 상태인지 확인합니다.

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

5. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계의 최종 업데이트를 수행하고 원래 대상 SVM에서 원래 소스 SVM으로 모든 변경 사항을 전송합니다.

```
snapmirror update -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 데이터를 제공하는 원래 대상 SVM, 'sVM_backup' 및 원래 소스 SVM, 'svm1' 간의 관계를 업데이트합니다.

```
cluster_src::> snapmirror update -source-path svm_backup:
-destination-path svm1:
```

에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계에 대한 예약된 전송을 중지합니다.

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 데이터를 제공하는 SVM, 'sVM_backup'과 원래 SVM, svm1 간의 예약된 전송을 중지합니다.

```
cluster_src::> snapmirror quiesce -source-path svm_backup:
-destination-path svm1:
```

7. 최종 업데이트가 완료되고 관계가 관계 상태에 "중지됨"으로 표시되면 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계를 나눕니다.

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 데이터를 제공하고 있는 원래 대상 SVM, 'sVM_backup' 및 원래 소스 SVM, 'svm1' 간의 관계를 나눕니다.

```
cluster_src::> snapmirror break -source-path svm_backup:
-destination-path svm1:
```

에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

8. 원래 소스 SVM이 이전에 중지된 경우 원래 소스 클러스터에서 원본 소스 SVM을 시작합니다.

```
vserver start -vserver <SVM>
```

다음 예에서는 원본 소스 SVM을 시작합니다.

```
cluster_src::> vserver start svm1
```

9. 원래 대상 SVM 또는 원래 대상 클러스터에서 원래 데이터 보호 관계를 다시 설정합니다.

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 원래 소스 SVM, svm1, 원래 대상 SVM, svm_backup 간의 관계를 다시 설정합니다.

```
cluster_dst::> snapmirror resync -source-path svm1: -destination
-path svm_backup:
```

10. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 데이터 보호 관계를 삭제합니다.

```
snapmirror delete -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 원래 대상 SVM, sVM_backup과 원래 소스 SVM, svm1 간의 역방향 관계를 삭제합니다.

```
cluster_src::> snapmirror delete -source-path svm_backup:
-destination-path svm1:
```

11. 원래 대상 SVM 또는 원래 대상 클러스터에서 역방향 데이터 보호 관계를 해제합니다.

```
snapmirror release -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 원래 대상 SVM, svm_backup 및 원래 소스 SVM, svm1 간의 역방향 관계를 해제합니다

```
cluster_dst::> snapmirror release -source-path svm_backup:
-destination-path svm1:
```

다음 단계

- 를 사용합니다 `snapmirror show` 명령을 사용하여 SnapMirror 관계가 생성되었는지 확인합니다.

  에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

- 클라이언트에서 원래 소스 SVM으로 쓰기 작업을 재개합니다.

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 초기화"
- "SnapMirror 중지"

- "SnapMirror 릴리즈"
- "스냅미러 재동기화"

FlexGroup 볼륨에 대해 원래의 **ONTAP SnapMirror** 소스 **SVM**을 다시 활성화합니다

대상에서 데이터를 더 이상 사용할 필요가 없을 경우 소스 및 타겟 SVM 간에 원래 데이터 보호 관계를 다시 설정할 수 있습니다. FlexGroup 볼륨을 사용할 때 원본 소스 SVM을 다시 활성화하려면 원래 SVM DR 관계를 삭제하고 관계를 반대로 설정하기 전에 원래 관계를 해제하는 등 몇 가지 추가 단계를 수행해야 합니다. 또한 예약된 전송을 중지하기 전에 역방향 관계를 해제하고 원래 관계를 다시 생성해야 합니다.

단계

1. 원래 대상 SVM 또는 원래 대상 클러스터에서 원래 SVM DR 관계를 삭제합니다.

   '스냅샷 삭제 - 소스 경로 SVM: - 대상 경로 SVM:

   '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 원래 소스 SVM, svm1, 원래 대상 SVM, svm_backup 간의 원래 관계를 삭제합니다.

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

2. 원본 소스 SVM 또는 원본 소스 클러스터에서 스냅샷을 그대로 유지하면서 원본 관계를 해제합니다.

   '냅미러 해제-소스-경로 SVM:-대상-경로 SVM:-관계-정보-전용 true'

   '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 원래 소스 SVM, svm1, 원래 대상 SVM, svm_backup 간의 원래 관계를 해제합니다.

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup: -relationship-info-only true
   ```

3. 원본 소스 SVM 또는 원본 소스 클러스터에서 동일한 구성, 정책 및 ID 보존 설정을 원본 SVM DR 관계로 사용하여 역방향 SVM DR 관계를 생성합니다.

   "napMirror create-source-path SVM:-destination-path SVM:

   '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 데이터를 제공하는 SVM과 SVM_BACKUP, 그리고 원래 소스 SVM, Svm1 간의 관계를

생성합니다.

```
cluster_src::> snapmirror create -source-path svm_backup: -destination
-path svm1:
```

4. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 데이터 보호 관계를 반대로 전환합니다.

   '스냅샷 미러 재동기화 - 소스 경로_SVM_: - 대상-경로_SVM_:'

   '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다.

   소스와 대상에 공통 스냅샷이 없는 경우 명령이 실패합니다. `snapmirror initialize`관계를 다시 초기화하는 데 사용합니다.

   다음 예에서는 원래 소스 SVM, svm1, 데이터를 제공하는 SVM, svm_backup의 관계를 반전시킵니다.

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

5. 원래 소스 SVM에 대한 데이터 액세스를 다시 설정할 준비가 되면 원래 타겟 SVM을 중지하고 원래 타겟 SVM에 현재 연결된 모든 클라이언트의 연결을 끊습니다.

   'vserver stop-vserver_SVM_'

   다음 예에서는 현재 데이터를 제공하고 있는 원래 대상 SVM을 중지합니다.

```
cluster_dst::> vserver stop svm_backup
```

6. 'vserver show' 명령을 사용하여 원래 대상 SVM이 중지됨 상태인지 확인합니다.

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

7. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계의 최종 업데이트를 수행하고 원래

대상 SVM에서 원래 소스 SVM으로 모든 변경 사항을 전송합니다.

'스냅미러 업데이트 - source-path_SVM_: - destination-path_SVM_:'

> '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 데이터를 제공하는 원래 대상 SVM, 'sVM_backup' 및 원래 소스 SVM, 'svm1' 간의 관계를 업데이트합니다.

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

8. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계에 대한 예약된 전송을 중지합니다.

   'sapmirror quiesce-source-path_SVM_:-destination-path_SVM_:'

   > '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 데이터를 제공하는 SVM, 'sVM_backup'과 원래 SVM, svm1 간의 예약된 전송을 중지합니다.

   ```
   cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
   -path svm1:
   ```

   에 대한 자세한 내용은 `snapmirror quiesce` "ONTAP 명령 참조입니다"을 참조하십시오.

9. 최종 업데이트가 완료되고 관계가 관계 상태에 "중지됨"으로 표시되면 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계를 나눕니다.

   '스냅미러 break-source-path_SVM_:-destination-path_SVM_:'

   > '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 데이터를 제공하고 있는 원래 대상 SVM, 'sVM_backup' 및 원래 소스 SVM, 'svm1' 간의 관계를 나눕니다.

   ```
   cluster_src::> snapmirror break -source-path svm_backup: -destination
   -path svm1:
   ```

   에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

10. 원래 소스 SVM이 이전에 중지된 경우 원래 소스 클러스터에서 원본 소스 SVM을 시작합니다.

'vserver start-vserver_SVM_'

다음 예에서는 원본 소스 SVM을 시작합니다.

```
cluster_src::> vserver start svm1
```

11. 원래 소스 SVM 또는 원본 소스 클러스터에서 역방향 SVM DR 관계를 삭제합니다.

    '스냅샷 삭제 - 소스 경로 SVM: - 대상 경로 SVM:

    '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

    다음 예에서는 원래 대상 SVM, svm_backup 및 원래 소스 SVM, svm1 간의 역방향 관계를 삭제합니다.

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

12. 원래의 대상 SVM 또는 원래의 대상 클러스터에서 스냅샷을 그대로 유지하면서 반대 관계를 해제합니다.

    '냅미러 해제-소스-경로 SVM:-대상-경로 SVM:-관계-정보-전용 true'

    '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

    다음 예에서는 원래 대상 SVM, svm_backup 및 원래 소스 SVM, svm1 간에 반전된 관계를 해제합니다.

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination
-path svm1: -relationship-info-only true
```

13. 원래 대상 SVM 또는 원래 대상 클러스터에서 원래 관계를 다시 생성합니다. 동일한 구성, 정책 및 ID 보존 설정을 원래 SVM DR 관계와 동일하게 사용:

    "napMirror create-source-path SVM:-destination-path SVM:

    '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

    다음 예에서는 원래 소스 SVM, svm1, 원래 대상 SVM, svm_backup 간에 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup:
```

14. 원래 대상 SVM 또는 원래 대상 클러스터에서 원래 데이터 보호 관계를 다시 설정합니다.

'스냅샷 미러 재동기화 - 소스 경로_SVM_: - 대상-경로_SVM_:'

> '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 원래 소스 SVM, svm1, 원래 대상 SVM, svm_backup 간의 관계를 다시 설정합니다.

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 초기화"
- "SnapMirror 중지"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"

ONTAP SnapMirror 대상 **SVM**에서 데이터를 다시 동기화합니다

ONTAP 9.11.1에는 재해 복구 연습을 수행할 때 전체 데이터 웨어하우스 재구축을 우회하는 옵션이 도입되어 생산 단계로 빠르게 돌아갈 수 있습니다.

ONTAP 9.8부터는 System Manager를 사용하여 소스 스토리지 VM의 데이터 및 구성 세부 정보를 손상된 보호 관계에 있는 대상 스토리지 VM으로 재동기화하고 관계를 다시 설정할 수 있습니다.

원래 관계의 대상에서만 재동기화 작업을 수행합니다. 재동기화를 수행하면 소스 스토리지 VM의 데이터보다 최신 대상 스토리지 VM의 데이터가 삭제됩니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 이 작업을 수행할 수 있습니다.

시스템 관리자

1. 타겟에서 원하는 보호 관계를 선택합니다. * 보호 > 관계 * 를 클릭합니다.
2. 선택적으로 * 빠른 재동기화 수행 * 을 선택하여 재해 복구 리허설 중에 전체 데이터 웨어하우스 재구축을 우회합니다.
3. 을 클릭하고 ⋮ * 재동기화 * 를 클릭합니다.
4. 관계 * 에서 관계에 대한 * 전송 상태 * 를 확인하여 재동기화 진행률을 모니터링합니다.

CLI를 참조하십시오

1. 대상 클러스터에서 관계를 다시 동기화합니다.

```
snapmirror resync -source-path <svm>: -destination-path <svm>:
-quick-resync true|false
```

관련 정보

- "스냅미러 재동기화"

ONTAP SnapMirror 볼륨 DR 관계를 SVM DR 관계로 변환합니다

소스의 각 볼륨(루트 볼륨 제외)이 복제되고 있는 경우, 볼륨을 소유하는 SVM(스토리지 가상 머신) 간의 복제 관계를 SVM(스토리지 가상 머신) 간에 복제 관계로 전환할 수 있습니다. 소스(루트 볼륨 포함)의 각 볼륨의 이름은 대상의 볼륨과 동일합니다.

이 작업에 대해

`volume rename`필요한 경우 SnapMirror 관계가 유휴 상태일 때 명령을 사용하여 대상 볼륨의 이름을 바꿉니다. 에 대한 자세한 내용은 `volume rename` link:https://docs.netapp.com/us-en/ontap-cli/volume-rename.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

단계

1. 타겟 SVM 또는 타겟 클러스터에서 소스 볼륨과 타겟 볼륨을 다시 동기화하려면 다음 명령을 실행합니다.

   ```
   snapmirror resync -source-path <SVM:volume> -destination-path <SVM:volume>
   -type DP|XDP -policy <policy>
   ```

   에 대한 자세한 내용은 snapmirror resync "ONTAP 명령 참조입니다"을 참조하십시오.

   재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다.

   다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA의 관계를 재동기화했습니다.

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA
```

2. 에 설명된 대로 소스 및 타겟 SVM 간에 SVM 복제 관계를 생성합니다 "SVM 구성 복제".

   복제 관계를 생성할 때 'napmirror create' 명령의 '-identity-preserve true' 옵션을 사용해야 합니다.

   에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 대상 SVM 중지:

   'vserver stop-vserver_SVM_'

   에 대한 자세한 내용은 `vserver stop` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 대상 SVM의 VM_BACKUP을 중지합니다.

```
cluster_dst::> vserver stop svm_backup
```

4. 타겟 SVM 또는 타겟 클러스터에서 다음 명령을 실행하여 소스 및 타겟 SVM을 다시 동기화하십시오.

   `snapmirror resync -source-path <SVM>: -destination-path <SVM>: -type DP|XDP -policy <policy>`

   > '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.
   >
   > 재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다.

   다음 예에서는 소스 SVM의 vm1과 대상 SVM의 vm_backup 간의 관계를 재동기화했습니다.

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

관련 정보

- "SnapMirror 생성"
- "스냅미러 재동기화"

ONTAP SnapMirror SVM 복제 관계를 삭제합니다

및 `snapmirror release` 명령을 사용하여 SVM 복제 관계를 삭제할 수 있습니다 `snapmirror delete`. 그런 다음 불필요한 대상 볼륨을 수동으로 삭제할 수 있습니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

이 작업에 대해

이 `snapmirror release` 명령은 SnapMirror에서 생성된 스냅샷을 소스에서 삭제합니다. 옵션을 사용하여 스냅샷을 보존할 수 `-relationship-info-only` 있습니다.

단계

1. 타겟 SVM 또는 타겟 클러스터에서 다음 명령을 실행하여 복제 관계를 중단하십시오.

   '스냅미러 break-source-path_SVM_:-destination-path_SVM_:'

   > '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 소스 SVM의 vm1과 대상 SVM의 vm_backup 간의 관계를 나눕니다.

   ```
   cluster_dst::> snapmirror break -source-path svm1: -destination-path
   svm_backup:
   ```

   에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 타겟 SVM 또는 타겟 클러스터에서 다음 명령을 실행하여 복제 관계를 삭제합니다.

   '스냅샷 삭제-소스-경로_SVM_:-대상-경로_SVM_:'

   > '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 소스 SVM의 vm1과 대상 SVM의 vm_backup 간의 관계를 삭제합니다.

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

   에 대한 자세한 내용은 `snapmirror delete` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 소스 클러스터 또는 소스 SVM에서 다음 명령을 실행하여 소스 SVM에서 복제 관계 정보를 해제합니다.

   '스냅미러 해제 - source-path_SVM_: - destination-path_SVM_:'

   > '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 소스 SVM의 vm1에서 지정된 복제 관계에 대한 정보를 해제합니다.

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup:
   ```

에 대한 자세한 내용은 `snapmirror release` "ONTAP 명령 참조입니다"을 참조하십시오.

SnapMirror 루트 볼륨 복제를 관리합니다

ONTAP SnapMirror 루트 볼륨 복제에 대해 알아보십시오

NAS 환경의 모든 SVM에는 고유한 네임스페이스가 있습니다. 운영 체제 및 관련 정보가 포함된 SVM_root 볼륨은 네임스페이스 계층 구조의 진입점입니다. 노드 운영 중단 또는 페일오버 발생 시 클라이언트가 데이터에 계속 액세스할 수 있도록 SVM 루트 볼륨의 로드 공유 미러 복사본을 생성해야 합니다.

SVM 루트 볼륨을 위한 로드 공유 미러의 주요 용도는 더 이상 로드 공유를 위한 것이 아니라, 재해 복구를 위한 것입니다.

- 루트 볼륨을 일시적으로 사용할 수 없는 경우 로드 공유 미러에서 루트 볼륨 데이터에 대한 읽기 전용 액세스를 자동으로 제공합니다.
- 루트 볼륨을 영구적으로 사용할 수 없는 경우 로드 공유 볼륨 중 하나를 승격하여 루트 볼륨 데이터에 대한 쓰기 액세스를 제공할 수 있습니다.

ONTAP 로드 공유 미러 관계를 생성하고 초기화합니다

클러스터에서 NAS 데이터를 처리하는 각 SVM 루트 볼륨에 대해 로드 공유 미러(LSM)를 생성해야 합니다. 두 개 이상의 HA 쌍으로 구성된 클러스터의 경우, HA 쌍의 두 노드 모두에 장애가 발생하더라도 클라이언트가 네임스페이스에 계속 액세스할 수 있도록 SVM 루트 볼륨의 로드 공유 미러를 고려해야 합니다. 로드 공유 미러는 단일 HA 쌍으로 구성된 클러스터에는 적합하지 않습니다.

시작하기 전에

ONTAP 9.16.1부터 로드 공유 미러 관계를 생성할 때 대상 SVM에서 저장소 제한을 활성화할 수 없습니다.

이 작업에 대해

동일한 노드에서 LSM을 생성하고 해당 노드를 사용할 수 없는 경우, 단일 장애 지점이 있으며, 클라이언트가 데이터에 계속 액세스할 수 있도록 하기 위한 두 번째 복제본이 없습니다. 그러나 루트 볼륨이 포함된 노드 이외의 노드 또는 다른 HA 쌍에서 LSM을 생성할 경우, 중단 시에도 데이터에 액세스할 수 있습니다.

예를 들어, 3개 노드에 루트 볼륨이 있는 4노드 클러스터의 경우:

- HA 1 노드 1의 루트 볼륨의 경우 HA 2 노드 1 또는 HA 2 노드 2에 LSM을 생성한다.
- HA 1 노드 2의 루트 볼륨의 경우 HA 2 노드 1 또는 HA 2 노드 2에 LSM을 생성한다.
- HA 2 노드 1의 루트 볼륨의 경우 HA 1 노드 1 또는 HA 1 노드 2에 LSM을 생성한다.

단계

1. LSM의 대상 볼륨을 생성한다.

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

대상 볼륨의 크기는 루트 볼륨보다 크거나 같아야 합니다.

루트 및 대상 볼륨에 접미사를 지정하는 것이 가장 좋습니다. 예를 들어, '_root' 및 '_m1' 등이 있습니다.

에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 "cluster_src"에 루트 볼륨 svm1_root에 대한 로드 공유 미러 볼륨을 생성합니다.

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "복제 작업 일정을 생성합니다".
3. SVM 루트 볼륨과 LSM의 대상 볼륨 간에 로드 공유 미러 관계를 생성합니다.

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type LS -schedule <schedule>
```

다음 예에서는 루트 볼륨 'vm1_root'와 로드 공유 미러 볼륨 'svm1_m1' 간에 로드 공유 미러 관계를 생성합니다.

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

부하 공유 미러의 유형 속성이 DP에서 LS로 변경됩니다.

에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 로드 공유 미러 초기화:

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

다음 예에서는 루트 볼륨 'svm1_root'에 대한 로드 공유 미러를 초기화합니다.

```
cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 로드 공유 미러 관계를 업데이트합니다

SVM에 볼륨이 마운트 또는 마운트 해제된 이후, 그리고 옵션을 포함하는 운영 `junction-path` 중에 SVM 루트 볼륨에 대한 로드 공유 미러(LSM) 관계가 자동으로 업데이트됩니다 `volume create`. 다음 번 예약된 업데이트 전에 업데이트하려는 경우 LSM 관계를 수동으로 업데이트할 수 있습니다.

다음과 같은 경우 로드 공유 미러 관계가 자동으로 업데이트됩니다.

- 예약된 업데이트를 할 시간입니다
- SVM 루트 볼륨의 볼륨에 대해 마운트 또는 마운트 해제 작업이 수행됩니다
- 에이 `volume create` 다음을 포함하는 명령이 발행됩니다. `junction-path` 옵션

  에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 로드 공유 미러 관계를 수동으로 업데이트:

   이 명령을 실행하기 전에 꺾쇠 괄호 안의 변수를 필수 값으로 바꾸어야 합니다.

   ```
   snapmirror update-ls-set -source-path <SVM:volume>
   ```

   다음 예에서는 루트 볼륨 'svm1_root'에 대한 로드 공유 미러 관계를 업데이트합니다.

   ```
   cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
   ```

   에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 로드 공유 미러를 상향 이동합니다

루트 볼륨을 영구적으로 사용할 수 없는 경우 LSM(Load-sharing mirror) 볼륨을 프로모션하여 루트 볼륨 데이터에 대한 쓰기 액세스를 제공할 수 있습니다.

시작하기 전에

이 작업에는 고급 권한 레벨 명령을 사용해야 합니다.

단계

1. 고급 권한 레벨로 변경:

   ```
   set -privilege advanced
   ```

2. LSM 볼륨 승격:

이 명령을 실행하기 전에 꺾쇠 괄호 안의 변수를 필수 값으로 바꾸어야 합니다.

```
snapmirror promote -destination-path <SVM:volume>
```

다음 예에서는 볼륨의 vm1_m2를 새 SVM 루트 볼륨으로 상향 이동합니다.

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
         cluster_src://svm1/svm1_root and replace it with
         cluster_src://svm1/svm1_m2. Because the volume is offline,
         it is not possible to determine whether this promote will
         affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

y를 입력합니다. ONTAP는 LSM 볼륨을 읽기/쓰기 볼륨으로 만들고, 액세스 가능한 경우 원래 루트 볼륨을 삭제한다.

> ⓘ 마지막 업데이트가 최근에 수행되지 않은 경우 상향 이동된 루트 볼륨에 원래 루트 볼륨에 있던 데이터가 모두 없을 수 있습니다.

에 대한 자세한 내용은 `snapmirror promote` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 관리자 권한 레벨로 돌아가기:

```
set -privilege admin
```

4. 루트 볼륨에 사용한 명명 규칙에 따라 승격된 볼륨의 이름을 바꿉니다.

이 명령을 실행하기 전에 꺾쇠 괄호 안의 변수를 필수 값으로 바꾸어야 합니다.

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

다음 예에서는 승격된 볼륨의 이름을 vm1_m2로 바꾸고 이름은 svm1_root로 바꿉니다.

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. 의 3단계에서 4단계에 설명된 대로 이름이 변경된 루트 볼륨을 보호합니다 "로드 공유 미러 관계 생성 및 초기화".

클라우드에 백업

ONTAP SnapMirror 클라우드 라이센스를 설치합니다

SnapMirror 클라우드 관계는 사전 검증된 타사 백업 애플리케이션을 사용하여 조정할 수 있습니다. ONTAP 9.9.1부터 System Manager를 사용하여 SnapMirror 클라우드 복제를 오케스트레이션할 수도 있습니다. System Manager를 사용하여 온프레미스 ONTAP를 오브젝트 스토리지 백업으로 조정하는 경우 SnapMirror 및 SnapMirror 클라우드 용량 라이센스가 모두 필요합니다. 또한 SnapMirror 클라우드 API 라이센스를 요청하여 설치해야 합니다.

이 작업에 대해

SnapMirror 클라우드 및 SnapMirror S3 라이센스는 노드 라이센스가 아니라 클러스터 라이센스이므로 ONTAP One 라이센스 번들과 함께 _ 제공되지 않습니다. 이러한 라이선스는 별도의 ONTAP One 호환성 번들에 포함되어 있습니다. SnapMirror 클라우드를 활성화하려면 이 번들을 요청해야 합니다.

또한 오브젝트 스토리지에 대한 SnapMirror 클라우드 백업을 System Manager에서 오케스트레이션하려면 SnapMirror Cloud API 키가 필요합니다. 이 API 라이센스는 단일 인스턴스 클러스터 전체 라이센스이므로 클러스터의 모든 노드에 설치할 필요가 없습니다.

단계

ONTAP One 호환성 번들과 SnapMirror Cloud API 라이센스를 요청하여 다운로드한 다음, System Manager를 사용하여 설치해야 합니다.

1. 라이센스할 클러스터의 클러스터 UUID를 찾아 기록합니다.

   클러스터에 맞는 ONTAP One 호환성 번들을 주문하기 위한 요청을 제출할 때 클러스터 UUID가 필요합니다.

2. NetApp 영업 팀에 문의하여 ONTAP One 호환성 번들을 요청하십시오.
3. NetApp 지원 사이트에 제공된 지침에 따라 SnapMirror 클라우드 API 라이센스를 요청합니다.

   "SnapMirror 클라우드 API 라이센스 키를 요청합니다"

4. 라이센스 파일을 받아 다운로드하면 시스템 관리자를 사용하여 ONTAP 클라우드 호환성 NLF 및 SnapMirror 클라우드 API NLF를 클러스터에 업로드합니다.
   a. 클러스터 > 설정 * 을 클릭합니다.
   b. 설정 * 창에서 * 라이센스 * 를 클릭합니다.
   c. 라이센스 * 창에서 를 + Add 클릭합니다.
   d. 라이센스 추가 * 대화 상자에서 * 찾아보기 * 를 클릭하여 다운로드한 NLF를 선택한 다음 * 추가 * 를 클릭하여 파일을 클러스터에 업로드합니다.

관련 정보

"SnapMirror를 사용하여 데이터를 클라우드에 백업합니다"

"NetApp 소프트웨어 라이센스 검색"

ONTAP SnapMirror를 사용하여 클라우드에 데이터를 백업합니다

ONTAP 9.9.1부터 System Manager를 사용하여 데이터를 클라우드로 백업하고 클라우드 스토리지에서 다른 볼륨으로 데이터를 복원할 수 있습니다. StorageGRID 또는 ONTAP S3를 클라우드 오브젝트 저장소로 사용할 수 있습니다.

ONTAP 9.18.1부터:

- SnapMirror 클라우드는 기존 "ONTAP REST API"을(를) 사용하여 MetroCluster 구성의 FlexGroup 볼륨에 대한 백업 및 복원 작업을 지원합니다. 이 기능을 통해 스위치오버 및 스위치백 후 파트너 사이트에서 유지 관리되는 MetroCluster 구성의 FlexGroup 볼륨에 대해 SnapMirror 클라우드 관계를 생성할 수 있습니다.

ONTAP 9.16.1부터:

- SnapMirror 클라우드 백업은 팬아웃 관계를 지원합니다. 즉, 서로 다른 두 오브젝트 저장소에서 SnapMirror 백업을 동시에 생성할 수 있습니다. SnapMirror 클라우드는 ONTAP 9.16.1을 통해 2가지 팬아웃 관계를 지원합니다. 팬아웃은 두 개의 오브젝트 저장소와 두 개의 서로 다른 오브젝트 저장소에 있는 하나 또는 두 개의 버킷으로 구성될 수 있습니다. 3개 이상의 팬아웃 관계를 생성하려는 시도는 실패합니다.
- SnapMirror 클라우드는 기존 볼륨을 사용하는 보다 효율적인 동기화 프로세스를 사용하여 클라우드로 마이그레이션된 볼륨을 백업할 수 있도록 "ONTAP REST API"지원합니다. 이 기능은 기준선 변경 작업을 수행할 필요 없이 클라우드의 마이그레이션된 볼륨에서 동일한 타겟 오브젝트 저장소 엔드포인트로 SnapMirror 클라우드 백업을 지원합니다. FlexVol 볼륨과 FlexGroup 볼륨이 모두 지원됩니다.

SnapMirror 클라우드 기능을 사용하기 전에 NetApp 지원 사이트에서 SnapMirror 클라우드 API 라이센스 키를 요청해야 합니다"SnapMirror 클라우드 API 라이센스 키를 요청합니다". 지침에 따라 비즈니스 기회에 대한 간단한 설명을 제공하고 제공된 이메일 주소로 이메일을 보내 API 키를 요청해야 합니다. API 키를 얻는 방법에 대한 추가 지침이 포함된 이메일 응답을 24시간 이내에 받아야 합니다.

클라우드 오브젝트 저장소를 추가합니다

SnapMirror 클라우드 백업을 구성하기 전에 StorageGRID 또는 ONTAP S3 클라우드 오브젝트 저장소를 추가해야 합니다.

단계

1. 보호 > 개요 > 클라우드 오브젝트 저장소 * 를 클릭합니다.
2. 을 클릭합니다 + Add .

기본 정책을 사용하여 백업합니다

기본 클라우드 보호 정책인 DailyBackup을 사용하여 기존 볼륨에 대한 SnapMirror 클라우드 백업을 빠르게 구성할 수 있습니다.

단계

1. 보호 > 개요 * 를 클릭하고 * Cloud에 볼륨 백업 * 을 선택합니다.
2. 처음으로 클라우드로 백업하는 경우 표시된 대로 라이센스 필드에 SnapMirror 클라우드 API 라이센스 키를 입력합니다.
3. 인증 및 계속 * 을 클릭합니다.
4. 소스 볼륨을 선택합니다.

5. 클라우드 오브젝트 저장소를 선택합니다.
6. 저장 * 을 클릭합니다.

사용자 지정 클라우드 백업 정책을 생성합니다

SnapMirror 클라우드 백업에 기본 DailyBackup 클라우드 정책을 사용하지 않으려면 자체 정책을 생성할 수 있습니다.

단계

1. 보호 > 개요 > 로컬 정책 설정 * 을 클릭하고 * 보호 정책 * 을 선택합니다.
2. 추가 * 를 클릭하고 새 정책 세부 정보를 입력합니다.
3. Policy Type * 섹션에서 * Back to Cloud * 를 선택하여 클라우드 정책을 생성하고 있음을 나타냅니다.
4. 저장 * 을 클릭합니다.

볼륨 * 페이지에서 백업을 생성합니다

한 번에 여러 볼륨에 대한 클라우드 백업을 선택하여 생성하거나 사용자 지정 보호 정책을 사용하려는 경우 System Manager * Volumes * 페이지를 사용할 수 있습니다.

단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 클라우드에 백업할 볼륨을 선택하고 * 보호 * 를 클릭합니다.
3. 볼륨 보호 * 창에서 * 추가 옵션 * 을 클릭합니다.
4. 정책을 선택합니다.

   기본 정책, DailyBackup 또는 직접 생성한 사용자 지정 클라우드 정책을 선택할 수 있습니다.

5. 클라우드 오브젝트 저장소를 선택합니다.
6. 저장 * 을 클릭합니다.

클라우드에서 복원

System Manager를 사용하여 클라우드 스토리지에서 소스 클러스터의 다른 볼륨으로 백업된 데이터를 복원할 수 있습니다.

ONTAP 9.16.1 이상을 사용 중이고 SnapMirror 클라우드 단일 파일 복원을 FlexGroup 볼륨으로 수행하는 경우 FlexGroup 볼륨의 새 디렉토리로만 파일을 복원해야 하며 세부 데이터는 타겟 FlexGroup 볼륨에서 로 설정해야 합니다. `advanced` 옵션 설정에 대한 자세한 `-granular-data advanced` 내용은 을 "파일 데이터를 재배포하여 ONTAP FlexGroup 볼륨의 균형을 조정합니다 "참조하십시오.

단계

1. SnapMirror-to-Cloud 관계의 소스 클러스터에서 * 스토리지 > 볼륨 * 을 클릭합니다.
2. 복원할 볼륨을 선택합니다.
3. Back Up to Cloud * 탭을 선택합니다.
4. 복원할 소스 볼륨 옆에 있는 을 ⋮ 클릭하여 메뉴를 표시하고 * Restore * 를 선택합니다.

5. 소스 * 에서 스토리지 VM을 선택한 다음 데이터를 복원할 볼륨의 이름을 입력합니다.
6. 대상 * 에서 복원할 스냅샷을 선택합니다.
7. 저장 * 을 클릭합니다.

SnapMirror 클라우드 관계를 삭제합니다

System Manager를 사용하여 클라우드 관계를 삭제할 수 있습니다.

단계

1. 스토리지 > 볼륨 * 을 클릭하고 삭제할 볼륨을 선택합니다.
2. 소스 볼륨 옆에 있는 을 ⋮ 클릭하고 * Delete * 를 선택합니다.
3. 클라우드 오브젝트 저장소 끝점을 삭제하려면 * 클라우드 오브젝트 저장소 끝점 삭제(선택 사항) * 를 선택합니다.
4. 삭제 * 를 클릭합니다.

클라우드 오브젝트 저장소를 제거합니다

클라우드 오브젝트 저장소가 클라우드 백업 관계의 일부가 아닌 경우 System Manager를 사용하여 클라우드 오브젝트 저장소를 제거할 수 있습니다. 클라우드 오브젝트 저장소가 클라우드 백업 관계의 일부인 경우 삭제할 수 없습니다.

단계

1. 보호 > 개요 > 클라우드 오브젝트 저장소 * 를 클릭합니다.
2. 삭제하려는 개체 저장소를 선택하고 를 ⋮ 클릭한 다음 * 삭제 * 를 선택합니다.

NetApp Backup and Recovery를 사용하여 데이터 백업

ONTAP 9.9.1부터 NetApp 백업 및 복구 서비스를 사용하여 System Manager에서 클라우드의 데이터를 백업할 수 있습니다.

백업 및 복구는 FlexVol 읽기-쓰기 볼륨과 데이터 보호(DP) 볼륨을 지원합니다. ONTAP 9.12.1부터 백업 및 복구는 FlexGroup 볼륨과 SnapLock 볼륨을 지원합니다.

자세히 알아보세요 "NetApp 백업 및 복구" .

시작하기 전에

NetApp 콘솔에서 계정을 설정하려면 다음 절차를 수행해야 합니다. 서비스 계정의 경우 "계정 관리자" 역할을 만들어야 합니다. (다른 서비스 계정 역할에는 시스템 관리자에서 연결을 설정하는 데 필요한 권한이 없습니다.)

1. "NetApp 콘솔에서 계정 만들기" .
2. "NetApp 콘솔에서 콘솔 에이전트 만들기"다음 클라우드 공급자 중 하나와 함께:
    - Microsoft Azure를 참조하십시오
    - AWS(Amazon Web Services)
    - Google Cloud Platform(GCP)
    - StorageGRID(ONTAP 9.10.1)

ONTAP 9.10.1부터 NetApp 콘솔이 온프레미스에 배포된 경우에만 StorageGRID 클라우드 백업 공급자로 선택할 수 있습니다. 콘솔 에이전트는 온프레미스에 설치해야 하며 NetApp 콘솔 SaaS(Software-as-a-Service) 애플리케이션을 통해 사용할 수 있어야 합니다.

3. "NetApp 콘솔에서 NetApp 백업 및 복구 구독"(적절한 라이센스가 필요합니다).
4. "NetApp 콘솔을 사용하여 액세스 키와 비밀 키 생성" .

NetApp 콘솔에 클러스터 등록

콘솔이나 시스템 관리자를 사용하여 NetApp 콘솔에 클러스터를 등록할 수 있습니다.

단계

1. System Manager에서 * 보호 개요 * 로 이동합니다.
2. * NetApp 백업 및 복구*에서 다음 세부 정보를 제공합니다.
   - 클라이언트 ID입니다
   - 클라이언트 암호 키입니다
3. Register and Continue * 를 선택합니다.

NetApp 백업 및 복구 활성화

클러스터가 NetApp 콘솔에 등록된 후 NetApp 백업 및 복구를 활성화하고 클라우드에 대한 첫 번째 백업을 시작해야 합니다.

단계

1. System Manager에서 * 보호 > 개요 * 를 선택한 다음 * Cloud Backup Service * 섹션으로 스크롤합니다.
2. 클라이언트 ID * 및 * 클라이언트 암호 * 를 입력합니다.

ONTAP 9.10.1부터 * 클라우드 사용 비용에 대해 자세히 알아보기 * 를 선택하여 클라우드 사용 비용에 대해 알아볼 수 있습니다.

3. 연결 및 Cloud Backup Service 활성화 * 를 선택합니다.
4. * NetApp 백업 및 복구 활성화* 페이지에서 선택한 공급자에 따라 다음 세부 정보를 제공합니다.

이 클라우드 공급자의 경우…	다음 데이터를 입력하십시오…
Azure를 지원합니다	• Azure 구독 ID입니다 • 지역 • 리소스 그룹 이름(기존 또는 신규)
설치하고	• AWS 계정 ID입니다 • 액세스 키 • 비밀 키 • 지역

Google Cloud Project(GCP)	• Google Cloud 프로젝트 이름 • Google Cloud Access 키 • Google Cloud 비밀 키 • 지역
StorageGRID (ONTAP 9.10.1 이상, NetApp 콘솔의 온프레미스 배포에만 해당)	• 서버 • SG 액세스 키 • SG 비밀 키

5. 보호 정책 * 선택:
   - * 기존 정책 *: 기존 정책을 선택합니다.
   - * 새 정책 *: 이름을 지정하고 전송 일정을 설정합니다.

     ONTAP 9.10.1부터 Azure 또는 AWS로 아카이빙할 것인지 여부를 지정할 수 있습니다.

     Azure 또는 AWS로 볼륨에 대한 아카이브를 활성화하면 아카이브를 비활성화할 수 없습니다.

     Azure 또는 AWS에 대해 아카이브를 설정하는 경우 다음을 지정합니다.

     - 볼륨이 아카이빙된 후 경과한 일 수입니다.
     - 아카이브에 보존할 백업 수입니다. 최신 백업까지 보관하려면 "0"(영)을 지정하십시오.
     - AWS의 경우 아카이브 스토리지 클래스를 선택합니다.
6. 백업할 볼륨을 선택합니다.
7. 저장 * 을 선택합니다.

NetApp 백업 및 복구에 사용되는 보호 정책 편집

NetApp Backup and Recovery에서 사용되는 보호 정책을 변경할 수 있습니다.

단계

1. System Manager에서 * 보호 > 개요 * 를 선택한 다음 * Cloud Backup Service * 섹션으로 스크롤합니다.
2. 을 선택한 다음 * 편집 * 을 선택합니다.
3. 보호 정책 * 선택:
   - * 기존 정책 *: 기존 정책을 선택합니다.
   - * 새 정책 *: 이름을 지정하고 전송 일정을 설정합니다.

     ONTAP 9.10.1부터 Azure 또는 AWS로 아카이빙할 것인지 여부를 지정할 수 있습니다.

     Azure 또는 AWS로 볼륨에 대한 아카이브를 활성화하면 아카이브를 비활성화할 수 없습니다.

Azure 또는 AWS에 대해 아카이브를 설정하는 경우 다음을 지정합니다.

- 볼륨이 아카이빙된 후 경과한 일 수입니다.
- 아카이브에 보존할 백업 수입니다. 최신 백업까지 보관하려면 "0"(영)을 지정하십시오.
- AWS의 경우 아카이브 스토리지 클래스를 선택합니다.

4. 저장 * 을 선택합니다.

클라우드에서 새 볼륨 또는 **LUN** 보호

새 볼륨 또는 LUN을 생성할 때 볼륨 또는 LUN에 대해 클라우드에 백업할 수 있도록 SnapMirror 보호 관계를 설정할 수 있습니다.

시작하기 전에

- SnapMirror 라이센스가 있어야 합니다.
- 인터클러스터 LIF를 구성해야 합니다.
- NTP를 구성해야 합니다.
- 클러스터에서 ONTAP 9.9.1 이상을 실행해야 함

이 작업에 대해

다음과 같은 클러스터 구성에서는 클라우드에서 새 볼륨 또는 LUN을 보호할 수 없습니다.

- 클러스터가 MetroCluster 환경에 있을 수 없습니다.
- SVM-DR은 지원되지 않습니다.
- FlexGroup 볼륨은 NetApp Backup and Recovery를 사용하여 백업할 수 없습니다.

단계

1. 볼륨 또는 LUN을 프로비저닝할 때 System Manager의 * 보호 * 페이지에서 * SnapMirror 사용(로컬 또는 원격) * 확인란을 선택합니다.
2. 백업 및 복구 정책 유형을 선택합니다.
3. 백업 및 복구가 활성화되어 있지 않으면 * NetApp 백업 및 복구를 사용하여 백업 활성화*를 선택합니다.

클라우드의 기존 볼륨 또는 **LUN** 보호

기존 볼륨 및 LUN에 대해 SnapMirror 보호 관계를 설정할 수 있습니다.

단계

1. 기존 볼륨 또는 LUN을 선택하고 * Protect * 를 선택합니다.
2. 볼륨 보호 페이지에서 보호 정책에 대해 * NetApp Backup and Recovery를 사용하여 백업*을 지정합니다.
3. protect * 를 선택합니다.
4. 보호 * 페이지에서 * SnapMirror 활성화(로컬 또는 원격) * 확인란을 선택합니다.
5. * NetApp 백업 및 복구 연결 및 활성화*를 선택합니다.

백업 파일에서 데이터를 복원합니다

데이터 복원, 관계 업데이트, 관계 삭제 등의 백업 관리 작업은 NetApp 콘솔을 사용하는 경우에만 수행할 수 있습니다. . "백업 파일에서 데이터를 복원합니다" 자세한 내용은.

SnapLock 기술을 사용한 아카이브 및 규정 준수

ONTAP SnapLock 에 대해 알아보세요

SnapLock는 WORM 스토리지를 사용하여 규정 및 거버넌스 목적으로 수정되지 않은 형태로 파일을 유지하는 조직을 위한 고성능 규정 준수 솔루션입니다.

SnapLock는 SEC 17a-4(f), HIPAA, FINRA, CFTC, GDPR과 같은 규정을 충족하도록 데이터의 삭제, 변경 또는 이름을 바꾸는 것을 방지합니다. SnapLock를 사용하면 파일을 저장한 후 지정된 보존 기간 또는 무기한으로 삭제할 수 없고 쓸 수 없는 상태로 커밋하는 특수한 용도의 볼륨을 생성할 수 있습니다. SnapLock에서는 CIFS 및 NFS와 같은 표준 개방형 파일 프로토콜을 통해 파일 레벨에서 이 보존을 수행할 수 있습니다. SnapLock에서 지원되는 개방형 파일 프로토콜은 NFS(버전 2, 3 및 4) 및 CIFS(SMB 1.0, 2.0 및 3.0)입니다.

SnapLock를 사용하여 파일 및 스냅샷을 WORM 스토리지에 커밋하고 WORM 보호 데이터의 보존 기간을 설정할 수 있습니다. SnapLock WORM 스토리지는 NetApp 스냅샷 기술을 사용하며 SnapMirror 복제 및 SnapVault 백업을 데이터에 대한 백업 복구 보호를 제공하기 위한 기본 기술로 활용할 수 있습니다. WORM 스토리지에 대해 자세히 "NetApp SnapLock-TR-4526을 사용하여 WORM 스토리지를 준수합니다"알아보십시오.

애플리케이션을 사용하여 NFS 또는 CIFS를 통해 WORM에 파일을 커밋하거나 SnapLock 자동 커밋 기능을 사용하여 파일을 WORM에 자동으로 커밋할 수 있습니다. _WORM 추가 가능 파일_을 사용하여 로그 정보와 같이 점증적으로 기록된 데이터를 보존할 수 있습니다. 자세한 내용은 을 참조하십시오 "볼륨 추가 모드를 사용하여 WORM 추가 가능 파일을 생성합니다".

SnapLock는 대부분의 규정 준수 요구사항을 충족하는 데이터 보호 방법을 지원합니다.

- SnapVault용 SnapLock를 사용하여 보조 스토리지에서 WORM으로 스냅샷을 보호할 수 있습니다. 을 "WORM에 스냅샷 커밋"참조하십시오.
- SnapMirror를 사용하여 재해 복구를 위해 WORM 파일을 다른 지리적 위치에 복제할 수 있습니다. 을 참조하십시오 "WORM 파일 미러링".

SnapLock 은 ONTAP 의 라이선스 기반 기능입니다. 단일 라이선스를 통해 엄격한 규정 준수 모드에서 SnapLock 사용하여 SEC 규칙 17a-4(f)와 같은 외부 의무를 충족하고, 느슨한 엔터프라이즈 모드에서 디지털 자산 보호를 위한 내부적으로 의무화된 규정을 충족할 수 있습니다. SnapLock 라이센스는 다음의 일부입니다. "ONTAP 1 을 참조하십시오" 소프트웨어 제품군.

SnapLock는 모든 AFF 및 FAS 시스템과 ONTAP Select에서 지원됩니다. SnapLock는 소프트웨어 전용 솔루션이 아니라 통합 하드웨어 및 소프트웨어 솔루션입니다. 이러한 차이는 통합 하드웨어 및 소프트웨어 솔루션이 필요한 SEC 17a-4(f)와 같은 엄격한 WORM 규정에서 중요합니다. 자세한 내용은 을 "전자 저장 매체 사용에 대한 중개 딜러에 대한 SEC 지침"참조하십시오.

SnapLock로 할 수 있는 일

SnapLock를 구성한 후 다음 작업을 수행할 수 있습니다.

- "WORM에 파일을 커밋합니다"

- "보조 스토리지를 위해 WORM에 스냅샷을 커밋합니다"
- "재해 복구를 위해 WORM 파일을 미러링합니다"
- "법적 증거 자료 보관 을 사용하여 소송 중에 WORM 파일을 보관하십시오"
- "권한 있는 삭제 기능을 사용하여 WORM 파일을 삭제합니다"
- "파일 보존 기간을 설정합니다"
- "SnapLock 볼륨을 이동합니다"
- "랜섬웨어 공격으로부터 보호하기 위해 스냅샷을 잠급니다"
- "감사 로그와 함께 SnapLock 사용을 검토합니다"
- "SnapLock API 사용"

SnapLock 규정 준수 및 엔터프라이즈 모드

SnapLock 규정 준수 및 엔터프라이즈 모드는 각 모드에서 WORM 파일을 보호하는 수준에 따라 크게 다릅니다.

SnapLock 모드	보호 수준	WORM 파일 보존 중 삭제
준수 모드	디스크 레벨에서 복구	삭제할 수 없습니다
엔터프라이즈 모드	파일 레벨에서	감사된 "특권 삭제" 절차를 사용하여 규정 준수 관리자가 삭제할 수 있습니다.

보존 기간이 경과하면 더 이상 필요하지 않은 파일을 삭제할 책임이 있습니다. 파일이 규정 준수 모드이든 엔터프라이즈 모드이든 WORM에 커밋되면 보존 기간이 만료된 후에도 수정할 수 없습니다.

보존 기간 중 또는 이후에 WORM 파일을 이동할 수 없습니다. WORM 파일을 복사할 수 있지만 WORM 특성이 유지되지 않습니다.

다음 표에는 SnapLock 규정 준수 및 엔터프라이즈 모드에서 지원하는 기능의 차이가 나와 있습니다.

제공합니다	SnapLock 규정 준수	SnapLock 엔터프라이즈
권한 있는 삭제를 사용하여 파일을 활성화 및 삭제합니다	아니요	예
디스크를 다시 초기화합니다	아니요	예
보존 기간 동안 SnapLock 애그리게이트 및 볼륨을 제거합니다	아니요	예. SnapLock 감사 로그 볼륨을 제외하고 가능합니다
Aggregate 또는 볼륨의 이름을 바꿉니다	아니요	예
비NetApp 디스크를 사용합니다	아니요	아니요

감사 로깅을 위해 SnapLock 볼륨을 사용합니다	예	예, ONTAP 9.5부터 시작합니다

SnapLock에서 지원 및 지원되지 않는 기능

다음 표에는 SnapLock 규정 준수 모드, SnapLock 엔터프라이즈 모드 또는 둘 다에서 지원되는 기능이 나와 있습니다.

피처	SnapLock 규정 준수 지원	SnapLock Enterprise에서 지원됩니다
일관성 그룹	아니요	아니요
암호화된 볼륨	네, 자세히 알아보세요 암호화 및 SnapLock .	네, 자세히 알아보세요 암호화 및 SnapLock .
SnapLock 애그리게이트에서 Fabric으로 구성	아니요	예, ONTAP 9.8부터 시작합니다. 에 대해 자세히 알아보십시오 FabricPool on SnapLock 엔터프라이즈 애그리게이트.
Flash Pool 애그리게이트로 전환 가능	예.	예.
플랙스클론	SnapLock 볼륨의 클론을 생성할 수는 있지만 SnapLock 볼륨의 파일은 복제할 수 없습니다.	SnapLock 볼륨의 클론을 생성할 수는 있지만 SnapLock 볼륨의 파일은 복제할 수 없습니다.
FlexGroup 볼륨	예, ONTAP 9.11.1부터 시작합니다. 에 대해 자세히 알아보십시오 [flexgroup].	예, ONTAP 9.11.1부터 시작합니다. 에 대해 자세히 알아보십시오 [flexgroup].
LUN을 클릭합니다	아니요 에 대해 자세히 알아보십시오 LUN 지원 SnapLock와 함께.	아니요 에 대해 자세히 알아보십시오 LUN 지원 SnapLock와 함께.
MetroCluster 구성	예, ONTAP 9.3부터 시작합니다. 에 대해 자세히 알아보십시오 MetroCluster 지원.	예, ONTAP 9.3부터 시작합니다. 에 대해 자세히 알아보십시오 MetroCluster 지원.
MAV(Multi-admin verification)	예, ONTAP 9.13.1. 에 대해 자세히 알아보십시오 MAV 지원.	예, ONTAP 9.13.1. 에 대해 자세히 알아보십시오 MAV 지원.
산	아니요	아니요
단일 파일 SnapRestore	아니요	예
SnapMirror 활성 동기화	아니요	아니요

SnapRestore	아니요	예
SMTape	아니요	아니요
SnapMirror Synchronous	아니요	아니요
SSD를 지원합니다	예.	예.
스토리지 효율성 기능	예, ONTAP 9.9.1부터 시작합니다. 에 대해 자세히 알아보십시오 스토리지 효율성 지원.	예, ONTAP 9.9.1부터 시작합니다. 에 대해 자세히 알아보십시오 스토리지 효율성 지원.

FabricPool on SnapLock 엔터프라이즈 애그리게이트

FabricPool은 ONTAP 9.8부터 SnapLock 엔터프라이즈 애그리게이트에서 지원됩니다. 그러나 클라우드 관리자가 해당 데이터를 삭제할 수 있으므로 FabricPool 데이터를 퍼블릭 또는 프라이빗 클라우드로 계층화하면 SnapLock에서 더 이상 보호되지 않는다는 사실을 NetApp 어카운트 팀이 설명하는 제품 분산 요청을 개설해야 합니다.

FabricPool에서 퍼블릭 또는 프라이빗 클라우드로 계층화하는 데이터는 클라우드 관리자가 삭제할 수 있으므로 SnapLock에서 더 이상 보호되지 않습니다.

FlexGroup 볼륨

SnapLock는 ONTAP 9.11.1부터 FlexGroup 볼륨을 지원하지만 다음 기능은 지원되지 않습니다.

- 법적 증거 자료 보관
- 이벤트 기반 보존
- SnapLock for SnapVault(ONTAP 9.12.1부터 지원됨)

또한 다음과 같은 행동을 인지해야 합니다.

- FlexGroup 볼륨의 VCC(Volume Compliance Clock)는 루트 구성 요소 VCC에 의해 결정됩니다. 모든 비루트 구성 요소들은 VCC를 루트 VCC와 긴밀히 동기화하게 됩니다.
- SnapLock 구성 속성은 FlexGroup 전체에 대해서만 설정됩니다. 개별 구성 요소마다 기본 보존 시간 및 자동 커밋 기간과 같은 서로 다른 구성 속성을 사용할 수 없습니다.

LUN 지원

LUN은 비 SnapLock 볼륨에서 생성된 스냅샷이 SnapLock 소산 관계의 일부로 보호를 위해 SnapLock 볼륨으로 전송되는 경우에만 SnapLock 볼륨에서 지원됩니다. LUN은 읽기/쓰기 SnapLock 볼륨에서 지원되지 않습니다. 변조 방지 스냅샷은 SnapMirror 소스 볼륨과 LUN이 포함된 타겟 볼륨 모두에서 지원됩니다.

MetroCluster 지원

MetroCluster 구성에서 SnapLock 지원은 SnapLock 규정 준수 모드와 SnapLock 엔터프라이즈 모드 간에 다릅니다.

SnapLock 규정 준수

- ONTAP 9.3부터 SnapLock 규정 준수는 미러링되지 않은 MetroCluster 애그리게이트에서 지원됩니다.
- ONTAP 9.3부터 SnapLock 규정 준수는 미러링된 애그리게이트에서 SnapLock 감사 로그 볼륨을 호스팅하는 데 사용되는 경우에만 지원됩니다.
- MetroCluster를 사용하여 SVM별 SnapLock 구성을 운영 사이트 및 2차 사이트에 복제할 수 있습니다.

SnapLock 엔터프라이즈

- SnapLock Enterprise 집계가 지원됩니다.
- ONTAP 9.3부터는 권한이 있는 삭제 기능이 있는 SnapLock 엔터프라이즈 애그리게이트가 지원됩니다.
- MetroCluster를 사용하여 SVM별 SnapLock 구성을 두 사이트 모두에 복제할 수 있습니다.

MetroCluster 구성 및 규정 준수 클럭

MetroCluster 구성에는 VCC(Volume Compliance Clock)와 SCC(System Compliance Clock)라는 두 가지 준수 클록 메커니즘이 사용됩니다. VCC 및 SCC는 모든 SnapLock 구성에 사용할 수 있습니다. 노드에 새 볼륨을 생성할 때 해당 노드에 있는 SCC의 현재 값으로 VCC가 초기화됩니다. 볼륨이 생성된 후에는 항상 VCC를 통해 볼륨 및 파일 보존 시간을 추적합니다.

볼륨이 다른 사이트에 복제되면 해당 VCC도 복제됩니다. 예를 들어, 사이트 A에서 사이트 B로 볼륨 전환이 발생하면 사이트 A의 SCC가 사이트 A가 오프라인이 되면 사이트 B에서 VCC가 계속 업데이트됩니다.

사이트 A가 다시 온라인 상태가 되고 볼륨 스위치백을 수행하면 볼륨의 VCC가 계속 업데이트되는 동안 사이트 A SCC 클록이 다시 시작됩니다. 스위치오버 및 스위치백 작업과 관계없이 VCC가 지속적으로 업데이트되기 때문에 파일 보존 시간은 SCC 클럭에 의존하지 않고 늘어나지 않습니다.

MAV(Multi-admin verification) 지원

ONTAP 9.13.1 부터는 클러스터 관리자가 일부 SnapLock 작업을 실행하기 전에 쿼럼을 승인해야 하는 클러스터에서 다중 관리 검증을 명시적으로 활성화할 수 있습니다. MAV가 활성화되면 기본 보존 시간, 최소 보존 시간, 최대 보존 시간, 볼륨 추가 모드, 자동 커밋 기간 및 권한 삭제 등의 SnapLock 볼륨 속성에 쿼럼이 승인되어야 합니다. 에 대해 자세히 알아보십시오 "5일".

스토리지 효율성

ONTAP 9.9.1부터 SnapLock은 데이터 컴팩션, 볼륨 간 중복제거, SnapLock 볼륨 및 애그리게이트를 위한 적응형 압축과 같은 스토리지 효율성 기능을 지원합니다. 스토리지 효율성에 대한 자세한 내용은 를 참조하십시오 "ONTAP 스토리지 효율성 개요".

암호화

ONTAP는 스토리지 미디어의 용도 변경, 반환, 잘못된 위치 변경 또는 도난 시 유휴 데이터를 읽을 수 없도록 소프트웨어 및 하드웨어 기반 암호화 기술을 모두 제공합니다.

- 법적 고지 사항: * NetApp은 자체 암호화 드라이브 또는 볼륨의 SnapLock 보호 WORM 파일이 인증 키가 손실되거나 실패한 인증 시도 횟수가 지정된 제한을 초과하여 드라이브가 영구적으로 잠기는 경우 이를 복구할 수 있다고 보장할 수 없습니다. 인증 실패에 대한 책임은 사용자에게 있습니다.

암호화된 볼륨은 SnapLock 집계에서 지원됩니다.

7-Mode 전환

7-Mode 전환 도구의 CBT(Copy-Based Transition) 기능을 사용하여 SnapLock 볼륨을 7-Mode에서 ONTAP로 마이그레이션할 수 있습니다. 대상 볼륨의 SnapLock 모드인 Compliance 또는 Enterprise는 소스 볼륨의 SnapLock 모드와 일치해야 합니다. CFT(Copy-Free Transition)를 사용하여 SnapLock 볼륨을 마이그레이션할 수는 없습니다.

SnapLock를 구성합니다

ONTAP SnapLock 구성에 대해 알아보세요

SnapLock를 사용하기 전에 "SnapLock 라이센스를 설치합니다"SnapLock 볼륨으로 애그리게이트를 호스팅하는 각 노드에 대해 등의 다양한 작업을 완료하여 SnapLock를 구성하고"규정 준수 시계", 를 초기화하며, ONTAP 9.10.1 이전의 ONTAP 릴리즈를 실행하는 클러스터에 대해 SnapLock 애그리게이트를 생성할 "SnapLock 볼륨을 생성하고 마운트합니다"수 있어야 합니다.

ONTAP 규정 준수 시계 초기화

SnapLock는 _ volume Compliance Clock _ 을(를) 사용하여 WORM 파일의 보존 기간을 변경할 수 있는 변조를 방지합니다. 먼저 SnapLock 애그리게이트를 호스팅하는 각 노드에서 _SYSTEM ComplianceClock_을 초기화해야 합니다.

ONTAP 9.14.1부터 SnapLock 볼륨이 없거나 스냅샷 잠금이 설정된 볼륨이 없는 경우 시스템 규정 준수 클록을 초기화하거나 다시 초기화할 수 있습니다. 시스템 관리자는 재초기화 기능을 사용하여 시스템 규정 준수 클록이 잘못 초기화되었을 수 있는 경우에 시스템 규정 준수 클록을 재설정하거나 시스템의 클럭 편차를 수정할 수 있습니다. ONTAP 9.13.1 이하 릴리즈에서는 노드에서 규정 준수 클록을 초기화한 후 다시 초기화할 수 없습니다.

시작하기 전에

규정 준수 클록을 다시 초기화하려면 다음을 수행합니다.

- 클러스터의 모든 노드가 정상 상태여야 합니다.
- 모든 볼륨이 온라인 상태여야 합니다.
- 복구 큐를 표시할 볼륨이 없습니다.
- SnapLock 볼륨이 없을 수 있습니다.
- 스냅샷 잠금이 활성화된 볼륨이 없을 수 있습니다.

규정 준수 시계 초기화를 위한 일반 요구 사항:

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- "노드에 SnapLock 라이센스가 설치되어 있어야 합니다"..

이 작업에 대해

시스템 Compliance Clock의 시간은 _ VOLUME Compliance Clock _ 에 의해 상속되며, 이 시간 중 후자는 볼륨에 있는 WORM 파일의 보존 기간을 제어합니다. 볼륨 준수 시계는 새 SnapLock 볼륨을 생성할 때 자동으로 초기화됩니다.

시스템 규정 준수 클럭의 초기 설정은 현재 하드웨어 시스템 클록을 기반으로 합니다. 따라서 각 노드에서 시스템 규정 준수 클록을 초기화하기 전에 시스템 시간과 시간대가 올바른지 확인해야 합니다. 노드에서 시스템 규정 준수 클록을 초기화하고 나면 SnapLock 볼륨 또는 잠금이 설정된 볼륨이 존재할 때 이를 다시 초기화할 수 없습니다.

단계

ONTAP CLI를 사용하여 규정 준수 클록을 초기화하거나 ONTAP 9.12.1부터 System Manager를 사용하여 규정 준수 클록을 초기화할 수 있습니다.

시스템 관리자

1. 클러스터 > 개요 * 로 이동합니다.
2. 노드 * 섹션에서 * SnapLock 준수 클럭 초기화 * 를 클릭합니다.
3. 규정 준수 시계 * 열을 표시하고 규정 준수 시계가 초기화되었는지 확인하려면 * 클러스터 > 개요 > 노드 * 섹션에서 * 표시/숨기기 * 를 클릭하고 * SnapLock 규정 준수 시계 * 를 선택합니다.

CLI를 참조하십시오

1. 시스템 규정 준수 클록을 초기화합니다.

   `snaplock compliance-clock initialize -node node_name`

   다음 명령을 실행하면 시스템 Compliance Clock On이 초기화됩니다 `node1`:

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

   에 대한 자세한 내용은 `snaplock compliance-clock initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 메시지가 표시되면 시스템 클록이 올바른지, 규정 준수 클록을 초기화할지 확인합니다.

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before
   proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. SnapLock 애그리게이트를 호스팅하는 각 노드에 대해 이 절차를 반복합니다.

NTP 구성 시스템에 대해 규정 준수 클럭 재동기화를 설정합니다

NTP 서버가 구성되면 SnapLock Compliance 시계 동기화 기능을 활성화할 수 있습니다.

시작하기 전에

- 이 기능은 고급 권한 수준에서만 사용할 수 있습니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- "노드에 SnapLock 라이센스가 설치되어 있어야 합니다"..
- 이 기능은 Cloud Volumes ONTAP, ONTAP Select 및 VIM 플랫폼에서만 사용할 수 있습니다.

이 작업에 대해

SnapLock 보안 클럭 데몬이 임계값을 초과하는 편중을 감지하면 ONTAP는 시스템 시간을 사용하여 시스템 및 볼륨 규정 준수 클럭을 모두 재설정합니다. 24시간이 기울기 임계값으로 설정됩니다. 즉, 편중이 하루 이상 지난 경우에만 시스템 규정 준수 클록이 시스템 클록과 동기화됩니다.

SnapLock 보안 클록 데몬은 편중을 감지하고 규정 준수 클럭을 시스템 시간으로 변경합니다. 시스템 시간이 NTP 시간과 동기화되는 경우에만 규정 준수 클록이 시스템 시간과 동기화되기 때문에 규정 준수 클록이 시스템 시간과 동기화되도록 시스템 시간을 수정하려는 시도가 실패합니다.

단계

1. NTP 서버가 구성된 경우 SnapLock Compliance 시계 동기화 기능을 활성화합니다.

   `snaplock compliance-clock ntp`

   다음 명령은 시스템 규정 준수 시계 동기화 기능을 활성화합니다.

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

   에 대한 자세한 내용은 `snaplock compliance-clock ntp modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 메시지가 표시되면 구성된 NTP 서버가 신뢰할 수 있고 통신 채널이 보안 상태인지 확인합니다.
3. 기능이 활성화되어 있는지 확인합니다.

   `snaplock compliance-clock ntp show`

   다음 명령은 시스템 규정 준수 시계 동기화 기능이 활성화되어 있는지 확인합니다.

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

   에 대한 자세한 내용은 `snaplock compliance-clock ntp show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapLock 집계 생성

볼륨 '-snaplock-type' 옵션을 사용하여 Compliance 또는 Enterprise SnapLock 볼륨 유형을 지정합니다. ONTAP 9.10.1 이전 릴리스의 경우 별도의 SnapLock 애그리게이트를 만들어야 합니다. ONTAP 9.10.1부터 SnapLock 및 비 SnapLock 볼륨은 동일한 애그리게이트에 존재할 수 있으므로, ONTAP 9.10.1을 사용하는 경우 더 이상 별도의 SnapLock 애그리게이트를 생성할 필요가 없습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 노드의 SnapLock"라이센스를 설치해야 합니다"입니다. 이 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오 "있습니다.
- "노드의 규정 준수 클록을 초기화해야 합니다"..
- 디스크를 "루트", "루트", "다토1" 및 "다토2"로 분할한 경우 스페어 디스크를 사용할 수 있는지 확인해야 합니다.

업그레이드 고려 사항

ONTAP 9.10.1로 업그레이드할 때 기존 SnapLock 및 비 SnapLock 애그리게이트는 SnapLock 볼륨과 비 SnapLock 볼륨 모두를 지원하도록 업그레이드되지만 기존 SnapLock 볼륨 특성은 자동으로 업데이트되지 않습니다. 예를 들어, 데이터 컴팩션, 볼륨 간 중복제거, 볼륨 간 백그라운드 중복제거 필드는 변경되지 않습니다. 기존 애그리게이트에 생성된 새로운 SnapLock 볼륨의 기본값이 비 SnapLock 볼륨과 같고, 새 볼륨 및 애그리게이트의 기본 값은 플랫폼에 따라 다릅니다.

되돌리기 고려 사항

9.10.1 이전의 ONTAP 버전으로 복구해야 하는 경우 모든 SnapLock 규정 준수, SnapLock 엔터프라이즈 및 SnapLock 볼륨을 고유한 SnapLock 애그리게이트로 이동해야 합니다.

이 작업에 대해

- SyncMirror 옵션을 사용하여 준수 애그리게이트를 생성할 수 없습니다.
- MetroCluster 구성에서 미러링된 Compliance Aggregate는 SnapLock 감사 로그 볼륨을 호스팅하는 데 사용되는 경우에만 생성할 수 있습니다.

> MetroCluster 구성에서는 SnapLock Enterprise가 미러링된 Aggregate 및 미러링되지 않은 Aggregate에서 지원됩니다. SnapLock 규정 준수는 미러링되지 않은 애그리게이트에서만 지원됩니다.

단계

1. SnapLock 애그리게이트 생성:

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

다음 명령을 실행하면 node1에 3개의 디스크가 있는 "aggr1"이라는 SnapLock "Compliance" Aggregate가 생성됩니다.

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

에 대한 자세한 내용은 `storage aggregate create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapLock 볼륨 생성 및 마운트

WORM 상태로 커밋하려는 파일 또는 스냅샷에 대한 SnapLock 볼륨을 생성해야 합니다. ONTAP 9.10.1.1부터 애그리게이트 유형에 관계없이 생성한 모든 볼륨은 기본적으로 비 SnapLock 볼륨으로 생성됩니다. SnapLock 유형으로 Compliance 또는 Enterprise를 지정하여 SnapLock 볼륨을 명시적으로 생성하려면 옵션을 사용해야 `-snaplock-type` 합니다. 기본적으로 SnapLock 유형은 로 `non-snaplock`설정됩니다.

시작하기 전에

- SnapLock 애그리게이트는 온라인 상태여야 합니다.
- 해야 "SnapLock 라이센스가 설치되어 있는지 확인합니다"합니다. 노드에 SnapLock 라이센스가 설치되어 있지 않으면 반드시 설치해야 "설치합니다"합니다. 이 라이센스는 에 "ONTAP 1 을 참조하십시오"포함되어 있습니다. ONTAP One 이전에는 SnapLock 라이센스가 보안 및 규정 준수 번들에 포함되어 있었습니다. 보안 및 규정 준수 번들은 더 이상 제공되지 않지만 여전히 유효합니다. 현재는 필요하지 않지만 기존 고객은 선택할 수 "ONTAP One으로 업그레이드하십시오"있습니다.
- "노드의 규정 준수 클록을 초기화해야 합니다"..

이 작업에 대해

적절한 SnapLock 권한을 사용하여 언제든지 엔터프라이즈 볼륨을 삭제하거나 이름을 바꿀 수 있습니다. 보존 기간이 경과하기 전에는 Compliance 볼륨을 폐기할 수 없습니다. Compliance 볼륨의 이름은 변경할 수 없습니다.

SnapLock 볼륨의 클론을 생성할 수는 있지만 SnapLock 볼륨의 파일은 복제할 수 없습니다. 클론 볼륨은 상위 볼륨과 동일한 SnapLock 유형이 됩니다.

> LUN은 SnapLock 볼륨에서 지원되지 않습니다. LUN은 비 SnapLock 볼륨에서 생성된 스냅샷이 SnapLock 소산 관계의 일부로 보호를 위해 SnapLock 볼륨으로 전송되는 경우에만 SnapLock 볼륨에서 지원됩니다. LUN은 읽기/쓰기 SnapLock 볼륨에서 지원되지 않습니다. 변조 방지 스냅샷은 SnapMirror 소스 볼륨과 LUN이 포함된 타겟 볼륨 모두에서 지원됩니다.

ONTAP 시스템 관리자 또는 ONTAP CLI를 사용하여 이 작업을 수행합니다.

시스템 관리자

ONTAP 9.12.1부터 시스템 관리자를 사용하여 SnapLock 볼륨을 생성할 수 있습니다.

단계

1. Storage > Volumes * 로 이동한 다음 * Add * 를 클릭합니다.
2. 볼륨 추가 * 창에서 * 추가 옵션 * 을 클릭합니다.
3. 볼륨의 이름과 크기를 포함하여 새 볼륨 정보를 입력합니다.
4. SnapLock 사용 * 을 선택하고 SnapLock 유형(준수 또는 엔터프라이즈)을 선택합니다.
5. 자동 커밋 파일 * 섹션에서 * 수정 * 을 선택하고 파일이 자동으로 커밋되기 전에 변경되지 않은 상태로 유지되는 시간을 입력합니다. 최소값은 5분이고 최대값은 10년입니다.
6. Data Retention * 섹션에서 최소 및 최대 보존 기간을 선택합니다.
7. 기본 보존 기간을 선택합니다.
8. 저장 * 을 클릭합니다.
9. 볼륨 * 페이지에서 새 볼륨을 선택하여 SnapLock 설정을 확인합니다.

CLI를 참조하십시오

1. SnapLock 볼륨 생성:

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise>
```

에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오. SnapLock 볼륨에는 , `-atime-update`, , `-is-autobalance-eligible` `-space-mgmt-try-first` 및 `vmalign` 옵션을 사용할 수 없습니다 `-nvfail`.

다음 명령을 실행하면 vs1에 vol1이라는 SnapLock "Compliance" 볼륨이 생성됩니다.

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
-snaplock-type compliance
```

SnapLock 볼륨을 마운트합니다

NAS 클라이언트 액세스를 위해 SVM 네임스페이스의 접합 경로에 SnapLock 볼륨을 마운트할 수 있습니다.

시작하기 전에

SnapLock 볼륨이 온라인 상태여야 합니다.

이 작업에 대해

- SnapLock 볼륨은 SVM의 루트 아래에서만 마운트할 수 있습니다.
- SnapLock 볼륨 아래에 일반 볼륨을 마운트할 수 없습니다.

단계

1. SnapLock 볼륨 마운트:

   '* 볼륨 마운트 - vserver_SVM_name_-volume_volume_name_-junction-path_path_*'

   에 대한 자세한 내용은 `volume mount` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 이름이 vol1인 SnapLock 볼륨이 VS1 네임스페이스에서 junction path/sales에 마운트됩니다.

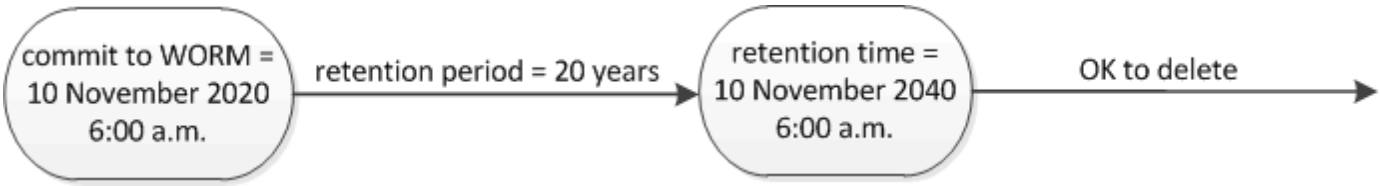
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

ONTAP SnapLock 보존 시간 설정

파일의 보존 시간을 명시적으로 설정하거나 볼륨에 대한 기본 보존 기간을 사용하여 보존 시간을 파생시킬 수 있습니다. 보존 시간을 명시적으로 설정하지 않으면 SnapLock에서는 기본 보존 기간을 사용하여 보존 시간을 계산합니다. 이벤트 후에 파일 보존을 설정할 수도 있습니다.

보존 기간 및 보존 시간에 대해 설명합니다

WORM 파일의 _retention period_는 파일이 WORM 상태로 커밋된 후 보존되어야 하는 시간을 지정합니다. WORM 파일의 _retention time_은 파일을 더 이상 보존할 필요가 없는 시간입니다. 예를 들어, 2020년 11월 10일 오전 6시부터 WORM 상태로 커밋된 파일의 보존 기간은 20년이며, 보존 기간은 2010년 11월 10일 오전 6시입니다



ONTAP 9.10.1부터 최대 10월 26일, 3058까지의 보존 기간 및 최대 100년의 보존 기간을 설정할 수 있습니다. 보존 날짜를 확장하면 이전 정책이 자동으로 변환됩니다. ONTAP 9.9.1 및 이전 릴리즈에서는 기본 보존 기간을 무한으로 설정하지 않으면 지원되는 최대 보존 시간은 1월 19 2071(GMT)입니다.

중요한 복제 고려 사항

1월 19일 2071(GMT) 이후의 보존 날짜를 사용하여 SnapLock 소스 볼륨과 SnapMirror 관계를 설정할 때 타겟 클러스터에서 ONTAP 9.10.1 이상이 실행 중이어야 하며, 그렇지 않으면 SnapMirror 전송이 실패합니다.

중요한 되돌리기 고려 사항

ONTAP 보존 기간이 "2071년 1월 19일 오전 8시 44분 7초" 이후인 파일이 있는 경우 클러스터를 ONTAP 9.10.1에서 이전 ONTAP 버전으로 되돌리는 것을 방지합니다.

보존 기간 이해

SnapLock 규정 준수 또는 엔터프라이즈 볼륨의 보존 기간은 4가지입니다.

- 최소 보존 기간(min), 기본값 0
- 최대 보존 기간(최대)(기본값: 30년

- ONTAP 9.10.1부터 준수 모드 및 엔터프라이즈 모드 모두에 대해 기본 보존 기간(기본값: "in")입니다. ONTAP 9.10.1 이전의 ONTAP 릴리즈에서는 기본 보존 기간이 모드에 따라 다릅니다.
  - 준수 모드의 경우 기본값은 'Max'입니다.
  - 엔터프라이즈 모드의 경우 기본값은 'in'입니다.
- 지정되지 않은 보존 기간.

> ⓘ ONTAP 9.10.1 이전 릴리스에서는 규정 준수 모드 파일을 WORM 상태로 커밋하기 전에 보존 시간을 명시적으로 설정하지 않고 기본값을 수정하지 않으면 해당 파일은 30년 동안 보존됩니다. 이 변경 사항은 실행 취소할 수 없습니다. 마찬가지로 ONTAP 9.10.1 이상에서는 엔터프라이즈 모드 파일을 WORM 상태로 커밋하기 전에 보존 시간을 명시적으로 설정하지 않고 기본값을 수정하지 않으면 해당 파일은 0년 동안 보존되거나 사실상 전혀 보존되지 않습니다.

ONTAP 9.8부터 볼륨에 있는 파일의 보존 기간을 '지정 안 됨'으로 설정하여 절대 보존 시간을 설정할 때까지 파일을 보존할 수 있습니다. 새 절대 보존 시간이 이전에 설정한 절대 시간보다 이후인 경우 절대 보존 시간을 지정하지 않은 보존으로 설정하고 다시 절대 보존으로 설정할 수 있습니다.

ONTAP 9.12.1부터 보존 기간이 설정된 WORM 파일 `unspecified` SnapLock 볼륨에 대해 구성된 최소 보존 기간으로 보존 기간을 설정해야 합니다. 에서 파일 보존 기간을 변경하는 경우 `unspecified` 지정된 새 보존 시간은 파일에 이미 설정된 최소 보존 시간보다 커야 합니다.

기본 보존 기간을 설정합니다

'volume SnapLock modify' 명령을 사용하여 SnapLock 볼륨의 파일에 대한 기본 보존 기간을 설정할 수 있습니다.

시작하기 전에

SnapLock 볼륨이 온라인 상태여야 합니다.

이 작업에 대해

다음 표에는 기본 보존 기간 옵션에 사용할 수 있는 값이 나와 있습니다.

> ⓘ 기본 보존 기간은 최소 보존 기간보다 크거나 같고 최대 보존 기간보다 작거나 같아야 합니다(<=).

값	단위	참고
0-65535	초	
0-24	시간	
0-365일	일	
0-12로 설정합니다	개월	
0-100입니다	년	ONTAP 9.10.1부터. 이전 ONTAP 릴리스의 경우 값은 0-70입니다.
최대	-	최대 보존 기간을 사용합니다.

값	단위	참고
최소	-	최소 보존 기간을 사용합니다.
무한대	-	파일을 영구적으로 보존합니다.
지정되지 않음	-	절대 보존 기간이 설정될 때까지 파일을 보존합니다.

최대 및 최소 보존 기간의 값과 범위는 해당되지 않는 최대 및 최소 보존 기간을 제외하고 동일합니다. 이 작업에 대한 자세한 내용은 을 참조하십시오 "보존 시간 개요를 설정합니다".

명령을 사용하여 볼륨의 보존 기간 설정을 볼 수 `volume snaplock show` 있습니다. 에 대한 자세한 내용은 `volume snaplock show` "ONTAP 명령 참조입니다"을 참조하십시오.

파일이 WORM 상태로 커밋된 후에는 보존 기간을 늘릴 수 있지만 줄일 수는 없습니다.

단계

1. SnapLock 볼륨에 있는 파일의 기본 보존 기간을 설정합니다.

   '* volume SnapLock modify -vserver_SVM_name_-volume_volume_name_-default-retention -period_default_retention_period_-minimum-retention-period_min_retention_period_-maximum-retention -period_max_retention_period_ *'

   에 대한 자세한 내용은 `volume snaplock modify` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 최소 및 최대 보존 기간이 이전에 수정되지 않은 것으로 가정합니다.

   다음 명령을 실행하면 Compliance 또는 Enterprise 볼륨의 기본 보존 기간이 20일로 설정됩니다.

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
   -retention-period 20days
   ```

   다음 명령을 실행하면 Compliance 볼륨의 기본 보존 기간이 70년으로 설정됩니다.

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
   -retention-period 70years
   ```

   다음 명령을 실행하면 엔터프라이즈 볼륨의 기본 보존 기간이 10년으로 설정됩니다.

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
   -retention-period max -maximum-retention-period 10years
   ```

   다음 명령을 실행하면 엔터프라이즈 볼륨의 기본 보존 기간이 10일로 설정됩니다.

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

다음 명령을 실행하면 Compliance 볼륨의 기본 보존 기간이 무한으로 설정됩니다.

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

파일의 보존 시간을 명시적으로 설정합니다

파일의 마지막 액세스 시간을 수정하여 파일의 보존 시간을 명시적으로 설정할 수 있습니다. NFS 또는 CIFS를 통해 적합한 명령 또는 프로그램을 사용하여 마지막 액세스 시간을 수정할 수 있습니다.

이 작업에 대해

파일이 WORM에 커밋된 후에는 보존 시간을 늘릴 수 있지만 줄일 수는 없습니다. 보존 시간은 파일의 atime 필드에 저장됩니다.

> ⓘ 파일의 보존 시간을 명시적으로 '무한'으로 설정할 수는 없습니다. 이 값은 기본 보존 기간을 사용하여 보존 시간을 계산하는 경우에만 사용할 수 있습니다.

단계

1. 적절한 명령 또는 프로그램을 사용하여 보존 시간을 설정할 파일의 마지막 액세스 시간을 수정합니다.

   UNIX 셸에서 다음 명령을 사용하여 2020년 11월 21일 오전 6:00의 보존 시간을 설정합니다 "document.txt" 파일에서 다음을 수행합니다.

   ```
   touch -a -t 202011210600 document.txt
   ```

   > ⓘ 적합한 명령 또는 프로그램을 사용하여 Windows의 마지막 액세스 시간을 수정할 수 있습니다.

이벤트 후 파일 보존 기간을 설정합니다

ONTAP 9.3부터 EBR(SnapLock_Event Based Retention)_Feature를 사용하여 이벤트 발생 후 파일이 유지되는 기간을 정의할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 SnapLock 관리자여야 합니다.

  "SnapLock 관리자 계정을 만듭니다"

- 보안 연결(SSH, 콘솔 또는 ZAPI)에 로그인해야 합니다.

이 작업에 대해

이벤트 보존 정책 _ 은(는) 이벤트가 발생한 후 파일의 보존 기간을 정의합니다. 정책은 단일 파일 또는 디렉토리의 모든 파일에 적용할 수 있습니다.

- 파일이 WORM 파일이 아닌 경우 정책에 정의된 보존 기간 동안 WORM 상태로 커밋됩니다.
- 파일이 WORM 파일 또는 WORM 추가 가능 파일인 경우 보존 기간은 정책에 정의된 보존 기간만큼 연장됩니다.

Compliance-mode 또는 Enterprise-mode 볼륨을 사용할 수 있습니다.

EBR 정책은 법적 증거 자료 보관 아래의 파일에 적용할 수 없습니다.

고급 사용법은 를 "NetApp SnapLock를 사용하여 WORM 스토리지 규정 준수"참조하십시오.

* _ EBR을 사용하여 이미 존재하는 WORM 파일의 보존 기간을 연장합니다. _ *
EBR은 기존 WORM 파일의 보존 기간을 연장하려는 경우에 편리합니다. 예를 들어, 직원이 원천징수를 변경한 후 3년 동안 직원 W-4 기록을 수정되지 않은 형태로 유지하는 것이 회사의 정책일 수 있습니다. 다른 회사 정책에서는 직원이 종료된 후 5년 동안 W-4 기록을 보관해야 할 수 있습니다. 이 경우 5년의 보존 기간을 사용하여 EBR 정책을 생성할 수 있습니다. 직원이 종료된 후("이벤트") 직원의 W-4 기록에 EBR 정책을 적용하여 보존 기간이 연장될 수 있습니다. 이는 일반적으로 보존 기간을 수동으로 연장하는 것보다 쉽습니다. 특히 많은 수의 파일이 관련된 경우 더욱 그렇습니다.

단계

1. EBR 정책 생성:

   `snaplock event-retention policy create -vserver` *`SVM_name`* `-name` *`policy_name`* `-retention-period` *`retention_period`*

   다음 명령은 VS1, 보존 기간 10년을 포함한 EBR 정책 'EMPLOYEE_EXIT'를 생성한다.

   ```
   cluster1::>snaplock event-retention policy create -vserver vs1 -name
   employee_exit -retention-period 10years
   ```

2. EBR 정책 적용:

   `snaplock event-retention apply -vserver` *`SVM_name`* `-name` *`policy_name`* `-volume` *`volume_name`* `-path` *`path_name`*

   다음 명령을 실행하면 VS1 디렉토리에 있는 모든 파일에 VS1 의 EBR 정책 'EMPLOYEE_EXIT'가 적용됩니다.

   ```
   cluster1::>snaplock event-retention apply -vserver vs1 -name
   employee_exit -volume vol1 -path /d1
   ```

관련 정보

- "SnapLock 이벤트 보존 정책 생성"

- "SnapLock 이벤트 보존 적용"

ONTAP SnapLock 으로 보호되는 감사 로그 생성

ONTAP 9.9.1 이하 버전을 사용하는 경우, 권한 있는 삭제 또는 SnapLock 볼륨 이동을 수행하기 전에 먼저 SnapLock 애그리게이트를 생성한 다음 SnapLock 보호 감사 로그를 생성해야 합니다. 감사 로그는 SnapLock 관리자 계정의 생성 및 삭제, 로그 볼륨 수정, 권한 있는 삭제 활성화 여부, 권한 있는 삭제 작업 및 SnapLock 볼륨 이동 작업을 기록합니다.

ONTAP 9.10.1부터는 SnapLock 애그리게이트를 생성할 수 없습니다. "SnapLock 볼륨을 명시적으로 생성합니다 "SnapLock 형식으로 Compliance 또는 Enterprise를 지정하려면 -SnapLock-type 옵션을 사용해야 합니다.

시작하기 전에

ONTAP 9.9.1 이하 버전을 사용하는 경우 SnapLock 애그리게이트를 생성하려면 클러스터 관리자여야 합니다.

이 작업에 대해

로그 파일 보존 기간이 경과할 때까지 감사 로그를 삭제할 수 없습니다. 보존 기간이 경과한 후에도 감사 로그를 수정할 수 없습니다. 이는 SnapLock 규정 준수 모드와 엔터프라이즈 모드 모두에서 마찬가지입니다.

> ONTAP 9.4 이하 버전에서는 감사 로깅을 위해 SnapLock 엔터프라이즈 볼륨을 사용할 수 없습니다. SnapLock 준수 볼륨을 사용해야 합니다. ONTAP 9.5 이상에서는 감사 로깅을 위해 SnapLock 엔터프라이즈 볼륨 또는 SnapLock 규정 준수 볼륨을 사용할 수 있습니다. 모든 경우에 감사 로그 볼륨은 교차점 경로 '/snaplock_audit_log'에 마운트되어야 합니다. 다른 볼륨은 이 접합 경로를 사용할 수 없습니다.

SnapLock Audit 로그는 감사 로그 볼륨의 루트 아래의 '/sSnapLock_log' 디렉토리에서 privdel_log'(권한 삭제 작업) 및 'system_log'(기타 모든 것)라는 하위 디렉토리에 있습니다. 감사 로그 파일 이름에는 첫 번째 기록 작업의 타임스탬프가 포함되어 있어 작업이 실행된 대략적인 시간만큼 레코드를 쉽게 검색할 수 있습니다.

- 'SnapLock log file show' 명령을 사용하여 감사 로그 볼륨에서 로그 파일을 볼 수 있습니다.
- 'SnapLock log file archive' 명령을 사용하여 현재 로그 파일을 보관하고 새 로그 파일을 만들 수 있습니다. 이 명령은 별도의 파일에 감사 로그 정보를 기록해야 하는 경우에 유용합니다.

및 `snaplock log file archive` 에 대한 자세한 `snaplock log file show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

> 데이터 보호 볼륨은 SnapLock 감사 로그 볼륨으로 사용할 수 없습니다.

단계

1. SnapLock Aggregate를 생성합니다.

   SnapLock Aggregate를 생성합니다

2. 감사 로깅을 위해 구성하려는 SVM에서 SnapLock 볼륨을 생성합니다.

   SnapLock 볼륨을 생성합니다

3. 감사 로깅을 위해 SVM 구성:

```
snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log
-size size -retention-period default_retention_period
```

> 감사 로그 파일의 최소 기본 보존 기간은 6개월입니다. 영향을 받는 파일의 보존 기간이 감사 로그의 보존 기간보다 긴 경우 로그의 보존 기간이 파일의 보존 기간을 상속합니다. 따라서 권한이 있는 삭제를 사용하여 삭제된 파일의 보존 기간이 10개월이고 감사 로그의 보존 기간이 8개월인 경우 로그 보존 기간은 10개월로 연장됩니다. 보존 시간 및 기본 보존 기간에 대한 자세한 내용은 을 참조하십시오"보존 시간을 설정합니다".

다음 명령어는 SnapLock volume logVol을 이용하여 Audit logging을 위한 'VM1'을 설정한다. 감사 로그의 최대 크기는 20GB이며 8개월 동안 유지됩니다.

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
20GB -retention-period 8months
```

에 대한 자세한 내용은 `snaplock log create` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 감사 로깅을 위해 구성한 SVM에서 SnapLock 볼륨을 연결 경로 '/sSnapLock_audit_log'에 마운트합니다.

   SnapLock 볼륨을 마운트합니다

ONTAP SnapLock 설정 확인

'volume file fingerprint start' 및 'volume file fingerprint dump' 명령을 사용하여 파일 유형(Regular, WORM 또는 WORM appendable), 볼륨 만료 날짜 등 파일 및 볼륨에 대한 주요 정보를 볼 수 있습니다.

단계

1. 파일 지문 생성:

   ```
   volume file fingerprint start -vserver <SVM_name> -file <file_path>
   ```

   ```
   svm1::> volume file fingerprint start -vserver svm1 -file
   /vol/sle/vol/f1
   File fingerprint operation is queued. Run "volume file fingerprint show
   -session-id 16842791" to view the fingerprint session status.
   ```

   이 명령어는 'volume file fingerprint dump' 명령어에 대한 입력으로 사용할 수 있는 세션 ID를 생성한다.

   > 세션 ID와 함께 볼륨 파일 fingerprint show 명령을 사용하여 지문 작업의 진행률을 모니터링할 수 있습니다. 지문 표시를 시도하기 전에 작업이 완료되었는지 확인하십시오.

2. 파일의 지문을 표시합니다.

   ```
   volume file fingerprint dump -session-id <session_ID>
   ```

```
svm1::> volume file fingerprint dump -session-id 33619976
        Vserver:svm1
        Session-ID:33619976
        Volume:slc_vol
        Path:/vol/slc_vol/f1
        Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
        Fingerprint Scope:data-and-metadata
        Fingerprint Start Time:1460612586
        Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
        Fingerprint Version:3
        **SnapLock License:available**
        Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
        Volume MSID:2152884007
        Volume DSID:1028
        Hostname:my_host
        Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
        Volume Containing Aggregate:slc_aggr1
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
        Access Time:-
```

```
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

WORM 파일 관리

ONTAP SnapLock 사용하여 WORM 파일 관리

WORM 파일은 다음과 같은 방법으로 관리할 수 있습니다.

- "WORM에 파일을 커밋합니다"
- "볼트 대상에서 WORM에 스냅샷을 커밋합니다"
- "재해 복구를 위해 WORM 파일을 미러링합니다"
- "소송 중에 WORM 파일 보존"
- "WORM 파일을 삭제합니다"

ONTAP SnapLock 사용하여 WORM에 파일 커밋

파일을 수동으로 커밋하거나 자동으로 커밋하여 WORM(Write Once, Read Many)에 커밋할 수 있습니다. WORM 추가 가능 파일을 생성할 수도 있습니다.

WORM에 파일을 수동으로 커밋합니다

파일을 읽기 전용으로 만들어 WORM에 파일을 수동으로 커밋합니다. NFS 또는 CIFS를 통해 적합한 명령 또는 프로그램을 사용하여 파일의 읽기-쓰기 속성을 읽기 전용으로 변경할 수 있습니다. 응용 프로그램이 파일에 대한 쓰기를 완료했는지 확인하여 파일이 너무 일찍 커밋되지 않았는지 또는 많은 볼륨 때문에 자동 커밋 스캐너에 대한 배율 조정 문제가 있는지 확인하려면 파일을 수동으로 커밋하도록 선택할 수 있습니다.

시작하기 전에

- 커밋하려는 파일이 SnapLock 볼륨에 있어야 합니다.
- 파일에 쓸 수 있어야 합니다.

이 작업에 대해

볼륨 ComplianceClock 시간은 명령이나 프로그램이 실행될 때 파일의 ctime 필드에 기록됩니다. ComplianceClock 시간은 파일의 보존 시간에 도달한 시점을 결정합니다.

단계

1. 적합한 명령 또는 프로그램을 사용하여 파일의 읽기-쓰기 속성을 읽기 전용으로 변경합니다.

   UNIX 셸에서 다음 명령을 사용하여 "document.txt"라는 파일을 읽기 전용으로 만듭니다.

```
chmod -w document.txt
```

Windows 셸에서 다음 명령을 사용하여 "document.txt"라는 파일을 읽기 전용으로 만듭니다.

```
attrib +r document.txt
```

파일을 **WORM**에 자동으로 커밋합니다

SnapLock 자동 커밋 기능을 사용하면 파일을 WORM에 자동으로 커밋할 수 있습니다. 자동 커밋 기능은 자동 커밋 기간 동안 파일이 변경되지 않은 경우 SnapLock 볼륨에서 파일을 WORM 상태로 커밋합니다. 자동 커밋 기능은 기본적으로 비활성화되어 있습니다.

시작하기 전에

- 자동 커밋하려는 파일이 SnapLock 볼륨에 있어야 합니다.
- SnapLock 볼륨이 온라인 상태여야 합니다.
- SnapLock 볼륨은 읽기-쓰기 볼륨이어야 합니다.

> SnapLock 자동 커밋 기능은 볼륨에 있는 모든 파일을 검사하여 자동 커밋 요구 사항을 충족하는 경우 파일을 커밋합니다. 파일이 자동 커밋될 준비가 된 시점과 SnapLock 자동 커밋 스캐너에서 실제로 커밋된 시점 사이에 시간 간격이 있을 수 있습니다. 그러나 파일이 자동 커밋될 수 있는 즉시 파일 시스템에 의해 수정 및 삭제로부터 보호됩니다.

이 작업에 대해

autocommit period _ 는 파일이 자동 커밋되기 전에 변경되지 않은 상태로 유지해야 하는 시간을 지정합니다. 자동 커밋 기간이 경과하기 전에 파일을 변경하면 파일의 자동 커밋 기간이 다시 시작됩니다.

다음 표에는 자동 커밋 기간에 대해 가능한 값이 나와 있습니다.

값	단위	참고
없음	-	기본값입니다.
5-5256000	분	-
1-87600)을 참조하십시오	시간	-
1-3650	일	-
1-120으로 설정합니다	개월	-
1-10	년	-

> 최소값은 5분이고 최대값은 10년입니다.

단계

1. SnapLock 볼륨의 파일을 WORM에 자동 커밋:

   '* volume SnapLock modify -vserver_SVM_name_-volume_volume_name_-autos커밋 -period_autosit_period_ *'

   에 대한 자세한 내용은 `volume snaplock modify` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령은 파일이 5시간 동안 변경되지 않는 한 SVM VS1 볼륨 'vol1'에 있는 파일을 자동으로 커밋합니다.

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
   -period 5hours
   ```

WORM 추가 가능 파일을 생성합니다

WORM 추가 가능 파일은 로그 항목과 같이 점진적으로 기록된 데이터를 유지합니다. 적합한 명령 또는 프로그램을 사용하여 WORM 추가 가능 파일을 생성하거나 SnapLock_VOLUME append mode_feature를 사용하여 기본적으로 WORM 추가 가능 파일을 생성할 수 있습니다.

명령 또는 프로그램을 사용하여 WORM 추가 가능 파일을 생성합니다

NFS 또는 CIFS를 통해 적합한 명령 또는 프로그램을 사용하여 WORM 추가 가능 파일을 생성할 수 있습니다. WORM 추가 가능 파일은 로그 항목과 같이 점진적으로 기록된 데이터를 유지합니다. 데이터는 256KB 청크로 파일에 추가됩니다. 각 청크가 쓰일 때 이전 청크는 WORM으로 보호됩니다. 보존 기간이 경과할 때까지 파일을 삭제할 수 없습니다.

시작하기 전에

WORM 추가 가능 파일이 SnapLock 볼륨에 있어야 합니다.

이 작업에 대해

데이터는 활성 256KB 청크에 순차적으로 쓸 필요가 없습니다. 파일의 n×256KB+1 바이트에 데이터를 쓸 때 이전 256KB 세그먼트는 WORM으로 보호됩니다.

현재 활성 256KB 청크를 초과하는 순서가 없는 쓰기는 활성 256KB 청크가 최신 오프셋으로 재설정되고 이전 오프셋에 대한 쓰기가 실패하고 'ROFS(읽기 전용 파일 시스템)' 오류가 발생합니다. 쓰기 오프셋은 클라이언트 애플리케이션에 따라 다릅니다. WORM 추가 파일 쓰기 의미를 준수하지 않는 클라이언트는 쓰기 콘텐츠가 잘못 종료될 수 있습니다. 따라서 클라이언트가 순서가 지정되지 않은 쓰기에 대한 오프셋 제한을 따르는지 확인하거나 파일 시스템을 동기식 모드로 마운트하여 동기식 쓰기를 보장하는 것이 좋습니다.

단계

1. 적합한 명령 또는 프로그램을 사용하여 원하는 보존 시간으로 길이가 0인 파일을 생성합니다.

   UNIX 셸에서 다음 명령을 사용하여 2020년 11월 21일 오전 6:00의 보존 시간을 설정합니다 길이가 0인 파일에서 document.txt:

   ```
   touch -a -t 202011210600 document.txt
   ```

2. 적합한 명령 또는 프로그램을 사용하여 파일의 읽기-쓰기 속성을 읽기 전용으로 변경합니다.

UNIX 셸에서 다음 명령을 사용하여 "document.txt"라는 파일을 읽기 전용으로 만듭니다.

```
chmod 444 document.txt
```

3. 적합한 명령 또는 프로그램을 사용하여 파일의 읽기-쓰기 속성을 다시 쓰기 가능으로 변경합니다.

   파일에 데이터가 없기 때문에 이 단계는 규정 준수 위험으로 간주되지 않습니다.

   UNIX 셸에서 다음 명령을 사용하여 "document.txt"라는 파일을 쓰기 가능하게 만듭니다.

   ```
   chmod 777 document.txt
   ```

4. 적절한 명령 또는 프로그램을 사용하여 파일에 데이터 쓰기를 시작합니다.

   UNIX 셸에서 다음 명령을 사용하여 데이터를 document.txt에 씁니다.

   ```
   echo test data >> document.txt
   ```

   파일에 데이터를 더 이상 추가할 필요가 없는 경우 파일 권한을 다시 읽기 전용으로 변경합니다.

볼륨 추가 모드를 사용하여 **WORM** 추가 가능 파일을 생성합니다

ONTAP 9.3부터는 SnapLock_VOLUME APPEND MODE_(VAM) 기능을 사용하여 기본적으로 WORM 추가 가능 파일을 생성할 수 있습니다. WORM 추가 가능 파일은 로그 항목과 같이 점진적으로 기록된 데이터를 유지합니다. 데이터는 256KB 청크로 파일에 추가됩니다. 각 청크가 쓰일 때 이전 청크는 WORM으로 보호됩니다. 보존 기간이 경과할 때까지 파일을 삭제할 수 없습니다.

시작하기 전에

- WORM 추가 가능 파일이 SnapLock 볼륨에 있어야 합니다.
- SnapLock 볼륨을 마운트 해제하고 스냅샷과 사용자가 생성한 파일을 비워야 합니다.

이 작업에 대해

데이터는 활성 256KB 청크에 순차적으로 쓸 필요가 없습니다. 파일의 n×256KB+1 바이트에 데이터를 쓸 때 이전 256KB 세그먼트는 WORM으로 보호됩니다.

볼륨에 대해 자동 커밋 기간을 지정하면 자동 커밋 기간보다 긴 기간 동안 수정되지 않은 WORM 추가 가능 파일이 WORM에 커밋됩니다.

VAM은 SnapLock 감사 로그 볼륨에서 지원되지 않습니다.

단계

1. VAM 활성화:

   '* volume SnapLock modify -vserver_SVM_name_-volume_volume_name_-is-volume-append-mode

-enabled true|false *

에 대한 자세한 내용은 `volume snaplock modify` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 SVM의 볼륨 'vol1'에서 VAM이 활성화됩니다.

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
-append-mode-enabled true
```

2. 적합한 명령 또는 프로그램을 사용하여 쓰기 권한이 있는 파일을 만듭니다.

   파일은 기본적으로 WORM-appendable입니다.

ONTAP 볼트 대상의 **WORM**에 스냅샷 커밋

SnapVault용 SnapLock를 사용하여 보조 스토리지에서 WORM으로 스냅샷을 보호할 수 있습니다. 볼트 대상에서 모든 기본 SnapLock 작업을 수행합니다. 대상 볼륨은 읽기 전용으로 자동 마운트되므로 WORM에 스냅샷을 명시적으로 커밋할 필요가 없습니다.

시작하기 전에

- System Manager를 사용하여 관계를 구성하려면 소스 클러스터와 대상 클러스터 모두에서 ONTAP 9.15.1 이상이 실행 중이어야 합니다.
- 대상 클러스터에서:
  - "SnapLock 라이센스를 설치합니다".
  - "준수 시계를 초기화합니다".
  - 9.10.1 이전의 ONTAP 릴리즈와 함께 CLI를 사용하는 경우, "SnapLock 애그리게이트를 생성합니다".
- 보호 정책은 "볼트" 유형이어야 합니다.
- 소스 및 타겟 애그리게이트는 64비트여야 합니다.
- 소스 볼륨은 SnapLock 볼륨일 수 없습니다.
- ONTAP CLI를 사용하는 경우 소스 볼륨과 타겟 볼륨을 에서 생성해야 합니다 "피어링된 클러스터" 및 "SVM".

이 작업에 대해

소스 볼륨은 NetApp 또는 비 NetApp 스토리지를 사용할 수 있습니다.

WORM 상태로 커밋된 스냅샷의 이름은 변경할 수 없습니다.

SnapLock 볼륨의 클론을 생성할 수는 있지만 SnapLock 볼륨의 파일은 복제할 수 없습니다.

LUN은 SnapLock 볼륨에서 지원되지 않습니다. LUN은 비 SnapLock 볼륨에서 생성된 스냅샷이 SnapLock 소산 관계의 일부로 보호를 위해 SnapLock 볼륨으로 전송되는 경우에만 SnapLock 볼륨에서 지원됩니다. LUN은 읽기/쓰기 SnapLock 볼륨에서 지원되지 않습니다. 하지만 변조 방지 스냅샷은 SnapMirror 소스 볼륨과 LUN이 포함된 타겟 볼륨 모두에서 지원됩니다.

ONTAP 9.10.1부터 SnapLock 및 비 SnapLock 볼륨은 동일한 애그리게이트에 존재할 수 있으므로, ONTAP 9.10.1을

사용하는 경우 더 이상 별도의 SnapLock 애그리게이트를 생성할 필요가 없습니다. '-snaplock-type' 볼륨 옵션을 사용하여 Compliance 또는 Enterprise SnapLock 볼륨 유형을 지정합니다. ONTAP 9.10.1 이전의 ONTAP 릴리즈에서는 SnapLock 모드, 규정 준수 또는 엔터프라이즈가 aggregate에서 상속됩니다. 버전에 상관없이 유연한 타겟 볼륨이 지원되지 않습니다. 대상 볼륨의 언어 설정은 소스 볼륨의 언어 설정과 일치해야 합니다.

볼트 대상인 SnapLock 볼륨에 기본 보존 기간이 할당되어 있습니다. 이 기간의 값은 처음에 SnapLock 엔터프라이즈 볼륨의 경우 0년, SnapLock 규정 준수 볼륨의 경우 최대 30년으로 설정됩니다. 각 NetApp 스냅샷은 처음에는 이 기본 보존 기간을 사용하여 커밋됩니다. 필요한 경우 보존 기간을 나중에 연장할 수 있습니다. 자세한 내용은 을 "보존 시간 개요를 설정합니다"참조하십시오.

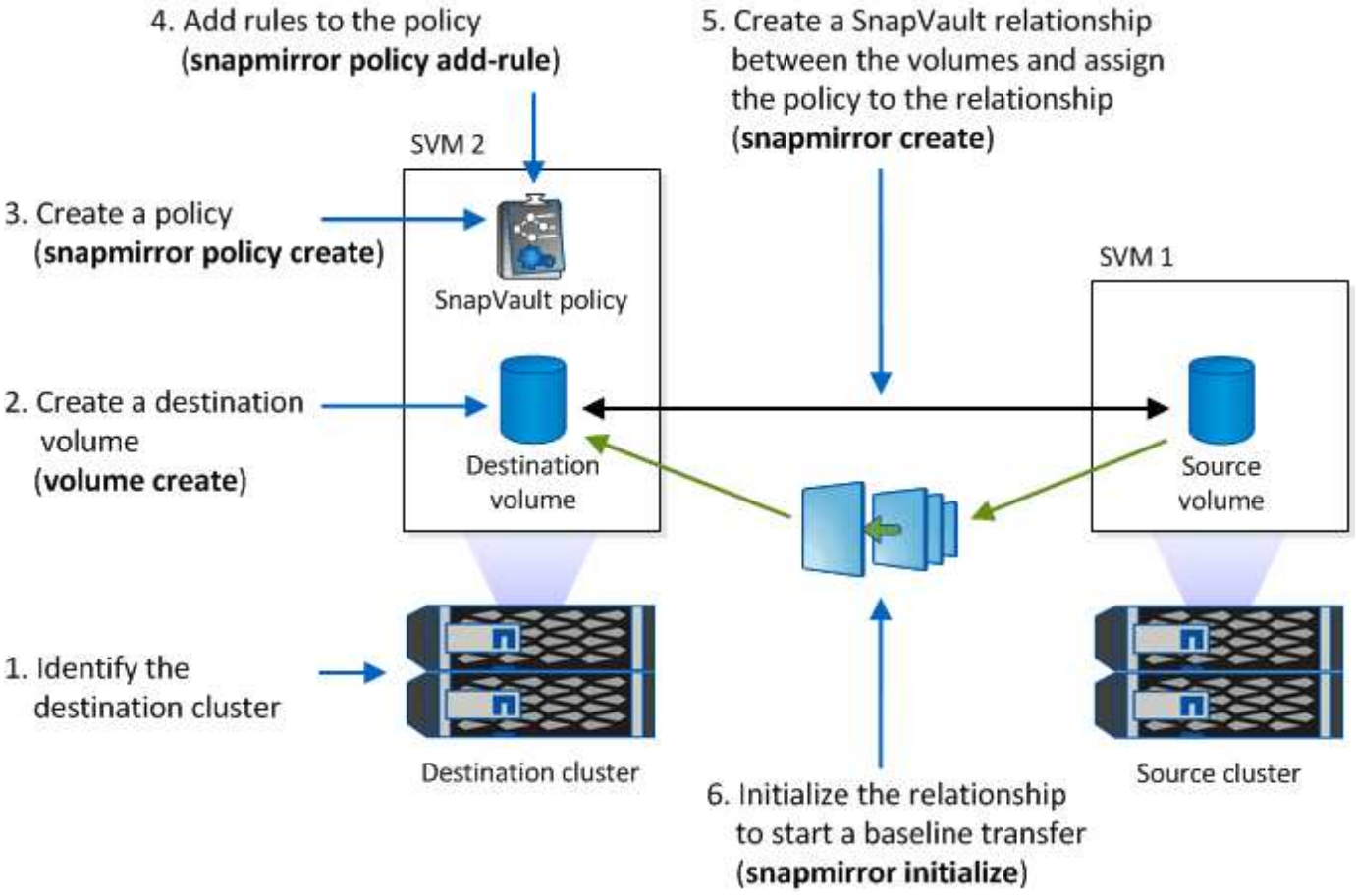
ONTAP 9.14.1부터 SnapMirror 관계의 SnapMirror 정책에서 특정 SnapMirror 레이블에 대한 보존 기간을 지정하여 소스에서 대상 볼륨으로의 복제된 스냅샷이 규칙에 지정된 보존 기간 동안 보존되도록 할 수 있습니다. 보존 기간을 지정하지 않으면 대상 볼륨의 기본 보존 기간이 사용됩니다.

ONTAP 9.13.1부터 옵션을 로 설정한 `non-snaplock` 상태로 FlexClone을 생성하고 볼륨 클론 생성 작업을 실행할 때 스냅샷을 "상위-스냅샷"으로 지정하여 SnapLock 소산 관계의 대상 SnapLock 볼륨에서 잠긴 스냅샷을 즉시 복원할 수 있습니다 `snaplock-type`. 에 대해 자세히 "SnapLock 형식으로 FlexClone 볼륨 생성"알아보십시오.

MetroCluster 구성의 경우 다음 사항에 유의해야 합니다.

- 동기식 소스 SVM과 동기식-타겟 SVM 간에는 동기식-소스 SVM 사이만이 아니라 SnapVault 관계를 생성할 수 있습니다.
- 동기화 소스 SVM의 볼륨에서 데이터 지원 SVM으로 SnapVault 관계를 생성할 수 있습니다.
- 데이터 지원 SVM의 볼륨에서 동기화 소스 SVM의 DP 볼륨으로 SnapVault 관계를 생성할 수 있습니다.

다음 그림에서는 SnapLock 볼트 관계를 초기화하는 절차를 보여 줍니다.



단계

ONTAP CLI를 사용하여 SnapLock 볼트 관계를 만들거나, ONTAP 9.15.1부터 시스템 관리자를 사용하여 SnapLock 볼트 관계를 만들 수 있습니다.

시스템 관리자

1. 볼륨이 아직 없는 경우 소스 클러스터에서 * 스토리지 > 볼륨 * 으로 이동한 후 * 추가 * 를 선택합니다.
2. Add Volume * (볼륨 추가 *) 창에서 * More Options * (추가 옵션 *)를 선택합니다.
3. 볼륨 이름, 크기, 엑스포트 정책 및 공유 이름을 입력합니다.
4. 변경 사항을 저장합니다.
5. 대상 클러스터에서 * 보호 > 관계 * 로 이동합니다.
6. 소스 * 열 위에서 * 보호 * 를 선택하고 메뉴에서 * 볼륨 * 을 선택합니다.
7. protect volumes * 창에서 보호 정책으로 * Vault * 를 선택합니다.
8. 소스 * 섹션에서 보호할 클러스터, 스토리지 VM 및 볼륨을 선택합니다.
9. 대상 * 섹션의 * 구성 세부 정보 * 에서 * 대상 스냅샷 잠금 * 을 선택한 다음 잠금 방법으로 * SnapLock for SnapVault * 를 선택합니다. * 선택한 정책 유형이 유형이 아닌 경우, SnapLock 라이센스가 설치되지 않았거나 규정 준수 클록이 초기화되지 않은 경우 * 잠금 방법 * 이 표시되지 `vault` 않습니다.
10. 아직 활성화되지 않은 경우 * SnapLock 준수 클럭 초기화 * 를 선택합니다.
11. 변경 사항을 저장합니다.

CLI를 참조하십시오

1. 대상 클러스터에서 소스 볼륨보다 크거나 같은 dP 유형의 SnapLock 대상 볼륨을 생성합니다.

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise> -type DP
-size <size>
```

다음 명령을 실행하면 이름이 2GB SnapLock Compliance 볼륨이 생성됩니다 `dstvolB` 인치 `SVM2` 애그리케이트 `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

2. 대상 클러스터에서 "기본 보존 기간을 설정합니다".
3. "새 복제 관계를 생성합니다" 비 SnapLock 소스와 사용자가 생성한 새 SnapLock 대상 간

이 예에서는 매일 및 매주 레이블이 지정된 스냅샷을 시간별 일정에 따라 볼팅하는 정책을 사용하여 `XDPDefault` 대상 SnapLock 볼륨과의 새로운 SnapMirror 관계를 `dstvolB` 생성합니다.

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```

"사용자 지정 복제 정책을 생성합니다" 또는 a "사용자 지정 일정" 사용 가능한 기본값이 적합하지 않은 경우

4. 대상 SVM에서 생성된 SnapVault 관계를 초기화합니다.

```
snapmirror initialize -destination-path <destination_path>
```

다음 명령을 실행하면 'VM1'의 소스 볼륨 'rcvolA'와 'VM2'의 대상 볼륨 'dstvolB'의 관계가 초기화됩니다.

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

5. 관계가 초기화되고 유휴 상태가 되면 대상에서 명령을 사용하여 `snapshot show` 복제된 스냅샷에 적용되는 SnapLock 만료 시간을 확인합니다.

이 예에서는 SnapMirror 레이블과 SnapLock 만료 날짜가 있는 볼륨의 스냅숏을 `dstvolB` 나열합니다.

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
snapmirror-label, snaplock-expiry-time
```

관련 정보

- "클러스터 및 SVM 피어링"
- "SnapVault를 사용한 볼륨 백업"
- "SnapMirror 초기화"

ONTAP SnapMirror 사용하여 재해 복구를 위한 **WORM** 파일 미러링

SnapMirror를 사용하여 재해 복구 및 기타 목적으로 WORM 파일을 다른 지리적 위치에 복제할 수 있습니다. 소스 볼륨과 타겟 볼륨을 모두 SnapLock에 대해 구성해야 하며 두 볼륨 모두 동일한 SnapLock 모드, Compliance 또는 Enterprise를 사용해야 합니다. 볼륨과 파일의 모든 주요 SnapLock 속성이 복제됩니다.

필수 구성 요소

피어링된 SVM이 있는 클러스터에서 소스 및 타겟 볼륨을 생성해야 합니다. 자세한 내용은 을 "클러스터 및 SVM 피어링"참조하십시오.

이 작업에 대해

- ONTAP 9.5부터 DP(데이터 보호) 유형 관계가 아닌 XDP(확장된 데이터 보호) 유형의 SnapMirror 관계로 WORM 파일을 복제할 수 있습니다. XDP 모드는 ONTAP 버전에 독립적이며 동일한 블록에 저장된 파일을 구분할 수 있으므로 복제된 Compliance 모드 볼륨을 재동기화하는 것이 훨씬 쉬워집니다. 기존 DP 유형 관계를 XDP 유형 관계로 변환하는 방법에 대한 자세한 내용은 을 참조하십시오 "데이터 보호".
- SnapLock에서 데이터 손실을 결정하면 DP 유형의 SnapMirror 관계에 대한 재동기화 작업이 Compliance-Mode 볼륨에 대해 실패합니다. 재동기화 작업이 실패하면 "volume clone create" 명령을 사용하여 대상 볼륨의 클론을 생성할 수 있습니다. 그런 다음 소스 볼륨을 클론과 다시 동기화할 수 있습니다.
- SnapLock 볼륨의 SnapMirror 관계는 다음을 지원합니다. `MirrorAllSnapshots` async-mirror 유형의 정책입니다. SnapLock 볼륨의 보존 기간은 볼륨이 보유하고 있는 모든 WORM 파일 중 최대 보존 기간에 따라

결정됩니다. 대상이 소스의 DR 복사본이므로 대상 SnapLock 볼륨의 보존 기간은 소스와 동일합니다.

- SnapLock 호환 볼륨 간의 XDP 유형의 SnapMirror 관계는 중단 후 대상의 데이터가 소스(중단 후)에서 분기된 경우에도 중단 후 재동기화를 지원합니다.

  재동기화에서 일반 스냅샷을 넘어 소스 간에 데이터 발산이 감지되면 대상에서 새 스냅샷이 잘려 이러한 발산을 캡처합니다. 새 스냅샷과 공통 스냅샷은 모두 다음과 같이 보존 시간으로 잠깁니다.

  - 대상의 볼륨 만료 시간입니다
  - 볼륨 만료 시간이 지난 시간이거나 설정되지 않은 경우 스냅샷이 30일 동안 잠깁니다
  - 대상에 법적 보류가 있는 경우 실제 볼륨 만료 기간이 마스킹되고 "무제한"으로 표시됩니다. 그러나 실제 볼륨 만료 기간 동안 스냅샷은 잠깁니다.

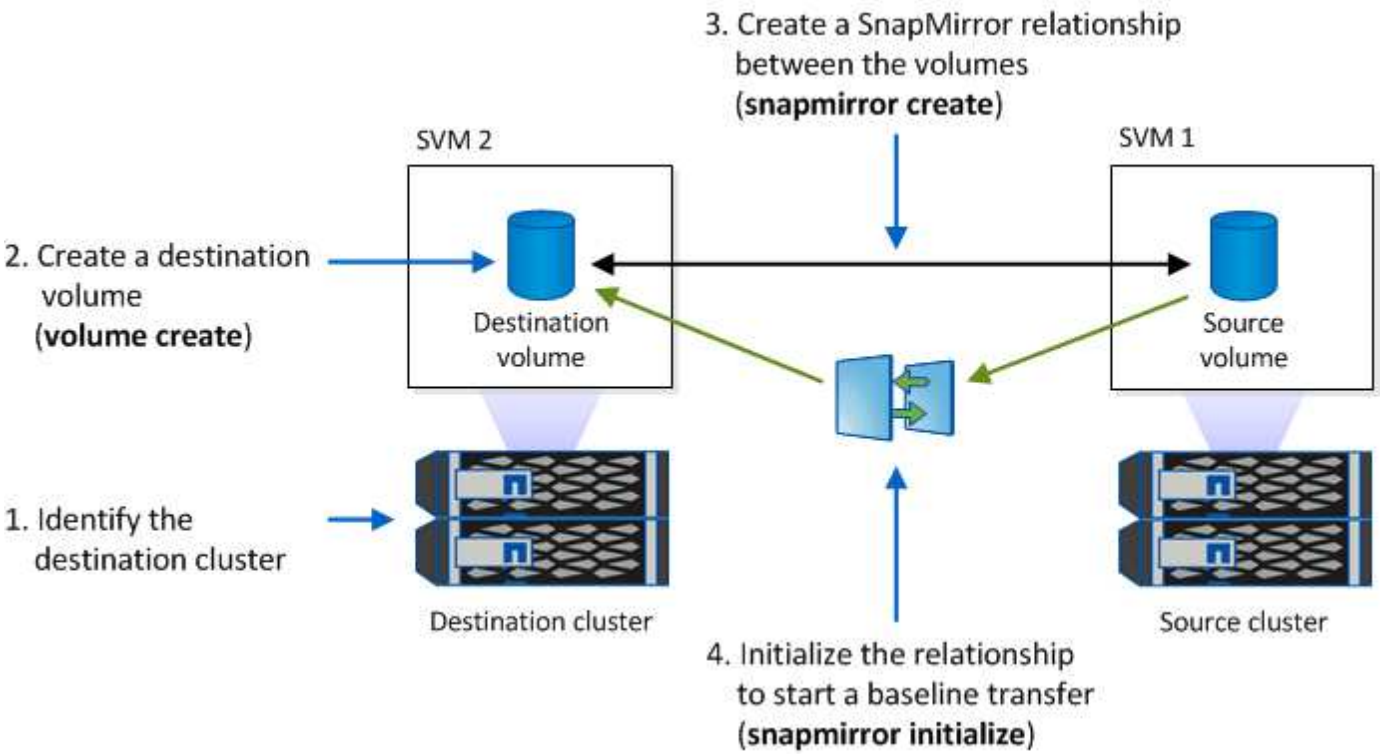
대상 볼륨의 만료 기간이 소스보다 이후인 경우 대상 만료 기간이 유지되고 재동기화 후 소스 볼륨의 만료 기간에 의해 덮어쓰이지 않습니다.

대상과 소스가 다른 법적 구속이 있는 대상에는 재동기화가 허용되지 않습니다. 재동기화를 시도하기 전에 소스와 대상에서 동일한 법적 증거 자료 보관 또는 모든 법적 고지를 해제해야 합니다.

다양한 데이터를 캡처하기 위해 생성된 대상 볼륨의 잠긴 스냅샷은 CLI를 사용하여 소스에 복사할 수 있습니다 `snapmirror update -s snapshot`. 복제된 스냅샷은 소스에서 계속 잠깁니다.

- SVM 데이터 보호 관계는 지원되지 않습니다.
- 로드 공유 데이터 보호 관계는 지원되지 않습니다.

다음 그림에서는 SnapMirror 관계를 초기화하는 절차를 보여 줍니다.



시스템 관리자

ONTAP 9.12.1부터 System Manager를 사용하여 WORM 파일의 SnapMirror 복제를 설정할 수 있습니다.

단계

1. Storage > Volumes * 로 이동합니다.
2. 표시/숨기기 * 를 클릭하고 * SnapLock 유형 * 을 선택하여 * 볼륨 * 창에 열을 표시합니다.
3. SnapLock 볼륨을 찾습니다.
4. 을 ⋮ 클릭하고 * 보호 * 를 선택합니다.
5. 대상 클러스터와 대상 스토리지 VM을 선택합니다.
6. 추가 옵션 * 을 클릭합니다.
7. 기존 정책 표시 * 를 선택하고 * DPDefault(레거시) * 를 선택합니다.
8. Destination Configuration details * 섹션에서 * Override transfer schedule * 을 선택하고 * hourly * 를 선택합니다.
9. 저장 * 을 클릭합니다.
10. 소스 볼륨 이름 왼쪽의 화살표를 클릭하여 볼륨 세부 정보를 확장하고 페이지 오른쪽의 원격 SnapMirror 보호 세부 정보를 검토합니다.
11. 원격 클러스터에서 * 보호 관계 * 로 이동합니다.
12. 관계를 찾고 대상 볼륨 이름을 클릭하여 관계 세부 정보를 봅니다.
13. 대상 볼륨 SnapLock 유형 및 기타 SnapLock 정보를 확인합니다.

CLI를 참조하십시오

1. 대상 클러스터를 식별합니다.
2. 대상 클러스터에서"SnapLock 라이센스를 설치합니다", "준수 시계를 초기화합니다"및 9.10.1 이전의 ONTAP 릴리즈를 사용하는 경우,"SnapLock 애그리게이트를 생성합니다"
3. 대상 클러스터에서 소스 볼륨과 크기가 같거나 더 큰 dP 유형의 SnapLock 대상 볼륨을 생성합니다.

   '* 볼륨 생성 - vserver_SVM_name_-volume_volume_name_-aggregate_aggregate_name_-snaplock-type compliance|enterprise-type dp-size_size_ *'

   > ⓘ ONTAP 9.10.1부터 SnapLock 볼륨과 SnapLock 아닌 볼륨이 동일한 집계에 존재할 수 있습니다. 따라서 ONTAP 9.10.1을 사용하는 경우 별도의 SnapLock 집계를 만들 필요가 없습니다. 볼륨 -snaplock-type 옵션을 사용하여 규정 준수 또는 엔터프라이즈 SnapLock 볼륨 유형을 지정합니다. ONTAP 9.10.1 이전의 ONTAP 릴리스에서는 SnapLock 모드(규정 준수 또는 엔터프라이즈)가 집계에서 상속되었습니다. 대상 볼륨의 언어 설정은 소스 볼륨의 언어 설정과 일치해야 합니다.

   다음 명령을 실행하면 node01_aggr 집계 'sVM2'에 dstvolB라는 이름의 2GB SnapLock 'Compliance' 볼륨이 생성됩니다.

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. 대상 SVM에서 SnapMirror 정책을 생성합니다.

   `snapmirror policy create -vserver SVM_name -policy policy_name`

   다음 명령을 실행하면 SVM 전체의 정책 'VM1-mirror'가 생성됩니다.

   ```
   SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
   ```

5. 대상 SVM에서 SnapMirror 일정을 생성합니다.

   '* 작업 일정 cron create-name_schedule_name_-DayOfWeek_day_of_week_-hour_hour_-minute_minute_*'

   다음 명령을 실행하면 "weekendcron"이라는 SnapMirror 스케줄이 생성됩니다.

   ```
   SVM2::> job schedule cron create -name weekendcron -dayofweek
   "Saturday, Sunday" -hour 3 -minute 0
   ```

6. 대상 SVM에서 SnapMirror 관계 생성:

   `snapmirror create -source-path source_path -destination-path destination_path -type XDP|DP -policy policy_name -schedule schedule_name`

   다음 명령을 실행하면 'VM1'의 소스 볼륨 'rcvolA'와 'VM2'의 대상 볼륨 'dstvolB'의 SnapMirror 관계가 생성되고 정책 'VM1-mirror'와 스케줄 'weekendcron'이 할당됩니다.

   ```
   SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
   -path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
   weekendcron
   ```

   > XDP 유형은 ONTAP 9.5 이상에서 사용할 수 있습니다. ONTAP 9.4 이전 버전에서 DP 유형을 사용해야 합니다.

7. 대상 SVM에서 SnapMirror 관계를 초기화합니다.

   `snapmirror initialize -destination-path destination_path`

   초기화 프로세스는 대상 볼륨에 대해 _baseline 전송_을 수행합니다. SnapMirror는 소스 볼륨의 스냅샷을 만든 다음 복사본과 이 복사본이 타겟 볼륨에 참조하는 모든 데이터 블록을 전송합니다. 또한 소스 볼륨의 다른 모든 스냅샷을 대상 볼륨으로 전송합니다.

   다음 명령을 실행하면 'VM1'의 소스 볼륨 'rcvolA'와 'VM2'의 대상 볼륨 'dstvolB'의 관계가 초기화됩니다.

   ```
   SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
   ```

관련 정보

- "클러스터 및 SVM 피어링"
- "볼륨 재해 복구 준비"
- "데이터 보호"
- "SnapMirror 생성"
- "SnapMirror 초기화"
- "스냅미러 정책 생성"

ONTAP SnapLock Legal Hold를 사용하여 소송 중 **WORM** 파일 보관

ONTAP 9.3부터는 *Legal Hold* 기능을 사용하여 소송 기간 동안 준수 모드 WORM 파일을 보존할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 SnapLock 관리자여야 합니다.

  "SnapLock 관리자 계정을 만듭니다"

- 보안 연결(SSH, 콘솔 또는 ZAPI)에 로그인해야 합니다.

이 작업에 대해

법적 증거 자료 보관 아래에 있는 파일은 무기한 보존 기간이 있는 WORM 파일처럼 작동합니다. 법적 증거 자료 보관 기간이 끝나는 시기를 지정하는 것은 귀하의 책임입니다.

법적 증거 자료 보관 아래에 넣을 수 있는 파일 수는 볼륨에서 사용 가능한 공간에 따라 다릅니다.

단계

1. 법적 증거 자료 보관 시작:

   ```
   snaplock legal-hold begin -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   다음 명령은 'vol1'의 모든 파일에 대해 법적 대기를 시작합니다.

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1
   -volume vol1 -path /
   ```

2. 법적 증거 자료 보관 종료:

   ```
   snaplock legal-hold end -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   다음 명령은 'vol1'의 모든 파일에 대해 법적 보류를 종료합니다.

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

관련 정보

- "SnapLock 법적 증거 자료 보관 이 시작됩니다"
- "SnapLock 법적 증거 자료 보관 종료"

ONTAP SnapLock 사용하여 **WORM** 파일 삭제

권한 있는 삭제 기능을 사용하여 보존 기간 동안 엔터프라이즈 모드 WORM 파일을 삭제할 수 있습니다. 이 기능을 사용하려면 먼저 SnapLock 관리자 계정을 만든 다음 계정을 사용하여 기능을 활성화해야 합니다.

SnapLock 관리자 계정을 만듭니다

권한 있는 삭제를 수행하려면 SnapLock 관리자 권한이 있어야 합니다. 이러한 권한은 vsadmin-SnapLock 역할에 정의되어 있습니다. 해당 역할이 아직 할당되지 않은 경우 클러스터 관리자에게 SnapLock 관리자 역할을 가진 SVM 관리자 계정을 만들도록 요청할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 보안 연결(SSH, 콘솔 또는 ZAPI)에 로그인해야 합니다.

단계

1. SnapLock 관리자 역할을 사용하여 SVM 관리자 계정을 생성합니다.

   '* 보안 로그인 create-vserver_SVM_name_-user-or-group-name_user_or_group_name_-application_application_-AuthMethod_authentication_method_-role_role_-comment_comment_*'

   다음 명령을 실행하면 사전 정의된 "vsadmin-snaplock" 역할을 사용하여 SVM 관리자 계정 'napLockAdmin'에서 암호를 사용하여 'VM1'에 액세스할 수 있습니다.

   ```
   cluster1::> security login create -vserver SVM1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role vsadmin-
   snaplock
   ```

   에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

권한 있는 삭제 기능을 활성화합니다

삭제하려는 WORM 파일이 포함된 엔터프라이즈 볼륨에서 권한 있는 삭제 기능을 명시적으로 활성화해야 합니다.

이 작업에 대해

'-privileged-delete' 옵션의 값은 권한 있는 삭제 활성화 여부를 결정합니다. 가능한 값은 '사용', '사용 안 함', '영구 사용 안 함'입니다.

영구 불활성 상태가 단자다. 상태를 "영구 비활성화"로 설정한 후에는 볼륨에 대한 권한 있는 삭제를 활성화할 수 없습니다.

단계

1. SnapLock 엔터프라이즈 볼륨에 대한 권한 있는 삭제 활성화:

   '* volume SnapLock modify -vserver_SVM_name_-volume_volume_name_-privileged-delete disabled|enabled|permanently-disabled *

   다음 명령을 실행하면 'VM1'의 엔터프라이즈 볼륨 'dataVol'에 대한 권한 있는 삭제 기능이 활성화됩니다.

```
SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
-delete enabled
```

엔터프라이즈 모드 **WORM** 파일을 삭제합니다

권한이 있는 삭제 기능을 사용하여 보존 기간 동안 엔터프라이즈 모드 WORM 파일을 삭제할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 SnapLock 관리자여야 합니다.
- SnapLock 감사 로그를 생성하고 엔터프라이즈 볼륨에서 권한 있는 삭제 기능을 활성화해야 합니다.

이 작업에 대해

만료된 WORM 파일을 삭제하려면 권한이 있는 삭제 작업을 사용할 수 없습니다. 명령을 사용하여 `volume file retention show` 삭제하려는 WORM 파일의 보존 시간을 볼 수 있습니다. 에 대한 자세한 내용은 `volume file retention show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 엔터프라이즈 볼륨에서 WORM 파일 삭제:

   '* 볼륨 파일 권한이 있는-삭제-vserver_SVM_name_-file_file_path_*'

   다음 명령을 실행하면 SVM 'sVM1'에서 파일 '/vol/dataVol/F1'이 삭제됩니다.

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

ONTAP SnapLock 볼륨 이동

ONTAP 9.8부터 SnapLock 볼륨을 엔터프라이즈부터 규정 준수까지 동일한 유형의 대상 Aggregate로 이동할 수 있습니다. SnapLock 볼륨을 이동하려면 SnapLock 보안 역할이 할당되어야 합니다.

SnapLock 보안 관리자 계정을 만듭니다

SnapLock 볼륨 이동을 수행하려면 SnapLock 보안 관리자 권한이 있어야 합니다. 이 권한은 ONTAP 9.8에 도입된 _SnapLock_역할을 통해 부여됩니다. 해당 역할이 아직 할당되지 않은 경우 클러스터 관리자에게 이 SnapLock 보안 역할을 가진 SnapLock 보안 사용자를 만들도록 요청할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 보안 연결(SSH, 콘솔 또는 ZAPI)에 로그인해야 합니다.

이 작업에 대해

SnapLock 역할은 데이터 SVM과 연결된 vsadmin-SnapLock 역할과는 달리 관리 SVM과 연결됩니다.

단계

1. SnapLock 관리자 역할을 사용하여 SVM 관리자 계정을 생성합니다.

   '* 보안 로그인 create-vserver_SVM_name_-user-or-group-name_user_or_group_name_-application_application_-AuthMethod_authentication_method_-role_role_-comment_comment_*'

   다음 명령을 실행하면 미리 정의된 "SnapLock" 역할을 사용하여 SVM 관리자 계정 'napLockAdmin'에서 암호를 사용하여 admin SVM 'cluster1'에 액세스할 수 있습니다.

   ```
   cluster1::> security login create -vserver cluster1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role snaplock
   ```

   에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

SnapLock 볼륨을 이동합니다

'volume move' 명령을 사용하여 SnapLock 볼륨을 대상 애그리게이트로 이동할 수 있습니다.

시작하기 전에

- SnapLock 볼륨 이동을 수행하기 전에 SnapLock으로 보호되는 감사 로그를 생성해야 합니다.

  "감사 로그를 생성합니다".

- ONTAP 9.10.1 이전 버전의 ONTAP를 사용하는 경우 대상 애그리게이트는 이동할 SnapLock 볼륨과 동일한 SnapLock 유형이어야 합니다. Compliance to Compliance 또는 Enterprise to Enterprise입니다. ONTAP 9.10.1부터는 이러한 제한이 없어지기 때문에 aggregate에 Compliance 및 Enterprise SnapLock 볼륨과 비 SnapLock 볼륨이 모두 포함될 수 있습니다.
- SnapLock 보안 역할을 가진 사용자여야 합니다.

단계

1. 보안 연결을 사용하여 ONTAP 클러스터 관리 LIF에 로그인합니다.

   ' * ssh SnapLock_user@cluster_mgmt_ip *'

2. SnapLock 볼륨 이동:

'* volume move start -vserver_SVM_name_-volume_snaplock_volume_name_-destination -aggregate_destination_name_*'

3. 볼륨 이동 작업의 상태를 확인합니다.

   '* 볼륨 이동 표시 -volume_snaplock_volume_name_-vserver_SVM_name_-필드 볼륨, 단계, SVM*

랜섬웨어 공격으로부터 보호하기 위해 **ONTAP** 스냅샷 잠금

ONTAP 9.12.1부터 비 SnapLock 볼륨에서 스냅샷을 잠가 랜섬웨어 공격으로부터 보호할 수 있습니다. 스냅샷을 잠그면 실수로 또는 악의적으로 삭제할 수 없습니다.

만료 시간에 도달할 때까지 스냅샷을 삭제할 수 없도록 SnapLock Compliance 시계 기능을 사용하여 지정된 기간 동안 스냅샷을 잠급니다. 스냅샷을 잠그면 무단 변경이 방지되어 랜섬웨어 위협으로부터 보호할 수 있습니다. 볼륨이 랜섬웨어 공격에 의해 손상된 경우 잠긴 스냅샷을 사용하여 데이터를 복구할 수 있습니다.

ONTAP 9.14.1부터 스냅샷 잠금은 SnapLock 볼트 대상 및 비 SnapLock SnapMirror 대상 볼륨에서 장기 보존 스냅샷을 지원합니다. 에 연결된 SnapMirror 정책 규칙을 사용하여 보존 기간을 설정하여 스냅샷 잠금을 기존 정책 레이블설정할 수 있습니다. 이 규칙은 볼륨에 설정된 기본 보존 기간을 재정의합니다. SnapMirror 레이블과 연결된 보존 기간이 없으면 볼륨의 기본 보존 기간이 사용됩니다.

