



SnapCenter software 설명서

SnapCenter software

NetApp
November 06, 2025

This PDF was generated from <https://docs.netapp.com/ko-kr/snapcenter-61/index.html> on November 06, 2025. Always check docs.netapp.com for the latest.

목차

SnapCenter software 설명서	1
릴리스 노트	2
릴리스 노트	2
SnapCenter 에 지원되는 업그레이드 경로	2
시작하기	3
SnapCenter software 에 대해 알아보세요	3
SnapCenter 개요	3
SnapCenter 의 보안 기능	7
SnapCenter 의 역할 기반 액세스 제어	8
SnapCenter 의 재해 복구	13
SnapCenter 에 필요한 라이선스	14
SnapCenter 의 SnapMirror 활성 동기화	16
데이터 보호의 핵심 개념	17
SnapCenter 에서 지원하는 스토리지 시스템 및 애플리케이션	19
SnapCenter 자격 증명에 대한 인증 방법	19
ASA r2 시스템에 지원되는 SnapCenter 작업	20
SnapCenter software 빠른 시작	21
SnapCenter 서버 설치 및 구성	23
SnapCenter 서버 설치를 준비하세요	23
SnapCenter 서버 설치 요구 사항	23
SnapCenter software 액세스하려면 등록하세요	29
다중 요소 인증(MFA)	29
SnapCenter 서버 설치	39
Windows 호스트에 SnapCenter 서버 설치	39
Linux 호스트에 SnapCenter 서버 설치	43
SnapCenter 등록	47
RBAC 인증을 사용하여 SnapCenter 에 로그인합니다.	47
SnapCenter 서버 구성	51
스토리지 시스템 추가 및 프로비저닝	51
SnapCenter Standard 컨트롤러 기반 라이선스 추가	71
고가용성 구성	76
역할 기반 액세스 제어(RBAC) 구성	80
감사 로그 설정 구성	108
SnapCenter Server를 사용하여 보안된 MySQL 연결 구성	110
인증서 기반 인증 구성	115
인증서 기반 인증 활성화	115
SnapCenter 서버에서 인증 기관(CA) 인증서 내보내기	116
Windows 플러그인 호스트에 CA 인증서 가져오기	116
UNIX 플러그인 호스트로 CA 인증서 가져오기	117

SnapCenter 인증서 내보내기	118
Windows 호스트에 대한 CA 인증서 구성	119
CA 인증서 CSR 파일 생성	119
CA 인증서 가져오기	120
CA 인증서 지문을 받으세요	120
Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성	121
SnapCenter 사이트에 CA 인증서 구성	122
SnapCenter 에 CA 인증서 활성화	122
Linux 호스트에 대한 CA 인증서 구성	123
nginx 인증서 구성	123
감사 로그 인증서 구성	123
SnapCenter 서비스 인증서 구성	124
Windows 호스트에서 양방향 SSL 통신을 구성하고 활성화합니다.	124
Windows 호스트에서 양방향 SSL 통신 구성	124
Windows 호스트에서 양방향 SSL 통신 활성화	127
Linux 호스트에서 양방향 SSL 통신을 구성하고 활성화합니다.	128
Linux 호스트에서 양방향 SSL 통신 구성	128
Linux 호스트에서 SSL 통신 활성화	129
Active Directory, LDAP 및 LDAPS 구성	130
신뢰할 수 없는 Active Directory 도메인 등록	130
Active Directory 읽기 권한을 활성화하기 위해 IIS 애플리케이션 풀 구성	131
LDAPS에 대한 CA 클라이언트 인증서 구성	132
Microsoft SQL Server 데이터베이스 보호	133
Microsoft SQL Server용 SnapCenter 플러그인	133
Microsoft SQL Server용 SnapCenter 플러그인 개요	133
Microsoft SQL Server용 SnapCenter 플러그인으로 할 수 있는 작업	133
Microsoft SQL Server용 SnapCenter 플러그인 기능	134
Windows 클러스터에서 비대칭 LUN 매핑 지원	135
Microsoft SQL Server용 SnapCenter 플러그인에서 지원하는 스토리지 유형	136
Microsoft SQL Server용 SnapCenter 플러그인에 대한 스토리지 레이아웃 권장 사항	138
SQL 플러그인에 필요한 최소 ONTAP 권한	140
SQL 서버용 플러그인을 위한 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비	143
SQL Server 리소스에 대한 백업 전략	143
SQL Server에 대한 복원 전략	147
SQL Server에 대한 복제 전략 정의	150
Microsoft SQL Server용 SnapCenter 플러그인 설치를 준비하세요	150
Microsoft SQL Server용 SnapCenter 플러그인 설치 워크플로	150
Microsoft SQL Server용 호스트 추가 및 SnapCenter 플러그인 설치를 위한 필수 구성 요소	151
Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	152
Windows용 SnapCenter 플러그인 패키지에 대한 자격 증명 설정	152
개별 SQL Server 리소스에 대한 자격 증명 구성	154

Windows Server 2016 이상에서 gMSA 구성	156
Microsoft SQL Server용 SnapCenter 플러그인 설치	157
CA 인증서 구성	163
재해 복구 구성	166
SnapCenter Plug-in for VMware vSphere 설치	168
CA 인증서 배포	168
CRL 파일 구성	169
데이터 보호를 준비하세요	169
Microsoft SQL Server용 SnapCenter 플러그인을 사용하기 위한 전제 조건	169
SQL Server를 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식	170
SQL Server 데이터베이스, 인스턴스 또는 가용성 그룹 백업	170
백업 워크플로	170
백업에 사용할 수 있는 리소스가 있는지 확인하세요	172
NetApp 스토리지 시스템으로 리소스 마이그레이션	173
SQL Server 데이터베이스에 대한 백업 정책 만들기	175
SQL Server에 대한 리소스 그룹 생성 및 정책 연결	181
ASA r2 시스템에서 Microsoft SQL Server 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다. ..	184
SQL 리소스 백업 요구 사항	186
PowerShell cmdlet을 사용하여 스토리지 시스템 연결 및 자격 증명 만들기	187
SQL 리소스 백업	188
SQL Server 리소스 그룹 백업	193
SnapCenter 작업 페이지에서 SQL 리소스 백업 작업을 모니터링합니다.	193
Microsoft SQL Server 백업 작업을 위한 SnapCenter 플러그인 취소	194
토폴로지 페이지에서 SQL Server 백업 및 복제본 보기	195
PowerShell cmdlet을 사용하여 보조 백업 수 정리	197
SQL Server 리소스 복원	198
워크플로 복원	198
데이터베이스 복원을 위한 요구 사항	198
SQL Server 데이터베이스 백업 복원	199
보조 저장소에서 SQL Server 데이터베이스 복원	206
PowerShell cmdlet을 사용하여 리소스 복원	207
가용성 그룹 데이터베이스 다시 시드	209
SQL 리소스 복원 작업 모니터링	210
SQL 리소스 복원 작업 취소	211
SQL Server 데이터베이스 리소스 복제	211
복제 워크플로	211
SQL Server 데이터베이스 백업에서 복제	212
복제 수명 주기 수행	219
SQL 데이터베이스 복제 작업 모니터링	222
SQL 리소스 복제 작업 취소	222
클론 분할	223

SAP HANA 데이터베이스 보호	225
SAP HANA 데이터베이스용 SnapCenter 플러그인	225
SAP HANA 데이터베이스용 SnapCenter 플러그인 개요	225
SAP HANA 데이터베이스용 SnapCenter 플러그인을 사용하여 수행할 수 있는 작업	225
SAP HANA 데이터베이스용 SnapCenter 플러그인 기능	225
SAP HANA 데이터베이스용 SnapCenter 플러그인에서 지원하는 스토리지 유형	226
SAP HANA 플러그인에 필요한 최소 ONTAP 권한	227
SAP HANA 데이터베이스를 위한 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비	230
SAP HANA 데이터베이스를 위한 백업 전략	230
SAP HANA 데이터베이스의 복원 및 복구 전략	233
SAP HANA 데이터베이스용 SnapCenter 플러그인 설치 준비	235
SAP HANA 데이터베이스용 SnapCenter 플러그인 설치 워크플로	236
SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치하고 호스트를 추가하기 위한 전제 조건	236
Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	239
Linux용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	240
SAP HANA 데이터베이스용 SnapCenter 플러그인에 대한 자격 증명 설정	241
Windows Server 2016 이상에서 gMSA 구성	243
SAP HANA 데이터베이스용 SnapCenter 플러그인 설치	245
CA 인증서 구성	251
SnapCenter Plug-in for VMware vSphere 설치	258
CA 인증서 배포	258
CRL 파일 구성	258
데이터 보호를 준비하세요	258
SAP HANA 데이터베이스용 SnapCenter 플러그인을 사용하기 위한 전제 조건	258
SAP HANA 데이터베이스를 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식	259
SAP HANA 리소스 백업	260
SAP HANA 리소스 백업	260
SAP HANA 데이터베이스에 대한 HDB 사용자 저장소 키 및 HDBSQL OS 사용자 구성	261
리소스를 검색하고 데이터 보호를 위한 멀티테넌트 데이터베이스 컨테이너를 준비합니다.	261
플러그인 호스트에 수동으로 리소스 추가	263
SAP HANA 데이터베이스에 대한 백업 정책 만들기	265
리소스 그룹을 만들고 정책을 첨부합니다.	269
ASA r2 시스템에서 SAP HANA 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.	273
PowerShell cmdlet을 사용하여 SAP HANA 데이터베이스용 스토리지 시스템 연결 및 자격 증명 만들기	275
SAP HANA 데이터베이스 백업	277
리소스 그룹 백업	283
SAP HANA 데이터베이스 백업 작업 모니터링	284
SAP HANA에 대한 백업 작업 취소	285
토폴로지 페이지에서 SAP HANA 데이터베이스 백업 및 복제본 보기	286
SAP HANA 데이터베이스 복원	288
워크플로 복원	288

수동으로 추가된 리소스 백업을 복원하고 복구합니다.	288
자동 검색된 데이터베이스 백업을 복원하고 복구합니다.	293
PowerShell cmdlet을 사용하여 리소스 복원	297
SAP HANA 데이터베이스 복원 작업 모니터링	299
SAP HANA 리소스 백업 복제	300
복제 워크플로	300
SAP HANA 데이터베이스 백업 복제	301
SAP HANA 데이터베이스 복제 작업 모니터링	304
클론 분할	305
SnapCenter 업그레이드 후 SAP HANA 데이터베이스 복제본 삭제 또는 분할	306
Oracle 데이터베이스 보호	308
Oracle Database용 SnapCenter 플러그인 개요	308
Oracle Database용 플러그인으로 무엇을 할 수 있나요?	308
Oracle Database용 플러그인의 특징	308
Oracle Database용 플러그인이 지원하는 저장 유형	310
Oracle용 플러그인을 위한 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비	312
Oracle용 플러그인에 필요한 최소 ONTAP 권한	312
Oracle Database용 SnapCenter 플러그인 설치	315
Oracle Database용 SnapCenter 플러그인 설치 워크플로	315
Linux 또는 AIX용 호스트 추가 및 플러그인 패키지 설치를 위한 전제 조건	315
GUI를 사용하여 Linux 또는 AIX용 호스트를 추가하고 플러그인 패키지를 설치합니다.	324
Linux 또는 AIX용 플러그인 패키지를 설치하는 대체 방법	327
SnapCenter 플러그인 Loader 서비스 구성	331
Linux 호스트에서 SnapCenter 플러그인 Loader (SPL) 서비스를 사용하여 CA 인증서 구성	334
플러그인에 대한 CA 인증서 활성화	336
Oracle용 SnapManager 및 SAP용 SnapManager 에서 SnapCenter 로 데이터 가져오기	337
SnapCenter Plug-in for VMware vSphere 설치	342
CA 인증서 배포	342
CRL 파일 구성	342
Oracle 데이터베이스 보호를 준비하세요	343
Oracle 데이터베이스 백업	344
백업 절차 개요	344
백업 구성 정보	345
Oracle 데이터베이스 백업 요구 사항	357
백업에 사용 가능한 Oracle 데이터베이스를 찾아보세요	357
Oracle 데이터베이스에 대한 백업 정책 생성	359
Oracle 데이터베이스에 대한 리소스 그룹을 만들고 정책을 첨부합니다.	365
ASA r2 시스템에서 Oracle 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.	367
Oracle 리소스 백업	369
Oracle 데이터베이스 리소스 그룹 백업	372
Oracle 데이터베이스 백업 모니터링	373

기타 백업 작업	374
데이터베이스 백업 마운트 및 마운트 해제	378
데이터베이스 백업 마운트	378
데이터베이스 백업 마운트 해제	379
Oracle 데이터베이스 복원 및 복구	380
워크플로 복원	380
Oracle 데이터베이스에 대한 복원 및 복구 전략 정의	380
특정 사전 스크립트 및 사후 스크립트를 복원하기 위한 사전 정의된 환경 변수	385
Oracle 데이터베이스 복원을 위한 요구 사항	386
Oracle 데이터베이스 복원 및 복구	387
지정 시점 복구를 사용하여 테이블스페이스 복원 및 복구	391
특정 시점 복구를 사용하여 플러그형 데이터베이스를 복원하고 복구합니다.	393
UNIX 명령을 사용하여 Oracle 데이터베이스 복원 및 복구	395
Oracle 데이터베이스 복원 작업 모니터링	396
Oracle 데이터베이스 복원 작업 취소	396
Oracle 데이터베이스 복제	397
복제 워크플로	397
Oracle 데이터베이스에 대한 복제 전략 정의	398
클론별 Prescript 및 Postscript에 대한 미리 정의된 환경 변수	399
Oracle 데이터베이스 복제를 위한 요구 사항	401
Oracle 데이터베이스 백업 복제	402
플러그형 데이터베이스 복제	410
UNIX 명령을 사용하여 Oracle 데이터베이스 백업 복제	414
Oracle 데이터베이스 복제본 분할	415
플러그형 데이터베이스의 분할 복제본	416
Oracle 데이터베이스 복제 작업 모니터링	416
클론 새로 고침	417
플러그형 데이터베이스의 복제본 삭제	418
애플리케이션 볼륨 관리	419
애플리케이션 볼륨이란 무엇입니까?	419
애플리케이션 볼륨 추가	419
백업 애플리케이션 볼륨	420
복제 애플리케이션 볼륨 백업	422
Windows 파일 시스템 보호	425
Microsoft Windows 개념에 대한 SnapCenter 플러그인	425
Microsoft Windows용 SnapCenter 플러그인 개요	425
Microsoft Windows용 SnapCenter 플러그인으로 할 수 있는 일	425
Windows용 SnapCenter 플러그인 기능	425
SnapCenter Windows 파일 시스템을 백업하는 방법	427
Microsoft Windows용 SnapCenter 플러그인에서 지원하는 스토리지 유형	427
Windows 플러그인에 필요한 최소 ONTAP 권한	429

SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비	431
Windows 파일 시스템에 대한 백업 전략 정의	432
Windows 파일 시스템용 복제본의 소스 및 대상	433
Microsoft Windows용 SnapCenter 플러그인 설치	434
Microsoft Windows용 SnapCenter 플러그인 설치 워크플로	434
Microsoft Windows용 SnapCenter 플러그인 설치 요구 사항	434
호스트를 추가하고 Microsoft Windows용 SnapCenter 플러그인을 설치합니다.	438
PowerShell cmdlet을 사용하여 여러 원격 호스트에 Microsoft Windows용 SnapCenter 플러그인 설치	442
명령줄에서 Microsoft Windows용 SnapCenter 플러그인을 자동으로 설치합니다.	442
SnapCenter 플러그인 패키지 설치 상태 모니터링	444
CA 인증서 구성	444
SnapCenter Plug-in for VMware vSphere 설치	448
CA 인증서 배포	448
CRL 파일 구성	448
Windows 파일 시스템 백업	448
Windows 파일 시스템 백업	448
Windows 파일 시스템의 리소스 가용성 확인	450
Windows 파일 시스템에 대한 백업 정책 만들기	450
Windows 파일 시스템에 대한 리소스 그룹 만들기	453
ASA r2 시스템에서 Windows 파일 시스템에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.	455
PowerShell cmdlet을 사용하여 스토리지 시스템 연결 및 자격 증명 만들기	458
Windows 파일 시스템에 대한 단일 리소스를 필요에 따라 백업합니다.	459
Windows 파일 시스템에 대한 리소스 그룹 백업	463
백업 작업 모니터링	464
백업 작업 취소	465
토폴로지 페이지에서 관련 백업 및 복제본 보기	466
PowerShell cmdlet을 사용하여 보조 백업 수 정리	468
Windows 파일 시스템 복원	468
Windows 파일 시스템 백업 복원	468
PowerShell cmdlet을 사용하여 리소스 복원	473
복원 작업 모니터링	476
복원 작업 취소	477
Windows 파일 시스템 복제	478
Windows 파일 시스템 백업에서 복제	478
복제 작업 모니터링	484
복제 작업 취소	485
클론 분할	485
Microsoft Exchange Server 데이터베이스 보호	488
Microsoft Exchange Server 개념에 대한 SnapCenter 플러그인	488
Microsoft Exchange Server용 SnapCenter 플러그인 개요	488
Microsoft Exchange Server용 SnapCenter 플러그인으로 할 수 있는 작업	488

Microsoft Windows 및 Microsoft Exchange Server용 SnapCenter 플러그인에서 지원하는 스토리지 유형	489
Exchange 플러그인에 필요한 최소 ONTAP 권한	490
SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비	493
Exchange Server 리소스에 대한 백업 전략 정의	493
Exchange 데이터베이스에 대한 복원 전략 정의	496
Microsoft Exchange Server용 SnapCenter 플러그인 설치	497
Microsoft Exchange Server용 SnapCenter 플러그인 설치 워크플로	497
Microsoft Exchange Server용 SnapCenter 플러그인을 설치하고 호스트를 추가하기 위한 전제 조건	497
Windows용 SnapCenter 플러그인에 대한 자격 증명 설정	501
Windows Server 2016 이상에서 gMSA 구성	502
호스트 추가 및 Exchange용 플러그인 설치	504
PowerShell cmdlet을 사용하여 SnapCenter 서버 호스트에서 Exchange용 플러그인 설치	509
명령줄에서 Exchange용 SnapCenter 플러그인을 자동으로 설치합니다.	509
SnapCenter 플러그인 패키지 설치 상태 모니터링	511
CA 인증서 구성	511
Exchange와 SnapCenter 공존하도록 SnapManager 7.x 구성	515
SnapCenter Plug-in for VMware vSphere 설치	516
CA 인증서 배포	516
CRL 파일 구성	517
데이터 보호를 준비하세요	517
Microsoft Exchange Server용 SnapCenter 플러그인을 사용하기 위한 전제 조건	517
Exchange Server를 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식	518
Exchange 리소스 백업	519
백업 워크플로	519
Exchange 데이터베이스 및 백업 검증	519
백업에 Exchange 리소스를 사용할 수 있는지 확인합니다.	520
Exchange Server 데이터베이스에 대한 백업 정책 만들기	521
Exchange Server에 대한 리소스 그룹 생성 및 정책 첨부	528
PowerShell cmdlet을 사용하여 Exchange Server용 스토리지 시스템 연결 및 자격 증명 만들기	530
Exchange 데이터베이스 백업	531
Exchange 리소스 그룹 백업	535
백업 작업 모니터링	536
Exchange 데이터베이스에 대한 백업 작업 취소	537
토폴로지 페이지에서 Exchange 백업 보기	538
Exchange 리소스 복원	540
워크플로 복원	540
Exchange 데이터베이스 복원을 위한 요구 사항	540
Exchange 데이터베이스 복원	540
메일 및 사서함의 세분화된 복구	545
보조 저장소에서 Exchange Server 데이터베이스 복원	545
수동 Exchange 노드 복제본을 다시 시드합니다.	545

PowerShell cmdlet을 사용하여 Exchange 데이터베이스에 대한 복제본을 다시 시도합니다.	546
복원 작업 모니터링	547
Exchange 데이터베이스에 대한 복원 작업 취소	548
IBM Db2 보호	549
IBM Db2용 SnapCenter 플러그인	549
IBM Db2용 SnapCenter 플러그인 개요	549
IBM Db2용 SnapCenter 플러그인을 사용하여 수행할 수 있는 작업	549
IBM Db2용 SnapCenter 플러그인 기능	550
IBM Db2용 SnapCenter 플러그인에서 지원하는 스토리지 유형	550
IBM Db2 플러그인에 필요한 최소 ONTAP 권한	551
IBM Db2용 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비	554
IBM Db2에 대한 백업 전략	554
IBM Db2에 대한 복원 및 복구 전략	556
IBM Db2용 SnapCenter 플러그인 설치를 준비하세요	558
IBM Db2용 SnapCenter 플러그인 설치 워크플로	558
Windows, Linux 또는 AIX용 호스트 추가 및 플러그인 패키지 설치를 위한 전제 조건	558
Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	563
Linux용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	564
IBM Db2용 SnapCenter 플러그인에 대한 자격 증명 설정	565
Windows Server 2016 이상에서 gMSA 구성	567
IBM Db2용 SnapCenter 플러그인 설치	568
CA 인증서 구성	573
데이터 보호를 준비하세요	581
IBM Db2용 SnapCenter 플러그인을 사용하기 위한 전제 조건	581
IBM Db2를 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식	581
IBM Db2 리소스 백업	582
IBM Db2 리소스 백업	582
데이터베이스를 자동으로 검색합니다	584
플러그인 호스트에 수동으로 리소스 추가	584
IBM Db2에 대한 백업 정책 만들기	585
리소스 그룹을 만들고 정책을 첨부합니다	588
ASA r2 시스템에서 IBM Db2 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다	591
PowerShell cmdlet을 사용하여 IBM Db2용 스토리지 시스템 연결 및 자격 증명 만들기	593
Db2 데이터베이스 백업	595
리소스 그룹 백업	600
IBM Db2 백업 작업 모니터링	601
IBM Db2에 대한 백업 작업 취소	602
토폴로지 페이지에서 IBM Db2 백업 및 복제본 보기	603
IBM Db2 복원	604
워크플로 복원	604
수동으로 추가된 리소스 백업 복원	605

자동 검색된 데이터베이스 백업을 복원하고 복구합니다.....	609
IBM Db2 복원 작업 모니터링	610
IBM Db2 리소스 백업 복제	611
복제 워크플로	611
IBM Db2 백업 복제	612
IBM Db2 복제 작업 모니터링	619
클론 분할	620
SnapCenter 업그레이드 후 IBM Db2 데이터베이스 복제본 삭제 또는 분할	621
PostgreSQL 보호	622
PostgreSQL용 SnapCenter 플러그인	622
PostgreSQL용 SnapCenter 플러그인 개요	622
PostgreSQL용 SnapCenter 플러그인을 사용하여 할 수 있는 일	622
PostgreSQL용 SnapCenter 플러그인 기능	622
PostgreSQL용 SnapCenter 플러그인이 지원하는 스토리지 유형	623
PostgreSQL 플러그인에 필요한 최소 ONTAP 권한	624
PostgreSQL을 위한 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비	627
PostgreSQL 백업 전략	627
PostgreSQL에 대한 복원 및 복구 전략	629
PostgreSQL용 SnapCenter 플러그인 설치를 준비하세요	631
PostgreSQL용 SnapCenter 플러그인 설치 워크플로	631
PostgreSQL용 SnapCenter 플러그인을 호스트 추가하고 설치하기 위한 전제 조건	631
Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	634
Linux용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	635
PostgreSQL용 SnapCenter 플러그인에 대한 자격 증명 설정	636
Windows Server 2016 이상에서 gMSA 구성	638
PostgreSQL용 SnapCenter 플러그인 설치	639
CA 인증서 구성	645
데이터 보호를 준비하세요	652
PostgreSQL용 SnapCenter 플러그인을 사용하기 위한 전제 조건	652
PostgreSQL을 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식	652
PostgreSQL 리소스 백업	653
PostgreSQL 리소스 백업	653
클러스터를 자동으로 검색합니다	655
플러그인 호스트에 수동으로 리소스 추가	655
PostgreSQL에 대한 백업 정책 생성	657
리소스 그룹을 만들고 정책을 첨부합니다	660
ASA r2 시스템에서 PostgreSQL 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다	663
PowerShell cmdlet을 사용하여 PostgreSQL용 스토리지 시스템 연결 및 자격 증명 만들기	665
PostgreSQL 백업	667
리소스 그룹 백업	672
PostgreSQL 백업 작업 모니터링	673

PostgreSQL에 대한 백업 작업 취소	674
토폴로지 페이지에서 PostgreSQL 백업 및 복제본 보기	675
PostgreSQL 복원	676
워크플로 복원	676
수동으로 추가된 리소스 백업을 복원하고 복구합니다.	677
자동 검색된 클러스터 백업 복원 및 복구	681
PowerShell cmdlet을 사용하여 리소스 복원	683
PostgreSQL 복원 작업 모니터링	686
PostgreSQL 리소스 백업 복제	687
복제 워크플로	687
PostgreSQL 백업 복제	688
PostgreSQL 복제 작업 모니터링	691
클론 분할	692
SnapCenter 업그레이드 후 PostgreSQL 클러스터 복제본 삭제 또는 분할	693
MySQL 보호	694
MySQL용 SnapCenter 플러그인	694
MySQL용 SnapCenter 플러그인 개요	694
MySQL용 SnapCenter 플러그인을 사용하여 할 수 있는 일	694
MySQL용 SnapCenter 플러그인 기능	694
MySQL용 SnapCenter 플러그인이 지원하는 스토리지 유형	695
MySQL 플러그인에 필요한 최소 ONTAP 권한	696
MySQL을 위한 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비	699
MySQL 백업 전략	699
MySQL에 대한 복원 및 복구 전략	701
MySQL용 SnapCenter 플러그인 설치 준비	702
MySQL용 SnapCenter 플러그인 설치 워크플로	702
MySQL용 SnapCenter 플러그인을 설치하고 호스트를 추가하기 위한 전제 조건	703
Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	706
Linux용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	707
MySQL용 SnapCenter 플러그인에 대한 자격 증명 설정	708
MySQL용 SnapCenter 플러그인 설치	710
CA 인증서 구성	715
데이터 보호를 준비하세요.	722
MySQL용 SnapCenter 플러그인을 사용하기 위한 전제 조건	722
MySQL을 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식	722
MySQL 리소스 백업	723
MySQL 리소스 백업	723
데이터베이스를 자동으로 검색합니다	725
플러그인 호스트에 수동으로 리소스 추가	725
MySQL에 대한 백업 정책 생성	726
리소스 그룹을 만들고 정책을 첨부합니다.	730

ASA r2 시스템에서 MySQL 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.	733
PowerShell cmdlet을 사용하여 MySQL용 스토리지 시스템 연결 및 자격 증명 만들기	735
MySQL 백업	737
리소스 그룹 백업	742
MySQL 백업 작업 모니터링	743
MySQL에 대한 백업 작업 취소	744
토폴로지 페이지에서 MySQL 백업 및 복제본 보기	745
MySQL 복원	746
워크플로 복원	746
수동으로 추가된 리소스 백업을 복원하고 복구합니다.	747
자동 검색된 데이터베이스 백업을 복원하고 복구합니다.	751
PowerShell cmdlet을 사용하여 리소스 복원	753
MySQL 복원 작업 모니터링	755
MySQL 리소스 백업 복제	756
복제 워크플로	756
MySQL 백업 복제	757
MySQL 복제 작업 모니터링	760
클론 분할	761
SnapCenter 업그레이드 후 MySQL 데이터베이스 복제본 삭제 또는 분할	762
NetApp 지원 플러그인을 사용하여 애플리케이션 보호	763
NetApp 지원 플러그인	763
NetApp 지원 플러그인 개요	763
NetApp 지원 플러그인으로 할 수 있는 작업	763
NetApp 지원 플러그인 기능	764
NetApp 지원 플러그인에서 지원하는 스토리지 유형	765
NetApp 지원 플러그인에 필요한 최소 ONTAP 권한	765
NetApp 지원 플러그인을 위한 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비	768
백업 전략 정의	768
NetApp 지원 플러그인에 대한 백업 전략	769
수동으로 추가된 NetApp 지원 플러그인 리소스에 대해 지원되는 복원 전략 유형	769
NetApp 지원 플러그인 설치를 준비하세요	770
SnapCenter NetApp 지원 플러그인 설치 워크플로	770
Windows, Linux 또는 AIX용 호스트 추가 및 플러그인 패키지 설치를 위한 전제 조건	770
Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	775
Linux 및 AIX용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항	776
NetApp 지원 플러그인에 대한 자격 증명 설정	777
Windows Server 2016 이상에서 gMSA 구성	778
NetApp 지원 플러그인을 설치하세요	780
CA 인증서 구성	786
데이터 보호를 준비하세요	793
NetApp 지원 플러그인을 사용하기 위한 전제 조건	793

NetApp 지원 플러그인 리소스를 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식	794
NetApp 지원 플러그인 리소스 백업	794
NetApp 지원 플러그인 리소스 백업	794
NetApp 지원 플러그인에 리소스 추가	795
NetApp 지원 플러그인 리소스에 대한 정책 생성	799
리소스 그룹을 만들고 정책을 첨부합니다.	803
ASA r2 시스템의 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.	806
PowerShell cmdlet을 사용하여 스토리지 시스템 연결 및 자격 증명 만들기	808
개별 NetApp 지원 플러그인 리소스 백업	809
NetApp 지원 플러그인 리소스의 리소스 그룹 백업	814
NetApp 지원 플러그인 리소스 백업 작업 모니터링	815
NetApp 지원 플러그인에 대한 백업 작업 취소	816
토폴로지 페이지에서 NetApp 지원 플러그인 리소스 관련 백업 및 복제본 보기	817
NetApp 지원 플러그인 리소스 복원	818
NetApp 지원 플러그인 리소스 복원	818
리소스 백업 복원	819
NetApp 지원 플러그인 리소스 복원 작업 모니터링	823
NetApp 지원 플러그인 리소스 백업 복제	824
NetApp 지원 플러그인 리소스 백업 복제	824
백업에서 복제	825
NetApp 지원 플러그인 리소스 복제 작업 모니터링	831
Unix 파일 시스템 보호	832
Unix 파일 시스템용 SnapCenter 플러그인으로 할 수 있는 일	832
지원되는 구성	832
제한 사항	833
특징	833
Unix 파일 시스템용 SnapCenter 플러그인 설치	833
Linux용 호스트 추가 및 플러그인 패키지 설치를 위한 전제 조건	833
GUI를 사용하여 Linux용 호스트 추가 및 플러그인 패키지 설치	834
SnapCenter 플러그인 Loader 서비스 구성	837
Linux 호스트에서 SnapCenter 플러그인 Loader (SPL) 서비스를 사용하여 CA 인증서 구성	840
플러그인에 대한 CA 인증서 활성화	843
SnapCenter Plug-in for VMware vSphere 설치	843
CA 인증서 배포	843
CRL 파일 구성	844
Unix 파일 시스템 보호를 준비하세요	844
Unix 파일 시스템 백업	844
백업에 사용할 수 있는 UNIX 파일 시스템을 알아보세요	844
Unix 파일 시스템에 대한 백업 정책 생성	845
Unix 파일 시스템에 대한 리소스 그룹을 만들고 정책을 첨부합니다.	847
ASA r2 시스템에서 Unix 파일 시스템에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.	849

Unix 파일 시스템 백업	851
Unix 파일 시스템 리소스 그룹 백업	853
Unix 파일 시스템 백업 모니터링	853
토폴로지 페이지에서 보호된 Unix 파일 시스템 보기	854
Unix 파일 시스템 복원 및 복구	856
Unix 파일 시스템 복원	857
Unix 파일 시스템 복원 작업 모니터링	858
유닉스 파일 시스템 복제	859
Unix 파일 시스템 백업 복제	859
클론 분할	860
Unix 파일 시스템 복제 작업 모니터링	861
Azure NetApp Files 에서 실행되는 애플리케이션 보호	863
Azure NetApp Files 에서 실행되는 애플리케이션 보호	863
제한 사항	863
SnapCenter 설치하고 자격 증명을 만듭니다.	863
Azure 가상 머신에 SnapCenter 설치	863
SnapCenter 에서 Azure 자격 증명 만들기	864
Azure 스토리지 계정 구성	865
플러그인 호스트를 추가하기 위한 자격 증명을 만듭니다.	866
SAP HANA 데이터베이스 보호	867
호스트를 추가하고 SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치합니다.	867
SAP HANA 데이터베이스 추가	867
SAP HANA 데이터베이스에 대한 백업 정책 만들기	868
리소스 그룹을 생성하고 SAP HANA 백업 정책을 연결합니다.	869
Azure NetApp Files 에서 실행되는 SAP HANA 데이터베이스 백업	869
SAP HANA 리소스 그룹 백업	870
SAP HANA 데이터베이스 복원 및 복구	871
SAP HANA 데이터베이스 백업 복제	872
Microsoft SQL Server 데이터베이스 보호	873
호스트를 추가하고 SQL Server 데이터베이스용 SnapCenter 플러그인을 설치합니다.	873
SQL Server 데이터베이스에 대한 백업 정책 만들기	873
리소스 그룹을 만들고 SQL 백업 정책을 첨부합니다.	875
Azure NetApp Files 에서 실행되는 SQL Server 데이터베이스 백업	876
SQL Server 리소스 그룹 백업	877
SQL Server 데이터베이스 복원 및 복구	877
SQL Server 데이터베이스 백업 복제	878
Oracle 데이터베이스 보호	880
호스트를 추가하고 Oracle 데이터베이스용 SnapCenter 플러그인을 설치합니다.	880
Oracle 데이터베이스에 대한 백업 정책 생성	880
리소스 그룹을 생성하고 Oracle 백업 정책을 첨부합니다.	881
Azure NetApp Files 에서 실행되는 Oracle 데이터베이스 백업	882

Oracle 리소스 그룹 백업	883
Oracle 데이터베이스 복원 및 복구	883
Oracle 데이터베이스 백업 복제	886
SnapCenter 서버 및 플러그인 관리	889
대시보드 보기	889
대시보드 개요	889
대시보드에서 정보를 보는 방법	892
대시보드에서 작업 상태 보고서 요청	893
대시보드에서 보호 상태 보고서 요청	893
RBAC 관리	894
역할 수정	894
사용자 및 그룹 수정	894
호스트 관리	895
가상 머신 정보 새로 고침	896
플러그인 호스트 수정	897
플러그인 서비스 시작 또는 재시작	897
호스트 유지 관리를 위한 일정을 일시 중단합니다.	898
리소스 페이지에서 지원되는 작업	898
정책 관리	899
정책 수정	899
정책 분리	900
정책 삭제	900
리소스 그룹 관리	901
리소스 그룹에서 작업 중지 및 재개	901
리소스 그룹 삭제	902
백업 관리	902
백업 이름 바꾸기	902
백업 삭제	903
보호 제거	903
클론 삭제	904
작업, 일정, 이벤트 및 로그를 모니터링합니다.	905
작업 모니터링	905
일정을 모니터링하세요	906
이벤트 모니터링	906
로그 모니터링	906
SnapCenter 에서 작업 및 로그 제거	907
SnapCenter 보고 기능 개요	908
액세스 보고서	909
보고서 필터링	909
보고서 내보내기 또는 인쇄	910
이메일 알림을 위한 SMTP 서버 설정	910

이메일로 보고서를 보내는 옵션을 구성하세요	911
SnapCenter 서버 저장소 관리	911
SnapCenter 저장소 보호를 위한 전제 조건	911
SnapCenter 저장소 백업	911
SnapCenter 저장소의 백업 보기	912
SnapCenter 데이터베이스 저장소 복원	912
SnapCenter 저장소 마이그레이션	913
SnapCenter 저장소 비밀번호 재설정	913
신뢰할 수 없는 도메인의 리소스 관리	914
신뢰할 수 없는 도메인 수정	914
신뢰할 수 없는 Active Directory 도메인 등록 취소	915
저장 시스템 관리	915
스토리지 시스템 구성 수정	915
저장 시스템 삭제	917
REST API 지원	917
EMS 데이터 수집 관리	918
EMS 데이터 수집 중지	918
EMS 데이터 수집 시작	919
EMS 데이터 수집 일정 및 대상 SVM 변경	919
EMS 데이터 수집 상태 모니터링	919
SnapCenter 서버 및 플러그인 업그레이드	920
사용 가능한 업데이트를 확인하기 위해 SnapCenter 구성합니다.	920
업그레이드 워크플로	920
지원되는 업그레이드 경로	920
Windows 호스트에서 SnapCenter 서버 업그레이드	921
Linux 호스트에서 SnapCenter 서버 업그레이드	923
플러그인 패키지를 업그레이드하세요	924
기술 업데이트	926
SnapCenter 서버 호스트의 기술 업데이트	926
F5 클러스터의 노드 기술 업데이트	927
이전 SnapCenter 서버 호스트 해제	927
이전 SnapCenter 서버 호스트로 롤백	927
재해 복구	927
SnapCenter 플러그인 호스트의 기술 업데이트	929
저장 시스템의 기술 업데이트	931
기본 저장소의 백업을 업데이트합니다.	932
보조 저장소의 백업을 업데이트합니다.	933
SnapCenter 서버 및 플러그인 제거	935
SnapCenter 플러그인 패키지 제거	935
호스트 제거를 위한 전제 조건	935
호스트 제거	936

SnapCenter GUI를 사용하여 플러그인 제거	936
PowerShell cmdlet을 사용하여 Windows 플러그인 제거	937
호스트에서 로컬로 플러그인 제거	938
CLI를 사용하여 Linux 또는 AIX용 플러그인 패키지 제거	938
Windows 호스트에서 SnapCenter 서버 제거	938
Linux 호스트에서 SnapCenter 서버 제거	939
REST API를 사용하여 자동화	941
REST API를 사용한 SnapCenter 자동화	941
SnapCenter REST API에 기본적으로 액세스하는 방법	941
REST 웹 서비스 기반	941
자원과 국가 대표	941
URI 엔드포인트	942
HTTP 메시지	942
JSON 포매팅	942
기본 작동 특성	942
요청 및 응답 API 트랜잭션	942
CRUD 작업 지원	942
객체 식별자	943
객체 인스턴스 및 컬렉션	943
동기 및 비동기 작업	943
보안	943
API 요청을 제어하는 입력 변수	944
HTTP 메서드	944
요청 헤더	944
요청 본문	944
객체 필터링	945
특정 객체 필드 요청	945
출력 세트에서 객체 정렬	946
컬렉션에서 객체를 검색할 때의 페이지 매김	946
크기 속성	947
API 응답 해석	947
HTTP 상태 코드	947
응답 헤더	948
대응 기관	948
오류	949
SnapCenter 서버 및 플러그인에 지원되는 REST API	949
인증	949
도메인	949
일자리	950
설정	950
호스트	950

리소스	951
백업	952
클론	953
클론 분할	953
리소스 그룹	953
정책	954
스토리지	954
공유하다	954
플러그인	955
보고서	956
알림	956
알박	956
구성	956
인증서 설정	957
저장소	957
버전	957
Swagger API 웹 페이지를 사용하여 REST API에 액세스하는 방법	957
REST API 시작하기	958
안녕하세요 세상	958
법적 고지 사항	959
저작권	959
상표	959
특허	959
개인정보 보호정책	959
오픈소스	959

SnapCenter software 설명서

릴리스 노트

릴리스 노트

SnapCenter 6.1에서 사용할 수 있는 새롭고 향상된 기능에 대해 알아보세요.

새로운 기능 및 향상된 기능의 전체 목록은 다음을 참조하세요. "[SnapCenter 6.1의 새로운 기능](#)".

알려진 문제, 제한 사항, 해결된 문제, 새 명령 및 변경된 명령에 대한 자세한 내용은 다음을 참조하세요. "[SnapCenter 소프트웨어 6.1 릴리스 노트](#)". 릴리스 노트에 액세스하려면 NetApp 계정으로 로그인하거나 계정을 만들어야 합니다.

SnapCenter 에 지원되는 업그레이드 경로

업그레이드 경로를 통해 SnapCenter 의 이전 버전 중에서 최신 버전의 SnapCenter 로 업그레이드할 수 있는 버전과 지원되는 플러그인 버전을 파악하는 데 도움이 됩니다.

SnapCenter 서버 버전을 사용 중이라면...	SnapCenter 서버를 직접 업그레이드할 수 있습니다...	지원되는 플러그인 버전
5.0	6.0	• 5.0 • 6.0
	6.0.1	• 6.0.1
	6.1	• 6.1
6.0	6.0.1	• 6.0 • 6.0.1
	6.1	• 6.1
6.0.1	6.1	• 6.0.1 • 6.1

SnapCenter Plug-in for VMware vSphere 업그레이드에 대한 정보는 다음을 참조하세요. "[SnapCenter Plug-in for VMware vSphere 업그레이드](#)".

시작하기

SnapCenter software 에 대해 알아보세요

SnapCenter 개요

SnapCenter software 애플리케이션과 일관된 데이터 보호를 위한 간단하고 중앙 집중화되고 확장 가능한 플랫폼입니다. 하이브리드 클라우드의 ONTAP 시스템에서 애플리케이션, 데이터베이스, 호스트 파일 시스템 및 VM을 보호합니다.

SnapCenter NetApp Snapshot, SnapRestore, FlexClone, SnapMirror 및 SnapVault 기술을 사용하여 다음을 제공합니다.

- 빠르고 공간 효율적이며 애플리케이션과 일관된 디스크 기반 백업
- 빠르고 세부적인 복원 및 애플리케이션 일관성 복구
- 빠르고 공간 효율적인 복제

SnapCenter에는 SnapCenter Server와 가벼운 플러그인이 포함되어 있습니다. 원격 애플리케이션 호스트에 대한 플러그인 배포를 자동화하고, 백업, 검증 및 복제 작업을 예약하고, 데이터 보호 작업을 모니터링할 수 있습니다.

SnapCenter 온프레미스나 퍼블릭 클라우드에 설치하여 데이터를 보호할 수 있습니다.

- 다음 사항을 보호하기 위해 사내에서 조치합니다.
 - ONTAP FAS, AFF 또는 ASA 기본 시스템에 있는 데이터이며 ONTAP FAS, AFF 또는 ASA 보조 시스템에 복제됨
 - ONTAP Select 기본 시스템에 있는 데이터
 - ONTAP FAS, AFF 또는 ASA 기본 및 보조 시스템에 있는 데이터이며 로컬 StorageGRID 개체 스토리지에 보호됩니다.
 - ONTAP ASA r2 기본 및 보조 시스템에 있는 데이터
- 하이브리드 클라우드의 온프레미스를 통해 다음을 보호하세요.
 - ONTAP FAS, AFF 또는 ASA 기본 시스템에 있는 데이터이며 Cloud Volumes ONTAP에 복제됨
 - NetApp 백업 및 복구 통합을 사용하여 ONTAP FAS, AFF 또는 ASA 기본 및 보조 시스템에 있는 데이터를 클라우드의 개체 및 아카이브 스토리지로 보호합니다.
- 퍼블릭 클라우드에서는 다음을 보호합니다.
 - Cloud Volumes ONTAP (이전 ONTAP Cloud) 기본 시스템에 있는 데이터
 - ONTAP 용 Amazon FSX에 있는 데이터
 - 기본 Azure NetApp Files (Oracle, Microsoft SQL 및 SAP HANA)에 있는 데이터

주요 특징

SnapCenter 다음과 같은 주요 기능을 제공합니다.

- 다양한 애플리케이션의 중앙 집중식, 애플리케이션 일관성 데이터 보호

데이터 보호는 ONTAP 시스템에서 실행되는 Microsoft Exchange Server, Microsoft SQL Server, Linux 또는 AIX의 Oracle 데이터베이스, SAP HANA 데이터베이스, IBM Db2, PostgreSQL, MySQL 및 Windows 호스트 파일 시스템에 대해 지원됩니다. SnapCenter MongoDB, Storage, MaxDB, Sybase ASE, ORASCPM과 같은 애플리케이션의 보호도 지원합니다.

- 정책 기반 백업

정책 기반 백업은 NetApp Snapshot 기술을 활용하여 빠르고 공간 효율적이며 애플리케이션 일관성이 있는 디스크 기반 백업을 생성합니다. 기존 보호 관계를 업데이트하여 보조 저장소에 대한 백업의 자동 보호를 설정할 수도 있습니다.

- 여러 리소스에 대한 백업

SnapCenter 리소스 그룹을 사용하면 동일한 유형의 여러 리소스(애플리케이션, 데이터베이스 또는 호스트 파일 시스템)를 한 번에 백업할 수 있습니다.

- 복원 및 복구

SnapCenter 백업의 빠르고 세부적인 복원과 애플리케이션 일관성을 갖춘 시간 기반 복구를 제공합니다. 하이브리드 클라우드의 어느 대상에서나 복원할 수 있습니다.

- 클로닝

SnapCenter 빠르고 공간 효율적이며 애플리케이션에 일관된 복제 기능을 제공합니다. 하이브리드 클라우드의 모든 대상에 복제할 수 있습니다.

- 단일 사용자 관리 그래픽 사용자 인터페이스

SnapCenter 모든 하이브리드 클라우드 대상에서 백업과 복제를 관리할 수 있는 단일 인터페이스를 제공합니다.

- REST API, Windows cmdlet, UNIX 명령

SnapCenter 모든 오케스트레이션 소프트웨어와의 통합을 위한 대부분의 기능에 대한 REST API를 제공하고, Windows PowerShell cmdlet과 명령줄 인터페이스를 사용할 수 있습니다.

- 중앙 집중식 데이터 보호 대시보드 및 보고

- 보안 및 위임을 위한 역할 기반 액세스 제어(RBAC)

- 모든 백업 메타데이터를 저장할 수 있는 고가용성 내장 리포지토리 데이터베이스

- 플러그인 자동 푸시 설치

- 고가용성

- 재해 복구(DR)

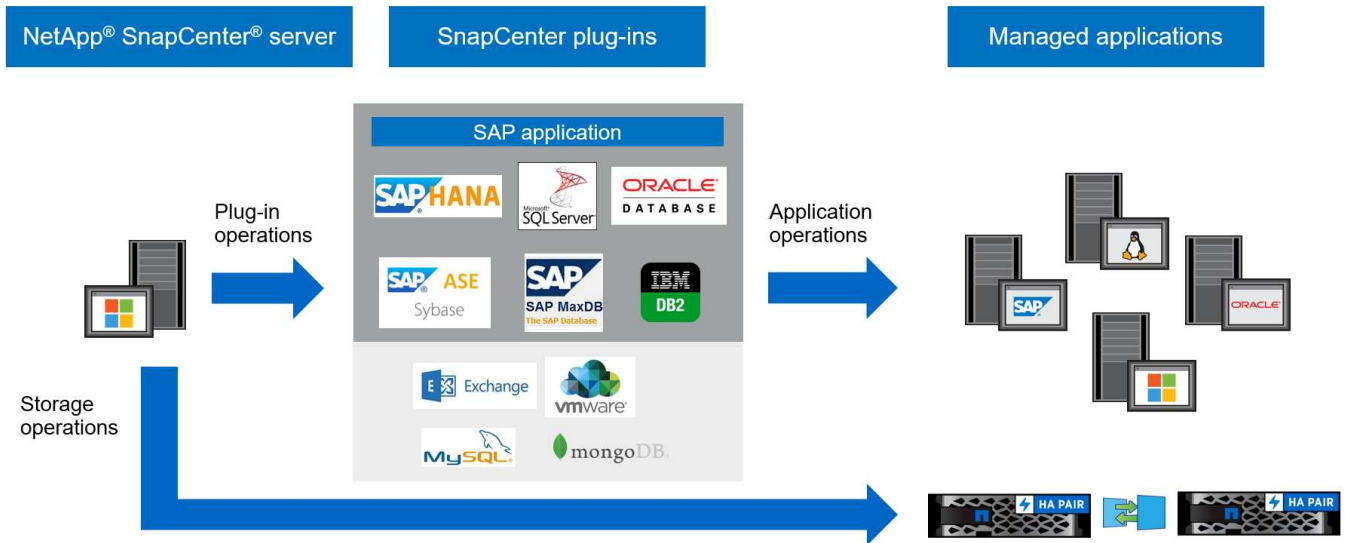
- SnapLock ["자세히 알아보기"](#)

- SnapMirror Active Sync(처음에는 SnapMirror Business Continuity[SM-BC]로 출시됨)

- 동기식 미러링 ["자세히 알아보기"](#)

SnapCenter 아키텍처 및 구성 요소

SnapCenter 중앙 관리 서버와 플러그인 호스트를 갖춘 계층형 디자인을 사용합니다. 서버와 플러그인 호스트는 서로 다른 위치에 있을 수 있습니다.



SnapCenter에는 SnapCenter 서버, Windows용 SnapCenter 플러그인 패키지, Linux용 SnapCenter 플러그인 패키지가 포함되어 있습니다. 각 패키지에는 다양한 애플리케이션과 인프라 구성 요소를 위한 플러그인이 포함되어 있습니다.

SnapCenter 서버

SnapCenter 서버는 Microsoft Windows 및 Linux(RHEL 8.x, RHEL 9.x, SLES 15 SP5) 운영 체제를 지원합니다. SnapCenter 서버에는 웹 서버, 중앙 집중식 HTML5 기반 사용자 인터페이스, PowerShell cmdlet, REST API 및 SnapCenter 저장소가 포함되어 있습니다.

SnapCenter SnapCenter 저장소에 작업 정보를 저장합니다.

SnapCenter 플러그인

각 SnapCenter 플러그인은 특정 환경, 데이터베이스 및 애플리케이션을 지원합니다.

플러그인 이름	설치 패키지에 포함됨	다른 플러그인이 필요합니다	호스트에 설치됨	지원되는 플랫폼
Microsoft SQL Server용 SnapCenter 플러그인	Windows용 플러그인 패키지	Windows용 플러그인	SQL Server 호스트	Windows
Windows용 SnapCenter 플러그인	Windows용 플러그인 패키지		윈도우 호스트	Windows
Microsoft Exchange Server용 SnapCenter 플러그인	Windows용 플러그인 패키지	Windows용 플러그인	Exchange Server 호스트	Windows

플러그인 이름	설치 패키지에 포함됨	다른 플러그인이 필요합니다	호스트에 설치됨	지원되는 플랫폼
Oracle Database용 SnapCentre 플러그인	Linux용 플러그인 패키지 및 AIX용 플러그인 패키지	UNIX용 플러그인	Oracle 호스트	리눅스 또는 AIX
SAP HANA 데이터베이스용 SnapCenter 플러그인	Linux용 플러그인 패키지 및 Windows용 플러그인 패키지	UNIX용 플러그인 또는 Windows용 플러그인	HDBSQL 클라이언트 호스트	리눅스 또는 윈도우
IBM Db2용 SnapCenter 플러그인	Linux용 플러그인 패키지 및 Windows용 플러그인 패키지	UNIX용 플러그인 또는 Windows용 플러그인	Db2 호스트	Linux, AIX 또는 Windows
PostgreSQL용 SnapCenter 플러그인	Linux용 플러그인 패키지 및 Windows용 플러그인 패키지	UNIX용 플러그인 또는 Windows용 플러그인	PostgreSQL 호스트	리눅스 또는 윈도우
MySQL용 SnapCenter 플러그인	Linux용 플러그인 패키지 및 Windows용 플러그인 패키지	UNIX용 플러그인 또는 Windows용 플러그인	MySQL 호스트	리눅스 또는 윈도우
MongoDB용 SnapCenter 플러그인	Linux용 플러그인 패키지 및 Windows용 플러그인 패키지	UNIX용 플러그인 또는 Windows용 플러그인	MongoDB 호스트	리눅스 또는 윈도우
ORASCPM(Oracle Applications)용 SnapCenter 플러그인	Linux용 플러그인 패키지 및 Windows용 플러그인 패키지	UNIX용 플러그인 또는 Windows용 플러그인	Oracle 호스트	리눅스 또는 윈도우
SAP ASE용 SnapCenter 플러그인	Linux용 플러그인 패키지 및 Windows용 플러그인 패키지	UNIX용 플러그인 또는 Windows용 플러그인	SAP 호스트	리눅스 또는 윈도우
SAP MaxDB용 SnapCenter 플러그인	Linux용 플러그인 패키지 및 Windows용 플러그인 패키지	UNIX용 플러그인 또는 Windows용 플러그인	SAP MaxDB 호스트	리눅스 또는 윈도우
스토리지 플러그인을 위한 SnapCenter 플러그인	Linux용 플러그인 패키지 및 Windows용 플러그인 패키지	UNIX용 플러그인 또는 Windows용 플러그인	스토리지 호스트	리눅스 또는 윈도우

SnapCenter Plug-in for VMware vSphere 가상 머신(VM), 데이터 저장소 및 가상 머신 디스크(VMDK)에 대한 충돌 일관성 및 VM 일관성 백업 및 복원 작업을 지원합니다. 또한 가상화된 데이터베이스와 파일 시스템에 대한 애플리케이션 일관성 백업 및 복원 작업도 지원합니다.

데이터베이스, 파일 시스템, VM 또는 VM의 데이터 저장소를 보호하려면 SnapCenter Plug-in for VMware vSphere 배포하세요. 자세한 내용은 다음을 참조하세요. "[SnapCenter Plug-in for VMware vSphere 설명서](#)".

SnapCenter 저장소

SnapCenter 저장소는 때때로 NSM 데이터베이스라고도 하며, 모든 SnapCenter 작업에 대한 정보와 메타데이터를 저장합니다.

SnapCenter 서버를 설치하면 기본적으로 MySQL 서버 저장소 데이터베이스가 설치됩니다. 이미 MySQL 서버를 설치했고 SnapCenter 서버를 새로 설치하려면 MySQL 서버를 제거해야 합니다.

SnapCenter SnapCenter 저장소 데이터베이스로 MySQL Server 8.0.37 이상을 지원합니다. 이전 버전의 SnapCenter 와 함께 이전 버전의 MySQL Server를 사용하는 경우 SnapCenter 업그레이드 프로세스를 통해 MySQL Server가 8.0.37 이상 버전으로 업그레이드됩니다.

SnapCenter 저장소는 다음 정보와 메타데이터를 저장합니다.

- 백업, 복제, 복원 및 검증 메타데이터
- 보고, 직무 및 이벤트 정보
- 호스트 및 플러그인 정보
- 역할, 사용자 및 권한 세부 정보
- 저장 시스템 연결 정보

SnapCenter 의 보안 기능

SnapCenter 엄격한 보안 및 인증 기능을 사용하여 귀하의 데이터를 안전하게 보호합니다.

SnapCenter 에는 다음과 같은 보안 기능이 포함되어 있습니다.

- SnapCenter 와의 모든 통신은 HTTPS(HTTP over SSL)를 사용합니다.
- SnapCenter 의 모든 자격 증명은 AES(Advanced Encryption Standard) 암호화를 사용하여 보호됩니다.
- 연방 정보 처리 표준(FIPS)을 준수하는 보안 알고리즘을 지원합니다.
- 고객이 제공한 공인 CA 인증서 사용을 지원합니다.
- ONTAP 과 통신하기 위해 TLS(전송 계층 보안) 1.3을 지원합니다. 클라이언트와 서버 간 통신에는 TLS 1.2를 사용할 수도 있습니다.
- 네트워크 통신 전반에 걸쳐 보안을 제공하기 위해 특정 SSL 암호화 제품군을 지원합니다. "[자세히 알아보기](#)".
- SnapCenter SnapCenter 서버에 대한 액세스를 활성화하고 SnapCenter 서버와 플러그인 간의 통신을 활성화하기 위해 회사 방화벽 내부에 설치됩니다.
- SnapCenter API 및 운영 액세스는 AES 암호화로 암호화된 토큰을 사용하며, 이 토큰은 24시간 후에 만료됩니다.
- SnapCenter Windows Active Directory와 통합되어 로그인 및 역할 기반 액세스 제어(RBAC)를 통해 액세스 권한을 관리합니다.
- IPsec은 Windows 및 Linux 호스트 머신의 ONTAP 에서 SnapCenter 통해 지원됩니다. "[자세히 알아보기](#)".
- SnapCenter PowerShell cmdlet은 세션 보안이 적용됩니다.
- SnapCenter 기본적으로 15분 동안 활동이 없으면 5분 후에 로그아웃된다는 경고를 표시합니다.

20분 동안 아무런 활동이 없으면 SnapCenter 로그아웃되며, 다시 로그인해야 합니다. 로그아웃 기간을 변경할 수 있습니다.

- 5번 이상 잘못된 로그인을 시도하면 로그인이 일시적으로 비활성화됩니다.
- SnapCenter Server와 ONTAP 간의 CA 인증서 인증을 지원합니다. ["자세히 알아보기"](#).
- 무결성 검증 도구는 SnapCenter 서버와 플러그인에 추가되며, 새로 설치 및 업그레이드 작업 중에 제공된 모든 바이너리의 유효성을 검사합니다.

CA 인증 개요

SnapCenter 서버 설치 프로그램은 설치 중에 중앙 집중식 SSL 인증서 지원을 활성화합니다. 서버와 플러그인 간의 보안 통신을 강화하기 위해 SnapCenter 고객이 제공한 공인 CA 인증서를 사용하도록 지원합니다.

SnapCenter 서버와 해당 플러그인을 설치한 후 CA 인증서를 배포해야 합니다. 자세한 내용은 다음을 참조하세요. ["CA 인증서 CSR 파일 생성"](#).

VMware vSphere용 SnapCenter 플러그인에 대한 CA 인증서를 배포할 수도 있습니다. 자세한 내용은 다음을 참조하세요. ["인증서 생성 및 가져오기"](#).

양방향 SSL 통신

양방향 SSL 통신은 SnapCenter Server와 플러그인 간의 상호 통신을 보호합니다.

인증서 기반 인증 개요

인증서 기반 인증은 SnapCenter 플러그인 호스트에 액세스하려는 각 사용자의 진위성을 검증합니다. 사용자는 개인 키 없이 SnapCenter 서버 인증서를 내보내고 플러그인 호스트 신뢰할 수 있는 저장소로 가져와야 합니다. 인증서 기반 인증은 양방향 SSL 기능이 활성화된 경우에만 작동합니다.

다중 요소 인증(MFA)

MFA는 SAML(Security Assertion Markup Language)을 통해 타사 IdP(Identity Provider)를 사용하여 사용자 세션을 관리합니다. 이 기능은 기존 사용자 이름 및 비밀번호와 함께 TOTP, 생체 인식, 푸시 알림 등 여러 요소를 사용할 수 있는 옵션을 제공하여 인증 보안을 강화합니다. 또한, 고객은 자체 사용자 ID 공급자를 사용하여 포트폴리오 전반에 걸쳐 통합 사용자 로그인(SSO)을 얻을 수 있습니다.

MFA는 SnapCenter 서버 UI 로그인에만 적용됩니다. 로그인에는 IdP Active Directory Federation Services(AD FS)를 통해 인증됩니다. AD FS에서 다양한 인증 요소를 구성할 수 있습니다. SnapCenter 는 서비스 공급자이며 AD FS에서 SnapCenter 신뢰 당사자로 구성해야 합니다. SnapCenter 에서 MFA를 활성화하려면 AD FS 메타데이터가 필요합니다.

MFA를 활성화하는 방법에 대한 정보는 다음을 참조하세요. ["다중 요소 인증 활성화"](#).

SnapCenter 의 역할 기반 액세스 제어

SnapCenter 역할 기반 액세스 제어(RBAC) 및 ONTAP 권한을 통해 SnapCenter 관리자는 SnapCenter 리소스 제어를 여러 사용자 또는 사용자 그룹에 위임할 수 있습니다. 중앙에서 관리되는 액세스를 통해 애플리케이션 관리자는 위임된 환경에서 안전하게 작업할 수 있습니다.

언제든지 역할을 만들고 수정할 수 있으며, 사용자에게 리소스 액세스 권한을 추가할 수 있습니다. 하지만 처음으로

SnapCenter 설정할 때는 최소한 Active Directory 사용자나 그룹을 역할에 추가한 다음, 해당 사용자나 그룹에 리소스 액세스 권한을 추가해야 합니다.



SnapCenter 사용하여 사용자 또는 그룹 계정을 만들 수 없습니다. 운영 체제나 데이터베이스의 Active Directory에서 사용자나 그룹 계정을 만들어야 합니다.

SnapCenter 의 RBAC 유형

SnapCenter 다음과 같은 유형의 역할 기반 액세스 제어를 사용합니다.

- SnapCenter RBAC
- 애플리케이션 수준 RBAC
- VMware vSphere RBAC용 SnapCenter 플러그인
- ONTAP 권한

SnapCenter RBAC

SnapCenter에는 미리 정의된 역할이 있으며, 이러한 역할에 사용자 또는 사용자 그룹을 할당할 수 있습니다. 미리 정의된 역할은 다음과 같습니다.

- SnapCenter 관리자 역할
- 앱 백업 및 복제 관리자 역할
- 백업 및 복제 뷰어 역할
- 인프라 관리자 역할

사용자에게 역할을 할당하면 SnapCenterAdmin 역할을 할당하지 않는 한 해당 사용자와 관련된 작업만 작업 페이지에 표시됩니다.

새로운 역할을 만들고 권한과 사용자를 관리할 수도 있습니다. 호스트, 스토리지 연결, 리소스 그룹 등의 SnapCenter 개체에 액세스하기 위한 권한을 사용자 또는 그룹에 할당할 수 있습니다.

동일한 포리스트 내의 사용자와 그룹, 그리고 다른 포리스트에 속한 사용자에게 RBAC 권한을 할당할 수 있습니다. 여러 포리스트에 걸쳐 중첩된 그룹에 속한 사용자에게 RBAC 권한을 할당할 수 없습니다.



사용자 지정 역할을 만드는 경우 SnapCenterAdmin 역할의 모든 권한을 포함해야 합니다. 예를 들어 호스트 추가나 호스트 제거 등 일부 권한만 복사하는 경우 해당 작업을 수행할 수 없습니다.

사용자는 로그인 시 그래픽 사용자 인터페이스(GUI) 또는 PowerShell cmdlet을 사용하여 인증을 제공해야 합니다. 사용자가 두 개 이상의 역할에 속한 경우 로그인 자격 증명을 입력한 후 사용하려는 역할을 지정하라는 메시지가 표시됩니다. 사용자는 API를 실행하기 위해 인증을 제공해야 합니다.

애플리케이션 수준 RBAC

SnapCenter 자격 증명을 사용하여 권한이 있는 SnapCenter 사용자에게 애플리케이션 수준 권한도 있는지 확인합니다.

예를 들어, SQL Server 환경에서 데이터 보호 작업을 수행하려면 적절한 Windows 또는 SQL 자격 증명을 사용하여 자격 증명을 설정해야 합니다. SnapCenter 서버는 두 가지 방법 중 하나를 사용하여 설정된 자격 증명을 인증합니다. ONTAP 스토리지의 Windows 파일 시스템 환경에서 데이터 보호 작업을 수행하려면 SnapCenter 관리자 역할에

Windows 호스트에 대한 관리자 권한이 있어야 합니다.

마찬가지로, Oracle 데이터베이스에서 데이터 보호 작업을 수행하려는 경우 데이터베이스 호스트에서 운영 체제(OS) 인증이 비활성화된 경우 Oracle 데이터베이스 또는 Oracle ASM 자격 증명으로 자격 증명을 설정해야 합니다. SnapCenter 서버는 작업에 따라 다음 방법 중 하나를 사용하여 설정된 자격 증명을 인증합니다.

SnapCenter Plug-in for VMware vSphere

VM 일관성 데이터 보호를 위해 SnapCenter VMware 플러그인을 사용하는 경우 vCenter Server는 추가 수준의 RBAC를 제공합니다. SnapCenter VMware 플러그인은 vCenter Server RBAC와 ONTAP RBAC를 모두 지원합니다. ["자세히 알아보기"](#)

모범 사례: NetApp SnapCenter Plug-in for VMware vSphere 대해 하나의 ONTAP 역할을 만들고 필요한 모든 권한을 할당할 것을 권장합니다.

ONTAP 권한

스토리지 시스템에 액세스하려면 필요한 권한이 있는 vsadmin 계정을 만들어야 합니다. ["자세히 알아보기"](#)

사전 정의된 SnapCenter 역할에 할당된 권한

역할에 사용자를 추가하는 경우 SVM(스토리지 가상 머신) 통신을 활성화하기 위해 StorageConnection 권한을 할당하거나 SVM을 사용할 수 있는 권한을 활성화하기 위해 사용자에게 SVM을 할당해야 합니다. 저장소 연결 권한을 통해 사용자는 SVM 연결을 생성할 수 있습니다.

예를 들어, SnapCenter 관리자 역할이 있는 사용자는 SVM 연결을 만들고 이를 앱 백업 및 복제 관리자 역할이 있는 사용자에게 할당할 수 있습니다. 이 역할은 기본적으로 SVM 연결을 만들거나 편집할 권한이 없습니다. SVM 연결 없이는 사용자는 백업, 복제 또는 복원 작업을 완료할 수 없습니다.

SnapCenter 관리자 역할

SnapCenter 관리자 역할에는 모든 권한이 활성화되어 있습니다. 이 역할에 대한 권한은 수정할 수 없습니다. 역할에 사용자와 그룹을 추가하거나 제거할 수 있습니다.

앱 백업 및 복제 관리자 역할

앱 백업 및 복제 관리자 역할에는 애플리케이션 백업 및 복제 관련 작업에 대한 관리 작업을 수행하는 데 필요한 권한이 있습니다. 이 역할에는 호스트 관리, 프로비저닝, 스토리지 연결 관리 또는 원격 설치에 대한 권한이 없습니다.

권한	활성화됨	만들다	읽다	업데이트	삭제
리소스 그룹	해당 없음	예	예	예	예
정책	해당 없음	예	예	예	예
지원	해당 없음	예	예	예	예
주인	해당 없음	예	예	예	예
스토리지 연결	해당 없음	아니요	예	아니요	아니요

권한	활성화됨	만들다	읽다	업데이트	삭제
복제	해당 없음	예	예	예	예
공급	해당 없음	아니요	예	아니요	아니요
계기반	예	해당 없음	해당 없음	해당 없음	해당 없음
보고서	예	해당 없음	해당 없음	해당 없음	해당 없음
복원하다	예	해당 없음	해당 없음	해당 없음	해당 없음
의지	예	예	예	예	예
플러그인 설치 /제거	아니요	해당 없음		해당 없음	해당 없음
이주	아니요	해당 없음	해당 없음	해당 없음	해당 없음
산	예	예	해당 없음	해당 없음	해당 없음
마운트 해제	예	예	해당 없음	해당 없음	해당 없음
전체 볼륨 복원	아니요	아니요	해당 없음	해당 없음	해당 없음
2차 보호	아니요	아니요	해당 없음	해당 없음	해당 없음
작업 모니터	예	해당 없음	해당 없음	해당 없음	해당 없음

백업 및 복제 뷰어 역할

백업 및 복제 뷰어 역할은 모든 권한에 대한 읽기 전용 보기 권한을 갖습니다. 이 역할에는 검색, 보고 및 대시보드 액세스에 대한 권한도 활성화되어 있습니다.

권한	활성화됨	만들다	읽다	업데이트	삭제
리소스 그룹	해당 없음	아니요	예	아니요	아니요
정책	해당 없음	아니요	예	아니요	아니요
지원	해당 없음	아니요	예	아니요	아니요
주인	해당 없음	아니요	예	아니요	아니요

권한	활성화됨	만들다	읽다	업데이트	삭제
스토리지 연결	해당 없음	아니요	예	아니요	아니요
복제	해당 없음	아니요	예	아니요	아니요
공급	해당 없음	아니요	예	아니요	아니요
계기반	예	해당 없음	해당 없음	해당 없음	해당 없음
보고서	예	해당 없음	해당 없음	해당 없음	해당 없음
복원하다	아니요	아니요	해당 없음	해당 없음	해당 없음
의지	아니요	아니요	예	예	아니요
플러그인 설치 /제거	아니요	해당 없음	해당 없음	해당 없음	해당 없음
이주	아니요	해당 없음	해당 없음	해당 없음	해당 없음
산	예	해당 없음	해당 없음	해당 없음	해당 없음
마운트 해제	예	해당 없음	해당 없음	해당 없음	해당 없음
전체 볼륨 복원	아니요	해당 없음	해당 없음	해당 없음	해당 없음
2차 보호	아니요	해당 없음	해당 없음	해당 없음	해당 없음
작업 모니터	예	해당 없음	해당 없음	해당 없음	해당 없음

인프라 관리자 역할

인프라 관리자 역할에는 호스트 관리, 스토리지 관리, 프로비저닝, 리소스 그룹, 원격 설치 보고서 및 대시보드 액세스에 대한 권한이 활성화되어 있습니다.

권한	활성화됨	만들다	읽다	업데이트	삭제
리소스 그룹	해당 없음	예	예	예	예
정책	해당 없음	아니요	예	예	예
지원	해당 없음	예	예	예	예

권한	활성화됨	만들다	읽다	업데이트	삭제
주인	해당 없음	예	예	예	예
스토리지 연결	해당 없음	예	예	예	예
복제	해당 없음	아니요	예	아니요	아니요
공급	해당 없음	예	예	예	예
계기반	예	해당 없음	해당 없음	해당 없음	해당 없음
보고서	예	해당 없음	해당 없음	해당 없음	해당 없음
복원하다	예	해당 없음	해당 없음	해당 없음	해당 없음
의지	예	예	예	예	예
플러그인 설치 /제거	예	해당 없음	해당 없음	해당 없음	해당 없음
이주	아니요	해당 없음	해당 없음	해당 없음	해당 없음
산	아니요	해당 없음	해당 없음	해당 없음	해당 없음
마운트 해제	아니요	해당 없음	해당 없음	해당 없음	해당 없음
전체 볼륨 복원	아니요	아니요	해당 없음	해당 없음	해당 없음
2차 보호	아니요	아니요	해당 없음	해당 없음	해당 없음
작업 모니터	예	해당 없음	해당 없음	해당 없음	해당 없음

SnapCenter 의 재해 복구

SnapCenter 재해 복구(DR) 기능을 사용하면 리소스 손상이나 서버 충돌과 같은 재해로부터 복구할 수 있습니다. SnapCenter 저장소, 서버 일정, 구성 구성 요소, SQL Server용 SnapCenter 플러그인 및 해당 저장소를 복원하는 데 도움이 됩니다.

이 섹션에서는 SnapCenter 의 두 가지 유형의 DR에 대해 설명합니다.

SnapCenter 서버 DR

- SnapCenter 서버 데이터는 백업되며 SnapCenter 서버에 플러그인을 추가하거나 관리하지 않고도 복구할 수 있습니다.

- 보조 SnapCenter 서버는 기본 SnapCenter 서버와 동일한 설치 디렉토리와 동일한 포트에 설치해야 합니다.
- 다중 인증(MFA)의 경우 SnapCenter 서버 DR 중에 모든 브라우저 탭을 닫고 브라우저를 다시 열어 다시 로그인하세요. 이렇게 하면 기존 또는 활성 세션 쿠키가 지워지고 올바른 구성 데이터가 업데이트됩니다.
- SnapCenter 재해 복구 기능은 REST API를 사용하여 SnapCenter 서버를 백업합니다. 보다 "[SnapCenter 서버 재해 복구를 위한 REST API 워크플로](#)".
- 감사 설정 관련 구성 파일은 DR 백업에 백업되지 않으며 복원 작업 후에는 DR 서버에도 백업되지 않습니다. 감사 로그 설정을 수동으로 반복해야 합니다.

SnapCenter 플러그인 및 스토리지 DR

DR은 SQL Server용 SnapCenter 플러그인에서만 사용할 수 있습니다. 플러그인이 다운된 경우 다른 SQL 호스트로 전환하고 몇 가지 단계에 따라 데이터를 복구하세요. 보다 "[SQL Server용 SnapCenter 플러그인의 재해 복구](#)".

SnapCenter ONTAP SnapMirror 사용하여 데이터를 복제하고, 이를 보조 사이트와 동기화하여 DR에 사용할 수 있습니다. 장애 조치를 시작하려면 SnapMirror 복제를 중단하세요. 폴백 중에는 동기화를 역으로 진행하여 DR 사이트의 데이터를 기본 위치로 복제합니다.

SnapCenter 에 필요한 라이선스

SnapCenter 애플리케이션, 데이터베이스, 파일 시스템 및 가상 머신의 데이터 보호를 위해 여러 라이선스가 필요합니다. 설치하는 SnapCenter 라이선스 유형은 스토리지 환경과 사용하려는 기능에 따라 달라집니다.

특허	필요한 경우
SnapCenter Standard 컨트롤러 기반	FAS, AFF, ASA 에 필요함 SnapCenter Standard 라이선스는 컨트롤러 기반 라이선스이며 NetApp ONTAP One의 일부로 포함됩니다. SnapManager Suite 라이선스가 있는 경우 SnapCenter Standard 라이선스 권한도 제공됩니다. FAS, AFF 또는 ASA 스토리지를 사용하여 SnapCenter 체험판으로 설치하려는 경우 영업 담당자에게 문의하여 NetApp ONTAP One 평가판 라이선스를 받을 수 있습니다. NetApp ONTAP One에 포함된 라이선스에 대한 정보는 다음을 참조하세요. "NetApp ONTAP One에 포함된 라이선스".  SnapCenter 데이터 보호 번들의 일부로도 제공됩니다. A400 이상을 구매한 경우 데이터 보호 번들을 구매해야 합니다.
SnapMirror 또는 SnapVault	ONTAP SnapCenter 에서 복제가 활성화된 경우 SnapMirror 또는 SnapVault 라이선스가 필요합니다.

특허	필요한 경우
SnapRestore	백업을 복원하고 확인하는 데 필요합니다. 1차 스토리지 시스템에서 • SnapVault 대상 시스템에서 원격 검증을 수행하고 백업에서 복원하는 데 필요합니다. • SnapMirror 대상 시스템에서 원격 검증을 수행하는 데 필요합니다.
FlexClone	데이터베이스 복제 및 검증 작업에 필요합니다. 1차 및 2차 저장 시스템에서 • SnapVault 대상 시스템에서 보조 볼트 백업으로부터 복제본을 생성하는 데 필요합니다. • SnapMirror 대상 시스템에서 보조 SnapMirror 백업으로부터 복제본을 생성하는 데 필요합니다.
프로토콜 라이선스	• LUN에 대한 iSCSI 또는 FC 라이선스 • SMB 주식에 대한 CIFS 라이선스 • NFS 유형 VMDK에 대한 NFS 라이선스 • VMFS 유형 VMDK에 대한 iSCSI 또는 FC 라이선스 소스 볼륨을 사용할 수 없는 경우 SnapMirror 대상 시스템에서 데이터를 제공하는 데 필요합니다.
SnapCenter Standard 라이선스(선택 사항)	2차 목적지  보조 대상에 SnapCenter Standard 라이선스를 추가하는 것이 권장되지만 필수는 아닙니다. 보조 대상에서 SnapCenter Standard 라이선스가 활성화되지 않은 경우 장애 조치 작업을 수행한 후 SnapCenter 사용하여 보조 대상의 리소스를 백업할 수 없습니다. 그러나 복제 및 검증 작업을 수행하려면 보조 대상에 FlexClone 라이선스가 필요합니다.

특허	필요한 경우
단일 사서함 복구(SMBR) 라이선스	Exchange용 SnapCenter 플러그인을 사용하여 Microsoft Exchange Server 데이터베이스와 SMBR(단일 사서함 복구)을 관리하는 경우, 사용자 사서함에 따라 별도로 구매해야 하는 SMBR에 대한 추가 라이선스가 필요합니다. NetApp® Single Mailbox Recovery는 2023년 5월 12일에 제공이 종료되었습니다(EOA). 자세한 내용은 다음을 참조하세요. "CPC-00507". NetApp 2020년 6월 24일에 출시된 마케팅 부품 번호를 통해 사서함 용량, 유지 관리 및 지원을 구매한 고객을 지원 자격 기간 동안 계속 지원할 것입니다. NetApp Single Mailbox Recovery는 Ontrack에서 제공하는 파트너 제품입니다. Ontrack PowerControls는 NetApp Single Mailbox Recovery와 유사한 기능을 제공합니다. 고객은 2023년 5월 12일 EOA 날짜 이후 세분화된 사서함 복구를 위해 Ontrack(licensingteam@ontrack.com)을 통해 새로운 Ontrack PowerControls 소프트웨어 라이선스와 Ontrack PowerControls 유지 관리 및 지원 갱신을 구매할 수 있습니다.



SnapCenter Advanced 및 SnapCenter NAS File Services 라이선스는 더 이상 제공되지 않습니다. Amazon FSx for NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP 및 Azure NetApp Files 더 이상 표준 라이선스 및 용량 기반 라이선스가 필요하지 않습니다.

SnapCenter 라이선스를 하나 이상 설치해야 합니다. 라이선스를 추가하는 방법에 대한 정보는 다음을 참조하세요. "[SnapCenter Standard 컨트롤러 기반 라이선스 추가](#)".

SnapCenter 의 SnapMirror 활성화 동기화

SnapMirror 액티브 동기화를 사용하면 사이트 전체에 장애가 발생하더라도 비즈니스 서비스가 계속 운영될 수 있으며, 보조 복사본을 사용하여 애플리케이션이 투명하게 장애 조치되도록 지원합니다. SnapMirror Active Sync를 사용하면 장애 조치를 트리거하는 데 수동 개입이나 추가 스크립팅이 필요하지 않습니다.

SnapMirror Active Sync에 대한 자세한 내용은 다음을 참조하세요. "[SnapMirror Active Sync 개요](#)".

SnapMirror Active Sync의 경우 다양한 하드웨어, 소프트웨어 및 시스템 구성 요구 사항을 충족했는지 확인하세요. 자세한 내용은 다음을 참조하세요. "[필수 조건](#)".

이 기능에 지원되는 플러그인은 SQL Server용 SnapCenter 플러그인, Windows용 SnapCenter 플러그인, Oracle 데이터베이스용 SnapCenter 플러그인, SAP HANA 데이터베이스용 SnapCenter 플러그인, Microsoft Exchange Server용 SnapCenter 플러그인, Unix용 SnapCenter 플러그인입니다.



SnapCenter 에서 호스트 개시자 근접성을 지원하려면 ONTAP 에서 소스 또는 대상 값을 설정해야 합니다.

SnapCenter 에서 지원되지 않는 사용 사례:

- ONTAP 에서 SnapMirror Active Sync 관계에 대한 정책을 _automatedfailover_에서 _automatedfailoverduplex_로 변경하여 기존 비대칭 SnapMirror Active Sync 워크로드를 대칭으로 변환하는 경우 SnapCenter 에서는 동일한 기능이 지원되지 않습니다.
- SnapCenter 에서 이미 보호된 리소스 그룹의 백업이 있는 경우 ONTAP 에서 SnapMirror 활성 동기화 관계의 스토리지 정책이 _automatedfailover_에서 _automatedfailoverduplex_로 변경되더라도 SnapCenter 에서는 동일한 정책이 지원되지 않습니다.

데이터 보호의 핵심 개념

SnapCenter 사용하기 전에 백업, 복제, 복원에 대한 핵심 개념을 이해하세요.

리소스

리소스에는 SnapCenter 로 백업되거나 복제된 데이터베이스, Windows 파일 시스템 또는 파일 공유가 포함됩니다. 환경에 따라 리소스는 데이터베이스 인스턴스, SQL Server 가용성 그룹, Oracle 데이터베이스, RAC 데이터베이스 또는 사용자 지정 애플리케이션 그룹일 수도 있습니다.

리소스 그룹

리소스 그룹은 호스트나 클러스터에 있는 리소스의 모음으로, 잠재적으로 여러 호스트와 클러스터에 속합니다. 리소스 그룹에서 수행되는 작업은 지정된 일정에 따라 모든 리소스에 적용됩니다. 개별 리소스나 그룹에 대해 주문형 또는 예약된 백업을 수행할 수 있습니다.



공유 리소스 그룹의 한 호스트가 유지 관리 모드로 전환되면 해당 그룹에 대해 예약된 모든 작업이 모든 호스트에서 중단됩니다.

특정 리소스를 백업하려면 관련 플러그인을 사용하세요. 데이터베이스용 데이터베이스 플러그인, 파일 시스템용 파일 시스템 플러그인, VM 및 데이터 저장소용 SnapCenter Plug-in for VMware vSphere 사용하세요.

정책

정책은 데이터 보호 작업의 백업 빈도, 사본 보존, 복제, 스크립트 및 기타 특성을 지정합니다.

리소스 그룹을 생성하거나 주문형 백업을 수행할 때 하나 이상의 정책을 선택할 수 있습니다.

리소스 그룹은 보호해야 할 내용과 보호해야 할 날짜와 시간을 정의합니다. 정책은 보호가 어떻게 수행될 것인지 설명합니다. 예를 들어, 호스트의 모든 데이터베이스나 파일 시스템을 백업해야 하는 경우, 호스트의 모든 데이터베이스나 파일 시스템을 포함하는 리소스 그룹을 생성할 수 있습니다. 그러면 리소스 그룹에 일일 정책과 시간당 정책이라는 두 가지 정책을 첨부할 수 있습니다.

리소스 그룹을 만들고 정책을 첨부할 때 매일 전체 백업을 수행하도록 구성하고 매시간 로그 백업을 위한 일정을 별도로 지정할 수 있습니다.

사용자 정의 사전 규정 및 사후 규정은 데이터 보호 작업에 사용될 수 있습니다. 이러한 스크립트를 사용하면 데이터 보호 작업 전이나 후에 자동화를 수행할 수 있습니다. 예를 들어, 스크립트는 데이터 보호 작업 실패나 경고를 자동으로 알릴 수 있습니다. 이러한 스크립트를 작성하는 데 필요한 요구 사항을 이해하는 것은 사전 스크립트와 사후 스크립트를 설정하는 데 중요합니다.

전치사와 후치사의 사용

사용자 정의 사전 스크립트와 사후 스크립트를 사용하면 작업 전이나 후에 데이터 보호 작업을 자동화할 수 있습니다. 예를 들어, 작업 실패나 경고를 알려주는 스크립트를 추가할 수 있습니다. 스크립트를 설정하기 전에 해당 스크립트에 대한 요구 사항을 이해했는지 확인하세요.

지원되는 스크립트 유형

Windows에서는 다음과 같은 유형의 스크립트가 지원됩니다.

- 배치 파일
- PowerShell 스크립트
- Perl 스크립트

UNIX에서는 다음과 같은 유형의 스크립트가 지원됩니다.

- Perl 스크립트
- 파이썬 스크립트
- 셸 스크립트



기본 bash 셸과 함께 sh-shell, k-shell, c-shell과 같은 다른 셸도 지원됩니다.

스크립트 경로

비가상화 및 가상화 스토리지 시스템 모두에서 SnapCenter 작업의 일부로 실행되는 모든 사전 스크립트와 사후 스크립트는 플러그인 호스트에서 실행됩니다.

- Windows 스크립트는 플러그인 호스트에 위치해야 합니다.



prescripts 또는 postscripts 경로에는 드라이브나 공유가 포함되어서는 안 됩니다. 경로는 SCRIPTS_PATH를 기준으로 해야 합니다.

- UNIX 스크립트는 플러그인 호스트에 위치해야 합니다.



스크립트 경로는 실행 시점에 검증됩니다.

스크립트를 지정할 위치

스크립트는 백업 정책에 지정됩니다. 백업 작업이 시작되면 정책은 스크립트를 백업되는 리소스와 자동으로 연결합니다. 백업 정책을 생성할 때 prescript 및 postscript 인수를 지정할 수 있습니다.



여러 스크립트를 지정할 수 없습니다.

스크립트 시간 초과

기본적으로 시간 제한은 60초로 설정됩니다. 시간 초과 값을 수정할 수 있습니다.

스크립트 출력

Windows 프리스크립트와 포스트스크립트 출력 파일의 기본 디렉토리는 Windows\System32입니다.

UNIX 스크립트와 포스트스크립트에 대한 기본 위치는 없습니다. 원하는 위치로 출력 파일을 리디렉션할 수 있습니다.

SnapCenter 에서 지원하는 스토리지 시스템 및 애플리케이션

SnapCenter 가 지원하는 스토리지 시스템, 애플리케이션, 데이터베이스를 알아야 합니다.

지원되는 스토리지 시스템

- NetApp ONTAP 9.12.1 이상
- Azure NetApp Files
- Amazon FSx for NetApp ONTAP

TCP(Transport Control Protocol)를 통한 NVMe(Non-Volatile Memory Express)를 지원합니다.

Amazon FSx for NetApp ONTAP 에 대한 정보는 다음을 참조하세요. ["Amazon FSx for NetApp ONTAP 설명서"](#).

- NetApp ONTAP 9.16.1을 실행하는 NetApp ASA r2 시스템.

지원되는 애플리케이션 및 데이터베이스

SnapCenter 다양한 애플리케이션과 데이터베이스의 보호를 지원합니다. 지원되는 애플리케이션 및 데이터베이스에 대한 자세한 내용은 다음을 참조하세요. ["NetApp 상호 운용성 매트릭스 도구"](#).

SnapCenter Amazon Web Services(AWS) 소프트웨어 정의 데이터 센터(SDDC) 환경의 VMware Cloud에서 Oracle 및 Microsoft SQL 워크로드 보호를 지원합니다. ["자세히 알아보기"](#).

SnapCenter 자격 증명에 대한 인증 방법

자격 증명은 애플리케이션이나 환경에 따라 다양한 인증 방법을 사용합니다. 자격 증명은 사용자를 인증하여 SnapCenter 작업을 수행할 수 있도록 합니다. 플러그인 설치를 위한 자격 증명 세트 하나와 데이터 보호 작업을 위한 자격 증명 세트 하나를 만들어야 합니다.

Windows 인증

Windows 인증 방법은 Active Directory를 기반으로 인증합니다. Windows 인증의 경우 Active Directory는 SnapCenter 외부에 설정됩니다. SnapCenter 추가 구성 없이 인증됩니다. 호스트를 추가하고, 플러그인 패키지를 설치하고, 작업을 예약하려면 Windows 자격 증명이 필요합니다.

신뢰할 수 없는 도메인 인증

SnapCenter 사용하면 신뢰할 수 없는 도메인에 속한 사용자와 그룹이 Windows 자격 증명을 생성할 수 있습니다. 인증이 성공하려면 신뢰할 수 없는 도메인을 SnapCenter 에 등록해야 합니다.

로컬 작업 그룹 인증

SnapCenter 사용하면 로컬 작업 그룹 사용자 및 그룹으로 Windows 자격 증명을 생성할 수 있습니다. 로컬 작업 그룹 사용자 및 그룹에 대한 Windows 인증은 Windows 자격 증명 생성 중에 발생하지 않지만 호스트 등록 및 기타 호스트 작업이 수행될 때까지 지연됩니다.

SQL Server 인증

SQL 인증 방법은 SQL Server 인스턴스를 대상으로 인증합니다. 즉, SQL Server 인스턴스는 SnapCenter 에서 검색되어야 합니다. 따라서 SQL 자격 증명을 추가하기 전에 호스트를 추가하고, 플러그인 패키지를 설치하고, 리소스를 새로 고쳐야 합니다. SQL Server에서 일정을 예약하거나 리소스를 검색하는 등의 작업을 수행하려면 SQL Server 인증이 필요합니다.

리눅스 인증

Linux 인증 방법은 Linux 호스트를 대상으로 인증합니다. SnapCenter GUI에서 Linux 호스트를 추가하고 Linux용 SnapCenter 플러그인 패키지를 원격으로 설치하는 초기 단계에서는 Linux 인증이 필요합니다.

AIX 인증

AIX 인증 방법은 AIX 호스트를 대상으로 인증합니다. SnapCenter GUI에서 원격으로 AIX 호스트를 추가하고 AIX용 SnapCenter 플러그인 패키지를 설치하는 초기 단계에서는 AIX 인증이 필요합니다.

Oracle 데이터베이스 인증

Oracle 데이터베이스 인증 방법은 Oracle 데이터베이스를 대상으로 인증합니다. 데이터베이스 호스트에서 운영 체제(OS) 인증이 비활성화된 경우 Oracle 데이터베이스에서 작업을 수행하려면 Oracle 데이터베이스 인증이 필요합니다. 따라서 Oracle 데이터베이스 자격 증명을 추가하기 전에 sysdba 권한이 있는 Oracle 사용자를 Oracle 데이터베이스에 만들어야 합니다.

Oracle ASM 인증

Oracle ASM 인증 방법은 Oracle Automatic Storage Management(ASM) 인스턴스를 대상으로 인증합니다. Oracle ASM 인스턴스에 액세스해야 하고 데이터베이스 호스트에서 OS 인증이 비활성화된 경우 Oracle ASM 인증이 필요합니다. Oracle ASM 자격 증명을 추가하기 전에 ASM 인스턴스에서 시스템 권한이 있는 Oracle 사용자를 만듭니다.

RMAN 카탈로그 인증

RMAN 카탈로그 인증 방법은 Oracle Recovery Manager(RMAN) 카탈로그 데이터베이스를 대상으로 인증합니다. 외부 카탈로그 메커니즘을 구성하고 데이터베이스를 카탈로그 데이터베이스에 등록한 경우 RMAN 카탈로그 인증을 추가해야 합니다.

ASA r2 시스템에 지원되는 SnapCenter 작업

ASA r2 스토리지 시스템은 SnapCenter 6.1부터 지원됩니다. ["ASA r2 시스템에 대해 자세히 알아보세요"](#)

SnapCenter ZAPI를 지원하지 않는 ASA r2 시스템에서 모든 작업을 수행하기 위해 REST API를 활용합니다.

- ASA r2 시스템용 SnapCenter 에서 지원하는 작업*

- VMDK를 통한 애플리케이션의 기본 백업 생성
- 일관성 그룹 스냅샷을 보조 스토리지 시스템으로 전송
- 기본 및 보조 스토리지 시스템에서 백업을 원래 호스트 또는 대체 호스트로 복원합니다.
 - VMware vMotion을 사용하여 기본 및 보조 스토리지 시스템에서 제자리 복원
 - 1차 및 2차 스토리지 시스템 모두에서 연결 및 복사 복원
- 백업을 원래 호스트 또는 대체 호스트로 복제

SnapCenter ONTAP 일관성 그룹을 검색하거나 생성할 수 있습니다. 또한 2차 보호를 위해 대상 클러스터에 대한 SnapMirror 관계를 프로비저닝하고 초기화할 수도 있습니다.

애플리케이션에 대한 ASA r2 시스템에서 보조 보호를 활성화하는 방법에 대한 자세한 내용은 다음을 참조하세요.

- ["Microsoft SQL Server 리소스에 대한 보조 보호 활성화"](#)
- ["SAP HANA 리소스에 대한 보조 보호 활성화"](#)
- ["Oracle 리소스에 대한 보조 보호 활성화"](#)
- ["Windows 파일 시스템에 대한 보조 보호 활성화"](#)
- ["IBM Db2 리소스에 대한 보조 보호 활성화"](#)
- ["PostgreSQL 리소스에 대한 보조 보호 활성화"](#)
- ["MySQL 리소스에 대한 보조 보호 활성화"](#)
- ["Unix 파일 시스템에 대한 보조 보호 활성화"](#)
- ASA r2 시스템용 SnapCenter 에서 지원하지 않는 작업*
- 원시 장치 매핑(RDM)
- Oracle용 애플리케이션 볼륨
- SAP HANA NDV
- 록볼트
- 변조 방지 스냅샷
- FlexGroup 볼륨
- 계층적 일관성 그룹
- ASA, AFF 또는 FAS 스토리지 시스템에서 ASA r2 스토리지 시스템으로 마이그레이션
- ASA, AFF 또는 FAS 리소스와 ASA r2 리소스가 혼합된 데이터베이스 보호
- 스냅샷 이름 바꾸기
- SQL 플러그인 호스트의 로그 디렉토리의 2차 프로비저닝

SnapCenter software 빠른 시작

빠른 시작 가이드에서는 SnapCenter software 설치하고 구성하는 기본 단계를 설명합니다.

1

SnapCenter 서버 설치를 준비하세요

SnapCenter 서버를 설치하는 데 필요한 모든 요구 사항이 충족되었는지 확인해야 합니다.

- ["요구 사항"](#)
- ["SnapCenter software 에 액세스하려면 등록하세요"](#)
- ["다중 요소 인증 활성화"](#)

2

SnapCenter 서버 설치

SnapCenter 서버는 Windows 또는 Linux 호스트에 설치할 수 있습니다. SnapCenter 서버 설치 패키지를 다운로드하세요. ["NetApp 지원 사이트"](#) 설치 프로그램을 실행합니다.

- ["Windows에 SnapCenter 서버 설치"](#)
- ["Linux에 SnapCenter 서버 설치"](#)

3

SnapCenter 서버 구성

SnapCenter 서버를 설치한 후에는 환경에 맞게 구성해야 합니다.

4

귀하의 애플리케이션에 플러그인을 설치하세요

사용 중인 애플리케이션에 따라 애플리케이션별 플러그인을 설치하는 데 필요한 모든 요구 사항이 충족되는지 확인한 다음, 해당 플러그인을 설치하세요.

5

귀하의 애플리케이션을 보호하세요

SnapCenter 서버와 필요한 플러그인을 성공적으로 설치한 후 애플리케이션 백업 생성을 시작할 수 있습니다. 이러한 백업은 나중에 필요할 때 복원 및 복제 목적으로 활용할 수 있습니다.

SnapCenter 서버 설치 및 구성

SnapCenter 서버 설치를 준비하세요

SnapCenter 서버 설치 요구 사항

Windows나 Linux 호스트에 SnapCenter Server를 설치하기 전에 환경에 대한 모든 요구 사항이 충족되는지 검토하고 확인해야 합니다.

Windows 호스트에 대한 도메인 및 작업 그룹 요구 사항

SnapCenter 서버는 도메인이나 작업 그룹에 있는 Windows 호스트에 설치할 수 있습니다.

관리자 권한이 있는 사용자는 SnapCenter 서버를 설치할 수 있습니다.

- Active Directory 도메인: 로컬 관리자 권한이 있는 도메인 사용자를 사용해야 합니다. 도메인 사용자는 Windows 호스트의 로컬 관리자 그룹의 구성원이어야 합니다.
- 작업 그룹: 로컬 관리자 권한이 있는 로컬 계정을 사용해야 합니다.

도메인 트러스트, 다중 도메인 포리스트 및 크로스 도메인 트러스트는 지원되지만 크로스 포리스트 도메인은 지원되지 않습니다. Active Directory 도메인 및 트러스트에 대한 Microsoft 설명서에 자세한 내용이 포함되어 있습니다.



SnapCenter 서버를 설치한 후에는 SnapCenter 호스트가 있는 도메인을 변경해서는 안 됩니다. SnapCenter Server가 설치될 당시에 있던 도메인에서 SnapCenter Server 호스트를 제거한 다음 SnapCenter Server를 제거하려고 하면 제거 작업이 실패합니다.

공간 및 크기 요구 사항

공간과 크기 요구 사항을 잘 알고 있어야 합니다.

목	Windows 호스트 요구 사항	Linux 호스트 요구 사항
운영 체제	마이크로소프트 윈도우 운영 체제는 영어, 독일어, 일본어, 간체 중국어 버전만 지원됩니다. 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. https://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT ["NetApp 상호 운용성 매트릭스 도구"^].	• Red Hat Enterprise Linux(RHEL) 8 및 9 • SUSE Linux Enterprise Server(SLES) 15 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. https://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT ["NetApp 상호 운용성 매트릭스 도구"^].
최소 CPU 수	4개의 코어	4개의 코어

목	Windows 호스트 요구 사항	Linux 호스트 요구 사항
최소 RAM	8GB  MySQL 서버 버퍼 풀은 전체 RAM의 20%를 사용합니다.	8GB
SnapCenter 서버 소프트웨어 및 로그에 대한 최소 하드 드라이브 공간	7GB  SnapCenter 서버가 설치된 드라이브에 SnapCenter 저장소가 있는 경우 15GB를 권장합니다.	15GB
SnapCenter 저장소의 최소 하드 드라이브 공간	8GB  참고: SnapCenter 저장소가 설치된 드라이브에 SnapCenter 서버가 있는 경우 15GB를 권장합니다.	해당 없음
필수 소프트웨어 패키지	• ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 • PowerShell 7.4.2 이상	• .NET Framework 8.0.12(및 이후의 모든 8.0.x 패치) • PowerShell 7.4.2 이상 • Nginx는 역방향 프록시로 사용할 수 있는 웹 서버입니다. • 팜-데벨 PAM(Pluggable Authentication Modules)은 시스템 관리자가 인증을 수행하는 프로그램을 다시 컴파일하지 않고도 인증 정책을 설정할 수 있도록 해주는 시스템 보안 도구입니다.



ASP.NET 코어는 Windows의 SnapCenter Server에 있는 임시 파일 시스템에 액세스하기 위해 IIS_IUSRS가 필요합니다.

SAN 호스트 요구 사항

SnapCenter에는 호스트 유틸리티나 DSM이 포함되어 있지 않습니다. SnapCenter 호스트가 SAN(FC/iSCSI) 환경의 일부인 경우 SnapCenter 서버 호스트에 추가 소프트웨어를 설치하고 구성해야 할 수도 있습니다.

- 호스트 유틸리티: 호스트 유틸리티는 FC와 iSCSI를 지원하며 Windows 서버에서 MPIO를 사용할 수 있게 해줍니다. ["자세히 알아보기"](#).
- Windows MPIO용 Microsoft DSM: 이 소프트웨어는 Windows MPIO 드라이버와 함께 작동하여 NetApp 과 Windows 호스트 컴퓨터 간의 여러 경로를 관리합니다. 고가용성 구성에는 DSM이 필요합니다.



ONTAP DSM을 사용하고 있다면 Microsoft DSM으로 마이그레이션해야 합니다. 자세한 내용은 다음을 참조하세요. ["ONTAP DSM에서 Microsoft DSM으로 마이그레이션하는 방법"](#).

브라우저 요구 사항

SnapCenter software Chrome 125 이상 및 Microsoft Edge 110.0.1587.17 이상을 지원합니다.

포트 요구 사항

SnapCenter software 다양한 구성 요소 간 통신을 위해 서로 다른 포트가 필요합니다.

- 애플리케이션은 포트를 공유할 수 없습니다.
- 사용자 정의 가능한 포트의 경우, 기본 포트를 사용하지 않으려면 설치 중에 사용자 정의 포트를 선택할 수 있습니다.
- 고정 포트의 경우 기본 포트 번호를 사용해야 합니다.
- 방화벽
 - 방화벽, 프록시 또는 기타 네트워크 장치는 연결을 방해해서는 안 됩니다.
 - SnapCenter 설치할 때 사용자 지정 포트를 지정하는 경우 SnapCenter 플러그인 로더의 해당 포트에 대한 방화벽 규칙을 Loader 호스트에 추가해야 합니다.

다음 표에는 다양한 포트와 기본값이 나열되어 있습니다.

포트 이름	포트 번호	규약	방향	설명
SnapCenter 웹 포트	8146	HTTPS	양방향	이 포트는 SnapCenter 클라이언트(SnapCenter 사용자)와 SnapCenter 서버 간 통신에 사용되며 플러그인 호스트에서 SnapCenter 서버로의 통신에도 사용됩니다. 포트 번호를 사용자 정의할 수 있습니다.

포트 이름	포트 번호	규약	방향	설명
SnapCenter SMCore 통신 포트	8145	HTTPS	양방향	이 포트는 SnapCenter 서버와 SnapCenter 플러그인이 설치된 호스트 간의 통신에 사용됩니다. 포트 번호를 사용자 정의할 수 있습니다.
스케줄러 서비스 포트	8154	HTTPS		이 포트는 SnapCenter 서버 호스트 내의 모든 관리 플러그인에 대한 SnapCenter 스케줄러 워크플로를 중앙 집중식으로 조율하는 데 사용됩니다. 포트 번호를 사용자 정의할 수 있습니다.
RabbitMQ 포트	5672	TCP		이는 RabbitMQ가 수신하는 기본 포트이며 Scheduler 서비스와 SnapCenter 간의 게시자-구독자 모델 통신에 사용됩니다.
MySQL 포트	3306	HTTPS		이 포트는 SnapCenter 저장소 데이터베이스와 통신하는 데 사용됩니다. SnapCenter 서버에서 MySQL 서버로 보안 연결을 생성할 수 있습니다. "자세히 알아보기"

포트 이름	포트 번호	규약	방향	설명
Windows 플러그인 호스트	135, 445	TCP		이 포트는 SnapCenter 서버와 플러그인이 설치되는 호스트 간의 통신에 사용됩니다. Microsoft에서 지정한 추가적인 동적 포트 범위도 열려 있어야 합니다.
Linux 또는 AIX 플러그인 호스트	22	SSH	단방향	이 포트는 SnapCenter 서버와 호스트 간의 통신에 사용되며, 서버에서 클라이언트 호스트로 시작됩니다.
Windows, Linux 또는 AIX용 SnapCenter 플러그인 패키지	8145	HTTPS	양방향	이 포트는 SMCORE와 플러그인 패키지가 설치된 호스트 간의 통신에 사용됩니다. 사용자 정의 가능. 포트 번호를 사용자 정의할 수 있습니다.
Oracle 데이터베이스용 SnapCenter 플러그인	27216			기본 JDBC 포트는 Oracle 플러그인이 Oracle 데이터베이스에 연결하는 데 사용됩니다.
Exchange 데이터베이스용 SnapCenter 플러그인	909			기본 NET.TCP 포트는 Windows 플러그인에서 Exchange VSS 콜백에 연결하는 데 사용됩니다.

포트 이름	포트 번호	규약	방향	설명
NetApp SnapCenter 위한 플러그인을 지원합니다.	9090	HTTPS		이는 플러그인 호스트에서만 사용되는 내부 포트입니다. 방화벽 예외는 필요하지 않습니다. SnapCenter 서버와 플러그인 간의 통신은 포트 8145를 통해 라우팅됩니다.
ONTAP 클러스터 또는 SVM 통신 포트	• 443(HTTPS) • 80(HTTP)	• HTTPS • HTTP	양방향	이 포트는 SnapCenter Server를 실행하는 호스트와 SVM 간의 통신을 위해 SAL(Storage Abstraction Layer)에서 사용됩니다. 이 포트는 현재 SnapCenter for Windows 플러그인 호스트의 SAL에서도 사용되어 SnapCenter 플러그인 호스트와 SVM 간 통신에 사용됩니다.
SAP HANA 데이터베이스용 SnapCenter 플러그인	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	양방향	다중 테넌트 데이터베이스 컨테이너(MDC) 단일 테넌트의 경우 포트 번호는 13으로 끝납니다. MDC가 아닌 경우 포트 번호는 15로 끝납니다. 포트 번호를 사용자 정의할 수 있습니다.

포트 이름	포트 번호	규약	방향	설명
PostgreSQL용 SnapCenter 플러그인	5432			이 포트는 PostgreSQL 플러그인이 PostgreSQL 클러스터와 통신하는데 사용하는 기본 PostgreSQL 포트입니다. 포트 번호를 사용자 정의할 수 있습니다.

SnapCenter software 액세스하려면 등록하세요

Amazon FSx for NetApp ONTAP 또는 Azure NetApp Files 처음 사용하고 기존 NetApp 계정이 없는 경우 SnapCenter software 에 액세스하려면 등록해야 합니다.

시작하기 전에

- 회사 이메일 ID에 액세스할 수 있어야 합니다.
- Azure NetApp Files 사용하는 경우 Azure 구독 ID가 있어야 합니다.
- Amazon FSx for NetApp ONTAP 사용하는 경우 FSx for ONTAP 파일 시스템의 파일 시스템 ID가 있어야 합니다.

이 작업에 관하여

귀하의 등록은 정보 검증을 거쳐야 하며, 새로운 NetApp 지원 사이트(NSS) 계정을 게스트 액세스에서 전체 액세스로 확인 및 업그레이드하는 데 최대 하루가 걸릴 수 있습니다.

단계

1. 팔각 하는 소리 <https://mysupport.netapp.com/site/user/registration> 등록을 위해.
2. 회사 이메일 ID를 입력하고, 캡차를 완료하고, NetApp의 개인정보 보호정책에 동의한 후 *제출*을 클릭하세요.
3. 이메일 ID로 전송된 OTP를 입력하여 등록을 인증하고 *계속*을 클릭하세요.
4. 등록 완료 페이지에서 다음 세부 정보를 입력하여 등록을 완료하세요.
 - a. * NetApp 고객/최종 사용자*를 선택하세요.
 - b. Azure NetApp Files 사용하는 경우 SERIAL NUMBER 필드에 Azure 구독 ID를 입력하고, Amazon FSx for NetApp ONTAP 사용하는 경우 파일 시스템 ID를 입력합니다.



티켓을 제출할 수 있습니다 <https://mysupport.netapp.com/site/help> 등록 중에 문제가 발생하거나 상태를 알고 싶은 경우.

다중 요소 인증(MFA)

다중 인증 요소(MFA) 관리

Active Directory Federation Service(AD FS) 서버와 SnapCenter 서버에서 다중 인증(MFA) 기능을 관리할 수 있습니다.

다중 요소 인증(MFA) 활성화

PowerShell 명령을 사용하여 SnapCenter Server에 대한 MFA 기능을 활성화할 수 있습니다.

이 작업에 관하여

- 다른 애플리케이션이 동일한 AD FS에 구성된 경우 SnapCenter SSO 기반 로그인을 지원합니다. 특정 AD FS 구성에서 SnapCenter AD FS 세션 지속성에 따라 보안상의 이유로 사용자 인증을 요구할 수 있습니다.
- cmdlet과 함께 사용할 수 있는 매개변수 및 해당 설명에 대한 정보는 다음을 실행하여 얻을 수 있습니다. `Get-Help command_name`. 또는 다음을 볼 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

시작하기 전에

- Windows Active Directory Federation Service(AD FS)가 해당 도메인에서 실행 중이어야 합니다.
- Azure MFA, Cisco Duo 등과 같이 AD FS에서 지원하는 다중 인증 서비스가 있어야 합니다.
- SnapCenter 와 AD FS 서버 타임스탬프는 시간대에 관계없이 동일해야 합니다.
- SnapCenter Server에 대한 공인 CA 인증서를 조달하고 구성합니다.

CA 인증서는 다음과 같은 이유로 필수입니다.

- 자체 서명된 인증서가 노드 수준에서 고유하기 때문에 ADFS-F5 통신이 중단되지 않도록 보장합니다.
- 독립 실행형 또는 고가용성 구성에서 업그레이드, 복구 또는 재해 복구(DR) 중에 자체 서명된 인증서가 다시 생성되지 않도록 하여 MFA 재구성을 방지합니다.
- IP-FQDN 확인을 보장합니다.

CA 인증서에 대한 정보는 다음을 참조하세요. "[CA 인증서 CSR 파일 생성](#)".

단계

1. Active Directory Federation Services(AD FS) 호스트에 연결합니다.
2. AD FS 페더레이션 메타데이터 파일을 다운로드합니다. "<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>".
3. 다운로드한 파일을 SnapCenter 서버에 복사하여 MFA 기능을 활성화합니다.
4. PowerShell을 통해 SnapCenter 관리자 사용자로 SnapCenter 서버에 로그인합니다.
5. PowerShell 세션을 사용하여 `New-SmMultifactorAuthenticationMetadata -path` cmdlet을 사용하여 SnapCenter MFA 메타데이터 파일을 생성합니다.

경로 매개변수는 SnapCenter 서버 호스트에 MFA 메타데이터 파일을 저장할 경로를 지정합니다.

6. 생성된 파일을 AD FS 호스트에 복사하여 SnapCenter 클라이언트 엔터티로 구성합니다.
7. 다음을 사용하여 SnapCenter 서버에 대한 MFA를 활성화합니다. `Set-SmMultiFactorAuthentication cmdlet`.

8. (선택 사항) 다음을 사용하여 MFA 구성 상태 및 설정을 확인하세요. `Get-SmMultiFactorAuthentication cmdlet`.
9. Microsoft 관리 콘솔(MMC)로 이동하여 다음 단계를 수행합니다.
 - a. 파일 > *스냅인 추가/제거*를 클릭합니다.
 - b. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
 - c. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
 - d. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 개인 > *인증서*를 클릭합니다.
 - e. SnapCenter 에 바인딩된 CA 인증서를 마우스 오른쪽 버튼으로 클릭한 다음 모든 작업 > *개인 키 관리*를 선택합니다.
 - f. 권한 마법사에서 다음 단계를 수행하세요.
 - i. *추가*를 클릭하세요.
 - ii. *위치*를 클릭하고 해당 호스트(계층 구조의 최상위)를 선택합니다.
 - iii. 위치 팝업 창에서 *확인*을 클릭합니다.
 - iv. 개체 이름 필드에 'IIS_IUSRS'를 입력하고 *이름 확인*을 클릭한 다음 *확인*을 클릭합니다.

검사가 성공하면 *확인*을 클릭하세요.

10. AD FS 호스트에서 AD FS 관리 마법사를 열고 다음 단계를 수행합니다.
 - a. 신뢰 당사자 트러스트*를 마우스 오른쪽 버튼으로 클릭하고 *신뢰 당사자 트러스트 추가 > *시작*을 클릭합니다.
 - b. 두 번째 옵션을 선택하고 SnapCenter MFA 메타데이터 파일을 찾은 후 *다음*을 클릭합니다.
 - c. 표시 이름을 지정하고 *다음*을 클릭합니다.
 - d. 필요에 따라 액세스 제어 정책을 선택하고 *다음*을 클릭합니다.
 - e. 다음 탭에서 설정을 기본값으로 선택하세요.
 - f. *마침*을 클릭하세요.

SnapCenter 이제 제공된 표시 이름을 사용하는 신뢰 당사자로 반영됩니다.

11. 이름을 선택하고 다음 단계를 수행하세요.
 - a. *청구 발행 정책 편집*을 클릭하세요.
 - b. *규칙 추가*를 클릭하고 *다음*을 클릭합니다.
 - c. 클레임 규칙의 이름을 지정합니다.
 - d. 속성 저장소로 *Active Directory*를 선택합니다.
 - e. 속성을 *User-Principal-Name*으로 선택하고, 나가는 클레임 유형을 *Name-ID*로 선택합니다.
 - f. *마침*을 클릭하세요.

12. ADFS 서버에서 다음 PowerShell 명령을 실행합니다.

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-SigningCertificateRevocationCheck None
```

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
```

-EncryptionCertificateRevocationCheck None

13. 메타데이터가 성공적으로 가져왔는지 확인하려면 다음 단계를 수행하세요.

- a. 신뢰 당사자 트러스트를 마우스 오른쪽 버튼으로 클릭하고 *속성*을 선택합니다.
- b. 엔드포인트, 식별자, 서명 필드가 채워져 있는지 확인하세요.

14. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성화된 세션 쿠키를 지우고 다시 로그인하세요.

SnapCenter MFA 기능은 REST API를 사용하여 활성화할 수도 있습니다.

문제 해결 정보는 다음을 참조하세요. ["여러 탭에서 동시 로그인 시도 시 MFA 오류가 표시됩니다."](#) .

AD FS MFA 메타데이터 업데이트

업그레이드, CA 인증서 갱신, DR 등 AD FS 서버에 수정 사항이 있을 때마다 SnapCenter 에서 AD FS MFA 메타데이터를 업데이트해야 합니다.

단계

1. AD FS 페더레이션 메타데이터 파일을 다운로드합니다. "<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>"
2. 다운로드한 파일을 SnapCenter 서버에 복사하여 MFA 구성을 업데이트합니다.
3. 다음 cmdlet을 실행하여 SnapCenter 에서 AD FS 메타데이터를 업데이트합니다.

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성화된 세션 쿠키를 지우고 다시 로그인하세요.

SnapCenter MFA 메타데이터 업데이트

ADFS 서버에 복구, CA 인증서 갱신, DR 등 수정 사항이 있을 때마다 AD FS에서 SnapCenter MFA 메타데이터를 업데이트해야 합니다.

단계

1. AD FS 호스트에서 AD FS 관리 마법사를 열고 다음 단계를 수행합니다.
 - a. *신뢰 당사자 트러스트*를 선택하세요.
 - b. SnapCenter 에 대해 생성된 신뢰 당사자 트러스트를 마우스 오른쪽 버튼으로 클릭하고 *삭제*를 선택합니다.

신뢰 당사자 신뢰의 사용자 정의 이름이 표시됩니다.

- c. 다중 요소 인증(MFA)을 활성화합니다.

보다 ["다중 요소 인증 활성화"](#) .

2. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성화된 세션 쿠키를 지우고 다시 로그인하세요.

다중 요소 인증(MFA) 비활성화

단계

1. MFA를 비활성화하고 MFA가 활성화되었을 때 생성된 구성 파일을 정리합니다. Set-

SmMultiFactorAuthentication cmdlet.

2. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성화된 세션 쿠키를 지우고 다시 로그인하세요.

Rest API, PowerShell 및 SCCLI를 사용하여 다중 인증 요소(MFA) 관리

MFA 로그인은 브라우저, REST API, PowerShell 및 SCCLI에서 지원됩니다. MFA는 AD FS ID 관리자를 통해 지원됩니다. GUI, REST API, PowerShell 및 SCCLI에서 MFA를 활성화, 비활성화하고 MFA를 구성할 수 있습니다.

AD FS를 OAuth/OIDC로 설정

Windows GUI 마법사를 사용하여 AD FS 구성

1. 서버 관리자 대시보드 > 도구 > *ADFS 관리*로 이동합니다.
2. **ADFS** > *응용 프로그램 그룹*으로 이동합니다.
 - a. *응용 프로그램 그룹*을 마우스 오른쪽 버튼으로 클릭합니다.
 - b. *애플리케이션 그룹 추가*를 선택하고 *애플리케이션 이름*을 입력합니다.
 - c. *서버 애플리케이션*을 선택하세요.
 - d. *다음*을 클릭하세요.
3. *클라이언트 식별자*를 복사하세요.

이것은 클라이언트 ID입니다. .. 리디렉트 URL에 콜백 URL(SnapCenter 서버 URL)을 추가합니다. ... *다음*을 클릭하세요.

4. *공유 비밀 생성*을 선택하세요.

비밀 값을 복사합니다. 이것은 고객의 비밀입니다. ... *다음*을 클릭하세요.

5. 요약 페이지에서 *다음*을 클릭합니다.
 - a. 완료 페이지에서 *닫기*를 클릭합니다.
6. 새로 추가된 *응용 프로그램 그룹*을 마우스 오른쪽 버튼으로 클릭하고 *속성*을 선택합니다.
7. 앱 속성에서 *애플리케이션 추가*를 선택합니다.
8. *애플리케이션 추가*를 클릭하세요.

웹 API를 선택하고 *다음*을 클릭합니다.

9. 웹 API 구성 페이지에서 이전 단계에서 만든 SnapCenter 서버 URL과 클라이언트 식별자를 식별자 섹션에 입력합니다.
 - a. *추가*를 클릭하세요.
 - b. *다음*을 클릭하세요.

10. 액세스 제어 정책 선택 페이지에서 요구 사항에 따라 제어 정책을 선택합니다(예: 모든 사람 허용 및 MFA 요구) 그리고 *다음*을 클릭합니다.
11. 애플리케이션 권한 구성 페이지에서 기본적으로 openid가 범위로 선택되어 있으므로 *다음*을 클릭합니다.

12. 요약 페이지에서 *다음*을 클릭합니다.

완료 페이지에서 *닫기*를 클릭합니다.

13. 샘플 애플리케이션 속성 페이지에서 *확인*을 클릭합니다.

14. 권한 부여 서버(AD FS)에서 발행하고 리소스에서 사용하도록 의도된 JWT 토큰입니다.

이 토큰의 'aud' 또는 청중 클레임은 리소스 또는 웹 API의 식별자와 일치해야 합니다.

15. 선택한 WebAPI를 편집하고 콜백 URL(SnapCenter 서버 URL)과 클라이언트 식별자가 올바르게 추가되었는지 확인하세요.

OpenID Connect를 구성하여 사용자 이름을 클레임으로 제공합니다.

16. 서버 관리자의 오른쪽 상단에 있는 도구 메뉴 아래에 있는 **AD FS** 관리 도구를 엽니다.

a. 왼쪽 사이드바에서 애플리케이션 그룹 폴더를 선택합니다.

b. 웹 API를 선택하고 *편집*을 클릭합니다.

c. 발급 변환 규칙 탭으로 이동

17. *규칙 추가*를 클릭합니다.

a. 클레임 규칙 템플릿 드롭다운에서 *LDAP 속성을 클레임으로 보내기*를 선택합니다.

b. *다음*을 클릭하세요.

18. 청구 규칙 이름을 입력하세요.

a. 속성 저장소 드롭다운에서 *Active Directory*를 선택합니다.

b. **LDAP** 속성 드롭다운에서 사용자 주체 이름*을 선택하고 *송신 클레임 유형 드롭다운에서 *UPN*을 선택합니다.

c. *마침*을 클릭하세요.

PowerShell 명령을 사용하여 애플리케이션 그룹 만들기

PowerShell 명령을 사용하여 애플리케이션 그룹과 웹 API를 만들고 범위와 클레임을 추가할 수 있습니다. 이러한 명령은 자동화된 스크립트 형식으로 제공됩니다. 자세한 내용은 <KB 문서 링크>를 참조하세요.

1. 다음 명령을 사용하여 AD FS에서 새 애플리케이션 그룹을 만듭니다.

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier  
-ApplicationGroupIdentifier $ClientRoleIdentifier
```

`ClientRoleIdentifier` 귀하의 애플리케이션 그룹 이름

`redirectURL` 승인 후 리디렉션을 위한 유효한 URL

2. AD FS 서버 애플리케이션을 만들고 클라이언트 비밀번호를 생성합니다.

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"  
-ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL  
-Identifier $identifier -GenerateClientSecret
```

3. ADFS 웹 API 애플리케이션을 만들고 사용해야 하는 정책 이름을 구성합니다.

```
$identifier = (New-Guid).Guid

Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
-Name "App Web API"

-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

4. 다음 명령의 출력에서 클라이언트 ID와 클라이언트 비밀번호를 얻으세요. 이는 한 번만 표시됩니다.

```
"client_id = $identifier"

"client_secret: $($ADFSApp.ClientSecret)"
```

5. AD FS 애플리케이션에 allatclaims 및 openid 권한을 부여합니다.

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
-ServerRoleIdentifier $identifier -ScopeNames @('openid')

$transformrule = @"

@RuleTemplate = "LdapClaims"

@RuleName = "AD User properties and Groups"

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer ==
"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. 변환 규칙 파일을 작성합니다.

```
$transformrule | Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii
$relativePath = Get-Item .\issueancetransformrules.tmp
```

7. 외부 파일을 사용하여 웹 API 애플리케이션의 이름을 지정하고 발급 변환 규칙을 정의합니다.

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

PowerShell 명령을 사용하여 액세스 토큰 만료 시간을 업데이트할 수 있습니다.

이 작업에 관하여

- 액세스 토큰은 사용자, 클라이언트, 리소스의 특정 조합에만 사용할 수 있습니다. 액세스 토큰은 취소할 수 없으며 만료일까지 유효합니다.
- 기본적으로 액세스 토큰의 만료 시간은 60분입니다. 이 최소 만료 시간은 충분하고 확장 가능합니다. 진행 중인 비즈니스에 중요한 작업을 피하기 위해 충분한 가치를 제공해야 합니다.

단계

애플리케이션 그룹 WebApi에 대한 액세스 토큰 만료 시간을 업데이트하려면 AD FS 서버에서 다음 명령을 사용합니다.

```
+
Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"
```

AD FS에서 베어러 토큰 가져오기

REST 클라이언트(예: Postman)에서 아래에 언급된 매개변수를 입력하면 사용자 자격 증명을 입력하라는 메시지가 표시됩니다. 또한, 소지자 토큰을 받으려면 2차 인증(본인이 소유한 것 및 본인인 것)을 입력해야 합니다.

+ 베어러 토큰의 유효성은 애플리케이션별로 AD FS 서버에서 구성할 수 있으며 기본 유효 기간은 60분입니다.

필드	가치
보조금 유형	승인 코드
콜백 URL	콜백 URL이 없으면 애플리케이션의 기본 URL을 입력하세요.
인증 URL	[adfs-도메인-이름]/adfs/oauth2/authorize
액세스 토큰 URL	[adfs-도메인-이름]/adfs/oauth2/토큰
클라이언트 ID	AD FS 클라이언트 ID를 입력하세요
클라이언트 비밀번호	AD FS 클라이언트 비밀번호를 입력하세요
범위	오픈아이디
클라이언트 인증	기본 AUTH 헤더로 보내기
의지	고급 옵션 탭에서 JWT 토큰의 "aud" 값으로 제공되는 콜백 URL과 동일한 값을 가진 리소스 필드를 추가합니다.

PowerShell, SCCLI 및 REST API를 사용하여 SnapCenter 서버에서 MFA 구성

PowerShell, SCCLI 및 REST API를 사용하여 SnapCenter 서버에서 MFA를 구성할 수 있습니다.

SnapCenter MFA CLI 인증

PowerShell과 SCCLI에서 기존 cmdlet(`Open-SmConnection`)은 사용자를 인증하기 위해 전달자 토큰을 사용하기 위해 "AccessToken"이라는 필드가 하나 더 확장되었습니다.

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port <String>] [-RoleName <String>] [-AccessToken <string>]
```

위의 cmdlet을 실행한 후 해당 사용자가 추가 SnapCenter cmdlet을 실행할 수 있는 세션이 생성됩니다.

SnapCenter MFA REST API 인증

REST API 클라이언트(Postman이나 Swagger 등)에서 *Authorization=Bearer* <액세스 토큰> 형식의 베어러 토큰을 사용하고 헤더에 사용자 RoleName을 언급하면 SnapCenter 에서 성공적인 응답을 받을 수 있습니다.

MFA Rest API 워크플로

MFA가 AD FS로 구성된 경우 Rest API를 통해 SnapCenter 애플리케이션에 액세스하려면 액세스(베어러) 토큰을 사용하여 인증해야 합니다.

이 작업에 관하여

- Postman, Swagger UI 또는 FireCamp와 같은 REST 클라이언트를 사용할 수 있습니다.
- 액세스 토큰을 받아서 이후 요청(SnapCenter Rest API)을 인증하여 모든 작업을 수행합니다.

단계

AD FS MFA를 통해 인증하려면

1. 액세스 토큰을 가져오기 위해 AD FS 엔드포인트를 호출하도록 REST 클라이언트를 구성합니다.

애플리케이션에 대한 액세스 토큰을 받기 위해 버튼을 누르면 AD FS SSO 페이지로 리디렉션되며, 이 페이지에서 AD 자격 증명을 제공하고 MFA로 인증해야 합니다. 1. AD FS SSO 페이지에서 사용자 이름 텍스트 상자에 사용자 이름이나 이메일을 입력합니다.

+ 사용자 이름은 user@domain 또는 domain\user 형식이어야 합니다.

2. 비밀번호 텍스트 상자에 비밀번호를 입력하세요.
3. *로그인*을 클릭하세요.
4. 로그인 옵션 섹션에서 인증 옵션을 선택하고 인증합니다(구성에 따라 다름).
 - 푸시: 휴대폰으로 전송되는 푸시 알림을 승인합니다.
 - QR 코드: AUTH Point 모바일 앱을 사용하여 QR 코드를 스캔한 다음 앱에 표시된 확인 코드를 입력하세요.
 - 일회용 비밀번호: 토큰의 일회용 비밀번호를 입력하세요.
5. 인증에 성공하면 액세스 토큰, ID 토큰, 새로 고침 토큰이 포함된 팝업이 열립니다.

액세스 토큰을 복사하여 SnapCenter Rest API에서 사용하여 작업을 수행합니다.

6. Rest API에서는 헤더 섹션에 액세스 토큰과 역할 이름을 전달해야 합니다.
7. SnapCenter AD FS에서 이 액세스 토큰의 유효성을 검사합니다.

유효한 토큰이면 SnapCenter 이를 디코딩하여 사용자 이름을 가져옵니다.

8. SnapCenter 사용자 이름과 역할 이름을 사용하여 API 실행을 위해 사용자를 인증합니다.

인증에 성공하면 SnapCenter 결과를 반환하고, 그렇지 않으면 오류 메시지가 표시됩니다.

Rest API, CLI 및 GUI에 대한 SnapCenter MFA 기능 활성화 또는 비활성화

GUI

단계

1. SnapCenter 관리자로 SnapCenter 서버에 로그인합니다.
2. 설정 > 전역 설정 > *다중 인증(MFA) 설정*을 클릭합니다.
3. MFA 로그인을 활성화하거나 비활성화하려면 인터페이스(GUI/RST API/CLI)를 선택하세요.

PowerShell 인터페이스

단계

1. GUI, Rest API, PowerShell 및 SCCLI에 대해 MFA를 활성화하려면 PowerShell 또는 CLI 명령을 실행합니다.

```
Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled  
-IsCliMFAEnabled -Path
```

경로 매개 변수는 AD FS MFA 메타데이터 xml 파일의 위치를 지정합니다.

지정된 AD FS 메타데이터 파일 경로로 구성된 SnapCenter GUI, Rest API, PowerShell 및 SCCLI에 대해 MFA를 활성화합니다.

2. 다음을 사용하여 MFA 구성 상태 및 설정을 확인하세요. `Get-SmMultiFactorAuthentication cmdlet`.

SCCLI 인터페이스

단계

1. # `sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path "C:\ADFS_metadata\abc.xml"`
2. # `sccli Get-SmMultiFactorAuthentication`

REST API

1. GUI, REST API, PowerShell 및 SCCLI에 대한 MFA를 활성화하기 위해 다음 게시물 API를 실행합니다.

매개변수	가치
요청된 URL	/api/4.9/설정/다중 인증
HTTP 메서드	우편
요청 본문	{ "IsGuiMFAEnabled": 거짓, "IsRestApiMFAEnabled": 참, "IsCliMFAEnabled": 거짓, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml" }
대응 기관	{ "MFAConfiguration": { "IsGuiMFAEnabled": 거짓, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": 널, "IsRestApiMFAEnabled": 참, "IsCliMFAEnabled": 거짓, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

2. 다음 API를 사용하여 MFA 구성 상태와 설정을 확인하세요.

매개변수	가치
요청된 URL	/api/4.9/설정/다중 인증
HTTP 메서드	얻다
대응 기관	{ "MFAConfiguration": { "IsGuiMFAEnabled": 거짓, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": 널, "IsRestApiMFAEnabled": 참, "IsCliMFAEnabled": 거짓, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

SnapCenter 서버 설치

Windows 호스트에 SnapCenter 서버 설치

SnapCenter Server 설치 프로그램 실행 파일을 실행하여 SnapCenter Server를 설치할 수 있습니다.

PowerShell cmdlet을 사용하여 여러 설치 및 구성 절차를 선택적으로 수행할 수 있습니다. PowerShell 7.4.2 이상을 사용해야 합니다.



명령줄에서 SnapCenter 서버를 자동으로 설치하는 것은 지원되지 않습니다.

시작하기 전에

- SnapCenter 서버 호스트는 보류 중인 시스템 재시작 없이 Windows 업데이트로 최신 상태를 유지해야 합니다.
- SnapCenter 서버를 설치하려는 호스트에 MySQL 서버가 설치되어 있지 않은지 확인해야 합니다.
- Windows 설치 프로그램 디버깅을 활성화해야 합니다.

활성화에 대한 정보는 Microsoft 웹 사이트를 참조하세요. "[Windows 설치 프로그램 로깅](#)".



Microsoft Exchange Server, Active Directory 또는 도메인 이름 서버가 있는 호스트에 SnapCenter 서버를 설치해서는 안 됩니다.

단계

1. SnapCenter 서버 설치 패키지를 다운로드하세요. "[NetApp 지원 사이트](#)".
2. 다운로드한 .exe 파일을 두 번 클릭하여 SnapCenter 서버 설치를 시작합니다.

설치를 시작하면 모든 사전 검사가 수행되고 최소 요구 사항을 충족하지 못하면 해당 오류나 경고 메시지가 표시됩니다.

경고 메시지를 무시하고 설치를 진행할 수 있습니다. 그러나 오류는 수정되어야 합니다.

3. SnapCenter 서버 설치에 필요한 미리 채워진 값을 검토하고 필요한 경우 수정합니다.

MySQL 서버 저장소 데이터베이스에 대한 비밀번호를 지정할 필요는 없습니다. SnapCenter 서버를 설치하는 동안 비밀번호가 자동으로 생성됩니다.



특수문자 "%" is not supported in the custom path for the repository database. If you include "" 경로에 %`가 있으면 설치가 실패합니다.

4. *지금 설치*를 클릭하세요.

잘못된 값을 지정한 경우 해당 오류 메시지가 표시됩니다. 값을 다시 입력한 다음 설치를 시작하세요.



취소 버튼을 클릭하면 실행 중인 단계가 완료되고, 이후 롤백 작업이 시작됩니다. SnapCenter 서버가 호스트에서 완전히 제거됩니다.

하지만 "SnapCenter 서버 사이트 재시작" 또는 " SnapCenter 서버 시작 대기" 작업이 수행되는 동안 *취소*를 클릭하면 작업을 취소하지 않고 설치가 진행됩니다.

로그 파일은 항상 관리자의 %temp% 폴더에 (가장 오래된 것부터) 나열됩니다. 로그 위치를 리디렉션하려면 명령 프롬프트에서 다음을 실행하여 SnapCenter 서버 설치를 시작하세요

```
.C:\installer_location\installer_name.exe /log"C:\\"
```

설치 중 Windows 호스트에서 활성화된 기능

SnapCenter 서버 설치 프로그램은 설치 중에 Windows 호스트에서 Windows 기능과 역할을 활성화합니다. 이러한 정보는 호스트 시스템의 문제 해결 및 유지 관리에 도움이 될 수 있습니다.

범주	특징
웹 서버	• 인터넷 정보 서비스 • 월드 와이드 웹 서비스 • 일반적인 HTTP 기능 ◦ 기본 문서 ◦ 디렉토리 탐색 ◦ HTTP 오류 ◦ HTTP 리디렉션 ◦ 정적 콘텐츠 ◦ WebDAV 게시 • 건강 및 진단 ◦ 사용자 정의 로깅 ◦ HTTP 로깅 ◦ 로깅 도구 ◦ 요청 모니터 ◦ 트레이싱 • 성능 특징 ◦ 정적 콘텐츠 압축 • 보안 ◦ IP 보안 ◦ 기본 인증 ◦ 중앙 집중식 SSL 인증서 지원 ◦ 클라이언트 인증서 매핑 인증 ◦ IIS 클라이언트 인증서 매핑 인증 ◦ IP 및 도메인 제한 ◦ 요청 필터링 ◦ URL 인증 ◦ Windows 인증 • 애플리케이션 개발 기능 ◦ .NET 확장성 4.5 ◦ 애플리케이션 초기화 ◦ ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 ◦ 서버 측 포함 ◦ 웹소켓 프로토콜 관리 도구

범주	특징
IIS 관리 스크립트 및 도구	• IIS 관리 서비스 • 웹 관리 도구
.NET Framework 8.0.12 기능	• ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 • Windows Communication Foundation(WCF) HTTP 활성화⁴⁵ ◦ TCP 활성화 ◦ HTTP 활성화
Windows 프로세스 활성화 서비스	프로세스 모델
구성 API	모두

Linux 호스트에 SnapCenter 서버 설치

SnapCenter Server 설치 프로그램 실행 파일을 실행하여 SnapCenter Server를 설치할 수 있습니다.

시작하기 전에

- SnapCenter 설치할 권한이 없는 루트가 아닌 사용자를 사용하여 SnapCenter 서버를 설치하려는 경우 NetApp 지원 사이트에서 sudoers 체크섬 파일을 받으세요. Linux 버전에 따라 적절한 체크섬 파일을 사용해야 합니다.
- SUSE Linux에서 sudo 패키지를 사용할 수 없는 경우 인증 실패를 방지하기 위해 sudo 패키지를 설치하세요.
- SUSE Linux의 경우 설치 실패를 방지하려면 호스트 이름을 구성하세요.
- 명령을 실행하여 보안 Linux 상태를 확인하세요. `sestatus`. `_SELinux` 상태가 "활성화"이고 `_현재 모드`가 "강제"인 경우 다음을 수행합니다.

- 다음 명령을 실행합니다: `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT>`

`_WEBAPP_EXTERNAL_PORT`의 기본값은 8146입니다.

- 방화벽이 포트를 차단하는 경우 다음을 실행하세요. `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT>/tcp`

`_WEBAPP_EXTERNAL_PORT`의 기본값은 8146입니다.

- 읽기 및 쓰기 권한이 있는 디렉토리에서 다음 명령을 실행하세요.

```
▪ sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx
```

명령이 "할 일 없음"을 반환하는 경우 SnapCenter Server를 설치한 후 명령을 다시 실행합니다.

- 명령이 `_my-nginx.pp`를 생성하는 경우, 명령을 실행하여 정책 패키지를 활성화합니다. `sudo`

```
semodule -i my-nginx.pp
```

- MySQL PID 디렉토리에 사용되는 경로는 `_var/opt/mysqld_`입니다. MySQL 설치에 대한 권한을 설정하려면 다음 명령을 실행하세요.

```
▪ mkdir /var/opt/mysqld
▪ sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"
▪ sudo restorecon -Rv /var/opt/mysqld
```

- MySQL 데이터 디렉토리에 사용된 경로는 `_INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/`입니다. MySQL 데이터 디렉토리에 대한 권한을 설정하려면 다음 명령을 실행하세요.

```
▪ mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL
▪ sudo semanage fcontext -a -t mysqld_db_t
  "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"
▪ sudo restorecon -Rv
  /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL
```

이 작업에 관하여

- SnapCenter Server가 Linux 호스트에 설치되면 MySQL, RabbitMq, ErLANG과 같은 타사 서비스가 설치됩니다. 이러한 프로그램을 제거해서는 안 됩니다.
- Linux 호스트에 설치된 SnapCenter 서버는 다음을 지원하지 않습니다.
 - 고가용성
 - Windows 플러그인
 - Active Directory(로컬 사용자만 지원, 루트 및 자격 증명이 있는 비 루트 사용자 모두)
 - SnapCenter 에 로그인하기 위한 키 기반 인증
- .NET 런타임을 설치하는 동안 *libicu* 라이브러리의 종속성을 해결하지 못하는 경우 다음 명령을 실행하여 `_libicu_`를 설치하세요. `yum install -y libicu`
- `_Perl_`을 사용할 수 없어 SnapCenter Server 설치에 실패하는 경우, 다음 명령을 실행하여 `_Perl_`을 설치하세요. `yum install -y perl`

단계

1. 다음을 다운로드하세요 "[NetApp 지원 사이트](#)" `_홈 디렉토리_`로.
 - SnapCenter 서버 설치 패키지 - **snapcenter-linux-server-(el8/el9/sles15).bin**
 - 공개 키 파일 - **snapcenter_public_key.pub**
 - 해당 서명 파일 - **snapcenter-linux-server-(el8/el9/sles15).bin.sig**
2. 서명 파일을 검증합니다.

```
$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>
```
3. 루트가 아닌 사용자로 설치하는 경우, .bin 설치 프로그램과 함께 제공되는 `*snapcenter_server_checksum_(el8/el9/sles15).txt*`에 지정된 visudo 콘텐츠를 추가합니다.
4. .bin 설치 프로그램에 실행 권한을 할당합니다.

```
chmod +x snapcenter-linux-server-(el8/el9/sles15).bin
```

5. SnapCenter Server를 설치하려면 다음 작업 중 하나를 수행하세요.

공연을 하고 싶다면...	이렇게 하세요...
대화형 설치	<code>./snapcenter-linux-server-(el8/el9/sles15).bin</code> 다음 세부 정보를 입력하라는 메시지가 표시됩니다. • Linux 호스트 외부에서 SnapCenter 서버에 액세스하는 데 사용되는 웹앱 외부 포트입니다. 기본값은 8146입니다. • SnapCenter Server를 설치할 SnapCenter Server 사용자입니다. • 패키지가 설치될 설치 디렉토리입니다.

공연을 하고 싶다면...	이렇게 하세요...
비대화형 설치	<pre> sudo ./snapcenter-linux-server- (e18/e19/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename> </pre> 예: <code>sudo ./snapcenter_linux_server.bin -i silent</code> <code>-DWEBAPP_EXTERNAL_PORT=8146</code> <code>-DSNAPCENTER_SERVER_USER=root</code> <code>-DUSER_INSTALL_DIR=/opt</code> <code>-DINSTALL_LOG_NAME=InstallerLog.log</code> 로그는 <code>_var/opt/snapcenter/logs_</code>에 저장됩니다. SnapCenter Server를 설치하기 위해 전달해야 하는 매개변수: • <code>DWEBAPP_EXTERNAL_PORT</code>: Linux 호스트 외부에서 SnapCenter 서버에 액세스하는 데 사용되는 웹앱 외부 포트입니다. 기본값은 8146입니다. • <code>DWEBAPP_INTERNAL_PORT</code>: Linux 호스트 내에서 SnapCenter 서버에 액세스하는 데 사용되는 웹앱 내부 포트입니다. 기본값은 8147입니다. • <code>DSMCORE_PORT</code>: smcore 서비스가 실행되는 SMCORE 포트입니다. 기본값은 8145입니다. • <code>DSCHEDULER_PORT</code>: 스케줄러 서비스가 실행되는 스케줄러 포트입니다. 기본값은 8154입니다. • <code>DSNAPCENTER_SERVER_USER</code>: SnapCenter Server를 설치할 SnapCenter Server 사용자입니다. <code>_DSNAPCENTER_SERVER_USER_</code>의 경우 기본값은 설치 프로그램을 실행하는 사용자입니다. • <code>DUSER_INSTALL_DIR</code>: 패키지가 설치될 설치 디렉토리입니다. <code>_DUSER_INSTALL_DIR_</code>의 경우 기본 설치 디렉토리는 <code>_opt_</code>입니다. • <code>DINSTALL_LOG_NAME</code>: 설치 로그가 저장될 로그 파일 이름입니다. 이것은 선택적인 매개변수이며, 지정하면 콘솔에 로그가 표시되지 않습니다. 이 매개변수를 지정하지 않으면 로그가 콘솔에 표시되고 기본 로그 파일에도 저장됩니다. • <code>DSELINUX</code>: <code>_SELinux_</code> 상태가 "활성화됨"이고, <code>_현재 모드_</code>가 "강제 실행"이며, 시작하기 전 섹션을 언급된 명령을 실행한 경우 이 매개변수를 지정하고 값을 1로 할당해야 합니다. 기본값은 0입니다.

다음은 무엇인가요?

- `_SELinux` 상태가 "활성화"이고 `_현재 모드`가 "강제"인 경우 `nginx` 서비스가 시작되지 않습니다. 다음 명령을 실행해야 합니다.
a. 홈 디렉토리로 이동합니다.
b. 다음 명령을 실행합니다: `journalctl -x|grep nginx.`
c. Webapp 내부 포트(8147)에서 수신이 허용되지 않으면 다음 명령을 실행하세요.
 - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
 - `semodule -i my-nginx.pp`
d. 달리다 `setsebool -P httpd_can_network_connect on`

설치 중 **Linux** 호스트에서 활성화된 기능

SnapCenter 서버는 호스트 시스템의 문제 해결 및 유지 관리에 도움이 되는 아래 소프트웨어 패키지를 설치합니다.

- 래빗앰큐
- 얼랑

SnapCenter 등록

NetApp 제품을 처음 사용하고 기존 NetApp 계정이 없는 경우 SnapCenter 등록하여 지원을 받아야 합니다.

단계

1. SnapCenter 설치한 후 *도움말 > 정보*로 이동합니다.
2. *SnapCenter* 정보 대화 상자에서 971로 시작하는 20자리 숫자인 SnapCenter 인스턴스를 기록해 둡니다.
3. 딸깍 하는 소리 <https://register.netapp.com>.
4. *저는 등록된 NetApp 고객이 아닙니다*를 클릭하세요.
5. 등록하려면 세부 정보를 입력하세요.
6. NetApp 참조 SN 필드를 비워 두세요.
7. 제품 라인 드롭다운에서 * SnapCenter*를 선택합니다.
8. 청구 제공자를 선택하세요.
9. 20자리 SnapCenter 인스턴스 ID를 입력하세요.
10. *제출*을 클릭하세요.

RBAC 인증을 사용하여 **SnapCenter** 에 로그인합니다.

SnapCenter 역할 기반 액세스 제어(RBAC)를 지원합니다. SnapCenter 관리자는 SnapCenter RBAC를 통해 작업 그룹이나 Active Directory의 사용자, 또는 Active Directory의 그룹에 역할과 리소스를 할당합니다. 이제 RBAC 사용자는 할당된 역할로 SnapCenter 에 로그인할 수 있습니다.

시작하기 전에

- Windows Server Manager에서 Windows Process Activation Service(WAS)를 활성화해야 합니다.
- SnapCenter 서버에 로그인하기 위해 Internet Explorer를 브라우저로 사용하려면 Internet Explorer의 보호 모드가 비활성화되어 있는지 확인해야 합니다.
- SnapCenter 서버가 Linux 호스트에 설치된 경우 SnapCenter 서버를 설치하는 데 사용된 사용자 계정을 사용하여 로그인해야 합니다.

이 작업에 관하여

SnapCenter 서버 설치 마법사는 설치하는 동안 바로 가기를 만들어 SnapCenter 설치된 호스트의 바탕 화면과 시작 메뉴에 놓습니다. 또한, 설치가 끝나면 설치 마법사가 설치 중에 제공한 정보를 기반으로 SnapCenter URL을 표시합니다. 원격 시스템에서 로그인하려는 경우 이 URL을 복사할 수 있습니다.



웹 브라우저에 여러 개의 탭이 열려 있는 경우 SnapCenter 브라우저 탭만 닫아도 SnapCenter 에서 로그아웃되지 않습니다. SnapCenter 와의 연결을 종료하려면 로그아웃 버튼을 클릭하거나 웹 브라우저 전체를 닫아 SnapCenter 에서 로그아웃해야 합니다.

모범 사례: 보안상의 이유로 브라우저에서 SnapCenter 비밀번호를 저장하지 않도록 설정하는 것이 좋습니다.

기본 GUI URL은 SnapCenter 서버가 설치된 서버의 기본 포트 8146(<https://server:8146>)에 대한 보안 연결입니다. SnapCenter 설치 중에 다른 서버 포트를 제공한 경우 해당 포트가 대신 사용됩니다.

고가용성(HA) 배포의 경우 가상 클러스터 IP [_https://Virtual_Cluster_IP_or_FQDN:8146_](https://Virtual_Cluster_IP_or_FQDN:8146)을 사용하여 SnapCenter 액세스해야 합니다. Internet Explorer(IE)에서 [_https://Virtual_Cluster_IP_or_FQDN:8146_](https://Virtual_Cluster_IP_or_FQDN:8146)으로 이동할 때 SnapCenter UI가 보이지 않으면 각 플러그인 호스트의 IE에서 가상 클러스터 IP 주소 또는 FQDN을 신뢰할 수 있는 사이트로 추가하거나 각 플러그인 호스트에서 IE 강화 보안을 비활성화해야 합니다. 자세한 내용은 다음을 참조하세요. ["외부 네트워크에서 클러스터 IP 주소에 액세스할 수 없습니다."](#)

SnapCenter GUI를 사용하는 것 외에도 PowerShell cmdlet을 사용하여 구성, 백업 및 복원 작업을 수행하는 스크립트를 만들 수 있습니다. 일부 cmdlet은 SnapCenter 출시될 때마다 변경되었을 수 있습니다. 그만큼 ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#) 자세한 내용을 알고 있습니다.



처음으로 SnapCenter 에 로그인하는 경우 설치 과정에서 제공한 자격 증명을 사용하여 로그인해야 합니다.

단계

1. 로컬 호스트 데스크톱에 있는 바로가기에서 SnapCenter 실행하거나, 설치가 끝날 때 제공된 URL에서 실행하거나, SnapCenter 관리자가 제공한 URL에서 실행하세요.
2. 사용자 자격 증명을 입력하세요.

다음 중 하나를 지정하려면...	다음 형식 중 하나를 사용하세요.
도메인 관리자	• NetBIOS\사용자 이름 • 사용자 이름@UPN 접미사 예를 들어, username@netapp.com • 도메인 FQDN\사용자 이름
지역 관리자	사용자 이름

3. 두 개 이상의 역할이 할당된 경우 역할 상자에서 이 로그인 세션에 사용할 역할을 선택합니다.

SnapCenter 에 로그인하면 현재 사용자와 관련 역할이 오른쪽 상단에 표시됩니다.

결과

대시보드 페이지가 표시됩니다.

사이트에 접속할 수 없다는 오류로 로깅이 실패하는 경우 SSL 인증서를 SnapCenter 에 매핑해야 합니다. ["자세히 알아보기"](#)

끝난 후

RBAC 사용자로 SnapCenter 서버에 처음 로그인한 후 리소스 목록을 새로 고칩니다.

SnapCenter 지원해야 할 신뢰할 수 없는 Active Directory 도메인이 있는 경우, 신뢰할 수 없는 도메인의 사용자 역할을 구성하기 전에 SnapCenter 에 해당 도메인을 등록해야 합니다. ["자세히 알아보기"](#).

Linux 호스트에서 실행되는 SnapCenter 에 플러그인 호스트를 추가하려면 `/opt/NetApp/snapcenter/SnapManagerWeb/Repository` 위치에서 체크섬 파일을 가져와야 합니다.

6.0 릴리스부터 SnapCenter PowerShell 바로 가기가 바탕 화면에 생성됩니다. 바로가기를 사용하여 SnapCenter PowerShell cmdlet에 직접 액세스할 수 있습니다.

다중 인증 요소(MFA)를 사용하여 **SnapCenter** 에 로그인하세요

SnapCenter Server는 Active Directory의 일부인 도메인 계정에 대한 MFA를 지원합니다.

시작하기 전에

MFA를 활성화했어야 합니다. MFA를 활성화하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["다중 요소 인증 활성화"](#)

이 작업에 관하여

- FQDN만 지원됩니다.
- 작업 그룹 및 크로스 도메인 사용자는 MFA를 사용하여 로그인할 수 없습니다.

단계

1. 로컬 호스트 데스크톱에 있는 바로가기에서 SnapCenter 실행하거나, 설치가 끝날 때 제공된 URL에서 실행하거나, SnapCenter 관리자가 제공한 URL에서 실행하세요.
2. AD FS 로그인 페이지에서 사용자 이름과 비밀번호를 입력합니다.

AD FS 페이지에 사용자 이름 또는 비밀번호가 올바르지 않다는 오류 메시지가 표시되면 다음 사항을 확인해야 합니다.

- 사용자 이름이나 비밀번호가 유효한지 여부
- 사용자 계정은 Active Directory(AD)에 있어야 합니다.
- AD에 설정된 허용된 최대 시도 횟수를 초과했는지 여부
- AD와 AD FS가 작동 중인지 여부

SnapCenter 기본 GUI 세션 시간 초과 수정

SnapCenter GUI 세션 시간 초과 기간을 기본 시간 초과 기간인 20분보다 짧게 또는 길게 수정할 수 있습니다.

보안 기능으로, SnapCenter 기본적으로 15분 동안 활동이 없으면 5분 후에 GUI 세션에서 로그아웃된다는 경고를 표시합니다. 기본적으로 SnapCenter 20분 동안 아무런 활동이 없으면 GUI 세션에서 로그아웃되며, 다시 로그인해야 합니다.

단계

1. 왼쪽 탐색 창에서 설정 > *전역 설정*을 클릭합니다.
2. 글로벌 설정 페이지에서 *구성 설정*을 클릭합니다.
3. 세션 시간 초과 필드에 새 세션 시간 초과를 분 단위로 입력한 다음 *저장*을 클릭합니다.

SSL 3.0을 비활성화하여 SnapCenter 웹 서버를 보호하세요.

보안을 위해 SnapCenter 웹 서버에서 SSL(Secure Socket Layer) 3.0 프로토콜이 활성화된 경우 Microsoft IIS에서 해당 프로토콜을 비활성화해야 합니다.

SSL 3.0 프로토콜에는 공격자가 연결 실패를 유발하거나 중간자 공격을 수행하여 웹사이트와 방문자 간의 암호화 트래픽을 관찰하는 데 사용할 수 있는 결함이 있습니다.

단계

1. SnapCenter 웹 서버 호스트에서 레지스트리 편집기를 시작하려면 시작 > *실행*을 클릭한 다음 regedit를 입력합니다.
2. 레지스트리 편집기에서
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\으로 이동합니다.
 - 서버 키가 이미 존재하는 경우:
 - i. 활성화된 DWORD를 선택한 다음 편집 > *수정*을 클릭합니다.
 - ii. 값을 0으로 변경한 다음 *확인*을 클릭합니다.
 - 서버 키가 존재하지 않는 경우:

- i. 편집 > 새로 만들기 > *키*를 클릭한 다음 키 이름을 Server로 지정합니다.
- ii. 새로운 서버 키를 선택한 후 편집 > 새로 만들기 > *DWORD*를 클릭합니다.
- iii. 새 DWORD 이름을 Enabled로 지정한 다음 값으로 0을 입력합니다.

3. 레지스트리 편집기를 닫습니다.

SnapCenter 서버 구성

스토리지 시스템 추가 및 프로비저닝

스토리지 시스템 추가

SnapCenter ONTAP 스토리지, ASA r2 시스템 또는 Amazon FSx for NetApp ONTAP 에 액세스하여 데이터 보호 및 프로비저닝 작업을 수행할 수 있도록 스토리지 시스템을 설정해야 합니다.

독립형 SVM을 추가하거나 여러 SVM으로 구성된 클러스터를 추가할 수 있습니다. Amazon FSx for NetApp ONTAP 사용하는 경우 fsxadmin 계정을 사용하여 여러 SVM으로 구성된 FSx 관리 LIF를 추가하거나 SnapCenter 에 FSx SVM을 추가할 수 있습니다.

시작하기 전에

- 저장소 연결을 생성하려면 인프라 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

스토리지 시스템 연결을 추가하는 동안에는 호스트 플러그인 설치가 진행 중이어서는 안 됩니다. 호스트 캐시가 업데이트되지 않고 SnapCenter GUI에 데이터베이스 상태가 “백업에 사용할 수 없음” 또는 “ NetApp 스토리지에 없음”으로 표시될 수 있기 때문입니다.

- 저장 시스템 이름은 고유해야 합니다.

SnapCenter 서로 다른 클러스터에 동일한 이름을 가진 여러 스토리지 시스템을 지원하지 않습니다. SnapCenter 에서 지원하는 각 스토리지 시스템은 고유한 이름과 고유한 데이터 LIF IP 주소를 가져야 합니다.

이 작업에 관하여

- 스토리지 시스템을 구성할 때 EMS(이벤트 관리 시스템) 및 AutoSupport 기능도 활성화할 수 있습니다. AutoSupport 도구는 시스템 상태에 대한 데이터를 수집하여 NetApp 기술 지원팀에 자동으로 전송하여 시스템 문제를 해결할 수 있도록 합니다.

이러한 기능을 활성화하면 리소스가 보호되거나, 복원 또는 복제 작업이 성공적으로 완료되거나, 작업이 실패할 때 SnapCenter AutoSupport 정보를 스토리지 시스템에 보내고 EMS 메시지를 스토리지 시스템 syslog에 보냅니다.

- SnapMirror 대상이나 SnapVault 대상으로 스냅샷을 복제하려는 경우 대상 SVM이나 클러스터와 소스 SVM이나 클러스터에 대한 스토리지 시스템 연결을 설정해야 합니다.



저장 시스템 비밀번호를 변경하면 예약된 작업, 주문형 백업 및 복원 작업이 실패할 수 있습니다. 스토리지 시스템 비밀번호를 변경한 후 스토리지 탭에서 *수정*을 클릭하면 비밀번호를 업데이트할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *저장 시스템*을 클릭합니다.
2. 스토리지 시스템 페이지에서 *새로 만들기*를 클릭합니다.
3. 스토리지 시스템 추가 페이지에서 다음 정보를 제공합니다.

이 분야에서는...	이렇게 하세요...
저장 시스템	저장 시스템 이름이나 IP 주소를 입력하세요.  도메인 이름을 제외한 스토리지 시스템 이름은 15자 이하여야 하며, 이름을 확인할 수 있어야 합니다. 이름이 15자 이상인 스토리지 시스템 연결을 만들려면 Add-SmStorageConnectionPowerShell cmdlet을 사용할 수 있습니다.  MetroCluster 구성(MCC)을 사용하는 스토리지 시스템의 경우 중단 없는 작업을 위해 로컬 클러스터와 피어 클러스터를 모두 등록하는 것이 좋습니다. SnapCenter 서로 다른 클러스터에서 동일한 이름을 가진 여러 SVM을 지원하지 않습니다. SnapCenter 에서 지원하는 각 SVM에는 고유한 이름이 있어야 합니다.  SnapCenter 에 스토리지 연결을 추가한 후에는 ONTAP 사용하여 SVM이나 클러스터의 이름을 바꾸면 안 됩니다.  SVM이 짧은 이름이나 FQDN으로 추가된 경우 SnapCenter 와 플러그인 호스트 모두에서 확인할 수 있어야 합니다.
사용자 이름/비밀번호	스토리지 시스템에 액세스하는 데 필요한 권한이 있는 스토리지 사용자의 자격 증명을 입력하세요.

이 분야에서는...	이렇게 하세요...
이벤트 관리 시스템(EMS) 및 AutoSupport 설정	스토리지 시스템 syslog에 EMS 메시지를 보내거나 적용된 보호, 완료된 복원 작업 또는 실패한 작업에 대해 스토리지 시스템에 AutoSupport 메시지를 보내려면 해당 확인란을 선택합니다. 실패한 작업에 대한 AutoSupport 알림을 스토리지 시스템에 보내기 확인란을 선택하면 AutoSupport 알림을 활성화하려면 EMS 메시징이 필요하므로 * SnapCenter 서버 이벤트를 syslog에 기록* 확인란도 선택됩니다.

4. 플랫폼, 프로토콜, 포트 및 시간 초과에 할당된 기본값을 수정하려면 *추가 옵션*을 클릭하세요.

a. 플랫폼에서 드롭다운 목록에서 옵션 중 하나를 선택합니다.

SVM이 백업 관계의 보조 스토리지 시스템인 경우 보조 확인란을 선택합니다. 보조 옵션을 선택하면 SnapCenter 즉시 라이선스 확인을 수행하지 않습니다.

SnapCenter 에 SVM을 추가한 경우 사용자는 드롭다운에서 플랫폼 유형을 수동으로 선택해야 합니다.

a. 프로토콜에서 SVM 또는 클러스터 설정 중에 구성된 프로토콜(일반적으로 HTTPS)을 선택합니다.

b. 스토리지 시스템이 허용하는 포트를 입력하세요.

일반적으로 기본 포트 443이 작동합니다.

c. 통신 시도가 중단되기 전까지 걸리는 시간을 초 단위로 입력하세요.

기본값은 60초입니다.

d. SVM에 여러 관리 인터페이스가 있는 경우 기본 IP 확인란을 선택한 다음 SVM 연결에 대한 기본 IP 주소를 입력합니다.

e. *저장*을 클릭하세요.

5. *제출*을 클릭하세요.

결과

스토리지 시스템 페이지의 유형 드롭다운에서 다음 작업 중 하나를 수행합니다.

- 추가된 모든 SVM을 보려면 * ONTAP SVM*을 선택하세요.

FSx SVM을 추가한 경우 FSx SVM이 여기에 나열됩니다.

- 추가된 모든 클러스터를 보려면 * ONTAP 클러스터*를 선택하세요.

fsxadmin을 사용하여 FSx 클러스터를 추가한 경우 FSx 클러스터가 여기에 나열됩니다.

클러스터 이름을 클릭하면 클러스터에 속한 모든 SVM이 스토리지 가상 머신 섹션에 표시됩니다.

ONTAP GUI를 사용하여 ONTAP 클러스터에 새로운 SVM을 추가한 경우 *재검색*을 클릭하여 새로 추가된

SVM을 확인합니다.

끝난 후

클러스터 관리자는 SnapCenter 액세스할 수 있는 모든 스토리지 시스템에서 이메일 알림을 보내려면 스토리지 시스템 명령줄에서 다음 명령을 실행하여 각 스토리지 시스템 노드에서 AutoSupport 활성화해야 합니다.

```
autosupport trigger modify -node nodename -autosupport-message client.app.info  
-to enable -noteto enable
```



SVM(Storage Virtual Machine) 관리자는 AutoSupport 에 액세스할 수 없습니다.

저장소 연결 및 자격 증명

데이터 보호 작업을 수행하기 전에 스토리지 연결을 설정하고 SnapCenter 서버와 SnapCenter 플러그인에서 사용할 자격 증명을 추가해야 합니다.

저장소 연결

스토리지 연결을 통해 SnapCenter 서버와 SnapCenter 플러그인은 ONTAP 스토리지에 액세스할 수 있습니다. 이러한 연결을 설정하는 데는 AutoSupport 및 EMS(이벤트 관리 시스템) 기능을 구성하는 것도 포함됩니다.

신임장

- 도메인 관리자 또는 관리자 그룹의 모든 구성원

SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹 구성원을 지정하세요. 사용자 이름 필드에 사용할 수 있는 형식은 다음과 같습니다.

- *NetBIOS*\사용자 이름
- 도메인 *FQDN*\사용자 이름
- 사용자 이름@*upn*

- 로컬 관리자(작업 그룹에만 해당)

작업 그룹에 속한 시스템의 경우, SnapCenter 플러그인을 설치할 시스템에 기본 제공되는 로컬 관리자를 지정하십시오. 사용자 계정에 승격된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우, 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다.

사용자 이름 필드의 유효한 형식은 다음과 같습니다. *UserName*

- 개별 리소스 그룹에 대한 자격 증명

개별 리소스 그룹에 대한 자격 증명을 설정하고 사용자 이름에 전체 관리자 권한이 없는 경우 최소한 리소스 그룹 및 백업 권한을 사용자 이름에 할당해야 합니다.

Windows 호스트에 스토리지 프로비저닝

igroups를 만들고 관리하세요

스토리지 시스템의 주어진 LUN에 어떤 호스트가 액세스할 수 있는지 지정하려면 이니시에이터 그룹(igroup)을 만듭니다. SnapCenter 사용하면 Windows 호스트에서 igroup을 생성, 이름 변경, 수정 또는 삭제할 수 있습니다.

igroup 만들기

SnapCenter 사용하면 Windows 호스트에 igroup을 만들 수 있습니다. LUN에 igroup을 매핑하면 디스크 생성 마법사 또는 디스크 연결 마법사에서 igroup을 사용할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *igroup*을 클릭합니다.
3. 개시자 그룹 페이지에서 *새로 만들기*를 클릭합니다.
4. Igroup 만들기 대화 상자에서 igroup을 정의합니다.

이 분야에서는...	이렇게 하세요...
저장 시스템	igroup에 매핑할 LUN에 대한 SVM을 선택합니다.
주인	igroup을 만들려는 호스트를 선택하세요.
Igroup 이름	igroup의 이름을 입력하세요.
개시자	개시자를 선택하세요.
유형	이니시에이터 유형을 iSCSI, FCP 또는 혼합(FCP 및 iSCSI) 중에서 선택합니다.

5. 입력한 내용이 마음에 들면 *확인*을 클릭하세요.

SnapCenter 스토리지 시스템에 igroup을 생성합니다.

igroup 이름 바꾸기

SnapCenter 사용하여 기존 igroup의 이름을 바꿀 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *igroup*을 클릭합니다.
3. 이니시에이터 그룹 페이지에서 스토리지 가상 머신 필드를 클릭하여 사용 가능한 SVM 목록을 표시한 다음, 이름을 바꾸려는 igroup의 SVM을 선택합니다.
4. SVM의 igroup 목록에서 이름을 바꾸려는 igroup을 선택하고 *이름 바꾸기*를 클릭합니다.

5. igroup 이름 바꾸기 대화 상자에서 igroup의 새 이름을 입력하고 *이름 바꾸기*를 클릭합니다.

igroup 수정

SnapCenter 사용하면 기존 igroup에 igroup 초기자를 추가할 수 있습니다. igroup을 만들 때 호스트를 하나만 추가할 수 있습니다. 클러스터에 대한 igroup을 만들려면 igroup을 수정하여 다른 노드를 해당 igroup에 추가할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *igroup*을 클릭합니다.
3. 이니시에이터 그룹 페이지에서 스토리지 가상 머신 필드를 클릭하여 사용 가능한 SVM의 드롭다운 목록을 표시한 다음, 수정하려는 igroup의 SVM을 선택합니다.
4. igroup 목록에서 igroup을 선택하고 *igroup에 시작자 추가*를 클릭합니다.
5. 호스트를 선택하세요.
6. 시작 프로그램을 선택하고 *확인*을 클릭합니다.

igroup 삭제

더 이상 필요하지 않은 igroup을 삭제하려면 SnapCenter 사용하면 됩니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *igroup*을 클릭합니다.
3. 이니시에이터 그룹 페이지에서 스토리지 가상 머신 필드를 클릭하여 사용 가능한 SVM의 드롭다운 목록을 표시한 다음, 삭제하려는 igroup의 SVM을 선택합니다.
4. SVM의 igroup 목록에서 삭제하려는 igroup을 선택하고 *삭제*를 클릭합니다.
5. igroup 삭제 대화 상자에서 *확인*을 클릭합니다.

SnapCenter igroup을 삭제합니다.

디스크 생성 및 관리

Windows 호스트는 스토리지 시스템의 LUN을 가상 디스크로 인식합니다. SnapCenter 사용하여 FC 연결 또는 iSCSI 연결 LUN을 만들고 구성할 수 있습니다.

- SnapCenter 기본 디스크만 지원합니다. 동적 디스크는 지원되지 않습니다.
- GPT의 경우 데이터 파티션은 하나만 허용되고, MBR의 경우 NTFS 또는 CSVFS로 포맷된 볼륨 하나와 마운트 경로가 하나인 기본 파티션 하나만 허용됩니다.
- 지원되는 파티션 스타일: GPT, MBR; VMware UEFI VM에서는 iSCSI 디스크만 지원합니다.



SnapCenter 디스크 이름 변경을 지원하지 않습니다. SnapCenter 에서 관리하는 디스크의 이름이 변경되면 SnapCenter 작업이 성공하지 못합니다.

호스트의 디스크 보기

SnapCenter 사용하여 관리하는 각 Windows 호스트의 디스크를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *디스크*를 클릭합니다.
3. 호스트 드롭다운 목록에서 호스트를 선택하세요.

디스크가 나열됩니다.

클러스터된 디스크 보기

SnapCenter 로 관리하는 클러스터에서 클러스터된 디스크를 볼 수 있습니다. 클러스터된 디스크는 호스트 드롭다운에서 클러스터를 선택할 때만 표시됩니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *디스크*를 클릭합니다.
3. 호스트 드롭다운 목록에서 클러스터를 선택합니다.

디스크가 나열됩니다.

iSCSI 세션을 설정합니다

iSCSI를 사용하여 LUN에 연결하는 경우 통신을 활성화하려면 LUN을 생성하기 전에 iSCSI 세션을 설정해야 합니다.

시작하기 전에

- 스토리지 시스템 노드를 iSCSI 대상으로 정의해야 합니다.
- 스토리지 시스템에서 iSCSI 서비스를 시작했어야 합니다. ["자세히 알아보기"](#)

이 작업에 관하여

iSCSI 세션은 동일한 IP 버전 간에만 설정할 수 있습니다. 즉, IPv6에서 IPv6로, IPv4에서 IPv4로 설정할 수 있습니다.

iSCSI 세션 관리와 호스트와 대상 간의 통신에는 링크 로컬 IPv6 주소를 사용할 수 있지만, 이는 둘 다 동일한 서브넷에 있는 경우에만 가능합니다.

iSCSI 이니시에이터의 이름을 변경하면 iSCSI 대상에 대한 액세스가 영향을 받습니다. 이름을 변경한 후에는 개시자가 액세스하는 대상을 다시 구성하여 새 이름을 인식할 수 있도록 해야 할 수도 있습니다. iSCSI 이니시에이터의 이름을 변경한 후에는 호스트를 다시 시작해야 합니다.

호스트에 iSCSI 인터페이스가 두 개 이상 있는 경우 첫 번째 인터페이스의 IP 주소를 사용하여 SnapCenter 에 iSCSI 세션을 설정하면 다른 IP 주소를 사용하여 다른 인터페이스에서 iSCSI 세션을 설정할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *iSCSI 세션*을 클릭합니다.
3. 스토리지 가상 머신 드롭다운 목록에서 iSCSI 대상에 대한 스토리지 가상 머신(SVM)을 선택합니다.
4. 호스트 드롭다운 목록에서 세션의 호스트를 선택합니다.
5. *세션 설정*을 클릭하세요.

세션 설정 마법사가 표시됩니다.

6. 세션 설정 마법사에서 대상을 식별합니다.

이 분야에서는...	입력하다...
대상 노드 이름	iSCSI 대상의 노드 이름 기존 대상 노드 이름이 있는 경우 해당 이름은 읽기 전용 형식으로 표시됩니다.
대상 포털 주소	대상 네트워크 포털의 IP 주소
대상 포털 포트	대상 네트워크 포털의 TCP 포트
개시자 포털 주소	개시자 네트워크 포털의 IP 주소

7. 입력한 내용이 마음에 들면 *연결*을 클릭하세요.

SnapCenter iSCSI 세션을 설정합니다.

8. 각 대상에 대한 세션을 설정하려면 이 절차를 반복합니다.

FC 연결 또는 iSCSI 연결 LUN 또는 디스크 생성

Windows 호스트는 스토리지 시스템의 LUN을 가상 디스크로 인식합니다. SnapCenter 사용하여 FC 연결 또는 iSCSI 연결 LUN을 만들고 구성할 수 있습니다.

SnapCenter 외부에서 디스크를 만들고 포맷하려면 NTFS 및 CSVFS 파일 시스템만 지원됩니다.

시작하기 전에

- 스토리지 시스템에서 LUN에 대한 볼륨을 생성했어야 합니다.

볼륨은 LUN만 보관해야 하며, SnapCenter 로 생성된 LUN만 보관해야 합니다.



클론이 이미 분할되지 않은 한 SnapCenter 에서 생성된 클론 볼륨에 LUN을 생성할 수 없습니다.

- 스토리지 시스템에서 FC 또는 iSCSI 서비스를 시작했어야 합니다.
- iSCSI를 사용하는 경우 스토리지 시스템과 iSCSI 세션을 설정해야 합니다.
- Windows용 SnapCenter 플러그인 패키지는 디스크를 생성하는 호스트에만 설치해야 합니다.

이 작업에 관하여

- LUN이 Windows Server 장애 조치(failover) 클러스터의 호스트에서 공유되지 않는 한 LUN을 두 개 이상의 호스트에 연결할 수 없습니다.
- CSV(클러스터 공유 볼륨)를 사용하는 Windows Server 장애 조치(failover) 클러스터의 호스트에서 LUN을 공유하는 경우, 클러스터 그룹을 소유한 호스트에 디스크를 만들어야 합니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *디스크*를 클릭합니다.
3. 호스트 드롭다운 목록에서 호스트를 선택하세요.
4. *새로 만들기*를 클릭합니다.

디스크 생성 마법사가 열립니다.

5. LUN 이름 페이지에서 LUN을 식별합니다.

이 분야에서는...	이렇게 하세요...
저장 시스템	LUN에 대한 SVM을 선택합니다.
LUN 경로	*찾아보기*를 클릭하여 LUN이 포함된 폴더의 전체 경로를 선택합니다.
LUN 이름	LUN의 이름을 입력하세요.
클러스터 크기	클러스터의 LUN 블록 할당 크기를 선택합니다. 클러스터 크기는 운영 체제와 애플리케이션에 따라 달라집니다.
LUN 레이블	선택적으로 LUN에 대한 설명 텍스트를 입력합니다.

6. 디스크 유형 페이지에서 디스크 유형을 선택합니다.

선택하다...	만약에...
전용 디스크	LUN은 하나의 호스트에서만 액세스할 수 있습니다. 리소스 그룹 필드를 무시하세요.

선택하다...	만약에...
공유 디스크	LUN은 Windows Server 장애 조치 클러스터의 호스트에서 공유됩니다. 리소스 그룹 필드에 클러스터 리소스 그룹의 이름을 입력합니다. 장애 조치 클러스터의 한 호스트에만 디스크를 생성해야 합니다.
클러스터 공유 볼륨(CSV)	LUN은 CSV를 사용하는 Windows Server 장애 조치 클러스터의 호스트에서 공유됩니다. 리소스 그룹 필드에 클러스터 리소스 그룹의 이름을 입력합니다. 디스크를 생성하는 호스트가 클러스터 그룹의 소유자인지 확인하세요.

7. 드라이브 속성 페이지에서 드라이브 속성을 지정합니다.

재산	설명
마운트 지점 자동 할당	SnapCenter 시스템 드라이브를 기반으로 볼륨 마운트 지점을 자동으로 할당합니다. 예를 들어, 시스템 드라이브가 C:인 경우 자동 할당은 C: 드라이브 아래에 볼륨 마운트 지점(C:\scmnt\...)을 생성합니다. 공유 디스크에는 자동 할당이 지원되지 않습니다.
드라이브 문자 할당	인접한 드롭다운 목록에서 선택한 드라이브에 디스크를 마운트합니다.
볼륨 마운트 지점 사용	인접 필드에 지정한 드라이브 경로에 디스크를 마운트합니다. 볼륨 마운트 지점의 루트는 디스크를 생성하는 호스트가 소유해야 합니다.
드라이브 문자 또는 볼륨 마운트 지점을 할당하지 마십시오.	Windows에서 디스크를 수동으로 마운트하려면 이 옵션을 선택하세요.
LUN 크기	LUN 크기를 지정하세요. 최소 150MB. 옆의 드롭다운 목록에서 MB, GB 또는 TB를 선택하세요.

재산	설명
이 LUN을 호스팅하는 볼륨에 씬 프로비저닝을 사용합니다.	LUN을 씬 프로비저닝합니다. 씬 프로비저닝은 한 번에 필요한 만큼의 저장 공간만 할당하므로 LUN이 사용 가능한 최대 용량까지 효율적으로 확장될 수 있습니다. 필요한 모든 LUN 스토리지를 수용할 수 있을 만큼 볼륨에 충분한 공간이 있는지 확인하세요.
파티션 유형을 선택하세요	GUID 파티션 테이블의 경우 GPT 파티션을 선택하고, 마스터 부트 레코드의 경우 MBR 파티션을 선택합니다. MBR 파티션은 Windows Server 장애 조치(failover) 클러스터에서 정렬 오류 문제를 일으킬 수 있습니다.  통합 확장 가능 펌웨어 인터페이스(UEFI) 파티션 디스크는 지원되지 않습니다.

8. LUN 매핑 페이지에서 호스트의 iSCSI 또는 FC 이니시에이터를 선택합니다.

이 분야에서는...	이렇게 하세요...
주인	클러스터 그룹 이름을 두 번 클릭하여 클러스터에 속한 호스트를 보여주는 드롭다운 목록을 표시한 다음, 개시자에 대한 호스트를 선택합니다. 이 필드는 LUN이 Windows Server 장애 조치 클러스터의 호스트에서 공유되는 경우에만 표시됩니다.
호스트 개시자를 선택하세요	Fibre Channel 또는 *iSCSI*를 선택한 다음 호스트에서 이니시에이터를 선택합니다. MPIO(멀티패스 I/O)를 사용하는 FC를 사용하는 경우 여러 개의 FC 이니시에이터를 선택할 수 있습니다.

9. 그룹 유형 페이지에서 기존 igroup을 LUN에 매핑할지 아니면 새 igroup을 만들지 지정합니다.

선택하다...	만약에...
선택한 개시자에 대한 새 igroup 만들기	선택한 개시자에 대한 새로운 igroup을 생성하려고 합니다.

선택하다...	만약에...
기존 igroup을 선택하거나 선택한 개시자에 대한 새 igroup을 지정합니다.	선택한 개시자에 대해 기존 igroup을 지정하거나 지정한 이름으로 새 igroup을 만들려고 합니다. igroup 이름 필드에 igroup 이름을 입력하세요. 기존 igroup 이름의 처음 몇 글자를 입력하면 필드가 자동 완성됩니다.

10. 요약 페이지에서 선택 사항을 검토한 다음 *마침*을 클릭합니다.

SnapCenter LUN을 생성하고 호스트의 지정된 드라이브 또는 드라이브 경로에 연결합니다.

디스크 크기 조정

저장 시스템의 변경 요구에 따라 디스크 크기를 늘리거나 줄일 수 있습니다.

이 작업에 관하여

- 씬 프로비저닝된 LUN의 경우 ONTAP LUN 지오메트리 크기는 최대 크기로 표시됩니다.
- 두꺼운 프로비저닝된 LUN의 경우 확장 가능한 크기(볼륨에서 사용 가능한 크기)는 최대 크기로 표시됩니다.
- MBR 스타일 파티션이 있는 LUN의 크기 제한은 2TB입니다.
- GPT 스타일 파티션이 있는 LUN의 스토리지 시스템 크기 제한은 16TB입니다.
- LUN 크기를 조정하기 전에 스냅샷을 만드는 것이 좋습니다.
- LUN 크기가 조정되기 전에 만든 스냅샷에서 LUN을 복원해야 하는 경우 SnapCenter 스냅샷 크기에 맞춰 LUN 크기를 자동으로 조정합니다.

복원 작업 후, 크기가 조정된 후 LUN에 추가된 데이터는 크기가 조정된 후 만들어진 스냅샷에서 복원되어야 합니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *디스크*를 클릭합니다.
3. 호스트 드롭다운 목록에서 호스트를 선택합니다.

디스크가 나열됩니다.

4. 크기를 조정하려는 디스크를 선택한 다음 *크기 조정*을 클릭합니다.
5. 디스크 크기 조정 대화 상자에서 슬라이더 도구를 사용하여 디스크의 새 크기를 지정하거나 크기 필드에 새 크기를 입력합니다.



크기를 수동으로 입력하는 경우, 축소 또는 확장 버튼이 적절하게 활성화되기 전에 크기 필드 외부로 클릭해야 합니다. 또한, 측정 단위를 지정하려면 MB, GB 또는 TB를 클릭해야 합니다.

6. 입력한 내용이 마음에 들면 필요에 따라 축소 또는 *확장*을 클릭하세요.

SnapCenter 디스크 크기를 조정합니다.

디스크 연결

디스크 연결 마법사를 사용하여 기존 LUN을 호스트에 연결하거나 연결이 끊어진 LUN을 다시 연결할 수 있습니다.

시작하기 전에

- 스토리지 시스템에서 FC 또는 iSCSI 서비스를 시작했어야 합니다.
- iSCSI를 사용하는 경우 스토리지 시스템과 iSCSI 세션을 설정해야 합니다.
- LUN이 Windows Server 장애 조치(failover) 클러스터의 호스트에서 공유되지 않는 한 LUN을 두 개 이상의 호스트에 연결할 수 없습니다.
- LUN이 CSV(클러스터 공유 볼륨)를 사용하는 Windows Server 장애 조치(failover) 클러스터의 호스트에서 공유되는 경우, 클러스터 그룹을 소유한 호스트의 디스크를 연결해야 합니다.
- Windows용 플러그인은 디스크를 연결하는 호스트에만 설치하면 됩니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *디스크*를 클릭합니다.
3. 호스트 드롭다운 목록에서 호스트를 선택하세요.
4. *연결*을 클릭하세요.

디스크 연결 마법사가 열립니다.

5. LUN 이름 페이지에서 연결할 LUN을 식별합니다.

이 분야에서는...	이렇게 하세요...
저장 시스템	LUN에 대한 SVM을 선택합니다.
LUN 경로	*찾아보기*를 클릭하여 LUN이 포함된 볼륨의 전체 경로를 선택합니다.
LUN 이름	LUN의 이름을 입력하세요.
클러스터 크기	클러스터의 LUN 블록 할당 크기를 선택합니다. 클러스터 크기는 운영 체제와 애플리케이션에 따라 달라집니다.
LUN 레이블	선택적으로 LUN에 대한 설명 텍스트를 입력합니다.

6. 디스크 유형 페이지에서 디스크 유형을 선택합니다.

선택하다...	만약에...
전용 디스크	LUN은 하나의 호스트에서만 액세스할 수 있습니다.
공유 디스크	LUN은 Windows Server 장애 조치 클러스터의 호스트에서 공유됩니다. 장애 조치 클러스터에서 하나의 호스트에만 디스크를 연결하면 됩니다.
클러스터 공유 볼륨(CSV)	LUN은 CSV를 사용하는 Windows Server 장애 조치 클러스터의 호스트에서 공유됩니다. 디스크에 연결하는 호스트가 클러스터 그룹의 소유자인지 확인하세요.

7. 드라이브 속성 페이지에서 드라이브 속성을 지정합니다.

재산	설명
자동 할당	SnapCenter 시스템 드라이브를 기반으로 볼륨 마운트 지점을 자동으로 할당하도록 합니다. 예를 들어, 시스템 드라이브가 C:인 경우 자동 할당 속성은 C: 드라이브 아래에 볼륨 마운트 지점(C:\scmnt)을 만듭니다. 공유 디스크에서는 자동 할당 속성이 지원되지 않습니다.
드라이브 문자 할당	옆의 드롭다운 목록에서 선택한 드라이브에 디스크를 마운트합니다.
볼륨 마운트 지점 사용	인접한 필드에 지정한 드라이브 경로에 디스크를 마운트합니다. 볼륨 마운트 지점의 루트는 디스크를 생성하는 호스트가 소유해야 합니다.
드라이브 문자 또는 볼륨 마운트 지점을 할당하지 마십시오.	Windows에서 디스크를 수동으로 마운트하려면 이 옵션을 선택하세요.

8. LUN 매핑 페이지에서 호스트의 iSCSI 또는 FC 이니시에이터를 선택합니다.

이 분야에서는...	이렇게 하세요...
주인	클러스터 그룹 이름을 두 번 클릭하면 클러스터에 속한 호스트를 보여주는 드롭다운 목록이 표시되고, 그런 다음 개시자에 대한 호스트를 선택합니다. 이 필드는 LUN이 Windows Server 장애 조치 클러스터의 호스트에서 공유되는 경우에만 표시됩니다.
호스트 개시자를 선택하세요	Fibre Channel 또는 *iSCSI* 를 선택한 다음 호스트에서 이니시에이터를 선택합니다. MPIO와 함께 FC를 사용하는 경우 여러 개의 FC 이니시에이터를 선택할 수 있습니다.

9. 그룹 유형 페이지에서 기존 igroup을 LUN에 매핑할지 아니면 새 igroup을 만들지 지정합니다.

선택하다...	만약에...
선택한 개시자에 대한 새 igroup 만들기	선택한 개시자에 대한 새로운 igroup을 생성하려고 합니다.
기존 igroup을 선택하거나 선택한 개시자에 대한 새 igroup을 지정합니다.	선택한 개시자에 대해 기존 igroup을 지정하거나 지정한 이름으로 새 igroup을 만들려고 합니다. igroup 이름 필드에 igroup 이름을 입력하세요. 기존 igroup 이름의 처음 몇 글자를 입력하면 필드가 자동으로 완성됩니다.

10. 요약 페이지에서 선택 사항을 검토하고 *마침*을 클릭합니다.

SnapCenter LUN을 호스트의 지정된 드라이브 또는 드라이브 경로에 연결합니다.

디스크 연결 해제

LUN의 내용에 영향을 미치지 않고 호스트에서 LUN을 분리할 수 있습니다. 단, 한 가지 예외가 있습니다. 복제본이 분할되기 전에 복제본의 연결을 끊으면 복제본의 내용이 손실됩니다.

시작하기 전에

- LUN이 어떤 애플리케이션에서도 사용되고 있지 않은지 확인하세요.
- LUN이 모니터링 소프트웨어로 모니터링되고 있지 않은지 확인하세요.
- LUN이 공유된 경우 LUN에서 클러스터 리소스 종속성을 제거하고 클러스터의 모든 노드가 전원이 켜져 있고 제대로 작동하며 SnapCenter 에서 사용할 수 있는지 확인하세요.

이 작업에 관하여

SnapCenter 에서 생성한 FlexClone 볼륨에서 LUN의 연결을 끊고 해당 볼륨의 다른 LUN이 연결되어 있지 않으면 SnapCenter 해당 볼륨을 삭제합니다. LUN 연결을 끊기 전에 SnapCenter FlexClone 볼륨이 삭제될 수 있다는 경고

메시지를 표시합니다.

FlexClone 볼륨이 자동으로 삭제되는 것을 방지하려면 마지막 LUN의 연결을 끊기 전에 볼륨의 이름을 바꿔야 합니다. 볼륨의 이름을 바꿀 때는 이름의 마지막 문자뿐만 아니라 여러 문자를 변경해야 합니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *디스크*를 클릭합니다.
3. 호스트 드롭다운 목록에서 호스트를 선택하세요.

디스크가 나열됩니다.

4. 연결을 끊을 디스크를 선택한 다음 *연결 끊기*를 클릭합니다.
5. 디스크 연결 끊기 대화 상자에서 *확인*을 클릭합니다.

SnapCenter 가 디스크 연결을 끊습니다.

디스크 삭제

더 이상 필요하지 않은 디스크는 삭제할 수 있습니다. 디스크를 삭제한 후에는 삭제를 취소할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *디스크*를 클릭합니다.
3. 호스트 드롭다운 목록에서 호스트를 선택하세요.

디스크가 나열됩니다.

4. 삭제할 디스크를 선택한 다음 *삭제*를 클릭합니다.
5. 디스크 삭제 대화 상자에서 *확인*을 클릭합니다.

SnapCenter 디스크를 삭제합니다.

SMB 공유 생성 및 관리

스토리지 가상 머신(SVM)에서 SMB3 공유를 구성하려면 SnapCenter 사용자 인터페이스나 PowerShell cmdlet을 사용할 수 있습니다.

모범 사례: SnapCenter 에서 제공하는 템플릿을 활용하여 공유 구성을 자동화할 수 있으므로 cmdlet을 사용하는 것이 좋습니다.

템플릿은 볼륨 및 공유 구성에 대한 모범 사례를 캡슐화합니다. Windows용 SnapCenter 플러그인 패키지의 설치 폴더의 Templates 폴더에서 템플릿을 찾을 수 있습니다.



편안하다면 제공된 모델을 따라 나만의 템플릿을 만들 수 있습니다. 사용자 지정 템플릿을 만들기 전에 cmdlet 설명서의 매개변수를 검토해야 합니다.

SMB 공유 만들기

SnapCenter 공유 페이지를 사용하여 스토리지 가상 머신(SVM)에 SMB3 공유를 만들 수 있습니다.

SnapCenter 사용하여 SMB 공유의 데이터베이스를 백업할 수 없습니다. SMB 지원은 프로비저닝에만 국한됩니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *공유*를 클릭합니다.
3. 스토리지 가상 머신 드롭다운 목록에서 SVM을 선택합니다.
4. *새로 만들기*를 클릭합니다.

새 공유 대화 상자가 열립니다.

5. 새 공유 대화 상자에서 공유를 정의합니다.

이 분야에서는...	이렇게 하세요...
설명	공유에 대한 설명 텍스트를 입력하세요.
공유 이름	공유 이름을 입력합니다(예: test_share). 공유에 입력한 이름은 볼륨 이름으로도 사용됩니다. 공유 이름: • UTF-8 문자열이어야 합니다. • 다음 문자를 포함할 수 없습니다: 0x00~0x1F(둘 다 포함)의 제어 문자, 0x22(큰따옴표) 및 특수 문자 \ / [] : (vertical bar) < > + = ; , ?
경로 공유	• 필드를 클릭하여 새 파일 시스템 경로를 입력합니다 (예: /). • 기존 파일 시스템 경로 목록에서 선택하려면 필드를 두 번 클릭합니다.

6. 입력한 내용이 마음에 들면 *확인*을 클릭하세요.

SnapCenter SVM에 SMB 공유를 생성합니다.

SMB 공유 삭제

더 이상 필요하지 않은 SMB 공유를 삭제할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *공유*를 클릭합니다.
3. 공유 페이지에서 저장소 가상 머신 필드를 클릭하여 사용 가능한 저장 가상 머신(SVM) 목록이 있는 드롭다운을 표시한 다음, 삭제하려는 공유의 SVM을 선택합니다.
4. SVM의 공유 목록에서 삭제하려는 공유를 선택하고 *삭제*를 클릭합니다.
5. 공유 삭제 대화 상자에서 *확인*을 클릭합니다.

SnapCenter SVM에서 SMB 공유를 삭제합니다.

저장 시스템에서 공간 확보

NTFS는 파일이 삭제되거나 수정될 때 LUN의 사용 가능한 공간을 추적하지만, 스토리지 시스템에 새로운 정보를 보고하지 않습니다. Windows 호스트용 플러그인에서 공간 회수 PowerShell cmdlet을 실행하면 새로 해제된 블록이 저장소에서 사용 가능한 것으로 표시됩니다.

원격 플러그인 호스트에서 cmdlet을 실행하는 경우 SnapCenterOpen-SMConnection cmdlet을 실행하여 SnapCenter 서버에 대한 연결을 열어야 합니다.

시작하기 전에

- 복원 작업을 수행하기 전에 공간 회수 프로세스가 완료되었는지 확인해야 합니다.
- LUN이 Windows Server 장애 조치(failover) 클러스터의 호스트에서 공유되는 경우 클러스터 그룹을 소유한 호스트에서 공간 회수를 수행해야 합니다.
- 최적의 저장 성능을 위해서는 가능한 한 자주 공간 회수를 수행해야 합니다.

전체 NTFS 파일 시스템이 검사되었는지 확인해야 합니다.

이 작업에 관하여

- 공간 회수는 시간이 많이 걸리고 CPU를 많이 사용하므로 일반적으로 스토리지 시스템과 Windows 호스트 사용량이 낮을 때 작업을 실행하는 것이 가장 좋습니다.
- 공간 회수는 사용 가능한 공간을 거의 모두 회수하지만 100% 회수하지는 못합니다.
- 공간 회수를 수행하는 동안 디스크 조각 모음을 동시에 실행하면 안 됩니다.

그렇게 하면 회수 과정이 느려질 수 있습니다.

단계

애플리케이션 서버 PowerShell 명령 프롬프트에서 다음 명령을 입력합니다.

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

drive_path는 LUN에 매핑된 드라이브 경로입니다.

PowerShell cmdlet을 사용하여 스토리지 프로비저닝

SnapCenter GUI를 사용하여 호스트 프로비저닝 및 공간 회수 작업을 수행하고 싶지 않은 경우 PowerShell cmdlet을 사용할 수 있습니다. cmdlet을 직접 사용하거나 스크립트에 추가할 수 있습니다.

원격 플러그인 호스트에서 cmdlet을 실행하는 경우 SnapCenter Open-SMConnection cmdlet을 실행하여 SnapCenter 서버에 대한 연결을 열어야 합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

서버에서 Windows용 SnapDrive 제거하여 SnapCenter PowerShell cmdlet이 손상된 경우 다음을 참조하세요. "[Windows용 SnapDrive 제거하면 SnapCenter cmdlet이 손상됨](#)".

VMware 환경에서 스토리지 프로비저닝

VMware 환경에서 Microsoft Windows용 SnapCenter 플러그인을 사용하면 LUN을 생성 및 관리하고 스냅샷을 관리할 수 있습니다.

지원되는 **VMware** 게스트 OS 플랫폼

- 지원되는 Windows Server 버전
- Microsoft 클러스터 구성

Microsoft iSCSI Software Initiator를 사용할 때 VMware에서 지원되는 최대 16개 노드 또는 FC를 사용할 때 최대 2개 노드 지원

- RDM LUN

일반 RDMS의 경우 4개의 LSI Logic SCSI 컨트롤러로 최대 56개의 RDM LUN을 지원하거나 Windows 구성을 위한 VMware VM MSCS 박스 간 플러그인에서 3개의 LSI Logic SCSI 컨트롤러로 최대 42개의 RDM LUN을 지원합니다.

VMware ParaVirtual SCSI 컨트롤러를 지원합니다. RDM 디스크에서는 최대 256개의 디스크를 지원할 수 있습니다.

지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "[NetApp 상호 운용성 매트릭스 도구](#)".

VMware ESXi 서버 관련 제한 사항

- ESXi 자격 증명을 사용하여 가상 머신의 Microsoft 클러스터에 Windows용 플러그인을 설치하는 것은 지원되지 않습니다.

클러스터된 가상 머신에 Windows용 플러그인을 설치할 때는 vCenter 자격 증명을 사용해야 합니다.

- 모든 클러스터 노드는 동일한 클러스터 디스크에 대해 동일한 대상 ID(가상 SCSI 어댑터에서)를 사용해야 합니다.
- Windows용 플러그인 외부에서 RDM LUN을 생성하는 경우 플러그인 서비스를 다시 시작해야 새로 생성된

디스크를 인식할 수 있습니다.

- VMware 게스트 OS에서는 iSCSI와 FC 이니시에이터를 동시에 사용할 수 없습니다.

SnapCenter RDM 작업에 필요한 최소 vCenter 권한

게스트 OS에서 RDM 작업을 수행하려면 호스트에 대한 다음 vCenter 권한이 있어야 합니다.

- 데이터 저장소: 파일 제거
- 호스트: 구성 > 스토리지 파티션 구성
- 가상 머신: 구성

이러한 권한은 Virtual Center 서버 수준의 역할에 할당해야 합니다. 이러한 권한을 할당한 역할은 루트 권한이 없는 사용자에게 할당될 수 없습니다.

이러한 권한을 할당한 후 게스트 OS에 Windows용 플러그인을 설치할 수 있습니다.

Microsoft 클러스터에서 FC RDM LUN 관리

Windows용 플러그인을 사용하면 FC RDM LUN을 사용하여 Microsoft 클러스터를 관리할 수 있지만, 먼저 플러그인 외부에서 공유 RDM 쿼럼과 공유 스토리지를 만든 다음 클러스터의 가상 머신에 디스크를 추가해야 합니다.

ESXi 5.5부터 ESX iSCSI 및 FCoE 하드웨어를 사용하여 Microsoft 클러스터를 관리할 수도 있습니다. Windows용 플러그인에는 Microsoft 클러스터에 대한 기본 지원이 포함되어 있습니다.

요구 사항

Windows용 플러그인은 두 개의 서로 다른 ESX 또는 ESXi 서버에 속한 두 개의 서로 다른 가상 머신에서 FC RDM LUN을 사용하는 Microsoft 클러스터를 지원합니다. 이는 특정 구성 요구 사항을 충족하는 경우, 클러스터 간 클러스터링이라고도 합니다.

- 가상 머신(VM)은 동일한 Windows Server 버전을 실행해야 합니다.
- ESX 또는 ESXi 서버 버전은 각 VMware 상위 호스트에서 동일해야 합니다.
- 각 부모 호스트에는 최소한 두 개의 네트워크 어댑터가 있어야 합니다.
- 두 ESX 또는 ESXi 서버 간에 공유되는 VMware 가상 머신 파일 시스템(VMFS) 데이터 저장소가 하나 이상 있어야 합니다.
- VMware에서는 공유 데이터 저장소를 FC SAN에 생성할 것을 권장합니다.

필요한 경우 공유 데이터 저장소를 iSCSI를 통해 생성할 수도 있습니다.

- 공유 RDM LUN은 물리적 호환 모드에 있어야 합니다.
- 공유 RDM LUN은 Windows용 플러그인 외부에서 수동으로 생성해야 합니다.

공유 스토리지에는 가상 디스크를 사용할 수 없습니다.

- 클러스터의 각 가상 머신에는 물리적 호환 모드에서 SCSI 컨트롤러를 구성해야 합니다.

Windows Server 2008 R2에서는 각 가상 머신에서 LSI Logic SAS SCSI 컨트롤러를 구성해야 합니다. 공유 LUN은 해당 유형의 SAS 컨트롤러가 하나만 존재하고 이미 C: 드라이브에 연결되어 있는 경우 기존 LSI Logic SAS 컨트롤러를 사용할 수 없습니다.

준가상화 유형의 SCSI 컨트롤러는 VMware Microsoft 클러스터에서 지원되지 않습니다.



물리적 호환 모드에서 가상 머신의 공유 LUN에 SCSI 컨트롤러를 추가하는 경우 VMware Infrastructure Client에서 새 디스크 만들기 옵션이 아닌 원시 장치 매핑(RDM) 옵션을 선택해야 합니다.

- Microsoft 가상 머신 클러스터는 VMware 클러스터의 일부가 될 수 없습니다.
- Microsoft 클러스터에 속한 가상 머신에 Windows용 플러그인을 설치하는 경우 ESX 또는 ESXi 자격 증명이 아닌 vCenter 자격 증명을 사용해야 합니다.
- Windows용 플러그인은 여러 호스트의 시작자로 단일 igroup을 생성할 수 없습니다.

모든 ESXi 호스트의 이니시에이터를 포함하는 igroup은 공유 클러스터 디스크로 사용될 RDM LUN을 생성하기 전에 스토리지 컨트롤러에 생성되어야 합니다.

- FC 이니시에이터를 사용하여 ESXi 5.0에서 RDM LUN을 생성해야 합니다.

RDM LUN을 생성하면 ALUA를 사용하여 이니시에이터 그룹이 생성됩니다.

제한 사항

Windows용 플러그인은 서로 다른 ESX 또는 ESXi 서버에 속한 다양한 가상 머신에서 FC/iSCSI RDM LUN을 사용하는 Microsoft 클러스터를 지원합니다.



이 기능은 ESX 5.5i 이전 릴리스에서는 지원되지 않습니다.

- Windows용 플러그인은 ESX iSCSI 및 NFS 데이터 저장소의 클러스터를 지원하지 않습니다.
- Windows용 플러그인은 클러스터 환경에서 혼합된 이니시에이터를 지원하지 않습니다.

이니시에이터는 FC 또는 Microsoft iSCSI 중 하나여야 하며, 둘 다일 수는 없습니다.

- ESX iSCSI 이니시에이터와 HBA는 Microsoft 클러스터의 공유 디스크에서 지원되지 않습니다.
- 가상 머신이 Microsoft 클러스터의 일부인 경우 Windows용 플러그인은 vMotion을 사용한 가상 머신 마이그레이션을 지원하지 않습니다.
- Windows용 플러그인은 Microsoft 클러스터의 가상 머신에서 MPIO를 지원하지 않습니다.

공유 FC RDM LUN 생성

Microsoft 클러스터의 노드 간에 저장소를 공유하기 위해 FC RDM LUN을 사용하려면 먼저 공유 쿼럼 디스크와 공유 저장소 디스크를 만든 다음, 클러스터의 두 가상 머신에 이를 추가해야 합니다.

공유 디스크는 Windows용 플러그인을 사용하여 생성되지 않습니다. 클러스터의 각 가상 머신에 공유 LUN을 만든 다음 추가해야 합니다. 자세한 내용은 다음을 참조하세요. "[물리적 호스트에 걸쳐 클러스터 가상 머신](#)".

SnapCenter Standard 컨트롤러 기반 라이선스 추가

FAS, AFF 또는 ASA 스토리지 컨트롤러를 사용하는 경우 SnapCenter Standard 컨트롤러 기반 라이선스가 필요합니다.

컨트롤러 기반 라이선스에는 다음과 같은 특징이 있습니다.

- 프리미엄 또는 플래시 번들 구매 시 SnapCenter Standard 권한이 포함됩니다(기본 팩에는 포함되지 않음)
- 무제한 저장 공간 사용
- ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 FAS, AFF 또는 ASA 스토리지 컨트롤러에 직접 추가합니다.



SnapCenter 컨트롤러 기반 라이선스의 경우 SnapCenter 사용자 인터페이스에 라이선스 정보를 입력하지 않습니다.

- 컨트롤러의 일련번호에 고정됨

필요한 라이선스에 대한 정보는 다음을 참조하세요. "[SnapCenter 라이선스](#)".

