



Active IQ Unified Manager 문서

Active IQ Unified Manager

NetApp
October 15, 2025

목차

Active IQ Unified Manager 문서	1
릴리스 노트	2
시작하기	3
VMware 설치를 위한 빠른 시작 지침	3
시스템 요구 사항	3
Active IQ Unified Manager 설치	3
Linux 설치를 위한 빠른 시작 지침	4
시스템 요구 사항	4
Active IQ Unified Manager 설치	4
Windows 설치를 위한 빠른 시작 지침	5
시스템 요구 사항	5
Active IQ Unified Manager 설치	6
VMware vSphere 시스템에 Unified Manager 설치	7
Active IQ Unified Manager 소개	7
Unified Manager 서버가 수행하는 작업	7
설치 순서 개요	7
Unified Manager 설치 요구 사항	8
가상 인프라 및 하드웨어 시스템 요구 사항	8
VMware 소프트웨어 및 설치 요구 사항	9
지원되는 브라우저	10
프로토콜 및 포트 요구 사항	10
워크시트를 완성하세요	14
Unified Manager 소프트웨어 설치, 업그레이드 및 제거	16
배포 프로세스 개요	16
Unified Manager 배포	17
Unified Manager 업그레이드	20
Unified Manager 가상 머신을 다시 시작합니다.	23
통합 관리자 제거	23
Linux 시스템에 Unified Manager 설치	24
Active IQ Unified Manager 소개	24
Unified Manager 서버가 수행하는 작업	24
설치 순서 개요	24
Unified Manager 설치 요구 사항	25
가상 인프라 및 하드웨어 시스템 요구 사항	25
Linux 소프트웨어 및 설치 요구 사항	27
지원되는 브라우저	29
프로토콜 및 포트 요구 사항	29
워크시트를 완성하세요	32
Unified Manager 소프트웨어 설치, 업그레이드 및 제거	34

설치 과정 개요	34
필요한 소프트웨어 저장소 설정	35
NFS 및 CIFS 공유에 대한 SELinux 요구 사항	37
Linux 시스템에 Unified Manager 설치	40
Red Hat Enterprise Linux에서 Unified Manager 업그레이드	46
Unified Manager 설치 후 타사 제품 업그레이드	51
Unified Manager를 다시 시작하세요	51
통합 관리자 제거	52
사용자 정의 umadmin 사용자 및 유지 관리 그룹 제거	53
Windows 시스템에 Unified Manager 설치	54
Active IQ Unified Manager 소개	54
Unified Manager 서버가 수행하는 작업	54
설치 순서 개요	54
Unified Manager 설치 요구 사항	55
가상 인프라 및 하드웨어 시스템 요구 사항	55
Windows 소프트웨어 및 설치 요구 사항	56
지원되는 브라우저	58
프로토콜 및 포트 요구 사항	58
워크시트를 완성하세요	61
Unified Manager 소프트웨어 설치, 업그레이드 및 제거	63
설치 과정 개요	63
Windows에 Unified Manager 설치	64
JBoss 비밀번호 변경	67
Unified Manager 버전에 지원되는 업그레이드 경로	68
Unified Manager 업그레이드	69
타사 제품 업그레이드	70
타사 제품 제거	71
Unified Manager를 다시 시작하세요	72
Unified Manager 제거	72
구성 및 관리 작업 수행	74
Active IQ Unified Manager 구성	74
구성 순서 개요	74
Unified Manager 웹 UI에 액세스하세요	74
Unified Manager 웹 UI의 초기 설정을 수행합니다.	75
클러스터 추가	77
Unified Manager를 구성하여 알림 알림을 보냅니다.	79
로컬 사용자 비밀번호 변경	87
세션 비활성 시간 초과 설정	87
CLI를 통해 세션 시간 초과 설정	88
Unified Manager 호스트 이름 변경	88
정책 기반 스토리지 관리 활성화 및 비활성화	92

Unified Manager 백업 구성	93
기능 설정 관리	93
정책 기반 스토리지 관리 활성화	93
API 게이트웨이 활성화	94
비활성 시간 초과 지정	94
Active IQ 포털 이벤트 활성화	94
규정 준수를 위한 보안 설정 활성화 및 비활성화	95
스크립트 업로드 활성화 및 비활성화	96
로그인 배너 추가	96
유지 관리 콘솔을 사용하세요	96
유지 관리 콘솔이 제공하는 기능은 무엇입니까?	96
유지 관리 사용자가 하는 일	97
진단 사용자 기능	97
유지 관리 콘솔에 액세스하세요	97
vSphere VM 콘솔을 사용하여 유지 관리 콘솔에 액세스합니다.	98
유지 관리 콘솔 메뉴	99
Windows에서 유지 관리 사용자 비밀번호 변경	104
Linux 시스템에서 umadmin 비밀번호 변경	104
Unified Manager가 HTTP 및 HTTPS 프로토콜에 사용하는 포트를 변경합니다.	104
네트워크 인터페이스 추가	105
Unified Manager 데이터베이스 디렉토리에 디스크 공간 추가	106
사용자 액세스 관리	109
사용자 추가	109
사용자 설정 편집	111
사용자 보기	111
사용자 또는 그룹 삭제	111
RBAC란 무엇인가	112
역할 기반 액세스 제어는 무엇을 합니까?	112
사용자 유형의 정의	112
사용자 역할의 정의	113
Unified Manager 사용자 역할 및 기능	114
SAML 인증 설정 관리	115
ID 공급자 요구 사항	115
SAML 인증 활성화	117
SAML 인증에 사용되는 ID 공급자 변경	118
Unified Manager 보안 인증서 변경 후 SAML 인증 설정 업데이트	118
SAML 인증 비활성화	119
유지 관리 콘솔에서 SAML 인증 비활성화	120
SAML 인증 페이지	121
인증 관리	121
인증 서버 편집	122

인증 서버 삭제	122
Active Directory 또는 OpenLDAP를 통한 인증	122
감사 로깅	123
원격 인증 페이지	125
보안 인증서 관리	128
HTTPS 보안 인증서 보기	128
HTTPS 인증서 서명 요청 다운로드	129
CA 서명 및 반환된 HTTPS 인증서 설치	129
외부 도구를 사용하여 생성된 HTTPS 인증서 설치	130
인증서 관리를 위한 페이지 설명	132
스토리지 모니터링 및 관리	135
Active IQ Unified Manager 소개	135
Active IQ Unified Manager 상태 모니터링 소개	135
Active IQ Unified Manager 성능 모니터링 소개	136
Unified Manager REST API 사용	137
Unified Manager 서버가 수행하는 작업	137
사용자 인터페이스를 이해하세요	138
일반적인 창 레이아웃	138
창 레이아웃 사용자 정의	139
Unified Manager 도움말 사용	140
즐거찾는 도움말 항목을 북마크하세요	141
저장소 객체 검색	141
저장소 데이터를 보고서로 내보내기	142
필터 인벤토리 페이지 콘텐츠	143
알림 벨에서 활성 이벤트 보기	144
대시보드에서 클러스터를 모니터링하고 관리합니다.	145
대시보드 페이지	146
Unified Manager에서 직접 ONTAP 문제 또는 기능을 관리하세요.	148
클러스터 관리	155
클러스터 검색 프로세스 작동 방식	155
모니터링되는 클러스터 목록 보기	156
클러스터 추가	156
클러스터 편집	158
클러스터 제거	159
클러스터 재발견	159
VMware 가상 인프라 모니터링	160
지원되지 않는 사항	162
vCenter Server 보기 및 추가	163
vCenter Server 제거	165
가상 머신 모니터링	165
재해 복구 설정에서 가상 인프라 보기	167

워크로드 프로비저닝 및 관리	168
워크로드 개요	169
성능 서비스 수준	175
스토리지 효율성 정책 관리	181
MetroCluster 구성 관리 및 모니터링	183
스위치오버 및 스위치백 중 볼륨 동작	183
FC 구성을 통한 MetroCluster 에 대한 클러스터 연결 상태 정의	186
FC를 통한 MetroCluster 에 대한 데이터 미러링 상태 정의	186
MetroCluster 구성 모니터링	187
MetroCluster 복제 모니터링	189
할당량 관리	190
할당량 한도는 무엇입니까?	191
사용자 및 사용자 그룹 할당량 보기	191
이메일 주소를 생성하는 규칙을 만듭니다.	191
사용자 및 사용자 그룹 할당량에 대한 이메일 알림 형식을 만듭니다.	192
사용자 및 그룹 할당량 이메일 주소 편집	192
할당량에 대해 자세히 알아보세요	193
할당량 대화 상자 설명	194
문제 해결	197
Unified Manager 데이터베이스 디렉토리에 디스크 공간 추가	197
성능 통계 수집 간격 변경	200
Unified Manager가 이벤트 및 성능 데이터를 보관하는 기간 변경	201
알 수 없는 인증 오류	202
사용자를 찾을 수 없습니다	202
다른 인증 서비스를 사용하여 LDAP를 추가하는 데 문제가 있습니다.	203
Windows 시스템의 NetApp Manageability SDK 로그 회전 문제	203
이벤트 및 알림 관리	204
이벤트 관리	204
Active IQ 플랫폼 이벤트는 무엇입니까?	204
이벤트 관리 시스템 이벤트란 무엇입니까?	204
이벤트가 수신되면 어떻게 되나요?	210
이벤트 및 이벤트 세부 정보 보기	211
할당되지 않은 이벤트 보기	212
이벤트 확인 및 해결	212
특정 사용자에게 이벤트 할당	213
원치 않는 이벤트 비활성화	214
Unified Manager 자동 수정을 사용하여 문제 해결	215
Active IQ 이벤트 보고 활성화 및 비활성화	216
새로운 Active IQ 규칙 파일 업로드	216
Active IQ 플랫폼 이벤트가 생성되는 방식	217
Active IQ 플랫폼 이벤트 해결	218

이벤트 보존 설정 구성	219
Unified Manager 유지 관리 기간이란 무엇입니까?	219
호스트 시스템 리소스 이벤트 관리	221
이벤트에 대해 더 자세히 알아보세요	222
이벤트 및 심각도 유형 목록	227
이벤트 창 및 대화 상자 설명	279
알림 관리	291
어떤 알림이 있나요?	292
알림 이메일에는 어떤 정보가 포함되어 있나요?	292
알림 추가	293
성능 이벤트에 대한 알림 추가	295
테스트 알림	296
해결됨 및 폐기됨 이벤트에 대한 알림 활성화 및 비활성화	296
재해 복구 대상 볼륨을 경고 생성에서 제외합니다.	297
알림 보기	298
알림 편집	298
알림 삭제	298
경고 창 및 대화 상자 설명	299
스크립트 관리	305
스크립트가 알림과 함께 작동하는 방식	305
스크립트 추가	306
스크립트 삭제	307
테스트 스크립트 실행	307
지원되는 Unified Manager CLI 명령	308
스크립트 창 및 대화 상자 설명	313
클러스터 성능 모니터링 및 관리	315
Active IQ Unified Manager 성능 모니터링 소개	315
Unified Manager 성능 모니터링 기능	315
스토리지 시스템 성능을 관리하는 데 사용되는 Unified Manager 인터페이스	316
클러스터 구성 및 성능 데이터 수집 활동	316
데이터 연속성 수집 주기란 무엇입니까?	317
수집된 데이터 및 이벤트에서 타임스탬프가 의미하는 것	318
Unified Manager GUI에서 성능 워크플로 탐색	318
UI에 로그인	319
그래픽 인터페이스 및 탐색 경로	319
저장소 객체 검색	325
필터 인벤토리 페이지 콘텐츠	326
대시보드에서 클러스터 성능 모니터링	328
대시보드의 성능 패널 이해하기	328
성능 배너 메시지 및 설명	328
성능 통계 수집 간격 변경	329

워크로드 분석기를 사용하여 워크로드 문제 해결	330
워크로드 분석기는 어떤 데이터를 표시합니까?	330
워크로드 분석기는 언제 사용합니까?	331
워크로드 분석기를 사용하세요	332
성능 클러스터 랜딩 페이지에서 클러스터 성능을 모니터링합니다.	332
성능 클러스터 랜딩 페이지 이해하기	332
성능 클러스터 랜딩 페이지	333
성능 인벤토리 페이지를 사용하여 성능 모니터링	337
모든 스토리지 개체에 대한 성능 인벤토리 페이지 보기	338
성능 인벤토리 페이지 내용 개선	343
클라우드로 데이터를 계층화하기 위한 Unified Manager 권장 사항을 이해합니다.	345
성능 탐색기 페이지를 사용하여 성능 모니터링	347
루트 객체를 이해하세요	347
그리드에서 상관관계가 있는 객체 목록을 줄이기 위해 필터링을 적용합니다.	347
상관관계가 있는 객체에 대한 시간 범위를 지정합니다.	347
비교 그래프를 위한 상관관계가 있는 객체 목록 정의	349
카운터 차트 이해하기	350
성과 카운터 차트의 유형	351
표시할 성과 차트를 선택하세요	353
카운터 차트 창 확장	353
카운터 차트 초점을 더 짧은 기간으로 변경합니다.	354
이벤트 타임라인에서 이벤트 세부 정보 보기	354
카운터 차트 확대 보기	355
클러스터 구성 요소별 볼륨 지연 시간 보기	357
프로토콜별 SVM IOPS 트래픽 보기	358
성능 보장을 확인하려면 볼륨 및 LUN 지연 차트를 확인하세요.	358
모든 SAN 어레이 클러스터의 성능 보기	359
로컬 노드에만 있는 작업 부하를 기반으로 노드 IOPS 보기	359
객체 랜딩 페이지의 구성 요소	360
QoS 정책 그룹 정보를 사용하여 성능 관리	365
스토리지 QoS가 작업 부하 처리량을 제어하는 방법	366
모든 클러스터에서 사용 가능한 모든 QoS 정책 그룹 보기	367
동일한 QoS 정책 그룹에 있는 볼륨 또는 LUN 보기	367
특정 볼륨 또는 LUN에 적용된 QoS 정책 그룹 설정을 확인합니다.	368
동일한 QoS 정책 그룹에 있는 볼륨이나 LUN을 비교하기 위해 성능 차트를 봅니다.	368
처리량 차트에 다양한 유형의 QoS 정책이 표시되는 방식	369
성능 탐색기에서 작업 부하 QoS 최소 및 최대 설정 보기	370
성능 용량 및 사용 가능한 IOPS 정보를 사용하여 성능을 관리합니다.	371
사용된 성능 용량은 무엇입니까?	372
성능 용량 사용 가치의 의미	373
사용 가능한 IOPS는 무엇입니까?	374

노드 보기 및 사용된 성능 용량 집계 값	375
노드 보기 및 사용 가능한 IOPS 값 집계	375
문제를 식별하기 위해 성능 용량 카운터 차트를 확인하세요.	376
성능 용량 사용 성능 임계값 조건	377
성능 관리에 사용된 성능 용량 카운터를 사용합니다.	378
노드 장애 조치 계획 페이지를 이해하고 사용하세요	378
노드 장애 조치 계획 페이지를 사용하여 시정 조치를 결정합니다.	379
노드 장애 조치 계획 페이지의 구성 요소	379
노드 장애 조치 계획 페이지에서 임계값 정책 사용	380
장애 조치 계획을 위해 성능 용량 사용 분석 차트를 사용하세요.	381
데이터 수집 및 워크로드 성능 모니터링	382
Unified Manager에서 모니터링하는 작업 유형	383
작업 부하 성능 측정 값	384
기대되는 성능 범위는 무엇입니까?	385
성능 분석에서 지연 시간 예측이 사용되는 방식	386
Unified Manager가 워크로드 대기 시간을 사용하여 성능 문제를 식별하는 방법	387
클러스터 작업이 워크로드 대기 시간에 어떤 영향을 미칠 수 있는지	388
MetroCluster 구성의 성능 모니터링	389
성능 이벤트 및 알림 이해	390
성과 이벤트의 소스	390
성능 이벤트 심각도 유형	390
Unified Manager에서 감지된 구성 변경 사항	391
시스템 정의 성능 임계값 정책 유형	392
성능 이벤트 분석 및 알림	394
Unified Manager가 이벤트의 성능 영향을 결정하는 방법	396
클러스터 구성 요소와 이들이 경쟁에 참여할 수 있는 이유	396
성능 이벤트에 관련된 작업 부하의 역할	398
성능 임계값 관리	399
사용자 정의 성능 임계값 정책의 작동 방식	400
성능 임계값 정책이 위반되면 어떻게 되나요?	401
임계값을 사용하여 추적할 수 있는 성능 카운터는 무엇입니까?	401
조합 임계값 정책에서 어떤 객체와 카운터를 사용할 수 있습니까?	403
사용자 정의 성능 임계값 정책 생성	404
스토리지 개체에 성능 임계값 정책 할당	405
성능 임계값 정책 보기	406
사용자 정의 성능 임계값 정책 편집	407
스토리지 개체에서 성능 임계값 정책 제거	407
성능 임계값 정책이 변경되면 어떻게 되나요?	408
객체가 이동되면 성능 임계값 정책은 어떻게 되나요?	408
성능 이벤트 분석	409
성능 이벤트에 대한 정보 표시	409

사용자 정의 성능 임계값에서 이벤트 분석	410
시스템 정의 성능 임계값에서 이벤트 분석	411
동적 성능 임계값에서 이벤트 분석	416
성능 이벤트 해결	423
지연 시간이 예상 범위 내에 있는지 확인하세요.	423
구성 변경이 워크로드 성능에 미치는 영향을 검토합니다.	423
클라이언트 측에서 작업 부하 성능을 개선하기 위한 옵션	424
클라이언트 또는 네트워크 문제를 확인하세요	424
QoS 정책 그룹의 다른 볼륨에 비정상적으로 높은 활동이 있는지 확인하십시오.	424
논리적 인터페이스(LIF) 이동	425
덜 바쁜 시간에 스토리지 효율성 작업을 실행하세요.	425
디스크 추가 및 데이터 재할당	426
노드에서 Flash Cache를 활성화하면 작업 부하 성능이 어떻게 향상될 수 있나요?	427
스토리지 집계에서 Flash Pool을 활성화하면 워크로드 성능이 어떻게 향상될 수 있나요?	427
MetroCluster 구성 상태 점검	427
MetroCluster 구성 확인	428
워크로드를 다른 집계로 이동	428
워크로드를 다른 노드로 이동	429
다른 노드의 집계로 작업 부하 이동	431
다른 HA 쌍의 노드로 작업 부하 이동	432
다른 HA 쌍의 다른 노드로 작업 부하 이동	434
QoS 정책 설정을 사용하여 이 노드의 작업 우선 순위를 지정합니다.	436
비활성 볼륨 및 LUN 제거	436
디스크를 추가하고 집계 레이아웃 재구성을 수행합니다.	437
Unified Manager 서버와 외부 데이터 공급자 간의 연결 설정	437
외부 서버로 전송할 수 있는 성능 데이터	437
Unified Manager에서 성능 데이터를 수신하도록 Graphite를 설정합니다.	438
Unified Manager 서버에서 외부 데이터 공급자로의 연결 구성	439
클러스터 상태 모니터링 및 관리	442
Active IQ Unified Manager 상태 모니터링 소개	442
물리적 및 논리적 용량	442
용량 측정 단위	442
Unified Manager 상태 모니터링 기능	443
스토리지 시스템 상태를 관리하는 데 사용되는 Unified Manager 인터페이스	444
클러스터 및 클러스터 개체 상태 관리 및 모니터링	444
클러스터 모니터링 이해하기	445
클러스터 목록 및 세부 정보 보기	446
MetroCluster 구성에서 클러스터의 상태를 확인합니다.	447
모든 SAN 어레이 클러스터의 상태 및 용량 상태를 확인합니다.	449
노드 목록 및 세부 정보 보기	449
계약 갱신을 위한 하드웨어 인벤토리 보고서 생성	450

저장소 VM 목록 및 세부 정보 보기	450
집계 목록 및 세부 정보 보기	451
FabricPool 용량 정보 보기	452
스토리지 풀 세부 정보 보기	453
볼륨 목록 및 세부 정보 보기	453
NFS 공유에 대한 세부 정보 보기	454
SMB/CIFS 주식에 대한 세부 정보 보기	455
스냅샷 복사본 목록 보기	455
스냅샷 사본 삭제	456
스냅샷 복사본에 대한 회수 가능 공간 계산	457
클러스터 객체 창 및 대화 상자 설명	457
공통 Unified Manager 상태 워크플로 및 작업	458
데이터 가용성 모니터링 및 문제 해결	459
용량 문제 해결	465
건강 임계값 관리	466
클러스터 보안 목표 관리	471
백업 및 복원 작업 관리	483
스크립트 관리	497
그룹 관리 및 모니터링	500
주석을 사용하여 스토리지 개체 이벤트의 우선 순위 지정	508
웹 UI 및 유지 관리 콘솔을 통해 지원 번들을 보내세요	516
여러 워크플로와 관련된 작업 및 정보	523
데이터 보호 및 복원	578
보호 관계 생성, 모니터링 및 문제 해결	578
SnapMirror 보호 유형	578
Unified Manager에서 보호 관계 설정	579
보호 관계 장애 조치 및 장애 복구 수행	582
보호 작업 실패 해결	586
지연 문제 해결	589
보호 관계 관리 및 모니터링	590
볼륨 보호 상태 보기	591
볼륨 보호 관계 보기	592
일관성 그룹 관계에서 LUN 모니터링	593
Health: All Volumes 보기에서 SnapVault 보호 관계를 만듭니다.	594
볼륨/상태 세부 정보 페이지에서 SnapVault 보호 관계를 만듭니다.	595
Health: All Volumes 보기에서 SnapMirror 보호 관계를 만듭니다.	596
볼륨/상태 세부 정보 페이지에서 SnapMirror 보호 관계를 만듭니다.	597
버전에 따라 유연한 복제를 통해 SnapMirror 관계 생성	598
백업 옵션이 있는 버전 유연한 복제를 통해 SnapMirror 관계 생성	599
목적지 효율성 설정 구성	600
SnapMirror 및 SnapVault 일정 만들기	600

기존 보호 관계에서 보호를 확장하기 위해 계단식 또는 팬아웃 관계를 만듭니다.	601
볼륨 관계 페이지에서 보호 관계 편집	601
볼륨/상태 세부 정보 페이지에서 보호 관계 편집	602
전송 효율성을 극대화하기 위해 SnapMirror 정책을 만듭니다.	602
전송 효율성을 극대화하기 위해 SnapVault 정책을 만듭니다.	603
볼륨 관계 페이지에서 활성 데이터 보호 전송을 중단합니다.	604
볼륨/상태 세부 정보 페이지에서 활성 데이터 보호 전송을 중단합니다.	604
볼륨 관계 페이지에서 보호 관계 중지	605
볼륨/상태 세부 정보 페이지에서 보호 관계 중지	606
볼륨 관계 페이지에서 SnapMirror 관계 해제	606
볼륨 관계 페이지에서 보호 관계 제거	607
볼륨 관계 페이지에서 정지된 관계에 대한 예약된 전송을 재개합니다.	607
볼륨/상태 세부 정보 페이지에서 정지된 관계에 대한 예약된 전송을 재개합니다.	608
볼륨 관계 페이지에서 보호 관계를 초기화하거나 업데이트합니다.	608
볼륨/상태 세부 정보 페이지에서 보호 관계 초기화 또는 업데이트	609
볼륨 관계 페이지에서 보호 관계를 다시 동기화합니다.	610
볼륨 관계 페이지에서 역방향 보호 관계	611
볼륨 및 볼륨/상태 세부 정보 페이지를 사용하여 데이터 복원	612
리소스 풀은 무엇입니까?	613
리소스 풀 생성	614
리소스 풀 편집	614
리소스 풀 인벤토리 보기	614
리소스 풀 멤버 추가	615
리소스 풀에서 집계 제거	615
리소스 풀 삭제	616
스토리지 VM 재해 복구 보호 관계 모니터링	616
스토리지 VM 연결 이해	618
스토리지 서비스를 지원하기 위한 SVM 및 리소스 풀 요구 사항	620
어떤 직업이 있나요?	621
작업 모니터링	621
채용공고 세부정보 보기	621
작업 중단	622
실패한 보호 작업을 다시 시도합니다.	622
보호 관계 창 및 대화 상자 설명	622
사용자 정의 보고서 생성	663
통합 관리자 보고	663
보고서 생성을 위한 액세스 포인트	663
보고서 이해	665
뷰와 보고서 관계 이해	665
보고서 유형	666
보고 제한 사항	667

보고서 작업	668
보고서 워크플로	668
빠른 시작 보고	669
예약된 보고서 검색	672
보고서 사용자 정의	672
보고서 다운로드	676
일정 보고서	676
보고서 예약	676
보고서 일정 관리	679
샘플 사용자 정의 보고서	681
클러스터 스토리지 보고서 사용자 정의	681
집계 용량 보고서 사용자 정의	684
볼륨 용량 보고서 사용자 정의	686
Qtree 용량 보고서 사용자 정의	689
NFS 공유 보고서 사용자 정의	690
스토리지 VM 보고서 사용자 정의	691
볼륨 관계 보고서 사용자 정의	693
볼륨 성능 보고서 사용자 정의	696
Microsoft Excel 보고서 샘플	697
집계 용량 표와 차트를 보여주는 보고서 만들기	697
총합계와 사용 가능한 용량 차트를 보여주는 보고서를 만듭니다.	700
사용 가능한 볼륨 용량 차트를 보려면 보고서를 만드세요.	703
가장 많은 사용 가능한 IOPS를 포함하는 집계를 보려면 보고서를 만듭니다.	705
REST API를 사용하여 스토리지 관리	708
Active IQ Unified Manager REST API 시작하기	708
이 콘텐츠의 대상 고객	708
Active IQ Unified Manager API 액세스 및 범주	708
Active IQ Unified Manager 에서 제공되는 REST 서비스	709
Active IQ Unified Manager 의 API 버전	710
ONTAP 의 스토리지 리소스	711
Active IQ Unified Manager 의 REST API 액세스 및 인증	712
인증	714
Active IQ Unified Manager 에서 사용되는 HTTP 상태 코드	715
Active IQ Unified Manager 용 API 사용에 대한 권장 사항	716
문제 해결을 위한 로그	716
작업 객체 비동기 프로세스	717
안녕하세요 API 서버	718
통합 관리자 REST API	722
API를 사용하여 데이터 센터의 스토리지 객체를 관리합니다.	722
프록시 액세스를 통해 ONTAP API에 액세스	727
API를 사용하여 관리 작업 수행	730

API를 사용하여 사용자 관리	731
API를 사용하여 성능 지표 보기	732
작업 및 시스템 세부 정보 보기	741
API를 사용하여 이벤트 및 알림 관리	742
API를 사용하여 작업 부하 관리	744
스토리지 관리를 위한 공통 API 워크플로	753
워크플로에서 사용되는 API 호출을 이해합니다.	753
API를 사용하여 집계의 공간 문제 확인	753
이벤트 API를 사용하여 스토리지 객체의 문제 확인	755
게이트웨이 API를 사용하여 ONTAP 볼륨 문제 해결	756
워크로드 관리를 위한 API 워크플로	759
법적 고지 사항	785
저작권	785
상표	785
특허	785
개인정보 보호정책	785
오픈소스	785

Active IQ Unified Manager 문서

릴리스 노트

Active IQ Unified Manager 9.16의 새로운 기능, 제한 사항 및 알려진 문제에 대한 요약을 제공합니다.

자세한 내용은 다음을 참조하세요. "[Active IQ Unified Manager 릴리스 노트](#)".

시작하기

VMware 설치를 위한 빠른 시작 지침

다운로드할 수 있습니다 .tar 루트 인증서가 포함된 파일 README 파일 및 OVA 파일을 만들고 Unified Manager를 가상 어플라이언스로 배포합니다.

시스템 요구 사항

- 운영 체제: VMware ESXi 8.0
- 램: 12GB
- CPU: 총 9572MHz
- 여유 디스크 공간: 5GB(싹 프로비저닝), 152GB(싹 프로비저닝)

자세한 시스템 요구 사항은 다음을 참조하세요. "[Unified Manager 설치 요구 사항](#)" 그리고 "[상호 운용성 매트릭스](#)".

Active IQ Unified Manager 설치

설치 프로그램을 다운로드하세요

1. 다운로드 .tar 루트 인증서가 포함된 파일 README 파일 및 OVA 파일.
2. vSphere Client에서 액세스할 수 있는 로컬 디렉토리나 네트워크 디렉토리에 파일을 저장합니다.
3. 다운로드한 디렉토리에서 .tar 파일을 입력하세요 `tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz` 명령. + 필요한 OVA 파일, 루트 인증서 및 README 파일이 대상 디렉토리에 압축 해제됩니다.

무결성 확인

당신은의 무결성을 확인할 수 있습니다 OVA 제공된 단계에 따라 파일을 README 파일.

Unified Manager 설치

1. vSphere Client에서 *파일 > OVF 템플릿 배포*를 클릭합니다.
2. OVA 파일을 찾아 마법사를 사용하여 ESXi 서버에 가상 어플라이언스를 배포합니다.
3. 검토 세부 정보 페이지의 게시자 섹션에서 메시지 Entrust Code Signing - OVCS2 (Trusted certificate) 다운로드한 파일의 무결성을 확인합니다 OVA 파일. 메시지에 대하여 Entrust Code Signing - OVCS2 (Invalid certificate) VMware vCenter Server를 7.0U3E 이상 버전으로 업그레이드하세요.
4. 사용자 지정 템플릿 페이지의 속성 탭에서 수행 중인 설치 유형에 따라 필요한 필드를 채웁니다.
 - 정적 구성의 경우 모든 필드에 필요한 정보를 입력하세요. 보조 **DNS** 필드에 대한 정보를 추가할 필요는 없습니다.
 - IPv4를 사용하는 DHCP의 경우, 어떤 필드에도 정보를 추가하지 마세요.
 - IPv6를 사용하는 DHCP의 경우 "자동 IPv6 주소 지정 사용" 상자를 선택합니다. 다른 필드에는 어떠한 정보도

추가하지 마세요.

5. VM의 전원을 켭니다.
6. 콘솔 탭을 클릭하면 초기 부팅 프로세스를 볼 수 있습니다.
7. 시간대를 구성합니다.
8. Unified Manager 유지 관리 사용자 이름과 비밀번호를 입력하세요.

설치가 끝나면 Unified Manager 웹 UI에 연결하기 위한 정보가 표시됩니다.

Linux 설치를 위한 빠른 시작 지침

설치 패키지를 다운로드하여 물리적 또는 가상 Red Hat Enterprise Linux 플랫폼에 Unified Manager를 설치할 수 있습니다.

시스템 요구 사항

- 운영 체제: x86_64 아키텍처를 기반으로 하는 Red Hat Enterprise Linux 버전 8.x 및 9.4, OS 설치 프로그램의 소프트웨어 선택 옵션에서 "GUI가 있는 서버" 기반 환경을 사용하여 설치됨
- RAM: 12GB, CPU: 총 9572MHz
- 여유 디스크 공간: 100GB의 디스크 공간 /opt/netapp/data 디렉토리, 루트 파티션에 50GB. 별도로 장착 /opt 그리고 /var/log 디렉토리를 확인하십시오 /opt 15GB가 있습니다 /var/log 16GB가 있고 /tmp 10GB의 여유 공간이 있습니다.

보안 사이트에 제품을 설치하는 방법에 대한 자세한 시스템 요구 사항과 정보는 다음을 참조하세요. ["Unified Manager 설치 요구 사항"](#) 그리고 ["상호 운용성 매트릭스"](#).

Active IQ Unified Manager 설치

설치 프로그램을 다운로드하세요

1. 다운로드 ActiveIQUnifiedManager-<version>.zip 코드 서명 인증서와 함께 제공되는 설치 패키지 (.pem) 및 디지털 서명 (.sig).
2. 설치 파일을 다운로드한 디렉토리에서 다음을 실행하세요.

```
# unzip ActiveIQUnifiedManager-<version>.zip
```

무결성 확인

다음 명령을 실행하여 설치 프로그램 패키지의 무결성을 확인하세요.

- 달리다 openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name> 코드 서명 인증서의 공개 키로 파일을 생성합니다.
- 달리다 openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip 설치 프로그램 패키지의 서명을 확인하세요.

저장소 구성 확인

Red Hat Enterprise Linux 저장소를 구성하는 절차는 사이트마다 다릅니다. 당신은 사용할 수 있습니다 `pre_install_check.sh` 설치 패키지에 포함된 스크립트를 사용하여 운영 체제의 구성을 확인합니다. 시스템이 인터넷에 연결되어 있으면 Red Hat Enterprise Linux 저장소를 설정하기 위한 지침이 자동으로 전송됩니다.

```
# sudo ./pre_install_check.sh
```

Unified Manager 설치

Unified Manager는 다음을 사용합니다. yum 소프트웨어와 그에 종속된 소프트웨어를 설치하는 유틸리티입니다. Red Hat Enterprise Linux의 이미지가 다양하기 때문에 설치되는 패키지는 이미지에 있는 소프트웨어에 따라 달라집니다. 그만큼 yum 유틸리티는 설치를 위한 종속 소프트웨어 패키지를 결정합니다. 종속 소프트웨어 패키지에 대한 자세한 정보가 필요한 경우 다음을 참조하세요. "[Linux 소프트웨어 및 설치 요구 사항](#)".

Unified Manager를 설치하려면 루트 사용자로 또는 다음을 사용하여 다음 명령을 실행하세요. sudo 설치 파일이 압축 해제된 디렉토리에서:

```
# yum install netapp-um<version>.x86_64.rpm
```

또는

```
% sudo yum install netapp-um<version>.x86_64.rpm
```

설치가 끝나면 Unified Manager 웹 UI에 연결하기 위한 정보가 표시됩니다. 웹 UI에 접속이 불가능한 경우 다음을 참조하세요. README 포트 443 제한에 대한 자세한 내용은 소프트웨어와 함께 제공되는 파일을 참조하세요.

Windows 설치를 위한 빠른 시작 지침

설치 패키지를 다운로드하고 Unified Manager를 설치하여 데이터 저장 용량, 가용성, 성능 및 보호 문제를 모니터링하고 해결할 수 있습니다.

시스템 요구 사항

- 운영 체제
 - Microsoft Windows Server 2019 Standard 및 Datacenter Edition
 - Microsoft Windows Server 2022 Standard 및 Datacenter Edition

Unified Manager는 다음 언어에 대해 64비트 Windows 운영 체제에서 지원됩니다.

- 영어
- 일본어
- 간체 중국어
- 램: 12GB
- CPU: 총 9572MHz
- 여유 디스크 공간: 설치 디렉토리용 100GB 디스크 공간, MySQL 데이터 디렉토리용 50GB 디스크 공간

자세한 시스템 요구 사항은 다음을 참조하세요. "[Unified Manager 설치 요구 사항](#)" 그리고 "[상호 운용성 매트릭스](#)".

Active IQ Unified Manager 설치

설치 프로그램을 다운로드하세요

1. 다운로드 ActiveIQUnifiedManager-<version>.exe 설치 패키지.
2. 설치 파일을 대상 시스템의 디렉토리에 복사합니다.

Unified Manager 설치

Unified Manager를 설치하려면 Microsoft .NET 4.5.2 이상 버전이 설치되어 있는지 확인하세요. Unified Manager는 설치 과정의 일부로 필요에 따라 다른 타사 패키지를 설치합니다. 종속 소프트웨어 패키지에 대한 자세한 내용은 다음을 참조하세요. "[Windows 소프트웨어 및 설치 요구 사항](#)".

1. 기본 로컬 관리자 계정을 사용하여 Windows에 로그인합니다.
2. 설치 파일을 다운로드한 디렉토리에서 마우스 오른쪽 버튼을 클릭하고 Unified Manager 실행 파일(.exe)을 관리자 권한으로 실행합니다.
3. 메시지가 표시되면 사용자 이름과 비밀번호를 입력하여 Unified Manager 유지 관리 사용자를 만듭니다.
4. 데이터베이스 연결 마법사에서 MySQL 루트 비밀번호를 입력합니다.
5. 나머지 메시지에 따라 설치를 완료하세요.
6. 설치가 끝나면 *마침*을 클릭하면 Unified Manager 웹 UI가 표시됩니다.

VMware vSphere 시스템에 Unified Manager 설치

Active IQ Unified Manager 소개

Active IQ Unified Manager (이전 OnCommand Unified Manager)를 사용하면 단일 인터페이스에서 ONTAP 스토리지 시스템의 상태와 성능을 모니터링하고 관리할 수 있습니다. Linux 서버, Windows 서버 또는 VMware 호스트의 가상 어플라이언스에 Unified Manager를 배포할 수 있습니다.

설치를 완료하고 관리하려는 클러스터를 추가하면 Unified Manager는 모니터링되는 스토리지 시스템의 용량, 가용성, 보호 및 성능 상태를 표시하는 그래픽 인터페이스를 제공합니다.

관련 정보

["NetApp 상호 운용성 매트릭스 도구"](#)

Unified Manager 서버가 수행하는 작업

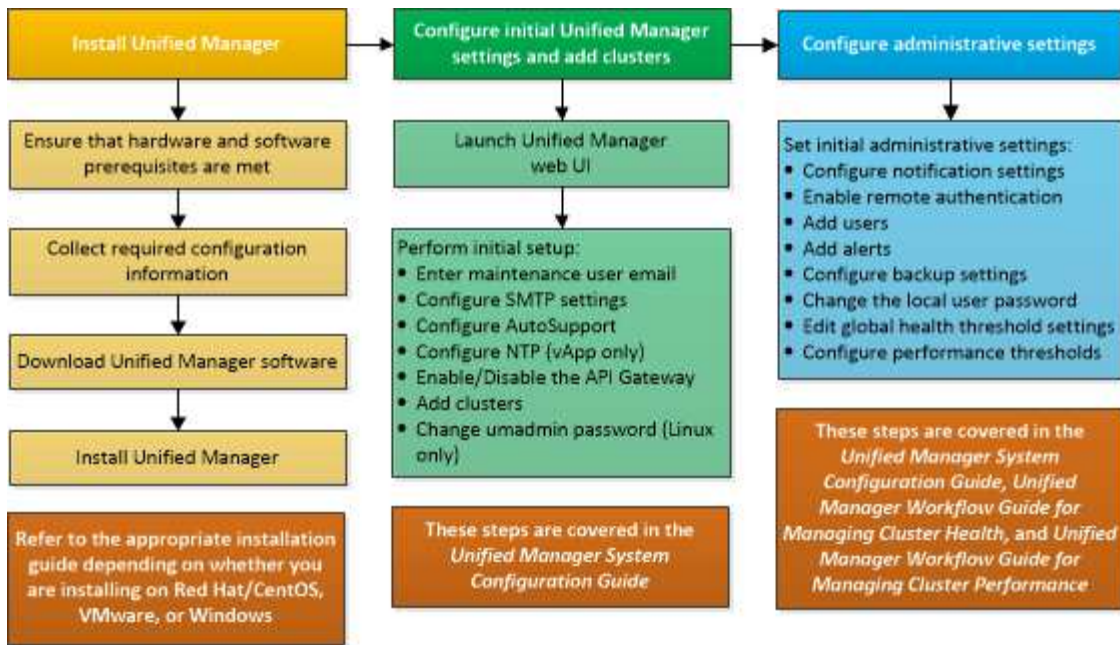
Unified Manager 서버 인프라는 데이터 수집 장치, 데이터베이스, 애플리케이션 서버로 구성됩니다. 검색, 모니터링, 역할 기반 액세스 제어(RBAC), 감사, 로깅 등의 인프라 서비스를 제공합니다.

Unified Manager는 클러스터 정보를 수집하고, 해당 데이터를 데이터베이스에 저장하고, 데이터를 분석하여 클러스터에 문제가 있는지 확인합니다.

설치 순서 개요

설치 워크플로는 Unified Manager를 사용하기 전에 수행해야 하는 작업을 설명합니다.

이 섹션에서는 아래 워크플로에 표시된 각 항목을 설명합니다.



Unified Manager 설치 요구 사항

설치 과정을 시작하기 전에 Unified Manager를 설치하려는 서버가 특정 소프트웨어, 하드웨어, CPU 및 메모리 요구 사항을 충족하는지 확인하세요.

NetApp Unified Manager 애플리케이션 코드의 수정을 지원하지 않습니다. Unified Manager 서버에 보안 조치를 적용해야 하는 경우 Unified Manager가 설치된 운영 체제를 변경해야 합니다.

Unified Manager 서버에 보안 조치를 적용하는 방법에 대한 자세한 내용은 기술 자료 문서를 참조하세요.

["Clustered Data ONTAP 용 Active IQ Unified Manager 에 적용된 보안 조치에 대한 지원 가능성"](#)

관련 정보

자세한 내용은 다음을 참조하세요. ["NetApp 상호 운용성 매트릭스 도구"](#)

가상 인프라 및 하드웨어 시스템 요구 사항

가상 인프라나 물리적 시스템에 Unified Manager를 설치하려면 메모리, CPU, 디스크 공간에 대한 최소 요구 사항을 충족해야 합니다.

다음 표는 메모리, CPU, 디스크 공간 리소스에 권장되는 값을 보여줍니다. 이러한 값은 Unified Manager가 허용 가능한 성능 수준을 충족하도록 검증되었습니다.

하드웨어 구성	권장 설정
숫양	12GB(최소 요구 사항 8GB)
프로세서	4개의 CPU

하드웨어 구성	권장 설정
CPU 사이클 용량	총 9572MHz(최소 요구 사항 9572MHz)
디스크 여유 공간	• 5GB(씬 프로비저닝) • 152GB(두꺼운 프로비저닝)

Unified Manager는 메모리 용량이 적은 시스템에도 설치할 수 있지만, 권장하는 12GB RAM을 사용하면 최적의 성능을 위해 충분한 메모리를 확보할 수 있으며, 구성이 커짐에 따라 시스템이 추가 클러스터와 스토리지 개체를 수용할 수 있습니다. Unified Manager가 배포된 VM에 메모리 제한을 설정해서는 안 되며, 소프트웨어가 시스템에 할당된 메모리를 활용하는 것을 방해하는 기능(예: 벌루닝)을 활성화해서는 안 됩니다.

또한 Unified Manager의 두 번째 인스턴스를 설치하기 전에 Unified Manager의 단일 인스턴스가 모니터링할 수 있는 노드 수에는 제한이 있습니다. 자세한 내용은 다음을 참조하세요. "[Unified Manager 모범 사례 가이드](#)".

메모리 페이지 스와핑은 시스템과 관리 애플리케이션의 성능에 부정적인 영향을 미칩니다. 전반적인 호스트 활용으로 인해 사용할 수 없는 CPU 리소스를 놓고 경쟁하면 성능이 저하될 수 있습니다.

전용 사용에 대한 요구 사항

Unified Manager를 설치하는 물리적 또는 가상 시스템은 Unified Manager에만 사용해야 하며 다른 애플리케이션과 공유해서는 안 됩니다. 다른 애플리케이션이 시스템 리소스를 소모하여 Unified Manager의 성능을 크게 저하시킬 수 있습니다.

백업을 위한 공간 요구 사항

Unified Manager 백업 및 복원 기능을 사용하려면 "data" 디렉터리나 디스크에 150GB의 공간을 확보하도록 추가 용량을 할당하세요. 백업은 로컬 대상이나 원격 대상에 기록될 수 있습니다. 가장 좋은 방법은 Unified Manager 호스트 시스템 외부에 있으며 최소 150GB의 공간이 있는 원격 위치를 식별하는 것입니다.

호스트 연결 요구 사항

Unified Manager를 설치하는 물리적 시스템이나 가상 시스템은 성공적으로 다음을 수행할 수 있도록 구성되어야 합니다. ping 호스트 자체의 호스트 이름입니다. IPv6 구성의 경우 다음 사항을 확인해야 합니다. ping6 Unified Manager 설치가 성공적으로 이루어지도록 호스트 이름이 성공적으로 지정되었습니다.

호스트 이름(또는 호스트 IP 주소)을 사용하여 제품 웹 UI에 액세스할 수 있습니다. 배포 중에 네트워크에 대한 정적 IP 주소를 구성한 경우 네트워크 호스트에 대한 이름을 지정했습니다. DHCP를 사용하여 네트워크를 구성한 경우 DNS에서 호스트 이름을 얻어야 합니다.

정규화된 도메인 이름(FQDN)이나 IP 주소 대신 짧은 이름을 사용하여 사용자가 Unified Manager에 액세스하도록 허용하려는 경우 네트워크 구성에서 이 짧은 이름을 유효한 FQDN으로 확인해야 합니다.

VMware 소프트웨어 및 설치 요구 사항

Unified Manager를 설치하는 VMware vSphere 시스템에는 특정 버전의 운영 체제와 특정 버전의 지원 소프트웨어가 필요합니다.

지원되는 운영 체제는 VMware ESXi 8.0입니다.



VMware vSphere 시스템의 Unified Manager OVA는 내부적으로 Debian OS 12(bookworm)를 실행합니다. 지원되는 ESXi 서버 버전이 지원할 수 있는 가상 머신 하드웨어 버전에 대한 자세한 내용은 VMware 설명서를 참조하세요.

다음 vSphere 버전이 지원됩니다.

- VMware vCenter Server 7.0 및 8.0

지원되는 ESXi 버전의 전체 및 최신 목록은 상호 운용성 매트릭스를 참조하세요.

["mysupport.netapp.com/매트릭스"](https://mysupport.netapp.com/매트릭스)

가상 어플라이언스가 올바르게 작동하려면 VMware ESXi 서버 시간이 NTP 서버 시간과 동일해야 합니다. VMware ESXi 서버 시간을 NTP 서버 시간과 동기화하면 시간 오류가 방지됩니다.

설치 요구 사항

Unified Manager 가상 어플라이언스에 대한 VMware 고가용성이 지원됩니다.

ONTAP 소프트웨어를 실행하는 스토리지 시스템에 NFS 데이터 저장소를 배포하는 경우 VMware VAAI용 NetApp NFS 플러그인을 사용하여 두꺼운 프로비저닝을 사용하세요.

고가용성 지원 환경에서 리소스가 부족하여 배포에 실패하는 경우 VM 재시작 우선 순위를 비활성화하고 호스트 격리 응답을 켜둔 상태로 두어 클러스터 기능 가상 머신 옵션을 수정해야 할 수 있습니다.



Unified Manager를 설치하거나 업그레이드하는 동안 필요한 타사 소프트웨어와 보안 패치가 VMware vSphere 시스템에 자동으로 설치되거나 업그레이드됩니다. Unified Manager 설치 및 업그레이드 프로세스가 이러한 구성 요소를 제어하므로 타사 구성 요소의 독립 실행형 설치 또는 업그레이드를 시도해서는 안 됩니다.

지원되는 브라우저

Unified Manager 웹 UI에 액세스하려면 지원되는 브라우저를 사용하세요.

상호 운용성 매트릭스에는 지원되는 브라우저 버전 목록이 있습니다.

["mysupport.netapp.com/매트릭스"](https://mysupport.netapp.com/매트릭스)

모든 브라우저에서 팝업 차단 기능을 비활성화하면 소프트웨어 기능이 제대로 표시됩니다.

SAML 인증을 위해 Unified Manager를 구성하여 ID 공급자(IdP)가 사용자를 인증할 수 있도록 계획하는 경우 IdP에서 지원하는 브라우저 목록도 확인해야 합니다.

프로토콜 및 포트 요구 사항

필요한 포트와 프로토콜은 Unified Manager 서버와 관리되는 스토리지 시스템, 서버 및 기타

구성 요소 간의 통신을 가능하게 합니다.

Unified Manager 서버에 대한 연결

일반적인 설치에서는 Unified Manager 웹 UI에 연결할 때 포트 번호를 지정할 필요가 없습니다. 기본 포트가 항상 사용되기 때문입니다. 예를 들어 Unified Manager는 항상 기본 포트에서 실행하려고 하기 때문에 다음을 입력할 수 있습니다. `https://<host>` 대신에 `https://<host>:443`.

Unified Manager 서버는 다음 인터페이스에 액세스하기 위해 특정 프로토콜을 사용합니다.

인터페이스	규약	포트	설명
Unified Manager 웹 UI	HTTP	80	Unified Manager 웹 UI에 액세스하는 데 사용되며, 자동으로 보안 포트 443으로 리디렉션됩니다.
API를 사용한 Unified Manager 웹 UI 및 프로그램	HTTPS	443	Unified Manager 웹 UI에 안전하게 액세스하거나 API 호출을 하는 데 사용됩니다. API 호출은 HTTPS를 사용해서만 이루어질 수 있습니다.
유지 관리 콘솔	SSH/SFTP	22	유지 관리 콘솔에 액세스하고 지원 번들을 검색하는 데 사용됩니다.
리눅스 명령줄	SSH/SFTP	22	Red Hat Enterprise Linux 명령줄에 액세스하고 지원 번들을 검색하는 데 사용됩니다.
시스템 로그	UDP	514	ONTAP 시스템에서 구독 기반 EMS 메시지에 액세스하고 메시지를 기반으로 이벤트를 생성하는 데 사용됩니다.
나머지	HTTPS	9443	인증된 ONTAP 시스템에서 실시간 REST API 기반 EMS 이벤트에 액세스하는 데 사용됩니다.
MySQL 데이터베이스	MySQL	3306	Unified Manager에 대한 OnCommand Workflow Automation 및 OnCommand API 서비스 액세스를 활성화하는 데 사용됩니다.

인터페이스	규약	포트	설명
AMQP QPID 브로커	TCP/IP	56072	내부 메시지 통신에 사용됩니다.
AMQP QPID 브로커	TCP를 통한 웹소켓	56080	ONTAP (클라우드 에이전트)에서 수신된 메시지를 이 포트에서 수신하는 데 사용됩니다.
AMQP QPID 브로커	TCP를 통한 웹소켓	56443	ONTAP (클라우드 에이전트)에서 수신된 메시지를 이 포트에서 수신하는 데 사용됩니다. 이 포트를 통한 통신은 TLS 또는 SSL에서 제공하는 암호화를 지원합니다.



VMware vSphere 시스템에 Unified Manager를 설치하는 동안 MySQL의 기본 포트인 3306은 localhost로만 제한됩니다. 이는 이전 구성이 유지되는 모든 업그레이드 시나리오에 영향을 미치지 않습니다. 이 구성은 수정될 수 있으며 다음을 사용하여 다른 호스트에서 연결을 사용할 수 있습니다. Control access to MySQL port 3306 유지 관리 콘솔의 옵션입니다. 자세한 내용은 다음을 참조하세요. ["추가 메뉴 옵션"](#). HTTP 및 HTTPS 통신에 사용되는 포트(포트 80 및 443)는 Unified Manager 유지 관리 콘솔을 사용하여 변경할 수 있습니다. 자세한 내용은 다음을 참조하세요. ["유지 관리 콘솔 메뉴"](#).

Unified Manager 서버에서의 연결

Unified Manager 서버와 관리형 스토리지 시스템, 서버 및 기타 구성 요소 간의 통신을 가능하게 하는 포트를 열도록 방화벽을 구성해야 합니다. 포트가 열려 있지 않으면 통신이 실패합니다.

환경에 따라 Unified Manager 서버가 특정 대상에 연결하는 데 사용하는 포트와 프로토콜을 수정할 수 있습니다.

Unified Manager 서버는 다음 프로토콜과 포트를 사용하여 관리되는 스토리지 시스템, 서버 및 기타 구성 요소에 연결합니다.

목적지	규약	포트	설명
저장 시스템	HTTPS	443/TCP	저장 시스템을 모니터링하고 관리하는 데 사용됩니다.  이 포트나 다른 포트를 사용하여 VMware vCenter Server 또는 ESXi 서버에 연결하는 경우 해당 포트를 사용할 수 있고 보안 사이트에서 연결할 수 있는지 확인하세요.
저장 시스템	NDMP	10000/TCP	특정 스냅샷 복원 작업에 사용됩니다.
AutoSupport 서버	HTTPS	443	AutoSupport 정보를 전송하는 데 사용됩니다. 이 기능을 수행하려면 인터넷 접속이 필요합니다.
인증 서버	LDAP	389	인증 요청, 사용자 및 그룹 조회 요청을 하는 데 사용됩니다.
LDAPS	636	보안 LDAP 통신에 사용됩니다.	메일 서버
SMTP	25	경고 알림 이메일을 보내는 데 사용됩니다.	SNMP 트랩 발신자
SNMPv1 또는 SNMPv3	162/UDP	SNMP 트랩에 대한 경고 알림을 보내는 데 사용됩니다.	외부 데이터 공급자 서버
TCP	2003	Graphite와 같은 외부 데이터 공급자에게 성능 데이터를 전송하는 데 사용됩니다.	NTP 서버

목적지	규약	포트	설명
엔티피	123/UDP	Unified Manager 서버의 시간을 외부 NTP 시간 서버와 동기화하는 데 사용됩니다. (VMware 시스템에만 해당)	시스템 로그

워크시트를 완성하세요

Unified Manager를 설치하고 구성하기 전에 해당 환경에 대한 구체적인 정보를 쉽게 사용할 수 있어야 합니다. 워크시트에 정보를 기록할 수 있습니다.

Unified Manager 설치 정보

Unified Manager를 설치하는 데 필요한 세부 정보입니다.

소프트웨어가 배포되는 시스템	당신의 가치
ESXi 서버 IP 주소	
호스트 정규화된 도메인 이름	
호스트 IP 주소	
네트워크 마스크	
게이트웨이 IP 주소	
기본 DNS 주소	
보조 DNS 주소	
도메인 검색	
유지 관리 사용자 이름	
유지관리 사용자 비밀번호	

Unified Manager 구성 정보

설치 후 Unified Manager를 구성하는 방법에 대한 세부 정보입니다. 일부 값은 구성에 따라 선택 사항입니다.

환경	당신의 가치
유지관리 사용자 이메일 주소	
NTP 서버	
SMTP 서버 호스트 이름 또는 IP 주소	
SMTP 사용자 이름	
SMTP 비밀번호	
SMTP 포트	25 (기본값)
알림이 전송되는 이메일	
인증 서버 호스트 이름 또는 IP 주소	
Active Directory 관리자 이름 또는 LDAP 바인딩 고유 이름	
Active Directory 암호 또는 LDAP 바인딩 암호	
인증 서버 기반 고유 이름	
ID 공급자(IdP) URL	
ID 공급자(IdP) 메타데이터	
SNMP 트랩 대상 호스트 IP 주소	
SNMP 포트	

클러스터 정보

Unified Manager를 사용하여 관리하는 스토리지 시스템에 대한 세부 정보입니다.

N 의 클러스터 1	당신의 가치
호스트 이름 또는 클러스터 관리 IP 주소	

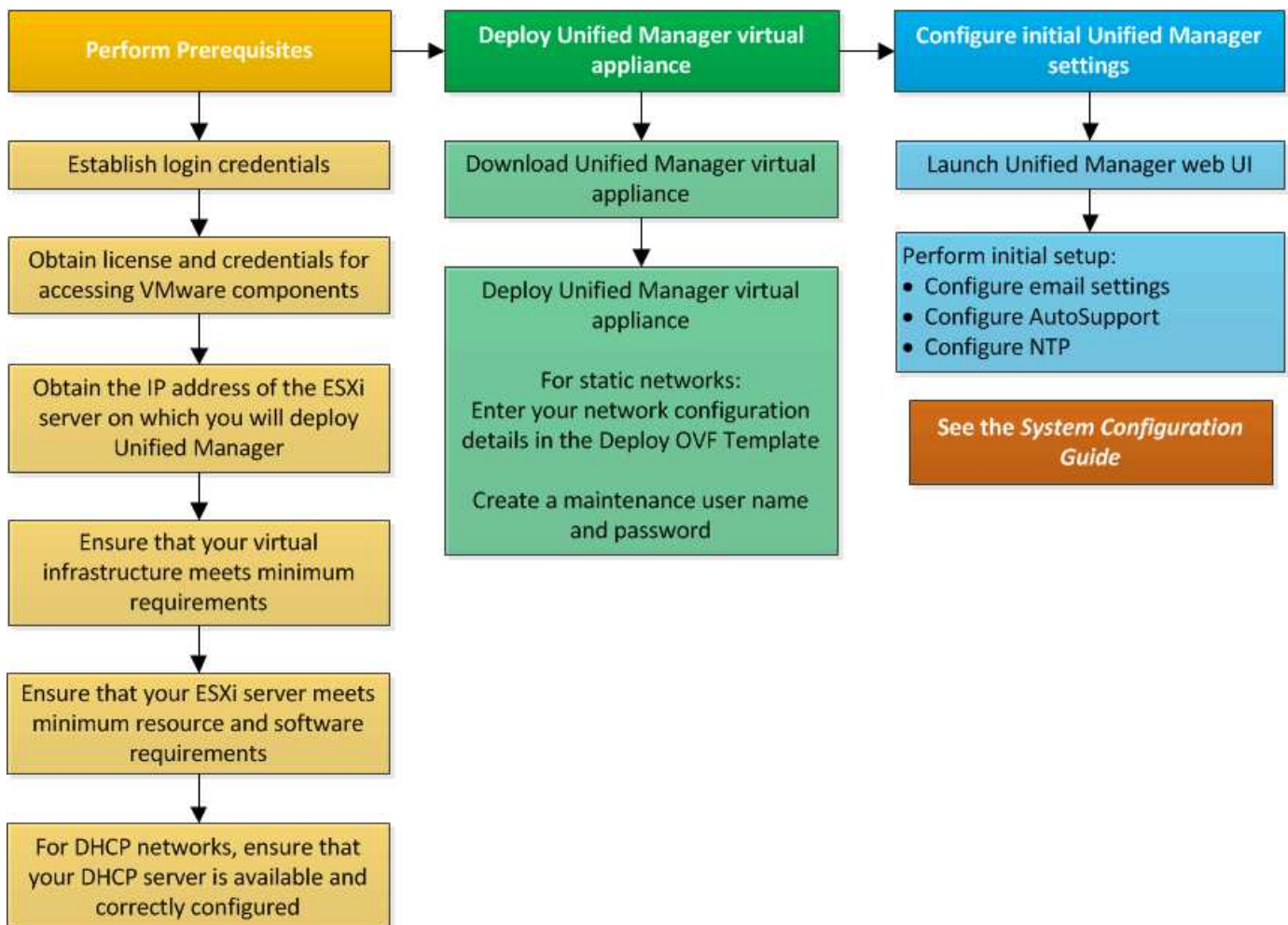
N의 클러스터 1	당신의 가치
ONTAP 관리자 사용자 이름	
 관리자에게 “admin” 역할이 할당되어야 합니다.	
ONTAP 관리자 비밀번호	
규약	HTTPS

Unified Manager 소프트웨어 설치, 업그레이드 및 제거

VMware vSphere 시스템에서 Unified Manager를 설치하고, 최신 버전의 소프트웨어로 업그레이드하거나 Unified Manager 가상 어플라이언스(vApp)를 제거할 수 있습니다.

배포 프로세스 개요

배포 워크플로는 Unified Manager를 사용하기 전에 수행해야 하는 작업을 설명합니다.



Unified Manager 배포

Unified Manager를 배포하려면 소프트웨어 다운로드, 가상 어플라이언스 배포, 유지 관리 사용자 이름과 비밀번호 생성, 웹 UI에서 초기 설정 수행이 필요합니다.

시작하기 전에

- 배포를 위해 시스템 요구 사항을 확인하고 완료해야 합니다.

보다 "[시스템 요구 사항](#)".

- 다음 정보가 있는지 확인하세요.
 - NetApp 지원 사이트에 대한 로그인 자격 증명
 - VMware vCenter Server 및 vSphere Web Client에 액세스하기 위한 자격 증명
 - Unified Manager 가상 어플라이언스를 배포하는 ESXi 서버의 IP 주소
 - 데이터 저장소의 저장 공간 및 메모리 요구 사항 등 데이터 센터에 대한 세부 정보
 - IPv6 주소 지정을 사용하려면 호스트에서 IPv6를 활성화해야 합니다.

VMware ESXi 서버에서 Unified Manager를 가상 어플라이언스로 배포할 수 있습니다.

SSH를 사용해서가 아니라 VMware 콘솔을 사용하여 유지 관리 콘솔에 액세스해야 합니다.



Unified Manager 9.8부터 VMware Tools가 Open VM Tools로 대체되었습니다. `open-vm-tools`). 더 이상 설치의 일부로 VMware Tools를 설치할 필요가 없습니다. `open-vm-tools` Unified Manager 설치 패키지에 포함되어 있습니다.

배포 및 초기 설정을 완료한 후에는 유지 관리 콘솔에서 클러스터를 추가하거나 추가 네트워크 설정을 구성한 다음 웹 UI에 액세스할 수 있습니다.

단계

1. 다음 단계를 따르세요 "[Unified Manager 다운로드](#)".
2. 또한 다음 단계를 따르세요 "[Unified Manager 가상 어플라이언스 배포](#)".

Unified Manager 설치 파일을 다운로드하세요

NetApp 지원 사이트에서 Unified Manager 설치 파일을 다운로드하여 Unified Manager를 가상 어플라이언스로 배포합니다.

시작하기 전에

NetApp 지원 사이트에 대한 로그인 자격 증명이 있어야 합니다.

설치 파일은 `.tar` 루트 인증서가 포함된 파일 README 파일 및 OVA 가상 어플라이언스에 맞게 구성된 Unified Manager 소프트웨어가 포함된 파일입니다.

단계

1. NetApp 지원 사이트에 로그인하고 Unified Manager 다운로드 페이지로 이동합니다.

"[NetApp 지원 사이트](#)"

- 필요한 Unified Manager 버전을 선택하고 최종 사용자 라이선스 계약(EULA)에 동의합니다.
- 다운로드하고 저장하세요 .tar vSphere Client에서 액세스할 수 있는 로컬 디렉토리나 네트워크 디렉토리에 VMware vSphere 설치용 파일을 저장합니다.
- 소프트웨어가 올바르게 다운로드되었는지 확인하려면 체크섬을 확인하세요.
- 다운로드한 디렉토리로 이동하세요 .tar 파일을 열고 터미널 창에 다음 명령을 입력하여 Unified Manager 번들을 확장합니다.

```
tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz
```

필요한 OVA 파일, 루트 인증서 및 README Unified Manager용 파일이 대상 디렉토리에 압축 해제됩니다.

- 무결성을 확인하십시오 OVA 제공된 단계에 따라 파일을 README 파일.

Unified Manager 가상 어플라이언스 배포

설치 파일을 다운로드한 후 Unified Manager를 가상 어플라이언스로 배포합니다. vSphere Web Client를 사용하여 ESXi 서버에 가상 어플라이언스를 배포합니다. 가상 어플라이언스를 배포하면 가상 머신이 생성됩니다.

시작하기 전에

시스템 요구 사항을 검토해야 합니다. Unified Manager 가상 어플라이언스를 배포하기 전에 필요한 변경 사항을 적용하세요.

보다"가상 인프라 요구 사항" .

보다"VMware 소프트웨어 및 설치 요구 사항" .

DHCP(동적 호스트 구성 프로토콜)를 사용하는 경우 DHCP 서버를 사용할 수 있는지, DHCP 및 가상 머신(VM) 네트워크 어댑터 구성이 올바른지 확인하세요. DHCP는 기본적으로 구성되어 있습니다.

정적 네트워크 구성을 사용하는 경우 동일한 서브넷에 IP 주소가 중복되지 않았는지 확인하고 적절한 DNS 서버 항목이 구성되었는지 확인하세요.

가상 어플라이언스를 배포하기 전에 다음 정보를 얻으세요.

- VMware vCenter Server 및 vSphere Web Client에 액세스하기 위한 자격 증명
- Unified Manager 가상 어플라이언스를 배포하는 ESXi 서버의 IP 주소
- 저장 공간 가용성 등 데이터 센터에 대한 세부 정보
- DHCP를 사용하지 않는 경우 연결하려는 네트워크 장치의 IPv4 또는 IPv6 주소를 얻으세요.
 - 호스트의 정규화된 도메인 이름(FQDN)
 - 호스트의 IP 주소
 - 네트워크 마스크
 - 기본 게이트웨이의 IP 주소
 - 기본 및 보조 DNS 주소

- 도메인 검색

Unified Manager 9.8부터 VMware Tools가 Open VM Tools로 대체되었습니다. *open-vm-tools*). 설치 프로세스의 일부로 VMware Tools를 설치할 필요는 없습니다. *open-vm-tools* Unified Manager 설치 패키지에 포함되어 있습니다.

가상 어플라이언스가 배포되면 HTTPS 액세스를 위한 고유한 자체 서명 인증서가 생성됩니다. Unified Manager 웹 UI에 액세스할 때 신뢰할 수 없는 인증서에 대한 브라우저 경고가 표시될 수 있습니다.

Unified Manager 가상 어플라이언스에 대한 VMware 고가용성이 지원됩니다.

단계

1. vSphere Client에서 파일 > *OVF 템플릿 배포*를 클릭합니다.
2. OVF 템플릿 배포 마법사를 완료하여 Unified Manager 가상 어플라이언스를 배포합니다.

리뷰 세부 정보 페이지에서:

- 게시자 섹션의 세부 정보를 확인하세요. **Entrust Code Signing - OVCS2**(신뢰할 수 있는 인증서) 메시지는 다운로드된 인증서의 무결성을 확인합니다. OVA 파일. + **Entrust** 코드 서명 - **OVCS2**(잘못된 인증서) 메시지가 나타나면 VMware vCenter Server를 7.0U3E 이상 버전으로 업그레이드하세요.

템플릿 사용자 정의 페이지에서:

- DHCP 및 IPv4 주소 지정을 사용하는 경우 모든 필드를 비워 두세요.
 - DHCP 및 IPv6 주소 지정을 사용할 때는 "자동 IPv6 주소 지정 사용" 상자를 선택하고 다른 모든 필드는 비워 둡니다.
 - 정적 네트워크 구성을 사용하려면 이 페이지의 필드를 작성하면 됩니다. 그러면 배포 중에 해당 설정이 적용됩니다. IP 주소가 배포된 호스트에서 고유한지, 이미 사용 중이 아닌지, 유효한 DNS 항목이 있는지 확인하세요.
3. Unified Manager 가상 어플라이언스를 ESXi 서버에 배포한 후 VM을 마우스 오른쪽 버튼으로 클릭하고 *전원 켜기*를 선택하여 VM의 전원을 켭니다.



리소스가 부족하여 전원 켜기 작업이 실패하는 경우 리소스를 추가한 후 설치를 다시 시도하세요.

4. 콘솔 탭을 클릭합니다.

초기 부팅 프로세스는 완료하는 데 몇 분이 걸립니다.

5. 시간대를 구성하려면 VM 콘솔 창에 표시된 대로 지리적 위치와 도시 또는 지역을 입력하세요.

표시되는 모든 날짜 정보는 관리되는 장치의 시간대 설정과 관계없이 Unified Manager에 구성된 시간대를 사용합니다. 스토리지 시스템과 관리 서버가 동일한 NTP 서버로 구성된 경우, 다르게 나타나더라도 동일한 순간을 나타냅니다. 예를 들어, 관리 서버와 다른 표준 시간대를 사용하여 구성된 장치를 사용하여 스냅샷 복사본을 만드는 경우 타임스탬프는 관리 서버 시간입니다.

6. DHCP 서비스를 사용할 수 없거나 정적 네트워크 구성 세부 정보에 오류가 있는 경우 다음 옵션 중 하나를 선택하세요.

만약 당신이 사용한다면...	그러면 이렇게 하세요...
DHCP	*DHCP 재시도*를 선택하세요. DHCP를 사용하려면 올바르게 구성되었는지 확인해야 합니다. DHCP 지원 네트워크를 사용하는 경우 FQDN 및 DNS 서버 항목이 가상 어플라이언스에 자동으로 제공됩니다. DHCP가 DNS로 올바르게 구성되지 않은 경우 호스트 이름 "UnifiedManager"가 자동으로 할당되고 보안 인증서와 연결됩니다. DHCP 지원 네트워크를 설정하지 않은 경우 네트워크 구성 정보를 수동으로 입력해야 합니다.
정적 네트워크 구성	a. *정적 네트워크 구성에 대한 세부 정보 입력*을 선택합니다. 구성 과정을 완료하는 데 몇 분이 걸립니다. b. 입력한 값을 확인하고 *Y*를 선택하세요.

7. 프롬프트에서 유지 관리 사용자 이름을 입력한 다음 *Enter*를 클릭합니다.

유지 관리 사용자 이름은 az로 시작해야 하며, 뒤에 -, az 또는 0-9를 조합하여 사용해야 합니다.

8. 프롬프트가 표시되면 비밀번호를 입력한 다음 *Enter*를 클릭합니다.

VM 콘솔에는 Unified Manager 웹 UI의 URL이 표시됩니다.

Unified Manager의 초기 설정을 수행하려면 웹 UI에 액세스할 수 있습니다. ["Active IQ Unified Manager 구성"](#) .

Unified Manager 업그레이드

Active IQ Unified Manager 릴리스 9.13 또는 9.14에서만 릴리스 9.16로 업그레이드할 수 있습니다.

업그레이드 프로세스 중에는 Unified Manager를 사용할 수 없습니다. Unified Manager를 업그레이드하기 전에 실행 중인 모든 작업을 완료해야 합니다.

Unified Manager가 OnCommand Workflow Automation 인스턴스와 페어링되어 있고 두 제품 모두에 사용 가능한 소프트웨어의 새 버전이 있는 경우, 업그레이드를 수행한 후 두 제품의 연결을 해제한 다음 새 Workflow Automation 연결을 설정해야 합니다. 제품 중 하나만 업그레이드하는 경우 업그레이드 후 Workflow Automation에 로그인하여 Unified Manager에서 여전히 데이터를 수집하고 있는지 확인해야 합니다.

단계

1. 다음 단계를 따르세요. ["Unified Manager ISO 이미지 다운로드"](#) .
2. 또한, 다음 단계를 따르세요. ["Unified Manager 업그레이드"](#) .

Unified Manager 버전에 지원되는 업그레이드 경로

Active IQ Unified Manager 각 버전에 대해 특정 업그레이드 경로를 지원합니다.

Unified Manager의 일부 버전은 이후 버전으로의 내부 업그레이드를 수행할 수 없습니다. Unified Manager 업그레이드는 N-2 모델로 제한됩니다. 즉, 모든 플랫폼에서 다음 2개 릴리스 내에서만 업그레이드를 수행할 수 있습니다. 예를 들어 Unified Manager 9.13 및 9.14에서만 Unified Manager 9.16로 업그레이드할 수 있습니다.

지원되는 버전보다 이전 버전을 실행 중인 경우 Unified Manager 인스턴스를 먼저 지원되는 버전 중 하나로 업그레이드한 다음, 현재 버전으로 업그레이드해야 합니다.

예를 들어, 설치된 버전이 Unified Manager 9.9이고 Unified Manager 9.14로 업그레이드하려는 경우 업그레이드 순서를 따르면 됩니다.

업그레이드 경로 샘플:

1. 9.11 → 9.13으로 업그레이드
2. 9.13 → 9.14로 업그레이드
3. 9.13 → 9.16으로 업그레이드
4. 9.14 → 9.16으로 업그레이드

업그레이드 경로 매트릭스에 대한 자세한 내용은 다음을 참조하세요. ["지식 기반\(KB\) 문서"](#).

Unified Manager 업그레이드 파일 다운로드

Unified Manager를 업그레이드하기 전에 NetApp 지원 사이트에서 Unified Manager 업그레이드 파일을 다운로드하세요.

시작하기 전에

NetApp 지원 사이트에 대한 로그인 자격 증명이 있어야 합니다.

단계

1. NetApp 지원 사이트에 로그인하세요.

["NetApp 지원 사이트"](#)

2. VMware vSphere에서 Unified Manager를 업그레이드하려면 다운로드 페이지로 이동하세요.
3. 다운로드 .iso 업그레이드할 이미지를 만들고 vSphere Client에서 액세스할 수 있는 로컬 디렉토리나 네트워크 디렉토리에 저장합니다.
4. 소프트웨어가 올바르게 다운로드되었는지 확인하려면 체크섬을 확인하세요.

Unified Manager 가상 어플라이언스 업그레이드

Active IQ Unified Manager 가상 어플라이언스를 릴리스 9.13 또는 9.14에서 9.16로 업그레이드할 수 있습니다.

시작하기 전에

다음 사항을 확인하세요.

- NetApp 지원 사이트에서 업그레이드 파일과 ISO 이미지를 다운로드했습니다.
- Unified Manager를 업그레이드하는 시스템은 시스템 및 소프트웨어 요구 사항을 충족합니다.

보다"가상 인프라 요구 사항" .

보다"VMware 소프트웨어 및 설치 요구 사항" .

- vSphere 6.5 이상 사용자의 경우 VMware Remote Console(VMRC)을 설치했습니다.
- 업그레이드하는 동안 성능 데이터를 13개월 동안 보관하는 기존 기본 설정을 유지할지, 아니면 6개월로 변경할지 묻는 메시지가 표시될 수 있습니다. 확인 후, 과거 성과 데이터는 6개월 후에 삭제됩니다.
- 다음 정보가 있습니다.
 - NetApp 지원 사이트에 대한 로그인 자격 증명
 - VMware vCenter Server 및 vSphere Web Client에 액세스하기 위한 자격 증명
 - Unified Manager 유지 관리 사용자에 대한 자격 증명

업그레이드 프로세스 중에는 Unified Manager를 사용할 수 없습니다. Unified Manager를 업그레이드하기 전에 실행 중인 모든 작업을 완료해야 합니다.

Workflow Automation과 Unified Manager를 페어링한 경우 Workflow Automation에서 호스트 이름을 수동으로 업데이트해야 합니다.

단계

1. vSphere Client에서 홈 > 인벤토리 > *VM 및 템플릿*을 클릭합니다.
2. Unified Manager 가상 어플라이언스가 설치된 가상 머신(VM)을 선택합니다.
3. Unified Manager VM이 실행 중이면 요약 > 명령 > *게스트 종료*로 이동합니다.
4. Unified Manager VM의 스냅샷이나 복제본과 같은 백업 사본을 만들어 애플리케이션과 일관된 백업을 만듭니다.
5. vSphere Client에서 Unified Manager VM의 전원을 켭니다.
6. VMware 원격 콘솔을 실행합니다.
7. **CDROM** 아이콘을 클릭하고 *디스크 이미지 파일(.iso)에 연결*을 선택합니다.
8. 선택하세요 ActiveIQUnifiedManager-<version>-virtual-update.iso 파일을 클릭하고 *열기*를 클릭합니다.
9. 콘솔 탭을 클릭합니다.
10. Unified Manager 유지 관리 콘솔에 로그인합니다.
11. 메인 메뉴에서 *업그레이드*를 선택하세요.

업그레이드 프로세스 중에는 Unified Manager를 사용할 수 없으며, 완료되면 다시 시작된다는 메시지가 표시됩니다.

12. 유형 *y* 계속하려면.

가상 어플라이언스가 있는 가상 머신을 백업하라는 경고가 표시됩니다.

13. 유형 *y* 계속하려면.

업그레이드 프로세스와 Unified Manager 서비스 재시작은 완료하는 데 몇 분 정도 걸릴 수 있습니다.

14. 계속하려면 아무 키나 누르세요.

유지 관리 콘솔에서 자동으로 로그아웃됩니다.

15. 선택 사항: 유지 관리 콘솔에 로그인하고 Unified Manager 버전을 확인하세요.

지원되는 웹 브라우저에서 새 창으로 웹 UI를 실행하고 로그인하여 Unified Manager 업그레이드 버전을 사용할 수 있습니다. UI에서 작업을 수행하기 전에 검색 프로세스가 완료될 때까지 기다려야 합니다.

Unified Manager 가상 머신을 다시 시작합니다.

유지 관리 콘솔에서 Unified Manager 가상 머신(VM)을 다시 시작할 수 있습니다. 새로운 보안 인증서를 생성한 후 또는 VM에 문제가 있는 경우 VM을 다시 시작해야 합니다.

시작하기 전에

- 가상 어플라이언스의 전원을 켜야 합니다.
- Unified Manager 유지 관리 콘솔에 유지 관리 사용자로 로그인해야 합니다.

VMware 게스트 다시 시작 옵션을 사용하여 vSphere에서 가상 머신을 다시 시작할 수도 있습니다 참조하다 ["Broadcom의 VMware vSphere PowerCLI CMDLET 참조에 있는 Restart-VMGuest cmdlet입니다."](#)

단계

1. 유지 관리 콘솔에서 시스템 구성 > *가상 머신 재부팅*을 선택합니다.
2. 브라우저에서 Unified Manager 웹 UI를 시작하고 로그인합니다.

통합 관리자 제거

Unified Manager 소프트웨어가 설치된 가상 머신(VM)을 제거하면 Unified Manager를 제거할 수 있습니다.

시작하기 전에

- VMware vCenter Server 및 vSphere Web Client에 액세스하려면 자격 증명이 있어야 합니다.
- Unified Manager 서버와 Workflow Automation 서버의 모든 활성 연결을 닫아야 합니다.
- 가상 머신(VM)을 제거하기 전에 Unified Manager 서버에서 모든 클러스터(데이터 소스)를 제거해야 합니다.

단계

1. Unified Manager 유지 관리 콘솔을 사용하여 Unified Manager 서버에 외부 데이터 공급자에 대한 활성 연결이 없는지 확인합니다.
2. vSphere Client에서 홈 > 인벤토리 > *VM 및 템플릿*을 클릭합니다.
3. 제거할 VM을 선택하고 요약 탭을 클릭합니다.
4. VM이 실행 중이면 전원 > *게스트 종료*를 클릭합니다.
5. 제거하려는 VM을 마우스 오른쪽 버튼으로 클릭하고 *디스크에서 삭제*를 클릭합니다.

Linux 시스템에 Unified Manager 설치

Active IQ Unified Manager 소개

Active IQ Unified Manager (이전 OnCommand Unified Manager)를 사용하면 단일 인터페이스에서 ONTAP 스토리지 시스템의 상태와 성능을 모니터링하고 관리할 수 있습니다. Linux 서버, Windows 서버 또는 VMware 호스트의 가상 어플라이언스(vApp)로 Unified Manager를 배포할 수 있습니다.

설치를 완료하고 관리하려는 클러스터를 추가하면 Unified Manager는 모니터링되는 스토리지 시스템의 용량, 가용성, 보호 및 성능 상태를 표시하는 그래픽 인터페이스를 제공합니다.

관련 정보

["NetApp 상호 운용성 매트릭스 도구"](#)

Unified Manager 서버가 수행하는 작업

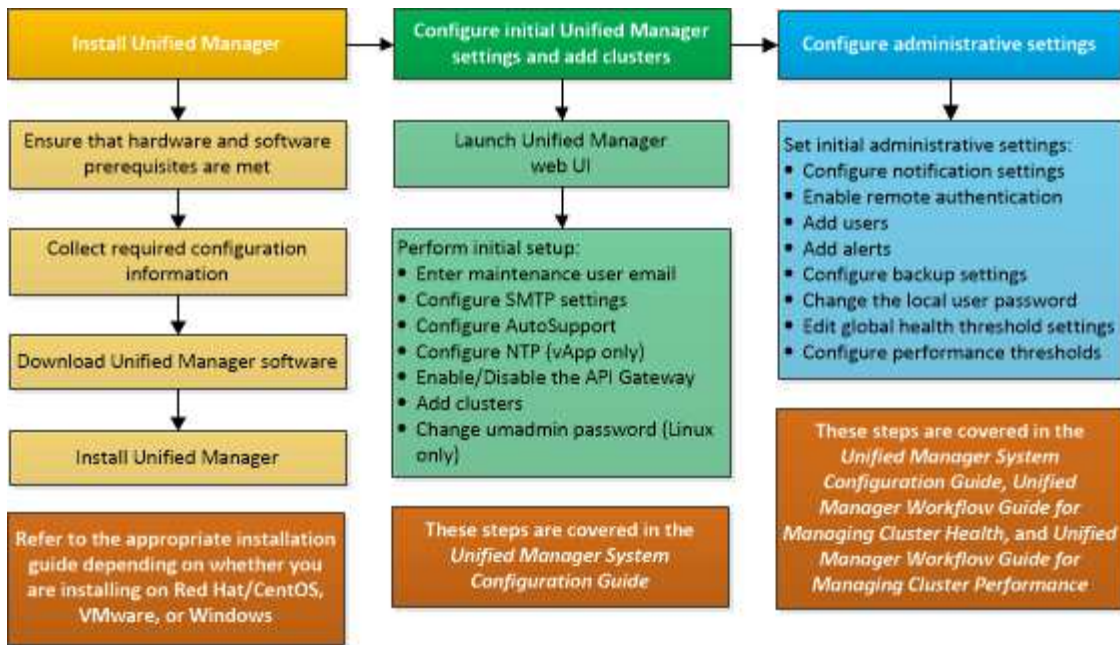
Unified Manager 서버 인프라는 데이터 수집 장치, 데이터베이스, 애플리케이션 서버로 구성됩니다. 검색, 모니터링, 역할 기반 액세스 제어(RBAC), 감사, 로깅 등의 인프라 서비스를 제공합니다.

Unified Manager는 클러스터 정보를 수집하고, 해당 데이터를 데이터베이스에 저장하고, 데이터를 분석하여 클러스터에 문제가 있는지 확인합니다.

설치 순서 개요

설치 워크플로는 Unified Manager를 사용하기 전에 수행해야 하는 작업을 설명합니다.

이 섹션에서는 아래 워크플로에 표시된 각 항목을 설명합니다.



Unified Manager 설치 요구 사항

설치 과정을 시작하기 전에 Unified Manager를 설치하려는 서버가 특정 소프트웨어, 하드웨어, CPU 및 메모리 요구 사항을 충족하는지 확인하세요.

NetApp Unified Manager 애플리케이션 코드의 수정을 지원하지 않습니다. Unified Manager 서버에 보안 조치를 적용해야 하는 경우 Unified Manager가 설치된 운영 체제를 변경해야 합니다.

Unified Manager 서버에 보안 조치를 적용하는 방법에 대한 자세한 내용은 기술 자료 문서를 참조하세요.

["Clustered Data ONTAP 용 Active IQ Unified Manager 에 적용된 보안 조치에 대한 지원 가능성"](#)

관련 정보

["NetApp 상호 운용성 매트릭스 도구"](#)

가상 인프라 및 하드웨어 시스템 요구 사항

가상 인프라나 물리적 시스템에 Unified Manager를 설치하려면 메모리, CPU, 디스크 공간에 대한 최소 요구 사항을 충족해야 합니다.

다음 표는 메모리, CPU, 디스크 공간 리소스에 권장되는 값을 보여줍니다. 이러한 값은 Unified Manager가 허용 가능한 성능 수준을 충족하도록 검증되었습니다.

하드웨어 구성	권장 설정
숫양	12GB(최소 요구 사항 8GB)
프로세서	4개의 CPU

하드웨어 구성	권장 설정
CPU 사이클 용량	총 9572MHz(최소 요구 사항 9572MHz)
디스크 여유 공간	150GB, 용량은 다음과 같이 할당됩니다. • 루트 파티션에 50GB 할당 • 100GB의 여유 디스크 공간이 할당되었습니다. /opt/netapp/data LVM 드라이브 또는 대상 시스템에 연결된 별도의 로컬 디스크에 마운트된 디렉토리  별도로 장착 /opt 그리고 /var/log 디렉토리를 확인하십시오 /opt 15GB가 있고 /var/log 16GB의 여유 공간이 있습니다. 그만큼 /tmp 디렉토리에는 최소 10GB의 여유 공간이 있어야 합니다.

Unified Manager는 메모리 용량이 적은 시스템에도 설치할 수 있지만, 권장하는 12GB RAM을 사용하면 최적의 성능을 위해 충분한 메모리를 확보할 수 있으며, 구성이 커짐에 따라 시스템이 추가 클러스터와 스토리지 개체를 수용할 수 있습니다. Unified Manager가 배포된 VM에 메모리 제한을 설정해서는 안 되며, 소프트웨어가 시스템에 할당된 메모리를 활용하는 것을 방해하는 기능(예: 벌루닝)을 활성화해서는 안 됩니다.

또한 Unified Manager의 두 번째 인스턴스를 설치하기 전에 Unified Manager의 단일 인스턴스가 모니터링할 수 있는 노드 수에는 제한이 있습니다. 자세한 내용은 [_모범 사례 가이드_](#)를 참조하세요.

"기술 보고서 4621: Unified Manager 모범 사례 가이드"

메모리 페이지 스와핑은 시스템과 관리 애플리케이션의 성능에 부정적인 영향을 미칩니다. 전반적인 호스트 활용으로 인해 사용할 수 없는 CPU 리소스를 놓고 경쟁하면 성능이 저하될 수 있습니다.

전용 사용에 대한 요구 사항

Unified Manager를 설치하는 물리적 또는 가상 시스템은 Unified Manager에만 사용해야 하며 다른 애플리케이션과 공유해서는 안 됩니다. 다른 애플리케이션이 시스템 리소스를 소모하여 Unified Manager의 성능을 크게 저하시킬 수 있습니다.

백업을 위한 공간 요구 사항

Unified Manager 백업 및 복원 기능을 사용하려면 "data" 디렉터리나 디스크에 150GB의 공간을 확보하도록 추가 용량을 할당하세요. 백업은 로컬 대상이나 원격 대상에 기록될 수 있습니다. 가장 좋은 방법은 Unified Manager 호스트 시스템 외부에 있으며 최소 150GB의 공간이 있는 원격 위치를 식별하는 것입니다.

호스트 연결 요구 사항

Unified Manager를 설치하는 물리적 시스템이나 가상 시스템은 성공적으로 다음을 수행할 수 있도록 구성되어야 합니다. ping 호스트 자체의 호스트 이름입니다. IPv6 구성의 경우 다음 사항을 확인해야 합니다. ping6 Unified Manager 설치가 성공적으로 이루어지도록 호스트 이름이 성공적으로 지정되었습니다.

호스트 이름(또는 호스트 IP 주소)을 사용하여 제품 웹 UI에 액세스할 수 있습니다. 배포 중에 네트워크에 대한 정적 IP

주소를 구성한 경우 네트워크 호스트에 대한 이름을 지정했습니다. DHCP를 사용하여 네트워크를 구성한 경우 DNS에서 호스트 이름을 얻어야 합니다.

정규화된 도메인 이름(FQDN)이나 IP 주소 대신 짧은 이름을 사용하여 사용자가 Unified Manager에 액세스하도록 허용하려는 경우 네트워크 구성에서 이 짧은 이름을 유효한 FQDN으로 확인해야 합니다.

Linux 소프트웨어 및 설치 요구 사항

Unified Manager를 설치하는 Linux 시스템에는 특정 버전의 운영 체제와 지원 소프트웨어가 필요합니다.

운영 체제 소프트웨어

Linux 시스템에는 다음 버전의 운영 체제와 지원 소프트웨어가 설치되어 있어야 합니다.

- x86_64 아키텍처를 기반으로 하는 Red Hat Enterprise Linux 버전 8.x 및 9.4.

지원되는 Red Hat Enterprise Linux 버전의 전체 및 최신 목록은 상호 운용성 매트릭스를 참조하세요.

["mysupport.netapp.com/매트릭스"](https://mysupport.netapp.com/매트릭스)

서버는 Unified Manager를 실행하는 데 전용되어야 합니다. 서버에 다른 애플리케이션을 설치하면 안 됩니다. 회사 규정으로 인해 Qualys와 같은 취약점 스캐너가 Linux 시스템에 설치되었을 수 있습니다. 설치가 실패하는 것을 방지하려면 Unified Manager를 설치하기 전에 취약점 스캐너를 비활성화해야 합니다.



취약점 스캐너(예: Qualys)는 가상 머신(VM)을 내부적으로(Unified Manager와 취약점 스캐너가 동일한 VM에 설치된 경우) 또는 외부적으로(Unified Manager와 취약점 스캐너가 두 개의 다른 서버에 설치되어 있고 취약점 스캐너가 Unified Manager가 설치된 VM을 스캔하는 경우) 스캔할 때 CPU 사용량이 높아질 수 있습니다. 이 문제는 종종 VM이 응답하지 않는 결과를 초래하고 Unified Manager 서비스에 영향을 미칩니다. 따라서 NetApp Unified Manager가 설치된 VM에서 취약점 스캐너를 비활성화할 것을 권장합니다. 스캐너를 비활성화하는 것이 불가능한 경우, 업무 시간 외에 VM을 스캔하고 스캔이 완료된 후 서비스를 다시 시작하세요.

타사 소프트웨어

Unified Manager는 WildFly 웹 서버에 배포됩니다. WildFly 26.1.3은 Unified Manager와 함께 번들로 제공됩니다.

다음 타사 패키지는 필요하지만 Unified Manager에 포함되어 있지 않습니다. 이러한 패키지는 자동으로 설치됩니다. yum 다음 섹션에 언급된 대로 저장소를 구성했다면 설치 중에 설치 프로그램을 사용할 수 있습니다.

- MySQL Community Edition 버전 8.4.4(MySQL 저장소에서)
- OpenJDK 버전 11.0.25(Red Hat Extra Enterprise Linux 서버 저장소에서)
- Python 3.9.x(Red Hat Extra Enterprise Linux 서버 저장소에서)
- p7zip 버전 16.02 이상(Red Hat Extra Packages for Enterprise Linux 저장소에서)



타사 소프트웨어를 업그레이드하기 전에 실행 중인 Unified Manager 인스턴스를 종료해야 합니다. 타사 소프트웨어 설치가 완료되면 Unified Manager를 다시 시작할 수 있습니다.

사용자 권한 요구 사항

Linux 시스템에 Unified Manager를 설치하는 작업은 루트 사용자 또는 루트가 아닌 사용자가 다음을 사용하여 수행할 수 있습니다. `sudo` 명령.

또한 기본 Unified Manager 설치에는 `sudoers` 파일에 `umadmin` 사용자(기본 유지 관리 사용자)와 `jboss` 사용자가 포함됩니다.(`ocum_sudoers` 그리고 `ocie_sudoers`)에서 `/etc/sudoers.d/` 예배 규칙서. 보안 정책이나 보안 모니터링 도구로 인해 환경에서 이 콘텐츠를 제거한 경우 다시 추가해야 합니다. 일부 Unified Manager 작업에는 `sudo` 권한이 필요하므로 `sudoers` 구성을 보존해야 합니다.

설치 요구 사항

시스템에 Red Hat Enterprise Linux와 관련 저장소를 설치하는 모범 사례는 아래와 같습니다. 다르게 설치 또는 구성된 시스템이나 오프프레미스(클라우드)에 배포된 시스템의 경우 추가 단계가 필요할 수 있으며, 이러한 배포에서는 Unified Manager가 제대로 실행되지 않을 수 있습니다.

- Red Hat 모범 사례에 따라 Red Hat Enterprise Linux를 설치해야 하며, 다음과 같은 기본 옵션을 선택해야 합니다. 이를 위해서는 "GUI가 있는 서버" 기반 환경을 선택해야 합니다.
- Red Hat Enterprise Linux에 Unified Manager를 설치하는 동안 시스템은 적절한 저장소에 액세스할 수 있어야 합니다. 이를 통해 설치 프로그램이 모든 필수 소프트웨어 종속성에 액세스하여 설치할 수 있습니다.
- 를 위해 `yum` Red Hat Enterprise Linux 저장소에서 종속 소프트웨어를 찾으려면 설치 프로그램을 사용하면 Red Hat Enterprise Linux 설치 중이나 나중에 유효한 Red Hat 구독을 사용하여 시스템을 등록해야 합니다.

Red Hat Subscription Manager에 대한 자세한 내용은 Red Hat 설명서를 참조하세요.

- 시스템에 필요한 타사 유틸리티를 성공적으로 설치하려면 EPEL(Enterprise Linux용 추가 패키지) 저장소를 활성화해야 합니다.

시스템에 EPEL 저장소가 구성되어 있지 않으면 저장소를 수동으로 다운로드하여 구성해야 합니다.

보다["EPEL 저장소 수동 구성"](#).

- 올바른 버전의 MySQL이 설치되지 않은 경우 MySQL 저장소를 활성화해야 시스템에 MySQL 소프트웨어를 성공적으로 설치할 수 있습니다.

시스템에 MySQL 저장소가 구성되어 있지 않으면 저장소를 수동으로 다운로드하여 구성해야 합니다.

보다["MySQL 저장소 수동 구성"](#).

- Unified Manager 호스트에는 Java 버전을 하나만 설치해야 합니다. 그렇지 않으면 시스템에서 사용할 버전을 결정하지 못할 수 있습니다. 보다 ["Active IQ Unified Manager 호스트에서 Java를 업데이트한 후 서비스가 시작되지 않습니다."](#).

시스템에 인터넷 접속이 없고, 인터넷에 연결된 시스템에서 연결되지 않은 시스템으로 저장소가 미러링되지 않은 경우, 설치 지침에 따라 시스템의 외부 소프트웨어 종속성을 확인해야 합니다. 그런 다음 필요한 소프트웨어를 인터넷에 연결된 시스템에 다운로드하고 복사할 수 있습니다. `.rpm` Unified Manager를 설치하려는 시스템에 파일을 추가합니다. 아티팩트와 패키지를 다운로드하려면 다음을 사용해야 합니다. `yum install` 명령. 두 시스템이 동일한 운영 체제 버전을 실행하고 있는지, 그리고 구독 라이선스가 적절한 Red Hat Enterprise Linux에 대한 것인지 확인해야 합니다.



여기에 나열된 저장소 이외의 다른 저장소에서 필요한 타사 소프트웨어를 설치해서는 안 됩니다. Red Hat 저장소에서 설치된 소프트웨어는 Red Hat Enterprise Linux용으로 명확하게 설계되었으며 Red Hat 모범 사례(디렉토리 레이아웃, 권한 등)를 준수합니다. 다른 위치의 소프트웨어는 이러한 지침을 따르지 않을 수 있으며, 이로 인해 Unified Manager 설치가 실패하거나 향후 업그레이드 시 문제가 발생할 수 있습니다.

포트 443 요구 사항

Red Hat Enterprise Linux의 일반 이미지는 포트 443에 대한 외부 액세스를 차단할 수 있습니다. 이러한 제한으로 인해 Unified Manager를 설치한 후 관리자 웹 UI에 연결하지 못할 수 있습니다. 다음 명령을 실행하면 일반 Red Hat Enterprise Linux의 모든 외부 사용자와 애플리케이션이 포트 443에 액세스할 수 있습니다.

```
# firewall-cmd --zone=public --add-port=443/tcp --permanent; firewall-cmd
--reload
```

"GUI가 있는 서버" 기반 환경에 Red Hat Enterprise Linux를 설치해야 합니다. Unified Manager 설치 지침에서 사용되는 명령을 제공합니다. 다른 기반 환경에서는 설치를 검증하거나 완료하기 위해 추가 명령을 설치해야 할 수도 있습니다. 만약 firewall-cmd 시스템에서 사용할 수 없는 경우 다음 명령을 실행하여 설치해야 합니다.

```
# sudo yum install firewalld
```

보안 정책에 따라 다른 절차가 필요한지 확인하려면 명령을 실행하기 전에 IT 부서에 문의하세요.



Red Hat 시스템에서는 THP(Transparent Huge Pages)를 비활성화해야 합니다. 이 기능을 활성화하면 특정 프로세스가 메모리를 너무 많이 사용하여 종료될 때 Unified Manager가 종료될 수 있습니다.

지원되는 브라우저

Unified Manager 웹 UI에 액세스하려면 지원되는 브라우저를 사용하세요.

상호 운용성 매트릭스에는 지원되는 브라우저 버전 목록이 있습니다.

["mysupport.netapp.com/매트릭스"](https://my.support.netapp.com/매트릭스)

모든 브라우저에서 팝업 차단 기능을 비활성화하면 소프트웨어 기능이 제대로 표시됩니다.

SAML 인증을 위해 Unified Manager를 구성하여 ID 공급자(IdP)가 사용자를 인증할 수 있도록 계획하는 경우 IdP에서 지원하는 브라우저 목록도 확인해야 합니다.

프로토콜 및 포트 요구 사항

필요한 포트와 프로토콜은 Unified Manager 서버와 관리되는 스토리지 시스템, 서버 및 기타 구성 요소 간의 통신을 가능하게 합니다.

Unified Manager 서버에 대한 연결

일반적인 설치에서는 Unified Manager 웹 UI에 연결할 때 포트 번호를 지정할 필요가 없습니다. 기본 포트가 항상 사용되기 때문입니다. 예를 들어 Unified Manager는 항상 기본 포트에서 실행하려고 하기 때문에 다음을 입력할 수 있습니다. `https://<host>` 대신에 `https://<host>:443`.

Unified Manager 서버는 다음 인터페이스에 액세스하기 위해 특정 프로토콜을 사용합니다.

인터페이스	규약	포트	설명
Unified Manager 웹 UI	HTTP	80	Unified Manager 웹 UI에 액세스하는 데 사용되며, 자동으로 보안 포트 443으로 리디렉션됩니다.
API를 사용한 Unified Manager 웹 UI 및 프로그램	HTTPS	443	Unified Manager 웹 UI에 안전하게 액세스하거나 API 호출을 하는 데 사용됩니다. API 호출은 HTTPS를 사용해서만 이루어질 수 있습니다.
유지 관리 콘솔	SSH/SFTP	22	유지 관리 콘솔에 액세스하고 지원 번들을 검색하는 데 사용됩니다.
리눅스 명령줄	SSH/SFTP	22	Red Hat Enterprise Linux 명령줄에 액세스하고 지원 번들을 검색하는 데 사용됩니다.
MySQL 데이터베이스	MySQL	3306	Unified Manager에 대한 OnCommand Workflow Automation 및 OnCommand API 서비스 액세스를 활성화하는 데 사용됩니다.
시스템 로그	UDP	514	ONTAP 시스템에서 구독 기반 EMS 메시지에 액세스하고 메시지를 기반으로 이벤트를 생성하는 데 사용됩니다.
나머지	HTTPS	9443	인증된 ONTAP 시스템에서 실시간 REST API 기반 EMS 이벤트에 액세스하는 데 사용됩니다.
MySQL 데이터베이스	MySQL	3306	Unified Manager에 대한 OnCommand Workflow Automation 및 OnCommand API 서비스 액세스를 활성화하는 데 사용됩니다.

인터페이스	규약	포트	설명
AMQP QPID 브로커	TCP/IP	56072	내부 메시지 통신에 사용됩니다.
AMQP QPID 브로커	TCP를 통한 웹소켓	56080	ONTAP (클라우드 에이전트)에서 수신된 메시지를 이 포트에서 수신하는 데 사용됩니다.
AMQP QPID 브로커	TCP를 통한 웹소켓	56443	ONTAP (클라우드 에이전트)에서 수신된 메시지를 이 포트에서 수신하는 데 사용됩니다. 이 포트를 통한 통신은 TLS 또는 SSL에서 제공하는 암호화를 지원합니다.



Linux 시스템에 Unified Manager를 설치하는 동안 MySQL의 기본 포트인 3306은 localhost로만 제한됩니다. 이는 이전 구성이 유지되는 모든 업그레이드 시나리오에 영향을 미치지 않습니다. 이 구성은 수정될 수 있으며 다음을 사용하여 다른 호스트에서 연결을 사용할 수 있습니다. Control access to MySQL port 3306 유지 관리 콘솔의 옵션입니다. 자세한 내용은 다음을 참조하세요. ["추가 메뉴 옵션"](#). HTTP 및 HTTPS 통신에 사용되는 포트(포트 80 및 443)는 Unified Manager 유지 관리 콘솔을 사용하여 변경할 수 있습니다. 자세한 내용은 다음을 참조하세요. ["유지 관리 콘솔 메뉴"](#).

Unified Manager 서버에서의 연결

Unified Manager 서버와 관리형 스토리지 시스템, 서버 및 기타 구성 요소 간의 통신을 가능하게 하는 포트를 열도록 방화벽을 구성해야 합니다. 포트가 열려 있지 않으면 통신이 실패합니다.

환경에 따라 Unified Manager 서버가 특정 대상에 연결하는 데 사용하는 포트와 프로토콜을 수정할 수 있습니다.

Unified Manager 서버는 다음 프로토콜과 포트를 사용하여 관리되는 스토리지 시스템, 서버 및 기타 구성 요소에 연결합니다.

목적지	규약	포트	설명
저장 시스템	HTTPS	443/TCP	저장 시스템을 모니터링하고 관리하는 데 사용됩니다.
저장 시스템	NDMP	10000/TCP	특정 스냅샷 복원 작업에 사용됩니다.
AutoSupport 서버	HTTPS	443	AutoSupport 정보를 전송하는 데 사용됩니다. 이 기능을 수행하려면 인터넷 접속이 필요합니다.

목적지	규약	포트	설명
인증 서버	LDAP	389	인증 요청, 사용자 및 그룹 조회 요청을 하는 데 사용됩니다.
LDAPS	636	보안 LDAP 통신에 사용됩니다.	메일 서버
SMTP	25	경고 알림 이메일을 보내는 데 사용됩니다.	SNMP 트랩 발신자
SNMPv1 또는 SNMPv3	162/UDP	SNMP 트랩에 대한 경고 알림을 보내는 데 사용됩니다.	외부 데이터 공급자 서버
TCP	2003	Graphite와 같은 외부 데이터 공급자에게 성능 데이터를 전송하는 데 사용됩니다.	NTP 서버
엔티피	123/UDP	Unified Manager 서버의 시간을 외부 NTP 시간 서버와 동기화하는 데 사용됩니다. (VMware 시스템에만 해당)	시스템 로그

워크시트를 완성하세요

Unified Manager를 설치하고 구성하기 전에 해당 환경에 대한 구체적인 정보를 쉽게 사용할 수 있어야 합니다. 워크시트에 정보를 기록할 수 있습니다.

Unified Manager 설치 정보

Unified Manager를 설치하는 데 필요한 세부 정보입니다.

소프트웨어가 배포되는 시스템	당신의 가치
호스트 정규화된 도메인 이름	
호스트 IP 주소	
네트워크 마스크	
게이트웨이 IP 주소	

소프트웨어가 배포되는 시스템	당신의 가치
기본 DNS 주소	
보조 DNS 주소	
도메인 검색	
유지 관리 사용자 이름	
유지관리 사용자 비밀번호	

Unified Manager 구성 정보

설치 후 Unified Manager를 구성하는 방법에 대한 세부 정보입니다. 일부 값은 구성에 따라 선택 사항입니다.

환경	당신의 가치
유지관리 사용자 이메일 주소	
SMTP 서버 호스트 이름 또는 IP 주소	
SMTP 사용자 이름	
SMTP 비밀번호	
SMTP 포트	25 (기본값)
알림이 전송되는 이메일	
인증 서버 호스트 이름 또는 IP 주소	
Active Directory 관리자 이름 또는 LDAP 바인딩 고유 이름	
Active Directory 암호 또는 LDAP 바인딩 암호	
인증 서버 기반 고유 이름	
ID 공급자(IdP) URL	
ID 공급자(IdP) 메타데이터	
SNMP 트랩 대상 호스트 IP 주소	

환경	당신의 가치
SNMP 포트	

클러스터 정보

Unified Manager를 사용하여 관리하는 스토리지 시스템에 대한 세부 정보입니다.

N의 클러스터 1	당신의 가치
호스트 이름 또는 클러스터 관리 IP 주소	
ONTAP 관리자 사용자 이름  관리자에게 “admin” 역할이 할당되어야 합니다.	
ONTAP 관리자 비밀번호	
규약	HTTPS

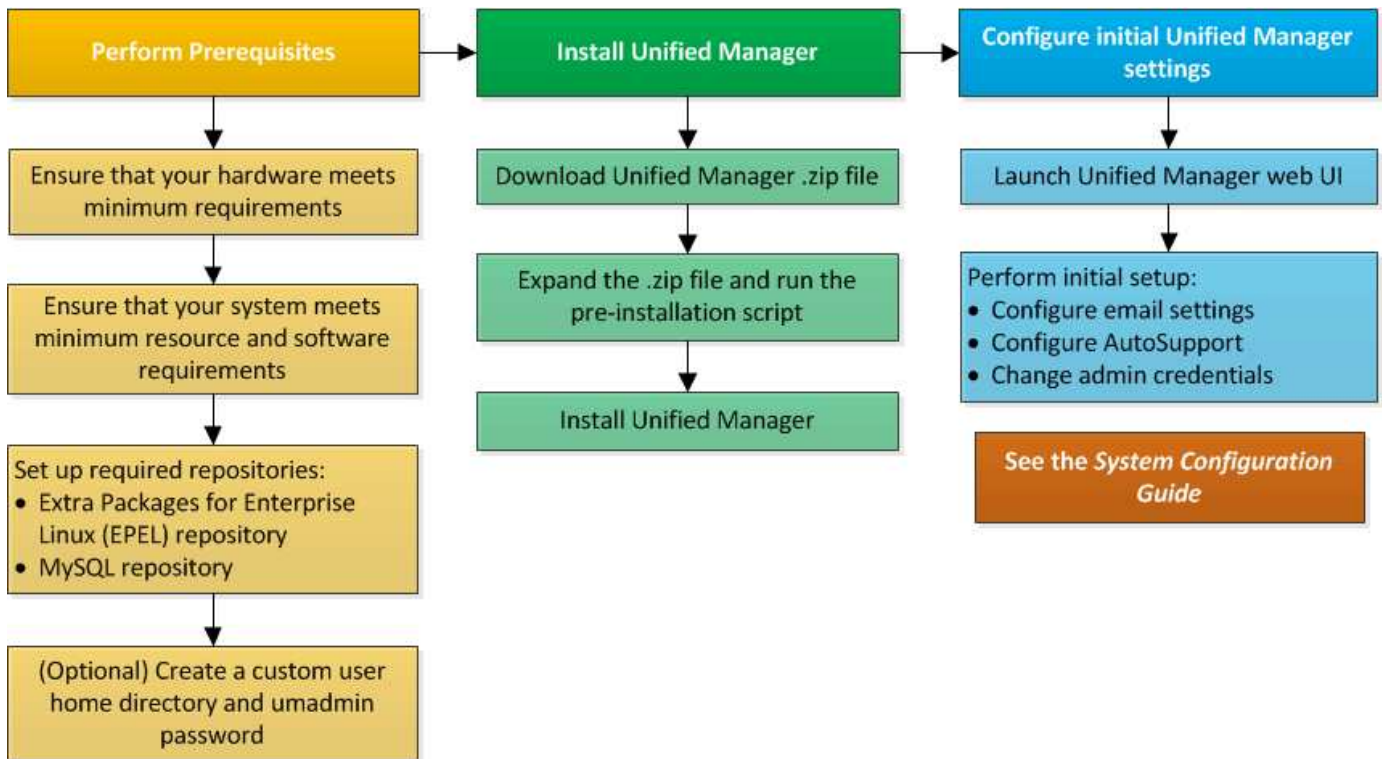
Unified Manager 소프트웨어 설치, 업그레이드 및 제거

Linux 시스템에서는 Unified Manager 소프트웨어를 설치하고, 최신 버전의 소프트웨어로 업그레이드하거나 Unified Manager를 제거할 수 있습니다.

Unified Manager는 Red Hat Enterprise Linux 서버에 설치할 수 있습니다. Unified Manager를 설치하는 Linux 서버는 물리적 머신에서 실행될 수도 있고, VMware ESXi, Microsoft Hyper-V 또는 Citrix XenServer에서 실행되는 가상 머신에서 실행될 수도 있습니다.

설치 과정 개요

설치 워크플로는 Unified Manager를 사용하기 전에 수행해야 하는 작업을 설명합니다.



필요한 소프트웨어 저장소 설정

설치 프로그램이 모든 필수 소프트웨어 종속성에 접근하여 설치할 수 있도록 시스템은 특정 저장소에 접근할 수 있어야 합니다.

EPEL 저장소를 수동으로 구성합니다.

Unified Manager를 설치하는 시스템에 EPEL(Enterprise Linux용 추가 패키지) 저장소에 액세스할 수 없는 경우, 성공적인 설치를 위해 저장소를 수동으로 다운로드하여 구성해야 합니다.

EPEL 저장소는 시스템에 설치해야 하는 필수 타사 유틸리티에 대한 액세스를 제공합니다. Red Hat Enterprise Linux 시스템에 Unified Manager를 설치하려면 EPEL 저장소를 사용합니다.

단계

1. 설치에 필요한 EPEL 저장소를 다운로드하세요. 버전 8은 다음에서 다운로드하세요.

```
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

버전 9는 다음에서 다운로드하세요:

```
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

2. EPEL 저장소를 구성하세요:

```
yum install epel-release-latest-<version>.noarch.rpm
```

예를 들어 Red Hat Enterprise Linux 8 시스템의 경우 모듈식 RPM 패키지가 포함된 내부 저장소가 있는 경우 `jvarkit-packages-filesystem-<version>.module.rpm` 모듈형 패키지의 메타데이터도 동일한 저장소에서

사용할 수 있는지 확인하세요.

MySQL 저장소를 수동으로 구성합니다.

Unified Manager를 설치하는 시스템에 MySQL Community Edition 저장소에 액세스할 수 없는 경우, 성공적인 설치를 위해 저장소를 수동으로 다운로드하여 구성해야 합니다.

MySQL 저장소는 시스템에 설치해야 하는 필수 MySQL 소프트웨어에 대한 액세스를 제공합니다.



시스템에 인터넷 연결이 없으면 이 작업이 실패할 수 있습니다. Unified Manager를 설치하는 시스템에 인터넷 접속이 불가능한 경우 MySQL 설명서를 참조하세요.

단계

1. 설치에 적합한 MySQL 저장소를 다운로드하세요. 버전 8은 다음에서 다운로드하세요.

```
wget http://repo.mysql.com/yum/mysql-8.4-community/el/8/x86_64/mysql84-community-release-el8-1.noarch.rpm
```

버전 9는 다음에서 다운로드하세요:

```
wget http://repo.mysql.com/yum/mysql-8.4-community/el/9/x86_64/mysql84-community-release-el9-1.noarch.rpm
```

2. MySQL 저장소를 구성합니다.

```
yum install mysql84-community-release-.noarch.rpm
```

Red Hat Enterprise Linux 8 시스템의 경우 AppStream 저장소에서 제공하는 java-11-openjdk, p7zip 및 기타 소프트웨어 패키지가 포함된 내부 저장소가 있는 경우 AppStream 저장소를 비활성화하고 MySQL Community Server를 설치해야 합니다. 다음 명령을 실행하세요.

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install mysql-community-server
```

키 누락 또는 키 불일치 오류가 발생하고 설치에 실패한 경우 다음 단계를 시도해 보세요.

- 연결된 시스템에서 다음 명령을 실행하여 업데이트된 MySQL 키를 가져옵니다.

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-<xxxx>
```

for example:

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2023
```

- 인터넷 연결이 없는 시스템에서는 MySQL repo 파일을 업데이트하고 비활성화하세요. gpgcheck 표시하여 gpgcheck=0 .

NFS 및 CIFS 공유에 대한 SELinux 요구 사항

마운트를 계획하고 있다면 /opt/netapp 또는 /opt/netapp/data NAS 또는 SAN 장치에서 SELinux를 활성화한 경우 몇 가지 고려 사항을 알아야 합니다.

마운트를 계획하고 있다면 /opt/netapp 또는 /opt/netapp/data 루트 파일 시스템이 아닌 다른 곳에서, 환경에서 SELinux를 활성화한 경우, 마운트된 디렉토리에 대한 올바른 컨텍스트를 설정해야 합니다. 사용자 환경에 적용되는 시나리오에 따라 올바른 SELinux 컨텍스트를 설정하고 확인하기 위한 다음 단계를 따르세요.

SELinux 컨텍스트를 구성합니다. /opt/netapp/data 마운트되어 있습니다

마운트한 경우 /opt/netapp/data 시스템에서 SELinux가 설정되어 있습니다. Enforcing, SELinux 컨텍스트 유형을 확인하십시오. /opt/netapp/data 로 설정됩니다 mysql_d_b_t 이는 데이터베이스 파일의 위치에 대한 기본 컨텍스트 요소입니다.

1. 컨텍스트를 확인하려면 다음 명령을 실행하세요.

```
ls -dZ /opt/netapp/data
```

샘플 출력:

```
drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0
/opt/netapp/data
```



이 출력에서 컨텍스트는 다음과 같습니다. default_t. 이 컨텍스트를 다음으로 변경해야 합니다. mysql_d_b_t.

2. 마운트한 방식에 따라 컨텍스트를 설정하려면 다음 단계를 수행하십시오. /opt/netapp/data.

- a. 다음 명령을 실행하여 컨텍스트를 설정하세요. mysql_d_b_t:

```
semanage fcontext -a -t mysql_d_b_t "/opt/netapp/data"
`restorecon -R -v /opt/netapp/data
```

- b. 구성한 경우 /opt/netapp/data ~에 /etc/fstab, 편집해야 합니다 /etc/fstab 파일. 를 위해 /opt/netapp/data/ 마운트 옵션에서 MySQL 레이블을 다음과 같이 추가합니다.

```
context=system_u:object_r:mysql_d_b_t:s0
```

- c. 언마운트하고 다시 마운트 /opt/netapp/data/ 맥락을 활성화하기 위해.

- d. 직접 NFS 마운트가 있는 경우 다음 명령을 실행하여 컨텍스트를 설정합니다. mysql_d_b_t:

```
mount <nfsshare>:<mountpoint> /opt/netapp/data -o
context=system_u:object_r:mysql_d_b_t:s0
```

3. 컨텍스트가 올바르게 설정되었는지 확인하세요.

```
ls -dZ /opt/netapp/data/
```

샘플 출력:

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysql_db_t:s0
/opt/netapp/data/
```

SELinux 컨텍스트를 구성합니다. /opt/netapp 마운트되어 있으며 /opt/netapp/data/ 또한 별도로 장착됩니다

이 시나리오에서는 먼저 컨텍스트를 설정해야 합니다. /opt/netapp/data/ 이전 섹션에서 설명한 대로. 올바른 컨텍스트를 설정한 후 /opt/netapp/data/ , 부모 디렉토리를 확인하세요 /opt/netapp SELinux 컨텍스트가 설정되어 있지 않습니다. file_t .

단계

1. 컨텍스트를 확인하려면 다음 명령을 실행하세요.

```
ls -dZ /opt/netapp
```

샘플 출력:

```
drwxr-xr-x. mysql root unconfined_u:object_r:file_t:s0 /opt/netapp
```

이 출력에서 컨텍스트는 다음과 같습니다. file_t 바뀌어야 합니다. 다음 명령은 컨텍스트를 설정합니다. usr_t . 컨텍스트를 다른 값으로 설정할 수 있습니다. file_t 귀하의 보안 요구 사항에 따라.

2. 마운트한 방식에 따라 컨텍스트를 설정하려면 다음 단계를 수행하십시오. /opt/netapp .
 - a. 다음 명령을 실행하여 컨텍스트를 설정하세요.

```
semanage fcontext -a -t usr_t "/opt/netapp"
restorecon -v /opt/netapp
```

1. 구성한 경우 /opt/netapp ~에 /etc/fstab , 편집해야 합니다 /etc/fstab 파일. 를 위해 /opt/netapp 마운트 옵션에서 MySQL 레이블을 다음과 같이 추가합니다.

```
context=system_u:object_r:usr_t:s0
```

2. 언마운트 후 다시 마운트 /opt/netapp 맥락을 활성화하기 위해.
3. 직접 NFS 마운트가 있는 경우 다음 명령을 실행하여 컨텍스트를 설정합니다.

```
mount <nfsshare>:<mountpoint> /opt/netapp -o
context=system_u:object_r:usr_t:s0
```

- a. 컨텍스트가 올바르게 설정되었는지 확인하세요.

```
ls -dZ /opt/netapp
```

샘플 출력

```
drwxr-xr-x. mysql root unconfined_u:object_r:usr_t:s0 /opt/netapp
```

SELinux 컨텍스트를 구성합니다. /opt/netapp 마운트되어 있으며 /opt/netapp/data/ 별도로 마운트되지 않습니다

마운트한 경우 /opt/netapp 시스템에서 SELinux가 설정되어 있습니다. Enforcing, SELinux 컨텍스트 유형을 확인하십시오. /opt/netapp 로 설정됩니다 mysql_d_b_t 이는 데이터베이스 파일의 위치에 대한 기본 컨텍스트 요소입니다.

단계

1. 컨텍스트를 확인하려면 다음 명령을 실행하세요.

```
ls -dZ /opt/netapp
```

샘플 출력:

```
drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0 /opt/netapp
```



이 출력에서 컨텍스트는 다음과 같습니다. default_t. 이 컨텍스트를 다음으로 변경해야 합니다. mysql_d_b_t.

2. 마운트 방법에 따라 컨텍스트를 설정하려면 다음 단계를 수행하십시오. /opt/netapp .

- a. 다음 명령을 실행하여 컨텍스트를 설정하세요. mysql_d_b_t :
semanage fcontext -a -t mysql_d_b_t "/opt/netapp"
`restorecon -R -v /opt/netapp
- b. 구성된 경우 /opt/netapp ~에 /etc/fstab , 편집하다 /etc/fstab 파일. 를 위해 /opt/netapp/ 마운트 옵션에서 MySQL 레이블을 다음과 같이 추가합니다.
context=system_u:object_r:mysql_d_b_t:s0
- c. 언마운트 후 다시 마운트 /opt/netapp/ 맥락을 활성화하기 위해.
- d. 직접 NFS 마운트가 있는 경우 다음 명령을 실행하여 컨텍스트를 설정합니다. mysql_d_b_t :
mount <nfsshare>:/<mountpoint> /opt/netapp -o
context=system_u:object_r:mysql_d_b_t:s0

3. 컨텍스트가 올바르게 설정되었는지 확인하세요.

```
ls -dZ /opt/netapp/
```

샘플 출력:

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysql_d_b_t:s0 /opt/netapp/
```

Linux 시스템에 Unified Manager 설치

Unified Manager를 다운로드하고 설치하는 단계의 순서는 설치 시나리오에 따라 다르다는 점을 이해하는 것이 중요합니다.

설치 전에 사용자 정의 사용자 홈 디렉토리와 **umadmin** 비밀번호를 만드세요.

Unified Manager를 설치하기 전에 사용자 정의 홈 디렉토리를 만들고 umadmin 사용자 비밀번호를 정의할 수 있습니다. 이 작업은 선택 사항이지만 일부 사이트에서는 Unified Manager 설치 기본 설정을 재정의하는 유연성이 필요할 수 있습니다.

시작하기 전에

- 시스템은 다음에 설명된 요구 사항을 충족해야 합니다. ["하드웨어 시스템 요구 사항"](#).
- Red Hat Enterprise Linux 시스템에 루트 사용자로 로그인할 수 있어야 합니다.

기본 Unified Manager 설치의 다음 작업을 수행합니다.

- umadmin 사용자를 생성합니다. /home/umadmin 홈 디렉토리로 사용.
- umadmin 사용자에게 기본 비밀번호 "admin"을 할당합니다.

일부 설치 환경은 액세스를 제한하기 때문에 /home, 설치가 실패합니다. 다른 위치에 홈 디렉토리를 만들어야 합니다. 또한, 일부 사이트에는 비밀번호 복잡성에 대한 규칙이 있거나 설치 프로그램에서 설정하는 대신 로컬 관리자가 비밀번호를 설정하도록 요구하는 경우도 있습니다.

설치 환경에서 이러한 설치 기본 설정을 재정의해야 하는 경우 다음 단계에 따라 사용자 지정 홈 디렉토리를 만들고 umadmin 사용자의 비밀번호를 정의하세요.

이 정보가 설치 전에 정의되어 있으면 설치 스크립트가 이러한 설정을 검색하여 설치 기본 설정 대신 정의된 값을 사용합니다.

또한 기본 Unified Manager 설치에는 sudoers 파일에 umadmin 사용자가 포함됩니다.(ocum_sudoers 그리고 ocie_sudoers)에서 /etc/sudoers.d/ 예배 규칙서. 보안 정책이나 일부 보안 모니터링 도구로 인해 환경에서 이 콘텐츠를 제거한 경우 다시 추가해야 합니다. 일부 Unified Manager 작업에는 sudo 권한이 필요하므로 sudoers 구성을 보존해야 합니다.

사용자 환경의 보안 정책은 Unified Manager 유지 관리 사용자의 sudo 권한을 제한해서는 안 됩니다. 권한이 제한되면 일부 Unified Manager 작업이 실패할 수 있습니다. 설치가 성공적으로 완료된 후 umadmin 사용자로 로그인하여 다음 sudo 명령을 실행할 수 있는지 확인하세요.

```
sudo systemctl status ocie
```

이 명령은 오류 없이 ocie 서비스의 적절한 상태를 반환해야 합니다.

단계

1. 서버에 루트 사용자로 로그인합니다.
2. "maintenance"라는 umadmin 그룹 계정을 만듭니다.

```
groupadd maintenance
```

3. 원하는 홈 디렉토리 아래의 유지 관리 그룹에 “umadmin” 사용자 계정을 만듭니다.

```
adduser --home <home_directory> -g maintenance umadmin
```

4. umadmin 비밀번호를 정의합니다:

```
passwd umadmin
```

시스템에서 umadmin 사용자에게 대한 새 비밀번호 문자열을 입력하라는 메시지가 표시됩니다.

Unified Manager를 설치한 후에는 umadmin 사용자 로그인 셸을 지정해야 합니다.

Unified Manager 다운로드

Unified Manager를 다운로드해야 합니다. .zip NetApp 지원 사이트에서 Unified Manager를 설치할 파일을 다운로드하세요.

시작하기 전에

NetApp 지원 사이트에 대한 로그인 자격 증명이 있어야 합니다.

Red Hat Enterprise Linux 시스템용 Unified Manager 설치 패키지를 다운로드합니다.

단계

1. NetApp 지원 사이트에 로그인하고 Unified Manager 다운로드 페이지로 이동합니다.

["NetApp 지원 사이트"](#)

2. 필요한 Unified Manager 버전을 선택하고 최종 사용자 라이선스 계약(EULA)에 동의합니다.

3. Linux용 Unified Manager 설치 프로그램 파일을 다운로드하고 저장하세요. .zip 파일을 대상 시스템의 디렉토리로 복사합니다.



◦ Red Hat Enterprise Linux 시스템에 맞는 올바른 버전의 설치 파일을 다운로드했는지 확인하세요. Red Hat Enterprise Linux 8 또는 9가 설치되어 있는지 여부에 따라 적절한 버전의 Unified Manager를 다운로드해야 합니다. .zip 파일.

◦ NetApp 코드 서명 인증서를 다운로드할 것을 권장합니다.(.pem) 및 디지털 서명(.sig)와 함께 .zip 파일.

4. 다운로드한 소프트웨어의 무결성을 위해 체크섬을 확인하세요.

5. 코드 서명 인증서와 디지털 서명을 다운로드했다면 설치 프로그램 파일의 무결성을 확인할 수 있습니다. 다음 명령을 사용하여 설치 프로그램 파일의 무결성을 확인할 수 있습니다.

◦ 이 명령은 코드 서명 인증서의 공개 키를 사용하여 파일을 생성합니다.

```
openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem >  
<public_key_file_name>
```

▪ 여기서 *AIQUM-RHEL-CLIENT-INTER-ROOT.pem*은 코드 서명 인증서가 포함된 파일입니다.

- 이 명령은 설치 프로그램 파일의 서명을 확인합니다.

```
openssl dgst -sha256 -verify <public_key_file_name> -signature
<signature_file_name> ActiveIQUnifiedManager-<version>.zip
```

다음과 유사한 메시지 Verified Ok 설치 프로그램 파일을 사용하는 것이 안전함을 확인합니다.

Unified Manager 설치

물리적 또는 가상 Red Hat Enterprise Linux 플랫폼에 Unified Manager를 설치할 수 있습니다.

시작하기 전에

- Unified Manager를 설치하려는 시스템은 시스템 및 소프트웨어 요구 사항을 충족해야 합니다.

보다"[하드웨어 시스템 요구 사항](#)".

보다"[Linux 소프트웨어 및 설치 요구 사항](#)".

- Unified Manager를 다운로드해야 합니다. .zip NetApp 지원 사이트에서 대상 시스템으로 파일을 복사합니다.
- 다운로드한 파일의 무결성을 검증했어야 합니다. .zip 파일.
- 지원되는 웹 브라우저가 있어야 합니다.
- 터미널 에뮬레이션 소프트웨어에서 스크롤백 기능이 활성화되어 있어야 합니다.

Red Hat Enterprise Linux 시스템에는 필요한 지원 소프트웨어(Java, MySQL, 추가 유틸리티)의 모든 필수 버전이 설치되어 있을 수도 있고, 필요한 소프트웨어 중 일부만 설치되어 있을 수도 있고, 필요한 소프트웨어가 전혀 설치되지 않은 새로 설치된 시스템일 수도 있습니다.

단계

1. Unified Manager를 설치할 서버에 로그인합니다.
2. 설치를 지원하기 위해 대상 시스템에 어떤 소프트웨어를 설치하거나 업그레이드해야 할지 평가하려면 적절한 명령을 입력하세요.

필수 소프트웨어 및 최소 버전	소프트웨어 및 버전을 확인하는 명령
OpenJDK 버전 11.0.25	java -version
MySQL 8.4.4 커뮤니티 에디션	`rpm -qa
grep -i mysql`	p7zip 16.02
`rpm -qa	grep p7zip`

3. 설치된 MySQL 버전이 MySQL 8.4.4 Community Edition보다 이전 버전인 경우 다음 명령을 입력하여 제거하세요.


```
rpm -e <mysql_package_name>
```

종속성 오류가 발생하면 다음을 추가해야 합니다. --nodeps 구성 요소를 제거하는 옵션입니다.

4. 설치를 다운로드한 디렉토리로 이동합니다. .zip 파일을 열고 Unified Manager 번들을 확장합니다.

```
unzip ActiveIQUnifiedManager-<version>.zip
```

필요한 .rpm Unified Manager용 모듈이 대상 디렉토리에 압축 해제됩니다.

5. 다음 모듈이 디렉토리에 있는지 확인하세요.

```
ls *.rpm
```

```
netapp-um<version>.x86_64.rpm
```

6. 사전 설치 스크립트를 실행하여 Unified Manager 설치와 충돌할 수 있는 시스템 구성 설정이나 설치된 소프트웨어가 없는지 확인하세요.

```
sudo ./pre_install_check.sh
```

사전 설치 스크립트는 시스템에 유효한 Red Hat Enterprise Linux 구독이 있는지, 그리고 필요한 소프트웨어 저장소에 액세스할 수 있는지 확인합니다. 스크립트에서 문제가 발견되면 Unified Manager를 설치하기 전에 해당 문제를 해결해야 합니다.

Red Hat Enterprise Linux 8 시스템의 경우 AppStream 저장소에서 제공하는 JDK 11 - OpenJDK, p7zip 및 기타 소프트웨어 패키지가 포함된 내부 저장소가 있는 경우 AppStream 저장소를 비활성화하고 MySQL Community Server를 설치해야 합니다. 다음 명령을 실행하세요.

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install  
mysql-community-server
```

7. 선택 사항: 시스템이 인터넷에 연결되어 있지 않고 설치에 필요한 패키지를 수동으로 다운로드해야 하는 경우에만 7단계를 수행해야 합니다. 시스템에 인터넷 접속이 가능하고 필요한 패키지를 모두 사용할 수 있는 경우 8단계로 이동합니다. 인터넷에 연결되지 않았거나 Red Hat Enterprise Linux 저장소를 사용하지 않는 시스템의 경우, 다음 단계를 수행하여 필수 패키지가 누락되었는지 확인한 다음, 해당 패키지를 다운로드하세요.

- a. Unified Manager를 설치하는 시스템에서 사용 가능한 패키지와 사용할 수 없는 패키지 목록을 확인하세요.

```
yum install netapp-um<version>.x86_64.rpm --assumeno
```

“설치 중:” 섹션의 항목은 현재 디렉토리에서 사용 가능한 패키지이고, “종속성을 위한 설치:” 섹션의 항목은 시스템에서 누락된 패키지입니다.

- b. 인터넷 접속이 가능한 시스템에서 누락된 패키지를 다운로드하세요.

```
yum install <package_name> --downloadonly --downloadaddir=.
```



Red Hat Enterprise Linux 시스템에서는 “yum-plugin-downloadonly” 플러그인이 항상 활성화되어 있지 않으므로 패키지를 설치하지 않고도 다운로드하는 기능을 활성화해야 할 수도 있습니다.

```
yum install yum-plugin-downloadonly
```

a. 인터넷에 연결된 시스템에서 누락된 패키지를 설치 시스템으로 복사합니다.

8. 루트 사용자로 또는 다음을 사용하여 `sudo` 다음 명령을 실행하여 소프트웨어를 설치하세요.

```
yum install netapp-um<version>.x86_64.rpm
```

이 명령은 .rpm 패키지, 기타 필요한 지원 소프트웨어, Unified Manager 소프트웨어를 설치합니다.

GPG NOKEY 오류로 인해 설치가 실패하면 다음을 사용하세요. rpm --import URL에서 키를 가져오려면:

rpm --가져오기 <https://repo.mysql.com/RPM-GPG-KEY-mysql-2023>



대체 명령(예:)을 사용하여 설치를 시도하지 마십시오. rpm -ivh). Red Hat Enterprise Linux 시스템에 Unified Manager를 성공적으로 설치하려면 모든 Unified Manager 파일과 관련 파일이 자동으로 적용되는 특정 디렉토리 구조에 특정 순서로 설치되어야 합니다. yum install netapp-um<version>.x86_64.rpm 명령.

9. 설치 메시지 바로 뒤에 표시되는 이메일 알림은 무시하세요.

이 이메일은 설치에 부정적인 영향을 미치지 않는 초기 크론 작업 실패를 루트 사용자에게 알립니다.

10. 설치 메시지가 완료되면 Unified Manager 웹 UI의 IP 주소 또는 URL, 유지 관리 사용자 이름(umadmin), 기본 암호가 시스템에 표시되는 메시지가 나올 때까지 메시지를 뒤로 스크롤합니다.

메시지는 다음과 비슷합니다.

```
Active IQ Unified Manager installed successfully.
Use a web browser and one of the following URL(s) to configure and
access the Unified Manager GUI.
https://default_ip_address/      (if using IPv4)
https://[default_ip_address]/    (if using IPv6)
https://fully_qualified_domain_name/

Log in to Unified Manager in a web browser by using following details:
  username: umadmin
  password: admin
```

11. IP 주소 또는 URL, 할당된 사용자 이름(umadmin), 현재 비밀번호를 기록해 둡니다.
12. Unified Manager를 설치하기 전에 사용자 지정 홈 디렉토리가 있는 umadmin 사용자 계정을 만든 경우 umadmin 사용자 로그인 셸을 지정해야 합니다.

```
usermod -s /bin/maintenance-user-shell.sh umadmin
```

umadmin 사용자의 기본 비밀번호를 변경하고 Unified Manager의 초기 설정을 수행하려면 웹 UI에 액세스하세요 .["Active IQ Unified Manager 구성"](#) . umadmin 사용자의 기본 비밀번호를 변경하는 것이 필수입니다.

Unified Manager 설치 중에 생성된 사용자

Red Hat Enterprise Linux에 Unified Manager를 설치하면 Unified Manager와 타사 유틸리티를 통해 umadmin, jboss, mysql이라는 사용자가 생성됩니다.

- 우마스터

Unified Manager에 처음 로그인하는 데 사용됩니다. 이 사용자에게는 "애플리케이션 관리자" 사용자 역할이 할당되고 "유지 관리 사용자" 유형으로 구성됩니다. 이 사용자는 Unified Manager에 의해 생성되었습니다.

- 제이보스

JBoss 유틸리티와 관련된 Unified Manager 서비스를 실행하는 데 사용됩니다. 이 사용자는 Unified Manager에 의해 생성되었습니다.

- 마이SQL

Unified Manager의 MySQL 데이터베이스 쿼리를 실행하는 데 사용됩니다. 이 사용자는 MySQL 타사 유틸리티에 의해 생성되었습니다.

이러한 사용자 외에도 Unified Manager는 maintenance, jboss, mysql이라는 해당 그룹도 생성합니다. 유지 관리 및 jboss 그룹은 Unified Manager에 의해 생성되고, MySQL 그룹은 타사 유틸리티에 의해 생성됩니다.



Unified Manager를 설치하기 전에 사용자 지정 홈 디렉토리를 만들고 고유한 umadmin 사용자 비밀번호를 정의한 경우, 설치 프로그램은 유지 관리 그룹이나 umadmin 사용자를 다시 만들지 않습니다.

JBoss 비밀번호 변경

설치 중에 설정된 인스턴스별 JBoss 비밀번호를 재설정할 수 있습니다. 사이트에 Unified Manager 설치 설정을 재정의하기 위해 이 보안 기능이 필요한 경우 선택적으로 비밀번호를 재설정할 수 있습니다. 이 작업은 JBoss가 MySQL에 액세스하는 데 사용하는 비밀번호도 변경합니다.

- Unified Manager가 설치된 Red Hat Enterprise Linux 시스템에 루트 사용자 액세스 권한이 있어야 합니다.
- NetApp 에서 제공하는 서비스에 액세스할 수 있어야 합니다. password.sh 디렉토리의 스크립트 `/opt/netapp/essentials/bin.`

단계

1. 시스템에 루트 사용자로 로그인합니다.
2. 다음 명령을 표시된 순서대로 입력하여 Unified Manager 서비스를 중지합니다.

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

연관된 MySQL 소프트웨어를 중지하지 마세요.

3. 비밀번호 변경 프로세스를 시작하려면 다음 명령을 입력하세요.

```
/opt/netapp/essentials/bin/password.sh resetJBossPassword
```

4. 메시지가 표시되면 새로운 JBoss 비밀번호를 입력한 다음 확인을 위해 두 번째로 비밀번호를 입력합니다.

비밀번호는 8~16자여야 하며, 숫자, 대문자, 소문자, 그리고 다음 특수 문자 중 하나 이상을 포함해야 합니다.

```
!@%^*-_=[]:<>./~+
```

5. 스크립트가 완료되면 다음 명령을 표시된 순서대로 입력하여 Unified Manager 서비스를 시작합니다.

```
systemctl start ocie
```

```
systemctl start ocieau
```

6. 모든 서비스가 시작된 후 Unified Manager UI에 로그인할 수 있습니다.

Red Hat Enterprise Linux에서 Unified Manager 업그레이드

새로운 버전이 출시되면 Unified Manager를 업그레이드할 수 있습니다.

NetApp 에서 제공하는 Unified Manager 소프트웨어 패치 릴리스는 새 릴리스와 동일한 절차를 사용하여 설치됩니다.

Unified Manager가 OnCommand Workflow Automation 인스턴스와 페어링되어 있고 두 제품 모두에 사용 가능한 소프트웨어의 새 버전이 있는 경우, 업그레이드를 수행한 후 두 제품의 연결을 해제한 다음 새 Workflow Automation 연결을 설정해야 합니다. 제품 중 하나만 업그레이드하는 경우 업그레이드 후 Workflow Automation에 로그인하여 Unified Manager에서 여전히 데이터를 수집하고 있는지 확인해야 합니다.

Unified Manager 버전에 지원되는 업그레이드 경로

Active IQ Unified Manager 각 버전에 대해 특정 업그레이드 경로를 지원합니다.

Unified Manager의 일부 버전은 이후 버전으로의 내부 업그레이드를 수행할 수 없습니다. Unified Manager 업그레이드는 N-2 모델로 제한됩니다. 즉, 모든 플랫폼에서 다음 2개 릴리스 내에서만 업그레이드를 수행할 수 있습니다. 예를 들어 Unified Manager 9.13 및 9.14에서만 Unified Manager 9.16로 업그레이드할 수 있습니다.

지원되는 버전보다 이전 버전을 실행 중인 경우 Unified Manager 인스턴스를 먼저 지원되는 버전 중 하나로 업그레이드한 다음, 현재 버전으로 업그레이드해야 합니다.

예를 들어, 설치된 버전이 Unified Manager 9.9이고 Unified Manager 9.14로 업그레이드하려는 경우 업그레이드 순서를 따르면 됩니다.

업그레이드 경로 샘플:

1. 9.11 → 9.13으로 업그레이드
2. 9.13 → 9.14로 업그레이드
3. 9.13 → 9.16으로 업그레이드
4. 9.14 → 9.16으로 업그레이드

업그레이드 경로 매트릭스에 대한 자세한 내용은 다음을 참조하세요. ["지식 기반\(KB\) 문서"](#).

Unified Manager 업그레이드

Linux 플랫폼에서 설치 파일을 다운로드하여 실행하면 Unified Manager 9.13 또는 9.14에서 9.16로 업그레이드할 수 있습니다.

시작하기 전에

- Unified Manager를 업그레이드하는 시스템은 시스템 및 소프트웨어 요구 사항을 충족해야 합니다.

보다 ["하드웨어 시스템 요구 사항"](#).

보다 ["Linux 소프트웨어 및 설치 요구 사항"](#).

- Red Hat Enterprise Linux Subscription Manager 구독이 필요합니다.
- Unified Manager를 업그레이드하기 전에 올바른 버전의 OpenJDK를 설치하거나 업그레이드해야 합니다.

보다 ["Linux에서 JRE 업그레이드"](#).

- 데이터 손실을 방지하려면 업그레이드 중에 문제가 발생할 경우를 대비해 Unified Manager 데이터베이스의 백업을 만들어야 합니다. NetApp 백업 파일을 다음에서 이동할 것을 권장합니다. /opt/netapp/data 외부 위치로의 디렉토리.
- 업그레이드하는 동안 성능 데이터를 13개월 동안 보관하는 기존 기본 설정을 유지할지, 아니면 6개월로 변경할지 묻는 메시지가 표시될 수 있습니다. 확인 후, 과거 성과 데이터는 6개월 후에 삭제됩니다.
- 업그레이드 프로세스 중에는 Unified Manager를 사용할 수 없으므로 실행 중인 모든 작업을 완료했어야 합니다.
- MySQL Community Edition은 Unified Manager 업그레이드 중에 자동으로 업그레이드됩니다. 시스템에 설치된 MySQL 버전이 8.4.4 이전인 경우 Unified Manager 업그레이드 프로세스는 자동으로 MySQL을 8.4.4로 업그레이드합니다.

단계

1. 대상 Red Hat Enterprise Linux 서버에 로그인합니다.
2. Unified Manager 번들을 서버에 다운로드합니다.

보다 ["Linux용 Unified Manager 다운로드"](#).

3. 대상 디렉토리로 이동하여 Unified Manager 번들을 확장합니다.

```
unzip ActiveIQUnifiedManager-<version>.zip
```

Unified Manager에 필요한 RPM 모듈이 대상 디렉토리에 압축 해제됩니다.

4. 다음 모듈이 디렉토리에 있는지 확인하세요.

```
ls *.rpm
```

```
netapp-um<version>.x86_64.rpm
```

5. 사전 설치 스크립트를 실행하여 업그레이드와 충돌할 수 있는 시스템 구성 설정이나 설치된 소프트웨어가 없는지 확인하세요.

```
sudo ./pre_install_check.sh
```

사전 설치 스크립트는 시스템에 유효한 Red Hat Enterprise Linux 구독이 있는지, 그리고 필요한 소프트웨어 저장소에 액세스할 수 있는지 확인합니다. 스크립트에서 문제가 발견되면 문제를 해결하고 업그레이드를 계속 진행해야 합니다.

누락된 패키지가 감지된 경우 다음 단계를 수행하십시오. **"누락된 패키지에 대해 수행해야 할 추가 단계"**. 누락된 패키지가 없으면 다음 단계로 넘어가세요.

6. 다음 스크립트를 사용하여 Unified Manager를 업그레이드하세요.

```
upgrade.sh
```

이 스크립트는 RPM 모듈을 자동으로 실행하여 필요한 지원 소프트웨어와 해당 모듈에서 실행되는 Unified Manager 모듈을 업그레이드합니다. 또한 업그레이드 스크립트는 업그레이드와 충돌할 수 있는 시스템 구성 설정이나 설치된 소프트웨어가 있는지 확인합니다. 스크립트에서 문제가 발견되면 Unified Manager를 업그레이드하기 전에 해당 문제를 해결해야 합니다. Unified Manager를 업그레이드하기 전에 `_net-snmp_`와 같은 패키지를 이미 설치한 경우, MySQL 종속성으로 인해 업그레이드 중에 해당 패키지가 제거될 수 있습니다. 계속해서 사용하려면 패키지를 다시 수동으로 설치해야 합니다.

7. 업그레이드가 완료되면 Unified Manager 웹 UI의 IP 주소 또는 URL, 유지 관리 사용자 이름(umadmin), 기본 비밀번호가 표시된 메시지가 나타날 때까지 메시지를 뒤로 스크롤합니다.

메시지는 다음과 비슷합니다.

```
Active IQ Unified Manager upgraded successfully.  
Use a web browser and one of the following URLs to access the Unified  
Manager GUI:
```

```
https://default_ip_address/      (if using IPv4)  
https://[default_ip_address]/    (if using IPv6)  
https://fully_qualified_domain_name/
```

지원되는 웹 브라우저의 새 창에 지정된 IP 주소 또는 URL을 입력하여 Unified Manager 웹 UI를 시작한 다음, 이전에 설정한 동일한 유지 관리 사용자 이름(umadmin)과 비밀번호를 사용하여 로그인합니다.

누락된 패키지에 대해 수행해야 할 추가 단계

업그레이드 중에 사이트에서 누락된 패키지가 감지되거나, 시스템이 인터넷에 연결되어 있지 않거나, Red Hat Enterprise Linux 저장소를 사용하지 않는 경우, 다음 단계를 수행하여 필요한 패키지가 누락되었는지 확인하고 해당 패키지를 다운로드하세요.



이러한 단계는 주요 절차의 **_5_ 단계** 이후에 수행되어야 합니다. 이 절차를 통해 Unified Manager가 업그레이드되므로 업그레이드를 위해 추가 단계를 실행할 필요가 없습니다.

1. 사용 가능한 패키지와 사용할 수 없는 패키지 목록을 확인하세요.

```
yum install netapp-um<version>.x86_64.rpm --assumeno
```

“설치 중:” 섹션의 항목은 현재 디렉토리에서 사용 가능한 패키지이고, “종속성을 위한 설치:” 섹션의 항목은 시스템에서 누락된 패키지입니다.

2. 인터넷에 접속할 수 있는 다른 시스템에서 다음 명령을 실행하여 누락된 패키지를 다운로드합니다.

```
yum install package_name --downloadonly --downloadaddr=.
```

패키지는 지정된 디렉토리에 다운로드됩니다. --downloadaddr=.

Red Hat Enterprise Linux 시스템에서는 “yum-plugin-downloadonly” 플러그인이 항상 활성화되어 있지 않으므로 패키지를 설치하지 않고도 다운로드하는 기능을 활성화해야 할 수도 있습니다.

```
yum install yum-plugin-downloadonly
```

3. 다운로드한 패키지를 설치 시스템에서 Unified Manager 번들을 압축 해제한 디렉토리에 복사합니다.
4. 해당 디렉토리로 디렉토리를 변경하고 다음 명령을 실행하여 누락된 패키지와 해당 종속성을 설치합니다.

```
yum install *.rpm
```

5. Unified Manager 서버를 시작합니다. 다음 명령을 실행하세요:

```
systemctl start ocie
```

```
systemctl start ocieau
```

이 프로세스를 통해 Unified Manager 업그레이드 프로세스가 완료됩니다. 지원되는 웹 브라우저의 새 창에 지정된 IP 주소 또는 URL을 입력하여 Unified Manager 웹 UI를 시작한 다음, 이전에 설정한 동일한 유지 관리 사용자 이름(umadmin)과 비밀번호를 사용하여 로그인합니다.

호스트 OS를 Red Hat Enterprise Linux 7.x에서 8.x로 업그레이드합니다.

이전에 Red Hat Enterprise Linux 7.x 시스템에 Unified Manager를 설치했고 Red Hat Enterprise Linux 8.x로 업그레이드해야 하는 경우 이 항목에 나열된 절차 중 하나를 따라야 합니다. 두 경우 모두 Red Hat Enterprise Linux 7.x 시스템에서 Unified Manager 백업을 만든 다음, 해당 백업을 Red Hat Enterprise Linux 8.x 시스템으로 복원해야 합니다. 지원되는 Red Hat Enterprise Linux 버전은 8.0~8.10입니다.

아래 나열된 두 옵션의 차이점은 한 경우에는 새로운 8.x 서버에 Unified Manager 복원을 수행하고, 다른 경우에는 동일한 서버에 복원 작업을 수행한다는 것입니다.

이 작업을 수행하려면 Red Hat Enterprise Linux 7.x 시스템에서 Unified Manager의 백업을 만들어야 하므로 Unified Manager가 오프라인 상태를 최단 시간 동안 유지하도록 전체 업그레이드 프로세스를 완료할 준비가 된 경우에만 백업을 만들어야 합니다. 수집된 데이터의 차이는 Red Hat Enterprise Linux 7.x 시스템이 종료되고 새로운 Red Hat Enterprise Linux 8.x가 시작되기 전까지의 기간 동안 Unified Manager UI에 나타납니다.

보다"백업 및 복원 작업 관리" 백업 및 복원 프로세스에 대한 자세한 지침을 검토해야 하는 경우

Red Hat Enterprise Linux 8.x 소프트웨어를 설치할 수 있는 예비 시스템이 있는 경우 다음 단계를 따라 Red Hat Enterprise Linux 7.x 시스템을 계속 사용할 수 있는 동안 해당 시스템에서 Unified Manager 복원을 수행할 수 있습니다.

1. Red Hat Enterprise Linux 8.x 소프트웨어로 새로운 서버를 설치하고 구성합니다.

보다"[Linux 소프트웨어 및 설치 요구 사항](#)".

2. Red Hat Enterprise Linux 8.x 시스템에서 기존 Red Hat Enterprise Linux 7.x 시스템에 있는 것과 동일한 버전의 Unified Manager 소프트웨어를 설치합니다.

보다"[Linux에 Unified Manager 설치](#)".

설치가 완료되면 UI를 실행하거나 클러스터, 사용자 또는 인증 설정을 구성하지 마세요. 백업 파일은 복원 과정 중에 이 정보를 채웁니다.

3. Red Hat Enterprise Linux 7.x 시스템에서 웹 UI의 관리 메뉴에서 Unified Manager 백업을 만든 다음 백업 파일을 복사합니다.(.7z 파일) 및 데이터베이스 저장소 디렉토리의 내용(/database-dumps-repo 하위 디렉토리)를 외부 위치로 복사합니다.
4. Red Hat Enterprise Linux 7.x 시스템에서 Unified Manager를 종료합니다.
5. Red Hat Enterprise Linux 8.x 시스템에서 백업 파일을 복사합니다.(.7z 외부 위치에서 파일)로 /opt/netapp/data/ocum-backup/ 그리고 데이터베이스 저장소 파일을 /database-dumps-repo 하위 디렉토리 /ocum-backup 예배 규칙서.
6. 백업 파일에서 Unified Manager 데이터베이스를 복원하려면 다음 명령을 입력하세요.

```
um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
```

7. 웹 브라우저에 IP 주소나 URL을 입력하여 Unified Manager 웹 UI를 시작한 다음 시스템에 로그인합니다.

시스템이 제대로 작동하는지 확인한 후 Red Hat Enterprise Linux 7.x 시스템에서 Unified Manager를 제거할 수 있습니다.

동일한 서버에서 호스트 **OS** 업그레이드

Red Hat Enterprise Linux 8.x 소프트웨어를 설치할 수 있는 여분의 시스템이 없는 경우 다음 단계를 따르세요.

1. 웹 UI의 관리 메뉴에서 Unified Manager 백업을 만든 다음 백업 파일을 복사합니다.(.7z 파일) 및 데이터베이스 저장소 디렉토리의 내용(/database-dumps-repo 하위 디렉토리)를 외부 위치로 복사합니다.
2. 시스템에서 Red Hat Enterprise Linux 7.x 이미지를 제거하고 시스템을 완전히 지웁니다.
3. 동일한 시스템에 Red Hat Enterprise Linux 8.x 소프트웨어를 설치하고 구성합니다.

보다"[Linux 소프트웨어 및 설치 요구 사항](#)".

4. Red Hat Enterprise Linux 8.x 시스템에서는 Red Hat Enterprise Linux 7.x 시스템에 있던 Unified Manager 소프트웨어와 동일한 버전을 설치합니다.

보다"[Linux에 Unified Manager 설치](#)".

설치가 완료되면 UI를 실행하거나 클러스터, 사용자 또는 인증 설정을 구성하지 마세요. 백업 파일은 복원 과정 중에 이 정보를 채웁니다.

5. 백업 파일을 복사하세요(.7z 외부 위치에서 파일)로 /opt/netapp/data/ocum-backup/ 그리고 데이터베이스 저장소 파일을 /database-dumps-repo 하위 디렉토리 /ocum-backup 예배 규칙서.

6. 백업 파일에서 Unified Manager 데이터베이스를 복원하려면 다음 명령을 입력하세요.

```
um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
```

7. 웹 브라우저에 IP 주소나 URL을 입력하여 Unified Manager 웹 UI를 시작한 다음 시스템에 로그인합니다.

Unified Manager 설치 후 타사 제품 업그레이드

Linux 시스템에 Unified Manager가 이미 설치되어 있는 경우 JRE와 같은 타사 제품을 업그레이드할 수 있습니다.

이러한 타사 제품을 개발하는 회사는 정기적으로 보안 취약점을 보고합니다. 귀하의 일정에 맞춰 이 소프트웨어의 최신 버전으로 업그레이드할 수 있습니다.

Linux에서 OpenJDK 업그레이드

Unified Manager가 설치된 Linux 서버에서 최신 버전의 OpenJDK로 업그레이드하면 보안 취약점에 대한 수정 사항을 얻을 수 있습니다.

시작하기 전에

Unified Manager가 설치된 Linux 시스템에 대한 루트 권한이 있어야 합니다.

릴리스 패밀리 내에서 OpenJDK 릴리스를 업데이트할 수 있습니다. 예를 들어, OpenJDK 11.0.14에서 OpenJDK 11.0.17로 업그레이드할 수 있지만, OpenJDK 11에서 OpenJDK 12로 직접 업데이트할 수는 없습니다.

단계

1. Unified Manager 호스트 머신에 루트 사용자로 로그인합니다.
2. 대상 시스템에 적합한 버전의 OpenJDK(64비트)를 다운로드합니다.
3. Unified Manager 서비스를 중지합니다.

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

4. 시스템에 최신 OpenJDK를 설치합니다.
5. Unified Manager 서비스를 시작합니다.

```
systemctl start ocie
```

```
systemctl start ocieau
```

Unified Manager를 다시 시작하세요

구성을 변경한 후에는 Unified Manager를 다시 시작해야 할 수도 있습니다.

시작하기 전에

Unified Manager가 설치된 Red Hat Enterprise Linux 서버에 루트 사용자 액세스 권한이 있어야 합니다.

단계

1. Unified Manager 서비스를 다시 시작하려는 서버에 루트 사용자로 로그인합니다.
2. 다음 순서대로 Unified Manager 서비스와 관련 MySQL 서비스를 중지합니다.

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

```
systemctl stop mysqld
```

3. 다음 순서대로 MySQL 및 Unified Manager 서비스를 시작합니다.

```
systemctl start mysqld
```

```
systemctl start ocie
```

```
systemctl start ocieau
```



'mysqld' MySQL 서버를 시작 및 중지하는 데 필요한 데몬 프로그램입니다.

통합 관리자 제거

단일 명령으로 Red Hat Enterprise Linux 호스트에서 Unified Manager를 중지하고 제거할 수 있습니다.

시작하기 전에

- Unified Manager를 제거하려는 서버에 대한 루트 사용자 액세스 권한이 있어야 합니다.
- Linux 시스템에서는 보안 강화 Linux(SELinux)를 비활성화해야 합니다. SELinux 런타임 모드를 "Permissive"로 변경하려면 다음을 사용하세요. `setenforce 0` 명령.
- 소프트웨어를 제거하기 전에 Unified Manager 서버에서 모든 클러스터(데이터 소스)를 제거해야 합니다.
- MySQL 포트 3306을 허용하거나 차단하기 위해 생성된 방화벽 규칙을 수동으로 삭제해야 합니다. 방화벽 규칙은 자동으로 삭제되지 않습니다.

단계

1. Unified Manager를 제거하려는 서버에 루트 사용자로 로그인합니다.
2. 서버에서 Unified Manager를 중지하고 제거합니다.

```
rpm -e netapp-um
```

이 단계에서는 관련된 모든 NetApp RPM 패키지가 제거됩니다. Java, MySQL, p7zip 등의 필수 소프트웨어 모듈은 제거되지 않습니다.

3. 선택 사항: 해당되는 경우 Java, MySQL, p7zip 등의 지원 소프트웨어 모듈을 제거합니다.

```
rpm -e p7zip mysql-community-client mysql-community-server mysql-community-common mysql-community-libs java-x.y
```

이 작업이 완료되면 소프트웨어가 제거됩니다. 모든 데이터는 /opt/netapp/data 디렉토리가 다음으로 이동되었습니다. /opt/netapp/data/BACKUP 제거 후 폴더. Unified Manager를 제거하면 시스템의 다른 애플리케이션에서 필요하고 사용되는 경우가 아니면 Java 및 MySQL 패키지도 제거됩니다. 하지만 MySQL 데이터는 삭제되지 않습니다.

사용자 정의 **umadmin** 사용자 및 유지 관리 그룹 제거

Unified Manager를 설치하기 전에 사용자 정의 홈 디렉토리를 만들어 고유한 umadmin 사용자 및 유지 관리 계정을 정의한 경우 Unified Manager를 제거한 후 이러한 항목을 제거해야 합니다.

표준 Unified Manager 제거에서는 사용자 정의 umadmin 사용자와 유지 관리 계정이 제거되지 않습니다. 이러한 항목은 수동으로 삭제해야 합니다.

단계

1. Red Hat Enterprise Linux 서버에 루트 사용자로 로그인합니다.
2. umadmin 사용자를 삭제합니다.

```
userdel umadmin
```

3. 유지 관리 그룹을 삭제합니다.

```
groupdel maintenance
```

Windows 시스템에 Unified Manager 설치

Active IQ Unified Manager 소개

Active IQ Unified Manager (이전 OnCommand Unified Manager)를 사용하면 단일 인터페이스에서 ONTAP 스토리지 시스템의 상태와 성능을 모니터링하고 관리할 수 있습니다. Linux 서버, Windows 서버 또는 VMware 호스트의 가상 어플라이언스에 Unified Manager를 배포할 수 있습니다.

설치를 완료하고 관리하려는 클러스터를 추가하면 Unified Manager는 모니터링되는 스토리지 시스템의 용량, 가용성, 보호 및 성능 상태를 표시하는 그래픽 인터페이스를 제공합니다.

관련 정보

["NetApp 상호 운용성 매트릭스 도구"](#)

Unified Manager 서버가 수행하는 작업

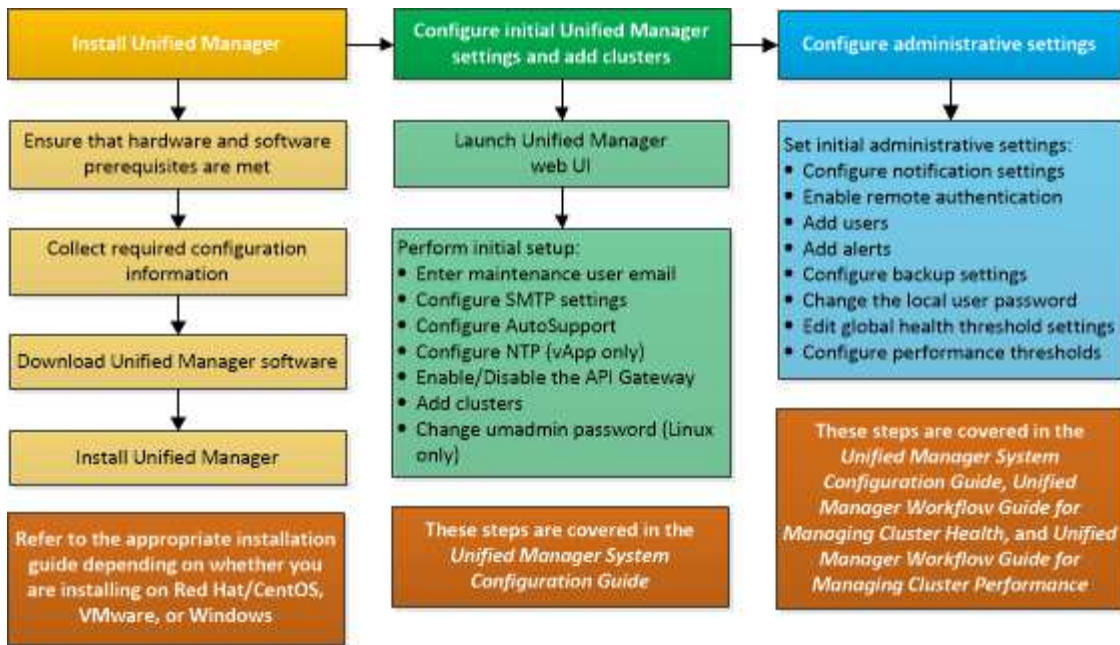
Unified Manager 서버 인프라는 데이터 수집 장치, 데이터베이스, 애플리케이션 서버로 구성됩니다. 검색, 모니터링, 역할 기반 액세스 제어(RBAC), 감사, 로깅 등의 인프라 서비스를 제공합니다.

Unified Manager는 클러스터 정보를 수집하고, 해당 데이터를 데이터베이스에 저장하고, 데이터를 분석하여 클러스터에 문제가 있는지 확인합니다.

설치 순서 개요

설치 워크플로는 Unified Manager를 사용하기 전에 수행해야 하는 작업을 설명합니다.

이 섹션에서는 아래 워크플로에 표시된 각 항목을 설명합니다.



Unified Manager 설치 요구 사항

설치 과정을 시작하기 전에 Unified Manager를 설치하려는 서버가 특정 소프트웨어, 하드웨어, CPU 및 메모리 요구 사항을 충족하는지 확인하세요.

NetApp Unified Manager 애플리케이션 코드의 수정을 지원하지 않습니다. Unified Manager 서버에 보안 조치를 적용해야 하는 경우 Unified Manager가 설치된 운영 체제를 변경해야 합니다.

Unified Manager 서버에 보안 조치를 적용하는 방법에 대한 자세한 내용은 기술 자료 문서를 참조하세요.

["Clustered Data ONTAP 용 Active IQ Unified Manager 에 적용된 보안 조치에 대한 지원 가능성"](#)

관련 정보

["NetApp 상호 운용성 매트릭스 도구"](#)

가상 인프라 및 하드웨어 시스템 요구 사항

가상 인프라나 물리적 시스템에 Unified Manager를 설치하려면 메모리, CPU, 디스크 공간에 대한 최소 요구 사항을 충족해야 합니다.

다음 표는 메모리, CPU, 디스크 공간 리소스에 권장되는 값을 보여줍니다. 이러한 값은 Unified Manager가 허용 가능한 성능 수준을 충족하도록 검증되었습니다.

하드웨어 구성	권장 설정
숫양	12GB(최소 요구 사항 8GB)
프로세서	4개의 CPU

하드웨어 구성	권장 설정
CPU 사이클 용량	총 9572MHz(최소 요구 사항 9572MHz)
디스크 여유 공간	150GB, 용량은 다음과 같이 할당됩니다. • 설치 디렉토리를 위한 100GB의 디스크 공간 • MySQL 데이터 디렉토리를 위한 50GB 디스크 공간

Unified Manager는 메모리 용량이 적은 시스템에도 설치할 수 있지만, 권장하는 12GB RAM을 사용하면 최적의 성능을 위해 충분한 메모리를 확보할 수 있으며, 구성이 커짐에 따라 시스템이 추가 클러스터와 스토리지 개체를 수용할 수 있습니다. Unified Manager가 배포된 VM에 메모리 제한을 설정해서는 안 되며, 소프트웨어가 시스템에 할당된 메모리를 활용하는 것을 방해하는 기능(예: 벌루닝)을 활성화해서는 안 됩니다.

또한 Unified Manager의 두 번째 인스턴스를 설치하기 전에 Unified Manager의 단일 인스턴스가 모니터링할 수 있는 노드 수에는 제한이 있습니다. 자세한 내용은 [_모범 사례 가이드_](#)를 참조하세요.

"기술 보고서 4621: Unified Manager 모범 사례 가이드"

메모리 페이지 스와핑은 시스템과 관리 애플리케이션의 성능에 부정적인 영향을 미칩니다. 전반적인 호스트 활용으로 인해 사용할 수 없는 CPU 리소스를 놓고 경쟁하면 성능이 저하될 수 있습니다.

전용 사용에 대한 요구 사항

Unified Manager를 설치하는 물리적 또는 가상 시스템은 Unified Manager에만 사용해야 하며 다른 애플리케이션과 공유해서는 안 됩니다. 다른 애플리케이션이 시스템 리소스를 소모하여 Unified Manager의 성능을 크게 저하시킬 수 있습니다.

백업을 위한 공간 요구 사항

Unified Manager 백업 및 복원 기능을 사용하려면 “data” 디렉터리나 디스크에 150GB의 공간을 확보하도록 추가 용량을 할당하세요. 백업은 로컬 대상이나 원격 대상에 기록될 수 있습니다. 가장 좋은 방법은 Unified Manager 호스트 시스템 외부에 있으며 최소 150GB의 공간이 있는 원격 위치를 식별하는 것입니다.

호스트 연결 요구 사항

Unified Manager를 설치하는 물리적 시스템이나 가상 시스템은 성공적으로 다음을 수행할 수 있도록 구성되어야 합니다. ping 호스트 자체의 호스트 이름입니다. IPv6 구성의 경우 다음 사항을 확인해야 합니다. ping6 Unified Manager 설치가 성공적으로 이루어지도록 호스트 이름이 성공적으로 지정되었습니다.

호스트 이름(또는 호스트 IP 주소)을 사용하여 제품 웹 UI에 액세스할 수 있습니다. 배포 중에 네트워크에 대한 정적 IP 주소를 구성한 경우 네트워크 호스트에 대한 이름을 지정했습니다. DHCP를 사용하여 네트워크를 구성한 경우 DNS에서 호스트 이름을 얻어야 합니다.

정규화된 도메인 이름(FQDN)이나 IP 주소 대신 짧은 이름을 사용하여 사용자가 Unified Manager에 액세스하도록 허용하려는 경우 네트워크 구성에서 이 짧은 이름을 유효한 FQDN으로 확인해야 합니다.

Windows 소프트웨어 및 설치 요구 사항

Windows에 Unified Manager를 성공적으로 설치하려면 Unified Manager를 설치하는

시스템이 소프트웨어 요구 사항을 충족하는지 확인해야 합니다.

운영 체제 소프트웨어

다음 Windows 버전에 Unified Manager를 설치할 수 있습니다.

- Microsoft Windows Server 2019 Standard 및 Datacenter Edition
- Microsoft Windows Server 2022 Standard 및 Datacenter Edition

Unified Manager는 다음 언어에 대해 64비트 Windows 운영 체제에서 지원됩니다.

- 영어
- 일본어
- 간체 중국어

지원되는 Windows 버전의 전체 및 최신 목록은 상호 운용성 매트릭스를 참조하세요.

["mysupport.netapp.com/매트릭스"](https://mysupport.netapp.com/매트릭스)



NetApp Microsoft System Center Configuration Manager(SCCM)와 같은 타사 도구를 사용하여 Unified Manager를 설치하는 것을 지원하지 않습니다.

서버는 Unified Manager를 실행하는 데 전용되어야 합니다. 서버에 다른 애플리케이션을 설치하면 안 됩니다. 회사 규정으로 인해 Windows 시스템에 활성 바이러스 백신 소프트웨어가 설치되어 있을 수 있습니다. Unified Manager를 설치하기 전에 바이러스 백신 소프트웨어를 비활성화하여 설치 실패를 방지하세요.

타사 소프트웨어

Unified Manager에는 다음과 같은 타사 패키지가 포함되어 있습니다. 이러한 타사 패키지가 시스템에 설치되어 있지 않으면 Unified Manager가 설치의 일부로 이를 설치합니다.

- Visual Studio 2015 버전 14.26.28720.3용 Microsoft Visual C 재배포 가능 패키지
- MySQL 커뮤니티 에디션 버전 8.4.4
- 파이썬 3.12.4
- OpenJDK 버전 11.0.25
- 7-zip 버전 23.01 이상



Unified Manager 9.5부터 OpenJDK가 Unified Manager 설치 패키지에 포함되어 자동으로 설치됩니다. Unified Manager 9.5부터 Oracle Java가 지원되지 않습니다.

MySQL이 사전 설치된 경우 다음 사항을 확인해야 합니다.

- 기본 포트를 사용하고 있습니다.
- 샘플 데이터베이스가 설치되지 않았습니다.
- 서비스 이름은 "MYSQL84"입니다.

Unified Manager는 WildFly 웹 서버에 배포됩니다. WildFly 26.1.3은 Unified Manager와 함께 번들로 제공됩니다.



타사 소프트웨어를 업그레이드하기 전에 실행 중인 Unified Manager 인스턴스를 종료해야 합니다. 타사 소프트웨어 설치가 완료되면 Unified Manager를 다시 시작할 수 있습니다.

설치 요구 사항

- Microsoft .NET 4.5.2 이상이 설치되어 있어야 합니다.
- 그만큼 temp 설치 파일을 추출하려면 디렉토리에 2GB의 디스크 공간을 구성해야 합니다. 디렉토리가 생성되었는지 확인하려면 명령줄 인터페이스에서 다음 명령을 실행하세요. `echo %temp%`
- Unified Manager MSI 파일을 캐싱하기 위해 Windows 드라이브에 2GB의 디스크 공간을 예약해야 합니다.
- Unified Manager를 설치하려는 Microsoft Windows Server는 다음과 같이 정규화된 도메인 이름(FQDN)으로 구성되어야 합니다. ping 호스트 이름과 FQDN에 대한 응답이 성공적입니다.
- Microsoft IIS 월드와이드 웹 게시 서비스를 비활성화하고 포트 80과 443이 사용 가능한지 확인해야 합니다.
- 설치하는 동안 "Windows Installer RDS 호환성"에 대한 원격 데스크톱 세션 호스트 설정이 비활성화되어 있는지 확인해야 합니다.
- UDP 포트 514는 비어 있어야 하며 다른 서비스에서 사용되어서는 안 됩니다.
- Unified Manager를 설치하기 전에 시스템의 모든 바이러스 백신 소프트웨어를 비활성화해야 합니다. 설치가 완료되면 다음 경로를 바이러스 백신 검사에서 수동으로 제외하세요.
 - 예를 들어 Unified Manager 데이터 디렉토리 `C:\ProgramData\NetApp\OnCommandAppData\`
 - Unified Manager 설치 디렉토리(예: `\C:\Program Files\NetApp\`)
 - 예를 들어 MySQL 데이터 디렉토리 `C:\ProgramData\MySQL\MySQLServerData`

지원되는 브라우저

Unified Manager 웹 UI에 액세스하려면 지원되는 브라우저를 사용하세요.

상호 운용성 매트릭스에는 지원되는 브라우저 버전 목록이 있습니다.

mysupport.netapp.com/매트릭스

모든 브라우저에서 팝업 차단 기능을 비활성화하면 소프트웨어 기능이 제대로 표시됩니다.

SAML 인증을 위해 Unified Manager를 구성하여 ID 공급자(IdP)가 사용자를 인증할 수 있도록 계획하는 경우 IdP에서 지원하는 브라우저 목록도 확인해야 합니다.

프로토콜 및 포트 요구 사항

필요한 포트와 프로토콜은 Unified Manager 서버와 관리되는 스토리지 시스템, 서버 및 기타 구성 요소 간의 통신을 가능하게 합니다.

Unified Manager 서버에 대한 연결

일반적인 설치에서는 Unified Manager 웹 UI에 연결할 때 포트 번호를 지정할 필요가 없습니다. 기본 포트가 항상 사용되기 때문입니다. 예를 들어 Unified Manager는 항상 기본 포트에서 실행하려고 하기 때문에 다음을 입력할 수

있습니다. `https://<host>` 대신에 `https://<host>:443`.

Unified Manager 서버는 다음 인터페이스에 액세스하기 위해 특정 프로토콜을 사용합니다.

인터페이스	규약	포트	설명
Unified Manager 웹 UI	HTTP	80	Unified Manager 웹 UI에 액세스하는 데 사용되며, 자동으로 보안 포트 443으로 리디렉션됩니다.
API를 사용한 Unified Manager 웹 UI 및 프로그램	HTTPS	443	Unified Manager 웹 UI에 안전하게 액세스하거나 API 호출을 하는 데 사용됩니다. API 호출은 HTTPS를 사용해서만 이루어질 수 있습니다.
유지 관리 콘솔	SSH/SFTP	22	유지 관리 콘솔에 액세스하고 지원 번들을 검색하는 데 사용됩니다.
리눅스 명령줄	SSH/SFTP	22	Red Hat Enterprise Linux 명령줄에 액세스하고 지원 번들을 검색하는 데 사용됩니다.
시스템 로그	UDP	514	ONTAP 시스템에서 구독 기반 EMS 메시지에 액세스하고 메시지를 기반으로 이벤트를 생성하는 데 사용됩니다.
나머지	HTTPS	9443	인증된 ONTAP 시스템에서 실시간 REST API 기반 EMS 이벤트에 액세스하는 데 사용됩니다.
MySQL 데이터베이스	MySQL	3306	Unified Manager에 대한 OnCommand Workflow Automation 및 OnCommand API 서비스 액세스를 활성화하는 데 사용됩니다.
AMQP QPID 브로커	TCP/IP	56072	내부 메시지 통신에 사용됩니다.

인터페이스	규약	포트	설명
AMQP QPID 브로커	TCP를 통한 웹소켓	56080	ONTAP (클라우드 에이전트)에서 수신된 메시지를 이 포트에서 수신하는 데 사용됩니다.
AMQP QPID 브로커	TCP를 통한 웹소켓	56443	ONTAP (클라우드 에이전트)에서 수신된 메시지를 이 포트에서 수신하는 데 사용됩니다. 이 포트를 통한 통신은 TLS 또는 SSL에서 제공하는 암호화를 지원합니다.



Windows 시스템에 Unified Manager를 설치하는 동안 MySQL의 기본 포트인 3306은 localhost로만 제한됩니다. 설치가 완료되면 방화벽을 활성화하여 MySQL 포트 3306에 대한 액세스를 제한합니다. 이는 이전 구성이 유지되는 모든 업그레이드 시나리오에 영향을 미치지 않습니다. 이 구성은 수정될 수 있으며 다음을 사용하여 다른 호스트에서 연결을 사용할 수 있습니다. `Control access to MySQL port 3306` 유지 관리 콘솔의 옵션입니다. 자세한 내용은 다음을 참조하세요. ["추가 메뉴 옵션"](#). HTTP 및 HTTPS 통신에 사용되는 포트(포트 80 및 443)는 Unified Manager 유지 관리 콘솔을 사용하여 변경할 수 있습니다. 자세한 내용은 다음을 참조하세요. ["Active IQ Unified Manager 구성"](#).

Unified Manager 서버에서의 연결

Unified Manager 서버와 관리형 스토리지 시스템, 서버 및 기타 구성 요소 간의 통신을 가능하게 하는 포트를 열도록 방화벽을 구성해야 합니다. 포트가 열려 있지 않으면 통신이 실패합니다.

환경에 따라 Unified Manager 서버가 특정 대상에 연결하는 데 사용하는 포트와 프로토콜을 수정할 수 있습니다.

Unified Manager 서버는 다음 프로토콜과 포트를 사용하여 관리되는 스토리지 시스템, 서버 및 기타 구성 요소에 연결합니다.

목적지	규약	포트	설명
저장 시스템	HTTPS	443/TCP	저장 시스템을 모니터링하고 관리하는 데 사용됩니다.
저장 시스템	NDMP	10000/TCP	특정 스냅샷 복원 작업에 사용됩니다.
AutoSupport 서버	HTTPS	443	AutoSupport 정보를 전송하는 데 사용됩니다. 이 기능을 수행하려면 인터넷 접속이 필요합니다.
인증 서버	LDAP	389	인증 요청, 사용자 및 그룹 조회 요청을 하는 데 사용됩니다.

목적지	규약	포트	설명
LDAPS	636	보안 LDAP 통신에 사용됩니다.	메일 서버
SMTP	25	경고 알림 이메일을 보내는 데 사용됩니다.	SNMP 트랩 발신자
SNMPv1 또는 SNMPv3	162/UDP	SNMP 트랩에 대한 경고 알림을 보내는 데 사용됩니다.	외부 데이터 공급자 서버
TCP	2003	Graphite와 같은 외부 데이터 공급자에게 성능 데이터를 전송하는 데 사용됩니다.	NTP 서버
엔티피	123/UDP	Unified Manager 서버의 시간을 외부 NTP 시간 서버와 동기화하는 데 사용됩니다. (VMware 시스템에만 해당)	AMQP QPID 브로커
TCP/IP	56072	내부 메시지 통신에 사용됩니다.	AMQP QPID 브로커
TCP를 통한 웹소켓	56080	ONTAP (클라우드 에이전트)에서 수신된 메시지를 이 포트에서 수신하는 데 사용됩니다.	AMQP QPID 브로커
TCP를 통한 웹소켓	56443	ONTAP (클라우드 에이전트)에서 수신된 메시지를 이 포트에서 수신하는 데 사용됩니다. 이 포트를 통한 통신은 TLS 또는 SSL에서 제공하는 암호화를 지원합니다.	시스템 로그

워크시트를 완성하세요

Unified Manager를 설치하고 구성하기 전에 해당 환경에 대한 구체적인 정보를 쉽게 사용할 수 있어야 합니다. 워크시트에 정보를 기록할 수 있습니다.

Unified Manager 설치 정보

Unified Manager를 설치하는 데 필요한 세부 정보입니다.

소프트웨어가 배포되는 시스템	당신의 가치
호스트 정규화된 도메인 이름	
호스트 IP 주소	
네트워크 마스크	
게이트웨이 IP 주소	
기본 DNS 주소	
보조 DNS 주소	
도메인 검색	
유지 관리 사용자 이름	
유지관리 사용자 비밀번호	

Unified Manager 구성 정보

설치 후 Unified Manager를 구성하는 방법에 대한 세부 정보입니다. 일부 값은 구성에 따라 선택 사항입니다.

환경	당신의 가치
유지관리 사용자 이메일 주소	
SMTP 서버 호스트 이름 또는 IP 주소	
SMTP 사용자 이름	
SMTP 비밀번호	
SMTP 포트	25 (기본값)
알림이 전송되는 이메일	
인증 서버 호스트 이름 또는 IP 주소	
Active Directory 관리자 이름 또는 LDAP 바인딩 고유 이름	
Active Directory 암호 또는 LDAP 바인딩 암호	

환경	당신의 가치
인증 서버 기반 고유 이름	
ID 공급자(IdP) URL	
ID 공급자(IdP) 메타데이터	
SNMP 트랩 대상 호스트 IP 주소	
SNMP 포트	

클러스터 정보

Unified Manager를 사용하여 관리하는 스토리지 시스템에 대한 세부 정보입니다.

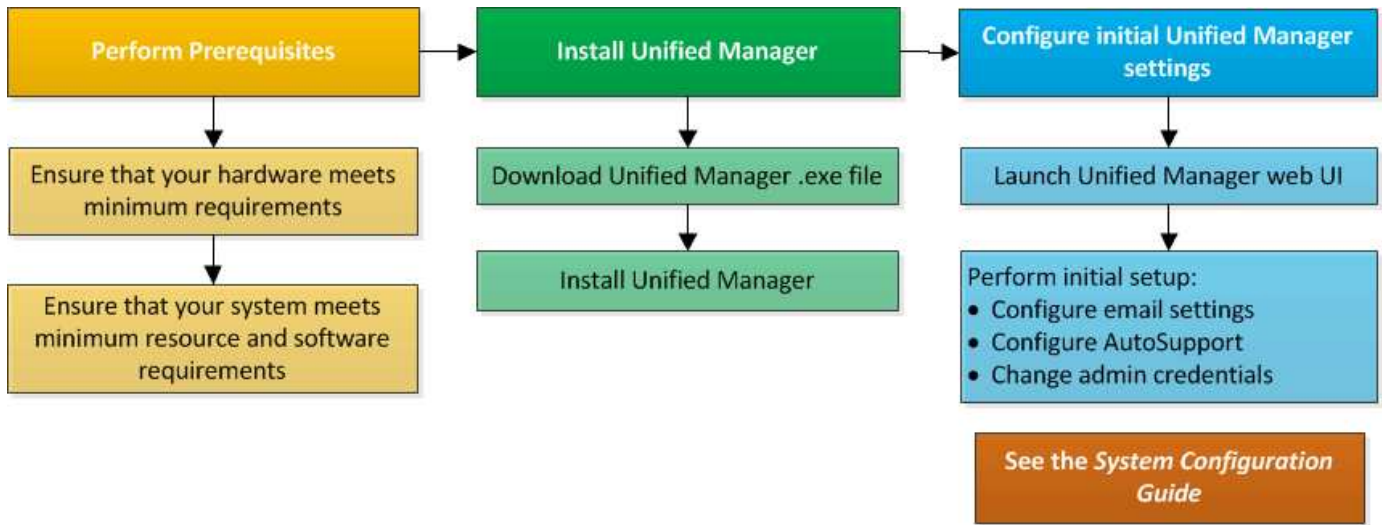
N의 클러스터 1	당신의 가치
호스트 이름 또는 클러스터 관리 IP 주소	
ONTAP 관리자 사용자 이름  관리자에게 “admin” 역할이 할당되어야 합니다.	
ONTAP 관리자 비밀번호	
규약	HTTPS

Unified Manager 소프트웨어 설치, 업그레이드 및 제거

Unified Manager를 설치하고, 최신 버전으로 업그레이드하거나, Unified Manager 애플리케이션을 제거할 수 있습니다.

설치 과정 개요

설치 워크플로는 Unified Manager를 사용하기 전에 수행해야 하는 작업을 설명합니다.



Windows에 Unified Manager 설치

Windows에 Unified Manager를 다운로드하고 설치하는 단계 순서를 이해하는 것이 중요합니다.

Unified Manager 설치

Unified Manager를 설치하면 데이터 저장 용량, 가용성, 성능 및 보호 문제를 모니터링하고 해결할 수 있습니다.

시작하기 전에

- Unified Manager를 설치하려는 시스템은 시스템 및 소프트웨어 요구 사항을 충족해야 합니다.

보다"하드웨어 시스템 요구 사항".

보다"Windows 소프트웨어 및 설치 요구 사항".



Unified Manager 9.5부터 OpenJDK가 설치 패키지에 포함되어 자동으로 설치됩니다. Unified Manager 9.5부터 Oracle Java가 지원되지 않습니다.

- Windows 관리자 권한이 있어야 합니다. 사용자 이름이 느낌표 “로 시작하지 않는지 확인하세요!”. Installation of Unified Manager might fail if the user name of user running the installation begins with " !".
- ASA r2 시스템을 제외한 모든 클러스터가 지원됩니다.
- 지원되는 웹 브라우저가 있어야 합니다.
- Unified Manager 유지 관리 사용자 비밀번호는 8~20자여야 하며 대문자 또는 소문자, 숫자, 특수문자를 포함해야 합니다.
- 유지 관리 사용자 또는 MySQL 루트 사용자의 비밀번호 문자열에는 다음 특수 문자가 허용되지 않습니다. " ' ` % , = & < > | ^ \ / () [] ; :

다음과 같은 특수 문자가 허용됩니다: ~ ! @ # \$ % ^ & * - ? . , + { }

단계

1. 기본 로컬 관리자 계정을 사용하여 Windows에 로그인합니다.

2. NetApp 지원 사이트에 로그인하고 Unified Manager 다운로드 페이지로 이동합니다.

["NetApp 지원 사이트"](#)

3. 필요한 Unified Manager 버전을 선택하고 최종 사용자 라이선스 계약(EULA)에 동의합니다.

4. Unified Manager Windows 설치 파일이나 zip 파일을 Windows 시스템의 대상 디렉토리에 다운로드합니다.

5. 필요한 경우 zip 파일을 추출하고 설치 파일이 있는 디렉토리로 이동합니다.

6. Unified Manager 설치 프로그램 실행 파일(.exe)을 마우스 오른쪽 버튼으로 클릭하고 관리자 권한으로 실행합니다.

Unified Manager는 누락되었거나 사전 설치된 타사 패키지를 감지하여 나열합니다. 필요한 타사 패키지가 시스템에 설치되어 있지 않으면 Unified Manager가 설치의 일부로 해당 패키지를 설치합니다.

7. *다음*을 클릭하세요.

8. 유지 관리 사용자를 생성하려면 사용자 이름과 비밀번호를 입력하세요.

9. 데이터베이스 연결 마법사에서 MySQL 루트 비밀번호를 입력합니다.

10. *변경*을 클릭하여 Unified Manager 설치 디렉터리와 MySQL 데이터 디렉터리의 새 위치를 지정합니다.

설치 디렉토리를 변경하지 않으면 Unified Manager가 기본 설치 디렉토리에 설치됩니다.

11. *다음*을 클릭하세요.

12. Shield 설치 준비 마법사에서 *설치*를 클릭합니다.

13. 설치가 완료되면 *마침*을 클릭하세요.

14. Windows 시스템에 활성 바이러스 백신 소프트웨어가 설치되어 있는 경우, 설치가 완료된 후 바이러스 백신 검사에서 다음 경로를 수동으로 제외하세요.

- Unified Manager 데이터 디렉토리
- Unified Manager 설치 디렉토리
- MySQL 데이터 디렉토리

설치하면 여러 개의 디렉토리가 생성됩니다.

- 설치 디렉토리

이는 설치 중에 지정한 Unified Manager의 루트 디렉토리입니다. 예: C:\Program Files\NetApp\

- MySQL 데이터 디렉토리

이는 MySQL 데이터베이스가 저장되는 디렉토리로, 설치 중에 지정했습니다. 예:

C:\ProgramData\MySQL\MySQLServerData\

- 자바 디렉토리

이는 OpenJDK가 설치된 디렉토리입니다. 예: C:\Program Files\NetApp\JDK\

- Unified Manager 애플리케이션 데이터 디렉터리(appDataDir)

이는 모든 애플리케이션 생성 데이터가 저장되는 디렉토리입니다. 여기에는 로그, 지원 번들, 백업 및 기타 모든 추가

데이터가 포함됩니다. 예: C:\ProgramData\NetApp\OnCommandAppData\

Unified Manager의 초기 설정을 수행하려면 웹 UI에 액세스할 수 있습니다. ["Active IQ Unified Manager 구성"](#).

Unified Manager의 무인 설치 수행

명령줄 인터페이스를 사용하면 사용자 개입 없이 Unified Manager를 설치할 수 있습니다. 키-값 쌍으로 매개변수를 전달하여 무인 설치를 완료할 수 있습니다.

단계

1. 기본 로컬 관리자 계정을 사용하여 Windows 명령줄 인터페이스에 로그인합니다.
2. Unified Manager를 설치할 위치로 이동하고 다음 옵션 중 하나를 선택하세요.

옵션	지침
타사 패키지가 사전 설치된 경우	<pre>ActiveIQUnifiedManager-x.y.exe /v"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_passw ord MAINTENANCE_USERNAME=maintenance_usern ame /qn /l*v CompletePathForLogFile"</pre> 예: <pre>ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR=\"C:\Program Files\NetApp\" MYSQL_DATA_DIR=\"C:\ProgramData\MySQL\ MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qn /l*v C:\install.log"</pre>

옵션	지침
타사 패키지가 설치되지 않은 경우	<pre>ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_passw ord MAINTENANCE_USERNAME=maintenance_usern ame /qr /l*v CompletePathForLogFile"</pre> 예: <pre>ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR=\"C:\Program Files\NetApp\" MYSQL_DATA_DIR=\"C:\ProgramData\MYSQL\ MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qr /l*v C:\install.log"</pre>

그만큼 /qr 이 옵션을 선택하면 사용자 인터페이스가 축소된 조용한 모드가 활성화됩니다. 설치 진행 상황을 보여주는 기본 사용자 인터페이스가 표시됩니다. 입력하라는 메시지가 표시되지 않습니다. JRE, MySQL, 7zip 등의 타사 패키지가 사전 설치되어 있지 않은 경우 다음을 사용해야 합니다. /qr 옵션. 설치가 실패하면 /qn 이 옵션은 타사 패키지가 설치되지 않은 서버에서 사용됩니다.

그만큼 /qn 이 옵션을 사용하면 사용자 인터페이스 없이 조용한 모드를 사용할 수 있습니다. 설치 중에는 사용자 인터페이스나 세부 정보가 표시되지 않습니다. 당신은 사용해서는 안됩니다 /qn 타사 패키지가 설치되지 않은 경우의 옵션입니다.

3. 다음 URL을 사용하여 Unified Manager 웹 사용자 인터페이스에 로그인하세요.

`https://IP address`

JBoss 비밀번호 변경

설치 중에 설정된 인스턴스별 JBoss 비밀번호를 재설정할 수 있습니다. 사이트에 Unified Manager 설치 설정을 재정의하기 위해 이 보안 기능이 필요한 경우 선택적으로 비밀번호를 재설정할 수 있습니다. 이 작업은 JBoss가 MySQL에 액세스하는 데 사용하는 비밀번호도 변경합니다.

시작하기 전에

- Unified Manager가 설치된 시스템에 대한 Windows 관리자 권한이 있어야 합니다.
- MySQL 루트 사용자의 비밀번호가 있어야 합니다.
- NetApp 에서 제공하는 서비스에 액세스할 수 있어야 합니다. password.bat 디렉토리의 스크립트

`C:\Program Files\NetApp\essentials\bin.`

단계

1. Unified Manager 호스트 컴퓨터에서 관리자 사용자로 로그인합니다.
2. Windows 서비스 콘솔을 사용하여 다음 Unified Manager 서비스를 중지합니다.
 - NetApp Active IQ 인수 서비스(Ocie-au)
 - NetApp Active IQ 관리 서버 서비스(Oncommandsvc)
3. 시작하다 password.bat 비밀번호 변경 프로세스를 시작하는 스크립트:

```
C:\Program Files\NetApp\essentials\bin> password.bat resetJBossPassword
```

4. 메시지가 표시되면 MySQL 루트 사용자 비밀번호를 입력합니다.
5. 메시지가 표시되면 새로운 JBoss 사용자 비밀번호를 입력한 다음 확인을 위해 다시 한 번 입력합니다.

비밀번호는 8~16자여야 하며, 숫자, 대문자, 소문자, 그리고 다음 특수 문자 중 하나 이상을 포함해야 합니다.

```
!@%^*-_=[ ]:<>./~/+
```

6. 스크립트가 완료되면 Windows 서비스 콘솔을 사용하여 Unified Manager 서비스를 시작합니다.
 - NetApp Active IQ 관리 서버 서비스(Oncommandsvc)
 - NetApp Active IQ 인수 서비스(Ocie-au)
7. 모든 서비스가 시작된 후 Unified Manager UI에 로그인할 수 있습니다.

Unified Manager 버전에 지원되는 업그레이드 경로

Active IQ Unified Manager 각 버전에 대해 특정 업그레이드 경로를 지원합니다.

Unified Manager의 일부 버전은 이후 버전으로의 내부 업그레이드를 수행할 수 없습니다. Unified Manager 업그레이드는 N-2 모델로 제한됩니다. 즉, 모든 플랫폼에서 다음 2개 릴리스 내에서만 업그레이드를 수행할 수 있습니다. 예를 들어 Unified Manager 9.13 및 9.14에서만 Unified Manager 9.16로 업그레이드할 수 있습니다.

지원되는 버전보다 이전 버전을 실행 중인 경우 Unified Manager 인스턴스를 먼저 지원되는 버전 중 하나로 업그레이드한 다음, 현재 버전으로 업그레이드해야 합니다.

예를 들어, 설치된 버전이 Unified Manager 9.9이고 Unified Manager 9.14로 업그레이드하려는 경우 업그레이드 순서를 따르면 됩니다.

업그레이드 경로 샘플:

1. 9.11 → 9.13으로 업그레이드
2. 9.13 → 9.14로 업그레이드
3. 9.13 → 9.16으로 업그레이드
4. 9.14 → 9.16으로 업그레이드

업그레이드 경로 매트릭스에 대한 자세한 내용은 다음을 참조하세요. ["지식 기반\(KB\) 문서"](#).

Unified Manager 업그레이드

Windows 플랫폼에서 설치 파일을 다운로드하여 실행하면 Unified Manager 9.13 또는 9.14을 9.16로 업그레이드할 수 있습니다.

시작하기 전에

- Unified Manager를 업그레이드하는 시스템은 시스템 및 소프트웨어 요구 사항을 충족해야 합니다.

보다"[하드웨어 시스템 요구 사항](#)".

보다"[Windows 소프트웨어 및 설치 요구 사항](#)".



Unified Manager 9.5부터 OpenJDK가 설치 패키지에 포함되어 자동으로 설치됩니다. Unified Manager 9.5부터 Oracle Java가 지원되지 않습니다.



업그레이드를 시작하기 전에 Microsoft .NET 4.5.2 이상이 시스템에 설치되어 있는지 확인하세요.

- MySQL Community Edition은 Unified Manager 업그레이드 중에 자동으로 업그레이드됩니다. 시스템에 설치된 MySQL 버전이 8.4.4 이전인 경우 Unified Manager 업그레이드 프로세스는 자동으로 MySQL을 8.4.4로 업그레이드합니다. 이전 버전의 MySQL을 8.4.4로 독립 실행형 업그레이드를 실행해서는 안 됩니다.
- ASA r2 시스템을 제외한 모든 클러스터가 지원됩니다.
- Windows 관리자 권한이 있어야 합니다. 사용자 이름이 느낌표 “로 시작하지 않는지 확인하세요!”. Installation of Unified Manager might fail if the user name of user running the installation begins with " !".
- NetApp 지원 사이트에 로그인하려면 유효한 자격 증명이 있어야 합니다.
- 데이터 손실을 방지하려면 업그레이드 중에 문제가 발생할 경우를 대비해 Unified Manager 컴퓨터의 백업을 만들어야 합니다.
- 업그레이드를 수행하려면 충분한 디스크 공간이 있어야 합니다.

설치 드라이브의 사용 가능한 공간은 데이터 디렉터리 크기보다 2.5GB 더 커야 합니다. 충분한 여유 공간이 없으면 업그레이드가 중지되고 추가할 공간의 양을 알려주는 오류 메시지가 표시됩니다.

- 업그레이드하는 동안 성능 데이터를 13개월 동안 보관하는 기존 기본 설정을 유지할지, 아니면 6개월로 변경할지 묻는 메시지가 표시될 수 있습니다. 확인 후, 6개월 이후의 과거 실적 데이터는 삭제됩니다.
- 업그레이드하기 전에 <InstallDir>\JDK 및 _MySQL Data Directory_에 있는 열려 있는 파일이나 폴더를 모두 닫아야 합니다.
- Windows 시스템에 활성 바이러스 백신 소프트웨어가 설치되어 있는 경우 Unified Manager 업그레이드가 실패할 수 있습니다. Unified Manager를 업그레이드하기 전에 시스템의 모든 바이러스 검사 소프트웨어를 비활성화해야 합니다.

업그레이드 프로세스 중에는 Unified Manager를 사용할 수 없습니다. Unified Manager를 업그레이드하기 전에 실행 중인 모든 작업을 완료해야 합니다.

Unified Manager가 OnCommand Workflow Automation 인스턴스와 페어링되어 있고 두 제품 모두에 사용 가능한 소프트웨어의 새 버전이 있는 경우, 업그레이드를 수행한 후 두 제품의 연결을 해제한 다음 새 Workflow Automation 연결을 설정해야 합니다. 제품 중 하나만 업그레이드하는 경우 업그레이드 후 Workflow Automation에 로그인하여 Unified Manager에서 여전히 데이터를 수집하고 있는지 확인해야 합니다.

단계

1. NetApp 지원 사이트에 로그인하고 Unified Manager 다운로드 페이지로 이동합니다.

"NetApp 지원 사이트".

2. 필요한 Unified Manager 버전을 선택하고 최종 사용자 라이선스 계약(EULA)에 동의합니다.
3. Unified Manager Windows 설치 파일이나 zip 파일을 Windows 시스템의 대상 디렉토리에 다운로드합니다. 필요한 경우 zip 파일을 추출하고 설치 파일이 있는 디렉토리로 이동합니다. Unified Manager 설치 프로그램 실행 파일(.exe)을 마우스 오른쪽 버튼으로 클릭하고 관리자 권한으로 실행합니다.

Unified Manager에서 다음 메시지가 표시됩니다.

This setup will perform an upgrade of Unified Manager. Do you want to continue?

4. *예*를 클릭한 후, *다음*을 클릭합니다.
5. 설치 중에 설정한 MySQL84 루트 비밀번호를 입력하고 *다음*을 클릭합니다.
6. 지원되는 웹 브라우저에서 새 창으로 웹 UI를 실행하고 로그인하여 Unified Manager 업그레이드 버전을 사용하세요.
7. Windows 시스템에 활성 바이러스 백신 소프트웨어가 설치되어 있는 경우 업그레이드가 완료된 후 바이러스 백신 검사에서 다음 경로를 수동으로 제외해야 합니다.
 - Unified Manager 데이터 디렉토리
 - Unified Manager 설치 디렉토리
 - MySQL 데이터 디렉토리



Unified Manager의 자동 업그레이드를 수행하려면 다음 명령을 실행하세요.

```
ActiveIQUnifiedManager-<version>.exe /s /v"MYSQL_PASSWORD=<password>  
/qn /l*v <system_drive>:\install.log"
```

타사 제품 업그레이드

Windows 시스템에 Unified Manager를 설치하면 JRE와 같은 타사 제품을 업그레이드할 수 있습니다.

이러한 타사 제품을 개발하는 회사는 정기적으로 보안 취약점을 보고합니다. 귀하의 일정에 맞춰 이 소프트웨어의 최신 버전으로 업그레이드할 수 있습니다.

OpenJDK 업그레이드

Unified Manager가 설치된 Windows 서버에서 최신 버전의 OpenJDK로 업그레이드하면 보안 취약점에 대한 수정 사항을 얻을 수 있습니다.

시작하기 전에

Unified Manager가 설치된 시스템에 대한 Windows 관리자 권한이 있어야 합니다.

릴리스 패밀리 내에서 OpenJDK 릴리스를 업데이트할 수 있습니다. 예를 들어, OpenJDK 11.0.16에서 OpenJDK 11.0.18로 업그레이드할 수 있지만, OpenJDK 11에서 OpenJDK 12로 직접 업데이트할 수는 없습니다.

단계

1. Unified Manager 호스트 컴퓨터에서 관리자 사용자로 로그인합니다.
2. OpenJDK 사이트에서 대상 시스템에 적합한 버전의 OpenJDK(64비트)를 다운로드합니다.

예를 들어 다운로드 `jdk-11.0.18_windows-x64_bin.zip` from <https://www.oracle.com/in/java/technologies/javase/jdk11-archive-downloads.html>.



파일을 다운로드하려면 Oracle 계정이 필요합니다. Oracle 계정이 없으면 다음으로 이동하세요. "[Oracle 계정 로그인](#)" 페이지를 만들어 보세요.

3. Windows 서비스 콘솔을 사용하여 다음 Unified Manager 서비스를 중지합니다.
 - NetApp Active IQ 인수 서비스(Ocie-au)
 - NetApp Active IQ 관리 서버 서비스(Oncommandsvc)
4. 확장하다 zip 파일.
5. 결과에서 디렉토리와 파일을 복사합니다. jdk 디렉토리(예: jdk-11.0.18 Java가 설치된 위치로. 예: `C:\Program Files\NetApp\JDK\`)
6. Windows 서비스 콘솔을 사용하여 Unified Manager 서비스를 시작합니다.
 - NetApp Active IQ 관리 서버 서비스(Oncommandsvc)
 - NetApp Active IQ 인수 서비스(Ocie-au)

타사 제품 제거

Unified Manager를 업그레이드한 후 Python이나 Microsoft Visual C++ 2013과 같은 타사 제품을 제거할 수 있습니다. 이는 선택 사항입니다.

Python 제거

단계

1. 제어판*에서 *프로그램 > *프로그램 및 기능*을 선택합니다.
2. 프로그램 목록에서 Python을 선택하세요.
3. *이 프로그램 제거*를 선택하세요. 3.12를 제외한 모든 Python 버전을 제거하세요. Python 버전 3.12를 유지하세요.

Microsoft Visual C++ 2013 제거

단계

1. 제어판*에서 *프로그램 > *프로그램 및 기능*을 선택합니다.
2. 프로그램 목록에서 *Microsoft Visual C++ 2013*을 선택합니다.
3. *이 프로그램 제거*를 선택하세요.

Unified Manager를 다시 시작하세요

구성을 변경한 후에는 Unified Manager를 다시 시작해야 할 수도 있습니다.

시작하기 전에

Windows 관리자 권한이 있어야 합니다.

단계

1. 기본 로컬 관리자 계정을 사용하여 Windows에 로그인합니다.
2. Unified Manager 서비스를 중지합니다.

...로부터	다음 순서대로 서비스를 중지하세요...
명령줄	a. <code>sc stop ocie-au</code> b. <code>sc stop Oncommandsvc</code>
Microsoft 서비스 관리자	a. NetApp Active IQ 인수 서비스(Ocie-au) b. NetApp Active IQ 관리 서버 서비스(Oncommandsvc)

3. Unified Manager 서비스를 시작합니다.

...로부터	다음 순서대로 서비스를 시작하세요...
명령줄	a. <code>sc start Oncommandsvc</code> b. <code>sc start ocie-au</code>
Microsoft 서비스 관리자	a. NetApp Active IQ 관리 서버 서비스(Oncommandsvc) b. NetApp Active IQ 인수 서비스(Ocie-au)

Unified Manager 제거

프로그램 및 기능 마법사를 사용하거나 명령줄 인터페이스에서 무인 설치 제거를 수행하여 Unified Manager를 제거할 수 있습니다.

시작하기 전에

- Windows 관리자 권한이 있어야 합니다.
- 소프트웨어를 제거하기 전에 Unified Manager 서버에서 모든 클러스터(데이터 소스)를 제거해야 합니다.
- MySQL 포트 3306을 허용하거나 차단하기 위해 생성된 방화벽 규칙을 수동으로 삭제해야 합니다. 방화벽 규칙은 자동으로 삭제되지 않습니다.

단계

1. 다음 옵션 중 하나를 선택하여 Unified Manager를 제거합니다.

- 프로그램 및 기능 마법사에서 Unified Manager를 제거하는 경우 다음 단계를 수행하세요.
 - i. 제어판 > *프로그램 및 기능*으로 이동합니다.
 - ii. Active IQ Unified Manager 선택하고 *제거*를 클릭합니다.
- 명령줄에서 Unified Manager를 제거하는 경우 다음 단계를 수행하세요.
 - i. 관리자 권한으로 Windows 명령줄에 로그인합니다.
 - ii. Active IQ Unified Manager 디렉토리로 이동하여 다음 명령을 실행합니다.

```
msiexec /x {A78760DB-7EC0-4305-97DB-E4A89CDFF4E1} /qn /l*v  
%systemdrive%\UmUnInstall.log
```

서버에서 UAC(사용자 계정 컨트롤)가 활성화되어 있고 도메인 사용자로 로그인한 경우 명령줄 제거 방법을 사용해야 합니다.

Unified Manager가 시스템에서 제거되었습니다.

2. Unified Manager 제거 중에 제거되지 않은 다음의 타사 패키지와 데이터를 제거하세요.

- 타사 패키지: JRE, MySQL, Microsoft Visual C++ 2015 재배포 가능 패키지, Python 및 7zip
- Unified Manager에서 생성된 MySQL 애플리케이션 데이터
- 애플리케이션 로그 및 애플리케이션 데이터 디렉토리 내용

구성 및 관리 작업 수행

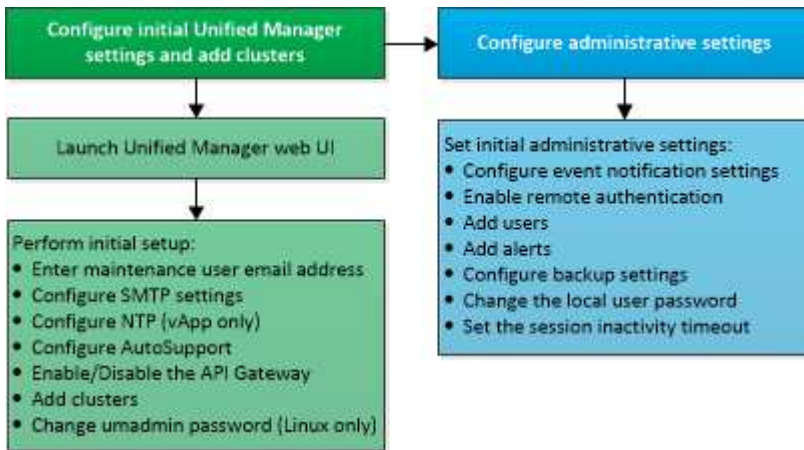
Active IQ Unified Manager 구성

Active IQ Unified Manager (이전 OnCommand Unified Manager)를 설치한 후 웹 UI에 액세스하려면 초기 설정(첫 번째 경험 마법사라고도 함)을 완료해야 합니다. 그런 다음 클러스터 추가, 원격 인증 구성, 사용자 추가, 알림 추가 등의 추가 구성 작업을 수행할 수 있습니다.

이 매뉴얼에 설명된 일부 절차는 Unified Manager 인스턴스의 초기 설정을 완료하는 데 필요합니다. 다른 절차로는 새 인스턴스에 설정하는 데 도움이 되는 권장 구성 설정이나 ONTAP 시스템의 정기 모니터링을 시작하기 전에 알아두면 좋은 내용이 있습니다.

구성 순서 개요

구성 워크플로는 Unified Manager를 사용하기 전에 수행해야 하는 작업을 설명합니다.



Unified Manager 웹 UI에 액세스하세요

Unified Manager를 설치한 후 웹 UI에 액세스하여 Unified Manager를 설정하고 ONTAP 시스템 모니터링을 시작할 수 있습니다.

시작하기 전에

- 웹 UI에 처음 접속하는 경우 유지 관리 사용자(Linux 설치의 경우 umadmin 사용자)로 로그인해야 합니다.
- 정규화된 도메인 이름(FQDN)이나 IP 주소 대신 짧은 이름을 사용하여 사용자가 Unified Manager에 액세스하도록 허용하려는 경우 네트워크 구성에서 이 짧은 이름을 유효한 FQDN으로 확인해야 합니다.
- 서버가 자체 서명된 디지털 인증서를 사용하는 경우 브라우저에 해당 인증서를 신뢰할 수 없다는 경고가 표시될 수 있습니다. 위험을 인정하고 계속 접근하거나, 서버 인증을 위해 인증 기관(CA) 서명 디지털 인증서를 설치할 수 있습니다.

단계

1. 설치가 끝나면 표시되는 URL을 사용하여 브라우저에서 Unified Manager 웹 UI를 시작합니다. URL은 Unified Manager 서버의 IP 주소 또는 정규화된 도메인 이름(FQDN)입니다.

링크 형식은 다음과 같습니다. `https://URL`.

2. 유지 관리 사용자 자격 증명을 사용하여 Unified Manager 웹 UI에 로그인합니다.



1시간 이내에 웹 UI에 로그인을 3회 연속 실패하면 시스템에서 잠기게 되며, 시스템 관리자에게 문의해야 합니다. 이는 로컬 사용자에게만 적용됩니다.

Unified Manager 웹 UI의 초기 설정을 수행합니다.

Unified Manager를 사용하려면 먼저 NTP 서버, 유지 관리 사용자 이메일 주소, SMTP 서버 호스트, ONTAP 클러스터 추가를 포함한 초기 설정 옵션을 구성해야 합니다.

시작하기 전에

다음 작업을 수행했어야 합니다.

- 설치 후 제공된 URL을 사용하여 Unified Manager 웹 UI를 시작했습니다.
- 설치 중에 생성된 유지 관리 사용자 이름 및 비밀번호(Linux 설치의 경우 umadmin 사용자)를 사용하여 로그인했습니다.

Active IQ Unified Manager 시작하기 페이지는 웹 UI에 처음 액세스할 때만 나타납니다. 아래 페이지는 VMware에 설치한 것입니다.

Active IQ Unified Manager

All

Search All Storage Objects and Actions

Getting Started

1

2

3

4

5

Email

AutoSupport

API Gateway

Add ONTAP Clusters

Finish

Notifications

Configure your email server for assistance in case you forget your password.

Maintenance User Email

Email

mgo@eng.netapp.com

SMTP Server

Host Name or IP Address

email.eng.netapp.com

Port

25

User Name

admin

Password

☐ Use STARTTLS
 [i](#)

☐ Use SSL
 [i](#)

Continue

나중에 이러한 옵션을 변경하려면 Unified Manager 왼쪽 탐색 창의 일반 옵션에서 원하는 옵션을 선택하면 됩니다. NTP 설정은 VMware 설치에만 적용되며, 나중에 Unified Manager 유지 관리 콘솔을 사용하여 변경할 수 있습니다.

단계

1. Active IQ Unified Manager 초기 설정 페이지에서 유지 관리 사용자 이메일 주소, SMTP 서버 호스트 이름 및 추가 SMTP 옵션, NTP 서버(Vmware 설치에만 해당)를 입력합니다. 그런 다음 *계속*을 클릭하세요.



STARTTLS 사용 또는 **SSL** 사용 옵션을 선택한 경우 계속 버튼을 클릭하면 인증서 페이지가 표시됩니다. 인증서 세부 정보를 확인하고 인증서를 수락하여 웹 UI의 초기 설정을 계속 진행합니다.

2. AutoSupport 페이지에서 *동의 및 계속*을 클릭하여 Unified Manager에서 NetAppActive IQ로 AutoSupport 메시지를 보내는 기능을 활성화합니다.

AutoSupport 콘텐츠를 보내기 위해 인터넷 접속을 제공하는 프록시를 지정해야 하는 경우 또는 AutoSupport 비활성화하려면 웹 UI에서 일반 > *AutoSupport* 옵션을 사용하세요.

3. Red Hat 시스템에서 umadmin 사용자 비밀번호를 기본 “admin” 문자열에서 개인화된 문자열로 변경합니다.

4. API Gateway 설정 페이지에서 ONTAP REST API를 사용하여 모니터링하려는 ONTAP 클러스터를 Unified Manager에서 관리할 수 있는 API Gateway 기능을 사용할지 여부를 선택합니다. 그런 다음 *계속*을 클릭하세요.

나중에 웹 UI에서 일반 > 기능 설정 > *API 게이트웨이*를 선택하여 이 설정을 활성화하거나 비활성화할 수 있습니다. API에 대한 자세한 내용은 다음을 참조하세요. "[Active IQ Unified Manager REST API 시작하기](#)".

5. Unified Manager에서 관리할 클러스터를 추가한 후 *다음*을 클릭합니다. 관리하려는 각 클러스터에 대해 사용자 이름과 비밀번호 자격 증명과 함께 호스트 이름 또는 클러스터 관리 IP 주소(IPv4 또는 IPv6)가 있어야 합니다. 사용자는 "admin" 역할이 있어야 합니다.

이 단계는 선택 사항입니다. 나중에 웹 UI의 저장소 관리 > *클러스터 설정*에서 클러스터를 추가할 수 있습니다.

6. 요약 페이지에서 모든 설정이 올바른지 확인하고 *마침*을 클릭합니다.

시작하기 페이지가 닫히고 Unified Manager 대시보드 페이지가 표시됩니다.

클러스터 추가

클러스터를 모니터링할 수 있도록 Active IQ Unified Manager에 클러스터를 추가할 수 있습니다. 여기에는 클러스터의 상태, 용량, 성능, 구성 등의 클러스터 정보를 얻는 기능이 포함되어 있어 발생할 수 있는 문제를 찾아 해결할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 다음 정보가 필요합니다.
 - Unified Manager는 온프레미스 ONTAP 클러스터, ONTAP Select, Cloud Volumes ONTAP 지원합니다.
 - 호스트 이름 또는 클러스터 관리 IP 주소

호스트 이름은 Unified Manager가 클러스터에 연결하는 데 사용하는 FQDN 또는 약어입니다. 호스트 이름은 클러스터 관리 IP 주소로 확인되어야 합니다.

클러스터 관리 IP 주소는 관리 스토리지 가상 머신(SVM)의 클러스터 관리 LIF여야 합니다. 노드 관리 LIF를 사용하면 작업이 실패합니다.

- 클러스터는 ONTAP 버전 9.1 이상 소프트웨어를 실행해야 합니다.
- ONTAP 관리자 사용자 이름 및 비밀번호

이 계정에는 *admin* 역할이 있어야 하며 애플리케이션 액세스 권한이 *ontapi*, *console*, *_http_*로 설정되어 있어야 합니다.

- HTTPS 프로토콜을 사용하여 클러스터에 연결할 포트 번호(일반적으로 포트 443)
- 귀하에게 필요한 인증서가 있습니다.

SSL(HTTPS) 인증서: 이 인증서는 Unified Manager의 소유입니다. Unified Manager를 새로 설치하면 기본 자체 서명 SSL(HTTPS) 인증서가 생성됩니다. NetApp 보안을 강화하기 위해 CA 서명 인증서로 업그레이드할 것을 권장합니다. 서버 인증서가 만료된 경우 인증서를 다시 생성하고 Unified Manager를 다시 시작하여 서비스에 새 인증서를 적용해야 합니다. SSL 인증서 재생성에 대한 자세한 내용은 다음을 참조하세요. "[HTTPS 보안 인증서 생성](#)".

EMS 인증서: 이 인증서는 Unified Manager의 소유입니다. ONTAP 에서 수신한 EMS 알림에 대한 인증 과정에서 사용됩니다.

상호 TLS 통신을 위한 인증서: Unified Manager와 ONTAP 간 상호 TLS 통신 중에 사용됩니다. 인증서 기반 인증은 ONTAP 버전을 기반으로 클러스터에 대해 활성화됩니다. ONTAP 버전을 실행하는 클러스터가 9.5보다 낮은 경우 인증서 기반 인증이 활성화되지 않습니다.

Unified Manager의 이전 버전을 업데이트하는 경우, 클러스터에 대해 인증서 기반 인증이 자동으로 활성화되지 않습니다. 하지만 클러스터 세부 정보를 수정하고 저장하면 해당 기능을 활성화할 수 있습니다. 인증서가 만료된 경우 새 인증서를 통합하기 위해 인증서를 다시 생성해야 합니다. 인증서 보기 및 재생성에 대한 자세한 내용은 다음을 참조하세요. "[클러스터 편집](#)".



- 웹 UI에서 클러스터를 추가할 수 있으며, 인증서 기반 인증이 자동으로 활성화됩니다.
- Unified Manager CLI를 통해 클러스터를 추가할 수 있으며, 인증서 기반 인증은 기본적으로 활성화되어 있지 않습니다. Unified Manager CLI를 사용하여 클러스터를 추가하는 경우 Unified Manager UI를 사용하여 클러스터를 편집해야 합니다. 당신은 볼 수 있습니다 "[지원되는 Unified Manager CLI 명령](#)" Unified Manager CLI를 사용하여 클러스터를 추가합니다.
- 클러스터에 대해 인증서 기반 인증이 활성화되어 있고 서버에서 Unified Manager 백업을 가져와 호스트 이름이나 IP 주소가 변경된 다른 Unified Manager 서버로 복원하는 경우 클러스터 모니터링이 실패할 수 있습니다. 실패를 방지하려면 클러스터 세부 정보를 편집하고 저장하세요. 클러스터 세부 정보 편집에 대한 자세한 내용은 다음을 참조하세요. "[클러스터 편집](#)".

+

클러스터 인증서: 이 인증서는 ONTAP 의 소유입니다. 만료된 인증서로는 Unified Manager에 클러스터를 추가할 수 없습니다. 인증서가 이미 만료된 경우 클러스터를 추가하기 전에 인증서를 다시 생성해야 합니다. 인증서 생성에 대한 정보는 지식 기반(KB) 문서를 참조하세요. "[System Manager 사용자 인터페이스에서 ONTAP 자체 서명 인증서를 갱신하는 방법](#)".

- Unified Manager 서버에 충분한 공간이 있어야 합니다. 데이터베이스 디렉터리의 공간이 90% 이상 사용된 경우 서버에 클러스터를 추가할 수 없습니다.

MetroCluster 구성의 경우 로컬 클러스터와 원격 클러스터를 모두 추가해야 하며, 클러스터를 올바르게 구성해야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *클러스터 설정*을 클릭합니다.
2. 클러스터 설정 페이지에서 *추가*를 클릭합니다.
3. 클러스터 추가 대화 상자에서 클러스터의 호스트 이름이나 IP 주소, 사용자 이름, 비밀번호, 포트 번호 등 필요한 값을 지정합니다.

클러스터 관리 IP 주소를 IPv6에서 IPv4로 또는 IPv4에서 IPv6로 변경할 수 있습니다. 다음 모니터링 주기가 완료된 후 새로운 IP 주소가 클러스터 그리드와 클러스터 구성 페이지에 반영됩니다.

4. *제출*을 클릭하세요.
5. 호스트 승인 대화 상자에서 *인증서 보기*를 클릭하여 클러스터에 대한 인증서 정보를 확인합니다.
6. *예*를 클릭하세요.

클러스터 세부 정보를 저장한 후 클러스터의 상호 TLS 통신에 대한 인증서를 볼 수 있습니다.

인증서 기반 인증이 활성화되어 있지 않으면 Unified Manager는 클러스터가 처음 추가될 때만 인증서를 확인합니다. Unified Manager는 ONTAP에 대한 각 API 호출에 대한 인증서를 확인하지 않습니다.

새 클러스터의 모든 개체가 검색된 후 Unified Manager는 지난 15일 동안의 과거 성능 데이터를 수집하기 시작합니다. 이러한 통계는 데이터 연속성 수집 기능을 사용하여 수집됩니다. 이 기능을 사용하면 클러스터가 추가된 직후부터 2주 이상에 걸친 성능 정보를 바로 확인할 수 있습니다. 데이터 연속성 수집 주기가 완료되면 기본적으로 5분마다 실시간 클러스터 성능 데이터가 수집됩니다.



15일간의 성능 데이터를 수집하는 데 CPU가 많이 사용되므로, 너무 많은 클러스터에서 동시에 데이터 연속성 수집 폴링이 실행되지 않도록 새 클러스터를 추가하는 작업을 단계적으로 수행하는 것이 좋습니다. 또한 데이터 연속성 수집 기간 동안 Unified Manager를 다시 시작하면 수집이 중단되고 누락된 기간의 성능 차트에 간격이 표시됩니다.



클러스터를 추가할 수 없다는 오류 메시지가 나타나면 두 시스템의 시계가 동기화되지 않았는지, Unified Manager HTTPS 인증서 시작 날짜가 클러스터의 날짜보다 이후인지 확인하세요. NTP나 유사한 서비스를 사용하여 시계가 동기화되었는지 확인해야 합니다.

관련 정보

["CA 서명 및 반환된 HTTPS 인증서 설치"](#)

Unified Manager를 구성하여 알림 알림을 보냅니다.

Unified Manager를 구성하여 사용자 환경에서 발생하는 이벤트에 대한 알림을 보낼 수 있습니다. 알림을 보내려면 먼저 여러 가지 Unified Manager 옵션을 구성해야 합니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

Unified Manager를 배포하고 초기 구성을 완료한 후에는 이벤트 수신에 따라 경고를 트리거하고 알림 이메일이나 SNMP 트랩을 생성하도록 환경을 구성하는 것을 고려해야 합니다.

단계

1. "이벤트 알림 설정 구성".

사용자 환경에서 특정 이벤트가 발생할 때 경고 알림을 보내려면 SMTP 서버를 구성하고 경고 알림을 보낼 이메일 주소를 제공해야 합니다. SNMP 트랩을 사용하려면 해당 옵션을 선택하고 필요한 정보를 제공하면 됩니다.

2. "원격 인증 활성화".

원격 LDAP 또는 Active Directory 사용자가 Unified Manager 인스턴스에 액세스하여 알림을 받을 수 있도록 하려면 원격 인증을 활성화해야 합니다.

3. "인증 서버 추가".

인증 서버를 추가하면 인증 서버 내의 원격 사용자가 Unified Manager에 액세스할 수 있습니다.

4. "사용자 추가".

여러 유형의 로컬 또는 원격 사용자를 추가하고 특정 역할을 할당할 수 있습니다. 알림을 만들 때 알림을 받을

사용자를 지정합니다.

5. "알림 추가".

알림을 보낼 이메일 주소를 추가하고, 알림을 받을 사용자를 추가하고, 네트워크 설정을 구성하고, 환경에 필요한 SMTP 및 SNMP 옵션을 구성한 후에 알림을 할당할 수 있습니다.

이벤트 알림 설정 구성

이벤트가 생성되거나 이벤트가 사용자에게 할당될 때 Unified Manager에서 경고 알림을 보내도록 구성할 수 있습니다. 알림을 보내는 데 사용되는 SMTP 서버를 구성하고 다양한 알림 메커니즘을 설정할 수 있습니다. 예를 들어, 알림은 이메일이나 SNMP 트랩으로 보낼 수 있습니다.

시작하기 전에

다음 정보가 필요합니다.

- 알림이 전송되는 이메일 주소

이메일 주소는 보낸 알림의 "보낸 사람" 필드에 표시됩니다. 어떤 이유로든 이메일을 전달할 수 없는 경우, 이 이메일 주소는 전달 불가 메일의 수신자로도 사용됩니다.

- SMTP 서버 호스트 이름, 서버에 액세스하기 위한 사용자 이름 및 비밀번호
- SNMP 트랩을 수신할 트랩 대상 호스트의 호스트 이름 또는 IP 주소, SNMP 버전, 아웃바운드 트랩 포트, 커뮤니티 및 기타 필수 SNMP 구성 값

여러 개의 트랩 대상을 지정하려면 각 호스트를 쉼표로 구분하세요. 이 경우 버전 및 아웃바운드 트랩 포트와 같은 다른 모든 SNMP 설정은 목록에 있는 모든 호스트에서 동일해야 합니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *알림*을 클릭합니다.
2. 알림 페이지에서 적절한 설정을 구성합니다.

참고사항:

- 보낸 사람 주소가 "ActiveIQUnifiedManager@localhost.com" 주소로 미리 입력되어 있는 경우 모든 이메일 알림이 성공적으로 전달되도록 실제로 작동하는 이메일 주소로 변경해야 합니다.
- SMTP 서버의 호스트 이름을 확인할 수 없는 경우 호스트 이름 대신 SMTP 서버의 IP 주소(IPv4 또는 IPv6)를 지정할 수 있습니다.

3. *저장*을 클릭하세요.
4. **STARTTLS** 사용 또는 **SSL** 사용 옵션을 선택한 경우 저장 버튼을 클릭하면 인증서 페이지가 표시됩니다. 인증서 세부 정보를 확인하고 인증서를 수락하여 알림 설정을 저장하세요.

인증서 세부 정보 보기 버튼을 클릭하면 인증서 세부 정보를 볼 수 있습니다. 기존 인증서가 만료된 경우 **STARTTLS** 사용 또는 **SSL** 사용 상자의 선택을 취소하고 알림 설정을 저장한 다음 **STARTTLS** 사용 또는 **SSL** 사용 상자를 다시 선택하여 새 인증서를 확인합니다.

원격 인증 활성화

Unified Manager 서버가 인증 서버와 통신할 수 있도록 원격 인증을 활성화할 수 있습니다. 인증 서버 사용자는 Unified Manager 그래픽 인터페이스에 액세스하여 저장소 개체와 데이터를 관리할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.



Unified Manager 서버는 인증 서버에 직접 연결되어야 합니다. SSSD(시스템 보안 서비스 데몬) 또는 NSLCD(이름 서비스 LDAP 캐싱 데몬)와 같은 로컬 LDAP 클라이언트를 비활성화해야 합니다.

Open LDAP 또는 Active Directory를 사용하여 원격 인증을 활성화할 수 있습니다. 원격 인증이 비활성화된 경우 원격 사용자는 Unified Manager에 액세스할 수 없습니다.

원격 인증은 LDAP 및 LDAPS(보안 LDAP)를 통해 지원됩니다. Unified Manager는 보안되지 않은 통신의 경우 기본 포트로 389를 사용하고, 보안된 통신의 경우 기본 포트로 636을 사용합니다.



사용자를 인증하는 데 사용되는 인증서는 X.509 형식을 준수해야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. 원격 인증 사용... 상자를 체크하세요.
3. 인증 서비스 필드에서 서비스 유형을 선택하고 인증 서비스를 구성합니다.

인증 유형의 경우...	다음 정보를 입력하세요...
액티브 디렉토리	• 다음 형식 중 하나로 된 인증 서버 관리자 이름: ◦ domainname\username ◦ username@domainname ◦ Bind Distinguished Name(적절한 LDAP 표기법 사용) • 관리자 비밀번호 • 기본 고유 이름(적절한 LDAP 표기법 사용)
LDAP를 엽니다	• 적절한 LDAP 표기법으로 고유 이름을 바인딩합니다. • 비밀번호 바인딩 • 기본 고유 이름

Active Directory 사용자 인증에 시간이 오래 걸리거나 시간 초과가 발생하는 경우, 인증 서버에서 응답하는 데 시간이 오래 걸리는 것일 수 있습니다. Unified Manager에서 중첩 그룹에 대한 지원을 비활성화하면 인증 시간이 줄어든 수 있습니다.

인증 서버에 대해 보안 연결 사용 옵션을 선택하면 Unified Manager는 SSL(Secure Sockets Layer) 프로토콜을 사용하여 인증 서버와 통신합니다.

4. 선택 사항: 인증 서버를 추가하고 인증을 테스트합니다.
5. *저장*을 클릭하세요.

원격 인증에서 중첩된 그룹 비활성화

원격 인증을 활성화한 경우 중첩 그룹 인증을 비활성화하여 개별 사용자만 Unified Manager에 원격으로 인증할 수 있고 그룹 구성원은 인증할 수 없도록 할 수 있습니다. Active Directory 인증 응답 시간을 개선하려면 중첩 그룹을 비활성화할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 역할이 있어야 합니다.
- 중첩 그룹을 비활성화하는 것은 Active Directory를 사용하는 경우에만 적용됩니다.

Unified Manager에서 중첩 그룹에 대한 지원을 비활성화하면 인증 시간이 줄어들 수 있습니다. 중첩된 그룹 지원이 비활성화되고 원격 그룹이 Unified Manager에 추가된 경우 개별 사용자는 Unified Manager에 인증하려면 원격 그룹의 구성원이어야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. 중첩 그룹 조회 비활성화 확인란을 선택하세요.
3. *저장*을 클릭하세요.

인증 서비스 설정

인증 서비스를 사용하면 Unified Manager에 대한 액세스 권한을 제공하기 전에 인증 서버에서 원격 사용자 또는 원격 그룹을 인증할 수 있습니다. 사전 정의된 인증 서비스(Active Directory 또는 OpenLDAP 등)를 사용하거나 고유의 인증 메커니즘을 구성하여 사용자를 인증할 수 있습니다.

시작하기 전에

- 원격 인증을 활성화해야 합니다.
- 애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. 다음 인증 서비스 중 하나를 선택하세요.

...을 선택하면	그러면 이렇게 하세요...
액티브 디렉토리	a. 관리자 이름과 비밀번호를 입력하세요. b. 인증 서버의 기본 고유 이름을 지정합니다. 예를 들어, 인증 서버의 도메인 이름이 <code>+ou@domain.com+</code>이면 기본 고유 이름은 <code>*cn=ou,dc=domain,dc=com*</code>입니다.
오픈LDAP	a. 바인드 고유 이름과 바인드 비밀번호를 입력하세요. b. 인증 서버의 기본 고유 이름을 지정합니다. 예를 들어, 인증 서버의 도메인 이름이 <code>+ou@domain.com+</code>이면 기본 고유 이름은 <code>*cn=ou,dc=domain,dc=com*</code>입니다.
기타	a. 바인드 고유 이름과 바인드 비밀번호를 입력하세요. b. 인증 서버의 기본 고유 이름을 지정합니다. 예를 들어, 인증 서버의 도메인 이름이 <code>+ou@domain.com+</code>이면 기본 고유 이름은 <code>*cn=ou,dc=domain,dc=com*</code>입니다. c. 인증 서버에서 지원하는 LDAP 프로토콜 버전을 지정합니다. d. 사용자 이름, 그룹 멤버십, 사용자 그룹 및 멤버 속성을 입력합니다.



인증 서비스를 수정하려면 기존 인증 서버를 삭제한 다음 새 인증 서버를 추가해야 합니다.

3. *저장*을 클릭하세요.

인증 서버 추가

관리 서버에서 인증 서버를 추가하고 원격 인증을 활성화하면 인증 서버 내의 원격 사용자가 Unified Manager에 액세스할 수 있습니다.

시작하기 전에

- 다음 정보를 사용할 수 있어야 합니다.
 - 인증 서버의 호스트 이름 또는 IP 주소
 - 인증 서버의 포트 번호
- 관리 서버가 인증 서버에서 원격 사용자나 그룹을 인증할 수 있도록 원격 인증을 활성화하고 인증 서비스를 구성해야 합니다.
- 애플리케이션 관리자 역할이 있어야 합니다.

추가하려는 인증 서버가 고가용성(HA) 쌍(동일한 데이터베이스 사용)의 일부인 경우 파트너 인증 서버도 추가할 수 있습니다. 이를 통해 인증 서버 중 하나에 연결할 수 없을 때 관리 서버가 파트너와 통신할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. 보안 연결 사용 옵션을 활성화하거나 비활성화합니다.

만약 당신이 원한다면...	그러면 이렇게 하세요...
활성화하세요	a. 보안 연결 사용 옵션을 선택하세요. b. 인증 서버 영역에서 *추가*를 클릭합니다. c. 인증 서버 추가 대화 상자에서 서버의 인증 이름이나 IP 주소(IPv4 또는 IPv6)를 입력합니다. d. 호스트 승인 대화 상자에서 인증서 보기를 클릭합니다. e. 인증서 보기 대화 상자에서 인증서 정보를 확인한 다음 *닫기*를 클릭합니다. f. 호스트 승인 대화 상자에서 *예*를 클릭합니다.  보안 연결 인증 사용 옵션을 활성화하면 Unified Manager가 인증 서버와 통신하여 인증서를 표시합니다. Unified Manager는 보안 통신의 경우 기본 포트로 636을 사용하고, 비보안 통신의 경우 포트 번호 389를 사용합니다.
비활성화하세요	a. 보안 연결 사용 옵션을 선택 취소합니다. b. 인증 서버 영역에서 *추가*를 클릭합니다. c. 인증 서버 추가 대화 상자에서 서버의 호스트 이름이나 IP 주소(IPv4 또는 IPv6)와 포트 세부 정보를 지정합니다. d. *추가*를 클릭하세요.

추가한 인증 서버가 서버 영역에 표시됩니다.

3. 추가한 인증 서버에서 사용자를 인증할 수 있는지 확인하기 위해 테스트 인증을 수행합니다.

인증 서버 구성 테스트

관리 서버가 인증 서버와 통신할 수 있는지 확인하기 위해 인증 서버 구성을 검증할 수 있습니다. 인증 서버에서 원격 사용자 또는 원격 그룹을 검색하고 구성된 설정을 사용하여 인증하여 구성을 검증할 수 있습니다.

시작하기 전에

- 원격 인증을 활성화하고 인증 서비스를 구성하여 Unified Manager 서버가 원격 사용자 또는 원격 그룹을 인증할 수 있도록 해야 합니다.
- 관리 서버가 이러한 서버에서 원격 사용자 또는 원격 그룹을 검색하고 인증할 수 있도록 인증 서버를 추가해야 합니다.
- 애플리케이션 관리자 역할이 있어야 합니다.

인증 서비스가 Active Directory로 설정되어 있고 인증 서버의 기본 그룹에 속한 원격 사용자의 인증을 검증하는 경우, 기본 그룹에 대한 정보는 인증 결과에 표시되지 않습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. *인증 테스트*를 클릭하세요.
3. 사용자 테스트 대화 상자에서 원격 사용자의 사용자 이름과 비밀번호 또는 원격 그룹의 사용자 이름을 지정한 다음 *테스트*를 클릭합니다.

원격 그룹을 인증하는 경우 비밀번호를 입력하면 안 됩니다.

알림 추가

특정 이벤트가 생성되면 알림을 받도록 알림을 구성할 수 있습니다. 단일 리소스, 리소스 그룹 또는 특정 심각도 유형의 이벤트에 대한 알림을 구성할 수 있습니다. 알림을 받을 빈도를 지정하고 알림에 스크립트를 연결할 수 있습니다.

시작하기 전에

- 이벤트가 생성될 때 Active IQ Unified Manager 서버가 이러한 설정을 사용하여 사용자에게 알림을 보낼 수 있도록 사용자 이메일 주소, SMTP 서버, SNMP 트랩 호스트와 같은 알림 설정을 구성해야 합니다.
- 알림을 발생시키고자 하는 리소스와 이벤트, 그리고 알림을 보내고자 하는 사용자의 사용자 이름이나 이메일 주소를 알아야 합니다.
- 이벤트에 따라 스크립트를 실행하려면 스크립트 페이지를 사용하여 Unified Manager에 스크립트를 추가해야 합니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

여기에 설명된 대로 알림 설정 페이지에서 알림을 만드는 것 외에도 이벤트를 수신한 후 이벤트 세부 정보 페이지에서 직접 알림을 만들 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *알림 설정*을 클릭합니다.
2. 알림 설정 페이지에서 *추가*를 클릭합니다.
3. 알림 추가 대화 상자에서 *이름*을 클릭하고 알림의 이름과 설명을 입력합니다.
4. *리소스*를 클릭하고 알림에 포함하거나 제외할 리소스를 선택합니다.

이름에 포함 필드에 텍스트 문자열을 지정하여 필터를 설정하여 리소스 그룹을 선택할 수 있습니다. 지정한 텍스트 문자열을 기준으로 사용 가능한 리소스 목록에는 필터 규칙과 일치하는 리소스만 표시됩니다. 지정하는 텍스트 문자열은 대소문자를 구분합니다.

리소스가 지정한 포함 및 제외 규칙을 모두 준수하는 경우 제외 규칙이 포함 규칙보다 우선하며 제외된 리소스와 관련된 이벤트에 대한 알림은 생성되지 않습니다.

5. *이벤트*를 클릭하고 알림을 트리거하려는 이벤트 이름이나 이벤트 심각도 유형에 따라 이벤트를 선택합니다.



두 개 이상의 이벤트를 선택하려면 선택하는 동안 Ctrl 키를 누르세요.

6. *작업*을 클릭하고 알림을 보낼 사용자를 선택하고, 알림 빈도를 선택하고, SNMP 트랩을 트랩 수신기로 보낼지 여부를 선택하고, 알림이 생성될 때 실행할 스크립트를 지정합니다.



사용자에게 지정된 이메일 주소를 수정하고 편집을 위해 알림을 다시 열면 수정된 이메일 주소가 이전에 선택된 사용자에 더 이상 매핑되지 않으므로 이름 필드가 비어 있게 됩니다. 또한, 사용자 페이지에서 선택한 사용자의 이메일 주소를 수정한 경우, 수정된 이메일 주소는 선택한 사용자의 이메일 주소에 업데이트되지 않습니다.

SNMP 트랩을 통해 사용자에게 알리도록 선택할 수도 있습니다.

7. *저장*을 클릭하세요.

알림 추가의 예

이 예제에서는 다음 요구 사항을 충족하는 알림을 만드는 방법을 보여줍니다.

- 알림 이름: HealthTest
- 리소스: 이름에 "abc"가 포함된 모든 볼륨을 포함하고 이름에 "xyz"가 포함된 모든 볼륨을 제외합니다.
- 이벤트: 모든 중요한 건강 이벤트 포함
- 작업: "sample@domain.com", "테스트" 스크립트가 포함되며 사용자는 15분마다 알림을 받아야 합니다.

알림 추가 대화 상자에서 다음 단계를 수행합니다.

단계

1. 이름*을 클릭하고 *알림 이름 필드에 *HealthTest*를 입력합니다.
2. *리소스*를 클릭하고 포함 탭의 드롭다운 목록에서 *볼륨*을 선택합니다.
 - a. 이름에 "abc"가 포함된 볼륨을 표시하려면 이름 포함 필드에 *abc*를 입력합니다.
 - b. +를 선택하세요 **[All Volumes whose name contains 'abc']** + 사용 가능한 리소스 영역에서 선택한 리소스 영역으로 이동합니다.
 - c. 제외*를 클릭하고 *이름에 포함 필드에 *xyz*를 입력한 다음 *추가*를 클릭합니다.
3. *이벤트*를 클릭하고 이벤트 심각도 필드에서 *중요*를 선택합니다.
4. 일치하는 이벤트 영역에서 *모든 중요 이벤트*를 선택하고 선택한 이벤트 영역으로 이동합니다.
5. *작업*을 클릭하고, 이 사용자에게 알림 필드에 *sample@domain.com*을 입력합니다.
6. 사용자에게 15분마다 알림을 보내려면 *15분마다 알림*을 선택하세요.

지정된 시간 동안 수신자에게 알림을 반복적으로 보내도록 알림을 구성할 수 있습니다. 경고에 대한 이벤트 알림이 활성화되는 시간을 결정해야 합니다.

7. 실행할 스크립트 선택 메뉴에서 테스트 스크립트를 선택합니다.

8. *저장*을 클릭하세요.

로컬 사용자 비밀번호 변경

잠재적인 보안 위험을 방지하기 위해 로컬 사용자 로그인 비밀번호를 변경할 수 있습니다.

시작하기 전에

로컬 사용자로 로그인해야 합니다.

유지 관리 사용자와 원격 사용자의 비밀번호는 이 단계를 통해 변경할 수 없습니다. 원격 사용자 비밀번호를 변경하려면 비밀번호 관리자에게 문의하세요. 유지 관리 사용자 비밀번호를 변경하려면 다음을 참조하세요. "[유지 관리 콘솔 사용](#)".

단계

1. Unified Manager에 로그인하세요.
2. 상단 메뉴바에서 사용자 아이콘을 클릭한 다음 *비밀번호 변경*을 클릭합니다.

원격 사용자의 경우 비밀번호 변경 옵션이 표시되지 않습니다.

3. 비밀번호 변경 대화 상자에서 현재 비밀번호와 새 비밀번호를 입력합니다.
4. *저장*을 클릭하세요.

Unified Manager가고가용성 구성으로 구성된 경우 설정의 두 번째 노드에서 비밀번호를 변경해야 합니다. 두 인스턴스 모두 동일한 비밀번호를 가져야 합니다.

세션 비활성 시간 초과 설정

Unified Manager에 대한 비활성 시간 초과 값을 지정하여 일정 시간 동안 비활성 상태가 지속되면 세션이 자동으로 종료되도록 할 수 있습니다. 기본적으로 제한 시간은 4,320분(72시간)으로 설정됩니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

이 설정은 로그인한 모든 사용자 세션에 영향을 미칩니다.



SAML(Security Assertion Markup Language) 인증을 활성화한 경우 이 옵션을 사용할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *기능 설정*을 클릭합니다.
2. 기능 설정 페이지에서 다음 옵션 중 하나를 선택하여 비활성 시간 초과를 지정합니다.

만약 당신이 원한다면...	그러면 이렇게 하세요...
세션이 자동으로 닫히지 않도록 시간 초과를 설정하지 마십시오.	비활성 시간 초과 패널에서 슬라이더 버튼을 왼쪽(끄기)으로 옮기고 *적용*을 클릭합니다.

만약 당신이 원한다면...	그러면 이렇게 하세요...
시간 초과 값으로 특정 분 수를 설정합니다.	비활성 시간 초과 패널에서 슬라이더 버튼을 오른쪽 (켜짐)으로 옮기고, 비활성 시간 초과 값을 분 단위로 지정한 다음 *적용*을 클릭합니다.

CLI를 통해 세션 시간 초과 설정

CLI를 사용하여 Unified Manager에 대한 최대 세션 시간 초과 값을 설정하면 특정 시간이 지나면 세션이 자동으로 종료됩니다. 기본적으로 세션 시간 초과는 최대값인 4,320분(72시간)으로 설정됩니다. 즉, 로그인하여 Unified Manager를 적극적으로 사용하고 있더라도 세션은 72시간 후에 자동으로 종료됩니다.

이 작업에 관하여

애플리케이션 관리자 역할이 있어야 합니다.

세션 시간 초과 설정은 로그인한 모든 사용자 세션에 영향을 미칩니다.

단계

1. Unified Manager CLI에 로그인하려면 다음을 입력하세요. `um cli login` 명령. 인증을 위해 유효한 사용자 이름과 비밀번호를 사용하세요.
2. 입력하세요 `um option set max.session.timeout.value=<in mins>` 세션 시간 초과 값을 수정하는 명령입니다.

Unified Manager 호스트 이름 변경

어느 시점에서 Unified Manager를 설치한 시스템의 호스트 이름을 변경하고 싶을 수도 있습니다. 예를 들어, Unified Manager 서버를 유형, 작업 그룹 또는 모니터링되는 클러스터 그룹별로 더 쉽게 식별할 수 있도록 호스트 이름을 바꿀 수 있습니다.

호스트 이름을 변경하는 데 필요한 단계는 Unified Manager가 VMware ESXi 서버, Red Hat Linux 서버 또는 Microsoft Windows 서버에서 실행되는지에 따라 다릅니다.

Unified Manager 가상 어플라이언스 호스트 이름 변경

Unified Manager 가상 어플라이언스가 처음 배포될 때 네트워크 호스트에 이름이 지정됩니다. 배포 후에 호스트 이름을 변경할 수 있습니다. 호스트 이름을 변경하는 경우 HTTPS 인증서도 다시 생성해야 합니다.

시작하기 전에

이러한 작업을 수행하려면 유지 관리 사용자로 Unified Manager에 로그인하거나 애플리케이션 관리자 역할이 할당되어야 합니다.

호스트 이름(또는 호스트 IP 주소)을 사용하여 Unified Manager 웹 UI에 액세스할 수 있습니다. 배포 중에 네트워크에 대한 정적 IP 주소를 구성한 경우 네트워크 호스트에 대한 이름을 지정했을 것입니다. DHCP를 사용하여 네트워크를 구성한 경우 호스트 이름은 DNS에서 가져와야 합니다. DHCP 또는 DNS가 올바르게 구성되지 않으면 호스트 이름 "Unified Manager"가 자동으로 할당되고 보안 인증서와 연결됩니다.

호스트 이름이 어떻게 할당되었는지와 관계없이 호스트 이름을 변경하고 새 호스트 이름을 사용하여 Unified Manager 웹 UI에 액세스하려는 경우 새 보안 인증서를 생성해야 합니다.

호스트 이름 대신 서버의 IP 주소를 사용하여 웹 UI에 액세스하는 경우 호스트 이름을 변경해도 새 인증서를 생성할 필요가 없습니다. 하지만 인증서의 호스트 이름이 실제 호스트 이름과 일치하도록 인증서를 업데이트하는 것이 가장 좋습니다.

Unified Manager에서 호스트 이름을 변경하는 경우 OnCommand Workflow Automation (WFA)에서 호스트 이름을 수동으로 업데이트해야 합니다. WFA에서는 호스트 이름이 자동으로 업데이트되지 않습니다.

Unified Manager 가상 머신을 다시 시작할 때까지 새 인증서가 적용되지 않습니다.

단계

1. HTTPS 보안 인증서 생성

새 호스트 이름을 사용하여 Unified Manager 웹 UI에 액세스하려면 HTTPS 인증서를 다시 생성하여 새 호스트 이름과 연결해야 합니다.

2. Unified Manager 가상 머신을 다시 시작합니다.

HTTPS 인증서를 다시 생성한 후에는 Unified Manager 가상 머신을 다시 시작해야 합니다.

HTTPS 보안 인증서 생성

Active IQ Unified Manager 처음 설치하면 기본 HTTPS 인증서가 설치됩니다. 기존 인증서를 대체하는 새로운 HTTPS 보안 인증서를 생성할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

DN(고유 이름)에 더 나은 값을 원하거나, 더 큰 키 크기나 더 긴 만료 기간을 원하거나, 현재 인증서가 만료된 경우 등 인증서를 다시 생성하는 데에는 여러 가지 이유가 있을 수 있습니다.

Unified Manager 웹 UI에 액세스할 수 없는 경우 유지 관리 콘솔을 사용하여 동일한 값으로 HTTPS 인증서를 다시 생성할 수 있습니다. 인증서를 재생성하는 동안 키 크기와 키 유효 기간을 정의할 수 있습니다. 당신이 사용하는 경우 Reset Server Certificate 유지 관리 콘솔에서 옵션을 선택하면 397일 동안 유효한 새로운 HTTPS 인증서가 생성됩니다. 이 인증서에는 2048비트 크기의 RSA 키가 있습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *HTTPS 인증서*를 클릭합니다.

2. *HTTPS 인증서 재생성*을 클릭합니다.

HTTPS 인증서 재생성 대화 상자가 표시됩니다.

3. 인증서를 생성하려는 방법에 따라 다음 옵션 중 하나를 선택하세요.

만약 당신이 원한다면...	이렇게 하세요...
현재 값으로 인증서를 다시 생성합니다.	현재 인증서 속성을 사용하여 다시 생성 옵션을 클릭합니다.

만약 당신이 원한다면...	이렇게 하세요...
다른 값을 사용하여 인증서 생성	현재 인증서 속성 업데이트 옵션을 클릭합니다. 새 값을 입력하지 않으면 일반 이름 및 대체 이름 필드는 기존 인증서의 값을 사용합니다. 일반 이름은 호스트의 FQDN으로 설정해야 합니다. 다른 필드에는 값이 필요하지 않지만, 인증서에 값을 채우려는 경우 이메일, 회사, 부서, 도시, 주, 국가 등의 값을 입력할 수 있습니다. 사용 가능한 키 크기(키 알고리즘은 "RSA")와 유효 기간 중에서 선택할 수도 있습니다.  • 키 크기에 허용되는 값은 다음과 같습니다. 2048 , 3072 그리고 4096 . • 유효기간은 최소 1일부터 최대 36,500일까지입니다. 유효기간은 36,500일이 허용되지만, 397일 또는 13개월을 넘지 않는 유효기간을 사용하는 것이 좋습니다. 유효 기간을 397일 이상으로 선택하고 이 인증서에 대한 CSR을 내보내고 잘 알려진 CA에서 서명을 받으려고 하는 경우, CA에서 반환한 서명된 인증서의 유효 기간은 397일로 줄어듭니다. • 인증서의 대체 이름 필드에서 로컬 식별 정보를 제거하려면 "로컬 식별 정보 제외(예: 로컬호스트)" 확인란을 선택할 수 있습니다. 이 확인란을 선택하면 필드에 입력한 내용만 대체 이름 필드에 사용됩니다. 이 필드를 비워 두면 인증서에 대체 이름 필드가 전혀 없습니다.

4. *예*를 클릭하여 인증서를 다시 생성합니다.
5. 새 인증서가 적용되도록 Unified Manager 서버를 다시 시작합니다.
6. HTTPS 인증서를 확인하여 새로운 인증서 정보를 확인하세요.

Unified Manager 가상 머신을 다시 시작합니다.

Unified Manager의 유지 관리 콘솔에서 가상 머신을 다시 시작할 수 있습니다. 새로운 보안 인증서를 생성한 후 또는 가상 머신에 문제가 있는 경우 다시 시작해야 합니다.

시작하기 전에

가상 어플라이언스의 전원이 켜져 있습니다.

유지 관리 사용자로 유지 관리 콘솔에 로그인했습니다.

게스트 다시 시작 옵션을 사용하여 vSphere에서 가상 머신을 다시 시작할 수도 있습니다. 자세한 내용은 VMware 설명서를 참조하세요.

단계

1. 유지 관리 콘솔에 액세스합니다.
2. 시스템 구성 > *가상 머신 재부팅*을 선택합니다.

Linux 시스템에서 Unified Manager 호스트 이름 변경

어느 시점에서 Unified Manager를 설치한 Red Hat Enterprise Linux 시스템의 호스트 이름을 변경하고 싶을 수도 있습니다. 예를 들어, Linux 컴퓨터를 나열할 때 Unified Manager 서버를 유형, 작업 그룹 또는 모니터링되는 클러스터 그룹별로 더 쉽게 식별할 수 있도록 호스트 이름을 바꿀 수 있습니다.

시작하기 전에

Unified Manager가 설치된 Linux 시스템에 루트 사용자 액세스 권한이 있어야 합니다.

호스트 이름(또는 호스트 IP 주소)을 사용하여 Unified Manager 웹 UI에 액세스할 수 있습니다. 배포 중에 네트워크에 대한 정적 IP 주소를 구성한 경우 네트워크 호스트에 대한 이름을 지정했을 것입니다. DHCP를 사용하여 네트워크를 구성한 경우 호스트 이름은 DNS 서버에서 가져와야 합니다.

호스트 이름이 어떻게 할당되었는지에 관계없이 호스트 이름을 변경하고 새 호스트 이름을 사용하여 Unified Manager 웹 UI에 액세스하려는 경우 새 보안 인증서를 생성해야 합니다.

호스트 이름 대신 서버의 IP 주소를 사용하여 웹 UI에 액세스하는 경우 호스트 이름을 변경해도 새 인증서를 생성할 필요가 없습니다. 하지만 인증서를 업데이트하여 인증서의 호스트 이름이 실제 호스트 이름과 일치하도록 하는 것이 가장 좋은 방법입니다. 새로운 인증서는 Linux 컴퓨터를 다시 시작할 때까지 적용되지 않습니다.

Unified Manager에서 호스트 이름을 변경하는 경우 OnCommand Workflow Automation (WFA)에서 호스트 이름을 수동으로 업데이트해야 합니다. WFA에서는 호스트 이름이 자동으로 업데이트되지 않습니다.

단계

1. 수정하려는 Unified Manager 시스템에 루트 사용자로 로그인합니다.
2. 다음 명령을 입력하여 Unified Manager 소프트웨어와 관련 MySQL 소프트웨어를 중지합니다.

```
systemctl stop ocieau ocie mysqld
```

3. Linux를 사용하여 호스트 이름 변경 hostnamectl 명령:

```
hostnamectl set-hostname new_FQDN
```

```
hostnamectl set-hostname nuhost.corp.widget.com
```

4. 서버에 대한 HTTPS 인증서를 다시 생성합니다.

```
/opt/netapp/essentials/bin/cert.sh create
```

5. 네트워크 서비스를 다시 시작합니다.

```
systemctl restart NetworkManager.service
```

6. 서비스를 다시 시작한 후 새 호스트 이름이 자기 자신을 ping할 수 있는지 확인하세요.

```
ping new_hostname
```

```
ping nuhost
```

이 명령은 원래 호스트 이름에 대해 이전에 설정된 것과 동일한 IP 주소를 반환해야 합니다.

7. 호스트 이름 변경을 완료하고 확인한 후 다음 명령을 입력하여 Unified Manager를 다시 시작합니다.

```
systemctl start mysqld ocie ocieau
```

정책 기반 스토리지 관리 활성화 및 비활성화

Unified Manager 9.7부터 ONTAP 클러스터에서 스토리지 워크로드(볼륨 및 LUN)를 프로비저닝하고, 할당된 성능 서비스 수준에 따라 해당 워크로드를 관리할 수 있습니다. 이 기능은 ONTAP System Manager에서 워크로드를 생성하고 QoS 정책을 첨부하는 것과 유사하지만 Unified Manager를 사용하여 적용하면 Unified Manager 인스턴스가 모니터링하는 모든 클러스터에서 워크로드를 프로비저닝하고 관리할 수 있습니다.