변조 방지 스냅샷 요구사항 및 고려사항

- ONTAP CLI를 사용하는 경우 클러스터의 모든 노드에서 ONTAP 9.12.1 이상을 실행해야 합니다. System Manager를 사용하는 경우 모든 노드에서 ONTAP 9.13.1 이상을 실행해야 합니다.
- "SnapLock 라이센스가 클러스터에 설치되어 있어야 합니다".. 이 라이센스는 에 "ONTAP 1 을 참조하십시오 "포함되어 있습니다.
- "클러스터의 규정 준수 클록을 초기화해야 합니다"..
- 볼륨에 스냅샷 잠금이 설정되어 있으면 클러스터를 ONTAP 9.12.1 이후의 ONTAP 버전으로 업그레이드할 수 있지만, 잠긴 스냅샷이 모두 만료 날짜에 도달하여 삭제되고 스냅샷 잠금이 해제될 때까지 이전 버전의 ONTAP로 되돌릴 수 없습니다.
- 스냅샷이 잠기면 볼륨 만료 시간이 스냅샷의 만료 시간으로 설정됩니다. 두 개 이상의 스냅샷이 잠겨 있는 경우 볼륨 만료 시간은 모든 스냅샷 중에서 가장 긴 만료 시간을 반영합니다.
- 잠긴 스냅샷의 보존 기간이 스냅샷 유지 수보다 우선합니다. 즉, 잠긴 스냅샷에 대한 스냅샷 보존 기간이 만료되지 않은 경우에는 유지 수 제한이 적용되지 않습니다.
- SnapMirror 관계에서 미러 볼트 정책 규칙에 보존 기간을 설정할 수 있으며 대상 볼륨에 스냅샷 잠금이 활성화된 경우 대상에 복제된 스냅샷에 보존 기간이 적용됩니다. 보존 기간이 유지 수보다 우선합니다. 예를 들어 만료 기간이 경과하지 않은 스냅샷은 유지 수를 초과하더라도 유지됩니다.
- 비 SnapLock 볼륨에서 스냅샷 이름을 바꿀 수 있습니다. SnapMirror 관계의 운영 볼륨에 대한 스냅샷 이름 바꾸기 작업은 정책이 MirrorAllSnapshots인 경우에만 보조 볼륨에 반영됩니다. 다른 정책 유형의 경우 이름이 바뀐 스냅샷은 업데이트 중에 전파되지 않습니다.
- ONTAP CLI를 사용하는 경우 잠긴 스냅샷이 가장 최근의 스냅샷인 경우에만 명령을 사용하여 잠긴 스냅샷을 복구할 수 `volume snapshot restore` 있습니다. 복구 중인 스냅샷보다 나중에 만료되지 않은 스냅샷이 있는 경우 스냅샷 복구 작업이 실패합니다.

변조 방지 스냅샷에서 지원되는 기능

- "Cloud Volumes ONTAP"

- FlexGroup 볼륨

  스냅샷 잠금은 FlexGroup 볼륨에 대해 지원됩니다. 스냅샷 잠금은 루트 구성 요소 스냅샷에서만 발생합니다. FlexGroup 볼륨은 루트 구성 요소 만료 시간이 경과한 경우에만 삭제할 수 있습니다.

- FlexVol에서 FlexGroup로의 변환

  잠긴 스냅샷이 있는 FlexVol volume를 FlexGroup 볼륨으로 변환할 수 있습니다. 변환 후에도 스냅샷은 잠긴 상태로 유지됩니다.

- SnapMirror 비동기

  소스와 대상 모두에서 컴플라이언스 클록을 초기화해야 합니다.

- SVM 데이터 이동성(소스 클러스터에서 타겟 클러스터로 SVM을 마이그레이션 또는 재배치하는 데 사용)

  ONTAP 9.14.1부터 지원됩니다.

- 를 사용하는 SnapMirror 정책 규칙입니다 `-schedule` 매개 변수
- SVM DR

  소스와 대상 모두에서 컴플라이언스 클록을 초기화해야 합니다.

- 볼륨 클론 및 파일 클론

  잠긴 스냅샷에서 볼륨 클론 및 파일 클론을 생성할 수 있습니다.

- FlexCache 볼륨

  ONTAP 9.16.1부터 지원됩니다.

지원되지 않는 기능입니다

다음 기능은 현재 변조 방지 스냅샷에서 지원되지 않습니다.

- 정합성 보장 그룹
- "FabricPool"

  변조 방지 스냅샷은 삭제할 수 없는 변경 불가능한 보호를 제공합니다. FabricPool에는 데이터 삭제 기능이 필요하므로 동일한 볼륨에서 FabricPool 및 스냅샷 잠금을 활성화할 수 없습니다.

- SMTape
- SnapMirror 활성 동기화
- SnapMirror 동기식

볼륨을 생성할 때 스냅샷 잠금을 설정합니다

ONTAP 9.12.1부터 새 볼륨을 생성할 때 또는 CLI에서 및 `volume modify` 명령의 옵션을 `volume create` 사용하여 기존 볼륨을 수정할 때 스냅샷 잠금을 설정할 수 있습니다 `-snapshot-locking-enabled`. ONTAP 9.13.1부터 System Manager를 사용하여 스냅샷 잠금을 설정할 수 있습니다.

시스템 관리자

1. Storage > Volumes * 로 이동하고 * Add * 를 선택합니다.
2. Add Volume * (볼륨 추가 *) 창에서 * More Options * (추가 옵션 *)를 선택합니다.
3. 볼륨 이름, 크기, 엑스포트 정책 및 공유 이름을 입력합니다.
4. 스냅샷 잠금 사용 * 을 선택합니다. SnapLock 라이센스가 설치되지 않은 경우에는 이 선택 항목이 표시되지 않습니다.
5. 아직 활성화되지 않은 경우 * SnapLock 준수 클럭 초기화 * 를 선택합니다.
6. 변경 사항을 저장합니다.
7. 볼륨 * 창에서 업데이트한 볼륨을 선택하고 * 개요 * 를 선택합니다.
8. SnapLock 스냅샷 잠금 * 이 * 사용 * 으로 표시되는지 확인합니다.

CLI를 참조하십시오

1. 새 볼륨을 생성하고 스냅샷 잠금을 설정하려면 다음 명령을 입력합니다.

   ```
   volume create -vserver <vserver_name> -volume <volume_name> -snapshot
   -locking-enabled true
   ```

   다음 명령을 실행하면 vol1이라는 새 볼륨에 대한 스냅샷 잠금이 설정됩니다.

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: snapshot locking is being enabled on volume "vol1" in
   Vserver "vs1". It cannot be disabled until all locked snapshots are
   past their expiry time. A volume with unexpired locked snapshots
   cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

기존 볼륨에 대한 스냅샷 잠금을 설정합니다

ONTAP 9.12.1부터 ONTAP CLI를 사용하여 기존 볼륨에 대한 스냅샷 잠금을 설정할 수 있습니다. ONTAP 9.13.1부터 System Manager를 사용하여 기존 볼륨에 대한 스냅샷 잠금을 설정할 수 있습니다.

시스템 관리자

1. Storage > Volumes * 로 이동합니다.
2. 를 ⋮ 선택하고 * 편집 > 볼륨 * 을 선택합니다.
3. 볼륨 편집 * 창에서 스냅샷(로컬) 설정 섹션을 찾아 * 스냅샷 잠금 활성화 * 를 선택합니다.

   SnapLock 라이센스가 설치되지 않은 경우에는 이 선택 항목이 표시되지 않습니다.

4. 아직 활성화되지 않은 경우 * SnapLock 준수 클럭 초기화 * 를 선택합니다.
5. 변경 사항을 저장합니다.
6. 볼륨 * 창에서 업데이트한 볼륨을 선택하고 * 개요 * 를 선택합니다.
7. * SnapLock 스냅샷 잠금*이 *활성화*로 표시되는지 확인합니다.

CLI를 참조하십시오

1. 기존 볼륨을 수정하여 스냅샷 잠금을 설정하려면 다음 명령을 입력합니다.

```
volume modify -vserver <vserver_name> -volume <volume_name> -snapshot
-locking-enabled true
```

잠긴 스냅샷 정책을 생성하고 보존을 적용합니다

ONTAP 9.12.1부터 스냅샷 정책을 생성하여 스냅샷 보존 기간을 적용하고 볼륨에 정책을 적용하여 지정된 기간 동안 스냅샷을 잠글 수 있습니다. 보존 기간을 수동으로 설정하여 스냅샷을 잠글 수도 있습니다. ONTAP 9.13.1부터 System Manager를 사용하여 스냅샷 잠금 정책을 생성하여 볼륨에 적용할 수 있습니다.

스냅샷 잠금 정책을 생성합니다

시스템 관리자

1. 스토리지 > 스토리지 VM * 으로 이동하여 스토리지 VM을 선택합니다.
2. 설정 * 을 선택합니다.
3. Snapshot Policies * 를 찾아 선택합니다 →.
4. 스냅샷 정책 추가 * 창에서 정책 이름을 입력합니다.
5. 를 선택합니다 + Add .
6. 스케줄 이름, 유지할 최대 스냅샷 및 SnapLock 보존 기간을 포함한 스냅샷 스케줄 세부 정보를 제공합니다.
7. SnapLock 보존 기간 * 열에 스냅샷을 보존할 시간, 일, 월 또는 년 수를 입력합니다. 예를 들어 보존 기간이 5일인 스냅샷 정책은 스냅샷이 생성된 시점부터 5일 동안 스냅샷을 잠그며, 이 시간 동안에는 삭제할 수 없습니다. 다음과 같은 보존 기간 범위가 지원됩니다.
   - 연도: 0-100
   - 월: 0-1200
   - 일 수: 0 - 36500
   - 시간: 0-24
8. 변경 사항을 저장합니다.

CLI를 참조하십시오

1. 스냅샷 정책을 생성하려면 다음 명령을 입력합니다.

   ```
   volume snapshot policy create -policy <policy_name> -enabled true
   -schedule1 <schedule1_name> -count1 <maximum snapshots> -retention-period1
   <retention_period>
   ```

   다음 명령을 실행하면 스냅샷 잠금 정책이 생성됩니다.

   ```
   cluster1> volume snapshot policy create -policy lock_policy -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   활성 보존 상태인 스냅샷은 대체되지 않습니다. 즉, 아직 만료되지 않은 잠긴 스냅샷이 있는 경우에는 보존 횟수가 유지되지 않습니다.

볼륨에 잠금 정책을 적용합니다

시스템 관리자

1. Storage > Volumes * 로 이동합니다.
2. 를 ⋮ 선택하고 * 편집 > 볼륨 * 을 선택합니다.
3. 볼륨 편집 * 창에서 * 스냅샷 예약 * 을 선택합니다.
4. 목록에서 스냅샷 잠금 정책을 선택합니다.
5. 스냅샷 잠금이 아직 활성화되지 않은 경우 * Enable snapshot locking * 을 선택합니다.
6. 변경 사항을 저장합니다.

CLI를 참조하십시오

1. 기존 볼륨에 스냅샷 잠금 정책을 적용하려면 다음 명령을 입력합니다.

```
volume modify -volume <volume_name> -vserver <vserver_name> -snapshot
-policy <policy_name>
```

수동 스냅샷 생성 중에 보존 기간을 적용합니다

스냅샷을 수동으로 생성할 때 스냅샷 보존 기간을 적용할 수 있습니다. 볼륨에 대해 스냅샷 잠금을 설정해야 합니다. 그렇지 않으면 보존 기간 설정이 무시됩니다.

시스템 관리자

1. Storage > Volumes * 로 이동하여 볼륨을 선택합니다.
2. 볼륨 세부 정보 페이지에서 * 스냅샷 * 탭을 선택합니다.
3. 를 선택합니다 + Add .
4. 스냅샷 이름과 SnapLock 만료 시간을 입력합니다. 보존 만료 날짜 및 시간을 선택할 달력을 선택할 수 있습니다.
5. 변경 사항을 저장합니다.
6. 볼륨 > 스냅샷 * 페이지에서 * 표시/숨기기 * 를 선택하고 * SnapLock 만료 시간 * 을 선택하여 * SnapLock 만료 시간 * 열을 표시하고 보존 시간이 설정되었는지 확인합니다.

CLI를 참조하십시오

1. 스냅샷을 수동으로 생성하고 잠금 보존 기간을 적용하려면 다음 명령을 입력합니다.

```
volume snapshot create -volume <volume_name> -snapshot <snapshot name>
-snaplock-expiry-time <expiration_date_time>
```

다음 명령을 실행하면 새 스냅샷이 생성되고 보존 기간이 설정됩니다.

```
cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
```

기존 스냅샷에 보존 기간을 적용합니다

시스템 관리자

1. Storage > Volumes * 로 이동하여 볼륨을 선택합니다.
2. 볼륨 세부 정보 페이지에서 * 스냅샷 * 탭을 선택합니다.
3. 스냅샷을 선택하고 를 선택한 다음 * SnapLock 만료 시간 수정 * 을 선택합니다. 보존 만료 날짜 및 시간을 선택할 달력을 선택할 수 있습니다.
4. 변경 사항을 저장합니다.
5. 볼륨 > 스냅샷 * 페이지에서 * 표시/숨기기 * 를 선택하고 * SnapLock 만료 시간 * 을 선택하여 * SnapLock 만료 시간 * 열을 표시하고 보존 시간이 설정되었는지 확인합니다.

CLI를 참조하십시오

1. 기존 스냅샷에 보존 기간을 수동으로 적용하려면 다음 명령을 입력합니다.

   ```
   volume snapshot modify-snaplock-expiry-time -volume <volume_name> -snapshot
   <snapshot name> -snaplock-expiry-time <expiration_date_time>
   ```

   다음 예에서는 기존 스냅샷에 보존 기간을 적용합니다.

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

기존 정책을 수정하여 장기 보존을 적용합니다

SnapMirror 관계에서 미러 볼트 정책 규칙에 보존 기간을 설정할 수 있으며 대상 볼륨에 스냅샷 잠금이 활성화된 경우 대상에 복제된 스냅샷에 보존 기간이 적용됩니다. 보존 기간이 유지 수보다 우선합니다. 예를 들어 만료 기간이 경과하지 않은 스냅샷은 유지 수를 초과하더라도 유지됩니다.

ONTAP 9.14.1부터 스냅샷의 장기 보존을 설정하는 규칙을 추가하여 기존 SnapMirror 정책을 수정할 수 있습니다. 이 규칙은 SnapLock 소산 대상 및 비 SnapLock SnapMirror 대상 볼륨에서 기본 볼륨 보존 기간을 재정의하는 데 사용됩니다.

1. 기존 SnapMirror 정책에 규칙 추가:

   ```
   snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
   -snapmirror-label <label name> -keep <number of snapshots> -retention-period
   [<integer> days|months|years]
   ```

   다음 예에서는 "LockVault"라는 기존 정책에 6개월의 보존 기간을 적용하는 규칙을 만듭니다.

   ```
   snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
   -label test1 -keep 10 -retention-period "6 months"
   ```

   에 대한 자세한 내용은 `snapmirror policy add-rule` "ONTAP 명령 참조입니다"을 참조하십시오.

정합성 보장 그룹

ONTAP 일관성 그룹에 대해 알아보세요

정합성 보장 그룹은 단일 유닛으로 관리되는 볼륨의 모음입니다. ONTAP에서 일관성 그룹을 사용하면 여러 볼륨에 걸쳐 있는 애플리케이션 워크로드를 손쉽게 관리하고 보호할 수 있습니다.

일관성 그룹을 사용하면 스토리지 관리를 간소화할 수 있습니다. 20개의 LUN을 아우르는 중요한 데이터베이스가 있다고 상상해 보십시오. LUN을 개별적으로 관리하거나 단일 정합성 보장 그룹으로 구성하여 LUN을 단일 데이터 세트로 처리할 수 있습니다.

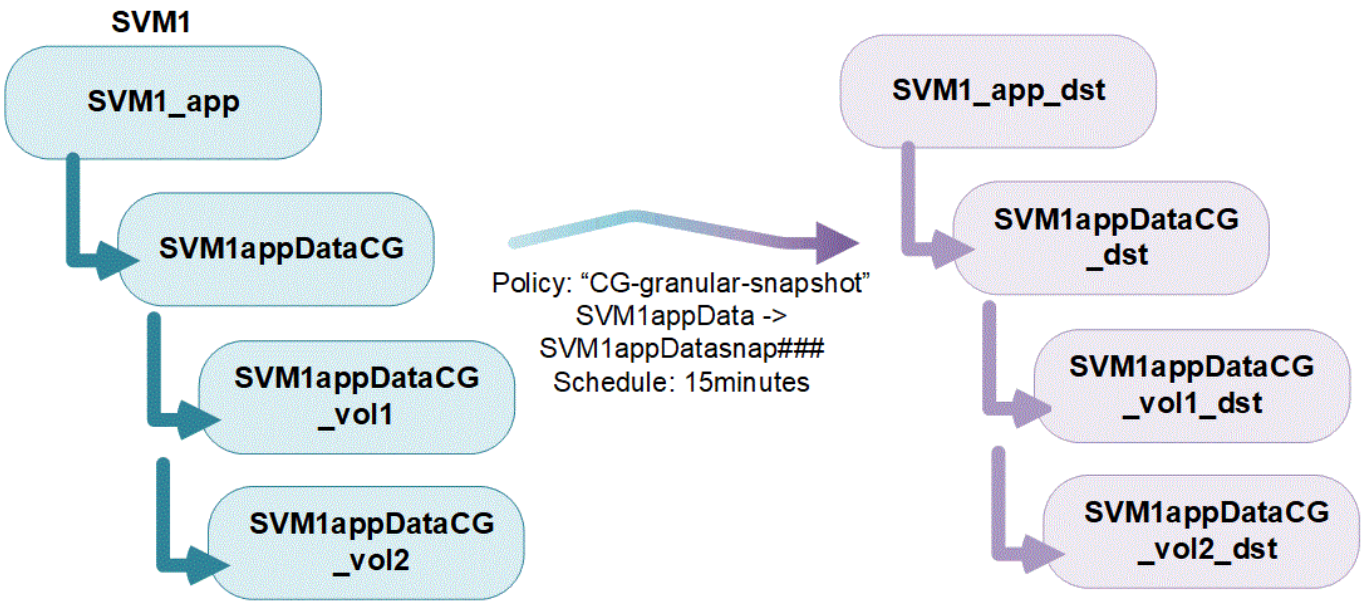
정합성 보장 그룹은 애플리케이션 워크로드 관리를 용이하게 하여, 쉽게 구성된 로컬 및 원격 보호 정책과 특정 시점에 볼륨 컬렉션에 대해 장애 발생 시 정합성이 보장되거나 애플리케이션 정합성이 보장되는 동시 스냅샷을 제공합니다. 일관성 그룹의 스냅샷을 사용하면 전체 애플리케이션 워크로드를 복구할 수 있습니다.

일관성 그룹에 대해 알아봅니다

일관성 그룹은 프로토콜(NAS, SAN 또는 NVMe)에 관계없이 모든 FlexVol 볼륨을 지원하며, ONTAP REST API를 통해 또는 System Manager의 * 스토리지 > 일관성 그룹 * 메뉴 항목에서 관리할 수 있습니다. ONTAP 9.14.1부터는 ONTAP CLI를 사용하여 일관성 그룹을 관리할 수 있습니다.

정합성 보장 그룹은 개별 엔터티(볼륨 컬렉션) 또는 다른 정합성 보장 그룹으로 구성된 계층적 관계로 존재할 수 있습니다. 개별 볼륨은 고유한 볼륨 세부 스냅샷 정책을 가질 수 있습니다. 또한 정합성 보장 그룹 전체의 스냅샷 정책이 있을 수 있습니다. 일관성 그룹에는 전체 일관성 그룹을 복구하는 데 사용할 수 있는 SnapMirror 활성 동기화 관계 및 공유 SnapMirror 정책이 하나만 있을 수 있습니다.

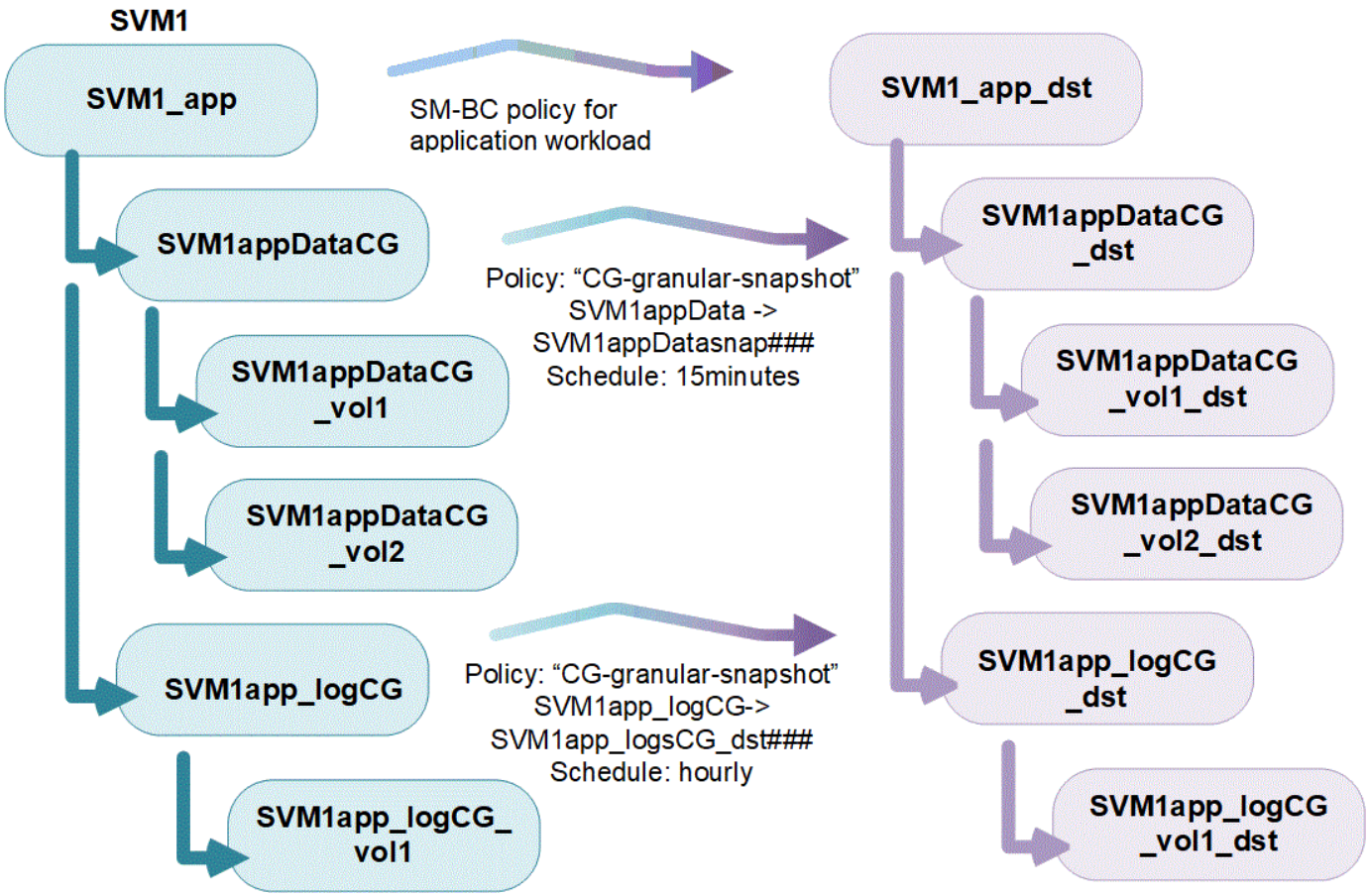
다음 다이어그램에서는 개별 일관성 그룹을 사용하는 방법을 보여 줍니다. 에서 호스팅되는 응용 프로그램의 데이터는 `SVM1` 및 의 두 볼륨에 걸쳐 `vol1` 있습니다. `vol2` 정합성 보장 그룹의 스냅샷 정책은 15분마다 데이터의 스냅샷을 캡처합니다.



애플리케이션 워크로드가 클수록 여러 개의 일관성 그룹이 필요할 수 있습니다. 이 경우 단일 일관성 그룹이 부모 일관성 그룹의 하위 구성요소가 되는 계층적 일관성 그룹을 생성할 수 있습니다. 상위 일관성 그룹에는 최대 5개의 하위 일관성 그룹이 포함될 수 있습니다. 개별 정합성 보장 그룹과 마찬가지로 원격 SnapMirror 활성 동기화 보호 정책을 정합성

보장 그룹(상위 및 하위)의 전체 구성에 적용하여 애플리케이션 워크로드를 복구할 수 있습니다.

다음 예제에서 응용 프로그램은 에서 호스팅됩니다. `SVM1` 관리자가 부모 일관성 그룹을 생성했으며 여기에는 `SVM1_app` 데이터와 `SVM1app_logCG` 로그에 대한 두 개의 하위 일관성 그룹이 `SVM1appDataCG` 포함됩니다. 각 하위 정합성 보장 그룹에는 고유한 스냅샷 정책이 있습니다. 의 볼륨 스냅샷은 `SVM1appDataCG` 15분마다 생성됩니다. 의 스냅샷은 `SVM1app_logCG` 매시간 생성됩니다. 부모 정합성 보장 그룹에는 `SVM1_app` 재해 발생 시 서비스를 지속할 수 있도록 데이터를 복제하는 SnapMirror 활성 동기화 정책이 있습니다.



ONTAP 9.12.1부터 정합성 보장 그룹이 지원됩니다 클론 복제 를 사용하여 정합성 보장 구성 구성원을 수정합니다 볼륨 추가 또는 제거 System Manager 및 ONTAP REST API 모두에서 ONTAP 9.12.1부터 ONTAP REST API는 다음을 지원합니다.

- 새 NFS 또는 SMB 볼륨 또는 NVMe 네임스페이스를 사용하여 일관성 그룹 생성
- 기존 일관성 그룹에 새 NFS 또는 SMB 볼륨 또는 NVMe 네임스페이스 추가

ONTAP REST API에 대한 자세한 내용은 를 참조하십시오 "ONTAP REST API 참조 설명서".

정합성 보장 그룹 모니터링

ONTAP 9.13.1부터 정합성 보장 그룹은 실시간 및 내역 용량과 성능 모니터링을 제공하여 애플리케이션 및 개별 정합성 보장 그룹의 성능에 대한 통찰력을 제공합니다.

모니터링 데이터는 5분마다 업데이트되고 최대 1년 동안 유지됩니다. 다음에 대한 메트릭을 추적할 수 있습니다.

- 성능: IOPS, 지연 시간, 처리량

- 용량: 크기, 사용된 논리적 용량, 사용 가능한 용량

System Manager의 정합성 보장 그룹 메뉴에 있는 개요 탭에서 모니터링 데이터를 보거나 REST API에 요청하여 모니터링 데이터를 볼 수 있습니다. ONTAP 9.14.1부터는 명령을 사용하여 CLI에서 일관성 그룹 메트릭을 볼 수 `consistency-group metrics show` 있습니다. 에 대한 자세한 내용은 `consistency-group metrics show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 9.13.1에서는 REST API를 사용하여 기간별 메트릭만 검색할 수 있습니다. ONTAP 9.14.1부터 System Manager에서 기간별 메트릭을 사용할 수 있습니다.

일관성 그룹 보호

일관성 그룹은 애플리케이션 정합성 보장 보호 기능을 제공하여 여러 볼륨 또는 LIF 전체에서 데이터 정합성을 보장합니다. 일관성 그룹의 스냅샷을 생성할 때 일관성 그룹에 "fence"가 설정됩니다. 펜스는 스냅샷 작업이 완료될 때까지 입출력에 대한 대기열을 시작하여 정합성 보장 그룹의 모든 엔티티에서 데이터의 시점 정합성을 보장합니다. 펜스는 예약된 스냅샷 정책이나 System Manager를 사용하여 스냅샷 생성과 같은 스냅샷 생성 작업 중에 일시적으로 지연 시간이 급증할 수 있습니다. REST API 및 CLI 컨텍스트에 대한 자세한 내용은 및 를 "ONTAP REST API 설명서 ""ONTAP 명령 참조입니다"참조하십시오.

정합성 보장 그룹은 다음을 통해 보호 기능을 제공합니다.

- 스냅샷 정책
- SnapMirror 활성 동기화
- [mcc] (ONTAP 9.11.1부터)
- SnapMirror 비동기 (ONTAP 9.13.1부터)
- "SVM 재해 복구" (ONTAP 9.14.1부터)

일관성 그룹을 생성해도 보호가 자동으로 설정되지는 않습니다. 정합성 보장 그룹을 생성하거나 생성한 후에 로컬 및 원격 보호 정책을 설정할 수 있습니다.

일관성 그룹에 대한 보호를 구성하려면 를 참조하십시오 "일관성 그룹 보호".

원격 보호를 사용하려면 에 대한 요구 사항을 충족해야 SnapMirror 활성 동기화합니다.

NAS 액세스를 위해 마운트된 볼륨에 SnapMirror 활성 동기화 관계를 설정할 수 없습니다.

일관성 그룹에 대한 다중 관리자 검증 지원

ONTAP 9.16.1부터 정합성 보장 그룹에 대해 MAV(다중 관리자 검증)를 사용하여 지정된 관리자의 승인 후에만 일관성 그룹 생성, 수정 또는 삭제와 같은 특정 작업을 실행할 수 있습니다. 따라서 손상되었거나 악의적이거나 경험이 부족한 관리자가 기존 구성을 원하지 않는 방식으로 변경하지 못하게 됩니다.

"자세한 정보"

MetroCluster 구성의 일관성 그룹

ONTAP 9.11.1부터 MetroCluster 구성 내에서 클러스터의 새 볼륨에 정합성 보장 그룹을 프로비저닝할 수 있습니다. 이러한 볼륨은 미러링된 Aggregate에 프로비저닝됩니다.

볼륨이 프로비저닝되면 미러링된 Aggregate와 미러링되지 않은 애그리게이트 간에 일관성 그룹에 연결된 볼륨을 이동할 수 있습니다. 따라서 일관성 그룹에 연결된 볼륨은 미러링된 애그리게이트, 미러링되지 않은 애그리게이트 또는 둘 다에 위치할 수 있습니다. 일관성 그룹에 연결된 볼륨이 포함된 미러링된 애그리게이트를 수정하여 미러링되지 않은 상태로 만들 수 있습니다. 마찬가지로, 정합성 보장 그룹과 연결된 볼륨이 포함된 미러링되지 않은 애그리게이트를 수정하여 미러링을 활성화할 수 있습니다.

미러링된 애그리게이트에 배치된 일관성 그룹과 연결된 볼륨 및 스냅샷은 원격 사이트(사이트 B)에 복제됩니다. 사이트 B의 볼륨 콘텐츠는 정합성 보장 그룹에 대한 쓰기 순서 보증을 제공하므로 재해 발생 시 사이트 B에서 복구할 수 있습니다. ONTAP 9.11.1 이상을 실행하는 클러스터에서 REST API 및 System Manager의 일관성 그룹을 사용하여 일관성 그룹 스냅샷에 액세스할 수 있습니다. ONTAP 9.14.1부터 ONTAP CLI를 사용하여 스냅샷에 액세스할 수도 있습니다.

일관성 그룹에 연결된 볼륨 중 일부 또는 모두가 현재 액세스할 수 없는 미러링되지 않은 애그리게이트에 있는 경우, 일관성 그룹의 가져오기 또는 삭제 작업은 로컬 볼륨 또는 호스팅 애그리게이트가 오프라인 상태인 것처럼 동작합니다.

복제에 대한 정합성 보장 그룹 구성

사이트 B에서 ONTAP 9.10.1 이하 버전을 실행하는 경우 미러링된 Aggregate에 있는 일관성 그룹과 연결된 볼륨만 사이트 B에 복제됩니다 정합성 보장 그룹 구성은 두 사이트가 모두 ONTAP 9.11.1 이상을 실행하는 경우 사이트 B에만 복제됩니다. 사이트 B를 ONTAP 9.11.1로 업그레이드한 후 사이트 A의 정합성 보장 그룹에 대한 모든 관련 볼륨이 미러링된 Aggregate에 배치된 데이터가 사이트 B에 복제됩니다

> 최적의 스토리지 성능과 가용성을 위해 미러링된 집계에 최소 20%의 여유 공간을 유지하는 것이 좋습니다. 미러링되지 않은 집계의 경우 권장 사항은 10%이지만, 추가된 10%의 공간은 파일 시스템에서 증분 변경 사항을 흡수하는 데 사용될 수 있습니다. ONTAP의 쓰기 시 리디렉션 스냅샷 기반 아키텍처로 인해 증분적 변경으로 인해 미러링된 집계의 공간 활용도가 높아집니다. 이러한 모범 사례를 준수하지 않으면 성과에 부정적인 영향을 미칠 수 있습니다.

업그레이드 고려 사항

ONTAP 9 ONTAP 9 .8 및 9.9.1에서 SnapMirror 활성 동기화(이전의 SnapMirror 비즈니스 연속성)로 생성된 일관성 그룹은 자동으로 업그레이드되고 시스템 관리자 또는 ONTAP REST API의 * 스토리지 > 일관성 그룹 * 에서 관리할 수 있습니다. ONTAP 9 .8 또는 9.9.1에서 업그레이드하는 방법에 대한 자세한 내용은 을 참조하십시오."SnapMirror 활성 동기화 업그레이드 및 되돌리기 고려 사항"

REST API에서 생성된 정합성 보장 그룹 스냅샷은 System Manager의 정합성 보장 그룹 인터페이스와 정합성 보장 그룹 REST API 엔드포인트를 통해 관리할 수 있습니다. ONTAP 9.14.1부터는 ONTAP CLI를 사용하여 일관성 그룹 스냅샷을 관리할 수도 있습니다.

> ONTAPI 명령을 사용하여 생성된 스냅샷은 `cg-start` `cg-commit` 일관성 그룹 스냅샷으로 인식되지 않으므로 System Manager의 일관성 그룹 인터페이스 또는 ONTAP REST API의 일관성 그룹 엔드포인트를 통해 관리할 수 없습니다. ONTAP 9.14.1부터 SnapMirror 비동기 정책을 사용하는 경우 이러한 스냅샷을 대상 볼륨에 미러링할 수 있습니다. 자세한 내용은 을 SnapMirror 비동기 구성참조하십시오.

릴리즈별 지원 기능

	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
계층적 일관성 그룹	✓	✓	✓	✓	✓	✓	✓
스냅샷을 통한 로컬 보호	✓	✓	✓	✓	✓	✓	✓

	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
SnapMirror 활성 동기화	✓	✓	✓	✓	✓	✓	✓
MetroCluster 지원	✓	✓	✓	✓	✓	✓	
2단계 커밋(REST API만 해당)	✓	✓	✓	✓	✓	✓	
응용 프로그램 및 구성 요소 태그	✓	✓	✓	✓	✓		
클론 정합성 보장 그룹	✓	✓	✓	✓	✓		
볼륨 추가 및 제거	✓	✓	✓	✓	✓		
새 NAS 볼륨으로 CG를 생성합니다	✓	✓	✓	✓	REST API만 해당		
새로운 NVMe 네임스페이스를 사용하여 CG를 생성합니다	✓	✓	✓	✓	REST API만 해당		
하위 일관성 그룹 간에 볼륨을 이동합니다	✓	✓	✓	✓			
정합성 보장 그룹 지오메트리를 수정합니다	✓	✓	✓	✓			
모니터링	✓	✓	✓	✓			
다중 관리 검증	✓						
SnapMirror 비동기식(단일 일관성 그룹만 해당)	✓	✓	✓	✓			
SVM 재해 복구(단일 일관성 그룹만 해당)	✓	✓	✓				
CLI 지원	✓	✓	✓				

일관성 그룹에 대해 자세히 알아보십시오

관련 정보

- "ONTAP 자동화 설명서"
- SnapMirror 활성 동기화
- SnapMirror 비동기식 재해 복구 기본 사항
- "MetroCluster 설명서"
- "다중 관리 검증"
- "ONTAP 명령 참조입니다"

ONTAP 일관성 그룹 제한에 대해 알아보세요

일관성 그룹을 계획 및 관리할 때는 클러스터와 부모 또는 자식 일관성 그룹 모두의 범위에서 개체 제한을 고려합니다.

적용된 제한

다음 표에는 일관성 그룹의 제한이 나와 있습니다. SnapMirror 액티브 동기화를 사용하는 일관성 그룹에 대해서는 별도의 제한 사항이 적용됩니다. 자세한 내용은 을 참조하십시오 "SnapMirror 활성 동기화 제한".

제한	범위	최소	최대
정합성 보장 그룹 수입니다	클러스터	0	클러스터 * 의 최대 볼륨 수와 동일합니다
상위 일관성 그룹의 수입니다	클러스터	0	클러스터의 최대 볼륨 수와 동일합니다

개별 및 상위 일관성 그룹의 수입니다	클러스터	0	클러스터의 최대 볼륨 수와 동일합니다
일관성 그룹에 있는 볼륨의 수입니다	단일 일관성 그룹	볼륨 1개	80개 볼륨
비동기식 SnapMirror를 사용하는 일관성 그룹에 있는 볼륨 수입니다	단일 일관성 그룹	볼륨 1개	• ONTAP 9.15.1 이상: 80개 볼륨 • ONTAP 9.13.1 및 9.14.1:16 볼륨
상위 일관성 그룹의 하위 볼륨에 있는 볼륨 수입니다	부모 일관성 그룹	볼륨 1개	80개 볼륨
하위 일관성 그룹의 볼륨 수입니다	하위 일관성 그룹	볼륨 1개	80개 볼륨
부모 일관성 그룹에 있는 하위 일관성 그룹의 수입니다	부모 일관성 그룹	일관성 그룹 1개	5개의 일관성 그룹
일관성 그룹이 있는 SVM 재해 복구 관계의 수(ONTAP 9.14.1부터 사용 가능)	클러스터	0	32

* SnapMirror 비동기로 설정된 최대 50개의 일관성 그룹을 클러스터에서 호스팅할 수 있습니다.

시행되지 않은 제한

정합성 보장 그룹에 대해 지원되는 최소 스냅샷 스케줄은 30분입니다. 이는 "FlexGroup 볼륨 테스트"정합성 보장 그룹과 동일한 스냅샷 인프라를 공유하는 을 기반으로 합니다.

단일 ONTAP 일관성 그룹 구성

일관성 그룹은 ONTAP 버전에 따라 기존 볼륨 또는 새 LUN이나 볼륨으로 생성할 수 있습니다. 볼륨 또는 LUN은 한 번에 하나의 일관성 그룹에만 연결할 수 있습니다.

이 작업에 대해

- ONTAP 9.10.1 ~ 9.11.1에서는 일관성 그룹이 생성된 후 해당 그룹의 구성원 볼륨을 수정할 수 없습니다.

  ONTAP 9.12.1부터 일관성 그룹의 구성원 볼륨을 수정할 수 있습니다. 이 프로세스에 대한 자세한 내용은 을 참조하십시오 일관성 그룹 수정.

- ONTAP 9.17.1부터 SnapMirror Active Sync 구성에서 VMware 워크로드에 대한 호스트를 NVMe 하위 시스템에 매핑하기 위해 NVMe 프로토콜을 선택할 수 있습니다.

새 **LUN** 또는 볼륨이 있는 일관성 그룹을 생성합니다

ONTAP 9.10.1 ~ 9.12.1에서는 새 LUN을 사용하여 일관성 그룹을 생성할 수 있습니다. 또한 ONTAP 9.13.1부터 System Manager에서는 새로운 NVMe 네임스페이스 또는 새 NAS 볼륨으로 일관성 그룹을 생성할 수 있습니다. (ONTAP 9.12.1부터 시작되는 ONTAP REST API에서도 지원됩니다.)

시스템 관리자(**ONTAP 9.16.1** 및 이전 버전)

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. Add * 를 선택한 다음 스토리지 객체에 대한 프로토콜을 선택합니다.

   ONTAP 9.10.1 ~ 9.12.1에서 새 스토리지 객체에 대한 유일한 옵션은 새 **LUN** 사용 입니다. ONTAP 9.13.1부터 System Manager는 새로운 NVMe 네임스페이스와 새로운 NAS 볼륨이 있는 일관성 그룹을 생성할 수 있도록 지원합니다.

3. 일관성 그룹의 이름을 지정합니다. 볼륨 또는 LUN의 수와 볼륨 또는 LUN당 용량을 지정합니다.
   a. 응용 프로그램 유형: ONTAP 9.12.1 이상을 사용하는 경우 응용 프로그램 유형을 선택합니다. 값을 선택하지 않으면 기본적으로 정합성 보장 그룹에 기타 유형이 할당됩니다. 에서 일관성 태그 지정에 대해 자세히 알아보십시오 응용 프로그램 및 구성 요소 태그. 원격 보호 정책을 사용하여 정합성 보장 그룹을 생성하려면 * 기타 * 를 사용해야 합니다.
   b. 새 LUN**: 호스트 운영 체제와 LUN 형식을 선택합니다. 호스트 이니시에이터 정보를 입력합니다.
   c. 새 **NAS** 볼륨: SVM의 NAS 구성에 따라 적절한 내보내기 옵션(NFS 또는 SMB/CIFS)을 선택합니다.
   d. 새 NVMe 네임스페이스**: 호스트 운영 체제와 NVMe 하위 시스템을 선택합니다.
4. 보호 정책을 구성하거나 하위 일관성 그룹을 추가하거나 액세스 권한을 부여하려면 * 추가 옵션 * 을 선택합니다.
5. 저장 * 을 선택합니다.
6. 작업이 완료되면 표시되는 기본 정합성 보장 그룹 메뉴로 돌아가 정합성 보장 그룹이 생성되었는지 확인합니다. 보호 정책을 설정하면 해당 정책, 원격 또는 로컬 아래에 녹색 방패 가 표시될 때 해당 정책이 적용되었음을 알 수 있습니다.

시스템 관리자(**ONTAP 9.17.1** 이상)

단계

1. *보호 > 일관성 그룹*을 선택합니다.
2. Add * 를 선택한 다음 스토리지 객체에 대한 프로토콜을 선택합니다.
3. 일관성 그룹의 이름을 지정합니다. 볼륨 또는 LUN 수와 볼륨 또는 LUN당 용량을 지정합니다. 애플리케이션 유형: 애플리케이션 유형을 선택합니다. 값을 선택하지 않으면 기본적으로 일관성 그룹에 기타 유형이 지정됩니다. 태그 일관성에 대해 자세히 알아보기 응용 프로그램 및 구성 요소 태그. 원격 보호 정책으로 일관성 그룹을 만들 계획이라면 *기타*를 사용해야 합니다
   a. 새 LUN**: 호스트 운영 체제와 LUN 형식을 선택합니다. 호스트 이니시에이터 정보를 입력합니다.
   b. 새 **NAS** 볼륨: SVM의 NAS 구성에 따라 적절한 내보내기 옵션(NFS 또는 SMB/CIFS)을 선택합니다.
   c. 새 NVMe 네임스페이스**: 호스트 운영 체제와 NVMe 하위 시스템을 선택합니다.
4. 보호 정책을 구성하거나 하위 일관성 그룹을 추가하거나 액세스 권한을 부여하려면 * 추가 옵션 * 을 선택합니다.
5. 저장 * 을 선택합니다.
6. 작업이 완료되면 표시되는 기본 정합성 보장 그룹 메뉴로 돌아가 정합성 보장 그룹이 생성되었는지 확인합니다. 보호 정책을 설정하면 해당 정책, 원격 또는 로컬 아래에 녹색 방패 가 표시될 때 해당 정책이 적용되었음을 알 수 있습니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 새 볼륨으로 새로운 일관성 그룹을 생성할 수 있습니다. 특정 매개변수는 볼륨이 SAN, NVMe 또는 NFS 볼륨에 따라 다릅니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

NFS 볼륨으로 일관성 그룹을 생성합니다

1. 정합성 보장 그룹을 생성합니다.

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -volume-prefix <prefix_for_new_volume_names>
-volume-count <number> -size <size> -export-policy <policy_name>
```

SAN 볼륨으로 정합성 보장 그룹을 생성합니다

1. 정합성 보장 그룹을 생성합니다.

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -lun <lun_name> -size <size> -lun-count <number>
-lun-os-type <LUN_operating_system_format> -igroup <igroup_name>
```

NVMe 네임스페이스로 일관성 그룹을 생성합니다

1. 정합성 보장 그룹을 생성합니다.

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency_group_name> -namespace <namespace_name> -volume-count <number>
-namespace-count <number> -size <size> -subsystem <subsystem_name>
```

에 대한 자세한 내용은 `consistency-group create` "ONTAP 명령 참조입니다"을 참조하십시오.

모두 끝냈군요

1. 를 사용하여 일관성 그룹이 생성되었는지 확인합니다 `consistency-group show` 명령.

에 대한 자세한 내용은 `consistency-group show` "ONTAP 명령 참조입니다"을 참조하십시오.

기존 볼륨이 있는 일관성 그룹을 생성합니다

기존 볼륨을 사용하여 일관성 그룹을 생성할 수 있습니다.

시스템 관리자(**ONTAP 9.16.1** 및 이전 버전)

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. * + 추가 * 를 선택한 다음 * 기존 볼륨 사용 * 을 선택합니다.
3. 일관성 그룹의 이름을 지정하고 스토리지 VM을 선택합니다.
   a. 응용 프로그램 유형: ONTAP 9.12.1 이상을 사용하는 경우 응용 프로그램 유형을 선택합니다. 값을 선택하지 않으면 기본적으로 정합성 보장 그룹에 기타 유형이 할당됩니다. 에서 일관성 태그 지정에 대해 자세히 알아보십시오 응용 프로그램 및 구성 요소 태그. 일관성 그룹에 SnapMirror 액티브 동기화 관계가 있는 경우 * 기타 * 를 사용해야 합니다.

   ⓘ ONTAP 9.15.1 이전의 ONTAP 버전에서는 SnapMirror 액티브 동기화를 SnapMirror 비즈니스 연속성이라고 합니다.

4. 포함할 기존 볼륨을 선택합니다. 정합성 보장 그룹에 아직 포함되지 않은 볼륨만 선택할 수 있습니다.

   ⓘ 기존 볼륨으로 일관성 그룹을 생성하는 경우 일관성 그룹은 FlexVol 볼륨을 지원합니다. 또는 SnapMirror 동기식 또는 SnapMirror 비동기식 관계가 있는 볼륨을 일관성 그룹에 추가할 수 있지만 일관성 그룹을 인식하지 않습니다. 일관성 그룹은 S3 버킷 또는 SVMDR 관계가 있는 스토리지 VM을 지원하지 않습니다.

5. 저장 * 을 선택합니다.
6. ONTAP 작업이 완료된 후 표시되는 기본 일관성 그룹 메뉴로 돌아가서 일관성 그룹이 생성되었는지 확인합니다. 보호 정책을 선택한 경우 메뉴에서 일관성 그룹을 선택하여 정책이 올바르게 설정되었는지 확인합니다. 보호 정책을 설정하는 경우 해당 정책(원격 또는 로컬)에서 찾기에 녹색 실드가 표시되면 해당 정책이 적용되었음을 알 수 있습니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 기존 볼륨과 함께 일관성 그룹을 생성할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

단계

1. 를 발행합니다 `consistency-group create` 명령. 를 클릭합니다 `-volumes` 매개 변수에는 쉼표로 구분된 볼륨 이름 목록을 사용할 수 있습니다.

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency-group-name> -volume <volumes>
   ```

   에 대한 자세한 내용은 `consistency-group create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 를 사용하여 일관성 그룹을 확인합니다 `consistency-group show` 명령.

   에 대한 자세한 내용은 `consistency-group show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 단계

- 일관성 그룹 보호
- 일관성 그룹 수정
- 일관성 그룹의 클론을 생성합니다

계층적 **ONTAP** 일관성 그룹 구성

계층적 일관성 그룹을 사용하여 여러 볼륨에 걸쳐 있는 대규모 워크로드를 관리할 수 있으므로 하위 일관성 그룹에 대한 우산 역할을 하는 부모 일관성 그룹을 생성할 수 있습니다.

계층적 일관성 그룹에는 최대 5개의 개별 일관성 그룹을 포함할 수 있는 부모가 있습니다. 계층적 정합성 보장 그룹은 정합성 보장 그룹 또는 개별 볼륨에 걸쳐 서로 다른 로컬 스냅샷 정책을 지원할 수 있습니다. 원격 보호 정책을 사용하는 경우 전체 계층 일관성 그룹(상위 및 하위)에 적용됩니다.

ONTAP 9.13.1부터 가능합니다 일관성 그룹의 구조를 수정합니다 및 하위 일관성 그룹 간에 볼륨을 이동합니다.

일관성 그룹의 개체 제한은 를 참조하십시오 일관성 그룹에 대한 개체 제한.

새 **LUN** 또는 볼륨이 있는 계층적 일관성 그룹을 생성합니다

계층적 일관성 그룹을 생성할 때 새 LUN으로 이를 채울 수 있습니다. ONTAP 9.13.1부터 새로운 NVMe 네임스페이스와 NAS 볼륨을 사용할 수도 있습니다.

시스템 관리자

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. Add * 를 선택한 다음 스토리지 객체에 대한 프로토콜을 선택합니다.

   ONTAP 9.10.1 ~ 9.12.1에서 새 스토리지 객체에 대한 유일한 옵션은 새 **LUN** 사용 입니다. ONTAP 9.13.1부터 System Manager는 새로운 NVMe 네임스페이스와 새로운 NAS 볼륨이 있는 일관성 그룹을 생성할 수 있도록 지원합니다.

3. 일관성 그룹의 이름을 지정합니다. 볼륨 또는 LUN의 수와 볼륨 또는 LUN당 용량을 지정합니다.
   a. 응용 프로그램 유형: ONTAP 9.12.1 이상을 사용하는 경우 응용 프로그램 유형을 선택합니다. 값을 선택하지 않으면 기본적으로 정합성 보장 그룹에 기타 유형이 할당됩니다. 에서 일관성 태그 지정에 대해 자세히 알아보십시오 응용 프로그램 및 구성 요소 태그. 원격 보호 정책을 사용하려는 경우 * 기타 * 를 선택해야 합니다.
4. 호스트 운영 체제 및 LUN 형식을 선택합니다. 호스트 이니시에이터 정보를 입력합니다.
   a. 새 LUN**: 호스트 운영 체제와 LUN 형식을 선택합니다. 호스트 이니시에이터 정보를 입력합니다.
   b. 새 **NAS** 볼륨: SVM의 NAS 구성에 따라 적절한 내보내기 옵션(NFS 또는 SMB/CIFS)을 선택합니다.
   c. 새 NVMe 네임스페이스**: 호스트 운영 체제와 NVMe 하위 시스템을 선택합니다.
5. 하위 일관성 그룹을 추가하려면 * 더 많은 옵션 * 을 선택한 다음 * + 하위 일관성 그룹 추가 * 를 선택합니다.
6. LUN 또는 볼륨당 성능 수준, LUN 또는 볼륨 수, 용량을 선택합니다. 사용 중인 프로토콜에 따라 적절한 내보내기 구성 또는 운영 체제 정보를 지정합니다.
7. 필요에 따라 로컬 스냅샷 정책을 선택하고 액세스 권한을 설정합니다.
8. 최대 5개의 하위 일관성 그룹에 대해 반복합니다.
9. 저장 * 을 선택합니다.
10. ONTAP 작업이 완료되면 표시되는 기본 일관성 그룹 메뉴로 돌아가 일관성 그룹이 생성되었는지 확인합니다. 보호 정책을 설정하는 경우 해당 정책, 원격 또는 로컬 아래에서 녹색 차폐가 체크 표시와 함께 표시되어야 합니다.

CLI를 참조하십시오

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

CLI에서 새 볼륨으로 계층적 정합성 보장 그룹을 생성할 때는 각 하위 정합성 보장 그룹을 개별적으로 생성해야 합니다.

단계

1. 를 사용하여 새 일관성 그룹을 생성합니다 `consistency-group create` 명령.

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency_group_name> -parent-consistency-group
<parent_consistency_group_name> -volume-prefix <volume_prefix> -volume
```

```
-count <number_of_volumes> -size <size>
```

2. CLI에서 메시지가 표시되면 새 부모 일관성 그룹을 생성할지 확인합니다. 를 `y`입력합니다.
3. 필요한 경우 1단계를 반복하여 하위 정합성 보장 그룹을 추가로 생성합니다.

   에 대한 자세한 내용은 `consistency-group create` "ONTAP 명령 참조입니다"을 참조하십시오.

기존 볼륨을 포함하는 계층적 일관성 그룹을 생성합니다

기존 볼륨을 계층적 일관성 그룹으로 구성할 수 있습니다.

시스템 관리자

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. * + 추가 * 를 선택한 다음 * 기존 볼륨 사용 * 을 선택합니다.
3. 스토리지 VM을 선택합니다.
4. 포함할 기존 볼륨을 선택합니다. 정합성 보장 그룹에 아직 포함되지 않은 볼륨만 선택할 수 있습니다.
5. 하위 일관성 그룹을 추가하려면 * + 하위 일관성 그룹 추가 * 를 선택합니다. 필요한 일관성 그룹을 생성합니다. 이 그룹의 이름은 자동으로 지정됩니다.
   a. 구성 요소 유형: ONTAP 9.12.1 이상을 사용하는 경우 "data", "logs" 또는 "other"의 구성 요소 유형을 선택합니다. 값을 선택하지 않으면 기본적으로 정합성 보장 그룹에 기타 유형이 할당됩니다. 에서 일관성 태그 지정에 대해 자세히 알아보십시오 응용 프로그램 및 구성 요소 태그. 원격 보호 정책을 사용하려는 경우 * 기타 * 를 사용해야 합니다.
6. 각 일관성 그룹에 기존 볼륨을 할당합니다.
7. 필요한 경우 로컬 스냅샷 정책을 선택합니다.
8. 최대 5개의 하위 일관성 그룹에 대해 반복합니다.
9. 저장 * 을 선택합니다.
10. ONTAP 작업이 완료되면 표시되는 기본 일관성 그룹 메뉴로 돌아가 일관성 그룹이 생성되었는지 확인합니다. 보호 정책을 선택한 경우 메뉴에서 정합성 보장 그룹을 선택하여 정책이 올바르게 설정되었는지 확인합니다. 해당 정책 유형 아래에 녹색 차폐가 있고 확인 표시가 있습니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 CLI를 사용하여 계층적 일관성 그룹을 생성할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

단계

1. 새 부모 정합성 보장 그룹을 프로비저닝하고 새 하위 정합성 보장 그룹에 볼륨을 할당합니다.

```
consistency-group create -vserver <svm_name> -consistency-group
<child_consistency_group_name> -parent-consistency-group
<parent_consistency_group_name> -volumes <volume_names>
```

2. 를 입력합니다 `y` 새 부모 및 자식 일관성 그룹을 생성하려면 다음을 수행합니다.

   에 대한 자세한 내용은 `consistency-group create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 단계

- 일관성 그룹의 구조를 수정합니다
- 일관성 그룹 수정

- 일관성 그룹 보호

ONTAP 일관성 그룹 보호

일관성 그룹은 여러 볼륨에 걸쳐 있는 SAN, NAS 및 NVMe 애플리케이션에 대해 쉽게 관리되는 로컬 및 원격 보호를 제공합니다.

일관성 그룹을 생성해도 보호가 자동으로 설정되지는 않습니다. 보호 정책은 생성 시 또는 일관성 그룹을 생성한 후에 설정할 수 있습니다. 다음을 사용하여 일관성 그룹을 보호할 수 있습니다.

- 로컬 스냅샷
- SnapMirror 액티브 동기화(9.15.1 이전의 ONTAP 버전에서는 SnapMirror 비즈니스 연속성이라고 함)
- MetroCluster(9.11.1부터)
- SnapMirror 비동기식(9.13.1부터)
- 비동기식 SVM 재해 복구(9.14.1부터)

중첩된 일관성 그룹을 사용하는 경우 상위 및 하위 일관성 그룹에 대해 서로 다른 보호 정책을 설정할 수 있습니다.

ONTAP 9.11.1부터 정합성 보장 그룹이 2단계 정합성 보장 그룹 스냅샷 생성제공합니다. 2단계 스냅샷 작업은 사전 검사를 실행하여 스냅샷이 성공적으로 캡처되었는지 확인합니다.

전체 정합성 보장 그룹, 계층적 구성의 단일 정합성 보장 그룹 또는 정합성 보장 그룹 내의 개별 볼륨에 대해 복구가 수행될 수 있습니다. 복구할 정합성 보장 그룹을 선택하고 스냅샷 유형을 선택한 다음 복구를 기반으로 할 스냅샷을 식별하여 복구할 수 있습니다. 이 프로세스에 대한 자세한 내용은 을 "이전 스냅샷에서 볼륨을 복원합니다"참조하십시오.

로컬 스냅샷 정책을 구성합니다

로컬 스냅샷 보호 정책을 설정하면 정합성 보장 그룹의 모든 볼륨을 포괄하는 정책을 생성할 수 있습니다.

이 작업에 대해

정합성 보장 그룹에 대해 지원되는 최소 스냅샷 스케줄은 30분입니다. 이는 "FlexGroup 볼륨 테스트"정합성 보장 그룹과 동일한 스냅샷 인프라를 공유하는 을 기반으로 합니다.

시스템 관리자

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 정합성 보장 그룹 메뉴에서 생성한 정합성 보장 그룹을 선택합니다.
3. 일관성 그룹의 개요 페이지 오른쪽 위에서 * 편집 * 을 선택합니다.
4. 스냅샷 예약(로컬) 옆에 있는 상자를 선택하세요.
5. 스냅샷 정책을 선택합니다. 새 사용자 지정 정책을 구성하려면 을 "사용자 지정 데이터 보호 정책을 생성합니다"참조하십시오.
6. 저장 * 을 선택합니다.
7. 일관성 그룹 개요 메뉴로 돌아갑니다. 왼쪽 열의 * Snapshots (Local) * 아래에서 상태는 옆에 보호됨으로 표시됩니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 CLI를 사용하여 일관성 그룹의 보호 정책을 수정할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

단계

1. 다음 명령을 실행하여 보호 정책을 설정하거나 수정합니다.

   하위 정합성 보장의 보호 정책을 수정하는 경우 를 사용하여 부모 정합성 보장 그룹을 식별해야 합니다 `-parent-consistency-group` *`parent_consistency_group_name`* 매개 변수.

   ```
   consistency-group modify -vserver svm_name -consistency-group
   consistency_group_name -snapshot-policy policy_name
   ```

필요 시 스냅샷을 생성합니다

일반적으로 예약된 정책 외에 일관성 그룹의 스냅샷을 생성해야 하는 경우 필요에 따라 생성할 수 있습니다.

시스템 관리자

단계

1. 스토리지 * > * Consistency groups * 로 이동합니다.
2. 필요 시 스냅샷을 생성할 정합성 보장 그룹을 선택합니다.
3. Snapshot 복사본 * 탭으로 전환한 다음 * + 추가 * 를 선택합니다.
4. 이름 * 및 * SnapMirror 레이블 * 을 제공하십시오. 정합성 * 드롭다운 메뉴에서 * 애플리케이션 정합성 * 또는 * 충돌 정합성 보장 * 을 선택합니다.
5. 저장 * 을 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 CLI를 사용하여 일관성 그룹의 주문형 스냅샷을 생성할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

단계

1. 스냅샷 생성:

   기본적으로 스냅샷 유형은 충돌 일치입니다. 선택적 매개 변수를 사용하여 스냅샷 유형을 수정할 수 `-type` 있습니다.

   ```
   consistency-group snapshot create -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

2단계 정합성 보장 그룹 스냅샷을 생성합니다

ONTAP 9.11.1부터 일관성 그룹은 CG(정합성 보장 그룹) 스냅샷 생성을 위한 2단계 커밋을 지원하며, 이 커밋은 스냅샷을 커밋하기 전에 사전 점검을 실행합니다. 이 기능은 ONTAP REST API에서만 사용할 수 있습니다.

2단계 CG 스냅샷 생성은 정합성 보장 그룹을 프로비저닝하거나 정합성 보장 그룹을 복구하는 것이 아니라 스냅샷 생성에만 사용할 수 있습니다.

2단계 CG 스냅샷은 스냅샷 생성 프로세스를 다음 두 단계로 나눕니다.

1. 첫 번째 단계에서는 API가 사전 검사를 실행하고 스냅샷 생성을 트리거합니다. 첫 번째 단계에는 스냅샷이 성공적으로 커밋될 시간을 지정하는 시간 제한 매개 변수가 포함됩니다.
2. 1단계의 요청이 성공적으로 완료되면 첫 번째 단계에서 지정된 간격 내에 두 번째 단계를 호출하여 스냅샷을 적절한 끝점에 커밋할 수 있습니다.

시작하기 전에

- 2단계 CG 스냅샷 생성을 사용하려면 클러스터의 모든 노드에서 ONTAP 9.11.1 이상을 실행해야 합니다.
- 정합성 보장 그룹 스냅샷 작업의 활성 호출은 한 번에 하나의 정합성 보장 그룹 인스턴스에서만 지원됩니다(1단계 또는 2단계). 다른 작업이 진행 중인 동안 스냅샷 작업을 호출하려고 하면 오류가 발생합니다.

- 스냅샷 생성을 호출할 때 옵션 시간 초과 값을 5초에서 120초 사이로 설정할 수 있습니다. 시간 초과 값을 제공하지 않으면 기본 값인 7초로 작업이 시간 초과됩니다. API에서 매개 변수를 사용하여 시간 초과 값을 `action_timeout` 설정합니다. CLI에서 `-timeout` 플래그를 사용합니다.

단계

REST API 또는 ONTAP 9.14.1부터 ONTAP CLI를 사용하여 2단계 스냅샷을 완료할 수 있습니다. 이 작업은 System Manager에서 지원되지 않습니다.

> API를 사용하여 스냅샷 생성을 호출하는 경우 API를 사용하여 스냅샷을 커밋해야 합니다. CLI를 사용하여 스냅샷 생성을 호출하는 경우 CLI를 사용하여 스냅샷을 커밋해야 합니다. 혼합 방법은 지원되지 않습니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 CLI를 사용하여 2단계 스냅샷을 생성할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

단계

1. 스냅샷을 시작합니다.

   ```
   consistency-group snapshot start -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
   -write-fence {true|false}]
   ```

2. 스냅샷이 생성되었는지 확인합니다.

   ```
   consistency-group snapshot show
   ```

3. 스냅샷 커밋:

   ```
   consistency-group snapshot commit svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

API를 참조하십시오

1. 스냅샷 생성을 호출합니다. 매개 변수를 사용하여 정합성 보장 그룹 끝점에 POST 요청을 `action=start` 보냅니다.

   ```
   curl -k -X POST 'https://<IP_address>/application/consistency-
   groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
   "accept: application/hal+json" -H "content-type: application/json"
   -d '
   {
     "name": "<snapshot_name>",
     "consistency_type": "crash",
     "comment": "<comment>",
     "snapmirror_label": "<SnapMirror_label>"
   }'
   ```

2. POST 요청이 성공하면 출력에 snapshot uid가 포함됩니다. 해당 uuid를 사용하여 스냅샷을 커밋할 패치 요청을 제출합니다.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"

For more information about the ONTAP REST API, see
link:https://docs.netapp.com/us-en/ontap-
automation/reference/api_reference.html[API reference^] or the
link:https://devnet.netapp.com/restapi.php[ONTAP REST API page^] at
the NetApp Developer Network for a complete list of API endpoints.
```

정합성 보장 그룹에 대한 원격 보호를 설정합니다

정합성 보장 그룹은 SnapMirror Active Sync 및 ONTAP 9.13.1, SnapMirror Asynchronous를 통해 원격 보호를 제공합니다.

SnapMirror 활성 동기화로 보호를 구성합니다

SnapMirror 활성 동기화를 사용하여 정합성 보장 그룹에 생성된 정합성 보장 그룹의 스냅샷이 대상으로 복제되도록 할 수 있습니다. SnapMirror 활성 동기화에 대한 자세한 내용 또는 CLI를 사용하여 SnapMirror 활성 동기화를 구성하는 방법에 대한 자세한 내용은 을 참조하십시오.무중단 업무 운영을 위한 보호 구성

시작하기 전에

- NAS 액세스를 위해 마운트된 볼륨에 SnapMirror 활성 동기화 관계를 설정할 수 없습니다.
- 소스 및 대상 클러스터의 정책 레이블이 일치해야 합니다.
- SnapMirror 활성 동기화는 SnapMirror 레이블이 있는 규칙이 미리 정의된 정책에 추가되고 해당 레이블을 사용하여 스냅샷이 생성되지 않는 한 스냅샷을 기본적으로 복제하지 않습니다. `AutomatedFailOver`

  이 프로세스에 대한 자세한 내용은 을 참조하십시오 "SnapMirror 액티브 동기화로 보호".

- 다중 구간 구축 SnapMirror 액티브 동기화에서는 지원되지 않습니다.
- ONTAP 9.13.1부터 무중단으로 업그레이드할 수 있습니다 볼륨을 일관성 그룹에 추가합니다 활성 SnapMirror 활성 동기화 관계가 있습니다. 일관성 그룹에 대한 다른 변경 사항은 SnapMirror 활성 동기화 관계를 해제하고 일관성 그룹을 수정한 다음 관계를 다시 설정하고 재동기화해야 합니다.

CLI를 사용하여 SnapMirror 활성 동기화를 구성하려면 를 참조하십시오 SnapMirror 액티브 동기화로 보호.

System Manager를 위한 단계

1. 을(를) 충족하는지 확인합니다 "SnapMirror 액티브 동기화 사용을 위한 사전 요구사항".
2. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
3. 정합성 보장 그룹 메뉴에서 생성한 정합성 보장 그룹을 선택합니다.
4. 개요 페이지 오른쪽 상단에서 * 자세히 * 를 선택한 다음 * 보호 * 를 선택합니다.
5. System Manager는 소스 측 정보를 자동으로 채웁니다. 대상에 적합한 클러스터 및 스토리지 VM을 선택합니다.

보호 정책을 선택합니다. Initialize relationship * 이 선택되어 있는지 확인합니다.

6. 저장 * 을 선택합니다.
7. 정합성 보장 그룹을 초기화하고 동기화해야 합니다. 정합성 보장 그룹 * 메뉴로 돌아가 동기화가 성공적으로 완료되었는지 확인합니다. SnapMirror (원격) * 상태가 `Protected` 옆에 표시됩니다.

SnapMirror 비동기 구성

ONTAP 9.13.1부터 단일 일관성 그룹에 대해 SnapMirror 비동기식 보호를 구성할 수 있습니다. ONTAP 9.14.1부터 SnapMirror 비동기식을 사용하여 일관성 그룹 관계를 사용하여 볼륨 세분화 스냅샷을 타겟 클러스터에 복제할 수 있습니다.

이 작업에 대해

볼륨 세분화 스냅샷을 복제하려면 ONTAP 9.14.1 이상을 실행해야 합니다. MirrorAndVault 및 Vault 정책의 경우, 볼륨 세분화 스냅샷 정책의 SnapMirror 레이블은 일관성 그룹의 SnapMirror 정책 규칙과 일치해야 합니다. 볼륨 세분화 스냅샷은 일관성 그룹 스냅샷과 관계없이 계산되는 일관성 그룹의 SnapMirror 정책의 Keep 값을 준수합니다. 예를 들어 대상에 두 개의 스냅샷을 유지하는 정책이 있는 경우 볼륨 세분화 스냅샷 두 개와 정합성 보장 그룹 스냅샷 두 개를 만들 수 있습니다.

SnapMirror 관계를 볼륨 세분화 스냅샷과 재동기화할 때 플래그로 볼륨 세분화 스냅샷을 보존할 수 `-preserve` 있습니다. 정합성 보장 그룹 스냅샷보다 최신 볼륨 세분화 스냅샷은 보존됩니다. 정합성 보장 그룹 스냅샷이 없는 경우 재동기화 작업에서 볼륨 세분화 스냅샷을 전송할 수 없습니다.

시작하기 전에

- SnapMirror 비동기식 보호는 단일 일관성 그룹에만 사용할 수 있습니다. 계층적 일관성 그룹에는 지원되지 않습니다. 계층적 일관성 그룹을 단일 일관성 그룹으로 변환하려면 을 참조하십시오 정합성 보장 그룹 아키텍처 수정.
- 소스 및 대상 클러스터의 정책 레이블이 일치해야 합니다.
- 무중단으로 확장 가능합니다 볼륨을 일관성 그룹에 추가합니다 활성 SnapMirror 비동기식 관계를 통해 원격 백업 기능을 지원합니다. 일관성 그룹이 변경되면 SnapMirror 관계를 중단시키고 일관성 그룹을 수정한 다음, 관계를 다시 설정하고 다시 동기화해야 합니다.
- SnapMirror 비동기 사용 시 보호되도록 설정된 일관성 그룹에는 제한 사항이 다릅니다. 자세한 내용은 을 참조하십시오 정합성 보장 그룹 제한.
- 여러 개별 볼륨에 대해 SnapMirror 비동기식 보호 관계를 구성한 경우 기존 스냅샷을 유지하면서 해당 볼륨을 정합성 보장 그룹으로 변환할 수 있습니다. 볼륨을 성공적으로 변환하려면 다음을 수행합니다.
  - 볼륨의 공통 스냅샷이 있어야 합니다.
  - 기존 SnapMirror 관계를 해제해야 합니다. 단일 일관성 그룹에 볼륨을 추가합니다그런 다음 다음 다음 다음 워크플로를 사용하여 관계를 다시 동기화합니다.

단계

1. 대상 클러스터에서 * 스토리지 > 일관성 그룹 * 을 선택합니다.
2. 정합성 보장 그룹 메뉴에서 생성한 정합성 보장 그룹을 선택합니다.
3. 개요 페이지 오른쪽 상단에서 * 자세히 * 를 선택한 다음 * 보호 * 를 선택합니다.
4. System Manager는 소스 측 정보를 자동으로 채웁니다. 대상에 적합한 클러스터 및 스토리지 VM을 선택합니다. 보호 정책을 선택합니다. Initialize relationship * 이 선택되어 있는지 확인합니다.

   비동기 정책을 선택할 때 전송 일정 재정의 옵션을 사용할 수 있습니다.

SnapMirror 비동기식을 사용하는 일관성 그룹에서 지원되는 최소 일정(복구 시점 목표 또는 RPO)은 30분입니다.

5. 저장 * 을 선택합니다.
6. 정합성 보장 그룹을 초기화하고 동기화해야 합니다. 정합성 보장 그룹 * 메뉴로 돌아가 동기화가 성공적으로 완료되었는지 확인합니다. SnapMirror (원격) * 상태가 `Protected` 옆에 표시됩니다.

SVM 재해 복구 구성

ONTAP 9.14.1부터 는 SVM 재해 복구일관성 그룹을 지원하므로 일관성 그룹 정보를 소스에서 타겟 클러스터로 미러링할 수 있습니다.

이미 일관성 그룹이 포함된 SVM에서 SVM 재해 복구를 사용하도록 설정하려면 의 SVM 구성 워크플로우를 따릅니다 시스템 관리자 또는 을 누릅니다 ONTAP CLI를 참조하십시오.

활성 및 정상 상태의 SVM 재해 복구 관계에 있는 SVM에 일관성 그룹을 추가하려면 대상 클러스터에서 SVM 재해 복구 관계를 업데이트해야 합니다. 자세한 내용은 을 참조하십시오 복제 관계를 수동으로 업데이트합니다. 일관성 그룹을 확장할 때는 언제든지 관계를 업데이트해야 합니다.

제한 사항

- SVM 재해 복구는 계층적 일관성 그룹을 지원하지 않습니다.
- SVM 재해 복구는 비동기식 SnapMirror로 보호되는 일관성 그룹을 지원하지 않습니다. SVM 재해 복구를 구성하기 전에 SnapMirror 관계를 해제해야 합니다.
- 두 클러스터에서 모두 ONTAP 9.14.1 이상을 실행해야 한다.
- 일관성 그룹이 포함된 SVM 재해 복구 구성에는 팬아웃 관계가 지원되지 않습니다.
- 기타 제한 사항은 를 참조하십시오 정합성 보장 그룹 제한.

관계를 시각화합니다

System Manager는 * Protection > Relationships * 메뉴에서 LUN 맵을 시각화합니다. 소스 관계를 선택하면 System Manager에서 소스 관계를 시각화합니다. 볼륨을 선택하면 이러한 관계를 자세히 살펴보고 포함된 LUN 및 이니시에이터 그룹 관계의 목록을 볼 수 있습니다. 이 정보는 개별 볼륨 보기에서 Excel 통합 문서로 다운로드할 수 있으며 다운로드 작업은 백그라운드에서 실행됩니다.

관련 정보

- "일관성 그룹의 클론을 생성합니다"
- "스냅샷을 구성합니다"
- "사용자 지정 데이터 보호 정책을 생성합니다"
- "스냅샷에서 복구합니다"
- "이전 스냅샷에서 볼륨을 복원합니다"
- "SnapMirror Active Sync 개요"
- "ONTAP 자동화 설명서"
- SnapMirror 비동기식 재해 복구 기본 사항

ONTAP 일관성 그룹의 멤버 볼륨 수정

ONTAP 9.12.1부터 볼륨을 제거하거나 볼륨을 추가(정합성 보장 그룹 확장)하여 정합성 보장 그룹을 수정할 수 있습니다. ONTAP 9.13.1부터 하위 정합성 보장 그룹이 공통 부모를 공유하는 경우 볼륨을 이동할 수 있습니다.

볼륨을 일관성 그룹에 추가합니다

ONTAP 9.12.1부터는 일관성 그룹에 볼륨을 무중단으로 추가할 수 있습니다.

이 작업에 대해

- 다른 일관성 그룹에 연결된 볼륨은 추가할 수 없습니다.
- 일관성 그룹은 NAS, SAN 및 NVMe 프로토콜을 지원합니다.
- 조정이 전체 내에 있는 경우 일관성 그룹에 한 번에 최대 16개의 볼륨을 추가할 수 있습니다 정합성 보장 그룹 제한.
- ONTAP 9.13.1부터 활성 SnapMirror 활성 동기화 또는 SnapMirror 비동기 보호 정책을 사용하여 운영 중단 없이 일관성 그룹에 볼륨을 추가할 수 있습니다.
- SnapMirror 액티브 동기화로 보호되는 일관성 그룹에 볼륨을 추가하면 새 볼륨에 대해 미러링 및 보호가 구성될 때까지 SnapMirror 액티브 동기화 관계 상태가 "확장"으로 변경됩니다. 이 프로세스가 완료되기 전에 운영 클러스터에서 재해가 발생하면 페일오버 작업의 일부로 정합성 보장 그룹이 원래 구성으로 되돌아갑니다.
- ONTAP 9.12.1 이하 버전에서는 SnapMirror 활성 동기화 관계의 일관성 그룹에 볼륨을 추가할 수 _ 없습니다. 먼저 SnapMirror 액티브 동기화 관계를 삭제하고 일관성 그룹을 수정한 다음 SnapMirror 액티브 동기화로 보호를 복원해야 합니다.
- ONTAP 9.12.1부터 ONTAP REST API는 정합성 보장 그룹에 *new* 또는 기존 볼륨을 추가할 수 있도록 지원합니다. ONTAP REST API에 대한 자세한 내용은 를 참조하십시오 "ONTAP REST API 참조 설명서".

  ONTAP 9.13.1부터 이 기능은 System Manager에서 지원됩니다.

- 정합성 보장 그룹을 확장할 때 수정 전에 캡처한 정합성 보장 그룹의 스냅샷은 부분적으로 간주됩니다. 해당 스냅샷을 기반으로 하는 모든 복구 작업은 스냅샷 시점에 정합성 보장 그룹을 반영합니다.
- ONTAP 9.10.1 ~ 9.11.1을 사용하는 경우 일관성 그룹을 수정할 수 없습니다. ONTAP 9.10.1 또는 9.11.1에서 일관성 그룹의 구성을 변경하려면 일관성 그룹을 삭제한 다음, 포함할 볼륨으로 새 일관성 그룹을 생성해야 합니다.
- ONTAP 9.14.1부터 SnapMirror 비동기식을 사용할 경우 볼륨 세분화 스냅샷을 대상 클러스터에 복제할 수 있습니다. SnapMirror 비동기식을 사용하여 일관성 그룹을 확장하는 경우, SnapMirror 정책이 MirrorAll 또는 MirrorAndVault일 때 정합성 보장 그룹을 확장한 후에만 볼륨 세부 스냅샷이 복제됩니다. 기본 정합성 보장 그룹 스냅샷보다 최신 볼륨 세분화 스냅샷만 복제됩니다.
- SVM 재해 복구 관계(ONTAP 9.14.1부터 지원)의 일관성 그룹에 볼륨을 추가하는 경우, 일관성 그룹을 확장한 후 대상 클러스터에서 SVM 재해 복구 관계를 업데이트해야 합니다. 자세한 내용은 다음을 참조하십시오. 복제 관계를 수동으로 업데이트합니다 .
- ONTAP 9.17.1에서 NVMe를 사용하는 경우 일관성 그룹을 수정할 수 없습니다.

예 **31.** 단계

시스템 관리자

ONTAP 9.12.1부터 System Manager로 이 작업을 수행할 수 있습니다.

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 수정할 일관성 그룹을 선택합니다.
3. 단일 일관성 그룹을 수정하는 경우 * Volumes * 메뉴 맨 위에서 * 더 보기 * 를 선택한 다음 * 확장 * 을 선택하여 볼륨을 추가합니다.

   하위 일관성 그룹을 수정할 경우 수정할 부모 일관성 그룹을 식별합니다. > * 버튼을 선택하여 하위 일관성 그룹을 표시한 다음, 수정할 하위 일관성 그룹의 이름 옆에 있는 을 선택합니다 ⋮ . 해당 메뉴에서 * Expand * 를 선택합니다.

4. 정합성 보장 그룹에 추가할 볼륨을 최대 16개까지 선택합니다.
5. 저장 * 을 선택합니다. 작업이 완료되면 정합성 보장 그룹의 * Volumes * 메뉴에서 새로 추가된 볼륨을 확인합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 일관성 그룹에 볼륨을 추가할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

기존 볼륨을 추가합니다

1. 다음 명령을 실행합니다. 를 클릭합니다 `-volumes` 매개 변수에는 쉼표로 구분된 볼륨 목록을 사용할 수 있습니다.

   만 포함합니다 `-parent-consistency-group` 일관성 그룹이 계층적 관계에 있는 경우 매개 변수입니다.

   ```
   consistency-group volume add -vserver svm_name -consistency-group
   consistency_group_name -parent-consistency-group parent_consistency_group
   -volume volumes
   ```

새 볼륨을 추가합니다

새 볼륨을 추가하는 절차는 사용 중인 프로토콜에 따라 다릅니다.

다음만 포함합니다. `-parent-consistency-group` 일관성 그룹이 계층적 관계에 있는 경우 매개변수입니다.

- 새 볼륨을 내보내지 않고 추가하려면 다음을 수행합니다.

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  child_consistency_group -parent-consistency-group existingParentCg -volume
  ```

volume_name -size *size*

- 새 NFS 볼륨 추가하기:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -volume volume-prefix -volume-count number -size
size -export-policy policy_name
```

- 새 SAN 볼륨 추가하기:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -lun lun_name -size size -lun-count number -igroup
igroup_name
```

- 새 NVMe 네임스페이스 추가하기:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -namespace namespace_name -volume-count number
-namespace-count number -size size -subsystem subsystem_name
```

일관성 그룹에서 볼륨을 제거합니다

일관성 그룹에서 제거된 볼륨은 삭제되지 않습니다. 클러스터에서 활성 상태로 유지됩니다.

이 작업에 대해

- SnapMirror 활성 동기화 또는 SVM 재해 복구 관계의 일관성 그룹에서 볼륨을 제거할 수는 없습니다. 먼저 SnapMirror 액티브 동기화 관계를 삭제하여 일관성 그룹을 수정한 다음 관계를 다시 설정해야 합니다.
- 제거 작업 후 일관성 그룹에 볼륨이 없으면 일관성 그룹이 삭제됩니다.
- 볼륨이 일관성 그룹에서 제거되면 일관성 그룹의 기존 스냅샷은 그대로 유지되지만 유효하지 않은 것으로 간주됩니다. 기존 스냅샷을 사용하여 정합성 보장 그룹의 컨텐츠를 복구할 수 없습니다. 볼륨 세분화 스냅샷은 유효합니다.
- 클러스터에서 볼륨을 삭제하면 해당 볼륨이 일관성 그룹에서 자동으로 제거됩니다.
- ONTAP 9.10.1 또는 9.11.1에서 일관성 그룹의 구성을 변경하려면 일관성 그룹을 삭제한 다음 원하는 구성원 볼륨을 가진 새 일관성 그룹을 생성해야 합니다.
- 클러스터에서 볼륨을 삭제하면 일관성 그룹에서도 자동으로 제거됩니다.

시스템 관리자

ONTAP 9.12.1부터 System Manager로 이 작업을 수행할 수 있습니다.

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 수정할 단일 또는 하위 일관성 그룹을 선택합니다.
3. Volumes * 메뉴에서 일관성 그룹에서 제거할 개별 볼륨 옆의 확인란을 선택합니다.
4. 정합성 보장 그룹에서 볼륨 제거 * 를 선택합니다.
5. 볼륨을 제거하면 정합성 보장 그룹의 모든 스냅샷이 무효화된다는 것을 이해했는지 확인하고 * Remove * 를 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터는 CLI를 사용하여 일관성 그룹에서 볼륨을 제거할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

단계

1. 볼륨을 제거합니다. 를 클릭합니다 `-volumes` 매개 변수에는 쉼표로 구분된 볼륨 목록을 사용할 수 있습니다.

   만 포함합니다 `-parent-consistency-group` 일관성 그룹이 계층적 관계에 있는 경우 매개 변수입니다.

   ```
   consistency-group volume remove -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volume volumes
   ```

일관성 그룹 간에 볼륨 이동

ONTAP 9.13.1부터 부모 항목을 공유하는 하위 일관성 그룹 간에 볼륨을 이동할 수 있습니다.

이 작업에 대해

- 동일한 상위 일관성 그룹 아래에 중첩된 일관성 그룹 간에만 볼륨을 이동할 수 있습니다.
- 기존 일관성 그룹 스냅샷이 잘못되어 일관성 그룹 스냅샷으로 더 이상 액세스할 수 없습니다. 개별 볼륨 스냅샷은 유효한 상태로 유지됩니다.
- 부모 정합성 보장 그룹의 스냅샷은 유효한 상태로 유지됩니다.
- 모든 볼륨을 하위 일관성 그룹 밖으로 이동하면 해당 일관성 그룹이 삭제됩니다.
- 정합성 보장 그룹에 대한 수정 사항은 을 준수해야 합니다 정합성 보장 그룹 제한.

시스템 관리자

ONTAP 9.12.1부터 System Manager로 이 작업을 수행할 수 있습니다.

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 이동할 볼륨이 포함된 상위 일관성 그룹을 선택합니다. 하위 일관성 그룹을 찾은 다음 볼륨 메뉴를 확장합니다. 이동할 볼륨을 선택합니다.
3. 이동을 선택합니다.
4. 볼륨을 새 일관성 그룹 또는 기존 그룹으로 이동할지 여부를 선택합니다.
   a. 기존 일관성 그룹으로 이동하려면 기존 자식 일관성 그룹을 선택한 다음 드롭다운 메뉴에서 일관성 그룹의 이름을 선택합니다.
   b. 새 일관성 그룹으로 이동하려면 새 하위 일관성 그룹을 선택합니다. 새 하위 일관성 그룹의 이름을 입력하고 구성 요소 유형을 선택합니다.
5. 이동을 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터는 ONTAP CLI를 사용하여 일관성 그룹 간에 볼륨을 이동할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

볼륨을 새 하위 정합성 보장 그룹으로 이동합니다

1. 다음 명령을 실행하면 지정된 볼륨이 포함된 새 하위 정합성 보장 그룹이 생성됩니다.

   새 일관성 그룹을 생성할 때 새 스냅샷, QoS 및 계층화 정책을 지정할 수 있습니다.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -new-consistency-group
   consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
   -policy policy]
   ```

볼륨을 기존 하위 정합성 보장 그룹으로 이동합니다

1. 볼륨을 재할당합니다. 를 클릭합니다 `-volumes` 매개 변수에는 쉼표로 구분된 볼륨 이름 목록을 사용할 수 있습니다.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -to-consistency-group
   target_consistency_group
   ```

관련 정보

- 정합성 보장 그룹 제한
- 일관성 그룹의 클론을 생성합니다

ONTAP 일관성 그룹 지오메트리 수정

ONTAP 9.13.1부터 정합성 보장 그룹의 지오메트리를 수정할 수 있습니다. 정합성 보장 그룹의 구조를 수정하면 지속적인 입출력 작업을 중단하지 않고 하위 또는 상위 정합성 보장 그룹의 구성을 변경할 수 있습니다.

정합성 보장 그룹 구조를 수정하면 정합성 보장 그룹의 기존 스냅샷에 영향을 줍니다. 자세한 내용은 수행하려는 지오메트리의 특정 수정 사항을 참조하십시오.

원격 보호 정책으로 구성된 정합성 보장 그룹의 구조는 수정할 수 없습니다. 먼저 보호 관계를 끊은 후 지오메트리를 수정한 다음 원격 보호를 복원해야 합니다.

새 하위 일관성 그룹을 추가합니다

ONTAP 9.13.1부터 새 하위 일관성 그룹을 기존 부모 일관성 그룹에 추가할 수 있습니다.

이 작업에 대해

- 부모 일관성 그룹에는 최대 5개의 자식 일관성 그룹이 포함될 수 있습니다. 을 참조하십시오 정합성 보장 그룹 제한 기타 제한.
- 단일 일관성 그룹에는 하위 일관성 그룹을 추가할 수 없습니다. 먼저 해야 합니다 [승격] 그러면 일관성 그룹을 자식 일관성 그룹에 추가할 수 있습니다.
- 확장 작업 전에 캡처된 정합성 보장 그룹의 기존 스냅샷은 부분적으로 간주됩니다. 해당 스냅샷을 기반으로 하는 모든 복구 작업은 스냅샷 시점에 정합성 보장 그룹을 반영합니다.

예 **32.** 단계

시스템 관리자

ONTAP 9.13.1부터 System Manager로 이 작업을 수행할 수 있습니다.

새 하위 일관성 그룹을 추가합니다

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 하위 일관성 그룹을 추가할 상위 일관성 그룹을 선택합니다.
3. 부모 일관성 그룹의 이름 옆에 있는 자세히 를 선택한 다음 새 자식 일관성 그룹 추가 를 선택합니다.
4. 일관성 그룹의 이름을 입력합니다.
5. 새 볼륨이나 기존 볼륨을 추가할지 여부를 선택합니다.
   a. 기존 볼륨을 추가하는 경우 **existing volumes** 를 선택한 다음 드롭다운 메뉴에서 볼륨을 선택합니다.
   b. 새 볼륨을 추가하는 경우 새 볼륨 을 선택한 다음 볼륨 수와 해당 크기를 지정합니다.
6. 추가 를 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 하위 정합성 보장 그룹을 추가할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

새 볼륨이 포함된 하위 정합성 보장 그룹을 추가합니다

1. 새 일관성 그룹을 생성합니다. 일관성 그룹 이름, 볼륨 접두사, 볼륨 수, 볼륨 크기, 스토리지 서비스 등의 값을 입력합니다. 및 엑스포트 정책 이름:

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
-volume-prefix prefix -volume-count number -size size -storage-service
service -export-policy policy_name
```

기존 볼륨이 있는 하위 정합성 보장 그룹을 추가합니다

1. 새 일관성 그룹을 생성합니다. 를 클릭합니다 `volumes` 매개 변수에는 쉼표로 구분된 볼륨 이름 목록을 사용할 수 있습니다.

```
consistency-group create -vserver SVM_name -consistency-group
new_consistency_group -parent-consistency-group parent_consistency_group
-volumes volume
```

하위 일관성 그룹을 분리합니다

ONTAP 9.13.1부터 부모 일관성 그룹을 제거하여 개별 일관성 그룹으로 변환할 수 있습니다.

이 작업에 대해

- 하위 정합성 보장 그룹을 분리하면 부모 정합성 보장 그룹의 스냅샷이 무효화되고 액세스할 수 없게 됩니다. 볼륨 세분화 스냅샷은 유효한 상태로 유지됩니다.
- 개별 정합성 보장 그룹의 기존 스냅샷은 유효한 상태로 유지됩니다.
- 분리할 하위 정합성 보장 그룹과 이름이 같은 기존 단일 정합성 보장 그룹이 있는 경우 이 작업이 실패합니다. 이 시나리오가 발생한 경우 일관성 그룹을 분리할 때 일관성 그룹의 이름을 변경해야 합니다.

예 **33.** 단계

시스템 관리자

ONTAP 9.13.1부터 System Manager로 이 작업을 수행할 수 있습니다.

하위 일관성 그룹을 분리합니다

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 분리할 자식이 포함된 부모 일관성 그룹을 선택합니다.
3. 분리하려는 하위 일관성 그룹 옆에 있는 자세히 를 선택한 다음 부모에서 분리 를 선택합니다.
4. 선택적으로 일관성 그룹의 이름을 바꾸고 애플리케이션 유형을 선택합니다.
5. 분리 를 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 하위 정합성 보장 그룹을 분리할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

하위 일관성 그룹을 분리합니다

1. 정합성 보장 그룹을 분리합니다. 필요한 경우 분리된 정합성 보장 그룹의 이름을 로 변경합니다 `-new-name` 매개 변수.

   ```
   consistency-group detach -vserver SVM_name -consistency-group
   child_consistency_group -parent-consistency-group parent_consistency_group
   [-new-name new_name]
   ```

부모 일관성 그룹 아래에서 기존 단일 일관성 그룹을 이동합니다

ONTAP 9.13.1부터 기존 단일 일관성 그룹을 하위 일관성 그룹으로 변환할 수 있습니다. 이동 작업 중에 일관성 그룹을 기존 부모 일관성 그룹 아래로 이동하거나 새 부모 일관성 그룹을 생성할 수 있습니다.

이 작업에 대해

- 상위 일관성 그룹의 하위 항목이 4개 이하가 되어야 합니다. 부모 일관성 그룹에는 최대 5개의 자식 일관성 그룹이 포함될 수 있습니다. 을 참조하십시오 정합성 보장 그룹 제한 기타 제한.
- 이 작업을 수행하기 전에 캡처한 _parent_consistency 그룹의 기존 스냅샷은 부분적으로 간주됩니다. 이러한 스냅샷 중 하나를 기반으로 하는 복구 작업은 스냅샷의 특정 시점에 정합성 보장 그룹을 반영합니다.

- 단일 일관성 그룹의 기존 일관성 그룹 스냅샷은 유효한 상태를 유지합니다.

예 **34.** 단계

시스템 관리자

ONTAP 9.13.1부터 System Manager로 이 작업을 수행할 수 있습니다.

부모 일관성 그룹 아래에서 기존 단일 일관성 그룹을 이동합니다

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 변환할 일관성 그룹을 선택합니다.
3. 더 보기 를 선택한 다음 다른 정합성 보장 그룹 아래로 이동** 을 선택합니다.
4. 선택적으로 일관성 그룹의 새 이름을 입력하고 구성요소 유형을 선택합니다. 기본적으로 부품 유형은 다른 유형입니다.
5. 기존 부모 일관성 그룹으로 마이그레이션하거나 새 부모 일관성 그룹을 생성할지 선택합니다.
   a. 기존 부모 일관성 그룹으로 마이그레이션하려면 기존 일관성 그룹을 선택한 다음 드롭다운 메뉴에서 일관성 그룹을 선택합니다.
   b. 새 부모 일관성 그룹을 생성하려면 새 일관성 그룹을 선택한 다음 새 일관성 그룹의 이름을 제공합니다.
6. 이동을 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터는 ONTAP CLI를 사용하여 단일 일관성 그룹을 부모 일관성 그룹 아래로 이동할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

일관성 그룹을 새 부모 일관성 그룹 아래로 이동합니다

1. 새 부모 일관성 그룹을 생성합니다. 를 클릭합니다 `-consistency-groups` 매개 변수는 기존 일관성 그룹을 새 부모로 마이그레이션합니다.

```
consistency-group attach -vserver svm_name -consistency-group
parent_consistency_group -consistency-groups child_consistency_group
```

기존 일관성 그룹 아래에서 일관성 그룹을 이동합니다

1. 정합성 보장 그룹 이동:

```
consistency-group add -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
```

하위 일관성 그룹을 승격합니다

ONTAP 9.13.1부터 단일 일관성 그룹을 부모 일관성 그룹으로 승격할 수 있습니다. 단일 일관성 그룹을 상위 일관성 그룹으로 승격하면 원래의 단일 일관성 그룹에 있는 모든 볼륨을 상속하는 새 하위 일관성 그룹도 생성됩니다.

이 작업에 대해

- 하위 일관성 그룹을 부모 일관성 그룹으로 변환하려면 먼저 해야 합니다 [detach] 그런 다음 하위 일관성 그룹을 이 절차에 따릅니다.
- 정합성 보장 그룹을 프로모션한 후에도 정합성 보장 그룹의 기존 스냅샷은 유효한 상태로 유지됩니다.

시스템 관리자

ONTAP 9.13.1부터 System Manager로 이 작업을 수행할 수 있습니다.

하위 일관성 그룹을 승격합니다

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 상향 이동할 정합성 보장 그룹을 선택합니다.
3. 더 보기 를 선택한 다음 부모 일관성 그룹으로 승격** 을 선택합니다.
4. 이름 을 입력하고 자식 일관성 그룹에 대한 구성 요소 형식 을 선택합니다.
5. 승격을 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터는 ONTAP CLI를 사용하여 단일 일관성 그룹을 부모 일관성 그룹 아래로 이동할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

하위 일관성 그룹을 승격합니다

1. 정합성 보장 그룹을 승격합니다. 이 명령은 부모 정합성 보장 그룹 하나와 자식 정합성 보장 그룹 하나를 생성합니다.

```
consistency-group promote -vserver SVM_name -consistency-group
existing_consistency_group -new-name new_child_consistency_group
```

상위 항목을 단일 일관성 그룹으로 강등합니다

ONTAP 9.13.1부터 부모 일관성 그룹을 단일 일관성 그룹으로 강등할 수 있습니다. 모체를 강등하면 정합성 보장 그룹의 계층 구조가 평평하여 연결된 모든 자식 일관성 그룹이 제거됩니다. 일관성 그룹의 모든 볼륨은 새로운 단일 일관성 그룹에 유지됩니다.

이 작업에 대해

- parent_consistency 그룹의 기존 스냅샷은 단일 정합성 보장으로 하향 이동한 후에도 유효한 상태로 유지됩니다. 해당 부모의 associated_child_consistency 그룹 중 하나라도 강등 시 기존 스냅샷이 유효하지 않게 됩니다. 하위 정합성 보장 그룹 내의 개별 볼륨 스냅샷은 볼륨 세분화 스냅샷으로 계속 액세스할 수 있습니다.

예 **35.** 단계

시스템 관리자

ONTAP 9.13.1부터 System Manager로 이 작업을 수행할 수 있습니다.

일관성 그룹을 강등합니다

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 강등할 상위 일관성 그룹을 선택합니다.
3. 더 보기 를 선택한 다음 단일 정합성 보장 그룹으로 하향 이동** 을 선택합니다.
4. 연결된 모든 하위 정합성 보장 그룹이 삭제되고 해당 볼륨이 새 단일 정합성 보장 그룹 아래로 이동된다는 경고 메시지가 표시됩니다. 하향 이동 을 선택하여 충격 이해 여부를 확인합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 일관성 그룹을 강등할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

일관성 그룹을 강등합니다

1. 정합성 보장 그룹을 강등합니다. 옵션 을 사용합니다 `-new-name` 일관성 그룹의 이름을 바꾸는 매개 변수입니다.

   ```
   consistency-group demote -vserver SVM_name -consistency-group
   parent_consistency_group [-new-name new_consistency_group_name]
   ```

ONTAP 일관성 그룹 애플리케이션 및 구성 요소 태그 수정

ONTAP 9.12.1부터 정합성 보장 그룹은 구성 요소 및 애플리케이션 태그 지정을 지원합니다. 애플리케이션 및 구성 요소 태그는 관리 툴로서 일관성 그룹의 다양한 워크로드를 필터링하고 식별할 수 있습니다.

이 작업에 대해

정합성 보장 그룹은 다음 두 가지 유형의 태그를 제공합니다.

- 응용 프로그램 태그: 이러한 태그는 개별 및 부모 일관성 그룹에 적용됩니다. 애플리케이션 태그는 MongoDB, Oracle, SQL Server와 같은 워크로드에 대한 레이블링을 제공합니다. 일관성 그룹의 기본 애플리케이션 태그는 기타입니다.
- 구성 요소 태그: 계층적인 정합성 보장 그룹의 하위 요소에는 응용 프로그램 태그 대신 구성 요소 태그가 있습니다. 구성 요소 태그에 대한 옵션은 "데이터", "로그" 또는 "기타"입니다. 기본값은 기타 입니다.

일관성 그룹을 생성하거나 일관성 그룹을 생성한 후에 태그를 적용할 수 있습니다.

일관성 그룹에 SnapMirror 활성 동기화 관계가 있는 경우 * 기타 * 를 애플리케이션 또는 구성 요소 태그로 사용해야 합니다.

단계

ONTAP 9.12.1부터 System Manager를 사용하여 응용 프로그램 및 구성 요소 태그를 수정할 수 있습니다. ONTAP 9.14.1부터 ONTAP CLI를 사용하여 응용 프로그램 및 구성 요소 태그를 수정할 수 있습니다.

시스템 관리자

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 태그를 수정할 일관성 그룹을 선택합니다. 일관성 그룹 이름 옆의 를 선택하고 * Edit * 를 선택합니다 .
3. 드롭다운 메뉴에서 적절한 응용 프로그램 또는 구성 요소 태그를 선택합니다.
4. 저장 * 을 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 기존 일관성 그룹의 애플리케이션 또는 구성 요소 태그를 수정할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

응용 프로그램 태그를 수정합니다

1. 애플리케이션 태그에는 제한된 수의 사전 설정 문자열을 사용할 수 있습니다. 허용되는 문자열 목록을 보려면 다음 명령을 실행합니다.
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type ?`
2. 출력에서 적절한 문자열을 선택하고 정합성 보장 그룹을 수정합니다.
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type application_type`

부품 태그를 수정합니다

1. 부품 유형을 수정합니다. 구성 요소 유형은 데이터, 로그 또는 기타일 수 있습니다. SnapMirror 액티브 동기화를 사용 중인 경우 "기타"여야 합니다.
   `consistency-group modify -vserver` *`svm`* `-consistency-group` *`child_consistency_group`* `-parent-consistency-group` *`parent_consistency_group`* `-application-component-type [data|logs|other]`

ONTAP 일관성 그룹 복제

ONTAP 9.12.1부터는 일관성 그룹을 클론 복제하여 일관성 그룹 및 해당 콘텐츠의 복사본을 생성할 수 있습니다. 일관성 그룹을 클론 복제하면 일관성 그룹 구성의 복사본, 애플리케이션 유형과 같은 메타데이터, 파일, 디렉토리, LUN 또는 NVMe 네임스페이스와 같은 모든 볼륨과 해당 콘텐츠의 복사본이 생성됩니다.

이 작업에 대해

일관성 그룹을 클론 복제할 때는 현재 구성으로 클론을 생성할 수 있지만 볼륨 콘텐츠를 그대로 사용하거나 기존 일관성 그룹 스냅샷을 기반으로 클론을 생성할 수 있습니다.

일관성 그룹의 클론은 전체 일관성 그룹에 대해서만 지원됩니다. 계층적 관계에서 개별 하위 일관성 그룹을 클론 복제할 수 없습니다. 전체 일관성 그룹 구성만 클론 복제할 수 있습니다.

일관성 그룹을 클론 복제할 때 다음 구성 요소는 클론 복제되지 않습니다.

- iGroup
- LUN 매핑
- NVMe 하위 시스템
- NVMe 네임스페이스 서브시스템 맵

시작하기 전에

- 일관성 그룹을 클론 복제할 때 공유 이름이 지정되지 않은 경우 ONTAP은 클론 복제된 볼륨에 대한 SMB 공유를 생성하지 않습니다. * 접합 경로가 지정되지 않은 경우 클론 생성된 정합성 보장 그룹이 마운트되지 않습니다.
- 정합성 보장 그룹의 현재 구성 볼륨을 반영하지 않는 스냅샷을 기반으로 정합성 보장 그룹을 클론 복제하려고 하면 작업이 실패합니다.
- 일관성 그룹의 클론을 생성한 후에는 적절한 매핑 작업을 수행해야 합니다.

  을 참조하십시오 여러 LUN에 igroup 매핑 또는 NVMe 네임스페이스를 하위 시스템에 매핑합니다 를 참조하십시오.

- 일관성 그룹의 클론 복제는 SnapMirror 액티브 동기화 관계의 일관성 그룹 또는 관련 DP 볼륨의 일관성 그룹에 대해 지원되지 않습니다.

시스템 관리자

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 일관성 그룹 * 메뉴에서 클론 복제할 일관성 그룹을 선택합니다.
3. 일관성 그룹의 개요 페이지 오른쪽 위에서 * Clone * 을 선택합니다.
4. 클론 복제된 새 일관성 그룹의 이름을 입력하거나 기본 이름을 그대로 사용합니다.
   a. 활성화 여부를 선택합니다 "* 씬 프로비저닝 *".
   b. 소스에서 정합성 보장 그룹을 분리시키고 클론 정합성 보장 그룹에 추가 디스크 공간을 할당하려면 * 클론 분할 * 을 선택합니다.
5. 일관성 그룹을 현재 상태로 복제하려면 *새 스냅샷 추가*를 선택합니다.

   스냅샷을 기반으로 일관성 그룹을 클론 복제하려면 * Use an existing snapshot * 을 선택합니다. 이 옵션을 선택하면 새 하위 메뉴가 열립니다. 클론 작업의 기준으로 사용할 스냅샷을 선택합니다.
6. 클론 * 을 선택합니다.
7. 정합성 보장 그룹 * 메뉴로 돌아가 정합성 보장 그룹의 클론이 생성되었는지 확인합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 클러스터 관리자 자격 증명과 함께 CLI를 사용하여 일관성 그룹을 클론 복제할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

일관성 그룹의 클론을 생성합니다

1. 이 `consistency-group clone create` 명령은 일관성 그룹의 현재 시점 상태를 복제합니다. 스냅샷을 기반으로 클론 작업의 기준을 설정하려면 `-source-snapshot` 매개 변수를 포함합니다.

   ```
   consistency-group clone create -vserver svm_name -consistency-group
   clone_name -source-consistency-group consistency_group_name [-source-
   snapshot snapshot_name]
   ```

   에 대한 자세한 내용은 `consistency-group clone create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 단계

- 여러 LUN에 igroup 매핑
- NVMe 네임스페이스를 하위 시스템에 매핑합니다

ONTAP 일관성 그룹 삭제

일관성 그룹이 더 이상 필요하지 않다고 결정한 경우 삭제할 수 있습니다.

이 작업에 대해

- 일관성 그룹을 삭제하면 일관성 그룹의 인스턴스가 삭제되며 구성 볼륨 또는 LUN에 영향을 주지 않습니다. 정합성 보장 그룹을 삭제해도 각 볼륨에 있는 스냅샷은 삭제되지 않지만 정합성 보장 그룹 스냅샷으로는 더 이상 액세스할 수 없습니다. 하지만 스냅샷은 일반 볼륨 세분화 스냅샷처럼 계속 관리할 수 있습니다.
- ONTAP은 일관성 그룹에 있는 볼륨이 모두 삭제된 경우 일관성 그룹을 자동으로 삭제합니다.
- 부모 일관성 그룹을 삭제하면 연결된 모든 하위 일관성 그룹이 삭제됩니다.
- 9.10.1 ~ 9.12.0 사이의 ONTAP 버전을 사용하는 경우 볼륨 자체가 삭제된 경우에만 정합성 보장 그룹에서 볼륨을 제거할 수 있으며, 이 경우 볼륨이 정합성 보장 그룹에서 자동으로 제거됩니다. ONTAP 9.12.1부터 일관성 그룹을 삭제하지 않고도 일관성 그룹에서 볼륨을 제거할 수 있습니다. 이 프로세스에 대한 자세한 내용은 을 참조하십시오 일관성 그룹 수정.

예 **36.** 단계

시스템 관리자

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 삭제할 일관성 그룹을 선택합니다.
3. 일관성 그룹 이름 옆의 * Delete * 를 차례로 선택합니다 ⋮ .

CLI를 참조하십시오

ONTAP 9.14.1부터 CLI를 사용하여 일관성 그룹을 삭제할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

일관성 그룹을 삭제합니다

1. 정합성 보장 그룹 삭제:

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

SnapMirror 활성 동기화

소개

ONTAP SnapMirror Active Sync에 대해 알아보세요

SnapMirror Active Sync는 SnapMirror Business Continuity(SM-BC)라고도 하며, 사이트 전체에 장애가 발생하더라도 비즈니스 서비스가 계속 작동할 수 있도록 합니다. 이 기술을 사용하면 수동 개입이나 사용자 정의 스크립팅 없이도 애플리케이션이 원활하게 보조 복사본으로 장애 조치될 수 있습니다.

NetApp SnapMirror Active Sync(SM-as)는 자동 장애 조치를 통해 보다 세분화되고 비용이 저렴하며 사용하기 쉬운

애플리케이션 수준 보호 기능을 제공하도록 설계되었습니다. SnapMirror 액티브 동기화를 사용하면 사이트 전체에 장애가 발생하는 경우에도 미션 크리티컬 비즈니스 서비스가 계속 운영될 수 있습니다. SnapMirror 활성 동기화를 사용하면 지리적으로 분산된 위치의 사이트 간에 애플리케이션의 여러 볼륨을 동기식으로 복제할 수 있습니다(일관성 그룹에 추가하여). 1차 데이터베이스가 중단되는 경우 자동으로 2차 데이터베이스로 장애 조치를 취해 1계층 애플리케이션의 비즈니스 연속성을 확보할 수 있습니다.

일부 국가의 금융 기관 규정에 따라 기업은 2차 데이터 센터에서 주기적으로 서비스를 제공받아야 합니다. SnapMirror Active Sync는 고가용성 클러스터를 통해 비즈니스 연속성을 위한 이러한 데이터 센터 전환을 지원합니다.

ONTAP 9.9.1부터 사용 가능한 SnapMirror Active Sync는 AFF 및 All-Flash SAN Array(ASA) 클러스터에서 지원됩니다. 기본 클러스터와 보조 클러스터는 ASA, ASA r2 또는 AFF 중 하나와 같은 유형이어야 합니다. SnapMirror Active Sync는 iSCSI 또는 FCP LUN 또는 NVMe 네임스페이스를 사용하여 애플리케이션을 보호합니다.

SnapMirror Active Sync는 대칭 및 비대칭 구성을 모두 지원합니다. ONTAP 9.15.1에서는 대칭적 액티브/액티브에 대한 지원이 도입되었습니다. 대칭적 활성/활성 구성을 사용하면 보호된 LUN의 두 사본 모두 양방향 동기 복제를 통해 읽기 및 쓰기 I/O 작업을 수행할 수 있으므로 각 LUN 사본이 로컬 I/O 요청을 처리할 수 있습니다.

2024년 7월부터 이전에 PDF로 게시된 기술 보고서의 콘텐츠가 ONTAP 제품 문서와 통합되었습니다. 이제 ONTAP SnapMirror 액티브 동기화 문서에 _TR-4878: SnapMirror active sync_의 콘텐츠가 포함되어 있습니다.

이점

SnapMirror 액티브 동기화는 다음과 같은 이점을 제공합니다.

- 비즈니스 크리티컬 애플리케이션을 위한 지속적인 가용성:
- 주요 애플리케이션을 운영 사이트와 보조 사이트에서 교대로 호스팅할 수 있습니다.
- 정합성 보장 그룹을 사용하여 애플리케이션 관리를 간소화하여 종속 쓰기 순서 정합성 보장
- 각 애플리케이션의 장애 조치를 테스트하는 기능
- 애플리케이션 가용성에 영향을 주지 않고 미러 클론을 즉시 생성
- 동일한 ONTAP 클러스터에 보호된 워크로드와 보호되지 않은 워크로드를 구축할 수 있습니다.
- LUN, NVMe 네임스페이스, NVMe 하위 시스템 또는 스토리지 장치 ID는 동일하게 유지되므로 애플리케이션은 이를 공유 가상 장치로 인식합니다.
- 2차 클러스터를 유연하게 재사용하여 애플리케이션 성능 또는 가용성에 영향을 주지 않고 개발 테스트, UAT 또는 보고용으로 애플리케이션 사용을 위한 즉각적인 클론을 생성할 수 있습니다.

SnapMirror 액티브 싱크를 사용하면 데이터 LUN 또는 NVMe 네임스페이스를 보호하여 재해 발생 시 비즈니스 연속성을 위해 애플리케이션을 투명하게 페일오버할 수 있습니다. 자세한 내용은 다음을 참조하세요. "사용 사례" .

주요 개념

SnapMirror Active Sync는 일관성 그룹을 사용하여 데이터가 복제되도록 보장합니다. SnapMirror Active Sync는 ONTAP Mediator를 사용하거나 ONTAP 9.17.1부터는 Cloud Mediator를 사용하여 자동 장애 조치를 수행하여 재해 발생 시에도 데이터가 제공되도록 보장합니다. SnapMirror Active Sync 배포를 계획할 때는 SnapMirror Active Sync의 핵심 개념과 아키텍처를 이해하는 것이 중요합니다.

비대칭 및 대칭

대칭형 액티브/액티브 구성에서는 두 사이트 모두 액티브 I/O를 위해 로컬 스토리지에 액세스할 수 있습니다. 대칭형 액티브/액티브 구성은 VMware vMSC, SQL 기반 Windows 장애 조치 클러스터, Oracle RAC를 포함한 클러스터형

애플리케이션에 최적화되어 있습니다.

비대칭 액티브/액티브 구성에서는 보조 사이트의 데이터가 LUN, 네임스페이스 또는 스토리지 장치에 프록시됩니다.

자세한 내용은 을 참조하십시오 SnapMirror 액티브 동기화 아키텍처.

일관성 그룹

AFF 및 ASA 시스템의 경우 "일관성 그룹" 비즈니스 연속성을 위해 보호해야 하는 애플리케이션 워크로드에 대한 일관성을 보장하는 FlexVol 볼륨의 집합입니다. ASA r2 시스템에서 일관성 그룹은 스토리지 유닛의 집합입니다.

일관성 그룹의 목적은 볼륨 또는 스토리지 유닛 컬렉션의 스냅샷 이미지를 동시에 생성하여 특정 시점에 해당 컬렉션의 충돌 발생 시에도 일관된 복사본을 유지하는 것입니다. 일관성 그룹은 데이터세트의 모든 볼륨이 정지되었다가 정확히 동일한 시점에 스냅샷되도록 보장합니다. 이를 통해 데이터세트를 지원하는 볼륨 또는 스토리지 유닛 전반에 걸쳐 데이터 일관성이 유지되는 복원 지점을 제공합니다. 따라서 일관성 그룹은 종속 쓰기 순서 일관성을 유지합니다. 비즈니스 연속성을 위해 애플리케이션을 보호하려는 경우, 해당 애플리케이션에 해당하는 볼륨 또는 스토리지 유닛 그룹을 일관성 그룹에 추가하여 소스 일관성 그룹과 대상 일관성 그룹 간에 데이터 보호 관계를 설정해야 합니다. 소스 일관성 그룹과 대상 일관성 그룹에는 동일한 개수와 유형의 볼륨이 포함되어야 합니다.

구성 요소

SnapMirror 활성 동기화 관계에서 보호되는 일관성 그룹의 일부인 개별 볼륨, LUN 또는 NVMe 네임스페이스(ONTAP 9.17.1부터 시작).

ONTAP 중재자

그만큼 "ONTAP 중재자" 피어링된 ONTAP 클러스터 및 노드에 대한 상태 정보를 수신하여 두 클러스터 간 오케스트레이션을 수행하고 각 노드/클러스터가 정상 작동 중인지 확인합니다. ONTAP Mediator는 다음에 대한 상태 정보를 제공합니다.

- 피어 ONTAP 클러스터
- 피어 ONTAP 클러스터 노드입니다
- 일관성 그룹(SnapMirror 활성 동기화 관계에서 페일오버 유닛을 정의). 각 일관성 그룹에 대해 다음 정보가 제공됩니다.
  - 복제 상태: 초기화되지 않음, 동기화 중 또는 동기화 중단
  - 운영 복제본을 호스팅하는 클러스터
  - 작업 컨텍스트(계획된 페일오버에 사용됨)

이 ONTAP 중재자 상태 정보를 통해 클러스터는 서로 다른 유형의 장애를 구별하고 자동 페일오버를 수행할지 여부를 결정할 수 있습니다. ONTAP mediator는 ONTAP 클러스터(기본 및 보조) 모두와 함께 SnapMirror 액티브 동기화 쿼럼의 세 가지 파티 중 하나입니다. 합의에 도달하기 위해서는 정족수 중 적어도 두 당사자가 일정한 운영에 합의하여야 한다.

ONTAP 9.15.1부터 System Manager는 두 클러스터의 SnapMirror 활성 동기화 관계 상태를 표시합니다. System Manager의 두 클러스터 중 하나에서 ONTAP 중재자의 상태를 모니터링할 수도 있습니다. 이전 ONTAP 릴리즈에서는 소스 클러스터의 SnapMirror 활성 동기화 관계 상태가 System Manager에 표시됩니다.

ONTAP 클라우드 중재자

ONTAP Cloud Mediator는 ONTAP 9.17.1부터 사용할 수 있습니다. ONTAP Cloud Mediator는 NetApp 콘솔을 사용하여 클라우드에서 호스팅된다는 점을 제외하면 ONTAP Mediator와 동일한 서비스를 제공합니다.

계획된 페일오버

SnapMirror 활성 동기화 관계에서 복사본의 역할을 변경하기 위한 수동 작업입니다. 운영 사이트는 2차 사이트가 되고 2차 사이트는 1차 사이트가 됩니다.

자동 비계획 페일오버**(AUFO)**

미러 복제본에 대한 페일오버를 수행하는 자동 작업입니다. 이 작업은 ONTAP 중재자의 도움을 받아 운영 복제본을 사용할 수 없음을 감지해야 합니다.

1차 **- 1**차 및 **1**차 편향

SnapMirror 액티브 동기화는 네트워크 파티션 시 I/O를 제공하기 위해 기본 복사본을 우선적으로 사용하는 기본 원칙을 사용합니다.

Primary-bias는 SnapMirror Active Sync Protected 데이터 세트의 가용성을 개선하는 특별한 쿼럼 구현입니다. 운영 복사본을 사용할 수 있는 경우 두 클러스터 모두에서 ONTAP 중재자에 연결할 수 없을 때 운영 바이어스가 적용됩니다.

Primary-first 및 primary bias는 ONTAP 9.15.1부터 SnapMirror 액티브 동기화에서 지원됩니다. 1차 복사본은 System Manager에서 지정되고 REST API 및 CLI를 사용하여 출력됩니다.

동기화 중단**(OOS)**

응용 프로그램 입출력이 보조 스토리지 시스템으로 복제되지 않으면** 비동기 상태로 보고됩니다. 동기화 중단 상태는 보조 볼륨이 기본(소스)과 동기화되지 않았으며 SnapMirror 복제가 발생하지 않음을 의미합니다.

미러 상태가 `Snapmirrored` 이는 SnapMirror 관계가 설정되었고 데이터 전송이 완료되었음을 나타냅니다. 즉, 대상 볼륨이 소스 볼륨과 최신 상태임을 의미합니다.

SnapMirror 액티브 동기화는 자동 재동기화를 지원하여 복사본이 InSync 상태로 돌아갈 수 있도록 합니다.

ONTAP 9.15.1부터 SnapMirror 액티브 동기화가 지원됩니다 "팬아웃 구성의 자동 재구성".

균일 및 비균일 설정

- 호스트 액세스 균일 두 사이트의 호스트가 두 사이트의 스토리지 클러스터에 대한 모든 경로에 접속되어 있음을 의미합니다. 사이트 간 경로가 거리 전체에 걸쳐 확장됩니다.
- 비균일 호스트 액세스 각 사이트의 호스트가 동일한 사이트의 클러스터에만 연결되어 있음을 의미합니다. 사이트 간 경로 및 확장 경로가 연결되지 않았습니다.

모든 SnapMirror 액티브 동기식 배포에 대해 통일된 호스트 액세스가 지원되며, 비균일 호스트 액세스는 대칭 액티브/액티브 구축에만 지원됩니다.

제로 **RPO**

RPO는 지정된 기간 동안 허용되는 데이터 손실량인 복구 시점 목표를 나타냅니다. RPO가 0이면 데이터 손실이 허용되지 않습니다.

즉각적인 **RTO**

RTO는 복구 시간 목표를 나타냅니다. 이 시간은 운영 중단, 장애 또는 기타 데이터 손실 이벤트가 발생한 후 애플리케이션이 운영 중단 없이 정상 작업으로 돌아가도록 허용할 수 있는 시간입니다. RTO가 0이면 가동 중지 시간이 허용되지 않는다는 의미입니다.

ONTAP 버전에서 **SnapMirror Active Sync** 구성 지원

SnapMirror Active Sync에 대한 지원은 ONTAP 버전에 따라 다릅니다.

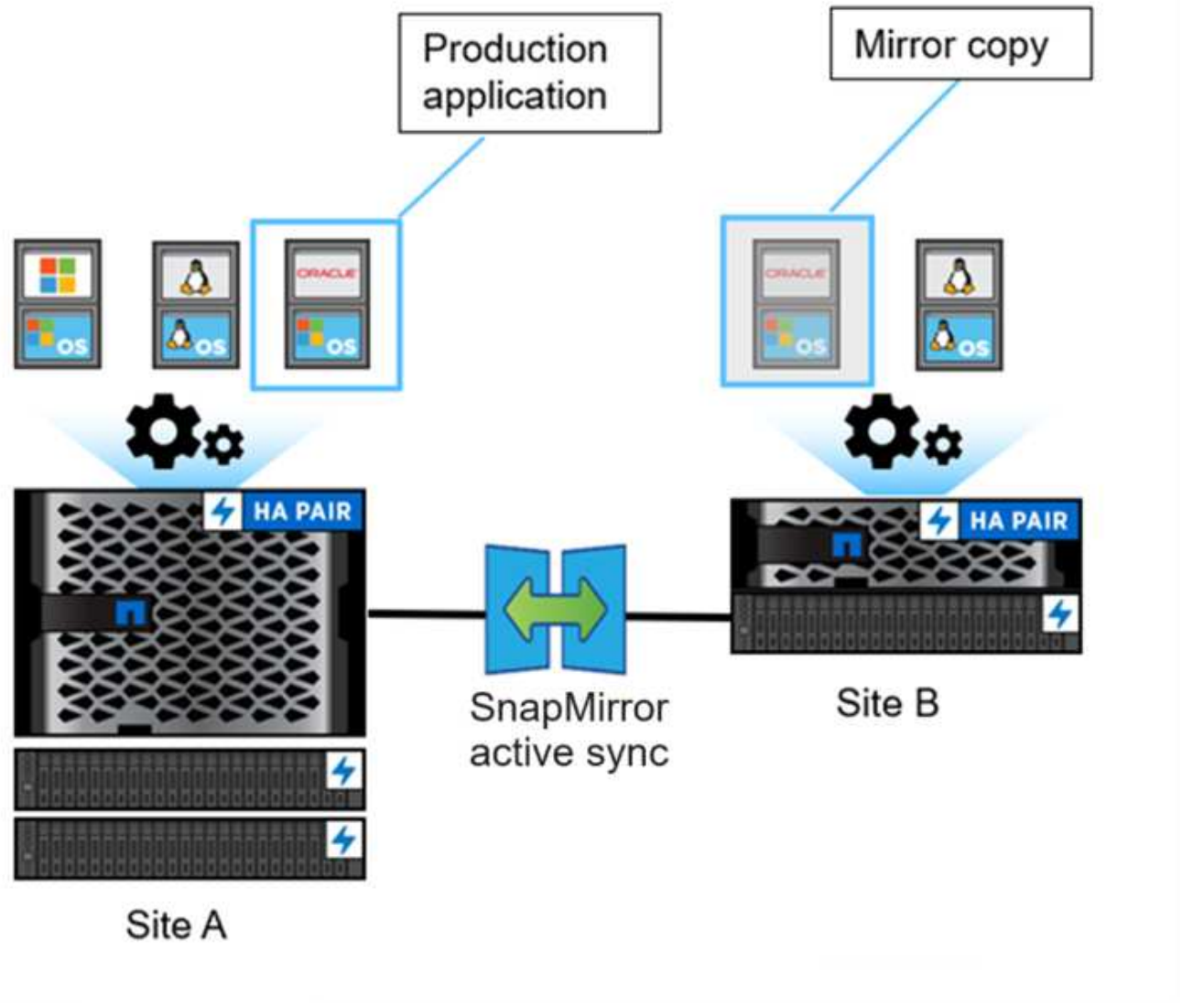
ONTAP 버전입니다	지원되는 클러스터	지원되는 프로토콜	지원되는 구성
9.17.1 이상	• AFF • ASA • C 시리즈 • ASA r2	• iSCSI • FC • VMware 워크로드를 위한 NVMe	• 비대칭 활성/활성 비대칭 활성/활성은 ASA r2 및 NVMe를 지원하지 않습니다. NVMe 지원에 대한 자세한 내용은 다음을 참조하세요. "NVMe 구성, 지원 및 제한 사항" . • 대칭적인 액티브/액티브
9.16.1 이상	• AFF • ASA • C 시리즈 • ASA r2	• iSCSI • FC	• 비대칭 활성/활성 • 대칭적 활성/활성 대칭적 활성/활성 구성은 ONTAP 9.16.1 이상에서 4노드 클러스터를 지원합니다. ASA r2의 경우 2노드 클러스터만 지원됩니다.
9.15.1 이상	• AFF • ASA • C 시리즈	• iSCSI • FC	• 비대칭 활성/활성 • 대칭적 활성/활성 대칭적 활성/활성 구성은 ONTAP 9.15.1에서 2노드 클러스터를 지원합니다. 4노드 클러스터는 ONTAP 9.16.1 이상에서 지원됩니다.
9.9.1 이상	• AFF • ASA • C 시리즈	• iSCSI • FC	비대칭 활성/활성

1차 및 2차 클러스터는 동일한 유형이어야 합니다. "ASA" , "ASA r2" , 또는 AFF.

ONTAP SnapMirror 액티브 싱크 아키텍처

SnapMirror 액티브 동기화 아키텍처는 두 클러스터 모두에서 활성 워크로드를 지원하여 기본 워크로드를 두 클러스터에서 동시에 처리할 수 있습니다. 일부 국가의 금융 기관 규정에서는 기업이 보조 데이터 센터에서도 주기적으로 서비스를 받을 수 있도록 요구합니다. 이를 "틱톡" 배포라고 하며, SnapMirror Active Sync를 통해 이를 구현할 수 있습니다.

비즈니스 연속성을 보호하기 위한 데이터 보호 관계는 스토리지 가상 머신(SVM) 내 여러 볼륨의 애플리케이션별 LUN 또는 NVMe 네임스페이스를 일관성 그룹에 추가하여 소스 스토리지 시스템과 대상 스토리지 시스템 간에 생성됩니다. 일반적인 운영 환경에서는 엔터프라이즈 애플리케이션이 기본 일관성 그룹에 데이터를 쓰고, 기본 일관성 그룹은 이 I/O를 미러 일관성 그룹에 동기적으로 복제합니다.



데이터 보호 관계에 두 개의 개별 데이터 사본이 존재하더라도 SnapMirror Active Sync는 동일한 LUN 또는 NVMe 네임스페이스 ID를 유지하므로 애플리케이션 호스트는 이를 여러 경로를 가진 공유 가상 장치로 인식하고, 한 번에 하나의 LUN 또는 NVMe 네임스페이스 사본에만 쓰기가 수행됩니다. 장애로 인해 기본 스토리지 시스템이 오프라인 상태가 되면 ONTAP 이 장애를 감지하고 Mediator를 사용하여 재확인합니다. ONTAP 과 Mediator 모두 기본 사이트에 ping을 보낼 수 없는 경우, ONTAP 자동 장애 조치(failover) 작업을 수행합니다. 이 프로세스를 통해 이전에는 장애

조치를 위해 필요했던 수동 개입이나 스크립팅 없이 특정 애플리케이션만 장애 조치할 수 있습니다.

기타 고려 사항:

- 비즈니스 연속성을 위한 보호 범위를 벗어나는 미러링되지 않은 볼륨이 지원됩니다.
- 비즈니스 연속성을 위해 보호되는 볼륨에 대해 하나의 다른 SnapMirror 비동기식 관계만 지원됩니다.
- Cascade 토폴로지는 무중단 업무 운영을 위한 보호 기능이 지원되지 않습니다.

중재자의 역할

SnapMirror Active Sync는 Mediator를 사용하여 SnapMirror Active Sync 복사본에 대한 수동 감시 역할을 합니다. 네트워크 파티션이 발생하거나 복사본 하나를 사용할 수 없는 경우, SnapMirror Active Sync는 Mediator를 사용하여 어떤 복사본이 I/O를 계속 처리할지 결정하고, 다른 복사본의 I/O는 중단합니다. 온프레미스 ONTAP Mediator 외에도 ONTAP 9.17.1부터 ONTAP Cloud Mediator를 설치하여 클라우드 배포 환경에서 동일한 기능을 제공할 수 있습니다. ONTAP Mediator 또는 ONTAP Cloud Mediator를 사용할 수 있지만, 동시에 사용할 수는 없습니다.

Mediator는 SnapMirror 액티브 동기화 구성에서 패시브 쿼럼 감시(passive quorum witness)로서 중요한 역할을 수행하여 쿼럼 유지 관리를 보장하고 장애 발생 시 데이터 액세스를 용이하게 합니다. 이는 컨트롤러가 피어 컨트롤러의 활성 상태를 확인하는 ping 프록시 역할을 합니다. Mediator는 스위치오버 작업을 직접 트리거하지는 않지만, 네트워크 통신 문제 발생 시 생존 노드가 파트너의 상태를 확인할 수 있도록 하는 중요한 기능을 제공합니다. ONTAP Mediator는 쿼럼 감시 역할을 수행하면서 피어 클러스터에 대한 대체 경로(실제로는 프록시 역할)를 제공합니다.

또한, 클러스터가 쿼럼 프로세스의 일부로 이 정보를 얻을 수 있도록 합니다. 통신 목적으로 노드 관리 LIF와 클러스터 관리 LIF를 사용합니다. 사이트 장애와 ISL(InterSwitch Link) 장애를 구분하기 위해 여러 경로를 통해 중복 연결을 설정합니다. 이벤트로 인해 클러스터가 Mediator 소프트웨어 및 모든 노드와의 연결이 끊어지면 연결할 수 없는 것으로 간주됩니다. 이 경우 경고가 발생하고 보조 사이트의 미러 일관성 그룹으로 자동 장애 조치가 활성화되어 클라이언트의 중단 없는 I/O가 보장됩니다. 복제 데이터 경로는 하트비트 메커니즘을 사용하며, 네트워크 오류나 이벤트가 일정 기간 이상 지속되면 하트비트 장애가 발생하여 관계가 동기화되지 않을 수 있습니다. 그러나 다른 포트로의 LIF 장애 조치와 같은 중복 경로가 있으면 하트비트를 유지하고 이러한 중단을 방지할 수 있습니다.

ONTAP 중재자

ONTAP Mediator는 모니터링하는 두 개의 ONTAP 클러스터와는 별개의 세 번째 장애 도메인에 설치됩니다. 이 설정에는 세 가지 핵심 구성 요소가 있습니다.

- SnapMirror 활성 동기화 운영 정합성 보장 그룹을 호스팅하는 운영 ONTAP 클러스터입니다
- 미러 정합성 보장 그룹을 호스팅하는 보조 ONTAP 클러스터입니다
- ONTAP 중재자

ONTAP Mediator는 다음 목적으로 사용됩니다.

- 정족수를 설정한다
- 자동 페일오버(AUFO)를 통한 지속적인 가용성
- 계획된 페일오버(PFO)

ONTAP Mediator 1.7은 비즈니스 연속성을 위해 10개의 클러스터 쌍을 관리할 수 있습니다.

ONTAP Mediator를 사용할 수 없는 경우 계획된 장애 조치나 자동 장애 조치를 수행할 수 없습니다. 애플리케이션 데이터는 어떠한 중단 없이 동기적으로 복제되므로 데이터 손실이 없습니다.

ONTAP 클라우드 중재자

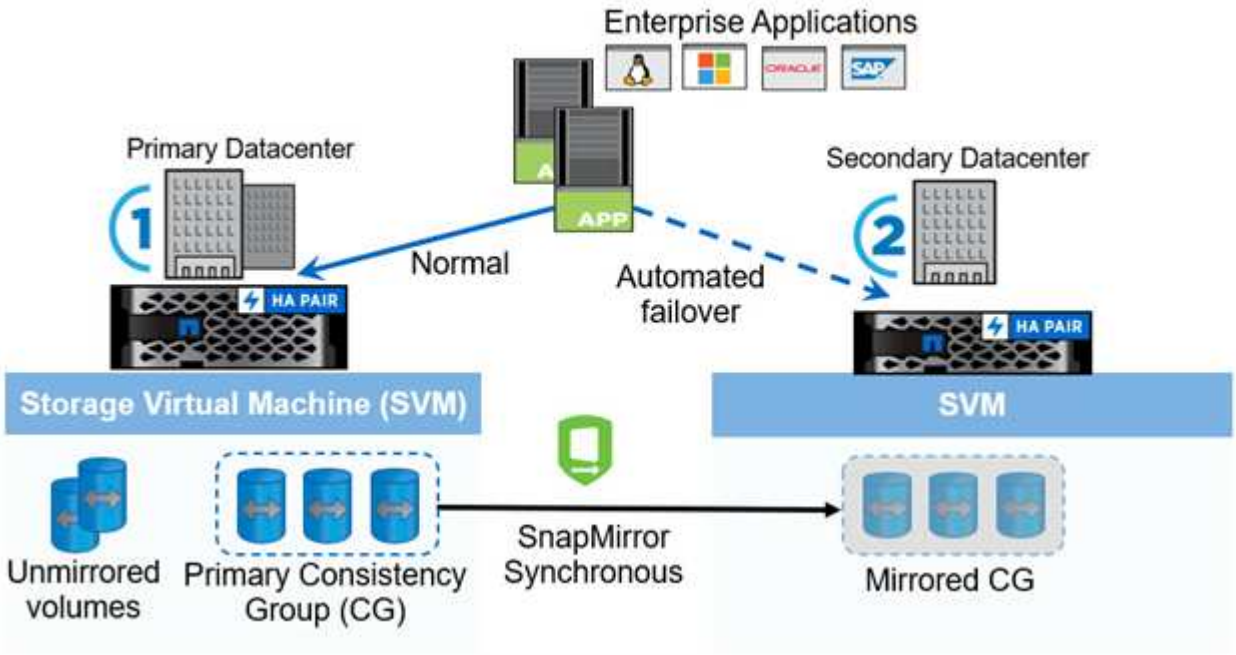
ONTAP 9.17.1부터 ONTAP Cloud Mediator는 NetApp 콘솔에서 클라우드 기반 서비스로 제공되며 SnapMirror Active Sync와 함께 사용할 수 있습니다. ONTAP Mediator와 유사하게 ONTAP Cloud Mediator는 SnapMirror 액티브 동기화 관계에서 다음과 같은 기능을 제공합니다.

- HA 또는 SnapMirror 활성 동기화 메타데이터에 대한 지속적이고 보호된 저장소를 제공합니다.
- 컨트롤러 활성을 위한 핑 프록시 역할을 합니다.
- quorum 결정에 도움이 되는 동기 노드 상태 쿼리 기능을 제공합니다.