1단계: SnapManager Suite 라이선스가 설치되었는지 확인

SnapCenter 사용자 인터페이스를 사용하여 SnapManager Suite 라이선스가 FAS, AFF 또는 ASA 기본 스토리지 시스템에 설치되어 있는지 확인하고 라이선스가 필요한 시스템을 식별할 수 있습니다. SnapManager Suite 라이선스는 기본 스토리지 시스템의 FAS, AFF, ASA SVM 또는 클러스터에만 적용됩니다.



컨트롤러에 이미 SnapManager Suite 라이선스가 있는 경우 SnapCenter 자동으로 Standard 컨트롤러 기반 라이선스 자격을 제공합니다. SnapManager Suite 라이선스와 SnapCenter Standard 컨트롤러 기반 라이선스라는 이름은 혼용되지만, 동일한 라이선스를 나타냅니다.

단계

1. 왼쪽 탐색 창에서 *저장 시스템*을 선택합니다.
2. 스토리지 시스템 페이지의 유형 드롭다운에서 추가된 모든 SVM 또는 클러스터를 볼지 여부를 선택합니다.
 - 추가된 모든 SVM을 보려면 * ONTAP SVM*을 선택하세요.
 - 추가된 모든 클러스터를 보려면 * ONTAP 클러스터*를 선택하세요.

클러스터 이름을 선택하면 클러스터에 속한 모든 SVM이 스토리지 가상 머신 섹션에 표시됩니다.

3. 저장소 연결 목록에서 컨트롤러 라이선스 열을 찾으세요.

컨트롤러 라이선스 열에는 다음 상태가 표시됩니다.

◦



SnapManager Suite 라이선스가 FAS, AFF 또는 ASA 기본 스토리지 시스템에 설치되었음을 나타냅니다.

◦



SnapManager Suite 라이선스가 FAS, AFF 또는 ASA 기본 스토리지 시스템에 설치되지 않았음을 나타냅니다.

◦

해당 없음은 스토리지 컨트롤러가 Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select 또는 보조 스토리지 플랫폼에 있기 때문에 SnapManager Suite 라이선스가 적용되지 않음을 나타냅니다.

2단계: 컨트롤러에 설치된 라이선스 식별

ONTAP 명령줄을 사용하면 컨트롤러에 설치된 모든 라이선스를 볼 수 있습니다. FAS, AFF 또는 ASA 시스템의 클러스터 관리자가 되어야 합니다.



컨트롤러는 SnapManagerSuite 라이선스로 SnapCenter Standard 컨트롤러 기반 라이선스를 표시합니다.

단계

1. ONTAP 명령줄을 사용하여 NetApp 컨트롤러에 로그인합니다.
2. license show 명령을 입력한 다음 출력을 보고 SnapManagerSuite 라이선스가 설치되었는지 확인합니다.

출력 예

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package          Type      Description          Expiration
-----
Base             site      Cluster Base License -

Serial Number: 1-81-000000000000000000000000xx
Owner: cluster1-01
Package          Type      Description          Expiration
-----
NFS              license   NFS License         -
CIFS             license   CIFS License        -
iSCSI            license   iSCSI License       -
FCP              license   FCP License         -
SnapRestore      license   SnapRestore License -
SnapMirror       license   SnapMirror License  -
FlexClone        license   FlexClone License   -
SnapVault        license   SnapVault License   -
SnapManagerSuite license   SnapManagerSuite License -
```

이 예에서는 SnapManagerSuite 라이선스가 설치되었으므로 추가적인 SnapCenter 라이선스 작업이 필요하지 않습니다.

3단계: 컨트롤러 일련 번호 검색

ONTAP 명령줄을 사용하여 컨트롤러 일련 번호를 가져옵니다. 컨트롤러 기반 라이선스 일련 번호를 얻으려면 FAS, AFF 또는 ASA 시스템의 클러스터 관리자가 되어야 합니다.

단계

1. ONTAP 명령줄을 사용하여 컨트롤러에 로그인합니다.
2. `system show -instance` 명령을 입력한 다음 출력을 검토하여 컨트롤러 일련 번호를 찾습니다.

출력 예

```
cluster1::> system show -instance
```

```
Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. 일련번호를 기록하세요.

4단계: 컨트롤러 기반 라이선스의 일련 번호 검색

FAS, ASA 또는 AFF 스토리지를 사용하는 경우 ONTAP 명령줄을 사용하여 설치하기 전에 NetApp 지원 사이트에서 SnapCenter 컨트롤러 기반 라이선스를 검색할 수 있습니다.

시작하기 전에

- 유효한 NetApp 지원 사이트 로그인 자격 증명이 있어야 합니다.

유효한 자격 증명을 입력하지 않으면 시스템은 검색에 대한 어떤 정보도 반환하지 않습니다.

- 컨트롤러 일련번호가 있어야 합니다.

단계

1. 에 로그인하세요 "[NetApp 지원 사이트](#)".
2. 시스템 > *소프트웨어 라이선스*로 이동합니다.
3. 선택 기준 영역에서 일련 번호(장치 뒷면에 있음)가 선택되었는지 확인하고, 컨트롤러 일련 번호를 입력한 다음 *시작!*을 선택합니다.



지정된 컨트롤러에 대한 라이선스 목록이 표시됩니다.

4. SnapCenter Standard 또는 SnapManagerSuite 라이선스를 찾아 기록합니다.

5단계: 컨트롤러 기반 라이선스 추가

FAS, AFF 또는 ASA 시스템을 사용하고 SnapCenter Standard 또는 SnapManagerSuite 라이선스가 있는 경우 ONTAP 명령줄을 사용하여 SnapCenter 컨트롤러 기반 라이선스를 추가할 수 있습니다.

시작하기 전에

- FAS, AFF 또는 ASA 시스템의 클러스터 관리자여야 합니다.
- SnapCenter Standard 또는 SnapManagerSuite 라이선스가 있어야 합니다.

이 작업에 관하여

FAS, AFF 또는 ASA 스토리지를 사용하여 SnapCenter 체험판으로 설치하려는 경우, 컨트롤러에 설치할 수 있는 프리미엄 번들 평가판 라이선스를 얻을 수 있습니다.

SnapCenter 체험판으로 설치하려면 영업 담당자에게 문의하여 컨트롤러에 설치할 수 있는 프리미엄 번들 평가판 라이선스를 받아야 합니다.

단계

1. ONTAP 명령줄을 사용하여 NetApp 클러스터에 로그인합니다.
2. SnapManagerSuite 라이선스 키를 추가합니다.

```
system license add -license-code license_key
```

이 명령은 관리자 권한 수준에서 사용할 수 있습니다.

3. SnapManagerSuite 라이선스가 설치되었는지 확인하세요.

```
license show
```

6단계: 평가판 라이선스 제거

컨트롤러 기반 SnapCenter Standard 라이선스를 사용 중이고 용량 기반 평가판 라이선스(일련 번호가 "50"으로 끝남)를 제거해야 하는 경우 MySQL 명령을 사용하여 평가판 라이선스를 수동으로 제거해야 합니다. 평가판 라이선스는 SnapCenter 사용자 인터페이스를 사용하여 삭제할 수 없습니다.



SnapCenter Standard 컨트롤러 기반 라이선스를 사용하는 경우에만 평가판 라이선스를 수동으로 제거해야 합니다.

단계

1. SnapCenter 서버에서 PowerShell 창을 열어 MySQL 비밀번호를 재설정합니다.

- SnapCenterAdmin 계정에 대한 SnapCenter 서버와의 연결을 설정하려면 Open-SmConnection cmdlet을 실행합니다.
- Set-SmRepositoryPassword를 실행하여 MySQL 비밀번호를 재설정합니다.

cmdlet에 대한 정보는 다음을 참조하세요. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

2. 명령 프롬프트를 열고 mysql -u root -p를 실행하여 MySQL에 로그인합니다.

MySQL에서 비밀번호를 입력하라는 메시지가 표시됩니다. 비밀번호를 재설정할 때 제공한 자격 증명을 입력하세요.

3. 데이터베이스에서 평가판 라이선스를 제거합니다.

```
use nsm;DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
```

고가용성 구성

고가용성을 위한 SnapCenter 서버 구성

Windows 또는 Linux에서 실행되는 SnapCenter 에서 고가용성(HA)을 지원하려면 F5 로드 밸런서를 설치할 수 있습니다. F5를 사용하면 SnapCenter 서버가 동일한 위치에 있는 최대 두 개의 호스트에서 액티브-패시브 구성을 지원할 수 있습니다. SnapCenter 에서 F5 로드 밸런서를 사용하려면 SnapCenter 서버를 구성하고 F5 로드 밸런서를 구성해야 합니다.

SnapCenter 고가용성을 설정하기 위해 네트워크 부하 분산(NLB)을 구성할 수도 있습니다. 고가용성을 위해서는 SnapCenter 설치 외부에서 NLB를 수동으로 구성해야 합니다.

클라우드 환경의 경우 Amazon Web Services(AWS) Elastic Load Balancing(ELB) 및 Azure Load Balancer를 사용하여 고가용성을 구성할 수 있습니다.

F5를 사용하여 고가용성 구성

F5 로드 밸런서를 사용하여 고가용성을 위해 SnapCenter 서버를 구성하는 방법에 대한 지침은 다음을 참조하세요. ["F5 로드 밸런서를 사용하여 고가용성을 위해 SnapCenter 서버를 구성하는 방법"](#).

F5 클러스터를 추가하고 제거하기 위해 다음 cmdlet을 사용하려면 SnapCenter 서버에서 로컬 관리자 그룹의 구성원이어야 합니다(SnapCenterAdmin 역할이 할당되어야 함).

- Add-SmServerCluster
- Add-SmServer
- Remove-SmServerCluster

자세한 내용은 다음을 참조하세요. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

추가 정보

- 고가용성을 위해 SnapCenter 설치하고 구성한 후 SnapCenter 바탕 화면 바로 가기를 편집하여 F5 클러스터 IP를 가리키도록 합니다.
- SnapCenter 서버 간에 장애 조치가 발생하고 기존 SnapCenter 세션이 있는 경우 브라우저를 닫고 SnapCenter에 다시 로그인해야 합니다.
- 로드 밸런서 설정(NLB 또는 F5)에서 NLB 또는 F5 호스트에 의해 부분적으로 해결된 호스트를 추가하고 SnapCenter 호스트가 이 호스트에 연결할 수 없는 경우 SnapCenter 호스트 페이지는 호스트의 다운 상태와 실행 상태 사이를 자주 전환합니다. 이 문제를 해결하려면 두 SnapCenter 호스트가 모두 NLB 또는 F5 호스트에서 호스트를 확인할 수 있는지 확인해야 합니다.
- MFA 설정을 위한 SnapCenter 명령은 모든 호스트에서 실행해야 합니다. 신뢰 당사자 구성은 F5 클러스터 세부 정보를 사용하여 AD FS(Active Directory Federation Services) 서버에서 수행해야 합니다. MFA가 활성화되면 호스트 수준 SnapCenter UI 액세스가 차단됩니다.
- 장애 조치 중에 감사 로그 설정은 두 번째 호스트에 반영되지 않습니다. 따라서 F5 수동 호스트가 활성화되면 감사 로그 설정을 수동으로 반복해야 합니다.

NLB(네트워크 부하 분산)를 사용하여 고가용성 구성

SnapCenter 고가용성을 설정하기 위해 네트워크 부하 분산(NLB)을 구성할 수 있습니다. 고가용성을 위해서는 SnapCenter 설치 외부에서 NLB를 수동으로 구성해야 합니다.

SnapCenter 사용하여 NLB(네트워크 부하 분산)를 구성하는 방법에 대한 정보는 다음을 참조하세요. ["SnapCenter로 NLB를 구성하는 방법"](#).

AWS Elastic Load Balancing(ELB)을 사용하여 고가용성 구성

Amazon Web Services(AWS)에서 두 개의 SnapCenter 서버를 별도의 가용성 영역(AZ)에 설정하고 자동 장애 조치를 구성하여 고가용성 SnapCenter 환경을 구성할 수 있습니다. 아키텍처에는 가상 사설 IP 주소, 라우팅 테이블, 활성 및 대기 MySQL 데이터베이스 간의 동기화가 포함됩니다.

단계

1. AWS에서 가상 사설 오버레이 IP를 구성합니다. 자세한 내용은 다음을 참조하세요. ["가상 사설 오버레이 IP 구성"](#).
2. Windows 호스트 준비
 - a. IPv6보다 IPv4를 우선시하도록 강제합니다.

- 위치: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
 - 키: DisabledComponents
 - 유형: REG_DWORD
 - 값: 0x20
- b. 완전히 정규화된 도메인 이름이 DNS 또는 로컬 호스트 구성을 통해 IPv4 주소로 확인될 수 있는지 확인하세요.
 - c. 시스템 프록시가 구성되어 있지 않은지 확인하세요.
 - d. Active Directory가 없는 설정을 사용하고 서버가 하나의 도메인에 속하지 않는 경우 두 Windows Server에서 관리자 암호가 동일한지 확인하세요.
 - e. 두 Windows 서버에 가상 IP를 추가합니다.
3. SnapCenter 클러스터를 생성합니다.
 - a. PowerShell을 시작하고 SnapCenter 에 연결합니다.
`Open-SmConnection`
 - b. 클러스터를 생성합니다.
`Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`
 - c. 보조 서버를 추가합니다.
`Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`
 - d.고가용성에 대한 세부 정보를 얻으세요.
`Get-SmServerConfig`
 4. AWS CloudWatch에서 모니터링하여 가상 사설 IP 엔드포인트를 사용할 수 없게 될 경우 라우팅 테이블을 조정하는 Lamda 함수를 생성합니다. 자세한 내용은 다음을 참조하세요. ["람다 함수 만들기"](#) .
 5. CloudWatch에서 모니터를 생성하여 SnapCenter 엔드포인트의 가용성을 모니터링합니다. 엔드포인트에 도달할 수 없는 경우 람다 함수를 트리거하도록 알람이 구성됩니다. Lambda 함수는 라우팅 테이블을 조정하여 트래픽을 활성 SnapCenter 서버로 리디렉션합니다. 자세한 내용은 다음을 참조하세요. ["합성 카나리아 만들기"](#) .
 6. CloudWatch 모니터링의 대안으로 단계 함수를 사용하여 워크플로를 구현하면 장애 조치 시간을 단축할 수 있습니다. 워크플로에는 SnapCenter URL을 테스트하는 Lambda 프로브 함수, 실패 횟수를 저장하는 DynamoDB 테이블, Step 함수 자체가 포함됩니다.
 - a. SnapCenter URL을 조사하려면 람다 함수를 사용합니다. 자세한 내용은 다음을 참조하세요. ["람다 함수 생성"](#) .
 - b. 두 Step Function 반복 사이의 실패 횟수를 저장하기 위해 DynamoDB 테이블을 만듭니다. 자세한 내용은 다음을 참조하세요. ["DynamoDB 테이블 시작하기"](#) .
 - c. 계단 함수를 만듭니다. 자세한 내용은 다음을 참조하세요. ["Step Function 문서"](#) .
 - d. 단일 단계를 테스트합니다.
 - e. 전체 기능을 테스트합니다.
 - f. IAM 역할을 생성하고 Lambda 함수를 실행할 수 있는 권한을 조정합니다.
 - g. Step Function을 트리거하기 위한 일정을 만듭니다. 자세한 내용은 다음을 참조하세요. ["Amazon EventBridge Scheduler를 사용하여 Step Functions 시작하기"](#) .

Azure 부하 분산 장치를 사용하여 고가용성 구성

Azure 부하 분산 장치를 사용하여 고가용성 SnapCenter 환경을 구성할 수 있습니다.

단계

1. Azure Portal을 사용하여 확장 집합에서 가상 머신을 만듭니다. Azure 가상 머신 확장 집합을 사용하면 부하 분산된 가상 머신 그룹을 만들고 관리할 수 있습니다. 가상 머신 인스턴스의 수는 수요나 정의된 일정에 따라 자동으로 늘어나거나 줄어든 수 있습니다. 자세한 내용은 다음을 참조하세요. ["Azure Portal을 사용하여 확장 집합에서 가상 머신 만들기"](#).

2. 가상 머신을 구성한 후 VM 세트의 각 가상 머신에 로그인하고 두 노드 모두에 SnapCenter Server를 설치합니다.

3. 호스트 1에 클러스터를 생성합니다.

```
Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>
```

4. 보조 서버를 추가합니다.

```
Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>
```

5. 고가용성 세부 정보를 얻으세요.

```
Get-SmServerConfig
```

6. 필요한 경우 보조 호스트를 다시 빌드합니다.

```
Set-SmRepositoryConfig -RebuildSlave -Verbose
```

7. 두 번째 호스트로 장애 조치합니다.

```
Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose
```

== 고가용성을 위해 NLB에서 F5로 전환

SnapCenter HA 구성을 네트워크 부하 분산(NLB)에서 F5 부하 분산 장치를 사용하도록 변경할 수 있습니다.

단계

1. F5를 사용하여 고가용성을 위해 SnapCenter 서버를 구성합니다. ["자세히 알아보기"](#).
2. SnapCenter 서버 호스트에서 PowerShell을 실행합니다.
3. Open-SmConnection cmdlet을 사용하여 세션을 시작한 다음 자격 증명을 입력합니다.
4. Update-SmServerCluster cmdlet을 사용하여 SnapCenter 서버가 F5 클러스터 IP 주소를 가리키도록 업데이트합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

SnapCenter MySQL 저장소의 고가용성

MySQL 복제는 MySQL 서버의 기능으로, 한 MySQL 데이터베이스 서버(마스터)에서 다른 MySQL 데이터베이스 서버(슬레이브)로 데이터를 복제할 수 있습니다. SnapCenter 두 개의 네트워크 부하 분산(NLB) 지원 노드에서만 고가용성을 위해 MySQL 복제를 지원합니다.

SnapCenter 마스터 저장소에서 읽기 또는 쓰기 작업을 수행하고, 마스터 저장소에 오류가 발생하면 슬레이브 저장소로 연결을 라우팅합니다. 그러면 슬레이브 저장소가 마스터 저장소가 됩니다. SnapCenter 또한 장애 조치 중에만 활성화되는 역방향 복제를 지원합니다.

MySQL 고가용성(HA) 기능을 사용하려면 첫 번째 노드에서 NLB(네트워크 로드 밸런서)를 구성해야 합니다. MySQL 저장소는 설치의 일부로 이 노드에 설치됩니다. 두 번째 노드에 SnapCenter 설치하는 동안 첫 번째 노드의 F5에 가입하고 두 번째 노드에 MySQL 저장소의 복사본을 만들어야 합니다.

SnapCenter MySQL 복제를 관리하기 위한 *Get-SmRepositoryConfig* 및 *Set-SmRepositoryConfig* PowerShell cmdlet을 제공합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

MySQL HA 기능과 관련된 제한 사항을 알고 있어야 합니다.

- NLB와 MySQL HA는 두 개 이상의 노드에서는 지원되지 않습니다.
- SnapCenter 독립 실행형 설치에서 NLB 설치로 전환하거나 그 반대로, MySQL 독립 실행형 설정에서 MySQL HA로 전환하는 것은 지원되지 않습니다.
- 슬레이브 저장소 데이터가 마스터 저장소 데이터와 동기화되지 않으면 자동 장애 조치가 지원되지 않습니다.

Set-SmRepositoryConfig cmdlet을 사용하여 강제 장애 조치를 시작할 수 있습니다.

- 장애 조치가 시작되면 실행 중인 작업이 실패할 수 있습니다.

MySQL 서버나 SnapCenter 서버가 다운되어 장애 조치가 발생하는 경우 실행 중인 모든 작업이 실패할 수 있습니다. 두 번째 노드로 장애 조치한 후 모든 후속 작업이 성공적으로 실행됩니다.

고가용성 구성에 대한 자세한 내용은 다음을 참조하세요. "[SnapCenter 사용하여 NLB 및 ARR을 구성하는 방법](#)".

역할 기반 액세스 제어(RBAC) 구성

역할 만들기

기존 SnapCenter 역할을 사용하는 것 외에도 사용자 고유의 역할을 만들고 권한을 사용자 정의할 수 있습니다.

자신의 역할을 생성하려면 "SnapCenterAdmin" 역할로 로그인해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *역할*을 클릭합니다.
3. 딸깍 하는 소리 .
4. 새 역할에 대한 이름과 설명을 지정합니다.



사용자 이름과 그룹 이름에는 공백(), 하이픈(-), 밑줄(_), 콜론(:) 등의 특수 문자만 사용할 수 있습니다.

5. *이 역할의 모든 구성원은 다른 구성원의 개체를 볼 수 있음*을 선택하면 해당 역할의 다른 구성원이 리소스 목록을 새로 고침 후 볼륨 및 호스트와 같은 리소스를 볼 수 있습니다.

이 역할의 멤버가 다른 멤버에게 할당된 개체를 보지 못하도록 하려면 이 옵션의 선택을 해제해야 합니다.



이 옵션을 활성화하면 사용자가 개체나 리소스를 만든 사용자와 동일한 역할에 속해 있는 경우 개체나 리소스에 대한 액세스 권한을 사용자에게 할당할 필요가 없습니다.

6. 권한 페이지에서 역할에 할당할 권한을 선택하거나 *모두 선택*을 클릭하여 역할에 모든 권한을 부여합니다.
7. *제출*을 클릭하세요.

보안 로그인 명령을 사용하여 **NetApp ONTAP RBAC** 역할 추가

스토리지 시스템에서 클러스터형 ONTAP 실행하는 경우 보안 로그인 명령을 사용하여 NetApp ONTAP RBAC 역할을 추가할 수 있습니다.

시작하기 전에

- 수행하고자 하는 작업(들)과 해당 작업을 수행하는 데 필요한 권한을 확인하세요.
- 명령 및/또는 명령 디렉토리에 권한을 부여합니다.

각 명령/명령 디렉토리에는 모든 액세스와 읽기 전용의 두 가지 액세스 수준이 있습니다.

항상 모든 접근 권한을 먼저 할당해야 합니다.

- 사용자에게 역할을 할당합니다.
- SnapCenter 플러그인이 전체 클러스터의 클러스터 관리자 IP에 연결되어 있는지, 아니면 클러스터 내의 SVM에 직접 연결되어 있는지에 따라 구성을 식별합니다.

이 작업에 관하여

스토리지 시스템에서 이러한 역할의 구성을 간소화하려면 NetApp 커뮤니티 포럼에 게시된 NetApp ONTAP 도구용 RBAC 사용자 생성기를 사용하면 됩니다.

이 도구는 ONTAP 권한을 올바르게 설정하는 작업을 자동으로 처리합니다. 예를 들어, NetApp ONTAP 도구용 RBAC User Creator는 모든 액세스 권한이 먼저 나타나도록 올바른 순서로 권한을 자동으로 추가합니다. 먼저 읽기 전용 권한을 추가한 다음 모든 액세스 권한을 추가하면 ONTAP 모든 액세스 권한을 중복으로 표시하고 무시합니다.



나중에 SnapCenter 또는 ONTAP 업그레이드하는 경우 NetApp ONTAP 도구용 RBAC User Creator를 다시 실행하여 이전에 만든 사용자 역할을 업데이트해야 합니다. 이전 버전의 SnapCenter 또는 ONTAP에서 생성된 사용자 역할은 업그레이드된 버전에서는 제대로 작동하지 않습니다. 도구를 다시 실행하면 자동으로 업그레이드가 처리됩니다. 역할을 다시 만들 필요는 없습니다.

ONTAP RBAC 역할 설정에 대한 자세한 내용은 다음을 참조하세요. ["ONTAP 9 관리자 인증 및 RBAC 전원 가이드"](#).

단계

1. 스토리지 시스템에서 다음 명령을 입력하여 새 역할을 만듭니다.

```
security login role create <role_name> -cmddirname "command" -access all  
-vserver <svm_name>
```

- svm_name은 SVM의 이름입니다. 이 항목을 비워 두면 기본적으로 클러스터 관리자가 됩니다.
- role_name은 역할에 지정하는 이름입니다.
- 명령은 ONTAP 기능입니다.



각 권한에 대해 이 명령을 반복해야 합니다. 모든 액세스 명령은 읽기 전용 명령보다 먼저 나열되어야 한다는 점을 기억하세요.

권한 목록에 대한 정보는 다음을 참조하세요. "[역할 생성 및 권한 할당을 위한 ONTAP CLI 명령](#)".

2. 다음 명령을 입력하여 사용자 이름을 만듭니다.

```
security login create -username <user_name\> -application ontapi -authmethod
<password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
"user_description"
```

- user_name은 생성하려는 사용자의 이름입니다.
- <password>는 귀하의 비밀번호입니다. 비밀번호를 지정하지 않으면 시스템에서 비밀번호를 입력하라고 요청합니다.
- svm_name은 SVM의 이름입니다.

3. 다음 명령을 입력하여 사용자에게 역할을 할당합니다.

```
security login modify username <user_name\> -vserver <svm_name\> -role
<role_name\> -application ontapi -application console -authmethod <password\>
```

- <user_name>은 2단계에서 생성한 사용자의 이름입니다. 이 명령을 사용하면 사용자를 수정하여 역할과 연결할 수 있습니다.
- <svm_name>은 SVM의 이름입니다.
- <role_name>은 1단계에서 만든 역할의 이름입니다.
- <password>는 귀하의 비밀번호입니다. 비밀번호를 지정하지 않으면 시스템에서 비밀번호를 입력하라고 요청합니다.

4. 다음 명령을 입력하여 사용자가 올바르게 생성되었는지 확인하세요.

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

user_name은 3단계에서 생성한 사용자의 이름입니다.

최소 권한으로 SVM 역할 생성

ONTAP 에서 새로운 SVM 사용자에게 대한 역할을 생성할 때 실행해야 하는 ONTAP CLI 명령이 여러 개 있습니다. ONTAP 에서 SVM을 구성하여 SnapCenter 와 함께 사용하고 vsadmin 역할을 사용하지 않으려는 경우 이 역할이 필요합니다.

단계

1. 스토리지 시스템에서 역할을 만들고 해당 역할에 모든 권한을 할당합니다.

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>  
-cmddirname <permission\>
```



각 권한에 대해 이 명령을 반복해야 합니다.

2. 사용자를 만들고 해당 사용자에게 역할을 할당합니다.

```
security login create -user <user_name\> -vserver <svm_name\> -application  
ontapi -authmethod password -role <SVM_Role_Name\>
```

3. 사용자의 잠금을 해제합니다.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

SVM 역할 생성 및 권한 할당을 위한 ONTAP CLI 명령

SVM 역할을 생성하고 권한을 할당하려면 실행해야 하는 ONTAP CLI 명령이 여러 개 있습니다.

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```

"snapmirror update" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror update-ls-set" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "version" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone split start" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone split stop" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume destroy" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume file clone create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume file show-disk-usage" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume modify" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume offline" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume online" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree delete" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree modify" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume restrict" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot create" -access all

```


- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```

"vserver export-policy" -access all

```

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all

ASA r2 시스템에 대한 SVM 역할 생성

ASA r2 시스템에서 새로운 SVM 사용자에게 대한 역할을 생성하려면 실행해야 하는 여러 가지 ONTAP CLI 명령이 있습니다. SnapCenter 와 함께 사용하기 위해 ASA r2 시스템에서 SVM을 구성하고 vsadmin 역할을 사용하지 않으려는 경우 이 역할이 필요합니다.

단계

1. 스토리지 시스템에서 역할을 만들고 해당 역할에 모든 권한을 할당합니다.

```

security login role create -vserver <svm_name>- role <SVM_Role_Name>
-cmddirname <permission>

```



각 권한에 대해 이 명령을 반복해야 합니다.

2. 사용자를 만들고 해당 사용자에게 역할을 할당합니다.

```
security login create -user <user_name\> -vserver <svm_name\> -application
http -authmethod password -role <SVM_Role_Name\>
```

3. 사용자의 잠금을 해제합니다.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

SVM 역할 생성 및 권한 할당을 위한 ONTAP CLI 명령

SVM 역할을 생성하고 권한을 할당하려면 실행해야 하는 ONTAP CLI 명령이 여러 개 있습니다.

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```
"snapmirror update-ls-set" -access all
```

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```

"vserver iscsi" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "volume clone split status" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume managed-feature" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem map" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem create" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem delete" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem modify" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem host" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem controller" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem show" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme namespace create" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme namespace delete" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme namespace modify" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme namespace show" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "storage-unit show" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "consistency-group" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "snapmirror protect" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "volume delete" -access all

• security login create -user-or-group-name user_name -application http
  -authentication-method password -role SVM_Role_Name -vserver SVM_Name

• security login create -user-or-group-name user_name -application ssh
  -authentication-method password -role SVM_Role_Name -vserver SVM_Name

```

최소 권한으로 **ONTAP** 클러스터 역할 생성

SnapCenter 에서 작업을 수행하기 위해 ONTAP 관리자 역할을 사용하지 않아도 되도록 최소한의 권한이 있는 ONTAP 클러스터 역할을 만들어야 합니다. 여러 ONTAP CLI 명령을 실행하여 ONTAP 클러스터 역할을 만들고 최소 권한을 할당할 수 있습니다.

단계

1. 스토리지 시스템에서 역할을 만들고 해당 역할에 모든 권한을 할당합니다.

```
security login role create -vserver <cluster_name>- role <role_name>  
-cmddirname <permission>
```



각 권한에 대해 이 명령을 반복해야 합니다.

2. 사용자를 만들고 해당 사용자에게 역할을 할당합니다.

```
security login create -user <user_name> -vserver <cluster_name> -application  
ontapi http -authmethod password -role <role_name>
```

3. 사용자의 잠금을 해제합니다.

```
security login unlock -user <user_name> -vserver <cluster_name>
```

클러스터 역할 생성 및 권한 할당을 위한 **ONTAP CLI** 명령

클러스터 역할을 만들고 권한을 할당하려면 실행해야 하는 ONTAP CLI 명령이 여러 개 있습니다.

- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"lun resize" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun serial" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface create" -access readonly

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface delete" -access readonly

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface modify" -access readonly

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface show" -access readonly

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem map" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem host" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem controller" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "security login" -access readonly

• security login role create -role Role_Name -cmddirname "snapmirror create"
  -vserver Cluster_name -access all

• security login role create -role Role_Name -cmddirname "snapmirror list-
  destinations" -vserver Cluster_name -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"version" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone split start" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone split stop" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume destroy" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume file clone create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume file show-disk-usage" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot modify-snaplock-expiry-time" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume offline" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume online" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume restrict" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot delete" -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```
"vserver export-policy delete" -access all
```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all

ASA r2 시스템에 대한 ONTAP 클러스터 역할 생성

SnapCenter 에서 작업을 수행하기 위해 ONTAP 관리자 역할을 사용하지 않아도 되도록 최소한의 권한이 있는 ONTAP 클러스터 역할을 만들어야 합니다. 여러 ONTAP CLI 명령을 실행하여 ONTAP 클러스터 역할을 만들고 최소 권한을 할당할 수 있습니다.

단계

1. 스토리지 시스템에서 역할을 만들고 해당 역할에 모든 권한을 할당합니다.

```
security login role create -vserver <cluster_name>- role <role_name>  
-cmddirname <permission>
```



각 권한에 대해 이 명령을 반복해야 합니다.

2. 사용자를 만들고 해당 사용자에게 역할을 할당합니다.

```
security login create -user <user_name> -vserver <cluster_name> -application  
http -authmethod password -role <role_name>
```

3. 사용자의 잠금을 해제합니다.

```
security login unlock -user <user_name> -vserver <cluster_name>
```

클러스터 역할 생성 및 권한 할당을 위한 ONTAP CLI 명령

클러스터 역할을 만들고 권한을 할당하려면 실행해야 하는 ONTAP CLI 명령이 여러 개 있습니다.

- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"lun mapping create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun mapping delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun mapping remove-reporting-nodes" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun mapping show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun move-in-volume" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun offline" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun online" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun persistent-reservation clear" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun resize" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun serial" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface create" -access readonly
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface delete" -access readonly
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface modify" -access readonly
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface show" -access readonly
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem map" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem host" -access all

```


- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```
"snapmirror update-ls-set" -access all
```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"vserver cifs modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs share modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs share create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs share delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs share modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs share show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy rule create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy rule delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy rule modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy rule show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver iscsi connection show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "storage-unit show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "consistency-group" show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror protect" show" -access all

```

```
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume delete" show" -access all
```

사용자 또는 그룹을 추가하고 역할과 자산을 할당합니다.

SnapCenter 사용자에게 대한 역할 기반 액세스 제어를 구성하려면 사용자나 그룹을 추가하고 역할을 할당하면 됩니다. 역할은 SnapCenter 사용자가 액세스할 수 있는 옵션을 결정합니다.

시작하기 전에

- "SnapCenterAdmin" 역할로 로그인해야 합니다.
- 운영 체제나 데이터베이스의 Active Directory에서 사용자 또는 그룹 계정을 만들어야 합니다. SnapCenter 사용하여 이러한 계정을 만들 수 없습니다.



사용자 이름과 그룹 이름에는 공백(), 하이픈(-), 밑줄(_), 콜론(:) 등의 특수 문자만 사용할 수 있습니다.

- SnapCenter 에는 미리 정의된 역할이 여러 개 포함되어 있습니다.

사용자에게 이러한 역할을 할당하거나 새로운 역할을 만들 수 있습니다.

- SnapCenter RBAC에 추가된 AD 사용자와 AD 그룹에는 Active Directory의 사용자 컨테이너와 컴퓨터 컨테이너에 대한 읽기 권한이 있어야 합니다.
- 적절한 권한이 포함된 역할을 사용자 또는 그룹에 할당한 후에는 호스트 및 스토리지 연결과 같은 SnapCenter 자산에 대한 사용자 액세스 권한을 할당해야 합니다.

이를 통해 사용자는 자신에게 할당된 자산에 대해 권한이 있는 작업을 수행할 수 있습니다.

- RBAC 권한과 효율성을 활용하려면 언젠가는 사용자나 그룹에 역할을 할당해야 합니다.
- 사용자 또는 그룹을 생성하는 동안 호스트, 리소스 그룹, 정책, 스토리지 연결, 플러그인, 자격 증명과 같은 자산을 사용자에게 할당할 수 있습니다.
- 특정 작업을 수행하기 위해 사용자에게 할당해야 하는 최소 자산은 다음과 같습니다.

작업	자산 할당
자원을 보호하세요	호스트, 정책
지원	호스트, 리소스 그룹, 정책
복원하다	호스트, 리소스 그룹
복제	호스트, 리소스 그룹, 정책
클론 라이프사이클	주인
리소스 그룹 만들기	주인

- Windows 클러스터 또는 DAG(Exchange Server Database Availability Group) 자산에 새 노드가 추가되고 이 새 노드가 사용자에게 할당된 경우 새 노드를 사용자 또는 그룹에 포함하려면 자산을 사용자 또는 그룹에 다시 할당해야 합니다.

새 노드를 RBAC 사용자 또는 그룹에 포함하려면 RBAC 사용자 또는 그룹을 클러스터 또는 DAG에 다시 할당해야 합니다. 예를 들어, 2노드 클러스터가 있고 해당 클러스터에 RBAC 사용자나 그룹을 할당했다고 가정해 보겠습니다. 클러스터에 다른 노드를 추가하는 경우 RBAC 사용자 또는 그룹에 새 노드를 포함하도록 RBAC 사용자 또는 그룹을 클러스터에 다시 할당해야 합니다.

- 스냅샷을 복제하려는 경우 작업을 수행하는 사용자에게 소스 볼륨과 대상 볼륨 모두에 대한 스토리지 연결을 할당해야 합니다.

사용자에게 액세스 권한을 할당하기 전에 자산을 추가해야 합니다.



SnapCenter Plug-in for VMware vSphere 기능을 사용하여 VM, VMDK 또는 데이터 저장소를 보호하는 경우 VMware vSphere GUI를 사용하여 vCenter 사용자를 SnapCenter Plug-in for VMware vSphere 역할에 추가해야 합니다. VMware vSphere 역할에 대한 정보는 다음을 참조하세요. "[SnapCenter Plug-in for VMware vSphere](#) 과 함께 제공되는 미리 정의된 역할".

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 사용자 및 액세스 > *를 클릭합니다.  *.
3. Active Directory 또는 작업 그룹에서 사용자/그룹 추가 페이지에서:

이 분야에서는...	이렇게 하세요...
접근 유형	도메인 또는 작업 그룹을 선택하세요 도메인 인증 유형의 경우, 사용자를 역할에 추가할 사용자 또는 그룹의 도메인 이름을 지정해야 합니다. 기본적으로 로그인한 도메인 이름이 미리 채워져 있습니다.  신뢰할 수 없는 도메인은 설정 > 전역 설정 > 도메인 설정 페이지에서 등록해야 합니다.
유형	사용자 또는 그룹을 선택하세요  SnapCenter 보안 그룹만 지원하고 배포 그룹은 지원하지 않습니다.

이 분야에서는...	이렇게 하세요...
사용자 이름	a. 사용자 이름의 일부를 입력한 다음 *추가*를 클릭합니다.  사용자 이름은 대소문자를 구분합니다. b. 검색 목록에서 사용자 이름을 선택하세요.  다른 도메인이나 신뢰할 수 없는 도메인의 사용자를 추가하는 경우 크로스 도메인 사용자에 대한 검색 목록이 없으므로 사용자 이름을 모두 입력해야 합니다. 선택한 역할에 추가 사용자나 그룹을 추가하려면 이 단계를 반복합니다.
역할	사용자를 추가할 역할을 선택하세요.

4. *할당*을 클릭한 다음 자산 할당 페이지에서 다음을 수행합니다.

- 자산 드롭다운 목록에서 자산 유형을 선택하세요.
- 자산 테이블에서 자산을 선택합니다.

사용자가 SnapCenter 에 자산을 추가한 경우에만 자산이 나열됩니다.

- 필요한 모든 자산에 대해 이 절차를 반복합니다.
- *저장*을 클릭하세요.

5. *제출*을 클릭하세요.

사용자 또는 그룹을 추가하고 역할을 할당한 후 리소스 목록을 새로 고칩니다.

감사 로그 설정 구성

SnapCenter 서버의 모든 활동에 대해 감사 로그가 생성됩니다. 기본적으로 감사 로그는 기본 설치 위치인 `_C:\Program Files\ NetApp\ SnapCenter WebApp\audit\_`에 보관됩니다.

감사 로그는 각 감사 이벤트에 대해 디지털 서명된 다이제스트를 생성하여 보안을 유지함으로써 무단 수정으로부터 보호됩니다. 생성된 다이제스트는 별도의 감사 체크섬 파일에 유지 관리되며, 콘텐츠의 무결성을 보장하기 위해 주기적인 무결성 검사를 거칩니다.

"SnapCenterAdmin" 역할로 로그인했어야 합니다.

이 작업에 관하여

- 알림은 다음과 같은 시나리오에서 전송됩니다.

- 감사 로그 무결성 검사 일정 또는 Syslog 서버가 활성화 또는 비활성화되었습니다.
- 감사 로그 무결성 검사, 감사 로그 또는 Syslog 서버 로그 실패
- 디스크 공간 부족
- 무결성 검사에 실패한 경우에만 이메일이 전송됩니다.
- 감사 로그 디렉토리와 감사 체크섬 로그 디렉토리 경로를 함께 수정해야 합니다. 그 중 하나만 수정할 수는 없습니다.
- 감사 로그 디렉토리와 감사 체크섬 로그 디렉토리 경로가 수정되면 이전 위치에 있는 감사 로그에 대한 무결성 검사를 수행할 수 없습니다.
- 감사 로그 디렉토리와 감사 체크섬 로그 디렉토리 경로는 SnapCenter Server의 로컬 드라이브에 있어야 합니다.

공유 또는 네트워크 마운트 드라이브는 지원되지 않습니다.

- Syslog 서버 설정에서 UDP 프로토콜을 사용하는 경우 포트가 다운되거나 사용할 수 없어 발생하는 오류는 SnapCenter 에서 오류나 알림으로 캡처될 수 없습니다.
- Set-SmAuditSettings 및 Get-SmAuditSettings 명령을 사용하여 감사 로그를 구성할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 Get-Help command_name을 실행하여 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. 설정 페이지에서 설정 > 전역 설정 > *감사 로그 설정*으로 이동합니다.
2. 감사 로그 섹션에 세부 정보를 입력합니다.
3. 감사 로그 디렉토리 및 *감사 체크섬 로그 디렉토리*를 입력합니다.
 - a. 최대 파일 크기를 입력하세요
 - b. 최대 로그 파일 입력
 - c. 알림을 보내려면 디스크 공간 사용량의 백분율을 입력하세요.
4. (선택 사항) *UTC 시간 기록*을 활성화합니다.
5. (선택 사항) *감사 로그 무결성 검사 일정*을 활성화하고 주문형 무결성 검사를 위해 *무결성 검사 시작*을 클릭합니다.

Start-SmAuditIntegrityCheck 명령을 실행하여 주문형 무결성 검사를 시작할 수도 있습니다.

6. (선택 사항) 원격 Syslog 서버로 감사 로그 전달을 활성화하고 Syslog 서버 세부 정보를 입력합니다.

TLS 1.2 프로토콜의 경우 Syslog 서버에서 '신뢰할 수 있는 루트'로 인증서를 가져와야 합니다.

 - a. Syslog 서버 호스트 입력
 - b. Syslog 서버 포트를 입력하세요
 - c. Syslog 서버 프로토콜 입력
 - d. RFC 형식 입력
7. *저장*을 클릭하세요.
8. 모니터 > *작업*을 클릭하면 감사 무결성 검사와 디스크 공간 검사를 볼 수 있습니다.

SnapCenter Server를 사용하여 보안된 MySQL 연결 구성

독립형 구성이나 NLB(네트워크 부하 분산) 구성에서 SnapCenter Server와 MySQL Server 간 통신을 보호하려면 SSL(Secure Sockets Layer) 인증서와 키 파일을 생성할 수 있습니다.

독립형 SnapCenter 서버 구성을 위한 보안 MySQL 연결 구성

SnapCenter Server와 MySQL Server 간 통신을 보호하려면 SSL(Secure Sockets Layer) 인증서와 키 파일을 생성할 수 있습니다. MySQL 서버와 SnapCenter 서버에서 인증서와 키 파일을 구성해야 합니다.

다음 인증서가 생성됩니다.

- CA 인증서
- 서버 공개 인증서 및 개인 키 파일
- 클라이언트 공개 인증서 및 개인 키 파일

단계

1. openssl 명령을 사용하여 Windows에서 MySQL 서버와 클라이언트에 대한 SSL 인증서와 키 파일을 설정합니다.

자세한 내용은 다음을 참조하세요. ["MySQL 버전 5.7: openssl을 사용하여 SSL 인증서 및 키 생성"](#)



서버 인증서, 클라이언트 인증서 및 키 파일에 사용되는 일반 이름 값은 각각 CA 인증서에 사용되는 일반 이름 값과 달라야 합니다. 일반 이름 값이 동일하면 OpenSSL을 사용하여 컴파일된 서버의 인증서 및 키 파일이 실패합니다.

모범 사례: 서버 인증서의 일반 이름으로 서버의 정규화된 도메인 이름(FQDN)을 사용해야 합니다.

2. SSL 인증서와 키 파일을 MySQL 데이터 폴더로 복사합니다.

기본 MySQL 데이터 폴더 경로는 다음과 같습니다. C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

3. MySQL 서버 구성 파일(my.ini)에서 CA 인증서, 서버 공개 인증서, 클라이언트 공개 인증서, 서버 개인 키, 클라이언트 개인 키 경로를 업데이트합니다.

기본 MySQL 서버 구성 파일(my.ini) 경로는 다음과 같습니다.

C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini.



MySQL 서버 설정 파일(my.ini)의 [mysqld] 섹션에서 CA 인증서, 서버 공개 인증서, 서버 개인 키 경로를 지정해야 합니다.

MySQL 서버 구성 파일(my.ini)의 [client] 섹션에서 CA 인증서, 클라이언트 공개 인증서 및 클라이언트 개인 키 경로를 지정해야 합니다.

다음 예제는 기본 폴더의 my.ini 파일의 [mysqld] 섹션에 복사된 인증서 및 키 파일을 보여줍니다.

C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data .

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

다음 예제는 my.ini 파일의 [client] 섹션에서 업데이트된 경로를 보여줍니다.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
key.pem"
```

4. IIS(인터넷 정보 서버)에서 SnapCenter 서버 웹 애플리케이션을 중지합니다.
5. MySQL 서비스를 다시 시작합니다.
6. SnapManager.Web.UI.dll.config 파일에서 MySQLProtocol 키 값을 업데이트합니다.

다음 예제에서는 SnapManager.Web.UI.dll.config 파일에서 업데이트된 MySQLProtocol 키 값을 보여줍니다.

```
<add key="MySQLProtocol" value="SSL" />
```

7. [client] 섹션의 my.ini 파일에 제공된 경로로 SnapManager.Web.UI.dll.config 파일을 업데이트합니다.

다음 예제는 my.ini 파일의 [client] 섹션에서 업데이트된 경로를 보여줍니다.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

8. IIS에서 SnapCenter Server 웹 애플리케이션을 시작합니다.

HA 구성을 위한 보안 MySQL 연결 구성

SnapCenter 서버와 MySQL 서버 간 통신을 보호하려면고가용성(HA) 노드 둘 다에 대한 SSL(Secure Sockets Layer) 인증서와 키 파일을 생성할 수 있습니다. MySQL 서버와 HA 노드에서 인증서와 키 파일을 구성해야 합니다.

다음 인증서가 생성됩니다.

- CA 인증서

HA 노드 중 하나에서 CA 인증서가 생성되고, 이 CA 인증서가 다른 HA 노드에 복사됩니다.

- 두 HA 노드 모두에 대한 서버 공개 인증서 및 서버 개인 키 파일
- 두 HA 노드에 대한 클라이언트 공개 인증서 및 클라이언트 개인 키 파일

단계

1. 첫 번째 HA 노드의 경우 openssl 명령을 사용하여 Windows의 MySQL 서버와 클라이언트에 대한 SSL 인증서와 키 파일을 설정합니다.

자세한 내용은 다음을 참조하세요. "[MySQL 버전 5.7: openssl을 사용하여 SSL 인증서 및 키 생성](#)"



서버 인증서, 클라이언트 인증서 및 키 파일에 사용되는 일반 이름 값은 각각 CA 인증서에 사용되는 일반 이름 값과 달라야 합니다. 일반 이름 값이 동일하면 OpenSSL을 사용하여 컴파일된 서버의 인증서 및 키 파일이 실패합니다.

모범 사례: 서버 인증서의 일반 이름으로 서버의 정규화된 도메인 이름(FQDN)을 사용해야 합니다.

2. SSL 인증서와 키 파일을 MySQL 데이터 폴더로 복사합니다.

기본 MySQL 데이터 폴더 경로는 C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data입니다.

3. MySQL 서버 구성 파일(my.ini)에서 CA 인증서, 서버 공개 인증서, 클라이언트 공개 인증서, 서버 개인 키, 클라이언트 개인 키 경로를 업데이트합니다.

기본 MySQL 서버 구성 파일(my.ini) 경로는 C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini입니다.



MySQL 서버 설정 파일(my.ini)의 [mysqld] 섹션에서 CA 인증서, 서버 공개 인증서, 서버 개인 키 경로를 지정해야 합니다.

MySQL 서버 설정 파일(my.ini)의 [client] 섹션에서 CA 인증서, 클라이언트 공개 인증서, 클라이언트 개인 키 경로를 지정해야 합니다.

다음 예제에서는 기본 폴더인 C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data에 있는 my.ini 파일의 [mysqld] 섹션에 복사된 인증서와 키 파일을 보여줍니다.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

다음 예제는 my.ini 파일의 [client] 섹션에서 업데이트된 경로를 보여줍니다.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
key.pem"
```

4. 두 번째 HA 노드의 경우 CA 인증서를 복사하고 서버 공개 인증서, 서버 개인 키 파일, 클라이언트 공개 인증서, 클라이언트 개인 키 파일을 생성합니다. 다음 단계를 수행합니다.

- a. 첫 번째 HA 노드에서 생성된 CA 인증서를 두 번째 NLB 노드의 MySQL 데이터 폴더로 복사합니다.

기본 MySQL 데이터 폴더 경로는 C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\입니다.



CA 인증서를 다시 생성해서는 안 됩니다. 서버 공개 인증서, 클라이언트 공개 인증서, 서버 개인 키 파일, 클라이언트 개인 키 파일만 생성해야 합니다.

- b. 첫 번째 HA 노드의 경우 openssl 명령을 사용하여 Windows의 MySQL 서버와 클라이언트에 대한 SSL 인증서와 키 파일을 설정합니다.

"MySQL 버전 5.7: openssl을 사용하여 SSL 인증서 및 키 생성"



서버 인증서, 클라이언트 인증서 및 키 파일에 사용되는 일반 이름 값은 각각 CA 인증서에 사용되는 일반 이름 값과 달라야 합니다. 일반 이름 값이 동일하면 OpenSSL을 사용하여 컴파일된 서버의 인증서 및 키 파일이 실패합니다.

서버 인증서의 일반 이름으로 서버 FQDN을 사용하는 것이 좋습니다.

- c. SSL 인증서와 키 파일을 MySQL 데이터 폴더로 복사합니다.

- d. MySQL 서버 구성 파일(my.ini)에서 CA 인증서, 서버 공개 인증서, 클라이언트 공개 인증서, 서버 개인 키, 클라이언트 개인 키 경로를 업데이트합니다.



MySQL 서버 설정 파일(my.ini)의 [mysqld] 섹션에서 CA 인증서, 서버 공개 인증서, 서버 개인 키 경로를 지정해야 합니다.

MySQL 서버 구성 파일(my.ini)의 [client] 섹션에서 CA 인증서, 클라이언트 공개 인증서 및 클라이언트 개인 키 경로를 지정해야 합니다.

다음 예제에서는 기본 폴더인 C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data에 있는 my.ini 파일의 [mysqld] 섹션에 복사된 인증서와 키 파일을 보여줍니다.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

다음 예제는 my.ini 파일의 [client] 섹션에서 업데이트된 경로를 보여줍니다.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

5. 두 HA 노드 모두에서 IIS(인터넷 정보 서버)의 SnapCenter 서버 웹 애플리케이션을 중지합니다.
6. 두 HA 노드에서 MySQL 서비스를 다시 시작합니다.
7. 두 HA 노드 모두의 SnapManager.Web.UI.dll.config 파일에서 MySQLProtocol 키 값을 업데이트합니다.

다음 예제는 SnapManager.Web.UI.dll.config 파일에서 업데이트된 MySQLProtocol 키 값을 보여줍니다.

```
<add key="MySQLProtocol" value="SSL" />
```

8. HA 노드 둘 다에 대한 my.ini 파일의 [client] 섹션에 지정한 경로로 SnapManager.Web.UI.dll.config 파일을 업데이트합니다.

다음 예제는 my.ini 파일의 [client] 섹션에서 업데이트된 경로를 보여줍니다.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/ca.pem" />
```

9. 두 HA 노드 모두의 IIS에서 SnapCenter 서버 웹 애플리케이션을 시작합니다.
10. HA 노드 중 하나에서 -Force 옵션과 함께 Set-SmRepositoryConfig -RebuildSlave -Force PowerShell cmdlet을 사용하여 두 HA 노드 모두에서 보안된 MySQL 복제를 설정합니다.

복제 상태가 정상이더라도 -Force 옵션을 사용하면 슬레이브 저장소를 다시 빌드할 수 있습니다.

인증서 기반 인증 구성

인증서 기반 인증은 SnapCenter 서버와 플러그인 호스트의 신원을 확인하여 보안을 강화하고 안전하고 암호화된 통신을 보장합니다.

인증서 기반 인증 활성화

SnapCenter 서버와 Windows 플러그인 호스트에 대한 인증서 기반 인증을 활성화하려면 다음 PowerShell cmdlet을 실행합니다. Linux 플러그인 호스트의 경우, 양방향 SSL을 활성화하면 인증서 기반 인증이 활성화됩니다.

- 클라이언트 인증서 기반 인증을 활성화하려면:

```
Set-SmConfigSettings -Agent -configSettings  
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- 클라이언트 인증서 기반 인증을 비활성화하려면:

```
Set-SmConfigSettings -Agent -configSettings  
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

SnapCenter 서버에서 인증 기관(CA) 인증서 내보내기

Microsoft 관리 콘솔(MMC)을 사용하여 SnapCenter 서버에서 플러그인 호스트로 CA 인증서를 내보내야 합니다.

시작하기 전에

양방향 SSL을 구성했어야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.
2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
3. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 개인 > *인증서*를 클릭합니다.
5. SnapCenter Server에 사용되는 구매한 CA 인증서를 마우스 오른쪽 버튼으로 클릭한 다음 모든 작업 > *내보내기*를 선택하여 내보내기 마법사를 시작합니다.
6. 마법사에서 다음 작업을 수행합니다.

이 옵션의 경우...	다음을 수행하세요...
개인 키 내보내기	*아니요, 개인 키를 내보내지 않습니다*를 선택한 후 *다음*을 클릭합니다.
내보내기 파일 형식	*다음*을 클릭하세요.
파일 이름	*찾아보기*를 클릭하고 인증서를 저장할 파일 경로를 지정한 후 *다음*을 클릭합니다.
인증서 내보내기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 내보내기를 시작합니다.



SnapCenter HA 구성 및 SnapCenter Plug-in for VMware vSphere 인증서 기반 인증이 지원되지 않습니다.

Windows 플러그인 호스트에 CA 인증서 가져오기

내보낸 SnapCenter 서버 CA 인증서를 사용하려면 Microsoft 관리 콘솔(MMC)을 사용하여 관련 인증서를 SnapCenter Windows 플러그인 호스트로 가져와야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.
2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
3. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 개인 > *인증서*를 클릭합니다.

5. "개인" 폴더를 마우스 오른쪽 버튼으로 클릭한 다음, 모든 작업 > *가져오기*를 선택하여 가져오기 마법사를 시작합니다.
6. 마법사에서 다음 작업을 수행합니다.

이 옵션의 경우...	다음을 수행하세요...
매장 위치	*다음*을 클릭하세요.
가져올 파일	
인증서 저장소	*다음*을 클릭하세요.
인증서 내보내기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.

UNIX 플러그인 호스트로 CA 인증서 가져오기

CA 인증서를 UNIX 플러그인 호스트로 가져와야 합니다.

이 작업에 관하여

- SPL 키 저장소의 비밀번호와 사용 중인 CA 서명 키 쌍의 별칭을 관리할 수 있습니다.
- SPL 키 저장소의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

단계

1. SPL 속성 파일에서 SPL 키 저장소 기본 비밀번호를 검색할 수 있습니다. 키에 해당하는 값입니다
SPL_KEYSTORE_PASS .
2. 키스토어 비밀번호를 변경하세요:
\$ keytool -storepasswd -keystore keystore.jks
3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.
\$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
4. SPL_KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다. spl.properties` 파일.
5. 비밀번호를 변경한 후 서비스를 다시 시작하세요.

SPL 신뢰 저장소에 루트 또는 중간 인증서 구성

루트 또는 중간 인증서를 SPL 신뢰 저장소로 구성해야 합니다. 루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

단계

1. SPL 키 저장소가 포함된 폴더로 이동합니다. /var/opt/snapcenter/spl/etc .
2. 파일을 찾으세요 keystore.jks .

3. 키 저장소에 추가된 인증서를 나열합니다.

```
$ keytool -list -v -keystore keystore.jks
```

4. 루트 또는 중간 인증서를 추가합니다.

```
$ keytool -import -trustcacerts -alias <AliasNameForCertificateToBeImported>  
-file /<CertificatePath> -keystore keystore.jks
```

5. 루트 또는 중간 인증서를 SPL 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

SPL 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 SPL 신뢰 저장소로 구성해야 합니다.

단계

1. SPL 키 저장소가 포함된 폴더로 이동합니다. /var/opt/snapcenter/spl/etc .

2. 파일을 찾으세요 keystore.jks` .

3. 키 저장소에 추가된 인증서를 나열합니다.

```
$ keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype  
pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

```
$ keytool -list -v -keystore keystore.jks
```

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.

7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 SPL 키 저장소 비밀번호는 SPL_KEYSTORE_PASS 키의 값입니다. spl.properties 파일.

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore  
keystore.jks`
```

8. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자(" ", ";", ",")가 포함된 경우 별칭 이름을 간단한 이름으로 변경합니다.

```
$ keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>"  
-keystore keystore.jks`
```

9. 키 저장소에서 별칭 이름을 구성합니다. spl.properties 파일. 이 값을 SPL_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

10. CA 서명 키 쌍을 SPL 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

SnapCenter 인증서 내보내기

SnapCenter 인증서는 .pfx 형식으로 내보내야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.

2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.

3. 인증서 스냅인 창에서 내 사용자 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 현재 사용자 > 신뢰할 수 있는 루트 인증 기관 > *인증서*를 클릭합니다.
5. SnapCenter Friendly Name이 있는 인증서를 마우스 오른쪽 버튼으로 클릭한 다음 모든 작업 > *내보내기*를 선택하여 내보내기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
개인 키 내보내기	예, 개인 키를 내보냅니다 옵션을 선택한 후 *다음*을 클릭합니다.
내보내기 파일 형식	변경하지 마세요. *다음*을 클릭하세요.
보안	내보낸 인증서에 사용할 새 비밀번호를 지정한 후 *다음*을 클릭합니다.
내보낼 파일	내보낸 인증서의 파일 이름을 지정하고(.pfx를 사용해야 함), *다음*을 클릭합니다.
인증서 내보내기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 내보내기를 시작합니다.

Windows 호스트에 대한 CA 인증서 구성

CA 인증서 CSR 파일 생성

인증서 서명 요청(CSR)을 생성하고, 생성된 CSR을 사용하여 인증 기관(CA)에서 얻을 수 있는 인증서를 가져올 수 있습니다. 인증서에는 개인 키가 연결됩니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.



CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 정보는 다음을 참조하세요. ["CA 인증서 CSR 파일을 생성하는 방법"](#).



도메인(*.domain.company.com)이나 시스템(machine1.domain.company.com)에 대한 CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN)과 해당 호스트 이름을 CA 인증서에 명시해야 합니다. 인증서를 구매하기 전에 주체 대체 이름(SAN) 필드를 입력하여 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(*.domain.company.com)의 경우 인증서에는 해당 도메인의 모든 호스트 이름이 암묵적으로 포함됩니다.

CA 인증서 가져오기

Microsoft 관리 콘솔(MMC)을 사용하여 CA 인증서를 SnapCenter 서버와 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.
2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
3. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > *인증서*를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 버튼으로 클릭한 다음, 모든 작업 > *가져오기*를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
개인 키 가져오기	예 옵션을 선택하고 개인 키를 가져온 후 *다음*을 클릭합니다.
가져오기 파일 형식	변경하지 마세요. *다음*을 클릭하세요.
보안	내보낸 인증서에 사용할 새 비밀번호를 지정한 후 *다음*을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.



인증서 가져오기는 개인 키와 함께 제공되어야 합니다(지원되는 형식: *.pfx, *.p12, *.p7b).

7. "개인" 폴더에 대해서도 5단계를 반복합니다.

CA 인증서 지문을 받으세요

인증서 지문은 인증서를 식별하는 16진수 문자열입니다. 지문은 지문 알고리즘을 사용하여 인증서 내용으로부터 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.
 - a. 인증서를 두 번 클릭합니다.
 - b. 인증서 대화 상자에서 세부정보 탭을 클릭합니다.
 - c. 필드 목록을 스크롤하여 *지문*을 클릭하세요.
 - d. 상자에서 16진수 문자를 복사하세요.

e. 16진수 사이의 공백을 제거하세요.

예를 들어, 지문이 "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b"인 경우 공백을 제거하면 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.

a. 다음 명령을 실행하여 설치된 인증서의 지문을 나열하고 주체 이름으로 최근에 설치된 인증서를 식별합니다.

```
Get-Childitem -경로 인증서:\LocalMachine\My
```

b. 지문을 복사하세요.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스로 CA 인증서를 구성해야 합니다.

SnapCenter 서버와 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하는 기존 인증서 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

예를 들어:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스에 바인딩합니다.
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

예를 들어:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

SnapCenter 사이트에 CA 인증서 구성

Windows 호스트의 SnapCenter 사이트에서 CA 인증서를 구성해야 합니다.

단계

1. SnapCenter 설치된 Windows Server에서 IIS 관리자를 엽니다.
2. 왼쪽 탐색 창에서 *연결*을 클릭합니다.
3. 서버 이름과 *사이트*를 확장합니다.
4. SSL 인증서를 설치할 SnapCenter 웹사이트를 선택하세요.
5. 작업 > *사이트 편집*으로 이동하여 *바인딩*을 클릭합니다.
6. 바인딩 페이지에서 *https에 대한 바인딩*을 선택합니다.
7. *편집*을 클릭하세요.
8. SSL 인증서 드롭다운 목록에서 최근에 가져온 SSL 인증서를 선택합니다.
9. *확인*을 클릭합니다.



SnapCenter Scheduler 사이트(기본 포트: 8154, HTTPS)는 자체 서명 인증서로 구성됩니다. 이 포트는 SnapCenter 서버 호스트 내에서 통신하며 CA 인증서로 구성할 필요가 없습니다. 하지만 사용자 환경에서 CA 인증서를 사용해야 하는 경우 SnapCenter Scheduler 사이트를 사용하여 5~9단계를 반복하세요.



최근 배포된 CA 인증서가 드롭다운 메뉴에 나열되지 않으면 CA 인증서가 개인 키와 연결되어 있는지 확인하세요.



다음 경로를 사용하여 인증서가 추가되었는지 확인하세요: 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > 인증서.

SnapCenter 에 CA 인증서 활성화

SnapCenter 서버에 대해 CA 인증서를 구성하고 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- Set-SmCertificateSettings cmdlet을 사용하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- Get-SmCertificateSettings cmdlet을 사용하여 SnapCenter 서버의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. 설정 페이지에서 설정 > 전역 설정 > *CA 인증서 설정*으로 이동합니다.
2. *인증서 검증 사용*을 선택합니다.
3. *적용*을 클릭하세요.

끝난 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- *  *는 플러그인 호스트에 활성화되거나 할당된 CA 인증서가 없음을 나타냅니다.
- *  *는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- *  *는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- *  *는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

Linux 호스트에 대한 CA 인증서 구성

Linux에 SnapCenter 서버를 설치한 후 설치 프로그램이 자체 서명 인증서를 생성합니다. CA 인증서를 사용하려면 nginx 역방향 프록시, 감사 로깅 및 SnapCenter 서비스에 대한 인증서를 구성해야 합니다.

nginx 인증서 구성

단계

1. `_etc/nginx/conf.d`로 이동합니다. `cd /etc/nginx/conf.d`
2. vi나 텍스트 편집기를 사용하여 `*snapcenter.conf*`를 엽니다.
3. 구성 파일의 서버 섹션으로 이동합니다.
4. `ssl_certificate` 및 `ssl_certificate_key` 경로를 CA 인증서를 가리키도록 수정합니다.
5. 파일을 저장하고 닫습니다.
6. nginx를 다시 로드하세요: `$nginx -s reload`

감사 로그 인증서 구성

단계

1. vi나 텍스트 편집기를 사용하여 `_INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config`를 엽니다.

`_INSTALL_DIR_`의 기본값은 `_opt_`입니다.
2. `AUDILOG_CERTIFICATE_PATH` 및 `AUDILOG_CERTIFICATE_PASSWORD` 키를 편집하여 각각 CA 인증서 경로와 비밀번호를 포함합니다.

감사 로그 인증서에는 `.pfx` 형식만 지원됩니다.

3. 파일을 저장하고 닫습니다.
4. `snapmanagerweb` 서비스를 다시 시작합니다. `$ systemctl restart snapmanagerweb`

SnapCenter 서비스 인증서 구성

단계

1. vi나 텍스트 편집기를 사용하여 다음 구성 파일을 엽니다.
 - `INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config`
 - `INSTALL_DIR/NetApp/snapcenter/SMCore/SMCoreServiceHost.dll.config`
 - `INSTALL_DIR/NetApp/snapcenter/Scheduler/Scheduler.Api.dll.config`

`INSTALL_DIR`의 기본값은 `/opt`입니다.
2. **SERVICE_CERTIFICATE_PATH** 및 **SERVICE_CERTIFICATE_PASSWORD** 키를 편집하여 각각 CA 인증서 경로와 비밀번호를 포함합니다.

SnapCenter 서비스 인증서에는 `.pfx` 형식만 지원됩니다.

3. 파일을 저장하고 닫습니다.
4. 모든 서비스를 다시 시작합니다.
 - `$ systemctl restart snapmanagerweb`
 - `$ systemctl restart smcore`
 - `$ systemctl restart scheduler`

Windows 호스트에서 양방향 SSL 통신을 구성하고 활성화합니다.

Windows 호스트에서 양방향 SSL 통신 구성

Windows 호스트의 SnapCenter Server와 플러그인 간의 상호 통신을 보호하려면 양방향 SSL 통신을 구성해야 합니다.

시작하기 전에

- 최소 지원 키 길이인 3072로 CA 인증서 CSR 파일을 생성했어야 합니다.
- CA 인증서는 서버 인증과 클라이언트 인증을 지원해야 합니다.
- 개인 키와 지문 정보가 포함된 CA 인증서가 있어야 합니다.
- 단방향 SSL 구성을 활성화했어야 합니다.

자세한 내용은 다음을 참조하세요. ["CA 인증서 섹션을 구성합니다."](#)

- 모든 플러그인 호스트와 SnapCenter 서버에서 양방향 SSL 통신을 활성화해야 합니다.

일부 호스트 또는 서버에서 양방향 SSL 통신이 활성화되지 않은 환경은 지원되지 않습니다.

단계

1. 포트를 바인딩하려면 PowerShell 명령을 사용하여 SnapCenter IIS 웹 서버 포트 8146(기본값)에 대해 SnapCenter 서버 호스트에서 다음 단계를 수행하고, SMCore 포트 8145(기본값)에 대해서도 다시 한 번 다음 단계를 수행합니다.

- a. 다음 PowerShell 명령을 사용하여 기존 SnapCenter 자체 서명 인증서 포트 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
```

예를 들어,

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

```
> netsh http delete sslcert ipport=0.0.0.0:8146
```

- b. 새로 조달한 CA 인증서를 SnapCenter 서버와 SMCore 포트에 연결합니다.

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>  
certhash=$cert appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

예를 들어,

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8146
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

2. CA 인증서에 대한 권한에 액세스하려면 다음 단계를 수행하여 새로 조달한 CA 인증서에 액세스하여 SnapCenter의 기본 IIS 웹 서버 사용자 "**IIS AppPool\ SnapCenter**"를 인증서 권한 목록에 추가합니다.

- a. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.

- b. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.

- c. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.

- d. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 개인 > *인증서*를 클릭합니다.

- e. SnapCenter 인증서를 선택하세요.

- f. 사용자권한 추가 마법사를 시작하려면 CA 인증서를 마우스 오른쪽 버튼으로 클릭하고 모든 작업 > *개인 키 관리*를 선택하세요.

- g. *추가*를 클릭하고 사용자 및 그룹 선택 마법사에서 위치를 로컬 컴퓨터 이름(계층 구조에서 가장 위)으로 변경합니다.
 - h. IIS AppPool\ SnapCenter 사용자를 추가하고 모든 제어 권한을 부여합니다.
3. *CA 인증서 IIS 권한*의 경우 다음 경로에서 SnapCenter 서버에 새 DWORD 레지스트리 키 항목을 추가합니다.

Windows 레지스트리 편집기에서 아래 언급된 경로로 이동합니다.

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
```

4. SCHANNEL 레지스트리 구성 컨텍스트에서 새로운 DWORD 레지스트리 키 항목을 만듭니다.

```
SendTrustedIssuerList = 0
```

```
ClientAuthTrustMode = 2
```

양방향 SSL 통신을 위한 SnapCenter Windows 플러그인 구성

PowerShell 명령을 사용하여 SnapCenter Windows 플러그인을 양방향 SSL 통신으로 구성해야 합니다.

시작하기 전에

CA 인증서 지문을 사용할 수 있는지 확인하세요.

단계

1. 포트를 바인딩하려면 SMCore 포트 8145(기본값)에 대한 Windows 플러그인 호스트에서 다음 작업을 수행합니다.

- a. 다음 PowerShell 명령을 사용하여 기존 SnapCenter 자체 서명 인증서 포트 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
```

예를 들어,

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- b. 새로 조달한 CA 인증서를 SMCore 포트에 바인딩합니다.

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert  
appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port>
```

예를 들어,

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8145
```

Windows 호스트에서 양방향 SSL 통신 활성화

PowerShell 명령을 사용하여 Windows 호스트의 SnapCenter 서버와 플러그인 간의 상호 통신을 보호하기 위해 양방향 SSL 통신을 활성화할 수 있습니다.

시작하기 전에

먼저 모든 플러그인과 SMCore 에이전트에 대한 명령을 실행한 다음 서버에 대한 명령을 실행합니다.

단계

1. 양방향 SSL 통신을 활성화하려면 플러그인, 서버 및 양방향 SSL 통신이 필요한 각 에이전트에 대해 SnapCenter 서버에서 다음 명령을 실행합니다.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName <Plugin_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. 다음 명령을 사용하여 IIS SnapCenter 애플리케이션 풀 재활용 작업을 수행합니다.

```
> Restart-WebAppPool -Name "SnapCenter"
```

3. Windows 플러그인의 경우 다음 PowerShell 명령을 실행하여 SMCore 서비스를 다시 시작합니다.

```
> Restart-Service -Name SnapManagerCoreService
```

양방향 SSL 통신 비활성화

PowerShell 명령을 사용하여 양방향 SSL 통신을 비활성화할 수 있습니다.

이 작업에 관하여

- 먼저 모든 플러그인과 SMCore 에이전트에 대한 명령을 실행한 다음 서버에 대한 명령을 실행합니다.
- 양방향 SSL 통신을 비활성화하면 CA 인증서와 해당 구성은 제거되지 않습니다.
- SnapCenter Server에 새로운 호스트를 추가하려면 모든 플러그인 호스트에 대해 양방향 SSL을 비활성화해야 합니다.
- NLB와 F5는 지원되지 않습니다.

단계

1. 양방향 SSL 통신을 비활성화하려면 모든 플러그인 호스트와 SnapCenter 호스트에 대해 SnapCenter 서버에서 다음 명령을 실행합니다.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName <Agent_HostName>  
  
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName localhost  
  
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. 다음 명령을 사용하여 IIS SnapCenter 애플리케이션 풀 재활용 작업을 수행합니다.

```
> Restart-WebAppPool -Name "SnapCenter"
```

3. Windows 플러그인의 경우 다음 PowerShell 명령을 실행하여 SMCore 서비스를 다시 시작합니다.

```
> Restart-Service -Name SnapManagerCoreService
```

Linux 호스트에서 양방향 SSL 통신을 구성하고 활성화합니다.

Linux 호스트에서 양방향 SSL 통신 구성

Linux 호스트의 SnapCenter Server와 플러그인 간의 상호 통신을 보호하려면 양방향 SSL 통신을 구성해야 합니다.

시작하기 전에

- Linux 호스트에 대한 CA 인증서를 구성했어야 합니다.
- 모든 플러그인 호스트와 SnapCenter 서버에서 양방향 SSL 통신을 활성화해야 합니다.

단계

1. *certificate.pem*을 `/etc/pki/ca-trust/source/anchors/`에 복사합니다.
2. Linux 호스트의 신뢰 목록에 인증서를 추가합니다.
 - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
 - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
 - `update-ca-trust extract`
3. 인증서가 신뢰 목록에 추가되었는지 확인하세요.
`trust list | grep "<CN of your certificate>"`
4. SnapCenter **nginx** 파일에서 **ssl_certificate** 및 *ssl_certificate_key*를 업데이트하고 다시 시작합니다.
 - `vim /etc/nginx/conf.d/snapcenter.conf`
 - `systemctl restart nginx`
5. SnapCenter 서버 GUI 링크를 새로 고칩니다.
6. *SnapManager.Web.UI.dll.config*(`/<설치 경로>/NetApp/snapcenter/SnapManagerWeb_`에 위치) 및 **SMCoreServiceHost.dll.config**(`/<설치 경로>/NetApp/snapcenter/SMCore_`에 위치)에서 다음 키의 값을 업데이트합니다.

◦ `<key="SERVICE_CERTIFICATE_PATH" value="<인증서.pfx 경로>" />`를 추가합니다.

◦ `<키 추가="서비스 인증서 비밀번호" 값="<비밀번호>" />`

7. 다음 서비스를 다시 시작합니다.

◦ `systemctl restart smcore.service`

◦ `systemctl restart snapmanagerweb.service`

8. 인증서가 SnapManager 웹 포트에 연결되어 있는지 확인하세요.

`openssl s_client -connect localhost:8146 -brief`

9. 인증서가 smcore 포트에 연결되어 있는지 확인하세요.

`openssl s_client -connect localhost:8145 -brief`

10. SPL 키스토어와 별칭에 대한 비밀번호를 관리합니다.

a. SPL 속성 파일의 **SPL_KEYSTORE_PASS** 키에 할당된 SPL 키 저장소 기본 비밀번호를 검색합니다.

b. 키스토어 비밀번호를 변경합니다.

`keytool -storepasswd -keystore keystore.jks`

c. 개인 키 항목의 모든 별칭에 대한 비밀번호를 변경합니다.

`keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`

d. `_spl.properties`의 **SPL_KEYSTORE_PASS** 키에 대해 동일한 비밀번호를 업데이트합니다.

e. 서비스를 다시 시작합니다.

11. 플러그인 Linux 호스트에서 SPL 플러그인의 키 저장소에 루트 및 중간 인증서를 추가합니다.

◦ `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`

◦ `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`

i. `keystore.jks`의 항목을 확인하세요.

`keytool -list -v -keystore <path to keystore.jks>`

ii. 필요한 경우 별칭의 이름을 바꾸세요.

`keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`

12. `spl.properties` 파일에 있는 **SPL_CERTIFICATE_ALIAS** 값을 `_keystore.jks`에 저장된 **certificate.pfx** 별칭으로 업데이트하고 SPL 서비스를 다시 시작합니다. `systemctl restart spl`

13. 인증서가 smcore 포트에 연결되어 있는지 확인하세요.

`openssl s_client -connect localhost:8145 -brief`

Linux 호스트에서 SSL 통신 활성화

PowerShell 명령을 사용하여 Linux 호스트의 SnapCenter 서버와 플러그인 간의 상호 통신을 보호하기 위해 양방향 SSL 통신을 활성화할 수 있습니다.

단계

1. 단방향 SSL 통신을 활성화하려면 다음을 수행하세요.
 - a. SnapCenter GUI에 로그인합니다.
 - b. 설정 > *전역 설정*을 클릭하고 * SnapCenter 서버에서 인증서 유효성 검사 사용*을 선택합니다.
 - c. 호스트 > *관리 호스트*를 클릭하고 단방향 SSL을 활성화하려는 플러그인 호스트를 선택합니다.
 - d. 딸깍 하는 소리  아이콘을 클릭한 다음 *인증서 유효성 검사 사용*을 클릭합니다.
2. SnapCenter Server Linux 호스트에서 양방향 SSL 통신을 활성화합니다.
 - Open-SmConnection
 - Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>
 - Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost
 - Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}

Active Directory, LDAP 및 LDAPS 구성

신뢰할 수 없는 Active Directory 도메인 등록

여러 개의 신뢰할 수 없는 Active Directory 도메인의 호스트, 사용자 및 그룹을 관리하려면 SnapCenter Server에 Active Directory를 등록해야 합니다.

시작하기 전에

LDAP 및 LDAPS 프로토콜

- LDAP 또는 LDAPS 프로토콜을 사용하여 신뢰할 수 없는 Active Directory 도메인을 등록할 수 있습니다.
- 플러그인 호스트와 SnapCenter 서버 간에 양방향 통신을 활성화해야 합니다.
- DNS 확인은 SnapCenter 서버에서 플러그인 호스트로 설정해야 하며 그 반대의 경우도 마찬가지입니다.

LDAP 프로토콜

- 정규화된 도메인 이름(FQDN)은 SnapCenter 서버에서 확인 가능해야 합니다.

신뢰할 수 없는 도메인을 FQDN으로 등록할 수 있습니다. SnapCenter 서버에서 FQDN을 확인할 수 없는 경우 도메인 컨트롤러 IP 주소로 등록하면 SnapCenter 서버에서 확인할 수 있습니다.

LDAPS 프로토콜

- LDAPS가 활성 디렉터리 통신 중에 중단 간 암호화를 제공하려면 CA 인증서가 필요합니다.

"LDAPS에 대한 CA 클라이언트 인증서 구성"

- 도메인 컨트롤러 호스트 이름(DCHostName)은 SnapCenter 서버에서 접근 가능해야 합니다.

이 작업에 관하여

- SnapCenter 사용자 인터페이스, PowerShell cmdlet 또는 REST API를 사용하여 신뢰할 수 없는 도메인을 등록할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *전역 설정*을 클릭합니다.
3. 글로벌 설정 페이지에서 *도메인 설정*을 클릭합니다.
4. 딸깍 하는 소리  새로운 도메인을 등록합니다.
5. 새 도메인 등록 페이지에서 **LDAP** 또는 *LDAPS*를 선택합니다.
 - a. *LDAP*를 선택하는 경우, LDAP에 신뢰할 수 없는 도메인을 등록하는 데 필요한 정보를 지정합니다.

이 분야에서는...	이렇게 하세요...
도메인 이름	도메인의 NetBIOS 이름을 지정합니다.
도메인 FQDN	FQDN을 지정하고 *확인*을 클릭합니다.
도메인 컨트롤러 IP 주소	SnapCenter 서버에서 도메인 FQDN을 확인할 수 없는 경우 하나 이상의 도메인 컨트롤러 IP 주소를 지정하세요. 자세한 내용은 다음을 참조하세요. "GUI에서 신뢰할 수 없는 도메인에 대한 도메인 컨트롤러 IP 추가" .

- b. *LDAPS*를 선택하는 경우, LDAPS에 신뢰할 수 없는 도메인을 등록하는 데 필요한 정보를 지정합니다.

이 분야에서는...	이렇게 하세요...
도메인 이름	도메인의 NetBIOS 이름을 지정합니다.
도메인 FQDN	FQDN을 지정하세요.
도메인 컨트롤러 이름	하나 이상의 도메인 컨트롤러 이름을 지정하고 *확인*을 클릭합니다.
도메인 컨트롤러 IP 주소	SnapCenter 서버에서 도메인 컨트롤러 이름을 확인할 수 없는 경우 DNS 확인을 수정해야 합니다.

6. *확인*을 클릭합니다.

Active Directory 읽기 권한을 활성화하기 위해 IIS 애플리케이션 풀 구성

SnapCenter 에 대한 Active Directory 읽기 권한을 활성화해야 할 때 사용자 지정 애플리케이션 풀 계정을 생성하기 위해 Windows Server에서 IIS(인터넷 정보 서비스)를 구성할 수 있습니다.

단계

1. SnapCenter 설치된 Windows Server에서 IIS 관리자를 엽니다.
2. 왼쪽 탐색 창에서 *애플리케이션 풀*을 클릭합니다.
3. 애플리케이션 풀 목록에서 SnapCenter 선택한 다음 작업 창에서 *고급 설정*을 클릭합니다.
4. ID를 선택한 다음 *...*를 클릭하여 SnapCenter 애플리케이션 풀 ID를 편집합니다.
5. 사용자 지정 계정 필드에 Active Directory 읽기 권한이 있는 도메인 사용자 또는 도메인 관리자 계정 이름을 입력합니다.
6. OK를 클릭합니다.

사용자 지정 계정은 SnapCenter 애플리케이션 풀의 기본 제공 ApplicationPoolIdentity 계정을 대체합니다.

LDAPS에 대한 CA 클라이언트 인증서 구성

Windows Active Directory LDAPS가 CA 인증서로 구성된 경우 SnapCenter 서버에서 LDAPS에 대한 CA 클라이언트 인증서를 구성해야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.
2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
3. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > *인증서*를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 버튼으로 클릭한 다음, 모든 작업 > *가져오기*를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
마법사의 두 번째 페이지에서	*찾아보기*를 클릭하고 _루트 인증서_를 선택한 후 *다음*을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.

7. 중간 인증서에 대해서도 5단계와 6단계를 반복합니다.

Microsoft SQL Server 데이터베이스 보호

Microsoft SQL Server용 SnapCenter 플러그인

Microsoft SQL Server용 SnapCenter 플러그인 개요

Microsoft SQL Server용 SnapCenter 플러그인은 Microsoft SQL Server 데이터베이스의 애플리케이션 인식 데이터 보호 관리를 지원하는 NetApp SnapCenter 소프트웨어의 호스트 측 구성 요소입니다. SQL Server용 플러그인은 SnapCenter 환경에서 SQL Server 데이터베이스 백업, 검증, 복원 및 복제 작업을 자동화합니다.

SQL Server용 플러그인을 설치하면 NetApp SnapMirror 기술과 함께 SnapCenter 사용하여 다른 볼륨에 백업 세트의 미리 복사본을 만들고 NetApp SnapVault 기술을 사용하여 표준 준수 또는 보관 목적으로 디스크 간 백업 복제를 수행할 수 있습니다.

- SnapCenter 환경에서 Microsoft SQL Server 데이터베이스에 대한 애플리케이션 인식 백업, 복원 및 복제 작업을 자동화합니다.
- SnapCenter Plug-in for VMware vSphere 배포하고 SnapCenter 에 플러그인을 등록하면 VMDK 및 RDM(원시 장치 매핑) LUN에서 Microsoft SQL Server 데이터베이스를 지원합니다.
- SMB 공유 프로비저닝만 지원합니다. SMB 공유에서 SQL Server 데이터베이스를 백업하는 기능은 제공되지 않습니다.
- Microsoft SQL Server용 SnapManager 에서 SnapCenter 로 백업을 가져오는 기능을 지원합니다.

Microsoft SQL Server용 SnapCenter 플러그인으로 할 수 있는 작업

Microsoft SQL Server용 SnapCenter 플러그인이 사용자 환경에 설치되면 SnapCenter 사용하여 SQL Server 데이터베이스를 백업, 복원 및 복제할 수 있습니다.

SQL Server 데이터베이스와 데이터베이스 리소스의 백업 작업, 복원 작업 및 복제 작업을 지원하는 다음 작업을 수행할 수 있습니다.

- SQL Server 데이터베이스 및 관련 트랜잭션 로그 백업

마스터 및 msdb 시스템 데이터베이스에 대한 로그 백업을 생성할 수 없습니다. 하지만 모델 시스템 데이터베이스에 대한 로그 백업을 생성할 수 있습니다.

- 데이터베이스 리소스 복원
 - 마스터 시스템 데이터베이스, msdb 시스템 데이터베이스, 모델 시스템 데이터베이스를 복원할 수 있습니다.
 - 여러 개의 데이터베이스, 인스턴스 및 가용성 그룹을 복원할 수 없습니다.
 - 시스템 데이터베이스를 대체 경로로 복원할 수 없습니다.
- 프로덕션 데이터베이스의 특정 시점 복제본 생성

tempdb 시스템 데이터베이스에서는 백업, 복원, 복제 및 복제 수명 주기 작업을 수행할 수 없습니다.

- 백업 작업을 즉시 확인하거나 나중에 확인을 연기합니다.

SQL Server 시스템 데이터베이스 검증이 지원되지 않습니다. SnapCenter 데이터베이스를 복제하여 검증 작업을 수행합니다. SnapCenter SQL Server 시스템 데이터베이스를 복제할 수 없으므로 이러한 데이터베이스의 검증은 지원되지 않습니다.

- 백업 작업 및 복제 작업 예약
- 백업 작업, 복원 작업 및 복제 작업 모니터링



SQL Server용 플러그인은 SMB 공유에서 SQL Server 데이터베이스의 백업 및 복구를 지원하지 않습니다.

Microsoft SQL Server용 SnapCenter 플러그인 기능

SQL Server용 플러그인은 Windows 호스트의 Microsoft SQL Server와 통합되고 스토리지 시스템의 NetApp Snapshot 기술과 통합됩니다. SQL Server용 플러그인을 사용하려면 SnapCenter 인터페이스를 사용합니다.

SQL Server용 플러그인에는 다음과 같은 주요 기능이 포함되어 있습니다.

- * SnapCenter 가 지원하는 통합 그래픽 사용자 인터페이스*

SnapCenter 인터페이스는 플러그인과 환경 전반에 걸쳐 표준화와 일관성을 제공합니다. SnapCenter 인터페이스를 사용하면 플러그인 전반에 걸쳐 일관된 백업 및 복원 프로세스를 완료하고, 중앙 집중식 보고를 사용하고, 한눈에 볼 수 있는 대시보드 보기를 사용하고, 역할 기반 액세스 제어(RBAC)를 설정하고, 모든 플러그인에서 작업을 모니터링할 수 있습니다. SnapCenter 백업 및 복제 작업을 지원하기 위해 중앙 집중식 스케줄링 및 정책 관리 기능도 제공합니다.

- 자동화된 중앙 관리

정기적인 SQL Server 백업을 예약하고, 정책 기반 백업 보존을 구성하고, 특정 시점 및 최신 복원 작업을 설정할 수 있습니다. SnapCenter 구성하여 이메일 알림을 보내면 SQL Server 환경을 사전에 모니터링할 수도 있습니다.

- 중단 없는 **NetApp** 스냅샷 기술

SQL Server용 플러그인은 Microsoft Windows용 NetApp SnapCenter 플러그인과 함께 NetApp Snapshot 기술을 사용합니다. 이를 통해 몇 초 안에 데이터베이스를 백업하고 SQL Server를 오프라인으로 전환하지 않고도 빠르게 복원할 수 있습니다. 스냅샷은 최소한의 저장 공간을 차지합니다.

이러한 주요 기능 외에도 SQL Server 플러그인은 다음과 같은 이점을 제공합니다.

- 백업, 복원, 복제 및 검증 워크플로 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임
- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 프로덕션 데이터베이스의 공간 효율적인 특정 시점 복사본 생성

복제본을 보관하는 스토리지 시스템에는 FlexClone 라이선스가 필요합니다.

- 중단 없는 자동 백업 검증
- 여러 서버에서 동시에 여러 백업을 실행할 수 있는 기능

- 백업, 확인, 복원 및 복제 작업 스크립팅을 위한 PowerShell cmdlet
- SQL Server에서 AlwaysOn 가용성 그룹(AG)을 지원하여 AG 설정, 백업 및 복원 작업을 가속화합니다.
- SQL Server 2014의 일부인 메모리 내 데이터베이스 및 버퍼 풀 확장(BPE)
- LUN 및 가상 머신 디스크(VMDK) 백업 지원
- 물리적 및 가상화된 인프라 지원
- NFS 및 VMFS를 통한 iSCSI, 파이버 채널, FCoE, 원시 장치 매핑(RDM), VMDK 지원



NAS 볼륨에는 스토리지 가상 머신(SVM)에 기본 내보내기 정책이 있어야 합니다.

- SQL Server 독립 실행형 데이터베이스에서 FileStream 및 파일 그룹을 지원합니다.
- Windows Server 2022에서 NVMe(Non-Volatile Memory Express) 지원
 - TCP/IP를 통한 NVMe에서 생성된 VMDK 레이아웃에 대한 백업, 복원, 복제 및 검증 워크플로.
 - ESX 8.0 업데이트 2부터 NVMe 펌웨어 버전 1.3을 지원하고 가상 하드웨어 버전 21이 필요합니다.
 - Windows Server 장애 조치(Failover) 클러스터링(WSFC)은 TCP/IP를 통한 NVMe의 VMDK를 통한 애플리케이션에서 지원되지 않습니다.
- 사이트 전체에 장애가 발생해도 비즈니스 서비스가 계속 운영될 수 있도록 하는 SnapMirror Active Sync(처음에는 SnapMirror Business Continuity[SM-BC]로 출시)를 지원하며, 보조 복사본을 사용하여 애플리케이션이 투명하게 장애 조치되도록 지원합니다. SnapMirror Active Sync를 사용하면 장애 조치를 트리거하는 데 수동 개입이나 추가 스크립팅이 필요하지 않습니다.

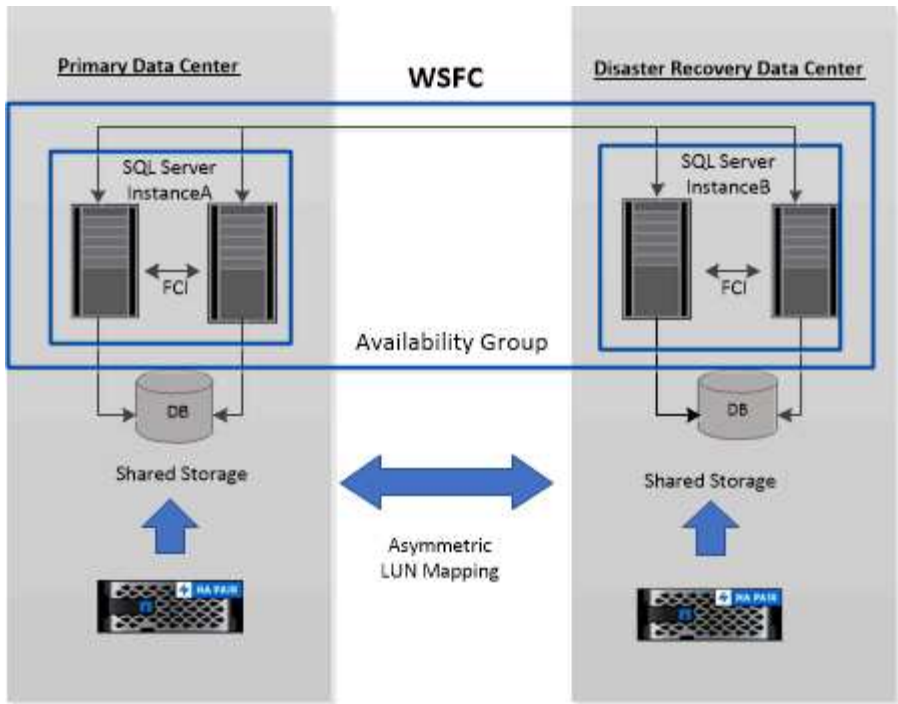
Windows 클러스터에서 비대칭 LUN 매핑 지원

Microsoft SQL Server용 SnapCenter 플러그인은 SQL Server 2012 이상에서 검색을 지원하고, 고가용성을 위한 ALM(비대칭 LUN 매핑) 구성과 재해 복구를 위한 가용성 그룹을 지원합니다. SnapCenter 리소스를 검색할 때 ALM 구성의 로컬 호스트와 원격 호스트에 있는 데이터베이스를 검색합니다.

ALM 구성은 기본 데이터 센터에 하나 이상의 노드와 재해 복구 센터에 하나 이상의 노드가 포함된 단일 Windows 서버 장애 조치 클러스터입니다.

다음은 ALM 구성의 예입니다.

- 다중 사이트 데이터 센터의 두 개의 장애 조치 클러스터 인스턴스(FCI)
- 재해 복구 사이트에서 독립형 인스턴스를 사용하여 재해 복구를 위한 로컬 고가용성(HA) 및 가용성 그룹(AG)을 위한 FCI



WSFC----Windows Server Failover Cluster

기본 데이터 센터의 저장소는 기본 데이터 센터에 있는 FCI 노드 간에 공유됩니다. 재해 복구 데이터 센터의 저장소는 재해 복구 데이터 센터에 있는 FCI 노드 간에 공유됩니다.

기본 데이터 센터의 스토리지는 재해 복구 데이터 센터의 노드에서 볼 수 없으며 그 반대의 경우도 마찬가지입니다.

ALM 아키텍처는 FCI가 사용하는 두 가지 공유 스토리지 솔루션과 SQL AG가 사용하는 비공유 또는 전용 스토리지 솔루션을 결합합니다. AG 솔루션은 여러 데이터 센터의 공유 디스크 리소스에 동일한 드라이브 문자를 사용합니다. WSFC 내의 노드 하위 집합 간에 클러스터 디스크를 공유하는 이러한 저장 배열을 ALM이라고 합니다.

Microsoft SQL Server용 SnapCenter 플러그인에서 지원하는 스토리지 유형

SnapCenter 물리적 머신과 가상 머신 모두에서 다양한 스토리지 유형을 지원합니다. 호스트에 패키지를 설치하기 전에 해당 스토리지 유형에 대한 지원이 제공되는지 확인해야 합니다.

SnapCenter 프로비저닝 및 데이터 보호 지원은 Windows Server에서 제공됩니다. 지원되는 버전에 대한 최신 정보는 다음을

참조하세요. <https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT>["NetApp 상호 운용성 매트릭스 도구"] .

기계	저장 유형	제공을 사용하여	지원 노트
물리적 서버	FC 연결 LUN	SnapCenter 그래픽 사용자 인터페이스(GUI) 또는 PowerShell cmdlet	
물리적 서버	iSCSI로 연결된 LUN	SnapCenter GUI 또는 PowerShell cmdlet	

기계	저장 유형	제공을 사용하여	지원 노트
물리적 서버	SVM(스토리지 가상 머신)에 있는 SMB3(CIFS) 공유	SnapCenter GUI 또는 PowerShell cmdlet	프로비저닝만 지원합니다.
VMware VM	FC 또는 iSCSI HBA로 연결된 RDM LUN	PowerShell cmdlet	
VMware VM	iSCSI 이니시에이터에 의해 게스트 시스템에 직접 연결된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	
VMware VM	가상 머신 파일 시스템(VMFS) 또는 NFS 데이터 저장소	VMware vSphere	
VMware VM	SVM에 있는 SMB3 공유에 연결된 게스트 시스템	SnapCenter GUI 또는 PowerShell cmdlet	프로비저닝만 지원합니다.
VMware VM	NFS와 SAN 모두에 있는 vVol 데이터 저장소	VMware vSphere용 ONTAP 도구	
Hyper-V VM	가상 파이버 채널 스위치로 연결된 가상 FC(vFC) LUN	SnapCenter GUI 또는 PowerShell cmdlet	가상 파이버 채널 스위치로 연결된 가상 FC(vFC) LUN을 프로비저닝하려면 Hyper-V 관리자를 사용해야 합니다.  NetApp 스토리지에 프로비저닝된 VHD(x)에 있는 Hyper-V 패스스루 디스크와 데이터베이스 백업은 지원되지 않습니다.

기계	저장 유형	제공을 사용하여	지원 노트
Hyper-V VM	iSCSI 이니시에이터에 의해 게스트 시스템에 직접 연결된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	 NetApp 스토리지에 프로비저닝된 VHD(x)에 있는 Hyper-V 패스스루 디스크와 데이터베이스 백업은 지원되지 않습니다.
Hyper-V VM	SVM에 있는 SMB3 공유에 연결된 게스트 시스템	SnapCenter GUI 또는 PowerShell cmdlet	프로비저닝만 지원합니다.  NetApp 스토리지에 프로비저닝된 VHD(x)에 있는 Hyper-V 패스스루 디스크와 데이터베이스 백업은 지원되지 않습니다.

Microsoft SQL Server용 SnapCenter 플러그인에 대한 스토리지 레이아웃 권장 사항

잘 설계된 스토리지 레이아웃을 통해 SnapCenter Server는 복구 목표를 충족하도록 데이터베이스를 백업할 수 있습니다. 저장소 레이아웃을 정의할 때는 데이터베이스 크기, 데이터베이스 변경률, 백업 빈도 등 여러 요소를 고려해야 합니다.

다음 섹션에서는 사용자 환경에 설치된 Microsoft SQL Server용 SnapCenter 플러그인을 사용하여 LUN 및 가상 머신 디스크(VMDK)에 대한 스토리지 레이아웃 권장 사항과 제한 사항을 정의합니다.

이 경우 LUN에는 게스트에 매핑된 VMware RDM 디스크와 iSCSI 직접 연결 LUN이 포함될 수 있습니다.

LUN 및 VMDK 요구 사항

최적의 성능과 다음 데이터베이스 관리를 위해 전용 LUN이나 VMDK를 선택적으로 사용할 수 있습니다.

- 마스터 및 모델 시스템 데이터베이스
- Tempdb
- 사용자 데이터베이스 파일(.mdf 및 .ndf)
- 사용자 데이터베이스 트랜잭션 로그 파일(.ldf)

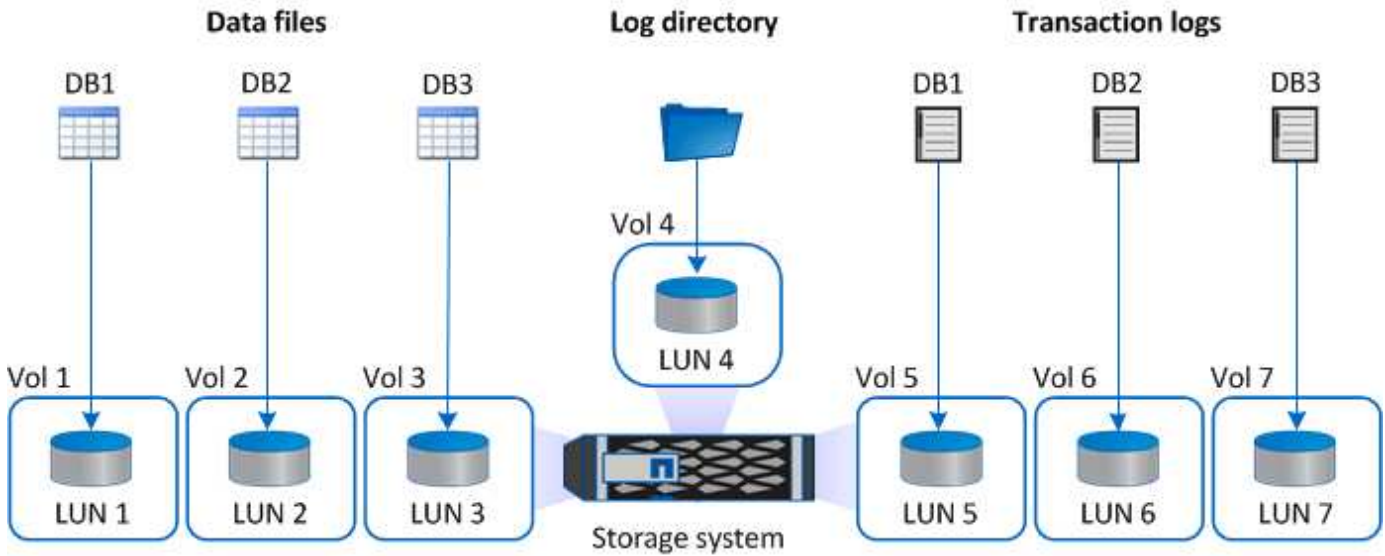
- 로그 디렉토리

대규모 데이터베이스를 복원하려면 전용 LUN이나 VMDK를 사용하는 것이 가장 좋습니다. 전체 LUN 또는 VMDK를 복원하는 데 걸리는 시간은 LUN 또는 VMDK에 저장된 개별 파일을 복원하는 데 걸리는 시간보다 짧습니다.

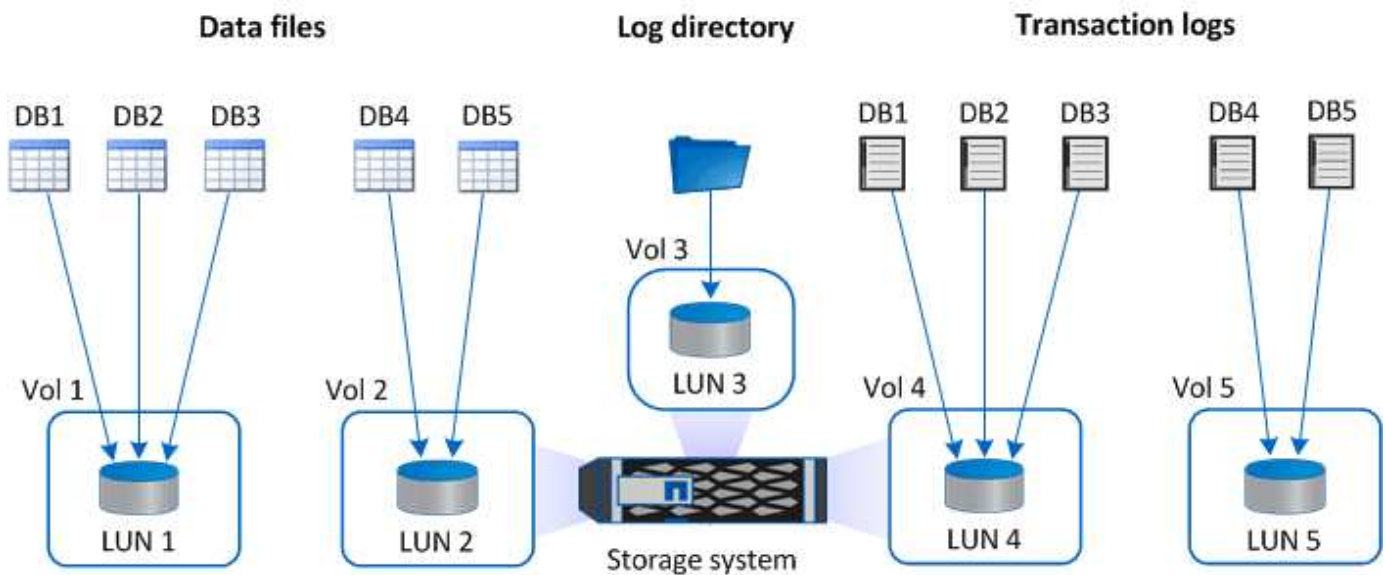
로그 디렉토리의 경우 데이터 또는 로그 파일 디스크에 충분한 여유 공간이 있도록 별도의 LUN이나 VMDK를 만들어야 합니다.

LUN 및 VMDK 샘플 레이아웃

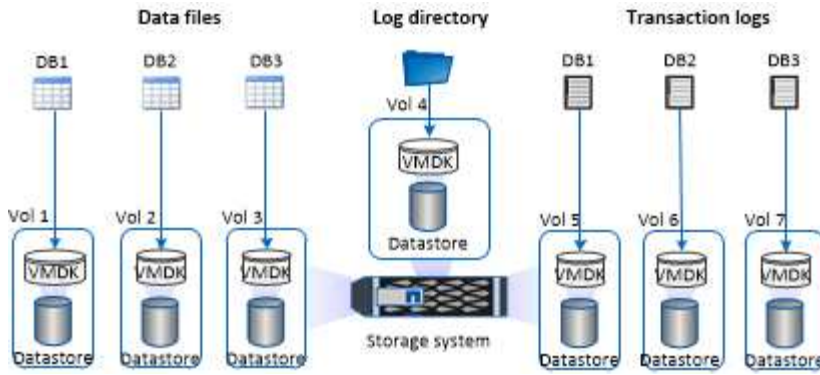
다음 그래픽은 LUN에서 대규모 데이터베이스에 대한 스토리지 레이아웃을 구성하는 방법을 보여줍니다.



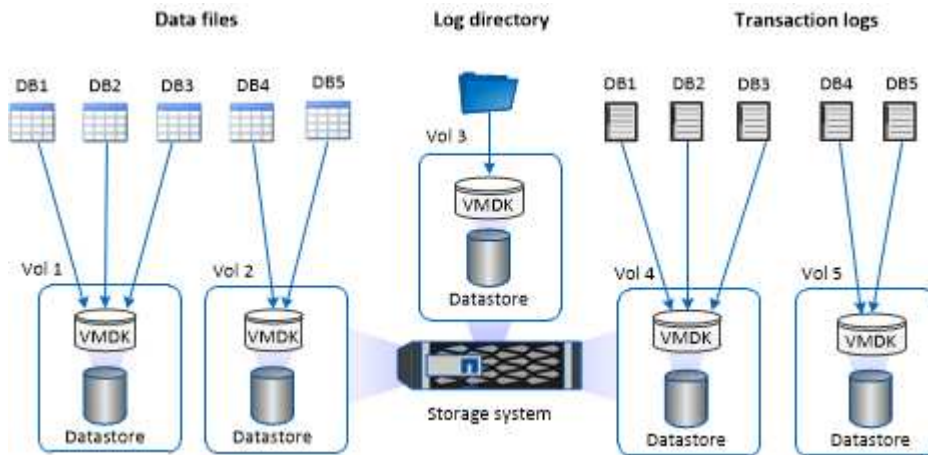
다음 그래픽은 LUN에서 중소형 데이터베이스에 대한 스토리지 레이아웃을 구성하는 방법을 보여줍니다.



다음 그래픽은 VMDK에서 대규모 데이터베이스에 대한 스토리지 레이아웃을 구성하는 방법을 보여줍니다.



다음 그래픽은 VMDK에서 중소형 데이터베이스의 스토리지 레이아웃을 구성하는 방법을 보여줍니다.



SQL 플러그인에 필요한 최소 ONTAP 권한

데이터 보호를 위해 사용하는 SnapCenter 플러그인에 따라 필요한 최소 ONTAP 권한은 다릅니다.

- 모든 액세스 명령: ONTAP 9.12.1 이상에 필요한 최소 권한
 - 이벤트 생성-자동 지원-로그
 - 작업 이력 표시
 - 작업 중지
 - 룰
 - lun 생성
 - lun 삭제
 - lun igroup 추가
 - lun igroup 생성
 - lun igroup 삭제
 - lun igroup 이름 바꾸기
 - 룰 아이그룹 쇼
 - lun 매핑 add-reporting-nodes

- lun 매핑 생성
- LUN 매핑 삭제
- LUN 매핑 제거-보고-노드
- lun 매핑 쇼
- lun 수정
- lun 이동량
- lun 오프라인
- lun 온라인
- lun 크기 조정
- lun 시리얼
- 런 쇼
- 스냅미러 정책 추가 규칙
- 스냅미러 정책 수정 규칙
- 스냅미러 정책 제거 규칙
- 스냅미러 정책 보기
- 스냅미러 복원
- 스냅미러 쇼
- 스냅미러 쇼 히스토리
- 스냅미러 업데이트
- 스냅미러 업데이트-ls-세트
- 스냅미러 목록-대상
- 버전
- 볼륨 복제 생성
- 볼륨 클론 쇼
- 볼륨 복제 분할 시작
- 볼륨 클론 분할 정지
- 볼륨 생성
- 볼륨 파괴
- 볼륨 파일 복제 생성
- 볼륨 파일 show-disk-usage
- 볼륨 오프라인
- 온라인 볼륨
- 볼륨 수정
- 볼륨 qtree 생성

- 볼륨 qtree 삭제
- 볼륨 qtree 수정
- 볼륨 qtree 쇼
- 볼륨 제한
- 볼륨 쇼
- 볼륨 스냅샷 생성
- 볼륨 스냅샷 삭제
- 볼륨 스냅샷 수정
- 볼륨 스냅샷 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- vservers cifs
- vservers cifs 공유 생성
- vservers cifs 공유 삭제
- vservers cifs 새도우 카피 쇼
- vservers cifs 공유 표시
- vservers cifs 쇼
- vservers 내보내기 정책
- vservers 내보내기 정책 생성
- vservers 내보내기 정책 삭제
- vservers 내보내기 정책 규칙 생성
- vservers 내보내기 정책 규칙 표시
- vservers 내보내기 정책 표시
- vserver iSCSI
- vservers iscsi 연결 표시
- vservers 쇼
- 네트워크 인터페이스
- 네트워크 인터페이스 표시
- vserver
- 메트로클러스터 쇼

SQL 서버용 플러그인을 위한 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비

ONTAP SnapMirror 기술과 함께 SnapCenter 플러그인을 사용하면 다른 볼륨에 백업 세트의 미러 사본을 생성할 수 있으며, ONTAP SnapVault 기술과 함께 사용하면 표준 준수 및 기타 거버넌스 관련 목적으로 디스크 간 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 구성하고 해당 관계를 초기화해야 합니다.

SnapCenter 스냅샷 작업을 완료한 후 SnapMirror와 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행됩니다. SnapMirror 활성화 동기화를 사용하는 경우 SnapMirror 활성화 동기화와 비동기 관계 모두에 기본 SnapMirror 또는 SnapVault 일정을 사용하세요.



NetApp SnapManager 제품을 통해 SnapCenter에 접속했고 구성된 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 기본 저장소(소스 볼륨)의 데이터를 보조 저장소(대상 볼륨)로 복제합니다. 관계를 초기화하면 ONTAP 소스 볼륨에서 참조되는 데이터 블록을 대상 볼륨으로 전송합니다.



SnapCenter SnapMirror와 SnapVault 볼륨 간의 계단식 관계(**Primary > Mirror > Vault**)를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter 버전에 따라 유연한 SnapMirror 관계 관리를 지원합니다. 버전에 따라 유연한 SnapMirror 관계와 이를 설정하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["ONTAP 문서"](#).

SQL Server 리소스에 대한 백업 전략

SQL Server 리소스에 대한 백업 전략 정의

백업 작업을 생성하기 전에 백업 전략을 정의하면 데이터베이스를 성공적으로 복원하거나 복제하는 데 필요한 백업이 있는지 확인하는 데 도움이 됩니다. 백업 전략은 주로 서비스 수준 계약(SLA), 복구 시간 목표(RTO), 복구 지점 목표(RPO)에 따라 결정됩니다.

SLA는 기대되는 서비스 수준을 정의하고 서비스 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RTO는 서비스가 중단된 후 비즈니스 프로세스를 복구해야 하는 시간입니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 수명에 대한 전략을 정의합니다. SLA, RTO, RPO는 백업 전략에 기여합니다.

지원되는 백업 유형

SnapCenter 사용하여 SQL Server 시스템 및 사용자 데이터베이스를 백업하려면 데이터베이스, SQL Server 인스턴스, 가용성 그룹(AG) 등의 리소스 유형을 선택해야 합니다. 스냅샷 기술은 리소스가 있는 볼륨의 온라인, 읽기 전용 복사본을 만드는 데 활용됩니다.

복사 전용 옵션을 선택하면 SQL Server가 트랜잭션 로그를 잘라내지 않도록 지정할 수 있습니다. 다른 백업 애플리케이션과 함께 SQL Server를 관리하는 경우 이 옵션을 사용해야 합니다. 거래 로그를 그대로 유지하면 모든 백업 애플리케이션이 시스템 데이터베이스를 복원할 수 있습니다. 복사 전용 백업은 예약된 백업 순서와 무관하며, 데이터베이스의 백업 및 복원 절차에 영향을 미치지 않습니다.

백업 유형	설명	백업 유형이 있는 복사 전용 옵션
전체 백업 및 로그 백업	시스템 데이터베이스를 백업하고 트랜잭션 로그를 잘라냅니다. SQL Server는 이미 데이터베이스에 커밋된 항목을 제거하여 트랜잭션 로그를 잘라냅니다. 전체 백업이 완료되면 이 옵션은 트랜잭션 정보를 캡처하는 트랜잭션 로그를 생성합니다. 일반적으로 이 옵션을 선택하는 것이 좋습니다. 하지만 백업 시간이 짧다면 전체 백업과 함께 트랜잭션 로그 백업을 실행하지 않도록 선택할 수 있습니다. 마스터 및 msdb 시스템 데이터베이스에 대한 로그 백업을 생성할 수 없습니다. 하지만 모델 시스템 데이터베이스에 대한 로그 백업을 생성할 수 있습니다.	로그를 잘라내지 않고 시스템 데이터베이스 파일과 트랜잭션 로그를 백업합니다. 복사 전용 백업은 차등 기반이나 차등 백업으로 사용할 수 없으며, 차등 기반에 영향을 미치지 않습니다. 복사 전용 전체 백업을 복원하는 것은 다른 전체 백업을 복원하는 것과 같습니다.
전체 데이터베이스 백업	시스템 데이터베이스 파일을 백업합니다. 마스터, 모델, msdb 시스템 데이터베이스에 대한 전체 데이터베이스 백업을 생성할 수 있습니다.	시스템 데이터베이스 파일을 백업합니다.
트랜잭션 로그 백업	가장 최근의 트랜잭션 로그가 백업된 이후 커밋된 트랜잭션만 복사하여 잘린 트랜잭션 로그를 백업합니다. 전체 데이터베이스 백업과 함께 자주 트랜잭션 로그 백업을 예약하면 세분화된 복구 지점을 선택할 수 있습니다.	트랜잭션 로그를 잘라내지 않고 백업합니다. 이 백업 유형은 정기적인 로그 백업의 순서에 영향을 미치지 않습니다. 복사 전용 로그 백업은 온라인 복원 작업을 수행하는 데 유용합니다.

SQL 서버용 플러그인 백업 일정

백업 빈도(일정 유형)는 정책에 지정되고, 백업 일정은 리소스 그룹 구성에 지정됩니다. 백업 빈도나 일정을 결정하는 가장 중요한 요소는 리소스의 변화율과 데이터의 중요도입니다. 자주 사용되는 리소스는 매시간 백업하고, 거의 사용되지 않는 리소스는 하루에 한 번 백업할 수도 있습니다. 기타 요소로는 조직에 대한 리소스의 중요성, 서비스 수준 계약(SLA), 복구 지점 목표(RPO) 등이 있습니다.

SLA는 기대되는 서비스 수준을 정의하고 서비스 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 수명에 대한 전략을 정의합니다.

SLA와 RPO는 데이터 보호 전략에 기여합니다.

많이 사용되는 리소스의 경우에도 하루에 한두 번 이상 전체 백업을 실행할 필요는 없습니다. 예를 들어, 정기적인 트랜잭션 로그 백업을 통해 필요한 백업을 확보하는 데 충분할 수 있습니다. 데이터베이스를 더 자주 백업할수록 SnapCenter 복원 시 사용해야 하는 트랜잭션 로그가 줄어들어 복원 작업이 더 빨라질 수 있습니다.

백업 일정은 다음과 같이 두 부분으로 구성됩니다.

- 백업 주파수

일부 플러그인의 경우 스케줄 유형이라고 하는 백업 빈도(백업을 수행하는 빈도)는 정책 구성의 일부입니다. 정책의 백업 빈도를 시간별, 일별, 주별 또는 월별로 선택할 수 있습니다. 이러한 주파수를 선택하지 않으면 생성된 정책은 주문형 정책만입니다. 설정 > *정책*을 클릭하면 정책에 액세스할 수 있습니다.

- 백업 일정

백업 일정(백업을 정확히 언제 수행해야 하는지)은 리소스 그룹 구성의 일부입니다. 예를 들어, 주간 백업에 대한 정책이 구성된 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 일정을 구성할 수 있습니다. 리소스 > *리소스 그룹*을 클릭하면 리소스 그룹 일정에 액세스할 수 있습니다.

데이터베이스에 필요한 백업 작업 수

필요한 백업 작업 수를 결정하는 요소에는 데이터베이스 크기, 사용된 볼륨 수, 데이터베이스 변경률, 서비스 수준 계약(SLA) 등이 있습니다.

데이터베이스 백업의 경우 선택하는 백업 작업 수는 일반적으로 데이터베이스를 배치한 볼륨 수에 따라 달라집니다. 예를 들어, 한 볼륨에 여러 개의 작은 데이터베이스를 배치하고 다른 볼륨에 큰 데이터베이스를 배치한 경우 작은 데이터베이스에 대한 백업 작업을 하나 만들고 큰 데이터베이스에 대한 백업 작업을 하나씩 만들 수 있습니다.

SQL Server용 플러그인의 백업 명명 규칙

기본 스냅샷 명명 규칙을 사용하거나 사용자 지정 명명 규칙을 사용할 수 있습니다. 기본 백업 명명 규칙은 스냅샷 이름에 타임스탬프를 추가하여 복사본이 생성된 시기를 식별하는 데 도움이 됩니다.

스냅샷은 다음과 같은 기본 명명 규칙을 사용합니다.

resourcegroupname_hostname_timestamp

다음 예와 같이 논리적으로 백업 리소스 그룹의 이름을 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예에서 구문 요소는 다음과 같은 의미를 갖습니다.

- _dts1_은 리소스 그룹 이름입니다.
- _mach1x88_은 호스트 이름입니다.
- _03-12-2015_23.17.26_은 날짜와 타임스탬프입니다.

또는, *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택하여 리소스나 리소스 그룹을 보호하는 동안 스냅샷 이름 형식을 지정할 수 있습니다. 예를 들어, customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname입니다. 기본적으로 타임스탬프 접미사는 스냅샷 이름에 추가됩니다.

SQL Server용 플러그인에 대한 백업 보존 옵션

백업 사본을 보관할 일수를 선택하거나 보관할 백업 사본 수를 지정할 수 있으며, ONTAP 최대 255개 사본까지 보관할 수 있습니다. 예를 들어, 귀하의 조직에서는 10일 분의 백업 사본이나 130개의 백업 사본을 보관하도록 요구할 수 있습니다.

정책을 생성하는 동안 백업 유형과 일정 유형에 대한 보존 옵션을 지정할 수 있습니다.

SnapMirror 복제를 설정하면 보존 정책이 대상 볼륨에 미러링됩니다.

SnapCenter 일정 유형과 일치하는 보존 레이블이 있는 보관된 백업을 삭제합니다. 리소스 또는 리소스 그룹의 일정 유형이 변경된 경우 이전 일정 유형 레이블이 지정된 백업이 시스템에 남아 있을 수 있습니다.



백업 사본을 장기간 보관하려면 SnapVault 백업을 사용해야 합니다.

소스 스토리지 시스템에서 트랜잭션 로그 백업을 보관하는 기간

Microsoft SQL Server용 SnapCenter 플러그인은 최신 복원 작업을 수행하기 위해 트랜잭션 로그 백업이 필요하며, 이를 통해 두 개의 전체 백업 사이의 시간으로 데이터베이스를 복원합니다.

예를 들어, SQL Server 플러그인이 오전 8시에 전체 백업을 수행하고 오후 5시에 또 다른 전체 백업을 수행한 경우 최신 트랜잭션 로그 백업을 사용하여 오전 8시와 오후 5시 사이의 임의의 시간으로 데이터베이스를 복원할 수 있습니다. 트랜잭션 로그를 사용할 수 없는 경우 SQL Server 플러그인은 지정 시간 복원 작업만 수행할 수 있으며, 이 경우 SQL Server 플러그인이 전체 백업을 완료한 시간으로 데이터베이스를 복원합니다.

일반적으로 최신 복구 작업은 하루나 이틀 정도만 필요합니다. 기본적으로 SnapCenter 최소 2일간 보관합니다.

동일한 볼륨에 여러 데이터베이스가 있음

백업 정책에 백업당 최대 데이터베이스 수를 설정하는 옵션이 있으므로(기본값은 100) 모든 데이터베이스를 동일한 볼륨에 넣을 수 있습니다.

예를 들어, 동일한 볼륨에 200개의 데이터베이스가 있는 경우 두 개의 스냅샷이 생성되고, 두 개의 스냅샷에는 각각 100개의 데이터베이스가 포함됩니다.

SQL Server용 플러그인의 기본 또는 보조 스토리지 볼륨을 사용한 백업 사본 검증

기본 저장소 볼륨이나 SnapMirror 또는 SnapVault 보조 저장소 볼륨에서 백업 사본을 확인할 수 있습니다. 보조 저장 볼륨을 사용하여 검증하면 기본 저장 볼륨의 부하가 줄어듭니다.

기본 또는 보조 스토리지 볼륨에 있는 백업을 검증하면 모든 기본 및 보조 스냅샷이 검증됨으로 표시됩니다.

SnapMirror 및 SnapVault 보조 스토리지 볼륨의 백업 사본을 확인하려면 SnapRestore 라이선스가 필요합니다.

검증 작업을 예약하는 시기

SnapCenter 백업을 생성한 직후에 백업을 검증할 수 있지만, 그렇게 하면 백업 작업을 완료하는데 필요한 시간이 크게 늘어나고 리소스도 많이 소모됩니다. 따라서 검증은 나중에 별도의 작업으로 예약하는 것이 항상 가장 좋습니다. 예를 들어, 매일 오후 5시에 데이터베이스를 백업하는 경우 1시간 후인 오후 6시에 검증이 수행되도록 예약할 수 있습니다.

같은 이유로, 백업을 수행할 때마다 백업 검증을 실행할 필요는 일반적으로 없습니다. 정기적으로(그러나 덜 빈번하게) 검증을 수행하는 것만으로도 백업의 무결성을 보장하는 데 충분합니다. 단일 검증 작업으로 여러 백업을 동시에 검증할 수 있습니다.

SQL Server에 대한 복원 전략

복원 작업의 소스 및 대상

기본 또는 보조 저장소의 백업 사본에서 SQL Server 데이터베이스를 복원할 수 있습니다. 원래 위치 외에도 다른 대상에 데이터베이스를 복원할 수 있으므로 요구 사항에 맞는 대상을 선택할 수 있습니다.

복원 작업을 위한 소스

기본 또는 보조 저장소에서 데이터베이스를 복원할 수 있습니다.

복원 작업의 대상지

다양한 대상에 데이터베이스를 복원할 수 있습니다.

목적지	설명
원래 위치	기본적으로 SnapCenter 동일한 SQL Server 인스턴스의 동일한 위치에 데이터베이스를 복원합니다.
다른 위치	동일한 호스트 내의 모든 SQL Server 인스턴스에서 데이터베이스를 다른 위치로 복원할 수 있습니다.
다른 데이터베이스 이름을 사용하는 원래 위치 또는 다른 위치	백업이 생성된 동일한 호스트의 모든 SQL Server 인스턴스에 다른 이름으로 데이터베이스를 복원할 수 있습니다.



VMDK(NFS 및 VMFS 데이터 저장소)의 SQL 데이터베이스에 대한 ESX 서버 간 대체 호스트로 복원하는 기능은 지원되지 않습니다.

SnapCenter 에서 지원하는 SQL Server 복구 모델

각 데이터베이스 유형에는 기본적으로 특정 복구 모델이 할당됩니다. SQL Server 데이터베이스 관리자는 각 데이터베이스를 다른 복구 모델로 재할당할 수 있습니다.

SnapCenter 세 가지 유형의 SQL Server 복구 모델을 지원합니다.

- 간단한 복구 모델

단순 복구 모델을 사용하면 트랜잭션 로그를 백업할 수 없습니다.

- 전체 복구 모델

전체 복구 모델을 사용하면 오류 발생 지점부터 이전 상태로 데이터베이스를 복원할 수 있습니다.

- 대량 로깅 복구 모델

대량 로깅 복구 모델을 사용하는 경우 대량 로깅 작업을 수동으로 다시 실행해야 합니다. 복원 전에 작업의 커밋 레코드가 포함된 트랜잭션 로그가 백업되지 않은 경우 대량으로 로깅된 작업을 수행해야 합니다. 대량 로깅 작업으로 데이터베이스에 1,000만 개의 행이 삽입되고 트랜잭션 로그가 백업되기 전에 데이터베이스에 오류가 발생하면 복원된 데이터베이스에는 대량 로깅 작업으로 삽입된 행이 포함되지 않습니다.

복원 작업 유형

SnapCenter 사용하면 SQL Server 리소스에 대해 다양한 유형의 복원 작업을 수행할 수 있습니다.

- 최신 정보를 복원합니다
- 이전 시점으로 복원

다음과 같은 상황에서는 최신 시점으로 복원하거나 이전 시점으로 복원할 수 있습니다.

- SnapMirror 또는 SnapVault 보조 저장소에서 복원
- 대체 경로(위치)로 복원



SnapCenter 볼륨 기반 SnapRestore 지원하지 않습니다.

최신 상태로 복원

최신 복원 작업(기본적으로 선택됨)에서는 데이터베이스가 오류 지점까지 복구됩니다. SnapCenter 다음 순서를 수행하여 이를 달성합니다.

1. 데이터베이스를 복원하기 전에 마지막 활성 트랜잭션 로그를 백업합니다.
2. 선택한 전체 데이터베이스 백업에서 데이터베이스를 복원합니다.
3. 데이터베이스에 커밋되지 않은 모든 트랜잭션 로그를 적용합니다(백업이 생성된 시점부터 가장 최근 시점까지의 백업에서 가져온 트랜잭션 로그 포함).

거래 로그가 앞으로 이동되어 선택한 데이터베이스에 적용됩니다.

최신 복원 작업에는 연속된 트랜잭션 로그 세트가 필요합니다.

SnapCenter 로그 전달 백업 파일에서 SQL Server 데이터베이스 트랜잭션 로그를 복원할 수 없기 때문에(로그 전달을 사용하면 기본 서버 인스턴스의 기본 데이터베이스에서 별도의 보조 서버 인스턴스의 하나 이상의 보조 데이터베이스로 트랜잭션 로그 백업을 자동으로 보낼 수 있음) 트랜잭션 로그 백업에서 최신 복원 작업을 수행할 수 없습니다. 이러한 이유로 SnapCenter 사용하여 SQL Server 데이터베이스 트랜잭션 로그 파일을 백업해야 합니다.

모든 백업에 대한 최신 복원 기능을 유지할 필요가 없는 경우 백업 정책을 통해 시스템의 트랜잭션 로그 백업 보존을 구성할 수 있습니다.

최신 복원 작업의 예

매일 정오에 SQL Server 백업을 실행하고, 수요일 오후 4시에 백업에서 복원해야 한다고 가정해 보겠습니다. 어떤 이유에서인지 수요일 정오에 백업한 내용을 검증하는 데 실패하여 화요일 정오에 백업한 내용을 복원하기로 결정했습니다. 그 후 백업이 복원되면 모든 트랜잭션 로그가 앞으로 이동하여 복원된 데이터베이스에 적용됩니다. 화요일 백업을 만들 때 커밋되지 않은 로그부터 시작하여 수요일 오후 4시에 작성된 최신 트랜잭션 로그(트랜잭션 로그가 백업된 경우)까지 계속됩니다.

이전 시점으로 복원

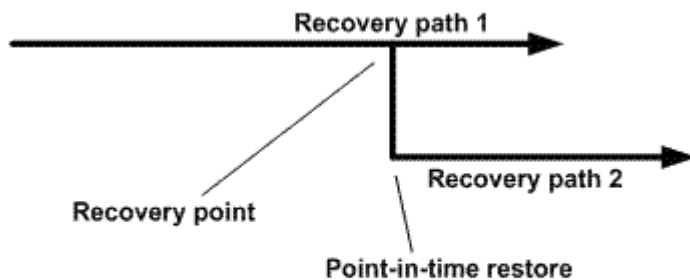
지정 시점 복원 작업에서는 데이터베이스가 과거의 특정 시점으로만 복원됩니다. 지정 시간 복원 작업은 다음과 같은 복원 상황에서 발생합니다.

- 데이터베이스는 백업된 트랜잭션 로그의 특정 시간으로 복원됩니다.
- 데이터베이스가 복원되고, 백업된 트랜잭션 로그의 하위 집합만 적용됩니다.



데이터베이스를 특정 시점으로 복원하면 새로운 복구 경로가 생성됩니다.

다음 이미지는 지정 시점 복원 작업이 수행될 때 발생하는 문제를 보여줍니다.



그림에서 복구 경로 1은 전체 백업과 그에 따른 여러 트랜잭션 로그 백업으로 구성됩니다. 데이터베이스를 특정 시점으로 복원합니다. 특정 시점 복원 작업 이후에 새로운 트랜잭션 로그 백업이 생성되며, 이로 인해 복구 경로 2가 생성됩니다. 새로운 전체 백업을 생성하지 않고 새로운 트랜잭션 로그 백업이 생성됩니다. 데이터 손상이나 기타 문제로 인해 새로운 전체 백업을 생성할 때까지 현재 데이터베이스를 복원할 수 없습니다. 또한, 복구 경로 2에서 생성된 트랜잭션 로그를 복구 경로 1에 속한 전체 백업에 적용할 수 없습니다.

트랜잭션 로그 백업을 적용하는 경우 백업된 트랜잭션의 적용을 중지할 특정 날짜와 시간을 지정할 수도 있습니다. 이를 위해 사용 가능한 범위 내에서 날짜와 시간을 지정하면 SnapCenter 해당 시점 이전에 커밋되지 않은 모든 트랜잭션을 제거합니다. 이 방법을 사용하면 손상이 발생하기 전 시점으로 데이터베이스를 복원하거나 실수로 데이터베이스나 테이블을 삭제한 경우 복구할 수 있습니다.

특정 시점 복원 작업의 예

자정에 전체 데이터베이스 백업을 한 번 하고, 매시간 트랜잭션 로그 백업을 한다고 가정해 보겠습니다. 데이터베이스는 오전 9시 45분에 충돌하지만, 여전히 실패한 데이터베이스의 트랜잭션 로그를 백업합니다. 다음 지정 시점 복원 시나리오 중에서 선택할 수 있습니다.

- 자정에 만든 전체 데이터베이스 백업을 복원하고 그 이후에 변경된 데이터베이스의 손실을 감수합니다. (옵션: 없음)
- 전체 데이터베이스 백업을 복원하고 오전 9시 45분까지 모든 트랜잭션 로그 백업을 적용합니다(옵션: 로그까지)
- 전체 데이터베이스 백업을 복원하고 트랜잭션 로그 백업을 적용하며, 마지막 트랜잭션 로그 백업 세트에서 트랜잭션을 복원할 시간을 지정합니다. (옵션: 특정 시간까지)

이 경우 특정 오류가 보고된 날짜와 시간을 계산하게 됩니다. 지정된 날짜와 시간 이전에 커밋되지 않은 모든 거래는 제거됩니다.

SQL Server에 대한 복제 전략 정의

복제 전략을 정의하면 데이터베이스를 성공적으로 복제할 수 있습니다.

1. 복제 작업과 관련된 제한 사항을 검토합니다.
2. 필요한 클론 유형을 결정하세요.

복제 작업의 한계

데이터베이스를 복제하기 전에 복제 작업의 제한 사항을 알고 있어야 합니다.

- 11.2.0.4에서 12.1.0.1까지의 Oracle 버전을 사용하는 경우 *renamedg* 명령을 실행하면 복제 작업이 중단됩니다. 이 문제를 해결하려면 Oracle 패치 19544733을 적용하세요.
- 호스트에 직접 연결된 LUN(예: Windows 호스트에서 Microsoft iSCSI Initiator 사용)에서 동일한 Windows 호스트의 VMDK 또는 RDM LUN이나 다른 Windows 호스트로 데이터베이스를 복제하는 것은 지원되지 않습니다.
- 볼륨 마운트 지점의 루트 디렉토리는 공유 디렉토리가 될 수 없습니다.
- 복제본이 포함된 LUN을 새 볼륨으로 이동하면 복제본을 삭제할 수 없습니다.

복제 작업의 유형

SnapCenter 사용하면 SQL Server 데이터베이스 백업이나 프로덕션 데이터베이스를 복제할 수 있습니다.

- 데이터베이스 백업에서 복제

복제된 데이터베이스는 새로운 애플리케이션을 개발하기 위한 기준으로 활용될 수 있으며, 프로덕션 환경에서 발생하는 애플리케이션 오류를 격리하는 데 도움이 됩니다. 복제된 데이터베이스는 소프 데이터베이스 오류를 복구하는 데에도 사용할 수 있습니다.

- 클론 라이프사이클

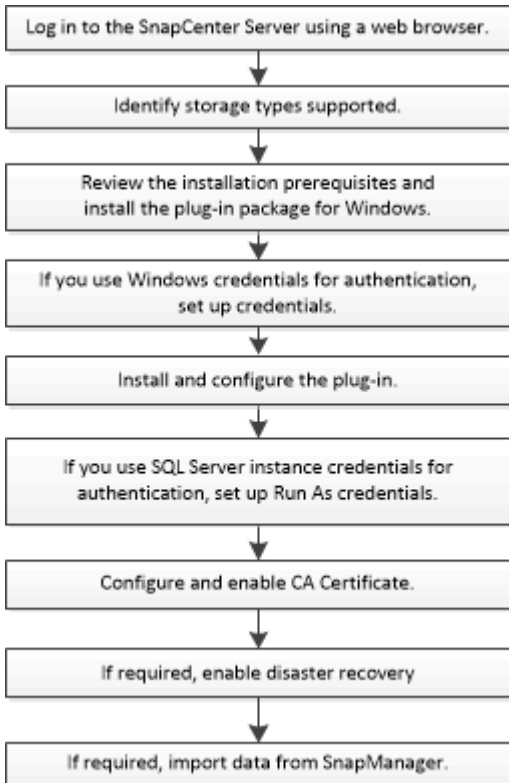
SnapCenter 사용하면 프로덕션 데이터베이스가 바쁘지 않을 때 발생하는 반복적인 복제 작업을 예약할 수 있습니다.

Microsoft SQL Server용 SnapCenter 플러그인 설치를 준비하세요

Microsoft SQL Server용 SnapCenter 플러그인 설치 워크플로

SQL Server 데이터베이스를 보호하려면 Microsoft SQL Server용 SnapCenter 플러그인을

설치하고 설정해야 합니다.



Microsoft SQL Server용 호스트 추가 및 SnapCenter 플러그인 설치를 위한 필수 구성 요소
호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 충족해야 합니다.

- iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.
- 원격 호스트에 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 사용자가 있어야 합니다.
- SnapCenter 에서 클러스터 노드를 관리하는 경우 클러스터의 모든 노드에 대한 관리 권한이 있는 사용자가 있어야 합니다.
- SQL Server에 대한 sysadmin 권한이 있는 사용자가 있어야 합니다.

Microsoft SQL Server용 SnapCenter 플러그인은 Microsoft VDI 프레임워크를 사용하는데, 이를 위해서는 시스템 관리자 액세스가 필요합니다.

"Microsoft 지원 문서 2926557: SQL Server VDI 백업 및 복원 작업에는 시스템 관리자 권한이 필요합니다."

- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.
- Microsoft SQL Server용 SnapManager 설치된 경우 서비스와 일정을 중지하거나 비활성화해야 합니다.

백업 또는 복제 작업을 SnapCenter 로 가져올 계획이라면 Microsoft SQL Server용 SnapManager 제거하지 마세요.

- 호스트는 서버에서 정규화된 도메인 이름(FQDN)으로 확인 가능해야 합니다.

호스트 파일을 수정하여 확인할 수 있도록 하고 호스트 파일에 짧은 이름과 FQDN이 모두 지정된 경우 SnapCenter

호스트 파일에 다음 형식으로 항목을 만듭니다. <ip_address> <host_fqdn> <host_name>

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항과 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	마이크로소프트 윈도우 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	• ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 • 파워셸 코어 7.4.2 • Java 11 Oracle Java 및 OpenJDK Java 11 Oracle Java 및 OpenJDK는 SAP HANA, IBM Db2, PostgreSQL, MySQL, NetApp 지원 플러그인 및 Windows 호스트에 설치할 수 있는 기타 사용자 정의 애플리케이션에만 필요합니다. 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구".

Windows용 SnapCenter 플러그인 패키지에 대한 자격 증명 설정

SnapCenter SnapCenter 작업을 위해 사용자를 인증하기 위해 자격 증명을 사용합니다. SnapCenter 플러그인을 설치하기 위한 자격 증명과 데이터베이스나 Windows 파일 시스템에서 데이터 보호 작업을 수행하기 위한 추가 자격 증명을 만들어야 합니다.

시작하기 전에

- 플러그인을 설치하기 전에 Windows 자격 증명을 설정해야 합니다.
- 원격 호스트의 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정해야 합니다.
- Windows 호스트의 SQL 인증

플러그인을 설치한 후 SQL 자격 증명을 설정해야 합니다.

Microsoft SQL Server용 SnapCenter 플러그인을 배포하는 경우 플러그인을 설치한 후 SQL 자격 증명을 설정해야 합니다. SQL Server sysadmin 권한이 있는 사용자에게 대한 자격 증명을 설정합니다.

SQL 인증 방법은 SQL Server 인스턴스를 대상으로 인증합니다. 즉, SQL Server 인스턴스는 SnapCenter 에서 검색되어야 합니다. 따라서 SQL 자격 증명을 추가하기 전에 호스트를 추가하고, 플러그인 패키지를 설치하고, 리소스를 새로 고쳐야 합니다. 일정 예약이나 리소스 검색 등의 작업을 수행하려면 SQL Server 인증이 필요합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *자격 증명*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 자격 증명 페이지에서 자격 증명을 구성하는 데 필요한 정보를 지정합니다.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.

이 분야에서는...	이렇게 하세요...
사용자 이름/비밀번호	인증에 사용할 사용자 이름과 비밀번호를 입력하세요. - 도메인 관리자 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자를 지정하세요. 사용자 이름 필드에 사용할 수 있는 형식은 다음과 같습니다. - NetBIOS\UserName - Domain FQDN\UserName - 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우, SnapCenter 플러그인을 설치할 시스템에 기본 제공되는 로컬 관리자를 지정하십시오. 사용자 계정에 승격된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우, 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다. UserName 비밀번호에 큰따옴표(")나 백틱(`)을 사용하지 마세요. 비밀번호에 '<' 기호와 '!>' 기호를 함께 사용하면 안 됩니다. 예를 들어, lessthan<!10, lessthan10<!, backtick`12.
인증 모드	사용할 인증 모드를 선택하세요. SQL 인증 모드를 선택하는 경우 SQL 서버 인스턴스와 SQL 인스턴스가 있는 호스트도 지정해야 합니다.

5. *확인*을 클릭합니다.

자격 증명 설정을 마친 후 사용자 및 액세스 페이지에서 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

개별 SQL Server 리소스에 대한 자격 증명 구성

각 사용자에게 대해 개별 SQL Server 리소스에 대한 데이터 보호 작업을 수행하기 위해 자격 증명을 구성할 수 있습니다. 자격 증명을 전역적으로 구성할 수 있지만 특정 리소스에 대해서만 이 작업을 수행하고 싶을 수도 있습니다.

이 작업에 관하여

- 인증을 위해 Windows 자격 증명을 사용하는 경우 플러그인을 설치하기 전에 자격 증명을 설정해야 합니다.

하지만 인증을 위해 SQL Server 인스턴스를 사용하는 경우 플러그인을 설치한 후 자격 증명을 추가해야 합니다.

- 자격 증명을 설정하는 동안 SQL 인증을 활성화한 경우, 검색된 인스턴스나 데이터베이스에 빨간색 자물쇠 아이콘이

표시됩니다.

자물쇠 아이콘이 나타나면 인스턴스 또는 데이터베이스 자격 증명을 지정해야 인스턴스 또는 데이터베이스를 리소스 그룹에 성공적으로 추가할 수 있습니다.

- 다음 조건이 충족되는 경우 sysadmin 액세스 권한이 없는 RBAC(역할 기반 액세스 제어) 사용자에게 자격 증명을 할당해야 합니다.
 - 자격 증명은 SQL 인스턴스에 할당됩니다.
 - SQL 인스턴스 또는 호스트는 RBAC 사용자에게 할당됩니다.

사용자는 리소스 그룹 권한과 백업 권한을 모두 가지고 있어야 합니다.

1단계: 자격 증명 추가 및 구성

1. 왼쪽 탐색 창에서 *설정*을 선택합니다.
2. 설정 페이지에서 *자격 증명*을 선택합니다.
 - a. 새로운 자격 증명을 추가하려면 *새로 만들기*를 선택하세요.
 - b. 자격 증명 페이지에서 자격 증명을 구성합니다.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.
사용자 이름	SQL Server 인증에 사용되는 사용자 이름을 입력하세요. • 도메인 관리자 또는 관리자 그룹의 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹의 구성원을 지정하세요. 사용자 이름 필드에 사용할 수 있는 형식은 다음과 같습니다. ◦ NetBIOS\사용자 이름 ◦ 도메인 FQDN\사용자 이름 • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우, SnapCenter 플러그인을 설치할 시스템에 기본 제공되는 로컬 관리자를 지정하십시오. 사용자 계정에 승격된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우, 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다: <i>UserName</i>
비밀번호	인증에 사용되는 비밀번호를 입력하세요.
인증 모드	SQL Server 인증 모드를 선택하세요. Windows 사용자에게 SQL 서버에서 sysadmin 권한이 있는 경우 Windows 인증을 선택할 수도 있습니다.
주인	호스트를 선택하세요.
SQL Server 인스턴스	SQL Server 인스턴스를 선택합니다.

- c. *확인*을 선택하여 자격 증명을 추가합니다.

2단계: 인스턴스 구성

1. 왼쪽 탐색 창에서 *리소스*를 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *인스턴스*를 선택합니다.
 - a. image:.../media/filter_icon.png[필터 아이콘]를 선택한 다음 호스트 이름을 선택하여 인스턴스를 필터링합니다.
 - b. 필터 창을 닫으려면 image:.../media/filter_icon.png[필터 아이콘]을 선택하세요.
3. 인스턴스 보호 페이지에서 인스턴스를 보호하고 필요한 경우 *자격 증명 구성*을 선택합니다.

SnapCenter 서버에 로그인한 사용자가 Microsoft SQL Server용 SnapCenter 플러그인에 액세스할 수 없는 경우 사용자는 자격 증명을 구성해야 합니다.



자격 증명 옵션은 데이터베이스와 가용성 그룹에는 적용되지 않습니다.

4. *리소스 새로고침*을 선택하세요.

Windows Server 2016 이상에서 gMSA 구성

Windows Server 2016 이상에서는 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 관리 서비스 계정(gMSA)을 만들 수 있습니다.

시작하기 전에

- Windows Server 2016 이상 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2016 이상 호스트가 있어야 합니다.

단계

1. gMSA의 각 개체에 대해 고유한 비밀번호를 생성하려면 KDS 루트 키를 만듭니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 다음 명령을 실행합니다. Add-KDSRootKey -EffectiveImmediately
3. gMSA를 만들고 구성하세요.
 - a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
domainName\accountName$  
.. 그룹에 컴퓨터 객체를 추가합니다.  
.. 방금 만든 사용자 그룹을 사용하여 gMSA를 만듭니다.
```

예를 들어,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. 달리다 `Get-ADServiceAccount` 서비스 계정을 확인하는 명령입니다.
```

4. 호스트에서 gMSA를 구성하세요.

- a. gMSA 계정을 사용하려는 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.

이렇게 하려면 PowerShell에서 다음 명령을 실행하세요.

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. 호스트를 다시 시작합니다.
- b. PowerShell 명령 프롬프트에서 다음 명령을 실행하여 호스트에 gMSA를 설치합니다. `Install-AdServiceAccount <gMSA>`
- c. 다음 명령을 실행하여 gMSA 계정을 확인하세요. `Test-AdServiceAccount <gMSA>`

5. 호스트에서 구성된 gMSA에 관리 권한을 할당합니다.

6. SnapCenter 서버에서 구성된 gMSA 계정을 지정하여 Windows 호스트를 추가합니다.

SnapCenter Server는 호스트에 선택된 플러그인을 설치하고, 플러그인 설치 중에 지정된 gMSA가 서비스 로그인 계정으로 사용됩니다.

Microsoft SQL Server용 SnapCenter 플러그인 설치

호스트를 추가하고 **Windows**용 **SnapCenter** 플러그인 패키지를 설치합니다.

호스트를 추가하고 플러그인 패키지를 설치하려면 SnapCenter 호스트 추가 페이지를 사용해야

합니다. 플러그인은 원격 호스트에 자동으로 설치됩니다.

시작하기 전에

- SnapCenter 서버 호스트의 운영 체제가 Windows 2019이고 플러그인 호스트의 운영 체제가 Windows 2022인 경우 다음을 수행해야 합니다.
 - Windows Server 2019(OS 빌드 17763.5936) 이상으로 업그레이드하세요.
 - Windows Server 2022(OS 빌드 20348.2402) 이상으로 업그레이드하세요.
- SnapCenter 관리자 역할과 같이 플러그인 설치 및 제거 권한이 있는 역할에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하면 호스트에서 UAC를 비활성화해야 합니다.
- 메시지 큐잉 서비스가 실행 상태인지 확인해야 합니다.
- 그룹 관리 서비스 계정(gMSA)을 사용하는 경우 관리자 권한으로 gMSA를 구성해야 합니다.

"Windows Server 2016 이상에서 SQL을 위한 그룹 관리 서비스 계정 구성"

이 작업에 관하여

SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.

개별 호스트나 클러스터에 대해 호스트를 추가하고 플러그인 패키지를 설치할 수 있습니다. 클러스터나 Windows Server 장애 조치(Failover) 클러스터링(WSFC)에 플러그인을 설치하는 경우 플러그인은 클러스터의 모든 노드에 설치됩니다.

호스트 관리에 대한 정보는 다음을 참조하세요. "[호스트 관리](#)".

단계

1. 왼쪽 탐색 창에서 *호스트*를 선택합니다.
2. 상단에 관리되는 호스트 탭이 선택되어 있는지 확인하세요.
3. *추가*를 선택하세요.
4. 호스트 페이지에서 다음을 수행합니다.

이 분야에서는...	이렇게 하세요...
호스트 유형	호스트 유형으로 Windows를 선택합니다. SnapCenter 서버는 호스트를 추가한 다음, 호스트에 플러그인이 아직 설치되어 있지 않으면 Windows용 플러그인을 설치합니다. 플러그인 페이지에서 Microsoft SQL Server 옵션을 선택하면 SnapCenter Server가 SQL Server용 플러그인을 설치합니다.

이 분야에서는...	이렇게 하세요...
호스트 이름	호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하세요. 신뢰할 수 없는 도메인 호스트의 경우 IP 주소는 FQDN으로 확인되는 경우에만 지원됩니다. SnapCenter DNS의 적절한 구성에 달려 있습니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다. 다음 중 하나의 IP 주소나 FQDN을 입력할 수 있습니다. • 독립형 호스트 • WSFC SnapCenter 사용하여 호스트를 추가하고 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.
신임장	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성하세요. 자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하세요. 지정한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다.  자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

6. *추가 옵션*을 선택하세요.

이 분야에서는...	이렇게 하세요...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정하세요. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트에 표시됩니다.  플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.
설치 경로	기본 경로는 C:\Program Files\NetApp\ SnapCenter 입니다. 선택적으로 경로를 사용자 정의할 수 있습니다.

이 분야에서는...	이렇게 하세요...
클러스터의 모든 호스트를 추가합니다.	WSFC 또는 SQL 가용성 그룹의 모든 클러스터 노드를 추가하려면 이 확인란을 선택합니다. 클러스터 내에서 사용 가능한 여러 SQL 가용성 그룹을 관리하고 식별하려면 GUI에서 적절한 클러스터 확인란을 선택하여 모든 클러스터 노드를 추가해야 합니다.
사전 설치 확인 건너뛰기	플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택하세요.
플러그인 서비스를 실행하려면 그룹 관리 서비스 계정(gMSA)을 사용하세요.	플러그인 서비스를 실행하기 위해 그룹 관리 서비스 계정(gMSA)을 사용하려면 이 확인란을 선택하세요. 다음 형식으로 gMSA 이름을 제공하세요: domainName\accountName\$.  호스트가 gMSA로 추가되고 gMSA에 로그인 및 시스템 관리자 권한이 있는 경우, gMSA는 SQL 인스턴스에 연결하는 데 사용됩니다.

7. *제출*을 선택하세요.

8. SQL 플러그인의 경우, 로그 디렉토리를 구성할 호스트를 선택합니다.

- a. *로그 디렉터리 구성*을 선택하고 호스트 로그 디렉터리 구성 페이지에서 *찾아보기*를 선택한 후 다음 단계를 완료합니다.

선택할 수 있는 항목은 NetApp LUN(드라이브)뿐입니다. SnapCenter 백업 작업의 일부로 호스트 로그 디렉토리를 백업하고 복제합니다.

Configure Plug-in for SQL Server

Configure the log backup directory for clusmigag.smsqlqa3.gdl.englab.netapp.com

Configure host log directory

Host

Host log directory
dedicated disk directory path
Apply
Browse

Configure FCI instance log directory

FCI instance
Nothing selected

FCI log directory
shared disk directory path
Apply
Browse

- i. 호스트 로그가 저장될 호스트의 드라이브 문자나 마운트 지점을 선택합니다.
- ii. 필요한 경우 하위 디렉토리를 선택하세요.
- iii. *저장*을 선택하세요.

9. *제출*을 선택하세요.

사전 검사 건너뛰기 확인란을 선택하지 않은 경우, 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 유효성 검사가 수행됩니다. 디스크 공간, RAM, PowerShell 버전, .NET 버전, 위치(Windows 플러그인의 경우), Java 버전(Linux 플러그인의 경우)이 최소 요구 사항을 충족하는지 검증됩니다. 최소 요구 사항을 충족하지 못하면 해당 오류 또는 경고 메시지가 표시됩니다.

오류가 디스크 공간이나 RAM과 관련된 경우 C:\Program Files\NetApp\ SnapCenter WebApp에 있는 web.config 파일을 업데이트하여 기본값을 수정할 수 있습니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.



HA 설정에서 web.config 파일을 업데이트하는 경우 두 노드에서 모두 파일을 업데이트해야 합니다.

10. 설치 진행 상황을 모니터링합니다.

cmdlet을 사용하여 여러 원격 호스트에 **Microsoft SQL Server용 SnapCenter** 플러그인을 설치합니다.

Install-SmHostPackage PowerShell cmdlet을 사용하여 여러 호스트에 Microsoft SQL Server용 SnapCenter 플러그인을 동시에 설치할 수 있습니다.

시작하기 전에

플러그인 패키지를 설치하려는 각 호스트에서 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter 에 로그인해야 합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 Open-SmConnection cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
3. Install-SmHostPackage cmdlet과 필요한 매개변수를 사용하여 여러 원격 호스트에 Microsoft SQL Server용 SnapCenter 플러그인을 설치합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

플러그인을 수동으로 이미 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려는 경우 `-skipprecheck` 옵션을 사용할 수 있습니다.

4. 원격 설치를 위한 자격 증명을 입력하세요.

명령줄에서 **Microsoft SQL Server용 SnapCenter** 플러그인을 자동으로 설치합니다.

SnapCenter 사용자 인터페이스 내에서 Microsoft SQL Server용 SnapCenter 플러그인을 설치해야 합니다. 하지만 어떤 이유로든 실행할 수 없다면 Windows 명령줄에서 자동 모드로 SQL Server 플러그인 설치 프로그램을 무인으로 실행할 수 있습니다.

시작하기 전에

- Microsoft SQL Server용 SnapCenter 플러그인을 설치하기 전에 이전 버전을 삭제해야 합니다.

자세한 내용은 다음을 참조하세요. "[플러그인 호스트에서 SnapCenter 플러그인을 수동으로 직접 설치하는 방법](#)".

단계

1. 플러그인 호스트에 C:\temp 폴더가 있는지, 로그인한 사용자가 해당 폴더에 대한 전체 액세스 권한이 있는지 확인합니다.
2. C:\ProgramData\NetApp\SnapCenter\Package Repository에서 SQL Server 소프트웨어 플러그인을 다운로드합니다.

이 경로는 SnapCenter 서버가 설치된 호스트에서 접근할 수 있습니다.

3. 플러그인을 설치하려는 호스트에 설치 파일을 복사합니다.
4. 로컬 호스트의 Windows 명령 프롬프트에서 플러그인 설치 파일을 저장한 디렉토리로 이동합니다.
5. SQL Server 소프트웨어용 플러그인을 설치하세요:

```
"snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"  
/log"Log_Path" BI_SNAPCENTER_PORT=Num  
SUITE_INSTALLDIR="Install_Directory_Path"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW,SCSQL
```

플레이스홀더 값을 데이터로 바꾸세요

- Debug_Log_Path는 제품군 설치 프로그램 로그 파일의 이름과 위치입니다.
- Log_Path는 플러그인 구성 요소(SCW, SCSQL, SMCore)의 설치 로그 위치입니다.
- Num은 SnapCenter SMCore와 통신하는 포트입니다.
- Install_Directory_Path는 호스트 플러그인 패키지 설치 디렉토리입니다.
- domain\administrator는 Microsoft Windows 웹 서비스 계정으로 SnapCenter 플러그인입니다.
- password는 Microsoft Windows 웹 서비스 계정으로 SnapCenter 플러그인의 비밀번호입니다.

```
"snapcenter_windows_host_plugin.exe"/silent  
/debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\\" BI_SNAPCENTER_PORT=8145  
SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW,SCSQL
```



SQL Server 플러그인을 설치하는 동안 전달되는 모든 매개변수는 대소문자를 구분합니다.

6. Windows 작업 스케줄러, 기본 설치 로그 파일 C:\Installdebug.log 및 C:\Temp에 있는 추가 설치 파일을 모니터링합니다.
7. %temp% 디렉토리를 모니터링하여 msix.exe 설치 프로그램이 오류 없이 소프트웨어를 설치하는지 확인합니다.



SQL Server용 플러그인을 설치하면 플러그인이 SnapCenter 서버가 아닌 호스트에 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록할 수 있습니다. 호스트가 추가되면 플러그인이 자동으로 검색됩니다.

SQL Server용 플러그인 설치 상태 모니터링

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행 상황을 모니터링할 수 있습니다. 설치가 완료되었는지 또는 문제가 있는지 확인하기 위해 설치 진행 상황을 확인하는

것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 플러그인 설치 작업만 나열되도록 목록을 필터링하려면 다음을 수행합니다.
 - a. *필터*를 클릭하세요.
 - b. 선택 사항: 시작 날짜와 종료 날짜를 지정합니다.
 - c. 유형 드롭다운 메뉴에서 *플러그인 설치*를 선택합니다.
 - d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
 - e. *적용*을 클릭하세요.
4. 설치 작업을 선택하고 *세부정보*를 클릭하면 작업 세부정보를 볼 수 있습니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

CA 인증서 구성

CA 인증서 CSR 파일 생성

인증서 서명 요청(CSR)을 생성하고, 생성된 CSR을 사용하여 인증 기관(CA)에서 얻을 수 있는 인증서를 가져올 수 있습니다. 인증서에는 개인 키가 연결됩니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.



CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 정보는 다음을 참조하세요. "[CA 인증서 CSR 파일을 생성하는 방법](#)".



도메인(*.domain.company.com)이나 시스템(machine1.domain.company.com)에 대한 CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN)과 해당 호스트 이름을 CA 인증서에 명시해야 합니다. 인증서를 구매하기 전에 주체 대체 이름(SAN) 필드를 입력하여 인증서를 업데이트할 수 있습니다. 와일드카드

인증서(*.domain.company.com)의 경우 인증서에는 해당 도메인의 모든 호스트 이름이 암묵적으로 포함됩니다.

CA 인증서 가져오기

Microsoft 관리 콘솔(MMC)을 사용하여 CA 인증서를 SnapCenter 서버와 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.
2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
3. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > *인증서*를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 버튼으로 클릭한 다음, 모든 작업 > *가져오기*를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
개인 키 가져오기	예 옵션을 선택하고 개인 키를 가져온 후 *다음*을 클릭합니다.
가져오기 파일 형식	변경하지 마세요. *다음*을 클릭하세요.
보안	내보낸 인증서에 사용할 새 비밀번호를 지정한 후 *다음*을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.



인증서 가져오기는 개인 키와 함께 제공되어야 합니다(지원되는 형식: *.pfx, *.p12, *.p7b).

7. "개인" 폴더에 대해서도 5단계를 반복합니다.

CA 인증서 지문을 받으세요

인증서 지문은 인증서를 식별하는 16진수 문자열입니다. 지문은 지문 알고리즘을 사용하여 인증서 내용으로부터 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.
 - a. 인증서를 두 번 클릭합니다.
 - b. 인증서 대화 상자에서 세부정보 탭을 클릭합니다.
 - c. 필드 목록을 스크롤하여 *지문*을 클릭하세요.

d. 상자에서 16진수 문자를 복사하세요.

e. 16진수 사이의 공백을 제거하세요.

예를 들어, 지문이 "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b"인 경우 공백을 제거하면 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.

a. 다음 명령을 실행하여 설치된 인증서의 지문을 나열하고 주체 이름으로 최근에 설치된 인증서를 식별합니다.

```
Get-Childitem -경로 인증서:\LocalMachine\My
```

b. 지문을 복사하세요.

Windows 호스트 플러그인 서비스를 사용하여 **CA** 인증서 구성

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스로 CA 인증서를 구성해야 합니다.

SnapCenter 서버와 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하는 기존 인증서 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

예를 들어:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스에 바인딩합니다.
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

예를 들어:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```


플러그인에 대한 CA 인증서 활성화

CA 인증서를 구성하고 SnapCenter 서버와 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- `Set-SmCertificateSettings` cmdlet을 실행하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- `_Get-SmCertificateSettings_`를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 하나 또는 여러 개의 플러그인 호스트를 선택하세요.
4. *추가 옵션*을 클릭하세요.
5. *인증서 검증 사용*을 선택합니다.

당신이 완료한 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- *  *는 CA 인증서가 활성화되지 않았거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- *  *는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- *  *는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- *  *는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

재해 복구 구성

SQL Server용 SnapCenter 플러그인의 재해 복구

SQL Server용 SnapCenter 플러그인이 다운되면 다음 단계에 따라 다른 SQL 호스트로 전환하고 데이터를 복구하세요.

시작하기 전에

- 보조 호스트는 기본 호스트와 동일한 운영 체제, 애플리케이션 및 호스트 이름을 가져야 합니다.
- 호스트 추가 또는 호스트 수정 페이지를 사용하여 SQL Server용 SnapCenter 플러그인을 다른 호스트에 푸시합니다. 보다 "[호스트 관리](#)" 자세한 내용은.

단계

1. 호스트 페이지에서 호스트를 선택하여 SQL Server용 SnapCenter 플러그인을 수정하고 설치합니다.

2. (선택 사항) 재해 복구(DR) 백업에서 SQL Server 구성 파일용 SnapCenter 플러그인을 새 컴퓨터로 교체합니다.
3. DR 백업의 SQL Server 폴더용 SnapCenter 플러그인에서 Windows 및 SQL 일정을 가져옵니다.

관련 정보

를 참조하십시오 ["재해 복구 API"](#) 동영상.

SQL Server용 SnapCenter 플러그인을 위한 스토리지 재해 복구(DR)

글로벌 설정 페이지에서 저장소에 대한 DR 모드를 활성화하여 SQL Server 저장소용 SnapCenter 플러그인을 복구할 수 있습니다.

시작하기 전에

- 플러그인이 유지 관리 모드인지 확인하세요.
- SnapMirror/ SnapVault 관계를 끊습니다. ["SnapMirror 관계 끊기"](#)
- 보조 머신의 LUN을 동일한 드라이브 문자로 호스트 머신에 연결합니다.
- 모든 디스크가 DR 이전에 사용된 것과 동일한 드라이브 문자를 사용하여 연결되었는지 확인하세요.
- MSSQL 서버 서비스를 다시 시작합니다.
- SQL 리소스가 다시 온라인 상태인지 확인하세요.

이 작업에 관하여

VMDK 및 RDM 구성에서는 재해 복구(DR)가 지원되지 않습니다.

단계

1. 설정 페이지에서 설정 > 전역 설정 > *재해 복구*로 이동합니다.
2. *재해 복구 활성화*를 선택합니다.
3. *적용*을 클릭하세요.
4. 모니터 > *작업*을 클릭하여 DR 작업이 활성화되어 있는지 확인하세요.

당신이 완료한 후

- 장애 조치 후 새 데이터베이스가 생성되면 해당 데이터베이스는 DR 모드가 아닙니다.
새로운 데이터베이스는 장애 조치 이전과 마찬가지로 계속 작동합니다.
- DR 모드에서 생성된 새 백업은 토폴로지 페이지의 SnapMirror 또는 SnapVault (보조)에 나열됩니다.
새 백업 옆에는 "i" 아이콘이 표시되어 해당 백업이 DR 모드 중에 생성되었음을 나타냅니다.
- UI나 다음 cmdlet을 사용하여 장애 조치 중에 생성된 SQL Server 백업용 SnapCenter 플러그인을 삭제할 수 있습니다. `Remove-SmBackup`
- 장애 조치 후 일부 리소스를 DR 모드가 아닌 모드로 전환하려면 다음 cmdlet을 사용하세요. `Remove-SmResourceDRMode`

자세한 내용은 다음을 참조하세요. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

- SnapCenter Server는 DR 모드 또는 비 DR 모드에 있는 개별 스토리지 리소스(SQL 데이터베이스)를 관리하지만,

DR 모드 또는 비 DR 모드에 있는 스토리지 리소스가 있는 리소스 그룹은 관리하지 않습니다.

SQL Server 보조 스토리지용 **SnapCenter** 플러그인에서 기본 스토리지로의 장애 복구

SQL Server 기본 저장소용 SnapCenter 플러그인이 다시 온라인 상태가 되면 기본 저장소로 장애 복구해야 합니다.

시작하기 전에

- 관리 호스트 페이지에서 SQL Server용 SnapCenter 플러그인을 유지 관리 모드로 전환합니다.
- 호스트에서 보조 저장소의 연결을 끊고 기본 저장소에서 연결합니다.
- 기본 저장소로 장애 복구하려면 역방향 재동기화 작업을 수행하여 관계 방향이 장애 조치 전과 동일하게 유지되도록 합니다.

역방향 재동기화 작업 후에 기본 및 보조 저장소의 역할을 유지하려면 역방향 재동기화 작업을 다시 한 번 수행합니다.

자세한 내용은 다음을 참조하세요. "[역방향 재동기화 미리 관계](#)"

- MSSQL 서버 서비스를 다시 시작합니다.
- SQL 리소스가 다시 온라인 상태인지 확인하세요.



플러그인의 장애 조치(failover) 또는 장애 복구(failback) 중에 플러그인의 전체 상태가 즉시 새로 고쳐지지 않습니다. 호스트와 플러그인의 전반적인 상태는 후속 호스트 새로 고침 작업 중에 업데이트됩니다.

단계

1. 설정 페이지에서 설정 > 전역 설정 > *재해 복구*로 이동합니다.
2. *재해 복구 활성화*를 선택 해제합니다.
3. *적용*을 클릭하세요.
4. 모니터 > *작업*을 클릭하여 DR 작업이 활성화되어 있는지 확인하세요.

당신이 완료한 후

UI나 다음 cmdlet을 사용하여 장애 조치 중에 생성된 SQL Server 백업용 SnapCenter 플러그인을 삭제할 수 있습니다.

`Remove-SmDRFailoverBackups`

SnapCenter Plug-in for VMware vSphere 설치

데이터베이스나 파일 시스템이 가상 머신(VM)에 저장되어 있거나 VM과 데이터 저장소를 보호하려는 경우 SnapCenter Plug-in for VMware vSphere 배포해야 합니다.

배포에 대한 정보는 다음을 참조하세요. "[배포 개요](#)".

CA 인증서 배포

SnapCenter Plug-in for VMware vSphere 사용하여 CA 인증서를 구성하려면 다음을 참조하세요. "[SSL 인증서 생성 또는 가져오기](#)".

CRL 파일 구성

SnapCenter Plug-in for VMware vSphere 미리 구성된 디렉토리에서 CRL 파일을 찾습니다. SnapCenter Plug-in for VMware vSphere 의 CRL 파일의 기본 디렉토리는 `_/opt/netapp/config/crl_`입니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

데이터 보호를 준비하세요

Microsoft SQL Server용 SnapCenter 플러그인을 사용하기 위한 전제 조건

SQL Server용 플러그인을 사용하기 전에 SnapCenter 관리자는 SnapCenter Server를 설치 및 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다.
- SnapCenter 에 로그인하세요.
- 스토리지 시스템 연결을 추가하거나 할당하고 자격 증명을 생성하여 SnapCenter 환경을 구성합니다.



SnapCenter 서로 다른 클러스터에서 동일한 이름을 가진 여러 SVM을 지원하지 않습니다. SnapCenter 가 지원하는 각 SVM에는 고유한 이름이 있어야 합니다.

- 호스트를 추가하고, 플러그인을 설치하고, 리소스를 검색(새로 고침)하고, 플러그인을 구성합니다.
- Invoke-SmConfigureResources를 실행하여 기존 Microsoft SQL Server 데이터베이스를 로컬 디스크에서 NetApp LUN으로 이동하거나 그 반대로 이동합니다.

cmdlet을 실행하기 위한 정보는 다음을 참조하세요. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)"

- VMware RDM LUN이나 VMDK에 있는 SQL 데이터베이스를 보호하기 위해 SnapCenter Server를 사용하는 경우 SnapCenter Plug-in for VMware vSphere 배포하고 SnapCenter 에 플러그인을 등록해야 합니다. SnapCenter Plug-in for VMware vSphere 대한 자세한 내용은 설명서를 참조하세요.

"[SnapCenter Plug-in for VMware vSphere 설명서](#)"

- Microsoft Windows용 SnapCenter 플러그인을 사용하여 호스트 측 스토리지 프로비저닝을 수행합니다.
- 백업 복제가 필요한 경우 SnapMirror 와 SnapVault 관계를 설정합니다.

자세한 내용은 SnapCenter 설치 정보를 참조하세요.

SnapCenter 4.1.1 사용자의 경우 SnapCenter Plug-in for VMware vSphere 설명서에는 가상화된 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 있습니다. SnapCenter 4.2.x 사용자, NetApp Data Broker 1.0 및 1.0.1의 경우, Linux 기반 NetApp Data Broker 가상 어플라이언스(Open Virtual Appliance 형식)에서 제공하는 SnapCenter Plug-in for VMware vSphere 사용하여 가상화된 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 설명서에 나와 있습니다. SnapCenter 4.3.x 사용자의 경우, SnapCenter Plug-in for VMware vSphere 설명서에는 Linux 기반 SnapCenter Plug-in for VMware vSphere (Open Virtual Appliance 형식)을 사용하여 가상화된 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 있습니다.

"[SnapCenter Plug-in for VMware vSphere 설명서](#)"

SQL Server를 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식

SnapCenter 사용하기 전에 수행하려는 백업, 복제 및 복원 작업과 관련된 기본 개념을 이해하는 것이 좋습니다. 다양한 작업을 위해 리소스, 리소스 그룹 및 정책과 상호 작용합니다.

- 리소스는 일반적으로 SnapCenter 사용하여 백업하거나 복제하는 데이터베이스, 데이터베이스 인스턴스 또는 Microsoft SQL Server 가용성 그룹입니다.
- SnapCenter 리소스 그룹은 호스트 또는 클러스터의 리소스 모음입니다.

리소스 그룹에서 작업을 수행하면 리소스 그룹에 대해 지정한 일정에 따라 리소스 그룹에 정의된 리소스에서 해당 작업이 수행됩니다.

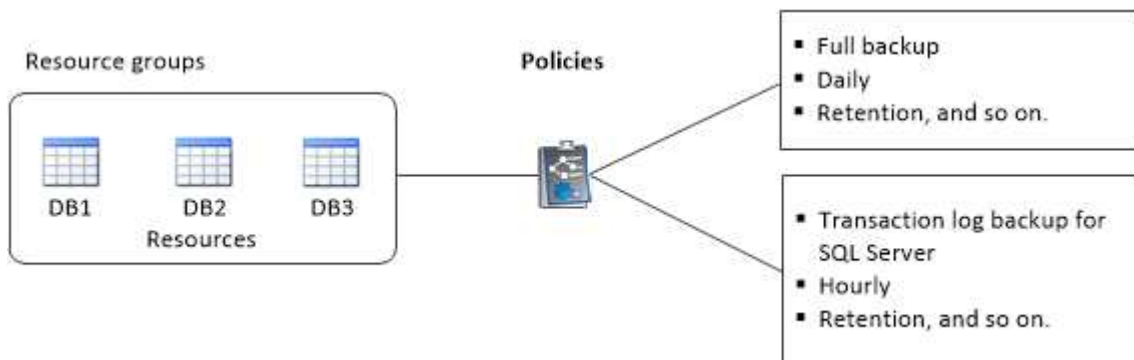
필요에 따라 단일 리소스나 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 수행할 수도 있습니다.

- 정책은 백업 빈도, 사본 보존, 복제, 스크립트 및 데이터 보호 작업의 기타 특성을 지정합니다.

리소스 그룹을 만들 때 해당 그룹에 대한 하나 이상의 정책을 선택합니다. 단일 리소스에 대해 주문형 백업을 수행할 때 정책을 선택할 수도 있습니다.

리소스 그룹은 보호하려는 내용과 보호하려는 날짜와 시간을 정의하는 것으로 생각하면 됩니다. 정책이란 그것을 어떻게 보호할 것인지를 정의하는 것이라고 생각하세요. 예를 들어, 호스트의 모든 데이터베이스나 모든 파일 시스템을 백업하는 경우 호스트의 모든 데이터베이스나 모든 파일 시스템을 포함하는 리소스 그룹을 만들 수 있습니다. 그런 다음 리소스 그룹에 일일 정책과 시간별 정책이라는 두 가지 정책을 첨부할 수 있습니다. 리소스 그룹을 만들고 정책을 첨부할 때 리소스 그룹을 구성하여 매일 전체 백업을 수행하고 매시간 로그 백업을 수행하는 일정을 설정할 수 있습니다.

다음 이미지는 데이터베이스의 리소스, 리소스 그룹 및 정책 간의 관계를 보여줍니다.



SQL Server 데이터베이스, 인스턴스 또는 가용성 그룹 백업

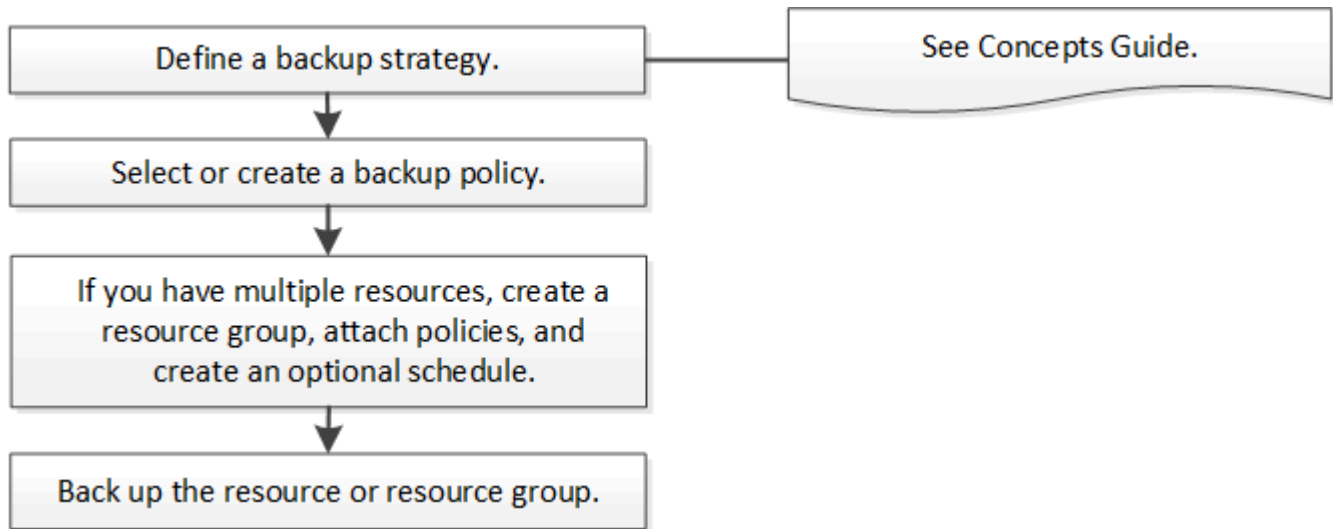
백업 워크플로

사용자 환경에 Microsoft SQL Server용 SnapCenter 플러그인을 설치하면 SnapCenter 사용하여 SQL Server 리소스를 백업할 수 있습니다.

여러 서버에서 동시에 실행되도록 여러 백업을 예약할 수 있습니다.

동일한 리소스에서 백업 및 복원 작업을 동시에 수행할 수 없습니다.

다음 워크플로는 백업 작업을 수행해야 하는 순서를 보여줍니다.



리소스 페이지에서 지금 백업, 복원, 백업 관리 및 복제 옵션은 NetApp LUN이 아닌 LUN, 손상된 데이터베이스 또는 복원 중인 데이터베이스를 선택하는 경우 비활성화됩니다.

PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원, 복구, 확인 및 복제 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 다음을 참조하세요. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#)

SnapCenter 데이터베이스를 백업하는 방법

SnapCenter 스냅샷 기술을 사용하여 LUN이나 VMDK에 있는 SQL Server 데이터베이스를 백업합니다. SnapCenter 데이터베이스의 스냅샷을 만들어 백업을 생성합니다.

리소스 페이지에서 전체 데이터베이스 백업을 위한 데이터베이스를 선택하면 SnapCenter 동일한 스토리지 볼륨에 있는 다른 모든 데이터베이스를 자동으로 선택합니다. LUN이나 VMDK가 단일 데이터베이스만 저장하는 경우 데이터베이스를 개별적으로 지우거나 다시 선택할 수 있습니다. LUN이나 VMDK에 여러 데이터베이스가 있는 경우 해당 데이터베이스를 그룹으로 지우거나 다시 선택해야 합니다.

단일 볼륨에 있는 모든 데이터베이스는 스냅샷을 사용하여 동시에 백업됩니다. 동시 백업 데이터베이스의 최대 수가 35이고, 스토리지 볼륨에 35개가 넘는 데이터베이스가 있는 경우 생성되는 스냅샷의 총 수는 데이터베이스 수를 35로 나눈 값과 같습니다.



백업 정책에서 각 스냅샷에 대한 최대 데이터베이스 수를 구성할 수 있습니다.

SnapCenter 스냅샷을 생성하면 전체 스토리지 시스템 볼륨이 스냅샷에 캡처됩니다. 하지만 백업은 백업이 생성된 SQL 호스트 서버에만 유효합니다.

다른 SQL 호스트 서버의 데이터가 동일한 볼륨에 있는 경우, 이 데이터는 스냅샷에서 복원할 수 없습니다.

더 많은 정보를 찾아보세요

["정지 또는 리소스 그룹화 작업이 실패합니다."](#)

백업에 사용할 수 있는 리소스가 있는지 확인하세요

리소스는 설치한 플러그인에 의해 유지 관리되는 데이터베이스, 애플리케이션 인스턴스, 가용성 그룹 및 유사한 구성 요소입니다. 데이터 보호 작업을 수행할 수 있도록 해당 리소스를 리소스 그룹에 추가할 수 있지만, 먼저 사용 가능한 리소스를 파악해야 합니다. 사용 가능한 리소스를 확인하면 플러그인 설치가 성공적으로 완료되었는지도 확인할 수 있습니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 생성, 자격 증명 추가 등의 작업을 이미 완료했어야 합니다.
- Microsoft SQL 데이터베이스를 검색하려면 다음 조건 중 하나를 충족해야 합니다.
 - SnapCenter Server에 플러그인 호스트를 추가하는 데 사용된 사용자는 Microsoft SQL Server에 대한 필수 권한(sysadmin)을 가져야 합니다.
 - 위의 조건이 충족되지 않으면 SnapCenter 서버에서 Microsoft SQL Server에 대한 필요한 권한(sysadmin)이 있는 사용자를 구성해야 합니다. 사용자는 Microsoft SQL Server 인스턴스 수준에서 구성되어야 하며, 사용자는 SQL 또는 Windows 사용자일 수 있습니다.
- Windows 클러스터에서 Microsoft SQL 데이터베이스를 검색하려면 FCI(Failover Cluster Instance) TCP/IP 포트를 차단 해제해야 합니다.
- 데이터베이스가 VMware RDM LUN 또는 VMDK에 있는 경우 SnapCenter Plug-in for VMware vSphere 배포하고 SnapCenter 에 플러그인을 등록해야 합니다.

자세한 내용은 다음을 참조하세요. "[SnapCenter Plug-in for VMware vSphere 배포](#)"

- 호스트가 gMSA로 추가되고 gMSA에 로그인 및 시스템 관리자 권한이 있는 경우, gMSA는 SQL 인스턴스에 연결하는 데 사용됩니다.

이 작업에 관하여

세부 정보 페이지의 전체 상태 옵션이 백업할 수 없음으로 설정된 경우 데이터베이스를 백업할 수 없습니다. 다음 중 하나라도 해당되면 전체 상태 옵션이 백업할 수 없음으로 설정됩니다.

- 데이터베이스가 NetApp LUN에 없습니다.
- 데이터베이스가 정상 상태가 아닙니다.

데이터베이스가 오프라인, 복구 중, 복구 보류, 의심 등의 상태에 있는 경우 데이터베이스는 정상 상태가 아닙니다.

- 데이터베이스에 권한이 부족합니다.

예를 들어, 사용자가 데이터베이스에 대한 보기 권한만 가지고 있는 경우, 데이터베이스의 파일과 속성을 식별할 수 없으므로 백업할 수 없습니다.



SQL Server Standard Edition에 가용성 그룹 구성이 있는 경우 SnapCenter 기본 데이터베이스만 백업할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 드롭다운 목록에서 데이터베이스, 인스턴스 또는 *가용성 그룹*을 선택합니다.

딸깍 하는 소리  호스트 이름과 SQL Server 인스턴스를 선택하여 리소스를 필터링합니다. 그런 다음 클릭할 수 있습니다.  필터 창을 닫으려면.

3. *리소스 새로고침*을 클릭하세요.

새로 추가되거나 이름이 변경되거나 삭제된 리소스는 SnapCenter 서버 인벤토리에 업데이트됩니다.



SnapCenter 외부에서 데이터베이스 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

리소스는 리소스 유형, 호스트 또는 클러스터 이름, 연관된 리소스 그룹, 백업 유형, 정책 및 전반적인 상태와 같은 정보와 함께 표시됩니다.

- 데이터베이스가 NetApp 스토리지가 아닌 곳에 있는 경우 Not available for backup 전체 상태 열에 표시됩니다.

NetApp 스토리지가 아닌 다른 스토리지에 있는 데이터베이스에서는 데이터 보호 작업을 수행할 수 없습니다.

- 데이터베이스가 NetApp 스토리지에 있고 보호되지 않은 경우 Not protected 전체 상태 열에 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되는 경우 사용자 인터페이스에 다음이 표시됩니다. Backup not run 전체 상태 열에 메시지가 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되어 있으며 데이터베이스에 대한 백업이 트리거되는 경우 사용자 인터페이스에 다음이 표시됩니다. Backup succeeded 전체 상태 열에 메시지가 표시됩니다.



자격 증명을 설정하는 동안 SQL 인증을 활성화한 경우, 검색된 인스턴스나 데이터베이스에 빨간색 자물쇠 아이콘이 표시됩니다. 자물쇠 아이콘이 나타나면 리소스 그룹에 인스턴스나 데이터베이스를 성공적으로 추가하려면 인스턴스 또는 데이터베이스 자격 증명을 지정해야 합니다.

1. SnapCenter 관리자가 RBAC 사용자에게 리소스를 할당한 후, RBAC 사용자는 로그인하여 *리소스 새로 고침*을 클릭하여 리소스의 최신 *전체 상태*를 확인해야 합니다.

NetApp 스토리지 시스템으로 리소스 마이그레이션

Microsoft Windows용 SnapCenter 플러그인을 사용하여 NetApp 스토리지 시스템을 프로비저닝한 후에는 SnapCenter 그래픽 사용자 인터페이스(GUI)나 PowerShell cmdlet을 사용하여 리소스를 NetApp 스토리지 시스템으로 마이그레이션하거나 한 NetApp LUN에서 다른 NetApp LUN으로 마이그레이션할 수 있습니다.

시작하기 전에

- SnapCenter 서버에 스토리지 시스템을 추가했어야 합니다.
- SQL Server 리소스를 새로 고침(검색)했어야 합니다.

이 마법사 페이지의 대부분 필드는 설명이 필요 없습니다. 다음 정보는 귀하에게 지침이 필요할 수 있는 몇몇 분야에 대해 설명합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 데이터베이스 또는 *인스턴스*를 선택합니다.

3. 목록에서 데이터베이스나 인스턴스를 선택하고 *마이그레이션*을 클릭합니다.

4. 리소스 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
데이터베이스 이름 (선택 사항)	마이그레이션할 인스턴스를 선택한 경우, 데이터베이스 드롭다운 목록에서 해당 인스턴스의 데이터베이스를 선택해야 합니다.
목적지 선택	데이터 및 로그 파일의 대상 위치를 선택합니다. 데이터 및 로그 파일은 각각 선택된 NetApp 드라이브 아래의 Data 및 Log 폴더로 이동됩니다. 폴더 구조에 폴더가 하나도 없으면 폴더가 생성되고 리소스가 마이그레이션됩니다.
데이터베이스 파일 세부 정보 표시 (선택 사항)	단일 데이터베이스의 여러 파일을 마이그레이션하려면 이 옵션을 선택하세요.  인스턴스 리소스를 선택하면 이 옵션이 표시되지 않습니다.
옵션	원본에서 데이터베이스 복사본을 삭제하려면 *원래 위치에서 마이그레이션된 데이터베이스 복사본 삭제*를 선택합니다. 선택 사항: 데이터베이스를 분리하기 전에 테이블에서 UPDATE STATISTICS 를 실행합니다.

5. 확인 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
데이터베이스 일관성 검사 옵션	마이그레이션 전에 데이터베이스의 무결성을 확인하려면 *실행 전*을 선택하세요. 마이그레이션 후 데이터베이스의 무결성을 확인하려면 *실행 후*를 선택하세요.

이 분야에서는...	이렇게 하세요...
DBCC CHECKDB 옵션	• PHYSICAL_ONLY 옵션을 선택하면 무결성 검사를 데이터베이스의 물리적 구조로 제한하고 찢어진 페이지, 체크섬 오류, 데이터베이스에 영향을 미치는 일반적인 하드웨어 오류를 감지합니다. • 모든 정보 메시지를 표시하지 않으려면 NO_INFOMSGS 옵션을 선택하세요. • ALL_ERRORMSG 옵션을 선택하면 개체별로 보고된 모든 오류가 표시됩니다. • 비클러스터형 인덱스를 확인하지 않으려면 NOINDEX 옵션을 선택하세요. SQL Server 데이터베이스는 Microsoft SQL Server 데이터베이스 일관성 검사기(DBCC)를 사용하여 데이터베이스에 있는 개체의 논리적 및 물리적 무결성을 검사합니다.  실행 시간을 줄이려면 이 옵션을 선택하는 것이 좋습니다. • 내부 데이터베이스 스냅샷을 사용하는 대신, 검사를 제한하고 잠금을 얻으려면 TABLOCK 옵션을 선택하세요.

6. 요약을 검토한 후 마침을 클릭합니다.

SQL Server 데이터베이스에 대한 백업 정책 만들기

SnapCenter 사용하여 SQL Server 리소스를 백업하기 전에 리소스 또는 리소스 그룹에 대한 백업 정책을 만들거나, 리소스 그룹을 만들거나 단일 리소스를 백업할 때 백업 정책을 만들 수 있습니다.

시작하기 전에

- 데이터 보호 전략을 정의해야 합니다.
- SnapCenter 설치, 호스트 추가, 리소스 식별, 스토리지 시스템 연결 생성 등의 작업을 완료하여 데이터 보호를 준비했어야 합니다.
- 로그 백업을 위해 호스트 로그 디렉토리를 구성해야 합니다.
- SQL Server 리소스를 새로 고침(검색)했어야 합니다.
- 스냅샷을 미리 또는 볼트에 복제하는 경우 SnapCenter 관리자가 소스 볼륨과 대상 볼륨 모두에 대한 스토리지 가상 머신(SVM)을 할당해야 합니다.

관리자가 사용자에게 리소스를 할당하는 방법에 대한 자세한 내용은 SnapCenter 설치 정보를 참조하세요.

- PowerShell 스크립트를 prescripts 및 postscripts로 실행하려면 web.config 파일에서 usePowershellProcessforScripts 매개변수 값을 true로 설정해야 합니다.

기본값은 false입니다.

- SnapMirror Active Sync의 특정 전제 조건과 제한 사항을 검토하세요. 자세한 내용은 다음을 참조하세요.
["SnapMirror Active Sync에 대한 개체 제한"](#).

이 작업에 관하여

- 백업 정책은 백업을 관리하고 보관하는 방법과 리소스 또는 리소스 그룹을 백업하는 빈도를 제어하는 일련의 규칙입니다. 또한 복제 및 스크립트 설정을 지정할 수 있습니다. 정책에서 옵션을 지정하면 다른 리소스 그룹에 정책을 재사용할 때 시간을 절약할 수 있습니다.

SCRIPTS_PATH는 플러그인 호스트의 SMCoreServiceHost.exe.Config 파일에 있는 PredefinedWindowsScriptsDirectory 키를 사용하여 정의됩니다.

필요한 경우 이 경로를 변경하고 SMcore 서비스를 다시 시작할 수 있습니다. 보안을 위해 기본 경로를 사용하는 것이 좋습니다.

키 값은 API를 통해 swagger에서 표시될 수 있습니다: API /4.7/configsettings

GET API를 사용하여 키 값을 표시할 수 있습니다. SET API는 지원되지 않습니다.

- SnapLock

- '특정 기간 동안 백업 사본을 보관합니다' 옵션을 선택한 경우 SnapLock 보관 기간은 언급된 보관 기간보다 짧거나 같아야 합니다.

스냅샷 잠금 기간을 지정하면 보존 기간이 만료될 때까지 스냅샷이 삭제되지 않습니다. 이를 통해 정책에 지정된 수보다 더 많은 수의 스냅샷을 보존할 수 있습니다.

ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

1단계: 정책 이름 만들기

1. 왼쪽 탐색 창에서 *설정*을 선택합니다.
2. 설정 페이지에서 *정책*을 선택합니다.
3. *새로 만들기*를 선택하세요.
4. 이름 페이지에서 정책 이름과 세부 정보를 입력합니다.

2단계: 정책 옵션 구성

1. 정책 유형 페이지에서 다음 단계를 수행합니다.
 - a. 저장 유형을 선택하세요.
 - b. 보험 범위를 선택하세요.

전체 백업 및 로그 백업

데이터베이스 파일과 트랜잭션 로그를 백업하고 트랜잭션 로그를 잘라냅니다.

- i. *전체 백업 및 로그 백업*을 선택하세요.
- ii. 각 스냅샷에 대해 백업해야 하는 데이터베이스의 최대 개수를 입력하세요.



여러 백업 작업을 동시에 실행하려면 이 값을 늘려야 합니다.

전체 백업

데이터베이스 파일을 백업하세요.

- i. *전체 백업*을 선택하세요.
- ii. 각 스냅샷에 대해 백업해야 하는 데이터베이스의 최대 개수를 입력하세요. 기본값은 100입니다



여러 백업 작업을 동시에 실행하려면 이 값을 늘려야 합니다.

로그 백업

- i. 거래 로그를 백업하세요.
- ii. *로그 백업*을 선택하세요.

복사 전용 백업

- i. 다른 백업 애플리케이션을 사용하여 리소스를 백업하는 경우 *백업만 복사*를 선택하세요.

트랜잭션 로그를 그대로 유지하면 모든 백업 애플리케이션이 데이터베이스를 복원할 수 있습니다. 일반적으로 다른 상황에서는 복사 전용 옵션을 사용해서는 안 됩니다.



Microsoft SQL에서는 보조 저장소에 대한 전체 백업 및 로그 백업 옵션과 함께 복사 전용 백업 옵션을 지원하지 않습니다.

3단계: 가용성 그룹 설정 구성

1. 가용성 그룹 설정 섹션에서 다음 작업을 수행합니다.

- a. 선호하는 백업 복제본에만 백업합니다.

선호하는 백업 복제본에만 백업하려면 이 옵션을 선택하세요. 선호하는 백업 복제본은 SQL Server에서 AG에 대해 구성된 백업 기본 설정에 따라 결정됩니다.

- b. 백업할 복제본을 선택하세요.

백업을 위해 기본 AG 복제본이나 보조 AG 복제본을 선택합니다.

- c. 백업 우선순위 선택(최소 및 최대 백업 우선순위)

백업할 AG 복제본을 결정하는 최소 백업 우선 순위 번호와 최대 백업 우선 순위 번호를 지정합니다. 예를 들어,

최소 우선순위를 10으로, 최대 우선순위를 50으로 지정할 수 있습니다. 이 경우, 우선순위가 10보다 크고 50보다 작은 모든 AG 복제본이 백업 대상으로 고려됩니다.

기본적으로 최소 우선순위는 1이고 최대 우선순위는 100입니다.



클러스터 구성에서 백업은 정책에 설정된 보존 설정에 따라 클러스터의 각 노드에 보존됩니다. AG의 소유자 노드가 변경되면 보존 설정에 따라 백업이 수행되고 이전 소유자 노드의 백업이 보존됩니다. AG에 대한 보존은 노드 수준에서만 적용됩니다.

4단계: 스냅샷 및 복제 설정 구성

1. 스냅샷 및 복제 페이지에서 다음 단계를 수행합니다.

a. 주문형, 시간별, 일별, 주별 또는 *월별*을 선택하여 일정 유형을 지정합니다.

정책에 대해 하나의 일정 유형만 선택할 수 있습니다.



리소스 그룹을 생성하는 동안 백업 작업에 대한 일정(시작 날짜, 종료 날짜, 빈도)을 지정할 수 있습니다. 이를 통해 동일한 정책과 백업 빈도를 공유하는 리소스 그룹을 만들 수 있지만, 각 정책에 다른 백업 일정을 할당할 수 있습니다.



오전 2시로 예약한 경우, 일광 절약 시간제(DST) 기간에는 일정이 실행되지 않습니다.

5단계: 최신 보존 설정 구성

1. 최신 보존 설정 섹션에서 백업 유형 페이지에서 선택한 백업 유형에 따라 다음 작업 중 하나 이상을 수행합니다.

특정 사본 수

특정 수의 스냅샷만 보관합니다.

1. 지난 <숫자>일 동안 로그 백업을 적용합니다 옵션을 선택하고 보관할 일수를 지정합니다. 이 한도에 가까워지면 이전 사본을 삭제하는 것이 좋습니다.

특정 일수

백업 사본을 특정 일수 동안 보관합니다.

1. 전체 백업의 마지막 <숫자>일에 적용되는 로그 백업 유지 옵션을 선택하고 로그 백업 사본을 보관할 일 수를 지정합니다.

6단계: 스냅샷 설정 구성

1. 전체 백업 보존 설정의 경우 다음 작업을 수행합니다.

a. 보관할 스냅샷의 총 수를 지정하세요

i. 보관할 스냅샷 수를 지정하려면 *보관할 사본*을 선택하세요.

ii. 스냅샷 수가 지정된 수를 초과하면 스냅샷이 삭제되고 가장 오래된 사본이 먼저 삭제됩니다.



기본적으로 보존 횟수 값은 2로 설정됩니다. 보존 횟수를 1로 설정하면 새 스냅샷이 대상에 복제될 때까지 첫 번째 스냅샷이 SnapVault 관계에 대한 참조 스냅샷이기 때문에 보존 작업이 실패할 수 있습니다.



최대 보존 값은 1018입니다. 보존 기간이 기본 NetApp ONTAP 버전에서 지원하는 것보다 높은 값으로 설정된 경우 백업이 실패합니다.

2. 스냅샷을 보관하는 기간

a. 스냅샷을 삭제하기 전에 보관할 일수를 지정하려면 *사본 보관 기간*을 선택하세요.

3. *스냅샷 복사 잠금 기간*을 선택하고 기간을 일, 월 또는 년 단위로 지정합니다.

스냅샷 보관 기간은 100년 미만이어야 합니다.

4. 정책 라벨을 선택하세요.



원격 복제를 위해 기본 스냅샷에 SnapMirror 레이블을 할당하면 기본 스냅샷이 SnapCenter 에서 ONTAP 보조 시스템으로 스냅샷 복제 작업을 오프로드할 수 있습니다. 정책 페이지에서 SnapMirror 또는 SnapVault 옵션을 활성화하지 않고도 이 작업을 수행할 수 있습니다.

7단계: 보조 복제 옵션 구성

1. 보조 복제 옵션 선택 섹션에서 다음 보조 복제 옵션 중 하나 또는 둘 다를 선택합니다.

SnapMirror 업데이트

로컬 스냅샷 복사본을 만든 후 SnapMirror 업데이트합니다.

1. 다른 볼륨에 백업 세트의 미러 복사본을 생성하려면 이 옵션을 선택하세요(SnapMirror).

SnapMirror Active Sync의 경우 이 옵션을 활성화해야 합니다.

2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고침됩니다.

보다 "[토폴로지 페이지에서 SQL Server 백업 및 복제본 보기](#)".

SnapVault 업데이트

스냅샷 사본을 만든 후 SnapVault 업데이트합니다.

1. 디스크 간 백업 복제를 수행하려면 이 옵션을 선택하세요.

2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고침됩니다.

ONTAP 에서 SnapLock Vault로 알려진 보조 노드에만 SnapLock 구성된 경우 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 보조 노드의 잠금 기간이 새로 고침됩니다.

SnapLock Vault에 대한 자세한 내용은 다음을 참조하세요. "[볼트 대상의 WORM에 스냅샷 복사본 커밋](#)"

보다 "[토폴로지 페이지에서 SQL Server 백업 및 복제본 보기](#)".

오류 재시도 횟수

1. 프로세스가 중단되기 전에 발생해야 하는 복제 시도 횟수를 입력합니다.

8단계: 스크립트 설정 구성

1. 스크립트 페이지에서 백업 작업 전이나 후에 실행해야 하는 프리스크립트나 포스트스크립트의 경로와 인수를 각각 입력합니다.

예를 들어, SNMP 트랩을 업데이트하고, 알림을 자동화하고, 로그를 보내는 스크립트를 실행할 수 있습니다.



prescripts 또는 postscripts 경로에는 드라이브나 공유가 포함되어서는 안 됩니다. 경로는 SCRIPTS_PATH를 기준으로 해야 합니다.



ONTAP 에서 SnapMirror 보존 정책을 구성하여 보조 저장소가 스냅샷의 최대 한도에 도달하지 않도록 해야 합니다.

9단계: 확인 설정 구성

확인 페이지에서 다음 단계를 수행하세요.

1. 다음 백업 일정에 대한 검증 실행 섹션에서 일정 빈도를 선택합니다.
2. 데이터베이스 일관성 검사 옵션 섹션에서 다음 작업을 수행합니다.
 - a. 무결성 구조를 데이터베이스의 물리적 구조로 제한합니다(PHYSICAL_ONLY)
 - i. 무결성 검사를 데이터베이스의 물리적 구조로 제한하고 찢어진 페이지, 체크섬 오류, 데이터베이스에 영향을 미치는 일반적인 하드웨어 오류를 감지하려면 *데이터베이스의 물리적 구조로 무결성 구조 제한(PHYSICAL_ONLY)*을 선택합니다.
 - b. 모든 정보 메시지 표시 안 함(NO INFO MSGS)
 - i. 모든 정보 메시지를 억제하려면 *모든 정보 메시지 억제(NO_INFO MSGS)*를 선택하세요. 기본적으로 선택됨.
 - c. 개체별로 보고된 모든 오류 메시지를 표시합니다(ALL_ERROR MSGS)
 - i. 보고된 모든 오류를 개체별로 표시하려면 *개체별로 보고된 모든 오류 메시지 표시(ALL_ERROR MSGS)*를 선택합니다.
 - d. 비클러스터형 인덱스(NOINDEX)를 검사하지 마십시오.
 - i. 비클러스터형 인덱스를 검사하지 않으려면 *비클러스터형 인덱스를 검사하지 않음(NOINDEX)*을 선택합니다. SQL Server 데이터베이스는 Microsoft SQL Server 데이터베이스 일관성 검사기(DBCC)를 사용하여 데이터베이스에 있는 개체의 논리적 및 물리적 무결성을 검사합니다.
 - e. 내부 데이터베이스 스냅샷(TABLOCK)을 사용하는 대신 검사를 제한하고 잠금을 획득합니다.
 - i. 내부 데이터베이스 스냅샷을 사용하는 대신 검사를 제한하고 잠금을 획득하려면 *검사를 제한하고 내부 데이터베이스 스냅샷 복사본을 사용하는 대신 잠금을 획득(TABLOCK)*을 선택합니다.
3. 로그 백업 섹션에서 *완료 시 로그 백업 확인*을 선택하여 완료 시 로그 백업을 확인합니다.
4. 확인 스크립트 설정 섹션에서는 각각 확인 작업 전이나 후에 실행해야 하는 프리스크립트나 포스트스크립트의 경로와 인수를 입력합니다.



prescripts 또는 postscripts 경로에는 드라이브나 공유가 포함되어서는 안 됩니다. 경로는 SCRIPTS_PATH를 기준으로 해야 합니다.

10단계: 요약 검토

1. 요약을 검토한 후 *마침*을 선택하세요.

SQL Server에 대한 리소스 그룹 생성 및 정책 연결

리소스 그룹은 함께 백업하고 보호하려는 리소스를 추가하는 컨테이너입니다. 리소스 그룹을 사용하면 주어진 애플리케이션과 관련된 모든 데이터를 동시에 백업할 수 있습니다. 모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한, 수행하려는 데이터 보호 작업 유형을 정의하려면 리소스 그룹에 하나 이상의 정책을 연결해야 합니다.

새로운 리소스 그룹을 만들지 않고도 리소스를 개별적으로 보호할 수 있습니다. 보호된 리소스에 대한 백업을 수행할 수 있습니다.

이 작업에 관하여

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

- SnapMirror 활성 동기화가 있는 리소스가 포함된 기존 리소스 그룹에 SnapMirror 활성 동기화 SnapMirror 없는 새 데이터베이스를 추가하는 것은 지원되지 않습니다.
- SnapMirror Active Sync의 장애 조치 모드에서 기존 리소스 그룹에 새 데이터베이스를 추가하는 것은 지원되지 않습니다. 일반 상태나 장애 복구 상태에서만 리소스 그룹에 리소스를 추가할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *데이터베이스*를 선택합니다.



최근에 SnapCenter 에 리소스를 추가한 경우, *리소스 새로 고침*을 클릭하여 새로 추가된 리소스를 확인하세요.

3. *새 리소스 그룹*을 클릭합니다.
4. 이름 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	리소스 그룹 이름을 입력하세요. 리소스 그룹 이름은 250자를 넘을 수 없습니다.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력하세요. 예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.
스냅샷 복사에 사용자 정의 이름 형식 사용	선택 사항: 사용자 지정 스냅샷 이름과 형식을 입력합니다. 예를 들어, customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

5. 리소스 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 호스트 이름, 리소스 유형 및 SQL Server 인스턴스를 선택하여 리소스 목록을 필터링합니다.



최근에 리소스를 추가한 경우 리소스 목록을 새로 고친 후에만 사용 가능한 리소스 목록에 표시됩니다.

- b. 사용 가능한 리소스 섹션에서 선택한 리소스 섹션으로 리소스를 이동하려면 다음 단계 중 하나를 수행합니다.
 - 동일한 볼륨에 있는 모든 리소스를 선택한 리소스 섹션으로 이동하려면 *동일한 저장소 볼륨에 있는 모든 리소스 자동 선택*을 선택합니다.
 - 사용 가능한 리소스 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 클릭하여 선택한 리소스 섹션으로 이동합니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다. *.

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

- b. 선택한 정책에 대한 일정 구성 섹션에서 *를 클릭합니다. * 일정을 구성하려는 정책에 대한 일정 구성 열에 있습니다.
- c. 정책_정책_이름_에 대한 일정 추가 대화 상자에서 시작 날짜, 만료 날짜, 빈도를 지정하여 일정을 구성한 다음 *확인*을 클릭합니다.

정책에 나열된 각 주파수에 대해 이 작업을 수행해야 합니다. 구성된 일정은 선택한 정책에 대한 일정 구성 섹션의 적용된 일정 열에 나열됩니다.

- d. Microsoft SQL Server 스케줄러를 선택합니다.

또한 스케줄링 정책과 연결할 스케줄러 인스턴스를 선택해야 합니다.

Microsoft SQL Server 스케줄러를 선택하지 않으면 기본값은 Microsoft Windows 스케줄러입니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다. Windows 스케줄러나 SQL Server 에이전트에서 생성된 백업 작업의 일정을 수정하거나 이름을 바꾸면 안 됩니다.

7. 확인 페이지에서 다음 단계를 수행하세요.

- a. 인증 서버 드롭다운 목록에서 인증 서버를 선택하세요.

이 목록에는 SnapCenter에 추가된 모든 SQL Server가 포함되어 있습니다. 여러 개의 검증 서버(로컬 호스트 또는 원격 호스트)를 선택할 수 있습니다.



검증 서버 버전은 기본 데이터베이스를 호스팅하는 SQL 서버의 버전 및 에디션과 일치해야 합니다.

- a. *로케이터 로드*를 클릭하여 SnapMirror 및 SnapVault 볼륨을 로드하여 보조 저장소에서 검증을 수행합니다.
- b. 확인 일정을 구성하려는 정책을 선택한 다음 *를 클릭합니다. *.
- c. 확인 일정 추가 policy_name 대화 상자에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	이렇게 하세요...
백업 후 검증 실행	*백업 후 검증 실행*을 선택하세요.
검증 일정을 예약하세요	*예약된 검증 실행*을 선택하세요.

- d. *확인*을 클릭합니다.

구성된 일정은 적용된 일정 열에 나열됩니다. *를 클릭하면 검토 후 편집할 수 있습니다.  * 또는 *를 클릭하여 삭제하세요 ✕ *.

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmSmtServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

9. 요약 검토 후 *마침*을 클릭하세요.

관련 정보

["SQL Server 데이터베이스에 대한 백업 정책 만들기"](#)

ASA r2 시스템에서 Microsoft SQL Server 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.

ASA r2 시스템에 있는 리소스를 추가하려면 리소스 그룹을 만들어야 합니다. 리소스 그룹을 생성하는 동안 보조 보호를 프로비저닝할 수도 있습니다.

시작하기 전에

- ONTAP 9.x 리소스와 ASA r2 리소스를 동일한 리소스 그룹에 추가하지 않도록 해야 합니다.
- ONTAP 9.x 리소스와 ASA r2 리소스가 모두 포함된 데이터베이스가 없는지 확인해야 합니다.

이 작업에 관하여

- 2차 보호는 로그인한 사용자에게 **SecondaryProtection** 기능이 활성화된 역할이 할당된 경우에만 사용할 수 있습니다.
- 2차 보호를 활성화한 경우 기본 및 2차 일관성 그룹을 생성하는 동안 리소스 그룹은 유지 관리 모드로 전환됩니다. 기본 및 보조 일관성 그룹이 생성된 후 리소스 그룹은 유지 관리 모드에서 해제됩니다.
- SnapCenter 클론 리소스에 대한 보조 보호를 지원하지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.
 - a. 이름 필드에 리소스 그룹의 이름을 입력합니다.



리소스 그룹 이름은 250자를 넘을 수 없습니다.

- b. 나중에 리소스 그룹을 검색하는 데 도움이 되도록 태그 필드에 하나 이상의 레이블을 입력하세요.

예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.

c. 이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다.
기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

d. 백업하지 않을 보관 로그 파일의 대상을 지정합니다.



필요한 경우 접두사를 포함하여 애플리케이션에 설정된 것과 정확히 동일한 목적지를 사용해야 합니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 데이터베이스 호스트 이름을 선택합니다.



리소스가 성공적으로 검색된 경우에만 해당 리소스가 사용 가능한 리소스 섹션에 나열됩니다.
최근에 리소스를 추가한 경우 리소스 목록을 새로 고침 후에만 사용 가능한 리소스 목록에 표시됩니다.

5. 사용 가능한 리소스 섹션에서 ASA r2 리소스를 선택하고 선택한 리소스 섹션으로 이동합니다.

6. 애플리케이션 설정 페이지에서 백업 옵션을 선택하세요.

7. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



또한 다음을 클릭하여 정책을 생성할 수도 있습니다.  .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.

c. 정책 _policy_name_에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 _policy_name_은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 선택한 정책에 대해 보조 보호가 활성화된 경우 보조 보호 페이지가 표시되며 다음 단계를 수행해야 합니다.

a. 복제 정책의 유형을 선택하세요.



동기 복제 정책은 지원되지 않습니다.

b. 사용할 일관성 그룹 접미사를 지정합니다.

c. 대상 클러스터 및 대상 SVM 드롭다운에서 사용하려는 피어링된 클러스터와 SVM을 선택합니다.



SnapCenter에서는 클러스터 및 SVM 피어링을 지원하지 않습니다. 클러스터 및 SVM 피어링을 수행하려면 System Manager 또는 ONTAP CLI를 사용해야 합니다.



리소스가 이미 SnapCenter 외부에서 보호되고 있는 경우 해당 리소스는 보조 보호 리소스 섹션에 표시됩니다.

1. 확인 페이지에서 다음 단계를 수행하세요.

- a. *로케이터 로드*를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 저장소에서 검증을 수행합니다.
- b. 딸깍 하는 소리  일정 구성 열에서 정책의 모든 일정 유형에 대한 확인 일정을 구성합니다.
- c. 확인 일정 추가 policy_name 대화 상자에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	이렇게 하세요...
백업 후 검증 실행	*백업 후 검증 실행*을 선택하세요.
검증 일정을 예약하세요	*예약된 확인 실행*을 선택한 다음 드롭다운 목록에서 일정 유형을 선택합니다.

- d. 보조 저장소 시스템에서 백업을 확인하려면 *보조 위치에서 확인*을 선택하세요.
- e. *확인*을 클릭합니다.

구성된 검증 일정은 적용된 일정 열에 나열됩니다.

2. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtplibServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

3. 요약 검토 후 *마침*을 클릭하세요.

SQL 리소스 백업 요구 사항

SQL 리소스를 백업하기 전에 몇 가지 요구 사항이 충족되는지 확인해야 합니다.

- NetApp 스토리지 시스템이 아닌 곳에서 NetApp 스토리지 시스템으로 리소스를 마이그레이션했어야 합니다.
- 백업 정책을 생성했어야 합니다.
- 보조 저장소에 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에 "snapmirror all" 권한이 포함되어야 합니다. 하지만 "vsadmin" 역할을 사용하는 경우 "snapmirror all" 권한은 필요하지 않습니다.
- SQL 인스턴스 자격 증명이 AD 사용자 또는 그룹에 할당되지 않으면 AD(Active Directory) 사용자가 시작한 백업 작업이 실패합니다. 설정 > 사용자 액세스 페이지에서 SQL 인스턴스 자격 증명을 AD 사용자 또는 그룹에 할당해야 합니다.
- 정책이 첨부된 리소스 그룹을 만들어야 합니다.

- 리소스 그룹에 서로 다른 호스트의 여러 데이터베이스가 있는 경우 네트워크 문제로 인해 일부 호스트의 백업 작업이 늦게 실행될 수 있습니다. Set-SmConfigSettings PS cmdlet을 사용하여 web.config에서 FMaxRetryForUninitializedHosts 값을 구성해야 합니다.

PowerShell cmdlet을 사용하여 스토리지 시스템 연결 및 자격 증명 만들기

PowerShell cmdlet을 사용하여 데이터 보호 작업을 수행하려면 먼저 SVM(스토리지 가상 머신) 연결과 자격 증명을 만들어야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 저장소 연결을 생성하려면 인프라 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

스토리지 시스템 연결을 추가하는 동안에는 호스트 플러그인 설치가 진행 중이어서는 안 됩니다. 호스트 캐시가 업데이트되지 않고 SnapCenter GUI에 데이터베이스 상태가 “백업에 사용할 수 없음” 또는 “NetApp 스토리지에 없음”으로 표시될 수 있기 때문입니다.

- 저장 시스템 이름은 고유해야 합니다.

SnapCenter 서로 다른 클러스터에 동일한 이름을 가진 여러 스토리지 시스템을 지원하지 않습니다. SnapCenter에서 지원하는 각 스토리지 시스템은 고유한 이름과 고유한 관리 LIF IP 주소를 가져야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 PowerShell Core 연결 세션을 시작합니다.

이 예제에서는 PowerShell 세션을 엽니다.