애플리케이션 관리자 역할이 있어야 합니다.

이 옵션은 기본적으로 활성화되어 있지만 Unified Manager를 사용하여 워크로드를 프로비저닝하고 관리하고 싶지 않으면 비활성화할 수 있습니다.

이 옵션을 활성화하면 사용자 인터페이스에 여러 가지 새로운 항목이 제공됩니다.

새로운 콘텐츠	위치
새로운 워크로드를 프로비저닝하는 페이지	일반 작업 > *프로비저닝*에서 사용 가능
성능 서비스 수준 정책을 생성하는 페이지	설정 > 정책 > *성능 서비스 수준*에서 사용 가능
성능 스토리지 효율성 정책을 생성하는 페이지	설정 > 정책 > *저장소 효율성*에서 사용 가능
현재 작업 부하 성능 및 작업 부하 IOPS를 설명하는 패널	대시보드에서 사용 가능

이 페이지와 기능에 대한 자세한 내용은 제품의 온라인 도움말을 참조하세요.

단계

1. 왼쪽 탐색 창에서 일반 > *기능 설정*을 클릭합니다.
2. 기능 설정 페이지에서 다음 옵션 중 하나를 선택하여 정책 기반 저장소 관리를 비활성화하거나 활성화합니다.

만약 당신이 원한다면...	그러면 이렇게 하세요...
정책 기반 스토리지 관리 비활성화	정책 기반 저장소 관리 패널에서 슬라이더 버튼을 왼쪽으로 이동합니다.
정책 기반 스토리지 관리 활성화	정책 기반 저장소 관리 패널에서 슬라이더 버튼을 오른쪽으로 이동합니다.

Unified Manager 백업 구성

호스트 시스템에서 수행되는 일련의 구성 단계와 유지 관리 콘솔을 통해 Unified Manager에서 백업 기능을 구성할 수 있습니다.

구성 단계에 대한 정보는 다음을 참조하세요. "[백업 및 복원 작업 관리](#)".

기능 설정 관리

기능 설정 페이지를 사용하면 Active IQ Unified Manager의 특정 기능을 활성화하거나 비활성화할 수 있습니다. 여기에는 정책에 따라 스토리지 객체를 생성하고 관리하고, API 게이트웨이와 로그인 배너를 활성화하고, 알림 관리를 위한 스크립트를 업로드하고, 비활성 시간에 따라 웹 UI 세션을 시간 초과하고, Active IQ 플랫폼 이벤트 수신을 비활성화하는 작업이 포함됩니다.



기능 설정 페이지는 애플리케이션 관리자 역할이 있는 사용자만 사용할 수 있습니다.

스크립트 업로드에 대한 정보는 다음을 참조하세요. "[스크립트 업로드 활성화 및 비활성화](#)".

정책 기반 스토리지 관리 활성화

정책 기반 스토리지 관리 옵션을 사용하면 서비스 수준 목표(SLO)에 따라 스토리지를 관리할 수 있습니다. 이 옵션은 기본적으로 활성화되어 있습니다.

이 기능을 활성화하면 Active IQ Unified Manager 인스턴스에 추가된 ONTAP 클러스터에서 스토리지 워크로드를 프로비저닝하고, 할당된 성능 서비스 수준 및 스토리지 효율성 정책에 따라 이러한 워크로드를 관리할 수 있습니다.

일반 > 기능 설정 > *정책 기반 저장소 관리*에서 이 기능을 활성화하거나 비활성화할 수 있습니다. 이 기능을 활성화하면 다음 페이지에서 작업 및 모니터링을 할 수 있습니다.

- 프로비저닝(스토리지 워크로드 프로비저닝)
- 정책 > 성능 서비스 수준
- 정책 > 저장 효율성
- 클러스터 설정 페이지의 성능 서비스 수준 열에 따라 관리되는 워크로드
- 대시보드의 작업 부하 성능 패널

화면을 사용하여 성능 서비스 수준 및 스토리지 효율성 정책을 만들고 스토리지 작업 부하를 프로비저닝할 수 있습니다. 할당된 성능 서비스 수준을 준수하는 스토리지 작업 부하와 준수하지 않는 작업 부하도 모니터링할 수 있습니다. 워크로드 성능 및 워크로드 IOPS 패널을 사용하면 프로비저닝된 스토리지 워크로드를 기준으로 데이터 센터 전반의 클러스터의 총 용량 및 성능(IOPS), 사용 가능한 용량 및 용량, 사용된 용량 및 성능(IOPS)을 평가할 수도 있습니다.

이 기능을 활성화한 후 Unified Manager REST API를 실행하여 메뉴 모음 > 도움말 버튼 > **API 문서** > 저장소 공급자 카테고리에서 일부 기능을 수행할 수 있습니다. 또는 <https://<hostname>/docs/api/> 형식으로 호스트 이름 또는 IP 주소와 REST API 페이지에 액세스할 URL을 입력할 수 있습니다.

API에 대한 자세한 내용은 다음을 참조하세요. "[Active IQ Unified Manager REST API 시작하기](#)".

API 게이트웨이 활성화

API Gateway 기능을 사용하면 Active IQ Unified Manager 단일 제어 평면으로 사용하여 개별적으로 로그인하지 않고도 여러 ONTAP 클러스터를 관리할 수 있습니다.

Unified Manager에 처음 로그인하면 나타나는 구성 페이지에서 이 기능을 활성화할 수 있습니다. 또는 일반 > 기능 설정 > *API 게이트웨이*에서 이 기능을 활성화하거나 비활성화할 수 있습니다.

Unified Manager REST API는 ONTAP REST API와 다르며, Unified Manager REST API를 사용하여 ONTAP REST API의 모든 기능을 활용할 수 있는 것은 아닙니다. 하지만 Unified Manager에 공개되지 않은 특정 기능을 관리하기 위해 ONTAP API에 액세스해야 하는 특정 비즈니스 요구 사항이 있는 경우 API Gateway 기능을 활성화하고 ONTAP API를 실행할 수 있습니다. 게이트웨이는 ONTAP API와 동일한 형식으로 헤더와 본문 요청을 유지하여 API 요청을 터널링하는 프록시 역할을 합니다. Unified Manager 자격 증명을 사용하고 특정 API를 실행하여 개별 클러스터 자격 증명을 전달하지 않고도 ONTAP 클러스터에 액세스하고 관리할 수 있습니다. Unified Manager는 Unified Manager 인스턴스에서 관리하는 ONTAP 클러스터 전반에서 API를 실행하기 위한 단일 관리 지점 역할을 합니다. API에서 반환된 응답은 ONTAP에서 직접 실행된 해당 ONTAP REST API에서 반환된 응답과 동일합니다.

이 기능을 활성화한 후, 메뉴 모음 > 도움말 버튼 > **API 문서** > 게이트웨이 카테고리에서 Unified Manager REST API를 실행할 수 있습니다. 또는 호스트 이름 또는 IP 주소와 REST API 페이지에 액세스하기 위한 URL을 다음 형식으로 입력할 수 있습니다. <https://<hostname>/docs/api/>

API에 대한 자세한 내용은 다음을 참조하세요. "[Active IQ Unified Manager REST API 시작하기](#)".

비활성 시간 초과 지정

Active IQ Unified Manager에 대한 비활성 시간 초과 값을 지정할 수 있습니다. 지정된 시간 동안 아무런 활동이 없으면 애플리케이션이 자동으로 로그아웃됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

일반 > 기능 설정 > 비활성 시간 초과*에서 이 기능을 비활성화하거나 시간을 수정할 수 있습니다. 이 기능을 활성화한 후에는 *로그아웃 후 필드에 비활성 시간 제한(분)을 지정해야 합니다. 시간이 지나면 시스템이 자동으로 로그아웃됩니다. 기본값은 4320분(72시간)입니다.



SAML(Security Assertion Markup Language) 인증을 활성화한 경우 이 옵션을 사용할 수 없습니다.

Active IQ 포털 이벤트 활성화

Active IQ 포털 이벤트를 활성화할지 비활성화할지 지정할 수 있습니다. 이 설정을 사용하면 Active IQ 포털에서 시스템 구성, 케이블링 등에 대한 추가 이벤트를 검색하고 표시할 수

있습니다. 이 옵션은 기본적으로 활성화되어 있습니다.

이 기능을 활성화하면 Active IQ Unified Manager Active IQ 포털에서 발견된 이벤트를 표시합니다. 이러한 이벤트는 모니터링되는 모든 스토리지 시스템에서 생성된 AutoSupport 메시지에 대해 일련의 규칙을 실행하여 생성됩니다. 이러한 이벤트는 다른 Unified Manager 이벤트와 다르며 시스템 구성, 케이블링, 모범 사례 및 가용성 문제와 관련된 사고나 위험을 식별합니다.

일반 > 기능 설정 > * Active IQ 포털 이벤트*에서 이 기능을 활성화하거나 비활성화할 수 있습니다. 외부 네트워크 접속이 불가능한 사이트에서는 저장소 관리 > 이벤트 설정 > *규칙 업로드*에서 수동으로 규칙을 업로드해야 합니다.

이 기능은 기본적으로 활성화되어 있습니다. 이 기능을 비활성화하면 Active IQ 이벤트가 Unified Manager에서 검색되거나 표시되지 않습니다. 이 기능을 비활성화한 경우, 활성화하면 Unified Manager가 해당 클러스터 시간대의 사전 정의된 시간인 00:15에 클러스터에서 Active IQ 이벤트를 수신할 수 있습니다.

규정 준수를 위한 보안 설정 활성화 및 비활성화

기능 설정 페이지의 보안 대시보드 패널에서 사용자 지정 버튼을 사용하면 Unified Manager에서 규정 준수 모니터링을 위한 보안 매개변수를 활성화하거나 비활성화할 수 있습니다.

이 페이지에서 활성화 또는 비활성화되는 설정은 Unified Manager의 클러스터 및 스토리지 VM의 전반적인 규정 준수 상태를 관리합니다. 선택 사항에 따라 해당 열린 클러스터 인벤토리 페이지의 보안: 모든 클러스터 보기와 스토리지 VM 인벤토리 페이지의 보안: 모든 스토리지 **VM** 보기에 표시됩니다.



관리자 역할을 가진 사용자만 이러한 설정을 편집할 수 있습니다.

ONTAP 클러스터, 스토리지 VM 및 볼륨에 대한 보안 기준은 다음에 정의된 권장 사항에 따라 평가됩니다. ["NetApp ONTAP 9 보안 강화 가이드"](#). 대시보드의 보안 패널과 보안 페이지에는 클러스터, 스토리지 VM 및 볼륨의 기본 보안 준수 상태가 표시됩니다. 보안 위반 사항이 있는 클러스터와 스토리지 VM에 대해 보안 이벤트가 생성되고 관리 작업이 활성화됩니다.

보안 설정 사용자 정의

ONTAP 환경에 맞게 규정 준수 모니터링 설정을 사용자 지정하려면 다음 단계를 따르세요.

단계

1. 일반 > 기능 설정 > 보안 대시보드 > 사용자 지정*을 클릭합니다. *보안 대시보드 설정 사용자 정의 팝업이 나타납니다.



활성화하거나 비활성화하는 보안 준수 매개변수는 클러스터 및 스토리지 VM 화면의 기본 보안 보기, 보고서 및 예약된 보고서에 직접적인 영향을 미칠 수 있습니다. 보안 매개변수를 수정하기 전에 이 화면에서 엑셀 보고서를 업로드했다면, 다운로드한 엑셀 보고서에 오류가 있을 수 있습니다.

2. ONTAP 클러스터에 대한 사용자 정의 설정을 활성화하거나 비활성화하려면 *클러스터*에서 필요한 일반 설정을 선택합니다. 클러스터 규정 준수를 사용자 정의하기 위한 옵션에 대한 정보는 다음을 참조하세요. ["클러스터 규정 준수 범주"](#).
3. 스토리지 VM에 대한 사용자 지정 설정을 활성화하거나 비활성화하려면 *스토리지 VM*에서 필요한 일반 설정을 선택하세요. 스토리지 VM 규정 준수를 사용자 정의하기 위한 옵션에 대한 정보는 다음을 참조하세요. ["스토리지 VM 규정 준수 범주"](#).

AutoSupport 및 인증 설정 사용자 지정

- AutoSupport 설정* 섹션에서 ONTAP 에서 AutoSupport 메시지를 보내는 데 HTTPS 전송을 사용할지 여부를 지정할 수 있습니다.

인증 설정 섹션에서 기본 ONTAP 관리자 사용자에게 대해 Unified Manager 경고가 발생하도록 설정할 수 있습니다.

스크립트 업로드 활성화 및 비활성화

스크립트를 Unified Manager에 업로드하고 실행하는 기능은 기본적으로 활성화되어 있습니다. 보안상의 이유로 조직에서 이러한 활동을 허용하지 않으려는 경우 이 기능을 비활성화할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *기능 설정*을 클릭합니다.
2. 기능 설정 페이지에서 다음 옵션 중 하나를 선택하여 스크립팅을 비활성화하거나 활성화합니다.

만약 당신이 원한다면...	그러면 이렇게 하세요...
스크립트 비활성화	스크립트 업로드 패널에서 슬라이더 버튼을 왼쪽으로 이동합니다.
스크립트 활성화	스크립트 업로드 패널에서 슬라이더 버튼을 오른쪽으로 이동합니다.

로그인 배너 추가

로그인 배너를 추가하면 조직에서 로그인 및 로그아웃 시 시스템에 누가 접근할 수 있는지, 이용약관 등의 정보를 표시할 수 있습니다.

저장소 운영자나 관리자 등 모든 사용자는 로그인, 로그아웃, 세션 시간 초과 시 이 로그인 배너 팝업을 볼 수 있습니다.

유지 관리 콘솔을 사용하세요

유지 관리 콘솔을 사용하여 네트워크 설정을 구성하고, Unified Manager가 설치된 시스템을 구성 및 관리하고, 발생 가능한 문제를 예방하고 해결하는 데 도움이 되는 기타 유지 관리 작업을 수행할 수 있습니다.

유지 관리 콘솔이 제공하는 기능은 무엇입니까?

Unified Manager 유지 관리 콘솔을 사용하면 Unified Manager 시스템의 설정을 유지 관리하고

문제 발생을 방지하기 위해 필요한 변경을 수행할 수 있습니다.

Unified Manager를 설치한 운영 체제에 따라 유지 관리 콘솔은 다음과 같은 기능을 제공합니다.

- 특히 Unified Manager 웹 인터페이스를 사용할 수 없는 경우 가상 어플라이언스에 문제가 있으면 해결하세요.
- Unified Manager의 최신 버전으로 업그레이드하세요
- 기술 지원팀에 보낼 지원 번들을 생성합니다.
- 네트워크 설정 구성
- 유지 관리 사용자 비밀번호 변경
- 외부 데이터 공급자에 연결하여 성능 통계를 전송합니다.
- 성능 데이터 수집 내부 변경
- 이전에 백업한 버전에서 Unified Manager 데이터베이스와 구성 설정을 복원합니다.

유지 관리 사용자가 하는 일

유지 관리 사용자는 Red Hat Enterprise Linux 시스템에 Unified Manager를 설치하는 동안 생성됩니다. 유지 관리 사용자 이름은 “umadmin” 사용자입니다. 유지 관리 사용자는 웹 UI에서 애플리케이션 관리자 역할을 맡고 있으며, 해당 사용자는 후속 사용자를 만들고 역할을 할당할 수 있습니다.

유지 관리 사용자 또는 umadmin 사용자도 Unified Manager 유지 관리 콘솔에 액세스할 수 있습니다.

진단 사용자 기능

진단 액세스의 목적은 기술 지원팀이 문제 해결을 도울 수 있도록 하는 것이며, 기술 지원팀의 지시가 있을 때에만 사용해야 합니다.

진단 사용자는 기술 지원팀의 지시에 따라 문제 해결을 위해 OS 수준 명령을 실행할 수 있습니다.

유지 관리 콘솔에 액세스하세요

Unified Manager 사용자 인터페이스가 작동하지 않거나 사용자 인터페이스에서 사용할 수 없는 기능을 수행해야 하는 경우 유지 관리 콘솔에 액세스하여 Unified Manager 시스템을 관리할 수 있습니다.

시작하기 전에

Unified Manager를 설치하고 구성해야 합니다.

15분 동안 아무런 활동이 없으면 유지 관리 콘솔에서 로그아웃됩니다.



VMware에 설치하는 경우 VMware 콘솔을 통해 유지 관리 사용자로 이미 로그인한 경우 Secure Shell을 사용하여 동시에 로그인할 수 없습니다.

단계

1. 유지 관리 콘솔에 액세스하려면 다음 단계를 따르세요.

이 운영체제에서는...	다음 단계를 따르세요...
VMware	- Secure Shell을 사용하여 Unified Manager 가상 어플라이언스의 IP 주소 또는 정규화된 도메인 이름에 연결합니다. - 유지 관리 사용자 이름과 비밀번호를 사용하여 유지 관리 콘솔에 로그인합니다.
리눅스	- Secure Shell을 사용하여 Unified Manager 시스템의 IP 주소 또는 정규화된 도메인 이름에 연결합니다. - 유지 관리 사용자(umadmin) 이름과 비밀번호로 시스템에 로그인합니다. - 명령을 입력하세요 <code>maintenance_console</code> 그리고 Enter를 누르세요.
Windows	- 관리자 자격 증명을 사용하여 Unified Manager 시스템에 로그인합니다. - Windows 관리자 권한으로 PowerShell을 실행합니다. - 명령을 입력하세요 <code>maintenance_console</code> 그리고 Enter를 누르세요.

Unified Manager 유지 관리 콘솔 메뉴가 표시됩니다.

vSphere VM 콘솔을 사용하여 유지 관리 콘솔에 액세스합니다.

Unified Manager 사용자 인터페이스가 작동하지 않거나 사용자 인터페이스에서 사용할 수 없는 기능을 수행해야 하는 경우 유지 관리 콘솔에 액세스하여 가상 어플라이언스를 재구성할 수 있습니다.

시작하기 전에

- 당신은 유지관리 사용자여야 합니다.
- 유지 관리 콘솔에 액세스하려면 가상 어플라이언스의 전원을 켜야 합니다.

단계

- vSphere Client에서 Unified Manager 가상 어플라이언스를 찾습니다.
- 콘솔 탭을 클릭합니다.
- 콘솔 창 안을 클릭하여 로그인하세요.
- 사용자 이름과 비밀번호를 사용하여 유지 관리 콘솔에 로그인하세요.

15분 동안 아무런 활동이 없으면 유지 관리 콘솔에서 로그아웃됩니다.

유지 관리 콘솔 메뉴

유지 관리 콘솔은 Unified Manager 서버의 특수 기능과 구성 설정을 유지 관리하고 관리할 수 있는 다양한 메뉴로 구성되어 있습니다.

Unified Manager를 설치한 운영 체제에 따라 유지 관리 콘솔은 다음 메뉴로 구성됩니다.

- Unified Manager 업그레이드(VMware만 해당)
- 네트워크 구성(VMware만 해당)
- 시스템 구성(VMware만 해당)
 - a. 지원/진단
 - b. 서버 인증서 재설정
 - c. 외부 데이터 공급자
 - d. 백업 복원
 - e. 성능 폴링 간격 구성
 - f. SAML 인증 비활성화
 - g. 애플리케이션 포트 보기/변경
 - h. 디버그 로그 구성
 - i. MySQL 포트 3306에 대한 액세스 제어
 - j. 출구

특정 메뉴 옵션에 접근하려면 목록에서 번호를 선택하세요. 예를 들어, 백업 및 복원의 경우 _4_를 선택합니다.

네트워크 구성 메뉴

네트워크 구성 메뉴를 사용하면 네트워크 설정을 관리할 수 있습니다. Unified Manager 사용자 인터페이스를 사용할 수 없는 경우 이 메뉴를 사용해야 합니다.



Red Hat Enterprise Linux 또는 Microsoft Windows에 Unified Manager가 설치된 경우 이 메뉴를 사용할 수 없습니다.

다음과 같은 메뉴 선택이 가능합니다.

• IP 주소 설정 표시

IP 주소, 네트워크, 브로드캐스트 주소, 넷마스크, 게이트웨이, DNS 서버를 포함하여 가상 어플라이언스의 현재 네트워크 설정을 표시합니다.

• IP 주소 설정 변경

IP 주소, 넷마스크, 게이트웨이 또는 DNS 서버를 포함하여 가상 어플라이언스의 네트워크 설정을 변경할 수 있습니다. 유지 관리 콘솔을 사용하여 네트워크 설정을 DHCP에서 정적 네트워킹으로 전환하는 경우 호스트 이름을 편집할 수 없습니다. 변경 사항을 적용하려면 *변경 사항 적용*을 선택해야 합니다.

• 도메인 이름 검색 설정 표시

호스트 이름을 확인하는 데 사용되는 도메인 이름 검색 목록을 표시합니다.

- 도메인 이름 검색 설정 변경

호스트 이름을 확인할 때 검색할 도메인 이름을 변경할 수 있습니다. 변경 사항을 적용하려면 *변경 사항 적용*을 선택해야 합니다.

- 정적 경로 표시

현재의 정적 네트워크 경로를 표시합니다.

- 정적 경로 변경

정적 네트워크 경로를 추가하거나 삭제할 수 있습니다. 변경 사항을 적용하려면 *변경 사항 적용*을 선택해야 합니다.

- 경로 추가

정적 경로를 추가할 수 있습니다.

- 경로 삭제

정적 경로를 삭제할 수 있습니다.

- 뒤쪽에

*메인 메뉴*로 돌아갑니다.

- 출구

유지 관리 콘솔을 종료합니다.

- 네트워크 인터페이스 비활성화

사용 가능한 모든 네트워크 인터페이스를 비활성화합니다. 사용 가능한 네트워크 인터페이스가 하나뿐인 경우 비활성화할 수 없습니다. 변경 사항을 적용하려면 *변경 사항 적용*을 선택해야 합니다.

- 네트워크 인터페이스 활성화

사용 가능한 네트워크 인터페이스를 활성화합니다. 변경 사항을 적용하려면 *변경 사항 적용*을 선택해야 합니다.

- 변경 사항 커밋

가상 어플라이언스의 네트워크 설정에 대한 모든 변경 사항을 적용합니다. 변경 사항을 적용하려면 이 옵션을 선택해야 하며, 그렇지 않으면 변경 사항이 발생하지 않습니다.

- 호스트에 핑 보내기

IP 주소 변경이나 DNS 구성을 확인하기 위해 대상 호스트에 ping을 보냅니다.

- 기본 설정으로 복원

모든 설정을 공장 기본값으로 재설정합니다. 변경 사항을 적용하려면 *변경 사항 적용*을 선택해야 합니다.

- 뒤쪽에

*메인 메뉴*로 돌아갑니다.

- 출구

유지 관리 콘솔을 종료합니다.

시스템 구성 메뉴

시스템 구성 메뉴를 사용하면 서버 상태 보기, 가상 머신 재부팅 및 종료 등 다양한 옵션을 제공하여 가상 어플라이언스를 관리할 수 있습니다.



Linux 또는 Microsoft Windows 시스템에 Unified Manager가 설치된 경우 이 메뉴에서는 "Unified Manager 백업에서 복원" 옵션만 사용할 수 있습니다.

다음과 같은 메뉴 선택이 가능합니다.

- 서버 상태 표시

현재 서버 상태를 표시합니다. 상태 옵션에는 실행 중 및 실행 중이 아님이 있습니다.

서버가 실행되고 있지 않으면 기술 지원팀에 문의해야 할 수도 있습니다.

- 가상 머신 재부팅

가상 머신을 재부팅하고 모든 서비스를 중지합니다. 재부팅 후 가상 머신과 서비스가 다시 시작됩니다.

- 가상 머신 종료

가상 머신을 종료하고 모든 서비스를 중지합니다.

이 옵션은 가상 머신 콘솔에서만 선택할 수 있습니다.

- <로그인한 사용자> 사용자 비밀번호 변경

현재 로그인한 사용자의 비밀번호를 변경합니다. 이 비밀번호는 유지 관리 사용자만 변경할 수 있습니다.

- 데이터 디스크 크기 늘리기

가상 머신의 데이터 디스크(디스크 3) 크기를 늘립니다.

- 스왑 디스크 크기 늘리기

가상 머신의 스왑 디스크(디스크 2) 크기를 늘립니다.

- 시간대 변경

시간대를 해당 지역의 시간대로 변경합니다.

- **NTP** 서버 변경

IP 주소나 정규화된 도메인 이름(FQDN)과 같은 NTP 서버 설정을 변경합니다.

- **NTP 서비스 변경**

사이를 전환합니다 ntp 그리고 systemd-timesyncd 서비스.

- **Unified Manager 백업에서 복원**

이전에 백업된 버전에서 Unified Manager 데이터베이스와 구성 설정을 복원합니다.

- **서버 인증서 재설정**

서버 보안 인증서를 재설정합니다.

- **호스트 이름 변경**

가상 어플라이언스가 설치된 호스트의 이름을 변경합니다.

- **뒤쪽에**

시스템 구성 메뉴를 종료하고 주 메뉴로 돌아갑니다.

- **출구**

유지 관리 콘솔 메뉴를 종료합니다.

지원 및 진단 메뉴

지원 및 진단 메뉴를 사용하면 문제 해결을 위해 기술 지원팀에 보낼 수 있는 지원 번들을 생성할 수 있습니다.

다음 메뉴 옵션을 사용할 수 있습니다.

- **빋 생성 지원 번들**

30일 분의 로그와 구성 데이터베이스 기록만 포함된 가벼운 지원 번들을 생성할 수 있습니다. 여기에는 성능 데이터, 인수 기록 파일, 서버 힙 덤프가 제외됩니다.

- **지원 번들 생성**

진단 사용자의 홈 디렉토리에 진단 정보가 포함된 전체 지원 번들(7-Zip 파일)을 생성할 수 있습니다. 시스템이 인터넷에 연결되어 있는 경우 지원 번들을 NetApp 에 업로드할 수도 있습니다.

이 파일에는 AutoSupport 메시지에서 생성된 정보, Unified Manager 데이터베이스의 내용, Unified Manager 서버 내부에 대한 자세한 데이터, AutoSupport 메시지나 경량 지원 번들에 일반적으로 포함되지 않는 자세한 로그 수준이 포함되어 있습니다.

추가 메뉴 옵션

다음 메뉴 옵션을 사용하면 Unified Manager 서버에서 다양한 관리 작업을 수행할 수 있습니다.

다음과 같은 메뉴 선택이 가능합니다.

- 서버 인증서 재설정

HTTPS 서버 인증서를 다시 생성합니다.

Unified Manager GUI에서 일반 > **HTTPS** 인증서 > *HTTPS 인증서 재생성*을 클릭하여 서버 인증서를 재생성할 수 있습니다.

- **SAML** 인증 비활성화

SAML 인증을 비활성화하여 ID 공급자(IdP)가 Unified Manager GUI에 액세스하는 사용자에게 로그온 인증을 더 이상 제공하지 않도록 합니다. 이 콘솔 옵션은 일반적으로 IdP 서버 또는 SAML 구성 문제로 인해 사용자가 Unified Manager GUI에 액세스할 수 없는 경우에 사용됩니다.

- 외부 데이터 제공자

Unified Manager를 외부 데이터 공급자에 연결하기 위한 옵션을 제공합니다. 연결을 설정한 후 성능 데이터가 외부 서버로 전송되고, 이를 통해 스토리지 성능 전문가가 타사 소프트웨어를 사용하여 성능 지표를 차트로 작성할 수 있습니다. 다음 옵션이 표시됩니다.

- 서버 구성 표시--외부 데이터 공급자에 대한 현재 연결 및 구성 설정을 표시합니다.
- 서버 연결 추가/수정--외부 데이터 공급자에 대한 새로운 연결 설정을 입력하거나 기존 설정을 변경할 수 있습니다.
- 서버 구성 수정--외부 데이터 공급자에 대한 새로운 구성 설정을 입력하거나 기존 설정을 변경할 수 있습니다.
- 서버 연결 삭제--외부 데이터 공급자에 대한 연결을 삭제합니다.

연결이 삭제되면 Unified Manager와 외부 서버 간의 연결이 끊어집니다.

- 백업 복원

자세한 내용은 다음 항목을 참조하세요. ["백업 및 복원 작업 관리"](#).

- 성능 폴링 간격 구성

Unified Manager가 클러스터에서 성능 통계 데이터를 수집하는 빈도를 구성하기 위한 옵션을 제공합니다. 기본 수집 간격은 5분입니다.

대규모 클러스터의 수집이 제때 완료되지 않는 경우 이 간격을 10분 또는 15분으로 변경할 수 있습니다.

- 애플리케이션 포트 보기/변경

보안을 위해 필요한 경우 Unified Manager가 HTTP 및 HTTPS 프로토콜에 사용하는 기본 포트를 변경하는 옵션을 제공합니다. HTTP의 기본 포트는 80이고 HTTPS의 기본 포트는 443입니다.

- **MySQL** 포트 **3306**에 대한 액세스 제어

기본 MySQL 포트 3306에 대한 호스트 액세스를 제어합니다. 보안상의 이유로 Linux, Windows 및 VMware vSphere 시스템에 Unified Manager를 새로 설치하는 동안 이 포트를 통한 액세스는 localhost로만 제한됩니다. 이 옵션을 사용하면 로컬 호스트와 원격 호스트 간에 이 포트의 가시성을 전환할 수 있습니다. 즉, 사용자 환경에서 로컬 호스트에만 사용하도록 설정된 경우 원격 호스트에서도 이 포트를 사용할 수 있습니다. 또는 모든 호스트에 대해 활성화하면 이 포트에 대한 액세스를 로컬호스트로만 제한할 수 있습니다. 이전에 원격 호스트에서 액세스가

활성화된 경우 업그레이드 시나리오에서 구성이 유지됩니다. 포트 가시성을 전환한 후 Windows 시스템에서 방화벽 설정을 확인해야 하며, MySQL 포트 3306에 대한 액세스를 제한하도록 설정이 구성된 경우 방화벽 설정을 비활성화해야 합니다.

- 출구

유지 관리 콘솔 메뉴를 종료합니다.

Windows에서 유지 관리 사용자 비밀번호 변경

필요한 경우 Unified Manager 유지 관리 사용자 비밀번호를 변경할 수 있습니다.

단계

1. Unified Manager 웹 UI 로그인 페이지에서 *비밀번호를 잊으셨나요?*를 클릭하세요.

비밀번호를 재설정하려는 사용자의 이름을 입력하라는 페이지가 표시됩니다.

2. 사용자 이름을 입력하고 *제출*을 클릭하세요.

해당 사용자 이름에 대해 정의된 이메일 주소로 비밀번호 재설정 링크가 포함된 이메일이 전송됩니다.

3. 이메일의 *비밀번호 재설정 링크*를 클릭하고 새로운 비밀번호를 입력하세요.
4. 웹 UI로 돌아가서 새 비밀번호를 사용하여 Unified Manager에 로그인합니다.

Linux 시스템에서 umadmin 비밀번호 변경

보안상의 이유로 설치 과정을 완료한 후에는 Unified Manager umadmin 사용자의 기본 비밀번호를 즉시 변경해야 합니다. 필요한 경우 나중에 언제든지 비밀번호를 변경할 수 있습니다.

시작하기 전에

- Unified Manager는 Red Hat Enterprise Linux Linux 시스템에 설치해야 합니다.
- Unified Manager가 설치된 Linux 시스템에 대한 루트 사용자 자격 증명이 있어야 합니다.

단계

1. Unified Manager가 실행 중인 Linux 시스템에 루트 사용자로 로그인합니다.
2. umadmin 비밀번호를 변경하세요:

```
passwd umadmin
```

시스템에서 umadmin 사용자에 대한 새 비밀번호를 입력하라는 메시지가 표시됩니다.

Unified Manager가 HTTP 및 HTTPS 프로토콜에 사용하는 포트를 변경합니다.

Unified Manager가 HTTP 및 HTTPS 프로토콜에 사용하는 기본 포트는 보안을 위해 필요한 경우 설치 후 변경할 수 있습니다. HTTP의 기본 포트는 80이고 HTTPS의 기본 포트는 443입니다.

시작하기 전에

Unified Manager 서버의 유지 관리 콘솔에 로그인하려면 권한이 있는 사용자 ID와 비밀번호가 있어야 합니다.



Mozilla Firefox나 Google Chrome 브라우저를 사용할 때 안전하지 않은 것으로 간주되는 포트가 몇 가지 있습니다. HTTP 및 HTTPS 트래픽에 대한 새로운 포트 번호를 할당하기 전에 브라우저를 확인하세요. 안전하지 않은 포트를 선택하면 시스템에 접근할 수 없게 되므로 해결을 위해 고객 지원에 문의해야 합니다.

포트를 변경하면 Unified Manager 인스턴스가 자동으로 다시 시작되므로 이때 잠시 시스템을 종료하는 것이 좋습니다.

1. SSH를 사용하여 Unified Manager 호스트에 유지 관리 사용자로 로그인합니다.

Unified Manager 유지 관리 콘솔 프롬프트가 표시됩니다.

2. *애플리케이션 포트 보기/변경*이라고 표시된 메뉴 옵션의 번호를 입력한 다음 Enter를 누릅니다.
3. 메시지가 표시되면 유지 관리 사용자 비밀번호를 다시 입력하세요.
4. HTTP 및 HTTPS 포트에 대한 새 포트 번호를 입력한 다음 Enter를 누릅니다.

포트 번호를 비워 두면 프로토콜의 기본 포트가 할당됩니다.

포트를 변경하고 지금 Unified Manager를 다시 시작할지 묻는 메시지가 표시됩니다.

5. *y*를 입력하여 포트를 변경하고 Unified Manager를 다시 시작합니다.
6. 유지 관리 콘솔을 종료합니다.

이 변경 후 사용자는 Unified Manager 웹 UI에 액세스하기 위해 URL에 새 포트 번호를 포함해야 합니다(예: <https://host.company.com:1234+> , <https://12.13.14.15:1122+> 또는 [https://\[2001:db8:0:1\]:2123+](https://[2001:db8:0:1]:2123+)).

네트워크 인터페이스 추가

네트워크 트래픽을 분리해야 하는 경우 새로운 네트워크 인터페이스를 추가할 수 있습니다.

시작하기 전에

vSphere를 사용하여 가상 어플라이언스에 네트워크 인터페이스를 추가했어야 합니다.

가상 어플라이언스의 전원을 켜야 합니다.



Red Hat Enterprise Linux 또는 Microsoft Windows에 Unified Manager가 설치된 경우 이 작업을 수행할 수 없습니다.

단계

1. vSphere 콘솔 주 메뉴에서 시스템 구성 > *운영 체제 재부팅*을 선택합니다.

재부팅 후 유지 관리 콘솔에서 새로 추가된 네트워크 인터페이스를 감지할 수 있습니다.

2. 유지 관리 콘솔에 액세스합니다.
3. 네트워크 구성 > *네트워크 인터페이스 활성화*를 선택합니다.

4. 새로운 네트워크 인터페이스를 선택하고 *Enter*를 누릅니다.

*eth1*을 선택하고 *Enter*를 누릅니다.

5. 네트워크 인터페이스를 활성화하려면 *y*를 입력하세요.

6. 네트워크 설정을 입력하세요.

정적 인터페이스를 사용하거나 DHCP가 감지되지 않으면 네트워크 설정을 입력하라는 메시지가 표시됩니다.

네트워크 설정을 입력하면 자동으로 네트워크 구성 메뉴로 돌아갑니다.

7. *변경 사항 적용*을 선택합니다.

네트워크 인터페이스를 추가하려면 변경 사항을 커밋해야 합니다.

Unified Manager 데이터베이스 디렉토리에 디스크 공간 추가

Unified Manager 데이터베이스 디렉토리에는 ONTAP 시스템에서 수집된 모든 상태 및 성능 데이터가 포함되어 있습니다. 어떤 상황에서는 데이터베이스 디렉토리의 크기를 늘려야 할 수도 있습니다.

예를 들어 Unified Manager가 각 클러스터에 많은 노드가 있는 많은 수의 클러스터에서 데이터를 수집하는 경우 데이터베이스 디렉토리가 가득 찰 수 있습니다. 데이터베이스 디렉토리가 90% 차면 경고 이벤트를 받고, 디렉토리가 95% 차면 위험 이벤트를 받게 됩니다.



디렉토리가 95% 채워진 후에는 클러스터에서 추가 데이터가 수집되지 않습니다.

데이터 디렉토리에 용량을 추가하는 데 필요한 단계는 Unified Manager가 VMware ESXi 서버, Red Hat 서버 또는 Microsoft Windows 서버에서 실행되는지에 따라 다릅니다.

Linux 호스트의 데이터 디렉토리에 공간 추가

디스크 공간을 충분히 할당하지 않은 경우 /opt/netapp/data Linux 호스트를 처음 설정한 후 Unified Manager를 설치한 경우 Unified Manager를 지원하는 디렉토리에서 디스크 공간을 늘려 설치 후 디스크 공간을 추가할 수 있습니다. /opt/netapp/data 예매 규칙서.

시작하기 전에

Unified Manager가 설치된 Red Hat Enterprise Linux 시스템에 루트 사용자 액세스 권한이 있어야 합니다.

데이터 디렉터리 크기를 늘리기 전에 Unified Manager 데이터베이스를 백업하는 것이 좋습니다.

단계

1. 디스크 공간을 추가하려는 Linux 컴퓨터에 루트 사용자로 로그인합니다.
2. 표시된 순서대로 Unified Manager 서비스와 관련 MySQL 소프트웨어를 중지합니다.

```
systemctl stop ocieau ocie mysqld
```

3. 임시 백업 폴더를 만듭니다(예: /backup-data) 현재 데이터를 포함할 수 있는 충분한 디스크 공간이 있음

/opt/netapp/data 예배 규칙서.

4. 기존의 콘텐츠 및 권한 구성을 복사합니다. /opt/netapp/data 백업 데이터 디렉토리로의 디렉토리:

```
cp -arp /opt/netapp/data/* /backup-data
```

5. SE Linux가 활성화된 경우:

- a. 기존 폴더에 대한 SE Linux 유형을 가져옵니다. /opt/netapp/data 접는 사람:

```
se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |  
head -1
```

시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
echo $se_type  
mysqld_db_t
```

- a. chcon 명령을 실행하여 백업 디렉토리의 SE Linux 유형을 설정합니다.

```
chcon -R --type=mysqld_db_t /backup-data
```

6. 내용을 제거하세요 /opt/netapp/data 예배 규칙서:

- a. cd /opt/netapp/data

- b. rm -rf *

7. 크기를 확장하세요 /opt/netapp/data LVM 명령을 통해 또는 추가 디스크를 추가하여 디렉토리를 최소 150GB로 늘릴 수 있습니다.



당신이 만든 경우 /opt/netapp/data 디스크에서 마운트를 시도해서는 안 됩니다. /opt/netapp/data NFS 또는 CIFS 공유로. 왜냐하면 이 경우 디스크 공간을 확장하려고 하면 다음과 같은 일부 LVM 명령이 resize 그리고 extend 예상대로 작동하지 않을 수도 있습니다.

8. 확인해주세요 /opt/netapp/data 디렉토리 소유자(mysql)와 그룹(root)은 변경되지 않습니다.

```
ls -ltr /opt/netapp/ | grep data
```

시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. SE Linux가 활성화된 경우 컨텍스트를 확인하십시오. /opt/netapp/data 디렉토리는 여전히 mysqld_db_t로 설정되어 있습니다.

- a. touch /opt/netapp/data/abc

- b. ls -Z /opt/netapp/data/abc

시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
-rw-r--r--. root root unconfined_u:object_r:mysql_db_t:s0
/opt/netapp/data/abc
```

10. 이 외부 파일로 인해 향후 데이터베이스 오류가 발생하지 않도록 abc 파일을 삭제하세요.
11. 백업 데이터의 내용을 확장된 파일로 다시 복사합니다. /opt/netapp/data 예매 규칙서:

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. SE Linux가 활성화된 경우 다음 명령을 실행하세요.

```
chcon -R --type=mysql_db_t /opt/netapp/data
```

13. MySQL 서비스를 시작합니다:

```
systemctl start mysqld
```

14. MySQL 서비스가 시작된 후, 표시된 순서대로 ocie 및 ocieau 서비스를 시작합니다.

```
systemctl start ocie ocieau
```

15. 모든 서비스가 시작된 후 백업 폴더를 삭제하세요. /backup-data :

```
rm -rf /backup-data
```

VMware 가상 머신의 데이터 디스크에 공간 추가

Unified Manager 데이터베이스의 데이터 디스크 공간을 늘려야 하는 경우 Unified Manager 유지 관리 콘솔을 사용하여 디스크 공간을 늘려 설치 후 용량을 추가할 수 있습니다.

시작하기 전에

- vSphere Client에 액세스할 수 있어야 합니다.
- 가상 머신에는 로컬로 저장된 스냅샷이 없어야 합니다.
- 유지 관리 사용자 자격 증명이 있어야 합니다.

가상 디스크 크기를 늘리기 전에 가상 머신을 백업하는 것이 좋습니다.

단계

1. vSphere 클라이언트에서 Unified Manager 가상 머신을 선택한 다음 데이터에 디스크 용량을 추가합니다. disk 3 . 자세한 내용은 VMware 설명서를 참조하세요.

드물지만 Unified Manager 배포에서는 데이터 디스크로 “하드 디스크 3” 대신 “하드 디스크 2”를 사용합니다. 배포 중에 이런 일이 발생한 경우, 더 큰 디스크의 공간을 늘리세요. 데이터 디스크는 항상 다른 디스크보다 더 많은 공간을 갖습니다.

2. vSphere 클라이언트에서 Unified Manager 가상 머신을 선택한 다음 콘솔 탭을 선택합니다.

3. 콘솔 창을 클릭한 다음 사용자 이름과 비밀번호를 사용하여 유지 관리 콘솔에 로그인합니다.
4. 메인 메뉴에서 시스템 구성 옵션에 대한 번호를 입력하세요.
5. 시스템 구성 메뉴에서 데이터 디스크 크기 늘리기 옵션에 대한 숫자를 입력합니다.

Microsoft Windows 서버의 논리 드라이브에 공간 추가

Unified Manager 데이터베이스의 디스크 공간을 늘려야 하는 경우 Unified Manager가 설치된 논리 드라이브에 용량을 추가할 수 있습니다.

시작하기 전에

Windows 관리자 권한이 있어야 합니다.

디스크 공간을 추가하기 전에 Unified Manager 데이터베이스를 백업하는 것이 좋습니다.

단계

1. 디스크 공간을 추가하려는 Windows 서버에 관리자로 로그인합니다.
2. 더 많은 공간을 추가하는 데 사용하려는 방법에 해당하는 단계를 따르세요.

옵션	설명
물리적 서버에서 Unified Manager 서버가 설치된 논리 드라이브에 용량을 추가합니다.	Microsoft 항목의 단계를 따르세요. "기본 볼륨 확장"
실제 서버에 하드 디스크 드라이브를 추가합니다.	Microsoft 항목의 단계를 따르세요. "하드 디스크 드라이브 추가"
가상 머신에서 디스크 파티션의 크기를 늘립니다.	VMware 항목의 단계를 따르세요. "디스크 파티션 크기 늘리기"

사용자 액세스 관리

Active IQ Unified Manager 에 대한 사용자 액세스를 제어하기 위해 역할을 만들고 기능을 할당할 수 있습니다. Unified Manager 내에서 선택한 개체에 액세스하는 데 필요한 기능을 갖춘 사용자를 식별할 수 있습니다. 이러한 역할과 기능을 가진 사용자만 Unified Manager에서 개체를 관리할 수 있습니다.

사용자 추가

사용자 페이지를 사용하여 로컬 사용자나 데이터베이스 사용자를 추가할 수 있습니다. 인증 서버에 속한 원격 사용자나 그룹을 추가할 수도 있습니다. 이러한 사용자에게 역할을 할당할 수 있으며, 역할의 권한에 따라 사용자는 Unified Manager를 사용하여 저장소 개체와 데이터를 관리하거나 데이터베이스의 데이터를 볼 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 역할이 있어야 합니다.
- 원격 사용자 또는 그룹을 추가하려면 원격 인증을 활성화하고 인증 서버를 구성해야 합니다.
- 그래픽 인터페이스에 액세스하는 사용자를 ID 공급자(IdP)가 인증하도록 SAML 인증을 구성하려는 경우 이러한 사용자가 “원격” 사용자로 정의되어 있는지 확인하세요.

SAML 인증이 활성화된 경우 “local” 또는 “maintenance” 유형의 사용자는 UI에 액세스할 수 없습니다.

Windows Active Directory에서 그룹을 추가하는 경우 중첩된 하위 그룹이 비활성화되지 않는 한 모든 직접 구성원과 중첩된 하위 그룹이 Unified Manager에 인증할 수 있습니다. OpenLDAP 또는 다른 인증 서비스에서 그룹을 추가하는 경우 해당 그룹의 직접 구성원만 Unified Manager에 인증할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *사용자*를 클릭합니다.
2. 사용자 페이지에서 *추가*를 클릭합니다.
3. 사용자 추가 대화 상자에서 추가하려는 사용자 유형을 선택하고 필요한 정보를 입력합니다.

필수 사용자 정보를 입력할 때 해당 사용자에게 고유한 이메일 주소를 지정해야 합니다. 여러 사용자가 공유하는 이메일 주소는 지정하지 마세요.

4. *추가*를 클릭하세요.

데이터베이스 사용자 생성

Workflow Automation과 Unified Manager 간의 연결을 지원하거나 데이터베이스 보기에 액세스하려면 먼저 Unified Manager 웹 UI에서 통합 스키마 또는 보고서 스키마 역할이 있는 데이터베이스 사용자를 만들어야 합니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

데이터베이스 사용자는 Workflow Automation과의 통합과 보고서별 데이터베이스 보기에 대한 액세스를 제공합니다. 데이터베이스 사용자는 Unified Manager 웹 UI나 유지 관리 콘솔에 액세스할 수 없으며 API 호출을 실행할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *사용자*를 클릭합니다.
2. 사용자 페이지에서 *추가*를 클릭합니다.
3. 사용자 추가 대화 상자의 유형 드롭다운 목록에서 *데이터베이스 사용자*를 선택합니다.
4. 데이터베이스 사용자의 이름과 비밀번호를 입력합니다.
5. 역할 드롭다운 목록에서 적절한 역할을 선택합니다.

만약 당신이라면...	이 역할을 선택하세요
Unified Manager를 Workflow Automation과 연결	통합 스키마

만약 당신이라면...	이 역할을 선택하세요
보고 및 기타 데이터베이스 보기에 액세스	보고서 스키마

6. *추가*를 클릭하세요.

사용자 설정 편집

각 사용자에게 지정된 이메일 주소, 역할 등의 사용자 설정을 편집할 수 있습니다. 예를 들어, 저장소 운영자인 사용자의 역할을 변경하고 해당 사용자에게 저장소 관리자 권한을 할당할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

사용자에게 할당된 역할을 수정하는 경우 다음 작업 중 하나가 발생할 때 변경 사항이 적용됩니다.

- 사용자가 Unified Manager에서 로그아웃한 후 다시 로그인합니다.
- 세션 시간이 24시간 초과되었습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *사용자*를 클릭합니다.
2. 사용자 페이지에서 설정을 편집할 사용자를 선택하고 *편집*을 클릭합니다.
3. 사용자 편집 대화 상자에서 사용자에게 지정된 적절한 설정을 편집합니다.
4. *저장*을 클릭하세요.

사용자 보기

사용자 페이지를 사용하면 Unified Manager를 사용하여 저장소 개체와 데이터를 관리하는 사용자 목록을 볼 수 있습니다. 사용자 이름, 사용자 유형, 이메일 주소, 사용자에게 할당된 역할 등 사용자에 대한 세부 정보를 볼 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *사용자*를 클릭합니다.

사용자 또는 그룹 삭제

특정 사용자가 Unified Manager에 액세스하지 못하도록 관리 서버 데이터베이스에서 하나 이상의 사용자를 삭제할 수 있습니다. 또한 그룹을 삭제하여 그룹 내 모든 사용자가 관리 서버에 더 이상 액세스할 수 없도록 할 수도 있습니다.

시작하기 전에

- 원격 그룹을 삭제할 때는 원격 그룹의 사용자에게 할당된 이벤트를 다시 할당해야 합니다.

로컬 사용자나 원격 사용자를 삭제하는 경우 해당 사용자에게 할당된 이벤트는 자동으로 할당 해제됩니다.

- 애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *사용자*를 클릭합니다.
2. 사용자 페이지에서 삭제하려는 사용자나 그룹을 선택한 다음 *삭제*를 클릭합니다.
3. *예*를 클릭하여 삭제를 확인하세요.

RBAC란 무엇인가

RBAC(역할 기반 액세스 제어)는 Active IQ Unified Manager 서버의 다양한 기능과 리소스에 누가 액세스할 수 있는지 제어하는 기능을 제공합니다.

역할 기반 액세스 제어는 무엇을 합니까?

역할 기반 액세스 제어(RBAC)를 사용하면 관리자가 역할을 정의하여 사용자 그룹을 관리할 수 있습니다. 특정 기능에 대한 액세스를 선택된 관리자에게만 제한해야 하는 경우 해당 관리자에 대한 관리자 계정을 설정해야 합니다. 관리자가 볼 수 있는 정보와 수행할 수 있는 작업을 제한하려면 생성한 관리자 계정에 역할을 적용해야 합니다.

관리 서버는 사용자 로그인 및 역할 권한에 RBAC를 사용합니다. 관리 서버의 관리자 사용자 액세스에 대한 기본 설정을 변경하지 않은 경우, 해당 설정을 보기 위해 로그인할 필요가 없습니다.

특정 권한이 필요한 작업을 시작하면 관리 서버에서 로그인하라는 메시지가 표시됩니다. 예를 들어, 관리자 계정을 만들려면 애플리케이션 관리자 계정 액세스 권한으로 로그인해야 합니다.

사용자 유형의 정의

사용자 유형은 사용자가 보유한 계정의 종류를 지정하며 여기에는 원격 사용자, 원격 그룹, 로컬 사용자, 데이터베이스 사용자, 유지 관리 사용자가 포함됩니다. 각 유형에는 고유한 역할이 있으며, 이 역할은 관리자 역할을 가진 사용자가 지정합니다.

Unified Manager 사용자 유형은 다음과 같습니다.

- 유지관리 사용자

Unified Manager의 초기 구성 중에 생성되었습니다. 그런 다음 유지 관리 사용자는 추가 사용자를 만들고 역할을 할당합니다. 유지 관리 사용자는 유지 관리 콘솔에 액세스할 수 있는 유일한 사용자이기도 합니다. Unified Manager가 Red Hat Enterprise Linux 시스템에 설치되면 유지 관리 사용자에게 "umadmin"이라는 사용자 이름이 지정됩니다.

- 로컬 사용자

Unified Manager UI에 액세스하고 유지 관리 사용자 또는 애플리케이션 관리자 역할이 있는 사용자가 제공한 역할에 따라 기능을 수행합니다.

- 원격 그룹

인증 서버에 저장된 자격 증명을 사용하여 Unified Manager UI에 액세스하는 사용자 그룹입니다. 이 계정의 이름은 인증 서버에 저장된 그룹 이름과 일치해야 합니다. 원격 그룹 내의 모든 사용자는 개별 사용자 자격 증명을 사용하여 Unified Manager UI에 액세스할 수 있습니다. 원격 그룹은 할당된 역할에 따라 기능을 수행할 수 있습니다.

- 원격 사용자

인증 서버에 저장된 자격 증명을 사용하여 Unified Manager UI에 액세스합니다. 원격 사용자는 유지 관리 사용자 또는 애플리케이션 관리자 역할이 있는 사용자가 부여한 역할에 따라 기능을 수행합니다.

- 데이터베이스 사용자

Unified Manager 데이터베이스의 데이터에 대한 읽기 전용 액세스 권한이 있으며, Unified Manager 웹 인터페이스나 유지 관리 콘솔에 대한 액세스 권한이 없으며, API 호출을 실행할 수 없습니다.

사용자 역할의 정의

유지 관리 사용자 또는 애플리케이션 관리자는 모든 사용자에게 역할을 할당합니다. 각 역할에는 특정 권한이 포함되어 있습니다. Unified Manager에서 수행할 수 있는 활동 범위는 할당된 역할과 해당 역할에 포함된 권한에 따라 달라집니다.

Unified Manager에는 다음과 같은 미리 정의된 사용자 역할이 포함되어 있습니다.

- 연산자

Unified Manager에서 수집한 스토리지 시스템 정보 및 기타 데이터(내역 및 용량 추세 포함)를 확인합니다. 이 역할을 통해 스토리지 운영자는 이벤트를 보고, 할당하고, 확인하고, 해결하고, 메모를 추가할 수 있습니다.

- 저장 관리자

Unified Manager 내에서 스토리지 관리 작업을 구성합니다. 이 역할을 통해 스토리지 관리자는 임계값을 구성하고 알림 및 기타 스토리지 관리 관련 옵션과 정책을 만들 수 있습니다.

- 애플리케이션 관리자

저장소 관리와 관련 없는 설정을 구성합니다. 이 역할을 통해 인증, SMTP, 네트워킹, AutoSupport 를 비롯한 사용자, 보안 인증서, 데이터베이스 액세스 및 관리 옵션을 관리할 수 있습니다.



Linux 시스템에 Unified Manager를 설치하면 애플리케이션 관리자 역할을 가진 초기 사용자는 자동으로 "umadmin"으로 지정됩니다.

- 통합 스키마

이 역할은 Unified Manager를 OnCommand Workflow Automation (WFA)과 통합하기 위해 Unified Manager 데이터베이스 뷰에 대한 읽기 전용 액세스를 제공합니다.

- 보고서 스키마

이 역할은 Unified Manager 데이터베이스에서 직접 보고 및 기타 데이터베이스 보기에 대한 읽기 전용 액세스를 허용합니다. 볼 수 있는 데이터베이스는 다음과 같습니다.

- 넷앱_모델_뷰
- 넷앱_성능
- 오컴
- ocum_report
- 오컴_리포트_버트
- 오피엠
- 스케일모니터

Unified Manager 사용자 역할 및 기능

할당된 사용자 역할에 따라 Unified Manager에서 수행할 수 있는 작업을 결정할 수 있습니다.

다음 표는 각 사용자 역할이 수행할 수 있는 기능을 보여줍니다.

기능	연산자	스토리지 관리자	애플리케이션 관리자	통합 스키마	보고서 스키마
저장 시스템 정보 보기	•	•	•	•	•
기록 및 용량 추세와 같은 다른 데이터를 확인하세요.	•	•	•	•	•
이벤트 보기, 할당 및 해결	•	•	•		
SVM 연결 및 리소스 풀과 같은 스토리지 서비스 개체 보기	•	•	•		
임계값 정책 보기	•	•	•		
SVM 연결 및 리소스 풀과 같은 스토리지 서비스 개체를 관리합니다.		•	•		
알림 정의		•	•		
저장소 관리 옵션 관리		•	•		

기능	연산자	스토리지 관리자	애플리케이션 관리자	통합 스키마	보고서 스키마
저장소 관리 정책 관리		•	•		
사용자 관리			•		
관리 옵션 관리			•		
임계값 정책 정의			•		
데이터베이스 액세스 관리			•		
WFA와의 통합을 관리하고 데이터베이스 뷰에 대한 액세스를 제공합니다.				•	
보고서 일정을 예약하고 저장하세요		•	•		
관리 작업에서 "수정" 작업 실행		•	•		
데이터베이스 뷰에 대한 읽기 전용 액세스 제공					•

SAML 인증 설정 관리

원격 인증 설정을 구성한 후에는 SAML(Security Assertion Markup Language) 인증을 활성화하여 원격 사용자가 Unified Manager 웹 UI에 액세스하기 전에 보안 ID 공급자(IdP)를 통해 인증을 받을 수 있도록 할 수 있습니다.

SAML 인증이 활성화된 후에는 원격 사용자만 Unified Manager 그래픽 사용자 인터페이스에 액세스할 수 있습니다. 로컬 사용자와 유지 관리 사용자는 UI에 액세스할 수 없습니다. 이 구성은 유지 관리 콘솔에 액세스하는 사용자에게 영향을 미치지 않습니다.

ID 공급자 요구 사항

모든 원격 사용자에게 대한 SAML 인증을 수행하기 위해 ID 공급자(IdP)를 사용하도록 Unified Manager를 구성하는 경우 Unified Manager에 대한 연결이 성공하려면 몇 가지 필수 구성

설정을 알고 있어야 합니다.

Unified Manager URI와 메타데이터를 IdP 서버에 입력해야 합니다. Unified ManagerSAML 인증 페이지에서 이 정보를 복사할 수 있습니다. Unified Manager는 SAML(Security Assertion Markup Language) 표준에서 서비스 공급자(SP)로 간주됩니다.

지원되는 암호화 표준

- 고급 암호화 표준(AES): AES-128 및 AES-256
- 보안 해시 알고리즘(SHA): SHA-1 및 SHA-256

검증된 ID 공급자

- 표어
- Active Directory 페더레이션 서비스(ADFS)

ADFS 구성 요구 사항

- Unified Manager가 이 신뢰 당사자 신뢰 항목에 대한 ADFS SAML 응답을 구문 분석하는 데 필요한 세 가지 클레임 규칙을 다음 순서대로 정의해야 합니다.

청구 규칙	가치
SAM 계정 이름	이름 ID
SAM 계정 이름	항아리:oid:0.9.2342.19200300.100.1.1
토큰 그룹 — 비정규 이름	항아리:oid:1.3.6.1.4.1.5923.1.5.1.1

- 인증 방법을 "양식 인증"으로 설정해야 합니다. 그렇지 않으면 사용자가 Unified Manager에서 로그아웃할 때 오류가 발생할 수 있습니다. 다음 단계를 따르세요.
 - a. ADFS 관리 콘솔을 엽니다.
 - b. 왼쪽 트리 보기에서 인증 정책 폴더를 클릭합니다.
 - c. 오른쪽의 작업에서 글로벌 기본 인증 정책 편집을 클릭합니다.
 - d. 기본 "Windows 인증" 대신 "폼 인증"으로 인트라넷 인증 방법을 설정합니다.
- 어떤 경우에는 Unified Manager 보안 인증서에 CA 서명이 있는 경우 IdP를 통한 로그인에 거부됩니다. 이 문제를 해결하는 방법은 두 가지가 있습니다.
 - 링크에 명시된 지침에 따라 체인된 CA 인증서와 관련된 신뢰 당사자에 대한 ADFS 서버에서 해지 확인을 비활성화합니다.

"신뢰 당사자 신뢰에 따른 해지 확인 비활성화"

- Unified Manager 서버 인증서 요청에 서명하려면 CA 서버가 ADFS 서버 내에 있어야 합니다.

기타 구성 요구 사항

- Unified Manager 클록 오차는 5분으로 설정되어 있으므로 IdP 서버와 Unified Manager 서버 간의 시간 차이는 5분을 넘을 수 없으며, 5분을 넘으면 인증이 실패합니다.

SAML 인증 활성화

원격 사용자가 Unified Manager 웹 UI에 액세스하기 전에 보안 ID 공급자(IdP)를 통해 인증을 받을 수 있도록 SAML(Security Assertion Markup Language) 인증을 활성화할 수 있습니다.

시작하기 전에

- 원격 인증을 구성하고 성공했는지 확인해야 합니다.
- 애플리케이션 관리자 역할이 있는 원격 사용자 또는 원격 그룹을 하나 이상 만들어야 합니다.
- ID 공급자(IdP)는 Unified Manager에서 지원되어야 하며 구성되어야 합니다.
- IdP URL과 메타데이터가 있어야 합니다.
- IdP 서버에 액세스할 수 있어야 합니다.

Unified Manager에서 SAML 인증을 활성화한 후에는 IdP가 Unified Manager 서버 호스트 정보로 구성될 때까지 사용자는 그래픽 사용자 인터페이스에 액세스할 수 없습니다. 따라서 구성 과정을 시작하기 전에 연결의 두 부분을 모두 완료할 준비가 되어 있어야 합니다. IdP는 Unified Manager를 구성하기 전이나 후에 구성할 수 있습니다.

SAML 인증이 활성화된 후에는 원격 사용자만 Unified Manager 그래픽 사용자 인터페이스에 액세스할 수 있습니다. 로컬 사용자와 유지 관리 사용자는 UI에 액세스할 수 없습니다. 이 구성은 유지 관리 콘솔, Unified Manager 명령 또는 ZAPI에 액세스하는 사용자에게 영향을 미치지 않습니다.



이 페이지에서 SAML 구성을 완료하면 Unified Manager가 자동으로 다시 시작됩니다.

단계

1. 왼쪽 탐색 창에서 일반 > *SAML 인증*을 클릭합니다.
2. **SAML** 인증 사용 확인란을 선택합니다.

IdP 연결을 구성하는 데 필요한 필드가 표시됩니다.

3. Unified Manager 서버를 IdP 서버에 연결하는 데 필요한 IdP URI와 IdP 메타데이터를 입력합니다.

Unified Manager 서버에서 IdP 서버에 직접 액세스할 수 있는 경우 IdP URI를 입력한 후 **IdP** 메타데이터 가져오기 버튼을 클릭하면 IdP 메타데이터 필드가 자동으로 채워집니다.

4. Unified Manager 호스트 메타데이터 URI를 복사하거나 호스트 메타데이터를 XML 텍스트 파일에 저장합니다.

이때 이 정보를 사용하여 IdP 서버를 구성할 수 있습니다.

5. *저장*을 클릭하세요.

구성을 완료하고 Unified Manager를 다시 시작할 것인지 확인하는 메시지 상자가 표시됩니다.

6. *확인 및 로그아웃*을 클릭하면 Unified Manager가 다시 시작됩니다.

다음에 권한이 있는 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 하면 Unified Manager 로그인 페이지 대신 IdP 로그인 페이지에 자격 증명을 입력하게 됩니다.

아직 완료되지 않았다면 IdP에 액세스하여 Unified Manager 서버 URI와 메타데이터를 입력하여 구성을 완료하세요.



ADFS를 ID 공급자로 사용하는 경우 Unified Manager GUI는 ADFS 시간 초과를 준수하지 않으며 Unified Manager 세션 시간 초과에 도달할 때까지 계속 작동합니다. 일반 > 기능 설정 > *비활성 시간 초과*를 클릭하면 GUI 세션 시간 초과를 변경할 수 있습니다.

SAML 인증에 사용되는 ID 공급자 변경

Unified Manager가 원격 사용자를 인증하는 데 사용하는 ID 공급자(IdP)를 변경할 수 있습니다.

시작하기 전에

- IdP URL과 메타데이터가 있어야 합니다.
- IdP에 액세스할 수 있어야 합니다.

새로운 IdP는 Unified Manager를 구성하기 전이나 후에 구성할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *SAML 인증*을 클릭합니다.
2. Unified Manager 서버를 IdP에 연결하는 데 필요한 새로운 IdP URI와 IdP 메타데이터를 입력합니다.

Unified Manager 서버에서 IdP에 직접 액세스할 수 있는 경우 IdP URL을 입력한 후 **IdP** 메타데이터 가져오기 버튼을 클릭하면 IdP 메타데이터 필드가 자동으로 채워집니다.

3. Unified Manager 메타데이터 URI를 복사하거나 메타데이터를 XML 텍스트 파일에 저장합니다.
4. *구성 저장*을 클릭합니다.

구성을 변경할 것인지 확인하는 메시지 상자가 표시됩니다.

5. *OK*를 클릭하세요.

새로운 IdP에 액세스하여 Unified Manager 서버 URI와 메타데이터를 입력하여 구성을 완료합니다.

다음에 권한이 있는 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 하면 이전 IdP 로그인 페이지 대신 새 IdP 로그인 페이지에 자격 증명을 입력하게 됩니다.

Unified Manager 보안 인증서 변경 후 SAML 인증 설정 업데이트

Unified Manager 서버에 설치된 HTTPS 보안 인증서를 변경하려면 SAML 인증 구성 설정을 업데이트해야 합니다. 호스트 시스템의 이름을 바꾸거나, 호스트 시스템에 새 IP 주소를 할당하거나, 시스템의 보안 인증서를 수동으로 변경하면 인증서가 업데이트됩니다.

보안 인증서가 변경되고 Unified Manager 서버가 다시 시작되면 SAML 인증이 작동하지 않으며 사용자는 Unified Manager 그래픽 인터페이스에 액세스할 수 없습니다. 사용자 인터페이스에 대한 액세스를 다시 활성화하려면 IdP 서버와 Unified Manager 서버 모두에서 SAML 인증 설정을 업데이트해야 합니다.

단계

1. 유지 관리 콘솔에 로그인합니다.
2. 메인 메뉴*에서 ***SAML** 인증 비활성화 옵션에 대한 번호를 입력합니다.

SAML 인증을 비활성화하고 Unified Manager를 다시 시작할 것인지 확인하는 메시지가 표시됩니다.

3. 업데이트된 FQDN 또는 IP 주소를 사용하여 Unified Manager 사용자 인터페이스를 시작하고, 브라우저에서 업데이트된 서버 인증서를 수락한 후 유지 관리 사용자 자격 증명을 사용하여 로그인합니다.
4. 설정/인증 페이지에서 **SAML** 인증 탭을 선택하고 IdP 연결을 구성합니다.
5. Unified Manager 호스트 메타데이터 URI를 복사하거나 호스트 메타데이터를 XML 텍스트 파일에 저장합니다.
6. *저장*을 클릭하세요.

구성을 완료하고 Unified Manager를 다시 시작할 것인지 확인하는 메시지 상자가 표시됩니다.

7. *확인 및 로그아웃*을 클릭하면 Unified Manager가 다시 시작됩니다.
8. IdP 서버에 액세스하여 Unified Manager 서버 URI와 메타데이터를 입력하여 구성을 완료합니다.

ID 공급자	구성 단계
ADFS	a. ADFS 관리 GUI에서 기존 신뢰 당사자 신뢰 항목을 삭제합니다. b. 다음을 사용하여 새로운 신뢰 당사자 신뢰 항목을 추가합니다. <code>saml_sp_metadata.xml</code> 업데이트된 Unified Manager 서버에서. c. Unified Manager가 이 신뢰 당사자 신뢰 항목에 대한 ADFS SAML 응답을 구문 분석하는 데 필요한 세 가지 클레임 규칙을 정의합니다. d. ADFS Windows 서비스를 다시 시작합니다.
표어	a. Unified Manager 서버의 새 FQDN을 업데이트합니다. <code>attribute-filter.xml</code> 그리고 <code>relying-party.xml</code> 파일. b. Apache Tomcat 웹 서버를 다시 시작하고 포트 8005가 온라인이 될 때까지 기다립니다.

9. Unified Manager에 로그인하여 IdP를 통해 SAML 인증이 예상대로 작동하는지 확인하세요.

SAML 인증 비활성화

Unified Manager 웹 UI에 로그인하기 전에 보안 ID 공급자(IdP)를 통해 원격 사용자를 인증하는 것을 중지하려면 SAML 인증을 비활성화할 수 있습니다. SAML 인증이 비활성화되면 Active Directory나 LDAP와 같은 구성된 디렉터리 서비스 공급자가 로그인 인증을 수행합니다.

SAML 인증을 비활성화하면 구성된 원격 사용자 외에도 로컬 사용자와 유지 관리 사용자가 그래픽 사용자 인터페이스에 액세스할 수 있습니다.

그래픽 사용자 인터페이스에 액세스할 수 없는 경우 Unified Manager 유지 관리 콘솔을 사용하여 SAML 인증을

비활성화할 수도 있습니다.



SAML 인증이 비활성화되면 Unified Manager가 자동으로 다시 시작됩니다.

단계

1. 왼쪽 탐색 창에서 일반 > *SAML 인증*을 클릭합니다.
2. **SAML** 인증 사용 체크박스의 선택을 취소합니다.
3. *저장*을 클릭하세요.

구성을 완료하고 Unified Manager를 다시 시작할 것인지 확인하는 메시지 상자가 표시됩니다.

4. *확인 및 로그아웃*을 클릭하면 Unified Manager가 다시 시작됩니다.

다음에 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 하면 IdP 로그인 페이지 대신 Unified Manager 로그인 페이지에 자격 증명을 입력하게 됩니다.

IdP에 액세스하여 Unified Manager 서버 URI와 메타데이터를 삭제합니다.

유지 관리 콘솔에서 **SAML** 인증 비활성화

Unified Manager GUI에 액세스할 수 없는 경우 유지 관리 콘솔에서 SAML 인증을 비활성화해야 할 수도 있습니다. 이는 구성이 잘못되었거나 IdP에 액세스할 수 없는 경우 발생할 수 있습니다.

시작하기 전에

유지 관리 사용자로서 유지 관리 콘솔에 액세스할 수 있어야 합니다.

SAML 인증이 비활성화되면 Active Directory나 LDAP와 같은 구성된 디렉터리 서비스 공급자가 로그인 인증을 수행합니다. 구성된 원격 사용자 외에도 로컬 사용자와 유지 관리 사용자는 그래픽 사용자 인터페이스에 액세스할 수 있습니다.

UI의 설정/인증 페이지에서 SAML 인증을 비활성화할 수도 있습니다.



SAML 인증이 비활성화되면 Unified Manager가 자동으로 다시 시작됩니다.

단계

1. 유지 관리 콘솔에 로그인합니다.
2. 메인 메뉴*에서 ***SAML** 인증 비활성화 옵션에 대한 번호를 입력합니다.

SAML 인증을 비활성화하고 Unified Manager를 다시 시작할 것인지 확인하는 메시지가 표시됩니다.

3. *y*를 입력한 다음 Enter 키를 누르면 Unified Manager가 다시 시작됩니다.

다음에 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 하면 IdP 로그인 페이지 대신 Unified Manager 로그인 페이지에 자격 증명을 입력하게 됩니다.

필요한 경우 IdP에 액세스하여 Unified Manager 서버 URL과 메타데이터를 삭제합니다.

SAML 인증 페이지

SAML 인증 페이지를 사용하면 Unified Manager가 보안 ID 공급자(IdP)를 통해 SAML을 사용하여 원격 사용자를 인증하도록 구성한 후 Unified Manager 웹 UI에 로그인할 수 있습니다.

- SAML 구성을 만들거나 수정하려면 애플리케이션 관리자 역할이 있어야 합니다.
- 원격 인증을 구성해야 합니다.
- 최소한 하나의 원격 사용자 또는 원격 그룹을 구성해야 합니다.

원격 인증과 원격 사용자가 구성된 후 SAML 인증 사용 확인란을 선택하여 보안 ID 공급자를 사용하여 인증을 활성화할 수 있습니다.

- **IdP URI**

Unified Manager 서버에서 IdP에 액세스하기 위한 URI입니다. 예시 URI는 아래와 같습니다.

ADFS 예제 URI:

```
https://win2016-dc.ntap2016.local/federationmetadata/2007-06/federationmetadata.xml
```

Shibboleth 예시 URI:

```
https://centos7.ntap2016.local/idp/shibboleth
```

- **IdP 메타데이터**

XML 형식의 IdP 메타데이터입니다.

Unified Manager 서버에서 IdP URL에 접근할 수 있는 경우 **IdP** 메타데이터 가져오기 버튼을 클릭하여 이 필드를 채울 수 있습니다.

- **호스트 시스템(FQDN)**

설치 중에 정의된 Unified Manager 호스트 시스템의 FQDN입니다. 필요한 경우 이 값을 변경할 수 있습니다.

- **호스트 URI**

IdP에서 Unified Manager 호스트 시스템에 액세스하기 위한 URI입니다.

- **호스트 메타데이터**

XML 형식의 호스트 시스템 메타데이터입니다.

인증 관리

Unified Manager 서버에서 LDAP 또는 Active Directory를 사용하여 인증을 활성화하고 원격 사용자를 인증하기 위해 서버와 함께 작동하도록 구성할 수 있습니다.

원격 인증 활성화, 인증 서비스 설정 및 인증 서버 추가에 대한 자세한 내용은 이전 섹션인 *Unified Manager를

구성하여 알림 보내기*를 참조하세요.

인증 서버 편집

Unified Manager 서버가 인증 서버와 통신하는 데 사용하는 포트를 변경할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. 중첩 그룹 조회 비활성화 상자를 선택하세요.
3. 인증 서버 영역에서 편집하려는 인증 서버를 선택한 다음 *편집*을 클릭합니다.
4. 인증 서버 편집 대화 상자에서 포트 세부 정보를 편집합니다.
5. *저장*을 클릭하세요.

인증 서버 삭제

Unified Manager 서버가 인증 서버와 통신하는 것을 방지하려면 인증 서버를 삭제할 수 있습니다. 예를 들어, 관리 서버가 통신하는 인증 서버를 변경하려는 경우 인증 서버를 삭제하고 새 인증 서버를 추가할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

인증 서버를 삭제하면 인증 서버의 원격 사용자나 그룹은 더 이상 Unified Manager에 액세스할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. 삭제하려는 인증 서버를 하나 이상 선택한 다음 *삭제*를 클릭합니다.
3. *예*를 클릭하여 삭제 요청을 확인하세요.

보안 연결 사용 옵션이 활성화된 경우 인증 서버와 연결된 인증서가 인증 서버와 함께 삭제됩니다.

Active Directory 또는 OpenLDAP를 통한 인증

관리 서버에서 원격 인증을 활성화하고 관리 서버가 인증 서버와 통신하도록 구성하여 인증 서버 내의 사용자가 Unified Manager에 액세스할 수 있도록 할 수 있습니다.

다음 사전 정의된 인증 서비스 중 하나를 사용하거나 고유한 인증 서비스를 지정할 수 있습니다.

- 마이크로소프트 액티브 디렉토리



Microsoft Lightweight Directory Services를 사용할 수 없습니다.

- 오픈LDAP

필요한 인증 서비스를 선택하고 적절한 인증 서버를 추가하여 인증 서버의 원격 사용자가 Unified Manager에 액세스할 수 있도록 할 수 있습니다. 원격 사용자 또는 그룹의 자격 증명은 인증 서버에서 유지 관리됩니다. 관리 서버는 LDAP(Lightweight Directory Access Protocol)를 사용하여 구성된 인증 서버 내에서 원격 사용자를 인증합니다.

Unified Manager에서 생성된 로컬 사용자의 경우, 관리 서버는 사용자 이름과 비밀번호의 자체 데이터베이스를 유지 관리합니다. 관리 서버는 인증을 수행하며 인증을 위해 Active Directory나 OpenLDAP를 사용하지 않습니다.

감사 로깅

감사 로그를 사용하면 감사 로그가 손상되었는지 감지할 수 있습니다. 사용자가 수행하는 모든 활동은 모니터링되어 감사 로그에 기록됩니다. 감사는 Active IQ Unified Manager 의 모든 사용자 인터페이스와 공개적으로 노출된 API 기능에 대해 수행됩니다.

*감사 로그: 파일 보기*를 사용하면 Active IQ Unified Manager 에서 사용 가능한 모든 감사 로그 파일을 보고 액세스할 수 있습니다. 감사 로그: 파일 보기의 파일은 생성 날짜를 기준으로 나열됩니다. 이 보기에서는 시스템에 설치 또는 업그레이드한 이후 현재까지 캡처된 모든 감사 로그에 대한 정보가 표시됩니다. Unified Manager에서 작업을 수행할 때마다 정보가 업데이트되어 로그에서 사용할 수 있습니다. 각 로그 파일의 상태는 "파일 무결성 상태" 속성을 사용하여 캡처되며, 이 속성은 로그 파일의 변조 또는 삭제를 감지하기 위해 적극적으로 모니터링됩니다. 감사 로그가 시스템에서 사용 가능한 경우 감사 로그는 다음 상태 중 하나를 가질 수 있습니다.

상태	설명
활동적인	현재 로그가 기록되고 있는 파일입니다.
정상	비활성화되어 압축되어 시스템에 저장된 파일입니다.
변조됨	사용자가 수동으로 파일을 편집하여 손상된 파일입니다.
수동 삭제	권한이 있는 사용자에 의해 삭제된 파일입니다.
롤오버 삭제	롤링 구성 정책에 따라 롤링 오프로 인해 삭제된 파일입니다.
예상치 못한 삭제	알 수 없는 이유로 삭제된 파일입니다.

감사 로그 페이지에는 다음과 같은 명령 단추가 포함되어 있습니다.

- 구성
- 삭제
- 다운로드

삭제 버튼을 사용하면 감사 로그 보기에 나열된 감사 로그를 삭제할 수 있습니다. 감사 로그를 삭제할 수 있으며, 선택적으로 파일을 삭제하는 이유를 제공할 수 있습니다. 이는 나중에 유효한 삭제를 판별하는 데 도움이 됩니다. REASON 옆에는 삭제 작업을 수행한 사용자의 이름과 이유가 나열됩니다.



로그 파일을 삭제하면 시스템에서 파일이 삭제되지만 DB 테이블의 항목은 삭제되지 않습니다.

감사 로그 섹션의 다운로드 버튼을 사용하여 Active IQ Unified Manager 에서 감사 로그를 다운로드하고 감사 로그 파일을 내보낼 수 있습니다. "NORMAL" 또는 "TAMPERED"로 표시된 파일은 압축 파일로 다운로드됩니다. .gzip 체재.

감사 로그 파일은 주기적으로 보관되며 참조를 위해 데이터베이스에 저장됩니다. 보관하기 전에 감사 로그는 보안과 무결성을 유지하기 위해 디지털 서명됩니다.

전체 AutoSupport 번들이 생성되면 지원 번들에는 보관된 감사 로그 파일과 활성 감사 로그 파일이 모두 포함됩니다. 하지만 가벼운 지원 번들이 생성되면 활성 감사 로그만 포함됩니다. 보관된 감사 로그는 포함되지 않습니다.

감사 로그 구성

감사 로그 섹션의 구성 버튼을 사용하면 감사 로그 파일에 대한 롤링 정책을 구성하고 감사 로그에 대한 원격 로깅을 활성화할 수 있습니다.

시스템에 저장하려는 데이터의 양과 빈도에 따라 최대 파일 크기 및 감사 로그 보존 일수 값을 설정할 수 있습니다. 총 감사 로그 크기 필드의 값은 시스템에 있는 총 감사 로그 데이터의 크기입니다. 롤오버 정책은 감사 로그 보존 일수, 최대 파일 크기, 총 감사 로그 크기 필드의 값에 따라 결정됩니다. 감사 로그 백업의 크기가 총 감사 로그 크기*에 구성된 값에 도달하면 먼저 보관된 파일이 삭제됩니다. 즉, 가장 오래된 파일이 삭제됩니다. 하지만 파일 항목은 데이터베이스에 계속 남아 있으며 "롤오버 삭제"로 표시됩니다. *감사 로그 보존 일수 값은 감사 로그 파일이 보존되는 일 수입니다. 이 필드에 설정된 값보다 오래된 파일은 롤오버됩니다.

단계

1. 감사 로그 > > *구성*을 클릭합니다.
2. 최대 파일 크기, 총 감사 로그 크기, *감사 로그 보존 일수*에 값을 입력합니다.

원격 로깅을 활성화하려면 *원격 로깅 활성화*를 선택해야 합니다. /// 2025-6-11, OTHERDOC-133

감사 로그의 원격 로깅 활성화

원격 감사 로깅을 활성화하려면 감사 로그 구성 대화 상자에서 원격 로깅 활성화 확인란을 선택하세요. 이 기능을 사용하면 감사 로그를 원격 Syslog 서버로 전송할 수 있습니다. 이를 통해 공간 제약이 있을 때에도 감사 로그를 관리할 수 있습니다.

감사 로그의 원격 로깅은 Active IQ Unified Manager 서버의 감사 로그 파일이 변조된 경우 변조 방지 백업을 제공합니다.

단계

1. 감사 로그 구성 대화 상자에서 원격 로깅 사용 확인란을 선택합니다.
- 원격 로깅을 구성하기 위한 추가 필드가 표시됩니다.
2. 연결하려는 원격 서버의 *호스트 이름*과 *포트*를 입력하세요.
 3. 서버 **CA** 인증서 필드에서 *찾아보기*를 클릭하여 대상 서버의 공개 인증서를 선택합니다.

인증서는 다음에 업로드되어야 합니다. .pem 체재. 이 인증서는 대상 Syslog 서버에서 얻어야 하며 만료되어서는 안 됩니다. 인증서에는 선택된 "호스트 이름"이 포함되어야 합니다. SubjectAltName (SAN) 속성.

4. 다음 필드에 값을 입력하세요: **CHARSET, CONNECTION TIMEOUT, RECONNECTION DELAY.**

이러한 필드의 값은 밀리초 단위여야 합니다.

5. **FORMAT** 및 **PROTOCOL** 필드에서 필요한 Syslog 형식과 TLS 프로토콜 버전을 선택합니다.

6. 대상 Syslog 서버에 인증서 기반 인증이 필요한 경우 클라이언트 인증 사용 확인란을 선택합니다.

감사 로그 구성을 저장하기 전에 클라이언트 인증 인증서를 다운로드하여 Syslog 서버에 업로드해야 합니다. 그렇지 않으면 연결이 실패합니다. Syslog 서버 유형에 따라 클라이언트 인증 인증서 해시를 만들어야 할 수도 있습니다.

예: syslog-ng는 다음 명령을 사용하여 인증서의 <해시>를 생성해야 합니다. `openssl x509 -noout -hash -in cert.pem` 그런 다음 클라이언트 인증 인증서를 <hash> .0 ...

7. *저장*을 클릭하여 서버와의 연결을 구성하고 원격 로깅을 활성화하세요.

감사 로그 페이지로 리디렉션됩니다.



연결 시간 초과 값은 구성에 영향을 줄 수 있습니다. 정의된 값보다 구성에 응답하는 데 시간이 오래 걸리는 경우 연결 오류로 인해 구성이 실패할 수 있습니다. 연결을 성공적으로 설정하려면 연결 시간 초과 값을 늘리고 구성을 다시 시도하세요.

원격 인증 페이지

원격 인증 페이지를 사용하여 Unified Manager가 인증 서버와 통신하여 Unified Manager 웹 UI에 로그인을 시도하는 원격 사용자를 인증하도록 구성할 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

원격 인증 사용 확인란을 선택하면 인증 서버를 사용하여 원격 인증을 사용할 수 있습니다.

- 인증 서비스

Active Directory, OpenLDAP 등의 디렉터리 서비스 공급자에서 사용자를 인증하도록 관리 서버를 구성하거나 고유한 인증 메커니즘을 지정할 수 있습니다. 원격 인증을 활성화한 경우에만 인증 서비스를 지정할 수 있습니다.

- 액티브 디렉토리

- 관리자 이름

인증 서버의 관리자 이름을 지정합니다.

- 비밀번호

인증 서버에 접근하기 위한 비밀번호를 지정합니다.

- 기본 고유 이름

인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어, 인증 서버의 도메인 이름이 `+ou@domain.com+`이면 기본 고유 이름은 `*cn=ou,dc=domain,dc=com*`입니다.

- 중첩된 그룹 조회 비활성화

중첩 그룹 조회 옵션을 활성화할지 비활성화할지 지정합니다. 기본적으로 이 옵션은 비활성화되어 있습니다. Active Directory를 사용하는 경우 중첩 그룹에 대한 지원을 비활성화하여 인증 속도를 높일 수 있습니다.

- 보안 연결 사용

인증 서버와 통신하는 데 사용되는 인증 서비스를 지정합니다.

- **오픈LDAP**

- 고유 이름 바인딩

인증 서버에서 원격 사용자를 찾기 위해 기본 고유 이름과 함께 사용되는 바인드 고유 이름을 지정합니다.

- 바인드 비밀번호

인증 서버에 접근하기 위한 비밀번호를 지정합니다.

- 기본 고유 이름

인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어, 인증 서버의 도메인 이름이 `+ou@domain.com+`이면 기본 고유 이름은 `*cn=ou,dc=domain,dc=com*`입니다.

- 보안 연결 사용

LDAP 인증 서버와 통신하는 데 보안 LDAP가 사용됨을 지정합니다.

- **기타**

- 고유 이름 바인딩

구성한 인증 서버에서 원격 사용자를 찾기 위해 기본 고유 이름과 함께 사용되는 바인드 고유 이름을 지정합니다.

- 바인드 비밀번호

인증 서버에 접근하기 위한 비밀번호를 지정합니다.

- 기본 고유 이름

인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어, 인증 서버의 도메인 이름이 `+ou@domain.com+`이면 기본 고유 이름은 `*cn=ou,dc=domain,dc=com*`입니다.

- 프로토콜 버전

인증 서버에서 지원하는 LDAP(Lightweight Directory Access Protocol) 버전을 지정합니다. 프로토콜 버전을 자동으로 감지할지 아니면 버전을 2 또는 3으로 설정할지 지정할 수 있습니다.

- 사용자 이름 속성

관리 서버에서 인증할 사용자 로그인 이름이 포함된 인증 서버의 속성 이름을 지정합니다.

- 그룹 멤버십 속성

사용자 인증 서버에 지정된 속성과 값을 기반으로 원격 사용자에게 관리 서버 그룹 멤버십을 할당하는 값을 지정합니다.

- 우지드

원격 사용자가 인증 서버의 GroupOfUniqueNames 개체의 멤버로 포함된 경우, 이 옵션을 사용하면 해당 GroupOfUniqueNames 개체의 지정된 속성을 기반으로 원격 사용자에게 관리 서버 그룹 멤버십을 할당할 수 있습니다.

- 중첩된 그룹 조회 비활성화

중첩 그룹 조회 옵션을 활성화할지 비활성화할지 지정합니다. 기본적으로 이 옵션은 비활성화되어 있습니다. Active Directory를 사용하는 경우 중첩 그룹에 대한 지원을 비활성화하여 인증 속도를 높일 수 있습니다.

- 회원

인증 서버가 그룹의 개별 멤버에 대한 정보를 저장하는 데 사용하는 속성 이름을 지정합니다.

- 사용자 객체 클래스

원격 인증 서버에서 사용자의 객체 클래스를 지정합니다.

- 그룹 객체 클래스

원격 인증 서버의 모든 그룹의 객체 클래스를 지정합니다.



Member, User Object Class, Group Object Class 특성에 입력한 값은 Active Directory, OpenLDAP, LDAP 구성에 추가된 값과 동일해야 합니다. 그렇지 않으면 인증이 실패할 수 있습니다.

- 보안 연결 사용

인증 서버와 통신하는 데 사용되는 인증 서비스를 지정합니다.



인증 서비스를 수정하려면 기존 인증 서버를 삭제하고 새 인증 서버를 추가해야 합니다.

인증 서버 영역

인증 서버 영역에는 관리 서버가 원격 사용자를 찾아 인증하기 위해 통신하는 인증 서버가 표시됩니다. 원격 사용자 또는 그룹의 자격 증명은 인증 서버에서 유지 관리됩니다.

- 명령 버튼

인증 서버를 추가, 편집 또는 삭제할 수 있습니다.

- 추가하다

인증 서버를 추가할 수 있습니다.

추가하려는 인증 서버가 고가용성 쌍(동일한 데이터베이스 사용)의 일부인 경우 파트너 인증 서버도 추가할 수

있습니다. 이를 통해 인증 서버 중 하나에 연결할 수 없을 때 관리 서버가 파트너와 통신할 수 있습니다.

- 편집하다

선택한 인증 서버의 설정을 편집할 수 있습니다.

- 삭제

선택한 인증 서버를 삭제합니다.

- 이름 또는 **IP** 주소

관리 서버에서 사용자를 인증하는 데 사용되는 인증 서버의 호스트 이름이나 IP 주소를 표시합니다.

- 포트

인증 서버의 포트 번호를 표시합니다.

- 테스트 인증

이 버튼은 원격 사용자나 그룹을 인증하여 인증 서버 구성을 검증합니다.

테스트 시 사용자 이름만 지정하면 관리 서버는 인증 서버에서 원격 사용자를 검색하지만 사용자를 인증하지는 않습니다. 사용자 이름과 비밀번호를 모두 지정하면 관리 서버는 원격 사용자를 검색하고 인증합니다.

원격 인증이 비활성화된 경우 인증을 테스트할 수 없습니다.

보안 인증서 관리

Unified Manager 서버에서 HTTPS를 구성하여 보안 연결을 통해 클러스터를 모니터링하고 관리할 수 있습니다.

HTTPS 보안 인증서 보기

HTTPS 인증서 세부 정보를 브라우저에서 검색된 인증서와 비교하여 브라우저의 Unified Manager에 대한 암호화된 연결이 가로채지 않는지 확인할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

인증서를 보면 재생성된 인증서의 내용을 확인하거나 Unified Manager에 액세스할 수 있는 주체 대체 이름(SAN)을 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *HTTPS 인증서*를 클릭합니다.

HTTPS 인증서는 페이지 상단에 표시됩니다.

HTTPS 인증서 페이지에 표시된 것보다 보안 인증서에 대한 더 자세한 정보를 보려면 브라우저에서 연결 인증서를 볼

수 있습니다.

HTTPS 인증서 서명 요청 다운로드

현재 HTTPS 보안 인증서에 대한 인증서 서명 요청서를 다운로드하여 인증 기관에 파일을 제공하여 서명을 받을 수 있습니다. CA 서명 인증서는 중간자 공격을 방지하는 데 도움이 되며 자체 서명 인증서보다 더 나은 보안 기능을 제공합니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *HTTPS 인증서*를 클릭합니다.
2. *HTTPS 인증서 서명 요청 다운로드*를 클릭합니다.
3. 저장하다 <hostname>.csr 파일.

인증 기관에 파일을 제공하여 서명을 받은 다음, 서명된 인증서를 설치할 수 있습니다.

CA 서명 및 반환된 HTTPS 인증서 설치

인증 기관에서 서명하고 반환한 후에 보안 인증서를 업로드하고 설치할 수 있습니다. 업로드하고 설치하는 파일은 기존 자체 서명 인증서의 서명된 버전이어야 합니다. CA 서명 인증서는 중간자 공격을 방지하는 데 도움이 되며 자체 서명 인증서보다 더 나은 보안을 제공합니다.

*무엇을 시작하기 전에

다음 작업을 완료했어야 합니다.

- 인증서 서명 요청 파일을 다운로드하고 인증 기관에서 서명을 받았습니다.
- PEM 형식으로 인증서 체인을 저장했습니다.
- Unified Manager 서버 인증서부터 루트 서명 인증서까지 체인의 모든 인증서가 포함되었으며 현재 존재하는 모든 중간 인증서도 포함됩니다.

애플리케이션 관리자 역할이 있어야 합니다.



CSR이 생성된 인증서의 유효 기간이 397일을 초과하는 경우 CA는 인증서에 서명하고 반환하기 전에 유효 기간을 397일로 줄입니다.

단계

1. 왼쪽 탐색 창에서 일반 > *HTTPS 인증서*를 클릭합니다.
2. *HTTPS 인증서 설치*를 클릭합니다.
3. 표시되는 대화 상자에서 *파일 선택...*을 클릭하여 업로드할 파일을 찾습니다.
4. 파일을 선택한 후 *설치*를 클릭하여 파일을 설치합니다.

자세한 내용은 다음을 참조하세요. ["외부 도구를 사용하여 생성된 HTTPS 인증서 설치"](#).

인증서 체인 예시

다음 예에서는 인증서 체인 파일이 어떻게 나타나는지 보여줍니다.

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

외부 도구를 사용하여 생성된 HTTPS 인증서 설치

OpenSSL, BoringSSL, LetsEncrypt와 같은 외부 도구를 사용하여 생성된 자체 서명 또는 CA 서명 인증서를 설치할 수 있습니다.

이러한 인증서는 외부에서 생성된 공개-개인 키 쌍이므로 인증서 체인과 함께 개인 키를 로드해야 합니다. 허용되는 키 쌍 알고리즘은 "RSA"와 "EC"입니다. **HTTPS** 인증서 설치 옵션은 일반 섹션의 HTTPS 인증서 페이지에서 사용할 수 있습니다. 업로드하는 파일은 다음 입력 형식이어야 합니다.

1. Active IQ Unified Manager 호스트에 속하는 서버의 개인 키
2. 개인키와 일치하는 서버의 인증서
3. 위 인증서에 서명하는 데 사용되는 루트까지의 역방향 CA 인증서

EC 키 쌍으로 인증서를 로드하기 위한 형식

허용되는 곡선은 "prime256v1"과 "secp384r1"입니다. 외부에서 생성된 EC 쌍이 포함된 인증서 샘플:

```
-----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```



```

-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----

```

RSA 키 쌍으로 인증서를 로드하기 위한 형식

호스트 인증서에 속한 RSA 키 쌍에 허용되는 키 크기는 2048, 3072 및 4096입니다. 외부에서 생성된 *RSA 키 쌍*이 있는 인증서:

```

-----BEGIN RSA PRIVATE KEY-----
<RSA private key of Server>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----

```

인증서를 업로드한 후 변경 사항을 적용하려면 Active IQ Unified Manager 인스턴스를 다시 시작해야 합니다.

외부에서 생성된 인증서를 업로드하는 동안 확인

시스템은 외부 도구를 사용하여 생성된 인증서를 업로드하는 동안 검사를 수행합니다. 검사 중 하나라도 실패하면 인증서가 거부됩니다. 제품 내 CSR에서 생성된 인증서와 외부 도구를 사용하여 생성된 인증서에 대한 검증도 포함됩니다.

- 입력의 개인 키는 입력의 호스트 인증서와 대조하여 검증됩니다.
- 호스트 인증서의 일반 이름(CN)은 호스트의 FQDN과 비교됩니다.

- 호스트 인증서의 일반 이름(CN)은 비어 있거나 공백이어서는 안 되며, localhost로 설정해서는 안 됩니다.
- 유효 시작일은 미래일 수 없으며, 인증서의 유효 만료일은 과거일 수 없습니다.
- 중간 CA 또는 CA가 존재하는 경우 인증서의 유효 시작 날짜는 미래가 아니어야 하며, 유효 만료 날짜도 과거가 아니어야 합니다.



입력된 개인 키는 암호화되어서는 안 됩니다. 암호화된 개인 키가 있는 경우 시스템에서 해당 키가 거부됩니다.

예제 1

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

예제 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

예제 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

인증서 설치에 실패하면 기술 자료(KB) 문서를

참조하세요. https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager가 외부에서 생성된 인증서를 설치하지 못했습니다."^]

인증서 관리를 위한 페이지 설명

HTTPS 인증서 페이지를 사용하여 현재 보안 인증서를 보고 새로운 HTTPS 인증서를 생성할 수 있습니다.

HTTPS 인증서 페이지

HTTPS 인증서 페이지에서는 현재 보안 인증서를 보고, 인증서 서명 요청을 다운로드하고, 새로운 자체 서명 HTTPS 인증서를 생성하거나 새로운 HTTPS 인증서를 설치할 수 있습니다.

새로운 자체 서명 HTTPS 인증서를 생성하지 않은 경우 이 페이지에 나타나는 인증서는 설치 중에 생성된

인증서입니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- **HTTPS 인증서 서명 요청 다운로드**

현재 설치된 HTTPS 인증서에 대한 인증 요청을 다운로드합니다. 브라우저에서 <hostname>.csr 파일을 저장하라는 메시지가 표시되어 인증 기관에 파일을 제공하여 서명할 수 있습니다.

- **HTTPS 인증서 설치**

인증 기관에서 서명하고 반환한 후 보안 인증서를 업로드하고 설치할 수 있습니다. 새 인증서는 관리 서버를 다시 시작한 후에 적용됩니다.

- **HTTPS 인증서 재생성**

현재 보안 인증서를 대체하는 새로운 자체 서명 HTTPS 인증서를 생성할 수 있습니다. Unified Manager를 다시 시작하면 새 인증서가 적용됩니다.

HTTPS 인증서 재생성 대화 상자

HTTPS 인증서 재생성 대화 상자를 사용하면 보안 정보를 사용자 지정한 다음 해당 정보로 새 HTTPS 인증서를 생성할 수 있습니다.

현재 인증서 정보는 이 페이지에 표시됩니다.

"현재 인증서 속성을 사용하여 다시 생성" 및 "현재 인증서 속성 업데이트" 선택을 사용하면 현재 정보로 인증서를 다시 생성하거나 새 정보로 인증서를 생성할 수 있습니다.

- 일반 이름

필수. 보호하려는 정규화된 도메인 이름(FQDN)입니다.

Unified Manager 고가용성 구성에서는 가상 IP 주소를 사용합니다.

- 이메일

선택 과목. 귀하의 조직에 연락할 이메일 주소입니다. 일반적으로 인증 관리자나 IT 부서의 이메일 주소입니다.

- 회사

선택 과목. 일반적으로 회사의 법인명입니다.

- 부서

선택 과목. 회사 내 부서의 이름입니다.

- 도시

선택 과목. 회사의 도시 위치입니다.

- 상태

선택 과목. 회사의 주 또는 도 소재지를 약어로 표기하지 마십시오.

- 국가

선택 과목. 회사의 국가 위치. 이는 일반적으로 국가의 두 글자 ISO 코드입니다.

- 대체 이름

필수의. 기존 로컬호스트나 다른 네트워크 주소 외에도 이 서버에 접속하는 데 사용할 수 있는 기본이 아닌 추가 도메인 이름입니다. 각 대체 이름은 쉼표로 구분합니다.

인증서의 대체 이름 필드에서 로컬 식별 정보를 제거하려면 "로컬 식별 정보 제외(예: 로컬호스트)" 확인란을 선택합니다. 이 확인란을 선택하면 필드에 입력한 내용만 대체 이름 필드에 사용됩니다. 이 필드를 비워 두면 인증서에 대체 이름 필드가 전혀 없습니다.

- 키 크기(키 알고리즘: **RSA**)

키 알고리즘은 RSA로 설정됩니다. 2048, 3072 또는 4096비트 중 하나의 키 크기를 선택할 수 있습니다. 기본 키 크기는 2048비트로 설정됩니다.

- 유효기간

기본 유효 기간은 397일입니다. 이전 버전에서 업그레이드한 경우 이전 인증서의 유효성이 변경되지 않은 것으로 보일 수 있습니다.

자세한 내용은 다음을 참조하세요. "[HTTPS 인증서 생성](#)".

스토리지 모니터링 및 관리

Active IQ Unified Manager 소개

Active IQ Unified Manager (이전 OnCommand Unified Manager)를 사용하면 단일 인터페이스에서 ONTAP 스토리지 시스템의 상태와 성능을 모니터링하고 관리할 수 있습니다.

Unified Manager는 다음과 같은 기능을 제공합니다.

- ONTAP 소프트웨어가 설치된 시스템에 대한 검색, 모니터링 및 알림.
- 환경의 용량, 보안 및 성능 상태를 보여주는 대시보드입니다.
- 향상된 알림, 이벤트 및 임계값 인프라.
- 시간 경과에 따른 작업 부하 활동을 나타내는 자세한 그래프를 표시합니다. 여기에는 IOPS(작업), MBps(처리량), 지연 시간(응답 시간), 사용률, 성능 용량, 캐시 비율 등이 포함됩니다.
- 클러스터 구성 요소를 과도하게 사용하는 작업 부하와 활동 증가로 인해 성능에 영향을 받는 작업 부하를 식별합니다.
- 특정 사건과 이벤트를 해결하기 위해 수행할 수 있는 시정 조치를 제안하고, 일부 이벤트에 대한 "수정" 버튼을 제공하여 문제를 즉시 해결할 수 있습니다.
- OnCommand Workflow Automation 과 통합되어 자동화된 보호 워크플로를 실행합니다.
- LUN이나 파일 공유와 같은 새로운 워크로드를 Unified Manager에서 직접 생성하고, 해당 워크로드를 사용하여 애플리케이션에 액세스하는 사용자의 성능 및 스토리지 목표를 정의하기 위해 성능 서비스 수준을 할당하는 기능입니다.

Active IQ Unified Manager 상태 모니터링 소개

Active IQ Unified Manager (이전 OnCommand Unified Manager)를 사용하면 중앙 사용자 인터페이스를 통해 ONTAP 소프트웨어를 실행하는 많은 수의 시스템을 모니터링할 수 있습니다. Unified Manager 서버 인프라는 확장성, 지원성, 향상된 모니터링 및 알림 기능을 제공합니다.

Unified Manager의 주요 기능으로는 모니터링, 알림, 클러스터 가용성 및 용량 관리, 보호 기능 관리, 진단 데이터 번들링 및 기술 지원팀으로 전송 등이 있습니다.

Unified Manager를 사용하여 클러스터를 모니터링할 수 있습니다. 클러스터에서 문제가 발생하면 Unified Manager는 이벤트를 통해 해당 문제의 세부 정보를 알려줍니다. 일부 이벤트에서는 문제를 바로잡는 데 필요한 시정 조치도 제공합니다. 문제가 발생하면 이메일과 SNMP 트랩을 통해 알림을 받을 수 있도록 이벤트에 대한 알림을 구성할 수 있습니다.

Unified Manager를 사용하면 주석과 연결하여 환경의 스토리지 객체를 관리할 수 있습니다. 사용자 정의 주석을 만들고 규칙을 통해 클러스터, 스토리지 가상 머신(SVM), 볼륨을 주석과 동적으로 연결할 수 있습니다.

각 클러스터 개체에 대한 용량 및 상태 차트에 제공된 정보를 사용하여 클러스터 개체의 저장 요구 사항을 계획할 수도 있습니다.

물리적 및 논리적 용량

Unified Manager는 ONTAP 스토리지 객체에 사용되는 물리적 공간과 논리적 공간의 개념을 활용합니다.

- 물리적 용량: 물리적 공간은 볼륨에 사용되는 물리적 저장 블록을 말합니다. "물리적 사용 용량"은 일반적으로 저장 효율성 기능(중복 제거 및 압축 등)으로 인한 데이터 감소로 인해 논리적 사용 용량보다 작습니다.
- 논리적 용량: 논리적 공간은 볼륨에서 사용 가능한 공간(논리적 블록)을 의미합니다. 논리적 공간은 중복 제거나 압축 결과를 고려하지 않고 이론적 공간을 어떻게 사용할 수 있는지를 나타냅니다. "사용된 논리적 공간"은 사용된 물리적 공간과 구성된 저장 효율성 기능(중복 제거 및 압축 등)을 통해 절감된 공간을 합친 것입니다. 이 측정값은 실제 사용 용량보다 크게 나타나는 경우가 많은데, 이는 여기에는 데이터 압축 및 기타 물리적 공간의 감소가 반영되지 않기 때문입니다. 따라서 총 논리적 용량은 제공된 공간보다 높을 수 있습니다.

용량 측정 단위

Unified Manager는 1024(2¹⁰)바이트의 이진 단위를 기준으로 저장 용량을 계산합니다. ONTAP 9.10.0 및 이전 버전에서는 이러한 단위가 KB, MB, GB, TB, PB로 표시되었습니다. ONTAP 9.10.1부터 Unified Manager에서는 KiB, MiB, GiB, TiB, PiB로 표시됩니다.



ONTAP의 모든 릴리스에서 처리량에 사용되는 단위는 초당 킬로바이트(Kbps), 초당 메가바이트(Mbps), 초당 기가바이트(Gbps), 초당 테라바이트(Tbps) 등으로 계속 사용됩니다.

ONTAP 9.10.0 및 이전 버전의 Unified Manager에 표시되는 용량 단위	ONTAP 9.10.1용 Unified Manager에 표시되는 용량 단위	계산	바이트 단위의 값
KB	키비	1024	1024바이트
엠비	미비	1024 * 1024	1,048,576바이트
영국	수코양이	1024 * 1024 * 1024	1,073,741,824바이트
결핵	티비	1024 * 1024 * 1024 * 1024	1,099,511,627,776바이트

Active IQ Unified Manager 성능 모니터링 소개

Active IQ Unified Manager (이전 OnCommand Unified Manager)는 NetApp ONTAP 소프트웨어를 실행하는 시스템에 대한 성능 모니터링 기능과 이벤트 근본 원인 분석을 제공합니다.

Unified Manager를 사용하면 클러스터 구성 요소를 과도하게 사용하여 클러스터의 다른 작업 부하의 성능을 저하시키는 작업 부하를 식별할 수 있습니다. 성능 임계값 정책을 정의하면 특정 성능 카운터에 대한 최대값을 지정하여 임계값이 초과되면 이벤트가 생성되도록 할 수도 있습니다. Unified Manager는 이러한 성능 이벤트에 대해 알림을 보내므로, 이를 통해 시정 조치를 취하고 성능을 정상적인 운영 수준으로 되돌릴 수 있습니다. Unified Manager UI에서 이벤트를 보고 분석할 수 있습니다.

Unified Manager는 두 가지 유형의 작업 부하의 성능을 모니터링합니다.

- 사용자 정의 워크로드

이러한 작업 부하에는 클러스터에서 생성한 FlexVol 볼륨과 FlexGroup 볼륨이 포함됩니다.

- 시스템 정의 워크로드

이러한 작업 부하는 내부 시스템 활동으로 구성됩니다.

Unified Manager REST API 사용

Active IQ Unified Manager 스토리지 환경 모니터링 및 관리에 대한 정보를 볼 수 있는 REST API를 제공합니다. API를 사용하면 정책에 따라 스토리지 객체를 프로비저닝하고 관리할 수도 있습니다.

Unified Manager에서 지원하는 API 게이트웨이를 사용하여 모든 ONTAP 관리 클러스터에서 ONTAP API를 실행할 수도 있습니다.

Unified Manager REST API에 대한 정보는 다음을 참조하세요. ["Active IQ Unified Manager REST API 시작하기"](#).

Unified Manager 서버가 수행하는 작업

Unified Manager 서버 인프라는 데이터 수집 장치, 데이터베이스, 애플리케이션 서버로 구성됩니다. 검색, 모니터링, 역할 기반 액세스 제어(RBAC), 감사, 로깅 등의 인프라 서비스를 제공합니다.

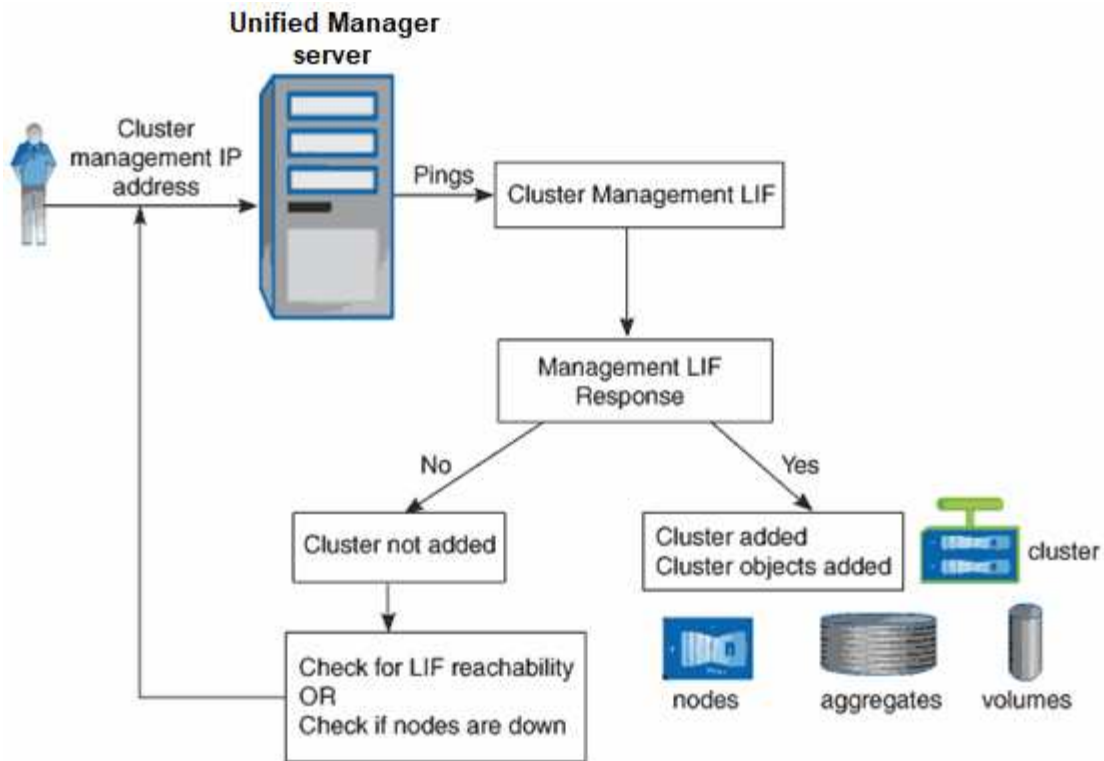
Unified Manager는 클러스터 정보를 수집하고, 해당 데이터를 데이터베이스에 저장하고, 데이터를 분석하여 클러스터에 문제가 있는지 확인합니다.

발견 프로세스가 작동하는 방식

Unified Manager에 클러스터를 추가하면 서버에서 클러스터 개체를 검색하여 데이터베이스에 추가합니다. 검색 프로세스가 작동하는 방식을 이해하면 조직의 클러스터와 해당 개체를 관리하는 데 도움이 됩니다.

기본 모니터링 간격은 15분입니다. Unified Manager 서버에 클러스터를 추가한 경우 Unified Manager UI에 클러스터 세부 정보가 표시되는 데 15분이 걸립니다.

다음 이미지는 Active IQ Unified Manager 에서의 검색 프로세스를 보여줍니다.



사용자 인터페이스를 이해하세요

Unified Manager 사용자 인터페이스는 주로 모니터링되는 객체를 한눈에 볼 수 있는 대시보드로 구성됩니다. 사용자 인터페이스는 모든 클러스터 객체를 볼 수 있는 기능도 제공합니다.

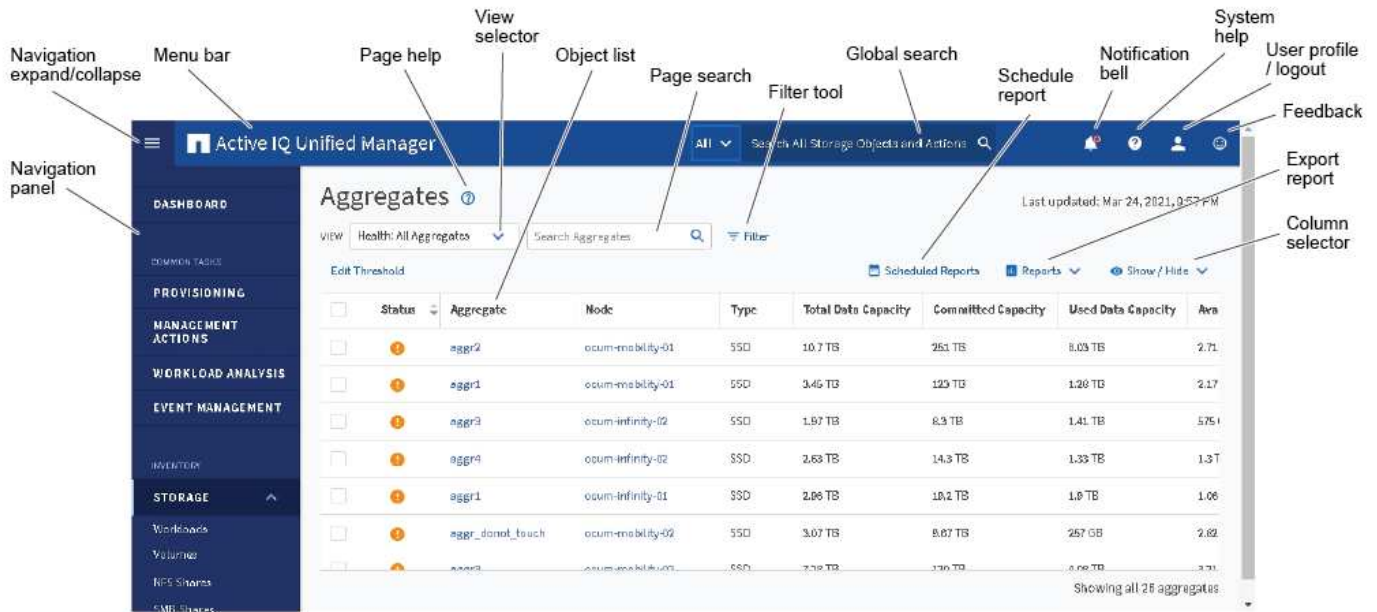
원하는 보기를 선택하고 필요에 따라 작업 버튼을 사용할 수 있습니다. 화면 구성은 작업 공간에 저장되므로 Unified Manager를 시작할 때 필요한 모든 기능을 사용할 수 있습니다. 하지만 한 뷰에서 다른 뷰로 이동한 후 다시 돌아오면 뷰가 동일하지 않을 수 있습니다.

일반적인 창 레이아웃

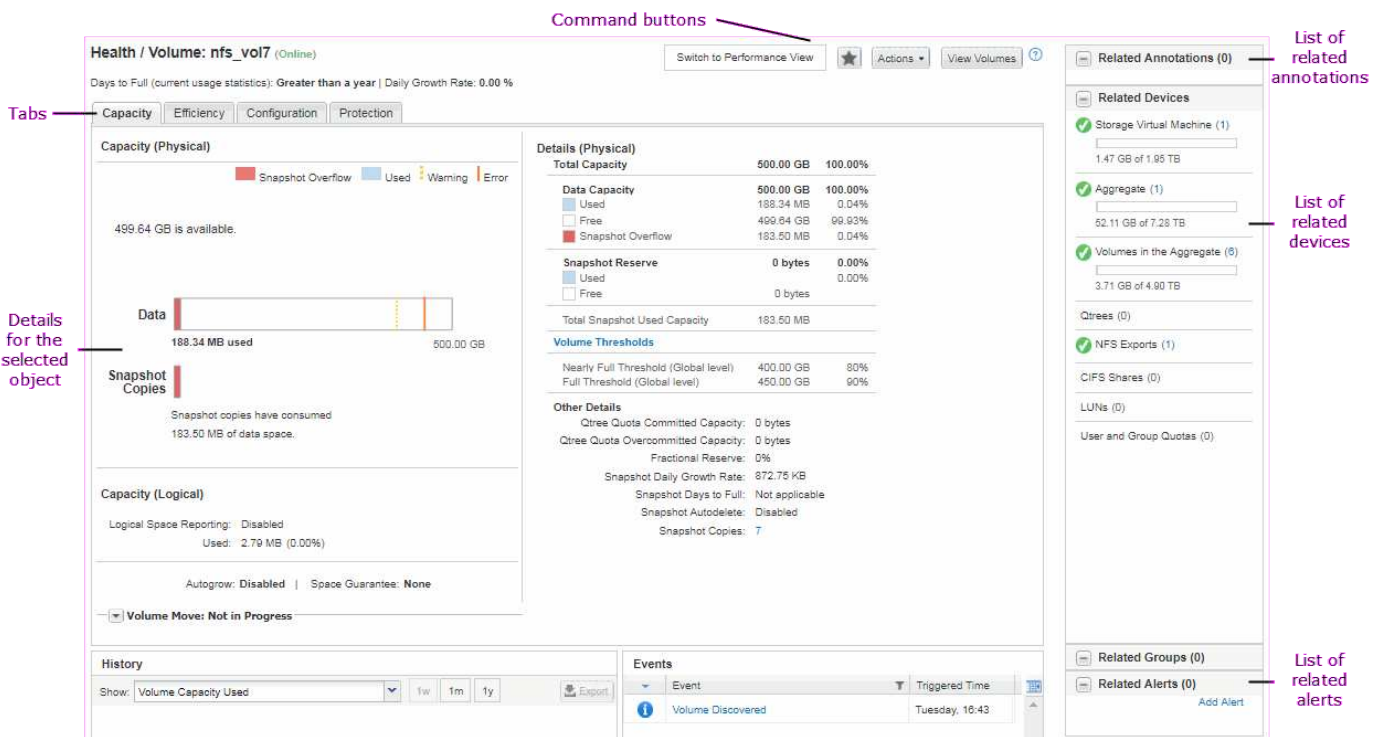
일반적인 창 레이아웃을 이해하면 Active IQ Unified Manager 효과적으로 탐색하고 사용하는 데 도움이 됩니다. 대부분의 Unified Manager 창은 개체 목록이나 세부 정보라는 두 가지 일반 레이아웃 중 하나와 비슷합니다. 권장되는 디스플레이 설정은 최소 1280 x 1024 픽셀입니다.

다음 다이어그램에 있는 모든 요소가 모든 창에 포함되어 있는 것은 아닙니다.

객체 목록 창 레이아웃



객체 세부 정보 창 레이아웃



창 레이아웃 사용자 정의

Active IQ Unified Manager 사용하면 저장소 및 네트워크 개체 페이지의 정보 레이아웃을 사용자 정의할 수 있습니다. 창을 사용자 지정하면 어떤 데이터를 볼 수 있는지, 데이터가 어떻게 표시되는지 제어할 수 있습니다.

- 정렬

열 머리글을 클릭하면 열 항목의 정렬 순서를 변경할 수 있습니다. 열 머리글을 클릭하면 정렬 화살표(▲ 그리고 ▼)이 해당 열에 나타납니다.

- 필터링

필터 아이콘을 클릭할 수 있습니다() 저장소 및 네트워크 개체 페이지에서 정보 표시를 사용자 정의하기 위한 필터를 적용하여 제공된 조건과 일치하는 항목만 표시되도록 합니다. 필터 창에서 필터를 적용합니다.

필터 창을 사용하면 선택한 옵션에 따라 대부분의 열을 필터링할 수 있습니다. 예를 들어, 상태: 모든 볼륨 보기에서 필터 창을 사용하여 상태 아래에서 적절한 필터 옵션을 선택하여 오프라인인 모든 볼륨을 표시할 수 있습니다.

모든 목록의 용량 관련 열에는 항상 적절한 단위로 용량 데이터가 표시되며 소수점 이하 두 자리까지 반올림됩니다. 이는 용량 열을 필터링할 때도 적용됩니다. 예를 들어, 상태: 모든 집계 보기의 총 데이터 용량 열에 있는 필터를 사용하여 20.45GB보다 큰 데이터를 필터링하는 경우 실제 용량인 20.454GB는 20.45GB로 표시됩니다. 마찬가지로 20.45GB 미만의 데이터를 필터링하면 실제 용량인 20.449GB는 20.45GB로 표시됩니다.

Health: All Aggregates 보기의 Available Data % 열에 있는 필터를 사용하여 20.45%를 넘는 데이터를 필터링하는 경우, 실제 용량인 20.454%는 20.45%로 표시됩니다. 마찬가지로 20.45% 미만의 데이터를 필터링하면 실제 용량인 20.449%는 20.45%로 표시됩니다.

- 열 숨기기 또는 표시

표시할 열을 선택하려면 열 표시 아이콘(표시/숨기기)을 클릭하세요. 적절한 열을 선택한 후 마우스로 끌어서 순서를 변경할 수 있습니다.

- 수색

검색창을 사용하여 특정 개체 속성을 검색하면 인벤토리 페이지의 항목 목록을 구체화하는 데 도움이 됩니다. 예를 들어, "cloud"를 입력하면 볼륨 인벤토리 페이지에서 볼륨 목록을 구체화하여 "cloud"라는 단어가 포함된 모든 볼륨을 볼 수 있습니다.

- 데이터 내보내기

보고서 버튼을 클릭하거나 내보내기 버튼을 클릭하여 데이터를 심표로 구분된 값으로 내보낼 수 있습니다. (.csv) 파일, (.pdf) 문서 또는 Microsoft Excel (.xlsx) 파일을 열고 내보낸 데이터를 사용하여 보고서를 작성합니다.

Unified Manager 도움말 사용

도움말에는 Active IQ Unified Manager 에 포함된 모든 기능에 대한 정보가 포함되어 있습니다. 목차, 색인 또는 검색 도구를 사용하여 기능에 대한 정보와 사용 방법을 찾을 수 있습니다.

각 탭과 Unified Manager 사용자 인터페이스의 메뉴 모음에서 도움말을 확인할 수 있습니다.

도움말의 검색 도구는 일부 단어에는 작동하지 않습니다.

- 특정 필드나 매개변수에 대해 알아보려면 클릭하세요. .
- 모든 도움말 내용을 보려면  * > *도움말/문서 메뉴 표시줄에 있습니다.

탐색 창에서 목차의 어느 부분이든 확장하면 더 자세한 정보를 찾을 수 있습니다.

- 도움말 내용을 검색하려면 탐색 창에서 검색 탭을 클릭하고 찾으려는 단어나 단어 시리즈를 입력한 후 *이동!*을 클릭하세요.
- 도움말 항목을 인쇄하려면 프린터 아이콘을 클릭하세요.

즐거찾는 도움말 항목을 북마크하세요

도움말 즐겨찾기 탭에서는 자주 사용하는 도움말 항목을 북마크할 수 있습니다. 북마크를 이용하면 즐겨찾는 주제에 빠르게 접근할 수 있습니다.

단계

1. 즐겨찾기에 추가하려는 도움말 항목으로 이동합니다.
2. *즐거찾기*를 클릭한 다음 *추가*를 클릭합니다.

저장소 객체 검색

특정 객체에 빠르게 액세스하려면 메뉴 막대 상단의 모든 저장소 객체 검색 필드를 사용하면 됩니다. 모든 개체에 대한 글로벌 검색 방법을 사용하면 유형별로 특정 개체를 빠르게 찾을 수 있습니다. 검색 결과는 저장소 객체 유형별로 정렬되며, 드롭다운 메뉴를 사용하여 객체별로 추가로 필터링할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 다음 역할 중 하나가 있어야 합니다. 운영자, 애플리케이션 관리자 또는 스토리지 관리자.
- 유효한 검색에는 최소 3개의 문자가 포함되어야 합니다.

드롭다운 메뉴 값 "전체"를 사용하면 글로벌 검색에서 모든 객체 카테고리에서 찾은 결과의 총 수가 표시됩니다. 각 객체 카테고리에 대해 최대 25개의 검색 결과가 표시됩니다. 드롭다운 메뉴에서 특정 객체 유형을 선택하면 특정 객체 유형 내에서 검색을 구체화할 수 있습니다. 이 경우 반환된 목록은 상위 25개 개체로 제한되지 않습니다.

검색할 수 있는 객체 유형은 다음과 같습니다.

- 클러스터
- 노드
- 스토리지 VM
- 골재
- 볼륨
- 큐트리스
- SMB 주식
- NFS 주식
- 사용자 또는 그룹 할당량
- LUN
- NVMe 네임스페이스
- 개시자 그룹

- 개시자
- 일관성 그룹

작업 부하 이름을 입력하면 해당 볼륨이나 LUN 범주에 속하는 작업 부하 목록이 반환됩니다.

검색 결과에서 원하는 객체를 클릭하면 해당 객체의 건강 세부 정보 페이지로 이동할 수 있습니다. 객체에 대한 직접적인 상태 페이지가 없는 경우 부모 객체의 상태 페이지가 표시됩니다. 예를 들어, 특정 LUN을 검색하는 경우 해당 LUN이 있는 SVM 세부 정보 페이지가 표시됩니다.

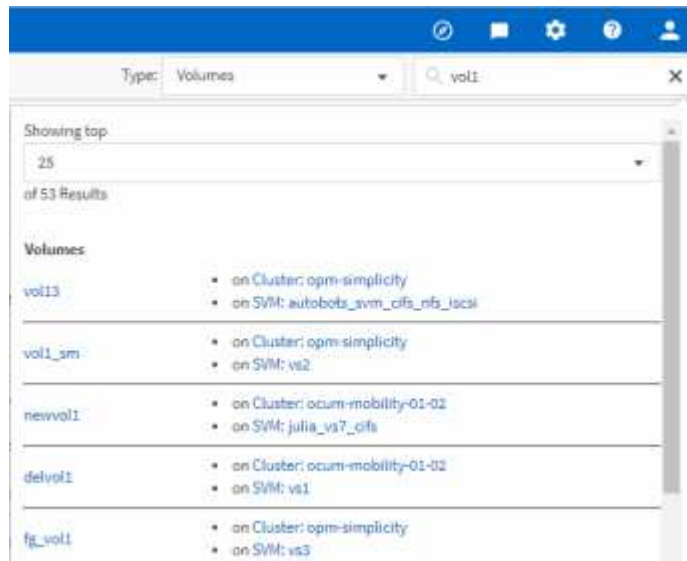


포트와 LIF는 글로벌 검색창에서 검색할 수 없습니다.

단계

1. 단일 객체 유형에 대한 검색 결과만 구체화하려면 메뉴에서 객체 유형을 선택하세요.
2. 모든 저장소 개체 검색 필드에 개체 이름을 최소 3자 이상 입력하세요.

이 예에서 드롭다운 상자에는 볼륨 개체 유형이 선택되어 있습니다. 모든 저장소 개체 검색 필드에 "vol1"을 입력하면 해당 문자가 포함된 이름을 가진 모든 볼륨 목록이 표시됩니다.



저장소 데이터를 보고서로 내보내기

다양한 출력 형식으로 저장 데이터를 내보낸 다음, 내보낸 데이터를 사용하여 보고서를 작성할 수 있습니다. 예를 들어, 해결되지 않은 중요 이벤트가 10개 있는 경우 이벤트 관리 인벤토리 페이지에서 데이터를 내보내 보고서를 만든 다음, 문제를 해결할 수 있는 관리자에게 보고서를 보낼 수 있습니다.

데이터를 내보낼 수 있습니다 .csv 파일, .xlsx 파일 또는 .pdf 저장소 및 네트워크 인벤토리 페이지에서 문서를 작성하고 내보낸 데이터를 사용하여 보고서를 작성합니다. 제품에는 다른 위치만 있습니다. .csv 또는 .pdf 파일을 생성할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

내보내고 싶다면...	이렇게 하세요...
저장소 객체 인벤토리 세부 정보	왼쪽 탐색 메뉴에서 저장소 또는 *네트워크*를 클릭한 다음, 저장소 개체를 선택합니다. 시스템에서 제공하는 보기 중 하나 또는 사용자가 만든 사용자 정의 보기를 선택하세요.
QoS 정책 그룹 세부 정보	왼쪽 탐색 메뉴에서 저장소 > *QoS 정책 그룹*을 클릭합니다.
저장 용량 및 보호 내역 세부 정보	저장소 > 집계 또는 저장소 > *볼륨*을 클릭한 다음, 단일 집계 또는 볼륨을 선택합니다.
이벤트 세부 정보	왼쪽 탐색 메뉴에서 *이벤트 관리*를 클릭합니다.
스토리지 객체 상위 10개 성능 세부 정보	저장소 > 클러스터 > 성능: 모든 클러스터*를 클릭한 다음, 클러스터를 선택하고 *상위 성능자 탭을 선택합니다. 그런 다음 저장소 개체와 성능 카운터를 선택합니다.

2. 보고서 버튼(일부 UI 페이지에서는 내보내기 버튼)을 클릭합니다.

3. **CSV** 다운로드, **PDF** 다운로드 또는 *Excel 다운로드*를 클릭하여 내보내기 요청을 확인하세요.

상위 성과자 탭에서는 보고 있는 단일 클러스터 또는 데이터 센터의 모든 클러스터에 대한 통계 보고서를 다운로드할 수 있습니다.

파일이 다운로드되었습니다.

4. 적절한 응용프로그램에서 파일을 엽니다.

관련 정보

["상태/클러스터 인벤토리 페이지"](#)

["보고서 예약"](#)

필터 인벤토리 페이지 콘텐츠

Unified Manager에서 인벤토리 페이지 데이터를 필터링하여 특정 기준에 따라 데이터를 빠르게 찾을 수 있습니다. 필터링을 사용하면 Unified Manager 페이지의 내용을 좁혀 관심 있는 결과만 표시할 수 있습니다. 이 방법은 귀하가 관심 있는 데이터만 표시하는 매우 효율적인 방법입니다.

*필터링*을 사용하여 기본 설정에 따라 그리드 보기를 사용자 지정하세요. 사용 가능한 필터 옵션은 그리드에 표시되는 개체 유형에 따라 달라집니다. 현재 필터가 적용되어 있는 경우, 적용된 필터의 수가 필터 버튼 오른쪽에 표시됩니다.

세 가지 유형의 필터 매개변수가 지원됩니다.

매개변수	확인
문자열(텍스트)	연산자는 포함, 시작, 끝남, *포함하지 않음*입니다.
숫자	연산자는 보다 크다, 보다 작다, 마지막에, *사이에*입니다.
열거형(텍스트)	연산자는 *is*와 *is not*입니다.

각 필터에는 열, 연산자, 값 필드가 필요합니다. 사용 가능한 필터는 현재 페이지에서 필터링 가능한 열을 반영합니다. 적용할 수 있는 필터의 최대 개수는 4개입니다. 필터링된 결과는 결합된 필터 매개변수를 기반으로 합니다. 필터링된 결과는 현재 표시된 페이지뿐만 아니라 필터링된 검색의 모든 페이지에 적용됩니다.

필터링 패널을 사용하여 필터를 추가할 수 있습니다.

1. 페이지 상단에서 필터 버튼을 클릭하세요. 필터링 패널이 표시됩니다.
2. 왼쪽 드롭다운 목록을 클릭하고 개체를 선택합니다. 예를 들어, _Cluster_나 성능 카운터를 선택합니다.
3. 가운데 드롭다운 목록을 클릭하고 사용할 연산자를 선택하세요.
4. 마지막 목록에서 값을 선택하거나 입력하여 해당 개체에 대한 필터를 완성합니다.
5. 다른 필터를 추가하려면 +필터 추가*를 클릭하세요. 추가 필터 필드가 표시됩니다. 이전 단계에서 설명한 프로세스를 사용하여 이 필터를 완료합니다. 네 번째 필터를 추가하면 *+필터 추가 버튼이 더 이상 표시되지 않습니다.
6. *필터 적용*을 클릭하세요. 필터 옵션은 그리드에 적용되고 필터 수는 필터 버튼 오른쪽에 표시됩니다.
7. 필터링 패널을 사용하여 제거할 필터 오른쪽에 있는 휴지통 아이콘을 클릭하여 개별 필터를 제거합니다.
8. 모든 필터를 제거하려면 필터링 패널 하단의 *재설정*을 클릭하세요.

필터링 예제

이 그림은 세 개의 필터가 있는 필터링 패널을 보여줍니다. 필터가 최대 4개보다 적을 경우 +필터 추가 버튼이 표시됩니다.

The screenshot shows a filter panel with three active filters. Each filter has a dropdown for the field (MBps, Node, Type), a dropdown for the operator (greater than, name starts with, is), and a text input for the value (5, test, FCP Port). To the right of each filter is a trash icon for removal. At the bottom left is a '+ Add Filter' button. At the bottom right are 'Cancel' and 'Apply Filter' buttons. The 'Apply Filter' button is highlighted in blue.

*필터 적용*을 클릭하면 필터링 패널이 닫히고 필터가 적용되며 적용된 필터 수가 표시됩니다(3).

알림 벨에서 활성 이벤트 보기

알림 벨() 메뉴 표시줄에서 Unified Manager가 추적하는 가장 중요한 활성 이벤트를 빠르게

볼 수 있는 방법을 제공합니다.

활성 이벤트 목록은 모든 클러스터에서 발생한 중요, 오류, 경고 및 업그레이드 이벤트의 총 수를 확인하는 방법을 제공합니다. 이 목록에는 지난 7일간의 이벤트가 포함되어 있으며, 정보 이벤트는 포함되어 있지 않습니다. 가장 관심 있는 이벤트 목록을 표시하려면 링크를 클릭하세요.

클러스터에 접근할 수 없는 경우 Unified Manager는 이 페이지에 해당 정보를 표시합니다. 세부정보 버튼을 클릭하면 접근할 수 없는 클러스터에 대한 자세한 정보를 볼 수 있습니다. 이 작업을 수행하면 이벤트 세부 정보 페이지가 열립니다. 관리 스테이션의 공간이나 RAM 부족 등의 규모 모니터링 문제도 이 페이지에 표시됩니다.

단계

1. 메뉴바에서 클릭하세요 .
2. 활성 이벤트에 대한 세부 정보를 보려면 "수용 인원 2명" 또는 "성능 4명"과 같은 이벤트 텍스트 링크를 클릭하세요.

대시보드에서 클러스터를 모니터링하고 관리합니다.

대시보드는 모니터링하는 ONTAP 시스템의 현재 상태에 대한 누적된 정보를 한눈에 볼 수 있도록 제공합니다. 대시보드는 모니터링 중인 클러스터의 전반적인 용량, 성능 및 보안 상태를 평가할 수 있는 "패널"을 제공합니다.

또한 ONTAP System Manager나 ONTAP CLI를 사용하지 않고도 Unified Manager 사용자 인터페이스에서 직접 수정할 수 있는 특정 ONTAP 문제도 있습니다.

대시보드 상단에서 패널에 모니터링되는 모든 클러스터에 대한 정보를 표시할지, 아니면 개별 클러스터에 대한 정보를 표시할지 선택할 수 있습니다. 모든 클러스터의 상태를 보고 나서 자세한 정보를 보고 싶을 때 개별 클러스터로 드릴다운할 수 있습니다.



아래 나열된 일부 패널은 구성에 따라 페이지에 나타나지 않을 수 있습니다.

패널	설명
관리 조치	Unified Manager가 문제에 대한 단일 해결책을 진단하고 결정할 수 있는 경우 해당 해결책은 수정 버튼과 함께 이 패널에 표시됩니다.
용량	로컬 계층과 클라우드 계층의 총 용량과 사용된 용량, 그리고 로컬 용량이 상한에 도달할 때까지 남은 일수를 표시합니다.
성능 용량	각 클러스터의 성능 용량 값과 성능 용량이 상한에 도달할 때까지 걸리는 일수를 표시합니다.
워크로드 IOPS	현재 특정 IOPS 범위에서 실행 중인 총 워크로드 수를 표시합니다.
작업 부하 성능	정의된 각 성능 서비스 수준에 할당된 적합 및 비적합 워크로드의 총 수를 표시합니다.

패널	설명
보안	규정을 준수하거나 준수하지 않는 클러스터 수, 규정을 준수하거나 준수하지 않는 SVM 수, 암호화되거나 암호화되지 않은 볼륨 수를 표시합니다.
보호	SVM-DR 관계로 보호되는 스토리지 VM 수, SnapMirror 관계로 보호되는 볼륨 수, Snapshot으로 보호되는 볼륨 수, MetroCluster 로 보호되는 클러스터 수를 표시합니다.
사용 개요	가장 높은 IOPS, 가장 높은 처리량(MBps), 가장 많이 사용된 물리적 용량을 기준으로 클러스터를 정렬하여 표시합니다.

대시보드 페이지

대시보드 페이지에는 모니터링 중인 클러스터의 높은 수준의 용량, 성능 및 보안 상태를 표시하는 "패널"이 있습니다. 이 페이지에서는 Unified Manager가 특정 이벤트를 해결하기 위해 수행할 수 있는 수정 사항을 나열하는 관리 작업 패널도 제공합니다.

대부분의 패널에는 해당 카테고리의 활성 이벤트 수와 지난 24시간 동안 추가된 새 이벤트 수도 표시됩니다. 이 정보는 이벤트를 해결하기 위해 추가로 분석해야 할 클러스터를 결정하는 데 도움이 됩니다. 이벤트를 클릭하면 상위 이벤트가 표시되고, 해당 카테고리에서 활성 이벤트를 표시하도록 필터링된 이벤트 관리 인벤토리 페이지로 연결되는 링크가 제공됩니다.

대시보드 상단에서 패널에 모니터링되는 모든 클러스터("모든 클러스터")에 대한 정보를 표시할지, 아니면 개별 클러스터에 대한 정보를 표시할지 선택할 수 있습니다. 모든 클러스터의 상태를 보고 나서 자세한 정보를 보고 싶을 때 개별 클러스터로 드릴다운할 수 있습니다.



아래 나열된 패널 중 일부는 구성에 따라 대시보드에 표시됩니다.

관리 작업 패널

Unified Manager는 특정 문제를 철저히 진단하고 단일 해결책을 제공할 수 있습니다. 가능한 경우 해당 해결 방법은 수정 또는 모두 수정 버튼과 함께 이 패널에 표시됩니다. ONTAP System Manager나 ONTAP CLI를 사용하지 않고도 Unified Manager에서 이러한 문제를 즉시 해결할 수 있습니다. 모든 문제를 보려면 보기를 클릭하세요. ["Unified Manager에서 직접 ONTAP 문제 해결"](#) 자세한 내용은.

용량 패널

모든 클러스터를 볼 때 이 패널에는 각 클러스터의 물리적 사용 용량(저장소 효율성 절감 적용 후)과 물리적 사용 가능 용량(잠재적 저장 효율성 절감 제외), 디스크가 가득 찰 것으로 예상되는 날짜 수, 구성된 ONTAP 저장 효율성 설정에 따른 데이터 감소율(스냅샷 복사본 없음)이 표시됩니다. 또한 구성된 클라우드 계층에 사용된 용량도 나열됩니다. 막대형 차트를 클릭하면 해당 클러스터의 집계 인벤토리 페이지로 이동합니다. "완전히 채워질 때까지 남은 일수" 텍스트를 클릭하면 남은 용량 일수가 가장 적은 집계를 나타내는 메시지가 표시됩니다. 자세한 내용을 보려면 집계 이름을 클릭하세요.

단일 클러스터를 볼 때 이 패널에는 로컬 계층의 각 디스크 유형별로 정렬된 데이터 집계에 대한 물리적 사용 용량과 물리적 사용 가능 용량, 그리고 클라우드 계층에 대한 물리적 사용 가능 용량이 표시됩니다. 디스크 유형에 대한 막대형 차트를 클릭하면 해당 디스크 유형을 사용하는 볼륨의 볼륨 인벤토리 페이지로 이동합니다.

성능 용량 패널

모든 클러스터를 볼 때 이 패널에는 각 클러스터의 성능 용량 값(지난 1시간 동안의 평균)과 성능 용량이 상한에 도달할 때까지 걸리는 일수(일일 성장률 기준)가 표시됩니다. 막대형 차트를 클릭하면 해당 클러스터의 노드 인벤토리 페이지로 이동합니다. 노드 인벤토리 페이지에는 지난 72시간 동안의 평균 성능 용량이 표시됩니다. "완전히 채워질 때까지 남은 일수" 텍스트를 클릭하면 남은 성능 용량 일수가 가장 적은 노드를 나타내는 메시지가 표시됩니다. 자세한 내용을 보려면 노드 이름을 클릭하세요.

단일 클러스터를 볼 때 이 패널에는 클러스터 성능 용량 사용 비율, 총 IOPS, 총 처리량(MB/s) 값과 이 세 가지 측정 항목이 각각 상한에 도달할 것으로 예상되는 날짜가 표시됩니다.

워크로드 IOPS 패널

단일 클러스터를 볼 때 이 패널에는 현재 특정 IOPS 범위에서 실행 중인 총 워크로드 수가 표시되고, 차트 위에 커서를 올려 놓으면 각 디스크 유형에 대한 숫자가 표시됩니다.

작업 부하 성능 패널

이 패널은 각 성능 서비스 수준(PSL) 정책에 할당된 적합 및 비적합 워크로드의 총 수를 표시합니다. 또한 PSL이 할당되지 않은 워크로드의 수도 표시됩니다. 막대형 차트를 클릭하면 작업 부하 페이지에서 해당 정책에 할당된 적합한 작업 부하로 이동합니다. 막대형 차트 뒤에 있는 숫자를 클릭하면 해당 정책에 할당된 적합 및 비적합 워크로드로 이동합니다.

보안 패널

보안 패널은 현재 보기에 따라 모든 클러스터 또는 단일 클러스터에 대한 높은 수준의 보안 상태를 표시합니다. 이 패널에는 다음이 표시됩니다.

- 지난 24시간 동안 수신된 보안 이벤트 목록입니다. 이벤트를 클릭하면 이벤트 세부 정보 페이지에서 세부 정보를 볼 수 있습니다.
- 클러스터 보안 상태(준수 클러스터와 비준수 클러스터 수)
- 스토리지 VM 보안 상태(규정을 준수하는 스토리지 VM과 규정을 준수하지 않는 스토리지 VM의 수)
- 볼륨 암호화 상태(암호화되었거나 암호화되지 않은 볼륨 수)
- 볼륨 랜섬웨어 방지 상태(랜섬웨어 방지가 활성화 또는 비활성화된 볼륨 수)

규정을 준수하는 클러스터와 준수하지 않는 클러스터, 스토리지 VMS, 암호화된 볼륨과 암호화되지 않은 볼륨, 볼륨 랜섬웨어 방지 상태의 막대형 차트를 클릭하면 해당 페이지로 이동하여 필터링된 클러스터, 스토리지 VM, 볼륨의 보안 세부 정보를 볼 수 있습니다.

규정 준수는 다음을 기반으로 합니다. "[ONTAP 9를 위한 NetApp 보안 강화 가이드](#)". 보안 페이지에서 모든 클러스터의 보안 세부 정보를 보려면 패널 상단의 오른쪽 화살표를 클릭하세요. 자세한 내용은 다음을 참조하세요. "[클러스터 및 스토리지 VM에 대한 자세한 보안 상태 보기](#)".

데이터 보호 패널

이 패널은 데이터 센터의 단일 클러스터 또는 모든 클러스터에 대한 데이터 보호 요약을 표시합니다. ONTAP에서 지난 24시간 동안 발생한 데이터 보호 이벤트, MetroCluster 이벤트, 활성 이벤트의 총 수를 표시합니다. 각 이벤트의 링크를 클릭하면 이벤트 세부 정보 페이지로 이동합니다. 모두 보기 링크를 클릭하면 이벤트 관리 인벤토리 페이지에서 모든 활성 보호 이벤트를 볼 수 있습니다. 패널에는 다음이 표시됩니다.

- 스냅샷 복사본으로 보호되는 데이터 센터의 클러스터 또는 모든 클러스터의 볼륨 수입니다.

- SnapMirror 관계로 보호되는 데이터 센터의 클러스터 또는 모든 클러스터에 있는 볼륨의 수입입니다. SnapMirror 관계의 경우 소스 클러스터의 볼륨 수가 고려됩니다.
- IP 또는 FC를 통한 MetroCluster 구성으로 보호되는 데이터 센터의 클러스터 수 또는 모든 클러스터입니다.
- SnapMirror 복구 지점 목표(RPO) 지연이 있는 볼륨 관계의 수는 지연 상태에 따라 달라집니다.

마우스를 올려 놓으면 각각의 카운트와 범례를 볼 수 있습니다. 패널 상단의 오른쪽 화살표를 클릭하면 데이터 보호 페이지에서 단일 클러스터나 모든 클러스터에 대한 세부 정보를 볼 수 있습니다. 또한, 다음을 클릭할 수 있습니다.

- 보호되지 않은 볼륨과 스냅샷 복사본으로 보호된 볼륨에 대한 막대형 차트를 통해 볼륨 페이지로 이동하여 세부 정보를 볼 수 있습니다.
- MetroCluster 구성으로 보호되거나 보호되지 않는 클러스터에 대한 막대형 차트를 통해 클러스터 페이지로 이동하여 세부 정보를 볼 수 있습니다.
- 모든 관계에 대한 막대형 차트는 관계 페이지로 이동하며, 여기서 세부 정보는 소스 클러스터를 기준으로 필터링됩니다.

자세한 내용은 다음을 참조하세요. ["볼륨 보호 상태 보기"](#).

사용 개요 패널

모든 클러스터를 볼 때 가장 높은 IOPS, 가장 높은 처리량(MB/s), 가장 많이 사용된 물리적 용량을 기준으로 클러스터를 정렬하여 볼 수 있습니다.

단일 클러스터를 볼 때 가장 높은 IOPS, 가장 높은 처리량(MB/s), 가장 많이 사용된 논리적 용량을 기준으로 작업 부하를 정렬하여 볼 수 있습니다.

관련 정보

["Unified Manager 자동 수정을 사용하여 문제 해결"](#)

["성능 이벤트에 대한 정보 표시"](#)

["성능 용량 및 사용 가능한 IOPS 정보를 사용하여 성능 관리"](#)

["볼륨/상태 세부 정보 페이지"](#)

["성능 이벤트 분석 및 알림"](#)

["이벤트 심각도 유형에 대한 설명"](#)

["성과 이벤트의 소스"](#)

["클러스터 보안 목표 관리"](#)

["성능 클러스터 랜딩 페이지에서 클러스터 성능을 모니터링합니다."](#)

["성능 인벤토리 페이지를 사용하여 성능 모니터링"](#)

Unified Manager에서 직접 **ONTAP** 문제 또는 기능을 관리하세요.

ONTAP System Manager나 ONTAP CLI를 사용하지 않고도 Unified Manager 사용자

인터페이스에서 직접 특정 ONTAP 문제를 해결하거나 특정 ONTAP 기능을 관리할 수 있습니다. "관리 작업" 옵션은 Unified Manager 이벤트를 트리거한 여러 ONTAP 문제에 대한 수정 사항을 제공합니다.

왼쪽 탐색 창에서 관리 작업 옵션을 선택하면 관리 작업 페이지에서 직접 문제를 해결할 수 있습니다. 관리 작업은 대시보드의 관리 작업 패널, 이벤트 세부 정보 페이지, 왼쪽 탐색 메뉴의 작업 부하 분석 선택에서도 사용할 수 있습니다.

Unified Manager는 특정 문제를 철저히 진단하고 단일 해결책을 제공할 수 있습니다. 랜섬웨어 방지 모니터링과 같은 특정 ONTAP 기능의 경우 Unified Manager는 내부 검사를 수행하고 특정 작업을 권장합니다. 해결 가능한 경우 해당 해결 방법은 관리 작업에 수정 버튼과 함께 표시됩니다. 문제를 해결하려면 수정 버튼을 클릭하세요. 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

Unified Manager는 클러스터에 ONTAP 명령을 보내 요청된 수정을 수행합니다. 수정이 완료되면 해당 이벤트는 더 이상 사용되지 않습니다.

일부 관리 작업을 통해 모두 수정 버튼을 사용하여 여러 저장소 개체에서 동일한 문제를 해결할 수 있습니다. 예를 들어, "볼륨 공간 가득 참" 이벤트가 발생한 볼륨이 5개 있을 수 있는데, 이 경우 "볼륨 자동 증가 사용"에 대한 모두 수정 관리 작업을 클릭하면 해결할 수 있습니다. 한 번의 클릭으로 5권의 문제를 해결할 수 있습니다.

자동 수정을 사용하여 관리할 수 있는 ONTAP 문제 및 기능에 대한 정보는 다음을 참조하세요. ["Unified Manager가 해결할 수 있는 문제는 무엇입니까?"](#).

수정 또는 모두 수정 버튼이 표시되면 어떤 옵션이 있습니까?

관리 작업 페이지에는 Unified Manager가 이벤트를 통해 알림을 받은 문제를 해결할 수 있는 수정 또는 모두 수정 버튼이 제공됩니다.

필요한 경우, 버튼을 클릭하여 문제를 해결하는 것이 좋습니다. 하지만 Unified Manager에서 권장하는 대로 문제를 해결하고 싶지 않은 경우 다음 작업을 수행할 수 있습니다.

당신은 무엇을 하고 싶습니까?	행동
Unified Manager를 사용하여 식별된 모든 개체의 문제를 해결하세요.	모두 수정 버튼을 클릭하세요.
지금은 식별된 개체에 대한 문제를 해결하지 말고, 이벤트가 다시 발생할 때까지 이 관리 작업을 숨기세요.	아래쪽 화살표를 클릭하고 *모두 닫기*를 클릭하세요.
식별된 일부 개체의 문제만 해결합니다.	관리 작업의 이름을 클릭하면 목록이 확장되고 모든 개별 수정 작업이 표시됩니다. 그런 다음 개별 관리 작업을 수정하거나 해제하는 단계를 따르세요.

당신은 무엇을 하고 싶습니까?	행동
Unified Manager를 이용해 문제를 해결하세요.	수정 버튼을 클릭하세요.
지금은 문제를 해결하지 말고 이벤트가 다시 발생할 때까지 이 관리 작업을 숨기세요.	아래쪽 화살표를 클릭하고 *닫기*를 클릭하세요.

당신은 무엇을 하고 싶습니까?	행동
이 이벤트에 대한 세부 정보를 표시하면 문제를 더 잘 이해할 수 있습니다.	- 수정 버튼을 클릭하고 나타나는 대화 상자에서 적용될 수정 사항을 검토하세요. - 아래쪽 화살표를 클릭하고 *이벤트 세부 정보 보기*를 클릭하면 이벤트 세부 정보 페이지가 표시됩니다. 문제를 해결하려면 두 결과 페이지 중 하나에서 *수정*을 클릭하세요.
문제를 더 잘 이해할 수 있도록 이 저장소 개체에 대한 세부 정보를 표시합니다.	스토리지 개체의 이름을 클릭하면 성능 탐색기 또는 상태 세부 정보 페이지에 세부 정보가 표시됩니다.

어떤 경우에는 수정 사항이 다음 15분 구성 폴에 반영됩니다. 다른 경우에는 구성 변경 사항을 검증하고 이벤트가 더 이상 사용되지 않도록 설정하는 데 최대 몇 시간이 걸릴 수 있습니다.

완료되었거나 진행 중인 관리 작업 목록을 보려면 필터 아이콘을 클릭하고 완료 또는 *진행 중*을 선택하세요.

모든 작업은 직렬 방식으로 실행되므로 진행 중 패널을 볼 때 일부 개체는 상태가 *진행 중*인 반면 다른 개체는 상태가 *예정*인 경우가 있습니다. 즉, 아직 구현을 기다리는 중입니다.

수정하기로 선택한 관리 작업의 상태를 확인하세요.

관리 작업 페이지에서 수정하기로 선택한 모든 관리 작업의 상태를 볼 수 있습니다. 대부분의 작업은 Unified Manager가 ONTAP 명령을 클러스터로 보낸 후 매우 빠르게 *완료*로 표시됩니다. 하지만 볼륨을 이동하는 등의 일부 작업은 시간이 더 오래 걸릴 수 있습니다.

관리 작업 페이지에는 세 가지 필터가 있습니다.

- *완료*는 성공적으로 완료된 관리 작업과 실패한 관리 작업을 모두 표시합니다. *실패한 작업*은 실패 이유를 제공하여 문제를 수동으로 해결할 수 있도록 합니다.
- *진행 중*은 구현 중인 관리 작업과 구현 예정인 관리 작업을 모두 보여줍니다.
- *권장*은 모니터링되는 모든 클러스터에 대해 현재 활성화된 모든 관리 작업을 표시합니다.

단계

1. 왼쪽 탐색 창에서 *관리 작업*을 클릭합니다. 또는 클릭하세요  대시보드의 관리 작업 패널 상단에서 보고 싶은 보기를 선택하세요.

관리 작업 페이지가 표시됩니다.

2. 설명 필드에서 관리 작업 옆에 있는 캐럿 아이콘을 클릭하면 문제에 대한 세부 정보와 문제를 해결하는 데 사용되는 명령을 볼 수 있습니다.
3. 실패한 작업을 보려면 완료 보기에서 상태 열을 기준으로 정렬하세요. 같은 목적으로 필터 도구를 사용할 수 있습니다.
4. 실패한 관리 작업에 대한 자세한 정보를 보거나 권장 관리 작업을 수정하려는 경우 관리 작업 옆에 있는 캐럿 아이콘을 클릭한 후 확장된 영역에서 이벤트 세부 정보 보기*를 클릭하면 됩니다. 해당 페이지에서 *수정* 버튼을 사용할 수 있습니다.

Unified Manager가 해결할 수 있는 문제는 무엇입니까?

Active IQ Unified Manager의 자동 수정 기능을 사용하면 특정 ONTAP 문제를 해결하거나 랜섬웨어 모니터링과 같은 특정 ONTAP 기능을 Unified Manager를 통해 효과적으로 관리할 수 있습니다.

이 표에서는 Unified Manager 웹 UI의 수정 또는 모두 수정 버튼을 통해 직접 관리할 수 있는 ONTAP 문제 또는 기능에 대해 설명합니다.

이벤트 이름 및 설명	관리 조치	"수정" 작업
볼륨 공간 가득 참 볼륨 공간이 거의 부족하여 용량 가득 참 임계값을 초과했습니다. 이 임계값은 기본적으로 볼륨 크기의 90%로 설정됩니다.	볼륨 자동 증가 활성화	Unified Manager는 이 볼륨에 대해 볼륨 자동 증가가 구성되어 있지 않다고 판단하므로 필요에 따라 볼륨 용량이 증가하도록 이 기능을 활성화합니다.
Inode가 가득 찼습니다 이 볼륨의 inode가 부족하여 새로운 파일을 수용할 수 없습니다.	볼륨의 inode 수 증가	볼륨의 inode 수가 2% 증가합니다.
스토리지 계층 정책 불일치가 감지되었습니다. 볼륨에 비활성 데이터가 많고 현재 계층화 정책이 "스냅샷 전용" 또는 "없음"으로 설정되어 있습니다.	자동 클라우드 티어링 활성화	볼륨이 이미 FabricPool에 있으므로 계층화 정책이 "자동"으로 변경되어 비활성 데이터가 비용이 저렴한 클라우드 계층으로 이동됩니다.
스토리지 계층 불일치가 감지되었습니다. 볼륨에는 비활성 데이터가 많이 있지만 클라우드 지원 스토리지 계층(FabricPool)에 상주하지 않습니다.	볼륨의 스토리지 계층 변경	볼륨을 클라우드 지원 스토리지 계층으로 이동하고 계층화 정책을 "자동"으로 설정하여 비활성 데이터를 클라우드 계층으로 이동합니다.
감사 로그 비활성화됨 저장소 VM에 대한 감사 로그가 활성화되지 않았습니다.	스토리지 VM에 대한 감사 로깅 활성화	스토리지 VM에서 감사 로깅을 활성화합니다. 스토리지 VM에는 이미 로컬 또는 원격 감사 로그 위치가 구성되어 있어야 합니다.
로그인 배너 비활성화됨 클러스터의 로그인 배너를 활성화하여 액세스 제한을 명확히 하여 보안을 강화해야 합니다.	클러스터에 대한 로그인 배너 설정	클러스터 로그인 배너를 "권한이 있는 사용자만 접근 가능"으로 설정합니다.

이벤트 이름 및 설명	관리 조치	"수정" 작업
로그인 배너 비활성화됨 스토리지 VM에 대한 로그인 배너를 활성화하여 액세스 제한을 명확히 하여 보안을 강화해야 합니다.	스토리지 VM에 대한 로그인 배너 설정	스토리지 VM 로그인 배너를 "권한이 있는 사용자만 액세스 가능"으로 설정합니다.
SSH가 안전하지 않은 암호를 사용하고 있습니다 접미사 "-cbc"가 붙은 암호는 안전하지 않은 것으로 간주됩니다.	클러스터에서 안전하지 않은 암호 제거	클러스터에서 aes192-cbc, aes128-cbc 등의 안전하지 않은 암호를 제거합니다.
SSH가 안전하지 않은 암호를 사용하고 있습니다 접미사 "-cbc"가 붙은 암호는 안전하지 않은 것으로 간주됩니다.	스토리지 VM에서 안전하지 않은 암호 제거	스토리지 VM에서 aes192-cbc 및 aes128-cbc와 같은 안전하지 않은 암호를 제거합니다.
AutoSupport HTTPS 전송이 비활성화되었습니다. AutoSupport 메시지를 기술 지원팀에 보내는 데 사용되는 전송 프로토콜은 암호화되어야 합니다.	AutoSupport 메시지의 전송 프로토콜로 HTTPS를 설정합니다.	클러스터의 AutoSupport 메시지에 대한 전송 프로토콜로 HTTPS를 설정합니다.
클러스터 부하 불균형 임계값 위반 클러스터 내 노드 간에 부하가 불균형하다는 것을 나타냅니다. 이 이벤트는 노드 간 성능 용량 사용 분산이 30%를 초과할 때 생성됩니다.	클러스터 워크로드 균형 조정	Unified Manager는 불균형을 줄이기 위해 한 노드에서 다른 노드로 이동할 최적의 볼륨을 식별한 다음 볼륨을 이동합니다.
클러스터 용량 불균형 임계값 위반 클러스터 내 집계 간의 용량 불균형을 나타냅니다. 이 이벤트는 집계 간 사용된 용량 차이가 70%를 넘을 때 생성됩니다.	클러스터 용량 균형	Unified Manager는 불균형을 줄이기 위해 한 집계에서 다른 집계로 이동할 최적의 볼륨을 식별한 다음 볼륨을 이동합니다.
성능 용량 사용 임계값 위반 한 개 이상의 활성 작업 부하로 사용률을 줄이지 않으면 노드의 부하가 과도하게 사용될 수 있음을 나타냅니다. 이 이벤트는 노드 성능 용량 사용 값이 12시간 이상 100% 이상일 때 생성됩니다.	노드의 높은 부하 제한	Unified Manager는 가장 높은 IOPS를 가진 볼륨을 식별하고 과거 예상 IOPS 수준과 최대 IOPS 수준을 사용하여 QoS 정책을 적용하여 노드의 부하를 줄입니다.

이벤트 이름 및 설명	관리 조치	"수정" 작업
동적 이벤트 경고 임계값 위반됨 일부 작업 부하가 비정상적으로 높아 노드가 이미 과부하 상태에서 작동하고 있음을 나타냅니다.	노드의 과부하를 줄이세요	Unified Manager는 가장 높은 IOPS를 가진 볼륨을 식별하고 과거 예상 IOPS 수준과 최대 IOPS 수준을 사용하여 QoS 정책을 적용하여 노드의 부하를 줄입니다.
인수가 불가능합니다 현재 장애 조치가 비활성화되어 있으므로 중단이나 재부팅 중에는 노드 리소스에 대한 액세스가 노드를 다시 사용할 수 있을 때까지 손실됩니다.	노드 장애 조치 활성화	Unified Manager는 클러스터의 모든 노드에서 장애 조치를 활성화하기 위해 적절한 명령을 보냅니다.
옵션 Cf.takeover.on_panic이 OFF로 구성되었습니다. nodeshell 옵션 "cf.takeover.on_panic"이 *off*로 설정되어 있어 HA 구성 시스템에서 문제가 발생할 수 있습니다.	패닉 시 인수 활성화	Unified Manager는 클러스터에 적절한 명령을 보내 이 설정을 *켜짐*으로 변경합니다.
nodeshell 옵션 snapmirror.enable을 비활성화합니다. 이전 nodeshell 옵션인 "snapmirror.enable"이 *on*으로 설정되어 있어 ONTAP 9.3 이상으로 업그레이드한 후 부팅하는 동안 문제가 발생할 수 있습니다.	snapmirror.enable 옵션을 off로 설정합니다.	Unified Manager는 클러스터에 적절한 명령을 보내 이 설정을 *off*로 변경합니다.
Telnet 활성화됨 Telnet은 안전하지 않고 암호화되지 않은 방식으로 데이터를 전달하기 때문에 잠재적인 보안 문제가 있음을 나타냅니다.	Telnet 비활성화	Unified Manager는 클러스터에 적절한 명령을 보내 Telnet을 비활성화합니다.

이벤트 이름 및 설명	관리 조치	"수정" 작업
스토리지 VM 랜섬웨어 방지 학습 구성 랜섬웨어 방지 모니터링 라이선스가 있는 클러스터를 주기적으로 확인합니다. 해당 클러스터에서 스토리지 VM이 NFS 또는 SMB 볼륨만 지원하는지 여부를 검증합니다.	스토리지 VM을 다음 위치에 두십시오. learning 랜섬웨어 방지 모니터링 모드	Unified Manager는 랜섬웨어 방지 모니터링을 설정합니다. learning 클러스터 관리 콘솔을 통해 스토리지 VM의 상태를 확인합니다. 스토리지 VM에 생성된 모든 새 볼륨에 대한 랜섬웨어 방지 모니터링은 자동으로 학습 모드로 전환됩니다. 이러한 기능을 통해 ONTAP 볼륨의 활동 패턴을 학습하고 잠재적인 악의적 공격으로 인한 이상을 감지할 수 있습니다.
볼륨 랜섬웨어 방지 학습 구성 랜섬웨어 방지 모니터링 라이선스가 있는 클러스터를 주기적으로 확인합니다. 해당 클러스터에서 볼륨이 NFS 또는 SMB 서비스만 지원하는지 여부를 검증합니다.	볼륨을 넣어 learning 랜섬웨어 방지 모니터링 모드	Unified Manager는 랜섬웨어 방지 모니터링을 설정합니다. learning 클러스터 관리 콘솔을 통해 볼륨에 대한 상태를 확인합니다. 이러한 기능을 통해 ONTAP 볼륨의 활동 패턴을 학습하고 잠재적인 악의적 공격으로 인한 이상을 감지할 수 있습니다.
볼륨 랜섬웨어 방지 활성화 랜섬웨어 방지 모니터링 라이선스가 있는 클러스터를 주기적으로 확인합니다. 볼륨이 다음 위치에 있는지 감지합니다. learning 45일 이상 랜섬웨어 방지 모니터링 모드를 유지하고, 활성 모드로 전환할 가능성을 판단합니다.	볼륨을 넣어 active 랜섬웨어 방지 모니터링 모드	Unified Manager는 랜섬웨어 방지 모니터링을 설정합니다. active 클러스터 관리 콘솔을 통해 볼륨에 대해. 이러한 기능을 통해 ONTAP 볼륨의 활동 패턴을 학습하고 잠재적인 악의적 공격으로 인한 이상을 감지하며 데이터 보호 조치에 대한 알림을 생성할 수 있습니다.
볼륨 랜섬웨어 방지 비활성화 랜섬웨어 방지 모니터링 라이선스가 있는 클러스터를 주기적으로 확인합니다. 볼륨에서 활성 랜섬웨어 모니터링 중에 반복적인 알림을 감지합니다(예: 잠재적인 랜섬웨어 공격에 대한 경고가 30일 동안 여러 번 반환됨).	볼륨에서 랜섬웨어 방지 모니터링 비활성화	Unified Manager는 클러스터 관리 콘솔을 통해 볼륨에 대한 랜섬웨어 방지 모니터링을 비활성화합니다.

스크립트를 통해 관리 작업 재정의

사용자 정의 스크립트를 만들고 이를 알림에 연결하여 특정 이벤트에 대한 특정 작업을 수행할 수 있으며, 관리 작업 페이지나 Unified Manager 대시보드에서 해당 이벤트에 대해 제공되는 기본 관리 작업을 선택하지 않을 수 있습니다.

Unified Manager에서 제공하는 관리 작업 기능의 일부로 이벤트 유형에 대한 특정 작업을 수행하고 이를 수정하지

않으려는 경우, 특정 작업에 대한 사용자 지정 스크립트를 구성할 수 있습니다. 그런 다음 스크립트를 해당 이벤트 유형에 대한 알림과 연결하고 이러한 이벤트를 개별적으로 처리할 수 있습니다. 이 경우, 관리 작업 페이지나 Unified Manager 대시보드에서 해당 특정 이벤트 유형에 대한 관리 작업이 생성되지 않습니다.

클러스터 관리

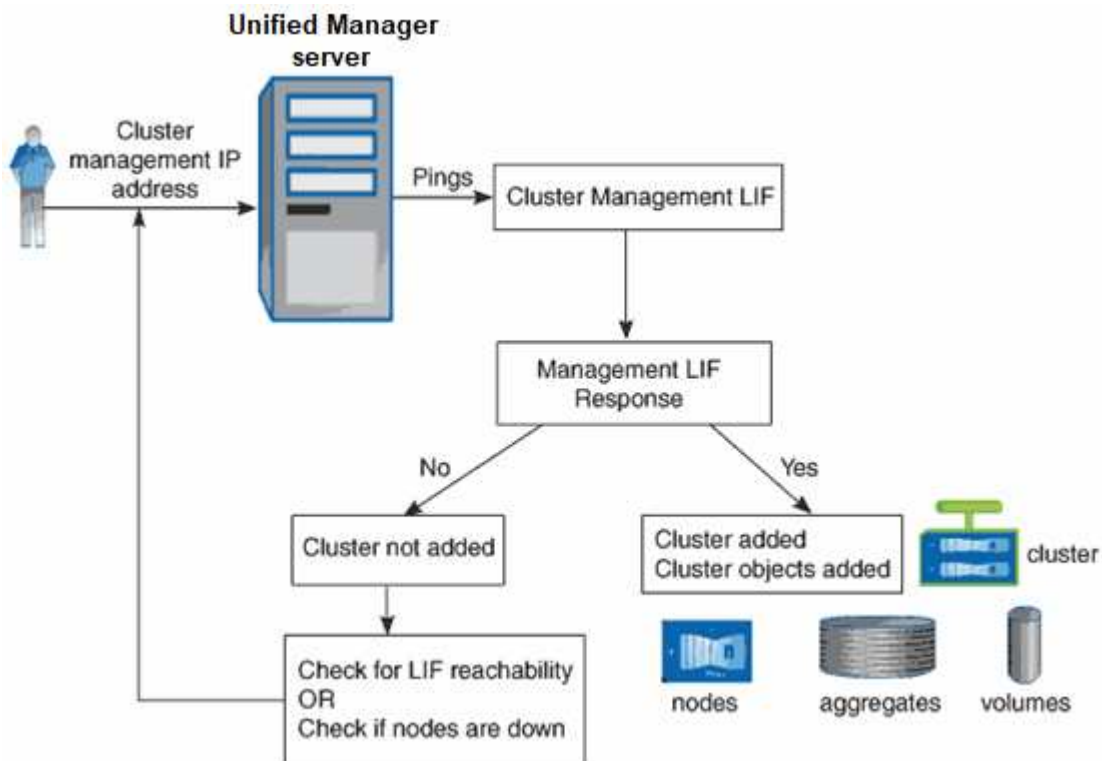
Unified Manager를 사용하여 ONTAP 클러스터를 모니터링, 추가, 편집, 제거하여 관리할 수 있습니다.

클러스터 검색 프로세스 작동 방식

Unified Manager에 클러스터를 추가하면 서버에서 클러스터 개체를 검색하여 데이터베이스에 추가합니다. 검색 프로세스가 작동하는 방식을 이해하면 조직의 클러스터와 해당 개체를 관리하는 데 도움이 됩니다.

클러스터 구성 정보를 수집하기 위한 모니터링 간격은 15분입니다. 예를 들어, 클러스터를 추가한 후 Unified Manager UI에 클러스터 개체가 표시되는 데 15분이 걸립니다. 이 기간은 클러스터를 변경할 때도 적용됩니다. 예를 들어, 클러스터의 SVM에 두 개의 새 볼륨을 추가하는 경우 다음 폴링 간격(최대 15분) 후에 UI에서 해당 새 객체를 볼 수 있습니다.

다음 이미지는 발견 과정을 보여줍니다.



새 클러스터의 모든 개체가 검색된 후 Unified Manager는 지난 15일 동안의 과거 성능 데이터를 수집하기 시작합니다. 이러한 통계는 데이터 연속성 수집 기능을 사용하여 수집됩니다. 이 기능을 사용하면 클러스터가 추가된 직후부터 2주 이상에 걸친 성능 정보를 바로 확인할 수 있습니다. 데이터 연속성 수집 주기가 완료되면 기본적으로 5분마다 실시간 클러스터 성능 데이터가 수집됩니다.



15일간의 성능 데이터를 수집하는 데 CPU가 많이 사용되므로, 너무 많은 클러스터에서 동시에 데이터 연속성 수집 폴링이 실행되지 않도록 새 클러스터를 추가하는 작업을 단계적으로 수행하는 것이 좋습니다.

모니터링되는 클러스터 목록 보기

클러스터 설정 페이지를 사용하여 클러스터 인벤토리를 볼 수 있습니다. 클러스터의 이름이나 IP 주소, 통신 상태 등 클러스터에 대한 세부 정보를 볼 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *클러스터 설정*을 클릭합니다.

Unified Manager에서 관리하는 스토리지 환경의 모든 클러스터가 표시됩니다. 클러스터 목록은 컬렉션 상태 심각도 수준 열에 따라 정렬됩니다. 열 머리글을 클릭하면 클러스터를 다양한 열로 정렬할 수 있습니다.

클러스터 추가

클러스터를 모니터링할 수 있도록 Active IQ Unified Manager 에 클러스터를 추가할 수 있습니다. 여기에는 클러스터의 상태, 용량, 성능, 구성 등의 클러스터 정보를 얻는 기능이 포함되어 있어 발생할 수 있는 문제를 찾아 해결할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 역할이나 스토리지 관리자 역할이 있어야 합니다.
- 다음 정보가 필요합니다.
 - Unified Manager는 온프레미스 ONTAP 클러스터, ONTAP Select, Cloud Volumes ONTAP 지원합니다.
 - 클러스터에 대한 호스트 이름이나 클러스터 관리 IP 주소(IPv4 또는 IPv6)가 있어야 합니다.

호스트 이름을 사용하는 경우 클러스터 관리 LIF에 대한 클러스터 관리 IP 주소로 확인되어야 합니다. 노드 관리 LIF를 사용하면 작업이 실패합니다.

- 클러스터에 액세스하려면 사용자 이름과 비밀번호가 필요합니다.

이 계정에는 *admin* 역할이 있어야 하며 애플리케이션 액세스 권한이 *ontapi*, *console*, *_http_*로 설정되어 있어야 합니다.

- HTTPS 프로토콜(일반적으로 포트 443)을 사용하여 클러스터에 연결하려면 포트 번호를 알아야 합니다.
- 클러스터는 ONTAP 버전 9.9 이상 소프트웨어를 실행해야 합니다.
- Unified Manager 서버에 충분한 공간이 있어야 합니다. 이미 90% 이상의 공간이 사용된 경우 서버에 클러스터를 추가할 수 없습니다.
- 귀하에게 필요한 인증서가 있습니다.

SSL(HTTPS) 인증서: 이 인증서는 Unified Manager의 소유입니다. Unified Manager를 새로 설치하면 기본

자체 서명 SSL(HTTPS) 인증서가 생성됩니다. NetApp 보안을 강화하기 위해 CA 서명 인증서로 업그레이드할 것을 권장합니다. 서버 인증서가 만료된 경우 인증서를 다시 생성하고 Unified Manager를 다시 시작하여 서비스에 새 인증서를 적용해야 합니다. SSL 인증서 재생성에 대한 자세한 내용은 다음을 참조하세요. "[HTTPS 보안 인증서 생성](#)".

EMS 인증서: 이 인증서는 Unified Manager의 소유입니다. ONTAP 에서 수신한 EMS 알림에 대한 인증 과정에서 사용됩니다.

상호 **TLS** 통신을 위한 인증서: Unified Manager와 ONTAP 간 상호 TLS 통신 중에 사용됩니다. 인증서 기반 인증은 ONTAP 버전을 기반으로 클러스터에 대해 활성화됩니다. ONTAP 버전을 실행하는 클러스터가 9.5보다 낮은 경우 인증서 기반 인증이 활성화되지 않습니다.

Unified Manager의 이전 버전을 업데이트하는 경우, 클러스터에 대해 인증서 기반 인증이 자동으로 활성화되지 않습니다. 하지만 클러스터 세부 정보를 수정하고 저장하면 해당 기능을 활성화할 수 있습니다. 인증서가 만료된 경우 새 인증서를 통합하기 위해 인증서를 다시 생성해야 합니다. 인증서 보기 및 재생성에 대한 자세한 내용은 다음을 참조하세요. "[클러스터 편집](#)".



- 웹 UI에서 클러스터를 추가할 수 있으며, 인증서 기반 인증이 자동으로 활성화됩니다.
- Unified Manager CLI를 통해 클러스터를 추가할 수 있으며, 인증서 기반 인증은 기본적으로 활성화되어 있지 않습니다. Unified Manager CLI를 사용하여 클러스터를 추가하는 경우 Unified Manager UI를 사용하여 클러스터를 편집해야 합니다. 당신은 볼 수 있습니다 "[지원되는 Unified Manager CLI 명령](#)" Unified Manager CLI를 사용하여 클러스터를 추가합니다.
- 클러스터에 대해 인증서 기반 인증이 활성화되어 있고 서버에서 Unified Manager 백업을 가져와 호스트 이름이나 IP 주소가 변경된 다른 Unified Manager 서버로 복원하는 경우 클러스터 모니터링이 실패할 수 있습니다. 실패를 방지하려면 클러스터 세부 정보를 편집하고 저장하세요. 클러스터 세부 정보 편집에 대한 자세한 내용은 다음을 참조하세요. "[클러스터 편집](#)".
- 클러스터 수준에서 Active IQ 인터페이스는 인증 방법 "cert"에 대해 두 개의 새로운 사용자 그룹 항목을 추가합니다.

+

클러스터 인증서: 이 인증서는 ONTAP 의 소유입니다. 만료된 인증서로는 Unified Manager에 클러스터를 추가할 수 없습니다. 인증서가 이미 만료된 경우 클러스터를 추가하기 전에 인증서를 다시 생성해야 합니다. 인증서 생성에 대한 정보는 지식 기반(KB) 문서를 참조하세요. "[System Manager 사용자 인터페이스에서 ONTAP 자체 서명 인증서를 갱신하는 방법](#)".

- Unified Manager의 단일 인스턴스는 특정 수의 노드를 지원할 수 있습니다. 지원되는 노드 수를 초과하는 환경을 모니터링해야 하는 경우 일부 클러스터를 모니터링하기 위해 Unified Manager의 추가 인스턴스를 설치해야 합니다. 지원되는 노드 수 목록을 보려면 다음을 참조하세요. "[Unified Manager 모범 사례 가이드](#)".

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *클러스터 설정*을 클릭합니다.
2. 클러스터 설정 페이지에서 *추가*를 클릭합니다.
3. 클러스터 추가 대화 상자에서 필요에 따라 값을 지정한 다음 *제출*을 클릭합니다.
4. 호스트 승인 대화 상자에서 *인증서 보기*를 클릭하여 클러스터에 대한 인증서 정보를 확인합니다.
5. *예*를 클릭하세요.

클러스터 세부 정보를 저장한 후 클러스터의 상호 TLS 통신에 대한 인증서를 볼 수 있습니다.

인증서 기반 인증이 활성화되어 있지 않으면 Unified Manager는 클러스터가 처음 추가될 때만 인증서를 확인합니다. Unified Manager는 ONTAP 에 대한 각 API 호출에 대한 인증서를 확인하지 않습니다.

새 클러스터의 모든 개체가 검색된 후 Unified Manager는 지난 15일 동안의 과거 성능 데이터를 수집하기 시작합니다. 이러한 통계는 데이터 연속성 수집 기능을 사용하여 수집됩니다. 이 기능을 사용하면 클러스터가 추가된 직후부터 2주 이상에 걸친 성능 정보를 바로 확인할 수 있습니다. 데이터 연속성 수집 주기가 완료되면 기본적으로 5분마다 실시간 클러스터 성능 데이터가 수집됩니다.



- 15일간의 성능 데이터를 수집하는 데는 CPU가 많이 사용됩니다. NetApp 너무 많은 클러스터에서 동시에 데이터 연속성 수집 폴링이 실행되지 않도록 새 클러스터를 추가하는 작업을 단계적으로 수행할 것을 권장합니다. 또한, 데이터 연속성 수집 기간 동안 Unified Manager를 다시 시작하면 수집이 중단되고 누락된 기간의 성능 차트에 간격이 표시됩니다.
- 9.14.1 이상 버전의 ONTAP 클러스터를 추가하면 클라우드 에이전트 기능을 통해 통신이 이루어집니다. ONTAP 읽기 전용 권한이 있는 내부 서비스 계정 사용자(예: clus-agent-xxxx)를 자동으로 생성합니다. Unified Manager는 다음과 같은 경우 해당 클러스터에서 데이터 수집을 중지합니다. clus-agent 사용자가 삭제되었습니다.

클러스터를 추가할 수 없다는 오류 메시지가 나타나면 다음 문제가 있는지 확인하세요.



- 두 시스템의 시계가 동기화되지 않고 Unified Manager HTTPS 인증서 시작 날짜가 클러스터의 날짜보다 이후인 경우. NTP나 유사한 서비스를 사용하여 시계가 동기화되었는지 확인해야 합니다.
- 클러스터가 EMS 알림 대상의 최대 수에 도달한 경우 Unified Manager 주소를 추가할 수 없습니다. 기본적으로 클러스터에서는 EMS 알림 대상을 20개만 정의할 수 있습니다.

관련 정보

["사용자 추가"](#)

["클러스터 목록 및 세부 정보 보기"](#)

["CA 서명 및 반환된 HTTPS 인증서 설치"](#)

클러스터 편집

클러스터 편집 대화 상자를 사용하여 호스트 이름이나 IP 주소, 사용자 이름, 비밀번호, 포트 등 기존 클러스터의 설정을 수정할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이나 스토리지 관리자 역할이 있어야 합니다.



Unified Manager 9.7부터 HTTPS를 사용해서만 클러스터를 추가할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *클러스터 설정*을 클릭합니다.
2. 클러스터 설정 페이지에서 편집하려는 클러스터를 선택한 다음 *편집*을 클릭합니다.
3. 클러스터 편집 대화 상자에서 필요에 따라 값을 수정합니다. + Unified Manager에 추가된 클러스터의 세부 정보를 수정한 경우 ONTAP 버전에 따라 상호 TLS 통신에 대한 인증서 세부 정보를 볼 수 있습니다. ONTAP 버전에 대한

자세한 내용은 다음을 참조하세요. "[상호 TLS 통신을 위한 인증서](#)". + 인증서 세부정보*를 클릭하면 인증서 세부정보를 볼 수 있습니다. 인증서가 만료된 경우 *다시 생성 버튼을 클릭하여 새 인증서를 통합하세요.

4. *제출*을 클릭하세요.
5. 호스트 승인 대화 상자에서 *인증서 보기*를 클릭하여 클러스터에 대한 인증서 정보를 확인합니다.
6. *예*를 클릭하세요.

관련 정보

["사용자 추가"](#)

["클러스터 목록 및 세부 정보 보기"](#)

클러스터 제거

클러스터 설정 페이지를 사용하여 Unified Manager에서 클러스터를 제거할 수 있습니다. 예를 들어, 클러스터 검색에 실패하거나 스토리지 시스템을 해제하려는 경우 클러스터를 제거할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이나 스토리지 관리자 역할이 있어야 합니다.

이 작업은 Unified Manager에서 선택한 클러스터를 제거합니다. 클러스터가 제거되면 더 이상 모니터링되지 않습니다. 제거된 클러스터에 등록된 Unified Manager 인스턴스도 클러스터에서 등록 해제됩니다.

클러스터를 제거하면 Unified Manager에서 모든 스토리지 개체, 기록 데이터, 스토리지 서비스 및 모든 관련 이벤트가 삭제됩니다. 이러한 변경 사항은 다음 데이터 수집 주기 이후 인벤토리 페이지와 세부 정보 페이지에 반영됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *클러스터 설정*을 클릭합니다.
2. 클러스터 설정 페이지에서 제거할 클러스터를 선택하고 *제거*를 클릭합니다.
3. 데이터 소스 제거 메시지 대화 상자에서 *제거*를 클릭하여 제거 요청을 확인합니다.

관련 정보

["사용자 추가"](#)

["클러스터 목록 및 세부 정보 보기"](#)

클러스터 재발견

클러스터 설정 페이지에서 클러스터를 수동으로 다시 검색하여 클러스터의 상태, 모니터링 상태 및 성능 상태에 대한 최신 정보를 얻을 수 있습니다.

클러스터를 업데이트하려는 경우(예: 공간이 부족하여 집계 크기를 늘리는 경우) 클러스터를 수동으로 다시 검색할 수 있으며 Unified Manager에서 변경 사항을 검색하도록 할 수 있습니다.

Unified Manager가 OnCommand Workflow Automation (WFA)과 페어링되면 페어링을 통해 WFA에서 캐시된 데이터가 다시 수집됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *클러스터 설정*을 클릭합니다.
2. 클러스터 설정 페이지에서 *재검색*을 클릭합니다.

Unified Manager는 선택된 클러스터를 다시 검색하고 최신 상태 및 성능 상태를 표시합니다.

관련 정보

["클러스터 목록 및 세부 정보 보기"](#)

VMware 가상 인프라 모니터링

Active IQ Unified Manager 가상 인프라의 가상 머신(VM)에 대한 가시성을 제공하고 가상 환경에서 스토리지 및 성능 문제를 모니터링하고 해결할 수 있도록 해줍니다. 이 기능을 사용하면 스토리지 환경에서 지연 문제가 있는지, 또는 vCenter Server에서 보고된 성능 이벤트가 있는지 확인할 수 있습니다.

ONTAP 에서의 일반적인 가상 인프라 배포에는 컴퓨팅, 네트워크 및 스토리지 계층에 걸쳐 분산된 다양한 구성 요소가 있습니다. VM 애플리케이션의 성능 지연은 각 계층의 다양한 구성 요소가 겪는 지연 시간의 조합으로 인해 발생할 수 있습니다. 이 기능은 가상 환경에서 성능 문제를 분석하고 문제가 발생한 구성 요소를 파악해야 하는 스토리지 및 vCenter Server 관리자와 IT 전문가에게 유용합니다.

이제 VMware 섹션의 vCenter 메뉴에서 vCenter Server에 액세스할 수 있습니다. 나열된 각 가상 머신의 미리보기에는 새 브라우저에서 vCenter Server를 시작하는 TOPOLOGY VIEW에 **VCENTER SERVER** 링크가 있습니다. 토폴로지 확장 버튼을 사용하여 vCenter Server를 시작하고 **vCenter**에서 보기 버튼을 클릭하여 vCenter Server의 데이터 저장소를 볼 수도 있습니다.

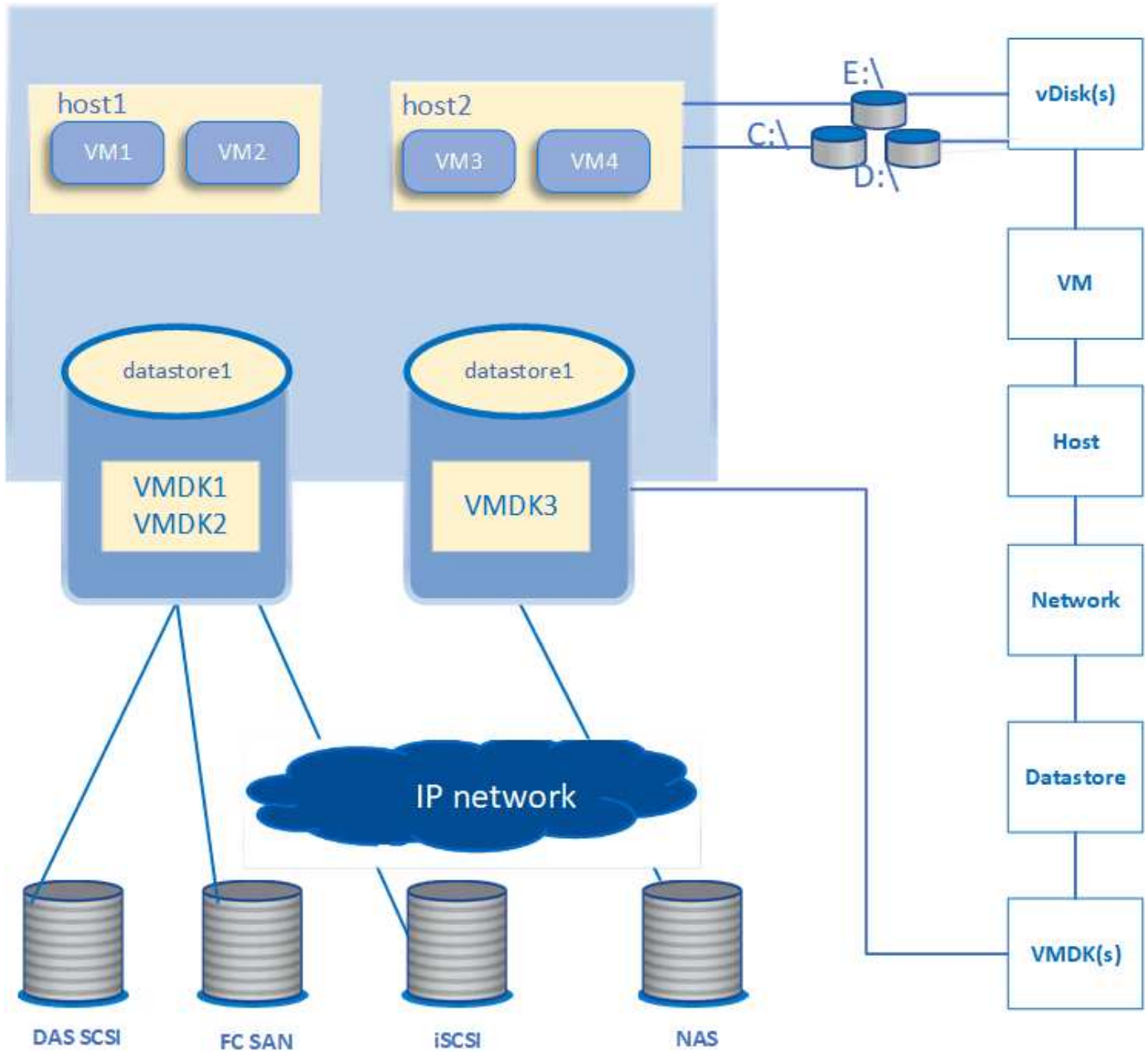
Unified Manager는 가상 환경의 기본 하위 시스템을 토폴로지 뷰로 표시하여 컴퓨팅 노드, 네트워크 또는 스토리지에서 지연 문제가 발생했는지 여부를 확인합니다. 또한 이 뷰에서는 성능 지연을 유발하는 특정 객체를 강조 표시하여 수정 조치를 취하고 기본 문제를 해결합니다.

ONTAP 스토리지에 배포된 가상 인프라에는 다음 개체가 포함됩니다.

- vCenter Server: 가상 환경에서 VMware VM, ESXi 호스트 및 모든 관련 구성 요소를 관리하기 위한 중앙 집중식 제어 평면입니다. vCenter Server에 대한 자세한 내용은 VMware 설명서를 참조하세요.
- 호스트: VMware의 가상화 소프트웨어인 ESXi를 실행하고 VM을 호스팅하는 물리적 또는 가상 시스템입니다.
- 데이터스토어: 데이터스토어는 ESXi 호스트에 연결된 가상 스토리지 개체입니다. 데이터스토어는 LUN이나 볼륨과 같은 ONTAP의 관리 가능한 스토리지 엔티티로, 로그 파일, 스크립트, 구성 파일, 가상 디스크와 같은 VM 파일의 저장소로 사용됩니다. 이들은 SAN이나 IP 네트워크 연결을 통해 환경 내의 호스트에 연결됩니다. ONTAP 외부의 데이터스토어가 vCenter Server에 매핑된 경우 Unified Manager에서 지원되거나 표시되지 않습니다.
- VM: VMware 가상 머신.
- 가상 디스크: VMDK라는 확장명을 가진 VM에 속한 데이터 저장소의 가상 디스크입니다. 가상 디스크의 데이터는 해당 VMDK에 저장됩니다.
- VMDK: 가상 디스크에 대한 저장 공간을 제공하는 데이터스토어의 가상 머신 디스크입니다. 각 가상 디스크에는 해당 VMDK가 있습니다.

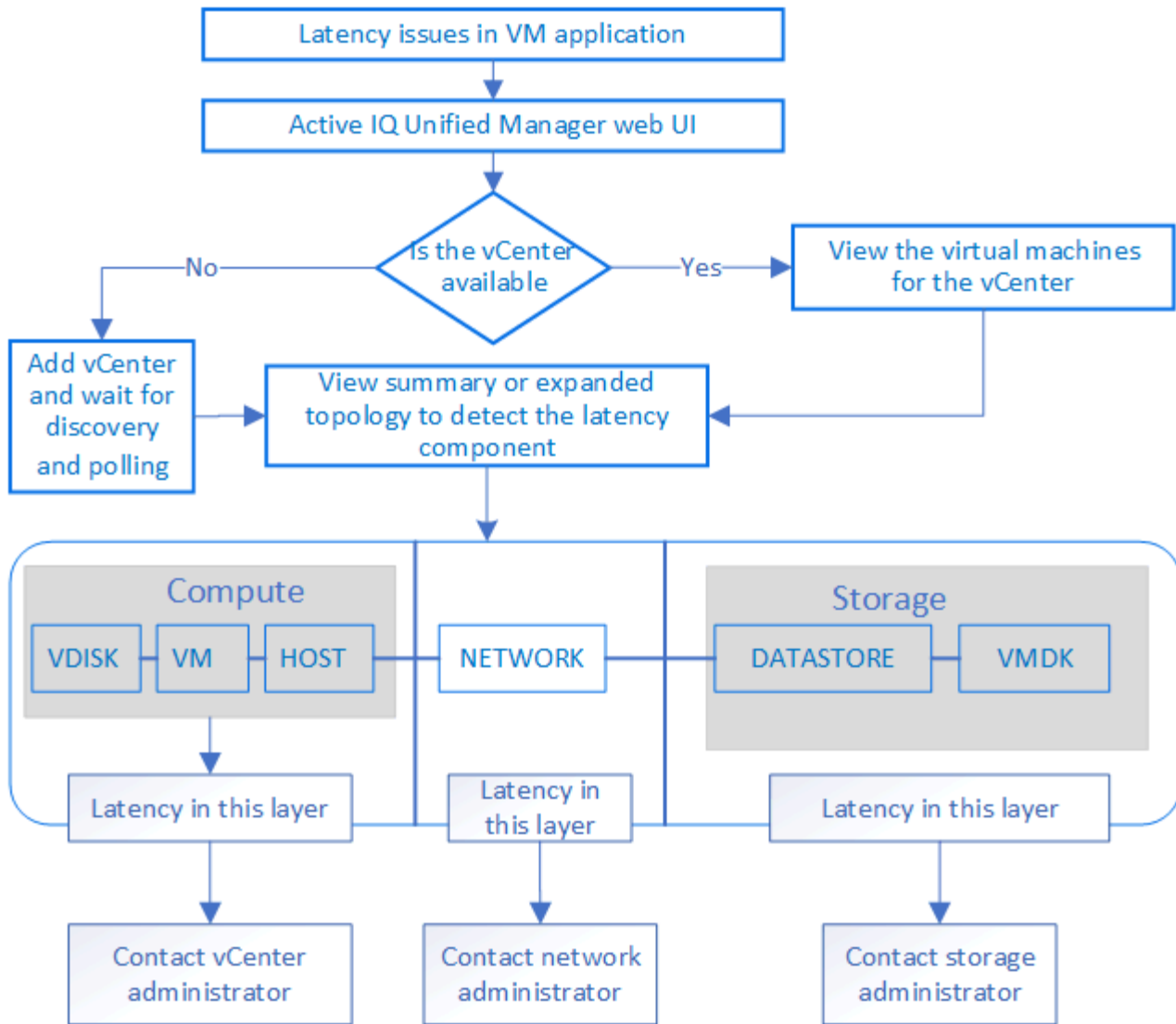
이러한 객체는 VM 토폴로지 뷰에 표현됩니다.

• ONTAP 에서의 VMware 가상화 *



사용자 워크플로

다음 다이어그램은 VM 토폴로지 뷰를 사용하는 일반적인 사용 사례를 보여줍니다.



지원되지 않는 사항

- ONTAP 외부에 있고 vCenter Server 인스턴스에 매핑된 데이터스토어는 Unified Manager에서 지원되지 않습니다. 해당 데이터스토어에 가상 디스크가 있는 VM도 지원되지 않습니다.
- 여러 LUN에 걸쳐 있는 데이터 저장소는 지원되지 않습니다.
- 데이터 LIF(액세스 엔드포인트)를 매핑하기 위해 NAT(네트워크 주소 변환)를 사용하는 데이터 저장소는 지원되지 않습니다.
- 여러 LIF 구성에서 동일한 IP 주소를 가진 서로 다른 클러스터에 볼륨이나 LUN을 데이터 저장소로 내보내는 것은 Unified Manager가 어떤 데이터 저장소가 어떤 클러스터에 속하는지 식별할 수 없기 때문에 지원되지 않습니다.

예: 클러스터 A에 데이터 저장소 A가 있다고 가정합니다. 데이터 저장소 A는 동일한 IP 주소 xxxx로 데이터 LIF를 통해 내보내지고 VM A는 이 데이터 저장소에 생성됩니다. 마찬가지로 클러스터 B에는 데이터 저장소 B가 있습니다. 데이터 저장소 B는 동일한 IP 주소 xxxx를 사용하여 데이터 LIF를 통해 내보내지고 VM B는 데이터 저장소 B에 생성됩니다. UM은 VM A의 토폴로지에 대한 데이터 저장소 A를 해당 ONTAP 볼륨/LUN에 매핑하거나 VM B를 매핑할 수 없습니다.

- 데이터 저장소로는 NAS 및 SAN 볼륨(VMFS의 경우 iSCSI 및 FCP)만 지원되며 가상 볼륨(vVols)은 지원되지 않습니다.

- iSCSI 가상 디스크만 지원됩니다. NVMe 및 SATA 유형의 가상 디스크는 지원되지 않습니다.
- 이러한 뷰에서는 다양한 구성 요소의 성능을 분석하기 위한 보고서를 생성할 수 없습니다.
- Unified Manager의 가상 인프라에만 지원되는 스토리지 가상 머신(스토리지 VM) 재해 복구(DR) 설정의 경우, 스위치오버 및 스위치백 시나리오에서 활성 LUN을 가리키도록 vCenter Server에서 구성을 수동으로 변경해야 합니다. 수동 개입 없이는 데이터 저장소에 접근할 수 없게 됩니다.

vCenter Server 보기 및 추가

가상 머신(VM)의 성능을 보고 문제를 해결하려면 연관된 vCenter Server를 Active IQ Unified Manager 인스턴스에 추가해야 합니다.

시작하기 전에

vCenter Server를 추가하거나 보기 전에 다음 사항을 확인하세요.

- vCenter Server 이름을 알고 있습니다.
- vCenter Server의 IP 주소를 알고 있으며 필요한 자격 증명이 있습니다. 자격 증명은 vCenter Server 관리자이거나 vCenter Server에 대한 읽기 전용 액세스 권한이 있는 루트 사용자여야 합니다.
- 추가하려는 vCenter Server는 vSphere 6.5 이상을 실행합니다.



VMware ESXi 및 vCenter Server에 대한 Unified Manager 지원은 영어와 일본어로 제공됩니다.

- vCenter Server의 데이터 수집 설정은 통계 수준으로 설정됩니다. *Level 3* 모든 모니터링 대상에 대해 필요한 수준의 메트릭 수집을 보장합니다. 간격 기간은 다음과 같아야 합니다. *5 minutes*, 그리고 저장 기간은 다음과 같아야 합니다. *1 day*.

자세한 내용은 VMware 설명서의 *_vSphere 모니터링 및 성능 가이드_*에서 “데이터 수집 수준” 섹션을 참조하세요.

- vCenter Server의 대기 시간 값은 대기 시간 값을 성공적으로 계산하기 위해 마이크로초가 아닌 밀리초로 구성됩니다.
- vCenter Server에 데이터스토어를 추가하는 동안 호스트의 IP 주소나 정규화된 도메인 이름(FQDN)을 모두 사용할 수 있습니다. FQDN을 추가하는 경우 Unified Manager 서버에서 도메인 이름을 확인할 수 있는지 확인하세요. 예를 들어 Linux 설치의 경우 도메인 이름이 추가되었는지 확인하십시오. */etc/resolv.conf* 파일.
- vCenter Server의 현재 시간은 vCenter Server 표준 시간대와 동기화됩니다.
- 성공적인 검색을 위해 vCenter Server에 접속할 수 있습니다.
- Unified Manager에 vCenter Server를 추가하면 VMware SDK에 대한 읽기 액세스 권한이 부여됩니다. 이는 구성 폴링에 필요합니다.

추가되고 검색된 모든 vCenter Server에 대해 Unified Manager는 vCenter Server 및 ESXi 서버 세부 정보, ONTAP 매핑, 데이터 저장소 세부 정보, 호스팅된 VM 수 등의 구성 데이터를 수집합니다. 또한 구성 요소의 성능 측정 항목을 수집합니다.

단계

1. **VMWARE** > *vCenter*로 이동하여 vCenter Server가 목록에서 사용 가능한지 확인하세요.



vCenter Server를 사용할 수 없는 경우 vCenter Server를 추가해야 합니다.

- a. *추가*를 클릭하세요.
- b. vCenter Server에 대한 올바른 IP 주소를 추가하고 장치에 접근할 수 있는지 확인하세요.
- c. vCenter Server에 대한 읽기 전용 액세스 권한이 있는 관리자 또는 루트 사용자의 사용자 이름과 비밀번호를 추가합니다.
- d. 기본 443이 아닌 다른 포트를 사용하는 경우 사용자 지정 포트 번호를 추가하세요.
- e. *저장*을 클릭하세요.

성공적으로 검색되면 수락할 수 있는 서버 인증서가 표시됩니다.

인증서를 수락하면 vCenter Server가 사용 가능한 vCenter Server 목록에 추가됩니다. 장치를 추가해도 연결된 VM에 대한 데이터가 수집되지 않으며, 수집은 예약된 간격으로 수행됩니다.

2. vCenter Server를 **vCenters** 페이지에서 사용할 수 있는 경우, 상태 필드 위에 마우스를 올려놓으면 vCenter Server가 예상대로 수행되고 있는지, 아니면 경고나 오류가 있는지 확인할 수 있습니다.



vCenter Server를 추가하면 다음 상태를 볼 수 있습니다. 하지만 vCenter Server를 추가한 후 해당 VM의 성능 및 지연 시간 데이터가 정확하게 반영되려면 최대 1시간이 걸릴 수 있습니다.

- 녹색: "정상"은 vCenter Server가 검색되었고 성능 측정 항목이 성공적으로 수집되었음을 나타냅니다.
- 노란색: "경고"(예: vCenter Server의 통계 수준이 각 개체에 대한 통계를 얻기 위해 3 이상으로 설정되지 않은 경우)
- 주황색: "오류"(예외, 구성 데이터 수집 실패 또는 vCenter Server에 접근할 수 없는 등의 내부 오류를 나타냄) 열 표시 아이콘(표시/숨기기)을 클릭하면 vCenter Server 상태에 대한 상태 메시지를 보고 문제를 해결할 수 있습니다.

3. vCenter Server에 접근할 수 없거나 자격 증명이 변경된 경우 **vCenter** > *편집*을 선택하여 vCenter Server 세부 정보를 편집합니다.
4. **VMware vCenter Server** 편집 페이지에서 필요한 변경 사항을 적용합니다.
5. *저장*을 클릭하세요.

vCenter Server 데이터 수집이 시작됩니다

vCenter Server는 실시간으로 20초 성능 데이터 샘플을 수집하여 5분 샘플로 정리합니다. Unified Manager의 성능 데이터 수집 일정은 vCenter Server의 기본 설정을 기반으로 합니다. Unified Manager는 vCenter Server에서 얻은 5분 샘플을 처리하고 가상 디스크, VM 및 호스트의 IOPS와 대기 시간의 시간당 평균을 계산합니다. 데이터 저장소의 경우 Unified Manager는 ONTAP 에서 얻은 샘플을 통해 IOPS와 대기 시간의 시간당 평균을 계산합니다. 이러한 값은 매시 정각에 제공됩니다. vCenter Server를 추가한 직후에는 성능 측정 항목을 사용할 수 없으며, 다음 시간이 시작되어야만 사용할 수 있습니다. 성능 데이터 폴링은 구성 데이터 수집 주기를 완료하면 시작됩니다.

vCenter Server 구성 데이터를 폴링하기 위해 Unified Manager는 클러스터 구성 데이터를 수집하는 경우와 동일한 일정을 따릅니다. vCenter Server 구성 및 성능 데이터 수집 일정에 대한 자세한 내용은 "클러스터 구성 및 성능 데이터 수집 활동"을 참조하세요.

관련 정보

["클러스터 구성 및 성능 데이터 수집 활동"](#)

vCenter Server 제거

Active IQ Unified Manager 인스턴스에서 vCenter Server를 제거할 수 있습니다. 예를 들어, vCenter Server 검색이 실패하거나 더 이상 필요하지 않은 경우 vCenter Server를 제거할 수 있습니다.

vCenter Server를 제거하면 해당 vCenter에 호스팅된 모든 가상 머신(VM)과 해당 구성 데이터도 삭제됩니다. vCenter Server를 제거하면 연결된 개체와 기록 데이터도 더 이상 모니터링되지 않습니다. 이러한 변경 사항은 vCenter 및 가상 머신 인벤토리 페이지에 반영됩니다.

시작하기 전에

vCenter Server를 제거하기 전에 다음 사항을 확인하세요.

- 애플리케이션 관리자 역할이나 스토리지 관리자 역할이 있습니다.
- vCenter Server 이름과 해당 IP 주소를 알고 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 *VMWARE>vCenter*를 클릭합니다.
2. vCenter 페이지에서 제거하려는 vCenter Server를 선택하고 *제거*를 클릭합니다.
3. **vCenter** 제거 메시지 대화 상자에서 *확인*을 클릭하여 제거 요청을 확인합니다.

가상 머신 모니터링

가상 머신(VM) 애플리케이션에서 지연 문제가 발생하는 경우 원인을 분석하고 문제를 해결하기 위해 VM을 모니터링해야 할 수도 있습니다. VM은 vCenter Server와 VM 스토리지를 호스팅하는 ONTAP 클러스터가 Unified Manager에 추가되면 사용할 수 있습니다.

VM에 대한 자세한 내용은 **VMWARE > > 가상 머신** 페이지에서 확인할 수 있습니다. 가용성, 상태, 사용 및 할당된 용량, 네트워크 지연 시간, VM, 데이터 저장소, 호스트의 IOPS 및 지연 시간과 같은 정보가 표시됩니다. 여러 데이터 저장소를 지원하는 VM의 경우 그리드는 지연 시간이 가장 긴 데이터 저장소의 메트릭을 표시하며, 별표 아이콘(*)은 추가 데이터 저장소를 나타냅니다. 아이콘을 클릭하면 추가 데이터 저장소의 메트릭이 표시됩니다. 일부 열은 정렬 및 필터링이 불가능합니다.



VM과 해당 세부 정보를 보려면 ONTAP 클러스터의 검색(폴링 또는 메트릭 수집)이 완료되어야 합니다. 클러스터가 Unified Manager에서 제거되면 다음 검색 주기 이후에는 해당 VM을 더 이상 사용할 수 없습니다.

이 페이지에서는 VM의 자세한 토폴로지를 볼 수 있으며, VM과 관련된 구성 요소(예: 호스트, 가상 디스크, 연결된 데이터 저장소)를 표시합니다. 토폴로지 보기는 다음 순서로 기본 구성 요소를 해당 계층에 표시합니다. 가상 디스크 > **VM** > 호스트 > 네트워크 > 데이터 저장소 > **VMDK**.

토폴로지 측면에서 I/O 경로와 구성 요소 수준 대기 시간을 확인하고 스토리지가 성능 문제의 원인인지 확인할 수 있습니다. 토폴로지의 요약 보기에는 I/O 경로가 표시되고, IOPS 및 지연 문제가 있는 구성 요소가 강조 표시되어 문제 해결 단계를 결정할 수 있습니다. 각 구성 요소를 별도로 묘사하고 해당 구성 요소의 지연 시간을 함께 보여주는 토폴로지의 확장된 보기를 가질 수도 있습니다. 레이어를 통해 강조 표시된 I/O 경로를 결정하기 위해 구성 요소를 선택할 수 있습니다.

요약 토폴로지 보기

요약 토폴로지에서 VM을 보고 성능 문제를 확인하려면 다음을 수행합니다.

1. **VMWARE** > *가상 머신*으로 이동합니다.
2. 검색창에 VM 이름을 입력하여 검색하세요. 필터 버튼을 클릭하면 특정 기준에 따라 검색 결과를 필터링할 수도 있습니다. 하지만 VM을 찾을 수 없는 경우 해당 vCenter Server가 추가되어 검색되었는지 확인하세요.



vCenter Server에서는 VM, 클러스터, 데이터스토어, 폴더 또는 파일과 같은 vSphere 엔터티의 이름에 특수 문자(예: %, &, *, \$, #, @, !, \, /, :, *, ?, ", <, >, |, ;, ')를 허용합니다. VMware vCenter Server와 ESX/ESXi Server는 표시 이름에 사용된 특수 문자를 이스케이프하지 않습니다. 하지만 Unified Manager에서 이름을 처리하면 다르게 표시됩니다. 예를 들어, 다음과 같은 이름의 VM %\$VC_AIQUM_clone_191124% vCenter Server에서는 다음과 같이 표시됩니다. %25\$VC_AIQUM_clone_191124%25 통합 관리자에서, 특수 문자가 포함된 이름을 가진 VM을 쿼리할 때 이 문제에 대해 기록해 두어야 합니다.

3. VM의 상태를 확인하세요. VM 상태는 vCenter Server에서 검색됩니다. 다음과 같은 상태를 사용할 수 있습니다. 이러한 상태에 대한 자세한 내용은 VMware 설명서를 참조하세요.
 - 정상
 - 경고
 - 알리다
 - 모니터링되지 않음
 - 알려지지 않은
4. 컴퓨팅, 네트워크 및 스토리지 계층 전반의 구성 요소 토폴로지에 대한 요약 보기를 보려면 VM 옆에 있는 아래쪽 화살표를 클릭하세요. 지연 문제가 있는 노드는 강조 표시됩니다. 요약 보기에는 구성 요소의 최악의 지연 시간이 표시됩니다. 예를 들어, VM에 두 개 이상의 가상 디스크가 있는 경우 이 보기에는 모든 가상 디스크 중에서 지연 시간이 가장 긴 가상 디스크가 표시됩니다.
5. 일정 기간 동안 데이터 저장소의 대기 시간과 처리량을 분석하려면 데이터 저장소 개체 아이콘 위에 있는 워크로드 분석기 버튼을 클릭합니다. 워크로드 분석 페이지로 이동하면 시간 범위를 선택하고 데이터 저장소의 성능 차트를 볼 수 있습니다. 워크로드 분석기에 대한 자세한 내용은 _워크로드 분석기를 사용한 워크로드 문제 해결_을 참조하세요.

확장된 토폴로지 보기

VM의 확장된 토폴로지를 보면 각 구성 요소를 개별적으로 자세히 살펴볼 수 있습니다.

단계

1. 요약 토폴로지 보기에서 *토폴로지 확장*을 클릭합니다. 각 객체의 지연 시간과 함께 각 구성 요소의 자세한 토폴로지를 개별적으로 볼 수 있습니다. 예를 들어 데이터 저장소나 VMDK에 여러 노드가 있는 것처럼 한 카테고리에 여러 노드가 있는 경우 지연 시간이 가장 긴 노드는 빨간색으로 강조 표시됩니다.
2. 특정 객체의 IO 경로를 확인하려면 해당 객체를 클릭하여 IO 경로와 해당 매핑을 확인하세요. 예를 들어, 가상 디스크의 매핑을 보려면 가상 디스크를 클릭하여 해당 VMDK에 대한 강조 표시된 매핑을 확인합니다. 이러한 구성 요소의 성능 지연이 발생하는 경우 ONTAP 에서 더 많은 데이터를 수집하여 문제를 해결할 수 있습니다.



VMDK에 대한 메트릭은 보고되지 않습니다. 토폴로지에서는 VMDK 이름만 표시되고 메트릭은 표시되지 않습니다.

["워크로드 분석기를 사용하여 워크로드 문제 해결"](#)

재해 복구 설정에서 가상 인프라 보기

MetroCluster 구성이나 스토리지 가상 머신(스토리지 VM) 재해 복구(SVM DR) 설정에서 호스팅되는 데이터스토어의 구성 및 성능 측정 항목을 볼 수 있습니다.

Unified Manager에서는 vCenter Server에 데이터스토어로 연결된 MetroCluster 구성의 NAS 볼륨이나 LUN을 볼 수 있습니다. MetroCluster 구성에서 호스팅되는 데이터 저장소는 표준 환경의 데이터 저장소와 동일한 토폴로지 뷰로 표현됩니다.

vCenter Server의 데이터스토어에 매핑된 스토리지 VM 재해 복구 구성의 NAS 볼륨이나 LUN도 볼 수 있습니다.

MetroCluster 구성에서 데이터 저장소 보기

MetroCluster 구성에서 데이터 저장소를 보기 전에 다음 필수 조건을 확인하세요.

- 스위치오버 및 스위치백이 발생하는 경우 HA 쌍의 기본 및 보조 클러스터와 vCenter Server를 검색해야 합니다.
- HA 쌍의 기본 및 보조 클러스터와 vCenter Server는 Unified Manager에서 관리해야 합니다.
- 필요한 설정은 ONTAP 및 vCenter Server에서 완료해야 합니다. 자세한 내용은 ONTAP 및 vCenter 설명서를 참조하세요.

["ONTAP 9 문서 센터"](#)

데이터 저장소를 보려면 다음 단계를 따르세요.

1. **VMWARE** > 가상 머신 페이지에서 데이터 저장소를 호스팅하는 VM을 클릭합니다. 워크로드 분석기 또는 데이터 저장소 개체 링크를 클릭합니다. 볼륨이나 LUN을 호스팅하는 기본 사이트가 예상대로 작동하는 표준 시나리오에서는 기본 사이트의 vServer 클러스터 세부 정보를 볼 수 있습니다.
2. 재해 발생 시 보조 사이트로 연속적으로 전환하면 데이터 저장소 링크는 보조 클러스터의 볼륨이나 LUN의 성능 지표를 가리킵니다. 이는 다음 클러스터 주기와 vServer 검색(획득)이 완료된 후에 반영됩니다.
3. 성공적인 스위치백 후, 데이터스토어 링크는 다시 기본 클러스터의 볼륨이나 LUN의 성능 측정 항목을 반영합니다. 이는 다음 클러스터 주기와 vServer 검색이 완료된 후에 반영됩니다.

스토리지 VM 재해 복구 구성의 데이터 저장소 보기

스토리지 VM 재해 복구 구성에서 데이터 저장소를 보기 전에 다음 필수 구성 요소를 확인하세요.

- 스위치오버 및 스위치백이 발생하는 경우 HA 쌍의 기본 및 보조 클러스터와 vCenter Server를 검색해야 합니다.
- 소스 및 대상 클러스터와 스토리지 VM 피어는 모두 Unified Manager에서 관리해야 합니다.
- 필요한 설정은 ONTAP 및 vCenter Server에서 완료해야 합니다.
 - NAS(NFS 및 VMFS) 데이터 저장소의 경우 재해 발생 시 다음 단계로 보조 저장소 VM을 시작하고, 데이터 LIF 및 경로를 확인하고, vCenter Server에서 끊어진 연결을 설정하고, VM을 시작합니다.

기본 사이트로 다시 전환하려면 기본 사이트에서 데이터 제공을 시작하기 전에 볼륨 간 데이터를 동기화해야

합니다.

- SAN(VMFS용 iSCSI 및 FC) 데이터 저장소의 경우 vCenter Server는 마운트된 LUN을 VMFS 형식으로 포맷합니다. 재해 발생 시, 해당 단계에는 보조 저장소 VM을 가동하고, 데이터 LIF와 경로를 검증하는 작업이 포함됩니다. iSCSI 대상 IP가 기본 LIF와 다른 경우 수동으로 추가해야 합니다. 새로운 LUN은 호스트의 스토리지 어댑터의 iSCSI 어댑터에서 장치로 사용할 수 있어야 합니다. 그 후, 새로운 LUN이 포함된 새로운 VMFS 데이터 저장소를 생성하고, 기존 VM을 새 이름으로 등록해야 합니다. VM이 작동 중이어야 합니다.

복구가 발생하는 경우 볼륨 간의 데이터를 동기화해야 합니다. 새로운 VMFS 데이터 저장소는 LUN과 새 이름으로 등록된 이전 VM을 사용하여 다시 생성해야 합니다.

설정에 대한 자세한 내용은 ONTAP 및 vCenter Server 설명서를 참조하세요.

"ONTAP 9 문서 센터"

데이터 저장소를 보려면 다음 단계를 따르세요.

1. **VMWARE** > 가상 머신 페이지에서 데이터 저장소를 호스팅하는 VM 인벤토리를 클릭합니다. 데이터 저장소 개체 링크를 클릭합니다. 표준 시나리오에서는 기본 스토리지 VM의 볼륨과 LUN의 성능 데이터를 볼 수 있습니다.
2. 재해 발생 시 보조 저장소 VM으로 연속적으로 전환하면 데이터 저장소 링크는 보조 저장소 VM의 볼륨이나 LUN의 성능 지표를 가리킵니다. 이는 다음 클러스터 주기와 vServer 검색(획득)이 완료된 후에 반영됩니다.
3. 성공적인 스위치백 후, 데이터 저장소 링크는 다시 기본 스토리지 VM의 볼륨이나 LUN의 성능 측정 항목을 반영합니다. 이는 다음 클러스터 주기와 vServer 검색이 완료된 후에 반영됩니다.

지원되지 않는 시나리오

- MetroCluster 구성의 경우 다음 제한 사항을 참고하세요.
 - 클러스터는 오직 NORMAL 그리고 SWITCHOVER 국가가 채택되었습니다. 다른 주, 예: PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK, 그리고 NOT_REACHABLE 지원되지 않습니다.
 - ASO(자동 전환)가 활성화되어 있지 않으면 기본 클러스터가 다운되면 보조 클러스터를 검색할 수 없으며 토폴로지는 계속해서 기본 클러스터의 볼륨이나 LUN을 가리킵니다.
- 스토리지 VM 재해 복구 구성의 경우 다음 제한 사항에 유의하세요.
 - SAN 스토리지 환경에서 Site Recovery Manager(SRM) 또는 Storage Replication Adapter(SRA)를 활성화한 구성은 지원되지 않습니다.

워크로드 프로비저닝 및 관리

Active IQ Unified Manager의 액티브 관리 기능은 데이터 센터에서 스토리지 워크로드를 프로비저닝, 모니터링 및 관리하기 위한 성능 서비스 수준, 스토리지 효율성 정책 및 스토리지 공급자 API를 제공합니다.



Unified Manager는 기본적으로 이 기능을 제공합니다. 이 기능을 사용하지 않으려면 저장소 관리 > *기능 설정*에서 비활성화할 수 있습니다.

이 기능을 활성화하면 Unified Manager 인스턴스에서 관리하는 ONTAP 클러스터에 워크로드를 프로비저닝할 수 있습니다. 또한, 워크로드에 성능 서비스 수준 및 스토리지 효율성 정책과 같은 정책을 할당하고 해당 정책에 따라 스토리지 환경을 관리할 수 있습니다.

이 기능을 사용하면 다음 기능을 사용할 수 있습니다.

- 추가된 클러스터에서 스토리지 워크로드를 자동으로 검색하여 스토리지 워크로드를 쉽게 평가하고 배포할 수 있습니다.
- NFS 및 CIFS 프로토콜을 지원하는 NAS 워크로드 프로비저닝
- iSCSI 및 FCP 프로토콜을 지원하는 SAN 워크로드 프로비저닝
- 동일한 파일 공유에서 NFS 및 CIFS 프로토콜 모두 지원
- 성능 서비스 수준 및 스토리지 효율성 정책 관리
- 스토리지 워크로드에 성능 서비스 수준 및 스토리지 효율성 정책 할당

UI의 왼쪽 창에 있는 프로비저닝, 스토리지 > 워크로드 및 정책 옵션을 사용하면 다양한 구성을 수정할 수 있습니다.

이러한 옵션을 사용하면 다음 기능을 수행할 수 있습니다.

- 저장소 > 작업 부하 페이지에서 저장소 작업 부하를 확인하세요.
- Provision Workload 페이지에서 스토리지 워크로드를 생성합니다.
- 정책에서 성능 서비스 수준을 생성하고 관리합니다.
- 정책에서 스토리지 효율성 정책을 만들고 관리합니다.
- 워크로드 페이지에서 스토리지 워크로드에 정책 할당

관련 정보

["정책 기반 스토리지 관리"](#)

워크로드 개요

작업 부하란 볼륨이나 LUN과 같은 저장 객체의 입출력(I/O) 작업을 나타냅니다. 저장소가 프로비저닝되는 방식은 예상되는 작업 부하 요구 사항을 기반으로 합니다. Active IQ Unified Manager는 스토리지 개체에 트래픽이 발생한 후에만 워크로드 통계를 추적합니다. 예를 들어, 작업 부하 IOPS와 대기 시간 값은 사용자가 데이터베이스나 이메일 애플리케이션을 사용하기 시작한 후에 사용할 수 있습니다.

워크로드 페이지에는 Unified Manager가 관리하는 ONTAP 클러스터의 스토리지 워크로드 요약이 표시됩니다. 성능 서비스 수준을 준수하는 스토리지 워크로드와 준수하지 않는 스토리지 워크로드에 대한 누적된 한눈에 보는 정보를 제공합니다. 또한 이를 통해 데이터 센터 전반의 클러스터의 총 용량, 사용 가능 용량, 사용된 용량 및 성능(IOPS)을 평가할 수 있습니다.



성능 서비스 수준에 맞지 않거나 사용할 수 없거나 관리되지 않는 스토리지 워크로드의 수를 평가하고, 적합성, 용량 사용량 및 IOPS를 보장하기 위해 필요한 조치를 취하는 것이 좋습니다.

워크로드 페이지에는 다음 두 섹션이 있습니다.

- 워크로드 개요: Unified Manager에서 관리하는 ONTAP 클러스터의 스토리지 워크로드 수에 대한 개요를 제공합니다.
- 데이터 센터 개요: 데이터 센터의 스토리지 워크로드 용량과 IOPS에 대한 개요를 제공합니다. 관련 데이터는 데이터

센터 수준과 개별 .별로 표시됩니다.

워크로드 개요 섹션

워크로드 개요 섹션에서는 스토리지 워크로드에 대한 누적된 정보를 한눈에 볼 수 있습니다. 스토리지 작업 부하의 상태는 할당된 성능 서비스 수준과 할당되지 않은 성능 서비스 수준을 기준으로 표시됩니다.

- 할당됨: 성능 서비스 수준이 할당된 스토리지 워크로드에 대해 다음 상태가 보고됩니다.
 - 적합: 스토리지 워크로드의 성능은 할당된 성능 서비스 수준을 기준으로 합니다. 스토리지 워크로드가 연관된 성능 서비스 수준에서 정의된 임계 대기 시간 내에 있는 경우 "적합"으로 표시됩니다. 적합한 작업 부하는 파란색으로 표시됩니다.
 - 비준수: 성능 모니터링 중에 스토리지 워크로드 지연 시간이 연관된 성능 서비스 수준에서 정의된 임계값 지연 시간을 초과하는 경우 스토리지 워크로드는 "비준수"로 표시됩니다. 규정에 맞지 않는 작업 부하는 주황색으로 표시됩니다.
 - 사용할 수 없음: 스토리지 워크로드가 오프라인이거나 해당 클러스터에 접근할 수 없는 경우 "사용할 수 없음"으로 표시됩니다. 사용할 수 없는 워크로드는 빨간색으로 표시됩니다.
- 할당되지 않음: 성능 서비스 수준이 할당되지 않은 스토리지 워크로드는 "할당되지 않음"으로 보고됩니다. 숫자는 정보 아이콘을 통해 전달됩니다.

총 작업 부하 수는 할당된 작업 부하와 할당되지 않은 작업 부하의 합계입니다.

이 섹션에 표시된 총 워크로드 수를 클릭하면 워크로드 페이지에서 볼 수 있습니다.

성능 서비스 수준별 적합성 하위 섹션에는 사용 가능한 스토리지 작업 부하의 총 수가 표시됩니다.

- 각 유형의 성능 서비스 수준에 맞춰
- 할당된 성과 서비스 수준과 권장되는 성과 서비스 수준 사이에 불일치가 있는 경우

데이터 센터 개요 섹션

데이터 센터 개요 섹션은 데이터 센터의 모든 클러스터에 대한 사용 가능한 용량과 사용된 용량, IOPS를 그래픽으로 나타냅니다. 이 데이터를 사용하여 스토리지 워크로드의 용량과 IOPS를 관리해야 합니다. 이 섹션에는 모든 클러스터의 스토리지 작업 부하에 대한 다음 정보도 표시됩니다.

- 데이터 센터의 모든 클러스터에 대한 총 용량, 사용 가능 용량 및 사용된 용량
- 데이터 센터의 모든 클러스터에 대한 총 IOPS, 사용 가능한 IOPS 및 사용된 IOPS
- 각 성능 서비스 수준에 따른 사용 가능한 용량 및 사용된 용량
- 각 성능 서비스 수준에 따른 사용 가능한 IOPS 및 사용된 IOPS
- 성능 서비스 수준이 할당되지 않은 작업 부하에서 사용되는 총 공간 및 IOPS

성능 서비스 수준을 기준으로 데이터 센터 용량 및 성능을 계산하는 방법

사용된 용량과 IOPS는 클러스터의 모든 스토리지 워크로드의 총 사용된 용량과 성능을 기준으로 검색됩니다.

사용 가능한 IOPS는 노드의 예상 지연 시간과 권장되는 성능 서비스 수준을 기반으로 계산됩니다. 여기에는 예상 지연 시간이 자체 예상 지연 시간보다 작거나 같은 모든 성능 서비스 수준에 대해 사용 가능한 IOPS가 포함됩니다.

사용 가능한 용량은 예상 지연 시간과 집계에 대한 권장 성능 서비스 수준을 기반으로 계산됩니다. 여기에는 예상 지연

시간이 자체 예상 지연 시간보다 작거나 같은 모든 성능 서비스 수준에 사용 가능한 용량이 포함됩니다.

워크로드 보기

Unified Manager에 클러스터를 추가하면 각 클러스터의 스토리지 워크로드가 자동으로 검색되어 워크로드 페이지에 표시됩니다.

Unified Manager는 스토리지 워크로드에서 I/O 작업이 시작된 후에만 권장 사항(권장 PSL)을 위한 워크로드 분석을 시작합니다.

FlexGroup 볼륨과 구성 요소는 제외됩니다.

워크로드 개요

워크로드 개요 페이지에는 데이터 센터의 워크로드 개요와 데이터 센터의 공간 및 성능 개요가 표시됩니다.

- 작업 부하 개요 패널: 총 작업 부하 수와 PSL이 할당된 작업 부하 수, 할당되지 않은 작업 부하 수가 표시됩니다. 각 PSL에 대한 작업 부하 수의 세부 내용도 표시됩니다. 개수를 클릭하면 필터링된 워크로드가 포함된 모든 워크로드 보기로 이동합니다. 시스템 권장 **PSL** 할당 버튼을 클릭하면 시스템 권장 사항을 준수하지 않는 워크로드의 수를 확인하고 해당 워크로드에 시스템 권장 PSL을 할당할 수도 있습니다.
- 데이터 센터 개요 패널: 데이터 센터의 사용 가능한 공간(TiB)과 사용된 공간(TiB) 및 성능(IOPS)을 표시합니다. 각 PSL에 따른 모든 워크로드의 사용 가능한 공간(TiB)과 사용된 공간(TiB) 및 성능(IOPS)도 표시됩니다.

모든 워크로드 보기

저장소 > 워크로드 > 모든 워크로드 페이지에는 Unified Manager에서 관리하는 ONTAP 클러스터와 관련된 스토리지 워크로드가 나열됩니다.

I/O 작업이 발생하지 않은 새로 발견된 스토리지 워크로드의 경우 상태는 "I/O 대기 중"입니다. 스토리지 워크로드에 대한 I/O 작업이 시작된 후 Unified Manager가 분석을 시작하고 워크로드 상태가 "학습 중..."으로 변경됩니다. 분석이 완료되면(I/O 작업 시작 후 24시간 이내) 스토리지 작업 부하에 권장되는 PSL이 표시됩니다.

이 페이지에서는 스토리지 작업 부하에 스토리지 효율성 정책(SEP)과 성능 서비스 수준(PSL)을 할당할 수도 있습니다. 여러 작업을 수행할 수 있습니다.

- 스토리지 워크로드 추가 또는 프로비저닝
- 작업 부하 목록 보기 및 필터링
- 스토리지 워크로드에 PSL 할당
- 시스템에서 권장하는 PSL을 평가하고 워크로드에 할당합니다.
- 스토리지 워크로드에 SEP 할당

스토리지 워크로드 추가 또는 프로비저닝

지원되는 LUN(iSCSI 및 FCP 프로토콜 모두 지원), NFS 파일 공유, SMB 공유에 스토리지 워크로드를 추가하거나 프로비저닝할 수 있습니다.

단계

1. *저장소 > 워크로드 > 모든 워크로드 > 생성*을 클릭합니다.
2. 작업 부하를 생성합니다. 자세한 내용은 다음을 참조하세요. ["워크로드 프로비저닝 및 관리"](#).

워크로드 보기 및 필터링

모든 워크로드 화면에서는 데이터 센터의 모든 워크로드를 볼 수 있고, PSL이나 이름을 기준으로 특정 스토리지 워크로드를 검색할 수 있습니다. 필터 아이콘을 사용하여 검색에 대한 구체적인 조건을 입력할 수 있습니다. 호스트 클러스터나 스토리지 VM 등 다양한 필터 조건으로 검색할 수 있습니다. 용량 총계 옵션을 사용하면 작업 부하의 총 용량(MB)을 기준으로 필터링할 수 있습니다. 하지만 이 경우 총 용량을 바이트 수준에서 비교하기 때문에 반환되는 작업 부하의 수는 달라질 수 있습니다.

각 작업 부하에 대해 호스트 클러스터, 스토리지 VM 등의 정보가 할당된 PSL 및 SEP와 함께 표시됩니다.

이 페이지에서는 작업 부하의 성능 세부 정보를 볼 수도 있습니다. 열 선택/정렬 버튼을 클릭하고 보려는 특정 열을 선택하면 워크로드의 IOPS, 용량 및 지연 시간에 대한 자세한 정보를 볼 수 있습니다. 성능 보기 열에는 작업 부하에 대한 평균 및 최대 IOPS가 표시되며, 작업 부하 분석기 아이콘을 클릭하면 자세한 IOPS 분석을 볼 수 있습니다.

작업 부하에 대한 성능 및 용량 기준 분석

IOPS 분석 팝업의 워크로드 분석 버튼을 클릭하면 워크로드 분석 페이지로 이동합니다. 여기서 시간 범위를 선택하고 선택한 워크로드에 대한 지연 시간, 처리량, 용량 추세를 볼 수 있습니다. 워크로드 분석기에 대한 자세한 내용은 다음을 참조하세요. "[워크로드 분석기를 사용하여 워크로드 문제 해결](#)".

성능 보기 열의 막대형 차트 아이콘을 클릭하면 작업 부하에 대한 성능 정보를 보고 문제 해결에 도움을 받을 수 있습니다. 개체를 분석하기 위해 워크로드 분석 페이지에서 성능 및 용량 차트를 보려면 워크로드 분석 버튼을 클릭하세요.

자세한 내용은 다음을 참조하세요. "[워크로드 분석기는 어떤 데이터를 표시합니까?](#)".

워크로드에 정책 할당

모든 워크로드 페이지에서 다양한 탐색 옵션을 사용하여 스토리지 워크로드에 스토리지 효율성 정책(SEP)과 성능 서비스 수준(PSL)을 할당할 수 있습니다.

단일 작업 부하에 정책 할당

단일 작업 부하에 PSL이나 SEP 또는 둘 다를 할당할 수 있습니다. 다음 단계를 따르세요.

1. 작업량을 선택하세요.
2. 행 옆에 있는 편집 아이콘을 클릭한 다음, *편집*을 클릭합니다.

할당된 성능 서비스 수준 및 스토리지 효율성 정책 필드가 활성화되었습니다.

3. 필요한 PSL이나 SEP, 또는 둘 다를 선택하세요.
4. 변경 사항을 적용하려면 확인 아이콘을 클릭하세요.



작업 부하를 선택하고 *추가 작업*을 클릭하여 정책을 할당할 수도 있습니다.

여러 스토리지 워크로드에 정책 할당

여러 스토리지 워크로드에 PSL이나 SEP를 함께 할당할 수 있습니다. 다음 단계를 따르세요.

1. 정책을 할당할 작업 부하에 대한 확인란을 선택하거나 데이터 센터의 모든 작업 부하를 선택합니다.

2. *추가 작업*을 클릭하세요.
3. PSL을 할당하려면 *성과 서비스 수준 할당*을 선택하세요. SEP를 할당하려면 *스토리지 효율성 정책 할당*을 선택하세요. 정책을 선택할 수 있는 팝업이 표시됩니다.
4. 적절한 정책을 선택하고 *적용*을 클릭하세요. 정책이 할당된 작업 부하의 수가 표시됩니다. 정책이 할당되지 않은 작업 부하도 원인과 함께 나열됩니다.



대량의 워크로드에 정책을 적용하는 경우 선택한 워크로드 수에 따라 시간이 다소 걸릴 수 있습니다. 백그라운드에서 실행 버튼을 클릭하면 작업이 백그라운드에서 실행되는 동안 다른 작업을 계속할 수 있습니다. 대량 할당이 완료되면 완료 상태를 볼 수 있습니다. 여러 작업 부하에 PSL을 적용하는 경우, 이전 대량 할당 작업이 실행 중일 때는 다른 요청을 트리거할 수 없습니다.

워크로드에 시스템 권장 PSL 할당

데이터 센터에서 PSL이 할당되지 않았거나 할당된 PSL이 시스템 권장 사항과 일치하지 않는 스토리지 워크로드에 시스템 권장 PSL을 할당할 수 있습니다. 이 기능을 사용하려면 시스템 권장 **PSL** 할당 버튼을 클릭하세요. 특정한 작업 부하를 선택할 필요는 없습니다.

권장 사항은 시스템 분석을 통해 내부적으로 결정되며, IOPS 및 기타 매개변수가 사용 가능한 PSL의 정의와 일치하지 않는 워크로드의 경우 건너뛰니다. 스토리지 워크로드 Waiting for I/O 학습 상태도 제외됩니다.



Unified Manager는 시스템 분석을 재정의하고 워크로드에 대해 다른 PSL을 권장하기 위해 워크로드 이름에서 특수 키워드를 찾습니다. 워크로드 이름에 "ora"라는 문자가 포함된 경우 **Extreme Performance** PSL이 권장됩니다. 그리고 워크로드 이름에 "vm"이라는 문자가 포함되어 있는 경우 **Performance** PSL이 권장됩니다.

또한 지식 기반(KB) 문서를 참조하세요. "[ActiveIQ Unified Manager '시스템 권장 성능 서비스 수준 할당'](#)은 매우 **가변적인 작업 부하에 적용하지 않습니다.**"

파일 공유 볼륨 제공

기존 클러스터와 스토리지 가상 머신(스토리지 VM)에서 워크로드 프로비저닝 페이지에서 CIFS/SMB 및 NFS 프로토콜을 지원하는 파일 공유 볼륨을 만들 수 있습니다.

시작하기 전에

- 스토리지 VM에는 파일 공유 볼륨을 프로비저닝하기 위한 공간이 있어야 합니다.
- 스토리지 VM에서 SMB 및 NFS 서비스 중 하나 또는 둘 다를 활성화해야 합니다.
- 워크로드에 대한 성능 서비스 수준(PSL)과 스토리지 효율성 정책(SEP)을 선택하고 할당하려면 워크로드를 생성하기 전에 해당 정책이 만들어져 있어야 합니다.

단계

1. 워크로드 프로비저닝 페이지에서 생성하려는 워크로드의 이름을 추가한 다음, 사용 가능한 목록에서 클러스터를 선택합니다.
2. 선택한 클러스터를 기반으로 저장 **VM** 필드는 해당 클러스터에 사용 가능한 저장 VM을 필터링합니다. 목록에서 필요한 스토리지 VM을 선택하세요.

스토리지 VM에서 지원되는 SMB 및 NFS 서비스에 따라 호스트 정보 섹션에서 NAS 옵션이 활성화됩니다.

3. 저장소 및 최적화 섹션에서 워크로드에 대한 저장소 용량과 PSL을 지정하고, 선택적으로 SEP를 지정합니다.

SEP에 대한 사양은 LUN에 할당되고 PSL에 대한 정의는 워크로드가 생성될 때 워크로드에 적용됩니다.

4. 작업 부하에 할당한 PSL을 적용하려면 성능 제한 적용 확인란을 선택합니다.

워크로드에 PSL을 할당하면 워크로드가 생성된 집계가 해당 정책에 정의된 성능 및 용량 목표를 지원할 수 있습니다. 예를 들어, 워크로드에 "극한 성능" PSL이 할당된 경우, 워크로드를 프로비저닝할 집계에는 SSD 스토리지와 같이 "극한 성능" 정책의 성능 및 용량 목표를 지원할 수 있는 기능이 있어야 합니다.



이 확인란을 선택하지 않으면 PSL이 작업 부하에 적용되지 않으며 대시보드에서 작업 부하 상태가 할당되지 않음으로 표시됩니다.

5. **NAS** 옵션을 선택하세요.

NAS 옵션이 활성화되어 있지 않으면 선택한 스토리지 VM이 SMB나 NFS, 또는 둘 다를 지원하는지 확인하세요.



스토리지 VM이 SMB와 NFS 서비스 모두에 대해 활성화된 경우, **NFS**로 공유 및 **SMB**로 공유 확인란을 선택하여 NFS와 SMB 프로토콜을 모두 지원하는 파일 공유를 만들 수 있습니다. SMB 또는 CIFS 공유를 만들려면 해당 확인란만 선택하세요.

6. NFS 파일 공유 볼륨의 경우 파일 공유 볼륨에 액세스할 호스트 또는 네트워크의 IP 주소를 지정합니다. 여러 호스트에 대해 심표로 구분된 값을 입력할 수 있습니다.

호스트 IP 주소를 추가하면 호스트 세부 정보와 스토리지 VM을 일치시키기 위한 내부 검사가 실행되고 해당 호스트에 대한 내보내기 정책이 생성되거나 기존 정책이 있는 경우 재사용됩니다. 동일한 호스트에 대해 여러 개의 NFS 공유가 생성된 경우, 일치하는 규칙이 있는 동일한 호스트에 대한 사용 가능한 내보내기 정책이 모든 파일 공유에 재사용됩니다. API를 사용하여 NFS 공유를 프로비저닝하면 개별 정책의 규칙을 지정하거나 특정 정책 키를 제공하여 정책을 재사용하는 기능을 사용할 수 있습니다.

7. SMB 공유의 경우, SMB 공유에 액세스할 수 있는 사용자 또는 사용자 그룹을 지정하고 필요한 권한을 할당합니다. 각 사용자 그룹에 대해 파일 공유를 생성하는 동안 새로운 액세스 제어 목록(ACL)이 생성됩니다.

8. *저장*을 클릭하세요.

작업 부하가 저장소 작업 부하 목록에 추가됩니다.

LUN 프로비저닝

기존 클러스터와 스토리지 가상 머신(스토리지 VM)에서 워크로드 프로비저닝 페이지에서 CIFS/SMB 및 NFS 프로토콜을 지원하는 LUN을 만들 수 있습니다.

시작하기 전에

- 스토리지 VM에는 LUN을 프로비저닝하기 위한 공간이 있어야 합니다.
- LUN을 생성하는 스토리지 VM에서는 iSCSI와 FCP를 모두 활성화해야 합니다.
- 워크로드에 대한 성능 서비스 수준(PSL)과 스토리지 효율성 정책(SEP)을 선택하고 할당하려면 워크로드를 생성하기 전에 해당 정책이 만들어져 있어야 합니다.

단계

1. 워크로드 프로비저닝 페이지에서 생성하려는 워크로드의 이름을 추가한 다음, 사용 가능한 목록에서 클러스터를 선택합니다.

선택한 클러스터를 기반으로 저장 **VM** 필드는 해당 클러스터에 사용 가능한 저장 VM을 필터링합니다.

2. iSCSI 및 FCP 서비스를 지원하는 스토리지 VM을 목록에서 선택합니다.

선택에 따라 호스트 정보 섹션에서 SAN 옵션이 활성화됩니다.

3. 저장 및 최적화 섹션에서 작업 부하에 대한 저장 용량과 PSL을 지정하고, 선택적으로 SEP를 지정합니다.

SEP에 대한 사양은 LUN에 할당되고 PSL에 대한 정의는 워크로드가 생성될 때 워크로드에 적용됩니다.

4. 작업 부하에 할당된 PSL을 적용하려면 성능 제한 적용 확인란을 선택합니다.

워크로드에 PSL을 할당하면 워크로드가 생성된 집계가 해당 정책에 정의된 성능 및 용량 목표를 지원할 수 있습니다. 예를 들어, 워크로드에 "극한 성능" PSL이 할당된 경우, 워크로드를 프로비저닝할 집계에는 SSD 스토리지와 같이 "극한 성능" 정책의 성능 및 용량 목표를 지원할 수 있는 기능이 있어야 합니다.



이 확인란을 선택하지 않으면 PSL이 작업 부하에 적용되지 않으며 대시보드의 작업 부하 상태가 다음과 같이 표시됩니다. `unassigned`.

5. **SAN** 옵션을 선택하세요. **SAN** 옵션이 활성화되어 있지 않으면 선택한 스토리지 VM이 iSCSI 및 FCP를 지원하는지 확인하세요.
6. 호스트 OS를 선택하세요.
7. LUN에 대한 이니시에이터의 액세스를 제어하기 위해 호스트 매핑을 지정합니다. 기존의 개시자 그룹(igroup)을 할당하거나 새로운 igroup을 정의하고 매핑할 수 있습니다.



LUN을 프로비저닝하는 동안 새로운 igroup을 생성하는 경우, 다음 검색 주기(최대 15분)까지 기다려야 사용할 수 있습니다. 따라서 사용 가능한 igroup 목록에서 기존 igroup을 사용하는 것이 좋습니다.

새로운 igroup을 만들려면 새 이니시에이터 그룹 만들기 버튼을 선택하고 igroup에 대한 정보를 입력하세요.

8. *저장*을 클릭하세요.

LUN이 스토리지 워크로드 목록에 추가됩니다.

성능 서비스 수준

성능 서비스 수준(PSL)을 사용하면 작업 부하에 대한 성능 및 스토리지 목표를 정의할 수 있습니다. 워크로드를 처음 생성할 때 또는 나중에 워크로드를 편집하여 워크로드에 PSL을 할당할 수 있습니다.

스토리지 리소스의 관리 및 모니터링은 서비스 수준 목표(SLO)를 기반으로 합니다. SLO는 필요한 성능과 용량을 기반으로 하는 서비스 수준 계약에 의해 정의됩니다. Unified Manager에서 SLO는 NetApp 스토리지에서 실행되는 애플리케이션의 PSL 정의를 나타냅니다. 저장 서비스는 기반 리소스의 성능과 활용도를 기준으로 차별화됩니다. PSL은 스토리지 서비스 목표에 대한 설명입니다. PSL을 사용하면 스토리지 공급자가 작업 부하에 대한 성능 및 용량 목표를 지정할 수 있습니다. 워크로드에 PSL을 할당하면 ONTAP의 해당 워크로드는 성능 및 용량 목표에 따라 관리됩니다. 각

PSL은 최대 IOP, 예상 IOP, 절대 최소 IOP, 예상 지연 시간에 따라 결정됩니다.

Unified Manager에는 다음과 같은 유형의 PSL이 있습니다.

- 시스템 정의: Unified Manager는 변경할 수 없는 몇 가지 고정 정책을 제공합니다. 미리 정의된 PSL은 다음과 같습니다.

- 극한의 성능
- 성능
- 가치

Extreme Performance, Performance, Value PSL은 데이터 센터의 대부분 일반적인 스토리지 워크로드에 적용할 수 있습니다.

Unified Manager는 데이터베이스 애플리케이션에 대해 세 가지 성능 서비스 수준도 제공합니다. 이러한 PSL은 버스티 IOPS를 지원하고 가장 높은 처리량 요구가 있는 데이터베이스 애플리케이션에 적합한 매우 고성능 PSL입니다.

- 데이터베이스 로그를 위한 Extreme
- 데이터베이스 공유 데이터에 대한 Extreme
- 데이터베이스 데이터를 위한 Extreme

- 사용자 정의: 미리 정의된 성과 서비스 수준이 요구 사항을 충족하지 못하는 경우, 요구 사항을 충족하는 새로운 PSL을 만들 수 있습니다. 자세한 내용은 다음을 참조하세요. "[성능 서비스 수준 생성 및 편집](#)".

- **Beyond Extreme:** Beyond Extreme PSL은 Extreme보다 높은 IOPS를 요구하는 워크로드에 권장되는 시스템 PSL입니다. 워크로드는 IOPS, 용량, 지연 시간을 기준으로 내부적으로 분석되며, 저장소 > 워크로드 > 모든 워크로드 화면에서 각 워크로드에 대해 Beyond Extreme PSL이 권장됩니다. 최적의 성능을 보장하기 위해 PSL을 워크로드에 적용할 수 있습니다.

워크로드에 대한 IOP 매개변수는 워크로드 동작에 따라 동적으로 생성되며 Beyond Extreme PSL의 이름에 다음 형식으로 추가됩니다. Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>. 예를 들어, 시스템이 작업 부하에 최대 및 예상 IOP가 있다고 판단하는 경우 106345 그리고 37929 각각 작업 부하에 대해 생성된 Beyond Extreme PSL은 다음과 같이 명명됩니다. Beyond Extreme 106345 37929. 이러한 PSL은 시스템에서 권장되지만 작업 부하에 할당하면 이러한 PSL은 다음과 같이 표시됩니다. User-defined 유형으로.

PSL을 할당하여 작업 부하를 관리합니다.

정책 > 성능 서비스 수준 페이지와 스토리지 공급자 API를 사용하여 PSL에 액세스할 수 있습니다. PSL을 할당하여 스토리지 작업 부하를 관리하면 개별적으로 스토리지 작업 부하를 관리할 필요가 없으므로 편리합니다. 모든 수정 사항은 개별적으로 관리하는 대신 다른 PSL을 재할당하여 관리할 수도 있습니다. Unified Manager를 사용하면 내부 평가 및 권장 사항을 기반으로 워크로드에 PSL을 할당할 수 있습니다.

작업 부하에 시스템 권장 PSL을 할당하는 방법에 대한 자세한 내용은 다음을 참조하세요. "[워크로드에 시스템 권장 PSL 할당](#)".

성과 서비스 수준 페이지에는 사용 가능한 PSL 정책이 나열되어 있으며, 이를 추가, 편집, 삭제할 수 있습니다.



시스템에서 정의되었거나 현재 작업 부하에 할당된 PSL은 수정할 수 없습니다. 작업 부하에 할당된 PSL을 삭제할 수 없으며, 해당 PSL이 유일하게 사용 가능한 PSL인 경우에도 삭제할 수 없습니다.

이 페이지에는 다음 정보가 표시됩니다.

필드	설명
이름	PSL의 이름.
유형	정책이 시스템 정의인지 사용자 정의인지 여부.
예상 IOPS/TB	LUN이나 파일 공유에서 애플리케이션이 수행할 것으로 예상되는 최소 IOPS 수입니다. 예상 IOPS는 할당된 스토리지 개체 크기를 기반으로 할당된 최소 예상 IOPS를 지정합니다.
최대 IOPS/TB	애플리케이션이 LUN 또는 파일 공유에서 수행할 수 있는 최대 IOPS 수입니다. 최대 IOPS는 할당된 스토리지 객체 크기 또는 사용된 스토리지 객체 크기를 기반으로 할당 가능한 최대 IOPS를 지정합니다. 최대 IOPS는 할당 정책에 따라 결정됩니다. 할당 정책은 할당된 공간 또는 사용된 공간입니다. 할당 정책이 할당된 공간으로 설정된 경우 최대 IOPS는 스토리지 개체의 크기를 기준으로 계산됩니다. 할당 정책이 사용 공간으로 설정된 경우 최대 IOPS는 스토리지 효율성을 고려하여 스토리지 개체에 저장된 데이터 양을 기준으로 계산됩니다. 기본적으로 할당 정책은 사용 공간으로 설정됩니다.

필드	설명
절대 최소 IOPS	예상 IOPS가 이 값보다 낮을 경우, 절대 최소 IOPS가 재정의로 사용됩니다. 시스템 정의 PSL의 기본값은 다음과 같습니다. - 극한 성능: 예상 IOPS ≥ 6144/TB인 경우 절대 최소 IOPS = 1000 - 성능: 예상 IOPS가 2048/TB 이상, 6144/TB 미만인 경우 절대 최소 IOPS = 500 - 값: 예상 IOPS가 128/TB 이상, 2048/TB 미만인 경우 절대 최소 IOPS = 75 시스템 정의 데이터베이스 PSL의 기본값은 다음과 같습니다. - 데이터베이스 로그의 경우 극단적: 예상 IOPS ≥ 22528인 경우 절대 최소 IOPS = 4000 - 데이터베이스 공유 데이터의 경우 극단적인 경우: 예상 IOPS가 16384 이상인 경우 절대 최소 IOPS는 2000입니다. - 데이터베이스 데이터의 경우 극단적인 경우: 예상 IOPS ≥ 12288인 경우 절대 최소 IOPS = 2000 사용자 정의 PSL의 절대 최소 IOPS의 상위 값은 최대 75000이 될 수 있습니다. 낮은 값은 다음과 같이 계산됩니다. 1000/예상 지연 시간
예상 지연 시간	작업당 밀리초 단위의 스토리지 IOPS에 대한 예상 지연 시간(ms/op).
용량	클러스터에서 사용 가능한 총 용량과 사용된 용량입니다.
작업 부하	PSL에 할당된 스토리지 워크로드의 수입니다.

최대 IOPS와 예상 IOPS가 ONTAP 클러스터에서 일관되고 차별화된 성능을 달성하는 데 어떻게 도움이 되는지에 대한 자세한 내용은 다음 KB 문서를

참조하세요. https://kb.netapp.com/Advice_and_Troubleshooting/Data_Infrastructure_Management/Active_IQ_Unified_Manager/What_is_Performance_Budgeting%3F["성과 예산이란 무엇인가요?"]

PSL에서 정의한 임계값을 위반하는 작업 부하에 대해 생성된 이벤트

이전 시간 동안 작업 부하가 예상 대기 시간 값을 30% 초과하는 경우 Unified Manager는 다음 이벤트 중 하나를 생성하여 잠재적인 성능 문제를 알려줍니다.

- 성능 서비스 수준 정책에 정의된 대로 작업 부하 볼륨 대기 시간 임계값이 위반되었습니다.

- 성능 서비스 수준 정책에 정의된 대로 워크로드 LUN 지연 임계값이 위반되었습니다.

대기 시간 값이 높아지는 원인을 파악하기 위해 작업 부하를 분석하는 것이 좋습니다.

자세한 내용은 다음 링크를 참조하세요.

- ["볼륨 이벤트"](#)
- ["성능 임계값 정책이 위반되면 어떻게 되나요?"](#)
- ["Unified Manager가 워크로드 대기 시간을 사용하여 성능 문제를 식별하는 방법"](#)
- ["어떤 성과 이벤트가 있나요?"](#)

시스템 정의 **PSL**

다음 표는 시스템 정의 PSL에 대한 정보를 제공합니다.

성능 서비스 수준	설명 및 사용 사례	예상 지연 시간(ms/op)	최대 IOPS	예상 IOPS	절대 최소 IOPS
극한의 성능	매우 낮은 대기 시간으로 매우 높은 처리량을 제공합니다. 지연 시간에 민감한 애플리케이션에 이상적입니다.	1	12288	6144	1000
성능	낮은 지연 시간으로 높은 처리량 제공 데이터베이스 및 가상화된 애플리케이션에 이상적입니다.	2	4096	2048	500
가치	높은 저장 용량과 적당한 지연 시간을 제공합니다. 이메일, 웹 콘텐츠, 파일 공유, 백업 대상 등 대용량 애플리케이션에 이상적입니다.	17	512	128	75

성능 서비스 수준	설명 및 사용 사례	예상 지연 시간(ms/op)	최대 IOPS	예상 IOPS	절대 최소 IOPS
데이터베이스 로그를 위한 Extreme	가장 낮은 지연 시간으로 최대 처리량을 제공합니다. 데이터베이스 로그를 지원하는 데이터베이스 애플리케이션에 이상적입니다. 이 PSL은 데이터베이스 로그가 매우 폭주하고 로깅에 대한 수요가 끊임없이 있기 때문에 가장 높은 처리량을 제공합니다.	1	45056	22528	4000
데이터베이스 공유 데이터에 대한 Extreme	가장 낮은 지연 시간으로 매우 높은 처리량을 제공합니다. 공통 데이터 저장소에 저장되어 있지만 여러 데이터베이스에서 공유되는 데이터베이스 애플리케이션 데이터에 이상적입니다.	1	32768	16384	2000
데이터베이스 데이터를 위한 Extreme	가장 낮은 지연 시간으로 높은 처리량을 제공합니다. 데이터베이스 테이블 정보 및 메타데이터와 같은 데이터베이스 애플리케이션 데이터에 이상적입니다.	1	24576	12288	2000

시스템에서 정의한 성능 서비스 수준이 워크로드 요구 사항과 일치하지 않는 경우 워크로드에 최적화된 자체 성능 서비스 수준을 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 역할이 있어야 합니다.
- 성능 서비스 수준 이름은 고유해야 하며 다음과 같은 예약 키워드를 사용할 수 없습니다.

Prime, Extreme, Performance, Value, Unassigned, Learning, Idle, Default, 그리고 None.

스토리지에 액세스하는 애플리케이션에 필요한 서비스 수준 목표를 정의하여 성능 서비스 수준 페이지에서 사용자 정의 성능 서비스 수준을 만들고 편집할 수 있습니다.



현재 작업 부하에 할당된 경우 성능 서비스 수준을 수정할 수 없습니다.

단계

1. 왼쪽 탐색 창의 설정*에서 *정책 > *성능 서비스 수준*을 선택합니다.
2. 성과 서비스 수준 페이지에서 새로운 성과 서비스 수준을 생성할지, 아니면 기존 성과 서비스 수준을 편집할지에 따라 적절한 버튼을 클릭합니다.

에게...	다음 단계를 따르세요...
새로운 성능 서비스 수준 생성	*추가*를 클릭하세요.
기존 성능 서비스 수준 편집	기존 성과 서비스 수준을 선택한 다음 *편집*을 클릭합니다.

성과 서비스 수준을 추가하거나 편집하는 페이지가 표시됩니다.

3. 성과 목표를 지정하여 성과 서비스 수준을 사용자 정의한 다음, *제출*을 클릭하여 성과 서비스 수준을 저장합니다.

워크로드 페이지나 새 워크로드를 프로비저닝할 때 새 성능 서비스 수준이나 변경된 성능 서비스 수준을 워크로드(LUN, NFS 파일 공유, CIFS 공유)에 적용할 수 있습니다.

스토리지 효율성 정책 관리

SEP(스토리지 효율성 정책)를 사용하면 작업 부하의 스토리지 효율성 특성을 정의할 수 있습니다. 워크로드를 처음 생성할 때 또는 나중에 워크로드를 편집하여 워크로드에 SEP를 할당할 수 있습니다.

스토리지 효율성에는 씬 프로비저닝, 중복 제거, 데이터 압축과 같은 기술을 사용하여 스토리지 활용도를 높이고 스토리지 비용을 낮추는 것이 포함됩니다. SEP를 만들 때 이러한 공간 절약 기술을 개별적으로 또는 함께 사용하여 최대의 보관 효율성을 달성할 수 있습니다. 정책을 스토리지 작업 부하와 연결하면 지정된 정책 설정이 해당 정책에 할당됩니다. Unified Manager를 사용하면 시스템 정의 및 사용자 정의 SEP를 할당하여 데이터 센터의 스토리지 리소스를 최적화할 수 있습니다.

Unified Manager는 높음과 낮음의 두 가지 시스템 정의 SEP를 제공합니다. 이러한 SEP는 데이터 센터의 대부분 스토리지 워크로드에 적용할 수 있지만, 시스템에서 정의한 SEP가 요구 사항을 충족하지 못하는 경우 사용자 고유의 정책을 만들 수 있습니다.

시스템에서 정의되었거나 현재 작업 부하에 할당된 SEP는 수정할 수 없습니다. 워크로드에 할당된 SEP를 삭제할 수 없으며, 해당 SEP가 유일하게 사용 가능한 SEP인 경우에도 삭제할 수 없습니다.

스토리지 효율성 정책 페이지에는 사용 가능한 SEP가 나열되어 있으며, 이를 통해 사용자 정의 SEP를 추가, 편집, 삭제할 수 있습니다. 이 페이지에는 다음 정보가 표시됩니다.

필드	설명
이름	SEP의 이름.
유형	정책이 시스템 정의인지 사용자 정의인지 여부.
우주 보호 구역	볼륨이 썸 프로비저닝되었는지 아니면 씹 프로비저닝되었는지 여부.
중복제거	워크로드에서 중복 제거가 활성화되어 있는지 여부: - 인라인: 작업 부하에 기록되는 동안 중복 제거가 발생합니다. - 배경: 중복 제거는 작업 부하에서 발생합니다. - 비활성화: 작업 부하에서 중복 제거가 비활성화됩니다.
압축	작업 부하에서 데이터 압축이 활성화되어 있는지 여부: - 인라인: 작업 부하에 기록되는 동안 데이터 압축이 발생합니다. - 배경: 데이터 압축은 작업 부하에서 발생합니다. - 비활성화: 작업 부하에서 데이터 압축이 비활성화됩니다.
작업 부하	SEP에 할당된 스토리지 워크로드 수

사용자 정의 스토리지 효율성 정책 생성을 위한 지침

기존 SEP가 스토리지 워크로드에 대한 정책 요구 사항을 충족하지 못하는 경우 사용자 지정 SEP를 만들 수 있습니다. 그러나 스토리지 작업 부하에는 시스템에서 정의한 SEP를 사용하고, 필요한 경우에만 사용자 정의 SEP를 만드는 것이 좋습니다.

모든 워크로드 페이지와 볼륨/상태 세부 정보 페이지에서 워크로드에 할당된 SEP를 볼 수 있습니다. 대시보드의 용량 패널과 용량: 모든 클러스터 보기에서 이러한 스토리지 효율성을 기반으로 한 클러스터 수준 데이터 감소 비율(스냅샷 복사본 없음)을 볼 수 있습니다.

시스템에서 정의한 스토리지 효율성 정책이 워크로드 요구 사항과 일치하지 않는 경우 워크로드에 최적화된 자체 스토리지 효율성 정책을 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 역할이 있어야 합니다.
- 스토리지 효율성 정책 이름은 고유해야 하며 다음과 같은 예약 키워드를 사용할 수 없습니다.

High, Low, Unassigned, Learning, Idle, Default, 그리고 None.

스토리지 효율성 정책 페이지에서 스토리지에 액세스하는 애플리케이션에 필요한 스토리지 효율성 특성을 정의하여 사용자 정의 스토리지 효율성 정책을 만들고 편집할 수 있습니다.



현재 작업 부하에 할당된 경우 스토리지 효율성 정책을 수정할 수 없습니다.

단계

1. 왼쪽 탐색 창의 설정*에서 *정책 > *저장소 효율성*을 선택합니다.
2. 저장소 효율성 정책 페이지에서 새 저장소 효율성 정책을 만들지, 아니면 기존 저장소 효율성 정책을 편집할지에 따라 적절한 버튼을 클릭합니다.

에게...	다음 단계를 따르세요...
새로운 스토리지 효율성 정책 만들기	*추가*를 클릭하세요
기존 스토리지 효율성 정책 편집	기존 스토리지 효율성 정책을 선택하고 *편집*을 클릭하세요.

저장소 효율성 정책을 추가하거나 편집하는 페이지가 표시됩니다.

3. 저장소 효율성 특성을 지정하여 저장소 효율성 정책을 사용자 정의한 다음, *제출*을 클릭하여 저장소 효율성 정책을 저장합니다.

워크로드 페이지나 새 워크로드를 프로비저닝할 때 새 스토리지 효율성 정책이나 변경된 스토리지 효율성 정책을 워크로드(LUN, NFS 파일 공유, CIFS 공유)에 적용할 수 있습니다.

MetroCluster 구성 관리 및 모니터링

Unified Manager 웹 UI에서 MetroCluster 구성에 대한 모니터링 지원을 통해 FC 및 IP 구성을 통한 MetroCluster 에서 연결 문제를 확인할 수 있습니다. 연결 문제를 일찍 발견하면 MetroCluster 구성을 효과적으로 관리할 수 있습니다.

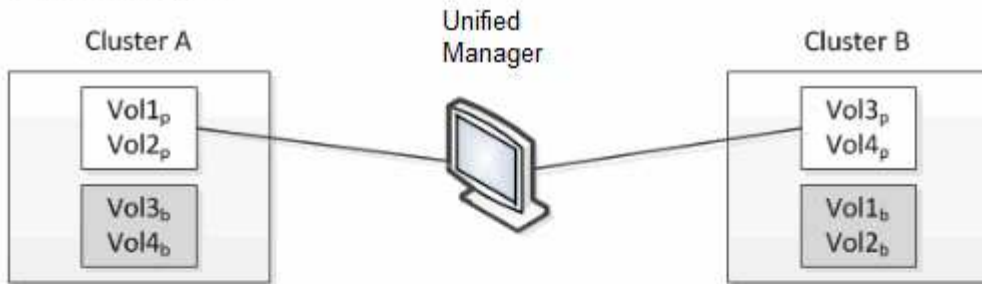
스위치오버 및 스위치백 중 볼륨 동작

스위치오버 또는 스위치백을 트리거하는 이벤트로 인해 재해 복구 그룹 내에서 활성 볼륨이 한 클러스터에서 다른 클러스터로 이동됩니다. 클러스터에서 활성화되어 클라이언트에 데이터를

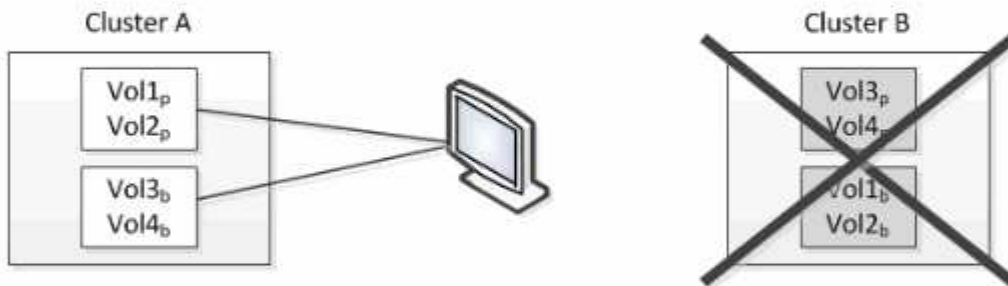
제공하던 볼륨이 중지되고, 다른 클러스터의 볼륨이 활성화되어 데이터 제공을 시작합니다. Unified Manager는 활성화되어 실행 중인 볼륨만 모니터링합니다.

볼륨이 한 클러스터에서 다른 클러스터로 이동하므로 두 클러스터를 모두 모니터링하는 것이 좋습니다. Unified Manager의 단일 인스턴스는 MetroCluster 구성에서 두 클러스터를 모두 모니터링할 수 있지만, 두 위치 사이의 거리로 인해 두 클러스터를 모두 모니터링하기 위해 두 개의 Unified Manager 인스턴스가 필요한 경우가 있습니다. 다음 그림은 Unified Manager의 단일 인스턴스를 보여줍니다.

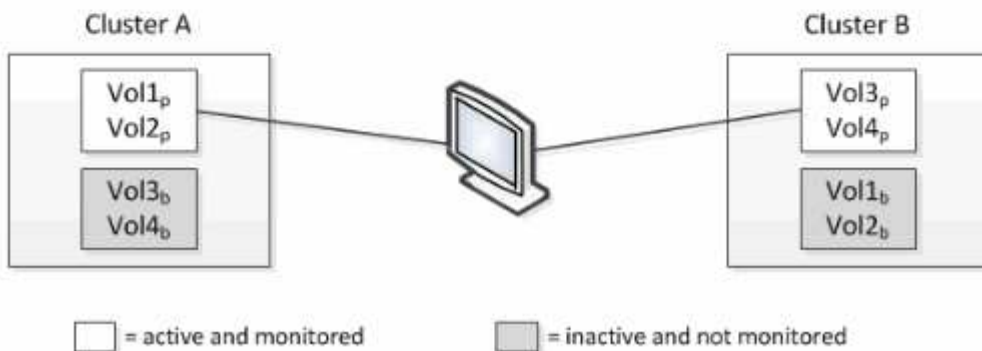
Normal operation



Cluster B fails --- switchover to Cluster A



Cluster B is repaired --- switchback to Cluster B



이름에 p가 포함된 볼륨은 기본 볼륨을 나타내고, 이름에 b가 포함된 볼륨은 SnapMirror에서 생성된 미러링된 백업 볼륨을 나타냅니다.

정상 작동 중:

- 클러스터 A에는 Vol1p와 Vol2p라는 두 개의 활성 볼륨이 있습니다.
- 클러스터 B에는 Vol3p와 Vol4p라는 두 개의 활성 볼륨이 있습니다.
- 클러스터 A에는 두 개의 비활성 볼륨인 Vol3b와 Vol4b가 있습니다.
- 클러스터 B에는 Vol1b와 Vol2b라는 두 개의 비활성 볼륨이 있습니다.

각 활성 볼륨에 대한 정보(통계, 이벤트 등)는 Unified Manager에 의해 수집됩니다. Vol1p 및 Vol2p 통계는 클러스터 A에서 수집되고, Vol3p 및 Vol4p 통계는 클러스터 B에서 수집됩니다.

치명적인 오류로 인해 활성 볼륨이 클러스터 B에서 클러스터 A로 전환된 경우:

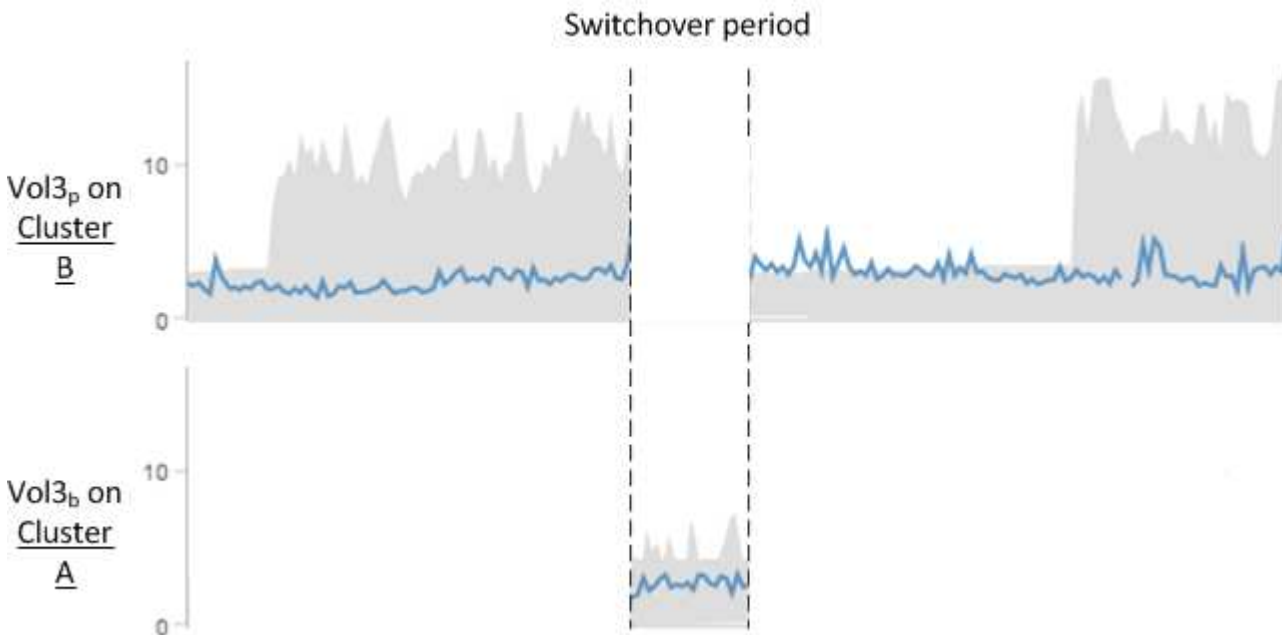
- 클러스터 A에는 Vol1p, Vol2p, Vol3b, Vol4b라는 4개의 활성 볼륨이 있습니다.
- 클러스터 B에는 Vol3p, Vol4p, Vol1b, Vol2b라는 4개의 비활성 볼륨이 있습니다.

일반 작업 중과 마찬가지로 각 활성 볼륨에 대한 정보는 Unified Manager에 의해 수집됩니다. 하지만 이 경우 Vol1p와 Vol2p 통계는 클러스터 A에서 수집되고, Vol3b와 Vol4b 통계도 클러스터 A에서 수집됩니다.

Vol3p와 Vol3b는 서로 다른 클러스터에 있으므로 동일한 볼륨이 아닙니다. Vol3p용 Unified Manager의 정보는 Vol3b와 다릅니다.

- 클러스터 A로 전환하는 동안 Vol3p 통계와 이벤트는 표시되지 않습니다.
- 첫 번째 전환에서 Vol3b는 이전 정보가 없는 새로운 볼륨처럼 보입니다.

클러스터 B가 수리되고 스위치백이 수행되면 Vol3p가 클러스터 B에서 다시 활성화되고, 스위치오버 동안의 기간 동안의 과거 통계와 통계 격차가 발생합니다. Vol3b는 다른 전환이 발생할 때까지 클러스터 A에서 볼 수 없습니다.



- 예를 들어 스위치백 후 클러스터 A의 Vol3b와 같이 비활성화된 MetroCluster 볼륨은 "이 볼륨은 삭제되었습니다"라는 메시지로 식별됩니다. 볼륨은 실제로 삭제되지는 않지만 활성 볼륨이 아니기 때문에 Unified Manager에서 현재 모니터링되고 있지 않습니다.
- 단일 Unified Manager가 MetroCluster 구성에서 두 클러스터를 모두 모니터링하는 경우 볼륨 검색은 해당 시점에 활성화된 볼륨에 대한 정보를 반환합니다. 예를 들어, "Vol3"을 검색하면 전환이 발생하고 Vol3이 클러스터 A에서 활성화된 경우 클러스터 A의 Vol3b에 대한 통계와 이벤트가 반환됩니다.

FC 구성을 통한 MetroCluster 에 대한 클러스터 연결 상태 정의

FC 구성을 통한 MetroCluster 의 클러스터 간 연결은 최적, 영향 받음 또는 중단 중 하나의 상태가 될 수 있습니다. 연결 상태를 이해하면 MetroCluster 구성을 효과적으로 관리할 수 있습니다.

연결 상태	설명	아이콘이 표시됨
최적	MetroCluster 구성에서 클러스터 간 연결은 정상입니다.	
영향을 받음	하나 이상의 오류로 인해 장애 조치 가용성 상태가 손상되었습니다. 그러나 MetroCluster 구성의 두 클러스터는 모두 계속 작동 중입니다. 예를 들어, ISL 링크가 다운된 경우, 클러스터 간 IP 링크가 다운된 경우 또는 파트너 클러스터에 접근할 수 없는 경우입니다.	
아래에	MetroCluster 구성에서 클러스터 간 연결이 끊어진 이유는 클러스터 중 하나 또는 둘 다 다운되었거나 클러스터가 장애 조치 모드에 있기 때문입니다. 예를 들어, 재해로 인해 파트너 클러스터가 중단되거나 테스트 목적으로 계획된 전환이 있는 경우입니다.	오류가 있는 전환:  전환 성공: 

FC를 통한 MetroCluster 에 대한 데이터 미러링 상태 정의

FC 구성을 통한 MetroCluster 데이터 미러링을 제공하고 전체 사이트를 사용할 수 없게 되면 장애 조치를 시작하는 추가 기능을 제공합니다. FC 구성을 통한 MetroCluster 의 클러스터 간 데이터 미러링 상태는 정상 또는 미러링 불가일 수 있습니다. 상태를 이해하면 MetroCluster 구성을 효과적으로 관리할 수 있습니다.

데이터 미러링 상태	설명	아이콘이 표시됨
정상	MetroCluster 구성에서 클러스터 간 데이터 미러링은 정상입니다.	

데이터 미러링 상태	설명	아이콘이 표시됨
미러링을 사용할 수 없습니다	전환으로 인해 MetroCluster 구성의 클러스터 간 데이터 미러링을 사용할 수 없습니다. 예를 들어, 재해로 인해 파트너 클러스터가 중단되거나 테스트 목적으로 계획된 전환이 있는 경우입니다.	오류가 있는 전환:  전환 성공: 

MetroCluster 구성 모니터링

MetroCluster 구성에서 연결 문제를 모니터링할 수 있습니다. 세부 정보에는 클러스터 내의 구성 요소 및 연결 상태와 MetroCluster 구성의 클러스터 간 연결 상태가 포함됩니다. 여기에서는 FC 및 IP 구성 MetroCluster 통한 MetroCluster 로 보호되는 클러스터에서 연결 문제를 모니터링하는 방법을 알아보겠습니다.

Active IQ Unified Manager 왼쪽 탐색 창에서 다음 보기를 통해 MetroCluster 구성을 모니터링할 수 있습니다.

- 저장소 > 클러스터 > 보호: **MetroCluster** 보기
- 보호 > 관계 > 관계: **MetroCluster** 보기

Unified Manager는 시스템 상태 알림을 사용하여 MetroCluster 구성의 구성 요소 및 연결 상태를 나타냅니다.

시작하기 전에

- MetroCluster 구성의 로컬 클러스터와 원격 클러스터는 모두 Active IQ Unified Manager 에 추가되어야 합니다.
- IP 구성을 통한 MetroCluster 에서 Mediator를 지원하려면 Mediator를 구성하고 해당 API를 통해 클러스터에 추가해야 합니다.
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

FC 구성을 통한 **MetroCluster** 의 연결 문제 모니터링

FC 구성을 통한 MetroCluster 의 클러스터의 경우 연결 차트는 클러스터/상태 세부 정보 페이지에 표시됩니다. 다음 단계를 따르세요.

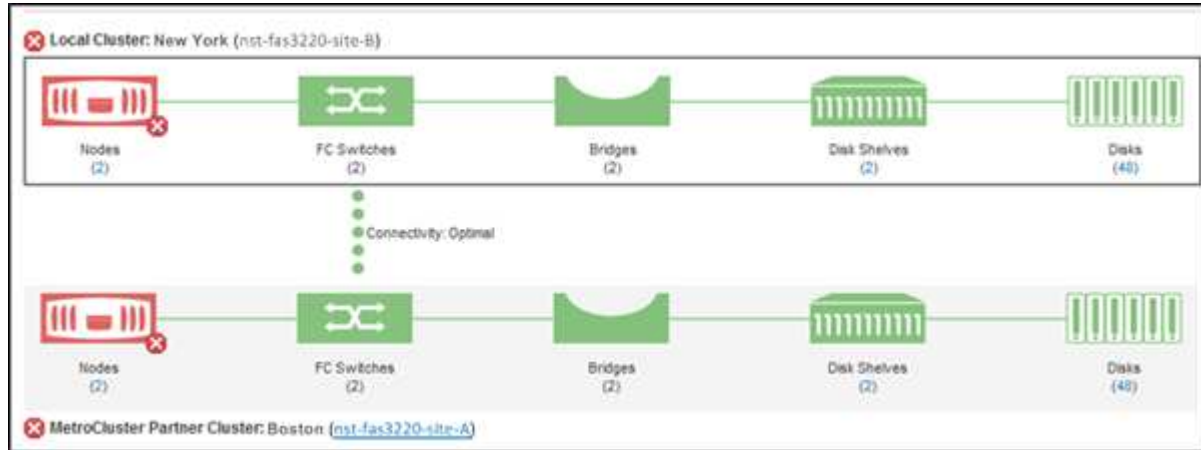
단계

1. 왼쪽 탐색 창에서 저장소 > *클러스터*를 클릭합니다.

모니터링된 모든 클러스터의 목록이 표시됩니다.

2. 보호: **MetroCluster** 보기에서 FC를 통한 MetroCluster 구성 세부 정보를 보려는 클러스터의 이름을 클릭합니다. 또는 MetroCluster 구성에서 클러스터별로 필터링할 수 있습니다.

- 클러스터/상태 세부 정보 페이지에서 * MetroCluster 연결* 탭을 클릭합니다. * MetroCluster 연결* 탭은 FC 구성을 통한 MetroCluster 에만 사용할 수 있습니다.



MetroCluster 구성의 토폴로지는 해당 클러스터 개체 영역에 표시됩니다. 클러스터/상태 세부 정보 페이지에 표시된 정보를 사용하여 연결 문제를 해결할 수 있습니다. 예를 들어, 클러스터의 노드와 스위치 간 연결이 끊어지면 다음 아이콘이 표시됩니다.



아이콘 위에 포인터를 올리면 생성된 이벤트에 대한 자세한 정보를 볼 수 있습니다.

MetroCluster 구성에서 연결 문제가 발견되면 System Manager에 로그인하거나 ONTAP CLI에 액세스하여 문제를 해결해야 합니다.

클러스터 상태를 확인하는 방법에 대한 자세한 내용은 다음을 참조하세요. "[FC 구성을 통해 MetroCluster 에서 클러스터 상태 확인](#)".

IP 구성을 통한 MetroCluster 의 연결 문제 모니터링

IP 구성을 통한 MetroCluster 의 클러스터에 대한 연결 차트는 클러스터 페이지에 표시됩니다. 다음 단계를 따르세요.

단계

- 왼쪽 탐색 창에서 저장소 > *클러스터*를 클릭합니다.

모니터링된 모든 클러스터의 목록이 표시됩니다.

- 보호: **MetroClusters** 보기에서 IP를 통한 MetroCluster 구성 세부 정보를 보려는 클러스터의 이름을 클릭합니다. 또는 MetroCluster 구성에서 클러스터별로 필터링할 수 있습니다.
- 캐럿을 클릭하여 행을 확장합니다. ∨ 상. 캐럿 아이콘은 IP 구성을 통해 MetroCluster 로 보호되는 클러스터에만 나타납니다.

연결에 사용된 중재자가 있는 경우 소스 및 미러 사이트의 토폴로지와 중재자도 볼 수 있습니다. 다음 정보를 볼 수 있습니다.

- 사이트 간 연결성
- 두 사이트 모두에 건강 및 가용성 문제가 있는 경우

- 중재자 관련 문제
- 복제 관련 문제.



다음 상태가 보고됩니다: 중요(❌), 오류(⚠️), 또는 일반(✅). 동일한 토폴로지에서 기본 데이터와 미러 데이터의 집계 데이터 복제 상태도 볼 수 있습니다.

다음 다이어그램에서는 소스 클러스터와 대상 클러스터 간의 사이트 간 연결을 사용할 수 없고, 두 클러스터 간의 중재자가 구성되지 않은 것을 확인할 수 있습니다.



- 상태 아이콘을 클릭하세요. 오류 정의가 포함된 메시지가 표시됩니다. IP 구성을 통한 MetroCluster 에서 문제에 대한 이벤트가 발생한 경우 메시지에서 이벤트 보기 버튼을 클릭하여 이벤트 세부 정보를 볼 수 있습니다. 문제와 이벤트를 해결하면 이 토폴로지의 상태 아이콘이 정상으로 바뀝니다(✅).
- 클러스터/상태 세부 정보 페이지의 구성 탭에 있는 * MetroCluster 개요* 및 보호 섹션에서 추가 구성 세부 정보를 볼 수 있습니다.



IP 구성을 통한 MetroCluster 의 경우에만 클러스터 페이지에서 클러스터 토폴로지를 볼 수 있습니다. FC 구성을 통한 MetroCluster 의 클러스터의 경우 토폴로지는 클러스터/상태 세부 정보 페이지의 * MetroCluster 연결* 탭에 표시됩니다.

관련 정보

- ["클러스터/상태 세부 정보 페이지"](#)
- 관계: **MetroCluster** 보기에 대한 정보는 다음을 참조하세요. ["MetroCluster 구성 모니터링"](#).
- 관계: 지난 1개월 전송 상태 보기에 대한 정보는 다음을 참조하세요. ["관계: 지난 1개월 전송 상태 보기"](#).
- 관계: 지난 1개월 전송률 보기에 대한 정보는 다음을 참조하세요. ["관계: 지난 1개월 전송률 보기"](#).
- 관계: 모든 관계 보기에 대한 정보는 다음을 참조하세요. ["관계: 모든 관계 보기"](#).

MetroCluster 복제 모니터링

데이터를 미러링하는 동안 논리적 연결의 전반적인 상태를 모니터링하고 진단할 수 있습니다.

집계, 노드, 스토리지 가상 머신 등 클러스터 구성 요소의 미러링을 방해하는 문제나 위험을 식별할 수 있습니다.

Unified Manager는 시스템 상태 알람을 사용하여 MetroCluster 구성의 구성 요소와 연결 상태를 모니터링합니다.

시작하기 전에

MetroCluster 구성의 로컬 및 원격 클러스터는 모두 Unified Manager에 추가되어야 합니다.

IP 구성을 통한 **MetroCluster**에 대한 복제 보기

IP를 통한 MetroCluster 구성의 경우, Unified Manager 왼쪽 탐색 창의 다음 보기에서 IP를 통한 MetroCluster로 보호되는 클러스터의 토폴로지 피크 보기에 데이터 복제 상태가 표시됩니다.

- 저장소 > 클러스터 > 보호: **MetroCluster** 보기
- 보호 > 관계 > 관계: **MetroCluster** 보기

자세한 내용은 다음을 참조하세요. "[IP를 통한 MetroCluster의 연결 문제 모니터링](#)".

FC 구성을 통한 **MetroCluster**에 대한 복제 보기

FC 구성을 통한 MetroCluster의 데이터 복제에 문제가 있는지 확인하려면 다음 단계를 따르세요.

단계

1. 왼쪽 탐색 창에서 저장소 > *클러스터*를 클릭합니다.

모니터링되는 클러스터 목록이 표시됩니다.

2. 상태: 모든 클러스터 보기에서 MetroCluster 복제 세부 정보를 보려는 클러스터의 이름을 클릭합니다. 클러스터/상태 세부 정보 페이지에서 *MetroCluster 복제* 탭을 클릭합니다.

복제될 MetroCluster 구성의 토폴로지는 데이터가 미러링되는 원격 사이트에 대한 정보와 함께 해당 클러스터 개체 영역의 로컬 사이트에 표시됩니다. 아이콘 위에 포인터를 올리면 생성된 이벤트에 대한 자세한 정보를 볼 수 있습니다.

클러스터/상태 세부 정보 페이지에 표시된 정보를 사용하여 복제 문제를 해결할 수 있습니다. MetroCluster 구성에서 미러링 문제가 발견되면 System Manager에 로그인하거나 ONTAP CLI에 액세스하여 문제를 해결해야 합니다.

관련 정보

"[클러스터/상태 세부 정보 페이지](#)"

할당량 관리

사용자 및 그룹 할당량을 사용하여 사용자나 사용자 그룹이 사용할 수 있는 디스크 공간이나 파일 수를 제한할 수 있습니다. 디스크 및 파일 사용량, 디스크에 설정된 다양한 한도 등 사용자 및 사용자 그룹 할당량 정보를 볼 수 있습니다.

할당량 한도는 무엇입니까?

사용자 할당량 한도는 Unified Manager 서버가 사용자의 공간 소비량이 한도에 근접했는지 또는 사용자 할당량에 의해 설정된 한도에 도달했는지 평가하는 데 사용하는 값입니다. 소프트 한도를 초과하거나 하드 한도에 도달하면 Unified Manager 서버는 사용자 할당량 이벤트를 생성합니다.

기본적으로 Unified Manager 서버는 할당량 소프트 한도를 초과했거나 할당량 하드 한도에 도달했으며 사용자 할당량 이벤트가 구성된 사용자에게 알림 이메일을 보냅니다. 애플리케이션 관리자 역할이 있는 사용자는 지정된 수신자에게 사용자 또는 사용자 그룹 할당량 이벤트를 알리는 알림을 구성할 수 있습니다.

ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 할당량 한도를 지정할 수 있습니다.

사용자 및 사용자 그룹 할당량 보기

저장소 VM/상태 세부 정보 페이지에는 SVM에 구성된 사용자 및 사용자 그룹 할당량에 대한 정보가 표시됩니다. 사용자 또는 사용자 그룹의 이름, 디스크와 파일에 설정된 제한, 사용된 디스크와 파일 공간, 알림을 위한 이메일 주소를 볼 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *저장소 VM*을 클릭합니다.
2. 상태: 모든 저장소 **VM** 보기에서 저장소 VM을 선택한 다음 사용자 및 그룹 할당량 탭을 클릭합니다.

관련 정보

["사용자 추가"](#)

이메일 주소를 생성하는 규칙을 만듭니다.

클러스터, 스토리지 가상 머신(SVM), 볼륨, Q트리, 사용자 또는 사용자 그룹과 관련된 사용자 할당량을 기반으로 이메일 주소를 지정하는 규칙을 만들 수 있습니다. 할당량 위반이 발생하면 지정된 이메일 주소로 알림이 전송됩니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 사용자 및 그룹 할당량 이메일 주소 생성 규칙 페이지의 지침을 검토했어야 합니다.

할당량 이메일 주소에 대한 규칙을 정의하고 실행하려는 순서대로 입력해야 합니다. 예를 들어, abc의 할당량 위반에 대한 알림을 받기 위해 [abc@xyz.com](#) 이메일 주소를 사용하고 다른 모든 그룹에는 dl-\$GROUP@\$DOMAIN 이메일 주소를 사용하려는 경우, 규칙을 다음 순서대로 나열해야 합니다.

- \$USER == 'abc'이면 abc@xyz.com입니다.
- \$GROUP == * 이면 dl-\$GROUP@\$DOMAIN

지정한 규칙에 대한 기준이 하나도 충족되지 않으면 기본 규칙이 사용됩니다.

\$USER_OR_GROUP == * 이면 \$USER_OR_GROUP@\$DOMAIN

단계

1. 왼쪽 탐색 창에서 일반 > *할당량 이메일 규칙*을 클릭합니다.
2. 귀하의 기준에 따라 규칙을 입력하세요.
3. *검증*을 클릭하여 규칙 구문을 검증합니다.

규칙의 구문이 올바르지 않으면 오류 메시지가 표시됩니다. 구문을 수정하고 *검증*을 다시 클릭해야 합니다.

4. *저장*을 클릭하세요.
5. 생성한 이메일 주소가 저장소 **VM**/상태 세부 정보 페이지의 사용자 및 그룹 할당량 탭에 표시되는지 확인하세요.

사용자 및 사용자 그룹 할당량에 대한 이메일 알림 형식을 만듭니다.

할당량 관련 문제(소프트 한도 초과 또는 하드 한도 도달)가 발생할 때 사용자 또는 사용자 그룹에 전송되는 이메일에 대한 알림 형식을 만들 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *할당량 이메일 형식*을 클릭합니다.
2. 보낸 사람, 제목, 이메일 세부 정보 필드에 세부 정보를 입력하거나 수정하세요.
3. *미리보기*를 클릭하면 이메일 알림을 미리 볼 수 있습니다.
4. 미리보기 창을 닫으려면 *닫기*를 클릭하세요.
5. 필요한 경우 이메일 알림 내용을 수정하세요.
6. *저장*을 클릭하세요.

사용자 및 그룹 할당량 이메일 주소 편집

클러스터, 스토리지 가상 머신(SVM), 볼륨, Q트리, 사용자 또는 사용자 그룹과 관련된 사용자 할당량에 따라 이메일 주소를 수정할 수 있습니다. 사용자 및 그룹 할당량 이메일 주소 생성 규칙 대화 상자에서 지정한 규칙에 따라 생성된 이메일 주소를 재정의하려면 이메일 주소를 수정할 수 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 당신은 검토해야 합니다"[규칙 생성을 위한 지침](#)".

이메일 주소를 편집하는 경우 사용자 및 그룹 할당량 이메일 주소를 생성하는 규칙이 더 이상 할당량에 적용되지 않습니다. 지정된 규칙에 따라 생성된 이메일 주소로 알림을 보내려면 이메일 주소를 삭제하고 변경 사항을 저장해야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *SVM*을 클릭합니다.
2. 상태: 모든 저장소 **VM** 보기에서 SVM을 선택한 다음 사용자 및 그룹 할당량 탭을 클릭합니다.
3. 탭 행 아래에 있는 *이메일 주소 편집*을 클릭하세요.
4. 이메일 주소 편집 대화 상자에서 적절한 작업을 수행합니다.

만약에...	그 다음에...
지정된 규칙에 의해 생성된 이메일 주소로 알림을 보내려고 합니다.	a. 이메일 주소 필드에서 이메일 주소를 삭제하세요. b. *저장*을 클릭하세요. c. F5를 눌러 브라우저를 새로 고치면 이메일 주소 편집 대화 상자가 다시 로드됩니다. 지정된 규칙에 의해 생성된 이메일 주소는 이메일 주소 필드에 표시됩니다.
지정된 이메일 주소로 알림을 보내려고 합니다.	a. 이메일 주소 필드에서 이메일 주소를 수정하세요. b. *저장*을 클릭하세요. 사용자 및 그룹 할당량 이메일 주소를 생성하는 규칙은 더 이상 할당량에 적용되지 않습니다.

할당량에 대해 자세히 알아보세요

할당량에 대한 개념을 이해하면 사용자 할당량과 사용자 그룹 할당량을 효율적으로 관리하는 데 도움이 됩니다.

할당 프로세스 개요

할당량은 유연할 수도 있고 엄격할 수도 있습니다. 소프트 할당량은 지정된 한도를 초과하면 ONTAP 알림을 보내게 하고, 하드 할당량은 지정된 한도를 초과하면 쓰기 작업이 성공하지 못하도록 합니다.

ONTAP 사용자 또는 사용자 그룹으로부터 FlexVol volume 에 쓰기 요청을 받으면 해당 볼륨에서 사용자 또는 사용자 그룹에 대한 할당량이 활성화되었는지 확인하고 다음 사항을 확인합니다.

- 하드 리미트에 도달할지 여부

그렇다면 하드 한도에 도달하고 하드 할당량 알림이 전송되면 쓰기 작업이 실패합니다.

- 소프트 리미트가 위반될지 여부

그렇다면 소프트 한도를 초과하고 소프트 할당량 알림이 전송되면 쓰기 작업이 성공합니다.

- 쓰기 작업이 소프트 한도를 초과하지 않는지 여부

그렇다면 쓰기 작업은 성공하고 알림은 전송되지 않습니다.

할당량에 대하여

할당량은 사용자, 그룹 또는 Qtree에서 사용하는 디스크 공간과 파일 수를 제한하거나 추적하는 방법을 제공합니다. 다음을 사용하여 할당량을 지정합니다. /etc/quotas 파일. 할당량은 특정 볼륨이나 Qtree에 적용됩니다.

왜 할당량을 사용합니까?

할당량을 사용하면 FlexVol 볼륨의 리소스 사용량을 제한하고, 리소스 사용량이 특정 수준에 도달하면 알림을 제공하거나, 리소스 사용량을 추적할 수 있습니다.

다음과 같은 이유로 할당량을 지정합니다.

- 사용자 또는 그룹이 사용할 수 있는 디스크 공간이나 파일 수, 또는 Qtree에 포함될 수 있는 파일 수를 제한하려면
- 제한을 두지 않고 사용자, 그룹 또는 Qtree가 사용하는 디스크 공간의 양이나 파일 수를 추적하려면
- 디스크 사용량이나 파일 사용량이 높을 때 사용자에게 경고합니다.

할당량 대화 상자 설명

Health: All Storage VMs 보기의 User and Group Quotas 탭에서 적절한 옵션을 사용하여 할당량 관련 문제가 발생할 때 전송되는 이메일 알림의 형식을 구성하고 사용자 할당량에 따라 이메일 주소를 지정하는 규칙을 구성할 수 있습니다.

이메일 알림 형식 페이지

이메일 알림 형식 페이지는 할당량 관련 문제(소프트 한도 위반 또는 하드 한도 도달)가 있을 때 사용자 또는 사용자 그룹에 전송되는 이메일의 규칙을 표시합니다.

이메일 알림은 다음 사용자 또는 사용자 그룹 할당량 이벤트가 생성될 때만 전송됩니다. 사용자 또는 그룹 할당량 디스크 공간 소프트 한도 위반, 사용자 또는 그룹 할당량 파일 수 소프트 한도 위반, 사용자 또는 그룹 할당량 디스크 공간 하드 한도 도달, 사용자 또는 그룹 할당량 파일 수 하드 한도 도달.

- 에서

이메일이 발송된 이메일 주소가 표시되며, 수정이 가능합니다. 기본적으로 이는 알림 페이지에 지정된 이메일 주소입니다.

- 주제

알림 이메일의 제목을 표시합니다.

- 이메일 세부 정보

알림 이메일의 텍스트를 표시합니다. 귀하의 요구 사항에 맞게 텍스트를 수정할 수 있습니다. 예를 들어, 할당량 속성과 관련된 정보를 제공하고 키워드 수를 줄일 수 있습니다. 하지만 키워드는 수정하면 안 됩니다.

유효한 키워드는 다음과 같습니다.

- \$이벤트_이름

이메일 알림을 발생시킨 이벤트 이름을 지정합니다.

- 할당량_목표

할당량이 적용되는 qtree 또는 볼륨을 지정합니다.

- 할당량_사용_퍼센트

사용자 또는 사용자 그룹에서 사용하는 디스크 하드 제한, 디스크 소프트웨어 제한, 파일 하드 제한 또는 파일 소프트웨어 제한의 백분율을 지정합니다.

- 할당량_한도

사용자 또는 사용자 그룹이 도달한 디스크 하드 한도 또는 파일 하드 한도를 지정하고 다음 이벤트 중 하나가 생성됩니다.

- 사용자 또는 그룹 할당량 디스크 공간 하드 한도에 도달했습니다.
- 사용자 또는 그룹 할당량 디스크 공간 소프트웨어 한도에 도달했습니다.
- 사용자 또는 그룹 할당량 파일 수 하드 제한에 도달했습니다.
- 사용자 또는 그룹 할당량 파일 수 소프트웨어 제한에 도달했습니다.

- \$QUOTA_USED

사용자 또는 사용자 그룹이 사용한 디스크 공간이나 생성한 파일 수를 지정합니다.

- \$QUOTA_USER

사용자 또는 사용자 그룹 이름을 지정합니다.

명령 버튼

명령 단추를 사용하면 이메일 알림 형식에 대한 변경 사항을 미리 보고, 저장하거나 취소할 수 있습니다.

- 시사

알림 이메일의 미리보기를 표시합니다.

- 공장 기본값으로 복원

알림 형식을 공장 기본값으로 복원할 수 있습니다.

- 구하다

알림 형식에 대한 변경 사항을 저장합니다.

사용자 및 그룹 할당량 이메일 주소 생성 규칙 페이지

사용자 및 그룹 할당량 이메일 주소 생성 규칙 페이지를 사용하면 클러스터, SVM, 볼륨, Q트리, 사용자 또는 사용자 그룹과 관련된 사용자 할당량을 기반으로 이메일 주소를 지정하는 규칙을 만들 수 있습니다. 할당량이 초과되면 지정된 이메일 주소로 알림이 전송됩니다.

규칙 영역

할당된 이메일 주소에 대한 규칙을 정의해야 합니다. 규칙을 설명하는 주석을 추가할 수도 있습니다.

규칙을 정의하는 방법

실행하려는 순서대로 규칙을 입력해야 합니다. 첫 번째 규칙의 기준이 충족되면 이 규칙에 따라 이메일 주소가 생성됩니다. 만약 기준이 충족되지 않으면 다음 규칙의 기준이 고려되고, 이런 식으로 계속됩니다. 각 줄에는 별도의 규칙이 나열되어 있습니다. 기본 규칙은 목록의 마지막 규칙입니다. 규칙의 우선순위를 변경할 수 있습니다. 하지만 기본 규칙의 순서는 변경할 수 없습니다.

예를 들어, qtree1의 할당량 위반에 대한 알림을 받기 위해 이메일 주소 qtree1@xyz.com을 사용하고 다른 모든 qtree에 대해 이메일 주소 admin@xyz.com을 사용하려는 경우, 규칙을 다음 순서로 나열해야 합니다.

- \$QTREE == 'qtree1'이면 qtree1@xyz.com입니다.
- \$QTREE == * 이면 admin@xyz.com입니다.

지정한 규칙에 대한 기준이 하나도 충족되지 않으면 기본 규칙이 사용됩니다.

\$USER_OR_GROUP == * 이면 \$USER_OR_GROUP@\$DOMAIN

두 명 이상의 사용자가 동일한 할당량을 가지고 있는 경우, 사용자 이름은 쉼표로 구분된 값으로 표시되며 해당 규칙은 할당량에 적용되지 않습니다.

댓글을 추가하는 방법

규칙을 설명하는 주석을 추가할 수 있습니다. 각 주석의 시작 부분에 #을 사용해야 하며, 각 줄에 별도의 주석을 나열해야 합니다.

규칙 구문

규칙의 구문은 다음 중 하나여야 합니다.

- 만약에 (valid variableoperator *) 그 다음에 email ID@domain name

if는 키워드이고 소문자입니다. 연산자는 ==입니다. 이메일 ID에는 모든 문자, 유효한 변수 \$USER_OR_GROUP, \$USER 또는 \$GROUP이 포함될 수 있으며, 모든 문자와 유효한 변수 \$USER_OR_GROUP, \$USER 또는 \$GROUP의 조합이 포함될 수 있습니다. 도메인 이름에는 모든 문자, 유효한 변수 \$DOMAIN, 또는 모든 문자와 유효한 변수 \$DOMAIN의 조합이 포함될 수 있습니다. 유효한 변수는 대문자 또는 소문자일 수 있지만 두 가지를 조합한 것은 허용되지 않습니다. 예를 들어, \$domain과 \$DOMAIN은 유효하지만 \$Domain은 유효한 변수가 아닙니다.

- 만약에 (valid variableoperator `string`) 그 다음에 email ID@domain name

if는 키워드이고 소문자입니다. 연산자는 포함 또는 ==일 수 있습니다. 이메일 ID에는 모든 문자, 유효한 변수 \$USER_OR_GROUP, \$USER 또는 \$GROUP이 포함될 수 있으며, 모든 문자와 유효한 변수 \$USER_OR_GROUP, \$USER 또는 \$GROUP의 조합이 포함될 수 있습니다. 도메인 이름에는 모든 문자, 유효한 변수 \$DOMAIN, 또는 모든 문자와 유효한 변수 \$DOMAIN의 조합이 포함될 수 있습니다. 유효한 변수는 대문자 또는 소문자일 수 있지만 두 가지를 조합한 것은 허용되지 않습니다. 예를 들어, \$domain과 \$DOMAIN은 유효하지만 \$Domain은 유효한 변수가 아닙니다.

명령 단추를 사용하면 생성된 규칙을 저장, 검증 또는 취소할 수 있습니다.

- 검증

생성된 규칙의 구문을 검증합니다. 검증 중에 오류가 발생하면 오류를 생성한 규칙과 오류 메시지가 표시됩니다.

- 공장 기본값으로 복원

주소 규칙을 공장 기본값으로 복원할 수 있습니다.

- 구하다

규칙의 구문을 검증하고 오류가 없으면 규칙을 저장합니다. 검증 중에 오류가 발생하면 오류를 생성한 규칙과 오류 메시지가 표시됩니다.

문제 해결

문제 해결 정보는 Unified Manager를 사용할 때 발생하는 문제를 식별하고 해결하는 데 도움이 됩니다.

Unified Manager 데이터베이스 디렉토리에 디스크 공간 추가

Unified Manager 데이터베이스 디렉토리에는 ONTAP 시스템에서 수집된 모든 상태 및 성능 데이터가 포함되어 있습니다. 어떤 상황에서는 데이터베이스 디렉터리의 크기를 늘려야 할 수도 있습니다.

예를 들어 Unified Manager가 각 클러스터에 많은 노드가 있는 많은 수의 클러스터에서 데이터를 수집하는 경우 데이터베이스 디렉터리가 가득 찰 수 있습니다. 데이터베이스 디렉터리가 90% 차면 경고 이벤트를 받고, 디렉터리가 95% 차면 위험 이벤트를 받게 됩니다.



디렉터리가 95% 채워진 후에는 클러스터에서 추가 데이터가 수집되지 않습니다.

데이터 디렉토리에 용량을 추가하는 데 필요한 단계는 Unified Manager가 VMware ESXi 서버, Red Hat Linux 서버 또는 Microsoft Windows 서버에서 실행되는지에 따라 다릅니다.

VMware 가상 머신의 데이터 디스크에 공간 추가

Unified Manager 데이터베이스의 데이터 디스크 공간을 늘려야 하는 경우 Unified Manager 유지 관리 콘솔을 사용하여 디스크 공간을 늘려 설치 후 용량을 추가할 수 있습니다.

시작하기 전에

- vSphere Client에 액세스할 수 있어야 합니다.
- 가상 머신에는 로컬로 저장된 스냅샷이 없어야 합니다.
- 유지 관리 사용자 자격 증명이 있어야 합니다.

가상 디스크 크기를 늘리기 전에 가상 머신을 백업하는 것이 좋습니다.

단계

1. vSphere 클라이언트에서 Unified Manager 가상 머신을 선택한 다음 데이터에 디스크 용량을 추가합니다. disk 3 . 자세한 내용은 VMware 설명서를 참조하세요.

드물지만 Unified Manager 배포에서는 "하드 디스크 3" 대신 "하드 디스크 2"를 데이터 디스크로 사용합니다. 배포 중에 이런 일이 발생한 경우, 더 큰 디스크의 공간을 늘리세요. 데이터 디스크는 항상 다른 디스크보다 더 많은 공간을 갖습니다.

2. vSphere 클라이언트에서 Unified Manager 가상 머신을 선택한 다음 콘솔 탭을 선택합니다.
3. 콘솔 창을 클릭한 다음 사용자 이름과 비밀번호를 사용하여 유지 관리 콘솔에 로그인합니다.
4. 메인 메뉴*에서 *시스템 구성 옵션의 번호를 입력하세요.
5. 시스템 구성 메뉴*에서 *데이터 디스크 크기 늘리기 옵션에 대한 숫자를 입력합니다.

Linux 호스트의 데이터 디렉토리에 공간 추가

디스크 공간을 충분히 할당하지 않은 경우 /opt/netapp/data Linux 호스트를 처음 설정한 후 Unified Manager를 설치한 경우 Unified Manager를 지원하는 디렉토리에서 디스크 공간을 늘려 설치 후 디스크 공간을 추가할 수 있습니다. /opt/netapp/data 예매 규칙서.

시작하기 전에

Unified Manager가 설치된 Red Hat Enterprise Linux 시스템에 루트 사용자 액세스 권한이 있어야 합니다.

데이터 디렉터리 크기를 늘리기 전에 Unified Manager 데이터베이스를 백업하는 것이 좋습니다.

단계

1. 디스크 공간을 추가하려는 Linux 컴퓨터에 루트 사용자로 로그인합니다.
2. 표시된 순서대로 Unified Manager 서비스와 관련 MySQL 소프트웨어를 중지합니다. `systemctl stop ocieau ocie mysqld`
3. 임시 백업 폴더를 만듭니다(예: /backup-data) 현재 데이터를 포함할 수 있는 충분한 디스크 공간이 있음 /opt/netapp/data 예매 규칙서.
4. 기존의 콘텐츠 및 권한 구성을 복사합니다. /opt/netapp/data 백업 데이터 디렉터리로의 디렉토리:

```
cp -arp /opt/netapp/data/* /backup-data
```

5. SE Linux가 활성화된 경우:

- a. 기존 폴더에 대한 SE Linux 유형을 가져옵니다. /opt/netapp/data 접는 사람:

```
se_type=`ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' | head -1
```

시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
echo $se_type
mysqld_db_t
```

- a. 실행하다 chcon 백업 디렉토리에 대한 SE Linux 유형을 설정하는 명령:

```
chcon -R --type=mysqlld_db_t /backup-data
```

6. 내용을 제거하세요 /opt/netapp/data 예매 규칙서:

a. `cd /opt/netapp/data`

b. `rm -rf *`

7. 크기를 확장하세요 /opt/netapp/data LVM 명령을 통해 또는 추가 디스크를 추가하여 디렉토리를 최소 150GB로 늘릴 수 있습니다.



당신이 만든 경우 /opt/netapp/data 디스크에서 마운트를 시도해서는 안 됩니다. /opt/netapp/data NFS 또는 CIFS 공유로. 왜냐하면 이 경우 디스크 공간을 확장하려고 하면 다음과 같은 일부 LVM 명령이 `resize` 그리고 `extend` 예상대로 작동하지 않을 수도 있습니다.

8. 확인해주세요 /opt/netapp/data 디렉토리 소유자(mysql)와 그룹(root)은 변경되지 않습니다.

```
ls -ltr /opt/netapp/ | grep data
```

시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. SE Linux가 활성화된 경우 컨텍스트를 확인하십시오. /opt/netapp/data 디렉토리는 여전히 `mysqlld_db_t`로 설정되어 있습니다.

a. `touch /opt/netapp/data/abc`

b. `ls -Z /opt/netapp/data/abc`

시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
-rw-r--r--. root root unconfined_u:object_r:mysqlld_db_t:s0  
/opt/netapp/data/abc
```

10. 파일을 삭제하세요 abc 이렇게 하면 이 외부 파일로 인해 나중에 데이터베이스 오류가 발생하지 않습니다.

11. 내용을 복사하세요 backup-data 확장된 것으로 돌아가기 /opt/netapp/data 예매 규칙서:

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. SE Linux가 활성화된 경우 다음 명령을 실행하세요.

```
chcon -R --type=mysqlld_db_t /opt/netapp/data
```

13. MySQL 서비스를 시작합니다:

```
systemctl start mysqld
```

14. MySQL 서비스가 시작된 후, 표시된 순서대로 ocie 및 ocieau 서비스를 시작합니다.

```
systemctl start ocie ocieau
```

15. 모든 서비스가 시작된 후 백업 폴더를 삭제하세요. /backup-data :

```
rm -rf /backup-data
```

Microsoft Windows 서버의 논리 드라이브에 공간 추가

Unified Manager 데이터베이스의 디스크 공간을 늘려야 하는 경우 Unified Manager가 설치된 논리 드라이브에 용량을 추가할 수 있습니다.

시작하기 전에

Windows 관리자 권한이 있어야 합니다.

디스크 공간을 추가하기 전에 Unified Manager 데이터베이스를 백업하는 것이 좋습니다.

단계

1. 디스크 공간을 추가하려는 Windows 서버에 관리자로 로그인합니다.
2. 더 많은 공간을 추가하는 데 사용하려는 방법에 해당하는 단계를 따르세요.

옵션	설명
물리적 서버에서 Unified Manager 서버가 설치된 논리 드라이브에 용량을 추가합니다.	Microsoft 항목의 단계를 따르세요. "기본 볼륨 확장"
실제 서버에 하드 디스크 드라이브를 추가합니다.	Microsoft 항목의 단계를 따르세요. "하드 디스크 드라이브 추가"
가상 머신에서 디스크 파티션의 크기를 늘립니다.	VMware 항목의 단계를 따르세요. "디스크 파티션 크기 늘리기"

성능 통계 수집 간격 변경

성능 통계의 기본 수집 간격은 5분입니다. 대규모 클러스터의 컬렉션이 기본 시간 내에 완료되지 않는 경우 이 간격을 10분 또는 15분으로 변경할 수 있습니다. 이 설정은 Unified Manager 인스턴스가 모니터링하는 모든 클러스터의 통계 수집에 영향을 미칩니다.

시작하기 전에

Unified Manager 서버의 유지 관리 콘솔에 로그인하려면 권한이 있는 사용자 ID와 비밀번호가 있어야 합니다.

성능 통계 수집이 제때 완료되지 않는 문제는 배너 메시지로 표시됩니다. Unable to consistently collect from cluster <cluster_name> or Data collection is taking too long on cluster

<cluster_name>.

통계 수집 문제로 인해 필요한 경우에만 수집 간격을 변경해야 합니다. 다른 이유로는 이 설정을 변경하지 마세요.



기본 설정인 5분에서 이 값을 변경하면 Unified Manager에서 보고하는 성능 이벤트의 수와 빈도에 영향을 미칠 수 있습니다. 예를 들어, 시스템에서 정의한 성능 임계값은 정책을 30분 동안 초과하면 이벤트를 트리거합니다. 5분 수집을 사용하는 경우, 해당 정책을 6회 연속으로 초과해야 합니다. 15분 간격 수거의 경우, 해당 정책은 두 번의 수거 기간 동안만 초과될 수 있습니다.

클러스터 설정 페이지 하단의 메시지는 현재 통계 데이터 수집 간격을 나타냅니다.

단계

1. SSH를 사용하여 Unified Manager 호스트에 유지 관리 사용자로 로그인합니다.

Unified Manager 유지 관리 콘솔 프롬프트가 표시됩니다.

2. *성능 폴링 간격 구성*이라고 표시된 메뉴 옵션의 번호를 입력한 다음 Enter 키를 누릅니다.
3. 메시지가 표시되면 유지 관리 사용자 비밀번호를 다시 입력하세요.
4. 설정하려는 새로운 폴링 간격에 대한 숫자를 입력한 다음 Enter를 누릅니다.

Unified Manager 수집 간격을 10분 또는 15분으로 변경하고 외부 데이터 공급자(예: Graphite)에 현재 연결되어 있는 경우, 데이터 공급자 전송 간격을 Unified Manager 수집 간격보다 크거나 같도록 변경해야 합니다.

Unified Manager가 이벤트 및 성능 데이터를 보관하는 기간 변경

기본적으로 Unified Manager는 모니터링되는 모든 클러스터에 대한 이벤트 데이터와 성능 데이터를 6개월 동안 저장합니다. 이 기간이 지나면 새로운 데이터를 위한 공간을 확보하기 위해 오래된 데이터는 자동으로 삭제됩니다. 이 기본 기간은 대부분의 구성에 적합하지만, 클러스터와 노드가 많은 대규모 구성의 경우 Unified Manager가 최적으로 작동하도록 보존 기간을 줄여야 할 수도 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

데이터 보존 페이지에서 이 두 가지 유형의 데이터에 대한 보존 기간을 변경할 수 있습니다. 이러한 설정은 Unified Manager 인스턴스가 모니터링하는 모든 클러스터의 데이터 보존에 영향을 미칩니다.



Unified Manager는 5분마다 성능 통계를 수집합니다. 매일 5분 통계가 시간별 성과 통계로 요약됩니다. 기본적으로 5분 단위의 과거 성과 데이터를 30일 동안 보관하고, 6개월 분의 시간 단위 요약 성과 데이터를 보관합니다.

보존 기간이 부족한 경우나 백업 및 기타 작업을 완료하는 데 시간이 매우 오래 걸리는 경우에만 보존 기간을 줄여야 합니다. 보존 기간을 줄이면 다음과 같은 효과가 있습니다.

- 오래된 성능 데이터는 자정 이후에 Unified Manager 데이터베이스에서 삭제됩니다.
- 이전 이벤트 데이터는 Unified Manager 데이터베이스에서 즉시 삭제됩니다.
- 보존 기간 이전의 이벤트는 더 이상 사용자 인터페이스에서 볼 수 없습니다.

- 시간별 성과 통계가 표시되는 UI 위치는 보존 기간 전에는 비어 있습니다.
- 이벤트 보존 기간이 성과 데이터 보존 기간을 초과하는 경우 성과 슬라이더 아래에 메시지가 표시되어 이전 성과 이벤트에는 연관된 차트에 백업 데이터가 없을 수 있다는 경고가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 정책 > *데이터 보존*을 클릭합니다.
2. 데이터 보존 페이지에서 이벤트 보존 또는 성과 데이터 보존 영역의 슬라이더 도구를 선택하고 데이터를 보존해야 하는 개월 수로 이동한 후 *저장*을 클릭합니다.

알 수 없는 인증 오류

원격 사용자나 그룹을 추가, 편집, 삭제 또는 테스트하는 등 인증 관련 작업을 수행하는 경우 다음과 같은 오류 메시지가 표시될 수 있습니다. Unknown authentication error.

원인

다음 옵션에 잘못된 값을 설정한 경우 이 문제가 발생할 수 있습니다.

- Active Directory 인증 서비스의 관리자 이름
- OpenLDAP 인증 서비스의 고유 이름 바인딩

시정 조치

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. 선택한 인증 서비스에 따라 관리자 이름 또는 바인딩 고유 이름에 대한 적절한 정보를 입력합니다.
3. *인증 테스트*를 클릭하여 지정한 세부 정보로 인증을 테스트합니다.
4. *저장*을 클릭하세요.

사용자를 찾을 수 없습니다

원격 사용자나 그룹을 추가, 편집, 삭제 또는 테스트하는 등 인증 관련 작업을 수행하는 경우 다음 오류 메시지가 표시됩니다. User not found.

원인

이 문제는 사용자가 AD 서버나 LDAP 서버에 존재하고 기본 고유 이름을 잘못된 값으로 설정한 경우 발생할 수 있습니다.

시정 조치

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. 기본 고유 이름에 대한 적절한 정보를 입력하세요.
3. *저장*을 클릭하세요.

다른 인증 서비스를 사용하여 **LDAP**를 추가하는 데 문제가 있습니다.

인증 서비스로 기타를 선택하면 사용자 및 그룹 개체 클래스는 이전에 선택한 템플릿의 값을 유지합니다. LDAP 서버가 동일한 값을 사용하지 않으면 작업이 실패할 수 있습니다.

원인

OpenLDAP에서 사용자가 올바르게 구성되지 않았습니다.

시정 조치

다음 해결 방법 중 하나를 사용하여 이 문제를 수동으로 해결할 수 있습니다.

LDAP 사용자 개체 클래스와 그룹 개체 클래스가 각각 사용자와 그룹인 경우 다음 단계를 수행합니다.

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. 인증 서비스 드롭다운 메뉴에서 *Active Directory*를 선택한 다음 *기타*를 선택합니다.
3. 텍스트 필드를 완성하세요.

LDAP 사용자 개체 클래스와 그룹 개체 클래스가 각각 posixAccount와 posixGroup인 경우 다음 단계를 수행합니다.

1. 왼쪽 탐색 창에서 일반 > *원격 인증*을 클릭합니다.
2. 인증 서비스 드롭다운 메뉴에서 *OpenLDAP*를 선택한 다음 *기타*를 선택합니다.
3. 텍스트 필드를 완성하세요.

첫 번째 두 가지 해결 방법이 적용되지 않으면 전화하십시오. option-set API를 설정하고 auth.ldap.userObjectClass 그리고 auth.ldap.groupObjectClass 옵션을 올바른 값으로 변경합니다.

Windows 시스템의 NetApp Manageability SDK 로그 회전 문제

Windows 운영 체제에서 Unified Manager에 ONTAPI API 기반 클러스터를 추가한 후 nmsdk.log 파일 크기가 커져서 10MB 크기 제한을 초과합니다.

원인

로그 회전이 발생하지 않으면 이 문제가 발생할 수 있습니다.

시정 조치

1. Unified Manager를 중지합니다.
2. Windows에 Unified Manager를 설치하는 경우 Logrotate 버전 0.0.0.18을 설치하세요. 자세한 내용은 다음을 참조하세요. "[NetApp Manageability SDK 기술 보고서에 대한 보안 강화 가이드](#)".
3. Unified Manager를 시작합니다.

이벤트 및 알림 관리

이벤트 관리

이벤트는 모니터링되는 클러스터의 문제를 식별하는 데 도움이 됩니다.

Active IQ 플랫폼 이벤트는 무엇입니까?

Unified Manager는 Active IQ 플랫폼에서 발견된 이벤트를 표시할 수 있습니다. 이러한 이벤트는 Unified Manager에서 모니터링하는 모든 스토리지 시스템에서 생성된 AutoSupport 메시지에 대해 일련의 규칙을 실행하여 생성됩니다.

자세한 내용은 다음을 참조하세요. "[Active IQ 플랫폼 이벤트가 생성되는 방식](#)".

Unified Manager는 자동으로 새로운 규칙 파일을 확인하고 새로운 규칙이 있는 경우에만 새 파일을 다운로드합니다. 외부 네트워크 접속이 불가능한 사이트에서는 저장소 관리 > 이벤트 설정 > *규칙 업로드*에서 수동으로 규칙을 업로드해야 합니다.

이러한 Active IQ 이벤트는 기존 Unified Manager 이벤트와 겹치지 않으며 시스템 구성, 케이블링, 모범 사례 및 가용성 문제와 관련된 사고나 위험을 식별합니다.

플랫폼 이벤트 활성화에 대한 자세한 내용은 다음을 참조하세요. "[Active IQ 포털 이벤트 활성화](#)". 규칙 파일 업로드에 대한 자세한 내용은 다음을 참조하세요. "[새로운 Active IQ 규칙 파일 업로드](#)".

NetApp Active IQ 는 NetApp 하이브리드 클라우드 전반에서 스토리지 시스템 운영을 최적화하기 위해 예측 분석과 사전 지원을 제공하는 클라우드 기반 서비스입니다. 보다 "[NetApp Active IQ](#)" 자세한 내용은.

이벤트 관리 시스템 이벤트란 무엇입니까?

이벤트 관리 시스템(EMS)은 ONTAP 커널의 다양한 부분에서 이벤트 데이터를 수집하고 이벤트 전달 메커니즘을 제공합니다. 이러한 ONTAP 이벤트는 Unified Manager에서 EMS 이벤트로 보고될 수 있습니다. 중앙 집중식 모니터링 및 관리를 통해 중요한 EMS 이벤트 구성과 이러한 EMS 이벤트에 따른 경고 알림이 용이해집니다.

Unified Manager에 클러스터를 추가하면 Unified Manager 주소가 클러스터에 알림 대상으로 추가됩니다. EMS 이벤트는 클러스터에서 이벤트가 발생하자마자 보고됩니다.

Unified Manager에서 EMS 이벤트를 수신하는 방법에는 두 가지가 있습니다.

- 일정 수의 중요한 EMS 이벤트가 자동으로 보고됩니다.
- 개별 EMS 이벤트를 수신하도록 구독할 수 있습니다.

Unified Manager에서 생성된 EMS 이벤트는 이벤트가 생성된 방법에 따라 다르게 보고됩니다.

기능성	자동 EMS 메시지	구독된 EMS 메시지
이용 가능한 EMS 이벤트	EMS 이벤트의 하위 집합	모든 EMS 이벤트

기능성	자동 EMS 메시지	구독된 EMS 메시지
트리거 시 EMS 메시지 이름	Unified Manager 이벤트 이름(EMS 이벤트 이름에서 변환됨)	"EMS 수신 오류" 형식은 구체적이지 않습니다. 자세한 메시지는 실제 EMS 이벤트의 점 표기 형식을 제공합니다.
수신된 메시지	클러스터가 발견되자마자	Unified Manager에 필요한 각 EMS 이벤트를 추가한 후 다음 15분 폴링 주기가 지난 후
이벤트 수명 주기	다른 Unified Manager 이벤트와 동일: 새 항목, 확인됨, 해결됨 및 사용되지 않음 상태	EMS 이벤트는 이벤트가 생성된 후 15분 후 클러스터가 새로 고쳐지면 더 이상 사용되지 않습니다.
Unified Manager 가동 중지 시간 동안 이벤트를 캡처합니다.	예, 시스템이 시작되면 각 클러스터와 통신하여 누락된 이벤트를 수집합니다.	아니요
이벤트 세부 정보	제안된 시정 조치는 일관된 해결책을 제공하기 위해 ONTAP에서 직접 가져옵니다.	이벤트 세부 정보 페이지에서 시정 조치를 사용할 수 없습니다.



새로운 자동 EMS 이벤트 중 일부는 이전 이벤트가 해결되었음을 나타내는 정보 이벤트입니다. 예를 들어, "FlexGroup 구성 요소 공간 상태 모두 정상" 정보 이벤트는 "FlexGroup 구성 요소에 공간 문제가 있습니다" 오류 이벤트가 해결되었음을 나타냅니다. 정보 이벤트는 다른 이벤트 심각도 유형과 동일한 이벤트 수명 주기를 사용하여 관리할 수 없습니다. 그러나 동일한 볼륨에서 다른 "공간 문제" 오류 이벤트가 수신되면 해당 이벤트는 자동으로 폐기됩니다.

Unified Manager에 자동으로 추가되는 **EMS** 이벤트

다음 ONTAP EMS 이벤트는 Unified Manager에 자동으로 추가됩니다. 이러한 이벤트는 Unified Manager가 모니터링하는 모든 클러스터에서 트리거될 때 생성됩니다.

ONTAP 9.5 이상 소프트웨어를 실행하는 클러스터를 모니터링할 때 다음 EMS 이벤트를 사용할 수 있습니다.

통합 관리자 이벤트 이름	EMS 이벤트 이름	영향을 받는 리소스	통합 관리자 심각도
집계 이전으로 인해 클라우드 계층 액세스가 거부됨	arl.netra.ca.check.실패	골재	오류
스토리지 장애 조치 중 집계 재배포에 대한 클라우드 계층 액세스 거부	gb.netra.ca.확인 실패	골재	오류
FabricPool 미러 복제 재동기화 완료	waf1.ca.재동기화.완료	무리	오류

통합 관리자 이벤트 이름	EMS 이벤트 이름	영향을 받는 리소스	통합 관리자 심각도
FabricPool 공간이 거의 가득 찼습니다	패브릭풀.거의.가득	무리	오류
NVMe-oF 유예 기간 시작됨	nvmf.유예기간.시작	무리	경고
NVMe-oF 유예 기간 활성화	nvmf.유예기간.활성	무리	경고
NVMe-oF 유예 기간 만료	nvmf.유예기간.만료됨	무리	경고
LUN이 파괴되었습니다	lun.destroy	LUN	정보
클라우드 AWS MetaDataConnFail	cloud.aws.metadataConnFail	마디	오류
클라우드 AWS IAMCreds만료됨	cloud.aws.iamCreds만료됨	마디	오류
클라우드 AWS IAMCredsInvalid	cloud.aws.iamCredsInvalid	마디	오류
클라우드 AWS IAMCredsNotFound	cloud.aws.iamCredsNotFound	마디	오류
클라우드 AWS IAMCredsNotInitialized	cloud.aws.iamNotInitialized	마디	정보
클라우드 AWS IAMRoleInvalid	cloud.aws.iamRoleInvalid	마디	오류
클라우드 AWS IAMRoleNotFound	cloud.aws.iamRoleNotFound	마디	오류
클라우드 계층 호스트를 확인할 수 없음	objstore.host.해결할 수 없음	마디	오류
클라우드 계층 클러스터 간 네트워크 인터페이스 다운	objstore.interclusterlifDown	마디	오류
요청 불일치 클라우드 계층 서명	osc.signatureMismatch	마디	오류
NFSv4 풀 중 하나가 소진되었습니다.	Nblade.nfsV4PoolExhaust	마디	비판적인

통합 관리자 이벤트 이름	EMS 이벤트 이름	영향을 받는 리소스	통합 관리자 심각도
QoS 모니터 메모리가 최대화됨	qos.모니터.메모리.최대화	마디	오류
QoS 모니터 메모리 감소	qos.모니터.메모리.감소됨	마디	정보
NVMeNS 파괴	NVMeNS.파괴	네임스페이스	정보
NVMeNS 온라인	NVMeNS.오프라인	네임스페이스	정보
NVMeNS 오프라인	NVMeNS.online	네임스페이스	정보
NVMeNS 공간 부족	NVMeNS 공간 부족	네임스페이스	경고
동기 복제가 동기화되지 않음	sms.상태.동기화 안 됨	SnapMirror 관계	경고
동기 복제가 복원되었습니다	sms.status.in.sync	SnapMirror 관계	정보
동기 복제 자동 재동기화 실패	sms.resync.attempt.failed	SnapMirror 관계	오류
많은 CIFS 연결	Nblade.cifsManyAuths	서포트 머신(SVM)	오류
최대 CIFS 연결 수를 초과했습니다.	Nblade.cifsMaxOpenSameFile	서포트 머신(SVM)	오류
사용자당 CIFS 연결 최대 수를 초과했습니다.	Nblade.cifsMaxSessPerUserConn	서포트 머신(SVM)	오류
CIFS NetBIOS 이름 충돌	Nblade.cifsNbNameConflict	서포트 머신(SVM)	오류
존재하지 않는 CIFS 공유에 연결 시도	Nblade.cifsNoPriv공유	서포트 머신(SVM)	비판적인
CIFS 새도 복사본 작업이 실패했습니다.	cifs.shadowcopy.실패	서포트 머신(SVM)	오류
AV 서버에서 바이러스 발견	Nblade.vscanVirusDetected	서포트 머신(SVM)	오류
바이러스 검사를 위한 AV 서버 연결 없음	Nblade.vscanNoScannerConn	서포트 머신(SVM)	비판적인

통합 관리자 이벤트 이름	EMS 이벤트 이름	영향을 받는 리소스	통합 관리자 심각도
등록된 AV 서버가 없습니다	Nblade.vscanNoRegdScanner	서포트 머신(SVM)	오류
응답하지 않는 AV 서버 연결	Nblade.vscanConn비활성화	서포트 머신(SVM)	정보
AV 서버가 너무 바빠서 새 스캔 요청을 수락할 수 없습니다.	Nblade.vscanConnBackPressure	서포트 머신(SVM)	오류
AV 서버에 대한 무단 사용자 시도	Nblade.vscanBadUserPrivAccess	서포트 머신(SVM)	오류
FlexGroup 구성 요소에 공간 문제가 있습니다.	flexgroup.구성원.공간.문제.	용량	오류
FlexGroup 구성 요소 공간 상태 모두 정상	flexgroup.구성 요소.공간.상태.모두.확인	용량	정보
FlexGroup 구성 요소에 Inode 문제가 있습니다.	flexgroup.구성원.아이노드.문제가 있습니다	용량	오류
FlexGroup 구성 요소 Inode 상태 모두 정상	flexgroup.구성 요소.inodes.상태.모두.ok	용량	정보
볼륨 논리 공간이 거의 가득 찼습니다	모니터.vol.nearFull.inc.sav	용량	경고
볼륨 논리 공간 가득 참	모니터.vol.full.inc.sav	용량	오류
볼륨 논리 공간 일반	모니터.vol.one.ok.inc.sav	용량	정보
WAFL 볼륨 자동 크기 조정 실패	wافل.vol.autoSize.실패	용량	오류
WAFL 볼륨 자동 크기 조정 완료	wافل.vol.autoSize.완료	용량	정보
WAFL READDIR 파일 작업 시간 초과	wافل.readdir.만료됨	용량	오류

ONTAP EMS 이벤트 구독하기

ONTAP 소프트웨어가 설치된 시스템에서 생성되는 이벤트 관리 시스템(EMS) 이벤트를

수신하도록 구독할 수 있습니다. 일부 EMS 이벤트는 Unified Manager에 자동으로 보고되지만, 추가 EMS 이벤트는 해당 이벤트를 구독한 경우에만 보고됩니다.

시작하기 전에

동일한 문제에 대해 두 개의 이벤트를 수신하게 되면 혼란이 생길 수 있으므로 Unified Manager에 자동으로 추가된 EMS 이벤트는 구독하지 마세요.

원하는 수의 EMS 이벤트에 가입할 수 있습니다. 구독한 모든 이벤트가 검증되고, 검증된 이벤트만 Unified Manager에서 모니터링하는 클러스터에 적용됩니다. ONTAP 9 EMS 이벤트 카탈로그는 ONTAP 9 소프트웨어의 특정 버전에 대한 모든 EMS 메시지에 대한 자세한 정보를 제공합니다. 해당 이벤트 목록을 보려면 ONTAP 9 제품 설명서 페이지에서 EMS 이벤트 카탈로그의 적절한 버전을 찾으세요.

"ONTAP 9 제품 라이브러리"

구독한 ONTAP EMS 이벤트에 대한 알림을 구성할 수 있으며, 이러한 이벤트에 대해 실행할 사용자 정의 스크립트를 만들 수 있습니다.



구독한 ONTAP EMS 이벤트를 받지 못하는 경우 클러스터의 DNS 구성에 문제가 있어 클러스터가 Unified Manager 서버에 도달하지 못할 수 있습니다. 이 문제를 해결하려면 클러스터 관리자가 클러스터의 DNS 구성을 수정한 다음 Unified Manager를 다시 시작해야 합니다. 이렇게 하면 보류 중인 EMS 이벤트가 Unified Manager 서버로 플러시됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *이벤트 설정*을 클릭합니다.
2. 이벤트 설정 페이지에서 **EMS** 이벤트 구독 버튼을 클릭합니다.
3. EMS 이벤트 구독 대화 상자에서 구독하려는 ONTAP EMS 이벤트의 이름을 입력합니다.

ONTAP 클러스터 셸에서 구독할 수 있는 EMS 이벤트의 이름을 보려면 다음을 사용할 수 있습니다. `event route show` 명령(ONTAP 9 이전) 또는 `event catalog show` 명령(ONTAP 9 이상).

"Active IQ Unified Manager 에서 ONTAP EMS 이벤트 구독에 대한 알림을 구성하고 수신하는 방법"

4. *추가*를 클릭하세요.

EMS 이벤트가 구독된 EMS 이벤트 목록에 추가되지만, 클러스터에 적용 가능 열에는 추가한 EMS 이벤트의 상태가 "알 수 없음"으로 표시됩니다.

5. *저장 및 닫기*를 클릭하여 클러스터에 EMS 이벤트 구독을 등록합니다.
6. *EMS 이벤트 구독*을 다시 클릭하세요.

추가한 EMS 이벤트의 적용 가능 클러스터 열에 상태 "예"가 나타납니다.

상태가 "예"가 아닌 경우 ONTAP EMS 이벤트 이름의 철자를 확인하세요. 이름을 잘못 입력한 경우 잘못된 이벤트를 삭제한 후 이벤트를 다시 추가해야 합니다.

ONTAP EMS 이벤트가 발생하면 이벤트 페이지에 이벤트가 표시됩니다. 이벤트 세부 정보 페이지에서 이벤트를 선택하면 EMS 이벤트에 대한 세부 정보를 볼 수 있습니다. 이벤트 처리를 관리하거나 이벤트에 대한 알림을 생성할 수도 있습니다.

이벤트가 수신되면 어떻게 되나요?

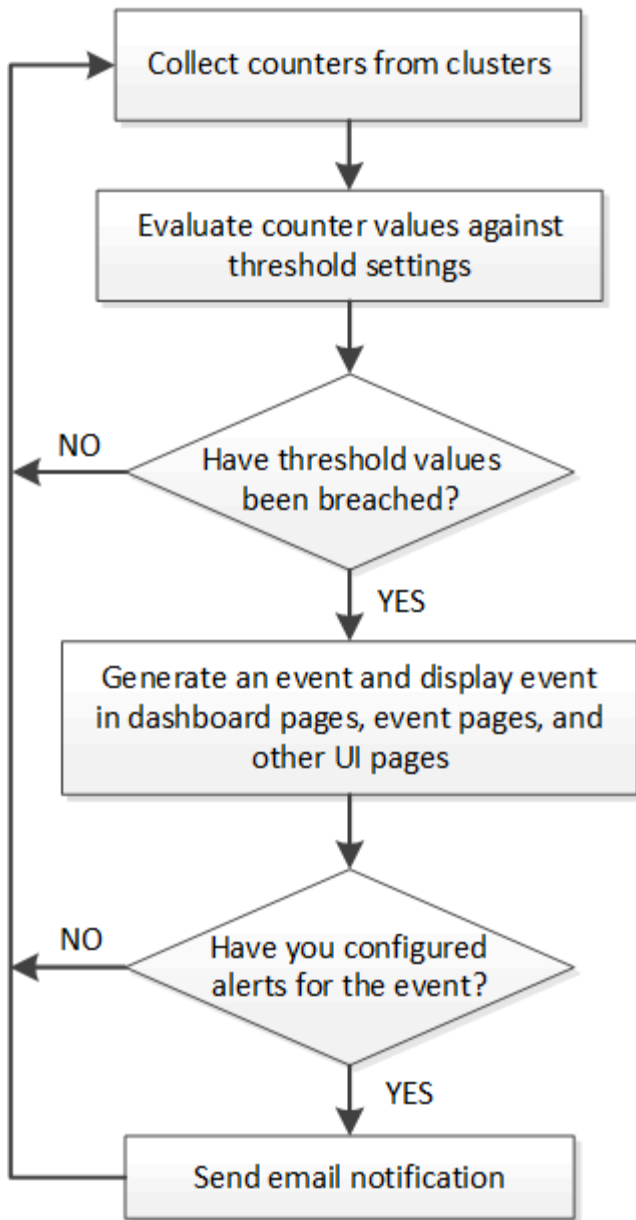
Unified Manager가 이벤트를 수신하면 대시보드 페이지, 이벤트 관리 인벤토리 페이지, 클러스터/성능 페이지의 요약 및 탐색기 탭, 개체별 인벤토리 페이지(예: 볼륨/상태 인벤토리 페이지)에 이벤트가 표시됩니다.

Unified Manager가 동일한 클러스터 구성 요소에 대해 동일한 이벤트 조건이 여러 번 연속적으로 발생하는 것을 감지하는 경우 모든 발생을 별도의 이벤트가 아닌 단일 이벤트로 처리합니다. 이벤트 기간이 증가하면 이벤트가 여전히 활성화되어 있음을 나타냅니다.

알림 설정 페이지에서 설정을 구성하는 방법에 따라 이러한 이벤트에 대해 다른 사용자에게 알릴 수 있습니다. 경고가 발생하면 다음 작업이 시작됩니다.

- 이벤트에 대한 이메일은 모든 Unified Manager 관리자 사용자에게 전송될 수 있습니다.
- 해당 이벤트는 추가 이메일 수신자에게 전송될 수 있습니다.
- SNMP 트랩은 트랩 수신기로 전송될 수 있습니다.
- 사용자 정의 스크립트를 실행하여 작업을 수행할 수 있습니다.

이 작업 흐름은 다음 다이어그램에 표시되어 있습니다.



이벤트 및 이벤트 세부 정보 보기

Unified Manager에서 트리거된 이벤트에 대한 세부 정보를 보고 시정 조치를 취할 수 있습니다. 예를 들어, 볼륨 오프라인이라는 상태 이벤트가 있는 경우 해당 이벤트를 클릭하면 세부 정보를 보고 시정 조치를 수행할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이벤트 세부 정보에는 이벤트 출처, 이벤트 원인, 이벤트와 관련된 참고 사항 등의 정보가 포함됩니다.

단계

1. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭합니다.

기본적으로 모든 활성 이벤트 보기에는 지난 7일 동안 생성되어 영향 수준이 사고 또는 위험인 새 이벤트와 확인된 (활성) 이벤트가 표시됩니다.

2. 예를 들어 용량 이벤트나 성능 이벤트 등 특정 이벤트 범주를 보려면 *보기*를 클릭하고 이벤트 유형 메뉴에서 선택하세요.
3. 자세한 내용을 보고 싶은 이벤트 이름을 클릭하세요.

이벤트 세부 정보는 이벤트 세부 정보 페이지에 표시됩니다.

할당되지 않은 이벤트 보기

할당되지 않은 이벤트를 보고 이를 해결할 수 있는 사용자에게 각각 할당할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭합니다.

기본적으로 새 이벤트와 확인된 이벤트는 이벤트 관리 인벤토리 페이지에 표시됩니다.

2. 필터 창에서 할당 대상 영역의 할당되지 않음 필터 옵션을 선택합니다.

이벤트 확인 및 해결

이벤트를 생성한 문제에 대한 작업을 시작하기 전에 이벤트를 확인해야 반복적으로 알림 알림을 받지 않을 수 있습니다. 특정 이벤트에 대한 시정 조치를 취한 후에는 해당 이벤트를 해결됨으로 표시해야 합니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

여러 이벤트를 동시에 확인하고 해결할 수 있습니다.



정보 이벤트를 확인할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭합니다.
2. 이벤트 목록에서 다음 작업을 수행하여 이벤트를 확인합니다.

만약 당신이 원한다면...	이렇게 하세요...
단일 이벤트를 확인하여 해결됨으로 표시합니다.	a. 이벤트 이름을 클릭하세요. b. 이벤트 세부 정보 페이지에서 이벤트의 원인을 확인하세요. c. *확인*을 클릭하세요. d. 적절한 시정 조치를 취하세요. e. *해결됨으로 표시*를 클릭하세요.

만약 당신이 원한다면...	이렇게 하세요...
여러 이벤트를 확인하여 해결됨으로 표시	a. 각 이벤트 세부 정보 페이지에서 이벤트의 원인을 확인하세요. b. 이벤트를 선택하세요. c. *확인*을 클릭하세요. d. 적절한 시정 조치를 취하세요. e. *해결됨으로 표시*를 클릭하세요.

이벤트가 해결됨으로 표시되면 해당 이벤트는 해결된 이벤트 목록으로 이동됩니다.

3. 선택 사항: 메모 및 업데이트 영역에서 이벤트를 어떻게 처리했는지에 대한 메모를 추가한 다음 *게시*를 클릭합니다.

특정 사용자에게 이벤트 할당

할당되지 않은 이벤트는 본인 또는 원격 사용자를 포함한 다른 사용자에게 할당할 수 있습니다. 필요한 경우 할당된 이벤트를 다른 사용자에게 재할당할 수 있습니다. 예를 들어, 스토리지 객체에서 자주 문제가 발생하는 경우 해당 객체를 관리하는 사용자에게 해당 문제에 대한 이벤트를 할당할 수 있습니다.

시작하기 전에

- 사용자 이름과 이메일 ID를 올바르게 구성해야 합니다.
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭합니다.
2. 이벤트 관리 인벤토리 페이지에서 할당하려는 이벤트를 하나 이상 선택합니다.
3. 다음 옵션 중 하나를 선택하여 이벤트를 할당하세요.

이벤트를 다음에 할당하려면...	그러면 이렇게 하세요...
당신 자신	할당 대상 > *나*를 클릭합니다.

이벤트를 다음에 할당하려면...	그러면 이렇게 하세요...
다른 사용자	a. 할당 대상 > *다른 사용자*를 클릭합니다. b. 소유자 할당 대화 상자에서 사용자 이름을 입력하거나 드롭다운 목록에서 사용자를 선택합니다. c. *할당*을 클릭합니다. 사용자에게 이메일 알림이 전송됩니다.  사용자 이름을 입력하지 않거나 드롭다운 목록에서 사용자를 선택하지 않고 *할당*을 클릭하면 이벤트가 할당되지 않은 상태로 유지됩니다.

원치 않는 이벤트 비활성화

모든 이벤트는 기본적으로 활성화되어 있습니다. 환경에서 중요하지 않은 이벤트에 대한 알림이 생성되는 것을 방지하기 위해 이벤트를 전역적으로 비활성화할 수 있습니다. 비활성화된 이벤트에 대한 알림을 다시 받고 싶을 때 해당 이벤트를 활성화할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이벤트를 비활성화하면 시스템에서 이전에 생성된 이벤트는 더 이상 사용되지 않는 것으로 표시되고, 이러한 이벤트에 대해 구성된 알림은 트리거되지 않습니다. 비활성화된 이벤트를 활성화하면 다음 모니터링 주기부터 해당 이벤트에 대한 알림이 생성됩니다.

개체에 대한 이벤트를 비활성화하는 경우(예: vol offline 이벤트)를 활성화한 후 나중에 이벤트를 활성화하면 Unified Manager는 이벤트가 비활성화 상태일 때 오프라인이 된 개체에 대해 새 이벤트를 생성하지 않습니다. Unified Manager는 이벤트가 다시 활성화된 후 개체 상태에 변경 사항이 있는 경우에만 새 이벤트를 생성합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *이벤트 설정*을 클릭합니다.
2. 이벤트 설정 페이지에서 다음 옵션 중 하나를 선택하여 이벤트를 비활성화하거나 활성화하세요.

만약 당신이 원한다면...	그러면 이렇게 하세요...
이벤트 비활성화	a. *비활성화*를 클릭합니다. b. 이벤트 비활성화 대화 상자에서 이벤트 심각도를 선택합니다. c. 일치하는 이벤트 열에서 이벤트 심각도에 따라 비활성화하려는 이벤트를 선택한 다음 오른쪽 화살표를 클릭하여 해당 이벤트를 비활성화 이벤트 열로 이동합니다. d. *저장 및 닫기*를 클릭하세요. e. 비활성화한 이벤트가 이벤트 설정 페이지의 목록 보기에 표시되는지 확인하세요.
이벤트 활성화	a. 활성화하려는 이벤트에 대한 확인란을 선택하세요. b. *활성화*를 클릭합니다.

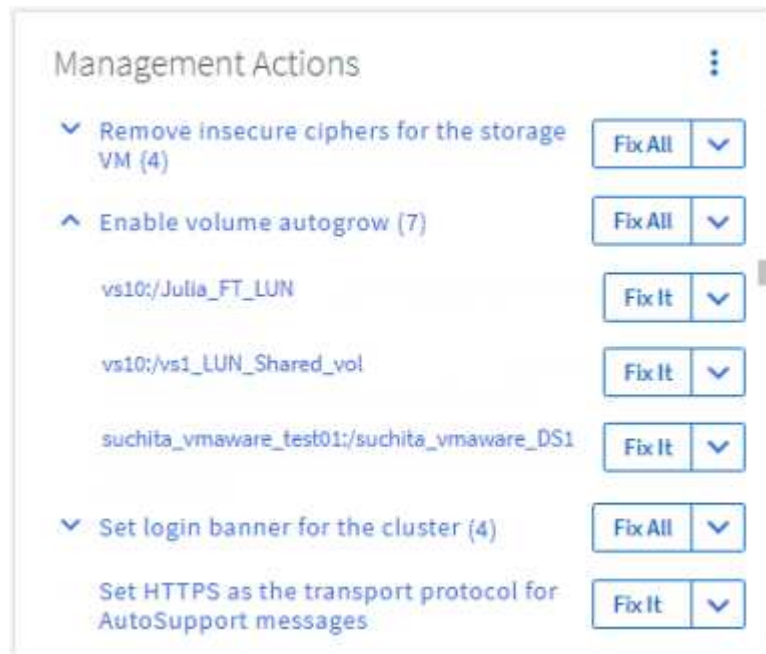
Unified Manager 자동 수정을 사용하여 문제 해결

Unified Manager는 특정 이벤트를 철저히 진단하고 수정 버튼을 사용하여 단일 해결책을 제공할 수 있습니다. 가능한 경우 해당 해결 방법은 대시보드, 이벤트 세부 정보 페이지, 왼쪽 탐색 메뉴의 작업 부하 분석 선택 항목에 표시됩니다.

대부분의 이벤트에는 이벤트 세부 정보 페이지에 표시되는 다양한 해결 방법이 있으므로 ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 최상의 솔루션을 구현할 수 있습니다. Unified Manager에서 문제를 해결할 수 있는 단일 해결책이 있고 ONTAP CLI 명령을 사용하여 해결할 수 있다고 판단한 경우 해결 작업을 사용할 수 있습니다.

단계

1. *대시보드*에서 수정할 수 있는 이벤트를 보려면 *대시보드*를 클릭하세요.



2. Unified Manager에서 해결할 수 있는 문제를 해결하려면 수정 버튼을 클릭하세요. 여러 개체에 존재하는 문제를 해결하려면 모두 수정 버튼을 클릭하세요.

자동 수정으로 해결할 수 있는 문제에 대한 정보는 다음을 참조하세요. "[Unified Manager가 해결할 수 있는 문제는 무엇입니까?](#)".

Active IQ 이벤트 보고 활성화 및 비활성화

Active IQ 플랫폼 이벤트는 기본적으로 Unified Manager 사용자 인터페이스에서 생성되어 표시됩니다. 이러한 이벤트가 너무 "시끄러운" 경우 또는 Unified Manager에서 이러한 이벤트를 보고 싶지 않은 경우 이러한 이벤트 생성을 비활성화할 수 있습니다. 나중에 다시 알림을 받으려면 해당 기능을 활성화하면 됩니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

이 기능을 비활성화하면 Unified Manager가 Active IQ 플랫폼 이벤트를 즉시 수신하지 않습니다.

이 기능을 활성화하면 Unified Manager는 클러스터의 시간대를 기준으로 자정 직후부터 Active IQ 플랫폼 이벤트를 수신하기 시작합니다. 시작 시간은 Unified Manager가 각 클러스터에서 AutoSupport 메시지를 수신하는 시점을 기준으로 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *기능 설정*을 클릭합니다.
2. 기능 설정 페이지에서 다음 옵션 중 하나를 선택하여 Active IQ 플랫폼 이벤트를 비활성화하거나 활성화합니다.

만약 당신이 원한다면...	그러면 이렇게 하세요...
Active IQ 플랫폼 이벤트 비활성화	• Active IQ Portal Events* 패널에서 슬라이더 버튼을 왼쪽으로 이동합니다.
Active IQ 플랫폼 이벤트 활성화	• Active IQ Portal Events* 패널에서 슬라이더 버튼을 오른쪽으로 이동합니다.

새로운 Active IQ 규칙 파일 업로드

Unified Manager는 새로운 Active IQ 이벤트(규칙) 파일을 자동으로 확인하고 새로운 규칙이 있으면 새 파일을 다운로드합니다. 하지만 외부 네트워크 접속이 불가능한 사이트에서는 규칙 파일을 수동으로 업로드해야 합니다.



Active IQ 규칙은 Config Advisor (CA) 보안 규칙이라고도 합니다.

네트워크 연결이 없는 사이트에서 Unified Manager를 특정 릴리스로 설치하거나 업그레이드하는 경우, 번들로 제공되는 Active IQ 규칙을 자동으로 업로드할 수 있습니다. 그러나 업데이트된 이벤트가 생성되고 스토리지 시스템이 계속해서 최적의 성능을 유지하려면 NetApp 지원 사이트에서 한 달에 한 번 정도 새로운 규칙 파일을 다운로드하는 것이 좋습니다.

시작하기 전에

- Active IQ 포털 이벤트 보고를 활성화해야 합니다. 이 기능은 기본적으로 활성화되어 있습니다. 자세한 내용은 다음을 참조하세요. "[Active IQ 포털 이벤트 활성화](#)".
- NetApp 지원 사이트에서 규칙 파일을 다운로드해야 합니다.

규칙 파일은 다음 위치에 있습니다. https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

단계

1. 네트워크 액세스가 가능한 컴퓨터에서 NetApp 지원 사이트로 이동하여 현재 규칙을 다운로드하세요. .zip 파일.

번들된 규칙 패키지에는 규칙 저장소, 데이터 소스, NetApp KB 문서가 포함되어 있습니다.



Windows 시스템에서 네트워크 연결이 없는 사이트의 경우 NetApp KB 문서는 기본적으로 설치 프로그램과 함께 제공되지 않습니다. 지원 사이트에서 *secure_rules.zip* 파일을 다운로드하고 업로드하면 모든 규칙에 대한 KB 문서를 볼 수 있습니다.

2. 규칙 파일을 보안 구역으로 가져올 수 있는 미디어로 옮긴 다음 보안 구역의 시스템에 복사합니다.
3. 왼쪽 탐색 창에서 저장소 관리 > *이벤트 설정*을 클릭합니다.
4. 이벤트 설정 페이지에서 규칙 업로드 버튼을 클릭합니다.
5. 업로드 규칙 대화 상자에서 규칙을 탐색하여 선택합니다. .zip 다운로드한 파일을 클릭하고 *업로드*를 클릭하세요.

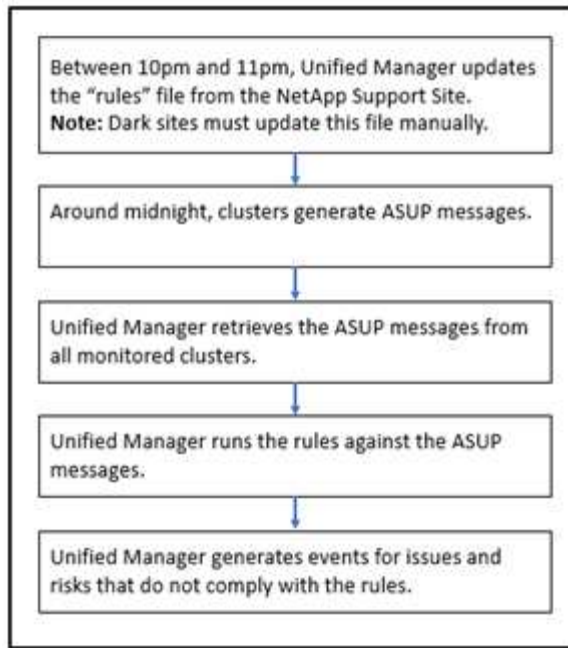
이 과정은 몇 분 정도 걸릴 수 있습니다.

규칙 파일은 Unified Manager 서버에서 압축이 풀립니다. 관리되는 클러스터가 자정 이후에 AutoSupport 파일을 생성하면 Unified Manager가 규칙 파일과 클러스터를 비교하여 필요에 따라 새로운 위험 및 사고 이벤트를 생성합니다.

자세한 내용은 다음 지식 기반(KB) 문서를 참조하세요. "[Active IQ Unified Manager 에서 AIQCA Secure 규칙을 수동으로 업데이트하는 방법](#)".

Active IQ 플랫폼 이벤트가 생성되는 방식

Active IQ 플랫폼 인시던트와 위험은 다음 다이어그램에 표시된 대로 Unified Manager 이벤트로 변환됩니다.

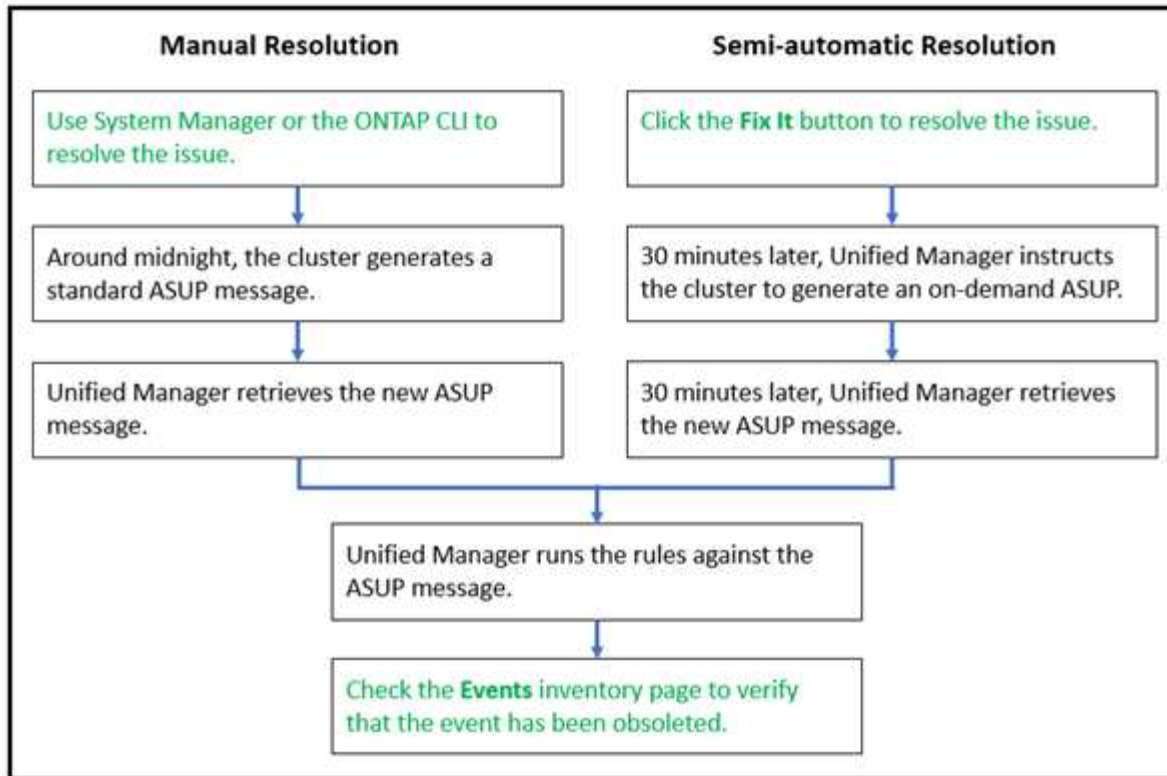


보시다시피, Active IQ 플랫폼에 컴파일된 규칙 파일은 최신 상태로 유지되고, 클러스터 AutoSupport 메시지는 매일 생성되며, Unified Manager는 매일 이벤트 목록을 업데이트합니다.

Active IQ 플랫폼 이벤트 해결

Active IQ 플랫폼 사고와 위험은 다른 Unified Manager 이벤트와 비슷합니다. 다른 사용자에게 할당하여 해결할 수 있고 사용 가능한 상태도 동일하기 때문입니다. 하지만 수정 버튼을 사용하여 이러한 유형의 이벤트를 해결하면 몇 시간 내에 해결 여부를 확인할 수 있습니다.

다음 다이어그램은 Active IQ 플랫폼에서 생성된 이벤트를 해결할 때 수행해야 하는 작업(녹색)과 Unified Manager가 수행하는 작업(검은색)을 보여줍니다.



수동 해결을 수행하는 경우 문제를 해결하려면 시스템 관리자나 ONTAP 명령줄 인터페이스에 로그인해야 합니다. 클러스터가 자정에 새로운 AutoSupport 메시지를 생성한 후에만 문제를 확인할 수 있습니다.

수정 버튼을 사용하여 반자동 해결을 수행하면 몇 시간 내에 문제가 성공적으로 해결되었는지 확인할 수 있습니다.

이벤트 보존 설정 구성

이벤트가 자동으로 삭제되기 전까지 Unified Manager 서버에 보관되는 개월 수를 지정할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

이벤트를 6개월 이상 보관하면 서버 성능에 영향을 줄 수 있으므로 권장하지 않습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *데이터 보존*을 클릭합니다.
2. 데이터 보존 페이지에서 이벤트 보존 영역의 슬라이더를 선택하고 이벤트를 보존해야 하는 개월 수로 이동한 후 *저장*을 클릭합니다.

Unified Manager 유지 관리 기간이란 무엇입니까?

클러스터 유지 관리를 예약한 경우 특정 기간 동안 이벤트와 알림을 억제하고 원치 않는 알림이 폭주하는 것을 방지하려면 Unified Manager 유지 관리 기간을 정의합니다.

유지 관리 창이 시작되면 "객체 유지 관리 창이 시작됨" 이벤트가 이벤트 관리 인벤토리 페이지에 게시됩니다. 이 이벤트는 유지 관리 기간이 종료되면 자동으로 종료됩니다.

유지 관리 기간 동안 해당 클러스터의 모든 개체와 관련된 이벤트는 계속 생성되지만, UI 페이지에는 나타나지 않으며, 이러한 이벤트에 대한 경고나 기타 유형의 알림은 전송되지 않습니다. 그러나 이벤트 관리 인벤토리 페이지에서 보기 옵션 중 하나를 선택하면 유지 관리 기간 동안 모든 저장소 개체에 대해 생성된 이벤트를 볼 수 있습니다.

나중에 시작될 유지 관리 기간을 예약할 수 있으며, 예약된 유지 관리 기간의 시작 및 종료 시간을 변경할 수 있으며, 예약된 유지 관리 기간을 취소할 수 있습니다.

클러스터 이벤트 알림을 비활성화하기 위한 유지 관리 기간 예약

예를 들어 클러스터를 업그레이드하거나 노드 중 하나를 이동하는 등 클러스터에 대한 가동 중지 시간이 계획된 경우 Unified Manager 유지 관리 기간을 예약하면 일반적으로 해당 기간 동안 생성되는 이벤트와 알림을 억제할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

유지 관리 기간 동안 해당 클러스터의 모든 개체와 관련된 이벤트는 계속 생성되지만 이벤트 페이지에는 나타나지 않으며 이러한 이벤트에 대한 경고나 기타 유형의 알림은 전송되지 않습니다.

유지 관리 기간에 입력한 시간은 Unified Manager 서버의 시간을 기준으로 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *클러스터 설정*을 클릭합니다.
2. 클러스터의 유지 관리 모드 열에서 슬라이더 버튼을 선택하고 오른쪽으로 이동합니다.

달력 창이 표시됩니다.

3. 유지 관리 기간의 시작 및 종료 날짜와 시간을 선택하고 *적용*을 클릭합니다.

슬라이더 버튼 옆에 "예약됨"이라는 메시지가 나타납니다.

시작 시간에 도달하면 클러스터가 유지 관리 모드로 전환되고 "개체 유지 관리 창 시작" 이벤트가 생성됩니다.

예약된 유지 관리 기간을 변경하거나 취소합니다.

Unified Manager 유지 관리 기간이 미래에 발생하도록 구성한 경우 시작 및 종료 시간을 변경하거나 유지 관리 기간이 발생하지 않도록 취소할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

예약된 유지 관리 기간 종료 시간 전에 클러스터 유지 관리를 완료하고 클러스터에서 이벤트와 알림을 다시 받으려는 경우 현재 실행 중인 유지 관리 기간을 취소하는 것이 유용합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *클러스터 설정*을 클릭합니다.
2. 클러스터의 유지 관리 모드 열에서:

만약 당신이 원한다면...	이 단계를 수행하세요...
예약된 유지 관리 기간의 시간 프레임 변경	a. 슬라이더 버튼 옆에 있는 "예약됨"이라는 텍스트를 클릭합니다. b. 시작 및/또는 종료 날짜와 시간을 변경하고 *적용*을 클릭합니다.
활성 유지 관리 기간의 길이를 연장합니다.	a. 슬라이더 버튼 옆에 있는 "활성"이라는 텍스트를 클릭하세요. b. 종료 날짜와 시간을 변경하고 *적용*을 클릭하세요.
예약된 유지 관리 기간 취소	슬라이더 버튼을 선택하여 왼쪽으로 이동하세요.
활성 유지 관리 창 취소	슬라이더 버튼을 선택하여 왼쪽으로 이동하세요.

유지 관리 기간 동안 발생한 이벤트 보기

필요한 경우 Unified Manager 유지 관리 기간 동안 모든 저장소 개체에 대해 생성된 이벤트를 볼 수 있습니다. 대부분의 이벤트는 유지 관리 기간이 완료되고 모든 시스템 리소스가 다시 백업되어 실행되면 사용되지 않음 상태로 표시됩니다.

시작하기 전에

이벤트를 사용하려면 최소한 하나의 유지 관리 기간이 완료되어야 합니다.

유지 관리 기간 동안 발생한 이벤트는 기본적으로 이벤트 관리 인벤토리 페이지에 나타나지 않습니다.

단계

1. 왼쪽 탐색 창에서 *이벤트*를 클릭합니다.

기본적으로 모든 활성 이벤트(새 이벤트 및 확인된 이벤트)는 이벤트 관리 인벤토리 페이지에 표시됩니다.

2. 보기 창에서 유지 관리 중에 생성된 모든 이벤트 옵션을 선택합니다.

지난 7일 동안 모든 유지 관리 창 세션과 모든 클러스터에서 발생한 이벤트 목록이 표시됩니다.

3. 단일 클러스터에 대해 여러 유지 관리 기간이 있는 경우 트리거된 시간 달력 아이콘을 클릭하고 보고 싶은 유지 관리 기간 이벤트의 기간을 선택할 수 있습니다.

호스트 시스템 리소스 이벤트 관리

Unified Manager에는 Unified Manager가 설치된 호스트 시스템의 리소스 문제를 모니터링하는 서비스가 포함되어 있습니다. 사용 가능한 디스크 공간 부족이나 호스트 시스템의 메모리 부족 등의 문제로 인해 UI 상단에 배너 메시지로 표시되는 관리 스테이션 이벤트가 발생할 수 있습니다.

관리 스테이션 이벤트는 Unified Manager가 설치된 호스트 시스템에 문제가 있음을 나타냅니다. 관리 스테이션 문제의

예로는 호스트 시스템의 디스크 공간이 부족한 경우, Unified Manager에서 정기적인 데이터 수집 주기가 누락된 경우, 다음 수집 폴링이 시작되어 통계 분석이 완료되지 않거나 늦게 완료되는 경우 등이 있습니다.

다른 모든 Unified Manager 이벤트 메시지와 달리 이러한 특정 관리 스테이션 경고 및 중요 이벤트는 배너 메시지에 표시됩니다.

단계

1. 관리 스테이션 이벤트 정보를 보려면 다음 작업을 수행하세요.

만약 당신이 원한다면...	이렇게 하세요...
이벤트 세부 정보 보기	이벤트 배너를 클릭하면 해당 문제에 대한 제안된 해결책이 포함된 이벤트 세부 정보 페이지가 표시됩니다.
모든 관리 스테이션 이벤트 보기	a. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭합니다. b. 이벤트 관리 인벤토리 페이지의 필터 창에서 소스 유형 목록의 관리 스테이션에 대한 상자를 클릭합니다.

이벤트에 대해 더 자세히 알아보세요

이벤트에 대한 개념을 이해하면 클러스터와 클러스터 객체를 효율적으로 관리하고 알림을 적절하게 정의하는 데 도움이 됩니다.

이벤트 상태 정의

이벤트 상태는 적절한 시정 조치가 필요한지 여부를 식별하는 데 도움이 됩니다. 이벤트는 새 이벤트, 확인 이벤트, 해결 이벤트 또는 폐기 이벤트일 수 있습니다. 새 이벤트와 확인된 이벤트는 모두 활성 이벤트로 간주됩니다.

이벤트 상태는 다음과 같습니다.

- 새로운

새로운 이벤트의 상태.

- 확인

당신이 사건을 인정했을 때의 사건의 상태.

- 해결됨

이벤트가 해결됨으로 표시될 때의 상태입니다.

- 폐기됨

이벤트가 자동으로 수정되거나 이벤트의 원인이 더 이상 유효하지 않은 상태입니다.



더 이상 발생하지 않는 이벤트는 확인하거나 해결할 수 없습니다.

이벤트의 다양한 상태의 예

다음 예에서는 수동 및 자동 이벤트 상태 변경을 설명합니다.

클러스터에 도달할 수 없음 이벤트가 발생하면 이벤트 상태는 새로 만들기입니다. 이벤트를 확인하면 이벤트 상태가 확인됨으로 변경됩니다. 적절한 시정 조치를 취한 후에는 해당 이벤트를 해결됨으로 표시해야 합니다. 그러면 이벤트 상태가 해결됨으로 변경됩니다.

정전으로 인해 클러스터에 접근할 수 없음 이벤트가 발생한 경우 전원이 복구되면 관리자의 개입 없이 클러스터가 작동을 시작합니다. 따라서 클러스터에 도달할 수 없음 이벤트는 더 이상 유효하지 않으며, 이벤트 상태는 다음 모니터링 주기에서 사용되지 않음으로 변경됩니다.

Unified Manager는 이벤트가 '폐기됨' 또는 '해결됨' 상태가 되면 알림을 보냅니다. 알림의 이메일 제목과 이메일 내용은 이벤트 상태에 대한 정보를 제공합니다. SNMP 트랩에는 이벤트 상태에 대한 정보도 포함되어 있습니다.

이벤트 심각도 유형에 대한 설명

각 이벤트는 심각도 유형과 연결되어 있어 즉각적인 시정 조치가 필요한 이벤트의 우선순위를 지정하는 데 도움이 됩니다.

• 비판적인

즉각적인 시정 조치를 취하지 않으면 서비스 중단으로 이어질 수 있는 문제가 발생했습니다.

성능이 중요한 이벤트는 사용자가 정의한 임계값에서만 전송됩니다.

• 오류

이벤트 소스는 여전히 수행되고 있습니다. 그러나 서비스 중단을 방지하기 위해 시정 조치가 필요합니다.

• 경고

이벤트 소스에서 사용자가 알아야 할 사건이 발생했거나, 클러스터 개체에 대한 성능 카운터가 정상 범위를 벗어났으며, 심각한 심각도에 도달하지 않도록 모니터링해야 합니다. 이 정도 심각도의 사건은 서비스 중단을 일으키지 않으며, 즉각적인 시정 조치가 필요하지 않을 수도 있습니다.

성능 경고 이벤트는 사용자 정의, 시스템 정의 또는 동적 임계값에서 전송됩니다.

• 정보

이 이벤트는 새로운 객체가 발견되거나 사용자 작업이 수행될 때 발생합니다. 예를 들어, 저장소 개체가 삭제되거나 구성이 변경되면 심각도 유형이 정보인 이벤트가 생성됩니다.

ONTAP 구성 변경을 감지하면 정보 이벤트를 직접 전송합니다.

이벤트 영향 수준 설명

각 이벤트는 영향 수준(사고, 위험, 이벤트 또는 업그레이드)과 연결되어 있어 즉각적인 시정

조치가 필요한 이벤트의 우선 순위를 지정하는 데 도움이 됩니다.

- 사건

사고는 클러스터가 클라이언트에 데이터 제공을 중단하고 데이터를 저장할 공간이 부족하게 만드는 일련의 이벤트입니다. 영향 수준이 '사건'인 이벤트가 가장 심각합니다. 서비스 중단을 방지하기 위해 즉각적인 시정 조치를 취해야 합니다.

- 위험

위험은 클러스터가 클라이언트에 데이터 제공을 중단하고 데이터를 저장할 공간이 부족해질 수 있는 일련의 이벤트입니다. 위험 수준의 영향이 있는 이벤트는 서비스 중단을 초래할 수 있습니다. 시정 조치가 필요할 수도 있습니다.

- 이벤트

이벤트는 저장 객체와 해당 속성의 상태 또는 상태 변화입니다. 영향 수준이 '이벤트'인 이벤트는 정보 제공용이며 시정 조치가 필요하지 않습니다.

- 치받이

업그레이드 이벤트는 Active IQ 플랫폼에서 보고되는 특정 유형의 이벤트입니다. 이러한 이벤트는 보안 권고에 따라 ONTAP 소프트웨어, 노드 펌웨어 또는 운영 체제 소프트웨어를 업그레이드해야 하는 문제를 식별합니다. 일부 문제는 즉시 시정 조치를 취해야 할 수도 있지만, 다른 문제는 다음에 예정된 유지 관리까지 기다릴 수 있습니다.

이벤트 영향 영역 설명

이벤트는 가용성, 용량, 구성, 성능, 보호, 보안의 6가지 영향 영역으로 분류되어 담당하는 이벤트 유형에 집중할 수 있습니다.

- 유효성

가용성 이벤트는 스토리지 개체가 오프라인 상태가 되거나, 프로토콜 서비스가 중단되거나, 스토리지 장애 조치에 문제가 발생하거나, 하드웨어에 문제가 발생하는 경우 알려줍니다.

- 용량

용량 이벤트는 집계, 볼륨, LUN 또는 네임스페이스가 크기 임계값에 접근하거나 도달한 경우 또는 사용자 환경에서 증가 속도가 비정상적일 경우 알려줍니다.

- 구성

구성 이벤트는 스토리지 개체의 검색, 삭제, 추가, 제거 또는 이름 변경에 대한 정보를 제공합니다. 구성 이벤트에는 이벤트의 영향 수준과 정보의 심각도 유형이 있습니다.

- 성능

성능 이벤트는 모니터링되는 스토리지 개체에서 데이터 스토리지 입력 또는 검색 속도에 부정적인 영향을 미칠 수 있는 클러스터의 리소스, 구성 또는 활동 조건을 알려줍니다.

- 보호

보호 이벤트는 SnapMirror 관계, 대상 용량 문제, SnapVault 관계 문제 또는 보호 작업 문제와 관련된 사고나 위험을 알려줍니다. 보조 볼륨과 보호 관계를 호스팅하는 모든 ONTAP 객체(특히 집계, 볼륨, SVM)는 보호 영향 영역에 분류됩니다.

- 보안

보안 이벤트는 ONTAP 클러스터, 스토리지 가상 머신(SVM) 및 볼륨이 정의된 매개변수를 기반으로 얼마나 안전한지 알려줍니다. ["ONTAP 9를 위한 NetApp 보안 강화 가이드"](#).

또한 이 영역에는 Active IQ 플랫폼에서 보고된 업그레이드 이벤트가 포함됩니다.

객체 상태가 계산되는 방식

객체 상태는 현재 새롭거나 확인된 상태를 유지하는 가장 심각한 이벤트에 따라 결정됩니다. 예를 들어, 객체 상태가 오류인 경우 해당 객체의 이벤트 중 하나의 심각도 유형은 오류입니다. 시정 조치가 취해지면 이벤트 상태가 해결됨으로 변경됩니다.

동적 성능 이벤트 차트 세부 정보

동적 성능 이벤트의 경우 이벤트 세부 정보 페이지의 시스템 진단 섹션에는 경쟁 중인 클러스터 구성 요소의 대기 시간이나 사용량이 가장 높은 상위 워크로드가 나열됩니다.

성능 통계는 성능 이벤트가 감지된 시간부터 이벤트가 마지막으로 분석된 시간까지의 시간을 기준으로 합니다. 차트에는 경쟁 중인 클러스터 구성 요소에 대한 과거 성능 통계도 표시됩니다.

예를 들어, 구성 요소의 활용도가 높은 워크로드를 식별하여 활용도가 낮은 구성 요소로 어떤 워크로드를 옮겨야 할지 결정할 수 있습니다. 작업 부하를 이동하면 현재 구성 요소의 작업량이 줄어들어 해당 구성 요소가 경쟁에서 벗어날 수 있습니다. 이 섹션의 맨 위에는 이벤트가 감지되어 마지막으로 분석된 시간과 날짜 범위가 표시됩니다. 활성 이벤트(새 이벤트 또는 확인된 이벤트)의 경우 마지막으로 분석된 시간이 업데이트됩니다.

대기 시간 및 활동 차트에는 차트 위에 커서를 올려 놓으면 가장 많은 작업 부하의 이름이 표시됩니다. 차트 오른쪽에 있는 작업 유형 메뉴를 클릭하면 이벤트에서의 역할(상어, 괴롭힘, 피해자 등)에 따라 작업 부하를 정렬할 수 있으며, 경쟁 중인 클러스터 구성 요소에서의 대기 시간과 사용량에 대한 세부 정보가 표시됩니다. 실제 값과 예상 값을 비교하면 작업 부하가 예상 대기 시간 또는 사용량 범위를 벗어난 경우를 확인할 수 있습니다. 자세한 내용은 다음을 참조하세요. ["Unified Manager에서 모니터링하는 작업 유형"](#).



대기 시간의 최대 편차를 기준으로 정렬할 경우 시스템에서 정의한 작업 부하가 표에 표시되지 않습니다. 대기 시간은 사용자 정의 작업 부하에만 적용되기 때문입니다. 대기 시간 값이 매우 낮은 작업 부하는 표에 표시되지 않습니다.

동적 성능 임계값에 대한 자세한 내용은 다음을 참조하세요. ["동적 성능 임계값에서 이벤트 분석"](#).

Unified Manager가 작업 부하를 순위 지정하고 정렬 순서를 결정하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["Unified Manager가 이벤트의 성능 영향을 결정하는 방법"](#).

그래프의 데이터는 이벤트가 마지막으로 분석되기 전 24시간 동안의 성능 통계를 보여줍니다. 각 워크로드에 대한 실제 값과 예상 값은 워크로드가 이벤트에 관련된 시간을 기준으로 합니다. 예를 들어, 이벤트가 감지된 후에 워크로드가 이벤트에 관련될 수 있으므로, 해당 워크로드의 성능 통계가 이벤트 감지 시점의 값과 일치하지 않을 수 있습니다. 기본적으로 작업 부하는 지연 시간의 최대(가장 높은) 편차를 기준으로 정렬됩니다.



Unified Manager는 최대 30일 동안 5분 단위의 과거 성능 및 이벤트 데이터를 보관하므로 이벤트가 30일을 넘으면 성능 데이터가 표시되지 않습니다.

- 작업량 정렬 열

- 지연 차트

마지막 분석 시 워크로드 지연에 대한 이벤트의 영향을 표시합니다.

- 구성요소 사용 열

경합 중인 클러스터 구성 요소의 작업 부하 사용에 대한 세부 정보를 표시합니다. 그래프에서 실제 사용량은 파란색 선으로 표시됩니다. 빨간색 막대는 감지 시간부터 마지막 분석 시간까지의 이벤트 기간을 강조 표시합니다. 자세한 내용은 다음을 참조하세요. "[작업 부하 성능 측정 값](#)".



네트워크 구성 요소의 경우 네트워크 성능 통계가 클러스터 외부 활동에서 나오므로 이 열은 표시되지 않습니다.

- 구성요소 사용

네트워크 처리, 데이터 처리 및 집계 구성 요소에 대한 활용 내역(백분율)이나 QoS 정책 그룹 구성 요소에 대한 활동 내역(백분율)을 표시합니다. 네트워크 또는 상호 연결 구성 요소에 대한 차트는 표시되지 않습니다. 특정 시점의 사용 통계를 보려면 통계를 가리킬 수 있습니다.

- 총 쓰기 **MB/s** 기록

MetroCluster 리소스 구성 요소에만 해당하며, MetroCluster 구성에서 파트너 클러스터에 미러링되는 모든 볼륨 작업 부하에 대한 총 쓰기 처리량을 초당 메가바이트(MBps) 단위로 표시합니다.

- 이벤트 내역

경쟁 중인 구성 요소의 이전 이벤트를 나타내기 위해 빨간색 음영 처리된 선을 표시합니다. 더 이상 발생하지 않은 이벤트의 경우, 차트에는 선택한 이벤트가 감지되기 전과 해결된 후에 발생한 이벤트가 표시됩니다.

Unified Manager에서 감지된 구성 변경 사항

Unified Manager는 클러스터의 구성 변경 사항을 모니터링하여 변경 사항이 성능 이벤트를 발생시키거나 성능 이벤트에 영향을 미쳤는지 확인하는 데 도움을 줍니다. 성능 탐색기 페이지에는 변경 이벤트 아이콘(●) 변경 사항이 감지된 날짜와 시간을 나타냅니다.

성능 탐색기 페이지와 워크로드 분석 페이지에서 성능 차트를 검토하여 변경 이벤트가 선택한 클러스터 개체의 성능에 영향을 미쳤는지 확인할 수 있습니다. 변경 사항이 성능 이벤트와 동시에 또는 거의 동시에 감지된 경우, 해당 변경 사항이 문제에 영향을 미쳐 이벤트 알림이 트리거되었을 수 있습니다.

Unified Manager는 정보 이벤트로 분류되는 다음과 같은 변경 이벤트를 감지할 수 있습니다.

- 볼륨은 집합체 사이를 이동합니다.

Unified Manager는 이동이 진행 중이거나 완료되었거나 실패한 경우를 감지할 수 있습니다. 볼륨 이동 중에 Unified Manager가 다운되더라도 다시 작동하면 볼륨 이동을 감지하고 해당 변경 이벤트를 표시합니다.

- 하나 이상의 모니터링되는 작업 부하가 포함된 QoS 정책 그룹의 처리량(MB/s 또는 IOPS) 제한이 변경됩니다.

정책 그룹 제한을 변경하면 지연 시간(응답 시간)이 간헐적으로 급증할 수 있으며, 이로 인해 정책 그룹에 대한 이벤트가 트리거될 수도 있습니다. 지연 시간은 점차 정상으로 돌아오고, 급증으로 인해 발생한 모든 이벤트는 더 이상 발생하지 않습니다.

- HA 쌍의 노드는 파트너 노드의 저장소를 인수하거나 반환해줍니다.

Unified Manager는 인수, 부분 인수 또는 반환 작업이 완료되는 시점을 감지할 수 있습니다. 인수가 패닉 상태의 노드로 인해 발생하는 경우 Unified Manager는 이벤트를 감지하지 못합니다.

- ONTAP 업그레이드 또는 되돌리기 작업이 성공적으로 완료되었습니다.

이전 버전과 새 버전이 표시됩니다.

이벤트 및 심각도 유형 목록

이벤트 목록을 사용하면 Unified Manager에서 볼 수 있는 각 이벤트의 이벤트 범주, 이벤트 이름 및 심각도 유형을 더 잘 알 수 있습니다. 이벤트는 객체 범주별로 알파벳순으로 나열됩니다.

이벤트 집계

집계 이벤트는 집계 상태에 대한 정보를 제공하므로 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 식별합니다.

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
오프라인 집계(ocumEvtAggregateStateOffline)	사건	골재	비판적인
집계 실패(ocumEvtAggregateStateFailed)	사건	골재	비판적인
제한된 집계(ocumEvtAggregateStateRestricted)	위험	골재	경고
집계 재구성(ocumEvtAggregateRaidStateReconstructing)	위험	골재	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
집계 저하(ocumEvtAggregateRaidStateDegraded)	위험	골재	경고
클라우드 계층 부분 도달 가능(ocumEventCloudTierPartiallyReachable)	위험	골재	경고
클라우드 계층에 도달할 수 없음(ocumEventCloudTierUnreachable)	위험	골재	오류
집계 재배치에 대한 클라우드 계층 액세스 거부 *(arlNetraCaCheckFailed)	위험	골재	오류
스토리지 장애 조치 중 집계 재배치에 대한 클라우드 계층 액세스 거부 *(gbNetraCaCheckFailed)	위험	골재	오류
MetroCluster 집계 남겨짐(ocumEvtMetroClusterAggregateLeftBehind)	위험	골재	오류
MetroCluster 집계 미러링 저하(ocumEvtMetroClusterAggregateMirrorDegraded)	위험	골재	오류

영향 영역: 용량

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
집계 공간 거의 가득 참(ocumEvtAggregateNearlyFull)	위험	골재	경고
집계 공간 가득 참(ocumEvtAggregateFull)	위험	골재	오류
만기까지 집계 일수(ocumEvtAggregateDaysUntilFullSoon)	위험	골재	오류

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
집계 초과 커밋(ocumEvtAggregateOvercommitted)	위험	골재	오류
집계 거의 초과 커밋(ocumEvtAggregateAlmostOvercommitted)	위험	골재	경고
집계 스냅샷 예약 가득 참(ocumEvtAggregateSnapshotReserveFull)	위험	골재	경고
집계 성장률 비정상(ocumEvtAggregateGrowthRateAbnormal)	위험	골재	경고

영향 영역: 구성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
발견된 집계(해당 없음)	이벤트	골재	정보
집계 이름 변경됨(해당 없음)	이벤트	골재	정보
집계 삭제됨(해당 없음)	이벤트	마디	정보

영향 영역: 성능

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
집계 IOPS 중요 임계값 위반(ocumAggregateIopsIncident)	사건	골재	비판적인
집계 IOPS 경고 임계값 위반(ocumAggregateIopsWarning)	위험	골재	경고
집계 MB/s 중요 임계값 위반(ocumAggregateMbpsIncident)	사건	골재	비판적인
집계 MB/s 경고 임계값 위반(ocumAggregateMbpsWarning)	위험	골재	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
집계 대기 시간 중요 임계값 위반(ocumAggregateLatenessIncident)	사건	골재	비판적인
집계 지연 경고 임계값 위반(ocumAggregateLatenessWarning)	위험	골재	경고
집계 성능 용량 사용 중요 임계값 위반(ocumAggregatePerfCapacityUsedIncident)	사건	골재	비판적인
집계 성능 용량 사용 경고 임계값 위반(ocumAggregatePerfCapacityUsedWarning)	위험	골재	경고
집계 활용도 중요 임계값 위반(ocumAggregateUtilizationIncident)	사건	골재	비판적인
집계 사용률 경고 임계값 위반(ocumAggregateUtilizationWarning)	위험	골재	경고
집계 디스크 과다 사용 임계값 위반(ocumAggregateDisksOverUtilizedWarning)	위험	골재	경고
집계 동적 임계값 위반(ocumAggregateDynamicEventWarning)	위험	골재	경고

클러스터 이벤트

클러스터 이벤트는 클러스터 상태에 대한 정보를 제공하므로 클러스터를 모니터링하여 잠재적인 문제를 파악할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 이름, 트랩 이름, 영향 수준, 소스 유형 및 심각도가 포함됩니다.

영향 영역: 가용성

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 식별합니다.

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
클러스터에 예비 디스크가 없습니다(ocumEvtDisksNoSpares)	위험	무리	경고
클러스터에 도달할 수 없음(ocumEvtClusterUnreachable)	위험	무리	오류
클러스터 모니터링 실패(ocumEvtClusterMonitoringFailed)	위험	무리	경고
클러스터 FabricPool 라이선스 용량 제한 위반(ocumEvtExternalCapacityTierSpaceFull)	위험	무리	경고
NVMe-oF 유예 기간 시작*(nvmfGracePeriodStart)	위험	무리	경고
NVMe-oF 유예 기간 활성화*(nvmfGracePeriodActive)	위험	무리	경고
NVMe-oF 유예 기간 만료*(nvmfGracePeriodExpired)	위험	무리	경고
객체 유지 관리 창 시작됨(objectMaintenanceWindowStarted)	이벤트	무리	비판적인
객체 유지 관리 기간이 종료되었습니다(objectMaintenanceWindowEnded)	이벤트	무리	정보
MetroCluster 남은 스페어 디스크(ocumEvtSpareDiskLeftBehind)	위험	무리	오류
MetroCluster 자동 계획되지 않은 전환 비활성화(ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	위험	무리	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
클러스터 사용자 비밀번호가 변경되었습니다. *(cluster.passwd.changed)	이벤트	무리	정보

영향 영역: 용량

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
클러스터 용량 불균형 임계값 위반(ocumConformanceNodeImbalanceWarning)	위험	무리	경고
클러스터 클라우드 계층 계획(clusterCloudTierPlanningWarning)	위험	무리	경고
FabricPool 미러 복제 재동기화 완료 *(wafCaResyncComplete)	이벤트	무리	경고
FabricPool 공간이 거의 가득 찹습니다 *(fabricpoolNearlyFull)	위험	무리	오류

영향 영역: 구성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
노드 추가됨(해당 없음)	이벤트	무리	정보
노드 제거됨(해당 없음)	이벤트	무리	정보
클러스터 제거됨(해당 없음)	이벤트	무리	정보
클러스터 추가 실패(해당 없음)	이벤트	무리	오류
클러스터 이름이 변경되었습니다(해당 없음)	이벤트	무리	정보
긴급 EMS 수신 (해당 없음)	이벤트	무리	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
중요 EMS 수신됨(해당 없음)	이벤트	무리	비판적인
EMS 알림 수신됨(해당 없음)	이벤트	무리	오류
EMS 수신 오류 (해당 없음)	이벤트	무리	경고
경고 EMS 수신됨 (해당 없음)	이벤트	무리	경고
디버그 EMS 수신됨(해당 없음)	이벤트	무리	경고
EMS 수신 알림 (해당 없음)	이벤트	무리	경고
정보 EMS 수신됨(해당 없음)	이벤트	무리	경고

ONTAP EMS 이벤트는 세 가지 Unified Manager 이벤트 심각도 수준으로 분류됩니다.

Unified Manager 이벤트 심각도 수준	ONTAP EMS 이벤트 심각도 수준
비판적인	비상 비판적인
오류	알리다
경고	오류 경고 디버그 알아채다 정보 제공

영향 영역: 성능

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
클러스터 부하 불균형 임계값 위반()	위험	무리	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
클러스터 IOPS 중요 임계값 위반(ocumClusterIopsIncident)	사건	무리	비판적인
클러스터 IOPS 경고 임계값 위반(ocumClusterIopsWarning)	위험	무리	경고
클러스터 MB/s 중요 임계값 위반(ocumClusterMbpsIncident)	사건	무리	비판적인
클러스터 MB/s 경고 임계값 위반(ocumClusterMbpsWarning)	위험	무리	경고
클러스터 동적 임계값 위반(ocumClusterDynamicEventWarning)	위험	무리	경고

영향 영역: 보안

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
AutoSupport HTTPS 전송 비활성화(ocumClusterASUPHhttpsConfiguredDisabled)	위험	무리	경고
로그 전달이 암호화되지 않음(ocumClusterAuditLogUnencrypted)	위험	무리	경고
기본 로컬 관리자 사용자 활성화(ocumClusterDefaultAdminEnabled)	위험	무리	경고
FIPS 모드 비활성화(ocumClusterFipsDisabled)	위험	무리	경고
로그인 배너 비활성화(ocumClusterLoginBannerDisabled)	위험	무리	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
로그인 배너가 변경되었습니다(ocumClusterLoginBannerChanged)	위험	무리	경고
로그 전달 대상 변경됨(ocumLogForwardDestinationsChanged)	위험	무리	경고
NTP 서버 이름이 변경되었습니다(ocumNtpServerNamesChanged)	위험	무리	경고
NTP 서버 수가 적습니다(securityConfigNTPServerCountLowRisk)	위험	무리	경고
클러스터 피어 통신이 암호화되지 않았습니다(ocumClusterPeerEncryptionDisabled)	위험	무리	경고
SSH가 안전하지 않은 암호를 사용하고 있습니다(ocumClusterSSHInsecure)	위험	무리	경고
Telnet 프로토콜 활성화(ocumClusterTelnetEnabled)	위험	무리	경고
일부 ONTAP 사용자 계정의 비밀번호는 보안 수준이 낮은 MD5 해시 함수(ocumClusterMD5PasswordHashUsed)를 사용합니다.	위험	무리	경고
클러스터는 자체 서명 인증서(ocumClusterSelfSignedCertificate)를 사용합니다.	위험	무리	경고
클러스터 원격 셸이 활성화되었습니다(ocumClusterRshDisabled)	위험	무리	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
클러스터 인증서 만료 임박(ocumEvtClusterCertificateAboutToExpire)	위험	무리	경고
클러스터 인증서가 만료되었습니다(ocumEvtClusterCertificateExpired)	위험	무리	오류

디스크 이벤트

디스크 이벤트는 디스크 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 도와줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
플래시 디스크 - 예비 블록이 거의 소모됨(ocumEvtClusterFlashDiskFewerSpareBlockError)	위험	무리	오류
플래시 디스크 - 예비 블록 없음(ocumEvtClusterFlashDiskNoSpareBlockCritical)	사건	무리	비판적인
일부 할당되지 않은 디스크(ocumEvtClusterUnassignedDisksSome)	위험	무리	경고
일부 실패한 디스크(ocumEvtDisksSomeFailed)	사건	무리	비판적인

인클로저 이벤트

인클로저 이벤트는 데이터 센터의 디스크 셸프 인클로저 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 해줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
디스크 쉘프 팬 고장(ocumEvtShelfFanFailed)	사건	보관 선반	비판적인
디스크 쉘프 전원 공급 장치 실패(ocumEvtShelfPowerSupplyFailed)	사건	보관 선반	비판적인
디스크 쉘프 멀티패스가 구성되지 않았습니다(ocumDiskShelfConnectivityNotInMultiPath) 이 이벤트는 다음에는 적용되지 않습니다. • MetroCluster 구성에 있는 클러스터 • 다음 플랫폼: FAS2554, FAS2552, FAS2520 및 FAS2240	위험	마디	경고
디스크 쉘프 경로 오류(ocumDiskShelfConnectivityPathFailure)	위험	보관 선반	경고

영향 영역: 구성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
디스크 쉘프가 발견되었습니다(해당 없음)	이벤트	마디	정보
디스크 선반 제거됨(해당 없음)	이벤트	마디	정보

팬 이벤트

팬 이벤트는 데이터 센터의 노드에 있는 팬의 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 해줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
하나 이상의 실패한 팬(ocumEvtFansOneOrMoreFailed)	사건	마디	비판적인

플래시카드 이벤트

플래시 카드 이벤트는 데이터 센터의 노드에 설치된 플래시 카드의 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 해줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
플래시 카드 오프라인(ocumEvtFlashCardOffline)	사건	마디	비판적인

Inode 이벤트

Inode 이벤트는 Inode가 가득 찼거나 거의 가득 찼을 때 정보를 제공하므로 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 용량

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
Inode가 거의 가득 참(ocumEvtInodesAlmost Full)	위험	용량	경고
Inode Full(ocumEvtInodesFull)	위험	용량	오류

네트워크 인터페이스(LIF) 이벤트

네트워크 인터페이스 이벤트는 네트워크 인터페이스(LIF) 상태에 대한 정보를 제공하므로 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
네트워크 인터페이스 상태 다운(ocumEvtLifStatusDo wn)	위험	인터페이스	오류
FC/FCoE 네트워크 인터페이스 상태 다운(ocumEvtFCLifStatus Down)	위험	인터페이스	오류
네트워크 인터페이스 장애 조치가 불가능합니다(ocumEvtLifF ailoverNotPossible)	위험	인터페이스	경고
네트워크 인터페이스가 홈 포트에 없음(ocumEvtLifNotAtHo mePort)	위험	인터페이스	경고

영향 영역: 구성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
네트워크 인터페이스 경로가 구성되지 않았습니다(해당 없음)	이벤트	인터페이스	정보

영향 영역: 성능

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
네트워크 인터페이스 MB/s 위험 임계값 위반(ocumNetworkLifMbps sIncident)	사건	인터페이스	비판적인
네트워크 인터페이스 MB/s 경고 임계값 위반(ocumNetworkLifMbps sWarning)	위험	인터페이스	경고
FC 네트워크 인터페이스 MB/s 위험 임계값 위반(ocumFcplifMbpsInci dent)	사건	인터페이스	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
FC 네트워크 인터페이스 MB/s 경고 임계값 위반(ocumFcpLifMbpsWarning)	위험	인터페이스	경고
NVMf FC 네트워크 인터페이스 MB/s 중요 임계값 위반(ocumNvmfFcLifMbpsIncident)	사건	인터페이스	비판적인
NVMf FC 네트워크 인터페이스 MB/s 경고 임계값 위반(ocumNvmfFcLifMbpsWarning)	위험	인터페이스	경고

LUN 이벤트

LUN 이벤트는 LUN 상태에 대한 정보를 제공하므로 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 식별합니다.

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
LUN 오프라인(ocumEvtLunOffline)	사건	LUN	비판적인
LUN 파괴됨 *(lunDestroy)	이벤트	LUN	정보
igroup에서 지원되지 않는 운영 체제로 LUN이 매핑되었습니다(igroupUnsupportedOsType)	사건	LUN	경고
LUN에 액세스하기 위한 단일 활성 경로(ocumEvtLunSingleActivePath)	위험	LUN	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
LUN에 액세스할 활성 경로가 없습니다(ocumEvtLunNotReachable)	사건	LUN	비판적인
LUN에 액세스하기 위한 최적화된 경로가 없습니다(ocumEvtLunOptimizedPathInactive)	위험	LUN	경고
HA 파트너에서 LUN에 액세스할 경로가 없습니다(ocumEvtLunHaPathInactive)	위험	LUN	경고
HA 쌍의 한 노드에서 LUN에 액세스할 경로가 없습니다(ocumEvtLunNodePathStatusDown)	위험	LUN	오류

영향 영역: 용량

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
LUN 스냅샷 복사를 위한 공간이 부족합니다(ocumEvtLunSnapshotNotPossible)	위험	용량	경고

영향 영역: 구성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
igroup에서 지원되지 않는 운영 체제로 LUN이 매핑되었습니다(igroupUnsupportedOsType)	위험	LUN	경고

영향 영역: 성능

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
LUN IOPS 위험 임계값 위반(ocumLunIopsIncident)	사건	LUN	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
LUN IOPS 경고 임계값 위반(ocumLunIopsWarning)	위험	LUN	경고
LUN MB/s 중요 임계값 위반(ocumLunMbpsIncident)	사건	LUN	비판적인
LUN MB/s 경고 임계값 위반(ocumLunMbpsWarning)	위험	LUN	경고
LUN 대기 시간(ms/op) 위험 임계값 위반(ocumLunLatencyIncident)	사건	LUN	비판적인
LUN 대기 시간(ms/op) 경고 임계값 위반(ocumLunLatencyWarning)	위험	LUN	경고
LUN 지연 시간 및 IOPS 위험 임계값 위반(ocumLunLatencyIopsIncident)	사건	LUN	비판적인
LUN 지연 시간 및 IOPS 경고 임계값 위반(ocumLunLatencyIopsWarning)	위험	LUN	경고
LUN 지연 시간 및 MB/s 중요 임계값 위반(ocumLunLatencyMbpsIncident)	사건	LUN	비판적인
LUN 지연 시간 및 MB/s 경고 임계값 위반(ocumLunLatencyMbpsWarning)	위험	LUN	경고
LUN 지연 시간 및 집계 성능 사용 용량 중요 임계값 위반(ocumLunLatencyAggregatePerfCapacityUsedIncident)	사건	LUN	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
LUN 지연 시간 및 총 성능 용량 사용 경고 임계값 위반(ocumLunLatencyAgg regatePerfCapacityUsed Warning)	위험	LUN	경고
LUN 지연 시간 및 집계 사용률 중요 임계값 위반(ocumLunLatencyAgg regateUtilizationIncident)	사건	LUN	비판적인
LUN 지연 시간 및 집계 사용률 경고 임계값 위반(ocumLunLatencyAgg regateUtilizationWarning)	위험	LUN	경고
LUN 지연 시간 및 노드 성능 사용 용량 위험 임계값 위반(ocumLunLatencyNod ePerfCapacityUsedIncide nt)	사건	LUN	비판적인
LUN 지연 시간 및 노드 성능 사용 용량 경고 임계값 위반(ocumLunLatencyNod ePerfCapacityUsedWarni ng)	위험	LUN	경고
LUN 지연 시간 및 노드 성능 사용 용량 - 인수 위험 임계값 위반(ocumLunLatencyAgg regatePerfCapacityUsedT akeoverIncident)	사건	LUN	비판적인
LUN 지연 시간 및 노드 성능 사용 용량 - 인수 경고 임계값 위반(ocumLunLatencyAgg regatePerfCapacityUsedT akeoverWarning)	위험	LUN	경고
LUN 지연 시간 및 노드 사용률 위험 임계값 위반(ocumLunLatencyNod eUtilizationIncident)	사건	LUN	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
LUN 지연 시간 및 노드 사용률 경고 임계값 위반(ocumLunLatencyNodeUtilizationWarning)	위험	LUN	경고
QoS LUN 최대 IOPS 경고 임계값 위반(ocumQosLunMaxIopsWarning)	위험	LUN	경고
QoS LUN 최대 MB/s 경고 임계값 위반(ocumQosLunMaxMbpsWarning)	위험	LUN	경고
성능 서비스 수준 정책(ocumConformanceLatencyWarning)에 정의된 대로 워크로드 LUN 대기 시간 임계값이 위반되었습니다.	위험	LUN	경고

관리 스테이션 이벤트

관리 스테이션 이벤트는 Unified Manager가 설치된 서버의 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 해줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 구성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
관리 서버 디스크 공간이 거의 가득 참습니다(ocumEvtUnifiedManagerDiskSpaceNearlyFull)	위험	관리국	경고
관리 서버 디스크 공간 가득 참(ocumEvtUnifiedManagerDiskSpaceFull)	사건	관리국	비판적인
관리 서버 메모리 부족(ocumEvtUnifiedManagerMemoryLow)	위험	관리국	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
관리 서버 메모리가 거의 부족합니다(ocumEvtUnifiedManagerMemoryAlmost Out)	사건	관리국	비판적인
MySQL 로그 파일 크기가 증가했습니다. 재시작이 필요합니다(ocumEvtMysqlLogFileSizeWarning)	사건	관리국	경고
총 감사 로그 크기 할당이 곧 가득 찰 예정입니다.	위험	관리국	경고
Syslog 서버 인증서가 만료됩니다	위험	관리국	경고
Syslog 서버 인증서가 만료되었습니다	위험	관리국	오류
감사 로그 파일이 변조되었습니다.	위험	관리국	경고
감사 로그 파일이 삭제되었습니다.	위험	관리국	경고
Syslog 서버 연결 오류	위험	관리국	오류
Syslog 서버 구성이 변경되었습니다	이벤트	관리국	경고

영향 영역: 성능

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
성능 데이터 분석에 영향이 있습니다(ocumEvtUnifiedManagerDataMissingAnalyze)	위험	관리국	경고
성능 데이터 수집에 영향이 있습니다(ocumEvtUnifiedManagerDataMissingCollection)	사건	관리국	비판적인



마지막 두 가지 성능 이벤트는 Unified Manager 7.2에서만 사용할 수 있습니다. 이러한 이벤트 중 하나가 새 상태에 존재하고 이후 Unified Manager 소프트웨어의 최신 버전으로 업그레이드하면 해당 이벤트는 자동으로 삭제되지 않습니다. 이벤트를 수동으로 해결된 상태로 옮겨야 합니다.

MetroCluster 브리지 이벤트

MetroCluster Bridge 이벤트는 FC 구성을 통한 MetroCluster 에서 잠재적인 문제를 모니터링할 수 있도록 브리지 상태에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
브리지에 접근할 수 없음(ocumEvtBridgeUnreachable)	사건	MetroCluster 브리지	비판적인
브리지 온도 비정상(ocumEvtBridgeTemperatureAbnormal)	사건	MetroCluster 브리지	비판적인

MetroCluster 연결 이벤트

연결 이벤트는 클러스터 구성 요소 간 연결과 FC를 통한 MetroCluster 및 IP 구성을 통한 MetroCluster 의 MetroCluster 간 연결에 대한 정보를 제공하므로 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

두 구성 모두에서 공통적인 이벤트

이러한 연결 이벤트는 FC를 통한 MetroCluster 와 IP를 통한 MetroCluster 구성 모두에서 공통적으로 발생합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
MetroCluster 파트너 간 모든 링크가 다운되었습니다(ocumEvtMetroClusterAllLinksBetweenPartnersDown)	사건	MetroCluster 관계	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
피어링 네트워크를 통해 MetroCluster 파트너에 접근할 수 없음(ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	사건	MetroCluster 관계	비판적인
MetroCluster 재해 복구 기능 영향(ocumEvtMetroClusterDRStatusImpacted)	위험	MetroCluster 관계	비판적인
MetroCluster 구성이 전환되었습니다(ocumEvtMetroClusterDRStatusImpacted)	위험	MetroCluster 관계	경고

FC 구성을 통한 MetroCluster

이러한 이벤트는 FC 구성을 통한 MetroCluster 와 관련이 있습니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
모든 스위치 간 링크 다운(ocumEvtMetroClusterAllISLBetweenSwitchesDown)	사건	MetroCluster 스위치 간 연결	비판적인
FC-SAS 브리지 투 스토리지 스택 링크 다운(ocumEvtBridgeSasPortDown)	사건	MetroCluster 브리지 스택 연결	비판적인
MetroCluster 구성이 부분적으로 전환됨(ocumEvtMetroClusterDRStatusPartiallyImpacted)	위험	MetroCluster 관계	오류
노드에서 FC로의 모든 FC-VI 상호 연결 링크 차단(ocumEvtMccNodeSwitchFcviLinksDown)	사건	MetroCluster 노드 스위치 연결	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
노드에서 FC로 전환 하나 이상의 FC-Initiator 링크 다운(ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	위험	MetroCluster 노드 스위치 연결	경고
노드에서 FC로 모든 FC 이니시에이터 링크를 전환합니다(ocumEvtMccNodeSwitchFcLinksDown)	사건	MetroCluster 노드 스위치 연결	비판적인
FC-SAS 브리지 FC 링크 다운(ocumEvtMccSwitchBridgeFcLinksDown)으로 전환	사건	MetroCluster 스위치 브리지 연결	비판적인
노드 간 모든 FC VI InterConnect 링크 다운(ocumEvtMccInterNodeLinksDown)	사건	노드 간 연결	비판적인
노드 간 하나 이상의 FC VI InterConnect 링크가 끊어짐(ocumEvtMccInterNodeLinksOneOrMoreDown)	위험	노드 간 연결	경고
노드-브리지 링크 다운(ocumEvtMccNodeBridgeLinksDown)	사건	노드 브리지 연결	비판적인
노드에서 스토리지 스택으로의 모든 SAS 링크가 다운됨(ocumEvtMccNodeStackLinksDown)	사건	노드 스택 연결	비판적인
노드에서 스토리지 스택으로 하나 이상의 SAS 링크가 다운됨(ocumEvtMccNodeStackLinksOneOrMoreDown)	위험	노드 스택 연결	경고

IP 구성을 통한 MetroCluster

이러한 이벤트는 IP 구성을 통한 MetroCluster 와 관련이 있습니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
MetroCluster IP 사이트 간 연결 상태가 다운되었습니다(mcclntersiteconnectivityStatusDown)	위험	MetroCluster 관계	비판적인
MetroCluster-IP 노드에서 스위치로의 연결 오프라인(mcclpPortStatusOffline)	위험	마디	오류

MetroCluster 스위치 이벤트

FC 구성을 통한 MetroCluster 에 대한 MetroCluster 스위치 이벤트는 MetroCluster 스위치의 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 해줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
스위치 온도 비정상(ocumEvtSwitchTemperatureAbnormal)	사건	MetroCluster 스위치	비판적인
스위치에 접근할 수 없음(ocumEvtSwitchUnreachable)	사건	MetroCluster 스위치	비판적인
스위치 팬 실패(ocumEvtSwitchFansOneOrMoreFailed)	사건	MetroCluster 스위치	비판적인
스위치 전원 공급 장치 실패(ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	사건	MetroCluster 스위치	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
스위치 온도 센서 실패(ocumEvtSwitchTemp eratureSensorFailed)  이 이벤트는 Cisco 스위치에만 적용됩니다.	사건	MetroCluster 스위치	비판적인

NVMe 네임스페이스 이벤트

NVMe 네임스페이스 이벤트는 네임스페이스의 상태에 대한 정보를 제공하므로 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 식별합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
NVMeNS 오프라인 *(nvmeNamespaceStatus Offline)	이벤트	네임스페이스	정보
NVMeNS 온라인 *(nvmeNamespaceStatus Online)	이벤트	네임스페이스	정보
NVMeNS 공간 부족 *(nvmeNamespaceSpace OutOfSpace)	위험	네임스페이스	경고
NVMeNS 파괴 *(nvmeNamespaceDestro y)	이벤트	네임스페이스	정보

영향 영역: 성능

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
NVMe 네임스페이스 IOPS 중요 임계값 위반(ocumNvmeNamespa celopsIncident)	사건	네임스페이스	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
NVMe 네임스페이스 IOPS 경고 임계값 위반(ocumNvmeNamespaceIopsWarning)	위험	네임스페이스	경고
NVMe 네임스페이스 MB/s 중요 임계값 위반(ocumNvmeNamespaceMbpsIncident)	사건	네임스페이스	비판적인
NVMe 네임스페이스 MB/s 경고 임계값 위반(ocumNvmeNamespaceMbpsWarning)	위험	네임스페이스	경고
NVMe 네임스페이스 대기 시간(ms/op) 중요 임계값 위반(ocumNvmeNamespaceLatencyIncident)	사건	네임스페이스	비판적인
NVMe 네임스페이스 대기 시간 ms/op 경고 임계값 위반(ocumNvmeNamespaceLatencyWarning)	위험	네임스페이스	경고
NVMe 네임스페이스 지연 시간 및 IOPS 중요 임계값 위반(ocumNvmeNamespaceLatencyIopsIncident)	사건	네임스페이스	비판적인
NVMe 네임스페이스 지연 시간 및 IOPS 경고 임계값 위반(ocumNvmeNamespaceLatencyIopsWarning)	위험	네임스페이스	경고
NVMe 네임스페이스 지연 시간 및 MB/s 중요 임계값 위반(ocumNvmeNamespaceLatencyMbpsIncident)	사건	네임스페이스	비판적인
NVMe 네임스페이스 지연 시간 및 MB/s 경고 임계값 위반(ocumNvmeNamespaceLatencyMbpsWarning)	위험	네임스페이스	경고

노드 이벤트

노드 이벤트는 노드 상태에 대한 정보를 제공하므로 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 식별합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
노드 루트 볼륨 공간이 거의 가득 찹니다(ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	위험	마디	경고
클라우드 AWS MetaDataConnFail *(ocumCloudAwsMetadataConnFail)	위험	마디	오류
클라우드 AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	위험	마디	오류
클라우드 AWS IAMCredsInvalid *(ocumCloudAwsIamCredsInvalid)	위험	마디	오류
클라우드 AWS IAMCredsNotFound *(ocumCloudAwsIamCredsNotFound)	위험	마디	오류
클라우드 AWS IAMCredsNotInitialized *(ocumCloudAwsIamCredsNotInitialized)	이벤트	마디	정보
클라우드 AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	위험	마디	오류

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
클라우드 AWS IAMRoleNotFound *(ocumCloudAwsIamRoleNotFound)	위험	마디	오류
클라우드 계층 호스트를 확인할 수 없음 *(ocumObjstoreHostUnresolvable)	위험	마디	오류
클라우드 계층 클러스터 간 네트워크 인터페이스 다운 *(ocumObjstoreInterClusterLifDown)	위험	마디	오류
NFSv4 풀 중 하나가 소진되었습니다. *(nbladeNfsv4PoolEXhaust)	사건	마디	비판적인
요청 불일치 클라우드 계층 서명 *(oscSignatureMismatch)	위험	마디	오류

영향 영역: 용량

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
QoS 모니터 메모리 최대화 *(ocumQosMonitorMemoryMaxed)	위험	마디	오류
QoS 모니터 메모리 감소 *(ocumQosMonitorMemoryAbated)	이벤트	마디	정보

영향 영역: 구성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
노드 이름이 변경됨(해당 없음)	이벤트	마디	정보

영향 영역: 성능

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
노드 IOPS 위험 임계값 위반(ocumNodeIopsIncident)	사건	마디	비판적인
노드 IOPS 경고 임계값 위반(ocumNodeIopsWarning)	위험	마디	경고
노드 MB/s 중요 임계값 위반(ocumNodeMbpsIncident)	사건	마디	비판적인
노드 MB/s 경고 임계값 위반(ocumNodeMbpsWarning)	위험	마디	경고
노드 대기 시간 ms/op 중요 임계값 위반(ocumNodeLatencyIncident)	사건	마디	비판적인
노드 지연 ms/op 경고 임계값 위반(ocumNodeLatencyWarning)	위험	마디	경고
노드 성능 용량 사용 임계값 위반(ocumNodePerfCapacityUsedIncident)	사건	마디	비판적인
노드 성능 용량 사용 경고 임계값 위반(ocumNodePerfCapacityUsedWarning)	위험	마디	경고
노드 성능 용량 사용 - 인수 위험 임계값 위반(ocumNodePerfCapacityUsedTakeoverIncident)	사건	마디	비판적인
노드 성능 용량 사용 - 인수 경고 임계값 위반(ocumNodePerfCapacityUsedTakeoverWarning)	위험	마디	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
노드 사용률 위험 임계값 위반(ocumNodeUtilizationIncident)	사건	마디	비판적인
노드 사용률 경고 임계값 위반(ocumNodeUtilizationWarning)	위험	마디	경고
노드 HA 쌍 과다 사용 임계값 위반(ocumNodeHaPairOverUtilizedInformation)	이벤트	마디	정보
노드 디스크 조각화 임계값 위반(ocumNodeDiskFragmentationWarning)	위험	마디	경고
성능 용량 사용 임계값 위반(ocumNodeOverUtilizedWarning)	위험	마디	경고
노드 동적 임계값 위반(ocumNodeDynamicEventWarning)	위험	마디	경고

영향 영역: 보안

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
권고 ID: NTAP-<권고 ID>(ocumx)	위험	마디	비판적인

NVRAM 배터리 이벤트

NVRAM 배터리 이벤트는 배터리 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 도와줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
NVRAM 배터리 부족(ocumEvtNvramBatteryLow)	위험	마디	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
NVRAM 배터리 방전(ocumEvtNvramBatteryDischarged)	위험	마디	오류
NVRAM 배터리 과충전(ocumEvtNvramBatteryOverCharged)	사건	마디	비판적인

포트 이벤트

포트 이벤트는 클러스터 포트에 대한 상태를 제공하여 포트가 다운되었는지 여부와 같이 포트의 변경 사항이나 문제를 모니터링할 수 있도록 해줍니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
포트 상태 다운(ocumEvtPortStatusDown)	사건	마디	비판적인

영향 영역: 성능

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
네트워크 포트 MB/s 위험 임계값 위반(ocumNetworkPortMbpsIncident)	사건	포트	비판적인
네트워크 포트 MB/s 경고 임계값 위반(ocumNetworkPortMbpsWarning)	위험	포트	경고
FCP 포트 MB/s 중요 임계값 위반(ocumFcpPortMbpsIncident)	사건	포트	비판적인
FCP 포트 MB/s 경고 임계값 위반(ocumFcpPortMbpsWarning)	위험	포트	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
네트워크 포트 사용률 위험 임계값 위반(ocumNetworkPortUtilizationIncident)	사건	포트	비판적인
네트워크 포트 사용률 경고 임계값 위반(ocumNetworkPortUtilizationWarning)	위험	포트	경고
FCP 포트 사용률 위험 임계값 위반(ocumFcpPortUtilizationIncident)	사건	포트	비판적인
FCP 포트 사용률 경고 임계값 위반(ocumFcpPortUtilizationWarning)	위험	포트	경고

전원 공급 이벤트

전원 공급 장치 이벤트는 하드웨어 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 도와줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
하나 이상의 전원 공급 장치 오류(ocumEvtPowerSupplyOneOrMoreFailed)	사건	마디	비판적인

보호 이벤트

보호 이벤트를 통해 작업이 실패하거나 중단되었는지 여부를 알 수 있으므로 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 보호

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
보호 작업 실패(ocumEvtProtectionJobTaskFailed)	사건	볼륨 또는 스토리지 서비스	비판적인
보호 작업이 중단되었습니다(ocumEvtProtectionJobAborted)	위험	볼륨 또는 스토리지 서비스	경고

Qtree 이벤트

Qtree 이벤트는 Qtree 용량과 파일 및 디스크 제한에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 도와줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 용량

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
Qtree 공간이 거의 가득 찹니다(ocumEvtQtreeSpaceNearlyFull)	위험	큐트리	경고
Qtree 공간 가득 참(ocumEvtQtreeSpaceFull)	위험	큐트리	오류
Qtree 공간 일반(ocumEvtQtreeSpaceThresholdOk)	이벤트	큐트리	정보
Qtree 파일 하드 한도에 도달했습니다(ocumEvtQtreeFilesHardLimitReached)	사건	큐트리	비판적인
Qtree 파일 소프트 한도 위반(ocumEvtQtreeFilesSoftLimitBreached)	위험	큐트리	경고
Qtree 공간 하드 한도에 도달했습니다(ocumEvtQtreeSpaceHardLimitReached)	사건	큐트리	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
Qtree 공간 소프트웨어 위반(ocumEvtQtreeSpaceSoftLimitBreached)	위험	큐트리	경고

서비스 프로세서 이벤트

서비스 프로세서 이벤트는 프로세서 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 해줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
서비스 프로세서가 구성되지 않았습니다(ocumEvtServiceProcessorNotConfigured)	위험	마디	경고
서비스 프로세서 오프라인(ocumEvtServiceProcessorOffline)	위험	마디	오류

SnapMirror 관계 이벤트

SnapMirror 관계 이벤트는 비동기 및 동기 SnapMirror 관계의 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 도와줍니다. 비동기 SnapMirror 관계 이벤트는 스토리지 VM과 볼륨 모두에 대해 생성되지만 동기 SnapMirror 관계 이벤트는 볼륨 관계에 대해서만 생성됩니다. 저장소 VM 재해 복구 관계의 일부인 구성 볼륨에 대해 생성된 이벤트가 없습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 보호

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 식별합니다.



SnapMirror 관계 이벤트는 Storage VM 재해 복구로 보호되는 Storage VM에 대해 생성되지만 구성 개체 관계에 대해서는 생성되지 않습니다.

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
미러 복제가 비정상입니다(ocumEvtSnapmirrorRelationshipUnhealthy)	위험	SnapMirror 관계	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
미러 복제 중단(ocumEvtSnapmirror RelationshipStateBrokenoff)	위험	SnapMirror 관계	오류
미러 복제 초기화 실패(ocumEvtSnapmirror RelationshipInitializeFailed)	위험	SnapMirror 관계	오류
미러 복제 업데이트 실패(ocumEvtSnapmirror RelationshipUpdateFailed)	위험	SnapMirror 관계	오류
미러 복제 지연 오류(ocumEvtSnapMirror RelationshipLagError)	위험	SnapMirror 관계	오류
미러 복제 지연 경고(ocumEvtSnapMirror RelationshipLagWarning)	위험	SnapMirror 관계	경고
미러 복제 재동기화 실패(ocumEvtSnapmirror RelationshipResyncFailed)	위험	SnapMirror 관계	오류
동기 복제가 동기화되지 않음 *(syncSnapmirrorRelationshipOutofsync)	위험	SnapMirror 관계	경고
동기 복제가 복원되었습니다. *(syncSnapmirrorRelationshipInSync)	이벤트	SnapMirror 관계	정보
동기 복제 자동 재동기화 실패 *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	위험	SnapMirror 관계	오류
클러스터에 Ontap Mediator가 추가되었습니다(snapmirror MediatorAdded)	이벤트	무리	정보

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
Ontap Mediator가 클러스터에서 제거되었습니다(snapmirror MediatorRemoved)	이벤트	무리	정보
Ontap Mediator는 클러스터에서 접근할 수 없습니다(snapmirrorMedia torUnreachable)	위험	중재인	경고
클러스터에서 Ontap Mediator에 액세스할 수 없습니다(snapmirrorMedia torMisconfigured)	위험	중재인	오류
Ontap Mediator Connectivity가 재설정되었으며 SnapMirror Active Sync(snapmirrorMediatorI nQuorum)를 위해 다시 동기화되고 준비되었습니다.	이벤트	중재인	정보

비동기 미러 및 볼트 관계 이벤트

비동기 미러 및 볼트 관계 이벤트는 비동기 SnapMirror 및 볼트 관계의 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 해줍니다. 비동기 미러 및 볼트 관계 이벤트는 볼륨 및 스토리지 VM 보호 관계 모두에서 지원됩니다. 하지만 저장소 VM 재해 복구에는 Vault 관계만 지원되지 않습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 보호



SnapMirror 및 Vault 관계 이벤트는 Storage VM 재해 복구로 보호되는 Storage VM에 대해서도 생성되지만 구성 개체 관계에 대해서는 생성되지 않습니다.

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
비동기 미러 및 볼트가 비정상입니다(ocumEvtMirr orVaultRelationshipUnhea lthy)	위험	SnapMirror 관계	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
비동기 미러 및 볼트가 끊어짐(ocumEvtMirrorVaultRelationshipStateBrokenoff)	위험	SnapMirror 관계	오류
비동기 미러 및 볼트 초기화 실패(ocumEvtMirrorVaultRelationshipInitializeFailed)	위험	SnapMirror 관계	오류
비동기 미러 및 볼트 업데이트 실패(ocumEvtMirrorVaultRelationshipUpdateFailed)	위험	SnapMirror 관계	오류
비동기 미러 및 볼트 지연 오류(ocumEvtMirrorVaultRelationshipLagError)	위험	SnapMirror 관계	오류
비동기 미러 및 볼트 지연 경고(ocumEvtMirrorVaultRelationshipLagWarning)	위험	SnapMirror 관계	경고
비동기 미러 및 볼트 재동기화 실패(ocumEvtMirrorVaultRelationshipResyncFailed)	위험	SnapMirror 관계	오류



"SnapMirror 업데이트 실패" 이벤트는 Active IQ 포털(Config Advisor)에서 발생합니다.

스냅샷 이벤트

스냅샷 이벤트는 스냅샷 상태에 대한 정보를 제공하며, 이를 통해 잠재적인 문제가 있는지 스냅샷을 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 이름, 트랩 이름, 영향 수준, 소스 유형 및 심각도가 포함됩니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
스냅샷 자동 삭제 비활성화 (해당 없음)	이벤트	용량	정보
스냅샷 자동 삭제 활성화 (해당 없음)	이벤트	용량	정보

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
스냅샷 자동 삭제 구성 수정됨(해당 없음)	이벤트	용량	정보

SnapVault 관계 이벤트

SnapVault 관계 이벤트는 SnapVault 관계 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 도와줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 보호

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
비동기 볼트 비정상(ocumEvtSnapVault RelationshipUnhealthy)	위험	SnapMirror 관계	경고
비동기 볼트가 끊어짐(ocumEvtSnapVault RelationshipStateBrokeno ff)	위험	SnapMirror 관계	오류
비동기 볼트 초기화 실패(ocumEvtSnapVaultR elationshipInitializeFailed)	위험	SnapMirror 관계	오류
비동기 볼트 업데이트 실패(ocumEvtSnapVaultR elationshipUpdateFailed)	위험	SnapMirror 관계	오류
비동기 볼트 지연 오류(ocumEvtSnapVaultR elationshipLagError)	위험	SnapMirror 관계	오류
비동기 볼트 지연 경고(ocumEvtSnapVaultR elationshipLagWarning)	위험	SnapMirror 관계	경고
비동기 볼트 재동기화 실패(ocumEvtSnapvaultR elationshipResyncFailed)	위험	SnapMirror 관계	오류

스토리지 장애 조치 설정 이벤트

저장소 장애 조치(SFO) 설정 이벤트는 저장소 장애 조치가 비활성화되었는지 또는 구성되지

않았는지에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
스토리지 장애 조치 상호 연결 하나 이상의 링크가 다운됨(ocumEvtSfoInterconnectOneOrMoreLinksDown)	위험	마디	경고
스토리지 장애 조치 비활성화(ocumEvtSfoSettingsDisabled)	위험	마디	오류
스토리지 장애 조치가 구성되지 않았습니니다(ocumEvtSfoSettingsNotConfigured)	위험	마디	오류
스토리지 장애 조치 상태 - 인수(ocumEvtSfoStateTakeover)	위험	마디	경고
스토리지 장애 조치 상태 - 부분적 반환(ocumEvtSfoStatePartialGiveback)	위험	마디	오류
스토리지 장애 조치 노드 상태 다운(ocumEvtSfoNodeStatusDown)	위험	마디	오류
스토리지 장애 조치 인수가 불가능합니다(ocumEvtSfoTakeoverNotPossible)	위험	마디	오류

스토리지 서비스 이벤트

스토리지 서비스 이벤트는 스토리지 서비스 생성 및 구독에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 도와줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 구성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
저장 서비스 생성됨(해당 없음)	이벤트	보관 서비스	정보
저장 서비스 가입(해당 없음)	이벤트	보관 서비스	정보
저장 서비스 해지(해당 없음)	이벤트	보관 서비스	정보

영향 영역: 보호

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
관리되는 SnapMirror 관계 ocumEvtStorageServiceUnsuportedRelationshipDeletion의 예기치 않은 삭제	위험	보관 서비스	경고
스토리지 서비스 멤버 볼륨의 예기치 않은 삭제(ocumEvtStorageServiceUnexpectedVolumeDeletion)	사건	보관 서비스	비판적인

보관 선반 이벤트

보관 선반 이벤트는 보관 선반에 비정상적인 상황이 있는지 알려주므로 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
비정상 전압 범위(ocumEvtShelfVoltageAbnormal)	위험	보관 선반	경고
비정상 전류 범위(ocumEvtShelfCurrentAbnormal)	위험	보관 선반	경고
비정상 온도(ocumEvtShelfTemperatureAbnormal)	위험	보관 선반	경고

스토리지 VM(스토리지 가상 머신, SVM이라고도 함) 이벤트는 스토리지 VM(SVM)의 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 해줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 식별합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
스토리지 VM CIFS 서비스 다운(ocumEvtVserverCifsServiceStatusDown)	사건	서포트 머신(SVM)	비판적인
SVM CIFS 서비스가 구성되지 않음(해당 없음)	이벤트	서포트 머신(SVM)	정보
존재하지 않는 CIFS 공유에 연결 시도 *(nbladeCifsNoPrivShare)	사건	서포트 머신(SVM)	비판적인
CIFS NetBIOS 이름 충돌 *(nbladeCifsNbNameConflict)	위험	서포트 머신(SVM)	오류
CIFS 새도 복사 작업이 실패했습니다. *(cifsShadowCopyFailure)	위험	서포트 머신(SVM)	오류
많은 CIFS 연결 *(nbladeCifsManyAuths)	위험	서포트 머신(SVM)	오류
최대 CIFS 연결 수를 초과했습니다. *(nbladeCifsMaxOpenSameFile)	위험	서포트 머신(SVM)	오류
사용자당 CIFS 연결 최대 수를 초과했습니다. *(nbladeCifsMaxSessPerUsrConn)	위험	서포트 머신(SVM)	오류
SVM FC/FCoE 서비스 다운(ocumEvtVserverFcServiceStatusDown)	사건	서포트 머신(SVM)	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
SVM iSCSI 서비스 다운(ocumEvtVserverIscsi ServiceStatusDown)	사건	서포트 머신(SVM)	비판적인
스토리지 VM NFS 서비스 다운(ocumEvtVserverNfsS erviceStatusDown)	사건	서포트 머신(SVM)	비판적인
SVM FC/FCoE 서비스가 구성되지 않음(해당 없음)	이벤트	서포트 머신(SVM)	정보
SVM iSCSI 서비스가 구성되지 않았습니니다(해당 없음)	이벤트	서포트 머신(SVM)	정보
SVM NFS 서비스가 구성되지 않았습니니다(해당 없음)	이벤트	서포트 머신(SVM)	정보
스토리지 VM이 중지되었습니다(ocumEvtV serverDown)	위험	서포트 머신(SVM)	경고
AV 서버가 너무 바빠서 새 스캔 요청을 수락할 수 없습니다. *(nbladeVscanConnBack Pressure)	위험	서포트 머신(SVM)	오류
바이러스 검사를 위한 AV 서버 연결이 없습니다. *(nbladeVscanNoScanner Conn)	사건	서포트 머신(SVM)	비판적인
등록된 AV 서버가 없습니다 *(nbladeVscanNoRegdSc anner)	위험	서포트 머신(SVM)	오류
응답하지 않는 AV 서버 연결 *(nbladeVscanConnInacti ve)	이벤트	서포트 머신(SVM)	정보
허가되지 않은 사용자가 AV 서버에 접근 시도 *(nbladeVscanBadUserPri vAccess)	위험	서포트 머신(SVM)	오류

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
AV 서버에서 발견된 바이러스 (nbladeVscanVirusDetected)	위험	서포트 머신(SVM)	오류

영향 영역: 구성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
SVM 발견됨(해당 없음)	이벤트	서포트 머신(SVM)	정보
SVM 삭제됨(해당 없음)	이벤트	무리	정보
SVM 이름 변경됨(해당 없음)	이벤트	서포트 머신(SVM)	정보

영향 영역: 성능

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
SVM IOPS 위험 임계값 위반(ocumSvmIopsIncident)	사건	서포트 머신(SVM)	비판적인
SVM IOPS 경고 임계값 위반(ocumSvmIopsWarning)	위험	서포트 머신(SVM)	경고
SVM MB/s 중요 임계값 위반(ocumSvmMbpsIncident)	사건	서포트 머신(SVM)	비판적인
SVM MB/s 경고 임계값 위반(ocumSvmMbpsWarning)	위험	서포트 머신(SVM)	경고
SVM 대기 시간 위험 임계값 위반(ocumSvmLatencyIncident)	사건	서포트 머신(SVM)	비판적인
SVM 지연 경고 임계값 위반(ocumSvmLatencyWarning)	위험	서포트 머신(SVM)	경고

영향 영역: 보안

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
감사 로그 비활성화(ocumVserverAuditLogDisabled)	위험	서포트 머신(SVM)	경고
로그인 배너 비활성화(ocumVserverLoginBannerDisabled)	위험	서포트 머신(SVM)	경고
SSH가 안전하지 않은 암호를 사용하고 있습니다(ocumVserverSSHInsecure)	위험	서포트 머신(SVM)	경고
로그인 배너가 변경되었습니다(ocumVserverLoginBannerChanged)	위험	서포트 머신(SVM)	경고
스토리지 VM 랜섬웨어 방지 모니터링이 비활성화되었습니다(antiRansomwareSvmStateDisabled)	위험	서포트 머신(SVM)	경고
스토리지 VM 랜섬웨어 방지 모니터링이 활성화되었습니다(학습 모드)(antiRansomwareSvmStateDryrun)	이벤트	서포트 머신(SVM)	정보
랜섬웨어 방지 모니터링에 적합한 스토리지 VM(학습 모드)(ocumEvtSvmArwCandidate)	이벤트	서포트 머신(SVM)	정보

사용자 및 그룹 할당량 이벤트

사용자 및 그룹 할당량 이벤트는 사용자 및 사용자 그룹 할당량의 용량과 파일 및 디스크 제한에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 해줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 용량

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
사용자 또는 그룹 할당량 디스크 공간 소프트 한도 위반(ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	위험	사용자 또는 그룹 할당량	경고
사용자 또는 그룹 할당량 디스크 공간 하드 한도에 도달했습니다(ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	사건	사용자 또는 그룹 할당량	비판적인
사용자 또는 그룹 할당량 파일 수 소프트 제한 위반(ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	위험	사용자 또는 그룹 할당량	경고
사용자 또는 그룹 할당량 파일 수 하드 제한에 도달했습니다(ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	사건	사용자 또는 그룹 할당량	비판적인

볼륨 이벤트

볼륨 이벤트는 볼륨 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 해줍니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 이름, 트랩 이름, 영향 수준, 소스 유형 및 심각도가 포함됩니다.

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 식별합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
볼륨 제한(ocumEvtVolumeRestricted)	위험	용량	경고
볼륨 오프라인(ocumEvtVolumeOffline)	사건	용량	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
볼륨 일부 사용 가능(ocumEvtVolumePartiallyAvailable)	위험	용량	오류
볼륨 마운트 해제됨(해당 없음)	이벤트	용량	정보
볼륨 마운트됨(해당 없음)	이벤트	용량	정보
볼륨 재마운트(해당 없음)	이벤트	용량	정보
볼륨 접합 경로 비활성(ocumEvtVolumeJunctionPathInactive)	위험	용량	경고
볼륨 자동 크기 조정 활성화(해당 없음)	이벤트	용량	정보
볼륨 자동 크기 조정 비활성화(해당 없음)	이벤트	용량	정보
볼륨 자동 크기 조정 최대 용량 수정됨(해당 없음)	이벤트	용량	정보
볼륨 자동 크기 증가 크기 수정됨(해당 없음)	이벤트	용량	정보

영향 영역: 용량

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
씬 프로비저닝된 볼륨 공간 위험(ocumThinProvisionVolumeSpaceAtRisk)	위험	용량	경고
볼륨 효율성 작업 오류(ocumEvtVolumeEfficiencyOperationError)	위험	용량	오류
볼륨 공간 가득 참(ocumEvtVolumeFull)	위험	용량	오류

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
볼륨 공간이 거의 가득 찹니다(ocumEvtVolumeNearlyFull)	위험	용량	경고
볼륨 논리 공간 가득 참 (*(volumeLogicalSpaceFull))	위험	용량	오류
볼륨 논리 공간이 거의 가득 찹니다. (*(volumeLogicalSpaceNearlyFull))	위험	용량	경고
볼륨 논리 공간 일반 (*(volumeLogicalSpaceAllOK))	이벤트	용량	정보
볼륨 스냅샷 예약 공간 가득 참(ocumEvtSnapshotFull)	위험	용량	경고
스냅샷 복사본이 너무 많습니다(ocumEvtSnapshotTooMany)	위험	용량	오류
볼륨 Qtree 할당량 초과 커밋(ocumEvtVolumeQtreeQuotaOvercommitted)	위험	용량	오류
볼륨 Qtree 할당량이 거의 초과 커밋됨(ocumEvtVolumeQtreeQuotaAlmostOvercommitted)	위험	용량	경고
볼륨 성장률 비정상(ocumEvtVolumeGrowthRateAbnormal)	위험	용량	경고
볼륨이 가득 찰 때까지 남은 일수(ocumEvtVolumeDaysUntilFullSoon)	위험	용량	오류
볼륨 공간 보장 비활성화 (해당 없음)	이벤트	용량	정보

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
볼륨 공간 보장 활성화됨 (해당 없음)	이벤트	용량	정보
볼륨 공간 보장 수정됨(해당 없음)	이벤트	용량	정보
볼륨 스냅샷 예약이 가득 찰 때까지 남은 일수(ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	위험	용량	오류
FlexGroup 구성 요소에 공간 문제가 있습니다. *(flexGroupConstituentsHaveSpaceIssues)	위험	용량	오류
FlexGroup 구성 요소 공간 상태 모두 정상 *(flexGroupConstituentsSpaceStatusAllOK)	이벤트	용량	정보
FlexGroup 구성 요소에 Inode 문제가 있습니다. *(flexGroupConstituentsHaveInodeIssues)	위험	용량	오류
FlexGroup 구성 요소 Inode 상태 모두 정상 *(flexGroupConstituentsInodesStatusAllOK)	이벤트	용량	정보
WAFL 볼륨 자동 크기 조정 실패 *(wafVolAutoSizeFail)	위험	용량	오류
WAFL 볼륨 자동 크기 조정 완료 *(wafVolAutoSizeDone)	이벤트	용량	정보
FlexGroup 볼륨이 80% 이상 활용되었습니다*	사건	용량	오류
FlexGroup 볼륨이 90% 이상 활용되었습니다*	사건	용량	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
볼륨 저장 효율성 이상(ocumVolumeAbnormalStorageEfficiencyWarning)	위험	용량	경고
볼륨 스냅샷 예약 활용 부족(volumeSnaphotReserveUnderutilizedWarning)	이벤트	용량	경고
볼륨 스냅샷 예약 미활용(volumeSnaphotReserveUnderutilizedCleared)	이벤트	용량	경고

영향 영역: 구성

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
볼륨 이름 변경됨(해당 없음)	이벤트	용량	정보
발견된 볼륨(해당 없음)	이벤트	용량	정보
볼륨 삭제됨(해당 없음)	이벤트	용량	정보

영향 영역: 성능

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
QoS 볼륨 최대 IOPS 경고 임계값 위반(ocumQosVolumeMaxIopsWarning)	위험	용량	경고
QoS 볼륨 최대 MB/s 경고 임계값 위반(ocumQosVolumeMaxMbpsWarning)	위험	용량	경고
QoS 볼륨 최대 IOPS/TB 경고 임계값 위반(ocumQosVolumeMaxIopsPerTbWarning)	위험	용량	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
성능 서비스 수준 정책(ocumConformanceLatencyWarning)에 정의된 대로 워크로드 볼륨 대기 시간 임계값이 위반되었습니다.	위험	용량	경고
볼륨 IOPS 중요 임계값 위반(ocumVolumeIopsIncident)	사건	용량	비판적인
볼륨 IOPS 경고 임계값 위반(ocumVolumeIopsWarning)	위험	용량	경고
볼륨 MB/s 중요 임계값 위반(ocumVolumeMbpsIncident)	사건	용량	비판적인
볼륨 MB/s 경고 임계값 위반(ocumVolumeMbpsWarning)	위험	용량	경고
볼륨 대기 시간 위험 임계값 위반(ocumVolumeLatencyIncident)	사건	용량	비판적인
볼륨 지연 경고 임계값 위반(ocumVolumeLatencyWarning)	위험	용량	경고
볼륨 캐시 미스 비율 위험 임계값 위반(ocumVolumeCacheMissRatioIncident)	사건	용량	비판적인
볼륨 캐시 미스 비율 경고 임계값 위반(ocumVolumeCacheMissRatioWarning)	위험	용량	경고
볼륨 지연 시간 및 IOPS 중요 임계값 위반(ocumVolumeLatencyIopsIncident)	사건	용량	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
볼륨 지연 시간 및 IOPS 경고 임계값 위반(ocumVolumeLatency IopsWarning)	위험	용량	경고
볼륨 대기 시간 및 MB/s 중요 임계값 위반(ocumVolumeLatency MbpsIncident)	사건	용량	비판적인
볼륨 지연 시간 및 MB/s 경고 임계값 위반(ocumVolumeLatency MbpsWarning)	위험	용량	경고
볼륨 대기 시간 및 집계 성능 사용 용량 중요 임계값 위반(ocumVolumeLatency AggregatePerfCapacityUs edIncident)	사건	용량	비판적인
볼륨 대기 시간 및 총 성능 용량 사용 경고 임계값 위반(ocumVolumeLatency AggregatePerfCapacityUs edWarning)	위험	용량	경고
볼륨 지연 시간 및 집계 사용률 중요 임계값 위반(ocumVolumeLatency AggregateUtilizationIncide nt)	사건	용량	비판적인
볼륨 대기 시간 및 집계 사용률 경고 임계값 위반(ocumVolumeLatency AggregateUtilizationWarni ng)	위험	용량	경고
볼륨 지연 시간 및 노드 성능 사용 용량 위험 임계값 위반(ocumVolumeLatency NodePerfCapacityUsedIn cident)	사건	용량	비판적인

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
볼륨 지연 시간 및 노드 성능 사용 용량 경고 임계값 위반(ocumVolumeLatency NodePerfCapacityUsedW arning)	위험	용량	경고
볼륨 지연 시간 및 노드 성능 사용 용량 - 인수 위험 임계값 위반(ocumVolumeLatency AggregatePerfCapacityUs edTakeoverIncident)	사건	용량	비판적인
볼륨 지연 시간 및 노드 성능 사용 용량 - 인수 경고 임계값 위반(ocumVolumeLatency AggregatePerfCapacityUs edTakeoverWarning)	위험	용량	경고
볼륨 지연 시간 및 노드 사용률 위험 임계값 위반(ocumVolumeLatency NodeUtilizationIncident)	사건	용량	비판적인
볼륨 지연 시간 및 노드 사용률 경고 임계값 위반(ocumVolumeLatency NodeUtilizationWarning)	위험	용량	경고

영향 영역: 보안

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
볼륨 랜섬웨어 방지 모니터링이 활성화되었습니다(활성 모드)(antiRansomwareVol umeStateEnabled)	이벤트	용량	정보
볼륨 랜섬웨어 방지 모니터링이 비활성화되었습니다(antiRa nsomwareVolumeStateDi sabled)	위험	용량	경고

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
볼륨 랜섬웨어 방지 모니터링이 활성화되었습니다(학습 모드)(antiRansomwareVol umeStateDryrun)	이벤트	용량	정보
볼륨 랜섬웨어 모니터링이 일시 중지되었습니다(학습 모드)(antiRansomwareVol umeStateDryrunPaused)	위험	용량	경고
볼륨 랜섬웨어 모니터링이 일시 중지됨(활성 모드)(antiRansomwareVol umeStateEnablePaused)	위험	용량	경고
볼륨 랜섬웨어 방지 모니터링이 비활성화됩니다(antiRanso mwareVolumeStateDisabl eInProgress)	위험	용량	경고
랜섬웨어 활동 발견(callHomeRansomwar eActivitySeen)	사건	용량	비판적인
랜섬웨어 방지 모니터링에 적합한 볼륨(학습 모드)(ocumEvtVolumeArw Candidate)	이벤트	용량	정보
랜섬웨어 방지 모니터링에 적합한 볼륨(활성 모드)(ocumVolumeSuited ForActiveAntiRansomwar eDetection)	위험	용량	경고
볼륨에서 노이즈가 있는 랜섬웨어 방지 경고가 표시됩니다(antiRansomwa reFeatureNoisyVolume).	위험	용량	경고

영향 영역: 데이터 보호

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
볼륨의 로컬 스냅샷 보호가 부족합니다(volumeLacksLocalProtectionWarning)	위험	용량	경고
볼륨의 로컬 스냅샷 보호가 충분하지 않습니다(volumeLacksLocalProtectionCleared)	위험	용량	경고

볼륨 이동 상태 이벤트

볼륨 이동 상태 이벤트는 볼륨 이동 상태를 알려주므로 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형, 심각도가 포함됩니다.

영향 영역: 용량

이벤트 이름(트랩 이름)	영향 수준	소스 유형	심각성
볼륨 이동 상태: 진행 중(해당 없음)	이벤트	용량	정보
볼륨 이동 상태 - 실패(ocumEvtVolumeMoveFailed)	위험	용량	오류
볼륨 이동 상태: 완료(해당 없음)	이벤트	용량	정보
볼륨 이동 - 컷오버 연기(ocumEvtVolumeMoveCutoverDeferred)	위험	용량	경고

이벤트 창 및 대화 상자 설명

이벤트는 사용자 환경에서 발생하는 문제를 알려줍니다. 이벤트 관리 인벤토리 페이지와 이벤트 세부 정보 페이지를 사용하여 모든 이벤트를 모니터링할 수 있습니다. 알림 설정 옵션 대화 상자를 사용하여 알림을 구성할 수 있습니다. 이벤트 설정 페이지를 사용하여 이벤트를 비활성화하거나 활성화할 수 있습니다.

알림 페이지

이벤트가 생성되거나 사용자에게 할당될 때 Unified Manager 서버가 알림을 보내도록 구성할 수 있습니다. 알림 메커니즘을 구성할 수도 있습니다. 예를 들어, 알림은 이메일이나 SNMP 트랩으로 전송될 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이메일

이 영역에서는 알림에 대한 다음 이메일 설정을 구성할 수 있습니다.

- 발신자 주소

경고 알림이 전송되는 이메일 주소를 지정합니다. 이 값은 보고서가 공유될 때 발신자 주소로도 사용됩니다. 보낸 사람 주소에 "ActiveIQUnifiedManager@localhost.com"이라는 주소가 미리 입력되어 있는 경우 모든 이메일 알림이 성공적으로 전달되도록 실제로 작동하는 이메일 주소로 변경해야 합니다.

SMTP 서버

이 영역에서는 다음 SMTP 서버 설정을 구성할 수 있습니다.

- 호스트 이름 또는 IP 주소

지정된 수신자에게 경고 알림을 보내는 데 사용되는 SMTP 호스트 서버의 호스트 이름을 지정합니다.

- 사용자 이름

SMTP 사용자 이름을 지정합니다. SMTP 사용자 이름은 SMTP 서버에서 SMTPAUTH가 활성화된 경우에만 필요합니다.

- 비밀번호

SMTP 비밀번호를 지정합니다. SMTP 사용자 이름은 SMTP 서버에서 SMTPAUTH가 활성화된 경우에만 필요합니다.

- 포트

SMTP 호스트 서버가 경고 알림을 보내는 데 사용하는 포트를 지정합니다.

기본값은 25입니다.

- **START/TLS** 사용

이 상자를 선택하면 TLS/SSL 프로토콜(start_tls 및 StartTLS라고도 함)을 사용하여 SMTP 서버와 관리 서버 간의 안전한 통신이 제공됩니다.

- **SSL**을 사용하세요

이 상자를 선택하면 SSL 프로토콜을 사용하여 SMTP 서버와 관리 서버 간의 안전한 통신이 제공됩니다.

SNMP

이 영역에서는 다음 SNMP 트랩 설정을 구성할 수 있습니다.

- 버전

필요한 보안 유형에 따라 사용할 SNMP 버전을 지정합니다. 옵션으로는 버전 1, 버전 3, 인증이 포함된 버전 3, 인증

및 암호화가 포함된 버전 3이 있습니다. 기본값은 버전 1입니다.

- 트랩 대상 호스트

관리 서버에서 보낸 SNMP 트랩을 수신하는 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)를 지정합니다. 여러 개의 트랩 대상을 지정하려면 각 호스트를 쉼표로 구분하세요.



"버전" 및 "아웃바운드 포트"와 같은 기타 모든 SNMP 설정은 목록에 있는 모든 호스트에서 동일해야 합니다.

- 아웃바운드 트랩 포트

SNMP 서버가 관리 서버에서 보낸 트랩을 수신하는 포트를 지정합니다.

기본값은 162입니다.

- 지역 사회

호스트에 접근하기 위한 커뮤니티 문자열입니다.

- 엔진 ID

SNMP 에이전트의 고유 식별자를 지정하며 관리 서버에서 자동으로 생성됩니다. 엔진 ID는 SNMP 버전 3, 인증 기능이 있는 SNMP 버전 3, 인증 및 암호화 기능이 있는 SNMP 버전 3에서 사용할 수 있습니다.

- 사용자 이름

SNMP 사용자 이름을 지정합니다. 사용자 이름은 SNMP 버전 3, 인증 기능이 있는 SNMP 버전 3, 인증 및 암호화 기능이 있는 SNMP 버전 3에서 사용할 수 있습니다.

- 인증 프로토콜

사용자를 인증하는 데 사용되는 프로토콜을 지정합니다. 프로토콜 옵션에는 MD5와 SHA가 있습니다. 기본값은 MD5입니다. 인증 프로토콜은 인증 기능이 있는 SNMP 버전 3 및 인증 및 암호화 기능이 있는 SNMP 버전 3에서 사용할 수 있습니다.

- 인증 비밀번호

사용자를 인증할 때 사용되는 비밀번호를 지정합니다. 인증 암호는 인증 기능이 있는 SNMP 버전 3 및 인증 및 암호화 기능이 있는 SNMP 버전 3에서 사용할 수 있습니다.

- 개인정보보호 프로토콜

SNMP 메시지를 암호화하는 데 사용되는 개인정보 보호 프로토콜을 지정합니다. 프로토콜 옵션에는 AES 128과 DES가 포함됩니다. 기본값은 AES 128입니다. SNMP 버전 3에서는 인증 및 암호화 기능을 갖춘 개인정보 보호 프로토콜을 사용할 수 있습니다.

- 개인정보 비밀번호

개인정보 보호 프로토콜을 사용할 때 비밀번호를 지정합니다. 개인 정보 보호 암호는 인증 및 암호화 기능이 있는 SNMP 버전 3에서 사용할 수 있습니다.

SNMP 개체 및 트랩에 대한 자세한 내용은 다음을 다운로드할 수 있습니다. "[Active IQ Unified Manager MIB](#)" NetApp 지원 사이트에서.

이벤트 관리 인벤토리 페이지

이벤트 관리 인벤토리 페이지를 사용하면 현재 이벤트와 해당 속성 목록을 볼 수 있습니다. 이벤트 확인, 해결, 할당 등의 작업을 수행할 수 있습니다. 특정 이벤트에 대한 알림을 추가할 수도 있습니다.

이 페이지의 정보는 최신 이벤트가 표시되도록 5분마다 자동으로 새로 고쳐집니다.

필터 구성 요소

이벤트 목록에 표시되는 정보를 사용자 지정할 수 있습니다. 다음 구성 요소를 사용하여 표시되는 이벤트 목록을 구체화할 수 있습니다.

- 미리 정의된 필터 선택 목록에서 선택하려면 메뉴를 봅니다.

여기에는 모든 활성(신규 및 확인된) 이벤트, 활성 성능 이벤트, 나(로그인한 사용자)에게 할당된 이벤트, 모든 유지 관리 기간 동안 생성된 모든 이벤트와 같은 항목이 포함됩니다.

- 검색 창에서 전체 또는 일부 용어를 입력하여 이벤트 목록을 구체화합니다.
- 이벤트 목록을 구체화하기 위해 사용 가능한 모든 필드와 필드 속성을 선택할 수 있는 필터 창을 시작하는 필터 버튼입니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 할당 대상

이벤트가 할당될 사용자를 선택할 수 있습니다. 사용자에게 이벤트를 할당하면 이벤트를 할당한 사용자 이름과 시간이 선택한 이벤트의 이벤트 목록에 추가됩니다.

- 나

현재 로그인한 사용자에게 이벤트를 할당합니다.

- 다른 사용자

이벤트를 다른 사용자에게 할당하거나 재할당할 수 있는 소유자 할당 대화 상자가 표시됩니다. 소유권 필드를 비워두면 이벤트 할당을 해제할 수도 있습니다.

- 인정하다

선택한 이벤트를 확인합니다.

이벤트를 확인하면 사용자 이름과 이벤트를 확인한 시간이 선택한 이벤트의 이벤트 목록에 추가됩니다. 이벤트를 확인하면 해당 이벤트를 관리할 책임이 있습니다.



정보 이벤트를 확인할 수 없습니다.

- 해결됨으로 표시

이벤트 상태를 해결됨으로 변경할 수 있습니다.

이벤트를 해결하면 사용자 이름과 이벤트를 해결한 시간이 선택한 이벤트의 이벤트 목록에 추가됩니다. 이벤트에 대한 시정 조치를 취한 후에는 이벤트를 해결됨으로 표시해야 합니다.

- 알림 추가

선택한 이벤트에 대한 알림을 추가할 수 있는 알림 추가 대화 상자가 표시됩니다.

- 보고서

현재 이벤트 보기의 세부 정보를 싼표로 구분된 값(.csv) 파일이나 PDF 문서로 내보낼 수 있습니다.

- 열 선택기 표시/숨기기

페이지에 표시되는 열을 선택하고, 표시되는 순서를 선택할 수 있습니다.

이벤트 목록

모든 이벤트의 세부 정보를 트리거된 시간에 따라 정렬하여 표시합니다.

기본적으로 모든 활성 이벤트 보기는 지난 7일 동안의 영향 수준이 사고 또는 위험인 새 이벤트와 확인된 이벤트를 보여줍니다.

- 트리거 시간

이벤트가 생성된 시간입니다.

- 심각성

이벤트 심각도: 중요(❌), 오류(💡), 경고(⚠️), 및 정보(i).

- 상태

이벤트 상태: 신규, 확인됨, 해결됨 또는 폐기됨.

- 영향 수준

이벤트 영향 수준: 사고, 위험, 이벤트 또는 업그레이드.

- 영향 영역

이벤트 영향 영역: 가용성, 용량, 성능, 보호, 구성 또는 보안.

- 이름

이벤트 이름. 이벤트 이름을 선택하면 해당 이벤트의 이벤트 세부 정보 페이지가 표시됩니다.

- 원천

이벤트가 발생한 객체의 이름입니다. 이름을 선택하면 해당 개체의 상태 또는 성능 세부 정보 페이지가 표시됩니다.

공유 QoS 정책 위반이 발생하면 가장 많은 IOPS 또는 MB/s를 소모하는 작업 부하 개체만 이 필드에 표시됩니다. 이 정책을 사용하는 추가 작업 부하가 이벤트 세부 정보 페이지에 표시됩니다.

- 소스 유형

이벤트가 연관된 개체 유형(예: 스토리지 VM, 볼륨 또는 Qtree)입니다.

- 담당자

이벤트가 할당된 사용자의 이름입니다.

- 이벤트 출처

이벤트가 "Active IQ Portal"에서 시작되었는지, 아니면 "Active IQ Unified Manager"에서 직접 시작되었는지 여부.

- 주석 이름

저장 객체에 할당된 주석의 이름입니다.

- 참고사항

이벤트에 추가된 메모의 수입니다.

- 미처리일수

이벤트가 처음 생성된 이후 경과된 일수입니다.

- 할당된 시간

이벤트가 사용자에게 할당된 이후 경과된 시간입니다. 경과된 시간이 일주일을 초과하면 이벤트가 사용자에게 할당된 타임스탬프가 표시됩니다.

- 확인자

이벤트를 확인한 사용자의 이름입니다. 이벤트가 확인되지 않으면 필드는 비어 있습니다.

- 확인된 시간

이벤트가 확인된 이후 경과된 시간입니다. 경과 시간이 일주일을 초과하면 이벤트가 확인된 타임스탬프가 표시됩니다.

- 해결자

이벤트를 해결한 사용자의 이름입니다. 이벤트가 해결되지 않으면 필드는 비어 있습니다.

- 해결 시간

이벤트가 해결된 이후 경과된 시간입니다. 경과 시간이 일주일을 초과하면 이벤트가 해결된 타임스탬프가 표시됩니다.

- 폐기된 시간

이벤트 상태가 더 이상 유효하지 않게 된 시점입니다.

이벤트 세부 정보 페이지

이벤트 세부 정보 페이지에서는 이벤트 심각도, 영향 수준, 영향 영역, 이벤트 소스 등 선택한 이벤트의 세부 정보를 볼 수 있습니다. 문제를 해결하기 위한 가능한 해결책에 대한 추가 정보도 볼 수 있습니다.

- 이벤트 이름

이벤트 이름과 이벤트가 마지막으로 확인된 시간입니다.

비성능 이벤트의 경우 이벤트가 새 이벤트 또는 확인된 상태인 동안에는 마지막으로 확인된 정보를 알 수 없으므로 숨겨집니다.

- 이벤트 설명

이벤트에 대한 간략한 설명입니다.

어떤 경우에는 이벤트가 발생한 이유가 이벤트 설명에 제공됩니다.

- 경쟁의 구성 요소

동적 성능 이벤트의 경우 이 섹션에는 클러스터의 논리적 및 물리적 구성 요소를 나타내는 아이콘이 표시됩니다. 구성 요소가 경합 중이면 해당 아이콘이 빨간색으로 동그라미로 표시됩니다.

여기에 표시된 구성 요소에 대한 설명은 `_클러스터 구성 요소와 이들이 경합할 수 있는 이유_`를 참조하세요.

이벤트 정보, 시스템 진단 및 제안된 작업 섹션은 다른 항목에서 설명합니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 노트 아이콘

이벤트에 대한 메모를 추가하거나 업데이트하고, 다른 사용자가 남긴 메모를 모두 검토할 수 있습니다.

작업 메뉴

- 나에게 할당

이벤트를 당신에게 할당합니다.

- 다른 사람에게 할당

이벤트를 다른 사용자에게 할당하거나 재할당할 수 있는 소유자 할당 대화 상자를 엽니다.

사용자에게 이벤트를 할당하면 해당 사용자의 이름과 이벤트가 할당된 시간이 선택한 이벤트의 이벤트 목록에 추가됩니다.

소유권 필드를 비워두면 이벤트 할당을 해제할 수도 있습니다.

- 인정하다

선택한 이벤트를 확인하여 반복적인 알림 알림을 더 이상 받지 않도록 합니다.

이벤트를 확인하면 사용자 이름과 이벤트를 확인한 시간이 선택한 이벤트의 이벤트 목록(확인자)에 추가됩니다. 어떤 사건을 인정하면, 그 사건을 관리할 책임을 맡게 됩니다.

- 해결됨으로 표시

이벤트 상태를 해결됨으로 변경할 수 있습니다.

이벤트를 해결하면 사용자 이름과 이벤트를 해결한 시간이 선택한 이벤트의 이벤트 목록(해결자)에 추가됩니다. 이벤트에 대한 시정 조치를 취한 후에는 이벤트를 해결됨으로 표시해야 합니다.

- 알림 추가

선택한 이벤트에 대한 알림을 추가할 수 있는 알림 추가 대화 상자가 표시됩니다.

이벤트 정보 섹션에 표시되는 내용

이벤트 세부 정보 페이지의 이벤트 정보 섹션을 사용하면 이벤트 심각도, 영향 수준, 영향 영역, 이벤트 소스 등 선택한 이벤트에 대한 세부 정보를 볼 수 있습니다.

이벤트 유형에 적용되지 않는 필드는 숨겨집니다. 다음 이벤트 세부 정보를 볼 수 있습니다.

- 이벤트 트리거 시간

이벤트가 생성된 시간입니다.

- 상태

이벤트 상태: 신규, 확인됨, 해결됨 또는 폐기됨.

- 폐기된 원인

예를 들어, 이벤트가 더 이상 사용되지 않게 된 원인이 되는 작업은 문제가 해결된 것입니다.

- 이벤트 기간

활성(새롭고 확인된) 이벤트의 경우 이는 감지 시간과 이벤트가 마지막으로 분석된 시간 사이의 시간입니다. 더 이상 발생하지 않는 이벤트의 경우, 이는 감지 시점과 이벤트가 해결되는 시점 사이의 시간입니다.

이 필드는 모든 성능 이벤트에 대해 표시되며, 다른 이벤트 유형의 경우 해결되거나 더 이상 사용되지 않는 경우에만 표시됩니다.

- 마지막으로 본 시간

이벤트가 마지막으로 활성화된 날짜와 시간입니다.

성능 이벤트의 경우 이 값은 이벤트 트리거 시간보다 최신일 수 있습니다. 이벤트가 활성 상태인 동안에는 새로운

성능 데이터가 수집될 때마다 이 필드가 업데이트되기 때문입니다. 다른 유형의 이벤트의 경우, 새 이벤트나 확인된 상태일 때 이 콘텐츠는 업데이트되지 않으므로 필드가 숨겨집니다.

- 심각성

이벤트 심각도: 중요(❌), 오류(❗), 경고(⚠), 및 정보(i).

- 영향 수준

이벤트 영향 수준: 사고, 위험, 이벤트 또는 업그레이드.

- 영향 영역

이벤트 영향 영역: 가용성, 용량, 성능, 보호, 구성 또는 보안.

- 원천

이벤트가 발생한 객체의 이름입니다.

공유 QoS 정책 이벤트에 대한 세부 정보를 볼 때, 가장 많은 IOPS 또는 MBps를 소모하는 최대 3개의 워크로드 개체가 이 필드에 나열됩니다.

소스 이름 링크를 클릭하면 해당 개체의 상태 또는 성능 세부 정보 페이지가 표시됩니다.

- 출처 주식

이벤트가 연관된 개체의 주식 이름과 값을 표시합니다.

이 필드는 클러스터, SVM 및 볼륨의 상태 이벤트에만 표시됩니다.

- 소스 그룹

영향을 받는 개체가 속한 모든 그룹의 이름을 표시합니다.

이 필드는 클러스터, SVM 및 볼륨의 상태 이벤트에만 표시됩니다.

- 소스 유형

이벤트와 연관된 개체 유형(예: SVM, 볼륨 또는 Qtree)입니다.

- 클러스터에서

이벤트가 발생한 클러스터의 이름입니다.

클러스터 이름 링크를 클릭하면 해당 클러스터의 상태 또는 성능 세부 정보 페이지가 표시됩니다.

- 영향을 받는 개체 수

이벤트로 인해 영향을 받는 객체의 수입니다.

이벤트의 영향을 받는 객체로 채워진 인벤토리 페이지를 표시하려면 객체 링크를 클릭하세요.

이 필드는 성능 이벤트에만 표시됩니다.

- 영향 받는 볼륨

이 이벤트로 인해 영향을 받는 볼륨 수입입니다.

이 필드는 노드 또는 집계기의 성능 이벤트에만 표시됩니다.

- 트리거 정책

이벤트를 발행한 임계값 정책의 이름입니다.

정책 이름 위에 커서를 올려 놓으면 임계값 정책의 세부 정보를 볼 수 있습니다. 적응형 QoS 정책의 경우 정의된 정책, 블록 크기, 할당 유형(할당된 공간 또는 사용된 공간)도 표시됩니다.

이 필드는 성능 이벤트에만 표시됩니다.

- 규칙 ID

Active IQ 플랫폼 이벤트의 경우 이는 이벤트를 생성하기 위해 트리거된 규칙의 번호입니다.

- 확인됨

이벤트를 확인한 사람의 이름과 이벤트가 확인된 시간입니다.

- 해결됨

사건을 해결한 사람의 이름과 사건이 해결된 시간입니다.

- 담당자

이벤트에 대한 작업을 맡은 사람의 이름입니다.

- 알림 설정

알림에 대한 다음 정보가 표시됩니다.

- 선택한 이벤트와 관련된 알림이 없는 경우 알림 추가 링크가 표시됩니다.

링크를 클릭하면 알림 추가 대화 상자를 열 수 있습니다.

- 선택한 이벤트와 연관된 알림이 하나 있는 경우, 해당 알림 이름이 표시됩니다.

링크를 클릭하면 알림 편집 대화 상자를 열 수 있습니다.

- 선택한 이벤트와 연관된 알림이 두 개 이상 있는 경우 알림 수가 표시됩니다.

링크를 클릭하면 알림 설정 페이지를 열어 이러한 알림에 대한 자세한 내용을 볼 수 있습니다.

비활성화된 알림은 표시되지 않습니다.

- 마지막 알림 전송됨

가장 최근의 경고 알림이 전송된 날짜와 시간입니다.

- 보내는 사람

경고 알림을 보내는 데 사용된 메커니즘: 이메일 또는 SNMP 트랩.

- 이전 스크립트 실행

경고가 생성되었을 때 실행된 스크립트의 이름입니다.

제안된 작업 섹션에 표시되는 내용

이벤트 세부 정보 페이지의 제안된 작업 섹션에서는 이벤트가 발생한 가능한 이유를 제공하고 사용자가 직접 이벤트를 해결할 수 있도록 몇 가지 작업을 제안합니다. 제안된 조치는 위반된 이벤트 유형이나 임계값 유형에 따라 사용자 지정됩니다.

이 영역은 일부 유형의 이벤트에만 표시됩니다.

어떤 경우에는 제안된 많은 작업에 대한 추가 정보를 참조하는 도움말 링크가 페이지에 제공되며, 여기에는 특정 작업을 수행하기 위한 지침도 포함됩니다. 일부 작업에는 Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, ONTAP CLI 명령 또는 이러한 도구의 조합을 사용하는 것이 포함될 수 있습니다.

여기에 제안된 조치는 이 이벤트를 해결하기 위한 지침일 뿐이므로 참고하시기 바랍니다. 이 이벤트를 해결하기 위해 취하는 조치는 사용자 환경의 맥락에 따라 결정되어야 합니다.

개체와 이벤트를 더 자세히 분석하려면 워크로드 분석 버튼을 클릭하여 워크로드 분석 페이지를 표시합니다.

Unified Manager는 특정 이벤트를 철저히 진단하고 단일 해결책을 제공할 수 있습니다. 해결 가능한 경우 해당 해결 방법은 수정 버튼과 함께 표시됩니다. 이 버튼을 클릭하면 Unified Manager가 이벤트를 발생시킨 문제를 해결합니다.

Active IQ 플랫폼 이벤트의 경우, 이 섹션에는 문제와 가능한 해결 방법을 설명하는 NetApp 기술 자료 문서에 대한 링크가 포함될 수 있습니다(사용 가능한 경우). 외부 네트워크 접속이 없는 사이트에서는 지식베이스 문서의 PDF가 로컬에서 열립니다. PDF는 Unified Manager 인스턴스에 수동으로 다운로드하는 규칙 파일의 일부입니다.

시스템 진단 섹션에 표시되는 내용

이벤트 세부 정보 페이지의 시스템 진단 섹션에서는 이벤트의 원인이 될 수 있는 문제를 진단하는데 도움이 되는 정보를 제공합니다.

이 영역은 일부 이벤트에만 표시됩니다.

일부 성과 이벤트는 트리거된 특정 이벤트와 관련된 차트를 제공합니다. 일반적으로 여기에는 IOPS 또는 MBps 차트와 지난 10일간의 지연 시간 차트가 포함됩니다. 이렇게 정리하면 이벤트가 활성화될 때 어떤 스토리지 구성 요소가 지연에 가장 큰 영향을 미치는지, 또는 지연의 영향을 받는지 확인할 수 있습니다.

동적 성능 이벤트의 경우 다음 차트가 표시됩니다.

- 워크로드 지연 시간 - 경합 중인 구성 요소에서 가장 큰 희생자, 괴롭힘 또는 상어 워크로드에 대한 지연 시간 기록을 표시합니다.
- 작업 부하 활동 - 경합 중인 클러스터 구성 요소의 작업 부하 사용에 대한 세부 정보를 표시합니다.
- 리소스 활동 - 경합 중인 클러스터 구성 요소에 대한 과거 성능 통계를 표시합니다.

일부 클러스터 구성 요소가 경쟁 중인 경우 다른 차트가 표시됩니다.

다른 이벤트는 시스템이 저장 객체에 대해 수행하는 분석 유형에 대한 간략한 설명을 제공합니다. 어떤 경우에는 시스템 정의 성능 정책이 여러 성능 카운터를 분석하는 경우, 분석된 각 구성 요소마다 하나씩, 하나 이상의 줄이 있을 수 있습니다. 이 시나리오에서는 진단 옆에 녹색 또는 빨간색 아이콘이 표시되어 해당 진단에서 문제가 발견되었는지 여부를 나타냅니다.

이벤트 설정 페이지

이벤트 설정 페이지에는 비활성화된 이벤트 목록이 표시되고, 연관된 개체 유형 및 이벤트의 심각도와 같은 정보가 제공됩니다. 이벤트를 전역적으로 비활성화하거나 활성화하는 등의 작업을 수행할 수도 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있는 경우에만 이 페이지에 액세스할 수 있습니다.

명령 버튼

명령 단추를 사용하면 선택한 이벤트에 대해 다음 작업을 수행할 수 있습니다.

- 장애를 입히다

이벤트를 비활성화하는 데 사용할 수 있는 이벤트 비활성화 대화 상자를 실행합니다.

- 할 수 있게 하다

이전에 비활성화하기로 선택한 이벤트를 선택하여 활성화합니다.

- 업로드 규칙

외부 네트워크 접속이 없는 사이트에서 Active IQ 규칙 파일을 수동으로 Unified Manager에 업로드할 수 있는 업로드 규칙 대화 상자를 실행합니다. 규칙은 Active IQ 플랫폼에서 정의한 시스템 구성, 케이بل링, 모범 사례 및 가용성에 대한 이벤트를 생성하기 위해 클러스터 AutoSupport 메시지에 대해 실행됩니다.

- **EMS** 이벤트 구독

모니터링하고 있는 클러스터에서 특정 EMS(이벤트 관리 시스템) 이벤트를 수신하도록 구독할 수 있는 EMS 이벤트 구독 대화 상자를 실행합니다. EMS는 클러스터에서 발생하는 이벤트에 대한 정보를 수집합니다. 구독된 EMS 이벤트에 대한 알림을 받으면 적절한 심각도에 따라 Unified Manager 이벤트가 생성됩니다.

목록 보기

목록 보기는 비활성화된 이벤트에 대한 정보를 (표 형식으로) 표시합니다. 열 필터를 사용하면 표시되는 데이터를 사용자 지정할 수 있습니다.

- 이벤트

비활성화된 이벤트의 이름을 표시합니다.

- 심각성

이벤트의 심각도를 표시합니다. 심각도는 '중요', '오류', '경고' 또는 '정보'일 수 있습니다.

- 소스 유형

이벤트가 생성된 소스 유형을 표시합니다.

이벤트 비활성화 대화 상자

이벤트 비활성화 대화 상자에는 이벤트를 비활성화할 수 있는 이벤트 유형 목록이 표시됩니다. 특정 심각도나 이벤트 집합에 따라 이벤트 유형에 대한 이벤트를 비활성화할 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이벤트 속성 영역

이벤트 속성 영역에서는 다음과 같은 이벤트 속성을 지정합니다.

- 이벤트 심각도

심각도 유형(중요, 오류, 경고 또는 정보)에 따라 이벤트를 선택할 수 있습니다.

- 이벤트 이름에 포함됨

지정된 문자가 포함된 이벤트를 필터링할 수 있습니다.

- 매칭 이벤트

이벤트 심각도 유형과 지정한 텍스트 문자열과 일치하는 이벤트 목록을 표시합니다.

- 이벤트 비활성화

비활성화하도록 선택한 이벤트 목록이 표시됩니다.

이벤트 이름과 함께 이벤트의 심각도도 표시됩니다.

명령 버튼

명령 단추를 사용하면 선택한 이벤트에 대해 다음 작업을 수행할 수 있습니다.

- 저장하고 닫기

이벤트 유형을 비활성화하고 대화 상자를 닫습니다.

- 취소

변경 사항을 취소하고 대화 상자를 닫습니다.

알림 관리

특정 이벤트나 특정 심각도 유형의 이벤트가 발생하면 자동으로 알림을 보내도록 알림을 구성할 수 있습니다. 알림이 발생할 때 실행되는 스크립트와 알림을 연결할 수도 있습니다.

어떤 알림이 있나요?

이벤트는 지속적으로 발생하지만 Unified Manager는 이벤트가 지정된 필터 기준을 충족할 때만 알림을 생성합니다. 알림을 생성할 이벤트를 선택할 수 있습니다. 예를 들어, 공간 임계값을 초과하거나 개체가 오프라인이 되는 경우입니다. 알림이 발생할 때 실행되는 스크립트와 알림을 연결할 수도 있습니다.

필터 기준에는 개체 클래스, 이름 또는 이벤트 심각도가 포함됩니다.

알림 이메일에는 어떤 정보가 포함되어 있나요?

Unified Manager 알림 이메일에는 이벤트 유형, 이벤트 심각도, 이벤트를 발생시킨 정책 또는 임계값의 이름, 이벤트에 대한 설명이 제공됩니다. 이메일 메시지에는 각 이벤트에 대한 하이퍼링크도 포함되어 있어 UI에서 이벤트의 세부 정보 페이지를 볼 수 있습니다.

알림 이메일은 알림 수신에 가입한 모든 사용자에게 전송됩니다.

수집 기간 동안 성능 카운터 또는 용량 값이 크게 변경되면 동일한 임계값 정책에 대해 위험 이벤트와 경고 이벤트가 동시에 트리거될 수 있습니다. 이 경우 경고 이벤트에 대한 이메일을 한 개, 중요 이벤트에 대한 이메일을 한 개 받을 수 있습니다. Unified Manager를 사용하면 경고 및 중요 임계값 위반에 대한 알림을 별도로 구독할 수 있기 때문입니다.

샘플 알림 이메일은 아래와 같습니다.

```
From: 10.11.12.13@company.com|
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from Active IQ Unified Manager: Thin-Provisioned Volume Space at Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk          - Thin-Provisioned Volume Space At Risk
Impact Area   - Capacity
Severity      - Warning
State         - New
Source        - svm_n1:/sm_vol_23
Cluster Name  - fas3250-39-33-37
Cluster FQDN  - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the
host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
https://10.11.12.13:443/events/94

Source details:
https://10.11.12.13:443/health/volumes/106

Alert details:
https://10.11.12.13:443/alerting/1
```

알림 추가

특정 이벤트가 생성되면 알림을 받도록 알림을 구성할 수 있습니다. 단일 리소스, 리소스 그룹 또는 특정 심각도 유형의 이벤트에 대한 알림을 구성할 수 있습니다. 알림을 받을 빈도를 지정하고 알림에 스크립트를 연결할 수 있습니다.

시작하기 전에

- 이벤트가 생성될 때 Active IQ Unified Manager 서버가 이러한 설정을 사용하여 사용자에게 알림을 보낼 수 있도록 사용자 이메일 주소, SMTP 서버, SNMP 트랩 호스트와 같은 알림 설정을 구성해야 합니다.
- 알림을 발생시키고자 하는 리소스와 이벤트, 그리고 알림을 보내고자 하는 사용자의 사용자 이름이나 이메일 주소를 알아야 합니다.
- 이벤트에 따라 스크립트를 실행하려면 스크립트 페이지를 사용하여 Unified Manager에 스크립트를 추가해야 합니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

여기에 설명된 대로 알림 설정 페이지에서 알림을 만드는 것 외에도 이벤트를 수신한 후 이벤트 세부 정보 페이지에서 직접 알림을 만들 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *알림 설정*을 클릭합니다.
2. 알림 설정 페이지에서 *추가*를 클릭합니다.
3. 알림 추가 대화 상자에서 *이름*을 클릭하고 알림의 이름과 설명을 입력합니다.
4. *리소스*를 클릭하고 알림에 포함하거나 제외할 리소스를 선택합니다.

이름에 포함 필드에 텍스트 문자열을 지정하여 필터를 설정하여 리소스 그룹을 선택할 수 있습니다. 지정한 텍스트 문자열을 기준으로 사용 가능한 리소스 목록에는 필터 규칙과 일치하는 리소스만 표시됩니다. 지정하는 텍스트 문자열은 대소문자를 구분합니다.

리소스가 지정한 포함 및 제외 규칙을 모두 준수하는 경우 제외 규칙이 포함 규칙보다 우선하며 제외된 리소스와 관련된 이벤트에 대한 알림은 생성되지 않습니다.

5. *이벤트*를 클릭하고 알림을 트리거하려는 이벤트 이름이나 이벤트 심각도 유형에 따라 이벤트를 선택합니다.



두 개 이상의 이벤트를 선택하려면 선택하는 동안 Ctrl 키를 누르세요.

6. *작업*을 클릭하고 알림을 보낼 사용자를 선택하고, 알림 빈도를 선택하고, SNMP 트랩을 트랩 수신기로 보낼지 여부를 선택하고, 알림이 생성될 때 실행할 스크립트를 지정합니다.



사용자에게 지정된 이메일 주소를 수정하고 편집을 위해 알림을 다시 열면 수정된 이메일 주소가 이전에 선택된 사용자에 더 이상 매핑되지 않으므로 이름 필드가 비어 있게 됩니다. 또한, 사용자 페이지에서 선택한 사용자의 이메일 주소를 수정한 경우, 수정된 이메일 주소는 선택한 사용자의 이메일 주소에 업데이트되지 않습니다.

SNMP 트랩을 통해 사용자에게 알리도록 선택할 수도 있습니다.

7. *저장*을 클릭하세요.

알림 추가의 예

이 예제에서는 다음 요구 사항을 충족하는 알림을 만드는 방법을 보여줍니다.

- 알림 이름: HealthTest
- 리소스: 이름에 "abc"가 포함된 모든 볼륨을 포함하고 이름에 "xyz"가 포함된 모든 볼륨을 제외합니다.
- 이벤트: 모든 중요한 건강 이벤트 포함
- 작업: "sample@domain.com", "테스트" 스크립트가 포함되며 사용자는 15분마다 알림을 받아야 합니다.

알림 추가 대화 상자에서 다음 단계를 수행합니다.

1. 이름*을 클릭하고 입력하세요. HealthTest * 알림 이름 필드에 *를 입력합니다.
2. *리소스*를 클릭하고 포함 탭의 드롭다운 목록에서 *볼륨*을 선택합니다.
 - a. 입력하다*abc 이름에 "abc"가 포함된 볼륨을 표시하려면 *이름에 다음이 포함됨 필드에 *를 입력합니다.
 - b. +를 선택하세요 [All Volumes whose name contains 'abc'] + 사용 가능한 리소스 영역에서 선택한 리소스 영역으로 이동합니다.
 - c. 제외*를 클릭하고 입력하세요. xyz *이름에 *포함*을 입력한 다음 *추가*를 클릭합니다.
3. *이벤트*를 클릭하고 이벤트 심각도 필드에서 *중요*를 선택합니다.
4. 일치하는 이벤트 영역에서 *모든 중요 이벤트*를 선택하고 선택한 이벤트 영역으로 이동합니다.
5. 작업*을 클릭하고 다음을 입력하세요. sample@domain.com * 이 사용자에게 경고 필드에서.
6. 사용자에게 15분마다 알림을 보내려면 *15분마다 알림*을 선택하세요.

지정된 시간 동안 수신자에게 알림을 반복적으로 보내도록 알림을 구성할 수 있습니다. 경고에 대한 이벤트 알림이 활성화되는 시간을 결정해야 합니다.
7. 실행할 스크립트 선택 메뉴에서 테스트 스크립트를 선택합니다.
8. *저장*을 클릭하세요.

알림 추가 지침

클러스터, 노드, 집계 또는 볼륨과 같은 리소스와 특정 심각도 유형의 이벤트를 기반으로 알림을 추가할 수 있습니다. 가장 좋은 방법은 개체가 속한 클러스터를 추가한 후 중요한 개체에 대한 알림을 추가하는 것입니다.

다음 지침과 고려 사항을 사용하여 시스템을 효과적으로 관리하기 위한 알림을 만들 수 있습니다.

• 경고 설명

알림을 효과적으로 추적할 수 있도록 알림에 대한 설명을 제공해야 합니다.

• 리소스

어떤 물리적 또는 논리적 리소스에 알림이 필요한지 결정해야 합니다. 필요에 따라 리소스를 포함하거나 제외할 수 있습니다. 예를 들어, 알림을 구성하여 집계를 면밀히 모니터링하려면 리소스 목록에서 필요한 집계를 선택해야 합니다.

예를 들어 리소스 범주를 선택하는 경우, *+[All User or Group Quotas] +*를 선택하면 해당 카테고리에 속한 모든 객체에 대한 알림을 받게 됩니다.



클러스터를 리소스로 선택하더라도 해당 클러스터 내의 스토리지 개체가 자동으로 선택되지는 않습니다. 예를 들어, 모든 클러스터의 모든 중요 이벤트에 대한 알림을 생성하면 클러스터 중요 이벤트에 대한 알림만 받게 됩니다. 노드, 집계 등의 중요 이벤트에 대한 알림은 받지 않습니다.

- 이벤트 심각도

지정된 심각도 유형(중요, 오류, 경고)의 이벤트가 알림을 트리거해야 하는지 여부와, 트리거한다면 어떤 심각도 유형을 사용해야 하는지 결정해야 합니다.

- 선택된 이벤트

생성된 이벤트 유형에 따라 알림을 추가하는 경우, 어떤 이벤트에 알림이 필요한지 결정해야 합니다.

이벤트 심각도를 선택했지만 개별 이벤트를 선택하지 않은 경우("선택한 이벤트" 열을 비워둔 경우) 해당 범주의 모든 이벤트에 대한 알림을 받게 됩니다.

- 행위

알림을 받는 사용자의 사용자 이름과 이메일 주소를 제공해야 합니다. SNMP 트랩을 알림 모드로 지정할 수도 있습니다. 경고가 생성될 때 스크립트가 실행되도록 경고에 스크립트를 연결할 수 있습니다.

- 알림 빈도

지정된 시간 동안 수신자에게 반복적으로 알림을 보내도록 알림을 구성할 수 있습니다. 경고에 대한 이벤트 알림이 활성화되는 시간을 결정해야 합니다. 이벤트가 확인될 때까지 이벤트 알림을 반복하려면 알림을 얼마나 자주 반복할지 결정해야 합니다.

- 스크립트 실행

스크립트를 알림과 연결할 수 있습니다. 알림이 생성되면 스크립트가 실행됩니다.

성능 이벤트에 대한 알림 추가

Unified Manager에서 수신한 다른 이벤트와 마찬가지로 개별 성능 이벤트에 대한 알림을 구성할 수 있습니다. 또한, 모든 성과 이벤트를 동일하게 처리하고 같은 사람에게 이메일을 보내려는 경우, 중요하거나 경고적인 성과 이벤트가 발생할 때 알려주는 단일 알림을 만들 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

아래 예에서는 모든 중요 지연 시간, IOPS, MBps 이벤트에 대한 이벤트를 만드는 방법을 보여줍니다. 동일한 방법을 사용하여 모든 성능 카운터와 모든 경고 이벤트에서 이벤트를 선택할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *알림 설정*을 클릭합니다.
2. 알림 설정 페이지에서 *추가*를 클릭합니다.

3. 알림 추가 대화 상자에서 *이름*을 클릭하고 알림의 이름과 설명을 입력합니다.

4. 리소스 페이지에서 어떤 리소스도 선택하지 마세요.

리소스가 선택되지 않았으므로 이벤트가 수신된 모든 클러스터, 집계, 볼륨 등에 알림이 적용됩니다.

5. *이벤트*를 클릭하고 다음 작업을 수행하세요.

a. 이벤트 심각도 목록에서 *중요*를 선택합니다.

b. 이벤트 이름 포함 필드에 다음을 입력합니다.*latency* 그런 다음 화살표를 클릭하여 일치하는 모든 이벤트를 선택합니다.

c. 이벤트 이름 포함 필드에 다음을 입력합니다.*iops* 그런 다음 화살표를 클릭하여 일치하는 모든 이벤트를 선택합니다.

d. 이벤트 이름 포함 필드에 다음을 입력합니다.*mbps* 그런 다음 화살표를 클릭하여 일치하는 모든 이벤트를 선택합니다.

6. 작업*을 클릭한 다음 *다음 사용자에게 알림 필드에서 알림 이메일을 받을 사용자의 이름을 선택합니다.

7. 이 페이지에서 SNMP 트랩을 발행하고 스크립트를 실행하기 위한 다른 옵션을 구성합니다.

8. *저장*을 클릭하세요.

테스트 알림

알림을 테스트하여 올바르게 구성했는지 확인할 수 있습니다. 이벤트가 발생하면 알림이 생성되고, 구성된 수신자에게 알림 이메일이 전송됩니다. 테스트 알림을 사용하면 알림이 전송되었는지, 스크립트가 실행되었는지 확인할 수 있습니다.

시작하기 전에

- 수신자의 이메일 주소, SMTP 서버, SNMP 트랩 등의 알림 설정을 구성했어야 합니다.

Unified Manager 서버는 이러한 설정을 사용하여 이벤트가 생성될 때 사용자에게 알림을 보낼 수 있습니다.

- 경고가 생성되면 스크립트를 할당하고 해당 스크립트를 실행하도록 구성해야 합니다.
- 애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *알림 설정*을 클릭합니다.

2. 알림 설정 페이지에서 테스트할 알림을 선택한 다음 *테스트*를 클릭합니다.

테스트 알림 이메일은 알림을 생성할 때 지정한 이메일 주소로 전송됩니다.

해결됨 및 폐기됨 이벤트에 대한 알림 활성화 및 비활성화

알림을 보내도록 구성한 모든 이벤트의 경우 해당 이벤트가 새로 만들기, 확인됨, 해결됨, 사용되지 않음 등 모든 사용 가능한 상태를 거칠 때 알림 메시지가 전송됩니다. 이벤트가 해결됨 및 폐기 상태로 전환될 때 알림을 받지 않으려면 해당 알림을 억제하도록 글로벌 설정을 구성할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

기본적으로 이벤트가 해결됨 및 폐기 상태로 전환되면 알림이 전송되지 않습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *알림 설정*을 클릭합니다.
2. 알림 설정 페이지에서 해결된 이벤트 및 폐기된 이벤트에 대한 알림 항목 옆에 있는 슬라이더 컨트롤을 사용하여 다음 작업 중 하나를 수행합니다.

에게...	이렇게 하세요...
이벤트가 해결되거나 더 이상 사용되지 않으면 알림 전송을 중지합니다.	슬라이더 컨트롤을 왼쪽으로 이동하세요
이벤트가 해결되거나 더 이상 사용되지 않으면 알림을 보내기 시작합니다.	슬라이더 컨트롤을 오른쪽으로 이동하세요

재해 복구 대상 볼륨을 경고 생성에서 제외합니다.

볼륨 알림을 구성할 때 알림 대화 상자에서 볼륨이나 볼륨 그룹을 식별하는 문자열을 지정할 수 있습니다. 하지만 SVM에 대한 재해 복구를 구성한 경우 소스 볼륨과 대상 볼륨의 이름이 같으므로 두 볼륨 모두에 대한 알림을 받게 됩니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

대상 SVM의 이름을 가진 볼륨을 제외하여 재해 복구 대상 볼륨에 대한 알림을 비활성화할 수 있습니다. 이는 볼륨 이벤트 식별자에 SVM 이름과 볼륨 이름이 모두 "<svm_name>:/<volume_name>" 형식으로 포함되어 있기 때문에 가능합니다.

아래 예에서는 기본 SVM "vs1"에서 볼륨 "vol1"에 대한 알림을 생성하는 방법을 보여 주지만, SVM "vs1-dr"에서 동일한 이름의 볼륨에 대한 알림이 생성되지 않도록 제외합니다.

알림 추가 대화 상자에서 다음 단계를 수행합니다.

단계

1. *이름*을 클릭하고 알림의 이름과 설명을 입력합니다.
2. 리소스*를 클릭한 다음 *포함 탭을 선택합니다.
 - a. 드롭다운 목록에서 볼륨*을 선택한 다음 입력하세요.vol1 이름에 "vol1"이 포함된 볼륨을 표시하려면 *이름에 다음이 포함됨 필드를 사용합니다.
 - b. +를 선택하세요[All Volumes whose name contains 'vol1'] + 사용 가능한 리소스 영역에서 선택한 리소스 영역으로 이동합니다.
3. 제외 탭을 선택하고 볼륨*을 선택한 후 다음을 입력합니다.vs1-dr *이름에 *포함*을 입력한 다음 *추가*를 클릭합니다.

이렇게 하면 SVM "vs1-dr"의 볼륨 "vol1"에 대한 경고가 생성되지 않습니다.

4. *이벤트*를 클릭하고 볼륨에 적용할 이벤트를 선택합니다.
5. 작업*을 클릭한 다음 *다음 사용자에게 알림 필드에서 알림 이메일을 받을 사용자의 이름을 선택합니다.
6. 이 페이지에서 SNMP 트랩을 발행하고 스크립트를 실행하기 위한 다른 옵션을 구성한 다음 *저장*을 클릭합니다.

알림 보기

다양한 이벤트에 대해 생성된 알림 목록은 알림 설정 페이지에서 볼 수 있습니다. 또한 알림 설명, 알림 방법 및 빈도, 알림을 트리거하는 이벤트, 알림의 이메일 수신자, 클러스터, 집계, 볼륨과 같은 영향을 받는 리소스와 같은 알림 속성을 볼 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *알림 설정*을 클릭합니다.

알림 목록은 알림 설정 페이지에 표시됩니다.

알림 편집

알림과 연관된 리소스, 이벤트, 수신자, 알림 옵션, 알림 빈도, 연관된 스크립트 등의 알림 속성을 편집할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *알림 설정*을 클릭합니다.
2. 알림 설정 페이지에서 편집하려는 알림을 선택하고 *편집*을 클릭합니다.
3. 알림 편집 대화 상자에서 필요에 따라 이름, 리소스, 이벤트 및 작업 섹션을 편집합니다.

알림과 관련된 스크립트를 변경하거나 제거할 수 있습니다.

4. *저장*을 클릭하세요.

알림 삭제

더 이상 필요하지 않은 알림은 삭제할 수 있습니다. 예를 들어, Unified Manager에서 더 이상 모니터링하지 않는 특정 리소스에 대해 생성된 알림을 삭제할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *알림 설정*을 클릭합니다.
2. 알림 설정 페이지에서 삭제하려는 알림을 선택하고 *삭제*를 클릭합니다.
3. *예*를 클릭하여 삭제 요청을 확인하세요.

경고 창 및 대화 상자 설명

이벤트에 대한 알림을 받으려면 알림 추가 대화 상자를 사용하여 알림을 구성해야 합니다. 알림 설정 페이지에서 알림 목록을 볼 수도 있습니다.

알림 설정 페이지

알림 설정 페이지에는 알림 목록이 표시되고 알림 이름, 상태, 알림 방법, 알림 빈도에 대한 정보가 제공됩니다. 이 페이지에서 알림을 추가, 편집, 제거, 활성화 또는 비활성화할 수도 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

명령 버튼

- 추가하다

새로운 알림을 추가할 수 있는 알림 추가 대화 상자를 표시합니다.

- 편집하다

선택한 알림을 편집할 수 있는 알림 편집 대화 상자를 표시합니다.

- 삭제

선택한 알림을 삭제합니다.

- 할 수 있게 하다

선택한 알림에 대한 알림을 보냅니다.

- 장애를 입히다

알림 전송을 일시적으로 중지하려면 선택한 알림을 비활성화합니다.

- 시험

추가 또는 편집 후 선택한 알림을 테스트하여 구성을 검증합니다.

- 해결된 이벤트 및 더 이상 사용되지 않는 이벤트에 대한 알림

이벤트가 해결됨 또는 사용되지 않음 상태로 이동하면 알림 전송을 활성화하거나 비활성화할 수 있습니다. 이를 통해 사용자는 불필요한 알림을 받는 것을 방지할 수 있습니다.

목록 보기

목록 보기에는 생성된 알림에 대한 정보가 표 형식으로 표시됩니다. 열 필터를 사용하면 표시되는 데이터를 사용자 지정할 수 있습니다. 알림을 선택하면 세부 정보 영역에서 해당 알림에 대한 자세한 내용을 볼 수 있습니다.

- 상태

경고가 활성화되었는지 여부를 지정합니다() 또는 장애인().

- 알리다

알림의 이름을 표시합니다.

- 설명

알림에 대한 설명을 표시합니다.

- 알림 방법

알림에 대해 선택된 알림 방법을 표시합니다. 이메일이나 SNMP 트랩을 통해 사용자에게 알릴 수 있습니다.

- 알림 빈도

이벤트가 확인되거나 해결되거나 폐기 상태로 전환될 때까지 관리 서버가 알림을 계속 보내는 빈도(분)를 지정합니다.

세부 정보 영역

세부 정보 영역에서는 선택한 알림에 대한 자세한 정보를 제공합니다.

- 경고 이름

알림의 이름을 표시합니다.

- 경고 설명

알림에 대한 설명을 표시합니다.

- 이벤트

알림을 트리거하려는 이벤트를 표시합니다.

- 자원

알림을 트리거할 리소스를 표시합니다.

- 포함

알림을 트리거하려는 리소스 그룹을 표시합니다.

- 제외

알림을 발생시키지 않을 리소스 그룹을 표시합니다.

- 알림 방법

경고에 대한 알림 방법을 표시합니다.

- 알림 빈도

이벤트가 확인되거나 해결되거나 폐기 상태로 전환될 때까지 관리 서버가 경고 알림을 계속 보내는 빈도를 표시합니다.

- 스크립트 이름

선택한 알림과 관련된 스크립트의 이름을 표시합니다. 이 스크립트는 알림이 생성되면 실행됩니다.

- 이메일 수신자

경고 알림을 받는 사용자의 이메일 주소를 표시합니다.

알림 추가 대화 상자

특정 이벤트가 생성되면 알림을 생성하여 문제를 신속하게 해결하고 환경에 미치는 영향을 최소화할 수 있습니다. 단일 리소스나 리소스 세트에 대한 알림을 만들 수 있으며, 특정 심각도 유형의 이벤트에 대해서도 알림을 만들 수 있습니다. 또한 알림 방법과 알림 빈도를 지정할 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이름

이 영역에서는 알림의 이름과 설명을 지정할 수 있습니다.

- 경고 이름

알림 이름을 지정할 수 있습니다.

- 경고 설명

알림에 대한 설명을 지정할 수 있습니다.

리소스

이 영역에서는 알림을 트리거하려는 동적 규칙에 따라 개별 리소스를 선택하거나 리소스를 그룹화할 수 있습니다. `_동적 규칙_`은 사용자가 지정한 텍스트 문자열을 기준으로 필터링되는 리소스 집합입니다. 드롭다운 목록에서 리소스 유형을 선택하여 리소스를 검색할 수도 있고, 정확한 리소스 이름을 지정하여 특정 리소스를 표시할 수도 있습니다.

저장소 개체 세부 정보 페이지에서 알림을 생성하는 경우 저장소 개체가 자동으로 알림에 포함됩니다.

- 포함하다

알림을 트리거할 리소스를 포함할 수 있습니다. 문자열을 지정하여 문자열과 일치하는 리소스를 그룹화하고 이 그룹을 선택하여 알림에 포함할 수 있습니다. 예를 들어, 이름에 "abc" 문자열이 포함된 모든 볼륨을 그룹화할 수 있습니다.

- 들어오지 못하게 하다

알림을 발생시키지 않으려는 리소스를 제외할 수 있습니다. 예를 들어, 이름에 "xyz" 문자열이 포함된 모든 볼륨을 제외할 수 있습니다.

제외 탭은 특정 리소스 유형의 모든 리소스를 선택한 경우에만 표시됩니다. 예: [+\[All Volumes\]](#) 또는 [\[All Volumes whose name contains 'xyz'\]](#) +.

리소스가 지정한 포함 및 제외 규칙을 모두 준수하는 경우 제외 규칙이 포함 규칙보다 우선하며 이벤트에 대한 알림은 생성되지 않습니다.

이벤트

이 영역에서는 알림을 생성할 이벤트를 선택할 수 있습니다. 특정 심각도나 일련의 이벤트에 따라 이벤트에 대한 알림을 만들 수 있습니다.

두 개 이상의 이벤트를 선택하려면 선택하는 동안 Ctrl 키를 누르고 있어야 합니다.

- 이벤트 심각도

심각도 유형(중요, 오류 또는 경고)에 따라 이벤트를 선택할 수 있습니다.

- 이벤트 이름에 포함됨

이름에 지정된 문자가 포함된 이벤트를 선택할 수 있습니다.

행위

이 영역에서는 알림이 발생했을 때 알림을 받을 사용자를 지정할 수 있습니다. 또한 알림 방법과 알림 빈도를 지정할 수 있습니다.

- 이러한 사용자에게 경고

알림을 받을 사용자의 이메일 주소나 사용자 이름을 지정할 수 있습니다.

사용자에게 지정된 이메일 주소를 수정하고 편집을 위해 알림을 다시 열면 수정된 이메일 주소가 이전에 선택된 사용자에게 더 이상 매핑되지 않으므로 이름 필드가 비어 있게 됩니다. 또한, 사용자 페이지에서 선택한 사용자의 이메일 주소를 수정한 경우, 수정된 이메일 주소는 선택한 사용자의 이메일 주소에 업데이트되지 않습니다.

- 알림 빈도

이벤트가 확인되거나 해결되거나 더 이상 유효하지 않은 상태로 이동될 때까지 관리 서버가 알림을 보내는 빈도를 지정할 수 있습니다.

다음 알림 방법을 선택할 수 있습니다.

- 한 번만 알림
- 지정된 빈도로 알림
- 지정된 시간 범위 내에서 지정된 빈도로 알림

- **SNMP** 트랩 발행

이 상자를 선택하면 SNMP 트랩을 전역적으로 구성된 SNMP 호스트로 보낼지 여부를 지정할 수 있습니다.

- 스크립트 실행

알림에 사용자 정의 스크립트를 추가할 수 있습니다. 이 스크립트는 알림이 생성되면 실행됩니다.



사용자 인터페이스에서 이 기능을 사용할 수 없는 경우 관리자가 해당 기능을 비활성화했기 때문입니다. 필요한 경우 저장소 관리 > *기능 설정*에서 이 기능을 활성화할 수 있습니다.

명령 버튼

- 구하다

알림을 만들고 대화 상자를 닫습니다.

- 취소

변경 사항을 취소하고 대화 상자를 닫습니다.

알림 편집 대화 상자

알림과 연관된 리소스, 이벤트, 스크립트, 알림 옵션 등의 알림 속성을 편집할 수 있습니다.

이름

이 영역에서는 알림의 이름과 설명을 편집할 수 있습니다.

- 경고 이름

알림 이름을 편집할 수 있습니다.

- 경고 설명

알림에 대한 설명을 지정할 수 있습니다.

- 경고 상태

알림을 활성화하거나 비활성화할 수 있습니다.

리소스

이 영역에서는 알림을 트리거하려는 동적 규칙에 따라 개별 리소스를 선택하거나 리소스를 그룹화할 수 있습니다. 드롭다운 목록에서 리소스 유형을 선택하여 리소스를 검색할 수도 있고, 정확한 리소스 이름을 지정하여 특정 리소스를 표시할 수도 있습니다.

- 포함하다

알림을 트리거할 리소스를 포함할 수 있습니다. 문자열을 지정하여 문자열과 일치하는 리소스를 그룹화하고 이 그룹을 선택하여 알림에 포함할 수 있습니다. 예를 들어, 이름에 “vol0” 문자열이 포함된 모든 볼륨을 그룹화할 수 있습니다.

- 들어오지 못하게 하다

알림을 발생시키지 않으려는 리소스를 제외할 수 있습니다. 예를 들어, 이름에 “xyz” 문자열이 포함된 모든 볼륨을 제외할 수 있습니다.



제외 탭은 특정 리소스 유형의 모든 리소스를 선택한 경우에만 표시됩니다. 예: [+\[All Volumes\]](#) + 또는 [+\[All Volumes whose name contains 'xyz'\]](#) +.

이벤트

이 영역에서는 알림을 트리거할 이벤트를 선택할 수 있습니다. 특정 심각도 또는 일련의 이벤트에 따라 이벤트에 대한 알림을 트리거할 수 있습니다.

- 이벤트 심각도

심각도 유형(중요, 오류 또는 경고)에 따라 이벤트를 선택할 수 있습니다.

- 이벤트 이름에 포함됨

이름에 지정된 문자가 포함된 이벤트를 선택할 수 있습니다.

행위

이 영역에서는 알림 방법과 알림 빈도를 지정할 수 있습니다.

- 이러한 사용자에게 경고

이메일 주소나 사용자 이름을 편집하거나, 알림을 받을 새 이메일 주소나 사용자 이름을 지정할 수 있습니다.

- 알림 빈도

이벤트가 확인되거나 해결되거나 더 이상 유효하지 않은 상태로 이동될 때까지 관리 서버가 알림을 보내는 빈도를 편집할 수 있습니다.

다음 알림 방법을 선택할 수 있습니다.

- 한 번만 알림
- 지정된 빈도로 알림
- 지정된 시간 범위 내에서 지정된 빈도로 알림

- **SNMP** 트랩 발행

SNMP 트랩을 전역적으로 구성된 SNMP 호스트로 보낼지 여부를 지정할 수 있습니다.

- 스크립트 실행

알림과 스크립트를 연결할 수 있습니다. 이 스크립트는 알림이 생성되면 실행됩니다.

명령 버튼

- 구하다

변경 사항을 저장하고 대화 상자를 닫습니다.

- 취소

변경 사항을 취소하고 대화 상자를 닫습니다.

스크립트 관리

스크립트를 사용하면 Unified Manager에서 여러 스토리지 개체를 자동으로 수정하거나 업데이트할 수 있습니다. 스크립트는 알림과 연결되어 있습니다. 이벤트로 인해 알림이 발생하면 스크립트가 실행됩니다. 사용자 정의 스크립트를 업로드하고 알림이 생성되면 실행을 테스트할 수 있습니다.

스크립트를 Unified Manager에 업로드하고 실행하는 기능은 기본적으로 활성화되어 있습니다. 보안상의 이유로 조직에서 이 기능을 허용하지 않으려는 경우, 저장소 관리 > *기능 설정*에서 이 기능을 비활성화할 수 있습니다.

관련 정보

["스크립트 업로드 기능 활성화 및 비활성화"](#)

스크립트가 알림과 함께 작동하는 방식

스크립트에 알림을 연결하면 Unified Manager에서 이벤트에 대한 알림이 발생할 때 스크립트가 실행됩니다. 스크립트를 사용하면 스토리지 개체의 문제를 해결하거나 이벤트를 생성하는 스토리지 개체를 식별할 수 있습니다.

Unified Manager에서 이벤트에 대한 알림이 생성되면 지정된 수신자에게 알림 이메일이 전송됩니다. 알림을 스크립트와 연결한 경우 스크립트가 실행됩니다. 스크립트에 전달된 인수의 세부 정보는 알림 이메일에서 얻을 수 있습니다.



사용자 지정 스크립트를 만들어 특정 이벤트 유형에 대한 알림과 연결한 경우 해당 이벤트 유형에 대한 사용자 지정 스크립트에 따라 작업이 수행되고, 수정 작업은 기본적으로 관리 작업 페이지나 Unified Manager 대시보드에서 사용할 수 없습니다.

스크립트는 실행을 위해 다음 인수를 사용합니다.

- -eventID
- -eventName
- -eventSeverity
- -eventSourceID
- -eventSourceName
- -eventSourceType

- -eventState
- -eventArgs

스크립트에서 인수를 사용하여 관련 이벤트 정보를 수집하거나 저장소 객체를 수정할 수 있습니다.

스크립트에서 인수를 얻는 예

```
`print "$ARGV[0] : $ARGV[1]\n"`
`print "$ARGV[7] : $ARGV[8]\n"`
```

경고가 생성되면 이 스크립트가 실행되고 다음 출력이 표시됩니다.