ONTAP Cloud Mediator는 NetApp Console 클라우드 서비스를 관리할 필요가 없는 제3의 사이트로 사용하여 SnapMirror 활성 동기화 배포를 간소화하는 데 도움이 됩니다. ONTAP Cloud Mediator 서비스는 온프레미스 ONTAP Mediator와 동일한 기능을 제공하지만, 제3의 사이트 유지 관리에 따른 운영 복잡성을 줄여줍니다 . 반면, ONTAP Cloud Mediator는 패키지 형태로 제공되며, 운영을 위한 독립적인 전원 및 네트워크 인프라를 갖춘 제3의 사이트에서 실행되는 Linux 호스트에 설치해야 합니다.

SnapMirror Active Sync 작업 워크플로

다음 그림에서는 개괄적인 SnapMirror 액티브 동기화의 설계를 보여 줍니다.



이 다이어그램은 운영 데이터 센터의 SVM(스토리지 VM)에서 호스팅되는 엔터프라이즈 애플리케이션을 보여 줍니다. SVM은 볼륨 5개를 포함하며, 볼륨 3개는 일관성 그룹의 일부입니다. 일관성 그룹의 볼륨 3개가 보조 데이터 센터에 미러링됩니다. 정상적인 상황에서는 모든 쓰기 작업이 운영 데이터 센터에 수행됩니다. 실제로 이 데이터 센터는 I/O 작업의 소스로 사용되고, 보조 데이터 센터는 대상으로 작동합니다.

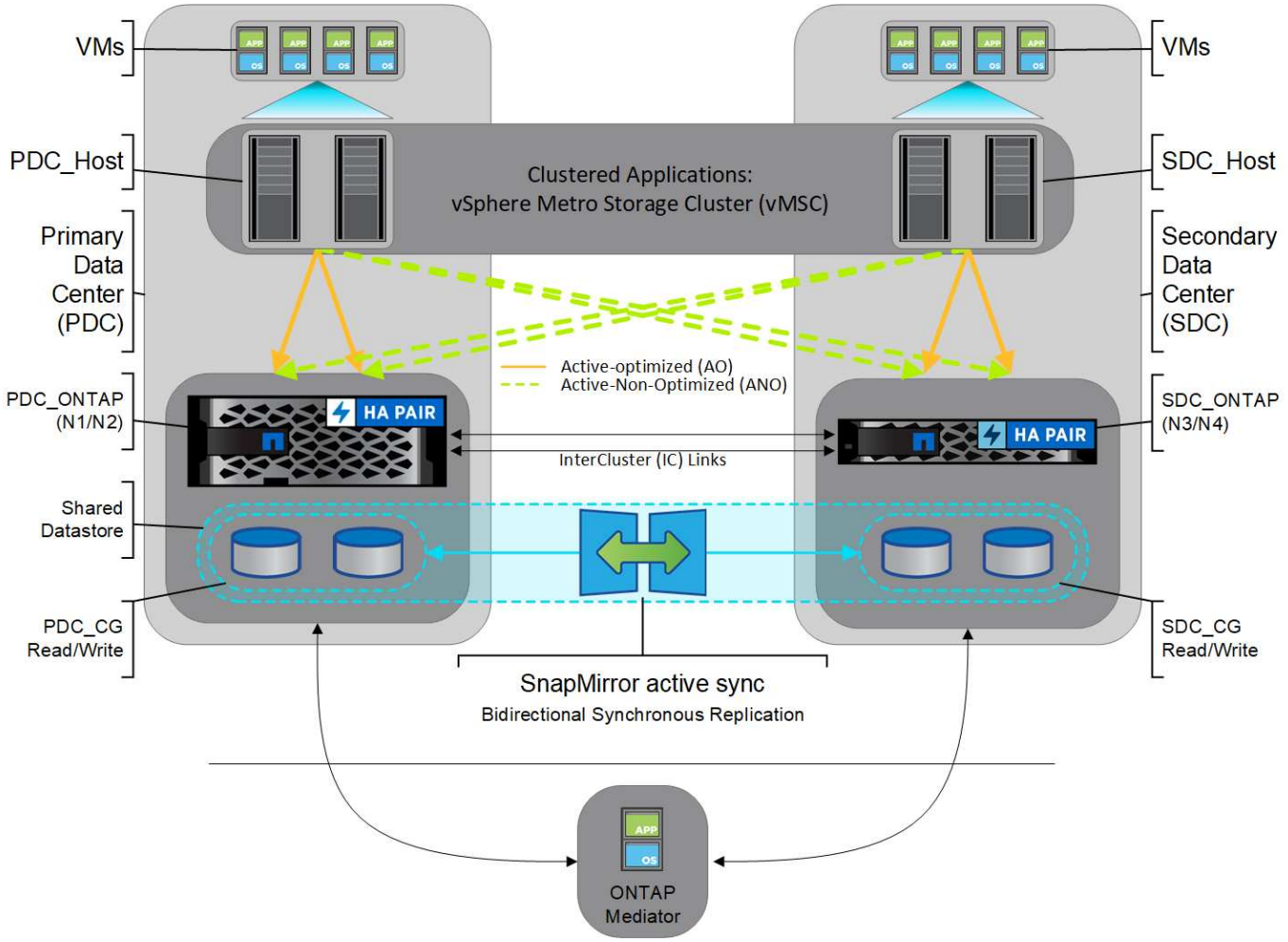
1차 데이터 센터에서 재해가 발생하는 경우 ONTAP 2차 데이터 센터가 1차 데이터 센터 역할을 하도록 지시하여 모든 I/O 작업을 처리합니다. 일관성 그룹에 미러링된 볼륨만 제공됩니다. SVM의 다른 두 권과 관련된 모든 작업은 재해 사건의 영향을 받습니다.

대칭적인 액티브/액티브

SnapMirror Active Sync는 비대칭 솔루션 및 대칭 솔루션을 제공합니다.

_비대칭 구성_에서 기본 스토리지 사본은 활성-최적화 경로를 노출하고 클라이언트 I/O를 능동적으로 처리합니다. 보조 사이트는 I/O에 원격 경로를 사용합니다. 보조 사이트의 스토리지 경로는 활성-비최적화로 간주됩니다. 쓰기 LUN에 대한 액세스는 보조 사이트에서 프록시됩니다. NVMe 프로토콜은 비대칭 구성에서 지원되지 않습니다.

_대칭 액티브/액티브 구성_에서는 액티브 최적화 경로가 양쪽 사이트에 모두 노출되고, 호스트별로 구성 가능하며, 구성 가능합니다. 즉, 양쪽 호스트가 액티브 I/O를 위해 로컬 스토리지에 액세스할 수 있습니다. ONTAP 9.16.1부터 대칭 액티브/액티브 구성은 최대 4개의 노드로 구성된 클러스터에서 지원됩니다. ONTAP 9.17.1부터 대칭 액티브/액티브 구성은 2노드 클러스터에서 NVMe 프로토콜을 지원합니다.



대칭 액티브/액티브는 VMware Metro Storage Cluster, Oracle RAC, SQL을 사용한 Windows 페일오버 클러스터링을 비롯한 클러스터 애플리케이션을 대상으로 합니다.

ONTAP SnapMirror Active Sync 사용 사례

전 세계적으로 연결된 비즈니스 환경에서는 사이버 공격, 정전, 자연 재해 등의 중단이 발생하더라도 데이터 손실 없이 비즈니스에 중요한 애플리케이션 데이터를 신속하게 복구해야 한다는 요구가 있습니다. 이러한 요구는 금융 분야나 GDPR(일반 데이터 보호 규정)과 같은 규제 의무를 준수하는 분야에서 더욱 높아집니다.

SnapMirror 액티브 동기화는 다음과 같은 사용 사례를 제공합니다.

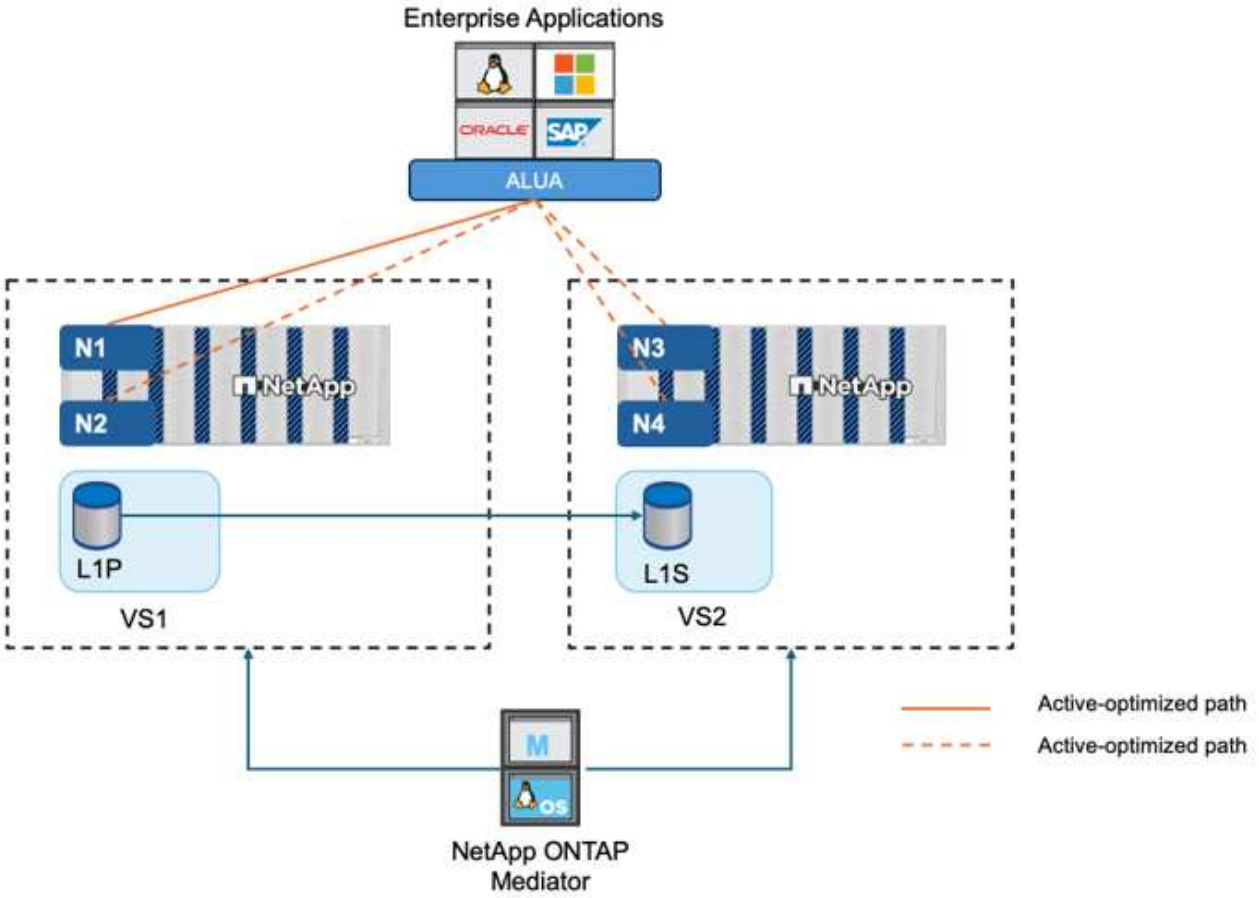
제로 복구 시간 목표**(RTO)**를 위한 애플리케이션 구축

SnapMirror Active Sync 배포에는 기본 클러스터와 보조 클러스터가 있습니다. 기본 클러스터의 LUN `L1P`) 거울이

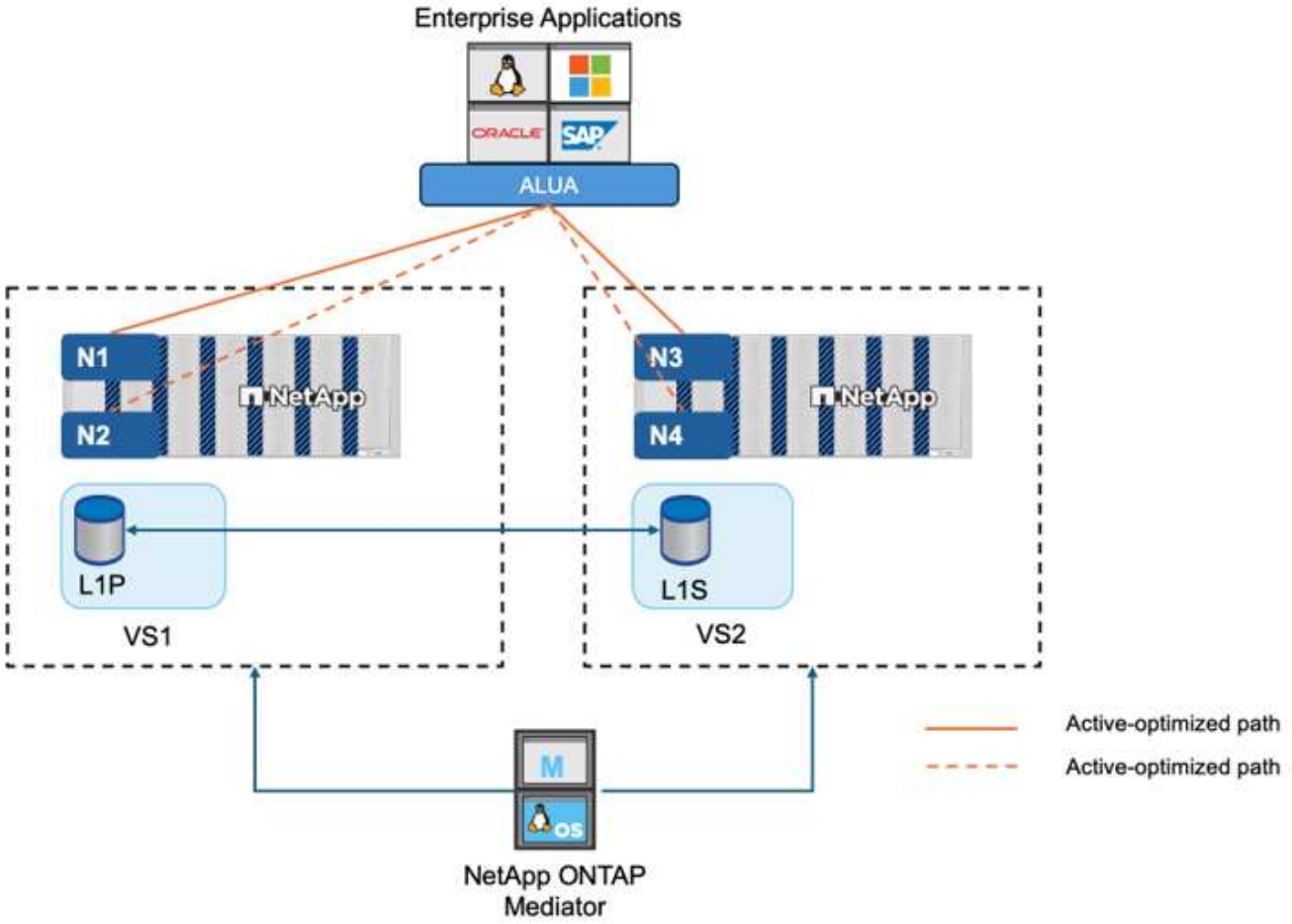
있어요 `L1S`) 보조 LUN에 있습니다. 두 LUN은 동일한 직렬 ID를 공유하며 호스트에 읽기-쓰기 LUN으로 보고됩니다. 그러나 비대칭 구성에서는 읽기 및 쓰기 작업이 기본 LUN으로만 처리됩니다. `L1P` . 미러에 대한 모든 쓰기 `L1S` 대리인을 통해 제공됩니다.

제로 **RTO** 또는 투명한 애플리케이션 페일오버**(TAF)**를 위한 애플리케이션 구축

TAF는 호스트 MPIO 소프트웨어 기반 경로 페일오버를 통해 스토리지에 대한 무중단 액세스를 구현합니다. 두 LUN 복사본(예: 기본 볼륨(L1P) 및 미러 볼륨(L1S))은 동일한 ID(일련 번호)를 가지며 호스트에 읽기/쓰기 가능으로 보고됩니다. 그러나 비대칭 구성에서는 읽기 및 쓰기가 기본 볼륨에서만 처리됩니다. 미러 볼륨에 대한 I/O는 기본 볼륨으로 프록시됩니다. 호스트에서 L1에 대한 기본 경로는 비대칭 논리 단위 액세스(ALUA) 액세스 상태가 활성 최적화(A/O)인 경우 VS1:N1입니다. ONTAP Mediator는 구축 과정의 일부로 필요하며, 주로 기본 볼륨의 스토리지 중단 시 페일오버(계획된 또는 계획되지 않은)를 수행합니다.



TAF는 자동 장애 조치(Automated Failover)와 자동 장애 조치 이중화(Automated Failover Duplex)의 두 가지 모드로 작동합니다. 자동 장애 조치를 사용하면 읽기 및 쓰기 작업이 기본 볼륨에서만 처리되므로, 자체적으로 쓰기 작업을 처리할 수 없는 미러 복사본에 대한 IO는 기본 복사본으로 프록시됩니다. 자동 장애 조치 이중화를 사용하면 기본 복사본과 보조 복사본 모두 IO를 처리할 수 있으므로 프록시가 필요하지 않습니다.



ONTAP 9.17.1에서 호스트 액세스에 NVMe를 사용하는 경우 AutomatedFailoverDuplex 정책만 지원됩니다.

SnapMirror Active Sync는 애플리케이션 호스트 다중 경로 소프트웨어에서 스토리지 어레이와의 애플리케이션 호스트 통신에 필요한 우선 순위 및 액세스 가용성을 통해 알려진 경로를 사용할 수 있도록 하는 메커니즘인 ALUA를 사용합니다. ALUA는 LUN을 소유한 컨트롤러에 대한 활성 최적화 경로를 최적화되지 않은 활성 경로로 표시하며, 기본 경로에 장애가 발생할 경우에만 사용됩니다.

NVMe 프로토콜을 사용하는 SnapMirror 액티브 동기화는 ANA(비대칭 네임스페이스 액세스)를 사용하여 애플리케이션 호스트가 보호되는 NVMe 네임스페이스에 대한 최적화된 경로와 최적화되지 않은 경로를 검색할 수 있도록 합니다. ONTAP NVMe 타겟은 적절한 경로 상태를 게시하여 애플리케이션 호스트가 보호되는 NVMe 네임스페이스에 대한 최적의 경로를 사용할 수 있도록 합니다.

클러스터된 애플리케이션

VMware Metro Storage Cluster, Oracle RAC, SQL을 사용한 Windows Failover Clustering을 포함한 클러스터형 애플리케이션은 성능 오버헤드 없이 VM을 다른 사이트로 장애 조치할 수 있도록 동시 액세스가 필요합니다. SnapMirror 액티브 싱크 대칭 액티브/액티브는 클러스터형 애플리케이션의 요구 사항을 충족하기 위해 양방향 복제를 통해 로컬로 IO를 제공합니다. ONTAP 9.16.1부터 4노드 클러스터 구성에서 대칭적 액티브/액티브가 지원되며, ONTAP 9.15.1의 2노드 클러스터 제한에서 확장되었습니다.

재해 시나리오

지리적으로 분산된 사이트 간에 애플리케이션을 위해 여러 볼륨을 동기식으로 복제합니다. 운영 중단 시 보조 복사본으로 자동으로 페일오버하여 계층 1 애플리케이션에 비즈니스 연속성을 제공할 수 있습니다. 기본 클러스터를 호스팅하는 사이트에 재해가 발생하면 호스트 다중 경로 소프트웨어는 클러스터를 통과하는 모든 경로를 중지로 표시하고 보조 클러스터의 경로를 사용합니다. 그 결과 ONTAP 중재자가 미러 복사본에 대해 무중단 페일오버를

수행합니다.

확장된 애플리케이션 지원

SnapMirror 액티브 동기화는 사용하기 쉬운 애플리케이션 수준의 세분성과 자동 장애 조치를 통해 유연성을 제공합니다. SnapMirror Active Sync는 IP 네트워크를 통한 검증된 SnapMirror 동기 복제를 사용하여 LAN이나 WAN을 통해 고속으로 데이터를 복제하여 Oracle, Microsoft SQL Server 등과 같은 비즈니스에 중요한 애플리케이션에 대한 높은 데이터 가용성과 빠른 데이터 복제를 가상 및 물리적 환경 모두에서 달성합니다.

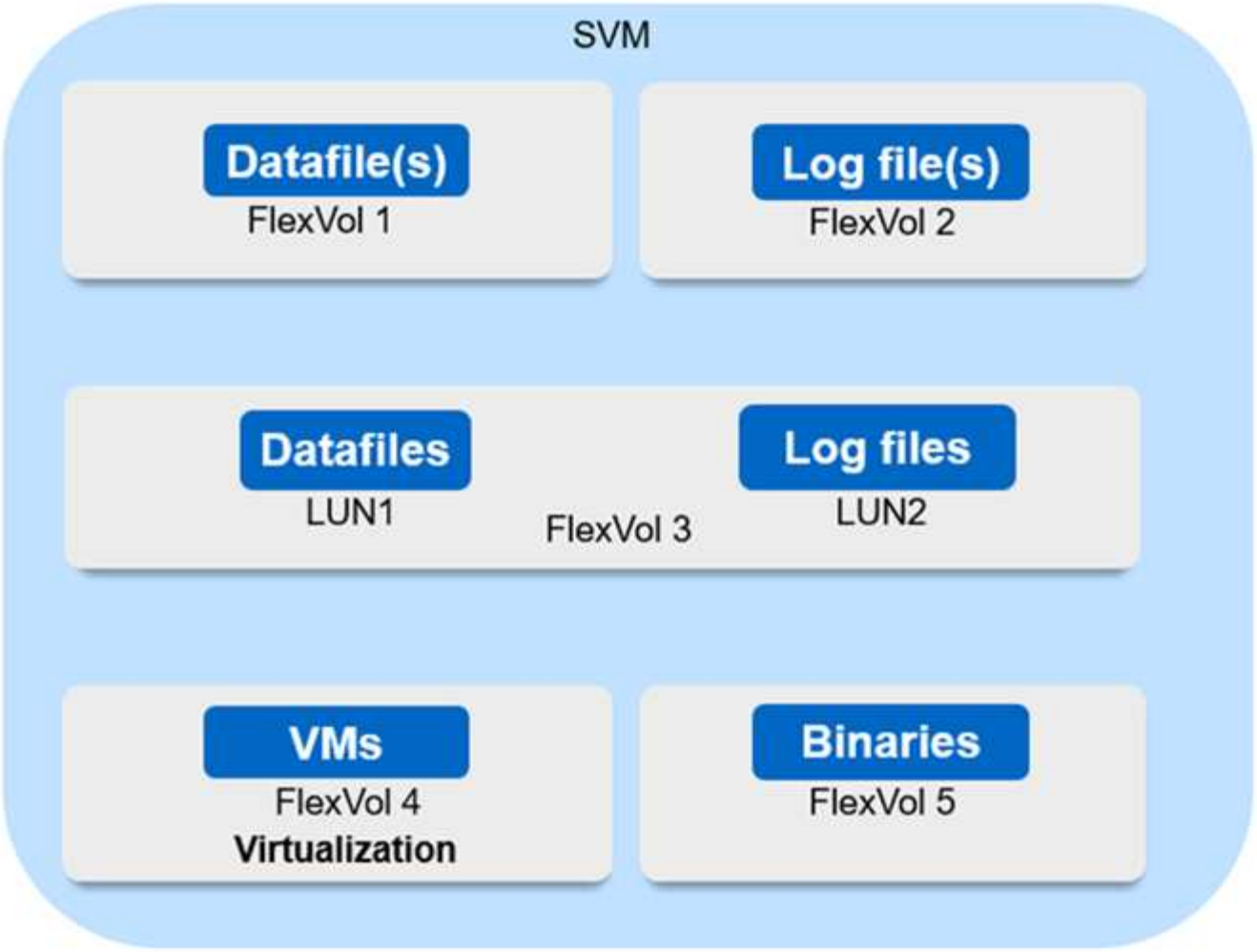
SnapMirror 액티브 동기화를 사용하면 사이트 전체에 장애가 발생하더라도 2차 복사본에 TAF를 적용하여 미션 크리티컬 비즈니스 서비스를 계속 운영할 수 있습니다. 이 장애 조치를 트리거하는 데 수동 개입이나 추가 스크립팅이 필요하지 않습니다.

ONTAP SnapMirror Active Sync를 위한 배포 전략 및 모범 사례

비즈니스 연속성을 위해 보호해야 할 워크로드를 명확하게 식별하여 데이터 보호 전략을 수립하는 것이 중요합니다. 데이터 보호 전략에서 가장 중요한 단계는 기업 애플리케이션 데이터 레이아웃을 명확히 하는 것입니다. 이를 통해 볼륨을 어떻게 분배하고 비즈니스 연속성을 보호할지 결정할 수 있습니다. 장애 조치는 애플리케이션별로 일관성 그룹 수준에서 발생하므로 일관성 그룹에 필요한 데이터 볼륨을 추가해야 합니다.

SVM 구성

다이어그램은 SnapMirror 액티브 동기화에 대한 권장 스토리지 VM(SVM) 구성을 캡처합니다.



- 데이터 볼륨의 경우:
  - 랜덤 읽기 워크로드는 순차적 쓰기에서 격리되므로, 데이터베이스 크기에 따라 데이터 및 로그 파일은 일반적으로 별도의 볼륨에 배치됩니다.
    - 대규모 중요 데이터베이스의 경우 단일 데이터 파일은 FlexVol 1에 있고 해당 로그 파일은 FlexVol 2에 있습니다.
    - 더 나은 통합을 위해 중요도가 낮은 크기의 중요하지 않은 데이터베이스는 모든 데이터 파일이 FlexVol 1에 있고 해당 로그 파일이 FlexVol 2에 있도록 그룹화됩니다. 그러나 이 그룹화를 통해 응용 프로그램 수준의 세분화가 손실됩니다.
  - 또 다른 변형은 모든 파일을 동일한 FlexVol 3 내에 두고, 데이터 파일은 lun1에, 로그 파일은 LUN 2에 저장하는 것입니다.
- 환경이 가상화되어 있으면 여러 엔터프라이즈 애플리케이션에 대한 모든 VM이 데이터 저장소에 공유됩니다. 일반적으로 VM 및 애플리케이션 바이너리는 SnapMirror를 사용하여 비동기식으로 복제됩니다.

계획

ONTAP SnapMirror Active Sync를 위한 필수 구성 요소

SnapMirror 활성 동기화 배포를 계획할 때 다양한 하드웨어, 소프트웨어 및 시스템 구성 요구 사항을 충족하는지 확인하십시오.

하드웨어

다음 표에서는 지원되는 NetApp 클러스터 구성을 간략하게 보여 줍니다.

클러스터 유형입니다	지원 모델	지원되는 기능	지원되는 최대 클러스터 노드
AFF	A-시리즈, C-시리즈	자동 페일오버 이중(대칭형 Active/Active), 자동 페일오버(비대칭형 Active/Active)	• 2 (ONTAP 9.9.1 이상) • 4 (대칭 활성/활성 구성이 있는 ONTAP 9.16.1)
ASA	A-시리즈, C-시리즈	자동 페일오버 이중(대칭형 Active/Active), 자동 페일오버(비대칭형 Active/Active)	• 2 (ONTAP 9.9.1 이상 • 4 (대칭 활성/활성 구성이 있는 ONTAP 9.16.1)
ASA r2	모두	자동 장애 조치 이중화(대칭형 액티브/액티브)	• 2 (ONTAP 9.17.1 또는 이전 버전) • 4 (ONTAP 9.18.1 이상)

아래 표에는 클러스터 유형 간 복제 기능이 간략하게 정리되어 있습니다.

클러스터 유형 1	클러스터 유형 2	복제가 지원됩니까?
AFF A-시리즈	AFF C-Series로 문의하십시오	예
ASA r2 A-시리즈	ASA r2 C-시리즈	예
AFF	ASA	아니요
ASA	ASA r2	아니요
ASA r2	ASA r2	예

소프트웨어

- ONTAP 9.9.1 이상
- ONTAP 중재자 1.2 이상
- 다음 중 하나를 실행하는 ONTAP Mediator용 Linux 서버 또는 가상 머신:

ONTAP 중재자 버전	지원되는 Linux 버전

1.11	• Red Hat Enterprise Linux ◦ 호환 가능: 9.5 [1] ◦ 권장: 10.1, 10.0, 9.7, 9.6, 9.4, 8.10 • Rocky Linux 10.1, 9.7 및 8.10 • Oracle Linux 10.0 및 9.6
1.10	• Red Hat Enterprise Linux ◦ 호환 가능: 9.5 [1] ◦ 권장: 10.0, 9.6, 9.4 및 8.10 • Rocky Linux 10.0, 9.6 및 8.10
1.9.1	• Red Hat Enterprise Linux ◦ 호환 가능 버전: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.5, 9.4, 9.2, 9.0, 8.10, 8.8 • Rocky Linux 9.5 및 8.10
1.9	• Red Hat Enterprise Linux ◦ 호환 가능 버전: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.5, 9.4, 9.2, 9.0, 8.10, 8.8 • Rocky Linux 9.5 및 8.10
1.8	• Red Hat Enterprise Linux: ◦ 호환 가능: 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9, 8.8 • Rocky Linux 9.4 및 8.10
1.7	• Red Hat Enterprise Linux: ◦ 호환 가능: 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.3, 9.2, 9.1, 9.0, 8.9, 8.8 • Rocky Linux 9.3 및 8.9
1.6	• Red Hat Enterprise Linux: ◦ 호환 가능: 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.2, 9.1, 9.0 및 8.8 • Rocky Linux 9.2 및 8.8

1.5	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6
1.4	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6
1.3	• Red Hat Enterprise Linux: 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6
1.2	• Red Hat Enterprise Linux: 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6

1. 호환 가능이란 Red Hat이 더 이상 이러한 RHEL 버전을 지원하지 않지만 ONTAP Mediator는 여전히 해당 버전에 설치할 수 있음을 의미합니다.

라이센싱

다음 SnapMirror 라이선스는 ONTAP One 라이선스 제품군의 일부로 제공되며 두 클러스터 모두에 적용해야 합니다.

- SnapMirror 동기식
- SnapMirror를 참조하십시오

> 2019년 6월 이전에 ONTAP 스토리지 시스템을 구매한 경우 다음을 참조하세요. "ONTAP 마스터 라이선스 키" 필요한 SnapMirror 동기 라이센스를 받으세요.

- vSphere Metro Storage Cluster(vMSC)의 경우 VMware vSphere 라이선스가 필요합니다.

네트워킹 환경

- 클러스터 간 지연 RTT(Round Trip Time)는 10밀리초 미만이어야 합니다.
- ONTAP 9.14.1부터 "SCSI-3 영구 예약" SnapMirror 액티브 동기화에서 지원됩니다.

지원되는 프로토콜

SnapMirror Active Sync는 SAN 프로토콜을 지원합니다.

- FC 및 iSCSI 프로토콜은 ONTAP 9.9.1부터 지원됩니다.
- NVMe 프로토콜은 ONTAP 9.17.1부터 VMware 워크로드에서 지원됩니다.

  SnapMirror Active Sync는 NVMe 프로토콜을 사용하여 다음을 지원하지 않습니다.

  - 4노드 대칭 액티브/액티브 구성
  - 비대칭 활성/활성 구성
  - 일관성 그룹 크기의 변화

SnapMirror 액티브 싱크에서 NVMe 프로토콜을 사용할 경우 일관성 그룹을 중단 없이 확장하거나 축소할 수 없습니다. SnapMirror 액티브 싱크에서 NVMe 프로토콜을 사용할 경우 일관성 그룹 확장 및 축소 작업은 중단을 수반합니다.

- 동일한 일관성 그룹에서 LUN과 네임스페이스가 공존합니다.

IPspace

SnapMirror Active Sync에서는 클러스터 피어 관계를 위해 기본 IP 공간이 필요합니다. 사용자 정의 IP 공간은 지원되지 않습니다.

NTFS 보안 스타일

SnapMirror 액티브 동기화 볼륨에서는 NTFS 보안 스타일이 * 지원되지 않음 *.

ONTAP 중재자

- ONTAP Mediator는 외부에서 프로비저닝되어야 하며 투명한 애플리케이션 장애 조치를 위해 ONTAP에 연결되어야 합니다.
- 완전한 기능을 갖추고 계획되지 않은 자동 장애 조치를 활성화하려면 외부 ONTAP Mediator를 ONTAP 클러스터로 프로비저닝하고 구성해야 합니다.
- ONTAP Mediator는 두 개의 ONTAP 클러스터와 별도로 세 번째 장애 도메인에 설치해야 합니다.
- ONTAP Mediator를 설치할 때 자체 서명된 인증서를 주요 신뢰할 수 있는 CA에서 서명한 유효한 인증서로 바꿔야 합니다.
- ONTAP Mediator에 대한 자세한 내용은 다음을 참조하세요. "ONTAP Mediator 설치 준비" .

기타 필수 구성 요소

- ONTAP 9.15.1 이전 릴리스에서는 SnapMirror 활성 동기화 관계가 읽기-쓰기 대상 볼륨(비대칭 활성-활성의 DP에서 읽기-쓰기로 변환된 볼륨)에서 지원되지 않습니다. 읽기-쓰기 볼륨을 사용하려면 먼저 볼륨 수준 SnapMirror 관계(비동기 또는 동기)를 생성한 다음 해당 관계를 삭제하여 해당 볼륨을 DP 볼륨으로 변환해야 합니다. 자세한 내용은 다음을 참조하십시오. "기존 SnapMirror 관계를 SnapMirror 활성 동기화로 변환" .
- SnapMirror Active Sync를 사용하는 스토리지 VM은 클라이언트 컴퓨터로 Active Directory에 가입할 수 없습니다.

추가 정보

- "Hardware Universe"
- "ONTAP 중재자 개요"

ONTAP SnapMirror Active Sync 상호 운용성

SnapMirror Active Sync는 다양한 운영 체제, 애플리케이션 호스트 및 ONTAP의 기타 기능과 호환됩니다.

여기에서 다루지 않은 자세한 지원 가능성 및 상호 운용성 정보는 상호 운용성 매트릭스 툴을 ("IMT"참조하십시오.

애플리케이션 호스트

SnapMirror Active Sync는 Hyper-V, ESXi, Red Hat Enterprise Linux(RHEL), Windows Server와 같은 운영 체제, vSphere Metro Storage Cluster(vMSC)와 같은 클러스터링 솔루션을 포함한 하이퍼바이저를 지원하며 ONTAP 9.14.1부터는 Windows Server Failover Cluster도 지원합니다.

운영 체제

SnapMirror Active Sync는 다음과 같은 다양한 운영 체제에서 지원됩니다.

- PVR을 통한 AIX(ONTAP 9.11.1부터)
- HP-UX(ONTAP 9.10.1 시작)
- Solaris 11.4(ONTAP 9.10.1 시작)

AIX

ONTAP 9.11.1부터 AIX는 다음 규정을 이해하는 데 동의하는 표준 엔지니어링 FPVR(Feature Policy Variance Request)을 통해 SnapMirror 액티브 동기화를 지원합니다.

- SnapMirror 액티브 동기화는 제로 RPO 데이터 보호를 제공할 수 있지만 AIX의 페일오버 프로세스에서는 경로 변경을 인식하기 위한 추가 단계가 필요합니다. 루트 볼륨 그룹에 속하지 않는 LUN은 가 될 때까지 I/O 일시 중지를 경험합니다 `cfgmgr` 명령이 실행됩니다. 이를 자동화할 수 있으며, 대부분의 애플리케이션은 추가 운영 중단 없이 운영을 재개합니다.
- 루트 볼륨 그룹에 포함된 LUN은 일반적으로 SnapMirror 활성 동기화를 통해 보호되지 않습니다. 을(를) 실행할 수 없습니다 `cfgmgr` 페일오버 후 명령입니다. 즉, SAN 경로의 변경 사항을 인식하려면 재부팅이 필요합니다. 루트 볼륨 그룹에 대해 제로 RPO 데이터 보호를 달성할 수 있지만, 페일오버는 중단을 야기합니다.

AIX와 SnapMirror active sync에 대한 자세한 내용은 NetApp 세일즈 팀에 문의하십시오.

HP-UX를 참조하십시오

ONTAP 9.10.1부터 HP-UX용 SnapMirror 액티브 동기화가 지원됩니다.

HP-UX를 사용한 자동 비계획 페일오버

기본 클러스터와 보조 클러스터 간의 연결이 끊어지고 기본 클러스터와 중재자 간의 연결도 끊어지면 이중 이벤트 실패로 인해 격리된 마스터 클러스터에서 자동 계획되지 않은 장애 조치(AUFO) 이벤트가 발생할 수 있습니다. 이는 다른 AUFO 행사와 달리 드문 행사로 간주됩니다.

- 이 시나리오에서는 HP-UX 호스트에서 입출력이 재개되는 데 120초 이상 걸릴 수 있습니다. 실행 중인 애플리케이션에 따라 I/O 중단 또는 오류 메시지가 발생할 수 없습니다.
- 문제를 해결하려면 중단 허용 시간이 120초 미만인 HP-UX 호스트에서 애플리케이션을 다시 시작해야 합니다.

Solaris

ONTAP 9.10.1부터 SnapMirror 액티브 동기화는 Solaris 11.4를 지원합니다.

SnapMirror 활성 동기화 환경에서 계획되지 않은 사이트 장애 조치(failover) 전환이 발생할 때 Solaris 클라이언트 애플리케이션이 중단되지 않도록 하려면 기본 Solaris OS 설정을 수정합니다. 권장 설정으로 Solaris를 구성하려면 다음을 참조하세요."NetApp 지식 기반: SnapMirror Active Sync에서 Solaris 호스트 지원 권장 설정" .

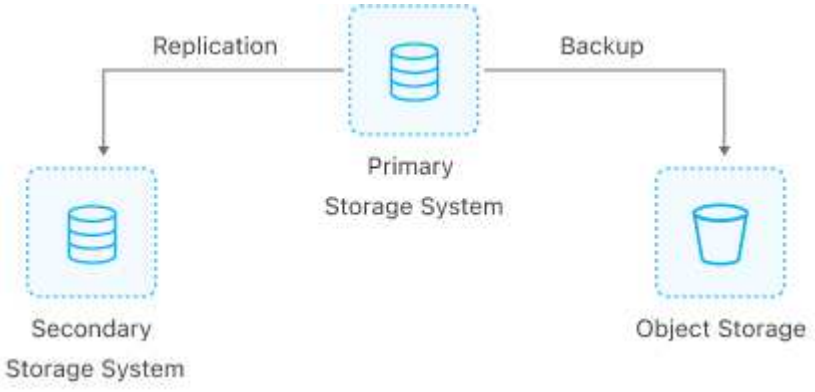
SnapMirror 액티브 동기화는 ONTAP의 구성 요소와 통합되어 데이터 보호 기능을 확장합니다.

FabricPool

SnapMirror 액티브 동기화는 없음, 스냅샷 또는 자동의 계층화 정책으로 FabricPool 애그리게이트에서 소스 및 타겟 볼륨을 지원합니다. SnapMirror 액티브 동기화는 All 의 계층화 정책을 사용하는 FabricPool 애그리게이트를 지원하지 않습니다.

팬아웃 구성

~ 안에팬아웃 구성 소스 볼륨을 SnapMirror 활성 동기화 대상 엔드포인트와 하나의 SnapMirror 비동기 관계에 미러링할 수 있습니다.



SnapMirror Active Sync는 팬아웃 구성 `MirrorAllSnapshots`ONTAP 9.11.1부터 정책 및 `MirrorAndVault` 정책을 지원합니다. 정책을 사용하는 SnapMirror 활성 동기화에서는 팬아웃 구성이 지원되지 `XDPDefault` 않습니다.

ONTAP 9.15.1부터 SnapMirror 액티브 동기화는 페일오버 이벤트 후 팬아웃 구간의 자동 재구성을 지원합니다. 운영 사이트에서 보조 사이트로 페일오버가 성공하면 보조 사이트를 소스로 처리하도록 3차 사이트가 자동으로 다시 구성됩니다. 비동기 팬아웃 구간은 정합성 보장 그룹 관계 또는 독립 볼륨 관계일 수 있습니다. 두 경우 모두 재구성을 수행할 수 있습니다. 재구성이 계획된 또는 계획되지 않은 페일오버에 의해 트리거됩니다. 운영 사이트로 페일백할 때도 재구성이 수행됩니다.

이전 릴리스의 ONTAP에서 팬아웃 구성을 관리하는 방법에 대한 자세한 내용은 을 참조하십시오 팬아웃 구성에서 보호를 재개합니다.

NDMP 복구입니다

ONTAP 9.13.1부터 SnapMirror 활성 동기화와 함께 을 사용할 수 NDMP를 사용하여 데이터를 복제하고 복구합니다있습니다. NDMP를 사용하면 데이터를 SnapMirror 활성 동기화 소스로 이동하여 보호를 일시 중지하지 않고 복원을 완료할 수 있습니다. 이 기능은 특히 팬아웃 구성에 유용합니다.

SnapCenter

SnapMirror 활성 동기화는 부터 SnapCenter에서 "SnapCenter 5.0 을 참조하십시오"지원됩니다. SnapCenter를 사용하면 애플리케이션 및 가상 머신을 보호하고 복구하는 데 사용할 수 있는 스냅샷을 생성할 수 있으므로, 애플리케이션 레벨 세분화로 상시 사용 가능한 스토리지 솔루션을 사용할 수 있습니다.

SnapRestore

SnapMirror 활성 동기화는 부분 및 단일 파일 SnapRestore를 지원합니다.

단일 파일 SnapRestore

ONTAP 9.11.1부터 단일 파일 SnapRestoreSnapMirror 활성 동기화 볼륨에 대해 이 지원됩니다. SnapMirror 활성 동기화 소스에서 대상으로 복제된 스냅샷에서 단일 파일을 복구할 수 있습니다. 볼륨에는 하나 이상의 LUN이 포함될 수 있으므로 이 기능을 사용하면 중단이 적은 복원 작업을 구현하고 다른 LUN을 중단하지 않고 하나의 LUN을 세부적으로 복원할 수 있습니다. Single File SnapRestore에는 데이터 이동 없는 것과 원본 이동 없는 두 가지 옵션이 있습니다.

부분 파일 SnapRestore

ONTAP 9.12.1부터 "부분 LUN 복원"SnapMirror 활성 동기화 볼륨에 대해 이 지원됩니다. SnapMirror 활성 동기화 소스(볼륨)와 대상(스냅샷) 볼륨 간에 복제된 응용 프로그램 생성 스냅샷에서 데이터를 복원할 수 있습니다. 여러 데이터베이스를 동일한 LUN에 저장하는 호스트에서 데이터베이스를 복구해야 하는 경우 부분 LUN 또는 파일 복구가 필요할 수 있습니다. 이 기능을 사용하려면 데이터 및 바이트 수의 시작 바이트 오프셋을 알고 있어야 합니다.

대용량 LUN 및 대용량 볼륨

대용량 LUN 및 대용량 볼륨(100TB 이상)에 대한 지원은 사용 중인 ONTAP 버전과 플랫폼에 따라 다릅니다.

ONTAP 9.12.1P2 이상

- ONTAP 9.12.1 P2 이상의 경우 SnapMirror Active Sync는 ASA 및 AFF(A 시리즈 및 C 시리즈)에서 100TB보다 큰 대용량 LUN과 볼륨을 지원합니다. 운영 클러스터와 2차 클러스터의 유형은 ASA 또는 AFF 중 하나여야 합니다. AFF A-Series에서 AFF C-Series로, 또는 그 반대로 복제가 지원됩니다.

ONTAP 릴리즈 9.12.1P2 이상의 경우 운영 클러스터와 보조 클러스터가 모두 ASA(All-Flash SAN Array) 또는 AFF(All-Flash Array)인지, 둘 다 ONTAP 9.12.1 P2 이상이 설치되어 있는지 확인해야 합니다. 보조 클러스터가 ONTAP 9.12.1P2 이전 버전을 실행 중이거나 스토리지 유형이 운영 클러스터와 동일하지 않은 경우 운영 볼륨이 100TB 이상 증가할 경우 동기식 관계가 동기화되지 않을 수 있습니다.

ONTAP 9.9.1 - 9.12.1P1

- ONTAP 9.9.1 ~ 9.12.1 P1(포함) 사이의 ONTAP 릴리즈의 경우 100TB를 초과하는 대형 LUN과 대용량 볼륨은 All-Flash SAN 어레이에서만 지원됩니다. AFF A-Series에서 AFF C-Series로, 또는 그 반대로 복제가 지원됩니다.

ONTAP 9.9.9.1과 9.12.1 P2 사이의 ONTAP 릴리즈의 경우 기본 클러스터와 보조 클러스터가 All-Flash SAN 어레이여야 하며 둘 다 ONTAP 9.9.1 이상이 설치되어 있어야 합니다. 2차 클러스터에서 ONTAP 9.9.1 이전 버전을 실행 중이거나 All-Flash SAN 어레이가 아닌 경우 운영 볼륨이 100TB보다 커지면 동기식 관계가 동기화되지 않을 수 있습니다.

추가 정보

- "SnapMirror 액티브 동기화에 대해 AIX 호스트를 구성하는 방법"

ONTAP SnapMirror Active Sync에 대한 개체 제한

SnapMirror 액티브 동기화를 사용하기 위한 준비를 할 때는 다음 개체 제한에 유의하십시오.

클러스터의 일관성 그룹

SnapMirror 액티브 동기화가 있는 클러스터의 일관성 그룹 제한은 관계에 따라 계산되며 사용되는 ONTAP 버전에 따라 달라집니다. 제한은 플랫폼에 독립적입니다.

ONTAP 버전입니다	최대 관계 수
ONTAP 9.11.1 이상	50 *
ONTAP 9.10.1	20
ONTAP 9.9.1	5

* ONTAP 9.16.1부터 SnapMirror 액티브 동기화는 대칭 액티브/액티브 구성의 4노드 클러스터를 지원합니다. 4노드 클러스터에서는 100개의 일관성 그룹이 지원됩니다.

정합성 보장 그룹당 볼륨

SnapMirror 활성 동기화가 있는 일관성 그룹당 최대 볼륨 수는 플랫폼과는 별개입니다.

ONTAP 버전입니다	일관성 그룹 관계에서 지원되는 최대 볼륨 수입니다
ONTAP 9.15.1 이상	80
ONTAP 9.10.1 - 9.14.1	16
ONTAP 9.9.1	12

볼륨

SnapMirror 활성 동기화의 볼륨 제한은 관계 수가 아닌 끝점 수를 기준으로 계산됩니다. 12개의 볼륨이 있는 일관성 그룹은 운영 클러스터와 보조 클러스터 모두에서 12개의 엔드포인트를 지원합니다. SnapMirror 활성 동기화와 SnapMirror 동기식 관계는 모두 총 엔드포인트 수에 기여합니다.

이러한 제한은 FAS, AFF 및 ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 또는 ASA A20)을 사용하는 경우 다음을 참조하십시오. "ASA r2 설명서" .

플랫폼당 최대 엔드포인트는 다음 표에 나와 있습니다.

플랫폼	**SnapMirror** 활성 동기화에 대한 **HA**당 엔드포인트			**HA**당 전체 동기화 및 **SnapMirror** 활성 동기화 엔드포인트		
	ONTAP 9.11.1 이상	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.11.1 이상	ONTAP 9.10.1	ONTAP 9.9.1
AFF	400 *	200	60	400	200	80
ASA	400 *	200	60	400	200	80

* ONTAP 9.16.1부터 SnapMirror 액티브 동기화는 대칭 액티브/액티브 구성의 4노드 클러스터를 지원합니다. 4노드 클러스터의 총 제한은 800개입니다.

SAN 오브젝트 제한

SAN 오브젝트 제한사항은 다음 표에 나와 있습니다. 이 제한은 플랫폼에 관계없이 적용됩니다.

SnapMirror 활성 동기화 관계의 개체	카운트
볼륨당 LUN	• 256(ONTAP 9.9.1 - ONTAP 9.15.0) • 512(ONTAP 9.15.1 이상)
2 x 2 SnapMirror Active Sync 솔루션당 고유한 LUN, 네임스페이스 또는 스토리지 유닛 수	4,096개
4 x 4 SnapMirror 액티브 동기화 솔루션당 고유한 LUN, 네임스페이스 또는 스토리지 유닛 수(ONTAP 9.16.1부터 사용 가능)	6,144
SVM당 LIF(SnapMirror 활성 동기화 관계에 볼륨이 하나 이상 있는 경우)	256
노드당 클러스터 간 LIF	4
클러스터당 클러스터 간 LIF	8

NVMe 객체 제한

ONTAP 9.17.1부터 SnapMirror Active Sync는 NVMe 프로토콜을 지원합니다. NVMe 객체 제한은 다음 표에 포함되어 있습니다.

SnapMirror 활성 동기화 관계의 최대 개체 수	카운트
노드당 네임스페이스 맵 수	4K
클러스터 크기	2개의 노드
HA 쌍당 일관성 그룹 수	50
단일 NVMe SnapMirror 활성 동기화 일관성 그룹의 볼륨 수	80
HA 쌍의 볼륨 수	400
일관성 그룹당 NVMe 서브시스템	16
일관성 그룹당 네임스페이스 맵	256

관련 정보

- "Hardware Universe"
- "정합성 보장 그룹 제한"

구성

SnapMirror 활성 동기화를 위한 **ONTAP** 클러스터 구성

SnapMirror 액티브 싱크는 장애 조치 발생 시 데이터를 보호하기 위해 피어링된 클러스터를 사용합니다. SnapMirror 액티브 싱크를 위해 ONTAP Mediator 또는 ONTAP Cloud Mediator를 구성하기 전에 먼저 클러스터가 올바르게 구성되었는지 확인해야 합니다.

시작하기 전에

ONTAP Mediator 또는 ONTAP Cloud Mediator를 구성하기 전에 다음 사항을 확인해야 합니다.

1. 클러스터 간에는 클러스터 피어링 관계가 존재합니다.

   > 클러스터 피어 관계를 위한 SnapMirror 액티브 동기화에 기본 IPspace가 필요합니다. 사용자 지정 IPspace는 지원되지 않습니다.

   "클러스터 피어 관계 생성"

2. SVM은 각 클러스터에 생성됩니다.

   "SVM 생성"

3. 각 클러스터의 SVM 사이에는 피어 관계가 존재합니다.

   "SVM 피어링 관계 생성"

4. 볼륨은 LUN에 대해 존재합니다.

   "볼륨을 생성하는 중입니다"

5. 두 클러스터의 각 노드에 최소한 하나의 SAN LIF(해당되는 경우 FC 또는 iSCSI)가 생성됩니다.

   "클러스터 SAN 환경에서 LIF에 대한 고려 사항"

   "LIF 생성"

6. 필요한 LUN이 생성되어 igroup에 매핑됩니다. igroup은 LUN을 애플리케이션 호스트의 개시자에 매핑하는 데 사용됩니다.

   "LUN을 생성하고 igroup을 매핑합니다"

7. 새로운 LUN을 발견하기 위해 애플리케이션 호스트를 다시 검사합니다.

SnapMirror Active Sync를 위한 **ONTAP Mediator** 구성

SnapMirror 액티브 동기화는 장애 조치 시나리오 발생 시 피어링된 클러스터를 사용하여 데이터를 보호합니다. ONTAP Mediator는 각 클러스터의 상태를 모니터링하여 비즈니스 연속성을 보장하는 핵심 리소스입니다. SnapMirror 액티브 동기화를 구성하려면 먼저 ONTAP Mediator를 설치하고 기본 및 보조 클러스터가 올바르게 구성되었는지 확인해야 합니다.

ONTAP Mediator를 설치하고 클러스터를 구성한 후, 자체 서명 인증서를 사용하여 SnapMirror Active Sync용 ONTAP Mediator 초기화 . 그런 다음 해야 SnapMirror 활성 동기화에 대한 일관성 그룹을 생성, 초기화 및 매핑합니다합니다.

ONTAP 중재자

ONTAP Mediator는 SnapMirror 활성 동기화 관계에서 ONTAP 클러스터가 사용하는 고가용성(HA) 메타데이터에 대한 지속적이고 펜싱된 저장소를 제공합니다. 또한 ONTAP Mediator는 쿼럼 확인을 지원하는 동기식 노드 상태 쿼리 기능을 제공하고 컨트롤러 활성화 감지를 위한 Ping 프록시 역할을 합니다.

각 클러스터 피어 관계는 단일 ONTAP 중재자 인스턴스와만 연결할 수 있습니다. HA 중재자 인스턴스는 지원되지 않습니다. 클러스터가 다른 클러스터와 여러 피어 관계에 있는 경우 다음과 같은 ONTAP 중재자 옵션을 사용할 수

있습니다.

- 각 관계에 SnapMirror 활성 동기화가 구성되어 있는 경우 각 클러스터 피어 관계마다 고유한 ONTAP 중재자 인스턴스가 있을 수 있습니다.
- 클러스터는 모든 피어 관계에 대해 동일한 ONTAP 중재자 인스턴스를 사용할 수 있습니다.

예를 들어 클러스터 B가 클러스터 A, 클러스터 C 및 클러스터 D와 피어 관계에 있는 경우 각 관계에 SnapMirror Active Sync가 구성되어 있을 때 세 클러스터 피어 관계 모두 고유한 연결된 ONTAP 중재자 인스턴스를 가질 수 있습니다. 또는, 클러스터 B는 3개의 피어 관계 모두에 동일한 ONTAP 중재자 인스턴스를 사용할 수 있습니다. 이 시나리오에서는 클러스터에 대해 ONTAP mediator의 동일한 인스턴스가 세 번 나열되어 있습니다.

ONTAP 9.17.1부터 다음을 구성할 수 있습니다. "ONTAP 클라우드 중재자" SnapMirror Active Sync 구성에서 클러스터의 상태를 모니터링하려면 두 개의 Mediator를 동시에 사용할 수 없습니다.

ONTAP 9.17.1과 함께 SnapMirror Active Sync 및 ONTAP Mediator 또는 ONTAP Cloud Mediator를 사용하는 경우 다음에서 *알려진 문제 및 제한 사항*을 검토해야 합니다."ONTAP 릴리즈 노트" 이러한 구성에 대한 중요한 정보는 다음을 참조하세요.

ONTAP 중재자 전제 조건

- ONTAP Mediator에는 자체적인 필수 구성 요소가 포함되어 있습니다. ONTAP Mediator를 설치하기 전에 이러한 필수 구성 요소를 충족해야 합니다.

  자세한 내용은 다음을 참조하세요. "ONTAP Mediator 서비스 설치를 준비하세요" .

- 기본적으로 ONTAP Mediator는 TCP 포트 31784를 통해 서비스를 제공합니다. ONTAP 클러스터와 ONTAP Mediator 사이에서 포트 31784가 열려 있고 사용 가능한지 확인해야 합니다.

ONTAP Mediator를 설치하고 클러스터 구성을 확인하세요**.**

ONTAP Mediator를 설치하고 클러스터 구성을 확인하려면 다음 단계를 각각 수행하세요. 각 단계에 대해 특정 구성이 수행되었는지 확인해야 합니다. 각 단계에는 따라야 할 특정 절차에 대한 링크가 포함되어 있습니다.

단계

1. 소스 및 대상 클러스터가 올바르게 구성되었는지 확인하기 전에 ONTAP Mediator를 설치하세요.

   ONTAP Mediator 설치 또는 업그레이드 준비

2. 클러스터 피어링 관계가 클러스터 간에 존재하는지 확인합니다.

   클러스터 피어 관계를 위한 SnapMirror 액티브 동기화에 기본 IPspace가 필요합니다. 사용자 지정 IPspace는 지원되지 않습니다.

   "SnapMirror 활성 동기화를 위한 ONTAP 클러스터 구성"

자체 서명 인증서를 사용하여 **SnapMirror Active Sync**용 **ONTAP Mediator** 초기화

ONTAP Mediator를 설치하고 클러스터 구성을 확인한 후, 클러스터 모니터링을 위해 ONTAP Mediator를 초기화해야 합니다. System Manager 또는 ONTAP CLI를 사용하여 ONTAP Mediator를 초기화할 수 있습니다.

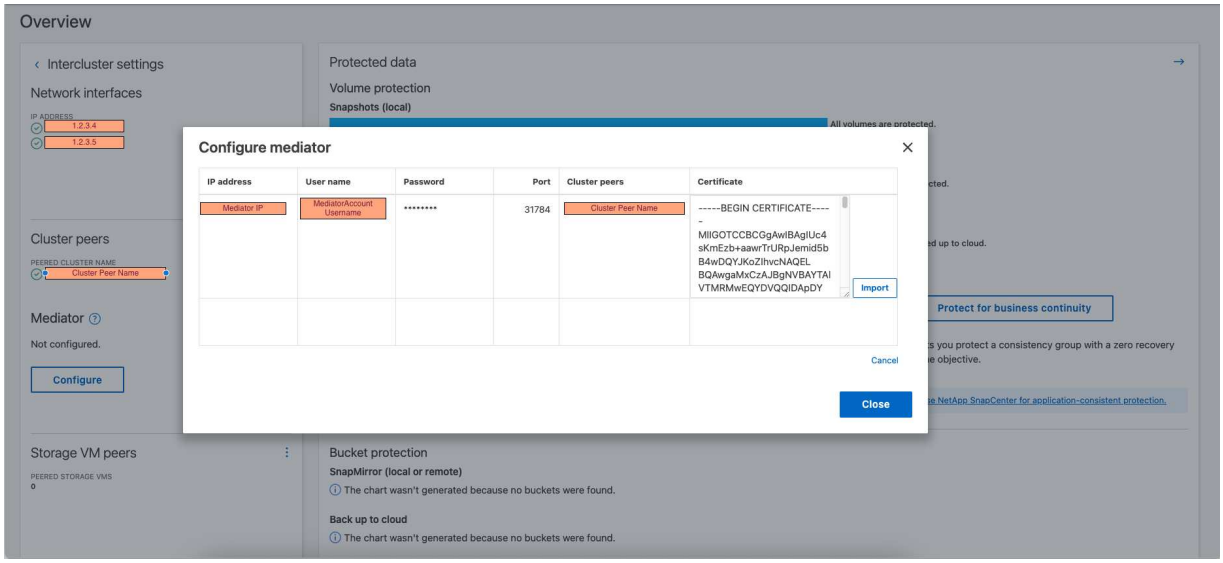
System Manager를 사용하면 ONTAP Mediator를 자동 장애 조치로 구성할 수 있습니다. 자체 서명된 SSL 및 CA를 타사 인증 SSL 인증서 및 CA로 대체할 수도 있습니다(아직 수행하지 않은 경우).

ONTAP 9.14.1부터 9.8까지 SnapMirror 액티브 동기화는 SnapMirror 비즈니스 연속성(SM-BC)이라고 합니다.

ONTAP 중재자 **1.9** 이상

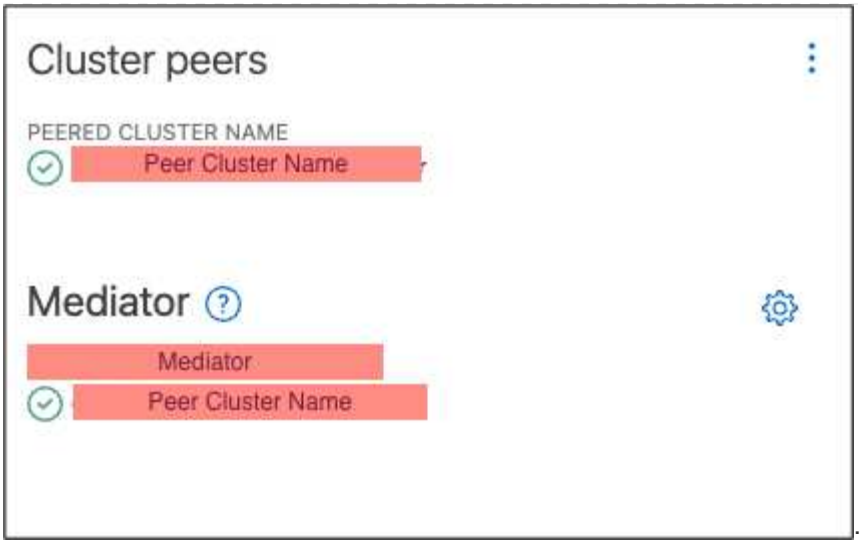
1. 보호 > 개요 > 중재자 > 구성 * 으로 이동합니다.
2. *추가*를 선택하고 다음 ONTAP Mediator 정보를 입력합니다.
   - IPv4 주소입니다
   - 사용자 이름
   - 암호
   - 인증서
3. 다음과 같은 두 가지 방법으로 인증서 입력을 제공할 수 있습니다.
   - * option (a) *: * Import * 를 선택하여 `intermediate.crt` 파일을 탐색하고 가져옵니다.
   - * option (b) *: 파일의 내용을 `intermediate.crt` 복사하여 * Certificate * 필드에 붙여 넣습니다.

   모든 세부 정보가 올바르게 입력되면 제공된 인증서가 모든 피어 클러스터에 설치됩니다.



인증서 추가가 완료되면 ONTAP Mediator가 ONTAP 클러스터에 추가됩니다.

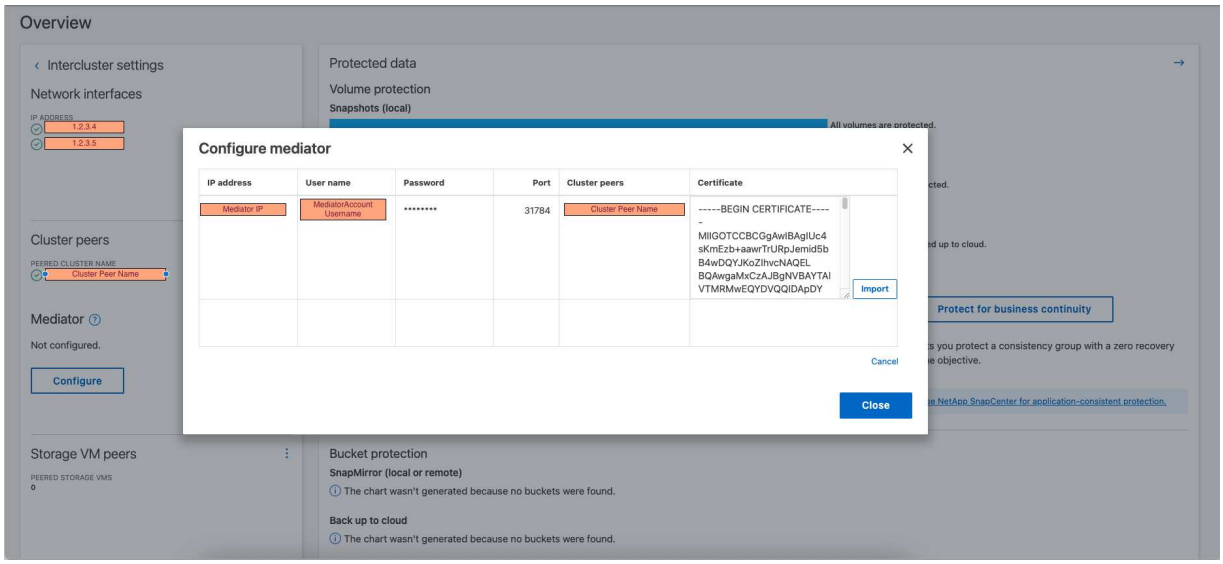
다음 이미지는 성공적인 ONTAP 중재자 구성을 보여줍니다.



ONTAP 중재자 **1.8** 이하

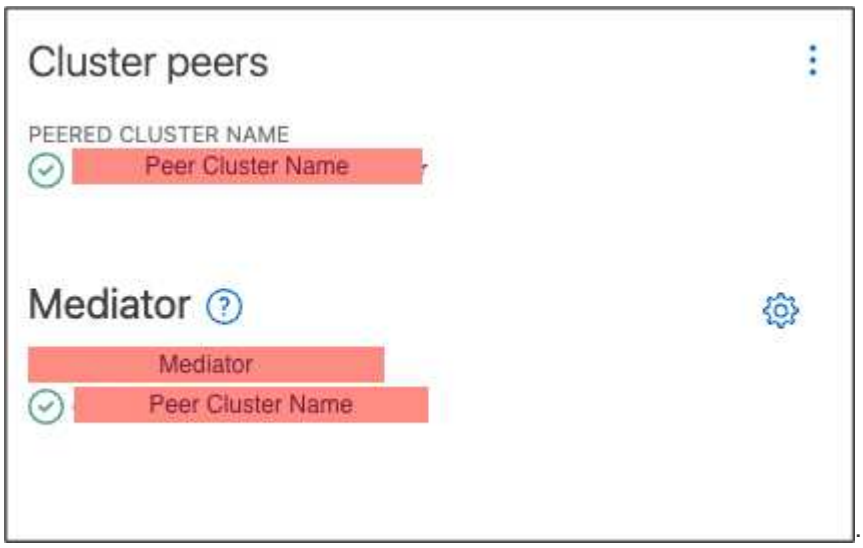
1. 보호 > 개요 > 중재자 > 구성 * 으로 이동합니다.
2. *추가*를 선택하고 다음 ONTAP Mediator 정보를 입력합니다.
   - IPv4 주소입니다
   - 사용자 이름
   - 암호
   - 인증서
3. 다음과 같은 두 가지 방법으로 인증서 입력을 제공할 수 있습니다.
   - * option (a) *: * Import * 를 선택하여 `ca.crt` 파일을 탐색하고 가져옵니다.
   - * option (b) *: 파일의 내용을 `ca.crt` 복사하여 * Certificate * 필드에 붙여 넣습니다.

   모든 세부 정보가 올바르게 입력되면 제공된 인증서가 모든 피어 클러스터에 설치됩니다.



인증서 추가가 완료되면 ONTAP Mediator가 ONTAP 클러스터에 추가됩니다.

다음 이미지는 성공적인 ONTAP 중재자 구성을 보여줍니다.



CLI를 참조하십시오

ONTAP CLI를 사용하여 기본 또는 보조 클러스터에서 ONTAP Mediator를 초기화할 수 있습니다 . `mediator add` 한 클러스터에서 명령을 실행하면 다른 클러스터에 ONTAP Mediator가 자동으로 추가됩니다.

ONTAP Mediator를 사용하여 SnapMirror 활성 동기화 관계를 모니터링하는 경우, 유효한 자체 서명 인증서 또는 인증 기관(CA) 인증서 없이는 ONTAP에서 ONTAP Mediator를 초기화할 수 없습니다. 피어링된 클러스터에 대한 인증서 저장소에 유효한 인증서를 추가합니다. ONTAP Mediator를 사용하여 MetroCluster IP 시스템을 모니터링하는 경우, 초기 구성 후 HTTPS가 사용되지 않으므로 인증서가 필요하지 않습니다.

ONTAP 중재자 **1.9** 이상

1. ONTAP 중재자 Linux VM/호스트 소프트웨어 설치 위치에서 ONTAP 중재자 CA 인증서를 찾습니다 `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. 피어링된 클러스터의 인증서 저장소에 유효한 인증 기관을 추가합니다.

   예:

   ```
   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

3. ONTAP 중재자 CA 인증서를 ONTAP 클러스터에 추가합니다. 메시지가 표시되면 ONTAP Mediator에서 받은 CA 인증서를 삽입하세요. 모든 피어 클러스터에서 단계를 반복합니다.

   ```
   security certificate install -type server-ca -vserver <vserver_name>
   ```

   예:

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. 생성된 인증서 이름을 사용하여 설치된 자체 서명된 CA 인증서를 봅니다.

   `security certificate show -common-name <common_name>`

   예:

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                           ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. 클러스터 중 하나에서 ONTAP Mediator를 초기화합니다. 다른 클러스터에는 ONTAP Mediator가 자동으로 추가됩니다.

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   예:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. 선택적으로 작업 ID 상태를 `job show -id` 확인하여 SnapMirror mediator add 명령이 성공적인지 확인합니다.

   예:

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. ONTAP 중재자 구성의 상태를 점검한다.

스냅미러 중재자 쇼

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

`Quorum Status` SnapMirror 일관성 그룹 관계가 ONTAP Mediator와 동기화되는지 여부를 나타냅니다. `true` 동기화가 성공했음을 나타냅니다.

ONTAP 중재자 **1.8** 이하

1. ONTAP 중재자 Linux VM/호스트 소프트웨어 설치 위치에서 ONTAP 중재자 CA 인증서를 찾습니다 `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. 피어링된 클러스터의 인증서 저장소에 유효한 인증 기관을 추가합니다.

   예:

```
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

3. ONTAP 중재자 CA 인증서를 ONTAP 클러스터에 추가합니다. 메시지가 표시되면 ONTAP 중재자로부터 얻은 CA 인증서를 삽입합니다. 모든 피어 클러스터에서 단계를 반복합니다.

   `security certificate install -type server-ca -vserver <vserver_name>`

   예:

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. 생성된 인증서 이름을 사용하여 설치된 자체 서명된 CA 인증서를 봅니다.

   `security certificate show -common-name <common_name>`

   예:

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                           ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. 클러스터 중 하나에서 ONTAP Mediator를 초기화합니다. 다른 클러스터에는 ONTAP Mediator가 자동으로 추가됩니다.

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   예:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. 선택적으로 작업 ID 상태를 `job show -id` 확인하여 SnapMirror mediator add 명령이 성공적인지 확인합니다.

   예:

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. ONTAP 중재자 구성의 상태를 점검한다.

스냅미러 중재자 쇼

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true
```

`Quorum Status` SnapMirror 일관성 그룹 관계가 ONTAP Mediator와 동기화되는지 여부를 나타냅니다. `true` 동기화가 성공했음을 나타냅니다.

타사 인증서로 **ONTAP** 중재자를 다시 초기화합니다

ONTAP Mediator를 다시 초기화해야 할 수도 있습니다. ONTAP Mediator IP 주소 변경, 인증서 만료 등 ONTAP Mediator를 다시 초기화해야 하는 상황이 발생할 수 있습니다.

다음 절차에서는 자체 서명된 인증서를 타사 인증서로 대체해야 하는 특정 경우에 대해 ONTAP 중재자를 다시 초기화하는 방법을 보여 줍니다.

이 작업에 대해

SnapMirror Active Sync 클러스터의 자체 서명 인증서를 타사 인증서로 교체하고 ONTAP에서 ONTAP Mediator 구성을 제거한 다음 ONTAP Mediator를 추가해야 합니다.

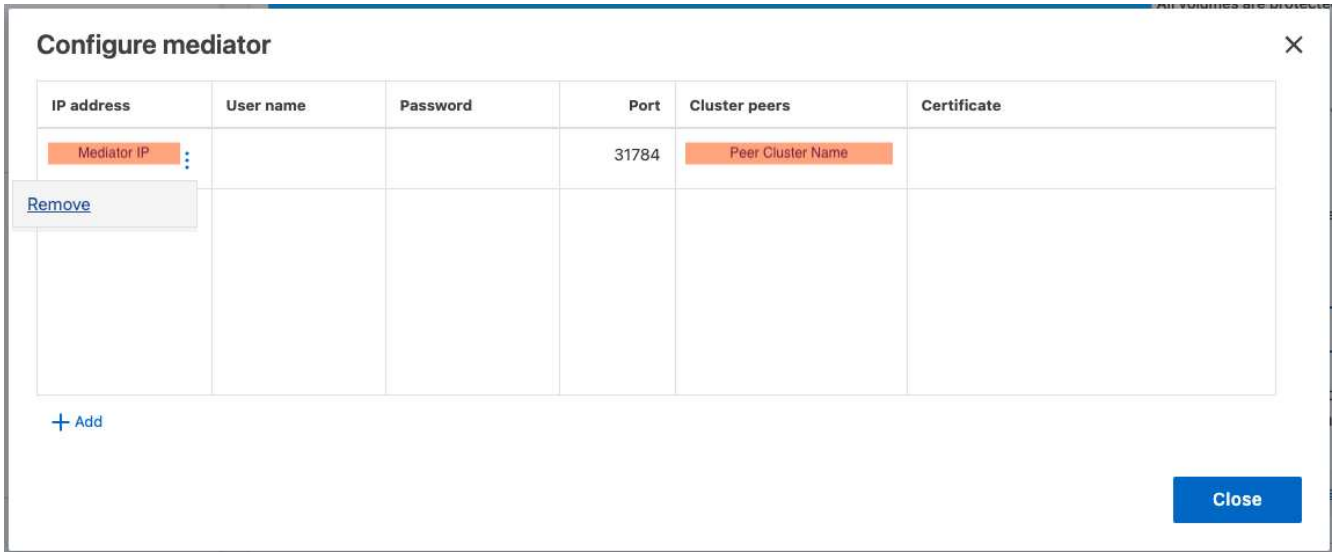
시스템 관리자

System Manager를 사용하여 ONTAP 클러스터에서 이전 자체 서명 인증서로 구성된 ONTAP Mediator 버전을 제거하고 새로운 타사 인증서로 ONTAP 클러스터를 다시 구성해야 합니다.

단계

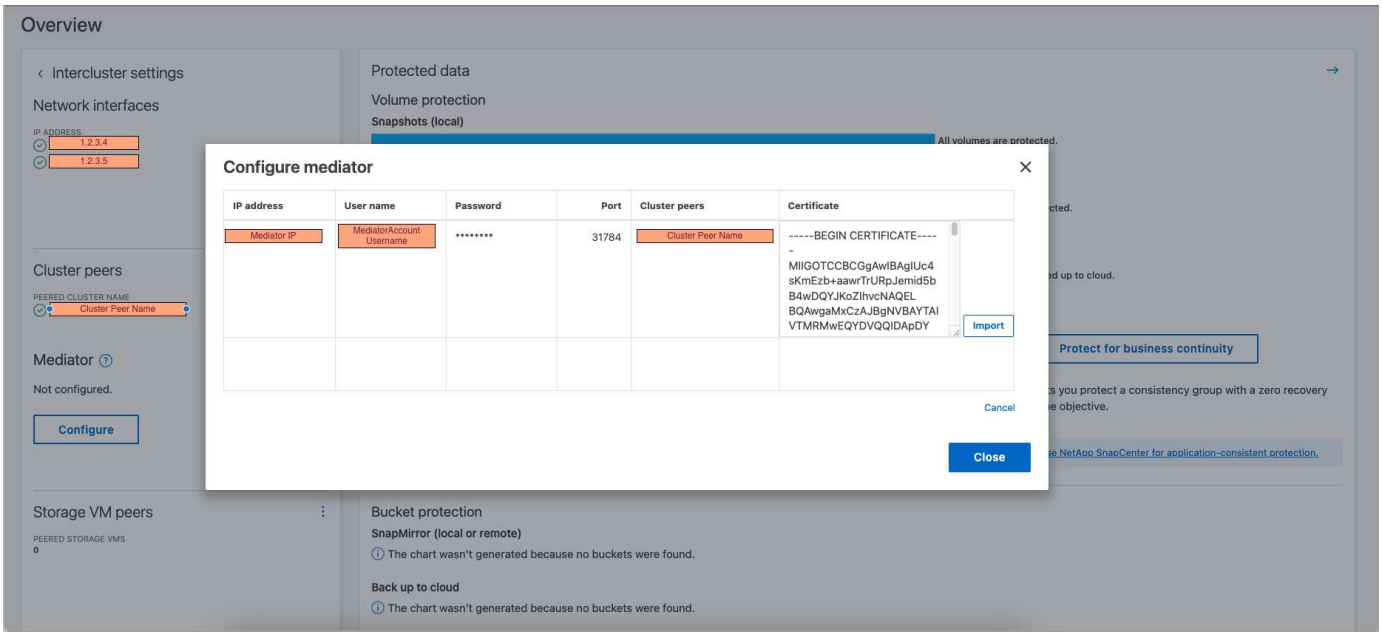
1. 메뉴 옵션 아이콘을 선택하고 *제거*를 선택하여 ONTAP Mediator를 제거하세요.

> ⓘ 이 단계에서는 자체 서명된 server-ca를 ONTAP 클러스터에서 제거하지 않습니다. NetApp에서는 타사 인증서를 추가하기 위해 다음 단계를 수행하기 전에 * Certificate * 탭으로 이동하여 수동으로 제거할 것을 권장합니다.



2. 올바른 인증서로 ONTAP Mediator를 다시 추가합니다.

ONTAP Mediator는 이제 새로운 타사 자체 서명 인증서로 구성되었습니다.



CLI를 참조하십시오

ONTAP CLI를 사용하여 자체 서명된 인증서를 타사 인증서로 대체하여 기본 또는 보조 클러스터에서 ONTAP Mediator를 다시 초기화할 수 있습니다.

ONTAP 중재자 **1.9** 이상

1. 모든 클러스터에 대해 자체 서명된 인증서를 사용할 때 이전에 설치한 자체 서명된 `intermediate.crt` 인증서를 제거합니다. 아래 예에서는 두 개의 클러스터가 있습니다.

   예:

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. 다음을 사용하여 이전에 구성된 ONTAP 중재자를 SnapMirror 활성 동기화 클러스터에서 제거합니다. `-force true`

   예:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. 하위 CA에서 인증서를 가져오는 방법에 대한 지침은 `intermediate.crt` 에 설명된 단계를 "자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿉니다"참조하십시오. 자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿉니다

에는 `intermediate.crt` 파일에 정의된 PKI 권한으로 전송되어야 하는 요청에서 파생되는 특정 속성이 있습니다 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. ONTAP 중재자 Linux VM/호스트 소프트웨어 설치 위치에서 새 타사 ONTAP 중재자 CA 인증서를 `intermediate.crt` 추가합니다.

   예:

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat intermediate.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. `intermediate.crt`피어링된 클러스터에 파일을 추가합니다. 모든 피어 클러스터에 대해 이 단계를 반복합니다.

   예:

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. SnapMirror 활성 동기화 클러스터에서 이전에 구성한 ONTAP 중재자를 제거합니다.

   예:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. ONTAP Mediator를 다시 추가합니다.

   예:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status` SnapMirror 일관성 그룹 관계가 중재자와의 동기화 여부, 즉 상태를 나타냅니다 `true` 동기화가 성공했음을 나타냅니다.

ONTAP 중재자 **1.8** 이하

1. 모든 클러스터에 대해 자체 서명된 인증서를 사용할 때 이전에 설치한 자체 서명된 `ca.crt` 인증서를 제거합니다. 아래 예에서는 두 개의 클러스터가 있습니다.

   예:

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. 다음을 사용하여 이전에 구성된 ONTAP 중재자를 SnapMirror 활성 동기화 클러스터에서 제거합니다. `-force true`

   예:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. 하위 CA에서 인증서를 가져오는 방법에 대한 지침은 `ca.crt` 에 설명된 단계를 "자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿉니다"참조하십시오. 자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿉니다

   > 에는 `ca.crt` 파일에 정의된 PKI 권한으로 전송되어야 하는 요청에서 파생되는 특정 속성이 있습니다 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. ONTAP 중재자 Linux VM/호스트 소프트웨어 설치 위치에서 새 타사 ONTAP 중재자 CA 인증서를 `ca.crt` 추가합니다.

예:

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. `intermediate.crt`피어링된 클러스터에 파일을 추가합니다. 모든 피어 클러스터에 대해 이 단계를 반복합니다.

   예:

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. SnapMirror 활성 동기화 클러스터에서 이전에 구성한 ONTAP 중재자를 제거합니다.

   예:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. ONTAP Mediator를 다시 추가합니다.

   예:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status` SnapMirror 일관성 그룹 관계가 중재자와의 동기화 여부, 즉 상태를 나타냅니다 `true` 동기화가 성공했음을 나타냅니다.

관련 정보

- "작업 표시"
- "보안 인증서 삭제"
- "보안 인증서 설치"
- "보안 인증서가 표시됩니다"
- "스냅미러 중재자 추가"
- "스냅미러 중재자 제거"

- "스냅미러 중재자 쇼"

ONTAP Cloud Mediator 구성을 준비하세요

당신 전에 "ONTAP Cloud Mediator 구성" , 전제 조건이 충족되었는지 확인해야 합니다.

방화벽 요구 사항

도메인 컨트롤러의 방화벽 설정은 HTTPS 트래픽을 허용해야 합니다. `api.bluexp.netapp.com` 두 클러스터 모두에서.

프록시 서버 요구 사항

SnapMirror Active Sync에 프록시 서버를 사용하는 경우 프록시 서버가 생성되었고 다음 프록시 서버 정보가 있는지 확인하세요.

- HTTPS 프록시 IP
- 포트
- 사용자 이름
- 암호

숨어 있음

NetApp 콘솔 클라우드 서버와 SnapMirror Active Sync 클러스터 피어 간의 권장 ping 지연 시간은 200ms 미만입니다.

루트 **CA** 인증서

클러스터에서 인증서를 확인하세요

ONTAP 에는 잘 알려진 루트 CA 인증서가 미리 설치되어 있으므로 대부분의 경우 NetApp 콘솔 서버의 루트 CA 인증서를 설치할 필요가 없습니다. ONTAP Cloud Mediator 구성을 시작하기 전에 클러스터를 확인하여 인증서가 있는지 확인할 수 있습니다.

예:

```
C1_cluster% openssl s_client -showcerts -connect
api.bluexp.netapp.com:443|egrep "s:|i:"
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert
Global Root G2
verify return:1
depth=1 C = US, O = Microsoft Corporation, CN = Microsoft Azure RSA TLS
Issuing CA 04
verify return:1
depth=0 C = US, ST = WA, L = Redmond, O = Microsoft Corporation, CN =
*.azureedge.net
verify return:1
 0 s:/C=US/ST=WA/L=Redmond/O=Microsoft Corporation/CN=*.azureedge.net
   i:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
```

```
04
 1 s:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
04
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
 2 s:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
<====

C1_cluster::> security certificate show -common-name DigiCert*
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
C1_cluster 0CE7E0EXXXXX46FE8FE560FC1BFXXXXX DigiCertAssuredIDRootCA
server-ca
    Certificate Authority: DigiCert Assured ID Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 0B931C3XXXXX67EA6723BFC3AF9XXXXX DigiCertAssuredIDRootG2
server-ca
    Certificate Authority: DigiCert Assured ID Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 0BA15AFXXXXXA0B54944AFCD24AXXXXX DigiCertAssuredIDRootG3
server-ca
    Certificate Authority: DigiCert Assured ID Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 083BE05XXXXX46B1A1756AC9599XXXXX DigiCertGlobalRootCA server-ca
    Certificate Authority: DigiCert Global Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 033AF1EXXXXXA9A0BB2864B11D0XXXXX DigiCertGlobalRootG2 server-ca
    Certificate Authority: DigiCert Global Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 055556BXXXXXA43535C3A40FD5AXXXXX DigiCertGlobalRootG3 server-ca
    Certificate Authority: DigiCert Global Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 02AC5C2XXXXX409B8F0B79F2AE4XXXXX DigiCertHighAssuranceEVRootCA
server-ca
    Certificate Authority: DigiCert High Assurance EV Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 059B1B5XXXXX2132E23907BDA77XXXXX DigiCertTrustedRootG4 server-
ca
```

```
    Certificate Authority: DigiCert Trusted Root G4
          Expiration Date: Fri Jan 15 17:30:00 2038
```

설치된 인증서에 대한 프록시 서버를 확인하세요

NetApp 콘솔에서 ONTAP Cloud Mediator 서비스에 연결하기 위해 프록시를 사용하는 경우 프록시 서버의 루트 CA 인증서가 ONTAP 에 설치되어 있는지 확인하세요.

예:

```
C1_cluster% openssl s_client -showcerts -proxy <ip:port> -connect
api.bluexp.netapp.com:443 |egrep "s:|i:"
```

CA 인증서를 다운로드하세요:

필요한 경우 인증 기관 웹사이트에서 루트 CA 인증서를 다운로드하여 클러스터에 설치할 수 있습니다.

예:

```
C1_cluster::> security certificate install -type server-ca -vserver
C1_cluster

C2_cluster::> security certificate install -type server-ca -vserver
C2_cluster
```

SnapMirror Active Sync를 위한 **ONTAP Cloud Mediator** 구성

ONTAP 9.17.1부터 ONTAP Cloud Mediator를 사용하여 각 클러스터의 상태를 모니터링하여 비즈니스 연속성을 확보할 수 있습니다. ONTAP Cloud Mediator는 클라우드 기반 서비스입니다. SnapMirror 활성 동기화와 함께 ONTAP Cloud Mediator를 사용하는 경우 먼저 NetApp 콘솔 서비스와 클라이언트 정보가 구성되어 있는지 확인하고 적절한 클러스터 피어링을 보장해야 합니다.

ONTAP Mediator와 마찬가지로 ONTAP Cloud Mediator는 SnapMirror 활성 동기화 관계에서 ONTAP 클러스터가 사용하는 고가용성(HA) 메타데이터를 위한 영구적이고 펜싱된 저장소를 제공합니다. ONTAP Cloud Mediator는 쿼럼 결정을 지원하는 동기식 노드 상태 쿼리 기능을 제공하고, 컨트롤러 활성 상태 감지를 위한 ping 프록시 역할을 합니다.

ONTAP 9.17.1과 함께 SnapMirror Active Sync 및 ONTAP Mediator 또는 ONTAP Cloud Mediator를 사용하는 경우 다음에서 *알려진 문제 및 제한 사항*을 검토해야 합니다."ONTAP 릴리즈 노트" 이러한 구성에 대한 중요한 정보는 다음을 참조하세요.

시작하기 전에

ONTAP Cloud Mediator를 구성하기 전에 다음 정보를 확인해야 합니다.

- 클러스터가 구성되었습니다.

  "SnapMirror 활성 동기화를 위한 ONTAP 클러스터 구성"

- NetApp 콘솔에서 NetApp 콘솔 조직 ID를 복사하고 ONTAP Cloud Mediator를 구성할 때 사용할 콘솔 구성원 서비스 계정을 생성했습니다. 서비스 계정을 생성할 때 조직은 ONTAP Cloud Mediator를 구성한 구독으로 설정해야 합니다. 범주는 *애플리케이션*으로, 역할 유형은 * ONTAP Mediator 설정 역할*로 설정해야 합니다. 역할을 생성할 때 클라이언트 ID와 클라이언트 비밀번호를 저장해야 합니다.

  "NetApp 콘솔 멤버 및 서비스 계정 추가"

단계

System Manager나 ONTAP CLI를 사용하여 ONTAP Cloud Mediator를 추가할 수 있습니다.

시스템 관리자

1. *보호 > 개요 > 중재자*로 이동하여 *추가*를 선택합니다.
2. 중개자 추가 창에서 중개자 유형으로 *클라우드*를 선택하고 다음 정보를 입력합니다.
   - NetApp 콘솔 조직 ID
   - NetApp 콘솔 클라이언트 ID
   - NetApp 콘솔 클라이언트 비밀번호
3. 클러스터 피어를 선택하세요.
4. HTTP 프록시를 사용 중이고 아직 구성하지 않은 경우 로컬 및 원격 호스트에 대한 HTTP 프록시 정보를 입력합니다.

   각 클러스터 피어에 대해 다른 프록시 서버를 사용하는 것이 좋습니다.
5. 선택 사항: 특히 프록시 서버를 사용하는 경우 ONTAP 에 루트 CA 인증서를 설치해야 하는 경우 제공된 텍스트 상자에 인증서를 붙여넣습니다.
6. 추가 * 를 선택합니다.
7. *보호 > 개요*로 이동하여 SnapMirror Active Sync 클러스터와 ONTAP Cloud Mediator 간의 관계 상태를 확인합니다.

CLI를 참조하십시오

1. ONTAP Cloud Mediator 구성:
   `snapmirror mediator add -peer-cluster <peerClusterName> -type cloud -bluexp -org-id <NetApp Console Organization ID> -service-account-client-id <Service Account Client ID> -use-http-proxy-local <true|false> -use-http -proxy-remote <true|false>`
2. ONTAP Cloud Mediator 상태 확인:
   `snapmirror mediator show`

   예:

```
C1_cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
0.0.0.0          C2_cluster       connected         true
cloud
```

ONTAP SnapMirror Active Sync로 보호하세요

SnapMirror 액티브 동기화는 ONTAP 9.15.1부터 대칭 액티브/액티브 보호까지 비대칭 보호를 제공합니다.

SnapMirror 활성 동기화를 사용하여 비대칭 보호를 구성하려면 ONTAP 소스 클러스터에서 LUN을 선택하고 일관성 그룹에 추가해야 합니다.

시작하기 전에

- SnapMirror 동기식 라이센스가 있어야 합니다.
- 클러스터 또는 스토리지 VM 관리자여야 합니다.
- 일관성 그룹의 모든 구성 볼륨은 단일 스토리지 VM(SVM)에 있어야 합니다.
  - LUN은 서로 다른 볼륨에 상주할 수 있습니다.
- 소스 클러스터와 대상 클러스터는 같을 수 없습니다.
- ASA 클러스터 및 비 ASA 클러스터에 걸쳐 SnapMirror 활성 동기화 일관성 그룹 관계를 설정할 수 없습니다.
- 클러스터 피어 관계를 위한 SnapMirror 액티브 동기화에 기본 IPspace가 필요합니다. 사용자 지정 IPspace는 지원되지 않습니다.
- 일관성 그룹의 이름은 고유해야 합니다.
- 보조(대상) 클러스터의 볼륨은 DP 유형이어야 합니다.
- 운영 SVM과 2차 SVM은 피어링된 관계에 있어야 합니다.

단계

ONTAP CLI 또는 System Manager를 사용하여 일관성 그룹을 구성할 수 있습니다.

ONTAP 9.10.1부터 ONTAP System Manager에서 일관성 그룹 엔드포인트와 메뉴를 제공하여 추가 관리 유틸리티를 제공합니다. ONTAP 9.10.1 이상을 사용하는 경우 다음을 참조하십시오. "일관성 그룹을 구성합니다" 그 다음에 "보호 구성" SnapMirror 활성 동기화 관계를 생성합니다.

ONTAP 9.14.1부터 9.8까지 SnapMirror 액티브 동기화는 SnapMirror 비즈니스 연속성(SM-BC)이라고 합니다.

시스템 관리자

1. 운영 클러스터에서 * 보호 > 개요 > 무중단 업무 운영 보호 > LUN 보호 * 로 이동합니다.
2. 보호할 LUN을 선택하고 보호 그룹에 추가합니다.
3. 대상 클러스터와 SVM을 선택합니다.
4. 기본적으로 * 관계 초기화 * 가 선택됩니다. 보호를 시작하려면 * 저장 * 을 클릭합니다.
5. 대시보드 > 성능 * 으로 이동하여 LUN의 IOPS 활동을 확인합니다.
6. 대상 클러스터에서 System Manager를 사용하여 비즈니스 연속성 관계에 대한 보호가 동기화 상태인지 확인합니다. * 보호 > 관계 *.

CLI를 참조하십시오

1. 타겟 클러스터에서 일관성 그룹 관계를 생성합니다.
   `destination::> snapmirror create -source-path` *`source-path`* `-destination-path` *`destination-path`* `-cg-item-mappings` *`volume-paths`* `-policy` *`policy-name`*

   를 사용하여 구성 볼륨을 최대 12개까지 매핑할 수 있습니다 `cg-item-mappings` 의 매개 변수입니다 `snapmirror create` 명령.

   다음 예에서는 두 개의 일관성 그룹을 생성합니다. `cg_src_ on the source with `vol1` 및 `vol2` 미러링된 타겟 정합성 보장 그룹, `cg_dst`.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOverDuplex
   ```

2. 대상 클러스터에서 일관성 그룹을 초기화합니다.

   `destination::>snapmirror initialize -destination-path` *`destination-consistency-group`*

3. 초기화 작업이 성공적으로 완료되었는지 확인하십시오. 상태는 InSync가 되어야 합니다.

   스냅미러 쇼

4. 각 클러스터에서 igroup을 생성하여 애플리케이션 호스트의 이니시에이터에 LUN을 매핑할 수 있습니다.
   `lun igroup create -igroup` *`name`* `-protocol` *`fcp|iscsi`* `-ostype` *`os`* `-initiator` *`initiator_name`*

   에 대한 자세한 내용은 `lun igroup create` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 각 클러스터에서 LUN을 igroup에 매핑합니다.

   `lun map -path` *`path_name`* `-igroup` *`igroup_name`*

6. 에서 LUN 매핑이 성공적으로 완료되었는지 확인합니다 `lun map` 명령. 그런 다음 애플리케이션 호스트에서 새 LUN을 검색할 수 있습니다.

System Manager 또는 ONTAP CLI를 사용하여 대칭 보호를 설정할 수 있습니다. 두 인터페이스 모두에서 에 대한 단계가 다릅니다 균일 및 비균일 설정.

시작하기 전에

- 두 클러스터에서 모두 ONTAP 9.15.1 이상을 실행해야 한다.
- 대칭 액티브/액티브 구성에는 이 필요합니다 `AutomatedFailoverDuplex` 보호 정책. 또는, 가능합니다 사용자 지정 SnapMirror 정책을 생성합니다 제공함 `-type` 있습니다 `automated-failover-duplex`.
- ONTAP 9.15.1에서 대칭 액티브/액티브는 2노드 클러스터에서만 지원됩니다.
- ONTAP 9.16.1 GA부터 SnapMirror 액티브 동기화는 4노드 클러스터에서 대칭 액티브/액티브 구성을 지원합니다.
  - 4노드 클러스터에서 SnapMirror 액티브 동기화를 사용하려면 ONTAP 9.16.1 GA 이상을 실행해야 합니다.
  - 4노드 구성을 배포하기 전에 먼저 해야 클러스터 피어 관계를 생성합니다합니다.
  - 4노드 클러스터의 경우 를 제한검토합니다.
  - 2노드 클러스터로 되돌리는 경우 되돌리기 전에 클러스터에서 SnapMirror 액티브 동기화 관계를 제거해야 합니다.
  - 4노드 구성을 사용하여 스토리지와 컨트롤러를 업그레이드할 수 있습니다. 이 프로세스는 무중단 작업으로, 볼륨을 새 노드로 이동하는 동안 클러스터를 확장합니다. 자세한 내용은 을 "클러스터를 새로 고칩니다 "참조하십시오.
- ONTAP 9.17.1부터 두 클러스터 모두 ONTAP 9.17.1 이상을 실행하는 경우에만 NVMe 네임스페이스에서 대칭적 액티브/액티브 보호를 구성할 수 있습니다.

SCSI SnapMirror 활성 동기화 구성을 사용하여 대칭 활성/활성 보호 구성

단계

시스템 관리자나 ONTAP CLI를 사용하여 SCSI 프로토콜 호스트 매핑을 사용하여 대칭적 활성/활성 보호를 구성할 수 있습니다.

시스템 관리자

균일 설정에 대한 단계

1. 운영 사이트에서 "새 LUN을 사용하여 일관성 그룹을 생성합니다."
   a. 일관성 그룹을 생성할 때 호스트 이니시에이터를 지정하여 igroup을 생성합니다.
   b. 확인란을 선택하여 **SnapMirror** 활성화 를 선택한 다음 을 선택합니다 `AutomatedFailoverDuplex` 정책.
   c. 표시되는 대화 상자에서 **Replicate initiator groups** 확인란을 선택하여 igroup을 복제합니다. 근접 설정 편집** 에서 호스트의 근접 SVM을 설정합니다.
   d. 저장을 선택합니다.

비균일 설정에 대한 단계

1. 운영 사이트에서 "새 LUN을 사용하여 일관성 그룹을 생성합니다."
   a. 일관성 그룹을 생성할 때 호스트 이니시에이터를 지정하여 igroup을 생성합니다.
   b. 확인란을 선택하여 **SnapMirror** 활성화 를 선택한 다음 을 선택합니다 `AutomatedFailoverDuplex` 정책.
   c. LUN, 일관성 그룹, igroup, SnapMirror 관계 및 igroup 매핑을 생성하려면 저장을 선택합니다.
2. 2차 사이트에서 igroup을 생성하고 LUN을 매핑합니다.
   a. **Hosts> SAN Initiator Groups** 로 이동합니다.
   b. 새 igroup을 생성하려면 **+** 추가 를 선택하십시오.
   c. 이름 제공, 호스트 운영 체제 를 선택한 다음 이니시에이터 그룹 구성원 을 선택합니다.
   d. 관계를 초기화하려면 저장 을 선택합니다.
3. 새로운 igroup을 대상 LUN에 매핑합니다.
   a. 스토리지 **>** LUN** 으로 이동합니다.
   b. igroup에 매핑할 모든 LUN을 선택합니다.
   c. 추가 를 선택한 다음 이니시에이터 그룹에 매핑** 을 선택합니다.

CLI를 참조하십시오

균일 설정에 대한 단계

1. 애플리케이션의 모든 볼륨을 그룹화하는 새로운 SnapMirror 관계를 생성합니다. 를 지정했는지 확인합니다 `AutomatedFailOverDuplex` 양방향 동기화 복제를 설정하는 정책입니다.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   예: 다음 예에서는 두 개의 일관성 그룹을 만듭니다. 소스에 vol1 및 vol2가 있는 cg_src와 대상에 미러링된 일관성 그룹인 cg_dst입니다.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
AutomatedFailOverDuplex
```

2. SnapMirror 관계 초기화:
`snapmirror initialize -destination-path <destination-consistency-group>`
3. 을(를) 기다리면 작업이 성공적으로 수행되었는지 확인합니다 `Mirrored State` 를 눌러 로 표시합니다 `SnapMirrored` 및 `Relationship Status` 현재 `Insync`.

   `snapmirror show -destination-path <destination_path>`
4. 호스트에서 필요에 따라 각 클러스터에 대한 액세스를 통해 호스트 연결을 구성합니다.
5. igroup 구성을 설정합니다. 로컬 클러스터에서 이니시에이터에 대한 기본 경로를 설정합니다. 역선호도를 위해 피어 클러스터로 구성을 복제하는 옵션을 지정합니다.

   ```
   SiteA::> igroup create -vserver <svm_name> -ostype <os_type> -igroup
   <igroup_name> -replication-peer <peer_svm_name> -initiator <host>
   ```

   ONTAP 9.16.1부터 `-proximal-vserver local` 이 명령의 매개 변수를 사용합니다.

   ```
   SiteA::> igroup add -vserver <svm_name> -igroup <igroup_name> -ostype
   <os_type> -initiator <host>
   ```

   ONTAP 9.16.1부터 `-proximal-vserver peer` 이 명령의 매개 변수를 사용합니다.
6. 호스트에서 경로를 검색하고 호스트에 기본 클러스터에서 스토리지 LUN으로 연결되는 활성/최적화된 경로가 있는지 확인합니다.
7. 애플리케이션을 배포하고 VM 워크로드를 클러스터 전체에 분산하여 필요한 로드 밸런싱을 수행합니다.

비균일 설정에 대한 단계

1. 애플리케이션의 모든 볼륨을 그룹화하는 새로운 SnapMirror 관계를 생성합니다. 를 지정했는지 확인합니다 `AutomatedFailOverDuplex` 양방향 동기화 복제를 설정하는 정책입니다.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   예: 다음 예에서는 두 개의 일관성 그룹을 만듭니다. 소스에 vol1 및 vol2가 있는 cg_src와 대상에 미러링된 일관성 그룹인 cg_dst입니다.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
   AutomatedFailOverDuplex
   ```

2. SnapMirror 관계 초기화:
   `snapmirror initialize -destination-path <destination-consistency-group>`
3. 을(를) 기다리면 작업이 성공적으로 수행되었는지 확인합니다 `Mirrored State` 를 눌러 로 표시합니다 `SnapMirrored` 및 `Relationship Status` 현재 `Insync`.

   ```
   snapmirror show -destination-path <destination_path>
   ```

4. 호스트에서 필요에 따라 각 클러스터에 대한 액세스를 통해 호스트 연결을 구성합니다.
5. 소스 및 대상 클러스터 모두에서 igroup 구성을 설정합니다.

   ```
   # primary site
   SiteA::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_1_name_>

   # secondary site
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_2_name>
   ```

6. 호스트에서 경로를 검색하고 호스트에 기본 클러스터에서 스토리지 LUN으로 연결되는 활성/최적화된 경로가 있는지 확인합니다.
7. 애플리케이션을 배포하고 VM 워크로드를 클러스터 전체에 분산하여 필요한 로드 밸런싱을 수행합니다.

NVMe SnapMirror 활성 동기화 구성을 사용하여 대칭 활성/활성 보호 구성

시작하기 전에

대칭적 액티브/액티브 보호를 구성하는 데 필요한 요구 사항 외에도 NVMe 프로토콜을 사용할 때 지원되는 구성과 지원되지 않는 구성을 알고 있어야 합니다.

- 일관성 그룹에는 하나 이상의 하위 시스템이 있을 수 있습니다.
- 일관성 그룹 내의 볼륨은 여러 하위 시스템의 네임스페이스 맵을 가질 수 있습니다.
- 하위 시스템은 두 개 이상의 일관성 그룹에 속하는 네임스페이스 맵을 가질 수 없습니다.
- 하위 시스템은 일관성 그룹에 속하는 일부 네임스페이스 맵과 일관성 그룹에 속하지 않는 일부 네임스페이스 맵을 가질 수 없습니다.
- 하위 시스템에는 동일한 일관성 그룹에 속하는 네임스페이스 맵이 있어야 합니다.

단계

ONTAP 9.17.1부터 System Manager나 ONTAP CLI를 사용하여 일관성 그룹을 만들고 NVMe 프로토콜 호스트 매핑을 사용하여 대칭적 활성/활성 보호를 구성할 수 있습니다.

시스템 관리자

1. 기본 사이트에서 "새로운 볼륨이나 NVMe 네임스페이스를 사용하여 일관성 그룹을 만듭니다."
2. *+추가*를 선택하고 *새 NVMe 네임스페이스 사용*을 선택합니다.
3. 일관성 그룹 이름을 입력하세요.
4. *더보기*를 선택하세요.
5. 보호 섹션에서 * SnapMirror 활성화*를 선택한 다음 다음을 선택합니다. `AutomatedFailoverDuplex` 정책.
6. 호스트 매핑 섹션에서 기존 **NVMe** 하위 시스템 또는 *새 NVMe 하위 시스템*을 선택합니다.
7. 근위 SVM을 변경하려면 *근접*을 선택하세요. 기본적으로 소스 SVM이 선택됩니다.
8. 필요한 경우 다른 NVMe 하위 시스템을 추가합니다.

CLI를 참조하십시오

1. 애플리케이션에서 사용하는 모든 NVMe 네임스페이스를 포함하는 모든 볼륨을 그룹화하는 새 SnapMirror 관계를 생성합니다 . `AutomatedFailOverDuplex` 양방향 동기화 복제를 설정하는 정책입니다.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   예:

   ```
   DST::> snapmirror create -source-path vs_src:/cg/cg_src_1
   -destination-path vs_dst:/cg/cg_dst_1 -cg-item-mappings
   vs_src_vol1:@vs_dst_vol1,vs_src_vol2:@vs_dst_vol2 -policy
   AutomatedFailOverDuplex
   ```

2. SnapMirror 관계 초기화:
   `snapmirror initialize -destination-path <destination-consistency-group>`

   예:

   ```
   DST::> snapmirror initialize -destination-path vs1:/cg/cg_dst_1
   ```

3. 을(를) 기다리면 작업이 성공적으로 수행되었는지 확인합니다 `Mirrored State` 를 눌러 로 표시합니다 `SnapMirrored` 및 `Relationship Status` 현재 `Insync`.

   ```
   snapmirror show -destination-path <destination_path>
   ```

   기본 볼륨의 NVMe 네임스페이스와 연결된 NVMe 하위 시스템은 자동으로 보조 클러스터에 복제됩니다.

4. 호스트에서 필요에 따라 각 클러스터에 대한 액세스를 통해 호스트 연결을 구성합니다.
5. 각 호스트에 인접한 SVM을 지정하세요. 이렇게 하면 호스트가 기본 클러스터의 경로를 사용하여 NVMe 네임스페이스에 액세스할 수 있습니다. 이는 기본 클러스터의 SVM 또는 DR 클러스터의 SVM일 수 있습니다.

다음 명령은 SVM VS_A가 호스트 H1에 근접해 있고 VS_A를 근접 SVM으로 설정함을 나타냅니다.

```
SiteA::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H1_NQN>
-proximal-vservers <VS_A>
```

다음 명령은 SVM VS_B가 호스트 H2에 근접해 있음을 나타내며 VS_B를 근접 SVM으로 설정합니다.

```
SiteB::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H2_NQN>
-proximal-vservers <VS_B>
```

6. 호스트에서 경로를 검색하고 호스트에 기본 클러스터의 스토리지로 가는 활성/최적화된 경로가 있는지 확인합니다.
7. 애플리케이션을 배포하고 VM 워크로드를 클러스터 전체에 분산하여 필요한 로드 밸런싱을 수행합니다.

관련 정보

- "SnapMirror 생성"
- "SnapMirror 초기화"
- "스냅미러 쇼"

기존 **ONTAP SnapMirror** 관계를 **SnapMirror Active Sync** 관계로 변환

SnapMirror 보호를 구성한 경우 관계를 SnapMirror 액티브 동기화로 변환할 수 있습니다. ONTAP 9.15.1부터 대칭 액티브/액티브 보호를 사용하도록 관계를 변환할 수 있습니다.

기존 **iSCSI** 또는 **FC SnapMirror** 관계를 비대칭 **SnapMirror Active Sync** 관계로 변환

소스 클러스터와 대상 클러스터 간에 기존 iSCSI 또는 FC SnapMirror 동기 관계가 있는 경우, 이를 비대칭 SnapMirror 활성 동기화 관계로 변환할 수 있습니다. 이를 통해 미러링된 볼륨을 일관성 그룹과 연결하여 다중 볼륨 워크로드에서 RPO를 0으로 유지할 수 있습니다. 또한 SnapMirror 활성 동기화 관계 설정 이전 시점으로 되돌려야 하는 경우 기존 SnapMirror 스냅샷을 보존할 수 있습니다.

이 작업에 대해

- Primary 및 Secondary 클러스터에서 클러스터 및 SVM 관리자여야 합니다.
- SnapMirror 정책을 변경하여 제로 RPO를 제로 RTO 동기화로 변환할 수 없습니다.
- 를 실행하기 전에 LUN이 매핑 해제되었는지 확인해야 합니다 `snapmirror create` 명령.

  2차 볼륨의 기존 LUN이 매핑되어 있는 경우 `AutomatedFailover` 정책이 구성되어 있습니다 `snapmirror create` 명령이 오류를 트리거합니다.

시작하기 전에

- 기본 클러스터와 보조 클러스터 사이에는 0 RPO SnapMirror 동기 관계가 존재해야 합니다.
- 제로 RTO SnapMirror 관계를 생성하기 전에 대상 볼륨의 모든 LUN을 매핑 해제해야 합니다.
- SnapMirror 액티브 동기화는 SAN 프로토콜만 지원합니다(NFS/CIFS 제외). NAS 액세스를 위해 정합성 보장 그룹의 구성 요소 가 마운트되지 않았는지 확인합니다.
- "ONTAP 중재자" SnapMirror Active Sync에 맞게 구성해야 합니다.

단계

1. 보조 클러스터에서 기존 관계에 대한 SnapMirror 업데이트를 수행합니다.

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

2. SnapMirror 업데이트가 성공적으로 완료되었는지 확인합니다.

```
SiteB::>snapmirror show
```

3. 각 제로 RPO 동기식 관계를 일시 중지합니다.

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. 각 제로 RPO 동기식 관계 삭제:

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1

SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. 소스 SnapMirror 관계를 해제하지만 공통 스냅샷은 보존합니다.

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1

SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. 제로 RTO SnapMirror 동기식 관계 생성:

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailover
```

7. 정합성 보장 그룹을 다시 동기화합니다.

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. 호스트 LUN 입출력 경로를 재검색하여 LUN에 대한 모든 경로를 복구합니다.

기존 **iSCSI** 또는 **FC SnapMirror** 관계를 대칭 활성/활성으로 변환

ONTAP 9.15.1부터 기존 iSCSI 또는 FC SnapMirror 관계를 SnapMirror 활성 동기화 대칭 활성/활성 관계로 변환할 수 있습니다.

시작하기 전에

- ONTAP 9.15.1 이상을 실행 중이어야 합니다.
- 운영 클러스터와 2차 클러스터 사이에 제로 RPO SnapMirror 동기화 관계가 있어야 합니다.
- 제로 RTO SnapMirror 관계를 생성하기 전에 대상 볼륨의 모든 LUN을 매핑 해제해야 합니다.

- SnapMirror 액티브 동기화는 SAN 프로토콜만 지원합니다(NFS/CIFS 제외). NAS 액세스를 위해 정합성 보장 그룹의 구성 요소 가 마운트되지 않았는지 확인합니다.
- "ONTAP 중재자" SnapMirror Active Sync에 맞게 구성해야 합니다.

단계

1. 보조 클러스터에서 기존 관계에 대한 SnapMirror 업데이트를 수행합니다.

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

2. SnapMirror 업데이트가 성공적으로 완료되었는지 확인합니다.

```
SiteB::>snapmirror show
```

3. 각 제로 RPO 동기식 관계를 일시 중지합니다.

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. 각 제로 RPO 동기식 관계 삭제:

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1

SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. 소스 SnapMirror 관계를 해제하지만 공통 스냅샷은 보존합니다.

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1

SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. AutomatedFailoverDuplex 정책을 사용하여 제로 RTO SnapMirror 동기식 관계를 생성합니다.

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailoverDuplex
```

7. 기존 호스트가 로컬 운영 클러스터인 경우 보조 클러스터에 호스트를 추가하고 각 클러스터에 대한 각 액세스 권한을 사용하여 연결을 설정합니다.
8. 2차 사이트에서 원격 호스트와 연결된 igroup에서 LUN 매핑을 삭제합니다.

   igroup에 복제되지 않은 LUN에 대한 맵이 포함되어 있지 않은지 확인합니다.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

9. 운영 사이트에서 기존 호스트의 이니시에이터 구성을 수정하여 로컬 클러스터의 이니시에이터에 대한 근위 경로를 설정합니다.

```
SiteA::> igroup initiator add-proximal-vserver -vserver <svm_name> -initiator
<host> -proximal-vserver <server>
```

10. 새로운 호스트에 대한 새로운 igroup 및 이니시에이터를 추가하고 호스트 선호도를 해당 로컬 사이트에 근접하게 설정합니다. Ennable igroup replication으로 구성을 복제하고 원격 클러스터에서 호스트 인접성을 반전합니다.

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator host2
-proximal-vserver vsB
```

11. 호스트에서 경로를 검색하고 호스트에 기본 클러스터에서 스토리지 LUN에 대한 활성/최적화 경로가 있는지 확인합니다
12. 애플리케이션을 배포하고 VM 워크로드를 클러스터 전체에 분산합니다.
13. 정합성 보장 그룹을 다시 동기화합니다.

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

14. 호스트 LUN 입출력 경로를 재검색하여 LUN에 대한 모든 경로를 복구합니다.

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 중지"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"
- "스냅미러 쇼"

ONTAP SnapMirror 활성 동기화 관계 유형 변환

ONTAP 9.15.1부터 비대칭에서 대칭 액티브/액티브로, 또는 그 반대로 SnapMirror 액티브 동기화 보호 유형 간에 전환할 수 있습니다.

대칭 액티브/액티브 관계로 변환합니다

비대칭 보호 기능이 있는 iSCSI 또는 FC SnapMirror 활성 동기화 관계를 대칭 활성/활성으로 변환할 수 있습니다.

시작하기 전에

- 두 클러스터에서 모두 ONTAP 9.15.1 이상을 실행해야 한다.
- 대칭 액티브/액티브 구성에는 이 필요합니다 `AutomatedFailoverDuplex` 보호 정책. 또는, 가능합니다 사용자 지정 SnapMirror 정책을 생성합니다 제공함 `-type` 있습니다 `automated-failover-duplex`.

시스템 관리자

균일 설정에 대한 단계

1. 대상 igroup 제거:
   a. 대상 클러스터에서 **Hosts** > **SAN Initiator Groups** 로 이동합니다.
   b. SnapMirror 관계가 있는 igroup을 선택한 다음 삭제 를 선택합니다.
   c. 대화 상자에서 연결된 **LUN** 매핑 해제 상자를 선택한 다음 삭제 를 선택합니다.
2. SnapMirror 활성 동기화 관계를 편집합니다.
   a. 보호> 관계 로 이동합니다.
   b. 수정할 관계 옆에 있는 kabob 메뉴를 선택한 다음 편집 을 선택합니다.
   c. 보호 정책을 AutomatedFailoverDuplex로 수정합니다.
   d. 선택 `AutoMatedFailoverDuplex` 호스트 근접 설정을 수정할 수 있는 대화 상자를 표시합니다. 초기자에 대해 초기자 근위에서부터 그리고 저장에 대한 적절한 옵션을 선택합니다.
   e. 저장을 선택합니다.
3. 보호 메뉴에서 관계가 로 표시될 때 작업이 성공했는지 확인합니다 `InSync`.

비균일 설정에 대한 단계

1. 대상 igroup 제거:
   a. 보조 사이트에서 **Hosts** > **SAN Initiator Groups** 로 이동합니다.
   b. SnapMirror 관계가 있는 igroup을 선택한 다음 삭제 를 선택합니다.
   c. 대화 상자에서 연결된 **LUN** 매핑 해제 상자를 선택한 다음 삭제 를 선택합니다.
2. 새로운 igroup 작성:
   a. 대상 사이트의 **SAN Initiator Groups** 메뉴에서 **Add** 를 선택합니다.
   b. 이름 제공, 호스트 운영 체제 를 선택한 다음 이니시에이터 그룹 구성원 을 선택합니다.
   c. 저장을 선택합니다.
3. 새로운 igroup을 대상 LUN에 매핑합니다.
   a. 스토리지 **>** LUN** 으로 이동합니다.
   b. igroup에 매핑할 모든 LUN을 선택합니다.
   c. 추가 를 선택한 다음 이니시에이터 그룹에 매핑** 을 선택합니다.
4. SnapMirror 활성 동기화 관계를 편집합니다.
   a. 보호> 관계 로 이동합니다.
   b. 수정할 관계 옆에 있는 kabob 메뉴를 선택한 다음 편집 을 선택합니다.
   c. 보호 정책을 AutomatedFailoverDuplex로 수정합니다.
   d. AutoMatedFailoverDuplex 를 선택하면 호스트 근접 설정을 수정하는 옵션이 시작됩니다. 초기자에 대해 초기자 근위에서부터 그리고 저장에 대한 적절한 옵션을 선택합니다.
   e. 저장을 선택합니다.

5. 보호 메뉴에서 관계가 로 표시될 때 작업이 성공했는지 확인합니다 `InSync`.

CLI를 참조하십시오

균일 설정에 대한 단계

1. 에서 SnapMirror 정책을 수정합니다 `AutomatedFailover` 를 선택합니다 `AutomatedFailoverDuplex`:

   ```
   snapmirror modify -destination-path <destination_path> -policy
   AutomatedFailoverDuplex
   ```

2. 정책을 수정하면 재동기화가 트리거됩니다. 다시 동기화가 완료될 때까지 기다린 다음 관계가 인지 확인합니다 `Insync`:

   ```
   snapmirror show -destination-path <destination_path>
   ```

3. 기존 호스트가 로컬 운영 클러스터인 경우 호스트를 두 번째 클러스터에 추가하고 각 클러스터에 대한 각 액세스 권한을 사용하여 연결을 설정합니다.
4. 2차 사이트에서 원격 호스트와 연결된 igroup에서 LUN 매핑을 삭제합니다.

   igroup에 복제되지 않은 LUN에 대한 맵이 포함되어 있지 않은지 확인합니다.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

5. 운영 사이트에서 권한 수준을 다음과 같이 설정합니다 `advanced`.

   ```
   SiteA::> set -privilege advanced
   ```

6. 기존 호스트의 이니시에이터 구성을 수정하여 로컬 클러스터의 이니시에이터에 대한 근위 경로를 설정합니다.

   ```
   SiteA::*> igroup initiator add-proximal-vserver -vserver <svm_name>
   -initiator <host> -proximal-vserver <server>
   ```

   이 단계를 완료한 후 권한 수준을 admin으로 다시 설정할 수 있습니다.

7. 새로운 호스트에 대한 새로운 igroup 및 이니시에이터를 추가하고 호스트 선호도를 해당 로컬 사이트에 근접하게 설정합니다. Ennable igroup replication으로 구성을 복제하고 원격 클러스터에서 호스트 인접성을 반전합니다.

   ```
   SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
   SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator
   host2 -proximal-vserver vsB
   ```

8. 호스트에서 경로를 검색하고 호스트에 기본 클러스터에서 스토리지 LUN에 대한 활성/최적화 경로가 있는지 확인합니다
9. 애플리케이션을 배포하고 VM 워크로드를 클러스터 전체에 분산합니다.

비균일 설정에 대한 단계

1. 에서 SnapMirror 정책을 수정합니다 `AutomatedFailover` 를 선택합니다 `AutomatedFailoverDuplex`:

   ```
   snapmirror modify -destination-path <destination_path> -policy
   AutomatedFailoverDuplex
   ```

2. 정책을 수정하면 재동기화가 트리거됩니다. 다시 동기화가 완료될 때까지 기다린 다음 관계가 인지 확인합니다 `Insync`:

   ```
   snapmirror show -destination-path <destination_path>
   ```

3. 기존 호스트가 운영 클러스터에 로컬인 경우 호스트를 두 번째 클러스터에 추가하고 각 클러스터에 대한 각 액세스 권한을 사용하여 연결을 설정합니다.
4. 2차 사이트에서 새로운 호스트에 대한 새로운 igroup 및 이니시에이터를 추가하고 호스트 유사성을 로컬 사이트에 설정합니다. LUN을 igroup에 매핑합니다.

   ```
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup>
   SiteB::> igroup add -vserver <svm_name> -igroup <igroup> -initiator
   <host_name>
   SiteB::> lun mapping create -igroup <igroup> -path <path_name>
   ```

5. 호스트에서 경로를 검색하고 호스트에 기본 클러스터에서 스토리지 LUN에 대한 활성/최적화 경로가 있는지 확인합니다
6. 애플리케이션을 배포하고 VM 워크로드를 클러스터 전체에 분산합니다.

대칭형 액티브/액티브 관계에서 비대칭형 **iSCSI** 또는 **FC** 관계로 변환

iSCSI 또는 FC를 사용하여 대칭적 액티브/액티브 보호를 구성한 경우 ONTAP CLI를 사용하여 해당 관계를 비대칭적 보호로 변환할 수 있습니다.

단계

1. 모든 VM 워크로드를 소스 클러스터의 로컬 호스트로 이동합니다.
2. VM 인스턴스를 관리하지 않는 호스트에 대한 igroup 구성을 제거한 다음 igroup 구성을 수정하여 igroup 복제를 종료합니다.

   ```
   igroup modify -vserver <svm_name> -igroup <igroup> -replication-peer -
   ```

3. 보조 사이트에서 LUN 매핑을 해제합니다.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

4. 보조 사이트에서 대칭 액티브/액티브 관계를 삭제합니다.

   ```
   SiteB::> snapmirror delete -destination-path <destination_path>
   ```

5. 운영 사이트에서 대칭 액티브/액티브 관계를 해제합니다.
   `SiteA::> snapmirror release -destination-path <destination_path> -relationship -info-only true`

6. 보조 사이트에서 정책을 사용하여 동일한 볼륨 세트에 대한 관계를 생성하여 `AutomatedFailover` 관계를 다시 동기화합니다.

```
SiteB::> snapmirror create -source-path <source_path> -destination-path
<destination_path> -cg-item-mappings <source:@destination> -policy
AutomatedFailover
SiteB::> snapmirror resync -destination-path vs1:/cg/cg1_dst -policy
<policy_type>
```

> 관계를 다시 생성하기 전에 보조 사이트의 정합성 보장 그룹이 "삭제할 수 있습니다"필요합니다. 대상 볼륨"DP 유형으로 변환해야 합니다" 볼륨을 DP로 변환하려면, `MirrorAllSnapshots` 또는 `Sync` 가 아닌 정책과 함께 명령을-`AutomatedFailover` 수행합니다 `snapmirror resync`. `MirrorAndVault`

7. 미러 상태 관계가 인지 확인합니다 `Snapmirrored` 관계 상태는 입니다 `Insync`.

```
snapmirror show -destination-path destination_path
```

8. 호스트에서 경로를 다시 검색합니다.

관련 정보

- "SnapMirror 삭제"
- "SnapMirror 수정"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"
- "스냅미러 쇼"

SnapMirror 활성 동기화를 관리하고 데이터를 보호합니다

ONTAP 일관성 그룹 간에 공통 스냅샷을 만듭니다.

정기적으로 예약된 스냅샷 작업 외에도 운영 SnapMirror 정합성 보장 그룹의 볼륨과 보조 SnapMirror 정합성 보장 그룹의 볼륨 간에 공통을 수동으로 생성할 수 "스냅샷"있습니다.

이 작업에 대해

예약된 스냅샷 생성 간격은 12시간입니다.

시작하기 전에

- SnapMirror 그룹 관계가 동기화되어 있어야 합니다.

단계

1. 일반 스냅샷 생성:

대상 경로 **VS1_DST:/CG/CG_DST**'의 경우, '목적지
> SnapMirror update-destination-path VS1_DST:/CG/CG_DST'

2. 업데이트 진행 상황 모니터링:

```
destination::>snapmirror show -fields newest-snapshot
```

관련 정보

- "스냅미러 쇼"

SnapMirror 활성 동기화 관계에서 **ONTAP** 클러스터의 계획된 장애 조치를 수행합니다**.**

SnapMirror 액티브 동기화 관계에서 ONTAP 클러스터의 계획된 페일오버에서는 운영 및 2차 클러스터의 역할을 전환하여 2차 클러스터가 운영 클러스터에서 페일오버되도록 합니다. 페일오버 중에 보조 클러스터는 클라이언트 작업을 중단하지 않고 로컬에서 입력 및 출력 요청을 처리합니다.

계획된 페일오버를 수행하여 재해 복구 구성의 상태를 테스트하거나 운영 클러스터에 대한 유지 관리를 수행할 수 있습니다.

이 작업에 대해

계획된 페일오버는 보조 클러스터의 관리자가 시작합니다. 이 작업을 수행하려면 운영 및 2차 역할을 전환하여 2차 클러스터가 운영 클러스터에서 대신 수행하게 해야 합니다. 그러면 새로운 운영 클러스터가 클라이언트 작업을 중단하지 않고 로컬에서 입력 및 출력 요청 처리를 시작할 수 있습니다.

시작하기 전에

- SnapMirror 활성 동기화 관계가 동기화되어 있어야 합니다.
- 무중단 운영이 진행 중인 경우에는 계획된 페일오버를 시작할 수 없습니다. 무중단 운영에는 볼륨 이동, 애그리게이트 재배치, 스토리지 페일오버가 포함됩니다.
- ONTAP 중재자는 구성, 연결 및 쿼럼에 있어야 합니다.

단계

ONTAP CLI 또는 System Manager를 사용하여 계획된 페일오버를 수행할 수 있습니다.

시스템 관리자

ONTAP 9.14.1부터 9.8까지 SnapMirror 액티브 동기화는 SnapMirror 비즈니스 연속성(SM-BC)이라고 합니다.

1. System Manager에서 보호 > 개요 > 관계 를 선택합니다.
2. 페일오버할 SnapMirror 활성 동기화 관계를 확인합니다. 이름 옆에 있는 을 선택합니다 … 관계의 이름 옆에 있는 장애 조치 를 선택합니다.
3. 페일오버 상태를 모니터링하려면 를 사용합니다 `snapmirror failover show` ONTAP CLI에서

CLI를 참조하십시오

1. 대상 클러스터에서 페일오버 작업을 시작합니다.

   대상 경로 VS1_DST:/CG/CG_DST'에 대한 오류 수정:::> SnapMirror 페일오버 시작 대상 경로 VS1_DST:/CG/CG_DST

2. 페일오버 진행률을 모니터링합니다.

   대상::> SnapMirror failover show'

3. 페일오버 작업이 완료되면 대상에서 SnapMirror 동기식 보호 관계 상태를 모니터링할 수 있습니다.

   목적지::> SnapMirror 쇼

관련 정보

- "스냅미러 페일오버 쇼"
- "스냅미러 페일오버 시작"
- "스냅미러 쇼"

계획되지 않은 자동 **ONTAP** 클러스터 장애 조치 작업에서 복구

자동 비계획 장애 조치(AUFO) 작업은 기본 클러스터가 다운되거나 격리될 때 발생합니다. ONTAP Mediator는 장애 조치가 발생할 때 이를 감지하고 보조 클러스터에 대한 자동적인 계획되지 않은 장애 조치를 실행합니다. 이 작업은 ONTAP Mediator의 도움을 받아서만 수행됩니다. 보조 클러스터는 기본 클러스터로 전환되어 클라이언트 서비스를 시작합니다. 이 작업은 ONTAP 중재자의 지원을 받아야만 수행됩니다.

예기치 않은 자동 페일오버 후에는 입출력 경로가 손실되지 않도록 호스트 LUN 입출력 경로를 재검색해야 합니다.

계획되지 않은 페일오버 후에 보호 관계를 다시 설정합니다

System Manager 또는 ONTAP CLI를 사용하여 보호 관계를 다시 설정할 수 있습니다.

시스템 관리자

단계

ONTAP 9.14.1부터 9.8까지 SnapMirror 액티브 동기화는 SnapMirror 비즈니스 연속성(SM-BC)이라고 합니다.

1. *보호 > 관계*로 이동하여 관계 상태가 "동기화되지 않음"으로 표시될 때까지 기다립니다.
2. 원래 소스 클러스터에서 작업을 재개하려면 를 ⋮ 클릭하고 * Failover * 를 선택합니다.

CLI를 참조하십시오

를 사용하여 자동 비계획 페일오버 상태를 모니터링할 수 있습니다 `snapmirror failover show` 명령.

예를 들면 다음과 같습니다.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

을 참조하십시오 "EMS 참조" 이벤트 메시지 및 수정 조치에 대해 알아보십시오.

페일오버 후 팬아웃 구성에서 보호를 재개합니다

ONTAP 9.15.1부터 SnapMirror 액티브 동기화는 페일오버 이벤트 후 팬아웃 구간의 자동 재구성을 지원합니다. 비동기 팬아웃 구간은 정합성 보장 그룹 관계 또는 독립 볼륨 관계일 수 있습니다. 자세한 내용은 을 "팬아웃 구성"참조하십시오.

ONTAP 9.14.1 이하를 사용 중이고 SnapMirror 활성 동기화 관계에서 2차 클러스터에서 페일오버가 발생한 경우 SnapMirror 비동기 대상이 비정상 상태가 됩니다. SnapMirror 비동기식 엔드포인트와의 관계를 삭제하고 다시 생성하여 보호를 수동으로 복원해야 합니다.

단계

1. 페일오버 작업이 성공적으로 완료되었는지 확인합니다. '스냅샷 페일오버 표시'입니다
2. SnapMirror 비동기 끝점에서 팬 아웃 끝점을 삭제합니다.
   `snapmirror delete -destination-path` *`destination_path`*
3. 세 번째 사이트에서 새로운 SnapMirror 액티브 동기식 운영 볼륨과 비동기 팬아웃 타겟 볼륨 간에 SnapMirror 비동기식 관계를 생성합니다.
   `snapmirror create -source-path` *`source_path`* `-destination-path` *`destination_path`* `-policy MirrorAllSnapshots -schedule` *`schedule`*

4. 관계 재동기화:
   `snapmirror resync -destination-path destination_path`
5. 관계 상태 및 상태 확인: '스냅샷 표시

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "스냅미러 페일오버 쇼"
- "스냅미러 재동기화"
- "스냅미러 쇼"

ONTAP SnapMirror 활성 동기화 작업 모니터링

다음 SnapMirror 활성 동기화 작업을 모니터링하여 SnapMirror 활성 동기화 구성의 상태를 확인할 수 있습니다.

- ONTAP 중재자
- 계획된 페일오버 작업
- 계획되지 않은 페일오버 작업을 자동으로 수행합니다
- SnapMirror 활성 동기화 가용성

ONTAP 9.15.1부터 System Manager는 두 클러스터의 SnapMirror 활성 동기화 관계 상태를 표시합니다. System Manager의 두 클러스터 중 하나에서 ONTAP 중재자의 상태를 모니터링할 수도 있습니다.

ONTAP 중재자

정상 작동 중에는 ONTAP 중재자 상태가 연결되어야 합니다. 다른 상태에 있는 경우 오류 상태를 나타낼 수 있습니다. 를 검토할 수 있습니다 "EMS(이벤트 관리 시스템) 메시지" 오류 및 적절한 수정 조치를 확인합니다.

계획된 페일오버 작업

'napmirror failover show' 명령을 사용하여 계획된 페일오버 작업의 상태 및 진행률을 모니터링할 수 있습니다. 예를 들면 다음과 같습니다.

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

페일오버 작업이 완료되면 새 대상 클러스터에서 SnapMirror 보호 상태를 모니터링할 수 있습니다. 예를 들면 다음과 같습니다.

```
ClusterA::> snapmirror show
```

을 참조하십시오 "EMS 참조" 이벤트 메시지 및 수정 조치에 대해 알아보십시오.

계획되지 않은 자동 페일오버 중에 를 사용하여 작업 상태를 모니터링할 수 있습니다 `snapmirror failover show` 명령.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
          Source Path: vs1:/cg/scg3
     Destination Path: vs3:/cg/dcg3
      Failover Status: completed
         Error Reason:
             End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

을 참조하십시오 "EMS 참조" 이벤트 메시지 및 수정 조치에 대해 알아보십시오.

SnapMirror 활성 동기화 가용성

운영 클러스터, 2차 클러스터 또는 둘 다에서 일련의 명령을 사용하여 SnapMirror 액티브 동기화 관계의 가용성을 확인할 수 있습니다.

사용하는 명령에는 1차 및 2차 클러스터 모두에 대한 'napmirror 중재자 표시' 명령을 사용하여 연결 및 쿼럼 상태, 'napmirror show' 명령 및 'volume show' 명령을 확인할 수 있습니다. 예를 들면 다음과 같습니다.

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored Insync -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored Insync   -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                      Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                       No-consensus
```

관련 정보

- "스냅미러 페일오버 쇼"
- "스냅미러 페일오버 시작"
- "스냅미러 중재자 쇼"

ONTAP 일관성 그룹에 볼륨 추가 또는 제거

애플리케이션 워크로드의 요구사항이 변경됨에 따라 비즈니스 연속성을 보장하기 위해 일관성 그룹에서 볼륨을 추가하거나 제거해야 할 수 있습니다. 활성 SnapMirror 활성 동기화 관계에서

볼륨을 추가 및 제거하는 프로세스는 사용 중인 ONTAP의 버전에 따라 다릅니다.

대부분의 경우 이 프로세스는 운영 중단을 야기하여 SnapMirror 관계를 삭제하고 일관성 그룹을 수정한 다음 보호를 재개해야 합니다. ONTAP 9.13.1부터 활성 SnapMirror 관계가 있는 일관성 그룹에 볼륨을 추가하는 것은 무중단 작업입니다.

이 작업에 대해

- ONTAP 9.9.1에서는 ONTAP CLI를 사용하여 일관성 그룹에 볼륨을 추가하거나 제거할 수 있습니다.
- ONTAP 9.10.1.1부터는 를 관리하는 것이 좋습니다 "정합성 보장 그룹" System Manager 또는 ONTAP REST API를 통해

  볼륨을 추가하거나 제거하여 일관성 그룹의 구성을 변경하려면 먼저 원래 관계를 삭제한 다음 새 구성도를 사용하여 일관성 그룹을 다시 생성해야 합니다.

- ONTAP 9.13.1부터 소스 또는 대상에서 활성 SnapMirror 관계가 있는 일관성 그룹에 중단 없이 볼륨을 추가할 수 있습니다. 이 작업은 NVMe 프로토콜에서는 지원되지 않습니다.

  볼륨 제거는 중단을 야기하는 작업입니다. 볼륨을 제거하기 전에 SnapMirror 관계를 삭제해야 합니다.