```
PS C:\> Open-SmConnection
```

2. Add-SmStorageConnection cmdlet을 사용하여 스토리지 시스템에 대한 새 연결을 만듭니다.

이 예제에서는 새로운 스토리지 시스템 연결을 만듭니다.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Add-SmCredential cmdlet을 사용하여 새 자격 증명을 만듭니다.

이 예제에서는 Windows 자격 증명을 사용하여 FinanceAdmin이라는 새 자격 증명을 만듭니다.

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

SQL 리소스 백업

리소스가 아직 어떤 리소스 그룹에도 속하지 않은 경우 리소스 페이지에서 리소스를 백업할 수 있습니다.

이 작업에 관하여

- 백업 작업을 최적화하려면 DNS 서버에서 Windows 클러스터 이름과 IP 주소에 대한 역방향 조회 레코드를 만들어야 합니다.
- Windows 자격 증명 인증의 경우 플러그인을 설치하기 전에 자격 증명을 설정해야 합니다.
- SQL Server 인스턴스 인증을 위해서는 플러그인을 설치한 후 자격 증명을 추가해야 합니다.
- gMSA 인증을 위해서는 SnapCenter 에 호스트를 등록하는 동안 호스트 추가 또는 호스트 수정 페이지에서 gMSA를 설정하여 gMSA를 활성화하고 사용해야 합니다.
- 호스트가 gMSA로 추가되고 gMSA에 로그인 및 시스템 관리자 권한이 있는 경우 gMSA는 SQL 인스턴스에 연결할 수 있습니다.
 - SnapCenter SQL 인스턴스에 대한 인증이 구성되어 있는지 확인합니다. 인증이 구성된 경우 이 자격 증명을 사용하여 SQL 인스턴스에 액세스합니다.
 - 인증이 구성되지 않은 경우 gMSA를 사용하여 SQL 플러그인이 현재 작동 중인지 확인하세요. 플러그인이 작동 중이면 SQL 인스턴스에 대한 연결을 설정하는 데 사용됩니다.
 - SQL 인스턴스에 대한 인증이 구성되지 않았고 플러그인이 작동하지 않는 경우 Windows 자격 증명 인증을 통해 SQL 인스턴스에 액세스합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 데이터베이스, 인스턴스 또는 *가용성 그룹*을 선택합니다.

- a. 백업할 데이터베이스, 인스턴스 또는 가용성 그룹을 선택합니다.

인스턴스를 백업할 때 마지막 백업 상태나 해당 인스턴스의 타임스탬프에 대한 정보는 리소스 페이지에서 사용할 수 없습니다.

토폴로지 보기에서는 백업 상태, 타임스탬프 또는 백업이 인스턴스에 대한 것인지 데이터베이스에 대한 것인지 구별할 수 없습니다.

3. 리소스 페이지에서 스냅샷 복사본에 대한 사용자 지정 이름 형식 확인란을 선택한 다음 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_policy_hostname 또는 resource_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

4. 정책 페이지에서 다음 작업을 수행합니다.

- a. 정책 섹션에서 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

*를 선택하여 정책을 생성할 수 있습니다.  * 정책 마법사를 시작합니다.

선택한 정책에 대한 일정 구성 섹션에는 선택한 정책이 나열됩니다.

- b. 선택하다 *  * 일정을 구성하려는 정책에 대한 일정 구성 옆에 있습니다.

- c. *정책 일정 추가*에서 policy_name 대화 상자에서 일정을 구성한 다음 *확인*을 선택합니다.

여기 policy_name 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 옆에 나열됩니다.

- a. **Microsoft SQL Server** 스케줄러 사용*을 선택한 다음, 스케줄링 정책과 연결된 *스케줄러 인스턴스* 드롭다운 목록에서 스케줄러 인스턴스를 선택합니다.

5. 확인 페이지에서 다음 단계를 수행하세요.

- a. 인증 서버 드롭다운 목록에서 인증 서버를 선택하세요.

여러 개의 검증 서버(로컬 호스트 또는 원격 호스트)를 선택할 수 있습니다.



검증 서버 버전은 기본 데이터베이스를 호스팅하는 SQL 서버 에디션 버전과 같거나 그 이상이어야 합니다.

- a. 보조 저장소 시스템의 백업을 확인하려면 *보조 저장소의 백업을 확인하기 위해 보조 로케이터 로드*를 선택하세요.

- b. 확인 일정을 구성하려는 정책을 선택한 다음 *를 선택합니다.  *.
- c. 확인 일정 추가 정책_이름 대화 상자에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	이렇게 하세요...
백업 후 검증 실행	*백업 후 검증 실행*을 선택하세요.
검증 일정을 예약하세요	*예약된 검증 실행*을 선택하세요.



검증 서버에 저장소 연결이 없으면 검증 작업이 실패하고 "디스크를 마운트하지 못했습니다" 오류가 발생합니다.

- d. *확인*을 선택하세요.

구성된 일정은 적용된 일정 옆에 나열됩니다.

6. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmSmtServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

7. 요약 검토 후 *마침*을 선택하세요.

데이터베이스 토폴로지 페이지가 표시됩니다.

8. *지금 백업*을 선택하세요.

9. 백업 페이지에서 다음 단계를 수행합니다.

- a. 리소스에 여러 정책을 적용한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. 백업을 확인하려면 *백업 후 확인*을 선택하세요.

- c. *백업*을 선택하세요.



Windows 스케줄러나 SQL Server 에이전트에서 생성된 백업 작업의 이름을 바꾸면 안 됩니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

암묵적 리소스 그룹이 생성됩니다. 사용자 액세스 페이지에서 해당 사용자 또는 그룹을 선택하면 이를 볼 수 있습니다. 암시적 리소스 그룹 유형은 "Resource"입니다.

10. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

당신이 완료한 후

- MetroCluster 구성에서 SnapCenter 장애 조치 후 보호 관계를 감지하지 못할 수 있습니다.

"MetroCluster 장애 조치 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다."

- VMDK에서 애플리케이션 데이터를 백업하고 SnapCenter Plug-in for VMware vSphere의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다. Java 힙 크기를 늘리려면 스크립트 파일 `/opt/netapp/init_scripts/scvservice`를 찾으세요. 해당 스크립트에서 `do_start` method 명령은 SnapCenter VMware 플러그인 서비스를 시작합니다. 해당 명령을 다음과 같이 업데이트하세요. `Java -jar -Xmx8192M -Xms4096M.`

관련 정보

"SQL Server 데이터베이스에 대한 백업 정책 만들기"

"TCP_TIMEOUT 지연으로 인해 MySQL 연결 오류로 인해 백업 작업이 실패합니다."

"Windows 스케줄러 오류로 인해 백업이 실패합니다."

"정지 또는 리소스 그룹화 작업이 실패합니다."

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.

2. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.

이 예제에서는 FullBackup의 SQL 백업 유형을 사용하여 새 백업 정책을 만듭니다.

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy  
-PluginPolicyType SCSQL -PolicyType Backup  
-SqlBackupType FullBackup -Verbose
```

이 예제에서는 CrashConsistent의 Windows 파일 시스템 백업 유형을 사용하여 새 백업 정책을 만듭니다.

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy  
-PluginPolicyType SCW -PolicyType Backup  
-ScwBackupType CrashConsistent -Verbose
```

3. Get-SmResources cmdlet을 사용하여 호스트 리소스를 검색합니다.

이 예제에서는 지정된 호스트에서 Microsoft SQL 플러그인에 대한 리소스를 검색합니다.

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com  
-PluginCode SCSQL
```

이 예제에서는 지정된 호스트에서 Windows 파일 시스템의 리소스를 검색합니다.

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com  
-PluginCode SCW
```

4. Add-SmResourceGroup cmdlet을 사용하여 SnapCenter 에 새 리소스 그룹을 추가합니다.

이 예제에서는 지정된 정책과 리소스를 사용하여 새로운 SQL 데이터베이스 백업 리소스 그룹을 만듭니다.

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource  
-Resources @{"Host"="visef6.org.com";  
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}  
-Policies "BackupPolicy"
```

이 예제에서는 지정된 정책과 리소스를 사용하여 새로운 Windows 파일 시스템 백업 리소스 그룹을 만듭니다.

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource  
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";  
"Type"="Windows Filesystem";"Names"="E:\"}  
-Policies "EngineeringBackupPolicy"
```

5. New-SmBackup cmdlet을 사용하여 새로운 백업 작업을 시작합니다.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy  
FinancePolicy
```

6. Get-SmBackupReport cmdlet을 사용하여 백업 작업의 상태를 확인합니다.

이 예제에서는 지정된 날짜에 실행된 모든 작업에 대한 작업 요약 보고서를 표시합니다.

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

SQL Server 리소스 그룹 백업

리소스 페이지에서 필요에 따라 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 첨부되고 일정이 구성된 경우 백업은 일정에 따라 자동으로 수행됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.

검색창에 리소스 그룹 이름을 입력하거나 다음을 선택하여 리소스 그룹을 검색할 수 있습니다.  , 그리고 태그를 선택합니다. 그런 다음 선택할 수 있습니다.  필터 창을 닫으려면.

3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음, *지금 백업*을 선택합니다.
4. 백업 페이지에서 다음 단계를 수행합니다.

- a. 리소스 그룹에 여러 정책을 연결한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. 백업 후, *확인*을 선택하여 주문형 백업을 확인하세요.

정책의 확인 옵션은 예약된 작업에만 적용됩니다.

- c. *백업*을 선택하세요.

5. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

관련 정보

["SQL Server 데이터베이스에 대한 백업 정책 만들기"](#)

["SQL Server에 대한 리소스 그룹 생성 및 정책 연결"](#)

["TCP_TIMEOUT 지연으로 인해 MySQL 연결 오류로 인해 백업 작업이 실패합니다."](#)

["Windows 스케줄러 오류로 인해 백업이 실패합니다."](#)

SnapCenter 작업 페이지에서 **SQL** 리소스 백업 작업을 모니터링합니다.

SnapCenterJobs 페이지를 사용하여 다양한 백업 작업의 진행 상황을 모니터링할 수 있습니다. 완료 시점이나 문제가 있는지 확인하기 위해 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 해당 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한

-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  백업 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *백업*을 선택합니다.
 - d. 상태 드롭다운에서 백업 상태를 선택합니다.
 - e. *적용*을 클릭하면 작업이 성공적으로 완료된 것을 볼 수 있습니다.
4. 백업 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인하세요.



백업 작업 상태가 표시됩니다.  작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 표시가 되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

활동 창에서 **SQL** 리소스에 대한 데이터 보호 작업 모니터링

활동 창에는 가장 최근에 수행된 5개의 작업이 표시됩니다. 활동 창에는 작업이 시작된 시점과 작업 상태도 표시됩니다.

활동 창에는 백업, 복원, 복제 및 예약된 백업 작업에 대한 정보가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 딸깍 하는 소리  활동 창에서 가장 최근의 작업 5개를 확인하세요.

작업 중 하나를 클릭하면 작업 세부 정보가 작업 세부 정보 페이지에 나열됩니다.

Microsoft SQL Server 백업 작업을 위한 **SnapCenter** 플러그인 취소

실행 중이거나 대기 중이거나 응답하지 않는 백업 작업은 취소할 수 있습니다. 백업 작업을 취소하면 SnapCenter Server는 작업을 중지하고, 생성된 백업이 SnapCenter Server에 등록되지 않은 경우 저장소에서 모든 스냅샷을 제거합니다. 백업이 이미 SnapCenter Server에 등록된 경우 취소가 트리거된 후에도 이미 생성된 스냅샷은 롤백되지 않습니다.

시작하기 전에

- 복원 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 대기 중이거나 실행 중인 로그 또는 전체 백업 작업만 취소할 수 있습니다.
- 검증이 시작된 후에는 작업을 취소할 수 없습니다.

검증 전에 작업을 취소할 경우, 작업이 취소되고 검증 작업이 수행되지 않습니다.

- 모니터 페이지나 활동 창에서 백업 작업을 취소할 수 있습니다.
- SnapCenter GUI를 사용하는 것 외에도 PowerShell cmdlet을 사용하여 작업을 취소할 수 있습니다.
- 취소할 수 없는 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자\그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 백업 작업을 취소할 수 있습니다.

단계

다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	1. 왼쪽 탐색 창에서 모니터 > *작업*을 선택합니다. 2. 작업을 선택하고 *작업 취소*를 선택하세요.
활동 창	1. 백업 작업을 시작한 후 다음을 선택하세요.  활동 창에서 가장 최근의 작업 5개를 확인하세요. 2. 작업을 선택하세요. 3. 작업 세부 정보 페이지에서 *작업 취소*를 선택합니다.

결과

작업이 취소되고 리소스는 이전 상태로 돌아갑니다. 취소한 작업이 취소 중 또는 실행 상태에서 응답하지 않는 경우 다음을 실행해야 합니다. `Cancel-SmJob -JobID <int> -Force` 백업 작업을 강제로 중지하는 cmdlet입니다.

토폴로지 페이지에서 SQL Server 백업 및 복제본 보기

리소스를 백업하거나 복제할 준비를 할 때 기본 및 보조 저장소에 있는 모든 백업과 복제본을 그래픽으로 표현해 보면 도움이 될 수 있습니다.

이 작업에 관하여

토폴로지 페이지에서는 선택한 리소스 또는 리소스 그룹에 사용 가능한 모든 백업과 복제본을 볼 수 있습니다. 해당 백업 및 복제의 세부 정보를 보고 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

사본 관리 보기에서 다음 아이콘을 검토하여 백업 및 복제본을 기본 저장소 또는 보조 저장소(미러 사본 또는 볼트 사본)에서 사용할 수 있는지 확인할 수 있습니다.

-  기본 스토리지에서 사용 가능한 백업 및 복제본의 수를 표시합니다.
-



SnapMirror 기술을 사용하여 보조 저장소에 미러링된 백업 및 복제본의 수를 표시합니다.



SnapVault 기술을 사용하여 보조 저장소에 복제된 백업 및 복제본의 수를 표시합니다.

- 표시된 백업 수에는 보조 저장소에서 삭제된 백업이 포함됩니다.

예를 들어, 4개의 백업만 보존하는 정책을 사용하여 6개의 백업을 만든 경우 표시되는 백업 수는 6개입니다.



미러 볼트 유형 볼륨의 버전 가변형 미러 백업의 복제본은 토폴로지 보기에 표시되지만, 토폴로지 보기의 미러 백업 수에는 버전 가변형 백업이 포함되지 않습니다.

SnapMirror Active Sync(처음에는 SnapMirror Business Continuity[SM-BC]로 출시됨)라는 보조 관계가 있는 경우 다음과 같은 추가 아이콘을 볼 수 있습니다.



복제 사이트가 오픈되었습니다.



복제 사이트가 다운되었습니다.



2차 거울이나 볼트 관계가 재설정되지 않았습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 리소스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 리소스를 선택합니다.

선택한 리소스가 복제된 데이터베이스인 경우 복제된 데이터베이스를 보호하면 복제본의 소스가 토폴로지 페이지에 표시됩니다. 복제에 사용된 백업을 보려면 *세부정보*를 클릭하세요.

리소스가 보호된 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. 요약 카드를 검토하여 기본 및 보조 저장소에서 사용 가능한 백업 및 복제본 수에 대한 요약을 확인하세요.

요약 카드 섹션에는 백업 및 복제의 총 수가 표시됩니다.

새로 고침 버튼을 클릭하면 저장소에 대한 쿼리가 시작되어 정확한 개수가 표시됩니다.

SnapLock 이 활성화된 백업을 수행한 경우 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간이 새로 고쳐집니다. 주간 일정은 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간도 새로 고칩니다.

애플리케이션 리소스가 여러 볼륨에 분산되어 있는 경우 백업에 대한 SnapLock 만료 시간은 볼륨의 스냅샷에 설정된 가장 긴 SnapLock 만료 시간이 됩니다. 가장 긴 SnapLock 만료 시간은 ONTAP 에서 검색됩니다.

SnapMirror 활성 동기화의 경우, 새로 고침 버튼을 클릭하면 ONTAP 기본 사이트와 복제 사이트를 모두 쿼리하여 SnapCenter 백업 인벤토리가 새로 고쳐집니다. 주간 일정은 SnapMirror 활성 동기화 관계가 포함된 모든 데이터베이스에 대해 이 활동을 수행합니다.

- SnapMirror 활성화 및 ONTAP 9.14.1의 경우에만 장애 조치 후 새 기본 대상에 대한 비동기 미러 또는 비동기 MirrorVault 관계를 수동으로 구성해야 합니다. ONTAP 9.15.1부터 비동기 미러 또는 비동기 미러볼트가 새로운 기본 대상으로 자동 구성됩니다.
 - 장애 조치 후에는 SnapCenter 에서 장애 조치를 인식할 수 있도록 백업을 만들어야 합니다. 백업이 생성된 후에만 *새로 고침*을 클릭할 수 있습니다.
5. 사본 관리 보기에서 기본 또는 보조 저장소의 백업 또는 *복제본*을 클릭하면 백업 또는 복제본의 세부 정보를 볼 수 있습니다.

백업 및 복제의 세부 정보는 표 형식으로 표시됩니다.

6. 표에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 복제, 이름 바꾸기, 삭제 작업을 수행합니다.



보조 저장소에 있는 백업은 이름을 바꾸거나 삭제할 수 없습니다.

7. 표에서 복제본을 선택하고 *복제 분할*을 클릭합니다.
8. 복제본을 삭제하려면 테이블에서 복제본을 선택한 다음 클릭하세요. .

PowerShell cmdlet을 사용하여 보조 백업 수 정리

Remove-SmBackup cmdlet을 사용하면 스냅샷이 없는 보조 백업의 백업 수를 정리할 수 있습니다. Manage Copies 토폴로지에 표시된 총 스냅샷 수가 보조 저장소 스냅샷 보존 설정과 일치하지 않는 경우 이 cmdlet을 사용할 수 있습니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146/
```

2. -CleanupSecondaryBackups 매개변수를 사용하여 보조 백업 수를 정리합니다.

이 예제에서는 스냅샷이 없는 보조 백업의 백업 수를 정리합니다.

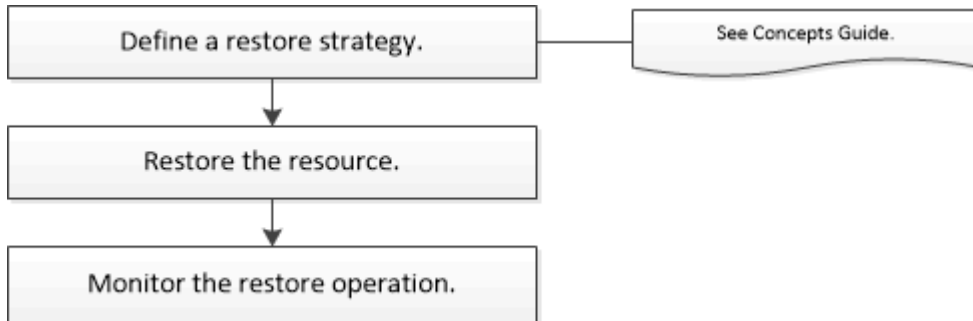
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```


SQL Server 리소스 복원

워크플로 복원

SnapCenter 사용하면 하나 이상의 백업에서 데이터를 활성 파일 시스템으로 복원한 다음 데이터베이스를 복구하여 SQL Server 데이터베이스를 복원할 수 있습니다. 가용성 그룹에 있는 데이터베이스를 복원한 다음 복원된 데이터베이스를 가용성 그룹에 추가할 수도 있습니다. SQL Server 데이터베이스를 복원하기 전에 몇 가지 준비 작업을 수행해야 합니다.

다음 워크플로는 데이터베이스 복원 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원, 복구, 확인 및 복제 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 다음을 참조하세요. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#)

더 많은 정보를 찾아보세요

["보조 저장소에서 SQL Server 데이터베이스 복원"](#)

["PowerShell cmdlet을 사용하여 리소스 복원 및 복구"](#)

["Windows 2008 R2에서 복원 작업이 실패할 수 있습니다."](#)

데이터베이스 복원을 위한 요구 사항

Microsoft SQL Server 백업용 SnapCenter 플러그인에서 SQL Server 데이터베이스를 복원하기 전에 몇 가지 요구 사항이 충족되는지 확인해야 합니다.

- 데이터베이스를 복원하려면 대상 SQL Server 인스턴스가 온라인 상태이고 실행 중이어야 합니다.
이는 사용자 데이터베이스 복원 작업과 시스템 데이터베이스 복원 작업 모두에 적용됩니다.
- 복원 중인 SQL Server 데이터에 대해 실행되도록 예약된 SnapCenter 작업은 원격 관리 또는 원격 확인 서버에서 예약된 모든 작업을 포함하여 비활성화해야 합니다.
- 시스템 데이터베이스가 작동하지 않는 경우 먼저 SQL Server 유틸리티를 사용하여 시스템 데이터베이스를 다시 빌드해야 합니다.
- 플러그인을 설치하는 경우 다른 역할에 가용성 그룹(AG) 백업을 복원할 수 있는 권한을 부여해야 합니다.

다음 조건 중 하나가 충족되면 AG 복원이 실패합니다.

- RBAC 사용자가 플러그인을 설치하고 관리자가 AG 백업을 복원하려고 시도하는 경우
- 플러그인이 관리자에 의해 설치되고 RBAC 사용자가 AG 백업을 복원하려고 시도하는 경우
- 사용자 정의 로그 디렉토리 백업을 대체 호스트로 복원하는 경우 SnapCenter 서버와 플러그인 호스트에 동일한 SnapCenter 버전이 설치되어 있어야 합니다.
- Microsoft 핫픽스 KB2887595를 설치했어야 합니다. Microsoft 지원 사이트에서 KB2887595에 대한 자세한 정보를 확인할 수 있습니다.

"Microsoft 지원 문서 2887595: Windows RT 8.1, Windows 8.1 및 Windows Server 2012 R2 업데이트 롤업: 2013년 11월"

- 리소스 그룹이나 데이터베이스를 백업해야 합니다.
- 스냅샷을 미리 또는 볼트에 복제하는 경우 SnapCenter 관리자가 소스 볼륨과 대상 볼륨 모두에 대한 스토리지 가상 머신(SVM)을 할당해야 합니다.

관리자가 사용자에게 리소스를 할당하는 방법에 대한 자세한 내용은 SnapCenter 설치 정보를 참조하세요.

- 데이터베이스를 복원하기 전에 모든 백업 및 복제 작업을 중지해야 합니다.
- 데이터베이스 크기가 테라바이트(TB)인 경우 복원 작업의 시간이 초과될 수 있습니다.

다음 명령을 실행하여 SnapCenter 서버의 RESTTimeout 매개변수 값을 20000000ms로 늘려야 합니다. Set-SmConfigSettings -Agent -configSettings @"{\"RESTTimeout\" = \"20000000\"}. 데이터베이스 크기에 따라 타임아웃 값을 변경할 수 있으며, 설정할 수 있는 최대값은 86400000ms입니다.

데이터베이스가 온라인 상태인 동안 복원하려면 복원 페이지에서 온라인 복원 옵션을 활성화해야 합니다.

SQL Server 데이터베이스 백업 복원

SnapCenter 사용하면 백업된 SQL Server 데이터베이스를 복원할 수 있습니다. 데이터베이스 복원은 지정된 SQL Server 백업에서 모든 데이터와 로그 페이지를 지정된 데이터베이스로 복사하는 다단계 프로세스입니다.

이 작업에 관하여

- 백업이 생성된 동일한 호스트의 다른 SQL Server 인스턴스로 백업된 SQL Server 데이터베이스를 복원할 수 있습니다.

SnapCenter 사용하면 백업된 SQL Server 데이터베이스를 대체 경로로 복원할 수 있으므로 프로덕션 버전을 교체하지 않아도 됩니다.

- SnapCenter SQL Server 클러스터 그룹을 오프라인으로 전환하지 않고도 Windows 클러스터의 데이터베이스를 복원할 수 있습니다.
- 복원 작업 중에 클러스터 오류(클러스터 그룹 이동 작업)가 발생하는 경우(예: 리소스를 소유한 노드가 중단되는 경우) SQL Server 인스턴스에 다시 연결한 다음 복원 작업을 다시 시작해야 합니다.
- 사용자나 SQL Server 에이전트 작업이 데이터베이스에 액세스하는 동안에는 데이터베이스를 복원할 수 없습니다.
- 시스템 데이터베이스를 대체 경로로 복원할 수 없습니다.
- SCRIPTS_PATH는 플러그인 호스트의 SMCoreServiceHost.exe.Config 파일에 있는 PredefinedWindowsScriptsDirectory 키를 사용하여 정의됩니다.

필요한 경우 이 경로를 변경하고 SMcore 서비스를 다시 시작할 수 있습니다. 보안을 위해 기본 경로를 사용하는 것이 좋습니다.

키 값은 API를 통해 swagger에서 표시될 수 있습니다: API /4.7/configsettings

GET API를 사용하여 키 값을 표시할 수 있습니다. SET API는 지원되지 않습니다.

- 복원 마법사 페이지의 대부분 필드는 설명이 필요 없습니다. 다음 정보는 귀하에게 지침이 필요할 수 있는 분야에 대한 설명입니다.
- SnapMirror Active Sync 복원 작업의 경우 기본 위치에서 백업을 선택해야 합니다.
- SnapLock 활성화된 정책의 경우 ONTAP 9.12.1 이하 버전에서 스냅샷 잠금 기간을 지정하면 복원의 일부로 변조 방지 스냅샷에서 생성된 복제본은 SnapLock 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 목록에서 데이터베이스나 리소스 그룹을 선택하세요.

토폴로지 페이지가 표시됩니다.

4. 사본 관리 보기에서 스토리지 시스템의 *백업*을 선택합니다.
5. 테이블에서 백업을 선택한 다음 클릭하십시오.  상.



6. 복원 범위 페이지에서 다음 옵션 중 하나를 선택하세요.

옵션	설명
백업이 생성된 동일한 호스트로 데이터베이스를 복원합니다.	백업이 수행된 동일한 SQL 서버로 데이터베이스를 복원하려면 이 옵션을 선택하세요.
데이터베이스를 대체 호스트로 복원합니다.	백업이 수행되는 동일하거나 다른 호스트의 다른 SQL 서버로 데이터베이스를 복원하려면 이 옵션을 선택하세요. 호스트 이름을 선택하고, 데이터베이스 이름을 제공하고(선택 사항), 인스턴스를 선택하고, 복원 경로를 지정합니다.  대체 경로에 제공된 파일 확장자는 원본 데이터베이스 파일의 파일 확장자와 동일해야 합니다. 데이터베이스를 대체 호스트로 복원 옵션이 복원 범위 페이지에 표시되지 않으면 브라우저 캐시를 지우세요.

옵션	설명
기존 데이터베이스 파일을 사용하여 데이터베이스 복원	백업이 수행되는 동일하거나 다른 호스트에 있는 대체 SQL Server로 데이터베이스를 복원하려면 이 옵션을 선택합니다. 데이터베이스 파일은 이미 주어진 기존 파일 경로에 존재해야 합니다. 호스트 이름을 선택하고, 데이터베이스 이름을 제공하고(선택 사항), 인스턴스를 선택하고, 복원 경로를 지정합니다.

7. 복구 범위 페이지에서 다음 옵션 중 하나를 선택하세요.

옵션	설명
None	로그 없이 전체 백업만 복원해야 하는 경우 *없음*을 선택합니다.
모든 로그 백업	전체 백업 후 사용 가능한 모든 로그 백업을 복원하려면 모든 로그 백업 최신 백업 복원 작업을 선택합니다.
로그 백업까지	*로그 백업 기준*을 선택하면 특정 날짜의 백업 로그를 기준으로 데이터베이스를 복원하는 지정 시간 복원 작업이 수행됩니다.
특정 날짜까지	복원된 데이터베이스에 트랜잭션 로그가 적용되지 않는 날짜와 시간을 지정하려면 *특정 날짜까지*를 선택합니다. 이 지정 시간 복원 작업은 지정된 날짜 및 시간 이후에 기록된 트랜잭션 로그 항목의 복원을 중지합니다.
사용자 정의 로그 디렉토리 사용	모든 로그 백업, 로그 백업 기준 또는 *특정 날짜 기준*을 선택했고 로그가 사용자 지정 위치에 있는 경우, *사용자 지정 로그 디렉터리 사용*을 선택한 다음 로그 위치를 지정합니다. 사용자 정의 로그 디렉터리 사용 옵션은 데이터베이스를 대체 호스트로 복원 또는 *기존 데이터베이스 파일을 사용하여 데이터베이스 복원*을 선택한 경우에만 사용할 수 있습니다. 공유 경로를 사용할 수도 있지만 SQL 사용자가 해당 경로에 액세스할 수 있는지 확인하세요.  사용자 정의 로그 디렉토리는 가용성 그룹 데이터베이스에서 지원되지 않습니다.

8. 사전 작업 페이지에서 다음 단계를 수행하세요.

a. 복원 전 옵션 페이지에서 다음 옵션 중 하나를 선택하세요.

- 동일한 이름의 데이터베이스를 복원하려면 *복원 중 동일한 이름으로 데이터베이스 덮어쓰기*를 선택하세요.
- 데이터베이스를 복원하고 기존 복제 설정을 유지하려면 *SQL 데이터베이스 복제 설정 유지*를 선택합니다.
- 복원 작업이 시작되기 전에 트랜잭션 로그를 생성하려면 *복원 전 트랜잭션 로그 백업 생성*을 선택합니다.
- 트랜잭션 로그 백업이 실패하면 복원 작업을 중단하려면 *복원 전 트랜잭션 로그 백업이 실패하면 복원 중지*를 선택합니다.

b. 복원 작업을 수행하기 전에 실행할 선택적 스크립트를 지정합니다.

예를 들어, SNMP 트랩을 업데이트하고, 알림을 자동화하고, 로그를 보내는 등의 작업을 수행하는 스크립트를 실행할 수 있습니다.



prescripts 또는 postscripts 경로에는 드라이브나 공유가 포함되어서는 안 됩니다. 경로는 SCRIPTS_PATH를 기준으로 해야 합니다.

9. Post Ops 페이지에서 다음 단계를 수행하세요.

a. 복원 완료 후 데이터베이스 상태 선택 섹션에서 다음 옵션 중 하나를 선택합니다.

- 지금 필요한 모든 백업을 복원하는 경우 *작동 중이지만 추가 트랜잭션 로그를 복원할 수 없음*을 선택합니다.

이는 커밋되지 않은 트랜잭션을 롤백하여 데이터베이스를 사용할 수 있도록 준비하는 기본 동작입니다. 백업을 생성하기 전까지는 추가 거래 로그를 복원할 수 없습니다.

- 커밋되지 않은 트랜잭션을 롤백하지 않고 데이터베이스를 비작동 상태로 두려면 *비작동 상태이지만 추가 트랜잭션 로그 복원에 사용 가능*을 선택합니다.

추가 거래 로그를 복원할 수 있습니다. 복구될 때까지 데이터베이스를 사용할 수 없습니다.

- 데이터베이스를 읽기 전용 모드로 두려면 *추가 트랜잭션 로그 복원에 사용 가능한 읽기 전용 모드*를 선택합니다.

이 옵션은 커밋되지 않은 트랜잭션을 실행 취소하지만, 실행 취소된 작업을 대기 파일에 저장하여 복구 효과를 되돌릴 수 있습니다.

실행 취소 디렉토리 옵션이 활성화된 경우 더 많은 트랜잭션 로그가 복원됩니다. 트랜잭션 로그에 대한 복원 작업이 실패하면 변경 사항을 롤백할 수 있습니다. 자세한 내용은 SQL Server 설명서를 참조하세요.

b. 복원 작업을 수행한 후 실행할 선택적 스크립트를 지정합니다.

예를 들어, SNMP 트랩을 업데이트하고, 알림을 자동화하고, 로그를 보내는 등의 작업을 수행하는 스크립트를 실행할 수 있습니다.



prescripts 또는 postscripts 경로에는 드라이브나 공유가 포함되어서는 안 됩니다. 경로는 SCRIPTS_PATH를 기준으로 해야 합니다.

10. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다.

11. 요약을 검토한 후 *마침*을 클릭하세요.

12. 모니터 > 작업 페이지를 사용하여 복원 프로세스를 모니터링합니다.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-Smconnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

이 예에서는 2015년 1월 29일부터 2015년 2월 3일까지의 백업에 대한 자세한 정보를 표시합니다.

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.


```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

보조 저장소에서 **SQL Server** 데이터베이스 복원

보조 스토리지 시스템의 물리적 LUN(RDM, iSCSI 또는 FCP)에서 백업된 SQL Server 데이터베이스를 복원할 수 있습니다. 복원 기능은 보조 스토리지 시스템에 있는 지정된 SQL Server 백업에서 모든 데이터와 로그 페이지를 지정된 데이터베이스로 복사하는 다단계 프로세스입니다.

시작하기 전에

- 기본 스토리지 시스템에서 보조 스토리지 시스템으로 스냅샷을 복제했어야 합니다.
- SnapCenter 서버와 플러그인 호스트가 보조 스토리지 시스템에 연결할 수 있는지 확인해야 합니다.
- 복원 마법사 페이지의 대부분 필드는 기본 복원 프로세스에서 설명됩니다. 다음 정보는 귀하에게 지침이 필요할 수

있는 몇몇 분야에 대해 설명합니다.

이 작업에 관하여

SnapLock 활성화된 정책의 경우 ONTAP 9.12.1 이하 버전에서 스냅샷 잠금 기간을 지정하면 복원의 일부로 변조 방지 스냅샷에서 생성된 복제본은 SnapLock 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 *SQL Server용 SnapCenter 플러그인*을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 데이터베이스 또는 리소스 그룹을 선택하세요.

데이터베이스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. '복사본 관리' 섹션에서 보조 저장 시스템(미러링 또는 볼트)의 *백업*을 선택합니다.
5. 목록에서 백업을 선택한 다음 클릭하세요. .
6. 위치 페이지에서 선택한 리소스를 복원할 대상 볼륨을 선택합니다.
7. 복원 마법사를 완료하고 요약을 검토한 후 *마침*을 클릭합니다.

다른 데이터베이스에서 공유하는 다른 경로로 데이터베이스를 복원한 경우 전체 백업과 백업 확인을 수행하여 복원된 데이터베이스에 물리적 수준의 손상이 없는지 확인해야 합니다.

PowerShell cmdlet을 사용하여 리소스 복원

리소스 백업을 복원하려면 SnapCenter 서버와 연결 세션을 시작하고, 백업을 나열하고 백업 정보를 검색하고, 백업을 복원해야 합니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-Smconnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----
1	Payroll Dataset_vise-f6_08... 8/4/2015	11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08... 8/4/2015	11:23:17 AM

이 예에서는 2015년 1월 29일부터 2015년 2월 3일까지의 백업에 대한 자세한 정보를 표시합니다.

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

가용성 그룹 데이터베이스 다시 시드

Reseed는 가용성 그룹(AG) 데이터베이스를 복원하는 옵션입니다. AG에서 보조 데이터베이스가 기본 데이터베이스와 동기화되지 않으면 보조 데이터베이스를 다시 시드할 수 있습니다.

시작하기 전에

- 복원하려는 보조 AG 데이터베이스의 백업을 만들어야 합니다.
- SnapCenter 서버와 플러그인 호스트에는 동일한 SnapCenter 버전이 설치되어 있어야 합니다.

이 작업에 관하여

- 기본 데이터베이스에서는 다시 시드 작업을 수행할 수 없습니다.

- 가용성 그룹에서 복제본 데이터베이스가 제거되면 다시 시드 작업을 수행할 수 없습니다. 복제본이 제거되면 다시 시드 작업이 실패합니다.
- SQL 가용성 그룹 데이터베이스에서 재시드 작업을 실행하는 동안 해당 가용성 그룹 데이터베이스의 복제본 데이터베이스에서 로그 백업을 트리거해서는 안 됩니다. 재시드 작업 중에 로그 백업을 트리거하면 재시드 작업이 실패하고 "미러 데이터베이스 "database_name"에 주 데이터베이스의 로그 백업 체인을 보존할 만큼 트랜잭션 로그 데이터가 부족합니다" 오류 메시지가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 *SQL Server용 SnapCenter 플러그인*을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *데이터베이스*를 선택합니다.
3. 목록에서 보조 AG 데이터베이스를 선택하세요.
4. *다시 시드*를 클릭하세요.
5. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

SQL 리소스 복원 작업 모니터링

작업 페이지를 사용하여 다양한 SnapCenter 복원 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

복원 후 상태는 복원 작업 후 리소스의 조건과 수행할 수 있는 추가 복원 작업을 설명합니다.

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복원 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복원*을 선택합니다.
 - d. 상태 드롭다운 목록에서 복원 상태를 선택합니다.

- e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
- 4. 복원 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
- 5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

SQL 리소스 복원 작업 취소

대기 중인 복원 작업을 취소할 수 있습니다.

복원 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

이 작업에 관하여

- 모니터 페이지나 활동 창에서 대기 중인 복원 작업을 취소할 수 있습니다.
- 실행 중인 복원 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 대기 중인 복원 작업을 취소할 수 있습니다.
- 취소할 수 없는 복원 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자 그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 복원 작업을 취소할 수 있습니다.

단계

다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	1. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. 2. 작업을 선택하고 *작업 취소*를 클릭하세요.
활동 창	1. 복원 작업을 시작한 후 다음을 클릭하세요.  활동 창에서 가장 최근의 작업 5개를 확인하세요. 2. 작업을 선택하세요. 3. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

SQL Server 데이터베이스 리소스 복제

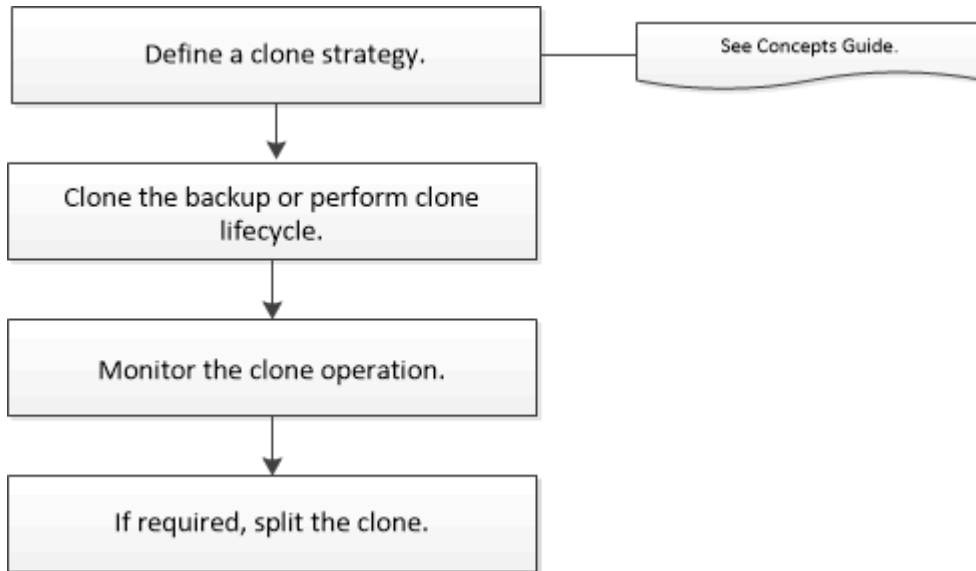
복제 워크플로

백업에서 데이터베이스 리소스를 복제하기 전에 SnapCenter Server를 사용하여 여러 작업을 수행해야 합니다. 데이터베이스 복제는 운영 데이터베이스나 백업 세트의 특정 시점 복사본을 만드는 프로세스입니다. 애플리케이션 개발 주기 동안 현재 데이터베이스 구조와 콘텐츠를 사용하여 구현해야 하는 기능을 테스트하거나, 데이터 웨어하우스를 채울 때 데이터 추출 및 조작 도구를 사용하거나, 실수로 삭제되거나 변경된 데이터를 복구하기 위해 데이터베이스를 복제할

수 있습니다.

데이터베이스 복제 작업은 작업 ID를 기반으로 보고서를 생성합니다.

다음 워크플로는 복제 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원, 복구, 확인 및 복제 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 다음을 참조하세요. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#)

더 많은 정보를 찾아보세요

["SQL Server 데이터베이스 백업에서 복제"](#)

["복제 수명 주기 수행"](#)

["기본 TCP_TIMEOUT 값을 사용하면 복제 작업이 실패하거나 완료하는 데 시간이 더 오래 걸릴 수 있습니다."](#)

SQL Server 데이터베이스 백업에서 복제

SnapCenter 사용하여 SQL Server 데이터베이스 백업을 복제할 수 있습니다. 이전 버전의 데이터에 액세스하거나 복원하려면 필요에 따라 데이터베이스 백업을 복제할 수 있습니다.

시작하기 전에

- 호스트 추가, 리소스 식별, 스토리지 시스템 연결 생성 등의 작업을 완료하여 데이터 보호를 준비했어야 합니다.
- 데이터베이스나 리소스 그룹을 백업했어야 합니다.
- 데이터 LUN과 로그 LUN에 대한 미러, 볼트 또는 미러-볼트와 같은 보호 유형은 로그 백업을 사용하여 대체 호스트에 복제하는 동안 보조 로케이터를 검색하기 위해 동일해야 합니다.
- SnapCenter 복제 작업 중에 마운트된 복제 드라이브를 찾을 수 없는 경우 SnapCenter 서버의 CloneRetryTimeout 매개변수를 300으로 변경해야 합니다.
- 볼륨을 호스팅하는 집계가 스토리지 가상 머신(SVM)의 할당된 집계 목록에 있는지 확인해야 합니다.

이 작업에 관하여

- 독립 실행형 데이터베이스 인스턴스에 복제하는 동안 마운트 지점 경로가 존재하고 전용 디스크인지 확인하세요.
- FCI(장애 조치 클러스터 인스턴스)에 복제하는 동안 마운트 지점이 있는지, 공유 디스크인지, 경로와 FCI가 동일한 SQL 리소스 그룹에 속해야 하는지 확인하세요.
- 각 호스트에 연결된 vFC 또는 FC 이니시에이터가 하나만 있는지 확인하세요. 이는 SnapCenter 호스트당 하나의 이니시에이터만 지원하기 때문입니다.
- 소스 데이터베이스 또는 대상 인스턴스가 클러스터 공유 볼륨(CSV)에 있는 경우 복제된 데이터베이스는 CSV에 있습니다.
- SCRIPTS_PATH는 플러그인 호스트의 SMCoreServiceHost.exe.Config 파일에 있는 PredefinedWindowsScriptsDirectory 키를 사용하여 정의됩니다.

필요한 경우 이 경로를 변경하고 SMcore 서비스를 다시 시작할 수 있습니다. 보안을 위해 기본 경로를 사용하는 것이 좋습니다.

키 값은 API를 통해 swagger에서 표시될 수 있습니다: API /4.7/configsettings

GET API를 사용하여 키 값을 표시할 수 있습니다. SET API는 지원되지 않습니다.



가상 환경(VMDK/RDM)의 경우 마운트 지점이 전용 디스크인지 확인하세요.

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 *SQL Server용 SnapCenter 플러그인*을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.



인스턴스 백업 복제는 지원되지 않습니다.

3. 데이터베이스 또는 리소스 그룹을 선택하세요.
4. 사본 관리 보기 페이지에서 기본 또는 보조(미러링 또는 보관) 스토리지 시스템에서 백업을 선택합니다.
5. 백업을 선택한 후 *를 선택하세요  *.
6. 복제 옵션 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
복제 서버	복제본을 생성할 호스트를 선택하세요.
인스턴스 복제	데이터베이스 백업을 복제할 복제 인스턴스를 선택합니다. 이 SQL 인스턴스는 지정된 복제 서버에 있어야 합니다.
클론 접미사	데이터베이스가 복제본임을 식별하기 위해 복제 파일 이름에 추가될 접미사를 입력하세요. 예를 들어, <i>db1_clone</i>. 원본 데이터베이스와 동일한 위치에 복제하는 경우 복제된 데이터베이스와 원본 데이터베이스를 구별하기 위해 접미사를 제공해야 합니다. 그렇지 않으면 작업이 실패합니다.
경로 아래에 마운트 지점 자동 할당 또는 볼륨 마운트 지점 자동 할당	경로 아래에 마운트 지점이나 볼륨 마운트 지점을 자동으로 할당할지 여부를 선택합니다. 경로 아래의 볼륨 마운트 지점을 자동으로 할당: 경로 아래의 마운트 지점을 사용하면 특정 디렉토리를 제공할 수 있습니다. 해당 디렉토리 내에 마운트 지점이 생성됩니다. 이 옵션을 선택하기 전에 디렉토리가 비어 있는지 확인해야 합니다. 디렉토리에 데이터베이스가 있는 경우 마운트 작업 후 데이터베이스는 유효하지 않은 상태가 됩니다.

7. 로그 페이지에서 다음 옵션 중 하나를 선택하세요.

이 분야에서는...	이렇게 하세요...
None	로그 없이 전체 백업만 복제하려는 경우 이 옵션을 선택하세요.
모든 로그 백업	전체 백업 이후의 모든 사용 가능한 로그 백업을 복제하려면 이 옵션을 선택합니다.
로그 백업까지	선택한 날짜의 백업 로그까지 생성된 백업 로그를 기반으로 데이터베이스를 복제하려면 이 옵션을 선택하세요.
특정 날짜까지	복제된 데이터베이스에 트랜잭션 로그가 적용되지 않는 날짜와 시간을 지정합니다. 이 시점 복제는 지정된 날짜 및 시간 이후에 기록된 트랜잭션 로그 항목의 복제를 중지합니다.

8. 스크립트 페이지에서 복제 작업 전이나 후에 실행해야 하는 스크립트 시간 초과, 경로, 프리스크립트 또는 포스트스크립트의 인수를 각각 입력합니다.

예를 들어, SNMP 트랩을 업데이트하고, 알림을 자동화하고, 로그를 보내는 등의 작업을 수행하는 스크립트를 실행할 수 있습니다.



prescripts 또는 postscripts 경로에는 드라이브나 공유가 포함되어서는 안 됩니다. 경로는 SCRIPTS_PATH를 기준으로 해야 합니다.

기본 스크립트 시간 초과는 60초입니다.

9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 수행된 복제 작업의 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtptServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

EMS의 경우 다음을 참조하세요. ["EMS 데이터 수집 관리"](#)

10. 요약을 검토한 후 *마침*을 선택하세요.
11. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

당신이 완료한 후

복제본을 만든 후에는 절대로 이름을 바꾸면 안 됩니다.

관련 정보

["기본 TCP_TIMEOUT 값을 사용하면 복제 작업이 실패하거나 완료하는 데 시간이 더 오래 걸릴 수 있습니다."](#)

"장애 조치(failover) 클러스터 인스턴스 데이터베이스 복제가 실패합니다."

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Get-SmBackup 또는 Get-SmResourceGroup cmdlet을 사용하여 복제할 수 있는 백업을 나열합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

이 예제에서는 지정된 리소스 그룹, 해당 리소스 및 관련 정책에 대한 정보를 표시합니다.

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMapping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
```

EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False

```

Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False

```

3. New-SmClone cmdlet을 사용하여 기존 백업에서 복제 작업을 시작합니다.

이 예제에서는 모든 로그를 포함하는 지정된 백업에서 복제본을 만듭니다.

```

PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy

```

이 예제에서는 지정된 Microsoft SQL Server 인스턴스에 대한 복제본을 만듭니다.

```
PS C:\> New-SmClone
-B BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-R Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-A AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-S Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. Get-SmCloneReport cmdlet을 사용하여 복제 작업의 상태를 확인합니다.

이 예제에서는 지정된 작업 ID에 대한 복제 보고서를 표시합니다.

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

복제 수명 주기 수행

SnapCenter 사용하면 리소스 그룹이나 데이터베이스에서 복제본을 만들 수 있습니다. 주문형 복제를 수행하거나 리소스 그룹이나 데이터베이스의 반복 복제 작업을 예약할 수 있습니다. 백업을 주기적으로 복제하면 복제본을 사용하여 애플리케이션을 개발하고, 데이터를 채우거나, 데이터를 복구할 수 있습니다.

SnapCenter 사용하면 여러 서버에서 동시에 여러 복제 작업을 실행하도록 예약할 수 있습니다.

시작하기 전에

- 독립 실행형 데이터베이스 인스턴스에 복제하는 동안 마운트 지점 경로가 존재하고 전용 디스크인지 확인하세요.
- FCI(장애 조치 클러스터 인스턴스)에 복제하는 동안 마운트 지점이 있는지, 공유 디스크인지, 경로와 FCI가 동일한 SQL 리소스 그룹에 속해야 하는지 확인하세요.
- 소스 데이터베이스 또는 대상 인스턴스가 클러스터 공유 볼륨(CSV)에 있는 경우 복제된 데이터베이스는 CSV에 있습니다.



가상 환경(VMDK/RDM)의 경우 마운트 지점이 전용 디스크인지 확인하세요.

이 작업에 관하여

- SCRIPTS_PATH는 플러그인 호스트의 SMCoreServiceHost.exe.Config 파일에 있는 PredefinedWindowsScriptsDirectory 키를 사용하여 정의됩니다.

필요한 경우 이 경로를 변경하고 SMcore 서비스를 다시 시작할 수 있습니다. 보안을 위해 기본 경로를 사용하는 것이 좋습니다.

키 값은 API를 통해 swagger에서 표시될 수 있습니다: API /4.7/configsettings

GET API를 사용하여 키 값을 표시할 수 있습니다. SET API는 지원되지 않습니다.

- 복제 수명 주기 마법사 페이지의 대부분 필드는 설명이 필요 없습니다. 다음 정보는 귀하에게 지침이 필요할 수 있는 분야에 대한 설명입니다.
- ONTAP 9.12.1 이하 버전의 경우 스냅샷 잠금 기간을 지정하면 변조 방지 스냅샷에서 생성된 복제본은 SnapLock 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 리소스 그룹이나 데이터베이스를 선택한 다음 *라이프사이클 복제*를 클릭합니다.
4. 옵션 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
복제 작업 이름	복제 수명 주기 작업을 모니터링하고 수정하는 데 도움이 되는 복제 수명 주기 작업 이름을 지정합니다.
복제 서버	복제본을 배치할 호스트를 선택하세요.
인스턴스 복제	데이터베이스를 복제할 복제 인스턴스를 선택합니다. 이 SQL 인스턴스는 지정된 복제 서버에 있어야 합니다.

이 분야에서는...	이렇게 하세요...
클론 접미사	복제본임을 식별하기 위해 복제본 데이터베이스에 추가될 접미사를 입력하세요. 복제 리소스 그룹을 만드는 데 사용되는 각 SQL 인스턴스에는 고유한 데이터베이스 이름이 있어야 합니다. 예를 들어, 복제 리소스 그룹에 SQL 인스턴스 "inst1"의 소스 데이터베이스 "db1"이 포함되어 있고, "db1"이 "inst1"에 복제된 경우, 복제 데이터베이스 이름은 "db1clone"이어야 합니다. "clone"은 데이터베이스가 동일한 인스턴스에 복제되므로 필수 사용자 정의 접미사입니다. "db1"이 SQL 인스턴스 "inst2"에 복제되면 복제 데이터베이스 이름은 "db1"(접미사는 선택 사항)로 유지될 수 있습니다. 데이터베이스가 다른 인스턴스에 복제되기 때문입니다.
경로 아래에 마운트 지점 자동 할당 또는 볼륨 마운트 지점 자동 할당	경로 아래에 마운트 지점이나 볼륨 마운트 지점을 자동으로 할당할지 여부를 선택합니다. 경로 아래에 볼륨 마운트 지점을 자동으로 할당하도록 선택하면 특정 디렉토리를 제공할 수 있습니다. 해당 디렉토리 내에 마운트 지점이 생성됩니다. 이 옵션을 선택하기 전에 디렉토리가 비어 있는지 확인해야 합니다. 디렉토리에 데이터베이스가 있는 경우 마운트 작업 후 데이터베이스는 유효하지 않은 상태가 됩니다.

5. 위치 페이지에서 복제본을 만들 저장 위치를 선택합니다.

6. 스크립트 페이지에서 복제 작업 전이나 후에 실행해야 하는 프리스크립트나 포스트스크립트의 경로와 인수를 각각 입력합니다.

예를 들어, SNMP 트랩을 업데이트하고, 알림을 자동화하고, 로그를 보내는 등의 작업을 수행하는 스크립트를 실행할 수 있습니다.



prescripts 또는 postscripts 경로에는 드라이브나 공유가 포함되어서는 안 됩니다. 경로는 SCRIPTS_PATH를 기준으로 해야 합니다.

기본 스크립트 시간 초과는 60초입니다.

7. 일정 페이지에서 다음 작업 중 하나를 수행합니다.

- 복제 작업을 즉시 실행하려면 *지금 실행*을 선택하세요.
- 복제 작업이 얼마나 자주 발생해야 하는지, 복제 일정을 언제 시작해야 하는지, 복제 작업이 어느 요일에 발생해야 하는지, 일정이 언제 만료되어야 하는지, 일정이 만료된 후 복제본을 삭제해야 하는지 여부를 결정하려면 *일정 구성*을 선택합니다.

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 수행된 복제 작업의 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

EMS의 경우 다음을 참조하세요. "[EMS 데이터 수집 관리](#)"

9. 요약을 검토한 후 *마침*을 클릭하세요.

모니터 > 작업 페이지를 사용하여 복제 프로세스를 모니터링해야 합니다.

SQL 데이터베이스 복제 작업 모니터링

작업 페이지를 사용하여 SnapCenter 복제 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복제 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복제*를 선택합니다.
 - d. 상태 드롭다운 목록에서 복제 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복제 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

SQL 리소스 복제 작업 취소

대기 중인 복제 작업을 취소할 수 있습니다.

복제 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

이 작업에 관하여

- 모니터 페이지나 활동 창에서 대기 중인 복제 작업을 취소할 수 있습니다.

- 실행 중인 복제 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 대기 중인 복제 작업을 취소할 수 있습니다.
- 역할을 생성할 때 사용자 그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 객체를 보고 조작할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 복제 작업을 취소할 수 있습니다.

단계

다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	1. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. 2. 작업을 선택하고 *작업 취소*를 클릭합니다.
활동 창	1. 복제 작업을 시작한 후 다음을 클릭하세요.  활동 창에서 가장 최근의 작업 5개를 확인하세요. 2. 작업을 선택하세요. 3. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

클론 분할

SnapCenter 사용하면 복제된 리소스를 부모 리소스에서 분할할 수 있습니다. 분할된 복제본은 부모 리소스로부터 독립됩니다.

이 작업에 관하여

- 중간 복제본에서는 복제 분할 작업을 수행할 수 없습니다.

예를 들어, 데이터베이스 백업에서 clone1을 만든 후 clone1의 백업을 만든 다음 이 백업(clone2)을 복제할 수 있습니다. clone2를 생성한 후 clone1은 중간 복제본이 되며 clone1에서 복제 분할 작업을 수행할 수 없습니다. 하지만 clone2에 대해 클론 분할 작업을 수행할 수 있습니다.

clone2를 분할한 후에는 clone1에 대해 clone 분할 작업을 수행할 수 있습니다. clone1은 더 이상 중간 클론이 아니기 때문입니다.

- 복제본을 분할하면 복제본의 백업 사본과 복제 작업이 삭제됩니다.
- FlexClone 볼륨 분할 작업에 대한 정보는 다음을 참조하세요. "[FlexClone 볼륨을 부모 볼륨에서 분할합니다.](#)".
- 스토리지 시스템의 볼륨이나 집계가 온라인인지 확인하세요.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 적절한 옵션을 선택하세요.

옵션	설명
데이터베이스 애플리케이션의 경우	보기 목록에서 *데이터베이스*를 선택합니다.

옵션	설명
파일 시스템의 경우	보기 목록에서 *경로*를 선택합니다.

3. 목록에서 적절한 리소스를 선택하세요.

리소스 토폴로지 페이지가 표시됩니다.

4. 사본 관리 보기에서 복제된 리소스(예: 데이터베이스 또는 LUN)를 선택한 다음 *를 클릭합니다.  *.

5. 분할할 클론의 예상 크기와 집계에 필요한 사용 가능한 공간을 검토한 다음 *시작*을 클릭합니다.

6. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

SMCore 서비스를 다시 시작하면 복제 분할 작업이 더 이상 응답하지 않습니다. 복제 분할 작업을 중지하려면 Stop-SmJob cmdlet을 실행한 다음 복제 분할 작업을 다시 시도해야 합니다.

복제본이 분할되었는지 여부를 확인하기 위해 더 긴 폴링 시간이나 더 짧은 폴링 시간이 필요한 경우 *SMCoreServiceHost.exe.config* 파일에서 *CloneSplitStatusCheckPollTime* 매개변수 값을 변경하여 SMCore가 복제본 분할 작업의 상태를 폴링하는 시간 간격을 설정할 수 있습니다. 값은 밀리초이고 기본값은 5분입니다.

예를 들어:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

백업, 복원 또는 다른 클론 분할이 진행 중이면 클론 분할 시작 작업이 실패합니다. 실행 중인 작업이 완료된 후에만 복제 분할 작업을 다시 시작해야 합니다.

관련 정보

"SnapCenter 복제 또는 검증이 집계 존재하지 않아 실패합니다."

SAP HANA 데이터베이스 보호

SAP HANA 데이터베이스용 SnapCenter 플러그인

SAP HANA 데이터베이스용 SnapCenter 플러그인 개요

SAP HANA 데이터베이스용 SnapCenter 플러그인은 NetApp SnapCenter software 의 호스트 측 구성 요소로, SAP HANA 데이터베이스의 애플리케이션 인식 데이터 보호 관리를 지원합니다. SAP HANA 데이터베이스용 플러그인은 SnapCenter 환경에서 SAP HANA 데이터베이스의 백업, 복원 및 복제를 자동화합니다.

SnapCenter 단일 컨테이너와 멀티테넌트 데이터베이스 컨테이너(MDC)를 지원합니다. Windows와 Linux 환경 모두에서 SAP HANA 데이터베이스 플러그인을 사용할 수 있습니다. HANA 데이터베이스 호스트에 설치되지 않은 플러그인을 중앙 집중식 호스트 플러그인이라고 합니다. 중앙 집중식 호스트 플러그인은 여러 호스트에 걸쳐 있는 여러 HANA 데이터베이스를 관리할 수 있습니다.

SAP HANA 데이터베이스용 플러그인이 설치되면 NetApp SnapMirror 기술과 함께 SnapCenter 사용하여 다른 볼륨에 백업 세트의 미러 사본을 만들 수 있습니다. NetApp SnapVault 기술과 함께 플러그인을 사용하면 표준을 준수하기 위해 디스크 간 백업 복제를 수행할 수도 있습니다.

SAP HANA 데이터베이스용 플러그인은 SnapMirror Active Sync(처음에는 SnapMirror Business Continuity[SM-BC]로 출시)를 지원하여 사이트 전체에 장애가 발생하더라도 비즈니스 서비스가 계속 운영될 수 있도록 하며, 보조 복사본을 사용하여 애플리케이션이 투명하게 장애 조치되도록 지원합니다. SnapMirror Active Sync를 사용하면 장애 조치를 트리거하는 데 수동 개입이나 추가 스크립팅이 필요하지 않습니다.

SAP HANA 데이터베이스용 SnapCenter 플러그인을 사용하여 수행할 수 있는 작업

사용자 환경에 SAP HANA 데이터베이스용 플러그인을 설치하면 SnapCenter 사용하여 SAP HANA 데이터베이스와 해당 리소스를 백업, 복원 및 복제할 수 있습니다. 해당 작업을 지원하는 작업도 수행할 수 있습니다.

- 데이터베이스를 추가합니다.
- 백업을 만듭니다.
- 백업에서 복원합니다.
- 백업을 복제합니다.
- 백업 작업을 예약합니다.
- 백업, 복원 및 복제 작업을 모니터링합니다.
- 백업, 복원 및 복제 작업에 대한 보고서를 확인합니다.

SAP HANA 데이터베이스용 SnapCenter 플러그인 기능

SnapCenter 플러그인 애플리케이션과 스토리지 시스템의 NetApp 기술과 통합됩니다. SAP HANA 데이터베이스 플러그인을 사용하려면 SnapCenter 그래픽 사용자 인터페이스를 사용합니다.

- 통합된 그래픽 사용자 인터페이스

SnapCenter 인터페이스는 플러그인과 환경 전반에 걸쳐 표준화와 일관성을 제공합니다. SnapCenter 인터페이스를 사용하면 플러그인 전반에 걸쳐 일관된 백업, 복원 및 복제 작업을 완료하고, 중앙 집중식 보고를 사용하고, 한눈에 볼 수 있는 대시보드 보기를 사용하고, 역할 기반 액세스 제어(RBAC)를 설정하고, 모든 플러그인에서 작업을 모니터링할 수 있습니다.

- 자동화된 중앙 관리

백업 작업을 예약하고, 정책 기반 백업 보존을 구성하고, 복원 작업을 수행할 수 있습니다. SnapCenter 구성하여 이메일 알림을 보내 환경을 사전에 모니터링할 수도 있습니다.

- 비중단 **NetApp** 스냅샷 복사 기술

SnapCenter SAP HANA 데이터베이스용 플러그인과 함께 NetApp Snapshot 기술을 사용하여 리소스를 백업합니다.

SAP HANA 데이터베이스 플러그인을 사용하면 다음과 같은 이점도 얻을 수 있습니다.

- 백업, 복원 및 복제 워크플로 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임

또한, 권한이 있는 SnapCenter 사용자에게 애플리케이션 수준 권한이 부여되도록 자격 증명을 설정할 수도 있습니다.

- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 리소스의 공간 효율적 및 특정 시점 복사본 생성

복제본을 생성하려는 스토리지 시스템에 FlexClone 라이선스가 필요합니다.

- 백업 생성의 일부로 ONTAP의 일관성 그룹(CG) 스냅샷 기능을 지원합니다.
- 여러 리소스 호스트에서 동시에 여러 백업을 실행할 수 있는 기능

단일 작업에서 단일 호스트의 리소스가 동일한 볼륨을 공유하는 경우 스냅샷이 통합됩니다.

- 외부 명령을 사용하여 스냅샷을 생성하는 기능.
- 파일 기반 백업 지원.
- XFS 파일 시스템에서 Linux LVM을 지원합니다.

SAP HANA 데이터베이스용 **SnapCenter** 플러그인에서 지원하는 스토리지 유형

SnapCenter 물리적 머신과 가상 머신(VM) 모두에서 다양한 스토리지 유형을 지원합니다. SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치하기 전에 스토리지 유형에 대한 지원을 확인해야 합니다.

기계	저장 유형
물리적 서버	• FC 연결 LUN • iSCSI로 연결된 LUN • NFS 연결 볼륨
VMware ESXi	• FC 또는 iSCSI ESXi HBA로 연결된 RDM LUN 호스트 버스 어댑터(HBA) 스캐닝은 SnapCenter 호스트에 있는 모든 호스트 버스 어댑터를 스캔하기 때문에 완료하는 데 오랜 시간이 걸릴 수 있습니다. _opt/ NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config_에 있는 LinuxConfig.pm 파일을 편집하여 SCSI_HOSTS_OPTIMIZED_RESCAN 매개변수 값을 1로 설정하면 HBA_DRIVER_NAMES에 나열된 HBA만 다시 스캔합니다. • iSCSI 이니시에이터에 의해 게스트 시스템에 직접 연결된 iSCSI LUN • NFS 데이터 저장소의 VMDK • VMFS에 VMDK가 생성됨 • 게스트 시스템에 직접 연결된 NFS 볼륨 • NFS와 SAN 모두에 있는 vVol 데이터 저장소 vVol 데이터스토어는 VMware vSphere용 ONTAP 도구를 사용해서만 프로비저닝할 수 있습니다.

SAP HANA 플러그인에 필요한 최소 ONTAP 권한

데이터 보호를 위해 사용하는 SnapCenter 플러그인에 따라 필요한 최소 ONTAP 권한은 다음과 같습니다.

- 모든 액세스 명령: ONTAP 9.12.1 이상에 필요한 최소 권한
 - 이벤트 생성-자동 지원-로그
 - 작업 이력 표시
 - 작업 중지
 - 룬
 - lun 생성
 - lun 생성
 - lun 생성
 - lun 삭제

- lun igroup 추가
- lun igroup 생성
- lun igroup 삭제
- lun igroup 이름 바꾸기
- lun igroup 이름 바꾸기
- 룬 아이그룹 쇼
- lun 매핑 add-reporting-nodes
- lun 매핑 생성
- LUN 매핑 삭제
- LUN 매핑 제거-보고-노드
- lun 매핑 쇼
- lun 수정
- lun 이동량
- lun 오프라인
- lun 온라인
- lun 지속적 예약 지우기
- lun 크기 조정
- lun 시리얼
- 룬 쇼
- 스냅미러 정책 추가 규칙
- 스냅미러 정책 수정 규칙
- 스냅미러 정책 제거 규칙
- 스냅미러 정책 보기
- 스냅미러 복원
- 스냅미러 쇼
- 스냅미러 쇼 히스토리
- 스냅미러 업데이트
- 스냅미러 업데이트-is-세트
- 스냅미러 목록-대상
- 버전
- 볼륨 복제 생성
- 볼륨 클론 쇼
- 볼륨 복제 분할 시작
- 볼륨 클론 분할 정지

- 볼륨 생성
- 볼륨 파괴
- 볼륨 파일 복제 생성
- 볼륨 파일 show-disk-usage
- 볼륨 오프라인
- 온라인 볼륨
- 볼륨 수정
- 볼륨 qtree 생성
- 볼륨 qtree 삭제
- 볼륨 qtree 수정
- 볼륨 qtree 쇼
- 볼륨 제한
- 볼륨 쇼
- 볼륨 스냅샷 생성
- 볼륨 스냅샷 삭제
- 볼륨 스냅샷 수정
- 볼륨 스냅샷 수정-스냅락-만료-시간
- 볼륨 스냅샷 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- vservers cifs
- vservers cifs 공유 생성
- vservers cifs 공유 삭제
- vservers cifs 새도우 카피 쇼
- vservers cifs 공유 표시
- vservers cifs 쇼
- vservers 내보내기 정책
- vservers 내보내기 정책 생성
- vservers 내보내기 정책 삭제
- vservers 내보내기 정책 규칙 생성
- vservers 내보내기 정책 규칙 표시
- vservers 내보내기 정책 표시

- v서버 iSCSI
- vservers iscsi 연결 표시
- vservers 쇼
- 읽기 전용 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
 - 네트워크 인터페이스
 - 네트워크 인터페이스 표시
 - v서버

SAP HANA 데이터베이스를 위한 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비

ONTAP SnapMirror 기술과 함께 SnapCenter 플러그인을 사용하면 다른 볼륨에 백업 세트의 미러 사본을 생성할 수 있으며, ONTAP SnapVault 기술과 함께 사용하면 표준 준수 및 기타 거버넌스 관련 목적으로 디스크 간 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 구성하고 해당 관계를 초기화해야 합니다.

SnapCenter 스냅샷 작업을 완료한 후 SnapMirror와 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행됩니다. SnapMirror 활성 동기화를 사용하는 경우 SnapMirror 활성 동기화와 비동기 관계 모두에 기본 SnapMirror 또는 SnapVault 일정을 사용하세요.



NetApp SnapManager 제품을 통해 SnapCenter에 접속했고 구성된 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 기본 저장소(소스 볼륨)의 데이터를 보조 저장소(대상 볼륨)로 복제합니다. 관계를 초기화하면 ONTAP 소스 볼륨에서 참조되는 데이터 블록을 대상 볼륨으로 전송합니다.



SnapCenter SnapMirror와 SnapVault 볼륨 간의 계단식 관계(**Primary > Mirror > Vault**)를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter 버전에 따라 유연한 SnapMirror 관계 관리를 지원합니다. 버전에 따라 유연한 SnapMirror 관계와 이를 설정하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["ONTAP 문서"](#).

SAP HANA 데이터베이스를 위한 백업 전략

SAP HANA 데이터베이스에 대한 백업 전략 정의

백업 작업을 생성하기 전에 백업 전략을 정의하면 리소스를 성공적으로 복원하거나 복제하는 데 필요한 백업을 확보하는 데 도움이 됩니다. 백업 전략은 주로 서비스 수준 계약(SLA), 복구 시간 목표(RTO), 복구 지점 목표(RPO)에 따라 결정됩니다.

이 작업에 관하여

SLA는 기대되는 서비스 수준을 정의하고 서비스의 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RTO는 서비스가 중단된 후 비즈니스 프로세스를 복구해야 하는 시간입니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 기간에 대한 전략을 정의합니다. SLA, RTO, RPO는 데이터 보호 전략에 기여합니다.

단계

1. 리소스를 백업해야 하는 시기를 결정하세요.
2. 필요한 백업 작업의 수를 결정합니다.
3. 백업의 이름을 어떻게 지을지 결정하세요.
4. 데이터베이스의 애플리케이션 일관성 스냅샷을 백업하기 위해 스냅샷 복사 기반 정책을 생성할지 여부를 결정합니다.
5. 데이터베이스의 무결성을 검증할지 여부를 결정합니다.
6. 복제를 위해 NetApp SnapMirror 기술을 사용할지, 장기 보존을 위해 NetApp SnapVault 기술을 사용할지 결정하세요.
7. 소스 스토리지 시스템과 SnapMirror 대상의 스냅샷 보존 기간을 결정합니다.
8. 백업 작업 전이나 후에 명령을 실행할지 여부를 결정하고 사전 스크립트나 사후 스크립트를 제공합니다.

Linux 호스트에서 리소스 자동 검색

리소스는 SnapCenter 에서 관리하는 Linux 호스트의 SAP HANA 데이터베이스와 비데이터 볼륨입니다. SAP HANA 데이터베이스 플러그인용 SnapCenter 플러그인을 설치하면 해당 Linux 호스트의 SAP HANA 데이터베이스가 자동으로 검색되어 리소스 페이지에 표시됩니다.

다음 SAP HANA 리소스에 대해 자동 검색이 지원됩니다.

- 단일 컨테이너

플러그인을 설치하거나 업그레이드한 후, 중앙 호스트 플러그인에 있는 단일 컨테이너 리소스는 수동으로 추가된 리소스로 계속 유지됩니다.

플러그인을 설치하거나 업그레이드한 후 SAP HANA 데이터베이스는 SnapCenter 에 직접 등록된 SAP HANA Linux 호스트에서만 자동으로 검색됩니다.

- 멀티테넌트 데이터베이스 컨테이너(MDC)

플러그인을 설치하거나 업그레이드한 후, 중앙 호스트 플러그인에 있는 MDC 리소스는 수동으로 추가된 리소스로 계속 유지됩니다.

SnapCenter 4.3으로 업그레이드한 후에도 중앙 호스트 플러그인에 MDC 리소스를 수동으로 추가해야 합니다.

SnapCenter 에 직접 등록된 SAP HANA Linux 호스트의 경우 플러그인을 설치하거나 업그레이드하면 호스트의 리소스가 자동으로 검색됩니다. 플러그인을 업그레이드한 후, 플러그인 호스트에 있는 모든 MDC 리소스에 대해 다른 GUID 형식을 가진 또 다른 MDC 리소스가 자동으로 검색되어 SnapCenter 에 등록됩니다. 새로운 리소스는 잠금 상태가 됩니다.

예를 들어 SnapCenter 4.2에서 E90 MDC 리소스가 플러그인 호스트에 위치하고 수동으로 등록된 경우 SnapCenter 4.3으로 업그레이드하면 다른 GUID를 가진 또 다른 E90 MDC 리소스가 검색되어 SnapCenter 에 등록됩니다.

다음 구성에서는 자동 검색이 지원되지 않습니다.

- RDM 및 VMDK 레이아웃



위의 리소스가 발견되는 경우, 해당 리소스에서는 데이터 보호 작업이 지원되지 않습니다.

- HANA 다중 호스트 구성
- 동일한 호스트에 여러 인스턴스가 있음
- 다중 계층 확장 HANA 시스템 복제
- 시스템 복제 모드의 계단식 복제 환경

지원되는 백업 유형

백업 유형은 생성하려는 백업 유형을 지정합니다. SnapCenter SAP HANA 데이터베이스에 대한 파일 기반 백업 및 스냅샷 복사 기반 백업 유형을 지원합니다.

파일 기반 백업

파일 기반 백업은 데이터베이스의 무결성을 확인합니다. 파일 기반 백업 작업이 특정 간격으로 실행되도록 예약할 수 있습니다. 활성 테넌트만 백업됩니다. SnapCenter 에서 파일 기반 백업을 복원하고 복제할 수 없습니다.

스냅샷 복사 기반 백업

스냅샷 복사 기반 백업은 NetApp 스냅샷 기술을 활용하여 SAP HANA 데이터베이스가 있는 볼륨의 온라인, 읽기 전용 복사본을 만듭니다.

SAP HANA 데이터베이스용 SnapCenter 플러그인이 일관성 그룹 스냅샷을 사용하는 방법

플러그인을 사용하면 리소스 그룹에 대한 일관성 그룹 스냅샷을 만들 수 있습니다. 일관성 그룹은 여러 볼륨을 수용하여 하나의 엔티티로 관리할 수 있는 컨테이너입니다. 일관성 그룹은 여러 볼륨의 동시 스냅샷으로, 볼륨 그룹의 일관된 복사본을 제공합니다.

또한 스토리지 컨트롤러가 스냅샷을 일관되게 그룹화하는 데 걸리는 대기 시간을 지정할 수도 있습니다. 이용 가능한 대기 시간 옵션은 긴급, 보통, *느긋함*입니다. 일관된 그룹 스냅샷 작업 중에 WAFL(Write Anywhere File Layout) 동기화를 활성화하거나 비활성화할 수도 있습니다. WAFL 동기화는 일관성 그룹 스냅샷의 성능을 향상시킵니다.

SnapCenter 로그 및 데이터 백업의 정리 작업을 관리하는 방법

SnapCenter 스토리지 시스템 및 파일 시스템 수준과 SAP HANA 백업 카탈로그 내에서 로그 및 데이터 백업의 정리 작업을 관리합니다.

기본 또는 보조 저장소의 스냅샷과 SAP HANA 카탈로그의 해당 항목은 보존 설정에 따라 삭제됩니다. SAP HANA 카탈로그 항목은 백업 및 리소스 그룹 삭제 중에도 삭제됩니다.

SAP HANA 데이터베이스 백업 일정을 결정하기 위한 고려 사항

백업 일정을 결정하는 가장 중요한 요소는 리소스의 변화율입니다. 자주 사용되는 리소스는 매시간 백업하고, 거의 사용되지 않는 리소스는 하루에 한 번 백업할 수도 있습니다. 기타 요소로는 조직에 대한 리소스의 중요성, 서비스 수준 계약(SLA), 복구 지점 목표(RPO) 등이 있습니다.

백업 일정은 다음과 같이 두 부분으로 구성됩니다.

- 백업 빈도(백업을 수행할 빈도)

일부 플러그인의 경우 일정 유형이라고도 하는 백업 빈도는 정책 구성의 일부입니다. 예를 들어, 백업 빈도를 매시간, 매일, 매주 또는 매월로 구성할 수 있습니다.

- 백업 일정(백업을 수행할 정확한 시기)

백업 일정은 리소스 또는 리소스 그룹 구성의 일부입니다. 예를 들어, 주간 백업을 위해 구성된 정책이 있는 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 일정을 구성할 수 있습니다.

SAP HANA 데이터베이스에 필요한 백업 작업 수

필요한 백업 작업 수를 결정하는 요소에는 리소스 크기, 사용된 볼륨 수, 리소스 변경률, 서비스 수준 계약(SLA) 등이 있습니다.

SAP HANA 데이터베이스용 플러그인에 대한 백업 명명 규칙

기본 스냅샷 명명 규칙을 사용하거나 사용자 지정 명명 규칙을 사용할 수 있습니다. 기본 백업 명명 규칙은 스냅샷 이름에 타임스탬프를 추가하여 복사본이 생성된 시기를 식별하는 데 도움이 됩니다.

스냅샷은 다음과 같은 기본 명명 규칙을 사용합니다.

resourcegroupname_hostname_timestamp

다음 예와 같이 논리적으로 백업 리소스 그룹의 이름을 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예에서 구문 요소는 다음과 같은 의미를 갖습니다.

- _dts1_은 리소스 그룹 이름입니다.
- _mach1x88_은 호스트 이름입니다.
- _03-12-2015_23.17.26_은 날짜와 타임스탬프입니다.

또는, *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택하여 리소스나 리소스 그룹을 보호하는 동안 스냅샷 이름 형식을 지정할 수 있습니다. 예를 들어, customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname입니다. 기본적으로 타임스탬프 접미사는 스냅샷 이름에 추가됩니다.

SAP HANA 데이터베이스의 복원 및 복구 전략

SAP HANA 리소스에 대한 복원 및 복구 전략 정의

데이터베이스를 복원하고 복구하기 전에 전략을 정의해야 복원 및 복구 작업을 성공적으로 수행할 수 있습니다.

단계

1. 수동으로 추가된 SAP HANA 리소스에 대해 지원되는 복원 전략을 확인합니다.
2. 자동 검색된 SAP HANA 데이터베이스에 지원되는 복원 전략을 확인합니다.
3. 수행할 복구 작업 유형을 결정합니다.

수동으로 추가된 **SAP HANA** 리소스에 지원되는 복원 전략 유형

SnapCenter 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다. 수동으로 추가된 SAP HANA 리소스에 대한 복원 전략에는 두 가지 유형이 있습니다. 수동으로 추가한 SAP HANA 리소스는 복구할 수 없습니다.



수동으로 추가한 SAP HANA 리소스는 복구할 수 없습니다.

리소스 복구 완료

- 리소스의 모든 볼륨, Qtree 및 LUN을 복원합니다.



리소스에 볼륨이나 Q트리가 포함되어 있는 경우 해당 볼륨이나 Q트리에서 복원을 위해 선택한 스냅샷 이후에 생성된 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 동일한 볼륨이나 Q트리에 다른 리소스가 호스팅되는 경우 해당 리소스도 삭제됩니다.

파일 수준 복원

- 볼륨, Qtree 또는 디렉토리에서 파일을 복원합니다.
- 선택된 LUN만 복원합니다.

자동으로 검색된 **SAP HANA** 데이터베이스에 지원되는 복원 전략 유형

SnapCenter 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다. 자동으로 검색된 SAP HANA 데이터베이스에는 두 가지 유형의 복원 전략이 있습니다.

리소스 복구 완료

- 리소스의 모든 볼륨, Qtree 및 LUN을 복원합니다.
 - 전체 볼륨을 복원하려면 볼륨 되돌리기 옵션을 선택해야 합니다.



리소스에 볼륨이나 Q트리가 포함되어 있는 경우 해당 볼륨이나 Q트리에서 복원을 위해 선택한 스냅샷 이후에 생성된 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 동일한 볼륨이나 Q트리에 다른 리소스가 호스팅되는 경우 해당 리소스도 삭제됩니다.

테넌트 데이터베이스

- 테넌트 데이터베이스를 복원합니다.

테넌트 데이터베이스 옵션을 선택한 경우 SnapCenter 외부의 HANA 스튜디오 또는 HANA 복구 스크립트를 사용하여 복구 작업을 수행해야 합니다.

자동 검색된 **SAP HANA** 데이터베이스에 대한 복원 작업 유형

SnapCenter 자동으로 검색된 SAP HANA 데이터베이스에 대해 볼륨 기반 SnapRestore (VBSR), 단일 파일 SnapRestore 및 연결 및 복사 복원 유형을 지원합니다.

볼륨 기반 **SnapRestore (VBSR)**는 다음 시나리오에 대해 **NFS** 환경에서 수행됩니다.

- 복원을 위해 선택된 백업이 SnapCenter 4.3 이전 릴리스에서 수행되고 전체 리소스 옵션이 선택된 경우에만 해당
- SnapCenter 4.3에서 복원을 위해 선택된 백업이 수행되고 볼륨 되돌리기 옵션이 선택된 경우

단일 파일 **SnapRestore** 다음 시나리오에 대해 **NFS** 환경에서 수행됩니다.

- SnapCenter 4.3에서 복원을 위해 선택된 백업이 수행되고 전체 리소스 옵션만 선택된 경우
- 다중 테넌트 데이터베이스 컨테이너(MDC)의 경우 복원을 위해 선택된 백업이 SnapCenter 4.3에서 수행되고 테넌트 데이터베이스 옵션이 선택된 경우
- 선택한 백업이 SnapMirror 또는 SnapVault 보조 위치에서 시작되고 전체 리소스 옵션이 선택된 경우

단일 파일 **SnapRestore** 다음 시나리오에 대해 **SAN** 환경에서 수행됩니다.

- SnapCenter 4.3 이전 릴리스에서 백업이 수행되고 전체 리소스 옵션이 선택된 경우에만
- SnapCenter 4.3에서 백업이 수행되고 전체 리소스 옵션이 선택된 경우에만
- SnapMirror 또는 SnapVault 보조 위치에서 백업을 선택하고 전체 리소스 옵션을 선택한 경우

연결 및 복사 기반 복원은 다음 시나리오에 대해 **SAN** 환경에서 수행됩니다.

- MDC의 경우 복원을 위해 선택된 백업이 SnapCenter 4.3에서 수행되고 테넌트 데이터베이스 옵션이 선택된 경우



전체 리소스, 볼륨 되돌리기 및 테넌트 데이터베이스 옵션은 복원 범위 페이지에서 사용할 수 있습니다.

SAP HANA 데이터베이스에 지원되는 복구 작업 유형

SnapCenter 사용하면 SAP HANA 데이터베이스에 대해 다양한 유형의 복구 작업을 수행할 수 있습니다.

- 데이터베이스를 최신 상태로 복구합니다.
- 특정 시점까지 데이터베이스를 복구합니다.

복구 날짜와 시간을 지정해야 합니다.

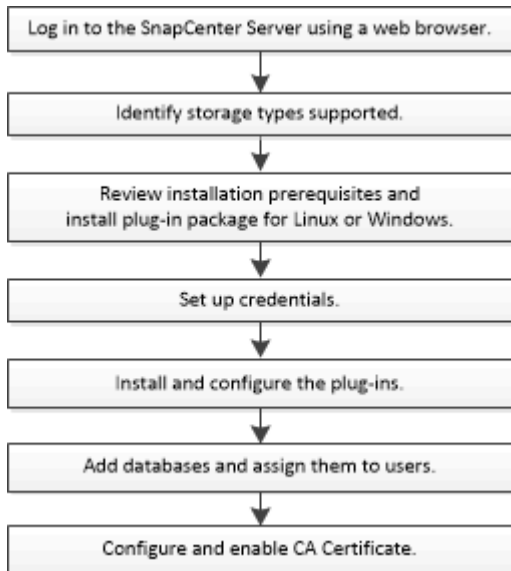
- 특정 데이터 백업까지 데이터베이스를 복구합니다.

SnapCenter SAP HANA 데이터베이스에 대해 복구 불가 옵션도 제공합니다.

SAP HANA 데이터베이스용 SnapCenter 플러그인 설치 준비

SAP HANA 데이터베이스용 SnapCenter 플러그인 설치 워크플로

SAP HANA 데이터베이스를 보호하려면 SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치하고 호스트를 추가하기 위한 전제 조건

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 충족해야 합니다. SAP HANA 데이터베이스용 SnapCenter 플러그인은 Windows와 Linux 환경에서 모두 사용할 수 있습니다.

- 호스트에 Java 11을 설치했어야 합니다.



IBM Java는 Windows 및 Linux 호스트에서 지원되지 않습니다.

- 호스트에 SAP HANA 데이터베이스 대화형 터미널(HDBSQL 클라이언트)을 설치해야 합니다.
- Windows의 경우 플러그인 생성 서비스는 “LocalSystem” Windows 사용자를 사용하여 실행해야 합니다. 이는 SAP HANA Database용 플러그인이 도메인 관리자로 설치된 경우의 기본 동작입니다.
- Windows의 경우 사용자 저장소 키는 SYSTEM 사용자로 생성되어야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에 속하는 경우 호스트에서 UAC를 비활성화해야 합니다. Microsoft Windows용 SnapCenter 플러그인은 기본적으로 Windows 호스트의 SAP HANA 플러그인과 함께 배포됩니다.
- Linux 호스트의 경우 HDB 보안 사용자 저장소 키는 HDBSQL OS 사용자로 액세스됩니다.
- SnapCenter 서버는 SAP HANA 데이터베이스 호스트용 플러그인의 8145 또는 사용자 지정 포트에 액세스할 수 있어야 합니다.

Windows 호스트

- 원격 호스트에 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 도메인 사용자가 있어야 합니다.

- Windows 호스트에 SAP HANA 데이터베이스용 플러그인을 설치하는 동안 Microsoft Windows용 SnapCenter 플러그인이 자동으로 설치됩니다.
- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.
- Windows 호스트에 Java 11을 설치했어야 합니다.

"모든 운영 체제용 JAVA 다운로드"

"NetApp 상호 운용성 매트릭스 도구"

리눅스 호스트

- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.
- Linux 호스트에 Java 11을 설치했어야 합니다.

"모든 운영 체제용 JAVA 다운로드"

"NetApp 상호 운용성 매트릭스 도구"

- Linux 호스트에서 실행되는 SAP HANA 데이터베이스의 경우 SAP HANA 데이터베이스용 플러그인을 설치하는 동안 UNIX용 SnapCenter 플러그인이 자동으로 설치됩니다.
- 플러그인 설치를 위해 기본 셸로 `*bash*`를 사용해야 합니다.

보충 명령

SAP HANA용 SnapCenter 플러그인에서 보충 명령을 실행하려면 `allowed_commands.config` 파일에 해당 명령을 포함해야 합니다.

- Windows 호스트의 기본 위치: `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux 호스트의 기본 위치: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`

플러그인 호스트에서 추가 명령을 허용하려면 편집기에서 `allowed_commands.config` 파일을 엽니다. 각 명령을 별도의 줄에 입력하세요. 명령은 대소문자를 구분하지 않습니다. 완전히 정규화된 경로 이름을 지정하고, 경로 이름에 공백이 포함된 경우 따옴표(")로 묶으세요.

예를 들어:

명령어: `mount`

명령어: `umount`

명령: `"C:\Program Files\ NetApp\SnapCreator commands\sdcli.exe"`

명령어: `myscript.bat`

`allowed_commands.config` 파일이 없으면 명령이나 스크립트 실행이 차단되고 다음 오류와 함께 워크플로가 실패합니다.

"[/mnt/mount -a] 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여합니다."

_allowed_commands.config_에 명령이나 스크립트가 없으면 명령이나 스크립트 실행이 차단되고 다음 오류와 함께 워크플로가 실패합니다.

"[/mnt/mount -a] 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여합니다."



모든 명령을 허용하려면 와일드카드 항목(*)을 사용해서는 안 됩니다.

Linux 호스트에 대한 루트가 아닌 사용자에게 대한 **sudo** 권한 구성

SnapCenter 2.0 및 이후 릴리스에서는 루트가 아닌 사용자로 Linux용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 루트가 아닌 사용자로 실행됩니다. 루트가 아닌 사용자에게 여러 경로에 대한 액세스 권한을 제공하려면 sudo 권한을 구성해야 합니다.

필요한 것

- Sudo 버전 1.8.7 이상.
- umask가 0027인 경우, java 폴더와 그 안에 있는 모든 파일에 555 권한이 있어야 합니다. 그렇지 않으면 플러그인 설치가 실패할 수 있습니다.
- 루트가 아닌 사용자의 경우 루트가 아닌 사용자의 이름과 사용자 그룹이 동일해야 합니다.
- `/etc/ssh/sshd_config` 파일을 편집하여 메시지 인증 코드 알고리즘(MAC hmac-sha2-256 및 MAC hmac-sha2-512)을 구성합니다.

구성 파일을 업데이트한 후 sshd 서비스를 다시 시작합니다.

예:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

이 작업에 관하여

루트가 아닌 사용자에게 다음 경로에 대한 액세스를 제공하려면 sudo 권한을 구성해야 합니다.

- `/home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/custom_location/ NetApp/snapcenter/spl/설치/플러그인/제거`
- `/custom_location/ NetApp/snapcenter/spl/bin/spl`

단계

1. Linux용 SnapCenter 플러그인 패키지를 설치하려는 Linux 호스트에 로그인합니다.
2. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 줄을 추가합니다.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,  
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,  
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc  
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/Linux_Prechecks.sh  
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config  
_Check.sh  
Cmnd_Alias SCCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/bin/sc_command_executor  
Cmnd_Alias SCCMDEXECUTOR =checksum_value==  
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor  
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,  
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD  
Defaults: LINUX_USER env_keep += "IATEMPDIR"  
Defaults: LINUX_USER env_keep += "JAVA_HOME"  
Defaults: LINUX_USER !visiblepw  
Defaults: LINUX_USER !requiretty
```



RAC 설정을 사용하는 경우 허용되는 다른 명령과 함께 다음을 /etc/sudoers 파일에 추가해야 합니다. '/<crs_home>/bin/olsnodes'

*crs_home*의 값은 */etc/oracle/olr.loc* 파일에서 얻을 수 있습니다.

*_LINUX_USER*는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

*_checksum_value*는 **sc_unix_plugins_checksum.txt** 파일에서 얻을 수 있습니다. 이 파일의 위치는 다음과 같습니다.

- SnapCenter Server가 Windows 호스트에 설치된 경우 *C:\ProgramData\NetApp\ SnapCenter \Package Repository\sc_unix_plugins_checksum.txt*.
- SnapCenter 서버가 Linux 호스트에 설치되어 있는 경우 */opt/ NetApp /snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt*.



이 예제는 귀하만의 데이터를 생성하기 위한 참고자료로만 사용해야 합니다.

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템

공간 요구 사항과 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	마이크로소프트 윈도우 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	• ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 • 파워셸 코어 7.4.2 • Java 11 Oracle Java 및 OpenJDK Java 11 Oracle Java 및 OpenJDK는 SAP HANA, IBM Db2, PostgreSQL, MySQL, NetApp 지원 플러그인 및 Windows 호스트에 설치할 수 있는 기타 사용자 정의 애플리케이션에만 필요합니다. 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .

Linux용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 및 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	• 레드햇 엔터프라이즈 리눅스 • SUSE Linux Enterprise Server(SLES) 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .

목	요구 사항
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	Java 11 Oracle Java 및 OpenJDK JAVA를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties에 있는 JAVA_HOME 옵션이 올바른 JAVA 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다. 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .

SAP HANA 데이터베이스용 SnapCenter 플러그인에 대한 자격 증명 설정

SnapCenter SnapCenter 작업을 위해 사용자를 인증하기 위해 자격 증명을 사용합니다. SnapCenter 플러그인을 설치하기 위한 자격 증명과 데이터베이스나 Windows 파일 시스템에서 데이터 보호 작업을 수행하기 위한 추가 자격 증명을 만들어야 합니다.

이 작업에 관하여

- 리눅스 호스트

Linux 호스트에 플러그인을 설치하려면 자격 증명을 설정해야 합니다.

플러그인 프로세스를 설치하고 시작하려면 루트 사용자 또는 sudo 권한이 있는 루트가 아닌 사용자의 자격 증명을 설정해야 합니다.

모범 사례: 호스트를 배포하고 플러그인을 설치한 후에도 Linux에 대한 자격 증명을 생성할 수 있지만, 가장 좋은 방법은 호스트를 배포하고 플러그인을 설치하기 전에 SVM을 추가한 후에 자격 증명을 생성하는 것입니다.

- Windows 호스트

플러그인을 설치하기 전에 Windows 자격 증명을 설정해야 합니다.

원격 호스트의 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정해야 합니다.

개별 리소스 그룹에 대한 자격 증명을 설정하고 사용자 이름에 전체 관리자 권한이 없는 경우 최소한 리소스 그룹 및 백업 권한을 사용자 이름에 할당해야 합니다.

단계

- 1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
- 2. 설정 페이지에서 *자격 증명*을 클릭합니다.
- 3. *새로 만들기*를 클릭합니다.

Credential

Provide information for the Credential you want to add

Credential Name

Name

Username

Username

Password

Password

Authentication

Linux

☐ Use sudo privileges

Cancel

OK

- 4. 자격 증명 페이지에서 자격 증명을 구성하는 데 필요한 정보를 지정합니다.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.

이 분야에서는...	이렇게 하세요...
사용자 이름	인증에 사용할 사용자 이름과 비밀번호를 입력하세요. - 도메인 관리자 또는 관리자 그룹의 모든 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹 구성원을 지정하세요. 사용자 이름 필드에 사용할 수 있는 형식은 다음과 같습니다. ◦ <i>NetBIOS</i> 사용자 이름 ◦ 도메인 <i>FQDN</i> 사용자 이름 - 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우, SnapCenter 플러그인을 설치할 시스템에 기본 제공되는 로컬 관리자를 지정하십시오. 사용자 계정에 승격된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우, 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다. <i>UserName</i> 비밀번호에 큰따옴표(")나 백틱(`)을 사용하지 마세요. 비밀번호에 '<' 기호와 '!' 기호를 함께 사용하면 안 됩니다. 예를 들어, <i>lessthan<!10</i>, <i>lessthan10<!</i>, <i>backtick`12</i>.
비밀번호	인증에 사용되는 비밀번호를 입력하세요.
인증 모드	사용할 인증 모드를 선택하세요.
sudo 권한을 사용하세요	루트가 아닌 사용자에게 자격 증명을 생성하는 경우 sudo 권한 사용 확인란을 선택합니다.  Linux 사용자에게만 적용됩니다.

5. *확인*을 클릭합니다.

자격 증명 설정을 마친 후 사용자 및 액세스 페이지에서 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

Windows Server 2016 이상에서 gMSA 구성

Windows Server 2016 이상에서는 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 관리 서비스 계정(gMSA)을 만들 수 있습니다.

시작하기 전에

- Windows Server 2016 이상 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2016 이상 호스트가 있어야 합니다.

단계

1. gMSA의 각 개체에 대해 고유한 비밀번호를 생성하려면 KDS 루트 키를 만듭니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 다음 명령을 실행합니다. Add-KDSRootKey -EffectiveImmediately
3. gMSA를 만들고 구성하세요.
 - a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
domainName\accountName$  
.. 그룹에 컴퓨터 객체를 추가합니다.  
.. 방금 만든 사용자 그룹을 사용하여 gMSA를 만듭니다.
```

예를 들어,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 달리다 `Get-ADServiceAccount` 서비스 계정을 확인하는 명령입니다.
```

4. 호스트에서 gMSA를 구성하세요.
 - a. gMSA 계정을 사용하려는 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.
이렇게 하려면 PowerShell에서 다음 명령을 실행하세요.

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

a. 호스트를 다시 시작합니다.

b. PowerShell 명령 프롬프트에서 다음 명령을 실행하여 호스트에 gMSA를 설치합니다. `Install-AdServiceAccount <gMSA>`

c. 다음 명령을 실행하여 gMSA 계정을 확인하세요. `Test-AdServiceAccount <gMSA>`

5. 호스트에서 구성된 gMSA에 관리 권한을 할당합니다.

6. SnapCenter 서버에서 구성된 gMSA 계정을 지정하여 Windows 호스트를 추가합니다.

SnapCenter Server는 호스트에 선택된 플러그인을 설치하고, 플러그인 설치 중에 지정된 gMSA가 서비스 로그인 계정으로 사용됩니다.

SAP HANA 데이터베이스용 SnapCenter 플러그인 설치

원격 호스트에 호스트를 추가하고 플러그인 패키지를 설치합니다.

SnapCenter 호스트 추가 페이지를 사용하여 호스트를 추가한 다음 플러그인 패키지를 설치해야 합니다. 플러그인은 원격 호스트에 자동으로 설치됩니다. 개별 호스트나 클러스터에 대해 호스트를 추가하고 플러그인 패키지를 설치할 수 있습니다.

시작하기 전에

- SnapCenter 서버 호스트의 운영 체제가 Windows 2019이고 플러그인 호스트의 운영 체제가 Windows 2022인 경우 다음을 수행해야 합니다.
 - Windows Server 2019(OS 빌드 17763.5936) 이상으로 업그레이드하세요.
 - Windows Server 2022(OS 빌드 20348.2402) 이상으로 업그레이드하세요.
- SnapCenter 관리자 역할과 같이 플러그인 설치 및 제거 권한이 있는 역할에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.

- 메시지 대기열 서비스가 실행 중인지 확인해야 합니다.
- 관리 문서에는 호스트 관리에 대한 정보가 포함되어 있습니다.
- 그룹 관리 서비스 계정(gMSA)을 사용하는 경우 관리자 권한으로 gMSA를 구성해야 합니다.

"SAP HANA를 위해 Windows Server 2016 이상에서 그룹 관리 서비스 계정 구성"

이 작업에 관하여

- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.
- SAP HANA 시스템 복제가 기본 및 보조 시스템 모두에서 리소스를 검색하려면 root 또는 sudo 사용자를 사용하여 기본 및 보조 시스템을 모두 추가하는 것이 좋습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 상단에 관리되는 호스트 탭이 선택되어 있는지 확인하세요.
3. *추가*를 클릭하세요.
4. 호스트 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
호스트 유형	호스트 유형을 선택하세요: • Windows • 리눅스  SAP HANA용 플러그인은 HDBSQL 클라이언트 호스트에 설치되며, 이 호스트는 Windows 시스템이나 Linux 시스템에 있을 수 있습니다.
호스트 이름	통신 호스트 이름을 입력하세요. 호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하세요. SnapCenter DNS의 적절한 구성에 달려 있습니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다. 이 호스트에서 HDBSQL 클라이언트와 HDBUserStore를 구성해야 합니다.

이 분야에서는...	이렇게 하세요...
신임장	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성하세요. 자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하세요. 제공한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다.  자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

6. (선택 사항) *추가 옵션*을 클릭합니다.

이 분야에서는...	이렇게 하세요...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정하세요. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트 번호로 표시됩니다.  플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.
설치 경로	SAP HANA용 플러그인은 HDBSQL 클라이언트 호스트에 설치되며, 이 호스트는 Windows 시스템이나 Linux 시스템에 있을 수 있습니다. - Windows용 SnapCenter 플러그인 패키지의 경우 기본 경로는 C:\Program Files\ NetApp\ SnapCenter 입니다. 선택적으로 경로를 사용자 정의할 수 있습니다. - Linux용 SnapCenter 플러그인 패키지의 경우 기본 경로는 /opt/ NetApp/snapcenter입니다. 선택적으로 경로를 사용자 정의할 수 있습니다.
사전 설치 확인 건너뛰기	플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택하세요.

이 분야에서는...	이렇게 하세요...
플러그인 서비스를 실행하려면 그룹 관리 서비스 계정(gMSA)을 사용하세요.	Windows 호스트의 경우 플러그인 서비스를 실행하기 위해 그룹 관리 서비스 계정(gMSA)을 사용하려면 이 확인란을 선택합니다.  다음 형식으로 gMSA 이름을 제공하세요: domainName\accountName\$.  gMSA는 Windows용 SnapCenter 플러그인 서비스에 대한 로그인 서비스 계정으로만 사용됩니다.

7. *제출*을 클릭하세요.

"사전 검사 건너뛰기" 확인란을 선택하지 않은 경우, 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 호스트의 유효성 검사가 수행됩니다. 디스크 공간, RAM, PowerShell 버전, .NET 버전, 위치(Windows 플러그인의 경우), Java 버전(Linux 플러그인의 경우)이 최소 요구 사항을 충족하는지 검증됩니다. 최소 요구 사항을 충족하지 못하면 해당 오류 또는 경고 메시지가 표시됩니다.

오류가 디스크 공간이나 RAM과 관련된 경우 C:\Program Files\NetApp\ SnapCenter WebApp에 있는 web.config 파일을 업데이트하여 기본값을 수정할 수 있습니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.



HA 설정에서 web.config 파일을 업데이트하는 경우 두 노드에서 모두 파일을 업데이트해야 합니다.

8. 호스트 유형이 Linux인 경우 지문을 확인한 다음 *확인 및 제출*을 클릭합니다.

클러스터 설정에서는 클러스터의 각 노드의 지문을 확인해야 합니다.



동일한 호스트가 이전에 SnapCenter 에 추가되었고 지문이 확인된 경우에도 지문 확인은 필수입니다.

9. 설치 진행 상황을 모니터링합니다.

설치 관련 로그 파일은 /custom_location/snapcenter/logs에 있습니다.

cmdlet을 사용하여 여러 원격 호스트에 **Linux** 또는 **Windows용 SnapCenter** 플러그인 패키지 설치

Install-SmHostPackage PowerShell cmdlet을 사용하여 Linux 또는 Windows용 SnapCenter 플러그인 패키지를 여러 호스트에 동시에 설치할 수 있습니다.

시작하기 전에

플러그인 패키지를 설치하려는 각 호스트에서 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter 에 로그인해야 합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 Open-SmConnection cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
3. Install-SmHostPackage cmdlet과 필요한 매개변수를 사용하여 여러 호스트에 플러그인을 설치합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려는 경우 `-skipprecheck` 옵션을 사용할 수 있습니다.

4. 원격 설치를 위한 자격 증명을 입력하세요.

명령줄 인터페이스를 사용하여 **Linux** 호스트에 **SAP HANA** 데이터베이스용 **SnapCenter** 플러그인을 설치합니다.

SnapCenter 사용자 인터페이스(UI)를 사용하여 SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치해야 합니다. 사용자 환경에서 SnapCenter UI에서 플러그인을 원격으로 설치할 수 없는 경우 명령줄 인터페이스(CLI)를 사용하여 콘솔 모드나 자동 모드로 SAP HANA 데이터베이스용 플러그인을 설치할 수 있습니다.

시작하기 전에

- HDBSQL 클라이언트가 있는 각 Linux 호스트에 SAP HANA 데이터베이스용 플러그인을 설치해야 합니다.
- SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치하는 Linux 호스트는 종속 소프트웨어, 데이터베이스 및 운영 체제 요구 사항을 충족해야 합니다.

상호 운용성 매트릭스 도구(IMT)에는 지원되는 구성에 대한 최신 정보가 포함되어 있습니다.

<https://imt.netapp.com/matrix/imt.jsp?components=121029;&solution=1259&isHWU&src=IMT>

- SAP HANA 데이터베이스용 SnapCenter 플러그인은 Linux용 SnapCenter 플러그인 패키지의 일부입니다. Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 Windows 호스트에 SnapCenter 이미 설치되어 있어야 합니다.

단계

1. Linux 설치 파일(SnapCenter)을 C:\ProgramData\ NetApp\ SnapCenter\Package Repository에서 SAP HANA 데이터베이스용 플러그인을 설치하려는 호스트로 복사합니다.

SnapCenter 서버가 설치된 호스트에서 이 경로에 액세스할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 복사한 디렉토리로 이동합니다.
3. 플러그인을 설치하세요: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin`
`-i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address`
`-DSERVER_HTTPS_PORT=port_number_for_server`
 - -DPORT는 SMCore HTTPS 통신 포트를 지정합니다.
 - -DSERVER_IP는 SnapCenter 서버 IP 주소를 지정합니다.
 - -DSERVER_HTTPS_PORT는 SnapCenter 서버 HTTPS 포트를 지정합니다.

- -DUSER_INSTALL_DIR은 Linux용 SnapCenter 플러그인 패키지를 설치할 디렉토리를 지정합니다.
- DINSTALL_LOG_NAME은 로그 파일의 이름을 지정합니다.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. /<설치 디렉토리>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties 파일을 편집한 다음 PLUGINS_ENABLED = hana:3.0 매개변수를 추가합니다.
5. Add-Smhost cmdlet과 필요한 매개변수를 사용하여 SnapCenter 서버에 호스트를 추가합니다.

명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 _Get-Help command_name_을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

SAP HANA 플러그인 설치 상태 모니터링

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행 상황을 모니터링할 수 있습니다. 설치가 완료되었는지 또는 문제가 있는지 확인하기 위해 설치 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 플러그인 설치 작업만 나열되도록 목록을 필터링하려면 다음을 수행합니다.
 - a. *필터*를 클릭하세요.
 - b. 선택 사항: 시작 날짜와 종료 날짜를 지정합니다.
 - c. 유형 드롭다운 메뉴에서 *플러그인 설치*를 선택합니다.
 - d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
 - e. *적용*을 클릭하세요.

4. 설치 작업을 선택하고 *세부정보*를 클릭하면 작업 세부정보를 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

CA 인증서 구성

CA 인증서 CSR 파일 생성

인증서 서명 요청(CSR)을 생성하고, 생성된 CSR을 사용하여 인증 기관(CA)에서 얻을 수 있는 인증서를 가져올 수 있습니다. 인증서에는 개인 키가 연결됩니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.



CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 정보는 다음을 참조하세요. "[CA 인증서 CSR 파일을 생성하는 방법](#)".



도메인(*.domain.company.com)이나 시스템(machine1.domain.company.com)에 대한 CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN)과 해당 호스트 이름을 CA 인증서에 명시해야 합니다. 인증서를 구매하기 전에 주체 대체 이름(SAN) 필드를 입력하여 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(*.domain.company.com)의 경우 인증서에는 해당 도메인의 모든 호스트 이름이 암묵적으로 포함됩니다.

CA 인증서 가져오기

Microsoft 관리 콘솔(MMC)을 사용하여 CA 인증서를 SnapCenter 서버와 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.
2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
3. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > *인증서*를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 버튼으로 클릭한 다음, 모든 작업 > *가져오기*를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
개인 키 가져오기	예 옵션을 선택하고 개인 키를 가져온 후 *다음*을 클릭합니다.
가져오기 파일 형식	변경하지 마세요. *다음*을 클릭하세요.

이 마법사 창에서...	다음을 수행하세요...
보안	내보낸 인증서에 사용할 새 비밀번호를 지정한 후 *다음*을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.



인증서 가져오기는 개인 키와 함께 제공되어야 합니다(지원되는 형식: *.pfx, *.p12, *.p7b).

7. "개인" 폴더에 대해서도 5단계를 반복합니다.

CA 인증서 지문을 받으세요

인증서 지문은 인증서를 식별하는 16진수 문자열입니다. 지문은 지문 알고리즘을 사용하여 인증서 내용으로부터 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.
 - a. 인증서를 두 번 클릭합니다.
 - b. 인증서 대화 상자에서 세부정보 탭을 클릭합니다.
 - c. 필드 목록을 스크롤하여 *지문*을 클릭하세요.
 - d. 상자에서 16진수 문자를 복사하세요.
 - e. 16진수 사이의 공백을 제거하세요.

예를 들어, 지문이 "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b"인 경우 공백을 제거하면 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.
 - a. 다음 명령을 실행하여 설치된 인증서의 지문을 나열하고 주체 이름으로 최근에 설치된 인증서를 식별합니다.

Get-ChildItem -경로 인증서:\LocalMachine\My

- b. 지문을 복사하세요.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스로 CA 인증서를 구성해야 합니다.

SnapCenter 서버와 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하는 기존 인증서 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

예를 들어:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스에
바인딩합니다.
```

```
> $cert = "<certificate thumbprint>"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port>_ certhash=$cert
appid="$guid"
```

예를 들어:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port>_ certhash=$cert
appid="$guid"
```

Linux 호스트에서 SnapCenter SAP HANA 플러그인 서비스에 대한 CA 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 `/opt/NetApp/snapcenter/scc/etc_`에 위치한 'keystore.jks' 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 CA 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 'KEYSTORE_PASS' 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

```
keytool -storepasswd -keystore keystore.jks
. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된
비밀번호와 동일하게 변경합니다.
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```


agent.properties 파일의 KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

3. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 있는 폴더로 이동합니다: /opt/ NetApp/snapcenter/scc/etc.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.
```



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 **CA** 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키스토어 /opt/ NetApp/snapcenter/scc/etc가 포함된 폴더로 이동합니다.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.

7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 agent.properties 파일의 KEYSTORE_PASS 키 값입니다.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자("*", ",", ")가 포함된 경우 별칭 이름을 간단한 이름으로 변경합니다.

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. agent.properties 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

8. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 'opt/ NetApp/snapcenter/scc/etc/crl'입니다.

단계

1. agent.properties 파일에서 기본 디렉토리를 CRL_PATH 키에 맞춰 수정하고 업데이트할 수 있습니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

Windows 호스트에서 **SnapCenter SAP HANA** 플러그인 서비스에 대한 **CA** 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_에 있는 _keystore.jks 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 **CA** 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 KEYSTORE_PASS 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

키툴 -스토어패스워드 -키스토어 키스토어.jks



Windows 명령 프롬프트에서 "keytool" 명령을 인식하지 못하는 경우 keytool 명령을 해당 전체 경로로 바꾸세요.

C:\Program Files\Java\<jdk_버전>\bin\keytool.exe" -storepasswd -keystore keystore.jks

3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.

키툴 -키패스워드 -별칭 "인증서의 별칭_이름" -키스토어 키스토어.jks

agent.properties 파일의 KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

4. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

keytool -list -v -keystore keystore.jks

4. 루트 또는 중간 인증서를 추가합니다.

keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. *keystore.jks* 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
키툴 -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -  
대상키스토어 keystore.jks -대상키스토어 유형 JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 agent.properties 파일의 KEYSTORE_PASS 키 값입니다.

```
키툴 -키패스워드 -별칭 "CA_인증서의_별칭_이름" -키스토어 키스토어.jks
```

8. agent.properties 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

9. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

SnapCenter 플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- 관련 CA 인증서에 대한 최신 CRL 파일을 다운로드하려면 다음을 참조하세요. "[SnapCenter CA 인증서에서 인증서 해지 목록 파일을 업데이트하는 방법](#)".
- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 '_C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\ etc\crl_'입니다.

단계

1. agent.properties 파일에서 기본 디렉토리를 CRL_PATH 키에 맞춰 수정하고 업데이트할 수 있습니다.
2. 이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다.

수신 인증서는 각 CRL에 대해 검증됩니다.

플러그인에 대한 CA 인증서 활성화

CA 인증서를 구성하고 SnapCenter 서버와 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- Set-SmCertificateSettings cmdlet을 실행하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- _Get-SmCertificateSettings_를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 _Get-Help command_name_을 실행하면 얻을 수

있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 하나 또는 여러 개의 플러그인 호스트를 선택하세요.
4. *추가 옵션*을 클릭하세요.
5. *인증서 검증 사용*을 선택합니다.

당신이 완료한 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- *  *는 CA 인증서가 활성화되지 않았거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- *  *는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- *  *는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- *  *는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

SnapCenter Plug-in for VMware vSphere 설치

데이터베이스나 파일 시스템이 가상 머신(VM)에 저장되어 있거나 VM과 데이터 저장소를 보호하려는 경우 SnapCenter Plug-in for VMware vSphere 배포해야 합니다.

배포에 대한 정보는 다음을 참조하세요. "[배포 개요](#)".

CA 인증서 배포

SnapCenter Plug-in for VMware vSphere 사용하여 CA 인증서를 구성하려면 다음을 참조하세요. "[SSL 인증서 생성 또는 가져오기](#)".

CRL 파일 구성

SnapCenter Plug-in for VMware vSphere 미리 구성된 디렉토리에서 CRL 파일을 찾습니다. SnapCenter Plug-in for VMware vSphere의 CRL 파일의 기본 디렉토리는 `_/opt/netapp/config/crl_`입니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

데이터 보호를 준비하세요

SAP HANA 데이터베이스용 **SnapCenter** 플러그인을 사용하기 위한 전제 조건

SAP HANA 데이터베이스용 SnapCenter 플러그인을 사용하기 전에 SnapCenter 관리자가

SnapCenter 서버를 설치하고 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다.
- SnapCenter 서버에 로그인합니다.
- 해당되는 경우 스토리지 시스템 연결을 추가하고 자격 증명을 생성하여 SnapCenter 환경을 구성합니다.
- Linux 또는 Windows 호스트에 Java 11을 설치합니다.

호스트 머신의 환경 경로 변수에 Java 경로를 설정해야 합니다.

- 백업 복제가 필요한 경우 SnapMirror와 SnapVault 설정하세요.
- SAP HANA 데이터베이스용 플러그인을 설치할 호스트에 HDBSQL 클라이언트를 설치합니다.

이 호스트를 통해 관리할 SAP HANA 노드에 대한 사용자 저장소 키를 구성합니다.

- SAP HANA 데이터베이스 2.0SPS05의 경우 SAP HANA 데이터베이스 사용자 계정을 사용하는 경우 SnapCenter 서버에서 백업, 복원 및 복제 작업을 수행할 수 있는 다음 권한이 있는지 확인하세요.
 - 백업 관리자
 - 카탈로그 읽기
 - 데이터베이스 백업 관리자
 - 데이터베이스 복구 연산자

SAP HANA 데이터베이스를 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식

SnapCenter 사용하기 전에 수행하려는 백업, 복제 및 복원 작업과 관련된 기본 개념을 이해하는 것이 좋습니다. 다양한 작업을 위해 리소스, 리소스 그룹 및 정책과 상호 작용합니다.

- 리소스는 일반적으로 SnapCenter로 백업하거나 복제하는 SAP HANA 데이터베이스입니다.
- SnapCenter 리소스 그룹은 호스트의 리소스 모음입니다.

리소스 그룹에서 작업을 수행하면 리소스 그룹에 대해 지정한 일정에 따라 리소스 그룹에 정의된 리소스에서 해당 작업이 수행됩니다.

필요에 따라 단일 리소스나 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 수행할 수도 있습니다.

- 정책은 데이터 보호 작업의 백업 빈도, 복제, 스크립트 및 기타 특성을 지정합니다.

리소스 그룹을 만들 때 해당 그룹에 대한 하나 이상의 정책을 선택합니다. 단일 리소스에 대해 주문형 백업을 수행할 때 정책을 선택할 수도 있습니다.

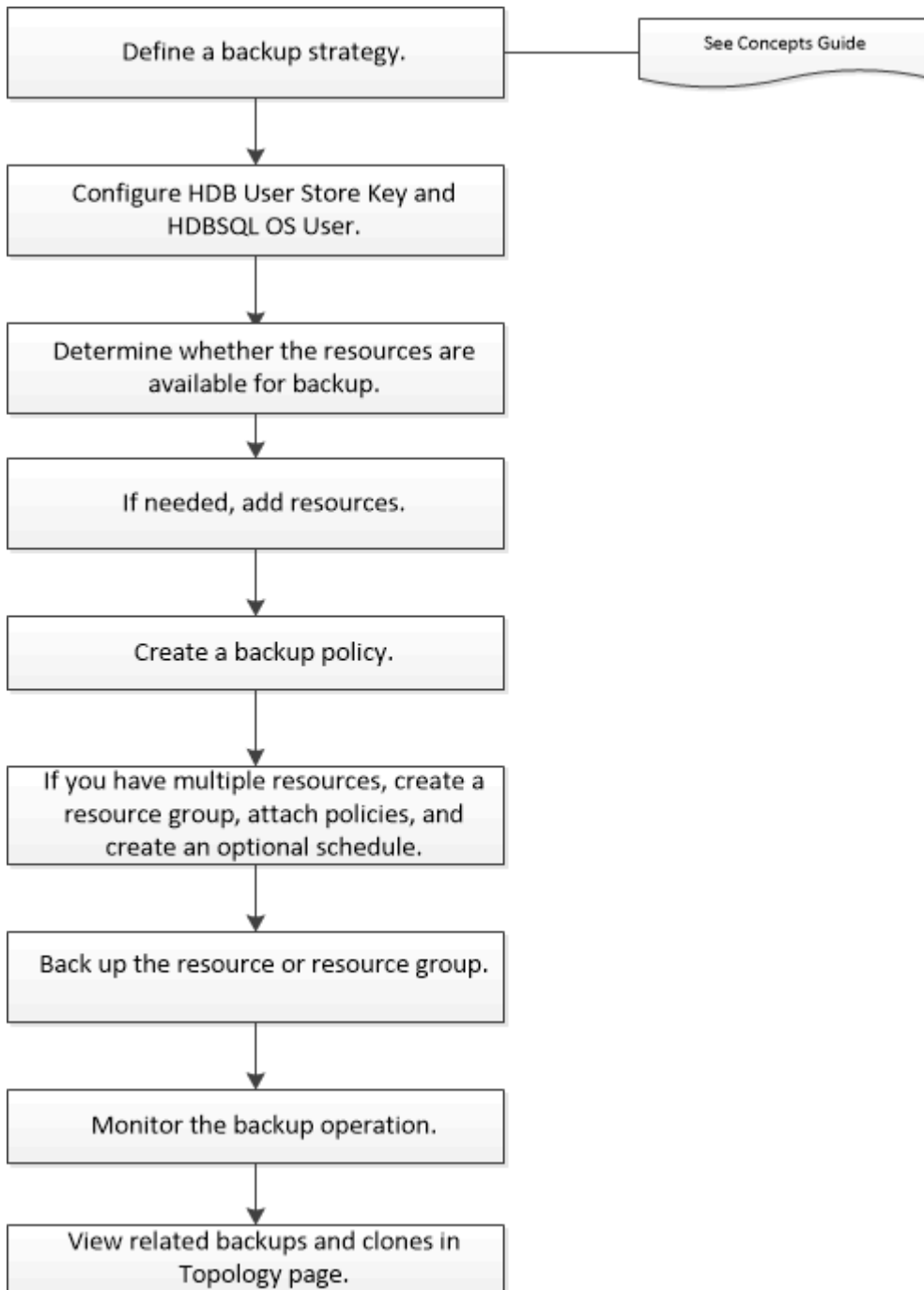
리소스 그룹은 무엇을 보호하고 싶은지, 언제 보호하고 싶은지 날짜와 시간을 정의하는 것으로 생각하면 됩니다. 정책이란 그것을 어떻게 보호할 것인지를 정의하는 것이라고 생각하세요. 예를 들어 모든 데이터베이스를 백업하는 경우 호스트의 모든 데이터베이스를 포함하는 리소스 그룹을 만들 수 있습니다. 그런 다음 리소스 그룹에 일일 정책과 시간별 정책이라는 두 가지 정책을 첨부할 수 있습니다. 리소스 그룹을 만들고 정책을 첨부할 때 리소스 그룹이 매일 전체 백업을 수행하도록 구성할 수 있습니다.

SAP HANA 리소스 백업

SAP HANA 리소스 백업

리소스(데이터베이스) 또는 리소스 그룹의 백업을 만들 수 있습니다. 백업 워크플로에는 계획, 백업할 데이터베이스 식별, 백업 정책 관리, 리소스 그룹 생성 및 정책 연결, 백업 생성, 작업 모니터링이 포함됩니다.

다음 워크플로는 백업 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

SAP HANA 데이터베이스에 대한 HDB 사용자 저장소 키 및 HDBSQL OS 사용자 구성

SAP HANA 데이터베이스에서 데이터 보호 작업을 수행하려면 HDB 사용자 저장소 키와 HDBSQL OS 사용자를 구성해야 합니다.

시작하기 전에

- SAP HANA 데이터베이스에 HDB 보안 사용자 저장 키와 HDB SQL OS 사용자가 구성되어 있지 않으면 자동 검색된 리소스에 대해서만 빨간색 자물쇠 아이콘이 나타납니다. 후속 검색 작업 중에 구성된 HDB 보안 사용자 저장 키가 올바르게 없거나 데이터베이스 자체에 대한 액세스를 제공하지 않는 것으로 확인되면 빨간색 자물쇠 아이콘이 다시 나타납니다.
- 데이터베이스를 보호하거나 리소스 그룹에 추가하여 데이터 보호 작업을 수행하려면 HDB 보안 사용자 저장 키와 HDB SQL OS 사용자를 구성해야 합니다.
- 시스템 데이터베이스에 액세스하려면 HDB SQL OS 사용자를 구성해야 합니다. HDB SQL OS 사용자가 테넌트 데이터베이스에만 액세스하도록 구성된 경우 검색 작업이 실패합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 SAP HANA 데이터베이스용 SnapCenter 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 리소스 유형을 선택합니다.
3. (선택사항) 클릭  호스트 이름을 선택하세요.

그런 다음 클릭할 수 있습니다  필터 창을 닫으려면.

4. 데이터베이스를 선택한 다음 *데이터베이스 구성*을 클릭합니다.
5. 데이터베이스 설정 구성 섹션에서 HDB 보안 사용자 저장소 키를 입력합니다.



플러그인 호스트 이름이 표시되고 HDB SQL OS 사용자가 자동으로 <sid>adm에 입력됩니다.

6. *확인*을 클릭합니다.

토폴로지 페이지에서 데이터베이스 구성을 수정할 수 있습니다.

리소스를 검색하고 데이터 보호를 위한 멀티테넌트 데이터베이스 컨테이너를 준비합니다.

데이터베이스를 자동으로 검색합니다

리소스는 SnapCenter 에서 관리하는 Linux 호스트의 SAP HANA 데이터베이스와 비데이터 볼륨입니다. 사용 가능한 SAP HANA 데이터베이스를 발견한 후 이러한 리소스를 리소스 그룹에 추가하여 데이터 보호 작업을 수행할 수 있습니다.

시작하기 전에

- SnapCenter 서버 설치, HDB 사용자 저장소 키 추가, 호스트 추가, 스토리지 시스템 연결 설정 등의 작업을 이미 완료했어야 합니다.
- Linux 호스트에서 HDB 보안 사용자 저장 키와 HDB SQL OS 사용자를 구성했어야 합니다.

- SID adm 사용자로 HDB 사용자 저장 키를 구성해야 합니다. 예를 들어, SID가 A22인 HANA 시스템의 경우 HDB 사용자 저장 키는 a22adm으로 구성되어야 합니다.

- SAP HANA 데이터베이스용 SnapCenter 플러그인은 RDM/VMDK 가상 환경에 있는 리소스의 자동 검색을 지원하지 않습니다. 데이터베이스를 수동으로 추가하는 동안 가상 환경에 대한 저장소 정보를 제공해야 합니다.

이 작업에 관하여

플러그인을 설치하면 해당 Linux 호스트의 모든 리소스가 자동으로 검색되어 리소스 페이지에 표시됩니다.

자동으로 검색된 리소스는 수정하거나 삭제할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 SAP HANA 데이터베이스용 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 리소스 유형을 선택합니다.
3. (선택사항) *를 클릭하세요  *를 선택한 다음 호스트 이름을 선택합니다.

그런 다음 *를 클릭할 수 있습니다.  * 필터 창을 닫습니다.

4. 호스트에서 사용 가능한 리소스를 알아보려면 *리소스 새로 고침*을 클릭하세요.

리소스는 리소스 유형, 호스트 이름, 연관된 리소스 그룹, 백업 유형, 정책 및 전반적인 상태와 같은 정보와 함께 표시됩니다.

- 데이터베이스가 NetApp 스토리지에 있고 보호되지 않은 경우 전체 상태 열에 보호되지 않음이 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되며 백업 작업이 수행되지 않은 경우, 전체 상태 열에 백업이 실행되지 않았습니라는 메시지가 표시됩니다. 그렇지 않으면 마지막 백업 상태에 따라 상태가 백업 실패 또는 백업 성공으로 변경됩니다.



SAP HANA 데이터베이스에 HDB 보안 사용자 저장소 키가 구성되어 있지 않으면 리소스 옆에 빨간색 자물쇠 아이콘이 나타납니다. 후속 검색 작업 중에 구성된 HDB 보안 사용자 저장 키가 올바르게 없거나 데이터베이스 자체에 대한 액세스를 제공하지 않는 것으로 확인되면 빨간색 자물쇠 아이콘이 다시 나타납니다.



SnapCenter 외부에서 데이터베이스 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

당신이 완료한 후

데이터베이스를 보호하거나 리소스 그룹에 추가하여 데이터 보호 작업을 수행하려면 HDB 보안 사용자 저장 키와 HDBSQL OS 사용자를 구성해야 합니다.

"SAP HANA 데이터베이스에 대한 HDB 사용자 저장소 키 및 HDBSQL OS 사용자 구성"

데이터 보호를 위한 멀티테넌트 데이터베이스 컨테이너 준비

SnapCenter 에 직접 등록된 SAP HANA 호스트의 경우 SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치하거나 업그레이드하면 호스트의 리소스가 자동으로 검색됩니다. 플러그인을 설치하거나 업그레이드한 후, 플러그인 호스트에 있는 모든 멀티테넌트 데이터베이스 컨테이너(MDC) 리소스에 대해 다른 GUID 형식으로 또 다른 MDC 리소스가 자동으로 검색되어 SnapCenter 에 등록됩니다. 새로운 리소스는 “잠김” 상태가 됩니다.

이 작업에 관하여

예를 들어 SnapCenter 4.2에서 E90 MDC 리소스가 플러그인 호스트에 위치하고 수동으로 등록된 경우 SnapCenter 4.3으로 업그레이드하면 다른 GUID를 가진 또 다른 E90 MDC 리소스가 검색되어 SnapCenter에 등록됩니다.



SnapCenter 4.2 및 이전 버전의 리소스와 관련된 백업은 보존 기간이 만료될 때까지 보관해야 합니다. 보존 기간이 만료된 후에는 이전 MDC 리소스를 삭제하고 자동으로 검색된 새 MDC 리소스를 계속 관리할 수 있습니다.

`Old MDC resource` SnapCenter 4.2 또는 이전 릴리스에서 수동으로 추가된 플러그인 호스트에 대한 MDC 리소스입니다.

SnapCenter 4.3에서 발견된 새로운 리소스를 데이터 보호 작업에 사용하려면 다음 단계를 수행하세요.

단계

1. 리소스 페이지에서 이전 SnapCenter 릴리스에 추가된 백업이 있는 이전 MDC 리소스를 선택하고 토폴로지 페이지에서 "유지 관리 모드"로 전환합니다.

리소스가 리소스 그룹의 일부인 경우 리소스 그룹을 "유지 관리 모드"로 전환합니다.

2. SnapCenter 4.3으로 업그레이드한 후 발견된 새로운 MDC 리소스를 구성하려면 리소스 페이지에서 새 리소스를 선택합니다.

"새로운 MDC 리소스"는 SnapCenter 서버와 플러그인 호스트가 4.3으로 업그레이드된 후 발견된 새로 발견된 MDC 리소스입니다. 새로운 MDC 리소스는 주어진 호스트에 대해 기존 MDC 리소스와 동일한 SID를 가진 리소스로 식별할 수 있으며, 리소스 페이지에서 해당 리소스 옆에 빨간색 자물쇠 아이콘이 표시됩니다.

3. SnapCenter 4.3으로 업그레이드한 후 발견된 새로운 MDC 리소스를 보호하려면 보호 정책, 일정 및 알림 설정을 선택합니다.
4. 보존 설정에 따라 SnapCenter 4.2 또는 이전 릴리스에서 수행된 백업을 삭제합니다.
5. 토폴로지 페이지에서 리소스 그룹을 삭제합니다.
6. 리소스 페이지에서 이전 MDC 리소스를 삭제합니다.

예를 들어, 기본 스냅샷 보존 기간이 7일이고 보조 스냅샷 보존 기간이 45일인 경우, 45일이 끝나고 모든 백업이 삭제되면 리소스 그룹과 이전 MDC 리소스를 삭제해야 합니다.

관련 정보

["SAP HANA 데이터베이스에 대한 HDB 사용자 저장소 키 및 HDBSQL OS 사용자 구성"](#)

["토폴로지 페이지에서 SAP HANA 데이터베이스 백업 및 복제본 보기"](#)

플러그인 호스트에 수동으로 리소스 추가

특정 HANA 인스턴스에서는 자동 검색이 지원되지 않습니다. 이러한 리소스는 수동으로 추가해야 합니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 설정, HDB 사용자 저장소 키 추가 등의 작업을 완료했어야 합니다.

- SAP HANA 시스템 복제의 경우, 해당 HANA 시스템의 모든 리소스를 하나의 리소스 그룹에 추가하고 리소스 그룹 백업을 수행하는 것이 좋습니다. 이를 통해 인수-장애 복구 모드에서 원활한 백업이 보장됩니다.

"리소스 그룹을 만들고 정책을 첨부합니다."

이 작업에 관하여

다음 구성에서는 자동 검색이 지원되지 않습니다.

- RDM 및 VMDK 레이아웃



위의 리소스가 발견되는 경우, 해당 리소스에서는 데이터 보호 작업이 지원되지 않습니다.

- HANA 다중 호스트 구성
- 동일한 호스트에 여러 인스턴스가 있음
- 다중 계층 확장 HANA 시스템 복제
- 시스템 복제 모드의 계단식 복제 환경

단계

1. 왼쪽 탐색 창에서 드롭다운 목록에서 SAP HANA 데이터베이스용 SnapCenter 플러그인을 선택한 다음 *리소스*를 클릭합니다.
2. 리소스 페이지에서 *SAP HANA 데이터베이스 추가*를 클릭합니다.
3. 리소스 세부 정보 제공 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
리소스 유형	리소스 유형을 입력하세요. 리소스 유형으로는 단일 컨테이너, 다중 테넌트 데이터베이스 컨테이너(MDC), 비데이터 볼륨이 있습니다.
HANA 시스템 이름	설명적인 SAP HANA 시스템 이름을 입력하세요. 이 옵션은 단일 컨테이너 또는 MDC 리소스 유형을 선택한 경우에만 사용할 수 있습니다.
시드	시스템 ID(SID)를 입력하세요. 설치된 SAP HANA 시스템은 단일 SID로 식별됩니다.
플러그인 호스트	플러그인 호스트를 선택하세요.
HDB 보안 사용자 저장 키	SAP HANA 시스템에 연결하려면 키를 입력하세요. 키에는 데이터베이스에 연결하기 위한 로그인 정보가 들어 있습니다. SAP HANA 시스템 복제의 경우 보조 사용자 키는 검증되지 않습니다. 이는 인수 시 사용됩니다.

이 분야에서는...	이렇게 하세요...
HDBSQL OS 사용자	HDB 보안 사용자 저장 키가 구성된 사용자 이름을 입력하세요. Windows의 경우 HDBSQL OS 사용자는 SYSTEM 사용자여야 합니다. 따라서 SYSTEM 사용자에 대한 HDB 보안 사용자 저장 키를 구성해야 합니다.

4. 스토리지 공간 제공 페이지에서 스토리지 시스템을 선택하고 하나 이상의 볼륨, LUN, Qtree를 선택한 다음 *저장*을 클릭합니다.

선택 사항: *를 클릭할 수 있습니다.  * 아이콘을 클릭하면 다른 스토리지 시스템에서 볼륨, LUN, Q트리를 추가할 수 있습니다.

5. 요약을 검토한 후 *마침*을 클릭하세요.

데이터베이스는 SID, 플러그인 호스트, 연관된 리소스 그룹 및 정책, 전반적인 상태와 같은 정보와 함께 표시됩니다.

사용자에게 리소스에 대한 액세스 권한을 제공하려면 사용자에게 리소스를 할당해야 합니다. 이를 통해 사용자는 자신에게 할당된 자산에 대해 권한이 있는 작업을 수행할 수 있습니다.

"사용자 또는 그룹을 추가하고 역할과 자산을 할당합니다."

데이터베이스를 추가한 후 SAP HANA 데이터베이스 세부 정보를 수정할 수 있습니다.

SAP HANA 리소스와 연결된 백업이 있는 경우 다음을 수정할 수 없습니다.

- 멀티테넌트 데이터베이스 컨테이너(MDC): SID 또는 HDBSQL 클라이언트(플러그인) 호스트
- 단일 컨테이너: SID 또는 HDBSQL 클라이언트(플러그인) 호스트
- 비데이터 볼륨: 리소스 이름, 연결된 SID 또는 플러그인 호스트

SAP HANA 데이터베이스에 대한 백업 정책 만들기

SnapCenter 사용하여 SAP HANA 데이터베이스 리소스를 백업하기 전에 백업하려는 리소스 또는 리소스 그룹에 대한 백업 정책을 만들어야 합니다. 백업 정책은 백업을 관리, 일정을 정하고 보관하는 방법을 규정하는 일련의 규칙입니다.

시작하기 전에

- 백업 전략을 정의했어야 합니다.

자세한 내용은 SAP HANA 데이터베이스에 대한 데이터 보호 전략 정의에 대한 정보를 참조하세요.

- SnapCenter 설치, 호스트 추가, 스토리지 시스템 연결 설정, 리소스 추가 등의 작업을 완료하여 데이터 보호를 준비했어야 합니다.
- 스냅샷을 미리 또는 볼트에 복제하는 경우 SnapCenter 관리자가 소스 및 대상 볼륨 모두에 대한 SVM을 할당해야 합니다.

또한 정책에서 복제, 스크립트 및 애플리케이션 설정을 지정할 수 있습니다. 이러한 옵션을 사용하면 다른 리소스

그룹에 대한 정책을 재사용할 때 시간을 절약할 수 있습니다.

- SnapMirror Active Sync의 특정 전제 조건과 제한 사항을 검토하세요. 자세한 내용은 다음을 참조하세요.
["SnapMirror Active Sync에 대한 개체 제한"](#).

이 작업에 관하여

- SAP HANA 시스템 복제

- 기본 SAP HANA 시스템을 보호하고 모든 데이터 보호 작업을 수행할 수 있습니다.
- 보조 SAP HANA 시스템을 보호할 수는 있지만 백업을 생성할 수는 없습니다.

장애 조치 후에는 보조 SAP HANA 시스템이 기본 SAP HANA 시스템이 되어 모든 데이터 보호 작업을 수행할 수 있습니다.

SAP HANA 데이터 볼륨에 대한 백업을 생성할 수 없지만 SnapCenter 비데이터 볼륨(NDV)을 계속 보호합니다.

- SnapLock

- '특정 기간 동안 백업 사본을 보관합니다' 옵션을 선택한 경우 SnapLock 보관 기간은 언급된 보관 기간보다 짧거나 같아야 합니다.
- 스냅샷 잠금 기간을 지정하면 보존 기간이 만료될 때까지 스냅샷이 삭제되지 않습니다. 이를 통해 정책에 지정된 수보다 더 많은 수의 스냅샷을 보존할 수 있습니다.
- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *정책*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 이름 페이지에서 정책 이름과 세부 정보를 입력합니다.
5. 정책 유형 페이지에서 다음 단계를 수행합니다.

- 저장 유형을 선택하세요
- 백업 유형을 선택하세요:

만약 당신이 원한다면...	이렇게 하세요...
스냅샷 기술을 사용하여 백업을 만듭니다.	*스냅샷 기반*을 선택하세요.
데이터베이스의 무결성 검사를 수행합니다.	*파일 기반 백업*을 선택하세요. 활성 테넌트만 백업됩니다.

6. 스냅샷 및 복제 페이지에서 다음 단계를 수행합니다.

- 주문형, 시간별, 일별, 주별 또는 *월별*을 선택하여 일정 유형을 지정합니다.



리소스 그룹을 생성하는 동안 백업 작업에 대한 일정(시작 날짜, 종료 날짜, 빈도)을 지정할 수 있습니다. 이를 통해 동일한 정책과 백업 빈도를 공유하는 리소스 그룹을 만들 수 있을 뿐만 아니라 각 정책에 다른 백업 일정을 할당할 수도 있습니다.



오전 2시로 예약한 경우, 일광 절약 시간제(DST) 기간에는 일정이 실행되지 않습니다.

7. 스냅샷 및 복제 페이지에서 백업 유형 페이지에서 선택한 백업 유형과 일정 유형에 대한 보존 설정을 지정합니다.

만약 당신이 원한다면...	그 다음에...
특정 수의 스냅샷을 보관하세요	*보관할 사본*을 선택한 다음 보관하려는 스냅샷 수를 지정합니다. 스냅샷 수가 지정된 수를 초과하면 가장 오래된 스냅샷이 먼저 삭제됩니다. 최대 보존 값은 1018입니다. 보존 기간이 ONTAP 버전에서 지원하는 것보다 높은 값으로 설정된 경우 백업이 실패합니다. 스냅샷 복사 기반 백업의 경우 SnapVault 복제를 활성화하려면 보존 횟수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷이 대상에 복제될 때까지 첫 번째 스냅샷이 SnapVault 관계에 대한 참조 스냅샷이 되기 때문에 보존 작업이 실패할 수 있습니다. SAP HANA 시스템 복제의 경우, SAP HANA 시스템의 모든 리소스를 하나의 리소스 그룹에 추가하는 것이 좋습니다. 이렇게 하면 적절한 수의 백업이 보관됩니다. SAP HANA 시스템 복제의 경우, 생성된 총 스냅샷은 리소스 그룹에 대해 설정된 보존 기간과 동일합니다. 가장 오래된 스냅샷을 제거하는 것은 가장 오래된 스냅샷이 위치한 노드에 따라 결정됩니다. 예를 들어, SAP HANA 시스템 복제가 기본이고 SAP HANA 시스템 복제가 보조인 리소스 그룹의 경우 보존 기간이 7로 설정됩니다. SAP HANA 시스템 복제 기본 및 SAP HANA 시스템 복제 보조를 모두 포함하여 한 번에 최대 7개의 스냅샷을 찍을 수 있습니다.

만약 당신이 원한다면...	그 다음에...
스냅샷을 특정 일수 동안 보관하세요	*사본 보관 기간*을 선택한 다음, 스냅샷을 삭제하기 전에 보관할 일수를 지정합니다.
스냅샷 복사 잠금 기간	*스냅샷 복사 잠금 기간*을 선택하고 일, 월 또는 년을 지정합니다. SnapLock 보존 기간은 100년 미만이어야 합니다.

8. 스냅샷 라벨을 선택하세요.



원격 복제를 위해 기본 스냅샷에 SnapMirror 레이블을 할당하면 기본 스냅샷이 SnapCenter 에서 ONTAP 보조 시스템으로 스냅샷 복제 작업을 오프로드할 수 있습니다. 정책 페이지에서 SnapMirror 또는 SnapVault 옵션을 활성화하지 않고도 이 작업을 수행할 수 있습니다.

9. 스냅샷 복사 기반 백업의 경우 보조 복제 옵션 선택 섹션에서 다음 보조 복제 옵션 중 하나 또는 둘 다를 선택합니다.

이 분야에서는...	이렇게 하세요...
로컬 스냅샷 복사본을 만든 후 SnapMirror 업데이트	다른 볼륨에 백업 세트의 미러 복사본을 생성하려면 이 필드를 선택합니다(SnapMirror 복제). SnapMirror Active Sync의 경우 이 옵션을 활성화해야 합니다. ONTAP 의 보호 관계가 미러 및 볼트 유형이고 이 옵션만 선택하는 경우, 기본에서 생성된 스냅샷은 대상으로 전송되지 않지만 대상에는 나열됩니다. 대상에서 이 스냅샷을 선택하여 복원 작업을 수행하는 경우, 선택한 보관/미러링 백업에 대해 보조 위치를 사용할 수 없다는 오류 메시지가 표시됩니다. 2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고침됩니다. 보다 "토폴로지 페이지에서 SAP HANA 데이터베이스 백업 및 복제본 보기".

이 분야에서는...	이렇게 하세요...
로컬 스냅샷 복사본을 만든 후 SnapVault 업데이트	디스크 간 백업 복제(SnapVault 백업)를 수행하려면 이 옵션을 선택하세요. 2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고침됩니다. ONTAP 에서 SnapLock Vault로 알려진 보조 노드에만 SnapLock 구성된 경우 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 보조 노드의 잠금 기간이 새로 고침됩니다. SnapLock Vault에 대한 자세한 내용은 다음을 참조하세요. "볼트 대상의 WORM에 스냅샷 복사본 커밋" 보다 "토폴로지 페이지에서 SAP HANA 데이터베이스 백업 및 복제본 보기" .
오류 재시도 횟수	작업이 중지되기 전에 허용할 수 있는 최대 복제 시도 횟수를 입력하세요.



보조 저장소의 스냅샷 최대 한도에 도달하지 않도록 하려면 ONTAP 에서 보조 저장소 SnapMirror 보존 정책을 구성해야 합니다.

10. 요약을 검토한 후 *마침*을 클릭하세요.

리소스 그룹을 만들고 정책을 첨부합니다.

리소스 그룹은 백업하고 보호하려는 리소스를 추가해야 하는 컨테이너입니다. 리소스 그룹을 사용하면 주어진 애플리케이션과 관련된 모든 데이터를 동시에 백업할 수 있습니다. 모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한, 수행하려는 데이터 보호 작업 유형을 정의하려면 리소스 그룹에 하나 이상의 정책을 연결해야 합니다.

이 작업에 관하여

- SAP HANA 시스템 복제 백업을 생성하려면 SAP HANA 시스템의 모든 리소스를 하나의 리소스 그룹에 추가하는 것이 좋습니다. 이를 통해 인수-장애 복구 모드에서 원활한 백업이 보장됩니다.
- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.
- SnapMirror 활성화 동기화가 있는 리소스가 포함된 기존 리소스 그룹에 SnapMirror 활성화 동기화 SnapMirror 없는 새 데이터베이스를 추가하는 것은 지원되지 않습니다.
- SnapMirror Active Sync의 장애 조치 모드에서 기존 리소스 그룹에 새 데이터베이스를 추가하는 것은 지원되지 않습니다. 일반 상태나 장애 복구 상태에서만 리소스 그룹에 리소스를 추가할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	리소스 그룹의 이름을 입력하세요.  리소스 그룹 이름은 250자를 넘을 수 없습니다.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력하세요. 예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.
스냅샷 복사에 사용자 정의 이름 형식 사용	이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다. 예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 호스트 이름을 선택하고 리소스 유형 드롭다운 목록에서 리소스 유형을 선택합니다.

이는 화면에 표시되는 정보를 필터링하는 데 도움이 됩니다.

5. 사용 가능한 리소스 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 클릭하여 선택한 리소스 섹션으로 이동합니다.
6. 애플리케이션 설정 페이지에서 다음을 수행합니다.

- a. 추가 백업 옵션을 설정하려면 백업 화살표를 클릭하세요.

일관성 그룹 백업을 활성화하고 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
일관성 그룹 스냅샷 작업이 완료될 때까지 기다릴 시간을 확보하세요.	스냅샷 작업이 완료될 때까지의 대기 시간을 지정하려면 긴급, 보통, *느슨함*을 선택합니다. 긴급 = 5초, 보통 = 7초, 여유 = 20초.
WAFL 동기화 비활성화	WAFL 일관성 지점을 강제로 적용하지 않으려면 이 옵션을 선택하세요.

+

- a. 스크립트 화살표를 클릭하고 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령을 입력합니다. 실패 시 종료하기 전에 실행할 사전 명령을 입력할 수도 있습니다.
- b. 사용자 정의 구성 화살표를 클릭하고 이 리소스를 사용하는 모든 데이터 보호 작업에 필요한 사용자 정의 키-값 쌍을 입력합니다.

매개변수	환경	설명
아카이브 로그 활성화	(예/아니요)	보관 로그 관리를 통해 보관 로그를 삭제할 수 있습니다.
아카이브 로그 보존	일수	보관 로그를 보관하는 일수를 지정합니다. 이 설정은 NTAP_SNAPSHOT_RETENTIONS보다 크거나 같아야 합니다.
아카이브_로그_디렉토리	변경_정보_디렉토리/로그	보관 로그가 포함된 디렉토리의 경로를 지정합니다.
아카이브_로그_확장	파일 확장자	보관 로그 파일 확장자 길이를 지정합니다. 예를 들어, 보관 로그가 log_backup_0_0_0_0.161518551942 9이고 file_extension 값이 5이면 로그 확장자는 5자리인 16151을 유지합니다.

매개변수	환경	설명
ARCHIVE_LOG_RECURSIVE_SE ARCH	(예/아니요)	하위 디렉토리 내의 보관 로그 관리를 활성화합니다. 보관 로그가 하위 디렉토리에 있는 경우 이 매개변수를 사용해야 합니다.



사용자 정의 키-값 쌍은 SAP HANA Linux 플러그인 시스템에서는 지원되고 중앙화된 Windows 플러그인으로 등록된 SAP HANA 데이터베이스에서는 지원되지 않습니다.

- c. 스냅샷 복사 도구* 화살표를 클릭하여 스냅샷을 만드는 도구를 선택하세요.

원하신다면...	그 다음에...
SnapCenter Windows용 플러그인을 사용하여 스냅샷을 만들기 전에 파일 시스템을 일관된 상태로 만듭니다. Linux 리소스의 경우 이 옵션은 적용되지 않습니다.	*파일 시스템 일관성을 갖춘 SnapCenter *를 선택하세요. 이 옵션은 SAP HANA 데이터베이스용 SnapCenter 플러그인에는 적용되지 않습니다.
SnapCenter 사용하여 스토리지 수준 스냅샷을 생성합니다.	*파일 시스템 일관성이 없는 SnapCenter *를 선택하세요.
스냅샷 복사본을 생성하기 위해 호스트에서 실행할 명령을 입력합니다.	*기타*를 선택한 다음 호스트에서 실행할 명령을 입력하여 스냅샷을 만듭니다.

7. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다. *.

정책은 '선택한 정책에 대한 일정 구성' 섹션에 나열되어 있습니다.

- b. 일정 구성 열에서 *를 클릭합니다. * 구성하려는 정책에 대해.
c. 정책 _policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 policy_name은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP 서버는 설정 > *전역 설정*에서 구성해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

ASA r2 시스템에서 SAP HANA 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.

ASA r2 시스템에 있는 리소스를 추가하려면 리소스 그룹을 만들어야 합니다. 리소스 그룹을 생성하는 동안 보조 보호를 프로비저닝할 수도 있습니다.

시작하기 전에

- ONTAP 9.x 리소스와 ASA r2 리소스를 동일한 리소스 그룹에 추가하지 않도록 해야 합니다.
- ONTAP 9.x 리소스와 ASA r2 리소스가 모두 포함된 데이터베이스가 없는지 확인해야 합니다.

이 작업에 관하여

- 2차 보호는 로그인한 사용자에게 **SecondaryProtection** 기능이 활성화된 역할이 할당된 경우에만 사용할 수 있습니다.
- 2차 보호를 활성화한 경우 기본 및 2차 일관성 그룹을 생성하는 동안 리소스 그룹은 유지 관리 모드로 전환됩니다. 기본 및 보조 일관성 그룹이 생성된 후 리소스 그룹은 유지 관리 모드에서 해제됩니다.
- SnapCenter 클론 리소스에 대한 보조 보호를 지원하지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.
 - a. 이름 필드에 리소스 그룹의 이름을 입력합니다.



리소스 그룹 이름은 250자를 넘을 수 없습니다.

- b. 나중에 리소스 그룹을 검색하는 데 도움이 되도록 태그 필드에 하나 이상의 레이블을 입력하세요.

예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.

- c. 이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

- d. 백업하지 않을 보관 로그 파일의 대상을 지정합니다.



필요한 경우 접두사를 포함하여 애플리케이션에 설정된 것과 정확히 동일한 목적지를 사용해야 합니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 데이터베이스 호스트 이름을 선택합니다.



리소스가 성공적으로 검색된 경우에만 해당 리소스가 사용 가능한 리소스 섹션에 나열됩니다. 최근에 리소스를 추가한 경우 리소스 목록을 새로 고친 후에만 사용 가능한 리소스 목록에 표시됩니다.

5. 사용 가능한 리소스 섹션에서 ASA r2 리소스를 선택하고 선택한 리소스 섹션으로 이동합니다.
6. 애플리케이션 설정 페이지에서 백업 옵션을 선택하세요.
7. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



또한 다음을 클릭하여 정책을 생성할 수도 있습니다. .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

- b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.
- c. 정책 `_policy_name_`에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 `_policy_name_`은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 선택한 정책에 대해 보조 보호가 활성화된 경우 보조 보호 페이지가 표시되며 다음 단계를 수행해야 합니다.
 - a. 복제 정책의 유형을 선택하세요.



동기 복제 정책은 지원되지 않습니다.

- b. 사용할 일관성 그룹 접미사를 지정합니다.
- c. 대상 클러스터 및 대상 SVM 드롭다운에서 사용하려는 피어링된 클러스터와 SVM을 선택합니다.



SnapCenter에서는 클러스터 및 SVM 피어링을 지원하지 않습니다. 클러스터 및 SVM 피어링을 수행하려면 System Manager 또는 ONTAP CLI를 사용해야 합니다.



리소스가 이미 SnapCenter 외부에서 보호되고 있는 경우 해당 리소스는 보조 보호 리소스 섹션에 표시됩니다.

1. 확인 페이지에서 다음 단계를 수행하세요.
 - a. *로케이터 로드*를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 저장소에서 검증을 수행합니다.
 - b. 딸깍 하는 소리  일정 구성 열에서 정책의 모든 일정 유형에 대한 확인 일정을 구성합니다.
 - c. 확인 일정 추가 `policy_name` 대화 상자에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	이렇게 하세요...
백업 후 검증 실행	*백업 후 검증 실행*을 선택하세요.
검증 일정을 예약하세요	*예약된 확인 실행*을 선택한 다음 드롭다운 목록에서 일정 유형을 선택합니다.

d. 보조 저장소 시스템에서 백업을 확인하려면 *보조 위치에서 확인*을 선택하세요.

e. *확인*을 클릭합니다.

구성된 검증 일정은 적용된 일정 열에 나열됩니다.

2. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

3. 요약 검토 후 *마침*을 클릭하세요.

PowerShell cmdlet을 사용하여 SAP HANA 데이터베이스용 스토리지 시스템 연결 및 자격 증명 만들기

PowerShell cmdlet을 사용하여 SAP HANA 데이터베이스를 백업, 복원 또는 복제하려면 먼저 SVM(스토리지 가상 머신) 연결과 자격 증명을 만들어야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 저장소 연결을 생성하려면 인프라 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

스토리지 시스템 연결을 추가하는 동안에는 호스트 플러그인 설치가 진행 중이어서는 안 됩니다. 호스트 캐시가 업데이트되지 않고 SnapCenter GUI에 데이터베이스 상태가 “백업에 사용할 수 없음” 또는 “NetApp 스토리지에 없음”으로 표시될 수 있기 때문입니다.

- 저장 시스템 이름은 고유해야 합니다.

SnapCenter 서로 다른 클러스터에 동일한 이름을 가진 여러 스토리지 시스템을 지원하지 않습니다. SnapCenter에서 지원하는 각 스토리지 시스템은 고유한 이름과 고유한 데이터 LIF IP 주소를 가져야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 PowerShell 연결 세션을 시작합니다.

```
PS C:\> Open-SmStorageConnection
```

2. Add-SmStorageConnection cmdlet을 사용하여 스토리지 시스템에 대한 새 연결을 만듭니다.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap  
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Add-SmCredential cmdlet을 사용하여 새 자격 증명을 만듭니다.

이 예제에서는 Windows 자격 증명을 사용하여 FinanceAdmin이라는 새 자격 증명을 만드는 방법을 보여줍니다.

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. SnapCenter 서버에 SAP HANA 통신 호스트를 추가합니다.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName  
FinanceAdmin -PluginCode hana
```

5. 호스트에 SAP HANA 데이터베이스용 패키지와 SnapCenter 플러그인을 설치합니다.

Linux의 경우:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode  
hana
```

Windows의 경우:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana  
-FileSystemCode scw -RunAsName FinanceAdmin
```

6. HDBSQL 클라이언트의 경로를 설정합니다.

Windows의 경우:

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode  
hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program  
Files\sap\hdbclient\hdbsql.exe"}
```

Linux의 경우:

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com
-PluginCode hana -configSettings
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

SAP HANA 데이터베이스 백업

리소스가 아직 어떤 리소스 그룹에도 속하지 않은 경우 리소스 페이지에서 리소스를 백업할 수 있습니다.

시작하기 전에

- 백업 정책을 생성했어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에 "snapmirror all" 권한이 포함되어야 합니다. 하지만 "vsadmin" 역할을 사용하는 경우 "snapmirror all" 권한은 필요하지 않습니다.
- 스냅샷 복사 기반 백업 작업의 경우 모든 테넌트 데이터베이스가 유효하고 활성화되어 있는지 확인하세요.
- SAP HANA 시스템 복제 백업을 생성하려면 SAP HANA 시스템의 모든 리소스를 하나의 리소스 그룹에 추가하는 것이 좋습니다. 이를 통해 인수-장애 복구 모드에서 원활한 백업이 보장됩니다.

"[리소스 그룹을 만들고 정책을 첨부합니다.](#)".

"리소스 그룹 백업"

- 하나 이상의 테넌트 데이터베이스가 다운된 경우 파일 기반 백업을 생성하려면 HANA 속성 파일에서 `ALLOW_FILE_BASED_BACKUP_IFINACTIVE_TENANTS_PRESENT` 매개변수를 *YES*로 설정합니다. `Set-SmConfigSettings` cmdlet.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `Get-Help _command_name_`을 실행하여 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

- 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령의 경우, 플러그인 호스트에서 다음 경로의 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 호스트의 기본 위치: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

선택하다  *를 선택한 다음 호스트 이름과 리소스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 선택할 수 있습니다  필터 창을 닫으려면.

3. 백업할 리소스를 선택하세요.
4. 리소스 페이지에서 *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택한 다음 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, *customtext_policy_hostname* 또는 *_resource_hostname_*입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

5. 애플리케이션 설정 페이지에서 다음을 수행합니다.

- 추가 백업 옵션을 설정하려면 백업 화살표를 선택하세요.

필요한 경우 일관성 그룹 백업을 활성화하고 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
"일관성 그룹 스냅샷" 작업이 완료될 때까지 기다릴 시간을 확보하세요.	스냅샷 작업이 완료될 때까지의 대기 시간을 지정하려면 긴급, 보통, *느슨함*을 선택합니다. 긴급 = 5초, 보통 = 7초, 여유 = 20초.
WAFL 동기화 비활성화	WAFL 일관성 지점을 강제로 적용하지 않으려면 이 옵션을 선택하세요.

- 스크립트 화살표를 선택하여 정지, 스냅샷 및 정지 해제 작업에 대한 사전 및 사후 명령을 실행합니다.

백업 작업을 종료하기 전에 사전 명령을 실행할 수도 있습니다. Prescript와 Postscript는 SnapCenter Server에서 실행됩니다.

- 사용자 정의 구성 화살표를 선택한 다음, 이 리소스를 사용하는 모든 작업에 필요한 사용자 정의 값 쌍을 입력합니다.
- 스냅샷 복사 도구* 화살표를 선택하여 스냅샷을 만드는 도구를 선택하세요.

원하신다면...	그 다음에...
SnapCenter 사용하여 스토리지 수준 스냅샷을 생성합니다.	*파일 시스템 일관성이 없는 SnapCenter *를 선택하세요.
SnapCenter Windows용 플러그인을 사용하여 파일 시스템을 일관된 상태로 만든 다음 스냅샷을 생성합니다.	*파일 시스템 일관성을 갖춘 SnapCenter *를 선택하세요.

원하신다면...	그 다음에...
스냅샷을 생성하는 명령을 입력하려면	*기타*를 선택한 다음 스냅샷을 만드는 명령을 입력합니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다. *.

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

b. 선택하다 * 일정을 구성하려는 정책에 대한 일정 구성 옆에 있습니다.

c. 정책 `_policy_name_`에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 선택합니다.

`_policy_name_`은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 옆에 나열됩니다.

7. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > *전역 설정*에서도 구성해야 합니다.

8. 요약 검토한 후 *마침*을 선택하세요.

리소스 토폴로지 페이지가 표시됩니다.

9. *지금 백업*을 선택하세요.
10. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스에 여러 정책을 적용한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.
 - b. *백업*을 선택하세요.
11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.
 - MetroCluster 구성에서 SnapCenter 장애 조치 후 보호 관계를 감지하지 못할 수 있습니다.

자세한 내용은 다음을 참조하세요. ["MetroCluster 장애 조치 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다."](#)
 - VMDK에서 애플리케이션 데이터를 백업하고 SnapCenter Plug-in for VMware vSphere의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다.

Java 힙 크기를 늘리려면 스크립트 파일 `/opt/netapp/init_scripts/scvservice_`를 찾으세요. 해당 스크립트에서 `_do_start` 메서드 명령은 SnapCenter VMware 플러그인 서비스를 시작합니다. 해당 명령을 다음으로 업데이트하세요: `Java -jar -Xmx8192M -Xms4096M`

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-smconnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146\
```

사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.

2. Add-SmResources cmdlet을 사용하여 리소스를 추가합니다.

이 예제에서는 SingleContainer 유형의 SAP HANA 데이터베이스를 추가하는 방법을 보여줍니다.

```
C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'
-DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint
(@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary"
}) -SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys
'HS10' -osdbuser 'h10adm' -filebackupprefix 'H10_'
```

이 예제에서는 MultipleContainers 유형의 SAP HANA 데이터베이스를 추가하는 방법을 보여줍니다.

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType
MultipleContainers -StorageFootPrint
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.net
app.com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType
'MultiTenant'
```

이 예제에서는 비데이터 볼륨 리소스를 만드는 방법을 보여줍니다.

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sscore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

3. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.

이 예제에서는 스냅샷 복사 기반 백업에 대한 백업 정책을 만듭니다.

```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType
Backup -PluginPolicyType hana -BackupType SnapShotBasedBackup
```

이 예제에서는 파일 기반 백업에 대한 백업 정책을 만듭니다.

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
-PluginPolicyType hana -BackupType FileBasedBackup
```

4. Add-SmResourceGroup cmdlet을 사용하여 리소스를 보호하거나 SnapCenter 에 새 리소스 그룹을 추가합니다.

이 예제에서는 단일 컨테이너 리소스를 보호합니다.

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies
hana_snapshotbased,hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

이 예제에서는 여러 컨테이너 리소스를 보호합니다.

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies
hana_snapshotbased,hana_Filebased
-Resources @{ "Host"="host.example.com"; "UID"="MDC\SID" }
-Description test -usesnapcenterwithoutfilesystemconsistency
```

이 예제에서는 지정된 정책과 리소스를 사용하여 새 리소스 그룹을 만듭니다.

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{ "Host"="sccorelinux61.sscore.test.com"; "Uid"="SID" },@{ "Host"="sc
corelinux62.sscore.test.com"; "Uid"="MDC\SID" })
-Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency -plugincode 'HANA'
```

이 예제에서는 비데이터 볼륨 리소스 그룹을 생성합니다.

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{ "Host"="SNAPCENTERN42.sscore.test.com"; "Uid"="H11"; "PluginName"=
"hana"},@{ "Host"="SNAPCENTERN42.sscore.test.com"; "Uid"="MDC\H31"; "Pl
uginName"="hana"},@{ "Host"="SNAPCENTERN42.sscore.test.com"; "Uid"="No
nDataVolume\S10\NonDataVolume"; "PluginName"="hana"}) -Policies
hanaprimary
```

5. New-SmBackup cmdlet을 사용하여 새로운 백업 작업을 시작합니다.

이 예제에서는 리소스 그룹을 백업하는 방법을 보여줍니다.

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

이 예제에서는 보호된 리소스를 백업합니다.

```
C:\PS> New-SMBackup -Resources
@{ "Host"="10.232.204.42"; "Uid"="MDC\SID"; "PluginName"="hana" }
-Policy hana_Filebased
```

6. Get-smJobSummaryReport cmdlet을 사용하여 작업 상태(실행 중, 완료 또는 실패)를 모니터링합니다.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Get-SmBackupReport cmdlet을 사용하여 복원 또는 복제 작업을 수행하기 위한 백업 ID, 백업 이름과 같은 백업 작업 세부 정보를 모니터링합니다.

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

리소스 그룹 백업

리소스 그룹은 호스트의 리소스 모음입니다. 리소스 그룹에 대한 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다.

시작하기 전에

- 정책이 첨부된 리소스 그룹을 만들어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에

“snapmirror all” 권한이 포함되어야 합니다. 하지만 “vsadmin” 역할을 사용하는 경우 “snapmirror all” 권한은 필요하지 않습니다.

이 작업에 관하여

리소스 페이지에서 필요에 따라 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 첨부되고 일정이 구성된 경우 백업은 일정에 따라 자동으로 수행됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.

검색창에 리소스 그룹 이름을 입력하거나 다음을 선택하여 리소스 그룹을 검색할 수 있습니다.  , 그리고 태그를 선택합니다. 그런 다음 선택할 수 있습니다.  필터 창을 닫으려면.

3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음, *지금 백업*을 선택합니다.
4. 백업 페이지에서 다음 단계를 수행합니다.

- a. 리소스 그룹에 여러 정책을 연결한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. *백업*을 선택하세요.

5. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

SAP HANA 데이터베이스 백업 작업 모니터링

SnapCenterJobs 페이지를 사용하여 다양한 백업 작업의 진행 상황을 모니터링할 수 있습니다. 완료 시점이나 문제가 있는지 확인하기 위해 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 해당 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.

- a. 딸깍 하는 소리  백업 작업만 나열되도록 목록을 필터링합니다.
- b. 시작일과 종료일을 지정하세요.
- c. 유형 드롭다운 목록에서 *백업*을 선택합니다.
- d. 상태 드롭다운에서 백업 상태를 선택합니다.
- e. *적용*을 클릭하면 작업이 성공적으로 완료된 것을 볼 수 있습니다.

4. 백업 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인하세요.



백업 작업 상태가 표시됩니다.  작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 표시가 되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

활동 창에서 **SAP HANA** 데이터베이스의 데이터 보호 작업을 모니터링합니다.

활동 창에는 가장 최근에 수행된 5개의 작업이 표시됩니다. 활동 창에는 작업이 시작된 시점과 작업 상태도 표시됩니다.

활동 창에는 백업, 복원, 복제 및 예약된 백업 작업에 대한 정보가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 딸깍 하는 소리  활동 창에서 가장 최근의 작업 5개를 확인하세요.

작업 중 하나를 클릭하면 작업 세부 정보가 작업 세부 정보 페이지에 나열됩니다.

SAP HANA에 대한 백업 작업 취소

대기 중인 백업 작업을 취소할 수 있습니다.

필요한 것

- 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 모니터 페이지나 활동 창에서 백업 작업을 취소할 수 있습니다.
- 실행 중인 백업 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 백업 작업을 취소할 수 있습니다.
- 취소할 수 없는 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 백업 작업을 취소할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	a. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. b. 작업을 선택한 다음 *작업 취소*를 클릭합니다.
활동 창	a. 백업 작업을 시작한 후 *를 클릭하세요.  * 활동 창에서 가장 최근의 작업 5개를 확인하세요. b. 작업을 선택하세요. c. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

작업이 취소되고 리소스는 이전 상태로 돌아갑니다.

토폴로지 페이지에서 **SAP HANA** 데이터베이스 백업 및 복제본 보기

리소스를 백업하거나 복제할 준비를 할 때 기본 및 보조 저장소에 있는 모든 백업과 복제본을 그래픽으로 표현해 보면 도움이 될 수 있습니다.

이 작업에 관하여

다음 아이콘을 '사본 관리' 보기에서 검토하여 백업 및 복제본을 기본 저장소 또는 보조 저장소(미러 사본 또는 볼트 사본)에서 사용할 수 있는지 확인할 수 있습니다.

-  기본 스토리지에서 사용 가능한 백업 및 복제본의 수를 표시합니다.
-  SnapMirror 기술을 사용하여 보조 저장소에 미러링된 백업 및 복제본의 수를 표시합니다.
-  SnapVault 기술을 사용하여 보조 저장소에 복제된 백업 및 복제본의 수를 표시합니다.



표시된 백업 수에는 보조 저장소에서 삭제된 백업이 포함됩니다. 예를 들어, 4개의 백업만 보존하는 정책을 사용하여 6개의 백업을 만든 경우 표시되는 백업 수는 6개입니다.



미러 볼트 유형 볼륨의 버전 가변형 미러 백업의 복제본은 토폴로지 보기에 표시되지만, 토폴로지 보기의 미러 백업 수에는 버전 가변형 백업이 포함되지 않습니다.

토폴로지 페이지에서는 선택한 리소스 또는 리소스 그룹에 사용 가능한 모든 백업과 복제본을 볼 수 있습니다. 해당 백업 및 복제의 세부 정보를 보고 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

SnapMirror Active Sync(처음에는 SnapMirror Business Continuity[SM-BC]로 출시됨)라는 보조 관계가 있는 경우 다음과 같은 추가 아이콘을 볼 수 있습니다.

-  복제 사이트가 오픈되었습니다.

-  복제 사이트가 다운되었습니다.
-  2차 거울이나 볼트 관계가 재설정되지 않았습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 리소스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 리소스를 선택합니다.

리소스가 보호된 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. *요약 카드*를 검토하여 기본 및 보조 저장소에서 사용 가능한 백업 및 복제본 수에 대한 요약 확인하세요.

요약 카드 섹션에는 파일 기반 백업, 스냅샷 복사 기반 백업 및 복제본의 총 수가 표시됩니다.

새로 고침 버튼을 클릭하면 저장소에 대한 쿼리가 시작되어 정확한 개수가 표시됩니다.

SnapLock 이 활성화된 백업을 수행한 경우 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간이 새로 고쳐집니다. 주간 일정은 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간도 새로 고칩니다.

애플리케이션 리소스가 여러 볼륨에 분산되어 있는 경우 백업에 대한 SnapLock 만료 시간은 볼륨의 스냅샷에 설정된 가장 긴 SnapLock 만료 시간이 됩니다. 가장 긴 SnapLock 만료 시간은 ONTAP 에서 검색됩니다.

SnapMirror 활성화 동기화의 경우, 새로 고침 버튼을 클릭하면 ONTAP 기본 사이트와 복제 사이트를 모두 쿼리하여 SnapCenter 백업 인벤토리가 새로 고쳐집니다. 주간 일정은 SnapMirror 활성화 동기화 관계가 포함된 모든 데이터베이스에 대해 이 활동을 수행합니다.

- SnapMirror 활성화 동기화 및 ONTAP 9.14.1의 경우에만 장애 조치 후 새 기본 대상에 대한 비동기 미러 또는 비동기 MirrorVault 관계를 수동으로 구성해야 합니다. ONTAP 9.15.1부터 비동기 미러 또는 비동기 미러볼트가 새로운 기본 대상으로 자동 구성됩니다.
- 장애 조치 후에는 SnapCenter 에서 장애 조치를 인식할 수 있도록 백업을 만들어야 합니다. 백업이 생성된 후에만 *새로 고침*을 클릭할 수 있습니다.

5. 복사본 관리 보기에서 기본 또는 보조 저장소의 백업 또는 *복제*를 클릭하면 백업 또는 복제의 세부 정보를 볼 수 있습니다.

백업 및 복제의 세부 정보는 표 형식으로 표시됩니다.

6. 표에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 복제, 삭제 작업을 수행합니다.



보조 저장소에 있는 백업은 이름을 바꾸거나 삭제할 수 없습니다.

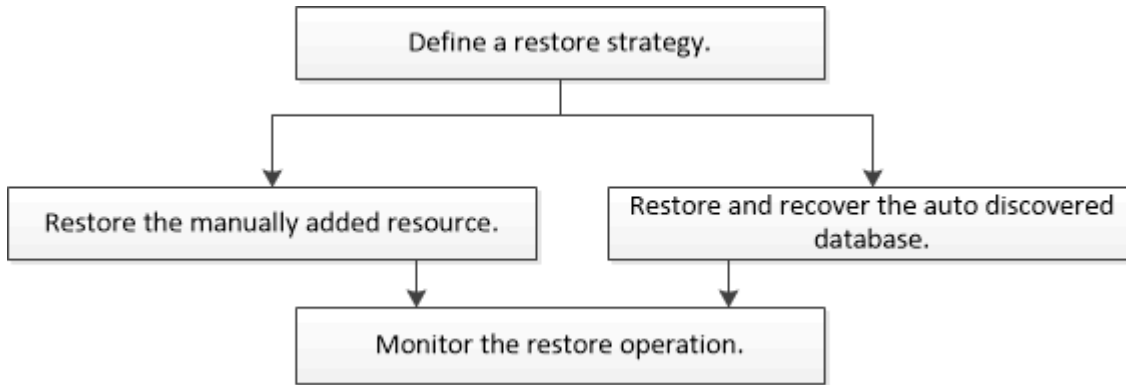
7. 복제본을 삭제하려면 테이블에서 복제본을 선택한 다음 클릭하세요. .
8. 복제본을 분할하려면 테이블에서 복제본을 선택한 다음 클릭하세요. .

SAP HANA 데이터베이스 복원

워크플로 복원

복원 및 복구 워크플로에는 계획, 복원 작업 수행, 작업 모니터링이 포함됩니다.

다음 워크플로는 복원 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

수동으로 추가된 리소스 백업을 복원하고 복구합니다.

SnapCenter 사용하면 하나 이상의 백업에서 데이터를 복원하고 복구할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 복원하려는 리소스 또는 리소스 그룹에 대해 현재 진행 중인 모든 백업 작업을 취소해야 합니다.
- 사전 복원, 사후 복원, 마운트 및 마운트 해제 명령의 경우, 다음 경로에서 플러그인 호스트에서 사용 가능한 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 호스트의 기본 위치: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- 파일 기반 백업 사본은 SnapCenter 에서 복원할 수 없습니다.
- SnapCenter 4.3으로 업그레이드한 후 SnapCenter 4.2에서 수행한 백업은 복원할 수 있지만 복구할 수는 없습니다. SnapCenter 4.2에서 수행한 백업을 복구하려면 SnapCenter 외부의 HANA 스튜디오 또는 HANA 복구 스크립트를 사용해야 합니다.
- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

- SnapMirror Active Sync 복원 작업의 경우 기본 위치에서 백업을 선택해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 함께 표시됩니다.



백업은 리소스 그룹을 위한 것일 수 있지만 복원할 때는 복원할 개별 리소스를 선택해야 합니다.

리소스가 보호되지 않은 경우 전체 상태 열에 "보호되지 않음"이 표시됩니다. 이는 리소스가 보호되지 않았거나 다른 사용자가 리소스를 백업했음을 의미할 수 있습니다.

3. 리소스를 선택하거나 리소스 그룹을 선택한 다음 해당 그룹에서 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 기본 백업 테이블에서 복원하려는 백업을 선택한 다음 *를 클릭합니다. .

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scscr0191685001_01-05-2017-01.35.06.6463	1/5/2017 1:35:27 AM 

6. 복원 범위 페이지에서 전체 리소스 또는 *파일 수준*을 선택합니다.
 - a. *전체 리소스*를 선택하면 SAP HANA 데이터베이스의 구성된 모든 데이터 볼륨이 복원됩니다.

리소스에 볼륨이나 Q트리가 포함되어 있는 경우 해당 볼륨이나 Q트리에서 복원을 위해 선택한 스냅샷 이후에 생성된 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 다른 리소스가 동일한 볼륨이나 Q트리에 호스팅된 경우 해당 리소스도 삭제됩니다.
 - b. *파일 수준*을 선택하면 *모두*를 선택하거나 특정 볼륨이나 Qtree를 선택한 다음 해당 볼륨이나 Qtree와 관련된 경로를 쉼표로 구분하여 입력할 수 있습니다.
 - 여러 개의 볼륨과 Q트리를 선택할 수 있습니다.
 - 리소스 유형이 LUN인 경우 전체 LUN이 복원됩니다.

여러 개의 LUN을 선택할 수 있습니다.



*모두*를 선택하면 볼륨, Q트리 또는 LUN의 모든 파일이 복원됩니다.

7. 사전 작업 페이지에서 복원 작업을 수행하기 전에 실행할 사전 복원 및 마운트 해제 명령을 입력합니다.

자동 검색된 리소스에는 마운트 해제 명령을 사용할 수 없습니다.

8. Post ops 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.

자동 검색된 리소스에는 마운트 명령을 사용할 수 없습니다.

9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > 전역 설정 페이지에서도 구성해야 합니다.

10. 요약을 검토한 후 *마침*을 클릭하세요.

11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-Smconnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

이 예에서는 2015년 1월 29일부터 2015년 2월 3일까지의 백업에 대한 자세한 정보를 표시합니다.

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

자동 검색된 데이터베이스 백업을 복원하고 복구합니다.

SnapCenter 사용하면 하나 이상의 백업에서 데이터를 복원하고 복구할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 복원하려는 리소스 또는 리소스 그룹에 대해 현재 진행 중인 모든 백업 작업을 취소해야 합니다.
- 사전 복원, 사후 복원, 마운트 및 마운트 해제 명령의 경우, 다음 경로에서 플러그인 호스트에서 사용 가능한 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

◦ Linux 호스트의 기본 위치: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- 파일 기반 백업 사본은 SnapCenter 에서 복원할 수 없습니다.
- SnapCenter 4.3으로 업그레이드한 후 SnapCenter 4.2에서 수행한 백업은 복원할 수 있지만 복구할 수는 없습니다. SnapCenter 4.2에서 수행한 백업을 복구하려면 SnapCenter 외부의 HANA 스튜디오 또는 HANA 복구 스크립트를 사용해야 합니다.
- ONTAP 9.12.1 및 이전 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속합니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.
- SnapMirror Active Sync 복원 작업의 경우 기본 위치에서 백업을 선택해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 함께 표시됩니다.



백업은 리소스 그룹을 위한 것일 수 있지만 복원할 때는 복원할 개별 리소스를 선택해야 합니다.

리소스가 보호되지 않은 경우 전체 상태 열에 "보호되지 않음"이 표시됩니다. 이는 리소스가 보호되지 않았거나 다른 사용자가 리소스를 백업했음을 의미할 수 있습니다.

3. 리소스를 선택하거나 리소스 그룹을 선택한 다음 해당 그룹에서 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 기본 백업 테이블에서 복원하려는 백업을 선택한 다음 *를 클릭합니다.  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scspr0191683001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. 복원 범위 페이지에서 *전체 리소스*를 선택하여 SAP HANA 데이터베이스의 구성된 데이터 볼륨을 복원합니다.



전체 리소스(볼륨 되돌리기* 포함 또는 미포함) 또는 *테넌트 데이터베이스*를 선택할 수 있습니다.

사용자가 테넌트 데이터베이스 또는 전체 복원 옵션을 선택하는 경우 SnapCenter Server는 여러 테넌트에 대한 복구 작업을 지원하지 않습니다. 복구 작업을 수행하려면 HANA Studio 또는 HANA Python 스크립트를 사용해야 합니다.

a. 전체 볼륨을 복원하려면 *볼륨 되돌리기*를 선택하세요.

이 옵션은 NFS 환경의 SnapCenter 4.3에서 수행된 백업에 사용할 수 있습니다.

리소스에 볼륨이나 Q트리가 포함되어 있는 경우 해당 볼륨이나 Q트리에서 복원을 위해 선택한 스냅샷 이후에 생성된 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 동일한 볼륨이나 Q트리에 다른 리소스가 호스팅되는 경우 해당 리소스도 삭제됩니다. 이는 복원을 위해 볼륨 되돌리기 옵션이 포함된 *리소스 완료*를 선택한 경우에 적용됩니다.

b. *테넌트 데이터베이스*를 선택하세요.

이 옵션은 MDC 리소스에만 사용할 수 있습니다.

복원 작업을 수행하기 전에 테넌트 데이터베이스를 중지해야 합니다.

테넌트 데이터베이스 옵션을 선택하는 경우 HANA Studio를 사용하거나 SnapCenter 외부의 HANA 복구 스크립트를 사용하여 복구 작업을 수행해야 합니다.

7. 복구 범위 페이지에서 다음 옵션 중 하나를 선택하세요.

만약 당신이...	이렇게 하세요...
현재 시간에 최대한 가깝게 복구하고 싶습니다.	*최근 상태로 복구*를 선택하세요. 단일 컨테이너 리소스의 경우 하나 이상의 로그 및 카탈로그 백업 위치를 지정합니다. 멀티테넌트 데이터베이스 컨테이너(MDC) 리소스의 경우 하나 이상의 로그 백업 위치와 백업 카탈로그 위치를 지정합니다. MDC 리소스의 경우 경로에는 시스템 데이터베이스 로그와 테넌트 데이터베이스 로그가 모두 포함되어야 합니다.

만약 당신이...	이렇게 하세요...
지정된 시점으로 복구하고 싶습니다	*특정 시점으로 복구*를 선택합니다. a. 시간대를 선택하세요. 브라우저 시간대는 기본적으로 입력됩니다. 선택한 시간대와 입력된 시간은 절대 GMT로 변환됩니다. b. 날짜와 시간을 입력하세요. 예를 들어, HANA Linux 호스트는 캘리포니아주 서니베일에 위치하고 노스캐롤라이나주 롤리의 사용자는 SnapCenter 로 로그인을 복구하고 있습니다. 두 위치 간의 시간 차이는 3시간이며, 사용자가 노스캐롤라이나주 롤리에서 로그인했으므로 GUI에서 선택되는 기본 브라우저 시간대는 GMT-04:00입니다. 사용자가 오전 5시(캘리포니아주 선니베일)로 복구를 수행하려는 경우 사용자는 브라우저 시간대를 HANA Linux 호스트 시간대(GMT-07:00)로 설정하고 날짜와 시간을 오전 5시로 지정해야 합니다. 단일 컨테이너 리소스의 경우 하나 이상의 로그 및 카탈로그 백업 위치를 지정합니다. MDC 리소스의 경우 하나 이상의 로그 백업 위치와 백업 카탈로그 위치를 지정합니다. MDC 리소스의 경우 경로에는 시스템 데이터베이스 로그와 테넌트 데이터베이스 로그가 모두 포함되어야 합니다.
특정 데이터 백업으로 복구하고 싶습니다	*지정된 데이터 백업으로 복구*를 선택합니다.
복구하고 싶지 않아요	*복구 안 함*을 선택하세요. HANA Studio에서 수동으로 복구 작업을 수행해야 합니다.

호스트와 플러그인이 모두 SnapCenter 4.3으로 업그레이드되었고, 복원을 위해 선택한 백업이 리소스가 자동 검색된 리소스로 변환되거나 검색된 후에 수행된 경우, SnapCenter 4.3으로 업그레이드한 후에 수행된 백업만 복구할 수 있습니다.

8. 사전 작업 페이지에서 복원 작업을 수행하기 전에 실행할 사전 복원 및 마운트 해제 명령을 입력합니다.

자동 검색된 리소스에는 마운트 해제 명령을 사용할 수 없습니다.

9. Post ops 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.

자동 검색된 리소스에는 마운트 명령을 사용할 수 없습니다.

10. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > 전역 설정 페이지에서도 구성해야 합니다.

11. 요약을 검토한 후 *마침*을 클릭하세요.
12. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet을 사용하여 리소스 복원

리소스 백업을 복원하려면 SnapCenter 서버와 연결 세션을 시작하고, 백업을 나열하고 백업 정보를 검색하고, 백업을 복원해야 합니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-Smconnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----
1	Payroll Dataset_vise-f6_08... 8/4/2015	11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08... 8/4/2015	11:23:17 AM

이 예에서는 2015년 1월 29일부터 2015년 2월 3일까지의 백업에 대한 자세한 정보를 표시합니다.

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName        : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName        : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

SAP HANA 데이터베이스 복원 작업 모니터링

작업 페이지를 사용하여 다양한 SnapCenter 복원 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

복원 후 상태는 복원 작업 후 리소스의 조건과 수행할 수 있는 추가 복원 작업을 설명합니다.

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중

-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복원 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복원*을 선택합니다.
 - d. 상태 드롭다운 목록에서 복원 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복원 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

SAP HANA 리소스 백업 복제

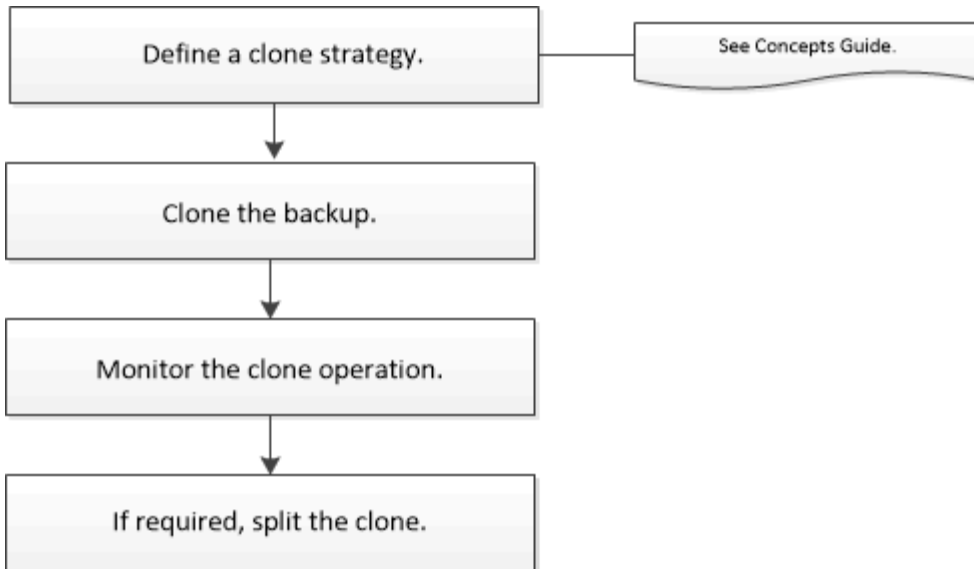
복제 워크플로

복제 워크플로에는 복제 작업을 수행하고 작업을 모니터링하는 작업이 포함됩니다.

이 작업에 관하여

- 소스 SAP HANA 서버에서 복제할 수 있습니다.
- 다음과 같은 이유로 리소스 백업을 복제할 수 있습니다.
 - 애플리케이션 개발 주기 동안 현재 리소스 구조 및 콘텐츠를 사용하여 구현해야 하는 기능을 테스트하려면
 - 데이터 웨어하우스를 채울 때 데이터 추출 및 조작 도구
 - 실수로 삭제되거나 변경된 데이터를 복구하려면

다음 워크플로는 복제 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

SAP HANA 데이터베이스 백업 복제

SnapCenter 사용하여 백업을 복제할 수 있습니다. 기본 또는 보조 백업에서 복제할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 볼륨을 호스팅하는 집계 스토리지 가상 머신(SVM)의 할당된 집계 목록에 있는지 확인해야 합니다.
- 파일 기반 백업은 복제할 수 없습니다.
- 대상 복제 서버는 대상 복제 SID 필드에 제공된 것과 동일한 SAP HANA 인스턴스 SID를 가져야 합니다.
- 복제 전 또는 복제 후 명령의 경우, 플러그인 호스트에서 다음 경로의 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows의 경우: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux의 경우: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- 복제 분할 작업 제한 사항에 대한 정보는 다음을 참조하세요. ["ONTAP 9 논리 스토리지 관리 가이드"](#).
- ONTAP 9.12.1 및 이전 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속합니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 같은 정보와 함께 표시됩니다.

3. 리소스 또는 리소스 그룹을 선택하세요.

리소스 그룹을 선택하는 경우 리소스를 선택해야 합니다.

리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 표에서 데이터 백업을 선택한 다음 클릭하세요.  .
6. 위치 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
플러그인 호스트	복제본을 마운트하고 플러그인을 설치할 호스트를 선택합니다.
대상 복제 SID	기존 백업에서 복제하려면 SAP HANA 인스턴스 ID를 입력하세요.
NFS 내보내기 IP 주소	복제된 볼륨을 내보낼 IP 주소나 호스트 이름을 입력합니다.
iSCSI 이니시에이터	LUN이 내보내질 호스트의 iSCSI 초기자 이름을 입력합니다. 이 옵션은 LUN 리소스 유형을 선택한 경우에만 사용할 수 있습니다.
규약	LUN 프로토콜을 입력하세요. 이 옵션은 LUN 리소스 유형을 선택한 경우에만 사용할 수 있습니다.

선택한 리소스가 LUN이고 보조 백업에서 복제하는 경우 대상 볼륨이 나열됩니다. 단일 소스에는 여러 개의 대상 볼륨이 있을 수 있습니다.



복제하기 전에 iSCSI 이니시에이터 또는 FCP가 있는지, 대체 호스트에 구성되어 로그인되어 있는지 확인해야 합니다.

7. 스크립트 페이지에서 다음 단계를 수행합니다.



스크립트는 플러그인 호스트에서 실행됩니다.

a. 복제 작업 전이나 후에 실행해야 하는 사전 복제 또는 사후 복제에 대한 명령을 각각 입력합니다.

- 사전 복제 명령: 동일한 이름을 가진 기존 데이터베이스 삭제
- 복제 후 명령: 데이터베이스를 확인하거나 데이터베이스를 시작합니다.

b. 호스트에 파일 시스템을 마운트하려면 mount 명령을 입력하세요.

Linux 머신에서 볼륨이나 qtree에 대한 마운트 명령:

NFS의 예: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

10. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-SmConnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146/
```

2. Get-SmBackup cmdlet을 사용하여 복제 작업을 수행하기 위해 백업을 검색합니다.

이 예에서는 복제에 사용할 수 있는 백업이 두 개 있음을 보여줍니다.

```
C:\PS> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
1	Payroll Dataset_vise-f6_08...
8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...
8/4/2015 11:23:17 AM	

3. 기존 백업에서 복제 작업을 시작하고 복제된 볼륨이 내보내지는 NFS 내보내기 IP 주소를 지정합니다.

이 예에서는 복제할 백업의 NFSExportIPs 주소가 10.232.206.169임을 보여줍니다.