```
-`eventID : 290`
-`eventSourceID : 4138`
```

스크립트 추가

Unified Manager에서 스크립트를 추가하고, 스크립트를 알림과 연결할 수 있습니다. 이러한 스크립트는 알림이 생성되면 자동으로 실행되며, 이벤트가 생성된 저장소 개체에 대한 정보를 얻을 수 있습니다.

시작하기 전에

- Unified Manager 서버에 추가하려는 스크립트를 만들고 저장했어야 합니다.
- 스크립트에 지원되는 파일 형식은 Perl, Shell, PowerShell, Python입니다. .bat 파일.

Unified Manager가 설치된 플랫폼	지원 언어
VMware	Perl 및 셸 스크립트
리눅스	Perl, Python 및 Shell 스크립트
Windows	PowerShell, Perl, Python 및 .bat 스크립트

- Perl 스크립트의 경우 Perl이 Unified Manager 서버에 설치되어 있어야 합니다. VMware 설치의 경우 Perl 5가 기본적으로 설치되고 스크립트는 Perl 5에서 지원하는 내용만 지원합니다. Unified Manager를 설치한 후 Perl을 설치한 경우 Unified Manager 서버를 다시 시작해야 합니다.
- PowerShell 스크립트의 경우 스크립트를 실행할 수 있도록 Windows 서버에서 적절한 PowerShell 실행 정책을 설정해야 합니다.



스크립트가 경고 스크립트 진행 상황을 추적하기 위해 로그 파일을 생성하는 경우 Unified Manager 설치 폴더 내에 로그 파일이 생성되지 않도록 해야 합니다.

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

사용자 정의 스크립트를 업로드하고 알림에 대한 이벤트 세부 정보를 수집할 수 있습니다.



사용자 인터페이스에서 이 기능을 사용할 수 없는 경우 관리자가 해당 기능을 비활성화했기 때문입니다. 필요한 경우 저장소 관리 > *기능 설정*에서 이 기능을 활성화할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *스크립트*를 클릭합니다.
2. 스크립트 페이지에서 *추가*를 클릭합니다.
3. 스크립트 추가 대화 상자에서 *찾아보기*를 클릭하여 스크립트 파일을 선택합니다.
4. 선택한 스크립트에 대한 설명을 입력하세요.
5. *추가*를 클릭하세요.

관련 정보

["스크립트 업로드 기능 활성화 및 비활성화"](#)

스크립트 삭제

스크립트가 더 이상 필요하지 않거나 유효하지 않으면 Unified Manager에서 스크립트를 삭제할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 스크립트는 알림과 연관되어서는 안 됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *스크립트*를 클릭합니다.
2. 스크립트 페이지에서 삭제하려는 스크립트를 선택한 다음 *삭제*를 클릭합니다.
3. 경고 대화 상자에서 *예*를 클릭하여 삭제를 확인합니다.

테스트 스크립트 실행

저장소 개체에 대한 알림이 생성되면 스크립트가 올바르게 실행되는지 확인할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 지원되는 파일 형식의 스크립트를 Unified Manager에 업로드해야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *스크립트*를 클릭합니다.
2. 스크립트 페이지에서 테스트 스크립트를 추가합니다.
3. 왼쪽 탐색 창에서 저장소 관리 > *알림 설정*을 클릭합니다.
4. 알림 설정 페이지에서 다음 작업 중 하나를 수행합니다.

에게...	이렇게 하세요...
알림 추가	a. *추가*를 클릭하세요. b. 작업 섹션에서 알림을 테스트 스크립트와 연결합니다.
알림 편집	a. 알림을 선택한 다음 *편집*을 클릭합니다. b. 작업 섹션에서 알림을 테스트 스크립트와 연결합니다.

5. *저장*을 클릭하세요.

6. 알림 설정 페이지에서 추가하거나 수정한 알림을 선택한 다음 *테스트*를 클릭합니다.

스크립트는 "-test" 인수로 실행되고, 알림 경고는 경고가 생성될 때 지정된 이메일 주소로 전송됩니다.

지원되는 Unified Manager CLI 명령

스토리지 관리자는 CLI 명령을 사용하여 스토리지 개체(예: 클러스터, 집계, 볼륨, Q트리, LUN)에 대한 쿼리를 수행할 수 있습니다. CLI 명령을 사용하여 Unified Manager 내부 데이터베이스와 ONTAP 데이터베이스를 쿼리할 수 있습니다. 작업의 시작이나 끝에서 실행되거나 경고가 발생할 때 실행되는 스크립트에서 CLI 명령을 사용할 수도 있습니다.

모든 명령은 다음 명령으로 시작해야 합니다. `um cli login` 인증을 위해 유효한 사용자 이름과 비밀번호가 필요합니다.



`um run` 명령을 실행하려면 계정에 `console` 애플리케이션 액세스 권한이 있는지 확인하세요.

CLI 명령	설명	산출
<code>um cli login -u <username> [-p <password>]</code>	CLI에 로그인합니다. 보안 문제 때문에 "-u" 옵션 뒤에는 사용자 이름만 입력해야 합니다. 이 방법을 사용하면 비밀번호를 입력하라는 메시지가 표시되며, 비밀번호는 기록이나 프로세스 테이블에 저장되지 않습니다. 세션은 로그인 후 3시간 후에 만료되며, 그 후 사용자는 다시 로그인해야 합니다.	해당 메시지를 표시합니다.
<code>um cli logout</code>	CLI에서 로그아웃합니다.	해당 메시지를 표시합니다.
<code>um help</code>	모든 첫 번째 레벨 하위 명령을 표시합니다.	모든 첫 번째 레벨 하위 명령을 표시합니다.

CLI 명령	설명	산출
um run cmd [-t <timeout>] <cluster> <command>	하나 이상의 호스트에서 명령을 실행하는 가장 간단한 방법입니다. 주로 ONTAP 에서 작업을 수행하거나 가져오기 위한 경고 스크립팅에 사용됩니다. 선택적인 timeout 인수는 클라이언트에서 명령이 완료되는 데 걸리는 최대 시간 제한(초)을 설정합니다. 기본값은 0(영원히 대기)입니다.	ONTAP 에서 받은 내용입니다.
um run query <sql command>	SQL 쿼리를 실행합니다. 데이터베이스에서 읽는 쿼리만 허용됩니다. 모든 업데이트, 삽입 또는 삭제 작업은 지원되지 않습니다.	결과는 표 형식으로 표시됩니다. 빈 집합이 반환되거나 구문 오류 또는 잘못된 요청이 있는 경우 해당 오류 메시지가 표시됩니다.
um datasource add -u <username> -P <password> [-t <protocol>] [-p <port>] <hostname-or-ip>	관리되는 스토리지 시스템 목록에 데이터 소스를 추가합니다. 데이터 소스는 저장 시스템에 대한 연결이 어떻게 이루어지는지 설명합니다. 데이터 소스를 추가할 때는 -u(사용자 이름) 및 -P(비밀번호) 옵션을 지정해야 합니다. -t(프로토콜) 옵션은 클러스터와 통신하는 데 사용되는 프로토콜(http 또는 https)을 지정합니다. 프로토콜을 지정하지 않으면 두 프로토콜이 모두 시도됩니다. -p(포트) 옵션은 클러스터와 통신하는 데 사용되는 포트를 지정합니다. 포트가 지정되지 않으면 적절한 프로토콜의 기본값이 시도됩니다. 이 명령은 스토리지 관리자만 실행할 수 있습니다.	사용자에게 인증서를 수락하라는 메시지를 표시하고 해당 메시지를 인쇄합니다.
um datasource list [<datasource-id>]	관리형 스토리지 시스템의 데이터 소스를 표시합니다.	다음 값을 표 형식으로 표시합니다. ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message .
um datasource modify [-h <hostname-or-ip>] [-u <username>] [-P <password>] [-t <protocol>] [-p <port>] <datasource-id>	하나 이상의 데이터 소스 옵션을 수정합니다. 저장소 관리자만 실행할 수 있습니다.	해당 메시지를 표시합니다.

CLI 명령	설명	산출
um datasource remove <datasource-id>	Unified Manager에서 데이터 소스 (클러스터)를 제거합니다.	해당 메시지를 표시합니다.
um option list [<option> ..]	set 명령을 사용하여 구성할 수 있는 모든 옵션을 나열합니다.	다음 값을 표 형식으로 표시합니다. Name, Value, Default Value, and Requires Restart.
um option set <option-name>=<option-value> [<option-name>=<option-value> ...]	하나 이상의 옵션을 설정합니다. 해당 명령은 스토리지 관리자만 실행할 수 있습니다.	해당 메시지를 표시합니다.
um version	Unified Manager 소프트웨어 버전을 표시합니다.	Version ("9.6")
um lun list [-q] [-ObjectType <object-id>]	지정된 객체를 필터링한 후 LUN을 나열합니다. -q는 모든 명령에 헤더를 표시하지 않도록 설정합니다. ObjectType은 lun, qtree, cluster, volume, quota 또는 svm일 수 있습니다. 예를 들어: um lun list -cluster 1 이 예에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령은 클러스터 내의 ID가 1인 모든 LUN을 나열합니다.	다음 값을 표 형식으로 표시합니다. ID and LUN path.
um svm list [-q] [-ObjectType <object-id>]	지정된 객체를 필터링한 후 스토리지 VM을 나열합니다. ObjectType은 lun, qtree, cluster, volume, quota 또는 svm이 될 수 있습니다. 예를 들어: um svm list -cluster 1 이 예에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령은 ID가 1인 클러스터 내의 모든 스토리지 VM을 나열합니다.	다음 값을 표 형식으로 표시합니다. Name and Cluster ID.

CLI 명령	설명	산출
um qtree list [-q] [-ObjectType <object-id>]	지정된 객체를 필터링한 후 qtree를 나열합니다. -q는 모든 명령에 헤더를 표시하지 않도록 설정합니다. ObjectType은 lun, qtree, cluster, volume, quota 또는 svm일 수 있습니다. 예를 들어: <pre>um qtree list -cluster 1</pre> 이 예에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령은 ID가 1인 클러스터 내의 모든 qtree를 나열합니다.	다음 값을 표 형식으로 표시합니다. Qtree ID and Qtree Name.
um disk list [-q] [-ObjectType <object-id>]	지정된 객체를 필터링한 후 디스크를 나열합니다. ObjectType은 disk, aggr, node 또는 cluster가 될 수 있습니다. 예를 들어: <pre>um disk list -cluster 1</pre> 이 예에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령은 클러스터 내에서 ID가 1인 모든 디스크를 나열합니다.	다음 값을 표 형식으로 표시합니다. ObjectType and object-id.
um cluster list [-q] [-ObjectType <object-id>]	지정된 객체를 필터링한 후 클러스터를 나열합니다. ObjectType은 disk, aggr, node, cluster, lun, qtree, volume, quota 또는 svm일 수 있습니다. 예를 들어: <pre>um cluster list -aggr 1</pre> 이 예에서 "-aggr"은 objectType이고 "1"은 objectId입니다. 이 명령은 ID 1의 집계기 속한 클러스터를 나열합니다.	다음 값을 표 형식으로 표시합니다. Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key.

CLI 명령	설명	산출
um cluster node list [-q] [-ObjectType <object-id>]	지정된 객체를 필터링한 후 클러스터 노드를 나열합니다. ObjectType은 disk, aggr, node 또는 cluster가 될 수 있습니다. 예를 들어: <pre>um cluster node list -cluster 1</pre> 이 예에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령은 ID가 1인 클러스터 내의 모든 노드를 나열합니다.	다음 값을 표 형식으로 표시합니다. Name and Cluster ID.
um volume list [-q] [-ObjectType <object-id>]	지정된 객체를 필터링한 후 볼륨을 나열합니다. ObjectType은 lun, qtree, cluster, volume, quota, svm 또는 aggregate가 될 수 있습니다. 예를 들어: <pre>um volume list -cluster 1</pre> 이 예에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령은 ID가 1인 클러스터 내의 모든 볼륨을 나열합니다.	다음 값을 표 형식으로 표시합니다. Volume ID and Volume Name.
um quota user list [-q] [-ObjectType <object-id>]	지정된 객체를 필터링한 후 할당량 사용자를 나열합니다. ObjectType은 qtree, cluster, volume, quota 또는 svm이 될 수 있습니다. 예를 들어: <pre>um quota user list -cluster 1</pre> 이 예에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령은 클러스터 내에서 ID가 1인 모든 할당량 사용자를 나열합니다.	다음 값을 표 형식으로 표시합니다. ID, Name, SID and Email.

CLI 명령	설명	산출
<code>um aggr list [-q] [-ObjectType <object-id>]</code>	지정된 객체를 필터링한 후 집계를 나열합니다. ObjectType은 disk, aggr, node, cluster 또는 volume이 될 수 있습니다. 예를 들어: um aggr list -cluster 1 이 예에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령은 ID가 1인 클러스터 내의 모든 집계를 나열합니다.	다음 값을 표 형식으로 표시합니다. Aggr ID, and Aggr Name .
<code>um event ack <event-ids></code>	하나 이상의 이벤트를 확인합니다.	해당 메시지를 표시합니다.
<code>um event resolve <event-ids></code>	하나 이상의 이벤트를 해결합니다.	해당 메시지를 표시합니다.
<code>um event assign -u <username> <event-id></code>	사용자에게 이벤트를 할당합니다.	해당 메시지를 표시합니다.
<code>um event list [-s <source>] [-S <event-state-filter-list>..] [<event-id> ..]</code>	시스템이나 사용자가 생성한 이벤트를 나열합니다. 소스, 상태, ID를 기준으로 이벤트를 필터링합니다.	다음 값을 표 형식으로 표시합니다. Source, Source type, Name, Severity, State, User and Timestamp .
<code>um backup restore -f <backup_file_path_and_name></code>		해당 메시지를 표시합니다.

스크립트 창 및 대화 상자 설명

스크립트 페이지를 사용하면 Unified Manager에 스크립트를 추가할 수 있습니다.

스크립트 페이지

스크립트 페이지를 사용하면 Unified Manager에 사용자 정의 스크립트를 추가할 수 있습니다. 이러한 스크립트를 알림과 연결하여 스토리지 객체를 자동으로 재구성할 수 있습니다.

스크립트 페이지를 사용하면 Unified Manager에서 스크립트를 추가하거나 삭제할 수 있습니다.

명령 버튼

- 추가하다

스크립트를 추가할 수 있는 스크립트 추가 대화 상자를 표시합니다.

- 삭제

선택한 스크립트를 삭제합니다.

목록 보기

목록 보기에는 Unified Manager에 추가한 스크립트가 표 형식으로 표시됩니다.

- 이름

스크립트의 이름을 표시합니다.

- 설명

스크립트에 대한 설명을 표시합니다.

스크립트 추가 대화 상자

스크립트 추가 대화 상자를 사용하면 Unified Manager에 스크립트를 추가할 수 있습니다. 스크립트를 사용하여 알림을 구성하여 스토리지 개체에 대해 생성된 이벤트를 자동으로 해결할 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

- 스크립트 파일 선택

알림에 대한 스크립트를 선택할 수 있습니다.

- 설명

스크립트에 대한 설명을 지정할 수 있습니다.

클러스터 성능 모니터링 및 관리

Active IQ Unified Manager 성능 모니터링 소개

Active IQ Unified Manager (이전 OnCommand Unified Manager)는 NetApp ONTAP 소프트웨어를 실행하는 시스템에 대한 성능 모니터링 기능과 이벤트 근본 원인 분석을 제공합니다.

Unified Manager를 사용하면 클러스터 구성 요소를 과도하게 사용하여 클러스터의 다른 작업 부하의 성능을 저하시키는 작업 부하를 식별할 수 있습니다. 성능 임계값 정책을 정의하면 특정 성능 카운터에 대한 최대값을 지정하여 임계값이 초과되면 이벤트가 생성되도록 할 수도 있습니다. Unified Manager는 이러한 성능 이벤트에 대해 알림을 보내므로, 이를 통해 시정 조치를 취하고 성능을 정상적인 운영 수준으로 되돌릴 수 있습니다. Unified Manager UI에서 이벤트를 보고 분석할 수 있습니다.

Unified Manager는 두 가지 유형의 작업 부하의 성능을 모니터링합니다.

- 사용자 정의 워크로드

이러한 작업 부하에는 클러스터에서 생성한 FlexVol 볼륨과 FlexGroup 볼륨이 포함됩니다.

- 시스템 정의 워크로드

이러한 작업 부하는 내부 시스템 활동으로 구성됩니다.

Unified Manager 성능 모니터링 기능

Unified Manager는 ONTAP 소프트웨어를 실행하는 시스템에서 성능 통계를 수집하고 분석합니다. 다양한 클러스터 구성 요소에 대한 다양한 성능 카운터를 모니터링하기 위해 동적 성능 임계값과 사용자 정의 성능 임계값을 사용합니다.

높은 응답 시간(대기 시간)은 볼륨과 같은 스토리지 객체가 평소보다 느리게 수행되고 있음을 나타냅니다. 이 문제는 볼륨을 사용하는 클라이언트 애플리케이션의 성능이 저하되었음을 나타냅니다. Unified Manager는 성능 문제가 있는 스토리지 구성 요소를 식별하고 성능 문제를 해결하기 위해 취할 수 있는 제안된 작업 목록을 제공합니다.

Unified Manager에는 다음과 같은 기능이 포함되어 있습니다.

- ONTAP 소프트웨어를 실행하는 시스템의 작업 부하 성능 통계를 모니터링하고 분석합니다.
- 클러스터, 노드, 집계, 포트, SVM, 볼륨, LUN, NVMe 네임스페이스 및 네트워크 인터페이스(LIF)에 대한 성능 카운터를 추적합니다.
- 시간 경과에 따른 작업 부하 활동을 나타내는 자세한 그래프를 표시합니다. 여기에는 IOPS(작업), MB/s(처리량), 지연 시간(응답 시간), 활용도, 성능 용량 및 캐시 비율이 포함됩니다.
- 임계값을 초과하면 이벤트를 트리거하고 이메일 알림을 보내는 사용자 정의 성능 임계값 정책을 만들 수 있습니다.
- 워크로드 활동에 대해 학습하여 성능 문제를 식별하고 경고하는 시스템 정의 임계값과 동적 성능 임계값을 사용합니다.
- 볼륨과 LUN에 적용되는 서비스 품질(QoS) 정책과 성능 서비스 수준 정책(PSL)을 식별합니다.
- 경합 중인 클러스터 구성 요소를 명확하게 식별합니다.

- 클러스터 구성 요소를 과도하게 사용하는 작업 부하와 활동 증가로 인해 성능에 영향을 받는 작업 부하를 식별합니다.

스토리지 시스템 성능을 관리하는 데 사용되는 **Unified Manager** 인터페이스

이 섹션에는 Active IQ Unified Manager 데이터 저장 용량, 가용성 및 보호 문제를 해결하기 위해 제공하는 두 가지 사용자 인터페이스에 대한 정보가 포함되어 있습니다. 두 가지 UI는 Unified Manager 웹 UI와 유지 관리 콘솔입니다.

Unified Manager의 보호 기능을 사용하려면 OnCommand Workflow Automation (WFA)도 설치하고 구성해야 합니다.

Unified Manager 웹 UI

Unified Manager 웹 UI를 사용하면 관리자가 데이터 저장 용량, 가용성 및 보호와 관련된 클러스터 문제를 모니터링하고 문제를 해결할 수 있습니다.

이 섹션에서는 관리자가 Unified Manager 웹 UI에 표시되는 스토리지 용량, 데이터 가용성 또는 보호 문제를 해결하기 위해 따를 수 있는 몇 가지 일반적인 워크플로를 설명합니다.

유지 관리 콘솔

Unified Manager 유지 관리 콘솔을 사용하면 관리자는 Unified Manager 서버 자체와 관련된 운영 체제 문제, 버전 업그레이드 문제, 사용자 액세스 문제 및 네트워크 문제를 모니터링, 진단 및 해결할 수 있습니다. Unified Manager 웹 UI를 사용할 수 없는 경우 유지 관리 콘솔을 통해서만 Unified Manager에 액세스할 수 있습니다.

이 정보를 사용하여 유지 관리 콘솔에 액세스하고 Unified Manager 서버 작동과 관련된 문제를 해결할 수 있습니다.

클러스터 구성 및 성능 데이터 수집 활동

_클러스터 구성 데이터_의 수집 간격은 15분입니다. 예를 들어, 클러스터를 추가한 후 Unified Manager UI에 클러스터 세부 정보가 표시되는 데 15분이 걸립니다. 이 간격은 클러스터를 변경할 때도 적용됩니다.

예를 들어, 클러스터의 SVM에 두 개의 새 볼륨을 추가하는 경우 다음 폴링 간격(최대 15분) 후에 UI에서 해당 새 객체를 볼 수 있습니다.

Unified Manager는 모니터링되는 모든 클러스터에서 5분마다 현재 _성능 통계_를 수집합니다. 이 데이터를 분석하여 성능 이벤트와 잠재적인 문제를 식별합니다. 5분 단위의 과거 성과 데이터를 30일 동안 보관하고, 1시간 단위의 과거 성과 데이터를 180일 동안 보관합니다. 이를 통해 현재 달의 매우 세부적인 성과 세부 정보와 최대 1년 동안의 일반적인 성과 추세를 볼 수 있습니다.

수집 폴링은 몇 분 간격으로 이루어지므로 모든 클러스터의 데이터가 동시에 전송되지 않아 성능에 영향을 미칠 수 있습니다.

다음 표에서는 Unified Manager가 수행하는 수집 활동을 설명합니다.

활동	시간 간격	설명
성과 통계 여론조사	5분마다	각 클러스터에서 실시간 성능 데이터를 수집합니다.
통계 분석	5분마다	모든 통계 폴링 후 Unified Manager는 수집된 데이터를 사용자 정의 임계값, 시스템 정의 임계값, 동적 임계값과 비교합니다. 성능 임계값이 초과되면 Unified Manager는 이벤트를 생성하고 지정된 사용자에게 이메일을 보냅니다(구성된 경우).
구성 폴	15분마다	각 클러스터에서 자세한 인벤토리 정보를 수집하여 모든 스토리지 개체 (노드, SVM, 볼륨 등)를 식별합니다.
요약	매 시간마다	최근 12개 5분 성과 데이터 수집을 시간당 평균으로 요약합니다. 시간당 평균 값은 일부 UI 페이지에서 사용되며 180일 동안 보관됩니다.
예측 분석 및 데이터 정리	매일 자정 이후	클러스터 데이터를 분석하여 향후 24시간 동안의 볼륨 지연 시간과 IOPS에 대한 동적 임계값을 설정합니다. 30일이 지난 5분 성능 데이터를 데이터베이스에서 삭제합니다.
데이터 정리	매일 오전 2시 이후	180일보다 오래된 이벤트와 180일보다 오래된 동적 임계값을 데이터베이스에서 삭제합니다.
데이터 정리	매일 오전 3시 30분 이후	180일이 지난 1시간 성능 데이터를 데이터베이스에서 삭제합니다.

데이터 연속성 수집 주기란 무엇입니까?

데이터 연속성 수집 주기는 기본적으로 5분마다 실행되는 실시간 클러스터 성능 수집 주기 외부에서 성능 데이터를 검색합니다. 데이터 연속성 수집을 통해 Unified Manager는 실시간 데이터를 수집하지 못했을 때 발생하는 통계 데이터 공백을 채울 수 있습니다.

Unified Manager는 다음 이벤트가 발생할 때 과거 성능 데이터에 대한 데이터 연속성 수집 폴링을 수행합니다.

- 클러스터는 처음에 Unified Manager에 추가됩니다.

Unified Manager는 지난 15일 동안의 과거 성능 데이터를 수집합니다. 이 기능을 사용하면 클러스터를 추가한 후 몇 시간 만에 해당 클러스터의 2주간의 과거 성능 정보를 볼 수 있습니다.

또한, 시스템에서 정의한 임계값 이벤트가 있으면 이전 기간에 대해 보고됩니다.

- 현재 성과 데이터 수집 주기가 예정대로 완료되지 않습니다.

실시간 성과 여론조사가 5분 수집 기간을 넘으면 누락된 정보를 수집하기 위해 데이터 연속성 수집 주기가 시작됩니다. 데이터 연속성 수집이 없으면 다음 수집 기간이 건너뛰니다.

- Unified Manager에 일정 시간 동안 액세스할 수 없다가 다음과 같은 상황에서 다시 온라인 상태로 돌아오는 경우가 있습니다.
 - 다시 시작되었습니다.
 - 소프트웨어 업그레이드 중이나 백업 파일을 생성하는 중에 종료되었습니다.
 - 네트워크 중단이 복구되었습니다.
- 다음 상황처럼 클러스터에 일정 시간 동안 액세스할 수 없다가 다시 온라인 상태로 돌아오는 경우가 있습니다.
 - 네트워크 중단이 복구되었습니다.
 - 광역 네트워크 연결 속도가 느려서 정상적인 성능 데이터 수집이 지연되었습니다.

데이터 연속성 수집 주기는 최대 24시간 분량의 과거 데이터를 수집할 수 있습니다. Unified Manager가 24시간 이상 다운되면 UI 페이지에 성능 데이터에 차이가 나타납니다.

데이터 연속성 수집 주기와 실시간 데이터 수집 주기는 동시에 실행할 수 없습니다. 실시간 성능 데이터 수집이 시작되기 전에 데이터 연속성 수집 주기가 완료되어야 합니다. 1시간 이상의 과거 데이터를 수집하기 위해 데이터 연속성 수집이 필요한 경우 알림 창 상단에 해당 클러스터에 대한 배너 메시지가 표시됩니다.

수집된 데이터 및 이벤트에서 타임스탬프가 의미하는 것

수집된 상태 및 성능 데이터에 나타나는 타임스탬프나 이벤트 감지 시간으로 나타나는 타임스탬프는 ONTAP 클러스터 시간을 기준으로 하며, 웹 브라우저에 설정된 표준 시간대에 맞춰 조정됩니다.

Unified Manager 서버, ONTAP 클러스터 및 웹 브라우저의 시간을 동기화하려면 NTP(네트워크 시간 프로토콜) 서버를 사용하는 것이 좋습니다.



특정 클러스터에 대해 잘못된 타임스탬프가 표시되는 경우 클러스터 시간이 올바르게 설정되었는지 확인하는 것이 좋습니다.

Unified Manager GUI에서 성능 워크플로 탐색

Unified Manager 인터페이스는 성능 정보를 수집하고 표시하기 위한 여러 페이지를 제공합니다. GUI의 페이지로 이동하려면 왼쪽 탐색 패널을 사용하고, 페이지의 탭과 링크를 사용하여 정보를 보고 구성합니다.

다음 페이지를 모두 사용하여 클러스터 성능 정보를 모니터링하고 문제를 해결할 수 있습니다.

- 대시보드 페이지
- 저장소 및 네트워크 개체 인벤토리 페이지
- 스토리지 개체 세부 정보 페이지(성능 탐색기 포함)
- 구성 및 설정 페이지
- 이벤트 페이지

UI에 로그인

지원되는 웹 브라우저를 사용하여 Unified Manager UI에 로그인할 수 있습니다.

시작하기 전에

- 웹 브라우저는 최소 요구 사항을 충족해야 합니다.

상호 운용성 매트릭스를 참조하세요. "mysupport.netapp.com/매트릭스" 지원되는 브라우저 버전의 전체 목록을 확인하세요.

- Unified Manager 서버의 IP 주소 또는 URL이 있어야 합니다.

1시간 동안 활동이 없으면 자동으로 세션에서 로그아웃됩니다. 이 기간은 일반 > *기능 설정*에서 구성할 수 있습니다.

단계

1. 웹 브라우저에 URL을 입력합니다. 여기서 URL은 Unified Manager 서버의 IP 주소 또는 정규화된 도메인 이름(FQDN)입니다.
 - IPv4의 경우: `https://URL/`
 - IPv6의 경우: `https://[URL]/`

서버가 자체 서명된 디지털 인증서를 사용하는 경우 브라우저에 해당 인증서를 신뢰할 수 없다는 경고가 표시될 수 있습니다. 위험을 인정하고 계속 접근하거나, 서버 인증을 위해 인증 기관(CA) 서명 디지털 인증서를 설치할 수 있습니다. 로그인 화면에서 사용자 이름과 비밀번호를 입력하세요.

Unified Manager 사용자 인터페이스에 대한 로그인이 SAML 인증을 사용하여 보호되는 경우 Unified Manager 로그인 페이지 대신 ID 공급자(IdP) 로그인 페이지에 자격 증명을 입력하게 됩니다.

대시보드 페이지가 표시됩니다.



Unified Manager 서버가 초기화되지 않은 경우 새 브라우저 창에 첫 번째 경험 마법사가 표시됩니다. 이메일 알림을 보낼 초기 이메일 수신자, 이메일 통신을 처리할 SMTP 서버, AutoSupport Unified Manager 설치에 대한 정보를 기술 지원팀에 보낼 수 있는지 여부를 입력해야 합니다. 이 정보를 완료하면 Unified Manager UI가 나타납니다.

그래픽 인터페이스 및 탐색 경로

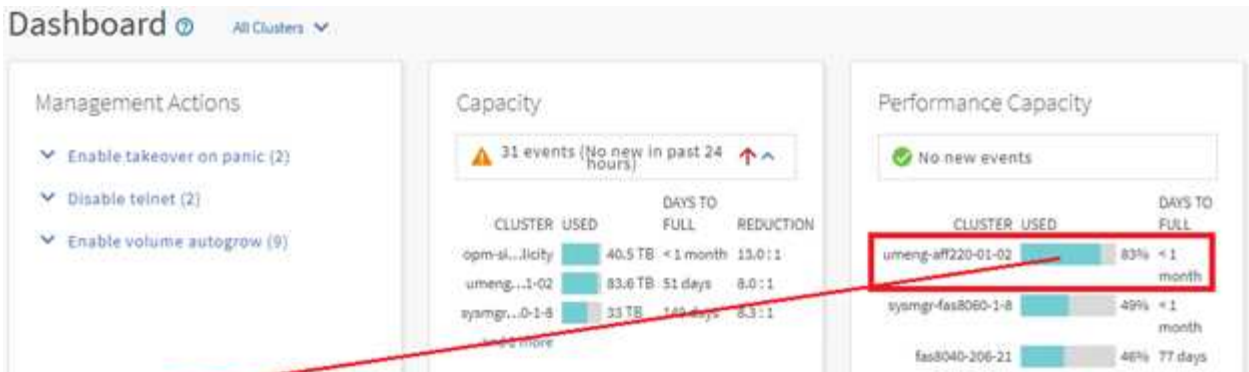
Unified Manager는 뛰어난 유연성을 제공하며 다양한 방법으로 여러 작업을 완료할 수 있습니다. Unified Manager에서 작업하는 동안 다양한 탐색 경로를 발견하게 될 것입니다. 가능한 모든 탐색 조합을 보여드릴 수는 없지만, 몇 가지 일반적인 시나리오는 알고 있어야 합니다.

Unified Manager가 관리하는 모든 클러스터의 모든 개체의 성능을 모니터링할 수 있습니다. 스토리지 객체를 모니터링하면 클러스터 및 객체 성능에 대한 개요를 얻을 수 있으며, 성능 이벤트 모니터링도 포함됩니다. 성능과 이벤트를 높은 수준에서 볼 수도 있고, 개체 성능과 성능 이벤트에 대한 세부 정보를 추가로 조사할 수도 있습니다.

다음은 가능한 여러 클러스터 개체 탐색의 한 예입니다.

1. 대시보드 페이지에서 성능 용량 패널의 세부 정보를 검토하여 가장 많은 성능 용량을 사용하는 클러스터를 식별하고 막대형 차트를 클릭하여 해당 클러스터의 노드 목록으로 이동합니다.
2. 가장 높은 성능 용량 사용 값을 갖는 노드를 찾아 해당 노드를 클릭합니다.
3. 노드/성능 탐색기 페이지에서 보기 및 비교 메뉴에서 *이 노드의 집계*를 클릭합니다.
4. 가장 많은 성능 용량을 사용하는 집계를 식별하고 해당 집계를 클릭합니다.
5. 집계/성능 탐색기 페이지에서 보기 및 비교 메뉴의 *이 집계의 볼륨*을 클릭합니다.
6. 가장 많은 IOPS를 사용하는 볼륨을 식별합니다.

이러한 볼륨을 조사하여 QoS 정책이나 성능 서비스 수준 정책을 적용해야 하는지, 아니면 정책 설정을 변경해야 하는지 확인해야 합니다. 이렇게 하면 해당 볼륨이 클러스터에서 너무 많은 비율의 IOPS를 사용하지 않게 됩니다.



Nodes

Last updated: Nov 15, 2019, 10:48 AM

VIEW: Nodes on umeng-aff220-01-02 Search Nodes Filter Hardware Inventory Report

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports Show/Hide

Status	Node	Latency	IOPS	MB/s	Performance Capacity Used	Utilization	Fr
✖	umeng-aff220-01	21.7 ms/op	27,333 IOPS	211 MB/s	73%	50%	3.1
✖	umeng-aff220-02	8.33 ms/op	83.4 IOPS	102 MB/s	53%	42%	6.1

Node / Performance : umeng-aff220-01

Summary Explorer Failover Planning Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Aggregates on this Node Filter

Aggregate	Latency	IOPS	MB/s	Perf...
NSLM12_002	12.4 ...	47.51...	5.6 M...	11%
NSLM12_001	11.4 ...	216 L...	4.33 ...	5%

Comparing 0 Additional Objects

umeng-aff220-01

Aggregate / Performance : NSLM12_002

Summary Explorer Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Volumes on this Aggregate Filter

Volume	Latency	IOPS	MB/s
suchita_vmware_d...	6.38 ms...	76.8 IOPS	2.55 MB/s
suchita_vmware_d...	5.82 ms...	4,775 L...	18.7 MB/s
aiqum_scale_do_no...	0.114 m...	< 1 IOPS	< 1 MB/s

Comparing 0 Additional Objects

NSLM12_002

클러스터 성능 탐색 모니터링

Unified Manager에서 관리하는 모든 클러스터의 성능을 모니터링할 수 있습니다. 클러스터를 모니터링하면 클러스터 및 개체 성능에 대한 개요를 얻을 수 있으며 성능 이벤트 모니터링도 포함됩니다. 성능과 이벤트를 높은 수준에서 볼 수 있으며, 클러스터와 개체 성능 및 성능 이벤트에 대한 세부 정보를 추가로 조사할 수 있습니다.

다음은 가능한 여러 클러스터 성능 탐색 경로 중 한 가지 예입니다.

1. 왼쪽 탐색 창에서 저장소 > *집계*를 클릭합니다.

2. 해당 집계의 성과에 대한 정보를 보려면 성과: 모든 집계 보기를 선택하세요.
3. 조사하려는 집계를 식별하고 해당 집계 이름을 클릭하여 집계/성능 탐색기 페이지로 이동합니다.
4. 선택적으로, 보기 및 비교 메뉴에서 이 집계와 비교할 다른 객체를 선택한 다음, 객체 중 하나를 비교 창에 추가합니다.

두 객체에 대한 통계는 비교를 위해 카운터 차트에 표시됩니다.

5. Explorer 페이지의 오른쪽에 있는 비교 창에서 카운터 차트 중 하나에서 *확대 보기*를 클릭하면 해당 집계에 대한 성과 기록에 대한 세부 정보를 볼 수 있습니다.

Aggregates

Last updated: Nov 15, 2019, 1:18 PM

VIEW **Performance: All Aggregates** Search Aggregates Filter

Assign Performance Threshold Policy

Clear Performance Threshold Policy

Scheduled Reports



Show / Hide

☐	Status	Aggregate	Type	Latency	IOPS	MB/s	Performance Capacity Used	Utilization
☐	!	aggr_evt	SSD	0.29 ms/op	3.79 IOPS	< 1 MB/s	< 1%	< 1%
☐	!	aggr4	HDD	5.74 ms/op	14.4 IOPS	1.31 MB/s	6%	5%
☐	!	aggr3	HDD	5.06 ms/op	3.06 IOPS	< 1 MB/s	6%	5%
☐	!	meg_aggr2	HDD	10.4 ms/op	52.9 IOPS	7.28 MB/s	3%	2%

Aggregate / Performance : aggr4

Switch to Health View Last updated: Nov 15, 2019, 1:20 PM

Summary

Explorer

Information

Compare the performance of associated objects and display detailed charts

TIME RANGE Last 72 Hours

VIEW AND COMPARE

Aggregates on same Node

Filter

Aggregate	Latency	IOPS	MB/s	Perf...	
aggr3	5.06 ...	3.06 ...	< 1 M...	6%	
aggr_evt	0.29 ...	3.79 ...	< 1 M...	< 1%	Add
aggr_automation	0.27 ...	6.35 ...	< 1 M...	< 1%	Add

Comparing

1 Additional Object

X

aggr4

aggr3

CHOOSE CHARTS 7 Charts Selected

Events for Aggregate: aggr4



No data to display

Latency

VIEW Total

Zoom View

Latency - Total view (ms/op)



Latency for Aggregate: aggr4

Last updated: Nov 15, 2019, 1:23 PM

Event Timeline: aggr4

TIME RANGE Last 72 Hours



Critical Events



Error Events



Warning Events



Information Events



No data to display

Comparing Objects

aggr4

aggr3

25 ms/op

20

15

10

5

0

Latency - Total view (ms/op)

aggr4

aggr3

Nov 14, 2019, 1:24 AM

4.25

3.97

Nov 15, 2019, 12:00 AM Nov 15, 2019, 12:00 PM Nov 14, 2019, 12:00 AM Nov 14, 2019, 12:00 PM Nov 15, 2019, 12:00 AM Nov 15, 2019, 12:00 PM

Unified Manager 이벤트 세부 정보 페이지는 모든 성능 이벤트를 심층적으로 살펴볼 수 있는 기능을 제공합니다. 이 기능은 성능 이벤트를 조사할 때, 문제를 해결할 때, 시스템 성능을 미세 조정할 때 유용합니다.

공연 이벤트의 유형에 따라 두 가지 유형의 이벤트 세부 정보 페이지 중 하나가 표시될 수 있습니다.

- 사용자 정의 및 시스템 정의 임계값 정책 이벤트에 대한 이벤트 세부 정보 페이지
- 동적 임계값 정책 이벤트에 대한 이벤트 세부 정보 페이지

이는 이벤트 조사 탐색의 한 예입니다.

1. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭합니다.
2. 보기 메뉴에서 *활성 성과 이벤트*를 클릭합니다.
3. 조사하려는 이벤트의 이름을 클릭하면 이벤트 세부 정보 페이지가 표시됩니다.
4. 이벤트 설명을 보고 제안된 작업(사용 가능한 경우)을 검토하여 문제를 해결하는 데 도움이 될 수 있는 이벤트에 대한 자세한 내용을 확인하세요. 작업량 분석 버튼을 클릭하면 문제를 더욱 자세히 분석하는 데 도움이 되는 자세한 성능 차트가 표시됩니다.

Event Management

Last updated: Nov 15, 2019, 11:23 AM

VIEW **Active performance events** Search Events Filter +

Assign To Acknowledge Mark as Resolved Add Alert

Show / Hide

Triggered Time	Severity	State	Impact Lev	Impact Area	Name	Source	Source Ty
Nov 14, 2019, 11:39 AM	Warning	New	Risk	Performance	QoS Volume Peak IOPS... Threshold Breached	vs7:/julia_feb12_vol3	Volume
Nov 14, 2019, 11:39 AM	Warning	New	Risk	Performance	QoS Volume Peak IOPS... Threshold Breached	vs7:/julia_non_shared_3	Volume
Nov 15, 2019, 5:04 AM	Warning	New	Risk	Performance	QoS Volume Peak IOPS... Threshold Breached	suchita_vmwvar...nt_delete_01	Volume
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency...Service Level Policy	iscsi_boot/ia.../ocum-c220-01	LUN
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency...Service Level Policy	iscsi_boot/ia.../ocum-c220-07	LUN

Event: QoS Volume Peak IOPS/TB Warning Threshold Breached

(Last Seen: Nov 15, 2019, 11:19 AM)

IOPS value of 570 IOPS on policy group NSLM_vs7_Performance_2_0 has triggered a WARNING event to identify performance problems for the workloads in this policy group.



Actions

Suggested Actions to Fix The Issue

Troubleshoot

Analyze Workload

Take Action

This is an Adaptive QoS Policy that might be used by other workloads in the system.

If it is acceptable that changes you make to the QoS setting will be applied to other workloads that are using this policy,

- Increase the threshold to 4950 IOPS/TB for this Adaptive QoS Policy.

If you are satisfied with the current limitation on workload throughput

- Leave the QoS configuration setting as it is.

Event Information

EVENT TRIGGER TIME	SEVERITY	SOURCE
Nov 14, 2019, 11:39 AM	Warning	vs7:/julia_non_shared_3
STATE	IMPACT LEVEL	SOURCE TYPE
New	Risk	Volume
EVENT DURATION	IMPACT AREA	ION CLUSTER
1 day 40 minutes	Performance	ocum-mobility-01-02
LAST SEEN		AFFECTED OBJECTS COUNT
Nov 15, 2019, 11:19 AM		1
		TRIGGERED POLICY
		QoS Peak IOPS/TB threshold

저장소 객체 검색

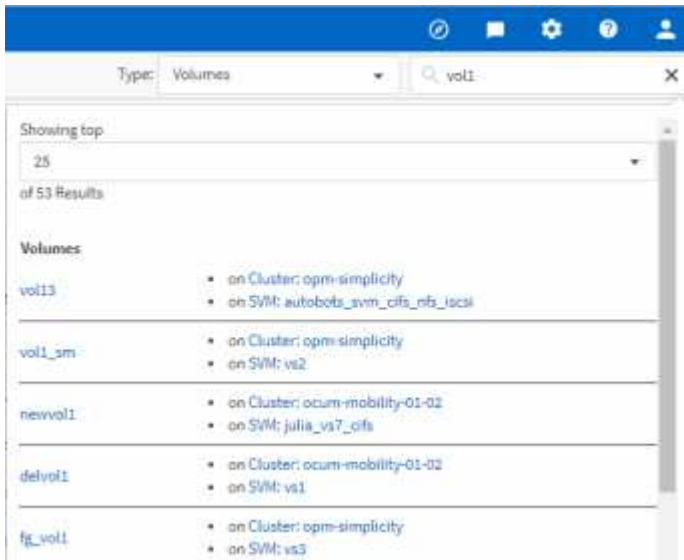
특정 객체에 빠르게 액세스하려면 메뉴 막대 상단의 모든 저장소 객체 검색 필드를 사용하면 됩니다. 모든 개체에 대한 글로벌 검색 방법을 사용하면 유형별로 특정 개체를 빠르게 찾을 수 있습니다. 검색 결과는 스토리지 객체 유형별로 정렬되며 드롭다운 메뉴를 사용하여 필터링할 수 있습니다. 유효한 검색에는 최소 3개의 문자가 포함되어야 합니다.

글로벌 검색에서는 전체 결과 수가 표시되지만, 상위 25개 검색 결과에만 접근할 수 있습니다. 이러한 이유로 글로벌 검색 기능은 빠르게 찾고 싶은 항목을 알고 있다면 특정 항목을 찾는 단축 도구로 생각할 수 있습니다. 완전한 검색

결과를 얻으려면 객체 인벤토리 페이지의 검색과 관련 필터링 기능을 사용하세요.

드롭다운 상자를 클릭하고 전체*를 선택하면 모든 개체와 이벤트를 동시에 검색할 수 있습니다. 또는 드롭다운 상자를 클릭하여 개체 유형을 지정할 수 있습니다. *모든 저장소 개체 검색 필드에 개체 또는 이벤트 이름을 최소 3자 이상 입력한 다음, **Enter** 키를 누르면 다음과 같은 검색 결과가 표시됩니다.

- 클러스터: 클러스터 이름
- 노드: 노드 이름
- 집계: 집계 이름
- SVM: SVM 이름
- 볼륨: 볼륨 이름
- LUN: LUN 경로



LIF와 포트는 글로벌 검색창에서 검색할 수 없습니다.

이 예에서는 드롭다운 상자에 볼륨 개체 유형이 선택되어 있습니다. 모든 저장소 개체 검색 필드에 "vol"을 입력하면 해당 문자가 포함된 이름을 가진 모든 볼륨 목록이 표시됩니다. 객체 검색의 경우, 검색 결과를 클릭하면 해당 객체의 성능 탐색기 페이지로 이동할 수 있습니다. 이벤트 검색의 경우, 검색 결과에서 항목을 클릭하면 이벤트 세부 정보 페이지로 이동합니다.

필터 인벤토리 페이지 콘텐츠

Unified Manager에서 인벤토리 페이지 데이터를 필터링하여 특정 기준에 따라 데이터를 빠르게 찾을 수 있습니다. 필터링을 사용하면 Unified Manager 페이지의 내용을 좁혀 관심 있는 결과만 표시할 수 있습니다. 이 방법은 귀하가 관심 있는 데이터만 표시하는 매우 효율적인 방법입니다.

*필터링*을 사용하여 기본 설정에 따라 그리드 보기를 사용자 지정하세요. 사용 가능한 필터 옵션은 그리드에 표시되는 개체 유형에 따라 달라집니다. 현재 필터가 적용되어 있는 경우, 적용된 필터의 수가 필터 버튼 오른쪽에 표시됩니다.

세 가지 유형의 필터 매개변수가 지원됩니다.

매개변수	확인
문자열(텍스트)	연산자는 포함, 시작, 끝남, *포함하지 않음*입니다.
숫자	연산자는 보다 크다, 보다 작다, 마지막에, *사이에*입니다.
열거형(텍스트)	연산자는 *is*와 *is not*입니다.

각 필터에는 열, 연산자, 값 필드가 필요합니다. 사용 가능한 필터는 현재 페이지에서 필터링 가능한 열을 반영합니다. 적용할 수 있는 필터의 최대 개수는 4개입니다. 필터링된 결과는 결합된 필터 매개변수를 기반으로 합니다. 필터링된 결과는 현재 표시된 페이지뿐만 아니라 필터링된 검색의 모든 페이지에 적용됩니다.

필터링 패널을 사용하여 필터를 추가할 수 있습니다.

1. 페이지 상단에서 필터 버튼을 클릭하세요. 필터링 패널이 표시됩니다.
2. 왼쪽 드롭다운 목록을 클릭하고 개체를 선택합니다. 예를 들어, _Cluster_나 성능 카운터를 선택합니다.
3. 가운데 드롭다운 목록을 클릭하고 사용할 연산자를 선택하세요.
4. 마지막 목록에서 값을 선택하거나 입력하여 해당 개체에 대한 필터를 완성합니다.
5. 다른 필터를 추가하려면 +필터 추가*를 클릭하세요. 추가 필터 필드가 표시됩니다. 이전 단계에서 설명한 프로세스를 사용하여 이 필터를 완료합니다. 네 번째 필터를 추가하면 *+필터 추가 버튼이 더 이상 표시되지 않습니다.
6. *필터 적용*을 클릭하세요. 필터 옵션은 그리드에 적용되고 필터 수는 필터 버튼 오른쪽에 표시됩니다.
7. 필터링 패널을 사용하여 제거할 필터 오른쪽에 있는 휴지통 아이콘을 클릭하여 개별 필터를 제거합니다.
8. 모든 필터를 제거하려면 필터링 패널 하단의 *재설정*을 클릭하세요.

필터링 예제

이 그림은 세 개의 필터가 있는 필터링 패널을 보여줍니다. 필터가 최대 4개보다 적을 경우 +필터 추가 버튼이 표시됩니다.

The screenshot shows a filter panel with three active filters. Each filter consists of a field dropdown, an operator dropdown, and a value input field. The first filter is 'MBps' with operator 'greater than' and value '5'. The second filter is 'Node' with operator 'name starts with' and value 'test'. The third filter is 'Type' with operator 'is' and value 'FCP Port'. To the right of each filter is a trash icon for removal. At the bottom left is a '+ Add Filter' button. At the bottom right are 'Cancel' and 'Apply Filter' buttons.

*필터 적용*을 클릭하면 필터링 패널이 닫히고 필터가 적용되며 적용된 필터 수가 표시됩니다(3).

대시보드에서 클러스터 성능 모니터링

Unified Manager 대시보드는 Unified Manager 인스턴스에서 모니터링하는 모든 클러스터의 높은 수준의 성능 상태를 표시하는 몇 개의 패널을 제공합니다. 관리되는 클러스터의 전반적인 성능을 평가하고, 식별된 특정 이벤트를 빠르게 기록, 찾거나 해결을 위해 할당할 수 있습니다.

대시보드의 성능 패널 이해하기

Unified Manager 대시보드는 사용자 환경에서 모니터링되는 모든 클러스터의 높은 수준의 성능 상태를 표시하는 몇 가지 패널을 제공합니다. 모든 클러스터 또는 개별 클러스터의 상태를 볼 수 있습니다.

대부분의 패널은 성과 정보를 표시하는 것 외에도 해당 카테고리의 활성 이벤트 수와 지난 24시간 동안 추가된 새 이벤트 수도 표시합니다. 이 정보는 보고된 이벤트를 해결하기 위해 추가적으로 분석해야 할 클러스터를 결정하는 데 도움이 됩니다. 이벤트를 클릭하면 상위 몇 개의 이벤트가 표시되고, 해당 카테고리의 이벤트를 표시하도록 필터링된 이벤트 관리 인벤토리 페이지로 연결되는 링크가 제공됩니다.

다음 패널은 성과 상태를 제공합니다.

- 성능 용량 패널

모든 클러스터를 볼 때 이 패널에는 각 클러스터의 성능 용량 값(지난 1시간 동안의 평균)과 성능 용량이 상한에 도달할 때까지 걸리는 일수(일일 성장률 기준)가 표시됩니다. 막대형 차트를 클릭하면 해당 클러스터의 노드 인벤토리 페이지로 이동합니다. 노드 인벤토리 페이지에는 지난 72시간 동안의 평균 성능 용량이 표시되므로 이 값이 대시보드 값과 일치하지 않을 수 있습니다.

단일 클러스터를 볼 때 이 패널에는 클러스터 성능 용량, 총 IOPS 및 총 처리량 값이 표시됩니다.

- 워크로드 IOPS 패널

워크로드 활성 관리가 활성화되어 있고 단일 클러스터를 보고 있는 경우, 이 패널에는 현재 특정 IOPS 범위에서 실행 중인 총 워크로드 수가 표시됩니다.

- 작업 부하 성능 패널

워크로드 활성 관리가 활성화된 경우 이 패널에는 정의된 각 성능 서비스 수준에 할당된 적합 및 비적합 워크로드의 총 수가 표시됩니다. 막대형 차트를 클릭하면 작업 부하 페이지에서 해당 정책에 할당된 작업 부하로 이동합니다.

- 사용 개요 패널

모든 클러스터를 볼 때 가장 높은 IOPS 또는 처리량(MB/초)을 기준으로 클러스터를 정렬하여 볼 수 있습니다.

단일 클러스터를 볼 때 해당 클러스터의 작업 부하를 가장 높은 IOPS 또는 처리량(MB/초)을 기준으로 정렬하여 볼 수 있습니다.

성능 배너 메시지 및 설명

Unified Manager는 특정 클러스터의 상태 문제를 경고하기 위해 알림 페이지(알림 벨)에 배너 메시지를 표시할 수 있습니다.

배너 메시지	설명	해결
No performance data is being collected from cluster <code>cluster_name</code> . Restart Unified Manager to correct this issue.	Unified Manager 수집 서비스가 중지되어 어떤 클러스터에서도 성능 데이터가 수집되지 않습니다.	이 문제를 해결하려면 Unified Manager를 다시 시작하세요. 그래도 문제가 해결되지 않으면 기술 지원팀에 문의하세요.
More than x hour(s) of historical data is being collected from cluster <code>cluster_name</code> . Current data collections will start after all historical data is collected.	실시간 클러스터 성능 수집 주기 외부에서 성능 데이터를 검색하기 위해 데이터 연속성 수집 주기가 현재 실행 중입니다.	아무런 조치도 필요하지 않습니다. 데이터 연속성 수집 주기가 완료된 후 현재 성과 데이터가 수집됩니다. 데이터 연속성 수집 주기는 새로운 클러스터가 추가되거나 Unified Manager가 어떤 이유로 현재 성능 데이터를 수집하지 못하는 경우 실행됩니다.

성능 통계 수집 간격 변경

성능 통계의 기본 수집 간격은 5분입니다. 대규모 클러스터의 컬렉션이 기본 시간 내에 완료되지 않는 경우 이 간격을 10분 또는 15분으로 변경할 수 있습니다. 이 설정은 Unified Manager 인스턴스가 모니터링하는 모든 클러스터의 통계 수집에 영향을 미칩니다.

시작하기 전에

Unified Manager 서버의 유지 관리 콘솔에 로그인하려면 권한이 있는 사용자 ID와 비밀번호가 있어야 합니다.

성능 통계 수집이 제때 완료되지 않는 문제는 배너 메시지로 표시됩니다. Unable to consistently collect from cluster <cluster_name> 또는 Data collection is taking too long on cluster <cluster_name>.

통계 수집 문제로 인해 필요한 경우에만 수집 간격을 변경해야 합니다. 다른 이유로는 이 설정을 변경하지 마세요.



기본 설정인 5분에서 이 값을 변경하면 Unified Manager에서 보고하는 성능 이벤트의 수와 빈도에 영향을 미칠 수 있습니다. 예를 들어, 시스템에서 정의한 성능 임계값은 정책을 30분 동안 초과하면 이벤트를 트리거합니다. 5분 수집을 사용하는 경우, 해당 정책을 6회 연속으로 초과해야 합니다. 15분 간격 수거의 경우, 해당 정책은 두 번의 수거 기간 동안만 초과될 수 있습니다.

클러스터 설정 페이지 하단의 메시지는 현재 통계 데이터 수집 간격을 나타냅니다.

단계

1. SSH를 사용하여 Unified Manager 호스트에 유지 관리 사용자로 로그인합니다.

Unified Manager 유지 관리 콘솔 프롬프트가 표시됩니다.

2. *성능 폴링 간격 구성*이라고 표시된 메뉴 옵션의 번호를 입력한 다음 Enter 키를 누릅니다.
3. 메시지가 표시되면 유지 관리 사용자 비밀번호를 다시 입력하세요.
4. 설정하려는 새로운 폴링 간격에 대한 숫자를 입력한 다음 Enter를 누릅니다.

Unified Manager 수집 간격을 10분 또는 15분으로 변경하고 외부 데이터 공급자(예: Graphite)에 현재 연결되어 있는 경우, 데이터 공급자 전송 간격을 Unified Manager 수집 간격보다 크거나 같도록 변경해야 합니다.

워크로드 분석기를 사용하여 워크로드 문제 해결

워크로드 분석기는 문제 해결을 지원하기 위해 단일 워크로드에 대한 중요한 상태 및 성능 기준을 단일 페이지에서 볼 수 있는 방법을 제공합니다. 워크로드에 대한 현재 및 과거 이벤트를 모두 확인하면 워크로드에 현재 성능이나 용량 문제가 발생한 이유를 더 잘 파악할 수 있습니다.

이 도구를 사용하면 애플리케이션 성능 문제의 원인이 저장소인지, 아니면 네트워킹이나 기타 관련 문제로 인해 문제가 발생하는지 확인하는 데도 도움이 됩니다.

사용자 인터페이스의 다양한 위치에서 이 기능을 시작할 수 있습니다.

- 왼쪽 탐색 메뉴의 작업 부하 분석 선택에서
- 이벤트 세부 정보 페이지에서 작업량 분석 버튼을 클릭합니다.
- 모든 작업 인벤토리 페이지(볼륨, LUN, 작업, NFS 공유 또는 SMB/CIFS 공유)에서 추가 아이콘을 클릭하여 , 그런 다음 작업량 분석
- Datastore 개체에서 작업 부하 분석 버튼을 클릭하여 가상 머신 페이지에서

왼쪽 탐색 메뉴에서 도구를 실행하면 분석하려는 작업 부하의 이름을 입력하고 문제를 해결하려는 시간 범위를 선택할 수 있습니다. 워크로드 또는 가상 머신 인벤토리 페이지에서 도구를 실행하면 워크로드 이름이 자동으로 채워지고 워크로드 데이터가 기본 2시간 범위로 표시됩니다. 이벤트 세부 정보 페이지에서 도구를 실행하면 작업 부하 이름이 자동으로 입력되고 10일 동안의 데이터가 표시됩니다.

워크로드 분석기는 어떤 데이터를 표시합니까?

워크로드 분석기 페이지에는 워크로드에 영향을 줄 수 있는 현재 이벤트에 대한 정보, 이벤트를 발생시킨 문제를 해결하기 위한 권장 사항, 성능 및 용량 기록을 분석하기 위한 차트가 표시됩니다.

페이지 상단에서 분석하려는 작업 부하(볼륨 또는 LUN)의 이름과 통계를 보고자 하는 기간을 지정합니다. 원하는 경우 언제든지 기간을 변경하여 더 짧거나 긴 기간을 볼 수 있습니다.

페이지의 다른 영역에는 분석 결과, 성능 및 용량 차트가 표시됩니다.



LUN에 대한 작업 부하 차트는 볼륨에 대한 차트와 동일한 수준의 통계를 제공하지 않으므로 이 두 가지 유형의 작업 부하를 분석할 때 차이점을 알 수 있습니다.

• 이벤트 요약 영역

특정 기간 동안 발생한 이벤트의 수와 유형에 대한 간략한 개요를 표시합니다. 다양한 영향 영역(예: 성능 및 용량)에서 이벤트가 발생하는 경우, 관심 있는 이벤트 유형에 대한 세부 정보를 선택할 수 있도록 이 정보가 표시됩니다. 이벤트 유형을 클릭하면 이벤트 이름 목록이 표시됩니다.

해당 기간 동안 이벤트가 하나만 있는 경우, 일부 이벤트에 대해 문제를 해결하기 위한 권장 사항 목록이 나열됩니다.

• 이벤트 타임라인

지정된 기간 동안 발생한 모든 이벤트를 표시합니다. 각 이벤트 위에 커서를 올려 놓으면 이벤트 이름을 볼 수 있습니다.

이벤트 세부 정보 페이지에서 작업량 분석 버튼을 클릭하여 이 페이지에 도달한 경우 선택한 이벤트의 아이콘이 더 크게 표시되어 이벤트를 식별할 수 있습니다.

• 성능 차트 영역

선택한 시간대에 따라 지연 시간, 처리량(IOPS와 MB/s 모두), 사용률(노드와 집계 모두)에 대한 차트를 표시합니다. 추가 분석을 수행하려는 경우 작업 부하에 대한 성능 탐색기 페이지를 표시하려면 성능 세부 정보 보기 링크를 클릭하세요.

- *대기 시간*은 선택한 기간 동안 작업 부하에 대한 대기 시간을 표시합니다. 차트에는 다음 내용을 볼 수 있는 세 가지 보기가 있습니다.
 - 전체 지연 시간
 - 분류 대기 시간(읽기, 쓰기 및 기타 프로세스로 구분)
 - 클러스터 구성 요소 지연 시간(클러스터 구성 요소별로 구분)

보다 "클러스터 구성 요소와 이들이 경쟁에 참여할 수 있는 이유" 여기에 표시되는 클러스터 구성 요소에 대한 설명은 다음과 같습니다. 처리량*은 선택한 기간 동안 작업 부하에 대한 **IOPS**와 **MB/s** 처리량을 모두 표시합니다. 차트에는 다음을 볼 수 있는 4가지 뷰가 있습니다. 전체 처리량 * 세부 처리량(읽기, 쓰기 및 기타 프로세스로 구분) * 클라우드 처리량(클라우드에 데이터를 쓰고 클라우드에서 데이터를 읽는 데 사용되는 MB/s. 클라우드에 용량을 계층화하는 워크로드의 경우) * 예측을 포함한 **IOPS**(해당 기간 동안 상한 및 하한 **IOPS** 처리량 값이 어떻게 될지에 대한 예측) 이 차트에는 구성된 경우 **QoS**(서비스 품질) 최대 및 최소 처리량 임계값 설정도 표시되므로 시스템이 **QoS** 정책을 사용하여 의도적으로 처리량을 제한하는 위치를 확인할 수 있습니다. *사용률*은 선택한 기간 동안 워크로드가 실행되는 집계 및 노드에 대한 사용률을 표시합니다. 여기에서 집계나 노드가 과도하게 사용되어 지연 시간이 길어지는지 확인할 수 있습니다. FlexGroup 볼륨을 분석하면 활용도 차트에 여러 노드와 여러 집계가 나열됩니다.

• 수용 인원 차트 영역

지난 한 달 동안의 작업 부하에 대한 데이터 용량과 스냅샷 용량에 대한 차트를 표시합니다.

볼륨의 경우, 추가 분석을 수행하려는 경우 작업 부하에 대한 상태 세부 정보 페이지를 표시하려면 용량 세부 정보 보기 링크를 클릭합니다. LUN에는 상태 세부 정보 페이지가 없으므로 LUN은 이 링크를 제공하지 않습니다.

- *용량 보기*는 작업 부하에 할당된 총 사용 가능 공간과 논리적으로 사용된 공간(모든 NetApp 최적화 후)을 표시합니다.
- *스냅샷 보기*는 스냅샷 복사본에 예약된 총 공간과 현재 사용 중인 공간의 양을 표시합니다. LUN은 스냅샷 보기를 제공하지 않습니다.
- *클라우드 계층 보기*는 로컬 성능 계층에서 얼마나 많은 용량이 사용되고 있는지, 그리고 클라우드 계층에서 얼마나 많은 용량이 사용되고 있는지를 표시합니다. 이러한 차트에는 해당 작업 부하에 대한 용량이 가득 차기까지 남은 시간에 대한 추정치가 포함되어 있습니다. 이 정보는 과거 사용 내역을 기반으로 하며 최소 10일 분의 데이터가 필요합니다. 남은 용량이 30일 미만이면 Unified Manager는 스토리지를 "거의 가득 참"으로 식별합니다.

워크로드 분석기는 언제 사용합니까?

일반적으로 워크로드 분석기는 사용자가 보고한 지연 문제를 해결하거나, 보고된 이벤트나 알림을 보다 철저히 분석하거나, 비정상적으로 작동하는 워크로드를 탐색하는 데 사용됩니다.

사용자가 사용 중인 애플리케이션이 매우 느리게 실행된다고 문의한 경우, 애플리케이션이 실행되는 작업 부하에 대한 대기 시간, 처리량 및 사용률 차트를 확인하여 스토리지가 성능 문제의 원인인지 확인할 수 있습니다. ONTAP 시스템에서 용량이 85% 이상 사용되면 성능 문제가 발생할 수 있으므로, 용량 차트를 사용하여 용량이 낮은지 확인할 수도 있습니다. 이러한 차트는 문제가 저장소로 인해 발생하는지, 네트워크이나 기타 관련 문제로 인해 발생하는지 확인하는 데 도움이 됩니다.

Unified Manager에서 성능 이벤트가 생성되었고 문제의 원인을 보다 자세히 검토하려는 경우 이벤트 세부 정보 페이지에서 워크로드 분석 버튼을 클릭하여 워크로드 분석기를 실행하여 워크로드에 대한 대기 시간, 처리량 및 용량 추세를 조사할 수 있습니다.

볼륨, LUN, 워크로드, NFS 공유 또는 SMB/CIFS 공유 등 워크로드 인벤토리 페이지를 볼 때 비정상적으로 작동하는 것으로 보이는 워크로드가 발견되는 경우 추가 아이콘을 클릭할 수 있습니다.  , *작업량 분석*을 클릭하면 작업량 분석 페이지가 열려 작업량을 자세히 살펴볼 수 있습니다.

워크로드 분석기를 사용하세요

사용자 인터페이스에서 워크로드 분석기를 시작하는 방법에는 여러 가지가 있습니다. 여기에서는 왼쪽 탐색 창에서 도구를 시작하는 방법을 설명합니다.

단계

1. 왼쪽 탐색 창에서 *작업 부하 분석*을 클릭합니다.

작업 부하 분석 페이지가 표시됩니다.

2. 작업 이름을 알고 있다면 이름을 입력하세요. 전체 이름이 확실하지 않은 경우 최소 3자를 입력하면 시스템이 해당 문자열과 일치하는 워크로드 목록을 표시합니다.
3. 기본 2시간보다 긴 시간 동안 통계를 보려면 시간 범위를 선택하고 *적용*을 클릭하세요.
4. 요약 영역에서 해당 기간 동안 발생한 이벤트를 확인하세요.
5. 성능 및 용량 차트를 보고 측정항목 중 비정상적인 항목이 있는지 확인하고 비정상적인 항목과 일치하는 이벤트가 있는지 확인하세요.

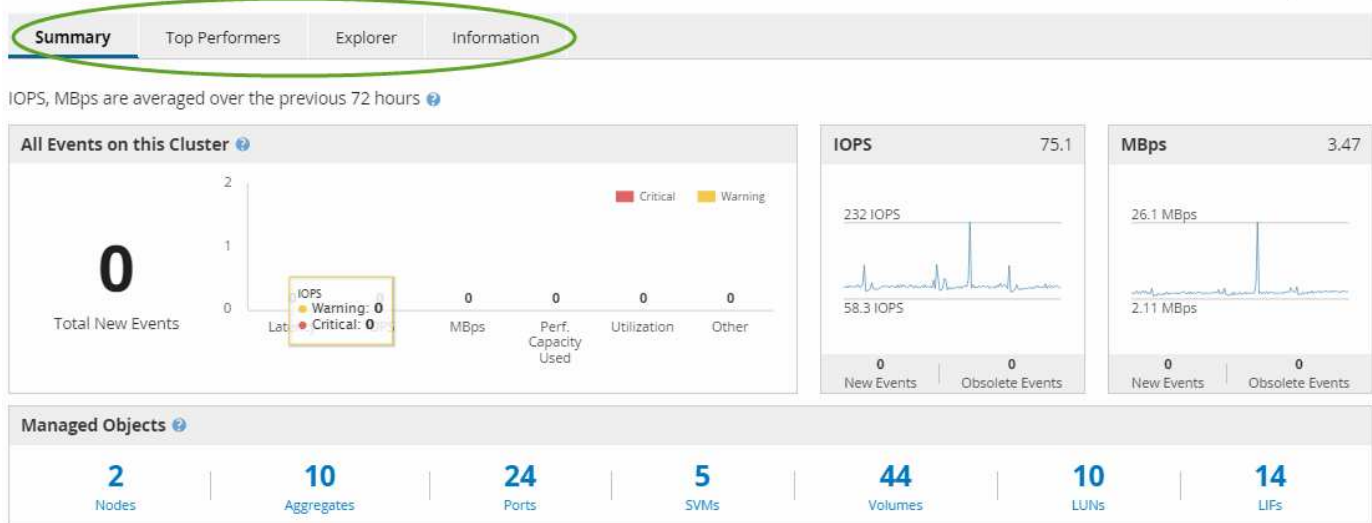
성능 클러스터 랜딩 페이지에서 클러스터 성능을 모니터링합니다.

성능 클러스터 랜딩 페이지에는 Unified Manager 인스턴스에서 모니터링 중인 선택된 클러스터의 상위 수준 성능 상태가 표시됩니다. 이 페이지를 사용하면 특정 클러스터의 전반적인 성능을 평가하고, 식별된 클러스터별 이벤트를 빠르게 기록, 찾거나 해결을 위해 할당할 수 있습니다.

성능 클러스터 랜딩 페이지 이해하기

성능 클러스터 랜딩 페이지는 선택한 클러스터의 성능 개요를 간략하게 제공하며, 특히 클러스터 내 상위 10개 개체의 성능 상태를 중점적으로 보여줍니다. 성능 문제는 이 클러스터의 모든 이벤트 패널의 페이지 상단에 표시됩니다.

성능 클러스터 랜딩 페이지는 Unified Manager 인스턴스에서 관리하는 각 클러스터에 대한 간략한 개요를 제공합니다. 이 페이지에서는 이벤트 및 성능에 대한 정보를 제공하고 클러스터를 모니터링하고 문제를 해결할 수 있습니다. 다음 이미지는 opm-mobility라는 클러스터의 성능 클러스터 랜딩 페이지의 예를 보여줍니다.



클러스터 요약 페이지의 이벤트 수가 성능 이벤트 인벤토리 페이지의 이벤트 수와 일치하지 않을 수 있습니다. 이는 클러스터 요약 페이지에서 조합 임계값 정책이 위반되었을 때 대기 시간 및 사용률 막대에 각각 하나의 이벤트가 표시되는 반면, 성능 이벤트 인벤토리 페이지에서는 조합 정책이 위반되었을 때 하나의 이벤트만 표시되기 때문입니다.



클러스터가 Unified Manager에서 관리에서 제외된 경우, 페이지 상단의 클러스터 이름 오른쪽에 제거된 상태가 표시됩니다.

성능 클러스터 랜딩 페이지

성능 클러스터 랜딩 페이지에는 선택한 클러스터의 상위 수준 성능 상태가 표시됩니다. 이 페이지에서는 선택한 클러스터의 스토리지 개체에 대한 각 성능 카운터의 전체 세부 정보에 액세스할 수 있습니다.

성능 클러스터 랜딩 페이지에는 클러스터 세부 정보를 4개 정보 영역으로 구분하는 4개의 탭이 있습니다.

- 요약 페이지
 - 클러스터 이벤트 창
 - MB/s 및 IOPS 성능 차트
 - 관리되는 개체 창
- 상위 성과자 페이지
- 탐색기 페이지
- 정보 페이지

성능 클러스터 요약 페이지

성능 클러스터 요약 페이지는 클러스터의 활성 이벤트, IOPS 성능, MB/s 성능에 대한 요약を提供합니다. 이 페이지에는 클러스터에 있는 스토리지 개체의 총 수도 포함되어 있습니다.

클러스터 성능 이벤트 창에는 클러스터의 성능 통계와 모든 활성 이벤트가 표시됩니다. 이 기능은 클러스터와 모든 클러스터 관련 성능 및 이벤트를 모니터링할 때 가장 유용합니다.

이 클러스터 창의 모든 이벤트

이 클러스터의 모든 이벤트 창에는 지난 72시간 동안의 모든 활성 클러스터 성능 이벤트가 표시됩니다. 총 활성 이벤트는 맨 왼쪽에 표시됩니다. 이 숫자는 이 클러스터의 모든 스토리지 개체에 대한 모든 새 이벤트와 확인된 이벤트의 총합을 나타냅니다. 총 활성 이벤트 링크를 클릭하면 이벤트 인벤토리 페이지로 이동하여 해당 이벤트를 필터링하여 표시할 수 있습니다.

클러스터의 총 활성 이벤트 막대 그래프는 활성 위험 및 경고 이벤트의 총 수를 표시합니다.

- 대기 시간(노드, 집계, SVM, 볼륨, LUN 및 네임스페이스의 총합)
- IOPS(클러스터, 노드, 집계, SVM, 볼륨, LUN 및 네임스페이스의 총합)
- MB/s(클러스터, 노드, 집계, SVM, 볼륨, LUN, 네임스페이스, 포트 및 LIF의 총합)
- 사용된 성능 용량(노드 및 집계에 대한 총계)
- 활용도(노드, 집계 및 포트의 총합)
- 기타(볼륨에 대한 캐시 미스 비율)

목록에는 사용자 정의 임계값 정책, 시스템 정의 임계값 정책 및 동적 임계값에서 트리거된 활성 성능 이벤트가 포함되어 있습니다.

그래프 데이터(수직 카운터 막대)는 빨간색으로 표시됩니다(■) 중요한 이벤트의 경우 노란색(■) 경고 이벤트에 대해. 각 수직 카운터 막대 위에 커서를 올려놓으면 실제 이벤트 유형과 수를 볼 수 있습니다. *새로 고침*을 클릭하면 카운터 패널 데이터를 업데이트할 수 있습니다.

범례에서 중요 및 경고 아이콘을 클릭하면 전체 활성 이벤트 성능 그래프에서 중요 이벤트와 경고 이벤트를 표시하거나 숨길 수 있습니다. 특정 이벤트 유형을 숨기면 범례 아이콘이 회색으로 표시됩니다.

카운터 패널

카운터 패널은 지난 72시간 동안의 클러스터 활동 및 성능 이벤트를 표시하며, 다음과 같은 카운터를 포함합니다.

• IOPS 카운터 패널

IOPS는 초당 입출력 작업 수로 클러스터의 작동 속도를 나타냅니다. 이 카운터 패널은 지난 72시간 동안의 클러스터 IOPS 상태에 대한 간략한 개요를 제공합니다. 그래프 추세선 위에 커서를 놓으면 특정 시간의 IOPS 값을 볼 수 있습니다.

• MB/s 카운터 패널

MB/s는 초당 클러스터와 주고받는 데이터 양을 메가바이트 단위로 나타냅니다. 이 카운터 패널은 지난 72시간 동안의 클러스터 MB/s 상태에 대한 간략한 개요를 제공합니다. 그래프 추세선 위에 커서를 놓으면 특정 시간의 MB/s 값을 볼 수 있습니다.

차트의 오른쪽 상단 회색 막대에 있는 숫자는 지난 72시간 동안의 평균값입니다. 추세선 그래프의 하단과 상단에 표시된 숫자는 지난 72시간 동안의 최소값과 최대값입니다. 차트 아래의 회색 막대에는 지난 72시간 동안의 활성(새 이벤트와 확인된 이벤트) 이벤트와 사용되지 않는 이벤트 수가 포함되어 있습니다.

카운터 패널에는 두 가지 유형의 이벤트가 포함되어 있습니다.

- 활동적인

성능 이벤트가 현재 활성화되어 있음을 나타냅니다(새로운 이벤트 또는 확인된 이벤트). 이벤트를 발생시킨 문제가 자체적으로 해결되지 않았거나 해결되지 않았습니다. 저장소 개체의 성능 카운터가 성능 임계값보다 높게 유지됩니다.

- 폐기됨

이벤트가 더 이상 활성화되지 않았음을 나타냅니다. 이벤트를 발생시킨 문제가 스스로 해결되었습니다. 저장소 개체의 성능 카운터가 더 이상 성능 임계값을 초과하지 않습니다.

*활성 이벤트*의 경우 이벤트가 하나 있으면 이벤트 아이콘 위에 커서를 놓고 이벤트 번호를 클릭하면 해당 이벤트 세부 정보 페이지로 연결됩니다. 이벤트가 두 개 이상인 경우 *모든 이벤트 보기*를 클릭하면 이벤트 인벤토리 페이지가 표시됩니다. 이 페이지는 선택한 개체 카운터 유형에 대한 모든 이벤트를 표시하도록 필터링됩니다.

관리되는 개체 창

성능 요약 탭의 관리 개체 창은 클러스터의 스토리지 개체 유형과 개수에 대한 최상위 개요를 제공합니다. 이 창을 사용하면 각 클러스터의 개체 상태를 추적할 수 있습니다.

관리되는 개체 수는 마지막 수집 기간을 기준으로 한 특정 시점의 데이터입니다. 15분 간격으로 새로운 물체가 발견됩니다.

모든 객체 유형에 연결된 숫자를 클릭하면 해당 객체 유형에 대한 객체 성능 인벤토리 페이지가 표시됩니다. 개체 인벤토리 페이지는 이 클러스터에 있는 개체만 표시하도록 필터링됩니다.

관리되는 객체는 다음과 같습니다.

- 노드

클러스터 내의 물리적 시스템.

- 집계

보호 및 프로비저닝을 위해 단일 단위로 관리할 수 있는 여러 개의 독립 디스크 중복 배열(RAID) 그룹 집합입니다.

- 포트

네트워크 상의 다른 장치에 연결하는 데 사용되는 노드의 물리적 연결 지점입니다.

- 저장 VM

고유한 네트워크 주소를 통해 네트워크 액세스를 제공하는 가상 머신입니다. SVM은 별도의 네임스페이스에서 데이터를 제공할 수 있으며, 클러스터의 나머지 부분과 별도로 관리할 수 있습니다.

- 권수

지원되는 하나 이상의 액세스 프로토콜을 통해 액세스 가능한 사용자 데이터를 보관하는 논리적 엔터티입니다. 이 계산에는 FlexVol 볼륨과 FlexGroup 볼륨이 모두 포함되며 FlexGroup 구성 요소는 포함되지 않습니다.

- LUN

FC(Fibre Channel) 논리 장치 또는 iSCSI 논리 장치의 식별자입니다. 논리 단위는 일반적으로 저장 볼륨에 해당하며, 컴퓨터 운영 체제 내에서는 장치로 표현됩니다.

- 네트워크 인터페이스

노드에 대한 네트워크 접근 지점을 나타내는 논리적 네트워크 인터페이스입니다. 이 계산에는 모든 인터페이스 유형이 포함됩니다.

상위 성과자 페이지

최고 성능자 페이지에는 선택한 성능 카운터를 기준으로 가장 높은 성능이나 가장 낮은 성능을 보이는 스토리지 개체가 표시됩니다. 예를 들어, 스토리지 VM 카테고리에서는 가장 높은 IOPS, 가장 높은 지연 시간, 가장 낮은 MB/s를 갖는 SVM을 표시할 수 있습니다. 이 페이지에서는 상위권 실적자가 활성 실적 이벤트(신규 또는 확인됨)를 진행 중인지 여부도 확인할 수 있습니다.

상위 성과자 페이지에는 각 개체가 최대 10개까지 표시됩니다. Volume 개체에는 FlexVol 볼륨과 FlexGroup 볼륨이 모두 포함됩니다.

- 시간 범위

가장 성과가 좋은 항목을 보려면 시간 범위를 선택할 수 있습니다. 선택한 시간 범위는 모든 스토리지 개체에 적용됩니다. 사용 가능한 시간 범위:

- 마지막 시간
- 지난 24시간
- 지난 72시간(기본값)
- 지난 7일

- 미터법

다른 카운터를 선택하려면 메트릭 메뉴를 클릭하세요. 카운터 옵션은 개체 유형에 따라 고유합니다. 예를 들어, 볼륨 개체에 사용할 수 있는 카운터는 대기 시간, **IOPS**, *MB/s*입니다. 카운터를 변경하면 선택한 카운터를 기준으로 상위 성과를 기록한 패널 데이터가 다시 로드됩니다.

사용 가능한 카운터:

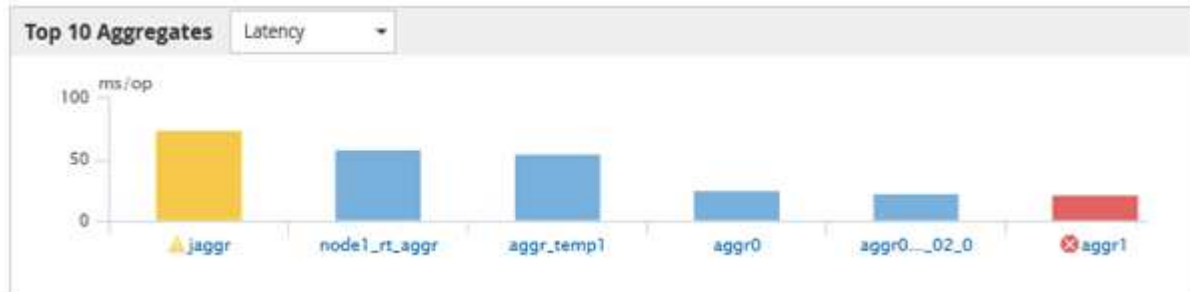
- 숨어 있음
- 아이오프스
- MB/초
- 사용된 성능 용량(노드 및 집계용)
- 활용도(노드 및 집계용)

- 종류

정렬 메뉴를 클릭하여 선택한 개체와 카운터에 대한 오름차순 또는 내림차순 정렬을 선택하세요. 옵션은 *높은 순에서 낮은 순으로*와 *낮은 순에서 높은 순으로*입니다. 이러한 옵션을 사용하면 성능이 가장 높은 개체나 성능이 가장 낮은 개체를 볼 수 있습니다.

- 카운터 바

그래프의 카운터 막대는 각 개체의 성능 통계를 보여주며, 해당 항목을 막대로 표현합니다. 막대 그래프는 색상으로 구분되어 있습니다. 카운터가 성능 임계값을 초과하지 않으면 카운터 막대가 파란색으로 표시됩니다. 임계값 위반이 활성화된 경우(새 이벤트 또는 확인된 이벤트) 막대는 이벤트 색상으로 표시됩니다. 경고 이벤트는 노란색으로 표시됩니다(■), 그리고 중요한 이벤트는 빨간색으로 표시됩니다(■). 임계값 위반은 경고 및 중요 이벤트에 대한 심각도 이벤트 표시기 아이콘을 통해 추가로 표시됩니다.



각 그래프의 X축에는 선택한 개체 유형에 대한 최고 성과 항목이 표시됩니다. Y축에는 선택된 카운터에 적용되는 단위가 표시됩니다. 각 수직 막대 그래프 요소 아래에 있는 개체 이름 링크를 클릭하면 선택한 개체의 성과 랜딩 페이지로 이동합니다.

- 심각도 이벤트 표시기

심각도 이벤트 표시기 아이콘은 활성 중요 이벤트의 개체 이름 왼쪽에 표시됩니다. (❌) 또는 경고 (⚠️) 상위 성과 그래프의 이벤트입니다. 심각도 이벤트 표시기 아이콘을 클릭하면 다음을 볼 수 있습니다.

- 한 가지 이벤트

해당 이벤트의 이벤트 세부 정보 페이지로 이동합니다.

- 두 개 이상의 이벤트

선택한 개체에 대한 모든 이벤트를 표시하도록 필터링된 이벤트 인벤토리 페이지로 이동합니다.

- 내보내기 버튼

생성합니다 .csv 카운터 막대에 나타나는 데이터가 포함된 파일입니다. 보고 있는 단일 클러스터에 대한 파일을 만들거나 데이터 센터의 모든 클러스터에 대한 파일을 만들도록 선택할 수 있습니다.

성능 인벤토리 페이지를 사용하여 성능 모니터링

개체 인벤토리 성능 페이지에는 개체 유형 범주 내 모든 개체의 성능 정보, 성능 이벤트 및 개체 상태가 표시됩니다. 이를 통해 클러스터 내 각 개체의 성능 상태를 한눈에 파악할 수 있습니다. 예를 들어 모든 노드나 모든 볼륨에 대한 성능 상태를 파악할 수 있습니다.

객체 인벤토리 성능 페이지는 객체 상태에 대한 전반적인 개요를 제공하여 모든 객체의 전반적인 성능을 평가하고 객체 성능 데이터를 비교할 수 있도록 해줍니다. 검색, 정렬, 필터링을 통해 객체 인벤토리 페이지의 콘텐츠를 구체화할 수 있습니다. 이 기능은 객체 성능을 모니터링하고 관리할 때 유용합니다. 성능 문제가 있는 객체를 빠르게 찾아 문제 해결 프로세스를 시작할 수 있기 때문입니다.

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

View

All Nodes

Search Nodes

Assign Performance Threshold Policy

Clear Performance Threshold Policy

Schedule Report

☐	Status	Node	Latency	IOPS	MBps	Flash Cache Reads	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster
☐		ocum-mobility-02	10.2 ms/op	18,884 IOPS	156 MBps	N/A	81%	35%	16.6 TB	23.2 TB	ocum-mobility-01-02
☒		opm-simplicity-01	2.01 ms/op	39,358 IOPS	153 MBps	< 1%	119%	88%	4.88 TB	18.3 TB	opm-simplicity
☐		ocum-mobility-01	0.018 ms/op	< 1 IOPS	18.2 MBps	N/A	23%	18%	8.69 TB	15.7 TB	ocum-mobility-01-02
☐		opm-simplicity-02	17 ms/op	14,627 IOPS	124 MBps	< 1%	29%	20%	212 GB	5.88 TB	opm-simplicity

기본적으로 성능 인벤토리 페이지의 개체는 개체 성능 중요도에 따라 정렬됩니다. 새로운 중요 성능 이벤트가 발생한 객체가 먼저 나열되고, 경고 이벤트가 발생한 객체가 두 번째로 나열됩니다. 이를 통해 해결해야 할 문제에 대한 즉각적인 시각적 표시가 제공됩니다. 모든 성과 데이터는 72시간 평균을 기준으로 합니다.

객체 이름 옆에서 객체 이름을 클릭하면 객체 인벤토리 성능 페이지에서 객체 세부 정보 페이지로 쉽게 이동할 수 있습니다. 예를 들어, 성능/모든 노드 인벤토리 페이지에서 노드 옆에 있는 노드 객체를 클릭합니다. 객체 세부 정보 페이지는 활성 이벤트의 나란히 비교를 포함하여 선택된 객체에 대한 심층적인 정보와 세부 정보를 제공합니다.

모든 스토리지 개체에 대한 성능 인벤토리 페이지 보기

성능 인벤토리 페이지를 사용하면 클러스터, 집계, 볼륨 등 사용 가능한 각 스토리지 개체에 대한 성능 정보 요약은 볼 수 있습니다. 특정 객체에 대한 자세한 정보를 보려면 성능 객체 세부 정보 페이지에 링크할 수 있습니다.

기본적으로 뷰 페이지의 객체는 이벤트 중요도에 따라 정렬됩니다. 중요한 이벤트가 발생한 객체는 먼저 나열되고, 경고 이벤트가 발생한 객체는 두 번째로 나열됩니다. 이를 통해 해결해야 할 문제에 대한 즉각적인 시각적 표시가 제공됩니다.

이 페이지에서 쉼표로 구분된 값으로 데이터를 내보낼 수 있습니다.(.csv) 파일, Microsoft Excel 파일(.xlsx), 또는 (.pdf 보고서 버튼을 사용하여 문서를 작성한 다음, 내보낸 데이터를 사용하여 보고서를 작성합니다. 또한, 페이지를 사용자 지정된 다음 예약된 보고서 버튼을 사용하여 정기적으로 보고서를 작성하여 이메일로 전송하도록 예약할 수 있습니다.

이 페이지의 모든 필드는 사용자 정의 보기와 보고서에서 사용할 수 있습니다. 일부 필드는 관련 페이지에 연결되어 있어 보다 자세한 보기가 가능합니다.

성능: 모든 클러스터 보기

성능: 모든 클러스터 보기는 Unified Manager 인스턴스에서 모니터링하는 각 클러스터의 성능 이벤트, 데이터 및 구성 정보에 대한 개요를 표시합니다. 이 페이지에서는 클러스터의 성능을 모니터링하고, 성능 문제와 임계값 이벤트를 해결할 수 있습니다.

성능 임계값 정책 할당 및 성능 임계값 정책 지우기 버튼을 사용하여 객체 인벤토리 페이지의 모든 객체에 성능 임계값 정책을 할당하거나 해당 객체에서 임계값 정책을 지울 수 있습니다.

성능: 모든 클러스터 보기의 몇 가지 중요한 필드는 다음과 같습니다.

- 클러스터 FQDN: 클러스터의 정규화된 도메인 이름(FQDN)입니다.
- IOPS: 클러스터의 초당 입출력 작업입니다.

- MB/s: 초당 MiB로 측정한 클러스터의 처리량입니다.
- 용량 필드: 여유 용량과 총 용량(GiB)
- 호스트 이름 또는 IP 주소: 클러스터 관리 LIF의 호스트 이름 또는 IP 주소(IPv4 또는 IPv6).
- OS 버전: 클러스터에 설치된 ONTAP 소프트웨어의 버전입니다.



클러스터의 노드에 서로 다른 버전의 ONTAP 소프트웨어가 설치된 경우 가장 낮은 버전 번호가 나열됩니다. 각 노드에 설치된 ONTAP 버전은 성능: 모든 노드 보기에서 볼 수 있습니다.

- 임계값 정책: 이 저장소 개체에서 활성화된 사용자 정의 성능 임계값 정책입니다. 줄임표(...)가 포함된 정책 이름 위에 커서를 놓으면 전체 정책 이름이나 할당된 정책 이름 목록을 볼 수 있습니다. 성능 임계값 정책 할당 및 성능 임계값 정책 지우기 버튼은 맨 왼쪽에 있는 확인란을 클릭하여 하나 이상의 객체를 선택할 때까지 비활성화된 상태로 유지됩니다.

성능: 모든 볼륨 보기

성능: 모든 볼륨 보기는 Unified Manager 인스턴스에서 모니터링되는 각 FlexVol volume 과 FlexGroup 볼륨에 대한 성능 이벤트, 카운터 데이터 및 구성 정보의 개요를 표시합니다. 이를 통해 볼륨의 성능을 빠르게 모니터링하고 성능 문제와 임계값 이벤트를 해결할 수 있습니다.

특정 객체의 대기 시간과 처리량을 분석하려면 추가 옵션 버튼을 클릭하세요. 그런 다음 *작업 부하 분석*을 선택하면 작업 부하 분석 페이지에서 성능 및 용량 차트를 볼 수 있습니다. System Manager에 대한 유효한 자격 증명이 있는 경우 System Manager에서 세부 정보를 볼 수 있습니다.



데이터 보호(DP) 볼륨의 경우 사용자가 생성한 트래픽에 대한 카운터 값만 표시됩니다. 이 페이지에는 루트 볼륨이 표시되지 않습니다.

성능: 모든 볼륨 보기의 몇 가지 중요한 필드는 다음과 같습니다.

- 스타일: FlexVol 또는 FlexGroup.
- 대기 시간: FlexVol 볼륨의 경우 이는 모든 I/O 요청에 대한 볼륨의 평균 응답 시간으로, 작업당 밀리초 단위로 표현됩니다. FlexGroup 볼륨의 경우 이는 모든 구성 볼륨의 평균 대기 시간입니다.
- IOPS/TB: 작업 부하에 의해 소비되는 총 공간을 기준으로 초당 처리되는 입출력 작업 수(테라바이트)입니다. 이 카운터는 주어진 저장 용량으로 얼마나 많은 성능을 제공할 수 있는지 측정합니다.
- IOPS: FlexVol 볼륨의 경우 이는 볼륨에 대한 초당 입출력 작업 수입니다. FlexGroup 볼륨의 경우 이는 모든 구성 볼륨의 IOPS 합계입니다.
- MB/s: FlexVol 볼륨의 경우 이는 초당 메가바이트 단위로 측정되는 볼륨의 처리량입니다. FlexGroup 볼륨의 경우 이는 모든 구성 볼륨의 MB/s 합계입니다.
- 용량 필드: 여유 용량과 총 용량(GiB)

자세한 내용은 다음 링크를 참조하세요.

- ["스토리지 객체에 성능 임계값 정책 할당"](#)
- ["저장소 개체에서 성능 임계값 정책 제거"](#)
- ["Unified Manager에서 모니터링하는 작업 유형"](#)
- ["특정 볼륨 또는 LUN에 적용된 QoS 정책 그룹 설정 보기"](#)

- ["클라우드 계층화하기 위한 Unified Manager 권장 사항 이해"](#)
- ["동일한 QoS 정책 그룹에 있는 볼륨이나 LUN을 비교하기 위해 성능 차트 보기"](#)

성능: 모든 집계 보기

성능: 모든 집계 보기는 Unified Manager 인스턴스에서 모니터링하는 각 집계에 대한 성능 이벤트, 데이터 및 구성 정보의 개요를 표시합니다. 이 페이지에서는 집계의 성능을 모니터링하고, 성능 문제와 임계값 이벤트를 해결할 수 있습니다.

성과: 모든 집계 보기의 몇 가지 중요한 필드는 다음과 같습니다.

- 유형: 집계 유형:
 - 하드디스크
 - 잡종. HDD와 SSD를 결합했지만 Flash Pool이 활성화되지 않았습니다.
 - 하이브리드(플래시 풀). HDD와 SSD를 결합하고, Flash Pool을 활성화했습니다.
 - SSD
 - SSD(FabricPool). SSD와 클라우드 계층을 결합합니다.
 - HDD(FabricPool). HDD와 클라우드 계층을 결합합니다.
 - VM디스크(SDS). 가상 머신 내의 가상 디스크
 - VMDisk(FabricPool). 가상 디스크와 클라우드 계층을 결합합니다.
 - LUN(FlexArray)
- 비활성 데이터 보고: 이 집계에서 비활성 데이터 보고 기능이 활성화되었는지 비활성화되었는지 여부입니다. 이 기능을 활성화하면 이 집계의 볼륨은 성능: 모든 볼륨 보기에서 콜드 데이터의 양을 표시합니다. ONTAP 버전이 비활성 데이터 보고를 지원하지 않는 경우 이 필드의 값은 "N/A"입니다.
- 임계값 정책: 이 저장소 개체에서 활성화된 사용자 정의 성능 임계값 정책입니다. 줄임표(...)가 포함된 정책 이름 위에 커서를 놓으면 전체 정책 이름이나 할당된 정책 이름 목록을 볼 수 있습니다. 성능 임계값 정책 할당 및 성능 임계값 정책 지우기 버튼은 맨 왼쪽에 있는 확인란을 클릭하여 하나 이상의 객체를 선택할 때까지 비활성화된 상태로 유지됩니다. 자세한 내용은 다음 링크를 참조하세요.
- ["스토리지 객체에 성능 임계값 정책 할당"](#)
- ["저장소 개체에서 성능 임계값 정책 제거"](#)

성능: 모든 노드 보기

성능: 모든 노드 보기는 Unified Manager 인스턴스에서 모니터링하는 각 노드에 대한 성능 이벤트, 데이터 및 구성 정보의 개요를 표시합니다. 이를 통해 노드의 성능을 빠르게 모니터링하고 성능 문제와 임계값 이벤트를 해결할 수 있습니다.



Flash Cache Reads는 디스크에서 반환되는 대신, 캐시에서 처리된 노드의 읽기 작업 비율을 반환합니다. Flash Cache 데이터는 노드에 대해서만 표시되며, 노드에 Flash Cache 모듈이 설치된 경우에만 표시됩니다.

Unified Manager와 이를 통해 관리되는 클러스터가 외부 네트워크 연결이 없는 사이트에 설치된 경우, 보고서 메뉴에서 하드웨어 인벤토리 보고서 옵션이 제공됩니다. 이 버튼을 클릭하면 하드웨어 모델 번호와 일련 번호, 디스크 유형과 개수, 설치된 라이선스 등 클러스터와 노드 정보의 전체 목록이 포함된 .csv 파일이 생성됩니다. 이 보고 기능은 NetApp Active IQ 플랫폼에 연결되지 않은 보안 사이트 내에서 계약을 갱신하는 데 유용합니다. 성능 임계값 정책 할당 및 성능

임계값 정책 지우기 버튼을 사용하여 객체 인벤토리 페이지의 모든 객체에 성능 임계값 정책을 할당하거나 해당 객체에서 임계값 정책을 지울 수 있습니다.

자세한 내용은 다음 링크를 참조하세요.

- ["스토리지 객체에 성능 임계값 정책 할당"](#)
- ["저장소 개체에서 성능 임계값 정책 제거"](#)
- ["계약 갱신을 위한 하드웨어 인벤토리 보고서 생성"](#)

성능: 모든 스토리지 VM 보기

성능: 모든 스토리지 VM 보기는 Unified Manager 인스턴스에서 모니터링되는 각 스토리지 가상 머신(SVM)에 대한 성능 이벤트, 데이터 및 구성 정보의 개요를 표시합니다. 이를 통해 SVM의 성능을 빠르게 모니터링하고 성능 문제와 임계값 이벤트를 해결할 수 있습니다. 이 페이지의 대기 시간 필드는 모든 I/O 요청에 대한 평균 응답 시간을 작업당 밀리초 단위로 보고합니다.



이 페이지에 나열된 SVM에는 데이터 SVM과 클러스터 SVM만 포함됩니다. Unified Manager는 관리자 또는 노드 SVM을 사용하거나 표시하지 않습니다.

자세한 내용은 다음 링크를 참조하세요.

- ["스토리지 객체에 성능 임계값 정책 할당"](#)
- ["저장소 개체에서 성능 임계값 정책 제거"](#)

성능: 모든 LUN 보기

성능: 모든 LUN 보기는 Unified Manager 인스턴스에서 모니터링되는 각 LUN에 대한 성능 이벤트, 데이터 및 구성 정보의 개요를 표시합니다. 이를 통해 LUN의 성능을 빠르게 모니터링하고 성능 문제와 임계값 이벤트를 해결할 수 있습니다.

특정 객체의 지연 시간과 처리량을 분석하려면 추가 아이콘을 클릭하세요.  , 워크로드 분석*을 선택하면 *워크로드 분석 페이지에서 성능 및 용량 차트를 볼 수 있습니다.

자세한 내용은 다음 링크를 참조하세요.

- ["일관성 그룹 관계에서 LUN 모니터링"](#)
- ["LUN 프로비저닝"](#)
- ["스토리지 객체에 성능 임계값 정책 할당"](#)
- ["저장소 개체에서 성능 임계값 정책 제거"](#)
- ["동일한 QoS 정책 그룹에 있는 볼륨 또는 LUN 보기".](#)
- ["특정 볼륨 또는 LUN에 적용된 QoS 정책 그룹 설정 보기"](#)
- ["API를 사용하여 LUN 프로비저닝"](#)

성능: 모든 NVMe 네임스페이스 보기

성능: 모든 NVMe 네임스페이스 보기는 Unified Manager 인스턴스에서 모니터링되는 각 NVMe 네임스페이스에 대한 성능 이벤트, 데이터 및 구성 정보의 개요를 표시합니다. 이를 통해 네임스페이스의 성능과 상태를 빠르게 모니터링하고,

문제 및 임계값 이벤트를 해결할 수 있습니다.

다음 정보를 비롯한 정보가 보고됩니다. 네임스페이스의 현재 상태. * 오프라인 - 네임스페이스에 대한 읽기 또는 쓰기 액세스가 허용되지 않습니다. * 온라인 - 네임스페이스에 대한 읽기 및 쓰기 액세스가 허용됩니다. * NVFail - NVRAM 오류로 인해 네임스페이스가 자동으로 오프라인 상태가 되었습니다. * 공간 오류 - 네임스페이스 공간이 부족합니다.

자세한 내용은 다음 링크를 참조하세요.

- ["스토리지 객체에 성능 임계값 정책 할당"](#)
- ["저장소 개체에서 성능 임계값 정책 제거"](#)

성능: 모든 네트워크 인터페이스 보기

성능: 모든 네트워크 인터페이스 보기는 Unified Manager의 이 인스턴스에서 모니터링되는 각 네트워크 인터페이스(LIF)에 대한 성능 이벤트, 데이터 및 구성 정보의 개요를 표시합니다. 이 페이지를 사용하면 인터페이스의 성능을 빠르게 모니터링하고 성능 문제와 임계값 이벤트를 해결할 수 있습니다. 성능: 모든 네트워크 인터페이스 보기의 몇 가지 중요한 필드는 다음과 같습니다.

- IOPS: 초당 입출력 작업 수. IOPS는 NFS LIF 및 CIFS LIF에 적용되지 않으며 이러한 유형의 경우 N/A로 표시됩니다.
- 대기 시간: 모든 I/O 요청에 대한 평균 응답 시간으로, 작업당 밀리초 단위로 표현됩니다. 대기 시간은 NFS LIF 및 CIFS LIF에는 적용되지 않으며 이러한 유형의 경우 N/A로 표시됩니다.
- 홈 위치: 인터페이스의 홈 위치로, 노드 이름과 포트 이름으로 표시되며 콜론(:)으로 구분됩니다. 위치가 줄임표(...)로 표시되는 경우, 위치 이름 위에 커서를 놓으면 전체 위치를 볼 수 있습니다.
- 현재 위치: 인터페이스의 현재 위치로, 노드 이름과 포트 이름으로 표시되며 콜론(:)으로 구분됩니다. 위치가 줄임표(...)로 표시되는 경우, 위치 이름 위에 커서를 놓으면 전체 위치를 볼 수 있습니다.
- 역할: 인터페이스 역할: 데이터, 클러스터, 노드 관리 또는 클러스터 간.



이 페이지에 나열된 인터페이스에는 데이터 LIF, 클러스터 LIF, 노드 관리 LIF, 클러스터 간 LIF가 포함됩니다. Unified Manager는 시스템 LIF를 사용하거나 표시하지 않습니다.

성능: 모든 포트 보기

성능: 모든 포트 보기는 Unified Manager 인스턴스에서 모니터링하는 각 포트에 대한 성능 이벤트, 데이터 및 구성 정보의 개요를 표시합니다. 이를 통해 포트 성능을 빠르게 모니터링하고 성능 문제와 임계값 이벤트를 해결할 수 있습니다. 포트 역할의 경우 네트워크 포트 기능(데이터 또는 클러스터)이 표시됩니다. FCP 포트에는 역할이 있을 수 없으며 역할은 N/A로 표시됩니다.



성능 카운터 값은 물리적 포트에 대해서만 표시됩니다. VLAN이나 인터페이스 그룹에 대한 카운터 값은 표시되지 않습니다.

자세한 내용은 다음 링크를 참조하세요.

- ["스토리지 객체에 성능 임계값 정책 할당"](#)
- ["저장소 개체에서 성능 임계값 정책 제거"](#)

성능: QoS 정책 그룹 보기

QoS 정책 그룹 보기에는 Unified Manager가 모니터링하는 클러스터에서 사용 가능한 QoS 정책 그룹이 표시됩니다. 여기에는 기존 QoS 정책, 적응형 QoS 정책, 성능 서비스 수준을 사용하여 할당된 QoS 정책이 포함됩니다.

성능: QoS 정책 그룹 보기의 몇 가지 중요한 필드는 다음과 같습니다.

- QoS 정책 그룹: QoS 정책 그룹의 이름입니다. Unified Manager 9.7 이상으로 가져온 NetApp Service Level Manager(NSLM) 1.3 정책의 경우 여기에 표시되는 이름에는 SVM 이름과 NSLM에서 성능 서비스 수준을 정의할 때 이름에 포함되지 않았던 기타 정보가 포함됩니다. 예를 들어, "NSLM_vs6_Performance_2_0"이라는 이름은 이것이 SVM "vs6"에서 예상 지연 시간이 "2ms/op"인 NSLM 시스템 정의 "성능" PSL 정책임을 의미합니다.
- SVM: QoS 정책 그룹이 속한 스토리지 VM(SVM)입니다. 스토리지 VM 이름을 클릭하면 해당 스토리지 VM의 세부 정보 페이지로 이동할 수 있습니다. QoS 정책이 관리 스토리지 VM에 생성된 경우 이 필드는 비어 있습니다. 이 스토리지 VM 유형은 클러스터를 나타냅니다.
- 최소 처리량: 정책 그룹이 보장하는 최소 처리량(IOPS)입니다. 적응형 정책의 경우 이는 볼륨이나 LUN에 할당된 TB당 예상 최소 IOPS이며, 스토리지 개체 할당 크기를 기준으로 합니다.
- 최대 처리량: 정책 그룹이 초과해서는 안 되는 처리량(IOPS 및/또는 MB/s)입니다. 이 필드가 비어 있으면 ONTAP에 정의된 최대값이 무한함을 의미합니다. 적응형 정책의 경우 이는 볼륨이나 LUN에 할당된 TB당 가능한 최대(피크) IOPS이며, 스토리지 개체 할당 크기나 스토리지 개체 사용 크기에 따라 결정됩니다.
- 절대 최소 IOPS: 적응형 정책의 경우 이는 예상 IOPS가 이 값보다 낮을 때 재정의로 사용되는 절대 최소 IOPS 값입니다.
- 블록 크기: QoS 적응 정책에 지정된 블록 크기입니다.
- 최소 할당: "할당된 공간" 또는 "사용된 공간"을 사용하여 최대 처리량(피크) IOPS를 결정합니다.
- 예상 대기 시간: 저장소 입출력 작업에 대한 예상 평균 대기 시간입니다.
- 공유: 기존 QoS 정책의 경우 정책 그룹에 정의된 처리량 값이 여러 개체 간에 공유되는지 여부입니다.
- 연관된 개체: QoS 정책 그룹에 할당된 작업 부하의 수입입니다. 확장 버튼을 클릭할 수 있습니다(▼) QoS 정책 그룹 이름 옆에 있는 아이콘을 클릭하면 정책 그룹에 대한 자세한 내용을 볼 수 있습니다.
- 할당된 용량: QoS 정책 그룹에 있는 개체가 현재 사용 중인 공간의 양입니다.
- 연관된 개체: QoS 정책 그룹에 할당된 작업 부하의 수로, 볼륨과 LUN으로 구분됩니다. 숫자를 클릭하면 선택한 볼륨이나 LUN에 대한 자세한 내용을 제공하는 페이지로 이동할 수 있습니다.

자세한 내용은 다음 항목을 참조하세요. "[QoS 정책 그룹 정보를 사용하여 성능 관리](#)".

성능 인벤토리 페이지 내용 개선

성능 개체의 인벤토리 페이지에는 개체 인벤토리 데이터 콘텐츠를 세분화하는 데 도움이 되는 도구가 포함되어 있어 특정 데이터를 빠르고 쉽게 찾을 수 있습니다.

성능 개체 인벤토리 페이지에 포함된 정보는 광범위할 수 있으며, 종종 여러 페이지에 걸쳐 있습니다. 이러한 포괄적인 데이터는 성과를 모니터링, 추적, 개선하는 데 매우 유용합니다. 그러나 특정 데이터를 찾으려면 해당 데이터를 빠르게 찾을 수 있는 도구가 필요합니다. 따라서 성능 개체 인벤토리 페이지에는 검색, 정렬, 필터링 기능이 포함되어 있습니다. 또한, 검색과 필터링을 함께 사용하면 검색 결과를 더욱 좁힐 수 있습니다.

객체 인벤토리 성능 페이지에서 검색

객체 인벤토리 성능 페이지에서 문자열을 검색할 수 있습니다. 페이지 오른쪽 상단에 있는 검색

필드를 사용하면 개체 이름이나 정책 이름을 기준으로 데이터를 빠르게 찾을 수 있습니다. 이를 통해 특정 개체와 관련 데이터를 빠르게 찾거나, 정책을 빠르게 찾아 관련 정책 개체 데이터를 볼 수 있습니다.

단계

1. 검색 요구 사항에 따라 다음 옵션 중 하나를 수행합니다.

이것을 찾으려면...	이것을 입력하세요...
특정 객체	검색 필드에 개체 이름을 입력하고 *검색*을 클릭합니다. 검색한 객체와 관련 데이터가 표시됩니다.
사용자 정의 성능 임계값 정책	정책 이름의 일부 또는 전부를 검색 필드에 입력하고 *검색*을 클릭하세요. 검색한 정책에 할당된 개체가 표시됩니다.

객체 인벤토리 성능 페이지에서 정렬

객체 인벤토리 성능 페이지의 모든 데이터를 오름차순이나 내림차순으로 원하는 열로 정렬할 수 있습니다. 이를 통해 개체 인벤토리 데이터를 빠르게 찾을 수 있어 성능을 조사하거나 문제 해결 프로세스를 시작할 때 유용합니다.

정렬을 위해 선택된 열은 강조된 열 제목 이름과 이름 오른쪽에 정렬 방향을 나타내는 화살표 아이콘으로 표시됩니다. 위쪽 화살표는 오름차순을 나타내고, 아래쪽 화살표는 내림차순을 나타냅니다. 기본 정렬 순서는 상태(이벤트 중요도)를 내림차순으로 정렬하며, 가장 중요한 성능 이벤트가 먼저 나열됩니다.

단계

1. 열 이름을 클릭하면 열의 정렬 순서를 오름차순이나 내림차순으로 전환할 수 있습니다.

객체 인벤토리 성능 페이지 내용은 선택한 열을 기준으로 오름차순 또는 내림차순으로 정렬됩니다.

객체 인벤토리 성능 페이지에서 데이터 필터링

객체 인벤토리 성능 페이지에서 데이터를 필터링하여 특정 기준에 따라 데이터를 빠르게 찾을 수 있습니다. 필터링을 사용하면 개체 인벤토리 성능 페이지의 내용을 좁혀 지정한 결과만 표시할 수 있습니다. 이 방법은 귀하가 관심 있는 성과 데이터만 표시하는 매우 효율적인 방법입니다.

필터링 패널을 사용하면 기본 설정에 따라 그리드 보기를 사용자 지정할 수 있습니다. 사용 가능한 필터 옵션은 그리드에 표시되는 개체 유형에 따라 달라집니다. 현재 필터가 적용되어 있는 경우, 적용된 필터의 수가 필터 버튼 오른쪽에 표시됩니다.

세 가지 유형의 필터 매개변수가 지원됩니다.

매개변수	확인
문자열(텍스트)	연산자는 포함, 시작, 끝남, *포함하지 않음*입니다.

매개변수	확인
숫자	연산자는 보다 크다, 보다 작다, 마지막에, *사이에*입니다.
열거형(텍스트)	연산자는 *is*와 *is not*입니다.

각 필터에는 열, 연산자, 값 필드가 필요합니다. 사용 가능한 필터는 현재 페이지에서 필터링 가능한 열을 반영합니다. 적용할 수 있는 필터의 최대 개수는 4개입니다. 필터링된 결과는 결합된 필터 매개변수를 기반으로 합니다. 필터링된 결과는 현재 표시된 페이지뿐만 아니라 필터링된 검색의 모든 페이지에 적용됩니다.

필터링 패널을 사용하여 필터를 추가할 수 있습니다.

1. 페이지 상단에서 필터 버튼을 클릭하세요. 필터링 패널이 표시됩니다.
2. 왼쪽 드롭다운 목록을 클릭하고 개체를 선택합니다. 예를 들어, _Cluster_나 성능 카운터를 선택합니다.
3. 가운데 드롭다운 목록을 클릭하고 사용할 연산자를 선택하세요.
4. 마지막 목록에서 값을 선택하거나 입력하여 해당 개체에 대한 필터를 완성합니다.
5. 다른 필터를 추가하려면 +필터 추가*를 클릭하세요. 추가 필터 필드가 표시됩니다. 이전 단계에서 설명한 프로세스를 사용하여 이 필터를 완료합니다. 네 번째 필터를 추가하면 *+필터 추가 버튼이 더 이상 표시되지 않습니다.
6. *필터 적용*을 클릭하세요. 필터 옵션은 그리드에 적용되고 필터 수는 필터 버튼 오른쪽에 표시됩니다.
7. 필터링 패널을 사용하여 제거할 필터 오른쪽에 있는 휴지통 아이콘을 클릭하여 개별 필터를 제거합니다.
8. 모든 필터를 제거하려면 필터링 패널 하단의 *재설정*을 클릭하세요.

필터링 예제

이 그림은 세 개의 필터가 있는 필터링 패널을 보여줍니다. 필터가 최대 4개보다 적을 경우 +필터 추가 버튼이 표시됩니다.

The screenshot shows a filter panel with three active filters. Each filter consists of a dropdown menu for the field, a dropdown for the operator, and a text input for the value. The filters are: 1. MBps greater than 5, 2. Node name starts with test, 3. Type is FCP Port. To the right of each filter is a trash icon for removal. At the bottom left is a '+ Add Filter' button. At the bottom right are 'Cancel' and 'Apply Filter' buttons. The 'Apply Filter' button is highlighted in blue.

*필터 적용*을 클릭하면 필터링 패널이 닫히고 필터가 적용되며 적용된 필터 수가 표시됩니다(3).

클라우드에 데이터를 계층화하기 위한 **Unified Manager** 권장 사항을 이해합니다.

성능: 모든 볼륨 보기는 비활성(콜드) 볼륨에 저장된 사용자 데이터의 크기와 관련된 정보를 표시합니다. 어떤 경우에는 Unified Manager가 FabricPool 지원 집계의 클라우드 계층(클라우드 공급자 또는 StorageGRID)에 비활성 데이터를 계층화하여 이점을 얻을 수 있는 특정

볼륨을 식별합니다.



FabricPool ONTAP 9.2에서 도입되었으므로 9.2 이전 버전의 ONTAP 소프트웨어를 사용하는 경우 Unified Manager의 데이터 계층화 권장 사항에 따라 ONTAP 소프트웨어를 업그레이드해야 합니다. 또한, **auto** ONTAP 9.4에서 계층화 정책이 도입되었습니다. **all** 계층화 정책은 ONTAP 9.6에서 도입되었으므로 자동 계층화 정책을 사용하는 것이 권장되는 경우 ONTAP 9.4 이상으로 업그레이드해야 합니다.

성능: 모든 볼륨 보기의 다음 세 필드는 비활성 데이터를 클라우드 계층으로 이동하여 스토리지 시스템의 디스크 활용도를 개선하고 성능 계층의 공간을 절약할 수 있는지 여부에 대한 정보를 제공합니다.

- 티어링 정책

계층화 정책은 볼륨의 데이터가 성능 계층에 남아 있을지 아니면 일부 데이터가 성능 계층에서 클라우드 계층으로 이동될지 여부를 결정합니다.

이 필드의 값은 볼륨이 현재 FabricPool 집계에 상주하지 않더라도 볼륨에 설정된 계층화 정책을 나타냅니다. 계층화 정책은 볼륨이 FabricPool 집계에 있는 경우에만 적용됩니다.

- 콜드 데이터

콜드 데이터는 비활성(콜드) 볼륨에 저장된 사용자 데이터의 크기를 표시합니다.

볼륨이 배포된 집계에 다음이 필요하기 때문에 ONTAP 9.4 이상 소프트웨어를 사용할 때에만 여기에 값이 표시됩니다. **inactive data reporting parameter** 로 설정 **enabled** 그리고 최소 냉각 일수 임계값이 충족되었는지(사용하는 볼륨의 경우) **snapshot-only** 또는 **auto** (티어링 정책). 그렇지 않으면 값은 "N/A"로 나열됩니다.

- 클라우드 추천

볼륨의 데이터 활동에 대한 충분한 정보가 수집되면 Unified Manager는 더 이상 조치가 필요하지 않다고 판단하거나 비활성 데이터를 클라우드 계층으로 계층화하여 성능 계층의 공간을 절약할 수 있다고 판단할 수 있습니다.



콜드 데이터 필드는 15분마다 업데이트되지만, 클라우드 권장 사항 필드는 볼륨에서 콜드 데이터 분석을 수행할 때 7일마다 업데이트됩니다. 따라서 정확한 콜드 데이터의 양은 필드마다 다를 수 있습니다. 클라우드 권장 사항 필드에는 분석이 실행된 날짜가 표시됩니다.

비활성 데이터 보고가 활성화되면 콜드 데이터 필드에 비활성 데이터의 정확한 양이 표시됩니다. 비활성 데이터 보고 기능이 없으면 Unified Manager는 성능 통계를 사용하여 볼륨에서 데이터가 비활성인지 확인합니다. 이 경우 비활성 데이터의 양은 콜드 데이터 필드에 표시되지 않지만, 클라우드 권장 사항을 보려면 *계층*이라는 단어 위에 커서를 올려 놓으면 표시됩니다.

표시되는 클라우드 권장 사항은 다음과 같습니다.

- 학습. 추천을 하기에 충분한 데이터가 수집되지 않았습니다.
- 층. 분석 결과, 볼륨에 비활성(콜드) 데이터가 포함되어 있으며 해당 데이터를 클라우드 계층으로 이동하도록 볼륨을 구성해야 하는 것으로 확인되었습니다. 어떤 경우에는 먼저 볼륨을 FabricPool 지원 집계로 이동해야 할 수도 있습니다. 볼륨이 이미 FabricPool 집계에 있는 다른 경우에는 계층화 정책만 변경하면 됩니다.
- 조치 없음. 볼륨에 비활성 데이터가 거의 없거나, 볼륨이 이미 FabricPool 집계에서 "auto" 계층화 정책으로

설정되어 있거나, 볼륨이 데이터 보호 볼륨입니다. 이 값은 볼륨이 오프라인이거나 MetroCluster 구성에서 사용 중일 때도 표시됩니다.

볼륨을 이동하거나 볼륨 계층화 정책이나 비활성 데이터 집계 보고 설정을 변경하려면 ONTAP System Manager, ONTAP CLI 명령 또는 이러한 도구를 조합하여 사용합니다.

애플리케이션 관리자 또는 스토리지 관리자 역할로 Unified Manager에 로그인한 경우, 계층*이라는 단어 위에 커서를 올려 놓으면 클라우드 권장 사항에서 *볼륨 구성 링크를 사용할 수 있습니다. 이 버튼을 클릭하면 시스템 관리자에서 볼륨 페이지가 열려 권장되는 변경 사항을 적용할 수 있습니다.

성능 탐색기 페이지를 사용하여 성능 모니터링

성능 탐색기 페이지에는 클러스터의 각 개체 성능에 대한 자세한 정보가 표시됩니다. 이 페이지는 모든 클러스터 개체의 성능에 대한 자세한 보기를 제공하여 다양한 기간 동안 특정 개체의 성능 데이터를 선택하고 비교할 수 있습니다.

모든 객체의 전반적인 성능을 평가하고, 객체 성능 데이터를 나란히 비교할 수도 있습니다.

루트 객체를 이해하세요

루트 객체는 다른 객체를 비교하는 기준이 됩니다. 이를 통해 다른 개체의 데이터를 보고 루트 개체와 비교할 수 있으며, 개체 성능 문제를 해결하고 개선하는 데 도움이 되는 성능 데이터 분석을 제공합니다.

루트 개체 이름은 비교 창의 맨 위에 표시됩니다. 추가 객체는 루트 객체 아래에 표시됩니다. 비교 창에 추가할 수 있는 추가 객체의 수에는 제한이 없지만 루트 객체는 하나만 허용됩니다. 루트 개체의 데이터는 카운터 차트 창의 그래프에 자동으로 표시됩니다.

루트 객체는 변경할 수 없습니다. 항상 현재 보고 있는 객체 페이지로 설정됩니다. 예를 들어, Volume1의 Volume Performance Explorer 페이지를 열면 Volume1이 루트 개체이므로 변경할 수 없습니다. 다른 루트 객체와 비교하려면 객체의 링크를 클릭하고 해당 랜딩 페이지를 열어야 합니다.



이벤트와 임계값은 루트 개체에 대해서만 표시됩니다.

그리드에서 상관관계가 있는 객체 목록을 줄이기 위해 필터링을 적용합니다.

필터링을 사용하면 그리드에서 더 작고 명확하게 정의된 객체 하위 집합을 표시할 수 있습니다. 예를 들어, 그리드에 볼륨이 25개 있는 경우 필터링을 통해 처리량이 90MBps 미만이거나 대기 시간이 1ms/op보다 큰 볼륨만 볼 수 있습니다.

상관관계가 있는 객체에 대한 시간 범위를 지정합니다.

성능 탐색기 페이지의 시간 범위 선택기를 사용하면 개체 데이터 비교에 대한 시간 범위를 지정할 수 있습니다. 시간 범위를 지정하면 성능 탐색기 페이지의 내용이 세분화되어 지정한 시간 범위 내의 개체 데이터만 표시됩니다.

시간 범위를 세분화하면 관심 있는 성과 데이터만 효율적으로 표시할 수 있습니다. 미리 정의된 시간 범위를 선택하거나 사용자 지정 시간 범위를 지정할 수 있습니다. 기본 시간 범위는 이전 72시간입니다.

미리 정의된 시간 범위를 선택하세요

미리 정의된 시간 범위를 선택하면 클러스터 개체 성능 데이터를 볼 때 데이터 출력을 사용자 지정하고 집중할 수 있는 빠르고 효율적인 방법입니다. 미리 정의된 시간 범위를 선택하면 최대 13개월 동안의 데이터를 사용할 수 있습니다.

단계

1. 성능 탐색기 페이지의 오른쪽 상단에서 *시간 범위*를 클릭합니다.
2. 시간 범위 선택 패널의 오른쪽에서 미리 정의된 시간 범위를 선택합니다.
3. *범위 적용*을 클릭합니다.

사용자 정의 시간 범위 지정

성과 탐색기 페이지를 사용하면 성과 데이터의 날짜 및 시간 범위를 지정할 수 있습니다. 사용자 지정 시간 범위를 지정하면 클러스터 개체 데이터를 구체화할 때 사전 정의된 시간 범위를 사용하는 것보다 더 큰 유연성을 제공합니다.

1시간에서 390일 사이의 시간 범위를 선택할 수 있습니다. 13개월은 390일입니다. 왜냐하면 각 달은 30일로 계산되기 때문입니다. 날짜와 시간 범위를 지정하면 더 자세한 정보를 얻을 수 있으며, 특정 성과 이벤트나 일련의 이벤트를 확대해서 살펴볼 수 있습니다. 시간 범위를 지정하면 잠재적인 성능 문제를 해결하는 데 도움이 됩니다. 날짜와 시간 범위를 지정하면 성능 이벤트와 관련된 데이터가 더 자세히 표시되기 때문입니다. 시간 범위 컨트롤을 사용하여 미리 정의된 날짜 및 시간 범위를 선택하거나 최대 390일까지 사용자 정의 날짜 및 시간 범위를 지정하세요. 미리 정의된 시간 범위에 대한 버튼은 *지난 1시간*부터 *지난 13개월*까지 다양합니다.

최근 **13**개월 옵션을 선택하거나 30일보다 큰 사용자 지정 날짜 범위를 지정하면 30일보다 큰 기간에 대한 성과 데이터가 5분 단위의 데이터 폴링이 아닌 시간 평균을 사용하여 차트로 표시된다는 경고 대화 상자가 나타납니다. 따라서 타임라인의 시각적 세분성이 손실될 수 있습니다. 대화 상자에서 다시 표시 안 함 옵션을 클릭하면 지난 **13**개월 옵션을 선택하거나 30일보다 큰 사용자 지정 날짜 범위를 지정해도 메시지가 나타나지 않습니다. 요약 데이터는 오늘로부터 30일 이상의 시간/날짜가 포함된 경우 더 짧은 시간 범위에도 적용됩니다.

시간 범위(사용자 지정 또는 사전 정의)를 선택할 때 30일 이하의 시간 범위는 5분 간격의 데이터 샘플을 기준으로 합니다. 30일 이상의 시간 범위는 1시간 간격의 데이터 샘플을 기준으로 합니다.

The screenshot displays a time range selection interface. It features two calendar views for April 2015. The 'From' calendar shows the 12th selected, and the 'To' calendar shows the 15th selected. To the right of the calendars is a list of predefined time ranges: 'Last Hour', 'Last 24 Hours', 'Last 72 Hours', 'Last 7 Days', 'Last 30 Days', 'Last 13 Months', and 'Custom Range'. Below the calendars are two 'Time' dropdown menus, both set to '6:00 am'. At the bottom right are 'Cancel' and 'Apply Range' buttons.

1. 시간 범위 드롭다운 상자를 클릭하면 시간 범위 패널이 표시됩니다.
2. 미리 정의된 시간 범위를 선택하려면 시간 범위 패널 오른쪽에 있는 마지막... 버튼 중 하나를 클릭합니다. 미리

정의된 시간 범위를 선택하면 최대 13개월 동안의 데이터를 사용할 수 있습니다. 선택한 사전 정의된 시간 범위 버튼이 강조 표시되고, 해당 날짜와 시간이 달력과 시간 선택기에 표시됩니다.

3. 사용자 지정 날짜 범위를 선택하려면 왼쪽의 시작 달력에서 시작 날짜를 클릭하세요. 달력에서 앞이나 뒤로 이동하려면 <* 또는 >를 클릭하세요. 종료 날짜를 지정하려면 오른쪽의 *종료 달력에서 날짜를 클릭하세요. 다른 종료 날짜를 지정하지 않는 한 기본 종료 날짜는 오늘입니다. 시간 범위 패널 오른쪽에 있는 사용자 지정 범위 버튼이 강조 표시되어 사용자 지정 날짜 범위를 선택했음을 나타냅니다.
4. 사용자 지정 시간 범위를 선택하려면 시작 달력 아래의 시간 컨트롤을 클릭하고 시작 시간을 선택하세요. 종료 시간을 지정하려면 오른쪽의 종료 달력 아래에 있는 시간 컨트롤을 클릭하고 종료 시간을 선택하세요. 시간 범위 패널 오른쪽에 있는 사용자 지정 범위 버튼이 강조 표시되어 사용자 지정 시간 범위를 선택했음을 나타냅니다.
5. 선택적으로, 미리 정의된 날짜 범위를 선택할 때 시작 시간과 종료 시간을 지정할 수 있습니다. 이전에 설명한 대로 미리 정의된 날짜 범위를 선택한 다음, 이전에 설명한 대로 시작 시간과 종료 시간을 선택합니다. 선택한 날짜는 달력에서 강조 표시되고, 지정한 시작 및 종료 시간은 시간 컨트롤에 표시되며, 사용자 지정 범위 버튼이 강조 표시됩니다.
6. 날짜와 시간 범위를 선택한 후 *범위 적용*을 클릭하세요. 해당 기간의 성과 통계는 차트와 이벤트 타임라인에 표시됩니다.

비교 그래프를 위한 상관관계가 있는 객체 목록 정의

카운터 차트 창에서 데이터와 성과를 비교하기 위해 상관관계가 있는 개체 목록을 정의할 수 있습니다. 예를 들어, 스토리지 가상 머신(SVM)에 성능 문제가 발생하는 경우 SVM의 모든 볼륨을 비교하여 어떤 볼륨이 문제를 일으키는지 파악할 수 있습니다.

상관관계가 있는 개체 그리드에 있는 모든 개체를 비교 및 카운터 차트 창에 추가할 수 있습니다. 이를 통해 여러 개체의 데이터를 보고 루트 개체와 비교할 수 있습니다. 상관관계가 있는 객체 그리드에서 객체를 추가하거나 제거할 수 있습니다. 그러나 비교 창의 루트 객체는 제거할 수 없습니다.



비교 창에 많은 객체를 추가하면 성능에 부정적인 영향을 미칠 수 있습니다. 성과를 유지하려면 데이터 비교를 위해 제한된 수의 차트를 선택해야 합니다.

단계

1. 개체 그리드에서 추가하려는 개체를 찾아 추가 버튼을 클릭합니다.

추가 버튼이 회색으로 바뀌고, 해당 개체가 비교 창의 추가 개체 목록에 추가됩니다. 해당 개체의 데이터는 카운터 차트 창의 그래프에 추가됩니다. 객체의 눈 아이콘의 색상()는 그래프에서 개체의 데이터 추세선 색상과 일치합니다.

2. 선택 사항: 선택한 개체의 데이터를 숨기거나 표시합니다.

이렇게 하려면...	이 작업을 수행하세요...
선택한 객체 숨기기	선택한 객체의 눈 모양 아이콘을 클릭합니다. ) 비교 창에서. 해당 객체의 데이터는 숨겨지고, 해당 객체의 눈 아이콘은 회색으로 바뀝니다.

이렇게 하려면...	이 작업을 수행하세요...
숨겨진 개체 표시	비교 창에서 선택한 개체의 회색 눈 아이콘을 클릭합니다. 눈 모양 아이콘이 원래 색상으로 돌아오고, 개체 데이터가 카운터 차트 창의 그래프에 다시 추가됩니다.

3. 선택 사항: 비교 창에서 선택한 객체를 제거합니다.

이렇게 하려면...	이 작업을 수행하세요...
선택한 개체 제거	비교 창에서 선택한 개체의 이름 위에 마우스를 올려놓으면 개체 제거 버튼(X)이 나타나고, 해당 버튼을 클릭합니다. 해당 개체가 비교 창에서 제거되고, 해당 데이터는 카운터 차트에서 지워집니다.
선택한 모든 개체 제거	비교 창 상단에 있는 모든 개체 제거 버튼(X)을 클릭합니다. 선택된 모든 개체와 해당 데이터가 제거되고 루트 개체만 남습니다.

카운터 차트 이해하기

카운터 차트 창의 차트를 사용하면 루트 개체와 상관관계가 있는 개체 그리드에서 추가한 개체에 대한 성능 데이터를 보고 비교할 수 있습니다. 이를 통해 성과 추세를 이해하고 성과 문제를 분리하여 해결할 수 있습니다.

기본적으로 표시되는 카운터 차트는 이벤트, 대기 시간, IOPS, MBps입니다. 선택하여 표시할 수 있는 선택적 차트로는 활용률, 사용된 성능 용량, 사용 가능한 IOPS, IOPS/TB, 캐시 미스 비율 등이 있습니다. 또한 대기 시간, IOPS, MBps, 성능 용량 사용 차트에 대한 전체 값이나 세부 값을 볼 수 있습니다.

성능 탐색기는 기본적으로 특정 카운터 차트를 표시합니다. 스토리지 개체가 모든 카운터 차트를 지원하는지 여부는 중요하지 않습니다. 카운터가 지원되지 않으면 카운터 차트가 비어 있고 메시지가 표시됩니다. Not applicable for <object> 표시됩니다.

차트는 루트 개체와 비교 창에서 선택한 모든 개체에 대한 성능 추세를 표시합니다. 각 차트의 데이터는 다음과 같이 정리됩니다.

- **X축**

지정된 기간을 표시합니다. 시간 범위를 지정하지 않으면 기본값은 이전 72시간 기간입니다.

- **Y축**

선택한 개체에 고유한 카운터 단위를 표시합니다.

추세선 색상은 비교 창에 표시된 개체 이름의 색상과 일치합니다. 추세선의 특정 지점 위에 커서를 놓으면 해당 지점의 시간과 가치에 대한 세부 정보를 볼 수 있습니다.

차트 내에서 특정 기간을 조사하려면 다음 방법 중 하나를 사용할 수 있습니다.

- <* 버튼을 사용하여 카운터 차트 창을 페이지 너비에 맞게 확장합니다.
- 커서가 돋보기로 바뀔 때 커서를 사용하여 차트에서 시간대의 일부를 선택하여 해당 영역에 초점을 맞추고 확대합니다. 차트 확대/축소 재설정을 클릭하면 차트를 기본 시간대로 되돌릴 수 있습니다.
- 확대 보기 버튼을 사용하면 확장된 세부 정보와 임계값 표시기가 포함된 대형 단일 카운터 차트를 표시할 수 있습니다.



가끔 추세선에 간격이 나타납니다. 이러한 차이는 Unified Manager가 스토리지 시스템에서 성능 데이터를 수집하지 못했거나 Unified Manager가 다운되었을 수 있음을 의미합니다.

성과 카운터 차트의 유형

선택한 저장 개체에 대한 카운터 값을 표시하는 표준 성능 차트가 있습니다. 각 분석 카운터 차트는 전체 값을 읽기, 쓰기 및 기타 범주로 구분하여 표시합니다. 또한, 일부 분석 카운터 차트는 확대/축소 보기에서 차트를 표시할 때 추가 세부 정보를 표시합니다.

다음 표는 사용 가능한 성능 카운터 차트를 보여줍니다.

사용 가능한 차트	차트 설명
이벤트	루트 개체의 통계 차트와 관련하여 중요, 오류, 경고 및 정보 이벤트를 표시합니다. 성과 이벤트 외에도 건강 이벤트가 표시되어 성과에 영향을 줄 수 있는 이유를 전체적으로 파악할 수 있습니다.
지연 시간 - 전체	애플리케이션 요청에 응답하는 데 필요한 시간(밀리초)입니다. 평균 지연 시간 값은 I/O 가중치를 적용한 값입니다.
지연 시간 - 고장	Latency Total에 표시된 정보와 동일하지만, 성능 데이터가 읽기, 쓰기 및 기타 지연 시간으로 구분되어 있습니다. 이 차트 옵션은 선택한 개체가 SVM, 노드, 집계, 볼륨, LUN 또는 네임스페이스인 경우에만 적용됩니다.
지연 시간 - 클러스터 구성 요소	Latency Total에 표시된 정보와 동일하지만, 클러스터 구성 요소별로 성능 데이터가 지연 시간으로 구분되어 있습니다. 이 차트 옵션은 선택한 객체가 볼륨인 경우에만 적용됩니다.
IOPS - 총	초당 처리되는 입출력 작업 수. 노드에 대해 표시되는 경우, "총계"를 선택하면 로컬 또는 원격 노드에 상주할 수 있는 이 노드를 통과하는 데이터의 IOPS가 표시되고, "총계 (로컬)"를 선택하면 현재 노드에만 상주하는 데이터의 IOPS가 표시됩니다.

사용 가능한 차트	차트 설명
IOPS - 고장	IOPS Total에 표시되는 정보와 동일하지만, 성능 데이터가 읽기, 쓰기 및 기타 IOPS로 구분되어 있습니다. 이 차트 옵션은 선택한 개체가 SVM, 노드, 집계, 볼륨, LUN 또는 네임스페이스인 경우에만 적용됩니다. 확대/축소 보기에서 표시되는 볼륨 차트에는 ONTAP에서 구성된 경우 QoS 최소 및 최대 처리량 값이 표시됩니다. 노드에 대해 표시되는 경우, "분류"를 선택하면 로컬 또는 원격 노드에 상주할 수 있는 이 노드를 통과하는 데이터에 대한 IOPS 분류가 표시되고, "분류(로컬)"를 선택하면 현재 노드에만 상주하는 데이터에 대한 IOPS 분류가 표시됩니다.
IOPS - 프로토콜	IOPS Total에 표시되는 정보와 동일하지만, 성능 데이터는 CIFS, NFS, FCP, NVMe 및 iSCSI 프로토콜 트래픽에 대한 개별 차트로 구분됩니다. 이 차트 옵션은 선택한 객체가 SVM인 경우에만 적용됩니다.
IOPS/TB - 총계	작업 부하에 의해 소비되는 총 공간을 기준으로 초당 처리되는 입출력 작업 수(테라바이트)입니다. I/O 밀도라고도 하는 이 카운터는 주어진 저장 용량으로 얼마나 많은 성능을 제공할 수 있는지 측정합니다. 줌 보기에서 볼륨 차트는 ONTAP에서 구성된 경우 예상 QoS 값과 최대 처리량 값을 표시합니다. 이 차트 옵션은 선택한 객체가 볼륨인 경우에만 적용됩니다.
MB/s - 총계	초당 객체와 주고받는 데이터의 메가바이트 수입입니다.
MB/s - 분석	MB/s 차트에 표시된 정보는 동일하지만, 처리량 데이터는 디스크 읽기, 플래시 캐시 읽기, 쓰기 및 기타로 구분됩니다. 확대/축소 보기에서 표시되는 볼륨 차트는 ONTAP에서 구성된 경우 QoS 최대 처리량 값을 표시합니다. 이 차트 옵션은 선택한 개체가 SVM, 노드, 집계, 볼륨, LUN 또는 네임스페이스인 경우에만 적용됩니다.  Flash Cache 데이터는 노드에 대해서만 표시되며, 노드에 Flash Cache 모듈이 설치된 경우에만 표시됩니다.
사용된 성능 용량 - 총계	노드 또는 집계에서 소비되는 성능 용량의 백분율입니다.

사용 가능한 차트	차트 설명
사용된 성능 용량 - 고장	성능 용량 사용된 데이터는 사용자 프로토콜과 시스템 백그라운드 프로세스로 구분됩니다. 또한, 무료로 제공되는 성능 용량도 표시됩니다.
사용 가능한 IOPS - 총계	이 객체에서 현재 사용 가능한(무료) 초당 입출력 작업 수입니다. 이 숫자는 Unified Manager가 개체가 수행할 수 있다고 계산한 총 IOPS에서 현재 사용 중인 IOPS를 뺀 결과입니다. 이 차트 옵션은 선택한 개체가 노드나 집계인 경우에만 적용됩니다.
활용도 - 총	사용 중인 객체의 사용 가능한 리소스 비율입니다. 사용률은 노드의 경우 노드 사용률, 집계의 경우 디스크 사용률, 포트의 경우 대역폭 사용률을 나타냅니다. 이 차트 옵션은 선택한 개체가 노드, 집계 또는 포트인 경우에만 적용됩니다.
캐시 미스 비율 - 전체	캐시에서 반환되는 대신 디스크에서 반환되는 클라이언트 애플리케이션의 읽기 요청 비율입니다. 이 차트 옵션은 선택한 객체가 볼륨인 경우에만 적용됩니다.

표시할 성과 차트를 선택하세요

차트 선택 드롭다운 목록을 사용하면 카운터 차트 창에 표시할 성과 카운터 차트 유형을 선택할 수 있습니다. 이를 통해 성능 요구 사항에 따라 특정 데이터와 카운터를 볼 수 있습니다.

단계

1. 카운터 차트 창에서 차트 선택 드롭다운 목록을 클릭합니다.
2. 차트 추가 또는 제거:

에게...	이렇게 하세요...
개별 차트 추가 또는 제거	표시하거나 숨기려는 차트 옆에 있는 확인란을 클릭하세요.
모든 차트 추가	*모두 선택*을 클릭하세요
모든 차트 제거	*모두 선택 해제*를 클릭하세요

선택한 차트는 카운터 차트 창에 표시됩니다. 차트를 추가하면 새 차트가 '차트 선택' 드롭다운 목록에 나열된 차트 순서와 일치하도록 '카운터 차트' 창에 삽입됩니다. 추가 차트를 선택하려면 추가로 스크롤해야 할 수도 있습니다.

카운터 차트 창 확장

카운터 차트 창을 확장하면 차트를 더 크고 읽기 쉽게 볼 수 있습니다.

비교 개체와 카운터의 시간 범위를 정의한 후에는 더 큰 카운터 차트 창을 볼 수 있습니다. 성능 탐색기 창 가운데에 있는 *< 버튼을 사용하여 창을 확장합니다.

단계

1. 카운터 차트 창을 확장하거나 축소합니다.

에게...	이렇게 하세요...
페이지 너비에 맞게 카운터 차트 창을 확장합니다.	< 버튼을 클릭하세요
카운터 차트 창을 페이지의 오른쪽 절반으로 줄입니다.	> 버튼을 클릭하세요

카운터 차트 초점을 더 짧은 기간으로 변경합니다.

카운터 차트 창이나 카운터 차트 확대/축소 보기 창에서 마우스를 사용하여 시간 범위를 줄여 특정 기간에 초점을 맞출 수 있습니다. 이를 통해 성능 데이터, 이벤트 및 임계값의 타임라인의 모든 부분을 보다 세부적이고 세부적으로 볼 수 있습니다.

시작하기 전에

이 기능이 활성화되어 있음을 나타내려면 커서가 돋보기 모양으로 바뀌어야 합니다.



이 기능을 사용하면 더 세부적인 표시에 해당하는 값을 표시하도록 타임라인을 변경하지만, 시간 범위 선택기의 시간 및 날짜 범위는 차트의 원래 값에서 변경되지 않습니다.

단계

1. 특정 기간을 확대하려면 돋보기를 사용하여 클릭하고 마우스를 끌어 자세히 보고 싶은 영역을 강조 표시합니다.

선택한 기간의 카운터 값이 카운터 차트를 채웁니다.

2. 시간 범위 선택기에서 설정한 원래 기간으로 돌아가려면 차트 확대/축소 재설정 버튼을 클릭하세요.

카운터 차트는 원래 상태로 표시됩니다.

이벤트 타임라인에서 이벤트 세부 정보 보기

성능 탐색기의 이벤트 타임라인 창에서 모든 이벤트와 관련 세부 정보를 볼 수 있습니다. 이는 지정된 시간 범위 동안 루트 개체에서 발생한 모든 상태 및 성능 이벤트를 빠르고 효율적으로 볼 수 있는 방법으로, 성능 문제를 해결할 때 도움이 될 수 있습니다.

이벤트 타임라인 창에는 선택한 기간 동안 루트 개체에서 발생한 중요, 오류, 경고 및 정보 이벤트가 표시됩니다. 각 이벤트의 심각도에는 고유한 타임라인이 있습니다. 단일 이벤트와 여러 이벤트는 타임라인에 이벤트 점으로 표시됩니다. 이벤트 점 위에 커서를 놓으면 이벤트 세부 정보를 볼 수 있습니다. 여러 이벤트의 시각적 세부성을 높이려면 시간 범위를 줄이면 됩니다. 이를 통해 여러 이벤트를 단일 이벤트로 분산하여 각 이벤트를 별도로 보고 조사할 수 있습니다.

이벤트 타임라인의 각 성과 이벤트 점은 이벤트 타임라인 아래에 표시되는 카운터 차트 추세선의 해당 스파이크와 수직으로 정렬됩니다. 이를 통해 이벤트와 전반적인 성과 간의 직접적인 시각적 상관관계를 파악할 수 있습니다. 건강 이벤트도 타임라인에 표시되지만, 이러한 유형의 이벤트는 반드시 성과 차트 중 하나의 급증과 일치하지는 않습니다.

단계

1. 이벤트 타임라인 창에서 타임라인의 이벤트 점 위에 커서를 놓으면 해당 이벤트 지점의 이벤트 요약을 볼 수 있습니다.

팝업 대화 상자에는 이벤트 유형, 이벤트가 발생한 날짜 및 시간, 상태, 이벤트 기간에 대한 정보가 표시됩니다.

2. 하나 또는 여러 이벤트에 대한 전체 이벤트 세부 정보 보기:

이렇게 하려면...	여기를 클릭하세요...
단일 이벤트에 대한 세부 정보 보기	팝업 대화 상자에서 *이벤트 세부 정보 보기*를 클릭하세요.
여러 이벤트에 대한 세부 정보 보기	팝업 대화 상자에서 *이벤트 세부 정보 보기*를 클릭하세요.  여러 이벤트 대화 상자에서 단일 이벤트를 클릭하면 해당 이벤트 세부 정보 페이지가 표시됩니다.

카운터 차트 확대 보기

카운터 차트는 지정된 기간 동안의 성과 세부 정보를 확대해서 볼 수 있는 확대 보기를 제공합니다. 이를 통해 성능 세부 정보와 이벤트를 훨씬 더 세부적으로 볼 수 있어 성능 문제를 해결할 때 유용합니다.

확대 보기에서 표시될 경우 일부 세부 차트는 확대 보기가 아닐 때 표시되는 것보다 추가 정보를 제공합니다. 예를 들어, IOPS, IOPS/TB 및 MBps 분석 차트 확대/축소 보기 페이지에는 ONTAP에 설정된 볼륨 및 LUN에 대한 QoS 정책 값이 표시됩니다.



시스템 정의 성능 임계값 정책의 경우, 정책 목록에서 “노드 리소스 과도하게 사용됨” 및 “QoS 처리량 제한 위반” 정책만 사용할 수 있습니다. 현재 다른 시스템 정의 임계값 정책을 사용할 수 없습니다.

카운터 차트 확대/축소 보기 표시

카운터 차트 확대/축소 보기는 선택한 카운터 차트와 관련 타임라인에 대한 세부 정보를 더욱 자세하게 보여줍니다. 이를 통해 카운터 차트 데이터가 확대되어 성과 이벤트와 그 근본 원인을 더욱 명확하게 볼 수 있습니다.

모든 카운터 차트에 대해 카운터 차트 확대/축소 보기를 표시할 수 있습니다.

단계

1. *확대 보기*를 클릭하면 선택한 차트가 새 브라우저 창에 열립니다.
2. 세부내역 차트를 보고 있을 때 *확대 보기*를 클릭하면 세부내역 차트가 확대 보기로 표시됩니다. 확대/축소 보기에서 *전체*를 선택하면 보기 옵션을 변경할 수 있습니다.

확대/축소 보기에서 시간 범위를 지정합니다.

카운터 차트 확대/축소 보기 창의 시간 범위 컨트롤을 사용하면 선택한 차트에 대한 날짜 및 시간 범위를 지정할 수 있습니다. 이를 통해 사전 설정된 시간 범위나 사용자가 지정한 시간 범위를 기준으로 특정 데이터를 빠르게 찾을 수 있습니다.

1시간에서 390일 사이의 시간 범위를 선택할 수 있습니다. 13개월은 390일입니다. 왜냐하면 각 달은 30일로 계산되기 때문입니다. 날짜와 시간 범위를 지정하면 더 자세한 정보를 얻을 수 있으며, 특정 성과 이벤트나 일련의 이벤트를 확대해서 살펴볼 수 있습니다. 시간 범위를 지정하면 잠재적인 성능 문제를 해결하는 데 도움이 됩니다. 날짜와 시간 범위를 지정하면 성능 이벤트와 관련된 데이터가 더 자세히 표시되기 때문입니다. 시간 범위 컨트롤을 사용하여 미리 정의된 날짜 및 시간 범위를 선택하거나 최대 390일까지 사용자 정의 날짜 및 시간 범위를 지정하세요. 미리 정의된 시간 범위에 대한 버튼은 *지난 1시간*부터 *지난 13개월*까지 다양합니다.

최근 **13**개월 옵션을 선택하거나 30일보다 큰 사용자 지정 날짜 범위를 지정하면 30일보다 큰 기간에 대한 성과 데이터가 5분 단위의 데이터 풀링이 아닌 시간 평균을 사용하여 차트로 표시된다는 경고 대화 상자가 나타납니다. 따라서 타임라인의 시각적 세분성이 손실될 수 있습니다. 대화 상자에서 다시 표시 안 함 옵션을 클릭하면 지난 **13**개월 옵션을 선택하거나 30일보다 큰 사용자 지정 날짜 범위를 지정해도 메시지가 나타나지 않습니다. 요약 데이터는 오늘로부터 30일 이상의 시간/날짜가 포함된 경우 더 짧은 시간 범위에도 적용됩니다.

시간 범위(사용자 지정 또는 사전 정의)를 선택할 때 30일 이하의 시간 범위는 5분 간격의 데이터 샘플을 기준으로 합니다. 30일 이상의 시간 범위는 1시간 간격의 데이터 샘플을 기준으로 합니다.

The screenshot displays a time range selection interface. It features two calendar views for April 2015. The 'From' calendar shows the 12th selected, and the 'To' calendar shows the 15th selected. To the right of the calendars is a list of preset ranges: 'Last Hour', 'Last 24 Hours', 'Last 72 Hours', 'Last 7 Days', 'Last 30 Days', 'Last 13 Months', and 'Custom Range'. Below the calendars are two 'Time' dropdown menus, both set to '6:00 am'. At the bottom right are 'Cancel' and 'Apply Range' buttons.

1. 시간 범위 드롭다운 상자를 클릭하면 시간 범위 패널이 표시됩니다.
2. 미리 정의된 시간 범위를 선택하려면 시간 범위 패널 오른쪽에 있는 마지막... 버튼 중 하나를 클릭합니다. 미리 정의된 시간 범위를 선택하면 최대 13개월 동안의 데이터를 사용할 수 있습니다. 선택한 사전 정의된 시간 범위 버튼이 강조 표시되고, 해당 날짜와 시간이 달력과 시간 선택기에 표시됩니다.
3. 사용자 지정 날짜 범위를 선택하려면 왼쪽의 시작 달력에서 시작 날짜를 클릭하세요. 달력에서 앞이나 뒤로 이동하려면 <* 또는 >를 클릭하세요. 종료 날짜를 지정하려면 오른쪽의 *종료 달력에서 날짜를 클릭하세요. 다른 종료 날짜를 지정하지 않는 한 기본 종료 날짜는 오늘입니다. 시간 범위 패널 오른쪽에 있는 사용자 지정 범위 버튼이 강조 표시되어 사용자 지정 날짜 범위를 선택했음을 나타냅니다.
4. 사용자 지정 시간 범위를 선택하려면 시작 달력 아래의 시간 컨트롤을 클릭하고 시작 시간을 선택하세요. 종료 시간을 지정하려면 오른쪽의 종료 달력 아래에 있는 시간 컨트롤을 클릭하고 종료 시간을 선택하세요. 시간 범위 패널 오른쪽에 있는 사용자 지정 범위 버튼이 강조 표시되어 사용자 지정 시간 범위를 선택했음을 나타냅니다.
5. 선택적으로, 미리 정의된 날짜 범위를 선택할 때 시작 시간과 종료 시간을 지정할 수 있습니다. 이전에 설명한 대로 미리 정의된 날짜 범위를 선택한 다음, 이전에 설명한 대로 시작 시간과 종료 시간을 선택합니다. 선택한 날짜는 달력에서 강조 표시되고, 지정한 시작 및 종료 시간은 시간 컨트롤에 표시되며, 사용자 지정 범위 버튼이 강조

표시됩니다.

6. 날짜와 시간 범위를 선택한 후 *범위 적용*을 클릭하세요. 해당 기간의 성과 통계는 차트와 이벤트 타임라인에 표시됩니다.

카운터 차트 확대/축소 보기에서 성능 임계값 선택

카운터 차트 확대/축소 보기에서 임계값을 적용하면 성능 임계값 이벤트 발생에 대한 자세한 보기가 제공됩니다. 이를 통해 임계값을 적용하거나 제거하고 결과를 즉시 볼 수 있어 문제 해결을 다음 단계로 삼을지 여부를 결정하는 데 도움이 될 수 있습니다.

카운터 차트 확대/축소 보기에서 임계값을 선택하면 성능 임계값 이벤트에 대한 정확한 데이터를 볼 수 있습니다. 카운터 차트 확대/축소 보기의 정책 영역에 나타나는 모든 임계값을 적용할 수 있습니다.

카운터 차트 확대/축소 보기에서는 한 번에 하나의 정책만 개체에 적용할 수 있습니다.

단계

1. 선택 또는 선택 해제  정책과 관련된 것.

선택한 임계값은 카운터 차트 확대/축소 보기에 적용됩니다. 위험 임계값은 빨간색 선으로 표시되고, 경고 임계값은 노란색 선으로 표시됩니다.

클러스터 구성 요소별 볼륨 지연 시간 보기

볼륨 성능 탐색기 페이지를 사용하면 볼륨에 대한 자세한 대기 시간 정보를 볼 수 있습니다. 대기 시간 - 전체 카운터 차트는 볼륨의 전체 대기 시간을 보여주고, 대기 시간 - 세부 카운터 차트는 볼륨에 대한 읽기 및 쓰기 대기 시간의 영향을 파악하는 데 유용합니다.

또한, 대기 시간 - 클러스터 구성 요소 차트는 각 클러스터 구성 요소의 대기 시간을 자세히 비교하여 각 구성 요소가 볼륨의 전체 대기 시간에 어떻게 기여하는지 확인하는 데 도움이 됩니다. 다음 클러스터 구성 요소가 표시됩니다.

- 회로망
- QoS 제한 최대
- QoS 제한 최소
- 네트워크 처리
- 클러스터 상호 연결
- Data Processing
- 집계 작업
- 볼륨 활성화
- MetroCluster 리소스
- 클라우드 지연 시간
- SnapMirror 동기화

단계

1. 선택한 볼륨의 볼륨 성능 탐색기 페이지에서 대기 시간 차트의 드롭다운 메뉴에서 *클러스터 구성 요소*를

선택합니다.

대기 시간 - 클러스터 구성 요소 차트가 표시됩니다.

2. 차트를 더 크게 보려면 *확대 보기*를 선택하세요.

클러스터 구성 요소 비교 차트가 표시됩니다. 선택 해제 또는 선택을 통해 비교를 제한할 수 있습니다.  각 클러스터 구성 요소와 연관되어 있습니다.

3. 구체적인 값을 보려면 커서를 차트 영역으로 옮겨 팝업 창을 확인하세요.

프로토콜별 SVM IOPS 트래픽 보기

성능/SVM 탐색기 페이지를 사용하면 SVM에 대한 자세한 IOPS 정보를 볼 수 있습니다. IOPS - 전체 카운터 차트는 SVM에서의 전체 IOPS 사용량을 보여주고, IOPS - 세부 카운터 차트는 SVM에서 읽기, 쓰기 및 기타 IOPS의 영향을 파악하는 데 유용합니다.

또한, IOPS - 프로토콜 차트는 SVM에서 사용되는 각 프로토콜에 대한 IOPS 트래픽을 자세히 비교한 결과를 보여줍니다. 사용 가능한 프로토콜은 다음과 같습니다.

- CIFS
- NFS
- FCP
- iSCSI
- NVMe-FC

단계

1. 선택한 SVM의 성능/**SVM** 탐색기 페이지에서 IOPS 차트의 드롭다운 메뉴에서 *프로토콜*을 선택합니다.

IOPS - 프로토콜 차트가 표시됩니다.

2. 차트를 더 크게 보려면 *확대 보기*를 선택하세요.

IOPS 고급 프로토콜 비교 차트가 표시됩니다. 선택 해제 또는 선택을 통해 비교를 제한할 수 있습니다.  프로토콜과 관련된 것.

3. 구체적인 값을 보려면 두 차트 중 하나의 차트 영역으로 커서를 옮겨 팝업 창을 확인하세요.

성능 보장을 확인하려면 볼륨 및 LUN 지연 차트를 확인하세요.

"성능 보장" 프로그램에 가입한 볼륨과 LUN을 확인하여 지연 시간이 보장된 수준을 초과하지 않았는지 확인할 수 있습니다.

지연 성능 보장은 초과해서는 안 되는 작업당 밀리초 값입니다. 이는 기본 5분 성과 수집 기간이 아닌 시간당 평균을 기준으로 합니다.

단계

1. 성능: 모든 볼륨 보기 또는 성능: 모든 LUN 보기에서 관심 있는 볼륨이나 LUN을 선택합니다.

2. 선택한 볼륨이나 LUN의 성능 탐색기 페이지에서 통계 보기 선택기에서 *시간 평균*을 선택합니다.

대기 시간 차트의 수평선은 5분 단위 수집이 시간당 평균으로 바뀌면서 더 부드러운 선으로 표시됩니다.

3. 동일한 집계에 성능 보장이 적용되는 다른 볼륨이 있는 경우 해당 볼륨을 추가하여 동일한 차트에서 해당 볼륨의 지연 시간 값을 볼 수 있습니다.

모든 SAN 어레이 클러스터의 성능 보기

성능: 모든 클러스터 보기를 사용하면 모든 SAN 어레이 클러스터의 성능 상태를 표시할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

모든 SAN 어레이 클러스터에 대한 개요 정보는 성능: 모든 클러스터 보기에서 볼 수 있으며, 세부 정보는 클러스터/성능 탐색기 페이지에서 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *클러스터*를 클릭합니다.

2. 상태: 모든 클러스터 보기에 "개성" 열이 표시되는지 확인하거나 표시/숨기기 컨트롤을 사용하여 추가하세요.

이 열에는 모든 SAN 어레이 클러스터에 대한 "모든 SAN 어레이"가 표시됩니다.

3. 해당 클러스터의 성능에 대한 정보를 보려면 성능: 모든 클러스터 보기를 선택하세요.

All SAN Array 클러스터의 성능 정보를 확인합니다.

4. 해당 클러스터의 성능에 대한 자세한 정보를 보려면 All SAN Array 클러스터의 이름을 클릭하세요.

5. 탐색기 탭을 클릭하세요.

6. 클러스터/성능 탐색기 페이지에서 보기 및 비교 메뉴에서 *이 클러스터의 노드*를 선택합니다.

이 클러스터의 두 노드의 성능 통계를 비교하면 두 노드의 부하가 거의 동일한지 확인할 수 있습니다. 두 노드 사이에 큰 차이가 있는 경우 두 번째 노드를 차트에 추가하고 더 긴 기간 동안 값을 비교하여 구성 문제를 파악할 수 있습니다.

로컬 노드에만 있는 작업 부하를 기반으로 노드 IOPS 보기

노드 IOPS 카운터 차트는 네트워크 LIF를 사용하여 원격 노드의 볼륨에 대한 읽기/쓰기 작업을 수행하는 로컬 노드를 통해서만 작업이 전달되는 위치를 강조할 수 있습니다. IOPS - "전체(로컬)" 및 "세부내역(로컬)" 차트는 현재 노드의 로컬 볼륨에만 있는 데이터의 IOPS를 표시합니다.

이러한 카운터 차트의 "로컬" 버전은 로컬 볼륨에 있는 데이터에 대한 통계만 표시하기 때문에 성능, 용량 및 활용도에 대한 노드 차트와 비슷합니다.

이러한 카운터 차트의 "로컬" 버전을 이러한 카운터 차트의 일반 전체 버전과 비교하면 원격 노드의 볼륨에 액세스하기 위해 로컬 노드를 통해 많은 트래픽이 이동하는지 확인할 수 있습니다. 로컬 노드를 통과하는 작업이 너무 많아 원격

노드의 볼륨에 도달하지 못하는 경우, 노드의 활용도가 높아져 성능 문제가 발생할 수 있습니다. 이러한 경우 볼륨을 로컬 노드로 이동하거나 해당 볼륨에 액세스하는 호스트의 트래픽을 연결할 수 있는 원격 노드에 LIF를 만들 수 있습니다.

단계

1. 선택한 노드의 성능/노드 탐색기 페이지에서 IOPS 차트의 드롭다운 메뉴에서 *전체*를 선택합니다.

IOPS - 전체 차트가 표시됩니다.

2. *확대 보기*를 클릭하면 새 브라우저 탭에서 차트의 더 큰 버전을 볼 수 있습니다.
3. 성능/노드 탐색기 페이지로 돌아가서 IOPS 차트의 드롭다운 메뉴에서 *전체(로컬)*를 선택합니다.

IOPS - 전체(로컬) 차트가 표시됩니다.

4. *확대 보기*를 클릭하면 새 브라우저 탭에서 차트의 더 큰 버전을 볼 수 있습니다.
5. 두 차트를 나란히 보고 IOPS 값이 상당히 다른 영역을 파악해 보세요.
6. 특정 시점의 로컬 IOPS와 전체 IOPS를 비교하려면 커서를 이 영역 위로 이동하세요.

객체 랜딩 페이지의 구성 요소

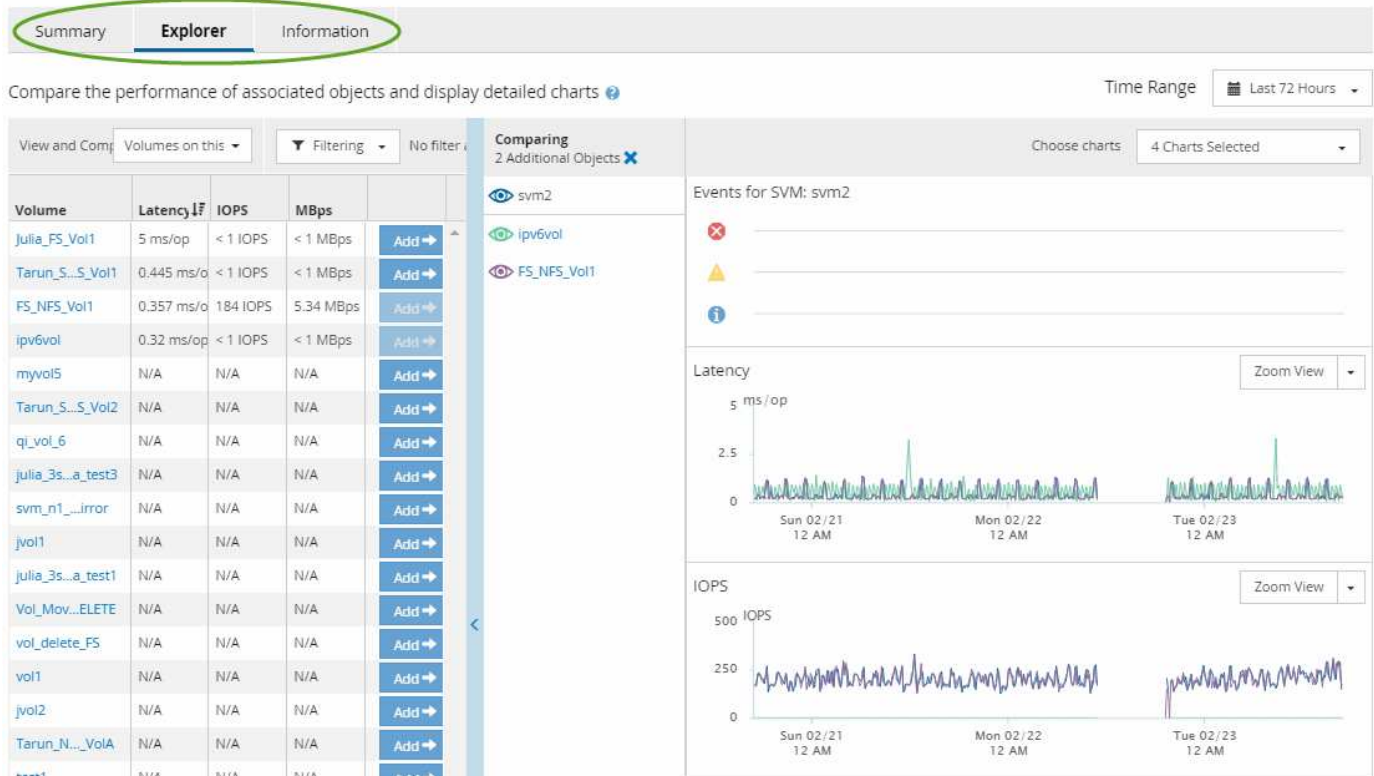
객체 랜딩 페이지는 모든 중요, 경고, 정보 이벤트에 대한 세부 정보를 제공합니다. 이러한 기능은 모든 클러스터 객체의 성능에 대한 자세한 보기를 제공하여 다양한 기간 동안 개별 객체를 선택하고 비교할 수 있도록 해줍니다.

객체 랜딩 페이지를 사용하면 모든 객체의 전반적인 성능을 검토하고, 객체 성능 데이터를 나란히 비교할 수 있습니다. 이는 성능을 평가하고 이벤트 문제를 해결할 때 유용합니다.



카운터 요약 패널과 카운터 차트에 표시되는 데이터는 5분 샘플링 간격을 기준으로 합니다. 페이지 왼쪽의 객체 인벤토리 그리드에 표시되는 데이터는 1시간 샘플링 간격을 기준으로 합니다.

다음 이미지는 탐색기 정보를 표시하는 개체 랜딩 페이지의 예를 보여줍니다.



보고 있는 저장소 객체에 따라 객체 랜딩 페이지에는 해당 객체에 대한 성능 데이터를 제공하는 다음과 같은 탭이 있을 수 있습니다.

- 요약

이전 72시간 동안의 이벤트와 개체별 성과를 담은 3~4개의 카운터 차트를 표시하며, 해당 기간 동안의 최고값과 최저값을 보여주는 추세선도 포함됩니다.

- 탐침

현재 개체와 관련된 저장소 개체의 그리드를 표시하여 현재 개체의 성능 값을 관련 개체의 성능 값과 비교할 수 있습니다. 이 탭에는 최대 11개의 카운터 차트와 시간 범위 선택기가 포함되어 있어 다양한 비교를 수행할 수 있습니다.

- 정보

ONTAP 소프트웨어의 설치된 버전, HA 파트너 이름, 포트 및 LIF 수를 포함하여 스토리지 개체에 대한 비성능 구성 속성 값을 표시합니다.

- 최고의 성과자들

클러스터의 경우: 선택한 성능 카운터를 기준으로 가장 높은 성능이나 가장 낮은 성능을 가진 스토리지 개체를 표시합니다.

- 장애 조치 계획

노드의 경우: 노드의 HA 파트너가 실패할 경우 노드의 성능에 미치는 영향의 추정치를 표시합니다.

- 세부

볼륨의 경우: 선택한 볼륨 작업 부하에 대한 모든 I/O 활동 및 작업에 대한 자세한 성능 통계를 표시합니다. 이 탭은 FlexVol 볼륨, FlexGroup 볼륨 및 FlexGroup 구성 요소에 사용할 수 있습니다.

요약 페이지

요약 페이지에는 지난 72시간 동안의 이벤트 및 개체별 성능에 대한 세부 정보가 포함된 카운터 차트가 표시됩니다. 이 데이터는 자동으로 새로 고쳐지지 않지만, 마지막 페이지 로드 시점을 기준으로 최신 상태입니다. 요약 페이지의 차트는 _더 살펴볼 필요가 있을까?_라는 질문에 대한 답을 제공합니다.

차트 및 카운터 통계

요약 차트는 지난 72시간 동안의 빠르고 간략한 개요를 제공하며, 추가 조사가 필요한 잠재적 문제를 식별하는 데 도움이 됩니다.

요약 페이지 카운터 통계는 그래프로 표시됩니다.

그래프의 추세선 위에 커서를 놓으면 특정 시점의 카운터 값을 볼 수 있습니다. 요약 차트에는 다음 카운터에 대한 이전 72시간 동안의 총 활성 위험 및 경고 이벤트 수도 표시됩니다.

- 숨어 있음

모든 I/O 요청에 대한 평균 응답 시간입니다. 작업당 밀리초로 표시됩니다.

모든 객체 유형에 대해 표시됩니다.

- IOPS

평균 작업 속도. 초당 입력/출력 작업으로 표현됩니다.

모든 객체 유형에 대해 표시됩니다.

- MB/초

평균 처리량, 초당 메가바이트로 표현.

모든 객체 유형에 대해 표시됩니다.

- 사용된 성능 용량

노드 또는 집계에서 사용되는 성능 용량의 백분율입니다.

노드와 집계에만 표시됩니다.

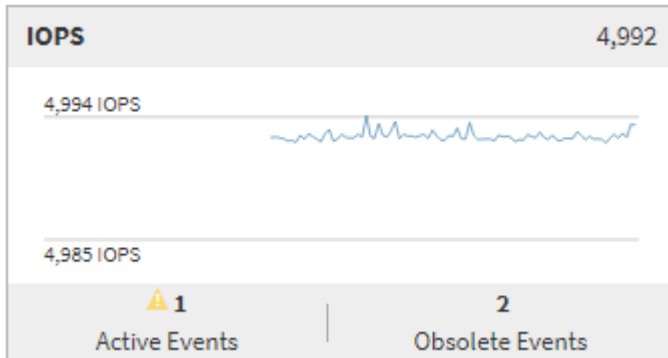
- 이용

노드 및 집계에 대한 개체 활용률 또는 포트에 대한 대역폭 활용률입니다.

노드, 집계 및 포트에만 표시됩니다.

활성 이벤트의 이벤트 수 위에 커서를 놓으면 이벤트의 유형과 수가 표시됩니다. 중요 이벤트는 빨간색으로 표시됩니다 (■), 경고 이벤트는 노란색으로 표시됩니다(■).

차트의 오른쪽 상단 회색 막대에 있는 숫자는 지난 72시간 동안의 평균값입니다. 추세선 그래프의 하단과 상단에 표시된 숫자는 지난 72시간 동안의 최소값과 최대값입니다. 차트 아래의 회색 막대에는 지난 72시간 동안의 활성(새 이벤트와 확인된 이벤트) 이벤트와 사용되지 않는 이벤트 수가 포함되어 있습니다.



• 지연 카운터 차트

대기 시간 카운터 차트는 이전 72시간 동안의 객체 대기 시간에 대한 개요를 제공합니다. 대기 시간은 모든 I/O 요청에 대한 평균 응답 시간을 말하며, 작업당 밀리초로 표현되며, 고려 중인 클러스터 스토리지 구성 요소에서 데이터 패킷이나 블록이 경험하는 서비스 시간, 대기 시간 또는 둘 다를 의미합니다.

상단(카운터 값): 헤더의 숫자는 이전 72시간 동안의 평균을 표시합니다.

중간(성능 그래프): 그래프 하단의 숫자는 가장 낮은 지연 시간을 표시하고, 그래프 상단의 숫자는 이전 72시간 동안의 가장 높은 지연 시간을 표시합니다. 특정 시간의 대기 시간 값을 보려면 그래프 추세선 위에 커서를 놓으세요.

하단(이벤트): 마우스를 올리면 팝업에 이벤트 세부 정보가 표시됩니다. 그래프 아래의 활성 이벤트 링크를 클릭하면 이벤트 인벤토리 페이지로 이동하여 전체 이벤트 세부 정보를 볼 수 있습니다.

• IOPS 카운터 차트

IOPS 카운터 차트는 이전 72시간 동안의 개체 IOPS 상태에 대한 개요를 제공합니다. IOPS는 초당 입출력 작업 수로 저장 시스템의 속도를 나타냅니다.

상단(카운터 값): 헤더의 숫자는 이전 72시간 동안의 평균을 표시합니다.

중간(성능 그래프): 그래프 하단의 숫자는 가장 낮은 IOPS를 표시하고, 그래프 상단의 숫자는 이전 72시간 동안의 가장 높은 IOPS를 표시합니다. 특정 시간의 IOPS 값을 보려면 그래프 추세선 위에 커서를 놓으세요.

하단(이벤트): 마우스를 올리면 팝업에 이벤트 세부 정보가 표시됩니다. 그래프 아래의 활성 이벤트 링크를 클릭하면 이벤트 인벤토리 페이지로 이동하여 전체 이벤트 세부 정보를 볼 수 있습니다.

• MB/s 카운터 차트

MB/s 카운터 차트는 객체 MB/s 성능을 표시하고, 초당 메가바이트 단위로 객체와 주고받은 데이터 양을 나타냅니다. MB/s 카운터 차트는 지난 72시간 동안의 객체의 MB/s 상태에 대한 개요를 제공합니다.

상단(카운터 값): 헤더의 숫자는 이전 72시간 동안의 평균 MB/s 수를 표시합니다.

중간(성능 그래프): 그래프 하단의 값은 가장 낮은 MB/s 수를 표시하고, 그래프 상단의 값은 이전 72시간 동안의

가장 높은 MB/s 수를 표시합니다. 특정 시간의 MB/s 값을 보려면 그래프 추세선 위에 커서를 놓으세요.

하단(이벤트): 마우스를 올리면 팝업에 이벤트 세부 정보가 표시됩니다. 그래프 아래의 활성 이벤트 링크를 클릭하면 이벤트 인벤토리 페이지로 이동하여 전체 이벤트 세부 정보를 볼 수 있습니다.

- 성능 용량 사용 카운터 차트

사용된 성능 용량 카운터 차트는 개체에서 사용되는 성능 용량의 백분율을 표시합니다.

상단(카운터 값): 헤더의 숫자는 이전 72시간 동안 사용된 평균 성능 용량을 표시합니다.

중간(성능 그래프): 그래프 하단의 값은 사용된 성능 용량의 가장 낮은 백분율을 표시하고, 그래프 상단의 값은 이전 72시간 동안 사용된 성능 용량의 가장 높은 백분율을 표시합니다. 특정 시간 동안 사용된 성능 용량 값을 보려면 그래프 추세선 위에 커서를 놓으세요.

하단(이벤트): 마우스를 올리면 팝업에 이벤트 세부 정보가 표시됩니다. 그래프 아래의 활성 이벤트 링크를 클릭하면 이벤트 인벤토리 페이지로 이동하여 전체 이벤트 세부 정보를 볼 수 있습니다.

- 활용 카운터 차트

활용 카운터 차트는 객체 활용률을 표시합니다. 사용률 카운터 차트는 이전 72시간 동안의 객체 또는 대역폭 사용을 백분율에 대한 개요를 제공합니다.

상단(카운터 값): 헤더의 숫자는 이전 72시간 동안의 평균 활용률을 표시합니다.

중간(성능 그래프): 그래프 하단의 값은 가장 낮은 활용률을 표시하고, 그래프 상단의 값은 이전 72시간 동안의 가장 높은 활용률을 표시합니다. 특정 시간의 활용도 값을 보려면 그래프 추세선 위에 커서를 놓으세요.

하단(이벤트): 마우스를 올리면 팝업에 이벤트 세부 정보가 표시됩니다. 그래프 아래의 활성 이벤트 링크를 클릭하면 이벤트 인벤토리 페이지로 이동하여 전체 이벤트 세부 정보를 볼 수 있습니다.

이벤트

해당되는 경우 이벤트 기록 표에는 해당 개체에서 발생한 가장 최근 이벤트가 나열됩니다. 이벤트 이름을 클릭하면 이벤트 세부 정보 페이지에 이벤트 세부 정보가 표시됩니다.

성능 탐색기 페이지의 구성 요소

성능 탐색기 페이지를 사용하면 클러스터 내의 유사한 개체(예: 클러스터 내의 모든 볼륨)의 성능을 비교할 수 있습니다. 이 기능은 성능 이벤트 문제를 해결하고 개체 성능을 미세 조정할 때 유용합니다. 또한 객체를 루트 객체와 비교할 수도 있는데, 루트 객체는 다른 객체를 비교하는 기준이 됩니다.

상태 보기로 전환 버튼을 클릭하면 이 개체의 상태 세부 정보 페이지가 표시됩니다. 어떤 경우에는 문제를 해결하는 데 도움이 될 수 있는 이 개체의 저장소 구성 설정에 대한 중요한 정보를 알아볼 수 있습니다.

성능 탐색기 페이지에는 클러스터 개체 목록과 해당 성능 데이터가 표시됩니다. 이 페이지는 동일한 유형의 모든 클러스터 개체(예: 볼륨 및 개체별 성능 통계)를 표 형식으로 표시합니다. 이 보기는 클러스터 개체 성능에 대한 효율적인 개요를 제공합니다.



표의 어떤 셀에든 "N/A"가 나타나면 해당 개체에 대한 I/O가 현재 없기 때문에 해당 카운터에 대한 값을 사용할 수 없음을 의미합니다.

성능 탐색기 페이지에는 다음 구성 요소가 포함되어 있습니다.

- 시간 범위

개체 데이터의 시간 범위를 선택할 수 있습니다.

미리 정의된 범위를 선택하거나 사용자 정의 시간 범위를 지정할 수 있습니다.

- 보기 및 비교

그리드에 표시할 상관관계 객체의 유형을 선택할 수 있습니다.

사용 가능한 옵션은 루트 개체 유형과 사용 가능한 데이터에 따라 달라집니다. 보기 및 비교 드롭다운 목록을 클릭하여 개체 유형을 선택할 수 있습니다. 선택한 개체 유형이 목록에 표시됩니다.

- 필터링

사용자의 선호도에 따라 수신하는 데이터 양을 줄일 수 있습니다.

개체 데이터에 적용되는 필터(예: IOPS가 4보다 큰 경우)를 만들 수 있습니다. 최대 4개의 필터를 동시에 추가할 수 있습니다.

- 비교

루트 개체와 비교하기 위해 선택한 개체 목록을 표시합니다.

비교 창에 있는 개체의 데이터는 카운터 차트에 표시됩니다.

- 통계 보기

볼륨 및 LUN의 경우 통계를 각 수집 주기(기본값 5분) 후에 표시할지, 아니면 통계를 시간당 평균으로 표시할지 선택할 수 있습니다. 이 기능을 사용하면 NetApp "성능 보장" 프로그램을 지원하는 지연 시간 차트를 볼 수 있습니다.

- 카운터 차트

각 개체 성능 범주에 대한 그래프 데이터를 표시합니다.

일반적으로 기본적으로 3~4개의 차트만 표시됩니다. 차트 선택 구성 요소를 사용하면 추가 차트를 표시하거나 특정 차트를 숨길 수 있습니다. 이벤트 타임라인을 표시하거나 숨기도록 선택할 수도 있습니다.

- 이벤트 타임라인

시간 범위 구성 요소에서 선택한 타임라인에서 발생하는 성능 및 상태 이벤트를 표시합니다.

QoS 정책 그룹 정보를 사용하여 성능 관리

Unified Manager를 사용하면 모니터링 중인 모든 클러스터에서 사용 가능한 서비스 품질(QoS)

정책 그룹을 볼 수 있습니다. 정책은 ONTAP 소프트웨어(System Manager 또는 ONTAP CLI) 또는 Unified Manager 성능 서비스 수준 정책을 사용하여 정의되었을 수 있습니다. Unified Manager는 QoS 정책 그룹이 할당된 볼륨과 LUN도 표시합니다.

QoS 설정 조정에 대한 자세한 내용은 다음을 참조하세요. ["성과 관리 개요"](#)

스토리지 **QoS**가 작업 부하 처리량을 제어하는 방법

워크로드에 대한 초당 I/O(IOPS) 또는 처리량(MB/s) 제한을 제어하기 위해 QoS(서비스 품질) 정책 그룹을 만들 수 있습니다. 워크로드가 기본 정책 그룹과 같이 설정된 제한이 없는 정책 그룹에 있는 경우 또는 설정된 제한이 요구 사항을 충족하지 못하는 경우 제한을 늘리거나 원하는 제한이 있는 새 정책 그룹이나 기존 정책 그룹으로 워크로드를 이동할 수 있습니다.

"기존" QoS 정책 그룹은 개별 작업 부하(예: 단일 볼륨 또는 LUN)에 할당될 수 있습니다. 이 경우 작업 부하가 전체 처리량 한도를 사용할 수 있습니다. QoS 정책 그룹은 여러 작업 부하에 할당될 수도 있습니다. 이 경우 처리량 제한은 작업 부하 간에 "공유"됩니다. 예를 들어, 3개의 작업 부하에 9,000 IOPS의 QoS 제한을 할당하면 결합된 IOPS가 9,000 IOPS를 초과하지 못합니다.

"적응형" QoS 정책 그룹은 개별 작업 부하나 여러 작업 부하에 할당될 수도 있습니다. 그러나 여러 작업 부하에 할당된 경우에도 각 작업 부하에는 다른 작업 부하와 처리량 값을 공유하는 대신 전체 처리량 한도가 적용됩니다. 또한, 적응형 QoS 정책은 볼륨 크기에 따라 작업 부하당 처리량 설정을 자동으로 조정하여 볼륨 크기가 변경되더라도 IOPS 대 테라바이트 비율을 유지합니다. 예를 들어, 적응형 QoS 정책에서 최대값을 5,000 IOPS/TB로 설정하면 10TB 볼륨의 처리량 최대값은 50,000 IOPS가 됩니다. 나중에 볼륨 크기가 20TB로 조정되면 적응형 QoS가 최대값을 100,000 IOPS로 조정합니다.

ONTAP 9.5부터 적응형 QoS 정책을 정의할 때 블록 크기를 포함할 수 있습니다. 워크로드가 매우 큰 블록 크기를 사용하고 궁극적으로 처리량의 큰 비율을 사용하는 경우 이를 통해 정책이 IOPS/TB 임계값에서 MB/s 임계값으로 효과적으로 변환됩니다.

공유 그룹 QoS 정책의 경우, 정책 그룹 내 모든 워크로드의 IOPS 또는 MB/s가 설정된 한도를 초과하면 정책 그룹이 워크로드를 조절하여 활동을 제한하는데, 이로 인해 정책 그룹 내 모든 워크로드의 성능이 저하될 수 있습니다. 정책 그룹 제한으로 인해 동적 성능 이벤트가 생성되면 이벤트 설명에 관련 정책 그룹의 이름이 표시됩니다.

성능: 모든 볼륨 보기에서 영향을 받은 볼륨을 IOPS 및 MB/s별로 정렬하여 이벤트에 영향을 미쳤을 수 있는 가장 높은 사용량을 가진 워크로드를 확인할 수 있습니다. 성능/볼륨 탐색기 페이지에서 다른 볼륨이나 볼륨의 LUN을 선택하여 영향을 받는 작업 부하 IOPS 또는 MBps 처리량 사용량과 비교할 수 있습니다.

노드 리소스를 과도하게 사용하는 작업 부하를 보다 제한적인 정책 그룹 설정에 할당하면 정책 그룹이 작업 부하를 조절하여 활동을 제한하고, 이를 통해 해당 노드의 리소스 사용을 줄일 수 있습니다. 하지만 작업 부하가 더 많은 노드 리소스를 사용할 수 있도록 하려면 정책 그룹의 값을 늘릴 수 있습니다.

시스템 관리자, ONTAP 명령 또는 Unified Manager 성능 서비스 수준을 사용하여 다음 작업을 포함하여 정책 그룹을 관리할 수 있습니다.

- 정책 그룹 생성
- 정책 그룹에서 작업 부하 추가 또는 제거
- 정책 그룹 간 작업 부하 이동
- 정책 그룹의 처리량 제한 변경
- 작업 부하를 다른 집계 및/또는 노드로 이동

모든 클러스터에서 사용 가능한 모든 QoS 정책 그룹 보기

Unified Manager가 모니터링하는 클러스터에서 사용 가능한 모든 QoS 정책 그룹 목록을 표시할 수 있습니다. 여기에는 기존 QoS 정책, 적응형 QoS 정책, Unified Manager 성능 서비스 수준 정책으로 관리되는 QoS 정책이 포함됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *QoS 정책 그룹*을 클릭합니다.

기본적으로 성능: 기존 QoS 정책 그룹 보기가 표시됩니다.

2. 사용 가능한 각 기존 QoS 정책 그룹에 대한 자세한 구성 설정을 확인합니다.
3. 확장 버튼을 클릭하세요 (▼) QoS 정책 그룹 이름 옆에 있는 아이콘을 클릭하면 정책 그룹에 대한 자세한 내용을 볼 수 있습니다.
4. 보기 메뉴에서 추가 옵션 중 하나를 선택하여 모든 적응형 QoS 정책 그룹을 보거나 Unified Manager 성능 서비스 수준을 사용하여 생성된 모든 QoS 정책 그룹을 봅니다.

동일한 QoS 정책 그룹에 있는 볼륨 또는 LUN 보기

동일한 QoS 정책 그룹에 할당된 볼륨 및 LUN 목록을 표시할 수 있습니다.

여러 볼륨 간에 "공유"되는 기존 QoS 정책 그룹의 경우, 특정 볼륨이 정책 그룹에 대해 정의된 처리량을 과도하게 사용하고 있는지 확인하는 데 도움이 될 수 있습니다. 또한 다른 볼륨에 부정적인 영향을 미치지 않고 정책 그룹에 다른 볼륨을 추가할 수 있는지 여부를 결정하는 데 도움이 될 수 있습니다.

적응형 QoS 정책과 Unified Manager 성능 서비스 수준 정책의 경우, 정책 그룹을 사용하는 모든 볼륨이나 LUN을 보고 QoS 정책의 구성 설정을 변경하면 어떤 개체가 영향을 받는지 확인하는 것이 도움이 될 수 있습니다.

단계

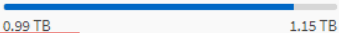
1. 왼쪽 탐색 창에서 저장소 > *QoS 정책 그룹*을 클릭합니다.

기본적으로 성능: 기존 QoS 정책 그룹 보기가 표시됩니다.

2. 전통적인 정책 그룹에 관심이 있다면 이 페이지를 계속 읽어보세요. 그렇지 않은 경우, 추가 보기 옵션 중 하나를 선택하여 모든 적응형 QoS 정책 그룹이나 Unified Manager 성능 서비스 수준에서 생성된 모든 QoS 정책 그룹을 표시합니다.
3. 관심 있는 QoS 정책에서 확장 버튼을 클릭합니다. (▼)을 클릭하면 자세한 내용을 볼 수 있습니다.

View Adaptive QoS Policy Groups Search Quality of Service

Schedule Report

QoS Policy Group	Cluster	SVM	Min Through...	Max Through...	Absolute Min...	Block Size	Asso
▼ julia_vs2_cifs_Performance	opm-simplicity	julia_vs2_cifs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		1
▲ julia_vs1_nfs_Performance	opm-simplicity	julia_vs1_nfs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		2
Details Allocated Capacity  0.99 TB 1.15 TB Associated Objects 2 Volumes 0 LUNs Events None							
▼ julia_nfs_extreme_Extreme_Performance	ocum-mobility-01-02	julia_nfs_extreme	6144.0 IOPS/TB	12288.0 IOPS/TB	1000IOPS	any	1
▼ julia_extreme_jan16_aqos	ocum-mobility-01-02	julia_nfs_extreme	10000.0 IOPS/TB	12000.0 IOPS/TB	1000IOPS	any	1

4. 이 QoS 정책을 사용하는 객체를 보려면 볼륨 또는 LUN 링크를 클릭하세요.

볼륨 또는 LUN의 성능 인벤토리 페이지에는 QoS 정책을 사용하는 개체의 정렬된 목록이 표시됩니다.

특정 볼륨 또는 **LUN**에 적용된 **QoS** 정책 그룹 설정을 확인합니다.

볼륨과 LUN에 적용된 QoS 정책 그룹을 볼 수 있으며, 성능/QoS 정책 그룹 보기에 연결하여 각 QoS 정책에 대한 자세한 구성 설정을 표시할 수 있습니다.

볼륨에 적용된 QoS 정책을 보는 단계는 아래와 같습니다. LUN에 대한 정보를 보는 단계는 비슷합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.

기본적으로 상태: 모든 볼륨 보기가 표시됩니다.

2. 보기 메뉴에서 *성능: QoS 정책 그룹의 볼륨*을 선택합니다.

3. 검토하려는 볼륨을 찾아 오른쪽으로 스크롤하여 **QoS** 정책 그룹 열이 보이도록 합니다.

4. QoS 정책 그룹 이름을 클릭합니다.

기존 QoS 정책인지, 적응형 QoS 정책인지, Unified Manager 성능 서비스 수준을 사용하여 생성된 QoS 정책인지에 따라 해당 서비스 품질 페이지가 표시됩니다.

5. QoS 정책 그룹에 대한 자세한 구성 설정을 확인합니다.

6. 확장 버튼을 클릭하세요 (▼) QoS 정책 그룹 이름 옆에 있는 아이콘을 클릭하면 정책 그룹에 대한 자세한 내용을 볼 수 있습니다.

동일한 **QoS** 정책 그룹에 있는 볼륨이나 **LUN**을 비교하기 위해 성능 차트를 봅니다.

동일한 QoS 정책 그룹에 있는 볼륨과 LUN을 보고 단일 IOPS, MB/s 또는 IOPS/TB 차트에서 성능을 비교하여 문제를 식별할 수 있습니다.

동일한 QoS 정책 그룹 내 볼륨의 성능을 비교하는 단계는 아래와 같습니다. LUN에 대한 정보를 보는 단계는 비슷합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.

기본적으로 상태: 모든 볼륨 보기가 표시됩니다.

2. 보기 메뉴에서 *성능: QoS 정책 그룹의 볼륨*을 선택합니다.
3. 검토하려는 볼륨의 이름을 클릭하세요.

볼륨에 대한 성능 탐색기 페이지가 표시됩니다.

4. 보기 및 비교 메뉴에서 *동일한 QoS 정책 그룹의 볼륨*을 선택합니다.

동일한 QoS 정책을 공유하는 다른 볼륨은 아래 표에 나열되어 있습니다.

5. 추가 버튼을 클릭하면 차트에 해당 볼륨이 추가되어 차트에서 선택한 모든 볼륨에 대한 IOPS, MB/s, IOPS/TB 및 기타 성능 카운터를 비교할 수 있습니다.

기본값인 72시간 외에도 다른 시간 간격으로 성과를 보려면 시간 범위를 변경할 수 있습니다.

처리량 차트에 다양한 유형의 QoS 정책이 표시되는 방식

볼륨이나 LUN에 적용된 ONTAP 에서 정의한 서비스 품질(QoS) 정책 설정은 성능 탐색기와 워크로드 분석 IOPS, IOPS/TB, MB/s 차트에서 볼 수 있습니다. 차트에 표시되는 정보는 작업 부하에 적용된 QoS 정책 유형에 따라 다릅니다.

처리량 최대값(또는 "피크") 설정은 작업 부하가 소비할 수 있는 최대 처리량을 정의하고, 이를 통해 시스템 리소스에 대한 경쟁 작업 부하에 미치는 영향을 제한합니다. 처리량 최소값(또는 "예상") 설정은 경쟁 워크로드의 수요에 관계없이 중요 워크로드가 최소 처리량 목표를 충족할 수 있도록 워크로드에 사용 가능해야 하는 최소 처리량을 정의합니다.

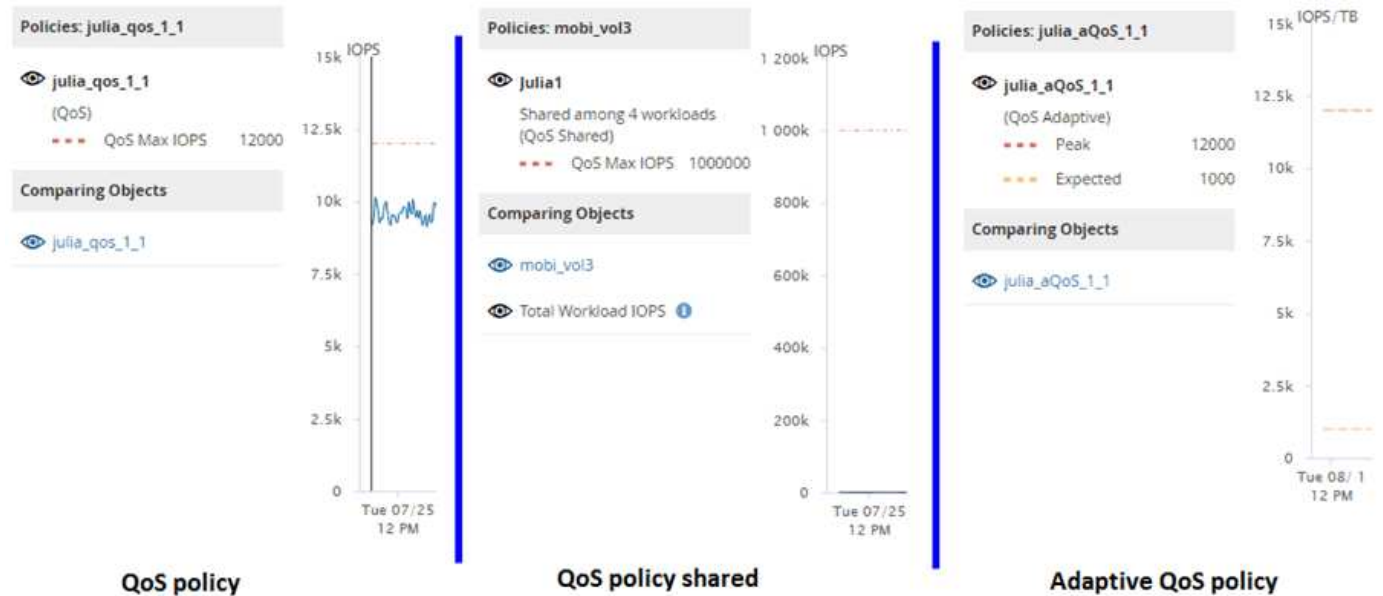
IOPS 및 MB/s에 대한 공유 및 비공유 QoS 정책은 최소값과 최대값을 정의하기 위해 "최소값"과 "최대값"이라는 용어를 사용합니다. ONTAP 9.3에 도입된 IOPS/TB에 대한 적응형 QoS 정책은 "예상"과 "피크"라는 용어를 사용하여 최저값과 최고값을 정의합니다.

ONTAP 사용하면 두 가지 유형의 QoS 정책을 만들 수 있지만, 작업 부하에 적용되는 방식에 따라 성능 차트에 QoS 정책이 표시되는 세 가지 방법이 있습니다.

정책 유형	기능성	Unified Manager 인터페이스의 표시기
단일 작업 부하에 할당된 QoS 공유 정책 또는 단일 작업 부하 또는 여러 작업 부하에 할당된 QoS 비공유 정책	각 작업 부하가 지정된 처리량 설정을 소모할 수 있습니다.	`(QoS)`가 표시됩니다.
여러 작업 부하에 할당된 QoS 공유 정책	모든 작업 부하가 지정된 처리량 설정을 공유합니다.	`(QoS 공유)`가 표시됩니다.

정책 유형	기능성	Unified Manager 인터페이스의 표시기
단일 작업 부하 또는 여러 작업 부하에 할당된 적응형 QoS 정책	각 작업 부하가 지정된 처리량 설정을 소모할 수 있습니다.	`(QoS Adaptive)`가 표시됩니다.

다음 그림은 세 가지 옵션이 카운터 차트에 어떻게 표시되는지에 대한 예를 보여줍니다.



IOPS에 정의된 일반 QoS 정책이 워크로드의 IOPS/TB 차트에 나타나면 ONTAP IOPS 값을 IOPS/TB 값으로 변환하고 Unified Manager는 해당 정책을 "IOPS에 정의된 QoS"라는 텍스트와 함께 IOPS/TB 차트에 표시합니다.

IOPS/TB 단위로 정의된 적응형 QoS 정책이 워크로드의 IOPS 차트에 나타나면 ONTAP IOPS/TB 값을 IOPS 값으로 변환하고 Unified Manager는 피크 IOPS 할당 설정이 구성된 방식에 따라 "QoS 적응형 - 사용됨, IOPS/TB 단위로 정의됨" 또는 "QoS 적응형 - 할당됨, IOPS/TB 단위로 정의됨"이라는 텍스트와 함께 IOPS 차트에 해당 정책을 표시합니다. 할당 설정이 "allocated-space"로 설정된 경우 최대 IOPS는 볼륨 크기를 기준으로 계산됩니다. 할당 설정이 "used-space"로 설정된 경우 최대 IOPS는 스토리지 효율성을 고려하여 볼륨에 저장된 데이터 양을 기준으로 계산됩니다.



IOPS/TB 차트는 볼륨에서 사용하는 논리적 용량이 128GB 이상일 때만 성능 데이터를 표시합니다. 선택한 기간 동안 사용된 용량이 128GB 미만으로 떨어지면 차트에 갭이 표시됩니다.

성능 탐색기에서 작업 부하 QoS 최소 및 최대 설정 보기

성능 탐색기 차트에서 볼륨이나 LUN에 대한 ONTAP 정의한 서비스 품질(QoS) 정책 설정을 볼 수 있습니다. 처리량 최대 설정은 시스템 리소스에 대한 경쟁 작업 부하의 영향을 제한합니다. 처리량 최소 설정은 경쟁 작업 부하의 수요에 관계없이 중요한 작업 부하가 최소 처리량 목표를 충족하도록 보장합니다.

QoS 처리량 "최소" 및 "최대" IOPS 및 MB/s 설정은 ONTAP에서 구성된 경우에만 카운터 차트에 표시됩니다. 처리량 최소 설정은 ONTAP 9.2 이상 소프트웨어를 실행하는 시스템과 AFF 시스템에서만 사용할 수 있으며, 현재는 IOPS에 대해서만 설정할 수 있습니다.

적응형 QoS 정책은 ONTAP 9.3부터 사용할 수 있으며 IOPS 대신 IOPS/TB를 사용하여 표현됩니다. 이러한 정책은 볼륨 크기에 따라 작업 부하당 QoS 정책 값을 자동으로 조정하여 볼륨 크기가 변경되더라도 IOPS 대 테라바이트 비율을 유지합니다. 볼륨에만 적응형 QoS 정책 그룹을 적용할 수 있습니다. 적응형 QoS 정책에는 최소값과 최대값 대신 "예상값"과 "피크값"이라는 QoS 용어가 사용됩니다.

Unified Manager는 이전 1시간 동안의 각 성능 수집 기간 동안 작업 부하 처리량이 정의된 QoS 최대 정책 설정을 초과할 경우 QoS 정책 위반에 대한 경고 이벤트를 생성합니다. 수집 기간 동안 워크로드 처리량은 짧은 시간 동안만 QoS 임계값을 초과할 수 있지만 Unified Manager는 차트에 수집 기간 동안의 "평균" 처리량을 표시합니다. 이러한 이유로 차트에 표시된 정책 임계값을 작업 부하의 처리량이 넘지 않았더라도 QoS 이벤트가 표시될 수 있습니다.

단계

1. 선택한 볼륨이나 LUN의 성능 탐색기 페이지에서 다음 작업을 수행하여 QoS 상한 및 하한 설정을 확인하세요.

만약 당신이 원한다면...	이렇게 하세요...
IOPS 상한(QoS 최대치) 보기	IOPS 전체 또는 세부 정보 차트에서 *확대 보기*를 클릭합니다.
MB/s 상한(QoS 최대치) 보기	MB/s 총계 또는 세부 정보 차트에서 *보기 확대*를 클릭합니다.
IOPS 플로어(QoS 최소값) 보기	IOPS 전체 또는 세부 정보 차트에서 *확대 보기*를 클릭합니다.
IOPS/TB 상한(QoS 피크) 보기	볼륨의 경우 IOPS/TB 차트에서 *확대 보기*를 클릭합니다.
IOPS/TB 플로어(예상 QoS) 보기	볼륨의 경우 IOPS/TB 차트에서 *확대 보기*를 클릭합니다.

점선으로 표시된 수평선은 ONTAP에 설정된 최대 또는 최소 처리량 값을 나타냅니다. QoS 값이 변경된 시점도 볼 수 있습니다.

2. QoS 설정과 비교한 특정 IOPS 및 MB/s 값을 보려면 커서를 차트 영역으로 옮겨 팝업 창을 확인하세요.

특정 볼륨이나 LUN의 IOPS 또는 MB/s가 매우 높아 시스템 리소스에 부담을 주는 경우, 시스템 관리자나 ONTAP CLI를 사용하여 QoS 설정을 조정하면 이러한 워크로드가 다른 워크로드의 성능에 영향을 미치지 않도록 할 수 있습니다.

QoS 설정 조정에 대한 자세한 내용은 다음을 참조하세요. ["성과 관리 개요"](#)

성능 용량 및 사용 가능한 IOPS 정보를 사용하여 성능을 관리합니다.

성능 용량은 리소스의 유용한 성능을 초과하지 않고도 리소스에서 얼마나 많은 처리량을 얻을 수 있는지를 나타냅니다. 기존 성능 카운터를 사용하여 볼 때, 성능 용량은 지연 시간이 문제가 되기 전에 노드나 집계에서 최대 활용도를 얻는 지점입니다.

Unified Manager는 각 클러스터의 노드와 집계에서 성능 용량 통계를 수집합니다. 사용된 성능 용량은 현재 사용 중인 성능 용량의 백분율이고, 사용 가능한 성능 용량은 여전히 사용 가능한 성능 용량의 백분율입니다.

성능 용량 무효는 여전히 사용 가능한 리소스의 일정 비율을 제공하는 반면, _사용 가능한 IOPS_는 최대 성능 용량에 도달하기 전에 리소스에 추가할 수 있는 IOPS 수를 알려줍니다. 이 지표를 사용하면 미리 정해진 수의 IOPS 작업 부하를 리소스에 추가할 수 있습니다.

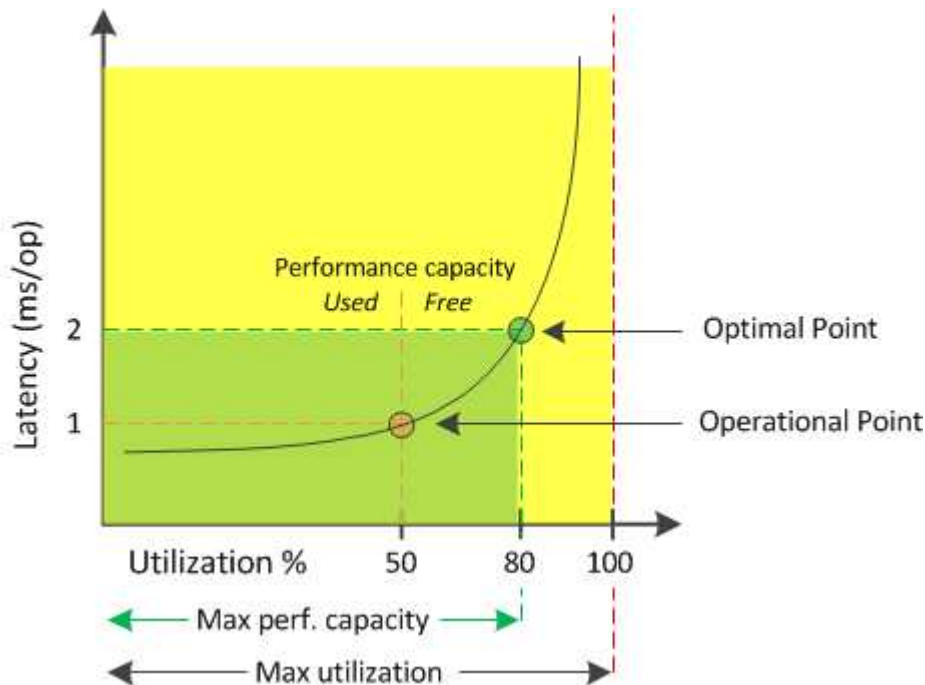
성능 용량 정보를 모니터링하면 다음과 같은 이점이 있습니다.

- 워크플로우 프로비저닝 및 밸런싱을 지원합니다.
- 노드에 과부하가 걸리거나 리소스를 최적 지점을 넘어 사용하는 것을 방지하여 문제 해결의 필요성을 줄여줍니다.
- 추가 저장 장비가 필요한 곳을 더욱 정확하게 파악하는 데 도움이 됩니다.

사용된 성능 용량은 무엇입니까?

사용된 성능 용량 카운터는 작업 부하가 증가하면 노드나 집계의 성능이 저하될 수 있는 지점에 도달했는지 여부를 식별하는 데 도움이 됩니다. 또한 특정 기간 동안 노드나 집계가 과도하게 사용되고 있는지도 보여줄 수 있습니다. 사용된 성능 용량은 활용도와 유사하지만, 전자는 특정 작업 부하에 대한 물리적 리소스에서 사용 가능한 성능 기능에 대한 더 많은 통찰력을 제공합니다.

최적의 사용 성능 용량은 노드 또는 집계가 최적의 활용도와 지연 시간(응답 시간)을 갖고 효율적으로 사용되는 지점입니다. 다음 그림은 집계에 대한 샘플 대기 시간 대 활용도 곡선을 보여줍니다.



이 예에서 _운영 지점_은 집계가 현재 1.0ms/op의 지연 시간으로 50% 활용도로 운영되고 있음을 나타냅니다. Unified Manager는 집계에서 수집된 통계를 기반으로 이 집계에 대해 추가 성능 용량을 사용할 수 있는지 확인합니다. 이 예에서 _최적 지점_은 집계가 80% 활용되고 지연 시간이 2.0ms/op인 지점으로 식별됩니다. 따라서 이 집계에 더 많은 볼륨과 LUN을 추가하여 시스템을 더 효율적으로 사용할 수 있습니다.

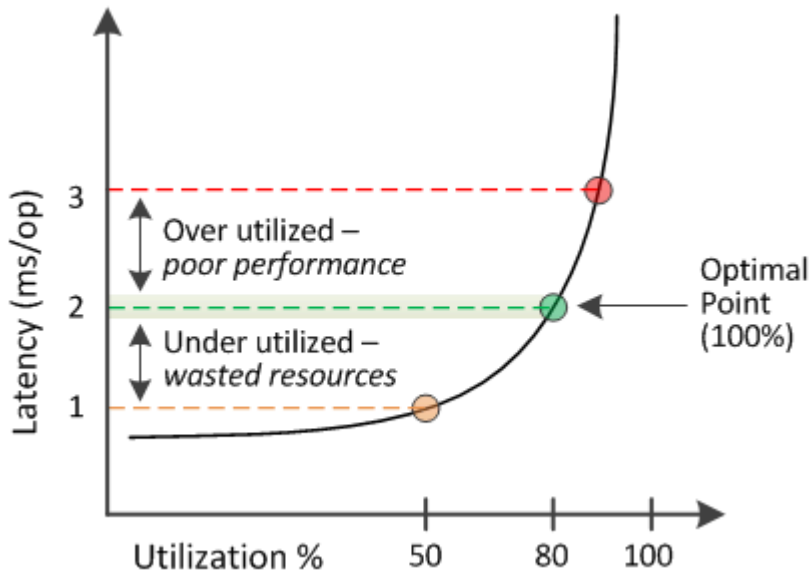
성능 용량 사용 카운터는 "사용률" 카운터보다 더 큰 숫자가 될 것으로 예상되는데, 그 이유는 성능 용량이 대기 시간에 영향을 미치기 때문입니다. 예를 들어, 노드나 집계가 70% 사용된 경우 성능 용량 값은 지연 시간 값에 따라 80%~100% 범위에 있을 수 있습니다.

하지만 어떤 경우에는 대시보드 페이지에서 사용량 카운터가 더 높게 표시될 수 있습니다. 이는 대시보드가 각 수집 기간마다 현재 카운터 값을 새로 고치기 때문에 발생하는 정상적인 현상입니다. Unified Manager 사용자 인터페이스의 다른 페이지처럼 특정 기간 동안의 평균을 표시하지 않습니다. 성능 용량 사용 카운터는 일정 기간 동안의 성능 평균을 나타내는 지표로 사용하는 것이 가장 좋고, 활용도 카운터는 리소스의 즉각적인 사용량을 확인하는 데 가장 적합합니다.

성능 용량 사용 가치의 의미

사용된 성능 용량 값은 현재 과도하게 활용되거나 활용도가 낮은 노드와 집계를 식별하는 데 도움이 됩니다. 이를 통해 작업 부하를 재분산하여 스토리지 리소스를 더욱 효율적으로 사용할 수 있습니다.

다음 그림은 리소스의 대기 시간 대 활용도 곡선을 보여주며, 현재 운영 지점이 위치할 수 있는 세 개의 영역을 색상이 있는 점으로 표시했습니다.



- 성능 용량 사용률이 100에 가까울 때 최적의 지점입니다.

이 시점에서는 리소스가 효율적으로 사용되고 있습니다.

- 100을 넘는 성능 용량 사용률은 노드 또는 집계가 과도하게 활용되고 있으며 워크로드가 최적이지 않은 성능을 받고 있음을 나타냅니다.

리소스에 새로운 작업 부하를 추가해서는 안 되며, 기존 작업 부하를 재분배해야 할 수도 있습니다.

- 100 미만의 성능 용량 사용률은 노드 또는 집계가 충분히 활용되지 않고 리소스가 효과적으로 사용되지 않고 있음을 나타냅니다.

리소스에 더 많은 작업 부하를 추가할 수 있습니다.



활용도와 달리 성능 용량 사용률은 100% 이상일 수 있습니다. 최대 비율은 없지만, 리소스가 과도하게 활용될 경우 일반적으로 110%~140% 범위에 속합니다. 백분율이 높을수록 리소스에 심각한 문제가 있음을 나타냅니다.

사용 가능한 IOPS는 무엇입니까?

사용 가능한 IOPS 카운터는 리소스가 한계에 도달하기 전에 노드나 집계에 추가할 수 있는 남은 IOPS 수를 식별합니다.

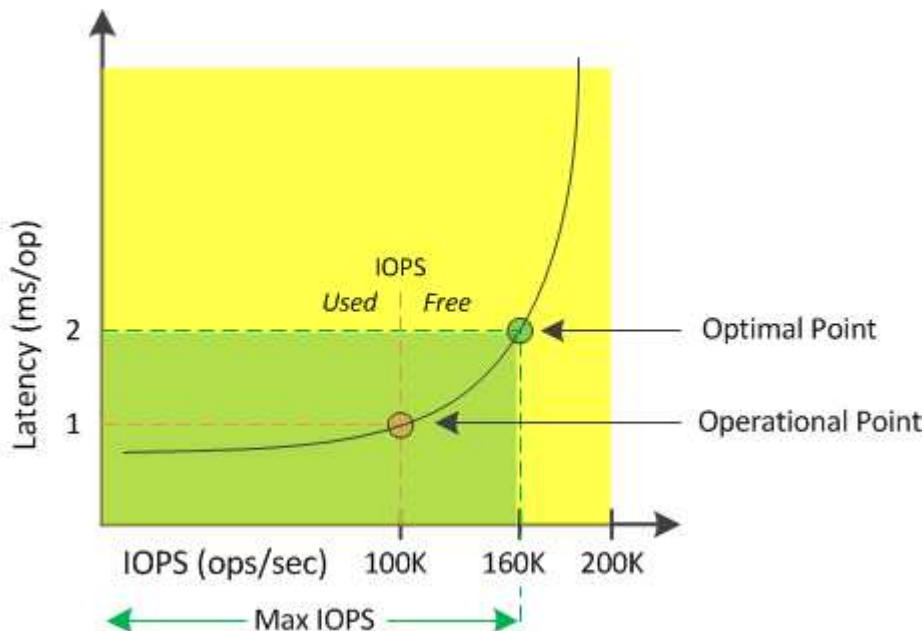
노드가 제공할 수 있는 총 IOPS는 노드의 물리적 특성(예: CPU 수, CPU 속도, RAM 용량)에 따라 결정됩니다. 집계에서 제공할 수 있는 총 IOPS는 디스크의 물리적 속성(예: SATA, SAS 또는 SSD 디스크)에 따라 달라집니다.

집계된 모든 볼륨의 총 IOPS가 해당 집계의 총 IOPS와 일치하지 않을 수 있습니다. 이는 다음 지식 기반 문서에서 논의됩니다: [KB"집계된 모든 볼륨 IOP의 합계가 집계 IOP와 일치하지 않는 이유는 무엇입니까?"](#)

성능 용량 여유 카운터는 여전히 사용 가능한 리소스의 백분율을 제공하는 반면, 사용 가능한 IOPS 카운터는 최대 성능 용량에 도달하기 전에 리소스에 추가할 수 있는 정확한 IOPS(워크로드) 수를 알려줍니다.

예를 들어, FAS2520과 FAS8060 스토리지 시스템을 함께 사용하는 경우 30%의 성능 용량 여유 값은 일부 여유 성능 용량이 있음을 의미합니다. 하지만 해당 값은 해당 노드에 얼마나 많은 추가 워크로드를 배포할 수 있는지에 대한 가시성을 제공하지 않습니다. 사용 가능한 IOPS 카운터는 FAS8060에서 사용 가능한 IOPS가 500이라고 표시할 수 있지만, FAS2520에서는 사용 가능한 IOPS가 100밖에 없다고 표시할 수 있습니다.

다음 그림은 노드의 샘플 대기 시간 대 IOPS 곡선을 보여줍니다.



리소스가 제공할 수 있는 최대 IOPS 수는 성능 용량 사용 카운터가 100%(최적 지점)일 때의 IOPS 수입니다. 운영 지점은 노드가 현재 1.0ms/op의 지연 시간과 함께 100K IOPS로 운영되고 있음을 나타냅니다. Unified Manager는 노드에서 수집한 통계를 기반으로 노드의 최대 IOPS가 160K라고 판단합니다. 즉, 60K의 여유 IOPS가 있거나 사용 가능한 IOPS가 있다는 의미입니다. 따라서 이 노드에 더 많은 작업 부하를 추가하여 시스템을 더 효율적으로 사용할 수 있습니다.



리소스에서 사용자 활동이 최소일 때, 사용 가능한 IOPS 값은 CPU 코어당 약 4,500 IOPS를 기준으로 일반적인 작업 부하를 가정하여 계산됩니다. Unified Manager에는 처리 중인 작업의 특성을 정확하게 추정할 수 있는 데이터가 없기 때문입니다.

노드 보기 및 사용된 성능 용량 집계 값

클러스터의 모든 노드 또는 모든 집계에 대해 사용된 성능 용량 값을 모니터링할 수도 있고, 단일 노드 또는 집계에 대한 세부 정보를 볼 수도 있습니다.

사용된 성능 용량 값은 대시보드, 성능 인벤토리 페이지, 상위 성과자 페이지, 임계값 정책 만들기 페이지, 성능 탐색기 페이지 및 세부 차트에 표시됩니다. 예를 들어, 성능: 모든 집계 페이지에는 모든 집계에 대한 성능 용량 사용 값을 볼 수 있는 성능 용량 사용 열이 제공됩니다.

Aggregates ⓘ Last updated: 04:11 PM, 08 Feb Refresh

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

Filtering No filter applied Search Aggregates Data Search

Assign Threshold Policy Clear Threshold Policy

	Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used IOPS	Utilization	Free Capacity	Total Capacity	Cluster	Node	Policy
☐	✓	opm_mo..._agg0	16.3 ms/op	124 IOPS	< 1 MBps	45%	9%	154 GB	3,179 GB	opm-mobility	opm-m...-02	
☐	✓	rt_agg2	19.8 ms/op	290 IOPS	< 1 MBps	45%	15%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
☐	✓	aggr_snap_mirror	13.9 ms/op	267 IOPS	< 1 MBps	38%	12%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
☐	✓	sdot_agg	17.3 ms/op	745 IOPS	< 1 MBps	24%	11%	26,621 GB	26,774 GB	opm-mobility	opm-m...-02	
☐	✓	aggr1	15.5 ms/op	434 IOPS	< 1 MBps	16%	6%	4,390 GB	20,080 GB	opm-mobility	opm-m...-01	
☐	✓	rt_agg1	22.3 ms/op	267 IOPS	< 1 MBps	11%	6%	6,691 GB	6,693 GB	opm-mobility	opm-m...-01	
☐	✓	aggr2	15.6 ms/op	259 IOPS	1.03 MBps	11%	5%	18,472 GB	20,080 GB	opm-mobility	opm-m...-02	
☐	✓	aggr2	9.52 ms/op	87 IOPS	20.8 MBps	Not Supported	5%	847 GB	984 GB	opm-io...vity	opm-io...ty-01	aggr_IOPS
☐	⚠	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-io...vity	opm-io...ty-01	aggr_IOPS

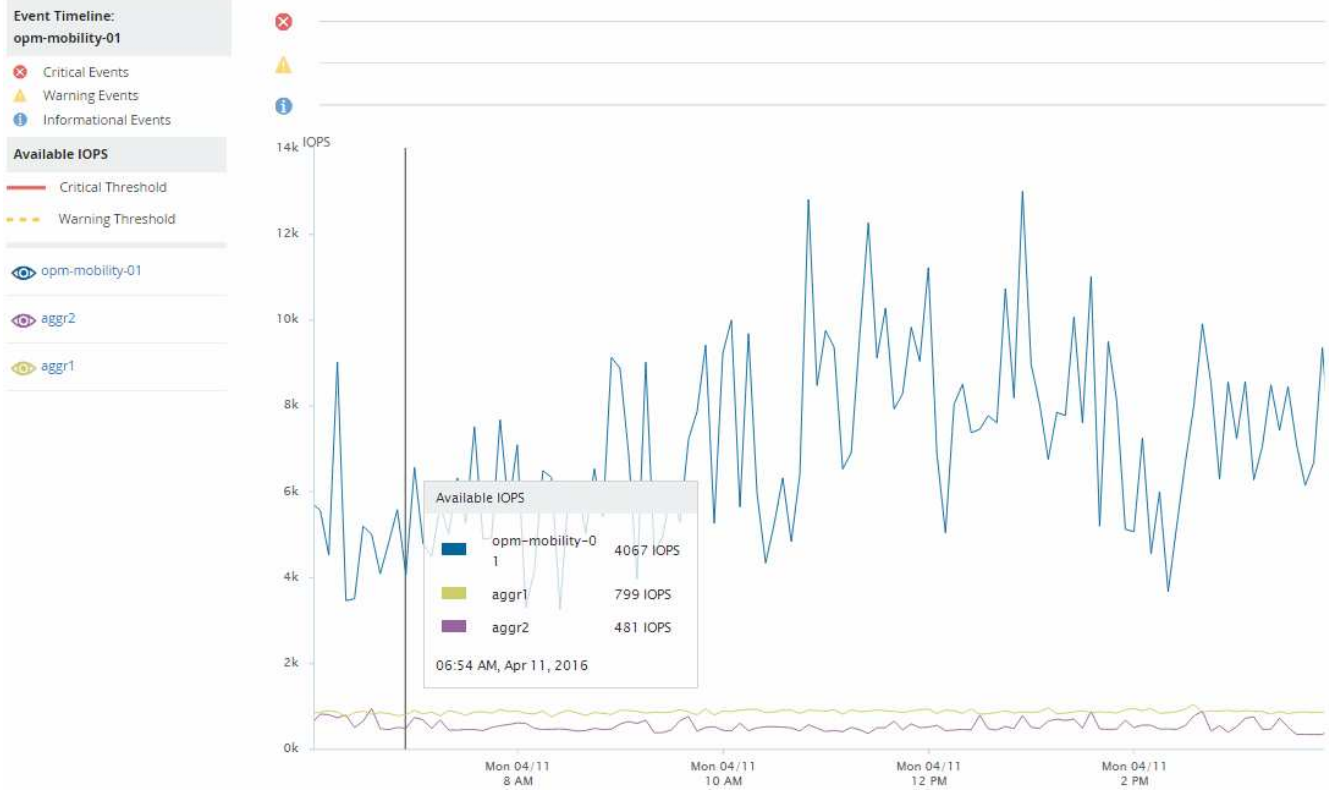
성능 용량 사용 카운터를 모니터링하면 다음 사항을 식별할 수 있습니다.

- 클러스터의 모든 노드 또는 집계에 고성능 용량 사용 값이 있는지 여부
- 클러스터의 모든 노드 또는 집계에 활성 성능 용량 사용 이벤트가 있는지 여부
- 클러스터에서 가장 높고 가장 낮은 성능 용량 사용 값을 갖는 노드 및 집계
- 고성능 용량 사용 값을 갖는 노드 또는 집계와 함께 사용되는 대기 시간 및 활용 카운터 값
- HA 쌍의 노드에 대해 사용된 성능 용량 값은 노드 중 하나가 실패할 경우 어떻게 영향을 받습니까?
- 고성능 용량 사용 값을 갖는 집계에서 가장 바쁜 볼륨 및 LUN

노드 보기 및 사용 가능한 IOPS 값 집계

클러스터의 모든 노드 또는 모든 집계에 대해 사용 가능한 IOPS 값을 모니터링할 수도 있고, 단일 노드 또는 집계에 대한 세부 정보를 볼 수도 있습니다.

사용 가능한 IOPS 값은 성능 인벤토리 페이지와 노드 및 집계에 대한 성능 탐색기 페이지 차트에 표시됩니다. 예를 들어, 노드/성능 탐색기 페이지에서 노드를 볼 때 목록에서 "사용 가능한 IOPS" 카운터 차트를 선택하여 노드와 해당 노드의 여러 집계에 사용 가능한 IOPS 값을 비교할 수 있습니다.



사용 가능한 IOPS 카운터를 모니터링하면 다음을 식별할 수 있습니다.

- 향후 워크로드를 배포할 수 있는 위치를 결정하는 데 도움이 되는 가장 큰 IOPS 값을 가진 노드 또는 집계입니다.
- 잠재적인 향후 성능 문제를 모니터링해야 하는 리소스를 식별하기 위해 사용 가능한 IOPS 값이 가장 작은 노드 또는 집계입니다.
- 사용 가능한 IOPS 값이 작은 집계에서 가장 바쁜 볼륨과 LUN입니다.

문제를 식별하기 위해 성능 용량 카운터 차트를 확인하세요.

성능 탐색기 페이지에서 노드와 집계에 사용된 성능 용량 차트를 볼 수 있습니다. 이를 통해 선택한 노드에 대한 자세한 성능 용량 데이터와 특정 기간 동안의 집계를 볼 수 있습니다.

표준 카운터 차트는 선택된 노드 또는 집계에 대해 사용된 성능 용량 값을 표시합니다. 분석 카운터 차트는 사용자 프로토콜 대비 백그라운드 시스템 프로세스에 따라 사용량을 구분하여 루트 개체의 전체 성능 용량 값을 표시합니다. 또한, 무료로 제공되는 성능 용량도 표시됩니다.



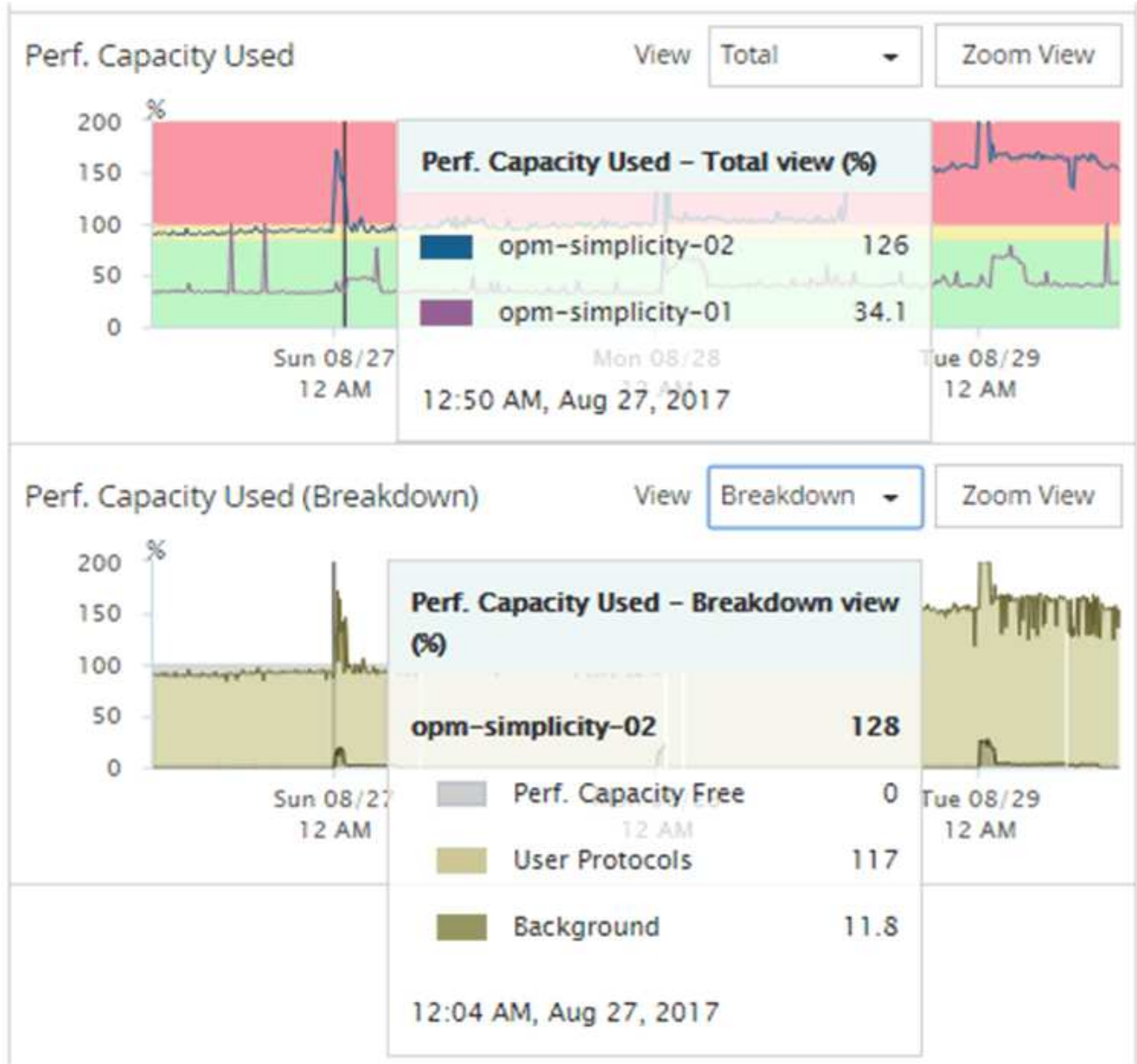
시스템 및 데이터 관리와 관련된 일부 백그라운드 활동은 사용자 작업 부하로 식별되고 사용자 프로토콜로 분류되므로 해당 프로세스가 실행될 때 사용자 프로토콜 비율이 인위적으로 높게 나타날 수 있습니다. 이러한 프로세스는 일반적으로 클러스터 사용량이 낮은 자정 무렵에 실행됩니다. 자정 무렵 사용자 프로토콜 활동이 급증하는 것을 확인하면 클러스터 백업 작업이나 기타 백그라운드 활동이 해당 시간에 실행되도록 구성되어 있는지 확인하세요.

단계

- 노드 또는 집계된 랜딩 페이지에서 탐색기 탭을 선택합니다.
- 카운터 차트 창에서 차트 선택*을 클릭한 다음 *성과*를 선택합니다. 사용 용량 차트.

3. 차트가 보일 때까지 아래로 스크롤하세요.

표준 차트의 색상은 객체가 최적 범위에 있을 때(노란색), 객체가 충분히 활용되지 않을 때(녹색), 객체가 과도하게 활용될 때(빨간색)를 보여줍니다. 분석 차트는 루트 개체에 대한 자세한 성능 용량 세부 정보만 표시합니다.



4. 두 차트를 전체 크기로 보려면 *확대 보기*를 클릭하세요.

이런 방식으로 별도의 창에서 여러 카운터 차트를 열어 동일한 기간 동안 사용된 성능 용량 값을 IOPS 또는 MBps 값과 비교할 수 있습니다.

성능 용량 사용 성능 임계값 조건

노드 또는 집계에 대한 성능 용량 사용 값이 정의된 성능 용량 사용 임계값 설정을 초과하면 이벤트가 트리거되도록 사용자 정의 성능 임계값 정책을 만들 수 있습니다.

또한, 노드는 "성능 용량 사용 인수" 임계값 정책으로 구성될 수 있습니다. 이 임계값 정책은 HA 쌍의 두 노드에 대해

사용된 성능 용량 통계를 합산하여 두 노드 중 하나에 장애가 발생할 경우 다른 노드의 용량이 충분한지 여부를 판별합니다. 장애 조치 중 작업 부하는 두 파트너 노드의 작업 부하의 조합이므로 인수 정책에 사용된 동일한 성능 용량을 두 노드에 모두 적용할 수 있습니다.



이 성능 용량은 일반적으로 노드 간에 동등성을 사용합니다. 그러나 장애 조치 파트너를 통해 노드 중 하나로 향하는 크로스 노드 트래픽이 상당히 많은 경우, 한 파트너 노드에서 모든 워크로드를 실행할 때 사용되는 총 성능 용량과 다른 파트너 노드에서 실행할 때 사용되는 총 성능 용량은 어느 노드가 장애를 일으켰는지에 따라 약간 다를 수 있습니다.

성능 용량 사용 조건은 LUN 및 볼륨에 대한 임계값을 정의할 때 조합 임계값 정책을 생성하기 위한 보조 성능 임계값 설정으로도 사용할 수 있습니다. 성능 용량 사용 조건은 볼륨이나 LUN이 있는 집계 또는 노드에 적용됩니다. 예를 들어, 다음 기준을 사용하여 조합 임계값 정책을 만들 수 있습니다.

저장 객체	성능 카운터	경고 임계값	임계 임계값	지속
용량	숨어 있음	15ms/op	25ms/op	20분
골재	사용된 성능 용량	80%	95%	

조합 임계값 정책은 두 조건이 모두 전체 기간 동안 위반되는 경우에만 이벤트가 생성되도록 합니다.

성능 관리에 사용된 성능 용량 카운터를 사용합니다.

일반적으로 조직에서는 최대 수요 기간의 수요를 지원하기 위해 추가적인 성능 용량을 예약하는 동시에 리소스를 효율적으로 사용할 수 있도록 성능 용량 사용 비율을 100 미만으로 유지하고자 합니다. 임계값 정책을 사용하면 고성능 용량 사용 값에 대한 알림이 전송되는 시기를 사용자 정의할 수 있습니다.

귀하의 성과 요구 사항에 따라 구체적인 목표를 설정할 수 있습니다. 예를 들어, 금융 서비스 회사는 거래의 적시 실행을 보장하기 위해 더 많은 성과 용량을 확보할 수 있습니다. 이러한 회사는 성능 용량 사용 임계값을 70~80% 범위로 설정하고 싶어할 수도 있습니다. 마진이 작은 제조업체의 경우, IT 비용을 보다 효율적으로 관리하기 위해 성과를 저해할 위험을 감수할 의향이 있다면 성과 용량을 적게 예약하는 것을 선택할 수도 있습니다. 이러한 회사는 성능 용량 사용 임계값을 85~95% 범위로 설정할 수 있습니다.

성능 용량 사용 값이 사용자 정의 임계값 정책에 설정된 백분율을 초과하면 Unified Manager는 알림 이메일을 보내고 이벤트를 이벤트 인벤토리 페이지에 추가합니다. 이를 통해 성능에 영향을 미치기 전에 잠재적인 문제를 관리할 수 있습니다. 이러한 이벤트는 노드와 집계 내에서 워크로드 이동 및 변경이 필요하다는 지표로 사용할 수도 있습니다.

노드 장애 조치 계획 페이지를 이해하고 사용하세요

성능/노드 장애 조치 계획 페이지는 노드의 고가용성(HA) 파트너 노드에 장애가 발생할 경우 노드의 성능에 미치는 영향을 추정합니다. Unified Manager는 HA 쌍의 노드에 대한 과거 성능을 기반으로 추정치를 계산합니다.

장애 조치의 성능 영향을 예측하면 다음과 같은 시나리오에서 계획을 세우는 데 도움이 됩니다.

- 장애 조치로 인해 인수 노드의 예상 성능이 지속적으로 허용할 수 없는 수준으로 저하되는 경우 장애 조치로 인한 성능 영향을 줄이기 위한 시정 조치를 취하는 것을 고려할 수 있습니다.

- 하드웨어 유지 관리 작업을 수행하기 위해 수동 장애 조치를 시작하기 전에, 장애 조치가 인수 노드의 성능에 어떤 영향을 미치는지 추정하여 작업을 수행하기에 가장 적합한 시간을 결정할 수 있습니다.

노드 장애 조치 계획 페이지를 사용하여 시정 조치를 결정합니다.

성능/노드 장애 조치 계획 페이지에 표시되는 정보를 기반으로 장애 조치로 인해 HA 쌍의 성능이 허용 수준 이하로 떨어지지 않도록 조치를 취할 수 있습니다.

예를 들어, 장애 조치의 예상 성능 영향을 줄이려면 HA 쌍의 노드에서 일부 볼륨이나 LUN을 클러스터의 다른 노드로 이동할 수 있습니다. 이렇게 하면 장애 조치 후에도 기본 노드가 계속해서 허용 가능한 성능을 제공할 수 있습니다.

노드 장애 조치 계획 페이지의 구성 요소

성능/노드 장애 조치 계획 페이지의 구성 요소는 그리드와 비교 창에 표시됩니다. 이 섹션에서는 노드 장애 조치가 인수 노드의 성능에 미치는 영향을 평가할 수 있습니다.

성능 통계 그리드

성능/노드 장애 조치 계획 페이지에는 지연 시간, IOPS, 활용도, 사용된 성능 용량에 대한 통계가 포함된 표가 표시됩니다.



이 페이지와 성능/노드 성능 탐색기 페이지에 표시되는 대기 시간 및 IOPS 값은 노드 장애 조치를 예측하는 데 사용되는 값에 따라 다른 성능 카운터가 사용되므로 일치하지 않을 수 있습니다.

그리드에서 각 노드에는 다음 역할 중 하나가 지정됩니다.

- 주요한

파트너가 실패할 때 HA 파트너를 대신하여 작업을 수행하는 노드입니다. 루트 객체는 항상 기본 노드입니다.

- 파트너

장애 조치 시나리오에서 실패한 노드입니다.

- 예상 인수

기본 노드와 동일합니다. 이 노드에 대해 표시되는 성능 통계는 실패한 파트너를 인수한 후 인수 노드의 성능을 보여줍니다.



인수 노드의 작업 부하가 장애 조치 후 두 노드의 작업 부하를 합친 것과 동일하지만, 예상 인수 노드의 통계는 기본 노드와 파트너 노드의 통계를 합친 것이 아닙니다. 예를 들어, 기본 노드의 지연 시간이 2ms/op이고 파트너 노드의 지연 시간이 3ms/op인 경우, 예상 인수 노드의 지연 시간은 4ms/op가 될 수 있습니다. 이 값은 Unified Manager가 수행하는 계산입니다.

루트 개체가 되도록 하려면 파트너 노드의 이름을 클릭하면 됩니다. 성능/노드 성능 탐색기 페이지가 표시된 후 장애 조치 계획 탭을 클릭하면 이 노드 장애 시나리오에서 성능이 어떻게 변하는지 확인할 수 있습니다. 예를 들어, Node1이 기본 노드이고 Node2가 파트너 노드인 경우 Node2를 클릭하여 기본 노드로 만들 수 있습니다. 이렇게 하면 어떤 노드가 실패하느냐에 따라 예상 성능이 어떻게 달라지는지 확인할 수 있습니다.

비교 창

다음 목록은 기본적으로 비교 창에 표시되는 구성 요소를 설명합니다.

- 이벤트 차트

이는 성능/노드 성능 탐색기 페이지와 동일한 형식으로 표시됩니다. 이는 기본 노드에만 적용됩니다.

- 카운터 차트

그리드에 표시된 성능 카운터에 대한 과거 통계를 표시합니다. 각 차트에서 예상 인수 노드의 그래프는 특정 시점에 장애 조치가 발생했을 경우 예상되는 성능을 보여줍니다.

예를 들어, 2월 8일 오전 11시에 예상 인수 노드의 활용도 차트가 73%를 보여준다고 가정해 보겠습니다. 만약 그 시점에 장애 조치가 발생했다면, 인수 노드의 활용도는 73%가 되었을 것입니다.

과거 통계는 장애 조치를 시작하기 위한 최적의 시간을 찾는 데 도움이 되며, 이를 통해 인수 노드에 과부하가 걸릴 가능성을 최소화할 수 있습니다. 인수 노드의 예상 성능이 허용 가능한 시간에만 장애 조치를 예약할 수 있습니다.

기본적으로 루트 개체와 파트너 노드에 대한 통계는 비교 창에 표시됩니다. 성능/노드 성능 탐색기 페이지와 달리 이 페이지에는 통계 비교를 위해 객체를 추가할 수 있는 추가 버튼이 표시되지 않습니다.

성능/노드 성능 탐색기 페이지에서와 같은 방식으로 비교 창을 사용자 지정할 수 있습니다. 다음 목록은 차트를 사용자 지정하는 예를 보여줍니다.

- 카운터 차트에서 노드 통계를 표시하거나 숨기려면 노드 이름을 클릭하세요.
- *확대 보기*를 클릭하면 새 창에 특정 카운터에 대한 자세한 차트가 표시됩니다.

노드 장애 조치 계획 페이지에서 임계값 정책 사용

잠재적인 장애 조치로 인해 인수 노드의 성능이 허용할 수 없는 수준으로 저하될 경우 성능/노드 장애 조치 계획 페이지에서 알림을 받을 수 있도록 노드 임계값 정책을 만들 수 있습니다.

"노드 HA 쌍 과다 사용"이라는 시스템 정의 성능 임계값 정책은 임계값이 6회 연속 수집 기간(30분) 동안 위반되면 경고 이벤트를 생성합니다. HA 쌍의 노드에서 사용된 결합된 성능 용량이 200%를 초과하면 임계값이 위반된 것으로 간주됩니다.

시스템 정의 임계값 정책의 이벤트는 장애 조치로 인해 인수 노드의 대기 시간이 허용할 수 없는 수준으로 증가할 것이라는 사실을 경고합니다. 특정 노드에 대해 이 정책에 의해 생성된 이벤트가 표시되면 해당 노드의 성능/노드 장애 조치 계획 페이지로 이동하여 장애 조치로 인한 예상 대기 시간 값을 확인할 수 있습니다.

이 시스템 정의 임계값 정책을 사용하는 것 외에도 "성능 용량 사용 - 인수" 카운터를 사용하여 임계값 정책을 만든 다음 선택한 노드에 정책을 적용할 수 있습니다. 200%보다 낮은 임계값을 지정하면 시스템 정의 정책의 임계값이 위반되기 전에 이벤트를 수신할 수 있습니다. 시스템 정의 정책 이벤트가 생성되기 전에 알림을 받으려면 임계값을 초과하는 최소 기간을 30분 미만으로 지정할 수도 있습니다.

예를 들어, HA 쌍의 노드에서 사용된 결합된 성능 용량이 10분 이상 175%를 초과하는 경우 경고 이벤트를 생성하는 임계값 정책을 정의할 수 있습니다. 이 정책은 HA 쌍을 형성하는 Node1과 Node2에 적용할 수 있습니다. Node1 또는 Node2에 대한 경고 이벤트 알림을 받은 후 해당 노드의 성능/노드 장애 조치 계획 페이지를 보고 인수 노드에 미치는 예상 성능 영향을 평가할 수 있습니다. 장애 조치가 발생하는 경우 인수 노드에 과부하가 걸리지 않도록 시정 조치를 취할 수 있습니다. 노드의 결합된 성능 용량이 200% 미만일 때 조치를 취하면, 이 시간 동안 장애 조치가 발생하더라도 인수 노드의 지연 시간이 허용할 수 없는 수준에 도달하지 않습니다.

장애 조치 계획을 위해 성능 용량 사용 분석 차트를 사용하세요.

자세한 성능 용량 사용 - 세부 차트는 기본 노드와 파트너 노드에 사용된 성능 용량을 보여줍니다. 또한 예상 인수 노드의 사용 가능한 성능 용량도 표시됩니다. 이 정보는 파트너 노드에 장애가 발생할 경우 성능 문제가 발생하는지 여부를 확인하는 데 도움이 됩니다.

분석 차트는 노드에 사용된 전체 성능 용량을 보여주는 것 외에도 각 노드의 값을 사용자 프로토콜과 백그라운드 프로세스로 분류합니다.

- 사용자 프로토콜은 사용자 애플리케이션과 클러스터 간의 I/O 작업입니다.
- 백그라운드 프로세스는 저장 효율성, 데이터 복제, 시스템 상태와 관련된 내부 시스템 프로세스입니다.

이러한 추가적인 세부 정보를 통해 성능 문제가 사용자 애플리케이션 활동으로 인해 발생하는지, 아니면 중복 제거, RAID 재구성, 디스크 스크러빙, SnapMirror 복사와 같은 백그라운드 시스템 프로세스로 인해 발생하는지 확인할 수 있습니다.

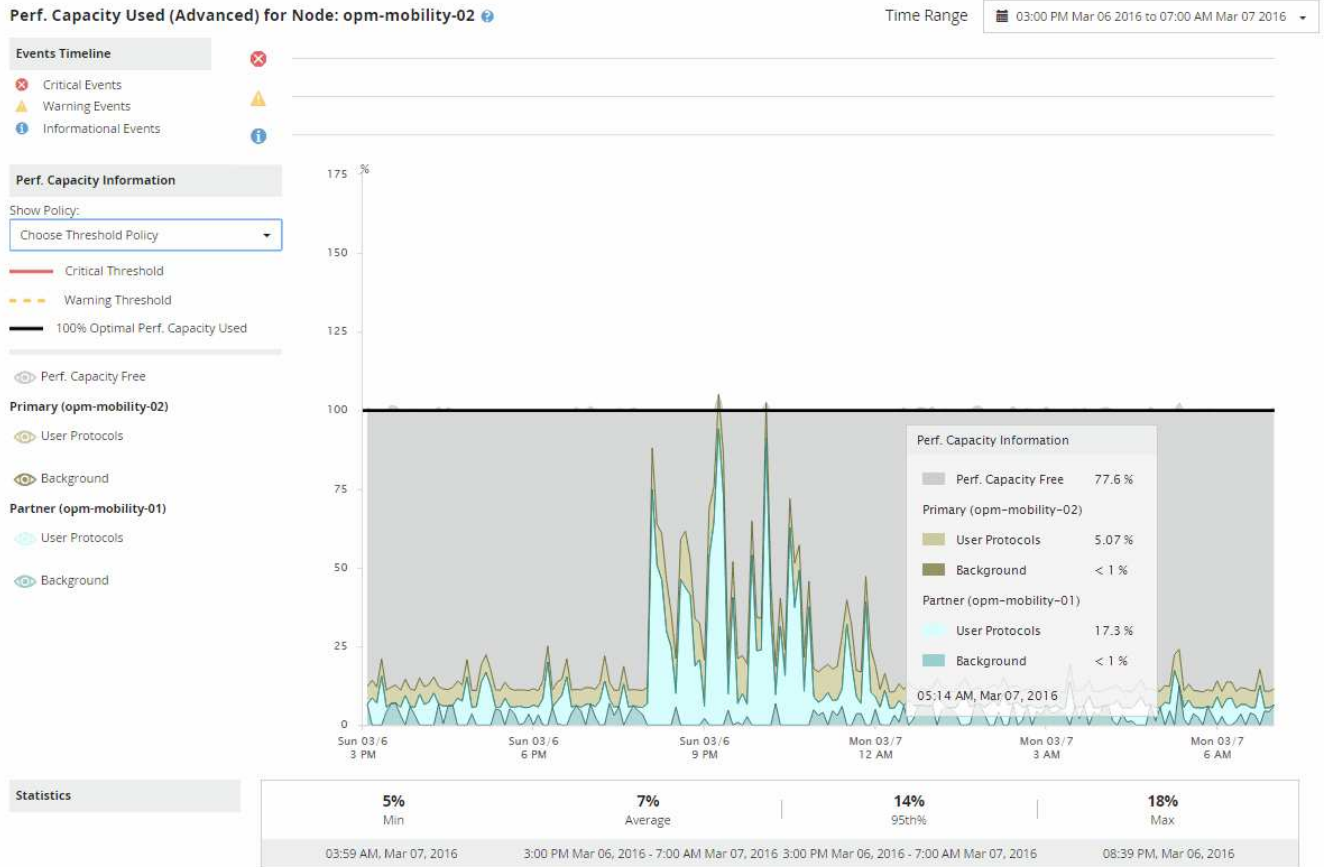
단계

1. 예상 인수 노드 역할을 할 노드의 성능/노드 장애 조치 계획 페이지로 이동합니다.
2. 시간 범위 선택기에서 카운터 그리드와 카운터 차트에 과거 통계가 표시되는 기간을 선택합니다.

기본 노드, 파트너 노드, 예상 인수 노드에 대한 통계가 포함된 카운터 차트가 표시됩니다.

3. 차트 선택 목록에서 성과를 선택합니다. 사용된 용량.
4. **Perf.**에서 사용 용량 차트에서 *세부 정보*를 선택하고 *보기 확대*를 클릭하세요.

Perf에 대한 자세한 차트입니다. 사용된 용량이 표시됩니다.



5. 팝업 창에서 사용된 성능 용량 정보를 보려면 상세 차트 위로 커서를 이동하세요.

퍼프. 여유 용량 백분율은 예상 인수 노드에서 사용 가능한 성능 용량입니다. 이는 장애 조치 후 인수 노드에 얼마나 많은 성능 용량이 남아 있는지를 나타냅니다. 0%인 경우 장애 조치로 인해 인수 노드에서 지연 시간이 허용할 수 없는 수준으로 증가합니다.

6. 낮은 성능 용량 여유 비율을 피하기 위해 시정 조치를 취하는 것을 고려하세요.

노드 유지 관리를 위해 장애 조치를 시작하려는 경우, 성능 용량 여유 비율이 0이 아닐 때 파트너 노드에 장애가 발생할 시간을 선택하세요.

데이터 수집 및 워크로드 성능 모니터링

Unified Manager는 5분마다 작업 부하 활동을 수집하고 분석하여 성능 이벤트를 식별하고 15분마다 구성 변경 사항을 감지합니다. 최대 30일 동안의 5분 단위 성능 및 이벤트 데이터를 보관하고, 이 데이터를 사용하여 모니터링되는 모든 워크로드에 대한 예상 지연 시간 범위를 예측합니다.

Unified Manager는 분석을 시작하고 I/O 응답 시간에 대한 지연 시간 예측을 워크로드 분석 페이지와 이벤트 세부 정보 페이지에 표시하기 전에 최소 3일 분의 워크로드 활동을 수집해야 합니다. 이 활동이 수집되는 동안 대기 시간 예측에는 작업 부하 활동으로 인해 발생하는 모든 변경 사항이 표시되지 않습니다. Unified Manager는 3일간의 활동을 수집한 후 24시간마다 오전 12시에 대기 시간 예측을 조정하여 작업 부하 활동의 변화를 반영하고 더욱 정확한 동적 성능 임계값을 설정합니다.

Unified Manager가 작업 부하를 모니터링하는 처음 4일 동안 마지막 데이터 수집 이후 24시간 이상이 지나면 지연 시간

차트에 해당 작업 부하에 대한 지연 시간 예측이 표시되지 않습니다. 마지막 수집 이전에 감지된 이벤트는 계속 사용할 수 있습니다.



일광 절약 시간제(DST)는 시스템 시간을 변경하는데, 이로 인해 모니터링되는 작업 부하에 대한 성능 통계의 지연 시간 예측이 변경됩니다. Unified Manager는 지연 시간 예측을 즉시 수정하기 시작하며, 완료하는 데 약 15일이 소요됩니다. 이 기간 동안 Unified Manager를 계속 사용할 수 있지만 Unified Manager는 지연 시간 예측을 사용하여 동적 이벤트를 감지하므로 일부 이벤트가 정확하지 않을 수 있습니다. 시간 변경 이전에 감지된 이벤트는 영향을 받지 않습니다.

Unified Manager에서 모니터링하는 작업 유형

Unified Manager를 사용하면 사용자 정의 워크로드와 시스템 정의 워크로드의 두 가지 유형의 성능을 모니터링할 수 있습니다.

• 사용자 정의 워크로드

애플리케이션에서 클러스터로의 I/O 처리량. 이는 읽기 및 쓰기 요청과 관련된 프로세스입니다. 볼륨, LUN, NFS 공유, SMB/CIFS 공유 및 작업 부하가 사용자 정의 작업 부하입니다.



Unified Manager는 클러스터의 작업 부하 활동만 모니터링합니다. 애플리케이션, 클라이언트 또는 애플리케이션과 클러스터 간의 경로를 모니터링하지 않습니다.

다음 중 하나 이상이 워크로드에 해당되는 경우 Unified Manager에서 모니터링할 수 없습니다.

- 이는 읽기 전용 모드의 데이터 보호(DP) 복사본입니다. (DP 볼륨은 사용자 생성 트래픽을 모니터링합니다.)
- 오프라인 데이터 복제본입니다.
- 이는 MetroCluster 구성의 미러링된 볼륨입니다.

• 시스템 정의 워크로드

저장 효율성, 데이터 복제 및 시스템 상태와 관련된 내부 프로세스에는 다음이 포함됩니다.

- 중복 제거와 같은 저장 효율성
- RAID 재구성, 디스크 스캐러빙 등을 포함하는 디스크 상태
- SnapMirror 복사와 같은 데이터 복제
- 경영 활동
- 다양한 WAFL 활동을 포함하는 파일 시스템 상태
- WAFL 스캔과 같은 파일 시스템 스캐너
- VMware 호스트에서 오프로드된 스토리지 효율성 작업과 같은 오프로드 복사
- 볼륨 이동, 데이터 압축 등과 같은 시스템 상태
- 모니터링되지 않는 볼륨

시스템 정의 워크로드에 대한 성능 데이터는 이러한 워크로드에서 사용되는 클러스터 구성 요소가 경합 중인 경우에만 GUI에 표시됩니다. 예를 들어, GUI에서 시스템 정의 워크로드의 이름을 검색하여 해당 성능 데이터를 볼 수는 없습니다.

측정	설명
편차	예상 값과 실제 값의 차이. 실제 값에서 기대 값을 뺀 값과 기대 범위의 상한 값에서 기대 값을 뺀 값의 비율입니다.  음의 편차 값은 워크로드 성과가 예상보다 낮음을 나타내고, 양의 편차 값은 워크로드 성과가 예상보다 높음을 나타냅니다.
예상되는	예상 값은 주어진 작업 부하에 대한 과거 성능 데이터 분석을 기반으로 합니다. Unified Manager는 이러한 통계적 값을 분석하여 값의 예상 범위(대기 시간 예측)를 결정합니다.
지연 시간 예측(예상 범위)	지연 시간 예측은 특정 시간에 상한 및 하한 성능 값이 어떻게 될 것인지에 대한 예측입니다. 작업 지연 시간의 경우 상위 값이 성능 임계값을 형성합니다. 실제 값이 성능 임계값을 넘으면 Unified Manager가 동적 성능 이벤트를 트리거합니다.
정점	일정 기간 동안 측정된 최대값.
피크 편차	일정 기간 동안 측정된 최대 편차 값입니다.
대기열 깊이	상호 연결 구성 요소에서 대기 중인 보류 중인 I/O 요청 수입니다.
이용	네트워크 처리, 데이터 처리 및 집계 구성 요소의 경우, 일정 기간 동안 작업 부하 작업을 완료하는 데 사용된 바쁜 시간의 백분율입니다. 예를 들어, 네트워크 처리 또는 데이터 처리 구성 요소가 I/O 요청을 처리하는 데 걸리는 시간 비율이나 집계기 읽기 또는 쓰기 요청을 이행하는 데 걸리는 시간 비율입니다.
쓰기 처리량	MetroCluster 구성에서 로컬 클러스터의 워크로드에서 파트너 클러스터로의 쓰기 처리량(초당 메가바이트(MB/s))입니다.

기대되는 성능 범위는 무엇입니까?

지연 시간 예측은 특정 시간에 상한 및 하한 성능 값이 어떻게 될 것인지에 대한 예측입니다. 작업 지연 시간의 경우 상위 값이 성능 임계값을 형성합니다. 실제 값이 성능 임계값을 넘으면 Unified Manager가 동적 성능 이벤트를 트리거합니다.

예를 들어, 정규 업무 시간인 오전 9시에서 오후 5시 사이에 대부분의 직원은 오전 9시에서 오전 10시 30분 사이에 이메일을 확인합니다. 이 시간 동안 이메일 서버에 대한 수요가 증가하면 백엔드 스토리지의 작업 부하 활동이 증가합니다. 직원들은 이메일 클라이언트의 응답 속도가 느리다고 느낄 수도 있습니다.

오후 12시부터 오후 1시까지의 점심시간과 오후 5시 이후 퇴근 시간에는 대부분 직원이 컴퓨터에서 멀어질 가능성이 높습니다. 이메일 서버에 대한 수요는 일반적으로 감소하며, 이에 따라 백엔드 저장소에 대한 수요도 감소합니다. 또는 오후 5시 이후에 시작되어 백엔드 스토리지의 활동을 증가시키는 스토리지 백업이나 바이러스 검사와 같은 예정된 작업 부하 작업이 있을 수 있습니다.

며칠 동안 작업 부하 활동의 증가와 감소에 따라 활동의 예상 범위(대기 시간 예측)가 결정되며, 작업 부하에 대한 상한과 하한이 결정됩니다. 객체의 실제 작업 부하 활동이 상한 또는 하한 경계를 벗어나고 일정 기간 동안 경계 밖에 머무르는 경우, 해당 객체가 과도하게 사용되거나 충분히 사용되지 않고 있음을 나타낼 수 있습니다.

지연 예측은 어떻게 형성되는가

Unified Manager는 분석을 시작하고 I/O 응답 시간에 대한 지연 시간 예측을 GUI에 표시하기 전에 최소 3일 분의 작업 부하 활동을 수집해야 합니다. 필요한 최소 데이터 수집에는 작업 부하 활동으로 인해 발생하는 모든 변경 사항이 반영되지 않습니다. Unified Manager는 처음 3일간의 활동을 수집한 후, 24시간마다 오전 12시에 대기 시간 예측을 조정하여 작업 부하 활동의 변화를 반영하고 더욱 정확한 동적 성능 임계값을 설정합니다.



일광 절약 시간제(DST)는 시스템 시간을 변경하는데, 이로 인해 모니터링되는 작업 부하에 대한 성능 통계의 지연 시간 예측이 변경됩니다. Unified Manager는 지연 시간 예측을 즉시 수정하기 시작하며, 완료하는 데 약 15일이 소요됩니다. 이 기간 동안 Unified Manager를 계속 사용할 수 있지만 Unified Manager는 지연 시간 예측을 사용하여 동적 이벤트를 감지하므로 일부 이벤트가 정확하지 않을 수 있습니다. 시간 변경 이전에 감지된 이벤트는 영향을 받지 않습니다.

성능 분석에서 지연 시간 예측이 사용되는 방식

Unified Manager는 모니터링되는 워크로드에 대한 일반적인 I/O 대기 시간(응답 시간) 활동을 나타내기 위해 대기 시간 예측을 사용합니다. 워크로드의 실제 지연 시간이 지연 예측의 상한을 초과하여 동적 성능 이벤트가 발생하는 경우 알림을 보내 성능 문제를 분석하고 이를 해결하기 위한 시정 조치를 취할 수 있도록 해줍니다.

지연 시간 예측은 작업 부하에 대한 성능 기준을 설정합니다. 시간이 지남에 따라 Unified Manager는 과거 성능 측정 결과를 학습하여 작업 부하에 대한 예상 성능 및 활동 수준을 예측합니다. 예상 범위의 상한은 동적 성능 임계값을 설정합니다. Unified Manager는 기준선을 사용하여 실제 지연 시간이 임계값보다 높거나 낮은지, 또는 예상 범위를 벗어나는지를 확인합니다. 실제 값과 예상 값을 비교하면 작업 부하에 대한 성능 프로필이 생성됩니다.

클러스터 구성 요소의 경합으로 인해 워크로드의 실제 대기 시간이 동적 성능 임계값을 초과하면 대기 시간이 길어지고 워크로드가 예상보다 느리게 수행됩니다. 동일한 클러스터 구성 요소를 공유하는 다른 작업 부하의 성능도 예상보다 느릴 수 있습니다.

Unified Manager는 임계값 초과 이벤트를 분석하고 해당 활동이 성능 이벤트인지 여부를 판별합니다. 높은 작업 부하 활동이 장기간(예: 몇 시간) 일관되게 유지되면 Unified Manager는 해당 활동을 정상적인 활동으로 간주하고 대기 시간 예측을 동적으로 조정하여 새로운 동적 성능 임계값을 형성합니다.

일부 작업 부하에서는 활동이 지속적으로 낮을 수 있으며, 이 경우 대기 시간에 대한 대기 시간 예측이 시간에 따라 크게 변하지 않습니다. 성능 이벤트 분석 중 이벤트 수를 최소화하기 위해 Unified Manager는 예상보다 작업 및 대기 시간이 훨씬 긴 저활동 볼륨에 대해서만 이벤트를 트리거합니다.



이 예에서 볼륨의 지연 시간은 회색으로 가장 낮은 작업당 3.5밀리초(ms/op)이고 가장 높은 작업당 5.5ms/op로 예측됩니다. 파란색으로 표시된 실제 지연 시간이 네트워크 트래픽의 간헐적 급증이나 클러스터 구성 요소의 경합으로 인해 갑자기 10ms/op로 증가하면 지연 시간 예측을 넘어서고 동적 성능 임계값을 초과한 것입니다.

네트워크 트래픽이 감소하거나 클러스터 구성 요소가 더 이상 경쟁하지 않으면 지연 시간은 지연 시간 예측 범위 내로 돌아갑니다. 지연 시간이 장시간 10ms/op 이상으로 유지되는 경우 이벤트를 해결하기 위해 시정 조치를 취해야 할 수도 있습니다.

Unified Manager가 워크로드 대기 시간을 사용하여 성능 문제를 식별하는 방법

작업 지연 시간(응답 시간)은 클러스터의 볼륨이 클라이언트 애플리케이션의 I/O 요청에 응답하는 데 걸리는 시간입니다. Unified Manager는 지연 시간을 이용해 성능 이벤트를 감지하고 경고합니다.

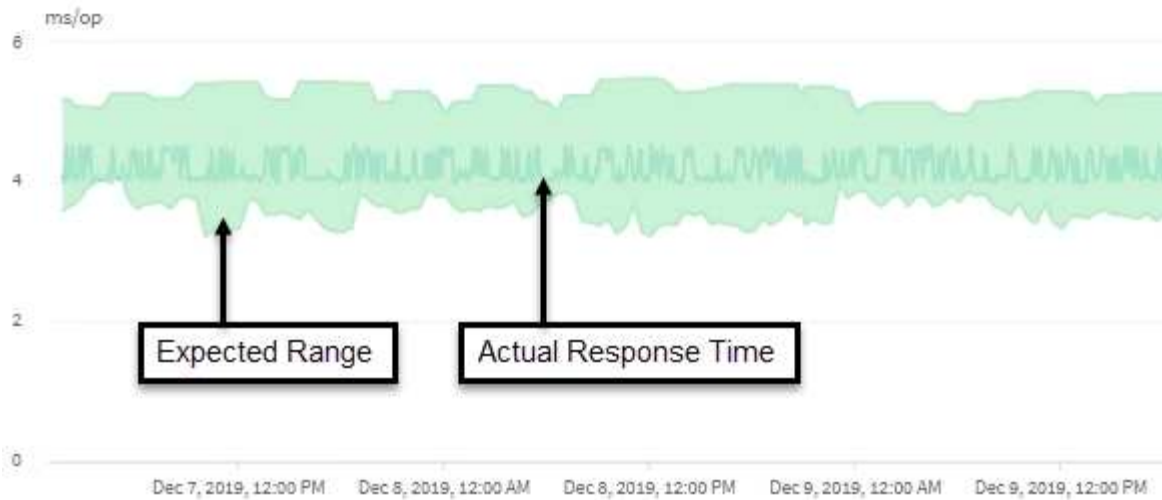
대기 시간이 길다는 것은 클러스터의 볼륨에 대한 애플리케이션의 요청이 평소보다 오래 걸린다는 것을 의미합니다. 높은 지연 시간의 원인은 하나 이상의 클러스터 구성 요소에서 경합이 발생하여 클러스터 자체에 있을 수 있습니다. 높은 지연 시간은 네트워크 병목 현상, 애플리케이션을 호스팅하는 클라이언트의 문제 또는 애플리케이션 자체의 문제 등 클러스터 외부의 문제로 인해 발생할 수도 있습니다.



Unified Manager는 클러스터의 작업 부하 활동만 모니터링합니다. 애플리케이션, 클라이언트 또는 애플리케이션과 클러스터 간의 경로를 모니터링하지 않습니다.

백업을 하거나 중복 제거를 실행하는 등 클러스터에서 수행하는 작업은 다른 작업에서 공유하는 클러스터 구성 요소에 대한 수요를 증가시켜 높은 지연 시간에 영향을 미칠 수도 있습니다. 실제 지연 시간이 예상 범위(지연 시간 예측)의 동적 성능 임계값을 초과하는 경우 Unified Manager는 이벤트를 분석하여 해결해야 할 성능 이벤트인지 확인합니다. 지연 시간은 작업당 밀리초(ms/op)로 측정됩니다.

워크로드 분석 페이지의 대기 시간 총계 차트에서 대기 시간 통계 분석을 보고 읽기 및 쓰기 요청과 같은 개별 프로세스의 활동이 전체 대기 시간 통계와 어떻게 비교되는지 확인할 수 있습니다. 비교를 통해 어떤 작업에서 가장 활동이 많은지, 또는 특정 작업에서 볼륨의 지연 시간에 영향을 미치는 비정상적인 활동이 있는지 확인하는 데 도움이 됩니다. 성능 이벤트를 분석할 때 대기 시간 통계를 사용하여 이벤트가 클러스터의 문제로 인해 발생했는지 확인할 수 있습니다. 이벤트에 관련된 특정 작업 부하 활동이나 클러스터 구성 요소를 식별할 수도 있습니다.



이 예에서는 대기 시간 차트를 보여줍니다. 실제 응답 시간(대기 시간) 활동은 파란색 선이고, 대기 시간 예측(예상 범위)은 녹색입니다.

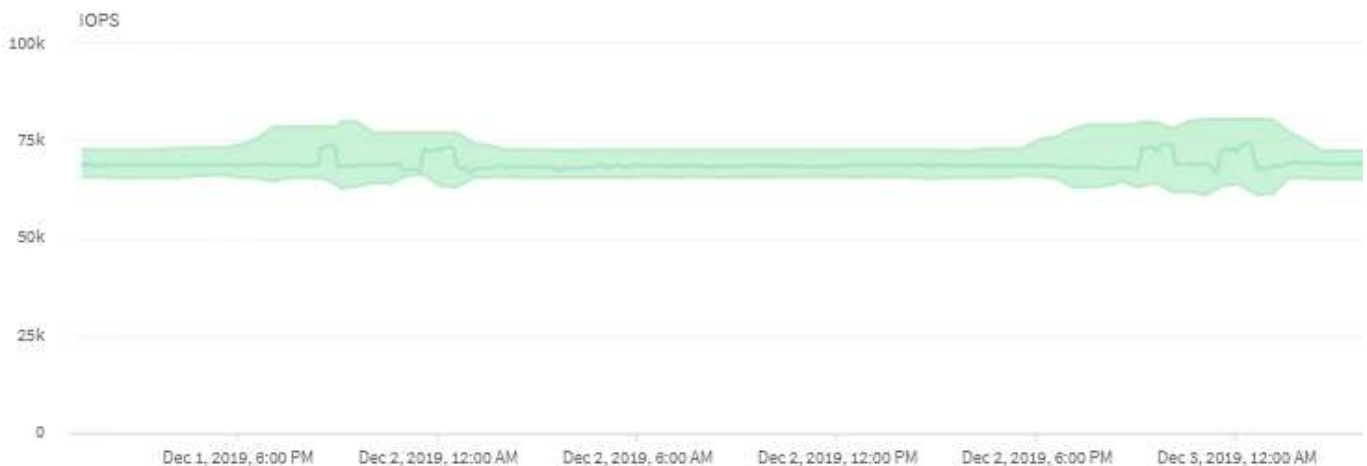


Unified Manager가 데이터를 수집하지 못한 경우 파란색 선에 간격이 생길 수 있습니다. 이는 클러스터 또는 볼륨에 접근할 수 없거나, 해당 시간 동안 Unified Manager가 꺼져 있거나, 수집이 5분 수집 기간보다 오래 걸리는 경우에 발생할 수 있습니다.

클러스터 작업이 워크로드 대기 시간에 어떤 영향을 미칠 수 있는지

작업(IOPS)은 클러스터에서 사용자 정의 및 시스템 정의 워크로드의 모든 활동을 나타냅니다. IOPS 통계는 백업이나 중복 제거 실행과 같은 클러스터 프로세스가 워크로드 지연 시간(응답 시간)에 영향을 미치는지, 아니면 성능 이벤트를 발생시켰거나 성능 이벤트에 기여했는지 확인하는 데 도움이 됩니다.

성능 이벤트를 분석할 때 IOPS 통계를 사용하여 성능 이벤트가 클러스터의 문제로 인해 발생했는지 확인할 수 있습니다. 성과 이벤트에 가장 크게 기여한 구체적인 작업 부하 활동을 파악할 수 있습니다. IOPS는 초당 작업 수(ops/sec)로 측정됩니다.



이 예에서는 IOPS 차트를 보여줍니다. 실제 운영 통계는 파란색 선이고 운영 통계의 IOPS 예측은 녹색입니다.



클러스터가 과부하된 경우 Unified Manager에서 다음 메시지가 표시될 수 있습니다. `Data collection is taking too long on Cluster cluster_name`. 이는 Unified Manager에서 분석하기에 충분한 통계가 수집되지 않았음을 의미합니다. 통계를 수집하려면 클러스터가 사용하는 리소스를 줄여야 합니다.

MetroCluster 구성의 성능 모니터링

Unified Manager를 사용하면 MetroCluster 구성의 클러스터 간 쓰기 처리량을 모니터링하여 쓰기 처리량이 많은 작업 부하를 식별할 수 있습니다.

이러한 고성능 작업 부하로 인해 로컬 클러스터의 다른 볼륨에서 I/O 응답 시간이 길어지는 경우 Unified Manager는 성능 이벤트를 트리거하여 사용자에게 알립니다.



Unified Manager는 MetroCluster 구성의 클러스터를 개별 클러스터로 처리합니다. 파트너인 클러스터를 구별하지 않으며 각 클러스터의 쓰기 처리량을 상관시키지 않습니다.

MetroCluster 구성의 로컬 클러스터가 데이터를 파트너 클러스터로 미러링하면 데이터는 NVRAM에 기록된 다음 ISL(스위치 간 링크)을 통해 원격 집계로 전송됩니다. Unified Manager는 NVRAM 분석하여 높은 쓰기 처리량으로 인해 NVRAM 과도하게 사용하고 NVRAM 경합 상태에 빠지는 작업 부하를 식별합니다.

응답 시간의 편차가 성능 임계값을 초과하는 워크로드를 `_희생자_`라고 하며, NVRAM에 대한 쓰기 처리량의 편차가 평소보다 높아서 경합이 발생하는 워크로드를 `_괴롭힘_`이라고 합니다. 쓰기 요청만 파트너 클러스터에 미러링되므로 Unified Manager는 읽기 처리량을 분석하지 않습니다.

다음 화면에서 해당 LUN과 볼륨의 작업 부하를 분석하여 MetroCluster 구성의 모든 클러스터의 처리량을 볼 수 있습니다. 클러스터별로 결과를 필터링할 수 있습니다. 왼쪽 탐색 창에서:

- 저장소 > 클러스터 > 성능: 모든 클러스터 보기. 보다
- 저장소 > 볼륨 > 성능: 모든 볼륨 보기.
- 저장소 > **LUN** > 성능: 모든 **LUN** 보기.
- 작업 부하 분석 > 모든 작업 부하

관련 정보

["성능 이벤트 분석 및 알림"](#)

["MetroCluster 구성에 대한 성능 이벤트 분석"](#)

["성능 이벤트에 관련된 작업 부하의 역할"](#)

["성능 이벤트에 관련된 피해자 작업 부하 식별"](#)

["성과 이벤트에 관련된 괴롭힘 작업량 식별"](#)

["성능 이벤트에 관련된 상어 작업량 식별"](#)

성능 이벤트 및 알림 이해

성능 이벤트는 클러스터의 워크로드 성능과 관련된 인시던트입니다. 응답 시간이 느린 작업 부하를 식별하는 데 도움이 됩니다. 동시에 발생한 건강 이벤트와 함께, 느린 응답 시간의 원인이 되었거나 이에 영향을 미친 문제를 파악할 수 있습니다.

Unified Manager가 동일한 클러스터 구성 요소에 대해 동일한 이벤트 조건이 여러 번 발생하는 것을 감지하는 경우, 모든 발생을 별도의 이벤트가 아닌 단일 이벤트로 처리합니다.

특정 심각도 유형의 성능 이벤트가 발생하면 자동으로 이메일 알림을 보내도록 알림을 구성할 수 있습니다.

성과 이벤트의 소스

성능 이벤트는 클러스터의 작업 부하 성능과 관련된 문제입니다. 이러한 기능은 응답 시간이 느린 스토리지 객체, 즉 높은 대기 시간을 식별하는 데 도움이 됩니다. 동시에 발생한 다른 건강 문제와 함께, 느린 대응 시간의 원인이 되었거나 이에 영향을 미친 문제를 파악할 수 있습니다.

Unified Manager는 다음 소스에서 성능 이벤트를 수신합니다.

- 사용자 정의 성능 임계값 정책 이벤트

사용자가 설정한 사용자 정의 임계값에 따라 성능 문제가 발생합니다. 예를 들어, 집계 및 볼륨과 같은 저장소 개체에 대한 성능 임계값 정책을 구성하면 성능 카운터의 임계값이 초과되면 이벤트가 생성됩니다.

이러한 이벤트를 수신하려면 성능 임계값 정책을 정의하고 이를 스토리지 개체에 할당해야 합니다.

- 시스템 정의 성능 임계값 정책 이벤트

시스템에서 정의된 임계값에 따른 성능 문제. 이러한 임계값 정책은 일반적인 성능 문제를 해결하기 위해 Unified Manager 설치에 포함됩니다.

이러한 임계값 정책은 기본적으로 활성화되어 있으며, 클러스터를 추가한 직후에 이벤트가 표시될 수 있습니다.

- 동적 성능 임계값 이벤트

IT 인프라의 장애나 오류, 또는 워크로드가 클러스터 리소스를 과도하게 활용하여 발생하는 성능 문제입니다. 이러한 이벤트의 원인은 시간이 지나면서 자체적으로 해결되는 간단한 문제일 수도 있고, 수리 또는 구성 변경으로 해결할 수 있는 문제일 수도 있습니다. 동적 임계값 이벤트는 공유 클러스터 구성 요소를 많이 사용하는 다른 작업 부하로 인해 ONTAP 시스템의 작업 부하가 느리다는 것을 나타냅니다.

이러한 임계값은 기본적으로 활성화되어 있으며, 새 클러스터에서 데이터를 수집한 후 3일이 지나면 이벤트가 표시될 수 있습니다.

성능 이벤트 심각도 유형

각 성과 이벤트는 심각도 유형과 연결되어 있어 즉각적인 시정 조치가 필요한 이벤트의 우선 순위를 지정하는 데 도움이 됩니다.

- 비판적인

시정 조치를 즉시 취하지 않으면 서비스 중단으로 이어질 수 있는 성능 이벤트가 발생했습니다.

중요 이벤트는 사용자가 정의한 임계값에서만 전송됩니다.

- 경고

클러스터 개체의 성능 카운터가 정상 범위를 벗어났으며, 심각한 심각도에 도달하지 않도록 모니터링해야 합니다. 이 정도 심각도의 사건은 서비스 중단을 일으키지 않으며, 즉각적인 시정 조치가 필요하지 않을 수도 있습니다.

경고 이벤트는 사용자 정의, 시스템 정의 또는 동적 임계값에서 전송됩니다.

- 정보

이 이벤트는 새로운 객체가 발견되거나 사용자 작업이 수행될 때 발생합니다. 예를 들어, 저장소 개체가 삭제되거나 구성이 변경되면 심각도 유형이 정보인 이벤트가 생성됩니다.

ONTAP 구성 변경을 감지하면 정보 이벤트를 직접 전송합니다.

자세한 내용은 다음 링크를 참조하세요.

- ["이벤트가 수신되면 어떻게 되나요?"](#)
- ["알림 이메일에는 어떤 정보가 포함되어 있나요?"](#)
- ["알림 추가"](#)
- ["성능 이벤트에 대한 알림 추가"](#)

Unified Manager에서 감지된 구성 변경 사항

Unified Manager는 클러스터의 구성 변경 사항을 모니터링하여 변경 사항이 성능 이벤트를 발생시키거나 성능 이벤트에 영향을 미쳤는지 확인하는 데 도움을 줍니다. 성능 탐색기 페이지에는 변경 이벤트 아이콘(●) 변경 사항이 감지된 날짜와 시간을 나타냅니다.

성능 탐색기 페이지와 워크로드 분석 페이지에서 성능 차트를 검토하여 변경 이벤트가 선택한 클러스터 개체의 성능에 영향을 미쳤는지 확인할 수 있습니다. 변경 사항이 성능 이벤트와 동시에 또는 거의 동시에 감지된 경우, 해당 변경 사항이 문제에 영향을 미쳐 이벤트 알림이 트리거되었을 수 있습니다.

Unified Manager는 정보 이벤트로 분류되는 다음과 같은 변경 이벤트를 감지할 수 있습니다.

- 볼륨은 집합체 사이를 이동합니다.

Unified Manager는 이동이 진행 중이거나 완료되었거나 실패한 경우를 감지할 수 있습니다. 볼륨 이동 중에 Unified Manager가 다운되더라도 다시 작동하면 볼륨 이동을 감지하고 해당 변경 이벤트를 표시합니다.

- 하나 이상의 모니터링되는 작업 부하가 포함된 QoS 정책 그룹의 처리량(MB/s 또는 IOPS) 제한이 변경됩니다.

정책 그룹 제한을 변경하면 지연 시간(응답 시간)이 간헐적으로 급증할 수 있으며, 이로 인해 정책 그룹에 대한 이벤트가 트리거될 수도 있습니다. 지연 시간은 점차 정상으로 돌아오고, 급증으로 인해 발생한 모든 이벤트는 더 이상 발생하지 않습니다.

- HA 쌍의 노드는 파트너 노드의 저장소를 인수하거나 반환해줍니다.

Unified Manager는 인수, 부분 인수 또는 반환 작업이 완료되는 시점을 감지할 수 있습니다. 인수가 패닉 상태의 노드로 인해 발생하는 경우 Unified Manager는 이벤트를 감지하지 못합니다.

- ONTAP 업그레이드 또는 되돌리기 작업이 성공적으로 완료되었습니다.

이전 버전과 새 버전이 표시됩니다.

시스템 정의 성능 임계값 정책 유형

Unified Manager는 클러스터 성능을 모니터링하고 이벤트를 자동으로 생성하는 몇 가지 표준 임계값 정책을 제공합니다. 이러한 정책은 기본적으로 활성화되어 있으며, 모니터링된 성능 임계값이 위반되면 경고 또는 정보 이벤트를 생성합니다.



시스템 정의 성능 임계값 정책은 Cloud Volumes ONTAP, ONTAP Edge 또는 ONTAP Select 시스템에서는 활성화되지 않습니다.

시스템에서 정의한 성능 임계값 정책에서 불필요한 이벤트를 수신하는 경우 이벤트 설정 페이지에서 개별 정책에 대한 이벤트를 비활성화할 수 있습니다.

클러스터 임계값 정책

시스템 정의 클러스터 성능 임계값 정책은 기본적으로 Unified Manager에서 모니터링하는 모든 클러스터에 할당됩니다.

- 클러스터 부하 불균형

클러스터의 다른 노드보다 한 노드가 훨씬 더 높은 부하로 작동하여 잠재적으로 작업 부하 지연에 영향을 미치는 상황을 식별합니다.

이 기능은 클러스터의 모든 노드에 대해 사용된 성능 용량 값을 비교하여 24시간 이상 30% 임계값을 초과한 노드가 있는지 확인합니다. 이는 경고 이벤트입니다.

- 클러스터 용량 불균형

클러스터 내 다른 집계보다 한 집계의 사용 용량이 훨씬 더 높은 상황을 식별하여 작업에 필요한 공간에 영향을 미칠 가능성이 있습니다.

클러스터 내 모든 집계의 사용된 용량 값을 비교하여 집계 간에 70%의 차이가 있는지 확인합니다. 이는 경고 이벤트입니다.

노드 임계값 정책

시스템 정의 노드 성능 임계값 정책은 기본적으로 Unified Manager에서 모니터링하는 클러스터의 모든 노드에 할당됩니다.

- 성능 용량 사용 임계값 위반

단일 노드가 운영 효율성의 한계를 넘어서 작동하고, 이로 인해 작업 대기 시간에 영향을 미칠 가능성이 있는 상황을 식별합니다.

이 기능은 12시간 이상 성능 용량의 100% 이상을 사용하는 노드를 찾아 이를 수행합니다. 이는 경고 이벤트입니다.

- 노드 HA 쌍이 과도하게 활용됨

HA 쌍의 노드가 HA 쌍 운영 효율성의 경계를 넘어서 작동하는 상황을 식별합니다.

이는 HA 쌍의 두 노드에 대해 사용된 성능 용량 값을 살펴봄으로써 수행됩니다. 두 노드에서 사용된 결합된 성능 용량이 12시간 이상 200%를 초과하는 경우 컨트롤러 장애 조치로 인해 작업 대기 시간이 영향을 받습니다. 이것은 정보 제공을 위한 행사입니다.

- 노드 디스크 조각화

집계된 디스크가 조각화되어 주요 시스템 서비스를 느리게 하고 노드의 작업 대기 시간에 영향을 미칠 수 있는 상황을 식별합니다.

이는 노드의 모든 집계에서 특정 읽기 및 쓰기 작업 비율을 살펴보는 방식으로 수행됩니다. 이 정책은 SyncMirror 재동기화 중이나 디스크 스냅 작업 중 오류가 발견될 때도 트리거될 수 있습니다. 이는 경고 이벤트입니다.



"노드 디스크 조각화" 정책은 HDD 전용 집계만 분석합니다. Flash Pool, SSD 및 FabricPool 집계는 분석되지 않습니다.

집계 임계값 정책

시스템 정의 집계 성능 임계값 정책은 Unified Manager에서 모니터링하는 클러스터의 모든 집계에 기본적으로 할당됩니다.

- 전체 디스크가 과도하게 활용됨

집계가 운영 효율성의 한계를 초과하여 작동하여 작업 대기 시간에 영향을 미칠 수 있는 상황을 식별합니다. 이 기능은 집계된 디스크가 30분 이상 95% 이상 활용되는 집계를 찾아 이러한 상황을 식별합니다. 이 다중 조건 정책은 문제의 원인을 파악하기 위해 다음과 같은 분석을 수행합니다.

- 집계된 디스크 중 현재 백그라운드 유지 관리 활동이 진행 중인가요?

디스크가 진행할 수 있는 백그라운드 유지 관리 활동으로는 디스크 재구성, 디스크 스냅러빙, SyncMirror 재동기화, 재패리티 등이 있습니다.

- 디스크 셀프 파이버 채널 상호 연결에 통신 병목 현상이 있습니까?
- 전체적으로 여유 공간이 너무 적습니까? 이 정책에 대한 경고 이벤트는 세 가지 하위 정책 중 하나(또는 그 이상)가 위반된 것으로 간주되는 경우에만 발행됩니다. 전체 디스크의 활용률이 95% 이상인 경우에만 성능 이벤트가 발생하지 않습니다.



"전체 디스크 과다 사용" 정책은 HDD 전용 집계와 Flash Pool(하이브리드) 집계를 분석합니다. SSD 및 FabricPool 집계는 분석되지 않습니다.

워크로드 지연 임계값 정책

시스템 정의 워크로드 지연 임계값 정책은 정의된 "예상 지연" 값을 갖는 구성된 성능 서비스 수준 정책이 있는 모든 워크로드에 할당됩니다.

- 성능 서비스 수준에 따라 정의된 작업 부하 볼륨/LUN 대기 시간 임계값 위반

예상 대기 시간 한도를 초과하고 작업 부하 성능에 영향을 미치는 볼륨(파일 공유) 및 LUN을 식별합니다. 이는 경고 이벤트입니다.

이는 이전 시간 동안 예상 대기 시간 값을 30% 초과한 작업 부하를 찾아 이를 수행합니다.

QoS 임계값 정책

시스템 정의 QoS 성능 임계값 정책은 ONTAP QoS 최대 처리량 정책(IOPS, IOPS/TB 또는 MB/s)이 구성된 모든 작업 부하에 할당됩니다. Unified Manager는 작업 부하 처리량 값이 구성된 QoS 값보다 15% 낮을 때 이벤트를 트리거합니다.

• QoS 최대 IOPS 또는 MB/s 임계값

QoS 최대 IOPS 또는 MB/s 처리량 한도를 초과하고 작업 대기 시간에 영향을 미치는 볼륨과 LUN을 식별합니다. 이는 경고 이벤트입니다.

단일 작업 부하가 정책 그룹에 할당되면 이전 1시간 동안의 각 수집 기간 동안 할당된 QoS 정책 그룹에 정의된 최대 처리량 임계값을 초과한 작업 부하를 찾아 이를 수행합니다.

여러 작업 부하가 단일 QoS 정책을 공유하는 경우 정책에 포함된 모든 작업 부하의 IOPS 또는 MB/s를 추가하고 해당 합계를 임계값과 비교하여 이를 수행합니다.

• QoS 피크 IOPS/TB 또는 블록 크기 임계값이 있는 IOPS/TB

적응형 QoS 최대 IOPS/TB 처리량 한도(또는 블록 크기 한도가 있는 IOPS/TB)를 초과하고 작업 대기 시간에 영향을 미치는 볼륨을 식별합니다. 이는 경고 이벤트입니다.

이 기능은 적응형 QoS 정책에 정의된 최대 IOPS/TB 임계값을 각 볼륨의 크기에 따라 QoS 최대 IOPS 값으로 변환한 다음, 이전 1시간 동안의 각 성능 수집 기간 동안 QoS 최대 IOPS를 초과한 볼륨을 찾습니다.



이 정책은 클러스터에 ONTAP 9.3 이상 소프트웨어가 설치된 경우에만 볼륨에 적용됩니다.

적응형 QoS 정책에서 "블록 크기" 요소가 정의된 경우 임계값은 각 볼륨의 크기에 따라 QoS 최대 MB/s 값으로 변환됩니다. 그런 다음 이전 1시간 동안의 각 성능 수집 기간 동안 QoS 최대 MB/s를 초과한 볼륨을 찾습니다.



이 정책은 클러스터에 ONTAP 9.5 이상 소프트웨어가 설치된 경우에만 볼륨에 적용됩니다.

성능 이벤트 분석 및 알림

성능 이벤트는 클러스터 구성 요소의 경합으로 인해 작업 부하의 I/O 성능 문제에 대해 알려줍니다. Unified Manager는 이벤트를 분석하여 관련된 모든 작업 부하, 경합 중인 구성 요소를 식별하고 이벤트가 여전히 해결해야 할 문제인지 여부를 확인합니다.

Unified Manager는 클러스터의 볼륨에 대한 I/O 지연 시간(응답 시간)과 IOPS(작업)를 모니터링합니다. 예를 들어, 다른 작업 부하가 클러스터 구성 요소를 과도하게 사용하면 해당 구성 요소는 경쟁 상태에 놓이게 되어 작업 부하 수요를 충족할 수 있는 최적의 수준으로 작업을 수행할 수 없습니다. 동일한 구성 요소를 사용하는 다른 작업 부하의 성능에 영향을 미쳐 대기 시간이 늘어날 수 있습니다. 지연 시간이 동적 성능 임계값을 넘으면 Unified Manager가 성능 이벤트를 트리거하여 사용자에게 알립니다.

이벤트 분석

Unified Manager는 지난 15일간의 성능 통계를 사용하여 다음 분석을 수행하여 이벤트에 관련된 피해자 워크로드, 괴롭힘 워크로드 및 클러스터 구성 요소를 식별합니다.

- 지연 시간이 동적 성능 임계값(지연 시간 예측의 상한)을 초과한 피해자 워크로드를 식별합니다.
 - HDD 또는 Flash Pool 하이브리드 집계(로컬 계층)의 볼륨의 경우 대기 시간이 5밀리초(ms)를 초과하고 IOPS가 초당 10개 작업(ops/sec)을 초과하는 경우에만 이벤트가 트리거됩니다.
 - 모든 SSD 집계 또는 FabricPool 집계(클라우드 계층)의 볼륨의 경우 지연 시간이 1ms보다 크고 IOPS가 초당 100ops를 초과하는 경우에만 이벤트가 트리거됩니다.
- 경합 중인 클러스터 구성 요소를 식별합니다.



클러스터 상호 연결에서 피해자 워크로드의 대기 시간이 1ms보다 크면 Unified Manager는 이를 심각한 문제로 간주하고 클러스터 상호 연결에 대한 이벤트를 트리거합니다.

- 클러스터 구성 요소를 과도하게 사용하여 경합을 일으키는 괴롭힘 작업 부하를 식별합니다.
- 클러스터 구성 요소의 활용도나 활동의 편차를 기준으로 관련 작업 부하를 순위를 매겨 클러스터 구성 요소 사용에서 가장 큰 변화를 보인 괴롭힘꾼과 가장 큰 영향을 받은 피해자를 파악합니다.

이벤트는 잠깐 동안만 발생할 수 있으며, 이벤트가 사용하는 구성 요소가 더 이상 경쟁하지 않으면 자동으로 수정될 수 있습니다. 연속 이벤트는 5분 간격으로 동일한 클러스터 구성 요소에 대해 반복 발생하고 활성 상태를 유지하는 이벤트입니다. 연속적인 이벤트의 경우 Unified Manager는 두 개의 연속된 분석 간격 동안 동일한 이벤트를 감지한 후 경고를 트리거합니다.

이벤트가 해결되면 해당 이벤트는 볼륨의 과거 성능 문제 기록의 일부로 Unified Manager에서 계속 사용할 수 있습니다. 각 이벤트에는 이벤트 유형과 관련된 볼륨, 클러스터, 클러스터 구성 요소를 식별하는 고유한 ID가 있습니다.



하나의 볼륨이 동시에 두 개 이상의 이벤트에 관련될 수 있습니다.

이벤트 상태

이벤트는 다음 상태 중 하나일 수 있습니다.

- 활동적인

성능 이벤트가 현재 활성화되어 있음을 나타냅니다(새로운 이벤트 또는 확인된 이벤트). 이벤트를 발생시킨 문제가 자체적으로 해결되지 않았거나 해결되지 않았습니다. 저장소 개체의 성능 카운터가 성능 임계값보다 높게 유지됩니다.

- 폐기됨

이벤트가 더 이상 활성화되지 않았음을 나타냅니다. 이벤트를 발생시킨 문제가 스스로 해결되었습니다. 저장소 개체의 성능 카운터가 더 이상 성능 임계값을 초과하지 않습니다.

이벤트 알림

이벤트는 대시보드 페이지와 사용자 인터페이스의 다른 여러 페이지에 표시되며, 해당 이벤트에 대한 알림은 지정된 이메일 주소로 전송됩니다. 이벤트에 대한 자세한 분석 정보를 보고 이벤트 세부 정보 페이지와 작업 부하 분석 페이지에서 해결을 위한 제안을 받을 수 있습니다.

이벤트 상호작용

이벤트 세부 정보 페이지와 작업 부하 분석 페이지에서 다음과 같은 방법으로 이벤트와 상호 작용할 수 있습니다.

- 이벤트 위로 마우스를 가져가면 이벤트가 감지된 날짜와 시간을 알려주는 메시지가 표시됩니다.

동일한 기간에 여러 개의 이벤트가 있는 경우 메시지에는 이벤트 수가 표시됩니다.

- 단일 이벤트를 클릭하면 해당 이벤트에 대한 더 자세한 정보(관련 클러스터 구성 요소 포함)를 보여 주는 대화 상자가 표시됩니다.

논쟁의 여지가 있는 구성 요소는 빨간색으로 표시되어 있습니다. *전체 분석 보기*를 클릭하면 이벤트 세부 정보 페이지에서 전체 분석을 볼 수 있습니다. 동일한 기간에 여러 이벤트가 있는 경우 대화 상자에는 가장 최근의 세 가지 이벤트에 대한 세부 정보가 표시됩니다. 이벤트를 클릭하면 이벤트 세부 정보 페이지에서 이벤트 분석을 볼 수 있습니다.

Unified Manager가 이벤트의 성능 영향을 결정하는 방법

Unified Manager는 작업 부하에 대한 활동, 활용도, 쓰기 처리량, 클러스터 구성 요소 사용 또는 I/O 지연(응답 시간)의 편차를 사용하여 작업 부하 성능에 미치는 영향 수준을 결정합니다. 이 정보는 이벤트에서 각 워크로드의 역할과 이벤트 세부 정보 페이지에서 워크로드의 순위가 결정되는 방식을 결정합니다.

Unified Manager는 워크로드에 대한 마지막 분석 값을 예상 범위(대기 시간 예측) 값과 비교합니다. 마지막으로 분석된 값과 예상 값 범위 간의 차이는 이벤트로 인해 성능에 가장 큰 영향을 받은 워크로드를 식별합니다.

예를 들어, 클러스터에 워크로드 A와 워크로드 B라는 두 가지 워크로드가 포함되어 있다고 가정해 보겠습니다. 워크로드 A에 대한 지연 시간은 작업당 5~10밀리초(ms/op)로 예측되고 실제 지연 시간은 일반적으로 약 7ms/op입니다. 워크로드 B에 대한 지연 시간은 10~20ms/op로 예측되며 실제 지연 시간은 일반적으로 15ms/op 정도입니다. 두 작업 모두 지연 시간 예측 범위 내에 있습니다. 클러스터에서의 경합으로 인해 두 작업 부하의 지연 시간이 40ms/op로 늘어나 지연 시간 예측의 상한인 동적 성능 임계값을 넘어서고 이벤트가 트리거됩니다. 워크로드 A의 경우 예상 값과 성능 임계값 이상의 값 사이의 지연 시간 편차는 약 33ms/op이고, 워크로드 B의 경우 편차는 약 25ms/op입니다. 두 워크로드의 지연 시간은 모두 40ms/op로 급증했지만, 워크로드 A는 지연 시간 편차가 33ms/op로 더 높아 성능에 더 큰 영향을 미쳤습니다.

이벤트 세부 정보 페이지의 시스템 진단 섹션에서 클러스터 구성 요소의 활동, 사용률 또는 처리량 편차를 기준으로 작업 부하를 정렬할 수 있습니다. 대기 시간을 기준으로 작업 부하를 정렬할 수도 있습니다. 정렬 옵션을 선택하면 Unified Manager는 이벤트가 감지된 이후 활동, 활용도, 처리량 또는 대기 시간의 편차를 예상 값과 비교하여 작업 부하 정렬 순서를 결정합니다. 지연 시간의 경우 빨간색 점(●)은 피해자 워크로드가 성능 임계값을 초과하고 이로 인해 지연 시간이 영향을 받는다는 것을 나타냅니다. 빨간색 점은 지연 시간의 편차가 더 크다는 것을 나타내며, 이를 통해 이벤트로 인해 지연 시간에 가장 큰 영향을 받은 피해자 워크로드를 식별하는 데 도움이 됩니다.

클러스터 구성 요소와 이들이 경쟁에 참여할 수 있는 이유

클러스터 구성 요소가 경합에 들어가면 클러스터 성능 문제를 식별할 수 있습니다. 해당 구성 요소를 사용하는 워크로드의 성능이 저하되고 클라이언트 요청에 대한 응답 시간(대기 시간)이 늘어나 Unified Manager에서 이벤트가 발생합니다.

경쟁 상태에 있는 구성 요소는 최적의 수준에서 성능을 발휘할 수 없습니다. 성능이 저하되었고, _피해자_라고 불리는 다른 클러스터 구성 요소와 워크로드의 성능으로 인해 지연 시간이 증가했을 수 있습니다. 구성 요소를 경쟁에서 벗어나게 하려면 작업 부하를 줄이거나 더 많은 작업을 처리할 수 있는 능력을 높여야 합니다. 이렇게 하면 성능이 정상

수준으로 돌아갈 수 있습니다. Unified Manager는 5분 간격으로 워크로드 성능을 수집하고 분석하므로 클러스터 구성 요소가 지속적으로 과도하게 사용되는 경우에만 감지합니다. 5분 간격 내에 짧은 시간 동안만 지속되는 과도한 사용의 일시적인 급증은 감지되지 않습니다.

예를 들어, 스토리지 집계는 하나 이상의 워크로드가 I/O 요청을 처리하기 위해 경쟁하고 있기 때문에 경합을 겪을 수 있습니다. 전체적으로 다른 작업 부하가 영향을 받아 성능이 저하될 수 있습니다. 집계된 활동량을 줄이려면 여러 가지 조치를 취할 수 있습니다. 예를 들어, 하나 이상의 작업 부하를 덜 바쁜 집계나 노드로 옮겨 현재 집계의 전반적인 작업 부하 수요를 줄이는 것입니다. QoS 정책 그룹의 경우 처리량 한도를 조정하거나 작업 부하를 다른 정책 그룹으로 이동하여 작업 부하가 더 이상 제한되지 않도록 할 수 있습니다.

Unified Manager는 다음 클러스터 구성 요소를 모니터링하여 해당 구성 요소가 경쟁 상태에 있을 때 경고합니다.

- 회로망

클러스터의 외부 네트워킹 프로토콜에 의한 I/O 요청의 대기 시간을 나타냅니다. 대기 시간이란 클러스터가 I/O 요청에 응답하기 전에 "전송 준비" 트랜잭션이 완료될 때까지 기다리는 시간입니다. 네트워크 구성 요소가 경합 중이면 프로토콜 계층에서 대기 시간이 길어져 하나 이상의 작업 부하 지연에 영향을 미치고 있음을 의미합니다.

- 네트워크 처리

프로토콜 계층과 클러스터 간의 I/O 처리와 관련된 클러스터의 소프트웨어 구성 요소를 나타냅니다. 이벤트가 감지된 이후 네트워크 처리를 담당하는 노드가 변경되었을 수 있습니다. 네트워크 처리 구성 요소가 경합 중이면 네트워크 처리 노드의 높은 활용도가 하나 이상의 작업 부하의 지연 시간에 영향을 미치고 있음을 의미합니다.

액티브-액티브 구성에서 All SAN 어레이 클러스터를 사용하는 경우 두 노드 모두에 대한 네트워크 처리 지연 값이 표시되므로 노드가 부하를 동등하게 공유하는지 확인할 수 있습니다.

- QoS 제한 최대

작업 부하에 할당된 스토리지 서비스 품질(QoS) 정책 그룹의 처리량 최대(피크) 설정을 나타냅니다. 정책 그룹 구성 요소가 경합 중이면 정책 그룹의 모든 작업 부하가 설정된 처리량 한도로 조절되고 있음을 의미하며, 이는 해당 작업 부하 중 하나 이상의 대기 시간에 영향을 미칩니다.

- QoS 제한 최소값

다른 워크로드에 할당된 QoS 처리량 최소(예상) 설정으로 인해 발생하는 워크로드 지연을 나타냅니다. 특정 작업 부하에 설정된 QoS 최소값이 약속된 처리량을 보장하기 위해 대부분의 대역폭을 사용하는 경우, 다른 작업 부하가 제한되고 지연 시간이 더 길어집니다.

- 클러스터 상호 연결

클러스터된 노드가 물리적으로 연결된 케이블과 어댑터를 나타냅니다. 클러스터 상호 연결 구성 요소가 경합 중이면 클러스터 상호 연결에서 I/O 요청에 대한 대기 시간이 길어져 하나 이상의 작업 부하 대기 시간에 영향을 미치고 있음을 의미합니다.

- * Data Processing*

클러스터와 작업 부하가 포함된 스토리지 집계 간의 I/O 처리와 관련된 클러스터의 소프트웨어 구성 요소를 나타냅니다. 이벤트가 감지된 이후 데이터 처리를 담당하는 노드가 변경되었을 수 있습니다. 데이터 처리 구성 요소가 경합 중이라는 것은 데이터 처리 노드의 높은 활용도가 하나 이상의 워크로드의 대기 시간에 영향을 미치고 있음을 의미합니다.

- 볼륨 활성화

모든 활성 볼륨의 사용량을 추적하는 프로세스를 나타냅니다. 1000개가 넘는 볼륨이 활성화된 대규모 환경에서 이 프로세스는 노드를 통해 동시에 리소스에 액세스해야 하는 중요 볼륨의 수를 추적합니다. 동시 활성 볼륨 수가 권장되는 최대 임계값을 초과하면 일부 비중요 볼륨에서 여기에 명시된 대로 지연이 발생합니다.

- * MetroCluster 리소스*

MetroCluster 구성에서 클러스터 간에 데이터를 미러링하는 데 사용되는 NVRAM 및 ISL(스위치 간 링크)을 포함한 MetroCluster 리소스를 나타냅니다. MetroCluster 구성 요소가 경합 중이면 로컬 클러스터의 작업 부하에서 높은 쓰기 처리량이 발생하거나 링크 상태 문제로 인해 로컬 클러스터에서 하나 이상의 작업 부하의 대기 시간이 영향을 받고 있음을 의미합니다. 클러스터가 MetroCluster 구성에 없으면 이 아이콘이 표시되지 않습니다.

- 집계 또는 **SSD** 집계 작업

워크로드가 실행되는 스토리지 집계를 나타냅니다. 집계 구성 요소가 경합 중이면 집계의 높은 활용도가 하나 이상의 워크로드의 대기 시간에 영향을 미치고 있음을 의미합니다. 집계는 모든 HDD로 구성되거나 HDD와 SSD의 혼합(Flash Pool 집계), 또는 HDD와 클라우드 계층의 혼합(FabricPool 집계)으로 구성됩니다. "SSD 집계"는 모든 SSD(울플래시 집계)로 구성되거나 SSD와 클라우드 계층(FabricPool 집계)의 혼합으로 구성됩니다.

- 클라우드 지연 시간

클러스터와 사용자 데이터가 저장된 클라우드 계층 간의 I/O 처리와 관련된 클러스터의 소프트웨어 구성 요소를 나타냅니다. 클라우드 지연 시간 구성 요소가 경합되는 경우 클라우드 계층에서 호스팅되는 볼륨에서 많은 양의 읽기가 하나 이상의 워크로드의 지연 시간에 영향을 미치고 있음을 의미합니다.

- * SnapMirror 동기화*

SnapMirror 동기 관계에서 기본 볼륨에서 보조 볼륨으로 사용자 데이터를 복제하는 데 관련된 클러스터의 소프트웨어 구성 요소를 나타냅니다. 동기화 SnapMirror 구성 요소가 경합 중이면 SnapMirror 동기 작업의 활동이 하나 이상의 워크로드의 대기 시간에 영향을 미치고 있음을 의미합니다.

성능 이벤트에 관련된 작업 부하의 역할

Unified Manager는 역할을 사용하여 성능 이벤트에서 워크로드의 관련성을 식별합니다. 역할에는 피해자, 괴롭힘꾼, 상어 등이 있습니다. 사용자 정의 워크로드는 동시에 피해자, 괴롭힘꾼, 상어가 될 수 있습니다.

역할	설명
피해자	클러스터 구성 요소를 과도하게 사용하는 다른 워크로드 (괴롭힘이라고 함)로 인해 성능이 저하된 사용자 정의 워크로드입니다. 사용자가 정의한 작업 부하만 피해자로 식별됩니다. Unified Manager는 지연 시간의 편차를 기준으로 피해자 워크로드를 식별합니다. 이벤트 중 실제 지연 시간은 지연 시간 예측(예상 범위)보다 크게 증가했습니다.

역할	설명
괴롭히는 사람	클러스터 구성 요소를 과도하게 사용하여 피해자라고 하는 다른 워크로드의 성능이 저하된 사용자 정의 또는 시스템 정의 워크로드입니다. Unified Manager는 이벤트 중에 실제 사용량이 예상 사용량 범위에서 크게 증가한 클러스터 구성 요소 사용량 편차를 기준으로 괴롭힘 워크로드를 식별합니다.
상어	이벤트에 관련된 모든 워크로드와 비교했을 때 클러스터 구성 요소를 가장 많이 사용하는 사용자 정의 워크로드입니다. Unified Manager는 이벤트 중에 클러스터 구성 요소의 사용을 기반으로 샤크 워크로드를 식별합니다.

클러스터의 작업 부하는 네트워크 및 데이터 처리를 위한 집계 및 CPU와 같은 많은 클러스터 구성 요소를 공유할 수 있습니다. 볼륨 등의 작업 부하가 클러스터 구성 요소의 사용량을 늘려 구성 요소가 작업 부하 수요를 효율적으로 충족할 수 없는 지점까지 이르면 해당 구성 요소는 경합 상태에 놓이게 됩니다. 클러스터 구성 요소를 과도하게 사용하는 작업 부하는 괴롭힘입니다. 이러한 구성 요소를 공유하고 괴롭힘에 의해 성과에 영향을 받는 다른 작업 부하가 피해자입니다. 중복 제거나 스냅샷 복사와 같은 시스템 정의 워크로드의 활동도 "괴롭힘"으로 확대될 수 있습니다.

Unified Manager가 이벤트를 감지하면 이벤트를 발생시킨 괴롭힘 워크로드, 경합 중인 클러스터 구성 요소, 괴롭힘 워크로드의 활동 증가로 인해 성능이 저하된 피해자 워크로드를 포함하여 관련된 모든 워크로드와 클러스터 구성 요소를 식별합니다.



Unified Manager가 위협적인 워크로드를 식별할 수 없는 경우, 피해 워크로드와 관련 클러스터 구성 요소에 대해서만 경고합니다.

Unified Manager는 괴롭힘 워크로드의 희생자가 되는 워크로드를 식별하고, 동일한 워크로드가 괴롭힘 워크로드가 되는 시점을 식별할 수 있습니다. 업무량은 스스로를 괴롭히는 요인이 될 수 있습니다. 예를 들어, 정책 그룹 제한으로 인해 고성능 워크로드가 제한되는 경우 정책 그룹 자체를 포함하여 해당 정책 그룹의 모든 워크로드가 제한됩니다. 진행 중인 성과 이벤트에서 괴롭힘을 주거나 피해를 주는 업무는 역할을 바꾸거나 더 이상 이벤트에 참여하지 않을 수 있습니다.

성능 임계값 관리

성능 임계값 정책을 사용하면 Unified Manager가 워크로드 성능에 영향을 줄 수 있는 문제에 대해 시스템 관리자에게 알리기 위해 이벤트를 생성하는 지점을 결정할 수 있습니다. 이러한 임계값 정책은 사용자 정의 성능 임계값이라고 합니다.

이 릴리스에서는 사용자 정의, 시스템 정의 및 동적 성능 임계값을 지원합니다. Unified Manager는 동적이고 시스템 정의된 성능 임계값을 사용하여 작업 부하 활동을 분석하여 적절한 임계값을 결정합니다. 사용자 정의 임계값을 사용하면 여러 성능 카운터와 여러 저장소 개체에 대한 상한 성능 한도를 정의할 수 있습니다.



시스템 정의 성능 임계값과 동적 성능 임계값은 Unified Manager에서 설정하며 구성할 수 없습니다. 시스템에서 정의한 성능 임계값 정책에서 불필요한 이벤트를 수신하는 경우 이벤트 설정 페이지에서 개별 정책을 비활성화할 수 있습니다.

사용자 정의 성능 임계값 정책의 작동 방식

클러스터에 성능 문제가 발생하고 있음을 스토리지 관리자에게 알리기 위해 이벤트를 스토리지 관리자에게 전송할 수 있도록 스토리지 개체(예: 집계 및 볼륨)에 성능 임계값 정책을 설정합니다.

다음은 수행하여 저장소 개체에 대한 성능 임계값 정책을 만듭니다.

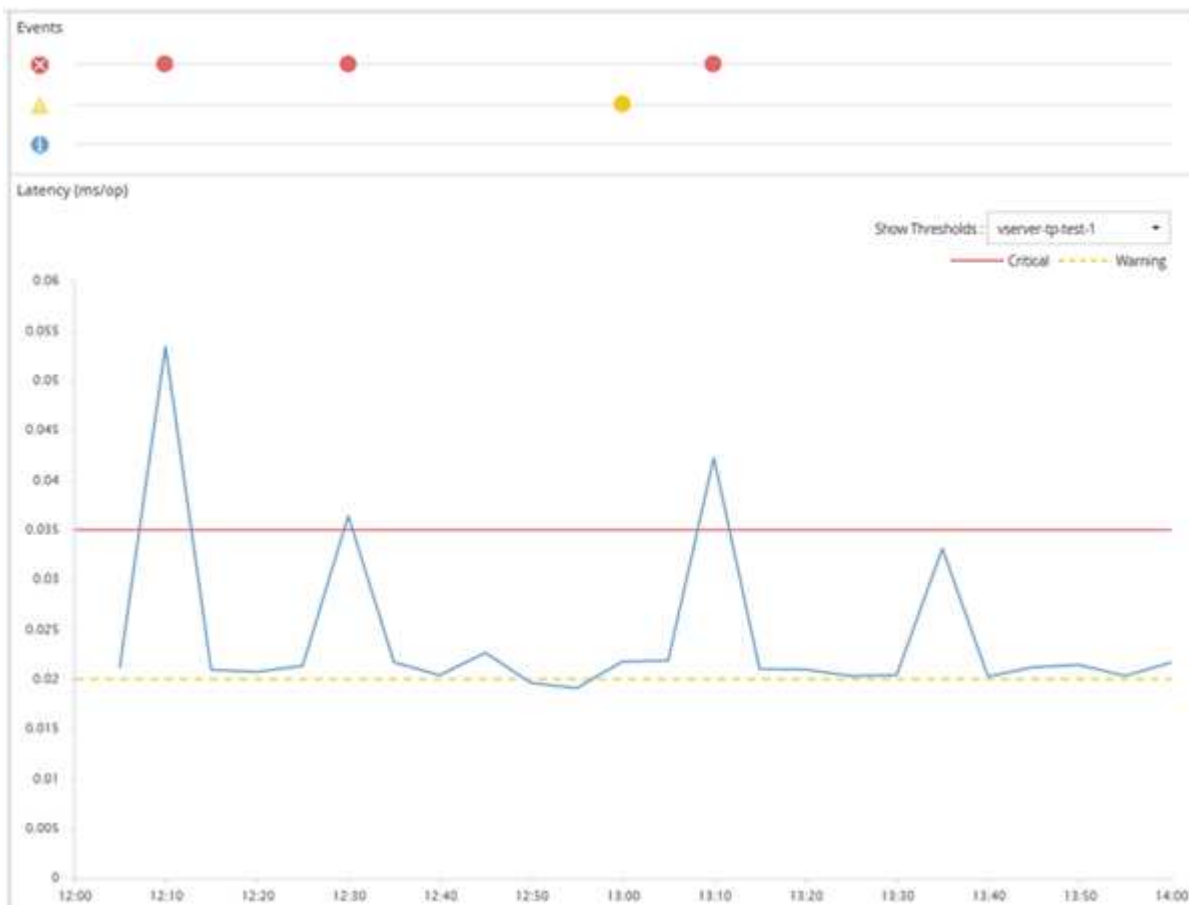
- 저장 객체 선택
- 해당 개체와 연관된 성능 카운터 선택
- 경고 및 위험 상황으로 간주되는 성능 카운터 상한을 정의하는 값 지정
- 카운터가 상한을 초과해야 하는 기간을 정의하는 기간 지정

예를 들어, 볼륨에 성능 임계값 정책을 설정하면 해당 볼륨의 IOPS가 10분 연속으로 초당 750개 작업을 초과할 때마다 중요 이벤트 알림을 받을 수 있습니다. 동일한 임계값 정책은 IOPS가 초당 500개 작업을 10분 동안 초과할 경우 경고 이벤트가 전송되도록 지정할 수도 있습니다.



현재 릴리스에서는 카운터 값이 임계값 설정을 초과할 때 이벤트를 전송하는 임계값을 제공합니다. 카운터 값이 임계값 설정 아래로 떨어지면 이벤트를 전송하는 임계값을 설정할 수 없습니다.

다음은 경고 임계값(노란색 아이콘)이 1:00에 위반되었고, 위험 임계값(빨간색 아이콘)이 12:10, 12:30, 1:10에 위반되었음을 나타내는 예시 카운터 차트입니다.



임계값 위반은 지정된 기간 동안 지속적으로 발생해야 합니다. 어떤 이유로든 임계값이 한도 값 아래로 떨어지면 후속 위반은 새로운 기간의 시작으로 간주됩니다.

일부 클러스터 개체와 성능 카운터를 사용하면 이벤트가 생성되기 전에 두 개의 성능 카운터가 최대 한도를 초과해야 하는 조합 임계값 정책을 만들 수 있습니다. 예를 들어, 다음 기준을 사용하여 임계값 정책을 만들 수 있습니다.

클러스터 객체	성능 카운터	경고 임계값	임계 임계값	지속
용량	숨어 있음	10밀리초	20밀리초	15분
골재	이용	65%	85%	

두 개의 클러스터 객체를 사용하는 임계값 정책은 두 조건이 모두 위반될 때만 이벤트를 생성합니다. 예를 들어, 표에 정의된 임계값 정책을 사용하면 다음과 같습니다.

볼륨 지연 시간이 평균화되면...	그리고 전체 디스크 활용도는...	그 다음에...
15밀리초	50%	아무런 사건도 보고되지 않았습니다.
15밀리초	75%	경고 이벤트가 보고되었습니다.
25밀리초	75%	경고 이벤트가 보고되었습니다.
25밀리초	90%	중대한 사건이 보고되었습니다.

성능 임계값 정책이 위반되면 어떻게 되나요?

카운터 값이 지속 시간에 지정된 시간 동안 정의된 성능 임계값을 초과하면 임계값이 초과되고 이벤트가 보고됩니다.

이 이벤트로 인해 다음 작업이 시작됩니다.

- 이벤트는 대시보드, 성능 클러스터 요약 페이지, 이벤트 페이지, 객체별 성능 인벤토리 페이지에 표시됩니다.
- (선택 사항) 이벤트에 대한 이메일 알림을 한 명 이상의 이메일 수신자에게 보낼 수 있으며, SNMP 트랩을 트랩 수신기에게 보낼 수 있습니다.
- (선택 사항) 스크립트를 실행하여 스토리지 객체를 자동으로 수정하거나 업데이트할 수 있습니다.

첫 번째 동작은 항상 실행됩니다. 알림 설정 페이지에서 선택적 작업을 수행할지 여부를 구성합니다. 경고 또는 위험 임계값 정책이 위반되었는지 여부에 따라 고유한 작업을 정의할 수 있습니다.

스토리지 개체에서 성능 임계값 정책 위반이 발생한 후에는 카운터 값이 임계값 아래로 떨어질 때까지 해당 정책에 대한 추가 이벤트가 생성되지 않습니다. 임계값 아래로 떨어지면 해당 제한에 대한 기간이 재설정됩니다. 임계값이 계속 초과되는 동안 이벤트 종료 시간은 이벤트가 진행 중임을 반영하기 위해 지속적으로 업데이트됩니다.

임계값 이벤트는 심각도 및 정책 정의와 관련된 정보를 캡처하거나 동결하여 나중에 임계값 정책이 수정되더라도 고유한 임계값 정보가 이벤트와 함께 표시되도록 합니다.

임계값을 사용하여 추적할 수 있는 성능 카운터는 무엇입니까?

IOPS 및 MB/s와 같은 일부 일반적인 성능 카운터에는 모든 스토리지 개체에 대한 임계값을

설정할 수 있습니다. 특정 저장 객체에 대해서만 임계값을 설정할 수 있는 다른 카운터도 있습니다.

사용 가능한 성능 카운터

저장 객체	성능 카운터	설명
무리	아이옴스	클러스터가 초당 처리하는 입출력 작업의 평균 수입입니다.
MB/초	초당 이 클러스터에서 전송되는 데이터의 평균 메가바이트 수입입니다.	마디
아이옴스	노드가 초당 처리하는 입출력 작업의 평균 수입입니다.	MB/초
초당 이 노드에서 전송되는 데이터의 평균 메가바이트 수입입니다.	숨어 있음	노드가 애플리케이션 요청에 응답하는 데 걸리는 평균 시간(밀리초)입니다.
이용	노드의 CPU와 RAM이 사용 중인 평균 비율입니다.	사용된 성능 용량
노드에서 소비되는 성능 용량의 평균 백분율입니다.	사용된 성능 용량 - 인수	노드에서 소비되는 성능 용량의 평균 백분율과 파트너 노드의 성능 용량을 합한 값입니다.
골재	아이옴스	초당 집계된 프로세스의 평균 입출력 작업 수입입니다.
MB/초	초당 이 집계에서 전송되는 데이터의 평균 메가바이트 수입입니다.	숨어 있음
집계된 데이터가 애플리케이션 요청에 응답하는 데 걸리는 평균 시간(밀리초)입니다.	이용	집계된 디스크 중 사용 중인 평균 비율입니다.
사용된 성능 용량	집계에 의해 소비되는 성능 용량의 평균 백분율입니다.	스토리지 VM
아이옴스	SVM이 초당 처리하는 입출력 작업의 평균 수입입니다.	MB/초
초당 이 SVM에서 전송되는 데이터의 평균 메가바이트 수입입니다.	숨어 있음	SVM이 애플리케이션 요청에 응답하는 데 걸리는 평균 시간(밀리초)입니다.

저장 객체	성능 카운터	설명
용량	아이옉스	볼륨이 초당 처리하는 입출력 작업의 평균 수입입니다.
MB/초	초당 이 볼륨에서 전송되는 데이터의 평균 메가바이트 수입입니다.	숨어 있음
볼륨이 애플리케이션 요청에 응답하는 데 걸리는 평균 시간(밀리초)입니다.	캐시 미스 비율	캐시에서 반환되는 대신 볼륨에서 반환되는 클라이언트 애플리케이션의 읽기 요청의 평균 백분율입니다.
LUN	아이옉스	LUN이 초당 처리하는 입출력 작업의 평균 수입입니다.
MB/초	초당 이 LUN에서 전송되는 데이터의 평균 메가바이트 수입입니다.	숨어 있음
LUN이 애플리케이션 요청에 응답하는 데 걸리는 평균 밀리초 수입입니다.	네임스페이스	아이옉스
네임스페이스가 초당 처리하는 평균 입출력 작업 수입입니다.	MB/초	초당 이 네임스페이스에서 전송되는 데이터의 평균 메가바이트 수입입니다.
숨어 있음	네임스페이스가 애플리케이션 요청에 응답하는 데 걸리는 평균 시간(밀리초)입니다.	포트
대역폭 활용도	포트의 사용 가능한 대역폭 중 현재 사용 중인 평균 비율입니다.	MB/초
초당 이 포트에서 전송되는 데이터의 평균 메가바이트 수입입니다.	네트워크 인터페이스(LIF)	MB/초

조합 임계값 정책에서 어떤 객체와 카운터를 사용할 수 있습니까?

일부 성능 카운터만 조합 정책에서 함께 사용할 수 있습니다. 1차 및 2차 성능 카운터가 지정되면 이벤트가 생성되기 전에 두 성능 카운터 모두 최대 한도를 초과해야 합니다.

1차 저장 객체 및 카운터	2차 저장 객체 및 카운터
볼륨 지연 시간	볼륨 IOPS
볼륨 MB/s	집계 활용

1차 저장 객체 및 카운터	2차 저장 객체 및 카운터
사용된 총 성능 용량	노드 활용도
사용된 노드 성능 용량	사용된 노드 성능 용량 - 인수
LUN 지연 시간	LUN IOPS
LUNMB/초	집계 활용
사용된 총 성능 용량	노드 활용도
사용된 노드 성능 용량	사용된 노드 성능 용량 - 인수



FlexVol 볼륨 대신 FlexGroup FlexVol volume 에 볼륨 조합 정책을 적용하는 경우 “볼륨 IOPS” 및 “볼륨 MB/s” 속성만 보조 카운터로 선택할 수 있습니다. 임계값 정책에 노드 또는 집계 속성 중 하나가 포함되어 있는 경우 해당 정책은 FlexGroup 볼륨에 적용되지 않으며, 이 경우를 설명하는 오류 메시지가 표시됩니다. 이는 FlexGroup 볼륨이 두 개 이상의 노드나 집계에 존재할 수 있기 때문입니다.

사용자 정의 성능 임계값 정책 생성

성능 카운터가 특정 값을 초과하면 알림이 전송되도록 스토리지 개체에 대한 성능 임계값 정책을 만듭니다. 이벤트 알림은 클러스터에 성능 문제가 발생하고 있음을 나타냅니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

성능 임계값 정책을 만들려면 성능 임계값 정책 만들기 페이지에서 임계값을 입력하세요. 이 페이지에서 모든 정책 값을 정의하여 새 정책을 만들거나 기존 정책의 복사본을 만들고 복사본의 값을 변경할 수 있습니다(복제라고 함).

유효한 임계값은 숫자의 경우 0.001~10,000,000이고, 백분율의 경우 0.001~100이며, 성능 용량 사용 백분율의 경우 0.001~200입니다.



현재 릴리스에서는 카운터 값이 임계값 설정을 초과할 때 이벤트를 전송하는 임계값을 제공합니다. 카운터 값이 임계값 설정 아래로 떨어지면 이벤트를 전송하는 임계값을 설정할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 이벤트 임계값 > *성능*을 선택합니다.

성능 임계값 페이지가 표시됩니다.

2. 새로운 정책을 구축할지, 아니면 유사한 정책을 복제하여 복제된 버전을 수정할지에 따라 적절한 버튼을 클릭합니다.

에게...	딸깍 하는 소리...
새로운 정책을 만듭니다	만들다
기존 정책 복제	기존 정책을 선택하고 *복제*를 클릭하세요.

성능 임계값 정책 생성 페이지 또는 성능 임계값 정책 복제 페이지가 표시됩니다.

3. 특정 저장소 개체에 대해 설정하려는 성능 카운터 임계값을 지정하여 임계값 정책을 정의합니다.

- a. 저장소 개체 유형을 선택하고 정책의 이름과 설명을 지정합니다.
- b. 추적할 성능 카운터를 선택하고 경고 및 중요 이벤트를 정의하는 제한 값을 지정합니다.

최소한 하나의 경고 또는 하나의 위험 한도를 정의해야 합니다. 두 가지 유형의 한계를 모두 정의할 필요는 없습니다.

- c. 필요한 경우 보조 성능 카운터를 선택하고 경고 및 중요 이벤트에 대한 제한 값을 지정합니다.

2차 카운터를 포함하려면 임계값이 초과되고 이벤트가 보고되기 전에 두 카운터가 모두 한도 값을 초과해야 합니다. 조합 정책을 사용하여 특정 개체와 카운터만 구성할 수 있습니다.

- d. 이벤트가 전송되기 위해 한계 값이 초과되어야 하는 시간 기간을 선택합니다.

기존 정책을 복제할 때는 정책의 새 이름을 입력해야 합니다.

4. 정책을 저장하려면 *저장*을 클릭하세요.

성능 임계값 페이지로 돌아갑니다. 페이지 상단의 성공 메시지는 임계값 정책이 생성되었음을 확인하고 해당 개체 유형의 인벤토리 페이지에 대한 링크를 제공하여 새 정책을 스토리지 개체에 즉시 적용할 수 있도록 합니다.

이때 저장소 개체에 새로운 임계값 정책을 적용하려면 지금 개체 유형으로 이동 링크를 클릭하여 인벤토리 페이지로 이동하면 됩니다.

스토리지 개체에 성능 임계값 정책 할당

Unified Manager가 성능 카운터 값이 정책 설정을 초과하면 이벤트를 보고하도록 사용자 정의 성능 임계값 정책을 저장소 개체에 할당합니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

개체에 적용하려는 성능 임계값 정책이 있어야 합니다.

한 번에 하나의 성능 정책만 개체 또는 개체 그룹에 적용할 수 있습니다.

각 저장소 개체에 최대 3개의 임계값 정책을 할당할 수 있습니다. 여러 개체에 정책을 할당할 때 개체 중 하나에 이미 최대 수의 정책이 할당된 경우 Unified Manager는 다음 작업을 수행합니다.

- 최대치에 도달하지 않은 선택된 모든 객체에 정책을 적용합니다.

- 최대 정책 수에 도달한 객체를 무시합니다.
- 정책이 모든 개체에 할당되지 않았다는 메시지를 표시합니다.

단계

1. 모든 저장소 개체의 성능 인벤토리 페이지에서 임계값 정책을 할당할 개체를 선택합니다.

임계값을 지정하려면...	딸깍 하는 소리...
단일 객체	해당 객체의 왼쪽에 있는 확인란입니다.
여러 개체	각 객체의 왼쪽에 있는 확인란입니다.
페이지의 모든 객체	그만큼 ☐ 드롭다운 상자를 선택하고 *이 페이지의 모든 개체 선택*을 선택하세요.
동일한 유형의 모든 객체	그만큼 ☐ 드롭다운 상자를 선택하고 *모든 개체 선택*을 선택하세요.

정렬 및 필터링 기능을 사용하면 인벤토리 페이지에서 개체 목록을 세분화하여 많은 개체에 임계값 정책을 더 쉽게 적용할 수 있습니다.

2. 선택한 후 *성능 임계값 정책 할당*을 클릭합니다.

성능 임계값 정책 할당 페이지가 표시되고, 해당 유형의 스토리지 개체에 대해 존재하는 임계값 정책 목록이 표시됩니다.

3. 각 정책을 클릭하면 성능 임계값 설정의 세부 정보가 표시되어 올바른 임계값 정책을 선택했는지 확인할 수 있습니다.
4. 적절한 임계값 정책을 선택한 후 *정책 할당*을 클릭합니다.

페이지 상단의 성공 메시지는 임계값 정책이 개체에 할당되었음을 확인하고, 이 개체와 정책에 대한 알림 설정을 구성할 수 있도록 알림 페이지에 대한 링크를 제공합니다.

특정 성능 이벤트가 생성되었음을 알리는 알림을 이메일이나 SNMP 트랩으로 보내려면 알림 설정 페이지에서 알림 설정을 구성해야 합니다.

성능 임계값 정책 보기

현재 정의된 모든 성능 임계값 정책은 성능 임계값 페이지에서 볼 수 있습니다.

임계값 정책 목록은 정책 이름을 기준으로 알파벳순으로 정렬되어 있으며, 모든 유형의 저장소 개체에 대한 정책이 포함되어 있습니다. 열 머리를 클릭하면 해당 열에 따라 정책을 정렬할 수 있습니다. 특정 정책을 찾는 경우 필터 및 검색 메커니즘을 사용하여 인벤토리 목록에 나타나는 임계값 정책 목록을 구체화하세요.

정책 이름과 조건 이름 위에 커서를 올려 놓으면 정책의 구성 세부 정보를 볼 수 있습니다. 또한 제공된 버튼을 사용하여 사용자 정의 임계값 정책을 생성, 복제, 편집 및 삭제할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 이벤트 임계값 > *성능*을 선택합니다.

성능 임계값 페이지가 표시됩니다.

사용자 정의 성능 임계값 정책 편집

기존 성능 임계값 정책에 대한 임계값 설정을 편집할 수 있습니다. 특정 임계값 조건에 대해 너무 많거나 너무 적은 알림을 받는 경우 이 기능이 유용할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

기존 임계값 정책에 대해 모니터링되는 저장소 개체의 정책 이름이나 유형을 변경할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 이벤트 임계값 > *성능*을 선택합니다.

성능 임계값 페이지가 표시됩니다.

2. 변경하려는 임계값 정책을 선택하고 *편집*을 클릭합니다.

성능 임계값 정책 편집 페이지가 표시됩니다.

3. 임계값 정책을 변경하고 *저장*을 클릭합니다.

성능 임계값 페이지로 돌아갑니다.

변경 사항이 저장된 후에는 해당 정책을 사용하는 모든 저장소 개체에 변경 사항이 즉시 업데이트됩니다.

정책에 적용한 변경 유형에 따라 알림 설정 페이지에서 해당 정책을 사용하는 개체에 대해 구성된 알림 설정을 검토할 수 있습니다.

스토리지 개체에서 성능 임계값 정책 제거

Unified Manager가 성능 카운터 값을 더 이상 모니터링하지 않도록 하려면 스토리지 개체에서 사용자 정의 성능 임계값 정책을 제거할 수 있습니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

선택한 개체에서 한 번에 하나의 정책만 제거할 수 있습니다.

목록에서 두 개 이상의 객체를 선택하여 여러 저장소 객체에서 임계값 정책을 제거할 수 있습니다.

단계

1. 모든 저장소 개체의 인벤토리 페이지에서 하나 이상의 성능 임계값 정책이 적용된 개체를 하나 이상 선택합니다.

임계값을 지우려면...	이렇게 하세요...
단일 객체	해당 객체의 왼쪽에 있는 확인란을 선택합니다.
여러 개체	각 객체의 왼쪽에 있는 확인란을 선택하세요.
페이지의 모든 객체	딸깍 하는 소리  열 머리글에.

2. *성능 임계값 정책 지우기*를 클릭하세요.

임계값 정책 지우기 페이지가 표시되고, 현재 저장소 개체에 할당된 임계값 정책 목록이 표시됩니다.

3. 개체에서 제거할 임계값 정책을 선택하고 *정책 지우기*를 클릭합니다.

임계값 정책을 선택하면 정책 세부 정보가 표시되어 적절한 정책을 선택했는지 확인할 수 있습니다.

성능 임계값 정책이 변경되면 어떻게 되나요?

기존 성능 임계값 정책의 카운터 값이나 기간을 조정하면 해당 정책을 사용하는 모든 스토리지 개체에 정책 변경 사항이 적용됩니다. 새로운 설정이 즉시 적용되고 Unified Manager는 새로 수집된 모든 성능 데이터에 대해 성능 카운터 값을 새로운 임계값 설정과 비교하기 시작합니다.

변경된 임계값 정책을 사용하는 개체에 대해 활성 이벤트가 있는 경우 해당 이벤트는 더 이상 사용되지 않음으로 표시되고 임계값 정책은 새로 정의된 임계값 정책으로 카운터 모니터링을 시작합니다.

임계값이 적용된 카운터를 카운터 차트 상세 보기에서 볼 때, 위험 및 경고 임계값 선은 현재 임계값 설정을 반영합니다. 이전 임계값 설정이 적용되었을 때의 기록 데이터를 보더라도 원래 임계값 설정은 이 페이지에 나타나지 않습니다.



이전 임계값 설정은 카운터 차트 상세 보기에 나타나지 않으므로 현재 임계값 선 아래에 과거 이벤트가 표시될 수 있습니다.

객체가 이동되면 성능 임계값 정책은 어떻게 되나요?

성능 임계값 정책은 스토리지 개체에 할당되므로 개체를 이동하면 이동이 완료된 후에도 할당된 모든 임계값 정책이 해당 개체에 연결된 상태로 유지됩니다. 예를 들어, 볼륨이나 LUN을 다른 집계로 이동하는 경우 임계값 정책은 새 집계의 볼륨이나 LUN에 대해 계속 활성화됩니다.

임계값 정책(조합 정책)에 대한 보조 카운터 조건이 있는 경우(예: 추가 조건이 집계 또는 노드에 할당된 경우) 보조 카운터 조건은 볼륨 또는 LUN이 이동된 새 집계 또는 노드에 적용됩니다.

변경된 임계값 정책을 사용하는 개체에 대해 새로운 활성 이벤트가 존재하는 경우 해당 이벤트는 더 이상 사용되지 않음으로 표시되고 임계값 정책은 새로 정의된 임계값 정책으로 카운터 모니터링을 시작합니다.

볼륨 이동 작업으로 인해 ONTAP 정보 변경 이벤트를 보냅니다. 이동 작업이 완료된 시간을 나타내기 위해 성능 탐색기 페이지와 워크로드 분석 페이지의 이벤트 타임라인에 변경 이벤트 아이콘이 나타납니다.



객체를 다른 클러스터로 이동하면 사용자 정의 임계값 정책이 객체에서 제거됩니다. 필요한 경우 이동 작업이 완료된 후 개체에 임계값 정책을 할당해야 합니다. 그러나 동적 및 시스템 정의 임계값 정책은 개체가 새 클러스터로 이동된 후 해당 개체에 자동으로 적용됩니다.

HA 인수 및 반환 중 임계값 정책 기능

고가용성(HA) 구성에서 인수 또는 반환 작업이 발생하는 경우 한 노드에서 다른 노드로 이동된 개체는 수동 이동 작업과 동일한 방식으로 임계값 정책을 유지합니다. Unified Manager는 15분마다 클러스터 구성 변경 사항을 확인하므로 새 노드로의 전환으로 인한 영향은 클러스터 구성의 다음 폴링 때까지 식별되지 않습니다.



15분의 구성 변경 수집 기간 내에 인수 및 반환 작업이 모두 발생하는 경우 성능 통계가 한 노드에서 다른 노드로 이동하지 않을 수 있습니다.

집계 이전 중 임계값 정책 기능

다음을 사용하여 한 노드에서 다른 노드로 집계를 이동하는 경우 `aggregate relocation start` 명령을 실행하면 모든 개체에 단일 및 조합 임계값 정책이 모두 유지되고 임계값 정책의 노드 부분이 새 노드에 적용됩니다.

MetroCluster 전환 중 임계값 정책 기능

MetroCluster 구성에서 한 클러스터에서 다른 클러스터로 이동하는 개체는 사용자 정의 임계값 정책 설정을 유지하지 않습니다. 필요한 경우 파트너 클러스터로 이동된 볼륨과 LUN에 임계값 정책을 적용할 수 있습니다. 객체가 원래 클러스터로 다시 이동한 후에는 사용자가 정의한 임계값 정책이 자동으로 다시 적용됩니다.

자세한 내용은 다음을 참조하세요. "[스위치오버 및 스위치백 중 볼륨 동작](#)".

성능 이벤트 분석

성능 이벤트를 분석하여 이벤트가 감지된 시점, 활성 상태(새 이벤트 또는 확인된 이벤트)인지 또는 오래된 이벤트인지, 관련된 워크로드 및 클러스터 구성 요소, 이벤트를 직접 해결하기 위한 옵션을 식별할 수 있습니다.

성능 이벤트에 대한 정보 표시

이벤트 관리 인벤토리 페이지를 사용하면 Unified Manager에서 모니터링하는 클러스터의 모든 성능 이벤트 목록을 볼 수 있습니다. 이 정보를 보면 가장 중요한 이벤트를 파악한 다음 자세한 정보를 분석하여 이벤트의 원인을 파악할 수 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이벤트 목록은 감지된 시간순으로 정렬되며, 가장 최근 이벤트가 먼저 나열됩니다. 열 머리글을 클릭하면 해당 열을 기준으로 이벤트를 정렬할 수 있습니다. 예를 들어, 상태 열별로 정렬하여 심각도별로 이벤트를 볼 수 있습니다. 특정 이벤트나 특정 유형의 이벤트를 찾는 경우 필터와 검색 메커니즘을 사용하여 목록에 나타나는 이벤트 목록을 구체화할 수 있습니다.

이 페이지에는 모든 출처의 이벤트가 표시됩니다.

- 사용자 정의 성능 임계값 정책
- 시스템 정의 성능 임계값 정책
- 동적 성능 임계값

이벤트 유형 열에는 이벤트 소스가 나열됩니다. 이벤트 세부 정보 페이지에서 이벤트를 선택하면 해당 이벤트에 대한 세부 정보를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭합니다.
2. 보기 메뉴에서 *활성 성능 이벤트*를 선택합니다.

이 페이지에는 지난 7일 동안 생성된 모든 새 성과 이벤트와 확인된 성과 이벤트가 표시됩니다.

3. 분석하려는 이벤트를 찾아 이벤트 이름을 클릭하세요.

이벤트에 대한 세부 정보 페이지가 표시됩니다.



성능 탐색기 페이지와 알림 이메일에서 이벤트 이름 링크를 클릭하면 이벤트의 세부 정보 페이지를 표시할 수도 있습니다.

사용자 정의 성능 임계값에서 이벤트 분석

사용자 정의 임계값에서 생성된 이벤트는 특정 스토리지 개체(예: 집계 또는 볼륨)에 대한 성능 카운터가 정책에서 정의한 임계값을 넘어섰음을 나타냅니다. 이는 클러스터 개체에 성능 문제가 발생하고 있음을 나타냅니다.

이벤트 세부 정보 페이지를 사용하여 성능 이벤트를 분석하고 필요한 경우 시정 조치를 취해 성능을 정상으로 되돌릴 수 있습니다.

사용자 정의 성능 임계값 이벤트에 응답

Unified Manager를 사용하면 성능 카운터가 사용자 정의 경고 또는 위험 임계값을 넘어선 경우 발생하는 성능 이벤트를 조사할 수 있습니다. Unified Manager를 사용하여 클러스터 구성 요소의 상태를 확인하여 구성 요소에서 최근에 감지된 상태 이벤트가 성능 이벤트에 영향을 미쳤는지 확인할 수도 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 공연 이벤트나 더 이상 진행되지 않는 공연 이벤트가 있어야 합니다.

단계

1. 이벤트에 대한 정보를 보려면 이벤트 세부 정보 페이지를 표시하세요.
2. 이벤트를 발생시킨 임계값 위반에 대한 설명이 있는 *설명*을 검토하세요.

예를 들어, "~456ms/op의 대기 시간 값이 400ms/op의 임계값 설정을 기반으로 경고 이벤트를 트리거했습니다"라는 메시지는 해당 개체에 대해 대기 시간 경고 이벤트가 발생했음을 나타냅니다.

3. 이벤트를 트리거한 임계값 정책에 대한 세부 정보를 표시하려면 정책 이름 위에 커서를 올려놓으세요.

여기에는 정책 이름, 평가 중인 성능 카운터, 중요 또는 경고 이벤트로 간주되기 위해 위반해야 하는 카운터 값, 카운터가 해당 값을 초과해야 하는 기간 등이 포함됩니다.

4. *이벤트 트리거 시간*을 기록해 두면 이 이벤트에 영향을 줄 수 있는 다른 이벤트가 동시에 발생했는지 조사할 수 있습니다.

5. 아래 옵션 중 하나를 따라 이벤트를 자세히 조사하고 성능 문제를 해결하기 위해 수행해야 할 작업이 있는지 확인하세요.

옵션	가능한 조사 조치
소스 개체 이름을 클릭하면 해당 개체의 탐색기 페이지가 표시됩니다.	이 페이지에서는 객체 세부 정보를 보고 이 객체를 다른 유사한 저장소 객체와 비교하여 다른 저장소 객체에 비슷한 시기에 성능 문제가 있는지 확인할 수 있습니다. 예를 들어, 동일한 집계에 있는 다른 볼륨에도 성능 문제가 있는지 확인합니다.
클러스터 이름을 클릭하면 클러스터 요약 페이지가 표시됩니다.	이 페이지에서는 이 개체가 있는 클러스터에 대한 세부 정보를 보고 비슷한 시기에 다른 성능 문제가 발생했는지 확인할 수 있습니다.

시스템 정의 성능 임계값에서 이벤트 분석

시스템에서 정의한 성능 임계값에서 생성된 이벤트는 특정 저장소 개체에 대한 성능 카운터 또는 성능 카운터 세트가 시스템에서 정의한 정책의 임계값을 넘어섰음을 나타냅니다. 이는 저장 객체 (예: 집계 또는 노드)에 성능 문제가 발생하고 있음을 나타냅니다.

이벤트 세부 정보 페이지를 사용하여 성능 이벤트를 분석하고 필요한 경우 시정 조치를 취해 성능을 정상으로 되돌릴 수 있습니다.



시스템 정의 임계값 정책은 Cloud Volumes ONTAP, ONTAP Edge 또는 ONTAP Select 시스템에서는 활성화되지 않습니다.

시스템 정의 성능 임계값 이벤트에 대응

Unified Manager를 사용하면 성능 카운터가 시스템에서 정의한 경고 임계값을 넘어선 경우 발생하는 성능 이벤트를 조사할 수 있습니다. Unified Manager를 사용하여 클러스터 구성 요소의 상태를 확인하여 구성 요소에서 최근에 감지된 이벤트가 성능 이벤트에 영향을 미쳤는지 확인할 수도 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 공연 이벤트나 더 이상 진행되지 않는 공연 이벤트가 있어야 합니다.

단계

1. 이벤트에 대한 정보를 보려면 이벤트 세부 정보 페이지를 표시하세요.

2. 이벤트를 발생시킨 임계값 위반에 대한 설명이 있는 *설명*을 검토하세요.

예를 들어, "노드 사용률 값이 90%로 인해 임계값 설정 85%에 따라 경고 이벤트가 발생했습니다"라는 메시지는 클러스터 개체에 대해 노드 사용률 경고 이벤트가 발생했음을 나타냅니다.

3. *이벤트 트리거 시간*을 기록해 두면 이 이벤트에 영향을 줄 수 있는 다른 이벤트가 동시에 발생했는지 조사할 수 있습니다.

4. *시스템 진단*에서 시스템 정의 정책이 클러스터 개체에 대해 수행하는 분석 유형에 대한 간략한 설명을 검토합니다.

일부 이벤트의 경우 진단 옆에 녹색 또는 빨간색 아이콘이 표시되어 해당 진단에서 문제가 발견되었는지 여부를 나타냅니다. 다른 유형의 시스템 정의 이벤트의 경우 카운터 차트는 개체의 성능을 표시합니다.

5. 제안된 작업*에서 *도움이 필요하면 알려주세요 링크를 클릭하면 성능 이벤트를 직접 해결하기 위해 수행할 수 있는 제안된 작업을 볼 수 있습니다.

QoS 정책 그룹 성능 이벤트에 응답

Unified Manager는 작업 부하 처리량(IOPS, IOPS/TB 또는 MBps)이 정의된 ONTAP QoS 정책 설정을 초과하고 작업 부하 지연에 영향을 미치는 경우 QoS 정책 경고 이벤트를 생성합니다. 이러한 시스템 정의 이벤트는 많은 작업 부하가 지연으로 인해 영향을 받기 전에 잠재적인 성능 문제를 해결할 수 있는 기회를 제공합니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 성과 이벤트, 인정된 성과 이벤트 또는 더 이상 진행되지 않는 성과 이벤트가 있어야 합니다.

Unified Manager는 이전 1시간 동안의 각 성능 수집 기간 동안 작업 부하 처리량이 정의된 QoS 정책 설정을 초과할 경우 QoS 정책 위반에 대한 경고 이벤트를 생성합니다. 수집 기간 동안 워크로드 처리량은 짧은 시간 동안만 QoS 임계값을 초과할 수 있지만 Unified Manager는 차트에 수집 기간 동안의 "평균" 처리량만 표시합니다. 이러한 이유로 차트에 표시된 정책 임계값을 워크로드 처리량이 넘지 않았더라도 QoS 이벤트가 발생할 수 있습니다.

시스템 관리자나 ONTAP 명령을 사용하여 다음 작업을 포함하여 정책 그룹을 관리할 수 있습니다.

- 작업 부하에 대한 새 정책 그룹 생성
- 정책 그룹에서 작업 부하 추가 또는 제거
- 정책 그룹 간 작업 부하 이동
- 정책 그룹의 처리량 제한 변경
- 작업 부하를 다른 집계 또는 노드로 이동

단계

1. 이벤트에 대한 정보를 보려면 이벤트 세부 정보 페이지를 표시하세요.
2. 이벤트를 발생시킨 임계값 위반에 대한 설명이 있는 *설명*을 검토하세요.

예를 들어, "vol1_NFS1에서 IOPS 값이 1,352 IOPS로 인해 작업 부하에 대한 잠재적인 성능 문제를 식별하기 위한 경고 이벤트가 발생했습니다"라는 메시지는 볼륨 vol1_NFS1에서 QoS 최대 IOPS 이벤트가 발생했음을 나타냅니다.

3. 이벤트 정보 섹션을 검토하여 이벤트가 발생한 시기와 이벤트가 진행된 기간에 대한 자세한 내용을 확인하세요.

또한 QoS 정책의 처리량을 공유하는 볼륨이나 LUN의 경우 가장 많은 IOPS 또는 MBps를 소모하는 상위 3개 워크로드의 이름을 볼 수 있습니다.

4. 시스템 진단 섹션에서 두 개의 차트를 검토합니다. 하나는 전체 평균 IOPS 또는 MBps(이벤트에 따라 다름)를 나타내는 차트이고, 다른 하나는 지연 시간을 나타내는 차트입니다. 이런 식으로 정리하면 작업 부하가 QoS 최대 한도에 접근했을 때 어떤 클러스터 구성 요소가 지연 시간에 가장 큰 영향을 미치는지 확인할 수 있습니다.

공유 QoS 정책 이벤트의 경우, 상위 3개 작업 부하가 처리량 차트에 표시됩니다. 3개 이상의 작업 부하가 QoS 정책을 공유하는 경우 추가 작업 부하가 "기타 작업 부하" 범주에 추가됩니다. 또한, 대기 시간 차트는 QoS 정책에 포함된 모든 작업 부하의 평균 대기 시간을 보여줍니다.

적응형 QoS 정책 이벤트의 경우 IOPS 및 MBps 차트는 ONTAP 볼륨 크기에 따라 할당된 IOPS/TB 임계값 정책에서 변환한 IOPS 또는 MBps 값을 표시합니다.

5. 제안된 작업 섹션에서 제안 사항을 검토하고 작업 부하로 인한 지연 시간이 증가하는 것을 방지하기 위해 수행해야 할 작업을 결정합니다.

필요한 경우 도움말 버튼을 클릭하여 성능 이벤트를 해결하기 위해 수행할 수 있는 제안된 작업에 대한 자세한 내용을 확인하세요.

정의된 블록 크기가 있는 적응형 **QoS** 정책의 이벤트를 이해합니다.

적응형 QoS 정책 그룹은 볼륨 크기에 따라 처리량 상한 또는 하한을 자동으로 조정하여 볼륨 크기가 변경되더라도 IOPS 대 TB 비율을 유지합니다. ONTAP 9.5부터 QoS 정책에서 블록 크기를 지정하여 동시에 MB/s 임계값을 효과적으로 적용할 수 있습니다.

적응형 QoS 정책에서 IOPS 임계값을 할당하면 각 작업 부하에서 발생하는 작업 수에만 제한이 적용됩니다. 작업 부하를 생성하는 클라이언트에 설정된 블록 크기에 따라 일부 IOPS에는 훨씬 더 많은 데이터가 포함되므로 작업을 처리하는 노드에 훨씬 더 큰 부담을 줍니다.

작업 부하에 대한 MB/s 값은 다음 공식을 사용하여 생성됩니다.

$$\text{MB/s} = (\text{IOPS} * \text{Block Size}) / 1000$$

작업 부하가 평균 3,000 IOPS이고 클라이언트의 블록 크기가 32KB로 설정된 경우, 이 작업 부하에 대한 효과적인 MB/s는 96입니다. 동일한 작업 부하가 평균 3,000 IOPS이고 클라이언트의 블록 크기가 48KB로 설정된 경우, 이 작업 부하에 대한 효과적인 MB/s는 144입니다. 블록 크기가 클수록 노드가 50% 더 많은 데이터를 처리하는 것을 볼 수 있습니다.

정의된 블록 크기가 있는 다음의 적응형 QoS 정책을 살펴보고 클라이언트에 설정된 블록 크기에 따라 이벤트가 어떻게 트리거되는지 알아보겠습니다.

정책을 만들고 최대 처리량을 블록 크기 32KB로 2,500 IOPS/TB로 설정합니다. 이를 통해 1TB 용량을 사용한 볼륨의 경우 MB/s 임계값이 80MB/s((2500 IOPS * 32KB) / 1000)로 효과적으로 설정됩니다. Unified Manager는 처리량 값이 정의된 임계값보다 10% 낮을 경우 경고 이벤트를 생성합니다. 이벤트는 다음과 같은 상황에서 생성됩니다.

사용된 용량	처리량이 이 숫자를 초과하면 이벤트가 생성됩니다.	
	아이오프스	MB/초
1TB	2,250 IOPS	72MB/초
2TB	4,500 IOPS	144MB/초
5TB	11,250 IOPS	360MB/초

볼륨이 사용 가능한 공간 중 2TB를 사용하고, IOPS가 4,000이며, 클라이언트에서 QoS 블록 크기가 32KB로 설정된 경우 MB/ps 처리량은 $128\text{MB/s}((4,000 \text{ IOPS} * 32\text{KB}) / 1000)$ 입니다. 이 시나리오에서는 4,000 IOPS와 128MB/s가 모두 2TB의 공간을 사용하는 볼륨에 대한 임계값보다 낮기 때문에 이벤트가 생성되지 않습니다.

볼륨이 사용 가능한 공간 중 2TB를 사용하고, IOPS가 4,000이며, 클라이언트에서 QoS 블록 크기가 64KB로 설정된 경우 MB/s 처리량은 $256\text{MB/s}((4,000 \text{ IOPS} * 64\text{KB}) / 1000)$ 입니다. 이 경우 4,000 IOPS는 이벤트를 생성하지 않지만 256MB/s의 MB/s 값은 144MB/s의 임계값을 초과하므로 이벤트가 생성됩니다.

이러한 이유로 블록 크기를 포함하는 적응형 QoS 정책에 대한 MB/s 위반을 기반으로 이벤트가 트리거되면 이벤트 세부 정보 페이지의 시스템 진단 섹션에 MB/s 차트가 표시됩니다. 적응형 QoS 정책에 대한 IOPS 위반으로 인해 이벤트가 트리거되는 경우 시스템 진단 섹션에 IOPS 차트가 표시됩니다. IOPS와 MB/s 모두에서 침해가 발생하면 두 가지 이벤트가 발생합니다.

QoS 설정 조정에 대한 자세한 내용은 다음을 참조하세요. ["성과 관리 개요"](#).

노드 리소스가 과도하게 사용되는 성능 이벤트에 대응합니다.

Unified Manager는 단일 노드가 운영 효율성의 한계를 초과하여 작동하고 이로 인해 워크로드 대기 시간에 영향을 미칠 가능성이 있는 경우 노드 리소스 과다 사용 경고 이벤트를 생성합니다. 이러한 시스템 정의 이벤트는 많은 작업 부하가 지연으로 인해 영향을 받기 전에 잠재적인 성능 문제를 해결할 수 있는 기회를 제공합니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 공연 이벤트나 더 이상 진행되지 않는 공연 이벤트가 있어야 합니다.

Unified Manager는 30분 이상 성능 용량의 100% 이상을 사용하는 노드를 찾아 노드 리소스가 과도하게 사용되는 정책 위반에 대한 경고 이벤트를 생성합니다.

시스템 관리자나 ONTAP 명령을 사용하여 다음 작업을 포함하여 이러한 유형의 성능 문제를 해결할 수 있습니다.

- 시스템 리소스를 과도하게 사용하는 볼륨이나 LUN에 QoS 정책을 만들고 적용합니다.
- 작업 부하가 적용된 정책 그룹의 QoS 최대 처리량 한도 감소
- 작업 부하를 다른 집계 또는 노드로 이동
- 노드에 디스크를 추가하거나 더 빠른 CPU와 더 많은 RAM을 갖춘 노드로 업그레이드하여 용량을 늘립니다.

단계

1. 이벤트에 대한 정보를 보려면 이벤트 세부 정보 페이지를 표시하세요.

- 이벤트를 발생시킨 임계값 위반에 대한 설명이 있는 *설명*을 검토하세요.

예를 들어, "Perf. simplicity-02에서 사용된 용량 값이 139%로 인해 데이터 처리 장치의 잠재적인 성능 문제를 식별하기 위한 경고 이벤트가 발생했습니다."는 노드 simplicity-02의 성능 용량이 과도하게 사용되어 노드 성능에 영향을 미치고 있음을 나타냅니다.

- 시스템 진단 섹션에서 세 개의 차트를 검토합니다. 하나는 노드에서 사용된 성능 용량, 다른 하나는 상위 워크로드에서 사용되는 평균 스토리지 IOPS, 다른 하나는 상위 워크로드의 대기 시간에 대한 차트입니다. 이런 식으로 정리하면 노드에서 지연을 유발하는 작업 부하가 무엇인지 확인할 수 있습니다.

커서를 IOPS 차트 위로 옮기면 어떤 워크로드에 QoS 정책이 적용되었고 어떤 워크로드에 적용되지 않았는지 확인할 수 있습니다.

- 제안된 작업 섹션에서 제안 사항을 검토하고 작업 부하로 인한 지연 시간이 증가하는 것을 방지하기 위해 수행해야 할 작업을 결정합니다.

필요한 경우 도움말 버튼을 클릭하여 성능 이벤트를 해결하기 위해 수행할 수 있는 제안된 작업에 대한 자세한 내용을 확인하세요.

클러스터 불균형 성능 이벤트에 대응

Unified Manager는 클러스터의 한 노드가 다른 노드보다 훨씬 높은 부하로 작동하고 이로 인해 작업 부하 대기 시간에 영향을 미칠 가능성이 있는 경우 클러스터 불균형 경고 이벤트를 생성합니다. 이러한 시스템 정의 이벤트는 많은 작업 부하가 지연으로 인해 영향을 받기 전에 잠재적인 성능 문제를 해결할 수 있는 기회를 제공합니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

Unified Manager는 클러스터의 모든 노드에 대해 사용된 성능 용량 값을 비교하여 노드 간에 30%의 부하 차이가 있는지 확인하여 클러스터 불균형 임계값 정책 위반에 대한 경고 이벤트를 생성합니다.

이러한 단계를 통해 다음 리소스를 식별하여 고성능 워크로드를 활용도가 낮은 노드로 이동할 수 있습니다.

- 동일 클러스터에서 활용도가 낮은 노드
- 새 노드에서 가장 적게 활용되는 집계
- 현재 노드에서 가장 높은 성능을 보이는 볼륨

단계

- 이벤트에 대한 정보를 보려면 이벤트 세부 정보 페이지를 표시합니다.
- 이벤트를 발생시킨 임계값 위반에 대한 설명이 있는 *설명*을 검토하세요.

예를 들어, "성능 용량 사용 카운터는 클러스터 Dallas-1-8의 노드 간에 62%의 부하 차이를 나타내며 시스템 임계값 30%에 따라 경고 이벤트를 트리거했습니다"라는 메시지는 노드 중 하나에서 성능 용량이 과도하게 사용되어 노드 성능에 영향을 미치고 있음을 나타냅니다.

- *제안된 작업*의 텍스트를 검토하여 고성능 볼륨을 고성능 용량 사용 값이 있는 노드에서 성능 용량 사용 값이 가장 낮은 노드로 이동합니다.
- 가장 높고 가장 낮은 성능 용량 사용 값을 갖는 노드를 식별합니다.

- a. 이벤트 정보 섹션에서 소스 클러스터의 이름을 클릭합니다.
 - b. 클러스터/성능 요약 페이지에서 관리되는 개체 영역의 *노드*를 클릭합니다.
 - c. 노드 인벤토리 페이지에서 성능 용량 사용 열에 따라 노드를 정렬합니다.
 - d. 가장 높고 가장 낮은 성능 용량 사용 값을 갖는 노드를 식별하고 해당 이름을 적어 둡니다.
5. 가장 높은 성능 용량 사용 값을 갖는 노드에서 가장 많은 IOPS를 사용하는 볼륨을 식별합니다.
 - a. 가장 높은 성능 용량 사용 값을 갖는 노드를 클릭하세요.
 - b. 노드/성능 탐색기 페이지에서 보기 및 비교 메뉴에서 *이 노드의 집계*를 선택합니다.
 - c. 가장 높은 성능 용량 사용 값을 갖는 집계를 클릭하세요.
 - d. 집계/성능 탐색기 페이지에서 보기 및 비교 메뉴에서 *이 집계의 볼륨*을 선택합니다.
 - e. **IOPS** 열로 볼륨을 정렬하고 가장 많은 IOPS를 사용하는 볼륨의 이름과 볼륨이 있는 집계의 이름을 적어 둡니다.
 6. 가장 낮은 성능 용량 사용 값을 갖는 노드에서 가장 낮은 활용도를 가진 집계를 식별합니다.
 - a. 저장 > 집계*를 클릭하여 *집계 인벤토리 페이지를 표시합니다.
 - b. 성과: 모든 집계 보기를 선택합니다.
 - c. 필터 버튼을 클릭하고 4단계에서 기록한 가장 낮은 성능 용량 사용 값을 가진 노드의 이름을 "노드"로 지정하여 필터를 추가합니다.
 - d. 가장 낮은 성능 용량 사용 값을 갖는 집계의 이름을 적어보세요.
 7. 과부하된 노드의 볼륨을 새 노드에서 사용률이 낮은 것으로 식별된 집계로 이동합니다.

ONTAP System Manager, OnCommand Workflow Automation, ONTAP 명령 또는 이러한 도구를 조합하여 이동 작업을 수행할 수 있습니다.

며칠 후에 이 클러스터에서 동일한 클러스터 불균형 이벤트가 발생하는지 확인하세요.

동적 성능 임계값에서 이벤트 분석

동적 임계값에서 생성된 이벤트는 워크로드에 대한 실제 응답 시간(대기 시간)이 예상 응답 시간 범위에 비해 너무 높거나 너무 낮음을 나타냅니다. 이벤트 세부 정보 페이지를 사용하여 성능 이벤트를 분석하고 필요한 경우 시정 조치를 취해 성능을 정상으로 되돌릴 수 있습니다.



Cloud Volumes ONTAP, ONTAP Edge 또는 ONTAP Select 시스템에서는 동적 성능 임계값이 활성화되지 않습니다.

동적 성능 이벤트에 관련된 피해자 작업 부하 식별

Unified Manager에서는 경쟁 중인 스토리지 구성 요소로 인해 응답 시간(대기 시간) 편차가 가장 큰 볼륨 워크로드를 식별할 수 있습니다. 이러한 작업 부하를 식별하면 해당 작업 부하에 액세스하는 클라이언트 애플리케이션의 성능이 평소보다 느린 이유를 이해하는 데 도움이 됩니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 동적 성과 이벤트, 인정된 이벤트 또는 더 이상 발생하지 않은 동적 성과 이벤트가 있어야 합니다.

이벤트 세부 정보 페이지에는 사용자 정의 및 시스템 정의 워크로드 목록이 표시되며, 구성 요소의 활동이나 사용에서 가장 큰 편차를 보이는 워크로드나 이벤트의 영향을 가장 많이 받는 워크로드 순으로 정렬됩니다. 값은 Unified Manager가 이벤트를 감지하고 마지막으로 분석했을 때 식별한 피크를 기반으로 합니다.

단계

1. 이벤트에 대한 정보를 보려면 이벤트 세부 정보 페이지를 표시하세요.
2. 워크로드 대기 시간 및 워크로드 활동 차트에서 *피해자 워크로드*를 선택합니다.
3. 차트 위에 커서를 올려 놓으면 해당 구성 요소에 영향을 미치는 상위 사용자 정의 워크로드와 피해자 워크로드의 이름을 볼 수 있습니다.

동적 성과 이벤트에 관련된 괴롭힘 작업 부하 식별

Unified Manager에서는 경쟁 중인 클러스터 구성 요소의 사용 편차가 가장 큰 워크로드를 식별할 수 있습니다. 이러한 작업 부하를 식별하면 클러스터의 특정 볼륨에서 응답 시간(대기 시간)이 느린 이유를 이해하는 데 도움이 됩니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 동적 성과 이벤트, 인정된 이벤트 또는 더 이상 발생하지 않은 동적 성과 이벤트가 있어야 합니다.

이벤트 세부 정보 페이지에는 구성 요소의 사용량이 가장 높거나 이벤트의 영향을 가장 많이 받는 순서대로 사용자 정의 및 시스템 정의 워크로드 목록이 표시됩니다. 값은 Unified Manager가 이벤트를 감지하고 마지막으로 분석했을 때 식별한 피크를 기반으로 합니다.

단계

1. 이벤트에 대한 정보를 보려면 이벤트 세부 정보 페이지를 표시합니다.
2. 워크로드 대기 시간 및 워크로드 활동 차트에서 *강력한 워크로드*를 선택합니다.
3. 차트 위에 커서를 올려 놓으면 해당 구성 요소에 영향을 미치는 가장 큰 사용자 정의 괴롭힘 워크로드를 볼 수 있습니다.

동적 성능 이벤트에 관련된 상어 작업 부하 식별

Unified Manager에서는 경합 중인 스토리지 구성 요소의 사용 편차가 가장 큰 워크로드를 식별할 수 있습니다. 이러한 작업 부하를 식별하면 해당 작업 부하를 활용도가 낮은 클러스터로 이동해야 하는지 여부를 결정하는 데 도움이 됩니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운, 인정된, 또는 더 이상 사용되지 않는 성과 동적 이벤트가 있습니다.

이벤트 세부 정보 페이지에는 구성 요소의 사용량이 가장 높거나 이벤트의 영향을 가장 많이 받는 순서대로 사용자 정의 및 시스템 정의 워크로드 목록이 표시됩니다. 값은 Unified Manager가 이벤트를 감지하고 마지막으로 분석했을 때 식별한 피크를 기반으로 합니다.

단계

1. 이벤트에 대한 정보를 보려면 이벤트 세부 정보 페이지를 표시하세요.
2. 워크로드 대기 시간 및 워크로드 활동 차트에서 *샤크 워크로드*를 선택합니다.
3. 차트 위에 커서를 올려 놓으면 해당 구성 요소에 영향을 미치는 상위 사용자 정의 워크로드와 샤크 워크로드의 이름을 볼 수 있습니다.

MetroCluster 구성에 대한 성능 이벤트 분석

Unified Manager를 사용하여 MetroCluster 구성에 대한 성능 이벤트를 분석할 수 있습니다. 이벤트에 관련된 작업 부하를 파악하고 이를 해결하기 위해 제안된 조치를 검토할 수 있습니다.

MetroCluster 성능 이벤트는 클러스터 간 ISL(스위치 간 링크)을 과도하게 활용하는 *bully* 워크로드나 링크 상태 문제로 인해 발생할 수 있습니다. Unified Manager는 파트너 클러스터의 성능 이벤트를 고려하지 않고 MetroCluster 구성의 각 클러스터를 독립적으로 모니터링합니다.

MetroCluster 구성의 두 클러스터에서 발생하는 성능 이벤트는 Unified Manager 대시보드 페이지에도 표시됩니다. Unified Manager의 상태 페이지를 통해 각 클러스터의 상태를 확인하고 클러스터 간의 관계를 확인할 수도 있습니다.

MetroCluster 구성의 클러스터에서 동적 성능 이벤트 분석

Unified Manager를 사용하면 성능 이벤트가 감지된 MetroCluster 구성의 클러스터를 분석할 수 있습니다. 클러스터 이름, 이벤트 감지 시간, 관련된 괴롭힘 및 피해 작업 부하를 식별할 수 있습니다.

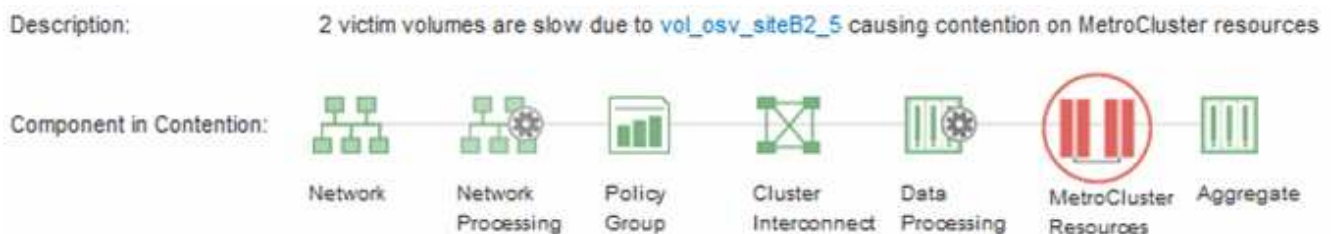
시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- MetroCluster 구성에는 새 성능 이벤트, 확인된 성능 이벤트 또는 오래된 성능 이벤트가 있어야 합니다.
- MetroCluster 구성의 두 클러스터는 모두 Unified Manager의 동일한 인스턴스에서 모니터링되어야 합니다.

단계

1. 이벤트에 대한 정보를 보려면 이벤트 세부 정보 페이지를 표시하세요.
2. 이벤트 설명을 검토하여 관련 작업 부하의 이름과 작업 부하의 수를 확인하세요.

이 예에서 MetroCluster 리소스 아이콘은 빨간색으로, MetroCluster 리소스가 경합 중임을 나타냅니다. 아이콘 위에 커서를 놓으면 아이콘에 대한 설명이 표시됩니다.

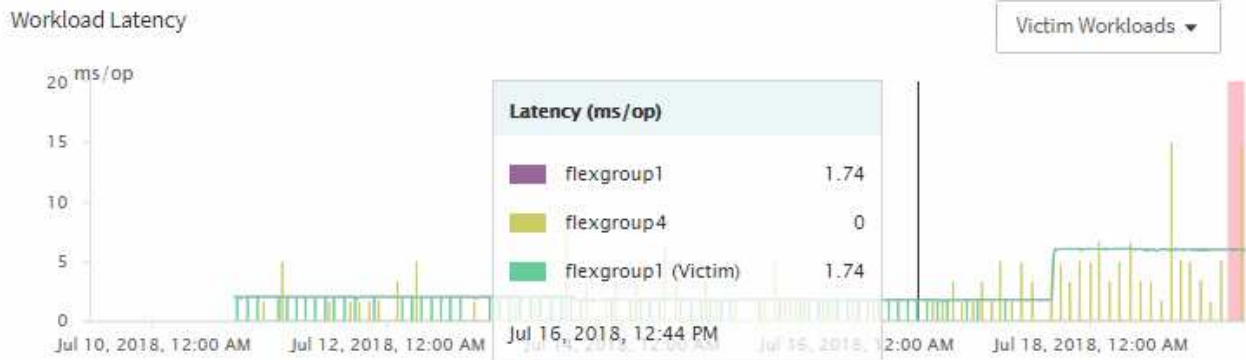


3. 파트너 클러스터의 성능 이벤트를 분석하는 데 사용할 수 있는 클러스터 이름과 이벤트 감지 시간을 기록해 두세요.
4. 차트에서 _피해자_의 작업 부하를 검토하여 응답 시간이 성능 임계값보다 높은지 확인합니다.

이 예에서 피해자 작업 부하가 호버 텍스트에 표시됩니다. 대기 시간 차트는 관련 피해자 워크로드에 대한 일관된

대기 시간 패턴을 높은 수준에서 표시합니다. 피해자 워크로드의 비정상적인 지연으로 인해 이벤트가 발생했지만, 일관된 지연 패턴은 워크로드가 예상 범위 내에서 수행되고 있지만 I/O의 급증으로 인해 지연이 늘어나 이벤트가 발생했음을 나타낼 수 있습니다.

System Diagnosis (Jul 9, 2018, 11:09 AM - Jul 19, 2018, 7:39 AM) ?



최근에 이러한 볼륨 작업 부하에 액세스하는 클라이언트에 애플리케이션을 설치했고 해당 애플리케이션이 해당 클라이언트에 많은 양의 I/O를 전송하는 경우 대기 시간이 증가할 것으로 예상할 수 있습니다. 워크로드에 대한 지연 시간이 예상 범위 내로 돌아오고 이벤트 상태가 '쓸모없음'으로 변경되고 이 상태가 30분 이상 지속되면 이벤트를 무시해도 됩니다. 이벤트가 진행 중이고 새로운 상태를 유지하는 경우, 다른 문제로 인해 이벤트가 발생했는지 확인하기 위해 추가로 조사할 수 있습니다.

5. 작업 부하 처리량 차트에서 *괴롭힘 작업 부하*를 선택하여 괴롭힘 작업 부하를 표시합니다.

괴롭힘 워크로드가 존재한다는 것은 로컬 클러스터에서 하나 이상의 워크로드가 MetroCluster 리소스를 과도하게 사용하여 이벤트가 발생했을 수 있음을 나타냅니다. 괴롭힘 작업 부하에서는 쓰기 처리량(MB/s)의 편차가 큼니다.

이 차트는 작업 부하에 대한 쓰기 처리량(MB/s) 패턴을 개략적으로 표시합니다. 쓰기 MB/s 패턴을 검토하여 비정상적인 처리량을 식별할 수 있습니다. 이는 워크로드가 MetroCluster 리소스를 과도하게 사용하고 있음을 나타낼 수 있습니다.

이벤트에 괴롭힘 워크로드가 포함되지 않은 경우, 해당 이벤트는 클러스터 간 링크의 상태 문제나 파트너 클러스터의 성능 문제로 인해 발생했을 수 있습니다. Unified Manager를 사용하면 MetroCluster 구성에서 두 클러스터의 상태를 확인할 수 있습니다. Unified Manager를 사용하여 파트너 클러스터의 성능 이벤트를 확인하고 분석할 수도 있습니다.

MetroCluster 구성의 원격 클러스터에 대한 동적 성능 이벤트 분석

Unified Manager를 사용하면 MetroCluster 구성의 원격 클러스터에서 동적 성능 이벤트를 분석할 수 있습니다. 분석을 통해 원격 클러스터의 이벤트가 파트너 클러스터에서 이벤트를 발생시켰는지 여부를 확인하는 데 도움이 됩니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- MetroCluster 구성의 로컬 클러스터에서 성능 이벤트를 분석하고 이벤트 감지 시간을 얻었어야 합니다.
- 성능 이벤트에 관련된 로컬 클러스터와 파트너 클러스터의 상태를 확인하고 파트너 클러스터의 이름을 얻어야 합니다.

단계

1. 파트너 클러스터를 모니터링하는 Unified Manager 인스턴스에 로그인합니다.
2. 왼쪽 탐색 창에서 *이벤트*를 클릭하면 이벤트 목록이 표시됩니다.
3. 시간 범위 선택기에서 *지난 1시간*을 선택한 다음 *범위 적용*을 클릭합니다.
4. 필터링 선택기에서 왼쪽 드롭다운 메뉴에서 *클러스터*를 선택하고, 텍스트 필드에 파트너 클러스터의 이름을 입력한 다음 *필터 적용*을 클릭합니다.

선택한 클러스터에서 지난 1시간 동안 이벤트가 발생하지 않은 경우, 파트너에서 이벤트가 감지된 시간 동안 클러스터에 성능 문제가 발생하지 않았음을 나타냅니다.

5. 선택한 클러스터에서 지난 1시간 동안 이벤트가 감지된 경우 이벤트 감지 시간을 로컬 클러스터의 이벤트 감지 시간과 비교합니다.

이러한 이벤트에 데이터 처리 구성 요소에서 경합을 일으키는 괴롭힘 작업 부하가 포함된 경우, 이러한 괴롭힘 중 하나 이상이 로컬 클러스터에서 이벤트를 발생시켰을 수 있습니다. 이벤트를 클릭하면 이벤트를 분석하고 이벤트 세부 정보 페이지에서 이벤트 해결을 위한 제안된 조치를 검토할 수 있습니다.

이러한 이벤트에 괴롭힘 워크로드가 포함되지 않은 경우 로컬 클러스터에서 성능 이벤트가 발생하지 않습니다.

QoS 정책 그룹 제한으로 인해 발생하는 동적 성능 이벤트에 대응

Unified Manager를 사용하면 작업 부하 처리량(MB/초)을 제한하는 서비스 품질(QoS) 정책 그룹으로 인해 발생한 성능 이벤트를 조사할 수 있습니다. 제한으로 인해 정책 그룹 내 볼륨 워크로드의 응답 시간(대기 시간)이 늘어났습니다. 이벤트 정보를 사용하여 제한을 중지하기 위해 정책 그룹에 대한 새로운 제한이 필요한지 여부를 확인할 수 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 성과 이벤트, 인정된 성과 이벤트 또는 더 이상 진행되지 않는 성과 이벤트가 있어야 합니다.

단계

1. 이벤트에 대한 정보를 보려면 이벤트 세부 정보 페이지를 표시하세요.
2. 제한에 의해 영향을 받는 워크로드의 이름이 표시된 *설명*을 읽어보세요.



설명에서는 피해자와 괴롭힘을 가하는 사람에게 동일한 작업 부하가 표시될 수 있는데, 이는 제한으로 인해 작업 부하가 그 자체로 피해자가 되기 때문입니다.

3. 텍스트 편집기와 같은 애플리케이션을 사용하여 볼륨의 이름을 기록합니다.

나중에 볼륨 이름을 검색하여 찾을 수 있습니다.

4. 워크로드 대기 시간 및 워크로드 활용도 차트에서 *강력한 워크로드*를 선택합니다.
5. 정책 그룹에 영향을 미치는 상위 사용자 정의 워크로드를 보려면 차트 위에 커서를 올려 놓으세요.

목록의 맨 위에 있는 작업 부하의 편차가 가장 크고 이로 인해 제한이 발생했습니다. 활동은 각 작업 부하에서 사용되는 정책 그룹 한도의 백분율입니다.

6. 제안된 작업 영역에서 가장 상위 작업 부하에 대한 작업 부하 분석 버튼을 클릭합니다.

7. 작업 부하 분석 페이지에서 대기 시간 차트를 설정하여 모든 클러스터 구성 요소를 보고, 처리량 차트를 설정하여 세부 정보를 봅니다.

세부 차트는 대기 시간 차트와 IOPS 차트 아래에 표시됩니다.

8. 대기 시간 차트에서 QoS 한도를 비교하여 이벤트 발생 시점에 얼마나 많은 제한이 대기 시간에 영향을 미쳤는지 확인하세요.

QoS 정책 그룹의 최대 처리량은 초당 1,000개의 작업(op/sec)이며, 그룹의 작업 부하가 전체적으로 이를 초과할 수 없습니다. 이벤트 발생 당시 정책 그룹의 작업 부하의 총 처리량은 1,200 op/sec가 넘었고, 이로 인해 정책 그룹은 활동을 1,000 op/sec로 제한했습니다.

9. 읽기/쓰기 대기 시간 값을 읽기/쓰기/기타 값과 비교합니다.

두 차트 모두 높은 지연 시간과 함께 많은 수의 읽기 요청을 보여주지만, 쓰기 요청의 요청 수와 지연 시간은 낮습니다. 이러한 값은 처리량이 많은지, 아니면 대기 시간을 증가시키는 작업 수가 많은지 여부를 확인하는 데 도움이 됩니다. 처리량이나 작업에 정책 그룹 제한을 적용할지 결정할 때 이러한 값을 사용할 수 있습니다.

10. ONTAP 시스템 관리자를 사용하여 정책 그룹의 현재 제한을 초당 1,300개로 늘립니다.
11. 하루가 지난 후 Unified Manager로 돌아와 3단계에서 기록한 작업 부하를 작업 부하 분석 페이지에 입력합니다.
12. 처리량 분석 차트를 선택합니다.

읽기/쓰기/기타 차트가 표시됩니다.

13. 페이지 상단에서 커서를 변경 이벤트 아이콘(●) 정책 그룹 한도 변경을 위해.
14. 읽기/쓰기/기타 차트를 대기 시간 차트와 비교해보세요.

읽기 및 쓰기 요청은 동일하지만, 제한이 중지되었고 지연 시간이 감소했습니다.

디스크 장애로 인해 발생하는 동적 성능 이벤트에 대응

Unified Manager를 사용하면 집계를 과도하게 활용하는 워크로드로 인해 발생한 성능 이벤트를 조사할 수 있습니다. Unified Manager를 사용하여 집계 상태를 확인하여 집계에서 감지된 최근 상태 이벤트가 성능 이벤트에 영향을 미쳤는지 확인할 수도 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 성과 이벤트, 인정된 성과 이벤트 또는 더 이상 진행되지 않는 성과 이벤트가 있어야 합니다.

단계

1. 이벤트에 대한 정보를 보려면 이벤트 세부 정보 페이지를 표시하세요.
2. 이벤트에 관련된 작업 부하와 경합 중인 클러스터 구성 요소를 설명하는 *설명*을 읽어보세요.

경쟁 중인 클러스터 구성 요소의 영향을 받는 지연 시간이 있는 피해자 볼륨이 여러 개 있습니다. 실패한 디스크를 예비 디스크로 교체하기 위한 RAID 재구성 중간에 있는 집계는 경쟁 중인 클러스터 구성 요소입니다. 경합 중인 구성 요소에서 집계 아이콘은 빨간색으로 강조 표시되고 집계 이름은 괄호 안에 표시됩니다.

3. 작업 부하 활용도 차트에서 *강력한 작업 부하*를 선택합니다.

4. 차트 위에 커서를 올려 놓으면 해당 구성 요소에 영향을 미치는 가장 큰 괴롭힘 워크로드를 볼 수 있습니다.

이벤트가 감지된 이후 가장 높은 피크 활용률을 보인 상위 워크로드가 차트 상단에 표시됩니다. 가장 중요한 작업 부하 중 하나는 RAID 재구성을 나타내는 시스템 정의 작업 부하인 디스크 상태입니다. 재구성은 예비 디스크를 사용하여 집계를 재구성하는 데 관련된 내부 프로세스입니다. 디스크 상태 작업 부하와 집계된 다른 작업 부하가 집계 및 관련 이벤트에서 경합을 일으켰을 가능성이 높습니다.

5. 디스크 상태 작업 부하로 인한 활동이 이벤트를 발생시켰는지 확인한 후 재구성이 완료되고 Unified Manager가 이벤트를 분석하여 집계가 여전히 경합 중인지 감지할 때까지 약 30분 동안 기다립니다.

6. *이벤트 세부정보*를 새로고침하세요.

RAID 재구성이 완료된 후 상태가 더 이상 사용되지 않아 이벤트가 해결되었는지 확인합니다.

7. 워크로드 활용도 차트에서 *강력한 워크로드*를 선택하면 최대 활용도에 따른 집계된 워크로드를 볼 수 있습니다.

8. 제안된 작업 영역에서 가장 상위 작업 부하에 대한 작업 부하 분석 버튼을 클릭합니다.

9. 작업 부하 분석 페이지에서 시간 범위를 설정하여 선택한 볼륨의 최근 24시간(1일) 데이터를 표시합니다.

이벤트 타임라인에서 빨간색 점(●)은 디스크 오류 이벤트가 발생한 시점을 나타냅니다.

10. 노드 및 집계 활용도 차트에서 노드 통계에 대한 줄을 숨겨 집계 줄만 남도록 합니다.

11. 이 차트의 데이터를 대기 시간 차트의 이벤트 발생 시점의 데이터와 비교해보세요.

이벤트 발생 시 집계 활용도는 RAID 재구성 프로세스로 인해 많은 양의 읽기 및 쓰기 활동을 보여주며, 이로 인해 선택한 볼륨의 대기 시간이 증가했습니다. 이벤트가 발생한 후 몇 시간이 지나면서 읽기 및 쓰기와 지연 시간이 모두 감소하여 집계가 더 이상 경합되지 않는다는 것이 확인되었습니다.

HA 인수로 인해 발생하는 동적 성능 이벤트에 대응

Unified Manager를 사용하면 고가용성(HA) 쌍에 있는 클러스터 노드에서 높은 데이터 처리로 인해 발생한 성능 이벤트를 조사할 수 있습니다. Unified Manager를 사용하여 노드의 상태를 확인하여 노드에서 최근에 감지된 상태 이벤트가 성능 이벤트에 영향을 미쳤는지 확인할 수도 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 성과 이벤트, 인정된 성과 이벤트 또는 더 이상 진행되지 않는 성과 이벤트가 있어야 합니다.

단계

1. 이벤트에 대한 정보를 보려면 이벤트 세부 정보 페이지를 표시하세요.
2. 이벤트에 관련된 작업 부하와 경합 중인 클러스터 구성 요소를 설명하는 *설명*을 읽어보세요.

경쟁 중인 클러스터 구성 요소의 영향을 받는 지연 시간이 있는 피해 볼륨이 하나 있습니다. 파트너 노드로부터 모든 작업 부하를 인수한 데이터 처리 노드는 경쟁 중인 클러스터 구성 요소입니다. 경합 중인 구성 요소에서 Data Processing 아이콘이 빨간색으로 강조 표시되고 이벤트 발생 시 데이터 처리를 담당하던 노드의 이름이 괄호 안에 표시됩니다.

3. *설명*에서 볼륨 이름을 클릭합니다.

볼륨 성능 탐색기 페이지가 표시됩니다. 페이지 상단의 이벤트 타임라인에 변경 이벤트 아이콘()은 Unified Manager가 HA 인수의 시작을 감지한 시간을 나타냅니다.

4. HA 인수에 대한 변경 이벤트 아이콘에 커서를 올리면 HA 인수에 대한 세부 정보가 호버 텍스트에 표시됩니다.

대기 시간 차트에서 이벤트는 HA 인수와 거의 동시에 높은 대기 시간으로 인해 선택된 볼륨이 성능 임계값을 초과했음을 나타냅니다.

5. *확대 보기*를 클릭하면 새 페이지에 대기 시간 차트가 표시됩니다.
6. 보기 메뉴에서 *클러스터 구성 요소*를 선택하면 클러스터 구성 요소별 총 지연 시간을 볼 수 있습니다.
7. HA 인수 시작을 위해 변경 이벤트 아이콘에 마우스 커서를 놓고 데이터 처리 지연 시간을 전체 지연 시간과 비교합니다.

HA 인수 시점에 데이터 처리 노드의 작업 부하 수요 증가로 인해 데이터 처리가 급증했습니다. CPU 사용률이 증가하면서 지연 시간이 늘어나고 이벤트가 발생했습니다.

8. 실패한 노드를 수정한 후 ONTAP 시스템 관리자를 사용하여 HA Giveback을 수행하여 작업 부하를 파트너 노드에서 수정된 노드로 이동합니다.
9. HA 반환이 완료된 후 Unified Manager에서 다음 구성 검색(약 15분)이 수행되면 이벤트 관리 인벤토리 페이지에서 HA 인수로 인해 발생한 이벤트와 작업 부하를 찾습니다.

HA 인수로 인해 발생한 이벤트는 이제 폐기 상태로 바뀌어 이벤트가 해결되었음을 나타냅니다. 데이터 처리 구성 요소의 대기 시간이 감소하여 전체 대기 시간이 줄었습니다. 선택된 볼륨이 현재 데이터 처리에 사용 중인 노드에서 이벤트가 해결되었습니다.

성능 이벤트 해결

제안된 작업을 사용하여 성능 이벤트를 직접 해결해 볼 수 있습니다. 처음 세 가지 제안은 항상 표시되고, 네 번째 제안에 따른 작업은 표시되는 이벤트 유형에 따라 달라집니다.

도움이 필요합니다 링크는 특정 작업을 수행하기 위한 지침을 포함하여 제안된 각 작업에 대한 추가 정보를 제공합니다. 일부 작업에는 Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, ONTAP CLI 명령 또는 이러한 도구의 조합을 사용하는 것이 포함될 수 있습니다.

지연 시간이 예상 범위 내에 있는지 확인하세요.

클러스터 구성 요소가 경합 중일 때 해당 구성 요소를 사용하는 볼륨 작업 부하의 응답 시간(대기 시간)이 감소할 수 있습니다. 경합 중인 구성 요소의 각 피해자 워크로드의 대기 시간을 검토하여 실제 대기 시간이 예상 범위 내에 있는지 확인할 수 있습니다. 볼륨 이름을 클릭하면 해당 볼륨의 과거 데이터를 볼 수도 있습니다.

성능 이벤트가 더 이상 유효하지 않은 상태인 경우 이벤트에 관련된 각 피해자의 지연 시간은 예상 범위 내로 돌아왔을 수 있습니다.

구성 변경이 워크로드 성능에 미치는 영향을 검토합니다.

디스크 오류, HA 장애 조치 또는 볼륨 이동과 같은 클러스터의 구성 변경은 볼륨 성능에 부정적인 영향을 미치고 지연 시간이 증가할 수 있습니다.

Unified Manager에서 워크로드 분석 페이지를 검토하여 최근 구성 변경이 발생한 시점을 확인하고 이를 작업 및 대기 시간(응답 시간)과 비교하여 선택한 볼륨 워크로드에 대한 활동에 변경이 있었는지 확인할 수 있습니다.

Unified Manager의 성능 페이지는 제한된 수의 변경 이벤트만 감지할 수 있습니다. 상태 페이지는 구성 변경으로 인해 발생하는 다른 이벤트에 대한 알림을 제공합니다. Unified Manager에서 볼륨을 검색하여 이벤트 기록을 확인할 수 있습니다.

클라이언트 측에서 작업 부하 성능을 개선하기 위한 옵션

성능 이벤트에 관련된 볼륨에 I/O를 보내는 애플리케이션이나 데이터베이스와 같은 클라이언트 작업 부하를 확인하여 클라이언트 측 변경으로 해당 이벤트가 수정될 수 있는지 확인할 수 있습니다.

클러스터의 볼륨에 연결된 클라이언트가 I/O 요청을 늘리면 클러스터는 수요를 충족하기 위해 더 열심히 작동해야 합니다. 클러스터의 특정 볼륨에 대해 많은 I/O 요청을 하는 클라이언트가 누구인지 알고 있다면 볼륨에 액세스하는 클라이언트 수를 조정하거나 볼륨에 대한 I/O 양을 줄여 클러스터 성능을 개선할 수 있습니다. 볼륨이 속한 QoS 정책 그룹에 제한을 적용하거나 늘릴 수도 있습니다.

클라이언트와 해당 애플리케이션을 조사하여 클라이언트가 평소보다 많은 I/O를 보내고 있는지 확인할 수 있으며, 이로 인해 클러스터 구성 요소에서 경합이 발생할 수 있습니다. 이벤트 세부 정보 페이지의 시스템 진단 섹션에는 경합 중인 구성 요소를 사용하는 상위 볼륨 워크로드가 표시됩니다. 특정 볼륨에 어떤 클라이언트가 액세스하는지 알고 있다면 해당 클라이언트로 가서 클라이언트 하드웨어나 애플리케이션이 예상대로 작동하지 않는지, 아니면 평소보다 많은 작업을 수행하고 있는지 확인할 수 있습니다.

MetroCluster 구성에서는 로컬 클러스터의 볼륨에 대한 쓰기 요청이 원격 클러스터의 볼륨으로 미러링됩니다. 로컬 클러스터의 소스 볼륨을 원격 클러스터의 대상 볼륨과 동기화하면 MetroCluster 구성에서 두 클러스터의 수요도 증가할 수 있습니다. 이러한 미러링된 볼륨에 대한 쓰기 요청을 줄이면 클러스터가 수행하는 동기화 작업이 줄어들어 다른 작업 부하에 미치는 성능 영향이 줄어듭니다.

클라이언트 또는 네트워크 문제를 확인하세요

클러스터의 볼륨에 연결된 클라이언트가 I/O 요청을 늘리면 클러스터는 수요를 충족하기 위해 더 열심히 작동해야 합니다. 클러스터에 대한 수요가 증가하면 구성 요소가 경합에 빠지고, 해당 구성 요소를 사용하는 워크로드의 대기 시간이 늘어나고, Unified Manager에서 이벤트가 발생할 수 있습니다.

이벤트 세부 정보 페이지의 시스템 진단 섹션에는 경합 중인 구성 요소를 사용하는 상위 볼륨 워크로드가 표시됩니다. 특정 볼륨에 어떤 클라이언트가 액세스하는지 알고 있다면 해당 클라이언트로 가서 클라이언트 하드웨어나 애플리케이션이 예상대로 작동하지 않는지, 아니면 평소보다 많은 작업을 수행하고 있는지 확인할 수 있습니다. 도움이 필요하면 클라이언트 관리자나 애플리케이션 공급업체에 문의해야 할 수도 있습니다.

네트워크 인프라를 검사하여 클러스터와 연결된 클라이언트 간의 I/O 요청이 예상보다 느리게 수행되는 원인이 될 수 있는 하드웨어 문제, 병목 현상 또는 경쟁 작업 부하가 있는지 확인할 수 있습니다. 도움이 필요하면 네트워크 관리자에게 문의하세요.

QoS 정책 그룹의 다른 볼륨에 비정상적으로 높은 활동이 있는지 확인하십시오.

활동 변화가 가장 큰 QoS(서비스 품질) 정책 그룹에서 작업 부하를 검토하여 두 개 이상의 작업 부하가 이벤트를 발생시켰는지 확인할 수 있습니다. 또한 다른 작업 부하가 여전히 설정된 처리량 한도를 초과하고 있는지, 아니면 예상 활동 범위 내로 돌아왔는지도 확인할 수 있습니다.

이벤트 세부 정보 페이지의 시스템 진단 섹션에서 활동의 최대 편차를 기준으로 워크로드를 정렬하면 활동에서 가장 큰 변화가 있는 워크로드가 표의 맨 위에 표시됩니다. 이러한 작업 부하는 활동이 설정된 한도를 초과하여 이벤트를 발생시켰을 수 있는 "괴롭힘꾼"일 수 있습니다.

각 볼륨 워크로드의 워크로드 분석 페이지로 이동하여 IOPS 활동을 검토할 수 있습니다. 작업 부하가 매우 높은 운영 활동 기간을 갖는 경우 이벤트에 영향을 미쳤을 수 있습니다. 작업 부하에 대한 정책 그룹 설정을 변경하거나 작업 부하를 다른 정책 그룹으로 이동할 수 있습니다.

다음과 같이 ONTAP 시스템 관리자나 ONTAP CLI 명령을 사용하여 정책 그룹을 관리할 수 있습니다.

- 정책 그룹을 만듭니다.
- 정책 그룹에 워크로드를 추가하거나 제거합니다.
- 정책 그룹 간에 작업 부하를 이동합니다.
- 정책 그룹의 처리량 한도를 변경합니다.

논리적 인터페이스(LIF) 이동

논리적 인터페이스(LIF)를 사용량이 적은 포트로 옮기면 부하 분산을 개선하고, 유지 관리 작업과 성능 조정을 지원하며, 간접 액세스를 줄이는 데 도움이 됩니다.

간접 접근은 시스템 효율성을 저하시킬 수 있습니다. 이는 볼륨 워크로드가 네트워크 처리와 데이터 처리에 서로 다른 노드를 사용할 때 발생합니다. 간접 액세스를 줄이려면 LIF를 재배열할 수 있습니다. 즉, 네트워크 처리와 데이터 처리에 동일한 노드를 사용하도록 LIF를 이동하는 것입니다. ONTAP 자동으로 바쁜 LIF를 다른 포트로 이동하도록 로드 밸런싱을 구성하거나 LIF를 수동으로 이동할 수 있습니다.

이익	고려사항
• 부하 분산을 개선합니다. • 간접 접근을 줄입니다.	 CIFS 공유에 연결된 LIF를 이동하면 CIFS 공유에 액세스하는 클라이언트의 연결이 끊어집니다. CIFS 공유에 대한 모든 읽기 또는 쓰기 요청이 중단됩니다.

ONTAP 명령을 사용하여 부하 분산을 구성합니다. 자세한 내용은 ONTAP 네트워킹 문서를 참조하세요.

ONTAP 시스템 관리자와 ONTAP CLI 명령을 사용하여 LIF를 수동으로 이동합니다.

덜 바쁜 시간에 스토리지 효율성 작업을 실행하세요.

영향을 받는 볼륨 작업 부하가 덜 바쁜 시간에 스토리지 효율성 작업을 처리하는 정책이나 일정을 실행하도록 수정할 수 있습니다.

저장소 효율성 작업은 많은 양의 클러스터 CPU 리소스를 사용할 수 있으며 작업이 실행되는 볼륨에 큰 부담을 줄 수 있습니다. 스토리지 효율성 작업이 실행되는 동시에 피해자 볼륨의 활동이 많으면 대기 시간이 늘어나 이벤트가 발생할 수 있습니다.

이벤트 세부 정보 페이지의 시스템 진단 섹션에는 활동의 최대 편차에 따라 QoS 정책 그룹의 작업 부하가 표시되어 괴롭힘 작업 부하를 식별합니다. 표 상단에 "저장 효율성"이 표시되면 이러한 작업이 피해자 워크로드를 괴롭히고 있는 것입니다. 이러한 작업 부하가 덜 바쁜 시간에 실행되도록 효율성 정책이나 일정을 수정하면 스토리지 효율성 작업으로

인해 클러스터에서 경합이 발생하는 것을 방지할 수 있습니다.

ONTAP System Manager를 사용하면 효율성 정책을 관리할 수 있습니다. ONTAP 명령을 사용하여 효율성 정책과 일정을 관리할 수 있습니다.

저장 효율성은 무엇입니까?

저장 효율성을 통해 가장 낮은 비용으로 최대 양의 데이터를 저장할 수 있으며, 더 적은 공간을 사용하면서 빠른 데이터 증가를 수용할 수 있습니다. NetApp 스토리지 효율성 전략은 핵심 ONTAP 운영 체제와 WAFL(Write Anywhere File Layout) 파일 시스템이 제공하는 내장 스토리지 가상화와 통합 스토리지 기반에 기반을 두고 있습니다.

스토리지 효율성에는 씬 프로비저닝, 스냅샷 복사, 중복 제거, 데이터 압축, FlexClone, SnapVault 및 볼륨 SnapMirror를 사용한 씬 복제, RAID-DP, Flash Cache, Flash Pool 집계, FabricPool 지원 집계와 같은 기술을 사용하는 것이 포함되며, 이러한 기술은 스토리지 활용도를 높이고 스토리지 비용을 줄이는 데 도움이 됩니다.

통합 스토리지 아키텍처를 사용하면 SAN(스토리지 영역 네트워크), NAS(네트워크 연결 스토리지), 보조 스토리지를 단일 플랫폼에 효율적으로 통합할 수 있습니다.

Flash Pool 집계 또는 Flash Cache 및 RAID-DP 기술로 구성된 직렬 고급 기술 연결(SATA) 드라이브와 같은 고밀도 디스크 드라이브는 성능과 복원력에 영향을 주지 않고 효율성을 높입니다.

FabricPool 지원 집계에는 로컬 성능 계층으로 모든 SSD 집계 또는 HDD 집계(ONTAP 9.8부터 시작)가 포함되고, 클라우드 계층으로 지정하는 개체 저장소가 포함됩니다. FabricPool 구성하면 데이터에 자주 액세스하는지 여부에 따라 어떤 스토리지 계층(로컬 계층 또는 클라우드 계층)에 데이터를 저장해야 하는지 관리하는 데 도움이 됩니다.

씬 프로비저닝, 스냅샷 복사, 중복 제거, 데이터 압축, SnapVault 및 볼륨 SnapMirror를 사용한 씬 복제, FlexClone과 같은 기술은 더 나은 절감 효과를 제공합니다. 이러한 기술을 개별적으로 또는 함께 사용하여 최대의 저장 효율성을 달성할 수 있습니다.

디스크 추가 및 데이터 재할당

집계에 디스크를 추가하여 저장 용량과 해당 집계의 성능을 높일 수 있습니다. 디스크를 추가한 후에는 추가한 디스크에 데이터를 재할당해야만 읽기 성능이 향상되는 것을 볼 수 있습니다.

Unified Manager가 동적 임계값이나 시스템 정의 성능 임계값에 의해 트리거된 집계 이벤트를 수신한 경우 다음 지침을 사용할 수 있습니다.

- 동적 임계값 이벤트를 수신하면 이벤트 세부 정보 페이지에서 경합 중인 집계를 나타내는 클러스터 구성 요소 아이콘이 빨간색으로 강조 표시됩니다.

아이콘 아래 괄호 안에는 디스크를 추가할 수 있는 집계를 식별하는 집계 이름이 있습니다.

- 시스템 정의 임계값 이벤트를 수신하면 이벤트 세부 정보 페이지에서 이벤트 설명 텍스트에 문제가 있는 집계의 이름이 나열됩니다.

이 집계에서 디스크를 추가하고 데이터를 재할당할 수 있습니다.

집계에 추가하는 디스크는 이미 클러스터에 존재해야 합니다. 클러스터에 사용 가능한 추가 디스크가 없는 경우 관리자에게 문의하거나 추가 디스크를 구매해야 할 수도 있습니다. ONTAP 시스템 관리자나 ONTAP 명령을 사용하여 디스크를 집계에 추가할 수 있습니다.



HDD 및 Flash Pool 집계를 사용할 때만 데이터를 재할당해야 합니다. SSD 또는 FabricPool 집계에 데이터를 재할당하지 마세요.

노드에서 **Flash Cache**를 활성화하면 작업 부하 성능이 어떻게 향상될 수 있나요?

클러스터의 각 노드에서 Flash Cache™ 지능형 데이터 캐싱을 활성화하면 워크로드 성능을 개선할 수 있습니다.

플래시 캐시 모듈 또는 성능 가속 모듈 PCIe 기반 메모리 모듈은 지능형 외부 읽기 캐시 역할을 하여 무작위 읽기 집약적 작업의 성능을 최적화합니다. 이 하드웨어는 ONTAP의 WAFL 외부 캐시 소프트웨어 구성 요소와 함께 작동합니다.

Unified Manager의 이벤트 세부 정보 페이지에서 경합 중인 집계를 나타내는 클러스터 구성 요소 아이콘이 빨간색으로 강조 표시됩니다. 아이콘 아래 괄호 안에는 집계의 이름이 표시되어 있으며, 이를 통해 집계를 식별할 수 있습니다. 집계가 있는 노드에서 Flash Cache를 활성화할 수 있습니다.

ONTAP 시스템 관리자나 ONTAP 명령을 사용하면 Flash Cache가 설치되었거나 활성화되어 있는지 확인하고, 아직 활성화되어 있지 않으면 활성화할 수 있습니다. 다음 명령은 특정 노드에서 Flash Cache가 활성화되어 있는지 여부를 나타냅니다. **cluster::> run local options flexscale.enable**

Flash Cache와 이를 사용하기 위한 요구 사항에 대한 자세한 내용은 다음 기술 보고서를 참조하세요.

["기술 보고서 3832: 플래시 캐시 모범 사례 가이드"](#)

스토리지 집계에서 **Flash Pool**을 활성화하면 워크로드 성능이 어떻게 향상될 수 있나요?

집계에서 Flash Pool 기능을 활성화하면 워크로드 성능을 개선할 수 있습니다. 플래시 풀은 HDD와 SSD를 모두 통합한 집합체입니다. HDD는 기본 저장 장치로 사용되고 SSD는 고성능 읽기 및 쓰기 캐시를 제공하여 전체 성능을 향상시킵니다.

Unified Manager에서 이벤트 세부 정보 페이지에는 경합 중인 집계의 이름이 표시됩니다. ONTAP 시스템 관리자나 ONTAP 명령을 사용하여 Flash Pool이 집계에 대해 활성화되어 있는지 확인할 수 있습니다. SSD가 설치되어 있는 경우 명령줄 인터페이스를 사용하여 SSD를 활성화할 수 있습니다. SSD가 설치되어 있는 경우 집계에서 다음 명령을 실행하여 Flash Pool이 활성화되어 있는지 확인할 수 있습니다. **cluster::> storage aggregate show -aggregate aggr_name -field hybrid-enabled**

이 명령에서, *aggr_name* 는 경합하는 집계와 같은 집계의 이름입니다.

Flash Pool과 이를 사용하기 위한 요구 사항에 대한 자세한 내용은 *_Clustered Data ONTAP 물리적 스토리지 관리 가이드_*를 참조하세요.

MetroCluster 구성 상태 점검

Unified Manager를 사용하면 IP 또는 FC를 통해 MetroCluster 구성의 클러스터 상태를 검토할 수 있습니다. 상태와 이벤트는 작업 부하의 성능에 영향을 미치는 하드웨어나 소프트웨어 문제가 있는지 확인하는 데 도움이 됩니다.

Unified Manager에서 이메일 알림을 보내도록 구성하면 로컬 또는 원격 클러스터에서 성능 이벤트에 영향을 미쳤을 수 있는 상태 문제가 있는지 이메일을 확인할 수 있습니다. Unified Manager GUI에서 *이벤트 관리*를 선택하면 현재 이벤트 목록을 볼 수 있으며, 필터를 사용하여 MetroCluster 구성 이벤트만 표시할 수 있습니다.

자세한 내용은 다음을 참조하세요. "[MetroCluster 구성에서 클러스터 상태 확인](#)"

MetroCluster 구성 확인

FC 및 IP 구성을 통한 MetroCluster 에서 미러링된 워크로드의 성능 문제를 방지하려면 MetroCluster 구성이 올바르게 설정되어 있는지 확인하세요. 구성을 변경하거나 소프트웨어나 하드웨어 구성 요소를 업그레이드하여 워크로드 성능을 개선할 수도 있습니다.

참조하다 "[MetroCluster 문서](#)" FC(Fibre Channel) 스위치, 케이블, ISL(스위치 간 링크)을 포함하여 MetroCluster 구성에서 클러스터를 설정하는 방법에 대한 지침을 참조하세요. 또한 로컬 및 원격 클러스터가 미리 볼륨 데이터와 통신할 수 있도록 MetroCluster 소프트웨어를 구성하는 데 도움이 됩니다. IP 설정을 통한 MetroCluster 에 대한 특정 정보는 다음을 참조하세요. "[MetroCluster IP 구성 설치](#)".

MetroCluster 구성을 요구 사항과 비교할 수 있습니다. "[MetroCluster 문서](#)" MetroCluster 구성에서 구성 요소를 변경하거나 업그레이드하면 작업 부하 성능이 향상될 수 있는지 확인합니다. 이러한 비교는 다음 질문에 답하는 데 도움이 될 수 있습니다.

- 컨트롤러가 귀하의 작업 부하에 적합합니까?
- 더 많은 처리량을 처리하기 위해 ISL 번들을 더 큰 대역폭으로 업그레이드해야 합니까?
- 스위치의 버퍼 간 크레딧(BBC)을 조정하여 대역폭을 늘릴 수 있나요?
- 워크로드가 SSD(Solid State Drive) 스토리지에 대한 쓰기 처리량이 높은 경우, 처리량을 수용하기 위해 FC-SAS 브리지를 업그레이드해야 합니까?

관련 정보

- MetroCluster 구성 요소를 교체하거나 업그레이드하는 방법에 대한 정보는 다음을 참조하세요. "[MetroCluster 문서](#)".
- 컨트롤러 업그레이드에 대한 정보는 다음을 참조하세요. "[스위치오버 및 스위치백을 사용하여 MetroCluster FC 구성에서 컨트롤러 업그레이드](#)" 그리고 "[스위치오버 및 스위치백을 사용하여 MetroCluster IP 구성에서 컨트롤러 업그레이드](#)".

워크로드를 다른 집계로 이동

Unified Manager를 사용하면 현재 작업 부하가 있는 집계보다 사용량이 적은 집계를 식별한 다음 선택한 볼륨이나 LUN을 해당 집계로 이동할 수 있습니다. 고성능 워크로드를 덜 바쁜 집계나 플래시 스토리지가 활성화된 집계로 옮기면 워크로드를 더 효율적으로 수행할 수 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 현재 성능 문제가 있는 집계의 이름을 기록해 두어야 합니다.
- 집계에서 이벤트를 수신한 날짜와 시간을 기록해야 합니다.
- Unified Manager는 한 달 이상의 성과 데이터를 수집하고 분석해야 합니다.

이러한 단계를 통해 다음 리소스를 식별하여 고성능 워크로드를 활용도가 낮은 집계로 이동할 수 있습니다.

- 동일한 클러스터에서 활용도가 낮은 집계
- 현재 집계에서 가장 높은 성과를 보인 볼륨

단계

1. 클러스터에서 가장 활용도가 낮은 집계를 식별합니다.

- a. 이벤트 세부 정보 페이지에서 집계가 있는 클러스터의 이름을 클릭합니다.

클러스터 세부 정보는 성능/클러스터 랜딩 페이지에 표시됩니다.

- b. 요약 페이지에서 관리되는 개체 창의 *집계*를 클릭합니다.

이 클러스터의 집계 목록이 표시됩니다.

- c. 활용률 열을 클릭하면 활용률이 가장 낮은 순으로 집계가 정렬됩니다.

또한 가장 큰 *여유 용량*을 가진 집계를 식별할 수도 있습니다. 이는 작업 부하를 이동하려는 잠재적인 집계 목록을 제공합니다.

- d. 작업 부하를 이동하려는 집계의 이름을 적어 두세요.

2. 이벤트를 수신한 집계에서 성과가 좋은 볼륨을 식별합니다.

- a. 성능 문제가 있는 집계를 클릭하세요.

집계 세부 정보는 성능/집계 탐색기 페이지에 표시됩니다.

- b. 시간 범위 선택기에서 *지난 30일*을 선택한 다음 *범위 적용*을 클릭합니다.

이를 통해 기본 72시간보다 더 긴 성과 기록 기간을 볼 수 있습니다. 지난 72시간 동안만이 아니라 지속적으로 많은 리소스를 사용하는 볼륨을 이동하려고 합니다.

- c. 보기 및 비교 컨트롤에서 *이 집계의 볼륨*을 선택합니다.

이 집계에 포함된 FlexVol 볼륨과 FlexGroup 구성 볼륨 목록이 표시됩니다.

- d. 가장 높은 성능을 보이는 볼륨을 확인하려면 가장 높은 MB/s 순으로 볼륨을 정렬한 다음 가장 높은 IOPS 순으로 정렬하세요.

- e. 다른 집계로 옮기고 싶은 볼륨의 이름을 적어 두세요.

3. 성과가 좋은 볼륨을 활용도가 낮은 것으로 파악된 집계로 이동합니다.

ONTAP System Manager, OnCommand Workflow Automation, ONTAP 명령 또는 이러한 도구를 조합하여 이동 작업을 수행할 수 있습니다.

며칠 후에 이 노드나 집계에서 동일한 유형의 이벤트를 수신하는지 확인하세요.

워크로드를 다른 노드로 이동

Unified Manager를 사용하면 현재 작업 부하가 실행 중인 노드보다 덜 바쁜 다른 노드의 집계를 식별한 다음 선택한 볼륨을 해당 집계로 이동할 수 있습니다. 고성능 작업 부하를 덜 바쁜 노드에 있는 집계로 옮기면 두 노드의 작업 부하가 더 효율적으로 수행될 수 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 현재 성능 문제가 있는 노드의 이름을 기록해 두어야 합니다.
- 노드가 성능 이벤트를 수신한 날짜와 시간을 기록했어야 합니다.
- Unified Manager는 1개월 이상 성과 데이터를 수집하고 분석해야 합니다.

이 절차를 통해 다음 리소스를 식별하여 고성능 작업 부하를 활용도가 낮은 노드로 이동할 수 있습니다.

- 동일한 클러스터에서 가장 큰 여유 성능 용량을 가진 노드
- 새 노드에서 가장 큰 여유 성능 용량을 가진 집계
- 현재 노드에서 가장 높은 성능을 보이는 볼륨

단계

1. 클러스터에서 가장 큰 여유 성능 용량을 가진 노드를 식별합니다.

- a. 이벤트 세부 정보 페이지에서 노드가 있는 클러스터의 이름을 클릭합니다.

클러스터 세부 정보는 성능/클러스터 랜딩 페이지에 표시됩니다.

- b. 요약 탭에서 관리되는 개체 창의 *노드*를 클릭합니다.

이 클러스터의 노드 목록이 표시됩니다.

- c. 성능 용량 사용 열을 클릭하면 노드가 가장 적게 사용된 순서대로 정렬됩니다.

이는 작업 부하를 이동할 수 있는 잠재적 노드 목록을 제공합니다.

- d. 작업 부하를 이동하려는 노드의 이름을 적어 두세요.

2. 새 노드에서 가장 활용도가 낮은 집계를 식별합니다.

- a. 왼쪽 탐색 창에서 저장소 > 집계*를 클릭하고 보기 메뉴에서 *성능 > *모든 집계*를 선택합니다.

성과: 모든 집계 보기가 표시됩니다.

- b. *필터링*을 클릭하고 왼쪽 드롭다운 메뉴에서 *노드*를 선택한 다음 텍스트 필드에 노드 이름을 입력하고 *필터 적용*을 클릭합니다.

성능: 모든 집계 보기가 이 노드에서 사용할 수 있는 집계 목록과 함께 다시 표시됩니다.

- c. 성능 용량 사용 열을 클릭하여 가장 적게 사용된 항목부터 집계를 정렬합니다.

이는 작업 부하를 이동하려는 잠재적인 집계 목록을 제공합니다.

- d. 작업 부하를 이동하려는 집계의 이름을 적어 두세요.

3. 이벤트를 수신한 노드에서 고성능 워크로드를 식별합니다.

- a. 이벤트의 이벤트 세부 정보 페이지로 돌아가세요.
- b. 영향을 받는 볼륨 필드에서 볼륨 수에 대한 링크를 클릭합니다.

성능: 모든 볼륨 보기에는 해당 노드의 볼륨이 필터링된 목록으로 표시됩니다.

- c. 총 용량 열을 클릭하여 할당된 가장 큰 공간순으로 볼륨을 정렬합니다.

이는 이동하고 싶을 수 있는 잠재적 볼륨 목록을 제공합니다.

- d. 이동하려는 볼륨의 이름과 해당 볼륨이 있는 현재 집계의 이름을 적어 두세요.

- 4. 새 노드에서 가장 큰 여유 성능 용량을 가진 것으로 식별된 집계로 볼륨을 이동합니다.

ONTAP System Manager, OnCommand Workflow Automation, ONTAP 명령 또는 이러한 도구를 조합하여 이동 작업을 수행할 수 있습니다.

며칠 후에 이 노드나 집계에서 동일한 유형의 이벤트를 수신하는지 확인할 수 있습니다.

다른 노드의 집계로 작업 부하 이동

Unified Manager를 사용하면 현재 작업 부하가 실행 중인 노드보다 덜 바쁜 다른 노드의 집계를 식별한 다음 선택한 볼륨을 해당 집계로 이동할 수 있습니다. 고성능 작업 부하를 덜 바쁜 노드에 모아두면 두 노드의 작업 부하가 더 효율적으로 수행될 수 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 현재 성능 문제가 있는 노드의 이름을 기록해 두어야 합니다.
- 노드가 성능 이벤트를 수신한 날짜와 시간을 기록했어야 합니다.
- Unified Manager는 한 달 이상의 성과 데이터를 수집하고 분석해야 합니다.

이러한 단계를 통해 다음 리소스를 식별하여 고성능 워크로드를 활용도가 낮은 노드로 이동할 수 있습니다.

- 동일 클러스터에서 활용도가 낮은 노드
- 새 노드에서 가장 적게 활용되는 집계
- 현재 노드에서 가장 높은 성능을 보이는 볼륨

단계

- 1. 클러스터에서 가장 활용도가 낮은 노드를 식별합니다.
 - a. 이벤트 세부 정보 페이지에서 노드가 있는 클러스터의 이름을 클릭합니다.

클러스터 세부 정보는 성능/클러스터 랜딩 페이지에 표시됩니다.

- b. 요약 페이지에서 관리되는 개체 창의 *노드*를 클릭합니다.

이 클러스터의 노드 목록이 표시됩니다.

- c. 활용률 열을 클릭하면 활용률이 가장 낮은 노드순으로 정렬됩니다.

또한 가장 큰 *여유 용량*을 가진 노드를 식별할 수도 있습니다. 이는 작업 부하를 이동할 수 있는 잠재적 노드 목록을 제공합니다.

d. 작업 부하를 이동하려는 노드의 이름을 적어 두세요.

2. 새 노드에서 가장 활용도가 낮은 집계를 식별합니다.

a. 왼쪽 탐색 창에서 저장소 > 집계*를 클릭하고 보기 메뉴에서 *성능 > *모든 집계*를 선택합니다.

성과: 모든 집계 보기가 표시됩니다.

b. *필터링*을 클릭하고 왼쪽 드롭다운 메뉴에서 *노드*를 선택한 다음 텍스트 필드에 노드 이름을 입력하고 *필터 적용*을 클릭합니다.

성능: 모든 집계 보기가 이 노드에서 사용할 수 있는 집계 목록과 함께 다시 표시됩니다.

c. 활용률 열을 클릭하면 활용률이 가장 낮은 순으로 집계가 정렬됩니다.

또한 가장 큰 *여유 용량*을 가진 집계를 식별할 수도 있습니다. 이는 작업 부하를 이동하려는 잠재적인 집계 목록을 제공합니다.

d. 작업 부하를 이동하려는 집계의 이름을 적어 두세요.

3. 이벤트를 수신한 노드에서 고성능 워크로드를 식별합니다.

a. 이벤트의 이벤트 세부정보 페이지로 돌아가세요.

b. 영향을 받는 볼륨 필드에서 볼륨 수에 대한 링크를 클릭합니다.

성능: 모든 볼륨 보기에는 해당 노드의 볼륨이 필터링된 목록으로 표시됩니다.

c. 총 용량 열을 클릭하여 할당된 가장 큰 공간순으로 볼륨을 정렬합니다.

이는 이동하고 싶을 수 있는 잠재적 볼륨 목록을 제공합니다.

d. 이동하려는 볼륨의 이름과 해당 볼륨이 있는 현재 집계의 이름을 적어 두세요.

4. 새 노드에서 활용도가 낮은 것으로 확인된 집계로 볼륨을 이동합니다.

ONTAP System Manager, OnCommand Workflow Automation, ONTAP 명령 또는 이러한 도구를 조합하여 이동 작업을 수행할 수 있습니다.

며칠 후에 이 노드나 집계에서 동일한 유형의 이벤트를 수신하는지 확인하세요.

다른 HA 쌍의 노드로 작업 부하 이동

Unified Manager를 사용하면 현재 워크로드가 실행 중인 HA 쌍보다 더 많은 여유 성능 용량을 가진 다른 고가용성(HA) 쌍의 노드에서 집계를 식별하는 데 도움이 될 수 있습니다. 그런 다음 선택한 볼륨을 새 HA 쌍의 집계로 이동할 수 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 클러스터는 최소 두 개의 HA 쌍으로 구성되어야 합니다.

클러스터에 HA 쌍이 하나만 있는 경우 이 수정 프로세스를 사용할 수 없습니다.

- 현재 성능 문제가 발생하고 있는 HA 쌍의 두 노드 이름을 기록해 두어야 합니다.
- 노드가 성능 이벤트를 수신한 날짜와 시간을 기록했어야 합니다.
- Unified Manager는 1개월 이상 성과 데이터를 수집하고 분석해야 합니다.

더 많은 여유 성능 용량을 갖춘 노드에 고성능 워크로드를 집계하면 두 노드의 워크로드가 더 효율적으로 수행될 수 있습니다. 이 절차를 통해 다음 리소스를 식별하여 다른 HA 쌍에서 더 많은 여유 성능 용량이 있는 노드로 고성능 워크로드를 이동할 수 있습니다.

- 동일한 클러스터의 다른 HA 쌍에 있는 노드 중 가장 큰 여유 성능 용량을 갖는 노드
- 가장 큰 여유 성능 용량을 가진 새로운 노드의 집계
- 현재 노드에서 가장 높은 성능을 보이는 볼륨

단계

1. 동일한 클러스터의 다른 HA 쌍에 속하는 노드를 식별합니다.
 - a. 이벤트 세부 정보 페이지에서 노드가 있는 클러스터의 이름을 클릭합니다.

클러스터 세부 정보는 성능/클러스터 랜딩 페이지에 표시됩니다.
 - b. 요약 페이지에서 관리되는 개체 창의 *노드*를 클릭합니다.

이 클러스터의 노드 목록은 성능: 모든 노드 보기에 표시됩니다.
 - c. 현재 성능 문제가 있는 HA 쌍과 다른 HA 쌍에 있는 노드의 이름을 적어 두세요.
2. 새로운 HA 쌍에서 가장 큰 여유 성능 용량을 가진 노드를 식별합니다.
 - a. 성능: 모든 노드 보기에서 사용된 성능 용량 열을 클릭하여 사용률이 가장 낮은 순으로 노드를 정렬합니다.

이는 작업 부하를 이동할 수 있는 잠재적 노드 목록을 제공합니다.
 - b. 작업 부하를 이동하려는 다른 HA 쌍의 노드 이름을 적어 두세요.
3. 새 노드에서 가장 큰 여유 성능 용량을 가진 집계를 식별합니다.
 - a. 성능: 모든 노드 보기에서 노드를 클릭합니다.

노드 세부 정보는 성능/노드 탐색기 페이지에 표시됩니다.
 - b. 보기 및 비교 메뉴에서 *이 노드의 집계*를 선택합니다.

이 노드의 집계는 그리드에 표시됩니다.
 - c. 성능 용량 사용 열을 클릭하여 가장 적게 사용된 항목부터 집계를 정렬합니다.

이는 작업 부하를 이동하려는 잠재적인 집계 목록을 제공합니다.
 - d. 작업 부하를 이동하려는 집계의 이름을 적어 두세요.
4. 이벤트를 수신한 노드에서 고성능 워크로드를 식별합니다.
 - a. 이벤트의 이벤트 세부정보 페이지로 돌아가세요.
 - b. 영향을 받는 볼륨 필드에서 첫 번째 노드의 볼륨 수에 대한 링크를 클릭합니다.

성능: 모든 볼륨 보기에는 해당 노드의 볼륨이 필터링된 목록으로 표시됩니다.

- c. 총 용량 열을 클릭하여 할당된 가장 큰 공간순으로 볼륨을 정렬합니다.

이는 이동하고 싶을 수 있는 잠재적 볼륨 목록을 제공합니다.

- d. 이동하려는 볼륨의 이름과 해당 볼륨이 있는 현재 집계의 이름을 적어 두세요.
- e. 이 이벤트에 포함된 두 번째 노드에 대해 4c 및 4d 단계를 수행하여 해당 노드에서 이동하려는 볼륨을 식별합니다.

- 5. 새 노드에서 가장 큰 여유 성능 용량을 가진 것으로 식별된 집계로 볼륨을 이동합니다.

ONTAP System Manager, OnCommand Workflow Automation, ONTAP 명령 또는 이러한 도구를 조합하여 이동 작업을 수행할 수 있습니다.

며칠 후에 이 노드나 집계에서 동일한 유형의 이벤트를 수신하는지 확인할 수 있습니다.

다른 HA 쌍의 다른 노드로 작업 부하 이동

Unified Manager를 사용하면 현재 워크로드가 실행 중인 HA 쌍보다 사용량이 적은 다른 HA 쌍의 노드에서 집계를 식별하는 데 도움이 될 수 있습니다. 그런 다음 선택한 볼륨을 새 HA 쌍의 집계로 이동할 수 있습니다. 고성능 작업 부하를 덜 바쁜 노드에 모아두면 두 노드의 작업 부하가 더 효율적으로 수행될 수 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 클러스터는 최소 두 개의 HA 쌍으로 구성되어야 합니다. 클러스터에 HA 쌍이 하나만 있는 경우 이 수정 프로세스를 사용할 수 없습니다.
- 현재 성능 문제가 발생하고 있는 HA 쌍의 두 노드 이름을 기록했어야 합니다.
- 노드가 성능 이벤트를 수신한 날짜와 시간을 기록했어야 합니다.
- Unified Manager는 한 달 이상의 성과 데이터를 수집하고 분석해야 합니다.

이러한 단계를 수행하면 다음 리소스를 식별하여 고성능 워크로드를 다른 HA 쌍의 활용도가 낮은 노드로 이동할 수 있습니다.

- 동일 클러스터의 다른 HA 쌍에 있는 노드 중 활용도가 낮은 노드
- 가장 적게 활용되는 새 노드의 집계
- 현재 노드에서 가장 높은 성능을 보이는 볼륨

단계

1. 동일한 클러스터의 다른 HA 쌍에 속하는 노드를 식별합니다.
 - a. 왼쪽 탐색 창에서 저장소 > 클러스터*를 클릭하고 보기 메뉴에서 *성능 > *모든 클러스터*를 선택합니다.

성능: 모든 클러스터 보기가 표시됩니다.
 - b. 현재 클러스터의 노드 수 필드에서 숫자를 클릭합니다.

성능: 모든 노드 보기가 표시됩니다.

c. 현재 성능 문제가 있는 HA 쌍과 다른 HA 쌍에 있는 노드의 이름을 적어 두세요.

2. 새로운 HA 쌍에서 가장 활용도가 낮은 노드를 식별합니다.

a. 활용률 열을 클릭하면 활용률이 가장 낮은 노드순으로 정렬됩니다.

또한 가장 큰 *여유 용량*을 가진 노드를 식별할 수도 있습니다. 이는 작업 부하를 이동할 수 있는 잠재적 노드 목록을 제공합니다.

b. 작업 부하를 이동하려는 노드의 이름을 적어 두세요.

3. 새 노드에서 가장 활용도가 낮은 집계를 식별합니다.

a. 왼쪽 탐색 창에서 저장소 > 집계*를 클릭하고 보기 메뉴에서 *성능 > *모든 집계*를 선택합니다.

성과: 모든 집계 보기가 표시됩니다.

b. *필터링*을 클릭하고 왼쪽 드롭다운 메뉴에서 *노드*를 선택한 다음 텍스트 필드에 노드 이름을 입력하고 *필터 적용*을 클릭합니다.

성능: 모든 집계 보기가 이 노드에서 사용할 수 있는 집계 목록과 함께 다시 표시됩니다.

c. 활용률 열을 클릭하면 활용률이 가장 낮은 순으로 집계가 정렬됩니다.

또한 가장 큰 *여유 용량*을 가진 집계를 식별할 수도 있습니다. 이는 작업 부하를 이동하려는 잠재적인 집계 목록을 제공합니다.

d. 작업 부하를 이동하려는 집계의 이름을 적어 두세요.

4. 이벤트를 수신한 노드에서 고성능 워크로드를 식별합니다.

a. 이벤트의 이벤트 세부정보 페이지로 돌아가세요.

b. 영향을 받는 볼륨 필드에서 첫 번째 노드의 볼륨 수에 대한 링크를 클릭합니다.

성능: 모든 볼륨 보기에는 해당 노드의 볼륨이 필터링된 목록으로 표시됩니다.

c. 총 용량 열을 클릭하여 할당된 가장 큰 공간순으로 볼륨을 정렬합니다.

이는 이동하고 싶을 수 있는 잠재적 볼륨 목록을 제공합니다.

d. 이동하려는 볼륨의 이름과 해당 볼륨이 있는 현재 집계의 이름을 적어 두세요.

e. 이 이벤트에 포함된 두 번째 노드에 대해 4c 및 4d 단계를 수행하여 해당 노드에서 이동하려는 볼륨을 식별합니다.

5. 새 노드에서 활용도가 낮은 것으로 확인된 집계로 볼륨을 이동합니다.

ONTAP System Manager, OnCommand Workflow Automation, ONTAP 명령 또는 이러한 도구를 조합하여 이동 작업을 수행할 수 있습니다.

며칠 후에 이 노드나 집계에서 동일한 유형의 이벤트를 수신하는지 확인하세요.

QoS 정책 설정을 사용하여 이 노드의 작업 우선 순위를 지정합니다.

QoS 정책 그룹에 제한을 설정하여 해당 그룹에 포함된 작업 부하에 대한 초당 I/O(IOPS) 또는 MBps 처리량 제한을 제어할 수 있습니다. 워크로드가 기본 정책 그룹과 같이 설정된 제한이 없는 정책 그룹에 있는 경우 또는 설정된 제한이 요구 사항을 충족하지 못하는 경우 설정된 제한을 늘리거나 원하는 제한이 있는 새 정책 그룹이나 기존 정책 그룹으로 워크로드를 이동할 수 있습니다.

노드의 성능 이벤트가 노드 리소스를 과도하게 사용하는 작업 부하로 인해 발생한 경우, 이벤트 세부 정보 페이지의 이벤트 설명에 관련 볼륨 목록에 대한 링크가 표시됩니다. 성능/볼륨 페이지에서 영향을 받은 볼륨을 IOPS 및 MBps별로 정렬하여 이벤트에 영향을 미쳤을 수 있는 가장 높은 사용량을 가진 워크로드를 확인할 수 있습니다.

노드 리소스를 과도하게 사용하는 볼륨을 보다 제한적인 정책 그룹 설정에 할당하면 정책 그룹이 작업 부하를 조절하여 활동을 제한하고, 이를 통해 해당 노드의 리소스 사용을 줄일 수 있습니다.

ONTAP 시스템 관리자나 ONTAP 명령을 사용하여 다음 작업을 포함하여 정책 그룹을 관리할 수 있습니다.

- 정책 그룹 생성
- 정책 그룹에서 작업 부하 추가 또는 제거
- 정책 그룹 간 작업 부하 이동
- 정책 그룹의 처리량 제한 변경

비활성 볼륨 및 LUN 제거

집계된 여유 공간이 문제로 식별되면 사용되지 않는 볼륨과 LUN을 검색하여 집계에서 삭제할 수 있습니다. 이렇게 하면 디스크 공간 부족 문제를 완화하는 데 도움이 될 수 있습니다.

집계에서 성능 이벤트가 디스크 공간 부족으로 인해 발생한 경우, 더 이상 사용되지 않는 볼륨과 LUN을 확인할 수 있는 몇 가지 방법이 있습니다.

사용되지 않는 볼륨을 식별하려면:

- 이벤트 세부 정보 페이지에서 영향을 받은 개체 수 필드는 영향을 받은 볼륨 목록을 표시하는 링크를 제공합니다.

링크를 클릭하면 성능: 모든 볼륨 보기에서 볼륨이 표시됩니다. 여기에서 영향을 받은 볼륨을 *IOPS*별로 정렬하여 어떤 볼륨이 활성화되지 않았는지 확인할 수 있습니다.

사용되지 않는 LUN을 식별하려면:

1. 이벤트 세부 정보 페이지에서 이벤트가 발생한 집계의 이름을 적어 두세요.
2. 왼쪽 탐색 창에서 저장소 > **LUN***을 클릭하고 보기 메뉴에서 *성능 > *모든 LUN*을 선택합니다.
3. *필터링*을 클릭하고 왼쪽 드롭다운 메뉴에서 *집계*를 선택한 다음, 텍스트 필드에 집계 이름을 입력하고 *필터 적용*을 클릭합니다.
4. 영향을 받은 LUN의 결과 목록을 *IOPS*별로 정렬하여 활성화되지 않은 LUN을 확인합니다.

사용되지 않는 볼륨과 LUN을 식별한 후에는 ONTAP 시스템 관리자나 ONTAP 명령을 사용하여 해당 객체를 삭제할 수 있습니다.

디스크를 추가하고 집계 레이아웃 재구성을 수행합니다.

집계에 디스크를 추가하여 저장 용량과 해당 집계의 성능을 높일 수 있습니다. 디스크를 추가한 후 집계를 재구성한 후에야 성능이 향상되는 것을 확인할 수 있습니다.

이벤트 세부 정보 페이지에서 시스템 정의 임계값 이벤트를 받으면 이벤트 설명 텍스트에 문제가 있는 집계의 이름이 나열됩니다. 이 집계에 디스크를 추가하고 데이터를 재구성할 수 있습니다.

집계에 추가하는 디스크는 이미 클러스터에 존재해야 합니다. 클러스터에 사용 가능한 추가 디스크가 없는 경우 관리자에게 문의하거나 추가 디스크를 구매해야 할 수도 있습니다. ONTAP 시스템 관리자나 ONTAP 명령을 사용하여 디스크를 집계에 추가할 수 있습니다.

["기술 보고서 3838: 스토리지 하위 시스템 구성 가이드"](#)

Unified Manager 서버와 외부 데이터 공급자 간의 연결 설정

Unified Manager 서버와 외부 데이터 공급자 간의 연결을 통해 클러스터 성능 데이터를 외부 서버로 전송할 수 있으므로 스토리지 관리자가 타사 소프트웨어를 사용하여 성능 지표를 차트로 작성할 수 있습니다.

Unified Manager 서버와 외부 데이터 공급자 간의 연결은 유지 관리 콘솔의 "외부 데이터 공급자"라는 메뉴 옵션을 통해 설정됩니다.

외부 서버로 전송할 수 있는 성능 데이터

Unified Manager는 모니터링하는 모든 클러스터에서 다양한 성능 데이터를 수집합니다. 특정 데이터 그룹을 외부 서버로 보낼 수 있습니다.

차트로 작성하려는 성과 데이터에 따라 다음 통계 그룹 중 하나를 선택하여 보낼 수 있습니다.

통계 그룹	포함된 데이터	세부
성능 모니터	다음 개체에 대한 고급 성능 통계: • LUN • 볼륨	이 그룹은 모니터링되는 모든 클러스터의 모든 LUN과 볼륨에 대한 총 IOPS 또는 대기 시간을 제공합니다. 이 그룹은 가장 적은 수의 통계를 제공합니다.
자원 활용	다음 개체에 대한 리소스 활용 통계: • 노드 • 골재	이 그룹은 모니터링되는 모든 클러스터의 노드와 물리적 리소스에 대한 활용 통계를 제공합니다. 또한 성능 모니터 그룹에서 수집된 통계도 제공합니다.

통계 그룹	포함된 데이터	세부
드릴 다운	추적된 모든 개체에 대한 저수준 읽기/쓰기 및 프로토콜별 통계: • 노드 • 골재 • LUN • 볼륨 • 디스크 • LIFs • 포트/NIC	이 그룹은 모니터링되는 모든 클러스터의 추적된 7개 객체 유형에 대한 읽기/쓰기 및 프로토콜별 분석을 제공합니다. 또한 성능 모니터 그룹과 리소스 활용도 그룹에서 수집된 통계도 제공합니다. 이 그룹은 가장 많은 통계를 제공합니다.



스토리지 시스템에서 클러스터 또는 클러스터 개체의 이름이 변경되면 이전 개체와 새 개체 모두 외부 서버의 성능 데이터(`metric\_path`라고 함)를 포함하게 됩니다. 두 객체는 동일한 객체로 연관되지 않습니다. 예를 들어, 볼륨의 이름을 "volume1_acct"에서 "acct_vol1"로 변경하면 이전 볼륨의 이전 성능 데이터와 새 볼륨의 새 성능 데이터가 표시됩니다.

외부 데이터 공급자에게 전송할 수 있는 모든 성능 카운터 목록은 기술 자료 문서 30096을 참조하세요.

"외부 데이터 공급자로 내보낼 수 있는 Unified Manager 성능 카운터"

Unified Manager에서 성능 데이터를 수신하도록 **Graphite**를 설정합니다.

Graphite는 컴퓨터 시스템의 성능 데이터를 수집하고 그래프로 표현하는 개방형 소프트웨어 도구입니다. Unified Manager에서 통계 데이터를 받으려면 Graphite 서버와 소프트웨어를 올바르게 구성해야 합니다.

NetApp Graphite나 다른 타사 도구의 특정 버전을 테스트하거나 검증하지 않습니다.



Graphite 서버는 Unified Manager에서 볼륨에 대한 성능 데이터를 받지 않습니다.

설치 지침에 따라 Graphite를 설치한 후 Unified Manager에서 통계 데이터 전송을 지원하려면 다음과 같이 변경해야 합니다.

- 에서 `/opt/graphite/conf/carbon.conf` 파일, 분당 Graphite 서버에서 생성할 수 있는 최대 파일 수는 `_200_`으로 설정해야 합니다. (`MAX_CREATES_PER_MINUTE = 200`).

구성에 포함된 클러스터 수와 전송하기로 선택한 통계 개체에 따라 처음에 만들어야 할 새 파일이 수천 개일 수 있습니다. 분당 200개의 파일을 처리하는 경우 모든 메트릭 파일이 처음 생성되기까지 15분 이상 걸릴 수 있습니다. 모든 고유한 메트릭 파일이 생성된 후에는 이 매개변수가 더 이상 관련이 없습니다.

- IPv6 주소를 사용하여 배포된 서버에서 Graphite를 실행하는 경우 `LINE_RECEIVER_INTERFACE`의 값은 `/opt/graphite/conf/carbon.conf` 파일을 "0.0.0.0"에서 ":::"로 변경해야 합니다. (`LINE_RECEIVER_INTERFACE = :::`)
- 에서 `/opt/graphite/conf/storage-schemas.conf` 파일, `retentions` 매개변수를 사용하여 빈도를

5분으로 설정하고 보존 기간을 환경에 적합한 일수로 설정해야 합니다.

보존 기간은 환경이 허용하는 한 길게 설정할 수 있지만, 적어도 하나의 보존 설정에 대해 빈도 값은 5분으로 설정해야 합니다. 다음 예에서는 Unified Manager에 대한 섹션이 다음을 사용하여 정의됩니다. `pattern` 매개변수와 값은 초기 빈도를 5분으로, 보존 기간을 100일로 설정합니다. [OPM]