ONTAP 9.9.1-9.13.0

시작하기 전에

- 에 있는 동안에는 일관성 그룹을 수정할 수 없습니다 `InSync` 상태.
- 대상 볼륨은 DP 유형이어야 합니다.
- 정합성 보장 그룹을 확장하기 위해 추가하는 새 볼륨에는 소스 볼륨과 대상 볼륨 사이에 공통 스냅샷 쌍이 있어야 합니다.

단계

두 볼륨 매핑에 표시된 예는 다음과 같습니다. `vol_src1 ←→ vol_dst1` 및 `vol_src2 ←→ vol_dst2`정합성 보장 그룹 관계에서 최종 지점 간의 관계를 나타냅니다 `vs1_src:/cg/cg_src` 및 `vs1_dst:/cg/cg_dst`.

1. 소스 및 대상 클러스터에서 명령을 사용하여 소스와 대상 클러스터 간에 공통 스냅샷이 있는지 확인합니다 `snapshot show -vserver` *`svm_name`* `-volume` *`volume_name`* `-snapshot` *`snapmirror`*

   'source::> snapshot show -vserver vs1_src -volume vol_src3 -snapshot SnapMirror *'

   대상::> snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot snapmirror *

2. 공통 스냅샷이 없는 경우 FlexVol SnapMirror 관계를 생성하고 초기화합니다.

   대상 경로 VS1_Dst:vol_dst3'이라는 메시지가 나타납니다

3. 정합성 보장 그룹 관계를 삭제합니다.

   대상 경로 VS1_DST:/CG/CG_DST'의 경우, "대상 경로::::> SnapMirror delete-destination-path VS1_DST:/CG/CG_DST"

4. 소스 SnapMirror 관계를 해제하고 공통 스냅샷을 보존합니다.

   'source::> snapmirror release-relationship-info-only true-destination-path vs1_dst:vol_dst3'

5. LUN 매핑을 해제하고 기존 일관성 그룹 관계를 삭제합니다.

   대상::> LUN 매핑 삭제 - vserver vs1_dst -path <lun_path> -igroup <igroup_name>'

   > 대상 LUN은 매핑 해제되지만 운영 복제본의 LUN은 계속해서 호스트 입출력을 처리합니다

   대상 경로 VS1_DST:/CG/CG_DST'의 경우, "대상 경로::::> SnapMirror delete-destination-path VS1_DST:/CG/CG_DST"

   '소스::> SnapMirror release-destination-path vs1_dst:/cg/cg_dst-relationship-info-only true'

6. **ONTAP 9.10.1~9.13.0**을 사용하는 경우 소스에서 정합성 보장 그룹을 삭제하고 올바른 구성으로 다시 만드십시오. 의 단계를 따르"일관성 그룹을 삭제합니다" 십시오"단일 일관성 그룹을 구성합니다". ONTAP ONTAP 는 없습니다.

   ONTAP 9.9.1을 사용하는 경우 다음 단계로 건너뜁니다.

7. 새 컴포지션을 사용하여 대상에 새 일관성 그룹을 생성합니다.

   대상 경로 VS1_Dst:/CG/CG_src-destination-path vs1_dst:/cg/cg_dst-item-mapping vol_src1:@vol_dst1, vol_src2:@vol_dst2, vol_src3:@vol_dst3

8. 제로급 RTO 정합성 보장 그룹 관계를 재동기화하여 동기화되도록 합니다.

   대상 경로 VS1_DST:/CG/CG_DST'를 다시 동기화하십시오

9. 5단계에서 매핑되지 않은 LUN을 다시 매핑합니다.

   ```
   destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
   ```

10. 호스트 LUN 입출력 경로를 재검색하여 LUN에 대한 모든 경로를 복구합니다.

ONTAP 9.13.1 이상

ONTAP 9.13.1부터 활성 SnapMirror 활성 동기화 관계가 있는 일관성 그룹에 볼륨을 중단 없이 추가할 수 있습니다. SnapMirror 액티브 동기화에서는 소스 또는 대상 모두에서 볼륨을 추가할 수 있습니다.

ONTAP 9.14.1부터 9.8까지 SnapMirror 액티브 동기화는 SnapMirror 비즈니스 연속성(SM-BC)이라고 합니다.

소스 정합성 보장 그룹에서 볼륨을 추가하는 방법에 대한 자세한 내용은 를 참조하십시오 일관성 그룹 수정.

타겟 클러스터에서 볼륨을 추가합니다

1. 대상 클러스터에서 보호 > 관계를 선택합니다.
2. 볼륨을 추가할 SnapMirror 구성을 찾습니다. 를 선택한 다음 확장 을 선택합니다 ⋮ .
3. 정합성 보장 그룹에 볼륨을 추가할 볼륨 관계를 선택합니다
4. **Expand**(확장**)를 선택합니다.

관련 정보

- "SnapMirror 삭제"
- "SnapMirror 초기화"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"

ONTAP SnapMirror Active Sync로 업그레이드하고 되돌리기

SnapMirror 액티브 동기화는 ONTAP 9.9.1부터 지원됩니다. ONTAP 클러스터 또는 컨트롤러의 업그레이드와 되돌리기는 업그레이드하거나 되돌리려는 ONTAP 버전에 따라 SnapMirror 활성 동기화 관계에 영향을 미칩니다.

클러스터를 새로 고칩니다

ONTAP 9.16.1부터 SnapMirror 액티브 동기화는 대칭 액티브/액티브 구성의 4노드 클러스터를 지원합니다. 4노드 클러스터를 사용하여 컨트롤러와 스토리지를 업그레이드할 수 있습니다.

시작하기 전에

- 를 검토합니다. "4노드 클러스터의 요구사항"
- 기술 업데이트 프로세스 중에 비대칭 구성을 만들 수 있지만 새로 고침을 완료한 후에는 대칭 구성으로 돌아가야 합니다.
- 이러한 지침은 50개 이하의 일관성 그룹과 400개 이하의 볼륨 엔드포인트를 가진 기존 4노드 구성에 적용됩니다.

단계

1. "모든 SnapMirror 활성 동기화 볼륨을 _single_high-availability(HA) 쌍으로 이동합니다"..
2. "클러스터에서 사용되지 않는 노드를 제거합니다"..
3. "클러스터에 새 노드를 추가합니다"..
4. "모든 볼륨을 이동합니다" 새 노드로 이동할 수 있습니다.
5. "클러스터에서 사용되지 않는 노드를 제거합니다" 그런 다음 교체합니다"새로운 노드로".

SnapMirror 활성 동기화로 ONTAP 업그레이드

SnapMirror 액티브 동기화를 사용하려면 소스 및 대상 클러스터의 모든 노드에서 ONTAP 9.9.1 이상을 실행해야 합니다.

활성 SnapMirror 활성 동기화 관계를 사용하여 ONTAP를 업그레이드할 때는 를 사용해야 합니다 자동 무중단 업그레이드(ANDU). ANDU를 사용하면 SnapMirror 활성 동기화 관계가 동기화되고 업그레이드 프로세스 중에 정상 상태가 됩니다.

ONTAP 업그레이드를 위해 SnapMirror 액티브 동기화 배포를 준비하기 위한 구성 단계가 없습니다. 그러나 업그레이드 전후에 다음 사항을 확인하는 것이 좋습니다.

- SnapMirror 활성 동기화 관계가 동기화됩니다.
- 이벤트 로그에 SnapMirror와 관련된 오류가 없습니다.
- 중재자는 온라인 상태이며 두 클러스터에서 모두 정상입니다.
- 모든 호스트는 LUN을 보호하기 위해 모든 경로를 올바르게 볼 수 있습니다.

ONTAP 9.9.1 또는 9.9.1에서 ONTAP 9.10.1 이상으로 클러스터를 업그레이드하면 ONTAP에서 새로운 을 생성합니다 정합성 보장 그룹 소스 및 대상 클러스터 모두에서 System Manager를 사용하여 SnapMirror 활성 동기화 관계를 구성할 수 있습니다.

를 클릭합니다 `snapmirror quiesce` 및 `snampirror resume` SnapMirror 활성 동기화에서는 명령이 지원되지 않습니다.

ONTAP 9.10.1에서 ONTAP 9.9.1로 되돌립니다

관계를 9.10.1에서 9.9.1로 되돌리려면 SnapMirror 활성 동기화 관계를 삭제한 다음 9.10.1 일관성 그룹 인스턴스를 따라야 합니다. 활성 SnapMirror 활성 동기화 관계가 있는 일관성 그룹은 삭제할 수 없습니다. 9.9.1 이전 버전에서 다른 스마트 컨테이너 또는 엔터프라이즈 앱과 이전에 연결된 9.10.1로 업그레이드된 FlexVol 볼륨은 더 이상 복원 시 연결되지 않습니다. 일관성 그룹을 삭제해도 구성 볼륨 또는 볼륨 세부 스냅샷은 삭제되지 않습니다. 을 참조하십시오 "일관성 그룹을 삭제합니다" ONTAP 9.10.1 이상에서 이 작업에 대한 자세한 내용을 확인하십시오.

ONTAP 9.9.1 이전 릴리즈보다 SnapMirror 활성 동기화는 혼합 ONTAP 클러스터에 지원되지 않습니다.

ONTAP 9.1.1에서 이전 버전의 ONTAP으로 되돌리는 경우 다음에 대해 알아야 합니다.

- 클러스터가 SnapMirror 활성 동기화 대상을 호스팅하는 경우 관계가 끊어져 삭제될 때까지 ONTAP 9.8 이전 버전으로 되돌릴 수 없습니다.
- 클러스터가 SnapMirror 액티브 동기화 소스를 호스팅하는 경우 관계가 해제될 때까지 ONTAP 9.8 이하로 되돌릴 수 없습니다.
- 사용자가 생성한 모든 맞춤형 SnapMirror 활성 동기화 정책을 삭제한 후 ONTAP 9.8 이하로 되돌려야 합니다.

이러한 요구 사항을 충족하려면 를 참조하십시오 "SnapMirror 활성 동기화 구성을 제거합니다".

단계

1. SnapMirror 활성 동기화 관계의 클러스터 중 하나에서 다음 명령을 입력하여 되돌릴 준비가 되었는지 확인합니다.

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   ```

   다음 샘플 출력에서는 정리 명령으로 되돌릴 준비가 되지 않은 클러스터를 보여 줍니다.

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   Error: command failed: The revert check phase failed. The following
   issues must be resolved before revert can be completed. Bring the data
   LIFs down on running vservers. Command to list the running vservers:
   vserver show -admin-state running Command to list the data LIFs that are
   up: network interface show -role data -status-admin up Command to bring
   all data LIFs down: network interface modify {-role data} -status-admin
   down
   Disable snapshot policies.
       Command to list snapshot policies: "snapshot policy show".
       Command to disable snapshot policies: "snapshot policy modify
   -vserver
      * -enabled false"

      Break off the initialized online data-protection (DP) volumes and
   delete
      Uninitialized online data-protection (DP) volumes present on the
   local
      node.
       Command to list all online data-protection volumes on the local
   node:
      volume show -type DP -state online -node <local-node-name>
       Before breaking off the initialized online data-protection volumes,
      quiesce and abort transfers on associated SnapMirror relationships
   and
   ```

```
   wait for the Relationship Status to be Quiesced.
    Command to quiesce a SnapMirror relationship: snapmirror quiesce
    Command to abort transfers on a SnapMirror relationship: snapmirror
   abort
    Command to see if the Relationship Status of a SnapMirror
relationship
   is Quiesced: snapmirror show
    Command to break off a data-protection volume: snapmirror break
    Command to break off a data-protection volume which is the
destination
   of a SnapMirror relationship with a policy of type "vault":
snapmirror
   break -delete-snapshots
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.9.1"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
   The command to delete a policy is :
    snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

2. 복원 검사의 요구 사항을 충족하면 을 참조하십시오 "ONTAP를 되돌립니다".

관련 정보

- "네트워크 인터페이스"
- "SnapMirror가 깨졌습니다"
- "스냅미러 정책 삭제"
- "스냅미러 정책 보기"
- "SnapMirror 중지"
- "스냅미러 쇼"

더 이상 제로 RTO SnapMirror 동기식 보호가 필요하지 않은 경우 SnapMirror 액티브 동기화 관계를 삭제할 수 있습니다.

비대칭 구성을 제거합니다

- SnapMirror 액티브 동기화 관계를 삭제하기 전에 대상 클러스터의 모든 LUN을 매핑 해제해야 합니다.
- LUN이 매핑 해제되었고 호스트가 다시 스캔되면 SCSI 타겟은 LUN 인벤토리가 변경되었음을 호스트에 알립니다. 제로 RTO 2차 볼륨의 기존 LUN은 제로 RTO 관계가 삭제된 후 새 ID를 반영하도록 변경됩니다. 호스트는 소스 볼륨 LUN과 관계가 없는 새 LUN으로 보조 볼륨 LUN을 검색합니다.
- 관계가 삭제된 후 보조 볼륨은 DP 볼륨으로 유지됩니다. 을(를) 실행할 수 있습니다 `snapmirror break` 읽기/쓰기로 변환하는 명령입니다.
- 관계가 반대로 설정되지 않은 경우 페일오버된 상태에서는 관계를 삭제할 수 없습니다.

단계

1. 보조 클러스터에서 소스 끝점과 대상 끝점 간의 SnapMirror 활성 동기화 일관성 그룹 관계를 제거합니다.

   대상 경로 VS1_DST:/CG/CG_DST'의 경우, "대상 경로:::> SnapMirror delete-destination-path VS1_DST:/CG/CG_DST"

2. 운영 클러스터에서 정합성 보장 그룹 관계 및 관계에 대해 생성된 스냅샷을 해제합니다.

   ```
   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   ```

3. 호스트 재검색을 수행하여 LUN 인벤토리를 업데이트합니다.
4. ONTAP 9.10.1부터 SnapMirror 관계를 삭제해도 일관성 그룹은 삭제되지 않습니다. 일관성 그룹을 삭제하려면 시스템 관리자 또는 ONTAP REST API를 사용해야 합니다. 을 참조하십시오 일관성 그룹을 삭제합니다 를 참조하십시오.

iSCSI 또는 **FC** 대칭 활성/활성 구성 제거

System Manager 또는 ONTAP CLI를 사용하여 대칭 구성을 제거할 수 있습니다. 두 인터페이스 모두에서 에 대한 단계가 다릅니다 균일 및 비균일 설정.

시스템 관리자

균일 설정에 대한 단계

1. 운영 사이트에서 igroup에서 원격 호스트를 제거하고 복제를 종료합니다.
   a. **Hosts**> * SAN Initiator Groups * 로 이동합니다.
   b. 수정할 igroup을 선택한 다음 편집 을 선택합니다.
   c. 원격 이니시에이터를 제거하고 igroup 복제를 종료합니다. 저장을 선택합니다.
2. 보조 사이트에서 LUN 매핑을 해제하여 복제된 관계를 삭제합니다.
   a. **Hosts**> **SAN Initiator Groups** 로 이동합니다.
   b. SnapMirror 관계가 있는 igroup을 선택한 다음 삭제 를 선택합니다.
   c. 대화 상자에서 연결된 **LUN** 매핑 해제 상자를 선택한 다음 삭제 를 선택합니다.
   d. 보호> 관계 로 이동합니다.
   e. SnapMirror 활성 동기화 관계를 선택한 다음 릴리즈 를 선택하여 관계를 삭제합니다.

비균일 설정에 대한 단계

1. 운영 사이트에서 igroup에서 원격 호스트를 제거하고 복제를 종료합니다.
   a. **Hosts**> * SAN Initiator Groups * 로 이동합니다.
   b. 수정할 igroup을 선택한 다음 편집 을 선택합니다.
   c. 원격 이니시에이터를 제거하고 igroup 복제를 종료합니다. 저장을 선택합니다.
2. 2차 사이트에서 SnapMirror 활성 동기화 관계를 제거합니다.
   a. 보호> 관계 로 이동합니다.
   b. SnapMirror 활성 동기화 관계를 선택한 다음 릴리즈 를 선택하여 관계를 삭제합니다.

CLI를 참조하십시오

균일 설정에 대한 단계

1. 모든 VM 워크로드를 SnapMirror 활성 동기화의 소스 클러스터로 호스트 로컬 이동합니다.
2. 소스 클러스터에서 igroup에서 이니시에이터를 제거하고 igroup 구성을 수정하여 igroup 복제를 종료합니다.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -initiator <host2>
SiteA::> igroup modify -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -replication-peer "-"
```

3. 2차 사이트에서 LUN 매핑을 삭제하고 igroup 구성을 제거합니다.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. 2차 사이트에서 SnapMirror 활성 동기화 관계를 삭제합니다.

```
SiteB::> snapmirror delete -destination-path destination_path
```

5. 기본 사이트에서 기본 사이트의 SnapMirror 활성 동기화 관계를 해제합니다.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. 경로를 다시 검색하여 호스트에서 로컬 경로만 사용할 수 있는지 확인합니다.

비균일 설정에 대한 단계

1. 모든 VM 워크로드를 SnapMirror 활성 동기화의 소스 클러스터로 호스트 로컬 이동합니다.
2. 소스 클러스터의 이니시에이터를 igroup에서 제거합니다.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -initiator
<host2>
```

3. 2차 사이트에서 LUN 매핑을 삭제하고 igroup 구성을 제거합니다.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. 2차 사이트에서 SnapMirror 활성 동기화 관계를 삭제합니다.

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. 기본 사이트에서 기본 사이트의 SnapMirror 활성 동기화 관계를 해제합니다.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. 경로를 다시 검색하여 호스트에서 로컬 경로만 사용할 수 있는지 확인합니다.

NVMe 대칭 활성/활성 구성 제거

시스템 관리자

단계

1. 소스 클러스터에서 *보호 > 복제*로 이동합니다.
2. 제거하려는 관계를 찾아 선택하세요. ⋮ *삭제*를 선택하세요.

CLI를 참조하십시오

1. 대상 클러스터에서 SnapMirror 활성 동기화 관계를 삭제합니다.

   ```
   snapmirror delete -destination-path <destination_path> -unmap-namespace
   true
   ```

   예:

   ```
   DST::> snapmirror delete -destination-path vs1:/cg/cg_dst_1 -force
   true
   ```

   하위 시스템과 해당 네임스페이스가 보조 클러스터에서 제거됩니다.

2. 소스 클러스터에서 기본 사이트의 SnapMirror 활성 동기화 관계를 해제합니다.

   ```
   snapmirror release -destination-path <destination_path>
   ```

   예:

   ```
   SRC::> snapmirror release -destination-path vs1:/cg/cg_dst_1
   ```

3. 경로를 다시 검색하여 호스트에서 로컬 경로만 사용할 수 있는지 확인합니다.

관련 정보

- "SnapMirror가 깨졌습니다"
- "SnapMirror 삭제"
- "SnapMirror 릴리즈"

ONTAP Mediator 또는 **ONTAP Cloud Mediator** 제거

ONTAP 클러스터에서 기존 ONTAP Mediator 또는 ONTAP Cloud Mediator 구성을 제거하려면 다음을 사용할 수 있습니다. `snapmirror mediator remove` 예 를 들어, 한 번에 한 가지 유형의 Mediator만 사용할 수 있으므로 다른 인스턴스를 설치하기 전에 기존 인스턴스를 제거해야 합니다.

단계

다음 단계 중 하나를 완료하여 ONTAP Mediator 또는 ONTAP Cloud Mediator를 제거할 수 있습니다.

ONTAP 중재자

1. ONTAP 중재자 제거:

   ```
   snapmirror mediator remove -mediator-address <address> -peer-cluster
   <peerClusterName>
   ```

   예:

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer
   -cluster cluster_xyz
   ```

ONTAP 클라우드 중재자

1. ONTAP Cloud Mediator 제거:

   ```
   snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud
   ```

   예:

   ```
   snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
   ```

관련 정보

- "스냅미러 중재자 제거"

문제 해결

ONTAP SnapMirror 삭제 작업이 테이크오버 상태에서 실패합니다**.**

다음 정보를 사용하십시오. `snapmirror delete` SnapMirror 활성 동기화 일관성 그룹 관계가 인수 상태인 경우 명령이 실패합니다.

문제:

ONTAP 9.9.1이 클러스터에 설치되면 다음을 실행합니다. `snapmirror delete` SnapMirror 활성 동기화 일관성 그룹 관계가 인수 상태인 경우 명령이 실패합니다.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

해결 방법

SnapMirror 활성 동기화 관계에 있는 노드가 인수 상태인 경우 "-force" 옵션을 true로 설정하여 SnapMirror 삭제 및 해제 작업을 수행합니다.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
         Consistency Group might not be made writable, deletable, or
modifiable
         after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

관련 정보

- "SnapMirror 삭제"

ONTAP SnapMirror 관계 생성 및 일관성 그룹 초기화 실패

SnapMirror 관계 생성 및 일관성 그룹 초기화에 실패하는 경우 다음 정보를 사용합니다.

문제:

SnapMirror 관계 및 일관성 그룹 초기화가 실패합니다.

솔루션:

클러스터당 일관성 그룹 제한을 초과하지 않았는지 확인합니다. SnapMirror 활성 동기화의 일관성 그룹 제한은 플랫폼과는 독립적이며 ONTAP 버전에 따라 다릅니다. 을 참조하십시오 "개체 제한" ONTAP 버전 관련 지침을 참조하십시오.

오류:

정합성 보장 그룹의 초기화가 중단된 경우 ONTAP REST API, System Manager 또는 'show-Expand' 명령을 사용하여 정합성 보장 그룹 초기화의 상태를 확인하십시오.

ONTAP 9.14.1부터 9.8까지 SnapMirror 액티브 동기화는 SnapMirror 비즈니스 연속성(SM-BC)이라고 합니다.

솔루션:

일관성 그룹이 초기화되지 않은 경우 SnapMirror 활성 동기화 관계를 제거하고 일관성 그룹을 삭제한 다음 관계를 다시 생성한 후 초기화합니다. 이 워크플로는 사용 중인 ONTAP 버전에 따라 다릅니다.

ONTAP 9.9.9.1을 사용하는 경우	ONTAP 9.10.1 이상을 사용하는 경우

1. "SnapMirror 활성 동기화 구성을 제거합니다" 2. "일관성 그룹 관계를 생성한 다음 일관성 그룹 관계를 초기화합니다"	1. 보호 > 관계 * 에서 일관성 그룹에서 SnapMirror 활성 동기화 관계를 찾습니다. ⋮를 선택한 다음 * Delete * 를 선택하여 SnapMirror 활성 동기화 관계를 제거합니다. 2. "일관성 그룹을 삭제합니다" 3. "일관성 그룹을 구성합니다"

계획된 **ONTAP** 클러스터 장애 조치가 실패했습니다.

계획된 장애 조치 작업이 실패한 경우 다음 정보를 사용하세요.

문제:

'napmirror failover start' 명령을 실행한 후 'napmirror failover show' 명령의 출력에 무중단 작업이 진행 중임을 나타내는 메시지가 표시됩니다.

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                                08:35:04
08:35:04
```

원인:

볼륨 이동, 애그리게이트 재배치, 스토리지 페일오버 등 무중단 운영이 진행 중인 경우에는 계획된 페일오버를 시작할 수 없습니다.

솔루션:

무중단 운영이 완료될 때까지 기다린 후 페일오버 작업을 다시 시도하십시오.

관련 정보

- "스냅미러 페일오버 쇼"
- "스냅미러 페일오버 시작"

ONTAP Mediator 또는 **ONTAP Cloud Mediator**에 연결할 수 없거나 **Mediator** 쿼럼 상태가 거짓입니다.

ONTAP Mediator 또는 ONTAP Cloud Mediator에 접근할 수 없거나 Mediator 쿼럼 상태가 거짓인 경우 다음 정보를 사용하세요.

문제:

실행 후 `snapmirror failover start` 명령, 출력 `snapmirror failover show` 명령은 ONTAP Mediator 또는 ONTAP Cloud Mediator가 구성되지 않았음을 나타내는 메시지를 표시합니다.

보다 "활성 동기화에 대해 ONTAP 중재자 및 클러스터를 구성합니다" 또는 "SnapMirror Active Sync를 위한 ONTAP Cloud Mediator 구성" .

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

원인:

중재자가 구성되지 않았거나 네트워크 연결 문제가 있습니다.

솔루션:

ONTAP 중재자가 구성되지 않은 경우 SnapMirror 활성 동기화 관계를 설정하기 전에 ONTAP 중재자를 구성해야 합니다. 네트워크 연결 문제를 해결합니다. SnapMirror 중재자 show 명령을 사용하여 중재자가 연결되어 있고 소스 사이트와 대상 사이트 모두에서 쿼럼 상태가 true 인지 확인합니다. 자세한 내용은 을 참조하십시오 "ONTAP 중재자를 구성합니다".

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

관련 정보

- "스냅미러 페일오버 쇼"
- "스냅미러 페일오버 시작"
- "스냅미러 중재자 쇼"

ONTAP Cloud Mediator에 접속 가능하지만 응답이 느립니다**.**

ONTAP Cloud Meditor가 ping 지연 시간이 권장 지연 시간보다 높다는 오류로 인해 실패하는 경우 다음 정보를 사용하세요.

문제:

시스템 관리자: Cloud Mediator 서비스에 접속할 수는 있지만 응답 속도가 느립니다.

CLI: `mediator add` 명령이 다음 오류로 인해 실패합니다.
`Error: command failed: The ping latency of the BlueXP cloud server is <x> ms which is higher than twice the recommended latency of 200 ms.`

원인:

클러스터가 NetApp 콘솔 클라우드 근처에 위치하지 않았거나 네트워크 경로 병목 현상이 있을 수 있습니다.

솔루션:

- NetApp Console 클라우드(미국 동부)의 지리적 위치와 근접성을 확인하세요.
- 네트워크 경로를 최적화하거나 병목 현상을 해결합니다.
- 네트워크 도구를 사용하여 왕복 시간(RTT)을 측정하고 지연 시간을 권장 한도 내로 줄입니다.
- HTTP 프록시를 사용하여 성능을 향상시키세요.

보다 "SnapMirror Active Sync를 위한 ONTAP Cloud Mediator 및 클러스터 구성" .

사이트 **B**에서 예기치 않은 자동 페일오버가 트리거되지 않습니다

사이트 A에서 장애가 발생해도 사이트 B에서 계획되지 않은 장애 조치가 발생하지 않는 경우 다음 정보를 사용합니다.

문제:

사이트 A에서 장애가 발생해도 사이트 B에서 계획되지 않은 페일오버가 트리거되지 않습니다

가능한 원인 **#1:**

ONTAP Mediator 또는 ONTAP Cloud Mediator가 구성되지 않았습니다. 이것이 원인인지 확인하려면 다음을 실행하세요. `snapmirror mediator show` 사이트 B 클러스터에 대한 명령입니다.

```
Cluster2::> snapmirror mediator show
This table is currently empty.
```

이 예는 Mediator가 사이트 B에 구성되지 않았음을 나타냅니다.

솔루션:

두 클러스터 모두에 Mediator가 구성되어 있고, 상태가 연결됨이고, 쿼럼이 True로 설정되어 있는지 확인하세요.

가능한 원인 **#2:**

SnapMirror 일관성 그룹이 동기화되지 않았습니다. 이 문제가 원인인지 확인하려면 이벤트 로그를 보고 사이트 장애 발생 시 정합성 보장 그룹이 동기화되어 있는지 확인합니다.

```
cluster::> event log show -event *out.of.sync*

Time                Node             Severity      Event
------------------- ---------------- -------------
---------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

솔루션:

사이트 B에서 강제 대체 작동을 수행하려면 다음 단계를 완료합니다

1. 사이트 B에서 정합성 보장 그룹에 속한 모든 LUN 매핑을 해제합니다
2. "강제" 옵션을 사용하여 SnapMirror 일관성 그룹 관계를 삭제합니다.
3. 정합성 보장 그룹 구성 볼륨의 '스냅샷 중단' 명령을 입력하여 볼륨을 DP에서 R/W로 변환한 후 사이트 B에서 입출력을 활성화합니다
4. 사이트 A 노드를 부팅하여 사이트 B에서 사이트 A로 RTO 관계가 0이 되도록 합니다
5. 사이트 A에서 정합성 보장 그룹을 해제하여 `relationship-info-only` 공통 스냅샷을 유지하고 정합성 보장 그룹에 속한 LUN의 매핑을 해제합니다.
6. Sync 정책 또는 Async 정책을 사용하여 볼륨 레벨 관계를 설정하여 사이트 A의 볼륨을 R/W에서 DP로 변환합니다.
7. 관계를 동기화하기 위해 '스냅샷 재동기화'를 실행합니다.
8. 사이트 A의 동기화 정책과 SnapMirror 관계를 삭제합니다
9. 사이트 B에서 'lationship-info-only true'를 사용하여 동기화 정책과 SnapMirror 관계를 해제합니다
10. 사이트 B에서 사이트 A로 일관성 그룹 관계를 생성합니다
11. 사이트 A에서 일관성 그룹 재동기화를 수행한 다음 일관성 그룹이 동기화 중인지 확인합니다.
12. 호스트 LUN 입출력 경로를 재검색하여 LUN에 대한 모든 경로를 복구합니다.

관련 정보

- "SnapMirror가 깨졌습니다"
- "스냅미러 중재자 쇼"
- "스냅미러 재동기화"

사이트 **B**와 **ONTAP Mediator** 간의 링크가 끊어지고 사이트 **A**가 끊어졌습니다**.**

ONTAP Mediator 또는 ONTAP Cloud Mediator의 연결을 확인하려면 다음을 사용하세요. `snapmirror mediator show` 명령입니다. 연결 상태가 "접근 불가"이고 사이트 B가 사이트 A에 접속할 수 없는 경우, 아래와 비슷한 출력이 표시됩니다. 해결 방법에 따라 연결을 복원하세요.

예:

ONTAP Cloud Mediator 출력 `snapmirror mediator show` 명령을 사용합니다.

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster    Connection Status Quorum Status Type
---------------- ---------------- ----------------- ------------- -------
0.0.0.0          C1_cluster       unreachable       true          cloud
```

ONTAP Mediator 출력 `snapmirror mediator show` 명령을 사용합니다.

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.237.86.17     C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

해결 방법

사이트 B에서 입출력을 사용하도록 페일오버를 강제 실행한 다음 사이트 B에서 사이트 A로 RTO 관계를 0으로 설정합니다 사이트 B에서 강제 대체 작동을 수행하려면 다음 단계를 완료합니다

1. 사이트 B에서 일관성 그룹에 속한 모든 LUN의 매핑을 해제합니다. 이 작업은 실패하므로 먼저 igroup을 수정하여 복제 피어 SVM을 제거한 다음 LUN 맵을 삭제해야 합니다.

예:

```
C1_cluster::> lun mapping show
Vserver    Path                                      Igroup   LUN ID
Protocol
---------- ----------------------------------------  -------  ------
--------
vs0        /vol/cg1_lun/lun_1                        igroup1       0
mixed
vs0        /vol/cg1_lun/lun_2                        igroup1       1
mixed
2 entries were displayed.

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_5 -igroup igroup1
Error: command failed: The peer cluster is unreachable and a SnapMirror
       Mediator is not configured. The configuration is locked for
replicated
       objects in this Vserver peer relationship on both clusters. The
only
       supported configuration change is to manually disable replication
on
       both sides of the relationship, after which configuration changes
are
       supported.
C1_cluster::> igroup modify -igroup igroup1 -replication-peer -

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_1 -igroup igroup1

C1_cluster::> lun mapping show
Vserver    Path                                      Igroup   LUN ID
Protocol
---------- ----------------------------------------  -------  ------
--------
vs0        /vol/cg1_lun/lun_2                        igroup1       1
mixed
1 entries were displayed.
```

1. 강제 옵션을 사용하여 SnapMirror 일관성 그룹 관계를 삭제합니다.
2. SnapMirror break 명령을 입력합니다 (`snapmirror break -destination_path` *svm*`:_volume_`)
   정합성 보장 그룹 구성 볼륨에서 볼륨을 DP에서 RW로 변환하여 사이트 B의 입출력을 활성화합니다

   일관성 그룹의 각 관계에 대해 SnapMirror break 명령을 실행해야 합니다. 예를 들어, 일관성 그룹에 볼륨이 3개인 경우 각 볼륨에 대해 명령을 실행합니다.
3. 사이트 A 노드를 부팅하여 사이트 B에서 사이트 A로 RTO 관계가 0이 되도록 합니다
4. 사이트 A에서 relationship-info-only를 사용하여 정합성 보장 그룹을 해제하여 공통 스냅샷을 유지하고 정합성 보장 그룹에 속하는 LUN의 매핑을 해제합니다.

5. 동기화 정책 또는 비동기 정책을 사용하여 볼륨 수준 관계를 설정하여 사이트 A의 볼륨을 RW에서 DP로 변환합니다.
6. 를 발행합니다 `snapmirror resync` 관계를 동기화하는 명령입니다.
7. 사이트 A에서 동기화 정책이 적용된 SnapMirror 관계를 삭제합니다
8. 사이트 B에서 relationship-info만 true를 사용하여 동기 정책과 SnapMirror 관계를 해제합니다
9. 사이트 B와 사이트 A 간의 정합성 보장 그룹 관계를 생성합니다
10. 소스 클러스터에서 정합성 보장 그룹을 다시 동기화합니다. 정합성 보장 그룹 상태가 동기화되어 있는지 확인합니다.
11. 호스트 LUN 입출력 경로를 다시 검색하여 LUN에 대한 모든 경로를 복구합니다.

관련 정보

- "SnapMirror가 깨졌습니다"
- "스냅미러 중재자 쇼"
- "스냅미러 재동기화"
- "스냅미러 쇼"

사이트 **A**와 **ONTAP Mediator** 간의 링크가 다운되고 사이트 **B**가 다운되었습니다**.**

SnapMirror 액티브 동기화를 사용할 경우 ONTAP 중재자 또는 피어링된 클러스터 간에 연결이 끊어질 수 있습니다. SnapMirror 활성 동기화 관계의 여러 부분에 대한 연결, 가용성 및 합의 상태를 확인한 다음 강제로 연결을 다시 시작하여 문제를 진단할 수 있습니다.

확인할 사항	**CLI** 명령	표시기
사이트 A의 중재자	스냅미러 중재자 쇼	연결 상태는 로 표시됩니다 `unreachable`
사이트 B 연결	클러스터 피어 쇼	사용 가능 여부는 로 표시됩니다 `unavailable`
SnapMirror 활성 동기화 볼륨의 합의 상태입니다	'volume show_volume_name_-fields smbc-Consensus'	를 클릭합니다 `sm-bc consensus` 필드가 표시됩니다 `Awaiting-consensus`

이 문제를 진단하고 해결하는 방법에 대한 추가 정보는 다음을 참조하십시오."NetApp 기술 자료: SnapMirror Active Sync를 사용할 때 사이트 A와 Mediator 간의 링크가 끊어지고 사이트 B가 끊어짐" .

관련 정보

- "클러스터 피어 쇼"
- "스냅미러 중재자 쇼"

대상 볼륨에 펜스가 설정된 경우 **ONTAP SnapMirror** 삭제 작업이 실패합니다**.**

대상 볼륨에 리디렉션 펜스가 설정되어 있는 경우 SnapMirror 삭제 작업이 실패하면 다음 정보를 사용합니다.

문제:

대상 볼륨에 리디렉션 펜스 세트가 있으면 SnapMirror 삭제 작업이 실패합니다.

해결 방법

다음 작업을 수행하여 리디렉션을 재시도하고 대상 볼륨에서 Fence를 제거합니다.

- SnapMirror 재동기화
- SnapMirror 업데이트

ONTAP 기본이 다운되면 볼륨 이동 작업이 중단됩니다.

SnapMirror 활성 동기화 관계에서 기본 사이트가 다운되어 볼륨 이동 작업이 컷오버 지연 상태로 무기한 중단되는 경우 다음 정보를 사용합니다.

문제:

SnapMirror 활성 동기화 관계에서 운영 사이트가 다운되면 볼륨 이동 작업이 컷오버가 지연된 상태로 무기한 중단됩니다.
운영 사이트가 다운되면 보조 사이트가 자동 예상치 못한 장애 조치(AUFO)를 수행합니다. AUFO가 트리거될 때 볼륨 이동 작업이 진행 중이면 볼륨 이동이 중단됩니다.

솔루션:

중단된 볼륨 이동 인스턴스를 중단하고 볼륨 이동 작업을 다시 시작하십시오.

스냅샷을 삭제할 수 없을 때 **ONTAP SnapMirror** 릴리스가 실패합니다.

스냅샷을 삭제할 수 없어 SnapMirror 릴리스 작업이 실패하는 경우 다음 정보를 사용하세요.

문제:

스냅샷을 삭제할 수 없으면 SnapMirror 릴리즈 작업이 실패합니다.

솔루션:

스냅샷에 임시 태그가 있습니다. `snapshot delete`임시 스냅샷을 제거하려면 옵션과 함께 명령을 `-ignore-owners` 사용합니다.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners
true -force true
```

'napmirror release' 명령을 재시도합니다.

관련 정보

- "SnapMirror 릴리즈"

볼륨 이동 참조 스냅샷이 **ONTAP SnapMirror** 관계에 대한 최신 정보로 표시됩니다.

볼륨 이동 작업 후 SnapMirror 관계에 대해 볼륨 이동 참조 스냅샷이 최신으로 표시되는 경우 다음 정보를 사용합니다.

문제:

정합성 보장 그룹 볼륨에서 볼륨 이동 작업을 수행한 후 볼륨 이동 참조 스냅샷이 SnapMirror 관계의 최신 스냅샷으로

잘못 표시될 수 있습니다.

다음 명령을 사용하여 최신 스냅샷을 볼 수 있습니다.

'스냅샷 표시-필드 최신-스냅샷 상태-확장'을 선택합니다

솔루션:
수동으로 '스냅샷 미러 재동기화'를 수행하거나 볼륨 이동 작업이 완료된 후 다음 자동 재동기화 작업을 기다리십시오.

관련 정보

- "스냅미러 재동기화"
- "스냅미러 쇼"

MetroCluster 및 SnapMirror Active Sync를 위한 ONTAP Mediator

ONTAP 중재자에 대해 자세히 알아보십시오

이 문서는 ONTAP Mediator의 온프레미스 버전을 참조합니다. ONTAP 9.17.1부터 제공되는 ONTAP Cloud Mediator에 대한 자세한 내용은 다음을 참조하십시오. "SnapMirror Active Sync 설명서" .

ONTAP Mediator는 ONTAP 기능에 대한 다양한 기능을 제공합니다.

- HA 메타데이터에 대한 영구적이고 울타리 저장소를 제공합니다.
- 컨트롤러 활성을 위한 핑 프록시 역할을 합니다.
- quorum 결정에 도움이 되는 동기 노드 상태 쿼리 기능을 제공합니다.

ONTAP Mediator는 두 가지 추가 systemctl 서비스를 제공합니다.

- **`ontap_mediator.service`**

  ONTAP 관계를 관리하기 위한 REST API 서버를 유지 관리합니다.

- **`mediator-scst.service`**

  SCST(iSCSI 모듈)의 시작 및 종료를 제어합니다.

시스템 관리자를 위해 제공되는 도구

시스템 관리자를 위해 제공되는 도구:

- **`/usr/local/bin/mediator_change_password`**

  현재 API 사용자 이름과 암호를 제공할 때 새 API 암호를 설정합니다.

- **`/usr/local/bin/mediator_change_user`**

현재 API 사용자 이름 및 암호를 제공할 때 새 API 사용자 이름을 설정합니다.

- **`/usr/local/bin/mediator_generate_support_bundle`**

  NetApp 고객 지원 커뮤니케이션하기 위해 필요한 모든 유용한 지원 정보를 포함하는 로컬 tgz 파일을 생성합니다. 여기에는 애플리케이션 구성, 로그 및 일부 시스템 정보가 포함됩니다. 번들은 로컬 디스크에 생성되고 필요에 따라 수동으로 전송할 수 있습니다. 스토리지 위치:/opt/netapp/data/support_bundle/

- **`/usr/local/bin/uninstall_ontap_mediator`**

  ONTAP 중재자 패키지와 SCST 커널 모듈을 제거합니다. 여기에는 모든 구성, 로그 및 메일박스 데이터가 포함됩니다.

- **`/usr/local/bin/mediator_unlock_user`**

  인증 재시도 한도에 도달하면 API 사용자 계정의 잠금을 해제합니다. 이 기능은 무차별 암호 대입(brute force password derivation)을 방지하는 데 사용됩니다. 사용자에게 올바른 사용자 이름과 암호를 묻는 메시지가 표시됩니다.

- **`/usr/local/bin/mediator_add_user`**

  (지원만 해당) 설치 시 API 사용자를 추가하는 데 사용됩니다.

특별 참고 사항

ONTAP mediator는 SCST에 의존하여 iSCSI를 제공합니다(참조 http://scst.sourceforge.net/index.html). 이 패키지는 커널 전용으로 설치하는 동안 컴파일되는 커널 모듈입니다. 커널에 대한 업데이트를 수행하려면 SCST를 다시 설치해야 할 수 있습니다. 또는 ONTAP Mediator를 제거한 다음 다시 설치하고 ONTAP 관계를 다시 구성하세요.

서버 OS 커널에 대한 모든 업데이트는 ONTAP의 유지 관리 창과 조율되어야 합니다.

ONTAP Mediator의 새로운 기능

ONTAP Mediator는 각 릴리스마다 새로운 기능 향상을 제공합니다. 새로운 기능

향상된 기능

SCST 버전 정보는 를 SCST 지원 매트릭스참조하십시오.

ONTAP 중재자 버전	향상된 기능

1.11	• RHEL 지원: ◦ 호환성: 9.5. ◦ 권장 버전: 10.1, 10.0, 9.7, 9.6, 9.4, 8.10. • Rocky Linux 10.1, 9.7 및 8.10을 지원합니다. • Oracle Linux 10.0 및 9.6 지원. • MetroCluster IP 구성에 IPv6에 대한 지원을 추가합니다. • fapolicyd에 대한 지원을 추가합니다.
1.10	• RHEL 지원: ◦ 호환성: 9.5. ◦ 권장 버전: 10.0, 9.6, 9.4, 8.10. • Rocky Linux 10.0, 9.6 및 8.10을 지원합니다. • 기본 Python 버전을 Python 3.9에서 Python 3.12로 업그레이드합니다.
1.9.1	• RHEL 지원: ◦ 호환 가능 버전: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, 8.4. ◦ 권장 버전: 9.5, 9.4, 9.2, 9.0, 8.10, 8.8. • Rocky Linux 9.5 및 8.10 지원. • 코드 서명 검증을 위한 새로운 인증서를 추가합니다. • 다음을 사용하여 코드 서명 확인 건너뛰기에 대한 지원이 추가되었습니다. `-skip -code-signature-check` 깃발. • 설치 프로그램은 만료된 코드 서명 인증서를 감지하면 경고를 표시합니다.
1.9	• RHEL 지원: ◦ 호환 가능 버전: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, 8.4. ◦ 권장 버전: 9.5, 9.4, 9.2, 9.0, 8.10, 8.8. • Rocky Linux 9.5 및 8.10 지원. • RHEL 및 Rocky Linux에 대한 FIPS 지원 • 확장성 향상을 위해 성능 향상 추가 • 파일 이름이 향상되어 PKI 서명 인증서의 설정이 간편해졌습니다.
1.8	• RHEL 지원: ◦ 호환 가능 버전: 8.7, 8.6, 8.5, 8.4. ◦ 권장 버전: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9, 8.8. • Rocky Linux 9.4 및 8.10 지원.

1.7	• RHEL 지원: ◦ 호환 가능 버전: 8.7, 8.6, 8.5, 8.4. ◦ 권장 버전: 9.3, 9.2, 9.1, 9.0, 8.9, 8.8. • Rocky Linux 9.3 및 8.9 지원. • 자체 서명된 인증서 및 타사 서명 인증서의 SAN(주체 대체 이름) 데이터 지원
1.6	• Python 3.9 업데이트. • RHEL 지원: ◦ 호환 가능 버전: 8.7, 8.6, 8.5, 8.4. ◦ 권장 버전: 9.2, 9.1, 9.0, 8.8. • Rocky Linux 9.2 및 8.8 지원. • RHEL 7.x/CentOS 모든 릴리스에 대한 지원이 중단되었습니다.
1.5	• RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6을 지원합니다. • CentOS 7.9, 7.8, 7.7 및 7.6 지원. • RHEL 7.x/CentOS 7.x에 대한 중단 경고를 포함합니다 • 대규모 SnapMirror 액티브 동기화 시스템에 맞게 속도 최적화 • 설치 프로그램에 암호화 코드 서명이 추가되었습니다.
1.4	• RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6을 지원합니다. • CentOS 7.9, 7.8, 7.7 및 7.6 지원. • UFEI 기반 펌웨어의 보안 부팅(SB) 지원이 추가되었습니다.
1.3	• RHEL 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6을 지원합니다. • CentOS 7.9, 7.8, 7.7 및 7.6 지원.
1.2	• RHEL 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6을 지원합니다. • CentOS 7.9, 7.8, 7.7 및 7.6 지원. • HTTPS 사서함 지원. • ONTAP 9.8 + MCC-IP AUSO 및 SnapMirror 액티브 동기화 ZRTO와 함께 사용
1.1	• RHEL 8.0 및 7.6 지원. • CentOS 7.6 지원. • Perl 종속성을 제거합니다.

1.0	• iSCSI 메일박스 지원 • ONTAP 9.7+ MCC-IP AUSO와 함께 사용. • RHEL/CentOS 7.6 지원

OS 지원 매트릭스

ONTAP 중재자를 위한 OS	1.11	1.10	1.9.1	1.9	1.8	1.7	1.6	1.5	1.4	1.3	1.2	1.1	1.0
RHEL 10.1	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 10.0	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.7	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.6	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.5 를 참조하십시오	호환 가능	호환 가능	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.4 를 참조하십시오	예	예	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.3 을 참조하십시오	아니요	아니요	호환 가능	호환 가능	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.2	아니요	아니요	예	예	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.1	아니요	아니요	호환 가능	호환 가능	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.0	아니요	아니요	예	예	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요

RHEL 8.10을 참조하십시오	예	예	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 8.9 를 참조하십시오	아니요	아니요	호환 가능	호환 가능	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 8.8	아니요	아니요	예	예	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 8.7	아니요	아니요	호환 가능	호환 가능	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 8.6을 참조하십시오	아니요	아니요	호환 가능	호환 가능	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 8.5	아니요	아니요	호환 가능	호환 가능	예	예	예	예	예	아니요	아니요	아니요	아니요
RHEL 8.4	아니요	아니요	호환 가능	호환 가능	예	예	예	예	예	아니요	아니요	아니요	아니요
RHEL 8.3	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	아니요	아니요	아니요
RHEL 8.2	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	아니요	아니요	아니요
RHEL 8.1	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	예	아니요	아니요
RHEL 8.0	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	예	예	아니요
RHEL 및 CentOS 7.9	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	호환 가능	아니요	아니요

RHEL 및 CentOS 7.8	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	예	아니요	아니요
RHEL 및 CentOS 7.7	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	예	아니요	아니요
RHEL 및 CentOS 7.6	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	예	예	예(RHEL에만 해당)
CentOS 8 및 스트림	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	해당 없음	해당 없음	해당 없음
로키 리눅스 10.0	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
록키 리눅스 9	예	예	예	예	예	예	예	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
Rocky Linux 8	예	예	예	예	예	예	예	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
오라클 리눅스 10.0	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
오라클 리눅스 9	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요

- "예"는 ONTAP 중재자 설치에 OS가 권장되며 완전히 호환되고 지원됨을 의미합니다.
- "아니요"는 OS 및 ONTAP 중재자가 호환되지 않음을 의미합니다.
- "호환"이란 Red Hat이 더 이상 이러한 RHEL 버전을 지원하지 않지만 ONTAP Mediator는 여전히 해당 버전에 설치할 수 있음을 의미합니다.
- ONTAP Mediator 1.6에서는 Rocky Linux 9 및 8에 대한 지원이 추가되었습니다.
- ONTAP 중재자 1.5는 RHEL 7.x 지사 운영 체제에서 마지막으로 지원되는 릴리스입니다.
- 재분개로 인해 모든 릴리스에 대해 CentOS 8이 제거되었습니다. CentOS Stream은 적합한 운영 대상 OS가 아닌

것으로 간주됩니다. 지원은 계획되어 있지 않습니다.

SCST 지원 매트릭스

다음 표는 ONTAP mediator의 각 버전에 대해 지원되는 SCST 버전을 보여줍니다.

ONTAP 중재자 버전	지원되는 SCST 버전입니다
ONTAP 중재자 1.11	scst-3.9.tar.gz
ONTAP 중재자 1.10	scst-3.9.tar.gz
ONTAP 중재자 1.9.1	scst-3.8.0.tar.bz2
ONTAP 중재자 1.9	scst-3.8.0.tar.bz2
ONTAP 중재자 1.8	scst-3.8.0.tar.bz2
ONTAP 중재자 1.7	scst - 3.7.0.tar.bz2
ONTAP 중재자 1.6	scst - 3.7.0.tar.bz2
ONTAP 중재자 1.5	scst - 3.6.0.tar.bz2
ONTAP 중재자 1.4	scst - 3.6.0.tar.bz2
ONTAP 중재자 1.3	scst - 3.5.0.tar.bz2
ONTAP 중재자 1.2	scst - 3.4.0.tar.bz2
ONTAP 중재자 1.1	scst - 3.4.0.tar.bz2
ONTAP 중재자 1.0	scst - 3.3.0.tar.bz2

설치 또는 업그레이드

ONTAP Mediator 설치 워크플로 요약

ONTAP Mediator를 설치하는 과정에는 설치 준비, 저장소 액세스 제공, 설치 패키지 다운로드, 코드 서명 확인, ONTAP Mediator 패키지 설치, 설치 후 구성 작업 수행이 포함됩니다.

1. "ONTAP Mediator 설치 또는 업그레이드 준비"

ONTAP Mediator를 설치하거나 업그레이드하려면 모든 필수 구성 요소가 충족되었는지 확인해야 합니다.

2. "호스트 OS 및 중재자 업그레이드"

ONTAP Mediator의 기존 버전을 업그레이드하는 경우, 먼저 이전 버전을 제거한 후 새 버전을 설치해야 합니다. ONTAP Mediator를 처음 설치하는 경우 이 단계를 건너뛸 수 있습니다.

3. "저장소 액세스 제공"

설치 과정에서 ONTAP Mediator가 필요한 패키지에 액세스할 수 있도록 저장소에 대한 액세스를 활성화해야 합니다.

4 **"ONTAP 중재자 설치 패키지를 다운로드합니다"**

ONTAP Mediator 다운로드 페이지에서 ONTAP Mediator 설치 패키지를 다운로드하세요.

5 **"ONTAP Mediator 설치 패키지의 코드 서명을 확인하세요."**

NetApp에서는 ONTAP Mediator 설치 패키지를 설치하기 전에 ONTAP Mediator 코드 서명을 확인할 것을 권장합니다.

6 **"ONTAP Mediator 설치"**

ONTAP Mediator를 설치하려면 설치 패키지를 받아서 호스트에서 설치 프로그램을 실행해야 합니다.

7 **"ONTAP Mediator 설치 확인"**

ONTAP Mediator를 설치한 후 성공적으로 실행되는지 확인하세요.

8 "설치 후 구성 작업 수행"

ONTAP Mediator를 설치하고 실행한 후에는 ONTAP Mediator 기능을 사용하기 위해 추가 구성 작업을 수행해야 합니다.

ONTAP Mediator 설치 또는 업그레이드

ONTAP Mediator를 설치하거나 업그레이드하려면 모든 필수 구성 요소를 충족하고, 설치 패키지를 다운로드한 다음 호스트에서 설치 프로그램을 실행해야 합니다.

- ONTAP 9.8부터는 모든 버전의 ONTAP Mediator를 사용하여 SnapMirror 활성 동기화 관계를 모니터링할 수 있습니다.
- ONTAP Mediator의 모든 버전을 사용하여 MetroCluster IP 구성을 모니터링할 수 있습니다.

설치 및 업그레이드 고려 사항

ONTAP Mediator를 업그레이드하거나 설치하기 전에 다음 사항을 검토하세요.

ONTAP Mediator 1.8 및 이전 버전은 Red Hat Enterprise Linux(RHEL) FIPS 모드와 호환되지 않아 성공적으로 설치할 수 없습니다. FIPS 모드가 활성화되어 있는지 확인하려면 다음을 사용하세요. `fips-mode-setup --check` 명령. 다음을 사용하여 FIPS 모드를 비활성화할 수 있습니다. `fips-modesetup --disable` 명령. ONTAP Mediator 1.8 또는 이전 버전을 성공적으로 설치하려면 FIPS 모드를 비활성화한 후 재부팅하세요.

- ONTAP Mediator를 최신 버전으로 업그레이드해야 합니다. 이전 버전은 모든 ONTAP 릴리스에서 여전히 작동하지만 최신 버전에는 타사 구성 요소에 대한 보안 패치가 포함되어 있습니다.
- 새 ONTAP 중재자 버전으로 업그레이드할 때 더 높은 버전을 사용할 수 없는 경우 설치 관리자는 자동으로 권장 SCST 버전으로 업그레이드합니다. 더 높은 SCST 버전을 수동으로 설치하는 방법은 을 참조하십시오"ONTAP 중재자 관리". 지원되는 버전은 를 "SCST 지원 매트릭스"참조하십시오.

- 설치에 실패하면 ONTAP Mediator의 최신 버전으로 업그레이드해야 할 수도 있습니다.
- 2025년 6월 15일부터 코드 서명 인증서가 만료되어 ONTAP Mediator 1.9 및 1.8을 설치하거나 업그레이드할 수 없습니다. 설치나 업그레이드가 실패하면 대신 ONTAP Mediator 1.9.1 패치 버전을 사용하세요.

- 를 설치하는 경우 `yum-utils` 패키지를 사용하면 을 사용할 수 있습니다 `needs-restarting` 명령.
- ONTAP Mediator 1.11부터 MetroCluster IP 구성에 IPv6가 지원됩니다.

호스트 요구 사항

RHEL 또는 Rocky Linux를 설치하고 관련 저장소를 구성할 때 다음 요구 사항을 따르세요.

설치 또는 구성 프로세스를 수정하는 경우 추가 단계를 수행해야 할 수 있습니다.

Linux 배포 요구 사항

- Red Hat의 모범 사례에 따라 RHEL 또는 Rocky Linux를 설치합니다. CentOS 8.x의 지원이 종료되었으므로, CentOS 8.x와 호환되는 버전은 권장되지 않습니다.
- ONTAP Mediator를 설치할 때 설치 프로그램이 모든 필수 소프트웨어 종속성을 검색하여 설치할 수 있도록 시스템이 필수 저장소에 액세스할 수 있는지 확인하세요.
- yum 설치 관리자가 RHEL 리포지토리에서 종속 소프트웨어를 찾을 수 있도록 하려면 설치 중 또는 이후에 유효한 Red Hat 서브스크립션을 사용하여 시스템을 등록합니다.

자세한 내용은 Red Hat 서브스크립션 관리자 설명서를 참조하십시오.

네트워킹 요구 사항

다음 포트가 ONTAP 중재자에 사용 가능하고 사용되지 않는지 확인합니다.

포트/서비스	출처	방향	목적지	목적
22/TCP	관리 호스트	인바운드	ONTAP 중재자	(선택 사항) SSH/ONTAP 중재자 관리
31784/TCP	클러스터 관리 LIF	인바운드	ONTAP 중재자 웹 서버	(필수) REST API(HTTPS)
3260/TCP 1	노드 데이터 LIF 또는 노드 관리 LIF	양방향	ONTAP는 iSCSI 대상을 중재합니다	(MetroCluster IP 구성에 필요) 사서함에 대한 iSCSI 데이터 연결

SMBC 고객의 경우 ONTAP는 포트 3260을 활성화 또는 연결할 필요가 없습니다.

- 타사 방화벽을 사용하는 경우 다음을 참조하세요."ONTAP 중재자를 위한 방화벽 요구 사항" .
- 인터넷에 액세스할 수 없는 Linux 호스트의 경우 로컬 리포지토리에서 필요한 패키지를 사용할 수 있는지 확인합니다.

Linux 환경에서 LACP(Link Aggregation Control Protocol)를 사용하는 경우 커널을 구성하고 `sysctl net.ipv4.conf.all.arp_ignore` 을 로 `2`설정합니다.

OS 요구 사항

OS는 다음 요구 사항을 충족해야 합니다.

- 64비트 물리적 설치 또는 가상 머신
- 8GB RAM
- 1GB 디스크 공간(응용 프로그램 설치, 서버 로그 및 데이터베이스에 사용됨)
- 사용자: 루트 액세스

다음 표는 ONTAP mediator 버전별로 지원되는 운영 체제를 보여줍니다.

ONTAP 중재자 버전	지원되는 Linux 버전
1.11	• Red Hat Enterprise Linux ◦ 호환 가능: 9.5 [1] ◦ 권장: 10.1, 10.0, 9.7, 9.6, 9.4, 8.10 • Rocky Linux 10.1, 9.7 및 8.10 • Oracle Linux 10.0 및 9.6
1.10	• Red Hat Enterprise Linux ◦ 호환 가능: 9.5 [1] ◦ 권장: 10.0, 9.6, 9.4 및 8.10 • Rocky Linux 10.0, 9.6 및 8.10
1.9.1	• Red Hat Enterprise Linux ◦ 호환 가능 버전: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.5, 9.4, 9.2, 9.0, 8.10, 8.8 • Rocky Linux 9.5 및 8.10
1.9	• Red Hat Enterprise Linux ◦ 호환 가능 버전: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.5, 9.4, 9.2, 9.0, 8.10, 8.8 • Rocky Linux 9.5 및 8.10
1.8	• Red Hat Enterprise Linux: ◦ 호환 가능: 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9, 8.8 • Rocky Linux 9.4 및 8.10

1.7	• Red Hat Enterprise Linux: ◦ 호환 가능: 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.3, 9.2, 9.1, 9.0, 8.9, 8.8 • Rocky Linux 9.3 및 8.9
1.6	• Red Hat Enterprise Linux: ◦ 호환 가능: 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.2, 9.1, 9.0 및 8.8 • Rocky Linux 9.2 및 8.8
1.5	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6
1.4	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6
1.3	• Red Hat Enterprise Linux: 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6
1.2	• Red Hat Enterprise Linux: 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6

1. 호환 가능이란 Red Hat이 더 이상 이러한 RHEL 버전을 지원하지 않지만 ONTAP Mediator는 여전히 해당 버전에 설치할 수 있음을 의미합니다.

OS 필수 패키지

ONTAP Mediator에는 다음 패키지가 필요합니다.

패키지는 사전 설치되거나 ONTAP 중재자 설치 프로그램에 의해 자동으로 설치됩니다.

모든 RHEL/CentOS 버전	RHEL 10.x / Rocky Linux 10용 추가 패키지	RHEL 9.x/Rocky Linux 9용 추가 패키지	RHEL 8.x/Rocky Linux 8용 추가 패키지

• OpenSSL • OpenSSL - devel • kernel-devel-$(uname-r) • GCC 를 참조하십시오 • 만듭니다 • libselinux-utils • 패치 • bzip2 • Perl - 데이터 - 덤프 • Perl-ExtUtils-MakeMaker • efootmgr • mokutil	• 파이썬3.12 • 파이썬3.12-개발	• elfutils -libelf -devel • 정책 코어 유틸리티 - 비톤 - 유틸리티 • 3단계 • python3-devel	• elfutils -libelf -devel • 정책 코어 유틸리티 - 비톤 - 유틸리티 • redhat-LSB-core를 참조하십시오 • python39 • 피톤39-데블

중재자 설치 패키지는 다음을 포함하는 자동 압축 tar 파일입니다.

- 지원되는 릴리즈의 리포지토리에서 가져올 수 없는 모든 종속성을 포함하는 RPM 파일입니다.
- 설치 스크립트

유효한 SSL 인증서를 권장합니다.

OS 업그레이드 고려 사항 및 커널 호환성

- 커널을 제외한 모든 라이브러리 패키지를 업데이트할 수 있지만 ONTAP Mediator에서 변경 사항을 적용하려면 재부팅이 필요할 수 있습니다. 재부팅이 필요한 경우 가동 중지 시간을 예약하세요.
- OS 커널을 최신 상태로 유지해야 합니다. 커널 코어를 지원되는 버전으로 업그레이드하세요."ONTAP 중재자 버전 매트릭스" . 시스템을 재부팅해야 하므로, 정전에 대비한 유지 관리 기간을 계획하세요.
  - 재부팅하기 전에 SCST 커널 모듈을 제거한 다음 나중에 다시 설치하세요.
  - 커널 OS 업그레이드를 시작하기 전에 지원되는 SCST 버전을 준비하여 다시 설치하세요.

- 커널 버전이 운영 체제 버전과 일치해야 합니다.
- 테스트된 SCST 모듈이 작동하지 않을 수 있으므로 ONTAP Mediator 릴리스에 대해 지원되는 OS 버전 이상으로 커널을 업그레이드하지 마세요.

UEFI 보안 부팅이 활성화된 경우 **ONTAP mediator**를 설치합니다

ONTAP mediator는 UEFI 보안 부팅이 활성화되어 있거나 활성화되지 않은 시스템에 설치할 수 있습니다.

이 작업에 대해

필요하지 않거나 ONTAP mediator 설치 문제를 해결하는 경우 ONTAP mediator를 설치하기 전에 UEFI 보안 부팅을 사용하지 않도록 선택할 수 있습니다. 시스템 설정에서 UEFI 보안 부팅 옵션을 비활성화합니다.

UEFI 보안 부팅을 비활성화하는 방법에 대한 자세한 지침은 호스트 OS 설명서를 참조하십시오.

UEFI 보안 부팅이 활성화된 ONTAP Mediator를 설치하려면 서비스를 시작하기 전에 보안 키를 등록해야 합니다. 이 키는 SCST 설치의 컴파일 단계 중에 생성되며 컴퓨터에 개인 공개 키 쌍으로 저장됩니다. 유틸리티를 사용하여 `mokutil` 공개 키를 UEFI 펌웨어에 컴퓨터 소유자 키(Mok)로 추가하여 시스템이 서명된 모듈을 신뢰하고 로드할 수 있도록 합니다. `mokutil`Mok를 활성화하기 위해 시스템을 재부팅할 때 필요하므로 암호를 안전한 위치에 저장합니다.

단계

1. 시스템에서 UEFI 보안 부팅이 활성화되어 있는지 확인합니다.

```
mokutil --sb-state
```

결과는 이 시스템에서 UEFI 보안 부팅이 활성화되었는지 여부를 나타냅니다.

만약…	이동…
UEFI 보안 부팅이 활성화되었습니다	
UEFI 보안 부팅이 비활성화되었습니다	"호스트 운영 체제를 업그레이드한 다음 ONTAP Mediator를 업그레이드합니다."

- 보안 위치에 저장해야 하는 암호를 만들라는 메시지가 표시됩니다. UEFI 부팅 관리자에서 키를 활성화하려면 이 암호가 필요합니다.
- ONTAP 중재자 1.2.0 및 이전 버전은 이 모드를 지원하지 않습니다.

2. 유틸리티가 설치되어 있지 않으면 `mokutil` 다음 명령을 실행합니다.

```
yum install mokutil
```

호스트 **OS** 및 **ONTAP** 중재자를 업그레이드합니다

ONTAP 중재자를 위한 호스트 OS를 최신 버전으로 업그레이드하려면 먼저 ONTAP 중재자를 제거해야 합니다.

이 작업에 대해

leapp-upgrade 도구를 사용하여 ONTAP Mediator의 호스트 OS를 업그레이드하기 전에 ONTAP Mediator를 제거하세요. 이 도구는 등록된 저장소에서 새로운 RPM 버전을 확인합니다.

ONTAP Mediator 설치 프로그램은 .rpm 파일을 설치하고, leapp-upgrade 도구는 이 파일을 검색에 포함합니다. 설치 프로그램이 등록된 저장소에서 파일을 다운로드하는 대신 압축을 풀기 때문에 도구에서 업그레이드를 찾을 수 없습니다. 패키지를 제거하려면 leapp-upgrade 도구를 사용해야 합니다.

단계

1. 로그 파일을 백업하세요.

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. leapp-upgrade 도구를 사용하여 업그레이드를 수행합니다.

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
  ..<snip upgrade checks>..
  ..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
  ..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. ONTAP Mediator를 다시 설치하세요:

로그 파일 손실을 방지하기 위해 ONTAP 중재자를 재설치한 후 바로 나머지 단계를 수행하십시오.

```
[rootmediator-host ~]# ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. ontap_mediator 중지:

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. 로그 파일을 교체합니다.

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. ontap_mediator를 시작합니다:

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. 모든 ONTAP 클러스터를 업그레이드된 ONTAP Mediator에 다시 연결합니다.

IP를 통한 MetroCluster

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          false
                        siteA-node1             true          false
                        siteB-node2             true          false
                        siteB-node2             true          false
siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It may
take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          true
                        siteA-node1             true          true
                        siteB-node2             true          true
                        siteB-node2             true          true
siteA::>
```

SnapMirror 활성 동기화

SnapMirror Active Sync의 경우 /opt/netapp 외부에 저장된 TLS 인증서를 다시 설치할 필요가 없습니다. /opt/netapp에 저장된 인증서를 백업하고 복원합니다.

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            unreachable       true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
39     mediator remove      peer1      peer1-node1    Success
     Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
peer1
        4A790360081F41145E14C5D7CE721DC6C210007F
                         ONTAPMediatorCA                        server-
ca
    Certificate Authority: ONTAP Mediator CA
        Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

 peer1::> security certificate install -type server-ca -vserver peer1

Please enter Certificate: Press <Enter> when done
  ..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254
```

```
The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

 Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..


You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237 -peer
-cluster peer2 -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 43] 'mediator add' job queued

peer1::> job show -id 43
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
43     mediator add         peer1      peer1-node2    Success
    Description: Creating a mediator entry

peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            connected         true

peer1::>
```

관련 정보

- "보안 인증서 삭제"
- "보안 인증서 설치"
- "보안 인증서가 표시됩니다"
- "스냅미러 중재자 추가"
- "스냅미러 중재자 제거"
- "스토리지 iSCSI 이니시에이터 표시"

ONTAP 중재자 설치를 위한 리포지토리 액세스를 제공합니다

설치 과정에서 ONTAP Mediator가 필요한 패키지에 액세스할 수 있도록 저장소에 대한 액세스를 활성화해야 합니다.

단계

1. 다음 표와 같이 액세스해야 하는 리포지토리를 결정합니다.

운영 체제가…	이러한 리포지토리에 대한 액세스를 제공해야 합니다…
RHEL 10.x	• rhel-10-for-x86_64-baseos-rpms • rhel-10-for-x86_64-appstream-rpms
RHEL 9.x를 참조하십시오	• RHEL-9-for-x86_64-baseos-rpms • RHEL-9-for-x86_64-appstream-rpms
RHEL 8.x를 참조하십시오	• RHEL-8-for-x86_64-baseos-rpms • RHEL-8-for-x86_64-appstream-rpms
RHEL 7.x를 참조하십시오	• RHEL-7-server-optional-rpms
CentOS 7.x	• C7.6.1810 - 기본 리포지토리입니다
로키 리눅스 10	• 애플리케이션 스트림 • 베이스코스
록키 리눅스 9	• 애플리케이션 스트림 • 베이스코스
Rocky Linux 8	• 애플리케이션 스트림 • 베이스코스

2. 다음 절차 중 하나를 사용하여 위에 나열된 리포지토리에 액세스할 수 있으므로 ONTAP 중재자가 설치 프로세스 중에 필요한 패키지에 액세스할 수 있습니다.

ONTAP Mediator에 "추가" 및 "선택" 저장소에 있는 Python 모듈에 대한 종속성이 있는 경우 액세스해야 할 수 있습니다. `rhel-X-for-x86_64-extras-rpms` 그리고 `rhel-X-for-x86_64-optional-rpms` 파일.

RHEL 10.x 운영 체제에 대한 절차

운영 체제가 *RHEL 10.x*인 경우 다음 절차를 사용하여 저장소에 대한 액세스를 활성화하세요.

단계

1. 필요한 리포지토리 구독:

```
subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
```

다음 예제에서는 이 명령의 실행을 보여 줍니다.

```
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
Repository 'rhel-10-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
Repository 'rhel-10-for-x86_64-appstream-rpms' is enabled for this system.
```

2. yum repolist 명령을 실행합니다.

새로 가입된 리포지토리가 목록에 나타납니다.

RHEL 9.x 운영 체제에 대한 절차

운영 체제가 * RHEL 9.x * 인 경우 다음 절차를 사용하여 리포지토리에 액세스할 수 있습니다.

단계

1. 필요한 리포지토리 구독:

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

다음 예제에서는 이 명령의 실행을 보여 줍니다.

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-baseos-rpms
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-appstream-rpms
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. yum repolist 명령을 실행합니다.

새로 가입된 리포지토리가 목록에 나타납니다.

RHEL 8.x 운영 체제에 대한 절차

운영 체제가 * RHEL 8.x * 인 경우 다음 절차를 사용하여 리포지토리에 액세스할 수 있습니다.

단계

1. 필요한 리포지토리 구독:

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

다음 예제에서는 이 명령의 실행을 보여 줍니다.

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-baseos-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. yum repolist 명령을 실행합니다.

새로 가입된 리포지토리가 목록에 나타납니다.

RHEL 7.x 운영 체제에 대한 절차

운영 체제가 * RHEL 7.x * 인 경우 다음 절차를 사용하여 리포지토리에 액세스할 수 있습니다.

단계

1. 필요한 리포지토리 구독:

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

다음 예제에서는 이 명령의 실행을 보여 줍니다.

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-
server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

2. yum repolist 명령을 실행합니다.

다음 예제에서는 이 명령의 실행을 보여 줍니다. "rhel-7-server-optional-rpms" 리포지토리가 목록에 나타나야 합니다.

```
[root@localhost ~]# yum repolist
Loaded plugins: product-id, search-disabled-repos, subscription-
manager
rhel-7-server-optional-rpms | 3.2 kB  00:00:00
rhel-7-server-rpms | 3.5 kB  00:00:00
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
|  26 kB  00:00:00
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
| 2.5 MB  00:00:00
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
| 8.3 MB  00:00:01
repo id                                    repo name
status
rhel-7-server-optional-rpms/7Server/x86_64   Red Hat Enterprise
Linux 7 Server - Optional (RPMs)   19,447
rhel-7-server-rpms/7Server/x86_64            Red Hat Enterprise
Linux 7 Server (RPMs)              26,758
repolist: 46,205
[root@localhost ~]#
```

CentOS 7.x 운영 체제에 대한 절차

운영 체제가 * CentOS 7.x * 인 경우 리포지토리에 대한 액세스를 활성화하려면 다음 절차를 따르십시오.

다음 예는 CentOS 7.6의 리포지토리를 보여 주고 있으며 다른 CentOS 버전에서는 작동하지 않을 수 있습니다. 사용 중인 CentOS 버전에 대한 기본 리포지토리를 사용합니다.

단계

1. C7.6.1810-Base 리포지토리를 추가합니다. C7.6.1810 - 기본 볼트 리포지토리에는 ONTAP 중재자를 위해 필요한 "kernel-devel" 패키지가 포함되어 있습니다.
2. /etc/yum.repos.d/CentOS-Vault.repo에 다음 줄을 추가합니다.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. yum repolist 명령을 실행합니다.

   다음 예제에서는 이 명령의 실행을 보여 줍니다. CentOS-7.6.1810-기본 리포지토리가 목록에 나타나야 합니다.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base                                | 3.6 kB  00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz         | 166 kB  00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db       | 6.0 MB  00:00:04
repo id                    repo name                status
C7.6.1810-base/x86_64      CentOS-7.6.1810 - Base   10,019
base/7/x86_64              CentOS-7 - Base          10,097
extras/7/x86_64            CentOS-7 - Extras        307
updates/7/x86_64           CentOS-7 - Updates       1,010
repolist: 21,433
[root@localhost ~]#
```

Rocky Linux 10, 9 또는 **8** 운영 체제에 대한 절차

운영 체제가 **Rocky Linux 10**, **Rocky Linux 9** 또는 *Rocky Linux 8*인 경우 다음 절차를 사용하여 저장소에 대한 액세스를 활성화하세요.

단계

1. 필요한 리포지토리 구독:

```
dnf config-manager --set-enabled baseos
```

```
dnf config-manager --set-enabled appstream
```

2. 을 수행합니다 `clean` 작동:

```
dnf clean all
```

3. 리포지토리 목록을 확인합니다.

```
dnf repolist
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 10 - AppStream
baseos                          Rocky Linux 10 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 9 - AppStream
baseos                          Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 8 - AppStream
baseos                          Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

ONTAP 중재자 설치 패키지를 다운로드합니다

ONTAP Mediator 설치 패키지를 다운로드하여 설치하세요.

단계

1. ONTAP Mediator 다운로드 페이지에서 ONTAP Mediator 설치 패키지를 다운로드하세요.

   "ONTAP 중재자 다운로드 페이지"

2. Mediator 설치 패키지를 현재 작업 디렉토리에 넣었는지 확인하세요.

   ```
   [root@sdot-r730-0003a-d6 ~]# ls ontap-mediator-1.11.0.tgz
   ```

   ```
   ontap-mediator-1.11.0.tgz
   ```

   ⓘ ONTAP 중재자 버전 1.4 및 이전 버전의 경우 설치 관리자의 이름이 지정됩니다 `ontap-mediator`.

   시스템에 인터넷 접속이 불가능한 경우, 설치 프로그램이 필요한 패키지에 접근할 수 있는지 확인하세요.

3. 필요한 경우 Mediator 설치 패키지를 설치 디렉터리로 이동합니다.
4. 설치 프로그램 패키지의 압축을 풉니다.

   ```
   tar xvfz ontap-mediator-1.11.0.tgz
   ```

```
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
```

ONTAP 중재자 코드 서명을 확인합니다

NetApp 설치 전에 ONTAP Mediator 코드 서명을 확인할 것을 권장합니다. 이 단계는 선택 사항입니다.

시작하기 전에

ONTAP Mediator 코드 서명을 확인하기 전에 시스템이 이러한 요구 사항을 충족하는지 확인하세요.

- 2025년 6월 15일부터 코드 서명 검증 인증서가 만료되어 ONTAP Mediator 1.9 및 1.8를 설치하거나 업그레이드할 수 없습니다. 대신 ONTAP Mediator 1.11 또는 1.10을 설치하거나 업그레이드하세요.
- 시스템이 아래 요구 사항을 충족하지 않는 경우 확인 프로세스가 필요하지 않으며 로 직접 이동할 수 있습니다"ONTAP 중재자 설치 패키지를 설치합니다".

- 기본 검증을 위한 OpenSSL 버전 1.0.2에서 3.0까지
- TSA(Time Stamping Authority) 작업을 위한 OpenSSL 버전 1.1.0 이상
- OCSP 검증을 위한 공용 인터넷 액세스

다운로드 패키지에는 다음 파일이 포함되어 있습니다.

파일	설명
`ONTAP-Mediator-production.pub`	서명을 확인하는 데 사용되는 공개 키입니다
`csc-prod-chain-ONTAP-Mediator.pem`	공공 인증 CA 신뢰 체인
`csc-prod-ONTAP-Mediator.pem`	키를 생성하는 데 사용되는 인증서입니다
`ontap-mediator-1.11.0`	버전 1.11에 대한 제품 설치 실행 파일
`ontap-mediator-1.11.0.sig`	SHA-256 해시된 후 csc-prod 키를 사용하여 RSA에 서명하여 설치 관리자를 서명합니다

`ontap-mediator-1.11.0.sig.tsr`	설치 관리자의 서명에 OCSCP가 사용할 해지 요청입니다
`ontap-mediator-1.11.0.tsr`	타임스탬프 서명 요청 파일입니다
`tsa-prod-ONTAP-Mediator.pem`	TSR의 공개 인증서
`tsa-prod-chain-ONTAP-Mediator.pem`	TSR의 공개 인증서 CA 체인

단계

1. 에 대해 해지 확인을 수행합니다 `csc-prod-ONTAP-Mediator.pem` 온라인 인증서 상태 프로토콜(OCSP)을 사용합니다.

   a. 인증서의 OCSP URL을 찾으세요. 개발자 인증서는 URI를 제공하지 않을 수 있습니다.

   ```
   openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
   ```

   b. 인증서에 대한 OCSP 요청을 생성합니다.

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem
   -reqout req.der
   ```

   c. OCSP Manager에 연결하여 OCSP 요청을 보냅니다.

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem  -url
   ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-
   chain-ONTAP-Mediator.pem
   ```

2. CSC의 신뢰 체인과 로컬 호스트에 대한 만료 날짜를 확인합니다.

   ```
   openssl verify
   ```

   를 클릭합니다 `openssl` 경로의 버전에 유효한 값이 있어야 합니다 `cert.pem` (자체 서명 안 됨).

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem  # Failure action: The Code-
Signature-Check certificate has expired or is invalid. Download a newer
version of the ONTAP Mediator.
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem  # Failure action: The Time-
Stamp certificate has expired or is invalid. Download a newer version of
the ONTAP Mediator.
```

3. 확인하다 `ontap-mediator-1.11.0.sig.tsr` 그리고 `ontap-mediator-1.11.0.tsr` 연관된 인증서를 사용하는 파일:

오픈SSL 3.x

```
openssl ts -verify -data ontap-mediator-1.11.0.sig -in ontap-mediator-
1.11.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
```

오픈SSL 1.x

```
openssl ts -verify -data ontap-mediator-1.11.0 -in ontap-mediator-
1.11.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -partial_chain
```

ⓘ `.tsr`파일에는 설치 프로그램과 관련된 타임스탬프 응답과 코드 서명이 포함되어 있습니다. 처리 과정에서는 타임스탬프에 TSA의 유효한 서명이 있고 입력 파일이 변경되지 않았음을 확인합니다. 귀하의 기기는 로컬에서 검증을 수행합니다. TSA 서버에 접속할 필요가 없습니다.

4. 키에 대한 서명 확인:

```
openssl -dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.11.0.sig ontap-mediator-1.11.0
```

ONTAP 중재자 설치 패키지를 설치합니다

ONTAP Mediator를 설치하려면 설치 패키지를 받아서 호스트에서 설치 프로그램을 실행해야 합니다.

단계

1. 설치 프로그램을 실행하고 필요에 따라 프롬프트에 응답합니다.

```
./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```

```
[root@scs000099753 ~]# ./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```

설치 중에 서명 확인을 건너뛰려면 다음 명령을 사용하세요. `./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y --skip-code-signature-check`

설치 프로그램은 필요한 계정을 생성하고 필요한 패키지를 설치합니다. Mediator가 이미 설치되어 있는 경우 업그레이드하라는 메시지가 표시됩니다.

ONTAP 중재자 설치의 예(콘솔 출력)

```
[root@mediator_host ~]# tar -zxvf ontap-mediator-1.11.0.tgz
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
[root@mediator_host ~]#./ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
   Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
Error querying OCSP responder
80BBA032607F0000:error:1E800080:HTTP
routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
data:crypto/http/http_client.c:549:
80BBA032607F0000:error:1E800067:HTTP
routines:OSSL_HTTP_REQ_CTX_exchange:error
receiving:crypto/http/http_client.c:901:server=http://ocsp.entrust.net:
80
   WARNING: The OCSP check failed while attempting to test the Code-
Signature-Check certificate
   Continue without code signature checking (only recommended if
integrity has been established manually)? yes/no: yes
 SKIPPING: Code signature check, manual override due to lack of OCSP
response
+ Unpacking the ONTAP Mediator installer

ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Would you like to use the default account names: netapp +
mediatoradmin? (Y(es)/n(o)): yes



Enter ONTAP Mediator user account (mediatoradmin) password:
```

```
Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode
The installer will change the SELinux context type of
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi from type 'lib_t' to
'bin_t'.


+ Checking for default Linux firewall


+ Installing required packages.


Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use
"rhc" or "subscription-manager" to register.

Last metadata expiration check: 5 days, 14:34:13 ago on Thu 10 Jul 2025
01:28:32 AM EDT.
Package openssl-1:3.2.2-16.el10.x86_64 is already installed.
Package libselinux-utils-3.8-1.el10.x86_64 is already installed.
Package perl-Data-Dumper-2.189-512.el10.x86_64 is already installed.
Package bzip2-1.0.8-25.el10.x86_64 is already installed.
Package efibootmgr-18-8.el10.x86_64 is already installed.
Package mokutil-2:0.6.0-11.el10.x86_64 is already installed.
Package policycoreutils-python-utils-3.8-1.el10.noarch is already
installed.
Package python3-3.12.9-1.el10.x86_64 is already installed.
Dependencies resolved.
================================================================================
================================================================================
================================================================================
=========================
 Package
Architecture                                        Version
Repository                                              Size
================================================================================
================================================================================
================================================================================
=========================
Installing:
 elfutils-libelf-devel
x86_64                                              0.192-5.el10
```

```
AppStream                                              50 k
 gcc
x86_64                                          14.2.1-7.el10
AppStream                                              37 M
 kernel-devel
x86_64                                          6.12.0-55.9.1.el10_0
AppStream                                              22 M
 make
x86_64                                          1:4.4.1-9.el10
BaseOS                                                591 k
 openssl-devel
x86_64                                          1:3.2.2-16.el10
AppStream                                             3.9 M
 patch
x86_64                                          2.7.6-26.el10
AppStream                                             134 k
 perl-ExtUtils-MakeMaker
noarch                                          2:7.70-513.el10
AppStream                                              297 k
 python3-devel
x86_64                                          3.12.9-1.el10
AppStream
 334 k
 python3-pip
noarch                                          23.3.2-7.el10
AppStream                                             3.2 M
Installing dependencies:
 annobin-docs
noarch                                          12.92-1.el10
AppStream                                              94 k
 annobin-plugin-gcc
x86_64                                          12.92-1.el10
AppStream                                             985 k
 bison
x86_64                                          3.8.2-9.el10
AppStream                                             1.0 M
 cmake-filesystem
x86_64                                          3.30.5-2.el10
AppStream                                              29 k
 cpp
x86_64                                          14.2.1-7.el10
AppStream                                              12 M
 dwz
x86_64                                          0.15-7.el10
AppStream                                             139 k
 efi-srpm-macros
```

```
noarch                                          6-6.el10
AppStream                                          25 k
 flex
x86_64                                          2.6.4-19.el10
AppStream                                         303 k
 fonts-srpm-macros
noarch                                          1:2.0.5-18.el10
AppStream                                          29 k
 forge-srpm-macros
noarch                                          0.4.0-6.el10
AppStream                                          23 k
 gcc-plugin-annobin
x86_64                                          14.2.1-7.el10
AppStream                                          62 k
 glibc-devel
x86_64                                          2.39-37.el10
AppStream                                         641 k
 go-srpm-macros
noarch                                          3.6.0-4.el10
AppStream                                          29 k
 kernel-headers
x86_64                                          6.12.0-55.9.1.el10_0
AppStream                                         2.3 M
 kernel-srpm-macros
noarch                                          1.0-25.el10
AppStream                                          11 k
 libxcrypt-devel
x86_64                                          4.4.36-10.el10
AppStream                                          33 k
 libzstd-devel
x86_64                                          1.5.5-9.el10
AppStream
  53 k
 lua-srpm-macros
noarch                                          1-15.el10
AppStream                                          10 k
 m4
x86_64                                          1.4.19-11.el10
AppStream                                         309 k
 ocaml-srpm-macros
noarch                                          10-4.el10
AppStream                                          10 k
 openblas-srpm-macros
noarch                                          2-19.el10
AppStream                                         9.0 k
 package-notes-srpm-macros
```

```
noarch                                          0.5-13.el10
AppStream                                          11 k
 perl-AutoSplit
noarch                                          5.74-512.el10
AppStream                                          23 k
 perl-Benchmark
noarch                                          1.25-512.el10
AppStream                                          28 k
 perl-CPAN-Meta-Requirements
noarch                                          2.143-11.el10
AppStream                                          39 k
 perl-CPAN-Meta-YAML
noarch                                          0.018-512.el10
AppStream                                          29 k
 perl-Devel-PPPort
x86_64                                          3.72-512.el10
AppStream                                         223 k
 perl-ExtUtils-Command
noarch                                          2:7.70-513.el10
AppStream                                          16 k
 perl-ExtUtils-Constant
noarch                                          0.25-512.el10
AppStream                                          47 k
 perl-ExtUtils-Install
noarch                                          2.22-511.el10
AppStream                                          47 k
 perl-ExtUtils-Manifest
noarch                                          1:1.75-511.el10
AppStream                                          37 k
 perl-ExtUtils-ParseXS
noarch                                          1:3.51-512.el10
AppStream                                         190 k
 perl-File-Compare
noarch                                          1.100.800-512.el10
AppStream                                          15 k
 perl-File-Copy
noarch                                          2.41-512.el10
AppStream                                          22 k
 perl-I18N-Langinfo
x86_64                                          0.24-512.el10
AppStream                                          28 k
 perl-JSON-PP
noarch                                          1:4.16-512.el10
AppStream                                          69 k
 perl-Test-Harness
noarch                                          1:3.48-512.el10
```

```
AppStream                                          288 k
 perl-lib
x86_64                                          0.65-512.el10
AppStream                                           16 k
 perl-srpm-macros
noarch                                          1-57.el10
AppStream                                          9.7 k
 perl-version
x86_64                                          8:0.99.32-4.el10
AppStream                                           68 k
 pyproject-srpm-macros
noarch                                          1.16.2-1.el10
AppStream                                           16 k
 python-srpm-macros
noarch                                          3.12-9.1.el10
AppStream                                           26 k
 python3-pyparsing
noarch                                          3.1.1-7.el10
BaseOS                                             273 k
 qt6-srpm-macros
noarch                                          6.8.1-3.el10
AppStream
 11 k
 redhat-rpm-config
noarch                                          288-1.el10
AppStream                                           83 k
 rust-toolset-srpm-macros
noarch                                          1.84.1-1.el10
AppStream                                           13 k
 systemtap-sdt-devel
x86_64                                          5.2-2.el10
AppStream                                           78 k
 systemtap-sdt-dtrace
x86_64                                          5.2-2.el10
AppStream                                           72 k
 zlib-ng-compat-devel
x86_64                                          2.2.3-1.el10
AppStream                                           41 k
Installing weak dependencies:
 perl-CPAN-Meta
noarch                                          2.150010-511.el10
AppStream                                          202 k
 perl-Encode-Locale
noarch                                          1.05-31.el10
AppStream                                           21 k
 perl-Time-HiRes
```

```
x86_64                                                 4:1.9777-511.el10
AppStream                                                  62 k
 perl-devel
x86_64                                                 4:5.40.1-512.el10
AppStream                                                 772 k
 perl-doc
noarch                                                 5.40.1-512.el10
AppStream                                                 4.9 M

Transaction Summary
================================================================================
================================================================================
================================================================================
=========================
Install  63 Packages

Total size: 94 M
Installed size: 282 M
Downloading Packages:
BaseOS Packages Red Hat Enterprise Linux 10
439 kB/s | 3.7 kB     00:00
Importing GPG key 0xFD431D51:
 Userid     : "Red Hat, Inc. (release key 2) <security@redhat.com>"
 Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Importing GPG key 0x5A6340B3:
 Userid     : "Red Hat, Inc. (auxiliary key 3) <security@redhat.com>"
  Fingerprint: 7E46 2425 8C40 6535 D56D 6F13 5054 E4A4 5A63 40B3
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Installing       : perl-version-8:0.99.32-4.el10.x86_64
1/63
  Installing       : perl-File-Copy-2.41-512.el10.noarch
2/63
  Installing       : perl-CPAN-Meta-Requirements-2.143-11.el10.noarch
3/63
  Installing       : perl-Time-HiRes-4:1.9777-511.el10.x86_64
4/63
```

```
  Installing       : perl-JSON-PP-1:4.16-512.el10.noarch
5/63
  Installing       : perl-File-Compare-1.100.800-512.el10.noarch
6/63
  Installing       : perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
7/63
  Installing       : m4-1.4.19-11.el10.x86_64
8/63
  Installing       : make-1:4.4.1-9.el10.x86_64
9/63
  Installing       : bison-3.8.2-9.el10.x86_64
10/63
  Installing       : flex-2.6.4-19.el10.x86_64
11/63
  Installing       : perl-ExtUtils-Command-2:7.70-513.el10.noarch
12/63
  Installing       : perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
13/63
  Installing       : systemtap-sdt-devel-5.2-2.el10.x86_64
14/63
  Installing       : rust-toolset-srpm-macros-1.84.1-1.el10.noarch
15/63
  Installing       : qt6-srpm-macros-6.8.1-3.el10.noarch
16/63
  Installing       : python3-pip-23.3.2-7.el10.noarch
17/63
  Installing       : pyproject-srpm-macros-1.16.2-1.el10.noarch
18/63
  Installing       : perl-srpm-macros-1-57.el10.noarch
19/63
  Installing       : perl-lib-0.65-512.el10.x86_64
20/63
  Installing       : perl-doc-5.40.1-512.el10.noarch
21/63
  Installing       : perl-I18N-Langinfo-0.24-512.el10.x86_64
22/63
  Installing       : perl-Encode-Locale-1.05-31.el10.noarch
23/63
  Installing       : perl-ExtUtils-Constant-0.25-512.el10.noarch
24/63
  Installing       : perl-Devel-PPPort-3.72-512.el10.x86_64
25/63
  Installing       : perl-CPAN-Meta-YAML-0.018-512.el10.noarch
26/63
  Installing       : perl-CPAN-Meta-2.150010-511.el10.noarch
27/63
```

```
  Installing       : perl-Benchmark-1.25-512.el10.noarch
28/63
  Installing       : perl-Test-Harness-1:3.48-512.el10.noarch
29/63
  Installing       : perl-AutoSplit-5.74-512.el10.noarch
30/63
  Installing       : package-notes-srpm-macros-0.5-13.el10.noarch
31/63
  Installing       : openssl-devel-1:3.2.2-16.el10.x86_64
32/63
  Installing       : openblas-srpm-macros-2-19.el10.noarch
33/63
  Installing       : ocaml-srpm-macros-10-4.el10.noarch
34/63
  Installing       : lua-srpm-macros-1-15.el10.noarch
35/63
  Installing       : libzstd-devel-1.5.5-9.el10.x86_64
36/63
  Installing       : kernel-srpm-macros-1.0-25.el10.noarch
37/63
  Installing       : kernel-headers-6.12.0-55.9.1.el10_0.x86_64
38/63
  Installing       : libxcrypt-devel-4.4.36-10.el10.x86_64
39/63
  Installing       : glibc-devel-2.39-37.el10.x86_64
40/63
  Installing       : efi-srpm-macros-6-6.el10.noarch
41/63
  Installing       : dwz-0.15-7.el10.x86_64
42/63
  Installing       : cpp-14.2.1-7.el10.x86_64
43/63
  Installing       : gcc-14.2.1-7.el10.x86_64
44/63
  Installing       : gcc-plugin-annobin-14.2.1-7.el10.x86_64
45/63
  Installing       : cmake-filesystem-3.30.5-2.el10.x86_64
46/63
  Installing       : zlib-ng-compat-devel-2.2.3-1.el10.x86_64
47/63
  Installing       : elfutils-libelf-devel-0.192-5.el10.x86_64
48/63
  Installing       : annobin-docs-12.92-1.el10.noarch
49/63
  Installing       : annobin-plugin-gcc-12.92-1.el10.x86_64
50/63
```

```
  Installing       : fonts-srpm-macros-1:2.0.5-18.el10.noarch
51/63
  Installing       : forge-srpm-macros-0.4.0-6.el10.noarch
52/63
  Installing       : go-srpm-macros-3.6.0-4.el10.noarch
53/63
  Installing       : python-srpm-macros-3.12-9.1.el10.noarch
54/63
  Installing       : redhat-rpm-config-288-1.el10.noarch
55/63
  Running scriptlet: redhat-rpm-config-288-1.el10.noarch
55/63
  Installing       : python3-pyparsing-3.1.1-7.el10.noarch
56/63
  Installing       : systemtap-sdt-dtrace-5.2-2.el10.x86_64
57/63
  Installing       : perl-devel-4:5.40.1-512.el10.x86_64
58/63
  Installing       : perl-ExtUtils-Install-2.22-511.el10.noarch
59/63
  Installing       : perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
60/63
  Installing       : kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Running scriptlet: kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Installing       : python3-devel-3.12.9-1.el10.x86_64
62/63
  Installing       : patch-2.7.6-26.el10.x86_64
63/63
  Running scriptlet: patch-2.7.6-26.el10.x86_64
63/63
Installed products updated.

Installed:
  annobin-docs-12.92-1.el10.noarch              annobin-plugin-gcc-
12.92-1.el10.x86_64            bison-3.8.2-9.el10.x86_64
cmake-filesystem-3.30.5-2.el10.x86_64           cpp-14.2.1-
7.el10.x86_64
  dwz-0.15-7.el10.x86_64                        efi-srpm-macros-6-
6.el10.noarch                  elfutils-libelf-devel-0.192-
5.el10.x86_64   flex-2.6.4-19.el10.x86_64                       fonts-
srpm-macros-1:2.0.5-18.el10.noarch
  forge-srpm-macros-0.4.0-6.el10.noarch         gcc-14.2.1-
7.el10.x86_64                          gcc-plugin-annobin-14.2.1-
7.el10.x86_64     glibc-devel-2.39-37.el10.x86_64                go-
```

```
srpm-macros-3.6.0-4.el10.noarch
  kernel-devel-6.12.0-55.9.1.el10_0.x86_64      kernel-headers-6.12.0-
55.9.1.el10_0.x86_64        kernel-srpm-macros-1.0-25.el10.noarch
libxcrypt-devel-4.4.36-10.el10.x86_64           libzstd-devel-1.5.5-
9.el10.x86_64
  lua-srpm-macros-1-15.el10.noarch              m4-1.4.19-
11.el10.x86_64                          make-1:4.4.1-9.el10.x86_64
ocaml-srpm-macros-10-4.el10.noarch              openblas-srpm-macros-2-
19.el10.noarch
  openssl-devel-1:3.2.2-16.el10.x86_64          package-notes-srpm-
macros-0.5-13.el10.noarch      patch-2.7.6-26.el10.x86_64
perl-AutoSplit-5.74-512.el10.noarch             perl-Benchmark-1.25-
512.el10.noarch
  perl-CPAN-Meta-2.150010-511.el10.noarch       perl-CPAN-Meta-
Requirements-2.143-11.el10.noarch  perl-CPAN-Meta-YAML-0.018-
512.el10.noarch   perl-Devel-PPPort-3.72-512.el10.x86_64          perl-
Encode-Locale-1.05-31.el10.noarch
  perl-ExtUtils-Command-2:7.70-513.el10.noarch  perl-ExtUtils-Constant-
0.25-512.el10.noarch       perl-ExtUtils-Install-2.22-511.el10.noarch
perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch  perl-ExtUtils-Manifest-
1:1.75-511.el10.noarch
  perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch  perl-File-Compare-
1.100.800-512.el10.noarch       perl-File-Copy-2.41-512.el10.noarch
perl-I18N-Langinfo-0.24-512.el10.x86_64         perl-JSON-PP-1:4.16-
512.el10.noarch
  perl-Test-Harness-1:3.48-512.el10.noarch      perl-Time-HiRes-
4:1.9777-511.el10.x86_64          perl-devel-4:5.40.1-512.el10.x86_64
perl-doc-5.40.1-512.el10.noarch                 perl-lib-0.65-
512.el10.x86_64
  perl-srpm-macros-1-57.el10.noarch             perl-version-8:0.99.32-
4.el10.x86_64              pyproject-srpm-macros-1.16.2-1.el10.noarch
python-srpm-macros-3.12-9.1.el10.noarch         python3-devel-3.12.9-
1.el10.x86_64
  python3-pip-23.3.2-7.el10.noarch              python3-pyparsing-
3.1.1-7.el10.noarch             qt6-srpm-macros-6.8.1-3.el10.noarch
redhat-rpm-config-288-1.el10.noarch             rust-toolset-srpm-
macros-1.84.1-1.el10.noarch
  systemtap-sdt-devel-5.2-2.el10.x86_64         systemtap-sdt-dtrace-
5.2-2.el10.x86_64            zlib-ng-compat-devel-2.2.3-1.el10.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.vdizgQ/ontap-
mediator-1.11.0/ontap-mediator-1.11.0/install_20250715160240.log)
    This step takes several minutes. View progress in the log file.
    Sudoer config verified
```

```
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20250715160240.log)
+ WARNING: This system supports UEFI
           Secure Boot (SB) is currently disabled on this system.
           If SB is enabled in the future, SCST will not work unless
the following action is taken:
           Using the keys in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow
           instructions in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modu
le-signing
           to sign the SCST kernel module. Note that a reboot is
needed.
     SCST does not start automatically when Secure Boot is enabled and
not configured properly.

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
        OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
root@mediator_host:~# systemctl status ontap_mediator
● ontap_mediator.service - ONTAP Mediator
     Loaded: loaded (/etc/systemd/system/ontap_mediator.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
9s ago
 Invocation: 395e9479487e4e308be2ae030c800c7f
    Process: 28745
ExecStartPre=/opt/netapp/lib/ontap_mediator/tools/otm_logs_fs.sh
(code=exited, status=0/SUCCESS)
   Main PID: 28759 (python)
      Tasks: 1 (limit: 22990)
     Memory: 66.8M (peak: 68.8M)
        CPU: 2.865s
```

```
     CGroup: /system.slice/ontap_mediator.service
             └─28759 /opt/netapp/lib/ontap_mediator/pyenv/bin/python
/opt/netapp/lib/ontap_mediator/ontap_mediator/server

Jul 15 16:07:29 mediator_host systemd[1]: Starting
ontap_mediator.service - ONTAP Mediator...
Jul 15 16:07:29 mediator_host systemd[1]: Started
ontap_mediator.service - ONTAP Mediator.
root@mediator_host:~# systemctl status mediator-scst
● mediator-scst.service
     Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
15s ago
 Invocation: f1d3be6ca1f9492b943e61872676f384
    Process: 28653 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
    Process: 28738 ExecStartPost=/usr/sbin/modprobe scst_vdisk
(code=exited, status=0/SUCCESS)
   Main PID: 28696 (iscsi-scstd)
      Tasks: 1 (limit: 22990)
     Memory: 5.2M (peak: 35.2M)
        CPU: 547ms
     CGroup: /system.slice/mediator-scst.service
             └─28696 /usr/local/sbin/iscsi-scstd

Jul 15 16:07:28 mediator_host systemd[1]: Starting mediator-
scst.service...
Jul 15 16:07:29 mediator_host iscsi-scstd[28694]: max_data_seg_len
1048576, max_queued_cmds 2048
Jul 15 16:07:29 mediator_host scst[28653]: Loading and configuring SCST
Jul 15 16:07:29 mediator_host systemd[1]: Started mediator-
scst.service.
root@mediator_host:~#
```

UEFI 보안 부팅을 위한 보안 키 등록

ONTAP Mediator 1.4부터 UEFI 시스템에서 보안 부팅 메커니즘이 활성화됩니다. 보안 부팅이 활성화된 경우 설치 후 보안 키를 등록하기 위한 추가 단계를 거쳐야 합니다.

단계

1. SCST 커널 모듈에 서명하려면 README 파일의 지침을 따르세요.

   ```
   /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
   signing
   ```

2. 필요한 키를 찾습니다.

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

설치 후 시스템 출력에는 README 파일과 키 위치가 제공됩니다.

3. Mok 목록에 공개 키를 추가합니다.

```
mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

개인 키는 기본 위치에 두거나 안전한 위치로 옮길 수 있습니다. 부트 관리자가 공개 키를 사용할 수 있도록 공개 키를 기존 위치에 보관해야 합니다. 자세한 내용은 README.module-signing 파일을 참조하세요.

```
[root@hostname ~]# ls
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
README.module-signing scst_module_key.der scst_module_key.priv
```

4. 호스트를 재부팅하고 장치의 UEFI 부팅 관리자를 사용하여 새 MOK를 승인합니다. 제공된 암호 문구가 필요합니다. `mokutil` 유용성"UEFI 보안 부팅이 활성화된 경우 ONTAP mediator를 설치합니다" .

SCST 커널 모듈 서명

ONTAP Mediator가 설치된 후 systemctl status가 `mediator-scst` 실패(비활성)로 표시되는 경우 다음 단계에 따라 SCST 커널 모듈에 서명하세요.

단계

1. 빌드 프로세스 중에 공개/비공개 키 쌍이 생성됩니다. `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/` 다음 명령을 사용하여 디렉토리로 이동합니다.

```
[root@mediator-host ~]# ls
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
README.module-signing scst_module_key.der scst_module_key.priv
[root@mediator-host ~]#
```

2. 다음 명령을 실행하여 UEFI 키 저장소로 공개 키를 가져오는 프로세스를 시작합니다.

```
[root@mediator-host ~]# mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
input password:
input password again:

[root@mediator-host ~]#
```

3. mokutil 소프트웨어는 가져오기 프로세스 중에 이 키에 사용할 임시 비밀번호를 요청합니다.
4. 가져오기 프로세스가 시작되었는지 확인하십시오. `mokutil --list-new` 그리고 시스템을 재부팅하세요.

부트로더는 EFI MOK 관리자를 시작합니다.

5. 화면의 메뉴를 사용하여 SCST 커널 모듈 키를 켭니다. 부팅 후 실행 `systemctl status mediator-scst`. 서비스가 시작되면 SCST 커널 모듈이 서명됩니다.

ONTAP 중재자 설치 상태를 확인합니다

ONTAP Mediator를 설치한 후 성공적으로 실행되는지 확인하세요.

단계

1. ONTAP Mediator의 상태를 확인하세요:

   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. ONTAP Mediator에서 사용하는 포트를 확인하세요.

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp    0    0 0.0.0.0:31784    0.0.0.0:*       LISTEN

         tcp    0    0 0.0.0.0:3260     0.0.0.0:*       LISTEN

         tcp6   0    0 :::3260          :::*            LISTEN
```

설치 후 **ONTAP** 중재자 구성

ONTAP Mediator를 설치하고 실행한 후에는 ONTAP Mediator 기능을 사용하기 위해 ONTAP 스토리지 시스템에서 추가 구성 작업을 수행해야 합니다.

- MetroCluster IP 구성에서 ONTAP Mediator를 사용하려면 다음을 참조하세요. "MetroCluster IP 구성에서 ONTAP Mediator 구성" .
- SnapMirror 활성 동기화를 사용하려면 을 참조하십시오"ONTAP Mediator를 설치하고 ONTAP 클러스터 구성을 확인하세요.".

ONTAP 중재자 보안 정책을 구성합니다

ONTAP Mediator는 여러 가지 구성 가능한 보안 설정을 지원합니다. 모든 설정의 기본값은 `low_space_threshold_mib: 10` 읽기 전용 파일로 제공됩니다.

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

에 배치된 모든 값 `ontap_mediator.user_config.yaml` 는 기본값을 무시하고 모든 ONTAP 중재자 업그레이드에 대해 유지됩니다.

수정 후 `ontap_mediator.user_config.yaml` , ONTAP Mediator를 다시 시작하세요:

```
systemctl restart ontap_mediator
```

ONTAP 중재자 특성을 수정합니다

필요한 경우 이 섹션에 설명된 ONTAP 중재자 속성을 수정할 수 있습니다.

> ONTAP 중재자 업그레이드 중에 수정된 값이 유지되지 않으므로 의 다른 기본값은 `ontap_mediator.config.yaml` 변경되지 않아야 합니다.

필요한 변수를 파일에 복사하여 기본 설정을 재정의하여 ONTAP 중재자 특성을 `ontap_mediator.user_config.yaml` 수정합니다.

타사 SSL 인증서를 설치합니다

자체 서명된 기본 인증서를 타사 SSL 인증서로 대체해야 하는 경우 다음 파일에서 특정 특성을 수정합니다.

- `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`
- `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`

이러한 파일의 변수는 ONTAP Mediator에서 사용되는 인증서 파일을 제어하는 데 사용됩니다.

ONTAP 중재자 **1.9** 이상

다음 표에 나열된 기본 변수가 파일에 포함되어 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` 있습니다.

변수	경로
`cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`
`ca_key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key`
`ca_serial_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl`
`cert_valid_days`	`1095`
`x509_passin_pwd`	`pass:ontap`

- `cert_valid_days` 클라이언트 인증서의 만료를 설정하는 데 사용됩니다. 최대값은 3년(1095일)입니다.
- `x509_passin_pwd` 은 서명된 클라이언트 인증서의 암호입니다.

다음 표에 나열된 기본 변수가 파일에 포함되어 `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` 있습니다.

변수	경로
`mediator_cert`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`mediator_key`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`

ONTAP 중재자 **1.8** 이하

다음 표에 나열된 기본 변수가 파일에 포함되어 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` 있습니다.

변수	경로
cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt
ca_key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key
ca_serial_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- `cert_valid_days` 클라이언트 인증서의 만료를 설정하는 데 사용됩니다. 최대값은 3년(1095일)입니다.
- `x509_passin_pwd` 은 서명된 클라이언트 인증서의 암호입니다.

다음 표에 나열된 기본 변수가 파일에 포함되어 `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` 있습니다.

변수	경로
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt

이러한 속성을 수정한 경우 ONTAP Mediator를 다시 시작하여 변경 사항을 적용하세요. 기본 인증서를 타사 인증서로 교체하는 방법에 대한 자세한 지침은 을 참조하십시오"자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿉니다".

암호 공격 보호

다음 설정은 무차별 암호 추측 공격에 대한 보호 기능을 제공합니다.

기능을 활성화하려면 및 `retry_limit` 의 값을 `window_seconds` 설정합니다.

예:

- 추측을 위한 5분 창을 제공한 다음 이 수를 0으로 재설정합니다.

```
authentication_lock_window_seconds: 300
```

- 기간 내에 5번의 장애가 발생할 경우 계정을 잠급니다.

```
authentication_retry_limit: 5
```

- 각 시도를 거부하기 전에 발생하는 지연을 설정하여 무차별 암호 추측 공격의 영향을 줄입니다.

```
authentication_failure_delay_seconds: 5
```

```
authentication_failure_delay_seconds: 0   # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null  # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null          # number of retries to allow
before locking API access, null = unlimited
```

암호 복잡성 규칙

다음 필드는 ONTAP 중재자 API 사용자 계정의 암호 복잡성 규칙을 제어합니다.

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters

password_lowercase_chars: 1    # min. lowercase character

password_special_chars: 1      # min. non-letter, non-digit

password_nonletter_chars: 2    # min. non-letter characters (digits,
specials, anything)
```

사용 가능한 공간 제어

디스크에 필요한 여유 공간을 제어하는 설정이 `/opt/netapp/lib/ontap_mediator` 있습니다.

공간이 설정된 임계값보다 낮으면 서비스에서 경고 이벤트를 실행합니다.

```
low_space_threshold_mib: 10
```

예약 로그 공간을 제어합니다

reserve_log_space는 특정 설정에 의해 제어됩니다. 기본적으로 ONTAP Mediator 설치 시 로그를 위한 별도의 디스크 공간이 생성됩니다. 설치 프로그램은 ONTAP Mediator 로깅에 명시적으로 사용할 총 700MB의 디스크 공간을 가진 새로운 고정 크기 파일을 생성합니다.

이 기능을 비활성화하고 기본 디스크 공간을 사용하려면 다음 단계를 수행하십시오.

1. 다음 파일에서 reserve_log_space 값을 1에서 0으로 변경합니다.

   ```
   /opt/netapp/lib/ontap_mediator/tools/mediator_env
   ```

2. 중재자 다시 시작:

   a. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

      ```
      RESERVE_LOG_SPACE=0
      ```

   b. `systemctl restart ontap_mediator`

이 기능을 다시 활성화하려면 값을 0에서 1로 변경하고 중재자를 다시 시작하십시오.

디스크 공간 간에 전환하면 기존 로그가 지워지지 않습니다. 이전 로그는 모두 백업된 다음 중재자를 전환하고 다시 시작한 후 현재 디스크 공간으로 이동합니다.

ONTAP 중재자 관리

사용자 자격 증명 변경, 서비스 중지 및 재활성화, 서비스 상태 확인, 호스트 유지 관리를 위한 SCST 설치 또는 제거를 포함하여 ONTAP Mediator를 관리합니다. 또한 자체 서명된 인증서 다시 생성, 신뢰할 수 있는 타사 인증서로 대체, 인증서 관련 문제 해결 등의 인증서를 관리할 수 있습니다.

사용자 이름을 변경합니다

다음 절차를 사용하여 사용자 이름을 변경할 수 있습니다.

이 작업에 대해

ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행합니다.

이 명령에 액세스할 수 없는 경우 다음 예에 표시된 대로 전체 경로를 사용하여 명령을 실행해야 할 수 있습니다.

'/usr/local/bin/중재자_username'

단계

다음 옵션 중 하나를 선택하여 사용자 이름을 변경합니다.

- * option (a) * : 명령을 실행합니다 `mediator_change_user` 를 클릭하고 다음 예에 표시된 프롬프트에 응답합니다.

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
                  Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- * option(b) *: 다음 명령을 실행합니다.

  MDIATOR_USERNAME=중재자_PASSWORD=mediator2 MEDIATOR_NEW_USERNAME=mediatoradmin 중재자_CHANGE_USER

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME=mediatoradmin
mediator_change_user
 The account username has been modified successfully.
 [root@mediator-host ~]#
```

암호를 변경합니다

다음 절차를 사용하여 암호를 변경할 수 있습니다.

이 작업에 대해

ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행합니다.

이 명령에 액세스할 수 없는 경우 다음 예에 표시된 대로 전체 경로를 사용하여 명령을 실행해야 할 수 있습니다.

'/usr/local/bin/중재자_change_password'

단계

다음 옵션 중 하나를 선택하여 암호를 변경합니다.

- * option (a) * : 를 실행합니다 `mediator_change_password` 다음 예에 표시된 대로 명령을 실행하고 프롬프트에 응답합니다.

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
   Mediator API User Name: mediatoradmin
             Old Password:
             New Password:
         Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- * option(b) *: 다음 명령을 실행합니다.

```
MEDIATOR_USERNAME=mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

이 예제에서는 암호가 "mediator1"에서 "mediator2"로 변경되었음을 보여 줍니다.

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
 The password has been updated successfully.
 [root@mediator-host ~]#
```

ONTAP 중재자 중단

ONTAP Mediator를 중지하려면 다음 단계를 수행하세요.

단계

1. ONTAP 중재자 중단:

```
systemctl stop ontap_mediator
```

2. SCST 중지:

```
systemctl stop mediator-scst
```

3. ONTAP Mediator 및 SCST 비활성화:

```
systemctl disable ontap_mediator mediator-scst
```

ONTAP Mediator 다시 활성화

ONTAP Mediator를 다시 활성화하려면 다음 단계를 수행하세요.

단계

1. ONTAP Mediator 및 SCST 활성화:

```
systemctl enable ontap_mediator mediator-scst
```

2. SCST 시작:

```
systemctl start mediator-scst
```

3. ONTAP 중재자 시작:

```
systemctl start ontap_mediator
```

ONTAP Mediator가 정상인지 확인하세요

ONTAP Mediator를 설치한 후 성공적으로 실행되는지 확인하세요.

단계

1. ONTAP Mediator의 상태를 확인하세요:

   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. ONTAP Mediator에서 사용하는 포트를 확인하세요.

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

ONTAP Mediator 제거

필요한 경우 ONTAP Mediator를 제거할 수 있습니다.

시작하기 전에

ONTAP을 제거하기 전에 ONTAP Mediator와 ONTAP의 연결을 해제해야 합니다.

이 작업에 대해

ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행합니다.

이 명령에 액세스할 수 없는 경우 다음 예에 표시된 대로 전체 경로를 사용하여 명령을 실행해야 할 수 있습니다.

'/usr/local/bin/uninstall_ontap_중재자'

단계

1. ONTAP Mediator 제거:

   uninstall_ontap_중재자

```
 [root@mediator-host ~]# uninstall_ontap_mediator

 ONTAP Mediator: Self Extracting Uninstaller

 + Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
 + Remove successful.
 [root@mediator-host ~]#
```

자체 서명된 임시 인증서를 다시 생성합니다

ONTAP mediator 1.7부터 다음 절차에 따라 자체 서명된 임시 인증서를 다시 생성할 수 있습니다.

이 절차는 ONTAP mediator 1.7 이상을 실행하는 시스템에서만 지원됩니다.

이 작업에 대해

- ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행합니다.
- ONTAP Mediator를 설치한 후 호스트 이름이나 호스트의 IP 주소가 변경되어 생성된 자체 서명 인증서가 더 이상 사용되지 않는 경우에만 이 작업을 수행할 수 있습니다.
- 임시 자체 서명된 인증서가 신뢰할 수 있는 타사 인증서로 대체되면 이 작업을 사용하여 인증서를 다시 생성합니다. 자체 서명된 인증서가 없으면 이 절차가 실패합니다.

단계

현재 호스트에 대해 자체 서명된 새 임시 인증서를 다시 생성하려면 다음 단계를 수행하십시오.

1. ONTAP Mediator를 다시 시작하세요:

   ```
   ./make_self_signed_certs.sh overwrite
   ```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
.................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

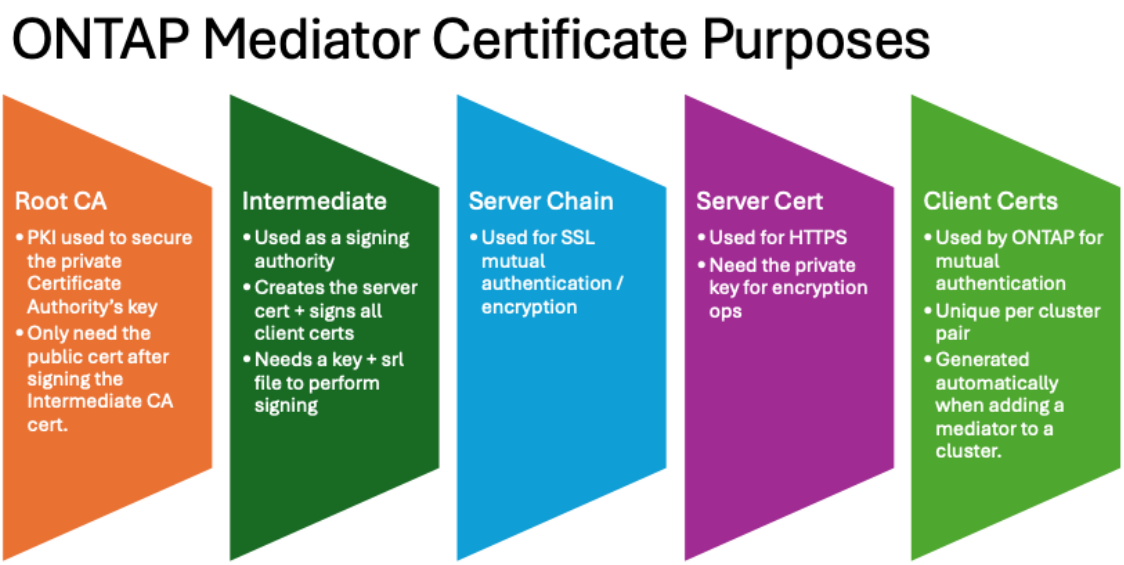
자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿉니다

지원되는 경우 자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿀 수 있습니다.

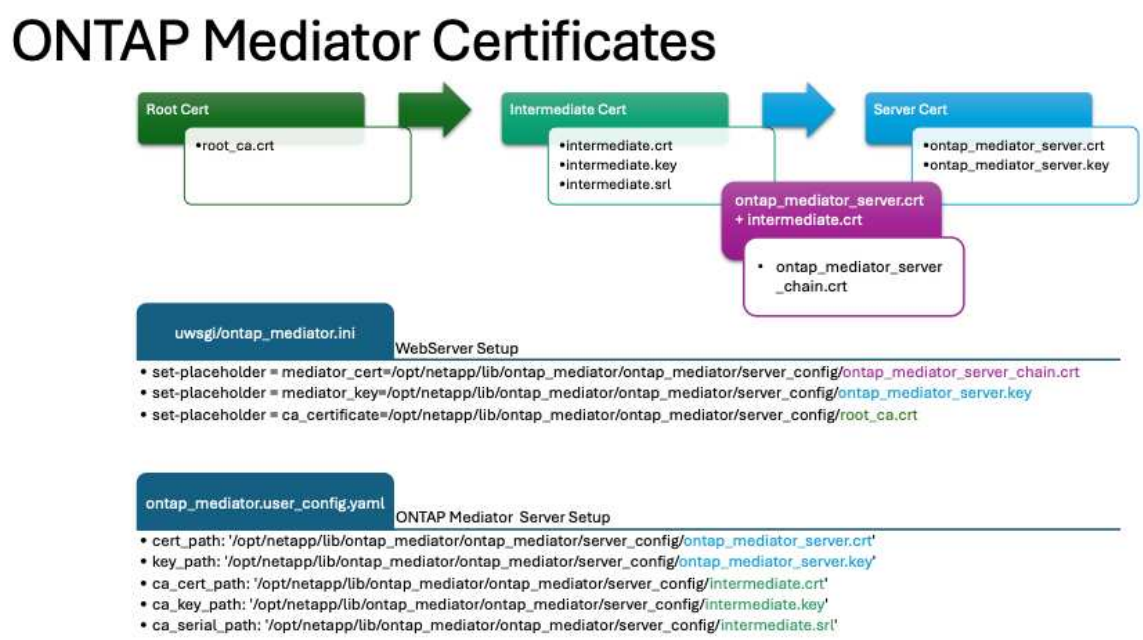
- 타사 인증서는 ONTAP 9.16.1 및 일부 이전 ONTAP 패치 릴리스에서만 지원됩니다. 을 "NetApp 버그 온라인 버그 ID CONTAP-243278"참조하십시오.
- 타사 인증서는 ONTAP mediator 1.7 이상을 실행하는 시스템에서만 지원됩니다.

이 작업에 대해

- ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행합니다.
- 생성된 자체 서명된 인증서를 신뢰할 수 있는 하위 CA(인증 기관)에서 가져온 인증서로 교체해야 하는 경우 이 작업을 수행할 수 있습니다. 이렇게 하려면 신뢰할 수 있는 PKI(공개 키 인프라) 권한에 액세스할 수 있어야 합니다.
- 다음 이미지는 각 ONTAP 중재자 인증서의 용도를 보여 줍니다.



- 다음 이미지는 웹 서버 설정과 ONTAP Mediator 설정에 대한 구성을 보여줍니다.



1단계**: CA** 인증서를 발급하는 타사로부터 인증서를 얻습니다

다음 절차를 사용하여 PKI 기관으로부터 인증서를 얻을 수 있습니다.

다음 예제에서는 자체 서명된 인증서 액터를 에 있는 타사 인증서 액터로 바꾸는 방법을 보여 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/` 줍니다.

이 예는 ONTAP Mediator에 필요한 인증서에 대한 필수 기준을 보여줍니다. 이 절차와 다른 방법으로 PKI 기관으로부터 인증서를 얻을 수 있습니다. 비즈니스 요구에 따라 절차를 조정합니다.

ONTAP 중재자 **1.9** 이상

1. PKI 기관에서 인증서를 생성하기 위해 사용할 개인 키와 구성 파일을 `openssl_ca.cnf` 만듭니다 `intermediate.key`.

   a. 개인 키를 `intermediate.key`생성합니다.

      ▪ 예 *

```
openssl genrsa -aes256 -out intermediate.key 4096
```

   a. 구성 파일 `openssl_ca.cnf` (에 위치 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`)은 생성된 인증서에 있어야 하는 속성을 정의합니다.

2. 개인 키 및 구성 파일을 사용하여 인증서 서명 요청을 만듭니다 `intermediate.csr`.

   ◦ 예: *

```
openssl req -key <private_key_name>.key -new -out
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key intermediate.key
-new -config openssl_ca.cnf -out intermediate.csr
Enter pass phrase for intermediate.key:
[root@scs000216655 server_config]# cat intermediate.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

3. PKI 기관에 인증서 서명 요청을 보내 `intermediate.csr` 서명을 받습니다.

   PKI 기관은 요청을 검증하고 서명합니다. `.csr` , 인증서 생성 `intermediate.crt` . 또한 다음을 얻어야 합니다. `root_ca.crt` 서명한 인증서 `intermediate.crt` PKI 기관의 인증서.

> SnapMirror Business Continuity(SM-BC) 클러스터의 경우 다음을 추가해야 합니다. `intermediate.crt` 그리고 `root_ca.crt` ONTAP 클러스터에 대한 인증서.
> 보다"SnapMirror Active Sync를 위한 ONTAP Mediator 및 클러스터 구성" .

ONTAP 중재자 **1.8** 이하

1. PKI 기관에서 인증서를 생성하기 위해 사용할 개인 키와 구성 파일을 `openssl_ca.cnf` 만듭니다 `ca.key`.

   a. 개인 키를 `ca.key`생성합니다.

      ▪ 예 *

```
openssl genrsa -aes256 -out ca.key 4096
```

   a. 구성 파일 `openssl_ca.cnf` (에 위치 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.c`

nf)은 생성된 인증서에 있어야 하는 속성을 정의합니다.

2. 개인 키 및 구성 파일을 사용하여 인증서 서명 요청을 만듭니다 ca.csr.

◦ 예: *

```
openssl req -key <private_key_name>.key -new -out
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key ca.key -new
-config openssl_ca.cnf -out ca.csr
Enter pass phrase for ca.key:
[root@scs000216655 server_config]# cat ca.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

3. PKI 기관에 인증서 서명 요청을 보내 ca.csr 서명을 받습니다.

PKI 권한은 요청을 확인하고 에 서명하여 .csr`인증서를 `ca.crt`생성합니다. 또한 PKI 기관으로부터 인증서를 얻어야 `root_ca.crt that signed the `ca.crt 합니다.

SM-BC(SnapMirror Business Continuity) 클러스터의 경우 및 인증서를 ONTAP 클러스터에 추가해야 ca.crt root_ca.crt 합니다. 을 "SnapMirror Active Sync를 위한 ONTAP Mediator 및 클러스터 구성"참조하십시오.

2단계**:** 타사 **CA** 인증서로 서명하여 서버 인증서를 생성합니다

ONTAP 중재자 **1.9** 이상

서버 인증서는 개인 키 및 타사 인증서로 `intermediate.crt` 서명해야 `intermediate.key` 합니다. 또한 구성 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` 파일에는 OpenSSL에서 발급한 서버 인증서에 필요한 속성을 지정하는 특정 특성이 포함되어 있습니다.

다음 명령을 사용하여 서버 인증서를 생성할 수 있습니다.

단계

1. 서버 CSR(인증서 서명 요청)을 생성하려면 폴더에서 다음 명령을 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` 실행합니다.

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
ontap_mediator_server.csr
```

2. CSR에서 서버 인증서를 생성하려면 폴더에서 다음 명령을 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` 실행합니다.

> 이러한 파일은 PKI 기관에서 가져왔습니다. 다른 인증서 이름을 사용하는 경우 `intermediate.crt` 및 를 `intermediate.key` 관련 파일 이름으로 바꿉니다.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA
intermediate.crt -CAkey intermediate.key -CAcreateserial -sha512 -days 1095
-req -in ontap_mediator_server.csr -out ontap_mediator_server.crt
```

◦ 이 `-CAcreateserial` 옵션은 파일을 생성하는 데 `intermediate.srl` 사용됩니다.

ONTAP 중재자 **1.8** 이하

서버 인증서는 개인 키 및 타사 인증서로 `ca.crt` 서명해야 `ca.key` 합니다. 또한 구성 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` 파일에는 OpenSSL에서 발급한 서버 인증서에 필요한 속성을 지정하는 특정 특성이 포함되어 있습니다.

다음 명령을 사용하여 서버 인증서를 생성할 수 있습니다.

단계

1. 서버 CSR(인증서 서명 요청)을 생성하려면 폴더에서 다음 명령을 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` 실행합니다.

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
ontap_mediator_server.csr
```

2. CSR에서 서버 인증서를 생성하려면 폴더에서 다음 명령을 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` 실행합니다.

> 이러한 파일은 PKI 기관에서 가져왔습니다. 다른 인증서 이름을 사용하는 경우 `ca.crt` 및 를 `ca.key` 관련 파일 이름으로 바꿉니다.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt
-CAkey ca.key -CAcreateserial -sha512 -days 1095 -req -in
ontap_mediator_server.csr -out ontap_mediator_server.crt
```

◦ 이 `-CAcreateserial` 옵션은 파일을 생성하는 데 `ca.srl` 사용됩니다.

3단계**: ONTAP** 중재자 구성에서 새로운 타사 **CA** 인증서와 서버 인증서를 교체합니다

ONTAP Mediator 1.10 이상

인증서 구성은 다음 위치에 있는 구성 파일에서 ONTAP Mediator에 제공됩니다. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` . 이 파일에는 다음과 같은 속성이 포함되어 있습니다.

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path` 및 `key_path` 서버 인증서 변수입니다.
- `ca_cert_path`, `ca_key_path`, 및 `ca_serial_path` CA 인증서 변수입니다.

단계

1. 모든 `intermediate.*` 파일을 타사 인증서로 바꿉니다.
2. 및 인증서에서 인증서 체인을 `intermediate.crt` `ontap_mediator_server.crt` 생성합니다.

   ```
   cat ontap_mediator_server.crt intermediate.crt >
   ontap_mediator_server_chain.crt
   ```

3. 업데이트 `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` 파일.

   값을 업데이트합니다 `ssl_keyfile` , `ssl_certfile` , 그리고 `ssl_ca_certs` :

   ```
   ssl_keyfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key

   ssl_certfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt

   ssl_ca_certs:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

- 그만큼 `ssl_keyfile` 값은 키 경로입니다 `ontap_mediator_server.crt` 파일입니다 `ontap_mediator_server.key` .
- 그만큼 `ssl_certfile` 값은 경로입니다 `ontap_mediator_server_chain.crt` 파일.
- 그만큼 `ssl_ca_certs` 값은 경로입니다 `root_ca.crt` 파일.

4. 새로 생성된 인증서의 다음 특성이 올바르게 설정되었는지 확인합니다.
   - Linux 그룹 소유자: `netapp:netapp`
   - Linux 권한: `600`
5. ONTAP Mediator를 다시 시작하세요:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 및 1.9

인증서 구성은 다음 위치에 있는 구성 파일에서 ONTAP Mediator에 제공됩니다. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` . 이 파일에는 다음과 같은 속성이 포함되어 있습니다.

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path` 및 `key_path` 서버 인증서 변수입니다.
- `ca_cert_path`, `ca_key_path`, 및 `ca_serial_path` CA 인증서 변수입니다.

단계

1. 모든 `intermediate.*` 파일을 타사 인증서로 바꿉니다.
2. 및 인증서에서 인증서 체인을 `intermediate.crt` `ontap_mediator_server.crt` 생성합니다.

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

3. `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`파일을 업데이트합니다.

, 및 의 값을 `mediator_cert` `mediator_key` `ca_certificate`업데이트합니다.

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

    - `mediator_cert`값은 파일의 경로입니다. `ontap_mediator_server_chain.crt`
    - `mediator_key value`는 파일의 키 경로입니다. `ontap_mediator_server.crt` `ontap_mediator_server.key`
    - `ca_certificate`값은 파일의 경로입니다. `root_ca.crt`

4. 새로 생성된 인증서의 다음 특성이 올바르게 설정되었는지 확인합니다.
    - Linux 그룹 소유자: `netapp:netapp`
    - Linux 권한: `600`
5. ONTAP Mediator를 다시 시작하세요:

```
systemctl restart ontap_mediator
```

ONTAP 중재자 **1.8** 이하

인증서 구성은 다음 위치에 있는 구성 파일에서 ONTAP Mediator에 제공됩니다. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` . 이 파일에는 다음과 같은 속성이 포함되어 있습니다.

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- `cert_path` 및 `key_path` 서버 인증서 변수입니다.
- `ca_cert_path`, `ca_key_path`, 및 `ca_serial_path` CA 인증서 변수입니다.

단계

1. 모든 `ca.*` 파일을 타사 인증서로 바꿉니다.
2. 및 인증서에서 인증서 체인을 `ca.crt` `ontap_mediator_server.crt` 생성합니다.

   ```
   cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
   ```

3. `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`파일을 업데이트합니다.

   , 및 의 값을 `mediator_cert` `mediator_key` `ca_certificate`업데이트합니다.

   ```
   set-placeholder = mediator_cert =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server_chain.crt

   set-placeholder = mediator_key =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server.key

   set-placeholder = ca_certificate =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

   - `mediator_cert`값은 파일의 경로입니다. `ontap_mediator_server_chain.crt`
   - `mediator_key value`는 파일의 키 경로입니다. `ontap_mediator_server.crt` `ontap_mediator_server.key`
   - `ca_certificate`값은 파일의 경로입니다. `root_ca.crt`
4. 새로 생성된 인증서의 다음 특성이 올바르게 설정되었는지 확인합니다.
   - Linux 그룹 소유자: `netapp:netapp`
   - Linux 권한: `600`
5. ONTAP Mediator를 다시 시작하세요:

   ```
   systemctl restart ontap_mediator
   ```

4단계**:** 타사 인증서에 다른 경로나 이름을 사용할 수도 있습니다

ONTAP Mediator 1.10 이상

이 아닌 다른 이름을 가진 타사 인증서를 사용하거나 타사 인증서를 다른 위치에 저장할 수 `intermediate.*` 있습니다.

단계

1. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`파일의 기본 변수 값을 재정의하도록 파일을 `ontap_mediator.config.yaml` 구성합니다.

   PKI 권한으로부터 얻은 `intermediate.crt` 개인 키를 해당 위치에 저장하면 `intermediate.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` `ontap_mediator.user_config.yaml` 파일은 다음 예제와 같이 표시됩니다.

   > 인증서에 서명하는 데 사용한 경우 `intermediate.crt` `ontap_mediator_server.crt` `intermediate.srl` 파일이 생성됩니다. 자세한 내용은 을 2단계: 타사 CA 인증서로 서명하여 서버 인증서를 생성합니다 참조하십시오.

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. 인증서 구조를 사용하는 경우 `root_ca.crt` 인증서는 다음을 제공합니다. `intermediate.crt` 서명하는 인증서 `ontap_mediator_server.crt` 인증서, 인증서 체인을 만듭니다. `intermediate.crt` 그리고 `ontap_mediator_server.crt` 인증서:

> ⓘ 절차의 앞부분에 있는 PKI 기관으로부터 및 인증서를 받아야 `intermediate.crt` `ontap_mediator_server.crt` 합니다.

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. 업데이트 `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` 파일.