```
New-SmClone -AppPluginCode hana -BackupName
scscscore1_sscore_test_com_hana_H73_scscscore1_06-07-
2017_02.54.29.3817 -Resources
@{"Host"="scscscore1.sscore.test.com";"Uid"="H73"} -CloneToInstance
shivsc4.sscore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data'
-preclonecreatecommands '/home/scripts/scpre_clone.sh'
-postclonecreatecommands '/home/scripts/scpost_clone.sh'
```



NFSExportIPs가 지정되지 않으면 기본값이 복제 대상 호스트로 내보내집니다.

4. Get-SmCloneReport cmdlet을 사용하여 복제 작업 세부 정보를 보고 백업이 성공적으로 복제되었는지 확인합니다.

클론 ID, 시작 날짜 및 시간, 종료 날짜 및 시간과 같은 세부 정보를 볼 수 있습니다.

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration              : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName            : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName      : OnDemand_Full_Log
SmBackupPolicyId     : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId          : 4
CloneName            : Draper__clone__08-03-2015_14.43.53
SourceResources       : {Don, Betty, Bobby, Sally}
ClonedResources       : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError            :
```

SAP HANA 데이터베이스 복제 작업 모니터링

작업 페이지를 사용하여 SnapCenter 복제 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복제 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복제*를 선택합니다.
 - d. 상태 드롭다운 목록에서 복제 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복제 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

클론 분할

SnapCenter 사용하면 복제된 리소스를 부모 리소스에서 분할할 수 있습니다. 분할된 복제본은 부모 리소스로부터 독립됩니다.

이 작업에 관하여

- 중간 복제본에서는 복제 분할 작업을 수행할 수 없습니다.

예를 들어, 데이터베이스 백업에서 clone1을 만든 후 clone1의 백업을 만든 다음 이 백업(clone2)을 복제할 수 있습니다. clone2를 생성한 후 clone1은 중간 복제본이 되며 clone1에서 복제 분할 작업을 수행할 수 없습니다. 하지만 clone2에 대해 클론 분할 작업을 수행할 수 있습니다.

clone2를 분할한 후에는 clone1에 대해 clone 분할 작업을 수행할 수 있습니다. clone1은 더 이상 중간 클론이 아니기 때문입니다.

- 복제본을 분할하면 복제본의 백업 사본과 복제 작업이 삭제됩니다.
- FlexClone 볼륨 분할 작업에 대한 정보는 다음을 참조하세요. "[FlexClone 볼륨을 부모 볼륨에서 분할합니다.](#)".
- 스토리지 시스템의 볼륨이나 집계가 온라인인지 확인하세요.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 적절한 옵션을 선택하세요.

옵션	설명
데이터베이스 애플리케이션의 경우	보기 목록에서 *데이터베이스*를 선택합니다.
파일 시스템의 경우	보기 목록에서 *경로*를 선택합니다.

3. 목록에서 적절한 리소스를 선택하세요.

리소스 토폴로지 페이지가 표시됩니다.

4. 사본 관리 보기에서 복제된 리소스(예: 데이터베이스 또는 LUN)를 선택한 다음 *를 클릭합니다.  *.
5. 분할할 클론의 예상 크기와 집계에 필요한 사용 가능한 공간을 검토한 다음 *시작*을 클릭합니다.
6. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

SMCore 서비스를 다시 시작하면 복제 분할 작업이 더 이상 응답하지 않습니다. 복제 분할 작업을 중지하려면 Stop-SmJob cmdlet을 실행한 다음 복제 분할 작업을 다시 시도해야 합니다.

복제본이 분할되었는지 여부를 확인하기 위해 더 긴 폴링 시간이나 더 짧은 폴링 시간이 필요한 경우 *SMCoreServiceHost.exe.config* 파일에서 *CloneSplitStatusCheckPollTime* 매개변수 값을 변경하여 SMCore가 복제본 분할 작업의 상태를 폴링하는 시간 간격을 설정할 수 있습니다. 값은 밀리초이고 기본값은 5분입니다.

예를 들어:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

백업, 복원 또는 다른 클론 분할이 진행 중이면 클론 분할 시작 작업이 실패합니다. 실행 중인 작업이 완료된 후에만 복제 분할 작업을 다시 시작해야 합니다.

관련 정보

"SnapCenter 복제 또는 검증이 집계 존재하지 않아 실패합니다."

SnapCenter 업그레이드 후 SAP HANA 데이터베이스 복제본 삭제 또는 분할

SnapCenter 4.3으로 업그레이드한 후에는 더 이상 복제본이 표시되지 않습니다. 복제본이 생성된 리소스의 토폴로지 페이지에서 복제본을 삭제하거나 분할할 수 있습니다.

이 작업에 관하여

숨겨진 복제본의 저장 공간을 찾으려면 다음 명령을 실행하세요. `Get-SmClone -ListStorageFootprint`

단계

1. remove-smbbackup cmdlet을 사용하여 복제된 리소스의 백업을 삭제합니다.

2. remove-smresourcegroup cmdlet을 사용하여 복제된 리소스의 리소스 그룹을 삭제합니다.
3. remove-smprotectresource cmdlet을 사용하여 복제된 리소스의 보호를 제거합니다.
4. 리소스 페이지에서 상위 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

5. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 복제본을 선택합니다.
6. 복제본을 선택한 다음 클릭하세요.  클론을 삭제하거나 클릭하세요  클론을 분할합니다.
7. *확인*을 클릭합니다.

Oracle 데이터베이스 보호

Oracle Database용 SnapCenter 플러그인 개요

Oracle Database용 플러그인으로 무엇을 할 수 있나요?

Oracle Database용 SnapCenter 플러그인은 Oracle 데이터베이스의 애플리케이션 인식 데이터 보호 관리를 가능하게 하는 NetApp SnapCenter 소프트웨어의 호스트 측 구성 요소입니다.

Oracle Database용 플러그인은 SnapCenter 환경에서 Oracle 데이터베이스의 백업, 카탈로그화 및 카탈로그 해제, 검증, 마운트, 마운트 해제, 복원, 복구 및 복제를 자동화합니다. Oracle Database용 플러그인은 UNIX용 SnapCenter 플러그인을 설치하여 모든 데이터 보호 작업을 수행합니다.

Oracle Database용 플러그인을 사용하면 SAP 애플리케이션을 실행하는 Oracle 데이터베이스의 백업을 관리할 수 있습니다. 하지만 SAP BR*Tools 통합은 지원되지 않습니다.

- 데이터 파일, 제어 파일, 보관 로그 파일을 백업합니다.

백업은 컨테이너 데이터베이스(CDB) 수준에서만 지원됩니다.

- 데이터베이스, CDB, 플러그형 데이터베이스(PDB)의 복원 및 복구.

PDB의 불완전한 복구는 지원되지 않습니다.

- 특정 시점까지의 프로덕션 데이터베이스 복제본을 만듭니다.

복제는 CDB 수준에서만 지원됩니다.

- 백업을 즉시 확인하세요.
- 복구 작업을 위해 데이터와 로그 백업을 마운트 및 마운트 해제합니다.
- 백업 및 검증 작업을 예약합니다.
- 모든 작업을 모니터링합니다.
- 백업, 복원 및 복제 작업에 대한 보고서를 확인합니다.
- SnapCenter 환경에서 Oracle 데이터베이스에 대한 애플리케이션 인식 백업, 복원, 복구, 검증, 마운트, 마운트 해제 및 복제 작업을 자동화합니다.
- SAP용 Oracle 데이터베이스를 지원하지만 SAP BR*Tools 통합은 제공되지 않습니다.

Oracle Database용 플러그인의 특징

Oracle Database용 플러그인은 Linux 또는 AIX 호스트의 Oracle 데이터베이스와 통합되고, 스토리지 시스템의 NetApp 기술과 통합됩니다.

- 통합된 그래픽 사용자 인터페이스

SnapCenter 인터페이스는 플러그인과 환경 전반에 걸쳐 표준화와 일관성을 제공합니다. SnapCenter

인터페이스를 사용하면 플러그인 전반에 걸쳐 일관된 백업, 복원, 복구 및 복제 작업을 완료하고, 중앙 집중식 보고를 사용하고, 한눈에 보이는 대시보드 보기를 사용하고, 역할 기반 액세스 제어(RBAC)를 설정하고, 모든 플러그인에서 작업을 모니터링할 수 있습니다.

- 자동화된 중앙 관리

백업 및 복제 작업을 예약하고, 정책 기반 백업 보존을 구성하고, 복원 작업을 수행할 수 있습니다. SnapCenter 구성하여 이메일 알림을 보내 환경을 사전에 모니터링할 수도 있습니다.

- 중단 없는 NetApp 스냅샷 기술

SnapCenter Oracle Database용 플러그인과 UNIX용 플러그인과 함께 NetApp Snapshot 기술을 사용하여 데이터베이스를 백업합니다. 스냅샷은 최소한의 저장 공간을 차지합니다.

Oracle Database용 플러그인은 다음과 같은 이점도 제공합니다.

- 백업, 복원, 복제, 마운트, 마운트 해제 및 검증 워크플로 지원
- 호스트에 구성된 Oracle 데이터베이스의 자동 검색
- Oracle Recovery Manager(RMAN)를 사용한 카탈로그화 및 카탈로그화 해제 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임

또한, 권한이 있는 SnapCenter 사용자에게 애플리케이션 수준 권한이 부여되도록 자격 증명을 설정할 수도 있습니다.

- 복원 및 복제 작업을 위한 ALM(아카이브 로그 관리) 지원
- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 프로덕션 데이터베이스의 공간 효율적인 특정 시점 복사본 생성

복제본을 생성하려는 스토리지 시스템에 FlexClone 라이선스가 필요합니다.

- SAN 및 ASM 환경에서 백업을 생성하는 일부로 ONTAP의 일관성 그룹(CG) 기능 지원
- 중단 없는 자동 백업 검증
- 여러 데이터베이스 호스트에서 동시에 여러 백업을 실행할 수 있는 기능

단일 호스트의 데이터베이스가 동일한 볼륨을 공유하는 경우 단일 작업으로 스냅샷이 통합됩니다.

- 물리적 및 가상화된 인프라 지원
- NFS, iSCSI, 파이버 채널(FC), RDM, NFS 및 VMFS를 통한 VMDK, NFS, SAN, RDM 및 VMDK를 통한 ASM 지원
- ONTAP의 SLM(Selective LUN Map) 기능 지원

기본적으로 활성화된 SLM 기능은 최적화된 경로가 없는 LUN을 주기적으로 검색하여 수정합니다. /var/opt/snapcenter/scu/etc에 있는 scu.properties 파일의 매개변수를 수정하여 SLM을 구성할 수 있습니다.

- ENABLE_LUNPATH_MONITORING 매개변수 값을 false로 설정하면 이 기능을 비활성화할 수 있습니다.
- LUNPATH_MONITORING_INTERVAL 매개변수에 값(시간)을 할당하여 LUN 경로가 자동으로 수정되는 빈도를 지정할 수 있습니다. SLM에 대한 정보는 다음을 참조하세요. ["ONTAP 9 SAN 관리 섹션"](#).

- Linux에서 NVMe(Non-Volatile Memory Express) 지원

- NVMe util은 호스트에 설치되어야 합니다.

대체 호스트에 복제하거나 마운트하려면 NVMe 유틸을 설치해야 합니다.

- 가상화된 환경(예: RDM)을 제외한 NVMe 하드웨어에서는 백업, 복원, 복제, 마운트, 마운트 해제, 카탈로그화, 카탈로그 해제 및 검증 작업이 지원됩니다.

위의 작업은 파티션이 없거나 단일 파티션이 있는 장치에서 지원됩니다.



커널에서 기본 멀티패스 옵션을 설정하여 NVMe 장치에 대한 멀티패스 솔루션을 구성할 수 있습니다. 장치 매핑(DM) 다중 경로가 지원되지 않습니다.

- 백업, 복원, 복제, 마운트, 마운트 해제, 카탈로그화, 카탈로그 해제 및 검증 워크플로는 TCP/IP를 통한 NVMe에서 지원됩니다.
- TCP/IP를 통한 NVMe에서 생성된 VMDK 레이아웃에서는 백업, 복원, 복제, 마운트, 마운트 해제, 카탈로그화, 카탈로그 해제 및 검증 워크플로가 지원됩니다.
- 사이트 전체에 장애가 발생해도 비즈니스 서비스가 계속 운영될 수 있도록 하는 SnapMirror Active Sync(처음에는 SnapMirror Business Continuity[SM-BC]로 출시)를 지원하며, 보조 복사본을 사용하여 애플리케이션이 투명하게 장애 조치되도록 지원합니다. SnapMirror Active Sync를 사용하면 장애 조치를 트리거하는 데 수동 개입이나 추가 스크립팅이 필요하지 않습니다.
- Oracle 및 Grid 대신 기본이 아닌 모든 사용자를 지원합니다.

기본이 아닌 사용자를 지원하려면 `_file /var/opt/snapcenter/sco/etc/_`에 있는 **sco.properties** 파일의 매개변수 값을 수정하여 기본이 아닌 사용자를 설정해야 합니다.

매개변수의 기본값은 oracle과 grid로 설정됩니다.

- DB_USER=오라클
- DB_GROUP=설치
- GI_USER=그리드
- GI_GROUP=설치 안 함

Oracle Database용 플러그인이 지원하는 저장 유형

SnapCenter 물리적 머신과 가상 머신 모두에서 다양한 스토리지 유형을 지원합니다. Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치하기 전에 스토리지 유형에 대한 지원을 확인해야 합니다.

SnapCenter Linux 및 AIX에 대한 스토리지 프로비저닝을 지원하지 않습니다.

Linux에서 지원되는 스토리지 유형

다음 표는 Linux에서 지원되는 저장 유형을 나열합니다.

기계	저장 유형
물리적 서버	• FC 연결 LUN • iSCSI로 연결된 LUN • NFS 연결 볼륨 • NVMe-FC • NVMe/TCP
VMware ESXi	• FC 또는 iSCSI ESXi HBA로 연결된 RDM LUN 호스트 버스 어댑터(HBA) 스캐닝은 SnapCenter 호스트에 있는 모든 호스트 버스 어댑터를 스캔하기 때문에 완료하는 데 오랜 시간이 걸릴 수 있습니다. _/_opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config_에 있는 LinuxConfig.pm 파일을 편집하여 SCSI_HOSTS_OPTIMIZED_RESCAN 매개변수 값을 1로 설정하면 HBA_DRIVER_NAMES에 나열된 HBA만 다시 스캔합니다. • iSCSI 이니시에이터에 의해 게스트 시스템에 직접 연결된 iSCSI LUN • NFS 데이터 저장소의 VMDK • NVMe/TCP를 통해 생성된 VMFS의 VMDK  RAC는 공유 VMDK를 지원하는 ESX 8.0U2에서 지원됩니다. • 게스트 시스템에 직접 연결된 NFS 볼륨 • NFS와 SAN 모두에 있는 vVol 데이터 저장소 vVol 데이터스토어는 VMware vSphere용 ONTAP 도구를 사용해서만 프로비저닝할 수 있습니다.

AIX에서 지원되는 스토리지 유형

다음 표는 AIX에서 지원되는 스토리지 유형을 나열합니다.

기계	저장 유형
물리적 서버	• FC 연결 및 iSCSI 연결 LUN. SAN 환경에서는 ASM, LVM, SAN 파일 시스템이 지원됩니다.  AIX 및 파일 시스템에서는 NFS가 지원되지 않습니다. • 향상된 저널링 파일 시스템(JFS2) SAN 파일 시스템과 LVM 레이아웃에 대한 인라인 로깅을 지원합니다.

그만큼 ["NetApp 상호 운용성 매트릭스 도구"](#) 지원되는 버전에 대한 최신 정보가 포함되어 있습니다.

Oracle용 플러그인을 위한 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비

ONTAP SnapMirror 기술과 함께 SnapCenter 플러그인을 사용하면 다른 볼륨에 백업 세트의 미러 사본을 생성할 수 있으며, ONTAP SnapVault 기술과 함께 사용하면 표준 준수 및 기타 거버넌스 관련 목적으로 디스크 간 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 구성하고 해당 관계를 초기화해야 합니다.

SnapCenter 스냅샷 작업을 완료한 후 SnapMirror와 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행됩니다. SnapMirror 활성 동기화를 사용하는 경우 SnapMirror 활성 동기화와 비동기 관계 모두에 기본 SnapMirror 또는 SnapVault 일정을 사용하세요.



NetApp SnapManager 제품을 통해 SnapCenter에 접속했고 구성된 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 기본 저장소(소스 볼륨)의 데이터를 보조 저장소(대상 볼륨)로 복제합니다. 관계를 초기화하면 ONTAP 소스 볼륨에서 참조되는 데이터 블록을 대상 볼륨으로 전송합니다.



SnapCenter SnapMirror와 SnapVault 볼륨 간의 계단식 관계(**Primary > Mirror > Vault**)를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter 버전에 따라 유연한 SnapMirror 관계 관리를 지원합니다. 버전에 따라 유연한 SnapMirror 관계와 이를 설정하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["ONTAP 문서"](#).

Oracle용 플러그인에 필요한 최소 ONTAP 권한

데이터 보호를 위해 사용하는 SnapCenter 플러그인에 따라 필요한 최소 ONTAP 권한은 다릅니다.

- 모든 액세스 명령: ONTAP 9.12.1 이상에 필요한 최소 권한
 - 이벤트 생성-자동 지원-로그

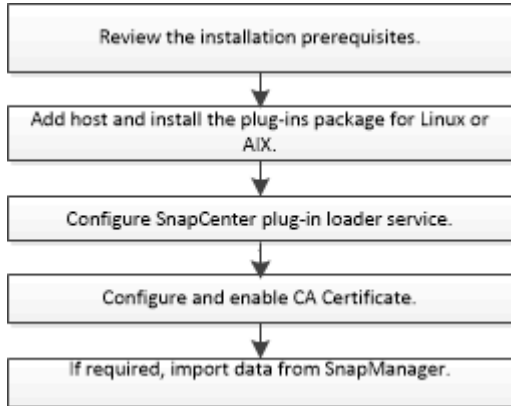
- 직업 이력 표시
- 작업 중지
- 룬
- lun 속성 표시
- lun 생성
- lun 삭제
- LUN 기하학
- lun igroup 추가
- lun igroup 생성
- lun igroup 삭제
- lun igroup 이름 바꾸기
- 룬 아이그룹 쇼
- lun 매핑 add-reporting-nodes
- lun 매핑 생성
- LUN 매핑 삭제
- LUN 매핑 제거-보고-노드
- lun 매핑 쇼
- lun 수정
- lun 이동량
- lun 오프라인
- lun 온라인
- lun 지속적 예약 지우기
- lun 크기 조정
- lun 시리얼
- 룬 쇼
- 스냅미러 정책 추가 규칙
- 스냅미러 정책 수정 규칙
- 스냅미러 정책 제거 규칙
- 스냅미러 정책 보기
- 스냅미러 복원
- 스냅미러 쇼
- 스냅미러 쇼 히스토리
- 스냅미러 업데이트
- 스냅미러 업데이트-ls-세트

- 스냅미러 목록-대상
- 버전
- 볼륨 복제 생성
- 볼륨 클론 쇼
- 볼륨 복제 분할 시작
- 볼륨 클론 분할 정지
- 볼륨 생성
- 볼륨 파괴
- 볼륨 파일 복제 생성
- 볼륨 파일 show-disk-usage
- 볼륨 오프라인
- 온라인 볼륨
- 볼륨 수정
- 볼륨 qtree 생성
- 볼륨 qtree 삭제
- 볼륨 qtree 수정
- 볼륨 qtree 쇼
- 볼륨 제한
- 볼륨 쇼
- 볼륨 스냅샷 생성
- 볼륨 스냅샷 삭제
- 볼륨 스냅샷 수정
- 볼륨 스냅샷 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- v서버
- vserver cifs
- vserver cifs 새도우 카피 쇼
- vserver 쇼
- 네트워크 인터페이스
- 네트워크 인터페이스 표시
- 메트로클러스터 쇼

Oracle Database용 SnapCenter 플러그인 설치

Oracle Database용 SnapCenter 플러그인 설치 워크플로

Oracle 데이터베이스를 보호하려면 Oracle 데이터베이스용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



Linux 또는 AIX용 호스트 추가 및 플러그인 패키지 설치를 위한 전제 조건

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 충족해야 합니다.

- iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.
- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.

Oracle Database용 SnapCenter 플러그인은 루트가 아닌 사용자도 설치할 수 있습니다. 하지만 루트가 아닌 사용자가 플러그인 프로세스를 설치하고 시작하려면 sudo 권한을 구성해야 합니다. 플러그인을 설치한 후에는 프로세스가 루트가 아닌 사용자 권한으로 실행됩니다.

- AIX 호스트에 AIX용 SnapCenter 플러그인 패키지를 설치하는 경우 디렉토리 수준 심볼릭 링크를 수동으로 해결했어야 합니다.

AIX용 SnapCenter 플러그인 패키지는 JAVA_HOME 절대 경로를 얻기 위해 파일 수준 심볼릭 링크는 자동으로 확인하지만 디렉토리 수준 심볼릭 링크는 확인하지 않습니다.

- 설치 사용자에게 대해 Linux 또는 AIX 인증 모드로 자격 증명을 생성합니다.
- Linux 또는 AIX 호스트에 Java 11을 설치했어야 합니다.
 - Linux에서는 Oracle 및 OpenJDK의 Java가 지원됩니다.
 - AIX용 IBM Java. 에서 다운로드할 수 있습니다 ["IBM Semeru 런타임 다운로드"](#)



Linux 호스트에 JAVA 11 인증 버전만 설치했는지 확인하세요.

- Linux 또는 AIX 호스트에서 실행되는 Oracle 데이터베이스의 경우 Oracle Database용 SnapCenter 플러그인과 UNIX용 SnapCenter 플러그인을 모두 설치해야 합니다.



Oracle Database용 플러그인을 사용하면 SAP용 Oracle 데이터베이스도 관리할 수 있습니다. 하지만 SAP BR*Tools 통합은 지원되지 않습니다.

- Oracle 데이터베이스 11.2.0.3 이상을 사용하는 경우 13366202 Oracle 패치를 설치해야 합니다.



SnapCenter 는 /etc/fstab 파일의 UUID 매핑을 지원하지 않습니다.

- 플러그인 설치를 위해 기본 셸로 *bash*를 사용해야 합니다.

Linux 호스트 요구 사항

Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 호스트가 요구 사항을 충족하는지 확인해야 합니다.

목	요구 사항
운영 체제	• 레드햇 엔터프라이즈 리눅스 • 오라클 리눅스  Oracle Linux 또는 Red Hat Enterprise Linux 6.6 또는 7.0 운영 체제에서 LVM에서 Oracle 데이터베이스를 사용하는 경우 최신 버전의 Logical Volume Manager(LVM)를 설치해야 합니다. • SUSE Linux Enterprise Server(SLES)
호스트의 SnapCenter 플러그인을 위한 최소 RAM	2GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.

목	요구 사항
필수 소프트웨어 패키지	Java 11 Oracle 및 OpenJDK  Linux 호스트에 JAVA 11 인증 버전만 설치했는지 확인하세요. JAVA를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties에 있는 JAVA_HOME 옵션이 올바른 JAVA 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다.

지원되는 버전에 대한 최신 정보는 다음을 참조하세요. ["NetApp 상호 운용성 매트릭스 도구"](#).

Linux 호스트에 대한 루트가 아닌 사용자에게 대한 **sudo** 권한 구성

SnapCenter 2.0 및 이후 릴리스에서는 루트가 아닌 사용자도 Linux용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 루트가 아닌 사용자로 실행됩니다. 루트가 아닌 사용자에게 여러 경로에 대한 액세스 권한을 제공하려면 sudo 권한을 구성해야 합니다.

필요한 것

- Sudo 버전 1.8.7 이상.
- umask가 0027인 경우, java 폴더와 그 안에 있는 모든 파일에 555 권한이 있어야 합니다. 그렇지 않으면 플러그인 설치가 실패할 수 있습니다.
- 루트가 아닌 사용자의 경우 루트가 아닌 사용자의 이름과 사용자 그룹이 동일해야 합니다.
- /etc/ssh/sshd_config 파일을 편집하여 메시지 인증 코드 알고리즘(MAC hmac-sha2-256 및 MAC hmac-sha2-512)을 구성합니다.

구성 파일을 업데이트한 후 sshd 서비스를 다시 시작합니다.

예:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

이 작업에 관하여

루트가 아닌 사용자에게 다음 경로에 대한 액세스를 제공하려면 sudo 권한을 구성해야 합니다.

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/ NetApp/snapcenter/spl/설치/플러그인/제거
- /custom_location/ NetApp/snapcenter/spl/bin/spl

단계

1. Linux용 SnapCenter 플러그인 패키지를 설치하려는 Linux 호스트에 로그인합니다.
2. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 줄을 추가합니다.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,  
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,  
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc  
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/Linux_Prechecks.sh  
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config  
_Check.sh  
Cmnd_Alias SCCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/bin/sc_command_executor  
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==  
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor  
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,  
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD  
Defaults: LINUX_USER env_keep += "IATEMPDIR"  
Defaults: LINUX_USER env_keep += "JAVA_HOME"  
Defaults: LINUX_USER !visiblepw  
Defaults: LINUX_USER !requiretty
```



RAC 설정을 사용하는 경우 허용되는 다른 명령과 함께 다음을 /etc/sudoers 파일에 추가해야 합니다. '<crs_home>/bin/olsnodes'

*crs_home*_의 값은 *_etc/oracle/olr.loc* 파일에서 얻을 수 있습니다.

*_LINUX_USER*_는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

*_checksum_value*_는 **sc_unix_plugins_checksum.txt** 파일에서 얻을 수 있습니다. 이 파일의 위치는 다음과 같습니다.

- SnapCenter Server가 Windows 호스트에 설치된 경우 *C:\ProgramData\NetApp\ SnapCenter \Package Repository\sc_unix_plugins_checksum.txt*.
- SnapCenter 서버가 Linux 호스트에 설치되어 있는 경우 */opt/ NetApp /snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt*.



이 예제는 귀하만의 데이터를 생성하기 위한 참고자료로만 사용해야 합니다.

AIX 호스트 요구 사항

AIX용 SnapCenter 플러그인 패키지를 설치하기 전에 호스트가 요구 사항을 충족하는지 확인해야 합니다.



AIX용 SnapCenter 플러그인 패키지의 일부인 UNIX용 SnapCenter 플러그인은 동시 볼륨 그룹을 지원하지 않습니다.

목	요구 사항
운영 체제	AIX 7.1 이상
호스트의 SnapCenter 플러그인을 위한 최소 RAM	4GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	자바 11 IBM 자바 JAVA를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties에 있는 JAVA_HOME 옵션이 올바른 JAVA 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다.

지원되는 버전에 대한 최신 정보는 다음을 참조하세요. ["NetApp 상호 운용성 매트릭스 도구"](#).

AIX 호스트에 대한 루트가 아닌 사용자에게 대한 sudo 권한 구성

SnapCenter 4.4 이상에서는 루트가 아닌 사용자도 AIX용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 루트가 아닌 사용자로 실행됩니다. 루트가 아닌 사용자에게 여러 경로에 대한 액세스 권한을 제공하려면 sudo 권한을 구성해야 합니다.

필요한 것

- Sudo 버전 1.8.7 이상.
- umask가 0027인 경우, java 폴더와 그 안에 있는 모든 파일에 555 권한이 있어야 합니다. 그렇지 않으면 플러그인 설치가 실패할 수 있습니다.
- /etc/ssh/sshd_config 파일을 편집하여 메시지 인증 코드 알고리즘(MAC hmac-sha2-256 및 MAC hmac-sha2-512)을 구성합니다.

구성 파일을 업데이트한 후 sshd 서비스를 다시 시작합니다.

예:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

이 작업에 관하여

루트가 아닌 사용자에게 다음 경로에 대한 액세스를 제공하려면 sudo 권한을 구성해야 합니다.

- /home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /custom_location/ NetApp/snapcenter/spl/설치/플러그인/제거
- /custom_location/ NetApp/snapcenter/spl/bin/spl

단계

1. AIX용 SnapCenter 플러그인 패키지를 설치하려는 AIX 호스트에 로그인합니다.
2. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 줄을 추가합니다.

```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



RAC 설정을 사용하는 경우 허용되는 다른 명령과 함께 다음을 `/etc/sudoers` 파일에 추가해야 합니다. '`<crs_home>/bin/olsnodes`'

`crs_home`의 값은 `_etc/oracle/olr.loc` 파일에서 얻을 수 있습니다.

`_AIX_USER`는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

`_checksum_value`는 `sc_unix_plugins_checksum.txt` 파일에서 얻을 수 있습니다. 이 파일의 위치는 다음과 같습니다.

- SnapCenter Server가 Windows 호스트에 설치된 경우 `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`.
- SnapCenter 서버가 Linux 호스트에 설치되어 있는 경우 `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`.



이 예제는 귀하만의 데이터를 생성하기 위한 참고자료로만 사용해야 합니다.

자격 증명 설정

SnapCenter 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다. Linux 또는 AIX 호스트에 플러그인 패키지를 설치하려면 자격 증명을 만들어야 합니다.

이 작업에 관하여

자격 증명은 루트 사용자 또는 플러그인 프로세스를 설치하고 시작할 수 있는 `sudo` 권한이 있는 루트가 아닌 사용자를 위해 생성됩니다.

자세한 내용은 다음을 참조하세요. [Linux 호스트에 대한 루트가 아닌 사용자에 대한 sudo 권한 구성](#) 또는 [AIX 호스트에 대한 루트가 아닌 사용자에 대한 sudo 권한 구성](#)

모범 사례: 호스트를 배포하고 플러그인을 설치한 후에도 자격 증명을 생성할 수 있지만, 가장 좋은 방법은 SVM을 추가한 후 호스트를 배포하고 플러그인을 설치하기 전에 자격 증명을 생성하는 것입니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *자격 증명*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 자격 증명 페이지에서 자격 증명 정보를 입력하세요.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.
사용자 이름/비밀번호	인증에 사용할 사용자 이름과 비밀번호를 입력하세요. • 도메인 관리자 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자를 지정하세요. 사용자 이름 필드에 사용할 수 있는 형식은 다음과 같습니다. ◦ <i>NetBIOS</i> 사용자 이름 ◦ 도메인 <i>FQDN</i> 사용자 이름 • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우, SnapCenter 플러그인을 설치할 시스템에 기본 제공되는 로컬 관리자를 지정하십시오. 사용자 계정에 승격된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우, 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다. <i>UserName</i>
인증 모드	사용할 인증 모드를 선택하세요. 플러그인 호스트의 운영 체제에 따라 Linux 또는 AIX를 선택하세요.
sudo 권한을 사용하세요	루트가 아닌 사용자에게 자격 증명을 생성하는 경우 sudo 권한 사용 확인란을 선택합니다.

5. *확인*을 클릭합니다.

자격 증명 설정을 마친 후에는 사용자 및 액세스 페이지에서 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

Oracle 데이터베이스에 대한 자격 증명 구성

Oracle 데이터베이스에서 데이터 보호 작업을 수행하는 데 사용되는 자격 증명을 구성해야 합니다.

이 작업에 관하여

Oracle 데이터베이스에서 지원되는 다양한 인증 방법을 검토해야 합니다. 자세한 내용은 다음을 참조하세요. "[자격 증명에 대한 인증 방법](#)".

개별 리소스 그룹에 대한 자격 증명을 설정하고 사용자 이름에 전체 관리자 권한이 없는 경우, 사용자 이름에는 최소한 리소스 그룹 및 백업 권한이 있어야 합니다.

Oracle 데이터베이스 인증을 활성화한 경우 리소스 보기에 빨간색 자물쇠 아이콘이 표시됩니다. 데이터베이스를 보호하거나 리소스 그룹에 추가하여 데이터 보호 작업을 수행하려면 데이터베이스 자격 증명을 구성해야 합니다.



자격 증명을 생성하는 동안 잘못된 세부 정보를 지정하면 오류 메시지가 표시됩니다. *취소*를 클릭한 후 다시 시도하세요.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *데이터베이스*를 선택합니다.
3. 딸깍 하는 소리 그런 다음 호스트 이름과 데이터베이스 유형을 선택하여 리소스를 필터링합니다.

그런 다음 클릭할 수 있습니다 필터 창을 닫으려면.

4. 데이터베이스를 선택한 다음 데이터베이스 설정 > *데이터베이스 구성*을 클릭합니다.
5. 데이터베이스 설정 구성 섹션의 기존 자격 증명 사용 드롭다운 목록에서 Oracle 데이터베이스에서 데이터 보호 작업을 수행하는 데 사용할 자격 증명을 선택합니다.



Oracle 사용자는 sysdba 권한이 있어야 합니다.

또한 다음을 클릭하여 자격 증명을 만들 수도 있습니다. .

6. ASM 설정 구성 섹션의 기존 자격 증명 사용 드롭다운 목록에서 ASM 인스턴스에서 데이터 보호 작업을 수행하는 데 사용할 자격 증명을 선택합니다.



ASM 사용자는 sysasm 권한이 있어야 합니다.

또한 다음을 클릭하여 자격 증명을 만들 수도 있습니다. .

7. RMAN 카탈로그 설정 구성 섹션의 기존 자격 증명 사용 드롭다운 목록에서 Oracle Recovery Manager(RMAN) 카탈로그 데이터베이스에서 데이터 보호 작업을 수행하는 데 사용할 자격 증명을 선택합니다.

또한 다음을 클릭하여 자격 증명을 만들 수도 있습니다. .

TNSName 필드에 SnapCenter 서버가 데이터베이스와 통신하는 데 사용할 TNS(Transparent Network Substrate) 파일 이름을 입력합니다.

8. 선호하는 **RAC** 노드 필드에서 백업에 선호하는 RAC(Real Application Cluster) 노드를 지정합니다.

선호되는 노드는 RAC 데이터베이스 인스턴스가 있는 하나 또는 모든 클러스터 노드일 수 있습니다. 백업 작업은 선호도 순서대로 이러한 선호 노드에서만 실행됩니다.

RAC One Node에서는 기본 노드에 노드가 하나만 나열되어 있으며, 이 기본 노드는 현재 데이터베이스가 호스팅되는 노드입니다.

RAC One Node 데이터베이스를 장애 조치하거나 이전한 후 SnapCenter 리소스 페이지에서 리소스를 새로 고치면 이전에 데이터베이스가 호스팅되었던 선호 **RAC** 노드 목록에서 호스트가 제거됩니다. 데이터베이스가 이전된 RAC 노드는 *RAC 노드*에 나열되며, 기본 RAC 노드로 수동으로 구성해야 합니다.

자세한 내용은 다음을 참조하세요. ["RAC 설정에서 선호하는 노드"](#).

9. *확인*을 클릭합니다.

GUI를 사용하여 Linux 또는 AIX용 호스트를 추가하고 플러그인 패키지를 설치합니다.

호스트 추가 페이지를 사용하여 호스트를 추가한 다음 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치할 수 있습니다. 플러그인은 원격 호스트에 자동으로 설치됩니다.

이 작업에 관하여

개별 호스트나 클러스터에 대해 호스트를 추가하고 플러그인 패키지를 설치할 수 있습니다. 클러스터(Oracle RAC)에 플러그인을 설치하는 경우 플러그인은 클러스터의 모든 노드에 설치됩니다. Oracle RAC One Node의 경우 액티브 노드와 패시브 노드 모두에 플러그인을 설치해야 합니다.



Oracle RAC에 플러그인을 설치하는 경우 암호 기반 인증만 지원됩니다. SSH 키 기반 인증은 지원되지 않습니다.

SnapCenter 관리자 역할과 같이 플러그인 설치 및 제거 권한이 있는 역할이 할당되어야 합니다.



SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 상단에 관리되는 호스트 탭이 선택되어 있는지 확인하세요.
3. *추가*를 클릭하세요.
4. 호스트 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
호스트 유형	호스트 유형으로 Linux 또는 *AIX*를 선택하세요. SnapCenter 서버는 호스트를 추가한 다음, 호스트에 플러그인이 아직 설치되어 있지 않으면 Oracle Database용 플러그인과 UNIX용 플러그인을 설치합니다.

이 분야에서는...	이렇게 하세요...
호스트 이름	호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하세요. SnapCenter DNS의 적절한 구성에 달려 있습니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다. 다음 중 하나의 IP 주소나 FQDN을 입력할 수 있습니다. • 독립형 호스트 • Oracle Real Application Clusters(RAC) 환경의 모든 노드  노드 VIP 또는 스캔 IP가 지원되지 않습니다. SnapCenter 사용하여 호스트를 추가하고 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.
신임장	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성하세요. 자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하세요. 지정한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다.  자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

6. (선택 사항) *추가 옵션*을 클릭합니다.

이 분야에서는...	이렇게 하세요...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정하세요. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트 번호로 표시됩니다.  플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.
설치 경로	기본 경로는 <code>_opt/ NetApp/snapcenter_</code>입니다. 선택적으로 경로를 사용자 정의할 수 있습니다.
Oracle RAC에 모든 호스트 추가	Oracle RAC의 모든 클러스터 노드를 추가하려면 이 확인란을 선택합니다. Flex ASM 설정에서는 허브 노드나 리프 노드인지에 관계없이 모든 노드가 추가됩니다.
선택적 사전 설치 확인 건너뛰기	플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택하세요.

7. *제출*을 클릭하세요.

사전 검사 건너뛰기 확인란을 선택하지 않은 경우 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 호스트가 검증됩니다.



사전 확인 스크립트는 방화벽 거부 규칙에 지정된 경우 플러그인 포트 방화벽 상태를 검증하지 않습니다.

최소 요구 사항을 충족하지 못하면 적절한 오류 또는 경고 메시지가 표시됩니다. 오류가 디스크 공간이나 RAM과 관련된 경우 `_C:\Program Files\ NetApp\ SnapCenter WebApp_`에 있는 `web.config` 파일을 업데이트하여 기본값을 수정할 수 있습니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.



HA 설정에서 `web.config` 파일을 업데이트하는 경우 두 노드에서 모두 파일을 업데이트해야 합니다.

8. 지문을 확인한 후 *확인 및 제출*을 클릭하세요.

클러스터 설정에서는 클러스터의 각 노드의 지문을 확인해야 합니다.



SnapCenter ECDSA 알고리즘을 지원하지 않습니다.



동일한 호스트가 이전에 SnapCenter 에 추가되었고 지문이 확인된 경우에도 지문 확인은 필수입니다.

9. 설치 진행 상황을 모니터링합니다.

설치 관련 로그 파일은 `_/custom_location/snapcenter/logs_`에 있습니다.

결과

호스트의 모든 데이터베이스는 자동으로 검색되어 리소스 페이지에 표시됩니다. 아무것도 표시되지 않으면 *리소스 새로 고침*을 클릭하세요.

모니터 설치 상태

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행 상황을 모니터링할 수 있습니다. 설치가 완료되었는지 또는 문제가 있는지 확인하기 위해 설치 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

- 진행 중
- 성공적으로 완료되었습니다
- 실패한
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
- 대기 중

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 플러그인 설치 작업만 나열되도록 목록을 필터링하려면 다음을 수행합니다.
 - a. *필터*를 클릭하세요.
 - b. 선택 사항: 시작 날짜와 종료 날짜를 지정합니다.
 - c. 유형 드롭다운 메뉴에서 *플러그인 설치*를 선택합니다.
 - d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
 - e. *적용*을 클릭하세요.
4. 설치 작업을 선택하고 *세부정보*를 클릭하면 작업 세부정보를 볼 수 있습니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

Linux 또는 AIX용 플러그인 패키지를 설치하는 대체 방법

cmdlet이나 CLI를 사용하여 Linux 또는 AIX용 플러그인 패키지를 수동으로 설치할 수도 있습니다.

플러그인을 수동으로 설치하기 전에 `_C:\ProgramData\NetApp\SnapCenter\Package Repository_`에 있는 키 **snapcenter_public_key.pub** 및 `*snapcenter_linux_host_plugin.bin.sig*`를 사용하여 바이너리 패키지의 서명을 확인해야 합니다.



플러그인을 설치하려는 호스트에 `*OpenSSL 1.0.2g*`가 설치되어 있는지 확인하세요.

다음 명령을 실행하여 바이너리 패키지의 서명을 검증합니다.

- Linux 호스트의 경우: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- AIX 호스트의 경우: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_aix_host_plugin.bsx.sig snapcenter_aix_host_plugin.bsx`

cmdlet을 사용하여 여러 원격 호스트에 설치

Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 여러 호스트에 설치하려면 *Install-SmHostPackage* PowerShell cmdlet을 사용해야 합니다.

필요한 것

플러그인 패키지를 설치하려는 각 호스트에서 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter에 로그인해야 합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 *Open-SmConnection* cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
3. *Install-SmHostPackage* cmdlet과 필요한 매개변수를 사용하여 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치합니다.

플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려는 경우 `-skipprecheck` 옵션을 사용할 수 있습니다.



사전 확인 스크립트는 방화벽 거부 규칙에 지정된 경우 플러그인 포트 방화벽 상태를 검증하지 않습니다.

4. 원격 설치를 위한 자격 증명을 입력하세요.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

클러스터 호스트에 설치

클러스터 호스트의 두 노드 모두에 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치해야 합니다.

클러스터 호스트의 각 노드에는 두 개의 IP가 있습니다. IP 중 하나는 해당 노드의 공용 IP가 되고, 두 번째 IP는 두 노드 간에 공유되는 클러스터 IP가 됩니다.

단계

1. 클러스터 호스트의 두 노드에 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치합니다.
2. `/var/opt/snapcenter/spl/etc/`에 있는 `spl.properties` 파일에 `SNAPCENTER_SERVER_HOST`, `SPL_PORT`, `SNAPCENTER_SERVER_PORT` 및 `SPL_ENABLED_PLUGINS` 매개변수에 대한 올바른 값이 지정되었는지 확인합니다.

`spl.properties`에 `SPL_ENABLED_PLUGINS`가 지정되어 있지 않으면 이를 추가하고 `SCO,SCU` 값을 할당할 수 있습니다.
3. SnapCenter 서버 호스트에서 `Open-SmConnection` cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
4. 각 노드에서 `Set-PreferredHostIPsInStorageExportPolicy` sccli 명령과 필요한 매개변수를 사용하여 노드의 기본 IP를 설정합니다.
5. SnapCenter 서버 호스트에서 `_C:\Windows\System32\drivers\etc\hosts_`에 클러스터 IP와 해당 DNS 이름에 대한 항목을 추가합니다.
6. `Add-SmHost` cmdlet을 사용하여 호스트 이름에 클러스터 IP를 지정하여 SnapCenter 서버에 노드를 추가합니다.

노드 1에서 Oracle 데이터베이스를 검색하고(클러스터 IP가 노드 1에 호스팅된다고 가정) 데이터베이스 백업을 만듭니다. 장애 조치가 발생하면 노드 1에서 생성된 백업을 사용하여 노드 2의 데이터베이스를 복원할 수 있습니다. 노드 1에서 생성된 백업을 사용하여 노드 2에 복제본을 생성할 수도 있습니다.



다른 SnapCenter 작업이 실행되는 동안 장애 조치가 발생하면 오래된 볼륨, 디렉토리 및 잠금 파일이 생성됩니다.

Linux용 플러그인 패키지를 자동 모드로 설치합니다.

명령줄 인터페이스(CLI)를 사용하여 Linux용 SnapCenter 플러그인 패키지를 자동 모드로 설치할 수 있습니다.

필요한 것

- 플러그인 패키지를 설치하기 위한 필수 구성 요소를 검토해야 합니다.
- `DISPLAY` 환경 변수가 설정되어 있지 않은지 확인해야 합니다.

`DISPLAY` 환경 변수가 설정되어 있는 경우 `unset DISPLAY`를 실행한 다음 플러그인을 수동으로 설치해보세요.

이 작업에 관하여

콘솔 모드로 설치하는 경우 필요한 설치 정보를 제공해야 하지만, 사일런트 모드로 설치하는 경우에는 설치 정보를 제공할 필요가 없습니다.

단계

1. SnapCenter 서버 설치 위치에서 Linux용 SnapCenter 플러그인 패키지를 다운로드합니다.

기본 설치 경로는 `_C:\ProgramData\NetApp\SnapCenter\PackageRepository_`입니다. 이 경로는 SnapCenter 서버가 설치된 호스트에서 접근할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 다운로드한 디렉토리로 이동합니다.

3. 달리다

```
./SnapCenter_linux_host_plugin.bin-i silent-DPORT=8145-  
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-  
DUSER_INSTALL_DIR==/opt/custom_path
```

4. `_var/opt/snapcenter/spl/etc/_`에 있는 `spl.properties` 파일을 편집하여
`SPL_ENABLED_PLUGINS=SCO,SCU`를 추가한 다음 SnapCenter 플러그인 Loader 서비스를 다시
시작합니다.



플러그인 패키지를 설치하면 플러그인이 SnapCenter 서버가 아닌 호스트에 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록해야 합니다. 호스트를 추가하는 동안 자격 증명으로 "없음"을 선택하세요. 호스트가 추가되면 설치된 플러그인이 자동으로 검색됩니다.

AIX용 플러그인 패키지를 자동 모드로 설치합니다.

명령줄 인터페이스(CLI)를 사용하여 AIX용 SnapCenter 플러그인 패키지를 자동 모드로 설치할 수 있습니다.

필요한 것

- 플러그인 패키지를 설치하기 위한 필수 구성 요소를 검토해야 합니다.
- DISPLAY 환경 변수가 설정되어 있지 않은지 확인해야 합니다.

DISPLAY 환경 변수가 설정되어 있는 경우 `unset DISPLAY`를 실행한 다음 플러그인을 수동으로 설치해보세요.

단계

1. SnapCenter 서버 설치 위치에서 AIX용 SnapCenter 플러그인 패키지를 다운로드합니다.

기본 설치 경로는 `_C:\ProgramData\NetApp\ SnapCenter\PackageRepository_`입니다. 이 경로는 SnapCenter 서버가 설치된 호스트에서 접근할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 다운로드한 디렉토리로 이동합니다.

3. 달리다

```
./snapcenter_aix_host_plugin.bsx-i silent-DPORT=8145-  
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-  
DUSER_INSTALL_DIR==/opt/custom path-  
DINSTALL_LOG_NAME=SnapCenter_AIX_Host_Plug-in_Install_MANUAL.log-  
DCHOSEN_FEATURE_LIST=CUSTOMDSPL_USER=install_user
```

4. `_var/opt/snapcenter/spl/etc/_`에 있는 `spl.properties` 파일을 편집하여
`SPL_ENABLED_PLUGINS=SCO,SCU`를 추가한 다음 SnapCenter 플러그인 Loader 서비스를 다시
시작합니다.



플러그인 패키지를 설치하면 플러그인이 SnapCenter 서버가 아닌 호스트에 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록해야 합니다. 호스트를 추가하는 동안 자격 증명으로 "없음"을 선택하세요. 호스트가 추가되면 설치된 플러그인이 자동으로 검색됩니다.

SnapCenter 플러그인 Loader 서비스 구성

SnapCenter 플러그인 Loader 서비스는 Linux 또는 AIX용 플러그인 패키지를 로드하여 SnapCenter 서버와 상호 작용합니다. SnapCenter 플러그인 Loader 서비스는 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치할 때 설치됩니다.

이 작업에 관하여

Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치하면 SnapCenter 플러그인 Loader 서비스가 자동으로 시작됩니다. SnapCenter 플러그인 Loader 서비스가 자동으로 시작되지 않으면 다음을 수행해야 합니다.

- 플러그인이 작동 중인 디렉토리가 삭제되지 않았는지 확인하세요.
- Java Virtual Machine에 할당된 메모리 공간을 늘리세요

`_/custom_location/ NetApp/snapcenter/spl/etc/_`에 있는 `spl.properties` 파일에는 다음 매개변수가 포함되어 있습니다. 이러한 매개변수에는 기본값이 할당됩니다.

매개변수 이름	설명
로그 레벨	지원되는 로그 수준을 표시합니다. 가능한 값은 TRACE, DEBUG, INFO, WARN, ERROR, FATAL입니다.
SPL_프로토콜	SnapCenter 플러그인 Loader 가 지원하는 프로토콜을 표시합니다. HTTPS 프로토콜만 지원됩니다. 기본값이 없는 경우 값을 추가할 수 있습니다.
SNAPCENTER_SERVER_프로토콜	SnapCenter Server에서 지원하는 프로토콜을 표시합니다. HTTPS 프로토콜만 지원됩니다. 기본값이 없는 경우 값을 추가할 수 있습니다.

매개변수 이름	설명
자바 홈 업데이트 건너뛰기	기본적으로 SPL 서비스는 Java 경로를 감지하고 JAVA_HOME 매개변수를 업데이트합니다. 따라서 기본값은 FALSE로 설정됩니다. 기본 동작을 비활성화하고 Java 경로를 수동으로 수정하려면 TRUE로 설정하면 됩니다.
SPL_키스토어_패스	키스토어 파일의 비밀번호를 표시합니다. 비밀번호를 변경하거나 새로운 키스토어 파일을 만드는 경우에만 이 값을 변경할 수 있습니다.
SPL_PORT	SnapCenter 플러그인 Loader 서비스가 실행 중인 포트 번호를 표시합니다. 기본값이 없는 경우 값을 추가할 수 있습니다.  플러그인을 설치한 후에는 값을 변경하지 마세요.
SNAPCENTER_SERVER_HOST	SnapCenter 서버의 IP 주소 또는 호스트 이름을 표시합니다.
SPL_키스토어_경로	키스토어 파일의 절대 경로를 표시합니다.
SNAPCENTER_SERVER_PORT	SnapCenter 서버가 실행 중인 포트 번호를 표시합니다.
LOGS_MAX_COUNT	/custom_location/snapcenter/spl/logs 폴더에 보관된 SnapCenter 플러그인 Loader 로그 파일의 수를 표시합니다. 기본값은 5000으로 설정되어 있습니다. 개수가 지정된 값보다 많으면 마지막으로 수정된 5000개의 파일이 보존됩니다. SnapCenter 플러그인 Loader 서비스가 시작된 후 24시간마다 파일 개수 확인이 자동으로 수행됩니다.  spl.properties 파일을 수동으로 삭제하면 보존되는 파일 수가 9999로 설정됩니다.
자바 홈	SPL 서비스를 시작하는 데 사용되는 JAVA_HOME의 절대 디렉토리 경로를 표시합니다. 이 경로는 설치 중 및 SPL 시작의 일부로 결정됩니다.

매개변수 이름	설명
로그 최대 크기	작업 로그 파일의 최대 크기를 표시합니다. 최대 크기에 도달하면 로그 파일이 압축되고 로그는 해당 작업의 새 파일에 기록됩니다.
지난 며칠 동안의 로그 보관	로그가 보관되는 일수를 표시합니다.
인증서 검증 활성화	호스트에 대해 CA 인증서 검증이 활성화된 경우 true로 표시됩니다. spl.properties를 편집하거나 SnapCenter GUI 또는 cmdlet을 사용하여 이 매개변수를 활성화하거나 비활성화할 수 있습니다.

이러한 매개변수 중 하나라도 기본값에 할당되지 않았거나 값을 할당하거나 변경하려는 경우 spl.properties 파일을 수정할 수 있습니다. spl.properties 파일을 확인하고 파일을 편집하여 매개변수에 할당된 값과 관련된 문제를 해결할 수도 있습니다. spl.properties 파일을 수정한 후에는 SnapCenter 플러그인 Loader 서비스를 다시 시작해야 합니다.

단계

1. 필요에 따라 다음 작업 중 하나를 수행합니다.

◦ SnapCenter 플러그인 Loader 서비스를 시작합니다.

- 루트 사용자로 다음을 실행합니다. `/custom_location/NetApp/snapcenter/spl/bin/spl start`
- 루트가 아닌 사용자로 다음을 실행합니다. `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`

◦ SnapCenter 플러그인 Loader 서비스를 중지합니다.

- 루트 사용자로 다음을 실행합니다. `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
- 루트가 아닌 사용자로 다음을 실행합니다. `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`



stop 명령과 함께 `-force` 옵션을 사용하면 SnapCenter 플러그인 Loader 서비스를 강제로 중지할 수 있습니다. 하지만 그렇게 하면 기존 작업도 종료되므로 주의해서 작업해야 합니다.

◦ SnapCenter 플러그인 Loader 서비스를 다시 시작합니다.

- 루트 사용자로 다음을 실행합니다. `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
- 루트가 아닌 사용자로 다음을 실행합니다. `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`

◦ SnapCenter 플러그인 Loader 서비스의 상태를 확인하세요.

- 루트 사용자로 다음을 실행합니다. `/custom_location/NetApp/snapcenter/spl/bin/spl`

status

- 루트 사용자가 아닌 경우 다음을 실행합니다. `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
- SnapCenter 플러그인 Loader 서비스에서 변경 사항을 찾으세요.
 - 루트 사용자로 다음을 실행합니다. `/custom_location/NetApp/snapcenter/spl/bin/spl change`
 - 루트가 아닌 사용자로 다음을 실행합니다. `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Linux 호스트에서 SnapCenter 플러그인 Loader (SPL) 서비스를 사용하여 CA 인증서 구성

SnapCenter 플러그인 Loader 서비스를 사용하여 SPL 키 저장소와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SPL 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.



SPL은 '/var/opt/snapcenter/spl/etc'에 위치한 'keystore.jks' 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 **SPL** 키 저장소 및 **CA** 서명 키 쌍의 별칭에 대한 비밀번호 관리

단계

1. SPL 속성 파일에서 SPL 키 저장소 기본 비밀번호를 검색할 수 있습니다.

이는 'SPL_KEYSTORE_PASS' 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

```
keytool -storepasswd -keystore keystore.jks
```

. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

spl.properties 파일에서 SPL_KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

3. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



SPL 키 저장소의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

SPL 신뢰 저장소에 루트 또는 중간 인증서 구성

SPL 신뢰 저장소에 대한 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. SPL 키 저장소가 포함된 폴더로 이동합니다: `/var/opt/snapcenter/spl/etc`.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias  
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore  
keystore.jks
```

. 루트 또는 중간 인증서를 SPL 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

SPL 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 SPL 신뢰 저장소에 구성해야 합니다.

단계

1. SPL 키 저장소 `/var/opt/snapcenter/spl/etc`가 포함된 폴더로 이동합니다.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
keytool -importkeystore -srckeystore <CertificatePathToImport>  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

. 키스토어에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.

. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 SPL 키 저장소 비밀번호는 `spl.properties` 파일의 `SPL_KEYSTORE_PASS` 키 값입니다.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks
```

. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자("*", ",", ")가 포함된 경우 별칭 이름을 간단한 이름으로 변경합니다.

```
keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks
```

. spl.properties 파일에 있는 키스토어에서 별칭 이름을 구성합니다.

이 값을 SPL_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

4. CA 서명 키 쌍을 SPL 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

SPL에 대한 인증서 해지 목록(CRL) 구성

SPL에 대한 CRL을 구성해야 합니다.

이 작업에 관하여

- SPL은 미리 구성된 디렉토리에서 CRL 파일을 찾습니다.
- SPL의 CRL 파일에 대한 기본 디렉토리는 `_var/opt/snapcenter/spl/etc/crl`입니다.

단계

1. spl.properties 파일에서 기본 디렉토리를 SPL_CRL_PATH 키에 맞춰 수정하고 업데이트할 수 있습니다.
2. 이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다.

수신 인증서는 각 CRL에 대해 검증됩니다.

플러그인에 대한 CA 인증서 활성화

CA 인증서를 구성하고 SnapCenter 서버와 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- `Set-SmCertificateSettings` cmdlet을 실행하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- `_Get-SmCertificateSettings_`를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.

3. 하나 또는 여러 개의 플러그인 호스트를 선택하세요.
4. *추가 옵션*을 클릭하세요.
5. *인증서 검증 사용*을 선택합니다.

당신이 완료한 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- *  *는 CA 인증서가 활성화되지 않았거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- *  *는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- *  *는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- *  *는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

Oracle용 SnapManager 및 SAP용 SnapManager 에서 SnapCenter 로 데이터 가져오기

Oracle용 SnapManager 및 SAP용 SnapManager 에서 SnapCenter 로 데이터를 가져오면 이전 버전의 데이터를 계속 사용할 수 있습니다.

명령줄 인터페이스(Linux 호스트 CLI)에서 가져오기 도구를 실행하여 Oracle용 SnapManager 및 SAP용 SnapManager 에서 SnapCenter 로 데이터를 가져올 수 있습니다.

가져오기 도구는 SnapCenter 에서 정책과 리소스 그룹을 생성합니다. SnapCenter 에서 생성된 정책과 리소스 그룹은 SnapManager for Oracle 및 SnapManager for SAP에서 해당 프로필을 사용하여 수행되는 프로필과 작업에 해당합니다. SnapCenter 가져오기 도구는 Oracle용 SnapManager 및 SAP용 SnapManager 저장소 데이터베이스와 가져오려는 데이터베이스와 상호 작용합니다.

- 프로필을 사용하여 수행된 모든 프로필, 일정 및 작업을 검색합니다.
- 프로필에 첨부된 각 고유한 작업과 각 일정에 대해 SnapCenter 백업 정책을 만듭니다.
- 각 대상 데이터베이스에 대한 리소스 그룹을 만듭니다.

`_/opt/ NetApp/snapcenter/spl/bin_`에 있는 `sc-migrate` 스크립트를 실행하여 가져오기 도구를 실행할 수 있습니다. 가져오려는 데이터베이스 호스트에 Linux용 SnapCenter 플러그인 패키지를 설치하면 `sc-migrate` 스크립트가 `_/opt/ NetApp/snapcenter/spl/bin_`에 복사됩니다.



SnapCenter 그래픽 사용자 인터페이스(GUI)에서는 데이터 가져오기가 지원되지 않습니다.

SnapCenter 7-Mode에서 작동하는 Data ONTAP 지원하지 않습니다. 7-Mode Transition Tool을 사용하면 7-Mode로 운영되는 Data ONTAP 시스템에 저장된 데이터와 구성을 ONTAP 시스템으로 마이그레이션할 수 있습니다.

데이터 가져오기에 지원되는 구성

Oracle용 SnapManager 3.4.x 및 SAP용 SnapManager 3.4.x에서 SnapCenter 로 데이터를 가져오기 전에 Oracle 데이터베이스용 SnapCenter 플러그인에서 지원되는 구성을 알아야 합니다.

Oracle Database용 SnapCenter 플러그인에서 지원되는 구성은 다음에 나열되어 있습니다. "[NetApp 상호 운용성 매트릭스 도구](#)".

SnapCenter 로 가져오는 내용

프로필을 사용하여 수행된 프로필, 일정 및 작업을 가져올 수 있습니다.

Oracle용 SnapManager 및 SAP용 SnapManager 에서	SnapCenter 로
어떠한 작업이나 일정도 없는 프로필	정책은 기본 백업 유형을 온라인으로, 백업 범위를 전체로 설정하여 생성됩니다.
하나 이상의 작업이 포함된 프로필	프로필과 해당 프로필을 사용하여 수행되는 작업의 고유한 조합을 기반으로 여러 정책이 생성됩니다. SnapCenter 에서 생성된 정책에는 프로필과 해당 작업에서 검색된 보관 로그 정리 및 보존 세부 정보가 포함되어 있습니다.
Oracle Recovery Manager(RMAN) 구성을 사용한 프로필	정책은 Oracle Recovery Manager를 사용한 카탈로그 백업 옵션을 활성화하여 생성됩니다. SnapManager 에서 외부 RMAN 카탈로그를 사용한 경우 SnapCenter 에서 RMAN 카탈로그 설정을 구성해야 합니다. 기존 자격증명을 선택하거나 새 자격증명을 만들 수 있습니다. SnapManager 의 제어 파일을 통해 RMAN이 구성된 경우 SnapCenter 에서 RMAN을 구성할 필요가 없습니다.
프로필에 첨부된 일정	일정에 대한 정책이 생성됩니다.
데이터 베이스	가져온 각 데이터베이스에 대해 리소스 그룹이 생성됩니다. RAC(Real Application Clusters) 설정에서 가져오기 도구를 실행하는 노드는 가져오기가 완료된 후 기본 노드가 되고 해당 노드에 대한 리소스 그룹이 생성됩니다.



프로필을 가져오면 백업 정책과 함께 검증 정책이 생성됩니다.

Oracle용 SnapManager 및 SAP용 SnapManager 프로필, 일정 및 프로필을 사용하여 수행되는 모든 작업을 SnapCenter 로 가져오면 다양한 매개변수 값도 함께 가져옵니다.

Oracle용 SnapManager 및 SAP용 SnapManager 매개변수 및 값	SnapCenter 매개변수 및 값	노트
백업 범위 • 가득한 • 데이터 • 통나무	백업 범위 • 가득한 • 데이터 • 통나무	
백업 모드 • 자동 • 온라인 • 오프라인	백업 유형 • 온라인 • 오프라인 종료	백업 모드가 자동인 경우 가져오기 도구는 작업이 수행될 당시의 데이터베이스 상태를 확인하고 백업 유형을 온라인 또는 오프라인 종료로 적절히 설정합니다.
보유 • 날 • 카운트	보유 • 날 • 카운트	Oracle용 SnapManager 와 SAP용 SnapManager 일수와 횟수를 모두 사용하여 보존 기간을 설정합니다. SnapCenter에는 일 또는 카운트가 있습니다. 따라서 SnapManager for Oracle과 SnapManager for SAP에서는 일수가 개수보다 우선하므로 보존 기간은 일수로 설정됩니다.
일정에 대한 가지치기 • 모두 • 시스템 변경 번호(SCN) • 날짜 • 지정된 시간, 일, 주, 월 이전에 생성된 로그	일정에 대한 가지치기 • 모두 • 지정된 시간 및 요일 이전에 생성된 로그	SnapCenter SCN, 날짜, 주, 월을 기준으로 한 정리를 지원하지 않습니다.
공고 • 성공적인 작업에 대해서만 이메일이 전송됩니다. • 실패한 작업에 대해서만 이메일이 전송됩니다. • 성공 및 실패한 작업에 대한 이메일이 전송되었습니다.	공고 • 언제나 • 실패 시 • 경고 • 오류	이메일 알림을 가져왔습니다. 하지만 SnapCenter GUI를 사용하여 SMTP 서버를 수동으로 업데이트해야 합니다. 이메일 제목은 비워두어 직접 구성하실 수 있습니다.

SnapCenter 로 가져오지 못하는 것

가져오기 도구는 모든 것을 SnapCenter 로 가져오지 않습니다.

SnapCenter 로 다음을 가져올 수 없습니다.

- 백업 메타데이터
- 부분 백업
- 원시 장치 매핑(RDM) 및 가상 스토리지 콘솔(VSC) 관련 백업
- Oracle용 SnapManager 및 SAP용 SnapManager 저장소에서 사용 가능한 역할 또는 자격 증명
- 검증, 복원 및 복제 작업과 관련된 데이터
- 운영을 위한 가지치기
- Oracle용 SnapManager 및 SAP용 SnapManager 프로필에 지정된 복제 세부 정보

가져온 후에는 SnapCenter 에서 생성된 해당 정책을 수동으로 편집하여 복제 세부 정보를 포함해야 합니다.

- 카탈로그화된 백업 정보

데이터 가져오기 준비

SnapCenter 로 데이터를 가져오기 전에 특정 작업을 수행하여 가져오기 작업을 성공적으로 실행해야 합니다.

단계

1. 가져오려는 데이터베이스를 식별합니다.
2. SnapCenter 사용하여 데이터베이스 호스트를 추가하고 Linux용 SnapCenter 플러그인 패키지를 설치합니다.
3. SnapCenter 사용하여 호스트의 데이터베이스에서 사용하는 스토리지 가상 머신(SVM)에 대한 연결을 설정합니다.
4. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
5. 리소스 페이지에서 가져올 데이터베이스가 검색되어 표시되는지 확인하세요.

가져오기 도구를 실행하려면 데이터베이스에 액세스할 수 있어야 하며, 그렇지 않으면 리소스 그룹 생성이 실패합니다.

데이터베이스에 자격 증명이 구성되어 있는 경우 SnapCenter 에서 해당 자격 증명을 만들고, 자격 증명을 데이터베이스에 할당한 다음 데이터베이스 검색을 다시 실행해야 합니다. 데이터베이스가 ASM(Automatic Storage Management)에 있는 경우 ASM 인스턴스에 대한 자격 증명을 만들고 해당 자격 증명을 데이터베이스에 할당해야 합니다.

6. 가져오기 도구를 실행하는 사용자에게 SnapManager for Oracle 또는 SnapManager for SAP 호스트에서 SnapManager for Oracle 또는 SnapManager for SAP CLI 명령(예: 일정을 일시 중단하는 명령)을 실행할 수 있는 충분한 권한이 있는지 확인하세요.
7. Oracle용 SnapManager 또는 SAP용 SnapManager 호스트에서 다음 명령을 실행하여 일정을 일시 중단합니다.
 - a. Oracle 호스트용 SnapManager 에서 일정을 일시 중단하려면 다음을 실행하세요.

```
smo credential set -repository -dbname repository_database_name -host  
host_name -port port_number -login -username  
user_name_for_repository_database
```

- `smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
- `smo credential set -profile -name profile_name`



호스트의 각 프로필에 대해 `smo credential set` 명령을 실행해야 합니다.

b. SAP 호스트용 SnapManager 에서 일정을 일시 중단하려면 다음을 실행하세요.

- `smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
- `smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
- `smsap credential set -profile -name profile_name`



호스트의 각 프로필에 대해 `smsap` 자격 증명 설정 명령을 실행해야 합니다.

8. `hostname -f`를 실행할 때 데이터베이스 호스트의 정규화된 도메인 이름(FQDN)이 표시되는지 확인하세요.

FQDN이 표시되지 않으면 `/etc/hosts`를 수정하여 호스트의 FQDN을 지정해야 합니다.

데이터 가져오기

데이터베이스 호스트에서 가져오기 도구를 실행하여 데이터를 가져올 수 있습니다.

이 작업에 관하여

가져온 후 생성된 SnapCenter 백업 정책은 서로 다른 명명 형식을 갖습니다.

- 어떠한 작업이나 일정도 없는 프로필에 대해 생성된 정책은 `SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED` 형식을 갖습니다.

프로필을 사용하여 아무 작업도 수행하지 않으면 기본 백업 유형이 온라인으로, 백업 범위가 전체로 설정된 해당 정책이 생성됩니다.

- 하나 이상의 작업이 포함된 프로필에 대해 생성된 정책은 `SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED` 형식을 갖습니다.
- 프로필에 첨부된 일정에 대해 생성된 정책은 `SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED` 형식을 갖습니다.

단계

1. 가져오려는 데이터베이스 호스트에 로그인합니다.
2. `_/opt/ NetApp/snapcenter/spl/bin_`에 있는 `sc-migrate` 스크립트를 실행하여 가져오기 도구를 실행합니다.
3. SnapCenter 서버 사용자 이름과 비밀번호를 입력하세요.

자격 증명을 검증한 후 SnapCenter 와 연결이 설정됩니다.

4. Oracle용 SnapManager 또는 SAP용 SnapManager 저장소 데이터베이스 세부 정보를 입력하세요.

저장소 데이터베이스는 호스트에서 사용 가능한 데이터베이스를 나열합니다.

5. 대상 데이터베이스 세부 정보를 입력하세요.

호스트의 모든 데이터베이스를 가져오려면 all을 입력하세요.

6. 실패한 작업에 대한 시스템 로그를 생성하거나 ASUP 메시지를 보내려면 *Add-SmStorageConnection* 또는 *Set-SmStorageConnection* 명령을 실행하여 해당 기능을 활성화해야 합니다.



가져오기 도구를 실행하는 동안이나 가져온 후에 가져오기 작업을 취소하려면 가져오기 작업의 일부로 생성된 SnapCenter 정책, 자격 증명 및 리소스 그룹을 수동으로 삭제해야 합니다.

결과

SnapCenter 백업 정책은 프로필, 일정 및 프로필을 사용하여 수행되는 작업에 대해 생성됩니다. 각 대상 데이터베이스에 대해서도 리소스 그룹이 생성됩니다.

데이터를 성공적으로 가져온 후, 가져온 데이터베이스와 연관된 일정은 SnapManager for Oracle 및 SnapManager for SAP에서 일시 중단됩니다.



가져온 후에는 SnapCenter 사용하여 가져온 데이터베이스나 파일 시스템을 관리해야 합니다.

가져오기 도구를 실행할 때마다 발생하는 로그는 */var/opt/snapcenter/spl/logs* 디렉토리에 *spl_migration_timestamp.log*라는 이름으로 저장됩니다. 이 로그를 참조하여 가져오기 오류를 검토하고 문제를 해결할 수 있습니다.

SnapCenter Plug-in for VMware vSphere 설치

데이터베이스나 파일 시스템이 가상 머신(VM)에 저장되어 있거나 VM과 데이터 저장소를 보호하려는 경우 SnapCenter Plug-in for VMware vSphere 배포해야 합니다.

배포에 대한 정보는 다음을 참조하세요. "[배포 개요](#)".

CA 인증서 배포

SnapCenter Plug-in for VMware vSphere 사용하여 CA 인증서를 구성하려면 다음을 참조하세요. "[SSL 인증서 생성 또는 가져오기](#)".

CRL 파일 구성

SnapCenter Plug-in for VMware vSphere 미리 구성된 디렉토리에서 CRL 파일을 찾습니다. SnapCenter Plug-in for VMware vSphere 의 CRL 파일의 기본 디렉토리는 *_/opt/netapp/config/crl_*입니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

Oracle 데이터베이스 보호를 준비하세요

백업, 복제 또는 복원 작업과 같은 데이터 보호 작업을 수행하기 전에 전략을 정의하고 환경을 설정해야 합니다. SnapMirror 및 SnapVault 기술을 사용하도록 SnapCenter 서버를 설정할 수도 있습니다.

SnapVault 및 SnapMirror 기술을 활용하려면 스토리지 장치의 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 구성하고 초기화해야 합니다. NetAppSystem Manager를 사용하거나 스토리지 콘솔 명령줄을 사용하여 이러한 작업을 수행할 수 있습니다.

Oracle Database용 플러그인을 사용하기 전에 SnapCenter 관리자는 SnapCenter 서버를 설치하고 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다. ["자세히 알아보기"](#)
- 스토리지 시스템 연결을 추가하여 SnapCenter 환경을 구성합니다. ["자세히 알아보기"](#)



SnapCenter 서로 다른 클러스터에서 동일한 이름을 가진 여러 SVM을 지원하지 않습니다. SVM 등록이나 클러스터 등록을 사용하여 SnapCenter에 등록된 각 SVM은 고유해야 합니다.

- 설치 사용자에게 대해 Linux 또는 AIX 인증 모드로 자격 증명을 생성합니다. ["자세히 알아보기"](#)
- 호스트를 추가하고, 플러그인을 설치하고, 리소스를 찾아보세요.
- VMware RDM LUN 또는 VMDK에 있는 Oracle 데이터베이스를 보호하기 위해 SnapCenter Server를 사용하는 경우 SnapCenter Plug-in for VMware vSphere 배포하고 SnapCenter에 플러그인을 등록해야 합니다.
- Linux 또는 AIX 호스트에 Java를 설치합니다.

보다 ["Linux 호스트 요구 사항"](#) 또는 ["AIX 호스트 요구 사항"](#) 자세한 내용은.

- 애플리케이션 방화벽의 시간 초과 값을 3시간 이상으로 설정해야 합니다.
- NFS 환경에 Oracle 데이터베이스가 있는 경우 마운트, 복제, 검증 및 복원 작업을 수행하기 위해 기본 또는 보조 저장소에 대해 하나 이상의 NFS 데이터 LIF를 구성해야 합니다.
- 여러 데이터 경로(LIF) 또는 dNFS 구성이 있는 경우 데이터베이스 호스트에서 SnapCenter CLI를 사용하여 다음을 수행할 수 있습니다.
 - 기본적으로 데이터베이스 호스트의 모든 IP 주소는 복제된 볼륨의 스토리지 가상 머신(SVM)에 있는 NFS 스토리지 내보내기 정책에 추가됩니다. 특정 IP 주소를 사용하거나 IP 주소의 하위 집합으로 제한하려면 Set-PreferredHostIPsInStorageExportPolicy CLI를 실행하세요.
 - SVM에 여러 개의 데이터 경로(LIF)가 있는 경우 SnapCenter NFS 복제 볼륨을 마운트하기 위해 적절한 데이터 경로(LIF)를 선택합니다. 하지만 특정 데이터 경로(LIF)를 지정하려면 Set-SvmPreferredDataPath CLI를 실행해야 합니다. 자세한 내용은 명령어 참조 가이드를 참조하세요.
- SAN 환경에 Oracle 데이터베이스가 있는 경우 다음 가이드에 언급된 권장 사항에 따라 SAN 환경이 구성되었는지 확인하세요.
 - ["ONTAP 스토리지와 함께 Linux 호스트 사용"](#)
 - ["AIX 호스트 유틸리티의 영향을 받는 호스트 설정"](#)
- Oracle Linux 또는 RHEL 운영 체제의 LVM에 Oracle 데이터베이스가 있는 경우 최신 버전의 LVM(논리 볼륨 관리)을 설치하세요.

- Oracle용 SnapManager 사용하고 Oracle Database용 SnapCenter 플러그인으로 마이그레이션하려는 경우 sccli 명령 sc-migrate를 사용하여 프로필을 SnapCenter의 정책 및 리소스 그룹으로 마이그레이션할 수 있습니다.
- 백업 복제를 원하는 경우 ONTAP에서 SnapMirror 및 SnapVault 구성합니다.

SnapCenter 4.1.1 사용자의 경우 SnapCenter Plug-in for VMware vSphere 설명서에는 가상화된 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 있습니다. SnapCenter 4.2.x 사용자, NetApp Data Broker 1.0 및 1.0.1의 경우, Linux 기반 NetApp Data Broker 가상 어플라이언스(Open Virtual Appliance 형식)에서 제공하는 SnapCenter Plug-in for VMware vSphere 사용하여 가상화된 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 설명서에 나와 있습니다. SnapCenter 4.3.x 사용자의 경우, SnapCenter Plug-in for VMware vSphere 설명서에는 Linux 기반 SnapCenter Plug-in for VMware vSphere (Open Virtual Appliance 형식)을 사용하여 가상화된 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 있습니다.

더 많은 정보를 찾아보세요

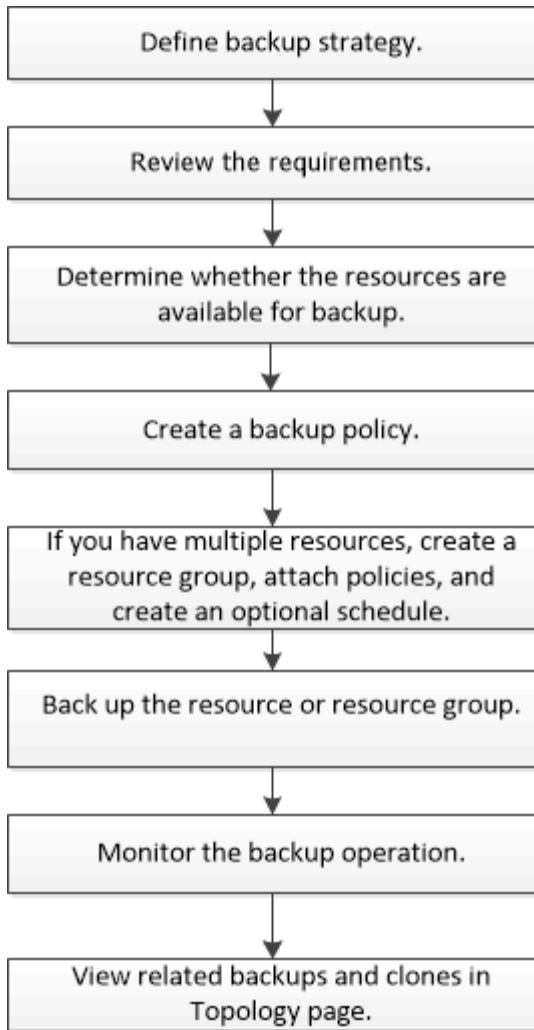
- ["상호 운용성 매트릭스 도구"](#)
- ["SnapCenter Plug-in for VMware vSphere 설명서"](#)
- ["RHEL 7 이상에서 다중 경로가 아닌 환경에서 데이터 보호 작업이 실패합니다."](#)

Oracle 데이터베이스 백업

백업 절차 개요

리소스(데이터베이스) 또는 리소스 그룹의 백업을 만들 수 있습니다. 백업 절차에는 계획, 백업 리소스 식별, 백업 정책 생성, 리소스 그룹 생성 및 정책 첨부, 백업 생성, 작업 모니터링이 포함됩니다.

다음 워크플로는 백업 작업을 수행해야 하는 순서를 보여줍니다.



Oracle 데이터베이스에 대한 백업을 생성하는 동안 여러 작업이 데이터베이스에서 실행되는 것을 방지하기 위해 Oracle 데이터베이스 호스트의 `/var/opt/snapcenter/sco/lock` 디렉토리에 작업 잠금 파일(`.sm_lock_dbsid`)이 생성됩니다. 데이터베이스가 백업된 후에는 운영 잠금 파일이 자동으로 제거됩니다.

하지만 이전 백업이 경고와 함께 완료된 경우 작업 잠금 파일이 삭제되지 않을 수 있으며, 다음 백업 작업이 대기 큐에 들어갈 수 있습니다. `.sm_lock_dbsid` 파일을 삭제하지 않으면 결국 취소될 수 있습니다. 이러한 시나리오에서는 다음 단계를 수행하여 수동으로 운영 잠금 파일을 삭제해야 합니다.

1. 명령 프롬프트에서 `_var/opt/snapcenter/sco/lock_`으로 이동합니다.
2. 작업 잠금을 삭제합니다. `rm -rf .sm_lock_dbsid.`

백업 구성 정보

백업을 위한 지원되는 **Oracle** 데이터베이스 구성

SnapCenter 다양한 Oracle 데이터베이스 구성의 백업을 지원합니다.

- Oracle Standalone
- Oracle Real Application Clusters(RAC)
- Oracle Standalone 레거시

- Oracle 독립형 컨테이너 데이터베이스(CDB)

- Oracle Data Guard 대기

Data Guard 대기 데이터베이스의 오프라인 마운트 백업만 생성할 수 있습니다. 오프라인 종료 백업, 보관 로그 전용 백업 및 전체 백업은 지원되지 않습니다.

- Oracle Active Data Guard 대기

Active Data Guard 대기 데이터베이스의 온라인 백업만 생성할 수 있습니다. 아카이브 로그만 백업하고 전체 백업은 지원되지 않습니다.

Data Guard 대기 또는 Active Data Guard 대기 데이터베이스의 백업을 생성하기 전에 관리형 복구 프로세스(MRP)가 중지되고 백업이 생성되면 MRP가 시작됩니다.

- 자동 스토리지 관리(ASM)
 - 가상 머신 디스크(VMDK)의 ASM 독립형 및 ASM RAC

Oracle 데이터베이스에 지원되는 모든 복원 방법 중에서 VMDK에서는 ASM RAC 데이터베이스에 대한 연결 및 복사 복원만 수행할 수 있습니다.

- ASM 독립형 및 원시 장치 매핑(RDM)의 ASM RAC + ASMLib을 사용하거나 사용하지 않고 ASM에서 Oracle 데이터베이스에 대한 백업, 복원 및 복제 작업을 수행할 수 있습니다.
- Oracle ASM 필터 드라이버(ASMFD)

PDB 마이그레이션 및 PDB 복제 작업은 지원되지 않습니다.

- 오라클 플렉스 ASM

지원되는 Oracle 버전에 대한 최신 정보는 다음을 참조하세요. ["NetApp 상호 운용성 매트릭스 도구"](#).

Oracle 데이터베이스에서 지원되는 백업 유형

백업 유형은 생성하려는 백업 유형을 지정합니다. SnapCenter Oracle 데이터베이스에 대한 온라인 및 오프라인 백업 유형을 지원합니다.

온라인 백업

데이터베이스가 온라인 상태일 때 생성되는 백업을 온라인 백업이라고 합니다. 핫 백업이라고도 하는 온라인 백업을 사용하면 데이터베이스를 종료하지 않고도 백업을 만들 수 있습니다.

온라인 백업의 일부로 다음 파일의 백업을 만들 수 있습니다.

- 데이터 파일과 제어 파일만
- 아카이브 로그 파일만(이 시나리오에서는 데이터베이스가 백업 모드로 전환되지 않음)
- 데이터 파일, 제어 파일 및 보관 로그 파일을 포함하는 전체 데이터베이스

오프라인 백업

데이터베이스가 마운트되거나 종료된 상태일 때 생성된 백업을 오프라인 백업이라고 합니다. 오프라인 백업은 콜드 백업이라고도 합니다. 오프라인 백업에는 데이터 파일과 제어 파일만 포함할 수 있습니다. 오프라인 마운트 또는

오프라인 종료 백업을 만들 수 있습니다.

- 오프라인 마운트 백업을 생성할 때 데이터베이스가 마운트된 상태인지 확인해야 합니다.

데이터베이스가 다른 상태에 있으면 백업 작업이 실패합니다.

- 오프라인 종료 백업을 생성할 때 데이터베이스는 어떤 상태든 될 수 있습니다.

백업을 생성하기 위해 데이터베이스 상태가 필요한 상태로 변경됩니다. 백업을 만든 후 데이터베이스 상태가 원래 상태로 돌아갑니다.

SnapCenter Oracle 데이터베이스를 검색하는 방법

리소스는 SnapCenter 에서 유지 관리하는 호스트의 Oracle 데이터베이스입니다. 사용 가능한 데이터베이스를 발견한 후 이러한 데이터베이스를 리소스 그룹에 추가하여 데이터 보호 작업을 수행할 수 있습니다.

다음 섹션에서는 SnapCenter 다양한 유형과 버전의 Oracle 데이터베이스를 검색하는 데 사용하는 프로세스를 설명합니다.

Oracle 버전 11g ~ 12cR1의 경우

RAC 데이터베이스

RAC 데이터베이스는 /etc/oratab 항목을 기반으로만 검색됩니다. /etc/oratab 파일에 데이터베이스 항목이 있어야 합니다.

독립형

독립형 데이터베이스는 /etc/oratab 항목을 기반으로만 검색됩니다.

아에스엠

ASM 인스턴스 항목은 /etc/oratab 파일에서 사용할 수 있어야 합니다.

RAC One 노드

RAC One Node 데이터베이스는 /etc/oratab 항목을 기반으로만 검색됩니다. 데이터베이스는 nomount, mount 또는 open 상태여야 합니다. /etc/oratab 파일에 데이터베이스 항목이 있어야 합니다.

데이터베이스가 이미 검색되었고 백업이 데이터베이스와 연결되어 있는 경우 RAC One Node 데이터베이스 상태는 이름이 변경됨 또는 삭제됨으로 표시됩니다.

데이터베이스가 이전된 경우 다음 단계를 수행해야 합니다.

1. 장애 조치된 RAC 노드의 /etc/oratab 파일에 재배치된 데이터베이스 항목을 수동으로 추가합니다.
2. 리소스를 수동으로 새로 고칩니다.
3. 리소스 페이지에서 RAC One Node 데이터베이스를 선택한 다음 데이터베이스 설정을 클릭합니다.
4. 데이터베이스를 구성하여 현재 데이터베이스를 호스팅하는 RAC 노드를 기본 클러스터 노드로 설정합니다.
5. SnapCenter 작업을 수행합니다.
6. 한 노드에서 다른 노드로 데이터베이스를 이전했고 이전 노드의 oratab 항목이 삭제되지 않은 경우 oratab 항목을 수동으로 삭제하여 동일한 데이터베이스가 두 번 표시되는 것을 방지하세요.

Oracle 버전 12cR2~18c, 19c 또는 21c의 경우

RAC 데이터베이스

RAC 데이터베이스는 `srvctl config` 명령을 사용하여 검색됩니다. `/etc/oratab` 파일에 데이터베이스 항목이 있어야 합니다.

독립형

독립형 데이터베이스는 `/etc/oratab` 파일의 항목과 `srvctl config` 명령의 출력을 기반으로 검색됩니다.

아에스엠

ASM 인스턴스 항목은 `/etc/oratab` 파일에 있을 필요가 없습니다.

RAC One 노드

RAC One Node 데이터베이스는 `srvctl config` 명령을 사용해서만 검색됩니다. 데이터베이스는 `nomount`, `mount` 또는 `open` 상태여야 합니다. 데이터베이스가 이미 검색되었고 백업이 데이터베이스와 연결되어 있는 경우 RAC One Node 데이터베이스 상태는 이름이 변경됨 또는 삭제됨으로 표시됩니다.

데이터베이스가 이전된 경우 다음 단계를 수행해야 합니다. 리소스를 수동으로 새로 고칩니다. . 리소스 페이지에서 RAC One Node 데이터베이스를 선택한 다음 데이터베이스 설정을 클릭합니다. . 데이터베이스를 구성하여 현재 데이터베이스를 호스팅하는 RAC 노드를 기본 클러스터 노드로 설정합니다. . SnapCenter 작업을 수행합니다.



`/etc/oratab` 파일에 Oracle 12cR2 및 18c 데이터베이스 항목이 있고 동일한 데이터베이스가 `srvctl config` 명령으로 등록된 경우 SnapCenter 중복된 데이터베이스 항목을 제거합니다. 오래된 데이터베이스 항목이 있는 경우 데이터베이스는 발견되지만 데이터베이스에 접근할 수 없게 되고 상태는 오프라인이 됩니다.

RAC 설정에서 선호하는 노드

Oracle Real Application Clusters(RAC) 설정에서 SnapCenter 백업 작업을 수행하는 데 사용하는 기본 노드를 지정할 수 있습니다. 기본 노드를 지정하지 않으면 SnapCenter 자동으로 노드를 기본 노드로 지정하고 해당 노드에 백업이 생성됩니다.

선호되는 노드는 RAC 데이터베이스 인스턴스가 있는 클러스터 노드 중 하나 또는 전체일 수 있습니다. 백업 작업은 선호도 순서대로 이러한 선호 노드에서만 실행됩니다.

예

RAC 데이터베이스 `cdbrac`에는 세 개의 인스턴스가 있습니다. 노드 1에 `cdbrac1`, 노드 2에 `cdbrac2`, 노드 3에 `cdbrac3`입니다.

`node1`과 `node2` 인스턴스는 기본 노드로 구성되며, `node2`는 첫 번째 기본 설정이고 `node1`은 두 번째 기본 설정입니다. 백업 작업을 수행할 때 작업은 우선적으로 노드2에서 시도됩니다. 이는 노드2가 첫 번째 기본 노드이기 때문입니다.

플러그인 에이전트가 호스트에서 실행되지 않거나, 호스트의 데이터베이스 인스턴스가 지정된 백업 유형에 필요한 상태가 아니거나, FlexASM 구성에서 `node2`의 데이터베이스 인스턴스가 로컬 ASM 인스턴스에서 제공되지 않는 등 여러 가지 이유로 `node2`가 백업할 수 없는 상태가 되면, 작업은 `node1`에서 시도됩니다.

`node3`은 선호 노드 목록에 없으므로 백업에 사용되지 않습니다.

Flex ASM 설정

Flex ASM 설정에서 RAC 클러스터의 노드 수보다 기수가 적으면 Leaf 노드는 기본 노드로 나열되지 않습니다. Flex ASM 클러스터 노드 역할에 변경 사항이 있는 경우 수동으로 검색하여 기본 노드가 새로 고쳐지도록 해야 합니다.

필수 데이터베이스 상태

백업이 성공적으로 완료되려면 기본 노드의 RAC 데이터베이스 인스턴스가 필요한 상태여야 합니다.

- 구성된 기본 노드의 RAC 데이터베이스 인스턴스 중 하나는 온라인 백업을 생성하기 위해 열린 상태여야 합니다.
- 구성된 기본 노드의 RAC 데이터베이스 인스턴스 중 하나는 마운트 상태여야 하며, 다른 기본 노드를 포함한 다른 모든 인스턴스는 오프라인 마운트 백업을 생성하려면 마운트 상태 이하여야 합니다.
- RAC 데이터베이스 인스턴스는 어떤 상태든 될 수 있지만 오프라인 종료 백업을 만들려면 기본 노드를 지정해야 합니다.

Oracle Recovery Manager를 사용하여 백업을 카탈로그화하는 방법

Oracle Recovery Manager(RMAN)를 사용하여 Oracle 데이터베이스의 백업을 카탈로그화하고 Oracle RMAN 저장소에 백업 정보를 저장할 수 있습니다.

카탈로그화된 백업은 나중에 블록 수준 복원이나 테이블스페이스 지정 시점 복구 작업에 사용할 수 있습니다. 이러한 카탈로그화된 백업이 필요하지 않으면 카탈로그 정보를 제거할 수 있습니다.

카탈로그화를 위해서는 데이터베이스가 마운트된 상태 이상이어야 합니다. 데이터 백업, 보관 로그 백업 및 전체 백업에 대한 카탈로그 작성을 수행할 수 있습니다. 여러 데이터베이스가 있는 리소스 그룹의 백업에 대해 카탈로그화가 활성화된 경우 각 데이터베이스에 대해 카탈로그화가 수행됩니다. Oracle RAC 데이터베이스의 경우 카탈로그화는 데이터베이스가 최소한 마운트된 상태인 기본 노드에서 수행됩니다.

RAC 데이터베이스의 백업을 카탈로그화하려면 해당 데이터베이스에 대해 다른 작업이 실행되고 있지 않은지 확인하세요. 다른 작업이 실행 중이면 카탈로그 작업은 대기열에 추가되지 않고 실패합니다.

외부 카탈로그 데이터베이스

기본적으로 대상 데이터베이스 제어 파일은 카탈로그화에 사용됩니다. 외부 카탈로그 데이터베이스를 추가하려면 SnapCenter 그래픽 사용자 인터페이스(GUI)의 데이터베이스 설정 마법사를 사용하여 외부 카탈로그의 자격 증명과 TNS(Transparent Network Substrate) 이름을 지정하여 구성할 수 있습니다. -OracleRmanCatalogCredentialName 및 -OracleRmanCatalogTnsName 옵션과 함께 Configure-SmOracleDatabase 명령을 실행하여 CLI에서 외부 카탈로그 데이터베이스를 구성할 수도 있습니다.

RMAN 명령

SnapCenter GUI에서 Oracle 백업 정책을 생성하는 동안 카탈로그화 옵션을 활성화한 경우 백업은 백업 작업의 일부로 Oracle RMAN을 사용하여 카탈로그화됩니다. 다음을 실행하여 백업의 지연 카탈로그를 수행할 수도 있습니다.

Catalog-SmBackupWithOracleRMAN 명령.

백업을 카탈로그화한 후 다음을 실행할 수 있습니다. Get-SmBackupDetails 카탈로그화된 데이터 파일의 태그, 제어 파일 카탈로그 경로, 카탈로그화된 보관 로그 위치와 같은 카탈로그화된 백업 정보를 얻기 위한 명령입니다.

명명 형식

ASM 디스크 그룹 이름이 16자 이상이면 SnapCenter 3.0부터 백업에 사용되는 명명 형식은 SC_HASHCODEofDISKGROUP_DBSID_BACKUPID입니다. 그러나 디스크 그룹 이름이 16자 미만이면 백업에

사용되는 명명 형식은 DISKGROUPNAME_DBSID_BACKUPID입니다. 이는 SnapCenter 2.0에서 사용되는 형식과 동일합니다.

HASHCODEofDISKGROUP은 각 ASM 디스크 그룹에 대해 자동으로 생성되는 고유한 숫자(2~10자리)입니다.

교차 확인 작업

저장소 레코드가 물리적 상태와 일치하지 않는 백업에 대한 오래된 RMAN 저장소 정보를 업데이트하기 위해 교차 검사를 수행할 수 있습니다. 예를 들어, 사용자가 운영 체제 명령을 사용하여 디스크에서 보관된 로그를 제거하는 경우, 제어 파일은 실제로는 로그가 디스크에 있지 않더라도 여전히 로그가 디스크에 있다고 표시합니다.

교차 검사 작업을 통해 제어 파일을 해당 정보로 업데이트할 수 있습니다. Set-SmConfigSettings 명령을 실행하고 ENABLE_CROSSCHECK 매개변수에 TRUE 값을 할당하여 교차 검사를 활성화할 수 있습니다. 기본값은 FALSE로 설정됩니다.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings  
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

카탈로그 정보 제거

Uncatalog-SmBackupWithOracleRMAN 명령을 실행하면 카탈로그 정보를 제거할 수 있습니다. SnapCenter GUI를 사용하여 카탈로그 정보를 제거할 수 없습니다. 그러나 카탈로그화된 백업의 정보는 백업을 삭제하거나 해당 카탈로그화된 백업과 연관된 보존 및 리소스 그룹을 삭제하는 동안 제거됩니다.



SnapCenter 호스트를 강제로 삭제하는 경우 해당 호스트와 연관된 카탈로그화된 백업 정보는 제거되지 않습니다. 호스트를 강제로 삭제하기 전에 해당 호스트에 대한 모든 카탈로그 백업 정보를 제거해야 합니다.

작업 시간이 ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT 매개변수에 지정된 시간 초과 값을 초과하여 카탈로그화 및 카탈로그 해제가 실패하는 경우 다음 명령을 실행하여 매개변수 값을 수정해야 합니다.

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType  
Plugin -PluginCode SCO-ConfigSettings  
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

매개변수 값을 수정한 후 다음 명령을 실행하여 SnapCenter 플러그인 Loader (SPL) 서비스를 다시 시작합니다.

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 Get-Help command_name을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수 있습니다. ["SnapCenter 소프트웨어 명령 참조 가이드"](#).

백업 특정 사전 스크립트 및 사후 스크립트를 위한 사전 정의된 환경 변수

SnapCenter 사용하면 백업 정책을 생성하는 동안 프리스크립트와 포스트스크립트를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다. 이 기능은 VMDK를 제외한 모든 Oracle 구성에서 지원됩니다.

SnapCenter 셸 스크립트가 실행되는 환경에서 직접 액세스할 수 있는 매개변수 값을 미리 정의합니다. 스크립트를 실행할 때 이러한 매개변수의 값을 수동으로 지정할 필요는 없습니다.

- ***SC_JOB_ID***는 작업의 작업 ID를 지정합니다.

예: 256

- ***SC_ORACLE_SID***는 데이터베이스의 시스템 식별자를 지정합니다.

작업에 여러 데이터베이스가 관련된 경우 매개변수에는 파이프로 구분된 데이터베이스 이름이 포함됩니다.

이 매개변수는 애플리케이션 볼륨에 대해 채워집니다.

예: NFSB32|NFSB31

- ***SC_HOST***는 데이터베이스의 호스트 이름을 지정합니다.

RAC의 경우 호스트 이름은 백업이 수행되는 호스트의 이름이 됩니다.

이 매개변수는 애플리케이션 볼륨에 대해 채워집니다.

예: scsmohost2.gdl.englabe.netapp.com

- ***SC_OS_USER***는 데이터베이스의 운영 체제 소유자를 지정합니다.

데이터는 <db1>@<osuser1>|<db2>@<osuser2> 형식으로 지정됩니다.

예: NFSB31@oracle|NFSB32@oracle

- ***SC_OS_GROUP***은 데이터베이스의 운영 체제 그룹을 지정합니다.

데이터는 <db1>@<osgroup1>|<db2>@<osgroup2> 형식으로 지정됩니다.

예: NFSB31@install|NFSB32@oinstall

- **SC_BACKUP_TYPE**은 백업 유형(온라인 전체, 온라인 데이터, 온라인 로그, 오프라인 종료, 오프라인 마운트)을 지정합니다.

예:

- 전체 백업의 경우: ONLINEFULL
- 데이터 전용 백업: ONLINEDATA
- 로그 전용 백업의 경우: ONLINELOG

- ***SC_BACKUP_NAME***은 백업의 이름을 지정합니다.

이 매개변수는 애플리케이션 볼륨에 대해 채워집니다.

예: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1|AV@RG2_scspr2417819002_07-20-2021_12.16.48.9267

- ***SC_BACKUP_ID***는 백업 ID를 지정합니다.

이 매개변수는 애플리케이션 볼륨에 대해 채워집니다.

예: DATA@203|LOG@205|AV@207

- *SC_ORACLE_HOME*은 Oracle 홈 디렉토리의 경로를 지정합니다.

예: NFSB32@/ora01/app/oracle/product/18.1.0/db_1|NFSB31@/ora01/app/oracle/product/18.1.0/db_1

- *SC_BACKUP_RETENTION*은 정책에 정의된 보존 기간을 지정합니다.

예:

- 전체 백업의 경우: 시간별|DATA@DAYS:3|LOG@COUNT:4
- 주문형 데이터 전용 백업의 경우: Ondemand|DATA@COUNT:2
- 주문형 로그 전용 백업의 경우: Ondemand|LOG@COUNT:2

- *SC_RESOURCE_GROUP_NAME*은 리소스 그룹의 이름을 지정합니다.

예: RG1

- *SC_BACKUP_POLICY_NAME*은 백업 정책의 이름을 지정합니다.

예: backup_policy

- *SC_AV_NAME*은 애플리케이션 볼륨의 이름을 지정합니다.

예: AV1|AV2

- *SC_PRIMARY_DATA_VOLUME_FULL_PATH*는 데이터 파일 디렉토리의 볼륨에 대한 SVM의 스토리지 매핑을 지정합니다. 이는 LUN과 QTree의 부모 볼륨 이름이 됩니다.

데이터는 <db1>@<SVM1:volume1>|<db2>@<SVM2:volume2> 형식으로 지정됩니다.

예:

- 동일한 리소스 그룹에 있는 2개의 데이터베이스의 경우:
NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA
- 여러 볼륨에 걸쳐 데이터 파일이 분산된 단일 데이터베이스의 경우:
buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/scspr2417819002_NFS

- *SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH*는 로그 파일 디렉토리의 볼륨에 대한 SVM의 스토리지 매핑을 지정합니다. 이는 LUN과 QTree의 부모 볼륨 이름이 됩니다.

예:

- 단일 데이터베이스 인스턴스의 경우: buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
- 여러 데이터베이스 인스턴스의 경우:
NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO|NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO

- *SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG*는 스토리지 시스템 이름과 볼륨 이름을 포함하는 스냅샷 목록을 지정합니다.

예:

- 단일 데이터베이스 인스턴스의 경우:
buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- 여러 데이터베이스 인스턴스의 경우:
NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

- *SC_PRIMARY_SNAPSHOT_NAMES*는 백업 중에 생성된 기본 스냅샷의 이름을 지정합니다.

예:

- 단일 데이터베이스 인스턴스의 경우: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- 여러 데이터베이스 인스턴스의 경우: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- 일관성을 위해 2개의 볼륨을 포함하는 그룹 스냅샷: cg3_R80404CBEF5V1_04-05-2021_03.08.03.4945_0_bfc279cc-28ad-465c-9d60-5487ac17b25d_2021_4_5_3_8_58_350

- *SC_PRIMARY_MOUNT_POINTS*는 백업의 일부인 마운트 지점 세부 정보를 지정합니다.

세부 정보에는 볼륨이 마운트된 디렉토리가 포함되지만 백업 중인 파일의 직접적인 부모는 포함되지 않습니다. ASM 구성의 경우 디스크 그룹의 이름입니다.

데이터는 <db1>@<mountpoint1,mountpoint2>|<db2>@<mountpoint1,mountpoint2> 형식으로 지정됩니다.

예:

- 단일 데이터베이스 인스턴스의 경우: /mnt/nfsdb3_data,/mnt/nfsdb3_log,/mnt/nfsdb3_data1
- 여러 데이터베이스 인스턴스의 경우:
NFSB31@/mnt/nfsdb31_data,/mnt/nfsdb31_log,/mnt/nfsdb31_data1|NFSB32@/mnt/nfsdb32_data,/mnt/nfsdb32_log,/mnt/nfsdb32_data1
- ASM의 경우: +DATA2DG,+LOG2DG

- *SC_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS*는 각 마운트 지점의 백업 중에 생성된 스냅샷의 이름을 지정합니다.

예:

- 단일 데이터베이스 인스턴스의 경우: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log
- 여러 데이터베이스 인스턴스의 경우: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-

2021_02.28.26.3973_1:/mnt/nfsb31_log|NFSB31@RG2_scspr2417819002_07-21-
2021_02.28.26.3973_0:/mnt/nfsb31_data, RG2_scspr2417819002_07-21-
2021_02.28.26.3973_1:/mnt/nfsb32_log

- ***SC_ARCHIVELOGS_LOCATIONS***는 보관 로그 디렉토리의 위치를 지정합니다.

디렉토리 이름은 보관 로그 파일의 바로 상위가 됩니다. 보관 로그가 두 개 이상의 위치에 저장되면 모든 위치가 캡처됩니다. 여기에는 FRA 시나리오도 포함됩니다. 디렉토리에 소프트링크가 사용되면 동일한 내용이 채워집니다.

예:

- NFS의 단일 데이터베이스의 경우: /mnt/nfsdb2_log
- NFS의 여러 데이터베이스와 두 개의 다른 위치에 배치된 NFSB31 데이터베이스 아카이브 로그의 경우:
NFSB31@/mnt/nfsdb31_log1,/mnt/nfsdb31_log2|NFSB32@/mnt/nfsdb32_log
- ASM의 경우: +LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15

- ***SC_REDO_LOGS_LOCATIONS***는 리두 로그 디렉토리의 위치를 지정합니다.

디렉토리 이름은 리두 로그 파일의 바로 상위 파일이 됩니다. 디렉토리에 소프트링크가 사용되면 동일한 내용이 채워집니다.

예:

- NFS의 단일 데이터베이스의 경우: /mnt/nfsdb2_data/newdb1
- NFS에 있는 여러 데이터베이스의 경우:
NFSB31@/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/newdb32
- ASM의 경우: +LOG2DG/ASMDB2/ONLINELOG

- ***SC_CONTROL_FILES_LOCATIONS***는 제어 파일 디렉토리의 위치를 지정합니다.

디렉토리 이름은 제어 파일의 바로 상위가 됩니다. 디렉토리에 소프트링크가 사용되면 동일한 내용이 채워집니다.

예:

- NFS의 단일 데이터베이스의 경우: /mnt/nfsdb2_data/fra/newdb1,/mnt/nfsdb2_data/newdb1
- NFS에 있는 여러 데이터베이스의 경우:
NFSB31@/mnt/nfsdb31_data/fra/newdb31,/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/fra/newdb32,/mnt/nfsdb32_data/newdb32
- ASM의 경우: +LOG2DG/ASMDB2/CONTROLFILE

- ***SC_DATA_FILES_LOCATIONS***는 데이터 파일 디렉토리의 위치를 지정합니다.

디렉토리 이름은 데이터 파일의 바로 상위 이름이 됩니다. 디렉토리에 소프트링크가 사용되면 동일한 내용이 채워집니다.

예:

- NFS의 단일 데이터베이스의 경우: /mnt/nfsdb3_data1,/mnt/nfsdb3_data/NEWDB3/datafile
- NFS에 있는 여러 데이터베이스의 경우:
NFSB31@/mnt/nfsdb31_data1,/mnt/nfsdb31_data/NEWDB31/datafile|NFSB32@/mnt/nfsdb32_data1,/mnt/nfsdb32_data/NEWDB32/datafile

◦ ASM의 경우: +DATA2DG/ASMDDB2/DATAFILE,+DATA2DG/ASMDDB2/TEMPFILE

- *SC_SNAPSHOT_LABEL*은 보조 레이블의 이름을 지정합니다.

예: 시간별, 일별, 주별, 월별 또는 사용자 정의 라벨.

지원되는 구분 기호

- *.*는 SVM 이름과 볼륨 이름을 구분하는 데 사용됩니다.

예: buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

- *@*는 데이터베이스 이름과 데이터를 구분하고 키와 값을 구분하는 데 사용됩니다.

예:

◦ NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

◦ NFSB31@오라클|NFSB32@오라클

- *|*는 두 개의 서로 다른 데이터베이스 간의 데이터를 구분하고 SC_BACKUP_ID, SC_BACKUP_RETENTION 및 SC_BACKUP_NAME 매개변수에 대한 두 개의 서로 다른 엔터티 간의 데이터를 구분하는 데 사용됩니다.

예:

◦ 데이터@203|로그@205

◦ 시간별|데이터@일:3|로그@카운트:4

◦ 데이터@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|로그@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1

- */*는 SC_PRIMARY_SNAPSHOT_NAMES 및 SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG 매개변수에 대한 볼륨 이름과 스냅샷을 구분하는 데 사용됩니다.

예: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

- *,*는 동일한 DB에 대한 변수 집합을 구분하는 데 사용됩니다.

예: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

백업 보존 옵션

백업 사본을 보관할 일수를 선택하거나 보관할 백업 사본 수를 지정할 수 있으며, ONTAP 최대 255개 사본까지 보관할 수 있습니다. 예를 들어, 귀하의 조직에서는 10일 분의 백업 사본이나 130개의 백업 사본을 보관하도록 요구할 수 있습니다.

정책을 생성하는 동안 백업 유형과 일정 유형에 대한 보존 옵션을 지정할 수 있습니다.

SnapMirror 복제를 설정하면 보존 정책이 대상 볼륨에 미러링됩니다.

SnapCenter 일정 유형과 일치하는 보존 레이블이 있는 보관된 백업을 삭제합니다. 리소스 또는 리소스 그룹의 일정 유형이 변경된 경우 이전 일정 유형 레이블이 지정된 백업이 시스템에 남아 있을 수 있습니다.



백업 사본을 장기간 보관하려면 SnapVault 백업을 사용해야 합니다.

백업 일정

백업 빈도(일정 유형)는 정책에 지정되고, 백업 일정은 리소스 그룹 구성에 지정됩니다. 백업 빈도나 일정을 결정하는 가장 중요한 요소는 리소스의 변화율과 데이터의 중요도입니다. 자주 사용되는 리소스는 매시간 백업하고, 거의 사용되지 않는 리소스는 하루에 한 번 백업할 수도 있습니다. 기타 요소로는 조직에 대한 리소스의 중요성, 서비스 수준 계약(SLA), 복구 지점 목표(RPO) 등이 있습니다.

SLA는 기대되는 서비스 수준을 정의하고 서비스 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 수명에 대한 전략을 정의합니다. SLA와 RPO는 데이터 보호 전략에 기여합니다.

많이 사용되는 리소스의 경우에도 하루에 한두 번 이상 전체 백업을 실행할 필요는 없습니다. 예를 들어, 정기적인 트랜잭션 로그 백업을 통해 필요한 백업을 확보하는 데 충분할 수 있습니다. 데이터베이스를 더 자주 백업할수록 SnapCenter 복원 시 사용해야 하는 트랜잭션 로그가 줄어들어 복원 작업이 더 빨라질 수 있습니다.

백업 일정은 다음과 같이 두 부분으로 구성됩니다.

• 백업 주파수

일부 플러그인의 경우 스케줄 유형이라고 하는 백업 빈도(백업을 수행하는 빈도)는 정책 구성의 일부입니다. 정책의 백업 빈도를 시간별, 일별, 주별 또는 월별로 선택할 수 있습니다. 이러한 주파수를 선택하지 않으면 생성된 정책은 주문형 정책만입니다. 설정 > *정책*을 클릭하면 정책에 액세스할 수 있습니다.

• 백업 일정

백업 일정(백업을 정확히 언제 수행해야 하는지)은 리소스 그룹 구성의 일부입니다. 예를 들어, 주간 백업에 대한 정책이 구성된 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 일정을 구성할 수 있습니다. 리소스 > *리소스 그룹*을 클릭하면 리소스 그룹 일정에 액세스할 수 있습니다.

백업 명명 규칙

기본 스냅샷 명명 규칙을 사용하거나 사용자 지정 명명 규칙을 사용할 수 있습니다. 기본 백업 명명 규칙은 스냅샷 이름에 타임스탬프를 추가하여 복사본이 생성된 시기를 식별하는 데 도움이 됩니다.

스냅샷은 다음과 같은 기본 명명 규칙을 사용합니다.

resourcegroupname_hostname_timestamp

다음 예와 같이 논리적으로 백업 리소스 그룹의 이름을 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예에서 구문 요소는 다음과 같은 의미를 갖습니다.

- `_dts1_`은 리소스 그룹 이름입니다.
- `_mach1x88_`은 호스트 이름입니다.
- `_03-12-2015_23.17.26_`은 날짜와 타임스탬프입니다.

또는, *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택하여 리소스나 리소스 그룹을 보호하는 동안 스냅샷 이름 형식을 지정할 수 있습니다. 예를 들어, `customtext_resourcegroup_policy_hostname` 또는 `resourcegroup_hostname`입니다. 기본적으로 타임스탬프 접미사는 스냅샷 이름에 추가됩니다.

Oracle 데이터베이스 백업 요구 사항

Oracle 데이터베이스를 백업하기 전에 필수 구성 요소가 완료되었는지 확인해야 합니다.

- 정책이 첨부된 리소스 그룹을 만들어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에 “snapmirror all” 권한이 포함되어야 합니다. 하지만 “vsadmin” 역할을 사용하는 경우 “snapmirror all” 권한은 필요하지 않습니다.
- 백업 작업에 사용되는 집계를 데이터베이스에서 사용하는 스토리지 가상 머신(SVM)에 할당했어야 합니다.
- 해당 데이터베이스에 대해 보조 보호가 활성화된 경우, 해당 데이터베이스에 속한 모든 데이터 볼륨과 보관 로그 볼륨이 보호되는지 확인해야 합니다.
- Oracle DBVERIFY 유틸리티를 사용하여 백업을 검증하려면 ASM 디스크 그룹에 파일이 있는 데이터베이스가 “MOUNT” 또는 “OPEN” 상태여야 합니다.
- 볼륨 마운트 지점 길이가 240자를 넘지 않는지 확인해야 합니다.
- 백업되는 데이터베이스가 큰 경우(TB 단위 크기) SnapCenter 서버 호스트의 `C:\Program Files\NetApp\SMCore\SMCoreServiceHost.exe.config` 파일에서 RESTTimeout 값을 86400000ms로 늘려야 합니다.

값을 수정하는 동안 실행 중인 작업이 없는지 확인하고 값을 늘린 후 SnapCenter SMCore 서비스를 다시 시작합니다.

백업에 사용 가능한 Oracle 데이터베이스를 찾아보세요

리소스는 SnapCenter 에서 관리하는 호스트의 Oracle 데이터베이스입니다. 사용 가능한 데이터베이스를 발견한 후 이러한 데이터베이스를 리소스 그룹에 추가하여 데이터 보호 작업을 수행할 수 있습니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 생성, 자격 증명 추가 등의 작업을 완료했어야 합니다.
- 데이터베이스가 VMDK(가상 머신 디스크) 또는 RDM(원시 장치 매핑)에 있는 경우 SnapCenter Plug-in for VMware vSphere 배포하고 SnapCenter 에 플러그인을 등록해야 합니다.

자세한 내용은 다음을 참조하세요. "[SnapCenter Plug-in for VMware vSphere 배포](#)".

- 데이터베이스가 VMDK 파일 시스템에 있는 경우 vCenter에 로그인하고 **VM** 옵션 > 고급 > *구성 편집*으로 이동하여 VM에 대한 `disk.enableUUID` 값을 true로 설정해야 합니다.
- SnapCenter Oracle 데이터베이스의 다양한 유형과 버전을 검색하는 프로세스를 검토했을 것입니다.

1단계: SnapCenter 데이터베이스가 아닌 항목을 검색하지 못하도록 방지

SnapCenter oratab 파일에 추가된 데이터베이스가 아닌 항목을 검색하지 못하도록 방지할 수 있습니다.

단계

1. Oracle용 플러그인을 설치한 후 루트 사용자는 `/var/opt/snapcenter/sco/etc/` 디렉토리 아래에 **sc_oratab.config** 파일을 만들어야 합니다.

Oracle 바이너리 소유자와 그룹에 쓰기 권한을 부여하여 나중에 파일을 유지 관리할 수 있도록 합니다.

2. 데이터베이스 관리자는 **sc_oratab.config** 파일에 데이터베이스가 아닌 항목을 추가해야 합니다.

`/etc/oratab` 파일에 있는 비데이터베이스 항목에 대해 정의된 동일한 형식을 유지하는 것이 좋습니다. 아니면 사용자가 비데이터베이스 엔터티 문자열을 추가할 수도 있습니다.



문자열은 대소문자를 구분합니다. 처음에 #이 있는 모든 텍스트는 주석으로 처리됩니다. 주석은 데이터베이스가 아닌 이름 뒤에 추가할 수 있습니다.

For example:

```
-----
# Sample entries
# Each line can have only one non-database name
# These are non-database name
oratar # Added by the admin group -1
#Added by the script team
NEWSPT
DBAGNT:/ora01/app/oracle/product/agent:N
-----
```

3. 리소스를 찾아보세요.

*sc_oratab.config*에 추가된 데이터베이스가 아닌 항목은 리소스 페이지에 나열되지 않습니다.



SnapCenter 플러그인을 업그레이드하기 전에 sc_oratab.config 파일을 백업하는 것이 좋습니다.

2단계: 리소스 찾기

플러그인을 설치하면 해당 호스트의 모든 데이터베이스가 자동으로 검색되어 리소스 페이지에 표시됩니다.

데이터베이스 검색이 성공하려면 데이터베이스가 최소한 마운트된 상태 이상이어야 합니다. Oracle Real Application Clusters(RAC) 환경에서 검색이 수행되는 호스트의 RAC 데이터베이스 인스턴스는 데이터베이스 인스턴스 검색이 성공하려면 최소한 마운트된 상태 이상이어야 합니다. 성공적으로 검색된 데이터베이스만 리소스 그룹에 추가할 수 있습니다.

호스트에서 Oracle 데이터베이스를 삭제한 경우 SnapCenter Server는 이를 인식하지 못하고 삭제된 데이터베이스를 나열합니다. SnapCenter 리소스 목록을 업데이트하려면 리소스를 수동으로 새로 고쳐야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *데이터베이스*를 선택합니다.

딸깍 하는 소리  필터 아이콘]을 선택한 다음 호스트 이름과 데이터베이스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 imagfilter_icon.gif[필터 아이콘]_icon.png] 아이콘을 클릭하여 필터 창을 닫을 수 있습니다.

3. *리소스 새로고침*을 클릭하세요.

RAC One Node 시나리오에서 데이터베이스는 현재 호스팅되는 노드의 RAC 데이터베이스로 검색됩니다.

결과

데이터베이스는 데이터베이스 유형, 호스트 또는 클러스터 이름, 연관된 리소스 그룹 및 정책, 상태와 같은 정보와 함께 표시됩니다.



SnapCenter 외부에서 데이터베이스 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

- 데이터베이스가 NetApp 스토리지 시스템이 아닌 다른 시스템에 있는 경우 사용자 인터페이스의 전체 상태 열에 백업할 수 없음 메시지가 표시됩니다.

NetApp 스토리지 시스템이 아닌 데이터베이스에는 데이터 보호 작업을 수행할 수 없습니다.

- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되지 않은 경우 사용자 인터페이스의 전체 상태 열에 보호되지 않음 메시지가 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되는 경우 사용자 인터페이스의 전체 상태 열에 백업 가능 메시지가 표시됩니다.



Oracle 데이터베이스 인증을 활성화한 경우 리소스 보기에 빨간색 자물쇠 아이콘이 표시됩니다. 데이터베이스를 보호하거나 리소스 그룹에 추가하여 데이터 보호 작업을 수행하려면 데이터베이스 자격 증명을 구성해야 합니다.

Oracle 데이터베이스에 대한 백업 정책 생성

SnapCenter 사용하여 Oracle 데이터베이스 리소스를 백업하기 전에 백업하려는 리소스 또는 리소스 그룹에 대한 백업 정책을 만들어야 합니다. 백업 정책은 백업을 관리, 일정을 정하고

보관하는 방법을 규정하는 일련의 규칙입니다. 복제, 스크립트, 백업 유형 설정도 지정할 수 있습니다. 정책을 만들면 다른 리소스나 리소스 그룹에서 정책을 재사용할 때 시간을 절약할 수 있습니다.

시작하기 전에

- 백업 전략을 정의했어야 합니다.
- SnapCenter 설치, 호스트 추가, 데이터베이스 검색, 스토리지 시스템 연결 생성 등의 작업을 완료하여 데이터 보호를 준비했어야 합니다.
- 스냅샷을 미리 또는 볼트 보조 스토리지에 복제하는 경우 SnapCenter 관리자가 소스 및 대상 볼륨 모두에 대한 SVM을 할당해야 합니다.
- 루트가 아닌 사용자로 플러그인을 설치한 경우, prescript 및 postscript 디렉토리에 대한 실행 권한을 수동으로 할당해야 합니다.
- SnapMirror Active Sync의 특정 전제 조건과 제한 사항을 검토하세요. 자세한 내용은 다음을 참조하세요.
["SnapMirror Active Sync에 대한 개체 제한"](#).

이 작업에 관하여

'특정 기간 동안 백업 사본을 보관합니다' 옵션을 선택한 경우 SnapLock 보관 기간은 언급된 보관 기간보다 짧거나 같아야 합니다.

+ 스냅샷 잠금 기간을 지정하면 보존 기간이 만료될 때까지 스냅샷이 삭제되는 것을 방지할 수 있습니다. 이를 통해 정책에 지정된 수보다 더 많은 수의 스냅샷을 보존할 수 있습니다.

+ ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속합니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *정책*을 클릭합니다.
3. 드롭다운 목록에서 *Oracle Database*를 선택합니다.
4. *새로 만들기*를 클릭합니다.
5. 이름 페이지에서 정책 이름과 세부 정보를 입력합니다.
6. 정책 유형 페이지에서 다음 단계를 수행합니다.
 - a. 저장 유형을 선택하세요.
 - b. 정책 범위 선택:
 - *온라인 백업을 생성*하려면 *온라인 백업*을 선택하세요.

모든 데이터 파일, 제어 파일, 보관 로그 파일을 백업할지, 데이터 파일과 제어 파일만 백업할지, 또는 보관 로그 파일만 백업할지 지정해야 합니다.

- 오프라인 백업을 생성하려면 *오프라인 백업*을 선택한 후 다음 옵션 중 하나를 선택하세요.
 - 데이터베이스가 마운트된 상태일 때 오프라인 백업을 만들려면 *마운트*를 선택하세요.
 - 데이터베이스를 종료 상태로 변경하여 오프라인 종료 백업을 만들려면 *종료*를 선택합니다.

플러그형 데이터베이스(PDB)가 있고 백업을 생성하기 전에 PDB 상태를 저장하려면 *PDB 상태 저장*을 선택해야 합니다. 이렇게 하면 백업이 생성된 후 PDB를 원래 상태로 되돌릴 수 있습니다.

- c. Oracle Recovery Manager(RMAN)를 사용하여 백업을 카탈로그화하려면 *Oracle Recovery Manager(RMAN)를 사용하여 백업 카탈로그화*를 선택하세요.

GUI를 사용하거나 SnapCenter CLI 명령 Catalog-SmBackupWithOracleRMAN을 사용하여 한 번에 하나의 백업에 대한 지연 카탈로그화를 수행할 수 있습니다.



RAC 데이터베이스의 백업을 카탈로그화하려면 해당 데이터베이스에 대해 다른 작업이 실행되고 있지 않은지 확인하세요. 다른 작업이 실행 중이면 카탈로그 작업은 대기열에 추가되지 않고 실패합니다.

- d. 백업 후 보관 로그를 정리하려면 *백업 후 보관 로그 정리*를 선택하세요.



데이터베이스에 구성되지 않은 아카이브 로그 대상에서 아카이브 로그를 정리하는 작업은 건너뛸니다.



Oracle Standard Edition을 사용하는 경우 아카이브 로그 백업을 수행하는 동안 LOG_ARCHIVE_DEST 및 LOG_ARCHIVE_DUPLEX_DEST 매개변수를 사용할 수 있습니다.

- 백업의 일부로 보관 로그 파일을 선택한 경우에만 보관 로그를 삭제할 수 있습니다.



삭제 작업이 성공하려면 RAC 환경의 모든 노드가 모든 보관 로그 위치에 액세스할 수 있어야 합니다.

만약 당신이 원한다면...	그 다음에...
모든 보관 로그 삭제	*모든 보관 로그 삭제*를 선택합니다.
오래된 보관 로그 삭제	*다음 기간보다 오래된 보관 로그 삭제*를 선택한 다음, 삭제할 보관 로그의 기간을 일수와 시간 단위로 지정합니다.
모든 대상에서 보관 로그 삭제	*모든 대상에서 보관 로그 삭제*를 선택합니다.
백업의 일부인 로그 대상에서 보관 로그를 삭제합니다.	*백업에 포함된 대상에서 보관 로그 삭제*를 선택합니다.

+

☒ Prune archive logs after backup

Prune log retention setting

☐ Delete all archive logs

☒ Delete archive logs older than days hours

Prune log destination setting

☐ Delete archive logs from all the destinations

☒ Delete archive logs from the destinations which are part of backup

7. 스냅샷 및 복제 페이지에서 다음 단계를 수행합니다.

a. 주문형, 매시간, 매일, 매주, 매월 중에서 선택하여 일정 빈도를 지정하세요.



리소스 그룹을 생성하는 동안 백업 작업에 대한 일정(시작 날짜 및 종료 날짜)을 지정할 수 있습니다. 이를 통해 동일한 정책과 백업 빈도를 공유하는 리소스 그룹을 만들 수 있지만, 각 정책에 다른 백업 일정을 할당할 수도 있습니다.



오전 2시로 예약한 경우, 일광 절약 시간제(DST) 기간에는 일정이 실행되지 않습니다.

a. 데이터 스냅샷 보존 설정 섹션에서 백업 유형 페이지에서 선택한 백업 유형과 일정 유형에 대한 보존 설정을 지정합니다.

만약 당신이 원한다면...	그 다음에...
특정 수의 스냅샷을 보관하세요	*보관할 사본*을 선택한 다음 보관하려는 스냅샷 수를 지정합니다. 스냅샷 수가 지정된 수를 초과하면 스냅샷이 삭제되고 가장 오래된 사본이 먼저 삭제됩니다. 최대 보존 값은 1018입니다. 보존 기간이 기본 ONTAP 버전에서 지원하는 것보다 높은 값으로 설정된 경우 백업이 실패합니다. SnapVault 복제를 활성화하려면 보존 횟수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷이 대상에 복제될 때까지 첫 번째 스냅샷이 SnapVault 관계에 대한 참조 스냅샷이 되기 때문에 보존 작업이 실패할 수 있습니다.
스냅샷을 특정 일수 동안 보관하세요	*사본 보관 기간*을 선택한 다음, 스냅샷을 삭제하기 전에 보관할 일수를 지정합니다.

스냅샷 복사 잠금 기간	*스냅샷 복사 잠금 기간*을 선택하고 기간을 일, 월 또는 년 단위로 지정합니다. SnapLock 보존 기간은 100년 미만이어야 합니다.

- b. 보관 로그 스냅샷 보존 설정 섹션에서 백업 유형 페이지에서 선택한 백업 유형과 일정 유형에 대한 보존 설정을 지정합니다.

만약 당신이 원한다면...	그 다음에...
특정 수의 스냅샷을 보관하세요	*보관할 사본*을 선택한 다음 보관하려는 스냅샷 수를 지정합니다. 스냅샷 수가 지정된 수를 초과하면 스냅샷이 삭제되고 가장 오래된 사본이 먼저 삭제됩니다.  최대 보존 값은 1018입니다. 보존 기간이 기본 ONTAP 버전에서 지원하는 것보다 높은 값으로 설정된 경우 백업이 실패합니다.  SnapVault 복제를 활성화하려면 보존 횟수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷이 대상에 복제될 때까지 첫 번째 스냅샷이 SnapVault 관계에 대한 참조 스냅샷이 되기 때문에 보존 작업이 실패할 수 있습니다.
스냅샷을 특정 일수 동안 보관하세요	*사본 보관 기간*을 선택한 다음, 스냅샷을 삭제하기 전에 보관할 일수를 지정합니다.
스냅샷 복사 잠금 기간	*스냅샷 복사 잠금 기간*을 선택하고 기간을 일, 월 또는 년 단위로 지정합니다. SnapLock 보존 기간은 100년 미만이어야 합니다.

- c. 정책 라벨을 선택하세요.



원격 복제를 위해 기본 스냅샷에 SnapMirror 레이블을 할당하면 기본 스냅샷이 SnapCenter에서 ONTAP 보조 시스템으로 스냅샷 복제 작업을 오프로드할 수 있습니다. 정책 페이지에서 SnapMirror 또는 SnapVault 옵션을 활성화하지 않고도 이 작업을 수행할 수 있습니다.

8. 보조 복제 옵션 선택 섹션에서 다음 보조 복제 옵션 중 하나 또는 둘 다를 선택합니다.



*보조 스냅샷 복사 잠금 기간*에 대한 보조 복제 옵션을 선택해야 적용됩니다.

이 분야에서는...	이렇게 하세요...
로컬 스냅샷을 생성한 후 SnapMirror 업데이트	다른 볼륨에 백업 세트의 미러 복사본을 생성하려면 이 필드를 선택합니다(SnapMirror 복제). SnapMirror Active Sync의 경우 이 옵션을 활성화해야 합니다. 2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고침됩니다.
로컬 스냅샷을 생성한 후 SnapVault 업데이트	디스크 간 백업 복제(SnapVault 백업)를 수행하려면 이 옵션을 선택하세요. ONTAP 에서 SnapLock Vault로 알려진 보조 노드에만 SnapLock 구성된 경우 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 보조 노드의 잠금 기간이 새로 고침됩니다. SnapLock Vault에 대한 자세한 내용은 다음을 참조하세요. "볼트 대상의 WORM에 스냅샷 복사본 커밋" 보다 "토폴로지 페이지에서 Oracle 데이터베이스 백업 및 복제본 보기" .
오류 재시도 횟수	작업이 중지되기 전에 허용할 수 있는 최대 복제 시도 횟수를 입력하세요.



보조 저장소의 스냅샷 최대 한도에 도달하지 않도록 하려면 ONTAP 에서 보조 저장소 SnapMirror 보존 정책을 구성해야 합니다.

9. 스크립트 페이지에서 백업 작업 전이나 후에 실행할 프리스크립트나 포스트스크립트의 경로와 인수를 각각 입력합니다.

사전 스크립트와 사후 스크립트는 `/var/opt/snapcenter/spl/scripts` 또는 이 경로 내부의 폴더에 저장해야 합니다. 기본적으로 `/var/opt/snapcenter/spl/scripts` 경로가 채워집니다. 이 경로 내에 스크립트를 저장하기 위한 폴더를 만든 경우 경로에 해당 폴더를 지정해야 합니다.

스크립트 시간 초과 값을 지정할 수도 있습니다. 기본값은 60초입니다.

SnapCenter 사용하면 프리스크립트와 포스트스크립트를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다. ["자세히 알아보기"](#)

10. 확인 페이지에서 다음 단계를 수행하세요.

- a. 검증 작업을 수행할 백업 일정을 선택합니다.

- b. 검증 스크립트 명령 섹션에서 검증 작업 전이나 후에 실행할 프리스크립트나 포스트스크립트의 경로와 인수를 각각 입력합니다.

사전 스크립트와 사후 스크립트는 `/var/opt/snapcenter/spl/scripts` 또는 이 경로 내부의 폴더에 저장해야 합니다. 기본적으로 `/var/opt/snapcenter/spl/scripts` 경로가 채워집니다. 이 경로 내에 스크립트를 저장하기 위한 폴더를 만든 경우 경로에 해당 폴더를 지정해야 합니다.

스크립트 시간 초과 값을 지정할 수도 있습니다. 기본값은 60초입니다.

11. 요약 검토 후 *마침*을 클릭하세요.

Oracle 데이터베이스에 대한 리소스 그룹을 만들고 정책을 첨부합니다.

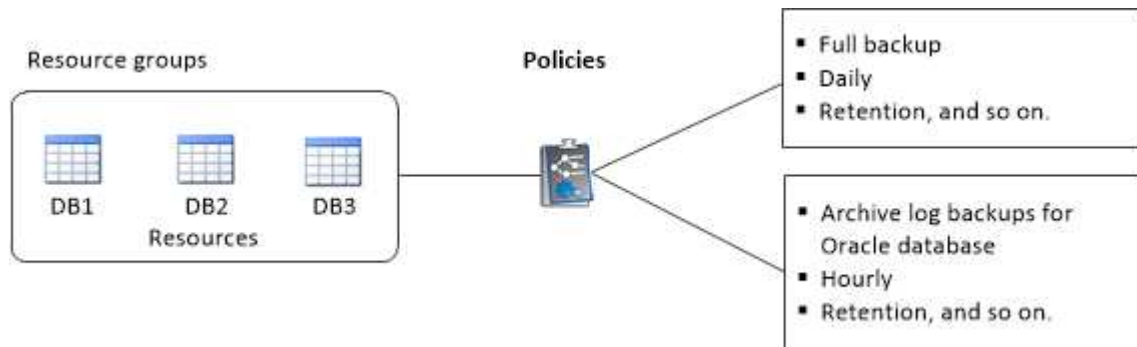
리소스 그룹은 백업하고 보호하려는 리소스를 추가하는 컨테이너입니다. 리소스 그룹을 사용하면 주어진 애플리케이션과 관련된 모든 데이터를 동시에 백업할 수 있습니다.

이 작업에 관하여

- ASM 디스크 그룹에 파일이 있는 데이터베이스는 Oracle DBVERIFY 유틸리티를 사용하여 백업을 확인하려면 "MOUNT" 또는 "OPEN" 상태여야 합니다.

리소스 그룹에 하나 이상의 정책을 연결하여 수행하려는 데이터 보호 작업 유형을 정의합니다.

다음 이미지는 데이터베이스의 리소스, 리소스 그룹 및 정책 간의 관계를 보여줍니다.



- SnapLock 활성화된 정책의 경우 ONTAP 9.12.1 이하 버전에서 스냅샷 잠금 기간을 지정하면 복원의 일부로 변조 방지 스냅샷에서 생성된 복제본은 SnapLock 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.
- SnapMirror 활성화 동기화가 있는 리소스가 포함된 기존 리소스 그룹에 SnapMirror 활성화 동기화 SnapMirror 없는 새 데이터베이스를 추가하는 것은 지원되지 않습니다.
- SnapMirror Active Sync의 장애 조치 모드에서 기존 리소스 그룹에 새 데이터베이스를 추가하는 것은 지원되지 않습니다. 일반 상태나 장애 복구 상태에서만 리소스 그룹에 리소스를 추가할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.
 - a. 이름 필드에 리소스 그룹의 이름을 입력합니다.



리소스 그룹 이름은 250자를 넘을 수 없습니다.

- b. 나중에 리소스 그룹을 검색하는 데 도움이 되도록 태그 필드에 하나 이상의 레이블을 입력하세요.

예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.

- c. 이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

- d. 백업하지 않을 보관 로그 파일의 대상을 지정합니다.



필요한 경우 접두사를 포함하여 Oracle에 설정된 것과 정확히 동일한 대상을 사용해야 합니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 Oracle 데이터베이스 호스트 이름을 선택합니다.



리소스가 성공적으로 검색된 경우에만 해당 리소스가 사용 가능한 리소스 섹션에 나열됩니다. 최근에 리소스를 추가한 경우 리소스 목록을 새로 고친 후에만 사용 가능한 리소스 목록에 표시됩니다.

5. 사용 가능한 리소스 섹션에서 리소스를 선택하고 선택한 리소스 섹션으로 이동합니다.



Linux와 AIX 호스트 모두의 데이터베이스를 단일 리소스 그룹에 추가할 수 있습니다.

6. 애플리케이션 설정 페이지에서 백업 옵션을 선택하세요.

7. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



또한 다음을 클릭하여 정책을 생성할 수도 있습니다.  .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

- b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.

- c. 정책 _policy_name_에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 _policy_name_은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 확인 페이지에서 다음 단계를 수행하세요.

- a. *로케이터 로드*를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 저장소에서 검증을 수행합니다.

- b. 딸깍 하는 소리  일정 구성 열에서 정책의 모든 일정 유형에 대한 확인 일정을 구성합니다.
- c. 확인 일정 추가 policy_name 대화 상자에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	이렇게 하세요...
백업 후 검증 실행	*백업 후 검증 실행*을 선택하세요.
검증 일정을 예약하세요	*예약된 확인 실행*을 선택한 다음 드롭다운 목록에서 일정 유형을 선택합니다.

- d. 보조 저장소 시스템에서 백업을 확인하려면 *보조 위치에서 확인*을 선택하세요.
- e. *확인*을 클릭합니다.

구성된 검증 일정은 적용된 일정 열에 나열됩니다.

9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

10. 요약 검토한 후 *마침*을 클릭하세요.

ASA r2 시스템에서 Oracle 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.

ASA r2 시스템에 있는 리소스를 추가하려면 리소스 그룹을 만들어야 합니다. 리소스 그룹을 생성하는 동안 보조 보호를 프로비저닝할 수도 있습니다.

시작하기 전에

- ONTAP 9.x 리소스와 ASA r2 리소스를 동일한 리소스 그룹에 추가하지 않도록 해야 합니다.
- ONTAP 9.x 리소스와 ASA r2 리소스가 모두 포함된 데이터베이스가 없는지 확인해야 합니다.

이 작업에 관하여

- 2차 보호는 로그인한 사용자에게 **SecondaryProtection** 기능이 활성화된 역할이 할당된 경우에만 사용할 수 있습니다.
- 2차 보호를 활성화한 경우 기본 및 2차 일관성 그룹을 생성하는 동안 리소스 그룹은 유지 관리 모드로 전환됩니다. 기본 및 보조 일관성 그룹이 생성된 후 리소스 그룹은 유지 관리 모드에서 해제됩니다.
- SnapCenter 클론 리소스에 대한 보조 보호를 지원하지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.

3. 이름 페이지에서 다음 작업을 수행합니다.

- a. 이름 필드에 리소스 그룹의 이름을 입력합니다.



리소스 그룹 이름은 250자를 넘을 수 없습니다.

- b. 나중에 리소스 그룹을 검색하는 데 도움이 되도록 태그 필드에 하나 이상의 레이블을 입력하세요.

예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.

- c. 이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

- d. 백업하지 않을 보관 로그 파일의 대상을 지정합니다.



필요한 경우 접두사를 포함하여 애플리케이션에 설정된 것과 정확히 동일한 목적지를 사용해야 합니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 데이터베이스 호스트 이름을 선택합니다.



리소스가 성공적으로 검색된 경우에만 해당 리소스가 사용 가능한 리소스 섹션에 나열됩니다. 최근에 리소스를 추가한 경우 리소스 목록을 새로 고친 후에만 사용 가능한 리소스 목록에 표시됩니다.

5. 사용 가능한 리소스 섹션에서 ASA r2 리소스를 선택하고 선택한 리소스 섹션으로 이동합니다.

6. 애플리케이션 설정 페이지에서 백업 옵션을 선택하세요.

7. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



또한 다음을 클릭하여 정책을 생성할 수도 있습니다.  .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

- b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.

- c. 정책_policy_name_에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 _policy_name_은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 선택한 정책에 대해 보조 보호가 활성화된 경우 보조 보호 페이지가 표시되며 다음 단계를 수행해야 합니다.

- a. 복제 정책의 유형을 선택하세요.



동기 복제 정책은 지원되지 않습니다.

- b. 사용할 일관성 그룹 접미사를 지정합니다.
- c. 대상 클러스터 및 대상 SVM 드롭다운에서 사용하려는 피어링된 클러스터와 SVM을 선택합니다.



SnapCenter에서는 클러스터 및 SVM 피어링을 지원하지 않습니다. 클러스터 및 SVM 피어링을 수행하려면 System Manager 또는 ONTAP CLI를 사용해야 합니다.



리소스가 이미 SnapCenter 외부에서 보호되고 있는 경우 해당 리소스는 보조 보호 리소스 섹션에 표시됩니다.

1. 확인 페이지에서 다음 단계를 수행하세요.

- a. *로케이터 로드*를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 저장소에서 검증을 수행합니다.
- b. 딸깍 하는 소리  일정 구성 열에서 정책의 모든 일정 유형에 대한 확인 일정을 구성합니다.
- c. 확인 일정 추가 policy_name 대화 상자에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	이렇게 하세요...
백업 후 검증 실행	*백업 후 검증 실행*을 선택하세요.
검증 일정을 예약하세요	*예약된 확인 실행*을 선택한 다음 드롭다운 목록에서 일정 유형을 선택합니다.

- d. 보조 저장소 시스템에서 백업을 확인하려면 *보조 위치에서 확인*을 선택하세요.
- e. *확인*을 클릭합니다.

구성된 검증 일정은 적용된 일정 열에 나열됩니다.

2. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtplibServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

3. 요약 검토한 후 *마침*을 클릭하세요.

Oracle 리소스 백업

리소스가 어떤 리소스 그룹에도 속하지 않은 경우 리소스 페이지에서 리소스를 백업할 수

있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *데이터베이스*를 선택합니다.
3. 딸깍 하는 소리  그런 다음 호스트 이름과 데이터베이스 유형을 선택하여 리소스를 필터링합니다.

그런 다음 클릭할 수 있습니다  필터 창을 닫으려면.

4. 백업할 데이터베이스를 선택하세요.

데이터베이스 보호 페이지가 표시됩니다.

5. 리소스 페이지에서 다음 단계를 수행합니다.

- a. 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, `customtext_policy_hostname` 또는 `resource_hostname`. 기본적으로 스냅샷 이름에 타임스탬프가 추가됩니다.

- b. 백업하지 않을 보관 로그 파일의 대상을 지정합니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.

정책을 생성하려면 다음을 클릭하세요. .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

- b. 딸깍 하는 소리  일정 구성 열에서 원하는 정책에 대한 일정을 구성합니다.

- c. 정책 `_policy_name_`에 대한 일정 추가 창에서 일정을 구성한 다음 다음을 선택합니다. OK .

`_policy_name_`은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

7. 확인 페이지에서 다음 단계를 수행하세요.

- a. *로케이터 로드*를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 저장소를 확인합니다.

- b. 딸깍 하는 소리  일정 구성 열에서 정책의 모든 일정 유형에 대한 확인 일정을 구성합니다. + 확인 일정 추가 정책_이름 대화 상자에서 다음 단계를 수행할 수 있습니다.

- c. *백업 후 검증 실행*을 선택하세요.

- d. *예약된 확인 실행*을 선택하고 드롭다운 목록에서 일정 유형을 선택합니다.



Flex ASM 설정에서는 RAC 클러스터의 노드 수보다 기수가 적은 경우 Leaf 노드에서 검증 작업을 수행할 수 없습니다.

e. 보조 저장소의 백업을 확인하려면 *보조 위치에서 확인*을 선택하세요.

f. *확인*을 클릭합니다.

구성된 검증 일정은 적용된 일정 열에 나열됩니다.

8. 알림 페이지에서 이메일 기본 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스에서 수행된 백업 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림의 경우 GUI 또는 PowerShell 명령을 사용하여 SMTP 서버 세부 정보를 지정해야 합니다. `Set-SmSmtServer`.

9. 요약을 검토한 후 *마침*을 클릭하세요.

데이터베이스 토폴로지 페이지가 표시됩니다.

10. *지금 백업*을 클릭하세요.

11. 백업 페이지에서 다음 단계를 수행합니다.

a. 리소스에 여러 정책을 적용한 경우 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

b. *백업*을 클릭하세요.

12. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

당신이 완료한 후

- AIX 설정에서는 다음을 사용할 수 있습니다. `lkdev` 잠금 명령 및 `rendev` 백업된 데이터베이스가 상주하던 디스크의 이름을 바꾸는 명령입니다.

해당 백업을 사용하여 복원하는 경우 장치를 잠그거나 이름을 변경해도 복원 작업에 영향을 미치지 않습니다.

- 데이터베이스 쿼리 실행 시간이 시간 초과 값을 초과하여 백업 작업이 실패하는 경우 다음을 실행하여 `ORACLE_SQL_QUERY_TIMEOUT` 및 `ORACLE_PLUGIN_SQL_QUERY_TIMEOUT` 매개변수 값을 변경해야 합니다. `Set-SmConfigSettings` cmdlet:

매개변수 값을 수정한 후 다음 명령을 실행하여 SnapCenter 플러그인 Loader (SPL) 서비스를 다시 시작합니다.
`/opt/NetApp/snapcenter/spl/bin/spl restart`

- 파일에 접근할 수 없고 검증 과정 중에 마운트 지점을 사용할 수 없는 경우, 지정된 파일이라는 오류 코드 DBV-00100이 발생하여 작업이 실패할 수 있습니다. `sco.properties`에서 `VERIFICATION_DELAY` 및 `VERIFICATION_RETRY_COUNT` 매개변수 값을 수정해야 합니다.

매개변수 값을 수정한 후 다음 명령을 실행하여 SnapCenter 플러그인 Loader (SPL) 서비스를 다시 시작합니다.
`/opt/NetApp/snapcenter/spl/bin/spl restart`

- MetroCluster 구성에서 SnapCenter 장애 조치 후 보호 관계를 감지하지 못할 수 있습니다.
- VMDK에서 애플리케이션 데이터를 백업하고 SnapCenter Plug-in for VMware vSphere의 Java 힙 크기가

충분히 크지 않으면 백업이 실패할 수 있습니다.

Java 힙 크기를 늘리려면 스크립트 파일 `_/opt/netapp/init_scripts/scvservice_`를 찾으세요. 해당 스크립트에서 `do_start method` 명령은 SnapCenter VMware 플러그인 서비스를 시작합니다. 해당 명령을 다음과 같이 업데이트하세요. `Java -jar -Xmx8192M -Xms4096M`.

더 많은 정보를 찾아보세요

- "MetroCluster 장애 조치 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다."
- "SnapCenter 작업을 수행하기 위해 Oracle RAC One Node 데이터베이스가 건너뛰니다."
- "Oracle 12c ASM 데이터베이스의 상태를 변경하지 못했습니다."
- "AIX 시스템의 백업, 복원 및 복제 작업을 위한 사용자 정의 가능한 매개변수"(로그인 필요)

Oracle 데이터베이스 리소스 그룹 백업

리소스 그룹은 호스트나 클러스터에 있는 리소스의 모음입니다. 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다.

리소스 페이지에서 필요에 따라 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 첨부되고 일정이 구성된 경우 일정에 따라 백업이 생성됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.
3. 검색창에 리소스 그룹 이름을 입력하거나 클릭하세요.  , 태그를 선택하세요.

딸깍 하는 소리  필터 창을 닫으려면.

4. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택합니다.



두 개의 데이터베이스가 있는 페더레이션 리소스 그룹이 있고 그 중 하나에 NetApp 스토리지가 아닌 스토리지에 데이터가 있는 경우, 다른 데이터베이스가 NetApp 스토리지에 있더라도 백업 작업이 중단됩니다.

5. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스 그룹과 연관된 정책이 여러 개 있는 경우 정책 드롭다운 목록에서 사용할 백업 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. *백업*을 선택하세요.

6. *모니터 > 작업*을 선택하여 진행 상황을 모니터링하세요.

당신이 완료한 후

- AIX 설정에서는 다음을 사용할 수 있습니다. `lkdev` 잠금 명령 및 `rendev` 백업된 데이터베이스가 상주하던 디스크의 이름을 바꾸는 명령입니다.

해당 백업을 사용하여 복원하는 경우 장치를 잠그거나 이름을 변경해도 복원 작업에 영향을 미치지 않습니다.

- 데이터베이스 쿼리 실행 시간이 시간 초과 값을 초과하여 백업 작업이 실패하는 경우 다음을 실행하여 ORACLE_SQL_QUERY_TIMEOUT 및 ORACLE_PLUGIN_SQL_QUERY_TIMEOUT 매개변수 값을 변경해야 합니다. Set-SmConfigSettings cmdlet:

매개변수 값을 수정한 후 다음 명령을 실행하여 SnapCenter 플러그인 Loader (SPL) 서비스를 다시 시작합니다.
`/opt/NetApp/snapcenter/spl/bin/spl restart`

- 파일에 접근할 수 없고 검증 과정 중에 마운트 지점을 사용할 수 없는 경우, 지정된 파일이라는 오류 코드 DBV-00100이 발생하여 작업이 실패할 수 있습니다. sco.properties에서 VERIFICATION_DELAY_ 및 VERIFICATION_RETRY_COUNT 매개변수 값을 수정해야 합니다.

매개변수 값을 수정한 후 다음 명령을 실행하여 SnapCenter 플러그인 Loader (SPL) 서비스를 다시 시작합니다.
`/opt/NetApp/snapcenter/spl/bin/spl restart`

Oracle 데이터베이스 백업 모니터링

백업 작업과 데이터 보호 작업의 진행 상황을 모니터링하는 방법을 알아보세요.

Oracle 데이터베이스 백업 작업 모니터링

SnapCenterJobs 페이지를 사용하여 다양한 백업 작업의 진행 상황을 모니터링할 수 있습니다. 완료 시점이나 문제가 있는지 확인하기 위해 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 해당 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  백업 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *백업*을 선택합니다.
 - d. 상태 드롭다운에서 백업 상태를 선택합니다.

e. *적용*을 클릭하면 작업이 성공적으로 완료된 것을 볼 수 있습니다.

4. 백업 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인하세요.



백업 작업 상태가 표시됩니다. ✅ 작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 표시가 되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

활동 창에서 데이터 보호 작업 모니터링

활동 창에는 가장 최근에 수행된 5개의 작업이 표시됩니다. 활동 창에는 작업이 시작된 시점과 작업 상태도 표시됩니다.

활동 창에는 백업, 복원, 복제 및 예약된 백업 작업에 대한 정보가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 딸깍 하는 소리  활동 창에서 가장 최근의 작업 5개를 확인하세요.

작업 중 하나를 클릭하면 작업 세부 정보가 작업 세부 정보 페이지에 나열됩니다.

기타 백업 작업

UNIX 명령을 사용하여 Oracle 데이터베이스 백업

백업 워크플로에는 계획, 백업 리소스 식별, 백업 정책 생성, 리소스 그룹 생성 및 정책 연결, 백업 생성, 작업 모니터링이 포함됩니다.

필요한 것

- *Add-SmStorageConnection* 및 *Add-SmCredential* 명령을 사용하여 스토리지 시스템 연결을 추가하고 자격 증명을 생성했어야 합니다.
- *Open-SmConnection* 명령을 사용하여 SnapCenter 서버와의 연결 세션을 설정했어야 합니다.

SnapCenter 계정 로그인 세션은 하나만 가질 수 있으며 토큰은 사용자 홈 디렉토리에 저장됩니다.



연결 세션은 24시간 동안만 유효합니다. 하지만 *TokenNeverExpires* 옵션을 사용하여 토큰을 생성하면 만료되지 않는 토큰을 생성할 수 있으며 세션은 항상 유효합니다.

이 작업에 관하여

SnapCenter 서버와의 연결을 설정하고, Oracle 데이터베이스 인스턴스를 검색하고, 정책과 리소스 그룹을 추가하고, 백업하고, 백업을 확인하려면 다음 명령을 실행해야 합니다.

명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 *Get-Help _command_name_*을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 명령 참조 가이드](#)".

단계

1. 지정된 사용자에게 대해 SnapCenter 서버와의 연결 세션을 시작합니다: *Open-SmConnection*
2. 호스트 리소스 검색 작업 수행: *Get-SmResources*
3. RAC(Real Application Cluster) 데이터베이스의 백업 작업을 위해 Oracle 데이터베이스 자격 증명 및 기본 노드를 구성합니다: *Configure-SmOracleDatabase*
4. 백업 정책 만들기: *Add-SmPolicy*
5. 보조(SnapVault 또는 SnapMirror) 저장소 위치에 대한 정보를 검색합니다: *Get-SmSecondaryDetails*

이 명령은 지정된 리소스의 기본 저장소와 보조 저장소 간의 매핑 세부 정보를 검색합니다. 백업 리소스 그룹을 생성하는 동안 매핑 세부 정보를 사용하여 보조 검증 설정을 구성할 수 있습니다.

6. SnapCenter 에 리소스 그룹 추가: *Add-SmResourceGroup*
7. 백업 만들기: *New-SmBackup*

WaitForCompletion 옵션을 사용하여 작업을 폴링할 수 있습니다. 이 옵션이 지정되면 명령은 백업 작업이 완료될 때까지 서버를 계속 폴링합니다.

8. SnapCenter 에서 로그 검색: *Get-SmLogs*

Oracle 데이터베이스 백업 작업 취소

실행 중이거나 대기 중이거나 응답하지 않는 백업 작업은 취소할 수 있습니다.

백업 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

이 작업에 관하여

백업 작업을 취소하면 SnapCenter Server는 작업을 중지하고, 생성된 백업이 SnapCenter Server에 등록되지 않은 경우 저장소에서 모든 스냅샷을 제거합니다. 백업이 이미 SnapCenter Server에 등록된 경우 취소가 트리거된 후에도 이미 생성된 스냅샷은 롤백되지 않습니다.

- 대기 중이거나 실행 중인 로그 또는 전체 백업 작업만 취소할 수 있습니다.
- 검증이 시작된 후에는 작업을 취소할 수 없습니다.

검증 전에 작업을 취소할 경우, 작업이 취소되고 검증 작업이 수행되지 않습니다.

- 카탈로그 작업이 시작된 후에는 백업 작업을 취소할 수 없습니다.
- 모니터 페이지나 활동 창에서 백업 작업을 취소할 수 있습니다.
- SnapCenter GUI를 사용하는 것 외에도 CLI 명령을 사용하여 작업을 취소할 수 있습니다.
- 취소할 수 없는 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자/그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 백업 작업을 취소할 수 있습니다.

단계

다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	1. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. 2. 작업을 선택하고 *작업 취소*를 클릭하세요.
활동 창	1. 백업 작업을 시작한 후 다음을 클릭하세요.  활동 창에서 가장 최근의 작업 5개를 확인하세요. 2. 작업을 선택하세요. 3. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

결과

작업이 취소되고 리소스가 원래 상태로 돌아갑니다.

취소한 작업이 취소 중 또는 실행 상태에서 응답하지 않는 경우 Cancel-SmJob -JobID <int> -Force를 실행하여 백업 작업을 강제로 중지해야 합니다.

토폴로지 페이지에서 **Oracle** 데이터베이스 백업 및 복제본 보기

리소스를 백업하거나 복제할 준비를 할 때 기본 및 보조 저장소에 있는 모든 백업과 복제본을 그래픽으로 표현해 보면 도움이 될 수 있습니다.

이 작업에 관하여

토폴로지 페이지에서는 선택한 리소스 또는 리소스 그룹에 사용 가능한 모든 백업과 복제본을 볼 수 있습니다. 해당 백업 및 복제의 세부 정보를 보고 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

다음 아이콘을 '사본 관리' 보기에서 검토하여 백업 및 복제본을 기본 저장소 또는 보조 저장소(미러 사본 또는 볼트 사본)에서 사용할 수 있는지 확인할 수 있습니다.

-  기본 스토리지에서 사용 가능한 백업 및 복제본의 수를 표시합니다.
-  SnapMirror 기술을 사용하여 보조 저장소에 미러링된 백업 및 복제본의 수를 표시합니다.
-  SnapVault 기술을 사용하여 보조 저장소에 복제된 백업 및 복제본의 수를 표시합니다.

표시된 백업 수에는 보조 저장소에서 삭제된 백업이 포함됩니다. 예를 들어, 4개의 백업만 보존하는 정책을 사용하여 6개의 백업을 만든 경우 표시되는 백업 수는 6개입니다.



미러 볼트 유형 볼륨의 버전 가변형 미러 백업의 복제본은 토폴로지 보기에 표시되지만, 토폴로지 보기의 미러 백업 수에는 버전 가변형 백업이 포함되지 않습니다.

SnapMirror Active Sync(처음에는 SnapMirror Business Continuity[SM-BC]로 출시됨)라는 보조 관계가 있는 경우 다음과 같은 추가 아이콘을 볼 수 있습니다.

-  복제 사이트가 오픈되었습니다.
-  복제 사이트가 다운되었습니다.
-  2차 거울이나 볼트 관계가 재설정되지 않았습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 리소스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 리소스를 선택합니다.

리소스가 보호된 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. 요약 카드를 검토하여 기본 및 보조 저장소에서 사용 가능한 백업 및 복제본 수에 대한 요약을 확인하세요.

요약 카드 섹션에는 총 백업 및 복제 수와 총 로그 백업 수가 표시됩니다.

새로 고침 버튼을 클릭하면 저장소에 대한 쿼리가 시작되어 정확한 개수가 표시됩니다.

SnapLock 이 활성화된 백업을 수행한 경우 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간이 새로 고쳐집니다. 주간 일정은 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간도 새로 고칩니다.

애플리케이션 리소스가 여러 볼륨에 분산되어 있는 경우 백업에 대한 SnapLock 만료 시간은 볼륨의 스냅샷에 설정된 가장 긴 SnapLock 만료 시간이 됩니다. 가장 긴 SnapLock 만료 시간은 ONTAP 에서 검색됩니다.

SnapMirror 활성화 동기화의 경우, 새로 고침 버튼을 클릭하면 ONTAP 기본 사이트와 복제 사이트를 모두 쿼리하여 SnapCenter 백업 인벤토리가 새로 고쳐집니다. 주간 일정은 SnapMirror 활성화 동기화 관계가 포함된 모든 데이터베이스에 대해 이 활동을 수행합니다.

- SnapMirror 활성화 동기화 및 ONTAP 9.14.1의 경우에만 장애 조치 후 새 기본 대상에 대한 비동기 미러 또는 비동기 MirrorVault 관계를 수동으로 구성해야 합니다. ONTAP 9.15.1부터 비동기 미러 또는 비동기 미러볼트가 새로운 기본 대상으로 자동 구성됩니다.

- 장애 조치 후에는 SnapCenter 에서 장애 조치를 인식할 수 있도록 백업을 만들어야 합니다. 백업이 생성된 후에만 *새로 고침*을 클릭할 수 있습니다.

5. 복사본 관리 보기에서 기본 또는 보조 저장소의 백업 또는 *복제*를 클릭하면 백업 또는 복제의 세부 정보를 볼 수 있습니다.

백업 및 복제의 세부 정보는 표 형식으로 표시됩니다.

6. 표에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 복제, 마운트, 마운트 해제, 이름 바꾸기, 카탈로그화, 카탈로그화 해제 및 삭제 작업을 수행합니다.



보조 저장소에 있는 백업은 이름을 바꾸거나 삭제할 수 없습니다.

- 로그 백업을 선택한 경우 이름 바꾸기, 마운트, 마운트 해제, 카탈로그화, 카탈로그 해제, 삭제 작업만 수행할 수 있습니다.

- Oracle Recovery Manager(RMAN)를 사용하여 백업을 카탈로그화한 경우 카탈로그화된 백업의 이름을 바꿀 수 없습니다.

7. 복제본을 삭제하려면 테이블에서 복제본을 선택한 다음 클릭하세요.  .

SnapmirrorStatusUpdateWaitTime에 할당된 값이 작으면 데이터 및 로그 볼륨이 성공적으로 보호되더라도 미러 및 볼트 백업 사본이 토폴로지 페이지에 나열되지 않습니다. `Set-SmConfigSettings` PowerShell cmdlet을 사용하여 SnapmirrorStatusUpdateWaitTime에 할당된 값을 늘려야 합니다.

명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `Get-Help _command_name_`을 실행하면 얻을 수 있습니다.

또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 명령 참조 가이드](#)" 또는 "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

데이터베이스 백업 마운트 및 마운트 해제

백업에 있는 파일에 액세스하려면 하나 또는 여러 개의 데이터와 로그 전용 백업을 마운트할 수 있습니다. 백업이 생성된 동일한 호스트에 백업을 마운트하거나 동일한 유형의 Oracle 및 호스트 구성을 갖는 원격 호스트에 마운트할 수 있습니다. 백업을 수동으로 마운트한 경우 작업을 완료한 후 백업을 수동으로 마운트 해제해야 합니다. 언제든지 데이터베이스 백업을 호스트 중 하나에 마운트할 수 있습니다. 작업을 수행하는 동안에는 하나의 백업만 마운트할 수 있습니다.



Flex ASM 설정에서는 RAC 클러스터의 노드 수보다 기수가 적으면 Leaf 노드에서 마운트 작업을 수행할 수 없습니다.

데이터베이스 백업 마운트

백업에 있는 파일에 액세스하려면 데이터베이스 백업을 수동으로 마운트해야 합니다.

필요한 것

- NFS 환경에 ASM(Automatic Storage Management) 데이터베이스 인스턴스가 있고 ASM 백업을 마운트하려는 경우 `asm_diskstring` 매개변수에 정의된 기존 경로에 ASM 디스크 경로 `/var/opt/snapcenter/sco/backup*/*/_/*_`를 추가해야 합니다.
- NFS 환경에 ASM 데이터베이스 인스턴스가 있고 복구 작업의 일부로 ASM 로그 백업을 마운트하려는 경우 `asm_diskstring` 매개변수에 정의된 기존 경로에 ASM 디스크 경로 `/var/opt/snapcenter/scu/clones/*/*_`를 추가해야 합니다.
- `asm_diskstring` 매개변수에서 ASMFED를 사용하는 경우 `_AFD:*`를 구성해야 하고, ASMLIB를 사용하는 경우 `_ORCL:*`를 구성해야 합니다.



`asm_diskstring` 매개변수를 편집하는 방법에 대한 자세한 내용은 다음을 참조하세요. "[asm_diskstring에 디스크 경로를 추가하는 방법](#)".

- 백업을 마운트하는 동안 소스 데이터베이스 호스트와 다른 경우 ASM 자격 증명과 ASM 포트를 구성해야 합니다.
- 대체 호스트에 마운트하려면 대체 호스트가 다음 요구 사항을 충족하는지 확인해야 합니다.
 - 원래 호스트와 동일한 UID 및 GID

- 원래 호스트와 동일한 Oracle 버전
- 원래 호스트와 동일한 OS 배포판 및 버전
- NVMe의 경우 NVMe util을 설치해야 합니다.
- LUN이 iSCSI와 FC의 혼합 프로토콜로 구성된 iGroup을 사용하여 AIX 호스트에 매핑되지 않았는지 확인해야 합니다. 자세한 내용은 다음을 참조하세요. ["LUN에 대한 장치를 검색할 수 없습니다. 오류가 발생하여 작업이 실패합니다."](#).

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 데이터베이스를 선택합니다.

데이터베이스 토폴로지 페이지가 표시됩니다.

4. 사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 *백업*을 선택합니다.
5. 테이블에서 백업을 선택한 다음 클릭하세요. .
6. 백업 마운트 페이지에서 백업을 마운트할 호스트 선택 드롭다운 목록에서 백업을 마운트할 호스트를 선택합니다.

마운트 경로 `_var/opt/snapcenter/sco/backup_mount/backup_name/database_name_`이 표시됩니다.

ASM 데이터베이스의 백업을 마운트하는 경우 마운트 경로 `+diskgroupname_SID_backupid`가 표시됩니다.

7. *마운트*를 클릭하세요.

끝난 후

- 다음 명령을 실행하면 마운트된 백업과 관련된 정보를 검색할 수 있습니다.

```
./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
```

- ASM 데이터베이스를 마운트한 경우 다음 명령을 실행하여 마운트된 백업과 관련된 정보를 검색할 수 있습니다.

```
./sccli Get-Smbbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
```

- 백업 ID를 검색하려면 다음 명령을 실행하세요.

```
./sccli Get-Smbbackup-BackupNamebackup_name
```

명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `Get-Help _command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 명령 참조 가이드"](#).

데이터베이스 백업 마운트 해제

더 이상 백업에 있는 파일에 액세스하지 않으려면 마운트된 데이터베이스 백업을 수동으로 마운트 해제할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 데이터베이스를 선택합니다.

데이터베이스 토폴로지 페이지가 표시됩니다.

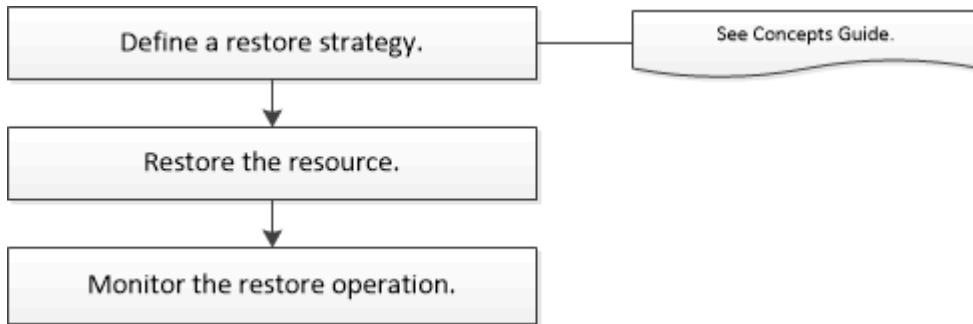
4. 마운트된 백업을 선택한 다음 클릭하세요.  .
5. *확인*을 클릭합니다.

Oracle 데이터베이스 복원 및 복구

워크플로 복원

복원 워크플로에는 계획, 복원 작업 수행, 작업 모니터링이 포함됩니다.

다음 워크플로는 복원 작업을 수행해야 하는 순서를 보여줍니다.



Oracle 데이터베이스에 대한 복원 및 복구 전략 정의

데이터베이스를 복원하고 복구하기 전에 전략을 정의해야 복원 및 복구 작업을 성공적으로 수행할 수 있습니다.

복원 및 복구 작업에 지원되는 백업 유형

SnapCenter 다양한 유형의 Oracle 데이터베이스 백업의 복원 및 복구를 지원합니다.

- 온라인 데이터 백업
- 오프라인 종료 데이터 백업
- 오프라인 마운트 데이터 백업



오프라인 종료 또는 오프라인 마운트 데이터 백업을 복원하는 경우 SnapCenter 데이터베이스를 오프라인 상태로 둡니다. 데이터베이스를 수동으로 복구하고 로그를 재설정해야 합니다.

- 전체 백업
- Data Guard 대기 데이터베이스의 오프라인 마운트 백업

- Active Data Guard 대기 데이터베이스의 데이터 전용 온라인 백업



Active Data Guard 대기 데이터베이스의 복구를 수행할 수 없습니다.

- RAC(Real Application Clusters) 구성에서의 온라인 데이터 백업, 온라인 전체 백업, 오프라인 마운트 백업 및 오프라인 종료 백업
- ASM(자동 스토리지 관리) 구성의 온라인 데이터 백업, 온라인 전체 백업, 오프라인 마운트 백업 및 오프라인 종료 백업

Oracle 데이터베이스에 지원되는 복원 방법 유형

SnapCenter Oracle 데이터베이스에 대한 연결 및 복사 또는 제자리 복원을 지원합니다. 복원 작업 중에 SnapCenter 데이터 손실 없이 복원하는 데 사용할 파일 시스템에 적합한 복원 방법을 결정합니다.



SnapCenter 볼륨 기반 SnapRestore 지원하지 않습니다.

연결 및 복사 복원

데이터베이스 레이아웃이 백업과 다르거나 백업이 생성된 후 새 파일이 있는 경우 연결 및 복사 복원이 수행됩니다. 연결 및 복사 복원 방법에서는 다음 작업이 수행됩니다.

단계

1. 볼륨은 스냅샷에서 복제되고 파일 시스템 스택은 복제된 LUN이나 볼륨을 사용하여 호스트에 구축됩니다.
2. 파일은 복제된 파일 시스템에서 원본 파일 시스템으로 복사됩니다.
3. 복제된 파일 시스템은 호스트에서 마운트 해제되고 복제된 볼륨은 ONTAP 에서 삭제됩니다.



Flex ASM 설정(카디널리티가 RAC 클러스터의 노드 수보다 작은 경우) 또는 VMDK 또는 RDM의 ASM RAC 데이터베이스의 경우 연결 및 복사 복원 방법만 지원됩니다.

강제로 제자리 복원을 활성화한 경우에도 SnapCenter 다음과 같은 시나리오에서 연결 및 복사 복원을 수행합니다.

- 보조 저장 시스템에서 복원
- 데이터베이스 인스턴스가 구성되지 않은 Oracle RAC 설정의 노드에 있는 ASM 디스크 그룹 복원
- Oracle RAC 설정에서 ASM 인스턴스 또는 클러스터 인스턴스가 실행 중이 아니거나 피어 노드가 다운된 경우 피어 노드 중 하나에서
- 제어 파일만 복원
- ASM 디스크 그룹에 있는 테이블스페이스 하위 집합 복원
- 디스크 그룹은 데이터 파일, sp 파일 및 암호 파일 간에 공유됩니다.
- RAC 환경의 원격 노드에 SnapCenter 플러그인 Loader (SPL) 서비스가 설치되지 않았거나 실행되지 않습니다.
- Oracle RAC에 새 노드가 추가되고 SnapCenter Server는 새로 추가된 노드를 인식하지 못합니다.

제자리 복원

데이터베이스 레이아웃이 백업과 유사하고 저장소 및 데이터베이스 스택에서 구성이 변경되지 않은 경우, 파일이나 LUN의 복원이 ONTAP 에서 수행되는 제자리 복원이 수행됩니다. SnapCenter 제자리 복원 방법의 일부로 SFSR(단일

파일 SnapRestore)만 지원합니다.



NetApp ONTAP 보조 위치에서의 원위치 복원을 지원합니다.

데이터베이스에서 제자리 복원을 수행하려면 ASM 디스크 그룹에 데이터 파일만 있는지 확인하세요. ASM 디스크 그룹이나 데이터베이스의 물리적 구조가 변경된 후에는 백업을 만들어야 합니다. 제자리 복원을 수행한 후에는 디스크 그룹에 백업 시점과 동일한 수의 데이터 파일이 포함됩니다.

디스크 그룹 또는 마운트 지점이 다음 기준과 일치하면 제자리 복원이 자동으로 적용됩니다.

- 백업 후 새로운 데이터 파일이 추가되지 않습니다(외부 파일 검사)
- 백업 후 ASM 디스크 또는 LUN 추가, 삭제 또는 재생성 없음(ASM 디스크 그룹 구조 변경 확인)
- LVM 디스크 그룹에 LUN 추가, 삭제 또는 재생성 없음(LVM 디스크 그룹 구조 변경 확인)



GUI, SnapCenter CLI 또는 PowerShell cmdlet을 사용하여 강제로 제자리 복원을 활성화하여 외부 파일 검사 및 LVM 디스크 그룹 구조 변경 검사를 재정의할 수도 있습니다.

ASM RAC에서 제자리 복원 수행

SnapCenter 에서 복원을 수행하는 노드를 기본 노드라고 하며, ASM 디스크 그룹이 있는 RAC의 다른 모든 노드를 피어 노드라고 합니다. SnapCenter 스토리지 복원 작업을 수행하기 전에 ASM 디스크 그룹이 마운트 상태인 모든 노드에서 ASM 디스크 그룹의 상태를 마운트 해제로 변경합니다. 저장소 복원이 완료되면 SnapCenter ASM 디스크 그룹의 상태를 복원 작업 전 상태로 변경합니다.

SAN 환경에서 SnapCenter 모든 피어 노드에서 장치를 제거하고 스토리지 복원 작업 전에 LUN 매핑 해제 작업을 수행합니다. 저장소 복구 작업 후 SnapCenter LUN 맵 작업을 수행하고 모든 피어 노드에 장치를 구성합니다. SAN 환경에서 Oracle RAC ASM 레이아웃이 LUN에 상주하는 경우 SnapCenter 복원하는 동안 ASM 디스크 그룹이 있는 RAC 클러스터의 모든 노드에서 LUN 매핑 해제, LUN 복원 및 LUN 매핑 작업을 수행합니다. RAC 노드의 모든 이니시에이터가 LUN에 사용되지 않았더라도 복원하기 전에 SnapCenter 복원 후 모든 RAC 노드의 모든 이니시에이터로 새 iGroup을 생성합니다.

- 피어 노드에서 사전 복구 작업 중에 오류가 발생하면 SnapCenter 사전 복구 작업이 성공한 피어 노드에서 복구를 수행하기 전의 ASM 디스크 그룹 상태를 자동으로 롤백합니다. 작업이 실패한 기본 노드와 피어 노드에 대한 롤백은 지원되지 않습니다. 다른 복원을 시도하기 전에 피어 노드에서 문제를 수동으로 해결하고 기본 노드의 ASM 디스크 그룹을 마운트 상태로 되돌려야 합니다.
- 복구 작업 중에 오류가 발생하면 복구 작업이 실패하고 롤백이 수행되지 않습니다. 다른 복원을 시도하기 전에 스토리지 복원 문제를 수동으로 해결하고 기본 노드의 ASM 디스크 그룹을 마운트 상태로 되돌려야 합니다.
- 피어 노드 중 하나에서 복원 후 작업 중에 오류가 발생하면 SnapCenter 다른 피어 노드에서 복원 작업을 계속합니다. 피어 노드에서 복원 후 문제를 수동으로 해결해야 합니다.

Oracle 데이터베이스에서 지원되는 복원 작업 유형

SnapCenter 사용하면 Oracle 데이터베이스에 대해 다양한 유형의 복원 작업을 수행할 수 있습니다.

데이터베이스를 복원하기 전에 백업을 검증하여 실제 데이터베이스 파일과 비교했을 때 누락된 파일이 있는지 확인합니다.

전체 복원

- 데이터 파일만 복원합니다.
- 제어 파일만 복원합니다.
- 데이터 파일과 제어 파일을 복원합니다.
- Data Guard 대기 및 Active Data Guard 대기 데이터베이스에서 데이터 파일, 제어 파일 및 리두 로그 파일을 복원합니다.

부분 복원

- 선택된 테이블스페이스만 복원합니다.
- 선택된 플러그형 데이터베이스(PDB)만 복원합니다.
- PDB의 선택된 테이블스페이스만 복원합니다.

Oracle 데이터베이스에서 지원되는 복구 작업 유형

SnapCenter 사용하면 Oracle 데이터베이스에 대해 다양한 유형의 복구 작업을 수행할 수 있습니다.

- 마지막 트랜잭션까지의 데이터베이스(모든 로그)
- 특정 시스템 변경 번호(SCN)까지의 데이터베이스
- 특정 날짜 및 시간까지의 데이터베이스

데이터베이스 호스트의 표준 시간대를 기준으로 복구 날짜와 시간을 지정해야 합니다.

SnapCenter Oracle 데이터베이스에 대한 복구 불가 옵션도 제공합니다.



Oracle 데이터베이스용 플러그인은 데이터베이스 역할을 대기로 설정하여 생성된 백업을 사용하여 복원한 경우 복구를 지원하지 않습니다. 물리적 대기 데이터베이스에 대해서는 항상 수동 복구를 수행해야 합니다.

Oracle 데이터베이스 복원 및 복구와 관련된 제한 사항

복원 및 복구 작업을 수행하기 전에 제한 사항을 알아야 합니다.

11.2.0.4에서 12.1.0.1까지의 Oracle 버전을 사용하는 경우 *renamedg* 명령을 실행하면 복원 작업이 중단됩니다. 이 문제를 해결하려면 Oracle 패치 19544733을 적용하세요.

다음 복원 및 복구 작업은 지원되지 않습니다.

- 루트 컨테이너 데이터베이스(CDB)의 테이블스페이스 복원 및 복구
- 임시 테이블스페이스 및 PDB와 연관된 임시 테이블스페이스 복원
- 여러 PDB에서 동시에 테이블스페이스 복원 및 복구
- 로그 백업 복원
- 백업을 다른 위치로 복원
- Data Guard 대기 또는 Active Data Guard 대기 데이터베이스 이외의 모든 구성에서 REDO 로그 파일 복원

- SPFILE 및 비밀번호 파일 복원
- 동일한 호스트에서 기존 데이터베이스 이름을 사용하여 재생성된 데이터베이스에서 복원 작업을 수행하고, SnapCenter 에서 관리하며, 유효한 백업이 있는 경우, DBID가 다르더라도 복원 작업은 새로 생성된 데이터베이스 파일을 덮어씁니다.

다음 작업 중 하나를 수행하면 이를 방지할 수 있습니다.

- 데이터베이스가 다시 생성된 후 SnapCenter 리소스를 검색합니다.
- 다시 생성된 데이터베이스의 백업을 만듭니다.

테이블스페이스의 특정 시점 복구와 관련된 제한 사항

- SYSTEM, SYSAUX 및 UNDO 테이블스페이스의 PITR(Point-in-Time Recovery)이 지원되지 않습니다.
- 테이블스페이스의 PITR은 다른 유형의 복원과 함께 수행할 수 없습니다.
- 테이블스페이스 이름이 변경되고 이름이 변경되기 전 시점으로 복구하려는 경우 테이블스페이스의 이전 이름을 지정해야 합니다.
- 한 테이블스페이스의 테이블에 대한 제약 조건이 다른 테이블스페이스에 포함되어 있는 경우 두 테이블스페이스를 모두 복구해야 합니다.
- 테이블과 해당 인덱스가 서로 다른 테이블스페이스에 저장된 경우 PITR을 수행하기 전에 인덱스를 삭제해야 합니다.
- PITR을 사용하여 현재 기본 테이블스페이스를 복구할 수 없습니다.
- PITR은 다음 개체가 포함된 테이블스페이스를 복구하는 데 사용할 수 없습니다.
 - 기본 객체(예: 구체화된 뷰)가 있는 객체 또는 포함된 객체(예: 분할된 테이블)가 모두 복구 세트에 없는 경우

또한, 파티션된 테이블의 파티션이 서로 다른 테이블스페이스에 저장되어 있는 경우 PITR을 수행하기 전에 테이블을 삭제하거나 PITR을 수행하기 전에 모든 파티션을 동일한 테이블스페이스로 이동해야 합니다.

- 세그먼트 실행 취소 또는 롤백
- 여러 수신자가 있는 Oracle 8 호환 고급 대기열
- SYS 사용자가 소유한 객체

이러한 유형의 객체의 예로는 PL/SQL, Java 클래스, 콜아웃 프로그램, 뷰, 동의어, 사용자, 권한, 차원, 디렉토리, 시퀀스 등이 있습니다.

Oracle 데이터베이스 복원을 위한 소스 및 대상

기본 저장소나 보조 저장소의 백업 사본에서 Oracle 데이터베이스를 복원할 수 있습니다. 동일한 데이터베이스 인스턴스의 동일한 위치로만 데이터베이스를 복원할 수 있습니다. 하지만 RAC(Real Application Cluster) 설정에서는 데이터베이스를 다른 노드로 복원할 수 있습니다.

복원 작업을 위한 소스

기본 저장소나 보조 저장소의 백업에서 데이터베이스를 복원할 수 있습니다. 다중 미러 구성에서 보조 저장소의 백업에서 복원하려는 경우 보조 저장소 미러를 소스로 선택할 수 있습니다.

복원 작업의 대상지

동일한 데이터베이스 인스턴스의 동일한 위치로만 데이터베이스를 복원할 수 있습니다.

RAC 설정에서는 클러스터의 모든 노드에서 RAC 데이터베이스를 복원할 수 있습니다.

특정 사전 스크립트 및 사후 스크립트를 복원하기 위한 사전 정의된 환경 변수

SnapCenter 사용하면 데이터베이스를 복원하는 동안 프리스크립트와 포스트스크립트를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다.

데이터베이스 복원을 위한 지원되는 사전 정의된 환경 변수

- *SC_JOB_ID*는 작업의 작업 ID를 지정합니다.

예: 257

- *SC_ORACLE_SID*는 데이터베이스의 시스템 식별자를 지정합니다.

작업에 여러 데이터베이스가 관련된 경우 파이프로 구분된 데이터베이스 이름이 포함됩니다.

예: NFSB31

- *SC_HOST*는 데이터베이스의 호스트 이름을 지정합니다.

이 매개변수는 애플리케이션 볼륨에 대해 채워집니다.

예: scsmohost2.gdl.englabe.netapp.com

- *SC_OS_USER*는 데이터베이스의 운영 체제 소유자를 지정합니다.

예: 오라클

- *SC_OS_GROUP*은 데이터베이스의 운영 체제 그룹을 지정합니다.

예: oinstall

- *SC_BACKUP_NAME*은 백업의 이름을 지정합니다.

이 매개변수는 애플리케이션 볼륨에 대해 채워집니다.

예:

- 데이터베이스가 ARCHIVELOG 모드로 실행되지 않는 경우: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1

- 데이터베이스가 ARCHIVELOG 모드에서 실행되는 경우: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1, RG2_scspr2417819002_07-21-2021_12.16.48.9267_1, RG2_scspr2417819002_07-22-2021_12.16.48.9267_1

- *SC_BACKUP_ID*는 백업의 ID를 지정합니다.

이 매개변수는 애플리케이션 볼륨에 대해 채워집니다.

예:

- 데이터베이스가 ARCHIVELOG 모드로 실행되지 않는 경우: DATA@203|LOG@205
- 데이터베이스가 ARCHIVELOG 모드에서 실행되는 경우: DATA@203|LOG@205,206,207

- *SC_RESOURCE_GROUP_NAME*은 리소스 그룹의 이름을 지정합니다.

예: RG1

- *SC_ORACLE_HOME*은 Oracle 홈 디렉토리의 경로를 지정합니다.

예: /ora01/app/oracle/product/18.1.0/db_1

- *SC_RECOVERY_TYPE*은 복구되는 파일과 복구 범위를 지정합니다.

예:

RESTORESCOPE:usingBackupControlfile=false|RECOVERYScope:allLogs=true,noLogs=false,untiltime=false,untilscn=false.

구분 기호에 대한 정보는 다음을 참조하세요. ["지원되는 구분 기호"](#).

Oracle 데이터베이스 복원을 위한 요구 사항

Oracle 데이터베이스를 복원하기 전에 필수 구성 요소가 완료되었는지 확인해야 합니다.

- 복구 및 복구 전략을 정의했어야 합니다.
- 스냅샷을 미리 또는 볼트에 복제하는 경우 SnapCenter 관리자가 소스 볼륨과 대상 볼륨 모두에 대한 스토리지 가상 머신(SVM)을 할당했어야 합니다.
- 백업의 일부로 보관 로그가 정리되는 경우, 필요한 보관 로그 백업을 수동으로 마운트해야 합니다.
- VMDK(가상 머신 디스크)에 있는 Oracle 데이터베이스를 복원하려면 복제된 VMDK를 할당하는 데 필요한 수의 여유 슬롯이 게스트 머신에 있는지 확인해야 합니다.
- 해당 데이터베이스에 대해 보조 보호가 활성화된 경우 해당 데이터베이스에 속한 모든 데이터 볼륨과 보관 로그 볼륨이 보호되는지 확인해야 합니다.
- 제어 파일이나 전체 데이터베이스 복원을 수행하려면 RAC One Node 데이터베이스가 "nomount" 상태인지 확인해야 합니다.
- NFS 환경에 ASM 데이터베이스 인스턴스가 있는 경우 asm_diskstring 매개변수에 정의된 기존 경로에 ASM 디스크 경로 _/var/opt/snapcenter/scu/clones/*/*_를 추가해야 복구 작업의 일부로 ASM 로그 백업을 성공적으로 마운트할 수 있습니다.
- asm_diskstring 매개변수에서 ASMFID를 사용하는 경우 _AFD:*_를 구성해야 하고, ASMLIB를 사용하는 경우 _ORCL:*_를 구성해야 합니다.



asm_diskstring 매개변수를 편집하는 방법에 대한 자세한 내용은 다음을 참조하세요.
["asm_diskstring에 디스크 경로를 추가하는 방법"](#)

- Oracle 데이터베이스에 대해 OS 인증을 비활성화하고 Oracle 데이터베이스 인증을 활성화한 경우, 해당 데이터베이스의 데이터 파일과 제어 파일을 복원하려는 경우, ASM 데이터베이스가 아닌 경우

\$_ORACLE_HOME/network/admin_에 있는 **listener.ora** 파일에서 정적 리스너를 구성해야 하고, ASM 데이터베이스의 경우 \$_GRID_HOME/network/admin_에 있는 **listener.ora** 파일에서 정적 리스너를 구성해야 합니다.

- 데이터베이스 크기가 테라바이트(TB)인 경우 Set-SmConfigSettings 명령을 실행하여 SCORestoreTimeout 매개변수 값을 늘려야 합니다.
- vCenter에 필요한 모든 라이선스가 설치되고 최신 상태인지 확인해야 합니다.

라이선스가 설치되지 않았거나 최신이 아닌 경우 경고 메시지가 표시됩니다. 경고를 무시하고 계속 진행하면 RDM에서 복원이 실패합니다.

- LUN이 iSCSI와 FC의 혼합 프로토콜로 구성된 iGroup을 사용하여 AIX 호스트에 매핑되지 않았는지 확인해야 합니다. 자세한 내용은 다음을 참조하세요. ["LUN에 대한 장치를 검색할 수 없습니다. 오류가 발생하여 작업이 실패합니다."](#).

Oracle 데이터베이스 복원 및 복구

데이터 손실이 발생한 경우 SnapCenter 사용하여 하나 이상의 백업에서 데이터를 활성 파일 시스템으로 복원한 다음 데이터베이스를 복구할 수 있습니다.

시작하기 전에

루트가 아닌 사용자로 플러그인을 설치한 경우, prescript 및 postscript 디렉토리에 대한 실행 권한을 수동으로 할당해야 합니다.

이 작업에 관하여

- 복구는 구성된 보관 로그 위치에서 사용 가능한 보관 로그를 사용하여 수행됩니다. 데이터베이스가 ARCHIVELOG 모드로 실행 중인 경우 Oracle 데이터베이스는 채워진 리두 로그 파일 그룹을 하나 이상의 오프라인 대상에 저장합니다. 이를 통칭하여 보관된 리두 로그라고 합니다. SnapCenter 지정된 SCN, 선택한 날짜 및 시간 또는 모든 로그 옵션을 기반으로 최적의 로그 백업 수를 식별하고 마운트합니다. 복구에 필요한 보관 로그를 구성된 위치에서 사용할 수 없는 경우 로그가 포함된 스냅샷을 마운트하고 경로를 외부 보관 로그로 지정해야 합니다.

ASMLIB에서 ASMFD로 ASM 데이터베이스를 마이그레이션하는 경우 ASMLIB로 생성된 백업을 사용하여 데이터베이스를 복원할 수 없습니다. ASMFD 구성에서 백업을 생성하고 해당 백업을 사용하여 복원해야 합니다. 마찬가지로 ASM 데이터베이스가 ASMFD에서 ASMLIB로 마이그레이션된 경우 ASMLIB 구성에서 백업을 생성하여 복원해야 합니다.

데이터베이스를 복원하면 여러 작업이 데이터베이스에서 실행되는 것을 방지하기 위해 Oracle 데이터베이스 호스트의 `/var/opt/snapcenter/sco/lock` 디렉토리에 작업 잠금 파일(.sm_lock_dbsid)이 생성됩니다. 데이터베이스가 복구되면 운영 잠금 파일이 자동으로 제거됩니다.



SPFILE 및 비밀번호 파일 복원은 지원되지 않습니다.

- SnapLock 활성화된 정책의 경우 ONTAP 9.12.1 이하 버전에서 스냅샷 잠금 기간을 지정하면 복원의 일부로 변조 방지 스냅샷에서 생성된 복제본은 SnapLock 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.

2. 리소스 페이지에서 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 데이터베이스를 선택합니다.

데이터베이스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 *백업*을 선택합니다.

5. 테이블에서 백업을 선택한 후 *를 클릭합니다.  *.

6. 복원 범위 페이지에서 다음 작업을 수행합니다.

a. RAC(Real Application Clusters) 환경에서 데이터베이스 백업을 선택한 경우 RAC 노드를 선택합니다.

b. 미러링 또는 볼트 데이터를 선택하는 경우:

- 미러 또는 볼트에 로그 백업이 없으면 아무것도 선택되지 않고 로케이터는 비어 있습니다.
- 미러 또는 볼트에 로그 백업이 있는 경우 최신 로그 백업이 선택되고 해당 로케이터가 표시됩니다.



선택한 로그 백업이 미러와 볼트 위치에 모두 있는 경우 두 로케이터가 모두 표시됩니다.

c. 다음 작업을 수행하세요.

복원하고 싶다면...	이렇게 하세요...
데이터베이스의 모든 데이터 파일	*모든 데이터 파일*을 선택합니다. 데이터베이스의 데이터 파일만 복원됩니다. 제어 파일, 보관 로그 또는 리두 로그 파일은 복원되지 않습니다.
테이블스페이스	*테이블스페이스*를 선택합니다. 복원할 테이블스페이스를 지정할 수 있습니다.
제어 파일	*제어 파일*을 선택합니다.  제어 파일을 복원하는 동안 디렉토리 구조가 존재하는지 또는 복원 프로세스를 통해 파일을 대상 위치로 복사할 수 있도록 올바른 사용자 및 그룹 소유권(있는 경우)으로 디렉토리 구조가 생성되었는지 확인합니다. 해당 디렉토리가 존재하지 않으면 복원 작업이 실패합니다.

복원하고 싶다면...	이렇게 하세요...
리두 로그 파일	*Redo 로그 파일*을 선택합니다. 이 옵션은 Data Guard 대기 또는 Active Data Guard 대기 데이터베이스에만 사용할 수 있습니다.  Data Guard 데이터베이스가 아닌 경우에는 Redo 로그 파일이 백업되지 않습니다. Data Guard 데이터베이스가 아닌 경우 복구는 보관 로그를 사용하여 수행됩니다.
플러그형 데이터베이스(PDB)	*플러그형 데이터베이스*를 선택한 다음 복원하려는 PDB를 지정합니다.
플러그형 데이터베이스(PDB) 테이블스페이스	*플러그형 데이터베이스(PDB) 테이블스페이스*를 선택한 다음 복원하려는 PDB와 해당 PDB의 테이블스페이스를 지정합니다. 이 옵션은 복원할 PDB를 선택한 경우에만 사용할 수 있습니다.

- d. 복원 및 복구에 필요한 경우 데이터베이스 상태 변경을 선택하여 복원 및 복구 작업을 수행하는 데 필요한 상태로 데이터베이스 상태를 변경합니다.

데이터베이스의 다양한 상태는 높은 것부터 낮은 것까지 있으며, 여기에는 열기, 마운트됨, 시작됨, 종료가 있습니다. 데이터베이스가 상위 상태에 있지만 복원 작업을 수행하기 위해 상태를 하위 상태로 변경해야 하는 경우 이 확인란을 선택해야 합니다. 데이터베이스가 하위 상태에 있지만 복원 작업을 수행하기 위해 상태를 상위 상태로 변경해야 하는 경우, 확인란을 선택하지 않더라도 데이터베이스 상태가 자동으로 변경됩니다.

데이터베이스가 열린 상태이고 복원을 위해 데이터베이스를 마운트된 상태로 유지해야 하는 경우, 이 확인란을 선택한 경우에만 데이터베이스 상태가 변경됩니다.

- a. 백업 후 새 데이터 파일이 추가되거나 LUN이 LVM 디스크 그룹에 추가, 삭제 또는 다시 생성되는 경우 제자리 복원을 수행하려면 *강제 제자리 복원*을 선택합니다.

7. 복구 범위 페이지에서 다음 작업을 수행합니다.

만약 당신이...	이렇게 하세요...
마지막 거래로 복구하고 싶습니다	*모든 로그*를 선택하세요.
특정 시스템 변경 번호(SCN)로 복구하려고 합니다.	*SCN(시스템 변경 번호)까지*를 선택하세요.
특정 데이터 및 시간으로 복구하고 싶습니다	*날짜 및 시간*을 선택하세요. 데이터베이스 호스트의 표준 시간대에 따른 날짜와 시간을 지정해야 합니다.

만약 당신이...	이렇게 하세요...
복구하고 싶지 않아요	*복구 안 함*을 선택하세요.
외부 보관 로그 위치를 지정하려고 합니다.	데이터베이스가 ARCHIVELOG 모드에서 실행되는 경우 SnapCenter 지정된 SCN, 선택한 날짜 및 시간 또는 모든 로그 옵션을 기반으로 최적의 로그 백업 수를 식별하고 마운트합니다. 외부 보관 로그 파일의 위치를 지정하려면 *외부 보관 로그 위치 지정*을 선택하세요. 백업의 일부로 보관 로그가 정리되고 필요한 보관 로그 백업을 수동으로 마운트한 경우, 복구를 위해 마운트된 백업 경로를 외부 보관 로그 위치로 지정해야 합니다.  외부 로그 위치로 나열하기 전에 마운트 경로의 경로와 내용을 확인해야 합니다. • "ONTAP 통한 Oracle 데이터 보호" • "ORA-00308 오류로 인해 작업이 실패합니다."

보관 로그 볼륨이 보호되지 않았지만 데이터 볼륨이 보호된 경우 보조 백업에서 복구를 통해 복원을 수행할 수 없습니다. *복구 안 함*을 선택해야만 복원이 가능합니다.

열린 데이터베이스 옵션을 선택하여 RAC 데이터베이스를 복구하는 경우 복구 작업이 시작된 RAC 인스턴스만 열린 상태로 돌아갑니다.



Data Guard 대기 및 Active Data Guard 대기 데이터베이스에는 복구가 지원되지 않습니다.

8. PreOps 페이지에서 복원 작업 전에 실행할 사전 스크립트의 경로와 인수를 입력합니다.

사전 스크립트는 `/var/opt/snapcenter/spl/scripts` 경로나 이 경로 내부의 폴더에 저장해야 합니다. 기본적으로 `/var/opt/snapcenter/spl/scripts` 경로가 채워집니다. 이 경로 내에 스크립트를 저장하기 위한 폴더를 만든 경우 경로에 해당 폴더를 지정해야 합니다.

스크립트 시간 초과 값을 지정할 수도 있습니다. 기본값은 60초입니다.

SnapCenter 사용하면 프리스크립트와 포스트스크립트를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다. ["자세히 알아보기"](#)

9. PostOps 페이지에서 다음 단계를 수행하세요.

a. 복원 작업 후 실행할 PostScript의 경로와 인수를 입력합니다.

포스트스크립트는 `/var/opt/snapcenter/spl/scripts` 또는 이 경로 내부의 폴더에 저장해야 합니다. 기본적으로 `/var/opt/snapcenter/spl/scripts` 경로가 채워집니다. 이 경로 내에 스크립트를 저장하기 위한 폴더를 만든 경우 경로에 해당 폴더를 지정해야 합니다.



복원 작업이 실패하면 포스트스크립트가 실행되지 않고 정리 작업이 직접 시작됩니다.

b. 복구 후 데이터베이스를 열려면 확인란을 선택하세요.

제어 파일이 있거나 없는 컨테이너 데이터베이스(CDB)를 복원한 후, 또는 CDB 제어 파일만 복원한 후 복구 후에 데이터베이스를 열도록 지정하면 해당 CDB에 있는 플러그형 데이터베이스(PDB)는 열리지 않고 CDB만 열립니다.

RAC 설정에서는 복구에 사용된 RAC 인스턴스만 복구 후에 열립니다.



제어 파일이 있는 사용자 테이블스페이스, 제어 파일이 있거나 없는 시스템 테이블스페이스, 제어 파일이 있거나 없는 PDB를 복원한 후에는 복원 작업과 관련된 PDB의 상태만 원래 상태로 변경됩니다. 복원에 사용되지 않은 다른 PDB의 상태는 해당 PDB의 상태가 저장되지 않았기 때문에 원래 상태로 변경되지 않습니다. 복원에 사용되지 않은 PDB의 상태를 수동으로 변경해야 합니다.

10. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일 알림을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 수행된 복구 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택해야 합니다.



이메일 알림을 받으려면 GUI 또는 PowerShell 명령 Set-SmSmtServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

11. 요약을 검토한 후 *마침*을 클릭하세요.

12. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

자세한 내용은

- "SnapCenter 작업을 수행하기 위해 Oracle RAC One Node 데이터베이스가 건너됩니다."
- "보조 SnapMirror 또는 SnapVault 위치에서 복원하지 못했습니다."
- "고아 화신의 백업에서 복원에 실패했습니다."
- "AIX 시스템의 백업, 복원 및 복제 작업을 위한 사용자 정의 가능한 매개변수"

지정 시점 복구를 사용하여 테이블스페이스 복원 및 복구

데이터베이스의 다른 테이블스페이스에 영향을 주지 않고 손상되거나 삭제된 테이블스페이스 하위 집합을 복원할 수 있습니다. SnapCenter RMAN을 사용하여 테이블스페이스의 PITR(지정 시점 복구)을 수행합니다.

시작하기 전에

- 테이블스페이스의 PITR을 수행하는 데 필요한 백업은 카탈로그화하고 마운트해야 합니다.
- 루트가 아닌 사용자로 플러그인을 설치한 경우, prescript 및 postscript 디렉토리에 대한 실행 권한을 수동으로 할당해야 합니다.

이 작업에 관하여

PITR 작업 중에 RMAN은 지정된 보조 대상에 보조 인스턴스를 생성합니다. 보조 대상은 마운트 지점이나 ASM 디스크 그룹이 될 수 있습니다. 마운트된 위치에 충분한 공간이 있는 경우 전용 마운트 지점 대신 마운트된 위치 중 하나를 재사용할 수 있습니다.

날짜와 시간 또는 SCN을 지정하면 테이블스페이스가 소스 데이터베이스에 복원됩니다.

ASM, NFS, SAN 환경에 있는 여러 테이블스페이스를 선택하고 복원할 수 있습니다. 예를 들어, 테이블스페이스 TS2와 TS3가 NFS에 있고 TS4가 SAN에 있는 경우 단일 PITR 작업을 수행하여 모든 테이블스페이스를 복원할 수 있습니다.



RAC 설정에서는 RAC의 모든 노드에서 테이블스페이스의 PITR을 수행할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 단일 인스턴스(멀티테넌트) 유형의 데이터베이스를 선택합니다.

데이터베이스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 *백업*을 선택합니다.

백업이 카탈로그화되어 있지 않으면 백업을 선택하고 *카탈로그*를 클릭해야 합니다.

5. 카탈로그화된 백업을 선택한 후  *를 클릭합니다.
6. 복원 범위 페이지에서 다음 작업을 수행합니다.
 - a. RAC(Real Application Clusters) 환경에서 데이터베이스 백업을 선택한 경우 RAC 노드를 선택합니다.
 - b. *테이블스페이스*를 선택한 다음 복원하려는 테이블스페이스를 지정합니다.



SYSAUX, SYSTEM 및 UNDO 테이블스페이스에서는 PITR을 수행할 수 없습니다.

- c. 복원 및 복구에 필요한 경우 데이터베이스 상태 변경을 선택하여 복원 및 복구 작업을 수행하는 데 필요한 상태로 데이터베이스 상태를 변경합니다.
7. 복구 범위 페이지에서 다음 작업 중 하나를 수행합니다.
 - 특정 시스템 변경 번호(SCN)로 복구하려면 *SCN까지*를 선택하고 SCN과 보조 대상을 지정합니다.
 - 특정 날짜와 시간으로 복구하려면 *날짜 및 시간*을 선택하고 날짜와 시간, 보조 대상을 지정하세요.

SnapCenter 지정된 SCN 또는 선택한 날짜와 시간을 기반으로 PITR을 수행하는 데 필요한 최적의 데이터 및 로그 백업 수를 식별한 다음 마운트하고 카탈로그화합니다.