```
pattern = ^netapp-performance\..
```

```
retentions = 5m:100d
```



기본 공급업체 태그가 `netapp-performance`에서 다른 것으로 변경된 경우 해당 변경 사항은 다음에 반영되어야 합니다. `pattern` 매개변수도 마찬가지로입니다.



Unified Manager 서버가 성능 데이터를 보내려고 할 때 Graphite 서버를 사용할 수 없는 경우 데이터가 전송되지 않고 수집된 데이터에 공백이 발생합니다.

Unified Manager 서버에서 외부 데이터 공급자로의 연결 구성

Unified Manager는 클러스터 성능 데이터를 외부 서버로 전송할 수 있습니다. 전송되는 통계 데이터의 유형과 데이터를 전송하는 간격을 지정할 수 있습니다.

시작하기 전에

- Unified Manager 서버의 유지 관리 콘솔에 로그인하려면 권한이 있는 사용자 ID가 있어야 합니다.
- 외부 데이터 공급자에 대한 다음 정보가 있어야 합니다.
 - 서버 이름 또는 IP 주소(IPv4 또는 IPv6)
 - 서버 기본 포트(기본 포트 2003을 사용하지 않는 경우)
- Unified Manager 서버에서 통계 데이터를 수신할 수 있도록 원격 서버와 타사 소프트웨어를 구성해야 합니다.
- 어떤 통계 그룹을 보내고 싶은지 알아야 합니다.
 - PERFORMANCE_INDICATOR: 성능 모니터 통계
 - RESOURCE_UTILIZATION: 리소스 활용도 및 성능 모니터 통계
 - DRILL_DOWN: 모든 통계
- 통계를 전송하려는 시간 간격을 알아야 합니다: 5분, 10분 또는 15분

기본적으로 Unified Manager는 5분 간격으로 통계를 수집합니다. 전송 간격을 10분(또는 15분)으로 설정하면 각 전송 동안 전송되는 데이터 양은 기본 5분 간격을 사용할 때보다 2배(또는 3배) 더 많아집니다.



Unified Manager 성능 수집 간격을 10분 또는 15분으로 변경하는 경우 전송 간격도 Unified Manager 수집 간격과 같거나 더 크게 변경해야 합니다.

하나의 Unified Manager 서버와 하나의 외부 데이터 공급자 서버 간의 연결을 구성할 수 있습니다.

단계

1. Unified Manager 서버의 유지 관리 콘솔에 유지 관리 사용자로 로그인합니다.

Unified Manager 유지 관리 콘솔 프롬프트가 표시됩니다.

2. 유지 관리 콘솔에서 외부 데이터 공급자 메뉴 옵션의 번호를 입력합니다.

외부 서버 연결 메뉴가 표시됩니다.

3. 서버 연결 추가/수정 메뉴 옵션의 번호를 입력하세요.

현재 서버 연결 정보가 표시됩니다.

4. 메시지가 표시되면 다음을 입력하십시오. **y** 계속하려면.

5. 메시지가 표시되면 대상 서버의 IP 주소 또는 이름과 서버 포트 정보(기본 포트 2003과 다른 경우)를 입력합니다.

6. 메시지가 표시되면 다음을 입력하십시오. **y** 입력한 정보가 정확한지 확인하세요.

7. 외부 서버 연결 메뉴로 돌아가려면 아무 키나 누르세요.

8. 서버 구성 수정 메뉴 옵션의 번호를 입력하세요.

현재 서버 구성 정보가 표시됩니다.

9. 메시지가 표시되면 다음을 입력하십시오. **y** 계속하려면.

10. 메시지가 표시되면 보낼 통계 유형, 통계를 보낼 시간 간격, 지금 통계 전송을 활성화할지 여부를 입력합니다.

을 위한..	입력하다...
통계 그룹 ID	0- 성능 지표(기본값) 1- 리소스 활용 2- 드릴다운
공급업체 태그	외부 서버에서 통계가 저장될 폴더에 대한 설명적 이름입니다. 기본 이름은 "netapp-performance"이지만 다른 값을 입력할 수 있습니다. 점 표기법을 사용하면 계층적 폴더 구조를 정의할 수 있습니다. 예를 들어, 다음을 입력하여 stats.performance.netapp 통계는 통계 > 성능 > *netapp*에서 확인할 수 있습니다.
전송 간격	5(기본), 10 , 또는 15 분
활성화/비활성화	0- 장애를 입히다 1- 활성화(기본값)

11. 메시지가 표시되면 다음을 입력하십시오. **y** 입력한 정보가 정확한지 확인하세요.

12. 외부 서버 연결 메뉴로 돌아가려면 아무 키나 누르세요.

13. 유형 **x** 유지 관리 콘솔을 종료합니다.

연결을 구성한 후, 선택한 성능 데이터가 지정한 시간 간격으로 대상 서버로 전송됩니다. 외부 도구에 지표가 나타나기까지는 몇 분이 걸립니다. 지표 계층 구조에서 새로운 지표를 보려면 브라우저를 새로 고쳐야 할 수도 있습니다.

클러스터 상태 모니터링 및 관리

Active IQ Unified Manager 상태 모니터링 소개

Active IQ Unified Manager (이전 OnCommand Unified Manager)를 사용하면 중앙 사용자 인터페이스를 통해 ONTAP 소프트웨어를 실행하는 많은 수의 시스템을 모니터링할 수 있습니다. Unified Manager 서버 인프라는 확장성, 지원성, 향상된 모니터링 및 알림 기능을 제공합니다.

Unified Manager의 주요 기능으로는 모니터링, 알림, 클러스터 가용성 및 용량 관리, 보호 기능 관리, 진단 데이터 번들링 및 기술 지원팀으로 전송 등이 있습니다.

Unified Manager를 사용하여 클러스터를 모니터링할 수 있습니다. 클러스터에서 문제가 발생하면 Unified Manager는 이벤트를 통해 해당 문제의 세부 정보를 알려줍니다. 일부 이벤트에서는 문제를 바로잡는 데 필요한 시정 조치도 제공합니다. 문제가 발생하면 이메일과 SNMP 트랩을 통해 알림을 받을 수 있도록 이벤트에 대한 알림을 구성할 수 있습니다.

Unified Manager를 사용하면 주석과 연결하여 환경의 스토리지 객체를 관리할 수 있습니다. 사용자 정의 주석을 만들고 규칙을 통해 클러스터, 스토리지 가상 머신(SVM), 볼륨을 주석과 동적으로 연결할 수 있습니다.

각 클러스터 개체에 대한 용량 및 상태 차트에 제공된 정보를 사용하여 클러스터 개체의 저장 요구 사항을 계획할 수도 있습니다.

물리적 및 논리적 용량

Unified Manager는 ONTAP 스토리지 객체에 사용되는 물리적 공간과 논리적 공간의 개념을 활용합니다.

- 물리적 용량: 물리적 공간은 볼륨에 사용되는 물리적 저장 블록을 말합니다. "물리적 사용 용량"은 일반적으로 저장 효율성 기능(중복 제거 및 압축 등)으로 인한 데이터 감소로 인해 논리적 사용 용량보다 작습니다.
- 논리적 용량: 논리적 공간은 볼륨에서 사용 가능한 공간(논리적 블록)을 의미합니다. 논리적 공간은 중복 제거나 압축 결과를 고려하지 않고 이론적 공간을 어떻게 사용할 수 있는지를 나타냅니다. "사용된 논리적 공간"은 사용된 물리적 공간과 구성된 저장 효율성 기능(중복 제거 및 압축 등)을 통해 절감된 공간을 합친 것입니다. 이 측정값은 실제 사용 용량보다 크게 나타나는 경우가 많은데, 이는 여기에는 데이터 압축 및 기타 물리적 공간의 감소가 반영되지 않기 때문입니다. 따라서 총 논리적 용량은 제공된 공간보다 높을 수 있습니다.

용량 측정 단위

Unified Manager는 1024(2^{10})바이트의 이진 단위를 기준으로 저장 용량을 계산합니다. ONTAP 9.10.0 및 이전 버전에서는 이러한 단위가 KB, MB, GB, TB, PB로 표시되었습니다. ONTAP 9.10.1부터 Unified Manager에서는 KiB, MiB, GiB, TiB, PiB로 표시됩니다.



ONTAP의 모든 릴리스에서 처리량에 사용되는 단위는 초당 킬로바이트(Kbps), 초당 메가바이트(Mbps), 초당 기가바이트(Gbps), 초당 테라바이트(Tbps) 등으로 계속 사용됩니다.

ONTAP 9.10.0 및 이전 버전의 Unified Manager에 표시되는 용량 단위	ONTAP 9.10.1용 Unified Manager에 표시되는 용량 단위	계산	바이트 단위의 값
KB	키비	1024	1024바이트

ONTAP 9.10.0 및 이전 버전의 Unified Manager에 표시되는 용량 단위	ONTAP 9.10.1용 Unified Manager에 표시되는 용량 단위	계산	바이트 단위의 값
엠비	미비	1024 * 1024	1,048,576바이트
영국	수코양이	1024 * 1024 * 1024	1,073,741,824바이트
결핵	티비	1024 * 1024 * 1024 * 1024	1,099,511,627,776바이트

Unified Manager 상태 모니터링 기능

Unified Manager는 확장성, 지원성, 향상된 모니터링 및 알림 기능을 제공하는 서버 인프라를 기반으로 구축되었습니다. Unified Manager는 ONTAP 소프트웨어를 실행하는 시스템의 모니터링을 지원합니다.

Unified Manager에는 다음과 같은 기능이 포함되어 있습니다.

- ONTAP 소프트웨어가 설치된 시스템에 대한 검색, 모니터링 및 알림:
 - 물리적 객체: 노드, 디스크, 디스크 셀프, SFO 쌍, 포트 및 플래시 캐시
 - 논리적 개체: 클러스터, 스토리지 가상 머신(SVM), 집계, 볼륨, LUN, 네임스페이스, qtree, LIF, 스냅샷 복사본, 연결 경로, NFS 공유, SMB 공유, 사용자 및 그룹 할당량, QoS 정책 그룹, 개시자 그룹
 - 프로토콜: CIFS, NFS, FC, iSCSI, NVMe 및 FCoE
 - 스토리지 효율성: SSD 집계, Flash Pool 집계, FabricPool 집계, 중복 제거 및 압축
 - 보호: SnapMirror 관계(동기 및 비동기) 및 SnapVault 관계
- 클러스터 검색 및 모니터링 상태 보기
- FC 및 IP 구성을 통한 MetroCluster : 클러스터 구성 요소의 구성, 문제 및 연결 상태를 보고 모니터링합니다. FC 구성을 통한 MetroCluster 위한 MetroCluster 스위치 및 브리지
- 향상된 경고, 이벤트 및 임계값 인프라
- LDAP, LDAPS, SAML 인증 및 로컬 사용자 지원
- RBAC(사전 정의된 역할 집합용)
- AutoSupport 및 지원 번들
- 환경의 용량, 가용성, 보호 및 성능 상태를 보여주는 향상된 대시보드
- 볼륨 이동 상호 운용성, 볼륨 이동 기록 및 집합 경로 변경 기록
- 일부 디스크 실패, MetroCluster 집계 미러링 저하, MetroCluster 예비 디스크 남음 이벤트와 같은 이벤트에 영향을 받는 리소스를 그래픽으로 표시하는 영향 범위 영역
- MetroCluster 이벤트의 효과를 표시하는 가능한 효과 영역
- 일부 디스크 실패, MetroCluster 집계 미러링 저하, MetroCluster 예비 디스크 남음 이벤트와 같은 이벤트를 해결하기 위해 수행할 수 있는 작업을 표시하는 제안된 시정 조치 영역
- 볼륨 오프라인 이벤트, 볼륨 제한 이벤트, 썸 프로비저닝 볼륨 공간 위험 이벤트와 같은 이벤트에 영향을 받을 수

있는 리소스를 표시하는 영향을 받을 수 있는 리소스 영역

- FlexVol 또는 FlexGroup 볼륨이 있는 SVM 지원
- 노드 루트 볼륨 모니터링 지원
- 회수 가능한 공간 계산 및 스냅샷 복사본 삭제를 포함한 향상된 스냅샷 복사본 모니터링
- 저장소 객체에 대한 주석
- 물리적 및 논리적 용량, 활용도, 공간 절약, 성능 및 관련 이벤트와 같은 스토리지 객체 정보의 보고서 생성 및 관리
- OnCommand Workflow Automation 과 통합하여 워크플로 실행

Storage Automation Store에는 OnCommand Workflow Automation (WFA)과 함께 사용하도록 개발된 NetApp 인증 자동화 스토리지 워크플로 팩이 포함되어 있습니다. 팩을 다운로드한 후 WFA로 가져와서 실행할 수 있습니다. 자동화된 워크플로는 여기에서 사용할 수 있습니다.

"스토리지 자동화 스토어"

스토리지 시스템 상태를 관리하는 데 사용되는 **Unified Manager** 인터페이스

이 섹션에는 Active IQ Unified Manager 데이터 저장 용량, 가용성 및 보호 문제를 해결하기 위해 제공하는 두 가지 사용자 인터페이스에 대한 정보가 포함되어 있습니다. 두 가지 UI는 Unified Manager 웹 UI와 유지 관리 콘솔입니다.

Unified Manager의 보호 기능을 사용하려면 OnCommand Workflow Automation (WFA)도 설치하고 구성해야 합니다.

Unified Manager 웹 UI

Unified Manager 웹 UI를 사용하면 관리자가 데이터 저장 용량, 가용성 및 보호와 관련된 클러스터 문제를 모니터링하고 문제를 해결할 수 있습니다.

이 섹션에서는 관리자가 Unified Manager 웹 UI에 표시되는 스토리지 용량, 데이터 가용성 또는 보호 문제를 해결하기 위해 따를 수 있는 몇 가지 일반적인 워크플로를 설명합니다.

유지 관리 콘솔

Unified Manager 유지 관리 콘솔을 사용하면 관리자는 Unified Manager 서버 자체와 관련된 운영 체제 문제, 버전 업그레이드 문제, 사용자 액세스 문제 및 네트워크 문제를 모니터링, 진단 및 해결할 수 있습니다. Unified Manager 웹 UI를 사용할 수 없는 경우 유지 관리 콘솔을 통해서만 Unified Manager에 액세스할 수 있습니다.

이 정보를 사용하여 유지 관리 콘솔에 액세스하고 Unified Manager 서버 작동과 관련된 문제를 해결할 수 있습니다.

클러스터 및 클러스터 개체 상태 관리 및 모니터링

Unified Manager는 주기적 API 쿼리와 데이터 수집 엔진을 사용하여 클러스터에서 데이터를 수집합니다. Unified Manager 데이터베이스에 클러스터를 추가하면 이러한 클러스터의 가용성 및 용량 위험을 모니터링하고 관리할 수 있습니다.

클러스터 모니터링 이해하기

Unified Manager 데이터베이스에 클러스터를 추가하여 CPU 사용률, 인터페이스 통계, 여유 디스크 공간, Qtree 사용률, 새시 환경 등의 가용성, 용량 및 기타 세부 정보를 모니터링할 수 있습니다.

상태가 비정상적이거나 사전 정의된 임계값을 초과하면 이벤트가 생성됩니다. 이렇게 구성된 경우 Unified Manager는 이벤트로 인해 경고가 발생할 때 지정된 수신자에게 알림을 보냅니다.

노드 루트 볼륨 이해

Unified Manager를 사용하여 노드 루트 볼륨을 모니터링할 수 있습니다. 가장 좋은 방법은 노드 루트 볼륨에 노드가 다운되는 것을 방지할 만큼 충분한 용량이 있어야 한다는 것입니다.

노드 루트 볼륨의 사용된 용량이 전체 노드 루트 볼륨 용량의 80%를 초과하면 노드 루트 볼륨 공간이 거의 가득 찼습니다 이벤트가 생성됩니다. 이벤트에 대한 알림을 구성하여 알림을 받을 수 있습니다. ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 노드가 다운되는 것을 방지하기 위한 적절한 조치를 취할 수 있습니다.



클러스터가 ONTAP 9.14.1 버전 이상을 실행하는 경우 노드 루트 볼륨 모니터링 기능을 사용할 수 없습니다.

노드 루트 집계에 대한 이벤트 및 임계값 이해

Unified Manager를 사용하여 노드 루트 집계를 모니터링할 수 있습니다. 노드가 중단되는 것을 방지하기 위해 루트 집계에서 루트 볼륨을 두껍게 프로비저닝하는 것이 가장 좋은 방법입니다.

기본적으로 루트 집계에 대한 용량 및 성능 이벤트는 생성되지 않습니다. 또한 Unified Manager에서 사용하는 임계값은 노드 루트 집계에 적용할 수 없습니다. 이러한 이벤트 생성에 대한 설정을 수정할 수 있는 사람은 기술 지원 담당자뿐입니다. 기술 지원 담당자가 설정을 수정하면 용량 임계값이 노드 루트 집계에 적용됩니다.

ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 노드가 중단되는 것을 방지하기 위한 적절한 조치를 취할 수 있습니다.



클러스터가 ONTAP 9.14.1 버전 이상을 실행하는 경우 노드 루트 집계 모니터링 기능을 사용할 수 없습니다.

정족수와 엡실론을 이해하세요

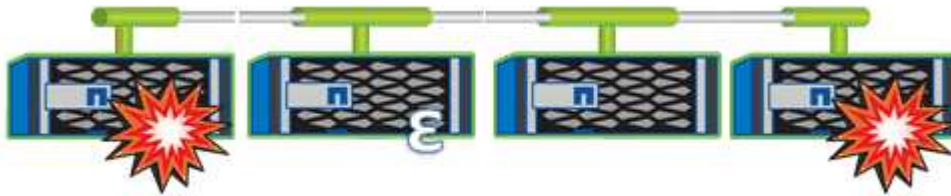
쿼럼과 엡실론은 클러스터의 상태와 기능을 측정하는 중요한 척도이며, 이를 통해 클러스터가 잠재적인 통신 및 연결 문제를 어떻게 해결하는지 알 수 있습니다.

쿼럼은 클러스터가 완벽하게 기능하기 위한 전제 조건입니다. 클러스터가 쿼럼에 속하면 노드의 과반수가 정상적이며 서로 통신할 수 있습니다. 쿼럼이 손실되면 클러스터는 정상적인 클러스터 작업을 수행할 수 없게 됩니다. 모든 노드가 집합적으로 데이터에 대한 단일 뷰를 공유하기 때문에 한 번에 하나의 노드 컬렉션만 쿼럼을 가질 수 있습니다. 따라서 통신하지 않는 두 노드가 서로 다른 방식으로 데이터를 수정하도록 허용되면 더 이상 데이터를 단일 데이터 뷰로 조정할 수 없습니다.

클러스터의 각 노드는 하나의 노드 마스터를 선출하는 투표 프로토콜에 참여합니다. 나머지 노드는 모두 보조 노드입니다. 마스터 노드는 클러스터 전체에서 정보를 동기화하는 역할을 합니다. 정족수가 형성되면 지속적인 투표를

통해 유지됩니다. 마스터 노드가 오프라인이 되고 클러스터가 여전히 퀴럼에 있는 경우 온라인 상태를 유지하는 노드에 의해 새 마스터가 선출됩니다.

짝수의 노드가 있는 클러스터에서는 동점이 발생할 가능성이 있으므로, 한 노드는 엡실론이라는 추가적인 분수 투표 가중치를 갖습니다. 대규모 클러스터의 두 개의 동일한 부분 사이의 연결이 끊어지면 epsilon을 포함하는 노드 그룹은 모든 노드가 정상이라고 가정하고 퀴럼을 유지합니다. 예를 들어, 다음 그림은 두 개의 노드에 장애가 발생한 4개 노드 클러스터를 보여줍니다. 그러나 살아남은 노드 중 하나가 엡실론을 보유하고 있기 때문에 건강한 노드의 단순 과반수가 없더라도 클러스터는 정족수를 유지합니다.



클러스터가 생성되면 Epsilon이 자동으로 첫 번째 노드에 할당됩니다. 엡실론을 보유한 노드가 비정상 상태가 되거나, 고가용성 파트너를 인수하거나, 고가용성 파트너에게 인수되는 경우, 엡실론은 다른 HA 쌍의 정상 노드에 자동으로 재할당됩니다.

노드를 오프라인으로 전환하면 클러스터가 퀴럼에 남는 능력에 영향을 미칠 수 있습니다. 따라서 ONTAP 클러스터를 퀴럼에서 제외하거나 퀴럼 손실 직전까지 클러스터를 중단시키는 작업을 시도하는 경우 경고 메시지를 발행합니다. 고급 권한 수준에서 cluster quorum-service options modify 명령을 사용하여 퀴럼 경고 메시지를 비활성화할 수 있습니다.

일반적으로 클러스터 노드 간에 안정적인 연결이 있다고 가정하면, 더 큰 클러스터가 더 작은 클러스터보다 더 안정적입니다. 24개 노드로 구성된 클러스터에서는 절반의 노드와 엡실론의 단순 과반수라는 정족수 요건을 유지하는 것이 2개 노드로 구성된 클러스터보다 쉽습니다.

2노드 클러스터는 퀴럼을 유지하는 데 있어 몇 가지 고유한 과제를 안고 있습니다. 2노드 클러스터는 클러스터 HA를 사용하는데, 여기서는 어느 노드도 엡실론을 보유하지 않습니다. 대신 두 노드가 지속적으로 폴링되어 한 노드가 실패하더라도 다른 노드가 데이터에 대한 전체 읽기-쓰기 액세스 권한과 논리적 인터페이스 및 관리 기능에 대한 액세스 권한을 갖도록 보장합니다.

클러스터 목록 및 세부 정보 보기

상태: 모든 클러스터 보기를 사용하면 클러스터 인벤토리를 볼 수 있습니다. 용량: 모든 클러스터 보기를 사용하면 모든 클러스터의 저장 용량과 활용도에 대한 요약 정보를 볼 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

클러스터/상태 세부 정보 페이지를 사용하면 클러스터 상태, 용량, 구성, LIF, 노드, 클러스터 내 디스크 등 개별 클러스터에 대한 세부 정보를 볼 수도 있습니다.

상태: 모든 클러스터 보기, 용량: 모든 클러스터 보기 및 클러스터/상태 세부 정보 페이지의 세부 정보는 스토리지를 계획하는 데 도움이 됩니다. 예를 들어, 새로운 집계를 프로비저닝하기 전에 상태: 모든 클러스터 보기에서 특정 클러스터를 선택하고 용량 세부 정보를 얻어 클러스터에 필요한 공간이 있는지 확인할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *클러스터*를 클릭합니다.
2. 보기 메뉴에서 상태: 모든 클러스터 보기를 선택하여 상태 정보를 보거나, 용량: 모든 클러스터 보기를 선택하여

모든 클러스터의 저장 용량 및 활용도에 대한 세부 정보를 봅니다.

- 클러스터 이름을 클릭하면 클러스터/상태 세부 정보 페이지에서 클러스터의 전체 세부 정보를 볼 수 있습니다.

관련 정보

- ["클러스터/상태 세부 정보 페이지"](#)
- ["성능: 모든 클러스터 보기"](#)
- ["MetroCluster 구성 모니터링"](#)
- ["클러스터 및 스토리지 VM의 보안 상태 보기"](#)
- ["어떤 보안 기준이 평가되고 있습니까?"](#)

MetroCluster 구성에서 클러스터의 상태를 확인합니다.

Active IQ Unified Manager (Unified Manager)를 사용하면 MetroCluster over FC 및 MetroCluster over IP 구성에서 클러스터와 해당 구성 요소의 운영 상태를 확인할 수 있습니다. Unified Manager에서 감지한 성능 이벤트에 클러스터가 관련된 경우 상태를 통해 하드웨어 또는 소프트웨어 문제가 이벤트에 영향을 미쳤는지 여부를 확인하는 데 도움이 될 수 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- MetroCluster 구성에 대한 성능 이벤트를 분석하고 관련 클러스터의 이름을 얻었을 것입니다.
- FC 및 IP를 통한 MetroCluster 구성의 두 클러스터는 모두 동일한 Unified Manager 인스턴스에서 모니터링되어야 합니다.

FC 구성을 통해 **MetroCluster** 에서 클러스터 상태 확인

FC 구성을 통한 MetroCluster 에서 클러스터 상태를 확인하려면 다음 단계를 따르세요.

단계

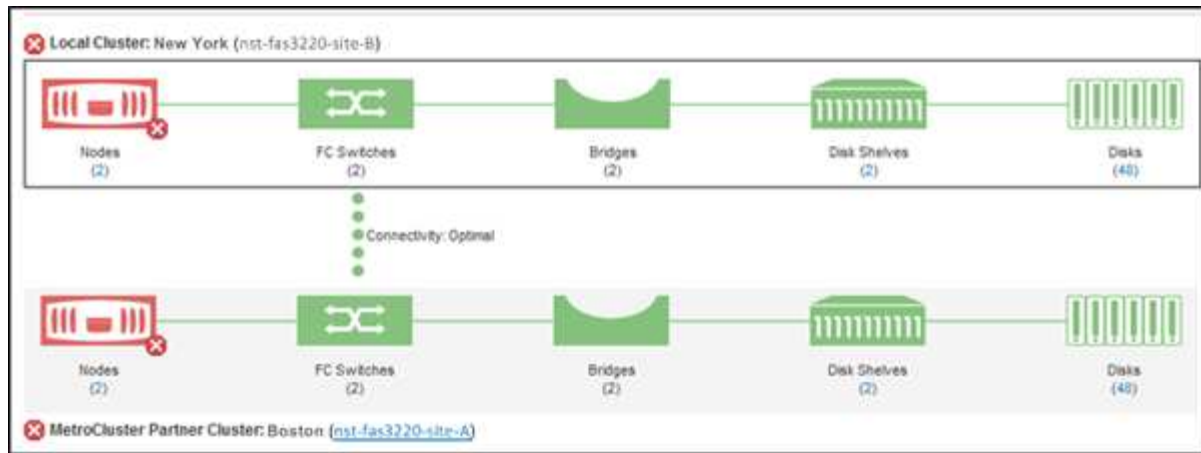
- 왼쪽 탐색 창에서 *이벤트 관리*를 클릭하여 이벤트 목록을 표시합니다.
- 필터 패널에서 소스 유형 카테고리 아래에 있는 모든 MetroCluster 필터를 선택합니다. 모든 MetroCluster 구성에 대해 환경에서 발생한 모든 이벤트를 볼 수 있습니다.
- MetroCluster 이벤트 옆에 있는 클러스터 이름을 클릭합니다.



MetroCluster 이벤트가 표시되지 않으면 검색 창을 사용하여 FC 구성을 통한 MetroCluster 와 관련된 이벤트에 관련된 클러스터 이름을 검색할 수 있습니다.

상태: 모든 클러스터 보기에는 이벤트에 대한 자세한 정보가 표시됩니다.

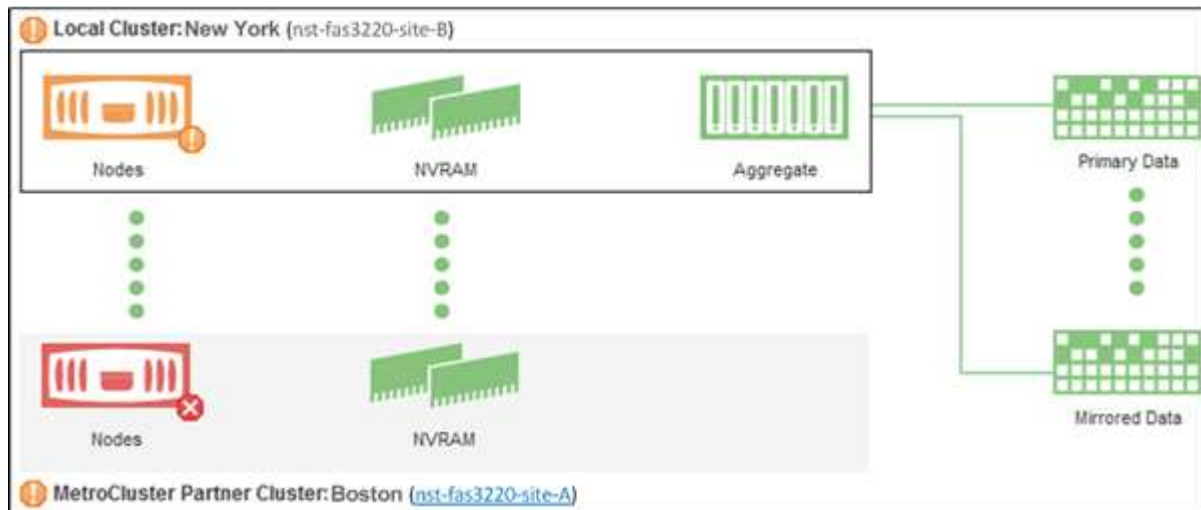
- 선택한 클러스터와 파트너 클러스터 간 연결 상태를 표시하려면 * MetroCluster Connectivity* 탭을 선택합니다.



이 예에서는 로컬 클러스터와 파트너 클러스터의 이름과 구성 요소가 표시됩니다. 노란색 또는 빨간색 아이콘은 강조 표시된 구성 요소의 상태 이벤트를 나타냅니다. 연결 아이콘은 클러스터 간의 링크를 나타냅니다. 마우스 커서를 아이콘에 대면 이벤트 정보가 표시되고, 아이콘을 클릭하면 이벤트가 표시됩니다. 두 클러스터 중 하나의 상태 문제가 성능 이벤트에 영향을 미칠 수 있습니다.

Unified Manager는 클러스터 간 링크의 NVRAM 구성 요소를 모니터링합니다. 로컬 또는 파트너 클러스터의 FC 스위치 아이콘이나 연결 아이콘이 빨간색인 경우 링크 상태 문제로 인해 성능 이벤트가 발생했을 수 있습니다.

5. * MetroCluster 복제* 탭을 선택합니다.



이 예에서 로컬 또는 파트너 클러스터의 NVRAM 아이콘이 노란색이나 빨간색이면 NVRAM에 대한 상태 문제로 인해 성능 이벤트가 발생했을 수 있습니다. 페이지에 빨간색이나 노란색 아이콘이 없는 경우 파트너 클러스터의 성능 문제로 인해 성능 이벤트가 발생했을 수 있습니다.

IP 구성을 통한 **MetroCluster** 에서 클러스터 상태 확인

IP 구성을 통한 MetroCluster 에서 클러스터 상태를 확인하려면 다음 단계를 따르세요.

단계

1. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭하여 이벤트 목록을 표시합니다.
2. 필터 패널의 소스 유형 카테고리에서 다음을 선택합니다. MetroCluster Relationship 필터. 모든 MetroCluster 구성에 대해 환경에서 발생한 모든 이벤트를 볼 수 있습니다.



보고된 MetroCluster 이벤트를 볼 수 없는 경우 검색 창을 사용하여 IP 구성을 통한 MetroCluster와 관련된 이벤트에 연루된 클러스터의 이름으로 검색할 수 있습니다.

- 해당 MetroCluster 이벤트 옆에 있는 클러스터 이름을 클릭합니다. 클러스터 페이지에 해당 클러스터의 세부 정보가 표시됩니다. 건강 문제 판별에 대한 정보는 다음을 참조하세요. "[IP 구성을 통한 MetroCluster의 연결 문제 모니터링](#)".

모든 **SAN** 어레이 클러스터의 상태 및 용량 상태를 확인합니다.

클러스터 인벤토리 페이지를 사용하면 모든 SAN 어레이 클러스터의 상태와 용량 상태를 표시할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

모든 SAN 어레이 클러스터에 대한 개요 정보는 상태: 모든 클러스터 보기 및 용량: 모든 클러스터 보기에서 볼 수 있습니다. 또한 클러스터/상태 세부 정보 페이지에서 세부 정보를 볼 수 있습니다.

단계

- 왼쪽 탐색 창에서 저장소 > *클러스터*를 클릭합니다.
- 상태: 모든 클러스터 보기에 "개성" 열이 표시되는지 확인하거나 표시/숨기기 컨트롤을 사용하여 추가하세요.

이 열에는 모든 SAN 어레이 클러스터에 대한 "모든 SAN 어레이"가 표시됩니다.

- 정보를 검토하세요.
- 해당 클러스터의 저장 용량에 대한 정보를 보려면 용량: 모든 클러스터 보기를 선택하세요.
- 해당 클러스터의 상태 및 저장 용량에 대한 자세한 정보를 보려면 All SAN Array 클러스터의 이름을 클릭하세요.

클러스터/상태 세부 정보 페이지의 상태, 용량 및 노드 탭에서 세부 정보를 확인하세요.

노드 목록 및 세부 정보 보기

클러스터의 노드 목록을 보려면 Health: All Nodes 보기를 사용하세요. 클러스터/상태 세부 정보 페이지를 사용하면 모니터링되는 클러스터에 속한 노드에 대한 자세한 정보를 볼 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

노드 상태, 노드가 포함된 클러스터, 집계 용량 세부 정보(사용됨 및 총 용량), 원시 용량 세부 정보(사용 가능, 예비 및 총 용량)와 같은 세부 정보를 볼 수 있습니다. HA 쌍, 디스크 헬프, 포트에 대한 정보도 얻을 수 있습니다.

단계

- 왼쪽 탐색 창에서 저장소 > *노드*를 클릭합니다.
- 상태: 모든 노드 보기에서 세부 정보를 보려는 노드를 클릭합니다.

선택한 노드에 대한 자세한 정보는 클러스터/상태 세부 정보 페이지에 표시됩니다. 왼쪽 창에는 HA 쌍 목록이 표시됩니다. 기본적으로 HA 세부 정보가 열려 있으며, 선택한 HA 쌍과 관련된 HA 상태 세부 정보와 이벤트가

표시됩니다.

3. 노드에 대한 다른 세부 정보를 보려면 적절한 작업을 수행하세요.

보려면...	딸깍 하는 소리...
디스크 선반에 대한 세부 정보	디스크 선반.
항만 관련 정보	항구.

자세한 내용은 다음을 참조하세요.

- ["성능: 모든 노드 보기"](#)
- ["노드 및 집계 가능한 IOPS 값 보기"](#)
- ["노드 및 집계 성능 용량 사용 값 보기"](#)

계약 갱신을 위한 하드웨어 인벤토리 보고서 생성

하드웨어 모델 번호 및 일련 번호, 디스크 유형 및 개수, 설치된 라이선스 등 클러스터 및 노드 정보의 전체 목록이 포함된 보고서를 생성할 수 있습니다. 이 보고서는 NetAppActive IQ 플랫폼에 연결되지 않은 보안 사이트("다크" 사이트) 내에서 계약을 갱신하는 데 유용합니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *노드*를 클릭합니다.
2. 상태: 모든 노드 보기 또는 성능: 모든 노드 보기로 이동합니다.
3. 보고서 > * > 하드웨어 재고 보고서*를 선택하세요.

하드웨어 재고 보고서는 현재 날짜까지의 전체 정보가 포함된 .csv 파일로 다운로드됩니다.

4. 계약 갱신을 위해 NetApp 지원 담당자에게 이 정보를 제공하세요.

저장소 VM 목록 및 세부 정보 보기

상태: 모든 스토리지 VM 보기에서 스토리지 가상 머신(SVM) 인벤토리를 모니터링할 수 있습니다. 스토리지 VM/상태 세부 정보 페이지를 사용하면 모니터링되는 SVM에 대한 자세한 정보를 볼 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

SVM의 용량, 효율성, 구성 등 SVM 세부 정보를 볼 수 있습니다. 해당 SVM에 대한 관련 장치 및 관련 알림에 대한 정보도 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *저장소 VM*을 클릭합니다.
2. 다음 방법 중 하나를 선택하여 SVM 세부 정보를 확인하세요.
 - 모든 클러스터의 모든 SVM 상태에 대한 정보를 보려면 보기 메뉴에서 상태: 모든 저장소 VM 보기를 선택합니다.
 - 자세한 내용을 보려면 스토리지 VM 이름을 클릭하세요.

최소 세부 정보 대화 상자에서 *세부 정보 보기*를 클릭하면 전체 세부 정보를 볼 수도 있습니다.

3. 최소 세부 정보 대화 상자에서 *관련 항목 보기*를 클릭하여 SVM과 관련된 객체를 봅니다.

관련 정보

- ["스토리지 VM: 상태 세부 정보 페이지"](#)
- ["성능: 모든 스토리지 VM 보기"](#)
- ["보안: 랜섬웨어 방지 보기"](#)
- ["클러스터 및 스토리지 VM의 보안 상태 보기"](#)
- ["관계: 모든 관계 보기"](#)

집계 목록 및 세부 정보 보기

상태: 모든 집계 보기에서 집계 인벤토리를 모니터링할 수 있습니다. 용량: 모든 집계 보기를 사용하면 모든 클러스터의 집계 용량 및 활용도에 대한 정보를 볼 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

집계/상태 세부 정보 페이지에서 집계 용량 및 구성, 디스크 정보와 같은 세부 정보를 볼 수 있습니다. 필요한 경우 임계값 설정을 구성하기 전에 이러한 세부 정보를 사용할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *집계*를 클릭합니다.
2. 다음 방법 중 하나를 선택하여 집계 세부 정보를 확인하세요.
 - 모든 클러스터의 모든 집계 상태에 대한 정보를 보려면 보기 메뉴에서 상태: 모든 집계 보기를 선택합니다.
 - 모든 클러스터의 모든 집계에 대한 용량 및 활용도에 대한 정보를 보려면 보기 메뉴에서 용량: 모든 집계 보기를 선택합니다.
 - 전체 세부 정보를 보려면 집계 이름을 클릭하세요.

최소 세부 정보 대화 상자에서 *세부 정보 보기*를 클릭하면 전체 세부 정보를 볼 수도 있습니다.

3. 최소 세부 정보 대화 상자에서 *관련 항목 보기*를 클릭하여 집계와 관련된 객체를 봅니다.

관련 정보

- ["집계/상태 세부 정보 페이지"](#)

- "성능: 모든 집계 보기"
- "집계 용량 보고서 사용자 정의"

FabricPool 용량 정보 보기

클러스터, 집계 및 볼륨에 대한 FabricPool 용량 정보는 이러한 개체에 대한 용량 및 성능 인벤토리와 세부 정보 페이지에서 볼 수 있습니다. 이 페이지에는 미리 계층이 구성된 경우 FabricPool 미리 정보도 표시됩니다.

이 페이지에는 로컬 성능 계층과 클라우드 계층에서 사용 가능한 용량, 두 계층에서 사용되는 용량, 어떤 집계가 클라우드 계층에 연결되어 있는지, 어떤 볼륨이 특정 정보를 클라우드 계층으로 이동하여 FabricPool 기능을 구현하고 있는지 등의 정보가 표시됩니다.

클라우드 계층이 다른 클라우드 공급자에 미러링되면('미러 계층') 두 클라우드 계층 모두 집계/상태 세부 정보 페이지에 표시됩니다.

단계

1. 다음 중 하나를 수행하세요.

...에 대한 용량 정보를 보려면	이렇게 하세요...
클러스터	a. 용량: 모든 클러스터 보기에서 클러스터를 클릭합니다. b. 클러스터/상태 세부 정보 페이지에서 구성 탭을 클릭합니다. 디스플레이에는 이 클러스터가 연결된 모든 클라우드 계층의 이름이 표시됩니다.
골재	a. 용량: 모든 집계 보기에서 유형 필드가 "SSD(FabricPool)" 또는 "HDD(FabricPool)"를 나타내는 집계를 클릭합니다. b. 집계/상태 세부 정보 페이지에서 용량 탭을 클릭합니다. 디스플레이에는 클라우드 계층에서 사용된 총 용량이 표시됩니다. c. 디스크 정보 탭을 클릭합니다. 디스플레이에는 클라우드 계층의 이름과 사용 용량이 표시됩니다. d. 구성 탭을 클릭합니다. 디스플레이에는 클라우드 계층의 이름과 클라우드 계층에 대한 기타 자세한 정보가 표시됩니다.

...에 대한 용량 정보를 보려면	이렇게 하세요...
볼륨	a. 용량: 모든 볼륨 보기에서 "계층화 정책" 필드에 정책 이름이 나타나는 볼륨을 클릭합니다. b. 볼륨/상태 세부 정보 페이지에서 구성 탭을 클릭합니다. 디스플레이에는 볼륨에 할당된 FabricPool 계층화 정책의 이름이 표시됩니다.

- 작업 부하 분석 페이지에서 용량 추세 영역의 "클라우드 계층 보기"를 선택하면 지난달에 로컬 성능 계층과 클라우드 계층에서 사용된 용량을 확인할 수 있습니다.

FabricPool 집계에 대한 자세한 내용은 다음을 참조하세요. ["디스크 및 집계 개요"](#).

스토리지 풀 세부 정보 보기

스토리지 풀의 세부 정보를 보고 스토리지 풀 상태, 총 캐시와 사용 가능한 캐시, 사용된 할당과 사용 가능한 할당을 모니터링할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

- 왼쪽 탐색 창에서 저장소 > *집계*를 클릭합니다.
- 집계 이름을 클릭하세요.

선택한 집계의 세부 정보가 표시됩니다.

- 디스크 정보 탭을 클릭합니다.

자세한 디스크 정보가 표시됩니다.



캐시 테이블은 선택한 집계가 스토리지 풀을 사용하는 경우에만 표시됩니다.

- 캐시 테이블에서 필요한 스토리지 풀의 이름 위로 포인터를 이동합니다.

스토리지 풀의 세부 정보가 표시됩니다.

볼륨 목록 및 세부 정보 보기

상태: 모든 볼륨 보기에서 볼륨 인벤토리를 모니터링할 수 있습니다. 용량: 모든 볼륨 보기를 사용하면 클러스터 내 볼륨의 용량 및 사용률에 대한 정보를 볼 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨/상태 세부 정보 페이지를 사용하면 용량, 효율성, 구성, 볼륨 보호 등 모니터링되는 볼륨에 대한 자세한 정보를 볼 수도 있습니다. 특정 볼륨에 대한 관련 장치 및 관련 알림에 대한 정보도 볼 수 있습니다.

단계

- 1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
- 2. 볼륨 세부 정보를 보려면 다음 방법 중 하나를 선택하세요.
 - 클러스터 내 볼륨의 상태에 대한 자세한 정보를 보려면 보기 메뉴에서 상태: 모든 볼륨 보기를 선택합니다.
 - 클러스터 내 볼륨의 용량 및 활용도에 대한 자세한 정보를 보려면 보기 메뉴에서 용량: 모든 볼륨 보기를 선택합니다.
 - 자세한 내용을 보려면 볼륨 이름을 클릭하세요.

최소 세부 정보 대화 상자에서 *세부 정보 보기*를 클릭하면 전체 세부 정보를 볼 수도 있습니다.

- 3. 선택 사항: 최소 세부 정보 대화 상자에서 *관련 항목 보기*를 클릭하여 볼륨과 관련된 객체를 봅니다.

관련 정보

- ["볼륨: 건강 세부 정보 페이지"](#)
- ["성능: 모든 볼륨 보기"](#)
- ["보안: 랜섬웨어 방지 보기"](#)
- ["볼륨 보호 관계 보기"](#)
- ["사용 가능한 볼륨 용량 차트를 보기 위한 보고서 만들기"](#)

NFS 공유에 대한 세부 정보 보기

모든 NFS 공유에 대한 세부 정보(상태, 볼륨(FlexGroup 볼륨 또는 FlexVol 볼륨)과 연결된 경로, NFS 공유에 대한 클라이언트의 액세스 수준, 내보내는 볼륨에 대해 정의된 내보내기 정책 등)를 볼 수 있습니다. Health: 모든 NFS 공유 보기를 사용하면 모니터링되는 모든 클러스터의 모든 NFS 공유를 볼 수 있으며, Storage VM/Health 세부 정보 페이지를 사용하면 특정 스토리지 가상 머신(SVM)의 모든 NFS 공유를 볼 수 있습니다.

시작하기 전에

- 클러스터에서 NFS 라이선스를 활성화해야 합니다.
- NFS 공유를 제공하는 네트워크 인터페이스를 구성해야 합니다.
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

- 1. 왼쪽 탐색 창에서 모든 NFS 공유를 볼지, 아니면 특정 SVM의 NFS 공유만 볼지에 따라 아래 단계를 따르세요.

에게...	다음 단계를 따르세요...
모든 NFS 공유 보기	저장소 > *NFS 공유*를 클릭하세요.

에게...	다음 단계를 따르세요...
단일 SVM에 대한 NFS 공유 보기	a. 저장소 > *저장소 VM*을 클릭합니다. b. NFS 공유 세부 정보를 보려는 SVM을 클릭합니다. c. 저장소 VM/상태 세부 정보 페이지에서 NFS 공유 탭을 클릭합니다.

자세한 내용은 다음을 참조하세요. "[파일 공유 볼륨 프로비저닝](#)" 그리고 "[API를 사용하여 CIFS 및 NFS 파일 공유 프로비저닝](#)".

SMB/CIFS 주식에 대한 세부 정보 보기

공유 이름, 연결 경로, 포함된 개체, 보안 설정, 공유에 대해 정의된 내보내기 정책 등 모든 SMB/CIFS 공유에 대한 세부 정보를 볼 수 있습니다. Health: All SMB Shares 보기를 사용하면 모니터링되는 모든 클러스터의 모든 SMB 공유를 볼 수 있으며, Storage VM/Health 세부 정보 페이지를 사용하면 특정 Storage Virtual Machine(SVM)의 모든 SMB 공유를 볼 수 있습니다.

시작하기 전에

- 클러스터에서 CIFS 라이선스를 활성화해야 합니다.
- SMB/CIFS 공유를 제공하는 네트워크 인터페이스를 구성해야 합니다.
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.



폴더의 공유는 표시되지 않습니다.

단계

1. 왼쪽 탐색 창에서 모든 SMB/CIFS 공유를 볼지, 아니면 특정 SVM의 공유만 볼지에 따라 아래 단계를 따르세요.

에게...	다음 단계를 따르세요...
모든 SMB/CIFS 주식 보기	저장소 > *SMB 공유*를 클릭하세요.
단일 SVM에 대한 SMB/CIFS 공유 보기	a. 저장소 > *저장소 VM*을 클릭합니다. b. SMB/CIFS 공유 세부 정보를 보려는 SVM을 클릭합니다. c. 저장소 VM/상태 세부 정보 페이지에서 SMB 공유 탭을 클릭합니다.

자세한 내용은 다음을 참조하세요. "[API를 사용하여 CIFS 및 NFS 파일 공유 프로비저닝](#)".

스냅샷 복사본 목록 보기

선택한 볼륨의 스냅샷 복사본 목록을 볼 수 있습니다. 스냅샷 복사본 목록을 사용하면 하나 이상의 스냅샷 복사본이 삭제된 경우 회수할 수 있는 디스크 공간의 양을 계산할 수 있으며,

필요한 경우 스냅샷 복사본을 삭제할 수 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 스냅샷 복사본이 포함된 볼륨은 온라인 상태여야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 상태: 모든 볼륨 보기에서 보려는 스냅샷 복사본이 포함된 볼륨을 선택합니다.
3. 볼륨/상태 세부 정보 페이지에서 용량 탭을 클릭합니다.
4. 용량 탭의 세부 정보 창에서 기타 세부 정보 섹션의 스냅샷 복사본 옆에 있는 링크를 클릭합니다.

스냅샷 복사본 수는 스냅샷 복사본 목록을 표시하는 링크입니다.

관련 정보

["상태/볼륨 페이지"](#)

스냅샷 사본 삭제

공간을 절약하거나 디스크 공간을 확보하기 위해 스냅샷 복사본을 삭제할 수 있으며, 더 이상 필요하지 않으면 스냅샷 복사본을 삭제할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

해당 볼륨은 온라인 상태여야 합니다.

사용 중이거나 잠긴 스냅샷 복사본을 삭제하려면 해당 복사본을 사용 중이던 애플리케이션에서 스냅샷 복사본을 해제해야 합니다.

- FlexClone 볼륨이 해당 스냅샷 복사본을 사용하는 경우 부모 볼륨의 기본 스냅샷 복사본을 삭제할 수 없습니다.

기본 스냅샷 복사본은 FlexClone 볼륨을 생성하는 데 사용되는 스냅샷 복사본이며 상태를 표시합니다. Busy 및 응용 프로그램 종속성 Busy, Vclone 부모 권에서.

- SnapMirror 관계에서 사용되는 잠긴 스냅샷 복사본은 삭제할 수 없습니다.

스냅샷 사본은 잠겨 있으며 다음 업데이트에 필요합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 상태: 모든 볼륨 보기에서 보려는 스냅샷 복사본이 포함된 볼륨을 선택합니다.

스냅샷 복사본 목록이 표시됩니다.

3. 볼륨/상태 세부 정보 페이지에서 용량 탭을 클릭합니다.

4. 용량 탭의 세부 정보 창에서 기타 세부 정보 섹션의 스냅샷 복사본 옆에 있는 링크를 클릭합니다.

스냅샷 복사본 수는 스냅샷 복사본 목록을 표시하는 링크입니다.

5. 스냅샷 복사본 보기에서 삭제할 스냅샷 복사본을 선택한 다음 *선택 항목 삭제*를 클릭합니다.

스냅샷 복사본에 대한 회수 가능 공간 계산

하나 이상의 스냅샷 복사본이 삭제된 경우 회수할 수 있는 디스크 공간의 양을 계산할 수 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 해당 볼륨은 온라인 상태여야 합니다.
- 볼륨은 FlexVol volume 이어야 합니다. 이 기능은 FlexGroup 볼륨에서는 지원되지 않습니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 상태: 모든 볼륨 보기에서 보려는 스냅샷 복사본이 포함된 볼륨을 선택합니다.

스냅샷 복사본 목록이 표시됩니다.

3. 볼륨/상태 세부 정보 페이지에서 용량 탭을 클릭합니다.
4. 용량 탭의 세부 정보 창에서 기타 세부 정보 섹션의 스냅샷 복사본 옆에 있는 링크를 클릭합니다.

스냅샷 복사본 수는 스냅샷 복사본 목록을 표시하는 링크입니다.

5. 스냅샷 복사본 보기에서 회수 가능한 공간을 계산하려는 스냅샷 복사본을 선택합니다.
6. *계산*을 클릭하세요.

볼륨에서 회수 가능한 공간(백분율, KB, MB, GB 등)이 표시됩니다.

7. 회수 가능한 공간을 다시 계산하려면 필요한 스냅샷 복사본을 선택하고 *다시 계산*을 클릭하세요.

클러스터 객체 창 및 대화 상자 설명

각 스토리지 객체 페이지에서 모든 클러스터와 클러스터 객체를 볼 수 있습니다. 해당 스토리지 객체 세부 정보 페이지에서 세부 정보를 볼 수도 있습니다. 이제 INVENTORY의 STORAGE 및 PROTECTION 섹션에서 시스템 관리자 사용자 인터페이스를 시작할 수 있습니다.

- 클러스터 인벤토리, 클러스터 상태 및 클러스터 성능 페이지
- 집계 재고, 집계 상태 및 집계 성과 페이지
- 볼륨 인벤토리, 볼륨 상태 및 볼륨 성능 페이지
- 노드 인벤토리 및 노드 성능 페이지
- StorageVM 인벤토리, StorageVM 상태 및 StorageVM 성능 페이지

공통 Unified Manager 상태 워크플로 및 작업

Unified Manager와 관련된 일반적인 관리 워크플로 및 작업에는 모니터링할 스토리지 클러스터 선택, 데이터 가용성, 용량 및 보호에 부정적인 영향을 미치는 조건 진단, 손실된 데이터 복원, 볼륨 구성 및 관리, 진단 데이터를 묶어 기술 지원팀에 전송(필요한 경우) 등이 있습니다.

Unified Manager를 사용하면 스토리지 관리자가 대시보드를 보고, 관리되는 스토리지 클러스터의 전체 용량, 가용성 및 보호 상태를 평가한 다음, 발생할 수 있는 특정 문제를 신속하게 식별, 찾고, 진단하고, 해결을 위해 할당할 수 있습니다.

관리되는 스토리지 개체의 스토리지 용량이나 데이터 가용성에 영향을 미치는 클러스터, 스토리지 가상 머신(SVM), 볼륨 또는 FlexGroup 볼륨과 관련된 가장 중요한 문제는 대시보드 페이지의 시스템 상태 그래프와 이벤트에 표시됩니다. 심각한 문제가 발견되면 이 페이지에서는 적절한 문제 해결 워크플로를 지원하는 링크를 제공합니다.

Unified Manager는 OnCommand Workflow Automation (WFA)과 같은 관련 관리 도구가 포함된 워크플로에 포함되어 스토리지 리소스의 직접적인 구성을 지원할 수도 있습니다.

이 문서에서는 다음 관리 작업과 관련된 일반적인 워크플로를 설명합니다.

- 가용성 문제 진단 및 관리

하드웨어 오류나 스토리지 리소스 구성 문제로 인해 대시보드 페이지에 데이터 가용성 이벤트가 표시되는 경우, 스토리지 관리자는 내장된 링크를 따라 영향을 받는 스토리지 리소스에 대한 연결 정보를 보고, 문제 해결 조언을 보고, 문제 해결을 다른 관리자에게 할당할 수 있습니다.

- 성능 사고 구성 및 모니터링

관리자는 모니터링되는 스토리지 시스템 리소스의 성능을 모니터링하고 관리할 수 있습니다. 를 참조하십시오 ["Active IQ Unified Manager 성능 모니터링 소개"](#) 자세한 내용은.

- 볼륨 용량 문제 진단 및 관리

대시보드 페이지에 볼륨 저장소 용량 문제가 표시되면 저장소 관리자는 내장된 링크를 따라 영향을 받는 볼륨의 저장소 용량과 관련된 현재 및 과거 추세를 보고, 문제 해결 조언을 보고, 다른 관리자에게 문제 해결을 할당할 수 있습니다.

- 보호 관계 문제 구성, 모니터링 및 진단

보호 관계를 만들고 구성한 후, 스토리지 관리자는 보호 관계와 관련된 잠재적인 문제, 보호 관계의 현재 상태, 영향을 받는 관계에 대한 현재 및 과거 보호 작업 성공 정보, 문제 해결 조언을 볼 수 있습니다. 를 참조하십시오 ["보호 관계 생성, 모니터링 및 문제 해결"](#) 자세한 내용은.

- 백업 파일을 생성하고 백업 파일에서 데이터를 복원합니다.

- 주석과 스토리지 객체 연결

스토리지 객체를 주석과 연결하면 스토리지 관리자가 스토리지 객체와 관련된 이벤트를 필터링하고 볼 수 있으며, 이를 통해 스토리지 관리자가 이벤트와 관련된 문제의 우선순위를 지정하고 해결할 수 있습니다.

- REST API를 사용하면 Unified Manager에서 수집한 상태, 용량 및 성능 정보를 보고 클러스터를 관리하는 데 도움이 됩니다. 보다 ["Active IQ Unified Manager REST API 시작하기"](#) 자세한 내용은.

- 기술 지원팀에 지원 번들 보내기

스토리지 관리자는 유지 관리 콘솔을 사용하여 지원 번들을 검색하여 기술 지원팀에 보낼 수 있습니다. 문제에 AutoSupport 메시지에서 제공하는 것보다 더 자세한 진단 및 문제 해결이 필요한 경우 지원 번들을 기술 지원팀에 보내야 합니다.

데이터 가용성 모니터링 및 문제 해결

Unified Manager는 권한이 있는 사용자가 저장된 데이터에 얼마나 안정적으로 액세스할 수 있는지 모니터링하고, 해당 액세스를 차단하거나 방해하는 조건에 대해 경고하며, 해당 조건을 진단하고 해결 방법을 할당하고 추적할 수 있도록 합니다.

이 섹션의 가용성 워크플로 항목에서는 스토리지 관리자가 Unified Manager 웹 UI를 사용하여 데이터 가용성에 부정적인 영향을 미치는 하드웨어 및 소프트웨어 조건을 검색, 진단하고 해결을 위해 할당하는 방법의 예를 설명합니다.

스토리지 장애 조치 상호 연결 링크 다운 조건을 스캔하고 해결합니다.

이 워크플로는 다운된 스토리지 장애 조치 상호 연결 링크 조건을 스캔, 평가 및 해결하는 방법에 대한 예를 제공합니다. 이 시나리오에서는 관리자가 되어 노드에서 ONTAP 버전 업그레이드를 시작하기 전에 Unified Manager를 사용하여 스토리지 장애 조치 위험을 스캔합니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

중단 없는 업그레이드를 시도하는 동안 HA 쌍 노드 간의 스토리지 장애 조치 상호 연결이 실패하면 업그레이드가 실패합니다. 따라서 일반적인 관행은 관리자가 업그레이드를 시작하기 전에 업그레이드 대상 클러스터 노드에서 스토리지 장애 조치 안정성을 모니터링하고 확인하는 것입니다.

단계

1. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭합니다.
2. 이벤트 관리 인벤토리 페이지에서 *활성 가용성 이벤트*를 선택합니다.
3. 이벤트 관리 인벤토리 페이지 상단의 이름 열을 클릭하세요.  그리고 입력 *failover* 텍스트 상자에서 이벤트를 저장소 장애 조치 관련 이벤트로만 표시합니다.

저장소 장애 조치 조건과 관련된 모든 과거 이벤트가 표시됩니다.

이 시나리오에서 Unified Manager는 가용성 사고 섹션에 “스토리지 장애 조치 상호 연결 하나 이상의 링크가 다운됨” 이벤트를 표시합니다.

4. 이벤트 관리 인벤토리 페이지에 스토리지 장애 조치와 관련된 이벤트가 하나 이상 표시되는 경우 다음 단계를 수행하세요.
 - a. 이벤트 제목 링크를 클릭하면 해당 이벤트에 대한 이벤트 세부 정보가 표시됩니다.

이 예에서는 이벤트 제목 “저장소 장애 조치 상호 연결 하나 이상의 링크가 다운됨”을 클릭합니다.

해당 이벤트에 대한 이벤트 세부 정보 페이지가 표시됩니다.

- a. 이벤트 세부 정보 페이지에서 다음 작업 중 하나 이상을 수행할 수 있습니다.

- 원인 필드에서 오류 메시지를 검토하고 문제를 평가하세요.
- 이벤트를 관리자에게 할당합니다.
- 이벤트를 확인합니다.

관련 정보

"이벤트 세부 정보 페이지"

"Unified Manager 사용자 역할 및 기능"

스토리지 장애 조치 상호 연결 링크가 다운된 경우 시정 조치를 수행합니다.

스토리지 장애 조치 관련 이벤트의 이벤트 세부 정보 페이지를 표시하면 페이지의 요약 정보를 검토하여 이벤트의 긴급성, 문제의 가능한 원인, 문제에 대한 가능한 해결책을 확인할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이 예제 시나리오에서 이벤트 세부 정보 페이지에 제공된 이벤트 요약에는 스토리지 장애 조치 상호 연결 링크 다운 조건에 대한 다음 정보가 포함되어 있습니다.

Event: Storage Failover Interconnect One or More Links Down

Summary

Severity: Warning

State: New

Impact Level: Risk

Impact Area: Availability

Source: aardvark

Source Type: Node

Acknowledged By:

Resolved By:

Assigned To:

Cause: At least one storage failover interconnected link
between the nodes aardvark and bonobo is down.
RDMA interconnect is up (Link0 up, Link1 down)

예시 이벤트 정보는 HA 쌍 노드 aardvark와 bonobo 사이의 스토리지 장애 조치 상호 연결 링크 Link1이 다운되었지만 Apple과 Boy 사이의 Link0은 활성화되어 있음을 나타냅니다. 한 링크가 활성화되어 있으므로 원격 동적 메모리 액세스(RDMA)가 계속 작동하고 스토리지 장애 조치 작업이 계속 성공할 수 있습니다.

하지만 링크 장애와 스토리지 장애 조치 보호가 완전히 비활성화되는 것을 방지하기 위해 Link1이 다운된 이유를 추가로 진단하기로 결정했습니다.

단계

1. 이벤트 세부 정보 페이지에서 소스 필드에 지정된 이벤트에 대한 링크를 클릭하면 스토리지 장애 조치 상호 연결 링크 다운 조건과 관련이 있을 수 있는 다른 이벤트에 대한 자세한 내용을 얻을 수 있습니다.

이 예에서 이벤트의 소스는 `aardvark`라는 노드입니다. 해당 노드 이름을 클릭하면 클러스터/상태 세부 정보 페이지의 노드 탭에 영향을 받은 HA 쌍인 `aardvark`와 `bonobo`에 대한 HA 세부 정보가 표시되고, 영향을 받은 HA 쌍에서 최근 발생한 다른 이벤트도 표시됩니다.

2. 이벤트와 관련된 자세한 내용은 *HA 세부 정보*를 확인하세요.

이 예에서 관련 정보는 이벤트 테이블에 있습니다. 표에는 "저장소 장애 조치 연결 하나 이상 링크 다운" 이벤트, 이벤트가 생성된 시간, 그리고 이 이벤트가 발생한 노드가 표시됩니다.

HA 세부 정보의 노드 위치 정보를 사용하여 영향을 받는 HA 쌍 노드의 스토리지 장애 조치 문제에 대한 물리적 검사 및 수리를 요청하거나 직접 완료합니다.

관련 정보

["이벤트 세부 정보 페이지"](#)

["Unified Manager 사용자 역할 및 기능"](#)

볼륨 오프라인 문제 해결

이 워크플로는 Unified Manager가 이벤트 관리 인벤토리 페이지에 표시할 수 있는 볼륨 오프라인 이벤트를 평가하고 해결하는 방법의 예를 제공합니다. 이 시나리오에서는 Unified Manager를 사용하여 하나 이상의 볼륨 오프라인 이벤트에 대한 문제를 해결하는 관리자입니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨이 오프라인으로 보고되는 데에는 여러 가지 이유가 있을 수 있습니다.

- SVM 관리자가 의도적으로 볼륨을 오프라인으로 전환했습니다.
- 볼륨의 호스팅 클러스터 노드가 다운되었고 HA 쌍 파트너에 대한 스토리지 장애 조치도 실패했습니다.
- 해당 SVM의 루트 볼륨을 호스팅하는 노드가 다운되어 볼륨을 호스팅하는 스토리지 가상 머신(SVM)이 중지되었습니다.
- 두 개의 RAID 디스크가 동시에 고장나서 볼륨의 호스팅 집계가 중단되었습니다.

이벤트 관리 인벤토리 페이지와 클러스터/상태, 스토리지 VM/상태, 볼륨/상태 세부 정보 페이지를 사용하여 이러한 가능성 중 하나 이상을 확인하거나 제거할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭합니다.
2. 이벤트 관리 인벤토리 페이지에서 *활성 가용성 이벤트*를 선택합니다.
3. 볼륨 오프라인 이벤트에 표시된 하이퍼텍스트 링크를 클릭하세요.

가용성 사건에 대한 이벤트 세부 정보 페이지가 표시됩니다.

4. 해당 페이지에서 SVM 관리자가 해당 볼륨을 오프라인으로 전환했다는 표시가 있는지 확인하세요.

5. 이벤트 세부 정보 페이지에서 다음 작업 중 하나 이상에 대한 정보를 검토할 수 있습니다.

- 진단에 도움이 될 만한 정보를 얻으려면 원인 필드에 표시된 정보를 검토하세요.

이 예에서 원인 필드의 정보는 볼륨이 오프라인 상태라는 사실만 알려줍니다.

- SVM 관리자가 의도적으로 해당 볼륨을 오프라인으로 전환한 흔적이 있는지 메모 및 업데이트 영역을 확인하세요.
- 이벤트 소스(이 경우 오프라인으로 보고된 볼륨)를 클릭하면 해당 볼륨에 대한 자세한 정보를 얻을 수 있습니다.
- 이벤트를 관리자에게 할당합니다.
- 해당 사건을 확인하거나, 적절한 경우 해결된 것으로 표시합니다.

볼륨 오프라인 조건에 대한 진단 작업 수행

오프라인으로 보고된 볼륨의 볼륨/상태 세부 정보 페이지로 이동한 후 볼륨 오프라인 상태를 진단하는 데 도움이 되는 추가 정보를 검색할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

오프라인으로 보고된 볼륨이 의도적으로 오프라인으로 전환된 것이 아니라면, 해당 볼륨은 여러 가지 이유로 오프라인 상태일 수 있습니다.

오프라인 볼륨의 볼륨/상태 세부 정보 페이지에서 시작하여 다른 페이지와 창으로 이동하여 가능한 원인을 확인하거나 제거할 수 있습니다.

- 볼륨이 오프라인 상태인지 확인하려면 볼륨/상태 세부 정보 페이지 링크를 클릭하세요. 볼륨의 호스트 노드가 다운되었고 HA 쌍 파트너에 대한 스토리지 장애 조치도 실패했기 때문입니다.

보다"볼륨 오프라인 상태가 다운 노드로 인해 발생하는지 확인".

- 볼륨/상태 세부 정보 페이지 링크를 클릭하여 볼륨이 오프라인 상태이고 해당 SVM의 루트 볼륨을 호스팅하는 노드가 다운되어 호스트 스토리지 가상 머신(SVM)이 중지되었는지 확인합니다.

보다"노드가 다운되어 볼륨이 오프라인 상태이고 SVM이 중지되었는지 확인".

- 호스트 집계에서 디스크가 손상되어 볼륨이 오프라인 상태인지 확인하려면 볼륨/상태 세부 정보 페이지 링크를 클릭하세요.

보다"집계된 디스크가 손상되어 볼륨이 오프라인 상태인지 확인".

관련 정보

"Unified Manager 사용자 역할 및 기능"

호스트 노드가 다운되어 볼륨이 오프라인 상태인지 확인합니다.

Unified Manager 웹 UI를 사용하면 호스트 노드가 다운되어 볼륨이 오프라인 상태일 가능성을

확인하거나 제거할 수 있으며, HA 쌍 파트너에 대한 스토리지 장애 조치가 실패할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨 오프라인 상태가 호스팅 노드의 실패와 그에 따른 스토리지 장애 조치 실패로 인해 발생하는지 확인하려면 다음 작업을 수행하세요.

단계

1. 오프라인 볼륨의 볼륨/상태 세부 정보 페이지의 관련 장치 창에서 SVM 아래에 표시된 하이퍼텍스트 링크를 찾아 클릭합니다.

저장소 VM/상태 세부 정보 페이지에는 오프라인 볼륨의 호스팅 저장소 가상 머신(SVM)에 대한 정보가 표시됩니다.

2. 저장소 **VM**/상태 세부 정보 페이지의 관련 장치 창에서 볼륨 아래에 표시된 하이퍼텍스트 링크를 찾아 클릭합니다.

상태: 모든 볼륨 보기에는 SVM에서 호스팅되는 모든 볼륨에 대한 정보 표가 표시됩니다.

3. 상태: 모든 볼륨 보기 상태 열 머리글에서 필터 기호를 클릭합니다.  을 선택한 다음, 오프라인 옵션을 선택하세요.

오프라인 상태인 SVM 볼륨만 나열됩니다.

4. 상태: 모든 볼륨 보기에서 그리드 기호를 클릭합니다.  을 선택한 다음 클러스터 노드 옵션을 선택합니다.

클러스터 노드 옵션을 찾으려면 그리드 선택 상자를 스크롤해야 할 수도 있습니다.

클러스터 노드 열은 볼륨 인벤토리에 추가되고 각 오프라인 볼륨을 호스팅하는 노드의 이름이 표시됩니다.

5. 상태: 모든 볼륨 보기에서 오프라인 볼륨 목록을 찾고, 해당 클러스터 노드 열에서 호스팅 노드의 이름을 클릭합니다.

클러스터/상태 세부 정보 페이지의 노드 탭에는 호스팅 노드가 속한 HA 노드 쌍의 상태가 표시됩니다. 호스팅 노드의 상태와 클러스터 장애 조치 작업의 성공 여부가 디스플레이에 표시됩니다.

호스트 노드가 다운되어 볼륨이 오프라인 상태가 되고 HA 쌍 파트너에 대한 스토리지 장애 조치가 실패한 것을 확인한 후, 해당 관리자나 운영자에게 연락하여 다운된 노드를 수동으로 다시 시작하고 스토리지 장애 조치 문제를 해결하세요.

노드가 다운되어 볼륨이 오프라인 상태이고 해당 **SVM**이 중지되었는지 확인합니다.

Unified Manager 웹 UI를 사용하면 해당 SVM의 루트 볼륨을 호스팅하는 노드가 다운되어 호스트 스토리지 가상 머신(SVM)이 중지되어 볼륨이 오프라인 상태일 가능성을 확인하거나 제거할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨 오프라인 상태가 해당 SVM의 루트 볼륨을 호스팅하는 노드가 다운되어 호스트 SVM이 중지된 것으로 인해 발생하는지 확인하려면 다음 작업을 수행하세요.

단계

1. 오프라인 볼륨의 볼륨/상태 세부 정보 페이지의 관련 장치 창에서 SVM 아래에 표시된 하이퍼텍스트 링크를 찾아

클릭합니다.

저장소 VM/상태 세부 정보 페이지에는 호스팅 SVM의 "실행 중" 또는 "중지됨" 상태가 표시됩니다. SVM 상태가 실행 중이면 볼륨 오프라인 조건은 해당 SVM의 루트 볼륨을 호스팅하는 노드가 다운되어 발생한 것이 아닙니다.

2. SVM 상태가 중지된 경우 *SVM 보기*를 클릭하여 호스팅 SVM이 중지된 원인을 자세히 파악하세요.
3. 상태: 모든 스토리지 **VM** 보기 SVM 열 머리글에서 필터 기호를 클릭합니다. 그런 다음 중지된 SVM의 이름을 입력합니다.

해당 SVM에 대한 정보는 표에 표시되어 있습니다.

4. 상태: 모든 저장소 **VM** 보기에서 다음을 클릭합니다. 그런 다음 루트 볼륨 옵션을 선택하세요.

루트 볼륨 열은 SVM 인벤토리에 추가되고 중지된 SVM의 루트 볼륨 이름이 표시됩니다.

5. 루트 볼륨 열에서 루트 볼륨의 이름을 클릭하면 해당 볼륨의 저장소 **VM**/상태 세부 정보 페이지가 표시됩니다.

SVM 루트 볼륨의 상태가 (온라인)인 경우 해당 SVM의 루트 볼륨을 호스팅하는 노드가 다운되었기 때문에 원래 볼륨 오프라인 조건이 발생하지 않습니다.

6. SVM 루트 볼륨의 상태가 (오프라인)인 경우 SVM 루트 볼륨의 볼륨/상태 세부 정보 페이지의 관련 장치 창에서 집계 아래에 표시된 하이퍼텍스트 링크를 찾아 클릭합니다.
7. 집계의 집계/상태 세부 정보 페이지의 관련 장치 창에서 노드 아래에 표시된 하이퍼텍스트 링크를 찾아 클릭합니다.

클러스터/상태 세부 정보 페이지의 노드 탭에는 SVM 루트 볼륨의 호스팅 노드가 속한 HA 노드 쌍의 상태가 표시됩니다. 노드의 상태는 디스플레이에 표시됩니다.

볼륨 오프라인 상태가 해당 볼륨의 호스트 SVM 오프라인 상태로 인해 발생하고, 해당 SVM의 루트 볼륨을 호스팅하는 노드가 다운되어 오프라인 상태가 발생하는지 확인한 후, 해당 관리자나 운영자에게 연락하여 다운된 노드를 수동으로 다시 시작하세요.

집계된 디스크가 손상되어 볼륨이 오프라인 상태인지 확인합니다.

RAID 디스크 문제로 인해 호스트 집계가 오프라인 상태가 되어 볼륨이 오프라인 상태일 가능성을 확인하거나 제거하려면 Unified Manager 웹 UI를 사용할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨 오프라인 상태가 호스팅 집계를 오프라인으로 만드는 RAID 디스크 문제로 인해 발생하는지 확인하려면 다음 작업을 수행하세요.

단계

1. 볼륨/상태 세부 정보 페이지의 관련 장치 창에서 집계 아래에 표시된 하이퍼텍스트 링크를 찾아 클릭합니다.

집계/상태 세부 정보 페이지에는 호스팅 집계의 온라인 또는 오프라인 상태가 표시됩니다. 집계 상태가 온라인인 경우 RAID 디스크 문제는 볼륨이 오프라인되는 원인이 아닙니다.

2. 집계 상태가 오프라인인 경우 디스크 정보*를 클릭하고 *디스크 정보 탭의 이벤트 목록에서 손상된 디스크 이벤트를 찾습니다.

3. 손상된 디스크를 더 자세히 식별하려면 관련 장치 창의 노드 아래에 표시된 하이퍼텍스트 링크를 클릭하세요.

클러스터/상태 세부 정보 페이지가 표시됩니다.

4. 디스크*를 클릭한 다음, *필터 창에서 *손상됨*을 선택하면 손상된 상태의 모든 디스크가 나열됩니다.

손상된 상태의 디스크로 인해 호스트 집계가 오프라인 상태가 된 경우, 영향을 받는 집계 열에 집계 이름이 표시됩니다.

볼륨 오프라인 상태가 손상된 RAID 디스크와 그에 따른 오프라인 호스트 집계로 인해 발생한 것인지 확인한 후, 해당 관리자나 운영자에게 연락하여 손상된 디스크를 수동으로 교체하고 집계를 다시 온라인으로 전환하세요.

용량 문제 해결

이 워크플로는 용량 문제를 해결하는 방법의 예를 제공합니다. 이 시나리오에서 귀하는 관리자 또는 운영자로서 Unified Manager 대시보드 페이지에 액세스하여 모니터링되는 스토리지 개체에 용량 문제가 있는지 확인합니다. 문제의 원인과 해결책을 파악하고 싶습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

대시보드 페이지에서 이벤트 드롭다운 목록 아래의 용량 패널에서 "볼륨 공간 가득 참" 오류 이벤트를 찾습니다.

단계

1. 대시보드 페이지의 용량 패널에서 볼륨 공간 가득 참 오류 이벤트의 이름을 클릭합니다.

오류에 대한 이벤트 세부 정보 페이지가 표시됩니다.

2. 이벤트 세부 정보 페이지에서 다음 작업 중 하나 이상을 수행할 수 있습니다.

- 원인 필드에서 오류 메시지를 검토하고 제안된 수정 조치 아래의 제안 사항을 클릭하여 가능한 수정 조치에 대한 설명을 검토합니다.
- 소스 필드에서 개체 이름(이 경우 볼륨)을 클릭하면 개체에 대한 세부 정보를 얻을 수 있습니다.
- 이 이벤트에 대해 추가되었을 수 있는 메모를 찾아보세요.
- 이벤트에 메모를 추가합니다.
- 이벤트를 다른 사용자에게 할당합니다.
- 이벤트를 확인합니다.
- 이벤트를 해결됨으로 표시합니다.

관련 정보

["이벤트 세부 정보 페이지"](#)

전체 볼륨에 대해 제안된 시정 조치를 수행합니다.

"볼륨 공간 가득 참" 오류 이벤트가 발생한 후 이벤트 세부 정보 페이지에서 제안된 시정 조치를 검토하고 제안된 조치 중 하나를 수행하기로 결정합니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

모든 역할을 가진 사용자는 Unified Manager를 사용하여 이 워크플로의 모든 작업을 수행할 수 있습니다.

이 예에서는 Unified Manager Event Management 인벤토리 페이지에서 볼륨 공간 가득 참 오류 이벤트가 표시되었고 이벤트 이름을 클릭했습니다.

전체 볼륨에 대해 수행할 수 있는 가능한 시정 조치는 다음과 같습니다.

- 볼륨에서 자동 증가, 중복 제거 또는 압축 활성화
- 볼륨 크기 조정 또는 이동
- 볼륨에서 데이터 삭제 또는 이동

이러한 모든 작업은 ONTAP System Manager나 ONTAP CLI에서 수행해야 하지만 Unified Manager를 사용하면 어떤 작업을 수행해야 할지 결정하는 데 필요한 정보를 찾을 수 있습니다.

단계

1. 이벤트 세부 정보 페이지에서 소스 필드의 볼륨 이름을 클릭하면 영향을 받은 볼륨에 대한 세부 정보를 볼 수 있습니다.
2. 볼륨/상태 세부 정보 페이지에서 *구성*을 클릭하면 볼륨에서 중복 제거 및 압축이 이미 활성화되어 있는 것을 확인할 수 있습니다.

볼륨 크기를 조절하기로 결정했습니다.

3. 관련 장치 창에서 호스팅 집계의 이름을 클릭하면 해당 집계가 더 큰 볼륨을 수용할 수 있는지 확인할 수 있습니다.
4. 집계/상태 세부 정보 페이지에서 전체 볼륨을 호스팅하는 집계에 커밋되지 않은 용량이 충분하다는 것을 확인했으므로 ONTAP 시스템 관리자를 사용하여 볼륨 크기를 조정하여 용량을 늘립니다.

관련 정보

["이벤트 세부 정보 페이지"](#)

건강 임계값 관리

모든 집계, 볼륨 및 Q트리에 대한 글로벌 상태 임계값을 구성하여 상태 임계값 위반을 추적할 수 있습니다.

저장 용량 상태 임계값은 무엇입니까?

저장소 용량 상태 임계값은 Unified Manager 서버가 저장소 개체의 용량 문제를 보고하기 위해 이벤트를 생성하는 지점입니다. 이러한 이벤트가 발생할 때마다 알림을 보내도록 알림을 구성할 수 있습니다.

모든 집계, 볼륨 및 Q트리에 대한 저장 용량 상태 임계값은 기본값으로 설정됩니다. 필요에 따라 개체 또는 개체 그룹에 대한 설정을 변경할 수 있습니다.

글로벌 상태 임계값 설정 구성

용량, 성장, 스냅샷 예약, 할당량 및 inode에 대한 글로벌 상태 임계값 조건을 구성하여 집계, 볼륨 및 Qtree 크기를 효과적으로 모니터링할 수 있습니다. 지연 임계값을 초과하는 이벤트를 생성하기 위한 설정을 편집할 수도 있습니다.

전역 상태 임계값 설정은 집계, 볼륨 등 연관된 모든 개체에 적용됩니다. 임계값을 초과하면 이벤트가 생성되고, 경고가 구성된 경우 경고 알림이 전송됩니다. 임계값 기본값은 권장 값으로 설정되어 있지만, 특정 요구 사항에 맞게 일정 간격으로 이벤트를 생성하도록 임계값을 수정할 수 있습니다. 임계값이 변경되면 다음 모니터링 주기에서 이벤트가 생성되거나 폐기됩니다.

전역 상태 임계값 설정은 왼쪽 탐색 메뉴의 이벤트 임계값 섹션에서 접근할 수 있습니다. 또한, 해당 개체의 인벤토리 페이지나 세부 정보 페이지에서 개별 개체에 대한 임계값 설정을 수정할 수도 있습니다.

- 자세한 내용은 다음을 참조하세요. ["전역 집계 상태 임계값 구성"](#).

모든 집계에 대한 용량, 성장 및 스냅샷 복사본에 대한 상태 임계값 설정을 구성하여 임계값 위반을 추적할 수 있습니다.

- 자세한 내용은 다음을 참조하세요. ["글로벌 볼륨 상태 임계값 구성"](#).

모든 볼륨의 용량, 스냅샷 복사본, Qtree 할당량, 볼륨 증가, 덮어쓰기 예약 공간 및 inode에 대한 상태 임계값 설정을 편집하여 임계값 위반을 추적할 수 있습니다.

- 자세한 내용은 다음을 참조하세요. ["글로벌 Qtree 상태 임계값 구성"](#).

모든 Qtree의 용량에 대한 상태 임계값 설정을 편집하여 임계값 위반을 추적할 수 있습니다.

- 자세한 내용은 다음을 참조하세요. ["관리되지 않는 보호 관계에 대한 지연 상태 임계값 설정 편집"](#).

경고 또는 오류 지연 시간 비율을 늘리거나 줄여서 사용자의 요구 사항에 더 적합한 간격으로 이벤트가 생성되도록 할 수 있습니다.

전역 집계 상태 임계값 구성

모든 집계에 대해 글로벌 상태 임계값을 구성하여 임계값 위반을 추적할 수 있습니다. 임계값 위반 시 적절한 이벤트가 생성되고 이러한 이벤트에 따라 예방 조치를 취할 수 있습니다. 모든 모니터링 집계에 적용되는 임계값에 대한 모범 사례 설정을 기반으로 글로벌 값을 구성할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

옵션을 전역적으로 구성하면 개체의 기본값이 수정됩니다. 그러나 기본값이 개체 수준에서 변경된 경우 전역 값은 수정되지 않습니다.

임계값 옵션에는 더 나은 모니터링을 위한 기본값이 있지만, 사용자 환경의 요구 사항에 맞게 값을 변경할 수 있습니다.

집계에 있는 볼륨에서 자동 증가가 활성화된 경우, 집계 용량 임계값은 원래 볼륨 크기가 아닌 자동 증가에 의해 설정된 최대 볼륨 크기를 기준으로 위반된 것으로 간주됩니다.



상태 임계값은 노드의 루트 집계에 적용되지 않습니다.

단계

1. 왼쪽 탐색 창에서 이벤트 임계값 > *집계*를 클릭합니다.
2. 용량, 성장 및 스냅샷 복사본에 대한 적절한 임계값을 구성합니다.
3. *저장*을 클릭하세요.

관련 정보

"사용자 추가"

글로벌 볼륨 상태 임계값 구성

모든 볼륨에 대한 글로벌 상태 임계값을 구성하여 임계값 위반을 추적할 수 있습니다. 건강 임계값 위반 시 적절한 이벤트가 생성되고, 이러한 이벤트에 따라 예방 조치를 취할 수 있습니다. 모든 모니터링 볼륨에 적용되는 임계값에 대한 모범 사례 설정을 기반으로 글로벌 값을 구성할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

대부분의 임계값 옵션에는 더 나은 모니터링을 위해 기본값이 있습니다. 하지만 사용자 환경의 요구 사항에 맞게 값을 변경할 수 있습니다.

볼륨에서 자동 증가가 활성화된 경우 해당 용량 임계값은 원래 볼륨 크기가 아닌 자동 증가에 의해 설정된 최대 볼륨 크기를 기준으로 위반된 것으로 간주됩니다.



1000개의 스냅샷 복사본의 기본값은 ONTAP 버전이 9.4 이상인 경우에만 FlexVol 볼륨에 적용되고, ONTAP 버전이 9.8 이상인 경우에만 FlexGroup 볼륨에 적용됩니다. 이전 버전의 ONTAP 소프트웨어가 설치된 클러스터의 경우 볼륨당 최대 스냅샷 복사본 수는 250개입니다. 이전 버전의 경우 Unified Manager는 1000(1000~250 사이의 모든 숫자)을 250으로 해석합니다. 즉, 스냅샷 복사본 수가 250에 도달하면 계속해서 이벤트를 받게 됩니다. 이전 버전에서 이 임계값을 250 미만으로 설정하려면 여기, 상태: 모든 볼륨 보기 또는 볼륨/상태 세부 정보 페이지에서 임계값을 250 이하로 설정해야 합니다.

단계

1. 왼쪽 탐색 창에서 이벤트 임계값 > *볼륨*을 클릭합니다.
2. 용량, 스냅샷 복사본, Qtree 할당량, 볼륨 증가 및 inode에 대한 적절한 임계값을 구성합니다.
3. *저장*을 클릭하세요.

관련 정보

"사용자 추가"

글로벌 Qtree 상태 임계값 구성

모든 qtree에 대한 글로벌 상태 임계값을 구성하여 임계값 위반을 추적할 수 있습니다. 건강

임계값 위반 시 적절한 이벤트가 생성되고, 이러한 이벤트에 따라 예방 조치를 취할 수 있습니다. 모든 모니터링된 Qtree에 적용되는 임계값에 대한 모범 사례 설정을 기반으로 글로벌 값을 구성할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

임계값 옵션에는 더 나은 모니터링을 위한 기본값이 있지만, 사용자 환경의 요구 사항에 맞게 값을 변경할 수 있습니다.

Qtree에 대한 이벤트는 Qtree 할당량이나 기본 할당량이 설정된 경우에만 생성됩니다. 사용자 할당량이나 그룹 할당량에 정의된 공간이 임계값을 초과하면 이벤트가 생성되지 않습니다.

단계

1. 왼쪽 탐색 창에서 이벤트 임계값 > *Qtree*를 클릭합니다.
2. 적절한 용량 임계값을 구성합니다.
3. *저장*을 클릭하세요.

관리되지 않는 보호 관계에 대한 지연 임계값 설정 구성

관리되지 않는 보호 관계에 대한 글로벌 기본 지연 경고 및 오류 상태 임계값 설정을 편집하여 요구 사항에 적합한 간격으로 이벤트가 생성되도록 할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

지연 시간은 정의된 전송 일정 간격을 넘을 수 없습니다. 예를 들어, 환승 일정이 매시간인 경우 지연 시간은 1시간을 넘을 수 없습니다. 지연 임계값은 지연 시간이 초과해서는 안 되는 백분율을 지정합니다. 1시간을 예로 들어, 지연 임계값이 150%로 정의된 경우 지연 시간이 1.5시간을 초과하면 이벤트를 받게 됩니다.

이 작업에 설명된 설정은 모든 관리되지 않는 보호 관계에 전역적으로 적용됩니다. 설정을 지정하여 하나의 관리되지 않는 보호 관계에만 독점적으로 적용할 수는 없습니다.

단계

1. 왼쪽 탐색 창에서 이벤트 임계값 > *관계*를 클릭합니다.
2. 필요에 따라 글로벌 기본 경고 또는 오류 지연 시간 백분율을 늘리거나 줄입니다.
3. 지연 임계값으로 인해 경고 또는 오류 이벤트가 발생하지 않도록 하려면 활성화 옆에 있는 상자의 선택을 취소합니다.
4. *저장*을 클릭하세요.

관련 정보

["사용자 추가"](#)

개별 집계 상태 임계값 설정 편집

하나 이상의 집계에 대한 집계 용량, 성장 및 스냅샷 복사본에 대한 상태 임계값 설정을 편집할 수 있습니다. 임계값을 넘으면 경고가 생성되고 알림을 받게 됩니다. 이러한 알림은 발생한 이벤트에

따라 예방 조치를 취하는 데 도움이 됩니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

임계값의 변경 사항에 따라 다음 모니터링 주기에서 이벤트가 생성되거나 폐기됩니다.

집계에 있는 볼륨에서 자동 증가가 활성화된 경우, 집계 용량 임계값은 원래 볼륨 크기가 아닌 자동 증가에 의해 설정된 최대 볼륨 크기를 기준으로 위반된 것으로 간주됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *집계*를 클릭합니다.
2. 상태: 모든 집계 보기에서 하나 이상의 집계를 선택한 다음 *임계값 편집*을 클릭합니다.
3. 집계 임계값 편집 대화 상자에서 용량, 성장 또는 스냅샷 복사본 중 하나의 임계값 설정을 편집하려면 해당 확인란을 선택한 다음 설정을 수정합니다.
4. *저장*을 클릭하세요.

관련 정보

["사용자 추가"](#)

개별 볼륨 상태 임계값 설정 편집

하나 이상의 볼륨에 대한 볼륨 용량, 성장, 할당량 및 공간 예약에 대한 상태 임계값 설정을 편집할 수 있습니다. 임계값을 넘으면 경고가 생성되고 알림을 받게 됩니다. 이러한 알림은 발생한 이벤트에 따라 예방 조치를 취하는 데 도움이 됩니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

임계값의 변경 사항에 따라 다음 모니터링 주기에서 이벤트가 생성되거나 폐기됩니다.

볼륨에서 자동 증가가 활성화된 경우 해당 용량 임계값은 원래 볼륨 크기가 아닌 자동 증가에 의해 설정된 최대 볼륨 크기를 기준으로 위반된 것으로 간주됩니다.



1000개의 스냅샷 복사본의 기본값은 ONTAP 버전이 9.4 이상인 경우에만 FlexVol 볼륨에 적용되고, ONTAP 버전이 9.8 이상인 경우에만 FlexGroup 볼륨에 적용됩니다. 이전 버전의 ONTAP 소프트웨어가 설치된 클러스터의 경우 볼륨당 최대 스냅샷 복사본 수는 250개입니다. 이전 버전의 경우 Unified Manager는 1000(1000~250 사이의 모든 숫자)을 250으로 해석합니다. 즉, 스냅샷 복사본 수가 250에 도달하면 계속해서 이벤트를 받게 됩니다. 이전 버전에서 이 임계값을 250 미만으로 설정하려면 여기, 상태: 모든 볼륨 보기 또는 볼륨/상태 세부 정보 페이지에서 임계값을 250 이하로 설정해야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 상태: 모든 볼륨 보기에서 하나 이상의 볼륨을 선택한 다음 *임계값 편집*을 클릭합니다.
3. 볼륨 임계값 편집 대화 상자에서 용량, 스냅샷 복사본, Qtree 할당량, 증가 또는 inode 중 하나의 임계값 설정을 편집하려면 적절한 확인란을 선택한 다음 설정을 수정합니다.

4. *저장*을 클릭하세요.

관련 정보

["사용자 추가"](#)

개별 **qtree** 상태 임계값 설정 편집

하나 이상의 Qtree에 대한 Qtree 용량의 상태 임계값 설정을 편집할 수 있습니다. 임계값을 넘으면 경고가 생성되고 알림을 받게 됩니다. 이러한 알림은 발생한 이벤트에 따라 예방 조치를 취하는 데 도움이 됩니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

임계값의 변경 사항에 따라 다음 모니터링 주기에서 이벤트가 생성되거나 폐기됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *Qtrees*를 클릭합니다.
2. 용량: 모든 **Qtree** 보기에서 하나 이상의 Qtree를 선택한 다음 *임계값 편집*을 클릭합니다.
3. **Qtree** 임계값 편집 대화 상자에서 선택한 Qtree 또는 여러 Qtree의 용량 임계값을 변경하고 *저장*을 클릭합니다.



Storage VM/Health 세부 정보 페이지의 Qtrees 탭에서 개별 Qtree 임계값을 설정할 수도 있습니다.

클러스터 보안 목표 관리

Unified Manager는 _NetApp 보안 강화 가이드 for ONTAP 9_에 정의된 권장 사항을 기반으로 ONTAP 클러스터, 스토리지 가상 머신(SVM) 및 볼륨의 보안 수준을 파악하는 대시보드를 제공합니다.

보안 대시보드의 목적은 ONTAP 클러스터가 NetApp 권장 가이드라인과 일치하지 않는 영역을 표시하여 이러한 잠재적 문제를 해결할 수 있도록 하는 것입니다. 대부분의 경우 ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 문제를 해결할 수 있습니다. 귀하의 조직이 모든 권장 사항을 따르지 않을 수 있으므로, 어떤 경우에는 아무런 변경도 할 필요가 없을 수도 있습니다.

를 참조하십시오 ["ONTAP 9를 위한 NetApp 보안 강화 가이드"](#) (TR-4569) 자세한 권장 사항과 해결책을 확인하세요.

Unified Manager는 보안 상태를 보고하는 것 외에도 보안 위반이 있는 모든 클러스터 또는 SVM에 대한 보안 이벤트를 생성합니다. 이벤트 관리 인벤토리 페이지에서 이러한 문제를 추적할 수 있으며, 이러한 이벤트에 대한 알림을 구성하여 새로운 보안 이벤트가 발생할 때 스토리지 관리자에게 알림을 보낼 수 있습니다.

자세한 내용은 다음을 참조하세요. ["어떤 보안 기준이 평가되고 있습니까?"](#).

어떤 보안 기준이 평가되고 있습니까?

일반적으로 ONTAP 클러스터, 스토리지 가상 머신(SVM) 및 볼륨에 대한 보안 기준은 _NetApp 보안 강화 가이드 for ONTAP 9_에 정의된 권장 사항을 기준으로 평가됩니다.

보안 검사에는 다음이 포함됩니다.

- 클러스터가 SAML과 같은 보안 인증 방법을 사용하는지 여부
- 피어링된 클러스터의 통신이 암호화되어 있는지 여부
- 스토리지 VM에 감사 로그가 활성화되어 있는지 여부
- 볼륨에 소프트웨어 또는 하드웨어 암호화가 활성화되어 있는지 여부

규정 준수 범주 및 다음 항목 참조 ["ONTAP 9를 위한 NetApp 보안 강화 가이드"](#) 자세한 내용은.



Active IQ 플랫폼에서 보고된 업그레이드 이벤트도 보안 이벤트로 간주됩니다. 이러한 이벤트는 보안 권고에 따라 ONTAP 소프트웨어, 노드 펌웨어 또는 운영 체제 소프트웨어를 업그레이드해야 하는 문제를 식별합니다. 이러한 이벤트는 보안 패널에 표시되지 않지만 이벤트 관리 인벤토리 페이지에서 사용할 수 있습니다.

자세한 내용은 다음을 참조하세요. ["클러스터 보안 목표 관리"](#).

클러스터 규정 준수 범주

이 표에서는 Unified Manager가 평가하는 클러스터 보안 규정 준수 매개변수, NetApp 권장 사항, 그리고 매개변수가 클러스터의 전반적인 규정 준수 여부 결정에 영향을 미치는지 여부를 설명합니다.

클러스터에 규정을 준수하지 않는 SVM이 있으면 클러스터의 규정 준수 값에 영향을 미칩니다. 따라서 어떤 경우에는 클러스터 보안이 규정을 준수하는 것으로 간주되기 전에 SVM의 보안 문제를 해결해야 할 수도 있습니다.

아래 나열된 모든 매개변수가 모든 설치에 적용되는 것은 아닙니다. 예를 들어, 피어링된 클러스터가 없거나 클러스터에서 AutoSupport 비활성화한 경우 UI 페이지에 클러스터 피어링이나 AutoSupport HTTPS 전송 항목이 표시되지 않습니다.

매개변수	설명	추천	클러스터 규정 준수에 영향을 미칩니다
글로벌 FIPS	글로벌 FIPS(연방 정보 처리 표준) 140-2 준수 모드가 활성화되어 있는지 비활성화되어 있는지 여부를 나타냅니다. FIPS가 활성화되면 TLSv1과 SSLv3는 비활성화되고 TLSv1.1과 TLSv1.2만 허용됩니다.	활성화됨	예
텔넷	시스템에 대한 Telnet 액세스가 활성화되어 있는지 비활성화되어 있는지를 나타냅니다. NetApp 안전한 원격 액세스를 위해 Secure Shell(SSH)을 권장합니다.	장애가 있는	예

매개변수	설명	추천	클러스터 규정 준수에 영향을 미칩니다
안전하지 않은 SSH 설정	SSH가 안전하지 않은 암호 (예: *cbc로 시작하는 암호)를 사용하는지 여부를 나타냅니다.	아니요	예
로그인 배너	시스템에 액세스하는 사용자에게 로그인 배너가 활성화되어 있는지 비활성화되어 있는지 여부를 나타냅니다.	활성화됨	예
클러스터 피어링	피어링된 클러스터 간 통신이 암호화되었는지 암호화되지 않았는지 여부를 나타냅니다. 이 매개변수가 규정을 준수하는 것으로 간주하려면 소스 클러스터와 대상 클러스터 모두에서 암호화를 구성해야 합니다.	암호화됨	예
네트워크 시간 프로토콜	클러스터에 하나 이상의 구성된 NTP 서버가 있는지 여부를 나타냅니다. 중복성과 최상의 서비스를 위해 NetApp 클러스터에 최소 3개의 NTP 서버를 연결할 것을 권장합니다.	구성됨	예
OCSP	9.14.1부터 Active IQ Unified Manager 스토리지 가상 머신(SVM, 이전에는 Vserver라고 함) 수준에서 OCSP(온라인 인증서 상태 프로토콜) 상태 정보를 제공합니다. 즉, OCSP 검증은 SVM에 대한 모든 SSL/TLS 연결에 적용되며 이러한 연결에 사용된 인증서의 무결성과 유효성을 보장합니다.	활성화됨	아니요
원격 감사 로깅	로그 전달(Syslog)이 암호화되었는지 여부를 나타냅니다.	암호화됨	예

매개변수	설명	추천	클러스터 규정 준수에 영향을 미칩니다
AutoSupport HTTPS 전송	NetApp 지원팀에 AutoSupport 메시지를 보낼 때 HTTPS가 기본 전송 프로토콜로 사용되는지 여부를 나타냅니다.	활성화됨	예
기본 관리자 사용자	기본 관리자 사용자(기본 제공)가 활성화되어 있는지 비활성화되어 있는지를 나타냅니다. NetApp 불필요한 기본 제공 계정을 잠그거나 비활성화할 것을 권장합니다.	장애가 있는	예
SAML 사용자	SAML이 구성되었는지 여부를 나타냅니다. SAML을 사용하면 Single Sign-On에 대한 로그인 방법으로 다중 인증 요소(MFA)를 구성할 수 있습니다.	아니요	아니요
Active Directory 사용자	Active Directory가 구성되었는지 여부를 나타냅니다. Active Directory와 LDAP는 클러스터에 액세스하는 사용자에게 선호되는 인증 메커니즘입니다.	아니요	아니요
LDAP 사용자	LDAP가 구성되었는지 여부를 나타냅니다. Active Directory와 LDAP는 로컬 사용자보다 클러스터를 관리하는 사용자에게 선호되는 인증 메커니즘입니다.	아니요	아니요
인증서 사용자	인증서 사용자가 클러스터에 로그인하도록 구성되었는지 여부를 나타냅니다.	아니요	아니요
로컬 사용자	로컬 사용자가 클러스터에 로그인하도록 구성되었는지 여부를 나타냅니다.	아니요	아니요

매개변수	설명	추천	클러스터 규정 준수에 영향을 미칩니다
원격 셸	RSH가 활성화되어 있는지 여부를 나타냅니다. 보안상의 이유로 RSH를 비활성화해야 합니다. 안전한 원격 액세스를 위해서는 Secure Shell(SSH)을 사용하는 것이 좋습니다.	장애가 있는	예
MD5 사용 중	ONTAP 사용자 계정에서 보안 수준이 낮은 MD5 해시 함수를 사용하는지 여부를 나타냅니다. MD5 해시된 사용자 계정은 SHA-512와 같은 보다 안전한 암호화 해시 함수로 마이그레이션하는 것이 좋습니다.	아니요	예
인증서 발급자 유형	사용된 디지털 인증서의 유형을 나타냅니다.	CA 서명	아니요

스토리지 VM 규정 준수 범주

이 표에서는 Unified Manager가 평가하는 스토리지 가상 머신(SVM) 보안 준수 기준, NetApp 권장 사항, 그리고 매개변수가 SVM이 전반적으로 적합 판정에 영향을 미치는지 여부를 설명합니다.

매개변수	설명	추천	SVM 규정 준수에 영향을 미칩니다
감사 로그	감사 로깅이 활성화되어 있는지 비활성화되어 있는지를 나타냅니다.	활성화됨	예
안전하지 않은 SSH 설정	SSH가 안전하지 않은 암호(예: 로 시작하는 암호)를 사용하는지 여부를 나타냅니다. cbc* .	아니요	예
로그인 배너	시스템의 SVM에 액세스하는 사용자에게 대해 로그인 배너가 활성화되어 있는지 비활성화되어 있는지 여부를 나타냅니다.	활성화됨	예

매개변수	설명	추천	SVM 규정 준수에 영향을 미칩니다
LDAP 암호화	LDAP 암호화가 활성화되어 있는지 비활성화되어 있는지를 나타냅니다.	활성화됨	아니요
NTLM 인증	NTLM 인증이 활성화되어 있는지 비활성화되어 있는지를 나타냅니다.	활성화됨	아니요
LDAP 페이로드 서명	LDAP 페이로드 서명이 활성화되어 있는지 비활성화되어 있는지를 나타냅니다.	활성화됨	아니요
CHAP 설정	CHAP가 활성화되어 있는지 비활성화되어 있는지를 나타냅니다.	활성화됨	아니요
케르베로스 V5	Kerberos V5 인증이 활성화되어 있는지 비활성화되어 있는지를 나타냅니다.	활성화됨	아니요
NIS 인증	NIS 인증 사용이 구성되었는지 여부를 나타냅니다.	장애가 있는	아니요
FPolicy 상태 활성화	FPolicy가 생성되었는지 여부를 나타냅니다.	예	아니요
SMB 암호화 활성화됨	SMB 서명 및 봉인이 활성화되어 있지 않은지 여부를 나타냅니다.	예	아니요
SMB 서명 활성화됨	SMB 서명이 활성화되어 있지 않은지 여부를 나타냅니다.	예	아니요

볼륨 준수 범주

이 표에서는 Unified Manager가 볼륨의 데이터가 무단 사용자의 액세스로부터 적절하게 보호되는지 여부를 판단하기 위해 평가하는 볼륨 암호화 매개변수를 설명합니다.

볼륨 암호화 매개변수는 클러스터 또는 스토리지 VM이 규정을 준수하는 것으로 간주되는지 여부에 영향을 미치지 않습니다.

매개변수	설명
소프트웨어 암호화	NetApp Volume Encryption(NVE) 또는 NetApp Aggregate Encryption(NAE) 소프트웨어 암호화 솔루션을 사용하여 보호되는 볼륨 수를 표시합니다.
하드웨어 암호화	NetApp Storage Encryption(NSE) 하드웨어 암호화를 사용하여 보호되는 볼륨 수를 표시합니다.
소프트웨어 및 하드웨어 암호화	소프트웨어 및 하드웨어 암호화로 보호되는 볼륨 수를 표시합니다.
암호화되지 않음	암호화되지 않은 볼륨의 수를 표시합니다.

규정을 준수하지 않는다는 것은 무엇을 의미합니까?

클러스터와 스토리지 가상 머신(SVM)은 NetApp 보안 강화 가이드 for ONTAP 9에 정의된 권장 사항에 대해 평가되는 보안 기준 중 하나라도 충족하지 못할 경우 규정을 준수하지 않는 것으로 간주됩니다. 또한, SVM 중 하나가 규정을 준수하지 않는 것으로 표시되면 클러스터는 규정을 준수하지 않는 것으로 간주됩니다.

보안 카드의 상태 아이콘은 규정 준수 여부에 따라 다음과 같은 의미를 갖습니다.

-  - 매개변수는 권장사항에 따라 구성되었습니다.
-  - 매개변수가 권장되는 대로 구성되지 않았습니다.
-  - 클러스터에서 해당 기능이 활성화되지 않았거나 매개변수가 권장 사항대로 구성되지 않았지만, 이 매개변수는 개체의 규정 준수에 기여하지 않습니다.

볼륨 암호화 상태는 클러스터나 SVM이 규정을 준수하는 것으로 간주되는지 여부에 영향을 미치지 않습니다.

클러스터 및 스토리지 **VM**의 보안 상태 보기

Active IQ Unified Manager 사용하면 인터페이스의 다양한 지점에서 환경 내 스토리지 개체의 보안 상태를 볼 수 있습니다. 정의된 매개변수를 기반으로 정보와 보고서를 수집하고 분석하고, 모니터링되는 클러스터와 스토리지 VM에서 의심스러운 동작이나 승인되지 않은 시스템 변경을 감지할 수 있습니다.

보안 권장 사항은 다음을 참조하세요. "[ONTAP 9를 위한 NetApp 보안 강화 가이드](#)"

보안 페이지에서 개체 수준 보안 상태 보기

시스템 관리자는 보안 페이지를 사용하여 데이터 센터 및 사이트 수준에서 ONTAP 클러스터와 스토리지 VM의 보안 강도를 파악할 수 있습니다. 지원되는 개체는 클러스터, 스토리지 VM, 볼륨입니다. 다음 단계를 따르세요.

단계

1. 왼쪽 탐색 창에서 *대시보드*를 클릭합니다.
2. 모니터링되는 모든 클러스터의 보안 상태를 볼지 또는 단일 클러스터의 보안 상태를 볼지에 따라 *모든 클러스터*

선택하거나 드롭다운 메뉴에서 단일 클러스터를 선택합니다.

3. 보안 패널에서 오른쪽 화살표를 클릭합니다. 보안 페이지가 표시됩니다.

막대형 차트, 개수 등을 클릭하면 View Reports 링크를 클릭하면 볼륨, 클러스터 또는 스토리지 VM 페이지로 이동하여 필요에 따라 해당 세부 정보를 보거나 보고서를 생성할 수 있습니다.

보안 페이지에는 다음 패널이 표시됩니다.

- 클러스터 규정 준수: 데이터 센터의 모든 클러스터의 보안 상태(규정을 준수하거나 준수하지 않는 클러스터 수)
- 저장소 **VM** 규정 준수: 데이터 센터의 모든 저장 VM에 대한 보안 상태(규정을 준수하거나 준수하지 않는 저장 VM 수)
- 볼륨 암호화: 사용자 환경의 모든 볼륨의 볼륨 암호화 상태(암호화되었거나 암호화되지 않은 볼륨 수)
- 볼륨 랜섬웨어 방지 상태: 사용자 환경의 모든 볼륨의 보안 상태(랜섬웨어 방지가 활성화 또는 비활성화된 볼륨 수)
- 클러스터 인증 및 인증서: SAML, Active Directory 또는 인증서 및 로컬 인증과 같은 각 유형의 인증 방법을 사용하는 클러스터 수입니다. 패널에는 인증서가 만료되었거나 60일 후에 만료될 예정인 클러스터 수도 표시됩니다.

클러스터 페이지에서 모든 클러스터의 보안 세부 정보를 확인하세요.

클러스터/보안 세부 정보 페이지에서는 클러스터 수준의 보안 준수 상태를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *저장소 > 클러스터*를 클릭합니다.
2. *보기 > 보안 > 모든 클러스터*를 선택합니다.

글로벌 FIPS, Telnet, 안전하지 않은 SSH 설정, 로그인 배너, 네트워크 시간 프로토콜, AutoSupport HTTPS 전송, 클러스터 인증서 만료 상태와 같은 기본 보안 매개변수가 표시됩니다.

클릭할 수 있습니다: 추가 옵션 버튼을 클릭하고 Unified Manager의 보안 페이지 또는 System Manager에서 보안 세부 정보를 볼 수 있습니다. 시스템 관리자에서 세부 정보를 보려면 유효한 자격 증명이 있어야 합니다.



클러스터에 만료된 인증서가 있는 경우 다음을 클릭할 수 있습니다. expired *클러스터 인증서 유효성*에서 System Manager(9.10.1 이상)에서 갱신하세요. 클릭할 수 없습니다 expired 시스템 관리자 인스턴스가 9.10.1 이전 릴리스인 경우.

스토리지 **VM** 페이지에서 모든 클러스터의 보안 세부 정보를 확인하세요.

저장소 **VM**/보안 세부 정보 페이지에서는 저장소 VM 수준의 보안 준수 상태를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *저장소 > 저장소 VM*을 클릭합니다.
2. *보기 > 보안 > 모든 저장소 VM*을 선택합니다. 보안 매개변수가 포함된 클러스터 목록이 표시됩니다.

스토리지 VM, 클러스터, 로그인 배너, 감사 로그, 안전하지 않은 SSH 설정 등의 보안 매개변수를 확인하여 스토리지 VM의 보안 준수 여부에 대한 기본 보기를 가질 수 있습니다.

클릭할 수 있습니다: 추가 옵션 버튼을 클릭하고 Unified Manager의 보안 페이지 또는 System Manager에서 보안 세부 정보를 볼 수 있습니다. 시스템 관리자에서 세부 정보를 보려면 유효한 자격 증명이 있어야 합니다.

볼륨 및 스토리지 VM에 대한 랜섬웨어 방지 보안 세부 정보는 다음을 참조하세요. "[모든 볼륨 및 스토리지 VM의 랜섬웨어 방지 상태 보기](#)".

소프트웨어 또는 펌웨어 업데이트가 필요할 수 있는 보안 이벤트 보기

"업그레이드"의 영향 영역이 있는 특정 보안 이벤트가 있습니다. 이러한 이벤트는 Active IQ 플랫폼에서 보고되며, 보안 권고에 따라 ONTAP 소프트웨어, 노드 펌웨어 또는 운영 체제 소프트웨어를 업그레이드해야 하는 문제를 식별합니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

일부 문제는 즉시 시정 조치를 취해야 할 수도 있지만, 다른 문제는 다음에 예정된 유지 관리까지 기다릴 수 있습니다. 이러한 모든 이벤트를 보고 문제를 해결할 수 있는 사용자에게 할당할 수 있습니다. 또한, 알림을 받고 싶지 않은 특정 보안 업그레이드 이벤트가 있는 경우 이 목록을 통해 해당 이벤트를 식별하여 비활성화할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭합니다.

기본적으로 모든 활성(신규 및 확인됨) 이벤트는 이벤트 관리 인벤토리 페이지에 표시됩니다.

2. 보기 메뉴에서 *이벤트 업그레이드*를 선택합니다.

이 페이지에는 모든 활성 업그레이드 보안 이벤트가 표시됩니다.

모든 클러스터에서 사용자 인증이 어떻게 관리되는지 확인하세요.

보안 페이지에는 각 클러스터에서 사용자를 인증하는 데 사용되는 인증 유형과 각 유형을 사용하여 클러스터에 액세스하는 사용자 수가 표시됩니다. 이를 통해 조직에서 정의한 대로 사용자 인증이 안전하게 수행되는지 확인할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *대시보드*를 클릭합니다.
2. 대시보드 상단의 드롭다운 메뉴에서 *모든 클러스터*를 선택합니다.
3. 보안 패널에서 오른쪽 화살표를 클릭하면 보안 페이지가 표시됩니다.
4. 클러스터 인증 카드를 보면 각 인증 유형을 사용하여 시스템에 액세스하는 사용자 수를 확인할 수 있습니다.
5. 클러스터 보안 카드를 보고 각 클러스터에서 사용자를 인증하는 데 사용되는 인증 메커니즘을 확인하세요.

일부 사용자가 안전하지 않은 방법을 사용하거나 NetApp에서 권장하지 않는 방법을 사용하여 시스템에 액세스하는 경우 해당 방법을 비활성화할 수 있습니다.

모든 볼륨의 암호화 상태 보기

모든 볼륨과 현재 암호화 상태 목록을 보고 볼륨의 데이터가 무단 사용자의 접근으로부터 적절하게 보호되고 있는지 확인할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨에 적용할 수 있는 암호화 유형은 다음과 같습니다.

- 소프트웨어 - NetApp Volume Encryption(NVE) 또는 NetApp Aggregate Encryption(NAE) 소프트웨어 암호화 솔루션을 사용하여 보호되는 볼륨입니다.
- 하드웨어 - NetApp Storage Encryption(NSE) 하드웨어 암호화를 사용하여 보호되는 볼륨입니다.
- 소프트웨어 및 하드웨어 - 소프트웨어와 하드웨어 암호화로 보호되는 볼륨입니다.
- 없음 - 암호화되지 않은 볼륨입니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 상태 > *볼륨 암호화*를 선택합니다.
3. 상태: 볼륨 암호화 보기에서 암호화 유형 필드를 기준으로 정렬하거나 필터를 사용하여 특정 암호화 유형을 갖는 볼륨이나 암호화되지 않은 볼륨(암호화 유형이 "없음"인 볼륨)을 표시합니다.

모든 볼륨 및 스토리지 **VM**의 랜섬웨어 방지 상태 보기

모든 볼륨과 스토리지 VM(SVM) 목록과 현재 랜섬웨어 방지 상태를 확인하여 볼륨과 SVM의 데이터가 랜섬웨어 공격으로부터 적절하게 보호되고 있는지 확인할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다양한 랜섬웨어 방지 상태에 대한 자세한 내용은 다음을 참조하세요. "[ONTAP: 랜섬웨어 방지 기능 활성화](#)".

랜섬웨어 탐지 기능으로 모든 볼륨의 보안 세부 정보 보기

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 상태 > 보안 > *랜섬웨어 방지*를 선택하세요.
3. 보안: 랜섬웨어 방지 보기에서는 다양한 필드별로 정렬하거나 필터를 사용할 수 있습니다.



랜섬웨어 방지 기능은 오프라인 볼륨, 제한된 볼륨, SnapLock 볼륨, FlexGroup 볼륨, FlexCache 볼륨, SAN 전용 볼륨, 중지된 스토리지 VM의 볼륨, 스토리지 VM의 루트 볼륨 또는 데이터 보호 볼륨에 지원되지 않습니다.

랜섬웨어 감지 기능을 통해 모든 스토리지 **VM**의 보안 세부 정보를 확인하세요.

단계

1. 왼쪽 탐색 창에서 *저장소 > 저장소 VM*을 클릭합니다.
2. *보기 > 보안 > 랜섬웨어 방지*를 선택합니다. 랜섬웨어 방지 상태가 있는 SVM 목록이 표시됩니다.



NAS 프로토콜이 활성화되지 않은 스토리지 VM에서는 랜섬웨어 방지 모니터링이 지원되지 않습니다.

모든 활성 보안 이벤트 보기

모든 활성 보안 이벤트를 보고 각 이벤트를 문제를 해결할 수 있는 사용자에게 할당할 수 있습니다. 또한, 수신하고 싶지 않은 특정 보안 이벤트가 있는 경우 이 목록을 통해 비활성화하려는 이벤트를 식별할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭합니다.

기본적으로 새 이벤트와 확인된 이벤트는 이벤트 관리 인벤토리 페이지에 표시됩니다.

2. 보기 메뉴에서 *활성 보안 이벤트*를 선택합니다.

이 페이지에는 지난 7일 동안 생성된 모든 새 보안 이벤트와 확인된 보안 이벤트가 표시됩니다.

보안 이벤트에 대한 알림 추가

Unified Manager에서 수신한 다른 이벤트와 마찬가지로 개별 보안 이벤트에 대한 알림을 구성할 수 있습니다. 또한, 모든 보안 이벤트를 동일하게 처리하고 같은 사람에게 이메일을 보내려는 경우 보안 이벤트가 발생할 때마다 알려주는 단일 알림을 만들 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

아래 예에서는 "Telnet Protocol Enabled" 보안 이벤트에 대한 알림을 만드는 방법을 보여줍니다. 클러스터에 대한 원격 관리 액세스를 위해 Telnet 액세스가 구성된 경우 경고가 전송됩니다. 동일한 방법을 사용하여 모든 보안 이벤트에 대한 알림을 생성할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *알림 설정*을 클릭합니다.
2. 알림 설정 페이지에서 *추가*를 클릭합니다.
3. 알림 추가 대화 상자에서 *이름*을 클릭하고 알림의 이름과 설명을 입력합니다.
4. *리소스*를 클릭하고 이 알림을 활성화하려는 클러스터 또는 클러스터를 선택합니다.
5. *이벤트*를 클릭하고 다음 작업을 수행하세요.
 - a. 이벤트 심각도 목록에서 *경고*를 선택합니다.
 - b. 일치하는 이벤트 목록에서 *Telnet 프로토콜 사용*을 선택합니다.
6. 작업*을 클릭한 다음 *다음 사용자에게 알림 필드에서 알림 이메일을 받을 사용자의 이름을 선택합니다.
7. 이 페이지에서 알림 빈도, SNMP 탭 발행, 스크립트 실행에 대한 다른 옵션을 구성합니다.
8. *저장*을 클릭하세요.

특정 보안 이벤트 비활성화

모든 이벤트는 기본적으로 활성화되어 있습니다. 사용자 환경에서 중요하지 않은 이벤트에 대한 알림이 생성되지 않도록 하려면 특정 이벤트를 비활성화할 수 있습니다. 비활성화된 이벤트에 대한 알림을 다시 받으려면 해당 이벤트를 활성화하면 됩니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이벤트를 비활성화하면 시스템에서 이전에 생성된 이벤트는 더 이상 사용되지 않는 것으로 표시되고, 이러한 이벤트에 대해 구성된 알림은 트리거되지 않습니다. 비활성화된 이벤트를 활성화하면 다음 모니터링 주기부터 해당 이벤트에 대한 알림이 생성됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *이벤트 설정*을 클릭합니다.
2. 이벤트 설정 페이지에서 다음 옵션 중 하나를 선택하여 이벤트를 비활성화하거나 활성화합니다.

만약 당신이 원한다면...	그러면 이렇게 하세요...
이벤트 비활성화	a. *비활성화*를 클릭합니다. b. 이벤트 비활성화 대화 상자에서 경고 심각도를 선택합니다. 이는 모든 보안 이벤트에 대한 카테고리입니다. c. 일치하는 이벤트 열에서 비활성화하려는 보안 이벤트를 선택한 다음 오른쪽 화살표를 클릭하여 해당 이벤트를 비활성화 이벤트 열로 이동합니다. d. *저장 및 닫기*를 클릭하세요. e. 비활성화한 이벤트가 이벤트 설정 페이지의 목록 보기에 표시되는지 확인하세요.
이벤트 활성화	a. 비활성화된 이벤트 목록에서 다시 활성화하려는 이벤트의 확인란을 선택합니다. b. *활성화*를 클릭합니다.

보안 이벤트

보안 이벤트는 _NetApp 보안 강화 가이드 for ONTAP 9_에 정의된 매개변수를 기반으로 ONTAP 클러스터, 스토리지 가상 머신(SVM) 및 볼륨의 보안 상태에 대한 정보를 제공합니다. 이러한 이벤트는 잠재적인 문제를 알려주므로 문제의 심각성을 평가하고 필요한 경우 문제를 해결할 수 있습니다.

보안 이벤트는 소스 유형별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 심각도가 포함됩니다. 이러한 이벤트는 클러스터 및 스토리지 VM 이벤트 범주에 나타납니다.

백업 및 복원 작업 관리

Active IQ Unified Manager의 백업을 만들고 복원 기능을 사용하여 시스템 장애 또는 데이터 손실 시 동일한(로컬) 시스템이나 새(원격) 시스템에 백업을 복원할 수 있습니다.

Unified Manager를 설치한 운영 체제와 관리되는 클러스터 및 노드 수에 따라 세 가지 백업 및 복원 방법이 있습니다.

운영 체제	배포 크기	권장 백업 방법
VMware vSphere	어느	Unified Manager 가상 어플라이언스의 VMware 스냅샷
레드햇 엔터프라이즈 리눅스	작은	Unified Manager MySQL 데이터베이스 덤프
	크기가 큰	Unified Manager 데이터베이스의 NetApp 스냅샷
마이크로소프트 윈도우	작은	Unified Manager MySQL 데이터베이스 덤프
	크기가 큰	iSCSI 프로토콜을 사용한 Unified Manager 데이터베이스의 NetApp 스냅샷

다음 섹션에서는 다양한 방법을 설명합니다.

가상 어플라이언스에서 **Unified Manager**에 대한 백업 및 복원

가상 어플라이언스에 설치된 Unified Manager의 백업 및 복원 모델은 전체 가상 애플리케이션의 이미지를 캡처하고 복원하는 것입니다.

다음 작업을 통해 가상 어플라이언스의 백업을 완료할 수 있습니다.

1. VM의 전원을 끄고 Unified Manager 가상 어플라이언스의 VMware 스냅샷을 만듭니다.
2. 데이터스토어에 NetApp 스냅샷 복사본을 만들어 VMware 스냅샷을 캡처합니다.

데이터 저장소가 ONTAP 소프트웨어를 실행하는 시스템에 호스팅되지 않은 경우 스토리지 공급업체의 지침에 따라 VMware 스냅샷의 백업을 생성하세요.

3. NetApp 스냅샷 복사본이나 스냅샷과 동등한 것을 대체 스토리지에 복제합니다.
4. VMware 스냅샷을 삭제합니다.

문제가 발생할 경우 Unified Manager 가상 어플라이언스가 보호되도록 이러한 작업을 사용하여 백업 일정을 구현해야 합니다.

VM을 복원하려면 생성한 VMware 스냅샷을 사용하여 VM을 백업 시점 상태로 복원할 수 있습니다.

MySQL 데이터베이스 덤프를 사용한 백업 및 복원

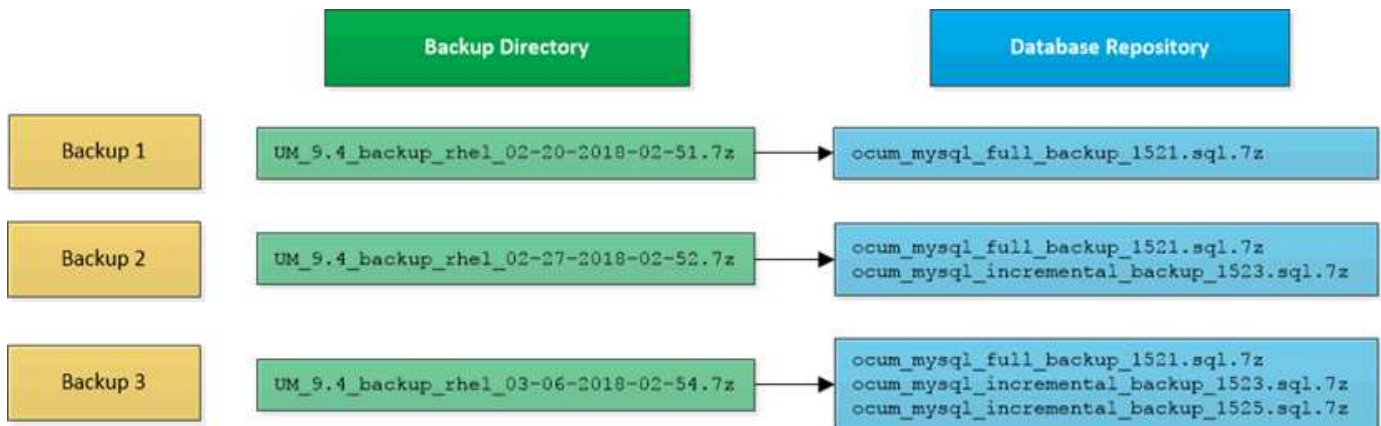
MySQL 데이터베이스 덤프 백업은 시스템 오류나 데이터 손실이 발생한 경우 사용할 수 있는 Active IQ Unified Manager 데이터베이스 및 구성 파일의 사본입니다. 로컬 대상이나 원격 대상에 백업을 기록하도록 예약할 수 있습니다. Active IQ Unified Manager 호스트 시스템 외부에 있는 원격 위치를 정의하는 것이 좋습니다.



Unified Manager가 Linux 및 Windows 서버에 설치되면 MySQL 데이터베이스 덤프가 기본 백업 메커니즘이 됩니다. 하지만 Unified Manager가 많은 수의 클러스터와 노드를 관리하거나 MySQL 백업을 완료하는 데 많은 시간이 걸리는 경우 스냅샷 복사본을 사용하여 백업할 수 있습니다. 이 기능은 Red Hat Enterprise Linux와 Windows에서 사용할 수 있습니다.

데이터베이스 덤프 백업은 백업 디렉토리의 단일 파일과 데이터베이스 저장소 디렉토리의 하나 이상의 파일로 구성됩니다. 백업 디렉토리의 파일은 백업을 다시 만드는 데 필요한 데이터베이스 저장소 디렉토리에 있는 파일에 대한 포인터만 포함하고 있기 때문에 매우 작습니다.

처음으로 데이터베이스 백업을 생성하면 백업 디렉토리에 단일 파일이 생성되고 데이터베이스 저장소 디렉토리에 전체 백업 파일이 생성됩니다. 다음에 백업을 생성하면 백업 디렉토리에 단일 파일이 생성되고 전체 백업 파일과의 차이점이 포함된 증분 백업 파일이 데이터베이스 저장소 디렉토리에 생성됩니다. 다음 그림에서 볼 수 있듯이, 최대 보존 설정까지 추가 백업을 생성하면서 이 프로세스가 계속됩니다.



이 두 디렉토리에 있는 백업 파일의 이름을 바꾸거나 제거하지 마세요. 그렇지 않으면 이후의 복원 작업이 실패합니다.

백업 파일을 로컬 시스템에 쓰는 경우, 전체 복원이 필요한 시스템 문제가 발생할 경우를 대비해 백업 파일을 원격 위치로 복사하는 프로세스를 시작해야 합니다.

백업 작업을 시작하기 전에 Active IQ Unified Manager 무결성 검사를 수행하여 필요한 모든 백업 파일과 백업 디렉토리가 존재하고 쓰기 가능한지 확인합니다. 또한 시스템에 백업 파일을 만들 수 있는 충분한 공간이 있는지 확인합니다.

데이터베이스 덤프 백업의 대상 및 일정을 구성합니다.

Unified Manager 데이터베이스 덤프 백업 설정을 구성하여 데이터베이스 백업 경로, 보존 횟수 및 백업 일정을 설정할 수 있습니다. 매일 또는 매주 예약된 백업을 활성화할 수 있습니다. 기본적으로 예약된 백업은 비활성화되어 있지만 백업 일정을 설정해야 합니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 백업 경로로 정의한 위치에는 최소 150GB의 사용 가능한 공간이 있어야 합니다.

Unified Manager 호스트 시스템 외부의 원격 위치를 사용하는 것이 좋습니다.

- Linux 시스템에 Unified Manager를 설치하고 MySQL 백업을 사용하는 경우 백업 디렉토리에 다음 권한과 소유권이 설정되어 있는지 확인하세요.

권한: 0750, 소유권: jboss:maintenance

- Unified Manager가 Windows 시스템에 설치되고 MySQL 백업을 사용하는 경우, 관리자만 백업 디렉토리에 액세스할 수 있도록 해야 합니다.

첫 번째 백업은 전체 백업이기 때문에 후속 백업보다 처음 백업을 수행할 때 더 많은 시간이 필요합니다. 전체 백업은 1GB가 넘을 수 있으며 3~4시간이 걸릴 수 있습니다. 이후 백업은 증분식으로 진행되므로 시간이 덜 걸립니다.



- 백업에 할당된 공간에 비해 증분 백업 파일의 수가 너무 많다고 생각되면 주기적으로 전체 백업을 수행하여 이전 백업과 증분 파일을 대체할 수 있습니다. 또 다른 옵션으로 스냅샷 복사본을 사용하여 백업을 수행할 수 있습니다.
- 새로운 클러스터를 추가한 후 처음 15일 동안 수행한 백업은 과거 성능 데이터를 얻기에 충분히 정확하지 않을 수 있습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *데이터베이스 백업*을 클릭합니다.
2. 데이터베이스 백업 페이지에서 *백업 설정*을 클릭합니다.
3. 백업 경로, 보존 횟수 및 일정에 적합한 값을 구성합니다.

보존 횟수의 기본값은 10입니다. 무제한 백업을 생성하려면 0을 사용할 수 있습니다.

4. 매일 예약 또는 매주 예약 버튼을 선택한 다음, 일정 세부 정보를 지정합니다.
5. *적용*을 클릭하세요.

데이터베이스 덤프 백업 파일은 일정에 따라 생성됩니다. 사용 가능한 백업 파일은 데이터베이스 백업 페이지에서 볼 수 있습니다.

데이터베이스 복원이란 무엇인가

MySQL 데이터베이스 복원은 기존 Unified Manager 백업 파일을 동일하거나 다른 Unified Manager 서버로 복원하는 프로세스입니다. Unified Manager 유지 관리 콘솔에서 복원 작업을 수행합니다.

동일한(로컬) 시스템에서 복원 작업을 수행하고 백업 파일이 모두 로컬에 저장된 경우 기본 위치를 사용하여 복원 옵션을 실행할 수 있습니다. 다른 Unified Manager 시스템(원격 시스템)에서 복원 작업을 수행하는 경우 복원 옵션을 실행하기 전에 보조 저장소에서 백업 파일을 로컬 디스크로 복사해야 합니다.

복원 프로세스 중에는 Unified Manager에서 로그아웃됩니다. 복원 프로세스가 완료되면 시스템에 로그인할 수 있습니다.

백업 이미지를 새 서버로 복원하는 경우 복원 작업이 완료된 후 새 HTTPS 보안 인증서를 생성하고 Unified Manager

서버를 다시 시작해야 합니다. 백업 이미지를 새 서버로 복원할 때 필요한 경우 SAML 인증 설정도 재구성해야 합니다.



Unified Manager가 최신 버전의 소프트웨어로 업그레이드된 후에는 이전 백업 파일을 사용하여 이미지를 복원할 수 없습니다. 공간을 절약하기 위해 Unified Manager를 업그레이드하면 최신 파일을 제외한 모든 이전 백업 파일이 자동으로 제거됩니다.

관련 정보

["HTTPS 보안 인증서 생성"](#)

["SAML 인증 활성화"](#)

["Active Directory 또는 OpenLDAP를 통한 인증"](#)

Windows에서 MySQL 데이터베이스 백업 복원

데이터 손실이나 데이터 손상이 발생한 경우 복원 기능을 사용하여 최소한의 손실로 Unified Manager를 이전의 안정적인 상태로 복원할 수 있습니다. Unified Manager 유지 관리 콘솔을 사용하여 Unified Manager MySQL 데이터베이스를 로컬 Windows 시스템이나 원격 Windows 시스템으로 복원할 수 있습니다.

시작하기 전에

- Windows 관리자 권한이 있어야 합니다.
- 복원 작업을 수행할 시스템에 Unified Manager 백업 파일과 데이터베이스 저장소 디렉토리의 내용을 복사해야 합니다.

백업 파일을 기본 디렉토리에 복사하는 것이 좋습니다.

`\ProgramData\NetApp\OnCommandAppData\ocum\backup` . 데이터베이스 저장소 파일을 복사해야 합니다. `\database_dumps_repo` 하위 디렉토리 `\backup` 예매 규칙서.

- 백업 파일은 다음과 같아야 합니다. `.7z` 유형.

복원 기능은 플랫폼과 버전에 따라 다릅니다. Unified Manager MySQL 백업은 동일한 버전의 Unified Manager에서만 복원할 수 있으며, Windows 백업은 Windows 플랫폼에서만 복원할 수 있습니다.



폴더 이름에 공백이 포함된 경우 백업 파일의 절대 경로 또는 상대 경로를 큰따옴표로 묶어야 합니다.

단계

1. Unified Manager를 설치한 후에는 새 서버로 복원을 수행하는 경우 UI를 시작하거나 설치가 완료된 후 클러스터, 사용자 또는 인증 설정을 구성하지 마세요. 백업 파일은 복원 과정 중에 이 정보를 채웁니다.
2. 관리자 자격 증명을 사용하여 Unified Manager 시스템에 로그인합니다.
3. Windows 관리자 권한으로 PowerShell이나 명령 프롬프트를 실행합니다.
4. 명령을 입력하세요 `maintenance_console` 그리고 Enter를 누르세요.
5. 유지 관리 콘솔의 메인 메뉴*에서 *백업 복원 옵션에 대한 번호를 입력합니다.
6. *MySQL 백업 복원*에 대한 번호를 입력하세요.
7. 메시지가 표시되면 백업 파일의 절대 경로를 입력합니다.