값을 업데이트합니다 `ssl_keyfile` , `ssl_certfile` , 그리고 `ssl_ca_certs` :

```
ssl_keyfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

ssl_certfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

ssl_ca_certs:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- 그만큼 `ssl_keyfile` 값은 키 경로입니다 `ontap_mediator_server.crt` 파일입니다 `ontap_mediator_server.key` .
- 그만큼 `ssl_certfile` 값은 경로입니다 `ontap_mediator_server_chain.crt` 파일.
- 그만큼 `ssl_ca_certs` 값은 경로입니다 `root_ca.crt` 파일.

> SnapMirror Business Continuity(SM-BC) 클러스터의 경우 다음을 추가해야 합니다. `intermediate.crt` 그리고 `root_ca.crt` ONTAP 클러스터에 대한 인증서. 보다"SnapMirror Active Sync를 위한 ONTAP Mediator 및 클러스터 구성" .

c. 새로 생성된 인증서의 다음 특성이 올바르게 설정되었는지 확인합니다.

- Linux 그룹 소유자: `netapp:netapp`
- Linux 권한: `600`

2. 구성 파일에서 인증서가 업데이트되면 ONTAP Mediator를 다시 시작합니다.

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 및 1.9

이 아닌 다른 이름을 가진 타사 인증서를 사용하거나 타사 인증서를 다른 위치에 저장할 수 `intermediate.*` 있습니다.

단계

1. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`파일의 기본 변수 값을 재정의하도록 파일을 `ontap_mediator.config.yaml` 구성합니다.

   PKI 권한으로부터 얻은 `intermediate.crt` 개인 키를 해당 위치에 저장하면 `intermediate.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` `ontap_mediator.user_config.yaml` 파일은 다음 예제와 같이 표시됩니다.

> 인증서에 서명하는 데 사용한 경우 `intermediate.crt` `ontap_mediator_server.crt` `intermediate.srl` 파일이 생성됩니다. 자세한 내용은 을 2단계: 타사 CA 인증서로 서명하여 서버 인증서를 생성합니다 참조하십시오.

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. 인증서 구조를 사용하는 경우 `root_ca.crt` 인증서는 다음을 제공합니다. `intermediate.crt` 서명하는 인증서 `ontap_mediator_server.crt` 인증서, 인증서 체인을 만듭니다. `intermediate.crt` 그리고 `ontap_mediator_server.crt` 인증서:

> ⓘ 절차의 앞부분에 있는 PKI 기관으로부터 및 인증서를 받아야 `intermediate.crt` `ontap_mediator_server.crt` 합니다.

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`파일을 업데이트합니다.

, 및 의 값을 mediator_cert mediator_key `ca_certificate`업데이트합니다.

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- `mediator_cert`값은 파일의 경로입니다. `ontap_mediator_server_chain.crt`
- `mediator_key`값은 파일의 키 경로입니다. `ontap_mediator_server.crt` `ontap_mediator_server.key`
- `ca_certificate`값은 파일의 경로입니다. `root_ca.crt`

> SnapMirror Business Continuity(SM-BC) 클러스터의 경우 다음을 추가해야 합니다. `intermediate.crt` 그리고 `root_ca.crt` ONTAP 클러스터에 대한 인증서. 보다"SnapMirror Active Sync를 위한 ONTAP Mediator 및 클러스터 구성" .

c. 새로 생성된 인증서의 다음 특성이 올바르게 설정되었는지 확인합니다.

- Linux 그룹 소유자: `netapp:netapp`
- Linux 권한: `600`

2. 구성 파일에서 인증서가 업데이트되면 ONTAP Mediator를 다시 시작합니다.

```
systemctl restart ontap_mediator
```

ONTAP 중재자 **1.8** 이하

이 아닌 다른 이름을 가진 타사 인증서를 사용하거나 타사 인증서를 다른 위치에 저장할 수 `ca.*` 있습니다.

단계

1. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`파일의 기본 변수 값을 재정의하도록 파일을 `ontap_mediator.config.yaml` 구성합니다.

   PKI 권한으로부터 얻은 `ca.crt` 개인 키를 해당 위치에 저장하면 `ca.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` `ontap_mediator.user_config.yaml` 파일은 다음 예제와 같이 표시됩니다.

> 인증서에 서명하는 데 사용한 경우 `ca.crt` `ontap_mediator_server.crt` `ca.srl` 파일이 생성됩니다. 자세한 내용은 을 2단계: 타사 CA 인증서로 서명하여 서버 인증서를 생성합니다 참조하십시오.

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

a. 인증서가 인증서를 서명하는 인증서를 제공하는 인증서 구조를 사용하는 경우 `root_ca.crt` `ca.crt` `ontap_mediator_server.crt` 및 인증서에서 인증서 체인을 만듭니다 `ca.crt` `ontap_mediator_server.crt` .

> 절차의 앞부분에 있는 PKI 기관으로부터 및 인증서를 받아야 `ca.crt` `ontap_mediator_server.crt` 합니다.

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

b. `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`파일을 업데이트합니다.

, 및 의 값을 `mediator_cert` `mediator_key` `ca_certificate`업데이트합니다.

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
```

```
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- `mediator_cert`값은 파일의 경로입니다. `ontap_mediator_server_chain.crt`
- `mediator_key`값은 파일의 키 경로입니다. `ontap_mediator_server.crt` `ontap_mediator_server.key`
- `ca_certificate`값은 파일의 경로입니다. `root_ca.crt`

> SM-BC(SnapMirror Business Continuity) 클러스터의 경우 및 인증서를 ONTAP 클러스터에 추가해야 `ca.crt` `root_ca.crt` 합니다. 을 "SnapMirror Active Sync를 위한 ONTAP Mediator 및 클러스터 구성"참조하십시오.

c. 새로 생성된 인증서의 다음 특성이 올바르게 설정되었는지 확인합니다.

- Linux 그룹 소유자: `netapp:netapp`
- Linux 권한: `600`

2. 구성 파일에서 인증서가 업데이트되면 ONTAP Mediator를 다시 시작합니다.

```
systemctl restart ontap_mediator
```

인증서 관련 문제 해결

인증서의 특정 속성을 확인할 수 있습니다.

인증서 만료 여부를 확인합니다

다음 명령을 사용하여 인증서 유효 범위를 식별합니다.

ONTAP 중재자 **1.9** 이상

```
[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

ONTAP 중재자 **1.8** 이하

```
[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

CA 인증에서 **X509v3** 확장을 확인합니다

다음 명령을 사용하여 CA 인증에서 X509v3 확장을 확인합니다.

ONTAP 중재자 **1.9** 이상

에 `openssl_ca.cnf` 정의된 속성이 **v3_ca** 에서와 같이 `X509v3 extensions` `intermediate.crt` 표시됩니다.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

ONTAP 중재자 **1.8** 이하

에 `openssl_ca.cnf` 정의된 속성이 **v3_ca** 에서와 같이 `X509v3 extensions` `ca.crt` 표시됩니다.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

서버 인증서 및 주체 대체 이름에서 **X509v3** 확장을 확인합니다

를 클릭합니다 `v3_req` 에 정의된 속성 `openssl_server.cnf` 구성 파일은 로 표시됩니다 `X509v3 extensions` 인증서에 입력합니다.

다음 예에서는 변수를 얻을 수 있습니다. `alt_names` 명령을 실행하여 섹션을 만듭니다. `hostname -A` 그리고 `hostname -I` ONTAP Mediator가 설치된 Linux VM에서.

변수의 올바른 값은 네트워크 관리자에게 문의하십시오.

ONTAP 중재자 **1.9** 이상

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

ONTAP 중재자 **1.8** 이하

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

개인 키가 인증서와 일치하는지 확인합니다

특정 개인 키가 인증서와 일치하는지 확인할 수 있습니다.

키와 인증서에 각각 다음 OpenSSL 명령을 사용합니다.

ONTAP 중재자 **1.9** 이상

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

ONTAP 중재자 **1.8** 이하

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
ca.key | openssl md5
Enter pass phrase for ca.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
ca.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

를 누릅니다 `-modulus` 특성 일치 모두에 대해 개인 키와 인증서 쌍이 호환되며 서로 작동할 수 있음을 나타냅니다.

서버 인증서가 특정 **CA** 인증서에서 생성되었는지 확인합니다

다음 명령을 사용하여 서버 인증서가 특정 CA 인증서에서 생성되었는지 확인할 수 있습니다.

ONTAP 중재자 **1.9** 이상

```
[root@mediator_host server_config]# openssl verify -CAfile root_ca.crt
--untrusted intermediate.crt ontap_mediator_server.crt
ontap_mediator_server.crt: OK
[root@mediator_host server_config]#
```

ONTAP 중재자 **1.8** 이하

```
[root@mediator_host server_config]# openssl verify -CAfile ca.crt
ontap_mediator_server.crt
ontap_mediator_server.crt: OK
```

OCSP(Online Certificate Status Protocol) 유효성 검사가 사용 중인 경우 명령을 "OpenSSL - 확인"사용합니다.

ONTAP 중재자를 위한 호스트 OS를 유지 관리합니다

최적의 성능을 얻으려면 ONTAP Mediator의 호스트 OS를 정기적으로 유지 관리하세요.

호스트를 재부팅합니다

클러스터가 정상일 때만 호스트를 재부팅하세요. ONTAP Mediator가 오프라인인 동안에는 클러스터가 장애에 대응할 수 없습니다. 재부팅하기 전에 유지관리 시간을 설정하세요.

ONTAP Mediator는 재부팅 중에 자동으로 다시 시작되고 ONTAP 클러스터와 이전에 구성된 관계를 다시 입력합니다.

호스트 패키지 업데이트

커널을 제외한 모든 라이브러리나 yum 패키지를 업데이트합니다. 변경 사항을 적용하려면 필요한 경우 호스트를 재부팅하세요. 호스트를 재부팅하기 전에 서비스 창을 예약하세요.

를 설치하는 경우 `yum-utils` 패키지를 사용하려면 를 사용합니다 `needs-restarting` 명령을 사용하여 패키지 변경 사항을 탐지하려면 재부팅해야 합니다.

변경 사항이 즉시 적용되지 않으므로 ONTAP Mediator 종속성을 업데이트한 후 재부팅하세요.

호스트 **OS** 커널 업그레이드

SCST는 사용 중인 커널에 맞게 컴파일해야 합니다. OS를 업데이트하려면 유지관리 시간을 예약해야 합니다.

단계

호스트 OS 커널을 업그레이드하려면 다음 단계를 따르세요.

> 커널을 업그레이드하기 전에 OS와 ONTAP Mediator 버전이 호환되는지 확인하세요. 지원되는 버전은 다음을 참조하세요."OS 지원 매트릭스" .

1. ONTAP 중재자를 중단하세요.
2. SCST 패키지를 제거하려면 다음을 참조하세요.호스트 유지관리 수행 . (SCST는 업그레이드 메커니즘을 제공하지 않습니다.)
3. OS를 업그레이드하고 재부팅합니다.
4. SCST 패키지를 다시 설치합니다.
5. ONTAP Mediator를 다시 활성화합니다.

호스트 유지관리 수행

VM 커널을 업그레이드하면 SCST 모듈과의 호환성 문제가 발생할 수 있습니다. SCST를 수동으로 제거했다가 다시 설치합니다.

1단계: SCST 제거

SCST를 제거하려면 ONTAP Mediator 버전용 tar 번들을 사용하세요.

단계

1. 다음 표에 표시된 대로 적절한 SCST 번들을 다운로드하고 압축을 풉니다.

이 버전의 경우…	이 tar 번들을 사용합니다…
ONTAP 중재자 1.11	scst-3.9.tar.gz
ONTAP 중재자 1.10	scst-3.9.tar.gz
ONTAP 중재자 1.9.1	scst-3.8.0.tar.bz2
ONTAP 중재자 1.9	scst-3.8.0.tar.bz2
ONTAP 중재자 1.8	scst-3.8.0.tar.bz2
ONTAP 중재자 1.7	scst - 3.7.0.tar.bz2
ONTAP 중재자 1.6	scst - 3.7.0.tar.bz2
ONTAP 중재자 1.5	scst - 3.6.0.tar.bz2
ONTAP 중재자 1.4	scst - 3.6.0.tar.bz2
ONTAP 중재자 1.3	scst - 3.5.0.tar.bz2
ONTAP 중재자 1.1	scst - 3.4.0.tar.bz2
ONTAP 중재자 1.0	scst - 3.3.0.tar.bz2

   a. 오픈 소스 패키지에 액세스하세요"SCST 소스포지 다운로드" .
   b. *출시된 버전 다운로드*를 선택하세요.
   c. 번들을 VM으로 추출합니다.
2. 다음 제거 명령을 실행하세요. `scst` 예배 규칙서:
   a. `systemctl stop mediator-scst`
   b. `make scstadm_uninstall`
   c. `make iscsi_uninstall`
   d. `make usr_uninstall`
   e. `make scst_uninstall`
   f. `depmod`

2단계**: SCST** 설치

SCST를 수동으로 설치하려면 ONTAP Mediator의 설치된 버전에 사용되는 SCST tar 번들이 필요합니다(참조).SCST 테이블).

ONTAP Mediator를 설치하기 전에 이 단계를 수행하세요. 사용 중인 SCST 버전이 ONTAP Mediator 설치 프로그램과 함께 제공되는 버전보다 최신인 경우 설치 프로그램은 이 단계를 건너뜁니다.

1. 다음 설치 명령을 실행하세요. `scst` 예배 규칙서:
   a. `make 2release`
   b. `make scst_install`
   c. `make usr_install`
   d. `make iscsi_install`
   e. `make scstadm_install`
   f. `depmod`

      처음으로 설치를 수행하고 ONTAP Mediator를 미리 설치하려면 다음 단계로 넘어가기 전에 다음 명령을 실행하세요.

      ```
      mkdir -p
      /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
      ```

   g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/`
   h. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`

      처음 설치할 때 ONTAP Mediator보다 SCST를 먼저 설치한 경우 이 단계를 건너뜁니다. 설치 프로그램은 관련 SCST 패치를 적용합니다.

2. 선택적으로 Secure Boot가 활성화되어 있는 경우 재부팅하기 전에 다음 단계를 수행하십시오.
   a. 각 파일 이름을 결정하세요 `scst_vdisk` , `scst` , 그리고 `iscsi_scst` 모듈:

      ```
      [root@localhost ~]# modinfo -n scst_vdisk
      [root@localhost ~]# modinfo -n scst
      [root@localhost ~]# modinfo -n iscsi_scst
      ```

   b. 커널 릴리스를 확인합니다.

      ```
      [root@localhost ~]# uname -r
      ```

   c. 각 모듈 파일에 커널을 서명합니다.

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.der \
_module-filename_
```

d. 펌웨어와 함께 UEFI 키를 설치합니다.

UEFI 키 설치 지침은 다음 웹 사이트에서 확인할 수 있습니다.

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
```

생성된 UEFI 키는 다음 위치에 있습니다.

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

3. 시스템을 재부팅하세요:

```
reboot
```

호스트가 호스트 이름 또는 **IP**로 변경됩니다

이 작업에 대해

- ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행합니다.
- ONTAP Mediator를 설치한 후 호스트 이름이나 IP 주소가 변경되어 자체 서명 인증서가 더 이상 유효하지 않은 경우에만 이 작업을 수행하세요.
- 임시 자체 서명 인증서가 신뢰할 수 있는 타사 인증서로 대체된 후에는 이 작업을 사용하여 인증서를 다시 생성할 수 없습니다. 자체 서명된 인증서가 없으면 이 절차를 사용할 수 없습니다.

단계

현재 호스트에 대한 임시 자체 서명 인증서를 만듭니다.

1. ONTAP Mediator를 다시 시작하세요:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
.................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

ONTAP System Manager를 사용한 MetroCluster IP 사이트 관리에 대해 알아보세요

MetroCluster 구성은 별도의 위치에 있는 두 ONTAP 클러스터 간에 데이터와 구성을 동기식으로 미러링합니다. ONTAP 9.8부터 System Manager를 사용하여 MetroCluster IP 구성을 간편하게 관리할 수 있습니다.

MetroCluster IP 구성에서 System Manager를 통해서만 MetroCluster 작업을 수행할 수 있습니다. MetroCluster FC 구성에서는 System Manager를 사용하여 MetroCluster 구성의 각 노드를 관리할 수 있지만 MetroCluster 관련 작업은 수행할 수 없습니다.

일반적으로, 별도의 두 지리적 사이트에서 MetroCluster 구성으로 클러스터를 설정하고 구성합니다. 그런 다음 클러스터 간에 피어링을 설정하여 데이터가 동기화되고 공유되도록 합니다. 피어링된 네트워크에 있는 두 클러스터는 양방향 DR(재해 복구)을 제공하며, 각 클러스터가 다른 클러스터의 소스와 백업될 수 있습니다. 8노드 또는 4노드 MetroCluster IP 구성에서 각 사이트는 하나 또는 두 개의 고가용성(HA) 쌍으로 구성된 스토리지 컨트롤러로

구성됩니다.

세 번째 위치에서 노드와 해당 DR 파트너의 상태를 모니터링할 수 "ONTAP Mediator 설치"있습니다. ONTAP Mediator는 재해 발생 시 Mediator 지원 비계획 전환(MAUSO)을 구현할 수 있습니다.

협상된 스위치오버를 수행하여 계획된 유지 관리를 위해 클러스터 중 하나를 가져올 수도 있습니다. 파트너 클러스터는 유지보수 작업을 수행한 클러스터를 불러와서 스위치백 작업을 수행할 때까지 두 클러스터에 대한 모든 데이터 I/O 작업을 처리합니다.

에서 System Manager를 사용하여 MetroCluster IP 구성을 설정 및 관리하는 절차를 찾을 수 "MetroCluster 설명서 "있습니다.

테이프 백업을 사용한 데이터 보호

ONTAP FlexVol 볼륨의 테이프 백업에 대해 알아보세요

ONTAP는 NDMP(네트워크 데이터 관리 프로토콜)를 통해 테이프 백업 및 복원을 지원합니다. NDMP를 사용하면 스토리지 시스템의 데이터를 테이프에 직접 백업할 수 있으므로 네트워크 대역폭을 효율적으로 사용할 수 있습니다. ONTAP는 테이프 백업을 위해 덤프 및 SMTape 엔진을 모두 지원합니다.

NDMP 호환 백업 애플리케이션을 사용하여 덤프 또는 SMTape 백업 또는 복구를 수행할 수 있습니다. NDMP 버전 4만 지원됩니다.

덤프를 사용한 테이프 백업

덤프는 파일 시스템 데이터가 테이프에 백업되는 스냅샷 기반 백업입니다. ONTAP 덤프 엔진은 파일, 디렉토리 및 해당 ACL(액세스 제어 목록) 정보를 테이프에 백업합니다. 전체 볼륨, 전체 qtree 또는 전체 볼륨 또는 전체 qtree가 아닌 하위 트리를 백업할 수 있습니다. 덤프는 기본, 차등 및 증분 백업을 지원합니다.

SMTape를 사용한 테이프 백업

SMTape는 데이터 블록을 테이프에 백업하는 ONTAP의 스냅샷 기반 재해 복구 솔루션입니다. SMTape를 사용하여 테이프에 볼륨 백업을 수행할 수 있습니다. 그러나 qtree 또는 하위 트리 레벨에서 백업을 수행할 수 없습니다. SMTape는 기본 백업, 차등 백업 및 증분 백업을 지원합니다.

ONTAP 9.13.1부터 SMTape를 사용한 테이프 백업이 와 함께 SnapMirror 활성 동기화지원됩니다.

ONTAP 테이프 백업 및 복원 워크플로

NDMP 지원 백업 애플리케이션을 사용하여 테이프 백업 및 복구 작업을 수행할 수 있습니다.

이 작업에 대해

테이프 백업 및 복원 워크플로우는 테이프 백업 및 복원 작업 수행과 관련된 작업에 대한 개요를 제공합니다. 백업 및 복원 작업 수행에 대한 자세한 내용은 백업 애플리케이션 설명서를 참조하십시오.

단계

1. NDMP 지원 테이프 토폴로지를 선택하여 테이프 라이브러리 구성을 설정합니다.
2. 스토리지 시스템에서 NDMP 서비스를 설정합니다.

NDMP 서비스는 노드 레벨 또는 SVM(스토리지 가상 시스템) 레벨에서 설정할 수 있습니다. 테이프 백업 및 복구 작업을 수행하도록 선택한 NDMP 모드에 따라 다릅니다.

3. NDMP 옵션을 사용하여 스토리지 시스템의 NDMP를 관리합니다.

   노드 레벨 또는 SVM 레벨에서 NDMP 옵션을 사용할 수 있습니다. 테이프 백업 및 복구 작업을 수행하도록 선택한 NDMP 모드에 따라 다릅니다.

   명령을 사용하여 노드 레벨에서 및 SVM 레벨에서 명령을 `vserver services ndmp modify` 사용하여 NDMP 옵션을 수정할 수 `system services ndmp modify` 있습니다. 및 `vserver services ndmp modify` 에 대한 자세한 `system services ndmp modify` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

4. NDMP 지원 백업 애플리케이션을 사용하여 테이프 백업 또는 복구 작업을 수행합니다.

   ONTAP는 테이프 백업 및 복구를 위해 덤프 엔진과 SMTape 엔진을 모두 지원합니다.

   백업 애플리케이션(_Data Management Applications_or_DMA_라고도 함)을 사용하여 백업 또는 복구 작업을 수행하는 방법에 대한 자세한 내용은 백업 애플리케이션 설명서를 참조하십시오.

관련 정보

일반적인 NDMP 테이프 백업 토폴로지

FlexVol 볼륨에 대한 덤프 엔진 이해

ONTAP SMTape 및 덤프 백업 엔진의 사용 사례

ONTAP는 SMTape와 dump의 두 가지 백업 엔진을 지원합니다. 테이프 백업 및 복원 작업을 수행할 백업 엔진을 선택하는 데 도움이 되는 SMTape 및 덤프 백업 엔진의 사용 사례를 알고 있어야 합니다.

덤프는 다음과 같은 경우에 사용할 수 있습니다.

- 파일 및 디렉토리의 DAR(Direct Access Recovery
- 특정 경로에 있는 하위 디렉터리 또는 파일의 하위 집합 백업
- 백업 중에 특정 파일 및 디렉토리를 제외합니다
- 장기간 백업 보존

SMTape는 다음과 같은 경우에 사용할 수 있습니다.

- 재해 복구 솔루션
- 복원 작업 중에 백업된 데이터의 중복 제거 절약 및 중복 제거 설정을 유지합니다
- 대용량 볼륨 백업

테이프 드라이브 관리

ONTAP 테이프 드라이브 관리에 대해 알아보세요

테이프 백업 또는 복구 작업을 수행하기 전에 테이프 라이브러리 연결을 확인하고 테이프 드라이브 정보를 볼 수 있습니다. 자격 없는 테이프 드라이브를 자격 있는 테이프 드라이브에 에뮬레이트하여 사용할 수 있습니다. 기존 별칭을 보는 것 외에도 테이프 별칭을 할당 및 제거할 수도 있습니다.

데이터를 테이프에 백업할 때 데이터는 테이프 파일에 저장됩니다. 파일 표시는 테이프 파일을 구분하며 파일에 이름이 없습니다. 테이프 파일의 위치를 사용하여 테이프 파일을 지정합니다. 테이프 디바이스를 사용하여 테이프 파일을 씁니다. 테이프 파일을 읽을 때 해당 테이프 파일을 쓰는 데 사용한 압축 유형이 동일한 디바이스를 지정해야 합니다.

테이프 드라이브, 미디어 체인저 및 테이프 드라이브 작업을 관리하기 위한 **ONTAP** 명령

클러스터의 테이프 드라이브 및 미디어 체인저에 대한 정보를 보고, 테이프 드라이브를 온라인 상태로 전환하고, 오프라인 상태로 만들고, 테이프 드라이브 카트리지 위치를 수정하고, 테이프 드라이브 별칭 이름을 설정 및 지우고, 테이프 드라이브를 재설정하는 데 사용되는 명령이 있습니다. 또한 테이프 드라이브 통계를 보거나 재설정할 수 있습니다.

원하는 작업	이 명령 사용...
테이프 드라이브를 온라인 상태로 전환합니다	'테이프 온라인 보관'
테이프 드라이브 또는 미디어 체인저의 별칭 이름을 지웁니다	'테이프 별칭 지우기'
테이프 드라이브에 대한 테이프 추적 작업을 활성화하거나 비활성화합니다	"테이프 추적 보관"
테이프 드라이브 카트리지 위치를 수정합니다	'테이프 보관 위치'
테이프 드라이브를 재설정합니다	'테이프 재설정'을 선택합니다 이 명령은 고급 권한 수준에서만 사용할 수 있습니다.
테이프 드라이브 또는 미디어 체인저의 별칭 이름을 설정합니다	'스토리지 테이프 별칭 세트'
테이프 드라이브를 오프라인 상태로 전환합니다	'테이프 오프라인 보관'
모든 테이프 드라이브 및 미디어 체인저에 대한 정보를 봅니다	'스토리지 테이프 쇼'
클러스터에 연결된 테이프 드라이브에 대한 정보를 봅니다	• '테이프 쇼테이프 드라이브 보관' • '시스템 노드 하드웨어 테이프 드라이브 표시

원하는 작업	이 명령 사용...
클러스터에 연결된 미디어 체인저에 대한 정보를 봅니다	'스토리지 테이프 쇼 미디어 체인저'
클러스터에 연결된 테이프 드라이브에 대한 오류 정보를 봅니다	'테이프 저장 표시 오류'입니다
클러스터의 각 노드에 연결된 모든 ONTAP 인증 및 지원 테이프 드라이브를 봅니다	'Storage tape show-supported-status'를 선택합니다
클러스터의 각 노드에 연결된 모든 테이프 드라이브 및 미디어 체인저의 별칭을 봅니다	'Storage tape alias show'
테이프 드라이브의 통계 판독값을 0으로 재설정합니다	'Storage stats tape zero' tape_name 이 명령은 노드 쉘에서 사용해야 합니다.
ONTAP에서 지원하는 테이프 드라이브를 봅니다	"torage show tape supported[-v]" 이 명령은 노드 쉘에서 사용해야 합니다. 각 테이프 드라이브에 대한 자세한 내용을 보려면 '-v' 옵션을 사용할 수 있습니다.
테이프 디바이스 통계를 보고 테이프 성능을 이해하고 사용 패턴을 확인합니다	'STORAGE STATS TAPE'TAPE_NAME'입니다 이 명령은 노드 쉘에서 사용해야 합니다.

관련 정보

- "저장 테이프"
- "저장 테이프 쇼"
- "저장 테이프 show-supported-status"
- "저장 테이프 쇼-테이프-드라이브"
- "저장 테이프 별칭 지우기"
- "저장 테이프 별칭 세트"
- "저장 테이프 별칭 표시"
- "저장 테이프 추적"

ONTAP 테이프 백업에 비적격 테이프 드라이브 사용

검증된 테이프 드라이브를 에뮬레이트할 수 있는 경우 스토리지 시스템에서 검증되지 않은 테이프 드라이브를 사용할 수 있습니다. 그런 다음 자격 있는 테이프 드라이브처럼 취급됩니다. 검증되지 않은 테이프 드라이브를 사용하려면 먼저 정규화된 테이프 드라이브를 에뮬레이트하는지 여부를 확인해야 합니다.

이 작업에 대해

검증되지 않은 테이프 드라이브는 스토리지 시스템에 연결되어 있지만 ONTAP에서 지원되거나 인식되지 않는 드라이브입니다.

단계

1. Storage tape show-supported-status 명령을 사용하여 스토리지 시스템에 연결된 검증되지 않은 테이프 드라이브를 확인합니다.

   다음 명령을 실행하면 스토리지 시스템에 연결된 테이프 드라이브와 각 테이프 드라이브의 지원 및 검증 상태가 표시됩니다. 검증되지 않은 테이프 드라이브도 나열됩니다. "tape_drive_vendor_name"은(는) 스토리지 시스템에 연결된 검증되지 않은 테이프 드라이브이지만 ONTAP에서 지원하지 않습니다.

```
cluster1::> storage tape show-supported-status -node Node1

          Node: Node1
                                    Is
          Tape Drive                Supported  Support Status
          --------------------      ---------  --------------
          "tape_drive_vendor_name"  false      Nonqualified tape drive
          Hewlett-Packard C1533A    true       Qualified
          Hewlett-Packard C1553A    true       Qualified
          Hewlett-Packard Ultrium 1 true       Qualified
          Sony SDX-300C             true       Qualified
          Sony SDX-500C             true       Qualified
          StorageTek T9840C         true       Dynamically Qualified
          StorageTek T9840D         true       Dynamically Qualified
          Tandberg LTO-2 HH         true       Dynamically Qualified
```

2. 검증된 테이프 드라이브를 에뮬레이트합니다.

   "NetApp 다운로드: 테이프 장치 구성 파일"

관련 정보

- 검증된 테이프 드라이브가 무엇입니까
- "저장 테이프 show-supported-status"

ONTAP 테이프 백업을 위해 테이프 드라이브 또는 미디어 체인저에 테이프 별칭을 할당합니다**.**

장치를 쉽게 식별할 수 있도록 테이프 드라이브 또는 미디어 체인저에 테이프 별칭을 할당할 수 있습니다. 별칭은 백업 디바이스의 논리적 이름과 테이프 드라이브 또는 미디어 체인저에 영구적으로 할당된 이름 간의 통신을 제공합니다.

단계

1. 'Storage tape alias set' 명령을 사용하여 테이프 드라이브 또는 미디어 체인저에 별칭을 할당합니다.

   에 대한 자세한 내용은 `storage tape alias set` "ONTAP 명령 참조입니다"을 참조하십시오.

'system node hardware tape drive show' 명령을 사용하여 테이프 드라이브에 대한 SN(일련 번호) 정보와 'system node hardware tape library show' 명령을 사용하여 테이프 라이브러리에 대한 정보를 볼 수 있습니다.

다음 명령은 일련 번호 SN[123456] L4가 노드 cluster1-01에 연결된 테이프 드라이브로 별칭 이름을 설정합니다.

```
cluster-01::> storage tape alias set  -node cluster-01 -name st3
-mapping SN[123456]L4
```

다음 명령은 일련 번호 SN[65432]이 노드 cluster1-01에 연결된 미디어 체인저로 별칭 이름을 설정합니다.

```
cluster-01::> storage tape alias set  -node cluster-01 -name mc1
-mapping SN[65432]
```

관련 정보

- 테이프 앨리어싱이란 무엇입니까
- 테이프 별칭을 제거하는 중입니다
- "저장 테이프 별칭 세트"

ONTAP 테이프 백업을 위해 테이프 드라이브 또는 미디어 체인저에 대한 테이프 별칭 제거

테이프 드라이브 또는 미디어 체인저에 영구 별칭이 더 이상 필요하지 않은 경우 'Storage tape alias clear' 명령을 사용하여 별칭을 제거할 수 있습니다.

단계

1. 'Storage tape alias clear' 명령어를 사용해 테이프 드라이브 또는 미디어 체인저에서 별칭을 삭제한다.

   에 대한 자세한 내용은 `storage tape alias clear` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 별칭 지우기 작업의 범위를 "테이프"로 지정하여 모든 테이프 드라이브의 별칭이 제거됩니다.

```
cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
```

작업을 마친 후

NDMP를 사용하여 테이프 백업 또는 복구 작업을 수행하는 경우 테이프 드라이브 또는 미디어 체인저에서 별칭을 제거한 후 테이프 디바이스에 계속 액세스하려면 테이프 드라이브 또는 미디어 체인저에 새 별칭 이름을 할당해야 합니다.

관련 정보

- 테이프 앨리어싱이란 무엇입니까
- 테이프 별칭 할당
- "저장 테이프 별칭 지우기"

ONTAP 테이프 예약 활성화 또는 비활성화

Tape.예약 옵션을 사용하여 ONTAP에서 테이프 디바이스 예약을 관리하는 방법을 제어할 수 있습니다. 기본적으로 테이프 예약이 해제되어 있습니다.

이 작업에 대해

테이프 예약 옵션을 활성화하면 테이프 드라이브, 미디어 체인저, 브리지 또는 라이브러리가 제대로 작동하지 않을 경우 문제가 발생할 수 있습니다. 테이프 명령이 디바이스를 사용하는 다른 스토리지 시스템이 없을 때 디바이스가 예약된다는 것을 보고하는 경우 이 옵션을 해제해야 합니다.

단계

1. SCSI 예약/해제 메커니즘 또는 SCSI 영구 보존 명령을 사용하여 테이프 예약을 비활성화하려면 다음 명령을 클러스터 쉘에 입력합니다.

   "* 옵션 -옵션 -이름 테이프.예약 -옵션 -값{scsi|persistent|off} *"

   SCSI Reserve/Release mechanism을 선택한다.

   '영구'는 SCSI 영구 예약을 선택합니다.

   OFF는 테이프 예약을 비활성화합니다.

관련 정보

테이프 예약이란

테이프 라이브러리 연결을 확인하기 위한 ONTAP 명령

스토리지 시스템과 스토리지 시스템에 연결된 테이프 라이브러리 구성 사이의 접속 경로에 대한 정보를 볼 수 있습니다. 이 정보를 사용하여 테이프 라이브러리 구성에 대한 연결 경로를 확인하거나 연결 경로와 관련된 문제를 해결할 수 있습니다.

새 테이프 라이브러리를 추가하거나 생성한 후 또는 테이프 라이브러리에 대한 단일 경로 또는 다중 경로 액세스에서 장애가 발생한 경로를 복원한 후 테이프 라이브러리 연결을 확인하기 위해 다음 테이프 라이브러리 세부 정보를 볼 수 있습니다. 또한 경로 관련 오류를 해결하거나 테이프 라이브러리에 대한 액세스가 실패하는 경우에도 이 정보를 사용할 수 있습니다.

- 테이프 라이브러리가 연결된 노드입니다
- 장치 ID입니다
- NDMP 경로
- 테이프 라이브러리 이름입니다
- 타겟 포트 및 이니시에이터 포트 ID
- 모든 타겟 또는 FC 이니시에이터 포트를 위한 테이프 라이브러리에 단일 경로 또는 다중 경로 액세스
- ""경로 오류"" 및 ""경로 Qual""와 같은 경로 관련 데이터 무결성 세부 정보
- LUN 그룹 및 LUN 수

원하는 작업	이 명령 사용...
클러스터의 테이프 라이브러리에 대한 정보를 봅니다	'system node hardware tape library show'
테이프 라이브러리의 경로 정보를 봅니다	'storage tape library path show'
모든 이니시에이터 포트에 대한 테이프 라이브러리의 경로 정보를 봅니다	'storage tape library path show-by-initiator'를 선택합니다
스토리지 테이프 라이브러리와 클러스터 간의 접속 정보를 봅니다	'storage tape library config show'를 선택합니다

관련 정보

- "스토리지 테이프 라이브러리 구성 표시"
- "시스템 노드 하드웨어 테이프 라이브러리 표시"
- "스토리지 테이프 라이브러리 경로 표시"
- "스토리지 테이프 라이브러리 경로 표시-이니시에이터별"

테이프 드라이브 정보

적격 **ONTAP** 테이프 드라이브에 대해 알아보세요

스토리지 시스템에서 제대로 작동하는 것으로 테스트 및 확인된 인증된 테이프 드라이브를 사용해야 합니다. 테이프 에일리어싱을 따르고 테이프 예약을 활성화하여 특정 시간에 한 스토리지 시스템만 테이프 드라이브에 액세스할 수 있습니다.

검증된 테이프 드라이브는 테스트를 거쳐 스토리지 시스템에서 올바르게 작동하는 것으로 확인된 테이프 드라이브입니다. 테이프 구성 파일을 사용하여 기존 ONTAP 릴리스에 대해 테이프 드라이브를 검증할 수 있습니다.

ONTAP 테이프 구성 파일의 형식

테이프 구성 파일 형식은 공급업체 ID, 제품 ID 등의 필드와 테이프 드라이브의 압축 유형에 대한 세부 정보로 구성됩니다. 또한 이 파일은 테이프 드라이브의 자동 로드 기능을 활성화하고 테이프 드라이브의 명령 시간 초과 값을 변경하기 위한 선택적 필드로 구성되어 있습니다.

다음 표에는 테이프 구성 파일의 형식이 나와 있습니다.

항목	크기	설명
(string) ndor_id	최대 8바이트	CSI Inquiry 명령으로 조회한 Vendor ID
'product_id'(문자열)	최대 16바이트	CSI Inquiry 명령으로 조회한 제품 ID

항목	크기	설명
"id_match_size"(숫자)		식별 대상 테이프 드라이브를 감지하기 위해 일치시키는 데 사용할 제품 ID의 바이트 수(Inquiry data에서 제품 ID의 첫 번째 문자로 시작).
거미줄(string)	최대 16바이트	이 매개 변수가 있으면 'storage tape show -device-names' 명령으로 출력되는 문자열로 지정되고, 그렇지 않으면 INQ_vendor_ID로 출력된다.
'PRODUCT_PRETY'(문자열)	최대 16바이트	이 파라미터가 있으면 'STORAGE TAPE SHOW-DEVICE-Names' 명령으로 출력되는 문자열로 지정되고, 그렇지 않으면 INQ_PRODUCT_ID가 출력된다.

신도 예쁘고 제품예쁘다 필드는 선택 사항이지만 값이 있으면 다른 필드에도 값이 있어야 합니다.

다음 표에서는 l, mh, h, a 등 다양한 압축 유형에 대한 설명, 밀도 코드 및 압축 알고리즘을 설명합니다.

항목	크기	설명
'{l	m	h
a}_description = (string)'	최대 24바이트	특정 밀도 설정의 특성을 설명하는 notes지옥의 명령어 sysconfig -t를 위해 인쇄할 문자열입니다.
`{l	m	h
a}_density=(16진수 코드)'		l, m, h 또는 a에 대해 원하는 밀도 코드에 해당하는 SCSI 모드 페이지 블록 설명자에서 설정할 밀도 코드입니다
`{l	m	h
a}_algorithm=(16진수 코드)'		밀도 코드와 원하는 밀도 특성에 해당하는 SCSI 압축 모드 페이지에서 설정할 압축 알고리즘입니다.

다음 표에는 테이프 구성 파일에서 사용할 수 있는 옵션 필드가 설명되어 있습니다.

필드에 입력합니다	설명
'자동 로드 = (부울 예/아니요)	테이프 드라이브에 자동 로드 기능이 있는 경우 이 필드는 '예'로 설정됩니다. 즉, 테이프 카트리지를 삽입한 후 'scsi load(start/stop unit)' 명령을 실행하지 않아도 테이프 드라이브가 준비됩니다. 이 필드의 기본값은 no입니다.
'cmd_timeout_0x'입니다	개별 제한 시간 값입니다. 테이프 드라이버에서 기본값으로 사용 중인 값과 다른 시간 제한 값을 지정하려면 이 필드만 사용해야 합니다. 샘플 파일에는 테이프 드라이브에서 사용되는 기본 SCSI 명령 시간 초과 값이 나열되어 있습니다. 시간 초과 값은 분(m), 초(s) 또는 밀리초(ms) 단위로 나타낼 수 있습니다. 이 필드는 변경할 수 없습니다.

NetApp Support 사이트에서 테이프 구성 파일을 다운로드하고 볼 수 있습니다.

테이프 구성 파일 형식의 예

HP LTO5 Ultrium 테이프 드라이브의 테이프 구성 파일 형식은 다음과 같습니다.

전성자(ndor_id) = "HP"

'PRODUCT_id'="Ultrium 5-SCSI"

id_match_size=9

거미장군=HP 휴렛팩커드

"PRODUCT_PRETY" = "LTO-5"

"l_description" = "LTO-3(ro)/4/800GB"

'l_density' = 0x00

'l_algorithm' = 0x00

Ms_description"="LTO-3(ro)/4 8/1600GB CMP"

mdensity' = 0x00

m_algorithm'=0x01

"h_description" = "LTO-5 1600GB"

"h_density" = 0x58

'h_algorithm' = 0x00

"A_DESCRIPTION"="LTO-5 3200GB CMP"

'A_Density' = 0x58

"A_알고리즘" = 0x01

"자동 로드" = "예"

관련 정보

- "NetApp 툴: 테이프 장치 구성 파일"
- "저장 테이프 쇼"

ONTAP 스토리지 시스템이 테이프 드라이브를 동적으로 적격화하는 방법

스토리지 시스템은 공급업체 ID 및 제품 ID를 테이프 검증 표에 포함된 정보와 일치시켜 테이프 드라이브를 동적으로 자격을 평가합니다.

테이프 드라이브를 스토리지 시스템에 연결할 때 테이프 검색 중에 얻은 정보와 내부 테이프 검증 표의 정보 간에 공급업체 ID와 제품 ID가 일치하는지 확인합니다. 스토리지 시스템이 일치 항목을 검색하면 테이프 드라이브가 검증된 것으로 표시되고 테이프 드라이브에 액세스할 수 있습니다. 스토리지 시스템에서 일치하는 항목을 찾을 수 없는 경우 테이프 드라이브는 비정규화된 상태로 유지되며 액세스할 수 없습니다.

테이프 장치 개요

ONTAP 테이프 장치에 대해 알아보세요

테이프 디바이스는 테이프 드라이브를 나타냅니다. 테이프 드라이브의 되감기 유형과 압축 기능의 특정 조합입니다.

테이프 디바이스는 되감기 유형과 압축 기능의 각 조합에 대해 생성됩니다. 따라서 테이프 드라이브 또는 테이프 라이브러리에는 여러 개의 테이프 디바이스가 연결될 수 있습니다. 테이프를 이동, 쓰기 또는 읽을 테이프 디바이스를 지정해야 합니다.

스토리지 시스템에 테이프 드라이브 또는 테이프 라이브러리를 설치할 때 ONTAP는 테이프 드라이브 또는 테이프 라이브러리와 연결된 테이프 디바이스를 생성합니다.

ONTAP는 테이프 드라이브 및 테이프 라이브러리를 감지하고 논리적 번호 및 테이프 디바이스를 할당합니다. ONTAP는 파이버 채널, SAS 및 병렬 SCSI 테이프 드라이브와 라이브러리가 인터페이스 포트에 연결될 때 이를 감지합니다. ONTAP는 인터페이스가 활성화되어 있을 때 이러한 드라이브를 감지합니다.

ONTAP 테이프 장치 이름의 형식

각 테이프 디바이스에는 정의된 형식으로 표시되는 관련 이름이 있습니다. 형식은 장치 유형, 되감기 유형, 별칭 및 압축 유형에 대한 정보를 포함합니다.

테이프 디바이스 이름의 형식은 다음과 같습니다.

Rwind_type의 'st'alias_number'compression_type입니다

rewind_type은 되감기 유형입니다.

다음 목록에서는 다양한 되감기 유형 값을 설명합니다.

- * r *

ONTAP는 테이프 파일 쓰기를 완료한 후 테이프를 되감습니다.

- * nr *

  ONTAP는 테이프 파일 쓰기를 완료한 후 테이프를 되감지 않습니다. 동일한 테이프에 여러 개의 테이프 파일을 쓰려면 이 되감기 유형을 사용해야 합니다.

- * ur *

  이것은 언로드/다시 로드 되감기 유형입니다. 이 되감기 유형을 사용하면 테이프 라이브러리가 테이프 파일의 끝에 도달하면 테이프를 언로드한 다음 다음 다음 테이프가 있으면 로드합니다.

  다음과 같은 경우에만 이 되감기 유형을 사용해야 합니다.

  - 이 장치와 연결된 테이프 드라이브가 테이프 라이브러리에 있거나 라이브러리 모드에 있는 미디어 체인저에 있습니다.
  - 이 장치와 연결된 테이프 드라이브가 스토리지 시스템에 연결되어 있습니다.
  - 수행 중인 작업에 충분한 테이프를 이 테이프 드라이브에 대해 정의된 라이브러리 테이프 시퀀스에서 사용할 수 있습니다.

되감기 안 함 장치를 사용하여 테이프를 녹음하는 경우 테이프를 읽기 전에 테이프를 되감아야 합니다.

't'는 테이프 드라이브의 표준 지정입니다.

alias_number는 ONTAP가 테이프 드라이브에 할당하는 별칭입니다. ONTAP가 새 테이프 드라이브를 감지하면 ONTAP가 테이프 드라이브에 별칭을 할당합니다.

compression_type은 테이프의 데이터 밀도와 압축 유형을 나타내는 드라이브별 코드입니다.

다음 목록에는 압축 유형 의 다양한 값이 설명되어 있습니다.

- * A *

  최고의 압축

- * 시간 *

  높은 압축

- m *

  중간 압축

- * l * 를 선택합니다

  낮은 압축

예

nrst0a는 가장 높은 압축을 사용하여 테이프 드라이브 0에 되감기 안 함 장치를 지정합니다.

테이프 디바이스 목록의 예

다음 예는 HP Ultrium 2-SCSI와 연결된 테이프 장치를 보여줍니다.

```
        Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
rst0l  -  rewind device,         format is: HP (200GB)
nrst0l -  no rewind device,      format is: HP (200GB)
urst0l -  unload/reload device, format is: HP (200GB)
rst0m  -  rewind device,         format is: HP (200GB)
nrst0m -  no rewind device,      format is: HP (200GB)
urst0m -  unload/reload device, format is: HP (200GB)
rst0h  -  rewind device,         format is: HP (200GB)
nrst0h -  no rewind device,      format is: HP (200GB)
urst0h -  unload/reload device, format is: HP (200GB)
rst0a  -  rewind device,         format is: HP (400GB w/comp)
nrst0a -  no rewind device,      format is: HP (400GB w/comp)
urst0a -  unload/reload device, format is: HP (400GB w/comp)
```

다음 목록에서는 위의 예제에서 약어를 설명합니다.

- GB — 기가바이트. 테이프의 용량입니다.
- w/comp — 압축을 사용하면 테이프 용량이 압축 상태로 표시됩니다.

동시에 지원되는 **ONTAP** 테이프 장치 수

ONTAP는 Fibre Channel, SCSI 또는 SAS 접속 장치를 혼합하여 각 스토리지 시스템(노드당)에 대해 최대 64개의 동시 테이프 드라이브 접속, 16개의 미디어 체인저 및 16개의 브리지 또는 라우터 디바이스를 지원합니다.

테이프 드라이브 또는 미디어 체인저는 물리적 또는 가상 테이프 라이브러리 또는 독립 실행형 디바이스의 디바이스일 수 있습니다.

> 스토리지 시스템에서 64개의 테이프 드라이브 연결을 감지할 수 있지만 동시에 수행할 수 있는 최대 백업 및 복구 세션 수는 백업 엔진의 확장성 제한에 따라 달라집니다.

관련 정보

덤프 백업 및 복원 세션에 대한 확장성 제한

테이프 에일리어싱

테이프 앨리어싱 개요

에일리어싱은 장치 식별 과정을 간소화합니다. 앨리어싱은 테이프 또는 미디어 체인저의 물리적 경로 이름(PPN) 또는 일련 번호(SN)를 영구적이지만 수정할 수 있는 별칭 이름에 바인딩합니다.

다음 표에서는 테이프 드라이브(또는 테이프 라이브러리 또는 미디어 체인저)가 항상 단일 별칭 이름과 연결되도록 하는 테이프 앨리어싱을 사용하는 방법을 설명합니다.

시나리오	별칭을 다시 할당합니다
시스템이 재부팅될 때	테이프 드라이브는 이전 별칭을 자동으로 재할당합니다.
테이프 디바이스가 다른 포트로 이동할 때	새 주소를 가리키도록 별칭을 조정할 수 있습니다.
둘 이상의 시스템에서 특정 테이프 디바이스를 사용하는 경우	사용자는 모든 시스템에 대해 별칭을 동일하게 설정할 수 있습니다.

Data ONTAP 8.1.x에서 Data ONTAP 8.2.x로 업그레이드하면 Data ONTAP 8.2.x의 테이프 별칭 기능이 기존 테이프 별칭 이름을 수정합니다. 이러한 경우 백업 애플리케이션에서 테이프 별칭 이름을 업데이트해야 할 수 있습니다.

테이프 별칭을 할당하면 백업 디바이스의 논리적 이름(예: st0 또는 MC1)과 포트, 테이프 드라이브 또는 미디어 체인저에 영구적으로 할당되는 이름이 일치하게 됩니다.

st0과 st00은 서로 다른 논리적 이름입니다.

논리 이름 및 일련 번호는 장치에 액세스하는 경우에만 사용됩니다. 디바이스에 액세스한 후에는 물리적 경로 이름을 사용하여 모든 오류 메시지를 반환합니다.

앨리어싱에는 물리적 경로 이름과 일련 번호라는 두 가지 유형의 이름을 사용할 수 있습니다.

물리적 경로 이름에 대해 알아보세요

물리적 경로 이름(PPN)은 ONTAP가 스토리지 시스템에 접속된 SCSI-2/3 어댑터 또는 스위치(특정 위치)를 기반으로 테이프 드라이브 및 테이프 라이브러리에 할당하는 숫자 주소 시퀀스입니다. PPN은 전기 이름이라고도 합니다.

직접 연결된 장치의 PPN은 'host_adapter' 형식을 사용한다. device_id_lun

LUN 값이 0이 아닌 테이프 및 미디어 체인저 디바이스에 대해서만 LUN 값이 표시됩니다. 즉, LUN 값이 0이면 PPN의 'LUN' 부분이 표시되지 않습니다.

예를 들어, PPN 8.6은 호스트 어댑터 번호가 8이고, 장치 ID는 6이며, 논리 장치 번호(LUN)는 0임을 나타냅니다.

SAS 테이프 장치도 직접 연결 장치입니다. 예를 들어, PPN 5c.4는 스토리지 시스템에서 SAS HBA가 슬롯 5에 연결되어 있고 SAS 테이프가 SAS HBA의 포트 C에 연결되어 있고 장치 ID가 4임을 나타냅니다.

Fibre Channel 스위치 접속 디바이스의 PPN은 'switch:port_id' 형식을 사용합니다. device_id_lun

예를 들어, PPN my_switch:5.3L2는 my_switch라는 스위치의 포트 5에 연결된 테이프 드라이브가 장치 ID 3으로 설정되어 있고 LUN 2를 가지고 있음을 나타냅니다.

LUN(논리 유닛 번호)은 드라이브에 의해 결정됩니다. Fibre Channel, SCSI 테이프 드라이브 및 라이브러리 및 디스크에는 PPN이 있습니다.

테이프 드라이브 및 라이브러리의 PPN은 스위치의 이름이 변경되거나, 테이프 드라이브 또는 라이브러리가 이동하거나, 테이프 드라이브 또는 라이브러리를 다시 구성하지 않는 한 변경되지 않습니다. 재부팅 후 PPN은 변경되지 않습니다. 예를 들어 my_switch:5.3L2라는 테이프 드라이브가 제거되고 디바이스 ID와 LUN이 동일한 새 테이프

드라이브가 스위치 my_switch의 포트 5에 연결된 경우 my_switch:5.3L2를 사용하여 새 테이프 드라이브에 액세스할 수 있습니다.

일련 번호에 대해 알아보세요

일련 번호(SN)는 테이프 드라이브 또는 미디어 체인저의 고유 식별자입니다. ONTAP는 WWN 대신 SN을 기반으로 별칭을 생성합니다.

SN은 테이프 드라이브 또는 미디어 체인저의 고유 식별자이므로 테이프 드라이브 또는 미디어 체인저에 대한 여러 연결 경로에 관계없이 별칭은 동일하게 유지됩니다. 이를 통해 스토리지 시스템은 테이프 라이브러리 구성에서 동일한 테이프 드라이브 또는 미디어 체인저를 추적할 수 있습니다.

테이프 드라이브 또는 미디어 체인저가 연결된 Fibre Channel 스위치의 이름을 바꾸어도 테이프 드라이브 또는 미디어 체인저의 SN은 변경되지 않습니다. 그러나 테이프 라이브러리에서 기존 테이프 드라이브를 새 테이프 드라이브로 교체할 경우 ONTAP는 테이프 드라이브의 SN이 변경되므로 새 별칭을 생성합니다. 또한 기존 테이프 드라이브를 테이프 라이브러리의 새 슬롯으로 이동하거나 테이프 드라이브의 LUN을 다시 매핑할 경우 ONTAP는 해당 테이프 드라이브에 대한 새 별칭을 생성합니다.

백업 애플리케이션을 새로 생성된 별칭으로 업데이트해야 합니다.

테이프 장치의 SN은 S N[xxxxxxxxxx]L[X] 형식을 사용합니다

X는 영숫자 문자이고 L은 테이프 디바이스의 LUN입니다. LUN이 0이면 문자열 L의 X 부분이 표시되지 않습니다.

각 SN은 최대 32자로 구성되며, SN의 형식은 대/소문자를 구분하지 않습니다.

ONTAP 다중 경로 테이프 액세스 구성 시 고려 사항

테이프 라이브러리의 테이프 드라이브를 액세스할 수 있도록 스토리지 시스템에서 두 개의 경로를 구성할 수 있습니다. 한 경로에 장애가 발생할 경우 스토리지 시스템은 다른 경로를 사용하여 장애가 발생한 경로를 즉시 복구하지 않고도 테이프 드라이브를 액세스할 수 있습니다. 이렇게 하면 테이프 작업을 다시 시작할 수 있습니다.

스토리지 시스템에서 다중 경로 테이프 액세스를 구성할 때는 다음 사항을 고려해야 합니다.

- LUN 매핑을 지원하는 테이프 라이브러리에서 LUN 그룹에 대한 다중 경로 액세스를 위해 LUN 매핑은 각 경로에서 대칭적이어야 합니다.

  테이프 드라이브와 미디어 체인저는 테이프 라이브러리의 LUN 그룹(동일한 이니시에이터 경로 세트를 공유하는 LUN 세트)에 할당됩니다. LUN 그룹의 모든 테이프 드라이브를 여러 경로에 대한 백업 및 복원 작업에 사용할 수 있어야 합니다.

- 스토리지 시스템에서 테이프 라이브러리의 테이프 드라이브를 액세스하도록 최대 2개의 경로를 구성할 수 있습니다.
- 다중 경로 테이프 액세스는 로드 밸런싱을 지원합니다. 로드 밸런싱은 기본적으로 비활성화되어 있습니다.

다음 예제에서 스토리지 시스템은 두 개의 이니시에이터 경로 0b 및 0d를 통해 LUN 그룹 0에 액세스합니다. 두 경로 모두에서 LUN 그룹은 LUN 번호, 0 및 LUN 수, 5를 동일하게 갖습니다. 스토리지 시스템은 이니시에이터 경로 1개만을 통해 LUN 그룹 1을 3D로 액세스합니다.

```
STSW-3070-2_cluster::> storage tape library config show

Node                      LUN Group   LUN Count  Library Name  Library
Target Port  Initiator
------------------------ ----------- ---------- -------------
-------------------- -----
STSW-3070-2_cluster-01        0       5          IBM 3573-TL_1
510a09800000412d     0b

0d
                              1       2          IBM 3573-TL_2
50050763124b4d6f     3d

3 entries were displayed
```

관련 정보

- "스토리지 테이프 라이브러리 구성 표시"

ONTAP 스토리지 시스템에 테이프 드라이브와 라이브러리를 추가하는 방법을 알아보세요.

스토리지 시스템을 오프라인으로 전환하지 않고도 테이프 드라이브와 라이브러리를 스토리지 시스템에 동적으로 추가할 수 있습니다.

새 미디어 체인저를 추가하면 스토리지 시스템이 미디어 체인저를 감지하여 구성에 추가합니다. 미디어 체인저가 별칭 정보에서 이미 참조되면 새 논리 이름이 생성되지 않습니다. 라이브러리가 참조되지 않으면 스토리지 시스템이 미디어 체인저에 대한 새 별칭을 생성합니다.

테이프 라이브러리 구성에서 ONTAP용 타겟 포트의 LUN 0에 테이프 드라이브 또는 미디어 체인저를 구성하여 해당 타겟 포트의 모든 미디어 체인저와 테이프 드라이브를 검색해야 합니다.

ONTAP 테이프 예약에 대해 알아보세요

여러 스토리지 시스템이 테이프 드라이브, 미디어 체인저, 브리지 또는 테이프 라이브러리에 대한 액세스를 공유할 수 있습니다. 테이프 예약은 SCSI 예약/해제 메커니즘 또는 모든 테이프 드라이브, 미디어 체인저, 브리지 및 테이프 라이브러리에 대한 SCSI 영구 예약을 활성화하여 특정 시간에 한 스토리지 시스템만 디바이스에 액세스할 수 있도록 합니다.

스위치가 포함되었는지 여부에 관계없이 라이브러리에서 디바이스를 공유하는 모든 시스템은 동일한 예약 방법을 사용해야 합니다.

디바이스 예약을 위한 SCSI 예약/해제 메커니즘은 정상 조건에서 잘 작동합니다. 그러나 인터페이스 오류 복구 절차 중에 예약을 유실할 수 있습니다. 이 경우 예약된 소유자 이외의 이니시에이터가 디바이스에 액세스할 수 있습니다.

SCSI 영구 예약으로 이루어진 예약은 루프 재설정 또는 대상 재설정과 같은 오류 복구 메커니즘의 영향을 받지 않지만 모든 장치에서 SCSI 영구 예약을 올바르게 구현하는 것은 아닙니다.

스토리지 시스템 간 데이터 전송

ndmpcopy를 사용하여 **ONTAP** 데이터 전송

ndmpcopy nodeswell 명령은 NDMP v4를 지원하는 스토리지 시스템 간에 데이터를 전송합니다. 전체 및 증분 데이터 전송을 모두 수행할 수 있습니다. 전체 또는 부분 볼륨, Qtree, 디렉토리 또는 개별 파일을 전송할 수 있습니다.

이 작업에 대해

ONTAP 8.x 및 이전 릴리즈를 사용하면 증분 전송은 최대 2개의 레벨(전체 백업 1개 및 최대 2개의 증분 백업)으로 제한됩니다.

ONTAP 9.0 이상 릴리즈부터 증분 전송은 최대 9개 레벨(전체 백업 1개 및 증분 백업 9개)으로 제한됩니다.

소스 및 대상 스토리지 시스템의 nodeswell 명령줄에서 ndmpcopy를 실행하거나 데이터 전송 소스 또는 대상이 아닌 스토리지 시스템을 실행할 수 있습니다. 또한 데이터 전송의 소스와 대상 모두에 대해 단일 스토리지 시스템에서 ndmpcopy를 실행할 수 있습니다.

ndmpcopy 명령에서 소스 및 대상 스토리지 시스템의 IPv4 또는 IPv6 주소를 사용할 수 있습니다. 경로 형식은 "/vserver_name/volume_name\[path\]"입니다.

단계

1. 소스 및 대상 스토리지 시스템에서 NDMP 서비스를 설정합니다.

의 소스 또는 대상에서 데이터 전송을 수행하는 경우…	다음 명령을 사용합니다…
SVM 범위의 NDMP 모드입니다	'vserver services ndmp on' admin SVM에서 NDMP 인증의 경우 사용자 계정은 admin이고 사용자 역할은 admin 또는 backup입니다. 데이터 SVM에서 사용자 계정은 vsadmin이고 사용자 역할은 vsadmin 또는 vsadmin-backup입니다.
노드 범위의 NDMP 모드입니다	'System services NDMP on'(시스템 서비스 NDMP 켜기)

2. 노드 쉘에서 'ndmpcopy' 명령을 사용하여 스토리지 시스템 내부 또는 스토리지 시스템 간에 데이터 전송:

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-
mcd {inet|inet6}] [-md {inet|inet6}]
```

DNS 이름은 ndmpcopy에서 지원되지 않습니다. 소스 및 대상의 IP 주소를 제공해야 합니다. 루프백 주소(127.0.0.1)는 소스 IP 주소 또는 대상 IP 주소에 대해 지원되지 않습니다.

- "ndmpcopy" 명령은 다음과 같이 제어 연결의 주소 모드를 결정합니다.

- 제어 연결의 주소 모드는 제공된 IP 주소에 해당합니다.
- '-mcs' 및 '-mcd' 옵션을 사용하여 이러한 규칙을 재정의할 수 있습니다.

◦ 소스 또는 타겟이 ONTAP 시스템인 경우 NDMP 모드(노드 범위 또는 SVM 범위)에 따라 타겟 볼륨에 액세스할 수 있는 IP 주소를 사용하십시오.

◦ 'source_path'와 'destination_path'는 볼륨, qtree, 디렉토리 또는 파일의 세밀한 수준까지 가는 절대 경로 이름입니다.

◦ '-mcs'는 소스 스토리지 시스템에 대한 제어 접속의 기본 주소 지정 모드를 지정합니다.

inet은 IPv4 주소 모드를 나타내며 inet6은 IPv6 주소 모드를 나타냅니다.

◦ '-MCD'는 대상 저장소 시스템에 대한 제어 연결에 대해 기본 주소 지정 모드를 지정합니다.

inet은 IPv4 주소 모드를 나타내며 inet6은 IPv6 주소 모드를 나타냅니다.

◦ '-MD'는 소스와 대상 스토리지 시스템 간의 데이터 전송을 위한 기본 주소 지정 모드를 지정합니다.

inet은 IPv4 주소 모드를 나타내며 inet6은 IPv6 주소 모드를 나타냅니다.

ndmpcopy 명령에서 '-md' 옵션을 사용하지 않으면 데이터 연결의 주소 지정 모드가 다음과 같이 결정됩니다.

- 제어 연결에 지정된 주소 중 하나가 IPv6 주소이면 데이터 연결의 주소 모드는 IPv6입니다.
- 제어 연결에 지정된 두 주소가 모두 IPv4 주소이면 ndmpcopy 명령이 먼저 데이터 연결에 대한 IPv6 주소 모드를 시도합니다.

이 명령이 실패하면 IPv4 주소 모드를 사용합니다.

ⓘ IPv6 주소가 지정된 경우 대괄호로 묶어야 합니다.

이 샘플 명령은 소스 경로('source_path')에서 대상 경로('Destination_path')로 데이터를 마이그레이션합니다.

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+
이 샘플 명령은 IPv6 주소 모드를 사용할 제어 연결과 데이터 연결을 명시적으로 설정합니다.

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdf:7e78]:/<dst_svm>/<dst_vol>
```

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ndmpcopy 명령에 대한 옵션입니다

nodeshell 명령에 사용할 수 있는 옵션을 `ndmpcopy` 이해해야 "데이터를 전송합니다"합니다.

다음 표에는 사용 가능한 옵션이 나와 있습니다.

옵션을 선택합니다	설명
'-sa"사용자 이름:['암호']	이 옵션은 소스 스토리지 시스템에 접속할 소스 인증 사용자 이름과 암호를 설정합니다. 필수 옵션입니다. admin 권한이 없는 사용자의 경우 시스템에서 생성한 NDMP 관련 암호를 지정해야 합니다. admin 및 non-admin 사용자 모두 시스템에서 생성한 암호는 필수입니다.
'-da"사용자 이름':['암호']	이 옵션은 대상 스토리지 시스템에 접속하기 위한 대상 인증 사용자 이름 및 암호를 설정합니다. 필수 옵션입니다.
'-st'{'md5'	'text'}
이 옵션은 소스 스토리지 시스템에 접속할 때 사용할 소스 인증 유형을 설정합니다. 이 옵션은 필수 옵션이므로 사용자는 "text" 또는 "md5" 옵션을 제공해야 합니다.	``dt'{'md5'
'text'}	이 옵션은 대상 스토리지 시스템에 접속할 때 사용할 대상 인증 유형을 설정합니다.
'-l'	이 옵션은 지정된 레벨 값으로 전송에 사용되는 덤프 레벨을 설정합니다. 유효한 값은 0, 1, 9, 0은 전체 전송을 나타내고 1은 9, 0은 증분 전송을 지정합니다. 기본값은 0입니다.
'-d'	이 옵션을 사용하면 ndmpcopy 디버그 로그 메시지를 생성할 수 있습니다. ndmpcopy 디버그 로그 파일은 '/mroot/etc/log' 루트 볼륨에 있습니다. ndmpcopy 디버그 로그 파일 이름은 ndmpcopy.yyyymmdd 형식으로 되어 있습니다.
"-f"	이 옵션은 강제 모드를 활성화합니다. 이 모드에서는 7-Mode 볼륨의 루트에 있는 '/etc' 디렉토리에서 시스템 파일을 덮어쓸 수 있습니다.
'-h'	이 옵션은 도움말 메시지를 인쇄합니다.

옵션을 선택합니다	설명
'-p'	이 옵션은 소스 및 대상 인증에 대한 암호를 입력하라는 메시지를 표시합니다. 이 암호는 '-sa' 및 '-da' 옵션에 지정된 암호보다 우선합니다. 이 옵션은 명령이 대화형 콘솔에서 실행 중인 경우에만 사용할 수 있습니다.
'-exclude'	이 옵션은 데이터 전송에 지정된 경로에서 지정된 파일 또는 디렉토리를 제외합니다. 값은 또는 과 `.txt` 같은 파일 이름 또는 디렉터리의 쉼표로 구분된 목록일 수 `.pst` 있습니다. 지원되는 제외 패턴의 최대 개수는 32개이고 지원되는 최대 문자 수는 255개입니다.

FlexVol 볼륨용 NDMP

ONTAP FlexVol 볼륨에 대한 NDMP에 대해 알아보세요

NDMP(Network Data Management Protocol)는 스토리지 시스템 및 테이프 라이브러리와 같은 운영 스토리지 디바이스와 보조 스토리지 디바이스 간의 백업, 복구 및 기타 데이터 전송 유형을 제어하는 표준화된 프로토콜입니다.

스토리지 시스템에서 NDMP 지원을 설정하면 해당 스토리지 시스템이 백업 또는 복구 작업에 참여하는 NDMP 지원 네트워크 연결 백업 애플리케이션(_Data Management Applications_or_DMA_라고도 함), 데이터 서버 및 테이프 서버와 통신할 수 있습니다. 모든 네트워크 통신은 TCPIP 또는 TCP/IPv6 네트워크를 통해 이루어집니다. NDMP는 또한 테이프 드라이브와 미디어 체인저에 대한 낮은 수준의 제어를 제공합니다.

노드 범위의 NDMP 모드 또는 SVM(스토리지 가상 시스템) 범위의 NDMP 모드에서 테이프 백업 및 복구 작업을 수행할 수 있습니다.

NDMP, 환경 변수 목록 및 지원되는 NDMP 테이프 백업 토폴로지를 사용하는 동안 고려해야 할 사항에 대해 알고 있어야 합니다. 향상된 DAR 기능을 사용하거나 사용하지 않도록 설정할 수도 있습니다. ONTAP에서 스토리지 시스템에 대한 NDMP 액세스를 인증하는 데 지원하는 두 가지 인증 방법은 일반 텍스트 및 본인 확인 방법입니다.

관련 정보

ONTAP에서 지원하는 환경 변수입니다

NDMP 작업 모드에 대해 설명합니다

ONTAP NDMP 작동 모드에 대해 알아보세요

노드 레벨 또는 스토리지 가상 머신(SVM) 레벨에서 테이프 백업 및 복원 작업을 수행하도록 선택할 수 있습니다. SVM 레벨에서 이러한 작업을 성공적으로 수행하려면 SVM에서 NDMP 서비스를 사용하도록 설정해야 합니다.

Data ONTAP 8.2에서 Data ONTAP 8.3으로 업그레이드할 경우 8.2에서 사용되는 NDMP 작업 모드는 업그레이드 후에도 8.2에서 8.3으로 유지됩니다.

Data ONTAP 8.2 이상을 사용하여 새 클러스터를 설치하는 경우 NDMP는 기본적으로 SVM 범위의 NDMP 모드에 있습니다. 노드 범위 NDMP 모드에서 테이프 백업 및 복구 작업을 수행하려면 노드 범위 NDMP 모드를 명시적으로 설정해야 합니다.

노드 범위 **ONTAP NDMP** 모드에 대해 알아보세요

노드 범위의 NDMP 모드에서는 노드 수준에서 테이프 백업 및 복구 작업을 수행할 수 있습니다. Data ONTAP 8.2에서 사용되는 NDMP 작업 모드는 업그레이드 후에도 8.2에서 8.3으로 유지됩니다.

노드 범위의 NDMP 모드에서는 볼륨을 소유하는 노드에서 테이프 백업 및 복구 작업을 수행할 수 있습니다. 이러한 작업을 수행하려면 볼륨 또는 테이프 디바이스를 소유한 노드에서 호스팅되는 LIF에 NDMP 제어 연결을 설정해야 합니다.

이 모드는 더 이상 사용되지 않으며 향후 주요 릴리즈에서 제거될 예정입니다.

SVM 범위 **ONTAP NDMP** 모드에 대해 알아보세요

SVM에서 NDMP 서비스가 활성화되어 있는 경우 SVM(스토리지 가상 시스템) 레벨에서 테이프 백업 및 복원 작업을 성공적으로 수행할 수 있습니다. 백업 애플리케이션이 CAB 확장을 지원하는 경우 클러스터 SVM의 여러 노드에서 호스팅되는 모든 볼륨을 백업 및 복원할 수 있습니다.

NDMP 제어 연결은 다른 LIF 유형에 설정할 수 있습니다. SVM 범위의 NDMP 모드에서 이러한 LIF는 데이터 SVM 또는 관리 SVM에 속합니다. 이 LIF를 소유한 SVM에서 NDMP 서비스를 사용하도록 설정한 경우에만 LIF에서 연결을 설정할 수 있습니다.

데이터 LIF는 데이터 SVM에 속하며 인터클러스터 LIF, 노드 관리 LIF 및 클러스터 관리 LIF는 관리 SVM에 속합니다.

SVM 범위의 NDMP 모드에서 백업 및 복원 작업에 대한 볼륨 및 테이프 장치의 가용성은 NDMP 제어 연결이 설정된 LIF 유형과 CAB 확장의 상태에 따라 다릅니다. 백업 애플리케이션이 CAB 확장 및 볼륨을 지원하고 테이프 디바이스가 동일한 선호도를 공유하는 경우 백업 애플리케이션은 3방향 백업 또는 복구 작업 대신 로컬 백업 또는 복구 작업을 수행할 수 있습니다.

관련 정보

노드 범위의 NDMP 모드를 관리하는 명령입니다

ONTAP NDMP 서비스 사용 시 고려 사항

스토리지 시스템에서 NDMP 서비스를 시작할 때는 여러 가지 고려 사항을 고려해야 합니다.

- 각 노드는 연결된 테이프 드라이브를 사용하여 최대 16개의 동시 백업, 복원 또는 2개의 조합을 지원합니다.
- NDMP 서비스는 NDMP 백업 애플리케이션의 요청에 따라 파일 기록 데이터를 생성할 수 있습니다.

  파일 기록은 백업 응용 프로그램에서 백업 이미지에서 선택한 데이터 하위 집합을 최적의 상태로 복구하는 데 사용됩니다. 파일 기록 생성 및 처리는 스토리지 시스템과 백업 애플리케이션 모두에 시간이 많이 걸리고 CPU가 많이 사용될 수 있습니다.

  SMTape는 파일 기록을 지원하지 않습니다.

  전체 백업 이미지가 복구될 재해 복구에 대해 데이터 보호가 구성된 경우 파일 기록 생성을 비활성화하여 백업 시간을 줄일 수 있습니다. NDMP 파일 기록 생성을 해제할 수 있는지 확인하려면 백업 애플리케이션 설명서를 참조하십시오.

- NDMP에 대한 방화벽 정책은 모든 LIF 유형에서 기본적으로 사용하도록 설정됩니다.
- 노드 범위의 NDMP 모드에서 FlexVol 볼륨을 백업하려면 백업 애플리케이션을 사용하여 볼륨을 소유하는 노드에서 백업을 시작해야 합니다.

  그러나 노드 루트 볼륨은 백업할 수 없습니다.

- 방화벽 정책에서 허용하는 한 모든 LIF에서 NDMP 백업을 수행할 수 있습니다.

  데이터 LIF를 사용하는 경우 페일오버에 대해 구성되지 않은 LIF를 선택해야 합니다. NDMP 작업 중에 데이터 LIF가 페일오버되면 NDMP 작업이 실패하고 다시 실행해야 합니다.

- NDMP 모드 및 SVM(Storage Virtual Machine) 범위의 NDMP 모드(CAB 확장 지원 안 함)에서는 NDMP 데이터 연결이 NDMP 제어 연결과 동일한 LIF를 사용합니다.
- LIF 마이그레이션 중에는 지속적인 백업 및 복원 작업이 중단됩니다.

  LIF 마이그레이션 후에 백업 및 복원 작업을 시작해야 합니다.

- NDMP 백업 경로는 '*/vserver_name/volume_name/path_name*' 형식입니다.

  path_name 는 선택 사항이며 디렉토리, 파일 또는 스냅샷의 경로를 지정합니다.

- 덤프 엔진을 사용하여 SnapMirror 대상을 테이프에 백업하는 경우 볼륨의 데이터만 백업됩니다.

  그러나 SMTape를 사용하여 SnapMirror 대상을 테이프에 백업하는 경우 메타데이터도 백업됩니다. SnapMirror 관계 및 관련 메타데이터는 테이프에 백업되지 않습니다. 따라서 복원 중에는 해당 볼륨의 데이터만 복원되지만 연결된 SnapMirror 관계는 복원되지 않습니다.

관련 정보

Cluster Aware Backup 확장의 기능

"시스템 관리"

환경 변수

ONTAP NDMP에 지원되는 환경 변수 알아보기

환경 변수는 NDMP 지원 백업 애플리케이션과 스토리지 시스템 간의 백업 또는 복구 작업에 대한 정보를 전달하는 데 사용됩니다.

예를 들어, 사용자가 백업 애플리케이션이 '/vserver1/vol1/dir1'을 백업하도록 지정하면 백업 애플리케이션이 파일 시스템 환경 변수를 '/vserver1/vol1/dir1'로 설정합니다. 마찬가지로 사용자가 백업을 레벨 1 백업으로 지정하면 백업 애플리케이션이 레벨 환경 변수를 1(1)로 설정합니다.

일반적으로 환경 변수의 설정 및 검사는 백업 관리자에게 영향을 미치지 않습니다. 즉, 백업 애플리케이션에서 자동으로 설정합니다.

백업 관리자는 환경 변수를 거의 지정하지 않지만, 기능 또는 성능 문제를 특성화하거나 해결할 수 있도록 백업 응용 프로그램에서 설정한 환경 변수의 값을 변경할 수 있습니다. 예를 들어, 관리자는 파일 기록 생성을 일시적으로 비활성화하여 백업 응용 프로그램의 파일 기록 정보 처리가 성능 문제 또는 기능 문제에 기여하는지 여부를 확인할 수 있습니다.

많은 백업 애플리케이션은 환경 변수를 재정의하거나 수정하거나 추가 환경 변수를 지정할 수 있는 수단을 제공합니다. 자세한 내용은 백업 애플리케이션 설명서를 참조하십시오.

ONTAP에서 지원하는 환경 변수입니다

ONTAP 연관된 기본값이 있는 환경 변수를 지원합니다. 하지만 이러한 기본값을 수동으로 수정할 수 있습니다.

백업 애플리케이션에서 설정한 값을 수동으로 수정하면 애플리케이션이 예상치 않게 작동할 수 있습니다. 이는 백업 또는 복원 작업에서 백업 애플리케이션이 예상한 작업을 수행하지 못할 수 있기 때문입니다. 그러나 경우에 따라 신중하게 수정하면 문제를 식별하거나 해결하는 데 도움이 될 수 있습니다.

다음 표에는 덤프 및 SMTape에 공통으로 사용되는 환경 변수와 덤프 및 SMTape에만 지원되는 변수가 나와 있습니다. 다음 표에는 ONTAP에서 지원하는 환경 변수가 사용되는 경우 해당 변수가 작동하는 방식이 설명되어 있습니다.

대부분의 경우 Y는 T, N도 F를 받아들입니다.

덤프 및 **SMTape**에 대해 지원되는 환경 변수입니다

환경 변수	유효한 값	기본값	설명
디버그	Y, N	N	디버깅 정보가 인쇄되도록 지정합니다.
파일 시스템	'트링'	"없음"	백업할 데이터의 루트 경로 이름을 지정합니다.
NDMP_version	RETURN_OVERY'를 선택합니다	"없음"	NDMP_VERSION 변수를 수정하면 안 됩니다. 백업 작업에 의해 생성된 NDMP_VERSION 변수는 NDMP 버전을 반환합니다. ONTAP는 내부 사용을 위해 백업 중에 NDMP_VERSION 변수를 설정하고 정보 제공을 위해 백업 애플리케이션에 전달합니다. NDMP 세션의 NDMP 버전이 이 변수로 설정되지 않았습니다.

환경 변수	유효한 값	기본값	설명
경로 이름_구분 기호입니다	RETURN_VALUE’입니다	"없음"	경로 이름 구분 문자를 지정합니다. 이 문자는 백업되는 파일 시스템에 따라 다릅니다. ONTAP의 경우 문자 ""/"가 이 변수에 할당됩니다. NDMP 서버는 테이프 백업 작업을 시작하기 전에 이 변수를 설정합니다.
유형	'둔부' 또는 '스머테이프'	둔부	테이프 백업 및 복원 작업을 수행하는 데 지원되는 백업 유형을 지정합니다.
자세한 정보	Y, N	N	테이프 백업 또는 복구 작업을 수행하는 동안 로그 메시지를 늘립니다.

덤프에 대해 지원되는 환경 변수입니다

환경 변수	유효한 값	기본값	설명
acl_start 를 선택합니다	RETURN_OVERY’를 선택합니다	"없음"	백업 작업에 의해 생성된 ACL_START 변수는 직접 액세스 복구 또는 재시작 가능한 NDMP 백업 작업에 사용되는 오프셋 값입니다. 오프셋 값은 덤프 파일에서 ACL 데이터(Pass V)가 시작되고 백업 끝에서 반환되는 바이트 오프셋입니다. 백업된 데이터를 올바르게 복원하기 위한 직접 액세스 복원 작업의 경우 ACL_START 값을 복구 작업이 시작될 때 복구 작업으로 전달해야 합니다. NDMP 재시작 가능 백업 작업에서는 acl_start 값을 사용하여 백업 스트림의 다시 시작 가능한 부분이 시작되는 백업 애플리케이션과 통신합니다.

환경 변수	유효한 값	기본값	설명
base_date 를 선택합니다	0, -1, dump_date 값	'-1'	증분 백업의 시작 날짜를 지정합니다. '-1'로 설정하면 base_date 증분 지정자가 비활성화됩니다. 레벨 0 백업에서 '0'으로 설정하면 증분 백업이 활성화됩니다. 초기 백업 후 이전 증분 백업의 dump_date 변수 값이 base_date 변수에 할당됩니다. 이러한 변수는 레벨 /업데이트 기반 증분 백업에 대한 대안입니다.
직접	Y, N	N	전체 테이프를 스캔하는 대신 복구가 파일 데이터가 상주하는 테이프 위치로 직접 빠르게 전달되도록 지정합니다. 직접 액세스 복구가 작동하려면 백업 애플리케이션이 위치 정보를 제공해야 합니다. 이 변수가 Y로 설정되어 있으면 백업 응용 프로그램에서 파일 또는 디렉터리 이름과 위치 지정 정보를 지정합니다.
dmp_name입니다	'트링'	"없음"	여러 하위 트리 백업의 이름을 지정합니다. 여러 하위 트리 백업에는 이 변수가 필수입니다.

환경 변수	유효한 값	기본값	설명
dump_date 를 참조하십시오	RETURN_VALUE’입니다	"없음"	이 변수를 직접 변경하지 않습니다. base_date 변수가 '-1’이 아닌 값으로 설정된 경우 백업에 의해 생성됩니다. dump_date 변수는 32비트 레벨 값을 덤프 소프트웨어에서 계산된 32비트 시간 값에 미리 추가하여 파생됩니다. 수준은 base_date 변수에 전달된 마지막 수준 값에서 증가합니다. 결과 값은 후속 증분 백업에서 base_date 값으로 사용됩니다.
Enhanced_DAR_ENABLED입니다	Y, N	N	향상된 DAR 기능의 사용 여부를 지정합니다. 향상된 DAR 기능은 NT 스트림이 있는 파일의 DAR 및 DAR 디렉토리를 지원합니다. 향상된 성능을 제공합니다. 복원 중 향상된 DAR는 다음 조건이 충족되는 경우에만 가능합니다. • ONTAP는 향상된 DAR를 지원합니다. • 백업 중에 파일 기록이 활성화됩니다(HIST=Y). • ndmpd.offset_map.enable 옵션이 on으로 설정되어 있습니다. • Enhanced_DAR_ENABLED 변수가 복원 중에 'Y’로 설정됩니다.

환경 변수	유효한 값	기본값	설명
제외	pattern_string	"없음"	데이터를 백업할 때 제외되는 파일 또는 디렉토리를 지정합니다. 제외 목록은 쉼표로 구분된 파일 또는 디렉토리 이름 목록입니다. 파일 또는 디렉토리의 이름이 목록의 이름 중 하나와 일치하면 백업에서 제외됩니다. 제외 목록에서 이름을 지정할 때 다음 규칙이 적용됩니다. • 파일 또는 디렉토리의 정확한 이름을 사용해야 합니다. • 와일드카드 문자인 별표(*)는 문자열의 첫 번째 문자 또는 마지막 문자여야 합니다. 각 문자열은 최대 2개의 별표를 포함할 수 있습니다. • 파일 또는 디렉터리 이름의 쉼표 앞에는 백슬래시가 있어야 합니다. • 제외 목록에는 최대 32개의 이름이 포함될 수 있습니다. non_quota_tree를 동시에 Y로 설정하면 백업 대상에서 제외되도록 지정된 파일 또는 디렉토리가 제외되지 않습니다.

환경 변수	유효한 값	기본값	설명
압축 풀기	Y, N, E	N	백업된 데이터 집합의 하위 트리를 복원하도록 지정합니다. 백업 응용 프로그램은 추출할 하위 트리의 이름을 지정합니다. 지정된 파일이 콘텐츠가 백업된 디렉토리와 일치하면 디렉토리의 압축이 재귀적으로 풀립니다. DAR를 사용하지 않고 복원 중에 파일, 디렉토리 또는 qtree의 이름을 바꾸려면 추출 환경 변수를 "E"로 설정해야 합니다.
extract_acl 을 선택합니다	Y, N	Y를 누릅니다	백업 파일의 ACL이 복구 작업에서 복원되도록 지정합니다. 기본값은 데이터를 복원할 때 ACLS를 복원하는 것입니다. 단, DARs(direct=Y)는 예외입니다.
하중	Y, N	N	복구 작업에서 대상 볼륨의 볼륨 공간 및 inode 가용성을 확인해야 하는지 여부를 결정합니다. 이 변수를 'Y'로 설정하면 복원 작업에서 대상 경로의 볼륨 공간 및 inode 가용성 검사를 건너뜁니다. 대상 볼륨에 충분한 볼륨 공간 또는 inode를 사용할 수 없는 경우 복구 작업은 대상 볼륨 공간과 inode 가용성에 의해 허용되는 많은 데이터를 복구합니다. 볼륨 공간 또는 inode를 사용할 수 없는 경우 복구 작업이 중지됩니다.

환경 변수	유효한 값	기본값	설명
하이스트	Y, N	N	파일 기록 정보가 백업 응용 프로그램으로 전송되도록 지정합니다. 대부분의 상용 백업 애플리케이션은 HIST 변수를 Y로 설정합니다. 백업 작업의 속도를 증가시키거나 파일 기록 수집 문제를 해결하려는 경우 이 변수를 "N"으로 설정할 수 있습니다. 백업 응용 프로그램이 파일 기록을 지원하지 않는 경우 HIST 변수를 'Y'로 설정하지 않아야 합니다.

환경 변수	유효한 값	기본값	설명
ctime 무시	Y, N	N	이전 증분 백업 이후에 ctime 값만 변경된 경우 파일이 증분 백업되지 않도록 지정합니다. 바이러스 검사 소프트웨어와 같은 일부 응용 프로그램은 파일 또는 해당 속성이 변경되지 않았더라도 inode 내의 파일의 ctime 값을 변경합니다. 따라서 증분 백업은 변경되지 않은 파일을 백업할 수 있습니다. ctime 값이 수정되었기 때문에 증분 백업에 허용 가능한 시간 또는 공간이 필요한 경우에만 ignore_ctime 변수를 지정해야 합니다. NDMP dump 명령은 기본적으로 ignore_ctime을 false로 설정합니다. "참"으로 설정하면 다음과 같은 데이터 손실이 발생할 수 있습니다. 1. 볼륨 레벨 증분 ndmpcopy를 사용하여 ignore_ctime을 true로 설정하면 소스의 qtree에서 이동된 파일이 삭제됩니다. 볼륨

환경 변수	유효한 값	기본값	설명
ignore_cQtree	Y, N	N	복구 작업이 백업된 qtree에서 qtree 정보를 복원하지 않음을 지정합니다.
레벨	0-31입니다	0	백업 레벨을 지정합니다. 레벨 0은 전체 데이터 세트를 복사합니다. 0보다 높은 값으로 지정된 증분 백업 레벨은 마지막 증분 백업 이후 모든 파일(새 파일 또는 수정된 파일)을 복사합니다. 예를 들어 레벨 1은 레벨 0 백업 이후에 새 파일이나 수정된 파일을 백업하며, 레벨 2는 레벨 1 백업 이후에 새 파일이나 수정된 파일을 백업합니다.
목록	Y, N	N	에는 실제로 데이터를 복원하지 않고 백업된 파일 이름 및 inode 번호가 나와 있습니다.
list_qtree 를 참조하십시오	Y, N	N	에는 실제로 데이터를 복원하지 않는 백업 qtree가 나와 있습니다.
multi_subtree_names를 선택합니다	'트링'	"없음"	백업이 여러 하위 트리 백업임을 지정합니다. 하위 트리 이름의 줄 바꿈, null 종료 목록인 문자열에 여러 개의 하위 트리가 지정됩니다. 하위 트리는 목록의 마지막 요소로 지정해야 하는 공통 루트 디렉터리를 기준으로 경로 이름으로 지정됩니다. 이 변수를 사용하는 경우 dmp_name 변수도 사용해야 합니다.

환경 변수	유효한 값	기본값	설명
NDMP_Unicode_FH	Y, N	N	파일 기록 정보에 있는 파일의 NFS 이름 외에 유니코드 이름이 포함되도록 지정합니다. 이 옵션은 대부분의 백업 응용 프로그램에서 사용되지 않으며, 이러한 추가 파일 이름을 받도록 백업 응용 프로그램을 설계하지 않는 한 설정해서는 안 됩니다. HIST 변수도 설정해야 합니다.
no_acls입니다	Y, N	N	데이터를 백업할 때 ACL을 복제하지 않도록 지정합니다.
non_quota_tree	Y, N	N	데이터를 백업할 때 Qtree의 파일 및 디렉토리를 무시하도록 지정합니다. 'Y'로 설정하면 파일 시스템 변수에 의해 지정된 데이터 세트의 qtree에 있는 항목이 백업되지 않습니다. 이 변수는 파일 시스템 변수가 전체 볼륨을 지정하는 경우에만 적용됩니다. non_quota_tree 변수는 레벨 0 백업에서만 작동하며 multi_subtree_names 변수가 지정된 경우에는 작동하지 않습니다. non_quota_tree를 동시에 Y로 설정하면 백업 대상에서 제외되도록 지정된 파일 또는 디렉토리가 제외되지 않습니다.

환경 변수	유효한 값	기본값	설명
노와이ITE	Y, N	N	복구 작업이 디스크에 데이터를 쓰지 않도록 지정합니다. 이 변수는 디버깅에 사용됩니다.

환경 변수	유효한 값	기본값	설명
반복	Y, N	Y를 누릅니다	DAR 복원 중에 디렉토리 항목을 확장하도록 지정합니다. DIRECT 및 Enhanced_DAR_ENABLED 환경 변수('Y'로 설정)도 활성화해야 합니다. 반복 변수가 비활성화된 경우('N'으로 설정), 원본 소스 경로의 모든 디렉토리에 대한 사용 권한과 ACL만 테이프에서 복원되며 디렉토리의 내용은 복구되지 않습니다. recursive 변수가 N으로 설정되어 있거나 recover_full_paths 변수가 Y로 설정되어 있으면 복구 경로가 원래 경로로 끝나야 합니다. 재귀 변수를 사용하지 않도록 설정하고 복구 경로가 둘 이상인 경우 모든 복구 경로가 복구 경로의 가장 긴 경로에 포함되어야 합니다. 그렇지 않으면 오류 메시지가 표시됩니다. 예를 들어 모든 복구 경로가 "foo/dir1/딥디르/myfile" 내에 있으므로 다음과 같은 복구 경로가 유효합니다. • '/foo' • "/foo/dir" • '/foo/dir1/딥디더' • '/foo/dir1/딥디르/myfile' 다음은 잘못된 복구 경로입니다. '/foo'

환경 변수	유효한 값	기본값	설명
RECOVER_FULL_경로	Y, N	N	전체 복구 경로에 DAR 이후에 복구된 해당 권한과 ACL이 포함되도록 지정합니다. Direct 및 Enhanced_DAR_ENABLED도 활성화('Y'로 설정)해야 합니다. recover_full_paths가 Y로 설정된 경우 복구 경로는 원래 경로로 끝나야 합니다. 대상 볼륨에 디렉토리가 이미 있으면 해당 사용 권한 및 ACL이 테이프에서 복원되지 않습니다.
업데이트	Y, N	Y를 누릅니다	레벨 기반 증분 백업을 사용하도록 메타데이터 정보를 업데이트합니다.

SMTape에 지원되는 환경 변수입니다

환경 변수	유효한 값	기본값	설명
base_date 를 선택합니다	dump_date를 선택합니다	'-1'	증분 백업의 시작 날짜를 지정합니다. `BASE_DATE` 은 참조 스냅샷 식별자의 문자열 표현입니다. SMTape는 문자열을 사용하여 `BASE_DATE` 참조 스냅샷을 찾습니다. 기본 백업에는 base_date가 필요하지 않습니다. 증분 백업의 경우 이전 기준 또는 증분 백업의 DUMP_DATE 변수 값이 기본_DATE 변수에 할당됩니다. 백업 애플리케이션은 이전 SMTape 기준 또는 증분 백업에서 DUMP_DATE 값을 할당합니다.
dump_date 를 참조하십시오	RETURN_VALUE’입니다	"없음"	SMTape 백업이 끝날 때 dump_date에는 해당 백업에 사용된 스냅샷을 식별하는 문자열 식별자가 포함됩니다. 이 스냅샷은 후속 증분 백업을 위한 참조 스냅샷으로 사용할 수 있습니다. dump_date의 결과 값은 후속 증분 백업의 base_date 값으로 사용됩니다.

환경 변수	유효한 값	기본값	설명
SMTape_backup_set_ID 입니다	'트링'	"없음"	기본 백업과 관련된 증분 백업의 시퀀스를 식별합니다. 백업 세트 ID는 기본 백업 중에 생성되는 128비트 고유 ID입니다. 백업 애플리케이션은 증분 백업 중에 이 ID를 'MTAPE_BACKUP_SET_ID' 변수에 대한 입력으로 할당합니다.
SMTape_snapshot_name 입니다	볼륨에서 사용 가능한 모든 유효한 스냅샷입니다	유효하지 않습니다	SMTAPE_snapshot_name 변수가 스냅샷으로 설정되면 해당 스냅샷과 이전 스냅샷이 테이프에 백업됩니다. 증분 백업의 경우 이 변수는 증분 스냅샷을 지정합니다. base_date 변수는 기준 스냅샷을 제공합니다.
SMTape_delete_snapshot	Y, N	N	SMTape에 의해 자동으로 생성된 스냅샷의 경우 SMTAPE_DELETE_SNAPSHOT 변수가 로 설정된 경우 ɣ 백업 작업이 완료된 후 SMTape가 이 스냅샷을 삭제합니다. 그러나 백업 애플리케이션에서 생성된 스냅샷은 삭제되지 않습니다.
SMTape_break_mirror입니다	Y, N	N	SMTAPE_break_mirror 변수가 Y로 설정되면 성공한 복구 후 dP 유형의 볼륨이 RW 볼륨으로 변경됩니다.

일반적인 **ONTAP NDMP** 테이프 백업 토폴로지에 대해 알아보세요**.**

NDMP는 백업 애플리케이션과 스토리지 시스템 또는 데이터(파일 시스템)와 테이프 서비스를 제공하는 다른 NDMP 서버 간의 다양한 토폴로지 및 구성을 지원합니다.

스토리지 시스템-로컬-테이프

가장 간단한 구성에서는 백업 애플리케이션이 스토리지 시스템의 데이터를 스토리지 시스템에 연결된 테이프 서브시스템으로 백업합니다. NDMP 제어 접속은 네트워크 경계를 넘어 존재합니다. 데이터와 테이프 서비스 간에

스토리지 시스템 내에 존재하는 NDMP 데이터 접속을 NDMP 로컬 구성이라고 합니다.

다른 스토리지 시스템에 연결된 스토리지 시스템-테이프

또한 백업 애플리케이션은 스토리지 시스템의 데이터를 다른 스토리지 시스템에 연결된 테이프 라이브러리(하나 이상의 테이프 드라이브가 있는 미디어 체인저)로 백업할 수도 있습니다. 이 경우 데이터와 테이프 서비스 간의 NDMP 데이터 연결은 TCP 또는 TCP/IPv6 네트워크 연결을 통해 제공됩니다. 이를 NDMP 3-way 스토리지 시스템-스토리지 시스템 구성이라고 합니다.

스토리지 시스템-네트워크 연결 테이프 라이브러리

NDMP 지원 테이프 라이브러리는 3방향 구성의 변형을 제공합니다. 이 경우 테이프 라이브러리는 TCP/IP 네트워크에 직접 연결되며 내부 NDMP 서버를 통해 백업 애플리케이션 및 스토리지 시스템과 통신합니다.

스토리지 시스템-데이터 서버-테이프 또는 데이터 서버-스토리지 시스템-테이프

NDMP는 스토리지 시스템-데이터-서버 및 데이터-서버-스토리지 시스템 3방향 구성도 지원합니다. 스토리지 시스템 대 서버 를 사용하면 스토리지 시스템 데이터를 백업 애플리케이션 호스트 또는 다른 데이터 서버 시스템에 연결된 테이프 라이브러리에 백업할 수 있습니다. 서버-스토리지 시스템 구성을 사용하면 서버 데이터를 스토리지 시스템에 연결된 테이프 라이브러리에 백업할 수 있습니다.

ONTAP 지원 **NDMP** 인증 방법

NDMP 연결 요청을 허용하는 인증 방법을 지정할 수 있습니다. ONTAP는 스토리지 시스템에 대한 NDMP 액세스를 인증하는 두 가지 방법인 일반 텍스트 및 본인 확인 방법을 지원합니다.

노드 범위 NDMP 모드에서는 기본적으로 본인 확인 및 일반 텍스트가 모두 설정됩니다. 그러나 챌린지를 비활성화할 수는 없습니다. 일반 텍스트를 사용하거나 사용하지 않도록 설정할 수 있습니다. 일반 텍스트 인증 방법에서는 로그인 암호가 일반 텍스트로 전송됩니다.

SVM(스토리지 가상 시스템) 범위의 NDMP 모드에서는 기본적으로 인증 방법이 본인 확인 방법입니다. 노드 범위 NDMP 모드와 달리 이 모드에서는 일반 텍스트 및 본인 확인 인증 방법을 모두 사용하거나 사용하지 않도록 설정할 수 있습니다.

관련 정보

노드 범위 NDMP 모드의 사용자 인증

SVM 범위의 NDMP 모드에서 사용자 인증

ONTAP에서 지원되는 **NDMP** 확장

NDMP v4는 핵심 NDMP v4 프로토콜을 수정하지 않고 NDMP v4 프로토콜 확장을 생성하는 메커니즘을 제공합니다. ONTAP에서 지원하는 NDMP v4 확장에 대해 알고 있어야 합니다.

ONTAP에서 지원되는 NDMP v4 확장은 다음과 같습니다.

- 운전실(Cluster Aware Backup)

  이러한 확장은 SVM 범위의 NDMP 모드에서만 지원됩니다.

- IPv6 지원을 위한 CAE(Connection Address Extension)

- 확장 클래스 0x2050

  이 확장은 재시작 가능한 백업 작업 및 Snapshot Management Extensions를 지원합니다.

  > Snapshot Management Extensions의 일부인 이 `NDMP_SNAP_RECOVER` 메시지는 복구 작업을 시작하고 로컬 스냅샷에서 로컬 파일 시스템 위치로 복구된 데이터를 전송하는 데 사용됩니다. ONTAP에서 이 메시지를 통해 볼륨 및 일반 파일만 복구할 수 있습니다.
  >
  > 이 `NDMP_SNAP_DIR_LIST` 메시지를 통해 볼륨의 스냅샷을 탐색할 수 있습니다. 탐색 작업이 진행 중인 동안 무중단 작업이 발생하면 백업 애플리케이션이 탐색 작업을 다시 시작해야 합니다.

- NDMP 재시작 가능 백업 확장

  NDMP RBE(재시작 가능한 백업 확장) 기능을 사용하여 장애가 발생하기 전에 데이터 스트림의 알려진 체크포인트에서 백업을 재시작할 수 있습니다.

ONTAP NDMP의 향상된 **DAR** 기능에 대해 알아보세요**.**

디렉토리 DAR 및 파일 및 NT 스트림의 DAR에 향상된 직접 액세스 복구(DAR) 기능을 사용할 수 있습니다. 기본적으로 향상된 DAR 기능은 활성화되어 있습니다.

향상된 DAR 기능을 사용하도록 설정하면 오프셋 맵을 생성하여 테이프에 기록해야 하기 때문에 백업 성능에 영향을 줄 수 있습니다. 노드 범위 및 SVM(스토리지 가상 머신) 범위 NDMP 모드 모두에서 향상된 DAR를 설정하거나 해제할 수 있습니다.

NDMP 세션에 대한 **ONTAP** 확장성 제한

서로 다른 시스템 메모리 용량의 스토리지 시스템에서 동시에 설정할 수 있는 NDMP 세션의 최대 수를 알고 있어야 합니다. 이 최대 개수는 스토리지 시스템의 시스템 메모리에 따라 다릅니다.

다음 표에 설명된 제한은 NDMP 서버에 대한 것입니다. '덤프 백업 및 복원 세션에 대한 계산 제한' 섹션에 언급된 제한은 덤프 및 복원 세션에 대한 것입니다.

덤프 백업 및 복원 세션에 대한 확장성 제한

스토리지 시스템의 시스템 메모리입니다	최대 **NDMP** 세션 수입니다
16GB 미만	8
16GB보다 크거나 같지만 24GB보다 작습니다	20
24GB보다 크거나 같습니다	36

명령(노드 쉘을 통해 사용 가능)을 사용하여 스토리지 시스템의 시스템 메모리를 확보할 수 `sysconfig -a` 있습니다. 에 대한 자세한 내용은 `sysconfig -a` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP FlexGroup 볼륨을 통한 NDMP 지원에 대해 알아보세요.

ONTAP 9.7부터는 FlexGroup 볼륨에서 NDMP가 지원됩니다.

ONTAP 9.7부터는 ndmpcopy 명령이 FlexVol 볼륨과 FlexGroup 볼륨 간의 데이터 전송에 지원됩니다.

ONTAP 9.7에서 이전 버전으로 되돌릴 경우 이전 전송의 증분 전송 정보가 유지되지 않으므로 되돌리기 후 기본 복사를 수행해야 합니다.

ONTAP 9.8부터는 FlexGroup 볼륨에서 다음 NDMP 기능이 지원됩니다.

- 확장자 클래스 0x2050의 ndmp_snap_recover 메시지는 FlexGroup 볼륨에서 개별 파일을 복구하는 데 사용할 수 있습니다.
- FlexGroup 볼륨에 대해 NDMP RBE(재시작 가능한 백업 확장)가 지원됩니다.
- FlexGroup 볼륨에 대해 환경 변수 exclude 및 multi_subtree_names가 지원됩니다.

ONTAP SnapLock 볼륨을 사용한 NDMP에 대해 알아보세요

규제가 적용되는 데이터의 여러 복제본을 생성하면 중복 복구 시나리오를 사용할 수 있으며, NDMP 덤프 및 복구를 사용하면 SnapLock 볼륨에서 소스 파일의 WORM(Write Once, Read Many) 특성을 보존할 수 있습니다.

SnapLock 볼륨의 파일에 있는 WORM 속성은 데이터를 백업, 복원 및 복사할 때 유지되지만 WORM 속성은 SnapLock 볼륨으로 복원할 때만 적용됩니다. SnapLock 볼륨의 백업이 SnapLock 볼륨 이외의 볼륨으로 복원되는 경우 WORM 속성은 유지되지만 무시되며 ONTAP에서 적용되지 않습니다.

FlexVol 볼륨에 대한 노드 범위 NDMP 모드를 관리합니다

FlexVol 볼륨에 대한 **ONTAP** 노드 범위 **NDMP** 모드 관리에 대해 알아보세요.

NDMP 옵션과 명령을 사용하여 노드 레벨에서 NDMP를 관리할 수 있습니다. 'options' 명령을 사용하여 NDMP 옵션을 수정할 수 있습니다. 테이프 백업 및 복구 작업을 수행하려면 NDMP 관련 자격 증명을 사용하여 스토리지 시스템을 액세스해야 합니다.

에 대한 자세한 내용은 `options` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 노드 범위 NDMP 모드를 관리하기 위한 명령

'system services ndmp' 명령을 사용하여 노드 레벨에서 NDMP를 관리할 수 있습니다. 이러한 명령 중 일부는 더 이상 사용되지 않으며 향후 주요 릴리즈에서 제거될 예정입니다.

다음 NDMP 명령은 고급 권한 수준에서만 사용할 수 있습니다.

- '시스템 서비스 NDMP 서비스 종료
- '시스템 서비스 NDMP 서비스 시작'
- '시스템 서비스 NDMP 서비스 중지'
- '시스템 서비스 NDMP 로그 시작'

- 'System services ndmp log stop'(시스템 서비스 NDMP 로그 중지)

원하는 작업	이 명령 사용...
NDMP 서비스를 설정합니다	'System services NDMP on' *
NDMP 서비스를 해제합니다	'시스템 서비스 NDMP 꺼짐' *
NDMP 구성을 표시합니다	'system services ndmp show' * 를 참조하십시오
NDMP 구성을 수정합니다	'시스템 서비스 NDMP 수정' *
기본 NDMP 버전을 표시합니다	'시스템 서비스 NDMP 버전' *
NDMP 서비스 구성을 표시합니다	'시스템 서비스 NDMP 서비스 쇼'
NDMP 서비스 구성을 수정합니다	'시스템 서비스 NDMP 서비스 수정'
모든 NDMP 세션을 표시합니다	'시스템 서비스 NDMP 상태'
모든 NDMP 세션에 대한 자세한 정보를 표시합니다	'System services ndmp probe
지정된 NDMP 세션을 종료합니다	'시스템 서비스 NDMP kill'
모든 NDMP 세션을 종료합니다	'시스템 서비스 NDMP kill-all'
NDMP 암호를 변경합니다	'시스템 서비스 NDMP 암호' *
노드 범위 NDMP 모드를 설정합니다	'System services NDMP node-scope-mode on' *
노드 범위 NDMP 모드를 해제합니다	'System services NDMP node-scope-mode off' *
노드 범위의 NDMP 모드 상태를 표시합니다	'System services NDMP node-scope-mode status' *
모든 NDMP 세션을 강제로 종료합니다	'시스템 서비스 NDMP 서비스 종료
NDMP 서비스 데몬을 시작합니다	'시스템 서비스 NDMP 서비스 시작'
NDMP 서비스 데몬을 중지합니다	'시스템 서비스 NDMP 서비스 중지'
지정된 NDMP 세션에 대해 로깅을 시작합니다	'시스템 서비스 NDMP 로그 시작' *
지정된 NDMP 세션에 대한 로깅을 중지합니다	'System services ndmp log stop' *

- 이러한 명령은 더 이상 사용되지 않으며 향후 주요 릴리즈에서 제거될 예정입니다.

에 대한 자세한 내용은 `system services ndmp` "ONTAP 명령 참조입니다"을 참조하십시오.

노드 범위 **NDMP** 모드의 사용자 인증

노드 범위 NDMP 모드에서는 NDMP 관련 자격 증명을 사용하여 스토리지 시스템에 액세스해야 테이프 백업 및 복구 작업을 수행할 수 있습니다.

기본 사용자 ID는 ""root""입니다. 노드에서 NDMP를 사용하기 전에 NDMP 사용자와 연결된 기본 NDMP 암호를 변경해야 합니다. 기본 NDMP 사용자 ID를 변경할 수도 있습니다.

관련 정보

노드 범위의 NDMP 모드를 관리하는 명령입니다

노드 범위의 NDMP 모드는 무엇입니까

FlexVol 볼륨에 대한 SVM 범위의 NDMP 모드를 관리합니다

FlexVol 볼륨에 대한 **ONTAP SVM** 범위 **NDMP** 모드 관리에 대해 알아보세요.

NDMP 옵션 및 명령을 사용하여 SVM별로 NDMP를 관리할 수 있습니다. 'vserver services ndmp modify' 명령을 사용하여 NDMP 옵션을 수정할 수 있습니다. SVM 범위의 NDMP 모드에서는 사용자 인증이 역할 기반 액세스 제어 메커니즘과 통합됩니다.

"vserver modify" 명령을 사용하여 허용 또는 허용되지 않는 프로토콜 목록에 NDMP를 추가할 수 있습니다. 기본적으로 NDMP는 허용되는 프로토콜 목록에 있습니다. NDMP가 허용되지 않는 프로토콜 목록에 추가되면 NDMP 세션을 설정할 수 없습니다.

옵션을 사용하여 NDMP 데이터 연결이 설정되는 LIF 유형을 제어할 수 `-preferred-interface-role` 있습니다. NDMP 데이터 연결을 설정하는 동안 NDMP는 이 옵션에 지정된 LIF 유형에 속하는 IP 주소를 선택합니다. IP 주소가 이러한 LIF 유형 중 하나에 속하지 않으면 NDMP 데이터 연결을 설정할 수 없습니다. 에 대한 자세한 내용은 `vserver services ndmp modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SVM 범위 **NDMP** 모드를 관리하기 위한 명령

'vserver services NDMP' 명령을 사용하여 각 스토리지 가상 머신(SVM, 이전 명칭 Vserver)에서 NDMP를 관리할 수 있습니다.

원하는 작업	이 명령 사용...
NDMP 서비스를 설정합니다	'vserver services ndmp on' NDMP 서비스는 항상 클러스터의 모든 노드에서 설정해야 합니다. 'system services ndmp on' 명령을 사용하여 노드에서 NDMP 서비스를 설정할 수 있습니다. 기본적으로 NDMP 서비스는 노드에 대해 항상 설정됩니다.

원하는 작업	이 명령 사용...
NDMP 서비스를 해제합니다	'vserver services ndmp off'
NDMP 구성을 표시합니다	'vserver services ndmp show'
NDMP 구성을 수정합니다	'vserver services ndmp modify
기본 NDMP 버전을 표시합니다	'vserver services ndmp version
모든 NDMP 세션을 표시합니다	'vserver services ndmp status'
모든 NDMP 세션에 대한 자세한 정보를 표시합니다	'vserver services ndmp probe'
지정된 NDMP 세션을 종료합니다	'vserver services ndmp kill'
모든 NDMP 세션을 종료합니다	'vserver services ndmp kill-all'
NDMP 암호를 생성합니다	'vserver services ndmp generate-password
NDMP 확장 상태를 표시합니다	'vserver services ndmp extensions show' 이 명령은 고급 권한 수준에서 사용할 수 있습니다.
NDMP 확장 상태를 수정(설정 또는 해제)합니다	'vserver services ndmp extensions modify(SVM 서비스 NDMP 확장 수정 이 명령은 고급 권한 수준에서 사용할 수 있습니다.
지정된 NDMP 세션에 대해 로깅을 시작합니다	'vserver services ndmp log start'를 선택합니다 이 명령은 고급 권한 수준에서 사용할 수 있습니다.
지정된 NDMP 세션에 대한 로깅을 중지합니다	'vserver services ndmp log stop' 이 명령은 고급 권한 수준에서 사용할 수 있습니다.

에 대한 자세한 내용은 `vserver services ndmp` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

SVM 범위의 NDMP 모드를 관리하는 명령입니다

Cluster Aware Backup 확장의 기능

SVM 범위의 NDMP 모드는 무엇입니까

"시스템 관리"

ONTAP NDMP용 클러스터 인식 백업 확장에 대해 알아보세요

CAB(클러스터 인식 백업)은 NDMP v4 프로토콜 확장입니다. 이 확장을 통해 NDMP 서버는 볼륨을 소유하는 노드에서 데이터 연결을 설정할 수 있습니다. 또한 백업 애플리케이션에서 볼륨 및 테이프 디바이스가 클러스터의 동일한 노드에 있는지 확인할 수 있습니다.

NDMP 서버가 볼륨을 소유하는 노드를 식별하고 이러한 노드에서 데이터 연결을 설정하도록 하려면 백업 애플리케이션이 CAB 확장을 지원해야 합니다. CAB 확장을 사용하려면 백업 애플리케이션에서 데이터 연결을 설정하기 전에 백업 또는 복구할 볼륨에 대해 NDMP 서버에 알려야 합니다. 이를 통해 NDMP 서버가 볼륨을 호스팅하는 노드를 확인하고 데이터 연결을 적절하게 설정할 수 있습니다.

백업 애플리케이션에서 지원되는 CAB 확장을 통해 NDMP 서버는 볼륨 및 테이프 디바이스에 대한 선호도 정보를 제공합니다. 볼륨 및 테이프 디바이스가 클러스터의 동일한 노드에 있는 경우 이러한 선호도 정보를 사용하여 백업 애플리케이션이 3방향 백업 대신 로컬 백업을 수행할 수 있습니다.

다양한 **LIF** 유형의 백업 및 복원을 위한 **ONTAP** 볼륨 및 테이프 장치의 가용성

클러스터의 모든 LIF 유형에서 NDMP 제어 연결을 설정하도록 백업 애플리케이션을 구성할 수 있습니다. SVM(스토리지 가상 시스템) 범위의 NDMP 모드에서는 이러한 LIF 유형과 CAB 확장 상태에 따라 백업 및 복원 작업에 대한 볼륨 및 테이프 장치의 가용성을 결정할 수 있습니다.

다음 표에는 NDMP 제어 연결 LIF 유형에 대한 볼륨 및 테이프 디바이스의 가용성과 CAB 확장의 상태가 나와 있습니다.

백업 애플리케이션에서 운전실 확장이 지원되지 않는 경우 볼륨 및 테이프 장치의 가용성을 유지할 수 있습니다

NDMP 제어 연결 **LIF** 유형입니다	백업 또는 복원에 사용할 수 있는 볼륨입니다	백업 또는 복원에 사용할 수 있는 테이프 디바이스입니다
노드 관리 LIF	노드에서 호스팅하는 모든 볼륨	노드 관리 LIF를 호스팅하는 노드에 연결된 테이프 디바이스입니다
데이터 LIF	데이터 LIF를 호스팅하는 노드에서 호스팅되는 SVM에 속하는 볼륨만	없음
클러스터 관리 LIF	클러스터 관리 LIF를 호스팅하는 노드에서 호스팅하는 모든 볼륨입니다	없음
인터클러스터 LIF	인터클러스터 LIF를 호스팅하는 노드에 의해 호스팅되는 모든 볼륨입니다	인터클러스터 LIF를 호스팅하는 노드에 연결된 테이프 장치

백업 애플리케이션에서 **CAB** 확장을 지원하는 경우 볼륨 및 테이프 장치의 가용성

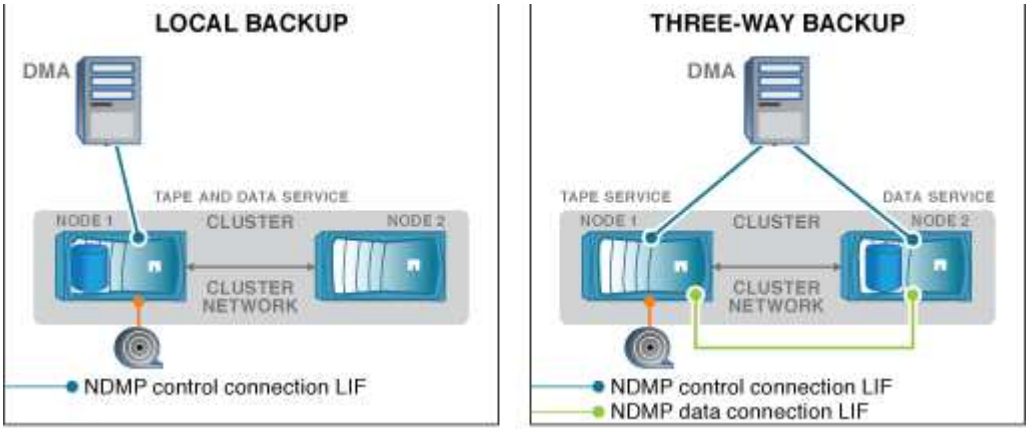
NDMP 제어 연결 **LIF** 유형입니다	백업 또는 복원에 사용할 수 있는 볼륨입니다	백업 또는 복원에 사용할 수 있는 테이프 디바이스입니다
노드 관리 LIF	노드에서 호스팅하는 모든 볼륨	노드 관리 LIF를 호스팅하는 노드에 연결된 테이프 디바이스입니다
데이터 LIF	데이터 LIF를 호스팅하는 SVM에 속한 모든 볼륨	없음
클러스터 관리 LIF	클러스터의 모든 볼륨	클러스터의 모든 테이프 디바이스
인터클러스터 LIF	클러스터의 모든 볼륨	클러스터의 모든 테이프 디바이스

ONTAP NDMP에 대한 친화성 정보에 대해 알아보세요

백업 애플리케이션이 CAB을 인식하면 NDMP 서버가 볼륨 및 테이프 디바이스에 대한 고유한 위치 정보를 제공합니다. 볼륨과 테이프 디바이스가 동일한 선호도를 공유하는 경우 이러한 선호도 정보를 사용하여 백업 애플리케이션이 3방향 백업 대신 로컬 백업을 수행할 수 있습니다.

노드 관리 LIF, 클러스터 관리 LIF에서 NDMP 제어 연결을 설정할 경우 또는 인터클러스터 LIF에서 백업 애플리케이션에서는 선호도 정보를 사용하여 볼륨 및 테이프 장치가 동일한 노드에 있는지 확인한 다음 로컬 또는 3방향 백업 또는 복원 작업을 수행할 수 있습니다. 데이터 LIF에서 NDMP 제어 연결이 설정되면 백업 애플리케이션이 항상 3방향 백업을 수행합니다.

로컬 **NDMP** 백업 및 **3**방향 **NDMP** 백업



DMA(백업 애플리케이션)는 볼륨 및 테이프 디바이스에 대한 선호도 정보를 사용하여 클러스터의 노드 1에 있는 볼륨 및 테이프 디바이스에 대해 로컬 NDMP 백업을 수행합니다. 볼륨이 노드 1에서 노드 2로 이동하는 경우 볼륨 및 테이프 디바이스에 대한 선호도 정보가 변경됩니다. 따라서 후속 백업을 위해 DMA는 3방향 NDMP 백업 작업을 수행합니다. 이렇게 하면 볼륨이 이동되는 노드에 관계없이 볼륨에 대한 백업 정책의 연속성을 보장할 수 있습니다.

관련 정보

Cluster Aware Backup 확장의 기능

NDMP 서버는 **SVM** 범위 모드에서 보안 **ONTAP** 제어 연결을 지원합니다**.**

보안 소켓(SSL/TLS)을 통신 메커니즘으로 사용하여 DMA(Data Management Application)와 NDMP 서버 간에 보안 제어 연결을 설정할 수 있습니다. 이 SSL 통신은 서버 인증서를 기반으로 합니다. NDMP 서버는 포트 30000에서 수신 대기합니다(IANA에서 ""ndmps"" 서비스에 할당).

이 포트에서 클라이언트와의 연결을 설정한 후 서버가 클라이언트에 인증서를 제공하는 표준 SSL 핸드셰이크가 발생합니다. 클라이언트가 인증서를 수락하면 SSL 핸드셰이크가 완료됩니다. 이 프로세스가 완료되면 클라이언트와 서버 간의 모든 통신이 암호화됩니다. NDMP 프로토콜 워크플로우는 이전과 동일하게 유지됩니다. 보안 NDMP 접속에는 서버 측 인증서 인증만 필요합니다. DMA는 보안 NDMP 서비스 또는 표준 NDMP 서비스에 연결하여 연결을 설정할 수 있습니다.

기본적으로 SVM(스토리지 가상 머신)에는 보안 NDMP 서비스가 사용되지 않습니다. 'vserver services ndmp modify -vserver vserver -is -secure-control -connection -enabled [true|false]' 명령을 사용하여 지정된 SVM에서 보안 NDMP 서비스를 설정하거나 해제할 수 있습니다.

NDMP ONTAP 데이터 연결 유형

SVM(스토리지 가상 머신) 범위의 NDMP 모드에서 지원되는 NDMP 데이터 연결 유형은 NDMP 제어 연결 LIF 유형과 CAB 확장 상태에 따라 다릅니다. 이 NDMP 데이터 연결 유형은 로컬 또는 3방향 NDMP 백업 또는 복구 작업을 수행할 수 있는지 여부를 나타냅니다.

TCP 또는 TCP/IPv6 네트워크를 통해 3방향 NDMP 백업 또는 복구 작업을 수행할 수 있습니다. 다음 표에서는 NDMP 제어 연결 LIF 유형과 CAB 확장의 상태를 기반으로 하는 NDMP 데이터 연결 유형을 보여 줍니다.

백업 애플리케이션에서 **CAB** 확장을 지원하는 경우의 **NDMP** 데이터 연결 유형입니다

NDMP 제어 연결 **LIF** 유형입니다	**NDMP** 데이터 연결 유형입니다
노드 관리 LIF	로컬, TCP, TCP/IPv6
데이터 LIF	TCP, TCP/IPv6
클러스터 관리 LIF	로컬, TCP, TCP/IPv6
인터클러스터 LIF	로컬, TCP, TCP/IPv6

백업 애플리케이션에서 **CAB** 확장을 지원하지 않는 경우 **NDMP** 데이터 연결 유형입니다

NDMP 제어 연결 **LIF** 유형입니다	**NDMP** 데이터 연결 유형입니다
노드 관리 LIF	로컬, TCP, TCP/IPv6
데이터 LIF	TCP, TCP/IPv6
클러스터 관리 LIF	TCP, TCP/IPv6

NDMP 제어 연결 **LIF** 유형입니다	**NDMP** 데이터 연결 유형입니다
인터클러스터 LIF	로컬, TCP, TCP/IPv6

관련 정보

Cluster Aware Backup 확장의 기능

"네트워크 관리"

SVM 범위 **NDMP** 모드에서 **ONTAP** 사용자 인증

SVM(스토리지 가상 시스템) 범위의 NDMP 모드에서는 NDMP 사용자 인증이 역할 기반 액세스 제어와 통합됩니다. SVM 맥락에서 NDMP 사용자는 ""vsadmin" 또는 ""vsadmin-backup" 역할을 가져야 합니다. 클러스터 컨텍스트에서 NDMP 사용자는 ""admin" 또는 ""backup" 역할이 있어야 합니다.

이러한 사전 정의된 역할을 제외하고, 사용자 지정 역할과 연결된 사용자 계정은 명령 디렉토리에 ""vserver services ndmp"" 폴더가 있고 폴더의 액세스 수준이 ""none""이 아닌 경우 NDMP 인증에 사용할 수 있습니다. 이 모드에서는 역할 기반 액세스 제어를 통해 생성된 특정 사용자 계정에 대해 NDMP 암호를 생성해야 합니다. admin 또는 백업 역할의 클러스터 사용자는 노드 관리 LIF, 클러스터 관리 LIF 또는 인터클러스터 LIF에 액세스할 수 있습니다. vsadmin-backup 또는 vsadmin 역할의 사용자는 해당 SVM의 데이터 LIF에만 액세스할 수 있습니다. 따라서 사용자의 역할에 따라 백업 및 복원 작업에 사용할 수 있는 볼륨 및 테이프 디바이스의 가용성이 달라집니다.

이 모드는 NIS 및 LDAP 사용자에 대한 사용자 인증도 지원합니다. 따라서 NIS 및 LDAP 사용자는 공통 사용자 ID 및 암호를 사용하여 여러 SVM에 액세스할 수 있습니다. 그러나 NDMP 인증은 Active Directory 사용자를 지원하지 않습니다.

이 모드에서는 사용자 계정이 SSH 애플리케이션 및 ""사용자 암호" 인증 방법과 연결되어 있어야 합니다.

관련 정보

SVM 범위의 NDMP 모드를 관리하는 명령입니다

"시스템 관리"

ONTAP NDMP 사용자를 위한 **NDMP** 특정 암호 생성

SVM(스토리지 가상 시스템) 범위의 NDMP 모드에서는 특정 사용자 ID에 대한 암호를 생성해야 합니다. 생성된 암호는 NDMP 사용자의 실제 로그인 암호를 기반으로 합니다. 실제 로그인 암호가 변경되면 NDMP 관련 암호를 다시 생성해야 합니다.

단계

1. NDMP 관련 암호를 생성하려면 'vserver services ndmp generate-password' 명령을 사용하십시오.

   현재 또는 미래의 모든 NDMP 작업에서 암호 입력이 필요한 경우 이 암호를 사용할 수 있습니다.

   스토리지 가상 시스템(SVM, 이전의 Vserver)에서 해당 SVM에 속하는 사용자에 대해서만 NDMP 암호를 생성할 수 있습니다.

   다음 예에서는 사용자 ID user1에 대한 NDMP 관련 암호를 생성하는 방법을 보여 줍니다.