8. PreOps 페이지에서 복원 작업 전에 실행할 사전 스크립트의 경로와 인수를 입력합니다.

사전 스크립트는 /var/opt/snapcenter/spl/scripts 경로나 이 경로 내부의 폴더에 저장해야 합니다. 기본적으로 /var/opt/snapcenter/spl/scripts 경로가 채워집니다. 이 경로 내에 스크립트를 저장하기 위한 폴더를 만든 경우 경로에 해당 폴더를 지정해야 합니다.

스크립트 시간 초과 값을 지정할 수도 있습니다. 기본값은 60초입니다.

SnapCenter 사용하면 프리스크립트와 포스트스크립트를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다.
["자세히 알아보기"](#)

9. PostOps 페이지에서 다음 단계를 수행하세요.

a. 복원 작업 후 실행할 PostScript의 경로와 인수를 입력합니다.



복원 작업이 실패하면 포스트스크립트가 실행되지 않고 정리 작업이 직접 시작됩니다.

b. 복구 후 데이터베이스를 열려면 확인란을 선택하세요.

10. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일 알림을 보낼 시나리오를 선택합니다.

11. 요약을 검토한 후 *마침*을 클릭하세요.

12. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

특정 시점 복구를 사용하여 플러그형 데이터베이스를 복원하고 복구합니다.

컨테이너 데이터베이스(CDB)의 다른 PDB에 영향을 주지 않고 손상되거나 삭제된 플러그형 데이터베이스(PDB)를 복원하고 복구할 수 있습니다. SnapCenter RMAN을 사용하여 PDB의 PITR(지정 시점 복구)을 수행합니다.

시작하기 전에

- PDB의 PITR을 수행하는 데 필요한 백업은 카탈로그화하고 마운트해야 합니다.



RAC 설정에서는 RAC 설정의 모든 노드에서 PDB를 수동으로 닫아 상태를 MOUNTED로 변경해야 합니다.

- 루트가 아닌 사용자 플러그인을 설치한 경우, prescript 및 postscript 디렉토리에 대한 실행 권한을 수동으로 할당해야 합니다.

이 작업에 관하여

PITR 작업 중에 RMAN은 지정된 보조 대상에 보조 인스턴스를 생성합니다. 보조 대상은 마운트 지점이나 ASM 디스크 그룹이 될 수 있습니다. 마운트된 위치에 충분한 공간이 있는 경우 전용 마운트 지점 대신 마운트된 위치 중 하나를 재사용할 수 있습니다.

PDB의 PITR을 수행하려면 날짜와 시간 또는 SCN을 지정해야 합니다. RMAN은 데이터 파일을 포함하여 읽기, 쓰기, 읽기 전용 또는 삭제된 PDB를 복구할 수 있습니다.

다음 항목만 복원 및 복구할 수 있습니다.

- 한 번에 하나의 PDB
- PDB의 한 테이블스페이스
- 동일한 PDB의 여러 테이블스페이스



RAC 설정에서는 RAC의 모든 노드에서 테이블스페이스의 PITR을 수행할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 단일 인스턴스(멀티테넌트) 유형의 데이터베이스를 선택합니다.

데이터베이스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 *백업*을 선택합니다.

백업이 카탈로그화되어 있지 않으면 백업을 선택하고 *카탈로그*를 클릭해야 합니다.

5. 카탈로그화된 백업을 선택한 후 *를 클릭합니다.  *.
6. 복원 범위 페이지에서 다음 작업을 수행합니다.
 - a. RAC(Real Application Clusters) 환경에서 데이터베이스 백업을 선택한 경우 RAC 노드를 선택합니다.
 - b. PDB를 복원할지, 아니면 PDB의 테이블스페이스를 복원할지에 따라 다음 작업 중 하나를 수행합니다.

만약 당신이 원한다면...	단계...
PDB 복원	i. *플러그형 데이터베이스(PDB)*를 선택합니다. ii. 복원하려는 PDB를 지정하세요.  PDB\$SEED 데이터베이스에서 PITR을 수행할 수 없습니다.
PDB에서 테이블스페이스 복원	i. *플러그형 데이터베이스(PDB) 테이블스페이스*를 선택합니다. ii. PDB를 지정하세요. iii. 복원할 단일 테이블스페이스 또는 여러 테이블스페이스를 지정합니다.  SYSAUX, SYSTEM 및 UNDO 테이블스페이스에서는 PITR을 수행할 수 없습니다.

- c. 복원 및 복구에 필요한 경우 데이터베이스 상태 변경을 선택하여 복원 및 복구 작업을 수행하는 데 필요한 상태로 데이터베이스 상태를 변경합니다.
7. 복구 범위 페이지에서 다음 작업 중 하나를 수행합니다.
 - 특정 시스템 변경 번호(SCN)로 복구하려면 *SCN까지*를 선택하고 SCN과 보조 대상을 지정합니다.
 - 특정 날짜와 시간으로 복구하려면 *날짜 및 시간*을 선택하고 날짜와 시간, 보조 대상을 지정하세요.

SnapCenter 지정된 SCN 또는 선택한 날짜와 시간을 기반으로 PITR을 수행하는 데 필요한 최적의 데이터 및 로그 백업 수를 식별한 다음 마운트하고 카탈로그화합니다.

8. PreOps 페이지에서 복원 작업 전에 실행할 사전 스크립트의 경로와 인수를 입력합니다.

사전 스크립트는 /var/opt/snapcenter/spl/scripts 경로나 이 경로 내부의 폴더에 저장해야 합니다. 기본적으로 /var/opt/snapcenter/spl/scripts 경로가 채워집니다. 이 경로 내에 스크립트를 저장하기 위한 폴더를 만든 경우 경로에 해당 폴더를 지정해야 합니다.

스크립트 시간 초과 값을 지정할 수도 있습니다. 기본값은 60초입니다.

SnapCenter 사용하면 프리스크립트와 포스트스크립트를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다. ["자세히 알아보기"](#)

9. PostOps 페이지에서 다음 단계를 수행하세요.

- a. 복원 작업 후 실행할 PostScript의 경로와 인수를 입력합니다.



복원 작업이 실패하면 포스트스크립트가 실행되지 않고 정리 작업이 직접 시작됩니다.

- b. 복구 후 데이터베이스를 열려면 확인란을 선택하세요.

RAC 설정에서 PDB는 데이터베이스가 복구된 노드에서만 열립니다. RAC 설정의 다른 모든 노드에서 복구된 PDB를 수동으로 열어야 합니다.

10. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일 알림을 보낼 시나리오를 선택합니다.

11. 요약을 검토한 후 *마침*을 클릭하세요.

12. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

UNIX 명령을 사용하여 Oracle 데이터베이스 복원 및 복구

복구 및 복구 워크플로에는 계획, 복구 및 복구 작업 수행, 작업 모니터링이 포함됩니다.

이 작업에 관하여

- SnapCenter 서버와의 연결을 설정하고, 백업을 나열하고 해당 정보를 검색하고, 백업을 복원하려면 다음 명령을 실행해야 합니다.

명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 Get-Help _command_name_을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 명령 참조 가이드"](#).

- SnapMirror Active Sync 복원 작업의 경우 기본 위치에서 백업을 선택해야 합니다.

단계

1. 지정된 사용자에게 대해 SnapCenter 서버와의 연결 세션을 시작합니다: *Open-SmConnection*
2. 복원하려는 백업에 대한 정보를 검색합니다: *Get-SmBackup*
3. 지정된 백업에 대한 자세한 정보를 검색합니다: *Get-SmBackupDetails*

이 명령은 주어진 백업 ID로 지정된 리소스의 백업에 대한 자세한 정보를 검색합니다. 해당 정보에는 데이터베이스 이름, 버전, 홈, 시작 및 종료 SCN, 테이블스페이스, 플러그형 데이터베이스 및 해당 테이블스페이스가 포함됩니다.

4. 백업에서 데이터 복원: *Restore-SmBackup*

Oracle 데이터베이스 복원 작업 모니터링

작업 페이지를 사용하여 다양한 SnapCenter 복원 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

복원 후 상태는 복원 작업 후 리소스의 조건과 수행할 수 있는 추가 복원 작업을 설명합니다.

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복원 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복원*을 선택합니다.
 - d. 상태 드롭다운 목록에서 복원 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복원 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

Oracle 데이터베이스 복원 작업 취소

대기 중인 복원 작업을 취소할 수 있습니다.

복원 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

이 작업에 관하여

- 모니터 페이지나 활동 창에서 대기 중인 복원 작업을 취소할 수 있습니다.

- 실행 중인 복원 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 대기 중인 복원 작업을 취소할 수 있습니다.
- 취소할 수 없는 복원 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자\그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 복원 작업을 취소할 수 있습니다.

단계

다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	1. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. 2. 작업을 선택하고 *작업 취소*를 클릭하세요.
활동 창	1. 복원 작업을 시작한 후 다음을 클릭하세요.  활동 창에서 가장 최근의 작업 5개를 확인하세요. 2. 작업을 선택하세요. 3. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

Oracle 데이터베이스 복제

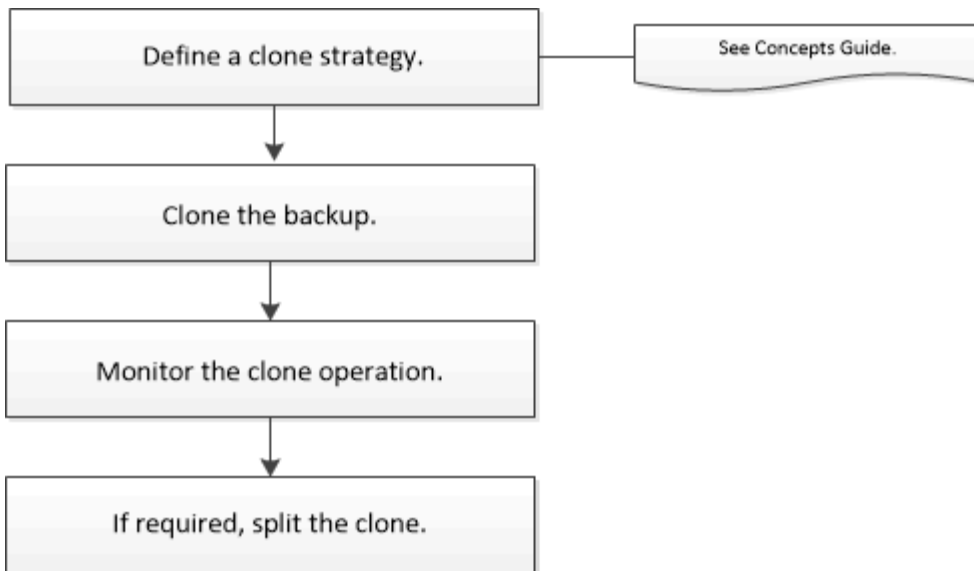
복제 워크플로

복제 워크플로에는 계획, 복제 작업 수행, 작업 모니터링이 포함됩니다.

다음과 같은 이유로 데이터베이스를 복제할 수 있습니다.

- 애플리케이션 개발 주기 동안 현재 데이터베이스 구조와 콘텐츠를 사용하여 구현해야 하는 기능을 테스트합니다.
- 데이터 추출 및 조작 도구를 사용하여 데이터웨어하우스를 채웁니다.
- 실수로 삭제되거나 변경된 데이터를 복구합니다.

다음 워크플로는 복제 작업을 수행해야 하는 순서를 보여줍니다.



Oracle 데이터베이스에 대한 복제 전략 정의

데이터베이스를 복제하기 전에 전략을 정의하면 복제 작업이 성공할 수 있습니다.

복제에 지원되는 백업 유형

SnapCenter 다양한 유형의 Oracle 데이터베이스 백업 복제를 지원합니다.

- 온라인 데이터 백업
- 온라인 전체 백업
- 오프라인 마운트 백업
- 오프라인 종료 백업
- Data Guard 대기 데이터베이스 및 Active Data Guard 대기 데이터베이스 백업
- RAC(Real Application Clusters) 구성에서의 온라인 데이터 백업, 온라인 전체 백업, 오프라인 마운트 백업 및 오프라인 종료 백업
- ASM(자동 스토리지 관리) 구성의 온라인 데이터 백업, 온라인 전체 백업, 오프라인 마운트 백업 및 오프라인 종료 백업



멀티패스 구성 파일의 `user_friendly_names` 옵션이 `yes`로 설정된 경우 SAN 구성은 지원되지 않습니다.



보관 로그 백업 복제는 지원되지 않습니다.

Oracle 데이터베이스에서 지원되는 복제 유형

Oracle 데이터베이스 환경에서 SnapCenter 데이터베이스 백업 복제를 지원합니다. 기본 및 보조 저장 시스템에서 백업을 복제할 수 있습니다.

SnapCenter 서버는 NetApp FlexClone 기술을 사용하여 백업을 복제합니다.

"Refresh-SmClone" 명령을 실행하여 복제본을 새로 고칠 수 있습니다. 이 명령은 데이터베이스의 백업을 생성하고, 기존 복제본을 삭제하고, 같은 이름의 복제본을 생성합니다.



복제 새로 고침 작업은 UNIX 명령을 사용해서만 수행할 수 있습니다.

Oracle 데이터베이스의 복제 명명 규칙

SnapCenter 3.0부터 파일 시스템 복제본에 사용되는 명명 규칙이 ASM 디스크 그룹 복제본과 다릅니다.

- SAN 또는 NFS 파일 시스템의 명명 규칙은 FileSystemNameofsourcedatabase_CLONESID입니다.
- ASM 디스크 그룹의 명명 규칙은 SC_HASHCODEofDISKGROUP_CLONESID입니다.

HASHCODEofDISKGROUP은 각 ASM 디스크 그룹에 대해 고유한 자동 생성 숫자(2~10자리)입니다.

Oracle 데이터베이스 복제의 한계

데이터베이스를 복제하기 전에 복제 작업의 제한 사항을 알고 있어야 합니다.

- 11.2.0.4에서 12.1.0.1까지의 Oracle 버전을 사용하는 경우 *renamedg* 명령을 실행하면 복제 작업이 중단됩니다. 이 문제를 해결하려면 Oracle 패치 19544733을 적용하세요.
- 호스트에 직접 연결된 LUN(예: Windows 호스트에서 Microsoft iSCSI Initiator 사용)에서 동일한 Windows 호스트의 VMDK 또는 RDM LUN이나 다른 Windows 호스트로 데이터베이스를 복제하는 것은 지원되지 않습니다.
- 볼륨 마운트 지점의 루트 디렉토리는 공유 디렉토리가 될 수 없습니다.
- 복제본이 포함된 LUN을 새 볼륨으로 이동하면 복제본을 삭제할 수 없습니다.

클론별 **Prescript** 및 **Postscript**에 대한 미리 정의된 환경 변수

SnapCenter 사용하면 데이터베이스를 복제하는 동안 프리스크립트와 포스트스크립트를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다.

데이터베이스 복제를 위한 지원되는 미리 정의된 환경 변수

- ***SC_ORIGINAL_SID***는 소스 데이터베이스의 SID를 지정합니다.

이 매개변수는 애플리케이션 볼륨에 대해 채워집니다.

예: NFSB32

- ***SC_ORIGINAL_HOST***는 소스 호스트의 이름을 지정합니다.

이 매개변수는 애플리케이션 볼륨에 대해 채워집니다.

예: asmrac1.gdl.englab.netapp.com

- ***SC_ORACLE_HOME***은 대상 데이터베이스의 Oracle 홈 디렉토리 경로를 지정합니다.

예: /ora01/app/oracle/product/18.1.0/db_1

- **SC_BACKUP_NAME**은 백업의 이름을 지정합니다.

이 매개변수는 애플리케이션 볼륨에 대해 채워집니다.

예:

- 데이터베이스가 ARCHIVELOG 모드로 실행되지 않는 경우: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
- 데이터베이스가 ARCHIVELOG 모드에서 실행되는 경우: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG:RG2_scspr2417819002_07-20-2021_12.16.48.9267_1, RG2_scspr2417819002_07-21-2021_12.16.48.9267_1, RG2_scspr2417819002_07-22-2021_12.16.48.9267_1

- *SC_AV_NAME*은 애플리케이션 볼륨의 이름을 지정합니다.

예: AV1|AV2

- *SC_ORIGINAL_OS_USER*는 소스 데이터베이스의 운영 체제 소유자를 지정합니다.

예: 오라클

- *SC_ORIGINAL_OS_GROUP*은 소스 데이터베이스의 운영 체제 그룹을 지정합니다.

예: oinstall

- **SC_TARGET_SID**"는 복제된 데이터베이스의 SID를 지정합니다.

PDB 복제 워크플로의 경우 이 매개변수 값은 미리 정의되지 않습니다.

이 매개변수는 애플리케이션 볼륨에 대해 채워집니다.

예: clonedb

- *SC_TARGET_HOST*는 데이터베이스가 복제될 호스트의 이름을 지정합니다.

이 매개변수는 애플리케이션 볼륨에 대해 채워집니다.

예: asmrac1.gdl.englab.netapp.com

- *SC_TARGET_OS_USER*는 복제된 데이터베이스의 운영 체제 소유자를 지정합니다.

PDB 복제 워크플로의 경우 이 매개변수 값은 미리 정의되지 않습니다.

예: 오라클

- *SC_TARGET_OS_GROUP*은 복제된 데이터베이스의 운영 체제 그룹을 지정합니다.

PDB 복제 워크플로의 경우 이 매개변수 값은 미리 정의되지 않습니다.

예: oinstall

- *SC_TARGET_DB_PORT*는 복제된 데이터베이스의 데이터베이스 포트를 지정합니다.

PDB 복제 워크플로의 경우 이 매개변수 값은 미리 정의되지 않습니다.

구분 기호에 대한 정보는 다음을 참조하세요. ["지원되는 구분 기호"](#).

Oracle 데이터베이스 복제를 위한 요구 사항

Oracle 데이터베이스를 복제하기 전에 필수 구성 요소가 모두 완료되었는지 확인해야 합니다.

- SnapCenter 사용하여 데이터베이스 백업을 만들어야 합니다.

복제 작업을 성공적으로 수행하려면 온라인 데이터 및 로그 백업이나 오프라인(마운트 또는 종료) 백업을 성공적으로 만들어야 합니다.

- 제어 파일이나 리두 로그 파일 경로를 사용자 지정하려면 필요한 파일 시스템이나 ASM(자동 스토리지 관리) 디스크 그룹을 미리 프로비저닝해야 합니다.

기본적으로 복제된 데이터베이스의 리두 로그와 제어 파일은 SnapCenter 에서 복제 데이터베이스의 데이터 파일을 위해 프로비저닝한 ASM 디스크 그룹이나 파일 시스템에 생성됩니다.

- NFS를 통해 ASM을 사용하는 경우 `asm_diskstring` 매개변수에 정의된 기존 경로에 `_var/opt/snapcenter/scu/clones/*/*_`를 추가해야 합니다.
- `asm_diskstring` 매개변수에서 ASMFED를 사용하는 경우 `_AFD:*`를 구성해야 하고, ASMLIB를 사용하는 경우 `_ORCL:*`를 구성해야 합니다.

`asm_diskstring` 매개변수를 편집하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["asm_diskstring에 디스크 경로를 추가하는 방법"](#).

- 대체 호스트에서 복제본을 생성하는 경우 대체 호스트는 다음 요구 사항을 충족해야 합니다.
 - Oracle Database용 SnapCenter 플러그인은 대체 호스트에 설치해야 합니다.
 - 복제 호스트는 기본 또는 보조 스토리지에서 LUN을 검색할 수 있어야 합니다.
 - 기본 스토리지 또는 보조(Vault 또는 Mirror) 스토리지에서 대체 호스트로 복제하는 경우 보조 스토리지와 대체 호스트 간에 iSCSI 세션이 설정되었거나 FC에 대해 적절하게 구역 지정되었는지 확인하세요.
 - Vault 또는 Mirror 스토리지에서 동일한 호스트로 복제하는 경우 Vault 또는 Mirror 스토리지와 호스트 간에 iSCSI 세션이 설정되었는지 또는 FC에 대해 적절하게 구역 지정되었는지 확인하세요.
 - 가상화된 환경에서 복제하는 경우 기본 또는 보조 스토리지와 대체 호스트를 호스팅하는 ESX 서버 간에 iSCSI 세션이 설정되었는지 또는 FC에 대해 적절하게 구역 지정되었는지 확인하세요.

자세한 내용은 다음을 참조하세요. ["호스트 유틸리티 문서"](#).

- 소스 데이터베이스가 ASM 데이터베이스인 경우:
 - 복제가 수행될 호스트에서 ASM 인스턴스가 실행 중이어야 합니다.
 - 복제된 데이터베이스의 보관 로그 파일을 전용 ASM 디스크 그룹에 배치하려면 복제 작업 전에 ASM 디스크 그룹을 프로비저닝해야 합니다.
 - 데이터 디스크 그룹의 이름은 구성할 수 있지만, 복제가 수행될 호스트의 다른 ASM 디스크 그룹에서 해당 이름이 사용되지 않는지 확인하세요.

ASM 디스크 그룹에 있는 데이터 파일은 SnapCenter 복제 워크플로의 일부로 프로비저닝됩니다.

- NVMe의 경우 NVMe util을 설치해야 합니다.
- 로그 백업을 사용하여 대체 호스트에 복제하는 동안 보조 로케이터를 검색하려면 데이터 LUN과 로그 LUN에 대한 보호 유형(예: 미러, 볼트 또는 미러-볼트)이 동일해야 합니다.
- 12_c_ 데이터베이스 백업을 복제하기 위해 시드 PDB 관련 정보를 검색하려면 소스 데이터베이스 매개변수 파일에서 `exclude_seed_cdb_view` 값을 FALSE로 설정해야 합니다.

시드 PDB는 CDB가 PDB를 생성하는 데 사용할 수 있는 시스템 제공 템플릿입니다. 시드 PDB의 이름은 PDB\$SEED입니다. PDB\$SEED에 대한 자세한 내용은 Oracle Doc ID 1940806.1을 참조하세요.



12_c_ 데이터베이스를 백업하기 전에 값을 설정해야 합니다.

- SnapCenter autofs 하위 시스템에서 관리하는 파일 시스템의 백업을 지원합니다. 데이터베이스를 복제하는 경우 플러그인 호스트의 루트 사용자는 autofs 마운트 지점의 루트 아래에 디렉토리를 생성할 권한이 없으므로 데이터 마운트 지점이 autofs 마운트 지점의 루트 아래에 있지 않은지 확인하세요.

제어 및 리두 로그 파일이 데이터 마운트 지점에 있는 경우 제어 파일 경로를 수정한 다음, 그에 따라 리두 로그 파일 경로를 수정해야 합니다.



새로 복제된 마운트 포인트를 autofs 하위 시스템에 수동으로 등록할 수 있습니다. 새로 복제된 마운트 포인트는 자동으로 등록되지 않습니다.

- TDE(자동 로그인)가 있고 동일하거나 다른 호스트에서 데이터베이스를 복제하려는 경우 소스 데이터베이스에서 `/etc/ORACLE/WALLET/$ORACLE_SID` 아래의 지갑(키 파일)을 복제된 데이터베이스로 복사해야 합니다.
- Oracle Linux 7 이상 또는 Red Hat Enterprise Linux(RHEL) 7 이상의 SAN(Storage Area Network) 환경에서 복제를 성공적으로 수행하려면 `_/etc/lvm/lvm.conf_`에서 `use_lvm2 = 0` 값을 설정하고 lvm2-lvm2metad 서비스를 중지해야 합니다.
- Oracle 데이터베이스 11.2.0.3 이상을 사용하고 NID 스크립트를 사용하여 보조 인스턴스의 데이터베이스 ID를 변경하는 경우 13366202 Oracle 패치를 설치해야 합니다.
- 볼륨을 호스팅하는 집계가 스토리지 가상 머신(SVM)의 할당된 집계 목록에 있는지 확인해야 합니다.
- NVMe의 경우 연결에서 대상 포트를 제외해야 하는 경우 `/var/opt/snapcenter/scu/etc/nvme.conf` 파일에 대상 노드 이름과 포트 이름을 추가해야 합니다.

해당 파일이 존재하지 않으면 아래 예시와 같이 파일을 생성해야 합니다.

```
blacklist {
nn-0x<target_node_name_1>:pn-0x<target_port_name_1>
nn-0x<target_node_name_2>:pn-0x<target_port_name_2>
}
```

- LUN이 iSCSI와 FC의 혼합 프로토콜로 구성된 iGroup을 사용하여 AIX 호스트에 매핑되지 않았는지 확인해야 합니다. 자세한 내용은 다음을 참조하세요. ["LUN에 대한 장치를 검색할 수 없습니다. 오류가 발생하여 작업이 실패합니다."](#).

Oracle 데이터베이스 백업 복제

SnapCenter 사용하면 데이터베이스 백업을 사용하여 Oracle 데이터베이스를 복제할 수

있습니다.

시작하기 전에

루트가 아닌 사용자로 플러그인을 설치한 경우, prescript 및 postscript 디렉토리에 대한 실행 권한을 수동으로 할당해야 합니다.

이 작업에 관하여

- 복제 작업은 데이터베이스 데이터 파일의 복사본을 생성하고, 새로운 온라인 리두 로그 파일과 제어 파일을 생성합니다. 지정된 복구 옵션에 따라 데이터베이스를 지정된 시간으로 복구할 수 있습니다.



Linux 호스트에서 생성된 백업을 AIX 호스트로 복제하려고 하거나 그 반대로 복제하려고 하면 복제가 실패합니다.

SnapCenter Oracle RAC 데이터베이스 백업에서 복제될 때 독립형 데이터베이스를 생성합니다. SnapCenter Data Guard 대기 데이터베이스와 Active Data Guard 대기 데이터베이스의 백업에서 복제본을 만드는 것을 지원합니다.

복제 중에 SnapCenter 복구 작업을 위해 SCN 또는 날짜와 시간을 기반으로 최적의 로그 백업 수를 마운트합니다. 복구 후 로그 백업이 마운트 해제됩니다. 이러한 모든 복제본은 `/var/opt/snapcenter/scu/clones/` 아래에 마운트됩니다. NFS를 통해 ASM을 사용하는 경우 `asm_diskstring` 매개변수에 정의된 기존 경로에 `_var/opt/snapcenter/scu/clones/*/*_`를 추가해야 합니다.

SAN 환경에서 ASM 데이터베이스의 백업을 복제하는 동안 복제된 호스트 장치에 대한 udev 규칙이 `_etc/udev/rules.d/999-scu-netapp.rules_`에 생성됩니다. 복제된 호스트 장치와 연관된 이러한 udev 규칙은 복제본을 삭제하면 삭제됩니다.



Flex ASM 설정에서는 RAC 클러스터의 노드 수보다 기수가 적으면 Leaf 노드에서 복제 작업을 수행할 수 없습니다.

- SnapLock 활성화된 정책의 경우 ONTAP 9.12.1 이하 버전에서 스냅샷 잠금 기간을 지정하면 복원의 일부로 변조 방지 스냅샷에서 생성된 복제본은 SnapLock 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

- 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
- 리소스 페이지에서 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
- 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 데이터베이스를 선택합니다.

데이터베이스 토폴로지 페이지가 표시됩니다.

- 복사본 관리 보기에서 로컬 복사본(기본), 미러 복사본(보조) 또는 볼트 복사본(보조) 중에서 백업을 선택합니다.
- 표에서 데이터 백업을 선택한 후 *를 클릭합니다.  *.
- 이름 페이지에서 다음 작업 중 하나를 수행합니다.

만약 당신이 원한다면...	단계...
데이터베이스 복제(CDB 또는 비 CDB)	a. 복제본의 SID를 지정합니다. 클론 SID는 기본적으로 제공되지 않으며, SID의 최대 길이는 8자입니다.  복제본이 생성될 호스트에 동일한 SID를 가진 데이터베이스가 없는지 확인해야 합니다.
플러그형 데이터베이스(PDB) 복제	a. *PDB 복제*를 선택합니다. b. 복제하려는 PDB를 지정합니다. c. 복제된 PDB의 이름을 지정합니다. PDB를 복제하는 자세한 단계는 다음을 참조하세요. "플러그형 데이터베이스 복제".

미러링 또는 볼트 데이터를 선택하는 경우:

- 미러 또는 볼트에 로그 백업이 없으면 아무것도 선택되지 않고 로케이터는 비어 있습니다.
- 미러 또는 볼트에 로그 백업이 있는 경우 최신 로그 백업이 선택되고 해당 로케이터가 표시됩니다.

 선택한 로그 백업이 미러와 볼트 위치에 모두 있는 경우 두 로케이터가 모두 표시됩니다.

7. 위치 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
호스트 복제	기본적으로 소스 데이터베이스 호스트가 채워져 있습니다. 대체 호스트에 복제본을 만들려면 소스 데이터베이스 호스트와 동일한 버전의 Oracle 및 OS를 갖춘 호스트를 선택하세요.

이 분야에서는...	이렇게 하세요...
데이터 파일 위치	기본적으로 데이터 파일 위치가 채워집니다. SAN 또는 NFS 파일 시스템에 대한 SnapCenter의 기본 명명 규칙은 <code>FileSystemNameofsourcedatabase_CLONESID</code>입니다. ASM 디스크 그룹에 대한 SnapCenter 기본 명명 규칙은 <code>SC_HASHCODEofDISKGROUP_CLONESID</code>입니다. <code>.HASHCODEofDISKGROUP</code>은 각 ASM 디스크 그룹마다 고유한 자동 생성 숫자(2~10자리)입니다.  ASM 디스크 그룹 이름을 사용자 지정하는 경우 이름 길이가 Oracle에서 지원하는 최대 길이를 준수하는지 확인하세요. 다른 경로를 지정하려면 복제 데이터베이스에 대한 데이터 파일 마운트 지점이나 ASM 디스크 그룹 이름을 입력해야 합니다. 데이터 파일 경로를 사용자 정의할 때는 제어 파일과 리두 로그 파일 ASM 디스크 그룹 이름이나 파일 시스템도 데이터 파일에 사용된 이름과 동일하게 변경하거나 기존 ASM 디스크 그룹이나 파일 시스템으로 변경해야 합니다.
제어 파일	기본적으로 제어 파일 경로가 채워집니다. 제어 파일은 데이터 파일과 동일한 ASM 디스크 그룹이나 파일 시스템에 배치됩니다. 제어 파일 경로를 재정의하려면 다른 제어 파일 경로를 제공하면 됩니다.  파일 시스템이나 ASM 디스크 그룹이 호스트에 있어야 합니다. 기본적으로 제어 파일의 수는 소스 데이터베이스의 수와 동일합니다. 제어 파일의 개수는 수정할 수 있지만, 데이터베이스를 복제하려면 최소한 하나의 제어 파일이 필요합니다. 소스 데이터베이스와 다른 파일 시스템(기존 파일 시스템)으로 제어 파일 경로를 사용자 정의할 수 있습니다.

이 분야에서는...	이렇게 하세요...
다시 실행 로그	기본적으로 리두 로그 파일 그룹, 경로 및 크기가 채워집니다. 리두 로그는 복제된 데이터베이스의 데이터 파일과 동일한 ASM 디스크 그룹이나 파일 시스템에 배치됩니다. 리두 로그 파일 경로를 재정의하려면 소스 데이터베이스와 다른 파일 시스템으로 리두 로그 파일 경로를 사용자 정의할 수 있습니다.  새로운 파일 시스템이나 ASM 디스크 그룹이 호스트에 있어야 합니다. 기본적으로 리두 로그 그룹, 리두 로그 파일의 수와 크기는 소스 데이터베이스와 동일합니다. 다음 매개변수를 수정할 수 있습니다. - 리두 로그 그룹의 수  데이터베이스를 복제하려면 최소 두 개의 리두 로그 그룹이 필요합니다. - 각 그룹의 Redo 로그 파일과 해당 경로 소스 데이터베이스와 다른 파일 시스템(기존 파일 시스템)으로 리두 로그 파일 경로를 사용자 정의할 수 있습니다.  데이터베이스를 복제하려면 리두 로그 그룹에 최소 하나의 리두 로그 파일이 필요합니다. - 리두 로그 파일의 크기

8. 자격 증명 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
sys 사용자의 자격 증명 이름	복제 데이터베이스의 sys 사용자 비밀번호를 정의하는 데 사용할 자격 증명을 선택합니다. 대상 호스트의 sqlnet.ora 파일에서 SQLNET.AUTHENTICATION_SERVICES가 NONE으로 설정된 경우 SnapCenter GUI에서 자격 증명으로 *없음*을 선택해서는 안 됩니다.

이 분야에서는...	이렇게 하세요...
ASM 인스턴스 자격 증명 이름	복제 호스트의 ASM 인스턴스에 연결하기 위해 OS 인증이 활성화된 경우 *없음*을 선택합니다. 그렇지 않은 경우, "sys" 사용자 또는 복제 호스트에 적용 가능한 "sysasm" 권한이 있는 사용자로 구성된 Oracle ASM 자격 증명을 선택합니다.

Oracle 홈, 사용자 이름 및 그룹 세부 정보는 소스 데이터베이스에서 자동으로 채워집니다. 복제본이 생성될 호스트의 Oracle 환경에 따라 값을 변경할 수 있습니다.

9. PreOps 페이지에서 다음 단계를 수행합니다.

- 복제 작업 전에 실행할 스크립트의 경로와 인수를 입력합니다.

사전 스크립트는 `/var/opt/snapcenter/spl/scripts` 또는 이 경로 내부의 폴더에 저장해야 합니다. 기본적으로 `/var/opt/snapcenter/spl/scripts` 경로가 채워집니다. 이 경로 내부의 폴더에 스크립트를 넣은 경우, 스크립트가 있는 폴더까지의 전체 경로를 제공해야 합니다.

SnapCenter 사용하면 프리스크립트와 포스트스크립트를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다. ["자세히 알아보기"](#)

- 데이터베이스 매개변수 설정 섹션에서 데이터베이스를 초기화하는 데 사용되는 미리 채워진 데이터베이스 매개변수의 값을 수정합니다.

*를 클릭하면 추가 매개변수를 추가할 수 있습니다.  *.

Oracle Standard Edition을 사용 중이고 데이터베이스가 아카이브 로그 모드에서 실행 중이거나 아카이브 리두 로그에서 데이터베이스를 복원하려는 경우 매개변수를 추가하고 경로를 지정합니다.

- 로그_아카이브_대상
- 로그_아카이브_듀플렉스_대상



미리 채워진 데이터베이스 매개변수에는 빠른 복구 영역(FRA)이 정의되어 있지 않습니다. 관련 매개변수를 추가하여 FRA를 구성할 수 있습니다.



`log_archive_dest_1`의 기본값은 `$ORACLE_HOME/clone_sid`이고 복제된 데이터베이스의 아카이브 로그는 이 위치에 생성됩니다. `log_archive_dest_1` 매개변수를 삭제한 경우 아카이브 로그 위치는 Oracle에 의해 결정됩니다. `log_archive_dest_1`을 편집하여 보관 로그의 새 위치를 정의할 수 있지만 파일 시스템이나 디스크 그룹이 존재하고 호스트에서 사용 가능해야 합니다.

- 기본 데이터베이스 매개변수 설정을 가져오려면 *재설정*을 클릭하세요.

10. PostOps 페이지에서는 복제된 데이터베이스를 복구하기 위해 기본적으로 *데이터베이스 복구*와 *취소할 때까지*가 선택되어 있습니다.

SnapCenter 복제를 위해 선택된 데이터 백업 이후에 보관 로그의 연속된 시퀀스가 있는 최신 로그 백업을 마운트하여 복구를 수행합니다. 기본 저장소에서 복제를 수행하려면 로그 및 데이터 백업이 기본 저장소에 있어야 하고, 보조 저장소에서 복제를 수행하려면 로그 및 데이터 백업이 보조 저장소에 있어야 합니다.

SnapCenter 적절한 로그 백업을 찾지 못하면 데이터베이스 복구 및 취소까지 옵션이 선택되지 않습니다. 로그 백업을 사용할 수 없는 경우 *외부 보관 로그 위치 지정*에서 외부 보관 로그 위치를 제공할 수 있습니다. 여러 개의 로그 위치를 지정할 수 있습니다.



FRA(플래시 복구 영역) 및 OMF(Oracle Managed Files)를 지원하도록 구성된 소스 데이터베이스를 복제하려는 경우 복구를 위한 로그 대상도 OMF 디렉토리 구조를 준수해야 합니다.

소스 데이터베이스가 Data Guard 대기 데이터베이스이거나 Active Data Guard 대기 데이터베이스인 경우 PostOps 페이지가 표시되지 않습니다. Data Guard 대기 데이터베이스 또는 Active Data Guard 대기 데이터베이스의 경우 SnapCenter SnapCenter GUI에서 복구 유형을 선택하는 옵션을 제공하지 않지만, 로그를 적용하지 않고 Until Cancel 복구 유형을 사용하여 데이터베이스를 복구합니다.

필드 이름	설명
취소할 때까지	SnapCenter 복제를 위해 선택된 데이터 백업 이후에 끊어지지 않은 아카이브 로그 시퀀스를 갖는 최신 로그 백업을 마운트하여 복구를 수행합니다. 복제된 데이터베이스는 누락되거나 손상된 로그 파일이 복구될 때까지 복구됩니다.
날짜와 시간	SnapCenter 지정된 날짜와 시간까지 데이터베이스를 복구합니다. 허용되는 형식은 mm/dd/yyyy hh:mm:ss입니다. 시간은 24시간 형식으로 지정할 수 있습니다.
SCN(시스템 변경 번호)까지	SnapCenter 지정된 시스템 변경 번호(SCN)까지 데이터베이스를 복구합니다.
외부 보관 로그 위치 지정	데이터베이스가 ARCHIVELOG 모드로 실행되는 경우 SnapCenter 지정된 SCN 또는 선택한 날짜와 시간을 기준으로 최적의 로그 백업 수를 식별하고 마운트합니다. 외부 보관 로그 위치를 지정할 수도 있습니다. '취소할 때까지'를 선택하면 SnapCenter 자동으로 로그 백업을 식별하고 마운트하지 않습니다.
새로운 DBID 생성	기본적으로 새 DBID 만들기 확인란이 선택되어 복제된 데이터베이스에 대한 고유 번호(DBID)를 생성하여 원본 데이터베이스와 구별합니다. 복제된 데이터베이스에 소스 데이터베이스의 DBID를 할당하려면 확인란의 선택을 취소합니다. 이 시나리오에서 소스 데이터베이스가 이미 등록된 외부 RMAN 카탈로그에 복제된 데이터베이스를 등록하려는 경우 작업이 실패합니다.

필드 이름	설명
임시 테이블스페이스에 대한 임시 파일을 생성합니다.	복제된 데이터베이스의 기본 임시 테이블스페이스에 대한 임시 파일을 만들려면 확인란을 선택합니다. 확인란을 선택하지 않으면 임시 파일 없이 데이터베이스 복제본이 생성됩니다.
복제본이 생성될 때 적용할 SQL 항목을 입력하세요.	복제본이 생성될 때 적용할 SQL 항목을 추가합니다.
복제 작업 후 실행할 스크립트를 입력하세요	복제 작업 후 실행할 PostScript의 경로와 인수를 지정합니다. Postscript는 <code>/var/opt/snapcenter/spl/scripts</code> 또는 이 경로 내부의 폴더에 저장해야 합니다. 기본적으로 <code>/var/opt/snapcenter/spl/scripts</code> 경로가 채워집니다. 이 경로 내부의 폴더에 스크립트를 넣은 경우, 스크립트가 있는 폴더까지의 전체 경로를 제공해야 합니다.  복제 작업이 실패하면 포스트스크립트가 실행되지 않고 정리 작업이 직접 시작됩니다.

11. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 수행된 복제 작업의 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

12. 요약을 검토한 후 *마침*을 클릭하세요.



복제본 생성 작업의 일부로 복구를 수행하는 동안 복구가 실패하더라도 경고와 함께 복제본이 생성됩니다. 이 복제본에서 수동 복구를 수행하여 복제본 데이터베이스를 일관된 상태로 되돌릴 수 있습니다.

13. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

결과

데이터베이스를 복제한 후 리소스 페이지를 새로 고쳐 복제된 데이터베이스를 백업에 사용할 수 있는 리소스 중 하나로 나열할 수 있습니다. 복제된 데이터베이스는 표준 백업 워크플로를 사용하여 다른 데이터베이스와 마찬가지로 보호할 수 있으며, 리소스 그룹(새로 생성되었거나 기존)에 포함할 수도 있습니다. 복제된 데이터베이스는 추가로 복제될 수 있습니다(복제의 복제).

복제 후에는 복제된 데이터베이스의 이름을 절대로 바꾸면 안 됩니다.



복제하는 동안 복구를 수행하지 않은 경우, 부적절한 복구로 인해 복제된 데이터베이스의 백업이 실패할 수 있으며, 수동 복구를 수행해야 할 수도 있습니다. 보관 로그에 대해 채워진 기본 위치가 NetApp 스토리지가 아닌 스토리지에 있거나 스토리지 시스템이 SnapCenter 로 구성되지 않은 경우에도 로그 백업이 실패할 수 있습니다.

AIX 설정에서 lkdev 명령을 사용하여 복제된 데이터베이스가 있는 디스크를 잠그고 rendev 명령을 사용하여 디스크의 이름을 바꿀 수 있습니다.

장치를 잠그거나 이름을 변경해도 복제본 삭제 작업에 영향을 미치지 않습니다. SAN 장치에 구축된 AIX LVM 레이아웃의 경우 복제된 SAN 장치에 대한 장치 이름 변경은 지원되지 않습니다.

더 많은 정보를 찾아보세요

- "ORA-00308 오류 메시지와 함께 복원 또는 복제가 실패합니다."
- "복제된 데이터베이스를 복구하지 못했습니다."
- "AIX 시스템의 백업, 복원 및 복제 작업을 위한 사용자 정의 가능한 매개변수"

호스트에서 선호하는 IP를 업데이트합니다.

복제 작업이 완료되면 SAL(Storage Access Layer)에서 복제본에 제공하는 경로는 `<nfs_lif_IP>:<JunctionPath>` 형식이 됩니다. 선호하는 IP를 제공하려면 SCCLI 명령을 사용하여 호스트에서 해당 IP를 구성해야 합니다.

단계

1. 데이터베이스 호스트에 로그인합니다.
2. 지정된 사용자에게 대해 SnapCenter 와 PowerShell 연결 세션을 시작합니다.

오픈-SmConnection

3. 빈 파일을 만듭니다.

`/var/opt/snapcenter/scu/etc/storagepreference.properties`를 터치합니다.

4. SVM에 대한 기본 데이터 LIF를 구성합니다.

`Add-SvmPreferredDataPath -SVM <SVM 이름> -DataPath <IP 주소 또는 FQDN>`

5. 선호하는 경로를 확인하세요.

`Get-SvmPreferredDataPath`

플러그형 데이터베이스 복제

동일한 호스트 또는 대체 호스트의 다른 또는 동일한 대상 CDB에 플러그형 데이터베이스 (PDB)를 복제할 수 있습니다. 복제된 PDB를 원하는 SCN이나 날짜 및 시간으로 복구할 수도 있습니다.

시작하기 전에

루트가 아닌 사용자로 플러그인을 설치한 경우, prescript 및 postscript 디렉토리에 대한 실행 권한을 수동으로 할당해야

합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 단일 인스턴스(멀티 테넌트) 유형의 데이터베이스를 선택합니다.

데이터베이스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 로컬 복사본(기본), 미러 복사본(보조) 또는 볼트 복사본(보조) 중에서 백업을 선택합니다.
5. 테이블에서 백업을 선택한 후 *를 클릭합니다.  *.
6. 이름 페이지에서 다음 작업을 수행합니다.
 - a. *PDB 복제*를 선택합니다.
 - b. 복제하려는 PDB를 지정합니다.

 한 번에 하나의 PDB만 복제할 수 있습니다.

- c. 복제 PDB의 이름을 지정합니다.
7. 위치 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
호스트 복제	기본적으로 소스 데이터베이스 호스트가 채워져 있습니다. 대체 호스트에 복제본을 만들려면 소스 데이터베이스 호스트와 동일한 버전의 Oracle 및 OS를 갖춘 호스트를 선택하세요.
타겟 CDB	복제된 PDB를 포함할 CDB를 선택합니다. 대상 CDB가 실행 중인지 확인해야 합니다.
데이터베이스 상태	PDB를 읽기-쓰기 모드로 열려면 복제된 PDB 를 읽기-쓰기 모드로 열기 확인란을 선택합니다.

데이터 파일 위치	기본적으로 데이터 파일 위치가 채워집니다. SAN 또는 NFS 파일 시스템에 대한 SnapCenter 기본 명명 규칙은 <code>FileSystemNameofsourcedatabase_SCJOBID</code>입니다. ASM 디스크 그룹에 대한 SnapCenter 기본 명명 규칙은 <code>SC_HASHCODEofDISKGROUP_SCJOBID</code>입니다. <code>HASHCODEofDISKGROUP</code>은 각 ASM 디스크 그룹마다 고유한 자동 생성 숫자(2~10자리)입니다. ASM 디스크 그룹 이름을 사용자 지정하는 경우 이름 길이가 Oracle에서 지원하는 최대 길이를 준수하는지 확인하세요. 다른 경로를 지정하려면 복제 데이터베이스에 대한 데이터 파일 마운트 지점이나 ASM 디스크 그룹 이름을 입력해야 합니다.

Oracle 홈, 사용자 이름 및 그룹 세부 정보는 소스 데이터베이스에서 자동으로 채워집니다. 복제본이 생성될 호스트의 Oracle 환경에 따라 값을 변경할 수 있습니다.

8. PreOps 페이지에서 다음 단계를 수행합니다.

- a. 복제 작업 전에 실행할 스크립트의 경로와 인수를 입력합니다.

사전 스크립트는 `/var/opt/snapcenter/spl/scripts` 또는 이 경로 내부의 폴더에 저장해야 합니다. 기본적으로 `/var/opt/snapcenter/spl/scripts` 경로가 채워집니다. 이 경로 내부의 폴더에 스크립트를 넣은 경우, 스크립트가 있는 폴더까지의 전체 경로를 제공해야 합니다.

SnapCenter 사용하면 프리스크립트와 포스트스크립트를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다. ["자세히 알아보기"](#)

- a. 보조 CDB 복제 데이터베이스 매개변수 설정 섹션에서 데이터베이스를 초기화하는 데 사용되는 미리 채워진 데이터베이스 매개변수 값을 수정합니다.

9. 기본 데이터베이스 매개변수 설정을 가져오려면 *재설정*을 클릭하세요.

10. PostOps 페이지에서는 복제된 데이터베이스를 복구하기 위해 기본적으로 *취소할 때까지*가 선택되어 있습니다.

SnapCenter 적절한 로그 백업을 찾지 못하면 취소까지 옵션이 선택되지 않습니다. 로그 백업을 사용할 수 없는 경우 *외부 보관 로그 위치 지정*에서 외부 보관 로그 위치를 제공할 수 있습니다. 여러 개의 로그 위치를 지정할 수 있습니다.



FRA(플래시 복구 영역) 및 OMF(Oracle Managed Files)를 지원하도록 구성된 소스 데이터베이스를 복제하려는 경우 복구를 위한 로그 대상도 OMF 디렉토리 구조를 준수해야 합니다.

필드 이름	설명
취소할 때까지	SnapCenter 복제를 위해 선택된 데이터 백업 이후에 보관 로그의 연속된 시퀀스를 갖는 최신 로그 백업을 마운트하여 복구를 수행합니다. 복제를 수행하려면 기본 저장소에 로그 및 데이터 백업을 해야 하며, 복제를 수행하려면 보조 저장소에 로그 및 데이터 백업을 해야 보조 저장소에 있습니다. 복제된 데이터베이스는 누락되거나 손상된 로그 파일이 복구될 때까지 복구됩니다.
날짜와 시간	SnapCenter 지정된 날짜와 시간까지 데이터베이스를 복구합니다.  시간은 24시간 형식으로 지정할 수 있습니다.
SCN(시스템 변경 번호)까지	SnapCenter 지정된 시스템 변경 번호(SCN)까지 데이터베이스를 복구합니다.
외부 보관 로그 위치 지정	외부 보관 로그 위치를 지정합니다.
새로운 DBID 생성	기본적으로 보조 복제 데이터베이스에는 새 DBID 만들기 확인란이 선택되어 있지 않습니다. 원본 데이터베이스와 구별되는 보조 복제 데이터베이스에 대한 고유 번호(DBID)를 생성하려면 확인란을 선택하세요.
임시 테이블스페이스에 대한 임시 파일을 생성합니다.	복제된 데이터베이스의 기본 임시 테이블스페이스에 대한 임시 파일을 만들려면 확인란을 선택합니다. 확인란을 선택하지 않으면 임시 파일 없이 데이터베이스 복제본이 생성됩니다.
복제본이 생성될 때 적용할 SQL 항목을 입력하세요.	복제본이 생성될 때 적용할 SQL 항목을 추가합니다.

필드 이름	설명
복제 작업 후 실행할 스크립트를 입력하세요	복제 작업 후 실행할 PostScript의 경로와 인수를 지정합니다. Postscript는 <code>/var/opt/snapcenter/spl/scripts</code> 또는 이 경로 내부의 폴더에 저장해야 합니다. 기본적으로 <code>/var/opt/snapcenter/spl/scripts</code> 경로가 채워집니다. 이 경로 내부의 폴더에 스크립트를 넣은 경우, 스크립트가 있는 폴더까지의 전체 경로를 제공해야 합니다.  복제 작업이 실패하면 포스트스크립트가 실행되지 않고 정리 작업이 직접 시작됩니다.

11. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 수행된 복제 작업의 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

12. 요약을 검토한 후 *마침*을 클릭하세요.

13. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

끝난 후

복제된 PDB의 백업을 만들려면 PDB가 복제된 대상 CDB를 백업해야 합니다. 복제된 PDB만 백업하는 것은 불가능하기 때문입니다. 보조 관계를 통해 백업을 생성하려면 대상 CDB에 대한 보조 관계를 생성해야 합니다.

RAC 설정에서 복제된 PDB의 저장소는 PDB 복제가 수행된 노드에만 연결됩니다. RAC의 다른 노드에 있는 PDB는 MOUNT 상태입니다. 복제된 PDB에 다른 노드에서 액세스할 수 있게 하려면 다른 노드에 스토리지를 수동으로 연결해야 합니다.

더 많은 정보를 찾아보세요

- ["ORA-00308 오류 메시지와 함께 복원 또는 복제가 실패합니다."](#)
- ["AIX 시스템의 백업, 복원 및 복제 작업을 위한 사용자 정의 가능한 매개변수"](#)

UNIX 명령을 사용하여 Oracle 데이터베이스 백업 복제

복제 워크플로에는 계획, 복제 작업 수행, 작업 모니터링이 포함됩니다.

이 작업에 관하여

Oracle 데이터베이스 복제 사양 파일을 만들고 복제 작업을 시작하려면 다음 명령을 실행해야 합니다.

명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `Get-Help _command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 명령 참조 가이드](#)".

단계

1. 지정된 백업에서 Oracle 데이터베이스 복제 사양을 만듭니다: *New-SmOracleCloneSpecification*



2차 데이터 보호 정책이 통합 미러 볼트인 경우 `-IncludeSecondaryDetails`만 지정합니다. `-SecondaryStorageType`을 지정할 필요는 없습니다.

이 명령은 지정된 소스 데이터베이스와 해당 백업에 대한 Oracle 데이터베이스 복제 사양 파일을 자동으로 생성합니다. 또한 복제 데이터베이스 SID를 제공해야 합니다. 그래야 생성될 복제 데이터베이스에 대해 자동으로 생성된 값이 사양 파일에 저장됩니다.



클론 사양 파일은 `_var/opt/snapcenter/sco/clone_specs_`에 생성됩니다.

2. 복제 리소스 그룹 또는 기존 백업에서 복제 작업을 시작합니다: *New-SmClone*

이 명령은 복제 작업을 시작합니다. 복제 작업을 위해 Oracle 복제 사양 파일 경로도 제공해야 합니다. 또한 복구 옵션, 복제 작업을 수행할 호스트, 사전 스크립트, 사후 스크립트 및 기타 세부 정보를 지정할 수 있습니다.

기본적으로 복제 데이터베이스의 아카이브 로그 대상 파일은 `_$ORACLE_HOME/CLONE_SIDs_`에 자동으로 채워집니다.

Oracle 데이터베이스 복제본 분할

SnapCenter 사용하면 복제된 리소스를 부모 리소스에서 분할할 수 있습니다. 분할된 복제본은 부모 리소스로부터 독립됩니다.

이 작업에 관하여

- 중간 복제본에서는 복제 분할 작업을 수행할 수 없습니다.

예를 들어, 데이터베이스 백업에서 clone1을 만든 후 clone1의 백업을 만든 다음 이 백업(clone2)을 복제할 수 있습니다. clone2를 생성한 후 clone1은 중간 복제본이 되며 clone1에서 복제 분할 작업을 수행할 수 없습니다. 하지만 clone2에 대해 클론 분할 작업을 수행할 수 있습니다.

clone2를 분할한 후에는 clone1에 대해 clone 분할 작업을 수행할 수 있습니다. clone1은 더 이상 중간 클론이 아니기 때문입니다.

- 복제본을 분할하면 복제본의 백업 사본이 삭제됩니다.
- FlexClone 볼륨 분할 작업에 대한 정보는 다음을 참조하세요. <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["FlexClone 볼륨을 부모 볼륨에서 분할합니다."]
- 스토리지 시스템의 볼륨이나 집계가 온라인인지 확인하세요.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *데이터베이스*를 선택합니다.

3. 복제된 리소스(예: 데이터베이스 또는 LUN)를 선택한 다음 클릭합니다.  .
4. 분할할 클론의 예상 크기와 집계에 필요한 사용 가능한 공간을 검토한 다음 *시작*을 클릭합니다.
5. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

SMCore 서비스가 다시 시작되고 복제 분할 작업이 수행된 데이터베이스가 리소스 페이지에 복제본으로 나열되면 복제 분할 작업이 응답하지 않습니다. *Stop-SmJob* cmdlet을 실행하여 복제 분할 작업을 중지한 다음 복제 분할 작업을 다시 시도해야 합니다.

복제본이 분할되었는지 여부를 확인하기 위해 더 긴 폴링 시간이나 더 짧은 폴링 시간이 필요한 경우, *SMCoreServiceHost.exe.config* 파일에서 *CloneSplitStatusCheckPollTime* 매개변수 값을 변경하여 SMCore가 복제본 분할 작업의 상태를 폴링하는 시간 간격을 설정할 수 있습니다. 값은 밀리초이고 기본값은 5분입니다.

예를 들어,

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```



백업, 복원 또는 다른 클론 분할이 진행 중이면 클론 분할 시작 작업이 실패합니다. 실행 중인 작업이 완료된 후에만 복제 분할 작업을 다시 시작해야 합니다.

플러그형 데이터베이스의 분할 복제본

SnapCenter 사용하면 복제된 플러그형 데이터베이스(PDB)를 분할할 수 있습니다.

이 작업에 관하여

PDB가 복제된 대상 CDB의 백업을 만든 경우 PDB 복제본을 분할하면 복제된 PDB가 포함된 대상 CDB의 모든 백업에서 복제된 PDB도 제거됩니다.



PDB 복제본은 인벤토리 또는 리소스 보기에 표시되지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 또는 리소스 그룹 보기에서 소스 컨테이너 데이터베이스(CDB)를 선택합니다.
3. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 *복제본*을 선택합니다.
4. PDB 복제본(targetCDB:PDBClone)을 선택한 다음 클릭하세요.  .
5. 분할할 클론의 예상 크기와 집계에 필요한 사용 가능한 공간을 검토한 다음 *시작*을 클릭합니다.
6. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

Oracle 데이터베이스 복제 작업 모니터링

작업 페이지를 사용하여 SnapCenter 복제 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복제 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복제*를 선택합니다.
 - d. 상태 드롭다운 목록에서 복제 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복제 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

클론 새로 고침

Refresh-SmClone 명령을 실행하여 복제본을 새로 고칠 수 있습니다. 이 명령은 데이터베이스의 백업을 생성하고, 기존 복제본을 삭제하고, 같은 이름의 복제본을 생성합니다.



PDB 복제본을 새로 고칠 수 없습니다.

필요한 것

- 예약된 백업이 활성화되지 않은 상태에서 온라인 전체 백업이나 오프라인 데이터 백업 정책을 만듭니다.
- 백업 실패에 대해서만 정책에서 이메일 알림을 구성합니다.
- 원치 않는 백업이 발생하지 않도록 주문형 백업의 보존 횟수를 적절히 정의합니다.
- 새로 고침 복제 작업을 위해 식별된 리소스 그룹에는 온라인 전체 백업 또는 오프라인 데이터 백업 정책만 연결되어 있는지 확인하세요.
- 데이터베이스가 하나만 있는 리소스 그룹을 만듭니다.
- 클론 새로 고침 명령에 대한 Cron 작업이 생성되는 경우 SnapCenter 일정과 Cron 일정이 데이터베이스 리소스 그룹에 대해 겹치지 않는지 확인하세요.

복제 새로 고침 명령에 대해 생성된 크론 작업의 경우 24시간마다 Open-SmConnection을 실행해야 합니다.

- 복제본 SID가 호스트에 대해 고유한지 확인하세요.

여러 개의 새로 고침 복제 작업에서 동일한 복제 사양 파일을 사용하거나 동일한 복제 SID를 가진 복제 사양 파일을 사용하는 경우 호스트에서 해당 SID를 가진 기존 복제본이 삭제된 다음 복제본이 생성됩니다.

- 백업 정책이 보조 보호와 함께 활성화되어 있는지 확인하고, 보조 백업을 사용하여 복제본을 생성하기 위해 "-IncludeSecondaryDetails"로 복제 사양 파일을 생성하세요.
 - 기본 복제 사양 파일이 지정되었지만 정책에 보조 업데이트 옵션이 선택된 경우 백업이 생성되고 업데이트가 보조로 전송됩니다. 하지만 복제본은 기본 백업에서 생성됩니다.
 - 기본 복제 사양 파일이 지정되고 정책에 보조 업데이트 옵션이 선택되지 않은 경우 백업은 기본에 생성되고 복제본은 기본에서 생성됩니다.

단계

1. 지정된 사용자에 대해 SnapCenter 서버와의 연결 세션을 시작합니다: *Open-SmConnection*
2. 지정된 백업에서 Oracle 데이터베이스 복제 사양을 만듭니다: *New-SmOracleCloneSpecification*



2차 데이터 보호 정책이 통합 미러 볼트인 경우 -IncludeSecondaryDetails만 지정합니다. -SecondaryStorageType을 지정할 필요는 없습니다.

이 명령은 지정된 소스 데이터베이스와 해당 백업에 대한 Oracle 데이터베이스 복제 사양 파일을 자동으로 생성합니다. 또한 복제 데이터베이스 SID를 제공해야 합니다. 그래야 생성될 복제 데이터베이스에 대해 자동으로 생성된 값이 사양 파일에 저장됩니다.



클론 사양 파일은 `_var/opt/snapcenter/sco/clone_specs_`에 생성됩니다.

3. `_Refresh-SmClone_`을 실행합니다.

"PL-SCO-20032: canExecute 작업이 오류로 인해 실패했습니다: PL-SCO-30031: Redo 로그 파일 +SC_2959770772_clmdb/clmdb/redolog/redo01_01.log가 있습니다" 오류 메시지와 함께 작업이 실패하는 경우 `_WaitToTriggerClone_`에 더 높은 값을 지정하세요.

UNIX 명령에 대한 자세한 내용은 다음을 참조하세요. "[SnapCenter 소프트웨어 명령 참조 가이드](#)".

플러그형 데이터베이스의 복제본 삭제

더 이상 필요하지 않으면 플러그형 데이터베이스(PDB)의 복제본을 삭제할 수 있습니다.

PDB가 복제된 대상 CDB의 백업을 만든 경우 PDB 복제본을 삭제하면 복제된 PDB도 대상 CDB의 백업에서 제거됩니다.



PDB 복제본은 인벤토리 또는 리소스 보기에 표시되지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.

2. 리소스 또는 리소스 그룹 보기에서 소스 컨테이너 데이터베이스(CDB)를 선택합니다.
3. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 *복제본*을 선택합니다.
4. PDB 복제본(targetCDB:PDBClone)을 선택한 다음 클릭하세요. .
5. *확인*을 클릭합니다.

애플리케이션 볼륨 관리

애플리케이션 볼륨이란 무엇입니까?

애플리케이션 볼륨은 Oracle 데이터베이스와 관련된 구성, 설치 프로그램 및 기타 비데이터 파일과 같은 정보가 저장되는 저장소입니다.

Oracle Database용 SnapCenter 플러그인을 사용하면 Oracle 데이터베이스와 함께 애플리케이션 볼륨(비데이터 볼륨)의 일관된 백업을 생성할 수 있습니다.

이 플러그인은 애플리케이션 볼륨의 백업과 복제를 자동화합니다.

- Oracle 데이터베이스 볼륨과 함께 애플리케이션 볼륨을 단일 리소스 그룹으로 보호합니다.
- 애플리케이션 볼륨의 백업을 만듭니다.
- 애플리케이션 볼륨과 함께 Oracle 데이터베이스의 백업을 만듭니다.
- 특정 시점까지의 애플리케이션 볼륨과 함께 데이터베이스 복제본을 만듭니다.
- 백업 작업을 예약합니다.
- 모든 작업을 모니터링합니다.
- 백업 및 복제 작업 보고서를 확인합니다.

애플리케이션 볼륨 추가

SnapCenter Oracle 데이터베이스의 애플리케이션 볼륨 백업 및 복제를 지원합니다. 애플리케이션 볼륨을 수동으로 추가해야 합니다. 애플리케이션 볼륨의 자동 검색은 지원되지 않습니다.



애플리케이션 볼륨은 직접 NFS 및 직접 iSCSI 연결만 지원합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
2. *애플리케이션 볼륨 추가*를 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.
 - 이름 필드에 애플리케이션 볼륨의 이름을 입력합니다.
 - 호스트 이름 필드에 호스트 이름을 입력합니다.
4. 스토리지 풋프린트 페이지에서 스토리지 시스템 이름을 입력하고, 볼륨을 하나 이상 선택한 후, 연관된 LUN이나 Qtree를 지정합니다.

여러 개의 저장 시스템을 추가할 수 있습니다.

5. 요약을 검토한 후 *마침*을 클릭하세요.
6. 리소스 페이지에서 보기 목록에서 *애플리케이션 볼륨*을 선택하면 추가한 모든 애플리케이션 볼륨을 볼 수 있습니다.

애플리케이션 볼륨 수정

백업이 생성되지 않으면 애플리케이션 볼륨을 추가하는 동안 지정한 모든 값을 수정할 수 있습니다. 백업이 생성되면 스토리지 시스템 세부 정보만 수정할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *신청 볼륨*을 선택합니다.

3.  값을 수정합니다.

4.  값을 수정합니다.

애플리케이션 볼륨 삭제

애플리케이션 볼륨을 삭제하면 해당 애플리케이션 볼륨과 연관된 백업이 있는 경우 해당 애플리케이션 볼륨은 유지 관리 모드로 전환되고 새로운 백업이 생성되지 않으며 이전 백업도 보존되지 않습니다. 연관된 백업이 없으면 모든 메타데이터가 삭제됩니다.

필요한 경우 SnapCenter 사용하여 삭제 작업을 실행 취소할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *신청 볼륨*을 선택합니다.
3. 딸깍 하는 소리  [삭제 아이콘]을 클릭하여 값을 수정합니다.

백업 애플리케이션 볼륨

백업 애플리케이션 볼륨

애플리케이션 볼륨이 어떤 리소스 그룹에도 속하지 않으면 리소스 페이지에서 애플리케이션 볼륨을 백업할 수 있습니다.

이 작업에 관하여

기본적으로 일관성 그룹(CG) 백업이 생성됩니다. 볼륨 기반 백업을 생성하려면 *web.config* 파일에서 **EnableOracleNdvVolumeBasedBackup** 값을 true로 설정해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *신청 볼륨*을 선택합니다.
3. *를 클릭하세요  *를 선택한 다음 호스트 이름과 데이터베이스 유형을 선택하여 리소스를 필터링합니다.

그런 다음 *를 클릭할 수 있습니다.  * 필터 창을 닫습니다.

4. 백업할 애플리케이션 볼륨을 선택하세요.

애플리케이션 볼륨 보호 페이지가 표시됩니다.

5. 리소스 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
스냅샷 복사에 사용자 정의 이름 형식 사용	이 확인란을 선택한 다음 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다. 예를 들어, customtext__policy_hostname 또는 resource_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.
백업에서 아카이브 로그 대상 제외	백업하지 않을 보관 로그 파일의 대상을 지정합니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다.  *.

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

- b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.
- c. 정책 _policy_name_에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

_policy_name_은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

7. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스에서 수행된 백업 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtplibServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

8. 요약 검토한 후 *마침*을 클릭하세요.

애플리케이션 볼륨 토폴로지 페이지가 표시됩니다.

9. *지금 백업*을 클릭하세요.
10. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스에 여러 정책을 적용한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.
 - b. *백업*을 클릭하세요.
11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

애플리케이션 볼륨 리소스 그룹을 백업합니다.

애플리케이션 볼륨만 포함된 리소스 그룹이나 애플리케이션 볼륨과 데이터베이스가 혼합된 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 대한 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다.

리소스 그룹에 여러 개의 애플리케이션 볼륨이 있는 경우 모든 애플리케이션 볼륨에 SnapMirror 또는 SnapVault 복제 정책이 있어야 합니다.

이 작업에 관하여

기본적으로 일관성 그룹(CG) 백업이 생성됩니다. 볼륨 기반 백업을 생성하려면 *web.config* 파일에서 **EnableOracleNdvVolumeBasedBackup** 값을 true로 설정해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.

검색창에 리소스 그룹 이름을 입력하거나 *를 클릭하여 리소스 그룹을 검색할 수 있습니다.  *를 클릭한 다음 태그를 선택합니다. 그런 다음 *를 클릭할 수 있습니다.  * 필터 창을 닫습니다.

3. 리소스 그룹 페이지에서 백업하려는 리소스 그룹을 선택한 다음, *지금 백업*을 클릭합니다.
4. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스 그룹에 여러 정책을 연결한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. *백업*을 클릭하세요.

5. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.



검증 작업은 데이터베이스에 대해서만 수행되고 애플리케이션 볼륨에 대해서는 수행되지 않습니다.

복제 애플리케이션 볼륨 백업

SnapCenter 사용하여 애플리케이션 볼륨 백업을 복제할 수 있습니다.

시작하기 전에

루트가 아닌 사용자로 플러그인을 설치한 경우, prescript 및 postscript 디렉토리에 대한 실행 권한을 수동으로 할당해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *신청 볼륨*을 선택합니다.
3. 애플리케이션 볼륨 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 애플리케이션 볼륨을 선택합니다.

애플리케이션 볼륨 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 로컬 복사본(기본), 미러 복사본(보조) 또는 볼트 복사본(보조) 중에서 백업을 선택합니다.
5. 테이블에서 백업을 선택한 후  *.
6. 위치 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
플러그인 호스트	복제본을 만들 호스트를 선택하세요.
대상 리소스 이름	리소스 이름을 지정합니다.

7. 스크립트 페이지에서 복제 전에 실행할 스크립트 이름, 파일 시스템을 마운트하는 명령, 복제 후에 실행할 스크립트 이름을 지정합니다.
8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 수행된 복제 작업의 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtplibServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

9. 요약 검토 후 *마침*을 클릭하세요.

애플리케이션 볼륨 복제본 분할

SnapCenter 사용하면 복제된 리소스를 부모 리소스에서 분할할 수 있습니다. 분할된 복제본은 부모 리소스로부터 독립됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *신청 볼륨*을 선택합니다.
3. 복제된 리소스를 선택하고 클릭하세요. .
4. 분할할 클론의 예상 크기와 집계에 필요한 사용 가능한 공간을 검토한 다음 *시작*을 클릭합니다.

5. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

애플리케이션 볼륨 복제본 삭제

더 이상 필요하지 않은 복제본은 삭제할 수 있습니다. 다른 클론의 소스 역할을 하는 클론은 삭제할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *신청 볼륨*을 선택합니다.
3. 목록에서 리소스 또는 리소스 그룹을 선택합니다.

리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 *복제본*을 선택합니다.
5. 복제본을 선택한 다음 클릭하세요.  .
6. 복제본 삭제 페이지에서 다음 작업을 수행합니다.
 - a. 사전 복제 삭제 필드에 복제본을 삭제하기 전에 실행할 스크립트의 이름을 입력합니다.
 - b. 언마운트 필드에 클론을 삭제하기 전에 클론을 언마운트하는 명령을 입력합니다.
7. *확인*을 클릭합니다.

Windows 파일 시스템 보호

Microsoft Windows 개념에 대한 SnapCenter 플러그인

Microsoft Windows용 SnapCenter 플러그인 개요

Microsoft Windows용 SnapCenter 플러그인은 NetApp SnapCenter 소프트웨어의 호스트 측 구성 요소로, Microsoft 파일 시스템 리소스의 애플리케이션 인식 데이터 보호 관리를 지원합니다. 또한 Windows 파일 시스템에 대한 스토리지 프로비저닝, 스냅샷 일관성 및 공간 회수 기능을 제공합니다. Windows용 플러그인은 SnapCenter 환경에서 파일 시스템 백업, 복원 및 복제 작업을 자동화합니다.

Windows용 플러그인을 설치하면 NetApp SnapMirror 기술과 함께 SnapCenter 사용하여 다른 볼륨에 백업 세트의 미러 사본을 만들고 NetApp SnapVault 기술을 사용하여 보관이나 표준 준수를 위해 디스크 간 백업 복제를 수행할 수 있습니다.

- SnapCenter 환경의 Windows 호스트에서 실행 중인 다른 플러그인에 대한 애플리케이션 인식 데이터 보호를 활성화합니다.
- SnapCenter 환경에서 Microsoft 파일 시스템에 대한 애플리케이션 인식 백업, 복원 및 복제 작업을 자동화합니다.
- Windows 호스트에 대한 스토리지 프로비저닝, 스냅샷 일관성 및 공간 회수를 지원합니다.



Windows용 플러그인은 물리적 LUN과 RDM LUN에서 SMB 공유와 Windows 파일 시스템을 프로비저닝하지만 SMB 공유에서 Windows 파일 시스템에 대한 백업 작업은 지원하지 않습니다.

Microsoft Windows용 SnapCenter 플러그인으로 할 수 있는 일

Windows용 플러그인이 사용자 환경에 설치되면 SnapCenter 사용하여 Windows 파일 시스템을 백업, 복원 및 복제할 수 있습니다. 해당 작업을 지원하는 작업도 수행할 수 있습니다.

- 리소스를 찾아보세요
- Windows 파일 시스템 백업
- 백업 작업 예약
- 파일 시스템 백업 복원
- 파일 시스템 백업 복제
- 백업, 복원 및 복제 작업 모니터링



Windows용 플러그인은 SMB 공유의 파일 시스템 백업 및 복원을 지원하지 않습니다.

Windows용 SnapCenter 플러그인 기능

Windows용 플러그인은 스토리지 시스템의 NetApp 스냅샷 기술과 통합됩니다. Windows용 플러그인을 사용하려면 SnapCenter 인터페이스를 사용하세요.

Windows용 플러그인에는 다음과 같은 주요 기능이 포함되어 있습니다.

- * SnapCenter 가 지원하는 통합 그래픽 사용자 인터페이스*

SnapCenter 인터페이스는 플러그인과 환경 전반에 걸쳐 표준화와 일관성을 제공합니다. SnapCenter 인터페이스를 사용하면 플러그인 전반에 걸쳐 일관된 백업 및 복원 프로세스를 완료하고, 중앙 집중식 보고를 사용하고, 한눈에 볼 수 있는 대시보드 보기를 사용하고, 역할 기반 액세스 제어(RBAC)를 설정하고, 모든 플러그인에서 작업을 모니터링할 수 있습니다. SnapCenter 백업 및 복제 작업을 지원하기 위해 중앙 집중식 스케줄링 및 정책 관리 기능도 제공합니다.

- 자동화된 중앙 관리

일상적인 파일 시스템 백업을 예약하고, 정책 기반 백업 보존을 구성하고, 복원 작업을 설정할 수 있습니다. SnapCenter 구성하여 이메일 알림을 보내 파일 시스템 환경을 사전에 모니터링할 수도 있습니다.

- 중단 없는 **NetApp** 스냅샷 기술

Windows용 플러그인은 NetApp Snapshot 기술을 사용합니다. 이를 통해 몇 초 만에 파일 시스템을 백업하고 호스트를 오프라인으로 전환하지 않고도 빠르게 복원할 수 있습니다. 스냅샷은 최소한의 저장 공간을 차지합니다.

이러한 주요 기능 외에도 Windows용 플러그인은 다음과 같은 이점을 제공합니다.

- 백업, 복원 및 복제 워크플로 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임
- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 프로덕션 파일 시스템의 공간 효율적인 복사본 생성

FlexClone 라이선싱 정보는 다음을 참조하세요. "[SnapCenter 라이선스](#)".

- 여러 서버에서 동시에 여러 백업을 실행할 수 있는 기능
- 백업, 복원 및 복제 작업 스크립팅을 위한 PowerShell cmdlet
- 파일 시스템 및 가상 머신 디스크(VMDK) 백업 지원
- 물리적 및 가상화된 인프라 지원
- iSCSI, 파이버 채널, FCoE, 원시 장치 매핑(RDM), 비대칭 LUN 매핑(ALM), NFS 및 VMFS를 통한 VMDK, 가상 FC 지원
- Windows Server 2022에서 NVMe(Non-Volatile Memory Express) 지원
 - TCP/IP를 통한 NVMe에서 생성된 VMDK 레이아웃에 대한 백업, 복원, 복제 및 검증 워크플로.
 - ESX 8.0 업데이트 2부터 NVMe 펌웨어 버전 1.3을 지원하고 가상 하드웨어 버전 21이 필요합니다.
 - Windows Server 장애 조치(Failover) 클러스터링(WSFC)은 TCP/IP를 통한 NVMe의 VMDK를 통한 애플리케이션에서 지원되지 않습니다.
- 사이트 전체에 장애가 발생해도 비즈니스 서비스가 계속 운영될 수 있도록 하는 SnapMirror Active Sync(처음에는 SnapMirror Business Continuity[SM-BC]로 출시)를 지원하며, 보조 복사본을 사용하여 애플리케이션이 투명하게 장애 조치되도록 지원합니다. SnapMirror Active Sync를 사용하면 장애 조치를 트리거하는 데 수동 개입이나 추가 스크립팅이 필요하지 않습니다.

SnapCenter Windows 파일 시스템을 백업하는 방법

SnapCenter 스냅샷 기술을 사용하여 Windows 클러스터의 LUN, CSV(클러스터 공유 볼륨), RDM(원시 장치 매핑) 볼륨, ALM(비대칭 LUN 매핑), VMFS/NFS(NFS를 사용하는 VMware Virtual Machine File System) 기반 VMDK에 있는 Windows 파일 시스템 리소스를 백업합니다.

SnapCenter 파일 시스템의 스냅샷을 만들어 백업을 생성합니다. 볼륨에 여러 호스트의 LUN이 포함된 연합 백업은 각 파일 시스템의 개별 스냅샷과 달리 볼륨의 스냅샷을 하나만 생성하므로 각 개별 LUN의 백업보다 빠르고 효율적입니다.

SnapCenter 스냅샷을 생성하면 전체 스토리지 시스템 볼륨이 스냅샷에 캡처됩니다. 하지만 백업은 백업이 생성된 호스트 서버에만 유효합니다.

다른 호스트 서버의 데이터가 동일한 볼륨에 있는 경우 스냅샷에서 해당 데이터를 복원할 수 없습니다.



Windows 파일 시스템에 데이터베이스가 포함되어 있는 경우, 파일 시스템을 백업하는 것은 데이터베이스를 백업하는 것과 다릅니다. 데이터베이스를 백업하려면 데이터베이스 플러그인 중 하나를 사용해야 합니다.

Microsoft Windows용 SnapCenter 플러그인에서 지원하는 스토리지 유형

SnapCenter 물리적 머신과 가상 머신 모두에서 다양한 스토리지 유형을 지원합니다. 호스트에 패키지를 설치하기 전에 해당 스토리지 유형에 대한 지원이 제공되는지 확인해야 합니다.

SnapCenter 프로비저닝 및 데이터 보호 지원은 Windows Server에서 제공됩니다. 지원되는 버전에 대한 최신 정보는 다음을

참조하세요. [https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT\[\"NetApp 상호 운용성 매트릭스 도구\"\]](https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT[\).

기계	저장 유형	제공을 사용하여	지원 노트
물리적 서버	FC 연결 LUN	SnapCenter 그래픽 사용자 인터페이스(GUI) 또는 PowerShell cmdlet	
물리적 서버	iSCSI로 연결된 LUN	SnapCenter GUI 또는 PowerShell cmdlet	
물리적 서버	SVM(스토리지 가상 머신)에 있는 SMB3(CIFS) 공유	SnapCenter GUI 또는 PowerShell cmdlet	프로비저닝만 지원합니다.
VMware VM	FC 또는 iSCSI HBA로 연결된 RDM LUN	PowerShell cmdlet	
VMware VM	iSCSI 이니시에이터에 의해 게스트 시스템에 직접 연결된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	

기계	저장 유형	제공을 사용하여	지원 노트
VMware VM	가상 머신 파일 시스템(VMFS) 또는 NFS 데이터 저장소	VMware vSphere	
VMware VM	SVM에 있는 SMB3 공유에 연결된 게스트 시스템	SnapCenter GUI 또는 PowerShell cmdlet	프로비저닝만 지원합니다.
VMware VM	NFS와 SAN 모두에 있는 vVol 데이터 저장소	VMware vSphere용 ONTAP 도구	
Hyper-V VM	가상 파이버 채널 스위치로 연결된 가상 FC(vFC) LUN	SnapCenter GUI 또는 PowerShell cmdlet	가상 파이버 채널 스위치로 연결된 가상 FC(vFC) LUN을 프로비저닝하려면 Hyper-V 관리자를 사용해야 합니다.  NetApp 스토리지에 프로비저닝된 VHD(x)에 있는 Hyper-V 패스스루 디스크와 데이터베이스 백업은 지원되지 않습니다.
Hyper-V VM	iSCSI 이니시에이터에 의해 게스트 시스템에 직접 연결된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	 NetApp 스토리지에 프로비저닝된 VHD(x)에 있는 Hyper-V 패스스루 디스크와 데이터베이스 백업은 지원되지 않습니다.

기계	저장 유형	제공을 사용하여	지원 노트
Hyper-V VM	SVM에 있는 SMB3 공유에 연결된 게스트 시스템	SnapCenter GUI 또는 PowerShell cmdlet	프로비저닝만 지원합니다.  NetApp 스토리지에 프로비저닝된 VHD(x)에 있는 Hyper-V 패스스루 디스크와 데이터베이스 백업은 지원되지 않습니다.

Windows 플러그인에 필요한 최소 **ONTAP** 권한

데이터 보호를 위해 사용하는 SnapCenter 플러그인에 따라 필요한 최소 ONTAP 권한은 다릅니다.

- 모든 액세스 명령: ONTAP 9.12.1 이상에 필요한 최소 권한
 - 이벤트 생성-자동 지원-로그
 - 작업 이력 표시
 - 작업 중지
 - 룬
 - lun 생성
 - lun 삭제
 - lun igroup 추가
 - lun igroup 생성
 - lun igroup 삭제
 - lun igroup 이름 바꾸기
 - 룬 아이그룹 쇼
 - lun 매핑 add-reporting-nodes
 - lun 매핑 생성
 - LUN 매핑 삭제
 - LUN 매핑 제거-보고-노드
 - lun 매핑 쇼
 - lun 수정
 - lun 이동량

- lun 오프라인
- lun 온라인
- lun 크기 조정
- lun 시리얼
- 런 쇼
- 스냅미러 정책 추가 규칙
- 스냅미러 정책 수정 규칙
- 스냅미러 정책 제거 규칙
- 스냅미러 정책 보기
- 스냅미러 복원
- 스냅미러 쇼
- 스냅미러 쇼 히스토리
- 스냅미러 업데이트
- 스냅미러 업데이트-ls-세트
- 스냅미러 목록-대상
- 버전
- 볼륨 복제 생성
- 볼륨 클론 쇼
- 볼륨 복제 분할 시작
- 볼륨 클론 분할 정지
- 볼륨 생성
- 볼륨 파괴
- 볼륨 파일 복제 생성
- 볼륨 파일 show-disk-usage
- 볼륨 오프라인
- 온라인 볼륨
- 볼륨 수정
- 볼륨 qtree 생성
- 볼륨 qtree 삭제
- 볼륨 qtree 수정
- 볼륨 qtree 쇼
- 볼륨 제한
- 볼륨 쇼
- 볼륨 스냅샷 생성

- 볼륨 스냅샷 삭제
- 볼륨 스냅샷 수정
- 볼륨 스냅샷 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- vservers cifs
- vservers cifs 공유 생성
- vservers cifs 공유 삭제
- vservers cifs 새도우 카피 쇼
- vservers cifs 공유 표시
- vservers cifs 쇼
- vservers 내보내기 정책
- vservers 내보내기 정책 생성
- vservers 내보내기 정책 삭제
- vservers 내보내기 정책 규칙 생성
- vservers 내보내기 정책 규칙 표시
- vservers 내보내기 정책 표시
- v서버 iSCSI
- vservers iscsi 연결 표시
- vservers 쇼
- 읽기 전용 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
 - 네트워크 인터페이스
 - 네트워크 인터페이스 표시
 - v서버

SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비

ONTAP SnapMirror 기술과 함께 SnapCenter 플러그인을 사용하면 다른 볼륨에 백업 세트의 미러 사본을 생성할 수 있으며, ONTAP SnapVault 기술과 함께 사용하면 표준 준수 및 기타 거버넌스 관련 목적으로 디스크 간 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 구성하고 해당 관계를 초기화해야 합니다.

SnapCenter 스냅샷 작업을 완료한 후 SnapMirror와 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행됩니다. SnapMirror 활성 동기화를 사용하는 경우 SnapMirror 활성 동기화와 비동기 관계 모두에 기본 SnapMirror 또는 SnapVault 일정을 사용하세요.



NetApp SnapManager 제품을 통해 SnapCenter 에 접속했고 구성된 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 기본 저장소(소스 볼륨)의 데이터를 보조 저장소(대상 볼륨)로 복제합니다. 관계를 초기화하면 ONTAP 소스 볼륨에서 참조되는 데이터 블록을 대상 볼륨으로 전송합니다.



SnapCenter SnapMirror 와 SnapVault 볼륨 간의 계단식 관계(**Primary > Mirror > Vault**)를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter 버전에 따라 유연한 SnapMirror 관계 관리를 지원합니다. 버전에 따라 유연한 SnapMirror 관계와 이를 설정하는 방법에 대한 자세한 내용은 다음을 참조하세요. "[ONTAP 문서](#)".

Windows 파일 시스템에 대한 백업 전략 정의

백업을 만들기 전에 백업 전략을 정의하면 파일 시스템을 성공적으로 복원하거나 복제하는 데 필요한 백업을 얻을 수 있습니다. 백업 전략은 주로 서비스 수준 계약(SLA), 복구 시간 목표(RTO), 복구 지점 목표(RPO)에 따라 결정됩니다.

SLA는 기대되는 서비스 수준을 정의하고 서비스의 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RTO는 서비스가 중단된 후 비즈니스 프로세스를 복구해야 하는 시간입니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 기간에 대한 전략을 정의합니다. SLA, RTO, RPO는 데이터 보호 전략에 기여합니다.

Windows 파일 시스템의 백업 일정

백업 빈도는 정책에 지정되고, 백업 일정은 리소스 그룹 구성에 지정됩니다. 백업 빈도나 일정을 결정하는 가장 중요한 요소는 리소스의 변화율과 데이터의 중요도입니다. 자주 사용되는 리소스는 매시간 백업하고, 거의 사용되지 않는 리소스는 하루에 한 번 백업할 수도 있습니다. 기타 요소로는 조직에 대한 리소스의 중요성, 서비스 수준 계약(SLA), 복구 지점 목표(RPO) 등이 있습니다.

SLA는 기대되는 서비스 수준을 정의하고 서비스 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 수명에 대한 전략을 정의합니다. SLA와 RPO는 데이터 보호 전략에 기여합니다.

많이 사용되는 리소스의 경우에도 하루에 한두 번 이상 전체 백업을 실행할 필요는 없습니다.

백업 일정은 다음과 같이 두 부분으로 구성됩니다.

- 백업 주파수

일부 플러그인의 경우 스케줄 유형 이라고 하는 백업 빈도(백업을 수행하는 빈도)는 정책 구성의 일부입니다. 예를 들어, 백업 빈도를 매시간, 매일, 매주 또는 매월로 구성하거나, 정책을 주문형 정책으로만 만드는 없음*을 지정할 수 있습니다. *설정 > *정책*을 클릭하면 정책에 액세스할 수 있습니다.

- 백업 일정

백업 일정(백업을 정확히 언제 수행해야 하는지)은 리소스 그룹 구성의 일부입니다. 예를 들어, 주간 백업에 대한 정책이 구성된 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 일정을 구성할 수 있습니다. 리소스 > *리소스 그룹*을 클릭하면 리소스 그룹 일정에 액세스할 수 있습니다.

Windows 파일 시스템에 필요한 백업 수

필요한 백업 수를 결정하는 요소에는 Windows 파일 시스템의 크기, 사용된 볼륨 수, 파일 시스템의 변경률, 서비스 수준 계약(SLA) 등이 있습니다.

Windows 파일 시스템의 백업 명명 규칙

Windows 파일 시스템 백업은 기본 스냅샷 명명 규칙을 사용합니다. 기본 백업 명명 규칙은 스냅샷 이름에 타임스탬프를 추가하여 복사본이 생성된 시기를 식별하는 데 도움이 됩니다.

스냅샷은 다음 기본 명명 규칙을 사용합니다: resourcegroupname_hostname_timestamp

다음 예와 같이 논리적으로 백업 리소스 그룹의 이름을 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예에서 구문 요소는 다음과 같은 의미를 갖습니다.

- `dts1` 리소스 그룹 이름입니다.
- `mach1x88` 호스트 이름입니다.
- `03-12-2016\_23.17.26` 날짜와 타임스탬프입니다.

백업을 생성할 때 백업을 식별하는 데 도움이 되는 설명 태그를 추가할 수도 있습니다. 반면, 사용자 지정 백업 명명 규칙을 사용하려면 백업 작업이 완료된 후 백업의 이름을 바꿔야 합니다.

백업 보존 옵션

백업 사본을 보관할 일수를 선택하거나 보관할 백업 사본 수를 지정할 수 있으며, ONTAP 최대 255개 사본까지 보관할 수 있습니다. 예를 들어, 귀하의 조직에서는 10일 분의 백업 사본이나 130개의 백업 사본을 보관하도록 요구할 수 있습니다.

정책을 생성하는 동안 백업 유형과 일정 유형에 대한 보존 옵션을 지정할 수 있습니다.

SnapMirror 복제를 설정하면 보존 정책이 대상 볼륨에 미러링됩니다.

SnapCenter 일정 유형과 일치하는 보존 레이블이 있는 보관된 백업을 삭제합니다. 리소스 또는 리소스 그룹의 일정 유형이 변경된 경우 이전 일정 유형 레이블이 지정된 백업이 시스템에 남아 있을 수 있습니다.



백업 사본을 장기간 보관하려면 SnapVault 백업을 사용해야 합니다.

Windows 파일 시스템용 복제본의 소스 및 대상

기본 저장소나 보조 저장소에서 파일 시스템 백업을 복제할 수 있습니다. 요구 사항에 맞는 대상을 선택할 수도 있습니다. 원래 백업 위치이거나 같은 호스트나 다른 호스트의 다른 대상일 수 있습니다. 대상은 복제본 소스 백업과 동일한 볼륨에 있어야 합니다.

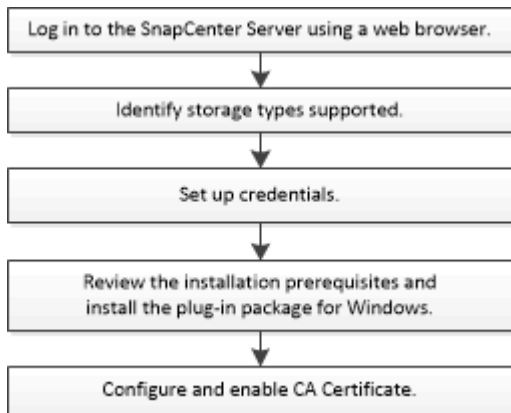
복제 대상	설명
원본, 출처, 위치	기본적으로 SnapCenter 복제본을 복제되는 백업과 동일한 위치와 호스트에 저장합니다.
다른 위치	복제본을 동일한 호스트의 다른 위치나 다른 호스트에 저장할 수 있습니다. 호스트에는 스토리지 가상 머신(SVM)에 대한 구성된 연결이 있어야 합니다.

복제 작업이 완료된 후 복제본의 이름을 바꿀 수 있습니다.

Microsoft Windows용 SnapCenter 플러그인 설치

Microsoft Windows용 SnapCenter 플러그인 설치 워크플로

데이터베이스 파일이 아닌 Windows 파일을 보호하려면 Microsoft Windows용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



Microsoft Windows용 SnapCenter 플러그인 설치 요구 사항

Windows용 플러그인을 설치하기 전에 특정 설치 요구 사항을 알아야 합니다.

Windows용 플러그인을 사용하기 전에 SnapCenter 관리자는 SnapCenter 서버를 설치하고 구성하고 필수 작업을 수행해야 합니다.

- Windows용 플러그인을 설치하려면 SnapCenter 관리자 권한이 있어야 합니다.
SnapCenter 관리자 역할에는 관리자 권한이 있어야 합니다.
- SnapCenter 서버를 설치하고 구성해야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.
- 백업 복제를 원하시면 SnapMirror와 SnapVault 설정해야 합니다.

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항과 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	마이크로소프트 윈도우 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" . Windows 클러스터 설정을 사용하는 경우 Windows 원격 관리(WinRM)도 설치하고 구성해야 합니다.
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	• ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 • 파워셸 코어 7.4.2 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .

Windows용 플러그인에 대한 자격 증명을 설정하세요

SnapCenter 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다. SnapCenter 플러그인을 설치하기 위한 자격 증명과 Windows 파일 시스템에서 데이터 보호 작업을 수행하기 위한 추가 자격 증명을 만들어야 합니다.

필요한 것

- 플러그인을 설치하기 전에 Windows 자격 증명을 설정해야 합니다.
- 원격 호스트에서 관리자 권한을 포함한 관리자 권한이 있는 자격 증명을 설정해야 합니다.
- 개별 리소스 그룹에 대한 자격 증명을 설정하고 사용자에게 전체 관리자 권한이 없는 경우 최소한 리소스 그룹 및 백업 권한을 사용자에게 할당해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.

2. 설정 페이지에서 *자격 증명*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 자격 증명 페이지에서 다음을 수행합니다.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.
사용자 이름/비밀번호	인증에 사용되는 사용자 이름과 비밀번호를 입력하세요. • 도메인 관리자 또는 관리자 그룹의 모든 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹 구성원을 지정하십시오. 사용자 이름 필드에 사용할 수 있는 형식은 다음과 같습니다. ◦ NetBIOS\UserName ◦ Domain FQDN\UserName ◦ UserName@upn • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우, SnapCenter 플러그인을 설치할 시스템에 기본 제공되는 로컬 관리자를 지정하십시오. 사용자 계정에 승격된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우, 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다. UserName 비밀번호에 큰따옴표(")나 백틱(`)을 사용하지 마세요. 비밀번호에 '<' 기호와 '!)' 기호를 함께 사용하면 안 됩니다. 예를 들어, lessthan<!10, lessthan10<!, backtick`12.
비밀번호	인증에 사용되는 비밀번호를 입력하세요.

5. *확인*을 클릭합니다.

자격 증명 설정을 마친 후 사용자 및 액세스 페이지에서 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

Windows Server 2016 이상에서 gMSA 구성

Windows Server 2016 이상에서는 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 관리 서비스 계정(gMSA)을 만들 수 있습니다.

시작하기 전에

- Windows Server 2016 이상 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2016 이상 호스트가 있어야 합니다.

단계

1. gMSA의 각 개체에 대해 고유한 비밀번호를 생성하려면 KDS 루트 키를 만듭니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 다음 명령을 실행합니다. Add-KDSRootKey -EffectiveImmediately
3. gMSA를 만들고 구성하세요.
 - a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
domainName\accountName$  
.. 그룹에 컴퓨터 객체를 추가합니다.  
.. 방금 만든 사용자 그룹을 사용하여 gMSA를 만듭니다.
```

예를 들어,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 달리다 `Get-ADServiceAccount` 서비스 계정을 확인하는 명령입니다.
```

4. 호스트에서 gMSA를 구성하세요.
 - a. gMSA 계정을 사용하려는 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.

이렇게 하려면 PowerShell에서 다음 명령을 실행하세요.


```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

a. 호스트를 다시 시작합니다.

b. PowerShell 명령 프롬프트에서 다음 명령을 실행하여 호스트에 gMSA를 설치합니다. `Install-AdServiceAccount <gMSA>`

c. 다음 명령을 실행하여 gMSA 계정을 확인하세요. `Test-AdServiceAccount <gMSA>`

5. 호스트에서 구성된 gMSA에 관리 권한을 할당합니다.

6. SnapCenter 서버에서 구성된 gMSA 계정을 지정하여 Windows 호스트를 추가합니다.

SnapCenter Server는 호스트에 선택된 플러그인을 설치하고, 플러그인 설치 중에 지정된 gMSA가 서비스 로그인 계정으로 사용됩니다.

호스트를 추가하고 **Microsoft Windows용 SnapCenter** 플러그인을 설치합니다.

SnapCenter 호스트 추가 페이지를 사용하여 Windows 호스트를 추가할 수 있습니다. Microsoft Windows용 SnapCenter 플러그인은 지정된 호스트에 자동으로 설치됩니다. 플러그인을 설치하는 데 권장되는 방법입니다. 개별 호스트나 클러스터에 호스트를 추가하고 플러그인을 설치할 수 있습니다.

시작하기 전에

- SnapCenter 서버 호스트의 운영 체제가 Windows 2019이고 플러그인 호스트의 운영 체제가 Windows 2022인 경우 다음을 수행해야 합니다.
 - Windows Server 2019(OS 빌드 17763.5936) 이상으로 업그레이드하세요.
 - Windows Server 2022(OS 빌드 20348.2402) 이상으로 업그레이드하세요.
- SnapCenter 관리자 역할과 같이 플러그인 설치 및 제거 권한이 있는 역할에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.

- SnapCenter 사용자는 Windows Server의 "서비스로 로그인" 역할에 추가되어야 합니다.
- 메시지 큐잉 서비스가 실행 상태인지 확인해야 합니다.
- 그룹 관리 서비스 계정(gMSA)을 사용하는 경우 관리자 권한으로 gMSA를 구성해야 합니다.

"Windows 파일 시스템에 대한 Windows Server 2016 이상에서 그룹 관리 서비스 계정 구성"

이 작업에 관하여

- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.
- Windows 플러그인
 - 마이크로소프트 윈도우
 - 마이크로소프트 익스체인지 서버
 - 마이크로소프트 SQL 서버
 - SAP 하나
- 클러스터에 플러그인 설치

클러스터(WSFC, Oracle RAC 또는 Exchange DAG)에 플러그인을 설치하면 해당 플러그인은 클러스터의 모든 노드에 설치됩니다.

- E-시리즈 스토리지

E-시리즈 스토리지에 연결된 Windows 호스트에는 Windows용 플러그인을 설치할 수 없습니다.



호스트가 이미 작업 그룹의 일부이고 다른 도메인으로 변경되었거나 그 반대의 경우, SnapCenter 동일한 호스트(플러그인 호스트)를 SnapCenter 에 추가하는 것을 지원하지 않습니다. 동일한 호스트를 추가하려면 SnapCenter 에서 호스트를 제거한 다음 다시 추가해야 합니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 맨 위에 *관리되는 호스트*가 선택되어 있는지 확인하세요.
3. *추가*를 클릭하세요.
4. 호스트 페이지에서 다음을 수행합니다.

이 분야에서는...	이렇게 하세요...
호스트 유형	호스트의 Windows 유형을 선택하세요. SnapCenter Server는 호스트를 추가한 다음, 호스트에 Windows용 플러그인이 아직 설치되어 있지 않으면 해당 플러그인을 설치합니다.

이 분야에서는...	이렇게 하세요...
호스트 이름	호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하세요. SnapCenter DNS의 적절한 구성에 달려 있습니다. 따라서 가장 좋은 방법은 정규화된 도메인 이름(FQDN)을 입력하는 것입니다. 다음 중 하나의 IP 주소나 FQDN을 입력할 수 있습니다. • 독립형 호스트 • Windows Server 장애 조치(Failover) 클러스터링(WSFC) SnapCenter 사용하여 호스트를 추가하고 해당 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.
신임장	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성하세요. 자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하세요. 사용자 이름, 도메인, 호스트 유형을 포함한 자격 증명에 대한 세부 정보를 보려면 해당 자격 증명 이름 위에 커서를 올려놓으세요.  인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

새로운 배포의 경우 플러그인 패키지가 나열되지 않습니다.

6. (선택 사항) *추가 옵션*을 클릭합니다.

이 분야에서는...	이렇게 하세요...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정하세요. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트로 표시됩니다.  플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.
설치 경로	기본 경로는 C:\Program Files\NetApp\SnapCenter입니다. 선택적으로 경로를 사용자 정의할 수 있습니다. Windows용 SnapCenter 플러그인 패키지의 경우 기본 경로는 C:\Program Files\NetApp\SnapCenter입니다. 하지만 원하는 경우 기본 경로를 사용자 지정할 수 있습니다.
클러스터의 모든 호스트를 추가합니다.	WSFC의 모든 클러스터 노드를 추가하려면 이 확인란을 선택합니다.
사전 설치 확인 건너뛰기	플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택하세요.
플러그인 서비스를 실행하려면 그룹 관리 서비스 계정(gMSA)을 사용하세요.	플러그인 서비스를 실행하기 위해 그룹 관리 서비스 계정(gMSA)을 사용하려면 이 확인란을 선택하세요. 다음 형식으로 gMSA 이름을 제공하세요: <i>domainName\accountName\$</i>.  gMSA는 Windows용 SnapCenter 플러그인 서비스에 대한 로그인 서비스 계정으로만 사용됩니다.

7. *제출*을 클릭하세요.

사전 검사 건너뛰기 확인란을 선택하지 않은 경우, 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 유효성 검사가 수행됩니다. 디스크 공간, RAM, PowerShell 버전, .NET 버전 및 위치는 최소 요구 사항을 기준으로 유효성 검사됩니다. 최소 요구 사항을 충족하지 못하면 해당 오류 또는 경고 메시지가 표시됩니다.

오류가 디스크 공간이나 RAM과 관련된 경우 다음 위치에 있는 web.config 파일을 업데이트할 수 있습니다. C:\Program Files\NetApp\SnapCenter 기본값을 수정하는 WebApp입니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.



HA 설정에서 web.config 파일을 업데이트하는 경우 두 노드에서 모두 파일을 업데이트해야 합니다.

8. 설치 진행 상황을 모니터링합니다.

PowerShell cmdlet을 사용하여 여러 원격 호스트에 Microsoft Windows용 SnapCenter 플러그인 설치

한 번에 여러 호스트에 Microsoft Windows용 SnapCenter 플러그인을 설치하려면 다음을 사용할 수 있습니다. `Install-SmHostPackage PowerShell cmdlet`.

플러그인을 설치하려는 각 호스트에서 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter 에 로그인해야 합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 다음을 사용하여 세션을 설정합니다. `Open-SmConnection cmdlet`을 입력한 다음 자격 증명을 입력합니다.
3. SnapCenter 사용하여 독립 실행형 호스트 또는 클러스터를 추가합니다. `Add-SmHost cmdlet`과 필요한 매개변수.

`cmdlet`과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

4. 다음을 사용하여 여러 호스트에 플러그인을 설치합니다. `Install-SmHostPackage cmdlet`과 필요한 매개변수.

당신은 사용할 수 있습니다 `-skipprecheck` 플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려는 경우의 옵션입니다.

명령줄에서 **Microsoft Windows용 SnapCenter** 플러그인을 자동으로 설치합니다.

SnapCenter GUI에서 원격으로 플러그인을 설치할 수 없는 경우 Windows 호스트에 로컬로 Microsoft Windows용 SnapCenter 플러그인을 설치할 수 있습니다. Windows 명령줄에서 SnapCenter 플러그인을 Microsoft Windows 설치 프로그램으로 자동 모드로 실행할 수 있습니다.

시작하기 전에

- ASP.NET Core Runtime 8.0.12(및 이후의 모든 8.0.x 패치) 호스팅 번들을 설치해야 합니다.
- PowerShell 7.4.2 이상을 설치해야 합니다.
- 호스트의 로컬 관리자여야 합니다.

단계

1. 설치 위치에서 Microsoft Windows용 SnapCenter 플러그인을 다운로드하세요.

예를 들어, 기본 설치 경로는 `C:\ProgramData\NetApp\ SnapCenter\Package Repository`입니다.

이 경로는 SnapCenter 서버가 설치된 호스트에서 접근할 수 있습니다.

2. 플러그인을 설치하려는 호스트에 설치 파일을 복사합니다.

3. 명령 프롬프트에서 설치 파일을 다운로드한 디렉토리로 이동합니다.

4. 다음 명령을 입력하고 변수를 사용자의 데이터로 바꾸세요.

```
"snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""  
BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=  
ISFeatureInstall=SCW
```

예를 들어:

```
`"C:\ProgramData\NetApp\SnapCenter\Package Repository  
\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:  
\HPPW_SCW_Install.log" /log"C:\\" BI_SNAPCENTER_PORT=8145  
SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW`
```



Windows용 플러그인을 설치하는 동안 전달되는 모든 매개변수는 대소문자를 구분합니다.

다음 변수의 값을 입력하세요.

변하기 쉬운	가치
/debuglog"<디버그_로그_경로>	다음 예와 같이 제품군 설치 프로그램 로그 파일의 이름과 위치를 지정합니다: Setup.exe /debuglog"C:\PathToLog\setupexe.log".
BI_SNAPCENTER_PORT	SnapCenter SMCore와 통신하는 포트를 지정합니다.
SUITE_INSTALLDIR	호스트 플러그인 패키지 설치 디렉토리를 지정합니다.
BI_SERVICEACCOUNT	Microsoft Windows 웹 서비스 계정에 대한 SnapCenter 플러그인을 지정합니다.
BI_SERVICEPWD	Microsoft Windows 웹 서비스 계정용 SnapCenter 플러그인의 비밀번호를 지정합니다.
ISFeature설치	SnapCenter 가 원격 호스트에 배포할 솔루션을 지정합니다.

debuglog 매개변수에는 SnapCenter 의 로그 파일 경로가 포함됩니다. 이 로그 파일에 쓰는 것은 문제 해결 정보를 얻는 가장 좋은 방법입니다. 이 파일에는 설치 과정에서 플러그인 필수 구성 요소를 확인하기 위해 수행한 검사 결과가 들어 있기 때문입니다.

필요한 경우 Windows 패키지용 SnapCenter 의 로그 파일에서 추가적인 문제 해결 정보를 찾을 수 있습니다. 패키지의 로그 파일은 %Temp% 폴더(예: C:\temp\)\에 가장 오래된 파일부터 나열됩니다.



Windows용 플러그인을 설치하면 플러그인이 SnapCenter 서버가 아닌 호스트에 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록할 수 있습니다. 호스트가 추가되면 플러그인이 자동으로 검색됩니다.

SnapCenter 플러그인 패키지 설치 상태 모니터링

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행 상황을 모니터링할 수 있습니다. 설치가 완료되었는지 또는 문제가 있는지 확인하기 위해 설치 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

- 진행 중
- 성공적으로 완료되었습니다
- 실패한
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
- 대기 중

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 플러그인 설치 작업만 나열되도록 목록을 필터링하려면 다음을 수행합니다.
 - a. *필터*를 클릭하세요.
 - b. 선택 사항: 시작 날짜와 종료 날짜를 지정합니다.
 - c. 유형 드롭다운 메뉴에서 *플러그인 설치*를 선택합니다.
 - d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
 - e. *적용*을 클릭하세요.
4. 설치 작업을 선택하고 *세부정보*를 클릭하면 작업 세부정보를 볼 수 있습니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

CA 인증서 구성

CA 인증서 CSR 파일 생성

인증서 서명 요청(CSR)을 생성하고, 생성된 CSR을 사용하여 인증 기관(CA)에서 얻을 수 있는 인증서를 가져올 수 있습니다. 인증서에는 개인 키가 연결됩니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.



CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 정보는 다음을 참조하세요. "[CA 인증서 CSR 파일을 생성하는 방법](#)".



도메인(*.domain.company.com)이나 시스템(machine1.domain.company.com)에 대한 CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN)과 해당 호스트 이름을 CA 인증서에 명시해야 합니다. 인증서를 구매하기 전에 주체 대체 이름(SAN) 필드를 입력하여 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(*.domain.company.com)의 경우 인증서에는 해당 도메인의 모든 호스트 이름이 암묵적으로 포함됩니다.

CA 인증서 가져오기

Microsoft 관리 콘솔(MMC)을 사용하여 CA 인증서를 SnapCenter 서버와 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.
2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
3. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > *인증서*를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 버튼으로 클릭한 다음, 모든 작업 > *가져오기*를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
개인 키 가져오기	예 옵션을 선택하고 개인 키를 가져온 후 *다음*을 클릭합니다.
가져오기 파일 형식	변경하지 마세요. *다음*을 클릭하세요.
보안	내보낸 인증서에 사용할 새 비밀번호를 지정한 후 *다음*을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.



인증서 가져오기는 개인 키와 함께 제공되어야 합니다(지원되는 형식: *.pfx, *.p12, *.p7b).

7. "개인" 폴더에 대해서도 5단계를 반복합니다.

CA 인증서 지문을 받으세요

인증서 지문은 인증서를 식별하는 16진수 문자열입니다. 지문은 지문 알고리즘을 사용하여 인증서 내용으로부터 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.

- 인증서를 두 번 클릭합니다.
- 인증서 대화 상자에서 세부정보 탭을 클릭합니다.
- 필드 목록을 스크롤하여 *지문*을 클릭하세요.
- 상자에서 16진수 문자를 복사하세요.
- 16진수 사이의 공백을 제거하세요.

예를 들어, 지문이 "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b"인 경우 공백을 제거하면 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.

- 다음 명령을 실행하여 설치된 인증서의 지문을 나열하고 주체 이름으로 최근에 설치된 인증서를 식별합니다.

```
Get-Childitem -경로 인증서:\LocalMachine\My
```

- 지문을 복사하세요.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스로 CA 인증서를 구성해야 합니다.

SnapCenter 서버와 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCORE 기본 포트 8145를 사용하는 기존 인증서 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

예를 들어:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스에 바인딩합니다.
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

예를 들어:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

플러그인에 대한 CA 인증서 활성화

CA 인증서를 구성하고 SnapCenter 서버와 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- `Set-SmCertificateSettings` cmdlet을 실행하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- `_Get-SmCertificateSettings_`를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 하나 또는 여러 개의 플러그인 호스트를 선택하세요.
4. *추가 옵션*을 클릭하세요.
5. *인증서 검증 사용*을 선택합니다.

당신이 완료한 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- *  *는 CA 인증서가 활성화되지 않았거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- *  *는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- *  *는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- *  *는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

SnapCenter Plug-in for VMware vSphere 설치

데이터베이스나 파일 시스템이 가상 머신(VM)에 저장되어 있거나 VM과 데이터 저장소를 보호하려는 경우 SnapCenter Plug-in for VMware vSphere 배포해야 합니다.

배포에 대한 정보는 다음을 참조하세요. ["배포 개요"](#).

CA 인증서 배포

SnapCenter Plug-in for VMware vSphere 사용하여 CA 인증서를 구성하려면 다음을 참조하세요. ["SSL 인증서 생성 또는 가져오기"](#).

CRL 파일 구성

SnapCenter Plug-in for VMware vSphere 미리 구성된 디렉토리에서 CRL 파일을 찾습니다. SnapCenter Plug-in for VMware vSphere 의 CRL 파일의 기본 디렉토리는 `_/opt/netapp/config/crl_`입니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

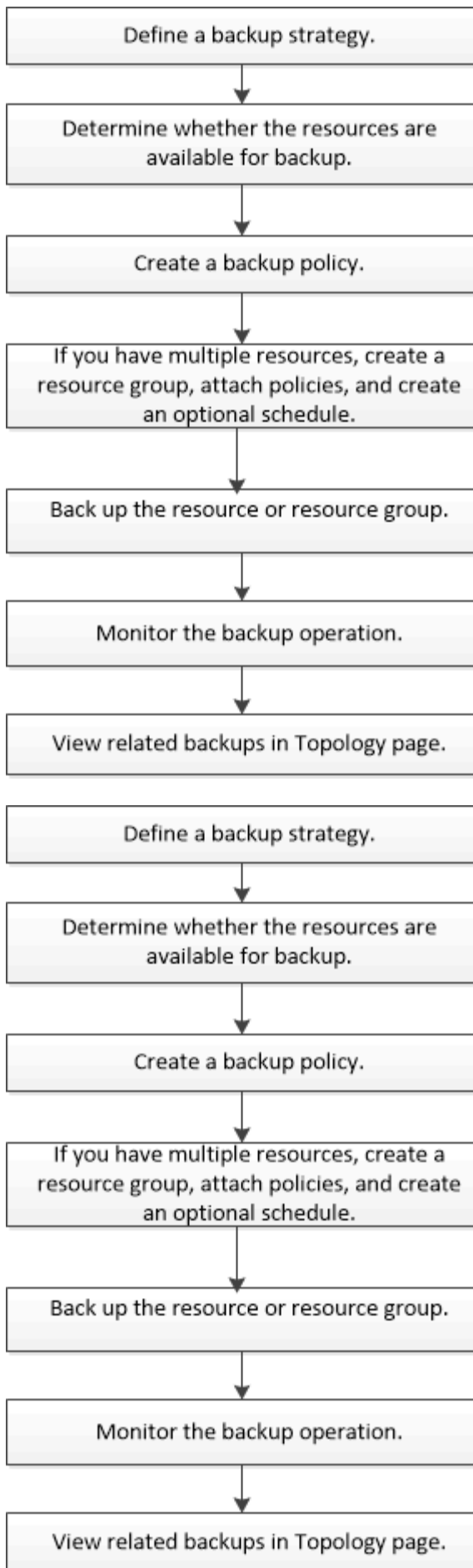
Windows 파일 시스템 백업

Windows 파일 시스템 백업

사용자 환경에 Microsoft Windows용 SnapCenter 플러그인을 설치하면 SnapCenter 사용하여 Windows 파일 시스템을 백업할 수 있습니다. 단일 파일 시스템이나 여러 파일 시스템이 포함된 리소스 그룹을 백업할 수 있습니다. 필요에 따라 또는 정의된 보호 일정에 따라 백업할 수 있습니다.

여러 서버에서 동시에 실행되도록 여러 백업을 예약할 수 있습니다. 동일한 리소스에서 백업 및 복원 작업을 동시에 수행할 수 없습니다.

다음 워크플로는 백업 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말 또는 "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)" PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

Windows 파일 시스템의 리소스 가용성 확인

리소스는 설치한 플러그인에 의해 유지 관리되는 파일 시스템의 LUN 및 유사한 구성 요소입니다. 여러 리소스에 대한 데이터 보호 작업을 수행할 수 있도록 해당 리소스를 리소스 그룹에 추가할 수 있지만, 먼저 사용 가능한 리소스를 파악해야 합니다. 사용 가능한 리소스를 검색하면 플러그인 설치가 성공적으로 완료되었는지 확인할 수도 있습니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 가상 머신(SVM) 연결 생성, 자격 증명 추가 등의 작업을 이미 완료했어야 합니다.
- 파일이 VMware RDM LUN이나 VMDK에 있는 경우 SnapCenter Plug-in for VMware vSphere 배포하고 SnapCenter에 플러그인을 등록해야 합니다. 자세한 내용은 다음을 참조하세요. "[SnapCenter Plug-in for VMware vSphere 설명서](#)".

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 목록에서 *파일 시스템*을 선택합니다.
3. 리소스 목록을 필터링할 호스트를 선택한 다음 *리소스 새로 고침*을 클릭합니다.

새로 추가되거나 이름이 변경되거나 삭제된 파일 시스템은 SnapCenter 서버 인벤토리에 업데이트됩니다.



SnapCenter 외부에서 데이터베이스 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

Windows 파일 시스템에 대한 백업 정책 만들기

SnapCenter 사용하여 Windows 파일 시스템을 백업하기 전에 리소스에 대한 새 백업 정책을 만들거나, 리소스 그룹을 만들거나 리소스를 백업할 때 새 백업 정책을 만들 수 있습니다.

시작하기 전에

- 백업 전략을 정의했어야 합니다. "[자세히 알아보기](#)"
- 데이터 보호를 위해 준비를 하셔야 합니다.

데이터 보호를 준비하려면 SnapCenter 설치, 호스트 추가, 리소스 검색, 스토리지 가상 머신(SVM) 연결 생성 등의 작업을 완료해야 합니다.

- 스냅샷을 미리 또는 볼트 보조 스토리지에 복제하는 경우 SnapCenter 관리자가 소스 및 대상 볼륨 모두에 대한 SVM을 할당해야 합니다.
- PowerShell 스크립트를 prescripts 및 postscripts로 실행하려면 web.config 파일에서 usePowershellProcessforScripts 매개변수 값을 true로 설정해야 합니다.

기본값은 false입니다

- SnapMirror Active Sync의 특정 전제 조건과 제한 사항을 검토하세요. 자세한 내용은 다음을 참조하세요.
["SnapMirror Active Sync에 대한 개체 제한"](#) .

이 작업에 관하여

- SCRIPTS_PATH는 플러그인 호스트의 SMCoreServiceHost.exe.Config 파일에 있는 PredefinedWindowsScriptsDirectory 키를 사용하여 정의됩니다.

필요한 경우 이 경로를 변경하고 SMcore 서비스를 다시 시작할 수 있습니다. 보안을 위해 기본 경로를 사용하는 것이 좋습니다.

키 값은 API를 통해 swagger에서 표시될 수 있습니다: API /4.7/configsettings

GET API를 사용하여 키 값을 표시할 수 있습니다. SET API는 지원되지 않습니다.

- SnapLock
 - '특정 기간 동안 백업 사본을 보관합니다' 옵션을 선택한 경우 SnapLock 보관 기간은 언급된 보관 기간보다 짧거나 같아야 합니다.
 - 스냅샷 잠금 기간을 지정하면 보존 기간이 만료될 때까지 스냅샷이 삭제되지 않습니다. 이를 통해 정책에 지정된 수보다 더 많은 수의 스냅샷을 보존할 수 있습니다.
 - ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 선택합니다.
2. 설정 페이지에서 *정책*을 선택합니다.
3. *새로 만들기*를 선택하세요.
4. 이름 페이지에서 정책 이름과 세부 정보를 입력합니다.
5. 백업 및 복제 페이지에서 다음 작업을 수행합니다.
 - a. 백업 설정을 선택하세요.

옵션	설명
파일 시스템 일관성 백업	백업 작업이 시작되기 전에 SnapCenter 파일 시스템이 있는 디스크 드라이브를 정지시키고 백업 작업이 끝난 후 디스크 드라이브를 다시 시작하도록 하려면 이 옵션을 선택합니다.
파일 시스템 충돌 시에도 일관된 백업	SnapCenter 파일 시스템이 있는 디스크 드라이브를 정지시키지 않도록 하려면 이 옵션을 선택하세요.

- b. 일정 빈도(정책 유형이라고도 함)를 선택합니다.

정책은 백업 빈도만 지정합니다. 백업을 위한 구체적인 보호 일정은 리소스 그룹에서 정의됩니다. 따라서 두 개 이상의 리소스 그룹이 동일한 정책과 백업 빈도를 공유할 수 있지만 백업 일정은 서로 다를 수 있습니다.



오전 2시로 예약한 경우, 일광 절약 시간제(DST) 기간에는 일정이 실행되지 않습니다.

c. 정책 라벨을 선택하세요.

선택한 스냅샷 레이블에 따라 ONTAP 레이블과 일치하는 보조 스냅샷 보존 정책을 적용합니다.



로컬 스냅샷 복사본을 만든 후 SnapMirror 업데이트를 선택한 경우 선택적으로 보조 정책 레이블을 지정할 수 있습니다. 하지만 로컬 스냅샷 복사본을 만든 후 SnapVault 업데이트를 선택한 경우 보조 정책 레이블을 지정해야 합니다.

6. 보조 복제 옵션 선택 섹션에서 다음 보조 복제 옵션 중 하나 또는 둘 다를 선택합니다.

이 분야에서는...	이렇게 하세요...
로컬 스냅샷 복사본을 만든 후 SnapMirror 업데이트	다른 볼륨에 백업 세트의 미리 복사본을 생성하려면 이 옵션을 선택하세요(SnapMirror). SnapSnapMirror Active Sync에서는 이 옵션을 활성화해야 합니다. 2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고쳐집니다. 보다 "토폴로지 페이지에서 관련 백업 및 복제본 보기".
스냅샷 복사본을 만든 후 SnapVault 업데이트	디스크 간 백업 복제를 수행하려면 이 옵션을 선택하세요. 2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고쳐집니다. ONTAP 에서 SnapLock Vault로 알려진 보조 노드에만 SnapLock 구성된 경우 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 보조 노드의 잠금 기간이 새로 고쳐집니다. SnapLock Vault에 대한 자세한 내용은 다음을 참조하세요. "볼트 대상의 WORM에 스냅샷 복사본 커밋"
오류 재시도 횟수	프로세스가 중단되기 전에 발생해야 하는 복제 시도 횟수를 입력합니다.



보조 저장소의 스냅샷 최대 한도에 도달하지 않도록 하려면 ONTAP 에서 보조 저장소 SnapMirror 보존 정책을 구성해야 합니다.

7. 보존 설정 페이지에서 주문형 백업과 선택한 각 일정 빈도에 대한 보존 설정을 지정합니다.

옵션	설명
보관할 총 스냅샷 사본	SnapCenter 가 자동으로 삭제하기 전에 저장하는 스냅샷 수를 지정하려면 이 옵션을 선택하세요.
스냅샷 사본을 보관하세요	SnapCenter 백업 사본을 삭제하기 전에 보관하는 일수를 지정하려면 이 옵션을 선택하세요.
스냅샷 복사 잠금 기간	스냅샷 잠금 기간을 선택하고 기간을 일, 월 또는 년으로 지정합니다. SnapLock 보존 기간은 100년 미만이어야 합니다.



보존 횟수를 2 이상으로 설정해야 합니다. 보존 횟수의 최소값은 2입니다.



최대 보존 값은 1018입니다. 보존 기간이 ONTAP 버전에서 지원하는 것보다 높은 값으로 설정된 경우 백업이 실패합니다.

8. 스크립트 페이지에서 SnapCenter 서버가 백업 작업 전이나 후에 실행할 프리스크립트 또는 포스트스크립트의 경로와 SnapCenter 스크립트가 실행될 때까지 기다리는 시간 제한을 입력합니다.

예를 들어, SNMP 트랩을 업데이트하고, 알림을 자동화하고, 로그를 보내는 스크립트를 실행할 수 있습니다.



prescripts 또는 postscripts 경로에는 드라이브나 공유가 포함되어서는 안 됩니다. 경로는 SCRIPTS_PATH를 기준으로 해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

Windows 파일 시스템에 대한 리소스 그룹 만들기

리소스 그룹은 보호하려는 여러 파일 시스템을 추가할 수 있는 컨테이너입니다. 또한 리소스 그룹에 하나 이상의 정책을 연결하여 수행하려는 데이터 보호 작업 유형을 정의한 다음 백업 일정을 지정해야 합니다.

이 작업에 관하여

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.
- SnapMirror 활성 동기화가 있는 리소스가 포함된 기존 리소스 그룹에 SnapMirror 활성 동기화가 없는 새 파일 시스템을 추가하는 것은 지원되지 않습니다.
- SnapMirror Active Sync의 장애 조치 모드에서 기존 리소스 그룹에 새 파일 시스템을 추가하는 것은 지원되지 않습니다. 일반 상태나 장애 복구 상태에서만 리소스 그룹에 리소스를 추가할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.

2. 리소스 페이지에서 목록에서 *파일 시스템*을 선택합니다.



최근 SnapCenter 에 파일 시스템을 추가한 경우 *리소스 새로 고침*을 클릭하여 새로 추가된 리소스를 확인하세요.

3. *새 리소스 그룹*을 클릭합니다.

4. 마법사의 이름 페이지에서 다음을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	리소스 그룹 이름을 입력하세요. 리소스 그룹 이름은 250자를 넘을 수 없습니다.
스냅샷 복사에 사용자 정의 이름 형식 사용	선택 사항: 사용자 지정 스냅샷 이름과 형식을 입력합니다. 예를 들어, customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.
꼬리표	리소스 그룹을 찾는 데 도움이 되는 설명 태그를 입력하세요.

5. 리소스 페이지에서 다음 작업을 수행합니다.

a. 리소스 목록을 필터링하려면 호스트를 선택하세요.

최근에 리소스를 추가한 경우 리소스 목록을 새로 고친 후에만 사용 가능한 리소스 목록에 표시됩니다.

b. 사용 가능한 리소스 섹션에서 백업하려는 파일 시스템을 클릭한 다음 오른쪽 화살표를 클릭하여 해당 파일을 추가된 섹션으로 이동합니다.

동일한 저장소 볼륨에 있는 모든 리소스 자동 선택 옵션을 선택하면 동일한 볼륨에 있는 모든 리소스가 선택됩니다. 볼륨을 추가된 섹션으로 이동하면 해당 볼륨의 모든 리소스가 함께 이동됩니다.

단일 파일 시스템을 추가하려면 동일한 저장소 볼륨의 모든 리소스 자동 선택 옵션을 선택 취소한 다음, 추가된 섹션으로 이동할 파일 시스템을 선택합니다.

6. 정책 페이지에서 다음 작업을 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.

기존 정책을 선택하고 *세부정보*를 클릭하면 해당 정책을 사용할 수 있는지 확인할 수 있습니다.

기존 정책이 귀하의 요구 사항을 충족하지 않는 경우 *를 클릭하여 새 정책을 만들 수 있습니다. * 정책 마법사를 시작합니다.

선택한 정책은 '선택한 정책에 대한 일정 구성' 섹션의 '정책' 열에 나열됩니다.

- b. 선택한 정책에 대한 일정 구성 섹션에서 *를 클릭합니다.  * 일정을 구성하려는 정책에 대한 일정 구성 열에 있습니다.
- c. 정책이 여러 일정 유형(빈도)과 연결되어 있는 경우 구성하려는 빈도를 선택합니다.
- d. 정책_정책_이름_에 대한 일정 추가 대화 상자에서 시작 날짜, 만료 날짜, 빈도를 지정하여 일정을 구성한 다음 *마침*을 클릭합니다.

구성된 일정은 '선택한 정책에 대한 일정 구성' 섹션의 '적용된 일정' 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다. Windows 작업 스케줄러와 SQL Server 에이전트의 일정을 수정해서는 안 됩니다.

7. 알림 페이지에서 다음과 같이 알림 정보를 제공합니다.

이 분야에서는...	이렇게 하세요...
이메일 환경 설정	백업 리소스 그룹을 만들고, 정책을 첨부하고, 일정을 구성한 후 수신자에게 이메일을 보내려면 항상, 실패 시, *실패 또는 경고 시*를 선택합니다. SMTP 서버, 기본 이메일 제목줄, 받는 사람 및 보낸 사람 이메일 주소를 입력하세요.
에서	이메일 주소
에게	이메일 주소로
주제	기본 이메일 제목줄

8. 요약을 검토한 후 *마침*을 클릭하세요.

필요에 따라 백업을 수행하거나 예약된 백업이 수행될 때까지 기다릴 수 있습니다.

ASA r2 시스템에서 Windows 파일 시스템에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.

ASA r2 시스템에 있는 리소스를 추가하려면 리소스 그룹을 만들어야 합니다. 리소스 그룹을 생성하는 동안 보조 보호를 프로비저닝할 수도 있습니다.

시작하기 전에

- ONTAP 9.x 리소스와 ASA r2 리소스를 동일한 리소스 그룹에 추가하지 않도록 해야 합니다.
- ONTAP 9.x 리소스와 ASA r2 리소스가 모두 포함된 데이터베이스가 없는지 확인해야 합니다.

이 작업에 관하여

- 2차 보호는 로그인한 사용자에게 **SecondaryProtection** 기능이 활성화된 역할이 할당된 경우에만 사용할 수 있습니다.

- 2차 보호를 활성화한 경우 기본 및 2차 일관성 그룹을 생성하는 동안 리소스 그룹은 유지 관리 모드로 전환됩니다. 기본 및 보조 일관성 그룹이 생성된 후 리소스 그룹은 유지 관리 모드에서 해제됩니다.
- SnapCenter 클론 리소스에 대한 보조 보호를 지원하지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.
 - a. 이름 필드에 리소스 그룹의 이름을 입력합니다.



리소스 그룹 이름은 250자를 넘을 수 없습니다.

- b. 나중에 리소스 그룹을 검색하는 데 도움이 되도록 태그 필드에 하나 이상의 레이블을 입력하세요.

예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.

- c. 이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_resource_group_policy_hostname 또는 resource_group_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

- d. 백업하지 않을 보관 로그 파일의 대상을 지정합니다.



필요한 경우 접두사를 포함하여 애플리케이션에 설정된 것과 정확히 동일한 목적지를 사용해야 합니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 데이터베이스 호스트 이름을 선택합니다.



리소스가 성공적으로 검색된 경우에만 해당 리소스가 사용 가능한 리소스 섹션에 나열됩니다. 최근에 리소스를 추가한 경우 리소스 목록을 새로 고친 후에만 사용 가능한 리소스 목록에 표시됩니다.

5. 사용 가능한 리소스 섹션에서 ASA r2 리소스를 선택하고 선택한 리소스 섹션으로 이동합니다.
6. 애플리케이션 설정 페이지에서 백업 옵션을 선택하세요.
7. 정책 페이지에서 다음 단계를 수행합니다.
 - a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



또한 다음을 클릭하여 정책을 생성할 수도 있습니다.  .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

- b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.
- c. 정책 _policy_name_에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 `_policy_name_`은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 선택한 정책에 대해 보조 보호가 활성화된 경우 보조 보호 페이지가 표시되며 다음 단계를 수행해야 합니다.

a. 복제 정책의 유형을 선택하세요.



동기 복제 정책은 지원되지 않습니다.

b. 사용할 일관성 그룹 접미사를 지정합니다.

c. 대상 클러스터 및 대상 SVM 드롭다운에서 사용하려는 피어링된 클러스터와 SVM을 선택합니다.



SnapCenter에서는 클러스터 및 SVM 피어링을 지원하지 않습니다. 클러스터 및 SVM 피어링을 수행하려면 System Manager 또는 ONTAP CLI를 사용해야 합니다.



리소스가 이미 SnapCenter 외부에서 보호되고 있는 경우 해당 리소스는 보조 보호 리소스 섹션에 표시됩니다.

1. 확인 페이지에서 다음 단계를 수행하세요.

a. *로케이터 로드*를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 저장소에서 검증을 수행합니다.

b. 딸깍 하는 소리  일정 구성 열에서 정책의 모든 일정 유형에 대한 확인 일정을 구성합니다.

c. 확인 일정 추가 `policy_name` 대화 상자에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	이렇게 하세요...
백업 후 검증 실행	*백업 후 검증 실행*을 선택하세요.
검증 일정을 예약하세요	*예약된 확인 실행*을 선택한 다음 드롭다운 목록에서 일정 유형을 선택합니다.

d. 보조 저장소 시스템에서 백업을 확인하려면 *보조 위치에서 확인*을 선택하세요.

e. *확인*을 클릭합니다.

구성된 검증 일정은 적용된 일정 열에 나열됩니다.

2. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 `Set-SmSmtplibServer`를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

3. 요약을 검토한 후 *마침*을 클릭하세요.

PowerShell cmdlet을 사용하여 스토리지 시스템 연결 및 자격 증명 만들기

PowerShell cmdlet을 사용하여 데이터 보호 작업을 수행하려면 먼저 SVM(스토리지 가상 머신) 연결과 자격 증명을 만들어야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 저장소 연결을 생성하려면 인프라 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

스토리지 시스템 연결을 추가하는 동안에는 호스트 플러그인 설치가 진행 중이어서는 안 됩니다. 호스트 캐시가 업데이트되지 않고 SnapCenter GUI에 데이터베이스 상태가 “백업에 사용할 수 없음” 또는 “NetApp 스토리지에 없음”으로 표시될 수 있기 때문입니다.

- 저장 시스템 이름은 고유해야 합니다.

SnapCenter 서로 다른 클러스터에 동일한 이름을 가진 여러 스토리지 시스템을 지원하지 않습니다. SnapCenter에서 지원하는 각 스토리지 시스템은 고유한 이름과 고유한 관리 LIF IP 주소를 가져야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 PowerShell Core 연결 세션을 시작합니다.

이 예제에서는 PowerShell 세션을 엽니다.

```
PS C:\> Open-SmConnection
```

2. Add-SmStorageConnection cmdlet을 사용하여 스토리지 시스템에 대한 새 연결을 만듭니다.

이 예제에서는 새로운 스토리지 시스템 연결을 만듭니다.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Add-SmCredential cmdlet을 사용하여 새 자격 증명을 만듭니다.

이 예제에서는 Windows 자격 증명을 사용하여 FinanceAdmin이라는 새 자격 증명을 만듭니다.

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

Windows 파일 시스템에 대한 단일 리소스를 필요에 따라 백업합니다.

리소스가 리소스 그룹에 없는 경우 리소스 페이지에서 필요에 따라 리소스를 백업할 수 있습니다.

이 작업에 관하여

보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 역할에 “snapmirror all” 권한이 포함되어야 합니다. 하지만 “vsadmin” 역할을 사용하는 경우 “snapmirror all” 권한은 필요하지 않습니다.



파일 시스템을 백업할 때 SnapCenter 백업 중인 파일 시스템의 볼륨 마운트 지점(VMP)에 마운트된 LUN을 백업하지 않습니다.



Windows 파일 시스템 컨텍스트에서 작업하는 경우 데이터베이스 파일을 백업하지 마세요. 그렇게 하면 일관되지 않은 백업이 생성되고 복원 시 데이터가 손실될 가능성이 있습니다. 데이터베이스 파일을 보호하려면 데이터베이스에 적합한 SnapCenter 플러그인을 사용해야 합니다(예: Microsoft SQL Server용 SnapCenter 플러그인 또는 Microsoft Exchange Server용 SnapCenter 플러그인).

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 파일 시스템 리소스 유형을 선택한 다음 백업할 리소스를 선택합니다.
3. 파일 시스템 보호 마법사가 자동으로 시작되지 않으면 *보호*를 클릭하여 마법사를 시작합니다.

리소스 그룹 생성 작업에 설명된 대로 보호 설정을 지정합니다.

4. 선택 사항: 마법사의 리소스 페이지에서 스냅샷에 대한 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname입니다.
기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

5. 정책 페이지에서 다음 작업을 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.

기존 정책을 선택한 다음 *세부정보*를 클릭하면 해당 정책을 사용할 수 있는지 확인할 수 있습니다.

기존 정책이 요구 사항을 충족하지 않는 경우 기존 정책을 복사하여 수정하거나 다음을 클릭하여 새 정책을 만들 수 있습니다.  정책 마법사를 시작합니다. 기존 정책이 요구 사항을 충족하지 않는 경우 기존 정책을 복사하여 수정하거나 다음을 클릭하여 새 정책을 만들 수 있습니다.  정책 마법사를 시작합니다.

선택한 정책은 '선택한 정책에 대한 일정 구성' 섹션의 '정책' 열에 나열됩니다.

- b. 선택한 정책에 대한 일정 구성 섹션에서 다음을 클릭합니다.  일정을 구성하려는 정책의 일정 구성 열에 있습니다.

- c. 정책_정책_이름_에 대한 일정 추가 대화 상자에서 시작 날짜, 만료 날짜, 빈도를 지정하여 일정을 구성한 다음 *마침*을 클릭합니다.

구성된 일정은 '선택한 정책에 대한 일정 구성' 섹션의 '적용된 일정' 열에 나열됩니다.

"예정된 작업이 실패할 수 있습니다"

6. 알림 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이메일 환경 설정	백업 리소스 그룹을 만들고, 정책을 첨부하고, 일정을 구성한 후 수신자에게 이메일을 보내려면 항상, 실패 시, *실패 또는 경고 시*를 선택합니다. SMTP 서버 정보, 기본 이메일 제목줄, "받는 사람" 및 "보낸 사람" 이메일 주소를 입력합니다.

이 분야에서는...	이렇게 하세요...
에서	이메일 주소
에게	이메일 주소로
주제	기본 이메일 제목줄

7. 요약을 검토한 후 *마침*을 클릭하세요.

데이터베이스 토폴로지 페이지가 표시됩니다.

8. *지금 백업*을 클릭하세요.

9. 백업 페이지에서 다음 단계를 수행합니다.

a. 리소스에 여러 정책을 적용한 경우 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

b. *백업*을 클릭하세요.

10. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.

2. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.

이 예제에서는 FullBackup의 SQL 백업 유형을 사용하여 새 백업 정책을 만듭니다.

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

이 예제에서는 CrashConsistent의 Windows 파일 시스템 백업 유형을 사용하여 새 백업 정책을 만듭니다.


```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Get-SmResources cmdlet을 사용하여 호스트 리소스를 검색합니다.

이 예제에서는 지정된 호스트에서 Microsoft SQL 플러그인에 대한 리소스를 검색합니다.

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

이 예제에서는 지정된 호스트에서 Windows 파일 시스템의 리소스를 검색합니다.

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Add-SmResourceGroup cmdlet을 사용하여 SnapCenter 에 새 리소스 그룹을 추가합니다.

이 예제에서는 지정된 정책과 리소스를 사용하여 새로운 SQL 데이터베이스 백업 리소스 그룹을 만듭니다.

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

이 예제에서는 지정된 정책과 리소스를 사용하여 새로운 Windows 파일 시스템 백업 리소스 그룹을 만듭니다.

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. New-SmBackup cmdlet을 사용하여 새로운 백업 작업을 시작합니다.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Get-SmBackupReport cmdlet을 사용하여 백업 작업의 상태를 확인합니다.

이 예제에서는 지정된 날짜에 실행된 모든 작업에 대한 작업 요약 보고서를 표시합니다.

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

Windows 파일 시스템에 대한 리소스 그룹 백업

리소스 그룹은 호스트나 클러스터에 있는 리소스의 모음입니다. 리소스 그룹에 대한 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다. 리소스 페이지에서 필요에 따라 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 첨부되고 일정이 구성된 경우 백업은 일정에 따라 자동으로 수행됩니다.

시작하기 전에

- 정책이 첨부된 리소스 그룹을 만들어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 역할에 "snapmirror all" 권한이 포함되어야 합니다. 하지만 "vsadmin" 역할을 사용하는 경우 "snapmirror all" 권한은 필요하지 않습니다.
- 리소스 그룹에 서로 다른 호스트의 여러 데이터베이스가 있는 경우 네트워크 문제로 인해 일부 호스트의 백업 작업이 늦게 실행될 수 있습니다. Set-SmConfigSettings PowerShell cmdlet을 사용하여 web.config에서 MaxRetryForUninitializedHosts 값을 구성해야 합니다.



파일 시스템을 백업할 때 SnapCenter 백업 중인 파일 시스템의 볼륨 마운트 지점(VMP)에 마운트된 LUN을 백업하지 않습니다.



Windows 파일 시스템 컨텍스트에서 작업하는 경우 데이터베이스 파일을 백업하지 마세요. 그렇게 하면 일관되지 않은 백업이 생성되고 복원 시 데이터가 손실될 가능성이 있습니다. 데이터베이스 파일을 보호하려면 데이터베이스에 적합한 SnapCenter 플러그인을 사용해야 합니다(예: Microsoft SQL Server용 SnapCenter 플러그인 또는 Microsoft Exchange Server용 SnapCenter 플러그인).

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.

검색창에 리소스 그룹 이름을 입력하거나 클릭하여 리소스 그룹을 검색할 수 있습니다. 태그를 선택합니다. 그런 다음 클릭할 수 있습니다. 필터 창을 닫으려면.

3. 리소스 그룹 페이지에서 백업하려는 리소스 그룹을 선택한 다음, *지금 백업*을 클릭합니다.



Oracle Database용 SnapCenter 플러그인의 경우 두 개의 데이터베이스가 있는 페더레이션 리소스 그룹이 있고 데이터베이스 중 하나에 NetApp 스토리지가 아닌 스토리지에 데이터 파일이 있는 경우 다른 데이터베이스가 NetApp 스토리지에 있더라도 백업 작업이 중단됩니다.

4. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스 그룹에 여러 정책을 연결한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

b. *백업*을 클릭하세요.

5. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

◦ MetroCluster 구성에서 SnapCenter 장애 조치 후 보호 관계를 감지하지 못할 수 있습니다.

"MetroCluster 장애 조치 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다."

◦ VMDK에서 애플리케이션 데이터를 백업하고 SnapCenter Plug-in for VMware vSphere의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다. Java 힙 크기를 늘리려면 스크립트 파일을 찾으세요. `/opt/netapp/init_scripts/scvservice`. 해당 스크립트에서 `do_start method` 명령은 SnapCenter VMware 플러그인 서비스를 시작합니다. 해당 명령을 다음과 같이 업데이트하세요. `Java -jar -Xmx8192M -Xms4096M`.

백업 작업 모니터링

SnapCenterJobs 페이지를 사용하여 다양한 백업 작업의 진행 상황을 모니터링할 수 있습니다. 완료 시점이나 문제가 있는지 확인하기 위해 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 해당 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  백업 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *백업*을 선택합니다.
 - d. 상태 드롭다운에서 백업 상태를 선택합니다.
 - e. *적용*을 클릭하면 작업이 성공적으로 완료된 것을 볼 수 있습니다.
4. 백업 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인하세요.



백업 작업 상태가 표시됩니다. 작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 표시가 되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

활동 창에서 작업 모니터링

활동 창에는 가장 최근에 수행된 5개의 작업이 표시됩니다. 활동 창에는 작업이 시작된 시점과 작업 상태도 표시됩니다.

활동 창에는 백업, 복원, 복제 및 예약된 백업 작업에 대한 정보가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 딸깍 하는 소리 활동 창에서 가장 최근의 작업 5개를 확인하세요.

작업 중 하나를 클릭하면 작업 세부 정보가 작업 세부 정보 페이지에 나열됩니다.

백업 작업 취소

대기 중인 백업 작업을 취소할 수 있습니다.

필요한 것

- 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 모니터 페이지나 활동 창에서 백업 작업을 취소할 수 있습니다.
- 실행 중인 백업 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 백업 작업을 취소할 수 있습니다.
- 취소할 수 없는 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자\그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 백업 작업을 취소할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	a. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. b. 작업을 선택한 다음 *작업 취소*를 클릭합니다.

...로부터	행동
활동 창	a. 백업 작업을 시작한 후 *를 클릭하세요.  * 활동 창에서 가장 최근의 작업 5개를 확인하세요. b. 작업을 선택하세요. c. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

작업이 취소되고 리소스는 이전 상태로 돌아갑니다.

토폴로지 페이지에서 관련 백업 및 복제본 보기

리소스를 백업하거나 복제할 준비를 할 때 기본 및 보조 저장소에 있는 모든 백업과 복제본을 그래픽으로 볼 수 있습니다. 토폴로지 페이지에서는 선택한 리소스 또는 리소스 그룹에 사용 가능한 모든 백업과 복제본을 볼 수 있습니다. 해당 백업 및 복제의 세부 정보를 보고 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

이 작업에 관하여

다음 아이콘을 '사본 관리' 보기에서 검토하여 백업 및 복제본을 기본 저장소 또는 보조 저장소(미러 사본 또는 볼트 사본)에서 사용할 수 있는지 확인할 수 있습니다.

-  기본 스토리지에서 사용 가능한 백업 및 복제본의 수를 표시합니다.
-  SnapMirror 기술을 사용하여 보조 저장소에 미러링된 백업 및 복제본의 수를 표시합니다.
-  미러 볼트 유형 볼륨의 버전 유연한 미러 백업의 복제본은 토폴로지 보기에 표시되지만 토폴로지 보기의 미러 백업 수에는 버전 유연한 백업이 포함되지 않습니다.
-  SnapVault 기술을 사용하여 보조 저장소에 복제된 백업 및 복제본의 수를 표시합니다.
 - 표시된 백업 수에는 보조 저장소에서 삭제된 백업이 포함됩니다. 예를 들어, 4개의 백업만 보존하는 정책을 사용하여 6개의 백업을 만든 경우 표시되는 백업 수는 6개입니다.
-  미러 볼트 유형 볼륨의 버전 유연한 미러 백업의 복제본은 토폴로지 보기에 표시되지만 토폴로지 보기의 미러 백업 수에는 버전 유연한 백업이 포함되지 않습니다.

SnapMirror Active Sync(처음에는 SnapMirror Business Continuity[SM-BC]로 출시됨)라는 보조 관계가 있는 경우 다음과 같은 추가 아이콘을 볼 수 있습니다.

-  복제 사이트가 오픈되었습니다.
-  복제 사이트가 다운되었습니다.



2차 거울이나 볼트 관계가 재설정되지 않았습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 리소스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 리소스를 선택합니다.

리소스가 보호된 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. 요약 카드를 검토하여 기본 및 보조 저장소에서 사용 가능한 백업 및 복제본 수에 대한 요약 확인하세요.

요약 카드 섹션에는 백업 및 복제의 총 수가 표시됩니다. Oracle 데이터베이스의 경우에만 요약 카드 섹션에 총 로그 백업 수도 표시됩니다.

새로 고침 버튼을 클릭하면 저장소에 대한 쿼리가 시작되어 정확한 개수가 표시됩니다.

SnapLock 이 활성화된 백업을 수행한 경우 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간이 새로 고쳐집니다. 주간 일정은 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간도 새로 고칩니다.

애플리케이션 리소스가 여러 볼륨에 분산되어 있는 경우 백업에 대한 SnapLock 만료 시간은 볼륨의 스냅샷에 설정된 가장 긴 SnapLock 만료 시간이 됩니다. 가장 긴 SnapLock 만료 시간은 ONTAP 에서 검색됩니다.

SnapMirror 활성화 동기화의 경우, 새로 고침 버튼을 클릭하면 ONTAP 기본 사이트와 복제 사이트를 모두 쿼리하여 SnapCenter 백업 인벤토리가 새로 고쳐집니다. 주간 일정은 SnapMirror 활성화 동기화 관계가 포함된 모든 데이터베이스에 대해 이 활동을 수행합니다.

- SnapMirror 활성화 동기화 및 ONTAP 9.14.1의 경우에만 장애 조치 후 새 기본 대상에 대한 비동기 미러 또는 비동기 MirrorVault 관계를 수동으로 구성해야 합니다. ONTAP 9.15.1부터 비동기 미러 또는 비동기 미러볼트가 새로운 기본 대상으로 자동 구성됩니다.
- 장애 조치 후에는 SnapCenter 에서 장애 조치를 인식할 수 있도록 백업을 만들어야 합니다. 백업이 생성된 후에만 *새로 고침*을 클릭할 수 있습니다.

5. 복사본 관리 보기에서 기본 또는 보조 저장소의 백업 또는 *복제*를 클릭하면 백업 또는 복제의 세부 정보를 볼 수 있습니다.

백업 및 복제의 세부 정보는 표 형식으로 표시됩니다.

6. 표에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 복제, 이름 바꾸기, 삭제 작업을 수행합니다.

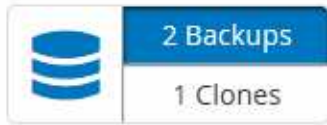


보조 저장 시스템에 있는 백업의 이름을 바꾸거나 삭제할 수 없습니다.

7. 복제본을 삭제하려면 테이블에서 복제본을 선택하고 클릭하십시오. 복제본을 삭제합니다.

기본 스토리지의 백업 및 복제를 보여주는 예

Manage Copies



Summary Card

2 Backups

1 Data Backups

1 Log Backups

1 Clones

PowerShell cmdlet을 사용하여 보조 백업 수 정리

Remove-SmBackup cmdlet을 사용하면 스냅샷이 없는 보조 백업의 백업 수를 정리할 수 있습니다. Manage Copies 토폴로지에 표시된 총 스냅샷 수가 보조 저장소 스냅샷 보존 설정과 일치하지 않는 경우 이 cmdlet을 사용할 수 있습니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146/
```

2. -CleanupSecondaryBackups 매개변수를 사용하여 보조 백업 수를 정리합니다.

이 예제에서는 스냅샷이 없는 보조 백업의 백업 수를 정리합니다.

```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```

Windows 파일 시스템 복원

Windows 파일 시스템 백업 복원

SnapCenter 사용하여 파일 시스템 백업을 복원할 수 있습니다. 파일 시스템 복원은 지정된 백업에서 모든 데이터를 파일 시스템의 원래 위치로 복사하는 다단계 프로세스입니다.

시작하기 전에

- 파일 시스템을 백업해야 합니다.
- 백업 작업과 같은 예약된 작업이 현재 파일 시스템에 대해 진행 중인 경우 복원 작업을 시작하기 전에 해당 작업을 취소해야 합니다.
- 파일 시스템 백업은 대체 경로가 아닌 원래 위치로만 복원할 수 있습니다.

복원된 파일 시스템은 파일 시스템의 원래 위치에 있는 모든 데이터를 덮어쓰기 때문에 백업에서 단일 파일을 복원할 수 없습니다. 파일 시스템 백업에서 단일 파일을 복원하려면 백업을 복제하고 복제본의 파일에 액세스해야 합니다.

- 시스템이나 부팅 볼륨을 복원할 수 없습니다.
- SnapCenter 클러스터 그룹을 오프라인으로 전환하지 않고도 Windows 클러스터의 파일 시스템을 복원할 수 있습니다.

이 작업에 관하여

- SCRIPTS_PATH는 플러그인 호스트의 SMCoreServiceHost.exe.Config 파일에 있는 PredefinedWindowsScriptsDirectory 키를 사용하여 정의됩니다.

필요한 경우 이 경로를 변경하고 SMcore 서비스를 다시 시작할 수 있습니다. 보안을 위해 기본 경로를 사용하는 것이 좋습니다.

키 값은 API를 통해 swagger에서 표시될 수 있습니다: API /4.7/configsettings

GET API를 사용하여 키 값을 표시할 수 있습니다. SET API는 지원되지 않습니다.

- SnapMirror Active Sync 복원 작업의 경우 기본 위치에서 백업을 선택해야 합니다.
- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 목록을 필터링하려면 파일 시스템 및 리소스 그룹 옵션을 선택하세요.
3. 목록에서 리소스 그룹을 선택한 다음 *복원*을 클릭합니다.
4. 백업 페이지에서 기본 스토리지 시스템 또는 보조 스토리지 시스템에서 복원할지 선택한 다음 복원할 백업을 선택합니다.
5. 복원 마법사에서 옵션을 선택하세요.
6. SnapCenter 복원 작업 전이나 후에 실행할 프리스크립트나 포스트스크립트의 경로와 인수를 각각 입력할 수 있습니다.

예를 들어, SNMP 트랩을 업데이트하고, 알림을 자동화하고, 로그를 보내는 등의 작업을 수행하는 스크립트를 실행할 수 있습니다.



prescripts 또는 postscripts 경로에는 드라이브나 공유가 포함되어서는 안 됩니다. 경로는 SCRIPTS_PATH를 기준으로 해야 합니다.

7. 알림 페이지에서 다음 옵션 중 하나를 선택하세요.

이 분야에서는...	이렇게 하세요...
SnapCenter 서버 이벤트를 스토리지 시스템 syslog에 기록합니다.	SnapCenter 서버 이벤트를 스토리지 시스템의 syslog에 기록하려면 이 옵션을 선택하세요.
실패한 작업에 대한 AutoSupport 알림을 스토리지 시스템으로 보냅니다.	AutoSupport 사용하여 실패한 작업에 대한 정보를 NetApp 에 보내려면 이 옵션을 선택하세요.
이메일 환경 설정	백업을 복원한 후 수신자에게 이메일 메시지를 보내려면 항상, 실패 시, *실패 또는 경고 시*를 선택하세요. SMTP 서버, 기본 이메일 제목줄, 받는 사람 및 보낸 사람 이메일 주소를 입력하세요.

8. 요약을 검토한 후 *마침*을 클릭하세요.
9. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.



복원된 파일 시스템에 데이터베이스가 포함되어 있는 경우 해당 데이터베이스도 복원해야 합니다. 데이터베이스를 복원하지 않으면 데이터베이스가 잘못된 상태가 될 수 있습니다. 데이터베이스 복원에 대한 자세한 내용은 해당 데이터베이스의 데이터 보호 가이드를 참조하세요.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-Smconnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

이 예에서는 2015년 1월 29일부터 2015년 2월 3일까지의 백업에 대한 자세한 정보를 표시합니다.

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId            : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

PowerShell cmdlet을 사용하여 리소스 복원

리소스 백업을 복원하려면 SnapCenter 서버와 연결 세션을 시작하고, 백업을 나열하고 백업 정보를 검색하고, 백업을 복원해야 합니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-Smconnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----

1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM

이 예에서는 2015년 1월 29일부터 2015년 2월 3일까지의 백업에 대한 자세한 정보를 표시합니다.

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

복원 작업 모니터링

작업 페이지를 사용하여 다양한 SnapCenter 복원 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

복원 후 상태는 복원 작업 후 리소스의 조건과 수행할 수 있는 추가 복원 작업을 설명합니다.

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중

-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복원 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복원*을 선택합니다.
 - d. 상태 드롭다운 목록에서 복원 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복원 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

복원 작업 취소

대기 중인 복원 작업을 취소할 수 있습니다.

복원 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

이 작업에 관하여

- 모니터 페이지나 활동 창에서 대기 중인 복원 작업을 취소할 수 있습니다.
- 실행 중인 복원 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 대기 중인 복원 작업을 취소할 수 있습니다.
- 취소할 수 없는 복원 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자\그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 복원 작업을 취소할 수 있습니다.

단계

다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	1. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. 2. 작업을 선택하고 *작업 취소*를 클릭하세요.
활동 창	1. 복원 작업을 시작한 후 다음을 클릭하세요.  활동 창에서 가장 최근의 작업 5개를 확인하세요. 2. 작업을 선택하세요. 3. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

Windows 파일 시스템 복제

Windows 파일 시스템 백업에서 복제

SnapCenter 사용하여 Windows 파일 시스템 백업을 복제할 수 있습니다. 실수로 삭제되거나 변경된 단일 파일의 사본이 필요한 경우 백업을 복제하여 복제본에서 해당 파일에 액세스할 수 있습니다.

시작하기 전에

- 호스트 추가, 리소스 식별, 스토리지 가상 머신(SVM) 연결 생성 등의 작업을 완료하여 데이터 보호를 준비했어야 합니다.
- 파일 시스템을 백업해야 합니다.
- 볼륨을 호스팅하는 집계가 스토리지 가상 머신(SVM)의 할당된 집계 목록에 있는지 확인해야 합니다.
- 리소스 그룹을 복제할 수 없습니다. 개별 파일 시스템 백업만 복제할 수 있습니다.
- 백업이 VMDK 디스크가 있는 가상 머신에 있는 경우 SnapCenter 백업을 물리적 서버로 복제할 수 없습니다.
- Windows 클러스터(예: 공유 LUN 또는 클러스터 공유 볼륨(CSV) LUN)를 복제하는 경우 복제본은 지정된 호스트에 전용 LUN으로 저장됩니다.
- 복제 작업의 경우 볼륨 마운트 지점의 루트 디렉토리는 공유 디렉토리가 될 수 없습니다.
- 집계의 홈 노드가 아닌 노드에는 복제본을 만들 수 없습니다.
- Windows 파일 시스템의 경우 반복되는 복제(복제 수명 주기) 작업을 예약할 수 없습니다. 백업은 수요에 따라서만 복제할 수 있습니다.
- 복제본이 포함된 LUN을 새 볼륨으로 이동하면 SnapCenter 더 이상 복제본을 지원할 수 없습니다. 예를 들어 SnapCenter 사용하여 해당 복제본을 삭제할 수 없습니다.
- 환경 간에 복제할 수 없습니다. 예를 들어, 실제 디스크에서 가상 디스크로 복제하거나 그 반대로 복제하는 경우입니다.

이 작업에 관하여

- SCRIPTS_PATH는 플러그인 호스트의 SMCoreServiceHost.exe.Config 파일에 있는 PredefinedWindowsScriptsDirectory 키를 사용하여 정의됩니다.

필요한 경우 이 경로를 변경하고 SMcore 서비스를 다시 시작할 수 있습니다. 보안을 위해 기본 경로를 사용하는 것이 좋습니다.

키 값은 API를 통해 swagger에서 표시될 수 있습니다: API /4.7/configsettings

GET API를 사용하여 키 값을 표시할 수 있습니다. SET API는 지원되지 않습니다.

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 목록에서 *파일 시스템*을 선택합니다.
3. 호스트를 선택하세요.

리소스가 보호되면 토폴로지 보기가 자동으로 표시됩니다.

4. 리소스 목록에서 복제하려는 백업을 선택한 다음 복제 아이콘을 클릭합니다.
5. 옵션 페이지에서 다음을 수행합니다.

이 분야에서는...	이렇게 하세요...
복제 서버	복제본을 생성할 호스트를 선택하세요.
“마운트 지점 자동 할당” 또는 “경로 아래에 볼륨 마운트 지점 자동 할당”	경로 아래에 마운트 지점이나 볼륨 마운트 지점을 자동으로 할당할지 여부를 선택합니다. 경로 아래의 볼륨 마운트 지점을 자동으로 할당: 경로 아래의 마운트 지점을 사용하면 마운트 지점이 생성될 특정 디렉토리를 제공할 수 있습니다. 이 옵션을 선택하기 전에 디렉토리가 비어 있는지 확인해야 합니다. 디렉토리에 백업이 있는 경우 마운트 작업 후 백업은 유효하지 않은 상태가 됩니다.
보관 위치	보조 백업을 복제하는 경우 보관 위치를 선택합니다.

6. 스크립트 페이지에서 실행하려는 사전 스크립트나 사후 스크립트를 지정합니다.



prescripts 또는 postscripts 경로에는 드라이브나 공유가 포함되어서는 안 됩니다. 경로는 SCRIPTS_PATH를 기준으로 해야 합니다.

7. 요약을 검토한 후 *마침*을 클릭하세요.
8. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Get-SmBackup 또는 Get-SmResourceGroup cmdlet을 사용하여 복제할 수 있는 백업을 나열합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

이 예제에서는 지정된 리소스 그룹, 해당 리소스 및 관련 정책에 대한 정보를 표시합니다.

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMaping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
```

Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}

```

AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False

```

3. New-SmClone cmdlet을 사용하여 기존 백업에서 복제 작업을 시작합니다.

이 예제에서는 모든 로그를 포함하는 지정된 백업에서 복제본을 만듭니다.

```

PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy

```

이 예제에서는 지정된 Microsoft SQL Server 인스턴스에 대한 복제본을 만듭니다.

```

PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"

```

4. Get-SmCloneReport cmdlet을 사용하여 복제 작업의 상태를 확인합니다.

이 예제에서는 지정된 작업 ID에 대한 복제 보고서를 표시합니다.

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

복제 작업 모니터링

작업 페이지를 사용하여 SnapCenter 복제 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.

2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복제 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복제*를 선택합니다.
 - d. 상태 드롭다운 목록에서 복제 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복제 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

복제 작업 취소

대기 중인 복제 작업을 취소할 수 있습니다.

복제 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

이 작업에 관하여

- 모니터 페이지나 활동 창에서 대기 중인 복제 작업을 취소할 수 있습니다.
- 실행 중인 복제 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 대기 중인 복제 작업을 취소할 수 있습니다.
- 역할을 생성할 때 사용자그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 객체를 보고 조작할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 복제 작업을 취소할 수 있습니다.

단계

다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	1. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. 2. 작업을 선택하고 *작업 취소*를 클릭합니다.
활동 창	1. 복제 작업을 시작한 후 다음을 클릭하세요.  활동 창에서 가장 최근의 작업 5개를 확인하세요. 2. 작업을 선택하세요. 3. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

클론 분할

SnapCenter 사용하면 복제된 리소스를 부모 리소스에서 분할할 수 있습니다. 분할된 복제본은 부모 리소스로부터 독립됩니다.

이 작업에 관하여

- 중간 복제본에서는 복제 분할 작업을 수행할 수 없습니다.

예를 들어, 데이터베이스 백업에서 clone1을 만든 후 clone1의 백업을 만든 다음 이 백업(clone2)을 복제할 수 있습니다. clone2를 생성한 후 clone1은 중간 복제본이 되며 clone1에서 복제 분할 작업을 수행할 수 없습니다. 하지만 clone2에 대해 클론 분할 작업을 수행할 수 있습니다.

clone2를 분할한 후에는 clone1에 대해 clone 분할 작업을 수행할 수 있습니다. clone1은 더 이상 중간 클론이 아니기 때문입니다.

- 복제본을 분할하면 복제본의 백업 사본과 복제 작업이 삭제됩니다.
- FlexClone 볼륨 분할 작업에 대한 정보는 다음을 참조하세요. "[FlexClone 볼륨을 부모 볼륨에서 분할합니다.](#)".
- 스토리지 시스템의 볼륨이나 집계가 온라인인지 확인하세요.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 적절한 옵션을 선택하세요.

옵션	설명
데이터베이스 애플리케이션의 경우	보기 목록에서 *데이터베이스*를 선택합니다.
파일 시스템의 경우	보기 목록에서 *경로*를 선택합니다.

3. 목록에서 적절한 리소스를 선택하세요.

리소스 토폴로지 페이지가 표시됩니다.

4. 사본 관리 보기에서 복제된 리소스(예: 데이터베이스 또는 LUN)를 선택한 다음 **.
5. 분할할 클론의 예상 크기와 집계에 필요한 사용 가능한 공간을 검토한 다음 *시작*을 클릭합니다.
6. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

SMCore 서비스를 다시 시작하면 복제 분할 작업이 더 이상 응답하지 않습니다. 복제 분할 작업을 중지하려면 Stop-SmJob cmdlet을 실행한 다음 복제 분할 작업을 다시 시도해야 합니다.

복제본이 분할되었는지 여부를 확인하기 위해 더 긴 폴링 시간이나 더 짧은 폴링 시간이 필요한 경우 *SMCoreServiceHost.exe.config* 파일에서 *CloneSplitStatusCheckPollTime* 매개변수 값을 변경하여 SMCore가 복제본 분할 작업의 상태를 폴링하는 시간 간격을 설정할 수 있습니다. 값은 밀리초이고 기본값은 5분입니다.

예를 들어:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

백업, 복원 또는 다른 클론 분할이 진행 중이면 클론 분할 시작 작업이 실패합니다. 실행 중인 작업이 완료된 후에만 복제 분할 작업을 다시 시작해야 합니다.

관련 정보

"SnapCenter 복제 또는 검증이 집계기 존재하지 않아 실패합니다."

Microsoft Exchange Server 데이터베이스 보호

Microsoft Exchange Server 개념에 대한 SnapCenter 플러그인

Microsoft Exchange Server용 SnapCenter 플러그인 개요

Microsoft Exchange Server용 SnapCenter 플러그인은 Exchange 데이터베이스의 애플리케이션 인식 데이터 보호 관리를 지원하는 NetApp SnapCenter 소프트웨어의 호스트 측 구성 요소입니다. Exchange용 플러그인은 SnapCenter 환경에서 Exchange 데이터베이스의 백업 및 복원을 자동화합니다.

Exchange용 플러그인을 설치하면 NetApp SnapMirror 기술과 함께 SnapCenter 사용하여 다른 볼륨에 백업 세트의 미리 사본을 만들고 NetApp SnapVault 기술을 사용하여 표준 준수 또는 보관 목적으로 디스크 간 백업 복제를 수행할 수 있습니다.

전체 Exchange 데이터베이스 대신 메일이나 사서함을 복원하고 복구하려는 경우 SMBR(Single Mailbox Recovery) 소프트웨어를 사용할 수 있습니다. NetApp® Single Mailbox Recovery는 2023년 5월 12일에 제공이 종료되었습니다(EOA). NetApp 2020년 6월 24일에 출시된 마케팅 부품 번호를 통해 사서함 용량, 유지 관리 및 지원을 구매한 고객을 지원 자격 기간 동안 계속 지원할 것입니다.

NetApp Single Mailbox Recovery는 Ontrack에서 제공하는 파트너 제품입니다. Ontrack PowerControls는 NetApp Single Mailbox Recovery와 유사한 기능을 제공합니다. 고객은 Ontrack(licensingteam@ontrack.com)을 통해 새로운 Ontrack PowerControls 소프트웨어 라이선스와 Ontrack PowerControls 유지관리 및 지원 갱신을 구매하여 세부적인 사서함 복구를 할 수 있습니다.

Exchange용 플러그인은 SnapMirror Active Sync(처음에는 SnapMirror Business Continuity[SM-BC]로 출시)를 지원하여 사이트 전체에 장애가 발생하더라도 비즈니스 서비스가 계속 운영될 수 있도록 하며, 보조 복사본을 사용하여 애플리케이션이 투명하게 장애 조치되도록 지원합니다. SnapMirror Active Sync를 사용하면 장애 조치를 트리거하는 데 수동 개입이나 추가 스크립팅이 필요하지 않습니다.

SnapMirror Active Sync의 비대칭, 장애 조치 또는 비이중 모드를 지원합니다. 이는 최적화된 경로가 기본 측 LUN 소유 노드에서만 생성되는 솔루션을 말합니다. 보조 클러스터 경로에서 발생하는 모든 I/O는 기본 클러스터로 프록시되어 처리됩니다. 동기 복제는 단방향, 즉 기본 복제에서 보조 복제로 진행됩니다.

- SnapCenter 환경에서 Microsoft Exchange Server 데이터베이스 및 DAG(데이터베이스 가용성 그룹)에 대한 애플리케이션 인식 백업 및 복원 작업을 자동화합니다.
- SnapCenter Plug-in for VMware vSphere 배포하고 SnapCenter 에 플러그인을 등록하면 RDM LUN에서 가상화된 Exchange 서버를 지원합니다.

Microsoft Exchange Server용 SnapCenter 플러그인으로 할 수 있는 작업

Exchange용 플러그인을 사용하면 Exchange Server 데이터베이스를 백업하고 복원할 수 있습니다.

- Exchange 데이터베이스 가용성 그룹(DAG), 데이터베이스 및 복제 세트의 활성 인벤토리를 보고 관리합니다.
- 백업 자동화에 대한 보호 설정을 제공하는 정책 정의
- 리소스 그룹에 정책 할당

- 개별 DAG 및 데이터베이스 보호
- 기본 및 보조 Exchange 사서함 데이터베이스 백업
- 1차 및 2차 백업에서 데이터베이스 복원

Microsoft Windows 및 Microsoft Exchange Server용 SnapCenter 플러그인에서 지원하는 스토리지 유형

SnapCenter 물리적 머신과 가상 머신 모두에서 다양한 스토리지 유형을 지원합니다. 호스트에 패키지를 설치하기 전에 해당 스토리지 유형에 대한 지원이 제공되는지 확인해야 합니다.

SnapCenter 프로비저닝 및 데이터 보호 지원은 Windows Server에서 제공됩니다. 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. <https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT> [NetApp 상호 운용성 매트릭스 도구].

기계	저장 유형	제공을 사용하여	지원 노트
물리적 서버	FC 연결 LUN	SnapCenter 그래픽 사용자 인터페이스(GUI) 또는 PowerShell cmdlet	
물리적 서버	iSCSI로 연결된 LUN	SnapCenter GUI 또는 PowerShell cmdlet	
VMware VM	FC 또는 iSCSI HBA로 연결된 RDM LUN	PowerShell cmdlet	물리적 호환성만  VMDK는 지원되지 않습니다.
VMware VM	iSCSI 이니시에이터에 의해 게스트 시스템에 직접 연결된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	 VMDK는 지원되지 않습니다.

기계	저장 유형	제공을 사용하여	지원 노트
Hyper-V VM	가상 파이버 채널 스위치로 연결된 가상 FC(vFC) LUN	SnapCenter GUI 또는 PowerShell cmdlet	가상 파이버 채널 스위치로 연결된 가상 FC(vFC) LUN을 프로비저닝하려면 Hyper-V 관리자를 사용해야 합니다.  NetApp 스토리지에 프로비저닝된 VHD(x)에 있는 Hyper-V 패스스루 디스크와 데이터베이스 백업은 지원되지 않습니다.
Hyper-V VM	iSCSI 이니시에이터에 의해 게스트 시스템에 직접 연결된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	 NetApp 스토리지에 프로비저닝된 VHD(x)에 있는 Hyper-V 패스스루 디스크와 데이터베이스 백업은 지원되지 않습니다.

Exchange 플러그인에 필요한 최소 **ONTAP** 권한

데이터 보호를 위해 사용하는 SnapCenter 플러그인에 따라 필요한 최소 ONTAP 권한은 다릅니다.

- 모든 액세스 명령: ONTAP 9.12.1 이상에 필요한 최소 권한
 - 이벤트 생성-자동 지원-로그
 - 작업 이력 표시
 - 작업 중지
 - 룰
 - lun 생성
 - lun 생성
 - lun 생성

- lun 삭제
- lun igroup 추가
- lun igroup 생성
- lun igroup 삭제
- lun igroup 이름 바꾸기
- lun igroup 이름 바꾸기
- 룬 아이그룹 쇼
- lun 매핑 add-reporting-nodes
- lun 매핑 생성
- LUN 매핑 삭제
- LUN 매핑 제거-보고-노드
- lun 매핑 쇼
- lun 수정
- lun 이동량
- lun 오프라인
- lun 온라인
- lun 지속적 예약 지우기
- lun 크기 조정
- lun 시리얼
- 런 쇼
- 스냅미러 정책 추가 규칙
- 스냅미러 정책 수정 규칙
- 스냅미러 정책 제거 규칙
- 스냅미러 정책 보기
- 스냅미러 복원
- 스냅미러 쇼
- 스냅미러 쇼 히스토리
- 스냅미러 업데이트
- 스냅미러 업데이트-is-세트
- 스냅미러 목록-대상
- 버전
- 볼륨 복제 생성
- 볼륨 클론 쇼
- 볼륨 복제 분할 시작

- 볼륨 클론 분할 정지
- 볼륨 생성
- 볼륨 파괴
- 볼륨 파일 복제 생성
- 볼륨 파일 show-disk-usage
- 볼륨 오프라인
- 온라인 볼륨
- 볼륨 수정
- 볼륨 qtree 생성
- 볼륨 qtree 삭제
- 볼륨 qtree 수정
- 볼륨 qtree 쇼
- 볼륨 제한
- 볼륨 쇼
- 볼륨 스냅샷 생성
- 볼륨 스냅샷 삭제
- 볼륨 스냅샷 수정
- 볼륨 스냅샷 수정-스냅락-만료-시간
- 볼륨 스냅샷 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- vservers cifs
- vservers cifs 공유 생성
- vservers cifs 공유 삭제
- vservers cifs 새도우 카피 쇼
- vservers cifs 공유 표시
- vservers cifs 쇼
- vservers 내보내기 정책
- vservers 내보내기 정책 생성
- vservers 내보내기 정책 삭제
- vservers 내보내기 정책 규칙 생성
- vservers 내보내기 정책 규칙 표시

- vservers 내보내기 정책 표시
- vserver iSCSI
- vserver iscsi 연결 표시
- vserver 쇼
- 읽기 전용 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
 - 네트워크 인터페이스
 - 네트워크 인터페이스 표시
 - vserver

SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비

ONTAP SnapMirror 기술과 함께 SnapCenter 플러그인을 사용하면 다른 볼륨에 백업 세트의 미러 사본을 생성할 수 있으며, ONTAP SnapVault 기술과 함께 사용하면 표준 준수 및 기타 거버넌스 관련 목적으로 디스크 간 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 구성하고 해당 관계를 초기화해야 합니다.

SnapCenter 스냅샷 작업을 완료한 후 SnapMirror와 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행됩니다. SnapMirror 활성 동기화를 사용하는 경우 SnapMirror 활성 동기화와 비동기 관계 모두에 기본 SnapMirror 또는 SnapVault 일정을 사용하세요.



NetApp SnapManager 제품을 통해 SnapCenter에 접속했고 구성된 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 기본 저장소(소스 볼륨)의 데이터를 보조 저장소(대상 볼륨)로 복제합니다. 관계를 초기화하면 ONTAP 소스 볼륨에서 참조되는 데이터 블록을 대상 볼륨으로 전송합니다.



SnapCenter SnapMirror와 SnapVault 볼륨 간의 계단식 관계(**Primary > Mirror > Vault**)를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter 버전에 따라 유연한 SnapMirror 관계 관리를 지원합니다. 버전에 따라 유연한 SnapMirror 관계와 이를 설정하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["ONTAP 문서"](#).

Exchange Server 리소스에 대한 백업 전략 정의

백업 작업을 생성하기 전에 백업 전략을 정의하면 데이터베이스를 성공적으로 복원하는 데 필요한 백업이 있는지 확인하는 데 도움이 됩니다. 백업 전략은 주로 서비스 수준 계약(SLA), 복구 시간 목표(RTO), 복구 지점 목표(RPO)에 따라 결정됩니다.

SLA는 기대되는 서비스 수준을 정의하고 서비스 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RTO는 서비스가 중단된 후 비즈니스 프로세스를 복구해야 하는 시간입니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 수명에 대한 전략을 정의합니다. SLA, RTO, RPO는 백업 전략에 기여합니다.

Exchange 데이터베이스에 지원되는 백업 유형

SnapCenter 사용하여 Exchange 사서함을 백업하려면 데이터베이스 및 DAG(데이터베이스 가용성 그룹)와 같은 리소스 유형을 선택해야 합니다. 스냅샷 기술은 리소스가 있는 볼륨의 온라인, 읽기 전용 복사본을 만드는 데 활용됩니다.

백업 유형	설명
전체 및 로그 백업	잘린 로그를 포함하여 데이터베이스와 모든 트랜잭션 로그를 백업합니다. 전체 백업이 완료되면 Exchange Server는 이미 데이터베이스에 커밋된 트랜잭션 로그를 잘라냅니다. 일반적으로 이 옵션을 선택하는 것이 좋습니다. 하지만 백업 시간이 짧다면 전체 백업과 함께 트랜잭션 로그 백업을 실행하지 않도록 선택할 수 있습니다.
전체 백업	데이터베이스와 트랜잭션 로그를 백업합니다. 잘린 트랜잭션 로그는 백업되지 않습니다.
로그 백업	모든 거래 로그를 백업합니다. 이미 데이터베이스에 커밋된 잘린 로그는 백업되지 않습니다. 전체 데이터베이스 백업 사이에 자주 트랜잭션 로그 백업을 예약하면 세분화된 복구 지점을 선택할 수 있습니다.

데이터베이스 플러그인에 대한 백업 일정

백업 빈도(일정 유형)는 정책에 지정되고, 백업 일정은 리소스 그룹 구성에 지정됩니다. 백업 빈도나 일정을 결정하는 가장 중요한 요소는 리소스의 변화율과 데이터의 중요도입니다. 자주 사용되는 리소스는 매시간 백업하고, 거의 사용되지 않는 리소스는 하루에 한 번 백업할 수도 있습니다. 기타 요소로는 조직에 대한 리소스의 중요성, 서비스 수준 계약(SLA), 복구 지점 목표(RPO) 등이 있습니다.

SLA는 기대되는 서비스 수준을 정의하고 서비스 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 수명에 대한 전략을 정의합니다. SLA와 RPO는 데이터 보호 전략에 기여합니다.

많이 사용되는 리소스의 경우에도 하루에 한두 번 이상 전체 백업을 실행할 필요는 없습니다. 예를 들어, 정기적인 트랜잭션 로그 백업을 통해 필요한 백업을 확보하는 데 충분할 수 있습니다. 데이터베이스를 더 자주 백업할수록 SnapCenter 복원 시 사용해야 하는 트랜잭션 로그가 줄어들어 복원 작업이 더 빨라질 수 있습니다.

백업 일정은 다음과 같이 두 부분으로 구성됩니다.

- 백업 주파수

일부 플러그인의 경우 **_스케줄 유형_**이라고 하는 백업 빈도(백업을 수행하는 빈도)는 정책 구성의 일부입니다. 정책의 백업 빈도를 시간별, 일별, 주별 또는 월별로 선택할 수 있습니다. 이러한 주파수를 선택하지 않으면 생성된 정책은 주문형 정책만입니다. 설정 > *정책*을 클릭하면 정책에 액세스할 수 있습니다.

- 백업 일정

백업 일정(백업을 정확히 언제 수행해야 하는지)은 리소스 그룹 구성의 일부입니다. 예를 들어, 주간 백업에 대한 정책이 구성된 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 일정을 구성할 수 있습니다. 리소스 > *리소스 그룹*을 클릭하면 리소스 그룹 일정에 액세스할 수 있습니다.

데이터베이스에 필요한 백업 작업 수

필요한 백업 작업 수를 결정하는 요소에는 리소스 크기, 사용된 볼륨 수, 리소스 변경률, 서비스 수준 계약(SLA) 등이 있습니다.

백업 명명 규칙

기본 스냅샷 명명 규칙을 사용하거나 사용자 지정 명명 규칙을 사용할 수 있습니다. 기본 백업 명명 규칙은 스냅샷 이름에 타임스탬프를 추가하여 복사본이 생성된 시기를 식별하는 데 도움이 됩니다.

스냅샷은 다음과 같은 기본 명명 규칙을 사용합니다.

resourcegroupname_hostname_timestamp

다음 예와 같이 논리적으로 백업 리소스 그룹의 이름을 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예에서 구문 요소는 다음과 같은 의미를 갖습니다.

- _dts1_은 리소스 그룹 이름입니다.
- _mach1x88_은 호스트 이름입니다.
- _03-12-2015_23.17.26_은 날짜와 타임스탬프입니다.

또는, *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택하여 리소스나 리소스 그룹을 보호하는 동안 스냅샷 이름 형식을 지정할 수 있습니다. 예를 들어, customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname입니다. 기본적으로 타임스탬프 접미사는 스냅샷 이름에 추가됩니다.

백업 보존 옵션

백업 사본을 보관할 일수를 선택하거나 보관할 백업 사본 수를 지정할 수 있으며, ONTAP 최대 255개 사본까지 보관할 수 있습니다. 예를 들어, 귀하의 조직에서는 10일 분의 백업 사본이나 130개의 백업 사본을 보관하도록 요구할 수 있습니다.

정책을 생성하는 동안 백업 유형과 일정 유형에 대한 보존 옵션을 지정할 수 있습니다.

SnapMirror 복제를 설정하면 보존 정책이 대상 볼륨에 미러링됩니다.

SnapCenter 일정 유형과 일치하는 보존 레이블이 있는 보관된 백업을 삭제합니다. 리소스 또는 리소스 그룹의 일정 유형이 변경된 경우 이전 일정 유형 레이블이 지정된 백업이 시스템에 남아 있을 수 있습니다.



백업 사본을 장기간 보관하려면 SnapVault 백업을 사용해야 합니다.

Exchange Server의 소스 저장소 볼륨에서 트랜잭션 로그 백업을 보관하는 기간

Microsoft Exchange Server용 SnapCenter 플러그인은 최신 복원 작업을 수행하기 위해 트랜잭션 로그 백업이 필요하며, 이를 통해 두 개의 전체 백업 사이의 시간으로 데이터베이스를 복원합니다.

예를 들어, Plug-in for Exchange가 오전 8시에 전체 백업과 트랜잭션 로그 백업을 수행하고 오후 5시에 또 다른 전체 백업과 트랜잭션 로그 백업을 수행한 경우 최신 트랜잭션 로그 백업을 사용하여 오전 8시와 오후 5시 사이의 어느 시간으로든 데이터베이스를 복원할 수 있습니다. 트랜잭션 로그를 사용할 수 없는 경우 Plug-in for Exchange는 특정 시점 복원 작업만 수행할 수 있으며, 이 경우 Plug-in for Exchange가 전체 백업을 완료한 시점으로 데이터베이스를 복원합니다.

일반적으로 최신 복구 작업은 하루나 이틀 정도만 필요합니다. 기본적으로 SnapCenter 최소 2일간 보관합니다.

Exchange 데이터베이스에 대한 복원 전략 정의

Exchange Server에 대한 복원 전략을 정의하면 데이터베이스를 성공적으로 복원할 수 있습니다.

Exchange Server에서 복원 작업을 위한 소스

기본 저장소의 백업 복사본에서 Exchange Server 데이터베이스를 복원할 수 있습니다.

기본 저장소에서만 데이터베이스를 복원할 수 있습니다.

Exchange Server에서 지원되는 복원 작업 유형

SnapCenter 사용하면 Exchange 리소스에 대해 다양한 유형의 복원 작업을 수행할 수 있습니다.

- 최신 정보를 복원합니다
- 이전 시점으로 복원

최신 상태로 복원

최신 복원 작업에서는 데이터베이스가 오류 발생 지점까지 복구됩니다. SnapCenter 다음 순서를 수행하여 이를 달성합니다.

1. 선택한 전체 데이터베이스 백업에서 데이터베이스를 복원합니다.
2. 백업된 모든 트랜잭션 로그와 가장 최근 백업 이후 생성된 모든 새 로그를 적용합니다.

거래 로그가 앞으로 이동되어 선택한 데이터베이스에 적용됩니다.

복원이 완료되면 Exchange에서 새로운 로그 체인을 만듭니다.

모범 사례: 복원이 완료된 후에는 새로운 전체 백업과 로그 백업을 수행하는 것이 좋습니다.

최신 복원 작업에는 연속된 트랜잭션 로그 세트가 필요합니다.

최신 복원을 수행한 후에는 복원에 사용한 백업을 특정 시점 복원 작업에만 사용할 수 있습니다.

모든 백업에 대한 최신 복원 기능을 유지할 필요가 없는 경우 백업 정책을 통해 시스템의 트랜잭션 로그 백업 보존을 구성할 수 있습니다.

이전 시점으로 복원

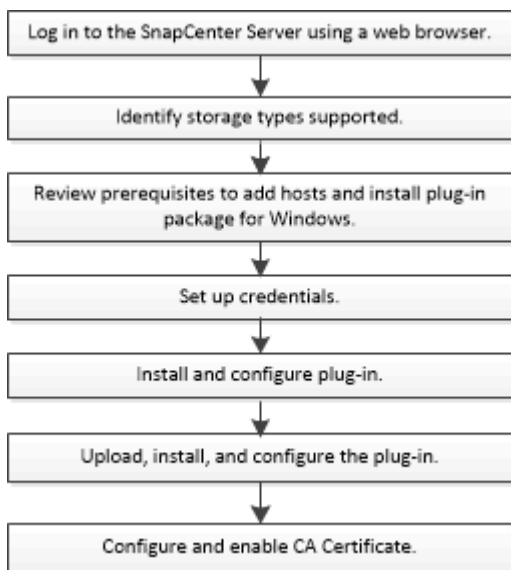
지정 시점 복원 작업에서는 데이터베이스가 과거의 특정 시점으로만 복원됩니다. 지정 시간 복원 작업은 다음과 같은 복원 상황에서 발생합니다.

- 데이터베이스는 백업된 트랜잭션 로그의 특정 시간으로 복원됩니다.
- 데이터베이스가 복원되고, 백업된 트랜잭션 로그의 하위 집합만 적용됩니다.

Microsoft Exchange Server용 SnapCenter 플러그인 설치

Microsoft Exchange Server용 SnapCenter 플러그인 설치 워크플로

Exchange 데이터베이스를 보호하려면 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



Microsoft Exchange Server용 SnapCenter 플러그인을 설치하고 호스트를 추가하기 위한 전제 조건

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 충족해야 합니다.

- iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.
- 원격 호스트에 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 도메인 사용자가 있어야 합니다.
- 독립 실행형 및 데이터베이스 가용성 그룹 구성에는 Microsoft Exchange Server 2013, 2016 또는 2019를 사용해야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.
- SnapCenter 에서 클러스터 노드를 관리하는 경우 클러스터의 모든 노드에 대한 관리 권한이 있는 사용자가 있어야 합니다.
- Exchange Server에 대한 관리 권한이 있는 사용자가 있어야 합니다.
- Microsoft Exchange Server용 SnapManager 와 Windows용 SnapDrive 이미 설치되어 있는 경우 SnapCenter

사용하여 데이터를 성공적으로 보호하려면 동일한 Exchange Server에 Exchange용 플러그인을 설치하기 전에 SnapDrive for Windows에서 사용하는 VSS 하드웨어 공급자를 등록 취소해야 합니다.

- SnapManager for Microsoft Exchange Server와 Plug-in for Exchange가 동일한 서버에 설치된 경우 SnapManager for Microsoft Exchange Server에서 생성한 모든 일정을 Windows 스케줄러에서 일시 중단하거나 삭제해야 합니다.
- 호스트는 서버에서 정규화된 도메인 이름(FQDN)으로 확인 가능해야 합니다. 호스트 파일을 수정하여 확인할 수 있게 하고 호스트 파일에 짧은 이름과 FQDN이 모두 지정된 경우 SnapCenter 호스트 파일에 다음 형식으로 항목을 만듭니다. <ip_address> <host_fqdn> <host_name>.
- 다음 포트가 방화벽에서 차단되어 있지 않은지 확인하세요. 차단되어 있으면 호스트 추가 작업이 실패합니다. 이 문제를 해결하려면 동적 포트 범위를 구성해야 합니다. 자세한 내용은 다음을 참조하세요. "[Microsoft 설명서](#)".
 - Windows 2016 및 Exchange 2016의 포트 범위 50000~51000
 - Windows 2012 R2 및 Exchange 2013의 경우 포트 범위 6000~6500
 - Windows 2019의 포트 범위 49152 - 65536

i

포트 범위를 식별하려면 다음 명령을 실행하세요.

- netsh int ipv4 show dynamicport tcp
- netsh int ipv4 show dynamicport udp
- netsh int ipv6 show dynamicport tcp
- netsh int ipv6 show dynamicport udp

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항과 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	마이크로소프트 윈도우 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구".
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	i 충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.

목	요구 사항
필수 소프트웨어 패키지	• ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 • 파워셸 코어 7.4.2 • Java 11 Oracle Java 및 OpenJDK Java 11 Oracle Java 및 OpenJDK는 SAP HANA, IBM Db2, PostgreSQL, MySQL, NetApp 지원 플러그인 및 Windows 호스트에 설치할 수 있는 기타 사용자 정의 애플리케이션에만 필요합니다. 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .

Exchange Server 권한이 필요합니다

SnapCenter Exchange Server 또는 DAG를 추가하고 호스트 또는 DAG에 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하도록 하려면 최소한의 권한 및 사용 권한이 있는 사용자의 자격 증명으로 SnapCenter 구성해야 합니다.

로컬 관리자 권한이 있는 도메인 사용자가 있어야 하며, 원격 Exchange 호스트에 대한 로컬 로그인 권한과 DAG의 모든 노드에 대한 관리 권한이 있어야 합니다. 도메인 사용자에게는 다음과 같은 최소 권한이 필요합니다.

- Add-MailboxDatabaseCopy
- Dismount-데이터베이스
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- Move-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly:\$true
- 마운트-데이터베이스
- 새 사서함 데이터베이스
- 새로운 공개 폴더 데이터베이스
- Remove-MailboxDatabase
- Remove-MailboxDatabaseCopy
- Remove-PublicFolderDatabase

- 이력서-사서함 데이터베이스 복사
- 광고 서버 설정 설정
- Set-MailboxDatabase -allowfilerestore:\$true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- 일시 중단-사서함 데이터베이스 복사
- 업데이트-사서함데이터베이스복사

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항과 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	마이크로소프트 윈도우 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	• ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 • 파워셀 코어 7.4.2 • Java 11 Oracle Java 및 OpenJDK Java 11 Oracle Java 및 OpenJDK는 SAP HANA, IBM Db2, PostgreSQL, MySQL, NetApp 지원 플러그인 및 Windows 호스트에 설치할 수 있는 기타 사용자 정의 애플리케이션에만 필요합니다. 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .

Windows용 SnapCenter 플러그인에 대한 자격 증명 설정

SnapCenter 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다. 플러그인 패키지를 설치하기 위한 자격 증명과 데이터베이스에서 데이터 보호 작업을 수행하기 위한 추가 자격 증명을 만들어야 합니다.

이 작업에 관하여

Windows 호스트에 플러그인을 설치하려면 자격 증명을 설정해야 합니다. 호스트를 배포하고 플러그인을 설치한 후에도 Windows에 대한 자격 증명을 만들 수 있지만 가장 좋은 방법은 호스트를 배포하고 플러그인을 설치하기 전에 SVM을 추가한 후에 자격 증명을 만드는 것입니다.

원격 호스트에 대한 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정합니다.

개별 리소스 그룹에 대한 자격 증명을 설정하고 사용자 이름에 전체 관리자 권한이 없는 경우 최소한 리소스 그룹 및 백업 권한을 사용자 이름에 할당해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *자격 증명*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.

자격 증명 창이 표시됩니다.

4. 자격 증명 페이지에서 다음을 수행합니다.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.

이 분야에서는...	이렇게 하세요...
사용자 이름	인증에 사용되는 사용자 이름을 입력하세요. • 도메인 관리자 또는 관리자 그룹의 모든 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹 구성원을 지정하세요. 사용자 이름 필드에 사용할 수 있는 형식은 다음과 같습니다. ◦ NetBIOS\UserName ◦ Domain FQDN\UserName • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우, SnapCenter 플러그인을 설치할 시스템에 기본 제공되는 로컬 관리자를 지정하십시오. 사용자 계정에 승격된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우, 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다. UserName
비밀번호	인증에 사용되는 비밀번호를 입력하세요.
인증	인증 모드로 Windows를 선택하세요.

5. *확인*을 클릭합니다.

Windows Server 2016 이상에서 gMSA 구성

Windows Server 2016 이상에서는 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 관리 서비스 계정(gMSA)을 만들 수 있습니다.

시작하기 전에

- Windows Server 2016 이상 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2016 이상 호스트가 있어야 합니다.

단계

1. gMSA의 각 개체에 대해 고유한 비밀번호를 생성하려면 KDS 루트 키를 만듭니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 다음 명령을 실행합니다. Add-KDSRootKey -EffectiveImmediately
3. gMSA를 만들고 구성하세요.
 - a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
domainName\accountName$
.. 그룹에 컴퓨터 객체를 추가합니다.
.. 방금 만든 사용자 그룹을 사용하여 gMSA를 만듭니다.
```

예를 들어,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. 달리다 `Get-ADServiceAccount` 서비스 계정을 확인하는 명령입니다.
```

4. 호스트에서 gMSA를 구성하세요.

- a. gMSA 계정을 사용하려는 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.

이렇게 하려면 PowerShell에서 다음 명령을 실행하세요.

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart	Needed	Exit Code	Feature Result
-----	-----	-----	-----	-----
True	No		Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. 호스트를 다시 시작합니다.
- b. PowerShell 명령 프롬프트에서 다음 명령을 실행하여 호스트에 gMSA를 설치합니다. `Install-ADServiceAccount <gMSA>`
- c. 다음 명령을 실행하여 gMSA 계정을 확인하세요. `Test-ADServiceAccount <gMSA>`

5. 호스트에서 구성된 gMSA에 관리 권한을 할당합니다.

6. SnapCenter 서버에서 구성된 gMSA 계정을 지정하여 Windows 호스트를 추가합니다.

SnapCenter Server는 호스트에 선택된 플러그인을 설치하고, 플러그인 설치 중에 지정된 gMSA가 서비스 로그인 계정으로 사용됩니다.

호스트 추가 및 Exchange용 플러그인 설치

SnapCenter 호스트 추가 페이지를 사용하여 Windows 호스트를 추가할 수 있습니다. Exchange용 플러그인은 지정된 호스트에 자동으로 설치됩니다. 플러그인을 설치하는 데 권장되는 방법입니다. 개별 호스트나 클러스터에 호스트를 추가하고 플러그인을 설치할 수 있습니다.

시작하기 전에

- SnapCenter 서버 호스트의 운영 체제가 Windows 2019이고 플러그인 호스트의 운영 체제가 Windows 2022인 경우 다음을 수행해야 합니다.
 - Windows Server 2019(OS 빌드 17763.5936) 이상으로 업그레이드하세요.
 - Windows Server 2022(OS 빌드 20348.2402) 이상으로 업그레이드하세요.
- SnapCenter 관리자와 같이 플러그인 설치 및 제거 권한이 있는 역할에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.
- 메시지 큐잉 서비스가 실행 중이어야 합니다.
- 그룹 관리 서비스 계정(gMSA)을 사용하는 경우 관리자 권한으로 gMSA를 구성해야 합니다. 자세한 내용은 다음을 참조하세요. "[Windows Server 2016 이상에서 Microsoft Exchange Server에 대한 그룹 관리 서비스 계정 구성](#)".

이 작업에 관하여

- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.
- 개별 호스트나 클러스터에 대해 호스트를 추가하고 플러그인 패키지를 설치할 수 있습니다.
- 교환 노드가 DAG의 일부인 경우 SnapCenter 서버에 노드를 하나만 추가할 수 없습니다.
- 클러스터(Exchange DAG)에 플러그인을 설치하는 경우 일부 노드에 NetApp LUN에 데이터베이스가 없더라도 클러스터의 모든 노드에 플러그인이 설치됩니다.

SnapCenter 4.6부터 SCE는 멀티테넌시를 지원하며 다음 방법을 사용하여 호스트를 추가할 수 있습니다.

호스트 작업 추가	4.5 및 이전 버전	4.6 이상
교차 도메인 또는 다른 도메인에 IP 없는 DAG 추가	지원되지 않음	지원됨
동일 도메인 또는 교차 도메인에 있는 고유한 이름을 가진 여러 IP DAG를 추가합니다.	지원됨	지원됨
동일한 호스트 이름 및/또는 DB 이름을 갖는 여러 IP 또는 IP 없는 DAG를 크로스 도메인에 추가합니다.	지원되지 않음	지원됨
동일한 이름과 교차 도메인을 갖는 여러 개의 IP/IP 없는 DAG 추가	지원되지 않음	지원됨
동일한 이름과 크로스 도메인을 가진 여러 독립형 호스트 추가	지원되지 않음	지원됨

Exchange용 플러그인은 Windows용 SnapCenter 플러그인 패키지에 따라 달라지며, 버전이 동일해야 합니다.

Exchange용 플러그인 설치 중에 Windows용 SnapCenter 플러그인 패키지가 기본적으로 선택되고 VSS 하드웨어 공급자와 함께 설치됩니다.

Microsoft Exchange Server용 SnapManager 와 Windows용 SnapDrive 이미 설치되어 있고 동일한 Exchange Server에 Exchange용 플러그인을 설치하려는 경우, Windows용 SnapDrive 에서 사용하는 VSS 하드웨어 공급자를 등록 취소해야 합니다. 이 공급자는 Exchange용 플러그인과 Windows용 SnapCenter 플러그인 패키지에 설치된 VSS 하드웨어 공급자와 호환되지 않기 때문입니다. 자세한 내용은 다음을 참조하세요. ["Data ONTAP VSS 하드웨어 공급자를 수동으로 등록하는 방법"](#).

단계

- 1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
- 2. 맨 위에 *관리되는 호스트*가 선택되어 있는지 확인하세요.
- 3. *추가*를 클릭하세요.
- 4. 호스트 페이지에서 다음을 수행합니다.

이 분야에서는...	이렇게 하세요...
호스트 유형	호스트 유형으로 *Windows*를 선택합니다. SnapCenter Server는 호스트를 추가한 다음 Windows용 플러그인과 Exchange용 플러그인이 아직 설치되어 있지 않으면 호스트에 이를 설치합니다. Windows용 플러그인과 Exchange용 플러그인은 동일한 버전이어야 합니다. 이전에 다른 버전의 Windows용 플러그인이 설치된 경우 SnapCenter 설치의 일부로 해당 버전을 업데이트합니다.

이 분야에서는...	이렇게 하세요...
호스트 이름	호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하세요. SnapCenter DNS의 적절한 구성에 달려 있습니다. 따라서 가장 좋은 방법은 정규화된 도메인 이름(FQDN)을 입력하는 것입니다. 신뢰할 수 없는 도메인 호스트의 경우 IP 주소는 FQDN으로 확인되는 경우에만 지원됩니다. SnapCenter 사용하여 호스트를 추가하고 해당 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다. 다음 중 하나의 IP 주소나 FQDN을 입력할 수 있습니다. • 독립형 호스트 • DAG 교환 Exchange DAG의 경우 다음을 수행할 수 있습니다. ◦ DAG 이름, DAG IP 주소, 노드 이름 또는 노드 IP 주소를 제공하여 DAG를 추가합니다. ◦ DAG 클러스터 노드 중 하나의 IP 주소나 FQDN을 제공하여 IP가 없는 DAG 클러스터를 추가합니다. ◦ 동일한 도메인이나 다른 도메인에 있는 IP 없는 DAG를 추가합니다. 이름은 같지만 도메인이 다른 여러 개의 IP/IP 없는 DAG를 추가할 수도 있습니다.  독립 실행형 호스트 또는 Exchange DAG(크로스 도메인 또는 동일 도메인)의 경우 호스트나 DAG의 FQDN 또는 IP 주소를 제공하는 것이 좋습니다.

이 분야에서는...	이렇게 하세요...
신임장	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성하세요. 자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하세요. 지정한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다.  자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

Exchange용 플러그인을 선택하면 Microsoft SQL Server용 SnapCenter 플러그인이 자동으로 선택 해제됩니다. Microsoft에서는 Exchange에서 사용되는 메모리 양과 기타 리소스 사용량 때문에 SQL Server와 Exchange 서버를 동일한 시스템에 설치하지 않는 것이 좋습니다.

6. (선택 사항) *추가 옵션*을 클릭합니다.

이 분야에서는...	이렇게 하세요...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정하세요. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트 번호로 표시됩니다.  플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.
설치 경로	기본 경로는 다음과 같습니다. C:\Program Files\NetApp\SnapCenter . 선택적으로 경로를 사용자 정의할 수 있습니다.
DAG에 모든 호스트 추가	DAG를 추가할 때 이 확인란을 선택하세요.
사전 설치 확인 건너뛰기	플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택하세요.

이 분야에서는...	이렇게 하세요...
플러그인 서비스를 실행하려면 그룹 관리 서비스 계정(gMSA)을 사용하세요.	플러그인 서비스를 실행하기 위해 그룹 관리 서비스 계정(gMSA)을 사용하려면 이 확인란을 선택하세요. 다음 형식으로 gMSA 이름을 제공하세요: <code>domainName\accountName\$</code>.  gMSA는 Windows용 SnapCenter 플러그인 서비스에 대한 로그인 서비스 계정으로만 사용됩니다.

7. *제출*을 클릭하세요.

"사전 검사 건너뛰기" 확인란을 선택하지 않은 경우, 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 유효성 검사를 실시합니다. 최소 요구 사항을 충족하지 못할 경우, 해당 오류 또는 경고 메시지가 표시됩니다.

오류가 디스크 공간이나 RAM과 관련된 경우 다음 위치에 있는 web.config 파일을 업데이트할 수 있습니다.
C:\Program Files\NetApp\SnapCenter 기본값을 수정하는 WebApp입니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.



HA 설정에서 web.config 파일을 업데이트하는 경우 두 노드에서 모두 파일을 업데이트해야 합니다.

8. 설치 진행 상황을 모니터링합니다.

NET TCP 통신을 위한 사용자 정의 포트 구성

기본적으로 SnapCenter 6.0 릴리스부터 Windows용 SnapCenter 플러그인은 NET TCP 통신에 포트 909를 사용합니다. 포트 909가 사용 중인 경우 NET TCP 통신을 위해 다른 포트를 구성할 수 있습니다.

단계

1. C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe.config_에 있는 _NetTCPPort 키 값을 필요한 포트 번호로 수정합니다.
<add key="NetTCPPort" value="new_port_number" />
2. C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\SnapDriveService.dll.config_에 있는 _NetTCPPort 키의 값을 필요한 포트 번호로 수정합니다.
<add key="NetTCPPort" value="new_port_number" />
3. 아래 명령을 실행하여 **Data ONTAP VSS Hardware Provider** 서비스의 등록을 취소합니다.
"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\navssprv.exe" -r service -u
_services.msc_의 서비스 목록에 해당 서비스가 표시되지 않는지 확인하세요.
4. 아래 명령을 실행하여 **Data ONTAP VSS** 하드웨어 공급자 서비스를 등록합니다.
"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem"
_services.msc_의 서비스 목록에 해당 서비스가 표시되는지 확인하세요.

5. Windows용 플러그인 서비스를 다시 시작합니다.

PowerShell cmdlet을 사용하여 SnapCenter 서버 호스트에서 Exchange용 플러그인 설치

SnapCenter GUI에서 Exchange 플러그인을 설치해야 합니다. GUI를 사용하지 않으려면 SnapCenter 서버 호스트나 원격 호스트에서 PowerShell cmdlet을 사용할 수 있습니다.

시작하기 전에

- SnapCenter 서버가 설치 및 구성되어 있어야 합니다.
- 호스트의 로컬 관리자이거나 관리자 권한이 있는 사용자여야 합니다.
- SnapCenter 관리자와 같이 플러그인, 설치 및 제거 권한이 있는 역할이 할당된 사용자여야 합니다.
- Exchange용 플러그인을 설치하기 전에 설치 요구 사항과 지원되는 구성 유형을 검토해야 합니다.
- Exchange 플러그인을 설치하려는 호스트는 Windows 호스트여야 합니다.

단계

1. SnapCenter 서버 호스트에서 *Open-SmConnection* cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
2. 필수 매개변수와 함께 *Add-SmHost* cmdlet을 사용하여 Exchange 플러그인을 설치할 호스트를 추가합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

호스트는 독립형 호스트이거나 DAG일 수 있습니다. DAG를 지정하는 경우 `-IsDAG` 매개변수가 필요합니다.

3. 필수 매개변수와 함께 *Install-SmHostPackage* cmdlet을 사용하여 Exchange용 플러그인을 설치합니다.

이 명령은 지정된 호스트에 Exchange용 플러그인을 설치한 다음 SnapCenter 에 플러그인을 등록합니다.

명령줄에서 **Exchange용 SnapCenter** 플러그인을 자동으로 설치합니다.

SnapCenter 사용자 인터페이스 내에서 Exchange용 플러그인을 설치해야 합니다. 하지만 어떤 이유로 실행할 수 없다면 Windows 명령줄에서 자동 모드로 Exchange 플러그인 설치 프로그램을 자동으로 실행할 수 있습니다.

시작하기 전에

- Microsoft Exchange Server 리소스를 백업해야 합니다.
- SnapCenter 플러그인 패키지를 설치해야 합니다.
- Microsoft SQL Server용 SnapCenter 플러그인을 설치하기 전에 이전 릴리스를 삭제해야 합니다.

자세한 내용은 다음을 참조하세요. "[플러그인 호스트에서 SnapCenter 플러그인을 수동으로 직접 설치하는 방법](#)".

단계

1. 플러그인 호스트에 `C:\temp` 폴더가 있는지, 로그인한 사용자가 해당 폴더에 대한 전체 액세스 권한이 있는지 확인합니다.

2. C:\ProgramData\NetApp\ SnapCenter \Package Repository에서 Microsoft Windows용 SnapCenter 플러그인을 다운로드하세요.

이 경로는 SnapCenter 서버가 설치된 호스트에서 접근할 수 있습니다.

3. 플러그인을 설치하려는 호스트에 설치 파일을 복사합니다.
4. 로컬 호스트의 Windows 명령 프롬프트에서 플러그인 설치 파일을 저장한 디렉토리로 이동합니다.
5. 플러그인을 설치하려면 다음 명령을 입력하세요.