```
Bundle to restore from:
\ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_bac
kup_windows_02-20-2020-02-51.7z
```

복원 작업이 완료되면 Unified Manager에 로그인할 수 있습니다.

백업을 복원한 후 OnCommand Workflow Automation 서버가 작동하지 않으면 다음 단계를 수행하세요.

1. Workflow Automation 서버에서 Unified Manager 서버의 IP 주소를 최신 컴퓨터를 가리키도록 변경합니다.
2. Unified Manager 서버에서 1단계에서 획득에 실패하면 데이터베이스 비밀번호를 재설정합니다.

NetApp 스냅샷을 사용한 백업 및 복원

NetApp 스냅샷 복사본은 시스템 장애나 데이터 손실이 발생한 경우 복원하는 데 사용할 수 있는 Unified Manager 데이터베이스와 구성 파일의 특정 시점 이미지를 생성합니다. ONTAP 클러스터 중 하나의 볼륨에 스냅샷 복사본을 주기적으로 기록하도록 예약하면 항상 최신 복사본을 보유할 수 있습니다.



이 기능은 가상 어플라이언스에 설치된 Active IQ Unified Manager에서는 사용할 수 없습니다.

Linux에서 백업 구성

Active IQ Unified Manager Linux 시스템에 설치된 경우 NetApp Snapshots를 사용하여 백업 및 복원을 구성할 수 있습니다.

스냅샷 복사는 일반적으로 몇 분 정도 소요되며, Unified Manager 데이터베이스는 매우 짧은 시간 동안만 잠기므로 설치가 중단되는 일이 거의 없습니다. 이미지는 최소한의 저장 공간을 사용하고 마지막 스냅샷 복사본이 만들어진 이후 파일의 변경 사항만 기록하므로 성능 오버헤드가 무시할 수 있을 정도입니다. 스냅샷은 ONTAP 클러스터에서 생성되므로 필요한 경우 SnapMirror와 같은 다른 NetApp 기능을 활용하여 보조 보호 기능을 만들 수 있습니다.

백업 작업을 시작하기 전에 Unified Manager는 무결성 검사를 수행하여 대상 시스템을 사용할 수 있는지 확인합니다.



- 동일한 버전의 Active IQ Unified Manager에서만 스냅샷 사본을 복원할 수 있습니다.

예를 들어 Unified Manager 9.16에서 백업을 만든 경우 해당 백업은 Unified Manager 9.16 시스템에서만 복원할 수 있습니다.

- 스냅샷 구성에 변경 사항이 있는 경우 스냅샷이 유효하지 않게 될 수 있습니다.

스냅샷 복사 위치 구성

ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 ONTAP 클러스터 중 하나에 스냅샷 복사본이 저장될 볼륨을 구성할 수 있습니다.

시작하기 전에

클러스터, 스토리지 VM 및 볼륨은 다음 요구 사항을 충족해야 합니다.

- 클러스터 요구 사항:
 - ONTAP 9.3 이상이 설치되어 있어야 합니다.
 - Unified Manager 서버와 지리적으로 가까워야 합니다.
 - Unified Manager로 모니터링이 가능하지만 필수는 아닙니다.
- 스토리지 VM 요구 사항:
 - 이름 스위치와 이름 매핑은 "files"를 사용하도록 설정해야 합니다.
 - 클라이언트 측 사용자와 통신하기 위해 생성된 로컬 사용자
 - 모든 읽기/쓰기 액세스가 선택되었는지 확인하세요.
 - 내보내기 정책에서 Superuser Access가 "any"로 설정되어 있는지 확인하세요.
 - Linux용 NetApp 스냅샷을 위한 NFS
 - NFSv4는 NFS 서버에서 활성화되어야 하며 클라이언트와 스토리지 VM에 지정된 NFSv4 ID 도메인이 필요합니다.
 - 볼륨은 Unified Manager/opt/netapp/data 디렉토리 크기의 최소 두 배여야 합니다.

du -sh /opt/netapp/data/ 명령을 사용하여 현재 크기를 확인합니다.
- 볼륨 요구 사항:
 - 볼륨은 Unified Manager /opt/netapp/data 디렉토리 크기의 최소 두 배여야 합니다.
 - 보안 스타일은 UNIX로 설정해야 합니다.
 - 로컬 스냅샷 정책을 비활성화해야 합니다.
 - 볼륨 자동 크기 조정을 활성화해야 합니다.
 - 성능 서비스 수준은 "Extreme"과 같이 높은 IOPS와 낮은 지연 시간을 갖는 정책으로 설정되어야 합니다.

NFS 볼륨을 생성하는 자세한 단계는 다음을 참조하세요. ["ONTAP 9에서 NFSv4를 구성하는 방법"](#) 그리고 ["ONTAP 9 NFS 구성 익스프레스 가이드"](#).

스냅샷 복사본의 대상 위치를 지정합니다.

ONTAP 클러스터 중 하나에 이미 구성한 볼륨에서 Active IQ Unified Manager 스냅샷 복사본의 대상 위치를 구성해야 합니다. 위치를 정의하려면 유지 관리 콘솔을 사용해야 합니다.

- Active IQ Unified Manager 설치된 Linux 호스트에 대한 루트 사용자 자격 증명이 있어야 합니다.
- Unified Manager 서버의 유지 관리 콘솔에 로그인하려면 권한이 있는 사용자 ID와 비밀번호가 있어야 합니다.
- 클러스터 관리 IP 주소, 스토리지 VM 이름, 볼륨 이름, 스토리지 시스템 사용자 이름과 비밀번호가 있어야 합니다.
- 볼륨을 Active IQ Unified Manager 호스트에 마운트해야 하며, 마운트 경로가 있어야 합니다.

단계

1. Secure Shell을 사용하여 Active IQ Unified Manager 시스템의 IP 주소 또는 FQDN에 연결합니다.
2. 유지 관리 사용자(umadmin) 이름과 비밀번호로 시스템에 로그인합니다.
3. 명령을 입력하세요 maintenance_console 그리고 Enter를 누르세요.

4. 유지 관리 콘솔의 메인 메뉴*에서 *백업 복원 옵션에 대한 번호를 입력합니다.
5. * NetApp 스냅샷 백업 구성*에 대한 번호를 입력하세요.
6. NFS를 구성하려면 번호를 입력하세요.
7. 제공해야 할 정보를 검토한 다음 *백업 구성 세부 정보 입력*에 대한 숫자를 입력하세요.
8. 스냅샷이 기록될 볼륨을 식별하려면 클러스터 관리 인터페이스의 IP 주소, 스토리지 VM의 이름, 볼륨 이름, LUN 이름, 스토리지 시스템 사용자 이름 및 비밀번호, 마운트 경로를 입력합니다.
9. 이 정보를 확인하고 입력하세요 y .

시스템은 다음과 같은 작업을 수행합니다.

- 클러스터에 대한 연결을 설정합니다.
 - 모든 서비스를 중지합니다
 - 볼륨에 새 디렉토리를 생성하고 Active IQ Unified Manager 데이터베이스 구성 파일을 복사합니다.
 - Active IQ Unified Manager 에서 파일을 삭제하고 새 데이터베이스 디렉토리에 대한 심볼릭 링크를 만듭니다.
 - 모든 서비스를 다시 시작합니다
10. 아직 스냅샷 복사 일정을 만들지 않았다면 유지 관리 콘솔을 종료하고 Active IQ Unified Manager 인터페이스를 실행하여 일정을 만드세요.

Windows에서 백업 구성

Active IQ Unified Manager iSCSI 프로토콜을 사용하는 LUN을 통해 Windows 운영 체제에서 NetApp 스냅샷을 사용하여 백업 및 복원을 지원합니다.

모든 Unified Manager 서비스가 실행되는 동안 스냅샷 기반 백업을 수행할 수 있습니다. 백업은 전체 데이터베이스에 글로벌 읽기 잠금을 걸어 동시 쓰기를 방지하므로 데이터베이스의 일관된 상태가 스냅샷의 일부로 캡처됩니다. Windows OS에 설치된 Unified Manager 시스템에서 NetApp 스냅샷을 사용하여 백업 및 복원을 수행하려면 먼저 유지 관리 콘솔을 사용하여 Unified Manager 백업을 스냅샷 기반으로 구성해야 합니다.

Unified Manager를 구성하여 스냅샷 복사본을 생성하기 전에 다음 구성 작업을 수행해야 합니다.

- ONTAP 클러스터 구성
- Windows 호스트 머신 구성

Windows용 백업 위치 구성

Windows에서 Unified Manager를 백업한 후 스냅샷 사본을 저장하기 위한 볼륨을 구성해야 합니다.

시작하기 전에

클러스터, 스토리지 VM 및 볼륨은 다음 요구 사항을 충족해야 합니다.

- 클러스터 요구 사항:
 - ONTAP 9.3 이상이 설치되어 있어야 합니다.
 - Unified Manager 서버와 지리적으로 가까워야 합니다.

- Unified Manager에서 모니터링합니다.
- 스토리지 VM 요구 사항:
 - ONTAP 클러스터의 iSCSI 연결
 - 구성된 머신에 대해 iSCSI 프로토콜을 활성화해야 합니다.
 - 백업 구성을 위해 전용 볼륨과 LUN이 있어야 합니다. 선택한 볼륨에는 LUN이 하나만 포함되어야 하며 다른 것은 포함되어서는 안 됩니다.
 - LUN의 크기는 9.9 Active IQ Unified Manager 에서 처리할 것으로 예상되는 데이터 크기의 최소 2배여야 합니다.

이는 볼륨에 대해서도 동일한 크기 요구 사항을 설정합니다.

- 모든 읽기/쓰기 액세스가 선택되었는지 확인하세요.
- 내보내기 정책에서 Superuser Access가 "any"로 설정되어 있는지 확인하세요.
- 볼륨 및 LUN 요구 사항:
 - 볼륨은 Unified Manager MySQL 데이터 디렉터리 크기의 최소 두 배여야 합니다.
 - 보안 스타일은 Windows로 설정해야 합니다.
 - 로컬 스냅샷 정책을 비활성화해야 합니다.
 - 볼륨 자동 크기 조정을 활성화해야 합니다.
 - 성능 서비스 수준은 "Extreme"과 같이 높은 IOPS와 낮은 지연 시간을 갖는 정책으로 설정되어야 합니다.

ONTAP 클러스터 구성

Windows 시스템에서 스냅샷 복사를 사용하여 Active IQ Unified Manager 백업하고 복원하려면 ONTAP 클러스터에서 몇 가지 사전 구성 단계를 수행해야 합니다.

명령 프롬프트나 시스템 관리자 사용자 인터페이스를 사용하여 ONTAP 클러스터를 구성할 수 있습니다. ONTAP 클러스터 구성에는 스토리지 VM에 iSCSI LIF로 할당할 수 있도록 데이터 LIF를 구성하는 작업이 포함됩니다. 다음 단계는 System Manager 사용자 인터페이스를 사용하여 iSCSI 지원 스토리지 VM을 구성하는 것입니다. 이 스토리지 VM에 대한 정적 네트워크 경로를 구성하여 LIF가 아웃바운드 트래픽에 네트워크를 사용하는 방식을 제어해야 합니다.



백업 구성을 위해 전용 볼륨과 LUN이 있어야 합니다. 선택한 볼륨에는 LUN이 하나만 포함되어야 합니다. LUN의 크기는 Active IQ Unified Manager 에서 처리할 것으로 예상되는 데이터 크기의 최소 2배여야 합니다.

다음 구성을 수행해야 합니다.

단계

1. iSCSI 지원 스토리지 VM을 구성하거나 동일한 구성을 가진 기존 스토리지 VM을 사용합니다.
2. 구성된 스토리지 VM에 대한 네트워크 경로를 구성합니다.
3. 적절한 용량의 볼륨과 그 안에 단일 LUN을 구성하여 볼륨이 이 LUN에만 전용되도록 합니다.



System Manager에서 LUN을 생성하는 시나리오에서 LUN 매핑을 해제하면 igroup이 삭제되고 복원이 실패할 수 있습니다. 이런 시나리오를 피하려면 LUN을 생성할 때 명시적으로 생성하고 LUN이 매핑 해제될 때 삭제되지 않도록 해야 합니다.

4. 스토리지 VM에서 개시자 그룹을 구성합니다.
5. 포트 세트를 구성합니다.
6. igroup을 portset과 통합합니다.
7. LUN을 igroup에 매핑합니다.

Windows 호스트 머신 구성

NetApp Snapshot을 사용하여 Active IQ Unified Manager 백업하고 복원하려면 먼저 Windows 호스트 컴퓨터를 구성해야 합니다. Windows 호스트 머신에서 Microsoft iSCSI 초기자를 시작하려면 검색 창에 "iscsi"를 입력하고 *iSCSI 초기자*를 클릭합니다.

시작하기 전에

호스트 머신의 이전 구성을 모두 정리해야 합니다.

Windows를 새로 설치한 상태에서 iSCSI 이니시에이터를 시작하려고 하면 확인 메시지가 나타나고, 확인이 완료되면 iSCSI 속성 대화 상자가 표시됩니다. 기존 Windows 설치인 경우 비활성화되었거나 연결을 시도 중인 대상이 표시된 iSCSI 속성 대화 상자가 표시됩니다. 따라서 Windows 호스트의 이전 구성이 모두 제거되었는지 확인해야 합니다.

단계

1. 호스트 머신의 이전 구성을 정리합니다.
2. 대상 포털을 발견하세요.
3. 대상 포털에 연결합니다.
4. 멀티패스를 사용하여 대상 포털에 연결합니다.
5. 두 가지 LIF를 모두 알아보세요.
6. Windows 컴퓨터에서 장치로 구성된 LUN을 검색합니다.
7. Windows에서 검색된 LUN을 새 볼륨 드라이브로 구성합니다.

Windows에서 스냅샷 복사본의 대상 위치 지정

ONTAP 클러스터 중 하나에 이미 구성한 볼륨에서 Active IQ Unified Manager 스냅샷 복사본의 대상 위치를 구성해야 합니다. 위치를 정의하려면 유지 관리 콘솔을 사용해야 합니다.

- Active IQ Unified Manager 설치된 Windows 호스트에 대한 관리자 권한이 있어야 합니다.
- Unified Manager 서버의 유지 관리 콘솔에 로그인하려면 권한이 있는 사용자 ID와 비밀번호가 있어야 합니다.
- 클러스터 관리 IP 주소, 스토리지 VM 이름, 볼륨 이름, LUN 이름, 스토리지 시스템 사용자 이름 및 비밀번호가 있어야 합니다.
- 볼륨을 Active IQ Unified Manager 호스트에 네트워크 드라이브로 마운트해야 하며, 마운트 드라이브가 있어야 합니다.

단계

1. PowerShell을 사용하여 Active IQ Unified Manager 시스템의 IP 주소 또는 정규화된 도메인 이름에 연결합니다.
2. 유지 관리 사용자(umadmin) 이름과 비밀번호로 시스템에 로그인합니다.
3. 명령을 입력하세요 maintenance_console 그리고 Enter를 누르세요.
4. 유지 관리 콘솔의 메인 메뉴*에서 *백업 복원 옵션에 대한 번호를 입력합니다.
5. * NetApp 스냅샷 백업 구성*에 대한 번호를 입력하세요.
6. iSCSI를 구성하려면 번호를 입력하세요.
7. 제공해야 할 정보를 검토한 다음 *백업 구성 세부 정보 입력*에 대한 숫자를 입력하세요.
8. 스냅샷이 기록될 볼륨을 식별하려면 클러스터 관리 인터페이스의 IP 주소, 스토리지 VM의 이름, 볼륨 이름, LUN 이름, 스토리지 시스템 사용자 이름 및 비밀번호, 마운트 드라이브를 입력합니다.
9. 이 정보를 확인하고 입력하세요 y .

시스템은 다음과 같은 작업을 수행합니다.

- 스토리지 VM이 검증되었습니다.
- 볼륨이 검증되었습니다
- 드라이브 마운트 및 상태가 검증되었습니다.
- LUN 존재 및 상태
- 네트워크 드라이브 존재
- 마운트된 볼륨에 권장 공간(MySQL 데이터 디렉토리의 2배 이상)이 존재하는지 검증합니다.
- 볼륨의 전용 LUN에 해당하는 LUN 경로
- igroup 이름
- 네트워크 드라이브가 마운트된 볼륨의 GUID
- ONTAP 과 통신하는 데 사용되는 iSCSI 이니시에이터

10. 유지 관리 콘솔을 종료하고 Active IQ Unified Manager 인터페이스를 실행하여 스냅샷 복사 일정을 만듭니다.

유지 관리 콘솔에서 스냅샷 복사로 백업 구성

스냅샷 복사를 사용하여 Active IQ Unified Manager 백업을 수행하려면 유지 관리 콘솔에서 몇 가지 구성 단계를 수행해야 합니다.

시작하기 전에

시스템에 대한 세부 정보는 다음과 같습니다.

- 클러스터 IP 주소
- 스토리지 VM 이름
- 볼륨 이름
- LUN 이름
- 산길
- 스토리지 시스템 자격 증명

단계

1. Unified Manager의 유지 관리 콘솔에 액세스합니다.
2. *백업 복원*을 선택하려면 4를 입력하세요.
3. * NetApp 스냅샷을 사용하여 백업 및 복원*을 선택하려면 2를 입력합니다.



백업 구성을 변경하려면 * NetApp 스냅샷 백업 구성 업데이트*를 선택하려면 3을 입력합니다. 비밀번호만 업데이트할 수 있습니다.

4. 메뉴에서 1을 입력하여 * NetApp 스냅샷 백업 구성*을 선택합니다.
5. 필요한 정보를 제공하려면 1을 입력하세요.
6. 유지 관리 콘솔에 대한 사용자 이름과 비밀번호를 제공한 다음 LUN이 호스트에 마운트되었는지 확인합니다.

그런 다음 프로세스에서는 사용자가 제공한 데이터 디렉터리, LUN 경로, 스토리지 VM, 볼륨, 공간 가용성, 드라이브 등이 올바른지 확인합니다. 백그라운드에서 진행되는 작업은 다음과 같습니다.

- 서비스가 중단되었습니다
- 데이터베이스 디렉터리가 마운트된 저장소로 이동되었습니다.
- 데이터베이스 디렉터리가 삭제되고 심볼릭 링크가 설정됩니다.
- 구성이 Active IQ Unified Manager 인터페이스에서 완료되면 백업 유형이 NetApp 스냅샷으로 수정되고 사용자 인터페이스에 데이터베이스 백업(스냅샷 기반)으로 반영됩니다.

백업 작업을 시작하기 전에 스냅샷 구성에 변경 사항이 있는지 확인해야 합니다. 변경 사항이 있으면 스냅샷이 유효하지 않게 될 수 있습니다. G 드라이브에 백업을 구성하고 스냅샷을 찍었다고 가정해 보겠습니다. 나중에 E 드라이브에 대한 백업을 재구성했고 데이터는 새로운 구성에 따라 E 드라이브에 저장됩니다. G 드라이브에 있는 동안 찍은 스냅샷을 복원하려고 하면 G 드라이브가 없다는 오류 메시지가 나타나서 실패합니다.

Linux 및 Windows에 대한 백업 일정 정의

Unified Manager UI를 사용하여 Unified Manager 스냅샷 복사본이 생성되는 일정을 구성할 수 있습니다.

시작하기 전에

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 스냅샷이 생성될 대상을 식별하려면 유지 관리 콘솔에서 스냅샷 복사본을 생성하기 위한 설정을 구성해야 합니다.

스냅샷 복사본은 몇 분 안에 생성되고 Unified Manager 데이터베이스는 몇 초 동안만 잠깁니다.



새로운 클러스터를 추가한 후 처음 15일 동안 수행한 백업은 과거 성능 데이터를 얻기에 충분히 정확하지 않을 수 있습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *데이터베이스 백업*을 클릭합니다.
2. 데이터베이스 백업 페이지에서 *백업 설정*을 클릭합니다.
3. 보존 횟수 필드에 보존하려는 스냅샷 사본의 최대 수를 입력합니다.

보존 횟수의 기본값은 10입니다. 스냅샷 복사본의 최대 수는 클러스터의 ONTAP 소프트웨어 버전에 따라 결정됩니다. ONTAP 버전에 관계없이 최대값을 구현하려면 이 필드를 비워둘 수 있습니다.

4. 매일 예약 또는 매주 예약 버튼을 선택한 다음, 일정 세부 정보를 지정합니다.
5. *적용*을 클릭하세요.

스냅샷 사본은 일정에 따라 생성됩니다. 사용 가능한 백업 파일은 데이터베이스 백업 페이지에서 볼 수 있습니다.

이 볼륨과 스냅샷의 중요성 때문에 이 볼륨에 대한 알림을 하나 또는 두 개 만들어 다음과 같은 경우 알림을 받도록 할 수 있습니다.

- 볼륨 공간이 90% 채워졌습니다. 볼륨 공간 가득 참 이벤트를 사용하여 알림을 설정하세요.

ONTAP System Manager나 ONTAP CLI를 사용하여 볼륨에 용량을 추가하면 Unified Manager 데이터베이스의 공간이 부족해지는 것을 방지할 수 있습니다.

- 스냅샷의 개수가 최대 개수에 가까워졌습니다. 스냅샷 사본이 너무 많음 이벤트를 사용하여 알림을 설정하세요.

ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 이전 스냅샷을 삭제하면 항상 새로운 스냅샷 복사본을 위한 공간을 확보할 수 있습니다.

알림 설정 페이지에서 알림을 구성합니다.

스냅샷 복사본을 사용하여 **Unified Manager** 복원

데이터 손실이나 데이터 손상이 발생하는 경우 최소한의 데이터 손실로 Unified Manager를 이전의 안정적인 상태로 복원할 수 있습니다. Unified Manager 유지 관리 콘솔을 사용하여 Unified Manager 스냅샷 데이터베이스를 로컬 또는 원격 운영 체제로 복원할 수 있습니다.

시작하기 전에

- Unified Manager가 설치된 Linux 호스트에 대한 루트 사용자 자격 증명과 Windows 호스트 컴퓨터에 대한 관리자 권한이 있어야 합니다.
- Unified Manager 서버의 유지 관리 콘솔에 로그인하려면 권한이 있는 사용자 ID와 비밀번호가 있어야 합니다.

복원 기능은 플랫폼과 버전에 따라 다릅니다. Unified Manager 백업은 동일한 버전의 Unified Manager에서만 복원할 수 있습니다.

단계

1. Unified Manager 시스템의 IP 주소 또는 정규화된 도메인 이름에 연결합니다.
 - 리눅스: 보안 셸
 - 윈도우: 파워셸
2. 루트 사용자 자격 증명을 사용하여 시스템에 로그인합니다.
3. 명령을 입력하세요 `maintenance_console` 그리고 Enter를 누르세요.
4. 유지 관리 콘솔의 메인 메뉴*에서 *백업 복원 옵션에 4를 입력합니다.
5. * NetApp 스냅샷을 사용하여 백업 및 복원*을 선택하려면 2를 입력합니다.

Unified Manager를 설치한 후에는 새 서버로 복원을 수행하는 경우 UI를 시작하거나 설치가 완료된 후 클러스터,

사용자 또는 인증 설정을 구성하지 마세요. * NetApp 스냅샷 백업 구성*을 선택하려면 1을 입력하고 원본 시스템에 있는 대로 스냅샷 복사본에 대한 설정을 구성합니다.

6. * NetApp 스냅샷을 사용하여 복원*을 선택하려면 3을 입력합니다.
7. Unified Manager를 복원할 스냅샷 복사본을 선택합니다. *Enter*를 누르세요.
8. 복원 프로세스가 완료되면 Unified Manager 사용자 인터페이스에 로그인합니다.

백업을 복원한 후 Workflow Automation 서버가 작동하지 않으면 다음 단계를 수행하세요.

1. Workflow Automation 서버에서 Unified Manager 서버의 IP 주소를 최신 컴퓨터를 가리키도록 변경합니다.
2. Unified Manager 서버에서 1단계에서 획득에 실패하면 데이터베이스 비밀번호를 재설정합니다.

백업 유형 수정

Active IQ Unified Manager 시스템의 백업 유형을 변경하려면 유지 관리 콘솔 옵션을 사용하면 됩니다. * NetApp 스냅샷 백업 구성 취소* 옵션을 사용하면 MySQL 기반 백업으로 돌아갈 수 있습니다.

시작하기 전에

Unified Manager 서버의 유지 관리 콘솔에 로그인하려면 권한이 있는 사용자 ID와 비밀번호가 있어야 합니다.

단계

1. 유지 관리 콘솔에 액세스합니다.
2. 백업 및 복원을 위해 *메인 메뉴*에서 4개를 선택하세요.
3. *백업 및 복원 메뉴*에서 2를 선택하세요.
4. * NetApp 스냅샷 백업 구성 해제*를 위해 4를 선택합니다.

수행되는 작업은 다음과 같습니다. 서비스 중지, 심볼릭 링크 끊기, 저장소에서 디렉토리로 데이터 이동, 그리고 서비스를 다시 시작합니다.

백업 방법이 수정되면 백업 메커니즘이 스냅샷 복사에서 기본 MySQL 백업으로 변경됩니다. 이 변경 사항은 일반 설정의 데이터베이스 백업 섹션에 나타납니다.

Unified Manager를 위한 주문형 백업

Active IQ Unified Manager 사용자 인터페이스를 사용하면 필요할 때마다 주문형 백업을 생성할 수 있습니다. 주문형 백업을 사용하면 기존 백업 방법을 사용하여 즉시 백업을 만들 수 있습니다. 온디맨드 백업은 MySQL 또는 NetApp 스냅샷 기반 백업을 구별하지 않습니다.

데이터베이스 백업 페이지에서 지금 백업 버튼을 사용하여 주문형 백업을 수행할 수 있습니다. 주문형 백업은 Active IQ Unified Manager 에 대해 구성된 일정에 따라 달라지지 않습니다.

Unified Manager 가상 어플라이언스를 Linux 시스템으로 마이그레이션

Unified Manager가 실행 중인 호스트 운영 체제를 변경하려는 경우 가상 어플라이언스에서 Unified Manager MySQL 데이터베이스 덤프 백업을 Red Hat Enterprise Linux 시스템으로

복원할 수 있습니다.

시작하기 전에

- 가상 어플라이언스에서:
 - 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
 - 복원 작업을 위해서는 Unified Manager 유지 관리 사용자의 이름을 알아야 합니다.
- Linux 시스템에서:
 - Linux 서버에 Unified Manager를 설치하려면 다음 지침을 따라야 합니다. "[Linux 시스템에 Unified Manager 설치](#)".
 - 이 서버의 Unified Manager 버전은 백업 파일을 사용하는 가상 어플라이언스의 버전과 동일해야 합니다.
 - 설치 후에는 Linux 시스템에서 UI를 실행하거나 클러스터, 사용자 또는 인증 설정을 구성하지 마세요. 백업 파일은 복원 과정 중에 이 정보를 채웁니다.
 - Linux 호스트에 대한 루트 사용자 자격 증명이 있어야 합니다.

이 단계에서는 가상 어플라이언스에서 백업 파일을 생성하고, 백업 파일을 Red Hat Enterprise Linux로 복사한 다음, 데이터베이스 백업을 새 시스템으로 복원하는 방법을 설명합니다.

단계

1. 가상 어플라이언스에서 관리 > *데이터베이스 백업*을 클릭합니다.
2. 데이터베이스 백업 페이지에서 *백업 설정*을 클릭합니다.
3. 백업 경로를 /jail/support로 변경합니다.
4. 일정 섹션에서 *매일 예약*을 선택하고 현재 시간보다 몇 분 후의 시간을 입력하면 백업이 곧 생성됩니다.
5. *적용*을 클릭하세요.
6. 백업이 생성될 때까지 몇 시간 정도 기다리세요.

전체 백업은 1GB가 넘을 수 있으며 완료하는 데 3~4시간이 걸릴 수 있습니다.

7. Unified Manager가 설치된 Linux 호스트에 루트 사용자로 로그인하고 SCP를 사용하여 가상 어플라이언스의 /support에서 백업 파일을 복사합니다..
`root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/* .`

```
root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
```

/database-dumps-repo 하위 디렉토리에 있는 .7z 백업 파일과 모든 .7z 저장소 파일을 복사했는지 확인하세요.

8. 명령 프롬프트에서 백업을 복원합니다.
`um backup restore -f /<backup_file_path>/<backup_file_name>`

```
um backup restore -f /UM_9.7.N151113.1348_backup_unix_02-12-2019-04-16.7z
```

9. 복원 작업이 완료되면 Unified Manager 웹 UI에 로그인합니다.

다음 작업을 수행해야 합니다.

- 새로운 HTTPS 보안 인증서를 생성하고 Unified Manager 서버를 다시 시작합니다.

- Linux 시스템에는 /jail/support 경로가 없으므로 백업 경로를 Linux 시스템의 기본 설정(/data/ocum-backup)으로 변경하거나 원하는 새 경로로 변경하세요.
- WFA를 사용하는 경우 Workflow Automation 연결의 양쪽을 다시 구성합니다.
- SAML을 사용하는 경우 SAML 인증 설정을 재구성합니다.

Linux 시스템에서 모든 것이 예상대로 실행되는지 확인한 후 Unified Manager 가상 어플라이언스를 종료하고 제거할 수 있습니다.

스크립트 관리

스크립트를 사용하면 Unified Manager에서 여러 스토리지 개체를 자동으로 수정하거나 업데이트할 수 있습니다. 스크립트는 알림과 연결되어 있습니다. 이벤트로 인해 알림이 발생하면 스크립트가 실행됩니다. 사용자 정의 스크립트를 업로드하고 알림이 생성되면 실행을 테스트할 수 있습니다.

스크립트를 Unified Manager에 업로드하고 실행하는 기능은 기본적으로 활성화되어 있습니다. 보안상의 이유로 조직에서 이 기능을 허용하지 않으려는 경우, 저장소 관리 > *기능 설정*에서 이 기능을 비활성화할 수 있습니다.

스크립트가 알림과 함께 작동하는 방식

스크립트에 알림을 연결하면 Unified Manager에서 이벤트에 대한 알림이 발생할 때 스크립트가 실행됩니다. 스크립트를 사용하면 스토리지 개체의 문제를 해결하거나 이벤트를 생성하는 스토리지 개체를 식별할 수 있습니다.

Unified Manager에서 이벤트에 대한 알림이 생성되면 지정된 수신자에게 알림 이메일이 전송됩니다. 알림을 스크립트와 연결한 경우 스크립트가 실행됩니다. 스크립트에 전달된 인수의 세부 정보는 알림 이메일에서 얻을 수 있습니다.



사용자 지정 스크립트를 만들어 특정 이벤트 유형에 대한 알림과 연결한 경우 해당 이벤트 유형에 대한 사용자 지정 스크립트에 따라 작업이 수행되고, 수정 작업은 기본적으로 관리 작업 페이지나 Unified Manager 대시보드에서 사용할 수 없습니다.

스크립트는 실행을 위해 다음 인수를 사용합니다.

- -eventID
- -eventName
- -eventSeverity
- -eventSourceID
- -eventSourceName
- -eventSourceType
- -eventState
- -eventArgs

스크립트에서 인수를 사용하여 관련 이벤트 정보를 수집하거나 저장소 객체를 수정할 수 있습니다.

스크립트에서 인수를 얻는 예

```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

경고가 생성되면 이 스크립트가 실행되고 다음 출력이 표시됩니다.

```
-eventID : 290
-eventSourceID : 4138
```

스크립트 추가

Unified Manager에서 스크립트를 추가하고, 스크립트를 알림과 연결할 수 있습니다. 이러한 스크립트는 알림이 생성되면 자동으로 실행되며, 이벤트가 생성된 저장소 개체에 대한 정보를 얻을 수 있습니다.

시작하기 전에

- Unified Manager 서버에 추가하려는 스크립트를 만들고 저장했어야 합니다.
- 스크립트에 지원되는 파일 형식은 Perl, Shell, PowerShell, Python입니다. .bat 파일.

Unified Manager가 설치된 플랫폼	지원 언어
VMware	Perl 및 셸 스크립트
리눅스	Perl, Python 및 Shell 스크립트
Windows	PowerShell, Perl, Python 및 .bat 스크립트

- Perl 스크립트의 경우 Perl이 Unified Manager 서버에 설치되어 있어야 합니다. VMware 설치의 경우 Perl 5가 기본적으로 설치되고 스크립트는 Perl 5에서 지원하는 내용만 지원합니다. Unified Manager를 설치한 후 Perl을 설치한 경우 Unified Manager 서버를 다시 시작해야 합니다.
- PowerShell 스크립트의 경우 스크립트를 실행할 수 있도록 Windows 서버에서 적절한 PowerShell 실행 정책을 설정해야 합니다.



스크립트가 경고 스크립트 진행 상황을 추적하기 위해 로그 파일을 생성하는 경우 Unified Manager 설치 폴더 내에 로그 파일이 생성되지 않도록 해야 합니다.

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

사용자 정의 스크립트를 업로드하고 알림에 대한 이벤트 세부 정보를 수집할 수 있습니다.



사용자 인터페이스에서 이 기능을 사용할 수 없는 경우 관리자가 해당 기능을 비활성화했기 때문입니다. 필요한 경우 저장소 관리 > *기능 설정*에서 이 기능을 활성화할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *스크립트*를 클릭합니다.
2. 스크립트 페이지에서 *추가*를 클릭합니다.
3. 스크립트 추가 대화 상자에서 *찾아보기*를 클릭하여 스크립트 파일을 선택합니다.
4. 선택한 스크립트에 대한 설명을 입력하세요.
5. *추가*를 클릭하세요.

스크립트 삭제

스크립트가 더 이상 필요하지 않거나 유효하지 않으면 Unified Manager에서 스크립트를 삭제할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 스크립트는 알림과 연관되어서는 안 됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *스크립트*를 클릭합니다.
2. 스크립트 페이지에서 삭제하려는 스크립트를 선택한 다음 *삭제*를 클릭합니다.
3. 경고 대화 상자에서 *예*를 클릭하여 삭제를 확인합니다.

테스트 스크립트 실행

저장소 개체에 대한 알림이 생성되면 스크립트가 올바르게 실행되는지 확인할 수 있습니다.

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 지원되는 파일 형식의 스크립트를 Unified Manager에 업로드해야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *스크립트*를 클릭합니다.
2. 스크립트 페이지에서 테스트 스크립트를 추가합니다.
3. 왼쪽 탐색 창에서 저장소 관리 > *알림 설정*을 클릭합니다.
4. 알림 설정 페이지에서 다음 작업 중 하나를 수행합니다.

에게...	이렇게 하세요...
알림 추가	a. *추가*를 클릭하세요. b. 작업 섹션에서 알림을 테스트 스크립트와 연결합니다.
알림 편집	a. 알림을 선택한 다음 *편집*을 클릭합니다. b. 작업 섹션에서 알림을 테스트 스크립트와 연결합니다.

5. *저장*을 클릭하세요.

6. 알림 설정 페이지에서 추가하거나 수정한 알림을 선택한 다음 *테스트*를 클릭합니다.

스크립트는 “-test” 인수로 실행되고, 알림 경고는 경고가 생성될 때 지정된 이메일 주소로 전송됩니다.

그룹 관리 및 모니터링

Unified Manager에서 그룹을 만들어 스토리지 객체를 관리할 수 있습니다.

그룹을 이해하세요

Unified Manager에서 그룹을 만들어 스토리지 객체를 관리할 수 있습니다. 그룹에 대한 개념과 그룹 규칙을 통해 그룹에 스토리지 객체를 추가하는 방법을 이해하면 환경 내에서 스토리지 객체를 관리하는 데 도움이 됩니다.

그룹이란 무엇인가

그룹은 이기종 저장 객체(클러스터, SVM 또는 볼륨)의 동적 컬렉션입니다. Unified Manager에서 그룹을 생성하면 스토리지 개체 세트를 쉽게 관리할 수 있습니다. 그룹의 멤버는 Unified Manager가 특정 시점에 모니터링하는 스토리지 개체에 따라 변경될 수 있습니다.

- 각 그룹에는 고유한 이름이 있습니다.
- 각 그룹에 대해 최소한 하나의 그룹 규칙을 구성해야 합니다.
- 하나의 그룹을 두 개 이상의 그룹 규칙과 연결할 수 있습니다.
- 각 그룹에는 클러스터, SVM, 볼륨 등 여러 유형의 스토리지 개체가 포함될 수 있습니다.
- 스토리지 개체는 그룹 규칙이 생성되거나 Unified Manager가 모니터링 주기를 완료할 때 그룹에 동적으로 추가됩니다.
- 볼륨에 대한 임계값을 설정하는 등의 작업을 그룹 내 모든 저장소 개체에 동시에 적용할 수 있습니다.

그룹에 대한 그룹 규칙의 작동 방식

그룹 규칙은 스토리지 개체(볼륨, 클러스터 또는 SVM)를 특정 그룹에 포함할 수 있도록 정의하는 기준입니다. 그룹에 대한 그룹 규칙을 정의하기 위해 조건 그룹이나 조건을 사용할 수 있습니다.

- 그룹 규칙은 그룹에 연결해야 합니다.
- 그룹 규칙에 대해서는 개체 유형을 연결해야 합니다. 그룹 규칙에 대해서는 하나의 개체 유형만 연결됩니다.
- 각 모니터링 주기가 끝나거나 규칙이 생성, 편집 또는 삭제될 때 저장소 개체가 그룹에 추가되거나 제거됩니다.
- 그룹 규칙은 하나 이상의 조건 그룹을 가질 수 있으며, 각 조건 그룹은 하나 이상의 조건을 가질 수 있습니다.
- 저장 객체는 사용자가 만든 그룹 규칙에 따라 여러 그룹에 속할 수 있습니다.

정황

여러 개의 조건 그룹을 만들 수 있으며, 각 조건 그룹에는 하나 이상의 조건이 포함될 수 있습니다. 그룹에 대한 그룹 규칙에서 정의된 모든 조건 그룹을 적용하여 그룹에 포함되는 스토리지 객체를 지정할 수 있습니다.

조건 그룹 내의 조건은 논리적 AND를 사용하여 실행됩니다. 조건 그룹의 모든 조건이 충족되어야 합니다. 그룹 규칙을 만들거나 수정하면 조건 그룹의 모든 조건을 충족하는 저장소 개체만 적용, 선택 및 그룹화하는 조건이 생성됩니다. 그룹에 포함할 스토리지 개체의 범위를 좁히려는 경우 조건 그룹 내에서 여러 조건을 사용할 수 있습니다.

다음 피연산자와 연산자를 사용하고 필요한 값을 지정하여 저장 객체로 조건을 생성할 수 있습니다.

저장 객체 유형	적용 가능한 피연산자
용량	- 객체 이름 - 소유 클러스터 이름 - SVM 이름 소유 - 주석
서포트 머신(SVM)	- 객체 이름 - 소유 클러스터 이름 - 주석
무리	- 객체 이름 - 주석

저장 객체에 대한 피연산자로 주석을 선택하면 "Is" 연산자를 사용할 수 있습니다. 다른 모든 피연산자의 경우 연산자로 "Is" 또는 "Contains"를 선택할 수 있습니다.

• 피연산자

Unified Manager의 피연산자 목록은 선택한 개체 유형에 따라 변경됩니다. 목록에는 Unified Manager에서 정의한 개체 이름, 소유 클러스터 이름, 소유 SVM 이름 및 주석이 포함됩니다.

• 연산자

연산자 목록은 조건에 대해 선택된 피연산자에 따라 변경됩니다. Unified Manager에서 지원되는 연산자는 "Is"와 "Contains"입니다.

"Is" 연산자를 선택하면, 선택된 피연산자에 대해 제공된 값과 피연산자 값이 정확히 일치하는지 여부가 조건 평가에서 평가됩니다.

Contains 연산자를 선택하면 조건이 다음 기준 중 하나를 충족하는지 평가됩니다.

- 피연산자 값은 선택된 피연산자에 제공된 값과 정확히 일치합니다.
- 피연산자 값에는 선택된 피연산자에 대해 제공된 값이 포함됩니다.

• 가치

값 필드는 선택한 피연산자에 따라 변경됩니다.

조건이 포함된 그룹 규칙의 예

다음 두 가지 조건을 갖춘 볼륨에 대한 조건 그룹을 고려하세요.

- 이름에 "vol"이 포함되어 있습니다.
- SVM 이름은 "data_svm"입니다.

이 조건 그룹은 이름에 "vol"이 포함되어 있고 이름이 "data_svm"인 SVM에 호스팅된 모든 볼륨을 선택합니다.

조건 그룹

조건 그룹은 논리적 OR을 사용하여 실행된 다음 저장소 개체에 적용됩니다. 저장 객체는 그룹에 포함되려면 조건 그룹 중 하나를 만족해야 합니다. 모든 조건 그룹의 저장 객체가 결합됩니다. 조건 그룹을 사용하면 그룹에 포함할 저장 객체의 범위를 늘릴 수 있습니다.

조건 그룹이 있는 그룹 규칙의 예

각 그룹에 다음 두 가지 조건이 포함된 볼륨에 대한 두 개의 조건 그룹을 고려하세요.

- 조건 그룹 1
 - 이름에 "vol"이 포함되어 있습니다.
 - SVM 이름은 "data_svm"입니다. 조건 그룹 1은 이름에 "vol"이 포함되어 있고 이름이 "data_svm"인 SVM에 호스팅된 모든 볼륨을 선택합니다.
- 조건 그룹 2
 - 이름에 "vol"이 포함되어 있습니다.
 - data-priority의 주식 값은 "critical"입니다. 조건 그룹 2는 이름에 "vol"이 포함되고 data-priority 주식 값이 "critical"로 주식이 달린 모든 볼륨을 선택합니다.

이 두 조건 그룹을 포함하는 그룹 규칙이 스토리지 개체에 적용되면 다음 스토리지 개체가 선택한 그룹에 추가됩니다.

- 이름에 "vol"이 포함되어 있고 이름이 "data_svm"인 SVM에 호스팅된 모든 볼륨입니다.
- 이름에 "vol"이 포함되어 있고 데이터 우선순위 주식 값 "critical"이 주식 처리된 모든 볼륨입니다.

그룹 작업이 저장소 개체에서 작동하는 방식

그룹 작업은 그룹 내의 모든 저장소 개체에 수행되는 작업입니다. 예를 들어, 볼륨 임계값 그룹 작업을 구성하여 그룹의 모든 볼륨의 볼륨 임계값을 동시에 변경할 수 있습니다.

그룹은 고유한 그룹 작업 유형을 지원합니다. 하나의 볼륨 상태 임계값 그룹 작업 유형만 갖는 그룹을 가질 수 있습니다. 하지만 가능한 경우 동일한 그룹에 대해 다른 유형의 그룹 작업을 구성할 수 있습니다. 그룹 작업의 순위는 작업이 저장 개체에 적용되는 순서를 결정합니다. 저장소 개체의 세부 정보 페이지는 저장소 개체에 적용되는 그룹 작업에 대한 정보를 제공합니다.

고유한 그룹 작업의 예

그룹 G1 및 G2에 속하는 볼륨 A를 고려하고, 이러한 그룹에 대해 다음과 같은 볼륨 상태 임계값 그룹 작업이 구성되어 있습니다.

- `Change\_capacity\_threshold` 볼륨 용량을 구성하기 위한 순위 1의 그룹 작업
- `Change\_snapshot\_copies` 볼륨의 스냅샷 복사본을 구성하기 위한 순위 2의 그룹 작업

그만큼 Change_capacity_threshold 그룹 행동은 항상 우선시됩니다. Change_snapshot_copies 그룹 작업이며 볼륨 A에 적용됩니다. Unified Manager가 모니터링의 한 주기를 완료하면 볼륨 A의 상태 임계값 관련 이벤트가 다시 평가됩니다. Change_capacity_threshold 집단행동. G1 또는 G2 그룹에 대해 다른 볼륨 임계값 유형의 그룹 작업을 구성할 수 없습니다.

그룹 추가

관리 편의성을 높이기 위해 클러스터, 볼륨, 스토리지 가상 머신(SVM)을 결합하는 그룹을 만들 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

그룹 규칙을 정의하여 그룹에 구성원을 추가하거나 제거하고, 그룹에 대한 그룹 작업을 수정할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *그룹*을 클릭합니다.
2. 그룹 탭에서 *추가*를 클릭합니다.
3. 그룹 추가 대화 상자에서 그룹의 이름과 설명을 입력합니다.
4. *추가*를 클릭하세요.

그룹 편집

Unified Manager에서 만든 그룹의 이름과 설명을 편집할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

그룹의 이름을 업데이트하기 위해 편집할 때는 고유한 이름을 지정해야 합니다. 기존 그룹 이름을 사용할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *그룹*을 클릭합니다.
2. 그룹 탭에서 편집하려는 그룹을 선택한 다음 *편집*을 클릭합니다.
3. 그룹 편집 대화 상자에서 그룹의 이름, 설명 또는 둘 다를 변경합니다.
4. *저장*을 클릭하세요.

그룹 삭제

더 이상 필요하지 않은 그룹은 Unified Manager에서 삭제할 수 있습니다.

시작하기 전에

- 삭제하려는 그룹과 연관된 그룹 규칙에는 어떠한 스토리지 개체(클러스터, SVM 또는 볼륨)도 연관되어서는 안 됩니다.

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *그룹*을 클릭합니다.
2. 그룹 탭에서 삭제하려는 그룹을 선택한 다음 *삭제*를 클릭합니다.
3. 경고 대화 상자에서 *예*를 클릭하여 삭제를 확인합니다.

그룹을 삭제해도 해당 그룹과 연관된 그룹 작업은 삭제되지 않습니다. 하지만 그룹이 삭제되면 이러한 그룹 작업은 매핑 해제됩니다.

그룹 규칙 추가

볼륨, 클러스터 또는 스토리지 가상 머신(SVM)과 같은 스토리지 객체를 그룹에 동적으로 추가하기 위해 그룹에 대한 그룹 규칙을 만들 수 있습니다. 그룹 규칙을 만들려면 최소한 하나의 조건이 포함된 최소한 하나의 조건 그룹을 구성해야 합니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

현재 모니터링 중인 저장소 개체는 그룹 규칙이 생성되는 즉시 추가됩니다. 모니터링 주기가 완료된 후에만 새로운 객체가 추가됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *그룹*을 클릭합니다.
2. 그룹 규칙 탭에서 *추가*를 클릭합니다.
3. 그룹 규칙 추가 대화 상자에서 그룹 규칙의 이름을 지정합니다.
4. 대상 개체 유형 필드에서 그룹화하려는 저장소 개체 유형을 선택합니다.
5. 그룹 필드에서 그룹 규칙을 만들려는 그룹을 선택합니다.
6. 조건 섹션에서 다음 단계를 수행하여 조건, 조건 그룹 또는 둘 다를 만듭니다.

창조하려면....	이렇게 하세요...
조건	a. 피연산자 목록에서 피연산자를 선택합니다. b. 연산자로 포함 또는 *있음*을 선택하세요. c. 값을 입력하거나 사용 가능한 목록에서 값을 선택하세요.

창조하려면....	이렇게 하세요...
조건 그룹	a. *조건 그룹 추가*를 클릭하세요. b. 피연산자 목록에서 피연산자를 선택합니다. c. 연산자로 포함 또는 *있음*을 선택하세요. d. 값을 입력하거나 사용 가능한 목록에서 값을 선택하세요. e. 필요한 경우 *조건 추가*를 클릭하여 더 많은 조건을 만들고 각 조건에 대해 a~d 단계를 반복합니다.

7. *추가*를 클릭하세요.

그룹 규칙을 만드는 예

그룹 규칙을 만들려면 그룹 규칙 추가 대화 상자에서 다음 단계를 수행하세요. 여기에는 조건 구성 및 조건 그룹 추가가 포함됩니다.

단계

1. 그룹 규칙의 이름을 지정합니다.
2. 객체 유형을 스토리지 가상 머신(SVM)으로 선택합니다.
3. 그룹 목록에서 그룹을 선택하세요.
4. 조건 섹션에서 피연산자로 *개체 이름*을 선택합니다.
5. 연산자로 *포함*을 선택합니다.
6. 값을 입력하세요 `svm_data`.
7. *조건 그룹 추가*를 클릭합니다.
8. 피연산자로 *개체 이름*을 선택합니다.
9. 연산자로 *포함*을 선택합니다.
10. 값을 입력하세요 `vol`.
11. *조건 추가*를 클릭하세요.
12. 8단계에서 피연산자로 *data-priority*를 선택하고, 9단계에서 연산자로 *Is*를 선택하고, 10단계에서 값으로 *critical*을 선택하여 8단계부터 10단계까지 반복합니다.
13. *추가*를 클릭하여 그룹 규칙에 대한 조건을 만듭니다.

그룹 규칙 편집

그룹 규칙을 편집하여 조건 그룹과 조건 그룹 내의 조건을 수정하고 특정 그룹에 저장소 객체를 추가하거나 제거할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *그룹*을 클릭합니다.
2. 그룹 규칙 탭에서 편집하려는 그룹 규칙을 선택한 다음 *편집*을 클릭합니다.
3. 그룹 규칙 편집 대화 상자에서 필요에 따라 그룹 규칙 이름, 연관된 그룹 이름, 조건 그룹 및 조건을 변경합니다.



그룹 규칙에 대한 대상 개체 유형을 변경할 수 없습니다.

4. *저장*을 클릭하세요.

그룹 규칙 삭제

그룹 규칙이 더 이상 필요하지 않으면 Active IQ Unified Manager 에서 해당 그룹 규칙을 삭제할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

그룹 규칙이 삭제되면 연관된 저장소 개체도 그룹에서 제거됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *그룹*을 클릭합니다.
2. 그룹 규칙 탭에서 삭제하려는 그룹 규칙을 선택한 다음 *삭제*를 클릭합니다.
3. 경고 대화 상자에서 *예*를 클릭하여 삭제를 확인합니다.

그룹 작업 추가

그룹 내 저장소 개체에 적용할 그룹 작업을 구성할 수 있습니다. 그룹에 대한 작업을 구성하면 각 개체에 개별적으로 작업을 추가할 필요가 없으므로 시간을 절약할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *그룹*을 클릭합니다.
2. 그룹 작업 탭에서 *추가*를 클릭합니다.
3. 그룹 작업 추가 대화 상자에서 작업의 이름과 설명을 입력합니다.
4. 그룹 메뉴에서 작업을 구성할 그룹을 선택합니다.
5. 작업 유형 메뉴에서 작업 유형을 선택합니다.

대화 상자가 확장되어 필요한 매개변수를 사용하여 선택한 작업 유형을 구성할 수 있습니다.

6. 그룹 작업을 구성하려면 필수 매개변수에 적절한 값을 입력하세요.
7. *추가*를 클릭하세요.

그룹 작업 편집

Unified Manager에서 구성한 그룹 작업 매개변수(그룹 작업 이름, 설명, 연관된 그룹 이름, 작업 유형 매개변수 등)를 편집할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *그룹*을 클릭합니다.
2. 그룹 작업 탭에서 편집하려는 그룹 작업을 선택한 다음 *편집*을 클릭합니다.
3. 그룹 작업 편집 대화 상자에서 필요에 따라 그룹 작업 이름, 설명, 연관된 그룹 이름 및 작업 유형의 매개변수를 변경합니다.
4. *저장*을 클릭하세요.

그룹에 대한 볼륨 상태 임계값 구성

용량, 스냅샷 복사본, Qtree 할당량, 성장 및 inode에 대한 그룹 수준 볼륨 상태 임계값을 구성할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

그룹 작업의 볼륨 상태 임계값 유형은 그룹의 볼륨에만 적용됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *그룹*을 클릭합니다.
2. 그룹 작업 탭에서 *추가*를 클릭합니다.
3. 그룹 작업에 대한 이름과 설명을 입력하세요.
4. 그룹 드롭다운 상자에서 그룹 작업을 구성하려는 그룹을 선택합니다.
5. 볼륨 상태 임계값으로 *작업 유형*을 선택합니다.
6. 임계값을 설정할 범주를 선택하세요.
7. 건강 임계값에 필요한 값을 입력하세요.
8. *추가*를 클릭하세요.

그룹 작업 삭제

그룹 작업이 더 이상 필요하지 않으면 Unified Manager에서 그룹 작업을 삭제할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨 상태 임계값에 대한 그룹 작업을 삭제하면 해당 그룹의 스토리지 개체에 글로벌 임계값이 적용됩니다. 저장소 개체에 설정된 개체 수준 상태 임계값은 영향을 받지 않습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *그룹*을 클릭합니다.
2. 그룹 작업 탭에서 삭제하려는 그룹 작업을 선택한 다음 *삭제*를 클릭합니다.
3. 경고 대화 상자에서 *예*를 클릭하여 삭제를 확인합니다.

그룹 작업 재정렬

그룹 내의 저장소 객체에 적용될 그룹 작업의 순서를 변경할 수 있습니다. 그룹 작업은 순위에 따라 순차적으로 저장 객체에 적용됩니다. 가장 낮은 순위는 마지막으로 구성된 그룹 작업에 할당됩니다. 귀하의 요구 사항에 따라 그룹 작업의 순위를 변경할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단일 행이나 여러 행을 선택한 다음 드래그 앤 드롭 작업을 여러 번 수행하여 그룹 작업의 순위를 변경할 수 있습니다. 하지만 우선순위 재지정이 그룹 작업 그리드에 반영되도록 하려면 변경 사항을 저장해야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *그룹*을 클릭합니다.
2. 그룹 작업 탭에서 *재정렬*을 클릭합니다.
3. 그룹 작업 재정렬 대화 상자에서 행을 끌어서 놓아 필요에 따라 그룹 작업 순서를 재정렬합니다.
4. *저장*을 클릭하세요.

주석을 사용하여 스토리지 개체 이벤트의 우선 순위 지정

스토리지 객체에 주석 규칙을 만들고 적용하면 적용된 주석 유형과 우선순위에 따라 해당 객체를 식별하고 필터링할 수 있습니다.

주석에 대해 자세히 알아보세요

주석에 대한 개념을 이해하면 사용자 환경의 스토리지 개체와 관련된 이벤트를 관리하는 데 도움이 됩니다.

주석은 무엇입니까?

주석은 다른 텍스트 문자열(값)에 할당된 텍스트 문자열(이름)입니다. 각 주석 이름-값 쌍은 주석 규칙을 사용하여 저장소 개체와 동적으로 연결될 수 있습니다. 저장소 객체를 사전 정의된 주석과 연결하면 해당 객체와 관련된 이벤트를 필터링하고 볼 수 있습니다. 클러스터, 볼륨 및 스토리지 가상 머신(SVM)에 주석을 적용할 수 있습니다.

각 주석 이름은 여러 개의 값을 가질 수 있으며, 각 이름-값 쌍은 규칙을 통해 저장 개체와 연결될 수 있습니다.

예를 들어, "Boston"과 "Canada" 값을 사용하여 "data-center"라는 이름의 주석을 만들 수 있습니다. 그런 다음 값 "Boston"을 사용하여 "data-center" 주석을 볼륨 v1에 적용할 수 있습니다. "data-center"라는 주석이 달린 볼륨 v1의 이벤트에 대한 알림이 생성되면 생성된 이메일에는 볼륨의 위치인 "Boston"이 표시되며, 이를 통해 문제의 우선순위를 지정하고 해결할 수 있습니다.

주식 규칙은 스토리지 개체(볼륨, 클러스터 또는 스토리지 가상 머신(SVM))에 주석을 달기 위해 정의하는 기준입니다. 주식 규칙을 정의하려면 조건 그룹이나 조건을 사용할 수 있습니다.

- 주식 규칙을 주식에 연결해야 합니다.
- 주식 규칙에 대해 개체 유형을 연결해야 합니다. 주식 규칙에 대해 하나의 개체 유형만 연결할 수 있습니다.
- Unified Manager는 각 모니터링 주기가 끝날 때마다 또는 규칙이 생성, 편집, 삭제 또는 재정렬될 때마다 스토리지 개체에 주석을 추가하거나 제거합니다.
- 주식 규칙에는 하나 이상의 조건 그룹이 있을 수 있으며, 각 조건 그룹에는 하나 이상의 조건이 있을 수 있습니다.
- 저장 객체에는 여러 개의 주석이 있을 수 있습니다. 특정 주식에 대한 주식 규칙은 규칙 조건에서 다른 주석을 사용하여 이미 주석이 달린 개체에 다른 주석을 추가할 수도 있습니다.

정황

여러 개의 조건 그룹을 만들 수 있으며, 각 조건 그룹에는 하나 이상의 조건이 포함될 수 있습니다. 저장소 객체에 주석을 달기 위해 주식 규칙에 정의된 모든 조건 그룹을 적용할 수 있습니다.

조건 그룹 내의 조건은 논리적 AND를 사용하여 실행됩니다. 조건 그룹의 모든 조건이 충족되어야 합니다. 주식 규칙을 만들거나 수정하면 조건 그룹의 모든 조건을 충족하는 스토리지 개체만 적용하고 선택하고 주석을 다는 조건이 생성됩니다. 저장 객체에 주석을 달 범위를 좁히려는 경우 조건 그룹 내에서 여러 조건을 사용할 수 있습니다.

다음 피연산자와 연산자를 사용하고 필요한 값을 지정하여 저장 객체로 조건을 생성할 수 있습니다.

저장 객체 유형	적용 가능한 피연산자
용량	• 객체 이름 • 소유 클러스터 이름 • SVM 이름 소유 • 주식
서포트 머신(SVM)	• 객체 이름 • 소유 클러스터 이름 • 주식
무리	• 객체 이름 • 주식

저장 객체에 대한 피연산자로 주석을 선택하면 “Is” 연산자를 사용할 수 있습니다. 다른 모든 피연산자의 경우 연산자로 “Is” 또는 “Contains”를 선택할 수 있습니다. “Is” 연산자를 선택하면, 선택된 피연산자에 제공된 값과 피연산자 값이 정확히 일치하는지 여부가 조건 평가에서 평가됩니다. Contains 연산자를 선택하면 조건이 다음 기준 중 하나를 충족하는지 평가됩니다.

- 피연산자 값은 선택한 피연산자 값과 정확히 일치합니다.
- 피연산자 값에는 선택된 피연산자에 대해 제공된 값이 포함됩니다.

조건이 포함된 주석 규칙의 예

다음 두 가지 조건이 있는 볼륨에 대한 하나의 조건 그룹이 있는 주석 규칙을 고려하세요.

- 이름에 "vol"이 포함되어 있습니다.
- SVM 이름은 "data_svm"입니다.

이 주석 규칙은 이름에 "vol"이 포함되고 이름이 "data_svm"인 SVM에 호스팅된 모든 볼륨에 선택한 주석과 주석 유형을 주석으로 지정합니다.

조건 그룹

조건 그룹은 논리적 OR을 사용하여 실행된 다음 저장소 개체에 적용됩니다. 저장 객체는 주석을 달기 위해 조건 그룹 중 하나의 요구 사항을 충족해야 합니다. 모든 조건 그룹의 조건을 충족하는 저장 객체에 주석이 달립니다. 조건 그룹을 사용하면 주석이 추가될 저장 객체의 범위를 늘릴 수 있습니다.

조건 그룹이 있는 주석 규칙의 예

볼륨에 대한 두 개의 조건 그룹이 있는 주석 규칙을 고려합니다. 각 그룹에는 다음 두 가지 조건이 포함되어 있습니다.

- 조건 그룹 1
 - 이름에 "vol"이 포함되어 있습니다.
 - SVM 이름은 "data_svm"입니다. 이 조건 그룹은 이름에 "vol"이 포함되어 있고 이름이 "data_svm"인 SVM에 호스팅된 모든 볼륨에 주석을 추가합니다.
- 조건 그룹 2
 - 이름에 "vol"이 포함되어 있습니다.
 - data-priority의 주석 값은 "critical"입니다. 이 조건 그룹은 이름에 "vol"이 포함되고 data-priority 주석 값이 "critical"인 모든 볼륨에 주석을 추가합니다.

이 두 조건 그룹을 포함하는 주석 규칙이 스토리지 개체에 적용되면 다음 스토리지 개체에 주석이 추가됩니다.

- 이름에 "vol"이 포함되어 있고 SVM에서 "data_svm"이라는 이름으로 호스팅되는 모든 볼륨입니다.
- 이름에 "vol"이 포함되어 있고 데이터 우선순위 주석 값이 "critical"로 주석 처리된 모든 볼륨입니다.

미리 정의된 주석 값에 대한 설명

데이터 우선순위는 미션 크리티컬, 높음, 낮음 값을 갖는 미리 정의된 주석입니다. 이러한 값을 사용하면 포함된 데이터의 우선순위에 따라 저장소 개체에 주석을 달 수 있습니다. 미리 정의된 주석 값은 편집하거나 삭제할 수 없습니다.

- 데이터 우선 순위: 미션 크리티컬

이 주석은 미션 크리티컬 데이터가 포함된 스토리지 개체에 적용됩니다. 예를 들어, 프로덕션 애플리케이션을 포함하는 객체는 미션 크리티컬로 간주될 수 있습니다.

- 데이터 우선 순위: 높음

이 주석은 우선순위가 높은 데이터가 포함된 스토리지 개체에 적용됩니다. 예를 들어, 비즈니스 애플리케이션을

호스팅하는 객체는 높은 우선순위로 간주될 수 있습니다.

- 데이터 우선순위: 낮음

이 주석은 우선순위가 낮은 데이터를 포함하는 저장소 객체에 적용됩니다. 예를 들어, 백업 및 미러 대상과 같은 보조 저장소에 있는 개체는 우선순위가 낮을 수 있습니다.

동적으로 주석 추가

사용자 정의 주석을 만들면 Unified Manager는 규칙을 사용하여 클러스터, 스토리지 가상 머신(SVM) 및 볼륨을 주석과 동적으로 연결합니다. 이러한 규칙은 자동으로 주석을 저장 객체에 할당합니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *주석*을 클릭합니다.
2. 주석 페이지에서 *주석 추가*를 클릭합니다.
3. 주석 추가 대화 상자에서 주석의 이름과 설명을 입력합니다.
4. 선택 사항: 주석 값 섹션에서 *추가*를 클릭하여 주석에 값을 추가합니다.
5. *저장*을 클릭하세요.

주석에 값 추가

주석에 값을 추가한 다음 저장소 객체를 특정 주석 이름-값 쌍과 연결할 수 있습니다. 주석에 값을 추가하면 저장소 객체를 보다 효과적으로 관리하는 데 도움이 됩니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

미리 정의된 주석에는 값을 추가할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *주석*을 클릭합니다.
2. 주석 페이지에서 값을 추가할 주석을 선택한 다음 값 섹션에서 *추가*를 클릭합니다.
3. 주석 값 추가 대화 상자에서 주석 값을 지정합니다.

지정한 값은 선택한 주석에 대해 고유해야 합니다.

4. *추가*를 클릭하세요.

주석 삭제

더 이상 필요하지 않은 사용자 정의 주석과 해당 값을 삭제할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 주식 값은 다른 주식이나 그룹 규칙에서 사용할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *주식*을 클릭합니다.
2. 주식 탭에서 삭제하려는 주식을 선택합니다.

선택한 주식의 세부 정보가 표시됩니다.

3. 작업 > *삭제*를 클릭하여 선택한 주식과 해당 값을 삭제합니다.
4. 경고 대화 상자에서 *예*를 클릭하여 삭제를 확인합니다.

주식 목록 및 세부 정보 보기

클러스터, 볼륨 및 스토리지 가상 머신(SVM)과 동적으로 연결된 주식 목록을 볼 수 있습니다. 또한 설명, 작성자, 작성 날짜, 값, 규칙, 주식과 연관된 개체 등의 세부 정보를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *주식*을 클릭합니다.
2. 주식 탭에서 주식 이름을 클릭하면 관련 세부 정보를 볼 수 있습니다.

주식에서 값 삭제

해당 값이 더 이상 주식에 적용되지 않으면 사용자 정의 주식과 연관된 값을 삭제할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 주식 값은 어떠한 주식 규칙이나 그룹 규칙과도 연관되어서는 안 됩니다.

미리 정의된 주식의 값을 삭제할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *주식*을 클릭합니다.
2. 주식 탭의 주식 목록에서 값을 삭제할 주식을 선택합니다.
3. 주식 탭의 값 영역에서 삭제하려는 값을 선택한 다음 *삭제*를 클릭합니다.
4. 경고 대화 상자에서 *예*를 클릭합니다.

값이 삭제되고 선택한 주식의 값 목록에 더 이상 표시되지 않습니다.

주식 규칙 만들기

Unified Manager가 볼륨, 클러스터 또는 스토리지 가상 머신(SVM)과 같은 스토리지 개체에 동적으로 주식을 달기 위해 사용하는 주식 규칙을 만들 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

현재 모니터링 중인 스토리지 객체는 주석 규칙이 생성되는 즉시 주석이 달립니다. 모니터링 주기가 완료된 후에만 새로운 객체에 주석이 달립니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *주석*을 클릭합니다.
2. 주석 규칙 탭에서 *추가*를 클릭합니다.
3. 주석 규칙 추가 대화 상자에서 주석 규칙의 이름을 지정합니다.
4. 대상 개체 유형 필드에서 주석을 달고자 하는 저장소 개체 유형을 선택합니다.
5. 주석 적용 필드에서 사용할 주석과 주석 값을 선택합니다.
6. 조건 섹션에서 적절한 작업을 수행하여 조건, 조건 그룹 또는 둘 다를 만듭니다.

만들려면...	이렇게 하세요...
조건	a. 피연산자 목록에서 피연산자를 선택합니다. b. 연산자로 포함 또는 *있음*을 선택하세요. c. 값을 입력하거나 사용 가능한 목록에서 값을 선택하세요.
조건 그룹	a. *조건 그룹 추가*를 클릭합니다. b. 피연산자 목록에서 피연산자를 선택합니다. c. 연산자로 포함 또는 *있음*을 선택하세요. d. 값을 입력하거나 사용 가능한 목록에서 값을 선택하세요. e. 필요한 경우 *조건 추가*를 클릭하여 더 많은 조건을 만들고 각 조건에 대해 a~d 단계를 반복합니다.

7. *추가*를 클릭하세요.

주석 규칙 생성 예

주석 규칙 추가 대화 상자에서 다음 단계를 수행하여 주석 규칙을 만듭니다. 여기에는 조건 구성 및 조건 그룹 추가가 포함됩니다.

단계

1. 주석 규칙의 이름을 지정합니다.
2. 대상 개체 유형을 스토리지 가상 머신(SVM)으로 선택합니다.
3. 주석 목록에서 주석을 선택하고 값을 지정합니다.
4. 조건 섹션에서 피연산자로 *개체 이름*을 선택합니다.
5. 연산자로 *포함*을 선택합니다.

6. 값을 입력하세요 `svm_data`.
7. *조건 그룹 추가*를 클릭합니다.
8. 피연산자로 *개체 이름*을 선택합니다.
9. 연산자로 *포함*을 선택합니다.
10. 값을 입력하세요 `vol`.
11. *조건 추가*를 클릭하세요.
12. 8단계에서 피연산자로 *data-priority*를 선택하고, 9단계에서 연산자로 *Is*를 선택하고, 10단계에서 값으로 *mission-critical*을 선택하여 8단계부터 10단계까지 반복합니다.
13. *추가*를 클릭하세요.

개별 저장소 객체에 수동으로 주석 추가

주석 규칙을 사용하지 않고도 선택한 볼륨, 클러스터 및 SVM에 수동으로 주석을 달 수 있습니다. 단일 저장소 개체 또는 여러 저장소 개체에 주석을 달 수 있으며, 주석에 필요한 이름-값 쌍 조합을 지정할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 주석을 달고 싶은 저장소 개체로 이동합니다.

주석을 추가하려면...	이렇게 하세요...
클러스터	a. 저장소 > *클러스터*를 클릭합니다. b. 하나 이상의 클러스터를 선택하세요.
볼륨	a. 저장소 > *볼륨*을 클릭합니다. b. 하나 이상의 볼륨을 선택하세요.
SVM	a. 저장소 > *SVM*을 클릭합니다. b. 하나 이상의 SVM을 선택하세요.

2. *주석*을 클릭하고 이름-값 쌍을 선택합니다.
3. *적용*을 클릭하세요.

주석 규칙 편집

주석 규칙을 편집하여 조건 그룹과 조건 그룹 내의 조건을 수정하고, 스토리지 객체에 주석을 추가하거나 스토리지 객체에서 주석을 제거할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

연관된 주식 규칙을 편집하면 주식이 저장소 개체에서 분리됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *주식*을 클릭합니다.
2. 주식 규칙 탭에서 편집하려는 주식 규칙을 선택한 다음 작업 > *편집*을 클릭합니다.
3. 주식 규칙 편집 대화 상자에서 필요에 따라 규칙 이름, 주식 이름 및 값, 조건 그룹, 조건을 변경합니다.

주식 규칙에 대한 대상 개체 유형을 변경할 수 없습니다.

4. *저장*을 클릭하세요.

주식 규칙에 대한 조건 구성

Unified Manager가 저장소 개체에 적용하는 주식 규칙을 생성하기 위해 하나 이상의 조건을 구성할 수 있습니다. 주식 규칙을 만족하는 저장 객체에는 규칙에 지정된 값이 주식으로 처리됩니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *주식*을 클릭합니다.
2. 주식 규칙 탭에서 *추가*를 클릭합니다.
3. 주식 규칙 추가 대화 상자에서 규칙의 이름을 입력합니다.
4. 대상 개체 유형 목록에서 하나의 개체 유형을 선택한 다음, 목록에서 주식 이름과 값을 선택합니다.
5. 대화 상자의 조건 섹션에서 목록에서 피연산자와 연산자를 선택하고 조건 값을 입력하거나 *조건 추가*를 클릭하여 새 조건을 만듭니다.
6. *저장 및 추가*를 클릭하세요.

주식 규칙에 대한 조건 구성의 예

객체 이름에 "svm_data"가 포함된 객체 유형 SVM에 대한 조건을 고려합니다.

주식 규칙 추가 대화 상자에서 다음 단계를 수행하여 조건을 구성합니다.

단계

1. 주식 규칙의 이름을 입력하세요.
2. 대상 객체 유형을 SVM으로 선택합니다.
3. 주식 목록에서 주식과 값을 선택합니다.
4. 조건 필드에서 피연산자로 *개체 이름*을 선택합니다.
5. 연산자로 *포함*을 선택합니다.
6. 값을 입력하세요 svm_data .

7. *추가*를 클릭하세요.

주석 규칙 삭제

규칙이 더 이상 필요하지 않으면 Active IQ Unified Manager 에서 주석 규칙을 삭제할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

주석 규칙을 삭제하면 주석이 연결 해제되고 저장소 개체에서 제거됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *주석*을 클릭합니다.
2. 주석 규칙 탭에서 삭제하려는 주석 규칙을 선택한 다음 *삭제*를 클릭합니다.
3. 경고 대화 상자에서 *예*를 클릭하여 삭제를 확인합니다.

주석 규칙 재정렬

Unified Manager가 스토리지 개체에 주석 규칙을 적용하는 순서를 변경할 수 있습니다. 주석 규칙은 순위에 따라 순차적으로 저장 객체에 적용됩니다. 주석 규칙을 구성하면 순위가 가장 낮습니다. 하지만 요구 사항에 따라 주석 규칙의 순위를 변경할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단일 행이나 여러 행을 선택하고 드래그 앤 드롭 작업을 여러 번 수행하여 주석 규칙의 순위를 변경할 수 있습니다. 하지만 우선순위 재지정이 주석 규칙 탭에 표시되도록 하려면 변경 사항을 저장해야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *주석*을 클릭합니다.
2. 주석 규칙 탭에서 *재정렬*을 클릭합니다.
3. 주석 규칙 재정렬 대화 상자에서 하나 또는 여러 행을 끌어서 놓아 주석 규칙의 순서를 재정렬합니다.
4. *저장*을 클릭하세요.

재정렬이 표시되려면 변경 사항을 저장해야 합니다.

웹 UI 및 유지 관리 콘솔을 통해 지원 번들을 보내세요

AutoSupport 메시지에서 제공하는 것보다 더 자세한 진단 및 문제 해결이 필요한 경우 지원 번들을 보내야 합니다. Unified Manager 웹 UI와 유지 관리 콘솔을 사용하여 기술 지원팀에 지원 번들을 보낼 수 있습니다.

Unified Manager는 한 번에 최대 2개의 전체 지원 번들과 3개의 경량 지원 번들을 저장합니다.

관련 정보

AutoSupport 메시지와 지원 번들을 기술 지원팀에 보냅니다.

AutoSupport 페이지를 사용하면 기술 지원팀에 미리 정의된 AutoSupport 메시지와 주문형 AutoSupport 메시지를 보내 환경이 올바르게 작동하는지 확인하고 환경의 무결성을 유지하는 데 도움을 받을 수 있습니다. AutoSupport 기본적으로 활성화되어 있으며 NetAppActive IQ의 이점을 얻으려면 비활성화해서는 안 됩니다.

필요할 때마다 Unified Manager 서버에 대한 진단 시스템 정보와 자세한 데이터를 메시지로 보낼 수 있으며, 주기적으로 메시지를 보내도록 예약하거나, 심지어 지원 번들을 생성하여 기술 지원 팀에 보낼 수도 있습니다.



스토리지 관리자 역할을 가진 사용자는 주문형 AutoSupport 메시지와 지원 번들을 생성하여 기술 지원팀에 보낼 수 있습니다. 그러나 관리자나 유지 관리 사용자만이 주기적 AutoSupport 활성화하거나 비활성화하고 HTTP 프록시 서버 설정 섹션에 설명된 대로 HTTP 설정을 구성할 수 있습니다. HTTP 프록시 서버를 사용해야 하는 환경에서는 스토리지 관리자가 기술 지원팀에 주문형 AutoSupport 메시지와 지원 번들을 보내기 전에 구성이 완료되어야 합니다.

주문형 **AutoSupport** 메시지 보내기

기술 지원팀이나 지정된 이메일 수신자, 또는 두 곳 모두에 주문형 메시지를 생성하여 보낼 수 있습니다.

단계

1. 일반 > * AutoSupport*로 이동하여 다음 작업 중 하나 또는 둘 다를 수행합니다.
2. AutoSupport 메시지를 기술 지원팀에 보내려면 기술 지원팀에 보내기 확인란을 선택하세요.
3. 특정 이메일 수신자에게 AutoSupport 메시지를 보내려면 이메일 수신자에게 보내기 확인란을 선택하고 수신자의 이메일 주소를 입력합니다.
4. *저장*을 클릭하세요.
5. * AutoSupport 생성 및 보내기*를 클릭하세요.

주기적 **AutoSupport** 활성화

문제 진단 및 해결을 위해 기술 지원팀에 구체적이고 미리 정의된 메시지를 주기적으로 보낼 수 있습니다. 이 기능은 기본적으로 활성화되어 있습니다. 비활성화된 경우 관리자나 유지 관리 사용자가 설정을 활성화할 수 있습니다.

단계

1. 일반 > * AutoSupport*로 이동합니다.
2. 주기적 AutoSupport 섹션에서 * Active IQ 에 AutoSupport 데이터 주기적으로 전송 활성화* 확인란을 선택합니다.
3. 필요한 경우 HTTP 프록시 서버 설정 섹션에 설명된 대로 HTTP 프록시 서버의 이름, 포트 및 인증 정보를 정의합니다.
4. *저장*을 클릭하세요.

주문형 지원 번들 업로드

문제 해결 요구 사항에 따라 지원 번들을 생성하여 기술 지원팀에 보낼 수 있습니다. Unified Manager는 가장 최근에 생성된 두 개의 지원 번들만 저장합니다. 이전 지원 번들은 시스템에서 삭제됩니다.

일부 유형의 지원 데이터는 많은 양의 클러스터 리소스를 사용하거나 완료하는 데 오랜 시간이 걸릴 수 있으므로 전체 지원 번들을 선택하면 특정 데이터 유형을 포함하거나 제외하여 지원 번들 크기를 줄일 수 있습니다. 또한 30일 분의 로그와 구성 데이터베이스 기록만 포함된 가벼운 지원 번들을 만드는 옵션도 있습니다. 여기에는 성능 데이터, 인수 기록 파일, 서버 힙 덤프가 제외됩니다.

단계

1. 일반 > * AutoSupport*로 이동합니다.
2. 주문형 지원 번들 섹션에서 *지원 번들 생성 및 전송*을 클릭합니다.
3. 기술 지원팀에 가벼운 지원 번들을 보내려면 지원 번들 생성 및 보내기 팝업에서 가벼운 지원 번들 생성 확인란을 선택합니다.
4. 또는 전체 지원 번들을 보내려면 전체 지원 번들 생성 확인란을 선택합니다. 지원 번들에 포함하거나 제외할 특정 데이터 유형을 선택합니다.



어떠한 데이터 유형도 선택하지 않더라도 지원 번들은 다른 Unified Manager 데이터와 함께 생성됩니다.

5. 번들을 기술 지원팀에 보내기 확인란을 선택하여 번들을 생성하고 기술 지원팀에 보냅니다. 이 확인란을 선택하지 않으면 번들이 생성되어 Unified Manager 서버에 로컬로 저장됩니다. 생성된 지원 번들은 나중에 VMware 시스템의 /support 디렉토리에서 사용할 수 있습니다. /opt/netapp/data/support/ Linux 시스템에서, 그리고 ProgramData\NetApp\OnCommandAppData\ocum\support Windows 시스템에서.
6. *보내기*를 클릭하세요.

HTTP 프록시 서버 설정

Unified Manager 서버에서 직접 액세스할 수 없는 환경인 경우, AutoSupport 콘텐츠를 지원팀에 보내기 위해 인터넷 액세스를 제공하는 프록시를 지정할 수 있습니다. 이 섹션은 관리자와 유지 관리 사용자만 사용할 수 있습니다.

• HTTP 프록시 사용

HTTP 프록시로 사용되는 서버를 식별하려면 이 상자를 선택하세요.

프록시 서버의 호스트 이름 또는 IP 주소와 서버에 연결하는 데 사용되는 포트 번호를 입력하세요.

• 인증을 사용하세요

HTTP 프록시로 사용되는 서버에 액세스하기 위해 인증 정보를 제공해야 하는 경우 이 상자를 선택하세요.

HTTP 프록시를 인증하는 데 필요한 사용자 이름과 비밀번호를 입력하세요.



기본 인증만 제공하는 HTTP 프록시는 지원되지 않습니다.

유지 관리 콘솔에 액세스하세요

Unified Manager 사용자 인터페이스가 작동하지 않거나 사용자 인터페이스에서 사용할 수 없는 기능을 수행해야 하는 경우 유지 관리 콘솔에 액세스하여 Unified Manager 시스템을 관리할 수 있습니다.

시작하기 전에

Unified Manager를 설치하고 구성해야 합니다.

15분 동안 아무런 활동이 없으면 유지 관리 콘솔에서 로그아웃됩니다.



VMware에 설치하는 경우 VMware 콘솔을 통해 유지 관리 사용자로 이미 로그인한 경우 Secure Shell을 사용하여 동시에 로그인할 수 없습니다.

단계

1. 유지 관리 콘솔에 액세스하려면 다음 단계를 따르세요.

이 운영체제에서는...	다음 단계를 따르세요...
VMware	a. Secure Shell을 사용하여 Unified Manager 가상 어플라이언스의 IP 주소 또는 정규화된 도메인 이름에 연결합니다. b. 유지 관리 사용자 이름과 비밀번호를 사용하여 유지 관리 콘솔에 로그인합니다.
리눅스	a. Secure Shell을 사용하여 Unified Manager 시스템의 IP 주소 또는 정규화된 도메인 이름에 연결합니다. b. 유지 관리 사용자(umadmin) 이름과 비밀번호로 시스템에 로그인합니다. c. 명령을 입력하세요 <code>maintenance_console</code> 그리고 Enter를 누르세요.
Windows	a. 관리자 자격 증명을 사용하여 Unified Manager 시스템에 로그인합니다. b. Windows 관리자 권한으로 PowerShell을 실행합니다. c. 명령을 입력하세요 <code>maintenance_console</code> 그리고 Enter를 누르세요.

Unified Manager 유지 관리 콘솔 메뉴가 표시됩니다.

지원 번들을 생성하고 업로드합니다.

진단 정보가 포함된 지원 번들을 생성한 후 기술 지원팀에 보내 문제 해결에 도움을 받을 수 있습니다.

Unified Manager 9.8부터 Unified Manager 서버가 인터넷에 연결되어 있으면 유지 관리 콘솔에서 NetApp 에 지원 번들을 업로드할 수도 있습니다.

시작하기 전에

유지 관리 사용자로서 유지 관리 콘솔에 액세스할 수 있어야 합니다.

일부 유형의 지원 데이터는 많은 양의 클러스터 리소스를 사용하거나 완료하는 데 오랜 시간이 걸릴 수 있으므로 전체 지원 번들을 선택하면 포함하거나 제외할 데이터 유형을 지정하여 지원 번들 크기를 줄일 수 있습니다. 또한 30일 분의 로그와 구성 데이터베이스 기록만 포함된 가벼운 지원 번들을 만드는 옵션도 있습니다. 여기에는 성능 데이터, 인수 기록 파일, 서버 힙 덤프가 제외됩니다.

Unified Manager는 가장 최근에 생성된 두 개의 지원 번들만 저장합니다. 이전 지원 번들은 시스템에서 삭제됩니다.

단계

1. 유지 관리 콘솔의 *메인 메뉴*에서 *지원/진단*을 선택합니다.
2. 지원 번들에 포함할 세부 정보 수준에 따라 가벼운 지원 번들 생성 또는 *지원 번들 생성*을 선택하세요.
3. 전체 지원 번들을 선택하는 경우 지원 번들에 포함하거나 제외할 다음 데이터 유형을 선택하거나 선택 해제합니다.

- 데이터베이스 덤프

MySQL 서버 데이터베이스의 덤프.

- 힙 덤프

Unified Manager 서버 프로세스의 주요 상태 스냅샷입니다. 이 옵션은 기본적으로 비활성화되어 있으며 고객 지원팀에서 요청할 때만 선택해야 합니다.

- 획득 녹음

Unified Manager와 모니터링되는 클러스터 간의 모든 통신을 기록합니다.



모든 데이터 유형을 선택 해제하더라도 지원 번들은 다른 Unified Manager 데이터와 함께 생성됩니다.

4. 유형 *g* 을 입력한 다음 Enter를 눌러 지원 번들을 생성합니다.

지원 번들 생성은 메모리를 많이 사용하는 작업이므로 이때 지원 번들을 생성할지 확인하라는 메시지가 표시됩니다.

5. 유형 *y* 을 입력한 다음 Enter를 눌러 지원 번들을 생성합니다.

지금 지원 번들을 생성하지 않으려면 다음을 입력하십시오. *n* 를 입력한 다음 Enter를 누릅니다.

6. 전체 지원 번들에 데이터베이스 덤프 파일을 포함한 경우 성능 통계를 포함할 기간을 지정하라는 메시지가 표시됩니다. 성능 통계를 포함하려면 많은 시간과 공간이 필요하므로 성능 통계를 포함하지 않고 데이터베이스를 덤프할 수도 있습니다.

- a. 시작 날짜를 YYYYMMDD 형식으로 입력하세요.

예를 들어 다음을 입력하세요. 20210101 2021년 1월 1일 기준. 입력하다 *n* 성과 통계를 포함하지 않으려면.

- b. 지정된 시작 날짜의 오전 12시부터 시작하여 포함할 통계의 일 수를 입력합니다.

1에서 10까지의 숫자를 입력할 수 있습니다.

성과 통계를 포함하는 경우 시스템은 성과 통계를 수집하는 기간을 표시합니다.

7. 지원 번들이 생성되면 NetApp 에 업로드할지 여부를 묻는 메시지가 표시됩니다. 유형 *y* 를 입력한 다음 Enter를

누릅니다.

지원 사례 번호를 입력하라는 메시지가 표시됩니다.

8. 이미 사건 번호가 있는 경우, 번호를 입력하고 Enter를 누르세요. 그렇지 않으면 Enter를 누르세요.

지원 번들은 NetApp에 업로드됩니다.

Unified Manager 서버가 인터넷에 연결되어 있지 않거나 다른 이유로 지원 번들을 업로드할 수 없는 경우, 해당 번들을 검색하여 수동으로 보낼 수 있습니다. SFTP 클라이언트를 사용하거나 UNIX 또는 Linux CLI 명령을 사용하여 검색할 수 있습니다. Windows 설치에서는 원격 데스크톱(RDP)을 사용하여 지원 번들을 검색할 수 있습니다.

생성된 지원 번들은 VMware 시스템의 /support 디렉토리, Linux 시스템의 /opt/netapp/data/support/ 디렉토리, Windows 시스템의 ProgramData\NetApp\OnCommandAppData\ocum\support 디렉토리에 있습니다.

관련 정보

"Unified Manager 사용자 역할 및 기능"

Windows 클라이언트를 사용하여 지원 번들 검색

Windows 사용자의 경우 Unified Manager 서버에서 지원 번들을 검색하는 도구를 다운로드하여 설치할 수 있습니다. 문제에 대한 보다 자세한 진단을 위해 기술 지원팀에 지원 번들을 보낼 수 있습니다. Filezilla나 WinSCP는 사용할 수 있는 도구의 예입니다.

시작하기 전에

이 작업을 수행하려면 유지 관리 사용자여야 합니다.

SCP 또는 SFTP를 지원하는 도구를 사용해야 합니다.

단계

1. 지원 번들을 검색하기 위한 도구를 다운로드하여 설치하세요.
2. 도구를 엽니다.
3. SFTP를 통해 Unified Manager 관리 서버에 연결합니다.

이 도구는 /support 디렉토리의 내용을 표시하며, 기존의 모든 지원 번들을 볼 수 있습니다.

4. 복사하려는 지원 번들의 대상 디렉토리를 선택하세요.
5. 복사하려는 지원 번들을 선택하고 도구를 사용하여 Unified Manager 서버에서 로컬 시스템으로 파일을 복사합니다.

UNIX 또는 Linux 클라이언트를 사용하여 지원 번들을 검색합니다.

UNIX 또는 Linux 사용자의 경우 Linux 클라이언트 서버에서 명령줄 인터페이스(CLI)를 사용하여 vApp에서 지원 번들을 검색할 수 있습니다. SCP 또는 SFTP를 사용하여 지원 번들을 검색할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 유지 관리 사용자여야 합니다.

유지 관리 콘솔을 사용하여 지원 번들을 생성해야 하며 지원 번들 이름을 사용할 수 있어야 합니다.

단계

1. Linux 클라이언트 서버를 사용하여 Telnet이나 콘솔을 통해 CLI에 액세스합니다.
2. 접속하세요/support 예매 규칙서.
3. 다음 명령을 사용하여 지원 번들을 검색하여 로컬 디렉토리에 복사합니다.

만약 당신이 사용하고 있다면...	그런 다음 다음 명령을 사용하세요...
SCP	<code>scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>
SFTP	<code>sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>

지원 번들의 이름은 유지 관리 콘솔을 사용하여 생성할 때 제공됩니다.

4. 유지관리 사용자 비밀번호를 입력하세요.

예시

다음 예제에서는 SCP를 사용하여 지원 번들을 검색합니다.

```
`$ scp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
support_bundle_20160216_145359.7z 100% 119MB 11.9MB/s 00:10
```

다음 예제에서는 SFTP를 사용하여 지원 번들을 검색합니다.

```
`$ sftp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
Connected to 10.228.212.69.
Fetching /support/support_bundle_20130216_145359.7z to
./support_bundle_20130216_145359.7z
/support/support_bundle_20160216_145359.7z
```

기술 지원팀에 지원 번들을 보내세요

문제에 AutoSupport 메시지에서 제공하는 것보다 더 자세한 진단 및 문제 해결 정보가 필요한

경우 기술 지원팀에 지원 번들을 보낼 수 있습니다.

시작하기 전에

기술 지원팀에 문의하려면 지원 번들에 액세스할 수 있어야 합니다.

기술 지원 웹사이트를 통해 생성된 사례 번호가 있어야 합니다.

단계

1. NetApp 지원 사이트에 로그인하세요.
2. 파일을 업로드하세요.

["NetApp 에 파일을 업로드하는 방법"](#)

여러 워크플로와 관련된 작업 및 정보

이벤트에 대한 메모 추가 및 검토, 이벤트 할당, 이벤트 확인 및 해결, 볼륨, 스토리지 가상 머신(SVM), 집계 등에 대한 세부 정보를 포함하여 워크플로를 이해하고 완료하는 데 도움이 되는 일부 작업과 참조 텍스트는 Unified Manager의 많은 워크플로에서 공통적입니다.

클러스터 구성 요소와 이들이 경쟁에 참여할 수 있는 이유

클러스터 구성 요소가 경합에 들어가면 클러스터 성능 문제를 식별할 수 있습니다. 해당 구성 요소를 사용하는 워크로드의 성능이 저하되고 클라이언트 요청에 대한 응답 시간(대기 시간)이 늘어나 Unified Manager에서 이벤트가 발생합니다.

경쟁 상태에 있는 구성 요소는 최적의 수준에서 성능을 발휘할 수 없습니다. 성능이 저하되었고, 피해자라고 불리는 다른 클러스터 구성 요소와 워크로드의 성능으로 인해 지연 시간이 증가했을 수 있습니다. 구성 요소를 경쟁에서 벗어나게 하려면 작업 부하를 줄이거나 더 많은 작업을 처리할 수 있는 능력을 높여야 합니다. 이렇게 하면 성능이 정상 수준으로 돌아갈 수 있습니다. Unified Manager는 5분 간격으로 워크로드 성능을 수집하고 분석하므로 클러스터 구성 요소가 지속적으로 과도하게 사용되는 경우에만 감지합니다. 5분 간격 내에 짧은 시간 동안만 지속되는 과도한 사용의 일시적인 급증은 감지되지 않습니다.

예를 들어, 스토리지 집계는 하나 이상의 워크로드가 I/O 요청을 처리하기 위해 경쟁하고 있기 때문에 경합을 겪을 수 있습니다. 전체적으로 다른 작업 부하가 영향을 받아 성능이 저하될 수 있습니다. 집계된 활동량을 줄이려면 여러 가지 조치를 취할 수 있습니다. 예를 들어, 하나 이상의 작업 부하를 덜 바쁜 집계나 노드로 옮겨 현재 집계의 전반적인 작업 부하 수요를 줄이는 것입니다. QoS 정책 그룹의 경우 처리량 한도를 조정하거나 작업 부하를 다른 정책 그룹으로 이동하여 작업 부하가 더 이상 제한되지 않도록 할 수 있습니다.

Unified Manager는 다음 클러스터 구성 요소를 모니터링하여 해당 구성 요소가 경쟁 상태에 있을 때 경고합니다.

- 회로망

클러스터의 외부 네트워킹 프로토콜에 의한 I/O 요청의 대기 시간을 나타냅니다. 대기 시간이란 클러스터가 I/O 요청에 응답하기 전에 "전송 준비" 트랜잭션이 완료될 때까지 기다리는 시간입니다. 네트워크 구성 요소가 경합 중이면 프로토콜 계층에서 대기 시간이 길어져 하나 이상의 작업 부하 지연에 영향을 미치고 있음을 의미합니다.

- 네트워크 처리

프로토콜 계층과 클러스터 간의 I/O 처리와 관련된 클러스터의 소프트웨어 구성 요소를 나타냅니다. 이벤트가 감지된 이후 네트워크 처리를 담당하는 노드가 변경되었을 수 있습니다. 네트워크 처리 구성 요소가 경합 중이면

네트워크 처리 노드의 높은 활용도가 하나 이상의 작업 부하의 지연 시간에 영향을 미치고 있음을 의미합니다.

액티브-액티브 구성에서 All SAN 어레이 클러스터를 사용하는 경우 두 노드 모두에 대한 네트워크 처리 지연 값이 표시되므로 노드가 부하를 동등하게 공유하는지 확인할 수 있습니다.

- **QoS 제한 최대**

작업 부하에 할당된 스토리지 서비스 품질(QoS) 정책 그룹의 처리량 최대(피크) 설정을 나타냅니다. 정책 그룹 구성 요소가 경합 중이면 정책 그룹의 모든 작업 부하가 설정된 처리량 한도로 조절되고 있음을 의미하며, 이는 해당 작업 부하 중 하나 이상의 대기 시간에 영향을 미칩니다.

- **QoS 제한 최소값**

다른 워크로드에 할당된 QoS 처리량 최소(예상) 설정으로 인해 발생하는 워크로드 지연을 나타냅니다. 특정 작업 부하에 설정된 QoS 최소값이 약속된 처리량을 보장하기 위해 대부분의 대역폭을 사용하는 경우, 다른 작업 부하가 제한되고 지연 시간이 더 길어집니다.

- **클러스터 상호 연결**

클러스터된 노드가 물리적으로 연결된 케이블과 어댑터를 나타냅니다. 클러스터 상호 연결 구성 요소가 경합 중이면 클러스터 상호 연결에서 I/O 요청에 대한 대기 시간이 길어져 하나 이상의 작업 부하 대기 시간에 영향을 미치고 있음을 의미합니다.

- *** Data Processing***

클러스터와 작업 부하가 포함된 스토리지 집계 간의 I/O 처리와 관련된 클러스터의 소프트웨어 구성 요소를 나타냅니다. 이벤트가 감지된 이후 데이터 처리를 담당하는 노드가 변경되었을 수 있습니다. 데이터 처리 구성 요소가 경합 중이라는 것은 데이터 처리 노드의 높은 활용도가 하나 이상의 워크로드의 대기 시간에 영향을 미치고 있음을 의미합니다.

- **볼륨 활성화**

모든 활성 볼륨의 사용량을 추적하는 프로세스를 나타냅니다. 1000개가 넘는 볼륨이 활성화된 대규모 환경에서 이 프로세스는 노드를 통해 동시에 리소스에 액세스해야 하는 중요 볼륨의 수를 추적합니다. 동시 활성 볼륨 수가 권장되는 최대 임계값을 초과하면 일부 비중요 볼륨에서 여기에 명시된 대로 지연이 발생합니다.

- *** MetroCluster 리소스***

MetroCluster 구성에서 클러스터 간에 데이터를 미러링하는 데 사용되는 NVRAM 및 ISL(스위치 간 링크)을 포함한 MetroCluster 리소스를 나타냅니다. MetroCluster 구성 요소가 경합 중이면 로컬 클러스터의 작업 부하에서 높은 쓰기 처리량이 발생하거나 링크 상태 문제로 인해 로컬 클러스터에서 하나 이상의 작업 부하의 대기 시간이 영향을 받고 있음을 의미합니다. 클러스터가 MetroCluster 구성에 없으면 이 아이콘이 표시되지 않습니다.

- **집계 또는 SSD 집계 작업**

워크로드가 실행되는 스토리지 집계를 나타냅니다. 집계 구성 요소가 경합 중이면 집계의 높은 활용도가 하나 이상의 워크로드의 대기 시간에 영향을 미치고 있음을 의미합니다. 집계는 모든 HDD로 구성되거나 HDD와 SSD의 혼합(Flash Pool 집계), 또는 HDD와 클라우드 계층의 혼합(FabricPool 집계)으로 구성됩니다. "SSD 집계"는 모든 SSD(울플래시 집계)로 구성되거나 SSD와 클라우드 계층(FabricPool 집계)의 혼합으로 구성됩니다.

- **클라우드 지연 시간**

클러스터와 사용자 데이터가 저장된 클라우드 계층 간의 I/O 처리와 관련된 클러스터의 소프트웨어 구성 요소를 나타냅니다. 클라우드 지연 시간 구성 요소가 경합되는 경우 클라우드 계층에서 호스팅되는 볼륨에서 많은 양의

읽기가 하나 이상의 워크로드의 지연 시간에 영향을 미치고 있음을 의미합니다.

- * SnapMirror 동기화*

SnapMirror 동기 관계에서 기본 볼륨에서 보조 볼륨으로 사용자 데이터를 복제하는 데 관련된 클러스터의 소프트웨어 구성 요소를 나타냅니다. 동기화 SnapMirror 구성 요소가 경합 중이면 SnapMirror 동기 작업의 활동이 하나 이상의 워크로드의 대기 시간에 영향을 미치고 있음을 의미합니다.

볼륨/상태 세부 정보 페이지

볼륨/상태 세부 정보 페이지를 사용하면 용량, 스토리지 효율성, 구성, 보호, 주식, 생성된 이벤트 등 선택한 볼륨에 대한 자세한 정보를 볼 수 있습니다. 해당 볼륨에 대한 관련 객체 및 관련 알림에 대한 정보도 볼 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

명령 버튼

명령 버튼을 사용하면 선택한 볼륨에 대해 다음 작업을 수행할 수 있습니다.

- 성능 보기로 전환

볼륨/성과 세부정보 페이지로 이동할 수 있습니다.

- 행위

- 알림 추가

선택한 볼륨에 알림을 추가할 수 있습니다.

- 임계값 편집

선택한 볼륨에 대한 임계값 설정을 수정할 수 있습니다.

- 주식 달기

선택한 볼륨에 주석을 달 수 있습니다.

- 보호하다

선택한 볼륨에 대해 SnapMirror 또는 SnapVault 관계를 만들 수 있습니다.

- 관계

다음 보호 관계 작업을 실행할 수 있습니다.

- 편집하다

기존 보호 관계에 대한 기존 SnapMirror 정책, 일정 및 최대 전송 속도를 변경할 수 있는 관계 편집 대화 상자를 실행합니다.

- 중단

선택한 관계에 대해 진행 중인 전송을 중단합니다. 선택적으로 기존 전송 이외의 전송에 대한 재시작 체크포인트를 제거할 수 있습니다. 기존 전송에 대한 체크포인트를 제거할 수 없습니다.

- 침묵하다

선택한 관계에 대한 예약된 업데이트를 일시적으로 비활성화합니다. 이미 진행 중인 전송은 관계가 중단되기 전에 완료되어야 합니다.

- 부서지다

소스 볼륨과 대상 볼륨 간의 관계를 끊고 대상을 읽기-쓰기 볼륨으로 변경합니다.

- 제거하다

선택한 소스와 대상 간의 관계를 영구적으로 삭제합니다. 볼륨은 파괴되지 않으며 볼륨의 스냅샷 복사본은 제거되지 않습니다. 이 작업은 실행 취소할 수 없습니다.

- 재개하다

정지된 관계에 대한 예약된 전송을 활성화합니다. 다음에 예정된 전송 간격에서는 재시작 체크포인트가 있는 경우 이를 사용합니다.

- 재동기화

이전에 끊어진 관계를 다시 동기화할 수 있습니다.

- 초기화/업데이트

새로운 보호 관계에 대한 최초의 기준 전송을 수행하거나 관계가 이미 초기화된 경우 수동 업데이트를 수행할 수 있습니다.

- 역방향 재동기화

이전에 끊어진 보호 관계를 재설정하고, 원본과 대상의 기능을 반대로 하여 원본을 원본 대상의 복사본으로 만들 수 있습니다. 소스의 콘텐츠는 대상의 콘텐츠로 덮어쓰여지고, 공통 스냅샷 복사본의 데이터보다 최신인 데이터는 삭제됩니다.

- 복원하다

한 볼륨에서 다른 볼륨으로 데이터를 복원할 수 있습니다. 자세한 내용은 다음을 참조하세요. "[볼륨/상태 세부 정보 페이지를 사용하여 데이터 복원](#)".



복원 버튼과 관계 작업 버튼은 동기식 보호 관계에 있는 볼륨에는 사용할 수 없습니다.

- 볼륨 보기

Health: All Volumes 보기로 이동할 수 있습니다.

용량 탭

용량 탭에는 선택한 볼륨에 대한 세부 정보(실제 용량, 논리적 용량, 임계값 설정, 할당량 용량, 볼륨 이동 작업에 대한 정보 등)가 표시됩니다.

- 물리적 수용 인원

볼륨의 물리적 용량을 자세히 설명합니다.

- 스냅샷 오버플로

스냅샷 복사본에 사용되는 데이터 공간을 표시합니다.

- 사용된

볼륨에서 데이터가 사용하는 공간을 표시합니다.

- 경고

볼륨의 공간이 거의 가득 찼음을 나타냅니다. 이 임계값을 초과하면 공간이 거의 가득 찼습니다 이벤트가 생성됩니다.

- 오류

볼륨의 공간이 가득 찼음을 나타냅니다. 이 임계값을 초과하면 공간 가득 참 이벤트가 생성됩니다.

- 쓸 수 없는

쓰인 프로비저닝된 볼륨 공간이 위험에 처해 있다는 이벤트가 생성되었으며, 쓰인 프로비저닝된 볼륨의 공간이 집계 용량 문제로 인해 위험에 처해 있음을 나타냅니다. 사용할 수 없는 용량은 쓰인 프로비저닝된 볼륨에 대해서만 표시됩니다.

- 데이터 그래프

볼륨의 총 데이터 용량과 사용된 데이터 용량을 표시합니다.

자동 증가가 활성화된 경우 데이터 그래프에는 집계에서 사용 가능한 공간도 표시됩니다. 데이터 그래프는 볼륨의 데이터가 사용할 수 있는 효과적인 저장 공간을 표시하며, 이는 다음 중 하나일 수 있습니다.

- 다음 조건에 따른 볼륨의 실제 데이터 용량:

- 자동 증가가 비활성화되었습니다.

- 자동 증가가 활성화된 볼륨이 최대 크기에 도달했습니다.

- 자동 증가가 활성화된 두껍게 프로비저닝된 볼륨은 더 이상 확장될 수 없습니다.

- 최대 볼륨 크기를 고려한 후 볼륨의 데이터 용량(쓰인 프로비저닝 볼륨 및 볼륨이 최대 크기에 도달할 수 있는 공간이 집계에 있는 경우 두꺼운 프로비저닝 볼륨의 경우)

- 다음 가능한 자동 증가 크기를 고려한 후 볼륨의 데이터 용량(자동 증가 백분율 임계값이 있는 두껍게 프로비저닝된 볼륨의 경우)

- 스냅샷 복사 그래프

이 그래프는 사용된 스냅샷 용량이나 스냅샷 예약이 0이 아닌 경우에만 표시됩니다.

두 그래프 모두 사용된 스냅샷 용량이 스냅샷 예약 용량을 초과하는 경우 스냅샷 용량이 스냅샷 예약 용량을 초과하는 용량을 표시합니다.

- 수용량 논리적

볼륨의 논리적 공간 특성을 표시합니다. 논리적 공간은 ONTAP 스토리지 효율성 기술을 사용하여 절감된 비용을 적용하지 않고 디스크에 저장되는 데이터의 실제 크기를 나타냅니다.

- 논리적 공간 보고

볼륨에 논리적 공간 보고가 구성되어 있는지 여부를 표시합니다. 값은 활성화, 비활성화 또는 적용 안 함으로 설정할 수 있습니다. 이전 버전의 ONTAP 에 있는 볼륨이나 논리적 공간 보고를 지원하지 않는 볼륨의 경우 "해당 없음"이 표시됩니다.

- 사용된

볼륨 내 데이터가 사용하는 논리적 공간의 양과 총 데이터 용량에 따른 논리적 공간 사용 비율을 표시합니다.

- 논리적 공간 강화

썬 프로비저닝 볼륨에 대해 논리적 공간 적용이 구성되어 있는지 여부를 표시합니다. 활성화로 설정하면 볼륨의 논리적 사용 크기는 현재 설정된 물리적 볼륨 크기보다 클 수 없습니다.

- 자동성장

볼륨에 공간이 부족할 때 볼륨을 자동으로 늘릴지 여부를 표시합니다.

- 공간 보장

볼륨이 집계에서 자유 블록을 제거할 때 FlexVol volume 설정 컨트롤을 표시합니다. 그러면 이러한 블록은 볼륨의 파일에 쓸 수 있도록 보장됩니다. 공간 보장은 다음 중 하나로 설정할 수 있습니다.

- None

볼륨에 대한 공간 보장이 구성되지 않았습니다.

- 파일

희소하게 기록된 파일(예: LUN)의 전체 크기가 보장됩니다.

- 용량

볼륨의 전체 크기가 보장됩니다.

- 부분적

FlexCache 볼륨은 크기에 따라 공간을 예약합니다. FlexCache 볼륨의 크기가 100MB 이상인 경우 최소 공간 보장은 기본적으로 100MB로 설정됩니다. FlexCache 볼륨의 크기가 100MB보다 작으면 최소 공간 보장은 FlexCache 볼륨의 크기로 설정됩니다. FlexCache 볼륨의 크기가 나중에 커지면 최소 공간 보장은 증가하지 않습니다.



볼륨이 Data-Cache 유형인 경우 공간 보장은 Partial입니다.

- 세부 정보(물리적)

볼륨의 물리적 특성을 표시합니다.

- 총 용량

볼륨의 총 물리적 용량을 표시합니다.

- 데이터 용량

볼륨에서 사용된 물리적 공간의 양(사용된 용량)과 볼륨에서 여전히 사용 가능한 물리적 공간의 양(여유 용량)을 표시합니다. 이러한 값은 전체 물리적 용량의 백분율로도 표시됩니다.

싹 프로비저닝된 볼륨에 대해 싹 프로비저닝된 볼륨 공간 위험 이벤트가 생성되면 볼륨에서 사용된 공간의 양(사용된 용량)과 볼륨에서 사용 가능하지만 집계 용량 문제로 인해 사용할 수 없는 공간의 양(사용 불가능 용량)이 표시됩니다.

- 스냅샷 예약

볼륨에서 스냅샷 복사본에 사용된 공간(사용된 용량)과 스냅샷 복사본에 사용 가능한 공간(여유 용량)을 표시합니다. 이러한 값은 전체 스냅샷 예약의 백분율로도 표시됩니다.

싹 프로비저닝된 볼륨에 대해 싹 프로비저닝된 볼륨 공간 위험 이벤트가 생성되면 스냅샷 복사본에 사용된 공간의 양(사용된 용량)과 볼륨에서 사용 가능하지만 집계 용량 문제로 인해 스냅샷 복사본을 만드는 데 사용할 수 없는 공간의 양(사용할 수 없는 용량)이 표시됩니다.

- 볼륨 임계값

다음 볼륨 용량 임계값을 표시합니다.

- 거의 가득 찬 임계값

볼륨이 거의 가득 찬 비율을 지정합니다.

- 전체 임계값

볼륨이 가득 찬 비율을 지정합니다.

- 기타 세부 정보

- 자동 증가 최대 크기

볼륨이 자동으로 커질 수 있는 최대 크기를 표시합니다. 생성 시 기본값은 볼륨 크기의 120%입니다. 이 필드는 볼륨에 대해 자동 증가가 활성화된 경우에만 표시됩니다.

- Qtree 할당량 약정 용량

할당량에 예약된 공간을 표시합니다.

- Qtree 할당량 초과 할당 용량

시스템에서 Volume Qtree Quota Overcommitted 이벤트를 생성하기 전에 사용할 수 있는 공간의 양을 표시합니다.

- 부분적 준비금

덮어쓰기 예약의 크기를 제어합니다. 기본적으로 부분 예약은 100으로 설정되어, 필요한 예약 공간의 100%가

예약되어 객체가 덮어쓰기로부터 완벽하게 보호된다는 것을 나타냅니다. 부분 예약률이 100% 미만이면 해당 볼륨의 모든 공간 예약 파일에 대한 예약 공간이 부분 예약률로 줄어듭니다.

- 스냅샷 일일 성장률

선택한 볼륨의 스냅샷 복사본에서 24시간마다 발생하는 변경 사항(백분율 또는 KB, MB, GB 등)을 표시합니다.

- 스냅샷 일수 ~ 전체

볼륨의 스냅샷 복사본에 예약된 공간이 지정된 임계값에 도달하기까지 남은 예상 일수를 표시합니다.

볼륨의 스냅샷 복사본 성장률이 0 또는 음수이거나 성장률을 계산하기에 충분한 데이터가 없는 경우, 스냅샷 완료까지의 일수 필드에는 '해당 없음' 값이 표시됩니다.

- 스냅샷 자동 삭제

집계된 공간 부족으로 인해 볼륨에 대한 쓰기가 실패할 경우 스냅샷 복사본을 자동으로 삭제하여 공간을 확보할지 여부를 지정합니다.

- 스냅샷 복사본

볼륨의 스냅샷 복사본에 대한 정보를 표시합니다.

볼륨의 스냅샷 복사본 수는 링크로 표시됩니다. 링크를 클릭하면 볼륨의 스냅샷 복사본 대화 상자가 열리고 스냅샷 복사본의 세부 정보가 표시됩니다.

스냅샷 복사 수는 약 1시간마다 업데이트됩니다. 그러나 스냅샷 복사 목록은 아이콘을 클릭하는 시점에 업데이트됩니다. 이로 인해 토폴로지에 표시되는 스냅샷 복사본 수와 아이콘을 클릭했을 때 나열되는 스냅샷 복사본 수 사이에 차이가 생길 수 있습니다.

- 볼륨 이동

볼륨에서 수행된 현재 또는 마지막 볼륨 이동 작업의 상태와 진행 중인 볼륨 이동 작업의 현재 단계, 소스 집계, 대상 집계, 시작 시간, 종료 시간, 예상 종료 시간과 같은 기타 세부 정보를 표시합니다.

또한 선택한 볼륨에서 수행된 볼륨 이동 작업의 수도 표시됩니다. 볼륨 이동 내역 링크를 클릭하면 볼륨 이동 작업에 대한 자세한 정보를 볼 수 있습니다.

구성 탭

구성 탭에는 선택한 볼륨에 대한 세부 정보(예: 볼륨의 내보내기 정책, RAID 유형, 용량 및 스토리지 효율성 관련 기능)가 표시됩니다.

- 개요

- 성명

볼륨의 전체 이름을 표시합니다.

- 골재

볼륨이 있는 집계의 이름이나 FlexGroup 볼륨이 있는 집계의 수를 표시합니다.

- 티어링 정책

볼륨이 FabricPool 지원 집계에 배포된 경우 볼륨에 설정된 계층화 정책이 표시됩니다. 정책은 없음, 스냅샷만, 백업, 자동 또는 모두일 수 있습니다.

- 스토리지 VM

볼륨이 포함된 SVM의 이름을 표시합니다.

- 교차로 경로

경로의 상태를 표시합니다. 경로의 상태는 활성 또는 비활성일 수 있습니다. 볼륨이 마운트된 SVM의 경로도 표시됩니다. 기록 링크를 클릭하면 교차로 경로의 가장 최근 5개 변경 사항을 볼 수 있습니다.

- 수출 정책

볼륨에 대해 생성된 내보내기 정책의 이름을 표시합니다. 링크를 클릭하면 SVM에 속한 볼륨에서 활성화된 내보내기 정책, 인증 프로토콜 및 액세스에 대한 세부 정보를 볼 수 있습니다.

- 스타일

볼륨 스타일을 표시합니다. 볼륨 스타일은 FlexVol 또는 FlexGroup 될 수 있습니다.

- 유형

선택한 볼륨의 유형을 표시합니다. 볼륨 유형은 읽기-쓰기, 부하 공유, 데이터 보호, 데이터 캐시 또는 임시가 될 수 있습니다.

- RAID 유형

선택한 볼륨의 RAID 유형을 표시합니다. RAID 유형은 RAID0, RAID4, RAID-DP 또는 RAID-TEC 가 될 수 있습니다.



FlexGroup 볼륨에는 여러 RAID 유형이 표시될 수 있습니다. FlexGroup의 구성 볼륨은 서로 다른 유형의 집합체에 있을 수 있기 때문입니다.

- SnapLock 타입

볼륨을 포함하는 집계의 SnapLock 유형을 표시합니다.

- SnapLock 만료

SnapLock 볼륨의 만료 날짜를 표시합니다.

- 용량

- 씬 프로비저닝

볼륨에 대해 씬 프로비저닝이 구성되어 있는지 여부를 표시합니다.

- 자동 성장

집계 내에서 유연한 볼륨이 자동으로 증가하는지 여부를 표시합니다.

- 스냅샷 자동 삭제

집계된 공간 부족으로 인해 볼륨에 대한 쓰기가 실패할 경우 스냅샷 복사본을 자동으로 삭제하여 공간을 확보할지 여부를 지정합니다.

- 할당량

볼륨에 대한 할당량을 활성화할지 여부를 지정합니다.

- 능력

- 압축

압축이 활성화되어 있는지 비활성화되어 있는지를 지정합니다.

- 중복제거

중복 제거가 활성화되어 있는지 비활성화되어 있는지를 지정합니다.

- 중복 제거 모드

볼륨에서 활성화된 중복 제거 작업이 수동, 예약 또는 정책 기반 작업인지 여부를 지정합니다. 모드가 예약으로 설정된 경우 작업 일정이 표시되고, 모드가 정책으로 설정된 경우 정책 이름이 표시됩니다.

- 중복 제거 유형

볼륨에서 실행되는 중복 제거 작업의 유형을 지정합니다. 볼륨이 SnapVault 관계에 있는 경우 표시되는 유형은 SnapVault 입니다. 다른 볼륨의 경우 유형은 일반으로 표시됩니다.

- 저장 효율성 정책

Unified Manager를 통해 이 볼륨에 할당된 스토리지 효율성 정책의 이름을 지정합니다. 이 정책은 압축 및 중복 제거 설정을 제어할 수 있습니다.

- 보호

- 스냅샷 복사본

자동 스냅샷 복사를 활성화할지 비활성화할지 지정합니다.

보호 탭

보호 탭에는 지연 정보, 관계 유형, 관계 토폴로지 등 선택한 볼륨에 대한 보호 세부 정보가 표시됩니다.

- 요약

선택한 볼륨에 대한 보호 관계(SnapMirror, SnapVault 또는 Storage VM DR) 속성을 표시합니다. 다른 관계 유형의 경우 관계 유형 속성만 표시됩니다. 기본 볼륨을 선택하면 관리형 및 로컬 스냅샷 복사 정책만 표시됩니다. SnapMirror 및 SnapVault 관계에 대해 표시되는 속성은 다음과 같습니다.

- 소스 볼륨

선택한 볼륨이 대상인 경우 선택한 볼륨의 소스 이름을 표시합니다.

- 지연 상태

보호 관계에 대한 업데이트 또는 전송 지연 상태를 표시합니다. 상태는 오류, 경고 또는 심각일 수 있습니다.

지연 상태는 동기 관계에는 적용되지 않습니다.

- 지연 시간

미러의 데이터가 소스보다 뒤처지는 시간을 표시합니다.

- 마지막으로 성공한 업데이트

가장 최근에 성공적으로 수행된 보호 업데이트의 날짜와 시간을 표시합니다.

마지막으로 성공한 업데이트는 동기 관계에는 적용되지 않습니다.

- 보관 서비스 회원

볼륨이 스토리지 서비스에 속하고 관리되는지 여부를 예 또는 아니요로 표시합니다.

- 버전 유연한 복제

예, 백업 옵션이 있는 예, 없음 중 하나를 표시합니다. '예'는 소스 볼륨과 대상 볼륨이 서로 다른 버전의 ONTAP 소프트웨어를 실행하고 있어도 SnapMirror 복제가 가능하다는 것을 나타냅니다. '예' 백업 옵션은 대상에 여러 버전의 백업 사본을 보관할 수 있는 SnapMirror 보호 기능이 구현되어 있음을 나타냅니다. 없음은 버전 유연 복제가 활성화되어 있지 않음을 나타냅니다.

- 관계 역량

보호 관계에 사용 가능한 ONTAP 기능을 나타냅니다.

- 보호 서비스

관계가 보호 파트너 애플리케이션에 의해 관리되는 경우 보호 서비스의 이름을 표시합니다.

- 관계 유형

비동기 미러, 비동기 볼트, 비동기 미러 볼트, StrictSync 및 Sync를 포함한 모든 관계 유형을 표시합니다.

- 관계 상태

SnapMirror 또는 SnapVault 관계의 상태를 표시합니다. 상태는 초기화되지 않음, 스냅 미러링됨 또는 중단됨일 수 있습니다. 소스 볼륨을 선택하면 관계 상태가 적용되지 않고 표시되지 않습니다.

- 전송 상태

보호 관계에 대한 전송 상태를 표시합니다. 전송 상태는 다음 중 하나일 수 있습니다.

- 중절

SnapMirror 전송은 활성화되어 있지만, 체크포인트 제거를 포함할 수 있는 전송 중단 작업이 진행 중입니다.

- 확인 중

대상 볼륨에 대한 진단 검사가 진행 중이며 전송이 진행 중이 아닙니다.

- 마무리 중

SnapMirror 전송이 활성화되었습니다. 해당 볼륨은 현재 증분형 SnapVault 전송을 위한 전송 후 단계에 있습니다.

- 게으른

전송이 활성화되어 있지만 전송이 진행 중이 아닙니다.

- 동기화됨

동기 관계에 있는 두 볼륨의 데이터는 동기화됩니다.

- 동기화되지 않음

대상 볼륨의 데이터가 소스 볼륨과 동기화되지 않았습니다.

- 준비 중

SnapMirror 전송이 활성화되었습니다. 해당 볼륨은 현재 SnapVault 증분 전송을 위한 사전 전송 단계에 있습니다.

- 대기 중

SnapMirror 전송이 활성화되었습니다. 전송이 진행 중이 아닙니다.

- 정지됨

SnapMirror 전송이 비활성화되었습니다. 전송이 진행되지 않습니다.

- 정지 중

SnapMirror 전송이 진행 중입니다. 추가 전송이 비활성화되었습니다.

- 전송 중

SnapMirror 전송이 활성화되어 있으며 전송이 진행 중입니다.

- 전환 중

소스 볼륨에서 대상 볼륨으로의 비동기 데이터 전송이 완료되었으며 동기 작업으로의 전환이 시작되었습니다.

- 대기 중

SnapMirror 전송이 시작되었지만, 일부 관련 작업이 대기열에 추가되기를 기다리고 있습니다.

- 최대 전송 속도

관계에 대한 최대 전송 속도를 표시합니다. 최대 전송 속도는 초당 킬로바이트(Kbps), 초당 메가바이트(Mbps), 초당 기가바이트(Gbps), 초당 테라바이트(Tbps) 단위의 숫자 값이 될 수 있습니다. 제한 없음이 표시되면 관계 간 기준 전송은 무제한입니다.

- SnapMirror 정책

볼륨에 대한 보호 정책을 표시합니다. DPDefault는 기본 비동기 미러 보호 정책을 나타내고, XDPDefault는 기본 비동기 볼트 정책을 나타내며, DPSyncDefault는 기본 비동기 미러 볼트 정책을 나타냅니다. StrictSync는 기본 동기식 Strict 보호 정책을 나타내고, Sync는 기본 동기식 정책을 나타냅니다. 정책 이름을 클릭하면 다음 정보를 포함하여 해당 정책과 관련된 세부 정보를 볼 수 있습니다.

- 전송 우선순위
- 접근 시간 설정 무시
- 시도 제한
- 댓글
- SnapMirror 라벨
- 보존 설정
- 실제 스냅샷 사본
- 스냅샷 사본 보존
- 보존 경고 임계값
- 보존 설정이 없는 스냅샷 복사본 소스가 데이터 보호(DP) 볼륨인 계단식 SnapVault 관계에서는 “sm_created” 규칙만 적용됩니다.

- 업데이트 일정

관계에 할당된 SnapMirror 일정을 표시합니다. 정보 아이콘 위에 커서를 놓으면 일정 세부 정보가 표시됩니다.

- 로컬 스냅샷 정책

볼륨에 대한 스냅샷 복사 정책을 표시합니다. 정책은 기본값, 없음 또는 사용자 지정 정책에 지정된 이름입니다.

- 보호됨

선택한 볼륨에 사용된 보호 유형을 표시합니다. 예를 들어, 볼륨이 Consistency Group과 SnapMirror 볼륨 관계로 보호되는 경우 이 필드에는 SnapMirror와 Consistency Group이 모두 표시됩니다. 이 필드는 또한 통합된 관계 상태를 볼 수 있는 관계 페이지로 리디렉션하는 링크를 제공합니다. 해당 링크는 구성 관계에만 적용됩니다.

- 일관성 그룹

SnapMirror 활성 동기화 관계로 보호되는 볼륨의 경우 이 열에는 볼륨의 일관성 그룹이 표시됩니다.

- 조회수

선택한 볼륨의 보호 토폴로지를 표시합니다. 토폴로지에는 선택된 볼륨과 관련된 모든 볼륨의 그래픽 표현이 포함됩니다. 선택된 볼륨은 짙은 회색 테두리로 표시되고, 토폴로지에서 볼륨 사이의 선은 보호 관계 유형을 나타냅니다. 토폴로지에서 관계의 방향은 왼쪽에서 오른쪽으로 표시되며, 각 관계의 소스는 왼쪽에, 대상은 오른쪽에 표시됩니다.

두 개의 굵은 선은 비동기 미러 관계를 지정하고, 한 개의 굵은 선은 비동기 볼트 관계를 지정하고, 두 개의 단일 선은 비동기 미러 볼트 관계를 지정하고, 굵은 선과 굵지 않은 선은 동기 관계를 지정합니다. 아래 표는 동기 관계가 StrictSync인지 Sync인지를 나타냅니다.

볼륨을 마우스 오른쪽 버튼으로 클릭하면 볼륨을 보호할지 아니면 볼륨에 데이터를 복원할지 선택할 수 있는 메뉴가 표시됩니다. 관계를 마우스 오른쪽 버튼으로 클릭하면 관계를 편집, 중단, 정지, 해제, 제거 또는 재개할 수 있는 메뉴가 표시됩니다.

다음의 경우에는 메뉴가 표시되지 않습니다.

- RBAC 설정에서 이 작업이 허용되지 않는 경우(예: 운영자 권한만 있는 경우)
- 볼륨이 동기 보호 관계에 있는 경우
- 볼륨 ID를 알 수 없는 경우, 예를 들어 클러스터 간 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우 토폴로지에서 다른 볼륨을 클릭하면 해당 볼륨에 대한 정보가 선택되어 표시됩니다. 물음표(?) 볼륨의 왼쪽 상단에 있는)은 볼륨이 누락되었거나 아직 발견되지 않았음을 나타냅니다. 또한 용량 정보가 누락되었을 수도 있습니다. 물음표 위에 커서를 놓으면 수정 조치에 대한 제안을 포함한 추가 정보가 표시됩니다.

토폴로지는 여러 가지 일반적인 토폴로지 템플릿 중 하나를 따르는 경우 볼륨 용량, 지연, 스냅샷 복사본 및 마지막으로 성공한 데이터 전송에 대한 정보를 표시합니다. 토폴로지가 해당 템플릿 중 하나에 맞지 않으면 볼륨 지연 및 마지막으로 성공한 데이터 전송에 대한 정보가 토폴로지 아래의 관계 테이블에 표시됩니다. 이 경우, 표에서 강조 표시된 행은 선택된 볼륨을 나타내고, 토폴로지 보기에서 파란색 점이 있는 굵은 선은 선택된 볼륨과 소스 볼륨 간의 관계를 나타냅니다.

토폴로지 뷰에는 다음 정보가 포함됩니다.

- 용량

볼륨에서 사용된 총 용량을 표시합니다. 토폴로지의 볼륨 위에 커서를 놓으면 현재 임계값 설정 대화 상자에 해당 볼륨의 현재 경고 및 위험 임계값 설정이 표시됩니다. 현재 임계값 설정 대화 상자에서 임계값 편집 링크를 클릭하여 임계값 설정을 편집할 수도 있습니다. 용량 확인란을 선택 취소하면 토폴로지의 모든 볼륨에 대한 모든 용량 정보가 숨겨집니다.

- 지연

수신 보호 관계의 지연 기간과 지연 상태를 표시합니다. 지연 확인란을 선택 취소하면 토폴로지의 모든 볼륨에 대한 지연 정보가 모두 숨겨집니다. 지연 확인란이 흐리게 표시되면 선택한 볼륨의 지연 정보가 토폴로지 아래의 관계 표에 표시되고, 모든 관련 볼륨의 지연 정보도 함께 표시됩니다.

- 스냅샷

볼륨에 사용 가능한 스냅샷 복사본 수를 표시합니다. 스냅샷 확인란을 선택 취소하면 토폴로지의 모든 볼륨에 대한 모든 스냅샷 복사 정보가 숨겨집니다. 스냅샷 복사 아이콘을 클릭합니다() 볼륨의 스냅샷 복사 목록을 표시합니다. 아이콘 옆에 표시되는 스냅샷 복사 수는 약 1시간마다 업데이트됩니다. 그러나 스냅샷 복사 목록은 아이콘을 클릭하는 시점에 업데이트됩니다. 이로 인해 토폴로지에 표시되는 스냅샷 복사본 수와 아이콘을 클릭했을 때 나열되는 스냅샷 복사본 수 사이에 차이가 생길 수 있습니다.

- 마지막 성공적인 전송

마지막으로 성공적으로 전송된 데이터 양, 기간, 시간, 날짜를 표시합니다. 마지막으로 성공한 전송 확인란이 흐리게 표시되면 선택한 볼륨에 대한 마지막 성공한 전송 정보가 토폴로지 아래의 관계 표에 표시되고, 모든 관련 볼륨에 대한 마지막 성공한 전송 정보도 표시됩니다.

◦ 역사

선택한 볼륨에 대한 수신 SnapMirror 및 SnapVault 보호 관계의 기록을 그래프로 표시합니다. 사용 가능한 세 가지 기록 그래프는 수신 관계 지연 기간, 수신 관계 전송 기간, 수신 관계 전송 크기입니다. 대상 볼륨을 선택할 때만 기록 정보가 표시됩니다. 기본 볼륨을 선택하면 그래프가 비어 있고, 데이터를 찾을 수 없습니다라는 메시지가 표시됩니다. 볼륨이 Consistency Group 및 SnapMirror 동기 관계로 보호되는 경우 관계 전송 기간 및 관계 전송 크기에 대한 정보는 표시되지 않습니다.

기록 창 상단의 드롭다운 목록에서 그래프 유형을 선택할 수 있습니다. 1주일, 1개월, 1년 중 하나를 선택하여 특정 기간에 대한 세부 정보를 볼 수도 있습니다. 기록 그래프는 추세를 파악하는 데 도움이 됩니다. 예를 들어, 하루 중 또는 주 중 같은 시간에 대량의 데이터가 전송되거나 지연 경고 또는 지연 오류 임계값이 지속적으로 초과되는 경우 적절한 조치를 취할 수 있습니다. 또한, 내보내기 버튼을 클릭하면 현재 보고 있는 차트에 대한 CSV 형식의 보고서를 만들 수 있습니다.

보호 내역 그래프에는 다음 정보가 표시됩니다.

• 관계 지연 기간

선택한 기간에 따라 세로(y) 축에 초, 분 또는 시간을 표시하고 가로(x) 축에 일, 월 또는 년을 표시합니다. y축의 위쪽 값은 x축에 표시된 기간 동안 도달한 최대 지연 기간을 나타냅니다. 그래프의 수평 주황색 선은 지연 오류 임계값을 나타내고, 수평 노란색 선은 지연 경고 임계값을 나타냅니다. 이 선 위에 커서를 놓으면 임계값 설정이 표시됩니다. 수평의 파란색 선은 지연 기간을 나타냅니다. 관심 있는 영역 위에 커서를 놓으면 그래프의 특정 지점에 대한 세부 정보를 볼 수 있습니다.

• 관계 이전 기간

선택한 기간에 따라 세로(y) 축에 초, 분 또는 시간을 표시하고 가로(x) 축에 일, 월 또는 년을 표시합니다. y축의 위쪽 값은 x축에 표시된 기간 동안 도달한 최대 전송 기간을 나타냅니다. 관심 있는 영역 위에 커서를 놓으면 그래프에서 특정 지점의 세부 정보를 볼 수 있습니다.



이 차트는 동기식 보호 관계에 있는 볼륨에는 사용할 수 없습니다.

• 관계 이전 크기

전송 크기에 따라 수직(y)축에 바이트, 킬로바이트, 메가바이트 등이 표시되고, 선택한 기간에 따라 수평(x)축에 일, 월 또는 년이 표시됩니다. y축의 위쪽 값은 x축에 표시된 기간 동안 도달한 최대 전송 크기를 나타냅니다. 관심 있는 영역 위에 커서를 놓으면 그래프의 특정 지점에 대한 세부 정보를 볼 수 있습니다.



이 차트는 동기식 보호 관계에 있는 볼륨에는 사용할 수 없습니다.

역사 지역

기록 영역에는 선택한 볼륨의 용량과 공간 예약에 대한 정보를 제공하는 그래프가 표시됩니다. 또한, 내보내기 버튼을 클릭하면 현재 보고 있는 차트에 대한 CSV 형식의 보고서를 만들 수 있습니다.

데이터나 볼륨 상태가 일정 기간 동안 변경되지 않으면 그래프가 비어 있을 수 있으며 '데이터를 찾을 수 없습니다'라는 메시지가 표시될 수 있습니다.

기록 창 상단의 드롭다운 목록에서 그래프 유형을 선택할 수 있습니다. 1주일, 1개월, 1년 중 하나를 선택하여 특정 기간에 대한 세부 정보를 볼 수도 있습니다. 기록 그래프는 추세를 파악하는 데 도움이 됩니다. 예를 들어, 볼륨 사용량이 지속적으로 '거의 가득 참' 임계값을 초과하는 경우 적절한 조치를 취할 수 있습니다.

기록 그래프는 다음 정보를 표시합니다.

- 사용된 볼륨 용량

수직(y)축에 바이트, 킬로바이트, 메가바이트 등의 선형 그래프로 볼륨에서 사용된 용량과 사용 내역을 기반으로 볼륨 용량이 어떻게 사용되는지 추세를 표시합니다. 기간은 수평(x)축에 표시됩니다. 일주일, 한 달, 또는 일년 중 원하는 기간을 선택할 수 있습니다. 그래프의 특정 지점에 대한 세부 정보를 보려면 커서를 특정 영역 위에 올려놓으세요. 해당 범례를 클릭하면 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어, 볼륨 사용 용량 범례를 클릭하면 볼륨 사용 용량 그래프 선이 숨겨집니다.

- 사용된 볼륨 용량 대 총 용량

수직(y)축에는 사용 내역을 기반으로 볼륨 용량 사용 추세를 표시하고, 사용된 용량, 총 용량, 중복 제거 및 압축을 통한 공간 절약 세부 정보를 바이트, 킬로바이트, 메가바이트 등의 선형 그래프로 표시합니다. 기간은 수평(x)축에 표시됩니다. 일주일, 한 달, 또는 일년 중 원하는 기간을 선택할 수 있습니다. 그래프의 특정 지점에 대한 세부 정보를 보려면 커서를 특정 영역 위에 올려놓으세요. 해당 범례를 클릭하면 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어, 사용된 추세 용량 범례를 클릭하면 사용된 추세 용량 그래프 선이 숨겨집니다.

- 사용된 볼륨 용량(%)

수직(y)축에 볼륨의 사용된 용량과 사용 내역을 기반으로 볼륨 용량이 어떻게 사용되는지 추세를 선 그래프로 백분율로 표시합니다. 기간은 수평(x)축에 표시됩니다. 일주일, 한 달, 또는 일년 중 원하는 기간을 선택할 수 있습니다. 그래프의 특정 지점에 대한 세부 정보를 보려면 커서를 특정 영역 위에 올려놓으세요. 해당 범례를 클릭하면 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어, 볼륨 사용 용량 범례를 클릭하면 볼륨 사용 용량 그래프 선이 숨겨집니다.

- 스냅샷 사용 용량(%)

수직(y) 축에 스냅샷 예약 및 스냅샷 경고 임계값을 선 그래프로 표시하고, 스냅샷 복사본에서 사용하는 용량을 영역 그래프로 백분율로 표시합니다. 스냅샷 오버플로는 다양한 색상으로 표현됩니다. 기간은 수평(x)축에 표시됩니다. 일주일, 한 달, 또는 일년 중 원하는 기간을 선택할 수 있습니다. 그래프의 특정 지점에 대한 세부 정보를 보려면 커서를 특정 영역 위에 올려놓으세요. 해당 범례를 클릭하면 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어, 스냅샷 예비 범례를 클릭하면 스냅샷 예비 그래프 선이 숨겨집니다.

이벤트 목록

이벤트 목록에는 새 이벤트와 확인된 이벤트에 대한 세부 정보가 표시됩니다.

- 심각성

이벤트의 심각도를 표시합니다.

- 이벤트

이벤트 이름을 표시합니다.

- 트리거 시간

이벤트가 생성된 이후 경과된 시간을 표시합니다. 경과 시간이 일주일을 초과하면 이벤트가 생성된 타임스탬프가 표시됩니다.

관련 주식 창

관련 주식 창을 사용하면 선택한 볼륨과 관련된 주식 세부 정보를 볼 수 있습니다. 세부 정보에는 볼륨에 적용되는 주식 이름과 주식 값이 포함됩니다. 관련 주식 창에서 수동 주석을 제거할 수도 있습니다.

관련 장치 창

관련 장치 창을 사용하면 볼륨과 관련된 SVM, 집계, Q트리, LUN 및 스냅샷 복사본을 보고 탐색할 수 있습니다.

- 저장 가상 머신

선택한 볼륨이 포함된 SVM의 용량과 상태를 표시합니다.

- 골재

선택한 볼륨이 포함된 집계의 용량과 상태를 표시합니다. FlexGroup 볼륨의 경우 FlexGroup 구성하는 집계의 수가 나열됩니다.

- 총 볼륨

선택한 볼륨의 부모 집계에 속하는 모든 볼륨의 수와 용량을 표시합니다. 볼륨의 상태도 가장 높은 심각도 수준을 기준으로 표시됩니다. 예를 들어, 집계에 10개의 볼륨이 포함되어 있고 그 중 5개가 경고 상태를 표시하고 나머지 5개가 중요 상태를 표시하는 경우 표시되는 상태는 중요입니다. 이 구성 요소는 FlexGroup 볼륨에는 나타나지 않습니다.

- 큐트리스

선택한 볼륨에 포함된 qtree의 수와 선택한 볼륨에 포함된 할당량이 있는 qtree의 용량을 표시합니다. 할당량이 있는 qtree의 용량은 볼륨 데이터 용량을 기준으로 표시됩니다. 가장 높은 심각도 수준을 기준으로 qtree의 상태도 표시됩니다. 예를 들어, 볼륨에 10개의 Q트리가 있고 그 중 5개가 경고 상태이고 나머지 5개가 위험 상태인 경우 표시되는 상태는 위험입니다.

- NFS 주식

볼륨과 연관된 NFS 공유의 수와 상태를 표시합니다.

- SMB 주식

SMB/CIFS 공유의 수와 상태를 표시합니다.

- LUN

선택한 볼륨에 있는 모든 LUN의 수와 전체 크기를 표시합니다. LUN의 상태도 가장 높은 심각도 수준을 기준으로 표시됩니다.

- 사용자 및 그룹 할당량

볼륨과 해당 Qtree에 연결된 사용자 및 사용자 그룹 할당량의 수와 상태를 표시합니다.

- * FlexClone 볼륨*

선택한 볼륨의 모든 복제된 볼륨의 수와 용량을 표시합니다. 선택한 볼륨에 복제된 볼륨이 포함되어 있는 경우에만 숫자와 용량이 표시됩니다.

- 부모 권

선택한 FlexClone 볼륨의 부모 볼륨 이름과 용량을 표시합니다. 선택한 볼륨이 FlexClone 볼륨인 경우에만 부모 볼륨이 표시됩니다.

관련 그룹 창

관련 그룹 창에서는 선택한 볼륨과 관련된 그룹 목록을 볼 수 있습니다.

관련 알림 창

관련 알림 창을 사용하면 선택한 볼륨에 대해 생성된 알림 목록을 볼 수 있습니다. 알림 추가 링크를 클릭하여 알림을 추가하거나 알림 이름을 클릭하여 기존 알림을 편집할 수도 있습니다.

스토리지 VM/상태 세부 정보 페이지

스토리지 VM/상태 세부 정보 페이지를 사용하면 상태, 용량, 구성, 데이터 정책, 논리 인터페이스(LIF), LUN, qtree, 사용자, 사용자 그룹 할당량, 보호 세부 정보 등 선택한 스토리지 VM에 대한 자세한 정보를 볼 수 있습니다. 스토리지 VM에 대한 관련 개체 및 관련 알림에 대한 정보도 볼 수 있습니다.



데이터 저장 VM만 모니터링할 수 있습니다.

명령 버튼

명령 버튼을 사용하면 선택한 스토리지 VM에 대해 다음 작업을 수행할 수 있습니다.

- 성능 보기로 전환

스토리지 VM/성능 세부 정보 페이지로 이동할 수 있습니다.

- 행위

- 알림 추가

선택한 스토리지 VM에 알림을 추가할 수 있습니다.

- 주석 달기

선택한 스토리지 VM에 주석을 달 수 있습니다.

- 스토리지 VM 보기

상태: 모든 저장소 VM 보기로 이동할 수 있습니다.

건강 탭

상태 탭에는 볼륨, 집계, NAS LIF, SAN LIF, LUN, 프로토콜, 서비스, NFS 공유, CIFS 공유 등 다양한 개체의 데이터 가용성, 데이터 용량 및 보호 문제에 대한 자세한 정보가 표시됩니다.

객체의 그래프를 클릭하면 필터링된 객체 목록을 볼 수 있습니다. 예를 들어, 경고를 표시하는 볼륨 용량 그래프를

클릭하면 심각도가 경고인 용량 문제가 있는 볼륨 목록을 볼 수 있습니다.

- 가용성 문제

가용성 문제가 있는 객체와 가용성 관련 문제가 없는 객체를 포함하여 총 객체 수를 그래프로 표시합니다. 그래프의 색상은 문제의 심각도 수준을 나타냅니다. 그래프 아래의 정보는 스토리지 VM의 데이터 가용성에 영향을 미칠 수 있거나 이미 영향을 미친 가용성 문제에 대한 세부 정보를 제공합니다. 예를 들어, 다운된 NAS LIF와 SAN LIF, 오프라인인 볼륨에 대한 정보가 표시됩니다.

현재 실행 중인 관련 프로토콜 및 서비스에 대한 정보와 NFS 및 CIFS 공유의 수와 상태도 볼 수 있습니다.

- 수용량 문제

용량 문제가 있는 객체와 용량 관련 문제가 없는 객체를 포함하여 총 객체 수를 그래프로 표시합니다. 그래프의 색상은 문제의 심각도 수준을 나타냅니다. 그래프 아래의 정보는 스토리지 VM의 데이터 용량에 영향을 미칠 수 있거나 이미 영향을 미친 용량 문제에 대한 세부 정보를 제공합니다. 예를 들어, 설정된 임계값을 위반할 가능성이 있는 집계에 대한 정보가 표시됩니다.

- 보호 문제

보호 문제가 있는 관계와 보호 관련 문제가 없는 관계를 포함하여 총 관계 수를 필드 대화 상자로 표시하여 스토리지 VM 보호 관련 상태에 대한 빠른 개요를 제공합니다. 선택한 스토리지 VM에 대한 스토리지 VM DR 관계의 상태도 볼 수 있습니다. 스토리지 VM DR 관계 이벤트가 여기에 표시되며, 이벤트를 클릭하면 이벤트 세부 정보 페이지로 이동합니다. 보호되지 않은 볼륨이 있는 경우 링크를 클릭하면 상태: 모든 볼륨 보기로 이동하여 스토리지 VM에 있는 보호되지 않은 볼륨의 필터링된 목록을 볼 수 있습니다. 그래프의 색상은 문제의 심각도 수준을 나타냅니다. 그래프를 클릭하면 관계: 모든 관계 보기로 이동하여 보호 관계 세부 정보의 필터링된 목록을 볼 수 있습니다. 그래프 아래의 정보는 스토리지 VM의 데이터 보호에 영향을 미칠 수 있거나 이미 영향을 미쳤던 보호 문제에 대한 세부 정보를 제공합니다. 예를 들어, 스냅샷 복사 예약이 거의 가득 찬 볼륨이나 SnapMirror 관계 지연 문제에 대한 정보가 표시됩니다.

용량 탭

용량 탭에는 선택한 SVM의 데이터 용량에 대한 자세한 정보가 표시됩니다.

FlexVol volume 또는 FlexGroup 볼륨이 있는 스토리지 VM에 대해 다음 정보가 표시됩니다.

- 용량

용량 영역에는 모든 볼륨에서 할당된 사용된 용량과 사용 가능한 용량에 대한 세부 정보가 표시됩니다.

- 총 용량

스토리지 VM의 총 용량을 표시합니다.

- 사용된

스토리지 VM에 속한 볼륨의 데이터가 사용하는 공간을 표시합니다.

- 보장 가능

저장소 VM의 볼륨에 사용 가능한 데이터에 대해 보장된 사용 가능 공간을 표시합니다.

- 보장되지 않음

스토리지 VM에서 씬 프로비저닝된 볼륨에 할당된 데이터에 남아 있는 사용 가능한 공간을 표시합니다.

- 용량 문제가 있는 볼륨

용량 문제가 있는 볼륨 목록에는 용량 문제가 있는 볼륨에 대한 세부 정보가 표 형식으로 표시됩니다.

- 상태

볼륨에 표시된 심각도의 용량 관련 문제가 있음을 나타냅니다.

볼륨에 대해 생성된 용량 관련 이벤트에 대한 자세한 정보를 보려면 포인터를 상태 위로 가져가세요.

볼륨 상태가 단일 이벤트에 의해 결정되는 경우 이벤트 이름, 이벤트가 트리거된 시간 및 날짜, 이벤트가 할당된 관리자 이름, 이벤트 원인 등의 정보를 볼 수 있습니다. 자세한 내용 보기 버튼을 사용하면 이벤트에 대한 자세한 정보를 볼 수 있습니다.

볼륨 상태가 동일한 심각도의 여러 이벤트에 의해 결정되는 경우, 상위 3개 이벤트가 이벤트 이름, 이벤트가 트리거된 시간 및 날짜, 이벤트가 할당된 관리자 이름 등의 정보와 함께 표시됩니다. 각 이벤트에 대한 자세한 내용을 보려면 이벤트 이름을 클릭하세요. 모든 이벤트 보기 링크를 클릭하면 생성된 이벤트 목록을 볼 수도 있습니다.



볼륨에는 동일하거나 다른 심각도의 이벤트가 여러 개 있을 수 있습니다. 하지만 가장 높은 심각도만 표시됩니다. 예를 들어, 볼륨에 오류와 경고의 심각도를 가진 두 개의 이벤트가 있는 경우 오류 심각도만 표시됩니다.

- 용량

볼륨의 이름을 표시합니다.

- 사용된 데이터 용량

볼륨 용량 사용에 대한 정보를 그래프로 표시합니다(백분율).

- 만기까지 걸리는 일수

볼륨이 최대 용량에 도달하기까지 남은 예상 일수를 표시합니다.

- 씬 프로비저닝

선택한 볼륨에 대해 공간 보장이 설정되어 있는지 여부를 표시합니다. 유효한 값은 예와 아니오입니다.

- 골재

FlexVol 볼륨의 경우 볼륨을 포함하는 집계의 이름을 표시합니다. FlexGroup 볼륨의 경우 FlexGroup 에서 사용되는 집계 수를 표시합니다.

구성 탭

구성 탭에는 클러스터, 루트 볼륨, 포함된 볼륨 유형(FlexVol 볼륨), 정책, 스토리지 VM에 생성된 보호 등 선택한 스토리지 VM에 대한 구성 세부 정보가 표시됩니다.

- 개요

- 무리

스토리지 VM이 속한 클러스터의 이름을 표시합니다.

- 허용된 볼륨 유형

스토리지 VM에서 생성할 수 있는 볼륨 유형을 표시합니다. 유형은 FlexVol 또는 FlexVol/ FlexGroup 이 될 수 있습니다.

- 루트 볼륨

스토리지 VM의 루트 볼륨 이름을 표시합니다.

- 허용된 프로토콜

스토리지 VM에서 구성할 수 있는 프로토콜 유형을 표시합니다. 또한 프로토콜이 작동 중인지 여부를 나타냅니다(●), 아래에 (●), 또는 구성되지 않았습니다(●).

- 데이터 네트워크 인터페이스

- NAS

스토리지 VM에 연결된 NAS 인터페이스의 수를 표시합니다. 또한 인터페이스가 작동 중인지 여부를 나타냅니다. (●) 또는 아래로 (●).

- SAN

스토리지 VM에 연결된 SAN 인터페이스의 수를 표시합니다. 또한 인터페이스가 작동 중인지 여부를 나타냅니다. (●) 또는 아래로 (●).

- FC-NVMe

스토리지 VM과 연결된 FC-NVMe 인터페이스의 수를 표시합니다. 또한 인터페이스가 작동 중인지 여부를 나타냅니다. (●) 또는 아래로 (●).

- 관리 네트워크 인터페이스

- 유효성

스토리지 VM에 연결된 관리 인터페이스의 수를 표시합니다. 또한 관리 인터페이스가 작동 중인지 여부를 나타냅니다. (●) 또는 아래로 (●).

- 정책

- 스냅샷

스토리지 VM에 생성된 스냅샷 정책의 이름을 표시합니다.

- 수출 정책

단일 정책이 생성된 경우 내보내기 정책의 이름을 표시하고, 여러 정책이 생성된 경우 내보내기 정책의 수를 표시합니다.

- 보호

- 스토리지 VM DR

선택한 스토리지 VM이 보호되는지, 대상인지, 보호되지 않는지와 스토리지 VM이 보호되는 대상의 이름을 표시합니다. 선택한 스토리지 VM이 대상인 경우 소스 스토리지 VM의 세부 정보가 표시됩니다. 팬아웃의 경우 이 필드에는 스토리지 VM이 보호되는 총 대상 스토리지 VM 수가 표시됩니다. 카운트 링크를 클릭하면 소스 스토리지 VM을 기준으로 필터링된 스토리지 VM 관계 그리드로 이동합니다.

- 보호된 볼륨

총 볼륨 중 선택된 스토리지 VM에 있는 보호된 볼륨의 수를 표시합니다. 대상 스토리지 VM을 보고 있는 경우 번호 링크는 선택한 스토리지 VM의 대상 볼륨을 나타냅니다.

- 보호되지 않은 볼륨

선택한 스토리지 VM에 있는 보호되지 않은 볼륨의 수를 표시합니다.

- 서비스

- 유형

스토리지 VM에 구성된 서비스 유형을 표시합니다. 유형은 DNS(도메인 이름 시스템) 또는 NIS(네트워크 정보 서비스)일 수 있습니다.

- 상태

서비스 상태를 표시합니다. 상태는 Up() , 아래에 () , 또는 구성되지 않음() .

- 도메인 이름

DNS 서비스의 경우 DNS 서버의 정규화된 도메인 이름(FQDN)을 표시하고, NIS 서비스의 경우 NIS 서버의 정규화된 도메인 이름(FQDN)을 표시합니다. NIS 서버가 활성화되면 NIS 서버의 활성 FQDN이 표시됩니다. NIS 서버가 비활성화되면 모든 FQDN 목록이 표시됩니다.

- IP 주소

DNS 또는 NIS 서버의 IP 주소를 표시합니다. NIS 서버가 활성화되면 NIS 서버의 활성 IP 주소가 표시됩니다. NIS 서버가 비활성화되면 모든 IP 주소 목록이 표시됩니다.

네트워크 인터페이스 탭

네트워크 인터페이스 탭에는 선택한 스토리지 VM에 생성된 데이터 네트워크 인터페이스(LIF)에 대한 세부 정보가 표시됩니다.

- 네트워크 인터페이스

선택한 스토리지 VM에 생성된 인터페이스의 이름을 표시합니다.

- 운영 상태

인터페이스의 작동 상태를 표시합니다. 작동 상태는 Up() , 아래에 () , 또는 알 수 없음() . 인터페이스의 작동 상태는 물리적 포트의 상태에 따라 결정됩니다.

- 행정 상태

인터페이스의 관리 상태를 표시합니다. 상태는 다음과 같습니다. ), 아래에 (), 또는 알 수 없음(). 인터페이스의 관리 상태는 스토리지 관리자가 구성을 변경하거나 유지 관리를 위해 제어합니다. 행정 상태는 운영 상태와 다를 수 있습니다. 하지만 인터페이스의 관리 상태가 '다운'인 경우 운영 상태도 기본적으로 '다운'입니다.

- **IP 주소 / WWPN**

이더넷 인터페이스의 IP 주소와 FC LIF의 WWPN(World Wide Port Name)을 표시합니다.

- **프로토콜**

CIFS, NFS, iSCSI, FC/FCoE, FC-NVMe, FlexCache 등 인터페이스에 지정된 데이터 프로토콜 목록을 표시합니다.

- **역할**

인터페이스 역할을 표시합니다. 역할은 데이터 또는 관리가 될 수 있습니다.

- **모함**

인터페이스가 원래 연결된 물리적 포트를 표시합니다.

- **현재 항구**

인터페이스가 현재 연결되어 있는 물리적 포트를 표시합니다. 인터페이스가 마이그레이션되면 현재 포트가 홈 포트와 다를 수 있습니다.

- **포트 세트**

인터페이스가 매핑된 포트 세트를 표시합니다.

- **장애 조치 정책**

인터페이스에 대해 구성된 장애 조치 정책을 표시합니다. NFS, CIFS 및 FlexCache 인터페이스의 경우 기본 장애 조치 정책은 다음 사용 가능 항목입니다. FC 및 iSCSI 인터페이스에는 장애 조치 정책이 적용되지 않습니다.

- **라우팅 그룹**

라우팅 그룹의 이름을 표시합니다. 라우팅 그룹 이름을 클릭하면 경로와 대상 게이트웨이에 대한 자세한 정보를 볼 수 있습니다.

ONTAP 8.3 이상에서는 라우팅 그룹이 지원되지 않으므로 이러한 클러스터에 대해 빈 열이 표시됩니다.

- **장애 조치 그룹**

장애 조치 그룹의 이름을 표시합니다.

Qtrees 탭

Qtrees 탭에는 Qtrees와 할당량에 대한 세부 정보가 표시됩니다. 하나 이상의 Qtree에 대한 Qtree 용량의 상태 임계값 설정을 편집하려면 임계값 편집 버튼을 클릭하면 됩니다.

내보내기 버튼을 사용하여 모니터링되는 모든 qtree의 세부 정보가 포함된 심표로 구분된 값(csv) 파일을 만듭니다. CSV 파일로 내보낼 때 현재 스토리지 VM, 현재 클러스터의 모든 스토리지 VM 또는 데이터 센터의 모든 클러스터에

대한 모든 스토리지 VM에 대한 Qtrees 보고서를 만들도록 선택할 수 있습니다. 내보낸 CSV 파일에 몇 가지 추가 qtrees 필드가 나타납니다.

- 상태

qtree의 현재 상태를 표시합니다. 상태는 중요(Critical)일 수 있습니다. (❌), 오류 (🚫), 경고 (⚠️), 또는 일반 (✅).

qtree에 대해 생성된 이벤트에 대한 자세한 정보를 보려면 상태 아이콘 위로 포인터를 이동하세요.

Qtree 상태가 단일 이벤트에 의해 결정되는 경우 이벤트 이름, 이벤트가 트리거된 시간 및 날짜, 이벤트가 할당된 관리자 이름, 이벤트 원인 등의 정보를 볼 수 있습니다. *자세한 내용 보기*를 클릭하면 이벤트에 대한 자세한 정보를 볼 수 있습니다.

Qtree 상태가 동일한 심각도의 여러 이벤트에 의해 결정되는 경우, 상위 3개 이벤트가 이벤트 이름, 이벤트가 트리거된 시간 및 날짜, 이벤트가 할당된 관리자 이름 등의 정보와 함께 표시됩니다. 각 이벤트에 대한 자세한 내용을 보려면 이벤트 이름을 클릭하세요. *모든 이벤트 보기*를 사용하여 생성된 이벤트 목록을 볼 수도 있습니다.



qtree에는 동일하거나 다른 심각도의 이벤트가 여러 개 있을 수 있습니다. 하지만 가장 높은 심각도만 표시됩니다. 예를 들어, qtree에 오류와 경고의 심각도를 가진 두 개의 이벤트가 있는 경우 오류 심각도만 표시됩니다.

- 큐트리

qtree의 이름을 표시합니다.

- 무리

qtree를 포함하는 클러스터의 이름을 표시합니다. 내보낸 CSV 파일에만 나타납니다.

- 저장 가상 머신

qtree를 포함하는 스토리지 가상 머신(SVM) 이름을 표시합니다. 내보낸 CSV 파일에만 나타납니다.

- 용량

qtree가 포함된 볼륨의 이름을 표시합니다.

볼륨 이름 위에 포인터를 놓으면 해당 볼륨에 대한 자세한 정보를 볼 수 있습니다.

- 할당량 설정

qtree에서 할당량이 활성화되었는지 비활성화되었는지를 나타냅니다.

- 할당량 유형

할당량이 사용자, 사용자 그룹 또는 Qtree에 대한 것인지 지정합니다. 내보낸 CSV 파일에만 나타납니다.

- 사용자 또는 그룹

사용자 또는 사용자 그룹의 이름을 표시합니다. 각 사용자와 사용자 그룹에 대해 여러 행이 있습니다. 할당량 유형이 qtree이거나 할당량이 설정되지 않은 경우 열은 비어 있습니다. 내보낸 CSV 파일에만 나타납니다.

- 사용된 디스크 %

사용된 디스크 공간의 백분율을 표시합니다. 디스크 하드 한도가 설정된 경우 이 값은 디스크 하드 한도를 기준으로 합니다. 디스크 하드 제한 없이 할당량을 설정하면 값은 볼륨 데이터 공간을 기준으로 합니다. 할당량이 설정되지 않았거나 Qtree가 속한 볼륨에서 할당량이 해제된 경우 그리드 페이지에 "해당 없음"이 표시되고 CSV 내보내기 데이터의 필드는 비어 있습니다.

- 디스크 하드 제한

qtree에 할당된 최대 디스크 공간을 표시합니다. Unified Manager는 이 한도에 도달하고 더 이상 디스크 쓰기가 허용되지 않을 때 위험 이벤트를 생성합니다. 다음 조건에서는 값이 "무제한"으로 표시됩니다. 디스크 하드 제한 없이 할당량이 설정된 경우, 할당량이 설정되지 않은 경우 또는 qtree가 속한 볼륨에서 할당량이 해제된 경우입니다.

- 디스크 소프트 리미트

경고 이벤트가 생성되기 전에 qtree에 할당된 디스크 공간의 양을 표시합니다. 다음 조건에서는 값이 "무제한"으로 표시됩니다. 디스크 소프트 한도 없이 할당량이 설정된 경우, 할당량이 설정되지 않은 경우 또는 qtree가 속한 볼륨에서 할당량이 꺼져 있는 경우입니다. 기본적으로 이 열은 숨겨져 있습니다.

- 디스크 임계값

디스크 공간에 설정된 임계값을 표시합니다. 다음 조건에서는 값이 "무제한"으로 표시됩니다. 디스크 임계값 제한 없이 할당량이 설정된 경우, 할당량이 설정되지 않은 경우 또는 qtree가 속한 볼륨에서 할당량이 해제된 경우입니다. 기본적으로 이 열은 숨겨져 있습니다.

- 사용된 파일 %

qtree에 사용된 파일의 백분율을 표시합니다. 파일 하드 한도가 설정된 경우, 이 값은 파일 하드 한도를 기준으로 합니다. 파일의 하드 한도 없이 할당량을 설정하면 값이 표시되지 않습니다. 할당량이 설정되지 않았거나 Qtree가 속한 볼륨에서 할당량이 해제된 경우 그리드 페이지에 "해당 없음"이 표시되고 CSV 내보내기 데이터의 필드는 비어 있습니다.

- 파일 하드 리미트

qtree에 허용되는 파일 수에 대한 하드 한도를 표시합니다. 다음 조건에서는 값이 "무제한"으로 표시됩니다. 파일 하드 한도 없이 할당량이 설정된 경우, 할당량이 설정되지 않은 경우 또는 qtree가 속한 볼륨에서 할당량이 해제된 경우입니다.

- 파일 소프트 리미트

qtree에 허용되는 파일 수에 대한 소프트 한도를 표시합니다. 다음 조건에서는 값이 "무제한"으로 표시됩니다. 파일 소프트 한도 없이 할당량이 설정된 경우, 할당량이 설정되지 않은 경우 또는 qtree가 속한 볼륨에서 할당량이 해제된 경우입니다. 기본적으로 이 열은 숨겨져 있습니다.

사용자 및 그룹 할당량 탭

선택한 스토리지 VM에 대한 사용자 및 사용자 그룹 할당량에 대한 세부 정보를 표시합니다. 할당량 상태, 사용자 또는 사용자 그룹 이름, 디스크와 파일에 설정된 소프트 및 하드 제한, 디스크 공간의 양과 사용된 파일 수, 디스크 임계값 등의 정보를 볼 수 있습니다. 사용자 또는 사용자 그룹과 연결된 이메일 주소를 변경할 수도 있습니다.

- 이메일 주소 편집 명령 버튼

선택한 사용자 또는 사용자 그룹의 현재 이메일 주소를 표시하는 이메일 주소 편집 대화 상자를 엽니다. 이메일

주소를 수정할 수 있습니다. 이메일 주소 편집 필드가 비어 있으면 기본 규칙이 선택된 사용자 또는 사용자 그룹의 이메일 주소를 생성하는 데 사용됩니다.

두 명 이상의 사용자가 동일한 할당량을 가지고 있는 경우, 사용자 이름은 쉼표로 구분된 값으로 표시됩니다. 또한, 기본 규칙은 이메일 주소를 생성하는 데 사용되지 않습니다. 따라서 알림을 보내려면 필요한 이메일 주소를 제공해야 합니다.

- 이메일 규칙 구성 명령 버튼

스토리지 VM에 구성된 사용자 또는 사용자 그룹 할당량에 대한 이메일 주소를 생성하는 규칙을 만들거나 수정할 수 있습니다. 할당량 위반이 발생하면 지정된 이메일 주소로 알림이 전송됩니다.

- 상태

할당량의 현재 상태를 표시합니다. 상태는 중요(Critical)일 수 있습니다. , 경고 () , 또는 일반().

할당량에 대해 생성된 이벤트에 대한 자세한 정보를 보려면 상태 아이콘 위에 포인터를 놓으세요.

할당량 상태가 단일 이벤트에 의해 결정되는 경우 이벤트 이름, 이벤트가 트리거된 시간 및 날짜, 이벤트가 할당된 관리자 이름, 이벤트 원인 등의 정보를 볼 수 있습니다. *자세한 내용 보기*를 클릭하면 이벤트에 대한 자세한 정보를 볼 수 있습니다.

할당량 상태가 동일한 심각도의 여러 이벤트에 의해 결정되는 경우, 상위 3개 이벤트가 이벤트 이름, 이벤트가 트리거된 시간 및 날짜, 이벤트가 할당된 관리자 이름 등의 정보와 함께 표시됩니다. 각 이벤트에 대한 자세한 내용을 보려면 이벤트 이름을 클릭하세요. *모든 이벤트 보기*를 사용하여 생성된 이벤트 목록을 볼 수도 있습니다.



할당량에는 심각도가 같거나 다른 여러 이벤트가 포함될 수 있습니다. 하지만 가장 높은 심각도만 표시됩니다. 예를 들어, 할당량에 오류와 경고의 심각도를 가진 두 개의 이벤트가 있는 경우 오류 심각도만 표시됩니다.

- 사용자 또는 그룹

사용자 또는 사용자 그룹의 이름을 표시합니다. 두 명 이상의 사용자가 동일한 할당량을 가지고 있는 경우, 사용자 이름은 쉼표로 구분된 값으로 표시됩니다.

ONTAP SecD 오류로 인해 유효한 사용자 이름을 제공하지 않으면 값이 "알 수 없음"으로 표시됩니다.

- 유형

할당량이 사용자 또는 사용자 그룹을 위한 것인지 지정합니다.

- 볼륨 또는 Qtree

사용자 또는 사용자 그룹 할당량이 지정된 볼륨이나 Qtree의 이름을 표시합니다.

볼륨이나 Qtree 이름 위에 포인터를 놓으면 해당 볼륨이나 Qtree에 대한 자세한 정보를 볼 수 있습니다.

- 사용된 디스크 %

사용된 디스크 공간의 백분율을 표시합니다. 디스크 하드 한도 없이 할당량이 설정된 경우 값은 "해당 없음"으로 표시됩니다.

- 디스크 하드 제한

할당량에 할당된 최대 디스크 공간을 표시합니다. Unified Manager는 이 한도에 도달하고 더 이상 디스크 쓰기가 허용되지 않을 때 중요 이벤트를 생성합니다. 디스크 하드 제한 없이 할당량이 설정된 경우 값은 "무제한"으로 표시됩니다.

- 디스크 소프트 리미트

경고 이벤트가 생성되기 전에 할당량에 할당된 디스크 공간의 양을 표시합니다. 디스크 소프트 한도 없이 할당량이 설정된 경우 값은 "무제한"으로 표시됩니다. 기본적으로 이 열은 숨겨져 있습니다.

- 디스크 임계값

디스크 공간에 설정된 임계값을 표시합니다. 디스크 임계값 제한 없이 할당량이 설정된 경우 값은 "무제한"으로 표시됩니다. 기본적으로 이 열은 숨겨져 있습니다.

- 사용된 파일 %

qtree에 사용된 파일의 백분율을 표시합니다. 파일의 하드 한도 없이 할당량이 설정된 경우 값은 "해당 없음"으로 표시됩니다.

- 파일 하드 리미트

할당량에 허용되는 파일 수에 대한 하드 한도를 표시합니다. 파일의 하드 한도 없이 할당량이 설정된 경우 값은 "무제한"으로 표시됩니다.

- 파일 소프트 리미트

할당량에 허용되는 파일 수에 대한 소프트 한도를 표시합니다. 파일 소프트 한도 없이 할당량이 설정된 경우 값은 "무제한"으로 표시됩니다. 기본적으로 이 열은 숨겨져 있습니다.

- 이메일 주소

할당량 위반이 발생할 경우 알림을 보낼 사용자 또는 사용자 그룹의 이메일 주소를 표시합니다.

NFS 공유 탭

NFS 공유 탭에는 NFS 공유 상태, 볼륨(FlexGroup 볼륨 또는 FlexVol 볼륨)과 관련된 경로, NFS 공유에 대한 클라이언트의 액세스 수준, 내보내는 볼륨에 대해 정의된 내보내기 정책 등 NFS 공유에 대한 정보가 표시됩니다. 다음과 같은 조건에서는 NFS 공유가 표시되지 않습니다. 볼륨이 마운트되지 않았거나 볼륨의 내보내기 정책과 연관된 프로토콜에 NFS 공유가 포함되어 있지 않은 경우입니다.

- 상태

NFS 공유의 현재 상태를 표시합니다. 상태는 오류(🚫) 또는 일반(✅).

- 분기점 경로

볼륨이 마운트된 경로를 표시합니다. 명시적 NFS 내보내기 정책이 qtree에 적용되는 경우, 해당 열에는 qtree에 액세스할 수 있는 볼륨의 경로가 표시됩니다.

- 분기점 경로 활성화

마운트된 볼륨에 액세스하는 경로가 활성 상태인지 비활성 상태인지 표시합니다.

- 볼륨 또는 **Qtree**

NFS 내보내기 정책이 적용되는 볼륨이나 qtree의 이름을 표시합니다. 볼륨의 qtree에 NFS 내보내기 정책이 적용되는 경우 해당 열에는 볼륨과 qtree의 이름이 모두 표시됩니다.

해당 세부 정보 페이지에서 해당 객체에 대한 세부 정보를 보려면 링크를 클릭하세요. 객체가 Q트리인 경우 Q트리와 볼륨에 대한 링크가 모두 표시됩니다.

- 볼륨 상태

내보내는 볼륨의 상태를 표시합니다. 상태는 오프라인, 온라인, 제한 또는 혼합일 수 있습니다.

- 오프라인

볼륨에 대한 읽기 또는 쓰기 액세스가 허용되지 않습니다.

- 온라인

볼륨에 대한 읽기 및 쓰기 액세스가 허용됩니다.

- 제한된

패리티 재구성과 같은 제한된 작업은 허용되지만 데이터 접근은 허용되지 않습니다.

- 혼합

FlexGroup 볼륨의 구성 요소는 모두 동일한 상태에 있지 않습니다.

- 보안 스타일

내보낸 볼륨에 대한 액세스 권한을 표시합니다. 보안 스타일은 UNIX, 통합, NTFS 또는 혼합이 될 수 있습니다.

- UNIX(NFS 클라이언트)

볼륨 내의 파일과 디렉토리에는 UNIX 권한이 있습니다.

- 통합

볼륨 내의 파일과 디렉토리는 통합된 보안 스타일을 갖습니다.

- NTFS(CIFS 클라이언트)

볼륨의 파일과 디렉토리에는 Windows NTFS 권한이 있습니다.

- 혼합

볼륨 내의 파일과 디렉토리는 UNIX 권한 또는 Windows NTFS 권한을 가질 수 있습니다.

- **UNIX** 권한

내보낸 볼륨에 대해 설정된 UNIX 권한 비트를 8진수 문자열 형식으로 표시합니다. 이는 UNIX 스타일의 권한 비트와 유사합니다.

- 수출 정책

내보낸 볼륨에 대한 액세스 권한을 정의하는 규칙을 표시합니다. 링크를 클릭하면 인증 프로토콜 및 액세스 권한 등 내보내기 정책과 관련된 규칙에 대한 세부 정보를 볼 수 있습니다.

SMB 주식 탭

선택한 스토리지 VM의 SMB 공유에 대한 정보를 표시합니다. SMB 공유 상태, 공유 이름, 스토리지 VM과 연결된 경로, 공유의 연결 경로 상태, 포함 개체, 포함 볼륨의 상태, 공유의 보안 데이터, 공유에 대해 정의된 내보내기 정책 등의 정보를 볼 수 있습니다. SMB 공유에 대한 동등한 NFS 경로가 있는지도 확인할 수 있습니다.



폴더의 공유 항목은 SMB 공유 탭에 표시되지 않습니다.

- 사용자 매핑 보기 명령 버튼

사용자 매핑 대화 상자를 시작합니다.

스토리지 VM에 대한 사용자 매핑 세부 정보를 볼 수 있습니다.

- ACL 명령 버튼 표시

공유에 대한 액세스 제어 대화 상자를 시작합니다.

선택한 공유에 대한 사용자 및 권한 세부 정보를 볼 수 있습니다.

- 상태

공유의 현재 상태를 표시합니다. 상태는 정상(✅) 또는 오류(❗).

- 공유 이름

SMB 공유의 이름을 표시합니다.

- 길

공유가 생성된 연결 경로를 표시합니다.

- 분기점 경로 활성화

공유에 액세스하는 경로가 활성 상태인지 비활성 상태인지 표시합니다.

- 포함된 객체

공유가 속한 포함 개체의 이름을 표시합니다. 포함하는 객체는 볼륨이나 qtree가 될 수 있습니다.

링크를 클릭하면 해당 세부 정보 페이지에서 해당 객체에 대한 세부 정보를 볼 수 있습니다. 포함 객체가 qtree인 경우 qtree와 볼륨에 대한 링크가 모두 표시됩니다.

- 볼륨 상태

내보내는 볼륨의 상태를 표시합니다. 상태는 오프라인, 온라인, 제한 또는 혼합일 수 있습니다.

- 오프라인

볼륨에 대한 읽기 또는 쓰기 액세스가 허용되지 않습니다.

- 온라인

볼륨에 대한 읽기 및 쓰기 액세스가 허용됩니다.

- 제한된

패리티 재구성과 같은 제한된 작업은 허용되지만 데이터 접근은 허용되지 않습니다.

- 혼합

FlexGroup 볼륨의 구성 요소는 모두 동일한 상태에 있지 않습니다.

- 보안

내보낸 볼륨에 대한 액세스 권한을 표시합니다. 보안 스타일은 UNIX, 통합, NTFS 또는 혼합이 될 수 있습니다.

- UNIX(NFS 클라이언트)

볼륨 내의 파일과 디렉토리에는 UNIX 권한이 있습니다.

- 통합

볼륨 내의 파일과 디렉토리는 통합된 보안 스타일을 갖습니다.

- NTFS(CIFS 클라이언트)

볼륨의 파일과 디렉토리에는 Windows NTFS 권한이 있습니다.

- 혼합

볼륨 내의 파일과 디렉토리는 UNIX 권한 또는 Windows NTFS 권한을 가질 수 있습니다.

- 수출 정책

공유에 적용되는 내보내기 정책의 이름을 표시합니다. 스토리지 VM에 대한 내보내기 정책이 지정되지 않은 경우 값은 '사용 안 함'으로 표시됩니다.

링크를 클릭하면 액세스 프로토콜 및 권한 등 내보내기 정책과 관련된 규칙에 대한 세부 정보를 볼 수 있습니다. 선택한 스토리지 VM에 대한 내보내기 정책이 비활성화된 경우 링크가 비활성화됩니다.

- NFS 동등물

공유에 대한 NFS 대응 항목이 있는지 여부를 지정합니다.

SAN 탭

선택한 스토리지 VM에 대한 LUN, 이니시에이터 그룹 및 이니시에이터에 대한 세부 정보를 표시합니다. 기본적으로 LUN 보기가 표시됩니다. 개시자 그룹 탭에서 개시자 그룹에 대한 세부 정보를 볼 수 있으며, 개시자 탭에서 개시자에

대한 세부 정보를 볼 수 있습니다.

- **LUN 탭**

선택한 스토리지 VM에 속한 LUN에 대한 세부 정보를 표시합니다. LUN 이름, LUN 상태(온라인 또는 오프라인), LUN이 포함된 파일 시스템 이름(볼륨 또는 qtree), 호스트 운영 체제 유형, 총 데이터 용량 및 LUN의 일련 번호와 같은 정보를 볼 수 있습니다. LUN 성능 열은 LUN/성능 세부 정보 페이지에 대한 링크를 제공합니다.

또한 LUN에서 씬 프로비저닝이 활성화되어 있는지 여부와 LUN이 이니시에이터 그룹에 매핑되어 있는지 여부에 대한 정보를 볼 수 있습니다. 이니시에이터에 매핑된 경우, 선택한 LUN에 매핑된 이니시에이터 그룹과 이니시에이터를 볼 수 있습니다.

- **이니시에이터 그룹 탭**

개시자 그룹에 대한 세부 정보를 표시합니다. 그룹의 이름, 액세스 상태, 그룹의 모든 이니시에이터에서 사용하는 호스트 운영 체제 유형, 지원되는 프로토콜 등의 세부 정보를 볼 수 있습니다. 액세스 상태 열의 링크를 클릭하면 개시자 그룹의 현재 액세스 상태를 볼 수 있습니다.

- 정상

개시자 그룹은 여러 액세스 경로에 연결되어 있습니다.

- 단일 경로

개시자 그룹은 단일 액세스 경로에 연결됩니다.

- 경로 없음

개시자 그룹에 연결된 액세스 경로가 없습니다.

포트 세트를 통해 이니시에이터 그룹이 모든 인터페이스에 매핑되었는지, 아니면 특정 인터페이스에 매핑되었는지 확인할 수 있습니다. 매핑된 인터페이스 열에서 카운트 링크를 클릭하면 모든 인터페이스가 표시되거나 포트 집합에 대한 특정 인터페이스가 표시됩니다. 대상 포털을 통해 매핑된 인터페이스는 표시되지 않습니다. 이니시에이터 그룹에 매핑된 이니시에이터와 LUN의 총 수가 표시됩니다.

선택한 이니시에이터 그룹에 매핑된 LUN과 이니시에이터도 볼 수 있습니다.

- **이니시에이터 탭**

선택한 스토리지 VM에 대한 이니시에이터의 이름과 유형, 그리고 이 이니시에이터에 매핑된 이니시에이터 그룹의 총 개수를 표시합니다.

```
initiator groups that are mapped to the selected initiator group.
```

관련 주석 창

관련 주석 창을 사용하면 선택한 스토리지 VM과 관련된 주석 세부 정보를 볼 수 있습니다. 세부 정보에는 스토리지 VM에 적용되는 주석 이름과 주석 값이 포함됩니다. 관련 주석 창에서 수동 주석을 제거할 수도 있습니다.

관련 장치 창

관련 장치 창에서는 스토리지 VM과 관련된 클러스터, 집계 및 볼륨을 볼 수 있습니다.

- 무리

스토리지 VM이 속한 클러스터의 상태를 표시합니다.

- 집계

선택한 스토리지 VM에 속하는 집계의 수를 표시합니다. 또한 가장 높은 심각도 수준을 기준으로 집계의 상태도 표시됩니다. 예를 들어, 스토리지 VM에 10개의 집계가 포함되어 있고 그 중 5개가 경고 상태를 표시하고 나머지 5개가 위험 상태를 표시하는 경우 표시되는 상태는 위험입니다.

- 할당된 집계

스토리지 VM에 할당된 집계 수를 표시합니다. 또한 가장 높은 심각도 수준을 기준으로 집계의 상태도 표시됩니다.

- 권수

선택한 스토리지 VM에 속한 볼륨의 수와 용량을 표시합니다. 볼륨의 상태도 가장 높은 심각도 수준을 기준으로 표시됩니다. 스토리지 VM에 FlexGroup 볼륨이 있는 경우 FlexGroup도 계산에 포함됩니다. FlexGroup 구성 요소는 계산에 포함되지 않습니다.

관련 그룹 창

관련 그룹 창에서는 선택한 스토리지 VM과 연관된 그룹 목록을 볼 수 있습니다.

관련 알림 창

관련 알림 창에서는 선택한 스토리지 VM에 대해 생성된 알림 목록을 볼 수 있습니다. 알림 추가 링크를 클릭하여 알림을 추가하거나 알림 이름을 클릭하여 기존 알림을 편집할 수도 있습니다.

클러스터/상태 세부 정보 페이지

클러스터/상태 세부 정보 페이지는 상태, 용량, 구성 세부 정보 등 선택한 클러스터에 대한 자세한 정보를 제공합니다. 또한 클러스터의 네트워크 인터페이스(LIF), 노드, 디스크, 관련 장치 및 관련 알림에 대한 정보를 볼 수 있습니다.

클러스터 이름 옆의 상태(예: (좋음))는 통신 상태를 나타냅니다. 즉, Unified Manager가 클러스터와 통신할 수 있는지 여부를 나타냅니다. 이는 클러스터의 장애 조치 상태나 전반적인 상태를 나타내지 않습니다.

명령 버튼

명령 버튼을 사용하면 선택한 클러스터에 대해 다음 작업을 수행할 수 있습니다.

- 성능 보기로 전환

클러스터/성능 세부 정보 페이지로 이동할 수 있습니다.

- 행위

- 알림 추가: 알림 추가 대화 상자를 열고 선택한 클러스터에 알림을 추가할 수 있습니다.
- 재검색: 클러스터의 수동 새로 고침을 시작하여 Unified Manager가 클러스터의 최근 변경 사항을 검색할 수 있도록 합니다.

Unified Manager가 OnCommand Workflow Automation 과 페어링된 경우 재검색 작업은 WFA에서 캐시된 데이터(있는 경우)도 다시 수집합니다.

재발견 작업이 시작된 후에는 관련 작업 세부 정보에 대한 링크가 표시되어 작업 상태를 추적할 수 있습니다.

- 주석 달기: 선택한 클러스터에 주석을 달 수 있습니다.

• 클러스터 보기

Health: All Clusters 보기로 이동할 수 있습니다.

건강 탭

노드, SVM, 집계 등 다양한 클러스터 개체의 데이터 가용성 및 데이터 용량 문제에 대한 자세한 정보를 표시합니다. 가용성 문제는 클러스터 객체의 데이터 제공 기능과 관련이 있습니다. 용량 문제는 클러스터 객체의 데이터 저장 기능과 관련이 있습니다.

객체의 그래프를 클릭하면 필터링된 객체 목록을 볼 수 있습니다. 예를 들어, 경고를 표시하는 SVM 용량 그래프를 클릭하면 필터링된 SVM 목록을 볼 수 있습니다. 이 목록에는 심각도 수준이 '경고'인 용량 문제가 있는 볼륨이나 Q트리가 있는 SVM이 포함되어 있습니다. 경고를 표시하는 SVM 가용성 그래프를 클릭하면 심각도 수준이 '경고'인 가용성 문제가 있는 SVM 목록을 볼 수 있습니다.

가용성 문제

가용성 문제가 있는 객체와 가용성 관련 문제가 없는 객체를 포함하여 총 객체 수를 그래픽으로 표시합니다. 그래프의 색상은 문제의 심각도 수준을 나타냅니다. 그래프 아래의 정보는 클러스터의 데이터 가용성에 영향을 미칠 수 있거나 이미 영향을 미쳤던 가용성 문제에 대한 세부 정보를 제공합니다. 예를 들어, 다운된 디스크 셀프와 오프라인인 집계에 대한 정보가 표시됩니다.



SFO 막대 그래프에 표시되는 데이터는 노드의 HA 상태를 기반으로 합니다. 다른 모든 막대 그래프에 표시되는 데이터는 생성된 이벤트를 기반으로 계산됩니다.

용량 문제

용량 문제가 있는 객체와 용량 관련 문제가 없는 객체를 포함하여 총 객체 수를 그래픽으로 표시합니다. 그래프의 색상은 문제의 심각도 수준을 나타냅니다. 그래프 아래의 정보는 클러스터의 데이터 용량에 영향을 미칠 수 있거나 이미 영향을 미친 용량 문제에 대한 세부 정보를 제공합니다. 예를 들어, 설정된 임계값을 위반할 가능성이 있는 집계에 대한 정보가 표시됩니다.

용량 탭

선택한 클러스터의 용량에 대한 자세한 정보를 표시합니다.

용량

할당된 모든 집계에서 사용된 용량과 사용 가능한 용량에 대한 데이터 용량 그래프를 표시합니다.

- 사용된 논리적 공간

ONTAP 스토리지 효율성 기술을 사용하여 절감한 비용을 적용하지 않고 이 클러스터의 모든 집계에 저장되는 데이터의 실제 크기입니다. 여기에는 스냅샷 사본은 포함되지 않습니다.

- 데이터 감소

스냅샷 사본 없이 두 개의 유효 숫자를 사용하여 비율을 표시합니다(예: 1.8 대 1). 이 비율은 구성된 ONTAP 스토리지 효율성 설정을 기반으로 합니다.

- 사용된

모든 집계의 데이터가 사용하는 물리적 용량입니다. 여기에는 패리티, 적정 크기 조정 및 예약에 사용되는 용량은 포함되지 않습니다.

- 사용 가능

사용 가능한 데이터 용량을 표시합니다.

- 예비품

모든 예비 디스크에 저장할 수 있는 저장 용량을 표시합니다.

- 제공됨

모든 기본 볼륨에 대해 프로비저닝된 용량을 표시합니다.

세부

사용된 용량과 사용 가능한 용량에 대한 자세한 정보를 표시합니다. 계산에는 루트 집계 데이터가 제외됩니다.

- 총 용량

클러스터의 총 용량을 표시합니다. 여기에는 패리티에 할당된 용량은 포함되지 않습니다.

- 사용된

데이터가 사용하는 용량을 표시합니다. 여기에는 패리티, 적정 크기 조정 및 예약에 사용되는 용량은 포함되지 않습니다.

- 사용 가능

사용 가능한 데이터 용량을 표시합니다.

- 제공됨

모든 기본 볼륨에 대해 프로비저닝된 용량을 표시합니다.

- 예비품

모든 예비 디스크에 저장할 수 있는 저장 용량을 표시합니다.

클라우드 티어

클러스터에서 FabricPool 지원 집계에 대해 사용된 총 클라우드 계층 용량과 연결된 각 클라우드 계층에 사용된 용량을 표시합니다. FabricPool 라이선스가 있을 수도 있고 없을 수도 있습니다.

디스크 유형별 물리적 용량 분석

디스크 유형별 물리적 용량 분석 영역에는 클러스터의 다양한 디스크 유형에 대한 디스크 용량에 대한 자세한 정보가 표시됩니다. 디스크 유형을 클릭하면 디스크 탭에서 디스크 유형에 대한 자세한 정보를 볼 수 있습니다.

- 총 사용 가능 용량

데이터 디스크의 사용 가능한 용량과 여유 용량을 표시합니다.

- 하드디스크

클러스터 내 모든 HDD 데이터 디스크의 사용된 용량과 사용 가능한 용량을 그래픽으로 표시합니다. 점선은 HDD의 데이터 디스크의 여유 용량을 나타냅니다.

- 플래시

- SSD 데이터

클러스터 내 SSD 데이터 디스크의 사용된 용량과 사용 가능한 용량을 그래픽으로 표시합니다.

- SSD 캐시

클러스터 내 SSD 캐시 디스크의 저장 가능 용량을 그래픽으로 표시합니다.

- SSD 스페어

클러스터의 SSD, 데이터 및 캐시 디스크의 여유 용량을 그래픽으로 표시합니다.

- 할당되지 않은 디스크

클러스터에서 할당되지 않은 디스크의 수를 표시합니다.

용량 문제 목록이 있는 집계

용량 위험 문제가 있는 집계의 사용된 용량과 사용 가능한 용량에 대한 세부 정보를 표 형식으로 표시합니다.

- 상태

집계에 특정 심각도의 용량 관련 문제가 있음을 나타냅니다.

집계에 대해 생성된 이벤트에 대한 자세한 정보를 보려면 상태 위로 포인터를 이동하세요.

집계 상태가 단일 이벤트에 의해 결정되는 경우 이벤트 이름, 이벤트가 트리거된 시간 및 날짜, 이벤트가 할당된 관리자 이름, 이벤트 원인 등의 정보를 볼 수 있습니다. 자세한 내용 보기 버튼을 클릭하면 이벤트에 대한 자세한 내용을 볼 수 있습니다.

집계 상태가 동일한 심각도의 여러 이벤트에 의해 결정되는 경우, 상위 3개 이벤트가 이벤트 이름, 이벤트가 트리거된 시간 및 날짜, 이벤트가 할당된 관리자 이름 등의 정보와 함께 표시됩니다. 각 이벤트에 대한 자세한 내용을

보려면 이벤트 이름을 클릭하세요. 모든 이벤트 보기 링크를 클릭하면 생성된 이벤트 목록을 볼 수도 있습니다.



집계에는 동일하거나 다른 심각도를 가진 여러 개의 용량 관련 이벤트가 있을 수 있습니다. 하지만 가장 높은 심각도만 표시됩니다. 예를 들어, 집계에 오류와 위험 심각도 수준을 가진 두 개의 이벤트가 있는 경우 위험 심각도만 표시됩니다.

- 골재

집계의 이름을 표시합니다.

- 사용된 데이터 용량

전체 용량 사용량에 대한 정보를 그래픽으로 표시합니다(백분율).

- 만기까지 걸리는 일수

집계가 최대 용량에 도달하기까지 남은 예상 일수를 표시합니다.

구성 탭

IP 주소, 연락처, 위치 등 선택한 클러스터에 대한 세부 정보를 표시합니다.

클러스터 개요

- 관리 인터페이스

Unified Manager가 클러스터에 연결하는 데 사용하는 클러스터 관리 LIF를 표시합니다. 인터페이스의 작동 상태도 표시됩니다.

- 호스트 이름 또는 IP 주소

Unified Manager가 클러스터에 연결하는 데 사용하는 클러스터 관리 LIF의 FQDN, 약어 또는 IP 주소를 표시합니다.

- FQDN

클러스터의 정규화된 도메인 이름(FQDN)을 표시합니다.

- OS 버전

클러스터가 실행 중인 ONTAP 버전을 표시합니다. 클러스터의 노드가 서로 다른 버전의 ONTAP 실행 중인 경우 가장 빠른 ONTAP 버전이 표시됩니다.

- 연락처

클러스터에 문제가 있는 경우 문의해야 할 관리자에 대한 세부 정보를 표시합니다.

- 위치

클러스터의 위치를 표시합니다.

- 성격

이것이 All SAN Array로 구성된 클러스터인지 식별합니다.

원격 클러스터 개요

MetroCluster 구성의 원격 클러스터에 대한 세부 정보를 제공합니다. 이 정보는 MetroCluster 구성에 대해서만 표시됩니다.

- 무리

원격 클러스터의 이름을 표시합니다. 클러스터 이름을 클릭하면 클러스터의 세부 정보 페이지로 이동할 수 있습니다.

- 호스트 이름 또는 IP 주소

원격 클러스터의 FQDN, 약어 또는 IP 주소를 표시합니다.

- 위치

원격 클러스터의 위치를 표시합니다.

MetroCluster 개요

FC를 통한 MetroCluster 또는 IP를 통한 MetroCluster 구성의 로컬 클러스터에 대한 세부 정보를 제공합니다. 이 정보는 FC 또는 IP 구성을 통한 MetroCluster에만 표시됩니다.

- 유형

MetroCluster 유형이 2노드인지 4노드인지 표시합니다. IP를 통한 MetroCluster의 경우 4노드만 지원됩니다.

- 구성

FC 및 IP를 통한 MetroCluster 구성을 표시합니다. 다음 값을 가질 수 있습니다.

FC용

- SAS 케이블을 사용한 스트레치 구성
- FC-SAS 브리지를 사용한 스트레치 구성
- FC 스위치를 사용한 패브릭 구성



4노드 MetroCluster의 경우 FC 스위치를 사용한 패브릭 구성만 지원됩니다.

IP용

- 이더넷 스위치를 사용한 IP 구성(클러스터 구성 방식에 따라 L2 또는 L3)
 - 자동 비계획 전환(AUSO)

로컬 클러스터에 대해 자동화된 계획되지 않은 전환이 활성화되어 있는지 여부를 표시합니다. 기본적으로 AUSO는 Unified Manager의 2노드 MetroCluster 구성에 있는 모든 클러스터에 대해 활성화됩니다. 명령줄 인터페이스를 사용하여 AUSO 설정을 변경할 수 있습니다. 이 기능은 FC를 통한 MetroCluster에만

지원됩니다.

- 스위치 오버 모드

IP 구성을 통한 MetroCluster 의 전환 모드를 표시합니다. 사용 가능한 값은 다음과 같습니다. Active , Negotiated Switchover , 그리고 Automatic Unplanned Switchover .

노드

- 유효성

작동 중인 노드 수를 표시합니다(●) 또는 아래로 (●) 클러스터에 있습니다.

- OS 버전

노드가 실행 중인 ONTAP 버전과 특정 버전의 ONTAP 실행하는 노드 수를 표시합니다. 예를 들어, 9.6(2), 9.3(1)은 두 개의 노드가 ONTAP 9.6을 실행하고 있고, 한 개의 노드가 ONTAP 9.3을 실행하고 있음을 지정합니다.

스토리지 가상 머신

- 유효성

작동 중인 SVM의 수를 표시합니다(●) 또는 아래로 (●) 클러스터에 있습니다.

네트워크 인터페이스

- 유효성

작동 중인 비데이터 LIF의 수를 표시합니다(●) 또는 아래로 (●) 클러스터에 있습니다.

- 클러스터 관리 인터페이스

클러스터 관리 LIF의 수를 표시합니다.

- 노드 관리 인터페이스

노드 관리 LIF의 수를 표시합니다.

- 클러스터 인터페이스

클러스터 LIF의 수를 표시합니다.

- 클러스터 간 인터페이스

클러스터 간 LIF의 수를 표시합니다.

프로토콜

- 데이터 프로토콜

클러스터에 대해 활성화된 라이선스 데이터 프로토콜 목록을 표시합니다. 데이터 프로토콜에는 iSCSI, CIFS, NFS,

NVMe, FC/FCoE가 포함됩니다.

보호

• 중재자

클러스터가 중재자를 지원하는지 여부와 중재자의 연결 상태를 표시합니다. 중재자가 구성되었는지 여부를 나타내며, 구성된 경우 중재자의 상태를 표시합니다.

◦ 해당 없음

클러스터가 중재자를 지원하지 않을 때 표시됩니다.

◦ 구성되지 않음

클러스터가 중재자를 지원하지만 중재자가 구성되지 않은 경우 표시됩니다.

◦ IP 주소

클러스터가 중재자를 지원하고 중재자가 구성된 경우 표시됩니다. 중재자 상태는 색상으로 표시됩니다. 녹색은 중재자 상태에 도달할 수 있음을 나타냅니다. 빨간색은 중재자 상태에 도달할 수 없음을 나타냅니다.

클라우드 계층

이 클러스터가 연결된 클라우드 계층의 이름을 나열합니다. 또한 유형(Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Google Cloud Storage, Alibaba Cloud Object Storage 또는 StorageGRID)과 클라우드 계층의 상태(사용 가능 또는 사용 불가능)도 나열합니다.

MetroCluster 연결 탭

FC 구성을 통한 MetroCluster의 클러스터 구성 요소의 문제와 연결 상태를 표시합니다. 클러스터의 재해 복구 파트너에 문제가 발생하면 해당 클러스터가 빨간색 상자에 표시됩니다.



MetroCluster 연결 탭은 FC 구성을 통한 MetroCluster에 있는 클러스터에만 표시됩니다.

원격 클러스터의 이름을 클릭하면 원격 클러스터의 세부 정보 페이지로 이동할 수 있습니다. 구성 요소의 개수 링크를 클릭하면 구성 요소의 세부 정보를 볼 수도 있습니다. 예를 들어, 클러스터의 노드 카운트 링크를 클릭하면 클러스터의 세부 정보 페이지에 노드 탭이 표시됩니다. 원격 클러스터의 디스크 개수 링크를 클릭하면 원격 클러스터의 세부 정보 페이지에 디스크 탭이 표시됩니다.



8노드 MetroCluster 구성을 관리할 때 디스크 셀프 구성 요소의 카운트 링크를 클릭하면 기본 HA 쌍의 로컬 셀프만 표시됩니다. 또한 다른 HA 쌍에 로컬 선반을 표시할 방법이 없습니다.

문제가 발생한 경우 구성 요소 위로 포인터를 옮기면 클러스터의 세부 정보와 연결 상태를 볼 수 있으며, 문제에 대해 생성된 이벤트에 대한 자세한 정보를 볼 수 있습니다.

구성 요소 간 연결 문제 상태가 단일 이벤트로 결정되는 경우 이벤트 이름, 이벤트가 트리거된 시간 및 날짜, 이벤트가 할당된 관리자 이름, 이벤트 원인 등의 정보를 볼 수 있습니다. 세부 정보 보기 버튼을 클릭하면 이벤트에 대한 자세한 정보를 볼 수 있습니다.

구성 요소 간 연결 문제 상태가 동일한 심각도의 여러 이벤트로 확인되는 경우, 상위 3개 이벤트가 이벤트 이름, 이벤트가

트리거된 시간 및 날짜, 이벤트가 할당된 관리자 이름 등의 정보와 함께 표시됩니다. 각 이벤트에 대한 자세한 내용을 보려면 이벤트 이름을 클릭하세요. 모든 이벤트 보기 링크를 클릭하면 생성된 이벤트 목록을 볼 수도 있습니다.

MetroCluster 복제 탭

FC 구성을 통해 MetroCluster 에서 복제되는 데이터의 상태를 표시합니다. MetroCluster 복제 탭을 사용하면 이미 피어링된 클러스터와 데이터를 동기적으로 미러링하여 데이터 보호를 보장할 수 있습니다. 클러스터의 재해 복구 파트너에 문제가 발생하면 해당 클러스터가 빨간색 상자에 표시됩니다.



MetroCluster 복제 탭은 FC 구성을 통한 MetroCluster 에 있는 클러스터에만 표시됩니다.

MetroCluster 환경에서 이 탭을 사용하여 로컬 클러스터와 원격 클러스터의 논리적 연결 및 피어링을 확인할 수 있습니다. 논리적 연결을 통해 클러스터 구성 요소의 객관적인 표현을 볼 수 있습니다. 이는 메타데이터와 데이터를 미러링하는 동안 발생할 수 있는 문제를 식별하는 데 도움이 됩니다.

MetroCluster 복제 탭에서 로컬 클러스터는 선택한 클러스터의 자세한 그래픽 표현을 제공하고 MetroCluster 파트너는 원격 클러스터를 나타냅니다.

네트워크 인터페이스 탭

선택한 클러스터에 생성된 모든 비데이터 LIF에 대한 세부 정보를 표시합니다.

네트워크 인터페이스

선택한 클러스터에 생성된 LIF의 이름을 표시합니다.

운영 상태

인터페이스의 작동 상태를 표시합니다. 작동 상태는 Up(↑), 아래에 (↓), 또는 알 수 없음(?). 네트워크 인터페이스의 작동 상태는 물리적 포트의 상태에 따라 결정됩니다.