```
cluster1::vserver services ndmp> generate-password -vserver vs1 -user
user1

Vserver: vs1
User: user1
Password: jWZiNt57huPOoD8d
```

2. 암호를 일반 스토리지 시스템 계정으로 변경하는 경우 이 절차를 반복하여 새 NDMP 관련 암호를 가져옵니다.

ONTAP MetroCluster 구성에서 재해 복구 중에 테이프 백업 및 복원 작업이 어떻게 영향을 받는가

MetroCluster 구성에서 재해 복구 중에 테이프 백업 및 복원 작업을 동시에 수행할 수 있습니다. 재해 복구 중에 이러한 작업이 어떻게 영향을 받는지 알아야 합니다.

재해 복구 관계에서 anSVM 볼륨에서 테이프 백업 및 복원 작업을 수행하는 경우, 전환 및 스위치백 후 증분 테이프 백업 및 복원 작업을 계속 수행할 수 있습니다.

FlexVol 볼륨의 덤프 엔진 정보

FlexVol 볼륨을 위한 **ONTAP** 덤프 엔진에 대해 알아보세요

덤프는 ONTAP의 스냅샷 기반 백업 및 복구 솔루션으로, 스냅샷에서 테이프 디바이스로 파일 및 디렉토리를 백업하고 백업된 데이터를 스토리지 시스템에 복구할 수 있도록 지원합니다.

덤프 백업을 사용하여 디렉토리, 파일 및 관련 보안 설정과 같은 파일 시스템 데이터를 테이프 디바이스에 백업할 수 있습니다. 전체 볼륨, 전체 qtree 또는 전체 볼륨 또는 전체 qtree가 아닌 하위 트리를 백업할 수 있습니다.

NDMP 호환 백업 애플리케이션을 사용하여 덤프 백업 또는 복구를 수행할 수 있습니다.

덤프 백업을 수행할 때 백업에 사용할 스냅샷을 지정할 수 있습니다. 백업에 대한 스냅샷을 지정하지 않으면 덤프 엔진이 백업에 대한 스냅샷을 생성합니다. 백업 작업이 완료되면 덤프 엔진이 이 스냅샷을 삭제합니다.

덤프 엔진을 사용하여 레벨 0, 증분 또는 차등 백업을 테이프에 수행할 수 있습니다.

Data ONTAP 8.3 이전의 릴리즈로 되돌린 후에는 증분 백업 작업을 수행하기 전에 기본 백업 작업을 수행해야 합니다.

관련 정보

"업그레이드, 되돌리기 또는 다운그레이드를 수행할 수 있습니다"

ONTAP NDMP를 사용한 덤프 백업 작동 방식

덤프 백업은 미리 정의된 프로세스를 사용하여 파일 시스템 데이터를 디스크에서 테이프로 씁니다. 볼륨, qtree 또는 전체 볼륨이나 qtree가 아닌 하위 트리를 백업할 수 있습니다.

다음 표에서는 ONTAP에서 덤프 경로로 표시된 개체를 백업하는 데 사용하는 프로세스를 설명합니다.

단계	조치
1	전체 볼륨 또는 전체 qtree 백업보다 작은 경우 ONTAP에서는 백업할 파일을 식별하기 위해 디렉토리를 통과합니다. 전체 볼륨 또는 qtree를 백업하는 경우 ONTAP는 이 단계를 2단계와 결합합니다.
2	전체 볼륨 또는 전체 qtree 백업의 경우 ONTAP는 백업할 볼륨 또는 qtree의 디렉토리를 식별합니다.
3	ONTAP는 디렉토리를 테이프에 기록합니다.
4	ONTAP는 파일을 테이프에 씁니다.
5	ONTAP는 ACL 정보(해당되는 경우)를 테이프에 기록합니다.

덤프 백업에서는 백업에 데이터 스냅샷을 사용합니다. 따라서 백업을 시작하기 전에 볼륨을 오프라인으로 전환할 필요가 없습니다.

덤프 백업은 생성하는 각 스냅샷의 이름을 `snapshot_for_backup.n` 지정합니다. 여기서 는 0부터 시작하는 정수입니다. `n` 덤프 백업이 스냅샷을 생성할 때마다 정수를 1씩 증가시킵니다. 스토리지 시스템이 재부팅되면 정수가 0으로 재설정됩니다. 백업 작업이 완료되면 덤프 엔진이 이 스냅샷을 삭제합니다.

ONTAP에서 동시에 여러 덤프 백업을 수행하면 덤프 엔진이 여러 개의 스냅샷을 생성합니다. 예를 들어 ONTAP에서 두 개의 덤프 백업을 동시에 실행하는 경우 데이터가 백업되는 볼륨에서 다음 스냅샷을 찾을 수 있습니다. `snapshot_for_backup.0` `snapshot_for_backup.1`

스냅샷에서 백업하는 경우 덤프 엔진은 추가 스냅샷을 생성하지 않습니다.

덤프 엔진이 백업하는 데이터 유형입니다

덤프 엔진을 사용하여 데이터를 테이프에 백업함으로써 재해 또는 컨트롤러 중단을 방지할 수 있습니다. 덤프 엔진은 파일, 디렉토리, qtree 또는 전체 볼륨과 같은 데이터 오브젝트를 백업할 뿐 아니라 각 파일에 대한 여러 유형의 정보를 백업할 수 있습니다. 덤프 엔진이 백업할 수 있는 데이터의 유형과 고려해야 할 제한 사항을 알면 재해 복구에 대한 접근 방식을 계획하는 데 도움이 됩니다.

덤프 엔진은 파일의 데이터 백업 외에도 각 파일에 대한 다음 정보를 필요에 따라 백업할 수 있습니다.

- UNIX GID, 소유자 UID 및 파일 권한
- UNIX 액세스, 생성 및 수정 시간
- 파일 형식
- 파일 크기
- DOS 이름, DOS 속성 및 생성 시간입니다
- 1,024개의 ACE(액세스 제어 항목)가 있는 ACL(액세스 제어 목록)
- Qtree 정보
- 접합 경로

연결 경로는 심볼 링크로 백업됩니다.

- LUN 및 LUN 복제

  전체 LUN 개체를 백업할 수 있지만 LUN 개체 내에서 단일 파일을 백업할 수는 없습니다. 마찬가지로, LUN 내에 단일 파일이 아니라 전체 LUN 개체를 복원할 수 있습니다.

  덤프 엔진은 LUN 클론을 독립 LUN으로 백업합니다.

- VM 정렬 파일

  Data ONTAP 8.1.2 이전 릴리즈에서는 VM 정렬 파일의 백업이 지원되지 않습니다.

스냅샷 지원 LUN 클론이 7-Mode에서 작동하는 Data ONTAP에서 ONTAP로 전환되면 일관성 없는 LUN이 됩니다. 덤프 엔진이 일관성 없는 LUN을 백업하지 않습니다.

볼륨에 데이터를 복구할 때는 복구 중인 LUN에서 클라이언트 입출력이 제한됩니다. LUN 제한은 덤프 복원 작업이 완료된 경우에만 제거됩니다. 마찬가지로, SnapMirror 단일 파일 또는 LUN 복원 작업 중에 클라이언트 I/O는 복원 중인 파일 및 LUN 모두에서 제한됩니다. 이 제한은 단일 파일 또는 LUN 복원 작업이 완료된 경우에만 제거됩니다. 덤프 복원 또는 SnapMirror 단일 파일 또는 LUN 복원 작업이 수행되고 있는 볼륨에서 덤프 백업을 수행하는 경우 클라이언트 I/O 제한이 있는 파일 또는 LUN은 백업에 포함되지 않습니다. 이러한 파일 또는 LUN은 클라이언트 입출력 제한이 제거된 경우 이후의 백업 작업에 포함됩니다.

Data ONTAP 8.3에서 실행 중이며 테이프에 백업된 LUN은 이전 릴리즈가 아닌 8.3 이상 릴리즈로만 복원할 수 있습니다. LUN이 이전 릴리즈로 복원되면 LUN이 파일로 복원됩니다.

SnapVault 보조 볼륨 또는 볼륨 SnapMirror 대상을 테이프에 백업하는 경우 볼륨의 데이터만 백업됩니다. 연결된 메타데이터는 백업되지 않습니다. 따라서 볼륨을 복원하려고 하면 해당 볼륨의 데이터만 복원됩니다. volume SnapMirror 관계에 대한 정보는 백업에서 제공되지 않으므로 복원되지 않습니다.

Windows NT 권한만 있는 파일을 덤프하고 UNIX 스타일 qtree 또는 볼륨으로 복원하면 해당 qtree 또는 볼륨에 대한 기본 UNIX 권한이 파일에 부여됩니다.

UNIX 사용 권한만 있는 파일을 덤프하고 NTFS 스타일 qtree 또는 볼륨으로 복원하면 해당 qtree 또는 볼륨에 대한 기본 Windows 사용 권한이 파일에 부여됩니다.

다른 덤프 및 복원으로 사용 권한이 보존됩니다.

VM 정렬 파일과 'VM 정렬 섹터' 옵션을 백업할 수 있습니다. VM 정렬 파일에 대한 자세한 내용은 을 참조하십시오 "논리적 스토리지 관리".

증가 체인과 **ONTAP NDMP**에 대해 알아보세요

증분 체인은 동일한 경로의 일련의 증분 백업입니다. 언제든지 백업 레벨을 지정할 수 있으므로 백업 및 복원을 효과적으로 수행할 수 있도록 증분 체인을 이해해야 합니다. 31가지 레벨의 증분 백업 작업을 수행할 수 있습니다.

증분 체인에는 두 가지 유형이 있습니다.

- 연속 증분 체인으로, 레벨 0부터 시작하여 각 후속 백업에서 1씩 상승하는 증분 백업의 시퀀스입니다.

- 증분 백업이 레벨을 건너뛰거나 0, 2, 3, 1, 2, 3, 1 등의 레벨이 시퀀스를 벗어난 경우 연속되지 않은 증분 체인입니다. 4 또는 0, 1, 1, 1 또는 0, 1, 2, 1, 2.

증분 백업은 가장 최근의 하위 레벨 백업을 기반으로 합니다. 예를 들어 백업 레벨 0, 2, 3, 1, 4의 시퀀스는 0, 2, 3 및 0, 1, 4의 두 증분 체인을 제공합니다. 다음 표에는 증분 백업의 기반이 정리되어 있습니다.

백업 순서	증분 수준	체인 증분	베이스	파일이 백업되었습니다
1	0	둘 다 해당되며	스토리지 시스템의 파일입니다	백업 경로에 있는 모든 파일
2	2	0, 2, 3	레벨 0 백업	레벨 0 백업 이후에 생성된 백업 경로의 파일입니다
3	3	0, 2, 3	레벨 2 백업	레벨 2 백업 이후에 생성된 백업 경로의 파일입니다
4	1	0, 1, 4	레벨 0 백업입니다. 레벨 1 백업보다 낮은 최신 레벨이기 때문입니다	레벨 0 백업 이후에 생성된 백업 경로의 파일(레벨 2 및 레벨 3 백업에 있는 파일 포함)입니다
5	4	0, 1, 4	레벨 1 백업은 하위 레벨이고 레벨 0, 레벨 2 또는 레벨 3 백업보다 최신이므로 레벨 1 백업입니다	레벨 1 백업 이후에 생성된 파일

차단 요소와 **ONTAP NDMP**에 대해 알아보세요

테이프 블록은 1,024바이트의 데이터입니다. 테이프 백업 또는 복원 중에 각 읽기/쓰기 작업에서 전송되는 테이프 블록 수를 지정할 수 있습니다. 이 수를 _blocking factor_라고 합니다.

4 ~ 256의 차단 계수를 사용할 수 있습니다. 백업을 수행하는 시스템 이외의 시스템에 백업을 복원하려는 경우 복원 시스템은 백업에 사용한 차단 계수를 지원해야 합니다. 예를 들어, 차단 계수 128을 사용하는 경우 해당 백업을 복원하는 시스템은 차단 계수 128을 지원해야 합니다.

NDMP 백업 중에 mover_record_size가 차단 계수를 결정합니다. ONTAP에서는 mover_record_size에 대해 최대 256KB의 값을 허용합니다.

ONTAP 덤프 백업을 다시 시작해야 하는 경우

테이프 쓰기 오류, 정전, 실수로 인한 사용자 중단 또는 스토리지 시스템의 내부 불일치 등과 같은 내부 또는 외부 오류로 인해 덤프 백업이 완료되지 않는 경우가 있습니다. 이러한 이유 중 하나로 인해 백업이 실패할 경우 백업을 다시 시작할 수 있습니다.

스토리지 시스템에서 트래픽이 많지 않은 기간을 피하거나 테이프 드라이브와 같은 스토리지 시스템의 다른 제한된 리소스에 대한 경쟁 방지를 위해 백업을 중단 및 재시작할 수 있습니다. 보다 긴급한 복원(또는 백업)에 동일한 테이프 드라이브가 필요한 경우 긴 백업을 중단하고 나중에 다시 시작할 수 있습니다. 재시작 가능한 백업은 재부팅 후에도 유지됩니다. 다음 조건이 참인 경우에만 중단된 테이프 백업을 다시 시작할 수 있습니다.

- 중단된 백업은 단계 IV에 있습니다
- dump 명령으로 잠긴 모든 관련 스냅샷을 사용할 수 있습니다.
- 파일 기록을 활성화해야 합니다.

이러한 덤프 작업이 중단되고 재시작 가능한 상태로 유지되면 연결된 스냅샷이 잠깁니다. 이러한 스냅샷은 백업 컨텍스트가 삭제된 후에 해제됩니다. 명령을 사용하여 백업 컨텍스트 목록을 볼 수 `vserver services ndmp restartable backup show` 있습니다.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

                        Vserver: vserver1
            Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
                   Volume Name: /vserver1/vol1
           Is Cleanup Pending?: false
            Backup Engine Type: dump
Is Snapshot Auto-created?: true
                   Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                   Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
               Has Offset Map?: true
                 Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
            Snapshot Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

덤프 복구는 미리 정의된 프로세스를 사용하여 파일 시스템 데이터를 테이프에서 디스크로 씁니다.

다음 표의 프로세스는 덤프 복구가 작동하는 방식을 보여 줍니다.

단계	조치
1	ONTAP는 테이프에서 추출해야 하는 파일을 카탈로그로 작성합니다.
2	ONTAP는 디렉토리와 빈 파일을 생성합니다.
3	ONTAP는 테이프에서 파일을 읽고 이를 디스크에 쓴 다음 해당 테이프에 대한 사용 권한(ACL 포함)을 설정합니다.
4	ONTAP는 지정된 모든 파일이 테이프에서 복사될 때까지 2단계와 3단계를 반복합니다.

덤프 엔진이 복원하는 데이터의 유형입니다

재해 또는 컨트롤러 중단이 발생할 경우 덤프 엔진은 단일 파일에서 파일 속성, 전체 디렉토리에 이르기까지 백업한 모든 데이터를 여러 가지 방법으로 복구할 수 있습니다. 덤프 엔진이 복구할 수 있는 데이터의 유형과 복구 방법을 언제 사용해야 다운타임을 최소화할 수 있는지 알고 있습니다.

데이터를 온라인 매핑된 LUN에 복원할 수 있습니다. 그러나 복구 작업이 완료될 때까지 호스트 애플리케이션이 이 LUN에 액세스할 수 없습니다. 복구 작업이 완료된 후 LUN 데이터의 호스트 캐시를 플러시하여 복구된 데이터에 대한 일관성을 제공해야 합니다.

덤프 엔진은 다음 데이터를 복구할 수 있습니다.

- 파일 및 디렉토리의 컨텐츠
- UNIX 파일 권한
- ACL

  NTFS qtree 또는 볼륨에 대한 UNIX 파일 권한만 있는 파일을 복원하는 경우 파일에 Windows NT ACL이 없습니다. 스토리지 시스템은 Windows NT ACL을 생성할 때까지 이 파일에 대한 UNIX 파일 권한만 사용합니다.

  > Data ONTAP 8.2를 실행하는 스토리지 시스템에서 백업된 ACL을 ACE 제한이 1,024 이하인 Data ONTAP 8.1.x 및 이전 버전의 스토리지 시스템으로 복원하는 경우 기본 ACL이 복원됩니다.

- Qtree 정보

  qtree 정보는 qtree가 볼륨의 루트에 복원되는 경우에만 사용됩니다. Qtree 정보는 "/vs1/vol1/subdir/lowerdir" 같은 하위 디렉토리로 qtree가 복원되고 qtree가 아닌 경우 사용되지 않습니다.

- 다른 모든 파일 및 디렉토리 속성
- Windows NT 스트림
- LUN을 클릭합니다

◦ LUN을 LUN으로 유지하려면 볼륨 레벨 또는 qtree 레벨로 복원해야 합니다.

디렉터리에 복원되면 유효한 메타데이터가 없기 때문에 파일로 복원됩니다.

◦ 7-Mode LUN은 ONTAP 볼륨에서 LUN으로 복구됩니다.

- 7-Mode 볼륨을 ONTAP 볼륨으로 복원할 수 있습니다.
- 대상 볼륨에 복원된 VM 정렬 파일은 대상 볼륨의 VM 정렬 속성을 상속합니다.
- 복구 작업의 대상 볼륨에 필수 잠금 또는 권장 잠금이 있는 파일이 있을 수 있습니다.

이러한 대상 볼륨에 대한 복구 작업을 수행하는 동안 덤프 엔진은 이러한 잠금을 무시합니다.

ONTAP NDMP로 데이터를 복원하기 전 고려 사항

백업된 데이터를 원래 경로 또는 다른 대상으로 복원할 수 있습니다. 백업된 데이터를 다른 대상으로 복원하는 경우 복원 작업을 위한 대상을 준비해야 합니다.

데이터를 원래 경로 또는 다른 대상으로 복원하기 전에 다음 정보가 있어야 하며 다음 요구 사항을 충족해야 합니다.

- 복구 수준입니다
- 데이터를 복원할 경로입니다
- 백업 중에 사용되는 차단 요소입니다
- 증분 복원을 수행하는 경우 모든 테이프가 백업 체인에 있어야 합니다
- 복원할 테이프와 호환 및 사용 가능한 테이프 드라이브

데이터를 다른 대상으로 복원하기 전에 다음 작업을 수행해야 합니다.

- 볼륨을 복원하는 경우 새 볼륨을 만들어야 합니다.
- qtree 또는 디렉토리를 복원하는 경우, 복원 중인 파일과 이름이 같은 파일을 이동하거나 이름을 변경해야 합니다.

ONTAP 9에서는 qtree 이름이 유니코드 형식을 지원합니다. 이전 버전의 ONTAP에서는 이 형식을 지원하지 않습니다. ONTAP 9의 유니코드 이름이 있는 qtree가 'ndmpcopy' 명령을 사용하여 ONTAP의 이전 릴리즈로 복제되거나 테이프의 백업 이미지에서 복원을 통해 복사되면 qtree가 유니코드 형식이 있는 qtree가 아닌 일반 디렉토리로 복원됩니다.

복구된 파일의 이름이 기존 파일과 같으면 복구된 파일이 기존 파일을 덮어씁니다. 그러나 디렉토리는 덮어쓰지 않습니다.

DAR를 사용하지 않고 복원 중에 파일, 디렉토리 또는 qtree의 이름을 바꾸려면 추출 환경 변수를 "E"로 설정해야 합니다.

대상 스토리지 시스템의 필수 공간입니다

대상 스토리지 시스템에 복원할 데이터 양보다 약 100MB의 공간이 필요합니다.

복구 작업은 복구 작업이 시작될 때 대상 볼륨의 볼륨 공간 및 inode 가용성을 확인합니다. 강제 환경 변수를 'Y'로 설정하면 복원 작업에서 대상 경로의 볼륨 공간 및 inode 가용성 검사를 건너뜁니다. 대상 볼륨에 사용 가능한 볼륨 공간 또는 inode가 충분하지 않은 경우 복구 작업은 대상 볼륨 공간과 inode 가용성에 의해 허용되는 데이터 양을 복구합니다. 볼륨 공간 또는 inode가 더 이상 남아 있지 않으면 복구 작업이 중지됩니다.

ONTAP 덤프 백업 및 복원 세션에 대한 확장성 제한

서로 다른 시스템 메모리 용량의 스토리지 시스템에서 동시에 수행할 수 있는 최대 덤프 백업 및 복원 세션 수에 대해 알고 있어야 합니다. 이 최대 개수는 스토리지 시스템의 시스템 메모리에 따라 다릅니다.

다음 표에 나와 있는 제한은 덤프 또는 복원 엔진에 대한 것입니다. NDMP 세션의 확장성 제한에서 언급한 제한은 엔진 제한값보다 높은 NDMP 서버에 대한 것입니다.

스토리지 시스템의 시스템 메모리입니다	총 덤프 백업 및 복원 세션 수입니다
16GB 미만	4
16GB보다 크거나 같지만 24GB보다 작습니다	16
24GB보다 크거나 같습니다	32

스토리지 시스템 내에서 데이터를 복제하기 위해 'ndmpcopy' 명령을 사용하는 경우 두 개의 NDMP 세션이 설정됩니다. 하나는 덤프 백업용이고 다른 하나는 덤프 복구용으로 설정됩니다.

명령(노드 쉘을 통해 사용 가능)을 사용하여 스토리지 시스템의 시스템 메모리를 확보할 수 `sysconfig -a` 있습니다. 에 대한 자세한 내용은 `sysconfig -a` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

NDMP 세션의 확장성 제한

ONTAP SVM 이름과 컨텍스트 **ID**를 제공하여 재시작 가능한 컨텍스트를 삭제합니다**.**

컨텍스트를 다시 시작하지 않고 백업을 시작하려면 컨텍스트를 삭제할 수 있습니다.

이 작업에 대해

SVM 이름과 컨텍스트 ID를 제공하여 "vserver services ndmp restable-backup delete" 명령을 사용하여 재시작 가능한 컨텍스트를 삭제할 수 있습니다.

단계

1. 재시작 가능한 컨텍스트 삭제:

   '* vserver services ndmp restarable-backup delete-vserver_vserver-name_-context-id_context_identifier_*'.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------- -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------- -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

ONTAP SnapVault 보조 볼륨에서 덤프가 작동하는 방식

SnapVault 보조 볼륨에 미러링되는 데이터에 대해 테이프 백업 작업을 수행할 수 있습니다. SnapVault 보조 볼륨에 미러링되는 데이터만 테이프에 백업할 수 있고 SnapVault 관계 메타데이터는 백업할 수 없습니다.

데이터 보호 미러 관계를 중단하거나 SnapMirror 재동기화가 발생하면 항상 기본 백업을 수행해야 합니다.

관련 정보

- "SnapMirror가 깨졌습니다"

ONTAP 스토리지 장애 조치 및 **ARL** 작업에서 덤프가 작동하는 방식

덤프 백업 또는 복원 작업을 수행하기 전에 이러한 작업이 스토리지 페일오버(테이크오버 및 반환) 또는 애그리게이트 재배치(ARL) 작업과 어떻게 연동되는지 이해해야 합니다. '-override-vetoes' 옵션은 스토리지 페일오버 또는 ARL 작업 중 덤프 엔진의 동작을 결정합니다.

덤프 백업 또는 복원 작업이 실행되고 '-override-vetoes' 옵션이 'false'로 설정되어 있으면 사용자 실행 스토리지 페일오버 또는 ARL 작업이 중지됩니다. 그러나 '–override-vetoes' 옵션이 true로 설정되어 있으면 스토리지 페일오버 또는 ARL 작업이 계속되고 덤프 백업 또는 복원 작업이 중단됩니다. 스토리지 시스템에 의해 스토리지 페일오버 또는 ARL 작업이 자동으로 시작되면 활성 덤프 백업 또는 복원 작업이 항상 중단됩니다. 스토리지 페일오버 또는 ARL 작업이 완료된 후에도 덤프 백업 및 복원 작업을 다시 시작할 수 없습니다.

운전실 확장이 지원되는 경우의 덤프 작업

백업 애플리케이션이 CAB 확장을 지원하는 경우 스토리지 페일오버 또는 ARL 작업 후 백업 정책을 재구성하지 않고 증분 덤프 백업 및 복원 작업을 계속 수행할 수 있습니다.

운전실 확장이 지원되지 않을 때 덤프 작업

백업 애플리케이션이 CAB 확장을 지원하지 않는 경우 백업 정책에 구성된 LIF를 대상 애그리게이트를 호스팅하는 노드로 마이그레이션할 경우 증분 덤프 백업 및 복원 작업을 계속 수행할 수 있습니다. 그렇지 않으면 스토리지 페일오버 및 ARL 작업 후에 증분 백업 작업을 수행하기 전에 기본 백업을 수행해야 합니다.

스토리지 페일오버 작업의 경우 백업 정책에 구성된 LIF를 파트너 노드로 마이그레이션해야 합니다.

관련 정보

"고가용성"

ONTAP 볼륨 이동 시 덤프 작동 방식

스토리지 시스템에서 최종 컷오버 단계를 시도할 때까지 테이프 백업 및 복원 작업과 볼륨 이동을 병렬로 실행할 수 있습니다. 이 단계 이후에는 이동 중인 볼륨에 대해 새 테이프 백업 및 복원 작업이 허용되지 않습니다. 그러나 현재 작업은 완료될 때까지 계속 실행됩니다.

다음 표에서는 볼륨 이동 작업 후 테이프 백업 및 복원 작업의 동작에 대해 설명합니다.

에서 테이프 백업 및 복원 작업을 수행하는 경우...	그러면...
백업 애플리케이션에서 CAB 확장이 지원되는 경우 SVM(스토리지 가상 머신) 범위가 NDMP 모드임	백업 정책을 재구성하지 않고도 읽기/쓰기 및 읽기 전용 볼륨에서 증분 테이프 백업 및 복원 작업을 계속 수행할 수 있습니다.
백업 애플리케이션에서 CAB 확장을 지원하지 않는 경우 SVM 범위의 NDMP 모드입니다	백업 정책에 구성된 LIF를 대상 애그리게이트를 호스팅하는 노드로 마이그레이션할 경우, 읽기/쓰기 및 읽기 전용 볼륨에서 증분 테이프 백업 및 복원 작업을 계속 수행할 수 있습니다. 그렇지 않으면 볼륨 이동 후 증분 백업 작업을 수행하기 전에 기본 백업을 수행해야 합니다.

볼륨 이동이 발생하는 경우, 대상 노드의 다른 SVM에 속한 볼륨의 이름이 이동한 볼륨의 이름과 동일한 경우 이동한 볼륨의 증분 백업 작업을 수행할 수 없습니다.

ONTAP FlexVol volume 가득 찼을 때 덤프가 작동하는 방식

증분 덤프 백업 작업을 수행하기 전에 FlexVol 볼륨에 충분한 여유 공간이 있는지 확인해야 합니다.

작업이 실패하면 크기를 늘리거나 스냅샷을 삭제하여 Flex Vol 볼륨의 여유 공간을 늘려야 합니다. 그런 다음 증분 백업 작업을 다시 수행합니다.

ONTAP 볼륨 액세스 유형이 변경될 때 덤프가 작동하는 방식

SnapMirror 대상 볼륨 또는 SnapVault 보조 볼륨의 상태가 읽기/쓰기에서 읽기 전용으로 또는 읽기 전용에서 읽기/쓰기로 변경되면 기본 테이프 백업 또는 복원 작업을 수행해야 합니다.

SnapMirror 타겟 및 SnapVault 보조 볼륨은 읽기 전용 볼륨입니다. 이러한 볼륨에 대해 테이프 백업 및 복원 작업을 수행할 경우 볼륨이 읽기 전용에서 읽기/쓰기 또는 읽기/쓰기에서 읽기 전용으로 상태가 변경될 때마다 기본 백업 또는 복원 작업을 수행해야 합니다.

ONTAP SnapMirror 단일 파일 또는 **LUN** 복원을 통한 덤프 작동 방식

SnapMirror 기술을 사용하여 단일 파일 또는 LUN이 복원되는 볼륨에서 덤프 백업 또는 복원 작업을 수행하기 전에 단일 파일 또는 LUN 복원 작업에서 덤프 작업이 어떻게 작동하는지 이해해야 합니다.

SnapMirror 단일 파일 또는 LUN 복원 작업 중에 클라이언트 I/O는 복원 중인 파일 또는 LUN에서 제한됩니다. 단일 파일 또는 LUN 복원 작업이 완료되면 파일 또는 LUN에 대한 입출력 제한이 제거됩니다. 단일 파일 또는 LUN이 복구되는 볼륨에서 덤프 백업을 수행하는 경우 클라이언트 I/O 제한이 있는 파일 또는 LUN은 덤프 백업에 포함되지 않습니다. 이후의 백업 작업에서는 입출력 제한이 제거된 후 이 파일 또는 LUN이 테이프로 백업됩니다.

동일한 볼륨에서 덤프 복구와 SnapMirror 단일 파일 또는 LUN 복원 작업을 동시에 수행할 수 없습니다.

ONTAP MetroCluster 구성에서 덤프 백업 및 복원 작업이 어떻게 영향을 받는가

MetroCluster 구성에서 덤프 백업 및 복원 작업을 수행하기 전에 스위치오버 또는 스위치백 작업이 수행될 때 덤프 작업이 어떻게 영향을 받는지 이해해야 합니다.

백업 또는 복구 작업을 덤프한 후 전환

클러스터 1과 클러스터 2의 두 클러스터를 고려합니다. 클러스터 1에서 덤프 백업 또는 복원 작업 중에 클러스터 1에서 클러스터 2로 전환이 시작되면 다음이 발생합니다.

- 'override-vetoes' 옵션의 값이 'false'이면 절체가 중단되고 백업 또는 복원 작업이 계속됩니다.
- 옵션 값이 true이면 덤프 백업 또는 복원 작업이 중단되고 전환이 계속됩니다.

백업 또는 복원 작업을 덤프한 다음 스위치백을 수행합니다

클러스터 1에서 클러스터 2로 전환이 수행되고 클러스터 2에서 덤프 백업 또는 복원 작업이 시작됩니다. 덤프 작업은 클러스터 2에 있는 볼륨을 백업 또는 복구합니다. 이 시점에서는 클러스터 2에서 클러스터 1로 스위치백을 시작한 경우 다음이 발생합니다.

- 'override-vetoes' 옵션의 값이 'false'인 경우, 스위치백을 취소하고 백업 또는 복원 작업을 계속합니다.
- 옵션 값이 true이면 백업 또는 복원 작업이 중단되고 스위치백이 계속됩니다.

스위치오버 또는 스위치백 중에 덤프 백업 또는 복원 작업이 시작되었습니다

클러스터 1에서 클러스터 2로 전환하는 동안 클러스터 1에서 덤프 백업 또는 복원 작업이 시작되면 백업 또는 복원 작업이 실패하고 전환이 계속됩니다.

클러스터 2에서 클러스터 1로 스위치백을 진행하는 동안 클러스터 2에서 덤프 백업 또는 복원 작업이 시작되면 백업

또는 복원 작업이 실패하고 스위치백을 계속합니다.

FlexVol 볼륨용 SMTape 엔진 정보

FlexVol 볼륨을 위한 ONTAP SMTape 엔진에 대해 알아보세요

SMTape는 데이터 블록을 테이프로 백업하는 ONTAP의 재해 복구 솔루션입니다. SMTape를 사용하여 테이프에 볼륨 백업을 수행할 수 있습니다. 그러나 qtree 또는 하위 트리 레벨에서 백업을 수행할 수 없습니다. SMTape는 기본 백업, 차등 백업 및 증분 백업을 지원합니다. SMTape에는 라이센스가 필요하지 않습니다.

NDMP 호환 백업 애플리케이션을 사용하여 SMTape 백업 및 복구 작업을 수행할 수 있습니다. SMTape를 선택하면 스토리지 가상 시스템(SVM) 범위 NDMP 모드에서만 백업 및 복원 작업을 수행할 수 있습니다.

> SMTape 백업 또는 복구 세션이 진행 중일 때는 되돌리기 프로세스가 지원되지 않습니다. 세션이 완료될 때까지 기다리거나 NDMP 세션을 중단해야 합니다.

SMTape를 사용하여 255개의 스냅샷을 백업할 수 있습니다. 이후 기준, 증분 또는 차등 백업의 경우 이전에 백업된 스냅샷을 삭제해야 합니다.

기준 복원을 수행하기 전에 데이터가 복원되는 볼륨은 DP 유형이어야 하며 이 볼륨은 제한된 상태여야 합니다. 성공적으로 복구되면 이 볼륨이 자동으로 온라인 상태가 됩니다. 백업을 수행한 순서대로 이 볼륨에 대해 이후의 증분 또는 차등 복원을 수행할 수 있습니다.

SMTape 백업 중 ONTAP 스냅샷 사용에 대해 알아보세요

SMTape 기준 백업 및 증분 백업 중에 스냅샷이 사용되는 방식을 이해해야 합니다. 또한 SMTape를 사용하여 백업을 수행하는 동안 유의해야 할 고려 사항도 있습니다.

기본 백업

기준 백업을 수행하는 동안 테이프에 백업할 스냅샷의 이름을 지정할 수 있습니다. 스냅샷이 지정되지 않은 경우 볼륨의 액세스 유형(읽기/쓰기 또는 읽기 전용)에 따라 스냅샷이 자동으로 생성되거나 기존 스냅샷이 사용됩니다. 백업에 대한 스냅샷을 지정하면 지정된 스냅샷보다 오래된 모든 스냅샷도 테이프에 백업됩니다.

백업에 대한 스냅샷을 지정하지 않으면 다음과 같은 현상이 발생합니다.

- 읽기/쓰기 볼륨의 경우 스냅샷이 자동으로 생성됩니다.

  새로 생성된 스냅샷과 모든 이전 스냅샷이 테이프에 백업됩니다.

- 읽기 전용 볼륨의 경우 최신 스냅샷을 포함한 모든 스냅샷이 테이프에 백업됩니다.

  백업이 시작된 후에 생성된 새 스냅샷은 백업되지 않습니다.

증분 백업

SMTape 증분 또는 차등 백업 작업의 경우 NDMP 호환 백업 애플리케이션에서 스냅샷을 생성하고 관리합니다.

증분 백업 작업을 수행하는 동안 항상 스냅샷을 지정해야 합니다. 성공적인 증분 백업 작업의 경우 이전 백업 작업(기본

또는 증분) 중에 백업된 스냅샷이 백업이 수행되는 볼륨에 있어야 합니다. 이 백업된 스냅샷을 사용하려면 백업 정책을 구성할 때 이 볼륨에 할당된 스냅샷 정책을 고려해야 합니다.

SnapMirror 대상에 대한 **SMTape** 백업 고려 사항

- 데이터 보호 미러 관계는 복제를 위해 대상 볼륨에 임시 스냅샷을 생성합니다.

  SMTape 백업에 이러한 스냅샷을 사용해서는 안 됩니다.

- 동일한 볼륨에서 SMTape 백업 작업 중에 데이터 보호 미러 관계의 대상 볼륨에서 SnapMirror 업데이트가 발생하면 SMTape에서 백업한 스냅샷은 소스 볼륨에서 삭제되지 않아야 합니다.

  백업 작업 중에 SMTape는 대상 볼륨의 스냅샷을 잠급니다. 소스 볼륨에서 해당 스냅샷이 삭제되면 후속 SnapMirror 업데이트 작업이 실패합니다.

- 증분 백업 중에는 이러한 스냅샷을 사용하지 마십시오.

ONTAP 테이프 백업 및 복원 작업을 최적화하는 **SMTape** 기능

스냅샷 백업, 증분 및 차등 백업, 복원된 볼륨에 대한 중복 제거 및 압축 기능 보존, 테이프 시딩과 같은 SMTape 기능을 사용하여 테이프 백업 및 복원 작업을 최적화할 수 있습니다.

SMTape는 다음과 같은 기능을 제공합니다.

- 재해 복구 솔루션을 제공합니다
- 증분 및 차등 백업을 지원합니다
- 스냅샷을 백업합니다
- 중복 제거된 볼륨을 백업 및 복원하고 복원된 볼륨에서 중복 제거를 유지할 수 있습니다
- 압축된 볼륨을 백업하고 복원된 볼륨의 압축을 유지합니다
- 테이프 시딩을 활성화합니다

SMTape는 4KB에서 256KB 사이의 4KB의 배수로 차단 계수를 지원합니다.

최대 2개의 주요 연속 ONTAP 릴리즈에서만 생성된 볼륨에 데이터를 복원할 수 있습니다.

SMTape 백업 및 복원 세션에 대한 **ONTAP** 확장성 제한

NDMP 또는 CLI(테이프 시드)를 통해 SMTape 백업 및 복원 작업을 수행하는 동안 시스템 메모리 용량이 서로 다른 스토리지 시스템에서 동시에 수행할 수 있는 SMTape 백업 및 복원 세션의 최대 수를 알고 있어야 합니다. 이 최대 개수는 스토리지 시스템의 시스템 메모리에 따라 다릅니다.

SMTape 백업 및 복구 세션 확장성 제한은 NDMP 세션 제한 및 덤프 세션 제한과 다릅니다.

스토리지 시스템의 시스템 메모리입니다	총 **SMTape** 백업 및 복구 세션 수입니다
16GB 미만	6

스토리지 시스템의 시스템 메모리입니다	총 **SMTape** 백업 및 복구 세션 수입니다
16GB보다 크거나 같지만 24GB보다 작습니다	16
24GB보다 크거나 같습니다	32

명령(노드 쉘을 통해 사용 가능)을 사용하여 스토리지 시스템의 시스템 메모리를 확보할 수 `sysconfig -a` 있습니다. 에 대한 자세한 내용은 `sysconfig -a` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- NDMP 세션의 확장성 제한
- 덤프 백업 및 복원 세션에 대한 확장성 제한

ONTAP 테이프 시딩에 대해 알아보세요

테이프 시딩은 데이터 보호 미러 관계에서 대상 FlexVol 볼륨을 초기화하는 데 도움이 되는 SMTape 기능입니다.

테이프 시딩을 사용하면 낮은 대역폭 연결을 통해 소스 시스템과 대상 시스템 간에 데이터 보호 미러 관계를 설정할 수 있습니다.

낮은 대역폭 연결을 통해 소스에서 대상으로 스냅샷을 증분 미러링할 수 있습니다. 그러나 기본 스냅샷의 초기 미러링은 저대역폭 연결보다 시간이 오래 걸립니다. 이 경우 소스 볼륨의 SMTape 백업을 테이프에 수행하고 테이프를 사용하여 초기 기본 스냅샷을 대상으로 전송할 수 있습니다. 그런 다음 낮은 대역폭 연결을 사용하여 대상 시스템에 대한 증분 SnapMirror 업데이트를 설정할 수 있습니다.

SMTape가 **ONTAP** 스토리지 장애 조치 및 **ARL** 작업과 함께 작동하는 방식

SMTape 백업 또는 복원 작업을 수행하기 전에 이러한 작업이 스토리지 페일오버(테이크오버 및 반환) 또는 애그리게이트 재배치(ARL) 작업에서 어떻게 작동하는지 이해해야 합니다. '-override-vetoes' 옵션은 스토리지 페일오버 또는 ARL 작업 중 SMTape 엔진의 동작을 결정합니다.

SMTape 백업 또는 복원 작업이 실행 중이고 '-override-vetoes' 옵션이 'false'로 설정되어 있으면 사용자 시작 스토리지 페일오버 또는 ARL 작업이 중지되고 백업 또는 복원 작업이 완료됩니다. 백업 애플리케이션이 CAB 확장을 지원하는 경우 백업 정책을 재구성하지 않고 증분 SMTape 백업 및 복원 작업을 계속 수행할 수 있습니다. 그러나 '–override-vetoes' 옵션이 "true"로 설정되어 있으면 스토리지 페일오버 또는 ARL 작업이 계속되고 SMTape 백업 또는 복원 작업이 중단됩니다.

관련 정보

"네트워크 관리"

"고가용성"

SMTape가 **ONTAP** 볼륨 이동과 함께 작동하는 방식

SMTape 백업 작업 및 볼륨 이동 작업은 스토리지 시스템이 최종 컷오버 단계를 시도할 때까지 병렬로 실행될 수 있습니다. 이 단계 이후에는 이동 중인 볼륨에서 새 SMTape 백업 작업을 실행할 수 없습니다. 그러나 현재 작업은 완료될 때까지 계속 실행됩니다.

볼륨의 컷오버 단계를 시작하기 전에 볼륨 이동 작업은 동일한 볼륨에서 활성 SMTape 백업 작업을 확인합니다. 활성 SMTape 백업 작업이 있는 경우 볼륨 이동 작업이 컷오버 지연 상태로 이동하고 SMTape 백업 작업을 완료할 수 있습니다. 이러한 백업 작업이 완료되면 볼륨 이동 작업을 수동으로 다시 시작해야 합니다.

백업 애플리케이션이 CAB 확장을 지원하는 경우 백업 정책을 재구성하지 않고도 읽기/쓰기 및 읽기 전용 볼륨에서 증분 테이프 백업 및 복원 작업을 계속 수행할 수 있습니다.

기본 복원 및 볼륨 이동 작업은 동시에 수행할 수 없지만 볼륨 이동 작업과 병행하여 증분 복원을 실행할 수 있으며, 볼륨 이동 작업 중에 SMTape 백업 작업과 유사한 동작을 수행할 수 있습니다.

SMTape가 **ONTAP** 볼륨 재호스트 작업과 함께 작동하는 방식

볼륨에서 볼륨 재호스트 작업이 진행 중인 경우 SMTape 작업을 시작할 수 없습니다. 볼륨이 볼륨 재호스트 작업에 관련되어 있는 경우 해당 볼륨에서 SMTape 세션을 시작하지 않아야 합니다.

볼륨 재호스트 작업이 진행 중인 경우 SMTape 백업 또는 복구가 실패합니다. SMTape 백업 또는 복구가 진행 중인 경우 볼륨 재호스트 작업이 실패하고 적절한 오류 메시지가 표시됩니다. 이 조건은 NDMP 기반 백업 및 CLI 기반 백업 또는 복구 작업에 모두 적용됩니다.

ADB 동안 **ONTAP NDMP** 백업 정책이 어떻게 영향을 받는가

ADB(자동 데이터 밸런서)가 활성화되면 밸런서는 애그리게이트의 사용 통계를 분석하여 구성된 상위 임계값 사용 비율을 초과한 애그리게이트를 식별합니다.

임계값을 초과한 애그리게이트를 식별한 후, 밸런서는 클러스터의 다른 노드에 있는 애그리게이트로 이동할 수 있는 볼륨을 식별하고 해당 볼륨을 이동하려고 시도합니다. 이 상황은 DMA(Data Management Application)가 CAB을 인식하지 못하는 경우 사용자가 백업 정책을 다시 구성하고 기본 백업 작업을 실행해야 하기 때문에 이 볼륨에 대해 구성된 백업 정책에 영향을 줍니다.

> DMA가 CAB을 인식하며 특정 인터페이스를 사용하여 백업 정책을 구성한 경우 ADB는 영향을 받지 않습니다.

ONTAP MetroCluster 구성에서 **SMTape** 백업 및 복원 작업이 어떻게 영향을 받는지

MetroCluster 구성에서 SMTape 백업 및 복원 작업을 수행하기 전에 전환 또는 스위치백 작업이 수행될 때 SMTape 작업이 어떤 영향을 받는지 알아야 합니다.

SMTape 백업 또는 복원 작업 후 전환

클러스터 1과 클러스터 2의 두 클러스터를 고려합니다. 클러스터 1에서 SMTape 백업 또는 복원 작업 중에 클러스터 1에서 클러스터 2로 전환을 시작하는 경우 다음이 발생합니다.

- '–override-vetoes' 옵션의 값이 false이면 전환 프로세스가 중단되고 백업 또는 복원 작업이 계속됩니다.
- 옵션 값이 "true"이면 SMTape 백업 또는 복구 작업이 중단되고 전환 프로세스가 계속됩니다.

SMTape 백업 또는 복원 작업 후 스위치백

클러스터 1에서 클러스터 2로 전환이 수행되고 클러스터 2에서 SMTape 백업 또는 복원 작업이 시작됩니다. SMTape 작업은 클러스터 2에 있는 볼륨을 백업 또는 복구합니다. 이 시점에서는 클러스터 2에서 클러스터 1로 스위치백을

시작한 경우 다음이 발생합니다.

- '–override-vetoes' 옵션의 값이 false이면 스위치백 프로세스가 중단되고 백업 또는 복원 작업이 계속됩니다.
- 옵션 값이 true이면 백업 또는 복원 작업이 중단되고 스위치백 프로세스가 계속됩니다.

전환 또는 스위치백 중에 **SMTape** 백업 또는 복원 작업이 시작되었습니다

클러스터 1에서 클러스터 2로 전환 프로세스 중에 클러스터 1에서 SMTape 백업 또는 복원 작업이 시작되면 백업 또는 복원 작업이 실패하고 전환이 계속됩니다.

클러스터 2에서 클러스터 1로 스위치백 프로세스 중에 클러스터 2에서 SMTape 백업 또는 복원 작업이 시작되는 경우 백업 또는 복원 작업이 실패하고 스위치백을 계속합니다.

FlexVol 볼륨에 대한 테이프 백업 및 복원 작업을 모니터링합니다

FlexVol 볼륨에 대한 **ONTAP** 테이프 백업 및 복원 작업 모니터링

이벤트 로그 파일을 보고 테이프 백업 및 복구 작업을 모니터링할 수 있습니다. ONTAP는 중요한 백업 및 복원 이벤트와 해당 이벤트가 발생한 시간을 컨트롤러의 '/etc/log/' 디렉토리에 있는 'backup'이라는 로그 파일에 자동으로 기록합니다. 기본적으로 이벤트 로깅은 "on"으로 설정됩니다.

다음과 같은 이유로 이벤트 로그 파일을 볼 수 있습니다.

- 야간 백업이 성공했는지 확인 중입니다
- 백업 작업에 대한 통계를 수집하는 중입니다
- 이전 이벤트 로그 파일의 정보를 사용하여 백업 및 복원 작업의 문제를 진단하는 데 사용됩니다

매주 한 번씩 이벤트 로그 파일이 회전합니다. '/etc/log/backup' 파일의 이름이 '/etc/log/backup.0'으로 바뀌고, '/etc/log/backup.0' 파일의 이름이 '/etc/log/backup.1'로 변경됩니다. 시스템은 로그 파일을 최대 6주 동안 저장하므로 최대 7개의 메시지 파일('/etc/log/backup.[0-5]' 및 현재 '/etc/log/backup' 파일)을 가질 수 있습니다.

테이프 백업 및 복원 작업을 위해 **ONTAP** 이벤트 로그 파일에 액세스합니다**.**

notes지옥의 'rdfile' 명령을 사용하여 '/etc/log/' 디렉토리에서 테이프 백업 및 복구 작업을 위한 이벤트 로그 파일에 액세스할 수 있습니다. 이러한 이벤트 로그 파일을 보고 테이프 백업 및 복원 작업을 모니터링할 수 있습니다.

이 작업에 대해

'pi' 웹 서비스를 이용할 수 있는 액세스 제어 역할 또는 'http' 액세스 방식으로 설정된 사용자 계정 등의 추가 구성을 통해 웹 브라우저를 사용하여 이러한 로그 파일에 액세스할 수도 있습니다.

단계

1. 노드 쉘에 액세스하려면 다음 명령을 입력합니다.

   ' * node run-node_node_name_ * '

   node_name은 노드의 이름입니다.

2. 테이프 백업 및 복원 작업을 위해 이벤트 로그 파일에 액세스하려면 다음 명령을 입력합니다.

   '* rdfile /etc/log/backup * '

관련 정보

"시스템 관리"

덤프 및 복원 이벤트 로그 메시지 형식은 무엇입니까

ONTAP 덤프 및 복원 이벤트 로그 메시지 형식

각 덤프 및 복원 이벤트에 대해 백업 로그 파일에 메시지가 기록됩니다.

덤프 및 복원 이벤트 로그 메시지의 형식은 다음과 같습니다.

'_TYPE TIMESTAMP IDENTIFIER EVENT (EVENT_INFO) _'

다음 목록에서는 이벤트 로그 메시지 형식의 필드를 설명합니다.

- 각 로그 메시지는 다음 표에 설명된 유형 표시기 중 하나로 시작됩니다.

유형	설명
로그	이벤트를 로깅하는 중입니다
DMP	덤프 이벤트
RST	복원 이벤트

- 타임 스탬프는 이벤트의 날짜와 시간을 표시합니다.
- 덤프 이벤트의 식별자 필드에는 덤프 경로와 덤프의 고유 ID가 포함됩니다. 복구 이벤트의 '식별자' 필드는 복구 대상 경로 이름만 고유 식별자로 사용합니다. 로깅 관련 이벤트 메시지에는 '식별자' 필드가 포함되지 않습니다.

ONTAP 로깅 이벤트에 대해 알아보세요

로그로 시작하는 메시지의 이벤트 필드는 로깅 시작 또는 로깅 종료를 지정합니다.

다음 표에 나와 있는 이벤트 중 하나가 포함되어 있습니다.

이벤트	설명
Start_Logging(로깅 시작)	로깅의 시작 또는 비활성화된 후 로깅이 다시 설정되었음을 나타냅니다.
Stop_Logging(로깅 중지)	로깅이 해제되었음을 나타냅니다.

ONTAP 덤프 이벤트에 대해 알아보세요

덤프 이벤트의 이벤트 필드에는 이벤트 유형 다음에 괄호 안에 이벤트 관련 정보가 표시됩니다.

다음 표에서는 덤프 작업에 대해 기록될 수 있는 이벤트, 설명 및 관련 이벤트 정보를 설명합니다.

이벤트	설명	이벤트 정보
시작	NDMP 덤프가 시작되었습니다	덤프 레벨과 덤프 유형입니다
끝	덤프가 성공적으로 완료되었습니다	처리된 데이터의 양입니다
중단	작업이 취소됩니다	처리된 데이터의 양입니다
옵션	지정된 옵션이 나열됩니다	NDMP 옵션을 포함한 모든 옵션과 관련 값
tape_open 을 참조하십시오	테이프가 읽기/쓰기를 위해 열려 있습니다	새 테이프 디바이스 이름입니다
테이프_닫기	읽기/쓰기를 위해 테이프가 닫혀 있습니다	테이프 디바이스 이름입니다
변경 단계	덤프가 새 처리 단계로 들어가고 있습니다	새 단계 이름입니다
오류	덤프에 예기치 않은 이벤트가 발생했습니다	오류 메시지
스냅샷	스냅샷이 생성되거나 배치됩니다	스냅샷의 이름과 시간입니다
base_dump입니다	내부 메타파일의 기본 덤프 항목이 있습니다	기본 덤프의 레벨 및 시간(증분 덤프에만 해당)

ONTAP 복원 이벤트에 대해 알아보세요

복원 이벤트의 이벤트 필드에는 이벤트 유형 다음에 이벤트 관련 정보가 괄호 안에 표시됩니다.

다음 표에서는 복구 작업을 위해 기록할 수 있는 이벤트, 설명 및 관련 이벤트 정보에 대한 정보를 제공합니다.

이벤트	설명	이벤트 정보
시작	NDMP 복구가 시작되었습니다	복구 레벨 및 복구 유형
끝	복원이 성공적으로 완료되었습니다	처리된 파일 수 및 데이터 양
중단	작업이 취소됩니다	처리된 파일 수 및 데이터 양

이벤트	설명	이벤트 정보
옵션	지정된 옵션이 나열됩니다	NDMP 옵션을 포함한 모든 옵션과 관련 값
tape_open 을 참조하십시오	테이프가 읽기/쓰기를 위해 열려 있습니다	새 테이프 디바이스 이름입니다
테이프_닫기	읽기/쓰기를 위해 테이프가 닫혀 있습니다	테이프 디바이스 이름입니다
변경 단계	복원이 새 처리 단계로 들어가고 있습니다	새 단계 이름입니다
오류	복원에서 예기치 않은 이벤트가 발생합니다	오류 메시지

ONTAP 테이프 백업 및 복원 작업에 대한 이벤트 로깅 활성화 또는 비활성화

이벤트 로깅을 설정하거나 해제할 수 있습니다.

단계

1. 이벤트 로깅을 사용하거나 사용하지 않도록 설정하려면 클러스터 쉘에서 다음 명령을 입력합니다.

   '* options_-option_name_backup.log.enable_-option-value_{on|off} *'

   On은 이벤트 로깅을 켭니다.

   OFF는 이벤트 로깅을 해제합니다.

   이벤트 로깅은 기본적으로 설정되어 있습니다.

FlexVol 볼륨의 테이프 백업 및 복원에 대한 오류 메시지입니다

백업 및 복원 오류 메시지

리소스 제한**:** 사용 가능한 스레드가 없습니다

- * 메시지 *

  자원 제한: 사용 가능한 스레드가 없습니다

- * 원인 *

  현재 사용 중인 최대 활성 로컬 테이프 입출력 스레드 수입니다. 최대 16개의 활성 로컬 테이프 드라이브를 사용할 수 있습니다.

- * 시정 조치 *

새 백업 또는 복원 작업을 시작하기 전에 일부 테이프 작업이 완료될 때까지 기다립니다.

테이프 예약이 사전 비어 있습니다

- * 메시지 *

  테이프 예약이 전제되었습니다

- * 원인 *

  테이프 드라이브가 다른 작업에서 사용 중이거나 테이프가 너무 일찍 닫혔습니다.

- * 시정 조치 *

  테이프 드라이브를 다른 작업에서 사용하고 있지 않은지, DMA 응용 프로그램이 작업을 중지하지 않았는지 확인한 다음 다시 시도하십시오.

미디어를 초기화할 수 없습니다

- * 메시지 *

  미디어를 초기화할 수 없습니다

- * 원인 *

  다음 이유 중 하나로 인해 이 오류가 발생할 수 있습니다.

  ◦ 백업에 사용된 테이프 드라이브가 손상되었거나 손상되었습니다.
  ◦ 테이프에 전체 백업이 포함되어 있지 않거나 손상되었습니다.
  ◦ 현재 사용 중인 최대 활성 로컬 테이프 입출력 스레드 수입니다.

  최대 16개의 활성 로컬 테이프 드라이브를 사용할 수 있습니다.

- * 시정 조치 *
  ◦ 테이프 드라이브가 손상되었거나 손상된 경우 유효한 테이프 드라이브로 작업을 재시도하십시오.
  ◦ 테이프에 전체 백업이 포함되어 있지 않거나 손상된 경우 복구 작업을 수행할 수 없습니다.
  ◦ 테이프 리소스를 사용할 수 없는 경우 일부 백업 또는 복구 작업이 완료될 때까지 기다린 다음 작업을 다시 시도하십시오.

진행 중인 최대 허용 덤프 또는 복원 수(최대 세션 제한)

- * 메시지 *

  허용되는 덤프 또는 복원 횟수 중 최대값 _ (최대 세션 제한) _ 이(가) 진행 중입니다

- * 원인 *

  최대 백업 또는 복원 작업 수가 이미 실행 중입니다.

- * 시정 조치 *

  현재 실행 중인 일부 작업이 완료된 후 작업을 재시도하십시오.

테이프 쓰기의 미디어 오류입니다

- * 메시지 *

  테이프 쓰기의 미디어 오류

- * 원인 *

  백업에 사용된 테이프가 손상되었습니다.

- * 시정 조치 *

  테이프를 교체하고 백업 작업을 다시 시도하십시오.

테이프 쓰기에 실패했습니다

- * 메시지 *

  테이프 쓰기가 실패했습니다

- * 원인 *

  백업에 사용된 테이프가 손상되었습니다.

- * 시정 조치 *

  테이프를 교체하고 백업 작업을 다시 시도하십시오.

테이프 쓰기 실패 - 새 테이프에 미디어 오류가 발생했습니다

- * 메시지 *

  테이프 쓰기 실패 - 새 테이프에 미디어 오류가 발생했습니다

- * 원인 *

  백업에 사용된 테이프가 손상되었습니다.

- * 시정 조치 *

  테이프를 교체하고 백업을 다시 시도하십시오.

테이프 쓰기 실패 - 새 테이프가 파손되었거나 쓰기 보호되어 있습니다

- * 메시지 *

  테이프 쓰기 실패 - 새 테이프가 파손되었거나 쓰기 보호되어 있습니다

- * 원인 *

  백업에 사용된 테이프가 손상되었거나 쓰기 보호되어 있습니다.

- * 시정 조치 *

  테이프를 교체하고 백업을 다시 시도하십시오.

테이프 쓰기 실패 - 새 테이프가 이미 미디어 끝에 있습니다

- * 메시지 *

  테이프 쓰기 실패 - 새 테이프가 이미 미디어 끝에 있습니다

- * 원인 *

  테이프에 공간이 부족하여 백업을 완료할 수 없습니다.

- * 시정 조치 *

  테이프를 교체하고 백업을 다시 시도하십시오.

테이프 쓰기 오류입니다

- * 메시지 *

  테이프 쓰기 오류 - 이전 테이프의 최소 용량(MB)이 이 이 테이프 작업의 최소 용량(MB)보다 적었습니다. 작업을 처음부터 다시 시작해야 합니다

- * 원인 *

  테이프 용량이 부족하여 백업 데이터를 포함할 수 없습니다.

- * 시정 조치 *

  용량이 큰 테이프를 사용하고 백업 작업을 재시도하십시오.

테이프 읽기에서 미디어 오류가 발생했습니다

- * 메시지 *

  '테이프 읽기에 미디어 오류'

- * 원인 *

  데이터가 복구되는 테이프가 손상되어 전체 백업 데이터가 포함되어 있지 않을 수 있습니다.

- * 시정 조치 *

  테이프에 전체 백업이 있는지 확인하려면 복구 작업을 다시 시도하십시오. 테이프에 전체 백업이 포함되어 있지 않으면 복구 작업을 수행할 수 없습니다.

테이프 읽기 오류입니다

- * 메시지 *

  "테이프 읽기 오류"

- * 원인 *

  테이프 드라이브가 손상되었거나 테이프에 전체 백업이 포함되어 있지 않습니다.

- * 시정 조치 *

  테이프 드라이브가 손상된 경우 다른 테이프 드라이브를 사용하십시오. 테이프에 전체 백업이 포함되어 있지 않으면 데이터를 복원할 수 없습니다.

이미 테이프 끝에 있습니다

- * 메시지 *

  이미 테이프 끝에 있습니다

- * 원인 *

  테이프에 데이터가 포함되어 있지 않거나 되감아야 합니다.

- * 시정 조치 *

  테이프에 데이터가 포함되어 있지 않은 경우 백업이 포함된 테이프를 사용하고 복구 작업을 다시 시도하십시오. 그렇지 않으면 테이프를 되감고 복구 작업을 다시 시도하십시오.

테이프 레코드 크기가 너무 작습니다. 더 큰 크기로 시도하십시오.

- * 메시지 *

  테이프 레코드 크기가 너무 작습니다. 더 큰 사이즈를 시도해 보세요

- * 원인 *

  복구 작업에 지정된 차단 계수가 백업 중에 사용된 차단 요소보다 작습니다.

- * 시정 조치 *

  백업 중에 지정된 것과 동일한 차단 계수를 사용합니다.

테이프 레코드 크기는 **block_size1**이 아니라 **block_size2**여야 합니다

- * 메시지 *

  테이프 레코드 크기는 block_size1이 아니라 block_size2여야 합니다

- * 원인 *

로컬 복구에 대해 지정된 차단 계수가 잘못되었습니다.

- * 시정 조치 *

  블록 크기1을 차단 요소로 사용하여 복원 작업을 재시도하십시오.

테이프 레코드 크기는 **4KB**에서 **256KB** 사이여야 합니다

- * 메시지 *

  테이프 레코드 크기는 4KB에서 256KB 사이여야 합니다

- * 원인 *

  백업 또는 복원 작업에 대해 지정된 차단 계수가 허용 범위 내에 있지 않습니다.

- * 시정 조치 *

  4KB ~ 256KB 범위의 차단 계수를 지정합니다.

NDMP 오류 메시지입니다

네트워크 통신 오류입니다

- * 메시지 *

  네트워크 통신 오류

- * 원인 *

  NDMP 3-way 연결에서 원격 테이프에 대한 통신이 실패했습니다.

- * 시정 조치 *

  원격 Mover에 대한 네트워크 연결을 확인하십시오.

Read Socket 의 메시지**: error_string**

- * 메시지 *

  '읽기 소켓의 메시지: error_string'

- * 원인 *

  NDMP 3-way 연결에서 원격 테이프에서 통신 복구 시 오류가 발생했습니다.

- * 시정 조치 *

  원격 Mover에 대한 네트워크 연결을 확인하십시오.

Write Dirnet의 메시지**: error_string**

- * 메시지 *

  '쓰기 Dirnet의 메시지: error_string'

- * 원인 *

  NDMP 3-way 연결에서 원격 테이프에 대한 백업 통신에 오류가 있습니다.

- * 시정 조치 *

  원격 Mover에 대한 네트워크 연결을 확인하십시오.

소켓 수신 **EOF**를 판독합니다

- * 메시지 *

  Read Socket Received EOF(읽기 소켓 수신 EOF)

- * 원인 *

  NDMP 3방향 연결에서 원격 테이프와 파일 끝 표시에 도달하려고 했습니다. 블록 크기가 더 큰 백업 이미지에서 3방향 복원을 시도할 수 있습니다.

- * 시정 조치 *

  올바른 블록 크기를 지정하고 복구 작업을 재시도하십시오.

ndmpd 잘못된 버전 번호**: version_number '**

- * 메시지 *

  'ndmpd 잘못된 버전 번호: version_number'

- * 원인 *

  지정된 NDMP 버전은 스토리지 시스템에서 지원되지 않습니다.

- * 시정 조치 *

  NDMP 버전 4를 지정합니다.

ndmpd 세션 **session_ID**가 활성 상태가 아닙니다

- * 메시지 *

  ndmpd session session_ID not active

- * 원인 *

  NDMP 세션이 없을 수 있습니다.

- * 시정 조치 *

  활성 NDMP 세션을 보려면 'ndmpd status' 명령을 사용합니다.

volume volume_name에 대한 **vol ref**를 가져올 수 없습니다

- * 메시지 *

  'vol_name 볼륨에 대한 vol ref를 얻을 수 없습니다.

- * 원인 *

  볼륨이 다른 작업에서 사용 중이므로 볼륨 참조를 가져올 수 없습니다.

- * 시정 조치 *

  나중에 작업을 다시 시도하십시오.

["IPv6"|"IPv4"] 제어 연결에서는 데이터 연결 유형 **["NDMP4_ADDR_TCP_IPv6"]** 이(가) 지원되지 않습니다

- * 메시지 *

  ["IPv6"|"IPv4"] 제어 연결에 대해 Data 연결 유형 ["NDMP4_ADDR_TCP_IPv6"] 지원되지 않습니다

- * 원인 *

  노드 범위 NDMP 모드에서는 설정된 NDMP 데이터 연결이 NDMP 제어 연결과 동일한 네트워크 주소 유형(IPv4 또는 IPv6)이어야 합니다.

- * 시정 조치 *

  백업 애플리케이션 공급업체에 문의하십시오.

데이터 수신**: CAB** 데이터 연결 준비 전제 조건 오류

- * 메시지 *

  dATA Listen: cab data connection prepare pre전제 조건 오류

- * 원인 *

  백업 애플리케이션이 NDMP 서버와 CAB 확장을 협상하고 NDMP_CAB_DATA_CONN_Prepare 및 NDMP_DATA_LECEIVE 메시지 간에 지정된 NDMP 데이터 연결 주소 유형이 일치하지 않으면 NDMP 데이터 수신 작업이 실패합니다.

- * 시정 조치 *

  백업 애플리케이션 공급업체에 문의하십시오.

데이터 연결**:CAB** 데이터 연결 준비 전제 조건 오류

- * 메시지 *

  "cab data connection prepare pre전제 조건 오류"

- * 원인 *

  백업 애플리케이션이 NDMP 서버와 CAB 확장을 협상하고 NDMP_CAB_DATA_CONN_Prepare 및 NDMP_DATA_CONNECT 메시지 간에 지정된 NDMP 데이터 연결 주소 유형이 일치하지 않으면 NDMP 데이터 연결이 실패합니다.

- * 시정 조치 *

  백업 애플리케이션 공급업체에 문의하십시오.

오류**:** 표시 실패**: '<**사용자 이름**>'** 사용자의 암호를 가져올 수 없습니다**.**

- * 메시지 *

  '<오류: 표시 실패: '<사용자 이름>' 사용자의 암호를 가져올 수 없습니다

- * 원인 *

  NDMP에 대한 사용자 계정 구성이 불완전합니다

- * 시정 조치 *

  사용자 계정이 SSH 액세스 방법과 연결되어 있고 인증 방법이 사용자 암호인지 확인합니다.

덤프 오류 메시지

대상 볼륨이 읽기 전용입니다

- * 메시지 *

  대상 볼륨이 읽기 전용입니다

- * 원인 *

  복구 작업이 시도되는 경로는 읽기 전용입니다.

- * 시정 조치 *

  데이터를 다른 위치로 복원해 보십시오.

타겟 **qtree**는 읽기 전용입니다

- * 메시지 *

  "대상 qtree는 읽기 전용입니다.

- * 원인 *

  복원이 시도되는 qtree는 읽기 전용입니다.

- * 시정 조치 *

  데이터를 다른 위치로 복원해 보십시오.

볼륨에 대해 일시적으로 비활성화된 덤프를 다시 시도하십시오

- * 메시지 *

  볼거리가 일시적으로 부피를 사용할 수 없게 되었습니다. 다시 시도하십시오

- * 원인 *

  NDMP 덤프 백업은 '스냅샷 중단' 또는 '스냅샷 재동기화' 작업의 일부인 SnapMirror 대상 볼륨에서 시도됩니다.

- * 시정 조치 *

  '스냅샷 미러 중단' 또는 '스냅샷 미러 재동기화' 작업이 완료될 때까지 기다린 다음 덤프 작업을 수행합니다.

> SnapMirror 대상 볼륨의 상태가 읽기/쓰기에서 읽기 전용으로 또는 읽기 전용에서 읽기/쓰기로 변경될 때마다 기본 백업을 수행해야 합니다.

관련 정보

- "SnapMirror가 깨졌습니다"
- "스냅미러 재동기화"

NFS 레이블을 인식할 수 없습니다

- * 메시지 *

  "오류: 중단 중: 덤프가 파일 시스템에서 NFS 보안 레이블을 발견했습니다.

- * 원인 *

  NFS 보안 레이블은 NFSv4.2가 활성화된 경우 ONTAP 9.9.1부터 지원됩니다. 그러나 덤프 엔진에서 NFS 보안 레이블을 현재 인식하지 않습니다. 파일, 디렉토리 또는 덤프 형식의 특수 파일에 NFS 보안 레이블이 있으면 덤프가 실패합니다.

- * 시정 조치 *

  파일 또는 디렉토리에 NFS 보안 레이블이 없는지 확인합니다.

파일이 생성되지 않았습니다

- * 메시지 *

  파일이 생성되지 않았습니다

- * 원인 *

  향상된 DAR 기능을 사용하지 않고 DAR 디렉토리 DAR을 시도했습니다.

- * 시정 조치 *

  향상된 DAR 기능을 사용하도록 설정하고 DAR를 다시 시도합니다.

file name> 파일을 복원하지 못했습니다

- * 메시지 *

  파일 이름을 복원하지 못했습니다

- * 원인 *

  대상 볼륨에 있는 LUN의 파일 이름과 동일한 파일 이름의 DAR(Direct Access Recovery)이 수행된 경우 DAR가 실패합니다.

- * 시정 조치 *

  파일의 DAR를 다시 시도하십시오.

src inode <inode number>... 에 대한 잘라내기에 실패했습니다

- * 메시지 *

  "src inode <inode number>에 대한 잘림 실패. 오류 <오류 번호>. inode를 건너뜁니다

- * 원인 *

  파일 inode는 파일이 복원될 때 삭제됩니다.

- * 시정 조치 *

  해당 볼륨을 사용하기 전에 볼륨의 복원 작업이 완료될 때까지 기다립니다.

덤프에 필요한 스냅샷을 잠글 수 없습니다

- * 메시지 *

  "덤프에 필요한 스냅샷을 잠글 수 없습니다.

- * 원인 *

  백업에 지정된 스냅샷을 사용할 수 없습니다.

- * 시정 조치 *

  다른 스냅샷을 사용하여 백업을 재시도합니다.

명령을 사용하여 `snap list` 사용 가능한 스냅샷 목록을 봅니다.

에 대한 자세한 내용은 `snap list` "ONTAP 명령 참조입니다"을 참조하십시오.

비트맵 파일을 찾을 수 없습니다

- * 메시지 *

  비트맵 파일을 찾을 수 없습니다

- * 원인 *

  백업 작업에 필요한 비트맵 파일이 삭제되었을 수 있습니다. 이 경우 백업을 다시 시작할 수 없습니다.

- * 시정 조치 *

  백업을 다시 수행합니다.

볼륨이 일시적으로 전환 상태입니다

- * 메시지 *

  용적이 과도기 상태에 있습니다

- * 원인 *

  백업되는 볼륨이 일시적으로 마운트 해제 상태입니다.

- * 시정 조치 *

  잠시 기다린 후 백업을 다시 수행합니다.

SMTape 오류 메시지입니다

청크가 순서가 아닙니다

- * 메시지 *

  "덩어리가 오르지 않았습니다.

- * 원인 *

  백업 테이프가 올바른 순서로 복구되지 않습니다.

- * 시정 조치 *

  복구 작업을 재시도하고 올바른 순서로 테이프를 로드합니다.

청크 형식이 지원되지 않습니다

- * 메시지 *

청크 형식이 지원되지 않습니다

- * 원인 *

  백업 이미지가 SMTape가 아닙니다.

- * 시정 조치 *

  백업 이미지가 SMTape가 아닌 경우 SMTape 백업이 있는 테이프를 사용하여 작업을 재시도하십시오.

메모리를 할당하지 못했습니다

- * 메시지 *

  메모리를 할당하지 못했습니다

- * 원인 *

  시스템의 메모리가 부족합니다.

- * 시정 조치 *

  시스템 사용량이 너무 많으면 나중에 작업을 다시 시도하십시오.

데이터 버퍼를 가져오지 못했습니다

- * 메시지 *

  데이터 버퍼를 가져오지 못했습니다

- * 원인 *

  스토리지 시스템의 버퍼가 부족했습니다.

- * 시정 조치 *

  일부 스토리지 시스템 작업이 완료될 때까지 기다린 다음 작업을 재시도하십시오.

스냅샷을 찾지 못했습니다

- * 메시지 *

  스냅샷을 찾지 못했습니다

- * 원인 *

  백업에 지정된 스냅샷을 사용할 수 없습니다.

- * 시정 조치 *

  지정된 스냅샷을 사용할 수 있는지 확인합니다. 그렇지 않은 경우 올바른 스냅샷을 사용하여 재시도하십시오.

스냅샷을 생성하지 못했습니다

- * 메시지 *

  스냅샷을 만들지 못했습니다

- * 원인 *

  볼륨에 이미 최대 스냅샷 수가 포함되어 있습니다.

- * 시정 조치 *

  일부 스냅샷을 삭제한 다음 백업 작업을 다시 시도하십시오.

스냅샷을 잠그지 못했습니다

- * 메시지 *

  스냅샷을 잠그는 데 실패했습니다

- * 원인 *

  스냅샷이 사용 중이거나 삭제되었습니다.

- * 시정 조치 *

  다른 작업에서 스냅샷을 사용 중인 경우 해당 작업이 완료될 때까지 기다린 다음 백업을 다시 시도하십시오. 스냅샷이 삭제된 경우 백업을 수행할 수 없습니다.

스냅샷을 삭제하지 못했습니다

- * 메시지 *

  스냅샷을 삭제하지 못했습니다

- * 원인 *

  자동 스냅샷이 다른 작업에서 사용 중이므로 삭제할 수 없습니다.

- * 시정 조치 *

  명령을 사용하여 `snap` 스냅샷의 상태를 확인합니다. 스냅샷이 필요하지 않은 경우 수동으로 삭제합니다.

최신 스냅샷을 가져오지 못했습니다

- * 메시지 *

  최근 스냅샷을 가져오지 못했습니다

- * 원인 *

  SnapMirror에서 볼륨을 초기화하는 중이므로 최신 스냅샷이 없을 수 있습니다.

- * 시정 조치 *

  초기화가 완료된 후 다시 시도하십시오.

새 테이프를 로드하지 못했습니다

- * 메시지 *

  새 테이프를 로드하지 못했습니다

- * 원인 *

  테이프 드라이브 또는 미디어에 오류가 있습니다.

- * 시정 조치 *

  테이프를 교체하고 작업을 다시 시도하십시오.

테이프를 초기화하지 못했습니다

- * 메시지 *

  테이프 초기화 실패

- * 원인 *

  다음 이유 중 하나로 인해 이 오류 메시지가 나타날 수 있습니다.

  ◦ 백업 이미지가 SMTape가 아닙니다.
  ◦ 지정된 테이프 차단 계수가 올바르지 않습니다.
  ◦ 테이프가 손상되었거나 손상되었습니다.
  ◦ 복원을 위해 잘못된 테이프가 로드되었습니다.

- * 시정 조치 *
  ◦ 백업 이미지가 SMTape가 아닌 경우 SMTape 백업이 있는 테이프를 사용하여 작업을 재시도하십시오.
  ◦ 차단 계수가 올바르지 않은 경우 올바른 차단 계수를 지정하고 작업을 재시도하십시오.
  ◦ 테이프가 손상된 경우 복원 작업을 수행할 수 없습니다.
  ◦ 잘못된 테이프가 로드된 경우 올바른 테이프를 사용하여 작업을 재시도하십시오.

복원 스트림을 초기화하지 못했습니다

- * 메시지 *

  복원 스트림을 초기화하지 못했습니다

- * 원인 *

  다음 이유 중 하나로 인해 이 오류 메시지가 나타날 수 있습니다.

- 백업 이미지가 SMTape가 아닙니다.
- 지정된 테이프 차단 계수가 올바르지 않습니다.
- 테이프가 손상되었거나 손상되었습니다.
- 복원을 위해 잘못된 테이프가 로드되었습니다.

- * 시정 조치 *
  - 백업 이미지가 SMTape가 아닌 경우 SMTape 백업이 있는 테이프를 사용하여 작업을 재시도하십시오.
  - 차단 계수가 올바르지 않은 경우 올바른 차단 계수를 지정하고 작업을 재시도하십시오.
  - 테이프가 손상된 경우 복원 작업을 수행할 수 없습니다.
  - 잘못된 테이프가 로드된 경우 올바른 테이프를 사용하여 작업을 재시도하십시오.

백업 이미지를 읽지 못했습니다

- * 메시지 *

  백업 이미지를 읽지 못했습니다

- * 원인 *

  테이프가 손상되었습니다.

- * 시정 조치 *

  테이프가 손상된 경우 복원 작업을 수행할 수 없습니다.

이미지 헤더가 없거나 손상되었습니다

- * 메시지 *

  '이미지 헤더 누락 또는 손상'

- * 원인 *

  테이프에 유효한 SMTape 백업이 없습니다.

- * 시정 조치 *

  유효한 백업이 포함된 테이프로 다시 시도하십시오.

내부 어설션

- * 메시지 *

  내부 어설션

- * 원인 *

  내부 SMTape 오류가 있습니다.

- * 시정 조치 *

  오류를 보고하고 기술 지원 부서에 'etc/log/backup' 파일을 보냅니다.

백업 이미지 매직 번호가 잘못되었습니다

- * 메시지 *

  백업 이미지 마술 번호가 잘못되었습니다

- * 원인 *

  백업 이미지가 SMTape가 아닙니다.

- * 시정 조치 *

  백업 이미지가 SMTape가 아닌 경우 SMTape 백업이 있는 테이프를 사용하여 작업을 재시도하십시오.

백업 이미지 체크섬이 잘못되었습니다

- * 메시지 *

  백업 이미지 체크섬이 잘못되었습니다

- * 원인 *

  테이프가 손상되었습니다.

- * 시정 조치 *

  테이프가 손상된 경우 복원 작업을 수행할 수 없습니다.

입력 테이프가 잘못되었습니다

- * 메시지 *

  잘못된 입력 테이프

- * 원인 *

  백업 이미지의 서명이 테이프 헤더에서 유효하지 않습니다. 테이프에 손상된 데이터가 있거나 유효한 백업 이미지가 없습니다.

- * 시정 조치 *

  유효한 백업 이미지로 복원 작업을 다시 시도하십시오.

볼륨 경로가 잘못되었습니다

- * 메시지 *

잘못된 볼륨 경로입니다

- * 원인 *

  백업 또는 복원 작업에 대해 지정된 볼륨을 찾을 수 없습니다.

- * 시정 조치 *

  유효한 볼륨 경로 및 볼륨 이름을 사용하여 작업을 재시도하십시오.

백업 세트 **ID**가 일치하지 않습니다

- * 메시지 *

  백업 세트 ID의 mismatch

- * 원인 *

  테이프 변경 중에 로드된 테이프는 백업 세트의 일부가 아닙니다.

- * 시정 조치 *

  올바른 테이프를 로드하고 작업을 재시도하십시오.

백업 타임 스탬프가 일치하지 않습니다

- * 메시지 *

  백업 타임 스탬프에 일치

- * 원인 *

  테이프 변경 중에 로드된 테이프는 백업 세트의 일부가 아닙니다.

- * 시정 조치 *

  'msape restore -h' 명령어를 사용하여 테이프의 헤더 정보를 확인한다.

종료로 인해 작업이 중단되었습니다

- * 메시지 *

  종료로 인해 작업이 중단되었습니다

- * 원인 *

  스토리지 시스템을 재부팅하는 중입니다.

- * 시정 조치 *

  스토리지 시스템이 재부팅된 후 작업을 재시도하십시오.

스냅샷 자동 삭제로 인해 작업이 중단되었습니다

- * 메시지 *

  `Job aborted due to snapshot autodelete`

- * 원인 *

  볼륨에 공간이 부족하여 스냅샷 자동 삭제를 트리거했습니다.

- * 시정 조치 *

  볼륨에서 공간을 확보하고 작업을 다시 시도하십시오.

현재 다른 작업에서 테이프를 사용하고 있습니다

- * 메시지 *

  테이프는 현재 다른 작업에서 사용 중입니다

- * 원인 *

  테이프 드라이브가 다른 작업에서 사용 중입니다.

- * 시정 조치 *

  현재 활성 작업이 완료된 후 백업을 다시 시도하십시오.

테이프 순서가 없습니다

- * 메시지 *

  테이프가 순서를 벗어났어

- * 원인 *

  복원 작업에 대한 테이프 시퀀스의 첫 번째 테이프에는 이미지 헤더가 없습니다.

- * 시정 조치 *

  이미지 헤더로 테이프를 로드하고 작업을 재시도하십시오.

전송 실패**(MetroCluster** 작업으로 인해 중단됨**)**

- * 메시지 *

  "전송 실패(MetroCluster 작업으로 인해 중단됨)

- * 원인 *

  전환 또는 스위치백 작업으로 인해 SMTape 작업이 중단됩니다.

- * 시정 조치 *

  스위치오버 또는 스위치백 작업이 완료된 후 SMTape 작업을 수행합니다.

전송 실패**(ARL** 시작 중단**)**

- * 메시지 *

  "전송 실패(ARL 시작 중단)"

- * 원인 *

  SMTape 작업이 진행 중인 동안 집계 재배치를 시작하면 SMTape 작업이 중단됩니다.

- * 시정 조치 *

  집계 재배치 작업이 완료된 후 SMTape 작업을 수행합니다.

전송 실패**(CFO**가 중단을 초기화함**)**

- * 메시지 *

  "전송 실패(CFO가 중단을 시작함)"

- * 원인 *

  SMTape 작업은 CFO 애그리게이트의 스토리지 페일오버(테이크오버 및 반환) 작업 때문에 중단됩니다.

- * 시정 조치 *

  CFO 애그리게이트의 스토리지 페일오버가 완료된 후 SMTape 작업을 수행합니다.

전송 실패**(SFO** 시작 중단**)**

- * 메시지 *

  전송 실패(SFO 시작 중단)

- * 원인 *

  SMTape 작업은 스토리지 페일오버(테이크오버 및 반환) 작업으로 인해 중단됩니다.

- * 시정 조치 *

  스토리지 페일오버(테이크오버 및 반환) 작업이 완료된 후 SMTape 작업을 수행합니다.

마이그레이션 중인 기본 애그리게이트

- * 메시지 *

  이주 중인 기본 골재

- * 원인 *

  마이그레이션 중인 Aggregate(스토리지 페일오버 또는 애그리게이트 재배치)에서 SMTape 작업이 시작되면 SMTape 작업이 실패합니다.

- * 시정 조치 *

  애그리게이트 마이그레이션이 완료된 후 SMTape 작업을 수행합니다.

볼륨이 현재 마이그레이션 중입니다

- * 메시지 *

  볼륨이 현재 마이그레이션 중입니다

- * 원인 *

  볼륨 마이그레이션 및 SMTape 백업을 동시에 실행할 수 없습니다.

- * 시정 조치 *

  볼륨 마이그레이션이 완료된 후 백업 작업을 다시 시도하십시오.

볼륨이 오프라인 상태입니다

- * 메시지 *

  볼륨 오프라인

- * 원인 *

  백업 중인 볼륨이 오프라인 상태입니다.

- * 시정 조치 *

  볼륨을 온라인으로 전환하고 백업을 다시 시도하십시오.

볼륨이 제한되지 않았습니다

- * 메시지 *

  볼륨이 제한되지 않음

- * 원인 *

  데이터가 복원되는 대상 볼륨은 제한되지 않습니다.

- * 시정 조치 *

  볼륨을 제한하고 복원 작업을 다시 시도하십시오.

NDMP 구성

ONTAP NDMP 구성에 대해 자세히 알아보십시오

타사 백업 애플리케이션을 사용하여 데이터를 테이프에 직접 백업하기 위해 NDMP(네트워크 데이터 관리 프로토콜)를 사용하도록 ONTAP 9 클러스터를 빠르게 구성할 수 있습니다.

백업 애플리케이션이 CAB(Cluster Aware Backup)를 지원하는 경우 NDMP를 _SVM-scope_or_node-scope_로 구성할 수 있습니다.

- 클러스터(admin SVM) 레벨에서 SVM 범위가 지정되므로 클러스터의 서로 다른 노드에 호스팅된 모든 볼륨을 백업할 수 있습니다. 가능한 경우 SVM 범위의 NDMP를 사용하는 것이 좋습니다.
- 노드 범위 NDMP에서는 해당 노드에서 호스팅되는 모든 볼륨을 백업할 수 있습니다.

백업 애플리케이션이 CAB를 지원하지 않는 경우 노드 범위 NDMP를 사용해야 합니다.

SVM 범위 및 노드 범위 NDMP는 상호 배타적이므로 동일한 클러스터에서 구성할 수 없습니다.

노드 범위 NDMP는 ONTAP 9에서 더 이상 사용되지 않습니다.

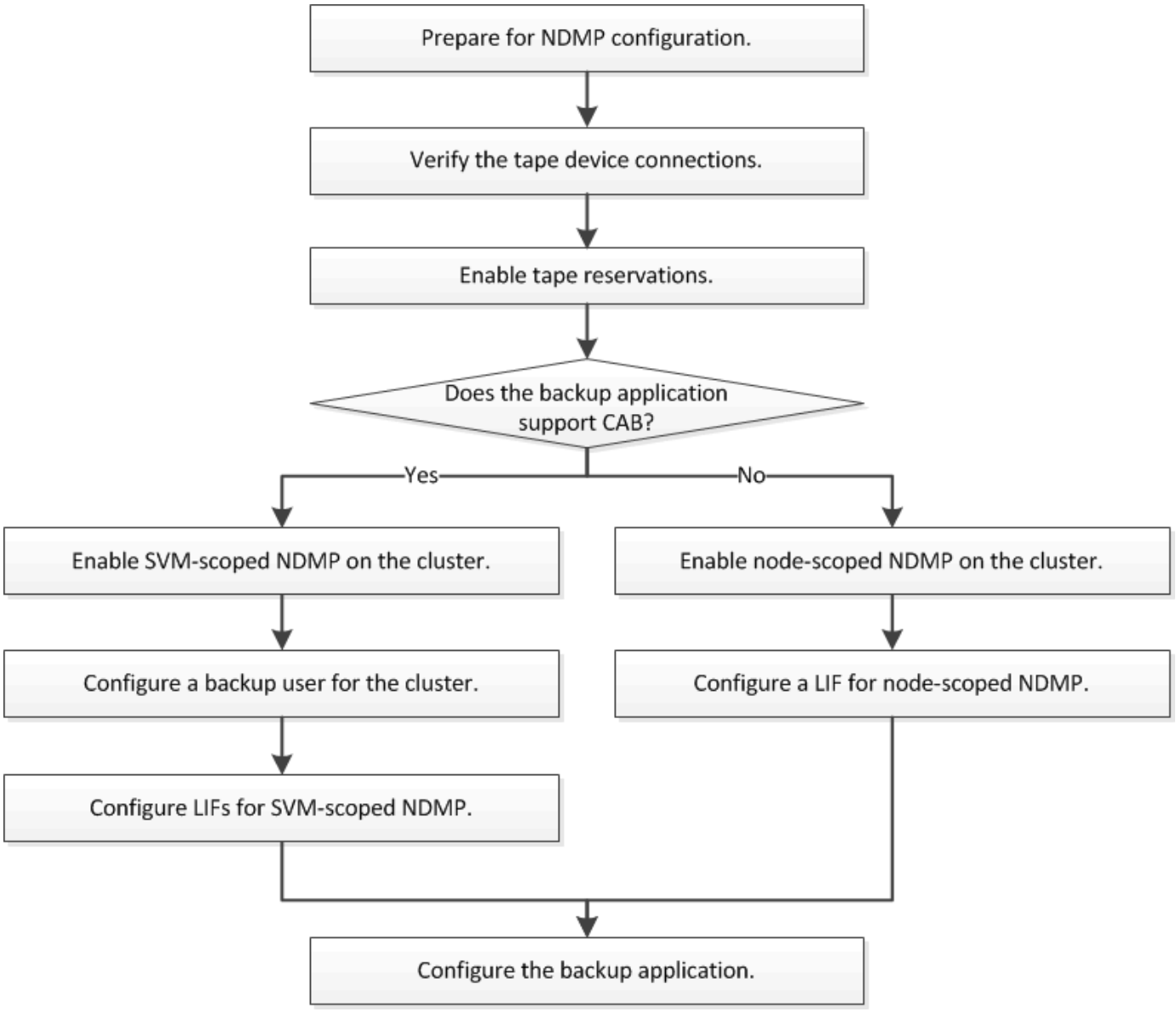
에 대해 자세히 "운전실(Cluster Aware Backup)"알아보십시오.

NDMP를 구성하기 전에 다음을 확인하십시오.

- 타사 백업 애플리케이션(DMA라고도 함)이 있습니다.
- 클러스터 관리자입니다.
- 테이프 장치 및 옵션 미디어 서버가 설치됩니다.
- 테이프 장치는 FC(파이버 채널) 스위치를 통해 또는 로컬로 연결된 상태로 클러스터에 연결됩니다.
- 하나 이상의 테이프 디바이스에 LUN(Logical Unit Number)이 0인 경우

ONTAP NDMP 구성 워크플로에 대해 알아보세요

NDMP를 통해 테이프 백업을 설정하려면 NDMP 구성 준비, 테이프 디바이스 연결 확인, 테이프 예약 활성화, SVM 또는 노드 레벨에서 NDMP 구성, 클러스터에서 NDMP 설정, 백업 사용자 구성, LIF 구성 및 백업 애플리케이션 구성이 필요합니다.



ONTAP NDMP 구성 준비

NDMP(Network Data Management Protocol)를 통해 테이프 백업 액세스를 구성하기 전에 계획된 구성이 지원되는지 확인하고, 테이프 드라이브가 각 노드의 적격 드라이브로 나열되는지 확인하고, 모든 노드에 인터클러스터 LIF가 있는지 확인해야 합니다. 백업 애플리케이션이 CAB(Cluster Aware Backup) 확장을 지원하는지 여부를 확인합니다.

단계

1. ONTAP 지원에 대한 자세한 내용은 백업 애플리케이션 공급자의 호환성 매트릭스를 참조하십시오(NetApp은 ONTAP 또는 NDMP를 통한 타사 백업 애플리케이션을 지원하지 않음).

   다음 NetApp 구성 요소가 호환되는지 확인해야 합니다.

   - 클러스터에서 실행 중인 ONTAP 9 버전입니다.
   - 백업 애플리케이션 공급업체 및 버전: 예: Veritas NetBackup 8.2 또는 CommVault.
   - 테이프 드라이브의 제조업체, 모델 및 인터페이스(예: IBM Ultrium 8 또는 HPE StoreEver Ultrium 30750

LTO-8)와 같은 테이프 장치 세부 정보

- 클러스터에 있는 노드 플랫폼: FAS8700 또는 A400.

> 에서 백업 애플리케이션에 대한 기존 ONTAP 호환성 지원 매트릭스를 확인할 수 있습니다 "NetApp 상호 운용성 매트릭스 툴".

2. 테이프 드라이브가 각 노드의 내장 테이프 구성 파일에 검증된 드라이브로 나열되어 있는지 확인합니다.

   a. CLI에서 Storage tape show-supported-status 명령을 사용하여 내장 테이프 구성 파일을 봅니다.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1
                                 Is
Tape Drives                      Supported  Support Status
-------------------------------  ---------
--------------------------------
Certance Ultrium 2               true       Dynamically Qualified
Certance Ultrium 3               true       Dynamically Qualified
Digital DLT2000                  true       Qualified
```

   b. 테이프 드라이브를 출력의 적격 드라이브 목록과 비교합니다.

> 출력에 표시되는 테이프 디바이스의 이름은 디바이스 레이블 또는 상호 운용성 매트릭스의 이름과 약간 다를 수 있습니다. 예를 들어 디지털 DLT2000은 DLT2K라고도 합니다. 이러한 사소한 이름 차이는 무시할 수 있습니다.

   c. 장치가 상호 운용성 매트릭스에 따라 적격 장치임에도 불구하고 출력에 적격 장치로 표시되지 않는 경우, NetApp Support 사이트의 지침에 따라 장치에 대한 업데이트된 구성 파일을 다운로드하여 설치하십시오.

   "NetApp 다운로드: 테이프 장치 구성 파일"

노드를 제공한 후 테이프 장치가 검증된 경우, 내장 테이프 구성 파일에 검증된 장치가 나열되지 않을 수 있습니다.

3. 클러스터의 모든 노드에 인터클러스터 LIF가 있는지 확인합니다.

   a. 'network interface show-role 인터클러스터' 명령을 사용하여 노드의 인터클러스터 LIF를 봅니다.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
```

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

b. 인터클러스터 LIF가 노드에 없으면 '네트워크 인터페이스 만들기' 명령을 사용하여 인터클러스터 LIF를 만듭니다.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster

cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

"네트워크 관리"

4. 백업 애플리케이션과 함께 제공된 설명서를 사용하여 백업 애플리케이션이 CAB(Cluster Aware Backup)를 지원하는지 여부를 확인합니다.

   CAB 지원은 수행할 수 있는 백업 유형을 결정하는 핵심 요소입니다.

관련 정보

- "저장 테이프 쇼"
- "저장 테이프 show-supported-status"

ONTAP NDMP 테이프 장치 연결 확인

모든 드라이브와 미디어 체인저가 ONTAP에 디바이스로 표시되는지 확인해야 합니다.

단계

1. 'storage tape show' 명령을 사용하여 모든 드라이브와 미디어 체인저에 대한 정보를 봅니다.

```
cluster1::> storage tape show

Node: cluster1-01
Device ID                 Device Type     Description
Status
------------------------  --------------  ------------------------------
--------
sw4:10.11                 tape drive      HP LTO-3
normal
0b.125L1                  media changer   HP MSL G3 Series
normal
0d.4                      tape drive      IBM LTO 5 ULT3580
normal
0d.4L1                    media changer   IBM 3573-TL
normal
...
```

2. 테이프 드라이브가 표시되지 않으면 문제를 해결합니다.
3. 미디어 체인저가 표시되지 않는 경우 'storage tape show -media-changer' 명령을 사용하여 미디어 체인저에 대한 정보를 확인한 후 문제를 해결하십시오.

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                      Initiator  Alias    Device State
Status
------------------------  ---------  -------  ------------------------
--------
cluster1-01               2b         mc0      in-use
normal
...
```

관련 정보

- "저장 테이프 쇼 미디어 체인저"

ONTAP NDMP 백업 작업에 대한 테이프 예약 활성화

NDMP 백업 작업을 위해 테이프 드라이브가 백업 애플리케이션에서 사용하도록 예약되어 있는지 확인해야 합니다.

이 작업에 대해

예약 설정은 백업 애플리케이션에 따라 다르며, 이러한 설정은 동일한 드라이브를 사용하는 백업 애플리케이션과 노드 또는 서버와 일치해야 합니다. 올바른 예약 설정은 백업 애플리케이션의 공급업체 설명서를 참조하십시오.

단계

1. options -option -name tape.예약 -option -value persistent 명령을 사용하여 예약을 활성화합니다.

   다음 명령을 실행하면 '영구적' 값을 가진 예약이 활성화됩니다.

```
cluster1::> options -option-name tape.reservations -option-value
persistent
2 entries were modified.
```

2. options tape.enervations 명령을 사용하여 모든 노드에서 예약이 활성화되었는지 확인한 다음 출력을 검토합니다.

```
cluster1::> options tape.reservations

cluster1-1
    tape.reservations                 persistent

cluster1-2
    tape.reservations                 persistent
2 entries were displayed.
```

SVM 범위 NDMP를 구성합니다

ONTAP 클러스터에서 SVM 범위 NDMP 활성화

DMA가 CAB(Cluster Aware Backup) 확장을 지원하는 경우 SVM 범위의 NDMP를 사용하도록 설정하고, 클러스터에서 NDMP 서비스를 설정하고(admin SVM), 데이터 및 제어 연결을 위해 LIF를 구성하여 클러스터의 여러 노드에서 호스팅되는 모든 볼륨을 백업할 수 있습니다.

시작하기 전에

CAB 확장은 DMA에서 지원해야 합니다.

이 작업에 대해

노드 범위의 NDMP 모드를 해제하면 클러스터에서 SVM 범위의 NDMP 모드가 설정됩니다.

단계

1. SVM 범위 NDMP 모드 활성화:

   ```
   cluster1::> system services ndmp node-scope-mode off
   ```

   SVM 범위 NDMP 모드가 설정되었습니다.

2. 관리자 SVM에서 NDMP 서비스 활성화:

   ```
   cluster1::> vserver services ndmp on -vserver cluster1
   ```

   기본적으로 인증 유형은 "challenge"로 설정되고 일반 텍스트 인증은 비활성화됩니다.

   보안 통신을 위해 일반 텍스트 인증을 사용하지 않도록 설정해야 합니다.

3. NDMP 서비스가 설정되었는지 확인합니다.

   ```
   cluster1::> vserver services ndmp show
   ```

```
Vserver        Enabled   Authentication type
-------------- --------- -------------------
cluster1       true      challenge
vs1            false     challenge
```

ONTAP NDMP 인증을 위한 백업 사용자 활성화

백업 애플리케이션에서 SVM 범위의 NDMP를 인증하려면 충분한 권한과 NDMP 암호를 가진 관리 사용자가 있어야 합니다.

이 작업에 대해

백업 관리자 사용자를 위해 NDMP 암호를 생성해야 합니다. 클러스터 또는 SVM 레벨에서 백업 관리자를 지원하고, 필요한 경우 새 사용자를 생성할 수 있습니다. 기본적으로 다음 역할을 가진 사용자는 NDMP 백업에 대해 인증할 수 있습니다.

- 클러스터 전체: `admin` 또는 `backup`
- 개별 SVM: `vsadmin` 또는 `vsadmin-backup`

NIS 또는 LDAP 사용자를 사용하는 경우 사용자는 해당 서버에 있어야 합니다. Active Directory 사용자는 사용할 수 없습니다.

단계

1. 현재 관리자 사용자 및 권한을 표시합니다.

   '보안 로그인 쇼'

   에 대한 자세한 내용은 `security login show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 필요한 경우 를 사용하여 새 NDMP 백업 사용자를 생성합니다 `security login create` 클러스터 전체 또는 개별 SVM 권한에 따라 명령을 수행하고 적절한 역할을 수행합니다.

   '-user-or-group-name' 매개 변수에 로컬 백업 사용자 이름 또는 NIS 또는 LDAP 사용자 이름을 지정할 수 있습니다.

   다음 명령을 실행하면 백업 사용자가 생성됩니다 `backup_admin1` 를 사용하여 `backup` 전체 클러스터의 역할:

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   다음 명령을 실행하면 백업 사용자가 생성됩니다 `vsbackup_admin1` 를 사용하여 `vsadmin-backup` 개별 SVM의 역할:

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

   새 사용자의 암호를 입력하고 확인합니다.

   에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 'vserver services ndmp generate password' 명령을 사용하여 admin SVM에 대한 암호를 생성합니다.

   생성된 암호를 사용하여 백업 애플리케이션에서 NDMP 접속을 인증해야 합니다.

```
cluster1::> vserver services ndmp generate-password -vserver cluster1
-user backup_admin1

 Vserver: cluster1
    User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

SVM 범위 **NDMP**에 대한 **ONTAP LIF** 구성

데이터와 테이프 리소스 간에 데이터 연결을 설정하고, 관리 SVM과 백업 애플리케이션 간의 연결을 제어하는 데 사용할 LIF를 식별해야 합니다. LIF를 식별한 후 서비스 및 페일오버 정책이 설정되었는지 확인해야 합니다.

ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 "지원되는 트래픽을 관리합니다"참조하십시오.

ONTAP 9.10.1 이상

단계

1. 매개 변수와 함께 명령을 `-service-policy` 사용하여 노드에 호스팅된 인터클러스터 LIF를 `network interface show` 식별합니다.

   네트워크 인터페이스 show-service-policy default-인터클러스터

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 매개 변수와 함께 명령을 `-service-policy` 사용하여 노드에 호스팅된 관리 LIF를 `network interface show` 식별합니다.

   ```
   network interface show -service-policy default-management
   ```

3. 인터클러스터 LIF에 서비스가 포함되는지 확인합니다. `backup-ndmp-control`

   네트워크 인터페이스 서비스 정책 쇼

   에 대한 자세한 내용은 `network interface service-policy show` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 모든 LIF에 대해 페일오버 정책이 적절하게 설정되었는지 확인합니다.

   a. 클러스터 관리 LIF의 페일오버 정책이 브로드캐스트 도메인 전체에 설정되어 있고, 인터클러스터 및 노드 관리 LIF에 대한 정책이 '네트워크 인터페이스 show-failover' 명령을 사용하여 '로컬 전용'으로 설정되어 있는지 확인합니다.

      다음 명령을 실행하면 클러스터 관리, 인터클러스터 및 노드 관리 LIF에 대한 페일오버 정책이 표시됩니다.

```
cluster1::> network interface show -failover

           Logical          Home             Failover    Failover
Vserver    Interface        Node:Port        Policy      Group
-------    --------------   --------------   ----------  --------
cluster    cluster1_clus1   cluster1-1:e0a   local-only  cluster
                                                         Failover
Targets:
                                                         .......
cluster1   cluster_mgmt     cluster1-1:e0m   broadcast-  Default
                                                domain-wide
                                                         Failover
Targets:
                                                         .......
           IC1              cluster1-1:e0a   local-only  Default
                                                         Failover
Targets:
           IC2              cluster1-1:e0b   local-only  Default
                                                         Failover
Targets:
                                                         .......
cluster1-1 c1-1_mgmt1       cluster1-1:e0m   local-only  Default
                                                         Failover
Targets:
                                                         ......
cluster1-2 c1-2_mgmt1       cluster1-2:e0m   local-only  Default
                                                         Failover
Targets:
                                                         ......
```

a. 페일오버 정책이 제대로 설정되지 않은 경우 -failover-policy 매개 변수와 함께 network interface modify 명령을 사용하여 페일오버 정책을 수정합니다.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 데이터 연결에 필요한 LIF를 'preferred-interface-role' 매개 변수와 함께 'vserver services ndmp modify' 명령을 사용하여 지정합니다.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

6. 'vserver services ndmp show' 명령을 사용하여 클러스터에 대해 기본 인터페이스 역할이 설정되어 있는지 확인합니다.

```
cluster1::> vserver services ndmp show -vserver cluster1

                Vserver: cluster1
                NDMP Version: 4
                .......
                .......
Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

ONTAP 9.9 이하

단계

1. '-role' 매개 변수가 있는 'network interface show' 명령을 사용하여 인터클러스터, 클러스터 관리 및 노드 관리 LIF를 식별합니다.

   다음 명령을 실행하면 인터클러스터 LIF가 표시됩니다.

```
cluster1::> network interface show -role intercluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ----------   ---------- ------------------ -------------
------- ----
cluster1    IC1          up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2          up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   다음 명령을 실행하면 클러스터 관리 LIF가 표시됩니다.

```
cluster1::> network interface show -role cluster-mgmt

            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ----------    ---------- ------------------ -----------
------- ----
cluster1    cluster_mgmt  up/up      192.0.2.60/24      cluster1-2
e0M     true
```

다음 명령을 실행하면 노드 관리 LIF가 표시됩니다.

```
cluster1::> network interface show -role node-mgmt

            Logical           Status     Network          Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask     Node
Port    Home
----------- ----------        ---------- ---------------
------------  ------  ------
cluster1    cluster1-1_mgmt1  up/up      192.0.2.69/24    cluster1-1
e0M     true
            cluster1-2_mgmt1  up/up      192.0.2.70/24    cluster1-2
e0M     true
```

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 방화벽 정책이 인터클러스터, 클러스터 관리(`cluster-mgmt`) 및 노드 관리에 NDMP에 대해 사용하도록 설정되어 있는지 확인(`node-mgmt`) LIF:

   a. 'system services firewall policy show' 명령을 사용하여 NDMP에 대해 방화벽 정책이 설정되어 있는지 확인합니다.

      다음 명령을 실행하면 클러스터 관리 LIF의 방화벽 정책이 표시됩니다.

```
cluster1::> system services firewall policy show -policy cluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -----------------
cluster     cluster      dns        0.0.0.0/0
                         http       0.0.0.0/0
                         https      0.0.0.0/0
                         ndmp       0.0.0.0/0
                         ndmps      0.0.0.0/0
                         ntp        0.0.0.0/0
                         rsh        0.0.0.0/0
                         snmp       0.0.0.0/0
                         ssh        0.0.0.0/0
                         telnet     0.0.0.0/0
10 entries were displayed.
```

      다음 명령을 실행하면 인터클러스터 LIF의 방화벽 정책이 표시됩니다.

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

다음 명령을 실행하면 노드 관리 LIF의 방화벽 정책이 표시됩니다.

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. 방화벽 정책이 활성화되지 않은 경우 '-service' 매개 변수를 사용하여 'system services firewall policy modify' 명령을 사용하여 방화벽 정책을 활성화합니다.

다음 명령을 실행하면 인터클러스터 LIF에 대한 방화벽 정책을 사용할 수 있습니다.

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. 모든 LIF에 대해 페일오버 정책이 적절하게 설정되었는지 확인합니다.

a. 클러스터 관리 LIF의 페일오버 정책이 브로드캐스트 도메인 전체에 설정되어 있고, 인터클러스터 및 노드 관리 LIF에 대한 정책이 '네트워크 인터페이스 show-failover' 명령을 사용하여 '로컬 전용'으로 설정되어 있는지 확인합니다.

   다음 명령을 실행하면 클러스터 관리, 인터클러스터 및 노드 관리 LIF에 대한 페일오버 정책이 표시됩니다.

```
cluster1::> network interface show -failover

           Logical            Home               Failover
Failover
Vserver    Interface          Node:Port          Policy
Group
---------- -----------------  ------------------ --------------------
--------
cluster    cluster1_clus1     cluster1-1:e0a     local-only
cluster
                                                     Failover
Targets:
                                                     .......

cluster1   cluster_mgmt       cluster1-1:e0m     broadcast-domain-
wide Default
                                                     Failover
Targets:
                                                     .......
           IC1                 cluster1-1:e0a     local-only
Default
                                                     Failover
Targets:
           IC2                 cluster1-1:e0b     local-only
Default
                                                     Failover
Targets:
                                                     .......
cluster1-1 cluster1-1_mgmt1   cluster1-1:e0m     local-only
Default
                                                     Failover
Targets:
                                                     ......
cluster1-2 cluster1-2_mgmt1   cluster1-2:e0m     local-only
Default
                                                     Failover
Targets:
                                                     ......
```

a. 페일오버 정책이 제대로 설정되지 않은 경우 -failover-policy 매개 변수와 함께 network interface modify

명령을 사용하여 페일오버 정책을 수정합니다.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 데이터 연결에 필요한 LIF를 'preferred-interface-role' 매개 변수와 함께 'vserver services ndmp modify' 명령을 사용하여 지정합니다.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. 'vserver services ndmp show' 명령을 사용하여 클러스터에 대해 기본 인터페이스 역할이 설정되어 있는지 확인합니다.

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
            Preferred Interface Role: intercluster, cluster-mgmt,
node-mgmt
```

노드 범위 **NDMP**를 구성합니다

ONTAP 클러스터에서 노드 범위 **NDMP** 활성화

노드 범위 NDMP를 설정하고, NDMP 서비스를 사용하도록 설정하고, 데이터 및 제어 연결을 위해 LIF를 구성하여 단일 노드에서 호스팅되는 볼륨을 백업할 수 있습니다. 이 작업은 클러스터의 모든 노드에 대해 수행할 수 있습니다.

노드 범위 NDMP는 ONTAP 9에서 더 이상 사용되지 않습니다.

이 작업에 대해

노드 범위 모드에서 NDMP를 사용하는 경우 노드 단위로 인증을 구성해야 합니다. 자세한 내용은 을 참조하십시오 "기술 자료 문서 "'노드 범위' 모드에서 NDMP 인증을 구성하는 방법"".

단계

1. 노드 범위 NDMP 모드 설정:

```
cluster1::> system services ndmp node-scope-mode on
```

NDMP 노드 범위 모드가 설정되었습니다.

2. 클러스터의 모든 노드에서 NDMP 서비스 설정:

와일드카드 "" * ""를 사용하면 모든 노드에서 동시에 NDMP 서비스를 사용할 수 있습니다.

백업 애플리케이션에서 NDMP 접속을 인증할 암호를 지정해야 합니다.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. 를 비활성화합니다 `-clear-text` NDMP 암호의 보안 통신을 위한 옵션:

와일드카드 "" * "를 사용하면 모든 노드에서 "-clear-text" 옵션을 동시에 사용할 수 없습니다.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. NDMP 서비스가 설정되어 있고 이 설정되어 있는지 확인합니다 `-clear-text` 옵션이 비활성화됨:

```
cluster1::> system services ndmp show
```

```
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false        root
cluster1-2            true      false        root
2 entries were displayed.
```

노드 범위 **NDMP**에 대한 **ONTAP LIF** 구성

노드와 백업 애플리케이션 간의 데이터 연결 및 제어 연결을 설정하는 데 사용할 LIF를 식별해야 합니다. LIF를 식별한 후 LIF에 대한 방화벽 및 페일오버 정책이 설정되어 있는지 확인해야 합니다.

ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 "지원되는 트래픽을 관리합니다"참조하십시오.

ONTAP 9.10.1 이상

단계

1. 매개 변수와 함께 명령을 `-service-policy` 사용하여 노드에 호스팅된 인터클러스터 LIF를 `network interface show` 식별합니다.

   네트워크 인터페이스 show-service-policy default-인터클러스터

2. 인터클러스터 LIF에 서비스가 포함되는지 확인합니다. `backup-ndmp-control`

   네트워크 인터페이스 서비스 정책 쇼

3. 인터클러스터 LIF에 대해 페일오버 정책이 적절하게 설정되었는지 확인합니다.

   a. 네트워크 인터페이스 show-failover 명령을 사용하여 인터클러스터 LIF의 페일오버 정책이 "로컬 전용 "으로 설정되었는지 확인합니다.

```
cluster1::> network interface show -failover
            Logical          Home               Failover
Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  -----------------  ------------
--------
cluster1    IC1               cluster1-1:e0a    local-only
Default
                                                    Failover
Targets:
                                                    .......
            IC2               cluster1-2:e0b    local-only
Default
                                                    Failover
Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
Default
                                                    Failover
Targets:
                                                    .......
```

   b. 페일오버 정책이 적절하게 설정되지 않은 경우 '-failover-policy' 매개 변수와 함께 'network interface modify' 명령을 사용하여 페일오버 정책을 수정합니다.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

에 대한 자세한 `network interface show` `network interface service-policy show`

내용은, 및 `network interface modify`"ONTAP 명령 참조입니다" 을 참조하십시오.

ONTAP 9.9 이하

단계

1. '-role' 매개 변수가 있는 'network interface show' 명령을 사용하여 노드에 호스팅된 인터클러스터 LIF를 식별합니다.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

2. 인터클러스터 LIF에서 NDMP에 대해 방화벽 정책이 활성화되어 있는지 확인합니다.

   a. 'system services firewall policy show' 명령을 사용하여 NDMP에 대해 방화벽 정책이 설정되어 있는지 확인합니다.

      다음 명령을 실행하면 인터클러스터 LIF의 방화벽 정책이 표시됩니다.

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

   b. 방화벽 정책이 활성화되지 않은 경우 '-service' 매개 변수를 사용하여 'system services firewall policy modify' 명령을 사용하여 방화벽 정책을 활성화합니다.

다음 명령을 실행하면 인터클러스터 LIF에 대한 방화벽 정책을 사용할 수 있습니다.

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. 인터클러스터 LIF에 대해 페일오버 정책이 적절하게 설정되었는지 확인합니다.

   a. 네트워크 인터페이스 show-failover 명령을 사용하여 인터클러스터 LIF의 페일오버 정책이 "로컬 전용 "으로 설정되었는지 확인합니다.

```
cluster1::> network interface show -failover
            Logical          Home               Failover
Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  -----------------  ------------
--------
cluster1    IC1               cluster1-1:e0a    local-only
Default
                                                    Failover
Targets:
                                                    .......
            IC2               cluster1-2:e0b    local-only
Default
                                                    Failover
Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
Default
                                                    Failover
Targets:
                                                    .......
```

   b. 페일오버 정책이 적절하게 설정되지 않은 경우 '-failover-policy' 매개 변수와 함께 'network interface modify' 명령을 사용하여 페일오버 정책을 수정합니다.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

및 `network interface modify` 에 대한 자세한 `network interface show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP NDMP 구성을 위한 백업 애플리케이션 구성

NDMP 액세스용으로 클러스터를 구성한 후에는 클러스터 구성에서 정보를 수집한 다음 백업 애플리케이션에서 나머지 백업 프로세스를 구성해야 합니다.

단계

1. ONTAP에서 이전에 구성한 다음 정보를 수집합니다.
   - 백업 애플리케이션이 NDMP 접속을 생성하는 데 필요한 사용자 이름 및 암호입니다
   - 백업 애플리케이션이 클러스터에 연결하는 데 필요한 인터클러스터 LIF의 IP 주소입니다
2. ONTAP에서 'storage tape alias show' 명령어를 사용해 각 디바이스에 할당된 ONTAP의 별칭을 출력한다.

   별칭은 백업 애플리케이션을 구성하는 데 유용합니다.

```
cluster1::> storage tape show -alias

  Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5

Node                          Alias     Mapping
----------------------------- --------- ------------------------------
stsw-3220-4a-4b-02            st2       SN[HU19497WVR]
...
```

3. 백업 애플리케이션에서 백업 애플리케이션의 설명서를 사용하여 나머지 백업 프로세스를 구성합니다.

작업을 마친 후

볼륨 이동 또는 LIF 마이그레이션과 같은 데이터 이동성 이벤트가 발생할 경우 중단된 백업 작업을 다시 초기화할 준비를 해야 합니다.

관련 정보

- "저장 테이프 별칭 표시"

NetApp Element 소프트웨어와 ONTAP 간 복제 개요

SnapMirror를 사용하여 Element 볼륨의 스냅샷을 ONTAP 대상에 복제하면 Element 시스템에서 비즈니스 연속성을 보장할 수 있습니다. Element 사이트에서 재해가 발생할 경우 ONTAP 시스템에서 클라이언트로 데이터를 제공하고 서비스가 복원되면 Element 시스템을 다시 활성화할 수 있습니다.

ONTAP 9.4부터는 ONTAP 노드에 생성된 LUN의 스냅샷을 Element 시스템에 다시 복제할 수 있습니다. Element 사이트에서 운영 중단 중에 LUN을 생성했거나, LUN을 사용하여 ONTAP에서 Element 소프트웨어로 데이터를 마이그레이션할 수 있습니다.

"NetApp Element 소프트웨어 및 ONTAP의 복제를 구성합니다"..

이벤트, 성능 및 상태 모니터링

System Manager로 클러스터 성능을 모니터링합니다

ONTAP 시스템 관리자를 사용하여 클러스터 성능 모니터링

이 섹션의 항목에서는 ONTAP 9.7 이상 릴리즈의 System Manager에서 클러스터 상태 및 성능을 관리하는 방법을 보여 줍니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 클러스터 성능을 모니터링합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

System Manager 대시보드에서 시스템에 대한 정보를 확인하여 클러스터 성능을 모니터링할 수 있습니다. 대시보드에는 중요한 알림, 스토리지 계층 및 볼륨의 효율성 및 용량, 클러스터에서 사용 가능한 노드, HA Pair의 노드 상태, 가장 활성화된 애플리케이션 및 개체에 대한 정보가 표시됩니다. 클러스터 또는 노드의 성능 메트릭과

대시보드를 통해 다음 정보를 확인할 수 있습니다.

- * 상태 *: 클러스터가 얼마나 양호합니까?
- * 용량 *: 클러스터에서 사용할 수 있는 용량은 무엇입니까?
- * 성능 *: 지연 시간, IOPS 및 처리량을 기준으로 클러스터의 성능은 어떻습니까?
- * 네트워크 *: 포트, 인터페이스 및 스토리지 VM과 같은 호스트 및 스토리지 객체로 네트워크를 구성하는 방법은 무엇입니까?

Health and Capacity 개요에서 을 클릭하여 추가 정보를 보고 작업을 수행할 수 있습니다 → .

성과 개요에서는 시간, 일, 주, 월 또는 연도를 기준으로 메트릭을 볼 수 있습니다.

네트워크 개요에서 네트워크의 각 개체 수가 표시됩니다(예: "8개의 NVMe/FC 포트"). 번호를 클릭하여 각 네트워크 개체에 대한 세부 정보를 볼 수 있습니다.

ONTAP System Manager 대시보드의 뷰 클러스터에 대해 알아보세요

System Manager 대시보드를 이용하면 단일 위치에서 ONTAP 클러스터를 빠르고 포괄적으로 확인할 수 있습니다.

System Manager 대시보드를 사용하면 중요한 경고와 알림, 스토리지 계층 및 볼륨의 효율성 및 용량, 클러스터에서 사용 가능한 노드, 고가용성(HA) 쌍의 노드 상태, 가장 활발한 애플리케이션 및 오브젝트의 상태에 대한 정보를 한눈에 볼 수 있습니다. 클러스터 또는 노드의 성능 메트릭을 파악할 수 있습니다.

대시보드에는 다음과 같이 설명된 4개의 패널이 포함되어 있습니다.

상태

상태 보기에는 클러스터에서 검색할 수 있는 모든 노드의 전반적인 상태에 대한 정보가 표시됩니다.

또한 상태 보기에는 구성되지 않은 노드 세부 정보와 같은 클러스터 레벨의 오류 및 경고가 표시되며, 클러스터 성능을 높이기 위해 수정할 수 있는 특성을 나타냅니다.

클러스터 이름, 버전, 클러스터 생성 날짜 및 시간 등과 같은 클러스터의 개요를 보려면 → 상태 보기를 클릭하여 확장합니다. 클러스터와 연결된 노드의 상태와 관련된 통계를 모니터링할 수도 있습니다. 환경에서 리소스를 그룹화하고 식별할 수 있는 태그를 관리할 수 있습니다. Insights 섹션은 시스템의 용량, 보안 규정 준수 및 구성을 최적화하는 데 도움이 됩니다.

용량

Capacity 보기에는 클러스터의 스토리지 공간이 표시됩니다. 사용된 총 논리적 공간, 사용된 총 물리적 공간 및 사용 가능한 디스크 공간을 볼 수 있습니다.

ActiveIQ에 등록하여 클러스터 데이터의 기간별 데이터를 볼 수 있습니다. →Capacity 뷰를 확장하면 클러스터와 관련된 계층의 개요를 볼 수 있습니다. 총 공간, 사용된 공간 및 사용 가능한 공간 등 각 계층에 대한 용량 정보를 볼 수 있습니다. 처리량, IOPS, 지연 시간에 대한 세부 정보가 표시됩니다. "이러한 용량 측정에 대한 자세한 내용은 System Manager를 참조하십시오"..

용량 보기를 사용하여 로컬 계층 또는 클라우드 계층을 추가할 수 있습니다. 자세한 내용은 을 "클러스터의 용량을 봅니다"참조하십시오.

네트워크

네트워크 보기에는 네트워크의 일부인 물리적 포트, 네트워크 인터페이스 및 스토리지 VM이 표시됩니다.

네트워크 보기에는 네트워크에 연결된 클라이언트 유형이 표시됩니다. 이러한 네트워크에 연결된 각 클라이언트는 숫자로 표시됩니다(예: "NVMe/FC 16"). 각 네트워크 요소에 대한 특정 세부 정보를 보려면 번호를 선택하십시오.

네트워크의 포트, 네트워크 인터페이스, 스토리지 VM 및 호스트를 포함하는 네트워크의 전체 페이지 보기를 보려면 → 클릭하십시오.

성능

성능 보기에는 ONTAP 클러스터의 상태와 효율성을 모니터링하는 데 도움이 되는 성능 통계가 표시됩니다. 통계에는 지연 시간, 처리량, IOPS 등 주요 클러스터 성능 표시기가 포함되어 있으며 그래프로 표시됩니다.

성능 보기에는 일, 시, 주 또는 연도별로 서로 다른 시간 간격의 성능 통계가 표시됩니다. 다양한 그래프를 사용하여 클러스터 성능을 빠르게 분석하고 최적화가 필요한 특성을 파악할 수 있습니다. 이 빠른 분석을 통해 워크로드를 추가 또는 이동하는 방법을 결정할 수 있습니다. 또한 최대 사용 시간을 살펴보고 잠재적 변경 사항을 계획할 수 있습니다.

성능 보기에는 지연 시간, 처리량 및 IOPS와 관련된 총 성능 메트릭이 표시됩니다.

9.15.1부터 성능 뷰가 향상되어 지연 시간, 처리량, IOPS와 관련된 읽기, 쓰기, 기타 및 총 성능 메트릭에 대한 그래프를 표시할 수 있습니다. 다른 메트릭에는 읽기 또는 쓰기가 아닌 작업이 포함됩니다.

성능 값은 3초마다 새로 고쳐지고 성능 그래프는 15초마다 새로 고쳐집니다. 클러스터 성능에 대한 정보를 사용할 수 없는 경우에는 그래프가 표시되지 않습니다.

시간, 일, 주, 월 및 연도별로 성능 메트릭을 전체 페이지 보기로 보려면 클릭합니다. 로컬 시스템에서 성능 메트릭 보고서를 다운로드할 수도 있습니다.

ONTAP 시스템 관리자에서 핫 볼륨 및 기타 객체 식별

자주 액세스하는 볼륨(핫 볼륨) 및 데이터(핫 오브젝트)를 식별하여 클러스터 성능을 가속화합니다.

ONTAP 9.10.1부터 파일 시스템 분석의 활동 추적 기능을 사용하여 볼륨의 핫 개체를 모니터링할 수 있습니다.

단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 자주 액세스하는 볼륨 및 데이터를 보려면 IOPS, 지연 시간 및 처리량 열을 필터링합니다.

ONTAP 시스템 관리자에서 QoS 수정

ONTAP 9.8부터 스토리지를 프로비저닝할 때 서비스 품질(QoS) 기본적으로 활성화되어 있습니다. 프로비저닝 프로세스 중에 QoS를 비활성화하거나 사용자 지정 QoS 정책을 선택할 수 있습니다. 스토리지에 프로비저닝된 후 QoS를 수정할 수도 있습니다.

단계

1. System Manager에서 * Storage * 와 * Volumes * 를 차례로 선택합니다.
2. QoS를 수정할 볼륨 옆에 있는 * 편집 * 을 선택합니다 ⋮ .

ONTAP 시스템 관리자에서 위험 모니터링

ONTAP 9.10.0부터, System Manager를 사용하여 Active IQ Digital Advisor(Digital Advisor)가 보고한 위험을 모니터링할 수 있습니다. ONTAP 9.10.1부터 System Manager를 사용하여 위험을 확인할 수도 있습니다.

NetApp Digital Advisor는 스토리지 환경의 위험을 줄이고 성능 및 효율성을 개선할 수 있는 기회를 보고합니다. System Manager를 사용하면 Digital Advisor가 보고한 위험에 대해 알아보고, 스토리지 관리를 지원하고, 가용성, 보안 및 스토리지 성능을 향상하는 데 도움이 되는 실행 가능한 인텔리전스를 받을 수 있습니다.

Digital Advisor 계정에 대한 링크

Digital Advisor의 위험에 대한 정보를 받으려면 먼저 System Manager에서 Digital Advisor 계정에 연결해야 합니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 클릭합니다.
2. Active IQ 등록 * 에서 * 등록 * 을 클릭합니다.
3. Digital Advisor 자격 증명을 입력하십시오.
4. 자격 증명이 인증되면 * 확인을 클릭하여 Active IQ를 System Manager*와 연결합니다.

위험 수를 확인합니다

ONTAP 9.10.0부터 System Manager의 대시보드에서 디지털 어드바이저가 보고한 위험 수를 확인할 수 있습니다.

시작하기 전에

System Manager와 Digital Advisor 계정의 연결을 설정해야 합니다. 을 Digital Advisor 계정에 대한 링크참조하십시오.

단계

1. System Manager에서 * 대시보드 * 를 클릭합니다.
2. 상태 * 섹션에서 보고된 위험 수를 확인합니다.

위험 수를 보여 주는 메시지를 클릭하여 각 위험에 대한 자세한 정보를 볼 수 있습니다. 을 참조하십시오 위험에 대한 세부 정보를 봅니다.

위험에 대한 세부 정보를 봅니다

ONTAP 9.10.0부터 Digital Advisor에서 보고한 위험이 영향 영역별로 분류된 것을 System Manager에서 확인할 수 있습니다. 또한 보고된 각 위험, 시스템에 미치는 잠재적 영향 및 취할 수 있는 수정 조치에 대한 자세한 정보를 볼 수 있습니다.

시작하기 전에

System Manager와 Digital Advisor 계정의 연결을 설정해야 합니다. 을 Digital Advisor 계정에 대한 링크참조하십시오.

단계

1. 이벤트 > 모든 이벤트 * 를 클릭합니다.
2. 개요 * 섹션의 * Active IQ 제안 * 아래에서 각 영향 영역 범주의 위험 수를 봅니다. 위험 범주는 다음과 같습니다.
   - 성능 및 효율성
   - 가용성 및 보호
   - 용량
   - 구성
   - 보안
3. Active IQ 제안 * 탭을 클릭하여 다음을 포함한 각 위험에 대한 정보를 확인하십시오.
   - 시스템에 미치는 영향 수준
   - 위험의 범주입니다
   - 영향을 받는 노드입니다
   - 필요한 완화 조치 유형
   - 수행할 수 있는 수정 조치

위험을 인정합니다

ONTAP 9.10.1부터 System Manager를 사용하여 열려 있는 위험을 확인할 수 있습니다.

단계

1. System Manager에서 의 절차를 수행하여 위험 목록을 표시합니다 위험에 대한 세부 정보를 봅니다.

2. 승인하려는 공개 위험의 위험 이름을 클릭합니다.
3. 다음 필드에 정보를 입력합니다.
    - 미리 알림(날짜)
    - 양쪽 맞춤
    - 설명
4. 확인 * 을 클릭합니다.

    위험을 인지한 후 Digital Advisor 제안 목록에 변경 사항이 반영되려면 몇 분 정도 걸립니다.

위험 확인 취소

ONTAP 9.10.1부터 System Manager를 사용하여 이전에 승인되었던 모든 위험을 확인할 수 있습니다.

단계

1. System Manager에서 의 절차를 수행하여 위험 목록을 표시합니다 위험에 대한 세부 정보를 봅니다.
2. 확인 취소할 확인된 위험의 위험 이름을 클릭합니다.
3. 다음 필드에 정보를 입력합니다.
    - 양쪽 맞춤
    - 설명
4. 승인 취소 * 를 클릭합니다.

    위험을 인지하지 못한 후 변경 사항이 Digital Advisor 제안 목록에 반영되려면 몇 분 정도 걸립니다.

ONTAP System Manager 통찰력으로 시스템을 최적화하세요

System Manager를 사용하면 시스템 최적화를 위한 통찰력을 얻을 수 있습니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 시스템을 최적화하는 데 도움이 되는 통찰력을 확인하세요. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

ONTAP 9.11.1부터 시스템 관리자에서 시스템 용량, 보안 규정 준수 및 구성을 최적화하는 데 도움이 되는 통찰력을 볼 수 있습니다.

- 확장 차단으로 인해 예기치 않은 결과가 발생할 수 있습니다. * ONTAP 9.11.1부터 시스템 관리자를 사용하여 스토리지 VM에 대한 기본 FPolicy를 활성화할 수 있습니다. 자신에게 권장되는 System Manager Insight 메시지를 받을 수 있습니다 "기본 FPolicy를 구성합니다" Insight 설문조사에 응답해 주세요.

FPolicy 기본 모드를 사용하면 특정 파일 확장자를 허용하거나 허용하지 않을 수 있습니다. System Manager는 과거 랜섬웨어 공격에 사용되었던 허용되지 않는 파일 확장자를 3000개 이상 권장합니다. 이러한 확장자 중 일부는 사용자 환경의 합법적인 파일에 의해 사용될 수 있으며 이러한 파일을 차단하면 예기치 않은 문제가 발생할 수 있습니다.

따라서 사용자 환경의 요구에 맞게 확장 목록을 수정하는 것이 좋습니다. 을 참조하십시오 "System Manager를 사용하여 System Manager에서 생성된 기본 FPolicy 구성에서 파일 확장명을 제거하여 정책을 재생성하는 방법".

기본 FPolicy에 대한 자세한 내용은 를 참조하십시오"FPolicy 구성 유형".

모범 사례에 따라 이러한 통찰력은 한 페이지에 표시되어 즉시 조치를 시작하여 시스템을 최적화할 수 있습니다. 자세한 내용은 을 "System Manager 인사이트"참조하십시오.

최적화 인사이트 보기

단계

1. System Manager의 왼쪽 탐색 열에서 * Insights * 를 클릭합니다.

   Insights * 페이지에는 인사이트 그룹이 표시됩니다. 각 인사이트 그룹에는 하나 이상의 통찰력이 포함될 수 있습니다. 다음 그룹이 표시됩니다.

   - 주의가 필요합니다
   - 위험 개선
   - 스토리지를 최적화하십시오
2. (선택 사항) 페이지의 오른쪽 위 모서리에 있는 다음 단추를 클릭하여 표시되는 통찰력을 필터링합니다.
   - 보안 관련 인사이트를 표시합니다.
   - 용량 관련 인사이트를 표시합니다.
   - 구성 관련 인사이트를 표시합니다.
   - 모든 정보를 표시합니다.

인사이트를 활용하여 시스템을 최적화합니다

System Manager에서 통찰력을 손실, 문제 해결을 위한 다양한 방법 모색 또는 문제 해결을 위한 프로세스 시작을 통해 통찰력을 얻을 수 있습니다.

단계

1. System Manager의 왼쪽 탐색 열에서 * Insights * 를 클릭합니다.

2. Insight 위로 마우스를 가져가면 다음 작업을 수행할 수 있는 버튼이 표시됩니다.
   - * Dismiss *: 뷰에서 통찰력을 제거합니다. 통찰력을 취소하려면 다음을 참조하세요. [customize-settings-insights] .
   - * Explore *: 통찰력에 언급된 문제를 해결하는 다양한 방법을 알아보십시오. 이 버튼은 둘 이상의 교정 방법이 있는 경우에만 나타납니다.
   - * 수정 *: 통찰력에 언급된 문제를 해결하는 프로세스를 시작합니다. 수정 사항을 적용하는 데 필요한 조치를 취할지 여부를 확인하는 메시지가 표시됩니다.

> 이러한 작업 중 일부는 System Manager의 다른 페이지에서 시작할 수 있지만 * Insights * 페이지에서는 이 한 페이지에서 이러한 작업을 시작할 수 있으므로 일상적인 작업을 간소화할 수 있습니다.

통찰력을 위한 설정을 사용자 지정합니다

System Manager에서 알림을 받을 인사이트를 사용자 지정할 수 있습니다.

단계

1. System Manager의 왼쪽 탐색 열에서 * Insights * 를 클릭합니다.
2. 페이지의 오른쪽 위 모서리에서 을 클릭한 다음 * 설정 * 을 선택합니다.
3. 설정 * 페이지에서 알림을 받을 인사이트 옆에 있는 확인란이 있는지 확인합니다. 이전에 통찰력을 닫은 경우 해당 확인란에 체크 표시를 하여 닫은 통찰력을 취소할 수 있습니다.
4. 저장 * 을 클릭합니다.

통찰력을 **PDF** 파일로 내보냅니다

해당하는 모든 통찰력을 PDF 파일로 내보낼 수 있습니다.

단계

1. System Manager의 왼쪽 탐색 열에서 * Insights * 를 클릭합니다.
2. 페이지의 오른쪽 위 모서리에서 을 클릭한 다음 * 내보내기 * 를 선택합니다.

ONTAP 시스템 관리자에서 기본 FPolicies 구성

ONTAP 9.11.1부터 기본 FPolicy 구현을 제안하는 System Manager Insight를 수신하면 스토리지 VM 및 볼륨에서 구성할 수 있습니다.

시작하기 전에

System Manager Insights의 * 모범 사례 적용 * 에 액세스하면 기본 FPolicy가 구성되지 않았다는 메시지가 표시될 수 있습니다.

FPolicy 구성 유형에 대한 자세한 내용은 을 "FPolicy 구성 유형"참조하십시오.

단계

1. System Manager의 왼쪽 탐색 열에서 * Insights * 를 클릭합니다.
2. Apply 모범 사례 * 에서 * 기본 FPolicy가 구성되지 않음 * 을 찾습니다.

3. 조치를 취하기 전에 다음 메시지를 읽으십시오.

◦ 확장 차단으로 인해 예기치 않은 결과가 발생할 수 있습니다. * ONTAP 9.11.1부터 시스템 관리자를 사용하여 스토리지 VM에 대한 기본 FPolicy를 활성화할 수 있습니다. FPolicy 기본 모드를 사용하면 특정 파일 확장자를 허용하거나 허용하지 않을 수 있습니다. System Manager는 과거 랜섬웨어 공격에 사용되었던 허용되지 않는 파일 확장자를 3000개 이상 권장합니다. 이러한 확장자 중 일부는 사용자 환경의 합법적인 파일에 의해 사용될 수 있으며 이러한 파일을 차단하면 예기치 않은 문제가 발생할 수 있습니다.

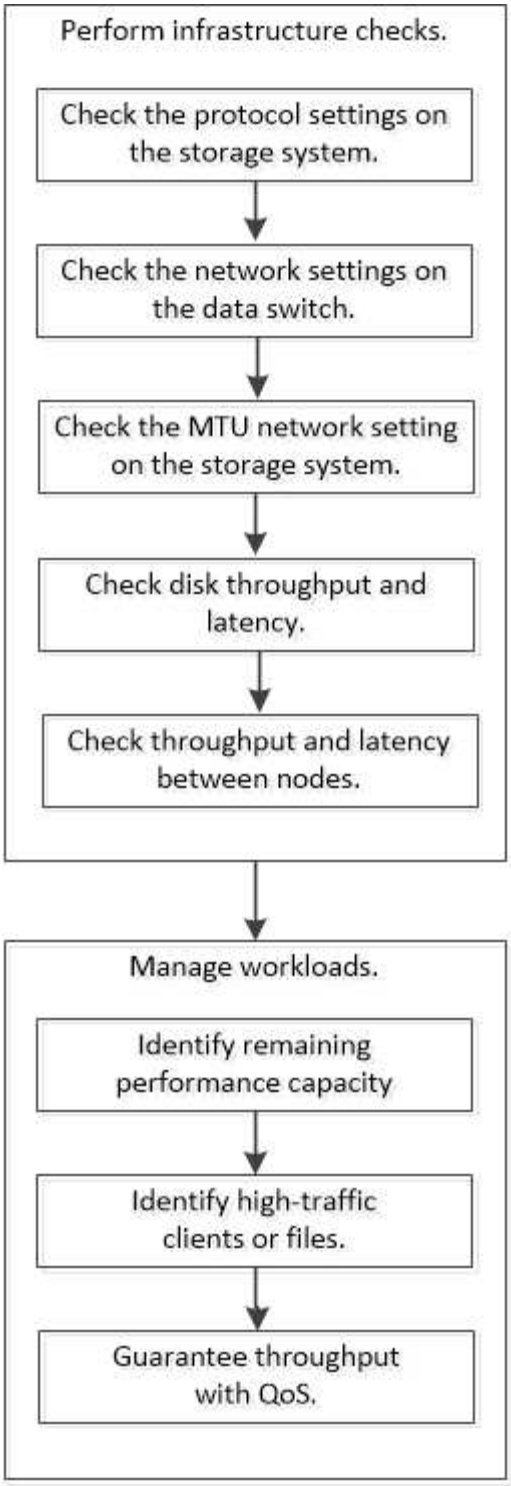
따라서 사용자 환경의 요구에 맞게 확장 목록을 수정하는 것이 좋습니다. 을 참조하십시오 "System Manager를 사용하여 System Manager에서 생성된 기본 FPolicy 구성에서 파일 확장명을 제거하여 정책을 재생성하는 방법".

4. 수정 * 을 클릭합니다.
5. 기본 FPolicy를 적용할 스토리지 VM을 선택합니다.
6. 각 스토리지 VM에 대해 기본 FPolicy를 받을 볼륨을 선택합니다.
7. 구성 * 을 클릭합니다.

CLI를 사용하여 클러스터 성능을 모니터링하고 관리합니다

ONTAP 성과 관리 워크플로

성능 문제를 식별한 후 인프라에 대한 몇 가지 기본적인 진단 검사를 수행하여 명백한 구성 오류를 배제할 수 있습니다. 정확히 찾아내지 못하는 문제라면 워크로드 관리 문제를 살펴보는 것이 좋습니다.



기본 인프라 검사를 수행합니다

스토리지 시스템의 프로토콜 설정을 확인합니다

ONTAP NFS TCP 최대 전송 크기를 확인하세요

NFS의 경우 읽기 및 쓰기에 대한 TCP 최대 전송 크기가 성능 문제를 일으킬 수 있는지 확인할 수 있습니다. 크기가 성능을 저하한다고 생각되면 크기를 늘릴 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자 권한이 있어야 합니다.
- 이 작업에는 고급 권한 레벨 명령을 사용해야 합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. TCP 최대 전송 크기를 확인합니다.

   'vserver nfs show -vserver_vserver_name_-instance'

3. TCP 최대 전송 크기가 너무 작은 경우 크기를 늘립니다.

   'vserver nfs modify -vserver_vserver_name_-tcp-max -xfer-size_integer_'

4. 관리 권한 수준으로 돌아가기:

   'Set-Privilege admin'입니다

예

다음 예에서는 'VM1'의 TCP 최대 전송 크기를 1048576으로 변경합니다.

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

ONTAP iSCSI TCP 읽기/쓰기 크기 확인

iSCSI의 경우 TCP 읽기/쓰기 크기를 확인하여 크기 설정이 성능 문제를 생성하고 있는지 확인할 수 있습니다. 크기가 문제의 원인이면 수정할 수 있습니다.

시작하기 전에

이 작업에는 고급 권한 레벨 명령이 필요합니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. TCP 윈도우 크기 설정을 확인합니다.

   'vserver iscsi show-vserv, er_vserver_name_-instance'

3. TCP 창 크기 설정을 수정합니다.

   'vserver iscsi modify -vserver_vserver_name_-tcp-window-size_integer_'

4. 관리 권한으로 돌아가기:

'Set-Privilege admin'입니다

예

다음 예에서는 'VM1'의 TCP 윈도우 크기를 131,400바이트로 변경합니다.

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

ONTAP CIFS/SMB 멀티플렉스 설정을 확인하세요

느린 CIFS 네트워크 성능으로 인해 성능 문제가 발생하는 경우 멀티플렉스 설정을 수정하여 성능을 개선하고 수정할 수 있습니다.

단계

1. CIFS 다중통신 설정을 점검한다.

   'vserver cifs options show -vserver_-vserver_name_-instance'

2. CIFS 다중통신 설정을 수정합니다.

   'vserver cifs options modify – vserver_-vserver_name_ – max-MPX_integer _'

예

다음 예에서는 'VM1'의 최대 다중통신 횟수를 255로 변경한다.

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

ONTAP FC 어댑터 포트 속도 확인

어댑터 대상 포트 속도는 성능을 최적화하기 위해 연결된 장치의 속도와 일치해야 합니다. 포트가 autonegotiation으로 설정된 경우 테이크오버 및 반환 또는 기타 중단이 발생한 후 다시 연결하는 데 시간이 더 오래 걸릴 수 있습니다.

시작하기 전에

이 어댑터를 홈 포트로 사용하는 모든 LIF는 오프라인 상태여야 합니다.

단계

1. 어댑터를 오프라인 상태로 전환:

   'network fcp adapter modify -node_nodename_-adapter_adapter_-state_down_'

   에 대한 자세한 내용은 `network fcp adapter modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 포트 어댑터의 최대 속도를 확인합니다.

   FCP 어댑터 show-instance(FCP 어댑터 show-instance)

에 대한 자세한 내용은 `fcp adapter show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 필요한 경우 포트 속도를 변경합니다.

   'network fcp adapter modify -node_nodename_-adapter_adapter_-speed{1|2|4|8|10|16|auto}'

4. 어댑터를 온라인으로 전환합니다.

   'network fcp adapter modify -node_nodename_-adapter_adapter_ - state up'

5. 어댑터에 있는 모든 LIF를 온라인으로 전환합니다.

   'network interface modify -vserver * -lif * {-home-node node1 -home-port e0c} -status -admin up'

   에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

예

다음 예에서는 node1의 어댑터 0d의 포트 속도를 2Gbps로 변경합니다.

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

데이터 스위치에서 **ONTAP** 네트워크 설정을 확인하세요

클라이언트, 서버 및 스토리지 시스템(즉, 네트워크 엔드포인트)에서 동일한 MTU 설정을 유지해야 하지만 성능에 영향을 주지 않도록 NIC 및 스위치와 같은 중간 네트워크 디바이스를 최대 MTU 값으로 설정해야 합니다.

최상의 성능을 얻으려면 네트워크의 모든 구성 요소가 점보 프레임(9000바이트 IP, 9022바이트 이더넷 포함)을 포워드할 수 있어야 합니다. 데이터 스위치는 최소 9022바이트로 설정해야 하지만 대부분의 스위치에서 일반적인 값 9216을 사용할 수 있습니다.

단계

1. 데이터 스위치의 경우 MTU 크기가 9022 이상으로 설정되어 있는지 확인합니다.

자세한 내용은 스위치 공급업체 설명서를 참조하십시오.

스토리지 시스템에서 **ONTAP MTU** 네트워크 설정을 확인하세요**.**

스토리지 시스템의 네트워크 설정이 클라이언트 또는 다른 네트워크 엔드포인트와 동일하지 않은 경우 변경할 수 있습니다. 관리 네트워크 MTU 설정은 1500으로 설정되어 있지만 데이터 네트워크 MTU 크기는 9000이어야 합니다.

이 작업에 대해

브로드캐스트 도메인 내의 모든 포트는 MTU 크기가 동일하며 e0M 포트 처리 관리 트래픽을 제외하고 있습니다. 포트가 broadcast-domain의 일부인 경우 broadcast-domain modify 명령을 사용하여 수정된 broadcast-domain 내의 모든 포트에 대한 MTU를 변경한다.

NIC 및 데이터 스위치와 같은 중간 네트워크 장치는 네트워크 엔드포인트보다 더 높은 MTU 크기로 설정할 수 있습니다.

자세한 내용은 을 "데이터 스위치의 네트워크 설정을 확인합니다"참조하십시오.

단계

1. 스토리지 시스템에서 MTU 포트 설정을 확인합니다.

   네트워크 포트 show-instance

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 포트에서 사용하는 브로드캐스트 도메인의 MTU를 변경합니다.

   'network port broadcast-domain modify -IPSpace_IPSpace_-broadcast-domain_broadcast_domain_ -MTU_new_MTU_'

예

다음 예에서는 MTU 포트 설정을 9000으로 변경합니다.

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain
Cluster -mtu 9000
```

ONTAP 디스크 처리량 및 대기 시간 확인

클러스터 노드의 디스크 처리량 및 지연 시간 메트릭을 확인하여 문제 해결을 지원할 수 있습니다.

이 작업에 대해

이 작업에는 고급 권한 레벨 명령이 필요합니다.

단계

1. 고급 권한 레벨로 변경:

   ```
   set -privilege advanced
   ```

2. 디스크 처리량 및 지연 시간 메트릭을 확인합니다.

   ```
   statistics disk show -sort-key latency
   ```

예

다음 예제는 'cluster1'의 'node2'에 대한 각 사용자의 읽기 또는 쓰기 작업의 합계를 표시합니다.

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                     Busy Total Read  Write  Read    Write   *Latency
  Disk       Node    (%)   Ops   Ops   Ops   (Bps)    (Bps)       (us)
------------ ----    ---- ----   ----- ----- ------   -----     -----

1.10.20      node2      4    5       3     2  95232  367616     23806
1.10.8       node2      4    5       3     2 138240  386048     22113

1.10.6       node2      3    4       2     2  48128  371712     19113
1.10.19      node2      4    6       3     2 102400  443392     19106

1.10.11      node2      4    4       2     2 122880  408576     17713
```

관련 정보

- "통계 디스크 표시"

ONTAP 처리량 및 노드 간 지연 시간 확인

'network test-path' 명령을 사용하여 네트워크 병목 현상을 식별하거나 노드 간 네트워크 경로를 다시 확인할 수 있습니다. 클러스터 간 노드 또는 클러스터 내 노드 간에 명령을 실행할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 이 작업에는 고급 권한 레벨 명령이 필요합니다.
- 인터클러스터 경로의 경우 소스 클러스터와 대상 클러스터를 피어링해야 합니다.

이 작업에 대해

노드 간 네트워크 성능이 경로 구성에 대한 기대치를 충족하지 못하는 경우가 있습니다. 예를 들어, SnapMirror 복제 작업에서 볼 수 있는 대규모 데이터 전송 유형에 대한 1Gbps의 전송 속도는 소스 클러스터와 대상 클러스터 간의 10GbE 링크와 일치하지 않습니다.

network test-path 명령을 사용하여 노드 간 처리량과 대기 시간을 측정할 수 있습니다. 클러스터 간 노드 또는 클러스터 내 노드 간에 명령을 실행할 수 있습니다.

> 이 테스트는 데이터가 네트워크 경로를 포화시키기 때문에, 시스템이 사용 중이 아닐 때나 노드 간 네트워크 트래픽이 과도하지 않을 때는 명령을 실행해야 합니다. 10초 후 테스트 시간이 초과됩니다. 명령은 ONTAP 9 노드 간에만 실행할 수 있습니다.

'세션 유형' 옵션은 네트워크 경로를 통해 실행 중인 작업 유형을 식별합니다(예: 원격 대상에 대한 SnapMirror 복제를 위한 "AsyncMirrorRemote"). 유형은 테스트에 사용되는 데이터의 양을 나타냅니다. 다음 표에서는 세션 유형을 정의합니다.