```
snapcenter_windows_host_plugin.exe"/silent /debuglog"<디버그_로그_경로>" /log"<로그_경로>"
BI_SNAPCENTER_PORT=<번호> SUITE_INSTALLDIR="<설치_디렉토리_경로>"
BI_SERVICEACCOUNT=<도메인\관리자> BI_SERVICEPWD=<비밀번호>
ISFeatureInstall=HPPW,SCW,SCE
```

예를 들어:

```
C:\ProgramData\NetApp\ SnapCenter\Package Repository\snapcenter_windows_host_plugin.exe"/silent
/debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\temp" BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C:\Program Files\NetApp\ SnapCenter" BI_SERVICEACCOUNT=도메인\관리자
BI_SERVICEPWD=암호 ISFeatureInstall=HPPW,SCW,SCE
```



Exchange 플러그인을 설치하는 동안 전달되는 모든 매개변수는 대소문자를 구분합니다.

변수에 다음 값을 입력하세요.

변하기 쉬운	가치
/debuglog"<디버그_로그_경로>	다음 예와 같이 제품군 설치 프로그램 로그 파일의 이름과 위치를 지정합니다. <i>Setup.exe /debuglog"C:\PathToLog\setupexe.log</i>
BI_SNAPCENTER_PORT	SnapCenter SMCore와 통신하는 포트를 지정합니다.
SUITE_INSTALLDIR	호스트 플러그인 패키지 설치 디렉토리를 지정합니다.
BI_SERVICEACCOUNT	Microsoft Windows 웹 서비스 계정에 대한 SnapCenter 플러그인을 지정합니다.
BI_SERVICEPWD	Microsoft Windows 웹 서비스 계정용 SnapCenter 플러그인의 비밀번호를 지정합니다.
ISFeature설치	SnapCenter 가 원격 호스트에 배포할 솔루션을 지정합니다.

6. Windows 작업 스케줄러, 기본 설치 로그 파일 C:\Installdebug.log 및 _C:\Temp_에 있는 추가 설치 파일을 모니터링합니다.
7. *msiexe.exe* 설치 프로그램이 오류 없이 소프트웨어를 설치하는지 확인하려면 %temp% 디렉터리를

모니터링하세요.



Exchange용 플러그인을 설치하면 플러그인이 SnapCenter 서버가 아닌 호스트에 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록할 수 있습니다. 호스트가 추가되면 플러그인이 자동으로 검색됩니다.

SnapCenter 플러그인 패키지 설치 상태 모니터링

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행 상황을 모니터링할 수 있습니다. 설치가 완료되었는지 또는 문제가 있는지 확인하기 위해 설치 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

- 진행 중
- 성공적으로 완료되었습니다
- 실패한
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
- 대기 중

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 플러그인 설치 작업만 나열되도록 목록을 필터링하려면 다음을 수행합니다.
 - a. *필터*를 클릭하세요.
 - b. 선택 사항: 시작 날짜와 종료 날짜를 지정합니다.
 - c. 유형 드롭다운 메뉴에서 *플러그인 설치*를 선택합니다.
 - d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
 - e. *적용*을 클릭하세요.
4. 설치 작업을 선택하고 *세부정보*를 클릭하면 작업 세부정보를 볼 수 있습니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

CA 인증서 구성

CA 인증서 CSR 파일 생성

인증서 서명 요청(CSR)을 생성하고, 생성된 CSR을 사용하여 인증 기관(CA)에서 얻을 수 있는 인증서를 가져올 수 있습니다. 인증서에는 개인 키가 연결됩니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.



CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 정보는 다음을 참조하세요. "[CA 인증서 CSR 파일을 생성하는 방법](#)".



도메인(*.domain.company.com)이나 시스템(machine1.domain.company.com)에 대한 CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN)과 해당 호스트 이름을 CA 인증서에 명시해야 합니다. 인증서를 구매하기 전에 주체 대체 이름(SAN) 필드를 입력하여 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(*.domain.company.com)의 경우 인증서에는 해당 도메인의 모든 호스트 이름이 암묵적으로 포함됩니다.

CA 인증서 가져오기

Microsoft 관리 콘솔(MMC)을 사용하여 CA 인증서를 SnapCenter 서버와 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.
2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
3. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > *인증서*를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 버튼으로 클릭한 다음, 모든 작업 > *가져오기*를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
개인 키 가져오기	예 옵션을 선택하고 개인 키를 가져온 후 *다음*을 클릭합니다.
가져오기 파일 형식	변경하지 마세요. *다음*을 클릭하세요.
보안	내보낸 인증서에 사용할 새 비밀번호를 지정한 후 *다음*을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.



인증서 가져오기는 개인 키와 함께 제공되어야 합니다(지원되는 형식: *.pfx, *.p12, *.p7b).

7. "개인" 폴더에 대해서도 5단계를 반복합니다.

CA 인증서 지문을 받으세요

인증서 지문은 인증서를 식별하는 16진수 문자열입니다. 지문은 지문 알고리즘을 사용하여 인증서 내용으로부터 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.

- 인증서를 두 번 클릭합니다.
- 인증서 대화 상자에서 세부정보 탭을 클릭합니다.
- 필드 목록을 스크롤하여 *지문*을 클릭하세요.
- 상자에서 16진수 문자를 복사하세요.
- 16진수 사이의 공백을 제거하세요.

예를 들어, 지문이 "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b"인 경우 공백을 제거하면 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.

- 다음 명령을 실행하여 설치된 인증서의 지문을 나열하고 주체 이름으로 최근에 설치된 인증서를 식별합니다.

```
Get-Childitem -경로 인증서:\LocalMachine\My
```

- 지문을 복사하세요.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스로 CA 인증서를 구성해야 합니다.

SnapCenter 서버와 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCORE 기본 포트 8145를 사용하는 기존 인증서 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

예를 들어:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스에 바인딩합니다.
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

예를 들어:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

플러그인에 대한 CA 인증서 활성화

CA 인증서를 구성하고 SnapCenter 서버와 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- `Set-SmCertificateSettings` cmdlet을 실행하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- `_Get-SmCertificateSettings`를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 하나 또는 여러 개의 플러그인 호스트를 선택하세요.
4. *추가 옵션*을 클릭하세요.
5. *인증서 검증 사용*을 선택합니다.

당신이 완료한 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- *  *는 CA 인증서가 활성화되지 않았거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- *  *는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- *  *는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- *  *는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

Exchange와 SnapCenter 공존하도록 SnapManager 7.x 구성

Microsoft Exchange Server용 SnapCenter 플러그인을 Microsoft Exchange Server용 SnapManager SnapManager 함께 사용하려면 SnapManager for Microsoft Exchange Server가 설치된 동일한 Exchange Server에 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하고, SnapManager for Exchange 일정을 비활성화한 다음, Microsoft Exchange Server용 SnapCenter 플러그인을 사용하여 새로운 일정과 백업을 구성해야 합니다.

시작하기 전에

- Microsoft Exchange Server용 SnapManager 와 Windows용 SnapDrive 이미 설치되어 있으며, Microsoft Exchange Server용 SnapManager 백업은 시스템과 SnapInfo 디렉터리에 있습니다.
- 더 이상 필요하지 않은 Microsoft Exchange Server용 SnapManager 에서 수행한 백업을 삭제하거나 회수했어야 합니다.
- Windows 스케줄러에서 Microsoft Exchange Server용 SnapManager 가 생성한 모든 일정을 일시 중단하거나 삭제해야 합니다.
- Microsoft Exchange Server용 SnapCenter 플러그인과 Microsoft Exchange Server용 SnapManager 동일한 Exchange Server에서 함께 사용할 수 있지만, 기존 Microsoft Exchange Server용 SnapManager 설치를 SnapCenter 로 업그레이드할 수는 없습니다.

SnapCenter 업그레이드 옵션을 제공하지 않습니다.

- SnapCenter Microsoft Exchange Server 백업을 위한 SnapManager 에서 Exchange 데이터베이스를 복원하는 것을 지원하지 않습니다.

Microsoft Exchange Server용 SnapCenter 플러그인을 설치한 후 Microsoft Exchange Server용 SnapManager 제거하지 않고 나중에 Microsoft Exchange Server용 SnapManager 백업을 복원하려면 추가 단계를 수행해야 합니다.

단계

1. 모든 DAG 노드에서 PowerShell을 사용하여 Windows VSS 하드웨어 공급자용 SnapDrive 등록되었는지 확인합니다. *vssadmin list providers*

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
Version: 7. 1. 4. 6845
```

2. SnapDrive 디렉토리에서 Windows용 SnapDrive 에서 VSS 하드웨어 공급자를 등록 취소합니다: *navssprv.exe -r service -u*
3. VSS 하드웨어 공급자가 제거되었는지 확인하세요: *vssadmin list providers*

4. SnapCenter 에 Exchange 호스트를 추가한 다음 Microsoft Windows용 SnapCenter 플러그인과 Microsoft Exchange Server용 SnapCenter 플러그인을 설치합니다.
5. 모든 DAG 노드의 Microsoft Windows용 SnapCenter 플러그인 디렉토리에서 VSS 하드웨어 공급자가 등록되었는지 확인합니다. *vssadmin list providers*

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
Version: 7. 0. 0. 5561
```

6. Microsoft Exchange Server 백업 일정에 대한 SnapManager 중지합니다.
7. SnapCenter GUI를 사용하여 주문형 백업을 만들고, 예약된 백업을 구성하고, 보존 설정을 구성합니다.
8. Microsoft Exchange Server용 SnapManager 제거합니다.

지금 SnapManager for Microsoft Exchange Server를 제거하지 않고 나중에 SnapManager for Microsoft Exchange Server 백업을 복원하려는 경우:

- a. 모든 DAG 노드에서 Microsoft Exchange Server용 SnapCenter 플러그인 등록을 취소합니다: *navssprv.exe -r service -u*

```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
Windows>navssprv.exe -r service -u
```

- b. *C:\Program Files\NetApp\SnapDrive* 디렉토리에서 모든 DAG 노드에 Windows용 SnapDrive 등록합니다: *navssprv.exe -r service -a hostname\username -p password*

SnapCenter Plug-in for VMware vSphere 설치

데이터베이스나 파일 시스템이 가상 머신(VM)에 저장되어 있거나 VM과 데이터 저장소를 보호하려는 경우 SnapCenter Plug-in for VMware vSphere 배포해야 합니다.

배포에 대한 정보는 다음을 참조하세요. "[배포 개요](#)".

CA 인증서 배포

SnapCenter Plug-in for VMware vSphere 사용하여 CA 인증서를 구성하려면 다음을 참조하세요. "[SSL 인증서 생성 또는 가져오기](#)".

CRL 파일 구성

SnapCenter Plug-in for VMware vSphere 미리 구성된 디렉토리에서 CRL 파일을 찾습니다. SnapCenter Plug-in for VMware vSphere의 CRL 파일의 기본 디렉토리는 `_/opt/netapp/config/crl_`입니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

데이터 보호를 준비하세요

백업, 복제 또는 복원 작업과 같은 데이터 보호 작업을 수행하기 전에 전략을 정의하고 환경을 설정해야 합니다. SnapMirror 및 SnapVault 기술을 사용하도록 SnapCenter 서버를 설정할 수도 있습니다.

SnapVault 및 SnapMirror 기술을 활용하려면 스토리지 장치의 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 구성하고 초기화해야 합니다. NetAppSystem Manager를 사용하거나 스토리지 콘솔 명령줄을 사용하여 이러한 작업을 수행할 수 있습니다.

더 많은 정보를 찾아보세요

["REST API 시작하기"](#)

Microsoft Exchange Server용 SnapCenter 플러그인을 사용하기 위한 전제 조건

Exchange용 플러그인을 사용하기 전에 SnapCenter 관리자가 SnapCenter 서버를 설치하고 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다.
- SnapCenter에 로그인하세요.
- 스토리지 시스템 연결을 추가하거나 할당하고 자격 증명을 생성하여 SnapCenter 환경을 구성합니다.



SnapCenter 서로 다른 클러스터에서 동일한 이름을 가진 여러 SVM을 지원하지 않습니다. SnapCenter가 지원하는 각 SVM에는 고유한 이름이 있어야 합니다.

- 호스트를 추가하고, Microsoft Windows용 SnapCenter 플러그인과 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하고, 리소스를 검색(새로 고침)합니다.
- Microsoft Windows용 SnapCenter 플러그인을 사용하여 호스트 측 스토리지 프로비저닝을 수행합니다.
- VMware RDM LUN에 있는 Exchange 데이터베이스를 보호하기 위해 SnapCenter Server를 사용하는 경우 SnapCenter Plug-in for VMware vSphere 배포하고 SnapCenter에 플러그인을 등록해야 합니다. SnapCenter Plug-in for VMware vSphere 대한 자세한 내용은 설명서를 참조하세요.



VMDK는 지원되지 않습니다.

- Microsoft Exchange 도구를 사용하여 기존 Microsoft Exchange Server 데이터베이스를 로컬 디스크에서 지원되는 저장소로 이동합니다.
- 백업 복제가 필요한 경우 SnapMirror와 SnapVault 관계를 설정합니다.

SnapCenter 4.1.1 사용자의 경우 SnapCenter Plug-in for VMware vSphere 설명서에는 가상화된 데이터베이스와

파일 시스템을 보호하는 방법에 대한 정보가 있습니다. SnapCenter 4.2.x 사용자, NetApp Data Broker 1.0 및 1.0.1의 경우, Linux 기반 NetApp Data Broker 가상 어플라이언스(Open Virtual Appliance 형식)에서 제공하는 SnapCenter Plug-in for VMware vSphere 사용하여 가상화된 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 설명서에 나와 있습니다. SnapCenter 4.3.x 사용자의 경우, SnapCenter Plug-in for VMware vSphere 설명서에는 Linux 기반 SnapCenter Plug-in for VMware vSphere (Open Virtual Appliance 형식)을 사용하여 가상화된 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 있습니다.

"SnapCenter Plug-in for VMware vSphere 설명서"

Exchange Server를 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식

SnapCenter 사용하기 전에 수행하려는 백업, 복원 및 다시 시드 작업과 관련된 기본 개념을 이해하는 것이 좋습니다. 다양한 작업을 위해 리소스, 리소스 그룹 및 정책과 상호 작용합니다.

- 리소스는 일반적으로 SnapCenter 사용하여 백업하는 사서함 데이터베이스 또는 Microsoft Exchange DAG(데이터베이스 가용성 그룹)입니다.
- SnapCenter 리소스 그룹은 호스트 또는 Exchange DAG의 리소스 모음이며, 리소스 그룹에는 전체 DAG 또는 개별 데이터베이스가 포함될 수 있습니다.

리소스 그룹에서 작업을 수행하면 리소스 그룹에 대해 지정한 일정에 따라 리소스 그룹에 정의된 리소스에서 해당 작업이 수행됩니다.

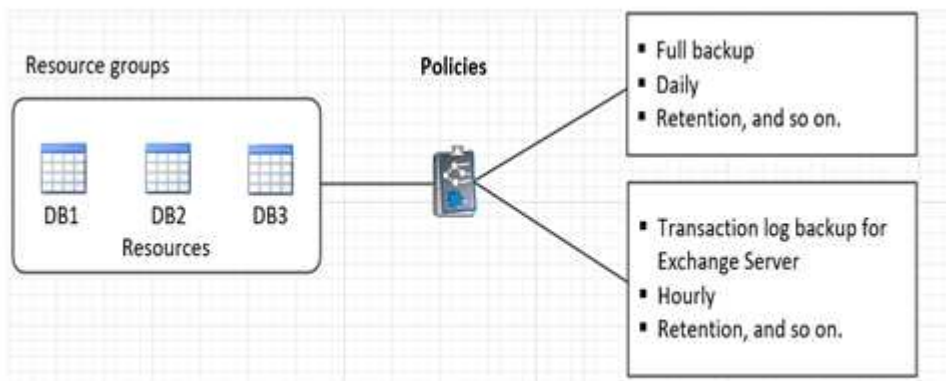
필요에 따라 단일 리소스나 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 수행할 수도 있습니다.

리소스 그룹은 이전에는 데이터 세트라고 알려져 있었습니다.

- 정책은 백업 빈도, 사본 보존 기간, 스크립트 및 데이터 보호 작업의 기타 특성을 지정합니다.

리소스 그룹을 만들 때 해당 그룹에 대한 하나 이상의 정책을 선택합니다. 단일 리소스에 대해 주문형 백업을 수행할 때 하나 이상의 정책을 선택할 수도 있습니다.

리소스 그룹은 보호하려는 내용과 보호하려는 날짜와 시간을 정의하는 것으로 생각하면 됩니다. 정책이란 그것을 어떻게 보호할 것인지를 정의하는 것이라고 생각하세요. 예를 들어 호스트의 모든 데이터베이스를 백업하는 경우 호스트의 모든 데이터베이스를 포함하는 리소스 그룹을 만들 수 있습니다. 그런 다음 리소스 그룹에 일일 정책과 시간별 정책이라는 두 가지 정책을 첨부할 수 있습니다. 리소스 그룹을 만들고 정책을 첨부할 때 리소스 그룹을 구성하여 매일 전체 백업을 수행하고 매시간 로그 백업을 수행하는 일정을 설정할 수 있습니다. 다음 이미지는 데이터베이스의 리소스, 리소스 그룹 및 정책 간의 관계를 보여줍니다.



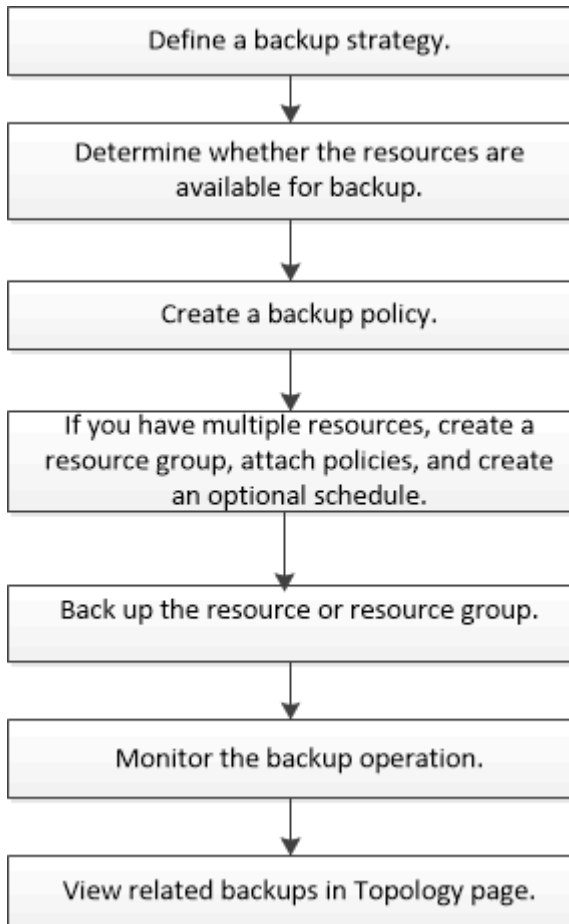
Exchange 리소스 백업

백업 워크플로

사용자 환경에 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하면 SnapCenter 사용하여 Exchange 리소스를 백업할 수 있습니다.

여러 서버에서 동시에 실행되도록 여러 백업을 예약할 수 있습니다. 동일한 리소스에서 백업 및 복원 작업을 동시에 수행할 수 없습니다. 동일한 볼륨에 대한 활성 및 수동 백업 복사본은 지원되지 않습니다.

다음 워크플로는 백업 작업을 수행해야 하는 순서를 보여줍니다.



Exchange 데이터베이스 및 백업 검증

Microsoft Exchange Server용 SnapCenter 플러그인은 백업 검증 기능을 제공하지 않습니다. 하지만 Exchange와 함께 제공되는 Eseutil 도구를 사용하면 Exchange 데이터베이스와 백업을 검증할 수 있습니다.

Microsoft Exchange Eseutil 도구는 Exchange 서버에 포함된 명령줄 유틸리티입니다. 이 유틸리티를 사용하면 일관성 검사를 수행하여 Exchange 데이터베이스와 백업의 무결성을 확인할 수 있습니다.

모범 사례: 최소 2개의 복제본이 있는 데이터베이스 가용성 그룹(DAG) 구성의 일부인 데이터베이스에서는 일관성 검사를 수행할 필요가 없습니다.

추가 정보는 다음을 참조하세요. "[Microsoft Exchange Server 설명서](#)".

백업에 **Exchange** 리소스를 사용할 수 있는지 확인합니다.

리소스는 설치한 플러그인에 의해 유지 관리되는 데이터베이스, Exchange 데이터베이스 가용성 그룹입니다. 데이터 보호 작업을 수행할 수 있도록 해당 리소스를 리소스 그룹에 추가할 수 있지만, 먼저 사용 가능한 리소스를 파악해야 합니다. 사용 가능한 리소스를 확인하면 플러그인 설치가 성공적으로 완료되었는지도 확인할 수 있습니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 생성, 자격 증명 추가, Exchange용 플러그인 설치 등의 작업을 이미 완료했어야 합니다.
- Single Mailbox Recovery 소프트웨어 기능을 활용하려면 Single Mailbox Recovery 소프트웨어가 설치된 Exchange Server에 활성 데이터베이스가 있어야 합니다.
- 데이터베이스가 VMware RDM LUN에 있는 경우 SnapCenter Plug-in for VMware vSphere 배포하고 SnapCenter에 플러그인을 등록해야 합니다. 그만큼 "[SnapCenter Plug-in for VMware vSphere 설명서](#)" 더 많은 정보가 있습니다.

이 작업에 관하여

- 세부 정보 페이지의 전체 상태 옵션이 백업할 수 없음으로 설정된 경우 데이터베이스를 백업할 수 없습니다. 다음 중 하나라도 해당되면 전체 상태 옵션이 백업할 수 없음으로 설정됩니다.
 - 데이터베이스가 NetApp LUN에 없습니다.
 - 데이터베이스가 정상 상태가 아닙니다.

데이터베이스가 마운트, 마운트 해제, 다시 시드 또는 복구 보류 상태에 있는 경우 해당 데이터베이스는 정상 상태가 아닙니다.

- DAG(데이터베이스 가용성 그룹)가 있는 경우 DAG에서 백업 작업을 실행하여 그룹의 모든 데이터베이스를 백업할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음, 리소스 페이지의 왼쪽 상단에 있는 플러그인 드롭다운 목록에서 *Microsoft Exchange Server*를 선택합니다.
2. 리소스 페이지의 보기 드롭다운 목록에서 데이터베이스, 데이터베이스 가용성 그룹 또는 *리소스 그룹*을 선택합니다.

모든 데이터베이스와 DAG는 FQDN 형식의 DAG 또는 호스트 이름과 함께 표시되므로 여러 데이터베이스를 구별할 수 있습니다.

딸깍 하는 소리  호스트 이름과 Exchange Server를 선택하여 리소스를 필터링합니다. 그런 다음 클릭할 수 있습니다  필터 창을 닫으려면.

3. *리소스 새로고침*을 클릭하세요.

새로 추가되거나 이름이 변경되거나 삭제된 리소스는 SnapCenter 서버 인벤토리에 업데이트됩니다.



SnapCenter 외부에서 데이터베이스 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

리소스는 리소스 이름, 데이터베이스 가용성 그룹 이름, 데이터베이스가 현재 활성화된 서버, 복사본이 있는 서버, 마지막 백업 시간, 전반적인 상태 등의 정보와 함께 표시됩니다.

- 데이터베이스가 NetApp 스토리지가 아닌 다른 스토리지에 있는 경우 전체 상태 열에 백업할 수 없음이 표시됩니다.

DAG에서 활성 데이터베이스 복사본이 NetApp 스토리지가 아닌 스토리지에 있고 최소 하나의 수동 데이터베이스 복사본이 NetApp 스토리지에 있는 경우 전체 상태 열에 보호되지 않음이 표시됩니다.

NetApp 스토리지 유형이 아닌 데이터베이스에서는 데이터 보호 작업을 수행할 수 없습니다.

- 데이터베이스가 NetApp 스토리지에 있고 보호되지 않은 경우, 전체 상태 열에 '보호되지 않음'이 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되는 경우 사용자 인터페이스의 전체 상태 열에 백업이 실행되지 않았습니더라는 메시지가 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되어 있으며 데이터베이스에 대한 백업이 트리거되면 사용자 인터페이스의 전체 상태 열에 백업 성공 메시지가 표시됩니다.

Exchange Server 데이터베이스에 대한 백업 정책 만들기

SnapCenter 사용하여 Microsoft Exchange Server 리소스를 백업하기 전에 Exchange 리소스 또는 리소스 그룹에 대한 백업 정책을 만들거나, 리소스 그룹을 만들거나 단일 리소스를 백업할 때 백업 정책을 만들 수 있습니다.

시작하기 전에

- 데이터 보호 전략을 정의해야 합니다.

자세한 내용은 Exchange 데이터베이스에 대한 데이터 보호 전략 정의에 대한 정보를 참조하세요.

- SnapCenter 설치, 호스트 추가, 리소스 식별, 스토리지 시스템 연결 생성 등의 작업을 완료하여 데이터 보호를 준비했어야 합니다.
- Exchange Server 리소스를 새로 고침(검색)했어야 합니다.
- 스냅샷을 미리 또는 볼트에 복제하는 경우 SnapCenter 관리자가 소스 볼륨과 대상 볼륨 모두에 대한 스토리지 가상 머신(SVM)을 할당해야 합니다.
- PowerShell 스크립트를 prescripts 및 postscripts로 실행하려면 다음 값을 설정해야 합니다.
usePowershellProcessforScripts 매개변수를 true로 설정 web.config 파일.

기본값은 false입니다.

- SnapMirror Active Sync의 특정 전제 조건과 제한 사항을 검토하세요. 자세한 내용은 다음을 참조하세요.
["SnapMirror Active Sync에 대한 개체 제한"](#).

이 작업에 관하여

- 백업 정책은 백업을 관리하고 보관하는 방법과 리소스 또는 리소스 그룹을 백업하는 빈도를 제어하는 일련의 규칙입니다. 또한 스크립트 설정을 지정할 수 있습니다. 정책에서 옵션을 지정하면 다른 리소스 그룹에 정책을 재사용할 때 시간을 절약할 수 있습니다.
- 전체 백업 보존은 주어진 정책에 따라 달라집니다. 전체 백업 보존 기간이 4인 정책 A를 사용하는 데이터베이스 또는 리소스는 전체 백업을 4개 보존하고, 보존 기간이 3인 동일한 데이터베이스 또는 리소스에 대한 정책 B에는 영향을 미치지 않습니다. 정책 B는 전체 백업을 3개 보존할 수 있습니다.

- 로그 백업 보존은 모든 정책에 적용되며, 데이터베이스나 리소스에 대한 모든 로그 백업에 적용됩니다. 따라서 정책 B를 사용하여 전체 백업을 수행하는 경우 로그 보존 설정은 동일한 데이터베이스 또는 리소스에서 정책 A가 생성한 로그 백업에 영향을 미칩니다. 마찬가지로, 정책 A에 대한 로그 보존 설정은 동일한 데이터베이스에서 정책 B가 생성한 로그 백업에 영향을 미칩니다.
- SCRIPTS_PATH는 플러그인 호스트의 SMCoreServiceHost.exe.Config 파일에 있는 PredefinedWindowsScriptsDirectory 키를 사용하여 정의됩니다.

필요한 경우 이 경로를 변경하고 SMcore 서비스를 다시 시작할 수 있습니다. 보안을 위해 기본 경로를 사용하는 것이 좋습니다.

키 값은 API를 통해 swagger에서 표시될 수 있습니다: API /4.7/configsettings

GET API를 사용하여 키 값을 표시할 수 있습니다. SET API는 지원되지 않습니다.

모범 사례: 전체적으로 보존하려는 전체 및 로그 백업의 수에 따라 보조 보존 정책을 구성하는 것이 가장 좋습니다. 보조 보존 정책을 구성할 때 데이터베이스와 로그가 서로 다른 볼륨에 있는 경우 각 백업에 스냅샷이 3개 있을 수 있고, 데이터베이스와 로그가 동일한 볼륨에 있는 경우 각 백업에 스냅샷이 2개 있을 수 있다는 점을 명심하세요.

- SnapLock
 - '특정 기간 동안 백업 사본을 보관합니다' 옵션을 선택한 경우 SnapLock 보관 기간은 언급된 보관 기간보다 짧거나 같아야 합니다.

스냅샷 잠금 기간을 지정하면 보존 기간이 만료될 때까지 스냅샷이 삭제되지 않습니다. 이를 통해 정책에 지정된 수보다 더 많은 수의 스냅샷을 보존할 수 있습니다.

ONTAP 9.12.1 이하 버전의 경우 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *정책*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 이름 페이지에서 정책 이름과 세부 정보를 입력합니다.
5. 백업 유형 및 복제 페이지에서 다음 단계를 수행합니다.

a. 백업 유형을 선택하세요:

만약 당신이 원한다면...	이렇게 하세요...
데이터베이스 파일과 필요한 트랜잭션 로그를 백업하세요.	*전체 백업 및 로그 백업*을 선택하세요. 데이터베이스는 로그 잘라내기를 통해 백업되며, 잘린 로그를 포함한 모든 로그가 백업됩니다.  이는 권장되는 백업 유형입니다.

만약 당신이 원한다면...	이렇게 하세요...
데이터베이스 파일과 커밋되지 않은 트랜잭션 로그를 백업합니다.	*전체 백업*을 선택하세요. 데이터베이스는 로그 잘림을 통해 백업되고, 잘린 로그는 백업되지 않습니다.
모든 거래 로그를 백업하세요	*로그 백업*을 선택하세요. 활성 파일 시스템의 모든 트랜잭션 로그가 백업되고 로그가 잘리지 않습니다. 라이브 로그와 동일한 디스크에 <i>scebackupinfo</i> 디렉토리가 생성됩니다. 이 디렉토리에는 Exchange 데이터베이스의 증분 변경 사항에 대한 포인터가 포함되어 있으며 전체 로그 파일과 동일하지 않습니다.
트랜잭션 로그 파일을 잘라내지 않고 모든 데이터베이스 파일과 트랜잭션 로그를 백업합니다.	*백업 복사*를 선택하세요. 모든 데이터베이스와 모든 로그가 백업되며, 로그가 잘리지 않습니다. 일반적으로 이 백업 유형은 복제본을 다시 시드하거나 문제를 테스트 또는 진단하는 데 사용됩니다.



최신(UTM) 보존 기간이 아닌 전체 백업 보존 기간을 기준으로 로그 백업에 필요한 공간을 정의해야 합니다.



Exchange 볼륨(LUN)을 처리할 때 로그와 데이터베이스에 대해 별도의 볼트 정책을 만들고, 동일한 레이블을 사용하여 로그 정책의 유지(보존)를 각 레이블의 두 배로 설정합니다. 자세한 내용은 다음을 참조하세요. ["Exchange 백업용 SnapCenter Vault 대상 로그 볼륨에 있는 스냅샷의 절반만 보관합니다."](#)

b. 데이터베이스 가용성 그룹 설정 섹션에서 다음 작업을 선택합니다.

이 분야에서는...	이렇게 하세요...
활성 사본 백업	선택한 데이터베이스의 활성 복사본만 백업하려면 이 옵션을 선택하세요. DAG(데이터베이스 가용성 그룹)의 경우 이 옵션은 DAG에 있는 모든 데이터베이스의 활성 복사본만 백업합니다. 수동 사본은 백업되지 않습니다.

이 분야에서는...	이렇게 하세요...
백업 작업 생성 시 선택할 서버에 백업 사본을 저장합니다.	선택한 서버의 데이터베이스 사본(활성 및 수동 모두)을 백업하려면 이 옵션을 선택하세요. DAG의 경우 이 옵션은 선택한 서버의 모든 데이터베이스의 활성 및 수동 복사본을 모두 백업합니다.



클러스터 구성에서 백업은 정책에 설정된 보존 설정에 따라 클러스터의 각 노드에 보존됩니다. 클러스터의 소유자 노드가 변경되면 이전 소유자 노드의 백업이 보존됩니다. 보존은 노드 수준에서만 적용됩니다.

c. 일정 빈도 섹션에서 다음 중 하나 이상의 빈도 유형을 선택합니다. 주문형, 시간별, 일별, 주별, 월별.



리소스 그룹을 생성하는 동안 백업 작업에 대한 일정(시작 날짜, 종료 날짜)을 지정할 수 있습니다. 이를 통해 동일한 정책과 백업 빈도를 공유하는 리소스 그룹을 만들 수 있지만, 각 정책에 다른 백업 일정을 할당할 수 있습니다.



오전 2시로 예약한 경우, 일광 절약 시간제(DST) 기간에는 일정이 실행되지 않습니다.

a. 정책 라벨을 선택합니다.



원격 복제를 위해 기본 스냅샷에 SnapMirror 레이블을 할당하면 기본 스냅샷이 SnapCenter에서 ONTAP 보조 시스템으로 스냅샷 복제 작업을 오프로드할 수 있습니다. 정책 페이지에서 SnapMirror 또는 SnapVault 옵션을 활성화하지 않고도 이 작업을 수행할 수 있습니다.

b. 보조 복제 옵션 선택 섹션에서 다음 보조 복제 옵션 중 하나 또는 둘 다를 선택합니다.

이 분야에서는...	이렇게 하세요...
로컬 스냅샷을 생성한 후 SnapMirror 업데이트	백업 세트의 미러 복사본을 다른 볼륨(SnapMirror)에 보관하려면 이 옵션을 선택하세요. 2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. SnapMirror Active Sync의 경우 이 옵션을 활성화해야 합니다.  Exchange ONTAP 볼륨에 대해 SnapMirror 활성 동기화가 설정된 경우 기본 전용 정책을 사용할 수 없습니다. SnapCenter 이를 허용하지 않습니다. "미러" 옵션을 활성화해야 합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고침됩니다. 보다 "토폴로지 페이지에서 Exchange 백업 보기" .
로컬 스냅샷을 생성한 후 SnapVault 업데이트	디스크 간 백업 복제를 수행하려면 이 옵션을 선택하세요.
오류 재시도 횟수	프로세스가 중단되기 전에 발생해야 하는 복제 시도 횟수를 입력합니다.



보조 저장소의 스냅샷 최대 한도에 도달하지 않도록 하려면 ONTAP 에서 보조 저장소 SnapMirror 보존 정책을 구성해야 합니다.

6. 보존 페이지에서 보존 설정을 구성합니다.

표시되는 옵션은 이전에 선택한 백업 유형과 빈도 유형에 따라 달라집니다.



최대 보존 값은 1018입니다. 보존 기간이 기본 ONTAP 버전에서 지원하는 것보다 높은 값으로 설정된 경우 백업이 실패합니다.



SnapVault 복제를 활성화하려면 보존 횟수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷이 대상에 복제될 때까지 첫 번째 스냅샷이 SnapVault 관계에 대한 참조 스냅샷이 되기 때문에 보존 작업이 실패할 수 있습니다.

a. 로그 백업 보존 설정 섹션에서 다음 중 하나를 선택하세요.

만약 당신이 원한다면...	이렇게 하세요...
특정 수의 로그 백업만 보관	*로그를 보관할 전체 백업 수*를 선택하고 최신 복원 기능을 원하는 전체 백업 수를 지정합니다. 최신(UTM) 보존은 전체 백업이나 로그 백업을 통해 생성된 로그 백업에 적용됩니다. 예를 들어, UTM 보존 설정이 마지막 5개 전체 백업의 로그 백업을 보존하도록 구성된 경우 마지막 5개 전체 백업의 로그 백업이 보존됩니다. 전체 백업과 로그 백업의 일부로 생성된 로그 폴더는 UTM의 일부로 자동으로 삭제됩니다. 로그 폴더를 수동으로 삭제할 수 없습니다. 예를 들어, 전체 또는 전체 및 로그 백업의 보존 설정이 1개월로 설정되고 UTM 보존 기간이 10일로 설정된 경우, 이러한 백업의 일부로 생성된 로그 폴더는 UTM에 따라 삭제됩니다. 결과적으로 10일 분량의 로그 폴더만 남게 되고 다른 모든 백업은 특정 시점 복원으로 표시됩니다. 최신 복원을 수행하지 않으려면 UTM 보존 값을 0으로 설정할 수 있습니다. 이를 통해 특정 시점의 복원 작업이 가능해집니다. 모범 사례: 전체 백업 보존 설정 섹션의 전체 스냅샷(전체 백업) 설정과 동일하게 설정하는 것이 가장 좋습니다. 이렇게 하면 전체 백업마다 로그 파일이 보존됩니다.
백업 사본을 특정 일수 동안 보관합니다.	마지막으로 로그 백업 보관 옵션을 선택하고 로그 백업 사본을 보관할 일 수를 지정합니다. 전체 백업의 일수만큼의 로그 백업이 보존됩니다.
스냅샷 잠금 기간	*스냅샷 복사 잠금 기간*을 선택하고 일, 월 또는 년을 선택합니다. SnapLock 보존 기간은 100년 미만이어야 합니다.

백업 유형으로 *로그 백업*을 선택한 경우, 로그 백업은 전체 백업에 대한 최신 보존 설정의 일부로 보존됩니다.

- b. 전체 백업 보존 설정 섹션에서 주문형 백업의 경우 다음 중 하나를 선택한 다음, 전체 백업의 경우 하나를 선택합니다.

이 분야에서는...	이렇게 하세요...
특정 수의 스냅샷만 보관	보관할 전체 백업의 수를 지정하려면 보관할 총 스냅샷 사본 옵션을 선택하고 보관할 스냅샷(전체 백업)의 수를 지정합니다. 전체 백업의 수가 지정된 수를 초과하는 경우, 지정된 수를 초과하는 전체 백업이 삭제되고, 가장 오래된 복사본이 먼저 삭제됩니다.
특정 기간 동안 전체 백업을 보관합니다.	스냅샷 복사본 보관 기간 옵션을 선택하고 스냅샷(전체 백업)을 보관할 일수를 지정합니다.
기본 스냅샷 잠금 기간	*기본 스냅샷 복사 잠금 기간*을 선택하고 일, 월 또는 년을 선택합니다. SnapLock 보존 기간은 100년 미만이어야 합니다.
2차 스냅샷 잠금 기간	*보조 스냅샷 복사 잠금 기간*을 선택하고 일, 월 또는 년을 선택합니다.

DAG 구성의 호스트에 로그 백업만 있고 전체 백업이 없는 데이터베이스가 있는 경우 로그 백업은 다음과 같은 방식으로 보관됩니다.

- 기본적으로 SnapCenter DAG의 다른 모든 호스트에서 이 데이터베이스에 대한 가장 오래된 전체 백업을 찾고, 전체 백업 이전에 수행된 이 호스트의 모든 로그 백업을 삭제합니다.
- DAG에 있는 호스트의 데이터베이스에 대해 로그 백업만 있는 경우 위의 기본 보존 동작을 재정의하려면 `C:\Program Files\NetApp\SnapCenter WebApp\web.config` 파일에 **MaxLogBackupOnlyCountWithoutFullBackup** 키를 추가합니다.

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

이 예에서 값 10은 호스트에 최대 10개의 로그 백업을 보관한다는 것을 의미합니다.

7. 스크립트 페이지에서 백업 작업 전이나 후에 실행해야 하는 프리스크립트나 포스트스크립트의 경로와 인수를 각각 입력합니다.

- 사전 스크립트 백업 인수에는 "\$Database"와 "\$ServerInstance"가 포함됩니다.
- Postscript 백업 인수에는 "\$Database", "\$ServerInstance", "\$BackupName", "\$LogDirectory", "\$LogSnapshot"이 포함됩니다.

스크립트를 실행하여 SNMP 트랩을 업데이트하고, 알림을 자동화하고, 로그를 보내는 등의 작업을 수행할 수 있습니다.



prescripts 또는 postscripts 경로에는 드라이브나 공유가 포함되어서는 안 됩니다. 경로는 SCRIPTS_PATH를 기준으로 해야 합니다.

8. 요약을 검토한 후 *마침*을 클릭하세요.

Exchange Server에 대한 리소스 그룹 생성 및 정책 첨부

모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한, 수행하려는 데이터 보호 작업 유형과 보호 일정을 정의하기 위해 리소스 그룹에 하나 이상의 정책을 연결해야 합니다.

이 작업에 관하여

- SCRIPTS_PATH는 플러그인 호스트의 SMCoreServiceHost.exe.Config 파일에 있는 PredefinedWindowsScriptsDirectory 키를 사용하여 정의됩니다.

필요한 경우 이 경로를 변경하고 SMcore 서비스를 다시 시작할 수 있습니다. 보안을 위해 기본 경로를 사용하는 것이 좋습니다.

키 값은 API를 통해 swagger에서 표시될 수 있습니다: API /4.7/configsettings

GET API를 사용하여 키 값을 표시할 수 있습니다. SET API는 지원되지 않습니다.

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.
- SnapMirror 활성화 동기화가 있는 리소스가 포함된 기존 리소스 그룹에 SnapMirror 활성화 동기화 SnapMirror 없는 새 데이터베이스를 추가하는 것은 지원되지 않습니다.
- SnapMirror Active Sync의 장애 조치 모드에서 기존 리소스 그룹에 새 데이터베이스를 추가하는 것은 지원되지 않습니다. 일반 상태나 장애 복구 상태에서만 리소스 그룹에 리소스를 추가할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 Microsoft Exchange Server 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *데이터베이스*를 선택합니다.



최근에 SnapCenter 에 리소스를 추가한 경우, *리소스 새로 고침*을 클릭하여 새로 추가된 리소스를 확인하세요.

3. *새 리소스 그룹*을 클릭합니다.
4. 이름 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	리소스 그룹 이름을 입력하세요.  리소스 그룹 이름은 250자를 넘을 수 없습니다.

이 분야에서는...	이렇게 하세요...
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력하세요. 예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.
스냅샷 복사에 사용자 정의 이름 형식 사용	선택 사항: 사용자 지정 스냅샷 이름과 형식을 입력합니다. 예를 들어, <code>customtext_resourcegroup_policy_hostname</code> 또는 <code>_resourcegroup_hostname</code>입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

5. 리소스 페이지에서 다음 단계를 수행합니다.

- a. 사용 가능한 리소스 목록을 필터링하려면 드롭다운 목록에서 리소스 유형과 데이터베이스 가용성 그룹을 선택하세요.



최근에 리소스를 추가한 경우 리소스 목록을 새로 고친 후에만 사용 가능한 리소스 목록에 표시됩니다.

사용 가능한 리소스 및 선택한 리소스 섹션에서는 데이터베이스 이름이 호스트의 FQDN과 함께 표시됩니다. 이 FQDN은 해당 데이터베이스가 특정 호스트에서 활성화되어 있으며 이 호스트에서 백업을 수행하지 않을 수도 있음을 나타냅니다. 정책에서 백업 작업 생성 시 선택할 서버에 복사본 백업 옵션을 선택한 경우, 백업을 수행할 서버 선택 옵션에서 하나 이상의 백업 서버를 선택해야 합니다.

- b. 검색 텍스트 상자에 리소스 이름을 입력하거나 스크롤하여 리소스를 찾으세요.
- c. 사용 가능한 리소스 섹션에서 선택한 리소스 섹션으로 리소스를 이동하려면 다음 단계 중 하나를 수행합니다.
- 동일한 볼륨에 있는 모든 리소스를 선택한 리소스 섹션으로 이동하려면 *동일한 저장소 볼륨에 있는 모든 리소스 자동 선택*을 선택합니다.
 - 사용 가능한 리소스 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 클릭하여 선택한 리소스 섹션으로 이동합니다.

Microsoft Exchange Server용 SnapCenter의 리소스 그룹은 스냅샷당 30개를 초과하는 데이터베이스를 가질 수 없습니다. 하나의 리소스 그룹에 30개가 넘는 데이터베이스가 있는 경우 추가 데이터베이스에 대한 두 번째 스냅샷이 생성됩니다. 따라서 기본 백업 작업 아래에 2개의 하위 작업이 생성됩니다. 2차 복제가 있는 백업의 경우 SnapMirror 또는 SnapVault 업데이트가 진행되는 동안 두 하위 작업에 대한 업데이트가 겹치는 시나리오가 발생할 수 있습니다. 로그에 작업이 완료되었다고 표시되어 있어도 주 백업 작업은 계속해서 실행됩니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다. *.



정책에 백업 작업 생성 시 선택할 서버에 복사본 백업 옵션이 포함되어 있는 경우 하나 이상의 서버를 선택할 수 있는 서버 선택 옵션이 표시됩니다. 서버 선택 옵션은 NetApp 스토리지에서 선택한 데이터베이스가 있는 서버만 나열합니다.

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

- b. 선택한 정책에 대한 일정 구성 섹션에서  * 일정을 구성하려는 정책의 *일정 구성 열에 있습니다.
- c. 정책 _정책_이름_에 대한 일정 추가 대화 상자에서 시작 날짜, 만료 날짜, 빈도를 지정하여 일정을 구성한 다음 *확인*을 클릭합니다.

정책에 나열된 각 주파수에 대해 이 작업을 수행해야 합니다. 구성된 일정은 '선택한 정책에 대한 일정 구성' 섹션의 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

7. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.

이메일 알림의 경우 GUI 또는 PowerShell 명령을 사용하여 SMTP 서버 세부 정보를 지정해야 합니다. `Set-SmSmtServer`.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

8. 요약 검토 후 *마침*을 클릭하세요.

PowerShell cmdlet을 사용하여 Exchange Server용 스토리지 시스템 연결 및 자격 증명 만들기

PowerShell cmdlet을 사용하여 백업하고 복원하기 전에 SVM(스토리지 가상 머신) 연결과 자격 증명을 만들어야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 저장소 연결을 생성하려면 인프라 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

스토리지 시스템 연결을 추가하는 동안에는 호스트 플러그인 설치가 진행 중이어서는 안 됩니다. 호스트 캐시가 업데이트되지 않고 SnapCenter GUI에 데이터베이스 상태가 "백업에 사용할 수 없음" 또는 "NetApp 스토리지에 없음"으로 표시될 수 있기 때문입니다.

- 저장 시스템 이름은 고유해야 합니다.

SnapCenter 서로 다른 클러스터에 동일한 이름을 가진 여러 스토리지 시스템을 지원하지 않습니다. SnapCenter에서 지원하는 각 스토리지 시스템은 고유한 이름과 고유한 데이터 LIF IP 주소를 가져야 합니다.

단계

1. 다음을 사용하여 PowerShell 연결 세션을 시작합니다. `Open-SmConnection cmdlet`.

이 예제에서는 PowerShell 세션을 엽니다.

```
PS C:\> Open-SmConnection
```

2. 다음을 사용하여 스토리지 시스템에 대한 새 연결을 만듭니다. `Add-SmStorageConnection cmdlet`.

이 예제에서는 새로운 스토리지 시스템 연결을 만듭니다.

```
PS C:\> Add-SmStorageConnection -SVM test_vs1 -Protocol Https  
-Timeout 60
```

3. 다음을 사용하여 새 실행 계정을 만듭니다. `Add-Credential cmdlet`.

이 예제에서는 Windows 자격 증명을 사용하여 ExchangeAdmin이라는 새 실행 계정을 만듭니다.

```
PS C:> Add-SmCredential -Name ExchangeAdmin -AuthMode Windows  
-Credential sddev\administrator
```

`cmdlet`과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

Exchange 데이터베이스 백업

데이터베이스가 어떤 리소스 그룹에도 속하지 않은 경우 리소스 페이지에서 데이터베이스나 데이터베이스 가용성 그룹을 백업할 수 있습니다.

시작하기 전에

- 백업 정책을 생성했어야 합니다.
- 백업 작업에 사용되는 집계를 데이터베이스에서 사용하는 SVM에 할당했어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 역할에 "snapmirror all" 권한이 포함되어야 합니다. 하지만 "vsadmin" 역할을 사용하는 경우 "snapmirror all" 권한은 필요하지 않습니다.
- NetApp 및 비 NetApp 스토리지에서 활성/수동 데이터베이스 복사본이 있는 데이터베이스 또는 데이터베이스 가용성 그룹의 백업을 수행하려는 경우, 정책에서 활성 복사본 백업 또는 백업 작업 생성 시간 동안 선택할 서버의 복사본 백업 옵션을 선택한 경우, 백업 작업은 경고 상태로 전환됩니다. NetApp 스토리지의 활성/수동 데이터베이스 복사에 대한 백업은 성공하고, NetApp 아닌 스토리지의 활성/수동 데이터베이스 복사에 대한 백업은 실패합니다.

모범 사례: 활성 및 수동 데이터베이스의 백업을 동시에 실행하지 마세요. 경쟁 조건이 발생하여 백업 중 하나가 실패할 수 있습니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 *Microsoft Exchange Server 플러그인*을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 데이터베이스 또는 *데이터베이스 가용성 그룹*을 선택합니다.

리소스 페이지에서  아이콘은 데이터베이스가 NetApp 스토리지가 아닌 다른 스토리지에 있음을 나타냅니다.



DAG에서 활성 데이터베이스 복사본이 NetApp 스토리지가 아닌 스토리지에 있고 최소 하나의 수동 데이터베이스 복사본이 NetApp 스토리지에 있는 경우 데이터베이스를 보호할 수 있습니다.

*를 클릭하세요  *를 선택한 다음 호스트 이름과 데이터베이스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 *를 클릭할 수 있습니다.  * 필터 창을 닫습니다.

- 데이터베이스를 백업하려면 데이터베이스 이름을 클릭하세요.
 - i. 토폴로지 보기가 표시되면 *보호*를 클릭합니다.
 - ii. 데이터베이스 - 리소스 보호 마법사가 표시되면 3단계로 진행합니다.
 - 데이터베이스 가용성 그룹을 백업하려면 데이터베이스 가용성 그룹 이름을 클릭합니다.
3. 사용자 지정 스냅샷 이름을 지정하려면 리소스 페이지에서 스냅샷 복사에 사용자 지정 이름 형식 사용 확인란을 선택한 다음 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, *customtext_policy_hostname* 또는 *_resource_hostname_*입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

4. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다.  *.



정책에 백업 작업 생성 시 선택할 서버에 복사본 백업 옵션이 포함되어 있는 경우 하나 이상의 서버를 선택할 수 있는 서버 선택 옵션이 표시됩니다. 서버 선택 옵션은 NetApp 스토리지에서 선택한 데이터베이스가 있는 서버만 나열합니다.

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

- b. *를 클릭하세요  * 일정을 구성하려는 정책에 대한 일정 구성 옆에 있습니다.
- c. 정책 *_policy_name_*에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 *_policy_name_*은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 옆에 나열됩니다.

- 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스에서 수행된 백업 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtplibServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

- 요약을 검토한 후 *마침*을 클릭하세요.

데이터베이스 토폴로지 페이지가 표시됩니다.

- *지금 백업*을 클릭하세요.

- 백업 페이지에서 다음 단계를 수행합니다.

- 리소스에 여러 정책을 적용한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- *백업*을 클릭하세요.

- 페이지 하단의 활동 창에서 작업을 두 번 클릭하여 작업 세부 정보 페이지를 표시하여 백업 진행 상황을 모니터링합니다.

- MetroCluster 구성에서 SnapCenter 장애 조치 후 보호 관계를 감지하지 못할 수 있습니다.

자세한 내용은 다음을 참조하세요. "[MetroCluster 장애 조치 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다.](#)"

- VMDK에서 애플리케이션 데이터를 백업하고 SnapCenter Plug-in for VMware vSphere의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다.

Java 힙 크기를 늘리려면 스크립트 파일 `/opt/netapp/init_scripts/scvservice`를 찾으세요. 해당 스크립트에서 `_do_start` 메서드 명령은 SnapCenter VMware 플러그인 서비스를 시작합니다. 해당 명령을 다음으로 업데이트하세요: `Java -jar -Xmx8192M -Xms4096M`

PowerShell cmdlet

단계

- Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-smconnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.

- Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.

이 예제에서는 전체 백업 및 로그 백업 Exchange 백업 유형을 사용하여 새 백업 정책을 만듭니다.


```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies
```

이 예제에서는 매시간 전체 백업과 로그 백업 Exchange 백업 유형을 사용하여 새 백업 정책을 만듭니다.

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Hourly_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies -ScheduleType Hourly
-RetentionSettings
@{'BackupType'='DATA'; 'ScheduleType'='Hourly'; 'RetentionCount'='10'}
```

이 예제에서는 Exchange 로그만 백업하는 새 백업 정책을 만듭니다.

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

3. Get-SmResources cmdlet을 사용하여 호스트 리소스를 검색합니다.

이 예제에서는 지정된 호스트에서 Microsoft Exchange Server 플러그인에 대한 리소스를 검색합니다.

```
C:\PS> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCE
```

4. Add-SmResourceGroup cmdlet을 사용하여 SnapCenter 에 새 리소스 그룹을 추가합니다.

이 예제에서는 지정된 정책과 리소스를 사용하여 새 Exchange Server 데이터베이스 백업 리소스 그룹을 만듭니다.

```
C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
-Description 'Backup ResourceGroup with Full and Log backup policy'
-PluginCode SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bkp_Policy
-Resources @{'Host'='sce-w2k12-exch'; 'Type'='Exchange Database'; 'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

이 예제에서는 지정된 정책과 리소스를 사용하여 새 Exchange 데이터베이스 가용성 그룹(DAG) 백업 리소스 그룹을 만듭니다.

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description  
'Backup ResourceGroup with Full and Log backup policy' -PluginCode  
SCE -Policies  
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Lo  
g_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database  
Availability Group";"Names"="DAGSCE0102"}
```

5. New-SmBackup cmdlet을 사용하여 새로운 백업 작업을 시작합니다.

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy  
SCE_w2k12_Full_Log_bkp_Policy
```

이 예제에서는 보조 저장소에 새 백업을 만듭니다.

```
New-SMBackup -DatasetName ResourceGroup1 -Policy  
Secondary_Backup_Policy4
```

6. Get-SmBackupReport cmdlet을 사용하여 백업 작업의 상태를 확인합니다.

이 예제에서는 지정된 날짜에 실행된 모든 작업에 대한 작업 요약 보고서를 표시합니다.

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

이 예에서는 특정 작업 ID에 대한 작업 요약 보고서를 표시합니다.

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조하세요. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

Exchange 리소스 그룹 백업

리소스 그룹은 호스트 또는 Exchange DAG에 있는 리소스의 모음이며, 리소스 그룹에는 전체 DAG 또는 개별 데이터베이스가 포함될 수 있습니다. 리소스 페이지에서 리소스 그룹을 백업할 수 있습니다.

시작하기 전에

- 정책이 첨부된 리소스 그룹을 만들어야 합니다.
- 백업 작업에 사용되는 집계를 데이터베이스에서 사용하는 스토리지 가상 머신(SVM)에 할당했어야 합니다.

- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 역할에 “snapmirror all” 권한이 포함되어야 합니다. 하지만 “vsadmin” 역할을 사용하는 경우 “snapmirror all” 권한은 필요하지 않습니다.
- 리소스 그룹에 서로 다른 호스트의 여러 데이터베이스가 있는 경우 네트워크 문제로 인해 일부 호스트의 백업 작업이 늦게 시작될 수 있습니다. 값을 구성해야 합니다. MaxRetryForUninitializedHosts ~에 web.config 를 사용하여 Set-SmConfigSettings PowerShell cmdlet.
- 리소스 그룹에서 NetApp 및 비 NetApp 스토리지에 활성/수동 데이터베이스 복사본이 있는 데이터베이스 또는 데이터베이스 가용성 그룹을 포함하고 정책에서 활성 복사본 백업 또는 백업 작업 생성 시간 동안 선택할 서버에 복사본 백업 옵션을 선택한 경우 백업 작업이 경고 상태로 전환됩니다.

NetApp 스토리지의 활성/수동 데이터베이스 복사에 대한 백업은 성공하고, NetApp 아닌 스토리지의 활성/수동 데이터베이스 복사에 대한 백업은 실패합니다.

이 작업에 관하여

리소스 페이지에서 필요에 따라 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 첨부되고 일정이 구성된 경우 백업은 일정에 따라 자동으로 수행됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 *Microsoft Exchange Server 플러그인*을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.

검색창에 리소스 그룹 이름을 입력하거나 *를 클릭하여 리소스 그룹을 검색할 수 있습니다.  *를 클릭한 다음 태그를 선택합니다. 그런 다음 *를 클릭할 수 있습니다.  * 필터 창을 닫습니다.

3. 리소스 그룹 페이지에서 백업하려는 리소스 그룹을 선택한 다음, *지금 백업*을 클릭합니다.
4. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스 그룹에 여러 정책을 연결한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. *백업*을 클릭하세요.

5. 페이지 하단의 활동 창에서 작업을 두 번 클릭하여 작업 세부 정보 페이지를 표시하여 백업 진행 상황을 모니터링합니다.

백업 작업 모니터링

SnapCenterJobs 페이지를 사용하여 다양한 백업 작업의 진행 상황을 모니터링할 수 있습니다. 완료 시점이나 문제가 있는지 확인하기 위해 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 해당 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한

-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  백업 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *백업*을 선택합니다.
 - d. 상태 드롭다운에서 백업 상태를 선택합니다.
 - e. *적용*을 클릭하면 작업이 성공적으로 완료된 것을 볼 수 있습니다.
4. 백업 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인하세요.



백업 작업 상태가 표시됩니다.  작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 표시가 되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

활동 창에서 작업 모니터링

활동 창에는 가장 최근에 수행된 5개의 작업이 표시됩니다. 활동 창에는 작업이 시작된 시점과 작업 상태도 표시됩니다.

활동 창에는 백업, 복원, 복제 및 예약된 백업 작업에 대한 정보가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 딸깍 하는 소리  활동 창에서 가장 최근의 작업 5개를 확인하세요.

작업 중 하나를 클릭하면 작업 세부 정보가 작업 세부 정보 페이지에 나열됩니다.

Exchange 데이터베이스에 대한 백업 작업 취소

대기 중인 백업 작업을 취소할 수 있습니다.

필요한 것

- 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 모니터 페이지나 활동 창에서 백업 작업을 취소할 수 있습니다.

- 실행 중인 백업 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 백업 작업을 취소할 수 있습니다.
- 취소할 수 없는 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자\그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 백업 작업을 취소할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	a. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. b. 작업을 선택한 다음 *작업 취소*를 클릭합니다.
활동 창	a. 백업 작업을 시작한 후 *를 클릭하세요.  * 활동 창에서 가장 최근의 작업 5개를 확인하세요. b. 작업을 선택하세요. c. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

작업이 취소되고 리소스는 이전 상태로 돌아갑니다.

토폴로지 페이지에서 **Exchange** 백업 보기

리소스를 백업할 준비를 할 때 기본 및 보조 저장소의 모든 백업을 그래픽으로 표현해 보면 도움이 될 수 있습니다.

이 작업에 관하여

토폴로지 페이지에서는 선택한 리소스 또는 리소스 그룹에 사용 가능한 모든 백업을 볼 수 있습니다. 해당 백업의 세부 정보를 보고, 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

다음 아이콘을 '사본 관리' 보기에서 검토하여 백업을 기본 저장소 또는 보조 저장소(미러 사본 또는 볼트 사본)에서 사용할 수 있는지 확인할 수 있습니다.

-  기본 저장소에서 사용 가능한 백업 수를 표시합니다.
-  SnapMirror 기술을 사용하여 보조 저장소에 미러링된 백업 수를 표시합니다.
-  SnapVault 기술을 사용하여 보조 저장소에 복제된 백업 수를 표시합니다.
 - 표시된 백업 수에는 보조 저장소에서 삭제된 백업이 포함됩니다.

예를 들어, 4개의 백업만 보존하는 정책을 사용하여 6개의 백업을 만든 경우 표시되는 백업 수는 6개입니다.

모범 사례: 복제된 백업의 올바른 수가 표시되도록 하려면 토폴로지를 새로 고치는 것이 좋습니다.

SnapMirror Active Sync(처음에는 SnapMirror Business Continuity[SM-BC]로 출시됨)라는 보조 관계가 있는 경우 다음과 같은 추가 아이콘을 볼 수 있습니다.

-  복제 사이트가 오픈되었습니다.
-  복제 사이트가 다운되었습니다.
-  2차 거울이나 볼트 관계가 재설정되지 않았습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 데이터베이스, 리소스 또는 리소스 그룹을 선택합니다.
3. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 리소스를 선택합니다.

리소스가 보호된 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. 요약 카드 섹션을 검토하여 기본 및 보조 저장소에서 사용 가능한 백업 수에 대한 요약を確認하세요.

요약 카드 섹션에는 총 백업 수와 총 로그 백업 수가 표시됩니다.

새로 고침 버튼을 클릭하면 저장소에 대한 쿼리가 시작되어 정확한 개수가 표시됩니다.

SnapLock 이 활성화된 백업을 수행한 경우 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간이 새로 고쳐집니다. 주간 일정은 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간도 새로 고칩니다.

애플리케이션 리소스가 여러 볼륨에 분산되어 있는 경우 백업에 대한 SnapLock 만료 시간은 볼륨의 스냅샷에 설정된 가장 긴 SnapLock 만료 시간이 됩니다. 가장 긴 SnapLock 만료 시간은 ONTAP 에서 검색됩니다.

SnapMirror 활성화 동기화의 경우, 새로 고침 버튼을 클릭하면 ONTAP 기본 사이트와 복제 사이트를 모두 쿼리하여 SnapCenter 백업 인벤토리가 새로 고쳐집니다. 주간 일정은 SnapMirror 활성화 동기화 관계가 포함된 모든 데이터베이스에 대해 이 활동을 수행합니다.

- SnapMirror 활성화 동기화 및 ONTAP 9.14.1의 경우에만 장애 조치 후 새 기본 대상에 대한 비동기 미러 또는 비동기 MirrorVault 관계를 수동으로 구성해야 합니다. ONTAP 9.15.1부터 비동기 미러 또는 비동기 미러볼트는 장애 조치 후 새로운 기본 대상으로 자동 구성됩니다.
- 장애 조치 후에는 SnapCenter 에서 장애 조치를 인식할 수 있도록 백업을 만들어야 합니다. 백업이 생성된 후에만 *새로 고침*을 클릭할 수 있습니다.

5. 복사본 관리 보기에서 기본 또는 보조 저장소의 *백업*을 클릭하면 백업 세부 정보를 볼 수 있습니다.

백업 세부정보는 표 형식으로 표시됩니다.

6. 표에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 이름 바꾸기, 삭제 작업을 수행합니다.



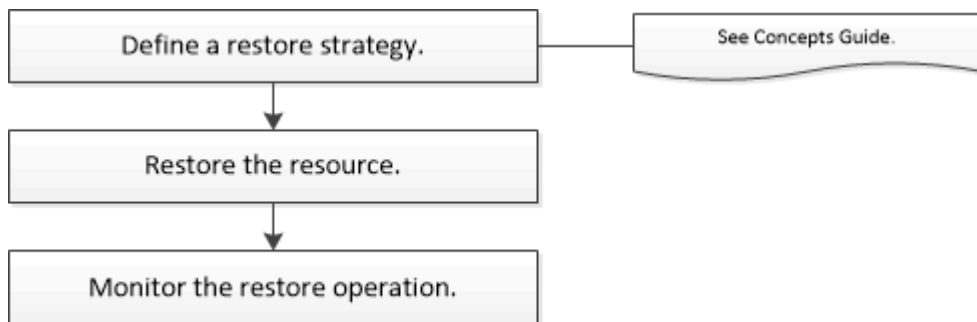
보조 저장소에 있는 백업은 이름을 바꾸거나 삭제할 수 없습니다. 스냅샷 삭제는 ONTAP 보존 설정에 따라 처리됩니다.

Exchange 리소스 복원

워크플로 복원

SnapCenter 사용하면 활성 파일 시스템에 하나 이상의 백업을 복원하여 Exchange 데이터베이스를 복원할 수 있습니다.

다음 워크플로는 Exchange 데이터베이스 복원 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업 및 복원 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 다음을 참조하세요. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

Exchange 데이터베이스 복원을 위한 요구 사항

Microsoft Exchange Server 백업용 SnapCenter 플러그인에서 Exchange Server 데이터베이스를 복원하기 전에 몇 가지 요구 사항이 충족되는지 확인해야 합니다.



복원 기능을 완벽하게 사용하려면 SnapCenter 서버와 Exchange 데이터베이스용 SnapCenter 플러그인을 모두 4.6으로 업그레이드해야 합니다.

- 데이터베이스를 복원하려면 Exchange Server가 온라인 상태이고 실행 중이어야 합니다.
- 데이터베이스는 Exchange Server에 있어야 합니다.



삭제된 데이터베이스 복원은 지원되지 않습니다.

- 데이터베이스에 대한 SnapCenter 일정을 일시 중단해야 합니다.
- SnapCenter 서버와 Microsoft Exchange Server 호스트용 SnapCenter 플러그인은 복원하려는 백업이 들어 있는 기본 및 보조 저장소에 연결되어야 합니다.

Exchange 데이터베이스 복원

SnapCenter 사용하면 백업된 Exchange 데이터베이스를 복원할 수 있습니다.

시작하기 전에

- 리소스 그룹, 데이터베이스 또는 DAG(데이터베이스 가용성 그룹)를 백업해야 합니다.
- Exchange 데이터베이스가 다른 위치로 마이그레이션되면 이전 백업에 대한 복원 작업이 작동하지 않습니다.
- 스냅샷을 미리 또는 볼트에 복제하는 경우 SnapCenter 관리자가 소스 볼륨과 대상 볼륨 모두에 대한 SVM을 할당해야 합니다.
- DAG에서 활성 데이터베이스 복사본이 NetApp 스토리지가 아닌 스토리지에 있고 NetApp 스토리지에 있는 수동 데이터베이스 복사본 백업에서 복원하려는 경우 수동 복사본(NetApp 스토리지)을 활성 복사본으로 만들고 리소스를 새로 고친 다음 복원 작업을 수행합니다.

실행하다 `Move-ActiveMailboxDatabase` 수동 데이터베이스 복사본을 활성 데이터베이스 복사본으로 만드는 명령입니다.

그만큼 "[Microsoft 설명서](#)" 이 명령에 대한 정보가 포함되어 있습니다.

이 작업에 관하여

- 데이터베이스에서 복원 작업을 수행하면 데이터베이스가 동일한 호스트에 다시 마운트되고 새 볼륨이 생성되지 않습니다.
- DAG 수준 백업은 개별 데이터베이스에서 복원해야 합니다.
- Exchange 데이터베이스(.edb) 파일 이외의 파일이 있는 경우 전체 디스크 복원은 지원되지 않습니다.

Exchange용 플러그인은 복제에 사용되는 것과 같은 Exchange 파일이 디스크에 포함되어 있는 경우 디스크에서 전체 복원을 수행하지 않습니다. 전체 복원이 Exchange 기능에 영향을 줄 수 있는 경우 Exchange용 플러그인은 단일 파일 복원 작업을 수행합니다.

- Exchange용 플러그인은 BitLocker로 암호화된 드라이브를 복원할 수 없습니다.
- `SCRIPTS_PATH`는 플러그인 호스트의 `SMCoreServiceHost.exe.Config` 파일에 있는 `PredefinedWindowsScriptsDirectory` 키를 사용하여 정의됩니다.

필요한 경우 이 경로를 변경하고 SMcore 서비스를 다시 시작할 수 있습니다. 보안을 위해 기본 경로를 사용하는 것이 좋습니다.

키 값은 API를 통해 swagger에서 표시될 수 있습니다: `API /4.7/configsettings`

GET API를 사용하여 키 값을 표시할 수 있습니다. SET API는 지원되지 않습니다.

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.
- SnapMirror Active Sync 복원 작업의 경우 기본 위치에서 백업을 선택해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 리소스 페이지의 왼쪽 상단 모서리에 있는 *리소스*를 클릭합니다.
2. 드롭다운 목록에서 Exchange Server 플러그인을 선택합니다.
3. 리소스 페이지의 보기 목록에서 *데이터베이스*를 선택합니다.
4. 목록에서 데이터베이스를 선택하세요.
5. 사본 관리 보기에서 기본 백업 표에서 *백업*을 선택한 다음 *를 클릭합니다.  *.
6. 옵션 페이지에서 다음 로그 백업 옵션 중 하나를 선택하세요.

옵션	설명
모든 로그 백업	*모든 로그 백업*을 선택하면 전체 백업 후 사용 가능한 모든 로그 백업을 복원하기 위해 최신 백업 복원 작업을 수행합니다.
로그 백업까지	 드롭다운 목록에 표시되는 로그 수는 UTM을 기준으로 합니다. 예를 들어, 전체 백업 보존 기간이 5이고 UTM 보존 기간이 3인 경우 사용 가능한 로그 백업 수는 5개이지만 드롭다운에는 복원 작업을 수행할 로그가 3개만 나열됩니다. *로그 백업 기준*을 선택하면 선택한 로그까지의 로그 백업을 기반으로 데이터베이스를 복원하는 지정 시간 복원 작업이 수행됩니다.
특정 날짜까지	복원된 데이터베이스에 트랜잭션 로그가 적용되는 날짜와 시간을 지정하려면 *특정 날짜까지*를 선택합니다. 이 지정 시간 복원 작업은 지정된 날짜와 시간에 마지막 백업까지 기록된 트랜잭션 로그 항목을 복원합니다.
None	로그 백업 없이 전체 백업만 복원해야 하는 경우 *없음*을 선택합니다.

다음 작업 중 하나를 수행할 수 있습니다.

- 복원 후 데이터베이스 복구 및 마운트 - 이 옵션은 기본적으로 선택되어 있습니다.
- 복원 전에 백업에서 트랜잭션 로그의 무결성을 확인하지 마세요 - 기본적으로 SnapCenter 복원 작업을 수행하기 전에 백업에서 트랜잭션 로그의 무결성을 확인합니다.

모범 사례: 이 옵션은 선택하지 마세요.

7. 스크립트 페이지에서 복원 작업 전이나 후에 실행해야 하는 프리스크립트나 포스트스크립트의 경로와 인수를 각각 입력합니다.

복원 사전 스크립트 인수에는 \$Database와 \$ServerInstance가 포함됩니다.

복원 포스트스크립트 인수에는 \$Database, \$ServerInstance, \$BackupName, \$LogDirectory 및 \$TargetServerInstance가 포함됩니다.

스크립트를 실행하여 SNMP 트랩을 업데이트하고, 알림을 자동화하고, 로그를 보내는 등의 작업을 수행할 수 있습니다.



prescripts 또는 postscripts 경로에는 드라이브나 공유가 포함되어서는 안 됩니다. 경로는 SCRIPTS_PATH를 기준으로 해야 합니다.

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

10. 페이지 하단의 활동 패널을 확장하면 복원 작업의 상태를 볼 수 있습니다.

모니터 > 작업 페이지를 사용하여 복원 프로세스를 모니터링해야 합니다.

백업에서 활성 데이터베이스를 복원할 때 복제본과 활성 데이터베이스 사이에 지연이 있는 경우 수동 데이터베이스가 일시 중단 또는 실패 상태로 전환될 수 있습니다.

상태 변경은 활성 데이터베이스의 로그 체인이 포크되어 복제를 중단하는 새로운 분기를 시작할 때 발생할 수 있습니다. Exchange Server는 복제본을 복구하려고 시도하지만 복구할 수 없는 경우 복원 후 새 백업을 만든 다음 복제본을 다시 시드해야 합니다.

PowerShell cmdlet

단계

1. 다음을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다. Open-SmConnection cmdlet.

```
Open-smconnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

2. 다음을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다. Get-SmBackup cmdlet.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
PS C:\> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
-----	-----
341	ResourceGroup_36304978_UTM...
12/8/2017 4:13:24 PM	Full Backup
342	ResourceGroup_36304978_UTM...
12/8/2017 4:16:23 PM	Full Backup
355	ResourceGroup_06140588_UTM...
12/8/2017 6:32:36 PM	Log Backup
356	ResourceGroup_06140588_UTM...
12/8/2017 6:36:20 PM	Full Backup

3. 다음을 사용하여 백업에서 데이터를 복원합니다. Restore-SmBackup cmdlet.

이 예제에서는 최신 백업을 복원합니다.

```
C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341 -IsRecoverMount:$true
```

이 예제에서는 특정 시점 백업을 복원합니다.

```
C:\ PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341 -IsRecoverMount:$true -LogRestoreType ByTransactionLogs -LogCount 2
```

이 예제에서는 보조 저장소의 백업을 기본 저장소로 복원합니다.

```
C:\ PS> Restore-SmBackup -PluginCode 'SCE' -AppObjectId 'DB2' -BackupId 81 -IsRecoverMount:$true -Confirm:$false -archive @{Primary="paw_vs:vol1";Secondary="paw_vs:vol1_mirror"} -logrestoretype All
```

그만큼 -archive 매개변수를 사용하면 복원에 사용할 기본 볼륨과 보조 볼륨을 지정할 수 있습니다.

그만큼 -IsRecoverMount:\$true 매개변수를 사용하면 복원 후 데이터베이스를 마운트할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

메일 및 사서함의 세분화된 복구

SMBR(Single Mailbox Recovery) 소프트웨어를 사용하면 전체 Exchange 데이터베이스 대신 메일이나 사서함을 복원하고 복구할 수 있습니다.

단 하나의 메일을 복구하기 위해 전체 데이터베이스를 복원하려면 많은 시간과 리소스가 소모됩니다. SMBR은 스냅샷의 복제본을 생성한 다음 Microsoft API를 사용하여 SMBR에 사서함을 마운트하여 메일을 빠르게 복구하는 데 도움이 됩니다. SMBR 사용 방법에 대한 정보는 다음을 참조하세요. ["SMBR 관리 가이드"](#).

SMBR에 대한 추가 정보는 다음을 참조하세요.

- ["SMBR을 사용하여 단일 항목을 수동으로 복원하는 방법\(Ontrack Power Control 복원에도 적용 가능\)"](#)
- ["SnapCenter 사용하여 SMBR의 보조 저장소에서 복원하는 방법"](#)
- ["SMBR을 사용하여 SnapVault 에서 Microsoft Exchange 메일 복구"](#)

보조 저장소에서 Exchange Server 데이터베이스 복원

보조 저장소(미러 또는 볼트)에서 백업된 Exchange Server 데이터베이스를 복원할 수 있습니다.

기본 저장소에서 보조 저장소로 스냅샷을 복제했어야 합니다.

이 작업에 관하여

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.
- SnapMirror Active Sync 복원 작업의 경우 기본 위치에서 백업을 선택해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 *Microsoft Exchange Server 플러그인*을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 데이터베이스나 리소스 그룹을 선택하세요.

데이터베이스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. '복사본 관리' 섹션에서 보조 저장 시스템(미러 또는 볼트)의 *백업*을 선택합니다.
5. 목록에서 백업을 선택한 다음 클릭하세요. .
6. 위치 페이지에서 선택한 리소스를 복원할 대상 볼륨을 선택합니다.
7. 복원 마법사를 완료하고 요약 검토한 후 *마침*을 클릭합니다.

수동 Exchange 노드 복제본을 다시 시드합니다.

예를 들어 복사본이 손상된 경우 복제본을 다시 시드해야 하는 경우 SnapCenter 의 다시 시드 기능을 사용하여 최신 백업으로 다시 시드할 수 있습니다.

시작하기 전에

다시 시딩하려는 데이터베이스의 백업을 만들어야 합니다.

+ 노드 간 지연을 방지하려면 재시드 작업을 수행하기 전에 새 백업을 만들거나 최신 백업이 있는 호스트를 선택할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 *Microsoft Exchange Server 플러그인*을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 적절한 옵션을 선택하세요.

옵션	설명
단일 데이터베이스를 다시 시드하려면	보기 목록에서 *데이터베이스*를 선택합니다.
DAG에서 데이터베이스를 다시 시드하려면	보기 목록에서 *데이터베이스 가용성 그룹*을 선택합니다.

3. 다시 시드할 리소스를 선택하세요.
4. 사본 관리 페이지에서 *다시 시드*를 클릭합니다.
5. 다시 시드 마법사의 비정상 데이터베이스 복사본 목록에서 다시 시드하려는 복사본을 선택한 후 *다음*을 클릭합니다.
6. 호스트 창에서 다시 시딩하려는 백업이 있는 호스트를 선택한 후 *다음*을 클릭합니다.
7. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다.

8. 요약을 검토한 후 *마침*을 클릭하세요.
9. 페이지 하단의 활동 패널을 확장하면 작업 상태를 볼 수 있습니다.



수동 데이터베이스 복사본이 NetApp 스토리지가 아닌 곳에 있는 경우 다시 시드 작업이 지원되지 않습니다.

PowerShell cmdlet을 사용하여 **Exchange** 데이터베이스에 대한 복제본을 다시 시드합니다.

PowerShell cmdlet을 사용하면 동일한 호스트의 최신 복사본이나 대체 호스트의 최신 복사본을 사용하여 비정상 복제본을 복원할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. 다음을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다. `Open-SmConnection cmdlet`.

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146/
```

2. 다음을 사용하여 데이터베이스를 다시 시드합니다. `reseed-SmDagReplicaCopy cmdlet`.

이 예제에서는 호스트 "mva-rx200.netapp.com"에 있는 execdb라는 데이터베이스의 실패한 복사본을 해당 호스트의 최신 백업을 사용하여 다시 시드합니다.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database  
execdb
```

이 예제에서는 대체 호스트 "mva-rx201.netapp.com"에 있는 데이터베이스의 최신 백업(운영/복사본)을 사용하여 execdb라는 데이터베이스의 실패한 복사본을 다시 시드합니다.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database  
execdb -BackupHost "mva-rx201.netapp.com"
```

복원 작업 모니터링

작업 페이지를 사용하여 다양한 SnapCenter 복원 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

복원 후 상태는 복원 작업 후 리소스의 조건과 수행할 수 있는 추가 복원 작업을 설명합니다.

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복원 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복원*을 선택합니다.
 - d. 상태 드롭다운 목록에서 복원 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.

4. 복원 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.

5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

Exchange 데이터베이스에 대한 복원 작업 취소

대기 중인 복원 작업을 취소할 수 있습니다.

복원 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

이 작업에 관하여

- 모니터 페이지나 활동 창에서 대기 중인 복원 작업을 취소할 수 있습니다.
- 실행 중인 복원 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 대기 중인 복원 작업을 취소할 수 있습니다.
- 취소할 수 없는 복원 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 복원 작업을 취소할 수 있습니다.

단계

다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	1. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. 2. 작업을 선택하고 *작업 취소*를 클릭하세요.
활동 창	1. 복원 작업을 시작한 후 다음을 클릭하세요.  활동 창에서 가장 최근의 작업 5개를 확인하세요. 2. 작업을 선택하세요. 3. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

IBM Db2 보호

IBM Db2용 SnapCenter 플러그인

IBM Db2용 SnapCenter 플러그인 개요

IBM Db2 데이터베이스용 SnapCenter 플러그인은 IBM Db2 데이터베이스의 애플리케이션 인식 데이터 보호 관리를 지원하는 NetApp SnapCenter software 의 호스트 측 구성 요소입니다. IBM Db2 데이터베이스용 플러그인은 SnapCenter 환경에서 IBM Db2 데이터베이스의 백업, 복원 및 복제를 자동화합니다.

- SnapCenter 6.0은 IBM Db2 10.5 이상을 지원합니다.
- SnapCenter 6.0.1은 IBM Db2 9.7.x 이상을 지원합니다. 또한 SnapCenter 6.0.1부터 AIX에서 IBM Db2가 지원됩니다.

SnapCenter 단일 인스턴스 및 다중 인스턴스 Db2 설정을 지원합니다. Linux와 Windows 환경 모두에서 IBM Db2 데이터베이스 플러그인을 사용할 수 있습니다. Windows 환경에서는 Db2가 수동 리소스로 지원됩니다.



Db2 pureScale 환경 및 Db2 다중 노드(DPF) 시스템은 지원되지 않습니다.

IBM Db2 데이터베이스용 플러그인이 설치되면 NetApp SnapMirror 기술과 함께 SnapCenter 사용하여 다른 볼륨에 백업 세트의 미러 사본을 만들 수 있습니다. NetApp SnapVault 기술과 함께 플러그인을 사용하면 표준을 준수하기 위해 디스크 간 백업 복제를 수행할 수도 있습니다.

Db2용 SnapCenter 플러그인은 ONTAP 및 Azure NetApp 파일 스토리지 레이아웃에서 NFS와 SAN을 지원합니다.

VMDK, vVol 및 RDM 가상 스토리지 레이아웃이 지원됩니다.

IBM Db2용 SnapCenter 플러그인을 사용하여 수행할 수 있는 작업

사용자 환경에 IBM Db2 데이터베이스용 플러그인을 설치하면 SnapCenter 사용하여 IBM Db2 데이터베이스와 해당 리소스를 백업, 복원 및 복제할 수 있습니다. 해당 작업을 지원하는 작업도 수행할 수 있습니다.

- 데이터베이스를 추가합니다.
- 백업을 만듭니다.
- 백업에서 복원합니다.
- 백업을 복제합니다.
- 백업 작업을 예약합니다.
- 백업, 복원 및 복제 작업을 모니터링합니다.
- 백업, 복원 및 복제 작업에 대한 보고서를 확인합니다.

IBM Db2용 SnapCenter 플러그인 기능

SnapCenter 플러그인 애플리케이션과 스토리지 시스템의 NetApp 기술과 통합됩니다. IBM Db2 데이터베이스용 플러그인을 사용하려면 SnapCenter 그래픽 사용자 인터페이스를 사용합니다.

- 통합된 그래픽 사용자 인터페이스

SnapCenter 인터페이스는 플러그인과 환경 전반에 걸쳐 표준화와 일관성을 제공합니다. SnapCenter 인터페이스를 사용하면 플러그인 전반에 걸쳐 일관된 백업, 복원 및 복제 작업을 완료하고, 중앙 집중식 보고를 사용하고, 한눈에 볼 수 있는 대시보드 보기를 사용하고, 역할 기반 액세스 제어(RBAC)를 설정하고, 모든 플러그인에서 작업을 모니터링할 수 있습니다.

- 자동화된 중앙 관리

백업 작업을 예약하고, 정책 기반 백업 보존을 구성하고, 복원 작업을 수행할 수 있습니다. SnapCenter 구성하여 이메일 알림을 보내 환경을 사전에 모니터링할 수도 있습니다.

- 비중단 **NetApp** 스냅샷 복사 기술

SnapCenter IBM Db2 Database용 플러그인과 함께 NetApp 스냅샷 기술을 사용하여 리소스를 백업합니다.

IBM Db2 플러그인을 사용하면 다음과 같은 이점도 얻을 수 있습니다.

- 백업, 복원 및 복제 워크플로 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임

또한, 권한이 있는 SnapCenter 사용자에게 애플리케이션 수준 권한이 부여되도록 자격 증명을 설정할 수도 있습니다.

- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 리소스의 공간 효율적 및 특정 시점 복사본 생성

복제본을 생성하려는 스토리지 시스템에 FlexClone 라이선스가 필요합니다.

- 백업 생성의 일부로 ONTAP 의 일관성 그룹(CG) 스냅샷 기능에 대한 지원.
- 여러 리소스 호스트에서 동시에 여러 백업을 실행할 수 있는 기능

단일 작업에서 단일 호스트의 리소스가 동일한 볼륨을 공유하는 경우 스냅샷이 통합됩니다.

- 외부 명령을 사용하여 스냅샷을 생성하는 기능.
- XFS 파일 시스템에서 Linux LVM을 지원합니다.

IBM Db2용 SnapCenter 플러그인에서 지원하는 스토리지 유형

SnapCenter 물리적 머신과 가상 머신(VM) 모두에서 다양한 스토리지 유형을 지원합니다. IBM Db2용 SnapCenter 플러그인을 설치하기 전에 스토리지 유형에 대한 지원을 확인해야 합니다.

기계	저장 유형
물리적 서버	• FC 연결 LUN • iSCSI로 연결된 LUN • NFS 연결 볼륨
VMware ESXi	• FC 또는 iSCSI ESXi HBA로 연결된 RDM LUN 호스트 버스 어댑터(HBA) 스캐닝은 SnapCenter 호스트에 있는 모든 호스트 버스 어댑터를 스캔하기 때문에 완료하는 데 오랜 시간이 걸릴 수 있습니다. <code>_opt/</code> <code>NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config_</code>에 있는 LinuxConfig.pm 파일을 편집하여 SCSI_HOSTS_OPTIMIZED_RESCAN 매개변수 값을 1로 설정하면 HBA_DRIVER_NAMES에 나열된 HBA만 다시 스캔합니다. • iSCSI 이니시에이터에 의해 게스트 시스템에 직접 연결된 iSCSI LUN • NFS 데이터 저장소의 VMDK • VMFS에 VMDK가 생성됨 • 게스트 시스템에 직접 연결된 NFS 볼륨 • NFS와 SAN 모두에 있는 vVol 데이터 저장소 vVol 데이터스토어는 VMware vSphere용 ONTAP 도구를 사용해서만 프로비저닝할 수 있습니다.

IBM Db2 플러그인에 필요한 최소 ONTAP 권한

데이터 보호를 위해 사용하는 SnapCenter 플러그인에 따라 필요한 최소 ONTAP 권한은 다음과 같습니다.

- 모든 액세스 명령: ONTAP 9.12.1 이상에 필요한 최소 권한
 - 이벤트 생성-자동 지원-로그
 - 작업 이력 표시
 - 작업 중지
 - 룰
 - lun 생성
 - lun 생성
 - lun 생성
 - lun 삭제

- lun igroup 추가
- lun igroup 생성
- lun igroup 삭제
- lun igroup 이름 바꾸기
- lun igroup 이름 바꾸기
- 룬 아이그룹 쇼
- lun 매핑 add-reporting-nodes
- lun 매핑 생성
- LUN 매핑 삭제
- LUN 매핑 제거-보고-노드
- lun 매핑 쇼
- lun 수정
- lun 이동량
- lun 오프라인
- lun 온라인
- lun 지속적 예약 지우기
- lun 크기 조정
- lun 시리얼
- 룬 쇼
- 스냅미러 정책 추가 규칙
- 스냅미러 정책 수정 규칙
- 스냅미러 정책 제거 규칙
- 스냅미러 정책 보기
- 스냅미러 복원
- 스냅미러 쇼
- 스냅미러 쇼 히스토리
- 스냅미러 업데이트
- 스냅미러 업데이트-is-세트
- 스냅미러 목록-대상
- 버전
- 볼륨 복제 생성
- 볼륨 클론 쇼
- 볼륨 복제 분할 시작
- 볼륨 클론 분할 정지

- 볼륨 생성
- 볼륨 파괴
- 볼륨 파일 복제 생성
- 볼륨 파일 show-disk-usage
- 볼륨 오프라인
- 온라인 볼륨
- 볼륨 수정
- 볼륨 qtree 생성
- 볼륨 qtree 삭제
- 볼륨 qtree 수정
- 볼륨 qtree 쇼
- 볼륨 제한
- 볼륨 쇼
- 볼륨 스냅샷 생성
- 볼륨 스냅샷 삭제
- 볼륨 스냅샷 수정
- 볼륨 스냅샷 수정-스냅락-만료-시간
- 볼륨 스냅샷 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- vservers cifs
- vservers cifs 공유 생성
- vservers cifs 공유 삭제
- vservers cifs 새도우 카피 쇼
- vservers cifs 공유 표시
- vservers cifs 쇼
- vservers 내보내기 정책
- vservers 내보내기 정책 생성
- vservers 내보내기 정책 삭제
- vservers 내보내기 정책 규칙 생성
- vservers 내보내기 정책 규칙 표시
- vservers 내보내기 정책 표시

- v서버 iSCSI
- vservers iscsi 연결 표시
- vservers 쇼
- 읽기 전용 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
 - 네트워크 인터페이스
 - 네트워크 인터페이스 표시
 - v서버

IBM Db2용 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비

ONTAP SnapMirror 기술과 함께 SnapCenter 플러그인을 사용하면 다른 볼륨에 백업 세트의 미리 사본을 생성할 수 있으며, ONTAP SnapVault 기술과 함께 사용하면 표준 준수 및 기타 거버넌스 관련 목적으로 디스크 간 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 구성하고 해당 관계를 초기화해야 합니다.

SnapCenter 스냅샷 작업을 완료한 후 SnapMirror와 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행되므로 별도의 ONTAP 일정을 만들지 마세요.



NetApp SnapManager 제품을 통해 SnapCenter에 접속했고 구성된 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 기본 저장소(소스 볼륨)의 데이터를 보조 저장소(대상 볼륨)로 복제합니다. 관계를 초기화하면 ONTAP 소스 볼륨에서 참조되는 데이터 블록을 대상 볼륨으로 전송합니다.



SnapCenter SnapMirror와 SnapVault 볼륨 간의 계단식 관계(**Primary > Mirror > Vault**)를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter 버전에 따라 유연한 SnapMirror 관계 관리를 지원합니다. 버전에 따라 유연한 SnapMirror 관계와 이를 설정하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["ONTAP 문서"](#).

IBM Db2에 대한 백업 전략

IBM Db2에 대한 백업 전략 정의

백업 작업을 생성하기 전에 백업 전략을 정의하면 리소스를 성공적으로 복원하거나 복제하는 데 필요한 백업을 확보하는 데 도움이 됩니다. 백업 전략은 주로 서비스 수준 계약(SLA), 복구 시간 목표(RTO), 복구 지점 목표(RPO)에 따라 결정됩니다.

이 작업에 관하여

SLA는 기대되는 서비스 수준을 정의하고 서비스의 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RTO는 서비스가 중단된 후 비즈니스 프로세스를 복구해야 하는 시간입니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 기간에 대한 전략을 정의합니다. SLA, RTO, RPO는 데이터 보호 전략에 기여합니다.

단계

1. 리소스를 백업해야 하는 시기를 결정하세요.
2. 필요한 백업 작업의 수를 결정합니다.
3. 백업의 이름을 어떻게 지을지 결정하세요.
4. 데이터베이스의 애플리케이션 일관성 스냅샷을 백업하기 위해 스냅샷 복사 기반 정책을 생성할지 여부를 결정합니다.
5. 복제를 위해 NetApp SnapMirror 기술을 사용할지, 장기 보존을 위해 NetApp SnapVault 기술을 사용할지 결정하세요.
6. 소스 스토리지 시스템과 SnapMirror 대상의 스냅샷 보존 기간을 결정합니다.
7. 백업 작업 전이나 후에 명령을 실행할지 여부를 결정하고 사전 스크립트나 사후 스크립트를 제공합니다.

Linux 호스트에서 리소스 자동 검색

리소스는 SnapCenter 에서 관리하는 Linux 호스트의 IBM Db2 데이터베이스와 인스턴스입니다. IBM Db2용 SnapCenter 플러그인을 설치하면 해당 Linux 호스트의 모든 인스턴스에 있는 IBM Db2 데이터베이스가 자동으로 검색되어 리소스 페이지에 표시됩니다.

지원되는 백업 유형

백업 유형은 생성하려는 백업 유형을 지정합니다. SnapCenter IBM Db2 데이터베이스에 대한 스냅샷 복사 기반 백업 유형을 지원합니다.

스냅샷 복사 기반 백업

스냅샷 복사 기반 백업은 NetApp 스냅샷 기술을 활용하여 IBM Db2 데이터베이스가 있는 볼륨의 온라인, 읽기 전용 복사본을 만듭니다.

IBM Db2용 SnapCenter 플러그인이 일관성 그룹 스냅샷을 사용하는 방법

플러그인을 사용하면 리소스 그룹에 대한 일관성 그룹 스냅샷을 만들 수 있습니다. 일관성 그룹은 여러 볼륨을 수용하여 하나의 엔티티로 관리할 수 있는 컨테이너입니다. 일관성 그룹은 여러 볼륨의 동시 스냅샷으로, 볼륨 그룹의 일관된 복사본을 제공합니다.

또한 스토리지 컨트롤러가 스냅샷을 일관되게 그룹화하는 데 걸리는 대기 시간을 지정할 수도 있습니다. 이용 가능한 대기 시간 옵션은 긴급, 보통, *느긋함*입니다. 일관된 그룹 스냅샷 작업 중에 WAFL(Write Anywhere File Layout) 동기화를 활성화하거나 비활성화할 수도 있습니다. WAFL 동기화는 일관성 그룹 스냅샷의 성능을 향상시킵니다.

SnapCenter 데이터 백업의 정리 작업을 관리하는 방법

SnapCenter 스토리지 시스템 및 파일 시스템 수준에서 데이터 백업의 정리 작업을 관리합니다.

기본 또는 보조 스토리지의 스냅샷과 IBM Db2 카탈로그의 해당 항목은 보존 설정에 따라 삭제됩니다.

IBM Db2 백업 일정을 결정하기 위한 고려 사항

백업 일정을 결정하는 가장 중요한 요소는 리소스의 변화율입니다. 자주 사용되는 리소스는 매시간 백업하고, 거의 사용되지 않는 리소스는 하루에 한 번 백업할 수도 있습니다. 기타

요소로는 조직에 대한 리소스의 중요성, 서비스 수준 계약(SLA), 복구 지점 목표(RPO) 등이 있습니다.

백업 일정은 다음과 같이 두 부분으로 구성됩니다.

- 백업 빈도(백업을 수행할 빈도)

일부 플러그인의 경우 일정 유형이라고도 하는 백업 빈도는 정책 구성의 일부입니다. 예를 들어, 백업 빈도를 매시간, 매일, 매주 또는 매월로 구성할 수 있습니다.

- 백업 일정(백업을 수행할 정확한 시기)

백업 일정은 리소스 또는 리소스 그룹 구성의 일부입니다. 예를 들어, 주간 백업을 위해 구성된 정책이 있는 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 일정을 구성할 수 있습니다.

IBM Db2에 필요한 백업 작업 수

필요한 백업 작업 수를 결정하는 요소에는 리소스 크기, 사용된 볼륨 수, 리소스 변경률, 서비스 수준 계약(SLA) 등이 있습니다.

IBM Db2 데이터베이스용 플러그인에 대한 백업 명명 규칙

기본 스냅샷 명명 규칙을 사용하거나 사용자 지정 명명 규칙을 사용할 수 있습니다. 기본 백업 명명 규칙은 스냅샷 이름에 타임스탬프를 추가하여 복사본이 생성된 시기를 식별하는 데 도움이 됩니다.

스냅샷은 다음과 같은 기본 명명 규칙을 사용합니다.

resourcegroupname_hostname_timestamp

다음 예와 같이 논리적으로 백업 리소스 그룹의 이름을 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예에서 구문 요소는 다음과 같은 의미를 갖습니다.

- `_dts1_`은 리소스 그룹 이름입니다.
- `_mach1x88_`은 호스트 이름입니다.
- `_03-12-2015_23.17.26_`은 날짜와 타임스탬프입니다.

또는, *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택하여 리소스나 리소스 그룹을 보호하는 동안 스냅샷 이름 형식을 지정할 수 있습니다. 예를 들어, `customtext_resourcegroup_policy_hostname` 또는 `resourcegroup_hostname`입니다. 기본적으로 타임스탬프 접미사는 스냅샷 이름에 추가됩니다.

IBM Db2에 대한 복원 및 복구 전략

IBM Db2 리소스에 대한 복원 및 복구 전략 정의

데이터베이스를 복원하고 복구하기 전에 전략을 정의해야 복원 및 복구 작업을 성공적으로 수행할 수 있습니다.



데이터베이스의 수동 복구만 지원됩니다.

단계

1. 수동으로 추가된 IBM Db2 리소스에 대해 지원되는 복원 전략을 확인합니다.
2. 자동 검색된 IBM Db2 데이터베이스에 지원되는 복원 전략을 확인합니다.

수동으로 추가된 **IBM Db2** 리소스에 대해 지원되는 복원 전략 유형

SnapCenter 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다. 수동으로 추가된 IBM Db2 리소스에 대한 복원 전략에는 두 가지 유형이 있습니다.



수동으로 추가한 IBM Db2 리소스는 복구할 수 없습니다.

리소스 복구 완료

- 리소스의 모든 볼륨, Qtree 및 LUN을 복원합니다.



리소스에 볼륨이나 Q트리가 포함되어 있는 경우 해당 볼륨이나 Q트리에서 복원을 위해 선택한 스냅샷 이후에 촬영된 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 동일한 볼륨이나 Q트리에 다른 리소스가 호스팅되는 경우 해당 리소스도 삭제됩니다.

자동으로 검색된 **IBM Db2**에 지원되는 복원 전략 유형

SnapCenter 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다.

전체 리소스 복원은 자동으로 검색된 IBM Db2 데이터베이스에 지원되는 복원 전략입니다. 이렇게 하면 리소스의 모든 볼륨, Q트리, LUN이 복원됩니다.

자동 검색된 **IBM Db2**에 대한 복원 작업 유형

IBM Db2용 SnapCenter 플러그인은 단일 파일 SnapRestore 및 자동으로 검색된 IBM Db2 데이터베이스에 대한 연결 및 복사 복원 유형을 지원합니다.

단일 파일 **SnapRestore** 다음 시나리오에 대해 **NFS** 환경에서 수행됩니다.

- 전체 리소스 옵션만 선택된 경우
- 선택한 백업이 SnapMirror 또는 SnapVault 보조 위치에서 시작되고 전체 리소스 옵션이 선택된 경우

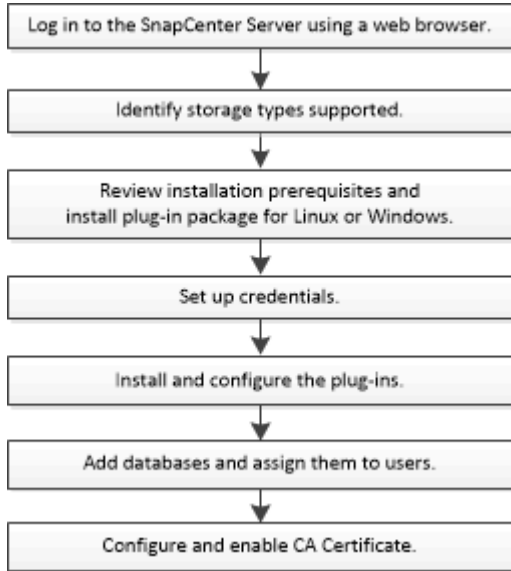
단일 파일 **SnapRestore** 다음 시나리오에 대해 **SAN** 환경에서 수행됩니다.

- 전체 리소스 옵션만 선택된 경우
- SnapMirror 또는 SnapVault 보조 위치에서 백업을 선택하고 전체 리소스 옵션을 선택한 경우

IBM Db2용 SnapCenter 플러그인 설치를 준비하세요

IBM Db2용 SnapCenter 플러그인 설치 워크플로

IBM Db2 데이터베이스를 보호하려면 IBM Db2용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



Windows, Linux 또는 AIX용 호스트 추가 및 플러그인 패키지 설치를 위한 전제 조건

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 충족해야 합니다. Windows, Linux 및 AIX 환경에서 지원되는 IBM Db2용 SnapCenter 플러그인입니다.

- 호스트에 Java 11을 설치했어야 합니다.



IBM Java는 Windows 및 Linux 호스트에서 지원되지 않습니다.

- Windows의 경우 플러그인 생성 서비스는 “LocalSystem” Windows 사용자를 사용하여 실행해야 합니다. 이는 IBM Db2용 플러그인이 도메인 관리자로 설치된 경우의 기본 동작입니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다. Microsoft Windows용 SnapCenter 플러그인은 기본적으로 Windows 호스트의 IBM Db2 플러그인과 함께 배포됩니다.
- SnapCenter 서버는 IBM Db2 호스트용 플러그인의 8145 또는 사용자 정의 포트에 액세스할 수 있어야 합니다.

Windows 호스트

- 원격 호스트에 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 도메인 사용자가 있어야 합니다.
- Windows 호스트에 IBM Db2용 플러그인을 설치하는 동안 Microsoft Windows용 SnapCenter 플러그인이 자동으로 설치됩니다.
- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.
- Windows 호스트에 Java 11을 설치했어야 합니다.

"Windows용 JAVA 다운로드"

"NetApp 상호 운용성 매트릭스 도구"

Linux 및 AIX 호스트

- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.
- Linux 호스트에 Java 11을 설치했어야 합니다.

"Linux용 JAVA 다운로드"

"AIX용 JAVA 다운로드"

"NetApp 상호 운용성 매트릭스 도구"

- Linux 호스트에서 실행되는 IBM Db2 데이터베이스의 경우 IBM Db2용 플러그인을 설치하는 동안 UNIX용 SnapCenter 플러그인이 자동으로 설치됩니다.
- 플러그인 설치를 위해 기본 셸로 `*bash*`를 사용해야 합니다.

보충 명령

IBM Db2용 SnapCenter 플러그인에서 보충 명령을 실행하려면 `allowed_commands.config` 파일에 해당 명령을 포함해야 합니다.

- Windows 호스트의 기본 위치: `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux 호스트의 기본 위치: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`

플러그인 호스트에서 추가 명령을 허용하려면 편집기에서 `allowed_commands.config` 파일을 엽니다. 각 명령을 별도의 줄에 입력하세요. 명령은 대소문자를 구분하지 않습니다. 완전히 정규화된 경로 이름을 지정하고, 경로 이름에 공백이 포함된 경우 따옴표(")로 묶으세요.

예를 들어:

명령어: `mount`

명령어: `umount`

명령: `"C:\Program Files\ NetApp\SnapCreator commands\sdcli.exe"`

명령어: `myscript.bat`

`allowed_commands.config` 파일이 없으면 명령이나 스크립트 실행이 차단되고 다음 오류와 함께 워크플로가 실패합니다.

`"/mnt/mount -a]` 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여합니다."

`_allowed_commands.config`에 명령이나 스크립트가 없으면 명령이나 스크립트 실행이 차단되고 다음 오류와 함께 워크플로가 실패합니다.

`"/mnt/mount -a]` 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여합니다."



모든 명령을 허용하려면 와일드카드 항목(*)을 사용해서는 안 됩니다.

Linux 호스트에 대한 루트가 아닌 사용자에게 대한 **sudo** 권한 구성

SnapCenter 사용하면 루트가 아닌 사용자도 Linux용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 루트가 아닌 사용자로 실행됩니다. 루트가 아닌 사용자에게 여러 경로에 대한 액세스 권한을 제공하려면 sudo 권한을 구성해야 합니다.

필요한 것

- Sudo 버전 1.8.7 이상.
- umask가 0027인 경우, java 폴더와 그 안에 있는 모든 파일에 555 권한이 있어야 합니다. 그렇지 않으면 플러그인 설치가 실패할 수 있습니다.
- 루트가 아닌 사용자의 경우 루트가 아닌 사용자의 이름과 사용자 그룹이 동일해야 합니다.
- `/etc/ssh/sshd_config` 파일을 편집하여 메시지 인증 코드 알고리즘(MAC hmac-sha2-256 및 MAC hmac-sha2-512)을 구성합니다.

구성 파일을 업데이트한 후 sshd 서비스를 다시 시작합니다.

예:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

이 작업에 관하여

루트가 아닌 사용자에게 다음 경로에 대한 액세스를 제공하려면 sudo 권한을 구성해야 합니다.

- `/home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/custom_location/ NetApp/snapcenter/spl/설치/플러그인/제거`
- `/custom_location/ NetApp/snapcenter/spl/bin/spl`

단계

1. Linux용 SnapCenter 플러그인 패키지를 설치하려는 Linux 호스트에 로그인합니다.
2. visudo Linux 유틸리티를 사용하여 `/etc/sudoers` 파일에 다음 줄을 추가합니다.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



RAC 설정을 사용하는 경우 허용되는 다른 명령과 함께 다음을 `/etc/sudoers` 파일에 추가해야 합니다. '`<crs_home>/bin/olsnodes`'

`crs_home`의 값은 `_etc/oracle/olr.loc` 파일에서 얻을 수 있습니다.

`_LINUX_USER`는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

`_checksum_value`는 `sc_unix_plugins_checksum.txt` 파일에서 얻을 수 있습니다. 이 파일의 위치는 다음과 같습니다.

- SnapCenter Server가 Windows 호스트에 설치된 경우 `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`.
- SnapCenter 서버가 Linux 호스트에 설치되어 있는 경우 `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`.



이 예제는 귀하만의 데이터를 생성하기 위한 참고자료로만 사용해야 합니다.

AIX 호스트에 대한 루트가 아닌 사용자에게 대한 **sudo** 권한 구성

SnapCenter 4.4 이상에서는 루트가 아닌 사용자도 AIX용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 루트가 아닌 사용자로 실행됩니다. 루트가 아닌 사용자에게 여러 경로에 대한 액세스 권한을 제공하려면 `sudo` 권한을 구성해야 합니다.

필요한 것

- Sudo 버전 1.8.7 이상.

- umask가 0027인 경우, java 폴더와 그 안에 있는 모든 파일에 555 권한이 있어야 합니다. 그렇지 않으면 플러그인 설치가 실패할 수 있습니다.
- `/etc/ssh/sshd_config` 파일을 편집하여 메시지 인증 코드 알고리즘(MAC hmac-sha2-256 및 MAC hmac-sha2-512)을 구성합니다.

구성 파일을 업데이트한 후 sshd 서비스를 다시 시작합니다.

예:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

이 작업에 관하여

루트가 아닌 사용자에게 다음 경로에 대한 액세스를 제공하려면 sudo 권한을 구성해야 합니다.

- `/home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/custom_location/ NetApp/snapcenter/spl/설치/플러그인/제거`
- `/custom_location/ NetApp/snapcenter/spl/bin/spl`

단계

1. AIX용 SnapCenter 플러그인 패키지를 설치하려는 AIX 호스트에 로그인합니다.
2. visudo Linux 유틸리티를 사용하여 `/etc/sudoers` 파일에 다음 줄을 추가합니다.

```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



RAC 설정을 사용하는 경우 허용되는 다른 명령과 함께 다음을 `/etc/sudoers` 파일에 추가해야 합니다. '`<crs_home>/bin/olsnodes`'

`crs_home`의 값은 `/etc/oracle/olr.loc` 파일에서 얻을 수 있습니다.

`_AIX_USER`는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

`_checksum_value`는 `sc_unix_plugins_checksum.txt` 파일에서 얻을 수 있습니다. 이 파일의 위치는 다음과 같습니다.

- SnapCenter Server가 Windows 호스트에 설치된 경우 `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`.
- SnapCenter 서버가 Linux 호스트에 설치되어 있는 경우 `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`.



이 예제는 귀하만의 데이터를 생성하기 위한 참고자료로만 사용해야 합니다.

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항과 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	마이크로소프트 윈도우 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	• ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 • 파워셸 코어 7.4.2 • Java 11 Oracle Java 및 OpenJDK 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .

Linux용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 및 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	• 레드햇 엔터프라이즈 리눅스 • SUSE Linux Enterprise Server(SLES) 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB

목	요구 사항
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	Java 11 Oracle Java 및 OpenJDK JAVA를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties에 있는 JAVA_HOME 옵션이 올바른 JAVA 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다. 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구".

IBM Db2용 SnapCenter 플러그인에 대한 자격 증명 설정

SnapCenter SnapCenter 작업을 위해 사용자를 인증하기 위해 자격 증명을 사용합니다. SnapCenter 플러그인을 설치하기 위한 자격 증명과 데이터베이스나 Windows 파일 시스템에서 데이터 보호 작업을 수행하기 위한 추가 자격 증명을 만들어야 합니다.

이 작업에 관하여

- 리눅스 호스트

Linux 호스트에 플러그인을 설치하려면 자격 증명을 설정해야 합니다.

플러그인 프로세스를 설치하고 시작하려면 루트 사용자 또는 sudo 권한이 있는 루트가 아닌 사용자의 자격 증명을 설정해야 합니다.

모범 사례: 호스트를 배포하고 플러그인을 설치한 후에도 Linux에 대한 자격 증명을 생성할 수 있지만, 가장 좋은 방법은 호스트를 배포하고 플러그인을 설치하기 전에 SVM을 추가한 후에 자격 증명을 생성하는 것입니다.

- Windows 호스트

플러그인을 설치하기 전에 Windows 자격 증명을 설정해야 합니다.

원격 호스트의 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정해야 합니다.

개별 리소스 그룹에 대한 자격 증명을 설정하고 사용자 이름에 전체 관리자 권한이 없는 경우 최소한 리소스 그룹 및 백업 권한을 사용자 이름에 할당해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *자격 증명*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 자격 증명 페이지에서 자격 증명을 구성하는 데 필요한 정보를 지정합니다.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.
사용자 이름	인증에 사용할 사용자 이름과 비밀번호를 입력하세요. • 도메인 관리자 또는 관리자 그룹의 모든 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹 구성원을 지정하세요. 사용자 이름 필드에 사용할 수 있는 형식은 다음과 같습니다. ◦ <i>NetBIOS</i> 사용자 이름 ◦ 도메인 <i>FQDN</i> 사용자 이름 • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우, SnapCenter 플러그인을 설치할 시스템에 기본 제공되는 로컬 관리자를 지정하십시오. 사용자 계정에 승격된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우, 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다. <i>UserName</i> 비밀번호에 큰따옴표(")나 백틱(`)을 사용하지 마세요. 비밀번호에 '<' 기호와 '!' 기호를 함께 사용하면 안 됩니다. 예를 들어, lessthan<!10, lessthan10<!, backtick`12.
비밀번호	인증에 사용되는 비밀번호를 입력하세요.
인증 모드	사용할 인증 모드를 선택하세요.
sudo 권한을 사용하세요	루트가 아닌 사용자에게 자격 증명을 생성하는 경우 sudo 권한 사용 확인란을 선택합니다.  Linux 사용자에게만 적용됩니다.

5. *확인*을 클릭합니다.

자격 증명 설정을 마친 후 사용자 및 액세스 페이지에서 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

Windows Server 2016 이상에서 gMSA 구성

Windows Server 2016 이상에서는 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 관리 서비스 계정(gMSA)을 만들 수 있습니다.

시작하기 전에

- Windows Server 2016 이상 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2016 이상 호스트가 있어야 합니다.

단계

1. gMSA의 각 개체에 대해 고유한 비밀번호를 생성하려면 KDS 루트 키를 만듭니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 다음 명령을 실행합니다. Add-KDSRootKey -EffectiveImmediately
3. gMSA를 만들고 구성하세요.
 - a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
domainName\accountName$  
.. 그룹에 컴퓨터 객체를 추가합니다.  
.. 방금 만든 사용자 그룹을 사용하여 gMSA를 만듭니다.
```

예를 들어,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 달리다 `Get-ADServiceAccount` 서비스 계정을 확인하는 명령입니다.
```

4. 호스트에서 gMSA를 구성하세요.
 - a. gMSA 계정을 사용하려는 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.

이렇게 하려면 PowerShell에서 다음 명령을 실행하세요.

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

a. 호스트를 다시 시작합니다.

b. PowerShell 명령 프롬프트에서 다음 명령을 실행하여 호스트에 gMSA를 설치합니다. `Install-AdServiceAccount <gMSA>`

c. 다음 명령을 실행하여 gMSA 계정을 확인하세요. `Test-AdServiceAccount <gMSA>`

5. 호스트에서 구성된 gMSA에 관리 권한을 할당합니다.

6. SnapCenter 서버에서 구성된 gMSA 계정을 지정하여 Windows 호스트를 추가합니다.

SnapCenter Server는 호스트에 선택된 플러그인을 설치하고, 플러그인 설치 중에 지정된 gMSA가 서비스 로그인 계정으로 사용됩니다.

IBM Db2용 SnapCenter 플러그인 설치

원격 호스트에 호스트를 추가하고 플러그인 패키지를 설치합니다.

SnapCenter 호스트 추가 페이지를 사용하여 호스트를 추가한 다음 플러그인 패키지를 설치해야 합니다. 플러그인은 원격 호스트에 자동으로 설치됩니다. 개별 호스트나 클러스터에 대해 호스트를 추가하고 플러그인 패키지를 설치할 수 있습니다.

시작하기 전에

- SnapCenter 서버 호스트의 운영 체제가 Windows 2019이고 플러그인 호스트의 운영 체제가 Windows 2022인 경우 다음을 수행해야 합니다.
 - Windows Server 2019(OS 빌드 17763.5936) 이상으로 업그레이드하세요.
 - Windows Server 2022(OS 빌드 20348.2402) 이상으로 업그레이드하세요.
- SnapCenter 관리자 역할과 같이 플러그인 설치 및 제거 권한이 있는 역할에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.

- 메시지 대기열 서비스가 실행 중인지 확인해야 합니다.
- 관리 문서에는 호스트 관리에 대한 정보가 포함되어 있습니다.
- 그룹 관리 서비스 계정(gMSA)을 사용하는 경우 관리자 권한으로 gMSA를 구성해야 합니다.

"IBM Db2에 대해 Windows Server 2016 이상에서 그룹 관리 서비스 계정 구성"

이 작업에 관하여

- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 상단에 관리되는 호스트 탭이 선택되어 있는지 확인하세요.
3. *추가*를 클릭하세요.
4. 호스트 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
호스트 유형	호스트 유형을 선택하세요: • Windows • 리눅스  IBM Db2용 플러그인은 IBM Db2 클라이언트 호스트에 설치되며, 이 호스트는 Windows 시스템이나 Linux 시스템에 있을 수 있습니다.
호스트 이름	통신 호스트 이름을 입력하세요. 호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하세요. SnapCenter DNS의 적절한 구성에 달려 있습니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다.
신임장	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성하세요. 자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하세요. 제공한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다.  자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

REST API를 사용하여 Db2용 플러그인을 설치하는 경우 버전을 3.0으로 전달해야 합니다. 예를 들어, Db2:3.0

6. (선택 사항) *추가 옵션*을 클릭합니다.

이 분야에서는...	이렇게 하세요...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정하세요. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트로 표시됩니다.  플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.
설치 경로	IBM Db2용 플러그인은 IBM Db2 클라이언트 호스트에 설치되며, 이 호스트는 Windows 시스템이나 Linux 시스템에 있을 수 있습니다. • Windows용 SnapCenter 플러그인 패키지의 경우 기본 경로는 C:\Program Files\ NetApp\ SnapCenter 입니다. 선택적으로 경로를 사용자 정의할 수 있습니다. • Linux용 SnapCenter 플러그인 패키지의 경우 기본 경로는 /opt/ NetApp/snapcenter입니다. 선택적으로 경로를 사용자 정의할 수 있습니다.
사전 설치 확인 건너뛰기	플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택하세요.
플러그인 서비스를 실행하려면 그룹 관리 서비스 계정(gMSA)을 사용하세요.	Windows 호스트의 경우 플러그인 서비스를 실행하기 위해 그룹 관리 서비스 계정(gMSA)을 사용하려면 이 확인란을 선택합니다.  다음 형식으로 gMSA 이름을 제공하세요: domainName\accountName\$.  gMSA는 Windows용 SnapCenter 플러그인 서비스에 대한 로그인 서비스 계정으로만 사용됩니다.

7. *제출*을 클릭하세요.

"사전 검사 건너뛰기" 확인란을 선택하지 않은 경우, 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 호스트의 유효성 검사가 수행됩니다. 디스크 공간, RAM, PowerShell 버전, .NET 버전, 위치(Windows 플러그인의 경우), Java 11(Windows 및 Linux 플러그인 모두)이 최소 요구 사항을 충족하는지 검증됩니다. 최소 요구 사항을

충족하지 못하면 해당 오류 또는 경고 메시지가 표시됩니다.

오류가 디스크 공간이나 RAM과 관련된 경우 C:\Program Files\ NetApp\ SnapCenter WebApp에 있는 web.config 파일을 업데이트하여 기본값을 수정할 수 있습니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.



HA 설정에서 web.config 파일을 업데이트하는 경우 두 노드에서 모두 파일을 업데이트해야 합니다.

8. 호스트 유형이 Linux인 경우 지문을 확인한 다음 *확인 및 제출*을 클릭합니다.

클러스터 설정에서는 클러스터의 각 노드의 지문을 확인해야 합니다.



동일한 호스트가 이전에 SnapCenter 에 추가되었고 지문이 확인된 경우에도 지문 확인은 필수입니다.

9. 설치 진행 상황을 모니터링합니다.

- Windows 플러그인의 경우 설치 및 업그레이드 로그는 다음 위치에 있습니다. C:\Windows\ SnapCenter plugin\Install<JOBID>\
- Linux 플러그인의 경우 설치 로그는 /var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plugin_Install<JOBID>.log에 있고 업그레이드 로그는 /var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plugin_Upgrade<JOBID>.log에 있습니다.

당신이 완료한 후

SnapCenter 6.0 이상으로 업그레이드하려는 경우 기존 PERL 기반 Db2 플러그인이 원격 플러그인 서버에서 제거됩니다.

cmdlet을 사용하여 여러 원격 호스트에 **Linux** 또는 **Windows**용 **SnapCenter** 플러그인 패키지 설치

Install-SmHostPackage PowerShell cmdlet을 사용하여 Linux 또는 Windows용 SnapCenter 플러그인 패키지를 여러 호스트에 동시에 설치할 수 있습니다.

시작하기 전에

플러그인 패키지를 설치하려는 각 호스트에서 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter 에 로그인해야 합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 Open-SmConnection cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
3. Install-SmHostPackage cmdlet과 필요한 매개변수를 사용하여 여러 호스트에 플러그인을 설치합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려는 경우 -skiprecheck 옵션을 사용할 수 있습니다.

4. 원격 설치를 위한 자격 증명을 입력하세요.

명령줄 인터페이스를 사용하여 **Linux** 호스트에 **IBM Db2용 SnapCenter** 플러그인을 설치합니다.

SnapCenter 사용자 인터페이스(UI)를 사용하여 IBM Db2 데이터베이스용 SnapCenter 플러그인을 설치해야 합니다. 사용자 환경에서 SnapCenter UI에서 플러그인을 원격으로 설치할 수 없는 경우 명령줄 인터페이스(CLI)를 사용하여 콘솔 모드나 자동 모드로 IBM Db2 데이터베이스용 플러그인을 설치할 수 있습니다.

시작하기 전에

- IBM Db2 클라이언트가 있는 각 Linux 호스트에 IBM Db2 데이터베이스용 플러그인을 설치해야 합니다.
- IBM Db2 데이터베이스용 SnapCenter 플러그인을 설치하는 Linux 호스트는 종속 소프트웨어, 데이터베이스 및 운영 체제 요구 사항을 충족해야 합니다.

상호 운용성 매트릭스 도구(IMT)에는 지원되는 구성에 대한 최신 정보가 포함되어 있습니다.

"NetApp 상호 운용성 매트릭스 도구"

- IBM Db2 데이터베이스용 SnapCenter 플러그인은 Linux용 SnapCenter 플러그인 패키지의 일부입니다. Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 Windows 호스트에 SnapCenter 이미 설치되어 있어야 합니다.

이 작업에 관하여

매개변수가 언급되지 않으면 SnapCenter 기본값으로 설치됩니다.

단계

1. Linux용 SnapCenter 플러그인 패키지 설치 파일(snapcenter_linux_host_plugin.bin)을 C:\ProgramData\NetApp\ SnapCenter\Package Repository에서 IBM Db2용 플러그인을 설치하려는 호스트로 복사합니다.

SnapCenter 서버가 설치된 호스트에서 이 경로에 액세스할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 복사한 디렉토리로 이동합니다.
3. 플러그인을 설치하세요: path_to_installation_bin_file/snapcenter_linux_host_plugin.bin
-i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address
-DSERVER_HTTPS_PORT=port_number_for_server
 - -DPORT는 SMCORE HTTPS 통신 포트를 지정합니다.
 - -DSERVER_IP는 SnapCenter 서버 IP 주소를 지정합니다.
 - -DSERVER_HTTPS_PORT는 SnapCenter 서버 HTTPS 포트를 지정합니다.
 - -DUSER_INSTALL_DIR은 Linux용 SnapCenter 플러그인 패키지를 설치할 디렉토리를 지정합니다.
 - DINSTALL_LOG_NAME은 로그 파일의 이름을 지정합니다.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. /<설치 디렉토리>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties 파일을 편집한 다음

PLUGINS_ENABLED = DB2:3.0 매개변수를 추가합니다.

5. Add-Smhost cmdlet과 필요한 매개변수를 사용하여 SnapCenter 서버에 호스트를 추가합니다.

명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

IBM Db2 플러그인 설치 상태 모니터링

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행 상황을 모니터링할 수 있습니다. 설치가 완료되었는지 또는 문제가 있는지 확인하기 위해 설치 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 플러그인 설치 작업만 나열되도록 목록을 필터링하려면 다음을 수행합니다.
 - a. *필터*를 클릭하세요.
 - b. 선택 사항: 시작 날짜와 종료 날짜를 지정합니다.
 - c. 유형 드롭다운 메뉴에서 *플러그인 설치*를 선택합니다.
 - d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
 - e. *적용*을 클릭하세요.
4. 설치 작업을 선택하고 *세부정보*를 클릭하면 작업 세부정보를 볼 수 있습니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

CA 인증서 구성

CA 인증서 CSR 파일 생성

인증서 서명 요청(CSR)을 생성하고, 생성된 CSR을 사용하여 인증 기관(CA)에서 얻을 수 있는 인증서를 가져올 수 있습니다. 인증서에는 개인 키가 연결됩니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.



CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 정보는 다음을 참조하세요. "[CA 인증서 CSR 파일을 생성하는 방법](#)".



도메인(*.domain.company.com)이나 시스템(machine1.domain.company.com)에 대한 CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN)과 해당 호스트 이름을 CA 인증서에 명시해야 합니다. 인증서를 구매하기 전에 주체 대체 이름(SAN) 필드를 입력하여 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(*.domain.company.com)의 경우 인증서에는 해당 도메인의 모든 호스트 이름이 암묵적으로 포함됩니다.

CA 인증서 가져오기

Microsoft 관리 콘솔(MMC)을 사용하여 CA 인증서를 SnapCenter 서버와 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.
2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
3. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > *인증서*를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 버튼으로 클릭한 다음, 모든 작업 > *가져오기*를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
개인 키 가져오기	예 옵션을 선택하고 개인 키를 가져온 후 *다음*을 클릭합니다.
가져오기 파일 형식	변경하지 마세요. *다음*을 클릭하세요.
보안	내보낸 인증서에 사용할 새 비밀번호를 지정한 후 *다음*을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.



인증서 가져오기는 개인 키와 함께 제공되어야 합니다(지원되는 형식: *.pfx, *.p12, *.p7b).

7. "개인" 폴더에 대해서도 5단계를 반복합니다.

CA 인증서 지문을 받으세요

인증서 지문은 인증서를 식별하는 16진수 문자열입니다. 지문은 지문 알고리즘을 사용하여 인증서 내용으로부터 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.

- 인증서를 두 번 클릭합니다.
- 인증서 대화 상자에서 세부정보 탭을 클릭합니다.
- 필드 목록을 스크롤하여 *지문*을 클릭하세요.
- 상자에서 16진수 문자를 복사하세요.
- 16진수 사이의 공백을 제거하세요.

예를 들어, 지문이 "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b"인 경우 공백을 제거하면 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.

- 다음 명령을 실행하여 설치된 인증서의 지문을 나열하고 주체 이름으로 최근에 설치된 인증서를 식별합니다.

```
Get-Childitem -경로 인증서:\LocalMachine\My
```

- 지문을 복사하세요.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스로 CA 인증서를 구성해야 합니다.

SnapCenter 서버와 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCORE 기본 포트 8145를 사용하는 기존 인증서 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

예를 들어:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스에 바인딩합니다.
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

예를 들어:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Linux 호스트에서 SnapCenter IBM Db2 플러그인 서비스에 대한 CA 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 `_opt/ NetApp/snapcenter/scc/etc_`에 위치한 'keystore.jks' 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 CA 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 'KEYSTORE_PASS' 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

```
keytool -storepasswd -keystore keystore.jks
. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된
비밀번호와 동일하게 변경합니다.
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

`agent.properties` 파일의 KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

3. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 있는 폴더로 이동합니다: /opt/ NetApp/snapcenter/scc/etc.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

· 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키스토어 /opt/ NetApp/snapcenter/scc/etc가 포함된 폴더로 이동합니다.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 agent.properties 파일의 KEYSTORE_PASS 키 값입니다.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자("*", ",", ")가 포함된 경우 별칭 이름을 간단한 이름으로 변경합니다.

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. agent.properties 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

8. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 'opt/ NetApp/snapcenter/scc/etc/crl'입니다.

단계

1. agent.properties 파일에서 기본 디렉토리를 CRL_PATH 키에 맞춰 수정하고 업데이트할 수 있습니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

Windows 호스트에서 **SnapCenter IBM Db2** 플러그인 서비스에 대한 **CA** 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc_에 있는 _keystore.jks 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 **CA** 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 KEYSTORE_PASS 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

키툴 -스토어패스워드 -키스토어 키스토어.jks



Windows 명령 프롬프트에서 "keytool" 명령을 인식하지 못하는 경우 keytool 명령을 해당 전체 경로로 바꾸세요.

```
C:\Program Files\Java\<jdk_버전>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.

키tool -키패스워드 -별칭 "인증서의 별칭_이름" -키스토어 키스토어.jks

agent.properties 파일의 KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

4. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc
2. keystore.jks 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

키툴 `-importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -대상키스토어 keystore.jks -대상키스토어 유형 JKS`

5. 키스토어에 추가된 인증서를 나열합니다.

`keytool -list -v -keystore keystore.jks`

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.

7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 `agent.properties` 파일의 `KEYSTORE_PASS` 키 값입니다.

키툴 -키패스워드 -별칭 "CA_인증서의_별칭_이름" -키스토어 키스토어.jks

8. `agent.properties` 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 `SCC_CERTIFICATE_ALIAS` 키에 대해 업데이트합니다.

9. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

SnapCenter 플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- 관련 CA 인증서에 대한 최신 CRL 파일을 다운로드하려면 다음을 참조하세요. "[SnapCenter CA 인증서에서 인증서 해지 목록 파일을 업데이트하는 방법](#)".
- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 `'C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\crl'`입니다.

단계

1. `agent.properties` 파일에서 기본 디렉토리를 `CRL_PATH` 키에 맞춰 수정하고 업데이트할 수 있습니다.
2. 이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다.

수신 인증서는 각 CRL에 대해 검증됩니다.

플러그인에 대한 CA 인증서 활성화

CA 인증서를 구성하고 SnapCenter 서버와 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- `Set-SmCertificateSettings` cmdlet을 실행하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- `_Get-SmCertificateSettings_`를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 하나 또는 여러 개의 플러그인 호스트를 선택하세요.
4. *추가 옵션*을 클릭하세요.
5. *인증서 검증 사용*을 선택합니다.

당신이 완료한 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- *  *는 CA 인증서가 활성화되지 않았거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- *  *는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- *  *는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- *  *는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

데이터 보호를 준비하세요

IBM Db2용 SnapCenter 플러그인을 사용하기 위한 전제 조건

IBM Db2용 SnapCenter 플러그인을 사용하기 전에 SnapCenter 관리자가 SnapCenter 서버를 설치하고 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다.
- SnapCenter 서버에 로그인합니다.
- 해당되는 경우 스토리지 시스템 연결을 추가하고 자격 증명을 생성하여 SnapCenter 환경을 구성합니다.
- Linux 또는 Windows 호스트에 Java 11을 설치합니다.

호스트 머신의 환경 경로 변수에 Java 경로를 설정해야 합니다.

- 백업 복제가 필요한 경우 SnapMirror 와 SnapVault 설정하세요.

IBM Db2를 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식

SnapCenter 사용하기 전에 수행하려는 백업, 복제 및 복원 작업과 관련된 기본 개념을 이해하는 것이 좋습니다. 다양한 작업을 위해 리소스, 리소스 그룹 및 정책과 상호 작용합니다.

- 리소스는 일반적으로 SnapCenter 로 백업하거나 복제하는 IBM Db2 데이터베이스입니다.
- SnapCenter 리소스 그룹은 호스트의 리소스 모음입니다.

리소스 그룹에서 작업을 수행하면 리소스 그룹에 대해 지정한 일정에 따라 리소스 그룹에 정의된 리소스에서 해당

작업이 수행됩니다.

필요에 따라 단일 리소스나 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 수행할 수도 있습니다.

- 정책은 데이터 보호 작업의 백업 빈도, 복제, 스크립트 및 기타 특성을 지정합니다.

리소스 그룹을 만들 때 해당 그룹에 대한 하나 이상의 정책을 선택합니다. 단일 리소스에 대해 주문형 백업을 수행할 때 정책을 선택할 수도 있습니다.

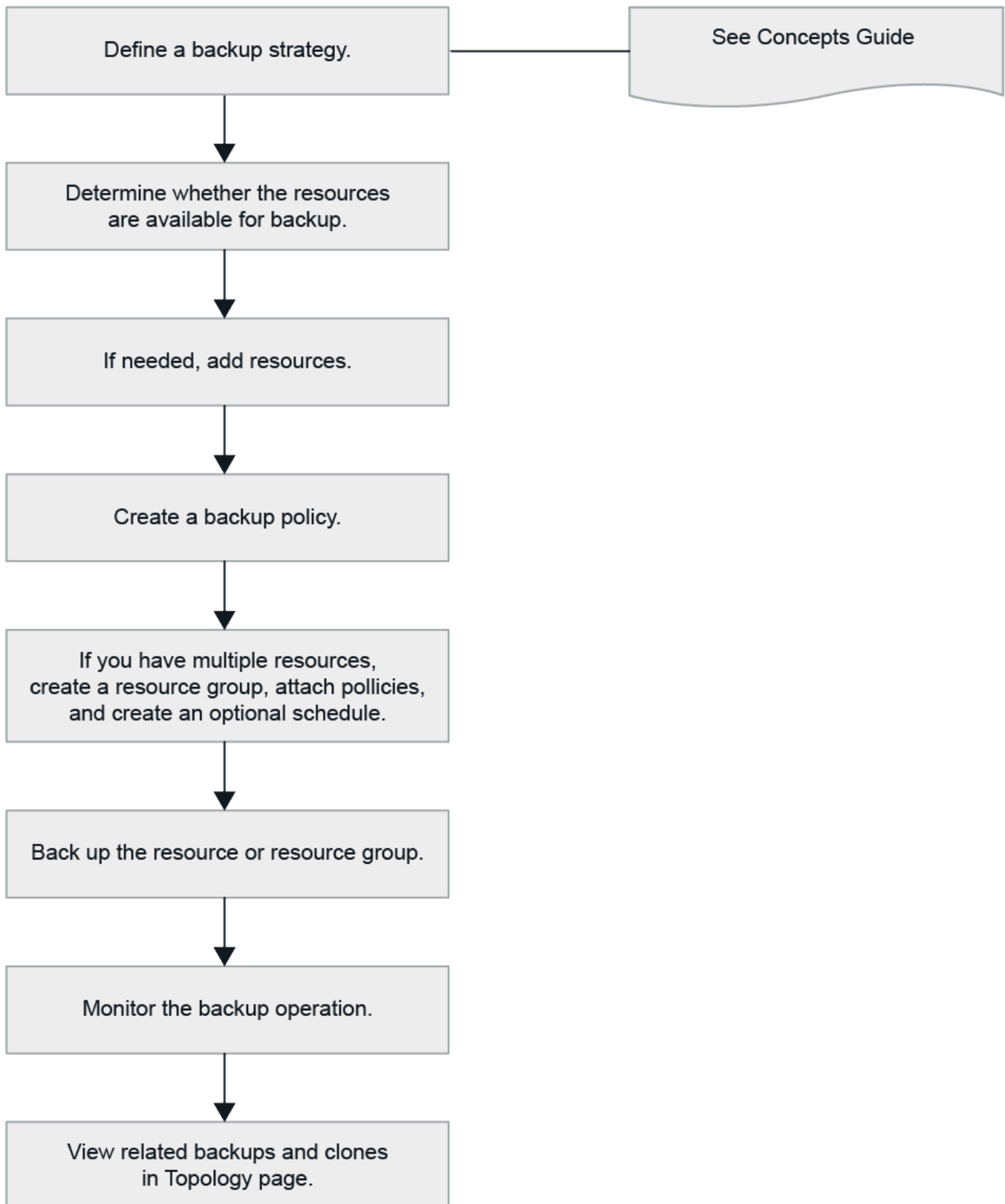
리소스 그룹은 무엇을 보호하고 싶은지, 언제 보호하고 싶은지 날짜와 시간을 정의하는 것으로 생각하면 됩니다. 정책이란 그것을 어떻게 보호할 것인지를 정의하는 것이라고 생각하세요. 예를 들어 모든 데이터베이스를 백업하는 경우 호스트의 모든 데이터베이스를 포함하는 리소스 그룹을 만들 수 있습니다. 그런 다음 리소스 그룹에 일일 정책과 시간별 정책이라는 두 가지 정책을 첨부할 수 있습니다. 리소스 그룹을 만들고 정책을 첨부할 때 리소스 그룹이 매일 전체 백업을 수행하도록 구성할 수 있습니다.

IBM Db2 리소스 백업

IBM Db2 리소스 백업

리소스(데이터베이스) 또는 리소스 그룹의 백업을 만들 수 있습니다. 백업 워크플로에는 계획, 백업할 데이터베이스 식별, 백업 정책 관리, 리소스 그룹 생성 및 정책 연결, 백업 생성, 작업 모니터링이 포함됩니다.

다음 워크플로는 백업 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

데이터베이스를 자동으로 검색합니다

리소스는 SnapCenter 에서 관리하는 Linux 호스트의 IBM Db2 데이터베이스입니다. 사용 가능한 IBM Db2 데이터베이스를 발견한 후 리소스 그룹에 리소스를 추가하여 데이터 보호 작업을 수행할 수 있습니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 설정 등의 작업을 이미 완료했어야 합니다.
- IBM Db2용 SnapCenter 플러그인은 RDM/VMDK 가상 환경에 있는 리소스의 자동 검색을 지원하지 않습니다. 데이터베이스를 수동으로 추가하는 동안 가상 환경에 대한 저장소 정보를 제공해야 합니다.

이 작업에 관하여

- 플러그인을 설치하면 해당 Linux 호스트의 모든 데이터베이스가 자동으로 검색되어 리소스 페이지에 표시됩니다.
- 데이터베이스만 자동으로 검색됩니다.

자동으로 검색된 리소스는 수정하거나 삭제할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 IBM Db2용 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 리소스 유형을 선택합니다.
3. (선택사항) *를 클릭하세요  *를 선택한 다음 호스트 이름을 선택합니다.

그런 다음 *를 클릭할 수 있습니다.  * 필터 창을 닫습니다.

4. 호스트에서 사용 가능한 리소스를 알아보려면 *리소스 새로 고침*을 클릭하세요.

리소스는 리소스 유형, 호스트 이름, 연관된 리소스 그룹, 백업 유형, 정책 및 전반적인 상태와 같은 정보와 함께 표시됩니다.

- 데이터베이스가 NetApp 스토리지에 있고 보호되지 않은 경우 전체 상태 열에 보호되지 않음이 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되며 백업 작업이 수행되지 않은 경우, 전체 상태 열에 백업이 실행되지 않았습나다라는 메시지가 표시됩니다. 그렇지 않으면 마지막 백업 상태에 따라 상태가 백업 실패 또는 백업 성공으로 변경됩니다.



SnapCenter 외부에서 데이터베이스 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

플러그인 호스트에 수동으로 리소스 추가

Windows 호스트에서는 자동 검색이 지원되지 않습니다. Db2 인스턴스와 데이터베이스 리소스를 수동으로 추가해야 합니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 설정 등의 작업을 완료했어야 합니다.

이 작업에 관하여

다음 구성에서는 수동 검색이 지원되지 않습니다.

- RDM 및 VMDK 레이아웃

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 드롭다운 목록에서 IBM Db2용 SnapCenter 플러그인을 선택합니다.
2. 리소스 페이지에서 *IBM DB2 리소스 추가*를 클릭합니다.
3. 리소스 세부 정보 제공 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	데이터베이스 이름을 지정하세요.
호스트 이름	호스트 이름을 입력하세요.
유형	데이터베이스 또는 인스턴스를 선택하세요.
사례	데이터베이스의 부모인 인스턴스의 이름을 지정합니다.
신임장	자격 증명을 선택하거나 자격 증명에 대한 정보를 추가하세요. 이는 선택 사항입니다.

4. 스토리지 공간 제공 페이지에서 스토리지 유형을 선택하고 하나 이상의 볼륨, LUN, Qtree를 선택한 다음 *저장*을 클릭합니다.

선택 사항: *를 클릭할 수 있습니다.  * 아이콘을 클릭하면 다른 스토리지 시스템에서 볼륨, LUN, Q트리를 추가할 수 있습니다.

5. 선택 사항: 리소스 설정 페이지에서 Windows 호스트의 리소스에 대해 IBM Db2 플러그인에 대한 사용자 정의 키-값 쌍을 입력합니다.
6. 요약 검토한 후 *마침*을 클릭하세요.

호스트 이름, 연관된 리소스 그룹 및 정책, 전반적인 상태와 같은 정보와 함께 데이터베이스가 표시됩니다.

사용자에게 리소스에 대한 액세스 권한을 제공하려면 사용자에게 리소스를 할당해야 합니다. 이를 통해 사용자는 자신에게 할당된 자산에 대해 권한이 있는 작업을 수행할 수 있습니다.

["사용자 또는 그룹을 추가하고 역할과 자산을 할당합니다."](#)

데이터베이스를 추가한 후 IBM Db2 데이터베이스 세부 정보를 수정할 수 있습니다.

IBM Db2에 대한 백업 정책 만들기

SnapCenter 사용하여 IBM Db2 리소스를 백업하기 전에 백업하려는 리소스 또는 리소스 그룹에 대한 백업 정책을 만들어야 합니다. 백업 정책은 백업을 관리, 일정을 정하고 보관하는 방법을 규정하는 일련의 규칙입니다.

시작하기 전에

- 백업 전략을 정의했어야 합니다.

자세한 내용은 IBM Db2 데이터베이스에 대한 데이터 보호 전략 정의에 대한 정보를 참조하세요.

- SnapCenter 설치, 호스트 추가, 스토리지 시스템 연결 설정, 리소스 추가 등의 작업을 완료하여 데이터 보호를 준비했어야 합니다.
- 스냅샷을 미리 또는 볼트에 복제하는 경우 SnapCenter 관리자가 소스 및 대상 볼륨 모두에 대한 SVM을 할당해야 합니다.

또한 정책에서 복제, 스크립트 및 애플리케이션 설정을 지정할 수 있습니다. 이러한 옵션을 사용하면 다른 리소스 그룹에 대한 정책을 재사용할 때 시간을 절약할 수 있습니다.

이 작업에 관하여

- SnapLock
 - '특정 기간 동안 백업 사본을 보관합니다' 옵션을 선택한 경우 SnapLock 보관 기간은 언급된 보관 기간보다 짧거나 같아야 합니다.
 - 스냅샷 잠금 기간을 지정하면 보존 기간이 만료될 때까지 스냅샷이 삭제되지 않습니다. 이로 인해 정책에 지정된 수보다 더 많은 수의 스냅샷을 보관하게 될 수 있습니다.
 - ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

- 왼쪽 탐색 창에서 *설정*을 클릭합니다.
- 설정 페이지에서 *정책*을 클릭합니다.
- *새로 만들기*를 클릭합니다.
- 이름 페이지에서 정책 이름과 세부 정보를 입력합니다.
- 정책 유형 페이지에서 다음을 수행합니다.
 - 저장 유형을 선택하세요.
 - 사용자 정의 백업 설정 섹션에서 플러그인에 키-값 형식으로 전달해야 하는 특정 백업 설정을 제공합니다.

플러그인에 전달할 여러 개의 키-값을 제공할 수 있습니다.

- 스냅샷 및 복제 페이지에서 다음 작업을 수행합니다.

- 주문형, 매시간, 매일, 매주, 매월 중에서 선택하여 일정 빈도를 지정하세요.



리소스 그룹을 생성하는 동안 백업 작업에 대한 일정(시작 날짜, 종료 날짜, 빈도)을 지정할 수 있습니다. 이를 통해 동일한 정책과 백업 빈도를 공유하는 리소스 그룹을 만들 수 있을 뿐만 아니라 각 정책에 다른 백업 일정을 할당할 수도 있습니다.



오전 2시로 예약한 경우, 일광 절약 시간제(DST) 기간에는 일정이 실행되지 않습니다.

- 스냅샷 설정 섹션에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	그 다음에...
특정 수의 스냅샷을 보관하세요	*보관할 사본*을 선택한 다음 보관하려는 스냅샷 수를 지정합니다. 스냅샷 수가 지정된 수를 초과하면 스냅샷이 삭제되고 가장 오래된 사본이 먼저 삭제됩니다.
스냅샷을 특정 일수 동안 보관하세요	*사본 보관 기간*을 선택한 다음, 스냅샷을 삭제하기 전에 보관할 일수를 지정합니다.
스냅샷 복사 잠금 기간	*스냅샷 복사 잠금 기간*을 선택하고 일, 월 또는 년을 지정합니다. 스냅샷 보관 기간은 100년 미만이어야 합니다.



스냅샷 복사 기반 백업의 경우 SnapVault 복제를 활성화하려면 보존 횟수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷이 대상에 복제될 때까지 첫 번째 스냅샷이 SnapVault 관계에 대한 참조 스냅샷이기 때문에 보존 작업이 실패할 수 있습니다.

b. 정책 라벨을 지정합니다.

원격 복제를 위해 기본 스냅샷에 SnapMirror 레이블을 할당하면 기본 스냅샷이 SnapCenter 에서 ONTAP 보조 시스템으로 스냅샷 복제 작업을 오프로드할 수 있습니다. 정책 페이지에서 SnapMirror 또는 SnapVault 옵션을 활성화하지 않고도 이 작업을 수행할 수 있습니다.

7. 보조 복제 옵션 선택 섹션에서 다음 보조 복제 옵션 중 하나 또는 둘 다를 선택합니다.

이 분야에서는...	이렇게 하세요...
로컬 스냅샷 복사본을 만든 후 SnapMirror 업데이트	다른 볼륨에 백업 세트의 미러 복사본을 생성하려면 이 필드를 선택합니다(SnapMirror 복제). SnapMirror Active Sync의 경우 이 옵션을 활성화해야 합니다.
로컬 스냅샷 복사본을 만든 후 SnapVault 업데이트	디스크 간 백업 복제(SnapVault 백업)를 수행하려면 이 옵션을 선택하세요.
오류 재시도 횟수	작업이 중지되기 전에 허용할 수 있는 최대 복제 시도 횟수를 입력하세요.



보조 저장소의 스냅샷 최대 한도에 도달하지 않도록 하려면 ONTAP 에서 보조 저장소 SnapMirror 보존 정책을 구성해야 합니다.

8. 요약 검토한 후 *마침*을 클릭하세요.

리소스 그룹을 만들고 정책을 첨부합니다.

리소스 그룹은 백업하고 보호하려는 리소스를 추가해야 하는 컨테이너입니다. 리소스 그룹을 사용하면 주어진 애플리케이션과 관련된 모든 데이터를 동시에 백업할 수 있습니다. 모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한, 수행하려는 데이터 보호 작업 유형을 정의하려면 리소스 그룹에 하나 이상의 정책을 연결해야 합니다.

이 작업에 관하여

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	리소스 그룹의 이름을 입력하세요.  리소스 그룹 이름은 250자를 넘을 수 없습니다.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력하세요. 예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.
스냅샷 복사에 사용자 정의 이름 형식 사용	이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다. 예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

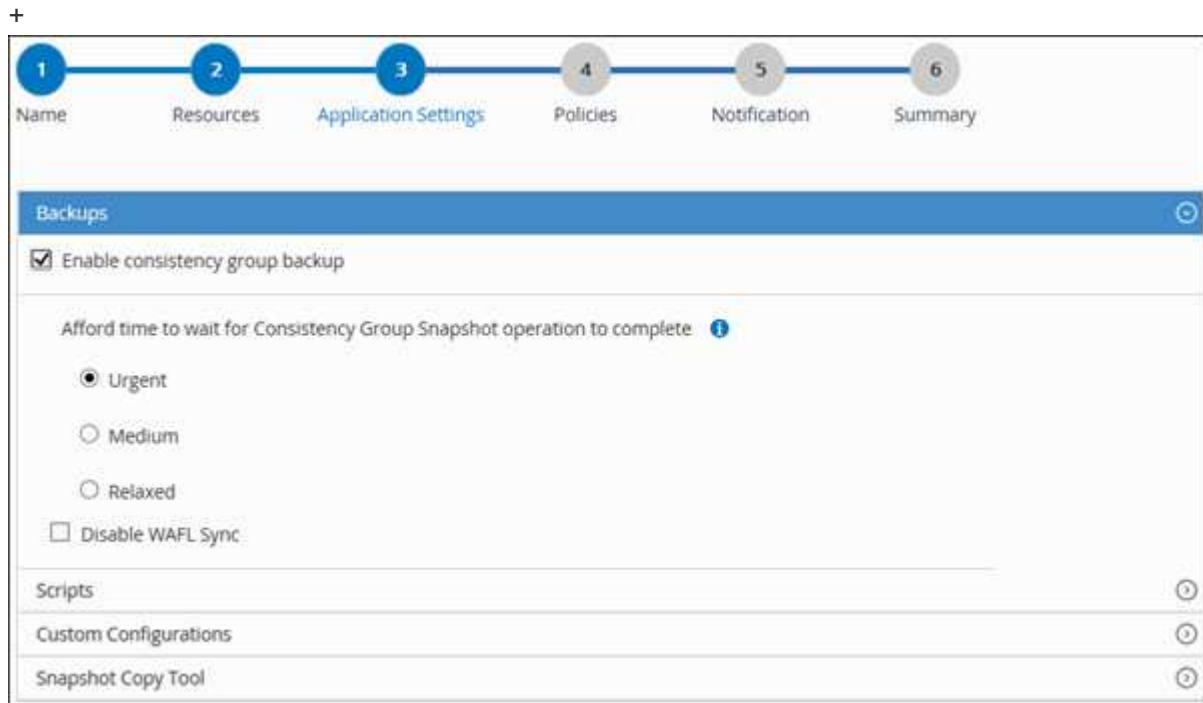
4. 리소스 페이지에서 호스트 드롭다운 목록에서 호스트 이름을 선택하고 리소스 유형 드롭다운 목록에서 리소스 유형을 선택합니다.

이는 화면에 표시되는 정보를 필터링하는 데 도움이 됩니다.

5. 사용 가능한 리소스 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 클릭하여 선택한 리소스 섹션으로 이동합니다.
6. 애플리케이션 설정 페이지에서 다음을 수행합니다.
 - a. 추가 백업 옵션을 설정하려면 백업 화살표를 클릭하세요.

일관성 그룹 백업을 활성화하고 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
일관성 그룹 스냅샷 작업이 완료될 때까지 기다릴 시간을 확보하세요.	스냅샷 작업이 완료될 때까지의 대기 시간을 지정하려면 긴급, 보통, *느슨함*을 선택합니다. 긴급 = 5초, 보통 = 7초, 여유 = 20초.
WAFL 동기화 비활성화	WAFL 일관성 지점을 강제로 적용하지 않으려면 이 옵션을 선택하세요.



- 스크립트 화살표를 클릭하고 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령을 입력합니다. 실패 시 종료하기 전에 실행할 사전 명령을 입력할 수도 있습니다.
- 사용자 정의 구성 화살표를 클릭하고 이 리소스를 사용하는 모든 데이터 보호 작업에 필요한 사용자 정의 키-값 쌍을 입력합니다.

매개변수	환경	설명
아카이브 로그 활성화	(예/아니요)	보관 로그 관리를 통해 보관 로그를 삭제할 수 있습니다.
아카이브 로그 보존	일수	보관 로그를 보관하는 일수를 지정합니다. 이 설정은 NTAP_SNAPSHOT_RETENTIONS보다 크거나 같아야 합니다.

매개변수	환경	설명
아카이브_로그_디렉토리	변경_정보_디렉토리/로그	보관 로그가 포함된 디렉토리의 경로를 지정합니다.
아카이브_로그_확장	파일 확장자	보관 로그 파일 확장자 길이를 지정합니다. 예를 들어, 보관 로그가 log_backup_0_0_0_0.161518551942 9이고 file_extension 값이 5이면 로그 확장자는 5자리인 16151을 유지합니다.
ARCHIVE_LOG_RECURSIVE_SE ARCH	(예/아니요)	하위 디렉토리 내의 보관 로그 관리를 활성화합니다. 보관 로그가 하위 디렉토리에 있는 경우 이 매개변수를 사용해야 합니다.



사용자 정의 키-값 쌍은 IBM Db2 Linux 플러그인 시스템에서는 지원되지만 중앙화된 Windows 플러그인으로 등록된 IBM Db2 데이터베이스에서는 지원되지 않습니다.

- c. 스냅샷 복사 도구* 화살표를 클릭하여 스냅샷을 만드는 도구를 선택하세요.

원하신다면...	그 다음에...
SnapCenter Windows용 플러그인을 사용하여 스냅샷을 생성하기 전에 파일 시스템을 일관된 상태로 만듭니다. Linux 리소스의 경우 이 옵션은 적용되지 않습니다.	*파일 시스템 일관성을 갖춘 SnapCenter *를 선택하세요.
SnapCenter 사용하여 스토리지 수준 스냅샷을 생성합니다.	*파일 시스템 일관성이 없는 SnapCenter *를 선택하세요.
스냅샷 복사본을 생성하기 위해 호스트에서 실행할 명령을 입력합니다.	*기타*를 선택한 다음 호스트에서 실행할 명령을 입력하여 스냅샷을 생성합니다.

7. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다. *.

정책은 '선택한 정책에 대한 일정 구성' 섹션에 나열되어 있습니다.

- b.

일정 구성 열에서 *를 클릭합니다.  * 구성하려는 정책에 대해.

- c. 정책 `_policy_name_`에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 `policy_name`은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP 서버는 설정 > *전역 설정*에서 구성해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

ASA r2 시스템에서 IBM Db2 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.

ASA r2 시스템에 있는 리소스를 추가하려면 리소스 그룹을 만들어야 합니다. 리소스 그룹을 생성하는 동안 보조 보호를 프로비저닝할 수도 있습니다.

시작하기 전에

- ONTAP 9.x 리소스와 ASA r2 리소스를 동일한 리소스 그룹에 추가하지 않도록 해야 합니다.
- ONTAP 9.x 리소스와 ASA r2 리소스가 모두 포함된 데이터베이스가 없는지 확인해야 합니다.

이 작업에 관하여

- 2차 보호는 로그인한 사용자에게 **SecondaryProtection** 기능이 활성화된 역할이 할당된 경우에만 사용할 수 있습니다.
- 2차 보호를 활성화한 경우 기본 및 2차 일관성 그룹을 생성하는 동안 리소스 그룹은 유지 관리 모드로 전환됩니다. 기본 및 보조 일관성 그룹이 생성된 후 리소스 그룹은 유지 관리 모드에서 해제됩니다.
- SnapCenter 클론 리소스에 대한 보조 보호를 지원하지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.
 - a. 이름 필드에 리소스 그룹의 이름을 입력합니다.



리소스 그룹 이름은 250자를 넘을 수 없습니다.

- b. 나중에 리소스 그룹을 검색하는 데 도움이 되도록 태그 필드에 하나 이상의 레이블을 입력하세요.

예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.

- c. 이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다.
기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

d. 백업하지 않을 보관 로그 파일의 대상을 지정합니다.



필요한 경우 접두사를 포함하여 애플리케이션에 설정된 것과 정확히 동일한 목적지를 사용해야 합니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 데이터베이스 호스트 이름을 선택합니다.



리소스가 성공적으로 검색된 경우에만 해당 리소스가 사용 가능한 리소스 섹션에 나열됩니다.
최근에 리소스를 추가한 경우 리소스 목록을 새로 고침 후에만 사용 가능한 리소스 목록에 표시됩니다.

5. 사용 가능한 리소스 섹션에서 ASA r2 리소스를 선택하고 선택한 리소스 섹션으로 이동합니다.

6. 애플리케이션 설정 페이지에서 백업 옵션을 선택하세요.

7. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



또한 다음을 클릭하여 정책을 생성할 수도 있습니다. .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.

c. 정책_policy_name_에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 _policy_name_은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 선택한 정책에 대해 보조 보호가 활성화된 경우 보조 보호 페이지가 표시되며 다음 단계를 수행해야 합니다.

a. 복제 정책의 유형을 선택하세요.



동기 복제 정책은 지원되지 않습니다.

b. 사용할 일관성 그룹 접미사를 지정합니다.

c. 대상 클러스터 및 대상 SVM 드롭다운에서 사용하려는 피어링된 클러스터와 SVM을 선택합니다.



SnapCenter에서는 클러스터 및 SVM 피어링을 지원하지 않습니다. 클러스터 및 SVM 피어링을 수행하려면 System Manager 또는 ONTAP CLI를 사용해야 합니다.



리소스가 이미 SnapCenter 외부에서 보호되고 있는 경우 해당 리소스는 보조 보호 리소스 섹션에 표시됩니다.

1. 확인 페이지에서 다음 단계를 수행하세요.

- a. *로케이터 로드*를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 저장소에서 검증을 수행합니다.
- b. 딸깍 하는 소리  일정 구성 열에서 정책의 모든 일정 유형에 대한 확인 일정을 구성합니다.
- c. 확인 일정 추가 policy_name 대화 상자에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	이렇게 하세요...
백업 후 검증 실행	*백업 후 검증 실행*을 선택하세요.
검증 일정을 예약하세요	*예약된 확인 실행*을 선택한 다음 드롭다운 목록에서 일정 유형을 선택합니다.

- d. 보조 저장소 시스템에서 백업을 확인하려면 *보조 위치에서 확인*을 선택하세요.
- e. *확인*을 클릭합니다.

구성된 검증 일정은 적용된 일정 열에 나열됩니다.

2. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*을 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtplibServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

3. 요약 검토 후 *마침*을 클릭하세요.

PowerShell cmdlet을 사용하여 IBM Db2용 스토리지 시스템 연결 및 자격 증명 만들기

PowerShell cmdlet을 사용하여 IBM Db2 데이터베이스를 백업, 복원 또는 복제하려면 먼저 SVM(스토리지 가상 머신) 연결과 자격 증명을 만들어야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 저장소 연결을 생성하려면 인프라 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

스토리지 시스템 연결을 추가하는 동안에는 호스트 플러그인 설치가 진행 중이어서는 안 됩니다. 호스트 캐시가 업데이트되지 않고 SnapCenter GUI에 데이터베이스 상태가 “백업에 사용할 수 없음” 또는 “NetApp 스토리지에 없음”으로 표시될 수 있기 때문입니다.

- 저장 시스템 이름은 고유해야 합니다.

SnapCenter 서로 다른 클러스터에 동일한 이름을 가진 여러 스토리지 시스템을 지원하지 않습니다. SnapCenter 에서 지원하는 각 스토리지 시스템은 고유한 이름과 고유한 데이터 LIF IP 주소를 가져야 합니다.

단계

1. *SnapCenterPS*를 클릭하여 PowerShell Core를 시작합니다.
2. Add-SmStorageConnection cmdlet을 사용하여 스토리지 시스템에 대한 새 연결을 만듭니다.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap  
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Add-SmCredential cmdlet을 사용하여 새 자격 증명을 만듭니다.

이 예제에서는 Windows 자격 증명을 사용하여 FinanceAdmin이라는 새 자격 증명을 만드는 방법을 보여줍니다.

```
PS C:\> Add-SmCredential -Name 'FinanceAdmin' -Type Linux  
-AuthenticationType PasswordBased -Credential db2hostuser  
-EnableSudoPrivileges:$true
```

4. SnapCenter Server에 IBM Db2 통신 호스트를 추가합니다.

Linux의 경우:

```
PS C:\> Add-SmHost -HostType Linux -HostName '10.232.204.61'  
-CredentialName 'defaultcreds'
```

Windows의 경우:

```
PS C:\> Add-SmHost -HostType Windows -HostName '10.232.204.61'  
-CredentialName 'defaultcreds'
```

5. 호스트에 패키지와 IBM Db2용 SnapCenter 플러그인을 설치합니다.

Linux의 경우:

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes  
DB2
```

Windows의 경우:

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes DB2, SCW
```

6. SQLLIB의 경로를 설정합니다.

Windows의 경우 Db2 플러그인은 SQLLIB 폴더의 기본 경로인 "C:\Program Files\IBM\SQLLIB\BIN"을 사용합니다.

기본 경로를 재정의하려면 다음 명령을 사용하세요.

```
PS C:\> Set-SmConfigSettings -Plugin -HostName '10.232.204.61' -PluginCode DB2 -configSettings @{"DB2_SQLLIB_CMD"="<custom_path>\IBM\SQLLIB\BIN"}
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

Db2 데이터베이스 백업

데이터베이스 백업에는 SnapCenter 서버와의 연결 설정, 리소스 추가, 정책 추가, 백업 리소스 그룹 생성 및 백업이 포함됩니다.

시작하기 전에

- 백업 정책을 생성했어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에 "snapmirror all" 권한이 포함되어야 합니다. 하지만 "vsadmin" 역할을 사용하는 경우 "snapmirror all" 권한은 필요하지 않습니다.
- 스냅샷 복사 기반 백업 작업의 경우 모든 테넌트 데이터베이스가 유효하고 활성화되어 있는지 확인하세요.
- 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령의 경우, 플러그인 호스트에서 다음 경로의 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Linux 호스트의 기본 위치: */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

선택하다 그런 다음 호스트 이름과 리소스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 선택할 수 있습니다. 필터 창을 닫으려면.

3. 백업할 리소스를 선택하세요.
4. 리소스 페이지에서 *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택한 다음 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, *customtext_policy_hostname* 또는 *_resource_hostname_*입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

5. 애플리케이션 설정 페이지에서 다음을 수행합니다.

- 추가 백업 옵션을 설정하려면 백업 화살표를 선택하세요.

필요한 경우 일관성 그룹 백업을 활성화하고 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
"일관성 그룹 스냅샷" 작업이 완료될 때까지 기다릴 시간을 확보하세요.	스냅샷 작업이 완료될 때까지의 대기 시간을 지정하려면 긴급, 보통, *느슨함*을 선택합니다. 긴급 = 5초, 보통 = 7초, 여유 = 20초.
WAFL 동기화 비활성화	WAFL 일관성 지점을 강제로 적용하지 않으려면 이 옵션을 선택하세요.

- 스크립트 화살표를 선택하여 정지, 스냅샷 및 정지 해제 작업에 대한 사전 및 사후 명령을 실행합니다.

백업 작업을 종료하기 전에 사전 명령을 실행할 수도 있습니다. Prescript와 Postscript는 SnapCenter Server에서 실행됩니다.

- 사용자 정의 구성 화살표를 선택한 다음, 이 리소스를 사용하는 모든 작업에 필요한 사용자 정의 값 쌍을 입력합니다.
- 스냅샷 복사 도구* 화살표를 선택하여 스냅샷을 만드는 도구를 선택하세요.

원하신다면...	그 다음에...
SnapCenter 사용하여 스토리지 수준 스냅샷을 생성합니다.	*파일 시스템 일관성이 없는 SnapCenter *를 선택하세요.
SnapCenter Windows용 플러그인을 사용하여 파일 시스템을 일관된 상태로 만든 다음 스냅샷을 생성합니다.	*파일 시스템 일관성을 갖춘 SnapCenter *를 선택하세요.

원하신다면...	그 다음에...
스냅샷을 생성하는 명령을 입력하려면	*기타*를 선택한 다음 스냅샷을 만드는 명령을 입력합니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다. *.

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

b. 선택하다 * 일정을 구성하려는 정책에 대한 일정 구성 옆에 있습니다.

c. 정책 _policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 선택합니다.

_policy_name_은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 옆에 나열됩니다.

7. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > *전역 설정*에서도 구성해야 합니다.

8. 요약 검토한 후 *마침*을 선택하세요.

리소스 토폴로지 페이지가 표시됩니다.

9. *지금 백업*을 선택하세요.
10. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스에 여러 정책을 적용한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.
 - b. *백업*을 선택하세요.
11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.
 - MetroCluster 구성에서 SnapCenter 장애 조치 후 보호 관계를 감지하지 못할 수 있습니다.

자세한 내용은 다음을 참조하세요. ["MetroCluster 장애 조치 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다."](#)

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-SmConnection
```

사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.

2. Add-SmResources cmdlet을 사용하여 수동 리소스를 추가합니다.

이 예제에서는 IBM Db2 인스턴스를 추가하는 방법을 보여줍니다.

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Instance -ResourceName db2inst1 -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

Db2 데이터베이스의 경우:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Database -ResourceName SALESDB -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\" -Instance DB2
```

3. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.
4. Add-SmResourceGroup cmdlet을 사용하여 리소스를 보호하거나 SnapCenter 에 새 리소스 그룹을 추가합니다.

5. New-SmBackup cmdlet을 사용하여 새로운 백업 작업을 시작합니다.

이 예제에서는 리소스 그룹을 백업하는 방법을 보여줍니다.

```
C:\PS> New-SMBackup -ResourceGroupName  
'ResourceGroup_with_Db2_Resources' -Policy db2_policy1
```

이 예제에서는 Db2 인스턴스를 백업합니다.

```
C:\PS> New-SMBackup -Resources  
@{"Host"="10.32.212.13";"Uid"="DB2INST1";"PluginName"="DB2"} -Policy  
db2_policy
```

이 예제에서는 Db2 데이터베이스를 백업합니다.

```
C:\PS> New-SMBackup -Resources  
@{"Host"="10.32.212.13";"Uid"="DB2INST1\WINARCD";"PluginName"="DB2"  
} -Policy db2_policy
```

6. Get-smJobSummaryReport cmdlet을 사용하여 작업 상태(실행 중, 완료 또는 실패)를 모니터링합니다.

```
PS C:\> Get-SmJobSummaryReport -JobId 467  
  
SmJobId           : 467  
JobCreatedDateTime :  
JobStartDateTime  : 27-Jun-24 01:40:09  
JobEndDateTime    : 27-Jun-24 01:41:15  
JobDuration       : 00:01:06.7013330  
JobName           : Backup of Resource Group  
'SCDB201WIN_RAVIR1_OPENLAB_NETAPP_LOCAL_DB2_DB2_WINCIR' with policy  
'snapshot-based-db2'  
JobDescription    :  
Status            : Completed  
IsScheduled       : False  
JobError          :  
JobType           : Backup  
PolicyName        : db2_policy  
JobResultData     :
```

7. Get-SmBackupReport cmdlet을 사용하여 복원 또는 복제 작업을 수행하기 위한 백업 ID, 백업 이름과 같은 백업 작업 세부 정보를 모니터링합니다.

```
PS C:\> Get-SmBackupReport -JobId 467
```

```
BackedUpObjects      : {WINCIR}
FailedObjects        : {}
IsScheduled          : False
HasMetadata          : False
SmBackupId           : 84
SmJobId              : 467
StartDateTime        : 27-Jun-24 01:40:09
EndDateTime          : 27-Jun-24 01:41:15
Duration             : 00:01:06.7013330
CreatedDateTime      : 27-Jun-24 18:39:45
Status               : Completed
ProtectionGroupName  : HOSTFQDN_DB2_DB2_WINCIR
SmProtectionGroupId  : 23
PolicyName           : db2_policy
SmPolicyId           : 13
BackupName           : HOSTFQDN _DB2_DB2_WINCIR_HOST_06-27-
2024_01.40.09.7397
VerificationStatus   : NotApplicable
VerificationStatuses :
SmJobError           :
BackupType           : SCC_BACKUP
CatalogingStatus     : NotApplicable
CatalogingStatuses   :
ReportDataCreatedDateTime :
PluginCode           : SCC
PluginName           : DB2
PluginDisplayName     : IBM DB2
JobTypeId            :
JobHost              : HOSTFQDN
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

리소스 그룹 백업

리소스 그룹은 호스트의 리소스 모음입니다. 리소스 그룹에 대한 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다.

시작하기 전에

- 정책이 첨부된 리소스 그룹을 만들어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에 "snapmirror all" 권한이 포함되어야 합니다. 하지만 "vsadmin" 역할을 사용하는 경우 "snapmirror all" 권한은

필요하지 않습니다.

이 작업에 관하여

리소스 페이지에서 필요에 따라 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 첨부되고 일정이 구성된 경우 백업은 일정에 따라 자동으로 수행됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.

검색창에 리소스 그룹 이름을 입력하거나 다음을 선택하여 리소스 그룹을 검색할 수 있습니다.  , 그리고 태그를 선택합니다. 그런 다음 선택할 수 있습니다.  필터 창을 닫으려면.

3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음, *지금 백업*을 선택합니다.
4. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스 그룹에 여러 정책을 연결한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. *백업*을 선택하세요.

5. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

IBM Db2 백업 작업 모니터링

SnapCenterJobs 페이지를 사용하여 다양한 백업 작업의 진행 상황을 모니터링할 수 있습니다. 완료 시점이나 문제가 있는지 확인하기 위해 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 해당 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  백업 작업만 나열되도록 목록을 필터링합니다.

- b. 시작일과 종료일을 지정하세요.
- c. 유형 드롭다운 목록에서 *백업*을 선택합니다.
- d. 상태 드롭다운에서 백업 상태를 선택합니다.
- e. *적용*을 클릭하면 작업이 성공적으로 완료된 것을 볼 수 있습니다.

4. 백업 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인하세요.



백업 작업 상태가 표시됩니다. 작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 표시가 되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

활동 창에서 **IBM Db2** 데이터베이스의 데이터 보호 작업 모니터링

활동 창에는 가장 최근에 수행된 5개의 작업이 표시됩니다. 활동 창에는 작업이 시작된 시점과 작업 상태도 표시됩니다.

활동 창에는 백업, 복원, 복제 및 예약된 백업 작업에 대한 정보가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 딸깍 하는 소리 활동 창에서 가장 최근의 작업 5개를 확인하세요.

작업 중 하나를 클릭하면 작업 세부 정보가 작업 세부 정보 페이지에 나열됩니다.

IBM Db2에 대한 백업 작업 취소

대기 중인 백업 작업을 취소할 수 있습니다.

필요한 것

- 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 모니터 페이지나 활동 창에서 백업 작업을 취소할 수 있습니다.
- 실행 중인 백업 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 백업 작업을 취소할 수 있습니다.
- 취소할 수 없는 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 백업 작업을 취소할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	a. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. b. 작업을 선택한 다음 *작업 취소*를 클릭합니다.
활동 창	a. 백업 작업을 시작한 후 *를 클릭하세요.  * 활동 창에서 가장 최근의 작업 5개를 확인하세요. b. 작업을 선택하세요. c. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

작업이 취소되고 리소스는 이전 상태로 돌아갑니다.

토폴로지 페이지에서 IBM Db2 백업 및 복제본 보기

리소스를 백업하거나 복제할 준비를 할 때 기본 및 보조 저장소에 있는 모든 백업과 복제본을 그래픽으로 표현해 보면 도움이 될 수 있습니다.

이 작업에 관하여

다음 아이콘을 '사본 관리' 보기에서 검토하여 백업 및 복제본을 기본 저장소 또는 보조 저장소(미러 사본 또는 볼트 사본)에서 사용할 수 있는지 확인할 수 있습니다.

-  기본 스토리지에서 사용 가능한 백업 및 복제본의 수를 표시합니다.
-  SnapMirror 기술을 사용하여 보조 저장소에 미러링된 백업 및 복제본의 수를 표시합니다.
-  SnapVault 기술을 사용하여 보조 저장소에 복제된 백업 및 복제본의 수를 표시합니다.



표시된 백업 수에는 보조 저장소에서 삭제된 백업이 포함됩니다. 예를 들어, 4개의 백업만 보존하는 정책을 사용하여 6개의 백업을 만든 경우 표시되는 백업 수는 6개입니다.



미러 볼트 유형 볼륨의 버전 가변형 미러 백업의 복제본은 토폴로지 보기에 표시되지만, 토폴로지 보기의 미러 백업 수에는 버전 가변형 백업이 포함되지 않습니다.

토폴로지 페이지에서는 선택한 리소스 또는 리소스 그룹에 사용 가능한 모든 백업과 복제본을 볼 수 있습니다. 해당 백업 및 복제의 세부 정보를 보고 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.

3. 리소스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 리소스를 선택합니다.

리소스가 보호된 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. *요약 카드*를 검토하여 기본 및 보조 저장소에서 사용 가능한 백업 및 복제본 수에 대한 요약を確認하세요.

요약 카드 섹션에는 스냅샷 복사 기반 백업과 복제본의 총 수가 표시됩니다.

새로 고침 버튼을 클릭하면 저장소에 대한 쿼리가 시작되어 정확한 개수가 표시됩니다.

SnapLock 이 활성화된 백업을 수행한 경우 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간이 새로 고쳐집니다. 주간 일정은 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간도 새로 고칩니다.

애플리케이션 리소스가 여러 볼륨에 분산되어 있는 경우 백업에 대한 SnapLock 만료 시간은 볼륨의 스냅샷에 설정된 가장 긴 SnapLock 만료 시간이 됩니다. 가장 긴 SnapLock 만료 시간은 ONTAP 에서 검색됩니다.

주문형 백업 후, 새로 고침 버튼을 클릭하면 백업이나 복제의 세부 정보가 새로 고침됩니다.

5. 복사본 관리 보기에서 기본 또는 보조 저장소의 백업 또는 *복제*를 클릭하면 백업 또는 복제의 세부 정보를 볼 수 있습니다.

백업 및 복제의 세부 정보는 표 형식으로 표시됩니다.

6. 표에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 복제, 삭제 작업을 수행합니다.



보조 저장소에 있는 백업은 이름을 바꾸거나 삭제할 수 없습니다.

7. 복제본을 삭제하려면 테이블에서 복제본을 선택한 다음 클릭하세요. .

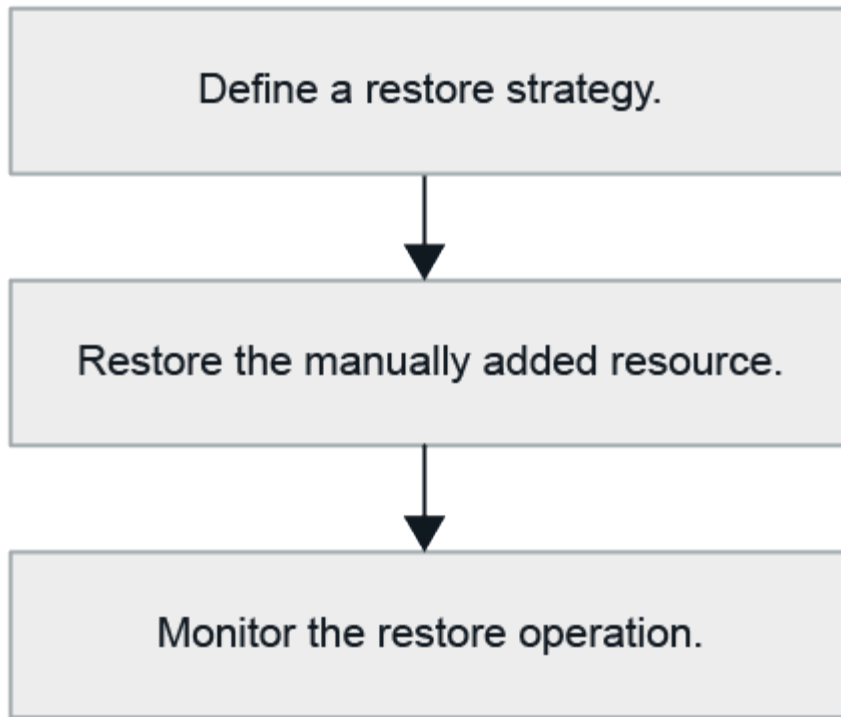
8. 복제본을 분할하려면 테이블에서 복제본을 선택한 다음 클릭하세요. .

IBM Db2 복원

워크플로 복원

복원 및 복구 워크플로에는 계획, 복원 작업 수행, 작업 모니터링이 포함됩니다.

다음 워크플로는 복원 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#) .

수동으로 추가된 리소스 백업 복원

SnapCenter 사용하면 하나 이상의 백업에서 데이터를 복원하고 복구할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 복원하려는 리소스 또는 리소스 그룹에 대해 현재 진행 중인 모든 백업 작업을 취소해야 합니다.
- 사전 복원, 사후 복원, 마운트 및 마운트 해제 명령의 경우, 다음 경로에서 플러그인 호스트에서 사용 가능한 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: `C:\Program Files\NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 호스트의 기본 위치: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 함께 표시됩니다.



백업은 리소스 그룹을 위한 것일 수 있지만 복원할 때는 복원할 개별 리소스를 선택해야 합니다.

리소스가 보호되지 않은 경우 전체 상태 열에 "보호되지 않음"이 표시됩니다. 이는 리소스가 보호되지 않았거나 다른 사용자가 리소스를 백업했음을 의미할 수 있습니다.

3. 리소스를 선택하거나 리소스 그룹을 선택한 다음 해당 그룹에서 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 기본 백업 테이블에서 복원하려는 백업을 선택한 다음 *를 클릭합니다. .

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scscr0191685001_01-05-2017-01:35:06.6463	1/5/2017 1:35:27 AM 

6. 복원 범위 페이지에서 *리소스 완료*를 선택합니다.

- a. *전체 리소스*를 선택하면 IBM Db2 데이터베이스의 구성된 모든 데이터 볼륨이 복원됩니다.

리소스에 볼륨이나 Q트리가 포함되어 있는 경우 해당 볼륨이나 Q트리에서 복원을 위해 선택한 스냅샷 이후에 생성된 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 다른 리소스가 동일한 볼륨이나 Q트리에 호스팅된 경우 해당 리소스도 삭제됩니다.

여러 개의 LUN을 선택할 수 있습니다.



*모두*를 선택하면 볼륨, Q트리 또는 LUN의 모든 파일이 복원됩니다.

7. 사전 작업 페이지에서 복원 작업을 수행하기 전에 실행할 사전 복원 및 마운트 해제 명령을 입력합니다.
8. Post ops 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.
9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > 전역 설정 페이지에서도 구성해야 합니다.

10. 요약을 검토한 후 *마침*을 클릭하세요.

11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

당신이 완료한 후

롤포워드 상태가 "DB 보류" 상태인 경우에만 복구가 가능합니다. 이 상태는 아카이브 로깅이 활성화된 Db2 데이터베이스에 적용됩니다.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-SmConnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 백업을 식별합니다.

이 예에서는 복원에 사용할 수 있는 백업이 두 개 있음을 보여줍니다.

```
PS C:\> Get-SmBackup -AppObjectId
cn24.sscore.test.com\DB2\db2inst1\Library

      BackupId      BackupName      BackupTime
-----
BackupType
-----
1      Payroll Dataset_vise-f6_08... 8/4/2015 11:02:32
AM Full Backup
2      Payroll Dataset_vise-f6_08... 8/4/2015 11:23:17
AM
```

이 예에서는 2015년 1월 29일부터 2015년 2월 3일까지의 백업에 대한 자세한 정보를 표시합니다.

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId          : 113
SmJobId              : 2032
StartDateTime        : 2/2/2015 6:57:03 AM
EndDateTime          : 2/2/2015 6:57:11 AM
Duration              : 00:00:07.3060000
CreatedDateTime       : 2/2/2015 6:57:23 AM
Status               : Completed
ProtectionGroupName  : Clone
SmProtectionGroupId   : 34
PolicyName            : Vault
SmPolicyId            : 18
BackupName            : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus    : NotVerified

SmBackupId          : 114
SmJobId              : 2183
StartDateTime        : 2/2/2015 1:02:41 PM
EndDateTime          : 2/2/2015 1:02:38 PM
Duration              : -00:00:03.2300000
CreatedDateTime       : 2/2/2015 1:02:53 PM
Status               : Completed
ProtectionGroupName  : Clone
SmProtectionGroupId   : 34
PolicyName            : Vault
SmPolicyId            : 18
BackupName            : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus    : NotVerified
```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.



AppObjectId는 "Host\Plugin\UID"이고, 여기서 UID = <instance_name>은 수동으로 검색된 DB2 인스턴스 리소스를 나타내고 UID = <instance_name>\<database_name>은 IBM Db2 데이터베이스 리소스를 나타냅니다. Get-smResources cmdlet에서 ResourceID를 가져올 수 있습니다.

```
Get-smResources -HostName cn24.sscore.test.com -PluginCode DB2
```

이 예제에서는 기본 저장소에서 데이터베이스를 복원하는 방법을 보여줍니다.

```
Restore-SmBackup -PluginCode DB2 -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 3
```

이 예제에서는 보조 저장소에서 데이터베이스를 복원하는 방법을 보여줍니다.

```
Restore-SmBackup -PluginCode 'DB2' -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false  
-Archive @( @{"Primary"="<Primary  
Vserver>:<PrimaryVolume>"; "Secondary"="<Secondary  
Vserver>:<SecondaryVolume>"})
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

자동 검색된 데이터베이스 백업을 복원하고 복구합니다.

SnapCenter 사용하면 하나 이상의 백업에서 데이터를 복원하고 복구할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 복원하려는 리소스 또는 리소스 그룹에 대해 현재 진행 중인 모든 백업 작업을 취소해야 합니다.
- 사전 복원, 사후 복원, 마운트 및 마운트 해제 명령의 경우, 다음 경로에서 플러그인 호스트에서 사용 가능한 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 호스트의 기본 위치: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- 자동 검색된 리소스의 경우 SFSR을 통해 복원이 지원됩니다.
- 자동 복구가 지원되지 않습니다.
- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 함께 표시됩니다.



백업은 리소스 그룹을 위한 것일 수 있지만 복원할 때는 복원할 개별 리소스를 선택해야 합니다.

리소스가 보호되지 않은 경우 전체 상태 옆에 "보호되지 않음"이 표시됩니다. 이는 리소스가 보호되지 않았거나 다른 사용자가 리소스를 백업했음을 의미할 수 있습니다.

3. 리소스를 선택하거나 리소스 그룹을 선택한 다음 해당 그룹에서 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.

5. 기본 백업 테이블에서 복원하려는 백업을 선택한 다음 *를 클릭합니다.  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scscr0191685001_01-05-2017-01:35:06.6463	1/5/2017 1:35:27 AM 

6. 복원 범위 페이지에서 *전체 리소스*를 선택하여 IBM Db2 데이터베이스의 구성된 데이터 볼륨을 복원합니다.

7. 사전 작업 페이지에서 복원 작업을 수행하기 전에 실행할 사전 복원 및 마운트 해제 명령을 입력합니다.

자동 검색된 리소스에는 마운트 해제 명령이 필요하지 않습니다.

8. Post ops 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.

자동 검색된 리소스에는 마운트 명령이 필요하지 않습니다.

9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > 전역 설정 페이지에서도 구성해야 합니다.

10. 요약을 검토한 후 *마침*을 클릭하세요.

11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

당신이 완료한 후

롤포워드 상태가 "DB 보류" 상태인 경우에만 복구가 가능합니다. 이 상태는 아카이브 로깅이 활성화된 Db2 데이터베이스에 적용됩니다.

IBM Db2 복원 작업 모니터링

작업 페이지를 사용하여 다양한 SnapCenter 복원 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

복원 후 상태는 복원 작업 후 리소스의 조건과 수행할 수 있는 추가 복원 작업을 설명합니다.

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복원 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복원*을 선택합니다.
 - d. 상태 드롭다운 목록에서 복원 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복원 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

IBM Db2 리소스 백업 복제

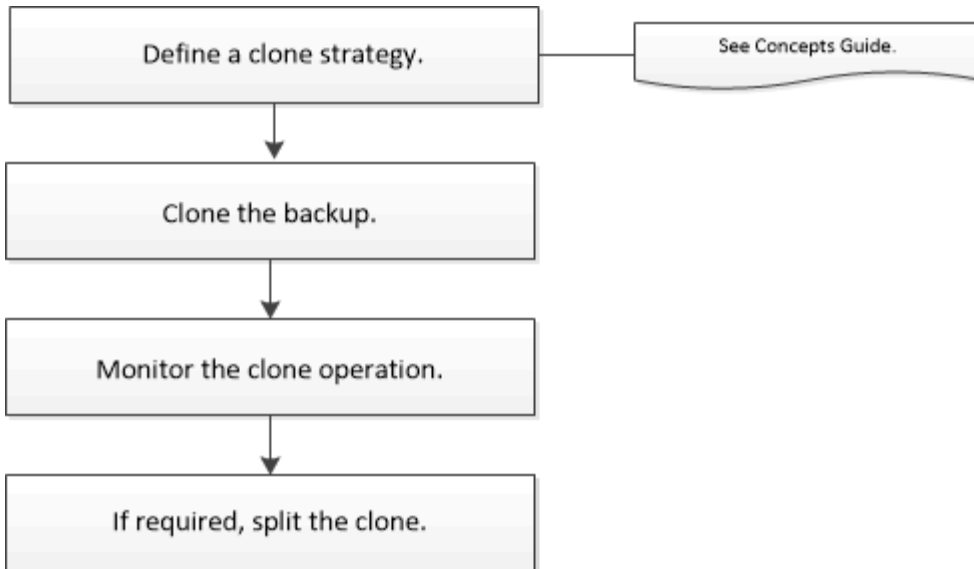
복제 워크플로

복제 워크플로에는 복제 작업을 수행하고 작업을 모니터링하는 작업이 포함됩니다.

이 작업에 관하여

- 소스 IBM Db2 서버에서 복제할 수 있습니다.
- 다음과 같은 이유로 리소스 백업을 복제할 수 있습니다.
 - 애플리케이션 개발 주기 동안 현재 리소스 구조 및 콘텐츠를 사용하여 구현해야 하는 기능을 테스트하려면
 - 데이터 웨어하우스를 채울 때 데이터 추출 및 조작 도구
 - 실수로 삭제되거나 변경된 데이터를 복구하려면

다음 워크플로는 복제 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

당신이 완료한 후

자동으로 검색된 Db2 리소스를 복제한 후 복제된 리소스는 수동 리소스로 표시됩니다. 복제된 Db2 리소스를 복구하려면 *리소스 새로 고침*을 클릭하세요. 복제본을 삭제하면 저장소와 호스트도 정리됩니다.

복제 작업 후 리소스를 새로 고치지 않고 복제본을 삭제하려고 하면 스토리지와 호스트가 정리되지 않습니다. fstab에서 항목을 수동으로 삭제해야 합니다.

IBM Db2 백업 복제

SnapCenter 사용하여 백업을 복제할 수 있습니다. 기본 또는 보조 백업에서 복제할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 볼륨을 호스팅하는 집계가 스토리지 가상 머신(SVM)의 할당된 집계 목록에 있는지 확인해야 합니다.
- 대체 호스트에서 Db2에 대한 복제본을 생성하는 동안 다른 호스트의 원래 마운트 경로와 동일한 복제본 마운트 경로에 대한 n-1 디렉토리 구조를 생성해야 합니다. 마운트 경로에는 755 실행 권한이 있어야 합니다.
- 복제 전 또는 복제 후 명령의 경우, 플러그인 호스트에서 다음 경로의 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: *C:\Program Files\NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Linux 호스트의 기본 위치: */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- FlexClone 볼륨 분할 작업에 대한 정보는 다음을 참조하세요. <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["FlexClone 볼륨을 부모 볼륨에서 분할합니다."].

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 같은 정보와 함께 표시됩니다.

3. 리소스 또는 리소스 그룹을 선택하세요.

리소스 그룹을 선택하는 경우 리소스를 선택해야 합니다.

리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 표에서 데이터 백업을 선택한 다음 클릭하세요.  .
6. 위치 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
복제 서버	복제본을 생성할 호스트를 선택하세요.
대상 복제 인스턴스	기존 백업에서 복제할 대상 Db2 복제 인스턴스 ID를 입력합니다. 이는 ANF 스토리지 유형 리소스에만 적용됩니다.
대상 클론 이름	복제본의 이름을 입력하세요. 이는 Db2 데이터베이스 리소스에만 적용됩니다.
NFS 내보내기 IP 주소	복제된 볼륨을 내보낼 IP 주소나 호스트 이름을 입력합니다. 이는 NFS 저장 유형 리소스에만 적용됩니다.
용량 풀 최대 처리량(MiB/s)	용량 풀의 최대 처리량을 입력하세요.

7. 스크립트 페이지에서 다음 단계를 수행합니다.



스크립트는 플러그인 호스트에서 실행됩니다.

- a. 복제 작업 전이나 후에 실행해야 하는 사전 복제 또는 사후 복제에 대한 명령을 각각 입력합니다.
 - 사전 복제 명령: 동일한 이름을 가진 기존 데이터베이스 삭제
 - 복제 후 명령: 데이터베이스를 확인하거나 데이터베이스를 시작합니다.

b. 호스트에 파일 시스템을 마운트하려면 mount 명령을 입력하세요.

Linux 머신에서 볼륨이나 qtree에 대한 마운트 명령:

NFS의 예: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

10. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

당신이 완료한 후

자동으로 검색된 Db2 리소스를 복제한 후 복제된 리소스는 수동 리소스로 표시됩니다. 복제된 Db2 리소스를 복구하려면 *리소스 새로 고침*을 클릭하세요. 복제본을 삭제하면 저장소와 호스트도 정리됩니다.

복제 작업 후 리소스를 새로 고치지 않고 복제본을 삭제하려고 하면 스토리지와 호스트가 정리되지 않습니다. fstab에서 항목을 수동으로 삭제해야 합니다.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Get-SmBackup 또는 Get-SmResourceGroup cmdlet을 사용하여 복제할 수 있는 백업을 나열합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

이 예제에서는 지정된 리소스 그룹, 해당 리소스 및 관련 정책에 대한 정보를 표시합니다.

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

Description :

CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMapping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :

```
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
```

3. New-SmClone cmdlet을 사용하여 기존 백업에서 복제 작업을 시작합니다.

이 예제에서는 모든 로그를 포함하는 지정된 백업에서 복제본을 만듭니다.

```
PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

이 예제에서는 지정된 Microsoft SQL Server 인스턴스에 대한 복제본을 만듭니다.

```
PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. Get-SmCloneReport cmdlet을 사용하여 복제 작업의 상태를 확인합니다.

이 예제에서는 지정된 작업 ID에 대한 복제 보고서를 표시합니다.

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

IBM Db2 복제 작업 모니터링

작업 페이지를 사용하여 SnapCenter 복제 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.

2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복제 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복제*를 선택합니다.
 - d. 상태 드롭다운 목록에서 복제 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복제 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

클론 분할

SnapCenter 사용하면 복제된 리소스를 부모 리소스에서 분할할 수 있습니다. 분할된 복제본은 부모 리소스로부터 독립됩니다.

이 작업에 관하여

- 중간 복제본에서는 복제 분할 작업을 수행할 수 없습니다.

예를 들어, 데이터베이스 백업에서 clone1을 만든 후 clone1의 백업을 만든 다음 이 백업(clone2)을 복제할 수 있습니다. clone2를 생성한 후 clone1은 중간 복제본이 되며 clone1에서 복제 분할 작업을 수행할 수 없습니다. 하지만 clone2에 대해 클론 분할 작업을 수행할 수 있습니다.

clone2를 분할한 후에는 clone1에 대해 clone 분할 작업을 수행할 수 있습니다. clone1은 더 이상 중간 클론이 아니기 때문입니다.

- 복제본을 분할하면 복제본의 백업 사본과 복제 작업이 삭제됩니다.
- FlexClone 볼륨 분할 작업에 대한 정보는 다음을 참조하세요. "[FlexClone 볼륨을 부모 볼륨에서 분할합니다.](#)".
- 스토리지 시스템의 볼륨이나 집계가 온라인인지 확인하세요.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 적절한 옵션을 선택하세요.

옵션	설명
데이터베이스 애플리케이션의 경우	보기 목록에서 *데이터베이스*를 선택합니다.
파일 시스템의 경우	보기 목록에서 *경로*를 선택합니다.

3. 목록에서 적절한 리소스를 선택하세요.

리소스 토폴로지 페이지가 표시됩니다.

4. 사본 관리 보기에서 복제된 리소스(예: 데이터베이스 또는 LUN)를 선택한 다음 *를 클릭합니다.  *.

5. 분할할 클론의 예상 크기와 집계에 필요한 사용 가능한 공간을 검토한 다음 *시작*을 클릭합니다.

6. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

SMCore 서비스를 다시 시작하면 복제 분할 작업이 더 이상 응답하지 않습니다. 복제 분할 작업을 중지하려면 Stop-SmJob cmdlet을 실행한 다음 복제 분할 작업을 다시 시도해야 합니다.

복제본이 분할되었는지 여부를 확인하기 위해 더 긴 폴링 시간이나 더 짧은 폴링 시간이 필요한 경우 *SMCoreServiceHost.exe.config* 파일에서 *CloneSplitStatusCheckPollTime* 매개변수 값을 변경하여 SMCore가 복제본 분할 작업의 상태를 폴링하는 시간 간격을 설정할 수 있습니다. 값은 밀리초이고 기본값은 5분입니다.

예를 들어:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

백업, 복원 또는 다른 클론 분할이 진행 중이면 클론 분할 시작 작업이 실패합니다. 실행 중인 작업이 완료된 후에만 복제 분할 작업을 다시 시작해야 합니다.

관련 정보

"SnapCenter 복제 또는 검증이 집계가 존재하지 않아 실패합니다."

SnapCenter 업그레이드 후 IBM Db2 데이터베이스 복제본 삭제 또는 분할

SnapCenter 4.3으로 업그레이드한 후에는 더 이상 복제본이 표시되지 않습니다. 복제본이 생성된 리소스의 토폴로지 페이지에서 복제본을 삭제하거나 분할할 수 있습니다.

이 작업에 관하여

숨겨진 복제본의 저장 공간을 찾으려면 다음 명령을 실행하세요. `Get-SmClone -ListStorageFootprint`

단계

1. remove-smbbackup cmdlet을 사용하여 복제된 리소스의 백업을 삭제합니다.
2. remove-smresourcegroup cmdlet을 사용하여 복제된 리소스의 리소스 그룹을 삭제합니다.
3. remove-smprotectresource cmdlet을 사용하여 복제된 리소스의 보호를 제거합니다.
4. 리소스 페이지에서 상위 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

5. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 복제본을 선택합니다.
6. 복제본을 선택한 다음 클릭하세요.  클론을 삭제하거나 클릭하세요.  클론을 분할합니다.
7. *확인*을 클릭합니다.

PostgreSQL 보호

PostgreSQL용 SnapCenter 플러그인

PostgreSQL용 SnapCenter 플러그인 개요

PostgreSQL 클러스터용 SnapCenter 플러그인은 PostgreSQL 클러스터의 애플리케이션 인식 데이터 보호 관리를 가능하게 하는 NetApp SnapCenter software 의 호스트 측 구성 요소입니다. PostgreSQL 클러스터용 플러그인은 SnapCenter 환경에서 PostgreSQL 클러스터의 백업, 복원 및 복제를 자동화합니다.

SnapCenter 단일 클러스터와 다중 클러스터 PostgreSQL 설정을 지원합니다. Linux와 Windows 환경 모두에서 PostgreSQL 클러스터용 플러그인을 사용할 수 있습니다. Windows 환경에서는 PostgreSQL이 수동 리소스로 지원됩니다.

PostgreSQL 클러스터용 플러그인이 설치되면 NetApp SnapMirror 기술과 함께 SnapCenter 사용하여 다른 볼륨에 백업 세트의 미러 복사본을 만들 수 있습니다. NetApp SnapVault 기술과 함께 플러그인을 사용하면 표준을 준수하기 위해 디스크 간 백업 복제를 수행할 수도 있습니다.

PostgreSQL용 SnapCenter 플러그인은 ONTAP 및 Azure NetApp 파일 스토리지 레이아웃에서 NFS와 SAN을 지원합니다.

VMDK, vVol 및 RDM 가상 스토리지 레이아웃이 지원됩니다.