행정 상태

인터페이스의 관리 상태를 표시합니다. 상태는 다음과 같습니다. ↑, 아래에 (↓), 또는 알 수 없음(?). 구성을 변경하거나 유지 관리하는 동안 인터페이스의 관리 상태를 제어할 수 있습니다. 행정 상태는 운영 상태와 다를 수 있습니다. 그러나 LIF의 관리 상태가 '중단'인 경우 운영 상태도 기본적으로 '중단'이 됩니다.

IP 주소

인터페이스의 IP 주소를 표시합니다.

역할

인터페이스의 역할을 표시합니다. 가능한 역할로는 클러스터 관리 LIF, 노드 관리 LIF, 클러스터 LIF, 클러스터 간 LIF가 있습니다.

모형

인터페이스가 원래 연결된 물리적 포트를 표시합니다.

현재 항구

인터페이스가 현재 연결되어 있는 물리적 포트를 표시합니다. LIF 마이그레이션 후 현재 포트가 홈 포트와 다를 수 있습니다.

장애 조치 정책

인터페이스에 대해 구성된 장애 조치 정책을 표시합니다.

라우팅 그룹

라우팅 그룹의 이름을 표시합니다. 라우팅 그룹 이름을 클릭하면 경로와 대상 게이트웨이에 대한 자세한 정보를 볼 수 있습니다.

ONTAP 8.3 이상에서는 라우팅 그룹이 지원되지 않으므로 이러한 클러스터에 대해 빈 열이 표시됩니다.

장애 조치 그룹

장애 조치 그룹의 이름을 표시합니다.

노드 탭

선택한 클러스터의 노드에 대한 정보를 표시합니다. HA 쌍, 디스크 셸프 및 포트에 대한 자세한 정보를 볼 수 있습니다.

HA 세부 정보

HA 쌍의 노드의 HA 상태와 상태를 그림으로 표현합니다. 노드의 상태는 다음 색상으로 표시됩니다.

- 녹색

노드는 작동 상태입니다.

- 노란색

노드가 파트너 노드를 인수했거나 노드가 환경 문제에 직면해 있습니다.

- 빨간색

노드가 다운되었습니다.

HA 쌍의 가용성에 대한 정보를 보고 위험을 방지하기 위해 필요한 조치를 취할 수 있습니다. 예를 들어, 인수 작업이 가능한 경우 다음 메시지가 표시됩니다. 스토리지 장애 조치가 가능합니다.

팬, 전원 공급 장치, NVRAM 배터리, 플래시 카드, 서비스 프로세서, 디스크 셸프 연결 등 HA 쌍 및 해당 환경과 관련된 이벤트 목록을 볼 수 있습니다. 이벤트가 발생한 시간도 볼 수 있습니다.

모델 번호 등 노드 관련 다른 정보를 볼 수 있습니다.

단일 노드 클러스터가 있는 경우 노드에 대한 세부 정보도 볼 수 있습니다.

디스크 선반

HA 쌍의 디스크 셸프에 대한 정보를 표시합니다.

디스크 셸프와 환경 구성 요소에 대해 생성된 이벤트와 이벤트가 트리거된 시간도 볼 수 있습니다.

- 선반 ID

디스크가 위치한 셸프의 ID를 표시합니다.

- 구성요소 상태

전원 공급 장치, 팬, 온도 센서, 전류 센서, 디스크 연결, 전압 센서 등 디스크 선반의 환경 세부 정보를 표시합니다. 환경 세부 정보는 다음 색상의 아이콘으로 표시됩니다.

- 녹색

환경적 요소가 제대로 작동하고 있습니다.

- 회색

환경적 요소에 대한 데이터는 없습니다.

- 빨간색

일부 환경적 요소가 감소했습니다.

- 상태

디스크 선반의 상태를 표시합니다. 가능한 상태는 오프라인, 온라인, 상태 없음, 초기화 필요, 누락, 알 수 없음입니다.

- 모델

디스크 선반의 모델 번호를 표시합니다.

- 로컬 디스크 셸프

디스크 셸프가 로컬 클러스터에 있는지, 원격 클러스터에 있는지를 나타냅니다. 이 열은 MetroCluster 구성의 클러스터에만 표시됩니다.

- 고유 ID

디스크 선반의 고유 식별자를 표시합니다.

- 펌웨어 버전

디스크 선반의 펌웨어 버전을 표시합니다.

포트

연관된 FC, FCoE 및 이더넷 포트에 대한 정보를 표시합니다. 포트 아이콘을 클릭하면 포트와 관련 LIF에 대한 세부 정보를 볼 수 있습니다.

포트에 대해 생성된 이벤트도 볼 수 있습니다.

다음 포트 세부 정보를 볼 수 있습니다.

- 포트 ID

포트의 이름을 표시합니다. 예를 들어, 포트 이름은 e0M, e0a, e0b가 될 수 있습니다.

- 역할

포트의 역할을 표시합니다. 가능한 역할은 클러스터, 데이터, 클러스터 간, 노드 관리 및 정의되지 않음입니다.

- 유형

포트에 사용된 물리적 계층 프로토콜을 표시합니다. 가능한 유형으로는 이더넷, 파이버 채널, FCoE가 있습니다.

- WWPN

포트의 WWPN(World Wide Port Name)을 표시합니다.

- 펌웨어 개정

FC/FCoE 포트의 펌웨어 개정판을 표시합니다.

- 상태

포트의 현재 상태를 표시합니다. 가능한 상태는 Up, Down, Link Not Connected 또는 Unknown입니다. (?)

이벤트 목록에서 포트 관련 이벤트를 볼 수 있습니다. LIF 이름, 운영 상태, IP 주소 또는 WWPN, 프로토콜, LIF와 연관된 SVM 이름, 현재 포트, 장애 조치 정책 및 장애 조치 그룹과 같은 연관된 LIF 세부 정보도 볼 수 있습니다.

디스크 탭

선택한 클러스터의 디스크에 대한 세부 정보를 표시합니다. 사용된 디스크 수, 예비 디스크, 손상된 디스크, 할당되지 않은 디스크 등 디스크 관련 정보를 볼 수 있습니다. 디스크 이름, 디스크 유형, 디스크 소유자 노드 등의 기타 세부 정보도 볼 수 있습니다.

디스크 풀 요약

FCAL, SAS, SATA, MSATA, SSD, NVMe SSD, SSD CAP, Array LUN, VMDISK 등 효과적인 유형별로 분류된 디스크 수와 디스크 상태를 표시합니다. 또한 집계 수, 공유 디스크, 예비 디스크, 손상된 디스크, 할당되지 않은 디스크, 지원되지 않는 디스크 등의 기타 세부 정보도 볼 수 있습니다. 유효 디스크 유형 개수 링크를 클릭하면 선택한 상태와 유효 유형의 디스크가 표시됩니다. 예를 들어, 디스크 상태가 손상되었고 유효 유형이 SAS인 디스크의 개수 링크를 클릭하면 디스크 상태가 손상되었고 유효 유형이 SAS인 모든 디스크가 표시됩니다.

디스크

디스크의 이름을 표시합니다.

RAID 그룹

RAID 그룹의 이름을 표시합니다.

소유자 노드

디스크가 속한 노드의 이름을 표시합니다. 디스크가 할당되지 않은 경우 이 열에 값이 표시되지 않습니다.

상태

디스크 상태를 표시합니다: 집계, 공유, 예비, 손상, 할당되지 않음, 지원되지 않음 또는 알 수 없음. 기본적으로 이 열은 다음 순서로 상태를 표시하도록 정렬됩니다. 손상됨, 할당되지 않음, 지원되지 않음, 예비, 집계 및 공유됨.

로컬 디스크

디스크가 로컬 클러스터에 있는지, 원격 클러스터에 있는지를 나타내는 '예' 또는 '아니요'를 표시합니다. 이 열은 MetroCluster 구성의 클러스터에만 표시됩니다.

위치

디스크의 위치를 컨테이너 유형(예: 복사, 데이터 또는 패리티)에 따라 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

영향을 받은 골재

실패한 디스크로 인해 영향을 받는 집계의 수를 표시합니다. 영향을 받은 집계를 보려면 포인터를 카운트 링크 위로 이동한 다음 집계 이름을 클릭하면 집계의 세부 정보를 볼 수 있습니다. 또한 집계 수를 클릭하면 Health: All Aggregates 보기에서 영향을 받은 집계 목록을 볼 수 있습니다.

다음의 경우에는 이 열에 값이 표시되지 않습니다.

- Unified Manager에 해당 디스크가 포함된 클러스터를 추가할 때 손상된 디스크의 경우
- 실패한 디스크가 없는 경우

스토리지 풀

SSD가 속한 스토리지 풀의 이름을 표시합니다. 스토리지 풀 이름 위에 포인터를 놓으면 스토리지 풀의 세부 정보를 볼 수 있습니다.

저장 가능 용량

사용 가능한 디스크 용량을 표시합니다.

원시 용량

적절한 크기 조정 및 RAID 구성 전의 원시, 포맷되지 않은 디스크의 용량을 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

유형

디스크 유형을 표시합니다(예: ATA, SATA, FCAL 또는 VMDISK).

효과적인 유형

ONTAP에서 할당한 디스크 유형을 표시합니다.

특정 ONTAP 디스크 유형은 집계를 만들고 추가하며, 예비 디스크를 관리하는 목적에 있어서 동등한 것으로 간주됩니다. ONTAP 각 디스크 유형에 효과적인 디스크 유형을 할당합니다.

예비 블록 소모량 %

SSD 디스크에서 소모된 여유 블록의 백분율을 표시합니다. SSD 디스크가 아닌 디스크의 경우 이 열은 비어 있습니다.

정격 수명 사용 %

실제 SSD 사용량과 제조업체의 SSD 수명 예측을 기반으로 사용된 SSD 수명의 추정치를 백분율로 표시합니다. 99보다 큰 값은 추정된 내구성이 소모되었음을 나타내지만 SSD 오류를 나타내지는 않을 수 있습니다. 값을 알 수 없으면 디스크는 생략됩니다.

펌웨어

디스크의 펌웨어 버전을 표시합니다.

분당 회전수

디스크의 분당 회전수(RPM)를 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

모델

디스크의 모델 번호를 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

공급업체

디스크 공급업체의 이름을 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

선반 ID

디스크가 위치한 쉘프의 ID를 표시합니다.

만

디스크가 위치한 베이의 ID를 표시합니다.

관련 주석 창

선택한 클러스터와 관련된 주석 세부 정보를 볼 수 있습니다. 세부 정보에는 클러스터에 적용되는 주석 이름과 주석 값이 포함됩니다. 관련 주석 창에서 수동 주석을 제거할 수도 있습니다.

관련 장치 창

선택한 클러스터와 연결된 장치 세부 정보를 볼 수 있습니다.

세부 정보에는 클러스터에 연결된 장치의 속성(장치 유형, 크기, 개수, 상태 등)이 포함됩니다. 해당 기기에 대한 추가 분석을 원하시면 카운트 링크를 클릭하세요.

MetroCluster 파트너 창을 사용하면 노드, 집계, SVM과 같은 연관된 클러스터 구성 요소와 함께 원격 MetroCluster 파트너에 대한 개수와 세부 정보를 얻을 수 있습니다. MetroCluster 파트너 창은 MetroCluster 구성의 클러스터에 대해서만 표시됩니다.

관련 장치 창을 사용하면 클러스터와 관련된 노드, SVM 및 집계를 보고 탐색할 수 있습니다.

MetroCluster 파트너

MetroCluster 파트너의 상태를 표시합니다. 카운트 링크를 사용하면 더 자세히 탐색하고 클러스터 구성 요소의 상태와 용량에 대한 정보를 얻을 수 있습니다.

노드

선택한 클러스터에 속한 노드의 수, 용량 및 상태를 표시합니다. 용량은 사용 가능한 용량을 가용 용량으로 나눈 총 사용 가능 용량을 나타냅니다.

스토리지 가상 머신

선택한 클러스터에 속한 SVM의 수를 표시합니다.

골재

선택한 클러스터에 속한 집계의 수, 용량 및 상태를 표시합니다.

관련 그룹 창

선택한 클러스터가 포함된 그룹 목록을 볼 수 있습니다.

관련 알림 창

관련 알림 창에서는 선택한 클러스터에 대한 알림 목록을 볼 수 있습니다. 알림 추가 링크를 클릭하여 알림을 추가하거나 알림 이름을 클릭하여 기존 알림을 편집할 수도 있습니다.

관련 정보

["볼륨 페이지" "클러스터 목록 및 세부 정보 보기"](#)

집계/상태 세부 정보 페이지

집계/상태 세부 정보 페이지를 사용하면 용량, 디스크 정보, 구성 세부 정보, 생성된 이벤트 등 선택한 집계에 대한 자세한 정보를 볼 수 있습니다. 해당 집계에 대한 관련 객체 및 관련 알림에 대한 정보도 볼 수 있습니다.

명령 버튼



FabricPool 활성화된 집계를 모니터링할 때 이 페이지의 커밋된 값과 초과 커밋된 값은 로컬 또는 성능 계층 용량에만 적용됩니다. 클라우드 계층에서 사용 가능한 공간의 양은 초과 할당 값에 반영되지 않습니다. 마찬가지로, 집계 임계값은 로컬 성능 계층에만 적용됩니다.

명령 단추를 사용하면 선택한 집계에 대해 다음 작업을 수행할 수 있습니다.

- 성능 보기로 전환

집계/성과 세부 정보 페이지로 이동할 수 있습니다.

- 행위

- 알림 추가

선택한 집계에 알림을 추가할 수 있습니다.

- 임계값 편집

선택한 집계에 대한 임계값 설정을 수정할 수 있습니다.

- 집계 보기

Health: All Aggregates 보기로 이동할 수 있습니다.

용량 탭

용량 탭에는 선택한 집계에 대한 자세한 정보(용량, 임계값, 일일 성장률 등)가 표시됩니다.

기본적으로 루트 집계에 대한 용량 이벤트는 생성되지 않습니다. 또한 Unified Manager에서 사용하는 임계값은 노드 루트 집계에 적용할 수 없습니다. 이러한 이벤트 생성에 대한 설정을 수정할 수 있는 사람은 기술 지원 담당자뿐입니다. 기술 지원 담당자가 설정을 수정하면 임계값이 노드 루트 집계에 적용됩니다.

- 용량

집계에 대한 용량 세부 정보를 표시하는 데이터 용량 그래프와 스냅샷 복사본 그래프를 표시합니다.

- 사용된 논리적 공간

ONTAP 저장 효율성 기술을 사용하여 절감한 비용을 적용하지 않고 집계된 데이터의 실제 크기입니다.

- 사용된

데이터가 집계하여 사용하는 물리적 용량입니다.

- 과도하게 헌신하다

전체 공간이 과도하게 할당된 경우 차트에는 과도하게 할당된 양이 표시된 플래그가 표시됩니다.

- 경고

경고 임계값이 설정된 위치에 점선을 표시합니다. 즉, 집계된 공간이 거의 가득 찼음을 의미합니다. 이 임계값을 초과하면 공간이 거의 가득 찼습니다 이벤트가 생성됩니다.

- 오류

오류 임계값이 설정된 위치에 실선이 표시됩니다. 즉, 집계 공간이 가득 찼음을 의미합니다. 이 임계값을 초과하면 공간 가득 참 이벤트가 생성됩니다.

- 스냅샷 복사본 그래프

이 그래프는 사용된 스냅샷 용량이나 스냅샷 예약이 0이 아닌 경우에만 표시됩니다.

두 그래프 모두 사용된 스냅샷 용량이 스냅샷 예약 용량을 초과하는 경우 스냅샷 용량이 스냅샷 예약 용량을

초과하는 용량을 표시합니다.

- 클라우드 티어

FabricPool 지원 집계에 대한 클라우드 계층의 데이터가 사용하는 공간을 표시합니다. FabricPool 라이선스가 있을 수도 있고 없을 수도 있습니다.

클라우드 계층이 다른 클라우드 공급자("미러 계층")에 미러링되면 두 클라우드 계층이 여기에 표시됩니다.

- 세부

용량에 대한 자세한 정보를 표시합니다.

- 총 용량

전체 용량을 집계하여 표시합니다.

- 데이터 용량

집계에서 사용된 공간의 양(사용된 용량)과 집계에서 사용 가능한 공간의 양(여유 용량)을 표시합니다.

- 스냅샷 예약

집계된 스냅샷 용량과 남은 스냅샷 용량을 표시합니다.

- 초과 할당 용량

전체 초과 약속을 표시합니다. 집계 초과 커밋을 사용하면 현재 모든 저장 공간이 사용되지 않는 한, 주어진 집계에서 실제로 사용 가능한 것보다 더 많은 저장 공간을 제공할 수 있습니다. 씬 프로비저닝을 사용하는 경우 집계된 볼륨의 총 크기가 집계의 총 용량을 초과할 수 있습니다.



집계에 과도한 용량을 할당한 경우 사용 가능한 공간을 주의 깊게 모니터링하고 필요에 따라 저장 공간을 추가해야 공간 부족으로 인한 쓰기 오류가 발생하지 않습니다.

- 클라우드 티어

FabricPool 지원 집계에 대한 클라우드 계층의 데이터가 사용하는 공간을 표시합니다. FabricPool 라이선스가 있을 수도 있고 없을 수도 있습니다. 클라우드 계층이 다른 클라우드 공급자(미러 계층)에 미러링되면 두 클라우드 계층이 여기에 표시됩니다.

- 총 캐시 공간

Flash Pool 집계에 추가된 SSD(솔리드 스테이트 드라이브) 또는 할당 단위의 총 공간을 표시합니다. 집계를 위해 Flash Pool을 활성화했지만 SSD를 추가하지 않은 경우 캐시 공간이 0KB로 표시됩니다.



집계에 대해 Flash Pool이 비활성화된 경우 이 필드는 숨겨집니다.

- 집계 임계값

다음의 집계 용량 임계값을 표시합니다.

- 거의 가득 찬 임계값

집계가 거의 채워지는 비율을 지정합니다.

- 전체 임계값

집계가 가득 찬 비율을 지정합니다.

- 거의 초과 할당 임계값

집계가 과도하게 할당되는 비율을 지정합니다.

- 초과 할당 임계값

집계가 과도하게 할당되는 비율을 지정합니다.

- 기타 세부 정보: 일일 성장률

마지막 두 샘플 간의 변화율이 24시간 동안 지속될 경우 집계에 사용된 디스크 공간을 표시합니다.

예를 들어, 집계가 오후 2시에 10GB의 디스크 공간을 사용하고 오후 6시에 12GB를 사용하는 경우 이 집계의 일일 증가율(GB)은 2GB입니다.

- 볼륨 이동

현재 진행 중인 볼륨 이동 작업의 수를 표시합니다.

- 볼륨 아웃

집계에서 이동되는 볼륨의 수와 용량을 표시합니다.

링크를 클릭하면 볼륨 이름, 볼륨이 이동된 집계, 볼륨 이동 작업의 상태, 예상 종료 시간 등의 자세한 내용을 볼 수 있습니다.

- 볼륨

집계로 이동 중인 볼륨의 수와 남은 용량을 표시합니다.

링크를 클릭하면 볼륨 이름, 볼륨이 이동된 집계, 볼륨 이동 작업 상태, 예상 종료 시간 등의 자세한 내용을 볼 수 있습니다.

- 볼륨 이동 후 예상 사용 용량

볼륨 이동 작업이 완료된 후 사용된 공간의 추정량(백분율, KB, MB, GB 등)을 집계하여 표시합니다.

- 용량 개요 - 볼륨

집계에 포함된 볼륨의 용량에 대한 정보를 제공하는 그래프를 표시합니다. 볼륨에서 사용된 공간의 양(사용된 용량)과 볼륨에서 사용 가능한 공간의 양(여유 용량)이 표시됩니다. 씬 프로비저닝된 볼륨에 대해 씬 프로비저닝된 볼륨 공간 위험 이벤트가 생성되면 볼륨에서 사용된 공간의 양(사용된 용량)과 볼륨에서 사용 가능하지만 집계 용량 문제로 인해 사용할 수 없는 공간의 양(사용 불가능 용량)이 표시됩니다.

드롭다운 목록에서 보고 싶은 그래프를 선택할 수 있습니다. 그래프에 표시된 데이터를 정렬하여 사용된 크기, 프로비저닝된 크기, 사용 가능한 용량, 가장 빠른 일일 성장률, 가장 느린 성장률과 같은 세부 정보를 표시할 수 있습니다. 집계된 볼륨을 포함하는 스토리지 가상 머신(SVM)을 기준으로 데이터를 필터링할 수 있습니다. 씬

프로비저닝된 볼륨에 대한 세부 정보도 볼 수 있습니다. 관심 있는 영역 위에 커서를 놓으면 그래프에서 특정 지점의 세부 정보를 볼 수 있습니다. 기본적으로 그래프는 집계된 상위 30개 필터링된 볼륨을 표시합니다.

디스크 정보 탭

RAID 유형 및 크기, 집계에 사용된 디스크 유형을 포함하여 선택한 집계에 있는 디스크에 대한 자세한 정보를 표시합니다. 이 탭에는 RAID 그룹과 사용된 디스크 유형(예: SAS, ATA, FCAL, SSD 또는 VMDISK)도 그래픽으로 표시됩니다. 커서를 패리티 디스크와 데이터 디스크 위에 놓으면 디스크 베이, 셸프, 회전 속도 등의 자세한 정보를 볼 수 있습니다.

• 데이터

전용 데이터 디스크, 공유 데이터 디스크 또는 둘 다에 대한 세부 정보를 그래픽으로 표시합니다. 데이터 디스크에 공유 디스크가 포함되어 있는 경우 공유 디스크의 그래픽 세부 정보가 표시됩니다. 데이터 디스크에 전용 디스크와 공유 디스크가 포함된 경우 전용 데이터 디스크와 공유 데이터 디스크 모두의 그래픽 세부 정보가 표시됩니다.

◦ RAID 세부 정보

RAID 세부 정보는 전용 디스크에 대해서만 표시됩니다.

▪ 유형

RAID 유형(RAID0, RAID4, RAID-DP 또는 RAID-TEC)을 표시합니다.

▪ 그룹 크기

RAID 그룹에서 허용되는 최대 디스크 수를 표시합니다.

▪ 여러 때

집계된 RAID 그룹의 수를 표시합니다.

◦ 사용된 디스크

▪ 효과적인 유형

데이터 디스크 유형(예: ATA, SATA, FCAL, SSD 또는 VMDISK)을 전체적으로 표시합니다.

▪ 데이터 디스크

집계에 할당된 데이터 디스크의 수와 용량을 표시합니다. 집계에 공유 디스크만 포함된 경우 데이터 디스크 세부 정보가 표시되지 않습니다.

▪ 패리티 디스크

집계에 할당된 패리티 디스크의 수와 용량을 표시합니다. 집계에 공유 디스크만 포함된 경우 패리티 디스크 세부 정보가 표시되지 않습니다.

▪ 공유 디스크

집계에 할당된 공유 데이터 디스크의 수와 용량을 표시합니다. 공유 디스크 세부 정보는 집계에 공유 디스크가 포함된 경우에만 표시됩니다.

- 예비 디스크

선택한 집계에서 노드에 사용 가능한 예비 데이터 디스크의 유효 디스크 유형, 개수 및 용량을 표시합니다.



집계가 파트너 노드로 장애 조치되면 Unified Manager는 집계와 호환되는 모든 예비 디스크를 표시하지 않습니다.

- **SSD 캐시**

전용 캐시 SSD 디스크와 공유 캐시 SSD 디스크에 대한 세부 정보를 제공합니다.

전용 캐시 SSD 디스크에 대한 세부 정보는 다음과 같습니다.

- **RAID** 세부 정보

- 유형

RAID 유형(RAID0, RAID4, RAID-DP 또는 RAID-TEC)을 표시합니다.

- 그룹 크기

RAID 그룹에서 허용되는 최대 디스크 수를 표시합니다.

- 여러 때

집계된 RAID 그룹의 수를 표시합니다.

- 사용된 디스크

- 효과적인 유형

집계된 캐시에 사용된 디스크가 SSD 유형임을 나타냅니다.

- 데이터 디스크

캐시에 대한 집계에 할당된 데이터 디스크의 수와 용량을 표시합니다.

- 패리티 디스크

캐시에 대한 집계에 할당된 패리티 디스크의 수와 용량을 표시합니다.

- 예비 디스크

캐시에 대해 선택된 집계에서 노드에 사용 가능한 예비 디스크의 효과적인 유형, 개수 및 용량을 표시합니다.



집계가 파트너 노드로 장애 조치되면 Unified Manager는 집계와 호환되는 모든 예비 디스크를 표시하지 않습니다.

공유 캐시에 대한 다음 세부 정보를 제공합니다.

- 저장 풀

스토리지 풀의 이름을 표시합니다. 스토리지 풀 이름 위에 포인터를 놓으면 다음 세부 정보를 볼 수 있습니다.

- 상태

스토리지 풀의 상태를 표시합니다. 상태는 정상 또는 비정상입니다.

- 총 할당량

총 할당 단위와 스토리지 풀의 크기를 표시합니다.

- 할당 단위 크기

집계에 할당할 수 있는 스토리지 풀의 최소 공간 크기를 표시합니다.

- 디스크

스토리지 풀을 생성하는 데 사용된 디스크 수를 표시합니다. 스토리지 풀 열의 디스크 수와 해당 스토리지 풀의 디스크 정보 탭에 표시된 디스크 수가 일치하지 않으면 하나 이상의 디스크가 손상되어 스토리지 풀이 정상적이지 않음을 나타냅니다.

- 사용된 할당

집계에서 사용되는 할당 단위의 수와 크기를 표시합니다. 집계 이름을 클릭하면 집계 세부 정보를 볼 수 있습니다.

- 사용 가능한 할당량

노드에 사용 가능한 할당 단위의 수와 크기를 표시합니다. 노드 이름을 클릭하면 집계 세부 정보를 볼 수 있습니다.

- 할당된 캐시

집계에서 사용되는 할당 단위의 크기를 표시합니다.

- 할당 단위

집계에 사용된 할당 단위 수를 표시합니다.

- 디스크

스토리지 풀에 포함된 디스크 수를 표시합니다.

- 세부

- 스토리지 풀

스토리지 풀의 수를 표시합니다.

- 전체 크기

스토리지 풀의 총 크기를 표시합니다.

- 클라우드 티어

FabricPool 활성화된 집계를 구성한 경우 클라우드 계층의 이름을 표시하고 사용된 총 공간을 보여줍니다. 클라우드

계층이 다른 클라우드 공급자(미러 계층)로 미러링되면 두 클라우드 계층에 대한 세부 정보가 여기에 표시됩니다.

구성 탭

구성 탭에는 클러스터 노드, 블록 유형, RAID 유형, RAID 크기, RAID 그룹 수 등 선택한 집계에 대한 세부 정보가 표시됩니다.

- 개요

- 마디

선택한 집계를 포함하는 노드의 이름을 표시합니다.

- 블록 유형

집계의 블록 형식을 32비트 또는 64비트로 표시합니다.

- RAID 유형

RAID 유형(RAID0, RAID4, RAID-DP, RAID-TEC 또는 혼합 RAID)을 표시합니다.

- RAID 사이즈

RAID 그룹의 크기를 표시합니다.

- RAID 그룹

집계된 RAID 그룹의 수를 표시합니다.

- SnapLock 타입

집계의 SnapLock 유형을 표시합니다.

- 클라우드 티어

이것이 FabricPool 지원 집계인 경우 클라우드 계층에 대한 세부 정보가 표시됩니다. 일부 필드는 저장소 제공업체에 따라 다릅니다. 클라우드 계층이 다른 클라우드 공급자("미러 계층")에 미러링되면 두 클라우드 계층이 여기에 표시됩니다.

- 공급자

스토리지 공급자의 이름(예: StorageGRID, Amazon S3, IBM Cloud Object Storage, Microsoft Azure Cloud, Google Cloud Storage 또는 Alibaba Cloud Object Storage)을 표시합니다.

- 이름

ONTAP 에서 클라우드 계층을 생성할 때 해당 클라우드 계층의 이름을 표시합니다.

- 섬기는 사람

클라우드 계층의 FQDN을 표시합니다.

- 포트

클라우드 공급자와 통신하는 데 사용되는 포트입니다.

- 액세스 키 또는 계정

클라우드 계층에 대한 액세스 키 또는 계정을 표시합니다.

- 컨테이너 이름

클라우드 계층의 버킷 또는 컨테이너 이름을 표시합니다.

- SSL

클라우드 계층에 SSL 암호화가 활성화되어 있는지 여부를 표시합니다.

역사 지역

기록 영역에는 선택한 집계 용량의 용량에 대한 정보를 제공하는 그래프가 표시됩니다. 또한, 내보내기 버튼을 클릭하면 현재 보고 있는 차트에 대한 CSV 형식의 보고서를 만들 수 있습니다.

기록 창 상단의 드롭다운 목록에서 그래프 유형을 선택할 수 있습니다. 1주일, 1개월, 1년 중 하나를 선택하여 특정 기간에 대한 세부 정보를 볼 수도 있습니다. 기록 그래프는 추세를 파악하는 데 도움이 됩니다. 예를 들어, 집계 사용량이 지속적으로 '거의 가득 참' 임계값을 초과하는 경우 적절한 조치를 취할 수 있습니다.

기록 그래프는 다음 정보를 표시합니다.

- 사용된 총 용량(%)

세로(y)축에 사용 내역을 기준으로 집계된 용량의 사용 추세와 사용된 용량을 백분율로 선 그래프로 표시합니다. 기간은 수평(x)축에 표시됩니다. 일주일, 한 달, 또는 일년 중 원하는 기간을 선택할 수 있습니다. 그래프의 특정 지점에 대한 세부 정보를 보려면 커서를 특정 영역 위에 올려놓으세요. 해당 범례를 클릭하면 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어, 사용된 용량 범례를 클릭하면 사용된 용량 그래프 선이 숨겨집니다.

- 사용된 총 용량 대비 총 용량

수직(y)축에 바이트, 킬로바이트, 메가바이트 등의 단위를 선 그래프로 표시하고, 사용 내역을 기반으로 집계 용량이 어떻게 사용되는지 추세를 표시하며, 사용된 용량과 전체 용량을 표시합니다. 기간은 수평(x)축에 표시됩니다. 일주일, 한 달, 또는 일년 중 원하는 기간을 선택할 수 있습니다. 그래프의 특정 지점에 대한 세부 정보를 보려면 커서를 특정 영역 위에 올려놓으세요. 해당 범례를 클릭하면 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어, 사용된 추세 용량 범례를 클릭하면 사용된 추세 용량 그래프 선이 숨겨집니다.

- 사용된 총 용량(%) 대비 약정된 용량(%)

수직(y)축에 사용 내역과 커밋된 공간을 기준으로 집계 용량이 어떻게 사용되는지 추세를 선 그래프로 백분율로 표시합니다. 기간은 수평(x)축에 표시됩니다. 일주일, 한 달, 또는 일년 중 원하는 기간을 선택할 수 있습니다. 그래프의 특정 지점에 대한 세부 정보를 보려면 커서를 특정 영역 위에 올려놓으세요. 해당 범례를 클릭하면 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어, 할당된 공간 범례를 클릭하면 할당된 공간 그래프 선이 숨겨집니다.

이벤트 목록

이벤트 목록에는 새 이벤트와 확인된 이벤트에 대한 세부 정보가 표시됩니다.

- 심각성

이벤트의 심각도를 표시합니다.

- 이벤트

이벤트 이름을 표시합니다.

- 트리거 시간

이벤트가 생성된 이후 경과된 시간을 표시합니다. 경과 시간이 일주일을 초과하면 이벤트가 생성된 타임스탬프가 표시됩니다.

관련 장치 창

관련 장치 창을 사용하면 집계와 관련된 클러스터 노드, 볼륨 및 디스크를 볼 수 있습니다.

- 마디

집계를 포함하는 노드의 용량과 상태를 표시합니다. 용량은 사용 가능한 용량을 가용 용량으로 나눈 총 사용 가능 용량을 나타냅니다.

- 노드의 집계

선택한 집계가 포함된 클러스터 노드에 있는 모든 집계의 수와 용량을 표시합니다. 또한 가장 높은 심각도 수준을 기준으로 집계의 상태도 표시됩니다. 예를 들어, 클러스터 노드에 10개의 집계가 포함되어 있고 그 중 5개가 경고 상태를 표시하고 나머지 5개가 위험 상태를 표시하는 경우 표시되는 상태는 위험입니다.

- 권수

FlexVol 볼륨과 FlexGroup 볼륨의 수와 용량을 전체적으로 표시합니다. 이 수치에는 FlexGroup 구성 요소는 포함되지 않습니다. 볼륨의 상태도 가장 높은 심각도 수준을 기준으로 표시됩니다.

- 자원 풀

집계와 관련된 리소스 풀을 표시합니다.

- 디스크

선택한 집계에 있는 디스크의 수를 표시합니다.

관련 알림 창

관련 알림 창을 사용하면 선택한 집계에 대해 생성된 알림 목록을 볼 수 있습니다. 알림 추가 링크를 클릭하여 알림을 추가하거나 알림 이름을 클릭하여 기존 알림을 편집할 수도 있습니다.

관련 정보

["스토리지 풀 세부 정보 보기"](#)

데이터 보호 및 복원

보호 관계 생성, 모니터링 및 문제 해결

Unified Manager를 사용하면 보호 관계를 생성하고, 관리되는 클러스터에 저장된 데이터의 미러 보호 및 백업 볼트 보호를 모니터링하고 문제를 해결하고, 데이터가 덮어쓰여지거나 손실된 경우 데이터를 복원할 수 있습니다.

SnapMirror 보호 유형

데이터 스토리지 토폴로지의 배포에 따라 Unified Manager를 사용하면 여러 유형의 SnapMirror 보호 관계를 구성할 수 있습니다. SnapMirror 보호의 모든 변형은 장애 조치 재해 복구 보호 기능을 제공하지만 성능, 버전 유연성 및 다중 백업 사본 보호 측면에서 제공하는 기능이 다릅니다.

기존 SnapMirror 비동기 보호 관계

기존 SnapMirror 비동기 보호는 소스 볼륨과 대상 볼륨 간에 블록 복제 미러 보호 기능을 제공합니다.

기존 SnapMirror 관계에서는 미러 작업이 블록 복제를 기반으로 하기 때문에 대체 SnapMirror 관계보다 미러 작업이 더 빠르게 실행됩니다. 그러나 기존 SnapMirror 보호 기능을 사용하려면 대상 볼륨이 동일한 주요 릴리스 내의 소스 볼륨과 동일하거나 그 이후의 ONTAP 소프트웨어 마이너 버전(예: 버전 8.x에서 8.x로 또는 9.x에서 9.x로)에서 실행되어야 합니다. 대상에서 이전 주요 버전이 실행되고 있기 때문에 9.1 소스에서 9.0 대상으로의 복제는 지원되지 않습니다.

SnapMirror 비동기 보호 및 버전 유연한 복제

SnapMirror 비동기 보호 기능과 버전 유연한 복제 기능은 소스 볼륨과 대상 볼륨 간에 논리적 복제 미러 보호 기능을 제공하며, 해당 볼륨이 서로 다른 ONTAP 8.3 이상 소프트웨어 버전(예: 버전 8.3에서 8.3.1, 8.3에서 9.1, 9.2.2에서 9.2)에서 실행되는 경우에도 마찬가지입니다.

버전에 따라 유연한 복제가 가능한 SnapMirror 관계에서는 미러 작업이 기존 SnapMirror 관계에서보다 빠르게 실행되지 않습니다.

SnapMirror의 버전 유연한 복제 보호 기능은 실행 속도가 느리기 때문에 다음 두 가지 상황에서는 구현하기에 적합하지 않습니다.

- 소스 객체에는 보호해야 할 파일이 1,000만 개 이상 포함되어 있습니다.
- 보호된 데이터의 복구 지점 목표는 2시간 이하입니다. (즉, 대상에는 항상 소스의 데이터보다 2시간 이상 오래되지 않은 미러링되고 복구 가능한 데이터가 포함되어 있어야 합니다.)

나열된 두 가지 상황 모두에서 기본 SnapMirror 보호의 더 빠른 블록 복제 기반 실행이 필요합니다.

SnapMirror 비동기 보호, 버전에 따라 유연한 복제 및 백업 옵션 제공

SnapMirror 비동기 보호 기능과 버전에 유연한 복제 및 백업 옵션은 소스 볼륨과 대상 볼륨 간의 미러 보호 기능을 제공하고 대상에 미러링된 데이터의 여러 사본을 저장하는 기능을 제공합니다.

스토리지 관리자는 어떤 스냅샷 복사본을 소스에서 대상으로 미러링할지 지정할 수 있으며, 소스에서 복사본이 삭제된

경우에도 대상에서 해당 복사본을 얼마나 오랫동안 보관할지 지정할 수 있습니다.

버전에 따라 유연한 복제 및 백업 옵션이 제공되는 SnapMirror 관계에서는 미리 작업이 기존 SnapMirror 관계에서보다 빠르게 실행되지 않습니다.

SnapMirror 통합 복제(미러 및 볼트)

SnapMirror 통합 복제를 사용하면 동일한 대상 볼륨에서 재해 복구와 보관을 구성할 수 있습니다. SnapMirror 와 마찬가지로 통합 데이터 보호 기능은 처음 호출할 때 기존 전송을 수행합니다. 기본 통합 데이터 보호 정책인 "MirrorAndVault"에 따른 기존선 전송은 소스 볼륨의 스냅샷 복사본을 만든 다음 해당 복사본과 참조하는 데이터 블록을 대상 볼륨으로 전송합니다. SnapVault 와 마찬가지로 통합 데이터 보호에는 기존선에 이전 스냅샷 사본이 포함되지 않습니다.

SnapMirror 엄격한 동기화를 통한 동기 보호

SnapMirror "strict" 동기화를 통한 동기 보호 기능은 기본 볼륨과 보조 볼륨이 항상 서로의 정확한 사본이 되도록 보장합니다. 보조 볼륨에 데이터를 쓰려고 할 때 복제 실패가 발생하면 기본 볼륨에 대한 클라이언트 I/O가 중단됩니다.

SnapMirror 정기 동기화를 통한 동기 보호

"일반" 동기화를 통한 SnapMirror 동기 보호는 기본 볼륨과 보조 볼륨이 항상 서로의 정확한 사본일 필요가 없으므로 기본 볼륨의 가용성을 보장합니다. 보조 볼륨에 데이터를 쓰려고 할 때 복제 오류가 발생하면 기본 볼륨과 보조 볼륨이 동기화되지 않고 클라이언트 I/O는 기본 볼륨으로 계속 진행됩니다.



동기식 보호 관계를 모니터링하는 경우 [상태: 모든 볼륨] 보기나 [볼륨/상태 세부 정보] 페이지에서 복원 버튼과 관계 작업 버튼을 사용할 수 없습니다.

SnapMirror 액티브 싱크

SnapMirror Active Sync 기능은 ONTAP 9.8 이상에서 사용할 수 있으며, LUN을 사용하여 애플리케이션을 보호하고 애플리케이션이 투명하게 장애 조치되도록 하여 재해 발생 시에도 비즈니스 연속성을 보장할 수 있습니다.

Unified Manager에서 클러스터 및 스토리지 가상 머신에 사용 가능한 일관성 그룹(CG)에 대한 동기식 SnapMirror 관계를 검색하고 모니터링할 수 있습니다. SnapMirror 액티브 동기화는 AFF 클러스터 또는 모든 SAN 어레이(ASA) 클러스터에서 지원되며, 여기서 기본 및 보조 클러스터는 AFF 또는 ASA 가 될 수 있습니다. SnapMirror Active Sync는 iSCSI 또는 FCP LUN을 사용하여 애플리케이션을 보호합니다.

SnapMirror 활성 동기화 관계로 보호되는 볼륨과 LUN을 볼 때 보호 관계, 볼륨 인벤토리의 일관성 그룹, 일관성 그룹 관계에 대한 보호 토폴로지 보기, 최대 1년 동안의 일관성 그룹 관계에 대한 기록 데이터 보기에 대한 통합된 보기를 얻을 수 있습니다. 보고서를 다운로드할 수도 있습니다. 일관성 그룹 관계 요약 보고, 일관성 그룹 관계에 대한 지원을 검색하고, 일관성 그룹으로 보호되는 볼륨에 대한 정보를 얻을 수도 있습니다.

관계 페이지에서는 일관성 그룹으로 보호되는 소스 및 대상 저장소 개체와 해당 개체의 관계에 대한 보호를 정렬, 필터링하고 확장할 수도 있습니다.

SnapMirror Active Sync에 대해 자세히 알아보려면 다음을 참조하세요. ["Snapmirror Active Sync\(이전 SM-BC\)에 대한 ONTAP 9 설명서"](#).

Unified Manager에서 보호 관계 설정

Unified Manager와 OnCommand Workflow Automation 사용하여 SnapMirror 와 SnapVault

관계를 설정하여 데이터를 보호하려면 여러 단계를 수행해야 합니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 두 개의 클러스터 또는 두 개의 스토리지 가상 머신(SVM) 간에 피어 관계를 설정해야 합니다.
- OnCommand Workflow Automation Unified Manager와 통합되어야 합니다.
 - ["OnCommand Workflow Automation 설정"](#).
 - ["Workflow Automation에서 Unified Manager 데이터 소스 캐싱 확인"](#).

단계

1. 만들려는 보호 관계 유형에 따라 다음 중 하나를 수행합니다.
 - ["SnapMirror 보호 관계 만들기"](#).
 - ["SnapVault 보호 관계 만들기"](#).
2. 관계에 대한 정책을 만들려면, 만들고 있는 관계 유형에 따라 다음 중 하나를 수행하세요.
 - ["SnapVault 정책 만들기"](#).
 - ["SnapMirror 정책 만들기"](#).
3. ["SnapMirror 또는 SnapVault 일정 만들기"](#).

Workflow Automation과 Unified Manager 간 연결 구성

OnCommand Workflow Automation (WFA)과 Unified Manager 간에 보안 연결을 구성할 수 있습니다. Workflow Automation에 연결하면 SnapMirror 및 SnapVault 구성 워크플로와 같은 보호 기능은 물론 SnapMirror 관계를 관리하는 명령도 사용할 수 있습니다.

시작하기 전에

- Workflow Automation의 설치된 버전은 5.1.1P6 이상이어야 합니다.



"클러스터형 Data ONTAP 관리를 위한 WFA 팩"은 WFA 5.1.1P6에 포함되어 있으므로 과거처럼 NetAppStorage Automation Store에서 이 팩을 다운로드하여 WFA 서버에 별도로 설치할 필요가 없습니다. ["ONTAP 관리를 위한 WFA 팩"](#)

- WFA 및 Unified Manager 연결을 지원하려면 Unified Manager에서 만든 데이터베이스 사용자 이름이 있어야 합니다.

이 데이터베이스 사용자에게는 통합 스키마 사용자 역할이 할당되어 있어야 합니다.

- Workflow Automation에서 관리자 역할이나 아키텍트 역할이 지정되어야 합니다.
- Workflow Automation 설정을 위해서는 호스트 주소, 포트 번호 443, 사용자 이름, 비밀번호가 필요합니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *워크플로 자동화*를 클릭합니다.
2. 워크플로 자동화 페이지*의 *데이터베이스 사용자 영역에서 Unified Manager 및 워크플로 자동화 연결을 지원하기

위해 생성한 데이터베이스 사용자의 이름을 선택하고 비밀번호를 입력합니다.

3. 해당 페이지의 워크플로 자동화 자격 증명 영역에서 워크플로 자동화 설정을 위한 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)와 사용자 이름 및 비밀번호를 입력합니다.

Unified Manager 서버 포트(포트 443)를 사용해야 합니다.

4. *저장*을 클릭하세요.
5. 자체 서명 인증서를 사용하는 경우 *예*를 클릭하여 보안 인증서를 승인합니다.

워크플로 자동화 페이지가 표시됩니다.

6. *예*를 클릭하면 웹 UI가 다시 로드되고 워크플로 자동화 기능이 추가됩니다.

관련 정보

["NetApp 설명서: OnCommand Workflow Automation \(현재 릴리스\)"](#)

Workflow Automation에서 Unified Manager 데이터 소스 캐싱 확인

Workflow Automation에서 데이터 소스 수집이 성공했는지 확인하여 Unified Manager 데이터 소스 캐싱이 올바르게 작동하는지 확인할 수 있습니다. Workflow Automation을 Unified Manager와 통합할 때 이 작업을 수행하면 통합 후에도 Workflow Automation 기능을 사용할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 Workflow Automation에서 관리자 역할이나 아키텍트 역할이 할당되어야 합니다.

단계

1. 워크플로 자동화 UI에서 실행 > *데이터 소스*를 선택합니다.
2. Unified Manager 데이터 소스의 이름을 마우스 오른쪽 버튼으로 클릭한 다음 *지금 가져오기*를 선택합니다.
3. 오류 없이 인수가 성공적으로 완료되었는지 확인하세요.

Workflow Automation과 Unified Manager의 통합을 성공시키려면 획득 오류를 해결해야 합니다.

OnCommand Workflow Automation 다시 설치하거나 업그레이드하면 어떻게 되나요?

OnCommand Workflow Automation 다시 설치하거나 업그레이드하기 전에 먼저 OnCommand Workflow Automation과 Unified Manager 간의 연결을 제거하고 현재 실행 중이거나 예약된 모든 OnCommand Workflow Automation 작업이 중지되었는지 확인해야 합니다.

OnCommand Workflow Automation에서 Unified Manager를 수동으로 삭제해야 합니다.

OnCommand Workflow Automation 다시 설치하거나 업그레이드한 후에는 Unified Manager와의 연결을 다시 설정해야 합니다.

Unified Manager에서 OnCommand Workflow Automation 설정 제거

더 이상 Workflow Automation을 사용하지 않으려면 Unified Manager에서 OnCommand Workflow Automation 설정을 제거할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 왼쪽 설정 메뉴의 일반 > *워크플로 자동화*를 클릭합니다.
2. 워크플로 자동화 페이지에서 *설치 제거*를 클릭합니다.

보호 관계 장애 조치 및 장애 복구 수행

하드웨어 장애나 재해로 인해 보호 관계에 있는 소스 볼륨이 비활성화되면 Unified Manager의 보호 관계 기능을 사용하여 보호 대상을 읽기/쓰기로 액세스 가능하게 만들고 소스가 다시 온라인 상태가 될 때까지 해당 볼륨으로 장애 조치할 수 있습니다. 그런 다음 데이터를 제공할 수 있게 되면 원래 소스로 장애 조치할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 이 작업을 수행하려면 OnCommand Workflow Automation 설정해야 합니다.

단계

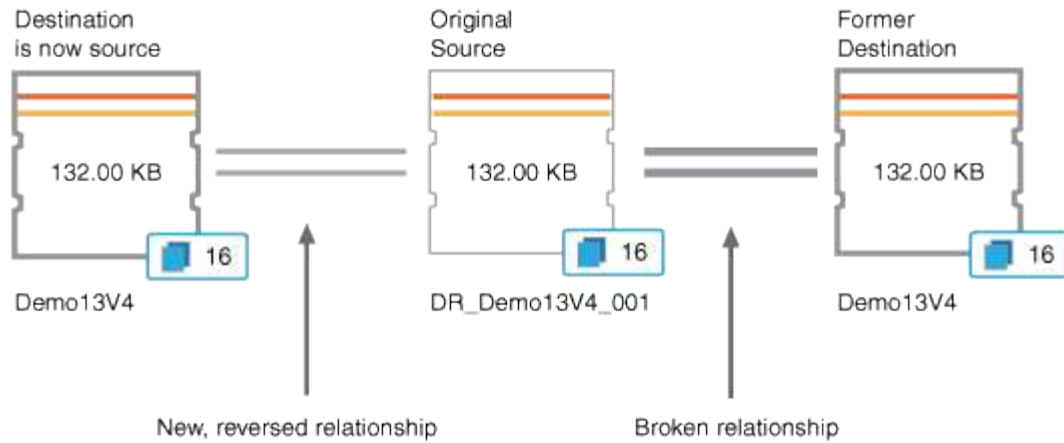
1. "[SnapMirror 관계 끊기](#)".

대상을 데이터 보호 볼륨에서 읽기/쓰기 볼륨으로 변환하려면 먼저 관계를 끊어야 하며, 관계를 되돌리려면 먼저 관계를 끊어야 합니다.

2. "[보호 관계 역전](#)".

원래 소스 볼륨을 다시 사용할 수 있게 되면 소스 볼륨을 복원하여 원래 보호 관계를 다시 설정할 수 있습니다. 소스를 복원하려면 먼저 이전 대상에 기록된 데이터와 소스를 동기화해야 합니다. 역방향 재동기화 작업을 사용하면 원래 관계의 역할을 반대로 바꾸고 소스 볼륨을 이전 대상과 동기화하여 새로운 보호 관계를 만들 수 있습니다. 새로운 관계에 대한 새로운 기준 스냅샷 복사본이 생성됩니다.

역방향 관계는 계단식 관계와 유사합니다.



3. "역방향 SnapMirror 관계 끊기".

원래 소스 볼륨이 다시 동기화되어 다시 데이터를 제공할 수 있게 되면 중단 작업을 사용하여 역전된 관계를 끊습니다.

4. "관계를 제거하세요".

역전된 관계가 더 이상 필요하지 않은 경우 원래 관계를 다시 설정하기 전에 해당 관계를 제거해야 합니다.

5. "관계를 다시 동기화합니다".

재동기화 작업을 사용하여 소스에서 대상으로 데이터를 동기화하고 원래 관계를 재설정합니다.

볼륨/상태 세부 정보 페이지에서 **SnapMirror** 관계 해제

볼륨/상태 세부 정보 페이지에서 보호 관계를 해제하고 SnapMirror 관계에서 소스 볼륨과 대상 볼륨 간의 데이터 전송을 중지할 수 있습니다. 재해 복구나 애플리케이션 테스트를 위해 데이터를 마이그레이션할 때 관계가 끊어질 수도 있습니다. 대상 볼륨이 읽기-쓰기 볼륨으로 변경됩니다. SnapVault 관계를 끊을 수 없습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

단계

1. 볼륨/상태 세부 정보 페이지의 보호 탭에서 해제하려는 SnapMirror 관계를 토폴로지에서 선택합니다.
2. 목적지를 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 *중단*을 선택합니다.

관계 끊기 대화 상자가 표시됩니다.

3. 관계를 종료하려면 *계속*을 클릭하세요.
4. 토폴로지에서 관계가 끊어졌는지 확인하세요.

재해로 인해 보호 관계의 소스 볼륨이 비활성화되면 소스를 복구하거나 교체하는 동안 대상 볼륨을 읽기/쓰기로 변환하여 데이터를 제공할 수 있습니다. 소스가 다시 데이터를 수신할 수 있게 되면 역방향 재동기화 작업을 사용하여 역방향으로 관계를 설정하고, 소스의 데이터를 읽기/쓰기 대상의 데이터와 동기화할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.
- 관계는 SnapVault 관계가 아니어야 합니다.
- 보호 관계가 이미 존재해야 합니다.
- 보호 관계는 반드시 끊어져야 합니다.
- 소스와 대상 모두 온라인이어야 합니다.
- 소스는 다른 데이터 보호 볼륨의 대상이어서는 안 됩니다.
- 이 작업을 수행하면 공통 스냅샷 복사본의 데이터보다 최신인 소스의 데이터는 삭제됩니다.
- 역방향 재동기화 관계에서 생성된 정책과 일정은 원래 보호 관계의 정책과 일정과 동일합니다.

정책과 일정이 없으면 생성됩니다.

단계

1. 볼륨/상태 세부 정보 페이지의 보호 탭에서 소스와 대상을 반대로 변경할 SnapMirror 관계를 토폴로지에서 찾아 마우스 오른쪽 버튼으로 클릭합니다.
2. 메뉴에서 *역방향 재동기화*를 선택합니다.

역방향 재동기화 대화 상자가 표시됩니다.

3. 역방향 재동기화 대화 상자에 표시된 관계가 역방향 재동기화 작업을 수행하려는 관계인지 확인한 다음, *제출*을 클릭합니다.

역방향 재동기화 대화 상자가 닫히고 볼륨/상태 세부 정보 페이지 상단에 작업 링크가 표시됩니다.

4. 선택 사항: 볼륨/상태* 세부 정보 페이지에서 *작업 보기*를 클릭하여 각 역방향 재동기화 작업의 상태를 추적합니다.
필터링된 작업 목록이 표시됩니다.

5. 선택 사항: 브라우저의 뒤로 화살표를 클릭하여 볼륨/상태 세부 정보 페이지로 돌아갑니다.

모든 작업이 성공적으로 완료되면 역방향 재동기화 작업이 완료됩니다.

볼륨/상태 세부 정보 페이지에서 보호 관계 제거

보호 관계를 제거하면 선택한 소스와 대상 간의 기존 관계를 영구적으로 삭제할 수 있습니다. 예를 들어, 다른 대상을 사용하여 관계를 만들려는 경우가 있습니다. 이 작업을 수행하면 모든 메타데이터가 제거되며 실행 취소할 수 없습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

단계

1. 볼륨/상태 세부 정보 페이지의 보호 탭에서 제거하려는 SnapMirror 관계를 토폴로지에서 선택합니다.
2. 목적지 이름을 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 *제거*를 선택합니다.

관계 제거 대화 상자가 표시됩니다.

3. 관계를 제거하려면 *계속*을 클릭하세요.

해당 관계는 볼륨/상태 세부 정보 페이지에서 제거됩니다.

볼륨/상태 세부 정보 페이지에서 보호 관계 재동기화

SnapMirror 또는 SnapVault 관계가 끊어진 후 대상이 읽기/쓰기로 설정된 경우 해당 관계의 데이터를 다시 동기화하여 소스의 데이터가 대상의 데이터와 일치하도록 할 수 있습니다. 소스 볼륨에서 필수 공통 스냅샷 복사본이 삭제되어 SnapMirror 또는 SnapVault 업데이트가 실패하는 경우에도 다시 동기화할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- OnCommand Workflow Automation 설정해야 합니다.

단계

1. 볼륨/상태 세부 정보 페이지의 보호 탭에서 토폴로지에서 다시 동기화하려는 보호 관계를 찾아 마우스 오른쪽 버튼으로 클릭합니다.
2. 메뉴에서 *재동기화*를 선택합니다.

또는 작업 메뉴에서 관계 > *다시 동기화*를 선택하여 현재 세부 정보를 보고 있는 관계를 다시 동기화합니다.

재동기화 대화 상자가 표시됩니다.

3. 재동기화 옵션 탭에서 전송 우선순위와 최대 전송 속도를 선택합니다.
4. 소스 스냅샷 복사본*을 클릭한 다음, *스냅샷 복사본 열에서 *기본값*을 클릭합니다.

소스 스냅샷 복사본 선택 대화 상자가 표시됩니다.

5. 기본 스냅샷 복사본을 전송하는 대신 기존 스냅샷 복사본을 지정하려면 *기존 스냅샷 복사본*을 클릭하고 목록에서 스냅샷 복사본을 선택합니다.
6. *제출*을 클릭하세요.

다시 동기화 대화 상자로 돌아갑니다.

7. 재동기화할 소스를 두 개 이상 선택한 경우 기존 스냅샷 복사본을 지정하려는 다음 소스에 대해 *기본값*을 클릭합니다.

8. 재동기화 작업을 시작하려면 *제출*을 클릭하세요.

재동기화 작업이 시작되고 볼륨/상태 세부 정보 페이지로 돌아가며 페이지 상단에 작업 링크가 표시됩니다.

9. 선택 사항: 볼륨/상태 세부 정보* 페이지에서 *작업 보기*를 클릭하여 각 재동기화 작업의 상태를 추적합니다.

필터링된 작업 목록이 표시됩니다.

10. 선택 사항: 브라우저의 뒤로 화살표를 클릭하여 볼륨/상태 세부 정보 페이지로 돌아갑니다.

모든 작업이 성공적으로 완료되면 재동기화 작업이 완료됩니다.

보호 작업 실패 해결

이 워크플로는 Unified Manager 대시보드에서 보호 작업 실패를 식별하고 해결하는 방법의 예를 제공합니다.

시작하기 전에

이 워크플로의 일부 작업을 수행하려면 관리자 역할을 사용하여 로그인해야 하므로 다양한 기능을 사용하는 데 필요한 역할에 대해 잘 알고 있어야 합니다.

이 시나리오에서는 대시보드 페이지에 접속하여 보호 작업에 문제가 있는지 확인합니다. 보호 사고 영역에서 작업 종료 사고가 있고 볼륨에서 보호 작업 실패 오류가 표시되어 있는 것을 확인할 수 있습니다. 이 오류를 조사하여 가능한 원인과 잠재적 해결책을 파악합니다.

단계

1. 대시보드의 해결되지 않은 사고 및 위험 영역의 보호 사고 패널에서 보호 작업 실패 이벤트를 클릭합니다.



이벤트에 대한 링크된 텍스트는 다음 형식으로 작성됩니다. `object_name:/object_name - Error Name`, 와 같은 `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

실패한 보호 작업에 대한 이벤트 세부 정보 페이지가 표시됩니다.

2. 요약 영역의 원인 필드에 있는 오류 메시지를 검토하여 문제를 파악하고 잠재적인 시정 조치를 평가합니다.

보다"문제를 식별하고 실패한 보호 작업에 대한 시정 조치를 수행합니다."

문제를 식별하고 실패한 보호 작업에 대한 시정 조치를 수행합니다.

이벤트 세부 정보 페이지의 원인 필드에서 작업 실패 오류 메시지를 검토한 결과, 스냅샷 복사 오류로 인해 작업이 실패한 것으로 확인되었습니다. 그런 다음 볼륨/상태 세부 정보 페이지로 이동하여 자세한 정보를 수집합니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

이벤트 세부 정보 페이지의 원인 필드에 제공된 오류 메시지에는 실패한 작업에 대한 다음 텍스트가 포함되어 있습니다.


```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

이 메시지는 다음과 같은 정보를 제공합니다.

- 백업 또는 미러링 작업이 성공적으로 완료되지 않았습니다.

이 작업에는 소스 볼륨 간의 보호 관계가 포함되었습니다. `cluster2_src_vol2` 가상 서버에서 `cluster2_src_svm` 그리고 대상 볼륨 `managed_svc2_vol3` 가상 서버에서 `cluster3_dst_svm`.

- 스냅샷 복사 작업이 실패했습니다. `0426cluster2_src_vol2snap` 소스 볼륨에서 `cluster2_src_svm:/cluster2_src_vol2`.

이 시나리오에서는 작업 실패의 원인과 잠재적인 시정 조치를 파악할 수 있습니다. 하지만 오류를 해결하려면 System Manager 웹 UI나 ONTAP CLI 명령에 액세스해야 합니다.

단계

- 오류 메시지를 검토한 결과, 소스 볼륨에서 스냅샷 복사 작업이 실패한 것으로 확인되었으며, 이는 소스 볼륨에 문제가 있을 가능성이 있음을 나타냅니다.

선택적으로 오류 메시지 끝에 있는 작업 세부 정보 링크를 클릭할 수 있지만, 이 시나리오의 목적을 위해 그렇게 하지 않기로 했습니다.

- 이벤트를 해결하려고 결정했다면 다음을 수행합니다.

- 할당 대상 버튼을 클릭하고 메뉴에서 *나*를 선택하세요.
- 이벤트에 대한 알림이 설정된 경우, 반복 알림이 더 이상 수신되지 않도록 하려면 확인 버튼을 클릭하세요.
- 선택적으로 이벤트에 대한 메모를 추가할 수도 있습니다.

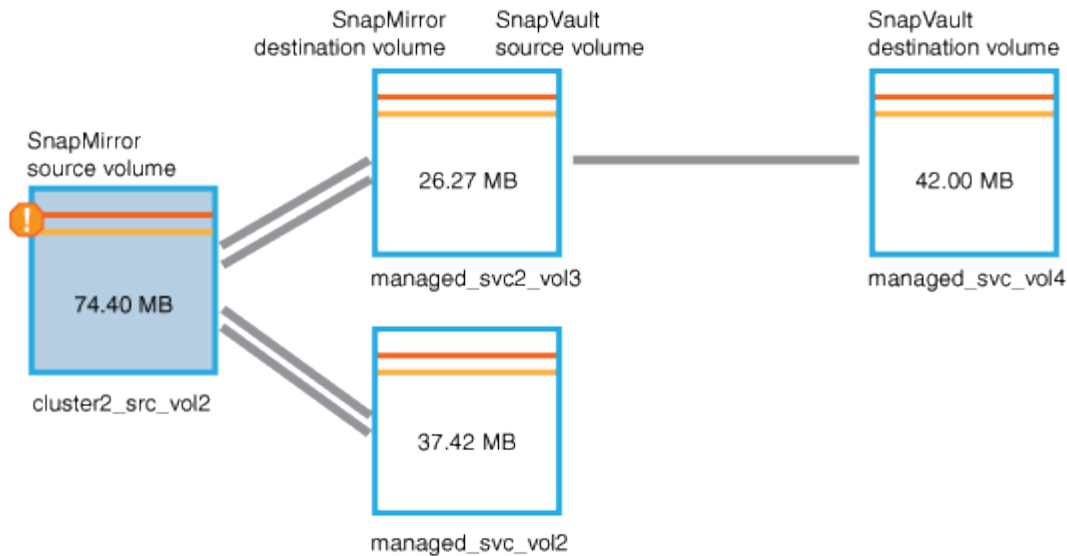
- 요약 창에서 소스 필드를 클릭하면 소스 볼륨에 대한 세부 정보를 볼 수 있습니다.

소스 필드에는 소스 개체의 이름이 포함됩니다. 이 경우 스냅샷 복사 작업이 예약된 볼륨입니다.

볼륨/상태 세부 정보 페이지가 표시됩니다. `cluster2_src_vol2` 보호 탭의 내용을 보여줍니다.

- 보호 토폴로지 그래프를 살펴보면 토폴로지의 첫 번째 볼륨과 연관된 오류 아이콘이 보이는데, 이는 SnapMirror 관계의 소스 볼륨입니다.

소스 볼륨 아이콘에 수평 막대가 표시되는데, 이는 해당 볼륨에 설정된 경고 및 오류 임계값을 나타냅니다.



5. 오류 아이콘 위에 커서를 놓으면 임계값 설정을 표시하는 팝업 대화 상자가 나타나고 볼륨이 오류 임계값을 초과했음을 알 수 있습니다. 이는 용량 문제를 나타냅니다.
6. 용량 탭을 클릭하세요.

볼륨에 대한 용량 정보 `cluster2_src_vol2` 디스플레이.

7. 용량 패널에서 막대 그래프에 오류 아이콘이 있는 것을 볼 수 있습니다. 이는 볼륨 용량이 볼륨에 대해 설정된 임계값 수준을 초과했음을 다시 한번 나타냅니다.
8. 용량 그래프 아래에서 볼륨 자동 증가가 비활성화되었고 볼륨 공간 보장이 설정되었음을 확인할 수 있습니다.

자동 증가를 활성화하기로 결정할 수도 있지만, 이 시나리오의 목적을 위해 용량 문제를 해결하는 방법을 결정하기 전에 자세히 조사하기로 결정했습니다.

9. 이벤트 목록으로 스크롤하면 보호 작업 실패, 볼륨이 가득 찰 때까지 남은 일수, 볼륨 공간 가득 참 이벤트가 생성된 것을 확인할 수 있습니다.
10. 이벤트 목록에서 볼륨 공간 가득 참 이벤트를 클릭하면 더 많은 정보를 얻을 수 있습니다. 이 이벤트가 용량 문제와 가장 관련이 있다고 판단하기 때문입니다.

이벤트 세부 정보 페이지에는 소스 볼륨에 대한 볼륨 공간 가득 참 이벤트가 표시됩니다.

11. 요약 영역에서 이벤트의 원인 필드를 읽어보세요. The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.
12. 요약 영역 아래에 제안된 시정 조치가 표시됩니다.



제안된 시정 조치는 일부 이벤트에만 표시되므로 모든 유형의 이벤트에 대해 이 영역이 표시되는 것은 아닙니다.

볼륨 공간 가득 참 이벤트를 해결하기 위해 수행할 수 있는 제안된 작업 목록을 클릭합니다.

- 이 볼륨에서 자동 증가를 활성화합니다.
- 볼륨 크기를 조절합니다.
- 이 볼륨에서 중복 제거를 활성화하고 실행합니다.

◦ 이 볼륨에서 압축을 활성화하고 실행합니다.

13. 볼륨에서 자동 증가를 활성화하기로 결정했지만, 그렇게 하려면 부모 집계에서 사용 가능한 여유 공간과 현재 볼륨 증가율을 확인해야 합니다.

a. 부모 집계를 살펴보세요. `cluster2_src_aggr1` 관련 장치 창에서.



집계 이름을 클릭하면 집계에 대한 자세한 내용을 볼 수 있습니다.

집계에 볼륨 자동 증가를 활성화할 수 있는 충분한 공간이 있는지 확인합니다.

b. 페이지 상단에서 중대한 사건을 나타내는 아이콘을 보고 아이콘 아래의 텍스트를 검토하세요.

"완전 완료까지 걸리는 일수: 1일 미만 | 일일 성장률: 5.4%"를 확인합니다.

14. 시스템 관리자로 이동하거나 ONTAP CLI에 액세스하여 활성화하세요. `volume autogrow` 옵션.



볼륨과 집계의 이름을 기록해 두면 자동 증가를 활성화할 때 사용할 수 있습니다.

15. 용량 문제를 해결한 후 Unified Manager 이벤트 세부 정보 페이지로 돌아가서 이벤트를 해결됨으로 표시합니다.

지연 문제 해결

이 워크플로는 지연 문제를 해결하는 방법에 대한 예를 제공합니다. 이 시나리오에서 귀하는 보호 관계에 문제가 있는지 확인하고, 문제가 있는 경우 해결책을 찾기 위해 Unified Manager 대시보드 페이지에 액세스하는 관리자 또는 운영자입니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

대시보드 페이지에서 해결되지 않은 사건 및 위험 영역을 살펴보면 보호 위험 아래의 보호 창에 SnapMirror 지연 오류가 표시됩니다.

단계

1. 대시보드 페이지의 보호 창에서 SnapMirror 관계 지연 오류를 찾아 클릭합니다.

지연 오류 이벤트에 대한 이벤트 세부 정보 페이지가 표시됩니다.

2. 이벤트 세부 정보 페이지에서 다음 작업 중 하나 이상을 수행할 수 있습니다.

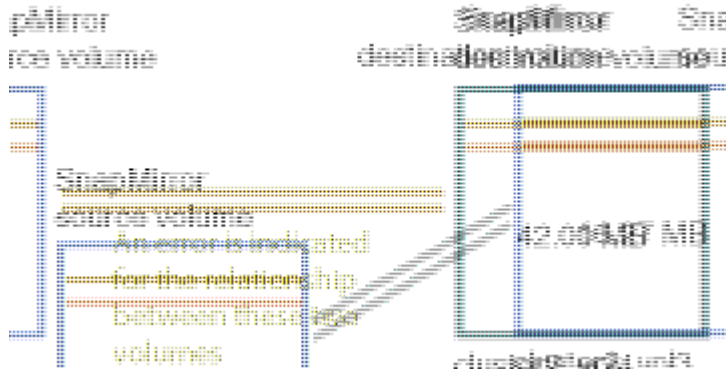
- 요약 영역의 원인 필드에 있는 오류 메시지를 검토하여 제안된 시정 조치가 있는지 확인하세요.
- 요약 영역의 소스 필드에서 개체 이름(이 경우 볼륨)을 클릭하면 볼륨에 대한 세부 정보를 얻을 수 있습니다.
- 이 이벤트에 대해 추가되었을 수 있는 메모를 찾아보세요.
- 이벤트에 메모를 추가합니다.
- 이벤트를 특정 사용자에게 할당합니다.
- 사건을 확인하거나 해결합니다.

3. 이 시나리오에서는 요약 영역의 소스 필드에서 개체 이름(이 경우 볼륨)을 클릭하여 볼륨에 대한 세부 정보를 얻습니다.

볼륨/상태 세부 정보 페이지의 보호 탭이 표시됩니다.

4. 보호 탭에서 토폴로지 다이어그램을 살펴보세요.

지연 오류가 있는 볼륨이 3개 볼륨으로 구성된 SnapMirror 캐스케이드의 마지막 볼륨이라는 점에 유의하세요. 선택한 볼륨은 짙은 회색으로 윤곽이 표시되고, 소스 볼륨에서 나오는 이중 주황색 선은 SnapMirror 관계 오류를 나타냅니다.



5. SnapMirror 계단식에서 각 볼륨을 클릭합니다.

각 볼륨을 선택하면 요약, 토폴로지, 기록, 이벤트, 관련 장치 및 관련 알림 영역의 보호 정보가 변경되어 선택한 볼륨과 관련된 세부 정보가 표시됩니다.

6. 요약 영역을 보고 각 권의 업데이트 일정 필드에 있는 정보 아이콘 위에 커서를 놓습니다.

이 시나리오에서는 SnapMirror 정책이 DPDefault이고 SnapMirror 일정은 매 시간 5분마다 업데이트된다는 점에 유의하세요. 관계의 모든 볼륨이 동시에 SnapMirror 전송을 완료하려고 시도하고 있다는 것을 알고 있습니다.

7. 지연 문제를 해결하려면 두 개의 캐스케이드 볼륨에 대한 일정을 수정하여 각 대상이 소스에서 전송을 완료한 후에 SnapMirror 전송을 시작하도록 합니다.

보호 관계 관리 및 모니터링

Active IQ Unified Manager 사용하면 보호 관계를 만들고, 관리되는 클러스터에서 SnapMirror 및 SnapVault 관계를 모니터링하고 문제를 해결하고, 데이터가 덮어쓰여지거나 손실된 경우 데이터를 복원할 수 있습니다.

SnapMirror 작업에는 두 가지 복제 유형이 있습니다.

- 비동기

기본 볼륨에서 보조 볼륨으로의 복제는 일정에 따라 결정됩니다.

- 동기식

복제는 기본 볼륨과 보조 볼륨에서 동시에 수행됩니다.

최대 10개의 보호 작업을 성능 저하 없이 동시에 수행할 수 있습니다. 11~30개의 작업을 동시에 실행하면 성능 저하가 발생할 수 있습니다. 30개 이상의 작업을 동시에 실행하는 것은 권장되지 않습니다.

볼륨 보호 상태 보기

데이터 보호 페이지는 단일 클러스터 또는 데이터 센터의 모든 클러스터에 대한 모든 보호 볼륨의 데이터 보호 세부 정보를 전체적으로 보여줍니다.

단계

1. 왼쪽 탐색 창에서 *대시보드*를 클릭합니다.
2. 모니터링되는 모든 클러스터에 대한 데이터 보호 상태를 볼지 또는 단일 클러스터에 대한 데이터 보호 상태를 볼지에 따라 *모든 클러스터*를 선택하거나 드롭다운 메뉴에서 단일 클러스터를 선택합니다.
3. 데이터 보호 패널 상단에 있는 오른쪽 화살표를 클릭하세요. 데이터 보호 페이지가 표시됩니다.

데이터 센터에서 단일 클러스터를 선택했는지 아니면 모든 클러스터를 선택했는지에 따라 이 페이지에는 스냅샷 복사본이나 SnapMirror 정책으로 보호되는 볼륨의 데이터 보호 상태가 표시되고, 보호되지 않는 볼륨의 수도 표시됩니다.

개별 클러스터 목록에서 클러스터를 선택하면 해당 클러스터의 보호된 볼륨에 대한 스냅샷 보호 및 SnapMirror 관계 상태가 표시됩니다.

이 페이지에서 이벤트를 클릭하면 이벤트 세부 정보 페이지로 이동합니다. 모두 보기 링크를 클릭하면 이벤트 관리 인벤토리 페이지에서 모든 활성 보호 이벤트를 볼 수 있습니다. 마우스를 올려 놓으면 각각의 카운트와 범례를 볼 수 있습니다. 클릭할 수 있습니다:

- 보호되지 않은 볼륨과 스냅샷 복사본으로 보호된 볼륨에 대한 막대형 차트를 통해 볼륨 페이지로 이동하여 세부 정보를 볼 수 있습니다.
- 모든 관계에 대한 막대형 차트는 관계 페이지로 이동하며, 여기서 세부 정보는 소스 클러스터별로 필터링됩니다.

스냅샷 복사본으로 보호되는 볼륨의 보호 상태 보기

스냅샷 복사본 개요: 스냅샷 복사본으로 보호되는 볼륨에 대한 개요입니다.예:

- 스냅샷 복사본으로 보호되는 볼륨과 보호되지 않는 볼륨의 총 수입입니다.
- 스냅샷 복사본에 대한 예약 공간을 사용하거나 초과하는 볼륨의 총 수입입니다.

*스냅샷 사본 분석*에서는 다음 정보를 자세히 설명합니다.

- 최근 24시간 동안 발생한 이벤트를 포함하여 스냅샷 사본의 개별 이벤트입니다.
- 스냅샷 복사본으로 보호되는 볼륨과 보호되지 않는 볼륨에 대한 자세한 차트입니다.
- 예약된 스냅샷 복사 용량을 사용 중이거나, 사용하지 않거나, 위반하는 볼륨입니다.
- 볼륨 카운트의 분할은 스냅샷 복사본의 수를 기준으로 합니다.

스냅샷 복사본에 대한 주의 사항

- 스냅샷 복사본으로 보호되는 볼륨을 계산할 때는 소스 볼륨과 대상 볼륨을 모두 고려합니다.
- 반환된 스냅샷 복사본 수는 온라인 상태이고 사용 가능한 볼륨에만 해당됩니다.
- 스냅샷 복사본 수에 대한 그래프 범위는 동적입니다. 선택한 클러스터에 있는 스냅샷 수를 기반으로 생성됩니다.
- 볼륨을 보호된 것으로 간주하려면 볼륨의 스냅샷 복사 일정을 활성화해야 합니다.

- 스냅샷 복사본을 위한 예약 공간 값은 사용된 디스크 공간의 양을 확인하거나 하나 이상의 스냅샷 복사본이 삭제된 경우 회수할 수 있는 공간을 계산하는 데 중요합니다.

SnapMirror 관계에 대한 보호 상태 보기

- SnapMirror 개요*: SnapMirror 정책으로 보호되는 볼륨에 대한 개요입니다. 예:
- 볼륨 SnapMirror 관계, 스토리지 VM 재해 복구(SVM-DR) 및 이들의 조합 등 각 SnapMirror 정책에 의해 보호되는 볼륨의 수입입니다.
- 지연 상태를 기준으로 복구 지점 목표(RPO) 지연이 발생한 SnapMirror 관계의 총 수입입니다.
- SnapMirror 분석*에서는 다음 정보를 자세히 설명합니다.
- SnapMirror 관계에 대해 발생한 개별 이벤트(지난 24시간 동안 발생한 이벤트 포함)
- 각 유형의 SnapMirror 정책으로 보호되는 볼륨 수입입니다.
- 비동기 미러, 비동기 볼트, 비동기 미러 볼트, StricxtSync, SnapMirror 활성 동기화 일관성 그룹 및 동기화와 같은 SnapMirror 관계 유형으로 보호되는 관계의 수입입니다.
- 건강한 관계와 건강하지 못한 관계의 수.
- 볼륨 관계 카운트의 분해. RPO 지연 시간 및 상태에 따라 차트를 전환할 수 있습니다.
- .
- 관리되지 않는 관계에 대한 지연 임계값. 설정 아이콘을 클릭할 수 있습니다() 지연 임계값 설정을 구성합니다. 자세한 내용은 다음을 참조하세요. "[관리되지 않는 보호 관계에 대한 지연 임계값 설정 구성](#)".

SnapMirror 관계에 대한 주의 사항

- SnapMirror 관계를 계산할 때는 읽기 및 쓰기가 활성화된 소스 볼륨을 계산합니다. 대상 볼륨과 루트 볼륨은 고려되지 않습니다.
- SnapMirror 관계의 경우 소스 클러스터에 대한 이벤트가 표시됩니다.
- SnapMirror 관계 수에는 동일하거나 다른 클러스터에 소스와 대상이 있는 볼륨 수가 포함됩니다.
- 데이터 복제에서 RPO 지연의 지연 기간은 SnapMirror 관계에 따라 결정됩니다. 상태는 다음과 같이 분류됩니다. `ok`, `warning`, 또는 `error`, 관계 임계값 설정을 기반으로 합니다. 상태를 살펴보면 매개변수가 예상대로 작동하는지, 아니면 문제를 해결해야 하는지 확인할 수 있습니다.
- 볼륨에 여러 개의 SnapMirror 관계가 있는 경우 각 관계 유형은 RPO 지연에 계산됩니다.
- 소스와 대상 간의 데이터 복제에 문제가 있는 경우(예: 관계가 끊어진 경우) 볼륨 관계는 정상적이지 않은 것으로 간주됩니다.

MetroCluster 구성으로 보호되는 클러스터 보기

데이터 보호 페이지의 * MetroCluster 보호* 패널에는 사이트에서 FC 또는 IP 구성을 통해 MetroCluster 로 보호되거나 보호되지 않는 클러스터 수가 표시됩니다. 이 패널의 막대형 차트를 클릭하면 클러스터 페이지로 이동하며, 여기서는 보호된 클러스터와 보호되지 않은 클러스터를 기준으로 클러스터 세부 정보가 필터링됩니다. MetroCluster 구성 모니터링에 대한 정보는 다음을 참조하세요. "[MetroCluster 구성 모니터링](#)".

볼륨 보호 관계 보기

관계: 모든 관계 보기와 볼륨 관계 페이지에서 기존 볼륨 SnapMirror 및 SnapVault 관계의 상태를 볼 수 있습니다. 또한 전송 및 지연 상태, 소스 및 대상 세부 정보, 일정 및 정책 정보 등을

포함하여 보호 관계에 대한 세부 정보를 검토할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이 페이지에서 관계 명령을 시작할 수도 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 관계 > *모든 관계*를 선택합니다.

관계: 모든 관계 보기가 표시됩니다.

3. 볼륨 보호 세부 정보를 보려면 다음 방법 중 하나를 선택하세요.

- 모든 볼륨 관계에 대한 최신 정보를 보려면 기본 모든 관계 페이지에 머물러 있습니다.
- 특정 기간 동안의 볼륨 전송 추세에 대한 자세한 정보를 보려면 보기 메뉴에서 관계: 지난 1개월 전송 상태 보기를 선택하세요.
- 일별 볼륨 전송 활동에 대한 자세한 정보를 보려면 보기 메뉴에서 관계: 지난 1개월 전송률 보기를 선택하세요.



볼륨 전송 뷰는 비동기 관계에 있는 볼륨에 대한 정보만 표시합니다. 동기 관계에 있는 볼륨은 표시되지 않습니다.

일관성 그룹 관계에서 **LUN** 모니터링

ONTAP 환경이 LUN을 사용하여 애플리케이션을 보호하기 위해 SnapMirror Active Sync를 지원하는 경우 Active IQ Unified Manager 에서 해당 LUN을 보고 모니터링할 수 있습니다.

SnapMirror Active Sync는 SAN 환경에서 장애 조치 시 RTO(복구 시간 목표)를 0으로 보장합니다. SnapMirror 활성 동기화를 지원하는 일반적인 배포에서 볼륨의 LUN은 일관성 그룹 관계로 보호됩니다.

이러한 기본 및 보조 LUN은 복합 LUN이거나 동일한 UUID와 일련 번호를 가진 복제 LUN 쌍입니다. I/O 작업(읽기와 쓰기 모두)은 이러한 복합 LUN의 소스 및 대상 사이트에서 다중화되어 투명성을 보장합니다.

복합 LUN을 보려면 일관성 그룹 관계에 속하는 LUN이 있는 기본 클러스터와 보조 클러스터를 모두 Unified Manager에 추가하고 검색해야 합니다. iSCSI 및 FCP LUN만 지원됩니다.

SnapMirror Active Sync에 대한 정보는 다음을 참조하세요. "[SnapMirror Active Sync\(이전 SM-BC\)에 대한 ONTAP 9 설명서](#)".

사용자 환경에서 복합 LUN을 보려면 다음 단계를 따르세요.

단계

1. 왼쪽 탐색 창에서 저장소 > *LUN*을 클릭합니다.
2. 보기 메뉴에서 관계 > *모든 LUN*을 선택합니다.

관계: 모든 LUN 보기가 표시됩니다.

LUN 이름, 볼륨, LUN을 호스팅하는 스토리지 VM, 클러스터, 일관성 그룹, 파트너 LUN 등의 LUN 세부 정보를 볼 수 있습니다. 각 구성 요소를 클릭하면 자세한 보기로 이동할 수 있습니다. 일관성 그룹을 클릭하면 관계 페이지로 이동합니다.

파트너 LUN을 클릭하면 파트너 LUN이 호스팅된 스토리지 VM의 스토리지 VM 세부 정보 페이지의 SAN 탭에서 해당 구성 세부 정보를 볼 수 있습니다. 파트너 LUN의 개시자, 개시자 그룹 및 기타 측면과 같은 정보가 표시됩니다.

사용자 환경의 보호된 LUN에 대한 보고서 정렬, 필터링, 생성 및 업로드와 같은 표준 그리드 수준 기능을 수행할 수 있습니다.

Health: All Volumes 보기에서 SnapVault 보호 관계를 만듭니다.

상태: 모든 볼륨 보기를 사용하면 동일한 스토리지 VM에 있는 하나 이상의 볼륨에 대한 SnapVault 관계를 만들어 보호 목적으로 데이터 백업을 활성화할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

다음의 경우에는 보호 메뉴가 표시되지 않습니다.

- RBAC 설정에서 이 작업이 허용되지 않는 경우(예: 운영자 권한만 있는 경우)
- 볼륨 ID를 알 수 없는 경우: 예를 들어 클러스터 간 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 상태: 모든 볼륨 보기에서 보호하려는 볼륨을 선택하고 *보호*를 클릭합니다.

또는 동일한 스토리지 가상 머신(SVM)에서 여러 보호 관계를 생성하려면 상태: 모든 볼륨 보기에서 하나 이상의 볼륨을 선택하고 도구 모음에서 *보호*를 클릭합니다.

3. 메뉴에서 * SnapVault*를 선택합니다.

보호 구성 대화 상자가 시작됩니다.

4. * SnapVault* 탭을 보고 보조 볼륨 정보를 구성하려면 * SnapVault*를 클릭하세요.
5. *고급*을 클릭하여 필요에 따라 중복 제거, 압축, 자동 증가 및 공간 보장을 설정한 다음 *적용*을 클릭합니다.
6. * SnapVault* 탭에서 대상 정보 영역과 관계 설정 영역을 작성합니다.
7. *적용*을 클릭하세요.

건강: 모든 볼륨 보기로 돌아갑니다.

8. 상태: 모든 볼륨 보기 상단에 있는 보호 구성 작업 링크를 클릭합니다.

보호 관계를 하나만 만드는 경우 작업 세부 정보 페이지가 표시됩니다. 그러나 보호 관계를 두 개 이상 만드는 경우 보호 작업과 관련된 모든 작업의 필터링된 목록이 표시됩니다.

9. 다음 중 하나를 수행하세요.

- 작업이 하나뿐인 경우 *새로 고침*을 클릭하여 보호 구성 작업과 관련된 작업 목록과 작업 세부 정보를 업데이트하고 작업이 완료되는 시점을 확인합니다.
- 두 개 이상의 작업이 있는 경우:
 - i. 작업 목록에서 작업을 클릭하세요.
 - ii. *새로 고침*을 클릭하면 보호 구성 작업과 관련된 작업 목록과 작업 세부 정보가 업데이트되고 작업이 완료되는 시점을 확인할 수 있습니다.
 - iii. 뒤로 버튼을 사용하여 필터링된 목록으로 돌아가서 다른 일자리를 확인하세요.

볼륨/상태 세부 정보 페이지에서 **SnapVault** 보호 관계를 만듭니다.

볼륨/상태 세부 정보 페이지를 사용하여 SnapVault 관계를 생성하면 볼륨의 보호 목적으로 데이터 백업이 활성화됩니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 이 작업을 수행하려면 워크플로 자동화를 설정해야 합니다.

다음의 경우에는 보호 메뉴가 표시되지 않습니다.

- RBAC 설정에서 이 작업이 허용되지 않는 경우(예: 운영자 권한만 있는 경우)
- 볼륨 ID를 알 수 없는 경우: 예를 들어 클러스터 간 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우

단계

1. 볼륨/상태 세부 정보 페이지의 보호 탭에서 보호하려는 토폴로지 보기의 볼륨을 마우스 오른쪽 버튼으로 클릭합니다.
2. 메뉴에서 보호 > * SnapVault*를 선택합니다.

보호 구성 대화 상자가 시작됩니다.

3. * SnapVault* 탭을 보고 보조 리소스 정보를 구성하려면 * SnapVault*를 클릭하세요.
4. *고급*을 클릭하여 필요에 따라 중복 제거, 압축, 자동 증가 및 공간 보장을 설정한 다음 *적용*을 클릭합니다.
5. 보호 구성 대화 상자에서 대상 정보 영역과 관계 설정 영역을 작성합니다.
6. *적용*을 클릭하세요.

볼륨/상태 세부 정보 페이지로 돌아갑니다.

7. 볼륨/상태 세부 정보 페이지 상단에 있는 보호 구성 작업 링크를 클릭합니다.

작업 세부 정보 페이지가 표시됩니다.

8. *새로 고침*을 클릭하면 보호 구성 작업과 관련된 작업 목록과 작업 세부 정보가 업데이트되고 작업이 완료되는 시점을 확인할 수 있습니다.

작업이 완료되면 새로운 관계가 볼륨/상태 세부 정보 페이지 토폴로지 보기에 표시됩니다.

Health: All Volumes 보기에서 SnapMirror 보호 관계를 만듭니다.

Health: All Volumes 보기를 사용하면 동일한 스토리지 VM에서 두 개 이상의 볼륨을 선택하여 한 번에 여러 SnapMirror 보호 관계를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

다음의 경우에는 보호 메뉴가 표시되지 않습니다.

- RBAC 설정에서 이 작업이 허용되지 않는 경우(예: 운영자 권한만 있는 경우)
- 볼륨 ID를 알 수 없는 경우: 예를 들어 클러스터 간 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우

단계

1. 상태: 모든 볼륨 보기에서 보호하려는 볼륨을 선택합니다.

또는 동일한 SVM에서 여러 보호 관계를 생성하려면 상태: 모든 볼륨 보기에서 하나 이상의 볼륨을 선택하고 도구 모음에서 보호 > * SnapMirror*를 클릭합니다.

보호 구성 대화 상자가 표시됩니다.

2. * SnapMirror* 탭을 보고 대상 정보를 구성하려면 * SnapMirror*를 클릭하세요.
3. 필요에 따라 *고급*을 클릭하여 공간 보장을 설정한 다음 *적용*을 클릭합니다.
4. * SnapMirror* 탭에서 대상 정보 영역과 관계 설정 영역을 작성합니다.
5. *적용*을 클릭하세요.

건강: 모든 볼륨 보기로 돌아갑니다.

6. 상태: 모든 볼륨 보기 상단에 있는 보호 구성 작업 링크를 클릭합니다.

보호 관계를 하나만 만드는 경우 작업 세부 정보 페이지가 표시됩니다. 그러나 보호 관계를 두 개 이상 만드는 경우 보호 작업과 관련된 모든 작업 목록이 표시됩니다.

7. 다음 중 하나를 수행하세요.

- 작업이 하나뿐인 경우 *새로 고침*을 클릭하여 보호 구성 작업과 관련된 작업 목록과 작업 세부 정보를 업데이트하고 작업이 완료되는 시점을 확인합니다.
- 두 개 이상의 작업이 있는 경우:
 - i. 작업 목록에서 작업을 클릭하세요.
 - ii. *새로 고침*을 클릭하면 보호 구성 작업과 관련된 작업 목록과 작업 세부 정보가 업데이트되고 작업이 완료되는 시점을 확인할 수 있습니다.
 - iii. 뒤로 버튼을 사용하여 필터링된 목록으로 돌아가서 다른 일자리를 확인하세요.

구성 중에 지정한 대상 SVM이나 고급 설정에서 활성화한 옵션에 따라 결과 SnapMirror 관계는 여러 가지 가능한 변형 중 하나가 될 수 있습니다.

- 소스 볼륨과 동일하거나 더 최신 버전의 ONTAP 에서 실행되는 대상 SVM을 지정한 경우 블록 복제 기반 SnapMirror 관계가 기본 결과입니다.
- 소스 볼륨과 동일하거나 더 최신 버전의 ONTAP 에서 실행되는 대상 SVM을 지정했지만 고급 설정에서 버전 유연한 복제를 활성화한 경우, 버전 유연한 복제를 사용하는 SnapMirror 관계가 생성됩니다.
- 소스 볼륨보다 이전 버전의 ONTAP 에서 실행되는 대상 SVM을 지정하고, 이전 버전이 버전 유연한 복제를 지원하는 경우, 버전 유연한 복제를 지원하는 SnapMirror 관계가 자동으로 생성됩니다.

볼륨/상태 세부 정보 페이지에서 **SnapMirror** 보호 관계를 만듭니다.

볼륨/상태 세부 정보 페이지를 사용하여 SnapMirror 관계를 생성하면 보호 목적으로 데이터 복제가 활성화됩니다. SnapMirror 복제를 사용하면 소스 볼륨에서 데이터가 손실된 경우 대상 볼륨에서 데이터를 복원할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

다음의 경우에는 보호 메뉴가 표시되지 않습니다.

- RBAC 설정에서 이 작업이 허용되지 않는 경우(예: 운영자 권한만 있는 경우)
- 볼륨 ID를 알 수 없는 경우: 예를 들어 클러스터 간 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우

최대 10개의 보호 작업을 성능 저하 없이 동시에 수행할 수 있습니다. 11~30개의 작업을 동시에 실행하면 성능 저하가 발생할 수 있습니다. 30개 이상의 작업을 동시에 실행하는 것은 권장되지 않습니다.

단계

1. 볼륨/상태 세부 정보 페이지의 보호 탭에서 토폴로지 보기에서 보호하려는 볼륨의 이름을 마우스 오른쪽 버튼으로 클릭합니다.
2. 메뉴에서 보호 > * SnapMirror*를 선택합니다.

보호 구성 대화 상자가 표시됩니다.

3. * SnapMirror* 탭을 보고 대상 정보를 구성하려면 * SnapMirror*를 클릭하세요.
4. 필요에 따라 *고급*을 클릭하여 공간 보장을 설정한 다음 *적용*을 클릭합니다.
5. 보호 구성 대화 상자에서 대상 정보 영역과 관계 설정 영역을 작성합니다.
6. *적용*을 클릭하세요.

볼륨/상태 세부 정보 페이지로 돌아갑니다.

7. 볼륨/상태 세부 정보 페이지 상단에 있는 보호 구성 작업 링크를 클릭합니다.

해당 직무의 과제와 세부 사항은 직무 세부 정보 페이지에 표시됩니다.

8. 작업 세부 정보 페이지에서 *새로 고침*을 클릭하면 보호 구성 작업과 관련된 작업 목록과 작업 세부 정보가 업데이트되고 작업이 완료되는 시점을 확인할 수 있습니다.
9. 작업이 완료되면 브라우저에서 뒤로*를 클릭하여 *볼륨/상태 세부 정보 페이지로 돌아갑니다.

새로운 관계는 볼륨/상태 세부 정보 페이지 토폴로지 보기에 표시됩니다.

구성 중에 지정한 대상 SVM이나 고급 설정에서 활성화한 옵션에 따라 결과 SnapMirror 관계는 여러 가지 가능한 변형 중 하나가 될 수 있습니다.

- 소스 볼륨과 동일하거나 더 최신 버전의 ONTAP 에서 실행되는 대상 SVM을 지정한 경우 블록 복제 기반 SnapMirror 관계가 기본 결과입니다.
- 소스 볼륨과 동일하거나 더 최신 버전의 ONTAP 에서 실행되는 대상 SVM을 지정했지만 고급 설정에서 버전 유연한 복제를 활성화한 경우, 버전 유연한 복제를 사용하는 SnapMirror 관계가 생성됩니다.
- 이전 버전의 ONTAP 에서 실행되는 대상 SVM을 지정하거나 소스 볼륨보다 상위 버전이고 이전 버전이 버전 유연한 복제를 지원하는 경우 버전 유연한 복제를 지원하는 SnapMirror 관계가 자동으로 생성됩니다.

버전에 따라 유연한 복제를 통해 **SnapMirror** 관계 생성

버전에 따라 유연한 복제를 통해 SnapMirror 관계를 만들 수 있습니다. 버전에 유연한 복제를 사용하면 소스 및 대상 볼륨이 서로 다른 ONTAP 버전에서 실행되는 경우에도 SnapMirror 보호를 구현할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.
- 소스 및 대상 SVM에는 각각 SnapMirror 라이선스가 활성화되어 있어야 합니다.
- 소스 및 대상 SVM은 각각 버전 유연한 복제를 지원하는 ONTAP 소프트웨어 버전에서 실행되어야 합니다.

버전 유연한 복제 기능을 갖춘 SnapMirror 사용하면 모든 스토리지가 하나의 ONTAP 버전으로 실행되지 않는 이기종 스토리지 환경에서도 SnapMirror 보호 기능을 구현할 수 있습니다. 그러나 버전 유연한 복제 기능을 갖춘 SnapMirror 에서 수행되는 미리 작업은 기존 블록 복제 SnapMirror 에서보다 빠르게 실행되지 않습니다.

단계

1. 보호하려는 볼륨에 대한 보호 구성 대화 상자를 표시합니다.

- 볼륨/상태 세부 정보 페이지의 보호 탭을 보고 있는 경우 보호하려는 볼륨의 이름이 있는 토폴로지 보기에서 마우스 오른쪽 버튼을 클릭하고 메뉴에서 보호 > * SnapMirror*를 선택합니다.
- 상태: 모든 볼륨 보기를 보고 있는 경우 보호하려는 볼륨을 찾아 마우스 오른쪽 버튼을 클릭한 다음 메뉴에서 보호 > * SnapMirror*를 선택합니다. 보호 구성 대화 상자가 표시됩니다.

2. * SnapMirror*를 클릭하면 * SnapMirror* 탭을 볼 수 있습니다.

3. 보호 구성 대화 상자에서 대상 정보 영역과 관계 설정 영역을 작성합니다.

보호하고 있는 소스 볼륨보다 이전 버전의 ONTAP 에서 실행되는 대상 SVM을 지정하고 해당 이전 버전이 버전 유연한 복제를 지원하는 경우, 이 작업은 SnapMirror 버전 유연한 복제로 자동으로 구성합니다.

4. 소스 볼륨과 동일한 ONTAP 버전에서 실행되는 대상 SVM을 지정했지만 SnapMirror 버전 유연한 복제로 구성하려는 경우 *고급*을 클릭하여 버전 유연한 복제를 활성화한 다음 *적용*을 클릭합니다.

5. *적용*을 클릭하세요.

볼륨/상태 세부 정보 페이지로 돌아갑니다.

6. 볼륨/상태 세부 정보 페이지 상단에 있는 보호 구성 작업 링크를 클릭합니다.

작업의 과제와 세부 정보는 작업 세부 정보 페이지에 표시됩니다.

7. 작업 세부 정보 페이지에서 *새로 고침*을 클릭하면 보호 구성 작업과 관련된 작업 목록과 작업 세부 정보가 업데이트되고 작업이 완료되는 시점을 확인할 수 있습니다.

8. 작업이 완료되면 브라우저에서 뒤로*를 클릭하여 *볼륨/상태 세부 정보 페이지로 돌아갑니다.

새로운 관계는 볼륨/상태 세부 정보 페이지 토폴로지 보기에 표시됩니다.

백업 옵션이 있는 버전 유연한 복제를 통해 **SnapMirror** 관계 생성

버전에 따라 유연한 복제 및 백업 옵션 기능을 통해 SnapMirror 관계를 만들 수 있습니다. 백업 옵션 기능을 사용하면 SnapMirror 보호를 구현하고 대상 위치에 여러 버전의 백업 사본을 보관할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.
- 소스 및 대상 SVM에는 각각 SnapMirror 라이선스가 활성화되어 있어야 합니다.
- 소스 및 대상 SVM에는 각각 SnapVault 라이선스가 활성화되어 있어야 합니다.
- 소스 및 대상 SVM은 각각 버전 유연한 복제를 지원하는 ONTAP 소프트웨어 버전에서 실행되어야 합니다.

SnapMirror 백업 옵션 기능으로 구성하면 볼륨 장애 조치 기능과 같은 SnapMirror 재해 복구 기능으로 데이터를 보호하고 동시에 다중 백업 사본 보호와 같은 SnapVault 기능도 제공할 수 있습니다.

단계

1. 보호하려는 볼륨에 대한 보호 구성 대화 상자를 표시합니다.
 - 볼륨/상태 세부 정보 페이지의 보호 탭을 보고 있는 경우 토폴로지 보기에서 보호하려는 볼륨의 이름을 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 보호 > * SnapMirror*를 선택합니다.
 - 상태: 모든 볼륨 보기를 보고 있는 경우 보호하려는 볼륨을 찾아 마우스 오른쪽 버튼을 클릭한 다음 메뉴에서 보호 > * SnapMirror*를 선택합니다. 보호 구성 대화 상자가 표시됩니다.
2. * SnapMirror*를 클릭하면 * SnapMirror* 탭을 볼 수 있습니다.
3. 보호 구성 대화 상자에서 대상 정보 영역과 관계 설정 영역을 작성합니다.
4. 고급*을 클릭하면 *고급 대상 설정 대화 상자가 표시됩니다.
5. 버전-유연한 복제 확인란이 아직 선택되어 있지 않으면 지금 선택하세요.
6. 백업 옵션 기능을 활성화하려면 백업 옵션 사용 확인란을 선택한 다음 *적용*을 클릭합니다.
7. *적용*을 클릭하세요.

볼륨/상태 세부 정보 페이지로 돌아갑니다.

8. 볼륨/상태 세부 정보 페이지 상단에 있는 보호 구성 작업 링크를 클릭합니다.

작업의 과제와 세부 정보는 작업 세부 정보 페이지에 표시됩니다.

9. 작업 세부 정보 페이지에서 *새로 고침*을 클릭하면 보호 구성 작업과 관련된 작업 목록과 작업 세부 정보가 업데이트되고 작업이 완료되는 시점을 확인할 수 있습니다.
10. 작업이 완료되면 브라우저에서 뒤로*를 클릭하여 *볼륨/상태 세부 정보 페이지로 돌아갑니다.

새로운 관계는 볼륨/상태 세부 정보 페이지 토폴로지 보기에 표시됩니다.

목적지 효율성 설정 구성

고급 대상 설정 대화 상자를 사용하여 보호 대상에서 중복 제거, 압축, 자동 증가, 공간 보장과 같은 대상 효율성 설정을 구성할 수 있습니다. 대상 볼륨이나 보조 볼륨의 공간 활용도를 극대화하려는 경우 이러한 설정을 사용합니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

기본적으로 효율성 설정은 SnapVault 관계의 압축 설정을 제외하고 소스 볼륨의 설정과 일치하며, 이 설정은 기본적으로 비활성화되어 있습니다.

단계

1. 구성하려는 관계 유형에 따라 보호 구성 대화 상자에서 * SnapMirror* 탭이나 * SnapVault* 탭을 클릭합니다.
2. 목적지 정보 영역에서 *고급*을 클릭합니다.

고급 대상 설정 대화 상자가 열립니다.

3. 필요에 따라 중복 제거, 압축, 자동 증가 및 공간 보장에 대한 효율성 설정을 활성화하거나 비활성화합니다.
4. 적용*을 클릭하여 선택 사항을 저장하고 *보호 구성 대화 상자*로 돌아갑니다.

SnapMirror 및 SnapVault 일정 만들기

기본 또는 고급 SnapMirror 및 SnapVault 일정을 만들어 소스 또는 기본 볼륨에서 자동 데이터 보호 전송을 활성화할 수 있습니다. 이를 통해 볼륨에서 데이터가 변경되는 빈도에 따라 전송 빈도를 높이거나 낮출 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 보호 구성 대화 상자에서 대상 정보 영역을 이미 완료했어야 합니다.
- 이 작업을 수행하려면 워크플로 자동화를 설정해야 합니다.

단계

1. 보호 구성 대화 상자의 * SnapMirror* 탭 또는 * SnapVault* 탭에서 관계 설정 영역의 일정 만들기 링크를 클릭합니다.

일정 만들기 대화 상자가 표시됩니다.

2. 일정 이름 필드에 일정에 지정할 이름을 입력합니다.
3. 다음 중 하나를 선택하세요.

- 기초적인

기본 간격 스타일 일정을 만들지 여부를 선택하세요.

- 고급의

Cron 스타일 일정을 만들지 여부를 선택하세요.

4. *만들기*를 클릭하세요.

새로운 일정은 SnapMirror 일정 또는 SnapVault 일정 드롭다운 목록에 표시됩니다.

기존 보호 관계에서 보호를 확장하기 위해 계단식 또는 팬아웃 관계를 만듭니다.

기존 관계의 소스 볼륨에서 팬아웃을 만들거나 기존 관계의 대상 볼륨에서 캐스케이드를 만들어 기존 관계의 보호를 확장할 수 있습니다. 한 사이트에서 여러 사이트로 데이터를 복사해야 하거나 추가 백업을 만들어 추가적인 보호를 제공해야 할 때 이 작업을 수행할 수 있습니다.

일관성 그룹을 사용하여 볼륨에 대한 보호를 확장할 수 있습니다. 일관성 그룹은 여러 볼륨을 보관하는 컨테이너로, 모든 볼륨을 하나의 엔티티로 관리할 수 있습니다. Unified Manager의 관계 페이지에서 SnapMirror 활성 동기화 일관성 그룹과 동기 일관성 그룹 관계를 볼 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

단계

1. 보호 > *관계*를 클릭합니다. 또는 볼륨 세부 정보 페이지에서 관계를 볼 수 있습니다.
2. 볼륨 관계 페이지에서 보호를 확장하려는 SnapMirror 관계를 선택합니다.
3. 작업 표시줄에서 *보호 확장*을 클릭합니다.
4. 메뉴에서 소스에서 팬아웃 관계를 생성하는지, 대상에서 캐스케이드 관계를 생성하는지에 따라 소스에서 또는 *대상에서*를 선택합니다.
5. 생성하는 보호 관계 유형에 따라 * SnapMirror 사용* 또는 * SnapVault 사용*을 선택하세요.

보호 구성 대화 상자가 표시됩니다.



이는 통합 관계/볼륨 관계 및 볼륨/상태 세부 정보 페이지에서 달성할 수 있습니다.

6. 보호 구성 대화 상자에 표시된 대로 정보를 완성합니다.

볼륨 관계 페이지에서 보호 관계 편집

기존 보호 관계를 편집하여 최대 전송 속도, 보호 정책 또는 보호 일정을 변경할 수 있습니다. 데이터가 자주 변경되므로 전송에 사용되는 대역폭을 줄이거나 예약된 전송 빈도를 늘리기 위해 관계를 편집할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

선택한 볼륨은 보호 관계 대상이어야 합니다. 소스 볼륨, 로드 공유 볼륨 또는 SnapMirror 또는 SnapVault 관계의 대상이 아닌 볼륨을 선택한 경우 관계를 편집할 수 없습니다.

단계

1. 볼륨 관계 페이지에서 볼륨 목록에서 동일한 SVM에서 관계 설정을 편집하려는 볼륨을 하나 이상 선택한 다음 도구 모음에서 *편집*을 선택합니다.

관계 편집 대화 상자가 표시됩니다.

2. 관계 편집 대화 상자에서 필요에 따라 최대 전송 속도, 보호 정책 또는 보호 일정을 편집합니다.
3. *적용*을 클릭하세요.

변경 사항은 선택한 관계에 적용됩니다.

볼륨/상태 세부 정보 페이지에서 보호 관계 편집

기존 보호 관계를 편집하여 현재 최대 전송 속도, 보호 정책 또는 보호 일정을 변경할 수 있습니다. 데이터가 자주 변경되므로 전송에 사용되는 대역폭을 줄이거나 예약된 전송 빈도를 늘리기 위해 관계를 편집할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설치하고 구성해야 합니다.

선택한 볼륨은 보호 관계 대상이어야 합니다. 소스 볼륨, 로드 공유 볼륨 또는 SnapMirror 또는 SnapVault 관계의 대상이 아닌 볼륨을 선택한 경우 관계를 편집할 수 없습니다.

단계

1. 볼륨/상태 세부 정보 페이지의 보호 탭에서 편집하려는 보호 관계를 토폴로지에서 찾아 마우스 오른쪽 버튼으로 클릭합니다.
2. 메뉴에서 *편집*을 선택하세요.

또는 작업 메뉴에서 관계 > *편집*을 선택하여 현재 세부 정보를 보고 있는 관계를 편집합니다.

관계 편집 대화 상자가 표시됩니다.

3. 관계 편집 대화 상자에서 필요에 따라 최대 전송 속도, 보호 정책 또는 보호 일정을 편집합니다.
4. *적용*을 클릭하세요.

변경 사항은 선택한 관계에 적용됩니다.

전송 효율성을 극대화하기 위해 **SnapMirror** 정책을 만듭니다.

보호 관계에 대한 SnapMirror 전송 우선 순위를 지정하기 위해 SnapMirror 정책을 만들 수

있습니다. SnapMirror 정책을 사용하면 우선 순위를 지정하여 낮은 우선 순위의 전송이 일반 우선 순위의 전송 이후에 실행되도록 예약함으로써 소스에서 목적지로의 전송 효율성을 극대화할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.
- 이 작업에서는 보호 구성 대화 상자에서 대상 정보 영역을 이미 완료했다고 가정합니다.

단계

1. 보호 구성 대화 상자의 * SnapMirror* 탭에서 관계 설정 영역에 있는 정책 만들기 링크를 클릭합니다.

SnapMirror 정책 만들기 대화 상자가 표시됩니다.

2. 정책 이름 필드에 정책에 지정할 이름을 입력합니다.
3. 전송 우선순위 필드에서 정책에 할당하려는 전송 우선순위를 선택합니다.
4. 주석 필드에 정책에 대한 선택적 주석을 입력합니다.
5. *만들기*를 클릭하세요.

새로운 정책이 SnapMirror 정책 드롭다운 목록에 표시됩니다.

전송 효율성을 극대화하기 위해 **SnapVault** 정책을 만듭니다.

SnapVault 전송의 우선순위를 설정하기 위해 새로운 SnapVault 정책을 만들 수 있습니다. 보호 관계에서 1차에서 2차로의 전송 효율성을 극대화하기 위해 정책을 사용합니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.
- 보호 구성 대화 상자에서 대상 정보 영역을 이미 완료했어야 합니다.

단계

1. 보호 구성 대화 상자의 * SnapVault* 탭에서 관계 설정 영역에 있는 정책 만들기 링크를 클릭합니다.

SnapVault 탭이 표시됩니다.

2. 정책 이름 필드에 정책에 지정할 이름을 입력합니다.
3. 전송 우선순위 필드에서 정책에 할당하려는 전송 우선순위를 선택합니다.
4. 선택 사항: 주석 필드에 정책에 대한 주석을 입력합니다.
5. 복제 레이블 영역에서 필요에 따라 복제 레이블을 추가하거나 편집합니다.
6. *만들기*를 클릭하세요.

새 정책이 정책 만들기 드롭다운 목록에 표시됩니다.

볼륨 관계 페이지에서 활성 데이터 보호 전송을 중단합니다.

진행 중인 SnapMirror 복제를 중지하려면 활성 데이터 보호 전송을 중단할 수 있습니다. 기존 전송 이후의 전송에 대해서도 재시작 체크포인트를 지울 수 있습니다. 볼륨 이동 등 다른 작업과 충돌하는 경우 전송을 중단할 수 있습니다.



일관성 그룹으로 보호되는 볼륨 관계는 중단할 수 없습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

다음의 경우에는 중단 동작이 표시되지 않습니다.

- RBAC 설정에서 이 작업이 허용되지 않는 경우(예: 운영자 권한만 있는 경우)
- 볼륨 ID를 알 수 없는 경우: 예를 들어 클러스터 간 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우

기준선 전송에 대한 재시작 체크포인트를 지울 수 없습니다.

단계

1. 하나 이상의 보호 관계에 대한 전송을 중단하려면 볼륨 관계 페이지에서 하나 이상의 볼륨을 선택하고 도구 모음에서 *중단*을 클릭합니다.

전송 중단 대화 상자가 표시됩니다.

2. 기준선 전송이 아닌 전송에 대한 재시작 체크포인트를 지우려면 *체크포인트 지우기*를 선택하세요.
3. *계속*을 클릭하세요.

전송 중단 대화 상자가 닫히고 중단 작업의 상태가 볼륨 관계 페이지 상단에 표시되고 작업 세부 정보에 대한 링크도 함께 표시됩니다.

4. 선택 사항: 세부 정보 보기 링크를 클릭하면 작업 세부 정보 페이지로 이동하여 추가 세부 정보를 확인하고 작업 진행 상황을 볼 수 있습니다.

볼륨/상태 세부 정보 페이지에서 활성 데이터 보호 전송을 중단합니다.

진행 중인 SnapMirror 복제를 중지하려면 활성 데이터 보호 전송을 중단할 수 있습니다. 기존 전송이 아닌 경우 전송에 대한 재시작 체크포인트를 지울 수도 있습니다. 볼륨 이동 등 다른 작업과 충돌하는 경우 전송을 중단할 수 있습니다.



일관성 그룹으로 보호되는 볼륨 관계는 중단할 수 없습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

다음의 경우에는 중단 동작이 표시되지 않습니다.

- RBAC 설정에서 이 작업이 허용되지 않는 경우(예: 운영자 권한만 있는 경우)
- 볼륨 ID를 알 수 없는 경우: 예를 들어 클러스터 간 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우

기준선 전송에 대한 재시작 체크포인트를 지울 수 없습니다.

단계

1. 볼륨/상태 세부 정보 페이지의 보호 탭에서 중단하려는 데이터 전송에 대한 토폴로지 보기의 관계를 마우스 오른쪽 버튼으로 클릭하고 *중단*을 선택합니다.

전송 중단 대화 상자가 표시됩니다.

2. 기준선 전송이 아닌 전송에 대한 재시작 체크포인트를 지우려면 *체크포인트 지우기*를 선택하세요.
3. *계속*을 클릭하세요.

전송 중단 대화 상자가 닫히고 중단 작업 상태가 볼륨/상태 세부 정보 페이지 상단에 작업 세부 정보에 대한 링크와 함께 표시됩니다.

4. 선택 사항: 세부 정보 보기 링크를 클릭하면 작업 세부 정보 페이지로 이동하여 추가 세부 정보를 확인하고 작업 진행 상황을 볼 수 있습니다.
5. 각 작업을 클릭하면 자세한 내용을 볼 수 있습니다.
6. 브라우저의 뒤로 화살표를 클릭하면 볼륨/상태 세부 정보 페이지로 돌아갑니다.

모든 작업이 성공적으로 완료되면 중단 작업이 종료됩니다.

볼륨 관계 페이지에서 보호 관계 중지

볼륨 관계 페이지에서 보호 관계를 중지하여 일시적으로 데이터 전송을 방지할 수 있습니다. 데이터베이스가 포함된 SnapMirror 대상 볼륨의 스냅샷 복사본을 만들고 스냅샷 복사 작업 중에 해당 내용이 안정적인지 확인하려는 경우 관계를 중지할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

다음의 경우에는 정지 동작이 표시되지 않습니다.

- RBAC 설정에서 이 작업이 허용되지 않는 경우(예: 운영자 권한만 있는 경우)
- 볼륨 ID를 알 수 없는 경우(예: 클러스터 간 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우)
- Workflow Automation과 Unified Manager를 페어링하지 않은 경우

단계

1. 하나 이상의 보호 관계에 대한 전송을 중지하려면 볼륨 관계 페이지에서 하나 이상의 볼륨을 선택하고 도구 모음에서 *중지*를 클릭합니다.

정지 대화 상자가 표시됩니다.

2. *계속*을 클릭하세요.

정지 작업의 상태는 볼륨/상태 세부 정보 페이지 상단에 작업 세부 정보에 대한 링크와 함께 표시됩니다.

3. 추가 세부 정보와 작업 진행 상황을 확인하려면 세부 정보 보기 링크를 클릭하세요.
4. 선택 사항: 브라우저의 뒤로 화살표를 클릭하여 볼륨 관계 페이지로 돌아갑니다.

모든 작업이 성공적으로 완료되면 정지 작업이 종료됩니다.

볼륨/상태 세부 정보 페이지에서 보호 관계 중지

보호 관계를 중지하여 일시적으로 데이터 전송을 방지할 수 있습니다. 데이터베이스가 포함된 SnapMirror 대상 볼륨의 스냅샷 복사본을 만들고 스냅샷 복사 중에 해당 내용이 안정적인지 확인하려는 경우 관계를 중지할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

다음의 경우에는 정지 동작이 표시되지 않습니다.

- RBAC 설정에서 이 작업이 허용되지 않는 경우(예: 운영자 권한만 있는 경우)
- 볼륨 ID를 알 수 없는 경우(예: 클러스터 간 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우)
- Workflow Automation과 Unified Manager를 페어링하지 않은 경우

단계

1. 볼륨/상태 세부 정보 페이지의 보호 탭에서 중지하려는 보호 관계에 대한 토폴로지 보기에서 관계를 마우스 오른쪽 버튼으로 클릭합니다.
2. 메뉴에서 *정지*를 선택하세요.
3. 계속하려면 *예*를 클릭하세요.

정지 작업의 상태는 볼륨/상태 세부 정보 페이지 상단에 작업 세부 정보에 대한 링크와 함께 표시됩니다.

4. 추가 세부 정보와 작업 진행 상황을 확인하려면 세부 정보 보기 링크를 클릭하세요.
5. 선택 사항: 브라우저의 뒤로 화살표를 클릭하여 볼륨/상태 세부 정보 페이지로 돌아갑니다.

모든 작업이 성공적으로 완료되면 정지 작업이 종료됩니다.

볼륨 관계 페이지에서 **SnapMirror** 관계 해제

SnapMirror 관계에서 소스 볼륨과 대상 볼륨 간의 데이터 전송을 중지하기 위해 보호 관계를 해제할 수 있습니다. 재해 복구나 애플리케이션 테스트를 위해 데이터를 마이그레이션할 때 관계가 끊어질 수도 있습니다. 대상 볼륨이 읽기/쓰기 볼륨으로 변경됩니다. SnapVault 관계를 끊을 수 없습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

단계

1. 볼륨 관계 페이지에서 데이터 전송을 중지하려는 보호 관계가 있는 볼륨을 하나 이상 선택하고 도구 모음에서 *중단*을 클릭합니다.

관계 끊기 대화 상자가 표시됩니다.

2. 관계를 종료하려면 *계속*을 클릭하세요.
3. 볼륨 관계 페이지에서 관계 상태 열에서 관계가 끊어졌는지 확인합니다.

관계 상태 열은 기본적으로 숨겨져 있으므로 표시/숨기기 열 목록에서 선택해야 할 수도 있습니다.  .

볼륨 관계 페이지에서 보호 관계 제거

볼륨 관계 페이지에서 보호 관계를 제거하면 선택한 소스와 대상 간의 기존 관계를 영구적으로 삭제할 수 있습니다. 예를 들어, 다른 대상을 사용하여 관계를 만들려는 경우가 있습니다. 이 작업을 수행하면 모든 메타데이터가 제거되며 실행 취소할 수 없습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

단계

1. 볼륨 관계 페이지에서 보호 관계를 제거하려는 볼륨을 하나 이상 선택하고 도구 모음에서 *제거*를 클릭합니다.

관계 제거 대화 상자가 표시됩니다.

2. 관계를 제거하려면 *계속*을 클릭하세요.

해당 관계는 볼륨 관계 페이지에서 제거됩니다.

볼륨 관계 페이지에서 정지된 관계에 대한 예약된 전송을 재개합니다.

예약된 전송이 발생하지 않도록 관계를 중지한 후에는 *다시 시작*을 사용하여 예약된 전송을 다시 활성화하여 소스 또는 기본 볼륨의 데이터를 보호할 수 있습니다. 검사점이 있는 경우, 다음에 예정된 검사점에서 검사가 재개됩니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

전송을 재개할 정지된 관계는 최대 10개까지 선택할 수 있습니다.

단계

1. 볼륨 관계 페이지에서 정지된 관계가 있는 볼륨을 하나 이상 선택하고 도구 모음에서 *다시 시작*을 클릭합니다.
2. 다시 시작 대화 상자에서 *계속*을 클릭합니다.

볼륨 관계 페이지로 돌아갑니다.

3. 관련 작업을 보고 진행 상황을 추적하려면 볼륨 관계 페이지 상단에 표시되는 작업 링크를 클릭하세요.
4. 다음 중 하나를 수행하세요.
 - 작업이 하나만 표시되는 경우 작업 세부 정보 페이지에서 *새로 고침*을 클릭하면 보호 구성 작업과 관련된 작업 목록과 작업 세부 정보가 업데이트되고 작업이 완료되는 시점을 확인할 수 있습니다.
 - 두 개 이상의 작업이 표시되는 경우
 - i. 채용정보 페이지에서 세부 정보를 보고 싶은 채용정보를 클릭합니다.
 - ii. 작업 세부 정보 페이지에서 *새로 고침*을 클릭하면 보호 구성 작업과 관련된 작업 목록과 작업 세부 정보가 업데이트되고 작업이 완료되는 시점을 확인할 수 있습니다. 작업이 완료되면 다음에 예정된 전송 간격으로 데이터 전송이 재개됩니다.

볼륨/상태 세부 정보 페이지에서 정지된 관계에 대한 예약된 전송을 재개합니다.

예약된 전송이 발생하지 않도록 관계를 중지한 후 볼륨/상태 세부 정보 페이지에서 *다시 시작*을 사용하여 예약된 전송을 다시 활성화하여 소스 또는 기본 볼륨의 데이터를 보호할 수 있습니다. 검사점이 있는 경우, 다음에 예정된 검사점에서 검사가 재개됩니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

단계

1. 볼륨/상태 세부 정보 페이지의 보호 탭에서 재개하려는 정지된 관계를 토폴로지 보기에서 마우스 오른쪽 버튼으로 클릭합니다.

또는 작업 > 관계 메뉴에서 *다시 시작*을 선택하세요.

2. 다시 시작 대화 상자에서 *계속*을 클릭합니다.

볼륨/상태 세부 정보 페이지로 돌아갑니다.

3. 관련 작업을 보고 진행 상황을 추적하려면 볼륨/상태 세부 정보 페이지 상단에 표시되는 작업 링크를 클릭하세요.
4. 작업 세부 정보 페이지에서 *새로 고침*을 클릭하면 보호 구성 작업과 관련된 작업 목록과 작업 세부 정보가 업데이트되고 작업이 완료되는 시점을 확인할 수 있습니다.

작업이 완료되면 다음에 예정된 전송 간격으로 데이터 전송이 재개됩니다.

볼륨 관계 페이지에서 보호 관계를 초기화하거나 업데이트합니다.

볼륨 관계 페이지에서 새로운 보호 관계에 대한 최초 기준 전송을 수행하거나, 이미 초기화된

관계를 업데이트하여 즉시 전송하기 위해 수동적이고 예약되지 않은 증분 업데이트를 수행할 수 있습니다.



일관성 그룹으로 보호되는 볼륨을 초기화하거나 업데이트할 수 없습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- OnCommand Workflow Automation 설정해야 합니다.

단계

1. 볼륨 관계 페이지에서 볼륨을 마우스 오른쪽 버튼으로 클릭하고 업데이트 또는 초기화하려는 관계가 있는 볼륨을 하나 이상 선택한 다음 도구 모음에서 *초기화/업데이트*를 클릭합니다.

초기화/업데이트 대화 상자가 표시됩니다.

2. 전송 옵션 탭에서 전송 우선순위와 최대 전송 속도를 선택하세요.
3. 소스 스냅샷 복사본*을 클릭한 다음, *스냅샷 복사본 열에서 *기본값*을 클릭합니다.

소스 스냅샷 복사본 선택 대화 상자가 표시됩니다.

4. 기본 스냅샷 복사본을 전송하는 대신 기존 스냅샷 복사본을 지정하려면 *기존 스냅샷 복사본*을 클릭하고 목록에서 스냅샷 복사본을 선택합니다.
5. *제출*을 클릭하세요.

초기화/업데이트 대화 상자로 돌아갑니다.

6. 초기화 또는 업데이트할 소스를 두 개 이상 선택한 경우 기존 스냅샷 복사본을 지정하려는 다음 소스에 대해 *기본값*을 클릭합니다.
7. 초기화 또는 업데이트 작업을 시작하려면 *제출*을 클릭하세요.

초기화 또는 업데이트 작업이 시작되면 볼륨 관계 페이지로 돌아가고, 페이지 상단에 작업 링크가 표시됩니다.

8. 선택 사항: 모든 볼륨의 상태* 보기에서 *작업 보기*를 클릭하여 각 초기화 또는 업데이트 작업의 상태를 추적합니다.
필터링된 작업 목록이 표시됩니다.

9. 선택 사항: 각 작업을 클릭하여 세부 정보를 확인하세요.

10. 선택 사항: 브라우저의 뒤로 화살표를 클릭하여 볼륨 관계 페이지로 돌아갑니다.

모든 작업이 성공적으로 완료되면 초기화 또는 업데이트 작업이 완료됩니다.

볼륨/상태 세부 정보 페이지에서 보호 관계 초기화 또는 업데이트

새로운 보호 관계에 대한 최초 기준 전송을 수행하거나, 이미 초기화된 관계를 업데이트하고 데이터를 즉시 전송하기 위해 수동적이고 예약되지 않은 증분 업데이트를 수행할 수 있습니다.

참고: 일관성 그룹으로 보호되는 볼륨은 초기화하거나 업데이트할 수 없습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- OnCommand Workflow Automation 설정해야 합니다.

단계

1. 볼륨/상태 세부 정보 페이지의 보호 탭에서 초기화하거나 업데이트하려는 보호 관계를 토폴로지에서 찾은 다음 마우스 오른쪽 버튼을 클릭합니다.

2. 메뉴에서 *초기화/업데이트*를 선택합니다.

또는 작업 메뉴에서 관계 > *초기화/업데이트*를 선택하여 현재 세부 정보를 보고 있는 관계를 초기화하거나 업데이트합니다.

초기화/업데이트 대화 상자가 표시됩니다.

3. 전송 옵션 탭에서 전송 우선순위와 최대 전송 속도를 선택하세요.
4. 소스 스냅샷 복사본*을 클릭한 다음, *스냅샷 복사본 열에서 *기본값*을 클릭합니다.

소스 스냅샷 복사본 선택 대화 상자가 표시됩니다.

5. 기본 스냅샷 복사본을 전송하는 대신 기존 스냅샷 복사본을 지정하려면 *기존 스냅샷 복사본*을 클릭하고 목록에서 스냅샷 복사본을 선택합니다.

6. *제출*을 클릭하세요.

초기화/업데이트 대화 상자로 돌아갑니다.

7. 초기화 또는 업데이트할 소스를 두 개 이상 선택한 경우 기존 스냅샷 복사본을 지정하려는 다음 읽기/쓰기 소스에 대해 *기본값*을 클릭합니다.

데이터 보호 볼륨에 대해 다른 스냅샷 복사본을 선택할 수 없습니다.

8. 초기화 또는 업데이트 작업을 시작하려면 *제출*을 클릭하세요.

초기화 또는 업데이트 작업이 시작되면 볼륨/상태 세부 정보 페이지로 돌아가고, 페이지 상단에 작업 링크가 표시됩니다.

9. 선택 사항: 볼륨/상태* 세부 정보 페이지에서 *작업 보기*를 클릭하여 각 초기화 또는 업데이트 작업의 상태를 추적합니다.

필터링된 작업 목록이 표시됩니다.

10. 선택 사항: 각 작업을 클릭하여 세부 정보를 확인하세요.

11. 선택 사항: 브라우저의 뒤로 화살표를 클릭하여 볼륨/상태 세부 정보 페이지로 돌아갑니다.

모든 작업이 성공적으로 완료되면 초기화 또는 업데이트 작업이 완료됩니다.

볼륨 관계 페이지에서 보호 관계를 다시 동기화합니다.

볼륨 관계 페이지에서 소스 볼륨을 비활성화한 이벤트에서 복구하거나 현재 소스를 다른

볼륨으로 변경하려는 경우 관계를 다시 동기화할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.

단계

1. 볼륨 관계 페이지에서 정지된 관계가 있는 볼륨을 하나 이상 선택하고 도구 모음에서 *재동기화*를 클릭합니다.

재동기화 대화 상자가 표시됩니다.

2. 재동기화 옵션 탭에서 전송 우선순위와 최대 전송 속도를 선택합니다.
3. 소스 스냅샷 복사본*을 클릭한 다음, *스냅샷 복사본 열에서 *기본값*을 클릭합니다.

소스 스냅샷 복사본 선택 대화 상자가 표시됩니다.

4. 기본 스냅샷 복사본을 전송하는 대신 기존 스냅샷 복사본을 지정하려면 *기존 스냅샷 복사본*을 클릭하고 목록에서 스냅샷 복사본을 선택합니다.
5. *제출*을 클릭하세요.

다시 동기화 대화 상자로 돌아갑니다.

6. 재동기화할 소스를 두 개 이상 선택한 경우 기존 스냅샷 복사본을 지정하려는 다음 소스에 대해 *기본값*을 클릭합니다.
7. 재동기화 작업을 시작하려면 *제출*을 클릭하세요.

재동기화 작업이 시작되고 볼륨 관계 페이지로 돌아가며 페이지 상단에 작업 링크가 표시됩니다.

8. 선택 사항: 볼륨 관계* 페이지에서 *작업 보기*를 클릭하여 각 재동기화 작업의 상태를 추적합니다.

필터링된 작업 목록이 표시됩니다.

9. 선택 사항: 브라우저의 뒤로 화살표를 클릭하여 볼륨 관계 페이지로 돌아갑니다.

모든 작업이 성공적으로 완료되면 재동기화 작업이 완료됩니다.

볼륨 관계 페이지에서 역방향 보호 관계

재해로 인해 보호 관계의 소스 볼륨이 비활성화되면 소스를 복구하거나 교체하는 동안 대상 볼륨을 읽기/쓰기 볼륨으로 변환하여 데이터를 제공할 수 있습니다. 소스가 다시 데이터를 수신할 수 있게 되면 역방향 재동기화 작업을 사용하여 역방향으로 관계를 설정하고, 소스의 데이터를 읽기/쓰기 대상의 데이터와 동기화할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 워크플로 자동화를 설정해야 합니다.
- 관계는 SnapVault 관계가 아니어야 합니다.

- 보호 관계가 이미 존재해야 합니다.
- 보호 관계는 반드시 끊어져야 합니다.
- 소스와 대상 모두 온라인이어야 합니다.
- 소스는 다른 데이터 보호 볼륨의 대상이어서는 안 됩니다.
- 이 작업을 수행하면 공통 스냅샷 복사본의 데이터보다 최신인 소스의 데이터는 삭제됩니다.
- 역방향 재동기화 관계에서 생성된 정책과 일정은 원래 보호 관계의 정책과 일정과 동일합니다.

정책과 일정이 없으면 생성됩니다.

단계

1. 볼륨 관계 페이지에서 되돌리려는 관계가 있는 볼륨을 하나 이상 선택하고 도구 모음에서 *역방향 재동기화*를 클릭합니다.

역방향 재동기화 대화 상자가 표시됩니다.

2. 역방향 재동기화 대화 상자에 표시된 관계가 역방향 재동기화 작업을 수행하려는 관계인지 확인한 다음, *제출*을 클릭합니다.

역방향 재동기화 작업이 시작되고 볼륨 관계 페이지로 돌아가며 페이지 상단에 작업 링크가 표시됩니다.

3. 선택 사항: 볼륨 관계* 페이지에서 *작업 보기*를 클릭하여 각 역방향 재동기화 작업의 상태를 추적합니다.

이 작업과 관련된 작업의 필터링된 목록이 표시됩니다.

4. 선택 사항: 브라우저의 뒤로 화살표를 클릭하여 볼륨 관계 페이지로 돌아갑니다.

모든 작업이 성공적으로 완료되면 역방향 재동기화 작업이 완료됩니다.

볼륨 및 볼륨/상태 세부 정보 페이지를 사용하여 데이터 복원

볼륨 및 볼륨/상태 세부 정보 페이지의 복원 기능을 사용하면 스냅샷 복사본에서 덮어쓰거나 삭제된 파일, 디렉토리 또는 전체 볼륨을 복원할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.



다음 사항에 유의하세요.

- NTFS 파일 스트림은 복원할 수 없습니다.
- 다음과 같은 경우 복원 옵션을 사용할 수 없습니다.
 - 볼륨 ID를 알 수 없습니다. 예를 들어, 클러스터 간 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우입니다.
 - 볼륨은 SnapMirror 동기 복제에 맞게 구성되었습니다.

단계

1. 왼쪽 탐색 창에서 *저장소 > 볼륨*으로 이동합니다.
2. 볼륨을 선택하고 복원 버튼을 클릭합니다. 또는 볼륨을 클릭하여 *볼륨/상태 세부 정보 > 작업 > 복원*으로 이동합니다. 복원 대화 상자가 표시됩니다. 이 페이지에 대한 정보는 다음을 참조하세요. "[복원 대화 상자](#)".
3. 기본값과 다를 경우 데이터를 복원할 볼륨과 스냅샷 복사본을 선택합니다.
4. 복원하려는 항목(예: 소스 LUN)을 선택합니다.

전체 볼륨을 복원할 수도 있고, 복원할 폴더와 파일을 지정할 수도 있습니다.

5. 선택한 항목을 복원할 위치를 선택합니다. 원래 위치 또는 대체 기존 위치 중에서 선택합니다.
6. 기존 위치를 대체하는 경우 다음 중 하나를 수행하세요.
 - 복원 경로 텍스트 필드에 데이터를 복원할 위치의 경로를 입력한 다음 *디렉토리 선택*을 클릭합니다.
 - *찾아보기*를 클릭하여 디렉토리 찾아보기 대화 상자를 시작하고 다음 단계를 완료하세요.
 - i. 복원할 대상 클러스터, 스토리지 VM(SVM), 볼륨을 선택합니다.
 - ii. 이름 테이블에서 복원해야 하는 디렉토리 이름을 선택합니다.
 - iii. *디렉토리 선택*을 클릭하세요.
7. *복원*을 클릭하세요.

복구 프로세스가 시작됩니다. 복원 프로세스를 완료하기 위해 백엔드에서 작업이 생성됩니다.

8. 작업 진행 상황을 보려면 왼쪽 탐색 창에서 *보호 > 작업*으로 이동하여 작업 목록에서 복원 작업의 상태를 확인하세요.



NDMP 오류로 인해 Cloud Volumes ONTAP HA 클러스터 간 복원 작업이 실패하는 경우 대상 클러스터에 명시적인 AWS 경로를 추가해야 할 수 있습니다. 그래야 대상이 소스 시스템의 클러스터 관리 LIF와 통신할 수 있습니다. NetApp Console 사용하여 이 구성 단계를 수행합니다.

리소스 풀은 무엇입니까?

리소스 풀은 스토리지 관리자가 Unified Manager를 사용하여 파트너 애플리케이션에 백업 관리를 위한 프로비저닝을 제공하기 위해 만든 집계 그룹입니다.

성과, 비용, 물리적 위치 또는 가용성과 같은 속성을 기준으로 리소스를 모을 수 있습니다. 관련 리소스를 풀로 그룹화하면 풀을 모니터링 및 프로비저닝을 위한 단일 단위로 처리할 수 있습니다. 이를 통해 리소스 관리가 간소화되고, 스토리지를 보다 유연하고 효율적으로 사용할 수 있습니다.

보조 스토리지 프로비저닝 중에 Unified Manager는 다음 기준을 사용하여 보호를 위한 리소스 풀에서 가장 적합한 집계를 결정합니다.

- 집계는 데이터 집계(루트 집계가 아님)이며 온라인 상태입니다.
- 집계는 대상 클러스터 노드에 있으며, 해당 노드의 ONTAP 버전은 소스 클러스터 주 버전과 같거나 더 높습니다.
- 집계는 리소스 풀의 모든 집계 중에서 가장 큰 사용 가능한 공간을 가지고 있습니다.
- 대상 볼륨을 프로비저닝한 후, 집계 공간은 집계에 대해 정의된 거의 가득 참 및 거의 초과 할당 임계값(적용 가능한 글로벌 또는 로컬 임계값) 내에 있습니다.

- 대상 노드의 FlexVol 볼륨 수는 플랫폼 제한을 초과해서는 안 됩니다.

리소스 풀 생성

리소스 풀 만들기 대화 상자를 사용하여 프로비저닝 목적으로 집계를 그룹화할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

리소스 풀은 서로 다른 클러스터의 집계를 포함할 수 있지만, 동일한 집계는 서로 다른 리소스 풀에 속할 수 없습니다.

1. 왼쪽 탐색 창에서 보호 > *리소스 풀*을 클릭합니다.
2. *리소스 풀 페이지*에서 *만들기*를 클릭합니다.
3. 리소스 풀 만들기 대화 상자의 지침에 따라 이름과 설명을 입력하고, 만들려는 리소스 풀에 집계를 멤버로 추가합니다.

리소스 풀 편집

리소스 풀 이름과 설명을 변경하고 싶을 때 기존 리소스 풀을 편집할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

편집 버튼은 하나의 리소스 풀이 선택된 경우에만 활성화됩니다. 두 개 이상의 리소스 풀을 선택한 경우 편집 버튼이 비활성화됩니다.

단계

1. 왼쪽 탐색 창에서 보호 > *리소스 풀*을 클릭합니다.
2. 목록에서 리소스 풀 하나를 선택하세요.
3. *편집*을 클릭하세요.

리소스 풀 편집 창이 표시됩니다.

4. 필요에 따라 리소스 풀 이름과 설명을 편집합니다.
5. *저장*을 클릭하세요.

새 이름과 설명이 리소스 풀 목록에 표시됩니다.

리소스 풀 인벤토리 보기

리소스 풀 페이지를 사용하면 리소스 풀 인벤토리를 보고 각 리소스 풀의 남은 용량을 모니터링할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 보호 > *리소스 풀*을 클릭합니다.

리소스 풀 인벤토리가 표시됩니다.

리소스 풀 멤버 추가

리소스 풀은 여러 멤버 집합으로 구성됩니다. 기존 리소스 풀에 집계를 추가하여 보조 볼륨 프로비저닝에 사용할 수 있는 공간을 늘릴 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

한 번에 리소스 풀에 추가할 수 있는 집계 수는 200개 이하입니다. 집계 대화 상자에 표시된 집계는 다른 리소스 풀에 속하지 않습니다.

단계

1. 왼쪽 탐색 창에서 보호 > *리소스 풀*을 클릭합니다.
2. 리소스 풀 목록에서 리소스 풀을 선택하세요.

리소스 풀 구성원은 리소스 풀 목록 아래 영역에 표시됩니다.

3. 리소스 풀 구성원 영역에서 *추가*를 클릭합니다.

집계 대화 상자가 표시됩니다.

4. 하나 이상의 집계를 선택하세요.
5. *추가*를 클릭하세요.

대화 상자가 닫히고 선택한 리소스 풀의 멤버 목록에 집계가 표시됩니다.

리소스 풀에서 집계 제거

기존 리소스 풀에서 집계를 제거할 수 있습니다. 예를 들어, 다른 목적으로 집계를 사용하려는 경우입니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

리소스 풀 멤버는 리소스 풀을 선택한 경우에만 표시됩니다.

단계

1. 왼쪽 탐색 창에서 보호 > *리소스 풀*을 클릭합니다.
2. 멤버 집계를 제거할 리소스 풀을 선택합니다.

멤버 집계 목록은 멤버 창에 표시됩니다.

3. 하나 이상의 집계를 선택하세요.

제거 버튼이 활성화되었습니다.

4. *제거*를 클릭하세요.

경고 대화 상자가 표시됩니다.

5. 계속하려면 *예*를 클릭하세요.

선택한 집계가 멤버 창에서 제거됩니다.

리소스 풀 삭제

더 이상 필요하지 않은 리소스 풀을 삭제할 수 있습니다. 예를 들어, 하나의 리소스 풀에서 여러 다른 리소스 풀로 멤버 집계를 재분배하여 원래 리소스 풀을 더 이상 사용하지 않게 만들 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

삭제 버튼은 하나 이상의 리소스 풀이 선택된 경우에만 활성화됩니다.

단계

1. 왼쪽 탐색 창에서 보호 > *리소스 풀*을 클릭합니다.
2. 삭제하려는 리소스 풀을 선택하세요.
3. *삭제*를 클릭하세요.

리소스 풀이 리소스 풀 목록에서 제거되고 해당 집계가 멤버 목록에서 제거됩니다.

스토리지 VM 재해 복구 보호 관계 모니터링

Active IQ Unified Manager 스토리지 VM 재해 복구 관계의 모니터링을 지원하여 스토리지 VM 수준의 세분성으로 재해 복구를 제공합니다. 스토리지 VM 재해 복구를 통해 스토리지 VM의 구성 볼륨에 있는 데이터를 복구하고 스토리지 VM 구성을 복구할 수 있습니다.

비동기 재해 복구를 제공하기 위해 소스 스토리지 VM에서 대상 스토리지 VM으로 스토리지 VM DR 관계가 생성됩니다. 클러스터 설정에 따라 데이터 볼륨과 함께 스토리지 VM 구성(네트워크 및 프로토콜 구성 제외)의 전체 또는 하위 집합을 복제하도록 선택할 수 있습니다.

저장소 VM 재해 복구 관계가 구성된 후, 하드웨어 장애나 환경 재해로 인해 소스 저장소 VM을 사용할 수 없게 되면 대상 저장소 VM이 시작되어 중단을 최소화하면서 데이터에 액세스할 수 있습니다. 마찬가지로, 소스 스토리지 VM이 사용 가능해지면 대상 스토리지 VM과 다시 동기화되고, 그 후 소스가 다시 시작되어 데이터를 제공합니다. SnapMirror 명령을 사용하여 스토리지 VM 재해 복구 관계를 구성하고 관리할 수 있습니다.

관계 페이지를 사용하여 스토리지 VM 모니터링

인벤토리의 보호 섹션에 있는 관계 페이지에서 스토리지 VM 재해 복구 관계를 모니터링할 수

있습니다. 기본적으로 관계 페이지에는 구성 요소 관계 필터가 적용됨에 따라 최상위 관계만 나열됩니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

필터를 사용하여 스토리지 VM 재해 복구 관계를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 보호 > *관계*를 클릭합니다.

이 페이지에는 볼륨, 일관성 그룹, 스토리지 VM 관계 등 모든 유형의 관계가 표시됩니다.

2. *필터*를 클릭한 다음 *관계 개체 유형*과 *스토리지 VM*을 선택하여 스토리지 VM 재해 복구 관계만 표시합니다.
3. *필터 적용*을 클릭하세요.



모든 보호 관계를 보려면 구성 요소 관계 필터를 지워야 합니다.

이 페이지에는 스토리지 VM 재해 복구 관계만 표시됩니다.

스토리지 **VM** 페이지에서 보호 관계 보기

저장소 VM 페이지를 사용하면 기존 저장소 VM의 재해 복구 관계 상태를 볼 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

또한 전송 및 지연 상태, 소스 및 대상 세부 정보를 포함하여 보호 관계에 대한 세부 정보를 검토할 수 있습니다. 원하는 형식으로 보고서를 예약하거나 기존 보고서를 다운로드할 수 있습니다. 표시/숨기기 버튼을 사용하면 기본적으로 표시되지 않는 보고서에 필요한 열을 추가할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *저장소 VM*을 클릭합니다.
2. 보기 메뉴에서 관계 > *모든 관계*를 선택합니다.

관계: 모든 관계 보기에는 구성된 모든 스토리지 VM이 표시됩니다.

보호 상태에 따라 스토리지 **VM** 보기

인벤토리의 스토리지 VM 페이지를 사용하면 Active IQ Unified Manager 의 모든 스토리지 VM을 보고 보호 상태에 따라 스토리지 VM을 필터링할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

스토리지 VM 보기에 새로운 열인 보호 역할이 추가되어 스토리지 VM이 보호되는지 보호되지 않는지에 대한 정보를 제공합니다.



소스 클러스터가 Active IQ Unified Manager 에 추가되지 않으면 해당 클러스터와 관련된 모든 정보를 그리드에서 사용할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *저장소 VM*을 클릭합니다.
2. 보기 메뉴에서 상태 > *모든 저장소 VM*을 선택합니다.

상태: 모든 스토리지 VM이 표시됩니다.

3. 다음 스토리지 VM 중 하나를 보려면 *필터*를 클릭하세요.

보려면	필터 값
보호된 스토리지 VM	*보호 역할*은 *보호됨*입니다.
보호되지 않은 스토리지 VM	*보호 역할*은 *보호되지 않음*입니다.



보호된 스토리지 VM과 보호되지 않은 스토리지 VM을 동시에 볼 수는 없습니다. 새로운 필터 옵션을 다시 적용하려면 기존 필터를 지워야 합니다.

4. *필터 적용*을 클릭하세요.

저장되지 않은 보기는 필터 선택에 따라 스토리지 VM 재해 복구로 보호되거나 보호되지 않은 모든 스토리지 VM을 표시합니다.

스토리지 **VM** 연결 이해

스토리지 가상 머신(스토리지 VM) 연결은 파트너 애플리케이션에서 리소스 선택 및 보조 볼륨 프로비저닝을 위해 사용되는 소스 스토리지 VM에서 대상 스토리지 VM으로의 매핑입니다.

대상 스토리지 VM이 2차 대상인지 3차 대상인지에 관계없이 소스 스토리지 VM과 대상 스토리지 VM 간에 연결이 생성됩니다. 2차 대상 저장소 VM을 소스로 사용하여 3차 대상 저장소 VM과 연결을 생성할 수 없습니다.

애플리케이션 관리자 또는 스토리지 관리자는 보호 > 스토리지 **VM** 연결 페이지에서 환경의 스토리지 VM 연결을 볼 수 있습니다.

SVM을 연결하는 방법은 세 가지가 있습니다.

- 모든 스토리지 **VM** 연결: 모든 기본 소스 스토리지 VM과 하나 이상의 대상 SVM 간에 연결을 생성할 수 있습니다. 즉, 현재 보호가 필요한 모든 기존 SVM과 향후 생성되는 모든 SVM이 지정된 대상 SVM과 연결됩니다. 예를 들어, 서로 다른 위치에 있는 여러 소스의 애플리케이션을 하나의 위치에 있는 하나 이상의 대상 SVM에 백업하려고 할 수 있습니다.
- 특정 스토리지 **VM** 연결: 특정 소스 스토리지 VM과 하나 이상의 특정 대상 SVM 간에 연결을 생성할 수 있습니다. 예를 들어, 서로 분리된 데이터가 필요한 여러 클라이언트에 스토리지 서비스를 제공하는 경우 이 옵션을 선택하여 특정 소스 스토리지 VM을 해당 클라이언트에만 할당된 특정 대상 스토리지 VM에 연결할 수 있습니다.
- 외부 스토리지 **VM**과 연결: 소스 스토리지 VM과 대상 스토리지 VM의 외부 유연 볼륨 간에 연결을 생성할 수 있습니다.

스토리지 VM 연결 생성

스토리지 가상 머신 연결 만들기 마법사를 사용하면 파트너 보호 애플리케이션이 SnapMirror 및 SnapVault 관계와 함께 사용할 소스 스토리지 VM을 대상 스토리지 VM과 연결할 수 있습니다. 파트너 애플리케이션은 대상 볼륨의 초기 프로비저닝 시 이러한 연결을 사용하여 선택할 리소스를 결정합니다.

시작하기 전에

- 연결하려는 스토리지 VM은 이미 존재해야 합니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

모든 소스 스토리지 VM 및 관계 유형의 경우 각 대상 클러스터에서 하나의 대상 스토리지 VM만 선택할 수 있습니다.

삭제 및 생성 기능을 사용하여 연결을 변경하면 향후 프로비저닝 작업에만 영향을 미칩니다. 기존 대상 볼륨은 이동하지 않습니다.

단계

1. 왼쪽 탐색 창에서 보호 > *저장소 VM 연결*을 클릭합니다.
2. 저장소 **VM** 연결 페이지에서 *만들기*를 클릭합니다.

스토리지 가상 머신 연결 만들기 마법사가 시작됩니다.

3. 다음 소스 중 하나를 선택하세요.

- 어느

기본 스토리지 VM 소스와 하나 이상의 대상 스토리지 VM 간의 연결을 생성하려면 이 옵션을 선택하세요. 즉, 현재 보호가 필요한 모든 기존 스토리지 VM과 향후 생성되는 모든 스토리지 VM이 지정된 대상 스토리지 VM과 연결됩니다. 예를 들어, 서로 다른 위치에 있는 여러 소스의 애플리케이션을 하나의 위치에 있는 하나 이상의 대상 스토리지 VM에 백업하고 싶을 수 있습니다.

- 하나의

하나 이상의 대상 스토리지 VM과 연관된 특정 소스 스토리지 VM을 선택하려면 이 옵션을 선택하세요. 예를 들어, 서로 분리된 데이터가 필요한 여러 클라이언트에 스토리지 서비스를 제공하는 경우 이 옵션을 선택하면 특정 스토리지 VM 소스를 해당 클라이언트에만 할당된 특정 스토리지 VM 대상에 연결할 수 있습니다.

- 없음(외부)

소스 스토리지 VM과 대상 스토리지 VM의 외부 유연 볼륨 간에 연결을 생성하려면 이 옵션을 선택하세요.

4. 만들려는 보호 관계 유형 중 하나 또는 둘 다를 선택하세요.
 - * SnapMirror*
 - * SnapVault*
5. *다음*을 클릭하세요.
6. 하나 이상의 스토리지 VM 보호 대상을 선택하세요.
7. *마침*을 클릭하세요.

스토리지 VM 연결 삭제

소스 및 대상 스토리지 VM 간의 보조 프로비저닝 관계를 제거하기 위해 파트너 애플리케이션의 스토리지 VM 연결을 삭제할 수 있습니다. 예를 들어, 대상 스토리지 VM이 가득 차서 새로운 스토리지 VM 보호 연결을 만들 때 이 작업을 수행할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

최소 하나의 스토리지 VM 연결이 선택될 때까지 삭제 버튼은 비활성화됩니다. 삭제 및 생성 기능을 사용하여 연결을 변경하면 향후 프로비저닝 작업에만 영향을 미치며 기존 대상 볼륨은 이동하지 않습니다.

단계

1. 왼쪽 탐색 창에서 보호 > *저장소 VM 연결*을 클릭합니다.
2. 최소한 하나의 스토리지 VM 연결을 선택하세요.

삭제 버튼이 활성화되었습니다.

3. *삭제*를 클릭하세요.

경고 대화 상자가 표시됩니다.

4. 계속하려면 *예*를 클릭하세요.

선택한 스토리지 VM 연결이 목록에서 제거됩니다.

스토리지 서비스를 지원하기 위한 SVM 및 리소스 풀 요구 사항

스토리지 서비스에 특정한 일부 SVM 연결 및 리소스 풀 요구 사항을 준수하면 파트너 애플리케이션에서의 적합성을 더 잘 보장할 수 있습니다. 예를 들어, 파트너 애플리케이션에서 제공하는 스토리지 서비스에서 보호 토폴로지를 지원하기 위해 Unified Manager에서 SVM을 연결하고 리소스 풀을 만드는 경우입니다.

일부 애플리케이션은 Unified Manager 서버와 협력하여 소스 볼륨과 2차 또는 3차 위치의 보호 볼륨 간에 SnapMirror 또는 SnapVault 백업 보호를 자동으로 구성하고 실행하는 서비스를 제공합니다. 이러한 보호 스토리지 서비스를 지원하려면 Unified Manager를 사용하여 필요한 SVM 연결 및 리소스 풀을 구성해야 합니다.

SnapMirror 소스 또는 SnapVault 기본 볼륨에서 대상 SnapMirror 또는 2차 또는 3차 위치에 있는 SnapVault 백업 볼륨으로의 복제를 포함하여 스토리지 서비스 단일 홈 또는 계단식 보호를 지원하려면 다음 요구 사항을 준수하세요.

- SnapMirror 소스 또는 SnapVault 기본 볼륨이 포함된 SVM과 보조 볼륨 또는 3차 볼륨이 있는 모든 SVM 간에 SVM 연결을 구성해야 합니다.
 - 예를 들어, 소스 볼륨 Vol_A가 SVM_1에 있고 SnapMirror 보조 대상 볼륨 Vol_B가 SVM_2에 있고 3차 SnapVault 백업 볼륨 Vol_C가 SVM_3에 있는 보호 토폴로지를 지원하려면 Unified Manager 웹 UI를 사용하여 SVM_1과 SVM_2 간의 SnapMirror 연결과 SVM_1과 SVM_3 간의 SnapVault 백업 연결을 구성해야 합니다.

이 예에서 SVM_2와 SVM_3 간의 SnapMirror 연결이나 SnapVault 백업 연결은 필요하지 않으며 사용되지 않습니다.

- 소스 볼륨 Vol_A와 SnapMirror 대상 볼륨 Vol_B가 모두 SVM_1에 있는 보호 토폴로지를 지원하려면 SVM_1과 SVM_1 간에 SnapMirror 연결을 구성해야 합니다.

- 리소스 풀에는 연관된 SVM에서 사용할 수 있는 클러스터 집계 리소스가 포함되어야 합니다.

Unified Manager 웹 UI를 통해 리소스 풀을 구성한 다음 파트너 애플리케이션을 통해 스토리지 서비스 2차 대상과 3차 대상 노드를 할당합니다.

어떤 작업이 있나요?

작업은 Unified Manager를 사용하여 모니터링할 수 있는 일련의 작업입니다. 작업과 관련 작업을 보면 작업이 성공적으로 완료되었는지 확인할 수 있습니다.

SnapMirror 및 SnapVault 관계를 생성할 때, 관계 작업(중단, 편집, 정지, 제거, 재개, 재동기화, 역방향 재동기화)을 수행할 때, 데이터 복원 작업을 수행할 때, 클러스터에 로그인할 때 등에서 작업이 시작됩니다.

작업을 시작하면 작업 페이지와 작업 세부 정보 페이지를 사용하여 작업과 관련 작업의 진행 상황을 모니터링할 수 있습니다.

작업 모니터링

작업 페이지를 사용하면 작업 상태를 모니터링하고 스토리지 서비스 유형, 상태, 제출 시간, 완료 시간과 같은 작업 속성을 보고 작업이 성공적으로 완료되었는지 확인할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 보호 > *작업*을 클릭합니다.

작업 페이지가 표시됩니다.

2. 현재 실행 중인 작업의 상태를 확인하려면 상태 열을 확인하세요.
3. 특정 직무에 대한 세부 정보를 보려면 직무 이름을 클릭하세요.

작업 세부 정보 페이지가 표시됩니다.

채용공고 세부정보 보기

작업을 시작한 후 작업 세부 정보 페이지에서 진행 상황을 추적하고 관련 작업에 오류가 있는지 모니터링할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 보호 > *작업*을 클릭합니다.

2. 작업 페이지에서 이름 옆에 있는 작업 이름을 클릭하면 해당 작업과 관련된 작업 목록이 표시됩니다.
3. 작업을 클릭하면 작업 목록 오른쪽에 있는 작업 세부 정보 창과 작업 메시지 창에 추가 정보가 표시됩니다.

작업 중단

작업을 완료하는 데 너무 오랜 시간이 걸리거나, 오류가 너무 많이 발생하거나, 더 이상 필요하지 않은 경우 작업 페이지를 사용하여 작업을 중단할 수 있습니다. 작업의 상태와 유형이 허용하는 경우에만 작업을 중단할 수 있습니다. 실행 중인 모든 작업을 중단할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 보호 > *작업*을 클릭합니다.
2. 작업 목록에서 하나의 작업을 선택한 다음 *중단*을 클릭합니다.
3. 확인 메시지가 나타나면 *예*를 클릭하여 선택한 작업을 중단합니다.

실패한 보호 작업을 다시 시도합니다.

실패한 보호 작업을 수정하기 위한 조치를 취한 후 *다시 시도*를 사용하여 작업을 다시 실행할 수 있습니다. 작업을 다시 시도하면 원래 작업 ID를 사용하여 새 작업이 생성됩니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

한 번에 실패한 작업은 하나만 다시 시도할 수 있습니다. 두 개 이상의 작업을 선택하면 다시 시도 버튼이 비활성화됩니다. 보호 구성 및 보호 관계 작업 유형의 작업만 다시 시도할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 보호 > *작업*을 클릭합니다.
2. 작업 목록에서 실패한 단일 보호 구성 또는 보호 관계 작업 유형 작업을 선택합니다.

다시 시도 버튼이 활성화되었습니다.

3. *다시 시도*를 클릭하세요.

작업이 다시 시작됩니다.

보호 관계 창 및 대화 상자 설명

리소스 풀, SVM 연결, 보호 작업 등 보호 관련 세부 정보를 보고 관리할 수 있습니다. 적절한 상태 임계값 페이지를 사용하여 집계, 볼륨 및 관계에 대한 글로벌 상태 임계값을 구성할 수 있습니다.

리소스 풀 페이지

리소스 풀 페이지에는 기존 리소스 풀과 해당 멤버가 표시되며, 프로비저닝 목적으로 리소스 풀을

생성, 모니터링 및 관리할 수 있습니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 만들다

리소스 풀을 생성하는 데 사용할 수 있는 리소스 풀 생성 대화 상자를 실행합니다.

- 편집하다

사용자가 만든 리소스 풀의 이름과 설명을 편집할 수 있습니다.

- 삭제

하나 이상의 리소스 풀을 삭제할 수 있습니다.

리소스 풀 목록

리소스 풀 목록에는 기존 리소스 풀의 속성이 (표 형식으로) 표시됩니다.

- 자원 풀

리소스 풀의 이름을 표시합니다.

- 설명

리소스 풀을 설명합니다.

- * SnapLock 타입*

리소스 풀의 집계에서 사용되는 SnapLock 유형을 표시합니다. SnapLock 유형에 유효한 값은 규정 준수, 엔터프라이즈 및 비 SnapLock 입니다. 리소스 풀에는 하나의 SnapLock 유형의 집계만 포함될 수 있습니다.

- 총 용량

리소스 풀의 총 용량(MB, GB 등)을 표시합니다.

- 사용 용량

리소스 풀에서 사용되는 공간의 양(MB, GB 등)을 표시합니다.

- 사용 가능한 용량

리소스 풀에서 사용 가능한 공간의 양(MB, GB 등)을 표시합니다.

- 사용된 %

리소스 풀에서 사용되는 공간의 백분율을 표시합니다.

멤버 목록 명령 버튼

멤버 목록 명령 단추를 사용하면 다음 작업을 수행할 수 있습니다.

- 추가하다

리소스 풀에 멤버를 추가할 수 있습니다.

- 삭제

리소스 풀에서 하나 이상의 멤버를 삭제할 수 있습니다.

회원 목록

리소스 풀을 선택하면 멤버 목록에 리소스 풀 멤버와 해당 속성이 (표 형식으로) 표시됩니다.

- 상태

멤버 집계의 현재 상태를 표시합니다. 상태는 중요(Critical)일 수 있습니다. , 오류 () , 경고 () , 또는 일반 () .

- 총계 이름

멤버 집계의 이름을 표시합니다.

- 상태

집계의 현재 상태를 표시합니다. 다음 중 하나일 수 있습니다.

- 오프라인

읽기 또는 쓰기 권한이 허용되지 않습니다.

- 온라인

이 집계에 호스팅된 볼륨에 대한 읽기 및 쓰기 액세스가 허용됩니다.

- 제한된

제한된 작업(패리티 재구성 등)은 허용되지만 데이터 접근은 허용되지 않습니다.

- 생성 중

집계가 생성되고 있습니다.

- 파괴하다

골재가 파괴되고 있습니다.

- 실패한

집계를 온라인으로 가져올 수 없습니다.

- 언

집계가 (일시적으로) 요청을 처리하지 않습니다.

- 일관성 없는

집계가 손상된 것으로 표시되었습니다. 기술 지원팀에 문의하시기 바랍니다.

- 철 제한

진단 도구는 집계하여 실행할 수 없습니다.

- 설치

골재가 장착되는 중입니다.

- 부분적

집계에 대해 하나 이상의 디스크가 발견되었지만 두 개 이상의 디스크가 누락되었습니다.

- 정지 중

집계가 중지됩니다.

- 정지됨

집계가 중지되었습니다.

- 되돌림

집계의 복귀가 완료되었습니다.

- 말 타지 않은

집계가 해제되었습니다.

- 언마운트

집계가 오프라인으로 전환됩니다.

- 알려지지 않은

집계는 발견되었지만 집계 정보는 아직 Unified Manager 서버에서 검색되지 않았습니다.

기본적으로 이 열은 숨겨져 있습니다.

- 무리

집계가 속한 클러스터의 이름을 표시합니다.

- 마디

집계가 있는 노드의 이름을 표시합니다.

- 총 용량

집계의 총 용량(MB, GB 등)을 표시합니다.

- 사용 용량

집계된 공간의 양(MB, GB 등)을 표시합니다.

- 사용 가능한 용량

전체적으로 사용 가능한 공간의 양(MB, GB 등)을 표시합니다.

- 사용된 %

집계에서 사용된 공간의 백분율을 표시합니다.

- 디스크 유형

RAID 구성 유형을 표시합니다. 다음 중 하나일 수 있습니다.

- RAID0: 모든 RAID 그룹은 RAID0 유형입니다.
- RAID4: 모든 RAID 그룹은 RAID4 유형입니다.
- RAID-DP: 모든 RAID 그룹은 RAID-DP 유형입니다.
- RAID-TEC: 모든 RAID 그룹은 RAID-TEC 유형입니다.
- 혼합 RAID: 집계에는 다양한 RAID 유형(RAID0, RAID4, RAID-DP, RAID-TEC)의 RAID 그룹이 포함됩니다. 기본적으로 이 열은 숨겨져 있습니다.

리소스 풀 생성 대화 상자

리소스 풀 만들기 대화 상자를 사용하여 새 리소스 풀의 이름을 지정하고 설명하고 해당 리소스 풀에 집계를 추가하거나 삭제할 수 있습니다.

리소스 풀 이름

텍스트 상자를 사용하면 다음 정보를 추가하여 리소스 풀을 만들 수 있습니다.

리소스 풀 이름을 지정할 수 있습니다.

설명

리소스 풀을 설명할 수 있습니다.

회원들

리소스 풀의 멤버를 표시합니다. 또한, 멤버를 추가하거나 삭제할 수도 있습니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 추가하다

특정 클러스터의 집계를 리소스 풀에 추가할 수 있도록 집계 대화 상자를 엽니다. 여러 클러스터에서 집계를 추가할 수 있지만, 동일한 집계를 두 개 이상의 리소스 풀에 추가할 수는 없습니다.

- 제거하다

리소스 풀에서 선택한 집계를 제거할 수 있습니다.

- 만들다

리소스 풀을 생성합니다. 이 버튼은 리소스 풀 이름이나 설명 필드에 정보가 입력될 때까지 활성화되지 않습니다.

- 취소

변경 사항을 취소하고 리소스 풀 만들기 대화 상자를 닫습니다.

리소스 풀 편집 대화 상자

리소스 풀 편집 대화 상자를 사용하여 기존 리소스 풀의 이름과 설명을 변경할 수 있습니다. 예를 들어, 원래 이름과 설명이 부정확하거나 올바르지 않은 경우, 더 정확하게 변경할 수 있습니다.

텍스트 상자

텍스트 상자를 사용하면 선택한 리소스 풀에 대한 다음 정보를 변경할 수 있습니다.

- 리소스 풀 이름

새로운 이름을 입력할 수 있습니다.

- 설명

새로운 설명을 입력할 수 있습니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 구하다

리소스 풀 이름과 설명에 대한 변경 사항을 저장합니다.

- 취소

변경 사항을 취소하고 리소스 풀 편집 대화 상자를 닫습니다.

집계 대화 상자

집계 대화 상자를 사용하여 리소스 풀에 추가할 집계를 선택할 수 있습니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 추가하다

선택한 집계를 리소스 풀에 추가합니다. 최소한 하나의 집계가 선택될 때까지 추가 버튼은 활성화되지 않습니다.

- 취소

변경 사항을 취소하고 집계 대화 상자를 닫습니다.

집계 목록

집계 목록은 모니터링된 집계의 이름과 속성을 (표 형식으로) 표시합니다.

- 상태

볼륨의 현재 상태를 표시합니다. 상태는 중요(Critical)일 수 있습니다. (❌), 오류 (💡), 경고 (⚠️), 또는 일반(✅).

볼륨에 대해 생성된 이벤트에 대한 자세한 정보를 보려면 포인터를 상태 위로 가져가세요.

- 총계 이름

집계의 이름을 표시합니다.

- 상태

집계의 현재 상태를 표시합니다. 다음 중 하나일 수 있습니다.

- 오프라인

읽기 또는 쓰기 권한이 허용되지 않습니다.

- 제한된

제한된 작업(패리티 재구성 등)은 허용되지만 데이터 접근은 허용되지 않습니다.

- 온라인

이 집계에 호스팅된 볼륨에 대한 읽기 및 쓰기 액세스가 허용됩니다.

- 생성 중

집계가 생성되고 있습니다.

- 파괴하다

골재가 파괴되고 있습니다.

- 실패한

집계를 온라인으로 가져올 수 없습니다.

- 언

집계가 (일시적으로) 요청을 처리하지 않습니다.

- 일관성 없는

집계가 손상된 것으로 표시되었습니다. 기술 지원팀에 문의하시기 바랍니다.

- 철 제한

진단 도구는 집계하여 실행할 수 없습니다.

- 설치

골재가 장착되는 중입니다.

- 부분적

집계에 대해 하나 이상의 디스크가 발견되었지만 두 개 이상의 디스크가 누락되었습니다.

- 정지 중

집계가 중지됩니다.

- 정지됨

집계가 중지되었습니다.

- 되돌림

집계의 복귀가 완료되었습니다.

- 말 타지 않은

집계가 오프라인입니다.

- 언마운트

집계가 오프라인으로 전환됩니다.

- 알려지지 않은

집계는 발견되었지만 집계 정보는 아직 Unified Manager 서버에서 검색되지 않았습니다.

- 무리

집계가 있는 클러스터의 이름을 표시합니다.

- 마디

집계를 포함하는 스토리지 컨트롤러의 이름을 표시합니다.

- 총 용량

집계된 총 데이터 크기(MB, GB 등)를 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

- 약정 용량

모든 볼륨에 대해 할당된 총 공간(MB, GB 등)을 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

- 사용 용량

집계된 공간의 양(MB, GB 등)을 표시합니다.

- 사용 가능한 용량

집계된 데이터에 사용할 수 있는 공간의 양(MB, GB 등)을 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

- 사용 가능 %

집계된 데이터에 사용할 수 있는 공간의 백분율을 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

- 사용된 %

집계된 데이터가 사용하는 공간의 백분율을 표시합니다.

- RAID 유형

선택한 볼륨의 RAID 유형을 표시합니다. RAID 유형은 RAID0, RAID4, RAID-DP, RAID-TEC 또는 혼합 RAID가 될 수 있습니다.

채용 페이지

작업 페이지에서는 현재 실행 중인 모든 파트너 애플리케이션 보호 작업과 완료된 작업에 대한 현재 상태 및 기타 정보를 볼 수 있습니다. 이 정보를 사용하면 어떤 작업이 아직 실행 중인지, 작업이 성공했는지 실패했는지 확인할 수 있습니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 중단

선택한 작업을 중단합니다. 이 옵션은 선택한 작업이 실행 중인 경우에만 사용할 수 있습니다.

- 다시 해 보다

보호 구성 또는 보호 관계 작업 유형의 실패한 작업을 다시 시작합니다. 한 번에 실패한 작업은 하나만 다시 시도할 수 있습니다. 실패한 작업을 두 개 이상 선택하면 다시 시도 버튼이 비활성화됩니다. 실패한 스토리지 서비스 작업은 다시 시도할 수 없습니다.

- 새로 고치다

작업 목록과 해당 작업과 관련된 정보를 새로 고칩니다.

작업 목록에는 진행 중인 작업 목록이 표 형식으로 표시됩니다. 기본적으로 목록에는 지난주에 생성된 작업만 표시됩니다. 열 정렬 및 필터링을 사용하여 어떤 작업이 표시되는지 사용자 지정할 수 있습니다.

- 상태

작업의 현재 상태를 표시합니다. 상태는 오류(🚨) 또는 일반(✅).

- 직무 ID

작업의 식별 번호를 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

작업 식별 번호는 고유하며 서버가 작업을 시작할 때 할당합니다. 열 필터에서 제공하는 텍스트 상자에 작업 식별 번호를 입력하여 특정 작업을 검색할 수 있습니다.

- 이름

작업 이름을 표시합니다.

- 유형

작업 유형을 표시합니다. 작업 유형은 다음과 같습니다.

- 클러스터 인수

Workflow Automation 작업에서 클러스터를 다시 검색하고 있습니다.

- 보호 구성

보호 작업은 Cron 일정, SnapMirror 정책 생성 등과 같은 워크플로 자동화 워크플로를 시작하는 것입니다.

- 보호 관계 운영

보호 작업은 SnapMirror 작업을 실행하고 있습니다.

- 보호 워크플로 체인

워크플로 자동화 작업은 여러 워크플로를 실행하는 것입니다.

- 복원하다

복원 작업이 실행 중입니다.

- 대청소

이 작업은 더 이상 복원 목적으로 필요하지 않은 스토리지 서비스 멤버 아티팩트를 정리하는 것입니다.

- 따르다

이 작업은 스토리지 서비스 멤버의 구성을 검사하여 규정에 맞는지 확인하는 것입니다.

- 파괴하다

이 작업은 스토리지 서비스를 파괴하는 것입니다.

- 수입

이 작업은 관리되지 않는 스토리지 객체를 기존 스토리지 서비스로 가져오는 것입니다.

- 수정하다

해당 작업은 기존 스토리지 서비스의 속성을 수정하는 것입니다.

- 구독하다

이 작업은 회원을 저장 서비스에 가입시키는 것입니다.

- 구독 취소

이 작업은 저장 서비스에서 회원의 구독을 취소하는 것입니다.

- 업데이트

보호 업데이트 작업이 실행 중입니다.

- **WFA** 구성

Workflow Automation 작업은 클러스터 자격 증명을 푸시하고 데이터베이스 캐시를 동기화하는 것입니다.

- 상태

작업의 실행 상태를 표시합니다. 상태 옵션은 다음과 같습니다.

- 중단됨

작업이 중단되었습니다.

- 중단

해당 작업은 중단 중입니다.

- 완전한

작업이 끝났습니다.

- 달리기

작업이 실행 중입니다.

- 제출 시간

작업이 제출된 시간을 표시합니다.

- 지속

작업이 완료되는 데 걸린 시간을 표시합니다. 이 열은 기본적으로 표시됩니다.

- 완료 시간

작업이 완료된 시간을 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

채용 정보 페이지

작업 세부 정보 페이지에서는 실행 중인 작업, 대기 중인 작업 또는 완료된 작업 중 특정 보호 작업에 대한 상태 및 기타 정보를 볼 수 있습니다. 이 정보를 사용하여 보호 작업 진행 상황을 모니터링하고 작업 실패 문제를 해결할 수 있습니다.

직무 요약

작업 요약에는 다음 정보가 표시됩니다.

- 작업 ID
- 유형
- 상태
- 제출 시간
- 완료 시간
- 지속

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 새로 고치다

작업 목록과 각 작업에 연결된 속성을 새로 고칩니다.

- 채용공고 보기

채용정보 페이지로 돌아갑니다.

작업 작업 목록

작업 목록은 특정 작업과 연관된 모든 작업과 각 작업과 관련된 속성을 표로 표시합니다.

- 시작 시간

작업이 시작된 날짜와 시간을 표시합니다. 기본적으로 가장 최근의 작업은 열의 맨 위에 표시되고, 오래된 작업은 맨 아래에 표시됩니다.

- 유형

작업 유형을 표시합니다.

- 상태

특정 작업의 상태:

- 완전한

작업이 완료되었습니다.

- 대기 중

작업이 실행되려고 합니다.

- 달리기

작업이 실행 중입니다.

- 대기 중

작업이 제출되었으며, 연관된 일부 작업이 대기열에 추가되어 실행되기를 기다리고 있습니다.

- 상태

작업 상태를 표시합니다.

- 오류 (🚫)

작업이 실패했습니다.

- 정상 (✅)

작업이 성공했습니다.

- 건너뛰기(🔄)

작업이 실패하여 후속 작업이 건너뛰어졌습니다.

- 지속

작업이 시작된 이후 경과된 시간을 표시합니다.

- 완료 시간

작업이 완료된 시간을 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

- 작업 ID

작업에 대한 개별 작업을 식별하는 GUID를 표시합니다. 열을 정렬하고 필터링할 수 있습니다. 기본적으로 이 열은 숨겨져 있습니다.

- 의존 순서

그래프에서 작업 순서를 나타내는 정수를 표시합니다. 첫 번째 작업에는 0이 할당됩니다. 기본적으로 이 열은 숨겨져 있습니다.

- 작업 세부 정보 창

작업 이름, 작업 설명, 작업이 실패한 경우 실패 이유 등 각 작업에 대한 추가 정보를 표시합니다.

- 작업 메시지 창

선택한 작업에 대한 구체적인 메시지를 표시합니다. 메시지에는 오류의 이유와 해결을 위한 제안이 포함될 수 있습니다. 모든 작업에서 작업 메시지가 표시되는 것은 아닙니다.

고급 보조 설정 대화 상자

고급 보조 설정 대화 상자를 사용하여 보조 볼륨에서 버전 유연한 복제, 다중 복사본 백업 및 공간 관련 설정을 활성화할 수 있습니다. 현재 설정을 활성화하거나 비활성화하려면 고급 보조 설정 대화 상자를 사용할 수 있습니다.

공간 관련 설정은 중복 제거, 데이터 압축, 자동 증가, 공간 보장 등을 포함하여 저장되는 데이터 양을 극대화합니다.

대화 상자에는 다음 필드가 포함되어 있습니다.

- 버전 유연한 복제 활성화

버전에 따라 유연한 복제 기능을 갖춘 SnapMirror 지원합니다. 버전 유연한 복제 기능을 사용하면 대상 볼륨이 소스 볼륨보다 이전 버전의 ONTAP에서 실행 중이더라도 소스 볼륨의 SnapMirror 보호가 가능합니다.

- 백업 활성화

버전에 따른 유연한 복제가 활성화된 경우 SnapMirror 소스 데이터의 여러 스냅샷 사본을 SnapMirror 대상에 전송하여 보관할 수도 있습니다.

- 중복 제거 활성화

SnapVault 관계에서 보조 볼륨에 대한 중복 제거를 활성화하여 중복된 데이터 블록을 제거하여 공간을 절약합니다. 최소 10% 이상의 공간 절약이 가능하고 데이터 덮어쓰기 속도가 빠르지 않은 경우 중복 제거를 사용할 수 있습니다. 중복 제거는 가상화된 환경, 파일 공유, 백업 데이터에 자주 사용됩니다. 이 설정은 기본적으로 비활성화되어 있습니다. 이 기능을 활성화하면 전송이 이루어질 때마다 작업이 시작됩니다.

- 압축 활성화

투명한 데이터 압축이 가능합니다. 최소 10%의 공간 절약이 가능하고, 잠재적 오버헤드가 허용 가능하며, 비수요 시간에 압축을 완료할 수 있는 충분한 시스템 리소스가 있는 경우 압축을 사용할 수 있습니다. SnapVault 관계에서는 이 설정이 기본적으로 비활성화되어 있습니다. 중복 제거를 선택한 경우에만 압축을 사용할 수 있습니다.

- 인라인 압축

디스크에 데이터를 쓰기 전에 데이터를 압축하여 즉각적인 공간 절약이 가능합니다. 최대 사용량 시간대에 시스템 사용률이 50%를 넘지 않고, 시스템이 최대 사용량 시간대에 새로운 쓰기 작업과 추가 CPU 작업을 처리할 수 있는 경우 인라인 압축을 사용할 수 있습니다. 이 설정은 "압축 사용"이 선택된 경우에만 사용할 수 있습니다.

- 자동 증가 활성화

연관된 집계에 사용 가능한 공간이 있는 한, 여유 공간 비율이 지정된 임계값보다 낮을 때 대상 볼륨을 자동으로 늘릴 수 있습니다.

- 최대 크기

볼륨이 증가할 수 있는 최대 비율을 설정합니다. 기본값은 소스 볼륨 크기보다 20% 더 큼니다. 현재 크기가 최대 자동 증가 백분율보다 크거나 같으면 볼륨이 자동으로 커지지 않습니다. 이 필드는 자동 증가 설정이 활성화된 경우에만 활성화됩니다.

- 크기 증가

소스 볼륨의 최대 백분율에 도달하기 전에 볼륨이 자동으로 커지는 백분율 증가량을 지정합니다.

- 공간 보장

데이터 전송이 항상 성공적으로 이루어지도록 보조 볼륨에 충분한 공간이 할당되도록 합니다. 공간 보장 설정은 다음 중 하나일 수 있습니다.

- 파일
- 용량
- 없음 + 예를 들어, 총 50GB의 파일이 포함된 200GB 볼륨이 있을 수 있습니다. 하지만 해당 파일은 10GB의 데이터만 보유합니다. 볼륨 보장은 소스의 콘텐츠에 관계없이 대상 볼륨에 200GB를 할당합니다. 파일 보장은 소스에 있는 파일에 충분한 공간이 예약되도록 50GB를 할당합니다. 이 시나리오에서 없음을 선택하면 소스의 파일 데이터가 실제로 사용하는 공간에 대해 대상에 10GB만 할당된다는 것을 의미합니다.

공간 보장은 기본적으로 볼륨으로 설정됩니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 적용하다

선택한 효율성 설정을 저장하고 보호 구성 대화 상자에서 *적용*을 클릭하면 해당 설정이 적용됩니다.

- 취소

선택 사항을 취소하고 고급 대상 설정 대화 상자를 닫습니다.

고급 대상 설정 대화 상자

고급 대상 설정 대화 상자를 사용하여 대상 볼륨에 대한 공간 보장 설정을 활성화할 수 있습니다. 소스에서 공간 보장이 비활성화되어 있지만 대상에서는 활성화하려는 경우 고급 설정을 선택할 수 있습니다. SnapMirror 관계에서 중복 제거, 압축 및 자동 증가에 대한 설정은 소스 볼륨에서 상속되며 변경할 수 없습니다.

공간 보장

데이터 전송이 항상 성공적으로 이루어지도록 대상 볼륨에 충분한 공간이 할당되도록 합니다. 공간 보장 설정은 다음 중 하나일 수 있습니다.

- 파일
- 용량

- None

예를 들어, 총 50GB의 파일이 포함된 200GB 볼륨이 있을 수 있습니다. 하지만 해당 파일에는 10GB의 데이터만 들어 있습니다. 볼륨 보장은 소스의 콘텐츠에 관계없이 대상 볼륨에 200GB를 할당합니다. 파일 보장은 대상에서 소스 파일을 위해 충분한 공간이 예약되도록 50GB를 할당합니다. 이 시나리오에서 *없음*을 선택하면 소스의 파일 데이터가 실제로 사용하는 공간에 대해 대상에 10GB만 할당된다는 것을 의미합니다.

공간 보장은 기본적으로 볼륨으로 설정됩니다.

복원 대화 상자

복원 대화 상자를 사용하여 특정 스냅샷 복사본에서 볼륨으로 데이터를 복원할 수 있습니다.

에서 복원

복원 원본 영역에서는 데이터를 복원할 원본 원본을 지정할 수 있습니다.

- 용량

데이터를 복원할 볼륨을 지정합니다. 기본적으로 복원 작업을 시작한 볼륨이 선택됩니다. 복원 작업을 시작한 볼륨과 보호 관계가 있는 모든 볼륨이 포함된 드롭다운 목록에서 다른 볼륨을 선택할 수 있습니다.

- 스냅샷 사본

데이터를 복원하는 데 사용할 스냅샷 복사본을 지정합니다. 기본적으로 가장 최근의 스냅샷 복사본이 선택됩니다. 드롭다운 목록에서 다른 스냅샷 사본을 선택할 수도 있습니다. 스냅샷 복사 목록은 선택한 볼륨에 따라 변경됩니다.

- 최대 995개의 파일 및 디렉토리를 나열합니다

기본적으로 최대 995개의 개체가 목록에 표시됩니다. 선택한 볼륨 내의 모든 객체를 보려면 이 확인란의 선택을 해제하세요. 항목 수가 매우 많으면 이 작업에 시간이 걸릴 수 있습니다.

복원할 항목을 선택하세요

복원할 항목 선택 영역에서는 전체 볼륨이나 복원하려는 특정 파일 및 폴더를 선택할 수 있습니다. 최대 10개의 파일, 폴더 또는 이 둘의 조합을 선택할 수 있습니다. 최대 개수의 항목을 선택하면 항목 선택 확인란이 비활성화됩니다.

- 경로 필드

복원하려는 데이터의 경로를 표시합니다. 복원하려는 폴더와 파일로 이동하거나 경로를 입력할 수 있습니다. 경로를 선택하거나 입력할 때까지 이 필드는 비어 있습니다. 클릭  경로를 선택하면 디렉토리 구조에서 한 단계 위로 이동합니다.

- 폴더 및 파일 목록

입력한 경로의 내용을 표시합니다. 기본적으로 루트 폴더가 처음에 표시됩니다. 폴더 이름을 클릭하면 폴더의 내용이 표시됩니다.

다음과 같이 복원할 항목을 선택할 수 있습니다.

- 경로 필드에 특정 파일 이름의 경로를 입력하면, 지정된 파일이 폴더 및 파일에 표시됩니다.

- 특정 파일을 지정하지 않고 경로를 입력하면 폴더의 내용이 폴더 및 파일 목록에 표시되고, 최대 10개의 파일, 폴더 또는 이 둘의 조합을 선택하여 복원할 수 있습니다.

폴더에 995개가 넘는 항목이 있는 경우 표시할 항목이 너무 많다는 메시지가 표시되고, 작업을 계속하면 지정된 폴더의 모든 항목이 복원됩니다. 선택한 볼륨 내의 모든 객체를 보려면 "최대 995개의 파일 및 디렉토리 나열" 체크박스의 선택을 해제할 수 있습니다.



NTFS 파일 스트림은 복원할 수 없습니다.

복원

복원 위치 영역을 사용하면 데이터를 복원할 위치를 지정할 수 있습니다.

- 볼륨 이름의 원래 위치

원래 데이터가 백업된 소스의 디렉토리에 선택한 데이터를 복원합니다.

- 대체 위치

선택한 데이터를 새 위치로 복원합니다.

- 경로 복원

선택한 데이터를 복원하기 위한 대체 경로를 지정합니다. 경로는 이미 존재해야 합니다. 찾아보기 버튼을 사용하여 데이터를 복원할 위치로 이동하거나 `cluster://svm/volume/path` 형식을 사용하여 경로를 수동으로 입력할 수 있습니다.

- 디렉토리 계층 구조 유지

이 옵션을 선택하면 원본 파일이나 디렉토리의 구조가 보존됩니다. 예를 들어, 소스가 `/A/B/C/myFile.txt`이고 대상이 `/X/Y/Z`인 경우 Unified Manager는 대상에서 다음 디렉터리 구조를 사용하여 데이터를 복원합니다. `/X/Y/Z/A/B/C/myFile.txt`.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 취소

선택 사항을 취소하고 복원 대화 상자를 닫습니다.

- 복원하다

선택 사항을 적용하고 복원 프로세스를 시작합니다.

디렉토리 찾아보기 대화 상자

원래 소스와 다른 클러스터 및 SVM의 디렉토리에 데이터를 복원하려는 경우 디렉토리 찾아보기 대화 상자를 사용할 수 있습니다. 기본적으로 원래 소스 클러스터와 볼륨이 선택됩니다.

디렉터리 찾아보기 대화 상자를 사용하면 데이터를 복원할 클러스터, SVM, 볼륨 및 디렉터리 경로를 선택할 수 있습니다.

- 무리

복원할 수 있는 사용 가능한 클러스터 대상을 나열합니다. 기본적으로 원본 볼륨의 클러스터가 선택됩니다.

- **SVM** 드롭다운 목록

선택한 클러스터에 사용 가능한 SVM을 나열합니다. 기본적으로 원본 볼륨의 SVM이 선택됩니다.

- 용량

선택한 SVM의 모든 읽기/쓰기 볼륨을 나열합니다. 볼륨을 이름과 사용 가능한 공간에 따라 필터링할 수 있습니다. 가장 많은 공간을 차지하는 볼륨이 먼저 나열되고, 이런 식으로 내림차순으로 나열됩니다. 기본적으로 원본 소스 볼륨이 선택됩니다.

- 파일 경로 텍스트 상자

데이터를 복구할 파일 경로를 입력할 수 있습니다. 입력하는 경로는 이미 존재해야 합니다.

- 이름

선택한 볼륨에 사용 가능한 폴더의 이름을 표시합니다. 이름 목록에서 폴더를 클릭하면 하위 폴더가 있는 경우 해당 폴더가 표시됩니다. 폴더에 포함된 파일은 표시되지 않습니다. 클릭  폴더를 선택하면 디렉토리 구조에서 한 단계 위로 이동합니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 디렉토리 선택

선택 사항을 적용하고 디렉토리 찾아보기 대화 상자를 닫습니다. 디렉토리를 선택하지 않으면 이 버튼은 비활성화됩니다.

- 취소

선택 사항을 취소하고 디렉토리 찾아보기 대화 상자를 닫습니다.

보호 구성 대화 상자

보호 구성 대화 상자를 사용하여 클러스터의 모든 읽기, 쓰기 및 데이터 보호 볼륨에 대한 SnapMirror 및 SnapVault 관계를 만들어 소스 볼륨이나 기본 볼륨의 데이터가 복제되도록 할 수 있습니다.

소스 탭

- 토폴로지 뷰

만들고 있는 관계의 시각적 표현을 표시합니다. 토폴로지의 소스는 기본적으로 강조 표시됩니다.

- 출처 정보

다음 정보를 포함하여 선택한 소스 볼륨에 대한 세부 정보를 표시합니다.

- 소스 클러스터 이름
- 소스 SVM 이름
- 누적 볼륨 총 크기

선택된 모든 소스 볼륨의 총 크기를 표시합니다.

- 누적 사용 볼륨 크기

선택한 모든 소스 볼륨에 대해 사용된 누적 볼륨 크기를 표시합니다.

- 소스 볼륨

다음 정보를 표로 표시합니다.

- 소스 볼륨

선택한 소스 볼륨의 이름을 표시합니다.

- 유형

볼륨 유형을 표시합니다.

- SnapLock 타입

볼륨의 SnapLock 유형을 표시합니다. 옵션은 규정 준수, 엔터프라이즈 및 비 SnapLock 입니다.

- 스냅샷 사본

기준선 전송에 사용되는 스냅샷 복사본을 표시합니다. 소스 볼륨이 읽기/쓰기인 경우 스냅샷 복사 열의 기본값은 기본적으로 새 스냅샷 복사본이 생성되고 기준 전송에 사용된다는 것을 나타냅니다. 소스 볼륨이 데이터 보호 볼륨인 경우 스냅샷 복사본 열의 기본값 값은 새 스냅샷 복사본이 생성되지 않고 모든 기존 스냅샷 복사본이 대상으로 전송됨을 나타냅니다. 스냅샷 복사 값을 클릭하면 기준 전송에 사용할 기존 스냅샷 복사본을 선택할 수 있는 스냅샷 복사본 목록이 표시됩니다. 소스 유형이 데이터 보호인 경우 다른 기본 스냅샷 복사본을 선택할 수 없습니다.

SnapMirror 탭

SnapMirror 관계를 생성하는 동안 보호 관계에 대한 대상 클러스터, 스토리지 가상 머신(SVM), 집계를 지정할 수 있으며 대상에 대한 명명 규칙도 지정할 수 있습니다. SnapMirror 정책과 일정을 지정할 수도 있습니다.

- 토폴로지 뷰

만들고 있는 관계의 시각적 표현을 표시합니다. 토폴로지의 SnapMirror 대상 리소스는 기본적으로 강조 표시됩니다.

- 목적지 정보

보호 관계에 대한 대상 리소스를 선택할 수 있습니다.

- 고급 링크

SnapMirror 관계를 만들 때 고급 대상 설정 대화 상자를 실행합니다.

- 무리

보호 대상 호스트로 사용할 수 있는 클러스터를 나열합니다. 이 필드는 필수입니다.

- 스토리지 가상 머신(SVM)

선택한 클러스터에서 사용 가능한 SVM을 나열합니다. SVM 목록을 채우기 전에 클러스터를 선택해야 합니다. 이 필드는 필수입니다.

- 골재

선택한 SVM에서 사용할 수 있는 집계를 나열합니다. 집계 목록을 채우기 전에 클러스터를 선택해야 합니다. 이 필드는 필수입니다. 집계 목록에는 다음 정보가 표시됩니다.

- 계급

여러 집계가 목적지에 대한 모든 요구 사항을 충족하는 경우 순위는 다음 조건에 따라 집계가 나열된 우선순위를 나타냅니다.

- A. 오류 도메인 분리를 위해서는 소스 볼륨 노드와 다른 노드에 위치한 집계가 선호됩니다.
 - B. 클러스터 내 노드 간 부하 분산을 활성화하려면 볼륨이 적은 노드에 대한 집계가 더 좋습니다.
 - C. 용량 균형을 맞추기 위해서는 다른 집계보다 여유 공간이 더 많은 집계가 선호됩니다. 1등급은 세 가지 기준에 따라 집계된 결과가 가장 선호된다는 것을 의미합니다.

- 집계 이름

집계의 이름

- 사용 가능한 용량

- 집계된 데이터에 사용 가능한 공간의 양

- 리소스 풀

집계가 속한 리소스 풀의 이름

- 명명 규칙

대상 볼륨에 적용되는 기본 명명 규칙을 지정합니다. 제공된 명명 규칙을 사용할 수도 있고, 사용자 정의 명명 규칙을 만들 수도 있습니다. 명명 규칙에는 %C, %M, %V, %N과 같은 속성이 있을 수 있습니다. 여기서 %C는 클러스터 이름이고, %M은 SVM 이름이고, %V는 소스 볼륨이고, %N은 토폴로지 대상 노드 이름입니다.

입력한 내용이 올바르지 않으면 명명 규칙 필드가 빨간색으로 강조 표시됩니다. "이름 미리 보기" 링크를 클릭하면 입력한 명명 규칙의 미리 보기가 표시되고, 텍스트 필드에 명명 규칙을 입력함에 따라 미리 보기 텍스트가 동적으로 업데이트됩니다. 관계가 생성될 때 대상 이름에 001에서 999 사이의 접미사가 추가되어 미리 보기 텍스트에 표시되는 nnn을 대체합니다. 즉, 001이 먼저 지정되고 002가 두 번째로 지정되는 식입니다.

- 관계 설정

보호 관계에 사용되는 최대 전송 속도, SnapMirror 정책 및 일정을 지정할 수 있습니다.

- 최대 전송 속도

네트워크를 통해 클러스터 간에 데이터가 전송되는 최대 속도를 지정합니다. 최대 전송 속도를 사용하지 않기로 선택하면 관계 간 기준 전송은 무제한입니다.

- SnapMirror 정책

관계에 대한 ONTAP SnapMirror 정책을 지정합니다. 기본값은 DPDefault입니다.

- 정책 생성

SnapMirror 정책 만들기 대화 상자를 실행하여 새 SnapMirror 정책을 만들고 사용할 수 있습니다.

- SnapMirror 일정

관계에 대한 ONTAP SnapMirror 정책을 지정합니다. 이용 가능한 일정에는 없음, 5분, 8시간, 매일, 매시간, 매주가 있습니다. 기본값은 없음으로, 관계에 일정이 연관되지 않았음을 나타냅니다. 일정이 없는 관계는 저장 서비스에 속하지 않는 한 지연 상태 값이 없습니다.

- 일정 만들기

새로운 SnapMirror 일정을 만들 수 있는 일정 만들기 대화 상자를 실행합니다.

SnapVault 탭

SnapVault 관계를 생성하는 동안 보호 관계에 대한 보조 클러스터, SVM 및 집계를 지정할 수 있으며 보조 볼륨에 대한 명명 규칙도 지정할 수 있습니다. SnapVault 정책과 일정을 지정할 수도 있습니다.

- 토폴로지 뷰

만들고 있는 관계의 시각적 표현을 표시합니다. 토폴로지의 SnapVault 보조 리소스는 기본적으로 강조 표시됩니다.

- 2차 정보

보호 관계에 대한 보조 리소스를 선택할 수 있습니다.

- 고급 링크

고급 보조 설정 대화 상자를 시작합니다.

- 무리

보조 보호 호스트로 사용 가능한 클러스터를 나열합니다. 이 필드는 필수입니다.

- 스토리지 가상 머신(SVM)

선택한 클러스터에서 사용 가능한 SVM을 나열합니다. SVM 목록을 채우기 전에 클러스터를 선택해야 합니다. 이 필드는 필수입니다.

- 골재

선택한 SVM에서 사용할 수 있는 집계를 나열합니다. 집계 목록을 채우기 전에 클러스터를 선택해야 합니다. 이 필드는 필수입니다. 집계 목록에는 다음 정보가 표시됩니다.

- 계급

여러 집계가 목적지에 대한 모든 요구 사항을 충족하는 경우 순위는 다음 조건에 따라 집계가 나열된 우선순위를 나타냅니다.

- A. 장애 도메인 분리를 위해서는 기본 볼륨 노드와 다른 노드에 위치한 집계가 선호됩니다.
 - B. 클러스터 내 노드 간 부하 분산을 활성화하려면 볼륨이 적은 노드에 대한 집계가 더 좋습니다.
 - C. 용량 균형을 맞추기 위해서는 다른 집계보다 여유 공간이 더 많은 집계가 선호됩니다. 1등급은 세 가지 기준에 따라 집계된 결과가 가장 선호된다는 것을 의미합니다.

- 집계 이름

집계의 이름

- 사용 가능한 용량
 - 집계된 데이터에 사용 가능한 공간의 양
 - 리소스 풀

집계가 속한 리소스 풀의 이름

- 명명 규칙

보조 볼륨에 적용되는 기본 명명 규칙을 지정합니다. 제공된 명명 규칙을 사용할 수도 있고, 사용자 정의 명명 규칙을 만들 수도 있습니다. 명명 규칙에는 %C, %M, %V, %N과 같은 속성이 있을 수 있습니다. 여기서 %C는 클러스터 이름이고, %M은 SVM 이름이고, %V는 소스 볼륨이고, %N은 토폴로지 보조 노드 이름입니다.

입력한 내용이 올바르지 않으면 명명 규칙 필드가 빨간색으로 강조 표시됩니다. "이름 미리 보기" 링크를 클릭하면 입력한 명명 규칙의 미리 보기가 표시되고, 텍스트 필드에 명명 규칙을 입력함에 따라 미리 보기 텍스트가 동적으로 업데이트됩니다. 잘못된 값을 입력하면 잘못된 정보가 미리 보기 영역에 빨간색 물음표로 표시됩니다. 관계가 생성될 때 2차 이름에 001~999 사이의 접미사가 추가되어 미리 보기 텍스트에 표시되는 nnn을 대체합니다. 즉, 001이 먼저 지정되고, 002가 두 번째로 지정되는 식입니다.

- 관계 설정

보호 관계에 사용되는 최대 전송 속도, SnapVault 정책 및 SnapVault 일정을 지정할 수 있습니다.

- 최대 전송 속도

네트워크를 통해 클러스터 간에 데이터가 전송되는 최대 속도를 지정합니다. 최대 전송 속도를 사용하지 않기로 선택하면 관계 간 기준 전송은 무제한입니다.

- SnapVault 정책

관계에 대한 ONTAP SnapVault 정책을 지정합니다. 기본값은 XDPDefault입니다.

- 정책 생성

SnapVault 정책 만들기 대화 상자를 실행하면 새 SnapVault 정책을 만들고 사용할 수 있습니다.

- SnapVault 일정

관계에 대한 ONTAP SnapVault 일정을 지정합니다. 이용 가능한 일정에는 없음, 5분, 8시간, 매일, 매시간, 매주 있습니다. 기본값은 없음으로, 관계에 일정이 연관되지 않았음을 나타냅니다. 일정이 없는 관계는 저장 서비스에 속하지 않는 한 지연 상태 값이 없습니다.

- 일정 만들기

SnapVault 일정을 만들 수 있는 일정 만들기 대화 상자를 실행합니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 취소

선택 사항을 취소하고 보호 구성 대화 상자를 닫습니다.

- 적용하다

선택 사항을 적용하고 보호 프로세스를 시작합니다.

일정 만들기 대화 상자

일정 만들기 대화 상자를 사용하면 SnapMirror 및 SnapVault 관계 전송에 대한 기본 또는 고급 보호 일정을 만들 수 있습니다. 데이터가 자주 업데이트되는 경우 데이터 전송 빈도를 높이기 위해 새로운 일정을 만들 수도 있고, 데이터가 자주 변경되지 않는 경우 덜 빈번한 일정을 만들 수도 있습니다.

SnapMirror 동기 관계에는 일정을 구성할 수 없습니다.

- 목적지 클러스터

보호 구성 대화 상자의 SnapVault 탭이나 SnapMirror 탭에서 선택한 클러스터의 이름입니다.

- 일정명

일정에 제공하는 이름입니다. 일정 이름은 A~Z, a~z, 0~9 문자와 ! 등의 특수 문자로 구성될 수 있습니다. @ # \$ % {캐럿} & * () _ -. 일정 이름에는 다음 문자를 포함할 수 없습니다: < >.

- 기본 또는 고급

사용하려는 일정 모드입니다.

기본 모드에는 다음 요소가 포함됩니다.

- 반복하다

예정된 환승이 발생하는 빈도. 선택 가능한 요금제로는 시간별, 일별, 주별 등이 있습니다.

- 낮

주간 반복을 선택하면 전송이 발생하는 요일이 지정됩니다.

- 시간

매일 또는 매주를 선택하면 전송이 발생하는 시간입니다.

고급 모드에는 다음 요소가 포함됩니다.

- 개월

1년의 월을 나타내는 십표로 구분된 숫자 목록입니다. 유효한 값은 0~11이며, 0은 1월을 나타냅니다. 이 요소는 선택 사항입니다. 이 필드를 비워두면 매월 이체가 발생한다는 것을 의미합니다.

- 날

해당 월의 날짜를 나타내는 십표로 구분된 숫자 목록입니다. 유효한 값은 1~31입니다. 이 요소는 선택 사항입니다. 이 필드를 비워두면 매월 매일 이체가 이루어진다는 것을 의미합니다.

- 주중

요일을 나타내는 십표로 구분된 숫자 목록입니다. 유효한 값은 0~6이며, 0은 일요일을 나타냅니다. 이 요소는 선택 사항입니다. 이 필드를 비워두면 주중 매일 이체가 발생한다는 것을 의미합니다. 요일은 지정되었지만 월의 날짜는 지정되지 않은 경우, 이체는 지정된 요일에만 발생하며 매일 발생하지 않습니다.

- 시간

하루의 시간을 나타내는 십표로 구분된 숫자 목록입니다. 유효한 값은 0~23이며, 0은 자정을 나타냅니다. 이 요소는 선택 사항입니다.

- 분

한 시간의 분을 나타내는 십표로 구분된 숫자 목록입니다. 유효한 값은 0~59입니다. 이 요소는 필수입니다.

SnapMirror 정책 만들기 대화 상자

SnapMirror 정책 만들기 대화 상자를 사용하면 SnapMirror 전송의 우선 순위를 설정하는 정책을 만들 수 있습니다. 정책을 사용하면 소스에서 목적지까지 전송하는 효율성을 극대화할 수 있습니다.

- 목적지 클러스터

보호 구성 대화 상자의 SnapMirror 탭에서 선택한 클러스터의 이름입니다.

- 대상 SVM

보호 구성 대화 상자의 SnapMirror 탭에서 선택한 SVM의 이름입니다.

- 정책명

새 정책에 제공하는 이름입니다. 정책 이름은 A~Z, a~z, 0~9, 마침표(.), 하이픈(-), 밑줄(_)로 구성될 수 있습니다.

- 전송 우선권

비동기 작업에 대한 전송이 실행되는 우선 순위입니다. 보통 또는 낮음 중에서 선택할 수 있습니다. 일반 전송 우선순위를 지정하는 정책이 있는 전송 관계는 낮은 전송 우선순위를 지정하는 정책이 있는 전송 관계보다 먼저 실행됩니다.

- 논평

정책에 대한 의견을 추가할 수 있는 선택 필드입니다.

- 전송 재시작

네트워크 중단 등의 중단 작업이나 오류로 인해 전송이 중단된 경우 수행할 재시작 작업을 나타냅니다. 다음 중 하나를 선택할 수 있습니다.

- 언제나

전송을 다시 시작하기 전에 새로운 스냅샷 복사본을 만든 다음, 복사본이 있으면 검사점에서 전송을 다시 시작한 후 새로 만든 스냅샷 복사본에서 증분 전송을 수행합니다.

- 절대

중단된 전송이 다시 시작되지 않도록 지정합니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 취소

선택 사항을 취소하고 보호 구성 대화 상자를 닫습니다.

- 적용하다

선택 사항을 적용하고 보호 프로세스를 시작합니다.

SnapVault 정책 만들기 대화 상자

SnapVault 정책 만들기 대화 상자를 사용하면 SnapVault 전송의 우선 순위를 설정하는 정책을 만들 수 있습니다. 정책을 사용하여 1차 볼륨에서 2차 볼륨으로의 전송 효율성을 극대화합니다.

- 목적지 클러스터

보호 구성 대화 상자의 SnapVault 탭에서 선택한 클러스터의 이름입니다.

- 대상 **SVM**

보호 구성 대화 상자의 SnapVault 탭에서 선택한 SVM의 이름입니다.

- 정책명

새 정책에 제공하는 이름입니다. 정책 이름은 A~Z, a~z, 0~9, 마침표(.), 하이픈(-), 밑줄(_)로 구성될 수 있습니다.

- 전송 우선권

전송이 실행되는 우선 순위입니다. 보통 또는 낮음 중에서 선택할 수 있습니다. 일반 전송 우선순위를 지정하는 정책이 있는 전송 관계는 낮은 전송 우선순위를 지정하는 정책이 있는 전송 관계보다 먼저 실행됩니다. 기본 설정은 일반입니다.

- 논평

SnapVault 정책에 대해 최대 255자까지 의견을 추가할 수 있는 선택 필드입니다.

- 접속 시간 무시

액세스 시간만 변경된 파일에 대해 증분 전송을 무시할지 여부를 지정합니다.

- 복제 라벨

ONTAP 에서 선택한 스냅샷 복사본과 관련된 규칙을 표로 나열하고, 정책에 특정 복제 레이블이 있는 복사본을 나열합니다. 다음 정보와 작업도 이용할 수 있습니다.

- 명령 버튼

명령 단추를 사용하면 다음 작업을 수행할 수 있습니다.

- 추가하다

스냅샷 사본 레이블과 보존 횟수를 생성할 수 있습니다.

- 보존 횟수 편집

기존 스냅샷 복사 레이블의 보존 횟수를 변경할 수 있습니다. 보존 횟수는 1~251 사이의 숫자여야 합니다. 모든 규칙에 대한 모든 보존 횟수의 합계는 251을 초과할 수 없습니다.

- 삭제

기존 스냅샷 복사 레이블을 삭제할 수 있습니다.

- 스냅샷 복사 라벨

스냅샷 복사 레이블을 표시합니다. 동일한 로컬 스냅샷 복사 정책이 있는 볼륨을 하나 이상 선택하면 정책의 각 레이블에 대한 항목이 표시됩니다. 두 개 이상의 로컬 스냅샷 복사 정책이 있는 여러 볼륨을 선택하는 경우 테이블에는 모든 정책의 모든 레이블이 표시됩니다.

- 일정

각 스냅샷 복사 레이블과 연관된 일정을 표시합니다. 레이블에 두 개 이상의 일정이 연결된 경우 해당 레이블의 일정은 쉼표로 구분된 목록으로 표시됩니다. 동일한 라벨이지만 일정이 다른 여러 볼륨을 선택하는 경우 일정에 "다양함"이 표시되어 선택한 볼륨에 두 개 이상의 일정이 연결되어 있음을 나타냅니다.

- 목적지 보존 횟수

SnapVault 보조 저장소에 보관된 지정된 레이블이 있는 스냅샷 복사본의 수를 표시합니다. 여러 일정이 있는

레이블의 보존 횟수는 각 레이블과 일정 쌍의 보존 횟수 합계를 표시합니다. 두 개 이상의 로컬 스냅샷 복사 정책이 있는 여러 볼륨을 선택하는 경우 보존 횟수는 비어 있습니다.

관계 편집 대화 상자

기존 보호 관계를 편집하여 최대 전송 속도, 보호 정책 또는 보호 일정을 변경할 수 있습니다.

목적지 정보

- 목적지 클러스터

선택한 대상 클러스터의 이름입니다.

- 대상 **SVM**

선택된 SVM의 이름

- 관계 설정

보호 관계에 사용되는 최대 전송 속도, SnapMirror 정책 및 일정을 지정할 수 있습니다.

- 최대 전송 속도

네트워크를 통해 클러스터 간에 기존 데이터가 전송되는 최대 속도를 지정합니다. 이 옵션을 선택하면 네트워크 대역폭이 지정한 값으로 제한됩니다. 숫자 값을 입력한 다음 초당 킬로바이트(KBps), 초당 메가바이트(MBps), 초당 기가바이트(GBps), 초당 테라바이트(TBps)를 선택할 수 있습니다. 지정하는 최대 전송 속도는 1KBps보다 크고 4TBps보다 작아야 합니다. 최대 전송 속도를 사용하지 않기로 선택하면 관계 간 기준 전송은 무제한입니다. 기본 클러스터와 보조 클러스터가 동일한 경우 이 설정은 비활성화됩니다.

- SnapMirror 정책

관계에 대한 ONTAP SnapMirror 정책을 지정합니다. 기본값은 DPDefault입니다.

- 정책 생성

SnapMirror 정책 만들기 대화 상자를 실행하여 새 SnapMirror 정책을 만들고 사용할 수 있습니다.

- SnapMirror 일정

관계에 대한 ONTAP SnapMirror 정책을 지정합니다. 이용 가능한 일정에는 없음, 5분, 8시간, 매일, 매시간, 매주 있습니다. 기본값은 없음으로, 관계에 일정이 연관되지 않았음을 나타냅니다. 일정이 없는 관계는 저장 서비스에 속하지 않는 한 지연 상태 값이 없습니다.

- 일정 만들기

새로운 SnapMirror 일정을 만들 수 있는 일정 만들기 대화 상자를 실행합니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 취소

선택 사항을 취소하고 보호 구성 대화 상자를 닫습니다.

- 제출하다

선택 사항을 적용하고 관계 편집 대화 상자를 닫습니다.

초기화/업데이트 대화 상자

초기화/업데이트 대화 상자를 사용하면 새 보호 관계에 대한 최초의 기준 전송을 수행하거나, 이미 초기화된 관계를 업데이트하고 예약되지 않은 수동 증분 업데이트를 수행할 수 있습니다.

전송 옵션 탭

전송 옵션 탭을 사용하면 전송의 초기화 우선순위를 변경하고 전송 중에 사용되는 대역폭을 변경할 수 있습니다.

- 전송 우선권

전송이 실행되는 우선 순위입니다. 보통 또는 낮음 중에서 선택할 수 있습니다. 일반 전송 우선순위를 지정하는 정책과의 관계는 낮은 전송 우선순위를 지정하는 정책과의 관계보다 먼저 실행됩니다. 기본적으로 일반이 선택되어 있습니다.

- 최대 전송 속도

네트워크를 통해 클러스터 간에 데이터가 전송되는 최대 속도를 지정합니다. 최대 전송 속도를 사용하지 않기로 선택하면 관계 간 기준 전송은 무제한입니다. 서로 다른 최대 전송 속도를 가진 두 개 이상의 관계를 선택하는 경우 다음 최대 전송 속도 설정 중 하나를 지정할 수 있습니다.

- 개별 관계 설정 또는 편집 중에 지정된 값을 사용합니다.

이 옵션을 선택하면 초기화 및 업데이트 작업에서 각 관계를 만들거나 편집할 때 지정된 최대 전송 속도가 사용됩니다. 이 필드는 서로 다른 전송 속도를 가진 여러 관계가 초기화되거나 업데이트되는 경우에만 사용할 수 있습니다.

- 제한 없는

관계 간 전송에 대역폭 제한이 없음을 나타냅니다. 이 필드는 서로 다른 전송 속도를 가진 여러 관계가 초기화되거나 업데이트되는 경우에만 사용할 수 있습니다.

- 대역폭을 제한합니다

이 옵션을 선택하면 네트워크 대역폭이 지정한 값으로 제한됩니다. 숫자 값을 입력한 다음 초당 킬로바이트(KBps), 초당 메가바이트(MBps), 초당 기가바이트(GBps), 초당 테라바이트(TBps)를 선택할 수 있습니다. 지정하는 최대 전송 속도는 1KBps보다 크고 4TBps보다 작아야 합니다.

소스 스냅샷 복사본 탭

소스 스냅샷 복사본 탭에는 기준 전송에 사용되는 소스 스냅샷 복사본에 대한 다음 정보가 표시됩니다.

- 소스 볼륨

해당 소스 볼륨의 이름을 표시합니다.

- 목적지 볼륨

선택한 대상 볼륨의 이름을 표시합니다.

- 소스 유형

볼륨 유형을 표시합니다. 유형은 읽기/쓰기 또는 데이터 보호가 될 수 있습니다.

- 스냅샷 사본

데이터 전송에 사용되는 스냅샷 복사본을 표시합니다. 스냅샷 복사 값을 클릭하면 소스 스냅샷 복사 선택 대화 상자가 표시됩니다. 이 대화 상자에서는 보호 관계 유형과 수행하는 작업에 따라 전송할 특정 스냅샷 복사를 선택할 수 있습니다. 데이터 보호 유형 소스에는 다른 스냅샷 복사본을 지정하는 옵션을 사용할 수 없습니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 취소

선택 사항을 취소하고 초기화/업데이트 대화 상자를 닫습니다.

- 제출하다

선택 사항을 저장하고 초기화 또는 업데이트 작업을 시작합니다.

재동기화 대화 상자

재동기화 대화 상자를 사용하면 이전에 끊어진 SnapMirror 또는 SnapVault 관계의 데이터를 재동기화한 후 대상이 읽기/쓰기 볼륨이 된 경우 해당 데이터를 재동기화할 수 있습니다. 소스 볼륨에서 필수 공통 스냅샷 복사본이 삭제되어 SnapMirror 또는 SnapVault 업데이트가 실패하는 경우에도 다시 동기화할 수 있습니다.

재동기화 옵션 탭

재동기화 옵션 탭을 사용하면 재동기화하는 보호 관계에 대한 전송 우선 순위와 최대 전송 속도를 설정할 수 있습니다.

- 전송 우선권

전송이 실행되는 우선 순위입니다. 보통 또는 낮음 중에서 선택할 수 있습니다. 일반 전송 우선 순위를 지정하는 정책과의 관계는 낮은 전송 우선 순위를 지정하는 정책과의 관계보다 먼저 실행됩니다.

- 최대 전송 속도

네트워크를 통해 클러스터 간에 데이터가 전송되는 최대 속도를 지정합니다. 이 옵션을 선택하면 네트워크 대역폭이 지정한 값으로 제한됩니다. 숫자 값을 입력한 다음 초당 킬로바이트(KBps), 초당 메가바이트(MBps), 초당 기가바이트(GBps) 또는 TBps를 선택할 수 있습니다. 최대 전송 속도를 사용하지 않기로 선택하면 관계 간 기준 전송은 무제한입니다.

소스 스냅샷 복사본 탭

소스 스냅샷 복사본 탭에는 기존 전송에 사용되는 소스 스냅샷 복사본에 대한 다음 정보가 표시됩니다.

- 소스 볼륨

해당 소스 볼륨의 이름을 표시합니다.

- 목적지 볼륨

선택한 대상 볼륨의 이름을 표시합니다.

- 소스 유형

볼륨 유형(읽기/쓰기 또는 데이터 보호)을 표시합니다.

- 스냅샷 사본

데이터 전송에 사용되는 스냅샷 복사본을 표시합니다. 스냅샷 복사 값을 클릭하면 소스 스냅샷 복사 선택 대화 상자가 표시됩니다. 이 대화 상자에서는 보호 관계 유형과 수행하는 작업에 따라 전송할 특정 스냅샷 복사를 선택할 수 있습니다.

명령 버튼

- 제출하다

재동기화 프로세스를 시작하고 재동기화 대화 상자를 닫습니다.

- 취소

선택 사항을 취소하고 재동기화 대화 상자를 닫습니다.

소스 스냅샷 복사 대화 상자 선택

소스 스냅샷 복사본 선택 대화 상자를 사용하여 보호 관계 간에 데이터를 전송할 특정 스냅샷 복사본을 선택하거나 관계를 초기화, 업데이트 또는 재동기화하는지 여부와 관계가 SnapMirror 인지 SnapVault 인지에 따라 달라지는 기본 동작을 선택합니다.

기본

SnapVault 및 SnapMirror 관계에 대한 초기화, 업데이트 및 재동기화 전송에 사용되는 스냅샷 복사본을 결정하기 위한 기본 동작을 선택할 수 있습니다.

SnapVault 전송을 수행하는 경우 각 작업에 대한 기본 동작은 다음과 같습니다.

작업	소스가 읽기/쓰기일 때의 기본 SnapVault 동작	소스가 DP(데이터 보호)인 경우의 기본 SnapVault 동작
초기화	새로운 스냅샷 사본을 만들어 전송합니다.	마지막으로 내보낸 스냅샷 사본을 전송합니다.

작업	소스가 읽기/쓰기일 때의 기본 SnapVault 동작	소스가 DP (데이터 보호)인 경우의 기본 SnapVault 동작
업데이트	정책에 명시된 대로 스냅샷 복사본만 전송합니다.	마지막으로 내보낸 스냅샷 사본을 전송합니다.
재동기화	최신 일반 스냅샷 복사본 이후에 생성된 모든 레이블이 지정된 스냅샷 복사본을 전송합니다.	가장 최신으로 레이블이 지정된 스냅샷 복사본을 전송합니다.

SnapMirror 전송을 수행하는 경우 각 작업에 대한 기본 동작은 다음과 같습니다.

작업	기본 SnapMirror 동작	SnapMirror 대 SnapMirror 캐스케이드에서 관계가 두 번째 홉일 때의 기본 SnapMirror 동작
초기화	새로운 스냅샷 복사본을 만들고, 새 스냅샷 복사본과 이전에 만들어진 모든 스냅샷 복사본을 전송합니다.	소스에서 모든 스냅샷 복사본을 전송합니다.
업데이트	새로운 스냅샷 복사본을 만들고, 새 스냅샷 복사본과 이전에 만들어진 모든 스냅샷 복사본을 전송합니다.	모든 스냅샷 사본을 전송합니다.
재동기화	새로운 스냅샷 복사본을 만든 다음 소스에서 모든 스냅샷 복사본을 전송합니다.	2차 볼륨에서 3차 볼륨으로 모든 스냅샷 복사본을 전송하고, 최신 공통 스냅샷 복사본을 만든 후 추가된 모든 데이터를 삭제합니다.

기존 스냅샷 복사본

해당 작업에 대해 스냅샷 복사 선택이 허용되는 경우 목록에서 기존 스냅샷 복사본을 선택할 수 있습니다.

- 스냅샷 사본

전송할 항목을 선택할 수 있는 기존 스냅샷 복사본을 표시합니다.

- 생성 날짜

스냅샷 복사본이 생성된 날짜와 시간을 표시합니다. 스냅샷 사본은 가장 최근 것부터 가장 오래된 것 순으로 나열되며, 가장 최근 사본이 목록의 맨 위에 표시됩니다.

SnapVault 전송을 수행하고 소스에서 대상으로 전송할 기존 스냅샷 복사본을 선택하려는 경우 각 작업에 대한 동작은 다음과 같습니다.

작업	스냅샷 복사본을 지정할 때 SnapVault 동작	캐스케이드에서 스냅샷 복사본을 지정할 때 SnapVault 동작
초기화	지정된 스냅샷 복사본을 전송합니다.	데이터 보호 볼륨에서는 소스 스냅샷 복사본 선택이 지원되지 않습니다.
업데이트	지정된 스냅샷 복사본을 전송합니다.	데이터 보호 볼륨에서는 소스 스냅샷 복사본 선택이 지원되지 않습니다.
재동기화	선택한 스냅샷 복사본을 전송합니다.	데이터 보호 볼륨에서는 소스 스냅샷 복사본 선택이 지원되지 않습니다.

SnapMirror 전송을 수행하고 소스에서 대상으로 전송할 기존 스냅샷 복사본을 선택하려는 경우 각 작업에 대한 동작은 다음과 같습니다.

작업	스냅샷 복사본을 지정할 때 SnapMirror 동작	캐스케이드에서 스냅샷 복사본을 지정할 때 SnapMirror 동작
초기화	지정된 스냅샷 복사본까지 소스의 모든 스냅샷 복사본을 전송합니다.	데이터 보호 볼륨에서는 소스 스냅샷 복사본 선택이 지원되지 않습니다.
업데이트	지정된 스냅샷 복사본까지 소스의 모든 스냅샷 복사본을 전송합니다.	데이터 보호 볼륨에서는 소스 스냅샷 복사본 선택이 지원되지 않습니다.
재동기화	소스에서 선택한 스냅샷 복사본까지 모든 스냅샷 복사본을 전송한 다음, 최신 공통 스냅샷 복사본을 만든 후 추가된 모든 데이터를 삭제합니다.	데이터 보호 볼륨에서는 소스 스냅샷 복사본 선택이 지원되지 않습니다.

명령 버튼

명령 버튼을 사용하면 다음 작업을 수행할 수 있습니다.

- 제출하다

선택 사항을 제출하고 소스 스냅샷 복사 선택 대화 상자를 닫습니다.

- 취소

선택 사항을 취소하고 소스 스냅샷 복사 선택 대화 상자를 닫습니다.

역방향 재동기화 대화 상자

소스 볼륨이 비활성화되고 대상이 읽기/쓰기 볼륨이 되어 보호 관계가 끊어진 경우 역방향 재동기화를 통해 관계의 방향을 반대로 바꿔 대상이 새로운 소스가 되고 소스가 새로운 대상이 됩니다.

재해로 인해 보호 관계의 소스 볼륨이 비활성화되면 대상 볼륨을 읽기/쓰기로 변환하여 데이터를 제공하는 동시에

소스를 복구하거나 교체하고, 소스를 업데이트하고, 관계를 재설정할 수 있습니다. 역방향 재동기화 작업을 수행하면 공통 스냅샷 복사본의 데이터보다 최신인 소스의 데이터는 삭제됩니다.

역방향 재동기화 전

역방향 재동기화 작업 전에 관계의 소스와 대상을 표시합니다.

- 소스 볼륨

역방향 재동기화 작업 전 소스 볼륨의 이름과 위치입니다.

- 목적지 볼륨

역방향 재동기화 작업 전 대상 볼륨의 이름과 위치입니다.

역방향 재동기화 후

예약 재동기화 작업 후 관계의 소스와 대상이 무엇인지 표시합니다.

- 소스 볼륨

역방향 재동기화 작업 후 소스 볼륨의 이름과 위치입니다.

- 목적지 볼륨

역방향 재동기화 작업 후 대상 볼륨의 이름과 위치입니다.

명령 버튼

명령 단추를 사용하면 다음 작업을 수행할 수 있습니다.

- 제출하다

역방향 재동기화 프로세스를 시작합니다.

- 취소

역방향 재동기화 작업을 시작하지 않고 역방향 재동기화 대화 상자를 닫습니다.

관계: 모든 관계 보기

관계: 모든 관계 보기는 스토리지 시스템의 보호 관계에 대한 정보를 표시합니다.

기본적으로 관계 페이지에 액세스하면 표시되는 보고서에는 볼륨과 스토리지 VM에 대한 최상위 보호 관계가 포함됩니다. 페이지 상단의 컨트롤을 사용하면 특정 보기를 선택하고, 특정 개체를 찾기 위한 검색을 수행하고, 표시되는 데이터 목록을 좁히기 위한 필터를 만들고 적용하고, 페이지에서 열을 추가/제거/재정렬하고, 페이지의 데이터를 .csv, .pdf 또는 .xlsx 파일로 내보낼 수 있습니다. 페이지를 사용자 지정한 후 결과를 사용자 지정 보기로 저장한 다음 이 데이터에 대한 보고서를 생성하여 정기적으로 이메일로 전송하도록 예약할 수 있습니다. 기본적으로 관계 메뉴를 선택하면 데이터 센터의 볼륨과 스토리지 VM에 대한 보호 관계가 포함된 보고서가 표시됩니다. 필터 옵션을 사용하면 선택한 스토리지 시스템(예: 볼륨만 또는 스토리지 VM만)만 볼 수 있습니다. 동일한 보고서가 저장소 페이지에 표시되며, 선택한 저장소 엔터티에 대해서만 표시됩니다. 볼륨 또는 스토리지 VM 관계를 보려면 스토리지 > 볼륨 >

관계: 모든 관계 페이지에 액세스하거나 보호 > 관계 > 관계: 모든 관계*에 액세스한 다음 *필터*에서 *관계 개체 유형 옵션을 사용하여 볼륨 또는 스토리지 VM 데이터만 필터링할 수 있습니다.

모든 보호 관계를 나열하는 관계 페이지에는 대상 클러스터에 대한 시스템 관리자에서 보기 링크가 있으며, 이를 통해 ONTAP 시스템 관리자에서 동일한 객체를 볼 수 있습니다.

- 상태

보호 관계의 현재 상태를 표시합니다.

상태는 오류 중 하나일 수 있습니다. , 경고 () , 또는 확인 ().

- 소스 스토리지 VM

소스 SVM의 이름을 표시합니다. SVM 이름을 클릭하면 소스 SVM에 대한 자세한 내용을 볼 수 있습니다.

클러스터에 SVM이 있지만 아직 Unified Manager 인벤토리에 추가되지 않았거나 클러스터의 마지막 새로 고침 이후에 SVM이 생성된 경우 이 필드는 비어 있습니다. SVM이 존재하는지 확인해야 하거나, 클러스터에서 재검색을 수행하여 리소스 목록을 새로 고쳐야 합니다.

- 원천

선택에 따라 보호되는 소스 볼륨이나 소스 스토리지 VM을 표시합니다. 볼륨 또는 스토리지 VM 이름을 클릭하면 소스 볼륨 또는 스토리지 VM에 대한 자세한 내용을 볼 수 있습니다.

메시지가 Resource-key not discovered 표시되는 경우 볼륨이 클러스터에 존재하지만 아직 Unified Manager 인벤토리에 추가되지 않았거나 볼륨이 클러스터의 마지막 새로 고침 이후에 생성되었음을 나타낼 수 있습니다. 볼륨이 존재하는지 확인해야 하거나 클러스터에서 재검색을 수행하여 리소스 목록을 새로 고쳐야 합니다.

- 대상 저장소 VM

대상 SVM의 이름을 표시합니다. SVM 이름을 클릭하면 대상 SVM에 대한 자세한 내용을 볼 수 있습니다.

- 목적지

선택에 따라 대상 볼륨이나 스토리지 VM의 이름을 표시합니다. 해당 개체 이름을 클릭하면 대상 볼륨이나 스토리지 VM에 대한 자세한 내용을 볼 수 있습니다.

- 관계 객체 유형

스토리지 VM, 볼륨, 일관성 그룹 등 관계에 사용된 개체 유형을 표시합니다. 일관성 관계에 있는 객체의 경우 관계 소스와 대상에 일관성 그룹이 표시되고, 이를 클릭하면 LUN 페이지로 이동하여 관계를 볼 수 있습니다.

- 정책

SnapMirror 관계에 대한 보호 정책의 이름을 표시합니다. 정책 이름을 클릭하면 다음 정보를 포함하여 해당 정책과 관련된 세부 정보를 볼 수 있습니다.

- 전송 우선 순위

비동기 작업에 대한 전송이 실행되는 우선 순위를 지정합니다. 전송 우선순위는 보통 또는 낮음입니다. 일반 우선순위 전송은 낮은 우선순위 전송보다 먼저 예약됩니다. 기본값은 일반입니다.

- 액세스 시간 무시

SnapVault 관계에만 적용됩니다. 이는 증분 전송에서 액세스 시간만 변경된 파일을 무시할지 여부를 지정합니다. 값은 True 또는 False입니다. 기본값은 False입니다.

- 관계가 동기화되지 않을 때

동기 관계를 동기화할 수 없을 때 ONTAP 수행하는 작업을 지정합니다. StrictSync 관계는 보조 볼륨과 동기화에 실패할 경우 기본 볼륨에 대한 액세스를 제한합니다. 동기화 관계는 보조 데이터베이스와의 동기화에 실패하더라도 기본 데이터베이스에 대한 액세스를 제한하지 않습니다.

- 시도 제한

SnapMirror 관계에 대한 각 수동 또는 예약된 전송을 시도하는 최대 횟수를 지정합니다. 기본값은 8입니다.

- 댓글

선택한 정책에 대한 구체적인 의견을 입력할 수 있는 텍스트 필드를 제공합니다.

- SnapMirror 라벨

스냅샷 복사 정책과 연관된 첫 번째 일정에 대한 SnapMirror 레이블을 지정합니다. SnapMirror 레이블은 SnapVault 하위 시스템에서 스냅샷 복사본을 SnapVault 대상에 백업할 때 사용됩니다.

- 보존 설정

백업 시간이나 백업 횟수에 따라 백업을 보관하는 기간을 지정합니다.

- 실제 스냅샷 사본

지정된 레이블과 일치하는 이 볼륨의 스냅샷 복사본 수를 지정합니다.

- 스냅샷 사본 보존

정책의 최대 한도에 도달하더라도 자동으로 삭제되지 않는 SnapVault 스냅샷 복사본 수를 지정합니다. 값은 True 또는 False입니다. 기본값은 False입니다.

- 보존 경고 임계값

최대 보존 한도에 거의 도달했음을 나타내는 경고가 전송되는 스냅샷 복사 한도를 지정합니다.

- 지연 시간

미러의 데이터가 소스보다 지연되는 시간을 표시합니다.

StrictSync 관계의 경우 지연 시간은 0초에 가깝거나 같아야 합니다.

- 지연 상태

관리되는 관계와 해당 관계와 연결된 일정이 있는 관리되지 않는 관계에 대한 지연 상태를 표시합니다. 지연 상태는 다음과 같습니다.

- 오류

지연 지속 시간은 지연 오류 임계값보다 크거나 같습니다.

- 경고

지연 지속 시간이 지연 경고 임계값보다 크거나 같습니다.

- OK

지연 시간은 정상 범위 내에 있습니다.

- 해당 없음

일정을 구성할 수 없으므로 동기 관계에는 지연 상태가 적용되지 않습니다.

- 마지막으로 성공적인 업데이트

마지막으로 성공한 SnapMirror 또는 SnapVault 작업의 시간을 표시합니다.

마지막으로 성공한 업데이트는 동기 관계에는 적용되지 않습니다.

- 구성원 관계

선택한 객체에 볼륨이 있는지 여부를 표시합니다.

- 관계 유형

볼륨을 복제하는 데 사용되는 관계 유형을 표시합니다. 관계 유형에는 다음이 포함됩니다.

- 비동기 미러
- 비동기 볼트
- 비동기 MirrorVault
- StrictSync
- 동조

- 전송 상태

보호 관계에 대한 전송 상태를 표시합니다. 전송 상태는 다음 중 하나일 수 있습니다.

- 종결

SnapMirror 전송은 활성화되어 있지만, 체크포인트 제거를 포함할 수 있는 전송 중단 작업이 진행 중입니다.

- 확인 중

대상 볼륨에 대한 진단 검사가 진행 중이며 전송이 진행 중이 아닙니다.

- 마무리 중

SnapMirror 전송이 활성화되었습니다. 해당 볼륨은 현재 증분형 SnapVault 전송을 위한 전송 후 단계에 있습니다.

- 게으른

전송이 활성화되어 있지만 전송이 진행 중이 아닙니다.

- 동기화됨

동기 관계에 있는 두 볼륨의 데이터는 동기화됩니다.

- 동기화되지 않음

대상 볼륨의 데이터가 소스 볼륨과 동기화되지 않았습니다.

- 준비 중

SnapMirror 전송이 활성화되었습니다. 해당 볼륨은 현재 SnapVault 증분 전송을 위한 사전 전송 단계에 있습니다.

- 대기 중

SnapMirror 전송이 활성화되었습니다. 전송이 진행 중이 아닙니다.

- 정지됨

SnapMirror 전송이 비활성화되었습니다. 전송이 진행되지 않습니다.

- 정지 중

SnapMirror 전송이 진행 중입니다. 추가 전송이 비활성화되었습니다.

- 전송 중

SnapMirror 전송이 활성화되어 있으며 전송이 진행 중입니다.

- 전환 중

소스 볼륨에서 대상 볼륨으로의 비동기 데이터 전송이 완료되었으며 동기 작업으로의 전환이 시작되었습니다.

- 대기 중

SnapMirror 전송이 시작되었지만, 일부 관련 작업이 대기열에 추가되기를 기다리고 있습니다.

- 마지막 전송 기간

마지막 데이터 전송이 완료되는 데 걸린 시간을 표시합니다.

StrictSync 관계에는 전송 기간이 적용되지 않습니다. 전송은 동시에 이루어져야 하기 때문입니다.

- 마지막 전송 크기

마지막 데이터 전송 크기를 바이트 단위로 표시합니다.

전송 크기는 StrictSync 관계에는 적용되지 않습니다.

- 중재자

중재자 상태를 표시합니다.

- 해당 없음

클러스터가 SnapMirror 활성 동기화를 지원하지 않는 경우.

- 구성되지 않음

구성되지 않았거나 구성되었지만 대상 클러스터만 추가되고 소스 클러스터는 Unified Manager에 추가되지 않은 경우입니다.

- 중재자 IP 주소

구성된 경우 소스 클러스터와 대상 클러스터가 모두 Unified Manager에 추가됩니다.

- 상태

SnapMirror 또는 SnapVault 관계의 상태를 표시합니다. 상태는 초기화되지 않음, 스냅 미러링됨 또는 중단됨일 수 있습니다. 소스 볼륨을 선택하면 관계 상태가 적용되지 않고 표시되지 않습니다.

- 관계 건강

클러스터의 관계 상태를 표시합니다.

- 건강에 해로운 이유

관계가 건강하지 못한 상태인 이유.

- 전송 우선권

전송이 실행되는 우선 순위를 표시합니다. 전송 우선순위는 보통 또는 낮음입니다. 일반 우선순위 전송은 낮은 우선순위 전송보다 먼저 예약됩니다.

동기 관계에는 전송 우선순위가 적용되지 않습니다. 모든 전송이 동일한 우선순위로 처리되기 때문입니다.

- 일정

관계에 할당된 보호 일정의 이름을 표시합니다.

이 일정은 동기 관계에는 적용되지 않습니다.

- 버전 유연한 복제

예, 백업 옵션이 있는 예, 없음 중 하나를 표시합니다.

- 소스 클러스터

SnapMirror 관계에 대한 소스 클러스터의 FQDN, 약어 또는 IP 주소를 표시합니다.

- 소스 클러스터 **FQDN**

SnapMirror 관계에 대한 소스 클러스터의 이름을 표시합니다.

- 소스 노드

볼륨의 SnapMirror 관계에 대한 소스 노드 이름 링크의 이름을 표시하고, 개체가 스토리지 VM 또는 일관성 그룹인 경우 SnapMirror 관계 노드 수 링크를 표시합니다.

사용자 정의 보기에서 노드 이름 링크를 클릭하면 해당 일관성 그룹의 볼륨이 SnapMirror 활성 동기화 관계에 속한 스토리지 개체에 대한 보호를 보고 확장할 수 있습니다.

노드 수 링크를 클릭하면 해당 관계에 연관된 노드가 있는 노드 페이지로 이동합니다. 노드 수가 0이면 관계와 연관된 노드가 없으므로 값이 표시되지 않습니다.

- 목적지 노드

볼륨의 SnapMirror 관계에 대한 대상 노드 이름 링크의 이름을 표시하고, 개체가 스토리지 VM 또는 일관성 그룹인 경우 SnapMirror 관계 노드 수 링크를 표시합니다.

노드 수 링크를 클릭하면 해당 관계에 연관된 노드가 있는 노드 페이지로 이동합니다. 노드 수가 0이면 관계와 연관된 노드가 없으므로 값이 표시되지 않습니다.

- 목적지 클러스터

SnapMirror 관계에 대한 대상 클러스터의 이름을 표시합니다.

- 대상 클러스터 **FQDN**

SnapMirror 관계에 대한 대상 클러스터의 FQDN, 약어 또는 IP 주소를 표시합니다.

- 보호됨

다양한 관계를 표시합니다. 이 열에서는 다음을 포함하여 클러스터 및 스토리지 가상 머신 주문에 대한 볼륨 및 일관성 그룹 관계를 볼 수 있습니다.

- SnapMirror
- 스토리지 VM DR
- SnapMirror, 스토리지 VM DR
- 일관성 그룹
- SnapMirror, 일관성 그룹.

관련 정보

- 관계: **MetroCluster** 보기에 대한 정보는 다음을 참조하세요. "[MetroCluster 구성 모니터링](#)".
- 관계: 지난 1개월 전송 상태 보기에 대한 정보는 다음을 참조하세요. "[관계: 지난 1개월 전송 상태 보기](#)".
- 관계: 모든 관계 보기에 대한 정보는 다음을 참조하세요. "[관계: 지난 1개월 전송률 보기](#)".

관계: 지난 1개월 전송 상태 보기

관계: 지난 1개월 전송 상태 보기를 사용하면 비동기 관계에 있는 볼륨 및 스토리지 VM의 특정

기간 동안의 전송 추세를 분석할 수 있습니다. 이 페이지에는 전송이 성공했는지 실패했는지도 표시됩니다.

페이지 상단의 컨트롤을 사용하면 특정 객체를 찾기 위한 검색을 수행하고, 표시되는 데이터 목록을 좁히기 위한 필터를 만들고 적용하고, 페이지에서 열을 추가/제거/재정렬하고, 페이지의 데이터를 내보낼 수 있습니다. .csv , .pdf , 또는 .xlsx 파일. 페이지를 사용자 지정한 후 결과를 사용자 지정 보기로 저장한 다음 이 데이터에 대한 보고서를 생성하여 정기적으로 이메일로 전송하도록 예약할 수 있습니다. 필터 옵션을 사용하면 선택한 스토리지 시스템(예: 볼륨만 또는 스토리지 VM만)만 볼 수 있습니다. 동일한 보고서가 저장소 페이지에 표시되며, 선택한 저장소 엔터티에 대해서만 표시됩니다. 예를 들어, 볼륨 관계를 보고 싶다면 저장소 > 저장소 **VM** > 관계: 지난 1개월 전송 상태 메뉴 또는 보호 > 관계 > 관계: 지난 1개월 전송 상태 메뉴에서 저장소 VM에 대한 관계: 지난 1개월 전송 상태 보고서에 액세스하고, * 필터*를 사용하여 볼륨에 대한 데이터만 볼 수 있습니다.

- 소스 볼륨

소스 볼륨 이름을 표시합니다.

- 목적지 볼륨

대상 볼륨 이름을 표시합니다.

- 작업 유형

볼륨 전송 유형을 표시합니다.

- 작업 결과

볼륨 전송이 성공했는지 여부를 표시합니다.

- 전송 시작 시간

볼륨 전송 시작 시간을 표시합니다.

- 전송 종료 시간

볼륨 전송 종료 시간을 표시합니다.

- 이전 기간

볼륨 전송을 완료하는 데 걸린 시간(시간)을 표시합니다.

- 전송 크기

전송된 볼륨의 크기(MB)를 표시합니다.

- 출처 **SVM**

스토리지 가상 머신(SVM) 이름을 표시합니다.

- 소스 클러스터

소스 클러스터 이름을 표시합니다.

- 대상 **SVM**

대상 SVM 이름을 표시합니다.

- 목적지 클러스터

대상 클러스터 이름을 표시합니다.

관련 정보

- 관계: 모든 관계 보기에 대한 정보는 다음을 참조하세요. "[관계: 모든 관계 보기](#)".
- 관계: **MetroCluster** 보기에 대한 정보는 다음을 참조하세요. "[MetroCluster 구성 모니터링](#)".
- 관계: 모든 관계 보기에 대한 정보는 다음을 참조하세요. "[관계: 지난 1개월 전송률 보기](#)".

관계: 지난 1개월 전송률 보기

관계: 지난 1개월 전송률 보기를 사용하면 비동기 관계의 볼륨에 대해 매일 전송되는 데이터 볼륨의 양을 분석할 수 있습니다. 이 페이지에서는 일일 전송에 대한 세부 정보와 볼륨 및 스토리지 VM에 대한 전송 작업을 완료하는 데 필요한 시간에 대한 정보도 제공합니다.

페이지 상단의 컨트롤을 사용하면 특정 객체를 찾기 위한 검색을 수행하고, 표시되는 데이터 목록을 좁히기 위한 필터를 만들고 적용하고, 페이지에서 열을 추가/제거/재정렬하고, 페이지의 데이터를 .csv, .pdf 또는 .xlsx 파일로 내보낼 수 있습니다. 페이지를 사용자 지정한 후 결과를 사용자 지정 보기로 저장한 다음 이 데이터에 대한 보고서를 생성하여 정기적으로 이메일로 전송하도록 예약할 수 있습니다. 예를 들어, 볼륨 관계를 보려면 저장소 > 볼륨 > 관계: 최근 1개월 전송률 메뉴에 액세스하거나 보호 > 관계 > 관계: 최근 1개월 전송률 메뉴에 액세스하고 *필터*를 사용하여 볼륨에 대한 데이터만 볼 수 있습니다.

- 총 전송 크기

볼륨 전송의 총 크기를 기가바이트 단위로 표시합니다.

- 낮

볼륨 전송이 시작된 날짜를 표시합니다.

- 종말 시간

볼륨 전송 종료 시간과 날짜를 표시합니다.

관련 정보

- 관계: **MetroCluster** 보기에 대한 정보는 다음을 참조하세요. "[MetroCluster 구성 모니터링](#)".
- 관계: 지난 1개월 전송 상태 보기에 대한 정보는 다음을 참조하세요. "[관계: 지난 1개월 전송 상태 보기](#)".
- 관계: 모든 관계 보기에 대한 정보는 다음을 참조하세요. "[관계: 지난 1개월 전송률 보기](#)".

사용자 정의 보고서 생성

통합 관리자 보고

Active IQ Unified Manager (이전 OnCommand Unified Manager)를 사용하면 ONTAP 스토리지 시스템에 대한 보고서를 보고, 사용자 지정하고, 다운로드하고, 일정을 예약할 수 있습니다. 보고서는 스토리지 시스템 용량, 상태, 성능, 보안 및 보호 관계에 대한 세부 정보를 제공할 수 있습니다.

Active IQ Unified Manager 9.6에 도입된 새로운 Unified Manager 보고 및 일정 관리 기능은 Unified Manager 버전 9.5에서 사용이 중단된 이전 보고 엔진을 대체합니다.

보고 기능은 네트워크에 대한 다양한 관점을 제공하고 용량, 상태, 성능, 보안 및 보호 데이터에 대한 실행 가능한 정보를 제공합니다. 열 표시, 숨기기, 재정렬, 데이터 필터링, 데이터 정렬, 결과 검색 등을 통해 보기를 사용자 지정할 수 있습니다. 사용자 정의 보기를 저장하여 재사용하거나, 보고서로 다운로드하거나, 반복 보고서로 예약하여 이메일로 배포할 수 있습니다.

Microsoft® Excel 형식으로 뷰를 다운로드하여 사용자 지정할 수 있습니다. 복잡한 정렬, 계층형 필터, 피벗 테이블, 차트 등 고급 Excel 기능을 사용할 수 있습니다. 만족스러운 Excel 보고서가 만들어지면 보고서를 예약하고 공유할 때마다 사용할 수 있도록 Excel 파일을 업로드할 수 있습니다.

사용자 인터페이스에서 보고서를 생성하는 것 외에도 다음과 같은 추가 방법을 사용하여 Unified Manager에서 상태, 보안 및 성능 데이터를 추출할 수 있습니다.

- ODBC(Open Database Connectivity) 및 ODBC 도구를 사용하여 클러스터 정보를 위해 데이터베이스에 직접 액세스합니다.
- 검토하려는 정보를 반환하기 위해 Unified Manager REST API를 실행합니다.

이번 Active IQ Unified Manager 릴리스에서는 보고서가 다음과 같이 향상되었습니다.

- 구성된 일정에 따라 보고서가 이메일로 전송됩니다. 주문형 보고서를 생성하는 경우에도 이메일을 받게 됩니다.
- 보고서의 파일 이름과 보고서의 메타데이터에는 보고서가 생성된 호스트 이름이 포함됩니다. 누군가가 파일 이름을 변경하더라도 이 향상된 기능으로 인해 보고서가 생성된 호스트 이름을 식별할 수 있습니다.

보고서 생성을 위한 액세스 포인트

Unified Manager에서 클러스터에 대한 정보를 수집하여 UI, MySQL 데이터베이스 쿼리, REST API에서 보고서를 만들 수 있습니다.

이 섹션에서는 UI를 통한 Unified Manager 보고 및 일정 예약에 대해 설명합니다.

Unified Manager가 제공하는 보고 기능에 액세스하는 방법은 세 가지가 있습니다.

- UI의 인벤토리 페이지에서 직접 데이터를 추출합니다.
- ODBC(Open Database Connectivity) 및 ODBC 도구를 사용하여 사용 가능한 모든 개체에 액세스합니다.
- 검토하려는 정보를 반환하기 위해 Unified Manager REST API를 실행합니다.

이 섹션에서는 UI를 통한 Unified Manager 보고 및 일정 예약에 대해 설명합니다.

사용자 정의 보고를 위해 접근 가능한 **Unified Manager** 데이터베이스

Unified Manager는 모니터링하는 클러스터의 데이터를 저장하기 위해 MySQL 데이터베이스를 사용합니다. 데이터는 MySQL 데이터베이스의 다양한 스키마에 저장됩니다.

다음 데이터베이스의 모든 테이블 데이터를 사용할 수 있습니다.

데이터 베이스	설명
넷애플_모델	ONTAP 컨트롤러의 객체에 대한 데이터입니다.
넷애플_모델_뷰	보고서 도구 사용에 적합한 ONTAP 컨트롤러의 객체에 대한 데이터입니다.
넷애플_성능	클러스터별 성능 카운터.
오컴	UI 필터링, 정렬 및 일부 파생 필드의 계산을 지원하기 위한 Unified Manager 애플리케이션 데이터 및 정보입니다.
ocum_report	재고 구성 및 용량 관련 정보에 대한 데이터입니다.
오컴_리포트_버트	보고서 도구 사용에 적합한 재고 구성 및 용량 관련 데이터에 대한 뷰입니다.
오피엠	성능 구성 설정 및 임계값 정보.
스케일모니터	Unified Manager 애플리케이션 상태 및 성능 문제에 대한 데이터입니다.
vmware_model	NetApp 스토리지에 호스팅된 데이터스토어에 대한 VMware 개체 데이터입니다.
vmware_model_view	NetApp 스토리지에 호스팅된 데이터 저장소의 VMware 개체 데이터에 대한 뷰로, 보고서 도구 사용에 적합합니다.
vmware_성능	NetApp 스토리지에 호스팅된 데이터스토어에 대한 VMware 성능 카운터 데이터입니다.

보고 사용자(보고서 스키마 역할이 있는 데이터베이스 사용자)는 이러한 테이블의 데이터에 액세스할 수 있습니다. 이 사용자는 Unified Manager 데이터베이스에서 직접 보고 및 기타 데이터베이스 보기에 대한 읽기 전용 액세스 권한을 갖습니다. 이 사용자는 사용자 데이터나 클러스터 자격 증명 정보가 포함된 테이블에 액세스할 수 있는 권한이 없습니다.

보고에 사용할 수 있는 Unified Manager REST API

REST API를 사용하면 Unified Manager에서 캡처한 상태, 용량, 성능 및 보안 정보를 보고 클러스터를 관리하는 데 도움이 됩니다.

REST API는 Swagger 웹 페이지를 통해 공개됩니다. Swagger 웹 페이지에 접속하면 Unified Manager REST API 문서를 볼 수 있고, 수동으로 API 호출을 실행할 수도 있습니다. Unified Manager 웹 UI의 메뉴 표시줄에서 도움말 버튼을 클릭한 다음 *API 문서*를 선택합니다. Unified Manager REST API에 대한 정보는 다음을 참조하세요. "[Active IQ Unified Manager REST API 시작하기](#)".

REST API에 액세스하려면 운영자, 스토리지 관리자 또는 애플리케이션 관리자 역할이 있어야 합니다.

보고서 이해

보고서는 스토리지, 네트워크, 서비스 품질, 보호 관계에 대한 자세한 정보를 표시하여 문제가 발생하기 전에 잠재적인 문제를 식별하고 해결하는 데 도움이 됩니다.

보기를 사용자 지정하면 나중에 사용할 수 있도록 고유한 이름으로 저장할 수 있습니다. 해당 보기를 기반으로 보고서를 정기적으로 실행하고 다른 사람들과 공유하도록 예약할 수 있습니다. 고급 Excel 기능을 사용하여 보기를 Excel로 다운로드한 다음 사용자 정의하고 해당 파일을 Unified Manager로 다시 업로드할 수도 있습니다. 해당 보기를 사용하여 보고서를 예약하면 업로드한 Excel 파일을 사용하여 공유할 수 있는 견고한 보고서가 생성됩니다.

보고서 일정 페이지에서 예약된 모든 보고서를 관리할 수 있습니다.



보고서를 관리하려면 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

보고서는 CSV(쉼표로 구분된 값), Excel 또는 PDF 파일로 다운로드할 수 있습니다.

뷰와 보고서 관계 이해

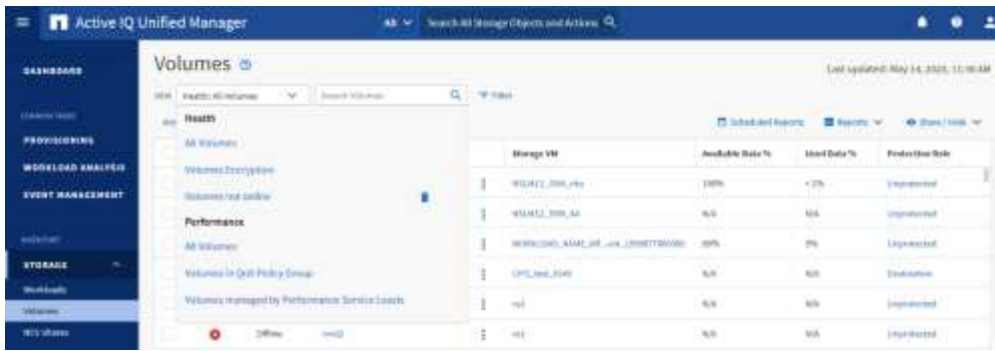
뷰와 인벤토리 페이지는 다운로드하거나 예약하면 보고서가 됩니다.

재사용을 위해 뷰와 인벤토리 페이지를 사용자 지정하고 저장할 수 있습니다. Unified Manager에서 볼 수 있는 거의 모든 항목은 보고서로 저장, 재사용, 사용자 정의, 예약 및 공유할 수 있습니다.

보기 드롭다운에서 삭제 아이콘이 있는 항목은 사용자 또는 다른 사용자가 만든 기존 사용자 정의 보기입니다. 아이콘이 없는 항목은 Unified Manager에서 제공하는 기본 보기입니다. 기본 보기는 수정하거나 삭제할 수 없습니다.



- 목록에서 사용자 지정 보기를 삭제하면 해당 보기를 사용하는 Excel 파일이나 예약된 보고서도 모두 삭제됩니다.
- 사용자 지정 보기를 변경하는 경우, 해당 보기를 사용하는 보고서는 다음에 보고서가 생성되어 보고서 일정에 따라 이메일로 전송될 때 변경 사항을 반영합니다. 보기를 변경할 때는 보고서에 사용된 모든 관련 Excel 사용자 지정 내용과 함께 변경 사항이 적용되는지 확인하세요. 필요한 경우 Excel 파일을 다운로드하여 필요한 변경 사항을 적용한 다음 보기에 대한 새로운 Excel 사용자 지정으로 업로드하여 업데이트할 수 있습니다.



애플리케이션 관리자 또는 스토리지 관리자 역할이 있는 사용자만 삭제 아이콘을 볼 수 있고, 보기를 변경하거나 삭제할 수 있으며, 예약된 보고서를 변경하거나 삭제할 수 있습니다.

보고서 유형

이 표는 사용자 정의, 다운로드 및 예약이 가능한 보고서로 제공되는 뷰와 인벤토리 페이지의 포괄적인 목록을 제공합니다.

Active IQ Unified Manager 보고서

유형	저장소 또는 네트워크 객체
용량	클러스터 골재 볼륨 큐트리스
건강	클러스터 노드 골재 스토리지 VM 볼륨 SMB/CIFS 주식 NFS 주식

유형	저장소 또는 네트워크 객체
성능	클러스터 노드 골재 스토리지 VM 볼륨 LUN NVMe 네임스페이스 네트워크 인터페이스(LIF) 포트
서비스 품질(QoS: Quality of Service)	기존 QoS 정책 그룹 적응형 QoS 정책 그룹 성능 서비스 수준 정책 그룹
볼륨 보호 관계(볼륨 페이지에서 사용 가능)	모든 관계 지난 1개월 이체 현황 최근 1개월 이체율
보안	스토리지 VM 클러스터

보고 제한 사항

새로운 Active IQ Unified Manager 보고 기능에는 알아야 할 몇 가지 제한 사항이 있습니다.

이전 버전의 **Unified Manager**에서 작성된 기존 보고서

Unified Manager 9.5 및 이전 릴리스에서는 .rptdesign 파일로 생성 및 가져온 기존 보고서의 일정과 수신자만 편집할 수 있습니다. Unified Manager 9.5 이하 버전에서 제공된 표준 보고서를 사용자 지정한 경우, 해당 사용자 지정 보고서는 새 보고 도구로 가져올 수 없습니다.

rptdesign 파일에서 가져온 기존 보고서를 편집해야 하는 경우 다음 중 하나를 수행하여 가져온 보고서를 제거하세요.

- 새 뷰를 만들고 해당 뷰에서 보고서를 예약합니다(권장)
- 보고서 위에 마우스를 올려놓고 SQL을 복사한 다음 외부 도구를 사용하여 데이터를 가져옵니다.

기본 보기는 사용자 정의 없이도 보고서로 생성될 수 있습니다. 새로운 보고 솔루션을 사용하면 사용자 정의 보고서를 다시 만들 수 있습니다.

일정 및 보고서 관계

저장된 각 보고서에 대해 수신자를 원하는 대로 조합하여 다양한 일정을 만들 수 있습니다. 하지만 여러 보고서에 대해 일정을 재사용할 수는 없습니다.

신고 보호

적절한 권한이 있는 모든 사용자는 보고서를 편집하거나 삭제할 수 있습니다. 다른 사용자가 저장된 보기나 일정을 삭제하거나 변경하는 것을 막을 방법은 없습니다.

이벤트 보고서

이벤트 보기를 사용자 지정하고 결과 보고서를 CSV 형식으로 다운로드할 수는 있지만, 반복 이벤트 보고서를 생성하고 배포하도록 예약할 수는 없습니다.

보고서 첨부 파일

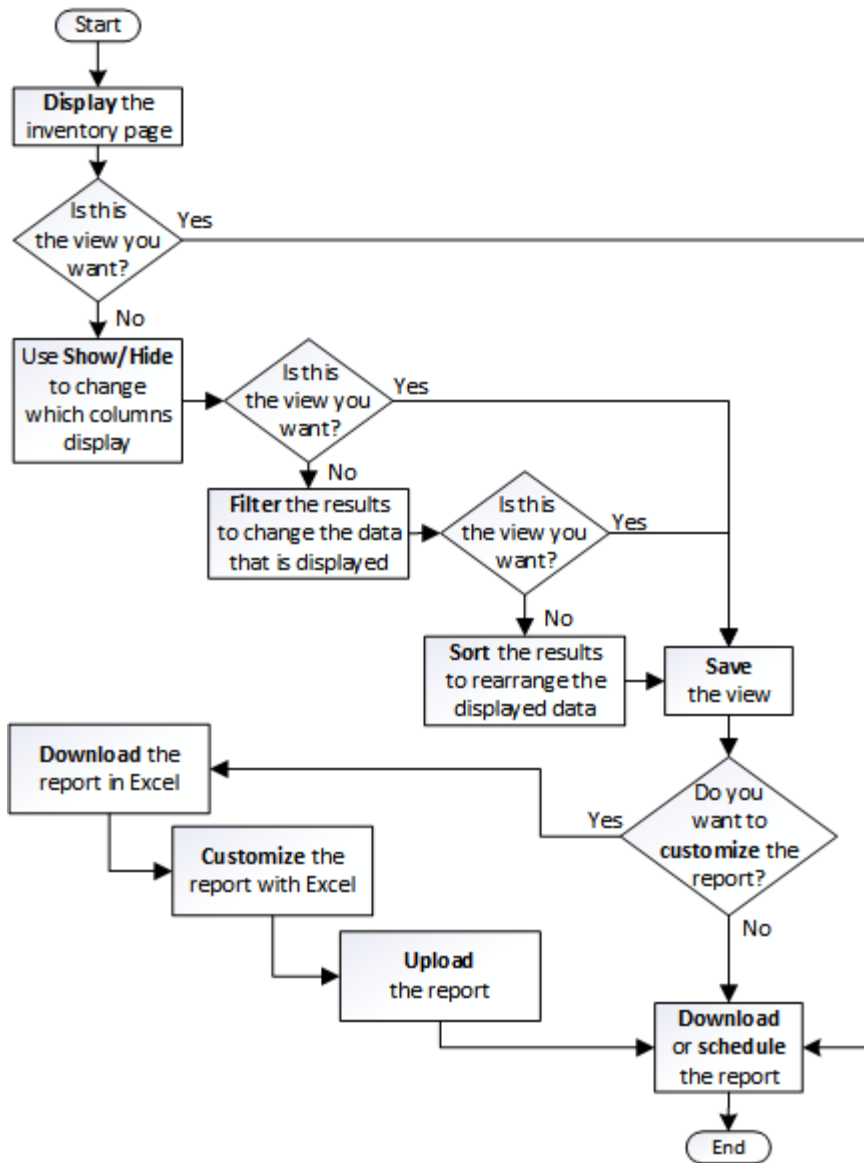
이메일 본문에 보고서를 넣을 수 없습니다. 대신 보고서는 PDF, Excel 또는 CSV 첨부 파일로만 전송됩니다.

보고서 작업

인벤토리 페이지 뷰를 찾아 공유 가능한 예약 보고서로 사용자 지정하는 방법을 알아보세요.

보고서 워크플로

보고서 워크플로를 설명하는 의사결정 트리입니다.



빠른 시작 보고

샘플 사용자 정의 보고서를 만들어서 뷰를 탐색하고 보고서를 예약하는 방법을 알아보세요. 이 빠른 시작 보고서는 비활성(콜드) 데이터가 상당히 많기 때문에 클라우드 계층으로 이동하는 것이 좋을 수 있는 볼륨 목록을 찾아줍니다. 성과: 모든 볼륨 보기를 열고 필터와 열을 사용하여 보기를 사용자 지정하고, 사용자 지정 보기를 보고서로 저장하고, 보고서를 일주일에 한 번 공유하도록 예약합니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- FabricPool 집계를 구성하고 해당 집계에 볼륨이 있어야 합니다.

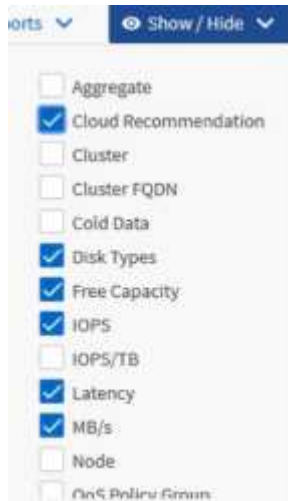
다음 단계에 따라 진행하세요.

- 기본 보기 열기
- 데이터를 필터링하고 정렬하여 열을 사용자 정의합니다.

- 뷰를 저장하세요
- 사용자 정의 보기에 대한 보고서 생성을 예약합니다.

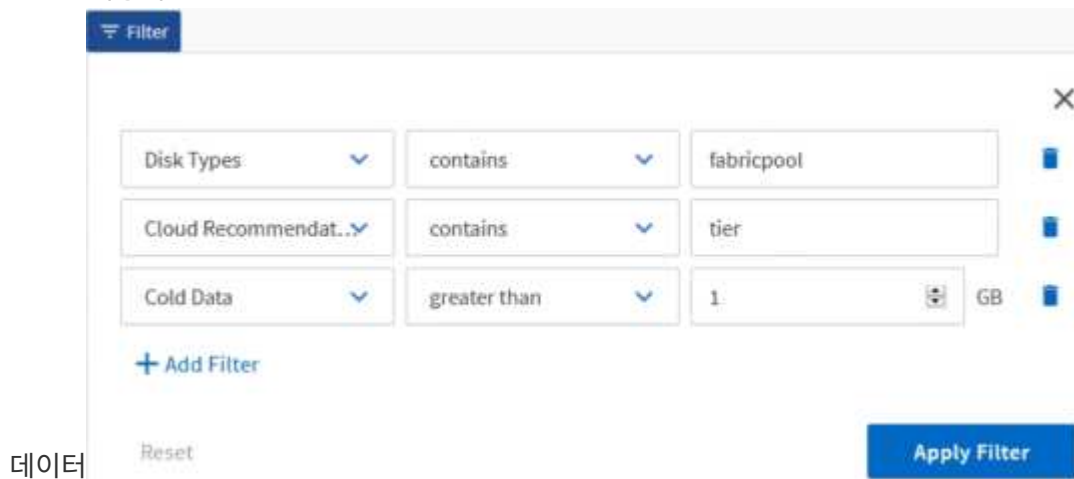
단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 성능 > *모든 볼륨*을 선택합니다.
3. *표시/숨기기*를 클릭하여 보기에 "디스크 유형" 열이 나타나는지 확인하세요.



보고서에 중요한 필드가 포함된 보기를 만들려면 다른 열을 추가하거나 제거하세요.

4. "디스크 유형" 열을 "클라우드 권장 사항" 열 옆으로 끌어다 놓습니다.
5. 필터 아이콘을 클릭하여 다음 세 가지 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 디스크 유형에는 FabricPool 포함되어 있습니다.
 - 클라우드 추천에는 계층이 포함되어 있습니다.
 - 10GB 이상의 콜드



각 필터는 논리적 AND로 결합되어 있으므로 반환된 모든 볼륨이 모든 기준을 충족해야 합니다. 최대 5개의 필터를 추가할 수 있습니다.

6. 콜드 데이터 열의 상단을 클릭하면 결과가 정렬되어 콜드 데이터가 가장 많은 볼륨이 보기의 맨 위에 표시됩니다.

7. 보기가 사용자 정의된 경우 보기 이름은 저장되지 않은 보기입니다. 뷰가 표시하는 내용을 반영하도록 뷰의 이름을 지정합니다(예: "Vols change tiering policy"). 완료되면 체크 표시를 클릭하거나 **Enter** 키를 눌러 새 이름으로 보기를 저장합니다.

Volumes - Performance / Vols change tiering policy ⓘ Last updated: Feb 8, 2019, 12:26 PM ↻

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View Vols change tiering policy 🔍 Search Volumes ⚙️

Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
rfa_vol4	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagntsdst	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

8. 일정을 정하거나 공유하기 전에 보고서를 **CSV**, **Excel** 또는 **PDF** 파일로 다운로드하여 결과를 확인하세요.

Microsoft Excel(CSV 또는 Excel)이나 Adobe Acrobat(PDF) 등 설치된 애플리케이션으로 파일을 열거나 파일을 저장합니다.



Excel 파일로 보기를 다운로드하면 복잡한 필터, 정렬, 피벗 테이블 또는 차트를 사용하여 보고서를 더욱 세부적으로 사용자 지정할 수 있습니다. Excel에서 파일을 연 후 고급 기능을 사용하여 보고서를 사용자 지정하세요. 만족스러우면 Excel 파일을 업로드하세요. 이 파일은 사용자 정의가 적용되어 보고서가 실행될 때 보기에 적용됩니다.

Excel을 사용하여 보고서를 사용자 지정하는 방법에 대한 자세한 내용은 Microsoft Excel 보고서 샘플을 참조하세요.

9. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요. 이 경우 볼륨과 관련된 모든 예약된 보고서가 목록에 나타납니다.

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports

Volumes - Scheduled Reports View all Scheduled Reports

Schedule Name	View	Recipients	Frequency	Format	
Weekly / Vols c... tiering policy	Performance / V... tiering policy	user@company.com	Weekly - Monday 1:00 PM	CSV	⋮

10. *일정 추가*를 클릭하면 보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
11. 보고서 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

다음 샘플 보고서는 CSV 형식입니다.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:52 PM - March 28, 2019, 12:52 PM)																
2	Generated At: March 28, 2019, 12:52 PM																
3																	
4	Status	Volume	Volume Ic	Tiering Po	Cold Data	Free Capa	Total Capa	Cluster	Cluster Id	Node	Node Id	Aggregate	Aggregate Id				
5	Ok	kjagnfsdst	101510	Snapshot	28.01	121.32	150	ocum-mo	99001	ocum-mo	99018	aggr5_vs	99040				
6	Ok	nfs_vol4	102294	Snapshot	379.64	2676.57	3072	ocum-mo	99001	ocum-mo	99113	aggr4	99141				

다음 샘플 보고서는 PDF 형식입니다.

Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:51 PM - March 28, 2019, 12:51 PM)
Generated At: March 28, 2019, 12:51 PM

Status	Volume	Tiering Policy	Cold Data (GB)	Free Capacity (GB)	Total Capacity (GB)	Cluster	Node	Aggregate
Ok	Snapshot	Snapshot Only	28.01	121.32	150	ocum-mobility-01-02	ocum-mobility-01	aggr5_vs
Ok	nfs_vol4	Snapshot Only	379.64	2676.57	3072	ocum-mobility-01-02	ocum-mobility-02	aggr4

보고서에 표시된 결과를 기반으로 ONTAP System Manager나 ONTAP CLI를 사용하여 특정 볼륨의 계층화 정책을 "auto" 또는 "all"로 변경하여 더 많은 콜드 데이터를 클라우드 계층으로 오프로드할 수 있습니다.

예약된 보고서 검색

이름, 보기 이름, 개체 유형 또는 수신자를 기준으로 예약된 보고서를 검색할 수 있습니다.

1. 왼쪽 탐색 창에서 저장소 관리 > *보고서 일정*을 클릭합니다.
2. 예약된 보고서 검색 텍스트 필드를 사용하세요.

보고서를 찾으려면...	노력하다 ...
일정 이름	보고서 일정 이름의 일부를 입력하세요.
보기 이름	보고서 보기 이름의 일부를 입력하세요. 기본 보기와 사용자 정의 보기가 보기 목록에 나타납니다.
받는 사람	이메일 주소의 일부를 입력하세요.
파일 유형	"PDF", "CSV" 또는 "XLSX"를 입력하세요.

3. 일정 이름이나 형식 등의 열 제목을 클릭하면 해당 열을 기준으로 보고서를 오름차순이나 내림차순으로 정렬할 수 있습니다.

보고서 사용자 정의

ONTAP 클러스터를 관리하는 데 필요한 모든 정보가 포함된 보고서를 만들 수 있도록 뷰를 사용자 지정할 수 있는 방법이 많습니다.

기본 인벤토리 페이지나 사용자 지정 보기로 시작한 다음, 열을 추가하거나 제거하고, 열 순서를 변경하고, 데이터를 필터링하거나, 특정 열을 오름차순이나 내림차순으로 정렬하여 사용자 지정합니다.

Unified Manager 9.8부터 Excel에서 보기를 다운로드하여 고급 기능을 사용하여 사용자 지정할 수도 있습니다. 완료되면 사용자 정의된 Excel 파일을 업로드하세요. 해당 보기를 사용하여 보고서를 예약하면 사용자 정의된 Excel 파일을 사용하여 공유할 수 있는 견고한 보고서를 만듭니다.

Excel을 사용하여 보고서를 사용자 지정하는 방법에 대한 자세한 내용은 _Microsoft Excel 보고서 샘플_을 참조하세요.



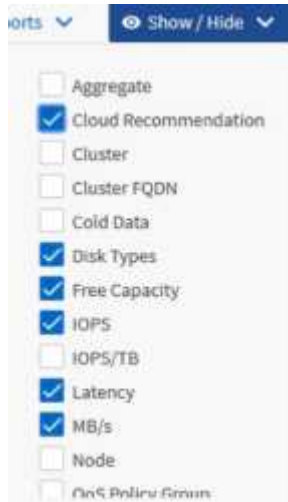
보고서를 관리하려면 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

열 사용자 정의

보고서에 사용할 열을 선택하려면 *표시/숨기기*를 사용하세요. 인벤토리 페이지에서 열을 끌어서 다시 정렬하세요.

단계

1. 열을 추가하거나 제거하려면 *표시/숨기기*를 클릭하세요.



2. 인벤토리 페이지에서 열을 끌어서 보고서에서 원하는 순서대로 다시 정렬합니다.
3. 변경 사항을 저장하려면 저장되지 않은 보기의 이름을 지정하세요.

데이터 필터링

데이터가 보고서 요구 사항과 일치하는지 확인하려면 데이터를 필터링하세요. 필터링을 사용하면 관심 있는 데이터만 표시할 수 있습니다.

단계

1. 필터 아이콘을 클릭하여 보고 싶은 결과에 필터를 추가한 다음 *필터 적용*을 클릭합니다.

The screenshot shows a filter configuration panel with a title bar 'Filter' and a close button 'X'. It contains three filter rules, each with a dropdown menu for the field, a dropdown for the operator, and a text input for the value. The first rule is 'Disk Types' contains 'fabricpool'. The second rule is 'Cloud Recommendation' contains 'tier'. The third rule is 'Cold Data' greater than '1' GB. Below the rules is a '+ Add Filter' button. At the bottom are 'Reset' and 'Apply Filter' buttons.

2. 변경 사항을 저장하려면 저장되지 않은 보기의 이름을 지정하세요.

데이터 정렬

결과를 정렬하려면 열을 클릭하고 오름차순 또는 내림차순을 선택하세요. 데이터를 정렬하면 보고서에 필요한 정보의 우선순위가 정해집니다.

단계

1. 열의 맨 위를 클릭하면 결과가 정렬되어 가장 중요한 정보가 보기 맨 위에 표시됩니다.
2. 변경 사항을 저장하려면 저장되지 않은 보기의 이름을 지정하세요.

검색을 사용하여 보기를 구체화하세요

원하는 보기를 얻은 후 검색 필드를 사용하여 결과를 더욱 세분화하여 보고서에 포함하려는 결과에 집중할 수 있습니다.

단계

1. 보고서의 기준으로 사용할 사용자 지정 보기나 기본 보기를 엽니다.
2. 보기에 나열된 데이터를 구체화하려면 검색 필드에 입력하세요. 표시된 열에 부분적인 데이터를 입력할 수 있습니다. 예를 들어, 이름에 "US_East"가 포함된 노드를 검색하려면 전체 노드 목록을 구체화할 수 있습니다.

검색 결과는 사용자 정의 보기에 저장되고, 그 결과로 생성되는 예약 보고서에 사용됩니다.

3. 변경 사항을 저장하려면 저장되지 않은 보기의 이름을 지정하세요.

Excel을 사용하여 보고서를 사용자 지정하세요

보기를 저장한 후 Excel 통합 문서 형식(.xlsx)으로 다운로드할 수 있습니다. Excel 파일을 열면 고급 Excel 기능을 사용하여 보고서를 사용자 지정할 수 있습니다.

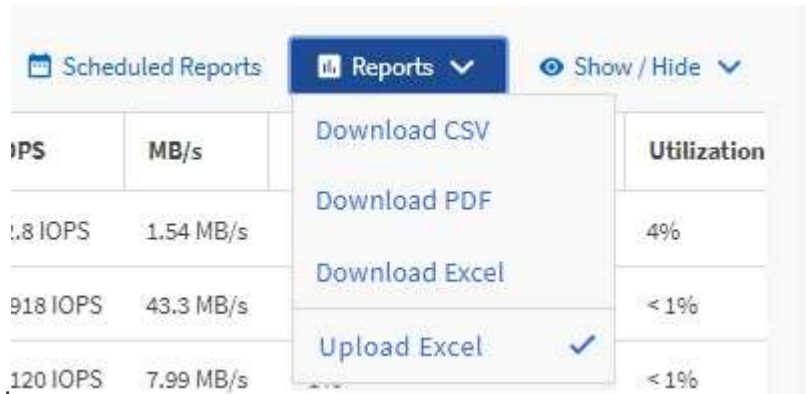
xlsx 확장자를 가진 **Excel** 통합 문서 파일만 업로드할 수 있습니다.

예를 들어, 보고서에서 사용할 수 있는 고급 Excel 기능은 다음과 같습니다.

- 다중 열 정렬

- 복잡한 필터링
- 피벗 테이블
- 차트

- 다운로드한 Excel 파일은 저장된 이름이 아닌, 보기의 기본 파일 이름을 사용합니다.
 - 형식은 다음과 같습니다 <View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx.
 - 예를 들어, 사용자 정의 저장된 뷰는 다음과 같습니다. Volumes-not online 파일 이름이 있습니다 health-volumes-05-May-2020-19-18-00.xlsx 해당 날짜와 시간에 저장했다면.
- Excel 파일에 시트를 추가할 수 있지만, 기존 시트는 변경할 수 없습니다.
 - 기존 시트, 데이터 및 정보를 변경하지 마세요. 대신, 새로 만든 페이지에 데이터를 복사하세요.
 - 위 규칙의 한 가지 예외는 "데이터" 페이지에서 수식을 만들 수 있다는 것입니다. 데이터 페이지 수식을 사용하여 새 페이지에 차트를 만듭니다.
 - 새로운 시트 데이터나 정보에 이름을 지정하지 마세요.
- 사용자 정의된 Excel 파일이 있는 경우 보고서 > **Excel** 업로드 메뉴 항목 옆에 체크 표시가 있습니다. Excel 파일을 다운로드하면 사용자 정의가 적용된 버전이 사용됩니다



단계

1. 보고서의 기준으로 사용할 기본, 사용자 지정 또는 저장된 보기를 엽니다.
2. 보고서 > *Excel 다운로드*를 선택합니다.
3. 파일을 저장합니다. 해당 파일은 다운로드 폴더에 저장됩니다.
4. 저장된 파일을 Excel에서 엽니다. 파일을 새 위치로 옮기지 마세요. 다른 위치에서 작업하는 경우 파일을 업로드하기 전에 원래 파일 이름을 사용하여 원래 위치에 파일을 다시 저장하세요.
5. 복잡한 정렬, 계층형 필터, 피벗 테이블 또는 차트와 같은 Excel 기능을 사용하여 파일을 사용자 지정합니다. 자세한 내용은 Microsoft® Excel 설명서를 참조하세요.
6. 보고서 > *Excel 업로드*를 선택하고 수정한 파일을 선택합니다. 가장 최근에 다운로드한 파일이 동일한 파일 위치에서 업로드됩니다.
7. 예약 보고서 기능을 사용하여 자신에게 테스트 보고서를 보내보세요.

보고서 다운로드

보고서를 다운로드하고 해당 데이터를 쉼표로 구분된 값(CSV) 파일, Microsoft Excel(.XLSX) 파일 또는 PDF 파일로 로컬 또는 네트워크 드라이브에 저장할 수 있습니다. Microsoft Excel과 같은 스프레드시트 응용 프로그램을 사용하면 CSV 및 XLSX 파일을 열 수 있으며, Adobe Acrobat과 같은 리더를 사용하면 PDF 파일을 열 수 있습니다.

단계

1. 보고서 버튼을 클릭하면 다음 중 하나의 보고서를 다운로드할 수 있습니다.

선택하다	에게...
CSV 다운로드	보고서를 쉼표로 구분된 값(CSV) 파일로 저장합니다.
PDF 다운로드	보고서를 .pdf 파일로 저장합니다.
엑셀 다운로드	보고서를 Microsoft Excel(XLSX) 파일로 저장합니다.

일정 보고서

보고서로 재사용하고 공유하려는 뷰가 있으면 Active IQ Unified Manager 사용하여 일정을 예약할 수 있습니다. 예약된 보고서를 관리하고, 각 보고서 일정에 대한 수신자와 배포 빈도를 변경할 수 있습니다.

Unified Manager에서 대부분의 뷰나 인벤토리 페이지를 예약할 수 있습니다. 예외는 이벤트입니다. 이벤트는 CSV 파일로 다운로드할 수 있는 보고서이지만 재생성 및 공유를 위해 이벤트를 예약할 수는 없습니다. 대시보드, 즐겨찾기 또는 구성 페이지를 다운로드하거나 예약할 수도 없습니다.

Active IQ Unified Manager 9.8부터 Microsoft® Excel 형식으로 뷰를 다운로드하여 사용자 지정할 수 있습니다. 복잡한 정렬, 계층형 필터, 피벗 테이블, 차트 등 고급 Excel 기능을 사용할 수 있습니다. 만족스러운 Excel 보고서가 만들어지면 보고서를 예약하고 공유할 때마다 사용할 수 있도록 Excel 파일을 업로드할 수 있습니다.

기본 제공 뷰나 사용자 정의 뷰를 예약할 수 있습니다. CSV, PDF 또는 XSLX 중에서 보낼 파일 형식을 선택할 수 있습니다. 처음으로 보고서를 예약할 때 보고서를 다운로드하고 해당 보고서를 볼 수 있는 유일한 수신자로 자신을 지정할 수 있습니다. 그러면 다른 수신자들도 보고서를 볼 수 있습니다.

보고서 예약

정기적으로 생성하고 배포할 뷰나 Excel 파일이 있으면 보고서를 예약할 수 있습니다.

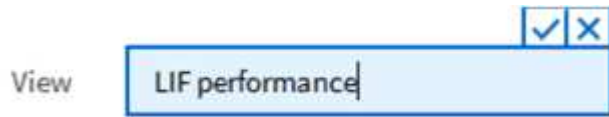
시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 보고 엔진이 Unified Manager 서버의 수신자 목록에 보고서를 이메일 첨부 파일로 보낼 수 있도록 일반 > 알림 페이지에서 SMTP 서버 설정을 구성해야 합니다.
- 생성된 이메일에 첨부 파일을 함께 보낼 수 있도록 이메일 서버를 구성해야 합니다.

다음 단계에 따라 뷰에 대한 보고서 생성을 테스트하고 예약하세요. 사용할 보기를 선택하거나 사용자 정의하세요. 다음 절차에서는 네트워크 인터페이스의 성능을 보여주는 네트워크 보기를 사용하지만 원하는 보기를 사용할 수 있습니다.

단계

1. 시야를 넓히세요. 이 예제에서는 LIF 성능을 보여주는 기본 네트워크 보기를 사용합니다. 왼쪽 탐색 창에서 *네트워크 > 네트워크 인터페이스*를 클릭합니다.
2. 기본 제공 Unified Manager 기능을 사용하여 필요에 따라 보기를 사용자 정의하세요.
3. 보기를 사용자 지정한 후 보기 필드에 고유한 이름을 입력하고 확인 표시를 클릭하여 저장할 수 있습니다.



4. Microsoft® Excel의 고급 기능을 사용하여 보고서를 사용자 지정할 수 있습니다. 자세한 내용은 다음을 참조하세요. ["Excel을 사용하여 보고서 사용자 지정"](#).
5. 일정을 예약하거나 공유하기 전에 출력을 확인하려면 다음을 수행하세요.

옵션	설명
Excel 을 사용하여 보고서를 사용자 지정한 경우	기존에 다운로드한 Excel 파일을 봅니다.
보고서를 사용자 정의하기 위해 Excel 을 사용하지 않은 경우	보고서를 CSV , PDF 또는 XLSX 파일로 다운로드하세요.

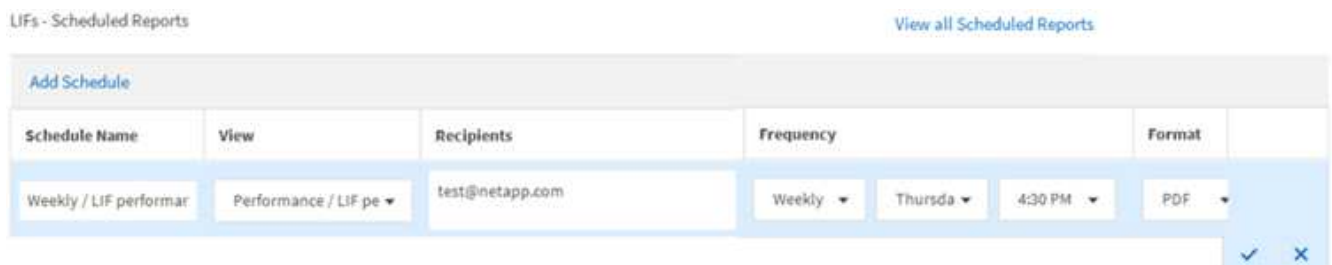
Microsoft Excel(CSV/XSLX)이나 Adobe Acrobat(PDF) 등 설치된 애플리케이션으로 파일을 엽니다.

6. 보고서에 만족하면 *예약된 보고서*를 클릭하세요.
7. 보고서 일정 페이지에서 *일정 추가*를 클릭합니다.
8. 보기 이름과 빈도를 조합한 기본 이름을 사용하거나 *일정 이름*을 사용자 정의합니다.
9. 예약된 보고서를 처음 테스트하려면 본인을 *수신자*로 추가하기만 하면 됩니다. 만족스러우면 모든 보고서 수신자의 이메일 주소를 추가합니다.
10. 보고서가 생성되어 수신자에게 전송되는 빈도를 지정합니다. 매일, 매주, 매월 중에서 선택할 수 있습니다.
11. **PDF**, **CSV**, **XSLX** 중에서 형식을 선택하세요.



Excel을 사용하여 콘텐츠를 사용자 지정한 보고서의 경우 항상 *XSLX*를 선택하세요.

12. 체크 표시를 클릭하세요 (✓) 보고서 일정을 저장합니다.



보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 예약된 빈도에 따라 등록된 수신자에게 이메일로 전송됩니다.

가져온 .rptdesign 보고서 일정

Unified Manager의 이전 릴리스에서 생성되어 가져온 기존 보고서를 예약할 수 있습니다.

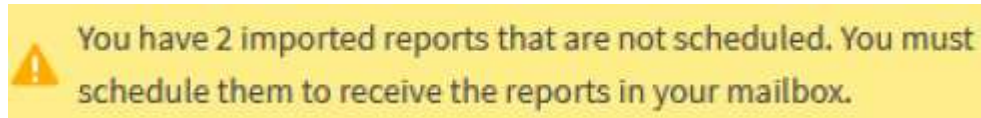
가져온 보고서를 예약하려면 다음이 필요합니다.

- 이전 Unified Manager 릴리스에서 가져온 BIRT 디자인 .rptdesign 파일 보고서
- Unified Manager 9.6 GA 이상으로 업그레이드할 때 적용 가능

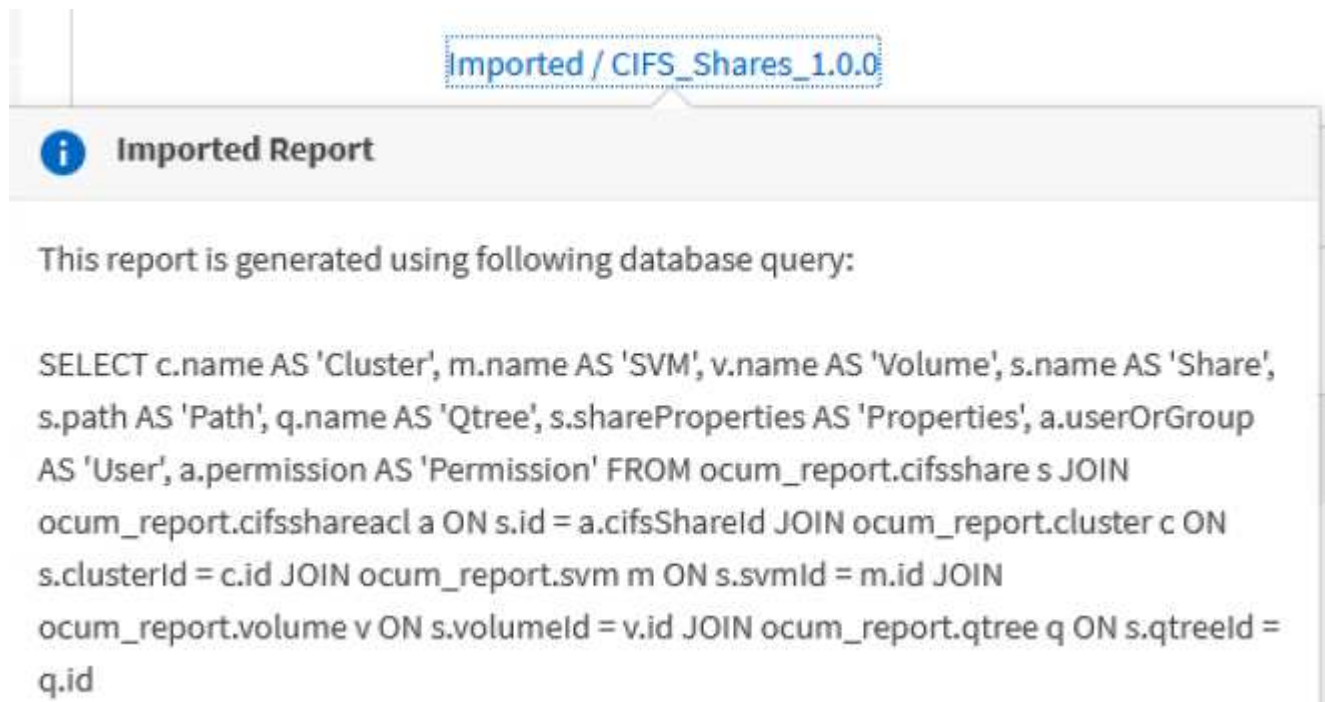
Unified Manager 9.6 GA 이상으로 업그레이드한 후 보고서 일정 페이지에 가져온 보고서가 나열됩니다. 이러한 보고서의 일정을 편집하여 수신자 이메일 주소, 빈도, 형식(PDF 또는 CSV)을 지정할 수 있습니다. 그렇지 않으면 이러한 보고서를 Unified Manager UI에서 편집하거나 볼 수 없습니다.

단계

1. 보고서 일정 페이지를 엽니다. 보고서를 가져온 경우 메시지가 나타납니다.



2. 보기 이름을 클릭하면 보고서 생성에 사용되는 SQL 쿼리가 표시됩니다.



3. 더 많은 아이콘을 클릭하세요  , *편집*을 클릭하고 보고서 일정 세부 정보를 정의한 다음 보고서를 저장합니다.



또한 더 보기 아이콘에서 원치 않는 보고서를 삭제할 수도 있습니다.  .

보고서 일정 관리

보고서 일정 페이지에서 보고서 일정을 관리할 수 있습니다. 기존 일정을 보고, 수정하고, 삭제할 수 있습니다.



시작하기 전에
보고서 일정 페이지에서는 새 보고서를 예약할 수 없습니다. 예약된 보고서는 객체 인벤토리 페이지에서만 추가할 수 있습니다.

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *보고서 일정*을 클릭합니다.
2. 보고서 일정 페이지에서:

만약 당신이 원한다면...	그 다음에...
기존 일정 보기	스크롤 막대와 페이지 컨트롤을 사용하여 기존 보고서 목록을 스크롤합니다.
기존 일정 편집	a. 더 많은 아이콘을 클릭하세요 사용하려는 일정에 맞게. b. *편집*을 클릭하세요. c. 필요한 변경 사항을 적용합니다. d. 변경 사항을 저장하려면 확인 표시를 클릭하세요.
기존 일정 삭제	a. 더 많은 아이콘을 클릭하세요 사용하려는 일정에 맞게. b. *삭제*를 클릭하세요. c. 결정을 확인하세요.

예약된 보고서 편집

보고서가 예약된 후, 보고서 일정 페이지에서 보고서를 편집할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *보고서 일정*을 클릭합니다.

Scheduled Reports ?

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Search Scheduled Reports					
Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	⋮
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	⋮
Weekly / LIF performance	Performance / LIF performance	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	⋮



적절한 권한이 있다면 시스템에서 보고서와 일정을 변경할 수 있습니다.

2. 더 많은 아이콘을 클릭하세요 ⋮ 변경하고 싶은 일정에 맞게.
3. *편집*을 클릭하세요.
4. 보고서 일정의 일정 이름, 수신자 목록, 빈도 및 *형식*을 변경할 수 있습니다.
5. 완료되면 체크 표시를 클릭하여 변경 사항을 저장하세요.

예약된 보고서 삭제

보고서가 예약된 후 보고서 일정 페이지에서 보고서를 삭제할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *보고서 일정*을 클릭합니다.

Scheduled Reports ?

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Search Scheduled Reports					
Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	⋮
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	⋮
Weekly / LIF performance	Performance / LIF performance	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	⋮



적절한 권한이 있다면 시스템에서 모든 보고서와 일정을 제거할 수 있습니다.

2. 더 많은 아이콘을 클릭하세요 ⋮ 제거하려는 일정에 대해.
3. *삭제*를 클릭하세요.
4. 결정을 확인하세요.

예약된 보고서는 목록에서 제거되고 더 이상 설정된 일정에 따라 생성 및 배포되지 않습니다.



인벤토리 페이지에서 사용자 지정 보기를 삭제하면 해당 보기를 사용하는 사용자 지정 Excel 파일이나 예약된 보고서도 삭제됩니다.

샘플 사용자 정의 보고서

이러한 샘플 사용자 정의 보고서는 잠재적인 문제를 식별하고 문제가 발생하기 전에 잠재적인 문제에 대응하는 데 일반적으로 사용됩니다.

이 섹션의 보고서 목록은 모든 내용을 담고 있지 않으며 시간이 지남에 따라 늘어날 것입니다. 문서 피드백을 제공하여 이 섹션에 추가할 사용자 정의 보고서를 제안할 수 있습니다.



보고서를 관리하려면 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

클러스터 스토리지 보고서 사용자 정의

이 섹션의 샘플 클러스터 스토리지 보고서는 스토리지 시스템 리소스를 모니터링하는 데 도움이 되는 클러스터 용량에 대한 보고서를 만드는 방법을 이해하는 데 도움이 되는 샘플일 뿐입니다.

클러스터 모델별 용량을 보려면 보고서를 만드세요.

스토리지 시스템 모델을 기반으로 클러스터의 스토리지 용량과 활용도를 분석하는 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계에 따라 클러스터 모델별 용량을 표시하는 사용자 지정 보기를 만든 다음, 해당 보기에 대한 보고서 생성을 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *클러스터*를 클릭합니다.
2. 보기 메뉴에서 용량 > *모든 클러스터*를 선택합니다.
3. 보고서에 원하지 않는 "클러스터 FQDN" 및 "OS 버전" 등의 열을 제거하려면 *표시/숨기기*를 선택합니다.
4. "총 원시 용량", "모델/제품군" 및 세 개의 집계 열을 "클러스터" 열 근처로 끌어다 놓습니다.
5. 클러스터 유형별로 결과를 정렬하려면 "모델/제품군" 열의 상단을 클릭하세요.
6. 뷰가 표시하는 내용을 반영하는 특정 이름(예: "클러스터 모델별 용량")으로 뷰를 저장합니다.
7. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
8. 일정 추가*를 클릭하면 *보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
9. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로

전송됩니다.

보고서에 표시된 결과에 따라 특정 클러스터에 더 많은 용량을 추가하거나 이전 클러스터 모델을 업그레이드할 수 있습니다.

가장 많은 할당되지 않은 **LUN** 용량을 가진 클러스터를 식별하기 위한 보고서를 만듭니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 할당되지 않은 LUN 용량이 가장 많은 클러스터를 표시하는 사용자 지정 보기를 만든 다음, 해당 보기에 대한 보고서 생성을 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *클러스터*를 클릭합니다.
2. 보기 메뉴에서 용량 > *모든 클러스터*를 선택합니다.
3. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
4. "할당되지 않은 LUN 용량" 열을 "HA 쌍" 열 근처로 끕니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 할당되지 않은 LUN 용량이 0.5TB보다 큼.
6. 할당되지 않은 LUN 용량 열의 상단을 클릭하면 할당되지 않은 LUN 용량이 가장 많은 순서대로 결과가 정렬됩니다.
7. 예를 들어 "'할당되지 않은 LUN 용량이 가장 많음'"과 같이 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장하고 확인 표시(✓).
8. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
9. *일정 추가*를 클릭하면 보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
10. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과에 따라 클러스터의 할당되지 않은 LUN 용량을 사용할 수 있습니다.

가장 사용 가능한 용량을 가진 **HA** 쌍을 보려면 보고서를 만듭니다.

새로운 볼륨과 LUN을 프로비저닝할 수 있는 용량이 가장 큰 고가용성(HA) 쌍을 찾는 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 새 볼륨과 LUN을 프로비저닝하기 위해 가장 사용 가능한 용량별로 정렬된 HA 쌍을 표시하는 사용자 지정 보기를 만든 다음, 해당 보기에 대한 보고서 생성을 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *클러스터*를 클릭합니다.
2. 보기 메뉴에서 용량 > *모든 클러스터*를 선택합니다.
3. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
4. "사용되지 않은 총 용량" 열을 "HA 쌍" 열 근처로 끌어다 놓습니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 총 미사용 용량이 0.5TB 이상
6. "사용되지 않은 총 용량" 열의 상단을 클릭하면 사용되지 않은 총 용량이 가장 많은 순서대로 결과가 정렬됩니다.
7. 예를 들어 "'가장 적게 사용된 집계 용량'"과 같이 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장하고 확인 표시(✓).
8. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
9. *일정 추가*를 클릭하면 보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
10. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 토대로 집계 용량을 기준으로 HA 쌍의 균형을 조정할 수 있습니다.

이전 버전의 **ONTAP** 실행하는 노드를 보려면 보고서를 만듭니다.

모든 클러스터 노드에 설치된 ONTAP 소프트웨어 버전을 표시하는 보고서를 만들어서 어떤 노드를 업그레이드해야 하는지 확인할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 이전 버전의 ONTAP 실행하는 노드를 표시하는 사용자 지정 보기를 만든 다음 해당 보기에 대한 보고서 생성을 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *노드*를 클릭합니다.
2. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
3. "OS 버전" 열을 "노드" 열 근처로 끌어다 놓습니다.
4. ONTAP의 가장 오래된 버전별로 결과를 정렬하려면 "OS 버전" 열의 상단을 클릭하세요.
5. 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장합니다(예: "ONTAP 버전별 노드").
6. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
7. *일정 추가*를 클릭하면 보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
8. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 이전 버전의 ONTAP 실행하는 노드를 업그레이드하는 것이 좋습니다.

집계 용량 보고서 사용자 정의

이러한 샘플 사용자 정의 보고서는 집계 스토리지 용량과 관련된 잠재적 문제를 식별하고 대응하는 데 도움이 됩니다.

이 섹션의 보고서는 스토리지 시스템 리소스를 모니터링하는 데 도움이 되는 집계 용량에 대한 보고서를 만드는 방법을 이해하는 데 도움이 되는 샘플일 뿐입니다.

전체 용량에 도달한 집계를 보려면 보고서를 만듭니다.

전체 용량에 도달한 집계를 찾아 보고서를 만들면 용량을 추가하거나 작업 부하를 다른 집계로 이동할 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 전체 용량에 도달한 집계를 표시하는 사용자 지정 보기를 만든 다음, 해당 보기에 대한 보고서가 생성되도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *집계*를 클릭합니다.
2. 보기 메뉴에서 용량 > *모든 집계*를 선택합니다.
3. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
4. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 45일 미만 완료까지 걸리는 일수
5. "최대 용량까지 남은 일수" 열의 상단을 클릭하면 최대 용량까지 남은 일수가 가장 적은 순으로 결과가 정렬됩니다.
6. 예를 들어 "전체 집계 용량까지 남은 일수"와 같이 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장하고 확인 표시(✓).
7. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
8. 일정 추가*를 클릭하면 *보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
9. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 토대로 전체 용량에 도달한 집계의 저장 용량을 늘리는 것이 좋습니다. 또한, 집계 공간이 부족해지는 상황에 대응할 수 있는 시간을 늘려주는 이벤트를 수신할 수 있도록 기본 7일보다 가득 찰 때까지 걸리는 일수 용량 임계값을 늘리는 것이 좋습니다.

80% 이상 채워진 집계를 보려면 보고서를 만듭니다.

80% 이상 채워진 집계를 강조하는 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계에 따라 80% 이상 채워진 집계를 표시하는 사용자 지정 보기를 만든 다음, 해당 보기에 대한 보고서가 생성되도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *집계*를 클릭합니다.
2. 보기 메뉴에서 용량 > *모든 집계*를 선택합니다.
3. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
4. "사용 가능한 데이터 %" 및 "사용된 데이터 %" 열을 "집계" 열 근처로 끌어다 놓습니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 사용된 데이터 %가 80%보다 큼.
6. "사용된 데이터 %" 열의 상단을 클릭하면 결과가 용량 백분율별로 정렬됩니다.
7. 예를 들어 "집계가 가득 차는 중"과 같이 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장하고 확인 표시(✓).
8. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
9. *일정 추가*를 클릭하면 보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
10. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과에 따라 특정 집계에서 일부 데이터를 옮기고 싶을 수도 있습니다.

과도하게 할당된 집계를 보려면 보고서를 만듭니다.

저장 용량과 집계 사용을 분석하고, 과도하게 할당된 집계를 확인하기 위한 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 초과 커밋 임계값을 초과하는 집계를 표시하는 사용자 지정 보기를 만든 다음 해당 보기에 대한 보고서가 생성되도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *집계*를 클릭합니다.
2. 보기 메뉴에서 용량 > *모든 집계*를 선택합니다.
3. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
4. "초과 할당 용량 %" 열을 "집계" 열 근처로 끌어다 놓습니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 *필터 적용*을 클릭합니다.

◦ 초과 할당 용량 %가 100%보다 큼니다.

6. "초과 할당 용량 %" 열의 상단을 클릭하면 결과가 용량 백분율별로 정렬됩니다.
7. 예를 들어 "Aggregates overcommitted"와 같이 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장하고 확인 표시(✓).
8. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
9. *일정 추가*를 클릭하면 보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
10. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과에 따라 집계에 더 많은 용량을 추가하거나 특정 집계에서 일부 데이터를 이동할 수 있습니다.

볼륨 용량 보고서 사용자 정의

이러한 샘플 사용자 정의 보고서는 볼륨 용량 및 성능과 관련된 잠재적 문제를 식별하고 대응하는 데 도움이 됩니다.

스냅샷 자동 삭제가 꺼진 볼륨 중 전체 용량에 근접한 볼륨을 식별하기 위한 보고서를 만듭니다.

스냅샷 자동 삭제 기능을 비활성화한 상태에서 전체 용량에 접근하는 볼륨 목록이 포함된 보고서를 만들 수 있습니다. 결과는 스냅샷 자동 삭제를 구성하려는 볼륨을 식별하는 데 도움이 될 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

아래 단계에 따라 필요한 열을 올바른 순서로 표시하는 사용자 지정 보기를 만든 다음, 해당 보기에 대한 보고서 생성을 예약하세요.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 용량 > *모든 볼륨*을 선택합니다.
3. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
4. "스냅샷 자동 삭제" 및 "전체 삭제까지 걸리는 일수" 열을 "사용 가능한 데이터 용량" 열 근처로 끌어다 놓습니다.
5. 필터 아이콘을 클릭하고 다음 두 개의 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 완료까지 걸리는 일수 30일 미만
 - 스냅샷 자동 삭제가 비활성화되었습니다
6. 완전 예약까지 남은 일수 열의 상단을 클릭하면 남은 일수가 가장 적은 볼륨이 목록 상단에 표시됩니다.
7. 뷰가 보여주는 내용을 반영하는 특정 이름으로 뷰를 저장합니다(예: "볼륨이 최대 용량에 가까워짐").
8. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
9. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 볼륨에서 스냅샷 자동 삭제를 활성화하거나 사용 가능한 공간을 늘릴 방법을 찾을 수 있습니다.

씬 프로비저닝이 비활성화된 볼륨에서 사용되는 공간을 식별하기 위한 보고서 생성

볼륨이 씬 프로비저닝되지 않은 경우 볼륨이 생성될 때 정의된 디스크 공간의 전체 양을 차지합니다. 씬 프로비저닝이 비활성화된 볼륨을 식별하면 특정 볼륨에서 씬 프로비저닝을 활성화할지 여부를 결정하는 데 도움이 됩니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

아래 단계에 따라 필요한 열을 올바른 순서로 표시하는 사용자 지정 보기를 만든 다음, 해당 보기에 대한 보고서 생성을 예약하세요.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 용량 > *모든 볼륨*을 선택합니다.
3. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
4. "사용된 데이터 %" 및 "씬 프로비저닝" 열을 "사용 가능한 데이터 용량" 열 근처로 끌어다 놓습니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가합니다. *씬 프로비저닝*은 *아니요*이고, *필터 적용*을 클릭합니다.
6. "사용된 데이터 %" 열의 상단을 클릭하면 결과가 정렬되어 볼륨 중 백분율이 가장 높은 순서로 목록 상단에 표시됩니다.
7. 뷰가 표시하는 내용을 반영하는 이름으로 뷰를 저장합니다(예: "Vols no thin provisioning").
8. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
9. 일정 추가*를 클릭하면 *보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
10. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과에 따라 특정 볼륨에서 씬 프로비저닝을 활성화할 수 있습니다.

FabricPool 집계에서 클라우드 계층으로 데이터를 이동해야 하는 볼륨을 식별하기 위한 보고서를 만듭니다.

현재 FabricPool 집계에 있는 볼륨 목록, Tier 클라우드 권장 사항, 대량의 콜드 데이터가 포함된 보고서를 만들 수 있습니다. 이 보고서는 더 많은 콜드(비활성) 데이터를 클라우드 계층으로 오프로드하기 위해 특정 볼륨의 계층화 정책을 "auto" 또는 "all"로 변경해야 하는지 결정하는 데 도움이 될 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- FabricPool 집계를 구성하고 해당 집계에 볼륨이 있어야 합니다.

아래 단계에 따라 필요한 열을 올바른 순서로 표시하는 사용자 지정 보기를 만든 다음, 해당 보기에 대한 보고서 생성을 예약하세요.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 성능 > *모든 볼륨*을 선택합니다.
3. 열 선택기에서 "디스크 유형" 열이 보기에 나타나는지 확인하세요.

보고서에 중요한 뷰를 만들려면 다른 열을 추가하거나 제거하세요.

4. "디스크 유형" 열을 "클라우드 권장 사항" 열 근처로 끌어다 놓습니다.
5. 필터 아이콘을 클릭하고 다음 세 가지 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 디스크 유형에 FabricPool 포함되어 있습니다.
 - 클라우드 추천에는 계층이 포함되어 있습니다.
 - 10GB 이상의 콜드 데이터

Disk Types	contains	fabricpool	
Cloud Recommendation	contains	tier	
Cold Data	greater than	10	GB

+ Add Filter

Reset **Cancel** **Apply Filter**

6. 콜드 데이터 열의 상단을 클릭하면 가장 많은 콜드 데이터가 있는 볼륨이 보기의 맨 위에 표시됩니다.
7. 뷰가 표시하는 내용을 반영하는 이름으로 뷰를 저장합니다(예: "Vols change tiering policy").

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View

Vols change tiering policy

Search Volumes

3

Assign Performance Threshold Policy		Clear Performance Threshold Policy		Schedule Report		
Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
nfs_vol4	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagnfsdst	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

- 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
- *일정 추가*를 클릭하면 보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
- 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 기반으로 시스템 관리자나 ONTAP CLI를 사용하여 특정 볼륨의 계층화 정책을 "auto" 또는 "all"로 변경하여 더 많은 콜드 데이터를 클라우드 계층으로 오프로드할 수 있습니다.

Qtree 용량 보고서 사용자 정의

이러한 샘플 사용자 정의 보고서는 Qtree 용량과 관련된 잠재적 문제를 식별하고 대응하는 데 도움이 됩니다.

거의 가득 찬 **Qtree**를 보려면 보고서를 만드세요.

Qtree의 저장 용량과 활용도를 분석하고, 거의 가득 찬 Qtree를 볼 수 있는 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 거의 가득 찬 Qtree를 표시하는 사용자 지정 보기를 만든 다음 해당 보기에 대한 보고서가 생성되도록 예약합니다.

단계

- 왼쪽 탐색 창에서 저장소 > *Qtrees*를 클릭합니다.
- 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
- "디스크 사용 %" 열을 "Qtrees" 열 근처로 끌어다 놓습니다.
- 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 디스크 사용률(%)이 75%보다 큼.

5. "디스크 사용률 %" 열의 상단을 클릭하면 결과가 용량 백분율별로 정렬됩니다.
6. 예를 들어 "Qtrees nearing full"과 같이 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장하고 확인 표시(✓).
7. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
8. 일정 추가*를 클릭하면 *보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
9. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과에 따라 디스크 하드 및 소프트 한도(설정된 경우)를 조정하거나 Q트리 전체에서 데이터의 균형을 맞출 수 있습니다.

NFS 공유 보고서 사용자 정의

스토리지 시스템의 볼륨에 대한 NFS 내보내기 정책 및 규칙에 대한 정보를 분석하기 위해 NFS 공유 보고서를 사용자 정의할 수 있습니다. 예를 들어, 액세스할 수 없는 마운트 경로가 있는 볼륨과 기본 내보내기 정책이 있는 볼륨을 표시하도록 보고서를 사용자 지정할 수 있습니다.

접근할 수 없는 마운트 경로가 있는 볼륨을 보려면 보고서를 만듭니다.

접근할 수 없는 마운트 경로가 있는 볼륨을 찾기 위해 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 액세스할 수 없는 마운트 경로가 있는 볼륨에 대한 사용자 지정 보기를 만든 다음 해당 보기에 대한 보고서 생성을 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *NFS 공유*를 클릭합니다.
2. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
3. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 마운트 경로가 활성화되어 있지 않습니다.
4. 예를 들어 "액세스할 수 없는 마운트 경로가 있는 볼륨"과 같이 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장하고 확인 표시(✓).
5. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
6. *일정 추가*를 클릭하면 보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
7. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 토대로, 접근할 수 없는 마운트 경로를 수정하는 것이 좋습니다.

기본 내보내기 정책을 사용하는 볼륨을 보려면 보고서를 만듭니다.

기본 내보내기 정책을 사용하는 볼륨을 찾기 위해 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계에 따라 기본 내보내기 정책을 사용하는 볼륨에 대한 사용자 지정 보기를 만든 다음, 해당 보기에 대한 보고서 생성을 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *NFS 공유*를 클릭합니다.
2. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
3. “내보내기 정책” 열을 “볼륨” 열 근처로 끌어다 놓습니다.
4. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 내보내기 정책에는 기본값이 포함되어 있습니다.
5. 예를 들어 "기본 내보내기 정책이 있는 볼륨"과 같이 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장하고 확인 표시(✓).
6. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
7. *일정 추가*를 클릭하면 보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
8. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과에 따라 사용자 지정 내보내기 정책을 구성할 수 있습니다.

스토리지 VM 보고서 사용자 정의

볼륨 정보를 분석하고 전반적인 상태와 스토리지 가용성을 확인하기 위해 스토리지 VM 보고서를 만들 수 있습니다. 예를 들어, 최대 볼륨 수에 도달한 SVM을 표시하고 중지된 SVM을 분석하는 보고서를 만들 수 있습니다.

최대 볼륨 제한에 도달한 스토리지 VM을 보려면 보고서를 만듭니다.

최대 볼륨 한도에 도달한 SVM을 찾기 위한 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 최대 볼륨 제한에 도달한 스토리지 VM을 표시하는 사용자 지정 보기를 만든 다음 해당 보기에 대한 보고서 생성을 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *저장소 VM*을 클릭합니다.

2. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
3. "볼륨 수" 및 "허용되는 최대 볼륨" 열을 "저장소 VM" 열 근처로 끌어다 놓습니다.
4. 최대 허용 볼륨 열의 상단을 클릭하면 볼륨 수가 가장 많은 순으로 결과가 정렬됩니다.
5. 예를 들어 "SVM이 최대 볼륨에 도달함"과 같이 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장하고 확인 표시(✓).
6. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
7. 일정 추가*를 클릭하면 *보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
8. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과에 따라 스토리지 VM에 할당된 볼륨의 균형을 조정하거나, 가능하다면 ONTAP 시스템 관리자를 사용하여 허용되는 최대 볼륨을 변경할 수 있습니다.

중지된 스토리지 **VM**을 보려면 보고서를 만듭니다.

중지된 모든 SVM 목록을 표시하는 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계에 따라 중지된 스토리지 VM을 표시하는 사용자 지정 보기를 만든 다음, 해당 보기에 대한 보고서 생성을 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *저장소 VM*을 클릭합니다.
2. 보기 메뉴에서 상태 > *모든 저장소 VM*을 선택합니다.
3. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
4. "상태" 열을 "저장소 VM" 열 근처로 끕니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 상태가 중지되었습니다
6. 예를 들어 "중지된 SVM"과 같이 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장하고 확인 표시(✓).
7. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
8. 일정 추가*를 클릭하면 *보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
9. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 SVM이 중지된 이유를 조사하여 중지된 SVM을 다시 시작해야 하는지 확인할 수 있습니다.

볼륨 관계 보고서 사용자 정의

볼륨 관계 인벤토리 보고서를 사용하면 클러스터의 스토리지 인벤토리 세부 정보를 분석하고, 볼륨에 필요한 보호 수준을 파악하고, 오류 소스, 패턴 및 일정을 기준으로 볼륨 세부 정보를 필터링할 수 있습니다.

실패 소스별로 볼륨 관계를 그룹화하는 보고서를 만듭니다.

관계가 좋지 않은 상태에 있는 이유에 따라 볼륨을 그룹화하는 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 실패 소스별로 볼륨을 그룹화하는 사용자 지정 보기를 만든 다음 해당 보기에 대한 보고서가 생성되도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 관계 > *모든 관계*를 선택합니다.
3. *표시/숨기기*를 선택하여 "관계 건강" 및 "건강하지 못한 이유" 열이 보기에 나타나도록 합니다.

보고서에 중요한 뷰를 만들려면 다른 열을 추가하거나 제거하세요.

4. "관계 건강" 및 "건강하지 못한 이유" 열을 "상태" 열 근처로 끕니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 관계 건강이 나쁘다
6. "건강에 해로운 이유" 열의 상단을 클릭하여 실패 원인별로 볼륨 관계를 그룹화합니다.
7. 뷰가 보여주는 내용을 반영하는 특정 이름으로 뷰를 저장합니다(예: "'실패에 따른 볼륨 관계').
8. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
9. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 각 유형의 실패의 출처와 영향을 조사할 수 있습니다.

문제별로 볼륨 관계를 그룹화하는 보고서를 만듭니다.

문제별로 볼륨 관계를 그룹화한 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 문제별로 볼륨 관계를 그룹화하는 사용자 지정 보기를 만든 다음 해당 보기에 대한 보고서가 생성되도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 관계 > *모든 관계*를 선택합니다.
3. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
4. "건강에 해로운 이유" 열을 "상태" 열 근처로 끌어다 놓습니다.
5. "건강에 해로운 이유" 열의 상단을 클릭하여 문제별로 볼륨을 그룹화합니다.
6. 보기가 보여주는 내용을 반영하는 특정 이름으로 보기를 저장합니다(예: "문제별 볼륨 관계").
7. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
8. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 각 유형의 문제의 근원과 영향을 조사할 수 있습니다.

특정 시간 간격의 볼륨 전송 추세를 보려면 보고서를 만드세요.

특정 시간 간격으로 볼륨 이동 추세를 표시하는 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계에 따라 특정 시간 간격으로 볼륨에 대한 사용자 지정 보기를 만든 다음 해당 보기에 대한 보고서가 생성되도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 관계 > *지난 1개월 전송 상태*를 선택합니다.
3. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
4. 전송 기간 열을 "운영 결과" 열 근처로 끌어다 놓습니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 지난 7일 동안의 전송 종료 시간
6. "전송 기간" 열의 상단을 클릭하여 볼륨을 시간 간격으로 정렬합니다.
7. 예를 들어 "기간별 볼륨"과 같이 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장합니다.
8. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
9. 보고서 일정에 대한 이름을 입력하고 빈도를 *주간*으로 설정한 다음 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 전송 시간 간격을 조사할 수 있습니다.

실패 또는 성공한 볼륨 전송을 보려면 보고서를 만드세요.

볼륨 전송 상태를 표시하는 보고서를 만들 수 있습니다. 이 보고서에서는 실패한 볼륨 전송과 성공한 볼륨 전송을 모두 볼 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계에 따라 실패한 전송과 성공한 전송을 보여주는 사용자 지정 보기를 만든 다음, 해당 보기에 대한 보고서가 생성되도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 관계 > *지난 1개월 전송 상태*를 선택합니다.
3. 보고서에 포함하지 않을 열을 제거하려면 *표시/숨기기*를 선택하세요.
4. "작업 결과" 열을 "상태" 열 근처로 끌어다 놓습니다.
5. "작업 결과" 열의 상단을 클릭하여 볼륨을 상태별로 정렬합니다.
6. 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장합니다(예: "전송 상태별 볼륨").
7. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
8. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 전송 상태를 조사할 수 있습니다.

전송 크기에 따라 볼륨 전송을 보려면 보고서를 만듭니다.

전송 크기에 따라 볼륨 전송을 볼 수 있는 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계에 따라 전송 크기에 따라 볼륨 전송에 대한 사용자 지정 보기를 만든 다음, 해당 보기에 대한 보고서가 생성되도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 관계 > *지난 1개월 이체율*을 선택합니다.
3. "총 전송 크기" 열의 상단을 클릭하여 볼륨 전송을 크기별로 정렬합니다.
4. 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장합니다(예: "전송 크기별 볼륨").
5. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
6. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 전송 크기에 따른 볼륨 관계를 조사할 수 있습니다.

일별로 그룹화된 볼륨 전송을 보려면 보고서를 만드세요.

일별로 그룹화된 볼륨 이동을 볼 수 있는 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계에 따라 일별로 그룹화된 볼륨 전송에 대한 사용자 지정 보기를 만든 다음, 해당 보기에 대한 보고서가 생성되도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 관계 > *지난 1개월 이체율*을 선택합니다.
3. "일" 열의 상단을 클릭하면 일별로 거래량 이전을 정렬할 수 있습니다.
4. 보기가 표시하는 내용을 반영하는 특정 이름으로 보기를 저장합니다(예: "일별 볼륨 전송").
5. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
6. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 일별 거래량 이동을 조사할 수 있습니다.

볼륨 성능 보고서 사용자 정의

이러한 샘플 사용자 정의 보고서는 볼륨 성능과 관련된 잠재적 문제를 식별하고 대응하는 데 도움이 됩니다.

FabricPool 활성화되지 않은 집계에서 많은 양의 콜드 데이터가 포함된 볼륨을 보려면 보고서를 만듭니다.

FabricPool 아닌 집계에서 콜드 데이터의 양이 많은 볼륨을 표시하는 보고서를 만들 수 있습니다. 이를 통해 FabricPool 집계로 이동해야 하는 볼륨을 식별하는 데 도움이 될 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 FabricPool 활성화되지 않은 집계에서 콜드 데이터가 많은 볼륨에 대한 사용자 지정 보기를 만든 다음 해당 보기에 대한 보고서 생성을 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 성능 > *모든 볼륨*을 선택합니다.
3. *표시/숨기기*를 선택하여 보기에 "디스크 유형" 열이 나타나도록 합니다.

보고서에 중요한 뷰를 만들려면 다른 열을 추가하거나 제거하세요.

4. "디스크 유형" 열을 "콜드 데이터" 열 근처로 끌어다 놓습니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 *필터 적용*을 클릭합니다.
 - 100GB 이상의 콜드 데이터
 - 디스크 유형에 SSD가 포함되어 있습니다.
6. "디스크 유형" 열의 상단을 클릭하여 디스크 유형별로 볼륨을 정렬합니다. 그러면 디스크 유형 SSD(FabricPool)가 맨 아래에 표시됩니다.
7. 뷰가 표시하는 내용을 반영하는 특정 이름으로 뷰를 저장합니다(예: "Cold data vols not FabricPool").
8. 인벤토리 페이지에서 예약된 보고서 버튼을 클릭하세요.
9. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 FabricPool 집계로 옮기기에 적합한 볼륨을 찾을 수 있습니다.

Microsoft Excel 보고서 샘플

이러한 Microsoft Excel 보고서 샘플은 Excel의 고급 기능을 사용하여 사용할 수 있는 보고 옵션을 소개하기 위해 만들어졌습니다.

Excel의 고급 기능을 사용하면 사용자의 요구 사항에 맞는 다양한 보고서를 만들 수 있습니다. Excel 사용 방법에 대한 자세한 내용은 제품 설명서를 참조하세요.



보고서를 관리하려면 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

집계 용량 표와 차트를 보여주는 보고서 만들기

합계와 클러스터형 막대형 차트 형식을 사용하여 Excel 파일에서 용량을 분석하는 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계에 따라 Health: All Aggregates 보기를 열고, Excel에서 보기를 다운로드하고, 사용 가능한 용량 차트를 만들고, 사용자 지정 Excel 파일을 업로드하고, 최종 보고서를 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *집계*를 클릭합니다.

2. 보고서 > *Excel 다운로드*를 선택합니다.



브라우저에 따라 파일을 저장하려면 *확인*을 클릭해야 할 수도 있습니다.

3. 필요한 경우 *편집 활성화*를 클릭하세요.

4. Excel에서 다운로드한 파일을 엽니다.

5. 새 시트 만들기 () 후에 data 시트를 만들고 *총 데이터 용량*이라고 이름을 지정합니다.

6. 새로운 총 데이터 용량 시트에 다음 열을 추가합니다.

- a. 총 데이터 용량(GB)
- b. 약정 용량(GB)
- c. 사용된 데이터 용량(GB)
- d. 사용 가능한 데이터 용량(GB)

7. 각 열의 첫 번째 행에 다음 수식을 입력하고, 데이터 시트(데이터!)를 참조하는지 확인하고, 캡처된 데이터에 대한 올바른 열 및 행 지정자를 참조하는지 확인합니다(총 데이터 용량은 열 E, 행 2~20에서 데이터를 가져옵니다).

- a. =SUM(데이터!E\$2:데이터!E\$20)
- b. =SUM(데이터!F\$2:데이터!F\$50)
- c. =SUM(데이터!G\$2:데이터!G\$50)
- d. =SUM(데이터!H\$2:데이터!H\$50)

이 수식은 현재 데이터를 기준으로 각 열의 합계를 계산합니다.

Total Data Capacity (GB)	Committed Capacity (GB)	Used Data Capacity (GB)	Available Data Capacity (GB)
5380.31	6892.47	11764.27	3911.03

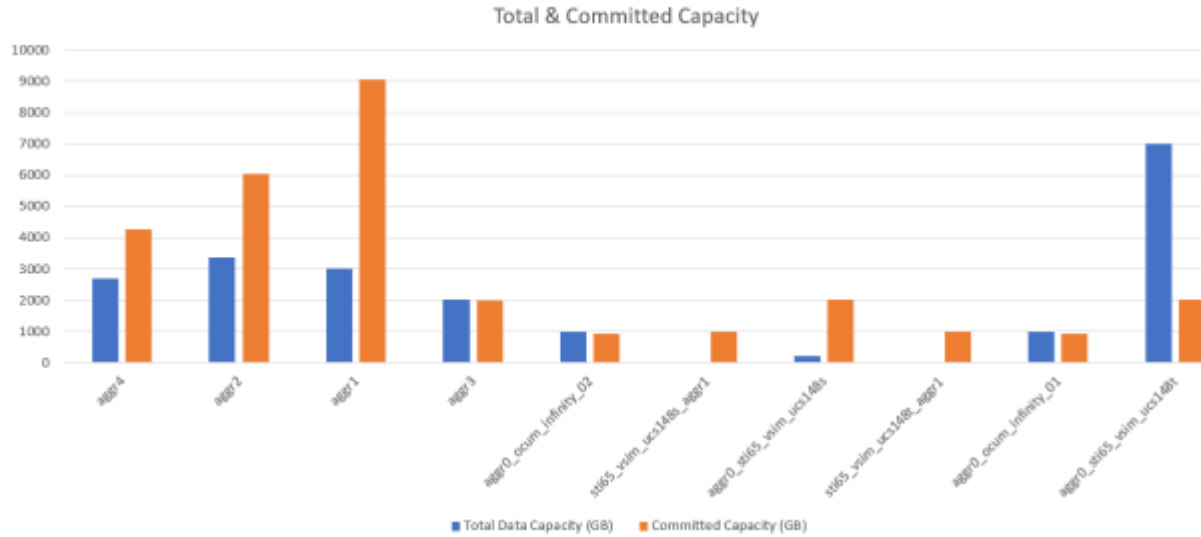
1. 데이터 시트에서 총 데이터 용량(**GB**) 및 약정 용량(**GB**) 열을 선택합니다.

2. 삽입 메뉴에서 *추천 차트*를 선택하고 *묶음 막대형 차트*를 선택합니다.

3. 차트를 마우스 오른쪽 버튼으로 클릭하고 *차트 이동*을 선택하여 차트를 이동합니다. Total Data Capacity 시트.

4. 차트를 선택하면 제공되는 디자인 및 서식 메뉴를 사용하여 차트의 모양을 사용자 지정할 수 있습니다.

5. 만족스러우면 변경 사항을 적용하여 파일을 저장합니다. 파일 이름이나 위치를 변경하지 마세요.



6. Unified Manager에서 보고서 > *Excel 업로드*를 선택합니다.



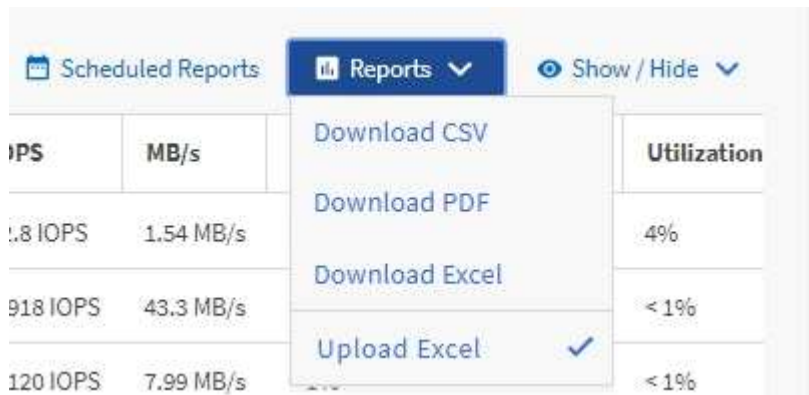
Excel 파일을 다운로드한 것과 같은 보기에 있는지 확인하세요.

7. 수정한 Excel 파일을 선택하세요.

8. *열기*를 클릭하세요.

9. *제출*을 클릭하세요.

보고서 > **Excel** 업로드 메뉴 항목 옆에 체크 표시가 나타납니다.



10. *예약된 보고서*를 클릭합니다.

11. *일정 추가*를 클릭하면 보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.



보고서에 **XLSX** 형식을 선택하세요.

12. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 네트워크 전반에서 사용 가능한 용량을 가장 효과적으로 활용하는 방법을 알아보고 싶을 수도 있습니다.

총합계와 사용 가능한 용량 차트를 보여주는 보고서를 만듭니다.

Excel 차트 형식으로 저장 용량 총량과 약정 용량을 분석하는 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계에 따라 Health: All Aggregates 보기를 열고, Excel에서 보기를 다운로드하고, 총 용량과 약정 용량 차트를 만들고, 사용자 지정 Excel 파일을 업로드하고, 최종 보고서를 예약합니다.

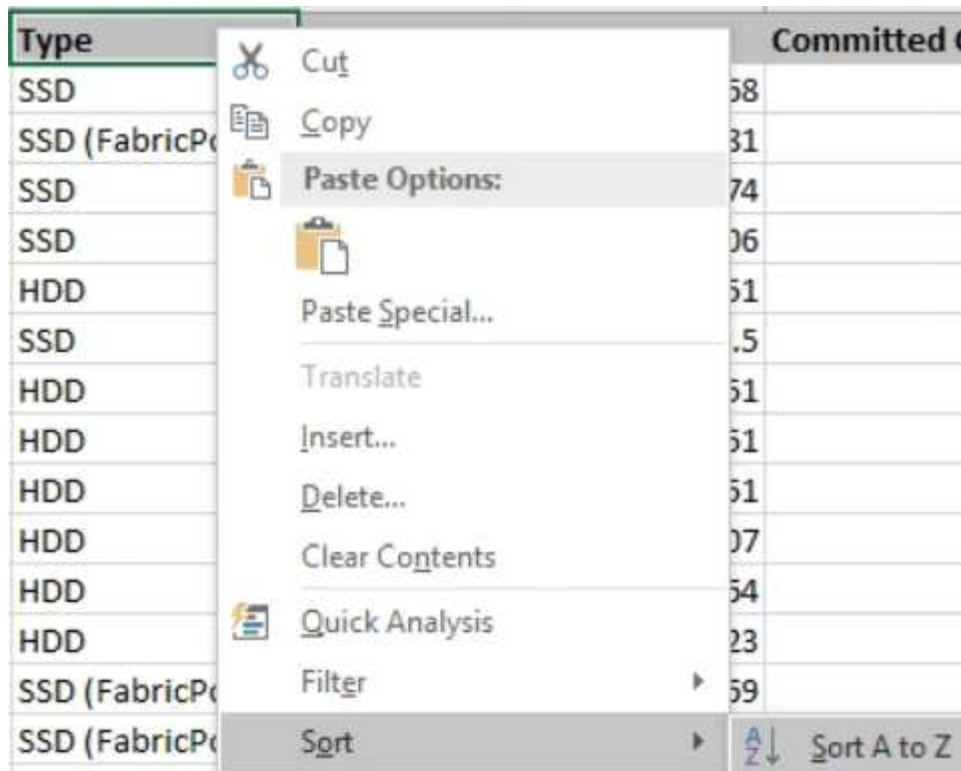
단계

1. 왼쪽 탐색 창에서 저장소 > *집계*를 클릭합니다.
2. 보고서 > *Excel 다운로드*를 선택합니다.



브라우저에 따라 파일을 저장하려면 *확인*을 클릭해야 할 수도 있습니다.

3. Excel에서 다운로드한 파일을 엽니다.
4. 필요한 경우 *편집 활성화*를 클릭하세요.
5. 데이터 시트에서 유형 열을 마우스 오른쪽 버튼으로 클릭하고 정렬 > *A-Z 정렬*을 선택합니다.



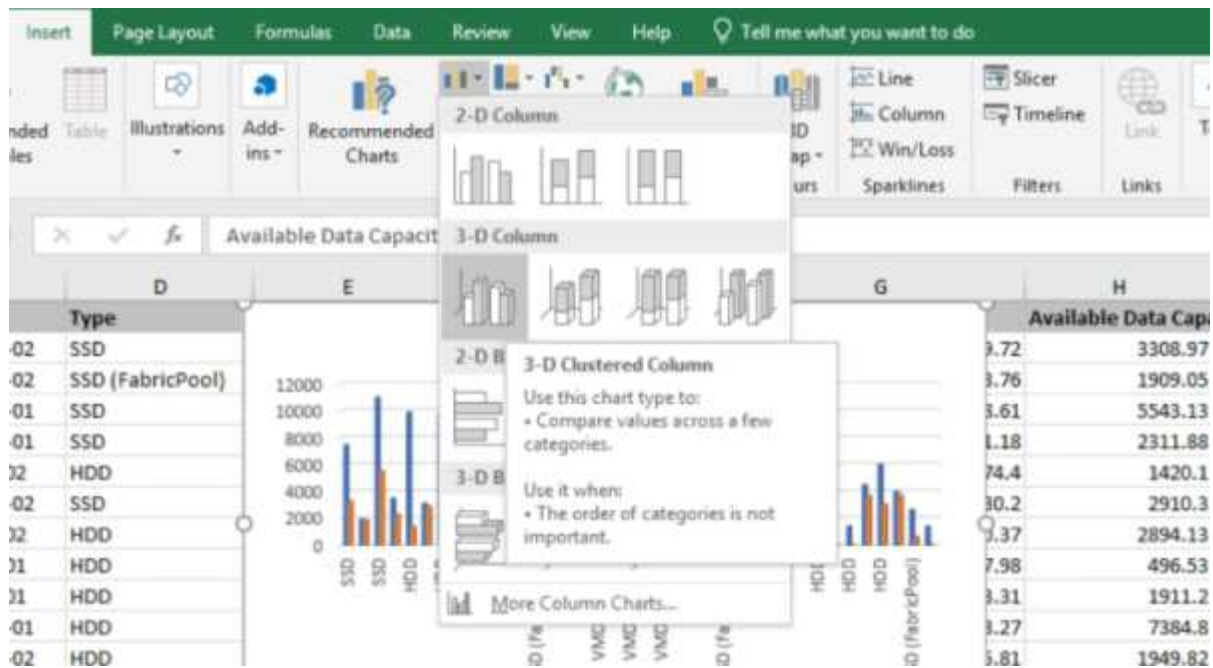
이렇게 하면 다음과 같이 저장 유형별로 데이터가 정렬됩니다.

- 하드디스크
- 잡종
- SSD
- SSD(FabricPool)

6. 선택하세요 Type, Total Data Capacity, 그리고 Available Data Capacity 기둥.

7. 삽입 메뉴에서 다음을 선택하세요. 3-D column 차트.

차트는 데이터 시트에 나타납니다.



8. 차트를 마우스 오른쪽 버튼으로 클릭하고 *차트 이동*을 선택합니다.

9. *새 시트*를 선택하고 시트 이름을 *총 저장 공간 차트*로 지정합니다.

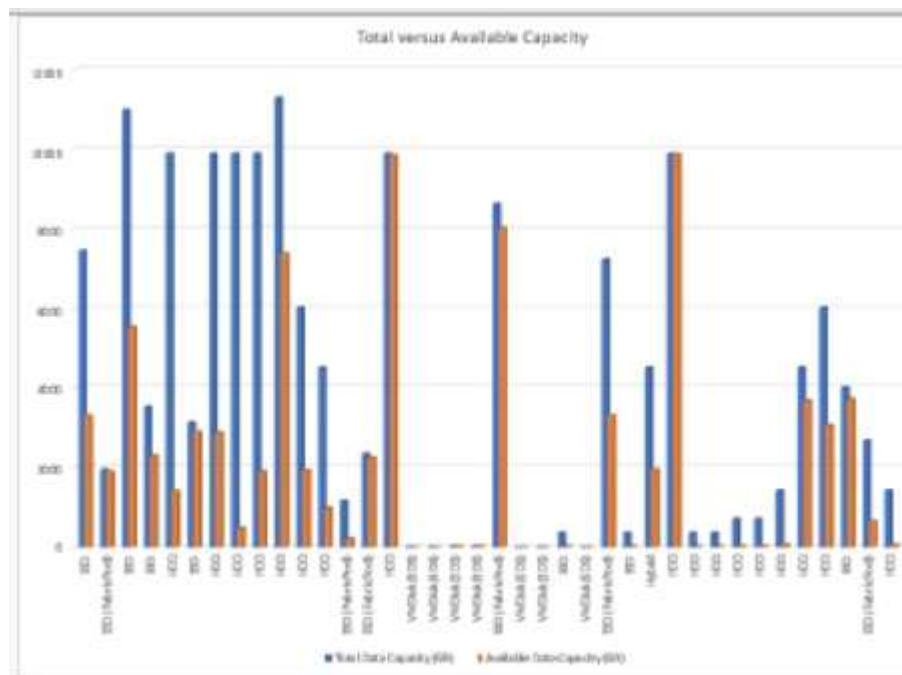


새로운 시트가 정보 및 데이터 시트 뒤에 나타나는지 확인하세요.

10. 차트 제목을 *전체 용량 대비 사용 가능한 용량*으로 지정하세요.

11. 차트를 선택하면 제공되는 디자인 및 서식 메뉴를 사용하여 차트의 모양을 사용자 지정할 수 있습니다.

12. 만족스러우면 변경 사항을 적용하여 파일을 저장합니다. 파일 이름이나 위치를 변경하지 마세요.



13. Unified Manager에서 보고서 > *Excel 업로드*를 선택합니다.



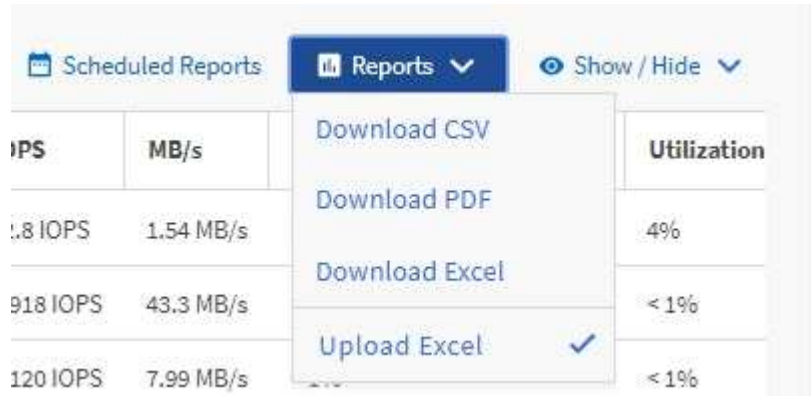
Excel 파일을 다운로드한 것과 같은 보기에 있는지 확인하세요.

14. 수정한 Excel 파일을 선택하세요.

15. *열기*를 클릭하세요.

16. *제출*을 클릭하세요.

보고서 > **Excel** 업로드 메뉴 항목 옆에 체크 표시가 나타납니다.



17. *예약된 보고서*를 클릭합니다.

18. 일정 추가*를 클릭하면 *보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.



보고서에 **XLSX** 형식을 선택하세요.

19. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 집계에 대한 부하를 균형 있게 조정하고 싶을 수 있습니다.

사용 가능한 볼륨 용량 차트를 보려면 보고서를 만드세요.

Excel 차트로 사용 가능한 볼륨 용량을 분석하는 보고서를 만들 수 있습니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계에 따라 Health: All Volumes 보기를 열고, Excel에서 보기를 다운로드하고, 사용 가능한 용량 차트를 만들고, 사용자 지정 Excel 파일을 업로드하고, 최종 보고서를 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보고서 > *Excel 다운로드*를 선택합니다.



브라우저에 따라 파일을 저장하려면 *확인*을 클릭해야 할 수도 있습니다.

3. 필요한 경우 *편집 활성화*를 클릭하세요.
4. Excel에서 다운로드한 파일을 엽니다.
5. 예 data 시트에서 사용할 데이터를 선택하세요. Volume 그리고 Available Data % 열.
6. 삽입 메뉴에서 다음을 선택하세요. 3-D piechart.

차트는 어느 볼륨이 가장 큰 사용 가능한 공간을 가지고 있는지 보여줍니다. 차트는 데이터 시트에 나타납니다.



네트워크 구성에 따라 전체 열을 선택하거나 너무 많은 데이터 행을 선택하면 파이 차트를 읽을 수 없게 될 수 있습니다. 이 샘플에서는 3차원 원형 차트를 사용하지만 다른 차트 유형을 사용할 수도 있습니다. 수집하려는 데이터를 가장 잘 보여주는 차트를 사용하세요.

7. 차트 제목을 *사용 가능한 용량*으로 지정하세요.
8. 차트를 마우스 오른쪽 버튼으로 클릭하고 *차트 이동*을 선택합니다.
9. *새 시트*를 선택하고 시트 이름을 *저장 용량 차트*로 지정합니다.



새로운 시트가 정보 및 데이터 시트 뒤에 나타나는지 확인하세요.



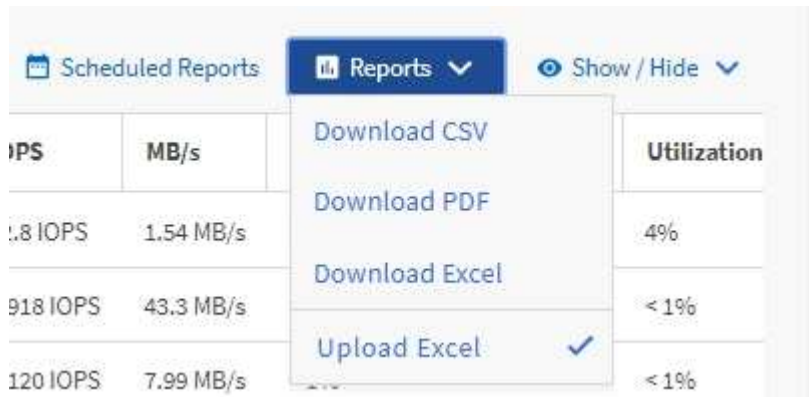
10. 차트를 선택하면 제공되는 디자인 및 서식 메뉴를 사용하여 차트의 모양을 사용자 지정할 수 있습니다.
11. 만족스러우면 변경 사항을 적용하여 파일을 저장합니다.
12. Unified Manager에서 보고서 > *Excel 업로드*를 선택합니다.



Excel 파일을 다운로드한 것과 같은 보기에 있는지 확인하세요.

13. 수정한 Excel 파일을 선택하세요.
14. *열기*를 클릭하세요.
15. *제출*을 클릭하세요.

보고서 > **Excel** 업로드 메뉴 항목 옆에 체크 표시가 나타납니다.



16. *예약된 보고서*를 클릭합니다.
17. 일정 추가*를 클릭하면 *보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
18. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.



보고서에 **XLSX** 형식을 선택하세요.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 볼륨에 대한 부하를 균형 있게 조정하는 것이 좋습니다.

가장 많은 사용 가능한 **IOPS**를 포함하는 집계를 보려면 보고서를 만듭니다.

이 보고서는 새로운 워크로드를 프로비저닝할 수 있는 집계 유형별로 가장 많은 IOPS를 제공하는 집계를 보여줍니다.

시작하기 전에

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계에 따라 Health: All Volumes 보기를 열고, Excel에서 보기를 다운로드하고, 사용 가능한 용량 차트를 만들고, 사용자 지정 Excel 파일을 업로드하고, 최종 보고서를 예약합니다.

단계

1. 왼쪽 탐색 창에서 저장소 > *집계*를 클릭합니다.
2. 보기 드롭다운에서 *성과: 모든 집계*를 선택합니다.
3. *표시/숨기기*를 선택하여 표시하세요. Available IOPS 열을 숨기고 Cluster FQDN, Inactive Data Reporting, 그리고 Threshold Policy 기둥.
4. 드래그 앤 드롭 Available IOPS 그리고 Free Capacity 옆에 있는 열 Type 열.
5. 사용자 정의 보기의 이름을 지정하고 저장합니다. Available IOPS Per Aggr.
6. 보고서 > *Excel 다운로드*를 선택합니다.



브라우저에 따라 파일을 저장하려면 *확인*을 클릭해야 할 수도 있습니다.

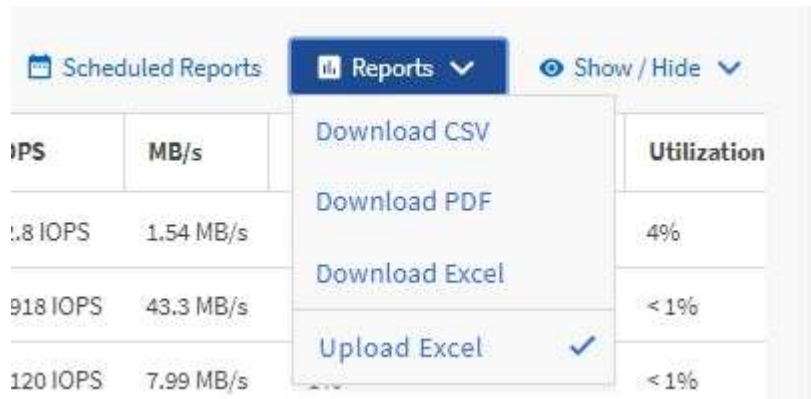
7. 필요한 경우 *편집 활성화*를 클릭하세요.
8. Excel에서 다운로드한 파일을 엽니다.
9. 데이터 시트에서 시트 왼쪽 상단에 있는 작은 삼각형을 클릭하여 시트 전체를 선택합니다.
10. 데이터 리본에서 *정렬*을 선택하세요. Sort & Filter area.
11. 다음 정렬 수준을 설정합니다.
 - a. 정렬 기준*을 다음과 같이 지정하세요. **Available IOPS (IOPS)**, *정렬 기준 Cell Values, 그리고 *주문*은 Largest to Smallest.
 - b. *레벨 추가*를 클릭하세요.
 - c. 정렬 기준*을 다음과 같이 지정하세요. **Type**, *정렬 기준 Cell Values, 그리고 *주문*은 Z to A.
 - d. *레벨 추가*를 클릭하세요.
 - e. 정렬 기준*을 다음과 같이 지정하세요. **Free Capacity (GB)**, *정렬 기준 Cell Values, 그리고 *주문*은 Largest to Smallest.
 - f. *OK*를 클릭하세요.
12. Excel 파일을 저장하고 닫습니다.
13. Unified Manager에서 보고서 > *Excel 업로드*를 선택합니다.



Excel 파일을 다운로드한 것과 같은 보기에 있는지 확인하세요.

14. 이 경우 수정한 Excel 파일을 선택하세요. performance-aggregates-<date>.xlsx.
15. *열기*를 클릭하세요.
16. *제출*을 클릭하세요.

보고서 > **Excel** 업로드 메뉴 항목 옆에 체크 표시가 나타납니다.



17. *예약된 보고서*를 클릭합니다.
18. *일정 추가*를 클릭하면 보고서 일정 페이지에 새 행이 추가되어 새 보고서에 대한 일정 특성을 정의할 수 있습니다.
19. 보고서 일정에 대한 이름을 입력하고 다른 보고서 필드를 완료한 다음 확인 표시(✓) 행의 끝에.



보고서에 **XLSX** 형식을 선택하세요.

보고서는 테스트로 즉시 전송됩니다. 그 후, 보고서가 생성되어 지정된 빈도로 등록된 수신자에게 이메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 사용 가능한 IOPS가 가장 큰 집계에 새로운 워크로드를 프로비저닝할 수 있습니다.

REST API를 사용하여 스토리지 관리

Active IQ Unified Manager REST API 시작하기

Active IQ Unified Manager 타사 통합을 위한 RESTful 웹 서비스 인터페이스를 통해 지원되는 스토리지 시스템의 스토리지 리소스를 관리하는 API 세트를 제공합니다.

이 항목에서는 Unified Manager API, 특정 문제를 해결하기 위한 샘플 워크플로, 몇 가지 샘플 코드에 대한 정보를 찾을 수 있습니다. 이 정보를 사용하면 NetApp 시스템을 관리하기 위한 NetApp Manageability 소프트웨어 솔루션의 RESTful 클라이언트를 만들 수 있습니다. API는 REST(Representational State Transfer) 아키텍처 스타일을 기반으로 합니다. 생성, 읽기, 업데이트, 삭제(CRUD라고도 함)의 4가지 REST 작업이 모두 지원됩니다.

보다 "[Active IQ Unified Manager](#)" Active IQ Unified Manager REST API의 이점에 대한 추가 리소스와 세부 정보를 확인하세요.

이 콘텐츠의 대상 고객

이 주제는 REST API를 통해 Active IQ Unified Manager 소프트웨어와 인터페이스하는 애플리케이션을 만드는 개발자를 대상으로 합니다.

스토리지 관리자와 설계자는 이 정보를 참조하여 Unified Manager REST API를 사용하여 NetApp 스토리지 시스템을 관리하고 모니터링하는 클라이언트 애플리케이션을 구축하는 방법에 대한 기본적인 이해를 얻을 수 있습니다.

스토리지 공급자, ONTAP 클러스터 및 관리 API를 사용하여 스토리지를 관리하려면 이 정보를 사용해야 합니다.



다음 역할 중 하나가 있어야 합니다: 운영자, 스토리지 관리자 또는 애플리케이션 관리자. REST API를 실행하려는 Unified Manager 서버의 IP 주소 또는 정규화된 도메인 이름을 알아야 합니다.

Active IQ Unified Manager API 액세스 및 범주

Active IQ Unified Manager API를 사용하면 사용자 환경의 스토리지 객체를 관리하고 프로비저닝할 수 있습니다. Unified Manager 웹 UI에 액세스하여 이러한 기능 중 일부를 수행할 수도 있습니다.

REST API에 직접 액세스하기 위한 **URL**을 구성합니다.

Python, C#, C++, JavaScript 등의 프로그래밍 언어를 통해 REST API에 직접 액세스할 수 있습니다. REST API에 액세스하려면 호스트 이름 또는 IP 주소와 URL을 다음 형식으로 입력하세요.

`https://<호스트 이름>/api`



기본 포트는 443입니다. 사용자 환경에 맞게 포트를 구성할 수 있습니다.

온라인 **API** 문서 페이지에 접속하세요

제품과 함께 제공되는 **API** 문서 참조 콘텐츠 페이지에 액세스하여 API 문서를 표시하고, 수동으로 API 호출을 실행할 수 있습니다(예: Swagger 인터페이스에서). 메뉴 모음 > 도움말 버튼 > *API 문서*를 클릭하면 이 문서에 액세스할 수

있습니다.

또는 REST API 페이지에 액세스하기 위한 호스트 이름 또는 IP 주소와 URL을 다음 형식으로 입력하세요.

`https://<호스트 이름>/docs/api/`

카테고리

API 호출은 영역이나 범주를 기준으로 기능별로 구성됩니다. 특정 API를 찾으려면 해당 API 카테고리를 클릭하세요.

Unified Manager와 함께 제공되는 REST API를 사용하면 관리, 모니터링 및 프로비저닝 기능을 수행할 수 있습니다. API는 다음 범주로 그룹화됩니다.

- 데이터센터

이 카테고리에는 Work Flow Automation 및 Ansible과 같은 도구를 사용하여 데이터 센터 스토리지 관리 및 분석에 도움이 되는 API가 포함되어 있습니다. 이 카테고리에 속하는 REST API는 데이터 센터의 클러스터, 노드, 집계, 볼륨, LUN, 파일 공유, 네임스페이스 및 기타 요소에 대한 정보를 제공합니다.

- 관리 서버

관리 서버 카테고리 아래의 API에는 다음이 포함됩니다. `jobs`, `system`, 그리고 `events` 아피스. 작업은 Unified Manager에서 스토리지 개체나 워크로드를 관리하는 것과 관련하여 비동기적으로 실행되도록 예약된 작업입니다. 그만큼 `events` API는 데이터 센터에서 이벤트를 반환하고 `system` API는 Unified Manager 인스턴스 세부 정보를 반환합니다.

- 저장소 제공자

이 범주에는 파일 공유, LUN, 성능 서비스 수준 및 스토리지 효율성 정책을 관리하고 프로비저닝하는 데 필요한 모든 프로비저닝 API가 포함되어 있습니다. API를 사용하면 액세스 엔드포인트와 Active Directory를 구성하고, 스토리지 워크로드에 대한 성능 서비스 수준과 스토리지 효율성 정책을 할당할 수도 있습니다.

- 관리

이 범주에는 백업 설정 유지 관리, Unified Manager 데이터 소스에 대한 신뢰 저장소 인증서 보기, Unified Manager의 데이터 소스로 ONTAP 클러스터 관리 등의 관리 작업을 실행하는 데 사용되는 API가 포함되어 있습니다.

- 게이트웨이

Unified Manager를 사용하면 게이트웨이 카테고리에 있는 API를 통해 ONTAP REST API를 호출하고 데이터 센터의 스토리지 객체를 관리할 수 있습니다.

- 보안

이 카테고리에는 Unified Manager 사용자를 관리하기 위한 API가 포함되어 있습니다.

Active IQ Unified Manager 에서 제공되는 REST 서비스

Active IQ Unified Manager API를 사용하기 전에 제공되는 REST 서비스와 운영에 대해 알고 있어야 합니다.

API 서버를 구성하는 데 사용되는 프로비저닝 및 관리 API는 읽기(GET) 또는 쓰기(POST, PATCH, DELETE) 작업을 지원합니다. 다음은 API에서 지원하는 GET, PATCH, POST, DELETE 작업의 몇 가지 예입니다.

- GET의 예: GET /datacenter/cluster/clusters 데이터 센터의 클러스터 세부 정보를 검색합니다. 반환되는 최대 레코드 수 GET 연산은 1000입니다.



API를 사용하면 지원되는 속성별로 레코드를 필터링, 정렬, 순서 지정할 수 있습니다.

- POST의 예: POST /datacenter/svm/svms 사용자 정의 스토리지 가상 머신(SVM)을 생성합니다.
- PATCH의 예: PATCH /datacenter/svm/svms/{key} 고유 키를 사용하여 SVM의 속성을 수정합니다.
- DELETE의 예: DELETE /storage-provider/access-endpoints/{key} 고유 키를 사용하여 LUN, SVM 또는 파일 공유에서 액세스 엔드포인트를 삭제합니다.

API를 사용하여 수행할 수 있는 REST 작업은 운영자, 스토리지 관리자 또는 애플리케이션 관리자 사용자의 역할에 따라 달라집니다.

사용자 역할	지원되는 REST 메서드
연산자	데이터에 대한 읽기 전용 액세스. 이 역할이 있는 사용자는 모든 GET 요청을 실행할 수 있습니다.
스토리지 관리자	모든 데이터에 대한 읽기 권한. 이 역할이 있는 사용자는 모든 GET 요청을 실행할 수 있습니다. 또한 특정 활동(예: 스토리지 서비스 개체 및 스토리지 관리 옵션 관리)을 수행하기 위한 쓰기 액세스 권한(PATCH, POST 및 DELETE 요청 실행)도 있습니다.
애플리케이션 관리자	모든 데이터에 대한 읽기 및 쓰기 액세스 권한. 이 역할을 가진 사용자는 모든 기능에 대해 GET, PATCH, POST 및 DELETE 요청을 실행할 수 있습니다.

모든 REST 작업에 대한 자세한 내용은 [_온라인 API 문서_](#)를 참조하세요.

Active IQ Unified Manager의 API 버전

Active IQ Unified Manager의 REST API URI는 버전 번호를 지정합니다. 예를 들어, /v2/datacenter/svm/svms. 버전 번호 v2 ~에 /v2/datacenter/svm/svms 특정 릴리스에서 사용된 API 버전을 나타냅니다. 버전 번호는 클라이언트가 처리할 수 있는 응답을 반환함으로써 클라이언트 소프트웨어에 대한 API 변경의 영향을 최소화합니다.

이 버전 번호의 숫자 부분은 릴리스와 관련하여 증가합니다. 버전 번호가 있는 URI는 향후 릴리스에서 이전 버전과의 호환성을 유지하는 일관된 인터페이스를 제공합니다. 예를 들어 버전이 없는 동일한 API도 찾을 수 있습니다. /datacenter/svm/svms, 버전이 없는 기본 API를 나타냅니다. 기본 API는 항상 최신 버전의 API입니다.



Swagger 인터페이스의 오른쪽 상단에서 사용할 API 버전을 선택할 수 있습니다. 기본적으로 가장 높은 버전이 선택됩니다. Unified Manager 인스턴스에서 사용 가능한 특정 API의 가장 높은 버전(증분 정수 기준)을 사용하는 것이 좋습니다.

모든 요청에 대해 사용하려는 API 버전을 명시적으로 요청해야 합니다. 버전 번호가 지정되면 서비스는 애플리케이션이 처리하도록 설계되지 않은 응답 요소를 반환하지 않습니다. REST 요청에는 버전 매개변수를 포함해야 합니다. 이전 버전의 API는 몇 번의 릴리스 이후 결국 더 이상 사용되지 않게 되었습니다. 이 릴리스에서는 v1 해당 API 버전은 더 이상 사용되지 않습니다.

ONTAP의 스토리지 리소스

ONTAP의 스토리지 리소스는 크게 물리적 스토리지 리소스와 논리적 스토리지 리소스로 분류할 수 있습니다. Active IQ Unified Manager에서 제공하는 API를 사용하여 ONTAP 시스템을 효과적으로 관리하려면 스토리지 리소스 모델과 다양한 스토리지 리소스 간의 관계를 이해해야 합니다.

- 물리적 저장 리소스

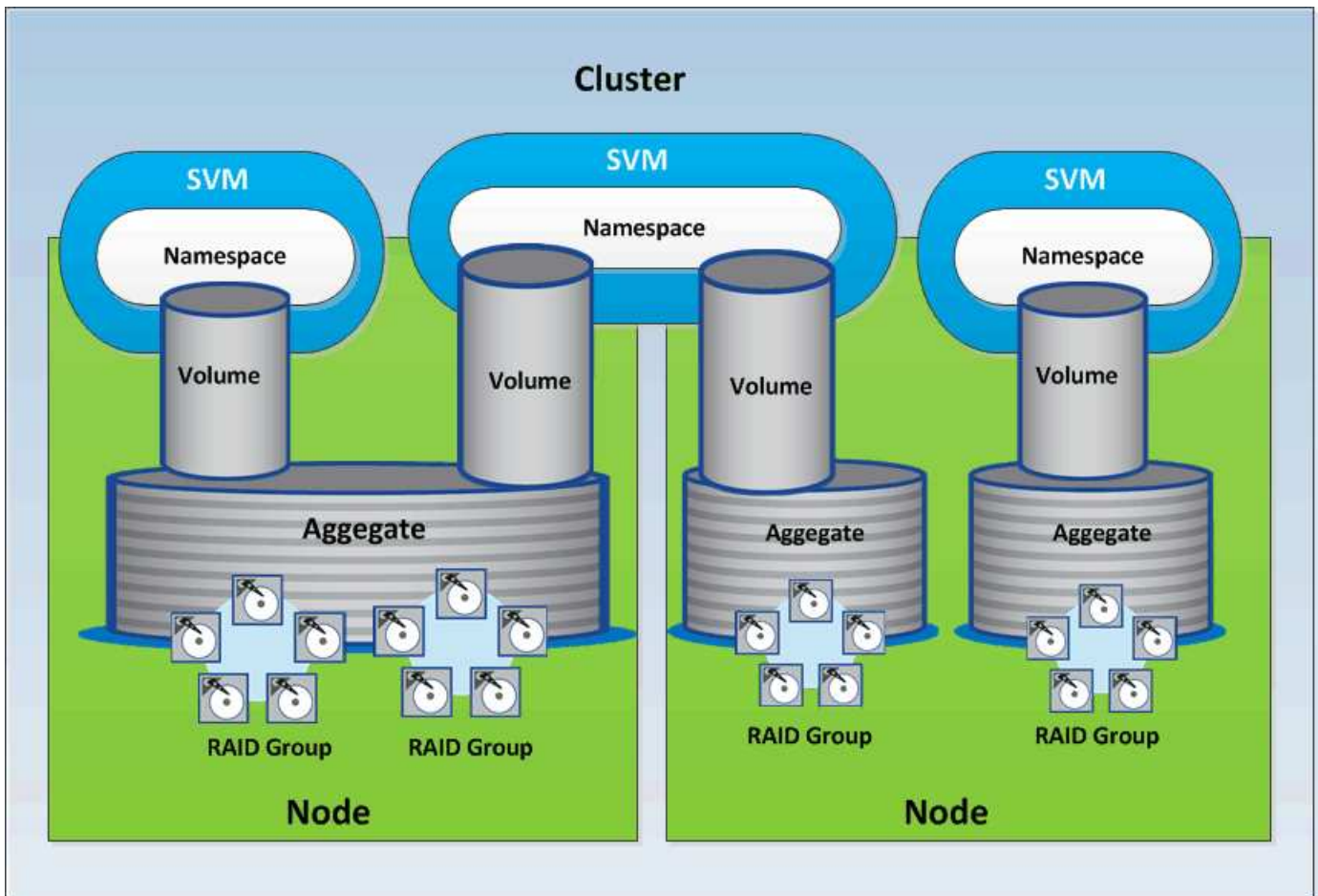
ONTAP에서 제공하는 물리적 저장 객체를 말합니다. 물리적 저장 리소스에는 디스크, 클러스터, 저장 컨트롤러, 노드, 집계 포함됩니다.

- 논리적 저장 리소스

물리적 리소스에 연결되지 않은 ONTAP이 제공하는 저장 리소스를 말합니다. 이러한 리소스는 스토리지 가상 머신(SVM, 이전에는 Vserver로 알려짐)과 연결되며 디스크, 어레이 LUN 또는 집계와 같은 특정 물리적 스토리지 리소스와 독립적으로 존재합니다.

논리적 스토리지 리소스에는 모든 유형의 볼륨과 Q트리 포함되며, 스냅샷 복사본, 중복 제거, 압축, 할당량 등 이러한 리소스와 함께 사용할 수 있는 기능과 구성도 포함됩니다.

다음 그림은 2노드 클러스터의 저장 리소스를 보여줍니다.



Active IQ Unified Manager 의 REST API 액세스 및 인증

Active IQ Unified Manager REST API는 기본 HTTP 인증 메커니즘을 사용하여 HTTP 요청을 발행할 수 있는 모든 REST 클라이언트나 프로그래밍 플랫폼을 사용하여 접근할 수 있습니다.

요청 및 응답 샘플:

- 요구