세션 유형	설명

AsyncMirrorLocal 을 선택합니다	동일한 클러스터의 노드 간에 SnapMirror가 사용하는 설정입니다
AsyncMirrorRemote 를 참조하십시오	서로 다른 클러스터 노드 간에 SnapMirror가 사용하는 설정(기본 유형)
RemoteDataTransfer를 참조하십시오	ONTAP에서 동일한 클러스터의 노드 간 원격 데이터 액세스를 위해 사용하는 설정(예: 다른 노드의 볼륨에 저장된 파일에 대해 노드에 NFS 요청)

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 노드 간 처리량 및 지연 시간 측정:

   'network test-path-source-node_source_nodename_|local-destination-cluster_destination_clustername_-destination-node_destination_nodename_-session-type Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer'

   소스 노드는 로컬 클러스터에 있어야 합니다. 대상 노드는 로컬 클러스터 또는 피어링된 클러스터에 있을 수 있습니다. '-source-node'의 "local" 값은 명령을 실행하는 노드를 지정합니다.

   다음 명령을 실행하면 로컬 클러스터의 노드1과 클러스터2의 노드3의 SnapMirror 유형 복제 작업에 대한 처리량과 지연 시간이 측정됩니다.

   ```
   cluster1::> network test-path -source-node node1 -destination-cluster
   cluster2 -destination-node node3 -session-type AsyncMirrorRemote
   ```

   샘플 출력(출력 세부 사항은 사용 중인 ONTAP 버전에 따라 다를 수 있음):

   ```
   Test Duration:      10.88 secs
   Send Throughput:    18.23 MB/sec
   Receive Throughput: 18.23 MB/sec
   MB sent:            198.31
   MB received:        198.31
   Avg latency in ms:  2301.47
   ```

   에 대한 자세한 내용은 `network test-path` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 관리 권한으로 돌아가기:

   'Set-Privilege admin'입니다

작업을 마친 후

성능이 경로 구성에 대한 기대를 충족하지 않는 경우 노드 성능 통계를 확인하고, 사용 가능한 툴을 사용하여 네트워크에서 문제를 격리하고, 스위치 설정을 확인하는 등의 작업을 수행해야 합니다.

워크로드 관리

ONTAP에 남아 있는 성능 용량을 식별합니다

성능 용량, 즉_FLO여유_는 리소스의 워크로드 성능이 지연 시간의 영향을 받기 전에 노드나 애그리게이트에 배치할 수 있는 작업의 양을 측정합니다. 클러스터에서 사용 가능한 성능 용량을 파악하면 워크로드를 프로비저닝하고 조정할 수 있습니다.

시작하기 전에

이 작업에는 고급 권한 레벨 명령이 필요합니다.

이 작업에 대해

'-object' 옵션에 다음 값을 사용하여 여유 공간 통계를 수집하고 표시할 수 있습니다.

- CPU의 경우 resource_refLO여유_cpu'입니다.
- Aggregate의 경우 RESOURCE_LOBLO여유_aggr입니다.

System Manager 및 Active IQ Unified Manager를 사용하여 이 작업을 완료할 수도 있습니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 실시간 여유 공간 통계 수집 시작:

   '통계 시작 – object resource_refo여유_cpu|aggr'

   에 대한 자세한 내용은 `statistics start` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 실시간 여유 공간 통계 정보 표시:

   'tortistics show-object resource_fre여유_cpu|aggr'

4. 관리 권한으로 돌아가기:

   'Set-Privilege admin'입니다

예

다음 예제에는 클러스터 노드의 평균 사용 시간 여유 공간 통계가 표시됩니다.

Optimal_point_Utilization 카운터에서 Current_Utilization 카운터를 빼서 노드에 대해 사용 가능한 성능 용량을 계산할 수 있습니다. 이 예에서는 CPU_sti2520-213의 사용률 용량이 -14%(72%-86%)로, 이는 CPU가 지난 1시간 동안 평균 초과 사용되었음을 나타냅니다.

같은 정보를 더 오랜 기간 평균한 값으로 얻기 위해 'ewma_daily', 'ewma_weekly', 'ewma_monthly'를 지정할 수도

있습니다.

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
  (statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213

    Counter                                                     Value
    -------------------------------- ----------------------------------
    ewma_hourly                                                     -
                         current_ops                             4376
                     current_latency                            37719
                 current_utilization                               86
                   optimal_point_ops                             2573
               optimal_point_latency                             3589
            optimal_point_utilization                              72
     optimal_point_confidence_factor                                1

Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214

    Counter                                                     Value
    -------------------------------- ----------------------------------
    ewma_hourly                                                     -
                         current_ops                                0
                     current_latency                                0
                 current_utilization                                0
                   optimal_point_ops                                0
               optimal_point_latency                                0
            optimal_point_utilization                              71
     optimal_point_confidence_factor                                1
2 entries were displayed.
```

에 대한 자세한 내용은 `statistics show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP에서 트래픽이 높은 클라이언트 또는 파일을 식별합니다

ONTAP 활성 개체 기술을 사용하여 불균형적으로 많은 양의 클러스터 트래픽을 담당하는 클라이언트 또는 파일을 식별할 수 있습니다. 이러한 "상위" 클라이언트 또는 파일을 식별한 후에는 클러스터 워크로드를 재조정하거나 다른 단계를 수행하여 문제를 해결할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 클러스터에 액세스하는 상위 클라이언트 보기:

   'tortistics top client show -node_name_-sort-key_sort_column_-interval_seconds_between_updates_ -iterations_-max_number_of_instances_'

   다음 명령을 실행하면 'cluster1'에 액세스하는 상위 클라이언트가 표시됩니다.

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10


                                              *Total
        Client Vserver           Node Protocol    Ops
-------------- ------- -------------- -------- ------
172.17.180.170     vs4 siderop1-vsim4      nfs    668
172.17.180.169     vs3 siderop1-vsim3      nfs    337
172.17.180.171     vs3 siderop1-vsim3      nfs    142
172.17.180.170     vs3 siderop1-vsim3      nfs    137
172.17.180.123     vs3 siderop1-vsim3      nfs    137
172.17.180.171     vs4 siderop1-vsim4      nfs     95
172.17.180.169     vs4 siderop1-vsim4      nfs     92
172.17.180.123     vs4 siderop1-vsim4      nfs     92
172.17.180.153     vs3 siderop1-vsim3      nfs      0
```

   에 대한 자세한 내용은 `statistics top client show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 클러스터에서 액세스하는 상위 파일을 봅니다.

   'tortistics top file show -node_node_name_-sort-key_sort_column_-interval_seconds_between_updates_ -iterations_-max_number_of_instances_'

   다음 명령을 실행하면 'cluster1'에서 액세스되는 최상위 파일이 표시됩니다.

```
cluster1::> statistics top file show

cluster1 : 3/23/2016 17:59:10

                                    *Total
                     File Volume Vserver          Node    Ops
------------------------ ------ ------- -------------- ------
/vol/vol1/vm170-read.dat   vol1     vs4 siderop1-vsim4     22
/vol/vol1/vm69-write.dat   vol1     vs3 siderop1-vsim3      6
     /vol/vol2/vm171.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol2/vm169.dat   vol2     vs3 siderop1-vsim3      2
      /vol/vol2/p123.dat   vol2     vs4 siderop1-vsim4      2
      /vol/vol2/p123.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol1/vm171.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim3      2
      /vol/vol1/p123.dat   vol1     vs4 siderop1-vsim4      2
```

에 대한 자세한 내용은 `statistics top file show` "ONTAP 명령 참조입니다"을 참조하십시오.

QoS로 처리량 보장

ONTAP에서 QoS 개요를 통해 처리량을 보장합니다

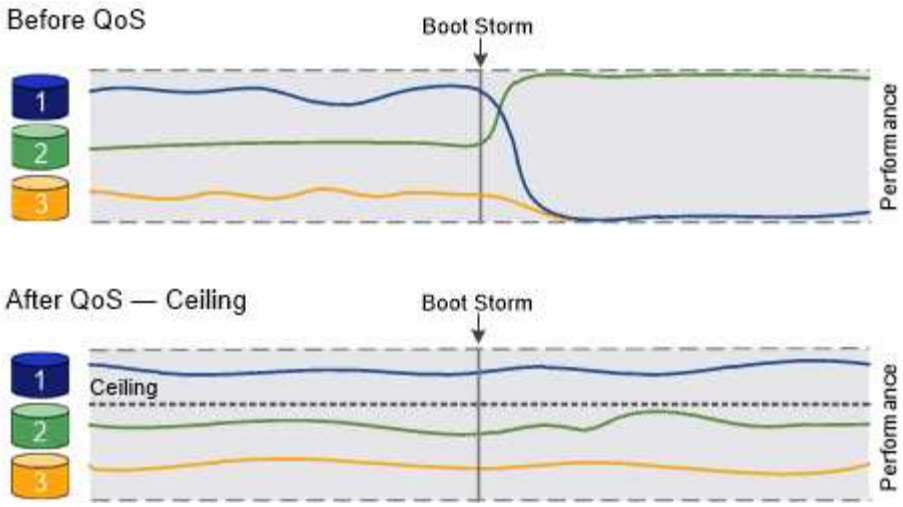
스토리지 QoS(서비스 품질)를 사용하여 주요 워크로드의 성능이 다른 워크로드에 의해 저하되지 않도록 보장할 수 있습니다. 경쟁 워크로드에 대한 throughput_ceiling_을 설정하여 시스템 리소스에 미치는 영향을 제한하거나 중요한 워크로드에 대한 throughput_floor_를 설정하여 경쟁 워크로드의 요구에 관계없이 최소 처리량 목표를 달성할 수 있습니다. 동일한 워크로드에 대해 천장과 바닥을 설정할 수도 있습니다.

처리량 한도(QoS 최대)

처리량 상한은 워크로드의 처리량을 최대 IOPS 또는 MBps, 즉 IOPS 및 MBps로 제한합니다. 아래 그림에서는 워크로드 2의 처리량 상한을 통해 워크로드 1과 3이 "괴롭지" 않도록 합니다.

policy group_은 하나 이상의 워크로드에 대한 처리량 한도를 정의합니다. 워크로드는 _ 스토리지 객체에 대한 입출력 작업을 나타냅니다. _ 볼륨, 파일, qtree 또는 LUN 또는 SVM의 모든 볼륨, 파일, Qtree 또는 LUN입니다. 정책 그룹을 생성할 때 상한을 지정하거나 워크로드를 모니터링하여 지정할 때까지 기다릴 수 있습니다.

> 워크로드에 대한 처리량이 지정된 상한을 최대 10% 초과할 수 있습니다. 특히, 작업 부하에 대한 처리량이 급격하게 변경될 경우 더욱 그렇습니다. 천장은 버스트를 처리하기 위해 최대 50%까지 초과될 수 있습니다. 토큰이 최대 150%까지 누적되면 단일 노드에서 버스트가 발생합니다



처리량 최저액**(QoS Min)**

처리량 한도 에서는 워크로드의 처리량이 최소 IOPS 또는 MBps, 즉 IOPS 및 MBps 미만으로 떨어지지 않도록 보장합니다. 아래 그림에서 워크로드 1과 워크로드 3의 처리량 플로어는 워크로드 2의 수요에 관계없이 최소 처리량 목표를 충족할 수 있도록 합니다.

예를 들어, 처리량 상한은 처리량을 직접 조절합니다. 처리량 플로어에서는 플로어가 설정된 워크로드에 우선 순위를 부여하여 간접적으로 처리량을 조절합니다.

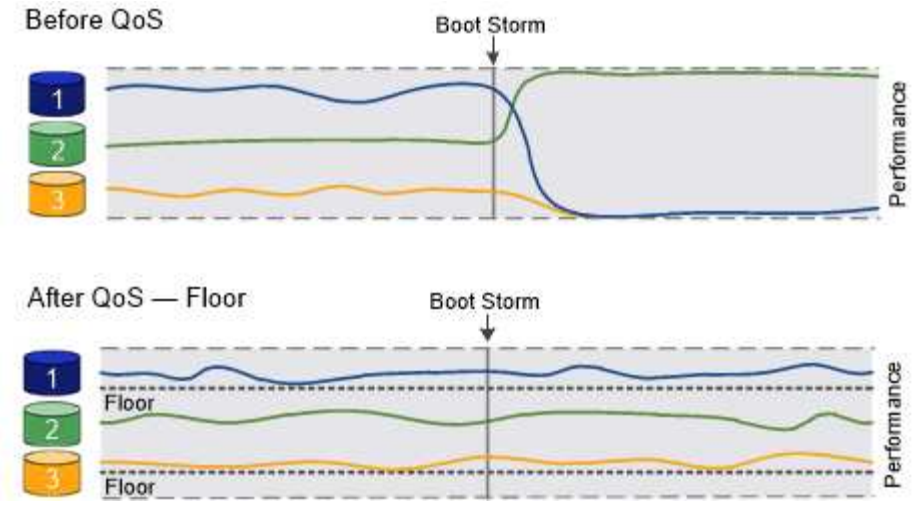
정책 그룹을 생성할 때 층을 지정하거나 워크로드를 모니터링하여 지정할 때까지 기다릴 수 있습니다.

ONTAP 9.13.1부터 를 사용하여 SVM 범위에서 처리량 플로트를 설정할 수 있습니다[adaptive-qos-templates]. 9.13.1 이전의 ONTAP 릴리즈에서는 처리량 플로어를 정의하는 정책 그룹을 SVM에 적용할 수 없습니다.

ONTAP 9.7 이전의 릴리즈에서는 사용 가능한 성능 용량이 충분한 경우 처리량 바닥이 보장됩니다.

ONTAP 9.7 이상에서는 사용 가능한 성능 용량이 부족하더라도 처리량 플로어를 보장할 수 있습니다. 이러한 새로운 바닥 동작을 바닥 v2라고 합니다. 보장 사항을 충족하기 위해 v2층은 처리량 공간 또는 바닥 설정을 초과하는 작업 환경에서 작업 부하에 대한 대기 시간이 더 길어질 수 있습니다. 버전 v2는 QoS 및 적응형 QoS에 모두 적용됩니다.

ONTAP 9.7P6 이상에서 새로운 바닥 v2의 동작을 활성화/비활성화하는 옵션을 사용할 수 있습니다. 과 같은 중요한 작업 중에는 워크로드가 지정된 설치 공간 아래로 떨어질 수 있습니다 `volume move trigger-cutover`. 충분한 용량을 사용할 수 있고 중요한 작업이 마련되어 있지 않더라도 워크로드의 처리량은 지정된 바닥 미만으로 최대 5% 떨어질 수 있습니다. 바닥이 초과 프로비저닝되고 성능 용량이 없는 경우 일부 워크로드가 지정된 설치 공간 아래로 떨어질 수 있습니다.



공유 및 비공유 **QoS** 정책 그룹

ONTAP 9.4부터 _non-shared_QoS 정책 그룹을 사용하여 정의된 처리량 상한 또는 최저가 각 구성원 워크로드에 개별적으로 적용되도록 지정할 수 있습니다. shared_policy 그룹의 동작은 정책 유형에 따라 달라집니다.

- 처리량 천장의 경우 공유 정책 그룹에 할당된 워크로드의 총 처리량은 지정된 한도를 초과할 수 없습니다.
- 처리량 플로어의 경우 공유 정책 그룹을 단일 워크로드에만 적용할 수 있습니다.

적응형 **QoS**

일반적으로 스토리지 객체에 할당한 정책 그룹의 값은 고정됩니다. 스토리지 오브젝트의 크기가 변경되면 값을 수동으로 변경해야 합니다. 예를 들어, 볼륨에 사용된 공간의 양을 늘리려면 일반적으로 볼륨에 지정된 처리량 상한을 늘려야 합니다.

_Adaptive QoS_는 워크로드 크기에 따라 정책 그룹 값을 자동으로 확장하며 워크로드 크기 변화에 따라 IOPS와 TB|GB의 비율을 유지합니다. 이는 대규모 구축 환경에서 수백 또는 수천 개의 워크로드를 관리할 때 큰 이점입니다.

일반적으로 적응형 QoS를 사용하여 처리량 한도를 조정할 수 있지만 워크로드 크기가 증가하는 경우 이를 사용하여 처리량 플로어를 관리할 수도 있습니다. 워크로드 크기는 스토리지 객체에 할당된 공간 또는 스토리지 객체가 사용하는 공간으로 표시됩니다.

ONTAP 9.5 이상의 처리량 층에서는 사용된 공간을 사용할 수 있습니다. ONTAP 9.4 및 이전 버전의 처리량 바닥재에서는 지원되지 않습니다.

- allocated space_policy는 스토리지 객체의 공칭 크기에 따라 IOPS/TB|GB 비율을 유지합니다. 비율이 100 IOPS/GB인 경우, 볼륨이 해당 크기로 유지되는 한 150 GB 볼륨의 처리량은 최대 15,000 IOPS입니다. 볼륨의 크기를 300GB로 변경하면 적응형 QoS는 처리량의 상한을 30,000 IOPS로 조정합니다.
- a_used space_policy(기본값)는 스토리지 효율성 이전에 저장된 실제 데이터의 양에 따라 IOPS/TB|GB 비율을 유지합니다. 비율이 100 IOPS/GB인 경우 100GB 데이터가 저장된 150GB 볼륨의 처리량은 최대 10,000 IOPS입니다. 사용된 공간의 양이 변경되면 적응형 QoS는 비율에 따라 처리량 상한을 조정합니다.

ONTAP 9.5부터 IOPS 및 MBPS 모두에서 처리량 제한을 나타낼 수 있도록 응용 프로그램에 대한 I/O 블록 크기를 지정할 수 있습니다. MBPS 제한은 블록 크기에 IOPS 제한을 곱하여 계산됩니다. 예를 들어, 6144IOPS/TB의 IOPS 한계 32K의 I/O 블록 크기는 192MBps의 MBPS 제한을 생성합니다.

처리량 천장과 바닥에 대해 다음과 같은 동작을 예상할 수 있습니다.

- 워크로드가 적응형 QoS 정책 그룹에 할당되면 상한 또는 하한 이 즉시 업데이트됩니다.
- 적응형 QoS 정책 그룹의 워크로드 크기를 조정하면 최대 또는 최저값이 약 5분 내에 업데이트됩니다.

업데이트를 적용하기 전에 처리량이 최소 10 IOPS 이상 증가해야 합니다.

적응형 QoS 정책 그룹은 항상 공유되지 않습니다. 정의된 처리량 상한 또는 최저값은 각 구성원 워크로드에 개별적으로 적용됩니다.

ONTAP 9.6부터 SSD가 장착된 ONTAP Select 프리미엄에서 처리량 플로어를 지원합니다.

적응형 정책 그룹 템플릿입니다

ONTAP 9.13.1부터 SVM에 적응형 QoS 템플릿을 설정할 수 있습니다. 적응형 정책 그룹 템플릿을 사용하면 SVM에서 모든 볼륨의 처리량 플로어 및 한도를 설정할 수 있습니다.

적응형 정책 그룹 템플릿은 SVM이 생성된 후에만 설정할 수 있습니다. 를 사용합니다 `vserver modify` 명령과 함께 `-qos-adaptive-policy-group-template` 매개 변수를 사용하여 정책을 설정합니다.

적응형 정책 그룹 템플릿을 설정하면 정책을 설정한 후 생성되거나 마이그레이션된 볼륨이 정책을 자동으로 상속합니다. 정책 템플릿을 할당할 때 SVM에 존재하는 볼륨은 영향을 받지 않습니다. SVM에서 정책을 사용하지 않도록 설정하면 이후에 SVM으로 마이그레이션되거나 SVM에서 생성된 모든 볼륨에서 정책을 받지 않습니다. 적응형 정책 그룹 템플릿을 사용하지 않도록 설정해도 정책 템플릿을 상속한 볼륨에는 영향을 주지 않습니다.

자세한 내용은 을 참조하십시오 적응형 정책 그룹 템플릿을 설정합니다.

일반 지원

다음 표에는 처리량 천장, 처리량 바닥 및 적응형 QoS 지원 차이의 차이가 나와 있습니다.

리소스 또는 기능	처리량 한도	처리량 플로어	처리량 플로어 **v2**	적응형 **QoS**
ONTAP 9 버전	모두	9.2 이상	9.7 이상	9.3 이상
플랫폼	모두	• AFF • C190(1) • ONTAP Select 프리미엄 및 SSD 1	• AFF • C190 • SSD가 포함된 ONTAP Select 프리미엄	모두
프로토콜	모두	모두	모두	모두
FabricPool	예	예. 계층화 정책이 "없음"으로 설정되고 클라우드에 블록이 없는 경우	예. 계층화 정책이 "없음"으로 설정되고 클라우드에 블록이 없는 경우	아니요
SnapMirror Synchronous	예	아니요	아니요	예

ONTAP 9.6 릴리스부터 C190 및 ONTAP Select 지원이 시작되었습니다.

처리량 상한에 대해 지원되는 워크로드

다음 표에서는 ONTAP 9 버전별 처리량 천장에 대한 워크로드 지원을 보여 줍니다. 루트 볼륨, 로드 공유 미러 및 데이터 보호 미러는 지원되지 않습니다.

워크로드 지원	**ONTAP 9.8** 이상	**ONTAP 9.7~9.4**	**ONTAP 9.3** 및 이전 버전
볼륨	예	예	예
파일	예	예	예
LUN을 클릭합니다	예	예	예
SVM	예	예	예
FlexGroup 볼륨	예	예	예(ONTAP 9.3만 해당)
qtree(1)	예	아니요	아니요
정책 그룹당 워크로드가 여러 개일 수 있습니다	예	예	예
비공유 정책 그룹입니다	예	예	아니요

[1] ONTAP 9.9.1부터 SMB가 활성화된 FlexVol 및 FlexGroup 볼륨의 qtree에서도 SMB 액세스가 지원됩니다. ONTAP 9.8부터 NFS가 활성화된 FlexVol 및 FlexGroup 볼륨의 qtree에서 NFS 액세스가 지원됩니다.

처리량 플로어에 대해 지원되는 워크로드

다음 표에는 ONTAP 9 버전별 처리량 플로어에 대한 워크로드 지원이 나와 있습니다. 루트 볼륨, 로드 공유 미러 및 데이터 보호 미러는 지원되지 않습니다.

워크로드 지원	**ONTAP 9.13.1** 이상	**ONTAP 9.8 ~ 9.13.0**	**ONTAP 9.4 - 9.7**	**ONTAP 9.3**
볼륨	예	예	예	예
파일	예	예	예	예
LUN을 클릭합니다	예	예	예	예
SVM	예	아니요	아니요	아니요
FlexGroup 볼륨	예	예	예	아니요
qtree(1)	예	예	아니요	아니요
정책 그룹당 워크로드가 여러 개일 수 있습니다	예	예	예	아니요

워크로드 지원	**ONTAP 9.13.1** 이상	**ONTAP 9.8 ~ 9.13.0**	**ONTAP 9.4 - 9.7**	**ONTAP 9.3**
비공유 정책 그룹입니다	예	예	예	아니요

ONTAP 9.8부터 NFS 액세스가 FlexVol 및 FlexGroup 볼륨에서 지원됩니다. ONTAP 9.9.1부터 SMB가 활성화된 FlexVol 및 FlexGroup 볼륨의 qtree에서도 SMB 액세스가 지원됩니다.

적응형 **QoS**에 지원되는 워크로드

다음 표는 ONTAP 9 버전별 적응형 QoS에 대한 워크로드 지원을 보여줍니다. 루트 볼륨, 로드 공유 미러 및 데이터 보호 미러는 지원되지 않습니다.

워크로드 지원	**ONTAP 9.13.1** 이상	**ONTAP 9.4 ~ 9.13.0**	**ONTAP 9.3**
볼륨	예	예	예
파일	예	예	아니요
LUN을 클릭합니다	예	예	아니요
SVM	예	아니요	아니요
FlexGroup 볼륨	예	예	아니요
정책 그룹당 워크로드가 여러 개일 수 있습니다	예	예	예
비공유 정책 그룹입니다	예	예	예

최대 워크로드 및 정책 그룹 수

다음 표에는 ONTAP 9 버전별 최대 워크로드 및 정책 그룹 수가 나와 있습니다.

워크로드 지원	**ONTAP 9.4** 이상	**ONTAP 9.3** 및 이전 버전
클러스터당 최대 워크로드	40,000개	12,000
노드당 최대 워크로드	40,000개	12,000
최대 정책 그룹 수	12,000	12,000

ONTAP 처리량 바닥 **v2** 활성화 또는 비활성화

AFF에서 Throughput Floor v2를 활성화 또는 비활성화할 수 있습니다. 기본값은 ENABLED입니다. v2를 지원하는 경우, 컨트롤러가 다른 워크로드에 지연 시간이 길어지는 대신 사용량이 많은 경우 처리량 플로어를 충족할 수 있습니다. 버전 v2는 QoS 및 Adaptive QoS 모두에 적용됩니다.

단계

1. 고급 권한 레벨로 변경:

   세트 프리빌리지 고급

2. 다음 명령 중 하나를 입력합니다.

원하는 작업	다음 명령을 사용합니다.
Floor v2를 비활성화합니다	QoS 설정 처리량-층-v2-활성화 거짓
Floor v2를 활성화합니다	QoS 설정 처리량-층-v2-활성화 true

MetroCluster 클러스터에서 처리량 층 v2를 비활성화하려면 를 실행해야 합니다

QoS 설정 처리량-층-v2-활성화 거짓

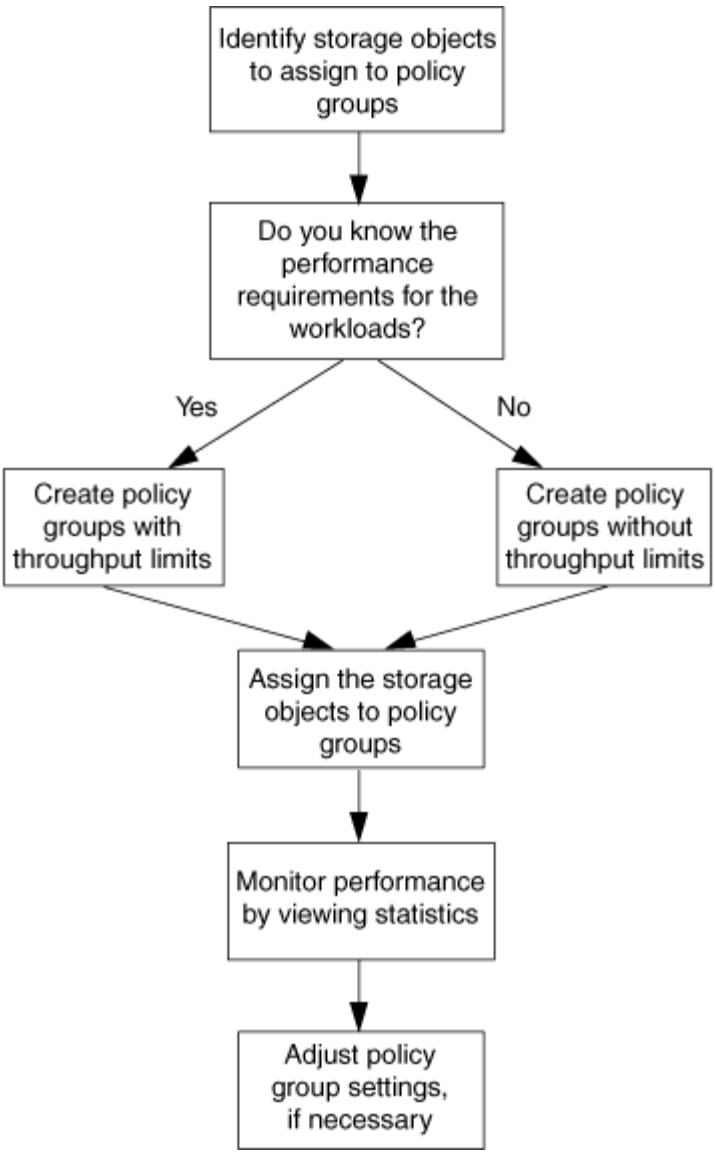
소스 클러스터와 대상 클러스터 모두에서 명령을 내립니다.

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

에 대한 자세한 내용은 `qos settings throughput-floors-v2` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 스토리지 **QoS** 워크플로

QoS를 사용하여 관리할 워크로드의 성능 요구사항을 이미 알고 있는 경우 정책 그룹을 생성할 때 처리량 한도를 지정할 수 있습니다. 그렇지 않으면 워크로드를 모니터링하여 한도를 지정할 때까지 기다릴 수 있습니다.



ONTAP에서 **QoS**를 사용하여 처리량의 한계를 설정합니다

정책 그룹에 대해 '최대 처리량' 필드를 사용하여 스토리지 오브젝트 워크로드의 처리량 한도(QoS Max)를 정의할 수 있습니다. 스토리지 객체를 생성하거나 수정할 때 정책 그룹을 적용할 수 있습니다.

시작하기 전에

- 정책 그룹을 생성하려면 클러스터 관리자여야 합니다.
- SVM에 정책 그룹을 적용하려면 클러스터 관리자여야 합니다.

이 작업에 대해

- ONTAP 9.4부터 _non-shared_QoS 정책 그룹을 사용하여 정의된 처리량 상한이 각 구성원 워크로드에 개별적으로 적용되도록 지정할 수 있습니다. 그렇지 않으면 정책 그룹이 _ 공유: _ 입니다. 정책 그룹에 할당된 워크로드의 총 처리량은 지정된 한도를 초과할 수 없습니다.

  비공유 정책 그룹을 지정하기 위해 QoS policy-group create 명령에 대해 -is-shared=false를 설정합니다.

- 천장에 대한 처리량 제한을 IOPS, MB/s 또는 IOPS, MB/s로 지정할 수 있습니다 IOPS와 MB/s를 모두 지정하는

경우, 어느 한쪽의 제한에 먼저 도달하더라도 적용됩니다.

> 동일한 워크로드에 대해 천장과 바닥을 설정하는 경우 IOPS만 사용하여 천장에 대한 처리량 제한을 지정할 수 있습니다.

- QoS 제한이 적용되는 스토리지 개체는 정책 그룹이 속한 SVM에 포함되어 있어야 합니다. 여러 정책 그룹이 동일한 SVM에 속할 수 있습니다.
- 포함하는 객체 또는 해당 하위 객체가 정책 그룹에 속해 있는 경우 스토리지 객체를 정책 그룹에 할당할 수 없습니다.
- 정책 그룹을 동일한 유형의 스토리지 객체에 적용하는 것은 QoS 모범 사례입니다.

단계

1. 정책 그룹 생성:

   "QoS policy-group create-policy-group_policy_group_-vserver_SVM_-max-throughput_number_of_IOPS_|MB/S|IOPS, MB/S-is-shared true|false

   에 대한 자세한 내용은 `qos policy-group create` "ONTAP 명령 참조입니다"을 참조하십시오.

   명령을 사용하여 처리량 한도를 조정할 수 `qos policy-group modify` 있습니다.

   다음 명령을 실행하면 최대 5,000 IOPS의 처리량을 갖는 공유 정책 그룹 'pg-vs1'이 생성됩니다.

   ```
   cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
   -max-throughput 5000iops -is-shared true
   ```

   다음 명령을 실행하면 비공유 정책 그룹 'pg-vs3'이 생성되고 최대 처리량은 100IOPS, 400KB/S입니다.

   ```
   cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
   -max-throughput 100iops,400KB/s -is-shared false
   ```

   다음 명령을 실행하면 처리량 제한 없이 비공유 정책 그룹 'pg-vs4'가 생성됩니다.

   ```
   cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
   -is-shared false
   ```

   에 대한 자세한 내용은 `qos policy-group modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. SVM, 파일, 볼륨 또는 LUN에 정책 그룹 적용:

   '*storage_object_create-vserver_SVM*-QoS-policy-group_policy_group_'

   이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오. 명령을 사용하여 스토리지 객체에 다른 정책 그룹을 적용할 수 *`storage_object`* `modify` 있습니다.

   다음 명령은 SVM 'VS1'에 정책 그룹 'pg-vs1'을 적용합니다.

```
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
```

다음 명령은 정책 그룹 pg-app을 볼륨 app1과 app2에 적용합니다.

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

3. 정책 그룹 성능 모니터링:

   QoS 통계 성능 표시

   에 대한 자세한 내용은 `qos statistics performance show` "ONTAP 명령 참조입니다"을 참조하십시오.

   > 클러스터의 성능 모니터링 호스트의 툴을 사용하여 성능을 모니터링하지 마십시오.

   다음 명령을 실행하면 정책 그룹 성능이 표시됩니다.

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_vs1                   5008       19.56MB/s     2.45ms
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

4. 워크로드 성능 모니터링:

   QoS 통계 워크로드 성능 표시

   > 클러스터의 성능 모니터링 호스트의 툴을 사용하여 성능을 모니터링하지 마십시오.

   다음 명령을 실행하면 워크로드 성능이 표시됩니다.

```
cluster1::> qos statistics workload performance show
Workload           ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-               -    12320        47.84MB/s  1215.00us
app1-wid7967       7967     7219        28.20MB/s   319.00us
vs1-wid12279      12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS      14       55        10.92KB/s   236.00us
_Scan_Backgro..    5688       20            0KB/s        0ms
```

에 대한 자세한 내용은 `qos statistics workload performance show` "ONTAP 명령 참조입니다"을 참조하십시오.

명령을 사용하여 QoS 워크로드에 대한 자세한 지연 시간 통계를 볼 수 `qos statistics workload latency show` 있습니다. 에 대한 자세한 내용은 `qos statistics workload latency show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP에서 **QoS**로 처리량 기준을 설정합니다

정책 그룹의 '처리량' 필드를 사용하여 스토리지 오브젝트 워크로드의 처리량(QoS Min)을 정의할 수 있습니다. 스토리지 객체를 생성하거나 수정할 때 정책 그룹을 적용할 수 있습니다. ONTAP 9.8부터는 처리량(IOPS 또는 MBps, IOPS 및 MBps)을 지정할 수 있습니다.

시작하기 전에

- 정책 그룹을 생성하려면 클러스터 관리자여야 합니다.
- ONTAP 9.13.1부터 를 사용하여 SVM 레벨에서 처리량 바닥글을 적용할 수 있습니다.적응형 정책 그룹 템플릿입니다 QoS 정책 그룹을 갖는 SVM에서는 적응형 정책 그룹 템플릿을 설정할 수 없습니다.

이 작업에 대해

- ONTAP 9.4부터 _non-shared_QoS 정책 그룹을 사용하여 각 구성원 작업 부하에 대해 정의된 처리 층을 개별적으로 적용할 수 있습니다. 이는 처리량 플로어의 정책 그룹을 여러 워크로드에 적용할 수 있는 유일한 조건입니다.

  비공유 정책 그룹을 지정하기 위해 QoS policy-group create 명령에 대해 -is-shared=false를 설정합니다.

- 노드나 애그리게이트에 성능 용량(여유 공간)이 충분하지 않은 경우 워크로드에 대한 처리량이 지정된 플로어에 아래로 떨어질 수 있습니다.
- QoS 제한이 적용되는 스토리지 개체는 정책 그룹이 속한 SVM에 포함되어 있어야 합니다. 여러 정책 그룹이 동일한 SVM에 속할 수 있습니다.
- 정책 그룹을 동일한 유형의 스토리지 객체에 적용하는 것은 QoS 모범 사례입니다.
- 처리량 플로어를 정의하는 정책 그룹은 SVM에 적용할 수 없습니다.

단계

1. 에 설명된 대로 노드 또는 애그리게이트에서 적절한 성능 용량이 있는지 확인합니다 "남은 성능 용량 식별".
2. 정책 그룹 생성:

'QoS policy-group create-policy group_policy_group_-vserver_SVM_-min-throughput_QoS_target_-is-shared true|false'

에 대한 자세한 내용은 `qos policy-group create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 명령을 사용하여 처리량 최저치를 조정할 수 `qos policy-group modify` 있습니다.

   다음 명령을 실행하면 처리량이 최소 1,000 IOPS인 공유 정책 그룹이 `pg-vs2` 생성됩니다.

   ```
   cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2
   -min-throughput 1000iops -is-shared true
   ```

   다음 명령을 실행하면 처리량 제한 없이 비공유 정책 그룹 'pg-vs4'가 생성됩니다.

   ```
   cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4
   -is-shared false
   ```

   에 대한 자세한 내용은 `qos policy-group modify` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 볼륨 또는 LUN에 정책 그룹 적용:

   `storage_object` `create -vserver` *`SVM`* `-qos-policy-group` *`policy_group`*`당신은 사용할 수 있습니다 `_storage_object_modify` 저장소 개체에 다른 정책 그룹을 적용하는 명령입니다.

   다음 명령은 정책 그룹 pg-app2를 볼륨 app2에 적용합니다.

   ```
   cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
   -qos-policy-group pg-app2
   ```

   이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

5. 정책 그룹 성능 모니터링:

   QoS 통계 성능 표시

   > 클러스터의 성능 모니터링 호스트의 툴을 사용하여 성능을 모니터링하지 마십시오.

   다음 명령을 실행하면 정책 그룹 성능이 표시됩니다.

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_app2                  7216       28.19MB/s   420.00us
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

에 대한 자세한 내용은 `qos statistics performance show` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 워크로드 성능 모니터링:

QoS 통계 워크로드 성능 표시

> 클러스터의 성능 모니터링 호스트의 툴을 사용하여 성능을 모니터링하지 마십시오.

다음 명령을 실행하면 워크로드 성능이 표시됩니다.

```
cluster1::> qos statistics workload performance show
Workload           ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app2-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

에 대한 자세한 내용은 `qos statistics workload performance show` "ONTAP 명령 참조입니다"을 참조하십시오.

> 명령을 사용하여 QoS 워크로드에 대한 자세한 지연 시간 통계를 볼 수 `qos statistics workload latency show` 있습니다. 에 대한 자세한 내용은 `qos statistics workload latency show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP에서 적응형 **QoS** 정책 그룹 사용

적응형 *QoS* 정책 그룹을 사용하면 볼륨 크기에 맞게 처리량 상한선이나 하한선을 자동으로 조정하여 볼륨 크기가 변경되더라도 IOPS 대 TB/GB 비율을 유지할 수 있습니다. 이는 대규모 배포에서 수백 또는 수천 개의 작업 부하를 관리할 때 상당한 이점입니다.

시작하기 전에

- ONTAP 9.3 이상을 실행해야 합니다. 적응형 QoS 정책 그룹은 ONTAP 9.3부터 사용할 수 있습니다.
- 정책 그룹을 생성하려면 클러스터 관리자여야 합니다.

이 작업에 대해

스토리지 개체는 적응형 정책 그룹 또는 비적응 정책 그룹의 구성원일 수 있지만 둘 다 속할 수는 없습니다. 스토리지 오브젝트 및 정책의 SVM은 동일해야 합니다. 스토리지 객체가 온라인 상태여야 합니다.

적응형 QoS 정책 그룹은 항상 공유되지 않습니다. 정의된 처리량 상한 또는 최저값은 각 구성원 워크로드에 개별적으로 적용됩니다.

스토리지 오브젝트 크기에 대한 처리량 제한의 비율은 다음 필드의 상호 작용에 의해 결정됩니다.

- `expected-iops`할당된 TB/GB당 예상 최소 IOPS입니다.

> `expected-iops` 는 AFF 플랫폼에서만 보장됩니다. `expected-iops` 계층화 정책이 "없음"으로 설정되어 있고 클라우드에 블록이 없는 경우에만 FabricPool에 대해 보장됩니다. `expected-iops` SnapMirror 동기식 관계에 없는 볼륨에 대해 보장합니다.

- `peak-iops`할당되거나 사용된 TB/GB당 가능한 최대 IOPS입니다.
- 'expected-IOPS-allocation'은 할당된 공간(기본값)이나 사용된 공간을 예상 IOPS에 사용할지 여부를 지정합니다.

> ONTAP 9.5 이상에서 '예상 IOPS 할당'을 사용할 수 있습니다. ONTAP 9.4 이하 버전에서는 지원되지 않습니다.

- peak-IOPS-allocation은 peak-IOPS를 위해 할당된 공간과 사용된 공간(기본값)을 사용할지 여부를 지정한다.
- 절대 최소 IOPS는 절대 최소 IOPS의 수입니다. 이 필드는 매우 작은 스토리지 객체와 함께 사용할 수 있습니다. 절대분 IOPS가 계산된 예상 IOPS보다 크면 peak-IOPS와 expected-IOPS를 모두 재정의합니다.

  예를 들어, 'expected-IOPS'를 1,000 IOPS/TB로 설정하고 볼륨 크기가 1GB 미만인 경우 계산된 'expected-IOPS'는 IOP가 분수 값이 됩니다. 계산된 피크 IOPS는 이보다 훨씬 적은 비율입니다. 절대-최소-IOPS를 실제 값으로 설정하면 이러한 문제를 방지할 수 있습니다.

- 블록 크기 는 애플리케이션 입출력 블록 크기를 지정합니다. 기본값은 32K입니다. 유효한 값은 8K, 16K, 32K, 64K, any입니다. Any는 블록 크기가 적용되지 않음을 의미합니다.

기본 적응형 **QoS** 정책 그룹

다음 표에 나와 있는 것처럼 세 가지 기본 적응형 QoS 정책 그룹을 사용할 수 있습니다. 이러한 정책 그룹을 볼륨에 직접 적용할 수 있습니다.

기본 정책 그룹입니다	예상 IOPS/TB	최대 IOPS/TB	절대 최소 IOPS
"익스트림"	6,144	12,288	1000입니다
'퍼포먼스'	2,048	4,096개	500입니다
값	128	512	75를

스토리지 개체 정책 그룹 할당 제한 사항

어떤 경우에는 정책 그룹에 저장 객체를 할당할 수 없습니다. 저장 객체를 포함하는 객체나 해당 객체의 자식 객체가 정책 그룹에 속해 있는 경우입니다.

ONTAP 9.18.1부터 중첩된 QoS 정책을 사용할 수 있습니다. 이를 통해 SVM과 같은 포함 개체와 볼륨과 같은 자식 개체 모두에 정책 그룹을 할당할 수 있습니다. 멀티 테넌트 환경에서 중첩된 QoS 정책을 사용하면 관리자가 SVM 내의 볼륨과 Q트리에서 SVM의 QoS 제한을 세분화하고, 컴퓨팅 환경 전반에서 스토리지 리소스의 균형을 맞추는 동시에 미션 크리티컬 워크로드의 우선 순위를 지정할 수 있습니다.

다음 개체 쌍에 대해 중첩된 QoS 정책이 지원됩니다.

- SVM에 포함된 SVM 및 FlexVol 또는 FlexGroup 볼륨.
- 볼륨 내의 FlexVol 또는 FlexGroup 볼륨과 qtree.

중첩된 QoS 정책의 경우 적용 가능한 가장 제한적인 정책이 사용됩니다.

다음 표에는 제한 사항이 나열되어 있습니다.

다음을 할당하는 경우...	그러면 정책 그룹에 할당할 수 없습니다.
SVM을 정책 그룹으로 이동합니다	SVM에 포함된 모든 저장 객체. ONTAP 9.18.1을 실행 중인 경우 SVM에 포함된 FlexVol 및 FlexGroup 볼륨을 정책 그룹에 할당할 수 있습니다.
볼륨을 정책 그룹에	볼륨이나 자식 LUN이 포함된 SVM입니다. ONTAP 9.18.1 이상을 실행 중인 경우 볼륨이 포함된 SVM을 정책 그룹에 할당할 수 있습니다. 또한 FlexVol 또는 FlexGroup 볼륨의 qtree를 할당할 수 있습니다.
정책 그룹에 LUN을 지정합니다	LUN을 포함하는 볼륨 또는 SVM
파일을 정책 그룹에 저장합니다	파일이 포함된 볼륨 또는 SVM

단계

1. 적응형 QoS 정책 그룹을 생성합니다.

   'QOS adaptive-policy-group create-policy group_group_-vserver_SVM_-expected-IOPS_number_of_IOPS_/TB|GB-peak-IOPS_number_of_IOPS_/TB|GB-expected-IOPS-allocation-space|used-space-peak-peak-IOPS-allocation-space|used-space-space-absolute-min-64K_K_number_K_number_K_number_K_K_number|K_K_K_number|K_MB|K_

   에 대한 자세한 내용은 `qos adaptive-policy-group create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 9.5 이상에서 '-expected-IOPS-allocation' 및 '-block-size를 사용할 수 있다. 이러한 옵션은 ONTAP 9.4 이전 버전에서는 지원되지 않습니다.

다음 명령을 실행하면 300 IOPS/TB로 설정된 adpg-app1 Adaptive QoS 정책 그룹, 1,000 IOPS/TB로 설정된 -peak-IOPS, 사용된 공간으로 설정된 -peak-IOPS-allocation, 50 IOPS로 설정된 -absolute-min-IOPS 정책 그룹,

```
cluster1::> qos adaptive-policy-group create -policy group adpg-app1
-vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
-allocation used-space -absolute-min-iops 50iops
```

2. 적응형 QoS 정책 그룹을 볼륨에 적용합니다.

'volume create-vserver SVM-volume_volume_-aggregate_aggregate_-size_number_of_TB|GB-QoS-adaptive-policy-group_policy_group_'

에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령은 Adaptive QoS 정책 그룹 'adpg-app1'을 볼륨 'app1'에 적용합니다.

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

다음 명령은 새 볼륨 app4와 기존 볼륨 app5에 기본 적응형 QoS 정책 그룹 "extreme"을 적용합니다. 정책 그룹에 대해 정의된 처리량 상한은 볼륨 app4 및 app5에 개별적으로 적용됩니다.

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

ONTAP에서 적응형 정책 그룹 템플릿을 설정합니다

ONTAP 9.13.1부터 적응형 정책 그룹 템플릿을 사용하여 SVM 레벨에서 처리량 하한과 상한을 적용할 수 있습니다.

이 작업에 대해

- 적응형 정책 그룹 템플릿은 기본 정책입니다 `apg1`. 정책은 언제든지 수정할 수 있습니다. CLI 또는 ONTAP REST API에서만 설정할 수 있고 기존 SVM에만 적용할 수 있습니다.
- 적응형 정책 그룹 템플릿은 정책을 설정한 후 SVM에서 생성되거나 SVM으로 마이그레이션된 볼륨에만 영향을 줍니다. SVM의 기존 볼륨은 기존 상태를 유지합니다.

적응형 정책 그룹 템플릿을 비활성화하면 SVM의 볼륨은 기존 정책을 그대로 유지합니다. 이후에 SVM에서 생성하거나 SVM으로 마이그레이션한 볼륨만 지원 해제에 의해 영향을 받습니다.

- QoS 정책 그룹을 갖는 SVM에서는 적응형 정책 그룹 템플릿을 설정할 수 없습니다.
- 적응형 정책 그룹 템플릿은 AFF 플랫폼용으로 설계되었습니다. 적응형 정책 그룹 템플릿은 다른 플랫폼에 설정할 수 있지만 정책이 최소 처리량을 적용하지 않을 수 있습니다. 마찬가지로, FabricPool 최소 처리량을 지원하지 않는 애그리게이트의 SVM에 적응형 정책 그룹 템플릿 을 추가할 수도 있지만, 처리량 수준이 적용되지 않습니다.
- SVM이 MetroCluster 구성 또는 SnapMirror 관계에 있는 경우 적응형 정책 그룹 템플릿이 미러링된 SVM에 적용됩니다.

단계

1. SVM을 수정하여 적응형 정책 그룹 템플릿을 적용합니다.
   `vserver modify -qos-adaptive-policy-group-template apg1`
2. 정책이 설정되었는지 확인합니다.
   `vserver show -fields qos-adaptive-policy-group`

Unified Manager를 사용하여 클러스터 성능을 모니터링하고 관리하세요.

ONTAP Unified Manager를 사용하여 클러스터 성능 모니터링

Active IQ Unified Manager를 사용하면 가용성을 최대화하고 NetApp AFF 및 FAS 스토리지 인프라에 대한 제어를 유지하여 확장성, 지원 가능성, 성능 및 보안을 향상할 수 있습니다.

Active IQ Unified Manager은 시스템 상태를 지속적으로 모니터링하고 알림을 전송하므로 조직에서 IT 직원 리소스를 여유 있게 사용할 수 있습니다. 단일 대시보드에서 스토리지 상태를 즉시 확인하고 권장 조치를 통해 문제를 빠르게 해결할 수 있습니다.

알림을 검색, 모니터링 및 수신하여 스토리지를 능동적으로 관리하고 신속하게 문제를 해결할 수 있으므로 데이터 관리가 간소화됩니다. 단일 대시보드에서 페타바이트급 데이터를 모니터링하고 규모에 맞게 데이터를 관리할 수 있으므로 관리 효율성이 향상됩니다.

Active IQ Unified Manager를 사용하면 변화하는 비즈니스 요구사항에 대응할 수 있으므로 성능 데이터 및 고급 분석을 사용하여 성능을 최적화할 수 있습니다. 보고 기능을 사용하면 표준 보고서에 액세스하거나 맞춤형 운영 보고서를 작성하여 비즈니스의 특정 요구를 충족할 수 있습니다.

관련 링크:

- "Active IQ Unified Manager에 대해 자세히 알아보십시오"
- "VMware용 Active IQ Unified Manager를 시작하십시오"
- "Linus용 Active IQ Unified Manager를 시작하십시오"
- "Active IQ Unified Manager for Windows를 시작합니다"

ONTAP Active IQ Unified Manager 성능 모니터링 및 관리에 대해 알아보세요

기본적인 성능 모니터링 및 관리 작업을 설정하고 일반적인 성능 문제를 식별하고 해결할 수

있습니다.

다음과 같은 가정이 상황에 적용되는 경우 이 절차를 사용하여 클러스터 성능을 모니터링하고 관리할 수 있습니다.

- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.
- ONTAP 명령줄 인터페이스 외에 Active IQ Unified Manager(이전의 OnCommand Unified Manager)를 사용하여 시스템 상태 및 경고를 표시하고, 클러스터 성능을 모니터링하고, 근본 원인 분석을 수행하려고 합니다.
- ONTAP 명령줄 인터페이스를 사용하여 스토리지 QoS(서비스 품질)를 구성합니다. QoS는 다음을 통해서도 사용할 수 있습니다.
  - 시스템 관리자
  - ONTAP REST API를 참조하십시오
  - VMware vSphere용 ONTAP 툴
  - NetApp 서비스 수준 관리자(NSLM)
  - OnCommand Workflow Automation(WFA)
- Linux 또는 Windows 기반 설치 대신 가상 어플라이언스를 사용하여 Active IQ Unified Manager 설치하려고 합니다.
- 소프트웨어를 설치하는 데 DHCP가 아닌 정적 구성을 사용할 수 있습니다.
- 고급 권한 수준에서 ONTAP 명령에 액세스할 수 있습니다.
- "admin" 역할을 가진 클러스터 관리자입니다.

관련 정보

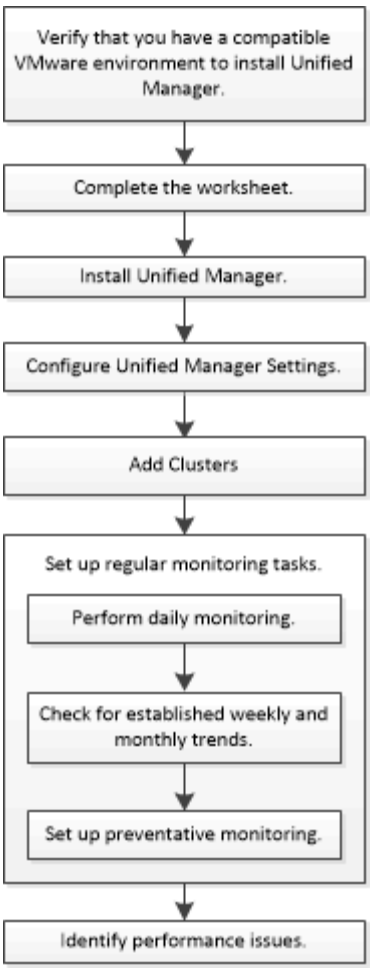
이러한 가정이 현재 상황에 맞지 않는 경우 다음 리소스를 참조하십시오.

- "Active IQ Unified Manager 9.8 설치"
- "시스템 관리"

성능을 모니터링합니다

ONTAP Active IQ Unified Manager 성능 모니터링 및 유지 관리 워크플로에 대해 알아보세요**.**

클러스터 성능을 모니터링하고 유지하려면 Active IQ Unified Manager 소프트웨어 설치, 기본 모니터링 작업 설정, 성능 문제 식별 및 필요에 따라 조정 작업이 필요합니다.



ONTAP Active IQ Unified Manager 에 대한 **VMware** 환경 요구 사항 확인

Active IQ Unified Manager를 성공적으로 설치하려면 VMware 환경이 필요한 요구 사항을 충족하는지 확인해야 합니다.

단계

1. VMware 인프라가 Unified Manager 설치를 위한 사이징 요구 사항을 충족하는지 확인합니다.
2. 로 이동합니다 "상호 운용성 매트릭스" 지원되는 다음 구성 요소 조합이 있는지 확인하려면 다음을 수행합니다.
    - ONTAP 버전입니다
    - ESXi 운영 체제 버전입니다
    - VMware vCenter Server 버전입니다
    - VMware Tools 버전입니다
    - 브라우저 유형 및 버전

    상호 운용성 매트릭스에는 Unified Manager에서 지원되는 구성이 나와 있습니다.
3. 선택한 설정의 설정 이름을 클릭합니다.

    해당 구성에 대한 세부 정보가 구성 세부 정보 창에 표시됩니다.

4. 다음 탭의 정보를 검토합니다.
   - 참고

     에는 사용자의 구성에 특정한 중요한 경고 및 정보가 나와 있습니다.

   - 정책 및 지침

     모든 구성에 대한 일반 지침을 제공합니다.

ONTAP Active IQ Unified Manager 워크시트

Active IQ Unified Manager를 설치, 구성 및 연결하기 전에 사용자 환경에 대한 특정 정보를 즉시 사용할 수 있어야 합니다. 워크시트에 정보를 기록할 수 있습니다.

Unified Manager 설치 정보

소프트웨어가 구축된 가상 머신입니다	귀사의 가치
ESXi 서버 IP 주소입니다	
호스트 정규화된 도메인 이름입니다	
호스트 IP 주소입니다	
네트워크 마스크	
게이트웨이 IP 주소입니다	
기본 DNS 주소입니다	
보조 DNS 주소입니다	
도메인 검색	
유지보수 사용자 이름입니다	
유지보수 사용자 암호입니다	

Unified Manager 구성 정보

설정	귀사의 가치
유지보수 사용자 이메일 주소	
NTP 서버	

SMTP 서버 호스트 이름 또는 IP 주소입니다	
SMTP 사용자 이름입니다	
SMTP 암호	
SMTP 기본 포트	25(기본값)
알림 알림이 전송되는 이메일입니다	
LDAP 바인딩 고유 이름입니다	
LDAP 바인딩 암호입니다	
Active Directory 관리자 이름입니다	
Active Directory 암호입니다	
인증 서버 기본 고유 이름입니다	
인증 서버 호스트 이름 또는 IP 주소입니다	

클러스터 정보

Unified Manager의 각 클러스터에 대해 다음 정보를 수집합니다.

클러스터 1/N	귀사의 가치
호스트 이름 또는 클러스터 관리 IP 주소입니다	
ONTAP 관리자 사용자 이름입니다 관리자는 "admin" 역할을 할당해야 합니다.	
ONTAP 관리자 암호입니다	
프로토콜(HTTP 또는 HTTPS)	

관련 정보

"관리자 인증 및 RBAC"

Active IQ Unified Manager를 설치합니다

ONTAP Active IQ Unified Manager 다운로드하고 배포하세요.

소프트웨어를 설치하려면 가상 어플라이언스(VA) 설치 파일을 다운로드한 다음 VMware vSphere Client를 사용하여 VMware ESXi 서버에 파일을 구축해야 합니다. VA는 OVA 파일에서 사용할 수 있습니다.

단계

1. NetApp Support 사이트 소프트웨어 다운로드 * 페이지로 이동하여 Active IQ Unified Manager을 찾으십시오.

   https://mysupport.netapp.com/products/index.html

2. Select Platform * (플랫폼 선택 *) 드롭다운 메뉴에서 * VMware vSphere * 를 선택하고 * Go! * (이동! *)를 클릭합니다
3. VMware vSphere Client에서 액세스할 수 있는 로컬 또는 네트워크 위치에 ""OVA"" 파일을 저장합니다.
4. VMware vSphere Client에서 * File * > * Deploy OVF Template * 을 클릭합니다.
5. ""OVA" 파일을 찾아 마법사를 사용하여 ESXi 서버에 가상 어플라이언스를 구축합니다.

   마법사의 * 속성 * 탭을 사용하여 정적 구성 정보를 입력할 수 있습니다.

6. VM의 전원을 켭니다.
7. 초기 부팅 프로세스를 보려면 * Console * 탭을 클릭합니다.
8. 프롬프트에 따라 VM에 VMware Tools를 설치합니다.
9. 시간대를 구성합니다.
10. 유지보수 사용자 이름과 암호를 입력합니다.
11. VM 콘솔에 표시된 URL로 이동합니다.

초기 ONTAP Active IQ Unified Manager 설정 구성

Active IQ Unified Manager 초기 설정 대화 상자는 웹 UI에 처음 액세스할 때 나타나며, 이 대화 상자에서 일부 초기 설정을 구성하고 클러스터를 추가할 수 있습니다.

단계

1. 기본 AutoSupport 사용 설정을 적용합니다.
2. NTP 서버 세부 정보, 유지보수 사용자 이메일 주소, SMTP 서버 호스트 이름 및 추가 SMTP 옵션을 입력한 다음 * 저장 * 을 클릭합니다.

작업을 마친 후

초기 설정이 완료되면 클러스터 세부 정보를 추가할 수 있는 클러스터 데이터 소스 페이지가 표시됩니다.

Active IQ Unified Manager 에서 모니터링할 ONTAP 클러스터를 지정합니다.

클러스터를 모니터링하고, 클러스터 검색 상태를 확인하고, 성능을 모니터링하려면 Active IQ Unified Manager 서버에 클러스터를 추가해야 합니다.

시작하기 전에

- 다음 정보가 있어야 합니다.
  - 호스트 이름 또는 클러스터 관리 IP 주소입니다

    호스트 이름은 Unified Manager에서 클러스터에 연결하는 데 사용하는 FQDN(정규화된 도메인 이름) 또는 짧은 이름입니다. 이 호스트 이름은 클러스터 관리 IP 주소로 확인되어야 합니다.

  클러스터 관리 IP 주소는 관리 스토리지 가상 시스템(SVM)의 클러스터 관리 LIF여야 합니다. 노드 관리 LIF를 사용하면 작업이 실패합니다.

  - ONTAP 관리자 사용자 이름 및 암호
  - 클러스터에서 구성할 수 있는 프로토콜 유형(HTTP 또는 HTTPS) 및 클러스터의 포트 번호입니다
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- ONTAP 관리자는 ONTAPI 및 SSH 관리자 역할이 있어야 합니다.
- Unified Manager FQDN이 ONTAP을 ping할 수 있어야 합니다.

  ONTAP 명령 'ping-node_node_name_-destination_Unified_Manager_FQDN_'을 사용하여 이를 확인할 수 있습니다.

이 작업에 대해

MetroCluster 구성의 경우 로컬 클러스터와 원격 클러스터를 모두 추가해야 하며 클러스터가 올바르게 구성되어야 합니다.

단계

1. 구성 * > * 클러스터 데이터 소스 * 를 클릭합니다.
2. 클러스터 페이지에서 * 추가 * 를 클릭합니다.
3. 클러스터 추가 * 대화 상자에서 클러스터의 호스트 이름 또는 IP 주소(IPv4 또는 IPv6), 사용자 이름, 암호, 통신 프로토콜 및 포트 번호와 같은 필수 값을 지정합니다.

   기본적으로 HTTPS 프로토콜이 선택됩니다.

   클러스터 관리 IP 주소를 IPv6에서 IPv4로, 또는 IPv4에서 IPv6로 변경할 수 있습니다. 새 IP 주소는 다음 모니터링 주기가 완료된 후 클러스터 그리드 및 클러스터 구성 페이지에 반영됩니다.

4. 추가 * 를 클릭합니다.
5. HTTPS를 선택한 경우 다음 단계를 수행하십시오.
   a. 호스트 인증 * 대화 상자에서 * 인증서 보기 * 를 클릭하여 클러스터에 대한 인증서 정보를 봅니다.
   b. 예 * 를 클릭합니다.

      Unified Manager는 처음에 클러스터가 추가된 경우에만 인증서를 검사하지만 ONTAP에 대한 각 API 호출에서는 인증서를 확인하지 않습니다.

   인증서가 만료된 경우 클러스터를 추가할 수 없습니다. SSL 인증서를 갱신한 다음 클러스터를 추가해야 합니다.

6. * 선택 사항 *: 클러스터 검색 상태 보기:

a. Cluster Setup * 페이지에서 클러스터 검색 상태를 검토합니다.

기본 모니터링 간격 약 15분이 지나면 클러스터가 Unified Manager 데이터베이스에 추가됩니다.

기본 모니터링 작업을 설정합니다

매일 **ONTAP Active IQ Unified Manager** 모니터링 수행

매일 모니터링을 수행하여 즉각적인 성능 문제가 발생하지 않도록 주의할 수 있습니다.

단계

1. Active IQ Unified Manager UI에서 * 이벤트 인벤토리 * 페이지로 이동하여 현재 이벤트와 사용되지 않는 이벤트를 모두 봅니다.
2. View* 옵션에서 "활성 성능 이벤트"를 선택하고 필요한 조치를 결정합니다.

ONTAP Active IQ Unified Manager 주간 및 월간 성능 추세를 사용하여 성능 문제를 식별합니다.

성능 추세를 파악하면 볼륨 지연 시간을 분석하여 클러스터가 과도하게 사용되고 있는지 또는 제대로 사용되고 있지 않는지를 파악하는 데 도움이 됩니다. 유사한 단계를 사용하여 CPU, 네트워크 또는 기타 시스템 병목 현상을 식별할 수 있습니다.

단계

1. 사용량이 적거나 과용되고 있다고 의심되는 볼륨을 찾습니다.
2. 볼륨 세부 정보 * 탭에서 * 30 d * 를 클릭하여 기록 데이터를 표시합니다.
3. "데이터 구분 기준" 드롭다운 메뉴에서 * 지연 시간 * 을 선택한 다음 * 제출 * 을 클릭합니다.
4. 클러스터 구성 요소 비교 차트에서 * Aggregate * 를 선택 취소한 다음 클러스터 지연 시간을 볼륨 지연 시간 차트와 비교합니다.
5. 클러스터 구성 요소 비교 차트에서 * Aggregate * 를 선택하고 다른 모든 구성 요소를 선택 취소한 다음, 애그리게이트 지연 시간과 볼륨 지연 시간 차트를 비교합니다.
6. 읽기/쓰기 지연 시간 차트를 볼륨 지연 시간 차트와 비교합니다.
7. 클라이언트 애플리케이션 로드로 인해 워크로드 경합이 발생했는지 확인하고 필요에 따라 워크로드를 재조정합니다.
8. Aggregate가 초과 사용되고 있는지 확인하고 필요에 따라 경합 및 워크로드 균형을 조정합니다.

ONTAP Active IQ Unified Manager 성능 임계값을 설정합니다.

성능 임계값을 설정하여 중요한 성능 문제를 모니터링할 수 있습니다. 사용자 정의 임계값은 시스템이 정의된 임계값에 접근하거나 이를 초과할 경우 경고 또는 중요 이벤트 알림을 트리거합니다.

단계

1. 경고 및 위험 이벤트 임계값을 생성합니다.
   a. 구성 * > * 성능 임계값 * 을 선택합니다.
   b. Create * 를 클릭합니다.

c. 객체 유형을 선택하고 정책의 이름과 설명을 지정합니다.

d. 개체 카운터 조건을 선택하고 경고 및 위험 이벤트를 정의하는 제한 값을 지정합니다.

e. 이벤트를 전송할 때 제한 값을 위반해야 하는 기간을 선택한 다음 * 저장 * 을 클릭합니다.

2. 스토리지 객체에 임계값 정책을 할당합니다.

a. 이전에 선택한 것과 동일한 클러스터 객체 유형에 대한 인벤토리 페이지로 이동하여 보기 옵션에서 * 성능 * 을 선택합니다.

b. 임계값 정책을 할당할 개체를 선택한 다음 * 임계값 정책 할당 * 을 클릭합니다.

c. 이전에 생성한 정책을 선택한 다음 * 정책 할당 * 을 클릭합니다.

예

사용자 정의 임계값을 설정하여 중요한 성능 문제를 확인할 수 있습니다. 예를 들어, Microsoft Exchange Server가 있는데 볼륨 지연 시간이 20밀리초를 초과하면 오류가 발생하는 경우 경고 임계값을 12밀리초로 설정하고 임계치를 15밀리초로 설정할 수 있습니다. 이 임계값 설정을 사용하면 볼륨 지연 시간이 제한을 초과할 때 알림을 받을 수 있습니다.

ONTAP Active IQ Unified Manager 알림 추가

이벤트는 Active IQ Unified Manager 미리 정의된 조건이 발생하거나 성능 카운터 값이 임계값을 초과할 때 자동으로 생성하는 알림입니다. 이벤트는 모니터링 중인 클러스터의 성능 문제를 파악하는 데 도움이 됩니다.

특정 이벤트가 생성되면 알림을 받도록 알림을 구성할 수 있습니다. 단일 리소스, 리소스 그룹 또는 특정 심각도 유형의 이벤트에 대한 알림을 구성할 수 있습니다. 알림 빈도를 지정하고 스크립트를 경고와 연결할 수 있습니다.

시작하기 전에

- Active IQ Unified Manager 서버가 이러한 설정을 사용하여 이벤트가 생성될 때 사용자에게 알림을 보낼 수 있도록 하려면 사용자 e-메일 주소, SMTP 서버 및 SNMP 트랩 호스트와 같은 알림 설정을 구성해야 합니다.
- 알림을 트리거할 리소스 및 이벤트와 알림을 보낼 사용자의 사용자 이름 또는 이메일 주소를 알고 있어야 합니다.
- 이벤트를 기반으로 스크립트를 실행하려면 스크립트 페이지를 사용하여 Unified Manager에 스크립트를 추가해야 합니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이 작업에 대해

여기서 설명하는 대로 알림 설정 페이지에서 알림을 생성할 뿐만 아니라 이벤트를 수신한 후 이벤트 세부 정보 페이지에서 직접 알림을 생성할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.
2. Alert Setup * 페이지에서 * Add * 를 클릭합니다.
3. 경고 추가 * 대화 상자에서 * 이름 * 을 클릭하고 경고의 이름과 설명을 입력합니다.

4. 리소스 * 를 클릭하고 경고에 포함되거나 제외될 리소스를 선택합니다.

   이름 포함 * 필드에서 텍스트 문자열을 지정하여 리소스 그룹을 선택하여 필터를 설정할 수 있습니다. 지정한 텍스트 문자열을 기준으로 사용 가능한 자원 목록에는 필터 규칙과 일치하는 자원만 표시됩니다. 지정하는 텍스트 문자열은 대/소문자를 구분합니다.

   자원이 지정한 포함 및 제외 규칙을 모두 준수하는 경우 제외 규칙이 포함 규칙보다 우선하며 제외된 리소스와 관련된 이벤트에 대해서는 알림이 생성되지 않습니다.

5. 이벤트 * 를 클릭하고 알림을 트리거할 이벤트 이름 또는 이벤트 심각도 유형을 기반으로 이벤트를 선택합니다.

   둘 이상의 이벤트를 선택하려면 Ctrl 키를 누른 상태에서 원하는 항목을 선택합니다.

6. Actions * 를 클릭하고 알릴 사용자를 선택하고, 알림 빈도를 선택하고, SNMP 트랩을 트랩 수신기로 전송할지 여부를 선택한 다음, 경고가 생성될 때 실행할 스크립트를 할당합니다.

   사용자에 대해 지정된 전자 메일 주소를 수정하고 편집을 위해 알림을 다시 열면 수정된 전자 메일 주소가 이전에 선택한 사용자에게 더 이상 매핑되지 않으므로 이름 필드가 비어 있습니다. 또한 사용자 페이지에서 선택한 사용자의 전자 메일 주소를 수정한 경우 선택한 사용자에 대해 수정된 전자 메일 주소가 업데이트되지 않습니다.

   SNMP 트랩을 통해 사용자에게 알리도록 선택할 수도 있습니다.

7. 저장 * 을 클릭합니다.

알림 추가 예

이 예제에서는 다음 요구 사항을 충족하는 알림을 생성하는 방법을 보여 줍니다.

- 알림 이름: 상태 테스트
- 리소스: 이름에 "abc"가 포함된 모든 볼륨을 포함하며 이름에 "xyz"가 포함된 모든 볼륨을 제외합니다.
- 이벤트: 모든 중요한 상태 이벤트를 포함합니다
- 작업: "sample@domain.com", "테스트" 스크립트를 포함하며 사용자에게 15분마다 알림을 받아야 합니다

경고 추가 대화 상자에서 다음 단계를 수행합니다.

1. 이름 * 을 클릭하고 * 알림 이름 * 필드에 '상태 테스트'를 입력합니다.
2. 리소스 * 를 클릭하고 포함 탭의 드롭다운 목록에서 * 볼륨 * 을 선택합니다.
   a. 이름에 abc가 포함된 볼륨을 표시하려면 * Name Contains * 필드에 abc를 입력합니다.
   b. 를 선택합니다[All Volumes whose name contains 'abc']Available Resources 영역에서 + * 를 선택한 다음 Selected Resources 영역으로 이동합니다.
   c. 제외 * 를 클릭하고 * 이름 포함 * 필드에 'xyz'를 입력한 다음 * 추가 * 를 클릭합니다.
3. 이벤트 * 를 클릭하고 이벤트 심각도 필드에서 * 긴급 * 을 선택합니다.
4. Matching Events 영역에서 * All Critical Events * 를 선택하고 Selected Events 영역으로 이동합니다.
5. [동작] * 을 클릭하고 다음 사용자에게 알림 필드에 'ample@domain.com'을 입력합니다.
6. 15분마다 사용자에게 알리려면 * 15분마다 알림 * 을 선택합니다.

지정된 시간 동안 수신자에게 반복적으로 알림을 보내도록 알림을 구성할 수 있습니다. 알림에 대해 이벤트 알림이 활성화되는 시간을 결정해야 합니다.

7. 실행할 스크립트 선택 메뉴에서 * 테스트 * 스크립트를 선택합니다.
8. 저장 * 을 클릭합니다.

ONTAP Active IQ Unified Manager 경고 설정 구성

Active IQ Unified Manager에서 알림을 트리거할 이벤트, 해당 알림의 e-메일 받는 사람 및 알림 빈도를 지정할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

이 작업에 대해

다음 유형의 성능 이벤트에 대해 고유한 알림 설정을 구성할 수 있습니다.

- 사용자 정의 임계값 위반으로 인해 발생하는 중요 이벤트입니다
- 경고 이벤트는 사용자 정의 임계값, 시스템 정의 임계값 또는 동적 임계값 위반으로 인해 발생합니다

기본적으로 모든 새 이벤트에 대해 Unified Manager 관리 사용자에게 이메일 경고가 전송됩니다. 해당 사용자의 전자 메일 주소를 추가하여 다른 사용자에게 전자 메일 알림을 보낼 수 있습니다.

특정 유형의 이벤트에 대해 알림이 전송되지 않도록 하려면 이벤트 범주의 모든 확인란의 선택을 해제해야 합니다. 이 작업을 수행해도 이벤트가 사용자 인터페이스에 나타나지 않습니다.

단계

1. 왼쪽 탐색 창에서 * Storage Management * > * Alert Setup * 을 선택합니다.

   경고 설정 페이지가 표시됩니다.

2. 추가 * 를 클릭하고 각 이벤트 유형에 적절한 설정을 구성합니다.

   여러 사용자에게 전자 메일 알림을 보내려면 각 전자 메일 주소 사이에 쉼표를 입력합니다.

3. 저장 * 을 클릭합니다.

ONTAP Active IQ Unified Manager 의 성능 문제 식별

성능 이벤트가 발생하면 Active IQ Unified Manager에서 문제의 원인을 찾아 다른 도구를 사용하여 문제를 해결할 수 있습니다. 매일 모니터링하는 동안 이벤트에 대한 이메일 알림을 받거나 이벤트를 알릴 수 있습니다.

단계

1. e-메일 알림의 링크를 클릭하면 성능 이벤트가 있는 스토리지 객체로 직접 이동됩니다.

만약…	그러면…

이벤트에 대한 이메일 알림을 받습니다	링크를 클릭하여 이벤트 세부 정보 페이지로 직접 이동합니다.
이벤트 인벤토리 페이지를 분석하는 동안 이벤트를 확인합니다	이벤트 세부 정보 페이지로 직접 이동할 이벤트를 선택합니다.

2. 이벤트가 시스템 정의 임계값을 초과한 경우 UI에서 제안된 작업을 수행하여 문제를 해결하십시오.
3. 이벤트가 사용자 정의 임계값을 초과한 경우 이벤트를 분석하여 조치를 취해야 하는지 결정합니다.
4. 문제가 지속되면 다음 설정을 확인하십시오.
   - 스토리지 시스템의 프로토콜 설정입니다
   - 이더넷 또는 패브릭 스위치의 네트워크 설정
   - 스토리지 시스템의 네트워크 설정입니다
   - 스토리지 시스템의 디스크 레이아웃 및 애그리게이트 메트릭
5. 문제가 지속되면 기술 지원 팀에 지원을 요청하십시오.

ONTAP Active IQ Digital Advisor 사용하여 시스템 성능을 확인하세요.

AutoSupport 툴을 NetApp으로 전송하는 모든 ONTAP 시스템에서 포괄적인 성능 및 용량 데이터를 볼 수 있습니다. Digital Advisor는 System Manager에서 볼 수 있는 것보다 더 오랜 기간 동안 시스템 성능을 표시합니다.

CPU 활용률, 지연 시간, IOPS, 프로토콜별 IOPS, 네트워크 처리량을 보여주는 그래프를 볼 수 있습니다. 다른 도구에서 분석할 수 있도록 이 데이터를 .csv 형식으로 다운로드할 수도 있습니다.

Digital Advisor는 성능 데이터 외에 워크로드별로 스토리지 효율성을 보여 주고 이러한 효율성을 해당 유형의 워크로드에 대해 예상되는 효율성과 비교할 수 있습니다. 용량 추세를 보고 특정 기간에 추가해야 할 추가 스토리지 양을 예측할 수 있습니다.

- 스토리지 효율성은 기본 대시보드 왼쪽의 고객, 클러스터 및 노드 레벨에서 사용할 수 있습니다.
- 성능은 메인 대시보드 왼쪽의 클러스터 및 노드 레벨에서 사용할 수 있습니다.

관련 정보

- "Digital Advisor 설명서"
- "Digital Advisor 비디오 재생 목록"
- "Digital Advisor Web Portal을 참조하십시오"

ONTAP Data Infrastructure Insights를 사용하여 클러스터 성능 모니터링

NetApp Data Infrastructure Insights는 전체 인프라에 대한 가시성을 제공하는 모니터링

도구입니다. Data Infrastructure Insights를 사용하면 퍼블릭 클라우드와 프라이빗 데이터 센터를 포함한 모든 리소스를 모니터링하고, 문제를 해결하고, 최적화할 수 있습니다.

모든 리소스를 모니터링, 문제 해결 및 최적화합니다

데이터 인프라 인사이트를 활용하면 문제 해결에 걸리는 시간을 크게 줄이고 최종 사용자에게 영향을 미치지 않도록 방지할 수 있습니다. 또한 클라우드 인프라 비용을 줄일 수 있습니다. 실행 가능한 인텔리전스로 데이터를 보호하여 내부자 위협에 대한 노출을 줄입니다.

Data Infrastructure Insights를 사용하면 퍼블릭 클라우드부터 데이터 센터까지 전체 하이브리드 인프라에 대한 가시성을 한곳에서 확보할 수 있습니다. 필요에 따라 맞춤 구성할 수 있는 관련 대시보드를 즉시 만들 수 있습니다. 조직의 요구 사항에 따라 구체적이고 관련 있는 조건부 경고를 만들 수도 있습니다.

고급 이상 징후 탐지 기능을 통해 문제가 발생하기 전에 사전에 해결할 수 있습니다. 리소스 경합 및 성능 저하를 자동으로 확인하여 영향을 받는 워크로드를 신속하게 복원할 수 있습니다. 스택 내 여러 구성 요소 간의 관계를 자동으로 계층 구조로 만들어 문제 해결 작업을 더욱 빠르게 수행할 수 있습니다.

환경 전반에서 사용되지 않거나 버려진 리소스를 식별할 수 있으므로, 인프라의 크기를 적절하게 조정하고 전체 비용을 최적화할 기회를 찾을 수 있습니다.

데이터 인프라 인사이트는 Kubernetes 아키텍처를 이해하기 위해 시스템 토폴로지를 시각화합니다. 문제가 있는 노드를 비롯하여 Kubernetes 클러스터의 상태를 모니터링하고 문제가 발생하면 확장할 수 있습니다.

Data Infrastructure Insights는 고급 머신 러닝과 이상 탐지를 통해 조직 데이터가 악의적이거나 손상된 사용자에 의해 오용되는 것을 방지하고 내부 위협에 대한 실행 가능한 정보를 제공합니다.

Data Infrastructure Insights를 사용하면 Kubernetes 메트릭을 시각화하여 포드, 노드, 클러스터 간의 관계를 완벽하게 이해할 수 있습니다. 현재 처리 중인 로드뿐만 아니라 클러스터 또는 작업 포드의 상태를 평가할 수 있으므로 K8S 클러스터의 명령을 수행하고 배포 상태와 비용을 모두 제어할 수 있습니다.

관련 링크

- "데이터 인프라 인사이트 시작하기"

로깅 감사

ONTAP 감사 로깅 구현에 대해 자세히 알아보십시오

감사 로그에 기록된 관리 활동은 표준 AutoSupport 보고서에 포함되고, 특정 로깅 활동은 EMS 메시지에 포함됩니다. 또한 감사 로그를 지정한 대상으로 전송할 수 있으며, ONTAP CLI 또는 웹 브라우저를 사용하여 감사 로그 파일을 표시할 수 있습니다.

ONTAP 9.11.1부터 시스템 관리자를 사용하여 감사 로그 내용을 표시할 수 있습니다.

ONTAP 9.12.1부터 ONTAP는 감사 로그에 대한 변조 경고를 제공합니다. ONTAP는 매일 백그라운드 작업을 실행하여 audit.log 파일의 변조를 확인하고 변경 또는 변조된 로그 파일이 발견되면 EMS 경고를 보냅니다.

ONTAP 9.17.1부터 ONTAP 9.16.1 P4 이상 9.16.1 패치 릴리스에서는"피어링된 클러스터에서 시작된 원격 관리 활동은 클러스터 간 작업을 사용하여 기록될 수도 있습니다.". 이러한 활동에는 다른 클러스터에서 발생하는 사용자 중심 작업과 내부 작업이 포함됩니다

ONTAP 에 기록된 관리 활동

ONTAP 클러스터에서 수행되는 관리 활동을 기록합니다. 여기에는 발행된 요청, 요청을 트리거한 사용자, 사용자의 액세스 방법, 요청 시간 등이 포함됩니다.

관리 활동은 다음 유형 중 하나일 수 있습니다.

- **SET** 요청:
  - 이러한 요청은 일반적으로 표시되지 않는 명령이나 작업에 적용됩니다.
  - 예를 들어, 'create', 'modify', 'delete' 명령을 실행하면 이러한 요청이 실행됩니다.
  - SET 요청은 기본적으로 기록됩니다.
- **GET** 요청:
  - 이러한 요청은 정보를 검색하여 관리 인터페이스에 표시합니다.
  - 예를 들어 'show' 명령을 실행하면 이러한 요청이 실행됩니다.
  - GET 요청은 기본적으로 기록되지 않지만 ONTAP CLI에서 전송된 GET 요청이 기록되는지 여부를 제어할 수 있습니다. (`-cliget`), ONTAP API에서 (`-ontapiget`), 또는 ONTAP REST API에서 (`-httpget`)이 파일에 기록됩니다.

감사 로그 기록 및 회전

ONTAP 기록 관리 활동 `/mroot/etc/log/mlog/audit.log` 노드 파일입니다. CLI 명령용 세 가지 셸(클러스터셸, 노드셸, 비대화형 시스템셸)과 API 명령이 여기에 기록됩니다. 대화형 시스템셸 명령은 기록되지 않습니다. 감사 로그에는 클러스터의 모든 노드가 동기화되었는지 여부를 보여주는 타임스탬프가 포함됩니다.

Audit.log 파일은 AutoSupport Tool에 의해 지정된 수신인에게 전송된다. 또한 Splunk 또는 syslog 서버와 같이 지정한 외부 대상에 콘텐츠를 안전하게 전달할 수 있습니다.

Audit.log 파일은 매일 순환한다. 회전은 크기가 100MB에 도달하고 이전 48개 사본이 보존될 때도 발생합니다(최대 총 49개 파일). 감사 파일이 매일 회전을 수행하면 EMS 메시지가 생성되지 않습니다. 파일 크기 제한이 초과되어 Audit 파일이 회전하면 EMS 메시지가 발생한다.

GET 감사를 활성화할 때, 빠른 로그 순환으로 인한 데이터 손실을 방지하기 위해 로그 전달을 구성하는 것이 좋습니다. 자세한 내용은 다음 기술 자료 문서를 참조하세요. "감사 로그 전달 활성화" .

ONTAP 감사 로깅의 변경 사항에 대해 알아봅니다

ONTAP 9부터는 Command-history.log 파일이 audit.log로 대체되고, mgwd.log 파일은 더 이상 Audit 정보를 포함하지 않는다. ONTAP 9로 업그레이드하는 경우 기존 파일과 해당 콘텐츠를 참조하는 스크립트나 도구를 검토해야 합니다.

ONTAP 9로 업그레이드한 후 기존 명령어 이력.log 파일을 보존한다. 새 감사.로그 파일이 (작성됨) 회전되면 해당 파일이 삭제(삭제)됩니다.

명령어-히스토리.로그 파일을 체크하는 툴과 스크립트는 업그레이드 시 명령어-히스토리.로그부터 audit.log로의 소프트 링크가 생성되기 때문에 계속 동작할 수 있다. 그러나 mgwd.log 파일을 확인하는 도구와 스크립트는 해당 파일에 더 이상 감사 정보가 없기 때문에 실패합니다.

또한 ONTAP 9 이상의 감사 로그에는 유용하지 않고 불필요한 로깅 활동을 유발하기 때문에 다음 항목이 더 이상 포함되지 않습니다.

- ONTAP에서 실행되는 내부 명령(즉, username=root)
- 명령 별칭(해당 명령이 가리키는 명령과는 별개)

ONTAP 9부터는 TCP 및 TLS 프로토콜을 사용하여 감사 로그를 외부 대상으로 안전하게 전송할 수 있습니다.

ONTAP 감사 로그 내용을 표시합니다

ONTAP CLI, System Manager 또는 웹 브라우저를 사용하여 클러스터의 `/mroot/etc/log/mlog/audit.log' 파일의 내용을 표시할 수 있습니다.

클러스터의 로그 파일 항목은 다음과 같습니다.

시간
: 로그 항목 타임 스탬프입니다.

응용 프로그램
: 클러스터에 연결하는 데 사용되는 애플리케이션입니다. 가능한 값의 예는 `internal` , `console`, `ssh`, `http`, , `ontapi`, 입니다. `snmp` `rsh`, , , `telnet` 및 `service-processor`.

사용자
: 원격 사용자의 사용자 이름입니다.

상태
: 감사 요청의 현재 상태는, `pending` 또는 일 수 있습니다 `success`. `error`

메시지
: 명령 상태에 대한 오류 또는 추가 정보를 포함할 수 있는 선택적 필드입니다.

세션 **ID**입니다
: 요청이 수신된 세션 ID입니다. 각 SSH_SESSION_에는 세션 ID가 할당되고 각 HTTP, ONTAPI 또는 SNMP_REQUEST_에는 고유한 세션 ID가 할당됩니다.

스토리지 **VM**
: 사용자가 연결하는 데 사용되는 SVM.

범위
: 데이터 스토리지 VM에 요청이 있으면 'VM'을 표시하고, 그렇지 않으면 '클러스터'를 표시합니다.

명령 **ID**입니다
: CLI 세션에서 수신한 각 명령의 ID입니다. 이렇게 하면 요청과 응답을 서로 연관시킬 수 있습니다. ZAPI, HTTP 및 SNMP 요청에는 명령 ID가 없습니다.

웹 브라우저에서 ONTAP CLI의 클러스터의 로그 항목을 표시하고 시스템 관리자에서 ONTAP 9.11.1로 시작할 수 있습니다.

시스템 관리자

- 인벤토리를 표시하려면 * 이벤트 및 작업 > 감사 로그 * 를 선택합니다. + 각 열에는 필터링, 정렬, 검색, 표시 및 인벤토리 범주를 제어하는 컨트롤이 있습니다. 재고 세부 정보는 Excel 통합 문서로 다운로드할 수 있습니다.
- 필터를 설정하려면 오른쪽 위에 있는 * Filter * (필터 *) 버튼을 클릭하고 원하는 필드를 선택합니다. +세션 ID 링크를 클릭하여 장애가 발생한 세션에서 실행된 모든 명령을 볼 수도 있습니다.

CLI를 참조하십시오

클러스터의 여러 노드에서 병합된 감사 항목을 표시하려면 + 를 입력합니다
`security audit log show <[parameters]>`

명령을 사용하여 개별 노드에 대한 감사 항목을 표시하거나 클러스터의 여러 노드에서 병합할 수 `security audit log show` 있습니다. 웹 브라우저를 사용하여 단일 노드에 디렉토리의 컨텐츠를 표시할 수도 `/mroot/etc/log/mlog` 있습니다. 에 대한 자세한 내용은 `security audit log show` "ONTAP 명령 참조입니다"을 참조하십시오.

웹 브라우저

웹 브라우저를 사용하여 단일 노드에 디렉토리의 컨텐츠를 표시할 수 `/mroot/etc/log/mlog` 있습니다. "웹 브라우저를 사용하여 노드의 로그, 코어 덤프 및 MIB 파일에 액세스하는 방법에 대해 알아봅니다"..

ONTAP 감사 가져오기 요청 설정을 관리합니다

설정된 요청이 기본적으로 기록되지만 GET 요청은 기록되지 않습니다. 그러나 ONTAP HTML('-HttpGet'), ONTAP CLI('-cliget') 또는 ONTAP API('-ontapiget')에서 보낸 GET 요청이 파일에 기록되는지 여부를 제어할 수 있습니다.

시스템 관리자에서 감사 로깅 설정을 ONTAP CLI에서 수정할 수 있으며 ONTAP 9.11.1부터 시작할 수 있습니다.

시스템 관리자

1. 이벤트 및 작업 > 감사 로그 * 를 선택합니다.
2. 오른쪽 상단 모서리를 클릭한 다음 추가 또는 제거할 요청을 선택합니다.

CLI를 참조하십시오

- ONTAP CLI 또는 API의 GET 요청을 감사 로그(audit.log 파일)에 기록하도록 지정하려면 기본 설정 요청 외에 + '보안 감사 수정[-cliget{on|off}][-HttpGet{ on|off}][-ontapiget{on|off}]'을 입력합니다
- 현재 설정을 표시하려면 + 보안 감사 표시 를 입력합니다

에 대한 자세한 내용은 `security audit show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 클러스터 간 감사 활성화

ONTAP 9.17.1부터, 그리고 ONTAP 9.16.1 P4 및 이후 9.16.1 패치 릴리스부터 ONTAP 에서 클러스터 간 감사를 활성화하여 피어링된 클러스터에서 시작된 작업을 기록할 수 있습니다. 이 원격 감사는 여러 ONTAP 클러스터가 상호 작용하는 환경에서 특히 유용하며, 원격 작업에 대한

추적성과 책임 소재를 제공합니다.

클러스터 간 감사는 사용자가 시작한 GET(읽기) 또는 SET(생성/수정/제거) 작업을 구분할 수 있습니다. 기본적으로 대상 클러스터에서는 사용자가 시작한 SET 작업만 감사됩니다. GET 또는 `show` CLI에서 명령을 실행하면 요청이 클러스터 간인지 여부에 관계없이 기본적으로 감사되지 않습니다.

시작하기 전에

- 당신은 있어야합니다 `advanced` 레벨 권한
- 클러스터는 다른 클러스터와 피어링되어야 하며, 두 클러스터 모두 ONTAP 9.16.1 P4 이상을 실행해야 합니다.

> 일부 노드만 ONTAP 9.16.1 P4 이상으로 업그레이드된 환경에서는 업그레이드된 버전을 실행하는 노드에서만 감사 로깅이 실행됩니다. 일관된 감사 동작을 보장하려면 모든 노드를 지원되는 버전으로 업그레이드하는 것이 좋습니다.

클러스터 간 감사 활성화 또는 비활성화

단계

1. 클러스터에서 크로스 클러스터 감사를 활성화(또는 비활성화)하려면 다음을 설정합니다. `cluster-peer` 매개변수 `on` 또는 `off` :

```
security audit modify -cluster-peer {on|off}
```

2. 현재 감사 상태를 확인하여 클러스터 피어 설정이 활성화 또는 비활성화되었는지 확인하세요.

```
security audit show
```

응답:

```
    Audit Setting State
    ------------- -----
         CLI GET: off
        HTTP GET: off
      ONTAPI GET: off
    Cluster Peer: on
```

GET 감사 활성화의 효과

ONTAP 9.17.1부터 "CLI, HTTP, ONTAPI GET 감사 활성화" 피어링된 클러스터에서는 클러스터 간 사용자 시작 GET 요청에 대한 감사도 활성화할 수 있습니다. 이전 ONTAP 버전에서는 GET 감사가 로컬 클러스터의 요청에만 적용되었습니다. ONTAP 9.17.1에서는 `cluster-peer` 옵션 설정 `on` 로컬 클러스터와 클러스터 간 요청이 모두 감사합니다.

ONTAP 감사 로그 대상을 관리합니다

감사 로그를 최대 10개의 대상으로 전달할 수 있습니다. 예를 들어, 모니터링, 분석 또는 백업을 위해 로그를 Splunk 또는 syslog 서버로 전달할 수 있습니다.

이 작업에 대해

전달을 구성하려면 syslog 또는 Splunk 호스트의 IP 주소, 포트 번호, 전송 프로토콜 및 전달된 로그에 사용할 syslog 기능을 제공해야 합니다. "syslog 기능에 대해 자세히 알아보십시오".

`-protocol`매개 변수를 사용하여 다음 전송 값 중 하나를 선택할 수 있습니다.

UDP 암호화되지 않음
: 보안이 없는 사용자 데이터그램 프로토콜(기본값)

TCP 암호화되지 않음
: 보안 기능이 없는 전송 제어 프로토콜

TCP 암호화
: 전송 계층 보안(TLS)이 있는 전송 제어 프로토콜 + A * 서버 확인 * 옵션은 TCP 암호화 프로토콜이 선택된 경우에 사용할 수 있습니다.

기본 포트는 UDP의 경우 514, TCP의 경우 6514이지만 네트워크 요구를 충족하는 포트를 지정할 수 있습니다.

`-message-format`명령을 사용하여 다음 메시지 형식 중 하나를 선택할 수 있습니다.

레거시 **- NetApp**
: RFC-3164 Syslog 형식의 변형(형식: <PRIVAL> 타임스탬프 HOSTNAME:MSG)

RFC-5424
: RFC-5424에 따른 syslog 형식(형식: <PRIVAL> 버전 타임스탬프 HOSTNAME:MSG)

ONTAP CLI에서 감사 로그를 전달하고 ONTAP 9.11.1부터 System Manager에서 전달할 수 있습니다.

시스템 관리자

- 감사 로그 대상을 표시하려면 * 클러스터 > 설정 * 을 선택합니다. +로그 대상 수가 * 알림 관리 타일 * 에 표시됩니다. ⋮세부 정보를 표시하려면 클릭하십시오.
- 감사 로그 대상을 추가, 수정 또는 삭제하려면 * 이벤트 및 작업 > 감사 로그 * 를 선택한 다음 화면 오른쪽 상단의 * 감사 대상 관리 * 를 클릭합니다. + 를 + Add 클릭하거나 ⋮ * 호스트 주소 * 열을 클릭하여 항목을 편집하거나 삭제합니다.

CLI를 참조하십시오

1. 감사 로그를 전달할 각 대상에 대해 대상 IP 주소 또는 호스트 이름 및 보안 옵션을 지정합니다.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 6514 -protocol tcp-encrypted -facility user
```

   - "cluster log-forwarding create" 명령이 대상 호스트를 ping하여 연결을 확인할 수 없으면 명령이 실패하고 오류가 표시됩니다. 권장하지는 않지만 명령과 함께 '-force' 매개 변수를 사용하면 연결 확인이 생략됩니다.
   - '-verify-server' 매개 변수를 'true'로 설정하면 로그 전달 대상 ID가 인증서의 유효성을 확인하여 확인됩니다. 프로토콜 필드에서 TCP 암호화 값을 선택한 경우에만 이 값을 'true'로 설정할 수 있습니다.

2. cluster log-forwarding show 명령을 사용하여 대상 레코드가 올바른지 확인합니다.

```
cluster1::> cluster log-forwarding show

                                                 Verify Syslog
Destination Host          Port   Protocol        Server Facility
------------------------- ------ --------        ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            6514   tcp-encrypted   true   user
2 entries were displayed.
```

관련 정보

- "클러스터 로그 전달 표시"
- "클러스터 로그 전달 생성"

AutoSupport

AutoSupport에 대해 자세히 알아보십시오

ONTAP AutoSupport에 대해 자세히 알아보십시오

AutoSupport는 시스템의 상태를 능동적으로 모니터링하고 NetApp 기술 지원, 내부 지원 조직 및 지원 파트너에게 메시지를 자동으로 보내는 메커니즘입니다. AutoSupport 기술 지원 메시지를 기본적으로 사용하도록 설정했지만 올바른 옵션을 설정하고 내부 지원 조직에 메시지를 보낼 수 있는 유효한 메일 호스트를 가지고 있어야 합니다.

클러스터 관리자만 AutoSupport 관리를 수행할 수 있습니다. 스토리지 가상 시스템(SVM) 관리자는 AutoSupport에 액세스할 수 없습니다.

스토리지 시스템을 처음 구성할 때 AutoSupport가 기본적으로 설정됩니다. AutoSupport는 AutoSupport가 활성화된 후 24시간 후에 기술 지원 부서에 메시지를 보내기 시작합니다. 시스템을 업그레이드 또는 되돌리거나, AutoSupport 구성을 수정하거나, 시스템 시간을 24시간 이외의 시간으로 변경하여 24시간을 단축할 수 있습니다.

> 언제든지 AutoSupport를 비활성화할 수 있지만, 이 기능을 활성 상태로 두어야 합니다. AutoSupport를 활성화하면 스토리지 시스템에서 문제가 발생할 경우 문제를 신속하게 확인하고 해결할 수 있습니다. 기본적으로 시스템에서는 AutoSupport를 사용하지 않도록 설정하더라도 AutoSupport 정보를 수집하여 로컬에 저장합니다.

AutoSupport에 대한 자세한 내용은 NetApp Support 사이트 를 참조하십시오.

관련 정보

- "NetApp 지원"
- "ONTAP 명령 참조입니다"

디지털 자문 및 ONTAP AutoSupport에 대해 알아보기

ONTAP의 AutoSupport 구성 요소는 원격 측정을 수집하여 분석을 위해 전송합니다. Digital Advisor는 AutoSupport에서 데이터를 분석하고 능동적 관리 및 최적화를 제공합니다. Digital Advisor는 인공 지능을 사용하여 잠재적 문제를 식별하고 비즈니스에 영향을 미치기 전에 해결할 수 있도록 지원합니다.

Digital Advisor를 사용하면 클라우드 기반 포털 및 모바일 앱을 통해 실행 가능한 예측 분석과 사전 예방적 지원을 제공하여 글로벌 하이브리드 클라우드 전반에서 데이터 인프라를 최적화할 수 있습니다. 활성 SupportEdge 계약을 보유한 모든 NetApp 고객은 디지털 어드바이저의 데이터 중심 인사이트와 권장 사항을 이용할 수 있습니다(기능은 제품 및 지원 계층에 따라 다름).

Digital Advisor로 할 수 있는 작업은 다음과 같습니다.

- 업그레이드 계획 Digital Advisor는 최신 버전의 ONTAP로 업그레이드하여 해결할 수 있는 환경 문제를 식별하며 업그레이드 관리자 구성 요소는 성공적인 업그레이드를 계획하는 데 도움이 됩니다.
- 시스템 상태 보기 Digital Advisor 대시보드에서 웰니스 문제를 보고하고 이러한 문제를 해결할 수 있습니다. 시스템 용량을 모니터링하여 스토리지 공간이 부족하지 않도록 하십시오. 시스템에 대한 지원 케이스를 봅니다.
- 성능 관리 Digital Advisor는 System Manager에서 볼 수 있는 것보다 더 오랜 기간 동안 시스템 성능을 표시합니다. 성능에 영향을 주는 구성 및 시스템 문제를 식별합니다.
- 효율성 극대화 스토리지 효율성 메트릭을 확인하고 더 적은 공간에 더 많은 데이터를 저장하는 방법을

알아보십시오.

- 인벤토리 및 구성을 봅니다. Digital Advisor는 전체 인벤토리와 소프트웨어 및 하드웨어 구성 정보를 표시합니다. 서비스 계약이 만료되는 시기를 확인하고 서비스 계약을 갱신하여 계속 지원을 받을 수 있도록 합니다.

관련 정보

"NetApp 설명서: 디지털 어드바이저"

"Digital Advisor를 실행합니다"

"SupportEdge 서비스"

ONTAP AutoSupport 메시지를 보내는 시기와 위치에 대해 알아봅니다

AutoSupport는 메시지 유형에 따라 다른 수신자에게 메시지를 보냅니다. AutoSupport에서 메시지를 보내는 시기와 위치를 파악하면 디지털 어드바이저 웹 사이트에서 전자 메일 또는 보기를 통해 받는 메시지를 이해하는 데 도움이 됩니다.

별도로 지정하지 않는 한 다음 표의 설정은 'system node AutoSupport modify' 명령의 매개 변수입니다.

이벤트가 트리거된 메시지입니다

시스템에서 수정 조치가 필요한 이벤트가 발생하면 AutoSupport는 자동으로 이벤트 트리거 메시지를 전송합니다.

메시지가 전송될 때	메시지가 전송되는 위치입니다
AutoSupport는 EMS에서 트리거 이벤트에 응답합니다	"to"와 "noteto"에 지정된 주소. (서비스에 영향을 주는 중요 이벤트만 전송됩니다.) '-PARTNER-ADDRESS'에 명시된 주소 기술 지원, 만약 '-support'가 'enable'로 설정되어 있으면

예약된 메시지입니다

AutoSupport는 정기적으로 여러 메시지를 자동으로 보냅니다.

메시지가 전송될 때	메시지가 전송되는 위치입니다
매일(기본적으로 오전 12:00 사이에 전송됨 오전 1시 로그 메시지로 사용)	'-PARTNER-ADDRESS'에 명시된 주소 기술 지원, 만약 '-support'가 'enable'로 설정되어 있으면
매일(기본적으로 오전 12:00 사이에 전송됨 오전 1시 성능 메시지로서 -perf 매개 변수가 true로 설정되어 있으면	'파트너 주소'에 지정된 주소 기술 지원, 만약 '-support'가 'enable'로 설정되어 있으면
매주(기본적으로 일요일 오전 12:00 사이에 전송됨 및 오전 1:00)	'-PARTNER-ADDRESS'에 명시된 주소 기술 지원, 만약 '-support'가 'enable'로 설정되어 있으면

AutoSupport 메시지를 수동으로 시작하거나 다시 보낼 수 있습니다.

메시지가 전송될 때	메시지가 전송되는 위치입니다
'system node AutoSupport invoke' 명령어를 이용하여 수동으로 메시지를 시작한다	System node AutoSupport invoke 명령에 '-Uri' 파라미터를 사용하여 URI를 지정하면 해당 URI로 메시지가 전송됩니다. 만약 '-Uri'를 생략하면 '-to', '-partner-address'에 지정된 주소로 메시지가 전송됩니다. 이 메시지는 '-support'가 'enable'로 설정되어 있는 경우 기술 지원부에도 전송됩니다.
'system node AutoSupport invoke-core-upload' 명령어를 이용하여 수동으로 메시지를 시작한다	System node AutoSupport invoke-core-upload 명령에서 '-Uri' 매개 변수를 사용하여 URI를 지정하면 해당 URI로 메시지가 전송되고 core dump 파일이 URI로 업로드된다. system node AutoSupport invoke-core-upload 명령에서 -uri를 생략하면 기술 지원 부서에 메시지가 전송되고 코어 덤프 파일이 기술 지원 사이트에 업로드됩니다. 두 시나리오 모두 '-support'가 'enable'로 설정되어 있고 'transport'가 'https' 또는 'http'로 설정되어 있어야 합니다. 코어 덤프 파일의 크기가 크기 때문에 '-to' 및 '-partner-addresses' 매개 변수에 지정된 주소로 메시지가 전송되지 않습니다.
'system node AutoSupport invoke-performance-archive' 명령어를 사용하여 수동으로 메시지를 시작한다	System node AutoSupport invoke-performance-archive 명령에서 '-Uri' 매개 변수를 사용하여 URI를 지정하면 해당 URI로 메시지가 전송되고 성능 아카이브 파일이 URI로 업로드됩니다. System node AutoSupport invoke-performance-archive에서 -Uri를 생략하면 기술 지원 부서에 메시지가 전송되고 성능 아카이브 파일이 기술 지원 사이트에 업로드됩니다. 두 시나리오 모두 '-support'가 'enable'로 설정되어 있고 'transport'가 'https' 또는 'http'로 설정되어 있어야 합니다. 대용량 성능 아카이브 파일로 인해 '-to' 및 '-partner-addresses' 매개 변수에 지정된 주소로 메시지가 전송되지 않습니다.
'시스템 노드 AutoSupport history retransmit' 명령어를 이용하여 수동으로 과거 메시지를 재전송한다	System node AutoSupport history retransmit 명령의 '-Uri' 파라미터에 지정하는 URI에만 해당

기술 지원 부서에서 트리거하는 메시지

기술 지원 부서는 AutoSupport OnDemand 기능을 사용하여 AutoSupport로부터 메시지를 요청할 수 있습니다.

메시지가 전송될 때	메시지가 전송되는 위치입니다
AutoSupport가 새 AutoSupport 메시지를 생성하기 위한 전달 지침을 얻는 경우	'-PARTNER-ADDRESS'에 명시된 주소 기술 지원인 -support가 enable로 설정되어 있고 -transport가 https로 설정되어 있으면
AutoSupport가 지난 AutoSupport 메시지를 다시 보내기 위한 전달 지침을 얻는 경우	기술 지원인 -support가 enable로 설정되어 있고 -transport가 https로 설정되어 있으면
AutoSupport가 코어 덤프 또는 성능 아카이브 파일을 업로드하는 새 AutoSupport 메시지를 생성하기 위한 전달 지침을 얻는 경우	기술 지원인 -support가 enable로 설정되어 있고 -transport가 https로 설정되어 있으면. 코어 덤프 또는 성능 아카이브 파일이 기술 지원 사이트에 업로드됩니다.

ONTAP AutoSupport 이벤트 트리거 메시지에 대해 알아봅니다

AutoSupport는 EMS가 트리거 이벤트를 처리할 때 이벤트 트리거 AutoSupport 메시지를 생성합니다. 이벤트가 트리거된 AutoSupport 메시지는 수신자에게 수정 조치가 필요한 문제를 경고하고 문제와 관련된 정보만 포함합니다. 포함할 콘텐츠 및 메시지를 받는 사람을 사용자 지정할 수 있습니다.

AutoSupport는 다음 프로세스를 사용하여 이벤트 트리거 AutoSupport 메시지를 만들고 보냅니다.

1. EMS가 trigger event를 처리할 때, EMS는 AutoSupport에게 request를 보낸다.

   트리거 이벤트는 AutoSupport 대상 및 이름이 callhome으로 시작하는 EMS 이벤트입니다.

2. AutoSupport에서 이벤트 트리거 AutoSupport 메시지를 생성합니다.

   AutoSupport는 트리거와 연결된 하위 시스템으로부터 기본 및 문제 해결 정보를 수집하여 트리거 이벤트와 관련된 정보만 포함된 메시지를 생성합니다.

   기본 하위 시스템 세트는 각 트리거와 연결됩니다. 그러나 'system node AutoSupport trigger modify' 명령을 사용하여 추가 서브시스템을 트리거에 연결할 수 있습니다.

3. AutoSupport는 시스템 노드 AutoSupport modify 명령에 의해 정의된 수신자에게 -to, -noteto, -partner-address, -support 매개 변수를 사용하여 이벤트 트리거 AutoSupport 메시지를 보냅니다.

   '-to' 및 '-noteto' 매개 변수를 사용하여 'system node AutoSupport trigger modify' 명령을 사용하여 특정 트리거에 대한 AutoSupport 메시지 전달을 활성화 또는 비활성화할 수 있습니다.

특정 이벤트에 대해 전송된 데이터의 예

Storage shelf PSU failed EMS 이벤트는 Mandatory, Log Files, Storage, RAID, HA의 기본 데이터가 포함된 메시지를 플랫폼, 네트워킹 하위 시스템 및 필수, 로그 파일 및 스토리지 하위 시스템의 데이터 문제 해결

향후 '스토리지 셸프 PSU 실패' 이벤트에 대한 응답으로 전송된 AutoSupport 메시지에 NFS에 대한 데이터를

포함시키기로 결정합니다. callhome.shlf.ps.fault 이벤트에 대해 NFS에 대한 문제 해결 수준 데이터를 활성화하려면 다음 명령을 입력합니다.

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

'system node AutoSupport trigger' 명령어를 사용하거나 CLI에서 AutoSupport 및 EMS 이벤트가 참조할 때 callhome.shlf.ps.fault 이벤트에서 callhome. 접두사가 삭제된다.

ONTAP AutoSupport 메시지 유형 및 내용

AutoSupport 메시지에는 지원되는 하위 시스템에 대한 상태 정보가 포함되어 있습니다. AutoSupport 메시지에 포함된 내용을 학습하면 디지털 어드바이저 웹 사이트에서 이메일 또는 열람으로 받은 메시지를 해석하거나 이에 대응하는 데 도움이 될 수 있습니다.

메시지 유형입니다	메시지에 포함된 데이터 유형입니다
이벤트가 트리거되었습니다	이벤트가 발생한 특정 하위 시스템에 대한 컨텍스트 기반 데이터를 포함하는 파일입니다
매일	로그 파일
성능	지난 24시간 동안 샘플링된 성능 데이터
매주	구성 및 상태 데이터
'system node AutoSupport invoke' 명령에 의해 발생한다	'-type' 파라미터에 지정된 값에 따라 다름: • "테스트"는 기본적인 데이터가 포함된 사용자 트리거 메시지를 보냅니다. 또한 이 메시지는 '-to' 옵션을 사용하여 기술 지원에서 특정 이메일 주소로 자동 이메일 응답을 트리거하여 AutoSupport 메시지가 수신되고 있는지 확인할 수 있도록 합니다. • '성능'은 성능 데이터를 전송합니다. • All은 서브시스템의 데이터 문제 해결 등 주간 메시지와 유사한 완전한 데이터 세트를 가진 사용자 트리거 메시지를 전송한다. 기술 지원 부서에서는 일반적으로 이 메시지를 요청합니다.

메시지 유형입니다	메시지에 포함된 데이터 유형입니다
'system node AutoSupport invoke-core-upload' 명령에 의해 발생한다	노드의 코어 덤프 파일
'system node AutoSupport invoke-performance-archive' 명령에 의해 트리거됩니다	지정된 기간 동안 성능 아카이브 파일
AutoSupport OnDemand에 의해 트리거됩니다	AutoSupport OnDemand는 새 메시지 또는 이전 메시지를 요청할 수 있습니다. • AutoSupport 수집 유형에 따라 테스트, 전체 또는 성능 중 새 메시지가 나타날 수 있습니다. • 지난 메시지는 다시 전송되는 메시지 유형에 따라 달라집니다. AutoSupport OnDemand에서는 다음 파일을 NetApp 지원 사이트 로 업로드하는 새 메시지를 요청할 수 있습니다 "mysupport.netapp.com". • 코어 덤프 • 성능 아카이브

ONTAP AutoSupport 하위 시스템을 봅니다

각 하위 시스템은 AutoSupport가 해당 메시지에 사용하는 기본 및 문제 해결 정보를 제공합니다. 또한 각 하위 시스템은 트리거 이벤트와 관련된 하위 시스템에서만 AutoSupport가 수집하도록 허용하는 트리거 이벤트와도 연결됩니다.

AutoSupport는 상황에 맞는 콘텐츠를 수집합니다.

단계

1. 하위 시스템 및 트리거 이벤트에 대한 정보를 봅니다.

```
system node autosupport trigger show
```

ONTAP AutoSupport 규모 및 시간 예산에 대해 알아보십시오

AutoSupport는 하위 시스템별로 정보를 수집하고 각 하위 시스템의 콘텐츠에 대한 크기 및 시간 예산을 적용합니다. 스토리지 시스템이 확장됨에 따라 AutoSupport 예산을 통해 AutoSupport 페이로드를 제어할 수 있으므로, AutoSupport 데이터를 확장 가능한 제공할 수 있습니다.

AutoSupport는 하위 시스템 컨텐츠가 크기 또는 시간 예산을 초과하는 경우 정보 수집을 중지하고 AutoSupport 콘텐츠를 잘라냅니다. 콘텐츠를 쉽게 자를 수 없는 경우(예: 이진 파일) AutoSupport에서 콘텐츠를 생략합니다.

NetApp Support에서 요청받은 경우에만 기본 크기 및 시간 예산을 수정해야 합니다. AutoSupport manifest show

명령을 사용하여 하위 시스템의 기본 크기 및 시간 예산을 검토할 수도 있습니다.

이벤트가 트리거되는 **ONTAP AutoSupport** 메시지에서 보낸 파일에 대해 알아봅니다

이벤트 트리거 AutoSupport 메시지에는 AutoSupport가 메시지를 생성하도록 한 이벤트와 연결된 하위 시스템의 기본 및 문제 해결 정보만 포함됩니다. 특정 데이터는 NetApp 지원 및 지원 파트너가 문제를 해결하는 데 도움이 됩니다.

AutoSupport는 다음 기준을 사용하여 이벤트 트리거 AutoSupport 메시지의 콘텐츠를 제어합니다.

- 포함된 하위 시스템

  데이터는 로그 파일과 같은 공통 하위 시스템 및 RAID와 같은 특정 하위 시스템을 포함한 하위 시스템으로 그룹화됩니다. 각 이벤트는 특정 하위 시스템의 데이터만 포함하는 메시지를 트리거합니다.

- 포함된 각 하위 시스템의 세부 수준

  포함된 각 하위 시스템의 데이터는 기본 또는 문제 해결 수준에서 제공됩니다.

'system node AutoSupport trigger show' 명령을 사용하여 가능한 모든 이벤트를 보고 각 이벤트에 대한 메시지에 포함할 하위 시스템을 '-instance' 매개 변수와 함께 확인할 수 있습니다.

각 이벤트에 기본적으로 포함되는 하위 시스템 외에도 '시스템 노드 AutoSupport trigger modify' 명령어를 사용하여 기본 또는 문제 해결 수준에서 하위 시스템을 추가할 수 있습니다.

AutoSupport 메시지로 전송된 로그 파일

AutoSupport 메시지에는 기술 지원 직원이 최근 시스템 작업을 검토할 수 있도록 하는 몇 가지 주요 로그 파일이 포함될 수 있습니다.

로그 파일 하위 시스템이 활성화된 경우 모든 유형의 AutoSupport 메시지에 다음 로그 파일이 포함될 수 있습니다.

로그 파일	파일에 포함된 데이터의 양입니다
• '/mroot/etc/log/mlog/' 디렉토리에서 파일을 기록합니다 • 메시지 로그 파일입니다	마지막 AutoSupport 메시지 이후 로그에 추가된 새 줄만 지정된 최대값까지 추가됩니다. 이렇게 하면 AutoSupport 메시지에 중복되지 않는 고유한 관련 데이터가 포함됩니다. (파트너의 로그 파일은 예외입니다. 파트너의 경우 허용되는 최대 데이터가 포함됩니다.)
• '/mroot/etc/log/shelflog/' 디렉토리의 로그 파일 • '/mroot/etc/log/acp/' 디렉토리의 로그 파일 • EMS(Event Management System) 로그 데이터	지정된 최대값까지의 최근 데이터 줄.

AutoSupport 메시지의 내용은 ONTAP 릴리스 간에 변경될 수 있습니다.

주간 **AutoSupport** 메시지로 전송된 파일입니다

Weekly AutoSupport 메시지에는 시간에 따른 시스템 변경 사항을 추적하는 데 유용한 추가 구성 및 상태 데이터가 포함되어 있습니다.

다음 정보는 주간 AutoSupport 메시지로 전송됩니다.

- 모든 하위 시스템에 대한 기본 정보
- 선택한 '/mroot/etc' 디렉토리 파일의 내용입니다
- 로그 파일
- 시스템 정보를 제공하는 명령의 출력
- RDB(복제 데이터베이스) 정보, 서비스 통계 등을 비롯한 추가 정보

ONTAP AutoSupport OnDemand가 기술 지원 부서의 제공 지침을 받는 방법에 대해 알아보십시오

AutoSupport OnDemand는 정기적으로 기술 지원 팀과 통신하여 AutoSupport 메시지 전송, 재전송 및 거부 방법과 대용량 파일을 NetApp Support 사이트에 업로드하는 방법에 대한 제공 지침을 얻습니다. AutoSupport OnDemand를 사용하면 AutoSupport 메시지가 주간 AutoSupport 작업이 실행되기를 기다리지 않고 필요 시 전송됩니다.

AutoSupport OnDemand는 다음과 같은 구성 요소로 이루어집니다.

- 각 노드에서 실행되는 AutoSupport OnDemand 클라이언트입니다
- 기술 지원에 상주하는 AutoSupport OnDemand 서비스입니다

AutoSupport OnDemand 클라이언트는 정기적으로 AutoSupport OnDemand 서비스를 폴링하여 기술 지원 부서의 제공 지침을 받습니다. 예를 들어 기술 지원 부서에서는 AutoSupport OnDemand 서비스를 사용하여 새 AutoSupport 메시지 생성이 요청될 수 있습니다. AutoSupport OnDemand 클라이언트가 AutoSupport OnDemand 서비스를 폴링하면 클라이언트는 배달 지침을 얻고 요청에 따라 새 AutoSupport 메시지를 보냅니다.

AutoSupport OnDemand는 기본적으로 사용하도록 설정됩니다. 그러나 AutoSupport OnDemand는 일부 AutoSupport 설정에 의존하여 기술 지원 팀과 계속 통신합니다. AutoSupport OnDemand는 다음 요구 사항이 충족되면 자동으로 기술 지원 팀과 통신합니다.

- AutoSupport가 활성화되었습니다.
- AutoSupport는 기술 지원 부서에 메시지를 전송하도록 구성되어 있습니다.
- AutoSupport는 HTTPS 전송 프로토콜을 사용하도록 구성되어 있습니다.

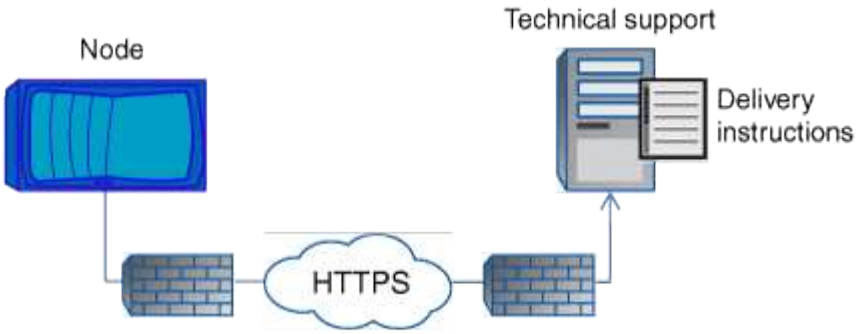
AutoSupport OnDemand 클라이언트는 AutoSupport 메시지가 전송되는 것과 동일한 기술 지원 위치로 HTTPS 요청을 보냅니다. AutoSupport OnDemand 클라이언트는 들어오는 연결을 허용하지 않습니다.

> AutoSupport OnDemand는 "AutoSupport" 사용자 계정을 사용하여 기술 지원 팀과 통신합니다. ONTAP에서는 이 계정을 삭제할 수 없습니다.

AutoSupport OnDemand를 사용하지 않도록 설정하고 AutoSupport를 계속 사용하도록 설정하려면 명령을 `system node autosupport modify -ondemand-state disable`사용합니다. 에 대한 자세한 내용은 `system node autosupport modify -ondemand-state disable` "ONTAP 명령 참조입니다"을

참조하십시오.

다음 그림에서는 AutoSupport OnDemand가 기술 지원 부서에 HTTPS 요청을 보내 전달 지침을 얻는 방법을 보여 줍니다.



배송 지침에는 AutoSupport에서 다음을 수행하도록 요청하는 내용이 포함될 수 있습니다.

- 새 AutoSupport 메시지를 생성합니다.

  기술 지원 부서에서는 문제 선별을 위해 새 AutoSupport 메시지를 요청할 수 있습니다.

- 핵심 덤프 파일 또는 성능 아카이브 파일을 NetApp Support 사이트에 업로드하는 새 AutoSupport 메시지를 생성합니다.

  기술 지원 부서에서는 문제를 선별하기 위해 코어 덤프 또는 성능 아카이브 파일을 요청할 수 있습니다.

- 이전에 생성된 AutoSupport 메시지를 다시 전송합니다.

  이 요청은 배달 실패로 인해 메시지를 받지 못한 경우 자동으로 발생합니다.

- 특정 트리거 이벤트에 대한 AutoSupport 메시지 전달을 비활성화합니다.

  기술 지원 부서에서는 사용되지 않는 데이터의 제공을 비활성화할 수 있습니다.

전자 메일로 보낸 **ONTAP AutoSupport** 메시지의 구조에 대해 알아봅니다

AutoSupport 메시지를 전자 메일로 보내면 메시지에 표준 제목, 간단한 본문 및 데이터가 포함된 7z 파일 형식의 대용량 첨부 파일이 포함됩니다.

AutoSupport가 개인 데이터를 숨기도록 구성된 경우 호스트 이름과 같은 특정 정보는 헤더, 제목, 본문 및 첨부 파일에서 생략되거나 마스킹됩니다.

제목

AutoSupport 메커니즘에서 보낸 메시지의 제목 줄에는 알림의 원인을 식별하는 텍스트 문자열이 포함됩니다. 제목 줄의 형식은 다음과 같습니다.

시스템_이름_(메시지)_심각도 _ 의 HA 그룹 알림

- _System_Name_은 AutoSupport 구성에 따라 호스트 이름 또는 시스템 ID입니다

바디

AutoSupport 메시지 본문에는 다음 정보가 포함됩니다.

- 메시지의 날짜 및 타임 스탬프입니다
- 메시지를 생성한 노드의 ONTAP 버전입니다
- 메시지를 생성한 노드의 시스템 ID, 일련 번호 및 호스트 이름입니다
- AutoSupport 시퀀스 번호
- SNMP 연락처 이름 및 위치(지정된 경우
- HA 파트너 노드의 시스템 ID 및 호스트 이름입니다

첨부 파일

AutoSupport 메시지의 주요 정보는 body.7z라는 7z 파일로 압축되어 메시지에 첨부되는 파일에 포함되어 있습니다.

첨부 파일에 포함된 파일은 AutoSupport 메시지 유형에 따라 다릅니다.

ONTAP AutoSupport 심각도 유형에 대해 알아봅니다

AutoSupport 메시지에는 각 메시지의 용도를 이해하는 데 도움이 되는 심각도 유형이 있습니다. 예를 들어 긴급 문제에 즉시 주의를 기울이거나 정보를 제공하는 용도로만 사용됩니다.

메시지에는 다음 심각도 중 하나가 있습니다.

- * 경고 *: 경고 메시지는 조치를 취하지 않을 경우 다음 단계의 이벤트가 발생할 수 있음을 나타냅니다.

  24시간 이내에 경고 메시지에 대해 조치를 취해야 합니다.

- * 비상 *: 중단이 발생했을 때 비상 메시지가 표시됩니다.

  긴급 메시지에 대해 즉시 조치를 취해야 합니다.

- * 오류 *: 오류 조건은 무시할 경우 발생할 수 있는 상황을 나타냅니다.
- * 알림 *: 정상이지만 심각한 상태입니다.
- * 정보 *: 무시할 수 있는 문제에 대한 세부 정보를 제공하는 정보 메시지입니다.
- **Debug**: 디버그 수준 메시지는 수행해야 하는 지침을 제공합니다.

내부 지원 조직이 이메일을 통해 AutoSupport 메시지를 수신하는 경우, 이메일 메시지의 제목 줄에 심각도가 표시됩니다.

ONTAP AutoSupport 메시지 설명을 확인합니다

수신하는 AutoSupport 메시지에 대한 설명은 ONTAP Syslog Translator를 통해 확인할 수 있습니다.

단계

1. 로 이동합니다 "Syslog 변환기".

2. [릴리스] 필드에 사용 중인 **ONTAP** 버전을 입력합니다. 검색 문자열** 필드에 "callhome"을 입력합니다. Translate * 를 선택합니다.
3. Syslog Translator는 사용자가 입력한 메시지 문자열과 일치하는 모든 이벤트를 알파벳 순으로 나열합니다.

ONTAP AutoSupport를 관리하는 명령입니다

'시스템 노드 AutoSupport' 명령어를 이용하여 AutoSupport 설정을 변경, 조회, 이전 AutoSupport 메시지 정보 표시, AutoSupport 메시지 전송, 재전송, 취소 등을 할 수 있다.

AutoSupport를 구성합니다

원하는 작업	이 명령 사용...
AutoSupport 메시지 전송 여부를 제어합니다	'system node AutoSupport modify'는 -state 매개 변수를 사용합니다
AutoSupport 메시지가 기술 지원 부서에 전송되는지 여부를 제어합니다	system node AutoSupport modify with the '-support' parameter
AutoSupport를 설정하거나 AutoSupport의 구성을 수정합니다	'시스템 노드 AutoSupport 수정
개별 트리거 이벤트에 대해 내부 지원 조직에 AutoSupport 메시지를 활성화 및 비활성화하고 개별 트리거 이벤트에 대한 응답으로 전송된 메시지에 포함할 추가 하위 시스템 보고서를 지정합니다	'시스템 노드 AutoSupport trigger modify

AutoSupport 구성에 대한 정보를 표시합니다

원하는 작업	이 명령 사용...
AutoSupport 설정을 표시합니다	'system node AutoSupport show'와 '-node' 매개 변수를 함께 사용합니다
AutoSupport 메시지를 수신하는 모든 주소 및 URL의 요약을 봅니다	'System node AutoSupport destinations show'가 나타납니다
개별 트리거 이벤트에 대해 내부 지원 조직에 전송되는 AutoSupport 메시지를 표시합니다	'시스템 노드 AutoSupport trigger show'
AutoSupport 구성 상태 및 다양한 대상에 대한 전송 상태를 표시합니다	'시스템 노드 AutoSupport check show'
AutoSupport 구성의 세부 상태와 다양한 대상에 대한 전송을 표시합니다	'시스템 노드 AutoSupport check show-details

지난 **AutoSupport** 메시지에 대한 정보를 표시합니다

원하는 작업	이 명령 사용...
최근 50개 AutoSupport 메시지 중 하나 이상에 대한 정보를 표시합니다	'시스템 노드 AutoSupport history show'
코어 덤프 또는 성능 아카이브 파일을 기술 지원 사이트나 지정된 URI에 업로드하기 위해 생성된 최근 AutoSupport 메시지에 대한 정보를 표시합니다	'시스템 노드 AutoSupport history show-upload-details'
메시지에 대해 수집된 각 파일의 이름과 크기를 비롯한 AutoSupport 메시지의 정보를 오류 메시지와 함께 확인합니다	'System node AutoSupport manifest show'

AutoSupport 메시지 보내기, 다시 보내기 또는 취소

원하는 작업	이 명령 사용...
AutoSupport 시퀀스 번호로 식별되는 로컬에 저장된 AutoSupport 메시지를 다시 전송합니다 AutoSupport 메시지를 다시 전송하고 해당 메시지를 이미 수신한 경우 지원 시스템에서 중복 케이스를 생성하지 않습니다. 반면에 지원부서에서 해당 메시지를 받지 못한 경우 AutoSupport 시스템은 메시지를 분석하고 필요한 경우 케이스를 생성합니다.	시스템 노드 AutoSupport history retransmit
AutoSupport 메시지 생성 및 전송 — 예를 들어, 테스트용으로 사용합니다	'시스템 노드 AutoSupport 호출' AutoSupport가 비활성화되었더라도 '-force' 매개 변수를 사용하여 메시지를 보냅니다. 구성된 대상 대신 지정한 대상으로 메시지를 보내려면 '-Uri' 매개 변수를 사용합니다.
AutoSupport 메시지를 취소합니다	'시스템 노드 AutoSupport history cancel

에 대한 자세한 내용은 `system node autosupport` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

"ONTAP 명령 참조입니다"

ONTAP AutoSupport 매니페스트에 포함된 정보에 대해 알아봅니다

AutoSupport 매니페스트는 각 AutoSupport 메시지에 대해 수집된 파일에 대한 자세한 보기를

제공합니다. AutoSupport 매니페스트에는 AutoSupport에서 필요한 파일을 수집할 수 없는 경우 컬렉션 오류에 대한 정보도 포함되어 있습니다.

AutoSupport 매니페스트에는 다음 정보가 포함됩니다.

- AutoSupport 메시지의 Sequence Number
- AutoSupport 메시지에 포함된 AutoSupport 파일
- 각 파일의 크기(바이트)입니다
- AutoSupport 매니페스트 컬렉션의 상태입니다
- AutoSupport가 하나 이상의 파일을 수집하지 못한 경우 오류 설명입니다

'system node AutoSupport manifest show' 명령을 사용하여 AutoSupport 매니페스트를 볼 수 있습니다.

AutoSupport 매니페스트는 모든 AutoSupport 메시지에 포함되어 있으며 XML 형식으로 표시됩니다. 즉, 일반 XML 뷰어를 사용하여 읽거나 디지털 어드바이저 포털을 사용하여 볼 수 있습니다.

계획

ONTAP AutoSupport 사용을 준비합니다

ONTAP 클러스터를 구성하여 AutoSupport 메시지를 NetApp에 전달할 수 있습니다. 또한 일반적으로 조직 내의 로컬 전자 메일 주소로 메시지 복사본을 보낼 수도 있습니다. 사용 가능한 옵션을 검토하여 AutoSupport를 구성할 준비를 해야 합니다.

AutoSupport 메시지를 **NetApp**에 전달합니다

AutoSupport 메시지는 HTTPS 또는 SMTP 프로토콜을 사용하여 NetApp에 전달될 수 있습니다. ONTAP 9.15.1부터 SMTP와 함께 TLS를 사용할 수도 있습니다.

AutoSupport OnDemand와의 통신 및 대용량 파일 업로드에 가능하면 항상 HTTPS를 사용하십시오.

또한 다음 사항에 유의하십시오.

- NetApp AutoSupport 메시지에 대해 하나의 전달 채널만 구성할 수 있습니다. 두 프로토콜을 사용하여 AutoSupport 메시지를 NetApp에 전달할 수는 없습니다.
- AutoSupport는 각 프로토콜의 최대 파일 크기를 제한합니다. AutoSupport 메시지의 크기가 구성된 제한을 초과하는 경우 AutoSupport는 메시지를 최대한 많이 전달하지만 잘립니다.
- 필요한 경우 최대 파일 크기를 변경할 수 있습니다. 에 대한 자세한 내용은 `system node autosupport modify` "ONTAP 명령 참조입니다"을 참조하십시오.
- 두 프로토콜 모두 이름이 확인되는 주소 패밀리에 따라 IPv4 또는 IPv6를 통해 전송할 수 있습니다.
- ONTAP에서 AutoSupport 메시지를 보내기 위해 설정한 TCP 연결은 일시적이며 단기간 동안 사용됩니다.

HTTPS

가장 강력한 기능을 제공합니다. 다음 사항에 유의하십시오.

- AutoSupport OnDemand 및 대용량 파일 전송이 지원됩니다.
- HTTPS PUT 요청이 먼저 시도됩니다. 전송 중에 요청이 실패하면 요청이 중지된 곳에서 다시 시작됩니다.
- 서버가 PUT를 지원하지 않으면 HTTPS POST 메서드가 대신 사용됩니다.
- HTTPS 전송의 기본 제한은 50MB입니다.
- HTTPS 프로토콜은 포트 443을 사용합니다.

SMTP

일반적으로 HTTPS가 허용되지 않거나 지원되지 않는 경우에만 SMTP를 사용해야 합니다. 다음 사항에 유의하십시오.

- AutoSupport OnDemand 및 대용량 파일 전송은 지원되지 않습니다.
- SMTP 로그인 자격 증명이 구성된 경우 암호화되지 않은 상태로 전송됩니다.
- 기본 전송 제한은 5MB입니다.
- 비보안 SMTP 프로토콜은 포트 25를 사용합니다.

TLS를 사용하여 **SMTP** 보안 개선

SMTP를 사용하는 경우 모든 트래픽이 암호화되지 않으므로 쉽게 가로채서 읽을 수 있습니다. ONTAP 9.15.1부터 SMTP(SMTPS)와 함께 TLS를 사용할 수도 있습니다. 이 경우 TCP 연결이 설정된 후 보안 채널을 활성화하는 _explicit TLS_가 사용됩니다.

일반적으로 SMTPS에 사용되는 포트는 포트 587입니다

추가 구성 고려 사항

AutoSupport를 구성할 때 고려해야 할 몇 가지 추가 사항이 있습니다.

이러한 고려 사항과 관련된 명령에 대한 자세한 내용은 을 참조하십시오"AutoSupport를 설정합니다".

이메일을 사용하여 로컬 사본을 보냅니다

AutoSupport 메시지를 NetApp에 전달하는 데 사용되는 프로토콜에 관계없이 각 메시지의 복사본을 하나 이상의 로컬 전자 메일 주소로 보낼 수도 있습니다. 예를 들어, 내부 지원 조직이나 파트너 조직에 메시지를 보낼 수 있습니다.

SMTP(또는 SMTPS)를 사용하여 NetApp에 메시지를 전달하고 해당 메시지의 로컬 이메일 사본을 보내는 경우 동일한 이메일 서버 구성이 사용됩니다.

HTTP 프록시

네트워크 구성에 따라 HTTPS 프로토콜을 사용하려면 프록시 URL을 추가로 구성해야 할 수 있습니다. HTTPS를 사용하여 AutoSupport 메시지를 기술 지원 부서에 보내고 프록시가 있는 경우 프록시의 URL을 식별해야 합니다. 프록시가 기본 포트(포트 3128)가 아닌 다른 포트를 사용하는 경우 해당 프록시의 포트를 지정할 수 있습니다. 프록시 인증에 사용할 사용자 이름과 암호를 선택적으로 지정할 수도 있습니다.

서버 인증서를 설치합니다

TLS(HTTPS 또는 SMTPS)를 사용하면 서버에서 다운로드한 인증서는 루트 CA 인증서를 기반으로 ONTAP에 의해 검증됩니다. HTTPS 또는 SMTPS를 사용하기 전에 루트 인증서가 ONTAP에 설치되어 있고 ONTAP에서 서버 인증서의 유효성을 검사할 수 있는지 확인해야 합니다. 이 유효성 검사는 서버 인증서에 서명한 CA를 기반으로

수행됩니다.

ONTAP에는 미리 설치된 루트 CA 인증서가 다수 포함되어 있습니다. 대부분의 경우 추가 구성 없이 ONTAP에서 서버의 인증서를 즉시 인식합니다. 서버 인증서 서명 방법에 따라 루트 CA 인증서 및 중간 인증서를 설치해야 할 수도 있습니다.