PostgreSQL용 SnapCenter 플러그인을 사용하여 할 수 있는 일

사용자 환경에 PostgreSQL 클러스터용 플러그인을 설치하면 SnapCenter 사용하여 PostgreSQL 클러스터와 해당 리소스를 백업, 복원 및 복제할 수 있습니다. 해당 작업을 지원하는 작업도 수행할 수 있습니다.

- 클러스터를 추가합니다.
- 백업을 만듭니다.
- 백업에서 복원합니다.
- 백업을 복제합니다.
- 백업 작업을 예약합니다.
- 백업, 복원 및 복제 작업을 모니터링합니다.
- 백업, 복원 및 복제 작업에 대한 보고서를 확인합니다.

PostgreSQL용 SnapCenter 플러그인 기능

SnapCenter 플러그인 애플리케이션과 스토리지 시스템의 NetApp 기술과 통합됩니다. PostgreSQL 클러스터용 플러그인을 사용하려면 SnapCenter 그래픽 사용자 인터페이스를 사용합니다.

- 통합된 그래픽 사용자 인터페이스

SnapCenter 인터페이스는 플러그인과 환경 전반에 걸쳐 표준화와 일관성을 제공합니다. SnapCenter 인터페이스를 사용하면 플러그인 전반에 걸쳐 일관된 백업, 복원 및 복제 작업을 완료하고, 중앙 집중식 보고를 사용하고, 한눈에 볼 수 있는 대시보드 보기를 사용하고, 역할 기반 액세스 제어(RBAC)를 설정하고, 모든 플러그인에서 작업을 모니터링할 수 있습니다.

- 자동화된 중앙 관리

백업 작업을 예약하고, 정책 기반 백업 보존을 구성하고, 복원 작업을 수행할 수 있습니다. SnapCenter 구성하여 이메일 알림을 보내 환경을 사전에 모니터링할 수도 있습니다.

- 비중단 **NetApp** 스냅샷 복사 기술

SnapCenter PostgreSQL 클러스터용 플러그인과 함께 NetApp 스냅샷 기술을 사용하여 리소스를 백업합니다.

PostgreSQL 플러그인을 사용하면 다음과 같은 이점도 있습니다.

- 백업, 복원 및 복제 워크플로 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임

또한, 권한이 있는 SnapCenter 사용자에게 애플리케이션 수준 권한이 부여되도록 자격 증명을 설정할 수도 있습니다.

- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 리소스의 공간 효율적 및 특정 시점 복사본 생성

복제본을 생성하려는 스토리지 시스템에 FlexClone 라이선스가 필요합니다.

- 백업 생성의 일부로 ONTAP 의 일관성 그룹(CG) 스냅샷 기능에 대한 지원.
- 여러 리소스 호스트에서 동시에 여러 백업을 실행할 수 있는 기능

단일 작업에서 단일 호스트의 리소스가 동일한 볼륨을 공유하는 경우 스냅샷이 통합됩니다.

- 외부 명령을 사용하여 스냅샷을 생성하는 기능.
- XFS 파일 시스템에서 Linux LVM을 지원합니다.

PostgreSQL용 SnapCenter 플러그인이 지원하는 스토리지 유형

SnapCenter 물리적 머신과 가상 머신(VM) 모두에서 다양한 스토리지 유형을 지원합니다. PostgreSQL용 SnapCenter 플러그인을 설치하기 전에 스토리지 유형에 대한 지원을 확인해야 합니다.

기계	저장 유형
물리적 서버	• FC 연결 LUN • iSCSI로 연결된 LUN • NFS 연결 볼륨

기계	저장 유형
VMware ESXi	• FC 또는 iSCSI ESXi HBA로 연결된 RDM LUN 호스트 버스 어댑터(HBA) 스캐닝은 SnapCenter 호스트에 있는 모든 호스트 버스 어댑터를 스캔하기 때문에 완료하는 데 오랜 시간이 걸릴 수 있습니다. <code>_opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config_</code>에 있는 LinuxConfig.pm 파일을 편집하여 SCSI_HOSTS_OPTIMIZED_RESCAN 매개변수 값을 1로 설정하면 HBA_DRIVER_NAMES에 나열된 HBA만 다시 스캔합니다. • iSCSI 이니시에이터에 의해 게스트 시스템에 직접 연결된 iSCSI LUN • NFS 데이터 저장소의 VMDK • VMFS의 VMDK • 게스트 시스템에 직접 연결된 NFS 볼륨 • NFS와 SAN 모두에 있는 vVol 데이터 저장소 vVol 데이터스토어는 VMware vSphere용 ONTAP 도구를 사용해서만 프로비저닝할 수 있습니다.

PostgreSQL 플러그인에 필요한 최소 ONTAP 권한

데이터 보호를 위해 사용하는 SnapCenter 플러그인에 따라 필요한 최소 ONTAP 권한은 다릅니다.

- 모든 액세스 명령: ONTAP 9.12.1 이상에 필요한 최소 권한
 - 이벤트 생성-자동 지원-로그
 - 작업 이력 표시
 - 작업 중지
 - 룰
 - lun 생성
 - lun 생성
 - lun 생성
 - lun 삭제
 - lun igroup 추가
 - lun igroup 생성
 - lun igroup 삭제

- lun igroup 이름 바꾸기
- lun igroup 이름 바꾸기
- 룬 아이그룹 쇼
- lun 매핑 add-reporting-nodes
- lun 매핑 생성
- LUN 매핑 삭제
- LUN 매핑 제거-보고-노드
- lun 매핑 쇼
- lun 수정
- lun 이동량
- lun 오프라인
- lun 온라인
- lun 지속적 예약 지우기
- lun 크기 조정
- lun 시리얼
- 런 쇼
- 스냅미러 정책 추가 규칙
- 스냅미러 정책 수정 규칙
- 스냅미러 정책 제거 규칙
- 스냅미러 정책 보기
- 스냅미러 복원
- 스냅미러 쇼
- 스냅미러 쇼 히스토리
- 스냅미러 업데이트
- 스냅미러 업데이트-ls-세트
- 스냅미러 목록-대상
- 버전
- 볼륨 복제 생성
- 볼륨 클론 쇼
- 볼륨 복제 분할 시작
- 볼륨 클론 분할 정지
- 볼륨 생성
- 볼륨 파괴
- 볼륨 파일 복제 생성

- 볼륨 파일 show-disk-usage
- 볼륨 오프라인
- 온라인 볼륨
- 볼륨 수정
- 볼륨 qtree 생성
- 볼륨 qtree 삭제
- 볼륨 qtree 수정
- 볼륨 qtree 쇼
- 볼륨 제한
- 볼륨 쇼
- 볼륨 스냅샷 생성
- 볼륨 스냅샷 삭제
- 볼륨 스냅샷 수정
- 볼륨 스냅샷 수정-스냅락-만료-시간
- 볼륨 스냅샷 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- vservers cifs
- vservers cifs 공유 생성
- vservers cifs 공유 삭제
- vservers cifs 새도우 카피 쇼
- vservers cifs 공유 표시
- vservers cifs 쇼
- vservers 내보내기 정책
- vservers 내보내기 정책 생성
- vservers 내보내기 정책 삭제
- vservers 내보내기 정책 규칙 생성
- vservers 내보내기 정책 규칙 표시
- vservers 내보내기 정책 표시
- v서버 iSCSI
- vservers iscsi 연결 표시
- vservers 쇼

- 읽기 전용 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
 - 네트워크 인터페이스
 - 네트워크 인터페이스 표시
 - v서버

PostgreSQL을 위한 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비

ONTAP SnapMirror 기술과 함께 SnapCenter 플러그인을 사용하면 다른 볼륨에 백업 세트의 미러 사본을 생성할 수 있으며, ONTAP SnapVault 기술과 함께 사용하면 표준 준수 및 기타 거버넌스 관련 목적으로 디스크 간 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 구성하고 해당 관계를 초기화해야 합니다.

SnapCenter 스냅샷 작업을 완료한 후 SnapMirror와 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행되므로 별도의 ONTAP 일정을 만들지 마세요.



NetApp SnapManager 제품을 통해 SnapCenter에 접속했고 구성된 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 기본 저장소(소스 볼륨)의 데이터를 보조 저장소(대상 볼륨)로 복제합니다. 관계를 초기화하면 ONTAP 소스 볼륨에서 참조되는 데이터 블록을 대상 볼륨으로 전송합니다.



SnapCenter SnapMirror와 SnapVault 볼륨 간의 계단식 관계(**Primary > Mirror > Vault**)를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter 버전에 따라 유연한 SnapMirror 관계 관리를 지원합니다. 버전에 따라 유연한 SnapMirror 관계와 이를 설정하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["ONTAP 문서"](#).

PostgreSQL 백업 전략

PostgreSQL에 대한 백업 전략 정의

백업 작업을 생성하기 전에 백업 전략을 정의하면 리소스를 성공적으로 복원하거나 복제하는 데 필요한 백업을 확보하는 데 도움이 됩니다. 백업 전략은 주로 서비스 수준 계약(SLA), 복구 시간 목표(RTO), 복구 지점 목표(RPO)에 따라 결정됩니다.

이 작업에 관하여

SLA는 기대되는 서비스 수준을 정의하고 서비스의 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RTO는 서비스가 중단된 후 비즈니스 프로세스를 복구해야 하는 시간입니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 기간에 대한 전략을 정의합니다. SLA, RTO, RPO는 데이터 보호 전략에 기여합니다.

단계

1. 리소스를 백업해야 하는 시기를 결정하세요.
2. 필요한 백업 작업의 수를 결정합니다.
3. 백업의 이름을 어떻게 지을지 결정하세요.

4. 클러스터의 애플리케이션 일관성 스냅샷을 백업하기 위해 스냅샷 복사 기반 정책을 생성할지 여부를 결정합니다.
5. 복제를 위해 NetApp SnapMirror 기술을 사용할지, 장기 보존을 위해 NetApp SnapVault 기술을 사용할지 결정하세요.
6. 소스 스토리지 시스템과 SnapMirror 대상의 스냅샷 보존 기간을 결정합니다.
7. 백업 작업 전이나 후에 명령을 실행할지 여부를 결정하고 사전 스크립트나 사후 스크립트를 제공합니다.

Linux 호스트에서 리소스 자동 검색

리소스는 SnapCenter 에서 관리하는 Linux 호스트의 PostgreSQL 클러스터와 인스턴스입니다. PostgreSQL용 SnapCenter 플러그인을 설치하면 해당 Linux 호스트의 모든 인스턴스에 있는 PostgreSQL 클러스터가 자동으로 검색되어 리소스 페이지에 표시됩니다.

지원되는 백업 유형

백업 유형은 생성하려는 백업 유형을 지정합니다. SnapCenter PostgreSQL 클러스터에 대한 스냅샷 복사 기반 백업 유형을 지원합니다.

스냅샷 복사 기반 백업

스냅샷 복사 기반 백업은 NetApp 스냅샷 기술을 활용하여 PostgreSQL 클러스터가 있는 볼륨의 온라인, 읽기 전용 복사본을 만듭니다.

PostgreSQL용 SnapCenter 플러그인이 일관성 그룹 스냅샷을 사용하는 방법

플러그인을 사용하면 리소스 그룹에 대한 일관성 그룹 스냅샷을 만들 수 있습니다. 일관성 그룹은 여러 볼륨을 수용하여 하나의 엔티티로 관리할 수 있는 컨테이너입니다. 일관성 그룹은 여러 볼륨의 동시 스냅샷으로, 볼륨 그룹의 일관된 복사본을 제공합니다.

또한 스토리지 컨트롤러가 스냅샷을 일관되게 그룹화하는 데 걸리는 대기 시간을 지정할 수도 있습니다. 이용 가능한 대기 시간 옵션은 긴급, 보통, *느긋함*입니다. 일관된 그룹 스냅샷 작업 중에 WAFL(Write Anywhere File Layout) 동기화를 활성화하거나 비활성화할 수도 있습니다. WAFL 동기화는 일관성 그룹 스냅샷의 성능을 향상시킵니다.

SnapCenter 데이터 백업의 정리 작업을 관리하는 방법

SnapCenter 스토리지 시스템 및 파일 시스템 수준에서 데이터 백업의 정리 작업을 관리합니다.

기본 또는 보조 저장소의 스냅샷과 PostgreSQL 카탈로그의 해당 항목은 보존 설정에 따라 삭제됩니다.

PostgreSQL 백업 일정을 결정하기 위한 고려 사항

백업 일정을 결정하는 가장 중요한 요소는 리소스의 변화율입니다. 자주 사용되는 리소스는 매시간 백업하고, 거의 사용되지 않는 리소스는 하루에 한 번 백업할 수도 있습니다. 기타 요소로는 조직에 대한 리소스의 중요성, 서비스 수준 계약(SLA), 복구 지점 목표(RPO) 등이 있습니다.

백업 일정은 다음과 같이 두 부분으로 구성됩니다.

- 백업 빈도(백업을 수행할 빈도)

일부 플러그인의 경우 일정 유형이라고도 하는 백업 빈도는 정책 구성의 일부입니다. 예를 들어, 백업 빈도를 매시간, 매일, 매주 또는 매월로 구성할 수 있습니다.

- 백업 일정(백업을 수행할 정확한 시기)

백업 일정은 리소스 또는 리소스 그룹 구성의 일부입니다. 예를 들어, 주간 백업을 위해 구성된 정책이 있는 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 일정을 구성할 수 있습니다.

PostgreSQL에 필요한 백업 작업 수

필요한 백업 작업 수를 결정하는 요소에는 리소스 크기, 사용된 볼륨 수, 리소스 변경률, 서비스 수준 계약(SLA) 등이 있습니다.

PostgreSQL 클러스터용 플러그인에 대한 백업 명명 규칙

기본 스냅샷 명명 규칙을 사용하거나 사용자 지정 명명 규칙을 사용할 수 있습니다. 기본 백업 명명 규칙은 스냅샷 이름에 타임스탬프를 추가하여 복사본이 생성된 시기를 식별하는 데 도움이 됩니다.

스냅샷은 다음과 같은 기본 명명 규칙을 사용합니다.

`resourcegroupname_hostname_timestamp`

다음 예와 같이 논리적으로 백업 리소스 그룹의 이름을 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예에서 구문 요소는 다음과 같은 의미를 갖습니다.

- `_dts1_`은 리소스 그룹 이름입니다.
- `_mach1x88_`은 호스트 이름입니다.
- `_03-12-2015_23.17.26_`은 날짜와 타임스탬프입니다.

또는, *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택하여 리소스나 리소스 그룹을 보호하는 동안 스냅샷 이름 형식을 지정할 수 있습니다. 예를 들어, `customtext_resourcegroup_policy_hostname` 또는 `resourcegroup_hostname`입니다. 기본적으로 타임스탬프 접미사는 스냅샷 이름에 추가됩니다.

PostgreSQL에 대한 복원 및 복구 전략

PostgreSQL 리소스에 대한 복원 및 복구 전략 정의

클러스터를 복원하고 복구하기 전에 전략을 정의해야 복원 및 복구 작업을 성공적으로 수행할 수 있습니다.



클러스터의 수동 복구만 지원됩니다.

단계

1. 수동으로 추가된 PostgreSQL 리소스에 대해 지원되는 복원 전략을 확인합니다.
2. 자동 검색된 PostgreSQL 클러스터에 지원되는 복원 전략을 확인합니다.
3. 수행할 복구 작업 유형을 결정합니다.

수동으로 추가된 **PostgreSQL** 리소스에 대해 지원되는 복원 전략 유형

SnapCenter 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다.



수동으로 추가한 PostgreSQL 리소스는 복구할 수 없습니다.

리소스 복구 완료

- 리소스의 모든 볼륨, Qtree 및 LUN을 복원합니다.



리소스에 볼륨이나 Q트리가 포함되어 있는 경우 해당 볼륨이나 Q트리에서 복원을 위해 선택한 스냅샷 이후에 촬영된 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 동일한 볼륨이나 Q트리에 다른 리소스가 호스팅되는 경우 해당 리소스도 삭제됩니다.

참고: PostgreSQL 플러그인은 수동으로 복구하는 데 도움이 되도록

`/<OS_temp_folder>/postgresql_sc_recovery<Restore_JobId>/_` 폴더에 backup_label과 tablespace_map을 생성합니다.

자동으로 검색된 **PostgreSQL**에 지원되는 복원 전략 유형

SnapCenter 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다.

전체 리소스 복원은 자동으로 검색된 PostgreSQL 클러스터에 지원되는 복원 전략입니다. 이렇게 하면 리소스의 모든 볼륨, Q트리, LUN이 복원됩니다.

자동 검색된 **PostgreSQL**에 대한 복원 작업 유형

PostgreSQL용 SnapCenter 플러그인은 단일 파일 SnapRestore 지원하고, 자동으로 검색된 PostgreSQL 클러스터에 대한 연결 및 복사 복원 유형을 지원합니다.

단일 파일 **SnapRestore** 다음 시나리오에 대해 **NFS** 환경에서 수행됩니다.

- 전체 리소스 옵션만 선택된 경우
- 선택한 백업이 SnapMirror 또는 SnapVault 보조 위치에서 시작되고 전체 리소스 옵션이 선택된 경우

단일 파일 **SnapRestore** 다음 시나리오에 대해 **SAN** 환경에서 수행됩니다.

- 전체 리소스 옵션만 선택된 경우
- SnapMirror 또는 SnapVault 보조 위치에서 백업을 선택하고 전체 리소스 옵션을 선택한 경우

PostgreSQL 클러스터에 지원되는 복구 작업 유형

SnapCenter 사용하면 PostgreSQL 클러스터에 대해 다양한 유형의 복구 작업을 수행할 수 있습니다.

- 클러스터를 최신 상태로 복구합니다.
- 특정 시점까지 클러스터를 복구합니다.

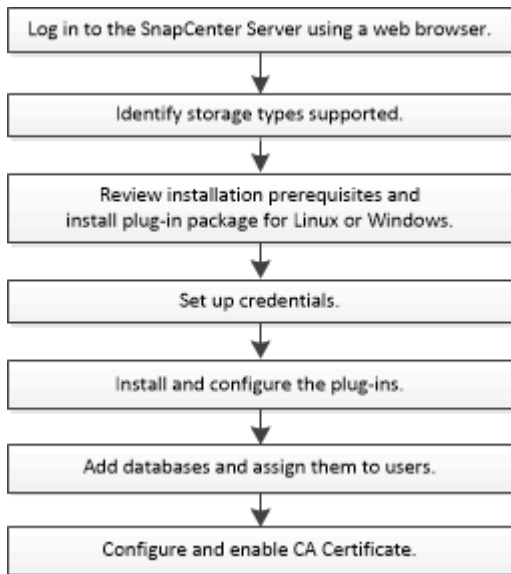
복구 날짜와 시간을 지정해야 합니다.

SnapCenter PostgreSQL 클러스터에 대해 복구 불가 옵션도 제공합니다.

PostgreSQL용 SnapCenter 플러그인 설치를 준비하세요

PostgreSQL용 SnapCenter 플러그인 설치 워크플로

PostgreSQL 클러스터를 보호하려면 PostgreSQL용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



PostgreSQL용 SnapCenter 플러그인을 호스트 추가하고 설치하기 위한 전제 조건

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 충족해야 합니다.

PostgreSQL용 SnapCenter 플러그인은 Windows와 Linux 환경 모두에서 사용할 수 있습니다.

- 호스트에 Java 11을 설치했어야 합니다.



IBM Java는 Windows 및 Linux 호스트에서 지원되지 않습니다.

- Windows의 경우 플러그인 생성 서비스는 “LocalSystem” Windows 사용자를 사용하여 실행해야 합니다. 이는 플러그인 for PostgreSQL을 도메인 관리자로 설치한 경우의 기본 동작입니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹

사용자에 속하는 경우 호스트에서 UAC를 비활성화해야 합니다. Microsoft Windows용 SnapCenter 플러그인은 기본적으로 Windows 호스트의 PostgreSQL 플러그인과 함께 배포됩니다.

- SnapCenter 서버는 PostgreSQL 호스트용 플러그인의 8145 또는 사용자 정의 포트에 액세스할 수 있어야 합니다.

Windows 호스트

- 원격 호스트에 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 도메인 사용자가 있어야 합니다.
- Windows 호스트에 PostgreSQL 플러그인을 설치하는 동안 Microsoft Windows용 SnapCenter 플러그인이 자동으로 설치됩니다.
- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.
- Windows 호스트에 Java 11을 설치했어야 합니다.

"모든 운영 체제용 JAVA 다운로드"

"NetApp 상호 운용성 매트릭스 도구"

리눅스 호스트

- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.
- Linux 호스트에 Java 11을 설치했어야 합니다.

"모든 운영 체제용 JAVA 다운로드"

"NetApp 상호 운용성 매트릭스 도구"

- Linux 호스트에서 실행되는 PostgreSQL 클러스터의 경우 PostgreSQL용 플러그인을 설치하는 동안 UNIX용 SnapCenter 플러그인이 자동으로 설치됩니다.
- 플러그인 설치를 위해 기본 셸로 *bash*를 사용해야 합니다.

보충 명령

PostgreSQL용 SnapCenter 플러그인에서 보충 명령을 실행하려면 *allowed_commands.config* 파일에 해당 명령을 포함해야 합니다.

- Windows 호스트의 기본 위치: *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Linux 호스트의 기본 위치: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

플러그인 호스트에서 추가 명령을 허용하려면 편집기에서 *allowed_commands.config* 파일을 엽니다. 각 명령을 별도의 줄에 입력하세요. 명령은 대소문자를 구분하지 않습니다. 완전히 정규화된 경로 이름을 지정하고, 경로 이름에 공백이 포함된 경우 따옴표(")로 묶으세요.

예를 들어:

명령: mount 명령: umount 명령: "C:\Program Files\ NetApp\SnapCreator commands\sdcli.exe" 명령: myscript.bat

allowed_commands.config 파일이 없으면 명령이나 스크립트 실행이 차단되고 다음 오류와 함께 워크플로가 실패합니다.

"[/mnt/mount -a] 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여합니다."

_allowed_commands.config_에 명령이나 스크립트가 없으면 명령이나 스크립트 실행이 차단되고 다음 오류와 함께 워크플로가 실패합니다.

"[/mnt/mount -a] 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여합니다."



모든 명령을 허용하려면 와일드카드 항목(*)을 사용해서는 안 됩니다.

Linux 호스트에 대한 루트가 아닌 사용자에게 대한 **sudo** 권한 구성

SnapCenter 사용하면 루트가 아닌 사용자도 Linux용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 루트가 아닌 사용자로 실행됩니다. 루트가 아닌 사용자에게 여러 경로에 대한 액세스 권한을 제공하려면 sudo 권한을 구성해야 합니다.

필요한 것

- Sudo 버전 1.8.7 이상.
- umask가 0027인 경우, java 폴더와 그 안에 있는 모든 파일에 555 권한이 있어야 합니다. 그렇지 않으면 플러그인 설치가 실패할 수 있습니다.
- 루트가 아닌 사용자의 경우 루트가 아닌 사용자의 이름과 사용자 그룹이 동일해야 합니다.
- /etc/ssh/sshd_config 파일을 편집하여 메시지 인증 코드 알고리즘(MAC hmac-sha2-256 및 MAC hmac-sha2-512)을 구성합니다.

구성 파일을 업데이트한 후 sshd 서비스를 다시 시작합니다.

예:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

이 작업에 관하여

루트가 아닌 사용자에게 다음 경로에 대한 액세스를 제공하려면 sudo 권한을 구성해야 합니다.

- /home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/ NetApp/snapcenter/spl/설치/플러그인/제거

- /custom_location/ NetApp/snapcenter/spl/bin/spl

단계

1. Linux용 SnapCenter 플러그인 패키지를 설치하려는 Linux 호스트에 로그인합니다.
2. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 줄을 추가합니다.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

_LINUX_USER_는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

_checksum_value_는 **sc_unix_plugins_checksum.txt** 파일에서 얻을 수 있습니다. 이 파일의 위치는 다음과 같습니다.

- SnapCenter 서버가 Windows 호스트에 설치된 경우 _C:\ProgramData\ NetApp\ SnapCenter \Package Repository\sc_unix_plugins_checksum.txt _
- _/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ SnapCenter 서버가 Linux 호스트에 설치된 경우.



이 예제는 귀하만의 데이터를 생성하기 위한 참고자료로만 사용해야 합니다.

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항과 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	마이크로소프트 윈도우 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구".
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	• ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 • 파워셀 코어 7.4.2 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구".

Linux용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 및 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	• 레드햇 엔터프라이즈 리눅스 • SUSE Linux Enterprise Server(SLES) 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구".
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB

목	요구 사항
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	Java 11 Oracle Java 및 OpenJDK JAVA를 최신 버전으로 업그레이드한 경우 <code>/var/opt/snapcenter/spl/etc/spl.properties</code>에 있는 <code>JAVA_HOME</code> 옵션이 올바른 JAVA 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다. 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구".

PostgreSQL용 SnapCenter 플러그인에 대한 자격 증명 설정

SnapCenter 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다. SnapCenter 플러그인을 설치하기 위한 자격 증명과 클러스터 또는 Windows 파일 시스템에서 데이터 보호 작업을 수행하기 위한 추가 자격 증명을 만들어야 합니다.

이 작업에 관하여

- 리눅스 호스트

Linux 호스트에 플러그인을 설치하려면 자격 증명을 설정해야 합니다.

플러그인 프로세스를 설치하고 시작하려면 루트 사용자 또는 sudo 권한이 있는 루트가 아닌 사용자의 자격 증명을 설정해야 합니다.

모범 사례: 호스트를 배포하고 플러그인을 설치한 후에도 Linux에 대한 자격 증명을 생성할 수 있지만, 가장 좋은 방법은 호스트를 배포하고 플러그인을 설치하기 전에 SVM을 추가한 후에 자격 증명을 생성하는 것입니다.

- Windows 호스트

플러그인을 설치하기 전에 Windows 자격 증명을 설정해야 합니다.

원격 호스트의 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정해야 합니다.

개별 리소스 그룹에 대한 자격 증명을 설정하고 사용자 이름에 전체 관리자 권한이 없는 경우 최소한 리소스 그룹 및 백업 권한을 사용자 이름에 할당해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *자격 증명*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 자격 증명 페이지에서 자격 증명을 구성하는 데 필요한 정보를 지정합니다.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.
사용자 이름	인증에 사용할 사용자 이름과 비밀번호를 입력하세요. • 도메인 관리자 또는 관리자 그룹의 모든 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹 구성원을 지정하세요. 사용자 이름 필드에 사용할 수 있는 형식은 다음과 같습니다. ◦ <i>NetBIOS</i> 사용자 이름 ◦ 도메인 <i>FQDN</i> 사용자 이름 • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우, SnapCenter 플러그인을 설치할 시스템에 기본 제공되는 로컬 관리자를 지정하십시오. 사용자 계정에 승격된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우, 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다. <i>UserName</i> 비밀번호에 큰따옴표(")나 백틱(`)을 사용하지 마세요. 비밀번호에 '<' 기호와 '!' 기호를 함께 사용하면 안 됩니다. 예를 들어, lessthan<!10, lessthan10<!, backtick`12.
비밀번호	인증에 사용되는 비밀번호를 입력하세요.
인증 모드	사용할 인증 모드를 선택하세요.
sudo 권한을 사용하세요	루트가 아닌 사용자에게 자격 증명을 생성하는 경우 sudo 권한 사용 확인란을 선택합니다.  Linux 사용자에게만 적용됩니다.

5. *확인*을 클릭합니다.

자격 증명 설정을 마친 후 사용자 및 액세스 페이지에서 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

Windows Server 2016 이상에서 gMSA 구성

Windows Server 2016 이상에서는 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 관리 서비스 계정(gMSA)을 만들 수 있습니다.

시작하기 전에

- Windows Server 2016 이상 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2016 이상 호스트가 있어야 합니다.

단계

1. gMSA의 각 개체에 대해 고유한 비밀번호를 생성하려면 KDS 루트 키를 만듭니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 다음 명령을 실행합니다. Add-KDSRootKey -EffectiveImmediately
3. gMSA를 만들고 구성하세요.
 - a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
domainName\accountName$  
.. 그룹에 컴퓨터 객체를 추가합니다.  
.. 방금 만든 사용자 그룹을 사용하여 gMSA를 만듭니다.
```

예를 들어,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 달리다 `Get-ADServiceAccount` 서비스 계정을 확인하는 명령입니다.
```

4. 호스트에서 gMSA를 구성하세요.
 - a. gMSA 계정을 사용하려는 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.
이렇게 하려면 PowerShell에서 다음 명령을 실행하세요.

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

a. 호스트를 다시 시작합니다.

b. PowerShell 명령 프롬프트에서 다음 명령을 실행하여 호스트에 gMSA를 설치합니다. `Install-AdServiceAccount <gMSA>`

c. 다음 명령을 실행하여 gMSA 계정을 확인하세요. `Test-AdServiceAccount <gMSA>`

5. 호스트에서 구성된 gMSA에 관리 권한을 할당합니다.

6. SnapCenter 서버에서 구성된 gMSA 계정을 지정하여 Windows 호스트를 추가합니다.

SnapCenter Server는 호스트에 선택된 플러그인을 설치하고, 플러그인 설치 중에 지정된 gMSA가 서비스 로그인 계정으로 사용됩니다.

PostgreSQL용 SnapCenter 플러그인 설치

원격 호스트에 호스트를 추가하고 플러그인 패키지를 설치합니다.

SnapCenter 호스트 추가 페이지를 사용하여 호스트를 추가한 다음 플러그인 패키지를 설치해야 합니다. 플러그인은 원격 호스트에 자동으로 설치됩니다. 개별 호스트에 대한 호스트를 추가하고 플러그인 패키지를 설치할 수 있습니다.

시작하기 전에

- SnapCenter 서버 호스트의 운영 체제가 Windows 2019이고 플러그인 호스트의 운영 체제가 Windows 2022인 경우 다음을 수행해야 합니다.
 - Windows Server 2019(OS 빌드 17763.5936) 이상으로 업그레이드하세요.
 - Windows Server 2022(OS 빌드 20348.2402) 이상으로 업그레이드하세요.
- SnapCenter 관리자 역할과 같이 플러그인 설치 및 제거 권한이 있는 역할에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.

- 메시지 대기열 서비스가 실행 중인지 확인해야 합니다.
- 관리 문서에는 호스트 관리에 대한 정보가 포함되어 있습니다.
- 그룹 관리 서비스 계정(gMSA)을 사용하는 경우 관리자 권한으로 gMSA를 구성해야 합니다.

"PostgreSQL을 위해 Windows Server 2016 이상에서 그룹 관리 서비스 계정 구성"

이 작업에 관하여

- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 상단에 관리되는 호스트 탭이 선택되어 있는지 확인하세요.
3. *추가*를 클릭하세요.
4. 호스트 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
호스트 유형	호스트 유형을 선택하세요: • Windows • 리눅스  PostgreSQL 플러그인은 PostgreSQL 클라이언트 호스트에 설치되며, 이 호스트는 Windows 시스템이나 Linux 시스템에 있을 수 있습니다.
호스트 이름	통신 호스트 이름을 입력하세요. 호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하세요. SnapCenter DNS의 적절한 구성에 달려 있습니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다.
신임장	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성하세요. 자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하세요. 제공한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다.  자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

REST API를 사용하여 PostgreSQL 플러그인을 설치하는 경우 버전을 3.0으로 전달해야 합니다. 예를 들어, PostgreSQL:3.0

6. (선택 사항) *추가 옵션*을 클릭합니다.

이 분야에서는...	이렇게 하세요...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정하세요. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트로 표시됩니다.  플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.
설치 경로	PostgreSQL 플러그인은 PostgreSQL 클라이언트 호스트에 설치되며, 이 호스트는 Windows 시스템이나 Linux 시스템에 있을 수 있습니다. • Windows용 SnapCenter 플러그인 패키지의 경우 기본 경로는 C:\Program Files\ NetApp\ SnapCenter 입니다. 선택적으로 경로를 사용자 정의할 수 있습니다. • Linux용 SnapCenter 플러그인 패키지의 경우 기본 경로는 /opt/ NetApp/snapcenter입니다. 선택적으로 경로를 사용자 정의할 수 있습니다.
사전 설치 확인 건너뛰기	플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택하세요.
클러스터의 모든 호스트를 추가합니다.	모든 클러스터 노드를 추가하려면 이 확인란을 선택하세요.

이 분야에서는...	이렇게 하세요...
플러그인 서비스를 실행하려면 그룹 관리 서비스 계정(gMSA)을 사용하세요.	Windows 호스트의 경우 플러그인 서비스를 실행하기 위해 그룹 관리 서비스 계정(gMSA)을 사용하려면 이 확인란을 선택합니다.  다음 형식으로 gMSA 이름을 제공하세요: domainName\accountName\$.  gMSA는 Windows용 SnapCenter 플러그인 서비스에 대한 로그인 서비스 계정으로만 사용됩니다.

7. *제출*을 클릭하세요.

"사전 검사 건너뛰기" 확인란을 선택하지 않은 경우, 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 호스트의 유효성 검사가 수행됩니다. 디스크 공간, RAM, PowerShell 버전, .NET 버전, 위치(Windows 플러그인의 경우), Java 버전(Linux 플러그인의 경우)이 최소 요구 사항을 충족하는지 검증됩니다. 최소 요구 사항을 충족하지 못하면 해당 오류 또는 경고 메시지가 표시됩니다.

오류가 디스크 공간이나 RAM과 관련된 경우 C:\Program Files\NetApp\ SnapCenter WebApp에 있는 web.config 파일을 업데이트하여 기본값을 수정할 수 있습니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.



HA 설정에서 web.config 파일을 업데이트하는 경우 두 노드에서 모두 파일을 업데이트해야 합니다.

8. 호스트 유형이 Linux인 경우 지문을 확인한 다음 *확인 및 제출*을 클릭합니다.

클러스터 설정에서는 클러스터의 각 노드의 지문을 확인해야 합니다.



동일한 호스트가 이전에 SnapCenter 에 추가되었고 지문이 확인된 경우에도 지문 확인은 필수입니다.

9. 설치 진행 상황을 모니터링합니다.

- Windows 플러그인의 경우 설치 및 업그레이드 로그는 다음 위치에 있습니다. C:\Windows\ SnapCenter plugin\Install<JOBID>_
- Linux 플러그인의 경우 설치 로그는 /var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log_에 있고 업그레이드 로그는 /var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade<JOBID>.log_에 있습니다.

cmdlet을 사용하여 여러 원격 호스트에 **Linux** 또는 **Windows용 SnapCenter** 플러그인 패키지 설치

Install-SmHostPackage PowerShell cmdlet을 사용하여 Linux 또는 Windows용 SnapCenter 플러그인 패키지를 여러 호스트에 동시에 설치할 수 있습니다.

시작하기 전에

플러그인 패키지를 설치하려는 각 호스트에서 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter 에 로그인해야

합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 Open-SmConnection cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
3. Install-SmHostPackage cmdlet과 필요한 매개변수를 사용하여 여러 호스트에 플러그인을 설치합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려는 경우 `-skipprecheck` 옵션을 사용할 수 있습니다.

4. 원격 설치를 위한 자격 증명을 입력하세요.

명령줄 인터페이스를 사용하여 **Linux** 호스트에 **PostgreSQL**용 **SnapCenter** 플러그인을 설치합니다.

SnapCenter 사용자 인터페이스(UI)를 사용하여 PostgreSQL 클러스터용 SnapCenter 플러그인을 설치해야 합니다. 사용자 환경에서 SnapCenter UI에서 플러그인을 원격으로 설치할 수 없는 경우 명령줄 인터페이스(CLI)를 사용하여 콘솔 모드나 자동 모드로 PostgreSQL 클러스터용 플러그인을 설치할 수 있습니다.

시작하기 전에

- PostgreSQL 클라이언트가 있는 각 Linux 호스트에 PostgreSQL 클러스터용 플러그인을 설치해야 합니다.
- PostgreSQL 클러스터용 SnapCenter 플러그인을 설치하는 Linux 호스트는 종속 소프트웨어, 클러스터 및 운영 체제 요구 사항을 충족해야 합니다.

상호 운용성 매트릭스 도구(IMT)에는 지원되는 구성에 대한 최신 정보가 포함되어 있습니다.

"NetApp 상호 운용성 매트릭스 도구"

- PostgreSQL 클러스터용 SnapCenter 플러그인은 Linux용 SnapCenter 플러그인 패키지의 일부입니다. Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 Windows 호스트에 SnapCenter 이미 설치되어 있어야 합니다.

단계

1. Linux용 SnapCenter 플러그인 패키지 설치 파일(snapcenter_linux_host_plugin.bin)을 C:\ProgramData\NetApp\SnapCenter\Package Repository에서 PostgreSQL용 플러그인을 설치하려는 호스트로 복사합니다.

SnapCenter 서버가 설치된 호스트에서 이 경로에 액세스할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 복사한 디렉토리로 이동합니다.
3. 플러그인을 설치하세요: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`
 - `-DPORT`는 SMCore HTTPS 통신 포트를 지정합니다.
 - `-DSERVER_IP`는 SnapCenter 서버 IP 주소를 지정합니다.

- -DSERVER_HTTPS_PORT는 SnapCenter 서버 HTTPS 포트를 지정합니다.
- -DUSER_INSTALL_DIR은 Linux용 SnapCenter 플러그인 패키지를 설치할 디렉토리를 지정합니다.
- DINSTALL_LOG_NAME은 로그 파일의 이름을 지정합니다.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. /<설치 디렉토리>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties 파일을 편집한 다음 PLUGINS_ENABLED = PostgreSQL:3.0 매개변수를 추가합니다.
5. Add-Smhost cmdlet과 필요한 매개변수를 사용하여 SnapCenter 서버에 호스트를 추가합니다.

명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

PostgreSQL 플러그인 설치 상태 모니터링

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행 상황을 모니터링할 수 있습니다. 설치가 완료되었는지 또는 문제가 있는지 확인하기 위해 설치 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 플러그인 설치 작업만 나열되도록 목록을 필터링하려면 다음을 수행합니다.
 - a. *필터*를 클릭하세요.
 - b. 선택 사항: 시작 날짜와 종료 날짜를 지정합니다.
 - c. 유형 드롭다운 메뉴에서 *플러그인 설치*를 선택합니다.
 - d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.

e. *적용*을 클릭하세요.

4. 설치 작업을 선택하고 *세부정보*를 클릭하면 작업 세부정보를 볼 수 있습니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

CA 인증서 구성

CA 인증서 CSR 파일 생성

인증서 서명 요청(CSR)을 생성하고, 생성된 CSR을 사용하여 인증 기관(CA)에서 얻을 수 있는 인증서를 가져올 수 있습니다. 인증서에는 개인 키가 연결됩니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.



CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 정보는 다음을 참조하세요. ["CA 인증서 CSR 파일을 생성하는 방법"](#).



도메인(*.domain.company.com)이나 시스템(machine1.domain.company.com)에 대한 CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN)과 해당 호스트 이름을 CA 인증서에 명시해야 합니다. 인증서를 구매하기 전에 주체 대체 이름(SAN) 필드를 입력하여 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(*.domain.company.com)의 경우 인증서에는 해당 도메인의 모든 호스트 이름이 암묵적으로 포함됩니다.

CA 인증서 가져오기

Microsoft 관리 콘솔(MMC)을 사용하여 CA 인증서를 SnapCenter 서버와 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.
2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
3. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > *인증서*를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 버튼으로 클릭한 다음, 모든 작업 > *가져오기*를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
개인 키 가져오기	예 옵션을 선택하고 개인 키를 가져온 후 *다음*을 클릭합니다.
가져오기 파일 형식	변경하지 마세요. *다음*을 클릭하세요.

이 마법사 창에서...	다음을 수행하세요...
보안	내보낸 인증서에 사용할 새 비밀번호를 지정한 후 *다음*을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.



인증서 가져오기는 개인 키와 함께 제공되어야 합니다(지원되는 형식: *.pfx, *.p12, *.p7b).

7. "개인" 폴더에 대해서도 5단계를 반복합니다.

CA 인증서 지문을 받으세요

인증서 지문은 인증서를 식별하는 16진수 문자열입니다. 지문은 지문 알고리즘을 사용하여 인증서 내용으로부터 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.
 - a. 인증서를 두 번 클릭합니다.
 - b. 인증서 대화 상자에서 세부정보 탭을 클릭합니다.
 - c. 필드 목록을 스크롤하여 *지문*을 클릭하세요.
 - d. 상자에서 16진수 문자를 복사하세요.
 - e. 16진수 사이의 공백을 제거하세요.

예를 들어, 지문이 "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b"인 경우 공백을 제거하면 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.
 - a. 다음 명령을 실행하여 설치된 인증서의 지문을 나열하고 주체 이름으로 최근에 설치된 인증서를 식별합니다.

Get-ChildItem -경로 인증서:\LocalMachine\My

- b. 지문을 복사하세요.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스로 CA 인증서를 구성해야 합니다.

SnapCenter 서버와 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하는 기존 인증서 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

예를 들어:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스에
바인딩합니다.
```

```
> $cert = "<certificate thumbprint>"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port>_ certhash=$cert
appid="$guid"
```

예를 들어:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port>_ certhash=$cert
appid="$guid"
```

Linux 호스트에서 SnapCenter PostgreSQL 플러그인 서비스에 대한 CA 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 `/opt/NetApp/snapcenter/scc/etc_`에 위치한 'keystore.jks' 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 CA 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 'KEYSTORE_PASS' 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

```
keytool -storepasswd -keystore keystore.jks
. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된
비밀번호와 동일하게 변경합니다.
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

agent.properties 파일의 KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

3. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 있는 폴더로 이동합니다: /opt/ NetApp/snapcenter/scc/etc.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.
```



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키스토어 /opt/ NetApp/snapcenter/scc/etc가 포함된 폴더로 이동합니다.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.

7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 agent.properties 파일의 KEYSTORE_PASS 키 값입니다.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자("*", ",", ")가 포함된 경우 별칭 이름을 간단한 이름으로 변경합니다.

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. agent.properties 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

8. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 'opt/ NetApp/snapcenter/scc/etc/crl'입니다.

단계

1. agent.properties 파일에서 기본 디렉토리를 CRL_PATH 키에 맞춰 수정하고 업데이트할 수 있습니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

Windows 호스트에서 **SnapCenter PostgreSQL** 플러그인 서비스에 대한 **CA** 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_에 있는 _keystore.jks 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 **CA** 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 KEYSTORE_PASS 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

키툴 -스토어패스워드 -키스토어 키스토어.jks



Windows 명령 프롬프트에서 "keytool" 명령을 인식하지 못하는 경우 keytool 명령을 해당 전체 경로로 바꾸세요.

C:\Program Files\Java\<jdk_버전>\bin\keytool.exe" -storepasswd -keystore keystore.jks

3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.

키툴 -키패스워드 -별칭 "인증서의 별칭_이름" -키스토어 키스토어.jks

agent.properties 파일의 KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

4. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

keytool -list -v -keystore keystore.jks

4. 루트 또는 중간 인증서를 추가합니다.

keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. *keystore.jks* 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
키툴 -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -  
대상키스토어 keystore.jks -대상키스토어 유형 JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 agent.properties 파일의 KEYSTORE_PASS 키 값입니다.

```
키툴 -키패스워드 -별칭 "CA_인증서의_별칭_이름" -키스토어 키스토어.jks
```

8. agent.properties 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

9. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

SnapCenter 플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- 관련 CA 인증서에 대한 최신 CRL 파일을 다운로드하려면 다음을 참조하세요. "[SnapCenter CA 인증서에서 인증서 해지 목록 파일을 업데이트하는 방법](#)".
- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 '_C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\ etc\crl_'입니다.

단계

1. agent.properties 파일에서 기본 디렉토리를 CRL_PATH 키에 맞춰 수정하고 업데이트할 수 있습니다.
2. 이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다.

수신 인증서는 각 CRL에 대해 검증됩니다.

플러그인에 대한 CA 인증서 활성화

CA 인증서를 구성하고 SnapCenter 서버와 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- Set-SmCertificateSettings cmdlet을 실행하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- _Get-SmCertificateSettings_를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 _Get-Help command_name_을 실행하면 얻을 수

있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 하나 또는 여러 개의 플러그인 호스트를 선택하세요.
4. *추가 옵션*을 클릭하세요.
5. *인증서 검증 사용*을 선택합니다.

당신이 완료한 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- *  *는 CA 인증서가 활성화되지 않았거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- *  *는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- *  *는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- *  *는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

데이터 보호를 준비하세요

PostgreSQL용 SnapCenter 플러그인을 사용하기 위한 전제 조건

PostgreSQL용 SnapCenter 플러그인을 사용하기 전에 SnapCenter 관리자가 SnapCenter 서버를 설치하고 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다.
- SnapCenter 서버에 로그인합니다.
- 해당되는 경우 스토리지 시스템 연결을 추가하고 자격 증명을 생성하여 SnapCenter 환경을 구성합니다.
- Linux 또는 Windows 호스트에 Java 11을 설치합니다.

호스트 머신의 환경 경로 변수에 Java 경로를 설정해야 합니다.

- 백업 복제가 필요한 경우 SnapMirror 와 SnapVault 설정하세요.

PostgreSQL을 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식

SnapCenter 사용하기 전에 수행하려는 백업, 복제 및 복원 작업과 관련된 기본 개념을 이해하는 것이 좋습니다. 다양한 작업을 위해 리소스, 리소스 그룹 및 정책과 상호 작용합니다.

- 리소스는 일반적으로 SnapCenter 로 백업하거나 복제하는 PostgreSQL 클러스터입니다.
- SnapCenter 리소스 그룹은 호스트의 리소스 모음입니다.

리소스 그룹에서 작업을 수행하면 리소스 그룹에 대해 지정한 일정에 따라 리소스 그룹에 정의된 리소스에서 해당 작업이 수행됩니다.

필요에 따라 단일 리소스나 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 수행할 수도 있습니다.

- 정책은 데이터 보호 작업의 백업 빈도, 복제, 스크립트 및 기타 특성을 지정합니다.

리소스 그룹을 만들 때 해당 그룹에 대한 하나 이상의 정책을 선택합니다. 단일 리소스에 대해 주문형 백업을 수행할 때 정책을 선택할 수도 있습니다.

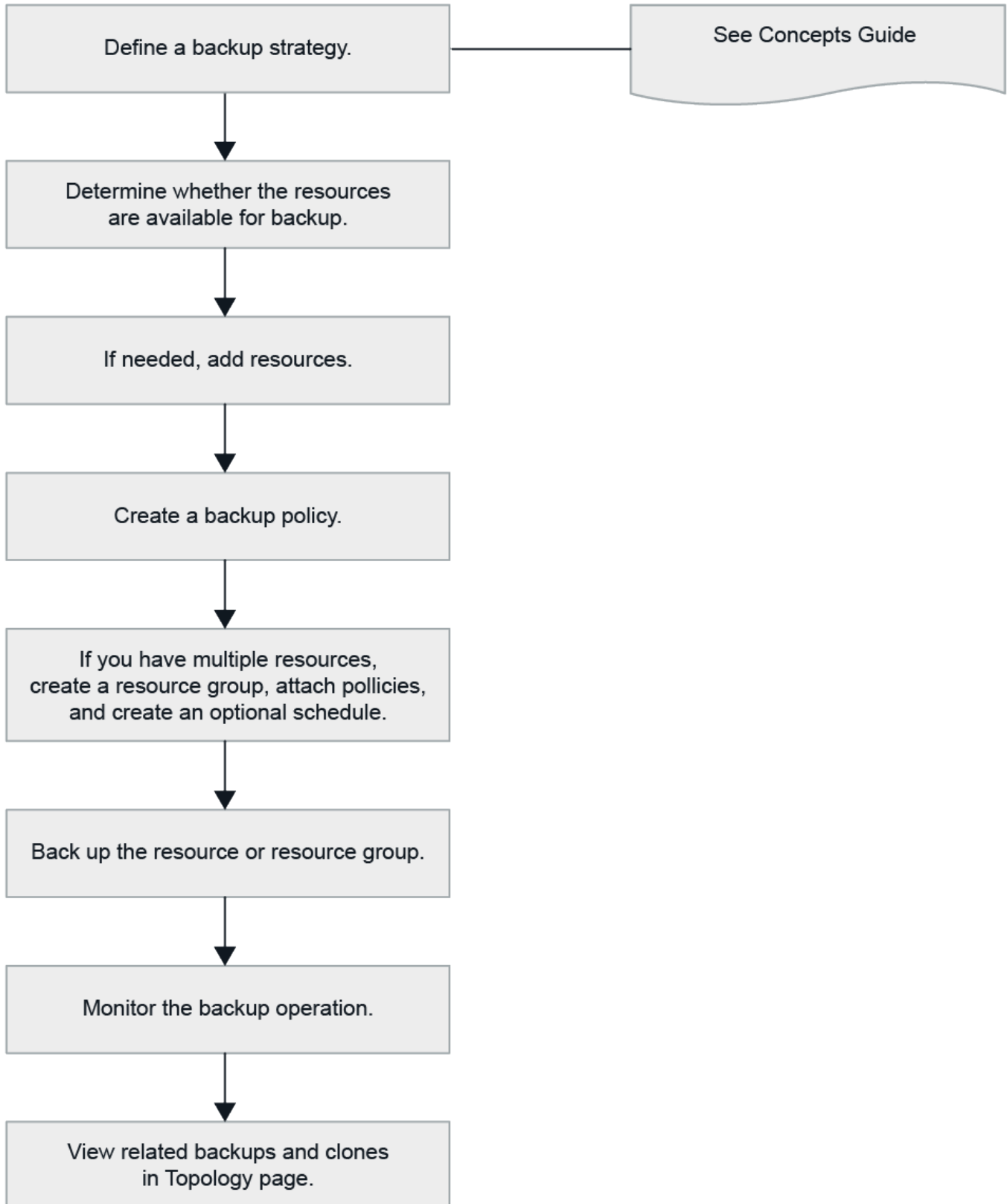
리소스 그룹은 무엇을 보호하고 싶은지, 언제 보호하고 싶은지 날짜와 시간을 정의하는 것으로 생각하면 됩니다. 정책이란 그것을 어떻게 보호할 것인지를 정의하는 것이라고 생각하세요. 예를 들어 모든 클러스터를 백업하는 경우 호스트의 모든 클러스터를 포함하는 리소스 그룹을 만들 수 있습니다. 그런 다음 리소스 그룹에 일일 정책과 시간별 정책이라는 두 가지 정책을 첨부할 수 있습니다. 리소스 그룹을 만들고 정책을 첨부할 때 리소스 그룹이 매일 전체 백업을 수행하도록 구성할 수 있습니다.

PostgreSQL 리소스 백업

PostgreSQL 리소스 백업

리소스(클러스터) 또는 리소스 그룹의 백업을 만들 수 있습니다. 백업 워크플로에는 계획, 백업할 클러스터 식별, 백업 정책 관리, 리소스 그룹 생성 및 정책 연결, 백업 생성, 작업 모니터링이 포함됩니다.

다음 워크플로는 백업 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

클러스터를 자동으로 검색합니다

리소스는 SnapCenter 에서 관리하는 Linux 호스트의 PostgreSQL 클러스터입니다. 사용 가능한 PostgreSQL 클러스터를 발견한 후 리소스 그룹에 리소스를 추가하여 데이터 보호 작업을 수행할 수 있습니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 설정 등의 작업을 이미 완료했어야 합니다.
- PostgreSQL용 SnapCenter 플러그인은 RDM/VMDK 가상 환경에 있는 리소스를 자동으로 검색하는 기능을 지원하지 않습니다.

이 작업에 관하여

- 플러그인을 설치하면 해당 Linux 호스트의 모든 클러스터가 자동으로 검색되어 리소스 페이지에 표시됩니다.
- 클러스터만 자동으로 검색됩니다.

자동으로 검색된 리소스는 수정하거나 삭제할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 PostgreSQL용 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 리소스 유형을 선택합니다.
3. (선택사항) *를 클릭하세요  *를 선택한 다음 호스트 이름을 선택합니다.

그런 다음 *를 클릭할 수 있습니다.  * 필터 창을 닫습니다.

4. 호스트에서 사용 가능한 리소스를 알아보려면 *리소스 새로 고침*을 클릭하세요.

리소스는 리소스 유형, 호스트 이름, 연관된 리소스 그룹, 백업 유형, 정책 및 전반적인 상태와 같은 정보와 함께 표시됩니다.

- 클러스터가 NetApp 스토리지에 있고 보호되지 않은 경우 전체 상태 열에 보호되지 않음이 표시됩니다.
- 클러스터가 NetApp 스토리지 시스템에 있고 보호되며 백업 작업이 수행되지 않은 경우 전체 상태 열에 백업이 실행되지 않았습나다라는 메시지가 표시됩니다. 그렇지 않으면 마지막 백업 상태에 따라 상태가 백업 실패 또는 백업 성공으로 변경됩니다.



SnapCenter 외부에서 클러스터 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

플러그인 호스트에 수동으로 리소스 추가

Windows 호스트에서는 자동 검색이 지원되지 않습니다. Postgresql 클러스터 리소스를 수동으로 추가해야 합니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 설정 등의 작업을 완료했어야 합니다.

이 작업에 관하여

다음 구성에서는 자동 검색이 지원되지 않습니다.

- RDM 및 VMDK 레이아웃

단계

1. 왼쪽 탐색 창에서 드롭다운 목록에서 Postgresql용 SnapCenter 플러그인을 선택한 다음 *리소스*를 클릭합니다.
2. 리소스 페이지에서 *Postgresql 리소스 추가*를 클릭합니다.
3. 리소스 세부 정보 제공 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	클러스터 이름을 지정합니다.
호스트 이름	호스트 이름을 입력하세요.
유형	클러스터를 선택하세요.
사례	클러스터의 부모인 인스턴스의 이름을 지정합니다.
신임장	자격 증명을 선택하거나 자격 증명에 대한 정보를 추가하세요. 이는 선택 사항입니다.

4. 스토리지 공간 제공 페이지에서 스토리지 유형을 선택하고 하나 이상의 볼륨, LUN, Qtree를 선택한 다음 *저장*을 클릭합니다.

선택 사항: *를 클릭할 수 있습니다.  * 아이콘을 클릭하면 다른 스토리지 시스템에서 볼륨, LUN, Q트리를 추가할 수 있습니다.

5. 선택 사항: 리소스 설정 페이지에서 Windows 호스트의 리소스에 대해 PostgreSQL 플러그인에 대한 사용자 정의 키-값 쌍을 입력합니다.
6. 요약 검토한 후 *마침*을 클릭하세요.

클러스터는 호스트 이름, 연관된 리소스 그룹 및 정책, 전반적인 상태와 같은 정보와 함께 표시됩니다.

사용자에게 리소스에 대한 액세스 권한을 제공하려면 사용자에게 리소스를 할당해야 합니다. 이를 통해 사용자는 자신에게 할당된 자산에 대해 권한이 있는 작업을 수행할 수 있습니다.

"사용자 또는 그룹을 추가하고 역할과 자산을 할당합니다."

당신이 완료한 후

- 클러스터를 추가한 후 PostgreSQL 클러스터 세부 정보를 수정할 수 있습니다.
- SnapCenter 5.0에서 마이그레이션된 리소스(테이블스페이스 및 클러스터)는 SnapCenter 6.0에서 PostgreSQL 클러스터 유형으로 태그가 지정됩니다.
- SnapCenter 5.0 이하 버전에서 마이그레이션된 수동으로 추가된 리소스를 수정하는 경우 사용자 지정 키 값 쌍에 대한 리소스 설정 페이지에서 다음을 수행하세요.

- 이름 필드에 "PORT"라는 용어를 지정하세요.
- 값 필드에 포트 번호를 지정합니다.

PostgreSQL에 대한 백업 정책 생성

SnapCenter 사용하여 PostgreSQL 리소스를 백업하기 전에 백업하려는 리소스 또는 리소스 그룹에 대한 백업 정책을 만들어야 합니다. 백업 정책은 백업을 관리, 일정을 정하고 보관하는 방법을 규정하는 일련의 규칙입니다.

시작하기 전에

- 백업 전략을 정의했어야 합니다.

자세한 내용은 PostgreSQL 클러스터에 대한 데이터 보호 전략 정의에 대한 정보를 참조하세요.

- SnapCenter 설치, 호스트 추가, 스토리지 시스템 연결 설정, 리소스 추가 등의 작업을 완료하여 데이터 보호를 준비했어야 합니다.
- 스냅샷을 미리 또는 볼트에 복제하는 경우 SnapCenter 관리자가 소스 및 대상 볼륨 모두에 대한 SVM을 할당해야 합니다.

또한 정책에서 복제, 스크립트 및 애플리케이션 설정을 지정할 수 있습니다. 이러한 옵션을 사용하면 다른 리소스 그룹에 대한 정책을 재사용할 때 시간을 절약할 수 있습니다.

이 작업에 관하여

- SnapLock
 - '특정 기간 동안 백업 사본을 보관합니다' 옵션을 선택한 경우 SnapLock 보관 기간은 언급된 보관 기간보다 짧거나 같아야 합니다.
 - 스냅샷 잠금 기간을 지정하면 보존 기간이 만료될 때까지 스냅샷이 삭제되지 않습니다. 이로 인해 정책에 지정된 수보다 더 많은 수의 스냅샷을 보관하게 될 수 있습니다.
 - ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *정책*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 이름 페이지에서 정책 이름과 세부 정보를 입력합니다.
5. 정책 유형 페이지에서 다음을 수행합니다.
 - a. 저장 유형을 선택하세요.
 - b. 사용자 정의 백업 설정 섹션에서 플러그인에 키-값 형식으로 전달해야 하는 특정 백업 설정을 제공합니다.

플러그인에 전달할 여러 개의 키-값을 제공할 수 있습니다.

6. 백업 및 복제 페이지에서 다음 작업을 수행합니다.

a. 주문형, 매시간, 매일, 매주, 매월 중에서 선택하여 일정 빈도를 지정하세요.



리소스 그룹을 생성하는 동안 백업 작업에 대한 일정(시작 날짜, 종료 날짜, 빈도)을 지정할 수 있습니다. 이를 통해 동일한 정책과 백업 빈도를 공유하는 리소스 그룹을 만들 수 있을 뿐만 아니라 각 정책에 다른 백업 일정을 할당할 수도 있습니다.



오전 2시로 예약한 경우, 일광 절약 시간제(DST) 기간에는 일정이 실행되지 않습니다.

a. 스냅샷 설정 섹션에서 백업 유형 페이지에서 선택한 백업 유형과 일정 유형에 대한 보존 설정을 지정합니다.

만약 당신이 원한다면...	그 다음에...
특정 수의 스냅샷을 보관하세요	*보관할 사본*을 선택한 다음 보관하려는 스냅샷 수를 지정합니다. 스냅샷 수가 지정된 수를 초과하면 스냅샷이 삭제되고 가장 오래된 사본이 먼저 삭제됩니다. SnapVault 복제를 활성화하려면 보존 횟수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷이 대상에 복제될 때까지 첫 번째 스냅샷이 SnapVault 관계에 대한 참조 스냅샷이 되기 때문에 보존 작업이 실패할 수 있습니다. 최대 보존 값은 1018입니다. 보존 기간이 ONTAP 버전에서 지원하는 것보다 높은 값으로 설정된 경우 백업이 실패합니다.
스냅샷을 특정 일수 동안 보관하세요	*사본 보관 기간*을 선택한 다음, 스냅샷을 삭제하기 전에 보관할 일수를 지정합니다.
스냅샷 복사 잠금 기간	*스냅샷 복사 잠금 기간*을 선택하고 일, 월 또는 년을 지정합니다. SnapLock 보존 기간은 100년 미만이어야 합니다.

7. 정책 라벨을 선택하세요.



원격 복제를 위해 기본 스냅샷에 SnapMirror 레이블을 할당하면 기본 스냅샷이 SnapCenter 에서 ONTAP 보조 시스템으로 스냅샷 복제 작업을 오프로드할 수 있습니다. 정책 페이지에서 SnapMirror 또는 SnapVault 옵션을 활성화하지 않고도 이 작업을 수행할 수 있습니다.

8. 보조 복제 옵션 선택 섹션에서 다음 보조 복제 옵션 중 하나 또는 둘 다를 선택합니다.

이 분야에서는...	이렇게 하세요...
로컬 스냅샷 복사본을 만든 후 SnapMirror 업데이트	다른 볼륨에 백업 세트의 미러 복사본을 생성하려면 이 필드를 선택합니다(SnapMirror 복제). ONTAP의 보호 관계가 미러 및 볼트 유형이고 이 옵션만 선택하는 경우, 기본에서 생성된 스냅샷은 대상으로 전송되지 않지만 대상에는 나열됩니다. 대상에서 이 스냅샷을 선택하여 복원 작업을 수행하는 경우 다음 오류 메시지가 표시됩니다. 선택한 보관/미러링 백업에 보조 위치를 사용할 수 없습니다. 2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고침됩니다. 보다 "토폴로지 페이지에서 PostgreSQL 리소스 관련 백업 및 복제본 보기".
로컬 스냅샷 복사본을 만든 후 SnapVault 업데이트	디스크 간 백업 복제(SnapVault 백업)를 수행하려면 이 옵션을 선택하세요. 2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고침됩니다. ONTAP에서 SnapLock Vault로 알려진 보조 노드에만 SnapLock 구성된 경우 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP에서 검색된 보조 노드의 잠금 기간이 새로 고침됩니다. SnapLock Vault에 대한 자세한 내용은 볼트 대상에서 WORM에 스냅샷 커밋을 참조하세요. 보다 "토폴로지 페이지에서 PostgreSQL 리소스 관련 백업 및 복제본 보기".
오류 재시도 횟수	작업이 중지되기 전에 허용할 수 있는 최대 복제 시도 횟수를 입력하세요.



보조 저장소의 스냅샷 최대 한도에 도달하지 않도록 하려면 ONTAP에서 보조 저장소 SnapMirror 보존 정책을 구성해야 합니다.

9. 요약 검토한 후 *마침*을 클릭하세요.

리소스 그룹을 만들고 정책을 첨부합니다.

리소스 그룹은 백업하고 보호하려는 리소스를 추가해야 하는 컨테이너입니다. 리소스 그룹을 사용하면 주어진 애플리케이션과 관련된 모든 데이터를 동시에 백업할 수 있습니다. 모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한, 수행하려는 데이터 보호 작업 유형을 정의하려면 리소스 그룹에 하나 이상의 정책을 연결해야 합니다.

이 작업에 관하여

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	리소스 그룹의 이름을 입력하세요.  리소스 그룹 이름은 250자를 넘을 수 없습니다.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력하세요. 예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.
스냅샷 복사에 사용자 정의 이름 형식 사용	이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다. 예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

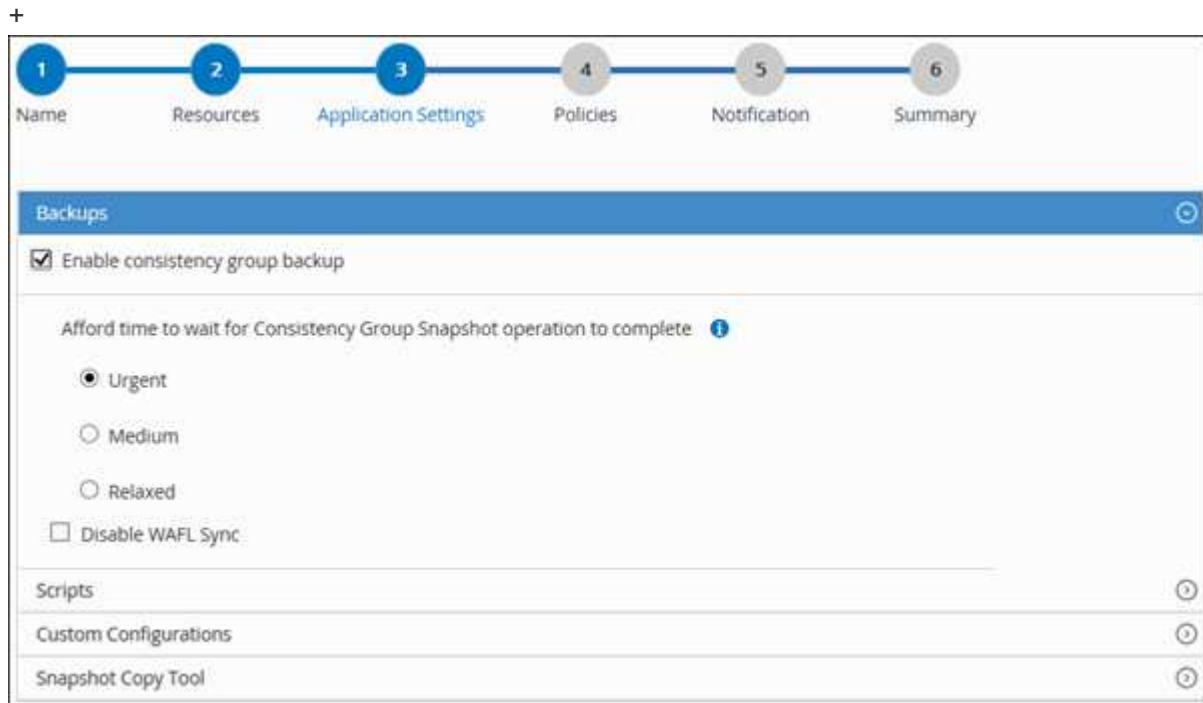
4. 리소스 페이지에서 호스트 드롭다운 목록에서 호스트 이름을 선택하고 리소스 유형 드롭다운 목록에서 리소스 유형을 선택합니다.

이는 화면에 표시되는 정보를 필터링하는 데 도움이 됩니다.

5. 사용 가능한 리소스 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 클릭하여 선택한 리소스 섹션으로 이동합니다.
6. 애플리케이션 설정 페이지에서 다음을 수행합니다.
 - a. 추가 백업 옵션을 설정하려면 백업 화살표를 클릭하세요.

일관성 그룹 백업을 활성화하고 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
일관성 그룹 스냅샷 작업이 완료될 때까지 기다릴 시간을 확보하세요.	스냅샷 작업이 완료될 때까지의 대기 시간을 지정하려면 긴급, 보통, *느슨함*을 선택합니다. 긴급 = 5초, 보통 = 7초, 여유 = 20초.
WAFL 동기화 비활성화	WAFL 일관성 지점을 강제로 적용하지 않으려면 이 옵션을 선택하세요.



- 스크립트 화살표를 클릭하고 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령을 입력합니다. 실패 시 종료하기 전에 실행할 사전 명령을 입력할 수도 있습니다.
- 사용자 정의 구성 화살표를 클릭하고 이 리소스를 사용하는 모든 데이터 보호 작업에 필요한 사용자 정의 키-값 쌍을 입력합니다.

매개변수	환경	설명
아카이브 로그 활성화	(예/아니요)	보관 로그 관리를 통해 보관 로그를 삭제할 수 있습니다.
아카이브 로그 보존	일수	보관 로그를 보관하는 일수를 지정합니다. 이 설정은 NTAP_SNAPSHOT_RETENTIONS보다 크거나 같아야 합니다.

매개변수	환경	설명
아카이브_로그_디렉토리	변경_정보_디렉토리/로그	보관 로그가 포함된 디렉토리의 경로를 지정합니다.
아카이브_로그_확장	파일 확장자	보관 로그 파일 확장자 길이를 지정합니다. 예를 들어, 보관 로그가 log_backup_0_0_0_0.161518551942 9이고 file_extension 값이 5이면 로그 확장자는 5자리인 16151을 유지합니다.
ARCHIVE_LOG_RECURSIVE_SE ARCH	(예/아니요)	하위 디렉토리 내의 보관 로그 관리를 활성화합니다. 보관 로그가 하위 디렉토리에 있는 경우 이 매개변수를 사용해야 합니다.



사용자 정의 키-값 쌍은 PostgreSQL Linux 플러그인 시스템에서는 지원되고 중앙화된 Windows 플러그인으로 등록된 PostgreSQL 클러스터에서는 지원되지 않습니다.

- c. 스냅샷 복사 도구* 화살표를 클릭하여 스냅샷을 만드는 도구를 선택하세요.

원하신다면...	그 다음에...
SnapCenter Windows용 플러그인을 사용하여 스냅샷을 생성하기 전에 파일 시스템을 일관된 상태로 만듭니다. Linux 리소스의 경우 이 옵션은 적용되지 않습니다.	*파일 시스템 일관성을 갖춘 SnapCenter *를 선택하세요.
SnapCenter 사용하여 스토리지 수준 스냅샷을 생성합니다.	*파일 시스템 일관성이 없는 SnapCenter *를 선택하세요.
스냅샷 복사본을 생성하기 위해 호스트에서 실행할 명령을 입력합니다.	*기타*를 선택한 다음 호스트에서 실행할 명령을 입력하여 스냅샷을 생성합니다.

7. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다.  *.

정책은 '선택한 정책에 대한 일정 구성' 섹션에 나열되어 있습니다.

- b.

일정 구성 열에서 *를 클릭합니다.  * 구성하려는 정책에 대해.

c. 정책 `_policy_name_`에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 `policy_name`은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP 서버는 설정 > *전역 설정*에서 구성해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

ASA r2 시스템에서 PostgreSQL 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.

ASA r2 시스템에 있는 리소스를 추가하려면 리소스 그룹을 만들어야 합니다. 리소스 그룹을 생성하는 동안 보조 보호를 프로비저닝할 수도 있습니다.

시작하기 전에

- ONTAP 9.x 리소스와 ASA r2 리소스를 동일한 리소스 그룹에 추가하지 않도록 해야 합니다.
- ONTAP 9.x 리소스와 ASA r2 리소스가 모두 포함된 데이터베이스가 없는지 확인해야 합니다.

이 작업에 관하여

- 2차 보호는 로그인한 사용자에게 **SecondaryProtection** 기능이 활성화된 역할이 할당된 경우에만 사용할 수 있습니다.
- 2차 보호를 활성화한 경우 기본 및 2차 일관성 그룹을 생성하는 동안 리소스 그룹은 유지 관리 모드로 전환됩니다. 기본 및 보조 일관성 그룹이 생성된 후 리소스 그룹은 유지 관리 모드에서 해제됩니다.
- SnapCenter 클론 리소스에 대한 보조 보호를 지원하지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.
 - a. 이름 필드에 리소스 그룹의 이름을 입력합니다.



리소스 그룹 이름은 250자를 넘을 수 없습니다.

- b. 나중에 리소스 그룹을 검색하는 데 도움이 되도록 태그 필드에 하나 이상의 레이블을 입력하세요.

예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.

c. 이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다.
기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

d. 백업하지 않을 보관 로그 파일의 대상을 지정합니다.



필요한 경우 접두사를 포함하여 애플리케이션에 설정된 것과 정확히 동일한 목적지를 사용해야 합니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 데이터베이스 호스트 이름을 선택합니다.



리소스가 성공적으로 검색된 경우에만 해당 리소스가 사용 가능한 리소스 섹션에 나열됩니다.
최근에 리소스를 추가한 경우 리소스 목록을 새로 고침 후에만 사용 가능한 리소스 목록에 표시됩니다.

5. 사용 가능한 리소스 섹션에서 ASA r2 리소스를 선택하고 선택한 리소스 섹션으로 이동합니다.

6. 애플리케이션 설정 페이지에서 백업 옵션을 선택하세요.

7. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



또한 다음을 클릭하여 정책을 생성할 수도 있습니다.  .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.

c. 정책 _policy_name_에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 _policy_name_은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 선택한 정책에 대해 보조 보호가 활성화된 경우 보조 보호 페이지가 표시되며 다음 단계를 수행해야 합니다.

a. 복제 정책의 유형을 선택하세요.



동기 복제 정책은 지원되지 않습니다.

b. 사용할 일관성 그룹 접미사를 지정합니다.

c. 대상 클러스터 및 대상 SVM 드롭다운에서 사용하려는 피어링된 클러스터와 SVM을 선택합니다.



SnapCenter에서는 클러스터 및 SVM 피어링을 지원하지 않습니다. 클러스터 및 SVM 피어링을 수행하려면 System Manager 또는 ONTAP CLI를 사용해야 합니다.



리소스가 이미 SnapCenter 외부에서 보호되고 있는 경우 해당 리소스는 보조 보호 리소스 섹션에 표시됩니다.

1. 확인 페이지에서 다음 단계를 수행하세요.

- *로케이터 로드*를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 저장소에서 검증을 수행합니다.
- 딸깍 하는 소리  일정 구성 열에서 정책의 모든 일정 유형에 대한 확인 일정을 구성합니다.
- 확인 일정 추가 policy_name 대화 상자에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	이렇게 하세요...
백업 후 검증 실행	*백업 후 검증 실행*을 선택하세요.
검증 일정을 예약하세요	*예약된 확인 실행*을 선택한 다음 드롭다운 목록에서 일정 유형을 선택합니다.

- 보조 저장소 시스템에서 백업을 확인하려면 *보조 위치에서 확인*을 선택하세요.
- *확인*을 클릭합니다.

구성된 검증 일정은 적용된 일정 열에 나열됩니다.

2. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*을 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

3. 요약 검토한 후 *마침*을 클릭하세요.

PowerShell cmdlet을 사용하여 PostgreSQL용 스토리지 시스템 연결 및 자격 증명 만들기

PowerShell cmdlet을 사용하여 PostgreSQL 클러스터를 백업, 복원 또는 복제하기 전에 스토리지 가상 머신(SVM) 연결과 자격 증명을 만들어야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 저장소 연결을 생성하려면 인프라 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

스토리지 시스템 연결을 추가하는 동안에는 호스트 플러그인 설치가 진행 중이어서는 안 됩니다. 호스트 캐시가 업데이트되지 않고 클러스터 상태가 SnapCenter GUI에 “백업에 사용할 수 없음” 또는 “NetApp 스토리지에 없음”으로 표시될 수 있기 때문입니다.

- 저장 시스템 이름은 고유해야 합니다.

SnapCenter 서로 다른 클러스터에 동일한 이름을 가진 여러 스토리지 시스템을 지원하지 않습니다. SnapCenter 에서 지원하는 각 스토리지 시스템은 고유한 이름과 고유한 데이터 LIF IP 주소를 가져야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 PowerShell Core 연결 세션을 시작합니다.

```
PS C:\> Open-SmConnection
```

2. Add-SmStorageConnection cmdlet을 사용하여 스토리지 시스템에 대한 새 연결을 만듭니다.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Add-SmCredential cmdlet을 사용하여 새 자격 증명을 만듭니다.

이 예제에서는 Windows 자격 증명을 사용하여 FinanceAdmin이라는 새 자격 증명을 만드는 방법을 보여줍니다.

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. SnapCenter 서버에 PostgreSQL 통신 호스트를 추가합니다.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName  
FinanceAdmin -PluginCode PostgreSQL
```

5. 호스트에 패키지와 PostgreSQL용 SnapCenter 플러그인을 설치합니다.

Linux의 경우:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode  
PostgreSQL
```

Windows의 경우:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode  
PostgreSQL -FilesystemCode scw -RunAsName FinanceAdmin
```

6. SQLLIB의 경로를 설정합니다.

Windows의 경우 PostgreSQL 플러그인은 SQLLIB 폴더의 기본 경로인 "C:\Program Files\IBM\SQLLIB\BIN"을 사용합니다.

기본 경로를 재정의하려면 다음 명령을 사용하세요.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode PostgreSQL -configSettings @{"PostgreSQL_SQLLIB_CMD" = "<custom_path>\IBM\SQLLIB\BIN"}
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

PostgreSQL 백업

리소스가 아직 어떤 리소스 그룹에도 속하지 않은 경우 리소스 페이지에서 리소스를 백업할 수 있습니다.

시작하기 전에

- 백업 정책을 생성했어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에 "snapmirror all" 권한이 포함되어야 합니다. 하지만 "vsadmin" 역할을 사용하는 경우 "snapmirror all" 권한은 필요하지 않습니다.
- 스냅샷 복사 기반 백업 작업의 경우 모든 테넌트 클러스터가 유효하고 활성화되어 있는지 확인하세요.
- 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령의 경우, 플러그인 호스트에서 다음 경로의 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Linux 호스트의 기본 위치: */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

선택하다  *를 선택한 다음 호스트 이름과 리소스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 선택할 수 있습니다  필터 창을 닫으려면.

3. 백업할 리소스를 선택하세요.
4. 리소스 페이지에서 *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택한 다음 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, *customtext_policy_hostname* 또는 *_resource_hostname_*입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

5. 애플리케이션 설정 페이지에서 다음을 수행합니다.

- 추가 백업 옵션을 설정하려면 백업 화살표를 선택하세요.

필요한 경우 일관성 그룹 백업을 활성화하고 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
"일관성 그룹 스냅샷" 작업이 완료될 때까지 기다릴 시간을 확보하세요.	스냅샷 작업이 완료될 때까지의 대기 시간을 지정하려면 긴급, 보통, *느슨함*을 선택합니다. 긴급 = 5초, 보통 = 7초, 여유 = 20초.
WAFL 동기화 비활성화	WAFL 일관성 지점을 강제로 적용하지 않으려면 이 옵션을 선택하세요.

- 스크립트 화살표를 선택하여 정지, 스냅샷 및 정지 해제 작업에 대한 사전 및 사후 명령을 실행합니다.

백업 작업을 종료하기 전에 사전 명령을 실행할 수도 있습니다. Prescript와 Postscript는 SnapCenter Server에서 실행됩니다.

- 사용자 정의 구성 화살표를 선택한 다음, 이 리소스를 사용하는 모든 작업에 필요한 사용자 정의 값 쌍을 입력합니다.
- 스냅샷 복사 도구* 화살표를 선택하여 스냅샷을 만드는 도구를 선택하세요.

원하신다면...	그 다음에...
SnapCenter 사용하여 스토리지 수준 스냅샷을 생성합니다.	*파일 시스템 일관성이 없는 SnapCenter *를 선택하세요.
SnapCenter Windows용 플러그인을 사용하여 파일 시스템을 일관된 상태로 만든 다음 스냅샷을 생성합니다.	*파일 시스템 일관성을 갖춘 SnapCenter *를 선택하세요.

원하신다면...	그 다음에...
스냅샷을 생성하는 명령을 입력하려면	*기타*를 선택한 다음 스냅샷을 만드는 명령을 입력합니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다. *.

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

b. 선택하다 * 일정을 구성하려는 정책에 대한 일정 구성 옆에 있습니다.

c. 정책 _policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 선택합니다.

_policy_name_은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 옆에 나열됩니다.

7. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > *전역 설정*에서도 구성해야 합니다.

8. 요약 검토한 후 *마침*을 선택하세요.

리소스 토폴로지 페이지가 표시됩니다.

9. *지금 백업*을 선택하세요.
10. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스에 여러 정책을 적용한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.
 - b. *백업*을 선택하세요.
11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.
 - MetroCluster 구성에서 SnapCenter 장애 조치 후 보호 관계를 감지하지 못할 수 있습니다.

자세한 내용은 다음을 참조하세요. ["MetroCluster 장애 조치 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다."](#)
 - VMDK에서 애플리케이션 데이터를 백업하고 SnapCenter Plug-in for VMware vSphere의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다.

Java 힙 크기를 늘리려면 스크립트 파일 `/opt/netapp/init_scripts/scvservice_`를 찾으세요. 해당 스크립트에서 `_do_start` 메서드 명령은 SnapCenter VMware 플러그인 서비스를 시작합니다. 해당 명령을 다음으로 업데이트하세요: `Java -jar -Xmx8192M -Xms4096M`

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-SmConnection
```

사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.

2. Add-SmResources cmdlet을 사용하여 수동 리소스를 추가합니다.

이 예제에서는 PostgreSQL 인스턴스를 추가하는 방법을 보여줍니다.

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode PostgreSQL
-ResourceType Instance -ResourceName postgresqlinst1
-StorageFootPrint
(@{"VolumeName"="winpostgresql01_data01";"LUNName"="winpostgresql01_
data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.
4. Add-SmResourceGroup cmdlet을 사용하여 리소스를 보호하거나 SnapCenter에 새 리소스 그룹을 추가합니다.
5. New-SmBackup cmdlet을 사용하여 새로운 백업 작업을 시작합니다.

이 예제에서는 리소스 그룹을 백업하는 방법을 보여줍니다.

```
C:\PS> New-SMBackup -ResourceGroupName 'ResourceGroup_wback-up-  
clusters-using-powershell-cmdlets-postgresql.adocith_Resources'  
-Policy postgresql_policy1
```

이 예제에서는 보호된 리소스를 백업합니다.

```
C:\PS> New-SMBackup -Resources  
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}  
-Policy postgresql_policy2
```

6. Get-smJobSummaryReport cmdlet을 사용하여 작업 상태(실행 중, 완료 또는 실패)를 모니터링합니다.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Get-SmBackupReport cmdlet을 사용하여 복원 또는 복제 작업을 수행하기 위한 백업 ID, 백업 이름과 같은 백업 작업 세부 정보를 모니터링합니다.

```

PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :

```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

리소스 그룹 백업

리소스 그룹은 호스트의 리소스 모음입니다. 리소스 그룹에 대한 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다.

시작하기 전에

- 정책이 첨부된 리소스 그룹을 만들어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에 "snapmirror all" 권한이 포함되어야 합니다. 하지만 "vsadmin" 역할을 사용하는 경우 "snapmirror all" 권한은 필요하지 않습니다.

이 작업에 관하여

리소스 페이지에서 필요에 따라 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 첨부되고 일정이 구성된 경우 백업은 일정에 따라 자동으로 수행됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.

검색창에 리소스 그룹 이름을 입력하거나 다음을 선택하여 리소스 그룹을 검색할 수 있습니다.  , 그리고 태그를 선택합니다. 그런 다음 선택할 수 있습니다.  필터 창을 닫으려면.

3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음, *지금 백업*을 선택합니다.
4. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스 그룹에 여러 정책을 연결한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. *백업*을 선택하세요.

5. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

PostgreSQL 백업 작업 모니터링

SnapCenterJobs 페이지를 사용하여 다양한 백업 작업의 진행 상황을 모니터링할 수 있습니다. 완료 시점이나 문제가 있는지 확인하기 위해 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 해당 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  백업 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *백업*을 선택합니다.
 - d. 상태 드롭다운에서 백업 상태를 선택합니다.
 - e. *적용*을 클릭하면 작업이 성공적으로 완료된 것을 볼 수 있습니다.

4. 백업 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인하세요.



백업 작업 상태가 표시됩니다. 작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 표시가 되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

활동 창에서 **PostgreSQL** 클러스터의 데이터 보호 작업을 모니터링합니다.

활동 창에는 가장 최근에 수행된 5개의 작업이 표시됩니다. 활동 창에는 작업이 시작된 시점과 작업 상태도 표시됩니다.

활동 창에는 백업, 복원, 복제 및 예약된 백업 작업에 대한 정보가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 딸깍 하는 소리 활동 창에서 가장 최근의 작업 5개를 확인하세요.

작업 중 하나를 클릭하면 작업 세부 정보가 작업 세부 정보 페이지에 나열됩니다.

PostgreSQL에 대한 백업 작업 취소

대기 중인 백업 작업을 취소할 수 있습니다.

필요한 것

- 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 모니터 페이지나 활동 창에서 백업 작업을 취소할 수 있습니다.
- 실행 중인 백업 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 백업 작업을 취소할 수 있습니다.
- 취소할 수 없는 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 백업 작업을 취소할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	a. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. b. 작업을 선택한 다음 *작업 취소*를 클릭합니다.

...로부터	행동
활동 창	a. 백업 작업을 시작한 후 *를 클릭하세요.  * 활동 창에서 가장 최근의 작업 5개를 확인하세요. b. 작업을 선택하세요. c. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

작업이 취소되고 리소스는 이전 상태로 돌아갑니다.

토폴로지 페이지에서 PostgreSQL 백업 및 복제본 보기

리소스를 백업하거나 복제할 준비를 할 때 기본 및 보조 저장소에 있는 모든 백업과 복제본을 그래픽으로 표현해 보면 도움이 될 수 있습니다.

이 작업에 관하여

다음 아이콘을 '사본 관리' 보기에서 검토하여 백업 및 복제본을 기본 저장소 또는 보조 저장소(미러 사본 또는 볼트 사본)에서 사용할 수 있는지 확인할 수 있습니다.

-  기본 스토리지에서 사용 가능한 백업 및 복제본의 수를 표시합니다.
-  SnapMirror 기술을 사용하여 보조 저장소에 미러링된 백업 및 복제본의 수를 표시합니다.
-  SnapVault 기술을 사용하여 보조 저장소에 복제된 백업 및 복제본의 수를 표시합니다.



표시된 백업 수에는 보조 저장소에서 삭제된 백업이 포함됩니다. 예를 들어, 4개의 백업만 보존하는 정책을 사용하여 6개의 백업을 만든 경우 표시되는 백업 수는 6개입니다.



미러 볼트 유형 볼륨의 버전 가변형 미러 백업의 복제본은 토폴로지 보기에 표시되지만, 토폴로지 보기의 미러 백업 수에는 버전 가변형 백업이 포함되지 않습니다.

토폴로지 페이지에서는 선택한 리소스 또는 리소스 그룹에 사용 가능한 모든 백업과 복제본을 볼 수 있습니다. 해당 백업 및 복제의 세부 정보를 보고 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

단계

- 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
- 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
- 리소스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 리소스를 선택합니다.

리소스가 보호된 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. *요약 카드*를 검토하여 기본 및 보조 저장소에서 사용 가능한 백업 및 복제본 수에 대한 요약 확인하세요.

요약 카드 섹션에는 스냅샷 복사 기반 백업과 복제본의 총 수가 표시됩니다.

새로 고침 버튼을 클릭하면 저장소에 대한 쿼리가 시작되어 정확한 개수가 표시됩니다.

SnapLock 이 활성화된 백업을 수행한 경우 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간이 새로 고쳐집니다. 주간 일정은 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간도 새로 고칩니다.

애플리케이션 리소스가 여러 볼륨에 분산되어 있는 경우 백업에 대한 SnapLock 만료 시간은 볼륨의 스냅샷에 설정된 가장 긴 SnapLock 만료 시간이 됩니다. 가장 긴 SnapLock 만료 시간은 ONTAP 에서 검색됩니다.

주문형 백업 후, 새로 고침 버튼을 클릭하면 백업이나 복제의 세부 정보가 새로 고칩니다.

5. 복사본 관리 보기에서 기본 또는 보조 저장소의 백업 또는 *복제*를 클릭하면 백업 또는 복제의 세부 정보를 볼 수 있습니다.

백업 및 복제의 세부 정보는 표 형식으로 표시됩니다.

6. 표에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 복제, 삭제 작업을 수행합니다.



보조 저장소에 있는 백업은 이름을 바꾸거나 삭제할 수 없습니다.

7. 복제본을 삭제하려면 테이블에서 복제본을 선택한 다음 클릭하세요. .

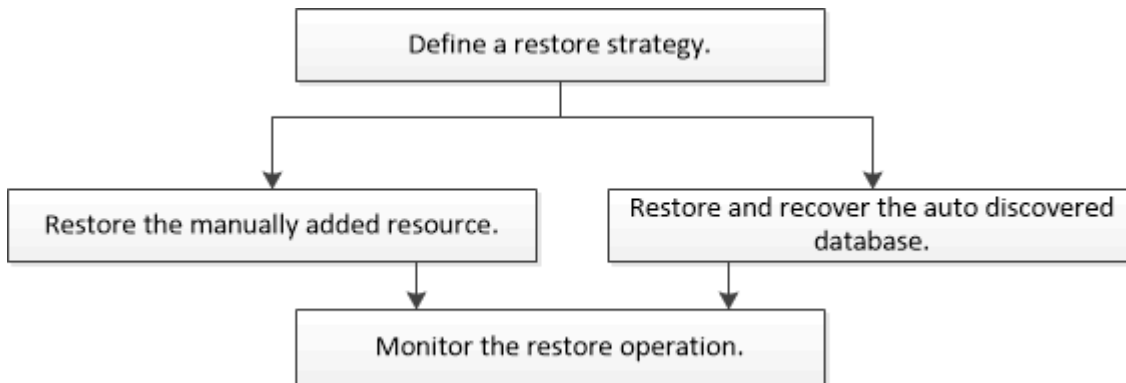
8. 복제본을 분할하려면 테이블에서 복제본을 선택한 다음 클릭하세요. .

PostgreSQL 복원

워크플로 복원

복원 및 복구 워크플로에는 계획, 복원 작업 수행, 작업 모니터링이 포함됩니다.

다음 워크플로는 복원 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#) .

수동으로 추가된 리소스 백업을 복원하고 복구합니다.

SnapCenter 사용하면 하나 이상의 백업에서 데이터를 복원하고 복구할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 복원하려는 리소스 또는 리소스 그룹에 대해 현재 진행 중인 모든 백업 작업을 취소해야 합니다.
- 사전 복원, 사후 복원, 마운트 및 마운트 해제 명령의 경우, 다음 경로에서 플러그인 호스트에서 사용 가능한 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Linux 호스트의 기본 위치: */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 함께 표시됩니다.



백업은 리소스 그룹을 위한 것일 수 있지만 복원할 때는 복원할 개별 리소스를 선택해야 합니다.

리소스가 보호되지 않은 경우 전체 상태 열에 "보호되지 않음"이 표시됩니다. 이는 리소스가 보호되지 않았거나 다른 사용자가 리소스를 백업했음을 의미할 수 있습니다.

3. 리소스를 선택하거나 리소스 그룹을 선택한 다음 해당 그룹에서 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 기본 백업 테이블에서 복원하려는 백업을 선택한 다음 *를 클릭합니다.  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scscr0191685001_01-05-2017-01.35.06.6463	1/5/2017 1:35:27 AM 

6. 복원 범위 페이지에서 *리소스 완료*를 선택합니다.

- a. *전체 리소스*를 선택하면 PostgreSQL 클러스터의 구성된 모든 데이터 볼륨이 복원됩니다.

리소스에 볼륨이나 Q트리가 포함되어 있는 경우 해당 볼륨이나 Q트리에서 복원을 위해 선택한 스냅샷 이후에 생성된 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 다른 리소스가 동일한 볼륨이나 Q트리에 호스팅된 경우 해당 리소스도 삭제됩니다.

여러 개의 LUN을 선택할 수 있습니다.



*모두*를 선택하면 볼륨, Q트리 또는 LUN의 모든 파일이 복원됩니다.

7. 사전 작업 페이지에서 복원 작업을 수행하기 전에 실행할 사전 복원 및 마운트 해제 명령을 입력합니다.

자동 검색된 리소스에는 마운트 해제 명령을 사용할 수 없습니다.

8. Post ops 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.

자동 검색된 리소스에는 마운트 명령을 사용할 수 없습니다.

9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > 전역 설정 페이지에서도 구성해야 합니다.

10. 요약을 검토한 후 *마침*을 클릭하세요.

11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-Smconnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

이 예에서는 2015년 1월 29일부터 2015년 2월 3일까지의 백업에 대한 자세한 정보를 표시합니다.

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

자동 검색된 클러스터 백업 복원 및 복구

SnapCenter 사용하면 하나 이상의 백업에서 데이터를 복원하고 복구할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 복원하려는 리소스 또는 리소스 그룹에 대해 현재 진행 중인 모든 백업 작업을 취소해야 합니다.
- 사전 복원, 사후 복원, 마운트 및 마운트 해제 명령의 경우, 다음 경로에서 플러그인 호스트에서 사용 가능한 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

◦ Linux 호스트의 기본 위치: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- 파일 기반 백업 사본은 SnapCenter 에서 복원할 수 없습니다.
- 자동 검색된 리소스의 경우 SFSR을 통해 복원이 지원됩니다.
- 자동 복구가 지원되지 않습니다.
- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 함께 표시됩니다.



백업은 리소스 그룹을 위한 것일 수 있지만 복원할 때는 복원할 개별 리소스를 선택해야 합니다.

리소스가 보호되지 않은 경우 전체 상태 열에 "보호되지 않음"이 표시됩니다. 이는 리소스가 보호되지 않았거나 다른 사용자가 리소스를 백업했음을 의미할 수 있습니다.

3. 리소스를 선택하거나 리소스 그룹을 선택한 다음 해당 그룹에서 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.

5. 기본 백업 테이블에서 복원하려는 백업을 선택한 다음 *를 클릭합니다. .

Primary Backup(s)	
search	T
Backup Name	End Date
rg1_scscr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. 복원 범위 페이지에서 *전체 리소스*를 선택하여 PostgreSQL 클러스터의 구성된 데이터 볼륨을 복원합니다.

7. 복구 범위 페이지에서 다음 옵션 중 하나를 선택하세요.

만약 당신이...	이렇게 하세요...
현재 시간에 최대한 가깝게 복구하고 싶습니다.	*최근 상태로 복구*를 선택하세요. 단일 컨테이너 리소스의 경우 하나 이상의 로그 및 카탈로그 백업 위치를 지정합니다.

지정된 시점으로 복구하고 싶습니다	*특정 시점으로 복구*를 선택합니다. a. 날짜와 시간을 입력하세요. 날짜와 시간을 입력하세요. 예를 들어, PostgreSQL Linux 호스트는 캘리포니아주 서니베일에 위치하고 노스캐롤라이나주 롤리의 사용자는 SnapCenter 로 로그를 복구하고 있습니다. 사용자가 오전 5시(캘리포니아주 서니베일)로 복구를 수행하려는 경우 사용자는 브라우저 시간대를 GMT-07:00인 PostgreSQL Linux 호스트 시간대로 설정하고 날짜와 시간을 오전 5시로 지정해야 합니다.
복구하고 싶지 않아요	*복구 안 함*을 선택하세요.



수동으로 추가한 PostgreSQL 리소스는 복구할 수 없습니다.



PostgreSQL용 SnapCenter 플러그인은 수동으로 복구하는 데 도움이 되도록 `/<OS_temp_folder>/postgresql_sc_recovery<Restore_JobId>/_` 폴더에 `backup_label`과 `tablespace_map`을 생성합니다.

1. 사전 작업 페이지에서 복원 작업을 수행하기 전에 실행할 사전 복원 및 마운트 해제 명령을 입력합니다.

자동 검색된 리소스에는 마운트 해제 명령을 사용할 수 없습니다.

2. Post ops 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.

자동 검색된 리소스에는 마운트 명령을 사용할 수 없습니다.

3. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > 전역 설정 페이지에서도 구성해야 합니다.

4. 요약 검토 후 *마침*을 클릭하세요.
5. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet을 사용하여 리소스 복원

리소스 백업을 복원하려면 SnapCenter 서버와 연결 세션을 시작하고, 백업을 나열하고 백업 정보를 검색하고, 백업을 복원해야 합니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-Smconnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----
1	Payroll Dataset_vise-f6_08... 8/4/2015	11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08... 8/4/2015	11:23:17 AM

이 예에서는 2015년 1월 29일부터 2015년 2월 3일까지의 백업에 대한 자세한 정보를 표시합니다.

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName        : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName        : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.


```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

PostgreSQL 복원 작업 모니터링

작업 페이지를 사용하여 다양한 SnapCenter 복원 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

복원 후 상태는 복원 작업 후 리소스의 조건과 수행할 수 있는 추가 복원 작업을 설명합니다.

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중

-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복원 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복원*을 선택합니다.
 - d. 상태 드롭다운 목록에서 복원 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복원 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

PostgreSQL 리소스 백업 복제

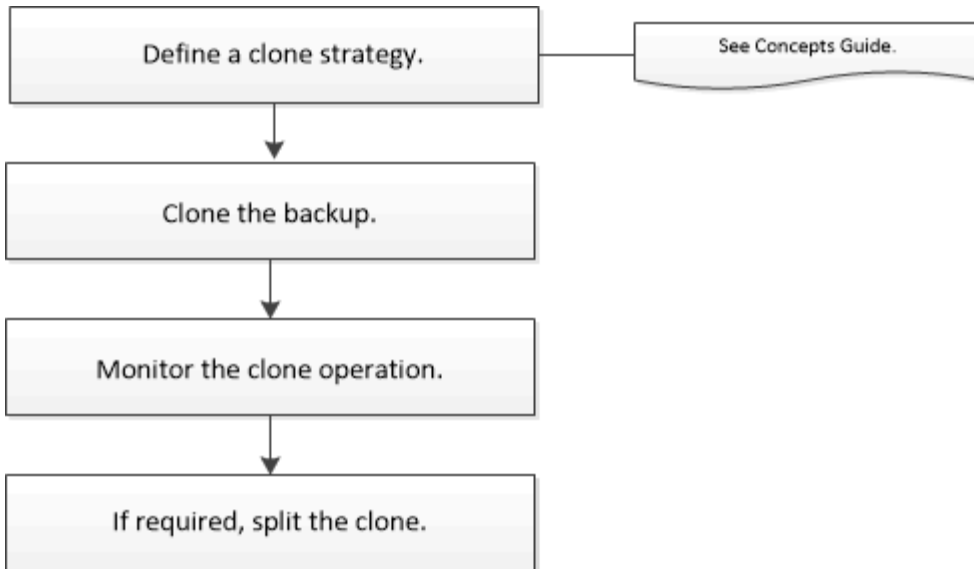
복제 워크플로

복제 워크플로에는 복제 작업을 수행하고 작업을 모니터링하는 작업이 포함됩니다.

이 작업에 관하여

- 소스 PostgreSQL 서버에서 복제할 수 있습니다.
- 다음과 같은 이유로 리소스 백업을 복제할 수 있습니다.
 - 애플리케이션 개발 주기 동안 현재 리소스 구조 및 콘텐츠를 사용하여 구현해야 하는 기능을 테스트하려면
 - 데이터 웨어하우스를 채울 때 데이터 추출 및 조작 도구
 - 실수로 삭제되거나 변경된 데이터를 복구하려면

다음 워크플로는 복제 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

PostgreSQL 백업 복제

SnapCenter 사용하여 백업을 복제할 수 있습니다. 기본 또는 보조 백업에서 복제할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 볼륨을 호스팅하는 집계가 스토리지 가상 머신(SVM)의 할당된 집계 목록에 있는지 확인해야 합니다.
- 복제 전 또는 복제 후 명령의 경우, 플러그인 호스트에서 다음 경로의 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: *C:\Program Files\NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Linux 호스트의 기본 위치: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- FlexClone 볼륨 분할 작업에 대한 정보는 다음을 참조하세요. <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["FlexClone 볼륨을 부모 볼륨에서 분할합니다."].
- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 같은 정보와 함께 표시됩니다.

3. 리소스 또는 리소스 그룹을 선택하세요.

리소스 그룹을 선택하는 경우 리소스를 선택해야 합니다.

리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 표에서 데이터 백업을 선택한 다음 클릭하세요.  .
6. 위치 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
복제 서버	복제본을 생성할 호스트를 선택하세요.
대상 포트	기존 백업에서 복제할 대상 PostgreSQL 대상 포트를 입력합니다.
NFS 내보내기 IP 주소	복제된 볼륨을 내보낼 IP 주소나 호스트 이름을 입력합니다. 이는 NFS 저장 유형 리소스에만 적용됩니다.
용량 풀 최대 처리량(MiB/s)	용량 풀의 최대 처리량을 입력하세요. 이는 ANF 스토리지 유형 리소스에만 적용됩니다.

7. 스크립트 페이지에서 다음 단계를 수행합니다.



스크립트는 플러그인 호스트에서 실행됩니다.

- a. 복제 작업 전이나 후에 실행해야 하는 사전 복제 또는 사후 복제에 대한 명령을 각각 입력합니다.
 - 사전 복제 명령: 동일한 이름을 가진 기존 클러스터 삭제
 - 복제 후 명령: 클러스터를 확인하거나 클러스터를 시작합니다.
- b. 호스트에 파일 시스템을 마운트하려면 mount 명령을 입력하세요.

Linux 머신에서 볼륨이나 qtree에 대한 마운트 명령:

NFS의 예: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

10. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-SmConnection
```

2. Get-SmBackup cmdlet을 사용하여 복제 작업을 수행하기 위해 백업을 검색합니다.

이 예에서는 복제에 사용할 수 있는 백업이 두 개 있음을 보여줍니다.

```
C:\PS> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
1	Payroll Dataset_vise-f6_08...
8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...
8/4/2015 11:23:17 AM	

3. 기존 백업에서 복제 작업을 시작하고 복제된 볼륨이 내보내지는 NFS 내보내기 IP 주소를 지정합니다.

이 예에서는 복제할 백업의 NFSExportIPs 주소가 10.32.212.14임을 보여줍니다.

PostgreSQL 클러스터의 경우:

```
PS C:\> New-SmClone -AppPluginCode PostgreSQL -BackupName "
scpostgresql01_ openenglab_netapp_com_PostgreSQL_postgres_5432_06-
26-2024_00_33_41_1570" -Resources @{"Host"="
10.32.212.13";"Uid"="postgres_5432"} -port 2345 -CloneToHost
10.32.212.14
```



NFSExportIPs가 지정되지 않으면 기본값이 복제 대상 호스트로 내보내집니다.

4. Get-SmCloneReport cmdlet을 사용하여 복제 작업 세부 정보를 보고 백업이 성공적으로 복제되었는지

확인합니다.

클론 ID, 시작 날짜 및 시간, 종료 날짜 및 시간과 같은 세부 정보를 볼 수 있습니다.

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration              : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName            : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName     : OnDemand_Full_Log
SmBackupPolicyId     : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId          : 4
CloneName            : Draper__clone__08-03-2015_14.43.53
SourceResources       : {Don, Betty, Bobby, Sally}
ClonedResources       : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError            :
```

PostgreSQL 복제 작업 모니터링

작업 페이지를 사용하여 SnapCenter 복제 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복제 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복제*를 선택합니다.
 - d. 상태 드롭다운 목록에서 복제 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복제 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

클론 분할

SnapCenter 사용하면 복제된 리소스를 부모 리소스에서 분할할 수 있습니다. 분할된 복제본은 부모 리소스로부터 독립됩니다.

이 작업에 관하여

- 중간 복제본에서는 복제 분할 작업을 수행할 수 없습니다.

예를 들어, 데이터베이스 백업에서 clone1을 만든 후 clone1의 백업을 만든 다음 이 백업(clone2)을 복제할 수 있습니다. clone2를 생성한 후 clone1은 중간 복제본이 되며 clone1에서 복제 분할 작업을 수행할 수 없습니다. 하지만 clone2에 대해 클론 분할 작업을 수행할 수 있습니다.

clone2를 분할한 후에는 clone1에 대해 clone 분할 작업을 수행할 수 있습니다. clone1은 더 이상 중간 클론이 아니기 때문입니다.

- 복제본을 분할하면 복제본의 백업 사본과 복제 작업이 삭제됩니다.
- FlexClone 볼륨 분할 작업에 대한 정보는 다음을 참조하세요. "[FlexClone 볼륨을 부모 볼륨에서 분할합니다.](#)".
- 스토리지 시스템의 볼륨이나 집계가 온라인인지 확인하세요.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 적절한 옵션을 선택하세요.

옵션	설명
데이터베이스 애플리케이션의 경우	보기 목록에서 *데이터베이스*를 선택합니다.
파일 시스템의 경우	보기 목록에서 *경로*를 선택합니다.

3. 목록에서 적절한 리소스를 선택하세요.

리소스 토폴로지 페이지가 표시됩니다.

4. 사본 관리 보기에서 복제된 리소스(예: 데이터베이스 또는 LUN)를 선택한 다음 *를 클릭합니다. .
5. 분할할 클론의 예상 크기와 집계에 필요한 사용 가능한 공간을 검토한 다음 *시작*을 클릭합니다.
6. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

SMCore 서비스를 다시 시작하면 복제 분할 작업이 더 이상 응답하지 않습니다. 복제 분할 작업을 중지하려면 Stop-SmJob cmdlet을 실행한 다음 복제 분할 작업을 다시 시도해야 합니다.

복제본이 분할되었는지 여부를 확인하기 위해 더 긴 폴링 시간이나 더 짧은 폴링 시간이 필요한 경우 *SMCoreServiceHost.exe.config* 파일에서 *CloneSplitStatusCheckPollTime* 매개변수 값을 변경하여 SMCore가 복제본 분할 작업의 상태를 폴링하는 시간 간격을 설정할 수 있습니다. 값은 밀리초이고 기본값은 5분입니다.

예를 들어:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

백업, 복원 또는 다른 클론 분할이 진행 중이면 클론 분할 시작 작업이 실패합니다. 실행 중인 작업이 완료된 후에만 복제 분할 작업을 다시 시작해야 합니다.

관련 정보

"SnapCenter 복제 또는 검증이 집계가 존재하지 않아 실패합니다."

SnapCenter 업그레이드 후 PostgreSQL 클러스터 복제본 삭제 또는 분할

SnapCenter 4.3으로 업그레이드한 후에는 더 이상 복제본이 표시되지 않습니다. 복제본이 생성된 리소스의 토폴로지 페이지에서 복제본을 삭제하거나 분할할 수 있습니다.

이 작업에 관하여

숨겨진 복제본의 저장 공간을 찾으려면 다음 명령을 실행하세요. `Get-SmClone -ListStorageFootprint`

단계

1. remove-smbbackup cmdlet을 사용하여 복제된 리소스의 백업을 삭제합니다.
2. remove-smresourcegroup cmdlet을 사용하여 복제된 리소스의 리소스 그룹을 삭제합니다.
3. remove-smprotectresource cmdlet을 사용하여 복제된 리소스의 보호를 제거합니다.
4. 리소스 페이지에서 상위 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

5. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 복제본을 선택합니다.
6. 복제본을 선택한 다음 클릭하세요.  클론을 삭제하거나 클릭하세요.  클론을 분할합니다.
7. *확인*을 클릭합니다.

MySQL 보호

MySQL용 SnapCenter 플러그인

MySQL용 SnapCenter 플러그인 개요

MySQL 데이터베이스용 SnapCenter 플러그인은 NetApp SnapCenter software 의 호스트 측 구성 요소로, MySQL 데이터베이스의 애플리케이션 인식 데이터 보호 관리를 지원합니다. MySQL 데이터베이스용 플러그인은 SnapCenter 환경에서 MySQL 데이터베이스의 백업, 복원 및 복제를 자동화합니다.

SnapCenter 단일 인스턴스 MySQL 설정을 지원합니다. Linux와 Windows 환경 모두에서 MySQL 데이터베이스 플러그인을 사용할 수 있습니다. Windows 환경에서는 MySQL이 수동 리소스로 지원됩니다.

MySQL 데이터베이스용 플러그인이 설치되면 NetApp SnapMirror 기술과 함께 SnapCenter 사용하여 다른 볼륨에 백업 세트의 미러 사본을 만들 수 있습니다. NetApp SnapVault 기술과 함께 플러그인을 사용하면 표준을 준수하기 위해 디스크 간 백업 복제를 수행할 수도 있습니다.

MySQL용 SnapCenter 플러그인은 ONTAP 및 Azure NetApp 파일 스토리지 레이아웃에서 NFS와 SAN을 지원합니다.

VMDK, vVol 및 RDM 가상 스토리지 레이아웃이 지원됩니다.

심볼릭 링크는 지원되지 않습니다.

MySQL용 SnapCenter 플러그인을 사용하여 할 수 있는 일

사용자 환경에 MySQL 데이터베이스용 플러그인을 설치하면 SnapCenter 사용하여 MySQL 인스턴스를 백업, 복원 및 복제할 수 있습니다. 해당 작업을 지원하는 작업도 수행할 수 있습니다.

- 인스턴스를 추가합니다.
- 백업을 만듭니다.
- 백업에서 복원합니다.
- 백업을 복제합니다.
- 백업 작업을 예약합니다.
- 백업, 복원 및 복제 작업을 모니터링합니다.
- 백업, 복원 및 복제 작업에 대한 보고서를 확인합니다.

MySQL용 SnapCenter 플러그인 기능

SnapCenter 플러그인 애플리케이션과 스토리지 시스템의 NetApp 기술과 통합됩니다. MySQL 데이터베이스 플러그인을 사용하려면 SnapCenter 그래픽 사용자 인터페이스를 사용합니다.

- 통합된 그래픽 사용자 인터페이스

SnapCenter 인터페이스는 플러그인과 환경 전반에 걸쳐 표준화와 일관성을 제공합니다. SnapCenter 인터페이스를 사용하면 플러그인 전반에 걸쳐 일관된 백업, 복원 및 복제 작업을 완료하고, 중앙 집중식 보고를 사용하고, 한눈에 볼 수 있는 대시보드 보기를 사용하고, 역할 기반 액세스 제어(RBAC)를 설정하고, 모든 플러그인에서 작업을 모니터링할 수 있습니다.

- 자동화된 중앙 관리

백업 작업을 예약하고, 정책 기반 백업 보존을 구성하고, 복원 작업을 수행할 수 있습니다. SnapCenter 구성하여 이메일 알림을 보내 환경을 사전에 모니터링할 수도 있습니다.

- 비중단 **NetApp** 스냅샷 복사 기술

SnapCenter MySQL 데이터베이스 플러그인과 함께 NetApp 스냅샷 기술을 사용하여 리소스를 백업합니다.

MySQL 플러그인을 사용하면 다음과 같은 이점도 있습니다.

- 백업, 복원 및 복제 워크플로 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임

또한, 권한이 있는 SnapCenter 사용자에게 애플리케이션 수준 권한이 부여되도록 자격 증명을 설정할 수도 있습니다.

- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 리소스의 공간 효율적 및 특정 시점 복사본 생성

복제본을 생성하려는 스토리지 시스템에 FlexClone 라이선스가 필요합니다.

- 백업 생성의 일부로 ONTAP 의 일관성 그룹(CG) 스냅샷 기능에 대한 지원.
- 여러 리소스 호스트에서 동시에 여러 백업을 실행할 수 있는 기능

단일 작업에서 단일 호스트의 리소스가 동일한 볼륨을 공유하는 경우 스냅샷이 통합됩니다.

- 외부 명령을 사용하여 스냅샷을 생성하는 기능.
- XFS 파일 시스템에서 Linux LVM을 지원합니다.

MySQL용 SnapCenter 플러그인이 지원하는 스토리지 유형

SnapCenter 물리적 머신과 가상 머신(VM) 모두에서 다양한 스토리지 유형을 지원합니다. MySQL용 SnapCenter 플러그인을 설치하기 전에 스토리지 유형에 대한 지원을 확인해야 합니다.

기계	저장 유형
물리적 서버	• FC 연결 LUN • iSCSI로 연결된 LUN • NFS 연결 볼륨

기계	저장 유형
VMware ESXi	• FC 또는 iSCSI ESXi HBA로 연결된 RDM LUN 호스트 버스 어댑터(HBA) 스캐닝은 SnapCenter 호스트에 있는 모든 호스트 버스 어댑터를 스캔하기 때문에 완료하는 데 오랜 시간이 걸릴 수 있습니다. <code>_opt/</code> <code>NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config_</code>에 있는 LinuxConfig.pm 파일을 편집하여 SCSI_HOSTS_OPTIMIZED_RESCAN 매개변수 값을 1로 설정하면 HBA_DRIVER_NAMES에 나열된 HBA만 다시 스캔합니다. • iSCSI 이니시에이터에 의해 게스트 시스템에 직접 연결된 iSCSI LUN • NFS 데이터 저장소의 VMDK • VMFS에 VMDK가 생성됨 • 게스트 시스템에 직접 연결된 NFS 볼륨 • NFS와 SAN 모두에 있는 vVol 데이터 저장소 vVol 데이터스토어는 VMware vSphere용 ONTAP 도구를 사용해서만 프로비저닝할 수 있습니다.

MySQL 플러그인에 필요한 최소 ONTAP 권한

데이터 보호를 위해 사용하는 SnapCenter 플러그인에 따라 필요한 최소 ONTAP 권한은 다릅니다.

- 모든 액세스 명령: ONTAP 9.12.1 이상에 필요한 최소 권한
 - 이벤트 생성-자동 지원-로그
 - 작업 이력 표시
 - 작업 중지
 - 룰
 - lun 생성
 - lun 생성
 - lun 생성
 - lun 삭제
 - lun igroup 추가
 - lun igroup 생성
 - lun igroup 삭제

- lun igroup 이름 바꾸기
- lun igroup 이름 바꾸기
- 룬 아이그룹 쇼
- lun 매핑 add-reporting-nodes
- lun 매핑 생성
- LUN 매핑 삭제
- LUN 매핑 제거-보고-노드
- lun 매핑 쇼
- lun 수정
- lun 이동량
- lun 오프라인
- lun 온라인
- lun 지속적 예약 지우기
- lun 크기 조정
- lun 시리얼
- 룬 쇼
- 스냅미러 정책 추가 규칙
- 스냅미러 정책 수정 규칙
- 스냅미러 정책 제거 규칙
- 스냅미러 정책 보기
- 스냅미러 복원
- 스냅미러 쇼
- 스냅미러 쇼 히스토리
- 스냅미러 업데이트
- 스냅미러 업데이트-ls-세트
- 스냅미러 목록-대상
- 버전
- 볼륨 복제 생성
- 볼륨 클론 쇼
- 볼륨 복제 분할 시작
- 볼륨 클론 분할 정지
- 볼륨 생성
- 볼륨 파괴
- 볼륨 파일 복제 생성

- 볼륨 파일 show-disk-usage
- 볼륨 오프라인
- 온라인 볼륨
- 볼륨 수정
- 볼륨 qtree 생성
- 볼륨 qtree 삭제
- 볼륨 qtree 수정
- 볼륨 qtree 쇼
- 볼륨 제한
- 볼륨 쇼
- 볼륨 스냅샷 생성
- 볼륨 스냅샷 삭제
- 볼륨 스냅샷 수정
- 볼륨 스냅샷 수정-스냅락-만료-시간
- 볼륨 스냅샷 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- vservers cifs
- vservers cifs 공유 생성
- vservers cifs 공유 삭제
- vservers cifs 새도우 카피 쇼
- vservers cifs 공유 표시
- vservers cifs 쇼
- vservers 내보내기 정책
- vservers 내보내기 정책 생성
- vservers 내보내기 정책 삭제
- vservers 내보내기 정책 규칙 생성
- vservers 내보내기 정책 규칙 표시
- vservers 내보내기 정책 표시
- v서버 iSCSI
- vservers iscsi 연결 표시
- vservers 쇼

- 읽기 전용 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
 - 네트워크 인터페이스
 - 네트워크 인터페이스 표시
 - v서버

MySQL을 위한 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비

ONTAP SnapMirror 기술과 함께 SnapCenter 플러그인을 사용하면 다른 볼륨에 백업 세트의 미러 사본을 생성할 수 있으며, ONTAP SnapVault 기술과 함께 사용하면 표준 준수 및 기타 거버넌스 관련 목적으로 디스크 간 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 구성하고 해당 관계를 초기화해야 합니다.

SnapCenter 스냅샷 작업을 완료한 후 SnapMirror와 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행되므로 별도의 ONTAP 일정을 만들지 마세요.



NetApp SnapManager 제품을 통해 SnapCenter에 접속했고 구성된 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 기본 저장소(소스 볼륨)의 데이터를 보조 저장소(대상 볼륨)로 복제합니다. 관계를 초기화하면 ONTAP 소스 볼륨에서 참조되는 데이터 블록을 대상 볼륨으로 전송합니다.



SnapCenter SnapMirror와 SnapVault 볼륨 간의 계단식 관계(**Primary > Mirror > Vault**)를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter 버전에 따라 유연한 SnapMirror 관계 관리를 지원합니다. 버전에 따라 유연한 SnapMirror 관계와 이를 설정하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["ONTAP 문서"](#).

MySQL 백업 전략

MySQL에 대한 백업 전략 정의

백업 작업을 생성하기 전에 백업 전략을 정의하면 리소스를 성공적으로 복원하거나 복제하는 데 필요한 백업을 확보하는 데 도움이 됩니다. 백업 전략은 주로 서비스 수준 계약(SLA), 복구 시간 목표(RTO), 복구 지점 목표(RPO)에 따라 결정됩니다.

이 작업에 관하여

SLA는 기대되는 서비스 수준을 정의하고 서비스의 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RTO는 서비스가 중단된 후 비즈니스 프로세스를 복구해야 하는 시간입니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 기간에 대한 전략을 정의합니다. SLA, RTO, RPO는 데이터 보호 전략에 기여합니다.

단계

1. 리소스를 백업해야 하는 시기를 결정하세요.
2. 필요한 백업 작업의 수를 결정합니다.
3. 백업의 이름을 어떻게 지을지 결정하세요.

4. 데이터베이스의 애플리케이션 일관성 스냅샷을 백업하기 위해 스냅샷 복사 기반 정책을 생성할지 여부를 결정합니다.
5. 복제를 위해 NetApp SnapMirror 기술을 사용할지, 장기 보존을 위해 NetApp SnapVault 기술을 사용할지 결정하세요.
6. 소스 스토리지 시스템과 SnapMirror 대상의 스냅샷 보존 기간을 결정합니다.
7. 백업 작업 전이나 후에 명령을 실행할지 여부를 결정하고 사전 스크립트나 사후 스크립트를 제공합니다.

Linux 호스트에서 리소스 자동 검색

리소스는 SnapCenter 에서 관리하는 Linux 호스트의 MySQL 인스턴스입니다. MySQL 플러그인용 SnapCenter 플러그인을 설치하면 해당 Linux 호스트의 MySQL 인스턴스가 자동으로 검색되어 리소스 페이지에 표시됩니다.

지원되는 백업 유형

백업 유형은 생성하려는 백업 유형을 지정합니다. SnapCenter MySQL 데이터베이스에 대한 스냅샷 복사 기반 백업 유형을 지원합니다.

스냅샷 복사 기반 백업

스냅샷 복사 기반 백업은 NetApp 스냅샷 기술을 활용하여 MySQL 데이터베이스가 있는 볼륨의 온라인, 읽기 전용 복사본을 만듭니다.

MySQL용 SnapCenter 플러그인이 일관성 그룹 스냅샷을 사용하는 방법

플러그인을 사용하면 리소스 그룹에 대한 일관성 그룹 스냅샷을 만들 수 있습니다. 일관성 그룹은 여러 볼륨을 수용하여 하나의 엔티티로 관리할 수 있는 컨테이너입니다. 일관성 그룹은 여러 볼륨의 동시 스냅샷으로, 볼륨 그룹의 일관된 복사본을 제공합니다.

또한 스토리지 컨트롤러가 스냅샷을 일관되게 그룹화하는 데 걸리는 대기 시간을 지정할 수도 있습니다. 이용 가능한 대기 시간 옵션은 긴급, 보통, *느긋함*입니다. 일관된 그룹 스냅샷 작업 중에 WAFL(Write Anywhere File Layout) 동기화를 활성화하거나 비활성화할 수도 있습니다. WAFL 동기화는 일관성 그룹 스냅샷의 성능을 향상시킵니다.

SnapCenter 로그 백업의 정리 작업을 관리하는 방법

SnapCenter 스토리지 시스템 및 파일 시스템 수준에서 데이터 백업의 정리 작업을 관리합니다.

MySQL 백업 일정을 결정하기 위한 고려 사항

백업 일정을 결정하는 가장 중요한 요소는 리소스의 변화율입니다. 자주 사용되는 리소스는 매시간 백업하고, 거의 사용되지 않는 리소스는 하루에 한 번 백업할 수도 있습니다. 기타 요소로는 조직에 대한 리소스의 중요성, 서비스 수준 계약(SLA), 복구 지점 목표(RPO) 등이 있습니다.

백업 일정은 다음과 같이 두 부분으로 구성됩니다.

- 백업 빈도(백업을 수행할 빈도)

일부 플러그인의 경우 일정 유형이라고도 하는 백업 빈도는 정책 구성의 일부입니다. 예를 들어, 백업 빈도를 매시간, 매일, 매주 또는 매월로 구성할 수 있습니다.

- 백업 일정(백업을 수행할 정확한 시기)

백업 일정은 리소스 또는 리소스 그룹 구성의 일부입니다. 예를 들어, 주간 백업을 위해 구성된 정책이 있는 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 일정을 구성할 수 있습니다.

MySQL에 필요한 백업 작업 수

필요한 백업 작업 수를 결정하는 요소에는 리소스 크기, 사용된 볼륨 수, 리소스 변경률, 서비스 수준 계약(SLA) 등이 있습니다.

MySQL 데이터베이스용 플러그인에 대한 백업 명명 규칙

기본 스냅샷 명명 규칙을 사용하거나 사용자 지정 명명 규칙을 사용할 수 있습니다. 기본 백업 명명 규칙은 스냅샷 이름에 타임스탬프를 추가하여 복사본이 생성된 시기를 식별하는 데 도움이 됩니다.

스냅샷은 다음과 같은 기본 명명 규칙을 사용합니다.

`resourcegroupname_hostname_timestamp`

다음 예와 같이 논리적으로 백업 리소스 그룹의 이름을 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예에서 구문 요소는 다음과 같은 의미를 갖습니다.

- `_dts1_`은 리소스 그룹 이름입니다.
- `_mach1x88_`은 호스트 이름입니다.
- `_03-12-2015_23.17.26_`은 날짜와 타임스탬프입니다.

또는, *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택하여 리소스나 리소스 그룹을 보호하는 동안 스냅샷 이름 형식을 지정할 수 있습니다. 예를 들어, `customtext_resourcegroup_policy_hostname` 또는 `resourcegroup_hostname`입니다. 기본적으로 타임스탬프 접미사는 스냅샷 이름에 추가됩니다.

MySQL에 대한 복원 및 복구 전략

MySQL 리소스에 대한 복원 및 복구 전략 정의

데이터베이스를 복원하고 복구하기 전에 전략을 정의해야 복원 및 복구 작업을 성공적으로 수행할 수 있습니다.



데이터베이스의 수동 복구만 지원됩니다.

단계

1. 수동으로 추가된 MySQL 리소스에 대해 지원되는 복원 전략을 확인합니다.
2. 자동 검색된 MySQL 데이터베이스에 지원되는 복원 전략을 확인합니다.
3. 수행할 복구 작업 유형을 결정합니다.

수동으로 추가된 **MySQL** 리소스에 대해 지원되는 복원 전략 유형

SnapCenter 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다. 수동으로 추가된 MySQL 리소스에는 두 가지 유형의 복원 전략이 있습니다.



수동으로 추가한 MySQL 리소스는 복구할 수 없습니다.

리소스 복구 완료

- 리소스의 모든 볼륨, Qtree 및 LUN을 복원합니다.



리소스에 볼륨이나 Q트리가 포함되어 있는 경우 해당 볼륨이나 Q트리에서 복원을 위해 선택한 스냅샷 이후에 촬영된 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 동일한 볼륨이나 Q트리에 다른 리소스가 호스팅되는 경우 해당 리소스도 삭제됩니다.

자동으로 검색된 **MySQL**에 지원되는 복원 전략 유형

SnapCenter 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다.

전체 리소스 복원은 자동으로 검색된 MySQL 데이터베이스에 지원되는 복원 전략입니다. 이렇게 하면 리소스의 모든 볼륨, Q트리, LUN이 복원됩니다.

자동 검색된 **MySQL**에 대한 복원 작업 유형

MySQL용 SnapCenter 플러그인은 단일 파일 SnapRestore 와 자동으로 검색된 MySQL 데이터베이스에 대한 연결 및 복사 복원 유형을 지원합니다.

단일 파일 **SnapRestore** 다음 시나리오에 대해 **NFS** 환경에서 수행됩니다.

- 전체 리소스 옵션만 선택된 경우
- 선택한 백업이 SnapMirror 또는 SnapVault 보조 위치에서 시작되고 전체 리소스 옵션이 선택된 경우

단일 파일 **SnapRestore** 다음 시나리오에 대해 **SAN** 환경에서 수행됩니다.

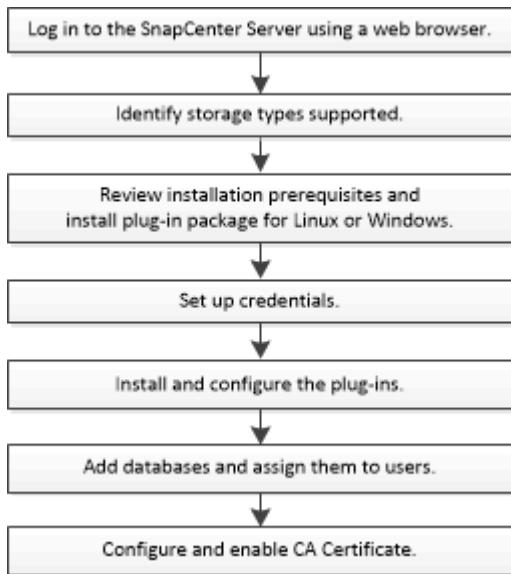
- 전체 리소스 옵션만 선택된 경우
- SnapMirror 또는 SnapVault 보조 위치에서 백업을 선택하고 전체 리소스 옵션을 선택한 경우

MySQL용 SnapCenter 플러그인 설치 준비

MySQL용 SnapCenter 플러그인 설치 워크플로

MySQL 데이터베이스를 보호하려면 MySQL용 SnapCenter 플러그인을 설치하고 설정해야

합니다.



MySQL용 SnapCenter 플러그인을 설치하고 호스트를 추가하기 위한 전제 조건

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 충족해야 합니다. MySQL용 SnapCenter 플러그인은 Windows와 Linux 환경에서 모두 사용할 수 있습니다.

- 호스트에 Java 11을 설치했어야 합니다.



IBM Java는 Windows 및 Linux 호스트에서 지원되지 않습니다.

- Windows의 경우 플러그인 생성 서비스는 “LocalSystem” Windows 사용자를 사용하여 실행해야 합니다. 이는 플러그인 for MySQL을 도메인 관리자로 설치한 경우의 기본 동작입니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에 속하는 경우 호스트에서 UAC를 비활성화해야 합니다. Microsoft Windows용 SnapCenter 플러그인은 기본적으로 Windows 호스트의 MySQL 플러그인과 함께 배포됩니다.
- SnapCenter 서버는 MySQL 호스트용 플러그인의 8145 또는 사용자 정의 포트에 액세스할 수 있어야 합니다.
- MySQL 5.7의 경우 binlog는 mysql 설정(my.cnf 또는 mysql-server.cnf) 파일에 지정되어야 합니다.

Windows 호스트

- 원격 호스트에 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 도메인 사용자가 있어야 합니다.
- Windows 호스트에 MySQL 플러그인을 설치하는 동안 Microsoft Windows용 SnapCenter 플러그인이 자동으로 설치됩니다.
- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.
- Windows 호스트에 Java 11을 설치했어야 합니다.

["모든 운영 체제용 JAVA 다운로드"](#)

["NetApp 상호 운용성 매트릭스 도구"](#)

리눅스 호스트

- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.
- Linux 호스트에 Java 11을 설치했어야 합니다.

"모든 운영 체제용 JAVA 다운로드"

"NetApp 상호 운용성 매트릭스 도구"

- Linux 호스트에서 실행되는 MySQL 데이터베이스의 경우 MySQL용 플러그인을 설치하는 동안 UNIX용 SnapCenter 플러그인이 자동으로 설치됩니다.
- 플러그인 설치를 위해 기본 셸로 `*bash*`를 사용해야 합니다.

보충 명령

MySQL용 SnapCenter 플러그인에서 보충 명령을 실행하려면 `allowed_commands.config` 파일에 해당 명령을 포함해야 합니다.

- Windows 호스트의 기본 위치: `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux 호스트의 기본 위치: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`

플러그인 호스트에서 추가 명령을 허용하려면 편집기에서 `allowed_commands.config` 파일을 엽니다. 각 명령을 별도의 줄에 입력하세요. 명령은 대소문자를 구분하지 않습니다. 완전히 정규화된 경로 이름을 지정하고, 경로 이름에 공백이 포함된 경우 따옴표(")로 묶으세요.

예를 들어:

명령: mount 명령: umount 명령: "C:\Program Files\ NetApp\SnapCreator commands\sdcli.exe" 명령: myscript.bat

`allowed_commands.config` 파일이 없으면 명령이나 스크립트 실행이 차단되고 다음 오류와 함께 워크플로가 실패합니다.

"[/mnt/mount -a] 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여합니다."

`_allowed_commands.config`에 명령이나 스크립트가 없으면 명령이나 스크립트 실행이 차단되고 다음 오류와 함께 워크플로가 실패합니다.

"[/mnt/mount -a] 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여합니다."



모든 명령을 허용하려면 와일드카드 항목(*)을 사용해서는 안 됩니다.

Linux 호스트에 대한 루트가 아닌 사용자에게 대한 **sudo** 권한 구성

SnapCenter 사용하면 루트가 아닌 사용자도 Linux용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 루트가 아닌 사용자로 실행됩니다. 루트가 아닌 사용자에게 여러 경로에 대한 액세스 권한을 제공하려면 `sudo` 권한을 구성해야 합니다.

필요한 것

- Sudo 버전 1.8.7 이상.
- umask가 0027인 경우, java 폴더와 그 안에 있는 모든 파일에 555 권한이 있어야 합니다. 그렇지 않으면 플러그인 설치가 실패할 수 있습니다.
- 루트가 아닌 사용자의 경우 루트가 아닌 사용자의 이름과 사용자 그룹이 동일해야 합니다.
- `/etc/ssh/sshd_config` 파일을 편집하여 메시지 인증 코드 알고리즘(MAC hmac-sha2-256 및 MAC hmac-sha2-512)을 구성합니다.

구성 파일을 업데이트한 후 sshd 서비스를 다시 시작합니다.

예:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

이 작업에 관하여

루트가 아닌 사용자에게 다음 경로에 대한 액세스를 제공하려면 sudo 권한을 구성해야 합니다.

- `/home/LINUX_USER/sc_netapp/snapcenter_linux_host_plugin.bin`
- `/custom_location/ NetApp/snapcenter/spl/설치/플러그인/제거`
- `/custom_location/ NetApp/snapcenter/spl/bin/spl`

단계

1. Linux용 SnapCenter 플러그인 패키지를 설치하려는 Linux 호스트에 로그인합니다.
2. visudo Linux 유틸리티를 사용하여 `/etc/sudoers` 파일에 다음 줄을 추가합니다.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
_LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
_LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
_LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



RAC 설정을 사용하는 경우 허용되는 다른 명령과 함께 다음을 /etc/sudoers 파일에 추가해야 합니다. '<crs_home>/bin/olsnodes'

*crs_home*의 값은 */etc/oracle/olr.loc* 파일에서 얻을 수 있습니다.

*_LINUX_USER*는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

*_checksum_value*는 **sc_unix_plugins_checksum.txt** 파일에서 얻을 수 있습니다. 이 파일의 위치는 다음과 같습니다.

- SnapCenter 서버가 Windows 호스트에 설치된 경우 *_C:\ProgramData\ NetApp\ SnapCenter \Package Repository\sc_unix_plugins_checksum.txt _*
- *_/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ SnapCenter* 서버가 Linux 호스트에 설치된 경우.



이 예제는 귀하만의 데이터를 생성하기 위한 참고자료로만 사용해야 합니다.

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항과 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	마이크로소프트 윈도우 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구".
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	• ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 • 파워셀 코어 7.4.2 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구".

Linux용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 및 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	• 레드햇 엔터프라이즈 리눅스 • SUSE Linux Enterprise Server(SLES) 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구".
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB

목	요구 사항
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	Java 11 Oracle Java 및 OpenJDK JAVA를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties에 있는 JAVA_HOME 옵션이 올바른 JAVA 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다. 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구".

MySQL용 SnapCenter 플러그인에 대한 자격 증명 설정

SnapCenter SnapCenter 작업을 위해 사용자를 인증하기 위해 자격 증명을 사용합니다. SnapCenter 플러그인을 설치하기 위한 자격 증명과 데이터베이스나 Windows 파일 시스템에서 데이터 보호 작업을 수행하기 위한 추가 자격 증명을 만들어야 합니다.

이 작업에 관하여

- 리눅스 호스트

Linux 호스트에 플러그인을 설치하려면 자격 증명을 설정해야 합니다.

플러그인 프로세스를 설치하고 시작하려면 루트 사용자 또는 sudo 권한이 있는 루트가 아닌 사용자의 자격 증명을 설정해야 합니다.

모범 사례: 호스트를 배포하고 플러그인을 설치한 후에도 Linux에 대한 자격 증명을 생성할 수 있지만, 가장 좋은 방법은 호스트를 배포하고 플러그인을 설치하기 전에 SVM을 추가한 후에 자격 증명을 생성하는 것입니다.

- Windows 호스트

플러그인을 설치하기 전에 Windows 자격 증명을 설정해야 합니다.

원격 호스트의 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정해야 합니다.

개별 리소스 그룹에 대한 자격 증명을 설정하고 사용자 이름에 전체 관리자 권한이 없는 경우 최소한 리소스 그룹 및 백업 권한을 사용자 이름에 할당해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *자격 증명*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 자격 증명 페이지에서 자격 증명을 구성하는 데 필요한 정보를 지정합니다.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.
사용자 이름	인증에 사용할 사용자 이름과 비밀번호를 입력하세요. • 도메인 관리자 또는 관리자 그룹의 모든 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹 구성원을 지정하세요. 사용자 이름 필드에 사용할 수 있는 형식은 다음과 같습니다. ◦ <i>NetBIOS</i> 사용자 이름 ◦ 도메인 <i>FQDN</i> 사용자 이름 • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우, SnapCenter 플러그인을 설치할 시스템에 기본 제공되는 로컬 관리자를 지정하십시오. 사용자 계정에 승격된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우, 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다. <i>UserName</i> 비밀번호에 큰따옴표(")나 백틱(`)을 사용하지 마세요. 비밀번호에 '<' 기호와 '!' 기호를 함께 사용하면 안 됩니다. 예를 들어, lessthan<!10, lessthan10<!, backtick`12.
비밀번호	인증에 사용되는 비밀번호를 입력하세요.
인증 모드	사용할 인증 모드를 선택하세요.
sudo 권한을 사용하세요	루트가 아닌 사용자에게 자격 증명을 생성하는 경우 sudo 권한 사용 확인란을 선택합니다.  Linux 사용자에게만 적용됩니다.

5. *확인*을 클릭합니다.

자격 증명 설정을 마친 후 사용자 및 액세스 페이지에서 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

MySQL용 SnapCenter 플러그인 설치

원격 호스트에 호스트를 추가하고 플러그인 패키지를 설치합니다.

SnapCenter 호스트 추가 페이지를 사용하여 호스트를 추가한 다음 플러그인 패키지를 설치해야 합니다. 플러그인은 원격 호스트에 자동으로 설치됩니다. 개별 호스트에 대한 호스트를 추가하고 플러그인 패키지를 설치할 수 있습니다.

시작하기 전에

- SnapCenter 서버 호스트의 운영 체제가 Windows 2019이고 플러그인 호스트의 운영 체제가 Windows 2022인 경우 다음을 수행해야 합니다.
 - Windows Server 2019(OS 빌드 17763.5936) 이상으로 업그레이드하세요.
 - Windows Server 2022(OS 빌드 20348.2402) 이상으로 업그레이드하세요.
- SnapCenter 관리자 역할과 같이 플러그인 설치 및 제거 권한이 있는 역할에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.
- 메시지 대기열 서비스가 실행 중인지 확인해야 합니다.
- 관리 문서에는 호스트 관리에 대한 정보가 포함되어 있습니다.

이 작업에 관하여

- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 상단에 관리되는 호스트 탭이 선택되어 있는지 확인하세요.
3. *추가*를 클릭하세요.
4. 호스트 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
호스트 유형	호스트 유형을 선택하세요: • Windows • 리눅스  MySQL 플러그인은 MySQL 데이터베이스 서버에 설치해야 합니다.

이 분야에서는...	이렇게 하세요...
호스트 이름	통신 호스트 이름을 입력하세요. 호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하세요. SnapCenter DNS의 적절한 구성에 달려 있습니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다.
신임장	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성하세요. 자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하세요. 제공한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다.  자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

REST API를 사용하여 MySQL 플러그인을 설치하는 경우 버전을 3.0으로 전달해야 합니다. 예를 들어, MySQL:3.0

6. (선택 사항) *추가 옵션*을 클릭합니다.

이 분야에서는...	이렇게 하세요...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정하세요. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트로 표시됩니다.  플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.
설치 경로	MySQL 플러그인은 MySQL 클라이언트 호스트에 설치되며, 이 호스트는 Windows 시스템이나 Linux 시스템에 있을 수 있습니다. - Windows용 SnapCenter 플러그인 패키지의 경우 기본 경로는 C:\Program Files\ NetApp\ SnapCenter 입니다. 선택적으로 경로를 사용자 정의할 수 있습니다. - Linux용 SnapCenter 플러그인 패키지의 경우 기본 경로는 /opt/ NetApp/snapcenter입니다. 선택적으로 경로를 사용자 정의할 수 있습니다.

이 분야에서는...	이렇게 하세요...
사전 설치 확인 건너뛰기	플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택하세요.
클러스터의 모든 호스트를 추가합니다.	해당 없음.
플러그인 서비스를 실행하려면 그룹 관리 서비스 계정(gMSA)을 사용하세요.	해당 없음.

7. *제출*을 클릭하세요.

"사전 검사 건너뛰기" 확인란을 선택하지 않은 경우, 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 호스트의 유효성 검사가 수행됩니다. 디스크 공간, RAM, PowerShell 버전, .NET 버전, 위치(Windows 플러그인의 경우), Java 버전(Linux 플러그인의 경우)이 최소 요구 사항을 충족하는지 검증됩니다. 최소 요구 사항을 충족하지 못하면 해당 오류 또는 경고 메시지가 표시됩니다.

오류가 디스크 공간이나 RAM과 관련된 경우 C:\Program Files\ NetApp\ SnapCenter WebApp에 있는 web.config 파일을 업데이트하여 기본값을 수정할 수 있습니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.



HA 설정에서 web.config 파일을 업데이트하는 경우 두 노드에서 모두 파일을 업데이트해야 합니다.

8. 호스트 유형이 Linux인 경우 지문을 확인한 다음 *확인 및 제출*을 클릭합니다.

클러스터 설정에서는 클러스터의 각 노드의 지문을 확인해야 합니다.



동일한 호스트가 이전에 SnapCenter 에 추가되었고 지문이 확인된 경우에도 지문 확인은 필수입니다.

9. 설치 진행 상황을 모니터링합니다.

- Windows 플러그인의 경우 설치 및 업그레이드 로그는 다음 위치에 있습니다. C:\Windows\ SnapCenter plugin\Install<JOBID>_
- Linux 플러그인의 경우 설치 로그는 /var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log_에 있고 업그레이드 로그는 /var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade<JOBID>.log_에 있습니다.

당신이 완료한 후

SnapCenter 6.0 버전으로 업그레이드하려는 경우, 기존 PERL 기반 MySQL 플러그인이 원격 플러그인 서버에서 제거됩니다.

cmdlet을 사용하여 여러 원격 호스트에 **Linux** 또는 **Windows**용 **SnapCenter** 플러그인 패키지 설치

Install-SmHostPackage PowerShell cmdlet을 사용하여 Linux 또는 Windows용 SnapCenter 플러그인 패키지를 여러 호스트에 동시에 설치할 수 있습니다.

시작하기 전에

플러그인 패키지를 설치하려는 각 호스트에서 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter 에 로그인해야 합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 Open-SmConnection cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
3. Install-SmHostPackage cmdlet과 필요한 매개변수를 사용하여 여러 호스트에 플러그인을 설치합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_` 을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려는 경우 `-skipprecheck` 옵션을 사용할 수 있습니다.

4. 원격 설치를 위한 자격 증명을 입력하세요.

명령줄 인터페이스를 사용하여 **Linux** 호스트에 **MySQL**용 **SnapCenter** 플러그인을 설치합니다.

SnapCenter 사용자 인터페이스(UI)를 사용하여 MySQL 데이터베이스용 SnapCenter 플러그인을 설치해야 합니다. 사용자 환경에서 SnapCenter UI에서 플러그인을 원격으로 설치할 수 없는 경우 명령줄 인터페이스(CLI)를 사용하여 콘솔 모드나 자동 모드로 MySQL 데이터베이스용 플러그인을 설치할 수 있습니다.

시작하기 전에

- MySQL 인스턴스를 보호해야 하는 각 Linux 호스트에 MySQL 데이터베이스용 플러그인을 설치해야 합니다.
- MySQL 데이터베이스용 SnapCenter 플러그인을 설치하는 Linux 호스트는 종속 소프트웨어, 데이터베이스 및 운영 체제 요구 사항을 충족해야 합니다.

상호 운용성 매트릭스 도구(IMT)에는 지원되는 구성에 대한 최신 정보가 포함되어 있습니다.

"NetApp 상호 운용성 매트릭스 도구"

- MySQL 데이터베이스용 SnapCenter 플러그인은 Linux용 SnapCenter 플러그인 패키지의 일부입니다. Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 Windows 호스트에 SnapCenter 이미 설치되어 있어야 합니다.

단계

1. Linux용 SnapCenter 플러그인 패키지 설치 파일(snapcenter_linux_host_plugin.bin)을 C:\ProgramData\NetApp\ SnapCenter\Package Repository에서 MySQL용 플러그인을 설치하려는 호스트로 복사합니다.

SnapCenter 서버가 설치된 호스트에서 이 경로에 액세스할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 복사한 디렉토리로 이동합니다.
3. 플러그인을 설치하세요: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`
 - -DPORT는 SMCORE HTTPS 통신 포트를 지정합니다.

- -DSERVER_IP는 SnapCenter 서버 IP 주소를 지정합니다.
- -DSERVER_HTTPS_PORT는 SnapCenter 서버 HTTPS 포트를 지정합니다.
- -DUSER_INSTALL_DIR은 Linux용 SnapCenter 플러그인 패키지를 설치할 디렉토리를 지정합니다.
- DINSTALL_LOG_NAME은 로그 파일의 이름을 지정합니다.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. /<설치 디렉토리>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties 파일을 편집한 다음 PLUGINS_ENABLED = MySQL:3.0 매개변수를 추가합니다.
5. Add-Smhost cmdlet과 필요한 매개변수를 사용하여 SnapCenter 서버에 호스트를 추가합니다.

명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_` 을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

MySQL 플러그인 설치 상태 모니터링

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행 상황을 모니터링할 수 있습니다. 설치가 완료되었는지 또는 문제가 있는지 확인하기 위해 설치 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 플러그인 설치 작업만 나열되도록 목록을 필터링하려면 다음을 수행합니다.
 - a. *필터*를 클릭하세요.
 - b. 선택 사항: 시작 날짜와 종료 날짜를 지정합니다.
 - c. 유형 드롭다운 메뉴에서 *플러그인 설치*를 선택합니다.

- d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
 - e. *적용*을 클릭하세요.
4. 설치 작업을 선택하고 *세부정보*를 클릭하면 작업 세부정보를 볼 수 있습니다.
 5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

CA 인증서 구성

CA 인증서 CSR 파일 생성

인증서 서명 요청(CSR)을 생성하고, 생성된 CSR을 사용하여 인증 기관(CA)에서 얻을 수 있는 인증서를 가져올 수 있습니다. 인증서에는 개인 키가 연결됩니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.



CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 정보는 다음을 참조하세요. "[CA 인증서 CSR 파일을 생성하는 방법](#)".



도메인(*.domain.company.com)이나 시스템(machine1.domain.company.com)에 대한 CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN)과 해당 호스트 이름을 CA 인증서에 명시해야 합니다. 인증서를 구매하기 전에 주체 대체 이름(SAN) 필드를 입력하여 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(*.domain.company.com)의 경우 인증서에는 해당 도메인의 모든 호스트 이름이 암묵적으로 포함됩니다.

CA 인증서 가져오기

Microsoft 관리 콘솔(MMC)을 사용하여 CA 인증서를 SnapCenter 서버와 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.
2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
3. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > *인증서*를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 버튼으로 클릭한 다음, 모든 작업 > *가져오기*를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
개인 키 가져오기	예 옵션을 선택하고 개인 키를 가져온 후 *다음*을 클릭합니다.

이 마법사 창에서...	다음을 수행하세요...
가져오기 파일 형식	변경하지 마세요. *다음*을 클릭하세요.
보안	내보낸 인증서에 사용할 새 비밀번호를 지정한 후 *다음*을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.



인증서 가져오기는 개인 키와 함께 제공되어야 합니다(지원되는 형식: *.pfx, *.p12, *.p7b).

7. "개인" 폴더에 대해서도 5단계를 반복합니다.

CA 인증서 지문을 받으세요

인증서 지문은 인증서를 식별하는 16진수 문자열입니다. 지문은 지문 알고리즘을 사용하여 인증서 내용으로부터 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.

- 인증서를 두 번 클릭합니다.
- 인증서 대화 상자에서 세부정보 탭을 클릭합니다.
- 필드 목록을 스크롤하여 *지문*을 클릭하세요.
- 상자에서 16진수 문자를 복사하세요.
- 16진수 사이의 공백을 제거하세요.

예를 들어, 지문이 "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b"인 경우 공백을 제거하면 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.

- 다음 명령을 실행하여 설치된 인증서의 지문을 나열하고 주체 이름으로 최근에 설치된 인증서를 식별합니다.

`Get-ChildItem -경로 인증서:\LocalMachine\My`

- 지문을 복사하세요.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스로 CA 인증서를 구성해야 합니다.

SnapCenter 서버와 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하는 기존 인증서 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

예를 들어:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스에 바인딩합니다.

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:_{SMCore Port}_ certhash=$cert
appid="$guid"
```

예를 들어:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:_{SMCore Port}_ certhash=$cert
appid="$guid"
```

Linux 호스트에서 SnapCenter MySQL 플러그인 서비스에 대한 CA 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 `_opt/ NetApp/snapcenter/scc/etc_`에 위치한 'keystore.jks' 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 CA 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 'KEYSTORE_PASS' 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

```
keytool -storepasswd -keystore keystore.jks
```

. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.


```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

agent.properties 파일의 KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

3. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 있는 폴더로 이동합니다: /opt/ NetApp/snapcenter/scc/etc.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키스토어 /opt/ NetApp/snapcenter/scc/etc가 포함된 폴더로 이동합니다.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 agent.properties 파일의 KEYSTORE_PASS 키 값입니다.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks
```

. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자("*", ",", ".")가 포함된 경우 별칭 이름을 간단한 이름으로 변경합니다.

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias" -keystore keystore.jks
```

. agent.properties 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

8. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 'opt/ NetApp/snapcenter/scc/etc/crl'입니다.

단계

1. agent.properties 파일에서 기본 디렉토리를 CRL_PATH 키에 맞춰 수정하고 업데이트할 수 있습니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

Windows 호스트에서 **SnapCenter MySQL** 플러그인 서비스에 대한 **CA** 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_에 있는 _keystore.jks 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 **CA** 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 `KEYSTORE_PASS` 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

키툴 -스토어패스워드 -키스토어 키스토어.jks



Windows 명령 프롬프트에서 "keytool" 명령을 인식하지 못하는 경우 keytool 명령을 해당 전체 경로로 바꾸세요.

`C:\Program Files\Java\<jdk_버전>\bin\keytool.exe" -storepasswd -keystore keystore.jks`

3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.

키툴 -키패스워드 -별칭 "인증서의 별칭_이름" -키스토어 키스토어.jks

`agent.properties` 파일의 `KEYSTORE_PASS` 키에 대해서도 동일하게 업데이트합니다.

4. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc`
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

`keytool -list -v -keystore keystore.jks`

4. 루트 또는 중간 인증서를 추가합니다.

`keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks`

5. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc`

2. *keystore.jks* 파일을 찾으세요.

3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
키툴 -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -  
대상키스토어 keystore.jks -대상키스토어 유형 JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.

7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 *agent.properties* 파일의 *KEYSTORE_PASS* 키 값입니다.

```
키툴 -키패스워드 -별칭 "CA_인증서의_별칭_이름" -키스토어 키스토어.jks
```

8. *agent.properties* 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 *SCC_CERTIFICATE_ALIAS* 키에 대해 업데이트합니다.

9. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

SnapCenter 플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- 관련 CA 인증서에 대한 최신 CRL 파일을 다운로드하려면 다음을 참조하세요. "[SnapCenter CA 인증서에서 인증서 해지 목록 파일을 업데이트하는 방법](#)".
- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 *'C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\ etc\crl'* _입니다.

단계

1. *agent.properties* 파일에서 기본 디렉토리를 *CRL_PATH* 키에 맞춰 수정하고 업데이트할 수 있습니다.

2. 이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다.

수신 인증서는 각 CRL에 대해 검증됩니다.

플러그인에 대한 CA 인증서 활성화

CA 인증서를 구성하고 SnapCenter 서버와 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- `Set-SmCertificateSettings` cmdlet을 실행하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- `_Get-SmCertificateSettings_`를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 하나 또는 여러 개의 플러그인 호스트를 선택하세요.
4. *추가 옵션*을 클릭하세요.
5. *인증서 검증 사용*을 선택합니다.

당신이 완료한 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- *  *는 CA 인증서가 활성화되지 않았거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- *  *는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- *  *는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- *  *는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

데이터 보호를 준비하세요

MySQL용 SnapCenter 플러그인을 사용하기 위한 전제 조건

MySQL용 SnapCenter 플러그인을 사용하기 전에 SnapCenter 관리자가 SnapCenter 서버를 설치하고 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다.
- SnapCenter 서버에 로그인합니다.
- 해당되는 경우 스토리지 시스템 연결을 추가하고 자격 증명을 생성하여 SnapCenter 환경을 구성합니다.
- Linux 또는 Windows 호스트에 Java 11을 설치합니다.

호스트 머신의 환경 경로 변수에 Java 경로를 설정해야 합니다.

- 백업 복제가 필요한 경우 SnapMirror와 SnapVault 설정하세요.

MySQL을 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식

SnapCenter 사용하기 전에 수행하려는 백업, 복제 및 복원 작업과 관련된 기본 개념을 이해하는

것이 좋습니다. 다양한 작업을 위해 리소스, 리소스 그룹 및 정책과 상호 작용합니다.

- 리소스는 일반적으로 SnapCenter 사용하여 백업하거나 복제하는 MySQL 인스턴스입니다.
- SnapCenter 리소스 그룹은 호스트의 리소스 모음입니다.

리소스 그룹에서 작업을 수행하면 리소스 그룹에 대해 지정한 일정에 따라 리소스 그룹에 정의된 리소스에서 해당 작업이 수행됩니다.

필요에 따라 단일 리소스나 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 수행할 수도 있습니다.

- 정책은 데이터 보호 작업의 백업 빈도, 복제, 스크립트 및 기타 특성을 지정합니다.

리소스 그룹을 만들 때 해당 그룹에 대한 하나 이상의 정책을 선택합니다. 단일 리소스에 대해 주문형 백업을 수행할 때 정책을 선택할 수도 있습니다.

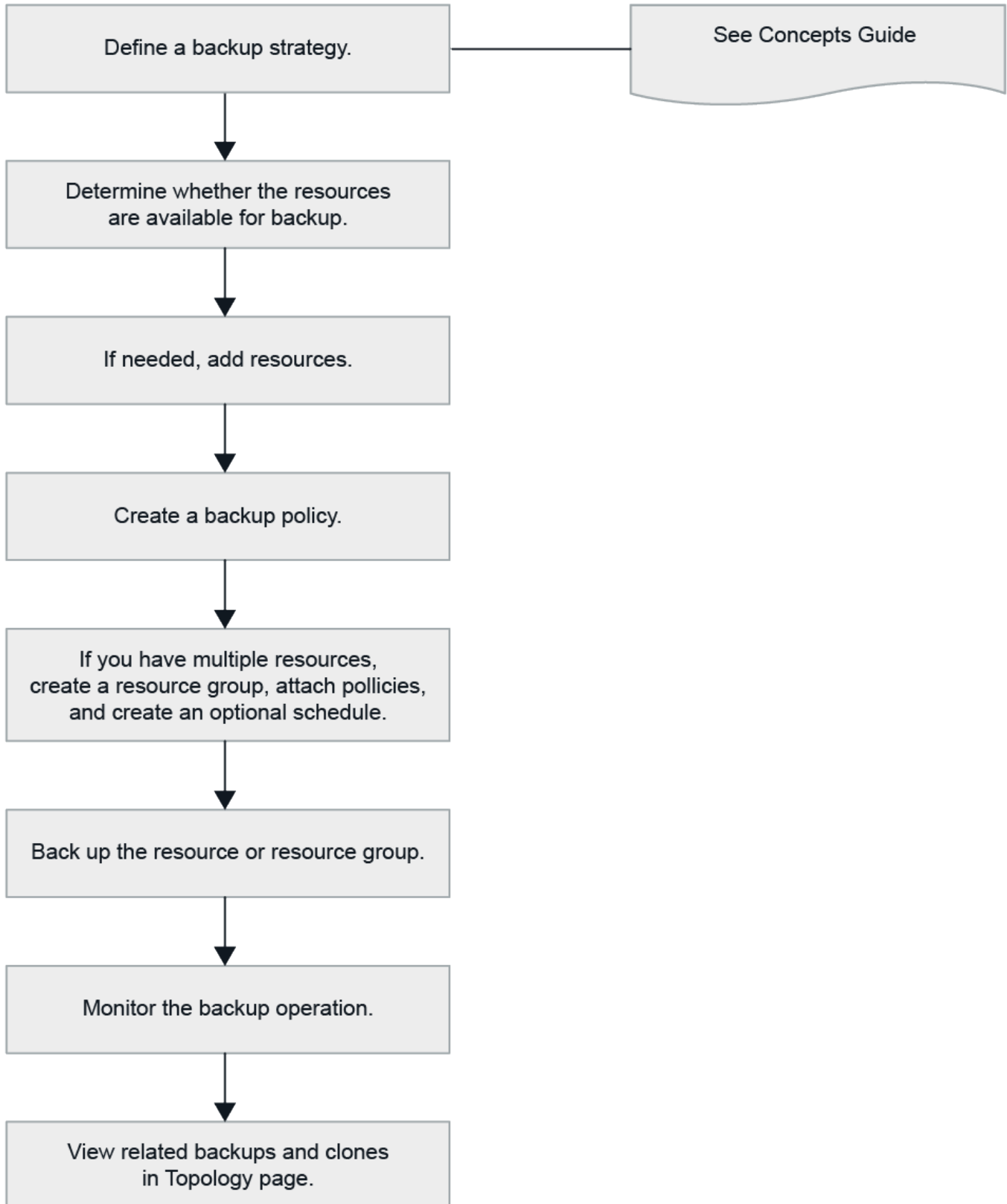
리소스 그룹은 무엇을 보호하고 싶은지, 언제 보호하고 싶은지 날짜와 시간을 정의하는 것으로 생각하면 됩니다. 정책이란 그것을 어떻게 보호할 것인지를 정의하는 것이라고 생각하세요. 예를 들어 모든 데이터베이스를 백업하는 경우 호스트의 모든 데이터베이스를 포함하는 리소스 그룹을 만들 수 있습니다. 그런 다음 리소스 그룹에 일일 정책과 시간별 정책이라는 두 가지 정책을 첨부할 수 있습니다. 리소스 그룹을 만들고 정책을 첨부할 때 리소스 그룹이 매일 전체 백업을 수행하도록 구성할 수 있습니다.

MySQL 리소스 백업

MySQL 리소스 백업

리소스(데이터베이스) 또는 리소스 그룹의 백업을 만들 수 있습니다. 백업 워크플로에는 계획, 백업할 데이터베이스 식별, 백업 정책 관리, 리소스 그룹 생성 및 정책 연결, 백업 생성, 작업 모니터링이 포함됩니다.

다음 워크플로는 백업 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

데이터베이스를 자동으로 검색합니다

리소스는 SnapCenter 에서 관리하는 Linux 호스트의 MySQL 데이터베이스입니다. 사용 가능한 MySQL 데이터베이스를 발견한 후 리소스 그룹에 리소스를 추가하여 데이터 보호 작업을 수행할 수 있습니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 설정 등의 작업을 이미 완료했어야 합니다.
- MySQL용 SnapCenter 플러그인은 RDM/VMDK 가상 환경에 있는 리소스를 자동으로 검색하는 기능을 지원하지 않습니다. 데이터베이스를 수동으로 추가하는 동안 가상 환경에 대한 저장소 정보를 제공해야 합니다.

이 작업에 관하여

- 플러그인을 설치하면 해당 Linux 호스트의 모든 데이터베이스가 자동으로 검색되어 리소스 페이지에 표시됩니다.
- 데이터베이스만 자동으로 검색됩니다.

자동으로 검색된 리소스는 수정하거나 삭제할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 MySQL용 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 리소스 유형을 선택합니다.
3. (선택사항) *를 클릭하세요  *를 선택한 다음 호스트 이름을 선택합니다.

그런 다음 *를 클릭할 수 있습니다.  * 필터 창을 닫습니다.

4. 호스트에서 사용 가능한 리소스를 알아보려면 *리소스 새로 고침*을 클릭하세요.

리소스는 리소스 유형, 호스트 이름, 연관된 리소스 그룹, 백업 유형, 정책 및 전반적인 상태와 같은 정보와 함께 표시됩니다.

- 데이터베이스가 NetApp 스토리지에 있고 보호되지 않은 경우 전체 상태 열에 보호되지 않음이 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되며 백업 작업이 수행되지 않은 경우, 전체 상태 열에 백업이 실행되지 않았습니라는 메시지가 표시됩니다. 그렇지 않으면 마지막 백업 상태에 따라 상태가 백업 실패 또는 백업 성공으로 변경됩니다.



SnapCenter 외부에서 인스턴스 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

플러그인 호스트에 수동으로 리소스 추가

Windows 호스트에서는 자동 검색이 지원되지 않습니다. MySQL 인스턴스와 데이터베이스 리소스를 수동으로 추가해야 합니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 설정 등의 작업을 완료했어야 합니다.

단계

1. 왼쪽 탐색 창에서 드롭다운 목록에서 MySQL용 SnapCenter 플러그인을 선택한 다음 *리소스*를 클릭합니다.

2. 리소스 페이지에서 *MySQL 리소스 추가*를 클릭합니다.
3. 리소스 세부 정보 제공 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	데이터베이스 이름을 지정하세요.
호스트 이름	호스트 이름을 입력하세요.
유형	인스턴스를 선택하세요.
사례	해당 없음.
신임장	자격 증명을 선택하거나 자격 증명에 대한 정보를 추가하세요. 이는 선택 사항입니다.

4. 스토리지 공간 제공 페이지에서 스토리지 유형을 선택하고 하나 이상의 볼륨, LUN, Qtree를 선택한 다음 *저장*을 클릭합니다.

선택 사항: *를 클릭할 수 있습니다.  * 아이콘을 클릭하면 다른 스토리지 시스템에서 볼륨, LUN, Q트리를 추가할 수 있습니다.

5. 선택 사항: 리소스 설정 페이지에서 MySQL 플러그인에 대한 사용자 정의 키-값 쌍을 입력합니다.
6. 요약을 검토한 후 *마침*을 클릭하세요.

호스트 이름, 연관된 리소스 그룹 및 정책, 전반적인 상태와 같은 정보와 함께 데이터베이스가 표시됩니다.

사용자에게 리소스에 대한 액세스 권한을 제공하려면 사용자에게 리소스를 할당해야 합니다. 이를 통해 사용자는 자신에게 할당된 자산에 대해 권한이 있는 작업을 수행할 수 있습니다.

"사용자 또는 그룹을 추가하고 역할과 자산을 할당합니다."

데이터베이스를 추가한 후 MySQL 데이터베이스 세부 정보를 수정할 수 있습니다.

MySQL에 대한 백업 정책 생성

SnapCenter 사용하여 MySQL 리소스를 백업하기 전에 백업하려는 리소스 또는 리소스 그룹에 대한 백업 정책을 만들어야 합니다. 백업 정책은 백업을 관리, 일정을 정하고 보관하는 방법을 규정하는 일련의 규칙입니다.

시작하기 전에

- 백업 전략을 정의했어야 합니다.

자세한 내용은 MySQL 데이터베이스에 대한 데이터 보호 전략 정의에 대한 정보를 참조하세요.

- SnapCenter 설치, 호스트 추가, 스토리지 시스템 연결 설정, 리소스 추가 등의 작업을 완료하여 데이터 보호를 준비했어야 합니다.
- 스냅샷을 미리 또는 볼트에 복제하는 경우 SnapCenter 관리자가 소스 및 대상 볼륨 모두에 대한 SVM을 할당해야 합니다.

또한 정책에서 복제, 스크립트 및 애플리케이션 설정을 지정할 수 있습니다. 이러한 옵션을 사용하면 다른 리소스 그룹에 대한 정책을 재사용할 때 시간을 절약할 수 있습니다.

이 작업에 관하여

- SnapLock
 - '특정 기간 동안 백업 사본을 보관합니다' 옵션을 선택한 경우 SnapLock 보관 기간은 언급된 보관 기간보다 짧거나 같아야 합니다.
 - 스냅샷 잠금 기간을 지정하면 보존 기간이 만료될 때까지 스냅샷이 삭제되지 않습니다. 이로 인해 정책에 지정된 수보다 더 많은 수의 스냅샷을 보관하게 될 수 있습니다.
 - ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *정책*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 이름 페이지에서 정책 이름과 세부 정보를 입력합니다.
5. 정책 유형 페이지에서 다음을 수행합니다.
 - a. 저장 유형을 선택하세요.
 - b. 사용자 정의 백업 설정 섹션에서 플러그인에 키-값 형식으로 전달해야 하는 특정 백업 설정을 제공합니다.

플러그인에 전달할 여러 개의 키-값을 제공할 수 있습니다.

6. 스냅샷 및 복제 페이지에서 다음 단계를 수행합니다.

- a. 주문형, 시간별, 일별, 주별 또는 *월별*을 선택하여 일정 유형을 지정합니다.



리소스 그룹을 생성하는 동안 백업 작업에 대한 일정(시작 날짜, 종료 날짜, 빈도)을 지정할 수 있습니다. 이를 통해 동일한 정책과 백업 빈도를 공유하는 리소스 그룹을 만들 수 있지만, 각 정책에 다른 백업 일정을 할당할 수도 있습니다.



오전 2시로 예약한 경우, 일광 절약 시간제(DST) 기간에는 일정이 실행되지 않습니다.

- a. 스냅샷 설정 섹션에서 백업 유형 페이지에서 선택한 백업 유형과 일정 유형에 대한 보존 설정을 지정합니다.

만약 당신이 원한다면...	그 다음에...
특정 수의 스냅샷을 보관하세요	*보관할 사본*을 선택한 다음 보관하려는 스냅샷 수를 지정합니다. 스냅샷 수가 지정된 수를 초과하면 스냅샷이 삭제되고 가장 오래된 사본이 먼저 삭제됩니다.  SnapVault 복제를 활성화하려면 보존 횟수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷이 대상에 복제될 때까지 첫 번째 스냅샷이 SnapVault 관계에 대한 참조 스냅샷이 되기 때문에 보존 작업이 실패할 수 있습니다.  최대 보존 값은 1018입니다. 보존 기간이 기본 ONTAP 버전에서 지원하는 것보다 높은 값으로 설정된 경우 백업이 실패합니다.
스냅샷을 특정 일수 동안 보관하세요	*사본 보관 기간*을 선택한 다음, 스냅샷을 삭제하기 전에 보관할 일수를 지정합니다.
스냅샷 복사 잠금 기간	*스냅샷 복사 잠금 기간*을 선택하고 일, 월 또는 년을 지정합니다. SnapLock 보존 기간은 100년 미만이어야 합니다.

b. 정책 라벨을 선택하세요.



원격 복제를 위해 기본 스냅샷에 SnapMirror 레이블을 할당하면 기본 스냅샷이 SnapCenter에서 ONTAP 보조 시스템으로 스냅샷 복제 작업을 오프로드할 수 있습니다. 정책 페이지에서 SnapMirror 또는 SnapVault 옵션을 활성화하지 않고도 이 작업을 수행할 수 있습니다.

7. 보조 복제 옵션 선택 섹션에서 다음 보조 복제 옵션 중 하나 또는 둘 다를 선택합니다.

이 분야에서는...	이렇게 하세요...
로컬 스냅샷 복사본을 만든 후 SnapMirror 업데이트	다른 볼륨에 백업 세트의 미러 복사본을 생성하려면 이 필드를 선택합니다(SnapMirror 복제). ONTAP의 보호 관계가 미러 및 볼트 유형이고 이 옵션만 선택하는 경우, 기본에서 생성된 스냅샷은 대상으로 전송되지 않지만 대상에는 나열됩니다. 대상에서 이 스냅샷을 선택하여 복원 작업을 수행하는 경우 다음 오류 메시지가 표시됩니다. 선택한 보관/미러링 백업에 보조 위치를 사용할 수 없습니다. 2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고침됩니다. 보다 "토폴로지 페이지에서 MySQL 리소스 관련 백업 및 복제본 보기".
로컬 스냅샷 복사본을 만든 후 SnapVault 업데이트	디스크 간 백업 복제(SnapVault 백업)를 수행하려면 이 옵션을 선택하세요. 2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고침됩니다. ONTAP에서 SnapLock Vault로 알려진 보조 노드에만 SnapLock 구성된 경우 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP에서 검색된 보조 노드의 잠금 기간이 새로 고침됩니다. SnapLock Vault에 대한 자세한 내용은 볼트 대상에서 WORM에 스냅샷 커밋을 참조하세요. 보다 "토폴로지 페이지에서 MySQL 리소스 관련 백업 및 복제본 보기".
오류 재시도 횟수	작업이 중지되기 전에 허용할 수 있는 최대 복제 시도 횟수를 입력하세요.



보조 저장소의 스냅샷 최대 한도에 도달하지 않도록 하려면 ONTAP에서 보조 저장소 SnapMirror 보존 정책을 구성해야 합니다.

8. 요약 검토한 후 *마침*을 클릭하세요.

리소스 그룹을 만들고 정책을 첨부합니다.

리소스 그룹은 백업하고 보호하려는 리소스를 추가해야 하는 컨테이너입니다. 리소스 그룹을 사용하면 주어진 애플리케이션과 관련된 모든 데이터를 동시에 백업할 수 있습니다. 모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한, 수행하려는 데이터 보호 작업 유형을 정의하려면 리소스 그룹에 하나 이상의 정책을 연결해야 합니다.

이 작업에 관하여

- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	리소스 그룹의 이름을 입력하세요.  리소스 그룹 이름은 250자를 넘을 수 없습니다.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력하세요. 예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.
스냅샷 복사에 사용자 정의 이름 형식 사용	이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다. 예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 호스트 이름을 선택하고 리소스 유형 드롭다운 목록에서 리소스 유형을 선택합니다.

이는 화면에 표시되는 정보를 필터링하는 데 도움이 됩니다.

5. 사용 가능한 리소스 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 클릭하여 선택한 리소스 섹션으로 이동합니다.
6. 애플리케이션 설정 페이지에서 다음을 수행합니다.
 - a. 추가 백업 옵션을 설정하려면 백업 화살표를 클릭하세요.

일관성 그룹 백업을 활성화하고 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
일관성 그룹 스냅샷 작업이 완료될 때까지 기다릴 시간을 확보하세요.	스냅샷 작업이 완료될 때까지의 대기 시간을 지정하려면 긴급, 보통, *느슨함*을 선택합니다. 긴급 = 5초, 보통 = 7초, 여유 = 20초.
WAFL 동기화 비활성화	WAFL 일관성 지점을 강제로 적용하지 않으려면 이 옵션을 선택하세요.

+

- 스크립트 화살표를 클릭하고 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령을 입력합니다. 실패 시 종료하기 전에 실행할 사전 명령을 입력할 수도 있습니다.
- 사용자 정의 구성 화살표를 클릭하고 이 리소스를 사용하는 모든 데이터 보호 작업에 필요한 사용자 정의 키-값 쌍을 입력합니다.

매개변수	환경	설명
아카이브 로그 활성화	(예/아니요)	보관 로그 관리를 통해 보관 로그를 삭제할 수 있습니다.
아카이브 로그 보존	일수	보관 로그를 보관하는 일수를 지정합니다. 이 설정은 NTAP_SNAPSHOT_RETENTIONS보다 크거나 같아야 합니다.

매개변수	환경	설명
아카이브_로그_디렉토리	변경_정보_디렉토리/로그	보관 로그가 포함된 디렉토리의 경로를 지정합니다.
아카이브_로그_확장	파일 확장자	보관 로그 파일 확장자 길이를 지정합니다. 예를 들어, 보관 로그가 log_backup_0_0_0_0.161518551942 9이고 file_extension 값이 5이면 로그 확장자는 5자리인 16151을 유지합니다.
ARCHIVE_LOG_RECURSIVE_SE ARCH	(예/아니요)	하위 디렉토리 내의 보관 로그 관리를 활성화합니다. 보관 로그가 하위 디렉토리에 있는 경우 이 매개변수를 사용해야 합니다.



사용자 정의 키-값 쌍은 MySQL Linux 플러그인 시스템에서는 지원되고, 중앙화된 Windows 플러그인으로 등록된 MySQL 데이터베이스에서는 지원되지 않습니다.

- c. 스냅샷 복사 도구* 화살표를 클릭하여 스냅샷을 만드는 도구를 선택하세요.

원하신다면...	그 다음에...
SnapCenter Windows용 플러그인을 사용하여 스냅샷을 생성하기 전에 파일 시스템을 일관된 상태로 만듭니다. Linux 리소스의 경우 이 옵션은 적용되지 않습니다.	*파일 시스템 일관성을 갖춘 SnapCenter *를 선택하세요.
SnapCenter 사용하여 스토리지 수준 스냅샷을 생성합니다.	*파일 시스템 일관성이 없는 SnapCenter *를 선택하세요.
스냅샷 복사본을 생성하기 위해 호스트에서 실행할 명령을 입력합니다.	*기타*를 선택한 다음 호스트에서 실행할 명령을 입력하여 스냅샷을 생성합니다.

7. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다.  *.

정책은 '선택한 정책에 대한 일정 구성' 섹션에 나열되어 있습니다.

- b.

일정 구성 열에서 *를 클릭합니다.  * 구성하려는 정책에 대해.

- c. 정책 `_policy_name_`에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 `policy_name`은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP 서버는 설정 > *전역 설정*에서 구성해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

ASA r2 시스템에서 MySQL 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.

ASA r2 시스템에 있는 리소스를 추가하려면 리소스 그룹을 만들어야 합니다. 리소스 그룹을 생성하는 동안 보조 보호를 프로비저닝할 수도 있습니다.

시작하기 전에

- ONTAP 9.x 리소스와 ASA r2 리소스를 동일한 리소스 그룹에 추가하지 않도록 해야 합니다.
- ONTAP 9.x 리소스와 ASA r2 리소스가 모두 포함된 데이터베이스가 없는지 확인해야 합니다.

이 작업에 관하여

- 2차 보호는 로그인한 사용자에게 **SecondaryProtection** 기능이 활성화된 역할이 할당된 경우에만 사용할 수 있습니다.
- 2차 보호를 활성화한 경우 기본 및 2차 일관성 그룹을 생성하는 동안 리소스 그룹은 유지 관리 모드로 전환됩니다. 기본 및 보조 일관성 그룹이 생성된 후 리소스 그룹은 유지 관리 모드에서 해제됩니다.
- SnapCenter 클론 리소스에 대한 보조 보호를 지원하지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.
 - a. 이름 필드에 리소스 그룹의 이름을 입력합니다.



리소스 그룹 이름은 250자를 넘을 수 없습니다.

- b. 나중에 리소스 그룹을 검색하는 데 도움이 되도록 태그 필드에 하나 이상의 레이블을 입력하세요.

예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.

- c. 이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다.
기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

d. 백업하지 않을 보관 로그 파일의 대상을 지정합니다.



필요한 경우 접두사를 포함하여 애플리케이션에 설정된 것과 정확히 동일한 목적지를 사용해야 합니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 데이터베이스 호스트 이름을 선택합니다.



리소스가 성공적으로 검색된 경우에만 해당 리소스가 사용 가능한 리소스 섹션에 나열됩니다.
최근에 리소스를 추가한 경우 리소스 목록을 새로 고침 후에만 사용 가능한 리소스 목록에 표시됩니다.

5. 사용 가능한 리소스 섹션에서 ASA r2 리소스를 선택하고 선택한 리소스 섹션으로 이동합니다.

6. 애플리케이션 설정 페이지에서 백업 옵션을 선택하세요.

7. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



또한 다음을 클릭하여 정책을 생성할 수도 있습니다. .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.

c. 정책_policy_name_에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 _policy_name_은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 선택한 정책에 대해 보조 보호가 활성화된 경우 보조 보호 페이지가 표시되며 다음 단계를 수행해야 합니다.

a. 복제 정책의 유형을 선택하세요.



동기 복제 정책은 지원되지 않습니다.

b. 사용할 일관성 그룹 접미사를 지정합니다.

c. 대상 클러스터 및 대상 SVM 드롭다운에서 사용하려는 피어링된 클러스터와 SVM을 선택합니다.



SnapCenter에서는 클러스터 및 SVM 피어링을 지원하지 않습니다. 클러스터 및 SVM 피어링을 수행하려면 System Manager 또는 ONTAP CLI를 사용해야 합니다.



리소스가 이미 SnapCenter 외부에서 보호되고 있는 경우 해당 리소스는 보조 보호 리소스 섹션에 표시됩니다.

1. 확인 페이지에서 다음 단계를 수행하세요.

- *로케이터 로드*를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 저장소에서 검증을 수행합니다.
- 딸깍 하는 소리  일정 구성 열에서 정책의 모든 일정 유형에 대한 확인 일정을 구성합니다.
- 확인 일정 추가 policy_name 대화 상자에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	이렇게 하세요...
백업 후 검증 실행	*백업 후 검증 실행*을 선택하세요.
검증 일정을 예약하세요	*예약된 확인 실행*을 선택한 다음 드롭다운 목록에서 일정 유형을 선택합니다.

- 보조 저장소 시스템에서 백업을 확인하려면 *보조 위치에서 확인*을 선택하세요.
- *확인*을 클릭합니다.

구성된 검증 일정은 적용된 일정 열에 나열됩니다.

2. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtptServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

3. 요약 검토한 후 *마침*을 클릭하세요.

PowerShell cmdlet을 사용하여 MySQL용 스토리지 시스템 연결 및 자격 증명 만들기

PowerShell cmdlet을 사용하여 MySQL 데이터베이스를 백업, 복원 또는 복제하려면 먼저 SVM(스토리지 가상 머신) 연결과 자격 증명을 만들어야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 저장소 연결을 생성하려면 인프라 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

스토리지 시스템 연결을 추가하는 동안에는 호스트 플러그인 설치가 진행 중이어서는 안 됩니다. 호스트 캐시가 업데이트되지 않고 SnapCenter GUI에 데이터베이스 상태가 “백업에 사용할 수 없음” 또는 “NetApp 스토리지에 없음”으로 표시될 수 있기 때문입니다.

- 저장 시스템 이름은 고유해야 합니다.

SnapCenter 서로 다른 클러스터에 동일한 이름을 가진 여러 스토리지 시스템을 지원하지 않습니다. SnapCenter 에서 지원하는 각 스토리지 시스템은 고유한 이름과 고유한 데이터 LIF IP 주소를 가져야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 PowerShell Core 연결 세션을 시작합니다.

```
PS C:\> Open-SmConnection
```

2. Add-SmStorageConnection cmdlet을 사용하여 스토리지 시스템에 대한 새 연결을 만듭니다.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Add-SmCredential cmdlet을 사용하여 새 자격 증명을 만듭니다.

이 예제에서는 Windows 자격 증명을 사용하여 FinanceAdmin이라는 새 자격 증명을 만드는 방법을 보여줍니다.

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. SnapCenter 서버에 MySQL 통신 호스트를 추가합니다.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName  
FinanceAdmin -PluginCode mysql
```

5. 호스트에 패키지와 MySQL용 SnapCenter 플러그인을 설치합니다.

Linux의 경우:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode  
mysql
```

Windows의 경우:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode mysql  
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. SQLLIB의 경로를 설정합니다.

Windows의 경우 MySQL 플러그인은 SQLLIB 폴더의 기본 경로인 "C:\Program Files\IBM\SQLLIB\BIN"을 사용합니다.

기본 경로를 재정의하려면 다음 명령을 사용하세요.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
MySQL -configSettings @{ "MySQL_SQLLIB_CMD" =
"<custom_path>\IBM\SQLLIB\BIN" }
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

MySQL 백업

리소스가 아직 어떤 리소스 그룹에도 속하지 않은 경우 리소스 페이지에서 리소스를 백업할 수 있습니다.

시작하기 전에

- 백업 정책을 생성했어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에 "snapmirror all" 권한이 포함되어야 합니다. 하지만 "vsadmin" 역할을 사용하는 경우 "snapmirror all" 권한은 필요하지 않습니다.
- 스냅샷 복사 기반 백업 작업의 경우 모든 테넌트 데이터베이스가 유효하고 활성화되어 있는지 확인하세요.
- 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령의 경우, 플러그인 호스트에서 다음 경로의 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: *C:\Program Files\NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Linux 호스트의 기본 위치: */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

선택하다  *를 선택한 다음 호스트 이름과 리소스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 선택할 수 있습니다  필터 창을 닫으려면.

3. 백업할 리소스를 선택하세요.
4. 리소스 페이지에서 *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택한 다음 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, *customtext_policy_hostname* 또는 *_resource_hostname_*입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

5. 애플리케이션 설정 페이지에서 다음을 수행합니다.

- 추가 백업 옵션을 설정하려면 백업 화살표를 선택하세요.

필요한 경우 일관성 그룹 백업을 활성화하고 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
"일관성 그룹 스냅샷" 작업이 완료될 때까지 기다릴 시간을 확보하세요.	스냅샷 작업이 완료될 때까지의 대기 시간을 지정하려면 긴급, 보통, *느슨함*을 선택합니다. 긴급 = 5초, 보통 = 7초, 여유 = 20초.
WAFL 동기화 비활성화	WAFL 일관성 지점을 강제로 적용하지 않으려면 이 옵션을 선택하세요.

- 스크립트 화살표를 선택하여 정지, 스냅샷 및 정지 해제 작업에 대한 사전 및 사후 명령을 실행합니다.

백업 작업을 종료하기 전에 사전 명령을 실행할 수도 있습니다. Prescript와 Postscript는 SnapCenter Server에서 실행됩니다.

- 사용자 정의 구성 화살표를 선택한 다음, 이 리소스를 사용하는 모든 작업에 필요한 사용자 정의 값 쌍을 입력합니다.
- 스냅샷 복사 도구* 화살표를 선택하여 스냅샷을 만드는 도구를 선택하세요.

원하신다면...	그 다음에...
SnapCenter 사용하여 스토리지 수준 스냅샷을 생성합니다.	*파일 시스템 일관성이 없는 SnapCenter *를 선택하세요.
SnapCenter Windows용 플러그인을 사용하여 파일 시스템을 일관된 상태로 만든 다음 스냅샷을 생성합니다.	*파일 시스템 일관성을 갖춘 SnapCenter *를 선택하세요.

원하신다면...	그 다음에...
스냅샷을 생성하는 명령을 입력하려면	*기타*를 선택한 다음 스냅샷을 만드는 명령을 입력합니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 클릭하여 정책을 생성할 수도 있습니다. *.

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

b. 선택하다 * 일정을 구성하려는 정책에 대한 일정 구성 옆에 있습니다.

c. 정책 `_policy_name_`에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 선택합니다.

`_policy_name_`은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 옆에 나열됩니다.

7. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > *전역 설정*에서도 구성해야 합니다.

8. 요약 검토한 후 *마침*을 선택하세요.

리소스 토폴로지 페이지가 표시됩니다.

9. *지금 백업*을 선택하세요.
10. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스에 여러 정책을 적용한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.
 - b. *백업*을 선택하세요.
11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.
 - MetroCluster 구성에서 SnapCenter 장애 조치 후 보호 관계를 감지하지 못할 수 있습니다.

자세한 내용은 다음을 참조하세요. ["MetroCluster 장애 조치 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다."](#)
 - VMDK에서 애플리케이션 데이터를 백업하고 SnapCenter Plug-in for VMware vSphere의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다.

Java 힙 크기를 늘리려면 스크립트 파일 `/opt/netapp/init_scripts/scvservice_`를 찾으세요. 해당 스크립트에서 `_do_start` 메서드 명령은 SnapCenter VMware 플러그인 서비스를 시작합니다. 해당 명령을 다음으로 업데이트하세요: `Java -jar -Xmx8192M -Xms4096M`

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-SmConnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146\
```

사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.

2. Add-SmResources cmdlet을 사용하여 수동 리소스를 추가합니다.

이 예제에서는 MySQL 인스턴스를 추가하는 방법을 보여줍니다.

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode MySQL
-ResourceType Instance -ResourceName mysqlinst1 -StorageFootPrint
(@{"VolumeName"="winmysql01_data01";"LUNName"="winmysql01_data01";"S
torageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.
4. Add-SmResourceGroup cmdlet을 사용하여 리소스를 보호하거나 SnapCenter에 새 리소스 그룹을 추가합니다.
5. New-SmBackup cmdlet을 사용하여 새로운 백업 작업을 시작합니다.

이 예제에서는 리소스 그룹을 백업하는 방법을 보여줍니다.

```
C:\PS> New-SmBackup -Resources  
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306";"P  
luginName"="MySQL"} -Policy "MySQL_snapshotbased"
```

이 예제에서는 보호된 리소스를 백업합니다.

```
C:\PS> New-SMBackup -Resources  
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}  
-Policy mysql_policy2
```

6. Get-smJobSummaryReport cmdlet을 사용하여 작업 상태(실행 중, 완료 또는 실패)를 모니터링합니다.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Get-SmBackupReport cmdlet을 사용하여 복원 또는 복제 작업을 수행하기 위한 백업 ID, 백업 이름과 같은 백업 작업 세부 정보를 모니터링합니다.


```

PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :

```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

리소스 그룹 백업

리소스 그룹은 호스트의 리소스 모음입니다. 리소스 그룹에 대한 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다.

시작하기 전에

- 정책이 첨부된 리소스 그룹을 만들어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에 "snapmirror all" 권한이 포함되어야 합니다. 하지만 "vsadmin" 역할을 사용하는 경우 "snapmirror all" 권한은 필요하지 않습니다.

이 작업에 관하여

리소스 페이지에서 필요에 따라 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 첨부되고 일정이 구성된 경우 백업은 일정에 따라 자동으로 수행됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.

검색창에 리소스 그룹 이름을 입력하거나 다음을 선택하여 리소스 그룹을 검색할 수 있습니다.  , 그리고 태그를 선택합니다. 그런 다음 선택할 수 있습니다.  필터 창을 닫으려면.

3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음, *지금 백업*을 선택합니다.
4. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스 그룹에 여러 정책을 연결한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. *백업*을 선택하세요.

5. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

MySQL 백업 작업 모니터링

SnapCenterJobs 페이지를 사용하여 다양한 백업 작업의 진행 상황을 모니터링할 수 있습니다. 완료 시점이나 문제가 있는지 확인하기 위해 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 해당 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  백업 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *백업*을 선택합니다.
 - d. 상태 드롭다운에서 백업 상태를 선택합니다.
 - e. *적용*을 클릭하면 작업이 성공적으로 완료된 것을 볼 수 있습니다.

4. 백업 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인하세요.



백업 작업 상태가 표시됩니다. 작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 표시가 되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

활동 창에서 **MySQL** 인스턴스의 데이터 보호 작업을 모니터링합니다.

활동 창에는 가장 최근에 수행된 5개의 작업이 표시됩니다. 활동 창에는 작업이 시작된 시점과 작업 상태도 표시됩니다.

활동 창에는 백업, 복원, 복제 및 예약된 백업 작업에 대한 정보가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 딸깍 하는 소리 활동 창에서 가장 최근의 작업 5개를 확인하세요.

작업 중 하나를 클릭하면 작업 세부 정보가 작업 세부 정보 페이지에 나열됩니다.

MySQL에 대한 백업 작업 취소

대기 중인 백업 작업을 취소할 수 있습니다.

필요한 것

- 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 모니터 페이지나 활동 창에서 백업 작업을 취소할 수 있습니다.
- 실행 중인 백업 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 백업 작업을 취소할 수 있습니다.
- 취소할 수 없는 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자 그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 백업 작업을 취소할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	a. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. b. 작업을 선택한 다음 *작업 취소*를 클릭합니다.

...로부터	행동
활동 창	a. 백업 작업을 시작한 후 *를 클릭하세요.  * 활동 창에서 가장 최근의 작업 5개를 확인하세요. b. 작업을 선택하세요. c. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

작업이 취소되고 리소스는 이전 상태로 돌아갑니다.

토폴로지 페이지에서 MySQL 백업 및 복제본 보기

리소스를 백업하거나 복제할 준비를 할 때 기본 및 보조 저장소에 있는 모든 백업과 복제본을 그래픽으로 표현해 보면 도움이 될 수 있습니다.

이 작업에 관하여

다음 아이콘을 '사본 관리' 보기에서 검토하여 백업 및 복제본을 기본 저장소 또는 보조 저장소(미러 사본 또는 볼트 사본)에서 사용할 수 있는지 확인할 수 있습니다.

-  기본 스토리지에서 사용 가능한 백업 및 복제본의 수를 표시합니다.
-  SnapMirror 기술을 사용하여 보조 저장소에 미러링된 백업 및 복제본의 수를 표시합니다.
-  SnapVault 기술을 사용하여 보조 저장소에 복제된 백업 및 복제본의 수를 표시합니다.



표시된 백업 수에는 보조 저장소에서 삭제된 백업이 포함됩니다. 예를 들어, 4개의 백업만 보존하는 정책을 사용하여 6개의 백업을 만든 경우 표시되는 백업 수는 6개입니다.



미러 볼트 유형 볼륨의 버전 가변형 미러 백업의 복제본은 토폴로지 보기에 표시되지만, 토폴로지 보기의 미러 백업 수에는 버전 가변형 백업이 포함되지 않습니다.

토폴로지 페이지에서는 선택한 리소스 또는 리소스 그룹에 사용 가능한 모든 백업과 복제본을 볼 수 있습니다. 해당 백업 및 복제의 세부 정보를 보고 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

단계

- 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
- 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
- 리소스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 리소스를 선택합니다.

리소스가 보호된 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. *요약 카드*를 검토하여 기본 및 보조 저장소에서 사용 가능한 백업 및 복제본 수에 대한 요약 확인하세요.

요약 카드 섹션에는 스냅샷 복사 기반 백업과 복제본의 총 수가 표시됩니다.

새로 고침 버튼을 클릭하면 저장소에 대한 쿼리가 시작되어 정확한 개수가 표시됩니다.

SnapLock 이 활성화된 백업을 수행한 경우 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간이 새로 고쳐집니다. 주간 일정은 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간도 새로 고칩니다.

애플리케이션 리소스가 여러 볼륨에 분산되어 있는 경우 백업에 대한 SnapLock 만료 시간은 볼륨의 스냅샷에 설정된 가장 긴 SnapLock 만료 시간이 됩니다. 가장 긴 SnapLock 만료 시간은 ONTAP 에서 검색됩니다.

주문형 백업 후, 새로 고침 버튼을 클릭하면 백업이나 복제의 세부 정보가 새로 고칩니다.

5. 복사본 관리 보기에서 기본 또는 보조 저장소의 백업 또는 *복제*를 클릭하면 백업 또는 복제의 세부 정보를 볼 수 있습니다.

백업 및 복제의 세부 정보는 표 형식으로 표시됩니다.

6. 표에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 복제, 삭제 작업을 수행합니다.



보조 저장소에 있는 백업은 이름을 바꾸거나 삭제할 수 없습니다.

7. 복제본을 삭제하려면 테이블에서 복제본을 선택한 다음 클릭하세요. .

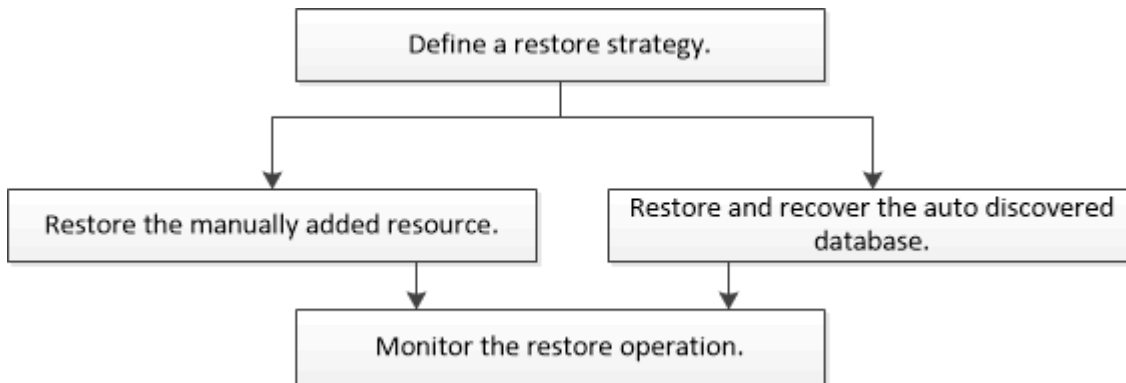
8. 복제본을 분할하려면 테이블에서 복제본을 선택한 다음 클릭하세요. .

MySQL 복원

워크플로 복원

복원 및 복구 워크플로에는 계획, 복원 작업 수행, 작업 모니터링이 포함됩니다.

다음 워크플로는 복원 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

수동으로 추가된 리소스 백업을 복원하고 복구합니다.

SnapCenter 사용하면 하나 이상의 백업에서 데이터를 복원하고 복구할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 복원하려는 리소스 또는 리소스 그룹에 대해 현재 진행 중인 모든 백업 작업을 취소해야 합니다.
- 사전 복원, 사후 복원, 마운트 및 마운트 해제 명령의 경우, 다음 경로에서 플러그인 호스트에서 사용 가능한 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Linux 호스트의 기본 위치: */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- ONTAP 9.12.1 및 이전 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속합니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 함께 표시됩니다.



백업은 리소스 그룹을 위한 것일 수 있지만 복원할 때는 복원할 개별 리소스를 선택해야 합니다.

리소스가 보호되지 않은 경우 전체 상태 열에 "보호되지 않음"이 표시됩니다. 이는 리소스가 보호되지 않았거나 다른 사용자가 리소스를 백업했음을 의미할 수 있습니다.

3. 리소스를 선택하거나 리소스 그룹을 선택한 다음 해당 그룹에서 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 기본 백업 테이블에서 복원하려는 백업을 선택한 다음 *를 클릭합니다.  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scscr0191685001_01-05-2017-01.35.06.6463	1/5/2017 1:35:27 AM 

6. 복원 범위 페이지에서 *리소스 완료*를 선택합니다.

- a. *전체 리소스*를 선택하면 MySQL 데이터베이스의 구성된 모든 데이터 볼륨이 복원됩니다.

리소스에 볼륨이나 Q트리가 포함되어 있는 경우 해당 볼륨이나 Q트리에서 복원을 위해 선택한 스냅샷 이후에 생성된 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 다른 리소스가 동일한 볼륨이나 Q트리에 호스팅된 경우 해당 리소스도 삭제됩니다.

여러 개의 LUN을 선택할 수 있습니다.



*모두*를 선택하면 볼륨, Q트리 또는 LUN의 모든 파일이 복원됩니다.

7. 사전 작업 페이지에서 복원 작업을 수행하기 전에 실행할 사전 복원 및 마운트 해제 명령을 입력합니다.

자동 검색된 리소스에는 마운트 해제 명령을 사용할 수 없습니다.

8. Post ops 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.

자동 검색된 리소스에는 마운트 명령을 사용할 수 없습니다.

9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > 전역 설정 페이지에서도 구성해야 합니다.

10. 요약을 검토한 후 *마침*을 클릭하세요.

11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-Smconnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

이 예에서는 2015년 1월 29일부터 2015년 2월 3일까지의 백업에 대한 자세한 정보를 표시합니다.


```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

자동 검색된 데이터베이스 백업을 복원하고 복구합니다.

SnapCenter 사용하면 하나 이상의 백업에서 데이터를 복원하고 복구할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 복원하려는 리소스 또는 리소스 그룹에 대해 현재 진행 중인 모든 백업 작업을 취소해야 합니다.
- 사전 복원, 사후 복원, 마운트 및 마운트 해제 명령의 경우, 다음 경로에서 플러그인 호스트에서 사용 가능한 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

◦ Linux 호스트의 기본 위치: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



명령 목록에 해당 명령이 없으면 작업이 실패합니다.

이 작업에 관하여

- 자동 검색된 리소스의 경우 SFSR을 통해 복원이 지원됩니다.
- 특정 시점 및 최신 자동 복구는 지원되지 않습니다.
- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 함께 표시됩니다.



백업은 리소스 그룹을 위한 것일 수 있지만 복원할 때는 복원할 개별 리소스를 선택해야 합니다.

리소스가 보호되지 않은 경우 전체 상태 열에 "보호되지 않음"이 표시됩니다. 이는 리소스가 보호되지 않았거나 다른 사용자가 리소스를 백업했음을 의미할 수 있습니다.

3. 리소스를 선택하거나 리소스 그룹을 선택한 다음 해당 그룹에서 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 기본 백업 테이블에서 복원하려는 백업을 선택한 다음 *를 클릭합니다.  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scscr0191683001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. 복원 범위 페이지에서 *전체 리소스*를 선택하여 MySQL 데이터베이스의 구성된 데이터 볼륨을 복원합니다.
7. 사전 작업 페이지에서 복원 작업을 수행하기 전에 실행할 사전 복원 및 마운트 해제 명령을 입력합니다.

자동 검색된 리소스에는 마운트 해제 명령을 사용할 수 없습니다.

8. Post ops 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.

자동 검색된 리소스에는 마운트 명령을 사용할 수 없습니다.

9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > 전역 설정 페이지에서도

구성해야 합니다.

10. 요약을 검토한 후 *마침*을 클릭하세요.
11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet을 사용하여 리소스 복원

리소스 백업을 복원하려면 SnapCenter 서버와 연결 세션을 시작하고, 백업을 나열하고 백업 정보를 검색하고, 백업을 복원해야 합니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-Smconnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM

이 예에서는 2015년 1월 29일부터 2015년 2월 3일까지의 백업에 대한 자세한 정보를 표시합니다.

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName        : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName        : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

MySQL 복원 작업 모니터링

작업 페이지를 사용하여 다양한 SnapCenter 복원 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

복원 후 상태는 복원 작업 후 리소스의 조건과 수행할 수 있는 추가 복원 작업을 설명합니다.

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중

-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복원 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복원*을 선택합니다.
 - d. 상태 드롭다운 목록에서 복원 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복원 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

MySQL 리소스 백업 복제

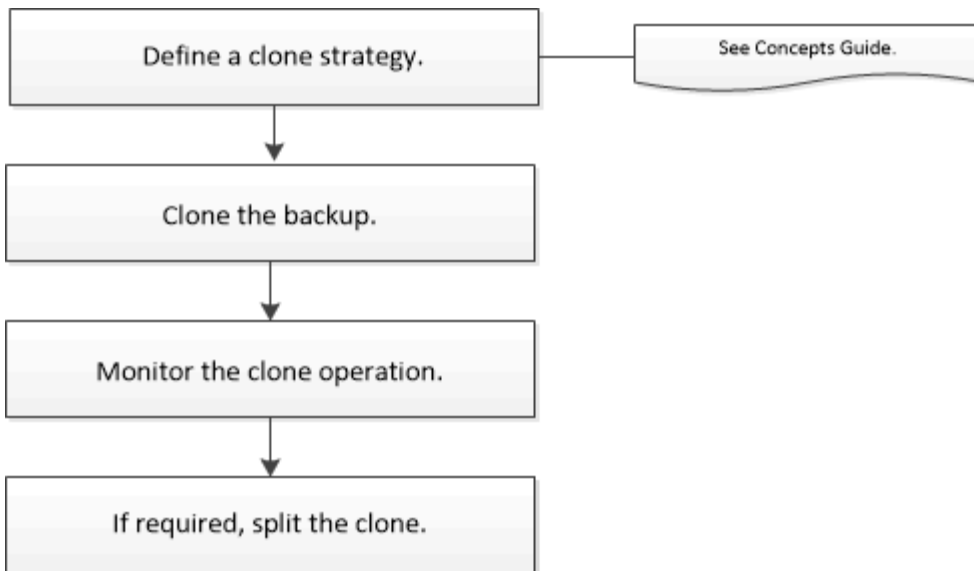
복제 워크플로

복제 워크플로에는 복제 작업을 수행하고 작업을 모니터링하는 작업이 포함됩니다.

이 작업에 관하여

- 소스 MySQL 서버에서 복제할 수 있습니다.
- 다음과 같은 이유로 리소스 백업을 복제할 수 있습니다.
 - 애플리케이션 개발 주기 동안 현재 리소스 구조 및 콘텐츠를 사용하여 구현해야 하는 기능을 테스트하려면
 - 데이터 웨어하우스를 채울 때 데이터 추출 및 조작 도구
 - 실수로 삭제되거나 변경된 데이터를 복구하려면

다음 워크플로는 복제 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

MySQL 백업 복제

SnapCenter 사용하여 백업을 복제할 수 있습니다. 기본 또는 보조 백업에서 복제할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 볼륨을 호스팅하는 집계가 스토리지 가상 머신(SVM)의 할당된 집계 목록에 있는지 확인해야 합니다.
- 복제 전 또는 복제 후 명령의 경우, 플러그인 호스트에서 다음 경로의 명령 목록에 해당 명령이 있는지 확인해야 합니다.
 - Windows 호스트의 기본 위치: *C:\Program Files\NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Linux 호스트의 기본 위치: */opt/ NetApp/ snapcenter/ scc/ etc/ allowed_commands.config*



명령 목록에 해당 명령이 없으면 작업이 실패합니다. * MySQL 5.7 버전의 경우 MySQL.properties 파일에서 IGNORE_MYSQLX_PORT = true(기본값은 false)를 설정해야 합니다.

이 작업에 관하여

- 복제된 MySQL 인스턴스를 보호할 수 없습니다.
- FlexClone 볼륨 분할 작업에 대한 정보는 다음을 참조하세요. <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["FlexClone 볼륨을 부모 볼륨에서 분할합니다."].
- ONTAP 9.12.1 및 이전 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속합니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트, 연관된 리소스 그룹 및 정책, 상태와 같은 정보와 함께 표시됩니다.

3. 리소스 또는 리소스 그룹을 선택하세요.

리소스 그룹을 선택하는 경우 리소스를 선택해야 합니다.

리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 표에서 데이터 백업을 선택한 다음 클릭하세요.  .
6. 위치 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
복제 서버	복제본을 생성할 호스트를 선택하세요.
포트	복제된 MySQL 인스턴스가 시작될 포트를 제공합니다.
NFS 내보내기 IP 주소	복제된 볼륨을 내보낼 IP 주소나 호스트 이름을 입력합니다.

7. 스크립트 페이지에서 다음 단계를 수행합니다.



스크립트는 플러그인 호스트에서 실행됩니다.

- a. 복제 작업 전이나 후에 실행해야 하는 사전 복제 또는 사후 복제에 대한 명령을 각각 입력합니다.
 - 사전 복제 명령: 동일한 이름을 가진 기존 데이터베이스 삭제
 - 복제 후 명령: 데이터베이스를 확인하거나 데이터베이스를 시작합니다.
- b. 호스트에 파일 시스템을 마운트하려면 mount 명령을 입력하세요.

Linux 머신에서 볼륨이나 qtree에 대한 마운트 명령:

NFS의 예: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

10. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-SmConnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

2. Get-SmBackup cmdlet을 사용하여 복제 작업을 수행하기 위해 백업을 검색합니다.

이 예에서는 복제에 사용할 수 있는 백업이 두 개 있음을 보여줍니다.