```
GET
https://<IP
address/hostname>:<port_number>/api/v2/datacenter/cluster/clusters
```

- 응답

```
{
  "records": [
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster,uid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
```

```

"name": "fas8040-206-21",
"uuid": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
"contact": null,
"location": null,
"version": {
  "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33
UTC 2019",
  "generation": 9,
  "major": 5,
  "minor": 0
},
"isSanOptimized": false,
"management_ip": "10.226.207.25",
"nodes": [
  {
    "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb",
    "uuid": "12cf06cc-2e3a-11e9-b9b4-00a0985badbb",
    "name": "fas8040-206-21-01",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb"
      }
    },
    "location": null,
    "version": {
      "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
      "generation": 9,
      "major": 5,
      "minor": 0
    },
    "model": "FAS8040",
    "uptime": 13924095,
    "serial_number": "701424000157"
  },
  {
    "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7",
    "uuid": "1ed606ed-2e3a-11e9-a270-00a0985bb9b7",
    "name": "fas8040-206-21-02",
    "_links": {

```

```

        "self": {
            "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-a3e2-00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-00a0985bb9b7"
        },
        "location": null,
        "version": {
            "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33 UTC 2019",
            "generation": 9,
            "major": 5,
            "minor": 0
        },
        "model": "FAS8040",
        "uptime": 14012386,
        "serial_number": "701424000564"
    },
    "_links": {
        "self": {
            "href": "/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-a3e2-00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb"
        }
    }
},

```

- ``IP address/hostname`` API 서버의 IP 주소 또는 정규화된 도메인 이름(FQDN)입니다.
- 포트 443

기본 HTTPS 포트는 443입니다. 필요한 경우 HTTPS 포트를 사용자 정의할 수 있습니다.

웹 브라우저에서 HTTP 요청을 발행하려면 REST API 브라우저 플러그인을 사용해야 합니다. cURL 및 Perl과 같은 스크립팅 플랫폼을 사용하여 REST API에 액세스할 수도 있습니다.

인증

Unified Manager는 API에 대한 기본 HTTP 인증 체계를 지원합니다. 안전한 정보 흐름(요청 및 응답)을 위해 REST API는 HTTPS를 통해서만 접근할 수 있습니다. API 서버는 서버 검증을 위해 모든 클라이언트에 자체 서명된 SSL 인증서를 제공합니다. 이 인증서는 사용자 정의 인증서(또는 CA 인증서)로 대체될 수 있습니다.

REST API를 호출하려면 API 서버에 대한 사용자 액세스를 구성해야 합니다. 사용자는 로컬 사용자(로컬 데이터베이스에 저장된 사용자 프로필)이거나 LDAP 사용자(API 서버가 LDAP를 통해 인증하도록 구성한 경우)일 수 있습니다. Unified Manager 관리 콘솔 사용자 인터페이스에 로그인하여 사용자 액세스를 관리할 수 있습니다.

Active IQ Unified Manager 에서 사용되는 HTTP 상태 코드

API를 실행하거나 문제를 해결하는 동안 Active IQ Unified Manager API에서 사용되는 다양한 HTTP 상태 코드와 오류 코드를 알고 있어야 합니다.

다음 표에는 인증과 관련된 오류 코드가 나열되어 있습니다.

HTTP 상태 코드	상태 코드 제목	설명
200	OK	동기 API 호출이 성공적으로 실행되면 반환됩니다.
201	생성됨	Active Directory 구성과 같은 동기 호출을 통한 새로운 리소스 생성.
202	수락됨	LUN 및 파일 공유 생성 등의 프로비저닝 기능에 대한 비동기 호출이 성공적으로 실행되면 반환됩니다.
400	잘못된 요청입니다	입력 검증에 실패했음을 나타냅니다. 사용자는 요청 본문에 유효한 키를 입력하는 등 입력 내용을 수정해야 합니다.
401	허가되지 않은 요청	해당 리소스를 볼 권한이 없습니다 /권한 없음.
403	금지된 요청	귀하가 접근하려고 하는 리소스에 접근하는 것은 금지되어 있습니다.
404	리소스를 찾을 수 없습니다	접근하려고 했던 리소스를 찾을 수 없습니다.
405	허용되지 않는 메서드	허용되지 않는 메서드입니다.
429	요청이 너무 많습니다	사용자가 특정 시간 내에 너무 많은 요청을 보냈을 때 반환됩니다.

HTTP 상태 코드	상태 코드 제목	설명
500	내부 서버 오류	내부 서버 오류입니다. 서버로부터 응답을 받지 못했습니다. 이 내부 서버 오류는 영구적일 수도 있고 그렇지 않을 수도 있습니다. 예를 들어, 다음을 실행하는 경우 GET 또는 GET ALL 작업을 수행하다가 이 오류가 발생하면 최소 5번 이상 이 작업을 반복하는 것이 좋습니다. 영구적인 오류인 경우 반환되는 상태 코드는 계속 500입니다. 작업이 성공하면 반환되는 상태 코드는 200입니다.

Active IQ Unified Manager 용 API 사용에 대한 권장 사항

Active IQ Unified Manager 에서 API를 사용할 때는 특정 권장 사례를 따라야 합니다.

- 유효한 실행을 위해서는 모든 응답 콘텐츠 유형이 다음 형식이어야 합니다.

```
application/json
```

- API 버전 번호는 제품 버전 번호와 관련이 없습니다. Unified Manager 인스턴스에 사용 가능한 최신 버전의 API를 사용해야 합니다. Unified Manager API 버전에 대한 자세한 내용은 "Active IQ Unified Manager 의 REST API 버전 관리" 섹션을 참조하세요.
- Unified Manager API를 사용하여 배열 값을 업데이트하는 경우 값의 전체 문자열을 업데이트해야 합니다. 배열에 값을 추가할 수 없습니다. 기존 배열만 교체할 수 있습니다.
- 예를 들어 메트릭 API의 IOPS 및 성능과 같이 이중 값을 제외한 모든 쿼리 매개변수에 파이프() 및 와일드카드(*)와 같은 필터 연산자를 사용할 수 있습니다.
- 필터 연산자 와일드카드(*)와 파이프()를 조합하여 사용하여 객체를 쿼리하지 마세요. 잘못된 개수의 객체를 검색할 수도 있습니다.
- 필터에 값을 사용할 때 값에 아무것도 포함되지 않았는지 확인하십시오. ? 성격. 이는 SQL 주입의 위험을 완화하기 위한 것입니다.
- 참고 사항 GET (모든) API에 대한 요청은 최대 1000개의 레코드를 반환합니다. 쿼리를 설정하여 실행하더라도 max_records 매개변수에 1000보다 큰 값을 입력하면 1000개의 레코드만 반환됩니다.
- 관리 기능을 수행하려면 Unified Manager UI를 사용하는 것이 좋습니다.

문제 해결을 위한 로그

시스템 로그를 사용하면 API를 실행하는 동안 발생할 수 있는 오류의 원인을 분석하고 문제를 해결하는 데 도움이 됩니다.

API 호출과 관련된 문제를 해결하려면 다음 위치에서 로그를 검색하세요.

로그 위치	사용
/var/log/ocie/access_log.log	API를 호출하는 사용자의 이름, 시작 시간, 실행 시간, 상태 및 URL과 같은 모든 API 호출 세부 정보가 포함되어 있습니다. 이 로그 파일을 사용하여 자주 사용되는 API를 확인하거나 GUI 워크플로 문제를 해결할 수 있습니다. 실행 시간에 따라 분석의 규모를 조정하는 데에도 사용할 수 있습니다.
/var/log/ocum/ocumserver.log	모든 API 실행 로그가 포함되어 있습니다. 이 로그 파일을 사용하여 API 호출의 문제를 해결하고 디버깅할 수 있습니다.
/var/log/ocie/server.log	모든 Wildfly 서버 배포 및 서비스 시작/중지 관련 로그가 포함되어 있습니다. 이 로그 파일을 사용하면 Wildfly 서버의 시작, 중지 또는 배포 중에 발생하는 문제의 근본 원인을 찾을 수 있습니다.
/var/log/ocie/au.log	수집 단위 관련 로그가 포함되어 있습니다. ONTAP 에서 객체를 생성, 수정 또는 삭제했지만 Active IQ Unified Manager REST API에 반영되지 않은 경우 이 로그 파일을 사용할 수 있습니다.

작업 객체 비동기 프로세스

Active IQ Unified Manager 다음을 제공합니다. `jobs` 다른 API를 실행하는 동안 수행된 작업에 대한 정보를 검색하는 API입니다. Job 객체를 사용하여 비동기 처리가 어떻게 작동하는지 알아야 합니다.

일부 API 호출, 특히 리소스를 추가하거나 수정하는 데 사용되는 호출은 다른 호출보다 완료하는 데 시간이 더 오래 걸릴 수 있습니다. Unified Manager는 이러한 장기 실행 요청을 비동기적으로 처리합니다.

Job 객체를 사용하여 설명된 비동기 요청

비동기적으로 실행되는 API 호출 후 HTTP 응답 코드 202는 요청이 성공적으로 검증되고 수락되었지만 아직 완료되지 않았음을 나타냅니다. 요청은 클라이언트에 대한 초기 HTTP 응답 이후에도 계속 실행되는 백그라운드 작업으로 처리됩니다. 응답에는 요청을 앵커링하는 Job 객체와 고유 식별자가 포함됩니다.

API 요청과 연관된 Job 객체를 쿼리합니다.

HTTP 응답으로 반환되는 Job 객체에는 여러 속성이 포함되어 있습니다. `state` 속성을 쿼리하여 요청이 성공적으로 완료되었는지 확인할 수 있습니다. Job 객체는 다음 상태 중 하나일 수 있습니다.

- NORMAL
- WARNING

- PARTIAL_FAILURES
- ERROR

작업의 최종 상태(성공 또는 실패)를 감지하기 위해 Job 객체를 폴링할 때 사용할 수 있는 두 가지 기술이 있습니다.

- 표준 폴링 요청: 현재 작업 상태가 즉시 반환됩니다.
- 긴 폴링 요청: 작업 상태가 다음으로 이동될 때 NORMAL, ERROR, 또는 PARTIAL_FAILURES.

비동기 요청의 단계

다음의 고급 절차를 사용하여 비동기 API 호출을 완료할 수 있습니다.

1. 비동기 API 호출을 실행합니다.
2. 요청이 성공적으로 수락되었음을 나타내는 HTTP 응답 202를 받습니다.
3. 응답 본문에서 Job 객체의 식별자를 추출합니다.
4. 루프 내에서 Job 객체가 최종 상태에 도달할 때까지 기다립니다. NORMAL, ERROR, 또는 PARTIAL_FAILURES.
5. 작업의 최종 상태를 확인하고 작업 결과를 검색합니다.

안녕하세요 API 서버

Hello API 서버 는 간단한 REST 클라이언트를 사용하여 Active IQ Unified Manager 에서 REST API를 호출하는 방법을 보여주는 샘플 프로그램입니다. 샘플 프로그램은 JSON 형식으로 API 서버에 대한 기본 세부 정보를 제공합니다(서버는 다음만 지원함) application/json 체재).

사용된 URI는 다음과 같습니다. <https://<hostname>/api/datacenter/svm/svms>. 이 샘플 코드는 다음과 같은 입력 매개변수를 사용합니다.

- API 서버 IP 주소 또는 FQDN
- 선택 사항: 포트 번호(기본값: 443)
- 사용자 이름
- 비밀번호
- 응답 형식(application/json)

REST API를 호출하려면 Jersey 및 RESTEasy와 같은 다른 스크립트를 사용하여 Active IQ Unified Manager 용 Java REST 클라이언트를 작성할 수도 있습니다. 샘플 코드에 대해 다음 사항을 고려해야 합니다.

- 지정된 REST URI를 호출하기 위해 Active IQ Unified Manager 에 대한 HTTPS 연결을 사용합니다.
- Active IQ Unified Manager 에서 제공하는 인증서를 무시합니다.
- 핸드셰이크 중 호스트 이름 확인을 건너뛵니다.
- 용도 javax.net.ssl.HttpURLConnection URI 연결의 경우
- 타사 라이브러리를 사용합니다(org.apache.commons.codec.binary.Base64) HTTP 기본 인증에

사용되는 Base64 인코딩 문자열을 구성하기 위해

샘플 코드를 컴파일하고 실행하려면 Java 컴파일러 1.8 이상을 사용해야 합니다.

```
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.URL;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSession;
import javax.net.ssl.TrustManager;
import javax.net.ssl.X509TrustManager;
import org.apache.commons.codec.binary.Base64;

public class HelloApiServer {

    private static String server;
    private static String user;
    private static String password;
    private static String response_format = "json";
    private static String server_url;
    private static String port = null;

    /*
     * * The main method which takes user inputs and performs the *
    necessary steps
     * to invoke the REST URI and show the response
    */ public static void main(String[] args) {
        if (args.length < 2 || args.length > 3) {
            printUsage();
            System.exit(1);
        }
        setUserArguments(args);
        String serverBaseUrl = "https://" + server;
        if (null != port) {
            serverBaseUrl = serverBaseUrl + ":" + port;
        }
        server_url = serverBaseUrl + "/api/datacenter/svm/svms";
        try {
            HttpURLConnection connection =
getAllTrustingHttpsURLConnection();
            if (connection == null) {
                System.err.println("FATAL: Failed to create HTTPS
```

```

connection to URL: " + server_url);
        System.exit(1);
    }
    System.out.println("Invoking API: " + server_url);
    connection.setRequestMethod("GET");
    connection.setRequestProperty("Accept", "application/" +
response_format);
    String authString = getAuthorizationString();
    connection.setRequestProperty("Authorization", "Basic " +
authString);
    if (connection.getResponseCode() != 200) {
        System.err.println("API Invocation Failed : HTTP error
code : " + connection.getResponseCode() + " : "
+ connection.getResponseMessage());
        System.exit(1);
    }
    BufferedReader br = new BufferedReader(new
InputStreamReader((connection.getInputStream())));
    String response;
    System.out.println("Response:");
    while ((response = br.readLine()) != null) {
        System.out.println(response);
    }
    connection.disconnect();
} catch (Exception e) {
    e.printStackTrace();
}
}

/* Print the usage of this sample code */ private static void
printUsage() {
    System.out.println("\nUsage:\n\tHelloApiServer <hostname> <user>
<password>\n");
    System.out.println("\nExamples:\n\tHelloApiServer localhost admin
mypassword");
    System.out.println("\tHelloApiServer 10.22.12.34:8320 admin
password");
    System.out.println("\tHelloApiServer 10.22.12.34 admin password
");
    System.out.println("\tHelloApiServer 10.22.12.34:8212 admin
password \n");
    System.out.println("\nNote:\n\t(1) When port number is not
provided, 443 is chosen by default.");
}

/* * Set the server, port, username and password * based on user

```

```

inputs. */ private static void setUserArguments(
    String[] args) {
    server = args[0];
    user = args[1];
    password = args[2];
    if (server.contains(":")) {
        String[] parts = server.split(":");
        server = parts[0];
        port = parts[1];
    }
}

/*
 * * Create a trust manager which accepts all certificates and * use
this trust
 * manager to initialize the SSL Context. * Create a
HttpsURLConnection for this
 * SSL Context and skip * server hostname verification during SSL
handshake. * *
 * Note: Trusting all certificates or skipping hostname verification *
is not
 * required for API Services to work. These are done here to * keep
this sample
 * REST Client code as simple as possible.
 */ private static HttpURLConnection
getAllTrustingHttpsURLConnection() {           HttpURLConnection conn =
null;      try {           /* Creating a trust manager that does not
validate certificate chains */           TrustManager[]
trustAllCertificatesManager = new           TrustManager[]{new
X509TrustManager(){
    public X509Certificate[] getAcceptedIssuers(){return null;}
    public void checkClientTrusted(X509Certificate[]
certs, String authType){}
    public void checkServerTrusted(X509Certificate[]
certs, String authType){}           }};           /* Initialize the
SSLContext with the all-trusting trust manager */
    SSLContext sslContext = SSLContext.getInstance("TLS");
    sslContext.init(null, trustAllCertificatesManager, new
SecureRandom());
    HttpURLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));           URL url = new URL(server_url);           conn =
(HttpURLConnection) url.openConnection();           /* Do not perform an
actual hostname verification during SSL Handshake.           Let all
hostname pass through as verified.*/
    conn.setHostnameVerifier(new HostnameVerifier() {           public
boolean verify(String host, SSLSession session) {

```

```

return true;                }                });                } catch (Exception e)
{                e.printStackTrace();                }                return conn;                }

    /*
    * * This forms the Base64 encoded string using the username and
password *
    * provided by the user. This is required for HTTP Basic
Authentication.
    */ private static String getAuthorizationString() {
    String userPassword = user + ":" + password;
    byte[] authEncodedBytes =
Base64.encodeBase64(userPassword.getBytes());
    String authString = new String(authEncodedBytes);
    return authString;
}

}

```

통합 관리자 REST API

이 섹션에는 Active IQ Unified Manager 용 REST API가 해당 카테고리별로 나열되어 있습니다.

Unified Manager 인스턴스에서 모든 REST API 호출에 대한 세부 정보가 포함된 온라인 문서 페이지를 볼 수 있습니다. 이 문서에서는 온라인 문서의 세부 내용을 반복하지 않습니다. 이 문서에 나열되거나 설명된 각 API 호출에는 문서 페이지에서 해당 호출을 찾는 데 필요한 정보만 포함되어 있습니다. 특정 API 호출을 찾은 후 입력 매개변수, 출력 형식, HTTP 상태 코드, 요청 처리 유형을 포함하여 해당 호출의 전체 세부 정보를 검토할 수 있습니다.

워크플로 내의 각 API 호출에 대해 다음 정보가 포함되어 있어 설명서 페이지에서 호출을 찾는 데 도움이 됩니다.

- 범주

API 호출은 설명서 페이지에서 기능적으로 관련된 영역이나 범주로 정리되어 있습니다. 특정 API 호출을 찾으려면 페이지 하단으로 스크롤한 다음 해당 API 카테고리를 클릭하세요.

- HTTP 동사(호출)

HTTP 동사는 리소스에서 수행되는 작업을 식별합니다. 각 API 호출은 단일 HTTP 동사를 통해 실행됩니다.

- 길

경로는 호출을 수행하는 과정에서 작업이 사용하는 구체적인 리소스를 결정합니다. 경로 문자열은 핵심 URL에 추가되어 리소스를 식별하는 완전한 URL을 형성합니다.

API를 사용하여 데이터 센터의 스토리지 객체를 관리합니다.

REST API는 다음과 같습니다. datacenter 카테고리를 사용하면 클러스터, 노드, 집계,

스토리지 VM, 볼륨, LUN, 파일 공유, 네임스페이스 등 데이터 센터의 스토리지 객체를 관리할 수 있습니다. 이러한 API는 객체의 구성을 쿼리하는 데 사용할 수 있으며, 일부 API를 사용하면 객체를 추가, 삭제 또는 수정하는 작업을 수행할 수 있습니다.

이러한 API의 대부분은 필터링, 정렬, 페이지 매김 지원 기능을 갖춘 클러스터 간 집계를 제공하는 GET 호출입니다. 이러한 API를 실행하면 데이터베이스에서 데이터가 반환됩니다. 따라서 새로 생성된 객체는 응답에 나타나기 위해 다음 획득 주기까지 발견되어야 합니다.

특정 객체의 세부 정보를 조회하려면 해당 객체의 고유 ID를 입력하여 세부 정보를 확인해야 합니다. 예를 들어, 스토리지 객체의 메트릭 및 분석 정보는 다음을 참조하세요. "[성능 지표 보기](#)".

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```



CURL 명령, 예제, 요청 및 API에 대한 응답은 Swagger API 인터페이스에서 사용할 수 있습니다. Swagger에 표시된 대로 특정 매개변수를 기준으로 결과를 필터링하고 정렬할 수 있습니다. 이러한 API를 사용하면 클러스터, 볼륨 또는 스토리지 VM과 같은 특정 스토리지 개체에 대한 결과를 필터링할 수 있습니다.

데이터 센터의 스토리지 객체를 위한 API

HTTP 동사	길	설명
GET	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}	이 방법을 사용하면 데이터 센터 전체의 ONTAP 클러스터 세부 정보를 볼 수 있습니다. API는 클러스터의 IPv4 또는 IPv6 주소, 노드 상태, 성능, 용량, 고가용성(HA) 쌍과 같은 노드에 대한 정보를 반환하고 클러스터가 All SAN 어레이인지 여부를 나타냅니다.
GET	/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}	데이터 센터의 클러스터에 설치된 라이선스의 세부 정보를 반환합니다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 라이선스 키, 클러스터 키, 만료 날짜, 라이선스 범위 등의 정보가 반환됩니다. 라이선스 키를 입력하면 특정 라이선스의 세부 정보를 검색할 수 있습니다.
GET	/datacenter/cluster/nodes /datacenter/cluster/nodes/{key}	이 방법을 사용하면 데이터 센터의 노드 세부 정보를 볼 수 있습니다. 노드의 클러스터, 노드 상태, 성능 용량 및 고가용성(HA) 쌍에 대한 정보를 볼 수 있습니다.

HTTP 동사	길	설명
GET	/datacenter/protocols/cifs/shares /datacenter/protocols/cifs/shares/{key}	이 방법을 사용하면 데이터 센터의 CIFS 공유에 대한 세부 정보를 볼 수 있습니다. 클러스터, SVM, 볼륨 세부 정보 외에도 ACL(액세스 제어 목록)에 대한 정보도 반환됩니다.
GET	/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}	이 방법을 사용하면 지원되는 NFS 서비스에 대한 내보내기 정책의 세부 정보를 볼 수 있습니다. 클러스터 또는 스토리지 VM에 대한 내보내기 정책을 쿼리하고 NFS 파일 공유 프로비저닝을 위해 내보내기 정책 키를 재사용할 수 있습니다. 워크로드에 대한 내보내기 정책 할당 및 재사용에 대한 자세한 내용은 "CIFS 및 NFS 파일 공유 프로비저닝"을 참조하세요.
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	이 방법을 사용하면 데이터 센터의 집계 컬렉션을 보거나 해당 집계에 대한 워크로드 프로비저닝 또는 모니터링을 위한 특정 집계를 볼 수 있습니다. 클러스터 및 노드 세부 정보, 사용된 성능 용량, 사용 가능한 공간과 사용된 공간, 스토리지 효율성 등의 정보가 반환됩니다.
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	이 방법을 사용하면 전체 데이터 센터의 LUN 컬렉션을 볼 수 있습니다. 클러스터 및 SVM 세부 정보, QoS 정책, igroup 등 LUN에 대한 정보를 볼 수 있습니다.
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	이 방법을 사용하면 데이터 센터의 스토리지 개체에 적용 가능한 모든 QoS 정책의 세부 정보를 볼 수 있습니다. 클러스터 및 SVM 세부 정보, 고정 또는 적응 정책 세부 정보, 해당 정책에 적용 가능한 개체 수와 같은 정보가 반환됩니다.

HTTP 동사	길	설명
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	이 방법을 사용하면 모든 FlexVol 볼륨이나 FlexGroup 볼륨에 대한 데이터 센터 전반의 Qtree 세부 정보를 볼 수 있습니다. 클러스터 및 SVM 세부 정보, FlexVol volume, 내보내기 정책 등의 정보가 반환됩니다.
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	이 방법을 사용하면 데이터 센터의 볼륨 컬렉션을 볼 수 있습니다. SVM 및 클러스터 세부 정보, QoS 및 내보내기 정책, 볼륨이 읽기-쓰기, 데이터 보호 또는 부하 공유 유형인지 여부와 같은 볼륨에 대한 정보가 반환됩니다. FlexVol 및 FlexClone 볼륨의 경우 해당 집계에 대한 정보를 볼 수 있습니다. FlexGroup 볼륨의 경우 쿼리는 구성 집계 목록을 반환합니다.
GET POST DELETE PATCH	/datacenter/protocols/san/igroups /datacenter/protocols/san/igroups/{key}	특정 LUN 대상에 액세스할 권한이 있는 개시자 그룹(igroup)을 할당할 수 있습니다. 기존 igroup이 있는 경우 할당할 수 있습니다. igroup을 생성하여 LUN에 할당할 수도 있습니다. 이러한 방법을 사용하면 각각 igroup을 쿼리, 생성, 삭제 및 수정할 수 있습니다. 주의 사항: • `POST:`igroup을 생성하는 동안 액세스 권한을 할당할 스토리지 VM을 지정할 수 있습니다. • `DELETE:`특정 igroup을 삭제하려면 igroup 키를 입력 매개변수로 제공해야 합니다. 이미 LUN에 igroup을 할당한 경우 해당 igroup을 삭제할 수 없습니다. • `PATCH:`특정 igroup을 수정하려면 igroup 키를 입력 매개변수로 제공해야 합니다. 업데이트하려는 속성과 해당 속성의 값도 입력해야 합니다.

HTTP 동사	길	설명
GET	/datacenter/svm/svms	이러한 방법을 사용하면 스토리지 가상 머신(스토리지 VM)을 보고, 만들고, 삭제하고, 수정할 수 있습니다. • POST: 생성하려는 스토리지 VM 객체를 입력 매개변수로 입력해야 합니다. 사용자 정의 스토리지 VM을 만든 다음 필요한 속성을 할당할 수 있습니다. • DELETE: 특정 스토리지 VM을 삭제하려면 스토리지 VM 키를 제공해야 합니다. • PATCH: 특정 스토리지 VM을 수정하려면 스토리지 VM 키를 제공해야 합니다. 업데이트하려는 속성과 해당 값도 입력해야 합니다.
POST	/datacenter/svm/svms/{key}	
DELETE		
PATCH		



주의 사항:

환경에서 SLO 기반 워크로드 프로비저닝을 활성화한 경우 스토리지 VM을 생성하는 동안 CIFS 또는 SMB, NFS, FCP, iSCSI 등 LUN 및 파일 공유를 프로비저닝하는 데 필요한 모든 프로토콜을 지원하는지 확인하세요. 스토리지 VM이 필요한 서비스를 지원하지 않으면 프로비저닝 워크플로가 실패할 수 있습니다. 각 유형의 워크로드에 대한 서비스도 스토리지 VM에서 활성화하는 것이 좋습니다.

환경에서 SLO 기반 워크로드 프로비저닝을 활성화한 경우 스토리지 워크로드가 프로비저닝된 스토리지 VM을 삭제할 수 없습니다. CIFS 또는 SMB 서버가 구성된 스토리지 VM을 삭제하면 이 API는 로컬 Active Directory 구성과 함께 CIFS 또는 SMB 서버도 삭제합니다. 그러나 CIFS 또는 SMB 서버 이름은 Active Directory 구성에 계속 남아 있으므로 Active Directory 서버에서 수동으로 삭제해야 합니다.

데이터 센터의 네트워크 요소를 위한 API

데이터 센터 카테고리의 다음 API는 사용자 환경의 포트 및 네트워크 인터페이스, 특히 FC 포트, FC 인터페이스, 이더넷 포트 및 IP 인터페이스에 대한 정보를 검색합니다.

HTTP 동사	길	설명
GET	/datacenter/network/ethernet/ports /datacenter/network/ethernet/ports/{key}	데이터 센터 환경의 모든 이더넷 포트에 대한 정보를 검색합니다. 포트 키를 입력 매개변수로 사용하면 해당 포트의 정보를 볼 수 있습니다. 클러스터 세부 정보, 브로드캐스트 도메인, 상태, 속도, 유형과 같은 포트 세부 정보, 포트가 활성화되었는지 여부 등의 정보가 검색됩니다.

HTTP 동사	길	설명
GET	/datacenter/network/fc/interfaces /datacenter/network/fc/interfaces/{key}	이 방법을 사용하면 데이터 센터 환경의 FC 인터페이스 세부 정보를 볼 수 있습니다. 인터페이스 키를 입력 매개변수로 사용하면 해당 인터페이스의 정보를 볼 수 있습니다. 클러스터 세부 정보, 홈 노드 세부 정보, 홈 포트 세부 정보와 같은 정보가 검색됩니다.
GET	/datacenter/network/fc/ports /datacenter/network/fc/ports/{key}	데이터 센터 환경의 노드에서 사용되는 모든 FC 포트에 대한 정보를 검색합니다. 포트 키를 입력 매개변수로 사용하면 해당 포트의 정보를 볼 수 있습니다. 클러스터 세부 정보, 포트 설명, 지원되는 프로토콜, 포트 상태 등의 정보가 검색됩니다.
GET	/datacenter/network/ip/interfaces /datacenter/network/ip/interfaces/{key}	이 방법을 사용하면 데이터 센터 환경의 IP 인터페이스 세부 정보를 볼 수 있습니다. 인터페이스 키를 입력 매개변수로 사용하면 해당 인터페이스의 정보를 볼 수 있습니다. 클러스터 세부 정보, IP 공간 세부 정보, 홈 노드 세부 정보, 장애 조치가 활성화되었는지 여부 등의 정보가 검색됩니다.

프록시 액세스를 통해 **ONTAP API**에 액세스

게이트웨이 API는 Active IQ Unified Manager 자격 증명을 사용하여 ONTAP REST API를 실행하고 스토리지 객체를 관리할 수 있는 이점을 제공합니다. 이러한 API는 Unified Manager 웹 UI에서 API Gateway 기능이 활성화된 경우 사용할 수 있습니다.

Unified Manager REST API는 ONTAP 클러스터인 Unified Manager 데이터 소스에서 수행할 선택된 작업 세트만 지원합니다. ONTAP API를 통해 다른 기능을 활용할 수 있습니다. 게이트웨이 API를 사용하면 Unified Manager가 관리하는 ONTAP 클러스터에서 수행되는 모든 API 요청을 터널링하기 위한 패스스루 인터페이스가 될 수 있으며, 각 데이터 센터 클러스터에 개별적으로 로그인하지 않아도 됩니다. Unified Manager 인스턴스에서 관리하는 ONTAP 클러스터 전반에서 API를 실행하기 위한 단일 관리 지점 역할을 합니다. API Gateway 기능을 사용하면 Unified Manager를 단일 제어 평면으로 사용하여 개별적으로 로그인하지 않고도 여러 ONTAP 클러스터를 관리할 수 있습니다. 게이트웨이 API를 사용하면 Unified Manager에 로그인한 상태를 유지하고 ONTAP REST API 작업을 실행하여 ONTAP 클러스터를 관리할 수 있습니다.



모든 사용자는 GET 작업을 사용하여 쿼리를 실행할 수 있습니다. 애플리케이션 관리자는 모든 ONTAP REST 작업을 실행할 수 있습니다.

게이트웨이는 ONTAP API와 동일한 형식으로 헤더와 본문 요청을 유지하여 API 요청을 터널링하는 프록시 역할을 합니다. Unified Manager 자격 증명을 사용하여 개별 클러스터 자격 증명을 전달하지 않고도 ONTAP 클러스터에 액세스하고 관리하기 위한 특정 작업을 실행할 수 있습니다. 클러스터 인증 및 클러스터 관리를 계속 관리하지만 API

요청을 특정 클러스터에서 직접 실행되도록 리디렉션합니다. API에서 반환된 응답은 ONTAP 에서 직접 실행된 해당 ONTAP REST API에서 반환된 응답과 동일합니다.

HTTP 동사	경로(URL)	설명
GET	/gateways	이 GET 메서드는 ONTAP REST 호출을 지원하는 Unified Manager에서 관리하는 모든 클러스터 목록을 검색합니다. 클러스터 세부 정보를 확인하고 클러스터 UUID 또는 UUID(Universal Unique Identifier)를 기반으로 다른 방법을 실행할 수 있습니다.  게이트웨이 API는 ONTAP 9.5 이상에서 지원하는 클러스터만 검색하고 HTTPS를 통해 Unified Manager에 추가합니다.
GET POST DELETE PATCH OPTIONS(Swagger에서는 사용할 수 없음) HEAD(Swagger에서는 사용할 수 없음)	/gateways/{uuid}/{path}  {uuid}의 값은 REST 작업이 수행될 클러스터 UUID로 대체되어야 합니다. 또한 UUID가 ONTAP 9.5 이상에서 지원하는 클러스터의 UUID이고 HTTPS를 통해 Unified Manager에 추가되었는지 확인하세요. {path}는 ONTAP REST URL로 대체되어야 합니다. 제거해야 합니다 /api/ URL에서.	이는 모든 ONTAP REST API에 대한 POST, DELETE, PATCH 작업 및 GET을 지원하는 단일 지점 프록시 API입니다. ONTAP 에서 지원하는 한 모든 API에는 제한이 적용되지 않습니다. 터널링이나 프록시 기능은 비활성화할 수 없습니다. 그만큼 OPTIONS 이 메서드는 ONTAP REST API에서 지원하는 모든 작업을 반환합니다. 예를 들어 ONTAP API가 다음만 지원하는 경우 GET 작업, 실행 중 OPTIONS 이 게이트웨이 API를 사용하여 메서드가 반환됩니다. GET 응답으로. 이 방법은 Swagger에서는 지원되지 않지만 다른 API 도구에서는 수행할 수 있습니다. 그만큼 OPTIONS 이 메서드는 리소스를 사용할 수 있는지 여부를 판별합니다. 이 작업은 HTTP 응답 헤더에서 리소스에 대한 메타데이터를 보는 데 사용할 수 있습니다. 이 방법은 Swagger에서는 지원되지 않지만 다른 API 도구에서는 수행할 수 있습니다.

API Gateway 터널링을 이해하세요

게이트웨이 API를 사용하면 Unified Manager를 통해 ONTAP 객체를 관리할 수 있습니다. Unified Manager는 클러스터와 인증 세부 정보를 관리하고 요청을 ONTAP REST 엔드포인트로 리디렉션합니다. 게이트웨이 API는 헤더와 응답 본문의 URL과 HATEOAS(Hypermedia as the Engine of Application State) 링크를 API 게이트웨이 기본 URL로 변환합니다. 게이트웨이 API는 ONTAP REST URL을 추가하고 필요한 ONTAP REST 엔드포인트를 실행하는 프록시 기반 URL 역할을 합니다.



ONTAP API가 API 게이트웨이를 통해 성공적으로 실행되려면 해당 API가 실행 중인 ONTAP 클러스터 버전에서 지원되어야 합니다. ONTAP 클러스터에서 지원되지 않는 API를 실행하면 아무런 결과도 반환되지 않습니다.

이 예에서 게이트웨이 API(프록시 기본 URL)는 다음과 같습니다. `/gateways/{uuid}/`

사용된 ONTAP API는 다음과 같습니다. `/storage/volumes`. 경로 매개변수 값으로 ONTAP API REST URL을 추가해야 합니다.



경로를 추가하는 동안 “를 제거했는지 확인하십시오.” symbol at the beginning of the URL. For the API `/storage/volumes`, 추가하다 `storage/volumes`.

첨부된 URL은 다음과 같습니다. `/gateways/{uuid}/storage/volumes`

실행 중 GET 작업에서 생성된 URL은 다음과 같습니다.

`GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes`

그만큼 `/api` 추가된 URL에서 ONTAP REST URL의 태그가 제거되고 게이트웨이 API의 태그는 유지됩니다.

샘플 cURL 명령

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

API는 해당 클러스터의 스토리지 볼륨 목록을 반환합니다. 응답 형식은 ONTAP 에서 동일한 API를 실행할 때 수신하는 것과 동일합니다. 반환된 상태 코드는 ONTAP REST 상태 코드입니다.

API 범위 설정

모든 API에는 클러스터 범위 내에 설정된 컨텍스트가 있습니다. 스토리지 VM을 기반으로 작동하는 API는 범위가 클러스터이기도 합니다. 즉, API 작업은 관리되는 클러스터 내의 특정 스토리지 VM에서 수행됩니다. 당신이 실행할 때 `/gateways/{uuid}/{path}` API를 사용하려면 작업을 실행하는 클러스터의 클러스터 UUID(Unified Manager 데이터 소스 UUID)를 입력해야 합니다. 해당 클러스터 내의 특정 스토리지 VM에 대한 컨텍스트를 설정하려면 스토리지 VM 키를 X-Dot-SVM-UUID 매개변수로 입력하거나 스토리지 VM 이름을 X-Dot-SVM-Name 매개변수로 입력합니다. 매개변수는 문자열 헤더에 필드로 추가되고 작업은 해당 클러스터 내의 해당 스토리지 VM 범위 내에서 실행됩니다.

샘플 cURL 명령

```
curl -X GET "https://<hostname>/api/gateways/e4f33f90-f75f-11e8-9ed9-00a098e3215f/storage/volume" -H "accept: application/hal+json" -H "X-Dot-SVM-UUID: d9c33ec0-5b61-11e9-8760-00a098e3215f" -H "Authorization: Basic <Base64EncodedCredentials>"
```

ONTAP REST API 사용에 대한 자세한 내용은 다음을 참조하세요. <https://docs.netapp.com/us-en/ontap-automation/index.html>["ONTAP REST API 자동화"]

API를 사용하여 관리 작업 수행

다음 API를 사용할 수 있습니다. `administration` 백업 설정을 수정하고, 백업 파일 정보와 클러스터 인증서를 확인하고, ONTAP 클러스터를 Active IQ Unified Manager 데이터 소스로 관리하는 범주입니다.



이러한 작업을 실행하려면 애플리케이션 관리자 역할이 있어야 합니다. Unified Manager 웹 UI를 사용하여 이러한 설정을 구성할 수도 있습니다.

HTTP 동사	길	설명
GET	/admin/backup-settings	당신은 사용할 수 있습니다 GET Unified Manager에 기본적으로 구성된 백업 일정의 설정을 보는 방법입니다. 다음 사항을 확인할 수 있습니다. - 일정이 활성화되어 있는지 비활성화되어 있는지 여부 - 예약된 백업 빈도(매일 또는 매주) - 백업 시간 - 애플리케이션에 보관해야 하는 백업 파일의 최대 수 백업 시간은 서버 시간대에 따라 결정됩니다. 데이터베이스 백업 설정은 기본적으로 Unified Manager에서 사용할 수 있으며, 백업 일정을 만들 수 없습니다. 하지만 다음을 사용할 수 있습니다. PATCH 기본 설정을 수정하는 방법입니다.
PATCH	/admin/backup-settings	

HTTP 동사	길	설명
GET	/admin/backup-file-info	Unified Manager의 백업 일정이 수정될 때마다 백업 덤프 파일이 생성됩니다. 이 방법을 사용하면 수정된 백업 설정에 따라 백업 파일이 생성되었는지, 그리고 파일의 정보가 수정된 설정과 일치하는지 확인할 수 있습니다.
GET	/admin/datasource-certificate	이 방법을 사용하면 신뢰 저장소에서 데이터 소스(클러스터) 인증서를 볼 수 있습니다. ONTAP 클러스터를 Unified Manager 데이터 소스로 추가하기 전에 인증서의 유효성을 검사해야 합니다.
GET POST PATCH DELETE	/admin/datasources/clusters /admin/datasources/clusters/{key}	당신은 사용할 수 있습니다 GET Unified Manager가 관리하는 데이터 소스(ONTAP 클러스터)의 세부 정보를 검색하는 방법입니다. Unified Manager에 새 클러스터를 데이터 소스로 추가할 수도 있습니다. 클러스터를 추가하려면 호스트 이름, 사용자 이름, 비밀번호를 알아야 합니다. Unified Manager에서 데이터 소스로 관리되는 클러스터를 수정하고 삭제하려면 ONTAP 클러스터 키를 사용하세요.

API를 사용하여 사용자 관리

API를 사용할 수 있습니다 security Active IQ Unified Manager 에서 선택된 클러스터 개체에 대한 사용자 액세스를 제어하는 범주입니다. 로컬 사용자나 데이터베이스 사용자를 추가할 수 있습니다. 인증 서버에 속한 원격 사용자나 그룹을 추가할 수도 있습니다. 사용자에게 할당한 역할의 권한에 따라 사용자는 Unified Manager에서 저장소 개체를 관리하거나 데이터를 볼 수 있습니다.



이러한 작업을 실행하려면 애플리케이션 관리자 역할이 있어야 합니다. Unified Manager 웹 UI를 사용하여 이러한 설정을 구성할 수도 있습니다.

API는 다음과 같습니다. security 카테고리는 키 매개변수가 아닌 사용자 이름인 users 매개변수를 사용자 엔터티의 고유 식별자로 사용합니다.

HTTP 동사	길	설명
GET POST	/security/users /security/users	이러한 방법을 사용하면 사용자 세부 정보를 얻거나 Unified Manager에 새 사용자를 추가할 수 있습니다. 사용자 유형에 따라 사용자에게 특정 역할을 추가할 수 있습니다. 사용자를 추가하는 동안 로컬 사용자, 유지 관리 사용자, 데이터베이스 사용자에 대한 비밀번호를 제공해야 합니다.
GET PATCH DELETE	/security/users/{name}	GET 메서드를 사용하면 이름, 이메일 주소, 역할, 권한 유형 등 사용자의 모든 세부 정보를 검색할 수 있습니다. PATCH 방식을 사용하면 세부 정보를 업데이트할 수 있습니다. DELETE 메서드를 사용하면 사용자를 제거할 수 있습니다.

API를 사용하여 성능 지표 보기

Active IQ Unified Manager 다음 API 세트를 제공합니다. /datacenter 데이터 센터의 클러스터와 스토리지 개체의 성능 데이터를 볼 수 있는 카테고리입니다. 이러한 API는 클러스터, 노드, LUN, 볼륨, 집계, 스토리지 VM, FC 인터페이스, FC 포트, 이더넷 포트, IP 인터페이스 등 다양한 스토리지 개체의 성능 데이터를 검색합니다.

그만큼 /metrics 그리고 /analytics API는 성능 측정 항목에 대한 다양한 보기를 제공하며, 이를 사용하여 데이터 센터의 다음 스토리지 개체에 대한 세부 정보를 다양한 수준으로 자세히 살펴볼 수 있습니다.

- 클러스터
- 노드
- 스토리지 VM
- 집계
- 볼륨
- LUN
- FC 인터페이스
- FC 포트
- 이더넷 포트
- IP 인터페이스

다음 표는 다음 사이의 비교를 그림니다. /metrics 그리고 /analytics 검색된 성능 데이터의 세부 사항과 관련된 API입니다.

메트릭	해석학
단일 개체에 대한 성능 세부 정보. 예를 들어, <code>/datacenter/cluster/clusters/{key}/metrics</code> API에서는 특정 클러스터에 대한 메트릭을 검색하기 위해 경로 매개변수로 클러스터 키를 입력해야 합니다.	데이터 센터 내 동일 유형의 여러 개체에 대한 성능 세부 정보입니다. 예를 들어, <code>/datacenter/cluster/clusters/analytics</code> API는 데이터 센터의 모든 클러스터에 대한 종합적인 지표를 검색합니다.
성능 측정 항목은 검색을 위한 시간 간격 매개변수를 기반으로 저장 개체에 대한 샘플을 제공합니다.	특정 기간(72시간 이상) 동안 특정 유형의 스토리지 개체에 대한 성능의 고수준 집계 값입니다.
노드나 클러스터의 세부 정보 등 객체의 기본 세부 정보를 검색합니다.	구체적인 세부 정보는 검색되지 않았습니다.
최소값, 최대값, 95백분위수, 일정 기간 동안의 평균 성능 값과 같은 누적 카운터는 읽기, 쓰기, 전체 및 기타 카운터와 같은 단일 개체에 대해 검색됩니다.	동일한 유형의 모든 개체에 대해 단일 집계 값이 표시됩니다.

메트릭	해석학
시간 범위와 샘플 데이터는 다음 일정을 기반으로 합니다. 데이터의 시간 범위. 예시로는 1시간, 12시간, 1일, 2일, 3일, 15일, 1주, 1개월, 2개월, 3개월, 6개월 등이 있습니다. 범위가 3일(72시간)을 넘으면 1시간 분량의 샘플을 얻을 수 있고, 그렇지 않으면 5분 분량의 샘플을 얻을 수 있습니다. 각 시간 범위의 기간은 다음과 같습니다. • 1시간: 5분 동안 샘플링된 가장 최근 1시간 동안의 지표입니다. • 12시간: 5분 동안 샘플링된 최근 12시간 동안의 지표입니다. • 1d: 5분 동안 샘플링된 가장 최근 날짜의 지표입니다. • 2d: 5분 동안 샘플링된 최근 2일간의 지표입니다. • 3d: 5분 동안 샘플링된 최근 3일간의 지표입니다. • 15일: 1시간 동안 샘플링된 최근 15일 동안의 지표입니다. • 1주: 1시간 동안 샘플링된 가장 최근 주에 대한 지표입니다. • 1m: 1시간 동안 샘플링된 가장 최근 한 달 동안의 지표입니다. • 2m: 1시간 동안 샘플링된 최근 2개월 동안의 지표입니다. • 3m: 1시간 동안 샘플링된 최근 3개월 동안의 지표입니다. • 6m: 1시간 동안 샘플링된 최근 6개월 동안의 지표입니다. 사용 가능한 값: 1시간, 12시간, 1일, 2일, 3일, 15일, 1주, 1개월, 2개월, 3개월, 6개월 기본값 : 1h	72시간 이상. 이 샘플이 계산되는 기간은 ISO-8601 표준 형식으로 표현됩니다.

메트릭 **API**에 대한 출력 샘플

예를 들어, `/datacenter/cluster/nodes/{key}/metrics` API는 노드에 대한 다음 세부 정보(기타 정보 포함)를 검색합니다.



요약 값의 95백분위수는 해당 기간 동안 수집된 샘플의 95%가 95백분위수로 지정된 값보다 낮은 카운터 값을 가지고 있음을 나타냅니다.

```
{
  "iops": {
    "local": {
```

```

        "other": 100.53,
        "read": 100.53,
        "total": 100.53,
        "write": 100.53
    },
    "other": 100.53,
    "read": 100.53,
    "total": 100.53,
    "write": 100.53
},
"latency": {
    "other": 100.53,
    "read": 100.53,
    "total": 100.53,
    "write": 100.53
},
"performance_capacity": {
    "available_iops_percent": 0,
    "free_percent": 0,
    "system_workload_percent": 0,
    "used_percent": 0,
    "user_workload_percent": 0
},
"throughput": {
    "other": 100.53,
    "read": 100.53,
    "total": 100.53,
    "write": 100.53
},
"timestamp": "2018-01-01T12:00:00-04:00",
"utilization_percent": 0
}
],
"start_time": "2018-01-01T12:00:00-04:00",
"summary": {
    "iops": {
        "local_iops": {
            "other": {
                "95th_percentile": 28,
                "avg": 28,
                "max": 28,
                "min": 5
            },
            "read": {
                "95th_percentile": 28,
                "avg": 28,

```

```
    "max": 28,  
    "min": 5  
  },  
  "total": {  
    "95th_percentile": 28,  
    "avg": 28,  
    "max": 28,  
    "min": 5  
  },  
  "write": {  
    "95th_percentile": 28,  
    "avg": 28,  
    "max": 28,  
    "min": 5  
  }  
},
```

분석 **API**에 대한 출력 샘플

예를 들어, /datacenter/cluster/nodes/analytics API는 모든 노드에 대해 다음 값을 검색합니다.

```
{
  "iops": 1.7471,
  "latency": 60.0933,
  "throughput": 5548.4678,
  "utilization_percent": 4.8569,
  "period": 72,
  "performance_capacity": {
    "used_percent": 5.475,
    "available_iops_percent": 168350
  },
  "node": {
    "key": "37387241-8b57-11e9-8974-00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a",
    "uuid": "95f94e8d-8b4e-11e9-8974-00a098e0219a",
    "name": "ocum-infinity-01",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/nodes/37387241-8b57-11e9-8974-00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a"
      }
    }
  },
  "cluster": {
    "key": "37387241-8b57-11e9-8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a",
    "uuid": "37387241-8b57-11e9-8974-00a098e0219a",
    "name": "ocum-infinity",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/clusters/37387241-8b57-11e9-8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a"
      }
    }
  },
  "_links": {
    "self": {
      "href": "/api/datacenter/cluster/nodes/analytics"
    }
  }
},
```

사용 가능한 API 목록

다음 표에서는 다음을 설명합니다. /metrics 그리고 /analytics API에 대한 자세한 정보.



이러한 API에서 반환된 IOPS 및 성능 측정 항목은 예를 들어 이중 값입니다. 100.53 . 파이프(|) 및 와일드카드(*) 문자로 이러한 부동 소수점 값을 필터링하는 것은 지원되지 않습니다.

HTTP 동사	길	설명
GET	/datacenter/cluster/clusters/{key}/metrics	클러스터 키의 입력 매개변수로 지정된 클러스터에 대한 성능 데이터(샘플 및 요약)를 검색합니다. 클러스터 키와 UUID, 시간 범위, IOPS, 처리량, 샘플 수와 같은 정보가 반환됩니다.
GET	/datacenter/cluster/clusters/analytics	데이터 센터의 모든 클러스터에 대한 고급 성능 측정 항목을 검색합니다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 집계된 IOPS, 처리량, 수집 기간(시간) 등의 값이 반환됩니다.
GET	/datacenter/cluster/nodes/{key}/metrics	노드 키의 입력 매개변수로 지정된 노드에 대한 성능 데이터(샘플 및 요약)를 검색합니다. 노드 UUID, 시간 범위, IOPS 요약, 처리량, 지연 시간 및 성능, 수집된 샘플 수, 활용률 등의 정보가 반환됩니다.
GET	/datacenter/cluster/nodes/analytics	데이터 센터의 모든 노드에 대한 고급 성능 측정 항목을 검색합니다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 노드 및 클러스터 키와 같은 정보와 집계된 IOPS, 처리량, 수집 기간(시간)과 같은 값이 반환됩니다.
GET	/datacenter/storage/aggregates/{key}/metrics	집계 키의 입력 매개변수로 지정된 집계에 대한 성능 데이터(샘플 및 요약)를 검색합니다. 시간 범위, IOPS 요약, 지연 시간, 처리량, 성능 용량, 각 카운터에 대해 수집된 샘플 수, 활용률 등의 정보가 반환됩니다.
GET	/datacenter/storage/aggregates/analytics	데이터 센터의 모든 집계에 대한 고급 성능 측정 항목을 검색합니다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 집계 및 클러스터 키와 같은 정보와 집계된 IOPS, 처리량, 수집 기간(시간)과 같은 값이 반환됩니다.

HTTP 동사	길	설명
GET	/datacenter/storage/luns/{key}/metrics /datacenter/storage/volumes/{key}/metrics	LUN 또는 볼륨 키의 입력 매개변수로 지정된 LUN 또는 파일 공유(볼륨)에 대한 성능 데이터(샘플 및 요약)를 검색합니다. 최소, 최대, 평균 읽기, 쓰기, 전체 IOPS, 지연 시간, 처리량 요약, 각 카운터에 대해 수집된 샘플 수 등의 정보가 반환됩니다.
GET	/datacenter/storage/luns/analytics /datacenter/storage/volumes/analytics	데이터 센터의 모든 LUN 또는 볼륨에 대한 고급 성능 측정 항목을 검색합니다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 스토리지 VM 및 클러스터 키와 같은 정보와 집계된 IOPS, 처리량, 수집 기간(시간)과 같은 값이 반환됩니다.
GET	/datacenter/svm/svms/{key}/metrics	스토리지 VM 키의 입력 매개변수로 지정된 스토리지 VM에 대한 성능 데이터(샘플 및 요약)를 검색합니다. 지원되는 각 프로토콜에 따른 IOPS 요약 nvmf, fcp, iscsi, 그리고 nfs, 처리량, 지연 시간, 수집된 샘플 수가 반환됩니다.
GET	/datacenter/svm/svms/analytics	데이터 센터의 모든 스토리지 VM에 대한 고급 성능 측정 항목을 검색합니다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 저장소 VM UUID, 집계된 IOPS, 지연 시간, 처리량, 수집 기간(시간) 등의 정보가 반환됩니다.
GET	/datacenter/network/ethernet/ports/{key}/metrics	포트 키의 입력 매개변수로 지정된 특정 이더넷 포트에 대한 성능 측정 항목을 검색합니다. 지원되는 범위에서 간격(시간 범위)이 제공되면 API는 최소값, 최대값, 해당 기간 동안의 평균 성능 값과 같은 누적된 카운터를 반환합니다.
GET	/datacenter/network/ethernet/ports/analytics	데이터 센터 환경의 모든 이더넷 포트에 대한 고급 성능 측정 항목을 검색합니다. 클러스터 및 노드 키와 UUID, 처리량, 수집 기간, 포트 활용률 등의 정보가 반환됩니다. 포트 키, 활용률, 클러스터 및 노드 이름, UUID 등과 같은 사용 가능한 매개변수를 기준으로 결과를 필터링할 수 있습니다.

HTTP 동사	길	설명
GET	/datacenter/network/fc/interfaces/{key}/metrics	인터페이스 키의 입력 매개변수로 지정된 특정 네트워크 FC 인터페이스에 대한 성능 측정 항목을 검색합니다. 지원되는 범위에서 간격(시간 범위)이 제공되면 API는 최소값, 최대값, 해당 기간 동안의 평균 성능 값과 같은 누적된 카운터를 반환합니다.
GET	/datacenter/network/fc/interfaces/analytics	데이터 센터 환경의 모든 이더넷 포트에 대한 고급 성능 측정 항목을 검색합니다. 클러스터 및 FC 인터페이스 키와 UUID, 처리량, IOPS, 지연 시간, 스토리지 VM과 같은 정보가 반환됩니다. 클러스터 및 FC 인터페이스 이름과 UUID, 스토리지 VM, 처리량 등과 같은 사용 가능한 매개변수를 기준으로 결과를 필터링할 수 있습니다.
GET	/datacenter/network/fc/ports/{key}/metrics	포트 키의 입력 매개변수로 지정된 특정 FC 포트에 대한 성능 측정 항목을 검색합니다. 지원되는 범위에서 간격(시간 범위)이 제공되면 API는 최소값, 최대값, 해당 기간 동안의 평균 성능 값과 같은 누적된 카운터를 반환합니다.
GET	/datacenter/network/fc/ports/analytics	데이터 센터 환경의 모든 FC 포트에 대한 고급 성능 측정 항목을 검색합니다. 클러스터 및 노드 키와 UUID, 처리량, 수집 기간, 포트 활용률 등의 정보가 반환됩니다. 포트 키, 활용률, 클러스터 및 노드 이름, UUID 등과 같은 사용 가능한 매개변수를 기준으로 결과를 필터링할 수 있습니다.
GET	/datacenter/network/ip/interfaces/{key}/metrics	인터페이스 키의 입력 매개변수에 의해 지정된 네트워크 IP 인터페이스에 대한 성능 측정 항목을 검색합니다. 지원되는 범위에서 간격(시간 범위)이 제공되면 API는 샘플 수, 누적 카운터, 처리량, 수신 및 전송된 패킷 수와 같은 정보를 반환합니다.

HTTP 동사	길	설명
GET	/datacenter/network/ip/interfaces/analytics	데이터 센터 환경의 모든 네트워크 IP 인터페이스에 대한 고급 성능 측정 항목을 검색합니다. 클러스터 및 IP 인터페이스 키와 UUID, 처리량, IOPS, 지연 시간과 같은 정보가 반환됩니다. 클러스터 및 IP 인터페이스 이름과 UUID, IOPS, 대기 시간, 처리량 등과 같은 사용 가능한 매개변수로 결과를 필터링할 수 있습니다.

작업 및 시스템 세부 정보 보기

당신은 사용할 수 있습니다 jobs API는 management-server 비동기 작업의 실행 세부 정보를 보려면 카테고리를 선택하세요. 그만큼 system API는 management-server 카테고리를 사용하면 Active IQ Unified Manager 환경에서 인스턴스 세부 정보를 볼 수 있습니다.

채용공고 보기

Active IQ Unified Manager에서는 리소스 추가 및 수정과 같은 작업이 동기 및 비동기 API 호출을 통해 수행됩니다. 비동기 실행을 위해 예약된 호출은 해당 호출에 대해 생성된 Job 객체를 통해 추적할 수 있습니다. 각 Job 객체에는 식별을 위한 고유한 키가 있습니다. 각 Job 객체는 사용자가 작업 진행 상황에 접근하고 이를 추적할 수 있도록 Job 객체 URI를 반환합니다. 이 API를 사용하면 각 실행의 세부 정보를 검색할 수 있습니다.

이 API를 사용하면 과거 데이터를 포함하여 데이터 센터의 모든 작업 객체를 쿼리할 수 있습니다. 기본적으로 모든 작업을 쿼리하면 웹 UI 및 API 인터페이스를 통해 트리거된 마지막 20개 작업의 세부 정보가 반환됩니다. 내장된 필터를 사용하여 특정 일자리를 확인하세요. Job 키를 사용하여 특정 작업의 세부 정보를 쿼리하고 리소스에 대한 다음 작업 세트를 실행할 수도 있습니다.

범주	HTTP 동사	길	설명
관리 서버	얻다	/management-server/jobs	모든 작업의 세부 정보를 반환합니다. 정렬 순서가 없으므로 마지막으로 제출된 Job 객체가 맨 위에 반환됩니다.
관리 서버	얻다	/management-server/jobs/{key} Job 객체의 작업 키를 입력하면 해당 작업의 구체적인 세부 정보를 볼 수 있습니다.	특정 Job 객체의 세부 정보를 반환합니다.

시스템 세부 정보 보기

를 사용하여 `/management-server/system` API를 사용하면 Unified Manager 환경의 인스턴스별 세부 정보를 쿼리할 수 있습니다. API는 시스템에 설치된 Unified Manager 버전, UUID, 공급업체 이름, 호스트 OS, Unified Manager 인스턴스에서 실행되는 서비스의 이름, 설명 및 상태 등 제품 및 서비스에 대한 정보를 반환합니다.

범주	HTTP 동사	길	설명
관리 서버	얻다	<code>/management-server/system</code>	이 API를 실행하려면 입력 매개변수가 필요하지 않습니다. 기본적으로 현재 Unified Manager 인스턴스의 시스템 세부 정보가 반환됩니다.

API를 사용하여 이벤트 및 알림 관리

그만큼 `events`, `alerts`, 그리고 `scripts` API는 다음과 같습니다. `management-server` 카테고리를 사용하면 Active IQ Unified Manager 환경에서 알림과 관련된 이벤트, 알림 및 스크립트를 관리할 수 있습니다.

이벤트 보기 및 수정

Unified Manager는 Unified Manager가 모니터링하고 관리하는 클러스터에 대해 ONTAP에서 생성된 이벤트를 수신합니다. 이러한 API를 사용하면 클러스터에 대해 생성된 이벤트를 보고, 이를 해결하고 업데이트할 수 있습니다.

실행하여 GET에 대한 방법 `/management-server/events` API를 사용하면 과거 데이터를 포함하여 데이터 센터의 이벤트를 쿼리할 수 있습니다. 이름, 영향 수준, 영향 영역, 심각도, 상태, 리소스 이름, 리소스 유형 등의 내장 필터를 사용하여 특정 이벤트를 확인하세요. 리소스 유형 및 영역 매개변수는 이벤트가 발생한 스토리지 개체에 대한 정보를 반환하고, 영향 영역은 가용성, 용량, 구성, 보안, 보호 및 성능과 같이 이벤트가 발생한 문제에 대한 정보를 반환합니다.

이 API에 대해 PATCH 작업을 실행하면 이벤트에 대한 해결 워크플로를 활성화할 수 있습니다. 이벤트를 자신 또는 다른 사용자에게 할당하고 이벤트 수신을 확인할 수 있습니다. 이벤트를 트리거한 문제를 해결하기 위해 리소스에 대한 단계를 수행하면 이 API를 사용하여 이벤트를 해결됨으로 표시할 수 있습니다.

이벤트에 대한 자세한 내용은 다음을 참조하세요. ["이벤트 관리"](#).

범주	HTTP 동사	길	설명
관리 서버	얻다	<code>/management-server/events</code> <code>/management-server/events/{key}</code>	Get ALL 메서드를 실행하면 응답 본문은 데이터 센터의 모든 이벤트에 대한 이벤트 세부 정보로 구성됩니다. 특정 키로 이벤트 세부 정보를 검색하면 특정 이벤트의 세부 정보를 보고 리소스에서 다음 작업 세트를 실행할 수 있습니다. 응답 본문은 해당 이벤트의 세부정보로 구성됩니다.

범주	HTTP 동사	길	설명
관리 서버	반점	management-server/events/{key}	이 API를 실행하여 이벤트를 할당하거나 상태를 확인됨 또는 해결됨으로 변경합니다. 이 방법을 사용하면 이벤트를 자신 또는 다른 사용자에게 할당할 수도 있습니다. 이는 동기적 작업입니다.

알림 관리

이벤트는 자동으로 지속적으로 생성됩니다. Unified Manager는 이벤트가 특정 필터 기준을 충족할 때만 알림을 생성합니다. 알림을 생성할 이벤트를 선택할 수 있습니다. 를 사용하여 /management-server/alerts API를 사용하면 특정 이벤트나 특정 심각도 유형의 이벤트가 발생할 때 자동으로 알림을 보내도록 알림을 구성할 수 있습니다.

알림에 대한 자세한 내용은 다음을 참조하세요. ["알림 관리"](#).

범주	HTTP 동사	길	설명
관리 서버	얻다	/management-server/alerts /management-server/alerts/{key}	alert 키를 사용하여 환경에 있는 모든 기존 알림이나 특정 알림을 쿼리합니다. 사용자 환경에서 생성된 알림에 대한 정보(알림 설명, 작업, 알림이 전송된 이메일 ID, 이벤트 및 심각도 등)를 볼 수 있습니다.
관리 서버	우편	/management-server/alerts	이 방법을 사용하면 특정 이벤트에 대한 알림을 추가할 수 있습니다. 경고 이름, 경고가 적용되는 물리적 또는 논리적 리소스 또는 이벤트, 경고가 활성화되었는지 여부, SNMP 트랩을 발행하는지 여부를 추가해야 합니다. 알림 스크립트를 추가하는 경우 작업, 알림 이메일 ID, 스크립트 세부 정보 등 알림을 생성하려는 추가 세부 정보를 추가할 수 있습니다.

범주	HTTP 동사	길	설명
관리 서버	패치 및 삭제	management-server/events/{key}	이러한 방법을 사용하면 특정 알림을 수정하고 삭제할 수 있습니다. 설명, 이름, 알림 활성화 및 비활성화 등 다양한 속성을 수정할 수 있습니다. 알림이 더 이상 필요하지 않으면 알림을 삭제할 수 있습니다.



알림을 추가하기 위한 리소스를 선택할 때 리소스로 클러스터를 선택하더라도 해당 클러스터 내의 스토리지 개체가 자동으로 선택되지 않는다는 점에 유의하세요. 예를 들어, 모든 클러스터의 모든 중요 이벤트에 대한 알림을 생성하면 클러스터 중요 이벤트에 대한 알림만 받게 됩니다. 노드, 집계 등의 중요 이벤트에 대한 알림은 받지 않습니다.

스크립트 관리

를 사용하여 /management-server/scripts API를 사용하면 알림이 트리거될 때 실행되는 스크립트와 알림을 연결할 수도 있습니다. 스크립트를 사용하면 Unified Manager에서 여러 스토리지 개체를 자동으로 수정하거나 업데이트할 수 있습니다. 스크립트는 알림과 연결되어 있습니다. 이벤트로 인해 알림이 발생하면 스크립트가 실행됩니다. 사용자 정의 스크립트를 업로드하고 알림이 생성되면 실행을 테스트할 수 있습니다. 스크립트에 알림을 연결하면 Unified Manager에서 이벤트에 대한 알림이 발생할 때 스크립트가 실행됩니다.

스크립트에 대한 자세한 내용은 다음을 참조하세요. "[스크립트 관리](#)".

범주	HTTP 동사	길	설명
관리 서버	얻다	/management-server/scripts	이 API를 사용하면 사용자 환경에 있는 모든 기존 스크립트를 쿼리할 수 있습니다. 표준 필터와 정렬 작업을 사용하여 특정 스크립트만 봅니다.
관리 서버	우편	/management-server/scripts	이 API를 사용하여 스크립트에 대한 설명을 추가하고 알림과 관련된 스크립트 파일을 업로드합니다.

API를 사용하여 작업 부하 관리

여기에 설명된 API는 스토리지 작업 부하 보기, LUN 및 파일 공유 생성, 성능 서비스 수준 및 스토리지 효율성 정책 관리, 스토리지 작업 부하에 대한 정책 할당 등 스토리지 관리의 다양한 기능을 포괄합니다.

API를 사용하여 스토리지 워크로드 보기

여기에 나열된 API를 사용하면 데이터 센터의 모든 ONTAP 클러스터에 대한 통합된 스토리지 워크로드 목록을 볼 수 있습니다. API는 또한 Active IQ Unified Manager 환경에서 프로비저닝된 스토리지 워크로드 수와 해당 용량 및 성능(IOPS) 통계에 대한 요약 보기를 제공합니다.

스토리지 워크로드 보기

다음 방법을 사용하면 데이터 센터의 모든 클러스터에 있는 모든 스토리지 작업 부하를 볼 수 있습니다. 특정 열을 기준으로 응답을 필터링하는 방법에 대한 자세한 내용은 Unified Manager 인스턴스에서 제공되는 API 참조 문서를 참조하세요.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/workloads

스토리지 워크로드 요약 보기

다음 방법을 사용하면 각 성능 서비스 수준에서 관리되는 사용된 용량, 사용 가능한 용량, 사용된 IOPS, 사용 가능한 IOPS 및 스토리지 워크로드 수를 평가할 수 있습니다. 표시되는 스토리지 작업 부하는 모든 LUN, NFS 파일 공유 또는 CIFS 공유에 대한 것일 수 있습니다. API는 스토리지 워크로드 개요, Unified Manager에서 프로비저닝한 스토리지 워크로드 개요, 데이터 센터 개요, 할당된 성능 서비스 수준에 따라 데이터 센터의 총 공간, 사용된 공간, 사용 가능한 공간 및 IOPS 개요를 제공합니다. 이 API에 대한 응답으로 수신된 정보는 Unified Manager UI의 대시보드를 채우는 데 사용됩니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/workloads-summary

API를 사용하여 액세스 엔드포인트 관리

스토리지 가상 머신(SVM), LUN 및 파일 공유를 프로비저닝하는 데 필요한 액세스 엔드포인트 또는 논리 인터페이스(LIF)를 만들어야 합니다. Active IQ Unified Manager 환경에서 SVM, LUN 또는 파일 공유에 대한 액세스 엔드포인트를 보고, 만들고, 수정하고, 삭제할 수 있습니다.

액세스 엔드포인트 보기

다음 방법을 사용하여 Unified Manager 환경에서 액세스 엔드포인트 목록을 볼 수 있습니다. 특정 SVM, LUN 또는 파일 공유의 액세스 엔드포인트 목록을 쿼리하려면 SVM, LUN 또는 파일 공유에 대한 고유 식별자를 입력해야 합니다. 고유한 액세스 엔드포인트 키를 입력하여 특정 액세스 엔드포인트의 세부 정보를 검색할 수도 있습니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

액세스 엔드포인트 추가

사용자 정의 액세스 엔드포인트를 만들고 필요한 속성을 할당할 수 있습니다. 생성하려는 액세스 엔드포인트의 세부 정보를 입력 매개변수로 입력해야 합니다. 이 API나 시스템 관리자 또는 ONTAP CLI를 사용하여 각 노드에 액세스 엔드포인트를 만들 수 있습니다. 액세스 엔드포인트 생성에는 IPv4 및 IPv6 주소가 모두 지원됩니다.



LUN과 파일 공유를 성공적으로 프로비저닝하려면 노드당 최소한의 액세스 엔드포인트 수로 SVM을 구성해야 합니다. 노드당 최소 두 개의 액세스 엔드포인트로 SVM을 구성해야 합니다. 하나는 CIFS 및 /또는 NFS 프로토콜을 지원하고, 다른 하나는 iSCSI 또는 FCP 프로토콜을 지원합니다.

범주	HTTP 동사	길
스토리지 제공자	우편	/storage-provider/access-endpoints

액세스 엔드포인트 삭제

다음 방법을 사용하여 특정 액세스 엔드포인트를 삭제할 수 있습니다. 특정 액세스 엔드포인트를 삭제하려면 액세스 엔드포인트 키를 입력 매개변수로 제공해야 합니다.

범주	HTTP 동사	길
스토리지 제공자	삭제	/storage-provider/access-endpoints/{key}

액세스 엔드포인트 수정

다음 방법을 사용하여 액세스 엔드포인트를 수정하고 해당 속성을 업데이트할 수 있습니다. 특정 액세스 엔드포인트를 수정하려면 액세스 엔드포인트 키를 제공해야 합니다. 또한 업데이트하려는 속성과 해당 속성을 입력해야 합니다.

범주	HTTP 동사	길
스토리지 제공자	반점	/storage-provider/access-endpoints/{key}

API를 사용하여 Active Directory 매핑 관리

여기에 나열된 API를 사용하면 SVM에서 CIFS 공유를 프로비저닝하는 데 필요한 Active Directory 매핑을 SVM에서 관리할 수 있습니다. SVM을 ONTAP 에 매핑하려면 Active Directory 매핑을 구성해야 합니다.

Active Directory 매핑 보기

다음 방법을 사용하여 SVM에 대한 Active Directory 매핑의 구성 세부 정보를 볼 수 있습니다. SVM에서 Active Directory 매핑을 보려면 SVM 키를 입력해야 합니다. 특정 매핑의 세부 정보를 쿼리하려면 매핑 키를 입력해야 합니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/active-directories-mappings /storage-provider/active-directories-mappings/{key}

Active Directory 매핑 추가

다음 방법을 사용하여 SVM에서 Active Directory 매핑을 만들 수 있습니다. 매핑 세부 정보를 입력 매개변수로 입력해야 합니다.

범주	HTTP 동사	길
스토리지 제공자	우편	/storage-provider/active-directories-mappings

API를 사용하여 파일 공유 관리

당신은 사용할 수 있습니다 /storage-provider/file-shares 데이터 센터 환경에서 CIFS 및 NFS 파일 공유 볼륨을 보고, 추가하고, 수정하고, 삭제할 수 있는 API입니다.

파일 공유 볼륨을 프로비저닝하기 전에 SVM이 생성되었고 지원되는 프로토콜로 프로비저닝되었는지 확인하세요. 프로비저닝 중에 성능 서비스 수준(PSL)이나 스토리지 효율성 정책(SEP)을 할당하는 경우 파일 공유를 만들기 전에 PSL이나 SEP를 만들어야 합니다.

파일 공유 보기

다음 방법을 사용하면 Unified Manager 환경에서 사용 가능한 파일 공유 볼륨을 볼 수 있습니다. Active IQ Unified Manager 에서 ONTAP 클러스터를 데이터 소스로 추가하면 해당 클러스터의 스토리지 워크로드가 Unified Manager 인스턴스에 자동으로 추가됩니다. 이 API는 Unified Manager 인스턴스에 자동 및 수동으로 추가된 파일 공유를 검색합니다. 이 API를 파일 공유 키와 함께 실행하면 특정 파일 공유의 세부 정보를 볼 수 있습니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/file-shares /storage-provider/file-shares/{key}

파일 공유 추가

다음 방법을 사용하여 SVM에 CIFS 및 NFS 파일 공유를 추가할 수 있습니다. 생성하려는 파일 공유의 세부 정보를 입력 매개변수로 입력해야 합니다. 이 API를 사용하여 FlexGroup 볼륨을 추가할 수 없습니다.

범주	HTTP 동사	길
스토리지 제공자	우편	/storage-provider/file-shares



액세스 제어 목록(ACL) 매개변수 또는 내보내기 정책 매개변수가 제공되는지에 따라 CIFS 공유 또는 NFS 파일 공유가 생성됩니다. ACL 매개변수에 대한 값을 제공하지 않으면 CIFS 공유가 생성되지 않고, 기본적으로 NFS 공유가 생성되어 모든 사용자에게 액세스 권한이 제공됩니다.

데이터 보호 볼륨 생성: SVM에 파일 공유를 추가하면 기본적으로 마운트되는 볼륨 유형은 다음과 같습니다. rw (읽기-쓰기). 데이터 보호(DP) 볼륨을 생성하려면 다음을 지정하세요. dp 에 대한 값으로서 type 매개변수.

파일 공유 삭제

다음 방법을 사용하여 특정 파일 공유를 삭제할 수 있습니다. 특정 파일 공유를 삭제하려면 파일 공유 키를 입력 매개변수로 입력해야 합니다.

범주	HTTP 동사	길
스토리지 제공자	삭제	/storage-provider/file-shares/{key}

파일 공유 수정

다음 방법을 사용하여 파일 공유를 수정하고 속성을 업데이트할 수 있습니다.

특정 파일 공유를 수정하려면 파일 공유 키를 제공해야 합니다. 또한, 업데이트하려는 속성과 해당 속성을 입력해야 합니다.



이 API를 한 번 호출하면 속성을 하나만 업데이트할 수 있습니다. 여러 개의 업데이트가 있는 경우 이 API를 여러 번 실행해야 합니다.

범주	HTTP 동사	길
스토리지 제공자	반점	/storage-provider/file-shares/{key}

API를 사용하여 LUN 관리

당신은 사용할 수 있습니다 /storage-provider/luns 데이터 센터 환경에서 LUN을 보고, 추가하고, 수정하고, 삭제하기 위한 API입니다.

LUN을 프로비저닝하기 전에 SVM이 생성되었고 지원되는 프로토콜로 프로비저닝되었는지 확인하세요. 프로비저닝 중에 성능 서비스 수준(PSL)이나 스토리지 효율성 정책(SEP)을 할당하는 경우 LUN을 생성하기 전에 PSL이나 SEP를

생성해야 합니다.

LUN 보기

다음 방법을 사용하여 Unified Manager 환경에서 LUN을 볼 수 있습니다. Active IQ Unified Manager 에서 ONTAP 클러스터를 데이터 소스로 추가하면 해당 클러스터의 스토리지 워크로드가 Unified Manager 인스턴스에 자동으로 추가됩니다. 이 API는 Unified Manager 인스턴스에 자동 및 수동으로 추가된 모든 LUN을 검색합니다. LUN 키로 이 API를 실행하면 특정 LUN의 세부 정보를 볼 수 있습니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/luns /storage-provider/luns/{key}

LUN 추가

다음 방법을 사용하여 SVM에 LUN을 추가할 수 있습니다.

범주	HTTP 동사	길
스토리지 제공자	우편	/storage-provider/luns



cURL 요청에서 입력에 선택적 매개변수 `volume_name_tag`에 대한 값을 제공하면 LUN을 생성하는 동안 볼륨의 이름을 지정할 때 해당 값이 사용됩니다. 이 태그를 사용하면 볼륨을 쉽게 검색할 수 있습니다. 요청 시 볼륨 키를 제공하면 태그 지정이 건너뛰됩니다.

LUN 삭제

다음 방법을 사용하여 특정 LUN을 삭제할 수 있습니다. 특정 LUN을 삭제하려면 LUN 키를 제공해야 합니다.



ONTAP 에서 볼륨을 생성한 다음 Unified Manager를 통해 해당 볼륨에 LUN을 프로비저닝한 경우 이 API를 사용하여 모든 LUN을 삭제하면 ONTAP 클러스터에서도 볼륨이 삭제됩니다.

범주	HTTP 동사	길
스토리지 제공자	삭제	/storage-provider/luns/{key}

LUN 수정

다음 방법을 사용하여 LUN을 수정하고 속성을 업데이트할 수 있습니다. 특정 LUN을 수정하려면 LUN 키를 제공해야 합니다. 업데이트하려는 LUN 속성과 해당 값도 입력해야 합니다. 이 API를 사용하여 LUN 어레이를 업데이트하려면 "API 사용에 대한 권장 사항"의 권장 사항을 검토해야 합니다.



이 API를 한 번 호출하면 속성을 하나만 업데이트할 수 있습니다. 여러 개의 업데이트가 있는 경우 이 API를 여러 번 실행해야 합니다.

범주	HTTP 동사	길
스토리지 제공자	반점	/storage-provider/luns/{key}

API를 사용하여 성능 서비스 수준 관리

Active IQ Unified Manager 의 스토리지 공급자 API를 사용하여 성능 서비스 수준을 보고, 만들고, 수정하고, 삭제할 수 있습니다.

성능 서비스 수준 보기

다음 방법을 사용하면 스토리지 작업 부하에 할당하기 위한 성능 서비스 수준을 볼 수 있습니다. API는 시스템에서 정의한 성능 서비스 수준과 사용자가 생성한 성능 서비스 수준을 모두 나열하고 모든 성능 서비스 수준의 속성을 검색합니다. 특정 성과 서비스 수준을 쿼리하려면 성과 서비스 수준의 고유 ID를 입력하여 세부 정보를 검색해야 합니다.

범주	HTTP 동사	길
스토리지 제공자	연다	/storage-provider/performance-service-levels /storage-provider/performance-service-levels/{key}

성능 서비스 수준 추가

시스템에서 정의한 성능 서비스 수준이 스토리지 워크로드에 필요한 서비스 수준 목표(SLO)를 충족하지 못하는 경우, 다음 방법을 사용하여 사용자 정의 성능 서비스 수준을 만들고 이를 스토리지 워크로드에 할당할 수 있습니다. 생성하려는 성과 서비스 수준에 대한 세부 정보를 입력하세요. IOPS 속성의 경우 유효한 값 범위를 입력했는지 확인하세요.

범주	HTTP 동사	길
스토리지 제공자	우편	/storage-provider/performance-service-levels

성능 서비스 수준 삭제

다음 방법을 사용하여 특정 성능 서비스 수준을 삭제할 수 있습니다. 작업 부하에 할당된 성능 서비스 수준이거나 사용 가능한 유일한 성능 서비스 수준인 경우 성능 서비스 수준을 삭제할 수 없습니다. 특정 성과 서비스 수준을 삭제하려면 성과 서비스 수준의 고유 ID를 입력 매개변수로 제공해야 합니다.

범주	HTTP 동사	길
스토리지 제공자	삭제	/storage-provider/performance-service-levels/{key}

성능 서비스 수준 수정

다음 방법을 사용하여 성능 서비스 수준을 수정하고 해당 속성을 업데이트할 수 있습니다. 시스템에서 정의되거나 작업 부하에 할당된 성능 서비스 수준은 수정할 수 없습니다. 특정 성능 서비스 수준을 수정하려면 고유 ID를 제공해야 합니다. 업데이트하려는 IOPS 속성과 유효한 값을 입력해야 합니다.

범주	HTTP 동사	길
스토리지 제공자	반점	/storage-provider/performance-service-levels/{key}

성능 서비스 수준에 따른 집계 기능 보기

다음 방법을 사용하면 성능 서비스 수준을 기반으로 집계 기능을 쿼리할 수 있습니다. 이 API는 데이터 센터에서 사용 가능한 집계 목록을 반환하고 해당 집계에서 지원할 수 있는 성능 서비스 수준 측면에서 기능을 나타냅니다. 볼륨에 워크로드를 프로비저닝하는 동안 특정 성능 서비스 수준을 지원하는 집계 기능을 확인하고 해당 기능에 따라 워크로드를 프로비저닝할 수 있습니다. 집계를 지정하는 기능은 API를 사용하여 워크로드를 프로비저닝하는 경우에만 사용할 수 있습니다. 이 기능은 Unified Manager 웹 UI에서 사용할 수 없습니다.

범주	HTTP 동사	길
스토리지 제공자	연다	/storage-provider/aggregate-capabilities /storage-provider/aggregate-capabilities/{key}

API를 사용하여 스토리지 효율성 정책 관리

스토리지 공급자 API를 사용하여 스토리지 효율성 정책을 보고, 만들고, 수정하고, 삭제할 수 있습니다.

다음 사항에 유의하세요.



- Unified Manager에서 워크로드를 생성하는 동안 스토리지 효율성 정책을 할당하는 것은 필수가 아닙니다.
- 정책이 워크로드에 할당된 후에는 워크로드에서 스토리지 효율성 정책의 할당을 해제할 수 없습니다.
- 워크로드에 중복 제거 및 압축과 같은 일부 스토리지 설정이 ONTAP 볼륨에 지정된 경우, Unified Manager에서 스토리지 워크로드를 추가할 때 적용하는 스토리지 효율성 정책에 지정된 설정으로 해당 설정을 덮어쓸 수 있습니다.

스토리지 효율성 정책 보기

다음 방법을 사용하면 스토리지 워크로드에 스토리지 효율성 정책을 할당하기 전에 해당 정책을 볼 수 있습니다. 이 API는 시스템에서 정의한 모든 스토리지 효율성 정책과 사용자가 생성한 모든 스토리지 효율성 정책을 나열하고 모든 스토리지 효율성 정책의 속성을 검색합니다. 특정 스토리지 효율성 정책을 쿼리하려면 정책의 고유 ID를 입력하여 세부 정보를 검색해야 합니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	<code>/storage-provider/storage-efficiency-policies</code> <code>/storage-provider/storage-efficiency-policies/{key}</code>

스토리지 효율성 정책 추가

다음 방법을 사용하여 사용자 지정 스토리지 효율성 정책을 만들고, 시스템 정의 정책이 스토리지 워크로드에 대한 프로비저닝 요구 사항을 충족하지 못하는 경우 해당 정책을 스토리지 워크로드에 할당할 수 있습니다. 생성하려는 스토리지 효율성 정책의 세부 정보를 입력 매개변수로 입력합니다.

범주	HTTP 동사	길
스토리지 제공자	우편	<code>/storage-provider/storage-efficiency-policies</code>

스토리지 효율성 정책 삭제

다음 방법을 사용하여 특정 스토리지 효율성 정책을 삭제할 수 있습니다. 워크로드에 할당된 스토리지 효율성 정책이나 사용 가능한 유일한 스토리지 효율성 정책인 경우 스토리지 효율성 정책을 삭제할 수 없습니다. 특정 스토리지 효율성 정책을 삭제하려면 스토리지 효율성 정책의 고유 ID를 입력 매개변수로 제공해야 합니다.

범주	HTTP 동사	길
스토리지 제공자	삭제	<code>/storage-provider/storage-efficiency-policies/{key}</code>

다음 방법을 사용하여 저장소 효율성 정책을 수정하고 해당 속성을 업데이트할 수 있습니다. 시스템에서 정의되거나 워크로드에 할당된 스토리지 효율성 정책은 수정할 수 없습니다. 특정 스토리지 효율성 정책을 수정하려면 스토리지 효율성 정책의 고유 ID를 제공해야 합니다. 또한, 업데이트하려는 부동산과 그 가치를 제공해야 합니다.

범주	HTTP 동사	길
스토리지 제공자	반점	/storage-provider/storage-efficiency-policies/{key}

스토리지 관리를 위한 공통 API 워크플로

공통 워크플로는 클라이언트 애플리케이션 개발자에게 Active IQ Unified Manager API가 클라이언트 애플리케이션에서 어떻게 호출되어 공통 스토리지 관리 기능을 실행할 수 있는지에 대한 예를 제공합니다. 이 섹션에는 몇 가지 샘플 워크플로가 포함되어 있습니다.

워크플로에서는 일반적으로 사용되는 스토리지 관리 사용 사례 중 일부를 설명하고, 사용할 수 있는 샘플 코드도 제공합니다. 각 작업은 하나 이상의 API 호출로 구성된 워크플로 프로세스를 사용하여 설명됩니다.

워크플로에서 사용되는 **API** 호출을 이해합니다.

Unified Manager 인스턴스에서 모든 REST API 호출에 대한 세부 정보가 포함된 온라인 문서 페이지를 볼 수 있습니다. 이 문서에서는 온라인 문서의 세부 내용을 반복하지 않습니다. 이 문서의 워크플로 샘플에서 사용된 각 API 호출에는 설명서 페이지에서 호출을 찾는 데 필요한 정보만 포함되어 있습니다. 특정 API 호출을 찾으려면 입력 매개변수, 출력 형식, HTTP 상태 코드, 요청 처리 유형을 포함한 호출의 전체 세부 정보를 검토할 수 있습니다.

워크플로 내의 각 API 호출에 대해 다음 정보가 포함되어 있어 설명서 페이지에서 호출을 찾는 데 도움이 됩니다.

- 카테고리: API 호출은 문서 페이지에서 기능적으로 관련된 영역이나 카테고리로 정리됩니다. 특정 API 호출을 찾으려면 페이지 하단으로 스크롤하여 해당 API 범주를 클릭하세요.
- HTTP 동사(호출): HTTP 동사는 리소스에서 수행되는 작업을 식별합니다. 각 API 호출은 단일 HTTP 동사를 통해 실행됩니다.
- 경로: 경로는 호출을 수행하는 일부로 작업이 적용되는 특정 리소스를 결정합니다. 경로 문자열은 핵심 URL에 추가되어 리소스를 식별하는 완전한 URL을 형성합니다.

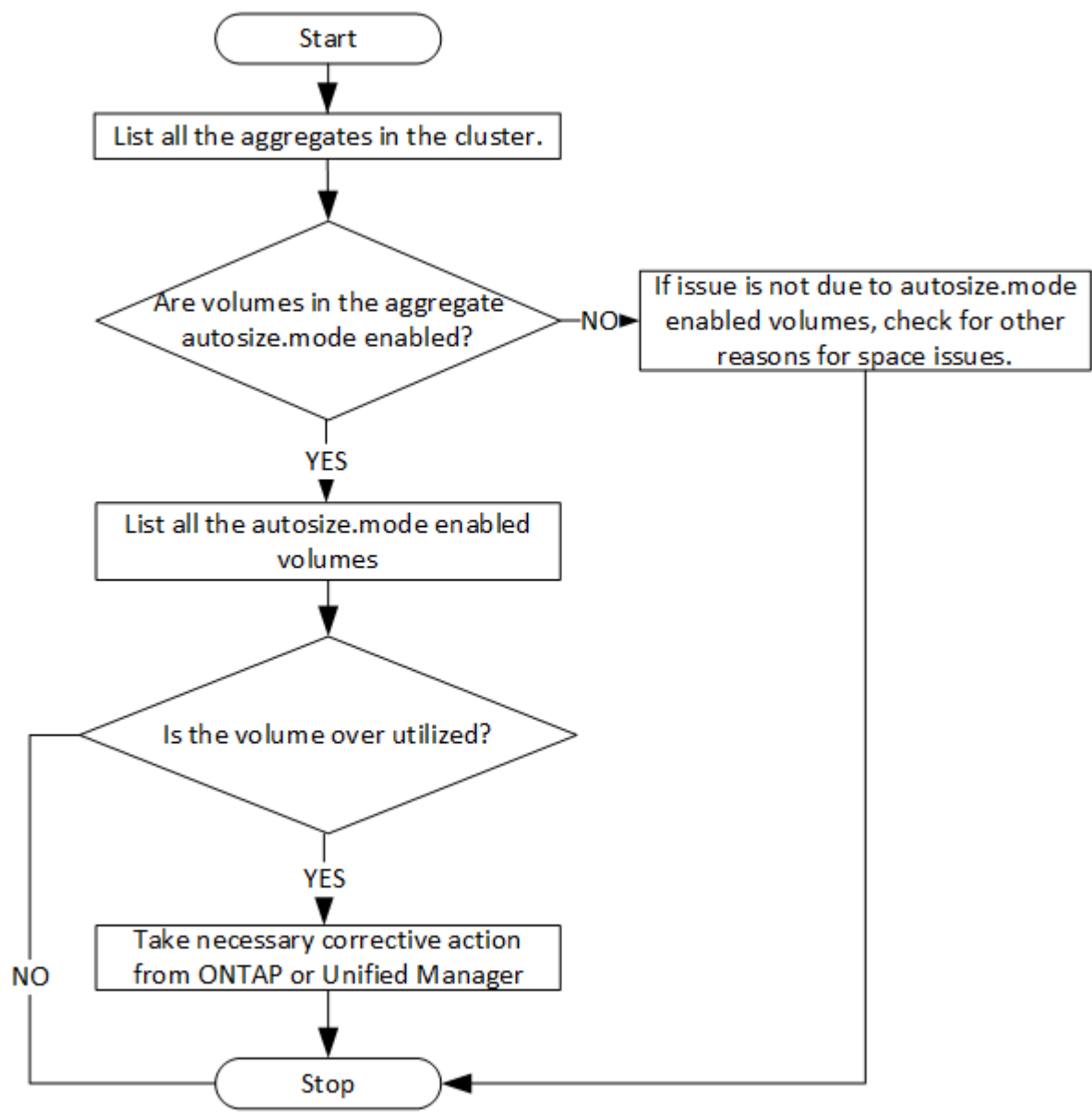
API를 사용하여 집계 공간 문제 확인

Active IQ Unified Manager의 데이터 센터 API를 사용하면 볼륨의 공간 가용성과 활용도를 모니터링할 수 있습니다. 볼륨의 공간 문제를 파악하고 과도하게 활용되거나 활용도가 낮은 스토리지 리소스를 식별할 수 있습니다.

집계를 위한 데이터 센터 API는 사용 가능한 공간과 사용된 공간, 공간 절약 효율성 설정에 대한 관련 정보를 검색합니다. 검색된 정보를 지정된 속성을 기준으로 필터링할 수도 있습니다.

집계에서 공간 부족을 확인하는 한 가지 방법은 자동 크기 조정 모드가 활성화된 볼륨이 환경에 있는지 확인하는 것입니다. 그런 다음 과도하게 사용되는 볼륨을 파악하고 이를 수정하기 위한 조치를 취해야 합니다.

다음 흐름도는 자동 크기 조정 모드가 활성화된 볼륨에 대한 정보를 검색하는 프로세스를 보여줍니다.



이 흐름에서는 클러스터가 이미 ONTAP 에 생성되어 Unified Manager에 추가되었다고 가정합니다.

1. 값을 알지 못하는 경우 클러스터 키를 얻으세요.

범주	HTTP 동사	길
데이터센터	얻다	/datacenter/cluster/clusters

2. 클러스터 키를 필터 매개변수로 사용하여 해당 클러스터의 집계를 쿼리합니다.

범주	HTTP 동사	길
데이터센터	얻다	/datacenter/storage/aggregates

- 응답을 통해 집계 공간 사용을 분석하고 어떤 집계에 공간 문제가 있는지 확인합니다. 공간 문제가 있는 각 집계에 대해 동일한 JSON 출력에서 집계 키를 얻습니다.
- 각 집계 키를 사용하여 autosize.mode 매개변수에 대한 값을 갖는 모든 볼륨을 필터링합니다. grow.

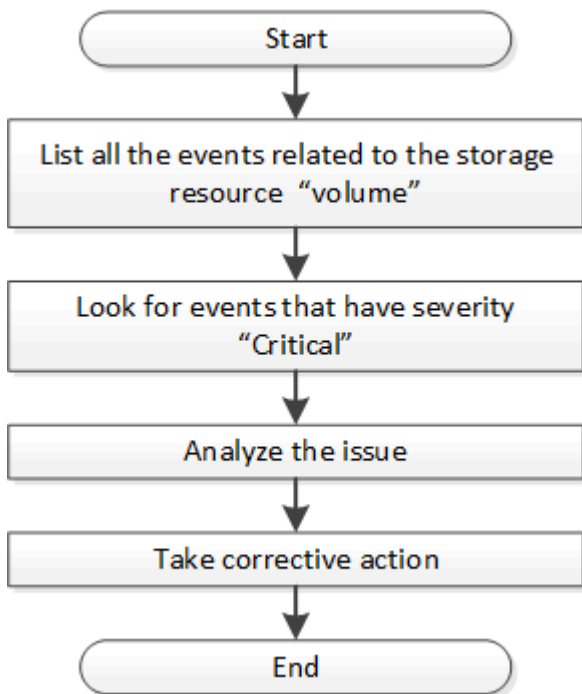
범주	HTTP 동사	길
데이터센터	얻다	/datacenter/storage/volumes

- 과도하게 활용되고 있는 볼륨을 분석합니다.
- 볼륨의 공간 문제를 해결하기 위해 볼륨을 여러 집계로 옮기는 등 필요한 시정 조치를 수행합니다. ONTAP 또는 Unified Manager 웹 UI에서 이러한 작업을 수행할 수 있습니다.

이벤트 API를 사용하여 스토리지 객체의 문제 확인

데이터 센터의 스토리지 객체가 임계값을 넘으면 해당 이벤트에 대한 알림을 받게 됩니다. 이 알림을 사용하면 문제를 분석하고 다음 방법으로 시정 조치를 취할 수 있습니다. events 아피스.

이 워크플로는 볼륨을 리소스 개체로 예로 들어 설명합니다. 당신은 사용할 수 있습니다 events 볼륨과 관련된 이벤트 목록을 검색하고, 해당 볼륨의 중요한 문제를 분석한 다음, 문제를 바로잡기 위한 시정 조치를 취하는 API입니다.



시정 조치를 취하기 전에 다음 단계에 따라 볼륨의 문제를 확인하세요.

단계

1. 데이터 센터의 볼륨에 대한 중요한 Active IQ Unified Manager 이벤트 알림을 분석합니다.
2. /management-server/events API에서 다음 매개변수를 사용하여 볼륨의 모든 이벤트를 쿼리합니다.

```
"resource_type": "volume"  
"severity": "critical"
```

범주	HTTP 동사	길
관리 서버	얻다	/관리-서버/이벤트

3. 출력을 보고 특정 볼륨의 문제를 분석합니다.
4. Unified Manager REST API나 웹 UI를 사용하여 필요한 작업을 수행하여 문제를 해결합니다.

게이트웨이 API를 사용하여 ONTAP 볼륨 문제 해결

게이트웨이 API는 ONTAP API를 호출하여 ONTAP 스토리지 객체에 대한 정보를 쿼리하고 보고된 문제를 해결하기 위한 시정 조치를 취하는 게이트웨이 역할을 합니다.

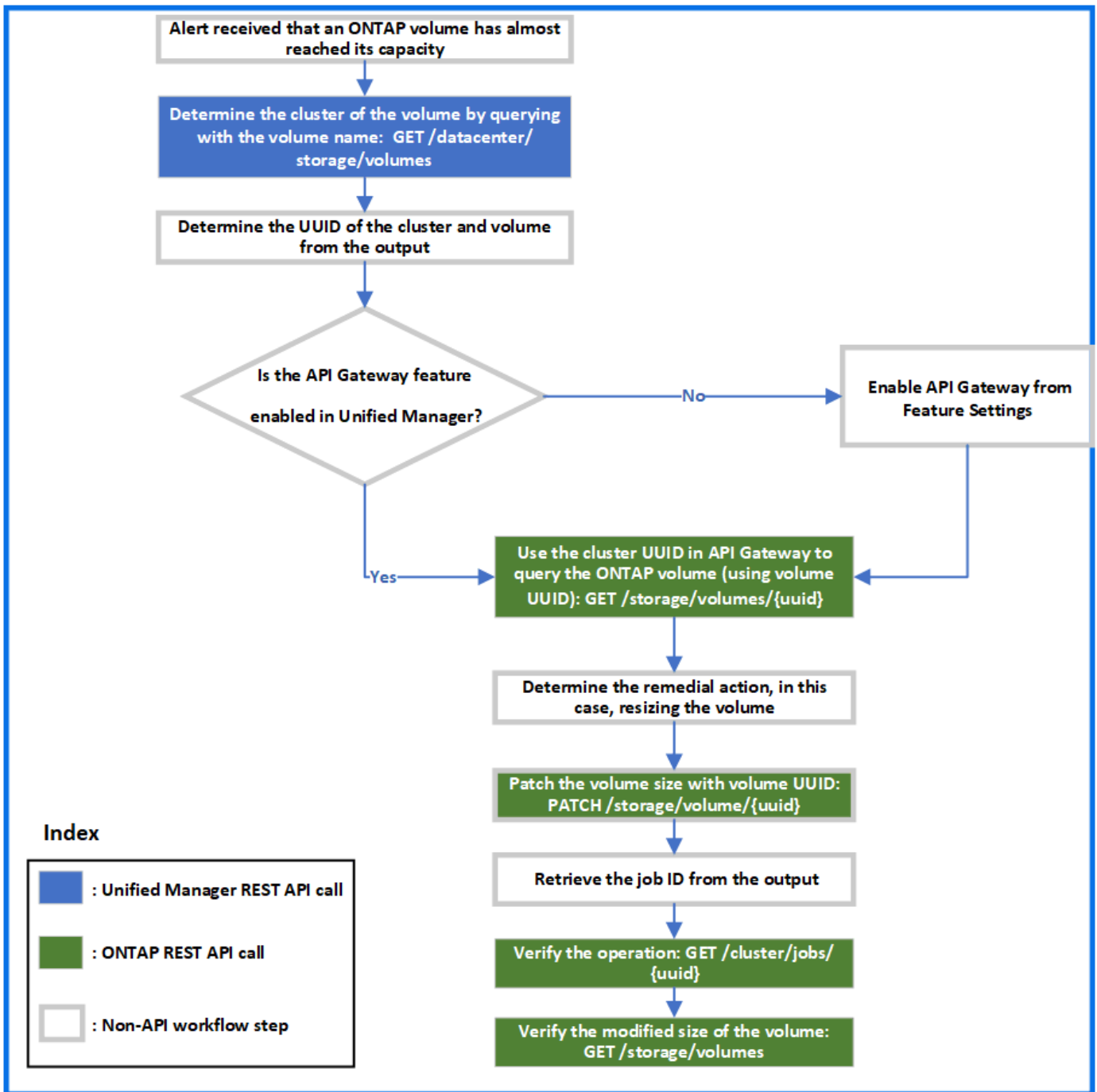
이 워크플로는 ONTAP 볼륨이 용량에 거의 도달했을 때 이벤트가 발생하는 샘플 사용 사례를 다룹니다. 또한 이 워크플로는 Active IQ Unified Manager 와 ONTAP REST API를 결합하여 이 문제를 해결하는 방법을 보여줍니다.

워크플로 단계를 실행하기 전에 다음 사항을 확인하세요.



- 게이트웨이 API와 그 사용 방법을 알고 있습니다. 자세한 내용은 다음을 참조하세요. "[프록시 액세스를 통해 ONTAP API에 액세스](#)".
- ONTAP REST API의 사용법을 알고 계십니다. ONTAP REST API 사용에 대한 정보는 다음을 참조하세요. <https://docs.netapp.com/us-en/ontap-automation/index.html>["ONTAP 자동화 문서"] .
- 귀하는 애플리케이션 관리자입니다.
- REST API 작업을 실행하려는 클러스터는 ONTAP 9.5 이상에서 지원되며, 해당 클러스터는 HTTPS를 통해 Unified Manager에 추가됩니다.

다음 다이어그램은 ONTAP 볼륨 용량 사용 문제를 해결하기 위한 워크플로의 각 단계를 보여줍니다.



워크플로는 Unified Manager와 ONTAP REST API의 호출 지점을 모두 다룹니다.

1. 볼륨 용량 사용률을 알리는 이벤트에서 볼륨 이름을 기록해 둡니다.
2. 볼륨 이름을 이름 매개변수의 값으로 사용하여 다음 Unified Manager API를 실행하여 볼륨을 쿼리합니다.

범주	HTTP 동사	길
데이터센터	얻다	/datacenter/storage/volumes

3. 출력에서 클러스터 UUID와 볼륨 UUID를 검색합니다.

4. Unified Manager 웹 UI에서 일반 > 기능 설정 > *API Gateway*로 이동하여 API Gateway 기능이 활성화되어 있는지 확인합니다. 활성화하지 않으면 게이트웨이 카테고리의 API를 호출할 수 없습니다. 해당 기능이 비활성화되어 있으면 활성화하세요.
5. 클러스터 UUID를 사용하여 ONTAP API를 실행합니다./storage/volumes/{uuid} API 게이트웨이를 통해. 볼륨 UUID가 API 매개변수로 전달되면 쿼리는 볼륨 세부 정보를 반환합니다.

API 게이트웨이를 통해 ONTAP API를 실행하는 경우 Unified Manager 자격 증명이 인증을 위해 내부적으로 전달되므로 개별 클러스터 액세스에 대해 추가 인증 단계를 실행할 필요가 없습니다.

범주	HTTP 동사	길
통합 관리자: 게이트웨이 ONTAP: 스토리지	얻다	게이트웨이 API: /gateways/{uuid}/{path} ONTAP API: /storage/volumes/{uuid}



/gateways/{uuid}/{path}에서 {uuid}의 값은 REST 작업이 수행될 클러스터 UUID로 대체되어야 합니다. {path}는 ONTAP REST URL /storage/volumes/{uuid}로 대체되어야 합니다.

첨부된 URL은 다음과 같습니다. /gateways/{cluster_uuid}/storage/volumes/{volume_uuid}

GET 작업을 실행하면 생성된 URL은 다음과 같습니다.

GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes/{volume_uuid}

샘플 cURL 명령

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7"
-H "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

6. 출력 결과를 바탕으로 크기, 사용법, 시정 조치를 결정합니다. 이 워크플로에서 취해지는 시정 조치는 볼륨 크기를 조정하는 것입니다.
7. 클러스터 UUID를 사용하고 API 게이트웨이를 통해 다음 ONTAP API를 실행하여 볼륨 크기를 조정합니다. 게이트웨이 및 ONTAP API의 입력 매개변수에 대한 자세한 내용은 5단계를 참조하세요.

범주	HTTP 동사	길
통합 관리자: 게이트웨이 ONTAP: 스토리지	반점	게이트웨이 API: /gateways/{uuid}/{path} ONTAP API: /storage/volumes/{uuid}



클러스터 UUID와 볼륨 UUID와 함께 볼륨 크기를 조정하기 위한 크기 매개변수 값을 입력해야 합니다. 값을 바이트 단위로 입력하세요. 예를 들어, 볼륨 크기를 100GB에서 120GB로 늘리려면 쿼리 끝에 매개변수 크기 값을 입력합니다. `-d {"size": 128849018880}`

샘플 cURL 명령

```
curl -X PATCH "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>" -d {"size": 128849018880}"
```

JSON 출력은 작업 UUID를 반환합니다.

- 작업 UUID를 사용하여 작업이 성공적으로 실행되었는지 확인합니다. 클러스터 UUID와 작업 UUID를 사용하여 API 게이트웨이를 통해 다음 ONTAP API를 실행합니다. 게이트웨이 및 ONTAP API의 입력 매개변수에 대한 자세한 내용은 5단계를 참조하세요.

범주	HTTP 동사	길
통합 관리자: 게이트웨이 ONTAP: 클러스터	업데이트	게이트웨이 API: /gateways/{uuid}/{path} ONTAP API: /cluster/jobs/{uuid}

반환된 HTTP 코드는 ONTAP REST API HTTP 상태 코드와 동일합니다.

- 다음 ONTAP API를 실행하여 크기가 조정된 볼륨의 세부 정보를 쿼리합니다. 게이트웨이 및 ONTAP API의 입력 매개변수에 대한 자세한 내용은 5단계를 참조하세요.

범주	HTTP 동사	길
통합 관리자: 게이트웨이 ONTAP: 스토리지	업데이트	게이트웨이 API: /gateways/{uuid}/{path} ONTAP API: /storage/volumes/{uuid}

출력에서는 볼륨 크기가 120GB로 증가한 것으로 표시됩니다.

워크로드 관리를 위한 API 워크플로

Active IQ Unified Manager 사용하면 스토리지 워크로드(LUN, NFS 파일 공유, CIFS 공유)를 프로비저닝하고 수정할 수 있습니다. 프로비저닝은 스토리지 가상 머신(SVM) 생성부터 스토리지 워크로드에 성능 서비스 수준 및 스토리지 효율성 정책 적용까지 여러 단계로 구성됩니다.

워크로드 수정은 특정 매개변수를 수정하고 해당 매개변수에 추가 기능을 활성화하는 단계로 구성됩니다.

다음 워크플로가 설명되어 있습니다.

- Unified Manager에서 스토리지 가상 머신(SVM)을 프로비저닝하기 위한 워크플로입니다.



이 워크플로는 Unified Manager에서 LUN이나 파일 공유를 프로비저닝하기 전에 수행해야 합니다.

- 파일 공유 프로비저닝.
- LUN 프로비저닝.
- LUN 및 파일 공유 수정(스토리지 작업 부하에 대한 성능 서비스 수준 매개변수를 업데이트하는 예를 사용).
- CIFS 프로토콜을 지원하도록 NFS 파일 공유 수정
- QoS를 AQoS로 업그레이드하기 위해 워크로드 수정



각 프로비저닝 워크플로(LUN 및 파일 공유)에 대해 클러스터의 SVM을 확인하기 위한 워크플로를 완료했는지 확인하세요.

워크플로에서 각 API를 사용하기 전에 권장 사항과 제한 사항을 꼭 읽어보세요. API에 대한 관련 세부 정보는 관련 개념 및 참조에 나열된 개별 섹션에서 확인할 수 있습니다.

API를 사용하여 클러스터의 SVM 확인

파일 공유나 LUN을 프로비저닝하기 전에 클러스터에 SVM(스토리지 가상 머신)이 생성되었는지 확인해야 합니다.



워크플로는 ONTAP 클러스터가 Unified Manager에 추가되었고 클러스터 키가 획득되었다고 가정합니다. 클러스터에는 LUN과 파일 공유를 프로비저닝하는 데 필요한 라이선스가 있어야 합니다.

1. 클러스터에 SVM이 생성되었는지 확인합니다.

범주	HTTP 동사	길
데이터센터	얻다	/datacenter/svm/svms /datacenter/svm/svms/{key }

샘플 cURL

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. SVM 키가 반환되지 않으면 SVM을 생성합니다. SVM을 생성하려면 SVM을 프로비저닝하는 클러스터 키가 필요합니다. SVM 이름도 지정해야 합니다. 다음 단계를 따르세요.

범주	HTTP 동사	길
데이터센터	얻다	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}

클러스터 키를 가져옵니다.

샘플 cURL

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

3. 출력에서 클러스터 키를 가져온 다음 SVM을 생성하기 위한 입력으로 사용합니다.



SVM을 생성하는 동안 CIFS, NFS, FCP, iSCSI 등 LUN과 파일 공유를 프로비저닝하는 데 필요한 모든 프로토콜을 지원하는지 확인하세요. SVM이 필요한 서비스를 지원하지 않으면 프로비저닝 워크플로가 실패할 수 있습니다. 각 유형의 워크로드에 대한 서비스도 SVM에서 활성화하는 것이 좋습니다.

범주	HTTP 동사	길
데이터센터	우편	/datacenter/svm/svms

샘플 cURL

SVM 객체 세부 정보를 입력 매개변수로 입력합니다.

```
curl -X POST "https://<hostname>/api/datacenter/svm/svms" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>" "{ \"aggregates\": [ { \"_links\": {}, \"key\": \"1cd8a442-86d1,type=objecttype,uid=1cd8a442-86d1-11e0-ae1c-9876567890123\", \"name\": \"cluster2\", \"uuid\": \"02c9e252-41be-11e9-81d5-00a0986138f7\" } ], \"cifs\": { \"ad_domain\": { \"fqdn\": \"string\", \"password\": \"string\", \"user\": \"string\" }, \"enabled\": true, \"name\": \"CIFS1\" }, \"cluster\": { \"key\": \"1cd8a442-86d1-11e0-ae1c-123478563412,type=object type,uid=1cd8a442-86d1-11e0-ae1c-9876567890123\" }, \"dns\": { \"domains\": [ \"example.com\", \"example2.example3.com\" ], \"servers\": [ \"10.224.65.20\", \"2001:db08:a0b:12f0::1\" ] }, \"fcg\": { \"enabled\": true }, \"ip_interface\": [ { \"enabled\": true, \"ip\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" } }, \"location\": { \"home_node\": { \"name\": \"node1\" } }, \"name\": \"dataLif1\" } ], \"ipspace\": { \"name\": \"exchange\" }, \"iscsi\": { \"enabled\": true }, \"language\": \"c.utf_8\", \"ldap\": { \"ad_domain\": \"string\", \"base_dn\": \"string\", \"bind_dn\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ] }, \"name\": \"svm1\", \"nfs\": { \"enabled\": true }, \"nis\": { \"domain\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ] }, \"nvme\": { \"enabled\": true }, \"routes\": [ { \"destination\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" }, \"gateway\": \"string\" } ], \"snapshot_policy\": { \"name\": \"default\" }, \"state\": \"running\", \"subtype\": \"default\"}"
```

JSON 출력에는 생성한 SVM을 확인하는 데 사용할 수 있는 Job 개체 키가 표시됩니다.

4. 쿼리에 대한 작업 객체 키를 사용하여 SVM 생성을 확인합니다. SVM이 성공적으로 생성되면 SVM 키가 응답으로 반환됩니다.

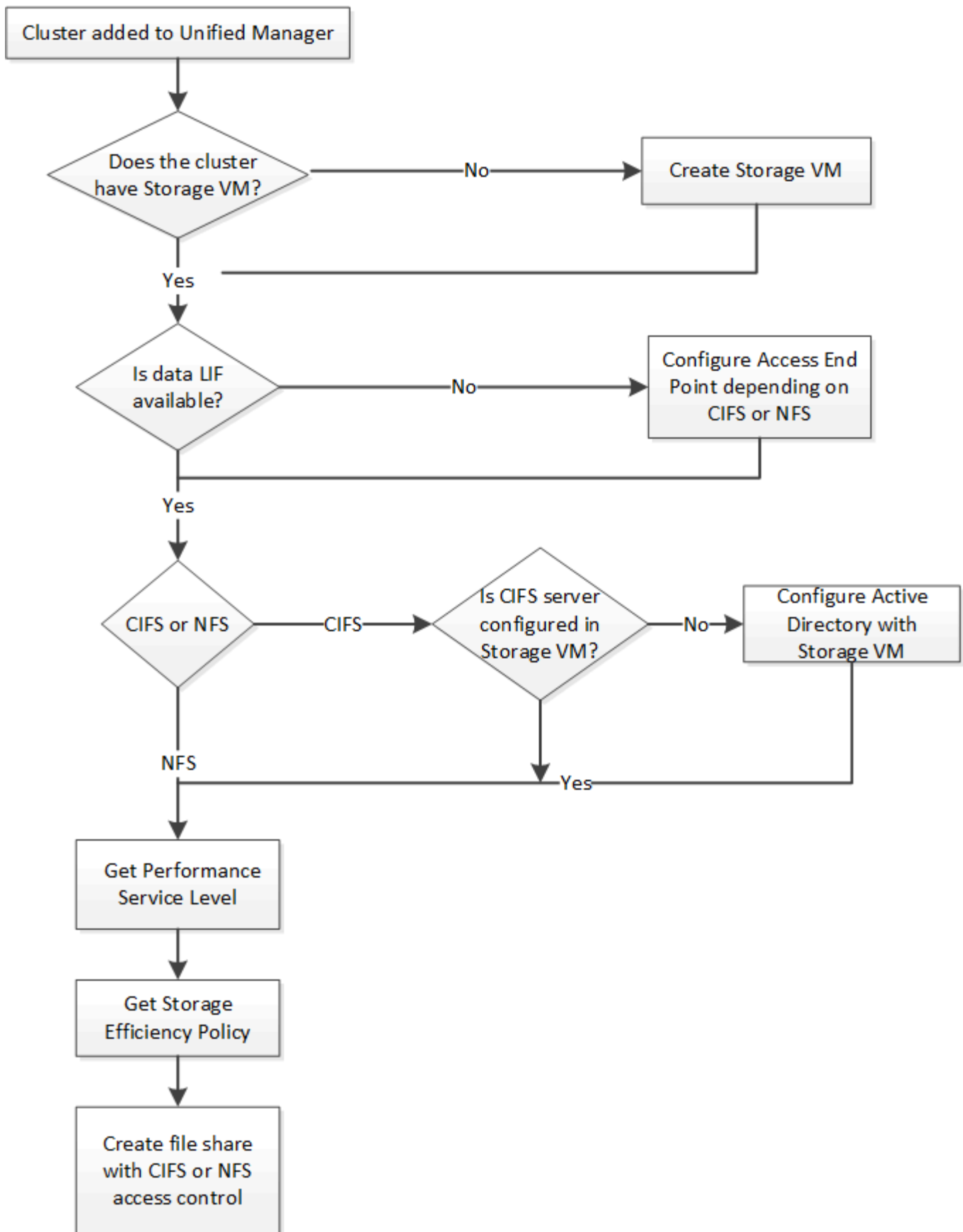
범주	HTTP 동사	길
관리 서버	연다	/management-server/jobs/{key}

API를 사용하여 CIFS 및 NFS 파일 공유 제공

Active IQ Unified Manager 의 일부로 제공되는 프로비저닝 API를 사용하여 스토리지 가상 머신(SVM)에서 CIFS 공유 및 NFS 파일 공유를 프로비저닝할 수 있습니다. 이 프로비저닝

워크플로는 파일 공유를 생성하기 전에 SVM 키, 성능 서비스 수준 및 스토리지 효율성 정책을 검색하는 단계를 자세히 설명합니다.

다음 다이어그램은 파일 공유 프로비저닝 워크플로의 각 단계를 보여줍니다. 여기에는 CIFS 공유와 NFS 파일 공유를 모두 프로비저닝하는 것이 포함됩니다.



다음 사항을 확인하세요.



- ONTAP 클러스터가 Unified Manager에 추가되었고 클러스터 키가 획득되었습니다.
- 클러스터에 SVM이 생성되었습니다.
- SVM은 CIFS 및 NFS 서비스를 지원합니다. SVM이 필요한 서비스를 지원하지 않으면 파일 공유 프로비저닝이 실패할 수 있습니다.
- FCP 포트가 포트 프로비저닝을 위해 온라인 상태입니다.

1. CIFS 공유를 만들려는 SVM에서 데이터 LIF 또는 액세스 엔드포인트를 사용할 수 있는지 확인합니다. SVM에서 사용 가능한 액세스 엔드포인트 목록을 가져옵니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

샘플 cURL

```
curl -X GET "https://<hostname>/api/storage-provider/access-endpoints?resource.key=7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. 액세스 엔드포인트가 목록에 있는 경우 액세스 엔드포인트 키를 얻고, 그렇지 않은 경우 액세스 엔드포인트를 만듭니다.



CIFS 프로토콜이 활성화된 액세스 엔드포인트를 생성해야 합니다. CIFS 프로토콜이 활성화된 액세스 엔드포인트를 생성하지 않으면 CIFS 공유 프로비저닝이 실패합니다.

범주	HTTP 동사	길
스토리지 제공자	우편	/storage-provider/access-endpoints

샘플 cURL

생성하려는 액세스 엔드포인트의 세부 정보를 입력 매개변수로 입력해야 합니다.

```
curl -X POST "https://<hostname>/api/storage-provider/access-endpoints"
-H "accept: application/json" -H "Content-Type: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
{ \"data_protocols\": \"nfs\",
  \"fileshare\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=volume,uuid=f3063d27-2c71-44e5-9a69-a3927c19c8fc\" },
  \"gateway\": \"10.132.72.12\",
  \"ip\": { \"address\": \"10.162.83.26\",
  \"ha_address\": \"10.142.83.26\",
  \"netmask\": \"255.255.0.0\" },
  \"lun\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=lun,uuid=d208cc7d-80a3-4755-93d4-5db2c38f55a6\" },
  \"mtu\": 15000, \"name\": \"aep1\",
  \"svm\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a178d39e12:type=vserver,uuid=1d1c3198-fc57-11e8-99ca-00a098d38e12\" },
  \"vlan\": 10}
```

JSON 출력에는 사용자가 만든 액세스 엔드포인트를 확인하는 데 사용할 수 있는 Job 개체 키가 표시됩니다.

3. 액세스 엔드포인트를 확인하세요.

범주	HTTP 동사	길
관리 서버	얻다	/management-server/jobs/{key}

4. CIFS 공유 또는 NFS 파일 공유를 만들어야 하는지 확인합니다. CIFS 공유를 생성하려면 다음 하위 단계를 따르세요.

- SVM에 CIFS 서버가 구성되어 있는지 확인합니다. 즉, SVM에 Active Directory 매핑이 생성되었는지 확인합니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/active-directories-mappings

- Active Directory 매핑이 생성되면 키를 가져오고, 그렇지 않으면 SVM에서 Active Directory 매핑을 만듭니다.

범주	HTTP 동사	길
스토리지 제공자	우편	/storage-provider/active-directories-mappings

샘플 cURL

Active Directory 매핑을 만드는 데 필요한 세부 정보를 입력 매개변수로 입력해야 합니다.

```
curl -X POST "https://<hostname>/api/storage-provider/active-directories-mappings" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
{ \ "_links\": {},
  \ "dns\": \ "10.000.000.000\ ",
  \ "domain\": \ "example.com\ ",
  \ "password\": \ "string\ ",
  \ "svm\": { \ "key\": \ "9f4ddea-e395-11e9-b660-005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9\ " },
  \ "username\": \ "string\ " }
```

+

이는 동기식 호출이며 출력에서 Active Directory 매핑이 생성되었는지 확인할 수 있습니다. 오류가 발생한 경우 오류 메시지가 표시되어 문제를 해결하고 요청을 다시 실행할 수 있습니다.

- 클러스터에서 SVM 확인 워크플로 항목에 설명된 대로 CIFS 공유 또는 NFS 파일 공유를 만들려는 SVM에 대한 SVM 키를 가져옵니다.
- 다음 API를 실행하고 응답에서 키를 검색하여 성능 서비스 수준에 대한 키를 얻습니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/performance-service-levels



시스템 정의 성능 서비스 수준의 세부 정보를 검색하려면 다음을 설정하세요. `system_defined` 입력 매개변수 `true`. 출력에서 파일 공유에 적용하려는 성능 서비스 수준의 키를 얻습니다.

- 선택적으로, 다음 API를 실행하고 응답에서 키를 검색하여 파일 공유에 적용하려는 스토리지 효율성 정책에 대한 스토리지 효율성 정책 키를 얻습니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/storage-efficiency-policies

- 파일 공유를 만듭니다. 액세스 제어 목록과 내보내기 정책을 지정하여 CIFS와 NFS를 모두 지원하는 파일 공유를 만들 수 있습니다. 다음 하위 단계에서는 볼륨에서 하나의 프로토콜만 지원하는 파일 공유를 만들려는 경우에 대한 정보를 제공합니다. NFS 공유를 만든 후 액세스 제어 목록을 포함하도록 NFS 파일 공유를 업데이트할 수도 있습니다. 자세한 내용은 저장소 워크로드 수정 항목을 참조하세요.
 - CIFS 공유만 생성하려면 액세스 제어 목록(ACL)에 대한 정보를 수집하세요. CIFS 공유를 생성하려면 다음

입력 매개변수에 유효한 값을 제공하세요. 할당된 각 사용자 그룹에 대해 CIFS/SMB 공유가 프로비저닝되면 ACL이 생성됩니다. ACL 및 Active Directory 매핑에 입력한 값을 기반으로 CIFS 공유가 생성될 때 해당 공유에 대한 액세스 제어 및 매핑이 결정됩니다.

샘플 값이 포함된 **cURL** 명령

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
  },
}
```

- b. NFS 파일 공유만 생성하려면 내보내기 정책에 대한 정보를 수집하세요. NFS 파일 공유를 생성하려면 다음 입력 매개변수에 유효한 값을 제공하세요. 사용자의 값에 따라, 내보내기 정책은 NFS 파일 공유가 생성될 때 첨부됩니다.



NFS 공유를 프로비저닝하는 동안 필요한 모든 값을 제공하여 내보내기 정책을 만들거나 내보내기 정책 키를 제공하고 기존 내보내기 정책을 재사용할 수 있습니다. 스토리지 VM에 대한 내보내기 정책을 재사용하려면 내보내기 정책 키를 추가해야 합니다. 키를 알지 못하면 다음을 사용하여 내보내기 정책 키를 검색할 수 있습니다.

/datacenter/protocols/nfs/export-policies API. 새로운 정책을 만들려면 다음 샘플에 표시된 대로 규칙을 입력해야 합니다. 입력된 규칙에 대해 API는 호스트, 스토리지 VM 및 규칙을 일치시켜 기존 내보내기 정책을 검색하려고 시도합니다. 기존 수출 정책이 있는 경우 해당 정책이 사용됩니다. 그렇지 않으면 새로운 수출 정책이 생성됩니다.

샘플 값이 포함된 **cURL** 명령

```
"export_policy": {
  "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=export_policy,uuid=1460288880641",
  "name_tag": "ExportPolicyNameTag",
  "rules": [
    {
      "clients": [
        {
          "match": "0.0.0.0/0"
        }
      ]
    }
  ]
}
```

액세스 제어 목록과 내보내기 정책을 구성한 후 CIFS와 NFS 파일 공유에 대한 필수 입력 매개변수에 유효한 값을 제공합니다.



저장소 효율성 정책은 파일 공유를 생성하기 위한 선택적 매개변수입니다.

범주	HTTP 동사	길
스토리지 제공자	우편	/storage-provider/file-shares

JSON 출력에는 생성한 파일 공유를 확인하는 데 사용할 수 있는 Job 개체 키가 표시됩니다. . 작업 쿼리에서 반환된 Job 개체 키를 사용하여 파일 공유 생성을 확인합니다.

범주	HTTP 동사	길
관리 서버	얻다	/management-server/jobs/{key}

응답이 끝나면 파일 공유 키가 생성된 것을 볼 수 있습니다.

```

],
"job_results": [
  {
    "name": "fileshareKey",
    "value": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6"
  }
],
"_links": {
  "self": {
    "href": "/api/management-server/jobs/06a6148bf9e862df:-2611856e:16e8d47e722:-7f87"
  }
}
}

```

1. 반환된 키로 다음 API를 실행하여 파일 공유가 생성되었는지 확인하세요.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/file-shares/{key}

샘플 JSON 출력

POST 메소드를 볼 수 있습니다. /storage-provider/file-shares 각 함수에 필요한 모든 API를 내부적으로 호출하고 객체를 생성합니다. 예를 들어, 다음을 호출합니다. /storage-provider/performance-service-levels/ 파일 공유에 대한 성능 서비스 수준을 할당하기 위한 API입니다.

```

{
  "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6",
  "name": "FileShare_377",
  "cluster": {
    "uuid": "7d5a59b3-953a-11e8-8857-00a098dcc959",
    "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959",
    "name": "AFFA300-206-68-70-72-74",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/clusters/7d5a59b3-953a-11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959"
      }
    }
  },
  "svm": {
    "uuid": "b106d7b1-51e9-11e9-8857-00a098dcc959",
    "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959",
    "name": "RRT_ritu_vs1",
    "_links": {
      "self": {
        "href": "/api/datacenter/svm/svms/7d5a59b3-953a-11e8-8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959"
      }
    }
  },
  "assigned_performance_service_level": {
    "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
    "name": "Value",
    "peak_iops": 75,
    "expected_iops": 75,
    "_links": {
      "self": {
        "href": "/api/storage-provider/performance-service-levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
      }
    }
  },
  "recommended_performance_service_level": {
    "key": null,
    "name": "Idle",

```



```

        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
    },
    "space": {
        "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
        "key": null,
        "name": "Unassigned",
        "_links": {}
    },
    "access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 1,
                    "protocols": [
                        "nfs3",
                        "nfs4"
                    ],
                    "ro_rule": [
                        "sys"
                    ],
                    "rw_rule": [
                        "sys"
                    ],
                    "superuser": [
                        "none"
                    ]
                }
            ]
        }
    }
}

```

```

    },
    {
      "anonymous_user": "65534",
      "clients": [
        {
          "match": "0.0.0.0/0"
        }
      ],
      "index": 2,
      "protocols": [
        "cifs"
      ],
      "ro_rule": [
        "ntlm"
      ],
      "rw_rule": [
        "ntlm"
      ],
      "superuser": [
        "none"
      ]
    }
  ],
  "_links": {
    "self": {
      "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
    }
  }
},
"_links": {
  "self": {
    "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
  }
}
}
}

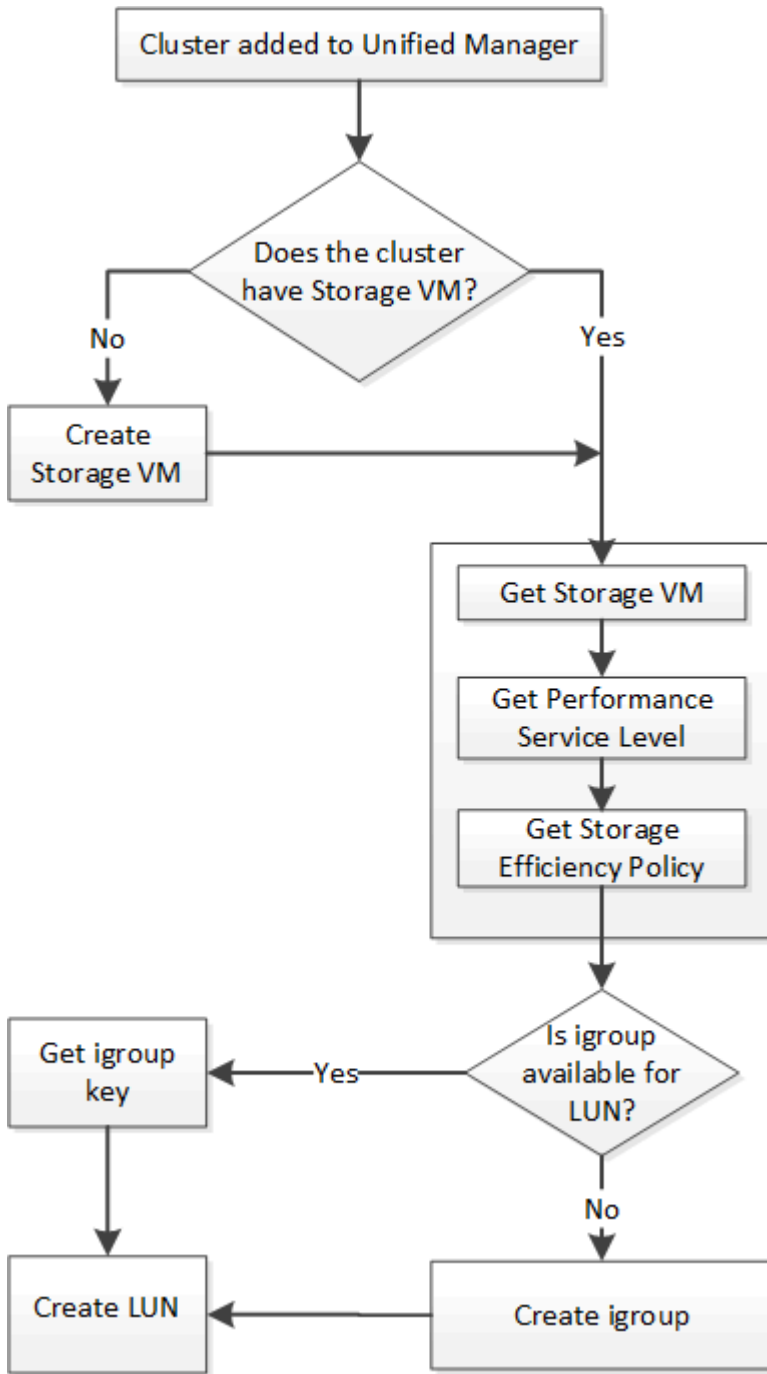
```

API를 사용하여 LUN 프로비저닝

Active IQ Unified Manager 의 일부로 제공되는 프로비저닝 API를 사용하여 스토리지 가상 머신(SVM)에 LUN을 프로비저닝할 수 있습니다. 이 프로비저닝 워크플로는 LUN을 생성하기

전에 SVM 키, 성능 서비스 수준 및 스토리지 효율성 정책을 검색하는 단계를 자세히 설명합니다.

다음 다이어그램은 LUN 프로비저닝 워크플로의 단계를 보여줍니다.



이 워크플로는 ONTAP 클러스터가 Unified Manager에 추가되었고 클러스터 키가 획득되었다고 가정합니다. 또한 워크플로는 SVM이 클러스터에 이미 생성되었다고 가정합니다.

1. 클러스터에서 SVM 확인 워크플로 항목에 설명된 대로 LUN을 생성하려는 SVM에 대한 SVM 키를 가져옵니다.
2. 다음 API를 실행하고 응답에서 키를 검색하여 성능 서비스 수준에 대한 키를 얻습니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/performance-service-levels



시스템 정의 성능 서비스 수준의 세부 정보를 검색하려면 다음을 설정하세요. `system_defined` 입력 매개변수 `true`. 출력에서 LUN에 적용하려는 성능 서비스 수준의 키를 얻습니다.

- 선택적으로 다음 API를 실행하고 응답에서 키를 검색하여 LUN에 적용하려는 스토리지 효율성 정책에 대한 스토리지 효율성 정책 키를 얻습니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/storage-efficiency-policies

- 생성하려는 LUN 대상에 대한 액세스 권한을 부여하기 위해 개시자 그룹(igroup)이 생성되었는지 확인합니다.

범주	HTTP 동사	길
데이터센터	얻다	/datacenter/protocols/san/igroups /datacenter/protocols/san/igroups/{key}

igroup이 액세스 권한을 부여한 SVM을 나타내는 매개변수 값을 입력해야 합니다. 또한 특정 igroup을 쿼리하려면 igroup 이름(키)을 입력 매개변수로 입력합니다.

- 출력에서 액세스 권한을 부여하려는 igroup을 찾으면 키를 얻습니다. 그렇지 않으면 igroup을 생성합니다.

범주	HTTP 동사	길
데이터센터	우편	/datacenter/protocols/san/igroups

생성하려는 igroup의 세부 정보를 입력 매개변수로 입력해야 합니다. 이는 동기 호출이며 출력에서 igroup 생성을 확인할 수 있습니다. 오류가 발생하면 문제를 해결하고 API를 다시 실행할 수 있는 메시지가 표시됩니다.

- LUN을 생성합니다.

범주	HTTP 동사	길
스토리지 제공자	우편	/storage-provider/luns

LUN을 생성하려면 검색된 값을 필수 입력 매개변수로 추가했는지 확인하세요.



스토리지 효율성 정책은 LUN을 생성하기 위한 선택적 매개변수입니다.

샘플 cURL

생성하려는 LUN의 모든 세부 정보를 입력 매개변수로 입력해야 합니다.

JSON 출력에는 생성한 LUN을 확인하는 데 사용할 수 있는 작업 개체 키가 표시됩니다.

7. 작업 쿼리에서 반환된 작업 개체 키를 사용하여 LUN 생성을 확인합니다.

범주	HTTP 동사	길
관리 서버	얻다	/management-server/jobs/{key}

응답이 끝나면 생성된 LUN의 키가 표시됩니다.

8. 반환된 키로 다음 API를 실행하여 LUN 생성을 확인하세요.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/luns/{key}

샘플 JSON 출력

POST 메소드를 볼 수 있습니다. /storage-provider/luns 각 함수에 필요한 모든 API를 내부적으로 호출하고 객체를 생성합니다. 예를 들어, 다음을 호출합니다. /storage-provider/performance-service-levels/ LUN에 성능 서비스 수준을 할당하기 위한 API입니다.

== LUN 생성 또는 매핑 실패에 대한 문제 해결 단계

이 워크플로를 완료한 후에도 LUN 생성에 오류가 발생할 수 있습니다. LUN이 성공적으로 생성되더라도 LUN을 생성한 노드에서 SAN LIF 또는 액세스 엔드포인트를 사용할 수 없어 igroup과의 LUN 매핑이 실패할 수 있습니다. 실패가 발생한 경우 다음과 같은 메시지가 표시됩니다.

```
The nodes <node_name> and <partner_node_name> have no LIFs configured with the iSCSI or FCP protocol for Vserver <server_name>. Use the access-endpoints API to create a LIF for the LUN.
```

이 문제를 해결하려면 다음 문제 해결 단계를 따르세요.

1. LUN을 생성하려고 시도한 SVM에서 iSCSI/FCP 프로토콜을 지원하는 액세스 엔드포인트를 생성합니다.

범주	HTTP 동사	길
스토리지 제공자	우편	/storage-provider/access-endpoints

샘플 cURL

생성하려는 액세스 엔드포인트의 세부 정보를 입력 매개변수로 입력해야 합니다.



입력 매개변수에 LUN의 홈 노드를 나타내는 주소와 홈 노드의 파트너 노드를 나타내는 ha_address를 추가했는지 확인하세요. 이 작업을 실행하면 홈 노드와 파트너 노드 모두에 액세스 엔드포인트가 생성됩니다.

2. JSON 출력에서 반환된 Job 개체 키로 작업을 쿼리하여 SVM에 액세스 엔드포인트를 추가하는 작업이 성공적으로 실행되었는지 확인하고 SVM에서 iSCSI/FCP 서비스가 활성화되었는지 확인합니다.

범주	HTTP 동사	길
관리 서버	얻다	/management-server/jobs/{key}

샘플 JSON 출력

출력의 끝에서 생성된 액세스 엔드포인트의 키를 볼 수 있습니다. 다음 출력에서 "name": "accessEndpointKey" 값은 키가 9c964258-14ef-11ea-95e2-00a098e32c28인 LUN의 홈 노드에 생성된 액세스 엔드포인트를 나타냅니다. "name": "accessEndpointHAKey" 값은 홈 노드의 파트너 노드에 생성된 액세스 엔드포인트를 나타내며, 키는 9d347006-14ef-11ea-8760-00a098e3215f입니다.

3. LUN을 수정하여 igroup 매핑을 업데이트합니다. 워크플로 수정에 대한 자세한 내용은 "스토리지 워크로드 수정"을 참조하세요.

범주	HTTP 동사	길
스토리지 제공자	반점	/storage-provider/lun/{key}

입력에서 LUN 매핑을 업데이트하려는 igroup 키와 LUN 키를 지정합니다.

샘플 cURL

JSON 출력에는 매핑이 성공했는지 확인하는 데 사용할 수 있는 Job 개체 키가 표시됩니다.

4. LUN 키로 쿼리하여 LUN 매핑을 확인합니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/luns/{key}

샘플 JSON 출력

출력에서 LUN이 처음 프로비저닝된 igroup(키 d19ec2fa-fec7-11e8-b23d-00a098e32c28)에 성공적으로 매핑되었음을 확인할 수 있습니다.

API를 사용하여 스토리지 워크로드 수정

스토리지 작업 부하를 수정하려면 매개변수가 누락된 LUN이나 파일 공유를 업데이트하거나 기존 매개변수를 변경해야 합니다.

이 워크플로는 LUN 및 파일 공유에 대한 성능 서비스 수준을 업데이트하는 예를 들어보겠습니다.



워크플로는 LUN 또는 파일 공유에 성능 서비스 수준이 프로비저닝되었다고 가정합니다.

파일 공유 수정

파일 공유를 수정하는 동안 다음 매개변수를 업데이트할 수 있습니다.

- 용량 또는 크기.
- 온라인 또는 오프라인 설정.
- 보관 효율성 정책.
- 성능 서비스 수준.
- 액세스 제어 목록(ACL) 설정.
- 정책 설정을 내보냅니다. 파일 공유에서 내보내기 정책 매개변수를 삭제하고 기본(빈) 내보내기 정책 규칙을 되돌릴 수도 있습니다.



단일 API 실행 중에는 매개변수를 하나만 업데이트할 수 있습니다.

이 절차에서는 파일 공유에 성능 서비스 수준을 추가하는 방법을 설명합니다. 다른 파일 공유 속성을 업데이트하는 데도 동일한 절차를 사용할 수 있습니다.

1. 업데이트하려는 파일 공유의 CIFS 공유 또는 NFS 파일 공유 키를 가져옵니다. 이 API는 데이터 센터의 모든 파일 공유를 쿼리합니다. 이미 파일 공유 키를 알고 있다면 이 단계를 건너뛰세요.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/file-shares

2. 획득한 파일 공유 키로 다음 API를 실행하여 파일 공유의 세부 정보를 확인하세요.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/file-shares/{key}

출력에서 파일 공유의 세부 정보를 확인합니다.

```
"assigned_performance_service_level": {
  "key": null,
  "name": "Unassigned",
  "peak_iops": null,
  "expected_iops": null,
  "_links": {}
},
```

3. 이 파일 공유에 할당하려는 성능 서비스 수준에 대한 키를 가져옵니다. 현재로서는 정책이 할당되지 않았습니다.

범주	HTTP 동사	길
성능 서비스 수준	얻다	/storage-provider/performance-service-levels



시스템 정의 성능 서비스 수준의 세부 정보를 검색하려면 다음을 설정하세요. `system_defined` 입력 매개변수 `true`. 출력에서 파일 공유에 적용하려는 성능 서비스 수준의 키를 얻습니다.

4. 파일 공유에 성능 서비스 수준을 적용합니다.

범주	HTTP 동사	길
스토리지 제공업체	반점	/storage-provider/file-shares/{key}

입력 시에는 업데이트하려는 매개변수와 파일 공유 키만 지정해야 합니다. 이 경우에는 성과 서비스 수준의 핵심이 됩니다.

샘플 **cURL**

```
curl -X POST "https://<hostname>/api/storage-provider/file-shares" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
"{
  \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-
fa163e82bbf2\" },
}"
```

JSON 출력에는 홈 및 파트너 노드의 액세스 엔드포인트가 성공적으로 생성되었는지 확인하는 데 사용할 수 있는 Job 개체가 표시됩니다.

5. 출력에 표시된 작업 개체 키를 사용하여 성능 서비스 수준이 파일 공유에 추가되었는지 확인합니다.

범주	HTTP 동사	길
관리 서버	얻다	/management-server/jobs/{key}

Job 객체의 ID로 쿼리하면 파일 공유가 성공적으로 업데이트되었는지 확인할 수 있습니다. 오류가 발생한 경우 오류를 해결하고 API를 다시 실행하세요. 성공적으로 생성되면 파일 공유를 쿼리하여 수정된 객체를 확인합니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/file-shares/{key}

출력에서 파일 공유의 세부 정보를 확인합니다.

```
"assigned_performance_service_level": {
  "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
  "name": "Value",
  "peak_iops": 75,
  "expected_iops": 75,
  "_links": {
    "self": {
      "href": "/api/storage-provider/performance-service-levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
    }
  }
}
```

LUN 업데이트

LUN을 업데이트하는 동안 다음 매개변수를 수정할 수 있습니다.

- 용량 또는 크기
- 온라인 또는 오프라인 설정
- 저장 효율성 정책
- 성능 서비스 수준
- LUN 맵



단일 API 실행 중에는 매개변수를 하나만 업데이트할 수 있습니다.

이 절차에서는 LUN에 성능 서비스 수준을 추가하는 방법을 설명합니다. 다른 LUN 속성을 업데이트하는 데도 동일한 절차를 사용할 수 있습니다.

1. 업데이트하려는 LUN의 LUN 키를 가져옵니다. 이 API는 데이터 센터의 모든 LUN에 대한 세부 정보를 반환합니다. 이미 LUN 키를 알고 있다면 이 단계를 건너뛰세요.

범주	HTTP 동사	길
스토리지 제공업체	얻다	/storage-provider/luns

2. 획득한 LUN 키로 다음 API를 실행하여 LUN의 세부 정보를 확인하세요.

범주	HTTP 동사	길
스토리지 제공업체	얻다	/storage-provider/luns/{key}

출력에서 LUN의 세부 정보를 확인합니다. 이 LUN에 성능 서비스 수준이 할당되지 않았음을 확인할 수 있습니다.

샘플 **JSON** 출력

```
"assigned_performance_service_level": {
  "key": null,
  "name": "Unassigned",
  "peak_iops": null,
  "expected_iops": null,
  "_links": {}
},
```

3. LUN에 할당하려는 성능 서비스 수준에 대한 키를 얻습니다.

범주	HTTP 동사	길
성능 서비스 수준	얻다	/storage-provider/performance-service-levels



시스템 정의 성능 서비스 수준의 세부 정보를 검색하려면 다음을 설정하세요. `system_defined` 입력 매개변수 `true`. 출력에서 LUN에 적용하려는 성능 서비스 수준의 키를 얻습니다.

4. LUN에 성능 서비스 수준을 적용합니다.

범주	HTTP 동사	길
스토리지 제공업체	반점	/storage-provider/lun/{key}

입력 시에는 LUN 키와 함께 업데이트하려는 매개변수만 지정해야 합니다. 이 경우에는 성과 서비스 수준의 핵심입니다.

샘플 **cURL**

```
curl -X PATCH "https://<hostname>/api/storage-provider/luns/7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>" -d "{ \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-fa163e82bbf2\" } }"
```

JSON 출력에는 업데이트한 LUN을 확인하는 데 사용할 수 있는 작업 개체 키가 표시됩니다.

5. 획득한 LUN 키로 다음 API를 실행하여 LUN의 세부 정보를 확인하세요.

범주	HTTP 동사	길
스토리지 제공업체	얻다	/storage-provider/luns/{key}

출력에서 LUN의 세부 정보를 확인합니다. 이 LUN에 성능 서비스 수준이 할당된 것을 볼 수 있습니다.

샘플 **JSON** 출력

```
{
  "assigned_performance_service_level": {
    "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
    "name": "Value",
    "peak_iops": 75,
    "expected_iops": 75,
    "_links": {
      "self": {
        "href": "/api/storage-provider/performance-service-levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
      }
    }
  }
}
```

CIFS를 지원하기 위해 **API**를 사용하여 **NFS** 파일 공유 수정

CIFS 프로토콜을 지원하도록 NFS 파일 공유를 수정할 수 있습니다. 파일 공유를 생성하는 동안 동일한 파일 공유에 대한 액세스 제어 목록(ACL) 매개변수와 내보내기 정책 규칙을 모두 지정할 수 있습니다. 하지만 NFS 파일 공유를 생성한 동일한 볼륨에서 CIFS를 활성화하려는 경우 해당 파일 공유의 ACL 매개변수를 업데이트하여 CIFS를 지원할 수 있습니다.

시작하기 전에

1. NFS 파일 공유는 내보내기 정책 세부 정보만으로 생성되어야 합니다. 자세한 내용은 파일 공유 관리 및 _스토리지 작업 부하 수정_을 참조하세요.
2. 이 작업을 실행하려면 파일 공유 키가 필요합니다. 작업 ID를 사용하여 파일 공유 세부 정보를 보고 파일 공유 키를 검색하는 방법에 대한 자세한 내용은 _CIFS 및 NFS 파일 공유 프로비저닝_을 참조하세요.

이는 ACL 매개변수가 아닌 내보내기 정책 규칙만 추가하여 만든 NFS 파일 공유에 적용됩니다. ACL 매개변수를 포함하도록 NFS 파일 공유를 수정합니다.

단계

1. NFS 파일 공유에서 다음을 수행합니다. PATCH CIFS 액세스를 허용하기 위한 ACL 세부 정보를 사용한 작업입니다.

범주	HTTP 동사	길
스토리지 제공자	반점	/storage-provider/file-shares

샘플 cURL

다음 샘플에서 표시된 것처럼 사용자 그룹에 할당한 액세스 권한에 따라 ACL이 생성되어 파일 공유에 할당됩니다.

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
  }
}
```

샘플 JSON 출력

이 작업은 업데이트를 실행하는 작업의 작업 ID를 반환합니다.

2. 동일한 파일 공유에 대한 파일 공유 세부 정보를 쿼리하여 매개변수가 올바르게 추가되었는지 확인합니다.

범주	HTTP 동사	길
스토리지 제공자	얻다	/storage-provider/file-shares/{key}

샘플 JSON 출력

```
"access_control": {
  "acl": [
    {
      "user_or_group": "everyone",
      "permission": "read"
    }
  ]
}
```

```

    }
  ],
  "export_policy": {
    "id": 1460288880641,
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
    "name": "default",
    "rules": [
      {
        "anonymous_user": "65534",
        "clients": [
          {
            "match": "0.0.0.0/0"
          }
        ],
        "index": 1,
        "protocols": [
          "nfs3",
          "nfs4"
        ],
        "ro_rule": [
          "sys"
        ],
        "rw_rule": [
          "sys"
        ],
        "superuser": [
          "none"
        ]
      },
      {
        "anonymous_user": "65534",
        "clients": [
          {
            "match": "0.0.0.0/0"
          }
        ],
        "index": 2,
        "protocols": [
          "cifs"
        ],
        "ro_rule": [
          "ntlm"
        ],
        "rw_rule": [
          "ntlm"
        ]
      }
    ]
  }
}

```

```

        ],
        "superuser": [
            "none"
        ]
    },
    ],
    "_links": {
        "self": {
            "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
        }
    }
},
"_links": {
    "self": {
        "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
    }
}
}

```

동일한 파일 공유에 내보내기 정책과 함께 할당된 ACL을 볼 수 있습니다.

법적 고지 사항

법적 고지사항은 저작권 표시, 상표, 특허 등에 대한 정보를 제공합니다.

저작권

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

상표

NETAPP, NETAPP 로고 및 NetApp 상표 페이지에 나열된 마크는 NetApp, Inc.의 상표입니다. 다른 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

특허

NetApp 이 소유한 현재 특허 목록은 다음에서 확인할 수 있습니다.

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

개인정보 보호정책

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

오픈소스

이 제품에 사용된 제3자 저작권 및 라이선스에 대한 정보입니다.

["Active IQ Unified Manager 9.16에 대한 알림"](#)

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 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 라이선스와 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 라이선스도 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 라이선스를 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 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.