필요한 경우 다음 절차에 따라 인증서를 설치합니다. 필요한 모든 인증서를 클러스터 수준에서 설치해야 합니다.

예 **37.** 단계

시스템 관리자

1. System Manager에서 * 클러스터 * > * 설정 * 을 선택합니다.
2. 아래로 스크롤하여 * 보안 * 섹션으로 이동합니다.
3. 인증서 * 옆에 있는 을 선택합니다 → .
4. 신뢰할 수 있는 인증 기관 * 탭에서 * 추가 * 를 클릭합니다.
5. 가져오기 * 를 클릭하고 인증서 파일을 선택합니다.
6. 사용자 환경에 대한 구성 매개 변수를 입력합니다.
7. 추가 * 를 클릭합니다.

CLI를 참조하십시오

1. 설치를 시작합니다.

```
security certificate install -type server-ca
```

에 대한 자세한 내용은 `security certificate install` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 다음 콘솔 메시지를 찾습니다.

```
Please enter Certificate: Press <Enter> when done
```

3. 텍스트 편집기로 인증서 파일을 엽니다.
4. 다음 행을 포함하여 전체 인증서를 복사합니다.

```
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. 명령 프롬프트 후 터미널에 인증서를 붙여 넣습니다.
6. Enter * 키를 눌러 설치를 완료합니다.
7. 다음 명령 중 하나를 실행하여 인증서가 설치되었는지 확인합니다.

```
security certificate show-user-installed
```

```
security certificate show
```

에 대한 자세한 내용은 `security certificate show` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "AutoSupport를 설정합니다"
- "ONTAP 명령 참조입니다"

ONTAP AutoSupport를 설정합니다

ONTAP 클러스터를 구성하여 AutoSupport 메시지를 NetApp 기술 지원에 전달하고 이메일 복사본을 내부 지원 조직에 보낼 수 있습니다. 이러한 작업의 일부로 프로덕션 환경에서 사용하기 전에 구성을 테스트할 수도 있습니다.

이 작업에 대해

ONTAP 9.5부터 클러스터의 모든 노드에 대해 동시에 AutoSupport를 설정하고 구성할 수 있습니다. 새 노드가 클러스터에 추가되면 노드는 동일한 AutoSupport 구성을 자동으로 상속합니다. 이를 지원하기 위해 CLI 명령의 범위를 지정합니다 `system node autosupport modify` 클러스터 레벨입니다. 를 클릭합니다 `-node` 명령 옵션은 이전 버전과의 호환성을 위해 유지되지만 무시됩니다.

ONTAP 9.4 이하 릴리즈에서는 명령을 사용합니다 `system node autosupport modify` 는 각 노드에 고유합니다. 클러스터에서 ONTAP 9.4 이하를 실행 중인 경우 클러스터의 각 노드에서 AutoSupport를 활성화하고 구성해야 합니다.

시작하기 전에

NetApp에 AutoSupport 메시지를 전달하기 위한 권장 전송 구성은 HTTPS(TLS 포함 HTTP)입니다. 이 옵션은 가장 강력한 기능과 최상의 보안을 제공합니다.

검토 "AutoSupport 사용을 준비합니다" 을 참조하십시오 ONTAP.

단계

1. AutoSupport가 활성화되어 있는지 확인합니다.

```
system node autosupport modify -state enable
```

2. NetApp 기술 지원 부서에서 AutoSupport 메시지를 받으려면 다음 명령을 사용하십시오.

```
system node autosupport modify -support enable
```

AutoSupport를 AutoSupport OnDemand와 함께 사용하도록 설정하거나 코어 덤프 및 성능 아카이브 파일과 같은 대용량 파일을 기술 지원 또는 지정된 URL에 업로드하려면 이 옵션을 활성화해야 합니다.

AutoSupport OnDemand는 HTTPS 전송 프로토콜을 사용하여 기술 지원 부서로 메시지를 보내도록 구성된 경우 기본적으로 활성화되며 작동합니다.

3. NetApp 기술 지원 부서에서 AutoSupport 메시지를 받도록 설정한 경우 이러한 메시지에 사용할 전송 프로토콜을 지정합니다.

다음 옵션 중에서 선택할 수 있습니다.

원하는 작업	그런 다음 'system node AutoSupport modify' 명령어의 다음 파라미터를 설정한다…
기본 HTTPS 프로토콜을 사용합니다	a. '-transport'를 'https'로 설정합니다. b. 프록시를 사용하는 경우 프록시 URL로 -proxy-url을 설정합니다. 이 구성은 AutoSupport OnDemand와의 통신 및 대용량 파일 업로드를 지원합니다.
SMTP를 사용합니다	'-transport'를 'MTP'로 설정합니다. 이 구성은 AutoSupport OnDemand 또는 대용량 파일 업로드를 지원하지 않습니다.

4. 내부 지원 조직 또는 지원 파트너가 AutoSupport 메시지를 받도록 하려면 다음 작업을 수행합니다.
   a. 'system node AutoSupport modify' 명령의 다음 매개 변수를 설정하여 조직의 수신자를 식별합니다.

이 매개 변수 설정…	이거면…
'-to'	내부 지원 조직에서 주요 AutoSupport 메시지를 받을 최대 5개의 쉼표로 구분된 개별 이메일 주소 또는 배포 목록
'-noteto'	내부 지원 조직에서 최대 5개의 쉼표로 구분된 개별 이메일 주소 또는 배포 목록을 통해 휴대폰과 기타 모바일 장치용으로 설계된 주요 AutoSupport 메시지의 축약된 버전을 받을 수 있습니다
파트너 주소	지원 파트너 조직에서 모든 AutoSupport 메시지를 쉼표로 구분하여 최대 5개의 개별 이메일 주소 또는 배포 목록을 받을 수 있습니다

   b. 'system node AutoSupport destinations show' 명령을 사용하여 대상을 나열하여 주소가 올바르게 구성되었는지 확인합니다.
5. 이전 단계에서 내부 지원 조직의 받는 사람 주소를 구성하거나 기술 지원 메시지의 SMTP 전송을 선택한 경우 명령의 다음 매개 변수를 설정하여 SMTP를 `system node autosupport modify` 구성합니다.
   - 메일 호스트를 쉼표로 구분하여 하나 이상의 메일 호스트로 설정합니다.

     최대 5개까지 설정할 수 있습니다.

   메일 호스트 이름 뒤에 콜론과 포트 번호를 지정하여 각 메일 호스트에 대한 포트 값을 구성할 수 있습니다. 예를 들어, mymailhost.example.com:5678`, 여기서 5678은 메일 호스트의 포트입니다.

   - AutoSupport 메시지를 보내는 e-메일 주소로 '-from'을 설정합니다.
6. DNS를 구성합니다.
7. 필요에 따라 특정 설정을 변경하려면 명령 옵션을 추가합니다.

이 작업을 수행하려면…	그런 다음 'system node AutoSupport modify' 명령어의 다음 파라미터를 설정한다…
메시지에서 중요한 데이터를 제거, 마스킹 또는 인코딩하여 개인 데이터를 숨깁니다	설정 `-remove-private-data` 를 선택합니다 `true`. 에서 변경한 경우 `false` 를 선택합니다 `true`모든 AutoSupport 기록 및 모든 관련 파일이 삭제됩니다.
Periodic AutoSupport 메시지로 성능 데이터 전송을 중지합니다	-perf를 false로 설정합니다.

8. SMTP를 사용하여 NetApp에 AutoSupport 메시지를 전달하는 경우 보안을 강화하기 위해 TLS를 선택적으로 활성화할 수 있습니다.
   a. 새 매개변수에 사용할 수 있는 값을 표시합니다.

   ```
   cluster1::> system node autosupport modify -smtp-encryption ?
   ```

   b. SMTP 메시지 배달을 위해 TLS 활성화:

   ```
   cluster1::> system node autosupport modify -smtp-encryption start_tls
   ```

   c. 현재 구성을 표시합니다.

   ```
   cluster1::> system node autosupport show -fields smtp-encryption
   ```

9. 'system node AutoSupport show' 명령을 '-node' 매개변수와 함께 사용하여 전체 설정을 확인한다.
10. 'system node AutoSupport check show' 명령어를 사용해 AutoSupport 작동을 확인한다.

    문제가 보고되면 'system node AutoSupport check show-details' 명령어를 사용하여 더 많은 정보를 볼 수 있다.

11. AutoSupport 메시지가 전송 및 수신되고 있는지 테스트합니다.
    a. 를 사용합니다 `system node autosupport invoke` 명령과 함께 `-type` 매개 변수를 로 설정합니다 `test`:

    ```
    cluster1::> system node autosupport invoke -type test -node node1
    ```

    b. NetApp에서 AutoSupport 메시지를 수신하는지 확인합니다.

    ```
    system node autosupport history show -node local
    ```

    최근 나가는 AutoSupport 메시지의 상태는 모든 해당 프로토콜 대상에 대해 '성공적으로 완료'로 변경되어야 합니다.

c. 필요에 따라 에 구성한 모든 주소의 이메일을 확인하여 AutoSupport 메시지가 내부 지원 조직 또는 지원 파트너에게 전송되는지 확인합니다 `-to`, `-noteto`, 또는 `-partner-address` 의 매개 변수 `system node autosupport modify` 명령.

관련 정보

- "AutoSupport 사용을 준비합니다"
- "ONTAP 명령 참조입니다"

구성

ONTAP AutoSupport 설정을 관리합니다

System Manager를 사용하여 AutoSupport 계정의 설정을 관리할 수 있습니다.

System Manager에서 사용할 수 없는 설정을 포함하여 AutoSupport 구성 옵션에 대한 자세한 내용은 의 "ONTAP 명령 참조입니다" 을 참조하십시오 `system-node-autosupport-modify`.

AutoSupport 설정을 봅니다

시스템 관리자를 사용하여 AutoSupport 계정의 설정을 볼 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 클릭합니다.

   AutoSupport* 섹션에 다음 정보가 표시됩니다.

   - 상태
   - 전송 프로토콜
   - 프록시 서버
   - 보낸 사람 이메일 주소

2. AutoSupport * 섹션에서 을 선택한 다음 * 추가 옵션 * 을 ⋮선택합니다.

   AutoSupport 연결 및 전자 메일 설정에 대한 추가 정보가 표시됩니다. 또한 메시지의 전송 기록이 나열됩니다.

AutoSupport 데이터를 생성하고 전송합니다

System Manager에서 AutoSupport 메시지 생성을 시작하고 데이터가 수집되는 클러스터 노드 또는 노드를 선택할 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 섹션에서 을 ⋮선택한 다음 * 생성 및 전송 * 을 선택합니다.
3. 제목을 입력합니다.
4. 데이터를 수집할 노드를 지정하려면 * 데이터 수집 위치 * 아래의 확인란을 선택합니다.

AutoSupport 연결을 테스트합니다

System Manager에서 테스트 메시지를 보내 AutoSupport에 대한 연결을 확인할 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 클릭합니다.
2. AutoSupport * 섹션에서 을 선택한 다음 * Test Connectivity * 를 선택합니다.
3. 메시지의 제목을 입력합니다.

AutoSupport를 활성화 또는 비활성화합니다

AutoSupport는 가능한 구성 문제의 사전 식별 및 신속한 지원 케이스 해결을 포함하여 NetApp 고객에게 검증된 비즈니스 이점을 제공합니다. AutoSupport는 새로운 시스템에서 기본적으로 활성화되어 있습니다. 필요한 경우, System Manager를 사용하여 AutoSupport의 기능을 해제하여 스토리지 시스템의 상태를 모니터링하고 알림 메시지를 보낼 수 있습니다. AutoSupport를 비활성화한 후 다시 활성화할 수 있습니다.

이 작업에 대해

AutoSupport를 사용하지 않도록 설정하기 전에 NetApp Call-Home 시스템을 끄면 다음과 같은 이점을 얻을 수 있다는 점에 유의해야 합니다.

- * 상태 모니터링 *: AutoSupport는 스토리지 시스템의 상태를 모니터링하고 기술 지원 부서 및 내부 지원 부서에 알림을 전송합니다.
- * 자동화 *: AutoSupport는 지원 사례 보고를 자동화합니다. 대부분의 지원 케이스는 고객이 문제를 인지하기 전에 자동으로 열립니다.
- * 신속한 해결 *: AutoSupport 데이터를 전송하는 시스템은 AutoSupport 데이터를 보내지 않는 시스템에 비해 절반의 시간 내에 지원 사례를 해결할 수 있습니다.
- * 더 빠른 업그레이드 *: AutoSupport는 System Manager의 버전 업그레이드, 애드온, 갱신 및 펌웨어 업데이트 자동화와 같은 고객 셀프 서비스 워크플로를 지원합니다.
- 추가 기능: 다른 도구의 특정 기능은 AutoSupport 활성화된 경우에만 작동합니다(예: NetApp 콘솔의 일부 워크플로).

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 섹션에서 을 선택한 다음 * 사용 안 함 * 을 선택합니다.
3. AutoSupport를 다시 활성화하려면 * AutoSupport * 섹션에서 를 선택한 다음 * 활성화 * 를 선택합니다.

지원 케이스 생성을 억제합니다

ONTAP 9.10.1부터 System Manager를 사용하여 AutoSupport에 요청을 보내 지원 케이스 생성을 억제할 수 있습니다.

이 작업에 대해

지원 케이스 생성을 억제하려면 노드 및 억제를 수행할 시간 수를 지정합니다.

시스템에서 유지 관리를 수행하는 동안 AutoSupport에서 자동화된 케이스를 생성하지 않으려는 경우 지원 케이스를 억제하면 특히 유용합니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 섹션에서 를 ⋮ 선택한 다음 * 지원 케이스 생성 안 함 * 을 선택합니다.
3. 억제가 발생할 시간을 입력합니다.
4. 기능 억제를 수행할 노드를 선택합니다.

지원 케이스 생성을 재개합니다

ONTAP 9.10.1부터 System Manager를 사용하면 AutoSupport에서 지원 케이스가 억제된 경우 해당 케이스를 다시 생성할 수 있습니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 섹션에서 를 ⋮ 선택한 다음 * 지원 케이스 생성 재개 * 를 선택합니다.
3. 생성을 재개할 노드를 선택합니다.

AutoSupport 설정을 편집합니다

시스템 관리자를 사용하여 AutoSupport 계정의 연결 및 이메일 설정을 수정할 수 있습니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. AutoSupport * 섹션에서 을 선택한 다음 * 추가 옵션 * 을 ⋮ 선택합니다.
3. 연결 * 섹션 또는 * 이메일 * 섹션에서 을 Edit 선택하여 어느 섹션의 설정을 수정합니다.

관련 정보

- "AutoSupport 사용을 준비합니다"
- "AutoSupport를 설정합니다"

예약된 유지 관리 기간 동안 **ONTAP AutoSupport** 케이스 생성을 억제합니다

AutoSupport 케이스 억제를 사용하면 예약된 유지 관리 기간 동안 트리거된 AutoSupport 메시지에 의해 불필요한 케이스가 생성되지 않도록 할 수 있습니다.

단계

1. 텍스트 문자열을 사용하여 AutoSupport 메시지를 수동으로 `MAINT=xh`호출합니다. 여기서 는 유지 보수 기간(시간) 입니다. `x <node>`를 AutoSupport 메시지를 보낼 노드의 이름으로 바꿉니다.

```
system node autosupport invoke -node <node> -message MAINT=xh
```

관련 정보

- "ONTAP 명령 참조입니다"
- "예약된 유지 보수 기간 동안 자동 케이스 생성을 억제하는 방법"

AutoSupport를 사용하여 파일을 업로드합니다

ONTAP AutoSupport 코어 덤프 파일을 업로드합니다

코어 덤프 파일이 저장되면 이벤트 메시지가 생성됩니다. AutoSupport 서비스가 활성화되어 NetApp 지원으로 메시지를 보내도록 구성된 경우 AutoSupport 메시지가 전송되고 자동 이메일 확인이 전송됩니다.

시작하기 전에

- 다음 설정으로 AutoSupport를 설정했습니다.
  - AutoSupport가 노드에서 활성화되어 있습니다.
  - AutoSupport는 기술 지원 부서에 메시지를 전송하도록 구성되어 있습니다.
  - AutoSupport는 HTTPS 전송 프로토콜을 사용하도록 구성되어 있습니다.

    코어 덤프 파일과 같이 큰 파일이 포함된 메시지를 보낼 때는 SMTP 전송 프로토콜이 지원되지 않습니다.

이 작업에 대해

NetApp 지원 요청이 있을 경우 'system node AutoSupport invoke-core-upload' 명령을 사용하여 HTTPS를 통해 코어 덤프 파일을 업로드할 수도 AutoSupport 있습니다.

"분석을 위해 ONTAP 9 코어 파일을 업로드하는 방법"

단계

1. system node coredump show 명령을 사용하여 노드의 코어 덤프 파일을 봅니다.

   다음 예에서는 로컬 노드에 대해 코어 덤프 파일이 표시됩니다.

   ```
   cluster1::> system node coredump show -node local
   Node:Type Core Name Saved Panic Time
   --------- ------------------------------------------- -----
   -----------------
   node:kernel
   core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
   ```

2. 'system node AutoSupport invoke-core-upload' 명령어를 사용해 AutoSupport 메시지를 생성하고 core dump 파일을 업로드 한다.

   다음 예에서는 AutoSupport 메시지가 생성되어 기술 지원인 기본 위치로 전송되고 코어 덤프 파일이 NetApp Support 사이트인 기본 위치에 업로드됩니다.

   ```
   cluster1::> system node autosupport invoke-core-upload -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

   다음 예에서는 AutoSupport 메시지가 생성되어 URI에 지정된 위치로 전송되며 코어 덤프 파일이 URI에 업로드됩니다.

```
cluster1::> system node autosupport invoke-core-upload -uri
https//files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

ONTAP AutoSupport 성능 아카이브 파일을 업로드합니다

성능 아카이브가 포함된 AutoSupport 메시지를 생성하고 보낼 수 있습니다. 기본적으로 NetApp 기술 지원에는 AutoSupport 메시지가 표시되고 성능 아카이브는 NetApp Support 사이트에 업로드됩니다. 메시지에 대한 대체 대상을 지정하고 업로드할 수 있습니다.

시작하기 전에

- 다음 설정으로 AutoSupport를 설정해야 합니다.
  - AutoSupport가 노드에서 활성화되어 있습니다.
  - AutoSupport는 기술 지원 부서에 메시지를 전송하도록 구성되어 있습니다.
  - AutoSupport는 HTTPS 전송 프로토콜을 사용하도록 구성되어 있습니다.

    성능 아카이브 파일과 같은 대용량 파일이 포함된 메시지를 보낼 때는 SMTP 전송 프로토콜이 지원되지 않습니다.

이 작업에 대해

업로드할 성능 아카이브 데이터의 시작 날짜를 지정해야 합니다. 대부분의 스토리지 시스템은 성능 아카이브를 2주 동안 유지하여 시작 날짜를 최대 2주 전에 지정할 수 있습니다. 예를 들어 오늘이 1월 15일인 경우 1월 2일의 시작 날짜를 지정할 수 있습니다.

단계

1. 'system node AutoSupport invoke-performance-archive' 명령어를 사용하여 AutoSupport 메시지를 생성하고 성능 아카이브 파일을 업로드합니다.

   다음 예에서는 2015년 1월 12일부터 4시간 동안 성능 아카이브 파일이 AutoSupport 메시지에 추가되고 NetApp Support 사이트인 기본 위치에 업로드됩니다.

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   다음 예에서는 2015년 1월 12일부터 4시간 동안의 성능 아카이브 파일이 AutoSupport 메시지에 추가되고 URI에 의해 지정된 위치에 업로드됩니다.

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h -uri
   https://files.company.com
   ```

문제 해결

메시지가 수신되지 않을 때 **ONTAP AutoSupport** 문제를 해결합니다

시스템에서 AutoSupport 메시지를 보내지 않는 경우 AutoSupport에서 메시지를 생성할 수 없거나 메시지를 전달할 수 없기 때문에 메시지를 보낼 수 있는지 여부를 확인할 수 있습니다.

단계

1. System node AutoSupport history show 명령을 사용하여 메시지의 delivery 상태를 확인한다.
2. 상태를 읽습니다.

이 상태입니다	의미합니다
초기화 중입니다	수집 프로세스가 시작됩니다. 이 상태가 일시적일 경우 모든 것이 좋습니다. 그러나 이 상태가 지속되면 문제가 있는 것입니다.
수집 실패	AutoSupport가 스풀 디렉터리에 AutoSupport 콘텐츠를 만들 수 없습니다. 'system node AutoSupport history show-detail' 명령어를 입력하여 AutoSupport가 수집하려는 정보를 확인할 수 있다.
수집 중입니다	AutoSupport가 AutoSupport 콘텐츠를 수집하고 있습니다. 'system node AutoSupport manifest show' 명령어를 입력하여 AutoSupport가 수집하는 정보를 확인할 수 있다.
대기열에 있습니다	AutoSupport 메시지는 전달 대기 상태이지만 아직 전달되지 않았습니다.
전송 중입니다	AutoSupport가 현재 메시지를 전달하고 있습니다.
전송됨 - 성공했습니다	AutoSupport가 메시지를 성공적으로 전달했습니다. 'system node AutoSupport history show-delivery' 명령어를 입력하여 AutoSupport가 메시지를 전달한 위치를 확인할 수 있다.
무시	AutoSupport에 메시지의 대상이 없습니다. 'system node AutoSupport history show-delivery' 명령어를 입력하여 전달 세부 정보를 볼 수 있다.
다시 대기 중입니다	AutoSupport가 메시지를 전달하려고 했지만 시도가 실패했습니다. 따라서 AutoSupport는 다른 시도를 위해 메시지를 배달 대기열에 다시 배치했습니다. System node AutoSupport history show 명령을 입력하여 오류를 확인할 수 있다.
전송 - 실패	AutoSupport가 지정된 횟수만큼 메시지를 배달하지 못하여 메시지 전달 시도를 중지했습니다. System node AutoSupport history show 명령을 입력하여 오류를 확인할 수 있다.
OnDemand - 무시	AutoSupport 메시지가 처리되었지만 AutoSupport OnDemand 서비스에서 무시하도록 선택했습니다.

3. 다음 작업 중 하나를 수행합니다.

이 상태를 표시합니다	이렇게 하십시오
초기화 또는 수집 실패	AutoSupport에서 메시지를 생성할 수 없으므로 NetApp 지원에 문의하십시오. 다음 기술 자료 문서를 언급합니다. "AutoSupport에서 전송 실패: 초기화 중에 상태가 고착됨"
무시, 다시 대기 중 또는 전송에 실패했습니다	AutoSupport에서 메시지를 전달할 수 없으므로 SMTP, HTTP 또는 HTTPS에 대해 대상이 올바르게 구성되었는지 확인합니다.

HTTPS를 통한 **ONTAP AutoSupport** 메시지 전달 문제 해결

시스템에서 예상 AutoSupport 메시지를 보내지 않고 HTTPS를 사용 중이거나 자동 업데이트 기능이 작동하지 않는 경우 여러 설정을 확인하여 문제를 해결할 수 있습니다.

시작하기 전에

기본 네트워크 연결 및 DNS 조회를 확인해야 합니다.

- 노드 관리 LIF가 운영 및 관리 상태이어야 합니다.
- 클러스터 관리 LIF(노드의 LIF가 아님)에서 동일한 서브넷에 있는 기능 호스트를 ping할 수 있어야 합니다.
- 클러스터 관리 LIF에서 서브넷 외부의 기능 호스트를 Ping할 수 있어야 합니다.
- IP 주소가 아닌 호스트의 이름을 사용하여 클러스터 관리 LIF에서 서브넷 외부의 기능 호스트를 Ping할 수 있어야 합니다.

이 작업에 대해

다음 단계는 AutoSupport에서 메시지를 생성할 수 있지만 HTTPS를 통해 메시지를 전달할 수 없는 경우를 위한 것입니다.

오류가 발생하거나 이 절차의 단계를 완료할 수 없는 경우 다음 단계로 진행하기 전에 문제를 확인하고 해결하십시오.

단계

1. AutoSupport 하위 시스템의 세부 상태를 표시합니다.

   'system node AutoSupport check show-details

   여기에는 테스트 메시지를 전송하고 AutoSupport 구성 설정에서 발생할 수 있는 오류 목록을 제공하여 AutoSupport 대상에 대한 연결을 확인하는 작업이 포함됩니다.

2. 노드 관리 LIF의 상태를 확인합니다.

```
network interface show -home-node local -role node-mgmt -fields
vserver,lif,status-oper,status-admin,address,role
```

`status-oper`및 `status-admin` 필드가 `up` 반환됩니다. 에 대한 자세한 내용은 `up` link:https://docs.netapp.com/us-en/ontap-cli/up.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

3. 나중에 사용할 수 있도록 SVM 이름, LIF 이름 및 LIF IP 주소를 기록합니다.
4. DNS가 올바르게 설정 및 구성되었는지 확인합니다.

```
vserver services name-service dns show
```

5. AutoSupport 메시지가 반환한 모든 오류를 해결합니다.

```
system node autosupport history show -node * -fields node,seq-
num,destination,last-update,status,error
```

반환된 오류 문제 해결에 대한 자세한 내용은 을 "ONTAP AutoSupport(전송 HTTPS 및 HTTP) 해상도 안내서입니다"참조하십시오.

6. 클러스터가 필요한 서버와 인터넷에 모두 액세스할 수 있는지 확인합니다.
   a. 'network traceroute-lif node-management_LIF-destination DNS server
   b. 네트워크 traceroute-lif node_management_LIF-destination support.netapp.com`

      주소인 upport.netapp.com` 자체는 ping/traceroute에 응답하지 않지만, per-hop 정보는 가치가 있다.

   c. '시스템 노드 AutoSupport show-fields proxy-url
   d. 'network traceroute-node_management_LIF-destination proxy_url

이러한 라우트가 작동하지 않는 경우 대부분의 타사 네트워크 클라이언트에서 발견되는 또는 `tracert` 유틸리티를 사용하여 클러스터와 동일한 서브넷의 작동 중인 호스트에서 동일한 라우트를 `traceroute` 시도합니다. 그런 다음 문제가 네트워크 구성 문제인지 아니면 클러스터 구성 문제인지 확인할 수 있습니다. 에 대한 자세한 내용은 `network traceroute` "ONTAP 명령 참조입니다"을 참조하십시오.

7. AutoSupport 전송 프로토콜에 HTTPS를 사용하는 경우 HTTPS 트래픽이 네트워크를 종료할 수 있는지 확인합니다.
   a. 클러스터 관리 LIF와 동일한 서브넷에 있는 웹 클라이언트를 구성합니다.

      동일한 프록시 서버, 사용자 이름, 암호 및 포트 사용을 포함하여 모든 구성 매개 변수가 AutoSupport 구성과 동일한 값인지 확인합니다.

   b. 웹 클라이언트를 사용하여 'https://support.netapp.com` 액세스합니다.

      접근이 성공할 것입니다. 그렇지 않은 경우 모든 방화벽이 HTTPS 및 DNS 트래픽을 허용하도록 올바르게 구성되었는지 확인하고, 프록시 서버가 올바르게 구성되었는지 확인하세요. support.netapp.com에 대한 정적 이름 확인 구성에 대한 자세한 내용은 다음을 참조하세요."NetApp 지식 기반: ONTAP 에서

support.netapp.com에 대한 HOST 항목을 추가하려면 어떻게 해야 하나요?"

8. ONTAP 9.10.1부터 자동 업데이트를 사용하도록 설정한 경우 다음 추가 URL에 HTTPS 연결이 있는지 확인합니다.
   - https://support-sg-naeast.netapp.com 으로 문의하십시오
   - https://support-sg-nawest.netapp.com 으로 문의하십시오

SMTP를 통한 **ONTAP AutoSupport** 메시지 배달 문제 해결

시스템이 SMTP를 통해 AutoSupport 메시지를 전달할 수 없는 경우 여러 설정을 확인하여 문제를 해결할 수 있습니다.

시작하기 전에

기본 네트워크 연결 및 DNS 조회를 확인해야 합니다.

- 노드 관리 LIF가 운영 및 관리 상태이어야 합니다.
- 클러스터 관리 LIF(노드의 LIF가 아님)에서 동일한 서브넷에 있는 기능 호스트를 ping할 수 있어야 합니다.
- 클러스터 관리 LIF에서 서브넷 외부의 기능 호스트를 Ping할 수 있어야 합니다.
- IP 주소가 아닌 호스트의 이름을 사용하여 클러스터 관리 LIF에서 서브넷 외부의 기능 호스트를 Ping할 수 있어야 합니다.

이 작업에 대해

다음 단계는 AutoSupport에서 메시지를 생성할 수 있지만 SMTP를 통해 메시지를 전달할 수 없는 경우를 위한 것입니다.

오류가 발생하거나 이 절차의 단계를 완료할 수 없는 경우 다음 단계로 진행하기 전에 문제를 확인하고 해결하십시오.

별도로 지정하지 않는 한 모든 명령은 ONTAP 명령줄 인터페이스에 입력됩니다.

단계

1. 노드 관리 LIF의 상태를 확인합니다.

   '* 네트워크 인터페이스 show-home-node local-role node-mgmt-fields vserver, lif, status-oper, status-admin, address, role *

   `status-oper`및 `status-admin` 필드가 `up` 반환됩니다. 에 대한 자세한 내용은 `up` link:https://docs.netapp.com/us-en/ontap-cli/up.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

2. 나중에 사용할 수 있도록 SVM 이름, LIF 이름 및 LIF IP 주소를 기록합니다.
3. DNS가 올바르게 설정 및 구성되었는지 확인합니다.

   ``vserver services name-service dns show *'’를 참조하십시오

4. AutoSupport에서 사용하도록 구성된 모든 서버를 표시합니다.

``시스템 노드 AutoSupport 표시 필드 메일-호스트*'

표시된 모든 서버 이름을 기록합니다.

5. 이전 단계에서 표시한 각 서버 및 'upport.netapp.com` 에 대해 노드에서 서버 또는 URL에 연결할 수 있는지 확인합니다.

   '* network traceroute-node local-destination_server_name_*'

   이러한 경로 중 하나라도 작동하지 않는 경우, 대부분의 타사 네트워크 클라이언트에 있는 ""traceroute"" 또는 ""tracert""" 유틸리티를 사용하여 클러스터와 동일한 서브넷의 작동 호스트에서 동일한 경로를 시도해 보십시오. 이렇게 하면 문제가 네트워크 구성에 있는지 또는 클러스터 구성에 있는지 여부를 확인할 수 있습니다.

6. 메일 호스트로 지정된 호스트에 로그인하고 SMTP 요청을 처리할 수 있는지 확인합니다.

   ``netstat-Aan|grep 25 *'

   수신 SMTP 포트 번호는 25입니다.

   다음 텍스트와 유사한 메시지가 표시됩니다.

   ```
   ff64878c tcp        0      0  *.25    *.*    LISTEN.
   ```

7. 다른 호스트에서 메일 호스트의 SMTP 포트로 텔넷 세션을 엽니다.

   '* telnet_mailhost_25 * '

   다음 텍스트와 유사한 메시지가 표시됩니다.

   ```
   220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
   10:49:04 PST
   ```

8. 텔넷 프롬프트에서 메일 호스트로부터 메시지를 전달할 수 있는지 확인합니다.

   ' * HELO_DOMAIN_NAME_ * '

   (* 메일 보낸 사람: _ your_email_address_ *)

   (* RCPT to:autosupport@netapp.com *)

   domain_name은 네트워크의 도메인 이름입니다.

   Relaying이 denied로 되어 있는 오류가 반환되면 메일 호스트에서 relaying이 활성화되지 않습니다. 시스템 관리자에게 문의하십시오.

9. 텔넷 프롬프트에서 테스트 메시지를 보냅니다.

   ' * 데이터 * '

   시험대상자: 시험 *' 이것은 시험이다 *'

`. * '

> 줄의 마지막 기간(.)을 직접 입력해야 합니다. 이 기간은 메일 호스트에 메시지가 완료되었음을 나타냅니다.

오류가 반환되면 메일 호스트가 올바르게 구성되지 않은 것입니다. 시스템 관리자에게 문의하십시오.

10. ONTAP 명령줄 인터페이스에서 AutoSupport 테스트 메시지를 액세스 권한이 있는 신뢰할 수 있는 전자 메일 주소로 보냅니다.

    '* 시스템 노드 AutoSupport invoke-node local-type test*'

11. 시도의 순서 번호를 찾습니다.

    ``시스템 노드 AutoSupport 이력 표시 노드 로컬 대상 SMTP*'

    타임 스탬프를 기준으로 시도 순서 번호를 찾습니다. 가장 최근에 시도한 시도일 것입니다.

12. 테스트 메시지 시도에 대한 오류를 표시합니다.

    '* system node AutoSupport history show -node local -seq -num seq_num -fields error *

    표시된 오류가 '로그인 거부'인 경우 SMTP 서버가 클러스터 관리 LIF의 전송 요청을 수락하지 않습니다. 전송 프로토콜로 HTTPS 사용을 변경하지 않으려면 사이트 네트워크 관리자에게 문의하여 이 문제를 해결할 SMTP 게이트웨이를 구성하십시오.

    이 테스트가 성공했지만 mailto:autosupport@netapp.com 으로 전송된 동일한 메시지가 없으면 모든 SMTP 메일 호스트에서 SMTP 릴레이가 활성화되어 있는지 확인하거나 HTTPS를 전송 프로토콜로 사용하십시오.

    로컬로 관리되는 전자 메일 계정에 대한 메시지도 성공하지 못한 경우 SMTP 서버가 다음 두 특성을 모두 사용하여 첨부 파일을 전달하도록 구성되었는지 확인합니다.

    - "7z" 접미사
    - "application/x-7x-compressed" MIME 형식.

ONTAP AutoSupport 하위 시스템의 문제를 해결합니다

'system node check show' 명령어를 이용하여 AutoSupport 구성 및 제공과 관련된 모든 문제를 확인하고 해결할 수 있다.

단계

1. 다음 명령을 사용하여 AutoSupport 하위 시스템의 상태를 표시합니다.

이 명령 사용...	수행할 작업...
'시스템 노드 AutoSupport check show'	AutoSupport HTTPS 대상, AutoSupport SMTP 대상, AutoSupport OnDemand 서버 및 AutoSupport 구성과 같은 AutoSupport 하위 시스템의 전체 상태를 표시합니다

이 명령 사용...	수행할 작업...
'system node AutoSupport check show-details	오류에 대한 자세한 설명과 수정 조치 등 AutoSupport 하위 시스템의 세부 상태를 표시합니다

상태 모니터링

ONTAP 시스템 상태 모니터링에 대해 알아보십시오

상태 모니터는 클러스터의 특정 중요한 상태를 능동적으로 모니터링하고 장애 또는 위험을 감지하는 경우 경고를 표시합니다. 활성 경고가 있는 경우 시스템 상태는 클러스터에 대한 성능 저하 상태를 보고합니다. 알림에는 저하된 시스템 상태에 응답하는 데 필요한 정보가 포함됩니다.

상태가 성능 저하인 경우 가능한 원인 및 권장 복구 조치를 포함하여 문제에 대한 세부 정보를 볼 수 있습니다. 문제를 해결한 후 시스템 상태는 자동으로 OK로 복귀합니다.

시스템 상태는 여러 개의 개별 상태 모니터를 반영합니다. 개별 상태 모니터의 성능 저하 상태는 전체 시스템 상태의 성능 저하 상태를 야기합니다.

ONTAP가 클러스터에서 시스템 상태 모니터링을 위해 클러스터 스위치를 지원하는 방법에 대한 자세한 내용은 _Hardware Universe_를 참조하십시오.

"Hardware Universe에서 지원되는 스위치입니다"

CSMM(Cluster Switch Health Monitor) AutoSupport 메시지의 원인과 이러한 경고를 해결하는 데 필요한 조치에 대한 자세한 내용은 기술 자료 문서를 참조하십시오.

"AutoSupport 메시지: 상태 모니터 프로세스 CSMM"

ONTAP 상태 모니터링 구성 요소에 대해 알아보십시오

개별 상태 모니터에는 특정 조건이 발생할 때 알림을 트리거하는 일련의 정책이 있습니다. 상태 모니터링 작동 방식을 이해하면 문제에 대응하고 향후 경고를 제어하는 데 도움이 됩니다.

상태 모니터링은 다음과 같은 구성 요소로 이루어집니다.

- 개별 상태는 특정 서브시스템에 대한 모니터링을 하며, 각 하위 시스템은 자체 상태를 가지고 있습니다

  예를 들어, 스토리지 서브시스템에는 노드 연결 상태 모니터가 있습니다.

- 개별 상태 모니터의 상태를 통합하는 전체 시스템 상태 모니터입니다

  단일 서브시스템의 성능 저하 상태가 전체 시스템의 성능 저하 상태를 초래하게 됩니다. 하위 시스템에 경고가 없으면 전체 시스템 상태가 정상입니다.

각 상태 모니터는 다음과 같은 주요 요소로 구성됩니다.

- 상태 모니터에서 발생할 수 있는 경고입니다

각 알림에는 알림의 심각도 및 가능한 원인과 같은 세부 정보가 포함된 정의가 있습니다.

- 각 알림이 트리거되는 시기를 식별하는 상태 정책입니다

  각 상태 정책에는 경고를 트리거하는 정확한 조건이나 변경 조건인 규칙 식이 있습니다.

상태 모니터는 서브시스템의 리소스에 대한 상태 또는 상태 변경을 지속적으로 모니터링 및 검증합니다. 상태 또는 상태 변경이 상태 정책의 규칙 식과 일치하면 상태 모니터에서 알림을 발생시킵니다. 알림을 통해 하위 시스템의 상태 및 전체 시스템 상태가 성능 저하 상태가 됩니다.

ONTAP 시스템 상태 경고 응답에 대해 알아보십시오

시스템 상태 경고가 발생하면 이를 확인하고, 자세히 알아보고, 기본 상태를 수리하고, 문제가 다시 발생하지 않도록 할 수 있습니다.

상태 모니터에서 알림을 발생시키면 다음 방법 중 하나를 사용하여 응답할 수 있습니다.

- 영향을 받는 리소스, 경고 심각도, 가능한 원인, 가능한 영향 및 수정 조치가 포함된 알림에 대한 정보를 얻을 수 있습니다.
- 알림이 발생한 시간, 다른 사용자가 이미 알림을 확인했는지 여부 등 알림에 대한 자세한 정보를 확인합니다.
- 특정 쉘프 또는 디스크와 같은 영향을 받는 리소스 또는 하위 시스템의 상태에 대한 상태 관련 정보를 가져옵니다.
- 누군가 문제를 해결하고 있음을 알리고 자신을 "확인자"로 식별합니다.
- 연결 문제를 해결하기 위해 케이블 연결 문제 해결 등 알림에 제공된 수정 조치를 수행하여 문제를 해결합니다.
- 시스템에서 자동으로 경고를 지우지 않은 경우 해당 경고를 삭제합니다.
- 알림을 표시하지 않도록 하여 하위 시스템의 상태에 영향을 주지 않도록 합니다.

  기능 억제는 문제를 이해할 때 유용합니다. 경고를 표시하지 않으면 알림이 계속 발생할 수 있지만 하위 시스템 상태가 "ok-with-suppressed"로 표시됩니다.

ONTAP 시스템 상태 경고 사용자 지정에 대해 자세히 알아보십시오

알림이 트리거되는 시기를 정의하는 시스템 상태 정책을 설정 및 해제하여 상태 모니터에서 생성되는 알림을 제어할 수 있습니다. 이를 통해 특정 환경에 맞게 상태 모니터링 시스템을 사용자 지정할 수 있습니다.

생성된 알림에 대한 세부 정보를 표시하거나 특정 상태 모니터, 노드 또는 알림 ID에 대한 정책 정의를 표시하여 정책의 이름을 확인할 수 있습니다.

상태 정책을 사용하지 않도록 설정하는 것은 알림을 표시하지 않는 것과 다릅니다. 알림을 표시하지 않으면 하위 시스템의 상태에 영향을 주지 않지만 알림은 계속 발생할 수 있습니다.

정책을 사용하지 않도록 설정하면 해당 정책 규칙 식에 정의된 조건이나 상태가 더 이상 알림을 트리거하지 않습니다.

비활성화하려는 알림의 예

예를 들어 사용자에게 유용하지 않은 경고가 발생한다고 가정합니다. 'system health alert show –instance' 명령을 사용하여 경고의 정책 ID를 가져옵니다. 'system health policy definition show' 명령에서 정책 ID를 사용하여 정책에 대한 정보를 확인할 수 있습니다. 규칙 식 및 정책에 대한 기타 정보를 검토한 후 정책을 사용하지 않도록 설정합니다.

'system health policy definition modify' 명령을 사용하여 정책을 사용하지 않도록 설정할 수 있습니다.

관련 정보

- "시스템 상태 경고 표시"

ONTAP AutoSupport 상태 경고 트리거에 대해 자세히 알아보십시오

시스템 상태 알림은 EMS(이벤트 관리 시스템)에서 AutoSupport 메시지 및 이벤트를 트리거하여, 상태 모니터링 시스템을 직접 사용하는 것 외에도 AutoSupport 메시지 및 EMS를 사용하여 시스템의 상태를 모니터링할 수 있습니다.

경고 후 5분 내에 AutoSupport 메시지가 전송됩니다. AutoSupport 메시지에는 이전 AutoSupport 메시지 이후에 생성된 모든 경고가 포함됩니다. 단, 이전 주 내에 동일한 리소스 및 가능한 원인에 대한 경고를 복제하는 알림은 제외됩니다.

일부 알림은 AutoSupport 메시지를 트리거하지 않습니다. 상태 정책에서 AutoSupport 메시지 전송을 사용하지 않도록 설정한 경우 알림은 AutoSupport 메시지를 트리거하지 않습니다. 예를 들어, 상태 정책은 기본적으로 AutoSupport 메시지를 사용하지 않도록 설정할 수 있습니다. 이 경우 문제가 발생할 때 AutoSupport에서 이미 메시지를 생성하므로 'system health policy definition modify' 명령을 사용하여 AutoSupport 메시지를 트리거하지 않도록 정책을 구성할 수 있습니다.

'system health AutoSupport trigger history show' 명령어를 사용해 지난 주에 보낸 모든 경고 트리거 AutoSupport 메시지의 목록을 볼 수 있다.

또한 알림은 EMS에 대한 이벤트 생성을 트리거합니다. 알림은 알림이 생성될 때마다 그리고 경고가 삭제될 때마다 생성됩니다.

사용 가능한 ONTAP 클러스터 상태 모니터에 대해 자세히 알아보십시오

클러스터의 여러 부분을 모니터링하는 상태 모니터가 여러 개 있습니다. 상태 모니터는 이벤트를 감지하고, 사용자에게 경고를 보내고, 이벤트를 삭제하여 ONTAP 시스템 내의 오류를 복구할 수 있도록 도와줍니다.

상태 모니터 이름(식별자)	하위 시스템 이름(식별자)	목적
이더넷 스위치	스위치(스위치 - 상태)	ONTAP 이더넷 스위치 상태 모니터(CSHM)는 분석을 위한 로그를 수집하는 동안 클러스터 및 스토리지 네트워크 스위치의 상태를 모니터링합니다. 기본적으로 CSHM은 5분마다 SNMPv2c를 통해 각 스위치를 폴링하여 지원 가능성, 모니터링 상태, 온도 센서, CPU 사용률, 인터페이스 구성 및 연결, 클러스터 스위치 이중화, 팬 및 전원 공급 장치 작업에 대한 정보를 바탕으로 리소스 테이블을 업데이트합니다. 또한, 구성된 경우 CSHM은 1시간마다 SSH/SCP를 통해 로그를 수집하며, 추가 분석을 위해 AutoSupport를 통해 로그를 전송합니다. 요청 시 CSHM은 SSH/SCP를 사용하여 보다 상세한 기술 지원 로그 수집을 수행할 수도 있습니다. 자세한 내용은 을 "스위치 상태 모니터링" 참조하십시오.
MetroCluster 패브릭	스위치	MetroCluster 구성 백엔드 Fabric 토폴로지를 모니터링하고 잘못된 케이블 연결 및 조닝, ISL 장애 등의 잘못된 구성을 감지합니다.
MetroCluster 상태	상호 연결, RAID 및 스토리지	FC-VI 어댑터, FC 이니시에이터 어댑터, 좌측 애그리게이트 및 디스크, 클러스터 간 포트를 모니터링합니다
노드 연결(노드 연결)	CIFS 무중단 운영(CIFS-NDO)	SMB 연결을 모니터링하여 Hyper-V 애플리케이션의 무중단 운영을 지원합니다.
스토리지(SAS-connect)	노드 레벨에서 쉘프, 디스크, 어댑터를 모니터링하여 적절한 경로와 연결을 설정합니다.	시스템
해당 없음	다른 상태 모니터의 정보를 집계합니다.	시스템 연결(시스템 연결)

ONTAP 시스템 상태 경고를 자동으로 수신합니다

명령을 사용하여 시스템 상태 경고를 수동으로 확인할 수 `system health alert show` 있습니다. 그러나 상태 모니터에서 알림을 생성할 때 알림을 자동으로 수신하려면 특정

EMS(이벤트 관리 시스템) 메시지에 가입해야 합니다.

이 작업에 대해

다음 절차에서는 모든 HM.ALERT.Raised 메시지 및 모든 HM.ALERT.clLEALEed 메시지에 대한 알림을 설정하는 방법을 보여 줍니다.

모든 HM.ALERT.Raised 메시지 및 모든 HM.ALERT.ALLEALEAN 메시지에는 SNMP 트랩이 포함됩니다. SNMP 트랩의 이름은 `HealthMonitorAlertRaised` 및 `HealthMonitorAlertCleared`입니다.

에 대한 자세한 내용은 `system health alert show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 이벤트 목적지 작성 명령을 사용하여 EMS 메시지를 보낼 대상을 정의합니다.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

   에 대한 자세한 내용은 `event destination create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. event route add-destinations 명령을 사용하여 hm.alert.Raised 메시지와 hm.alert.clined 메시지를 목적지로 라우트한다.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

   에 대한 자세한 내용은 `event route add-destinations` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "System Manager를 사용하여 ONTAP 네트워크를 시각화합니다"
- "DATA ONTAP 에서 SNMP 모니터링을 구성하는 방법"

성능이 저하된 **ONTAP** 시스템 상태에 응답합니다

시스템 상태가 성능 저하 상태일 때 경고를 표시하고 가능한 원인 및 수정 조치를 읽으면서 저하된 서브시스템에 대한 정보를 표시하고 문제를 해결할 수 있습니다. 억제된 알림도 표시되어 이를 수정하고 확인되었는지 확인할 수 있습니다.

이 작업에 대해

AutoSupport 메시지 또는 EMS 이벤트를 보거나 '시스템 상태' 명령을 사용하여 알림이 생성되었는지 확인할 수 있습니다.

단계

1. 'system health alert show' 명령을 사용하면 시스템 상태를 훼손하는 경고를 볼 수 있습니다.
2. 경고의 가능한 원인, 가능한 영향 및 수정 조치를 읽고 문제를 해결할 수 있는지 또는 추가 정보가 필요한지 확인하십시오.

3. 자세한 정보가 필요하면 'system health alert show-instance' 명령을 사용하여 경고에 사용할 수 있는 추가 정보를 확인하십시오.
4. '-ACKNOWLEDGE' 매개 변수와 함께 'system health alert modify' 명령을 사용하여 특정 경고를 작업 중임을 나타냅니다.
5. 경고의 "수정 조치" 필드에 설명된 대로 문제를 해결하기 위해 수정 조치를 취합니다.

   수정 조치에는 시스템 재부팅이 포함될 수 있습니다.

   문제가 해결되면 경고가 자동으로 지워집니다. 하위 시스템에 다른 경고가 없으면 하위 시스템의 상태가 'OK'로 바뀝니다. 모든 서브시스템의 상태가 정상이면 전체 시스템 상태가 정상(OK)으로 바뀝니다.

6. 'system status show' 명령을 사용하여 시스템 상태가 'OK'인지 확인합니다.

   시스템 상태가 '정상'이 아닌 경우 이 절차를 반복합니다.

관련 정보

- "시스템 상태 경고 수정"

성능이 저하된 **ONTAP** 시스템 상태에 대한 응답에 대해 자세히 알아보십시오

노드에 대한 경로가 2개인 셸프로 인해 성능이 저하된 시스템 상태의 특정 예를 검토하여 경고에 응답할 때 CLI가 표시되는 내용을 볼 수 있습니다.

ONTAP를 시작한 후 시스템 상태를 확인하고 성능이 저하되었습니다.

```
cluster1::>system health status show
  Status
  ---------------
  degraded
```

경고를 표시하여 문제가 발생한 위치를 확인하고 쉘프 2에서 노드 1에 대한 경로가 2개 있지 않음을 확인할 수 있습니다.

```
      cluster1::>system health alert show
                 Node: node1
             Resource: Shelf ID 2
             Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

경고 ID를 비롯한 추가 정보를 얻기 위해 알림에 대한 세부 정보를 표시합니다.

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
          Acknowledge: false
             Suppress: false
               Policy: DualPathToDiskShelf_Policy
         Acknowledger: -
           Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

이 알림은 작업 중임을 나타냅니다.

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

쉘프 2와 노드 1 사이의 케이블 연결을 수정한 다음 시스템을 재부팅합니다. 그런 다음 시스템 상태를 다시 확인하고 상태가 "OK"인지 확인합니다.

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

관련 정보

- "시스템 상태 경고 수정"

ONTAP 시스템의 상태를 모니터링하는 명령입니다

명령을 사용하여 시스템 리소스 상태에 대한 정보를 표시하고, 경고에 응답하고, 향후 경고를 구성할 수 `system health` 있습니다. CLI 명령을 사용하면 상태 모니터링 구성 방법에 대한 자세한 정보를 볼 수 있습니다. 에 대한 자세한 내용은 `system health` "ONTAP 명령 참조입니다"을 참조하십시오.

시스템 상태의 상태를 표시합니다

원하는 작업	이 명령 사용...
개별 상태 모니터의 전체 상태를 반영하는 시스템의 상태를 표시합니다	'시스템 상태 표시
상태 모니터링을 사용할 수 있는 서브시스템의 상태를 표시합니다	시스템 상태 하위 시스템이 표시됩니다

노드 접속 상태를 표시합니다

원하는 작업	이 명령 사용...
포트 정보, HBA 포트 속도, I/O 처리량, 초당 I/O 작업 속도 등 노드에서 스토리지 셸프로의 접속에 대한 세부 정보를 표시합니다	'Storage shelf show-connectivity '-instance' 매개 변수를 사용하여 각 쉘프에 대한 자세한 정보를 표시합니다.
사용 가능한 공간, 쉘프 및 베이 번호, 소유 노드 이름 등의 드라이브 및 어레이 LUN에 대한 정보를 표시합니다	스토리지 디스크 쇼 각 드라이브에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 사용하십시오.
포트 유형, 속도 및 상태를 포함한 스토리지 쉘프 포트에 대한 자세한 정보를 표시합니다	'Storage port show' 각 어댑터에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 사용하십시오.

클러스터 및 스토리지 네트워크 스위치를 모니터링합니다

원하는 작업	이 명령 사용… **(ONTAP 9.8** 이상)	이 명령 사용… **(ONTAP 9.7** 이하)
클러스터에서 모니터링하는 스위치를 표시합니다	'시스템 스위치 이더넷 쇼	'system cluster-switch show'
삭제한 스위치(명령 출력의 Reason 열에 표시)를 포함하여 클러스터에서 현재 모니터링하는 스위치 표시 이 명령은 advanced 권한 수준에서 사용할 수 있습니다	'시스템 스위치 이더넷 show-all'	'system cluster-switch show-all'
검색되지 않은 스위치의 모니터링을 구성합니다	'시스템 스위치 이더넷 생성	'system cluster-switch create
클러스터에서 모니터링하는 스위치에 대한 정보 수정(예: 장치 이름, IP 주소, SNMP 버전 및 커뮤니티 문자열)	'시스템 스위치 이더넷 수정	'시스템 클러스터 스위치 수정
모니터링에서 스위치를 비활성화합니다	'시스템 스위치 이더넷 수정-비활성화-모니터링	'system cluster-switch modify-disable-monitoring
모니터링에서 스위치를 삭제합니다	'시스템 스위치 이더넷 삭제	'system cluster-switch delete
데이터베이스에 저장된 스위치 구성 정보를 영구적으로 제거합니다(이렇게 하면 스위치의 자동 검색이 다시 활성화됩니다).	'시스템 스위치 이더넷 삭제-강제	'system cluster-switch delete-force'를 선택합니다
스위치를 사용하여 로그 수집을 수행합니다	'시스템 스위치 이더넷 로그	'시스템 클러스터-스위치 로그

자세한 내용은 및 "로그 수집을 구성합니다"를 "스위치 상태 모니터링"참조하십시오.

생성된 알림에 응답합니다

원하는 작업	이 명령 사용…
알림이 트리거된 리소스 및 노드, 알림의 심각도 및 추정 원인과 같이 생성된 알림에 대한 정보를 표시합니다	'시스템 상태 경고 표시
생성된 각 알림에 대한 정보를 표시합니다	'시스템 상태 경고 표시 - 인스턴스'
다른 사용자가 알림을 작업 중임을 나타냅니다	시스템 상태 알림 수정

원하는 작업	이 명령 사용...
알림을 확인합니다	'시스템 상태 경고 수정 - 확인'
하위 시스템의 상태에 영향을 주지 않도록 후속 경고를 표시하지 않습니다	'시스템 상태 경고 수정 - 억제'
자동으로 지워지지 않은 알림을 삭제합니다	'시스템 상태 경고 삭제
예를 들어, 알림이 AutoSupport 메시지를 트리거했는지 여부와 같이 지난 주 내에 트리거된 알림을 표시하는 AutoSupport 메시지에 대한 정보를 표시합니다	'시스템 상태 AutoSupport 트리거 기록 표시

향후 알림을 구성합니다

원하는 작업	이 명령 사용...
특정 리소스 상태가 특정 경고를 발생시키는지 여부를 제어하는 정책을 사용하거나 사용하지 않도록 설정합니다	'시스템 상태 정책 정의 수정

상태 모니터링 구성 방법에 대한 정보를 표시합니다

원하는 작업	이 명령 사용...
노드, 이름, 하위 시스템 및 상태와 같은 상태 모니터에 대한 정보를 표시합니다	'시스템 상태 구성 쇼' 각 상태 모니터에 대한 세부 정보를 표시하려면 '-instance' 매개 변수를 사용합니다.
상태 모니터에서 잠재적으로 생성할 수 있는 알림에 대한 정보를 표시합니다	시스템 상태 경고 정의가 표시됩니다 각 경고 정의에 대한 자세한 정보를 표시하려면 '-instance' 매개 변수를 사용합니다.
알림이 발생하는 시기를 결정하는 상태 모니터링 정책에 대한 정보를 표시합니다	시스템 상태 정책 정의가 표시됩니다 각 정책에 대한 세부 정보를 표시하려면 '-instance' 매개 변수를 사용합니다. 다른 매개 변수를 사용하여 알림 목록을 정책 상태(사용 여부), 상태 모니터, 알림 등으로 필터링할 수 있습니다.

관련 정보

- "저장 포트 표시"

- "보관 선반 쇼"
- "시스템 상태 경고 삭제"

ONTAP 환경 정보 보기

센서를 통해 시스템의 환경 구성요소를 모니터링할 수 있습니다. 환경 센서에 대해 볼 수 있는 정보에는 해당 유형, 이름, 상태, 값 및 임계값 경고가 포함됩니다.

단계

1. 환경 센서에 대한 정보를 표시하려면 'system node environment sensors show' 명령을 사용합니다.

파일 시스템 분석

ONTAP 파일 시스템 분석에 대해 알아보십시오

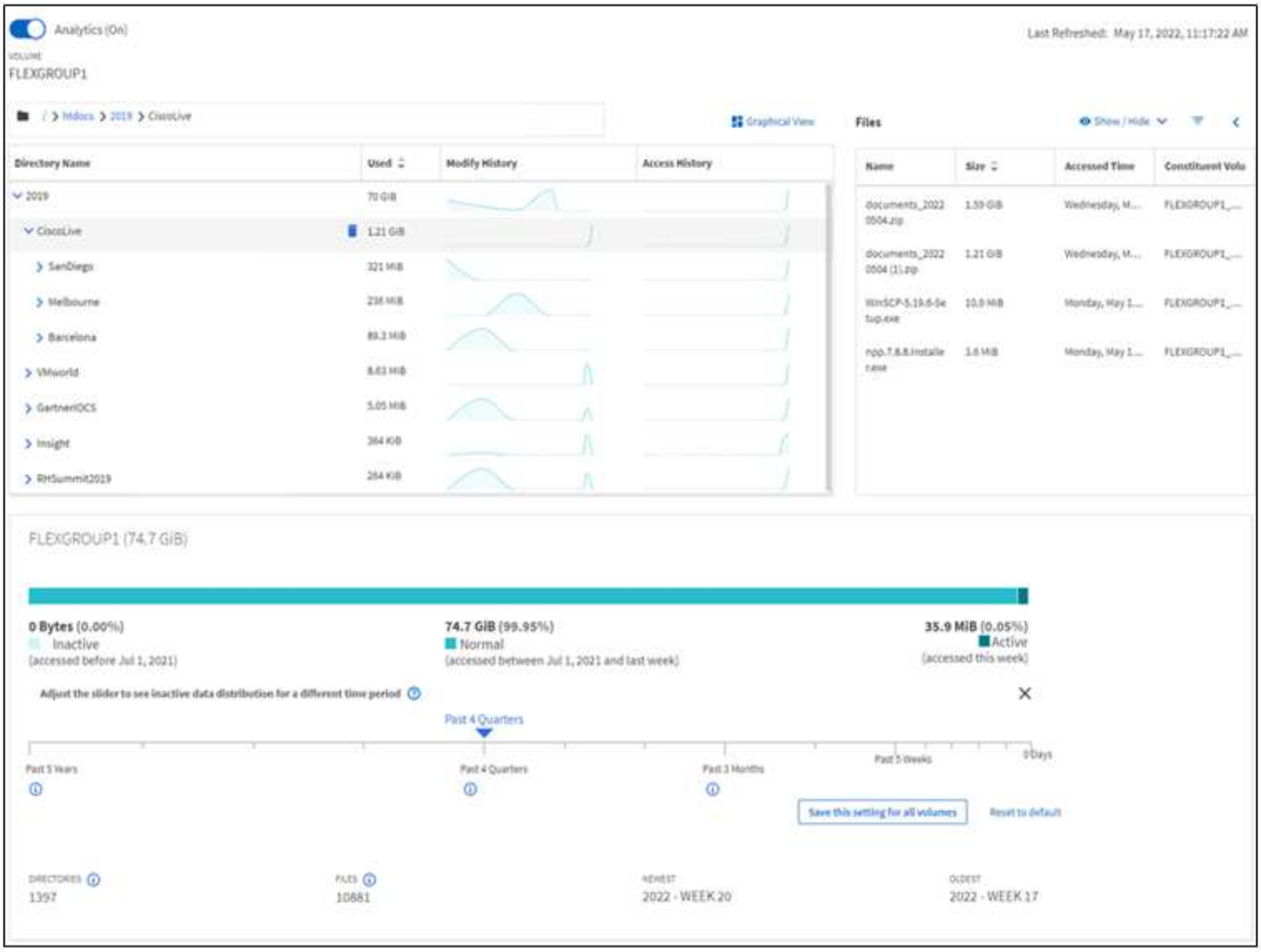
ONTAP 9.8에서 파일 시스템 분석(FSA)이 처음 도입되어 ONTAP FlexGroup 또는 FlexVol 볼륨 내의 파일 사용 및 스토리지 용량 추세를 실시간으로 파악할 수 있게 되었습니다. 이 기본 기능을 사용하면 외부 툴이 필요하지 않으며 스토리지가 사용되는 방법과 비즈니스 요구사항에 맞게 스토리지를 최적화할 수 있는 기회가 있는지 여부에 대한 주요 통찰력을 얻을 수 있습니다.

FSA를 사용하면 NAS에 있는 볼륨의 파일 시스템 계층 구조의 모든 수준에 대한 가시성을 확보할 수 있습니다. 예를 들어, SVM(Storage VM), 볼륨, 디렉토리, 파일 레벨에서 사용량 및 용량 인사이트를 얻을 수 있습니다. FSA를 사용하여 다음과 같은 질문에 답할 수 있습니다.

- 내 저장소를 채우는 것은 무엇이며, 다른 저장 위치로 이동할 수 있는 대용량 파일이 있습니까?
- 가장 활성화된 볼륨, 디렉토리 및 파일은 무엇입니까? 스토리지 성능이 사용자의 요구사항에 최적화되어 있습니까?
- 지난 달에 추가된 데이터의 양은 어느 정도입니까?
- 가장 활동적이거나 활동이 적은 스토리지 사용자는 누구입니까?
- 기본 스토리지에 얼마나 비활성 또는 휴면 데이터가 있습니까? 해당 데이터를 저비용 콜드 계층으로 이동할 수 있습니까?
- 계획된 서비스 품질 변경이 자주 액세스하는 중요한 파일에 대한 액세스에 부정적인 영향을 미칩니까?

파일 시스템 분석은 ONTAP 시스템 관리자에 통합됩니다. System Manager 내에서 제공되는 뷰:

- 실시간 가시성을 통해 데이터를 효과적으로 관리하고 운영할 수 있습니다
- 실시간 데이터 수집 및 집계
- 관련 성능 프로파일과 함께 하위 디렉토리와 파일 크기 및 개수를 계산합니다
- 수정 및 액세스 기록을 위한 파일 에이지 히스토그램



지원되는 볼륨 유형

파일 시스템 분석은 FlexCache 캐시 및 SnapMirror 대상 볼륨을 제외하고 활성 NAS 데이터가 있는 볼륨에 대한 가시성을 제공하도록 설계되었습니다.

파일 시스템 분석 기능 가용성

각 ONTAP 릴리즈는 파일 시스템 분석 범위를 확장합니다.

	ONTAP 9.14.1 이상	**ONTAP 9.13.1**	**ONTAP 9.12.1**	**ONTAP 9.11.1**	**ONTAP 9.10.1**	**ONTAP 9.9.1**	**ONTAP 9.8**
System Manager의 시각화	예	예	예	예	예	예	예
용량 분석	예	예	예	예	예	예	예
비활성 데이터 정보	예	예	예	예	예	예	예
Data ONTAP 7-Mode에서 전환된 볼륨 지원	예	예	예	예	예	예	아니요
System Manager에서 비활성 기간을 사용자 지정할 수 있습니다	예	예	예	예	예	예	아니요

	ONTAP 9.14.1 이상	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
볼륨 레벨 활동 추적	예	예	예	예	예	아니요	아니요
활동 추적 데이터를 CSV로 다운로드합니다	예	예	예	예	예	아니요	아니요
SVM 레벨의 활동 추적 을 참조하십시오	예	예	예	예	아니요	아니요	아니요
타임라인	예	예	예	예	아니요	아니요	아니요
사용 분석	예	예	예	아니요	아니요	아니요	아니요
File System Analytics를 기본적으로 설정하는 옵션입니다	예	예	아니요	아니요	아니요	아니요	아니요
초기화 스캔 진행 모니터	예	아니요	아니요	아니요	아니요	아니요	아니요

파일 시스템 분석에 대해 자세히 알아보십시오

관련 정보

- "TR 4687: ONTAP 파일 시스템 분석에 대한 모범 사례 지침"
- "기술 자료: NetApp ONTAP 파일 시스템 분석을 켠 후 지연 시간이 길거나 변동이 심한 경우"

ONTAP 파일 시스템 분석 활성화

용량 분석과 같은 사용 데이터를 수집하고 표시하려면 볼륨에 대해 File System Analytics를 활성화해야 합니다.

ONTAP 9.17.1부터 NAS 프로토콜에 할당된 ONTAP 클러스터의 새로 생성된 SVM에 생성된 볼륨에는 파일 시스템 분석(FSA)이 기본적으로 활성화됩니다. FSA는 볼륨이 생성되는 즉시 자동으로 활성화되어 추가 구성 없이 즉시 분석 기능을 제공합니다. 새 볼륨에서 파일 시스템 분석을 활성화하지 않으려면 다음을 수행해야 합니다. "새 볼륨에서 FSA 비활성화" SVM에서.

이 작업에 대해

- ONTAP 9.8부터 새 볼륨이나 기존 볼륨에서 파일 시스템 분석을 활성화할 수 있습니다. 시스템을 ONTAP 9.8 이상으로 업그레이드하는 경우 파일 시스템 분석을 활성화하기 전에 모든 업그레이드 프로세스가 완료되었는지 확인하십시오.
- 분석을 지원하는 데 걸리는 시간은 볼륨의 크기와 콘텐츠에 따라 다릅니다. System Manager에서 진행 상황을 표시하고 완료되면 분석 데이터를 표시합니다. 초기화 스캔 진행률에 대한 보다 정확한 정보가 필요한 경우 ONTAP CLI 명령을 사용할 수 있습니다 `volume analytics show`.
  - ONTAP 9.15.1부터 한 노드에서 4개의 초기화 스캔만 동시에 수행할 수 있습니다. 새 스캔을 시작하기 전에 스캔이 완료될 때까지 기다려야 합니다. 또한 ONTAP는 볼륨에 사용 가능한 공간이 충분한지 확인하고, 없는 경우 오류 메시지를 표시합니다. 볼륨의 사용 가능한 공간의 최소 5 ~ 8%가 사용 가능한지 확인합니다. 볼륨에 자동 크기 조정이 활성화되어 있는 경우 최대 자동 확장 크기를 기준으로 사용 가능한 크기를 계산합니다.
  - ONTAP 9.14.1부터 ONTAP는 스캔 진행률에 영향을 주는 임계치 조절 이벤트에 대한 알림과 더불어 초기화 스캔에 대한 진행률 추적을 제공합니다.
  - 초기화 스캔과 관련된 추가 고려 사항은 를 참조하십시오 스캔 고려 사항.
  - 에 대한 자세한 내용은 `volume analytics show` "ONTAP 명령 참조입니다"을 참조하십시오.

기존 볼륨에서 파일 시스템 분석을 활성화합니다

ONTAP System Manager 또는 CLI를 사용하여 파일 시스템 분석을 활성화할 수 있습니다.

예 **38.** 단계

시스템 관리자

ONTAP 9.10.1 이상	**ONTAP 9.9.1** 및 **ONTAP 9.8**
1. 스토리지 > 볼륨 * 을 선택합니다. 2. 원하는 볼륨을 선택합니다. 개별 볼륨 메뉴에서 * 파일 시스템 > 탐색기 * 를 선택합니다. 3. 분석 활성화 * 또는 * 분석 비활성화 * 를 선택합니다.	1. 스토리지 > 볼륨 * 을 선택합니다. 2. 원하는 볼륨을 선택한 다음 * Explorer * 를 선택합니다. 3. 분석 활성화 * 또는 * 분석 비활성화 * 를 선택합니다.

CLI를 참조하십시오

CLI를 사용하여 **File System Analytics**를 설정합니다

1. 다음 명령을 실행하세요.

```
volume analytics on -vserver <svm_name> -volume <volume_name> [-
foreground {true|false}]
```

   기본적으로 이 명령은 포그라운드에서 실행됩니다. ONTAP 진행 상황을 표시하고 완료되면 분석 데이터를 제공합니다. 더 정확한 정보가 필요하면 다음을 사용하여 백그라운드에서 명령을 실행할 수 있습니다. `-foreground false` 옵션을 선택한 다음 사용하세요 `volume analytics show` CLI에서 초기화 진행률을 표시하는 명령입니다.

2. 파일 시스템 분석을 성공적으로 활성화한 후 System Manager 또는 ONTAP REST API를 사용하여 분석 데이터를 표시할 수 있습니다.

에 대한 자세한 내용은 `volume analytics on` "ONTAP 명령 참조입니다"을 참조하십시오.

기본 파일 시스템 분석 설정을 수정합니다

ONTAP 9.13.1부터 SVM 또는 클러스터 설정을 수정하여 새 볼륨에 대해 파일 시스템 분석을 기본적으로 활성화할 수 있습니다.

예 **39.** 단계

시스템 관리자

System Manager를 사용하는 경우, 기본적으로 볼륨 생성 시 용량 분석 및 활동 추적을 사용하도록 스토리지 VM 또는 클러스터 설정을 수정할 수 있습니다. 기본 활성화는 기존 볼륨이 아니라 설정을 수정한 후에만 생성된 볼륨에만 적용됩니다.

클러스터에서 파일 시스템 분석 설정을 수정합니다

1. 시스템 관리자에서 *클러스터 설정*으로 이동합니다.
2. *클러스터 설정*에서 파일 시스템 설정 탭을 검토합니다. 설정을 수정하려면 상.
3. 활동 추적 필드에는 기본적으로 활동 추적을 활성화할 SVM의 이름을 입력합니다. 필드를 비워 두면 모든 SVM에서 활동 추적이 비활성화됩니다.

   새 스토리지 VM에서 기본적으로 활동 추적을 비활성화하려면 새 스토리지 **VM**에서 활성화 상자의 선택을 해제합니다.

4. 분석 필드에 용량 분석을 기본적으로 활성화할 스토리지 VM의 이름을 입력합니다. 필드를 비워 두면 모든 SVM에서 용량 분석이 비활성화됩니다.

   새 스토리지 VM에서 기본적으로 용량 분석을 비활성화하려면 새 스토리지 **VM**에서 활성화 상자의 선택을 취소합니다.

5. 저장 * 을 선택합니다.

SVM에서 파일 시스템 분석 설정을 수정합니다

1. 수정하려는 SVM을 선택한 다음 *스토리지 VM 설정*을 선택합니다.
2. 파일 시스템 분석 카드에서 토글을 사용하여 스토리지 VM의 모든 새 볼륨에 대한 활동 추적 및 용량 분석을 활성화하거나 비활성화합니다.

CLI를 참조하십시오

ONTAP CLI를 사용하여 새 볼륨에서 파일 시스템 분석을 기본적으로 사용하도록 스토리지 VM을 구성할 수 있습니다.

SVM에서 기본적으로 파일 시스템 분석 지원

1. 새로 생성된 모든 볼륨에서 기본적으로 용량 분석 및 활동 추적을 활성화하도록 SVM을 수정합니다.

   ```
   vserver modify -vserver <svm_name> -auto-enable-activity-tracking
   true -auto-enable-analytics true
   ```

   에 대한 자세한 내용은 `vserver modify` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "ONTAP 명령 참조입니다"

FSA를 사용하여 ONTAP 파일 시스템 활동 보기

FSA(File System Analytics)를 활성화한 후 선택한 볼륨의 루트 디렉토리 컨텐츠를 각 하위 트리에 사용된 공간으로 정렬할 수 있습니다.

파일 시스템 객체를 선택하여 파일 시스템을 탐색하고 디렉토리의 각 객체에 대한 세부 정보를 표시합니다. 디렉토리에 대한 정보도 그래픽으로 표시할 수 있습니다. 시간이 지남에 따라 각 하위 트리에 대한 기록 데이터가 표시됩니다. 사용된 공간은 3000 개가 넘는 디렉토리가 있는 경우 정렬되지 않습니다.

탐색기

파일 시스템 분석 * 탐색기 * 화면은 다음 세 가지 영역으로 구성됩니다.

- 디렉터리 및 하위 디렉터리의 트리 보기; 이름, 크기, 수정 기록 및 액세스 기록을 표시하는 확장 가능한 목록.
- 디렉토리 목록에서 선택한 객체에 대한 이름, 크기 및 액세스 시간을 표시하는 파일.
- 디렉토리 목록에서 선택한 객체에 대한 활성 및 비활성 데이터 비교

  ONTAP 9.9.1부터 보고할 범위를 사용자 지정할 수 있습니다. 기본값은 1년입니다. 이러한 사용자 지정을 기반으로 볼륨 이동 및 계층화 정책 수정 등의 수정 조치를 수행할 수 있습니다.

액세스 시간은 기본적으로 표시됩니다. 그러나 볼륨 기본값이 CLI에서 변경된 경우('볼륨 수정' 명령으로 '-atime-update' 옵션을 'false'로 설정) 마지막으로 수정한 시간만 표시됩니다. 예를 들면 다음과 같습니다.

- 트리 보기에는 * 액세스 기록 * 이 표시되지 않습니다.
- 파일 보기가 변경됩니다.
- 활성/비활성 데이터 뷰는 수정된 시간('시간')을 기준으로 합니다.

이러한 디스플레이를 사용하여 다음을 검사할 수 있습니다.

- 파일 시스템 위치는 공간을 가장 많이 소모합니다
- 디렉토리 및 하위 디렉토리 내의 파일 및 하위 디렉토리 수를 비롯한 디렉토리 트리에 대한 자세한 정보
- 이전 데이터가 포함된 파일 시스템 위치(예: 스크래치, 임시 또는 로그 트리)

FSA 출력을 해석할 때는 다음 사항을 염두에 두십시오.

- FSA는 데이터가 처리되는 양이 아니라 데이터의 사용 위치 및 시기를 보여 줍니다. 예를 들어, 최근에 액세스하거나 수정한 파일에 의한 대규모 공간 소비는 시스템 처리 부하가 높음을 나타내는 것은 아닙니다.
- Volume Explorer * 탭에서 FSA의 공간 소비를 계산하는 방식은 다른 도구와 다를 수 있습니다. 특히 볼륨에 스토리지 효율성 기능이 활성화되어 있는 경우 * 볼륨 개요 * 에 보고된 소비량과 비교하여 큰 차이가 있을 수 있습니다. 이는 * Volume Explorer * 탭에 효율성 절약 효과가 포함되지 않기 때문입니다.
- 디렉토리 표시의 공간 제한으로 인해 _List View_에서 8개 수준 이상의 디렉토리 깊이를 볼 수 없습니다. 8개 수준 이상의 디렉토리를 보려면 _Graphical View_로 전환하고 원하는 디렉토리를 찾은 다음 _List View_로 다시 전환해야 합니다. 그러면 디스플레이에 추가 화면 공간이 허용됩니다.

단계

1. 선택한 볼륨의 루트 디렉토리 컨텐츠를 봅니다.

ONTAP 9.10.1부터 시작합니다	ONTAP 9.9.1 및 9.8에서
Storage > Volumes * 를 선택하고 원하는 볼륨을 선택합니다. 개별 볼륨 메뉴에서 * 파일 시스템 > 탐색기 * 를 선택합니다.	Storage > Volumes * 를 클릭하고 원하는 볼륨을 선택한 다음 * Explorer * 를 클릭합니다.

관련 정보

- "볼륨 수정"

FSA를 사용하여 ONTAP 활동 추적 활성화

ONTAP 9.10.1부터 파일 시스템 분석에는 핫 객체를 식별하고 데이터를 CSV 파일로 다운로드할 수 있는 활동 추적 기능이 포함되어 있습니다. ONTAP 9.11.1부터 활동 추적 기능이 SVM 범위로 확장됩니다. 또한 ONTAP 9.11.1부터 시스템 관리자는 활동 추적 타임라인을 제공하여 최대 5분의 활동 추적 데이터를 조회할 수 있습니다.

Activity Tracking(활동 추적)을 사용하면 다음 네 가지 범주로 모니터링할 수 있습니다.

- 디렉토리
- 파일
- 클라이언트
- 사용자

모니터링되는 각 범주에 대해 작업 추적은 읽기 IOPS, 쓰기 IOPS, 읽기 처리량 및 쓰기 처리량을 표시합니다. 작업 추적에 대한 쿼리는 이전 5초 간격 동안 시스템에 표시되는 핫 스팟과 관련하여 10-15초마다 새로 고쳐집니다.

활동 추적 정보는 근사치이며, 데이터의 정확도는 수신되는 I/O 트래픽의 분포에 따라 달라집니다.

System Manager의 볼륨 레벨에서 활동 추적을 보면 확장된 볼륨의 메뉴만 활발하게 새로 고쳐집니다. 볼륨 보기가 축소되면 볼륨 표시가 확장될 때까지 볼륨이 새로 고쳐지지 않습니다. 새로 고침 일시 중지 * 버튼을 사용하여 새로 고침을 중지할 수 있습니다. 활동 데이터는 선택한 볼륨에 대해 캡처된 모든 시점 데이터를 표시하는 CSV 형식으로 다운로드할 수 있습니다.

ONTAP 9.11.1부터 타임라인 기능을 사용할 수 있으므로 볼륨 또는 SVM에 핫스팟 활동을 기록하여 약 5초마다 지속적으로 업데이트하고 이전 5분의 데이터를 유지할 수 있습니다. 시간 표시 막대 데이터는 페이지의 표시 영역에 있는 필드에만 유지됩니다. 시간 표시 막대가 표시되지 않도록 추적 범주를 축소하거나 스크롤하면 시간 표시 막대가 데이터 수집을 중지합니다. 기본적으로 타임라인은 비활성화되어 있으며 활동 탭에서 멀리 이동하면 자동으로 비활성화됩니다.

단일 볼륨에 대해 활동 추적을 활성화합니다

ONTAP 시스템 관리자 또는 CLI를 사용하여 활동 추적을 설정할 수 있습니다.

이 작업에 대해

ONTAP REST API 또는 시스템 관리자와 함께 RBAC를 사용하는 경우 활동 추적에 대한 액세스를 관리하기 위해 사용자 지정 역할을 만들어야 합니다. 을 참조하십시오 역할 기반 액세스 제어 참조하십시오.

시스템 관리자

단계

1. 스토리지 > 볼륨 * 을 선택합니다. 원하는 볼륨을 선택합니다. 개별 볼륨 메뉴에서 파일 시스템 을 선택한 다음 활동 탭을 선택합니다.
2. 상위 디렉토리, 파일, 클라이언트 및 사용자에 대한 개별 보고서를 보려면 * Activity Tracking * 이 켜져 있어야 합니다.
3. 새로 고침 없이 보다 깊이 있는 데이터를 분석하려면 * 새로 고침 일시 중지 * 를 선택합니다. 데이터를 다운로드하여 보고서의 CSV 레코드도 가질 수 있습니다.

CLI를 참조하십시오

단계

1. 활동 추적 활성화:

   ```
   volume activity-tracking on -vserver svm_name -volume volume_name
   ```

2. 다음 명령을 사용하여 볼륨에 대한 Activity Tracking 상태가 On 또는 Off 인지 확인합니다.

   ```
   volume activity-tracking show -vserver svm_name -volume volume_name -state
   ```

3. 활성화되면 ONTAP 시스템 관리자 또는 ONTAP REST API를 사용하여 활동 추적 데이터를 표시합니다.

여러 볼륨에 대해 활동 추적을 활성화합니다

System Manager 또는 CLI를 사용하여 여러 볼륨의 활동 추적을 설정할 수 있습니다.

이 작업에 대해

ONTAP REST API 또는 시스템 관리자와 함께 RBAC를 사용하는 경우 활동 추적에 대한 액세스를 관리하기 위해 사용자 지정 역할을 만들어야 합니다. 을 참조하십시오 역할 기반 액세스 제어 참조하십시오.

시스템 관리자

특정 볼륨에 대해 활성화합니다

1. 스토리지 > 볼륨 * 을 선택합니다. 원하는 볼륨을 선택합니다. 개별 볼륨 메뉴에서 파일 시스템 을 선택한 다음 활동 탭을 선택합니다.
2. 활동 추적을 활성화할 볼륨을 선택합니다. 볼륨 목록 상단에서 * 추가 옵션 * 버튼을 선택합니다. 작업 추적 활성화 * 를 선택합니다.
3. SVM 레벨에서 활동 추적을 보려면 * 스토리지 > 볼륨 * 에서 보려는 특정 SVM을 선택합니다. File System(파일 시스템) 탭, Activity(활동) 로 이동하면 Activity Tracking(활동 추적)이 활성화된 볼륨에 대한 데이터가 표시됩니다.

모든 볼륨에 대해 활성화

1. 스토리지 > 볼륨 * 을 선택합니다. 메뉴에서 SVM을 선택합니다.
2. File System * 탭으로 이동하고 * More * 탭을 선택하여 SVM의 모든 볼륨에서 활동 추적을 활성화합니다.

CLI를 참조하십시오

ONTAP 9.13.1부터 ONTAP CLI를 사용하여 여러 볼륨에 대한 활동 추적을 설정할 수 있습니다.

단계

1. 활동 추적 활성화:

   ```
   volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
   ```

   사용 * 지정된 스토리지 VM의 모든 볼륨에 대해 작업 추적을 설정하려면 다음을 수행합니다.

   사용 ! 볼륨 이름 다음에 볼륨 이름을 사용하여 SVM의 모든 볼륨에서 활동 추적을 활성화합니다. 단, 볼륨 이름은 예외입니다.

2. 작업이 성공했는지 확인합니다.

   ```
   volume show -fields activity-tracking-state
   ```

3. 활성화되면 ONTAP 시스템 관리자 또는 ONTAP REST API를 사용하여 활동 추적 데이터를 표시합니다.

FSA를 사용하여 **ONTAP** 사용 분석 활성화

ONTAP 9.12.1부터 사용 분석을 통해 볼륨 내에서 공간이 가장 많은 디렉토리를 볼 수 있습니다. 볼륨의 총 디렉토리 수 또는 볼륨의 총 파일 수를 볼 수 있습니다. 보고는 가장 많은 공간을 사용하는 25개 디렉토리로 제한됩니다.

대규모 디렉토리에 대한 분석 기능은 15분마다 업데이트됩니다. 페이지 맨 위에서 마지막으로 새로 고친 타임스탬프를 확인하여 가장 최근 새로 고침을 모니터링할 수 있습니다. 다운로드 단추를 클릭하여 Excel 통합 문서로 데이터를 다운로드할 수도 있습니다. 다운로드 작업은 백그라운드에서 실행되며 선택한 볼륨에 대해 가장 최근에 보고된 정보를 제공합니다. 검사가 결과 없이 반환되는 경우 볼륨이 온라인 상태인지 확인합니다. SnapRestore와 같은 이벤트로 인해 파일 시스템 분석 시 대규모 디렉토리 목록이 재구축됩니다.

단계

1. 스토리지 > 볼륨 * 을 선택합니다. 원하는 볼륨을 선택합니다.
2. 개별 볼륨 메뉴에서 * 파일 시스템 * 을 선택합니다. 그런 다음 * Usage * 탭을 선택합니다.
3. 분석 * 스위치를 전환하여 사용 분석을 활성화합니다.
4. System Manager는 크기가 가장 큰 디렉토리를 내림차순으로 식별하는 막대 그래프를 표시합니다.

> 최상위 디렉토리 목록이 수집되는 동안 ONTAP는 부분 데이터를 표시하거나 데이터를 전혀 표시하지 않을 수 있습니다. 스캔 진행 상황은 스캔 중에 표시되는 * Usage * (사용 *) 탭에 있을 수 있습니다.

특정 디렉토리에 대한 더 많은 통찰력을 얻을 수 ONTAP 파일 시스템 활동 보기있습니다.

FSA에서 ONTAP 분석을 기반으로 시정 조치를 취하세요

ONTAP 9.9.1부터 파일 시스템 분석 디스플레이에서 직접 현재 데이터와 원하는 결과를 기반으로 수정 조치를 수행할 수 있습니다.

디렉토리 및 파일을 삭제합니다

탐색기 디스플레이에서 삭제할 디렉터리 또는 개별 파일을 선택할 수 있습니다. 디렉토리는 지연 시간이 짧은 비동기 디렉토리 삭제 기능으로 삭제됩니다. 비동기 디렉토리 삭제는 분석 기능을 사용하지 않고 ONTAP 9.1.1부터 사용할 수도 있습니다.

ONTAP 9.10.1부터 시작합니다	**ONTAP 9.9.1**에서
1. *저장소 > 볼륨*을 선택하고 원하는 볼륨 이름을 선택합니다. 2. 개별 볼륨 페이지에서 파일 시스템 탭을 선택한 다음 탐색기 탭을 선택합니다. 3. 탐색기 보기에서 원하는 디렉토리를 선택합니다. 4. 삭제하려면 파일이나 폴더 위에 마우스를 올려놓고 삭제를 클릭합니다. 옵션이 나타납니다. 한 번에 하나의 개체만 삭제할 수 있습니다. 디렉토리와 파일이 삭제되면 새 스토리지 용량 값이 즉시 표시되지 않습니다.	1. 스토리지 > 볼륨 * 을 선택합니다. 2. 원하는 볼륨을 선택한 다음 * Explorer * 를 선택합니다. 3. 탐색기 보기에서 원하는 디렉토리를 선택합니다. 4. 삭제하려면 파일이나 폴더 위에 마우스를 올려놓고 삭제를 클릭합니다. 옵션이 나타납니다.

스토리지 계층에서 미디어 비용을 할당하여 비활성 데이터 스토리지 위치의 비용을 비교합니다

미디어 비용은 스토리지 비용 평가를 기준으로 할당한 값이며, 선택한 통화는 GB당 통화입니다. 설정할 경우 System Manager에서 볼륨을 이동할 때 할당된 미디어 비용을 사용하여 예상 절감액을 투영합니다.

설정한 미디어 비용은 지속적이지 않으며 단일 브라우저 세션에만 설정할 수 있습니다.

단계

1. Storage > Tiers * 를 클릭한 다음 원하는 로컬 계층(집계) 타일에서 * Set Media Cost * 를 클릭합니다.

   비교를 활성화하려면 활성 계층과 비활성 계층을 선택해야 합니다.

2. 통화 유형 및 금액을 입력합니다.

   미디어 비용을 입력하거나 변경하면 모든 미디어 유형에 변경 사항이 적용됩니다.

스토리지 비용을 줄이기 위해 볼륨을 이동합니다

분석 표시 및 미디어 비용 비교를 기반으로, 볼륨을 로컬 계층의 저렴한 스토리지로 이동할 수 있습니다.

한 번에 하나의 볼륨만 비교 및 이동할 수 있습니다.

단계

1. 미디어 비용 표시를 활성화한 후 * Storage > Tiers * 를 클릭하고 * Volumes * 를 클릭합니다.
2. 볼륨에 대한 대상 옵션을 비교하려면 볼륨에 대해 를 ⋮ 클릭한 다음 * Move * 를 클릭합니다.
3. 대상 로컬 계층 선택 * 디스플레이에서 대상 계층을 선택하여 예상 비용 차이를 표시합니다.
4. 옵션을 비교한 후 원하는 계층을 선택하고 * Move * (이동 *)를 클릭합니다.

ONTAP 파일 시스템 분석을 통해 역할 기반 액세스 제어

ONTAP 9.12.1부터 ONTAP에는 이라는 미리 정의된 RBAC(역할 기반 액세스 제어) 역할이 포함되어 `admin-no-fsa` 있습니다. 이 `admin-no-fsa` 역할은 관리자 수준의 Privileges를 허용하지만 사용자가 ONTAP CLI, REST API 및 System Manager에서 엔드포인트(예: 파일 시스템 분석)와 관련된 작업을 수행할 수 없게 `files` 합니다.

에 대한 자세한 내용은 를 참조하십시오 `admin-no-fsa` 역할, 을 참조하십시오 클러스터 관리자를 위한 사전 정의된 역할.

ONTAP 9.12.1 이전 버전의 ONTAP를 사용하는 경우 파일 시스템 분석에 대한 액세스를 제어하는 전용 역할을 만들어야 합니다. ONTAP 9.12.1 이전의 ONTAP 버전에서는 ONTAP CLI 또는 ONTAP REST API를 통해 RBAC 권한을 구성해야 합니다.

시스템 관리자

ONTAP 9.12.1부터 시스템 관리자를 사용하여 파일 시스템 분석에 대한 RBAC 권한을 구성할 수 있습니다.

단계

1. 클러스터 > 설정 * 을 선택합니다. 보안 * 에서 * 사용자 및 역할 * 로 이동하고 를 선택합니다 →.
2. 역할 * 에서 을 + Add 선택합니다.
3. 역할의 이름을 지정하십시오. 역할 속성 에서 적절한 를 제공하여 사용자 역할에 대한 액세스 또는 제한을 구성합니다 "API 엔드포인트". File System Analytics 액세스 또는 제한을 구성하기 위한 기본 경로 및 보조 경로는 아래 표를 참조하십시오.

제한	기본 경로	보조 경로
볼륨의 활동 추적	`/api/storage/volumes`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
SVM에서 활동 추적	`/api/svm/svms`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
모든 파일 시스템 분석 작업	`/api/storage/volumes`	`/:uuid/files`

   을 사용할 수 있습니다 `/*/` 엔드포인트에서 모든 볼륨 또는 SVM에 대한 정책을 설정할 UUID가 아닌

   각 엔드포인트에 대한 액세스 권한을 선택합니다.

4. 저장 * 을 선택합니다.
5. 사용자 또는 사용자에게 역할을 할당하려면 을 참조하십시오 관리자 액세스 제어.

CLI를 참조하십시오

ONTAP 9.12.1 이전 버전의 ONTAP를 사용하는 경우 ONTAP CLI를 사용하여 사용자 지정 역할을 만듭니다.

단계

1. 모든 기능에 액세스할 수 있는 기본 역할을 만듭니다.

이 작업은 제한된 역할을 생성하기 전에 수행해야 하며, 해당 역할이 활동 추적에서만 제한적인지 확인해야 합니다.

'Security login role create-cmddirname default-access all-role StorageAdmin

2. 제한적인 역할 생성:

보안 로그인 역할 create-cmddirname "volume file show-disk-usage" -access none-role StorageAdmin"

3. SVM의 웹 서비스에 액세스할 수 있는 역할 승인:

◦ REST API 호출의 경우 'st'입니다
◦ 암호 보호를 위한 보안
◦ System Manager 액세스를 위한 sysmgr입니다

```
vserver services web access create -vserver <svm-name> -name rest -role
storageAdmin

vserver services web access create -vserver <svm-name> -name security
-role storageAdmin
```

```
vserver services web access create -vserver <svm-name> -name sysmgr -role
storageAdmin
```

4. 사용자를 생성합니다.

사용자에게 적용하려는 각 응용 프로그램에 대해 고유한 create 명령을 실행해야 합니다. 같은 사용자에 대해 여러 번 만들기 를 호출하면 해당 사용자에게 모든 응용 프로그램이 적용되고 매번 새 사용자가 작성되지는 않습니다. 애플리케이션 유형에 대한 http 파라미터는 ONTAP REST API와 System Manager에 적용된다.

보안 로그인 create-user-or-group-name storageUser-authentication-method password-application http-role StorageAdmin

5. 새로운 사용자 자격 증명을 사용하여 System Manager에 로그인하거나 ONTAP REST API를 사용하여 파일 시스템 분석 데이터에 액세스할 수 있습니다.

추가 정보

- 클러스터 관리자를 위한 사전 정의된 역할
- System Manager로 관리자 액세스 제어
- "RBAC 역할 및 ONTAP REST API에 대해 자세히 알아보십시오"
- "보안 로그인 생성"

ONTAP 파일 시스템 분석을 위한 고려 사항

File System Analytics 구축과 관련된 특정 사용량 제한 및 잠재적 성능 영향을 알고 있어야 합니다.

SVM 보호 관계

SVM이 포함된 볼륨에서 파일 시스템 분석을 사용하도록 설정한 경우, 분석 데이터가 타겟 SVM에 복제되지 않습니다. 복구 작업에서 소스 SVM을 재동기화해야 하는 경우 복구 후 원하는 볼륨에 대한 분석을 수동으로 다시 활성화해야 합니다.

성능 고려 사항

경우에 따라 초기 메타데이터 수집 중에 파일 시스템 분석을 사용하도록 설정하면 성능에 부정적인 영향을 미칠 수 있습니다. 이는 일반적으로 최대 사용률이 있는 시스템에서 가장 많이 나타납니다. 이러한 시스템에 대한 분석을 사용하지 않으려면 ONTAP System Manager 성능 모니터링 툴을 사용하면 됩니다.

지연 시간이 눈에 띄게 증가하는 경우 다음을 참조하세요."NetApp 지식 기반: NetApp ONTAP 파일 시스템 분석을 켠 후 대기 시간이 길어지거나 변동함" .

스캔 고려 사항

용량 분석을 활성화하면 ONTAP에서 용량 분석을 위한 초기화 스캔을 수행합니다. 이 스캔은 용량 분석이 활성화된 볼륨의 모든 파일에 대한 메타데이터에 액세스합니다. 스캔 중에 파일 데이터가 읽혀지지 않습니다. ONTAP 9.14.1부터 REST API, 시스템 관리자의 ** 탐색기 탭 또는 CLI 명령을 사용하여 스캔 진행률을 추적할 수 `volume analytics show` 있습니다. 임계치 조절 이벤트가 있는 경우 ONTAP에서 알림을 제공합니다.

볼륨에서 File System Analytics를 활성화할 때는 볼륨의 사용 가능한 공간의 5~8%가 사용 가능한지 확인하십시오. 볼륨에 자동 크기 조정이 활성화되어 있는 경우 최대 자동 확장 크기를 기준으로 사용 가능한 크기를 계산합니다. ONTAP 9.15.1부터 볼륨에서 파일 시스템 분석을 활성화할 때 사용 가능한 공간이 충분하지 않으면 ONTAP에 오류 메시지가 표시됩니다.

검사가 완료된 후 파일 시스템이 변경되면 File System Analytics는 실시간으로 계속 업데이트됩니다.

스캔에 필요한 시간은 볼륨의 디렉토리 및 파일 수에 비례합니다. 스캔은 메타데이터를 수집하므로 파일 크기는 스캔 시간에 영향을 주지 않습니다.

초기화 스캔에 대한 자세한 내용은 을 참조하십시오 "TR-4867: 파일 시스템 분석을 위한 모범 사례 지침".

모범 사례

애그리게이트를 공유하지 않는 볼륨에서 스캔을 시작해야 합니다. 명령을 사용하여 현재 어떤 애그리게이트가 어떤 볼륨을 호스팅하고 있는지 확인할 수 있습니다.

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

검사가 실행되는 동안 볼륨은 계속해서 클라이언트 트래픽을 처리합니다. 클라이언트 트래픽이 낮을 것으로 예상되는 기간 동안 스캔을 시작하는 것이 좋습니다.

클라이언트 트래픽이 증가하면 시스템 리소스가 소모되고 스캔 시간이 길어집니다.

ONTAP 9.12.1부터는 ONTAP CLI와 System Manager에서 데이터 수집을 일시 중지할 수 있습니다.

- ONTAP CLI를 사용하는 경우:
  - 다음 명령을 사용하여 데이터 수집을 일시 중지할 수 있습니다. `volume analytics initialization pause -vserver svm_name -volume volume_name`
  - 클라이언트 트래픽이 느려지면 다음 명령을 사용하여 데이터 수집을 다시 시작할 수 있습니다. `volume`

```
analytics initialization resume -vserver svm_name -volume volume_name
```

- System Manager를 사용하는 경우 볼륨 메뉴의 * 탐색기 * 보기에서 * 데이터 수집 일시 중지 * 및 * 데이터 수집 다시 시작 * 버튼을 사용하여 스캔을 관리합니다.

EMS 구성

ONTAP EMS 구성에 대해 자세히 알아보십시오

즉각적인 주의가 필요한 시스템 문제를 즉시 알 수 있도록 중요한 EMS(이벤트 관리 시스템) 이벤트 알림을 이메일 주소, syslog 서버, SNMP(Simple Management Network Protocol) 트라프호스트 또는 웹후크 애플리케이션에 직접 보내도록 ONTAP 9를 구성할 수 있습니다.

중요 이벤트 알림은 기본적으로 활성화되어 있지 않으므로 이메일 주소, syslog 서버, SNMP traphost 또는 webhook 애플리케이션에 알림을 보내도록 EMS를 구성해야 합니다.

의 릴리스 특정 버전을 검토합니다 "ONTAP 9 EMS 참조".

EMS 이벤트 매핑에 사용되지 않는 ONTAP 명령 집합(예: 이벤트 대상, 이벤트 경로)을 사용하는 경우 매핑을 업데이트하는 것이 좋습니다. "사용되지 않는 ONTAP 명령에서 EMS 매핑을 업데이트하는 방법을 알아보십시오"..

System Manager를 사용하여 ONTAP EMS 이벤트 알림 및 필터를 구성합니다

System Manager를 사용하면 즉각적인 주의가 필요한 시스템 문제를 알릴 수 있도록 이벤트 관리 시스템(EMS)에서 이벤트 알림을 보내는 방법을 구성할 수 있습니다.

ONTAP 버전입니다	System Manager를 사용하면…
ONTAP 9.12.1 이상	원격 syslog 서버로 이벤트를 보낼 때 TLS(Transport Layer Security) 프로토콜을 지정합니다.
ONTAP 9.10.1 이상	e-메일 주소, syslog 서버, webhook 애플리케이션 및 SNMP traphosts를 구성합니다.
ONTAP 9.10.0~9.7	SNMP traphosts만 구성합니다. ONTAP CLI로 다른 EMS 대상을 구성할 수 있다. 을 참조하십시오 "EMS 구성 개요".

EMS 이벤트 알림 대상을 추가합니다

System Manager를 사용하여 EMS 메시지를 보낼 위치를 지정할 수 있습니다.

ONTAP 9.12.1부터 EMS 이벤트는 TLS(Transport Layer Security) 프로토콜을 통해 원격 syslog 서버의 지정된 포트로 전송될 수 있습니다. 에 대한 자세한 내용은 `event notification destination create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 알림 관리 * 섹션에서 를 클릭한 ⋮ 다음 * 이벤트 대상 보기 * 를 클릭합니다.

3. 알림 관리 * 페이지에서 * 이벤트 대상 * 탭을 선택합니다.
4. 을 + Add 클릭합니다.
5. 이름, EMS 대상 유형 및 필터를 지정합니다.

   필요한 경우 새 필터를 추가할 수 있습니다. 새 이벤트 필터 추가 * 를 클릭합니다.

6. 선택한 EMS 대상 유형에 따라 다음을 지정합니다.

구성하려면…	지정 또는 선택…
SNMP traphost를 참조하십시오	• traphost 이름입니다
이메일 (9.10.1부터)	• 대상 이메일 주소입니다 • 메일 서버 • 보낸 사람 이메일 주소
Syslog 서버 (9.10.1부터)	• 서버의 호스트 이름 또는 IP 주소입니다 • Syslog 포트(9.12.1로 시작) • Syslog 전송(9.12.1로 시작) TCP 암호화 * 를 선택하면 TLS(Transport Layer Security) 프로토콜이 활성화됩니다. Syslog port * 에 대해 값을 입력하지 않으면 * Syslog transport * 선택 항목에 따라 기본값이 사용됩니다.
웹훅 (9.10.1부터)	• 웹후크 URL • 클라이언트 인증(클라이언트 인증서를 지정하려면 이 옵션 선택)

새 **EMS** 이벤트 알림 필터를 생성합니다

ONTAP 9.10.1부터 시스템 관리자를 사용하여 EMS 알림 처리 규칙을 지정하는 새로운 사용자 지정 필터를 정의할 수 있습니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 알림 관리 * 섹션에서 를 클릭한 다음 * 이벤트 대상 보기 * 를 클릭합니다.
3. 알림 관리 * 페이지에서 * 이벤트 필터 * 탭을 선택합니다.
4. 을 + Add 클릭합니다.
5. 이름을 지정하고 기존 이벤트 필터에서 규칙을 복사할지 또는 새 규칙을 추가할지 여부를 선택합니다.
6. 선택에 따라 다음 단계를 수행하십시오.

선택하십시오.	그런 다음 다음 다음 단계를 수행합니다.

• 기존 이벤트 필터에서 규칙 복사 *	1. 기존 이벤트 필터를 선택합니다. 2. 기존 규칙을 수정합니다. 3. 필요한 경우 을 클릭하여 다른 규칙을 + Add 추가합니다.
• 새 규칙 추가 *	각 새 규칙의 유형, 이름 패턴, 심각도 및 SNMP 트랩 유형을 지정합니다.

EMS 이벤트 알림 대상을 편집합니다

ONTAP 9.10.1부터 시스템 관리자를 사용하여 이벤트 알림 대상 정보를 변경할 수 있습니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 알림 관리 * 섹션에서 를 클릭한 ⋮다음 * 이벤트 대상 보기 * 를 클릭합니다.
3. 알림 관리 * 페이지에서 * 이벤트 대상 * 탭을 선택합니다.
4. 이벤트 대상의 이름 옆에 있는 을 ⋮클릭한 다음 * 편집 * 을 클릭합니다.
5. 이벤트 대상 정보를 수정한 다음 * 저장 * 을 클릭합니다.

EMS 이벤트 알림 필터를 편집합니다

ONTAP 9.10.1.1부터 시스템 관리자를 사용하여 사용자 지정된 필터를 수정하여 이벤트 알림의 처리 방법을 변경할 수 있습니다.

ⓘ 시스템 정의 필터는 수정할 수 없습니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 알림 관리 * 섹션에서 를 클릭한 ⋮다음 * 이벤트 대상 보기 * 를 클릭합니다.
3. 알림 관리 * 페이지에서 * 이벤트 필터 * 탭을 선택합니다.
4. 이벤트 필터 이름 옆에 있는 을 ⋮클릭한 다음 * 편집 * 을 클릭합니다.
5. 이벤트 필터 정보를 수정한 다음 * 저장 * 을 클릭합니다.

EMS 이벤트 알림 대상을 삭제한다

ONTAP 9.10.1부터 System Manager를 사용하여 EMS 이벤트 알림 대상을 삭제할 수 있습니다.

ⓘ SNMP 대상은 삭제할 수 없습니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 알림 관리 * 섹션에서 를 클릭한 ⋮다음 * 이벤트 대상 보기 * 를 클릭합니다.
3. 알림 관리 * 페이지에서 * 이벤트 대상 * 탭을 선택합니다.

4. 이벤트 대상의 이름 옆에 있는 을 클릭한 다음 * 삭제 * 를 클릭합니다.

EMS 이벤트 알림 필터를 삭제한다

ONTAP 9.10.1부터 시스템 관리자를 사용하여 사용자 정의 필터를 삭제할 수 있습니다.

시스템 정의 필터는 삭제할 수 없습니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 알림 관리 * 섹션에서 를 클릭한 다음 * 이벤트 대상 보기 * 를 클릭합니다.
3. 알림 관리 * 페이지에서 * 이벤트 필터 * 탭을 선택합니다.
4. 이벤트 필터 이름 옆에 있는 을 클릭한 다음 * 삭제 * 를 클릭합니다.

관련 정보

- "ONTAP EMS 참조"
- "CLI를 사용하여 이벤트 알림을 수신하도록 SNMP traphosts를 구성합니다"

CLI로 EMS 이벤트 알림을 설정한다

ONTAP EMS 구성 워크플로우

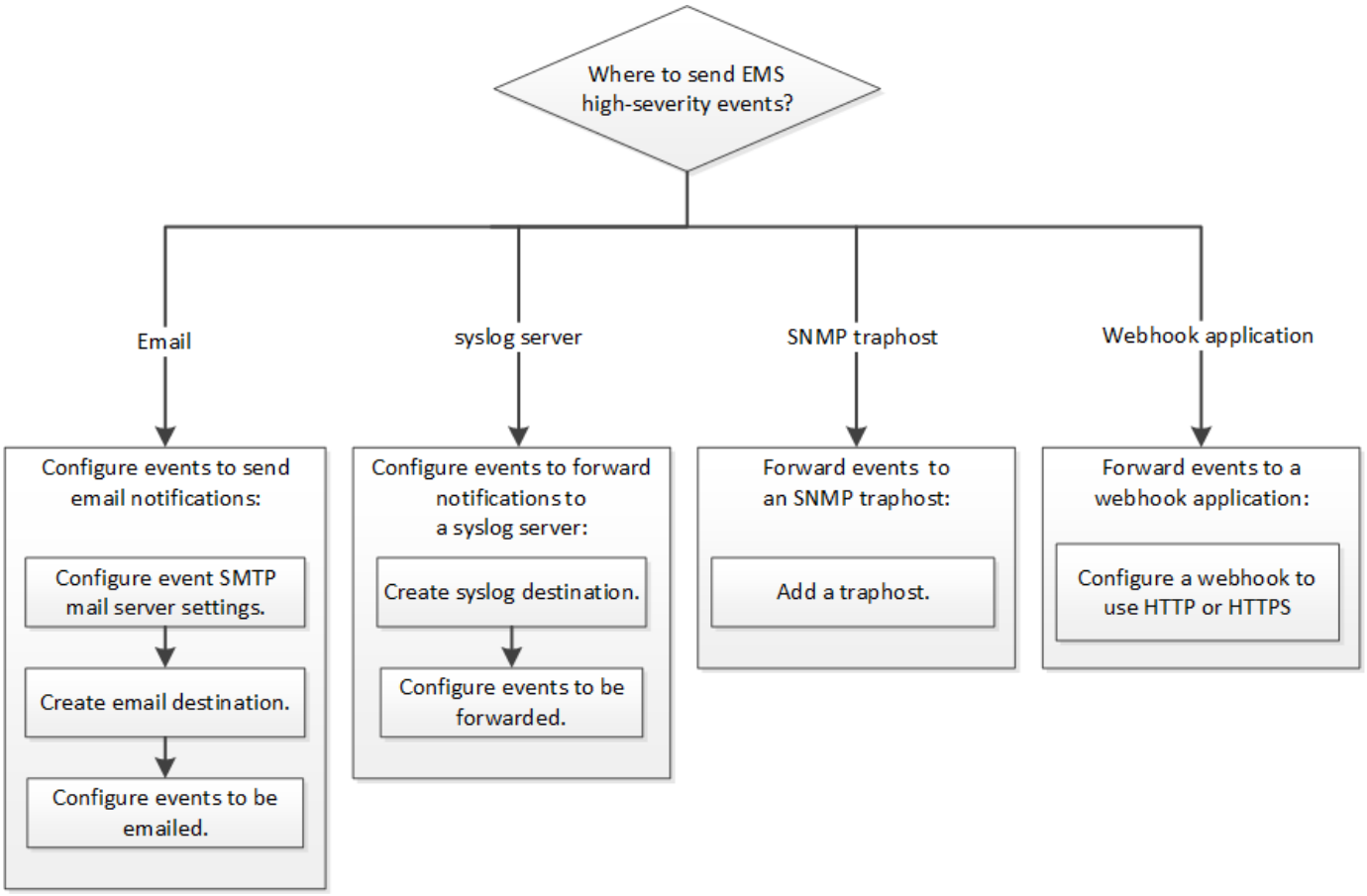
중요한 EMS 이벤트 알림을 e-메일로 보내거나, syslog 서버로 전달하거나, SNMP traphost로 전달하거나, webhook 애플리케이션으로 전달되도록 구성해야 합니다. 이를 통해 적시에 수정 조치를 취함으로써 시스템 중단을 방지할 수 있습니다.

이 작업에 대해

환경에 서버 및 애플리케이션과 같은 다른 시스템에서 기록된 이벤트를 집계하기 위한 syslog 서버가 이미 포함되어 있는 경우, 해당 syslog 서버를 사용하여 스토리지 시스템의 중요한 이벤트 알림도 쉽게 확인할 수 있습니다.

환경에 syslog 서버가 아직 포함되어 있지 않은 경우 중요한 이벤트 알림에 e-메일을 사용하는 것이 더 쉽습니다.

이벤트 알림을 SNMP traaphost에 이미 전달하는 경우 해당 traaphost에서 중요한 이벤트를 모니터링할 수 있습니다.



선택

- 이벤트 알림을 보내도록 EMS를 설정합니다.

원하는 작업	참조 항목…
EMS는 중요한 이벤트 알림을 이메일 주소로 전송합니다	e-메일 알림을 보내도록 중요한 EMS 이벤트를 구성합니다
중요한 이벤트 알림을 syslog 서버로 전달하는 EMS입니다	syslog 서버로 알림을 전달하도록 중요한 EMS 이벤트를 구성합니다
EMS에서 이벤트 알림을 SNMP traaphost로 전달하도록 하려는 경우	이벤트 알림을 수신하도록 SNMP traaphosts를 구성합니다
EMS에서 이벤트 알림을 Webhook 애플리케이션으로 전달하려는 경우	Webhook 애플리케이션에 알림을 전달하도록 중요한 EMS 이벤트를 구성합니다

이메일 알림을 보내도록 중요 **ONTAP EMS** 이벤트를 구성합니다

가장 중요한 이벤트의 이메일 알림을 수신하려면 중요한 활동을 나타내는 이벤트에 대한 이메일 메시지를 보내도록 EMS를 구성해야 합니다.

시작하기 전에

클러스터에서 DNS를 구성하여 이메일 주소를 확인해야 합니다.

이 작업에 대해

ONTAP 명령줄에 명령을 입력하여 클러스터가 실행 중일 때마다 이 작업을 수행할 수 있습니다.

단계

1. 이벤트 SMTP 메일 서버 설정을 구성합니다.

   'event config modify-mail-server mailhost.your_domain-mail-from cluster_admin@your_domain'

   에 대한 자세한 내용은 `event config modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 이벤트 알림을 위한 e-메일 대상 생성:

   '이벤트 알림 대상 create-name storage-admins-email@your_domain'으로 이메일을 보냅니다

   에 대한 자세한 내용은 `event notification destination create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. e-메일 알림을 보내도록 중요한 이벤트를 구성합니다.

   이벤트 알림 create-filter-name important-events-destinations storage-admins입니다

   에 대한 자세한 내용은 `event notification create` "ONTAP 명령 참조입니다"을 참조하십시오.

알림을 **syslog** 서버로 전달하도록 중요한 **ONTAP EMS** 이벤트를 구성합니다

syslog 서버에서 가장 심각한 이벤트의 알림을 기록하려면 중요한 활동을 나타내는 이벤트에 대한 알림을 전달하도록 EMS를 구성해야 합니다.

시작하기 전에

syslog 서버 이름을 확인하기 위해 클러스터에 DNS를 구성해야 합니다.

이 작업에 대해

환경에 이벤트 알림에 대한 syslog 서버가 아직 포함되어 있지 않은 경우 먼저 syslog 서버를 생성해야 합니다. 사용자 환경에 다른 시스템의 이벤트를 로깅하기 위한 syslog 서버가 이미 포함되어 있는 경우 중요한 이벤트 알림에 이 서버를 사용할 수 있습니다.

ONTAP CLI에서 명령을 입력하여 클러스터가 실행 중일 때마다 이 작업을 수행할 수 있습니다.

ONTAP 9.12.1부터 EMS 이벤트는 TLS(Transport Layer Security) 프로토콜을 통해 원격 syslog 서버의 지정된 포트로 전송될 수 있습니다. 두 가지 새로운 매개 변수를 사용할 수 있습니다.

`tcp-encrypted`

시기 `tcp-encrypted` 에 대해 지정됩니다 `syslog-transport`, ONTAP 는 해당 인증서를 검증하여 대상 호스트의 ID를 확인합니다. 기본값은 입니다 `udp-unencrypted`.

`syslog-port`

기본값입니다 `syslog-port` 매개 변수는 의 설정에 따라 다릅니다 `syslog-transport` 매개 변수. If(경우 `syslog-transport` 가 로 설정되어 있습니다 `tcp-encrypted`, `syslog-port` 기본값은 6514입니다.

단계

1. 중요한 이벤트에 대한 syslog 서버 대상을 생성합니다.

   `event notification destination create -name syslog-ems -syslog syslog-server-address -syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}`

   ONTAP 9.12.1부터 에 대해 다음 값을 지정할 수 있습니다 `syslog-transport`:

   - `udp-unencrypted` 보안 기능이 없는 사용자 데이터그램 프로토콜
   - `tcp-unencrypted` 보안 기능이 없는 전송 제어 프로토콜
   - `tcp-encrypted` 전송 계층 보안(TLS)이 있는 전송 제어 프로토콜

     기본 프로토콜은 `udp-unencrypted` 입니다.

   에 대한 자세한 내용은 `event notification destination create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. syslog 서버로 알림을 전달할 중요 이벤트를 구성합니다.

   `event notification create -filter-name important-events -destinations syslog-ems`

   에 대한 자세한 내용은 `event notification create` "ONTAP 명령 참조입니다"을 참조하십시오.

이벤트 알림을 수신하도록 **ONTAP SNMP traphosts**를 구성합니다

SNMP traaphost에서 이벤트 알림을 수신하려면 traphost를 구성해야 합니다.

시작하기 전에

- 클러스터에서 SNMP 및 SNMP 트랩을 활성화해야 합니다.

  SNMP 및 SNMP 트랩은 기본적으로 사용하도록 설정됩니다.

- traphost 이름을 확인하기 위해 클러스터에서 DNS를 구성해야 합니다.

이 작업에 대해

이벤트 알림(SNMP 트랩)을 받도록 구성된 SNMP 트랩 호스트가 아직 없는 경우 이를 추가해야 합니다.

ONTAP 명령줄에 명령을 입력하여 클러스터가 실행 중일 때마다 이 작업을 수행할 수 있습니다.

단계

1. 환경에 이벤트 알림을 수신하도록 구성된 SNMP traaphost가 아직 없는 경우 다음 중 하나를 추가하십시오.

   'System snmp traphost add-peer-address_snmp_traphost_name_'

   기본적으로 SNMP에서 지원하는 모든 이벤트 알림은 SNMP traphost로 전달됩니다.

Webhook 애플리케이션에 알림을 전달하도록 중요한 ONTAP EMS 이벤트를 구성합니다

중요한 이벤트 알림을 Webhook 애플리케이션에 전달하도록 ONTAP를 구성할 수 있습니다. 필요한 구성 단계는 선택한 보안 수준에 따라 다릅니다.

EMS 이벤트 전달을 구성할 준비를 합니다

이벤트 알림을 웹 후크 응용 프로그램으로 전달하도록 ONTAP를 구성하기 전에 고려해야 할 몇 가지 개념과 요구 사항이 있습니다.

Webhook 응용 프로그램

ONTAP 이벤트 알림을 받을 수 있는 웹 후크 응용 프로그램이 필요합니다. Webhook은 사용자가 정의한 콜백 루틴으로, 이 루틴이 실행되는 원격 응용 프로그램 또는 서버의 기능을 확장합니다. Webhook는 대상 URL로 HTTP 요청을 전송하여 클라이언트(이 경우 ONTAP)에 의해 호출되거나 활성화됩니다. 특히 ONTAP는 웹 후크 응용 프로그램을 호스팅하는 서버에 HTTP POST 요청을 보내고 XML로 포맷된 이벤트 알림 세부 정보를 보냅니다.

보안 옵션

TLS(Transport Layer Security) 프로토콜을 사용하는 방법에 따라 몇 가지 보안 옵션을 사용할 수 있습니다. 선택한 옵션에 따라 필요한 ONTAP 구성이 결정됩니다.

TLS는 인터넷에서 널리 사용되는 암호화 프로토콜입니다. 하나 이상의 공개 키 인증서를 사용하여 개인 정보 보호와 데이터 무결성 및 인증을 제공합니다. 인증서는 신뢰할 수 있는 인증 기관에서 발급합니다.

HTTP

HTTP를 사용하여 이벤트 알림을 전송할 수 있습니다. 이 구성에서는 연결이 안전하지 않습니다. ONTAP 클라이언트 및 웹 후크 응용 프로그램의 ID가 확인되지 않습니다. 또한 네트워크 트래픽은 암호화되거나 보호되지 않습니다. 을 참조하십시오 "HTTP를 사용하도록 웹 후크 대상을 구성합니다" 를 참조하십시오.

HTTPS

추가 보안을 위해 Webhook 루틴을 호스팅하는 서버에 인증서를 설치할 수 있습니다. ONTAP는 HTTPS 프로토콜을 사용하여 웹 후크 응용 프로그램 서버의 ID와 네트워크 트래픽의 개인 정보 보호와 무결성을 보장합니다. 을 참조하십시오 "HTTPS를 사용하도록 웹 후크 대상을 구성합니다" 를 참조하십시오.

상호 인증을 사용하는 HTTPS

웹북 요청을 실행하는 ONTAP 시스템에 클라이언트 인증서를 설치하여 HTTPS 보안을 강화할 수 있습니다. webhook 응용 프로그램 서버의 ID를 확인하고 네트워크 트래픽을 보호하는 ONTAP 외에도 webhook 응용 프로그램은 ONTAP 클라이언트의 ID를 확인합니다. 이 양방향 피어 인증을 _Mutual TLS_라고 합니다. 을 참조하십시오 "상호 인증과 함께 HTTPS를 사용하도록 웹 후크 대상을 구성합니다" 를 참조하십시오.

관련 정보

- "TLS(Transport Layer Security) 프로토콜 버전 1.3"

HTTP를 사용하도록 웹 후크 대상을 구성합니다

HTTP를 사용하여 웹 후크 응용 프로그램에 이벤트 알림을 전달하도록 ONTAP를 구성할 수 있습니다. 이 옵션은 가장 안전하지는 않지만 가장 간단한 설치 방법입니다.

단계

1. 이벤트를 수신할 새 대상 'restapi-EMS'를 생성합니다.

   이벤트 알림 목적지 create-name restapi-ems-rest-api-url\http://<webhook-application>`

   위 명령에서 대상에 대해 * HTTP * 체계를 사용해야 합니다.

   에 대한 자세한 내용은 `event notification destination create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 중요 이벤트 필터를 "restapi-EMS" 대상으로 연결하는 알림 생성:

   이벤트 알림 create-filter-name important-events-destinations reapi-EMS

   에 대한 자세한 내용은 `event notification create` "ONTAP 명령 참조입니다"을 참조하십시오.

HTTPS를 사용하도록 웹 후크 대상을 구성합니다

HTTPS를 사용하여 이벤트 알림을 웹 후크 응용 프로그램으로 전달하도록 ONTAP를 구성할 수 있습니다. ONTAP는 서버 인증서를 사용하여 웹 후크 응용 프로그램의 ID를 확인하고 네트워크 트래픽을 보호합니다.

시작하기 전에

- Webhook 응용 프로그램 서버에 대한 개인 키와 인증서를 생성합니다
- ONTAP에 설치할 수 있는 루트 인증서를 가지고 있어야 합니다

단계

1. 웹 후크 응용 프로그램을 호스팅하는 서버에 적절한 서버 개인 키와 인증서를 설치합니다. 특정 구성 단계는 서버에 따라 다릅니다.
2. ONTAP에 서버 루트 인증서 설치:

   보안 인증서설치형 server-ca

   명령이 인증서를 요청합니다.

3. 이벤트를 수신할 'restapi-EMS' 대상을 생성합니다.

   이벤트 알림 목적지 create-name restapi-ems-rest-api-url\https://<webhook-application>`

   위의 명령에서 대상에 대해 * HTTPS * 구성표를 사용해야 합니다.

4. 중요 이벤트 필터를 새 restapi-EMS 대상과 연결하는 알림을 생성합니다.

   이벤트 알림 create-filter-name important-events-destinations reapi-EMS

상호 인증과 함께 **HTTPS**를 사용하도록 웹 후크 대상을 구성합니다

상호 인증을 사용하여 HTTPS를 사용하여 이벤트 알림을 웹 후크 응용 프로그램에 전달하도록 ONTAP를 구성할 수 있습니다. 이 구성에는 두 개의 인증서가 있습니다. ONTAP는 서버 인증서를 사용하여 webhook 응용 프로그램의 ID를 확인하고 네트워크 트래픽을 보호합니다. 또한 webhook를 호스팅하는 응용 프로그램은 클라이언트 인증서를 사용하여 ONTAP 클라이언트의 ID를 확인합니다.

시작하기 전에

ONTAP를 구성하기 전에 다음을 수행해야 합니다.

- Webhook 응용 프로그램 서버에 대한 개인 키와 인증서를 생성합니다
- ONTAP에 설치할 수 있는 루트 인증서를 가지고 있어야 합니다
- ONTAP 클라이언트에 대한 개인 키와 인증서를 생성합니다

단계

1. 작업의 처음 두 단계를 수행합니다 "HTTPS를 사용하도록 웹 후크 대상을 구성합니다" ONTAP가 서버의 ID를 확인할 수 있도록 서버 인증서를 설치합니다.
2. 웹 후크 응용 프로그램에 적절한 루트 및 중간 인증서를 설치하여 클라이언트 인증서를 확인합니다.
3. ONTAP에 클라이언트 인증서 설치:

   보안 인증서 설치형 클라이언트

   명령에서 개인 키와 인증서를 요청합니다.

4. 이벤트를 수신할 'restapi-EMS' 대상을 생성합니다.

   '이벤트 알림 대상 create-name restapi-EMS-REST-API-URL\https://<webhook-application> - certificate-authority <클라이언트 인증서 발급자> - certificate-serial <클라이언트 인증서 직렬>'

   위의 명령에서 대상에 대해 * HTTPS * 구성표를 사용해야 합니다.

5. 중요 이벤트 필터를 새 restapi-EMS 대상과 연결하는 알림을 생성합니다.

   이벤트 알림 create-filter-name important-events-destinations reapi-EMS

관련 정보

- "보안 인증서 설치"

더 이상 사용되지 않는 **EMS** 이벤트 매핑을 업데이트합니다

ONTAP EMS 이벤트 매핑 모델에 대해 알아봅니다

ONTAP 9.0 이전에는 EMS 이벤트가 이벤트 이름 패턴 일치를 기준으로 이벤트 대상에만 매핑될 수 있었습니다. 이 모델을 사용하는 ONTAP 명령 집합('이벤트 대상', '이벤트 경로')은 최신 버전의 ONTAP에서 계속 사용할 수 있지만 ONTAP 9.0부터는 더 이상 사용되지 않습니다.

ONTAP 9.0부터 ONTAP EMS 이벤트 대상 매핑의 모범 사례는 이벤트 필터, 이벤트 알림, 이벤트 알림 대상 명령 집합을 사용하여 여러 필드에서 패턴 일치를 수행하는 보다 확장 가능한 이벤트 필터 모델을 사용하는 것입니다.

더 이상 사용되지 않는 명령을 사용하여 EMS 매핑을 구성한 경우 `event notification`, 및 `event notification destination` 명령 집합을 사용하도록 매핑을 업데이트해야 `event filter` 합니다. 에 대한 자세한 내용은 `event` "ONTAP 명령 참조입니다"을 참조하십시오.

이벤트 대상에는 두 가지 유형이 있습니다.

1. * 시스템 생성 대상 *: 기본적으로 5개의 시스템 생성 이벤트 대상이 있습니다.
   - '대들레부들'
   - "ASUP"
   - '비판들
   - 페이저
   - 트라프호스트

     시스템 생성 대상 중 일부는 특별한 목적으로 사용됩니다. 예를 들어, ASUP 대상은 callhome. * 이벤트를 ONTAP의 AutoSupport 모듈로 라우팅하여 AutoSupport 메시지를 생성합니다.
2. * 사용자 작성 대상 *: '이벤트 목적지 작성' 명령을 사용하여 수동으로 생성됩니다.

```
cluster-1::event*> destination show
                                                                    Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
traphost          -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
test              test@xyz.com      -                  -
false
traphost          -                 -                  -
false
6 entries were displayed.
```

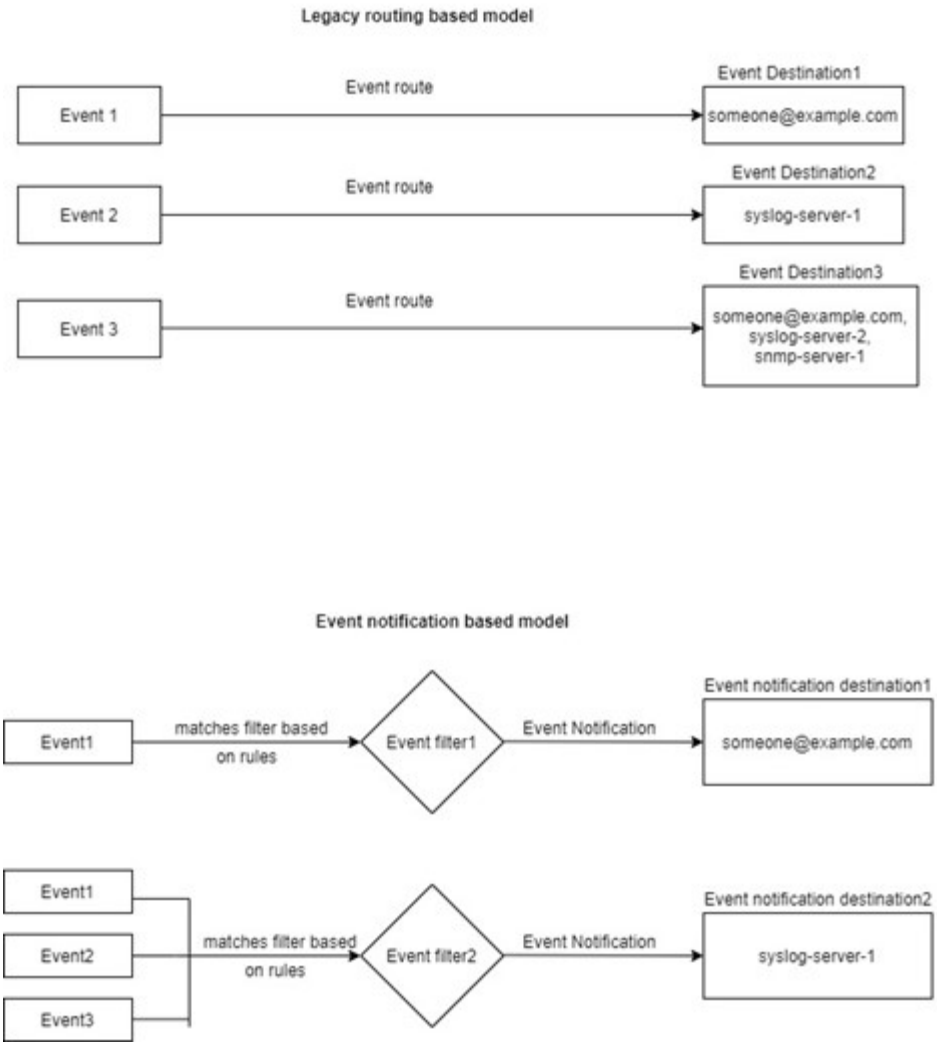
사용되지 않는 모델에서는 이벤트 라우트 add-destinations 명령을 사용하여 EMS 이벤트가 대상에 개별적으로 매핑됩니다.

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                                  Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

보다 확장성이 뛰어난 새로운 EMS 이벤트 알림 메커니즘은 이벤트 필터 및 이벤트 알림 대상을 기반으로 합니다. 새 이벤트 알림 메커니즘에 대한 자세한 내용은 다음 KB 문서를 참조하십시오.

- "ONTAP 9용 이벤트 관리 시스템 개요"



사용되지 않는 명령에서 **ONTAP EMS** 이벤트 매핑을 업데이트합니다

EMS 이벤트 매핑이 사용되지 않는 ONTAP 명령 집합('이벤트 대상', '이벤트 경로')을 사용하여 현재 구성된 경우 다음 절차에 따라 매핑을 업데이트하여 '이벤트 필터', '이벤트 알림' 및 '이벤트 알림 대상' 명령 집합을 사용해야 합니다.

단계

1. 'event destination show' 명령을 사용하여 시스템의 모든 이벤트 대상을 나열합니다.

```
cluster-1::event*> destination show

Hide
Name              Mail Dest.         SNMP Dest.          Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                  -                  -
false
asup              -                  -                  -
false
criticals         -                  -                  -
false
pager             -                  -                  -
false
test              test@xyz.com       -                  -
false
traphost          -                  -                  -
false
6 entries were displayed.
```

2. 각 목적지에 대해 'event route show-destinations <destination name>' 명령어를 이용하여 해당 목적지에 맵핑되는 이벤트를 나열한다.

```
cluster-1::event*> route show -destinations test
                                                                    Freq
Time
Message                           Severity       Destinations    Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort          NOTICE         test            0       0
raid.aggr.autoGrow.success        NOTICE         test            0       0
raid.aggr.lock.conflict           INFORMATIONAL  test            0       0
raid.aggr.log.CP.count            DEBUG          test            0       0
4 entries were displayed.
```

3. 이러한 모든 이벤트 하위 집합을 포함하는 해당 이벤트 필터를 만듭니다. 예를 들어, 'raid.aggr.' * 이벤트만 포함하려면 필터를 생성할 때 'essage-name' 매개 변수에 와일드카드를 사용합니다. 단일 이벤트에 대한 필터를 만들 수도 있습니다.

   에 대한 자세한 내용은 `event filter` "ONTAP 명령 참조입니다"을 참조하십시오.

   최대 50개의 이벤트 필터를 만들 수 있습니다.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. 각 '이벤트 대상' 엔드포인트(SMTP/SNMP/syslog)에 대해 '이벤트 알림 대상'을 생성한다.

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name            Type        Destination
--------------  ----------  --------------------
dest1           email       test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost   snmp        - (from "system snmp traphost")
2 entries were displayed.
```

및 `event destination` 에 대한 자세한 `event notification destination` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

5. 이벤트 필터를 이벤트 알림 대상에 매핑하여 이벤트 알림을 생성합니다.

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                    Destinations
---- ------------------------------ -----------------
1    default-trap-events            snmp-traphost
2    asup_events                    dest1
2 entries were displayed.
```

6. 이벤트 경로 매핑이 있는 각 이벤트 대상에 대해 1-5단계를 반복합니다.

SNMP 대상으로 라우팅된 이벤트는 NMP-traphost 이벤트 알림 대상에 매핑되어야 합니다. SNMP traphost 대상은 시스템에서 구성한 SNMP traphost를 사용합니다.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

               Destination Name: snmp-traphost
             Type of Destination: snmp
                     Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```

ONTAP 명령 참조입니다

각 주요 ONTAP 릴리스의 경우 일반적으로 사용 가능한 CLI 명령(ONTAP 매뉴얼 페이지 또는 man 페이지)이 번들로 제공됩니다. "ONTAP 명령 참조" 이러한 명령 참조에서는 각 ONTAP 릴리스에서 CLI 명령을 사용하는 방법을 설명합니다.

ONTAP 명령줄에서도 Man 페이지를 사용할 수 있습니다. `man` 명령. 자세히 알아보세요 `man` 에서 "ONTAP 명령 참조입니다" .

제한된 ONTAP 지원 버전에 대한 명령 참조(PDF만 해당)

- "ONTAP 9.4"

CLI 비교 툴

을 사용하여 ONTAP 릴리스 간에 CLI(Command-Line Interface) 명령의 변경 사항을 확인할 수 있습니다 "CLI 비교 도구" 를 방문하십시오.

관련 정보

- ONTAP 명령줄 인터페이스를 사용합니다
- CLI 명령 디렉토리 탐색 방법
- "저장 디스크 표시"

법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인 정보 보호 정책

"https://www.netapp.com/company/legal/privacy-policy/"

오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이센스에 대한 정보를 제공합니다.

ONTAP

"ONTAP 9.18.1에 대한 공지" "ONTAP 9.17.1에 대한 공지" "ONTAP 9.16.1 참고 사항" "ONTAP 9.16.0 참고 사항" "ONTAP 9.15.1에 대한 고지 사항" "ONTAP 9.15.0에 대한 고지 사항" "ONTAP 9.14.1에 대한 고지 사항" "ONTAP 9.14.0에 대한 고지 사항" "ONTAP 9.13.1 참고 사항" "ONTAP 9.12.1에 대한 고지 사항" "ONTAP 9.12.0에 대한 고지 사항" "ONTAP 9.11.1에 대한 고지 사항" "ONTAP 9.10.1에 대한 고지 사항" "ONTAP 9.10.0에 대한 고지 사항" "ONTAP 9.9.1에 대한 참고 사항" "ONTAP 9.8에 대한 고지 사항" "ONTAP 9.7에 대한 고지 사항" "ONTAP 9.6에 대한 고지 사항" "ONTAP 9.5에 대한 고지 사항" "ONTAP 9.4에 대한 고지 사항" "ONTAP 9.3에 대한 고지 사항" "ONTAP 9.2에 대한 고지 사항" "ONTAP 9.1에 대한 참고 사항"

MetroCluster IP 구성을 위한 ONTAP 중재자

"ONTAP Mediator 1.11에 대한 공지" "ONTAP Mediator 1.10에 대한 공지" "ONTAP Mediator 1.9.1에 대한 공지" "ONTAP Mediator 1.8에 대한 공지" "ONTAP Mediator 1.7에 대한 공지" "ONTAP Mediator 1.5에 대한 공지"

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.