```
C:\PS> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
1	Payroll Dataset_vise-f6_08...
8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...
8/4/2015 11:23:17 AM	

3. 기존 백업에서 복제 작업을 시작하고 복제된 볼륨이 내보내지는 NFS 내보내기 IP 주소를 지정합니다.

이 예에서는 복제할 백업의 NFSExportIPs 주소가 10.32.212.14임을 보여줍니다.

```
PS C:\> New-SmClone -AppPluginCode MySQL -BackupName  
"scs000211748_gdl_englab_netapp_com_MySQL_mysqlid_3306_scs000211748_0  
6-26-2024_06.08.35.4307" -Resources  
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqlid_3306"}  
-Port 3320 -CloneToHost shivarhel30.rtp.openenglab.netapp.com
```



NFSExportIPs가 지정되지 않으면 기본값이 복제 대상 호스트로 내보내집니다.

4. Get-SmCloneReport cmdlet을 사용하여 복제 작업 세부 정보를 보고 백업이 성공적으로 복제되었는지 확인합니다.

클론 ID, 시작 날짜 및 시간, 종료 날짜 및 시간과 같은 세부 정보를 볼 수 있습니다.

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration             : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName           : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName     : OnDemand_Full_Log
SmBackupPolicyId     : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId          : 4
CloneName            : Draper__clone__08-03-2015_14.43.53
SourceResources      : {Don, Betty, Bobby, Sally}
ClonedResources      : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError           :
```

MySQL 복제 작업 모니터링

작업 페이지를 사용하여 SnapCenter 복제 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.

3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복제 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복제*를 선택합니다.
 - d. 상태 드롭다운 목록에서 복제 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복제 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

클론 분할

SnapCenter 사용하면 복제된 리소스를 부모 리소스에서 분할할 수 있습니다. 분할된 복제본은 부모 리소스로부터 독립됩니다.

이 작업에 관하여

- 중간 복제본에서는 복제 분할 작업을 수행할 수 없습니다.

예를 들어, 데이터베이스 백업에서 clone1을 만든 후 clone1의 백업을 만든 다음 이 백업(clone2)을 복제할 수 있습니다. clone2를 생성한 후 clone1은 중간 복제본이 되며 clone1에서 복제 분할 작업을 수행할 수 없습니다. 하지만 clone2에 대해 클론 분할 작업을 수행할 수 있습니다.

clone2를 분할한 후에는 clone1에 대해 clone 분할 작업을 수행할 수 있습니다. clone1은 더 이상 중간 클론이 아니기 때문입니다.

- 복제본을 분할하면 복제본의 백업 사본과 복제 작업이 삭제됩니다.
- FlexClone 볼륨 분할 작업에 대한 정보는 다음을 참조하세요. "[FlexClone 볼륨을 부모 볼륨에서 분할합니다.](#)".
- 스토리지 시스템의 볼륨이나 집계가 온라인인지 확인하세요.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 적절한 옵션을 선택하세요.

옵션	설명
데이터베이스 애플리케이션의 경우	보기 목록에서 *데이터베이스*를 선택합니다.
파일 시스템의 경우	보기 목록에서 *경로*를 선택합니다.

3. 목록에서 적절한 리소스를 선택하세요.

리소스 토폴로지 페이지가 표시됩니다.
4. 사본 관리 보기에서 복제된 리소스(예: 데이터베이스 또는 LUN)를 선택한 다음 *를 클릭합니다.  *.
5. 분할할 클론의 예상 크기와 집계에 필요한 사용 가능한 공간을 검토한 다음 *시작*을 클릭합니다.

6. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

SMCore 서비스를 다시 시작하면 복제 분할 작업이 더 이상 응답하지 않습니다. 복제 분할 작업을 중지하려면 Stop-SmJob cmdlet을 실행한 다음 복제 분할 작업을 다시 시도해야 합니다.

복제본이 분할되었는지 여부를 확인하기 위해 더 긴 폴링 시간이나 더 짧은 폴링 시간이 필요한 경우 *SMCoreServiceHost.exe.config* 파일에서 *CloneSplitStatusCheckPollTime* 매개변수 값을 변경하여 SMCore가 복제본 분할 작업의 상태를 폴링하는 시간 간격을 설정할 수 있습니다. 값은 밀리초이고 기본값은 5분입니다.

예를 들어:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

백업, 복원 또는 다른 클론 분할이 진행 중이면 클론 분할 시작 작업이 실패합니다. 실행 중인 작업이 완료된 후에만 복제 분할 작업을 다시 시작해야 합니다.

관련 정보

"SnapCenter 복제 또는 검증이 집계가 존재하지 않아 실패합니다."

SnapCenter 업그레이드 후 MySQL 데이터베이스 복제본 삭제 또는 분할

SnapCenter 4.3으로 업그레이드한 후에는 더 이상 복제본이 표시되지 않습니다. 복제본이 생성된 리소스의 토폴로지 페이지에서 복제본을 삭제하거나 분할할 수 있습니다.

이 작업에 관하여

숨겨진 복제본의 저장 공간을 찾으려면 다음 명령을 실행하세요. `Get-SmClone -ListStorageFootprint`

단계

1. remove-smbbackup cmdlet을 사용하여 복제된 리소스의 백업을 삭제합니다.
2. remove-smresourcegroup cmdlet을 사용하여 복제된 리소스의 리소스 그룹을 삭제합니다.
3. remove-smprotectresource cmdlet을 사용하여 복제된 리소스의 보호를 제거합니다.
4. 리소스 페이지에서 상위 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

5. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 복제본을 선택합니다.
6. 복제본을 선택한 다음 클릭하세요.  클론을 삭제하거나 클릭하세요  클론을 분할합니다.
7. *확인*을 클릭합니다.

NetApp 지원 플러그인을 사용하여 애플리케이션 보호

NetApp 지원 플러그인

NetApp 지원 플러그인 개요

MongoDB, ORASCPM(Oracle Applications), SAP ASE, SAP MaxDB 및 사용하는 애플리케이션에 대한 Storage 플러그인과 같은 NetApp 지원 플러그인을 사용한 다음 SnapCenter 사용하여 이러한 애플리케이션을 백업, 복원 또는 복제할 수 있습니다. NetApp에서 지원하는 플러그인은 NetApp SnapCenter 소프트웨어의 호스트 측 구성 요소 역할을 하여 애플리케이션 인식 데이터 보호 및 리소스 관리를 지원합니다.

NetApp 지원하는 플러그인을 설치하면 NetApp SnapMirror 기술과 함께 SnapCenter 사용하여 다른 볼륨에 백업 세트의 미러 사본을 만들고 NetApp SnapVault 기술을 사용하여 디스크 간 백업 복제를 수행할 수 있습니다. NetApp에서 지원하는 플러그인은 Windows와 Linux 환경 모두에서 사용할 수 있습니다.



SnapCenterCLI는 NetApp 지원 플러그인 명령을 지원하지 않습니다.

NetApp SnapCenter에 내장된 플러그인 프레임워크를 사용하여 ONTAP 스토리지의 데이터 볼륨에 대한 데이터 보호 작업을 수행하는 스토리지 플러그인을 제공합니다.

호스트 추가 페이지에서 NetApp 지원 플러그인을 설치할 수 있습니다.

"원격 호스트에 호스트를 추가하고 플러그인 패키지를 설치합니다."



SnapCenter 지원 정책은 플러그인 프레임워크, 코어 엔진 및 관련 API에 대한 지원을 다룹니다. 플러그인 프레임워크에 기반한 플러그인 소스 코드와 관련 스크립트는 지원 대상이 아닙니다.

NetApp 지원 플러그인으로 할 수 있는 작업

MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB 및 Storage 플러그인과 같은 NetApp 지원 플러그인을 데이터 보호 작업에 사용할 수 있습니다.

- 데이터베이스, 인스턴스, 문서 또는 테이블스페이스와 같은 리소스를 추가합니다.
- 백업을 만듭니다.
- 백업에서 복원합니다.
- 백업을 복제합니다.
- 백업 작업을 예약합니다.
- 백업, 복원 및 복제 작업을 모니터링합니다.
- 백업, 복원 및 복제 작업에 대한 보고서를 확인합니다.

데이터 보호 작업에 NetApp 지원 플러그인을 사용할 수 있습니다.

- ONTAP 클러스터 전반의 스토리지 볼륨에 대한 일관성 그룹 스냅샷을 만듭니다.

- 내장된 사전 및 사후 스크립팅 프레임워크를 사용하여 사용자 정의 애플리케이션 백업

ONTAP 볼륨, LUN 또는 Qtree를 백업할 수 있습니다.

- SnapCenter 정책을 사용하여 기존 복제 관계(SnapVault/ SnapMirror /통합 복제)를 활용하여 기본에서 촬영한 스냅샷을 ONTAP 보조로 업데이트합니다.

ONTAP 기본 및 보조는 ONTAP FAS, AFF, ASA, ONTAP Select 또는 Cloud Volumes ONTAP 될 수 있습니다.

- ONTAP 볼륨, LUN 또는 파일을 모두 복구합니다.

제품에는 탐색이나 인덱싱 기능이 내장되어 있지 않으므로 해당 파일 경로를 수동으로 제공해야 합니다.

Qtree 또는 디렉토리 복원은 지원되지 않지만 백업 범위가 Qtree 수준에서 정의된 경우에만 Qtree를 복제하고 내보낼 수 있습니다.

NetApp 지원 플러그인 기능

SnapCenter 플러그인 애플리케이션과 스토리지 시스템의 NetApp 기술과 통합됩니다. MongoDB, ORASCPM(Oracle Applications), SAP ASE, SAP MaxDB 및 Storage 플러그인과 같은 NetApp 지원 플러그인을 사용하려면 SnapCenter 그래픽 사용자 인터페이스를 사용합니다.

- 통합된 그래픽 사용자 인터페이스

SnapCenter 인터페이스는 플러그인과 환경 전반에 걸쳐 표준화와 일관성을 제공합니다. SnapCenter 인터페이스를 사용하면 플러그인 전반에 걸쳐 일관된 백업, 복원, 복구 및 복제 작업을 완료하고, 중앙 집중식 보고를 사용하고, 한눈에 보이는 대시보드 보기를 사용하고, 역할 기반 액세스 제어(RBAC)를 설정하고, 모든 플러그인에서 작업을 모니터링할 수 있습니다.

- 자동화된 중앙 관리

백업 작업을 예약하고, 정책 기반 백업 보존을 구성하고, 복원 작업을 수행할 수 있습니다. SnapCenter 구성하여 이메일 알림을 보내 환경을 사전에 모니터링할 수도 있습니다.

- 중단 없는 **NetApp** 스냅샷 기술

SnapCenter NetApp 지원 플러그인과 함께 NetApp Snapshot 기술을 사용하여 리소스를 백업합니다. 스냅샷은 최소한의 저장 공간을 차지합니다.

NetApp 지원하는 플러그인은 다음과 같은 이점도 제공합니다.

- 백업, 복원 및 복제 워크플로 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임

또한, 권한이 있는 SnapCenter 사용자에게 애플리케이션 수준 권한이 부여되도록 자격 증명을 설정할 수도 있습니다.

- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 리소스의 공간 효율적 및 특정 시점 복사본 생성

복제본을 생성하려는 스토리지 시스템에 FlexClone 라이선스가 필요합니다.

- 백업 생성의 일부로 ONTAP의 일관성 그룹(CG) 스냅샷 기능을 지원합니다.
- 여러 리소스 호스트에서 동시에 여러 백업을 실행할 수 있는 기능

단일 작업에서 단일 호스트의 리소스가 동일한 볼륨을 공유하는 경우 스냅샷이 통합됩니다.

- 외부 명령을 사용하여 스냅샷을 생성하는 기능.
- Windows 환경에서 파일 시스템과 일관된 스냅샷을 생성하는 기능.

NetApp 지원 플러그인에서 지원하는 스토리지 유형

SnapCenter 물리적 머신과 가상 머신 모두에서 다양한 스토리지 유형을 지원합니다. NetApp 지원 플러그인을 설치하기 전에 스토리지 유형에 대한 지원을 확인해야 합니다.

기계	저장 유형
VM 호스트에 대한 물리적 및 NFS 직접 마운트(VMDK 및 RDM LUN은 지원되지 않음)	FC 연결 LUN
VM 호스트에 대한 물리적 및 NFS 직접 마운트(VMDK 및 RDM LUN은 지원되지 않음)	iSCSI로 연결된 LUN
VM 호스트에 대한 물리적 및 NFS 직접 마운트(VMDK 및 RDM LUN은 지원되지 않음)	NFS 연결 볼륨
VMware ESXi	NFS와 SAN 모두에 있는 vVol 데이터 저장소 vVol 데이터스토어는 VMware vSphere용 ONTAP 도구를 사용해서만 프로비저닝할 수 있습니다.

NetApp 지원 플러그인에 필요한 최소 ONTAP 권한

데이터 보호를 위해 사용하는 SnapCenter 플러그인에 따라 필요한 최소 ONTAP 권한은 다릅니다.

- 모든 액세스 명령: ONTAP 9.12.1 이상에 필요한 최소 권한
 - 이벤트 생성-자동 지원-로그
 - 작업 이력 표시
 - 작업 중지
 - lun 속성 표시
 - lun 생성
 - lun 삭제
 - LUN 기하학

- lun igroup 추가
- lun igroup 생성
- lun igroup 삭제
- lun igroup 이름 바꾸기
- 룬 아이그룹 쇼
- lun 매핑 add-reporting-nodes
- lun 매핑 생성
- LUN 매핑 삭제
- LUN 매핑 제거-보고-노드
- lun 매핑 쇼
- lun 수정
- lun 이동량
- lun 오프라인
- lun 온라인
- lun 크기 조정
- lun 시리얼
- 룬 쇼
- 네트워크 인터페이스
- 스냅미러 정책 추가 규칙
- 스냅미러 정책 수정 규칙
- 스냅미러 정책 제거 규칙
- 스냅미러 정책 보기
- 스냅미러 복원
- 스냅미러 쇼
- 스냅미러 쇼 히스토리
- 스냅미러 업데이트
- 스냅미러 업데이트-ls-세트
- 스냅미러 목록-대상
- 버전
- 볼륨 복제 생성
- 볼륨 클론 쇼
- 볼륨 복제 분할 시작
- 볼륨 클론 분할 정지
- 볼륨 생성

- 볼륨 파괴
 - 볼륨 파일 복제 생성
 - 볼륨 파일 show-disk-usage
 - 볼륨 오프라인
 - 온라인 볼륨
 - 볼륨 수정
 - 볼륨 qtree 생성
 - 볼륨 qtree 삭제
 - 볼륨 qtree 수정
 - 볼륨 qtree 쇼
 - 볼륨 제한
 - 볼륨 쇼
 - 볼륨 스냅샷 생성
 - 볼륨 스냅샷 삭제
 - 볼륨 스냅샷 수정
 - 볼륨 스냅샷 이름 바꾸기
 - 볼륨 스냅샷 복원
 - 볼륨 스냅샷 복원 파일
 - 볼륨 스냅샷 표시
 - 볼륨 마운트 해제
 - vservers cifs
 - vservers cifs 공유 생성
 - vservers cifs 공유 삭제
 - vservers cifs 새도우 카피 쇼
 - vservers cifs 공유 표시
 - vservers cifs 쇼
 - vservers 내보내기 정책 생성
 - vservers 내보내기 정책 삭제
 - vservers 내보내기 정책 규칙 생성
 - vservers 내보내기 정책 규칙 표시
 - vservers 내보내기 정책 표시
 - vservers iscsi 연결 표시
 - vservers 쇼
- 읽기 전용 명령: ONTAP 8.3.0 이상에 필요한 최소 권한

NetApp 지원 플러그인을 위한 SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비

ONTAP SnapMirror 기술과 함께 SnapCenter 플러그인을 사용하면 다른 볼륨에 백업 세트의 미러 사본을 생성할 수 있으며, ONTAP SnapVault 기술과 함께 사용하면 표준 준수 및 기타 거버넌스 관련 목적으로 디스크 간 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 구성하고 해당 관계를 초기화해야 합니다.

SnapCenter 스냅샷 작업을 완료한 후 SnapMirror와 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행되므로 별도의 ONTAP 일정을 만들지 마세요.



NetApp SnapManager 제품을 통해 SnapCenter에 접속했고 구성된 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 기본 저장소(소스 볼륨)의 데이터를 보조 저장소(대상 볼륨)로 복제합니다. 관계를 초기화하면 ONTAP 소스 볼륨에서 참조되는 데이터 블록을 대상 볼륨으로 전송합니다.



SnapCenter SnapMirror와 SnapVault 볼륨 간의 계단식 관계(**Primary > Mirror > Vault**)를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter 버전에 따라 유연한 SnapMirror 관계 관리를 지원합니다. 버전에 따라 유연한 SnapMirror 관계와 이를 설정하는 방법에 대한 자세한 내용은 다음을 참조하세요. "[ONTAP 문서](#)".

백업 전략 정의

백업 작업을 생성하기 전에 백업 전략을 정의하면 리소스를 성공적으로 복원하거나 복제하는 데 필요한 백업이 있는지 확인할 수 있습니다. 백업 전략은 주로 서비스 수준 계약(SLA), 복구 시간 목표(RTO), 복구 지점 목표(RPO)에 따라 결정됩니다.

이 작업에 관하여

SLA는 기대되는 서비스 수준을 정의하고 서비스의 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RTO는 서비스가 중단된 후 비즈니스 프로세스를 복구해야 하는 시간입니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 기간에 대한 전략을 정의합니다. SLA, RTO, RPO는 데이터 보호 전략에 기여합니다.

단계

1. 리소스를 백업해야 하는 시기를 결정하세요.
2. 필요한 백업 작업의 수를 결정합니다.
3. 백업의 이름을 어떻게 지을지 결정하세요.
4. 일관성 그룹 스냅샷을 원하는지 결정하고 일관성 그룹 스냅샷을 삭제하기 위한 적절한 옵션을 결정합니다.
5. 복제를 위해 NetApp SnapMirror 기술을 사용할지, 장기 보존을 위해 NetApp SnapVault 기술을 사용할지 결정하세요.
6. 소스 스토리지 시스템과 SnapMirror 대상의 스냅샷 보존 기간을 결정합니다.
7. 백업 작업 전이나 후에 명령을 실행할지 결정하고 사전 스크립트나 사후 스크립트를 제공합니다.

NetApp 지원 플러그인에 대한 백업 전략

NetApp 지원 플러그인 리소스의 백업 일정

백업 일정을 결정하는 가장 중요한 요소는 리소스의 변화율입니다. 리소스를 더 자주 백업할수록 SnapCenter 복원에 사용해야 하는 아카이브 로그가 줄어들어 복원 작업이 더 빨라질 수 있습니다.

자주 사용되는 리소스는 매시간 백업하고, 거의 사용되지 않는 리소스는 하루에 한 번 백업할 수도 있습니다. 기타 요소로는 조직에 대한 리소스의 중요성, 서비스 수준 계약(SLA), 복구 지점 목표(RPO) 등이 있습니다.

SLA는 기대되는 서비스 수준을 정의하고 서비스 가용성과 성능을 포함한 많은 서비스 관련 문제를 해결합니다. RPO는 장애 발생 후 정상적인 작업을 재개하기 위해 백업 저장소에서 복구해야 하는 파일의 기간에 대한 전략을 정의합니다. SLA와 RPO는 데이터 보호 전략에 기여합니다.

백업 일정은 다음과 같이 두 부분으로 구성됩니다.

- 백업 주파수

백업 빈도(백업을 수행하는 빈도)는 일부 플러그인의 경우 일정 유형이라고도 하며 정책 구성의 일부입니다. 예를 들어, 백업 빈도를 매시간, 매일, 매주 또는 매월로 구성할 수 있습니다. SnapCenter GUI에서 정책에 액세스하려면 설정 > *정책*을 클릭하세요.

- 백업 일정

백업 일정(백업을 정확히 언제 수행해야 하는지)은 리소스 또는 리소스 그룹 구성의 일부입니다. 예를 들어, 주간 백업에 대한 정책이 구성된 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 일정을 구성할 수 있습니다. SnapCenter GUI에서 리소스 그룹 일정에 액세스하려면 리소스*를 클릭한 다음 적절한 플러그인을 선택하고 *보기 > *리소스 그룹*을 클릭합니다.

필요한 백업 작업 수

필요한 백업 작업 수를 결정하는 요소에는 리소스 크기, 사용된 볼륨 수, 리소스 변경률, 서비스 수준 계약(SLA) 등이 있습니다.

일반적으로 선택하는 백업 작업의 수는 리소스를 배치한 볼륨의 수에 따라 달라집니다. 예를 들어, 한 볼륨에 작은 리소스 그룹을 배치하고 다른 볼륨에 큰 리소스를 배치한 경우 작은 리소스에 대한 백업 작업을 하나 만들고 큰 리소스에 대한 백업 작업을 하나 만들 수 있습니다.

수동으로 추가된 NetApp 지원 플러그인 리소스에 대해 지원되는 복원 전략 유형

SnapCenter 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다. 수동으로 추가된 NetApp 지원 플러그인 리소스에는 두 가지 유형의 복원 전략이 있습니다.



수동으로 추가한 NetApp 지원 플러그인 리소스는 복구할 수 없습니다.

리소스 복구 완료

- 리소스의 모든 볼륨, Qtree 및 LUN을 복원합니다.



리소스에 볼륨이나 Q트리가 포함되어 있는 경우 해당 볼륨이나 Q트리에서 복원을 위해 선택한 스냅샷 이후에 생성된 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 동일한 볼륨이나 Q트리에 다른 리소스가 호스팅되는 경우 해당 리소스도 삭제됩니다.

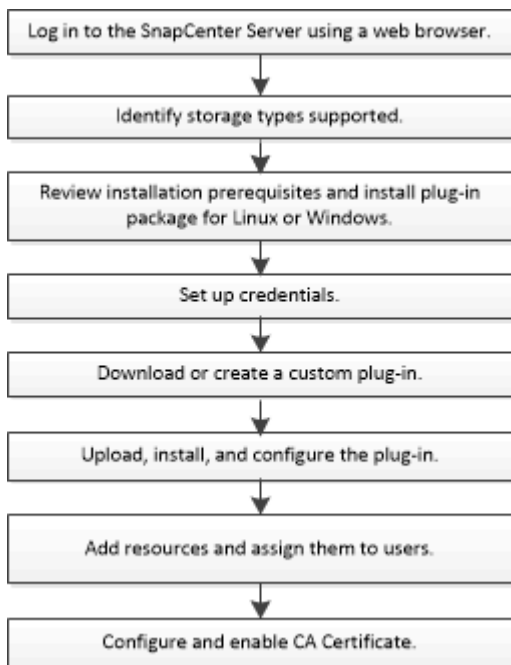
파일 수준 복원

- 볼륨, Qtree 또는 디렉토리에서 파일을 복원합니다.
- 선택된 LUN만 복원합니다.

NetApp 지원 플러그인 설치를 준비하세요

SnapCenter NetApp 지원 플러그인 설치 워크플로

NetApp 지원 플러그인 리소스를 보호하려면 SnapCenter NetApp 지원 플러그인을 설치하고 설정해야 합니다.



Windows, Linux 또는 AIX용 호스트 추가 및 플러그인 패키지 설치를 위한 전제 조건

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 충족해야 합니다. NetApp 지원 플러그인은 Windows, Linux 및 AIX 환경에서 지원됩니다.



AIX에서는 스토리지와 Oracle 애플리케이션이 지원됩니다.

- Linux, Windows 또는 AIX 호스트에 Java 11을 설치했어야 합니다.



IBM Java는 Windows 및 Linux 호스트에서 지원되지 않습니다.

- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹

사용자에 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.

- MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB 및 Storage 플러그인과 같은 NetApp 지원 플러그인은 호스트 추가 작업이 수행되는 클라이언트 호스트에서 사용할 수 있어야 합니다.

일반적인

iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.

Windows 호스트

- 원격 호스트에 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 도메인 사용자가 있어야 합니다.
- SnapCenter 에서 클러스터 노드를 관리하는 경우 클러스터의 모든 노드에 대한 관리 권한이 있는 사용자가 있어야 합니다.
- Microsoft Windows용 SnapCenter 플러그인을 수동으로 선택해야 합니다.

["Windows용 JAVA 다운로드"](#)

Linux 및 AIX 호스트



AIX에서는 스토리지와 Oracle 애플리케이션이 지원됩니다.

- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 SSH 연결을 활성화해야 합니다.
- Linux 호스트에 Java 11을 설치했어야 합니다.

SnapCenter 서버 호스트로 Windows Server 2019 또는 Windows Server 2016을 사용하는 경우 Java 11을 설치해야 합니다. 상호 운용성 매트릭스 도구(IMT)에는 요구 사항에 대한 최신 정보가 포함되어 있습니다.

["Linux용 JAVA 다운로드"](#)

["AIX용 JAVA 다운로드"](#)

["NetApp 상호 운용성 매트릭스 도구"](#)

- 루트가 아닌 사용자에게 여러 경로에 대한 액세스 권한을 제공하려면 sudo 권한을 구성해야 합니다. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 줄을 추가합니다.



Sudo 버전 1.8.7 이상을 사용하고 있는지 확인하세요.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Precchecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```

_LINUX_USER_는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

_checksum_value_는 **sc_unix_plugins_checksum.txt** 파일에서 얻을 수 있습니다. 이 파일의 위치는 다음과 같습니다.

- SnapCenter Server가 Windows 호스트에 설치된 경우 *C:\ProgramData\NetApp\ SnapCenter \Package Repository\sc_unix_plugins_checksum.txt*.
- SnapCenter 서버가 Linux 호스트에 설치되어 있는 경우 */opt/ NetApp /snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt*.



이 예제는 귀하만의 데이터를 생성하기 위한 참고자료로만 사용해야 합니다.

AIX 호스트 요구 사항

AIX용 SnapCenter 플러그인 패키지를 설치하기 전에 호스트가 요구 사항을 충족하는지 확인해야 합니다.



AIX에서는 스토리지와 Oracle 애플리케이션이 지원됩니다.



AIX용 SnapCenter 플러그인 패키지의 일부인 UNIX용 SnapCenter 플러그인은 동시 볼륨 그룹을 지원하지 않습니다.

목	요구 사항
운영 체제	AIX 7.1 이상

목	요구 사항
호스트의 SnapCenter 플러그인을 위한 최소 RAM	4GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	자바 11 IBM 자바 JAVA를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties에 있는 JAVA_HOME 옵션이 올바른 JAVA 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다.

지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "[NetApp 상호 운용성 매트릭스 도구](#)".

AIX 호스트에 대한 루트가 아닌 사용자에게 대한 **sudo** 권한 구성

SnapCenter 4.4 이상에서는 루트가 아닌 사용자도 AIX용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 루트가 아닌 사용자로 실행됩니다. 루트가 아닌 사용자에게 여러 경로에 대한 액세스 권한을 제공하려면 sudo 권한을 구성해야 합니다.

필요한 것

- Sudo 버전 1.8.7 이상.
- /etc/ssh/sshd_config 파일을 편집하여 메시지 인증 코드 알고리즘(MAC hmac-sha2-256 및 MAC hmac-sha2-512)을 구성합니다.

구성 파일을 업데이트한 후 sshd 서비스를 다시 시작합니다.

예:


```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

이 작업에 관하여

루트가 아닌 사용자에게 다음 경로에 대한 액세스를 제공하려면 sudo 권한을 구성해야 합니다.

- /home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /custom_location/ NetApp/snapcenter/spl/설치/플러그인/제거
- /custom_location/ NetApp/snapcenter/spl/bin/spl

단계

1. AIX용 SnapCenter 플러그인 패키지를 설치하려는 AIX 호스트에 로그인합니다.
2. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 줄을 추가합니다.

```
Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```



RAC 설정을 사용하는 경우 허용되는 다른 명령과 함께 다음을 `/etc/sudoers` 파일에 추가해야 합니다. `'/<crs_home>/bin/olsnodes'`

`crs_home_`의 값은 `_etc/oracle/olr.loc` 파일에서 얻을 수 있습니다.

`_AIX_USER_`는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

`_checksum_value_`는 **`sc_unix_plugins_checksum.txt`** 파일에서 얻을 수 있습니다. 이 파일의 위치는 다음과 같습니다.

- SnapCenter Server가 Windows 호스트에 설치된 경우 `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`.
- SnapCenter 서버가 Linux 호스트에 설치되어 있는 경우 `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`.



이 예제는 귀하만의 데이터를 생성하기 위한 참고자료로만 사용해야 합니다.

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항과 크기 요구 사항을 숙지해야 합니다.

목	요구 사항
운영 체제	마이크로소프트 윈도우 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.

목	요구 사항
필수 소프트웨어 패키지	• ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 • 파워셸 코어 7.4.2 • Java 11 Oracle Java 및 OpenJDK Java 11 Oracle Java 및 OpenJDK는 SAP HANA, IBM Db2, PostgreSQL, MySQL, NetApp 지원 플러그인 및 Windows 호스트에 설치할 수 있는 기타 사용자 정의 애플리케이션에만 필요합니다. 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구".

Linux 및 AIX용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Linux 또는 AIX용 SnapCenter 플러그인 패키지를 설치하기 전에 호스트가 요구 사항을 충족하는지 확인해야 합니다.



AIX에서는 스토리지와 Oracle 애플리케이션이 지원됩니다.

목	요구 사항
운영 체제	• 레드햇 엔터프라이즈 리눅스 • 오라클 리눅스 • SUSE Linux Enterprise Server(SLES)
호스트의 SnapCenter 플러그인을 위한 최소 RAM	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB 충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	Java 11 Oracle Java 또는 OpenJDK JAVA를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties에 있는 JAVA_HOME 옵션이 올바른 JAVA 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다.

지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "[NetApp 상호 운용성 매트릭스 도구](#)"

NetApp 지원 플러그인에 대한 자격 증명 설정

SnapCenter SnapCenter 작업을 위해 사용자를 인증하기 위해 자격 증명을 사용합니다. SnapCenter 플러그인을 설치하기 위한 자격 증명과 데이터베이스나 Windows 파일 시스템에서 데이터 보호 작업을 수행하기 위한 추가 자격 증명을 만들어야 합니다.

시작하기 전에

- Linux 또는 AIX 호스트

Linux 또는 AIX 호스트에 플러그인을 설치하려면 자격 증명을 설정해야 합니다.

플러그인 프로세스를 설치하고 시작하려면 루트 사용자 또는 sudo 권한이 있는 루트가 아닌 사용자의 자격 증명을 설정해야 합니다.

모범 사례: 호스트를 배포하고 플러그인을 설치한 후에도 Linux에 대한 자격 증명을 생성할 수 있지만, 가장 좋은 방법은 호스트를 배포하고 플러그인을 설치하기 전에 SVM을 추가한 후에 자격 증명을 생성하는 것입니다.

- Windows 호스트

플러그인을 설치하기 전에 Windows 자격 증명을 설정해야 합니다.

원격 호스트의 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정해야 합니다.

- NetApp 지원 플러그인 애플리케이션

플러그인은 리소스를 추가하는 동안 선택하거나 생성된 자격 증명을 사용합니다. 데이터 보호 작업 중에 리소스에 자격 증명이 필요하지 않은 경우 자격 증명을 *없음*으로 설정할 수 있습니다.

이 작업에 관하여

개별 리소스 그룹에 대한 자격 증명을 설정하고 사용자 이름에 전체 관리자 권한이 없는 경우 최소한 리소스 그룹 및 백업 권한을 사용자 이름에 할당해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *자격 증명*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 자격 증명 페이지에서 자격 증명을 구성하는 데 필요한 정보를 지정합니다.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.

이 분야에서는...	이렇게 하세요...
사용자 이름	인증에 사용할 사용자 이름과 비밀번호를 입력하세요. • 도메인 관리자 또는 관리자 그룹의 모든 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹 구성원을 지정하세요. 사용자 이름 필드에 사용할 수 있는 형식은 다음과 같습니다. ◦ <i>NetBIOS</i> 사용자 이름 ◦ 도메인 <i>FQDN</i> 사용자 이름 • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우, SnapCenter 플러그인을 설치할 시스템에 기본 제공되는 로컬 관리자를 지정하십시오. 사용자 계정에 승격된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우, 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다. <i>UserName</i>
비밀번호	인증에 사용되는 비밀번호를 입력하세요.
인증 유형	사용할 인증 유형을 선택하세요.
sudo 권한을 사용하세요	루트가 아닌 사용자에게 자격 증명을 생성하는 경우 sudo 권한 사용 확인란을 선택합니다.  Linux 및 AIX 사용자에게만 적용됩니다.

5. *확인*을 클릭합니다.

자격 증명 설정을 마친 후 사용자 및 액세스 페이지에서 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

Windows Server 2016 이상에서 gMSA 구성

Windows Server 2016 이상에서는 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 관리 서비스 계정(gMSA)을 만들 수 있습니다.

시작하기 전에

- Windows Server 2016 이상 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2016 이상 호스트가 있어야 합니다.

단계

1. gMSA의 각 개체에 대해 고유한 비밀번호를 생성하려면 KDS 루트 키를 만듭니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 다음 명령을 실행합니다. Add-KDSRootKey -EffectiveImmediately
3. gMSA를 만들고 구성하세요.
 - a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
domainName\accountName$  
.. 그룹에 컴퓨터 객체를 추가합니다.  
.. 방금 만든 사용자 그룹을 사용하여 gMSA를 만듭니다.
```

예를 들어,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 달리다 `Get-ADServiceAccount` 서비스 계정을 확인하는 명령입니다.
```

4. 호스트에서 gMSA를 구성하세요.
 - a. gMSA 계정을 사용하려는 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.
이렇게 하려면 PowerShell에서 다음 명령을 실행하세요.

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. 호스트를 다시 시작합니다.

b. PowerShell 명령 프롬프트에서 다음 명령을 실행하여 호스트에 gMSA를 설치합니다. `Install-AdServiceAccount <gMSA>`

c. 다음 명령을 실행하여 gMSA 계정을 확인하세요. `Test-AdServiceAccount <gMSA>`

5. 호스트에서 구성된 gMSA에 관리 권한을 할당합니다.

6. SnapCenter 서버에서 구성된 gMSA 계정을 지정하여 Windows 호스트를 추가합니다.

SnapCenter Server는 호스트에 선택된 플러그인을 설치하고, 플러그인 설치 중에 지정된 gMSA가 서비스 로그인 계정으로 사용됩니다.

NetApp 지원 플러그인을 설치하세요

원격 호스트에 호스트를 추가하고 플러그인 패키지를 설치합니다.

SnapCenter 호스트 추가 페이지를 사용하여 호스트를 추가한 다음 플러그인 패키지를 설치해야 합니다. 플러그인은 원격 호스트에 자동으로 설치됩니다. 개별 호스트나 클러스터에 대해 호스트를 추가하고 플러그인 패키지를 설치할 수 있습니다.

시작하기 전에

- SnapCenter 관리자 역할과 같이 플러그인 설치 및 제거 권한이 있는 역할에 할당된 사용자여야 합니다.
- 메시지 대기열 서비스가 실행 중인지 확인해야 합니다.
- 그룹 관리 서비스 계정(gMSA)을 사용하는 경우 관리자 권한으로 gMSA를 구성해야 합니다.

"사용자 지정 애플리케이션을 위해 Windows Server 2016 이상에서 그룹 관리 서비스 계정 구성"

- Windows 호스트의 경우 Windows용 SnapCenter 플러그인을 선택해야 합니다.

이 작업에 관하여

- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.
- 클러스터(WRFC)에 플러그인을 설치하면 플러그인이 클러스터의 모든 노드에 설치됩니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 선택합니다.
2. 상단에 관리되는 호스트 탭이 선택되어 있는지 확인하세요.
3. *추가*를 선택하세요.
4. 호스트 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
호스트 유형	호스트 유형을 선택하세요: • Windows • 리눅스 • 에이엑스  NetApp 지원 플러그인은 Windows, Linux, AIX 환경에서 사용할 수 있습니다.  AIX에서는 스토리지와 Oracle 애플리케이션이 지원됩니다.
호스트 이름	호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하세요. SnapCenter DNS의 적절한 구성에 달려 있습니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다. Windows 환경의 경우 IP 주소는 FQDN으로 확인되는 경우에만 신뢰할 수 없는 도메인 호스트에 대해 지원됩니다. 독립형 호스트의 IP 주소나 FQDN을 입력할 수 있습니다. SnapCenter 사용하여 호스트를 추가하고 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.
신임장	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성하세요. 자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하세요. 지정한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다.  자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

목록에서 다음 플러그인을 설치할 수 있습니다.

- 몽고디비
- ORASCPM(Oracle Applications로 표시됨)
- SAP ASE
- SAP 맥스DB
- 스토리지

6. (선택 사항) 다른 플러그인을 설치하려면 *추가 옵션*을 선택하세요.

이 분야에서는...	이렇게 하세요...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정하세요. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트 번호로 표시됩니다.  플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.
설치 경로	NetApp 지원 플러그인은 Windows 시스템이나 Linux 시스템에 설치할 수 있습니다. • Windows용 SnapCenter 플러그인 패키지의 경우 기본 경로는 C:\Program Files\ NetApp\ SnapCenter 입니다. 선택적으로 경로를 사용자 정의할 수 있습니다. • Linux용 SnapCenter 플러그인 패키지 및 AIX용 SnapCenter 플러그인 패키지의 경우 기본 경로는 다음과 같습니다. /opt/NetApp/snapcenter . 선택적으로 경로를 사용자 정의할 수 있습니다.
사전 설치 확인 건너뛰기	플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택하세요.

이 분야에서는...	이렇게 하세요...
플러그인 서비스를 실행하려면 그룹 관리 서비스 계정(gMSA)을 사용하세요.	Windows 호스트의 경우 플러그인 서비스를 실행하기 위해 그룹 관리 서비스 계정(gMSA)을 사용하려면 이 확인란을 선택합니다.  다음 형식으로 gMSA 이름을 제공하세요: domainName\accountName\$.  gMSA는 Windows용 SnapCenter 플러그인 서비스에 대한 로그인 서비스 계정으로만 사용됩니다.

7. *제출*을 선택하세요.

사전 검사 건너뛰기 확인란을 선택하지 않은 경우, 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 호스트 유효성 검사가 수행됩니다. 디스크 공간, RAM, PowerShell 버전, .NET 버전, 위치(Windows 플러그인의 경우), Java 버전(Linux 플러그인의 경우)이 최소 요구 사항을 충족하는지 검증됩니다. 최소 요구 사항을 충족하지 못하면 해당 오류 또는 경고 메시지가 표시됩니다.

오류가 디스크 공간이나 RAM과 관련된 경우 다음 위치에 있는 web.config 파일을 업데이트할 수 있습니다. C:\Program Files\NetApp\SnapCenter WebApp 기본값을 수정합니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.



HA 설정에서 SnapManager.Web.UI.dll.config를 업데이트하는 경우 두 노드에서 파일을 업데이트하고 SnapCenter 앱 풀을 다시 시작해야 합니다.

Windows 기본 경로는 다음과 같습니다. C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config

Linux 기본 경로는 다음과 같습니다.

/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config

8. 호스트 유형이 Linux인 경우 지문을 확인한 다음 *확인 및 제출*을 선택합니다.



동일한 호스트가 이전에 SnapCenter에 추가되었고 지문이 확인된 경우에도 지문 확인은 필수입니다.

9. 설치 진행 상황을 모니터링합니다.

설치별 로그 파일은 다음 위치에 있습니다. /custom_location/snapcenter/ 로그.

cmdlet을 사용하여 여러 원격 호스트에 **Linux, Windows** 또는 **AIX용 SnapCenter** 플러그인 패키지 설치

Install-SmHostPackage PowerShell cmdlet을 사용하여 Linux, Windows 또는 AIX용 SnapCenter 플러그인 패키지를 여러 호스트에 동시에 설치할 수 있습니다.

시작하기 전에

호스트를 추가하는 사용자는 해당 호스트에 대한 관리 권한이 있어야 합니다.



AIX에서는 스토리지와 Oracle 애플리케이션이 지원됩니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 Open-SmConnection cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
3. Install-SmHostPackage cmdlet과 필요한 매개변수를 사용하여 여러 호스트에 플러그인을 설치합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려는 경우 `-skipprecheck` 옵션을 사용할 수 있습니다.

4. 원격 설치를 위한 자격 증명을 입력하세요.

명령줄 인터페이스를 사용하여 **Linux** 호스트에 **NetApp** 지원 플러그인을 설치합니다.

SnapCenter 사용자 인터페이스(UI)를 사용하여 NetApp 지원 플러그인을 설치해야 합니다. 사용자 환경에서 SnapCenter UI에서 플러그인을 원격으로 설치할 수 없는 경우 명령줄 인터페이스(CLI)를 사용하여 콘솔 모드나 자동 모드로 NetApp 지원 플러그인을 설치할 수 있습니다.

단계

1. Linux용 SnapCenter 플러그인 패키지 설치 파일(snapcenter_linux_host_plugin.bin)을 C:\ProgramData\NetApp\ SnapCenter\Package Repository에서 NetApp 지원 플러그인을 설치하려는 호스트로 복사합니다.

SnapCenter 서버가 설치된 호스트에서 이 경로에 액세스할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 복사한 디렉토리로 이동합니다.
3. 플러그인을 설치하세요: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin`
`-i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address`
`-DSERVER_HTTPS_PORT=port_number_for_server`
 - -DPORT는 SMCore HTTPS 통신 포트를 지정합니다.
 - -DSERVER_IP는 SnapCenter 서버 IP 주소를 지정합니다.
 - -DSERVER_HTTPS_PORT는 SnapCenter 서버 HTTPS 포트를 지정합니다.
 - -DUSER_INSTALL_DIR은 Linux용 SnapCenter 플러그인 패키지를 설치할 디렉토리를 지정합니다.
 - _DINSTALL_LOG_NAME은 로그 파일의 이름을 지정합니다.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Add-Smhost cmdlet과 필요한 매개변수를 사용하여 SnapCenter 서버에 호스트를 추가합니다.

명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name` 을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

5. SnapCenter 에 로그인하고 UI 또는 PowerShell cmdlet을 사용하여 NetApp 지원 플러그인을 업로드합니다.

UI에서 NetApp 지원 플러그인을 업로드하려면 다음을 참조하세요. "[원격 호스트에 호스트를 추가하고 플러그인 패키지를 설치합니다.](#)" 부분.

SnapCenter cmdlet 도움말과 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

"[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

NetApp 지원 플러그인 설치 상태 모니터링

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행 상황을 모니터링할 수 있습니다. 설치가 완료되었는지 또는 문제가 있는지 확인하기 위해 설치 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 플러그인 설치 작업만 나열되도록 목록을 필터링하려면 다음을 수행합니다.
 - a. *필터*를 클릭하세요.
 - b. 선택 사항: 시작 날짜와 종료 날짜를 지정합니다.

- c. 유형 드롭다운 메뉴에서 *플러그인 설치*를 선택합니다.
 - d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
 - e. *적용*을 클릭하세요.
4. 설치 작업을 선택하고 *세부정보*를 클릭하면 작업 세부정보를 볼 수 있습니다.
 5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

CA 인증서 구성

CA 인증서 CSR 파일 생성

인증서 서명 요청(CSR)을 생성하고, 생성된 CSR을 사용하여 인증 기관(CA)에서 얻을 수 있는 인증서를 가져올 수 있습니다. 인증서에는 개인 키가 연결됩니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.



CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 정보는 다음을 참조하세요. ["CA 인증서 CSR 파일을 생성하는 방법"](#).



도메인(*.domain.company.com)이나 시스템(machine1.domain.company.com)에 대한 CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN)과 해당 호스트 이름을 CA 인증서에 명시해야 합니다. 인증서를 구매하기 전에 주체 대체 이름(SAN) 필드를 입력하여 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(*.domain.company.com)의 경우 인증서에는 해당 도메인의 모든 호스트 이름이 암묵적으로 포함됩니다.

CA 인증서 가져오기

Microsoft 관리 콘솔(MMC)을 사용하여 CA 인증서를 SnapCenter 서버와 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. Microsoft 관리 콘솔(MMC)로 이동한 다음 파일 > *스냅인 추가/제거*를 클릭합니다.
2. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
3. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
4. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > *인증서*를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 버튼으로 클릭한 다음, 모든 작업 > *가져오기*를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료하세요.

이 마법사 창에서...	다음을 수행하세요...
개인 키 가져오기	예 옵션을 선택하고 개인 키를 가져온 후 *다음*을 클릭합니다.
가져오기 파일 형식	변경하지 마세요. *다음*을 클릭하세요.
보안	내보낸 인증서에 사용할 새 비밀번호를 지정한 후 *다음*을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 *마침*을 클릭하여 가져오기를 시작합니다.



인증서 가져오기는 개인 키와 함께 제공되어야 합니다(지원되는 형식: *.pfx, *.p12, *.p7b).

7. "개인" 폴더에 대해서도 5단계를 반복합니다.

CA 인증서 지문을 받으세요

인증서 지문은 인증서를 식별하는 16진수 문자열입니다. 지문은 지문 알고리즘을 사용하여 인증서 내용으로부터 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.

- 인증서를 두 번 클릭합니다.
- 인증서 대화 상자에서 세부정보 탭을 클릭합니다.
- 필드 목록을 스크롤하여 *지문*을 클릭하세요.
- 상자에서 16진수 문자를 복사하세요.
- 16진수 사이의 공백을 제거하세요.

예를 들어, 지문이 "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b"인 경우 공백을 제거하면 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.

- 다음 명령을 실행하여 설치된 인증서의 지문을 나열하고 주체 이름으로 최근에 설치된 인증서를 식별합니다.

```
Get-ChildItem -경로 인증서:\LocalMachine\My
```

- 지문을 복사하세요.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서 구성

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스로 CA 인증서를 구성해야 합니다.

SnapCenter 서버와 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하는 기존 인증서 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

예를 들어:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스에 바인딩합니다.
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

예를 들어:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Linux 호스트에서 NetApp 지원 플러그인 서비스에 대한 CA 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 `_opt/ NetApp/snapcenter/scc/etc_`에 위치한 'keystore.jks' 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 CA 서명 키 쌍의 플러그인 키 저장소 및 별칭에 대한 비밀번호 관리

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 'KEYSTORE_PASS' 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

```
keytool -storepasswd -keystore keystore.jks
```

. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

agent.properties 파일의 KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

3. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 있는 폴더로 이동합니다: /opt/ NetApp/snapcenter/scc/etc.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키스토어 /opt/ NetApp/snapcenter/scc/etc가 포함된 폴더로 이동합니다.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```


4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.

7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 agent.properties 파일의 KEYSTORE_PASS 키 값입니다.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자("*", ",", ")가 포함된 경우 별칭 이름을 간단한 이름으로 변경합니다.

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. agent.properties 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

8. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 'opt/ NetApp/snapcenter/scc/etc/crl'입니다.

단계

1. agent.properties 파일에서 기본 디렉토리를 CRL_PATH 키에 맞춰 수정하고 업데이트할 수 있습니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

Windows 호스트에서 **NetApp** 지원 플러그인 서비스에 대한 **CA** 인증서 구성

플러그인 키스토어와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SnapCenter 플러그인 서비스를 사용하여 플러그인 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

플러그인은 C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_에 있는 _keystore.jks 파일을 신뢰 저장소와 키 저장소로 사용합니다.

단계

1. 플러그인 에이전트 속성 파일에서 플러그인 키스토어 기본 비밀번호를 검색할 수 있습니다.

이는 `KEYSTORE_PASS` 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

키툴 -스토어패스워드 -키스토어 키스토어.jks



Windows 명령 프롬프트에서 "keytool" 명령을 인식하지 못하는 경우 keytool 명령을 해당 전체 경로로 바꾸세요.

`C:\Program Files\Java\<jdk_버전>\bin\keytool.exe" -storepasswd -keystore keystore.jks`

3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.

키툴 -키패스워드 -별칭 "인증서의 별칭_이름" -키스토어 키스토어.jks

`agent.properties` 파일의 `KEYSTORE_PASS` 키에 대해서도 동일하게 업데이트합니다.

4. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



플러그인 키스토어의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

플러그인 신뢰 저장소에 루트 또는 중간 인증서 구성

플러그인 trust-store에 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc`
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

`keytool -list -v -keystore keystore.jks`

4. 루트 또는 중간 인증서를 추가합니다.

`keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks`

5. 플러그인 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

플러그인 신뢰 저장소에 **CA** 서명 키 쌍 구성

CA 서명 키 쌍을 플러그인 신뢰 저장소에 구성해야 합니다.

단계

1. 플러그인 키 저장소가 포함된 폴더로 이동합니다. *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. *keystore.jks* 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
키툴 -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -  
대상키스토어 keystore.jks -대상키스토어 유형 JKS
```

5. 키스토어에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

6. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 플러그인 키 저장소 비밀번호는 *agent.properties* 파일의 *KEYSTORE_PASS* 키 값입니다.

```
키툴 -키패스워드 -별칭 "CA_인증서의_별칭_이름" -키스토어 키스토어.jks
```

8. *agent.properties* 파일에서 CA 인증서의 별칭 이름을 구성합니다.

이 값을 *SCC_CERTIFICATE_ALIAS* 키에 대해 업데이트합니다.

9. CA 서명 키 쌍을 플러그인 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

SnapCenter 플러그인에 대한 인증서 해지 목록(CRL) 구성

이 작업에 관하여

- 관련 CA 인증서에 대한 최신 CRL 파일을 다운로드하려면 다음을 참조하세요. "[SnapCenter CA 인증서에서 인증서 해지 목록 파일을 업데이트하는 방법](#)".
- SnapCenter 플러그인은 미리 구성된 디렉토리에서 CRL 파일을 검색합니다.
- SnapCenter 플러그인의 CRL 파일에 대한 기본 디렉토리는 *_C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl_*입니다.

단계

1. *agent.properties* 파일에서 기본 디렉토리를 *CRL_PATH* 키에 맞춰 수정하고 업데이트할 수 있습니다.
2. 이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다.

수신 인증서는 각 CRL에 대해 검증됩니다.

플러그인에 대한 CA 인증서 활성화

CA 인증서를 구성하고 SnapCenter 서버와 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- `Set-SmCertificateSettings` cmdlet을 실행하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- `_Get-SmCertificateSettings_`를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 하나 또는 여러 개의 플러그인 호스트를 선택하세요.
4. *추가 옵션*을 클릭하세요.
5. *인증서 검증 사용*을 선택합니다.

당신이 완료한 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- *  *는 CA 인증서가 활성화되지 않았거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- *  *는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- *  *는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- *  *는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

데이터 보호를 준비하세요

NetApp 지원 플러그인을 사용하기 위한 전제 조건

SnapCenter NetApp 지원 플러그인을 사용하기 전에 SnapCenter 관리자가 SnapCenter 서버를 설치하고 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다.
- SnapCenter 서버에 로그인합니다.
- 해당되는 경우 스토리지 시스템 연결을 추가하고 자격 증명을 생성하여 SnapCenter 환경을 구성합니다.
- 호스트를 추가하고 플러그인을 설치하여 업로드합니다.
- 해당되는 경우 플러그인 호스트에 Java 11을 설치합니다.

- 여러 데이터 경로(LIF) 또는 dNFS 구성이 있는 경우 데이터베이스 호스트에서 SnapCenter CLI를 사용하여 다음을 수행할 수 있습니다.
 - 기본적으로 데이터베이스 호스트의 모든 IP 주소는 복제된 볼륨의 스토리지 가상 머신(SVM)에 있는 NFS 스토리지 내보내기 정책에 추가됩니다. 특정 IP 주소를 사용하거나 IP 주소의 하위 집합으로 제한하려면 Set-PreferredHostIPsInStorageExportPolicy CLI를 실행하세요.
 - SVM에 여러 개의 데이터 경로(LIF)가 있는 경우 SnapCenter NFS 복제 볼륨을 마운트하기 위해 적절한 데이터 경로(LIF)를 선택합니다. 하지만 특정 데이터 경로(LIF)를 지정하려면 Set-SvmPreferredDataPath CLI를 실행해야 합니다. 명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 명령 참조 가이드](#)".
- 백업 복제가 필요한 경우 SnapMirror와 SnapVault 설정하세요.
- 호스트의 다른 애플리케이션이 포트 9090을 사용하지 않는지 확인하세요.

포트 9090은 SnapCenter에 필요한 다른 포트 외에도 NetApp 지원 플러그인에서 사용하도록 예약해야 합니다.

NetApp 지원 플러그인 리소스를 보호하기 위해 리소스, 리소스 그룹 및 정책이 사용되는 방식

SnapCenter 사용하기 전에 수행하려는 백업, 복제 및 복원 작업과 관련된 기본 개념을 이해하는 것이 좋습니다. 다양한 작업을 위해 리소스, 리소스 그룹 및 정책과 상호 작용합니다.

- 리소스는 일반적으로 SnapCenter로 백업하거나 복제하는 데이터베이스, Windows 파일 시스템 또는 VM입니다.
- SnapCenter 리소스 그룹은 호스트 또는 클러스터의 리소스 모음입니다.

리소스 그룹에서 작업을 수행하면 리소스 그룹에 대해 지정한 일정에 따라 리소스 그룹에 정의된 리소스에서 해당 작업이 수행됩니다.

필요에 따라 단일 리소스나 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 수행할 수도 있습니다.

- 정책은 백업 빈도, 사본 보존, 복제, 스크립트 및 데이터 보호 작업의 기타 특성을 지정합니다.

리소스 그룹을 만들 때 해당 그룹에 대한 하나 이상의 정책을 선택합니다. 단일 리소스에 대해 주문형 백업을 수행할 때 정책을 선택할 수도 있습니다.

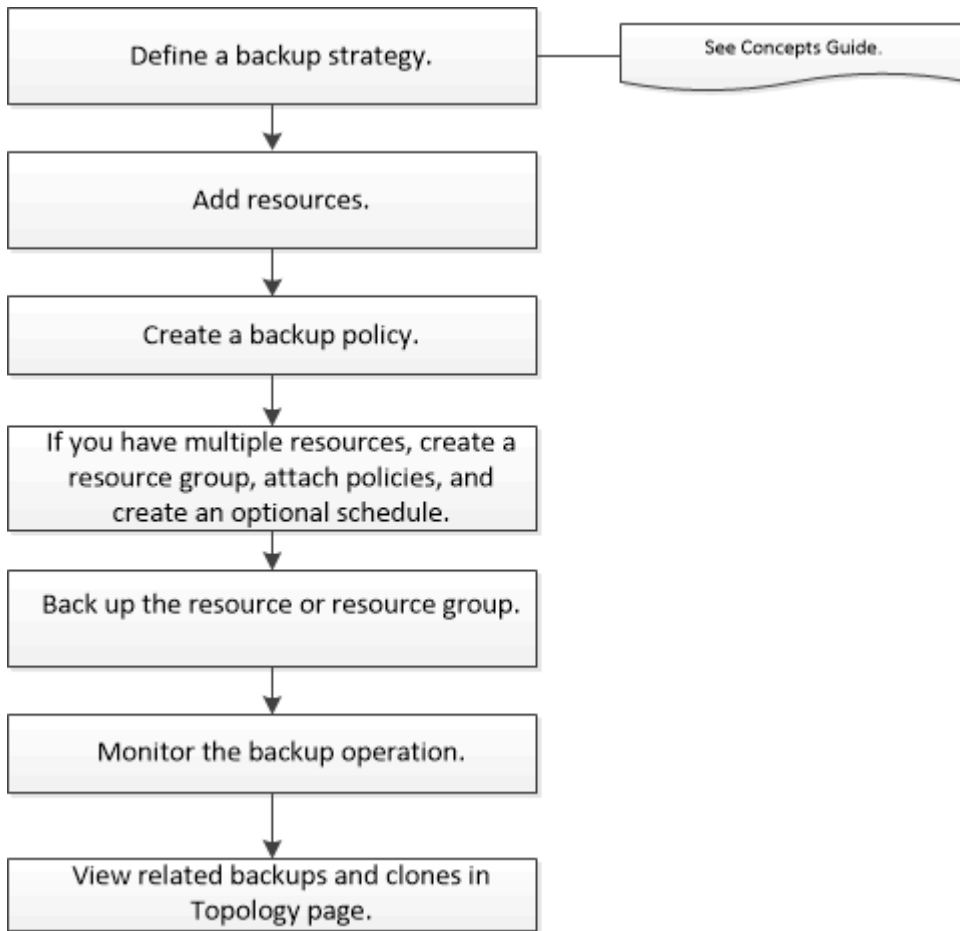
리소스 그룹은 보호하려는 내용과 보호하려는 날짜와 시간을 정의하는 것으로 생각하면 됩니다. 정책이란 그것을 어떻게 보호할 것인지를 정의하는 것이라고 생각하세요. 예를 들어, 호스트의 모든 데이터베이스나 모든 파일 시스템을 백업하는 경우 호스트의 모든 데이터베이스나 모든 파일 시스템을 포함하는 리소스 그룹을 만들 수 있습니다. 그런 다음 리소스 그룹에 일일 정책과 시간별 정책이라는 두 가지 정책을 첨부할 수 있습니다. 리소스 그룹을 만들고 정책을 첨부할 때 리소스 그룹을 구성하여 파일 기반 백업을 매일 수행하고 스냅샷 기반 백업을 매시간 수행하는 일정을 설정할 수 있습니다.

NetApp 지원 플러그인 리소스 백업

NetApp 지원 플러그인 리소스 백업

백업 워크플로에는 계획, 백업 리소스 식별, 백업 정책 관리, 리소스 그룹 생성 및 정책 연결, 백업 생성, 작업 모니터링이 포함됩니다.

다음 워크플로는 백업 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 다음을 참조하세요. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#)

NetApp 지원 플러그인에 리소스 추가

백업하거나 복제할 리소스를 추가해야 합니다. 환경에 따라 리소스는 백업 또는 복제하려는 데이터베이스 인스턴스나 컬렉션일 수 있습니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 생성, 자격 증명 추가 등의 작업을 완료했어야 합니다.
- SnapCenter 서버에 플러그인을 업로드해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *리소스 추가*를 선택합니다.
3. 리소스 세부 정보 제공 페이지에서 다음 작업을 수행합니다.

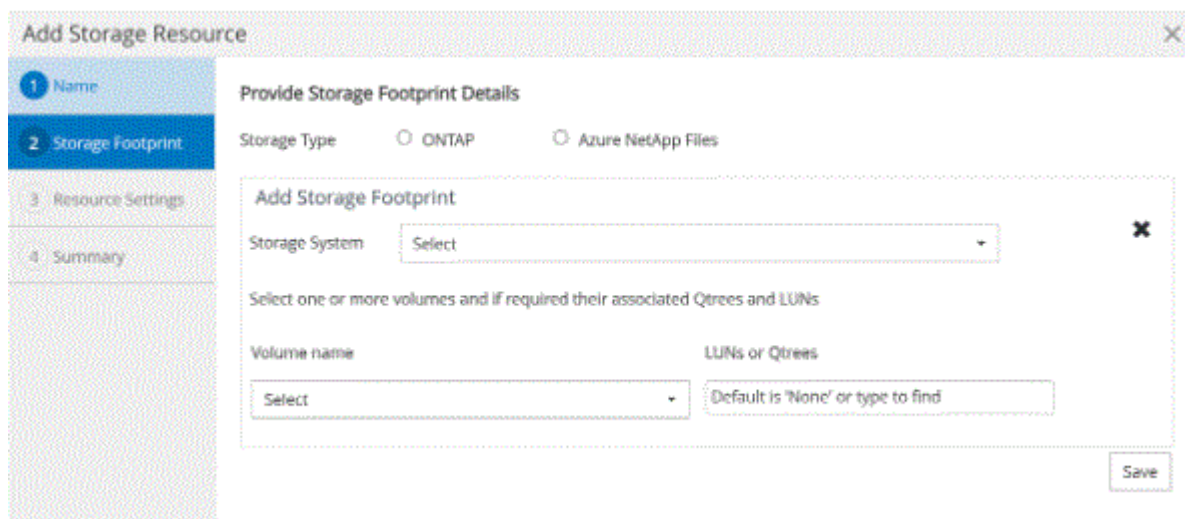
이 분야에서는...	이렇게 하세요...
이름	리소스의 이름을 입력하세요.
호스트 이름	호스트를 선택하세요.
유형	유형을 선택하세요. 유형은 플러그인 설명 파일에 따라 사용자가 정의합니다. 예를 들어, 데이터베이스와 인스턴스. 선택한 유형에 상위 항목이 있는 경우 상위 항목의 세부 정보를 입력하세요. 예를 들어, 유형이 데이터베이스이고 부모가 인스턴스인 경우 인스턴스의 세부 정보를 입력합니다.
자격 증명 이름	자격 증명을 선택하거나 새 자격 증명을 만듭니다.
산길	리소스가 마운트되는 마운트 경로를 입력하세요. 이는 Windows 호스트에만 적용됩니다.

4. 스토리지 공간 제공 페이지에서 스토리지 시스템을 선택하고 하나 이상의 볼륨, LUN, Qtree를 선택한 다음 *저장*을 선택합니다.

선택 사항: 다음을 선택하세요.  다른 스토리지 시스템에서 볼륨, LUN, Qtree를 추가하려면 아이콘을 클릭합니다.



NetApp 지원하는 플러그인은 리소스의 자동 검색을 지원하지 않습니다. 물리적 환경과 가상 환경의 저장 세부 정보도 자동으로 검색되지 않습니다. 리소스를 생성하는 동안 물리적 환경과 가상 환경에 대한 저장 정보를 제공해야 합니다.



5. 리소스 설정 페이지에서 리소스에 대한 사용자 지정 키-값 쌍을 제공합니다.



사용자 정의 키 이름이 대문자인지 확인하세요.

Custom key-value pairs for MySQL plug-in

Name	Value	
HOST	localhost	✕
PORT	3306	✕
MASTER_SLAVE	NO	+ ✕

각 플러그인 매개변수에 대해서는 다음을 참조하세요. "[리소스를 구성하기 위한 매개변수](#)"

6. 요약을 검토한 후 *마침*을 선택하세요.

결과

리소스는 유형, 호스트 또는 클러스터 이름, 연관된 리소스 그룹 및 정책, 전반적인 상태와 같은 정보와 함께 표시됩니다.



SnapCenter 외부에서 데이터베이스 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

당신이 완료한 후

다른 사용자에게 자산에 대한 액세스 권한을 제공하려면 SnapCenter 관리자가 해당 사용자에게 자산을 할당해야 합니다. 이를 통해 사용자는 자신에게 할당된 자산에 대해 권한이 있는 작업을 수행할 수 있습니다.

리소스를 추가한 후 리소스 세부 정보를 수정할 수 있습니다. NetApp 지원 플러그인 리소스에 백업이 연결되어 있는 경우 리소스 이름, 리소스 유형, 호스트 이름 필드는 수정할 수 없습니다.

리소스를 구성하기 위한 매개변수

플러그인을 수동으로 추가하는 경우 다음 매개변수를 사용하여 리소스 설정 페이지에서 리소스를 구성할 수 있습니다.

MongoDB용 플러그인

리소스 설정:

- MONGODB_APP_SERVER=(샤드 클러스터 리소스 유형의 경우) 또는 MONGODB_REPLICASET_SERVER=(레플리카 세트 리소스 유형의 경우)
- OPLOG_PATH=(MongoDB.propertiesfile에서 제공되는 경우 선택적 매개변수)
- MONGODB_AUTHENTICATION_TYPE= (LDAP 인증의 경우 PLAIN, 기타의 경우 None)

MongoDB.properties 파일에 다음 매개변수를 제공해야 합니다.

- 서비스_시작_중지_비활성화=
 - 플러그인이 시작/중지 서비스를 수행하는 경우 N입니다.
 - 사용자가 시작/중지 서비스를 수행하는 경우 Y입니다.
 - 기본값인 선택적 매개변수는 N으로 설정됩니다.
- OPLOG_PATH_= (SnapCenter 에서 사용자 정의 키-값 쌍으로 이미 제공된 경우의 선택적 매개변수).

MaxDB용 플러그인

리소스 설정:

- XUSER_ENABLE(Y|N)은 데이터베이스 사용자에게 대한 암호가 필요하지 않도록 MaxDB에 대한 xuser 사용을 활성화하거나 비활성화합니다.
- HANDLE_LOGWRITER(Y|N)는 일시 중단 로그 작성기(N) 또는 재개 로그 작성기(Y) 작업을 실행합니다.
- DBMCLICMD(path_to_dbmcli_cmd)는 MaxDB dbmcli 명령의 경로를 지정합니다. 설정하지 않으면 검색 경로의 dbmcli가 사용됩니다.



Windows 환경의 경우 경로는 큰따옴표("...")로 묶어야 합니다.

- SQLCLICMD(path_to_sqlcli_cmd)는 MaxDB sqlcli 명령의 경로를 지정합니다. 경로가 설정되지 않으면 검색 경로에서 sqlcli가 사용됩니다.
- MAXDB_UPDATE_HIST_LOG(Y|N)는 MaxDB 백업 프로그램에 MaxDB 기록 로그를 업데이트해야 하는지 여부를 지시합니다.
- MAXDB_CHECK_SNAPSHOT_DIR: 예: SID1:directory[,directory...]; [SID2:directory[,directory...]]는 Snap Creator 스냅샷 복사 작업이 성공했는지 확인하고 스냅샷이 생성되었는지 확인합니다.

이는 NFS에만 적용됩니다. 해당 디렉토리는 .snapshot 디렉토리가 포함된 위치를 가리켜야 합니다. 여러 개의 디렉토리를 쉼표로 구분된 목록에 포함할 수 있습니다.

MaxDB 7.8 이상 버전에서는 데이터베이스 백업 요청이 백업 기록에 실패로 표시됩니다.

- MAXDB_BACKUP_TEMPLATES: 각 데이터베이스에 대한 백업 템플릿을 지정합니다.

템플릿은 반드시 존재해야 하며 외부 유형의 백업 템플릿이어야 합니다. MaxDB 7.8 이상에서 스냅샷 통합을 활성화하려면 MaxDB 백그라운드 서버 기능이 있어야 하며 EXTERNAL 유형의 MaxDB 백업 템플릿이 이미 구성되어 있어야 합니다.

- MAXDB_BG_SERVER_PREFIX: 백그라운드 서버 이름의 접두사를 지정합니다.

MAXDB_BACKUP_TEMPLATES 매개변수가 설정된 경우 MAXDB_BG_SERVER_PREFIX 매개변수도 설정해야 합니다. 접두사를 설정하지 않으면 기본값 na_bg_가 사용됩니다.

SAP ASE용 플러그인

리소스 설정:

- SYBASE_SERVER(data_server_name)은 Sybase 데이터 서버 이름을 지정합니다(isql 명령의 -S 옵션). 예를 들어, p_test.
- SYBASE_DATABASES_EXCLUDE(db_name)을 사용하면 "ALL" 구문을 사용하는 경우 데이터베이스를 제외할 수 있습니다.

세미콜론으로 구분된 목록을 사용하여 여러 데이터베이스를 지정할 수 있습니다. 예를 들어: pubs2;test_db1.

- SYBASE_USER: user_name은 isql 명령을 실행할 수 있는 운영 체제 사용자를 지정합니다.

UNIX에 필요합니다. Snap Creator Agent 시작 및 중지 명령을 실행하는 사용자(일반적으로 루트 사용자)와 isql 명령을 실행하는 사용자가 다른 경우 이 매개변수가 필요합니다.

- SYBASE_TRAN_DUMP db_name:directory_path를 사용하면 스냅샷을 생성한 후 Sybase 트랜잭션 덤프를 수행할 수 있습니다. 예를 들어, pubs2:/sybasedumps/ pubs2

트랜잭션 덤프가 필요한 각 데이터베이스를 지정해야 합니다.

- SYBASE_TRAN_DUMP_COMPRESS (Y|N)는 기본 Sybase 트랜잭션 덤프 압축을 활성화하거나 비활성화합니다.
- SYBASE_ISQL_CMD(예: /opt/sybase/OCS-15_0/bin/isql)는 isql 명령의 경로를 정의합니다.
- SYBASE_EXCLUDE_TEMPDB(Y|N)를 사용하면 사용자가 생성한 임시 데이터베이스를 자동으로 제외할 수 있습니다.

Oracle 애플리케이션용 플러그인(ORASCPM)

리소스 설정:

- SQLPLUS_CMD는 SQLplus의 경로를 지정합니다.
- ORACLE_DATABASES는 백업할 Oracle 데이터베이스와 해당 사용자(database:user)를 나열합니다.
- CNTL_FILE_BACKUP_DIR은 제어 파일 백업을 위한 디렉토리를 지정합니다.
- ORA_TEMP는 임시 파일의 디렉토리를 지정합니다.
- ORACLE_HOME은 Oracle 소프트웨어가 설치된 디렉토리를 지정합니다.
- ARCHIVE_LOG_ONLY는 보관 로그를 백업할지 여부를 지정합니다.
- ORACLE_BACKUPMODE는 온라인 백업을 수행할지, 오프라인 백업을 수행할지 지정합니다.
- ORACLE_EXPORT_PARAMETERS는 `_bin/su <user running sqlplus> -c sqlplus /nolog <cmd> _`를 실행하는 동안 위에 정의된 환경 변수를 다시 내보내야 하는지 여부를 지정합니다. 이는 일반적으로 sqlplus를 실행하는 사용자가 `_connect / as sysdba_`를 사용하여 데이터베이스에 연결하는 데 필요한 모든 환경 변수를 설정하지 않은 경우에 발생합니다.

NetApp 지원 플러그인 리소스에 대한 정책 생성

SnapCenter 사용하여 NetApp 지원 플러그인 특정 리소스를 백업하기 전에 백업하려는 리소스 또는 리소스 그룹에 대한 백업 정책을 만들어야 합니다.

시작하기 전에

- 백업 전략을 정의했어야 합니다.

자세한 내용은 NetApp 지원 플러그인에 대한 데이터 보호 전략 정의에 대한 정보를 참조하세요.

- 데이터 보호를 위해 준비를 해야 했습니다.

데이터 보호를 준비하려면 SnapCenter 설치, 호스트 추가, 스토리지 시스템 연결 생성, 리소스 추가 등의 작업이 필요합니다.

- 미러링 또는 볼트 작업을 위해 스토리지 가상 머신(SVM)을 할당해야 합니다.

스냅샷을 미리 또는 볼트에 복제하는 경우 SnapCenter 관리자가 소스 및 대상 볼륨 모두에 대한 SVM을 할당해야 합니다.

- 보호하려는 리소스를 수동으로 추가했어야 합니다.

이 작업에 관하여

- 백업 정책은 백업을 관리, 일정을 정하고 보관하는 방법을 규정하는 일련의 규칙입니다. 또한 복제, 스크립트 및 애플리케이션 설정을 지정할 수 있습니다.
- 정책에서 옵션을 지정하면 다른 리소스 그룹에 정책을 재사용할 때 시간을 절약할 수 있습니다.
- SnapLock
 - '특정 기간 동안 백업 사본을 보관합니다' 옵션을 선택한 경우 SnapLock 보관 기간은 언급된 보관 기간보다 짧거나 같아야 합니다.
 - 스냅샷 잠금 기간을 지정하면 보존 기간이 만료될 때까지 스냅샷이 삭제되지 않습니다. 이를 통해 정책에 지정된 수보다 더 많은 수의 스냅샷을 보존할 수 있습니다.
 - ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.



기본 SnapLock 설정은 SnapCenter 백업 정책에서 관리되고 보조 SnapLock 설정은 ONTAP 에서 관리됩니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *정책*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 이름 페이지에서 정책 이름과 세부 정보를 입력합니다.
5. 정책 유형 페이지에서 다음을 수행합니다.
 - a. 저장 유형을 선택하세요.
 - b. 사용자 정의 백업 설정 섹션에서 플러그인에 키-값 형식으로 전달해야 하는 특정 백업 설정을 제공합니다.

플러그인에 전달할 여러 개의 키-값을 제공할 수 있습니다.

6. 스냅샷 및 복제 페이지에서 다음 단계를 수행합니다.

- a. 주문형, 시간별, 일별, 주별 또는 *월별*을 선택하여 일정 유형을 지정합니다.



리소스 그룹을 생성하는 동안 백업 작업에 대한 일정(시작 날짜, 종료 날짜, 빈도)을 지정할 수 있습니다. 이를 통해 동일한 정책과 백업 빈도를 공유하는 리소스 그룹을 만들 수 있지만, 각 정책에 다른 백업 일정을 할당할 수도 있습니다.



오전 2시로 예약한 경우, 일광 절약 시간제(DST) 기간에는 일정이 실행되지 않습니다.

- a. 스냅샷 설정 섹션에서 백업 유형 페이지에서 선택한 백업 유형과 일정 유형에 대한 보존 설정을 지정합니다.

만약 당신이 원한다면...	그 다음에...
특정 수의 스냅샷을 보관하세요	*보관할 사본*을 선택한 다음 보관하려는 스냅샷 수를 지정합니다. 스냅샷 수가 지정된 수를 초과하면 스냅샷이 삭제되고 가장 오래된 사본이 먼저 삭제됩니다.  SnapVault 복제를 활성화하려면 보존 횟수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷이 대상에 복제될 때까지 첫 번째 스냅샷이 SnapVault 관계에 대한 참조 스냅샷이 되기 때문에 보존 작업이 실패할 수 있습니다.  최대 보존 값은 1018입니다. 보존 기간이 기본 ONTAP 버전에서 지원하는 것보다 높은 값으로 설정된 경우 백업이 실패합니다.
스냅샷을 특정 일수 동안 보관하세요	*사본 보관 기간*을 선택한 다음, 스냅샷을 삭제하기 전에 보관할 일수를 지정합니다.
스냅샷 복사 잠금 기간	*스냅샷 복사 잠금 기간*을 선택하고 일, 월 또는 년을 지정합니다. SnapLock 보존 기간은 100년 미만이어야 합니다.

b. 정책 라벨을 선택하세요.



원격 복제를 위해 기본 스냅샷에 SnapMirror 레이블을 할당하면 기본 스냅샷이 SnapCenter에서 ONTAP 보조 시스템으로 스냅샷 복제 작업을 오프로드할 수 있습니다. 정책 페이지에서 SnapMirror 또는 SnapVault 옵션을 활성화하지 않고도 이 작업을 수행할 수 있습니다.

7. 보조 복제 옵션 선택 섹션에서 다음 보조 복제 옵션 중 하나 또는 둘 다를 선택합니다.

이 분야에서는...	이렇게 하세요...
로컬 스냅샷 복사본을 만든 후 SnapMirror 업데이트	다른 볼륨에 백업 세트의 미러 복사본을 생성하려면 이 필드를 선택합니다(SnapMirror 복제). ONTAP의 보호 관계가 미러 및 볼트 유형이고 이 옵션만 선택하는 경우, 기본에서 생성된 스냅샷은 대상으로 전송되지 않지만 대상에는 나열됩니다. 대상에서 이 스냅샷을 선택하여 복원 작업을 수행하는 경우 다음 오류 메시지가 표시됩니다. 선택한 보관/미러링 백업에 보조 위치를 사용할 수 없습니다. 2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고침됩니다. 보다 "토폴로지 페이지에서 NetApp 지원 플러그인 리소스 관련 백업 및 복제본 보기".
로컬 스냅샷 복사본을 만든 후 SnapVault 업데이트	디스크 간 백업 복제(SnapVault 백업)를 수행하려면 이 옵션을 선택하세요. 2차 복제 중에 SnapLock 만료 시간은 기본 SnapLock 만료 시간을 로드합니다. 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP에서 검색된 보조 및 기본 SnapLock 만료 시간이 새로 고침됩니다. ONTAP에서 SnapLock Vault로 알려진 보조 노드에만 SnapLock 구성된 경우 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP에서 검색된 보조 노드의 잠금 기간이 새로 고침됩니다. SnapLock Vault에 대한 자세한 내용은 볼트 대상의 WORM에 스냅샷 커밋을 참조하세요. 보다 "토폴로지 페이지에서 NetApp 지원 플러그인 리소스 관련 백업 및 복제본 보기".
오류 재시도 횟수	작업이 중지되기 전에 허용할 수 있는 최대 복제 시도 횟수를 입력하세요.



보조 저장소의 스냅샷 최대 한도에 도달하지 않도록 하려면 ONTAP에서 보조 저장소 SnapMirror 보존 정책을 구성해야 합니다.

8. 요약 검토한 후 *마침*을 클릭하세요.

리소스 그룹을 만들고 정책을 첨부합니다.

리소스 그룹은 백업하고 보호하려는 리소스를 추가해야 하는 컨테이너입니다. 이를 통해 특정 애플리케이션과 관련된 모든 데이터를 동시에 백업할 수 있습니다. 또한, 수행하려는 데이터 보호 작업 유형을 정의하려면 리소스 그룹에 하나 이상의 정책을 연결해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 새 리소스 그룹을 선택합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	리소스 그룹의 이름을 입력하세요. 참고: 리소스 그룹 이름은 250자를 넘을 수 없습니다.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력하세요. 예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.
스냅샷 복사에 사용자 정의 이름 형식 사용	이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다. 예를 들어, <code>_customtext_resource_group_policy_hostname</code> 또는 <code>resource_group_hostname</code> 입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

4. 선택 사항: 리소스 페이지에서 호스트 드롭다운 목록에서 호스트 이름을 선택하고 리소스 유형 드롭다운 목록에서 리소스 유형을 선택합니다.

이는 화면에 표시되는 정보를 필터링하는 데 도움이 됩니다.

5. 사용 가능한 리소스 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 선택하여 선택한 리소스 섹션으로 이동합니다.
6. 선택 사항: 애플리케이션 설정 페이지에서 다음을 수행합니다.

- a. 추가 백업 옵션을 설정하려면 백업 화살표를 선택하세요.

일관성 그룹 백업을 활성화하고 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
일관성 그룹 스냅샷 작업이 완료될 때까지 기다릴 시간을 확보하세요.	스냅샷 작업이 완료될 때까지의 대기 시간을 지정하려면 긴급, 보통 또는 느긋함을 선택합니다. 긴급 = 5초, 보통 = 7초, 여유 = 20초.
WAFL 동기화 비활성화	WAFL 일관성 지점을 강제로 적용하지 않으려면 이 옵션을 선택하세요.

+

- 스크립트 화살표를 선택하고 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령을 입력합니다. 실패 시 종료하기 전에 실행할 사전 명령을 입력할 수도 있습니다.
- 사용자 정의 구성 화살표를 선택하고 이 리소스를 사용하는 모든 데이터 보호 작업에 필요한 사용자 정의 키-값 쌍을 입력합니다.

매개변수	환경	설명
아카이브 로그 활성화	(예/아니요)	보관 로그 관리를 통해 보관 로그를 삭제할 수 있습니다.
아카이브 로그 보존	일수	보관 로그를 보관하는 일수를 지정합니다. 이 설정은 NTAP_SNAPSHOT_RETENTIONS보다 크거나 같아야 합니다.

매개변수	환경	설명
아카이브_로그_디렉토리	변경_정보_디렉토리/로그	보관 로그가 포함된 디렉토리의 경로를 지정합니다.
아카이브_로그_확장	파일 확장자	보관 로그 파일 확장자 길이를 지정합니다. 예를 들어, 보관 로그가 log_backup_0_0_0_0.161518551942 9이고 file_extension 값이 5이면 로그 확장자는 5자리인 16151을 유지합니다.
ARCHIVE_LOG_RECURSIVE_SE ARCH	(예/아니요)	하위 디렉토리 내의 보관 로그 관리를 활성화합니다. 보관 로그가 하위 디렉토리에 있는 경우 이 매개변수를 사용해야 합니다.

c. 스냅샷 복사 도구* 화살표를 선택하여 스냅샷을 만드는 도구를 선택하세요.

원하신다면...	그 다음에...
SnapCenter Windows용 플러그인을 사용하여 스냅샷을 만들기 전에 파일 시스템을 일관된 상태로 만듭니다. Linux 리소스의 경우 이 옵션은 적용되지 않습니다.	*파일 시스템 일관성을 갖춘 SnapCenter *를 선택하세요. 이 옵션은 SAP HANA 데이터베이스용 SnapCenter 플러그인에는 적용되지 않습니다.
SnapCenter 사용하여 스토리지 수준 스냅샷을 생성합니다.	*파일 시스템 일관성이 없는 SnapCenter *를 선택하세요.
스냅샷을 생성하기 위해 호스트에서 실행할 명령을 입력합니다.	*기타*를 선택한 다음 호스트에서 실행할 명령을 입력하여 스냅샷을 만듭니다.

7. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



*를 선택하여 정책을 생성할 수도 있습니다. *.

정책은 선택한 정책에 대한 일정 구성 섹션에 나열되어 있습니다.

b. 일정 구성 열에서 *를 선택하세요. * 구성하려는 정책에 대해.

c. 정책 _policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성하고 확인을 선택합니다.

여기서 policy_name은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다. 타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP 서버는 설정 > *전역 설정*에서 구성해야 합니다.

9. 요약 검토한 후 *마침*을 선택하세요.

ASA r2 시스템의 리소스에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.

ASA r2 시스템에 있는 리소스를 추가하려면 리소스 그룹을 만들어야 합니다. 리소스 그룹을 생성하는 동안 보조 보호를 프로비저닝할 수도 있습니다.

시작하기 전에

- ONTAP 9.x 리소스와 ASA r2 리소스를 동일한 리소스 그룹에 추가하지 않도록 해야 합니다.
- ONTAP 9.x 리소스와 ASA r2 리소스가 모두 포함된 데이터베이스가 없는지 확인해야 합니다.

이 작업에 관하여

- 2차 보호는 로그인한 사용자에게 **SecondaryProtection** 기능이 활성화된 역할이 할당된 경우에만 사용할 수 있습니다.
- 2차 보호를 활성화한 경우 기본 및 2차 일관성 그룹을 생성하는 동안 리소스 그룹은 유지 관리 모드로 전환됩니다. 기본 및 보조 일관성 그룹이 생성된 후 리소스 그룹은 유지 관리 모드에서 해제됩니다.
- SnapCenter 클론 리소스에 대한 보조 보호를 지원하지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.
 - a. 이름 필드에 리소스 그룹의 이름을 입력합니다.



리소스 그룹 이름은 250자를 넘을 수 없습니다.

- b. 나중에 리소스 그룹을 검색하는 데 도움이 되도록 태그 필드에 하나 이상의 레이블을 입력하세요.

예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.

- c. 이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

- d. 백업하지 않을 보관 로그 파일의 대상을 지정합니다.



필요한 경우 접두사를 포함하여 애플리케이션에 설정된 것과 정확히 동일한 목적지를 사용해야 합니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 데이터베이스 호스트 이름을 선택합니다.



리소스가 성공적으로 검색된 경우에만 해당 리소스가 사용 가능한 리소스 섹션에 나열됩니다. 최근에 리소스를 추가한 경우 리소스 목록을 새로 고친 후에만 사용 가능한 리소스 목록에 표시됩니다.

5. 사용 가능한 리소스 섹션에서 ASA r2 리소스를 선택하고 선택한 리소스 섹션으로 이동합니다.

6. 애플리케이션 설정 페이지에서 백업 옵션을 선택하세요.

7. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



또한 다음을 클릭하여 정책을 생성할 수도 있습니다.  .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.

c. 정책 `_policy_name_`에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 `_policy_name_`은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 선택한 정책에 대해 보조 보호가 활성화된 경우 보조 보호 페이지가 표시되며 다음 단계를 수행해야 합니다.

a. 복제 정책의 유형을 선택하세요.



동기 복제 정책은 지원되지 않습니다.

b. 사용할 일관성 그룹 접미사를 지정합니다.

c. 대상 클러스터 및 대상 SVM 드롭다운에서 사용하려는 피어링된 클러스터와 SVM을 선택합니다.



SnapCenter에서는 클러스터 및 SVM 피어링을 지원하지 않습니다. 클러스터 및 SVM 피어링을 수행하려면 System Manager 또는 ONTAP CLI를 사용해야 합니다.



리소스가 이미 SnapCenter 외부에서 보호되고 있는 경우 해당 리소스는 보조 보호 리소스 섹션에 표시됩니다.

1. 확인 페이지에서 다음 단계를 수행하세요.

a. *로케이터 로드*를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 저장소에서 검증을

수행합니다.

- b. 딸깍 하는 소리  일정 구성 열에서 정책의 모든 일정 유형에 대한 확인 일정을 구성합니다.
- c. 확인 일정 추가 policy_name 대화 상자에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	이렇게 하세요...
백업 후 검증 실행	*백업 후 검증 실행*을 선택하세요.
검증 일정을 예약하세요	*예약된 확인 실행*을 선택한 다음 드롭다운 목록에서 일정 유형을 선택합니다.

- d. 보조 저장소 시스템에서 백업을 확인하려면 *보조 위치에서 확인*을 선택하세요.
- e. *확인*을 클릭합니다.

구성된 검증 일정은 적용된 일정 열에 나열됩니다.

2. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*을 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSntpServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

3. 요약 검토 후 *마침*을 클릭하세요.

PowerShell cmdlet을 사용하여 스토리지 시스템 연결 및 자격 증명 만들기

PowerShell cmdlet을 사용하여 데이터 보호 작업을 수행하려면 먼저 SVM(스토리지 가상 머신) 연결과 자격 증명을 만들어야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 저장소 연결을 생성하려면 인프라 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

스토리지 시스템 연결을 추가하는 동안에는 호스트 플러그인 설치가 진행 중이어서는 안 됩니다. 호스트 캐시가 업데이트되지 않고 SnapCenter GUI에 데이터베이스 상태가 “백업에 사용할 수 없음” 또는 “NetApp 스토리지에 없음”으로 표시될 수 있기 때문입니다.

- 저장 시스템 이름은 고유해야 합니다.

SnapCenter 서로 다른 클러스터에 동일한 이름을 가진 여러 스토리지 시스템을 지원하지 않습니다. SnapCenter에서 지원하는 각 스토리지 시스템은 고유한 이름과 고유한 관리 LIF IP 주소를 가져야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 PowerShell Core 연결 세션을 시작합니다.

이 예제에서는 PowerShell 세션을 엽니다.

```
PS C:\> Open-SmConnection
```

2. Add-SmStorageConnection cmdlet을 사용하여 스토리지 시스템에 대한 새 연결을 만듭니다.

이 예제에서는 새로운 스토리지 시스템 연결을 만듭니다.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Add-SmCredential cmdlet을 사용하여 새 자격 증명을 만듭니다.

이 예제에서는 Windows 자격 증명을 사용하여 FinanceAdmin이라는 새 자격 증명을 만듭니다.

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

개별 NetApp 지원 플러그인 리소스 백업

개별 NetApp 지원 플러그인 리소스가 어떤 리소스 그룹에도 속하지 않은 경우 리소스 페이지에서 리소스를 백업할 수 있습니다. 필요에 따라 리소스를 백업할 수 있으며, 리소스에 정책이 첨부되고 일정이 구성된 경우 일정에 따라 백업이 자동으로 수행됩니다.

시작하기 전에

- 백업 정책을 생성했어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에 "snapmirror all" 권한이 포함되어야 합니다. 하지만 "vsadmin" 역할을 사용하는 경우 "snapmirror all" 권한은 필요하지 않습니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

딸깍 하는 소리  그런 다음 호스트 이름과 리소스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 클릭할 수 있습니다  필터 창을 닫으려면.

3. 백업할 리소스를 클릭하세요.
4. 리소스 페이지에서 사용자 정의 이름을 사용하려면 스냅샷 복사에 사용자 정의 이름 형식 사용 확인란을 선택한 다음 스냅샷 이름에 대한 사용자 정의 이름 형식을 입력합니다.

예를 들어, `customtext_policy_hostname` 또는 `_resource_hostname_`입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

5. 애플리케이션 설정 페이지에서 다음을 수행합니다.

- a. 추가 백업 옵션을 설정하려면 백업 화살표를 클릭하세요.

필요한 경우 일관성 그룹 백업을 활성화하고 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
일관성 그룹 스냅샷 작업이 완료될 때까지 기다릴 시간을 확보하세요.	스냅샷 작업이 완료될 때까지의 대기 시간을 지정하려면 긴급, 보통 또는 느긋함을 선택합니다. 긴급 = 5초, 보통 = 7초, 여유 = 20초.
WAFL 동기화 비활성화	WAFL 일관성 지점을 강제로 적용하지 않으려면 이 옵션을 선택하세요.

+

- a. 스크립트 화살표를 클릭하면 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령을 실행할 수 있습니다. 백업 작업을 종료하기 전에 사전 명령을 실행할 수도 있습니다.

Prescript와 Postscript는 SnapCenter Server에서 실행됩니다.

- b. 사용자 정의 구성 화살표를 클릭한 다음, 이 리소스를 사용하는 모든 작업에 필요한 사용자 정의 값 쌍을 입력합니다.
- c. 스냅샷 복사 도구* 화살표를 클릭하여 스냅샷을 만드는 도구를 선택하세요.

원하신다면...	그 다음에...
SnapCenter 사용하여 스토리지 레벨 스냅샷을 촬영합니다.	*파일 시스템 일관성이 없는 SnapCenter *를 선택하세요.
SnapCenter Windows용 플러그인을 사용하여 파일 시스템을 일관된 상태로 만든 다음 스냅샷을 찍습니다.	*파일 시스템 일관성을 갖춘 SnapCenter *를 선택하세요.
스냅샷을 생성하는 명령을 입력하려면	*기타*를 선택한 다음 스냅샷을 만드는 명령을 입력합니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



또한 다음을 클릭하여 정책을 생성할 수도 있습니다. .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

- b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.
- c. 정책 _policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 _policy_name_은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

7. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > *전역 설정*에서도 구성해야 합니다.

8. 요약을 검토한 후 *마침*을 클릭하세요.

리소스 토폴로지 페이지가 표시됩니다.

9. *지금 백업*을 클릭하세요.

10. 백업 페이지에서 다음 단계를 수행합니다.

- a. 리소스에 여러 정책을 적용한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. *백업*을 클릭하세요.

11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-smconnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146\
```

사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.

2. Add-SmResources cmdlet을 사용하여 리소스를 추가합니다.

이 예제에서는 리소스를 추가합니다.

```
Add-SmResource -HostName 'scc55.sccore.test.com' -PluginCode
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database
-StorageFootPrint (
@{"VolumeName"="qtree_vol1_scc55_sccore_test_com";"QTREENAME"="qtree
Vol1";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

3. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.

이 예제에서는 새로운 백업 정책을 만듭니다.

```
Add-SmPolicy -PolicyName 'test2' -PolicyType 'Backup'  
-PluginPolicyType DummyPlugin -description 'testPolicy'
```

4. Add-SmResourceGroup cmdlet을 사용하여 SnapCenter 에 새 리소스 그룹을 추가합니다.

이 예제에서는 지정된 정책과 리소스를 사용하여 새 리소스 그룹을 만듭니다.

```
Add-SmResourceGroup -ResourceGroupName  
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'  
-Resources  
@(@{"Host"="scc55.sccore.test.com";"Uid"="QTREE2";"PluginName"="DummyPlugin"},@{"Host"="scc55.sccore.test.com";"Uid"="QTREE";"PluginName"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'  
-usesnapcenterwithoutfilesystemconsistency
```

5. New-SmBackup cmdlet을 사용하여 새로운 백업 작업을 시작합니다.

```
New-SMBackup -DatasetName  
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy  
test2
```

6. Get-SmBackupReport cmdlet을 사용하여 백업 작업의 상태를 확인합니다.

이 예제에서는 지정된 날짜에 실행된 모든 작업에 대한 작업 요약 보고서를 표시합니다.


```
Get-SmBackupReport -JobId 149
```

```
BackedUpObjects      : {QTREE2, QTREE}
FailedObjects        : {}
IsScheduled           : False
HasMetadata           : False
SmBackupId            : 1
SmJobId               : 149
StartDateTime         : 1/15/2024 1:35:17 AM
EndDateTime          : 1/15/2024 1:36:19 AM
Duration              : 00:01:02.4265750
CreatedDateTime       : 1/15/2024 1:35:51 AM
Status                : Completed
ProtectionGroupName   :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows
SmProtectionGroupId   : 1
PolicyName            : test2
SmPolicyId            : 4
BackupName            :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows_scc55_01-
15-2024_01.35.17.4467
VerificationStatus    : NotApplicable
VerificationStatuses  :
SmJobError            :
BackupType            : SCC_BACKUP
CatalogingStatus      : NotApplicable
CatalogingStatuses    :
ReportDataCreatedDateTime :
PluginCode            : SCC
PluginName            : DummyPlugin
PluginDisplayName     : DummyPlugin
JobTypeId             :
JobHost               : scc55.sscore.test.com
```

NetApp 지원 플러그인 리소스의 리소스 그룹 백업

리소스 페이지에서 필요에 따라 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 첨부되고 일정이 구성된 경우 백업은 일정에 따라 자동으로 수행됩니다.

시작하기 전에

- 정책이 첨부된 리소스 그룹을 만들어야 합니다.
- 보조 저장소와 SnapMirror 관계가 있는 리소스를 백업하려면 저장소 사용자에게 할당된 ONTAP 역할에 “snapmirror all” 권한이 포함되어야 합니다. 하지만 “vsadmin” 역할을 사용하는 경우 “snapmirror all” 권한은

필요하지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.

검색창에 리소스 그룹 이름을 입력하거나 클릭하여 리소스 그룹을 검색할 수 있습니다.  태그를 선택합니다. 그런 다음 클릭할 수 있습니다.  필터 창을 닫으려면.

3. 리소스 그룹 페이지에서 백업하려는 리소스 그룹을 선택한 다음, *지금 백업*을 클릭합니다.
4. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스 그룹에 여러 정책을 연결한 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. *백업*을 클릭하세요.

5. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

- MetroCluster 구성에서 SnapCenter 장애 조치 후 보호 관계를 감지하지 못할 수 있습니다.

"MetroCluster 장애 조치 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다."

- VMDK에서 애플리케이션 데이터를 백업하고 SnapCenter Plug-in for VMware vSphere의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다. Java 힙 크기를 늘리려면 스크립트 파일 `/opt/netapp/init_scripts/scvservice`를 찾으세요. 해당 스크립트에서 `do_start method` 명령은 SnapCenter VMware 플러그인 서비스를 시작합니다. 해당 명령을 다음과 같이 업데이트하세요. `Java -jar -Xmx8192M -Xms4096M`.

NetApp 지원 플러그인 리소스 백업 작업 모니터링

SnapCenterJobs 페이지를 사용하여 다양한 백업 작업의 진행 상황을 모니터링할 수 있습니다. 완료 시점이나 문제가 있는지 확인하기 위해 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 해당 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  백업 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *백업*을 선택합니다.
 - d. 상태 드롭다운에서 백업 상태를 선택합니다.
 - e. *적용*을 클릭하면 작업이 성공적으로 완료된 것을 볼 수 있습니다.
4. 백업 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인하세요.



백업 작업 상태가 표시됩니다.  작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 표시가 되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

NetApp 지원 플러그인에 대한 백업 작업 취소

대기 중인 백업 작업을 취소할 수 있습니다.

필요한 것

- 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 모니터 페이지나 활동 창에서 백업 작업을 취소할 수 있습니다.
- 실행 중인 백업 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 백업 작업을 취소할 수 있습니다.
- 취소할 수 없는 작업의 경우 작업 취소 버튼이 비활성화됩니다.
- 역할을 생성할 때 사용자\그룹 페이지에서 *이 역할의 모든 구성원은 다른 구성원 개체를 보고 작업할 수 있음*을 선택한 경우, 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 백업 작업을 취소할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

...로부터	행동
모니터 페이지	a. 왼쪽 탐색 창에서 모니터 > *작업*을 클릭합니다. b. 작업을 선택한 다음 *작업 취소*를 클릭합니다.

...로부터	행동
활동 창	a. 백업 작업을 시작한 후 *를 클릭하세요.  * 활동 창에서 가장 최근의 작업 5개를 확인하세요. b. 작업을 선택하세요. c. 작업 세부 정보 페이지에서 *작업 취소*를 클릭합니다.

작업이 취소되고 리소스는 이전 상태로 돌아갑니다.

토폴로지 페이지에서 NetApp 지원 플러그인 리소스 관련 백업 및 복제본 보기

리소스를 백업하거나 복제할 준비를 할 때 기본 및 보조 저장소에 있는 모든 백업과 복제본을 그래픽으로 표현해 보면 도움이 될 수 있습니다. 토폴로지 페이지에서는 선택한 리소스 또는 리소스 그룹에 사용 가능한 모든 백업과 복제본을 볼 수 있습니다. 해당 백업 및 복제의 세부 정보를 보고 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

이 작업에 관하여

다음 아이콘을 '사본 관리' 보기에서 검토하여 백업 및 복제본을 기본 저장소 또는 보조 저장소(미러 사본 또는 볼트 사본)에서 사용할 수 있는지 확인할 수 있습니다.

-  기본 스토리지에서 사용 가능한 백업 및 복제본의 수를 표시합니다.
-  SnapMirror 기술을 사용하여 보조 저장소에 미러링된 백업 및 복제본의 수를 표시합니다.
-  미러 볼트 유형 볼륨의 버전 유연한 미러 백업의 복제본은 토폴로지 보기에 표시되지만 토폴로지 보기의 미러 백업 수에는 버전 유연한 백업이 포함되지 않습니다.
-  SnapVault 기술을 사용하여 보조 저장소에 복제된 백업 및 복제본의 수를 표시합니다.

표시된 백업 수에는 보조 저장소에서 삭제된 백업이 포함됩니다. 예를 들어, 4개의 백업만 보존하는 정책을 사용하여 6개의 백업을 만든 경우 표시되는 백업 수는 6개입니다.

-  미러 볼트 유형 볼륨의 버전 유연한 미러 백업의 복제본은 토폴로지 보기에 표시되지만 토폴로지 보기의 미러 백업 수에는 버전 유연한 백업이 포함되지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 리소스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 리소스를 선택합니다.

리소스가 보호된 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. 요약 카드를 검토하여 기본 및 보조 저장소에서 사용 가능한 백업 및 복제본 수에 대한 요약을 확인하세요.

요약 카드 섹션에는 백업 및 복제의 총 수가 표시됩니다.

새로 고침 버튼을 클릭하면 저장소에 대한 쿼리가 시작되어 정확한 개수가 표시됩니다.

SnapLock 이 활성화된 백업을 수행한 경우 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간이 새로 고쳐집니다. 주간 일정은 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간도 새로 고칩니다.

애플리케이션 리소스가 여러 볼륨에 분산되어 있는 경우 백업에 대한 SnapLock 만료 시간은 볼륨의 스냅샷에 설정된 가장 긴 SnapLock 만료 시간이 됩니다. 가장 긴 SnapLock 만료 시간은 ONTAP 에서 검색됩니다.

주문형 백업 후, 새로 고침 버튼을 클릭하면 백업이나 복제의 세부 정보가 새로 고침됩니다.

5. 복사본 관리 보기에서 기본 또는 보조 저장소의 백업 또는 *복제*를 클릭하면 백업 또는 복제의 세부 정보를 볼 수 있습니다.

백업 및 복제의 세부 정보는 표 형식으로 표시됩니다.

6. 표에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 복제, 이름 바꾸기, 삭제 작업을 수행합니다.



보조 저장 시스템에 있는 백업의 이름을 바꾸거나 삭제할 수 없습니다.



기본 스토리지 시스템에 있는 백업의 이름을 바꿀 수 없습니다.

7. 복제본을 삭제하려면 테이블에서 복제본을 선택하고 클릭하십시오. 복제본을 삭제합니다.

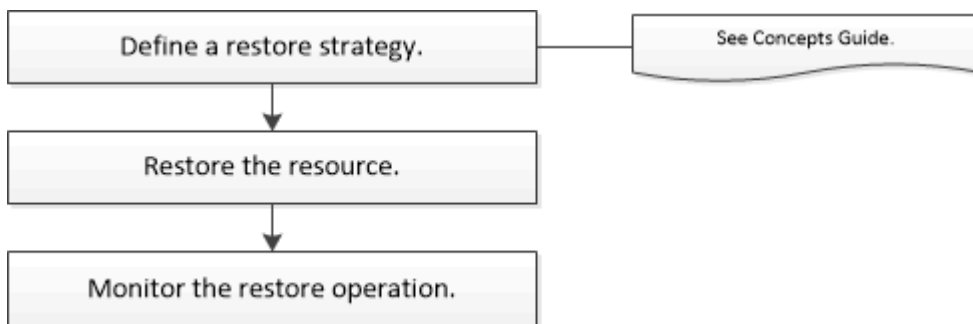
NetApp 지원 플러그인 리소스 복원

NetApp 지원 플러그인 리소스 복원

복원 및 복구 워크플로에는 계획, 복원 작업 수행, 작업 모니터링이 포함됩니다.

이 작업에 관하여

다음 워크플로는 복원 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다.

PowerShell cmdlet에 대한 정보는 SnapCenter cmdlet 도움말을 사용하거나 다음을 참조하세요. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

리소스 백업 복원

SnapCenter 사용하여 리소스를 복원할 수 있습니다. 복원 작업의 기능은 사용하는 플러그인에 따라 달라집니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 스냅샷을 미리 또는 볼트에 복제하는 경우 SnapCenter 관리자가 소스 볼륨과 대상 볼륨 모두에 대한 스토리지 가상 머신(SVM)을 할당해야 합니다.
- 복원하려는 리소스 또는 리소스 그룹에 대해 현재 진행 중인 모든 백업 작업을 취소했어야 합니다.

이 작업에 관하여

- 기본 복원 작업은 저장소 개체만 복원합니다. 애플리케이션 수준의 복원 작업은 NetApp 에서 지원하는 플러그인이 해당 기능을 제공하는 경우에만 수행할 수 있습니다.
- ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.

리소스는 유형, 호스트 또는 클러스터 이름, 연관된 리소스 그룹 및 정책, 상태와 같은 정보와 함께 표시됩니다.



백업은 리소스 그룹을 위한 것일 수 있지만 복원할 때는 복원할 개별 리소스를 선택해야 합니다.

리소스가 보호되지 않은 경우, 전체 상태 열에 _보호되지 않음_이 표시됩니다.

전체 상태 열의 보호되지 않음 상태는 리소스가 보호되지 않았거나 다른 사용자가 리소스를 백업했음을 의미할 수 있습니다.

3. 리소스를 선택하거나 리소스 그룹을 선택한 다음 해당 그룹에서 리소스를 선택합니다.

리소스 토폴로지 페이지가 표시됩니다.

4. 사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.

5. 기본 백업 테이블에서 복원하려는 백업을 선택한 다음 클릭하십시오. .



6. 복원 범위 페이지에서 전체 리소스 또는 *파일 수준*을 선택합니다.

- a. *리소스 완료*를 선택한 경우 리소스 백업이 복원됩니다.

리소스에 스토리지 공간으로 볼륨이나 Q트리 포함되어 있는 경우 해당 볼륨이나 Q트리의 최신 스냅샷은 삭제되며 복구할 수 없습니다. 또한, 다른 리소스가 동일한 볼륨이나 Q트리에 호스팅된 경우 해당 리소스도 삭제됩니다.

- b. *파일 수준*을 선택한 경우 *모두*를 선택하거나 볼륨이나 Qtree를 선택한 다음 선택한 볼륨이나 Qtree와 관련된 경로를 쉼표로 구분하여 입력할 수 있습니다.

- 여러 개의 볼륨과 Q트리를 선택할 수 있습니다.
- 리소스 유형이 LUN인 경우 전체 LUN이 복원됩니다. 여러 개의 LUN을 선택할 수 있습니다. + 참고: *모두*를 선택하면 볼륨, Qtree 또는 LUN의 모든 파일이 복원됩니다.

7. 사전 작업 페이지에서 복원 작업을 수행하기 전에 실행할 pre restore 및 unmount 명령을 입력합니다.
8. 작업 후 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.
9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > 전역 설정 페이지에서도 구성해야 합니다.

10. 요약을 검토한 후 *마침*을 클릭하세요.

11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
PS C:\> Open-Smconnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

이 예에서는 2015년 1월 29일부터 2015년 2월 3일까지의 백업에 대한 자세한 정보를 표시합니다.


```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

NetApp 지원 플러그인 리소스 복원 작업 모니터링

작업 페이지를 사용하여 다양한 SnapCenter 복원 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

복원 후 상태는 복원 작업 후 리소스의 조건과 수행할 수 있는 추가 복원 작업을 설명합니다.

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중

-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복원 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복원*을 선택합니다.
 - d. 상태 드롭다운 목록에서 복원 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복원 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

NetApp 지원 플러그인 리소스 백업 복제

NetApp 지원 플러그인 리소스 백업 복제

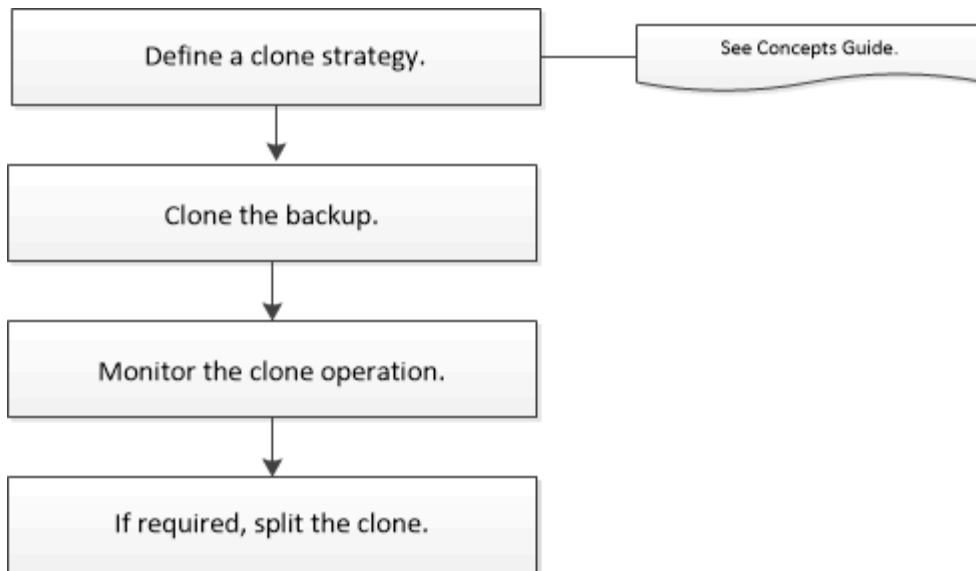
복제 워크플로에는 복제 작업을 수행하고 작업을 모니터링하는 작업이 포함됩니다.

이 작업에 관하여

다음과 같은 이유로 리소스 백업을 복제할 수 있습니다.

- 애플리케이션 개발 주기 동안 현재 리소스 구조 및 콘텐츠를 사용하여 구현해야 하는 기능을 테스트하려면
- 데이터 웨어하우스를 채울 때 데이터 추출 및 조작 도구
- 실수로 삭제되거나 변경된 데이터를 복구하려면

다음 워크플로는 복제 작업을 수행해야 하는 순서를 보여줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트로 사용하여 백업, 복원 및 복제 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 다음을 참조하세요. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

백업에서 복제

SnapCenter 사용하여 백업을 복제할 수 있습니다. 기본 또는 보조 백업에서 복제할 수 있습니다. 복제 작업의 기능은 사용하는 플러그인에 따라 달라집니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 기본 복제 작업은 저장소 객체만 복제합니다. 애플리케이션 수준의 복제 작업은 NetApp 에서 지원하는 플러그인이 해당 기능을 제공하는 경우에만 수행할 수 있습니다.
- 볼륨을 호스팅하는 집계가 스토리지 가상 머신(SVM)의 할당된 집계 목록에 있는지 확인해야 합니다.

이 작업에 관하여

ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 리소스 유형을 기준으로 리소스를 필터링합니다.

리소스는 유형, 호스트 또는 클러스터 이름, 연관된 리소스 그룹 및 정책, 상태와 같은 정보와 함께 표시됩니다.

3. 리소스 또는 리소스 그룹을 선택하세요.

리소스 그룹을 선택하는 경우 리소스를 선택해야 합니다.

리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 표에서 데이터 백업을 선택한 다음 클릭하세요.  .
6. 위치 페이지에서 다음을 수행합니다.

이 분야에서는...	이렇게 하세요...
복제 서버	기본적으로 소스 호스트가 채워져 있습니다. 다른 호스트를 지정하려면 복제본을 마운트하고 플러그인을 설치할 호스트를 선택하세요.
클론 접미사	복제 대상이 소스와 동일한 경우 이는 필수입니다. 새로 복제된 리소스 이름에 추가될 접미사를 입력하세요. 접미사는 복제된 리소스가 호스트에서 고유하도록 보장합니다. 예를 들어, rs1_clone. 원본 리소스와 동일한 호스트에 복제하는 경우 복제된 리소스와 원본 리소스를 구별하기 위해 접미사를 제공해야 합니다. 그렇지 않으면 작업이 실패합니다.

선택한 리소스가 LUN이고 보조 백업에서 복제하는 경우 대상 볼륨이 나열됩니다. 단일 소스는 여러 개의 대상 볼륨을 가질 수 있습니다.

7. 설정 페이지에서 다음을 수행하세요.

이 분야에서는...	이렇게 하세요...
개시자 이름	호스트 개시자 이름(IQDN 또는 WWPN)을 입력합니다.
Igroup 프로토콜	Igroup 프로토콜을 선택하세요.



설정 페이지는 저장 유형이 LUN인 경우에만 표시됩니다.

- 스크립트 페이지에서 복제 작업 전이나 후에 실행해야 하는 사전 복제 또는 사후 복제에 대한 명령을 입력합니다. 호스트에 파일 시스템을 마운트하려면 mount 명령을 입력하세요.

예를 들어:

- 사전 복제 명령: 동일한 이름을 가진 기존 데이터베이스 삭제
- 복제 후 명령: 데이터베이스를 확인하거나 데이터베이스를 시작합니다.

Linux 머신에서 볼륨 또는 qtree에 대한 마운트 명령:

```
mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>
```

- 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다.

- 요약을 검토하고 *마침*을 클릭하세요.

- 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

PowerShell cmdlet

단계

- Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter 서버와의 연결 세션을 시작합니다.

```
Open-SmConnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

- Get-SmBackup 또는 Get-SmResourceGroup cmdlet을 사용하여 복제할 수 있는 백업을 나열합니다.

이 예제에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

이 예제에서는 지정된 리소스 그룹에 대한 정보를 표시합니다.

```
PS C:\> Get-SmResourceGroup
```

```
Description           :  
CreationTime           : 10/10/2016 4:45:53 PM  
ModificationTime       : 10/10/2016 4:45:53 PM  
EnableEmail            : False  
EmailSMTPServer        :  
EmailFrom              :  
EmailTo                :  
EmailSubject           :  
EnableSysLog           : False  
ProtectionGroupType    : Backup  
EnableAsupOnFailure    : False  
Policies               : {}  
HostResourceMapping    : {}  
Configuration          :
```

```
SMCoreContracts.SmCloneConfiguration
```

```
LastBackupStatus       : Completed  
VerificationServer     :  
EmailBody              :  
EmailNotificationPreference : Never  
VerificationServerInfo :  
SchedulerSQLInstance   :  
CustomText             :  
CustomSnapshotFormat   :  
SearchResources        : False  
ByPassCredential       : False  
IsCustomSnapshot       :  
MaintenanceStatus      : Production  
PluginProtectionGroupTypes : {SMSQL}  
Tag                    :  
IsInternal             : False  
EnableEmailAttachment  : False  
VerificationSettings   : {}  
Name                   : NFS_DB  
Type                   : Group  
Id                     : 2  
Host                   :  
UserName               :  
Passphrase             :  
Deleted                : False  
Auth                   : SMCoreContracts.SmAuth  
IsClone                : False  
CloneLevel             : 0  
Hosts                  :  
StorageName            :
```

```

ResourceGroupNames      :
PolicyNames              :

Description              :
CreationTime             : 10/10/2016 4:51:36 PM
ModificationTime         : 10/10/2016 5:27:57 PM
EnableEmail              : False
EmailSMTPServer          :
EmailFrom                :
EmailTo                  :
EmailSubject             :
EnableSysLog             : False
ProtectionGroupType      : Backup
EnableAsupOnFailure      : False
Policies                 : {}
HostResourceMapping      : {}
Configuration            :
SMCoreContracts.SmCloneConfiguration
LastBackupStatus         : Failed
VerificationServer        :
EmailBody                :
EmailNotificationPreference : Never
VerificationServerInfo    :
SchedulerSQLInstance      :
CustomText               :
CustomSnapshotFormat      :
SearchResources          : False
ByPassRunAs              : False
IsCustomSnapshot         :
MaintenanceStatus        : Production
PluginProtectionGroupTypes : {SMSQL}
Tag                      :
IsInternal               : False
EnableEmailAttachment     : False
VerificationSettings      : {}
Name                     : Test
Type                     : Group
Id                       : 3
Host                     :
UserName                 :
Passphrase               :
Deleted                  : False
Auth                     : SMCoreContracts.SmAuth
IsClone                  : False
CloneLevel               : 0
Hosts                    :

```



```
StorageName      :
ResourceGroupNames :
PolicyNames      :
```

3. New-SmClone cmdlet을 사용하여 복제 리소스 그룹이나 기존 백업에서 복제 작업을 시작합니다.

이 예제에서는 모든 로그를 포함하는 지정된 백업에서 복제본을 만듭니다.

```
New-SmClone -BackupName
Verify_delete_clone_on_qtree_windows_scc54_10-04-2016_19.05.48.0886
-Resources @{"Host"="scc54.sccore.test.com";"Uid"="QTREE1"} -
CloneToInstance scc54.sccore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sccore.test.com' -igroupprotocol 'mixed'
```

4. Get-SmCloneReport cmdlet을 사용하여 복제 작업의 상태를 확인합니다.

이 예제에서는 지정된 작업 ID에 대한 복제 보고서를 표시합니다.

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId      : 1
SmJobId        : 186
StartDateTime  : 8/3/2015 2:43:02 PM
EndDateTime    : 8/3/2015 2:44:08 PM
Duration       : 00:01:06.6760000
Status         : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName     : OnDemand_Clone
SmPolicyId     : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName  : SCSPR0054212005.mycompany.com
CloneHostId    : 4
CloneName      : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError     :
```

NetApp 지원 플러그인 리소스 복제 작업 모니터링

작업 페이지를 사용하여 SnapCenter 복제 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복제 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복제*를 선택합니다.
 - d. 상태 드롭다운 목록에서 복제 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복제 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

Unix 파일 시스템 보호

Unix 파일 시스템용 SnapCenter 플러그인으로 할 수 있는 일

Unix 파일 시스템용 플러그인이 사용자 환경에 설치되면 SnapCenter 사용하여 Unix 파일 시스템을 백업, 복원 및 복제할 수 있습니다. 해당 작업을 지원하는 작업도 수행할 수 있습니다.

- 리소스를 찾아보세요
- Unix 파일 시스템 백업
- 백업 작업 예약
- 파일 시스템 백업 복원
- 파일 시스템 백업 복제
- 백업, 복원 및 복제 작업 모니터링

지원되는 구성

목	지원되는 구성
환경	• 물리적 서버 • 가상 서버 NFS와 SAN 모두에 vVol 데이터 저장소가 있습니다. vVol 데이터 저장소는 VMware vSphere용 ONTAP 도구를 사용해서만 프로비저닝할 수 있습니다.
운영 체제	• 레드햇 엔터프라이즈 리눅스 • 오라클 리눅스 • SUSE Linux Enterprise Server(SLES)
파일 시스템	• 산: ◦ LVM 기반 및 비 LVM 기반 파일 시스템 모두 ◦ VMDK ext3, ext4 및 xfs를 통한 LVM • NFS: NFS v3, NFS v4.x
프로토콜	• FC • FCoE • iSCSI • NFS
다중 경로	예

제한 사항

- 볼륨 그룹에서 RDM과 가상 디스크를 혼합하여 사용할 수 없습니다.
- 파일 수준 복원은 지원되지 않습니다.

하지만 백업을 복제한 다음 파일을 수동으로 복사하여 파일 수준 복원을 수동으로 수행할 수 있습니다.

- NFS와 VMFS 데이터 저장소 모두에서 나오는 VMDK에 분산된 파일 시스템의 혼합은 지원되지 않습니다.
- NVMe는 지원되지 않습니다.
- 프로비저닝이 지원되지 않습니다.

특징

- Linux 또는 AIX 시스템에서 기본 호스트 스토리지 스택을 처리하여 Oracle 데이터베이스에서 데이터 보호 작업을 수행할 수 있도록 Oracle 데이터베이스용 플러그인을 활성화합니다.
- ONTAP 실행하는 스토리지 시스템에서 NFS(네트워크 파일 시스템) 및 SAN(스토리지 영역 네트워크) 프로토콜을 지원합니다.
- Linux 시스템의 경우 SnapCenter Plug-in for VMware vSphere 배포하고 SnapCenter 에 플러그인을 등록하면 VMDK 및 RDM LUN의 Oracle 데이터베이스가 지원됩니다.
- SAN 파일 시스템과 LVM 레이아웃에서 AIX용 Mount Guard를 지원합니다.
- SAN 파일 시스템에서 인라인 로깅을 지원하는 향상된 저널링 파일 시스템(JFS2)과 AIX 시스템에서만 LVM 레이아웃을 지원합니다.

SAN 기본 장치, 파일 시스템 및 SAN 장치에 구축된 LVM 레이아웃이 지원됩니다.

- SnapCenter 환경에서 UNIX 파일 시스템에 대한 애플리케이션 인식 백업, 복원 및 복제 작업을 자동화합니다.

Unix 파일 시스템용 SnapCenter 플러그인 설치

Linux용 호스트 추가 및 플러그인 패키지 설치를 위한 전제 조건

Linux용 호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 충족해야 합니다.

- iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.
- 루트 또는 루트가 아닌 사용자에게 대해 비밀번호 기반 인증을 사용하거나 SSH 키 기반 인증을 사용할 수 있습니다.

Unix 파일 시스템용 SnapCenter 플러그인은 루트가 아닌 사용자도 설치할 수 있습니다. 하지만 루트가 아닌 사용자가 플러그인 프로세스를 설치하고 시작하려면 sudo 권한을 구성해야 합니다. 플러그인을 설치한 후에는 프로세스가 루트가 아닌 사용자 권한으로 실행됩니다.

- 설치 사용자에게 대해 Linux 인증 모드로 자격 증명을 생성합니다.
- Linux 호스트에 Java 11을 설치했어야 합니다.



Linux 호스트에 JAVA 11 인증 버전만 설치했는지 확인하세요.

JAVA 다운로드에 대한 자세한 내용은 다음을 참조하세요. "[모든 운영 체제용 Java 다운로드](#)"

- 플러그인 설치를 위해 기본 셸로 *bash*를 사용해야 합니다.

Linux 호스트 요구 사항

Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 호스트가 요구 사항을 충족하는지 확인해야 합니다.

목	요구 사항
운영 체제	• 레드햇 엔터프라이즈 리눅스 • 오라클 리눅스 • SUSE Linux Enterprise Server(SLES)
호스트의 SnapCenter 플러그인을 위한 최소 RAM	2GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB  충분한 디스크 공간을 할당하고 로그 폴더의 저장 공간 소비를 모니터링해야 합니다. 필요한 로그 공간은 보호해야 할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행된 작업에 대한 로그가 생성되지 않습니다.
필수 소프트웨어 패키지	Java 11 Oracle Java 및 OpenJDK  Linux 호스트에 JAVA 11 인증 버전만 설치했는지 확인하세요. JAVA를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties에 있는 JAVA_HOME 옵션이 올바른 JAVA 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다.

지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "[NetApp 상호 운용성 매트릭스 도구](#)".

GUI를 사용하여 Linux용 호스트 추가 및 플러그인 패키지 설치

호스트 추가 페이지를 사용하여 호스트를 추가한 다음 Linux용 SnapCenter 플러그인 패키지를 설치할 수 있습니다. 플러그인은 원격 호스트에 자동으로 설치됩니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 상단에 관리되는 호스트 탭이 선택되어 있는지 확인하세요.

3. *추가*를 클릭하세요.
4. 호스트 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
호스트 유형	호스트 유형으로 *Linux*를 선택하세요.
호스트 이름	호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력하세요. SnapCenter DNS의 적절한 구성에 달려 있습니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다. SnapCenter 사용하여 호스트를 추가하고 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.
신임장	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성하세요. 자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하세요. 지정한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다.  자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 *Unix 파일 시스템*을 선택합니다.
6. (선택 사항) *추가 옵션*을 클릭합니다.

이 분야에서는...	이렇게 하세요...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정하세요. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트 번호로 표시됩니다.  플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.

이 분야에서는...	이렇게 하세요...
설치 경로	기본 경로는 <code>_/opt/ NetApp/snapcenter_</code> 입니다. 선택적으로 경로를 사용자 정의할 수 있습니다. 사용자 정의 경로를 사용하는 경우 <code>sudoers</code> 의 기본 콘텐츠가 사용자 정의 경로로 업데이트되었는지 확인하세요.
선택적 사전 설치 확인 건너뛰기	플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택하세요.

7. *제출*을 클릭하세요.

사전 검사 건너뛰기 확인란을 선택하지 않은 경우 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 호스트가 검증됩니다.



사전 확인 스크립트는 방화벽 거부 규칙에 지정된 경우 플러그인 포트 방화벽 상태를 검증하지 않습니다.

최소 요구 사항을 충족하지 못하면 적절한 오류 또는 경고 메시지가 표시됩니다. 오류가 디스크 공간이나 RAM과 관련된 경우 `_C:\Program Files\ NetApp\ SnapCenter WebApp_`에 있는 `web.config` 파일을 업데이트하여 기본값을 수정할 수 있습니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.



HA 설정에서 `web.config` 파일을 업데이트하는 경우 두 노드에서 모두 파일을 업데이트해야 합니다.

8. 지문을 확인한 후 *확인 및 제출*을 클릭하세요.



SnapCenter ECDSA 알고리즘을 지원하지 않습니다.



동일한 호스트가 이전에 SnapCenter 에 추가되었고 지문이 확인된 경우에도 지문 확인은 필수입니다.

9. 설치 진행 상황을 모니터링합니다.

설치 관련 로그 파일은 `_/custom_location/snapcenter/logs_`에 있습니다.

결과

호스트에 마운트된 모든 파일 시스템은 자동으로 검색되어 리소스 페이지에 표시됩니다. 아무것도 표시되지 않으면 *리소스 새로 고침*을 클릭하세요.

모니터 설치 상태

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행 상황을 모니터링할 수 있습니다. 설치가 완료되었는지 또는 문제가 있는지 확인하기 위해 설치 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 플러그인 설치 작업만 나열되도록 목록을 필터링하려면 다음을 수행합니다.
 - a. *필터*를 클릭하세요.
 - b. 선택 사항: 시작 날짜와 종료 날짜를 지정합니다.
 - c. 유형 드롭다운 메뉴에서 *플러그인 설치*를 선택합니다.
 - d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
 - e. *적용*을 클릭하세요.
4. 설치 작업을 선택하고 *세부정보*를 클릭하면 작업 세부정보를 볼 수 있습니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

SnapCenter 플러그인 Loader 서비스 구성

SnapCenter 플러그인 Loader 서비스는 Linux가 SnapCenter 서버와 상호 작용할 수 있도록 플러그인 패키지를 로드합니다. SnapCenter 플러그인 Loader 서비스는 Linux용 SnapCenter 플러그인 패키지를 설치할 때 설치됩니다.

이 작업에 관하여

Linux용 SnapCenter 플러그인 패키지를 설치하면 SnapCenter 플러그인 Loader 서비스가 자동으로 시작됩니다. SnapCenter 플러그인 Loader 서비스가 자동으로 시작되지 않으면 다음을 수행해야 합니다.

- 플러그인이 작동 중인 디렉토리가 삭제되지 않았는지 확인하세요.
- Java Virtual Machine에 할당된 메모리 공간을 늘리세요

`_/custom_location/ NetApp/snapcenter/spl/etc/_`에 있는 `spl.properties` 파일에는 다음 매개변수가 포함되어 있습니다. 이러한 매개변수에는 기본값이 할당됩니다.

매개변수 이름	설명
로그 레벨	지원되는 로그 수준을 표시합니다. 가능한 값은 TRACE, DEBUG, INFO, WARN, ERROR, FATAL입니다.
SPL_프로토콜	SnapCenter 플러그인 Loader 가 지원하는 프로토콜을 표시합니다. HTTPS 프로토콜만 지원됩니다. 기본값이 없는 경우 값을 추가할 수 있습니다.
SNAPCENTER_SERVER_프로토콜	SnapCenter Server에서 지원하는 프로토콜을 표시합니다. HTTPS 프로토콜만 지원됩니다. 기본값이 없는 경우 값을 추가할 수 있습니다.
자바 홈 업데이트 건너뛰기	기본적으로 SPL 서비스는 Java 경로를 감지하고 JAVA_HOME 매개변수를 업데이트합니다. 따라서 기본값은 FALSE로 설정됩니다. 기본 동작을 비활성화하고 Java 경로를 수동으로 수정하려면 TRUE로 설정하면 됩니다.
SPL_키스토어_패스	키스토어 파일의 비밀번호를 표시합니다. 비밀번호를 변경하거나 새로운 키스토어 파일을 만드는 경우에만 이 값을 변경할 수 있습니다.
SPL_PORT	SnapCenter 플러그인 Loader 서비스가 실행 중인 포트 번호를 표시합니다. 기본값이 없는 경우 값을 추가할 수 있습니다.  플러그인을 설치한 후에는 값을 변경하지 마세요.
SNAPCENTER_SERVER_HOST	SnapCenter 서버의 IP 주소 또는 호스트 이름을 표시합니다.
SPL_키스토어_경로	키스토어 파일의 절대 경로를 표시합니다.
SNAPCENTER_SERVER_PORT	SnapCenter 서버가 실행 중인 포트 번호를 표시합니다.

매개변수 이름	설명
LOGS_MAX_COUNT	/custom_location/snapcenter/spl/logs 폴더에 보관된 SnapCenter 플러그인 Loader 로그 파일의 수를 표시합니다. 기본값은 5000으로 설정되어 있습니다. 개수가 지정된 값보다 많으면 마지막으로 수정된 5000개의 파일이 보존됩니다. SnapCenter 플러그인 Loader 서비스가 시작된 후 24시간마다 파일 개수 확인이 자동으로 수행됩니다.  spl.properties 파일을 수동으로 삭제하면 보존되는 파일 수가 9999로 설정됩니다.
자바 홈	SPL 서비스를 시작하는 데 사용되는 JAVA_HOME의 절대 디렉토리 경로를 표시합니다. 이 경로는 설치 중 및 SPL 시작의 일부로 결정됩니다.
로그 최대 크기	작업 로그 파일의 최대 크기를 표시합니다. 최대 크기에 도달하면 로그 파일이 압축되고 로그는 해당 작업의 새 파일에 기록됩니다.
지난 며칠 동안의 로그 보관	로그가 보관되는 일수를 표시합니다.
인증서 검증 활성화	호스트에 대해 CA 인증서 검증이 활성화된 경우 true로 표시됩니다. spl.properties를 편집하거나 SnapCenter GUI 또는 cmdlet을 사용하여 이 매개변수를 활성화하거나 비활성화할 수 있습니다.

이러한 매개변수 중 하나라도 기본값에 할당되지 않았거나 값을 할당하거나 변경하려는 경우 spl.properties 파일을 수정할 수 있습니다. spl.properties 파일을 확인하고 파일을 편집하여 매개변수에 할당된 값과 관련된 문제를 해결할 수도 있습니다. spl.properties 파일을 수정한 후에는 SnapCenter 플러그인 Loader 서비스를 다시 시작해야 합니다.

단계

1. 필요에 따라 다음 작업 중 하나를 수행합니다.

- SnapCenter 플러그인 Loader 서비스를 시작합니다.
 - 루트 사용자로 다음을 실행합니다. /custom_location/NetApp/snapcenter/spl/bin/spl start
 - 루트가 아닌 사용자로 다음을 실행합니다. sudo /custom_location/NetApp/snapcenter/spl/bin/spl start
- SnapCenter 플러그인 Loader 서비스를 중지합니다.

- 루트 사용자로 다음을 실행합니다. `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
- 루트가 아닌 사용자로 다음을 실행합니다. `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`



stop 명령과 함께 `-force` 옵션을 사용하면 SnapCenter 플러그인 Loader 서비스를 강제로 중지할 수 있습니다. 하지만 그렇게 하면 기존 작업도 종료되므로 주의해서 작업해야 합니다.

- SnapCenter 플러그인 Loader 서비스를 다시 시작합니다.
 - 루트 사용자로 다음을 실행합니다. `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
 - 루트가 아닌 사용자로 다음을 실행합니다. `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
- SnapCenter 플러그인 Loader 서비스의 상태를 확인하세요.
 - 루트 사용자로 다음을 실행합니다. `/custom_location/NetApp/snapcenter/spl/bin/spl status`
 - 루트 사용자가 아닌 경우 다음을 실행합니다. `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
- SnapCenter 플러그인 Loader 서비스에서 변경 사항을 찾으세요.
 - 루트 사용자로 다음을 실행합니다. `/custom_location/NetApp/snapcenter/spl/bin/spl change`
 - 루트가 아닌 사용자로 다음을 실행합니다. `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Linux 호스트에서 SnapCenter 플러그인 Loader (SPL) 서비스를 사용하여 CA 인증서 구성

SnapCenter 플러그인 Loader 서비스를 사용하여 SPL 키 저장소와 인증서의 비밀번호를 관리하고, CA 인증서를 구성하고, SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, SPL 신뢰 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.



SPL은 `'/var/opt/snapcenter/spl/etc'`에 위치한 `'keystore.jks'` 파일을 신뢰 저장소와 키 저장소로 사용합니다.

사용 중인 **SPL** 키 저장소 및 **CA** 서명 키 쌍의 별칭에 대한 비밀번호 관리

단계

1. SPL 속성 파일에서 SPL 키 저장소 기본 비밀번호를 검색할 수 있습니다.

이는 `'SPL_KEYSTORE_PASS'` 키에 해당하는 값입니다.

2. 키스토어 비밀번호를 변경하세요:

```
keytool -storepasswd -keystore keystore.jks
```

. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 비밀번호를 키 저장소에 사용된 비밀번호와 동일하게 변경합니다.

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

spl.properties 파일에서 SPL_KEYSTORE_PASS 키에 대해서도 동일하게 업데이트합니다.

3. 비밀번호를 변경한 후 서비스를 다시 시작하세요.



SPL 키 저장소의 비밀번호와 개인 키의 모든 관련 별칭 비밀번호는 동일해야 합니다.

SPL 신뢰 저장소에 루트 또는 중간 인증서 구성

SPL 신뢰 저장소에 대한 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. SPL 키 저장소가 포함된 폴더로 이동합니다: */var/opt/snapcenter/spl/etc*.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

. 루트 또는 중간 인증서를 추가합니다.

```
keytool -import -trustcacerts -alias  
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore  
keystore.jks
```

. 루트 또는 중간 인증서를 SPL 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.



루트 CA 인증서를 추가한 다음 중간 CA 인증서를 추가해야 합니다.

SPL 신뢰 저장소에 CA 서명 키 쌍 구성

CA 서명 키 쌍을 SPL 신뢰 저장소에 구성해야 합니다.

단계

1. SPL 키 저장소 */var/opt/snapcenter/spl/etc*가 포함된 폴더로 이동합니다.
2. 'keystore.jks' 파일을 찾으세요.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

. 개인 키와 공개 키를 모두 포함하는 CA 인증서를 추가합니다.

```
keytool -importkeystore -srckeystore <CertificatePathToImport>  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

. 키스토어에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

. 키 저장소에 추가된 새 CA 인증서에 해당하는 별칭이 키 저장소에 포함되어 있는지 확인합니다.

. CA 인증서에 추가된 개인 키 비밀번호를 키 저장소 비밀번호로 변경합니다.

기본 SPL 키 저장소 비밀번호는 spl.properties 파일의 SPL_KEYSTORE_PASS 키 값입니다.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore  
keystore.jks
```

. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자("*", ",", ")가 포함된 경우 별칭 이름을 간단한 이름으로 변경합니다.

```
keytool -changealias -alias "<OriginalAliasName>" -destalias  
"<NewAliasName>" -keystore keystore.jks
```

. spl.properties 파일에 있는 키스토어에서 별칭 이름을 구성합니다.

이 값을 SPL_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

4. CA 서명 키 쌍을 SPL 신뢰 저장소로 구성한 후 서비스를 다시 시작합니다.

SPL에 대한 인증서 해지 목록(CRL) 구성

SPL에 대한 CRL을 구성해야 합니다.

이 작업에 관하여

- SPL은 미리 구성된 디렉토리에서 CRL 파일을 찾습니다.
- SPL의 CRL 파일에 대한 기본 디렉토리는 `/var/opt/snapcenter/spl/etc/crl_`입니다.

단계

1. spl.properties 파일에서 기본 디렉토리를 SPL_CRL_PATH 키에 맞춰 수정하고 업데이트할 수 있습니다.
2. 이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다.

수신 인증서는 각 CRL에 대해 검증됩니다.

플러그인에 대한 CA 인증서 활성화

CA 인증서를 구성하고 SnapCenter 서버와 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- `Set-SmCertificateSettings` cmdlet을 실행하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- `_Get-SmCertificateSettings_`를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 하나 또는 여러 개의 플러그인 호스트를 선택하세요.
4. *추가 옵션*을 클릭하세요.
5. *인증서 검증 사용*을 선택합니다.

당신이 완료한 후

관리되는 호스트 탭 호스트에는 자물쇠 모양이 표시되고 자물쇠 모양 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- *  *는 CA 인증서가 활성화되지 않았거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- *  *는 CA 인증서가 성공적으로 검증되었음을 나타냅니다.
- *  *는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- *  *는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색이나 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

SnapCenter Plug-in for VMware vSphere 설치

데이터베이스나 파일 시스템이 가상 머신(VM)에 저장되어 있거나 VM과 데이터 저장소를 보호하려는 경우 SnapCenter Plug-in for VMware vSphere 배포해야 합니다.

배포에 대한 정보는 다음을 참조하세요. "[배포 개요](#)".

CA 인증서 배포

SnapCenter Plug-in for VMware vSphere 사용하여 CA 인증서를 구성하려면 다음을 참조하세요. "[SSL 인증서 생성 또는 가져오기](#)".

CRL 파일 구성

SnapCenter Plug-in for VMware vSphere 미리 구성된 디렉토리에서 CRL 파일을 찾습니다. SnapCenter Plug-in for VMware vSphere의 CRL 파일의 기본 디렉토리는 `_/opt/netapp/config/crl_`입니다.

이 디렉토리에 두 개 이상의 CRL 파일을 넣을 수 있습니다. 수신 인증서는 각 CRL에 대해 검증됩니다.

Unix 파일 시스템 보호를 준비하세요

백업, 복제, 복원 작업과 같은 데이터 보호 작업을 수행하기 전에 환경을 설정해야 합니다. SnapMirror 및 SnapVault 기술을 사용하도록 SnapCenter 서버를 설정할 수도 있습니다.

SnapVault 및 SnapMirror 기술을 활용하려면 스토리지 장치의 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 구성하고 초기화해야 합니다. NetAppSystem Manager를 사용하거나 스토리지 콘솔 명령줄을 사용하여 이러한 작업을 수행할 수 있습니다.

Unix 파일 시스템용 플러그인을 사용하기 전에 SnapCenter 관리자는 SnapCenter 서버를 설치하고 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다. ["자세히 알아보기"](#)
- 스토리지 시스템 연결을 추가하여 SnapCenter 환경을 구성합니다. ["자세히 알아보기"](#)



SnapCenter 서로 다른 클러스터에서 동일한 이름을 가진 여러 SVM을 지원하지 않습니다. SVM 등록이나 클러스터 등록을 사용하여 SnapCenter에 등록된 각 SVM은 고유해야 합니다.

- 호스트를 추가하고, 플러그인을 설치하고, 리소스를 찾아보세요.
- VMware RDM LUN이나 VMDK에 있는 Unix 파일 시스템을 보호하기 위해 SnapCenter Server를 사용하는 경우 SnapCenter Plug-in for VMware vSphere 배포하고 SnapCenter에 플러그인을 등록해야 합니다.
- Linux 호스트에 Java를 설치합니다.
- 백업 복제가 필요한 경우 ONTAP에서 SnapMirror와 SnapVault 구성합니다.

Unix 파일 시스템 백업

백업에 사용할 수 있는 **UNIX** 파일 시스템을 알아보세요

플러그인을 설치하면 해당 호스트의 모든 파일 시스템이 자동으로 검색되어 리소스 페이지에 표시됩니다. 이러한 파일 시스템을 리소스 그룹에 추가하여 데이터 보호 작업을 수행할 수 있습니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 연결 생성 등의 작업을 완료했어야 합니다.
- 파일 시스템이 VMDK(가상 머신 디스크) 또는 RDM(원시 장치 매핑)에 있는 경우 SnapCenter Plug-in for VMware vSphere 배포하고 SnapCenter에 플러그인을 등록해야 합니다.

자세한 내용은 다음을 참조하세요. ["SnapCenter Plug-in for VMware vSphere 배포"](#).

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *경로*를 선택합니다.
3. *리소스 새로고침*을 클릭하세요.

파일 시스템은 유형, 호스트 이름, 연관된 리소스 그룹 및 정책, 상태와 같은 정보와 함께 표시됩니다.

Unix 파일 시스템에 대한 백업 정책 생성

SnapCenter 사용하여 Unix 파일 시스템을 백업하기 전에 백업하려는 리소스 또는 리소스 그룹에 대한 백업 정책을 만들어야 합니다. 백업 정책은 백업을 관리, 일정을 정하고 보관하는 방법을 규정하는 일련의 규칙입니다. 복제, 스크립트, 백업 유형 설정도 지정할 수 있습니다. 정책을 만들면 다른 리소스나 리소스 그룹에서 정책을 재사용할 때 시간을 절약할 수 있습니다.

시작하기 전에

- SnapCenter 설치, 호스트 추가, 파일 시스템 검색, 스토리지 시스템 연결 생성 등의 작업을 완료하여 데이터 보호를 준비했어야 합니다.
- 스냅샷을 미리 또는 볼트 보조 스토리지에 복제하는 경우 SnapCenter 관리자가 소스 및 대상 볼륨 모두에 대한 SVM을 할당해야 합니다.
- SnapMirror Active Sync의 특정 전제 조건과 제한 사항을 검토하세요. 자세한 내용은 다음을 참조하세요. ["SnapMirror Active Sync에 대한 개체 제한"](#).

이 작업에 관하여

- SnapLock
 - '특정 기간 동안 백업 사본을 보관합니다' 옵션을 선택한 경우 SnapLock 보관 기간은 언급된 보관 기간보다 짧거나 같아야 합니다.

스냅샷 잠금 기간을 지정하면 보존 기간이 만료될 때까지 스냅샷이 삭제되지 않습니다. 이를 통해 정책에 지정된 수보다 더 많은 수의 스냅샷을 보존할 수 있습니다.

ONTAP 9.12.1 이하 버전의 경우 복원의 일부로 SnapLock Vault 스냅샷에서 생성된 복제본은 SnapLock Vault 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *정책*을 클릭합니다.
3. 드롭다운 목록에서 *Unix 파일 시스템*을 선택합니다.
4. *새로 만들기*를 클릭합니다.
5. 이름 페이지에서 정책 이름과 세부 정보를 입력합니다.
6. 백업 및 복제 페이지에서 다음 작업을 수행합니다.
 - a. 백업 설정을 지정합니다.
 - b. 주문형, 매시간, 매일, 매주, 매월 중에서 선택하여 일정 빈도를 지정하세요.

c. 보조 복제 옵션 선택 섹션에서 다음 보조 복제 옵션 중 하나 또는 둘 다를 선택합니다.

이 분야에서는...	이렇게 하세요...
로컬 스냅샷 복사본을 만든 후 SnapMirror 업데이트	다른 볼륨에 백업 세트의 미러 복사본을 생성하려면 이 필드를 선택합니다(SnapMirror 복제). SnapMirror Active Sync의 경우 이 옵션을 활성화해야 합니다.
로컬 스냅샷 복사본을 만든 후 SnapVault 업데이트	디스크 간 백업 복제(SnapVault 백업)를 수행하려면 이 옵션을 선택하세요.
오류 재시도 횟수	작업이 중지되기 전에 허용할 수 있는 최대 복제 시도 횟수를 입력하세요.

7. 보존 페이지에서 백업 및 복제 페이지에서 선택한 백업 유형과 일정 유형에 대한 보존 설정을 지정합니다.

만약 당신이 원한다면...	그 다음에...
특정 수의 스냅샷을 보관하세요	*보관할 사본*을 선택한 다음 보관하려는 스냅샷 수를 지정합니다. 스냅샷 수가 지정된 수를 초과하면 스냅샷이 삭제되고 가장 오래된 사본이 먼저 삭제됩니다.  최대 보존 값은 1018입니다. 보존 기간이 기본 ONTAP 버전에서 지원하는 것보다 높은 값으로 설정된 경우 백업이 실패합니다.  SnapVault 복제를 활성화하려면 보존 횟수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷이 대상에 복제될 때까지 첫 번째 스냅샷이 SnapVault 관계에 대한 참조 스냅샷이 되기 때문에 보존 작업이 실패할 수 있습니다.
스냅샷을 특정 일수 동안 보관하세요	*사본 보관 기간*을 선택한 다음, 스냅샷을 삭제하기 전에 보관할 일수를 지정합니다.
스냅샷 복사 잠금 기간	*스냅샷 복사 잠금 기간*을 선택하고 기간을 일, 월 또는 년 단위로 지정합니다. 스냅샷 보관 기간은 100년 미만이어야 합니다.

8. 정책 라벨을 선택하세요.



원격 복제를 위해 기본 스냅샷에 SnapMirror 레이블을 할당하면 기본 스냅샷이 SnapCenter 에서 ONTAP 보조 시스템으로 스냅샷 복제 작업을 오프로드할 수 있습니다. 정책 페이지에서 SnapMirror 또는 SnapVault 옵션을 활성화하지 않고도 이 작업을 수행할 수 있습니다.

9. 스크립트 페이지에서 백업 작업 전이나 후에 실행할 프리스크립트나 포스트스크립트의 경로와 인수를 각각 입력합니다.



플러그인 호스트에서 사용 가능한 명령 목록에 해당 명령이 있는지 `_ /opt/ NetApp/snapcenter/scc/etc/allowed_commands.config_` 경로에서 확인해야 합니다.

스크립트 시간 초과 값을 지정할 수도 있습니다. 기본값은 60초입니다.

10. 요약을 검토한 후 *마침*을 클릭하세요.

Unix 파일 시스템에 대한 리소스 그룹을 만들고 정책을 첨부합니다.

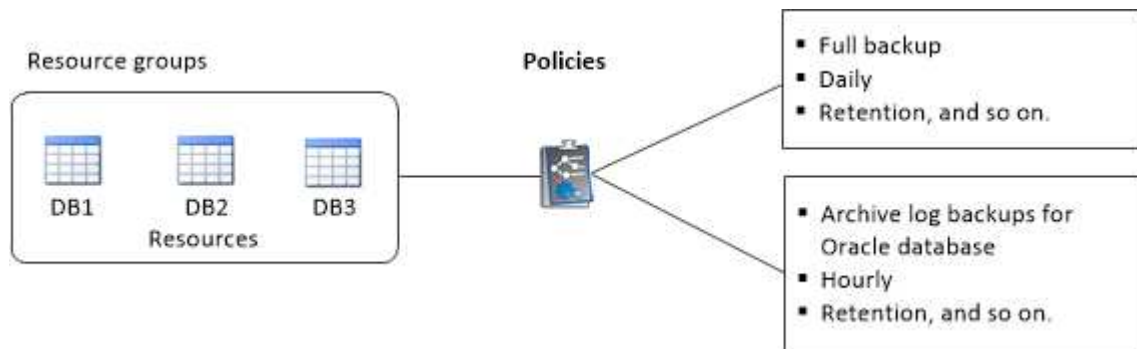
리소스 그룹은 백업하고 보호하려는 리소스를 추가하는 컨테이너입니다. 리소스 그룹을 사용하면 파일 시스템과 관련된 모든 데이터를 백업할 수 있습니다.

이 작업에 관하여

- ASM 디스크 그룹에 파일이 있는 데이터베이스는 Oracle DBVERIFY 유틸리티를 사용하여 백업을 확인하려면 "MOUNT" 또는 "OPEN" 상태여야 합니다.

리소스 그룹에 하나 이상의 정책을 연결하여 수행하려는 데이터 보호 작업 유형을 정의합니다.

다음 이미지는 데이터베이스의 리소스, 리소스 그룹 및 정책 간의 관계를 보여줍니다.



- SnapLock 활성화된 정책의 경우 ONTAP 9.12.1 이하 버전에서 스냅샷 잠금 기간을 지정하면 복원의 일부로 변조 방지 스냅샷에서 생성된 복제본은 SnapLock 만료 시간을 상속받습니다. 스토리지 관리자는 SnapLock 만료 시간 이후에 복제본을 수동으로 정리해야 합니다.
- SnapMirror 활성 동기화가 없는 새 파일 시스템을 SnapMirror 활성 동기화가 있는 리소스가 포함된 기존 리소스 그룹에 추가하는 것은 지원되지 않습니다.
- SnapMirror Active Sync의 장애 조치 모드에서 기존 리소스 그룹에 새 파일 시스템을 추가하는 것은 지원되지 않습니다. 일반 상태나 장애 복구 상태에서만 리소스 그룹에 리소스를 추가할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.

3. 이름 페이지에서 다음 작업을 수행합니다.

- a. 이름 필드에 리소스 그룹의 이름을 입력합니다.



리소스 그룹 이름은 250자를 넘을 수 없습니다.

- b. 나중에 리소스 그룹을 검색하는 데 도움이 되도록 태그 필드에 하나 이상의 레이블을 입력하세요.

예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.

- c. 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 Unix 파일 시스템 호스트 이름을 선택합니다.



리소스가 성공적으로 검색된 경우에만 해당 리소스가 사용 가능한 리소스 섹션에 나열됩니다. 최근에 리소스를 추가한 경우 리소스 목록을 새로 고친 후에만 사용 가능한 리소스 목록에 표시됩니다.

5. 사용 가능한 리소스 섹션에서 리소스를 선택하고 선택한 리소스 섹션으로 이동합니다.

6. 애플리케이션 설정 페이지에서 다음을 수행합니다.

- 스크립트 화살표를 선택하고 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령을 입력합니다. 실패 시 종료하기 전에 실행할 사전 명령을 입력할 수도 있습니다.
- 백업 일관성 옵션 중 하나를 선택하세요.
 - 백업을 생성하기 전에 파일 시스템에 캐시된 데이터가 플러시되고 백업을 생성하는 동안 파일 시스템에서 입력이나 출력 작업이 허용되지 않도록 하려면 *파일 시스템 일관성*을 선택합니다.



파일 시스템 일관성을 위해 볼륨 그룹에 포함된 LUN에 대한 일관성 그룹 스냅샷이 생성됩니다.

- 백업을 생성하기 전에 파일 시스템에 캐시된 데이터가 플러시되도록 하려면 *충돌 일관성*을 선택합니다.



리소스 그룹에 다른 파일 시스템을 추가한 경우 리소스 그룹의 다른 파일 시스템에 있는 모든 볼륨은 일관성 그룹에 배치됩니다.

7. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



또한 다음을 클릭하여 정책을 생성할 수도 있습니다.  .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

- b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.

c. 정책 `_policy_name_`에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 `_policy_name_`은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 `Set-SmSntpServer`를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

ASA r2 시스템에서 Unix 파일 시스템에 대한 리소스 그룹을 만들고 보조 보호를 활성화합니다.

ASA r2 시스템에 있는 리소스를 추가하려면 리소스 그룹을 만들어야 합니다. 리소스 그룹을 생성하는 동안 보조 보호를 프로비저닝할 수도 있습니다.

시작하기 전에

- ONTAP 9.x 리소스와 ASA r2 리소스를 동일한 리소스 그룹에 추가하지 않도록 해야 합니다.
- ONTAP 9.x 리소스와 ASA r2 리소스가 모두 포함된 데이터베이스가 없는지 확인해야 합니다.

이 작업에 관하여

- 2차 보호는 로그인한 사용자에게 **SecondaryProtection** 기능이 활성화된 역할이 할당된 경우에만 사용할 수 있습니다.
- 2차 보호를 활성화한 경우 기본 및 2차 일관성 그룹을 생성하는 동안 리소스 그룹은 유지 관리 모드로 전환됩니다. 기본 및 보조 일관성 그룹이 생성된 후 리소스 그룹은 유지 관리 모드에서 해제됩니다.
- SnapCenter 클론 리소스에 대한 보조 보호를 지원하지 않습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.
 - a. 이름 필드에 리소스 그룹의 이름을 입력합니다.



리소스 그룹 이름은 250자를 넘을 수 없습니다.

- b. 나중에 리소스 그룹을 검색하는 데 도움이 되도록 태그 필드에 하나 이상의 레이블을 입력하세요.

예를 들어, HR을 여러 리소스 그룹에 태그로 추가하면 나중에 해당 HR 태그와 연관된 모든 리소스 그룹을 찾을 수 있습니다.

c. 이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

예를 들어, customtext_resource group_policy_hostname 또는 resource group_hostname입니다.
기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.

d. 백업하지 않을 보관 로그 파일의 대상을 지정합니다.



필요한 경우 접두사를 포함하여 애플리케이션에 설정된 것과 정확히 동일한 목적지를 사용해야 합니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 데이터베이스 호스트 이름을 선택합니다.



리소스가 성공적으로 검색된 경우에만 해당 리소스가 사용 가능한 리소스 섹션에 나열됩니다.
최근에 리소스를 추가한 경우 리소스 목록을 새로 고침 후에만 사용 가능한 리소스 목록에 표시됩니다.

5. 사용 가능한 리소스 섹션에서 ASA r2 리소스를 선택하고 선택한 리소스 섹션으로 이동합니다.

6. 애플리케이션 설정 페이지에서 백업 옵션을 선택하세요.

7. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



또한 다음을 클릭하여 정책을 생성할 수도 있습니다.  .

선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

b. 딸깍 하는 소리  일정을 구성하려는 정책에 대한 일정 구성 열에서.

c. 정책 _policy_name_에 대한 일정 추가 창에서 일정을 구성한 다음 *확인*을 클릭합니다.

여기서 _policy_name_은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

타사 백업 일정은 SnapCenter 백업 일정과 겹치는 경우 지원되지 않습니다.

8. 선택한 정책에 대해 보조 보호가 활성화된 경우 보조 보호 페이지가 표시되며 다음 단계를 수행해야 합니다.

a. 복제 정책의 유형을 선택하세요.



동기 복제 정책은 지원되지 않습니다.

b. 사용할 일관성 그룹 접미사를 지정합니다.

c. 대상 클러스터 및 대상 SVM 드롭다운에서 사용하려는 피어링된 클러스터와 SVM을 선택합니다.



SnapCenter에서는 클러스터 및 SVM 피어링을 지원하지 않습니다. 클러스터 및 SVM 피어링을 수행하려면 System Manager 또는 ONTAP CLI를 사용해야 합니다.



리소스가 이미 SnapCenter 외부에서 보호되고 있는 경우 해당 리소스는 보조 보호 리소스 섹션에 표시됩니다.

1. 확인 페이지에서 다음 단계를 수행하세요.

- a. *로케이터 로드*를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 저장소에서 검증을 수행합니다.
- b. 딸깍 하는 소리  일정 구성 열에서 정책의 모든 일정 유형에 대한 확인 일정을 구성합니다.
- c. 확인 일정 추가 policy_name 대화 상자에서 다음 작업을 수행합니다.

만약 당신이 원한다면...	이렇게 하세요...
백업 후 검증 실행	*백업 후 검증 실행*을 선택하세요.
검증 일정을 예약하세요	*예약된 확인 실행*을 선택한 다음 드롭다운 목록에서 일정 유형을 선택합니다.

- d. 보조 저장소 시스템에서 백업을 확인하려면 *보조 위치에서 확인*을 선택하세요.
- e. *확인*을 클릭합니다.

구성된 검증 일정은 적용된 일정 열에 나열됩니다.

2. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스 그룹에서 수행된 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtplibServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

3. 요약 검토한 후 *마침*을 클릭하세요.

Unix 파일 시스템 백업

리소스가 어떤 리소스 그룹에도 속하지 않은 경우 리소스 페이지에서 리소스를 백업할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 *경로*를 선택합니다.
3. 딸깍 하는 소리  그런 다음 호스트 이름과 Unix 파일 시스템을 선택하여 리소스를 필터링합니다.
4. 백업할 파일 시스템을 선택하세요.
5. 리소스 페이지에서 다음 단계를 수행할 수 있습니다.
 - a. 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

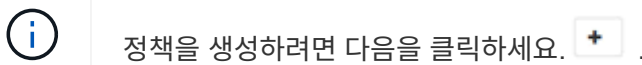
예를 들어, `customtext_policy_hostname` 또는 `resource_hostname`. 기본적으로 스냅샷 이름에 타임스탬프가 추가됩니다.

6. 애플리케이션 설정 페이지에서 다음을 수행합니다.

- 스크립트 화살표를 선택하고 정지, 스냅샷, 정지 해제 작업에 대한 사전 및 사후 명령을 입력합니다. 실패 시 종료하기 전에 실행할 사전 명령을 입력할 수도 있습니다.
- 백업 일관성 옵션 중 하나를 선택하세요.
 - 백업을 생성하기 전에 파일 시스템에 캐시된 데이터가 플러시되고 백업을 생성하는 동안 파일 시스템에서 아무런 작업도 수행되지 않도록 하려면 *파일 시스템 일관성*을 선택합니다.
 - 백업을 생성하기 전에 파일 시스템에 캐시된 데이터가 플러시되도록 하려면 *충돌 일관성*을 선택합니다.

7. 정책 페이지에서 다음 단계를 수행합니다.

- a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.



선택한 정책에 대한 일정 구성 섹션에서는 선택한 정책이 나열됩니다.

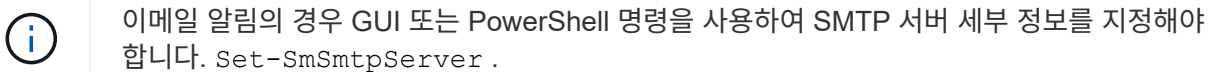
- b. 딸깍 하는 소리  일정 구성 열에서 원하는 정책에 대한 일정을 구성합니다.
- c. 정책 `_policy_name_`에 대한 일정 추가 창에서 일정을 구성한 다음 다음을 선택합니다. OK .

`_policy_name_`은 선택한 정책의 이름입니다.

구성된 일정은 적용된 일정 열에 나열됩니다.

8. 알림 페이지에서 이메일 기본 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 리소스에서 수행된 백업 작업 보고서를 첨부하려면 *작업 보고서 첨부*을 선택하세요.



9. 요약 검토한 후 *마침*을 클릭하세요.

토폴로지 페이지가 표시됩니다.

10. *지금 백업*을 클릭하세요.

11. 백업 페이지에서 다음 단계를 수행합니다.

- a. 리소스에 여러 정책을 적용한 경우 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. *백업*을 클릭하세요.

12. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

Unix 파일 시스템 리소스 그룹 백업

리소스 그룹에 정의된 Unix 파일 시스템을 백업할 수 있습니다. 리소스 페이지에서 필요에 따라 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 첨부되고 일정이 구성된 경우 일정에 따라 백업이 생성됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택하고 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.
3. 검색창에 리소스 그룹 이름을 입력하거나 클릭하세요. , 태그를 선택하세요.

딸깍 하는 소리  필터 창을 닫으려면.

4. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택합니다.
5. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스 그룹과 연관된 정책이 여러 개 있는 경우 정책 드롭다운 목록에서 사용할 백업 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. *백업*을 선택하세요.
6. *모니터 > 작업*을 선택하여 진행 상황을 모니터링하세요.

Unix 파일 시스템 백업 모니터링

백업 작업과 데이터 보호 작업의 진행 상황을 모니터링하는 방법을 알아보세요.

Unix 파일 시스템 백업 작업 모니터링

SnapCenterJobs 페이지를 사용하여 다양한 백업 작업의 진행 상황을 모니터링할 수 있습니다. 완료 시점이나 문제가 있는지 확인하기 위해 진행 상황을 확인하는 것이 좋습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 해당 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  백업 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *백업*을 선택합니다.
 - d. 상태 드롭다운에서 백업 상태를 선택합니다.
 - e. *적용*을 클릭하면 작업이 성공적으로 완료된 것을 볼 수 있습니다.
4. 백업 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인하세요.



백업 작업 상태가 표시됩니다.  작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 표시가 되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

활동 창에서 데이터 보호 작업 모니터링

활동 창에는 가장 최근에 수행된 5개의 작업이 표시됩니다. 활동 창에는 작업이 시작된 시점과 작업 상태도 표시됩니다.

활동 창에는 백업, 복원, 복제 및 예약된 백업 작업에 대한 정보가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 딸깍 하는 소리  활동 창에서 가장 최근의 작업 5개를 확인하세요.

작업 중 하나를 클릭하면 작업 세부 정보가 작업 세부 정보 페이지에 나열됩니다.

토폴로지 페이지에서 보호된 **Unix** 파일 시스템 보기

리소스를 백업, 복원 또는 복제할 준비를 할 때 기본 및 보조 저장소에 있는 모든 백업, 복원된 파일 시스템 및 복제본의 그래픽 표현을 보는 것이 도움이 될 수 있습니다.

이 작업에 관하여

토폴로지 페이지에서는 선택한 리소스 또는 리소스 그룹에 사용 가능한 모든 백업, 복원된 파일 시스템 및 복제본을 볼 수 있습니다. 해당 백업, 복원된 파일 시스템 및 복제본의 세부 정보를 보고 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

다음 아이콘을 '사본 관리' 보기에서 검토하여 백업 및 복제본을 기본 저장소 또는 보조 저장소(미러 사본 또는 볼트 사본)에서 사용할 수 있는지 확인할 수 있습니다.

•



기본 스토리지에서 사용 가능한 백업 및 복제본의 수를 표시합니다.



SnapMirror 기술을 사용하여 보조 저장소에 미러링된 백업 및 복제본의 수를 표시합니다.



SnapVault 기술을 사용하여 보조 저장소에 복제된 백업 및 복제본의 수를 표시합니다.

표시된 백업 수에는 보조 저장소에서 삭제된 백업이 포함됩니다. 예를 들어, 4개의 백업만 보존하는 정책을 사용하여 6개의 백업을 만든 경우 표시되는 백업 수는 6개입니다.



미러 볼트 유형 볼륨의 버전 가변형 미러 백업의 복제본은 토폴로지 보기에 표시되지만, 토폴로지 보기의 미러 백업 수에는 버전 가변형 백업이 포함되지 않습니다.

SnapMirror Active Sync(처음에는 SnapMirror Business Continuity[SM-BC]로 출시됨)라는 보조 관계가 있는 경우 다음과 같은 추가 아이콘을 볼 수 있습니다.



복제 사이트가 오픈되었습니다.



복제 사이트가 다운되었습니다.



2차 거울이나 볼트 관계가 재설정되지 않았습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 리소스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 리소스를 선택합니다.

리소스가 보호된 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. 요약 카드를 검토하여 기본 및 보조 저장소에서 사용 가능한 백업 및 복제본 수에 대한 요약 확인하세요.

요약 카드 섹션에는 백업 및 복제의 총 수가 표시됩니다.

새로 고침 버튼을 클릭하면 저장소에 대한 쿼리가 시작되어 정확한 개수가 표시됩니다.

SnapLock 이 활성화된 백업을 수행한 경우 새로 고침 버튼을 클릭하면 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간이 새로 고쳐집니다. 주간 일정은 ONTAP 에서 검색된 기본 및 보조 SnapLock 만료 시간도 새로 고칩니다.

파일 시스템이 여러 볼륨에 분산되어 있는 경우 백업에 대한 SnapLock 만료 시간은 볼륨의 스냅샷에 설정된 가장 긴 SnapLock 만료 시간이 됩니다. 가장 긴 SnapLock 만료 시간은 ONTAP 에서 검색됩니다.

SnapMirror 활성 동기화의 경우, 새로 고침 버튼을 클릭하면 ONTAP 기본 사이트와 복제 사이트를 모두 쿼리하여 SnapCenter 백업 인벤토리가 새로 고쳐집니다. 주간 일정은 SnapMirror 활성 동기화 관계가 포함된 모든 데이터베이스에 대해 이 활동을 수행합니다.

- SnapMirror 활성화 및 ONTAP 9.14.1의 경우에만 장애 조치 후 새 기본 대상에 대한 비동기 미러 또는 비동기 MirrorVault 관계를 수동으로 구성해야 합니다. ONTAP 9.15.1부터 비동기 미러 또는 비동기 미러볼트가 새로운 기본 대상으로 자동 구성됩니다.
- 장애 조치 후에는 SnapCenter 에서 장애 조치를 인식할 수 있도록 백업을 만들어야 합니다. 백업이 생성된 후에만 *새로 고침*을 클릭할 수 있습니다.

5. 복사본 관리 보기에서 기본 또는 보조 저장소의 백업 또는 *복제*를 클릭하면 백업 또는 복제의 세부 정보를 볼 수 있습니다.

백업 및 복제의 세부 정보는 표 형식으로 표시됩니다.

6. 표에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 복제, 삭제 작업을 수행합니다.



보조 저장소에 있는 백업은 이름을 바꾸거나 삭제할 수 없습니다.

7. 복제본을 삭제하려면 테이블에서 복제본을 선택한 다음 클릭하세요.  .

기본 스토리지의 백업 및 복제를 보여주는 예

Manage Copies	Summary Card
 2 Backups	2 Backups
1 Clone	1 Clone
Local copies	0 Snapshots Locked

Unix 파일 시스템 복원 및 복구

Unix 파일 시스템 복원

데이터 손실이 발생한 경우 SnapCenter 사용하여 Unix 파일 시스템을 복원할 수 있습니다.

이 작업에 관하여

- SnapCenter 서버와의 연결을 설정하고, 백업을 나열하고 해당 정보를 검색하고, 백업을 복원하려면 다음 명령을 실행해야 합니다.

명령과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `Get-Help _command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 명령 참조 가이드](#)".

- SnapMirror Active Sync 복원 작업의 경우 기본 위치에서 백업을 선택해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 경로 또는 *리소스 그룹*을 선택합니다.
3. 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 파일 시스템을 선택합니다.

토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 *백업*을 선택합니다.

5. 테이블에서 백업을 선택한 후 *를 클릭합니다.  *.

6. 복원 범위 페이지에서:

- NFS 파일 시스템의 경우 기본적으로 연결 및 복사 복원이 선택됩니다. 볼륨 되돌리기 또는 *빠른 복원*을 선택할 수도 있습니다.
- NFS가 아닌 파일 시스템의 경우, 복원 범위는 레이아웃에 따라 선택됩니다.

백업 후 생성된 새 파일은 파일 시스템 유형 및 레이아웃에 따라 복원 후에 사용할 수 없을 수 있습니다.

7. PreOps 페이지에서 복원 작업을 수행하기 전에 실행할 복원 전 명령을 입력합니다.
8. PostOps 페이지에서 복원 작업을 수행한 후 실행할 복원 후 명령을 입력합니다.



플러그인 호스트의 `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config` 경로에서 사용 가능한 명령 목록에 해당 명령이 있는지 확인해야 합니다.

9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일 알림을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 수행된 복구 작업 보고서를 첨부하려면 *작업 보고서 첨부*를 선택해야 합니다.



이메일 알림을 받으려면 GUI 또는 PowerShell 명령 `Set-SmSmtplibServer`를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

10. 요약 검토 후 *마침*을 클릭하세요.



복원 작업이 실패하면 롤백이 지원되지 않습니다.



볼륨 그룹에 있는 파일 시스템을 복원하는 경우, 파일 시스템의 이전 내용은 삭제되지 않습니다. 복제된 파일 시스템의 콘텐츠만 소스 파일 시스템으로 복사됩니다. 이는 볼륨 그룹에 여러 개의 파일 시스템이 있고 기본 NFS 파일 시스템을 복원하는 경우에 적용됩니다.

11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

Unix 파일 시스템 복원 작업 모니터링

작업 페이지를 사용하여 다양한 SnapCenter 복원 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

복원 후 상태는 복원 작업 후 리소스의 조건과 수행할 수 있는 추가 복원 작업을 설명합니다.

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복원 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복원*을 선택합니다.
 - d. 상태 드롭다운 목록에서 복원 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.
4. 복원 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

로그 보기 버튼을 클릭하면 선택한 작업에 대한 자세한 로그가 표시됩니다.

유닉스 파일 시스템 복제

Unix 파일 시스템 백업 복제

SnapCenter 사용하면 파일 시스템의 백업을 사용하여 Unix 파일 시스템을 복제할 수 있습니다.

시작하기 전에

- *agent.properties* 파일(/opt/NetApp/snapcenter/scc/etc)에서 *SKIP_FSTAB_UPDATE* 값을 *true*로 설정하면 fstab 파일 업데이트를 건너뛸 수 있습니다.
- *agent.properties* 파일(/opt/NetApp/snapcenter/scc/etc)에서 *USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT* 값을 *true*로 설정하면 정적 복제 볼륨 이름과 연결 경로를 사용할 수 있습니다. 파일을 업데이트한 후 다음 명령을 실행하여 SnapCenter 플러그인 생성 서비스를 다시 시작해야 합니다. /opt/NetApp/snapcenter/scc/bin/scc restart .

예: 이 속성이 없으면 복제 볼륨 이름과 접합 경로는 <Source_volume_name>_Clone_<Timestamp>와 같지만 이제는 <Source_volume_name>_Clone_<Clone_Name>이 됩니다.

이렇게 하면 이름이 일정하게 유지되므로 SnapCenter 에서 fstab을 업데이트하지 않으려는 경우 fstab 파일을 수동으로 업데이트할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 경로 또는 *리소스 그룹*을 선택합니다.
3. 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 파일 시스템을 선택합니다.

토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 로컬 복사본(기본), 미러 복사본(보조) 또는 볼트 복사본(보조) 중에서 백업을 선택합니다.
5. 테이블에서 백업을 선택한 후 *를 클릭합니다.  *.
6. 위치 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
복제 서버	기본적으로 소스 호스트가 채워져 있습니다.
클론 마운트 지점	파일 시스템이 마운트될 경로를 지정합니다.

7. 스크립트 페이지에서 다음 단계를 수행합니다.

- a. 복제 작업 전이나 후에 실행해야 하는 사전 복제 또는 사후 복제에 대한 명령을 각각 입력합니다.



플러그인 호스트에서 사용 가능한 명령 목록에 해당 명령이 있는지 /opt/NetApp/snapcenter/scc/etc/allowed_commands.config 경로에서 확인해야 합니다.

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. 수행된 복제 작업의 보고서를 첨부하려면 *작업 보고서 첨부*를 선택하세요.



이메일 알림을 받으려면 GUI나 PowerShell 명령 Set-SmSmtServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

10. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

클론 분할

SnapCenter 사용하면 복제된 리소스를 부모 리소스에서 분할할 수 있습니다. 분할된 복제본은 부모 리소스로부터 독립됩니다.

이 작업에 관하여

- 중간 복제본에서는 복제 분할 작업을 수행할 수 없습니다.

예를 들어, 데이터베이스 백업에서 clone1을 만든 후 clone1의 백업을 만든 다음 이 백업(clone2)을 복제할 수 있습니다. clone2를 생성한 후 clone1은 중간 복제본이 되며 clone1에서 복제 분할 작업을 수행할 수 없습니다. 하지만 clone2에 대해 클론 분할 작업을 수행할 수 있습니다.

clone2를 분할한 후에는 clone1에 대해 clone 분할 작업을 수행할 수 있습니다. clone1은 더 이상 중간 클론이 아니기 때문입니다.

- 복제본을 분할하면 복제본의 백업 사본과 복제 작업이 삭제됩니다.
- FlexClone 볼륨 분할 작업에 대한 정보는 다음을 참조하세요. ["FlexClone 볼륨을 부모 볼륨에서 분할합니다."](#) .
- 스토리지 시스템의 볼륨이나 집계가 온라인인지 확인하세요.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 적절한 옵션을 선택하세요.

옵션	설명
데이터베이스 애플리케이션의 경우	보기 목록에서 *데이터베이스*를 선택합니다.
파일 시스템의 경우	보기 목록에서 *경로*를 선택합니다.

3. 목록에서 적절한 리소스를 선택하세요.

리소스 토폴로지 페이지가 표시됩니다.

4. 사본 관리 보기에서 복제된 리소스(예: 데이터베이스 또는 LUN)를 선택한 다음 *를 클릭합니다.  *.
5. 분할할 클론의 예상 크기와 집계에 필요한 사용 가능한 공간을 검토한 다음 *시작*을 클릭합니다.
6. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

SMCore 서비스를 다시 시작하면 복제 분할 작업이 더 이상 응답하지 않습니다. 복제 분할 작업을 중지하려면 Stop-SmJob cmdlet을 실행한 다음 복제 분할 작업을 다시 시도해야 합니다.

복제본이 분할되었는지 여부를 확인하기 위해 더 긴 폴링 시간이나 더 짧은 폴링 시간이 필요한 경우 *SMCoreServiceHost.exe.config* 파일에서 *CloneSplitStatusCheckPollTime* 매개변수 값을 변경하여 SMCore가 복제본 분할 작업의 상태를 폴링하는 시간 간격을 설정할 수 있습니다. 값은 밀리초이고 기본값은 5분입니다.

예를 들어:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

백업, 복원 또는 다른 클론 분할이 진행 중이면 클론 분할 시작 작업이 실패합니다. 실행 중인 작업이 완료된 후에만 복제 분할 작업을 다시 시작해야 합니다.

관련 정보

"SnapCenter 복제 또는 검증이 집계기 존재하지 않아 실패합니다."

Unix 파일 시스템 복제 작업 모니터링

작업 페이지를 사용하여 SnapCenter 복제 작업의 진행 상황을 모니터링할 수 있습니다. 작업이 완료되었는지 또는 문제가 있는지 확인하기 위해 작업 진행 상황을 확인하고 싶을 수 있습니다.

이 작업에 관하여

다음 아이콘은 작업 페이지에 나타나며 작업 상태를 나타냅니다.

-  진행 중
-  성공적으로 완료되었습니다
-  실패한
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다.
-  대기 중
-  취소

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *작업*을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행합니다.
 - a. 딸깍 하는 소리  복제 작업만 나열되도록 목록을 필터링합니다.
 - b. 시작일과 종료일을 지정하세요.
 - c. 유형 드롭다운 목록에서 *복제*를 선택합니다.
 - d. 상태 드롭다운 목록에서 복제 상태를 선택합니다.
 - e. 성공적으로 완료된 작업을 보려면 *적용*을 클릭하세요.

4. 복제 작업을 선택한 다음 *세부 정보*를 클릭하여 작업 세부 정보를 확인합니다.
5. 작업 세부 정보 페이지에서 *로그 보기*를 클릭합니다.

Azure NetApp Files 에서 실행되는 애플리케이션 보호

Azure NetApp Files 에서 실행되는 애플리케이션 보호

SnapCenter Azure NetApp Files 에 있는 Oracle, SQL, SAP HANA와 같은 애플리케이션을 보호하는 것을 지원합니다. SnapCenter 6.0.1 릴리스부터 장기 복구, 보관 및 규정 준수를 위한 완전 관리형 백업 솔루션을 제공하여 Azure NetApp Files 의 데이터 보호 기능을 확장하는 Azure NetApp Files 백업 기능을 지원합니다.

Azure NetApp Files 는 장기 백업 보존에 비용이 많이 들 수 있는 프리미엄 스토리지 솔루션입니다. 비용을 최적화하려면 Azure NetApp Files 저장소에서 Azure 개체 저장소로 백업을 이동할 수 있습니다. SnapCenter 6.0.1부터 Azure NetApp Files 에 있는 애플리케이션을 Azure Blob Storage(개체 저장소)로 백업하고 복제할 수 있습니다. 단기 복구를 위해 Azure NetApp Files 저장소에 볼륨 스냅샷 복사본을 보관하고, 장기 복구를 위해 Azure Blob Storage에 또 다른 복사본을 보관하여 두 개의 데이터 복사본을 유지할 수 있습니다.

Azure NetApp Files 백업이 포함된 정책이 활성화되고 리소스와 연결되면 SnapCenter 볼륨 스냅샷을 생성하고 Azure Blob Storage에 백업합니다. SnapCenter 백업 볼트를 생성하고 볼륨에 대한 백업을 활성화합니다. 볼륨에 대한 백업을 활성화한 경우 SnapCenter 기존 볼트를 활용합니다.

제한 사항

- FAS, ASA 또는 AFF ONTAP 및 Amazon FSx for NetApp ONTAP 스토리지 시스템에 대한 개체 스토리지 기능은 지원되지 않습니다.
- Oracle 및 SAP HANA 마운트 및 카탈로그 워크플로는 개체 스토리지 백업에는 지원되지 않지만 스냅샷에는 지원됩니다.
- Oracle PDB 복제본은 개체 스토리지 백업에는 지원되지 않지만 스냅샷에는 지원됩니다.
- 개체 스토리지에서의 백업 검증, REST API 지원, 개체 스토리지에서의 복제 수명 주기 관리, 개체 스토리지 백업에 대한 보고 기능은 지원되지 않습니다.
- Azure Blob Storage의 백업에서 Azure NetApp Files 로 복원하는 기능은 지원되지 않습니다. 또는 복제 옵션을 사용할 수도 있습니다.
- 복제 분할은 지원되지 않습니다.

SnapCenter 설치하고 자격 증명을 만듭니다.

Azure 가상 머신에 SnapCenter 설치

NetApp 지원 사이트에서 SnapCenter software 다운로드하여 Azure 가상 머신에 소프트웨어를 설치할 수 있습니다.

시작하기 전에

- Azure Windows 가상 머신이 SnapCenter 서버 설치에 필요한 요구 사항을 충족하는지 확인하세요. 자세한 내용은 다음을 참조하세요. "[SnapCenter 서버 설치 요구 사항](#)".
- Azure NetApp Files 처음 사용하고 기존 NetApp 계정이 없는 경우 SnapCenter 소프트웨어에 액세스할 수 있도록 등록했는지 확인하세요. 자세한 내용은 다음을 참조하세요. "[SnapCenter software 액세스하려면 등록하세요](#)".

단계

1. SnapCenter 서버 설치 패키지를 다운로드하세요. "[NetApp 지원 사이트](#)".
2. 다운로드한 .exe 파일을 두 번 클릭하여 SnapCenter 서버 설치를 시작합니다.

설치를 시작하면 모든 사전 검사가 수행되고 최소 요구 사항을 충족하지 못하면 해당 오류 또는 경고 메시지가 표시됩니다. 경고 메시지를 무시하고 설치를 진행할 수 있습니다. 그러나 오류는 수정되어야 합니다.

3. SnapCenter 서버 설치에 필요한 미리 채워진 값을 검토하고 필요한 경우 수정합니다.

MySQL 서버 저장소 데이터베이스에 대한 비밀번호를 지정할 필요는 없습니다. SnapCenter 서버를 설치하는 동안 비밀번호가 자동으로 생성됩니다.



저장소 데이터베이스의 사용자 지정 경로에서는 특수 문자 "%"가 지원되지 않습니다. 경로에 "%"를 포함하면 설치가 실패합니다.

4. *지금 설치*를 클릭하세요.

잘못된 값을 지정한 경우 해당 오류 메시지가 표시됩니다. 값을 다시 입력한 다음 설치를 시작하세요.



취소 버튼을 클릭하면 실행 중인 단계가 완료되고, 이후 롤백 작업이 시작됩니다. SnapCenter 서버가 호스트에서 완전히 제거됩니다.

하지만 "SnapCenter 서버 사이트 재시작" 또는 "SnapCenter 서버 시작 대기" 작업이 수행되는 동안 *취소*를 클릭하면 작업을 취소하지 않고 설치가 진행됩니다.

지원을 받으려면 제품을 등록하세요

NetApp 처음 사용하고 기존 NetApp 계정이 없는 경우 지원을 받으려면 제품을 등록해야 합니다.

단계

1. SnapCenter 설치한 후 *도움말 > 정보*로 이동합니다.
2. SnapCenter 정보 대화 상자에서 971로 시작하는 20자리 숫자인 SnapCenter 인스턴스를 기록해 둡니다.
3. 딸깍 하는 소리 <https://register.netapp.com>.
4. *저는 등록된 NetApp 고객이 아닙니다*를 클릭하세요.
5. 등록하려면 세부 정보를 입력하세요.
6. NetApp 참조 SN 필드를 비워 두세요.
7. 제품 라인 드롭다운에서 *SnapCenter*를 선택합니다.
8. 청구 제공자를 선택하세요.
9. 20자리 SnapCenter 인스턴스 ID를 입력하세요.
10. *제출*을 클릭하세요.

SnapCenter 에서 Azure 자격 증명 만들기

Azure NetApp 계정에 액세스하려면 SnapCenter 에서 Azure 자격 증명을 만들어야 합니다.

시작하기 전에

- Azure에서 서비스 주체를 만들었는지 확인하세요.
- 서비스 주체와 연결된 테넌트 ID, 클라이언트 ID 및 비밀 키를 사용할 수 있는지 확인하세요.
 - 테넌트 ID는 Azure Portal의 Entra ID 개요 페이지에서 찾을 수 있습니다.
 - 클라이언트 ID는 엔터프라이즈 앱/서비스 주체의 애플리케이션 ID라고도 합니다. 이는 SnapCenter의 서비스 주체 역할을 하도록 만든 엔터프라이즈 애플리케이션의 개요 페이지에 있는 Azure Portal에서 찾을 수 있습니다.
 - 클라이언트 비밀 키는 비밀 값이라고도 합니다. Azure Portal에서 Entra ID 아래의 *앱 등록*으로 이동하여 이 클라이언트 비밀번호를 만들 수 있습니다. 생성한 엔터프라이즈 앱을 선택한 후 *인증서 및 비밀번호*로 이동한 다음 *새 클라이언트 비밀번호*로 이동합니다.



비밀 값은 생성될 때만 접근할 수 있습니다. 나중에 접근할 수 없습니다.

- 서비스 주체에게 권한을 부여해야 합니다. 기여자 역할을 통해 서비스 주체는 Azure에서 필요한 작업을 수행할 수 있습니다. 이는 구독 페이지 내의 액세스 제어(IAM) 페이지에서 부여할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *자격 증명*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 자격 증명 페이지에서 자격 증명을 만드는 데 필요한 다음 정보를 지정하세요.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.
인증 모드	드롭다운 목록에서 *Azure 자격 증명*을 선택합니다.
세입자 ID	세입자 ID를 입력하세요.
클라이언트 ID	클라이언트 ID를 입력하세요.
클라이언트 비밀 키	클라이언트 비밀 키를 입력하세요.

5. *확인*을 클릭합니다.

Azure 스토리지 계정 구성

SnapCenter에서 Azure 스토리지 계정을 구성해야 합니다.

Azure 스토리지 계정에는 구독 ID, Azure 자격 증명 및 Azure NetApp 계정에 대한 세부 정보가 포함되어 있습니다.



Azure NetApp Files에는 표준 라이선스 및 용량 기반 라이선스가 필요하지 않습니다.

단계

1. 왼쪽 탐색 창에서 *저장 시스템*을 클릭합니다.
2. 스토리지 시스템 페이지에서 * Azure NetApp Files*를 선택하고 *새로 만들기*를 클릭합니다.
3. 해당 드롭다운 목록에서 자격 증명, 구독 ID 및 NetApp 계정을 선택합니다.
4. *제출*을 클릭하세요.

플러그인 호스트를 추가하기 위한 자격 증명을 만듭니다.

SnapCenter 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다.

SnapCenter 플러그인을 설치하기 위한 자격 증명과 데이터 보호 작업을 수행하기 위한 추가 자격 증명을 만들어야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *자격 증명*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 자격 증명 페이지에서 자격 증명을 만드는 데 필요한 다음 정보를 지정하세요.

이 분야에서는...	이렇게 하세요...
자격 증명 이름	자격 증명의 이름을 입력하세요.
인증 모드	드롭다운 목록에서 인증 모드를 선택하세요.
인증 유형	비밀번호 기반 또는 *SSH 키 기반*을 선택하세요(Linux 호스트에만 해당).
사용자 이름	사용자 이름을 지정하세요.
비밀번호	비밀번호 기반 인증을 선택한 경우 비밀번호를 지정합니다.
SSH 개인 키	SSH 키 기반 인증을 선택한 경우 개인 키를 지정합니다.
sudo 권한을 사용하세요	루트가 아닌 사용자에게 자격 증명을 생성하는 경우 sudo 권한 사용 확인란을 선택합니다.  이는 Linux 사용자에게만 적용됩니다.

5. *확인*을 클릭합니다.

SAP HANA 데이터베이스 보호

호스트를 추가하고 **SAP HANA** 데이터베이스용 **SnapCenter** 플러그인을 설치합니다.

SnapCenter 호스트 추가 페이지를 사용하여 호스트를 추가한 다음 플러그인 패키지를 설치해야 합니다. 플러그인은 원격 호스트에 자동으로 설치됩니다.

시작하기 전에

- SnapCenter 관리자 역할과 같이 플러그인 설치 및 제거 권한이 있는 역할에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.
- 중앙 호스트에 설치하는 경우 SAP HANA 클라이언트 소프트웨어가 해당 호스트에 설치되어 있는지 확인하고 SAP HANA 데이터베이스 호스트에서 필요한 포트를 열어 HDB SQL 쿼리를 원격으로 실행하세요.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 관리되는 호스트 탭이 선택되어 있는지 확인하세요.
3. *추가*를 클릭하세요.
4. 호스트 페이지에서 다음 작업을 수행합니다.
 - a. 호스트 유형 필드에서 호스트 유형을 선택합니다.
 - b. 호스트 이름 필드에 호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력합니다.
 - c. 자격 증명 필드에 귀하가 만든 자격 증명을 입력합니다.
5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.
6. (선택 사항) *추가 옵션*을 클릭하고 세부 정보를 지정합니다.
7. *제출*을 클릭하세요.
8. 호스트 유형이 Linux인 경우 지문을 확인한 다음 *확인 및 제출*을 클릭합니다.

클러스터 설정에서는 클러스터의 각 노드의 지문을 확인해야 합니다.

9. 설치 진행 상황을 모니터링합니다.

SAP HANA 데이터베이스 추가

SAP HANA 데이터베이스를 수동으로 추가해야 합니다.

이 작업에 관하여

플러그인이 중앙 서버에 설치된 경우 리소스를 수동으로 추가해야 합니다. SAP HANA 플러그인이 HANA 데이터베이스 호스트에 설치된 경우 HANA 시스템이 자동으로 검색됩니다.



HANA 멀티 호스트 구성에서는 자동 검색이 지원되지 않으므로 중앙 플러그인을 통해서만 추가해야 합니다.

단계

1. 왼쪽 탐색 창에서 드롭다운 목록에서 SAP HANA 데이터베이스용 SnapCenter 플러그인을 선택한 다음 *리소스*를 클릭합니다.
2. 리소스 페이지에서 *SAP HANA 데이터베이스 추가*를 클릭합니다.
3. 리소스 세부 정보 제공 페이지에서 다음 작업을 수행합니다.
 - a. 리소스 유형을 단일 컨테이너, 다중 테넌트 데이터베이스 컨테이너 또는 비데이터 볼륨으로 입력합니다.
 - b. SAP HANA 시스템 이름을 입력하세요.
 - c. 시스템 ID(SID)를 입력하세요.
 - d. 플러그인 호스트를 선택하세요.
 - e. SAP HANA 시스템에 연결하려면 키를 입력하세요.
 - f. HDB 보안 사용자 저장 키가 구성된 사용자 이름을 입력하세요.
4. 저장소 공간 제공 페이지에서 저장소 유형으로 * Azure NetApp Files*를 선택합니다.
 - a. Azure NetApp 계정을 선택합니다.
 - b. 용량 풀과 관련 볼륨을 선택합니다.
 - c. *저장*을 클릭하세요.
5. 요약을 검토한 후 *마침*을 클릭하세요.

SAP HANA 데이터베이스에 대한 백업 정책 만들기

SnapCenter 사용하여 SAP HANA 데이터베이스 리소스를 백업하기 전에 백업하려는 리소스 또는 리소스 그룹에 대한 백업 정책을 만들어야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *정책*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 이름 페이지에서 정책 이름과 설명을 입력합니다.
5. 정책 유형 페이지에서 다음 단계를 수행합니다.
 - a. 저장소 유형으로 * Azure NetApp Files*를 선택합니다.
 - b. 데이터베이스의 무결성 검사를 수행하려면 *파일 기반*을 선택합니다.
 - c. 스냅샷 기술을 사용하여 백업을 만들려면 *스냅샷 기반*을 선택하세요.
6. 스냅샷 및 백업 페이지에서 다음 단계를 수행합니다.
 - a. 예약된 백업의 빈도를 선택하세요.
 - b. 보존 설정을 지정합니다.
 - c. Azure NetApp Files 백업을 활성화하려면 *백업 활성화*를 선택하고 보존 설정을 지정합니다.
7. 요약을 검토하고 *마침*을 클릭하세요.

리소스 그룹을 생성하고 **SAP HANA** 백업 정책을 연결합니다.

리소스 그룹은 백업하고 보호하려는 리소스를 추가해야 하는 컨테이너입니다.

리소스 그룹을 사용하면 주어진 애플리케이션과 관련된 모든 데이터를 동시에 백업할 수 있습니다. 모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한, 수행하려는 데이터 보호 작업 유형을 정의하려면 리소스 그룹에 하나 이상의 정책을 연결해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	리소스 그룹의 이름을 입력하세요.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력하세요.
스냅샷 복사에 사용자 정의 이름 형식 사용	이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 호스트 이름을 선택하고 리소스 유형 드롭다운 목록에서 리소스 유형을 선택합니다.
5. 사용 가능한 리소스 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 클릭하여 선택한 리소스 섹션으로 이동합니다.
6. 정책 페이지에서 다음 단계를 수행합니다.
 - a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.
 - b. 일정 구성 열에서 *를 클릭합니다.  * 구성하려는 정책에 대해.
 - c. 정책 _policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 클릭합니다.
7. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.
8. 요약 검토 후 *마침*을 클릭하세요.

Azure NetApp Files 에서 실행되는 **SAP HANA** 데이터베이스 백업

리소스가 아직 어떤 리소스 그룹에도 속하지 않은 경우 리소스 페이지에서 리소스를 백업할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.
3. 백업할 리소스를 선택하세요.

4. 리소스 페이지에서 *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택한 다음 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.
 5. 애플리케이션 설정 페이지에서 다음을 수행합니다.
 - a. 추가 백업 옵션을 설정하려면 백업 화살표를 선택하세요.
 - b. 스크립트 화살표를 선택하여 정지, 스냅샷 및 정지 해제 작업에 대한 사전 및 사후 명령을 실행합니다.
 - c. 사용자 정의 구성 화살표를 선택한 다음, 이 리소스를 사용하는 모든 작업에 필요한 사용자 정의 값 쌍을 입력합니다.
 - d. 스냅샷을 생성하려면 *스냅샷 복사 도구 > 파일 시스템 일관성 없는 SnapCenter *를 선택합니다.

파일 시스템 일관성 옵션은 Windows 호스트에서 실행되는 애플리케이션에만 적용할 수 있습니다.
 6. 정책 페이지에서 다음 단계를 수행합니다.
 - a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.
 - b. 선택하다 *  * 일정을 구성하려는 정책에 대한 일정 구성 열에 있습니다.
 - c. 정책 _policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 선택합니다.

_policy_name_은 선택한 정책의 이름입니다.
 7. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.
- 또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > *전역 설정*에서도 구성해야 합니다.
8. 요약을 검토한 후 *마침*을 선택하세요.
 9. *지금 백업*을 선택하세요.
 10. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스에 여러 정책이 연결되어 있는 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.
 11. *백업*을 선택하세요.
 12. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

SAP HANA 리소스 그룹 백업

리소스 그룹은 호스트의 리소스 모음입니다. 리소스 그룹에 대한 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.
3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음, *지금 백업*을 선택합니다.

4. 백업 페이지에서 다음 단계를 수행합니다.

- a. 리소스 그룹과 여러 정책이 연관된 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

주문형 백업에 대해 선택한 정책이 백업 일정과 연결되어 있는 경우, 주문형 백업은 일정 유형에 지정된 보존 설정에 따라 보존됩니다.

- b. *백업*을 선택하세요.

5. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

SAP HANA 데이터베이스 복원 및 복구

백업에서 데이터를 복원하고 복구할 수 있습니다.

이 작업에 관하여

자동으로 검색된 HANA 시스템의 경우 전체 리소스 옵션을 선택하면 단일 파일 스냅샷 복원 기술을 사용하여 복원이 수행됩니다. 빠른 복원 확인란을 선택하면 볼륨 되돌리기 기술이 사용됩니다.

수동으로 추가된 리소스의 경우 항상 볼륨 되돌리기 기술이 사용됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.
3. 리소스를 선택하거나 리소스 그룹을 선택한 다음 해당 그룹에서 리소스를 선택합니다.
4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 볼트) 스토리지 시스템의 *백업*을 선택합니다.
5. 기본 백업 테이블에서 복원하려는 백업을 선택한 다음 **를 클릭합니다.
6. 복원 범위 페이지에서 *리소스 완료*를 선택합니다.

SAP HANA 데이터베이스의 구성된 모든 데이터 볼륨이 복원되었습니다.

7. 자동으로 검색된 HANA 시스템의 경우 복구 범위 페이지에서 다음 작업을 수행합니다.
 - a. 현재 시간에 최대한 가깝게 복구하려면 *최근 상태로 복구*를 선택하세요.
 - b. 지정된 시점으로 복구하려면 *지정된 시점으로 복구*를 선택하세요.
 - c. 특정 데이터 백업으로 복구하려면 *지정된 데이터 백업으로 복구*를 선택하세요.
 - d. 지금 복구하지 않으려면 *복구 안 함*을 선택하세요.
 - e. 로그 백업 위치를 지정합니다.
 - f. 백업 카탈로그 위치를 지정합니다.
8. 사전 작업 페이지에서 복원 작업을 수행하기 전에 실행할 사전 복원 및 마운트 해제 명령을 입력합니다.
9. Post ops 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.
10. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 발신자와 수신자의 이메일 주소와 이메일 제목을 지정해야 합니다. SMTP는 설정 > 전역 설정 페이지에서도 구성해야 합니다.

11. 요약을 검토한 후 *마침*을 클릭하세요.
12. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

SAP HANA 데이터베이스 백업 복제

SnapCenter 사용하면 데이터베이스 백업을 사용하여 SAP HANA 데이터베이스를 복제할 수 있습니다. 생성된 복제본은 두꺼운 복제본이며 부모 용량 풀에 생성됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 리소스 유형을 기준으로 보기 드롭다운 목록에서 리소스를 필터링합니다.
3. 리소스 또는 리소스 그룹을 선택하세요.
4. 복사본 관리 보기에서 기본 스토리지 시스템의 *백업*을 선택합니다.
5. 표에서 데이터 백업을 선택한 다음 클릭하세요. .
6. 위치 페이지에서 다음 작업을 수행합니다.
 - a. 복제된 HANA 시스템을 관리하기 위해 SAP HANA 플러그인이 설치된 호스트를 선택하세요.

중앙 집중식 플러그인 호스트 또는 HANA 시스템 호스트가 될 수 있습니다.



HANA 플러그인이 다른 호스트의 HANA 데이터베이스를 관리하는 중앙 호스트에 설치된 경우, SnapCenter 복제본을 생성하거나 삭제하는 동안 대상 서버가 중앙 호스트이므로 호스트 측 작업 (파일 시스템 마운트 또는 마운트 해제)을 의도적으로 건너뛴다. 마운트 및 마운트 해제 작업을 수행하려면 사용자 정의 사전 또는 사후 복제 스크립트를 사용해야 합니다.

- a. 기존 백업에서 복제하려면 SAP HANA SID를 입력하세요.
- b. 복제된 볼륨을 내보낼 IP 주소나 호스트 이름을 입력합니다.
- c. SAP HANA 데이터베이스 ANF 볼륨이 수동 QOS 용량 풀에 구성된 경우 복제된 볼륨에 대한 QOS를 지정합니다.

복제된 볼륨의 QOS가 지정되지 않으면 소스 볼륨의 QOS가 사용됩니다. 자동 QOS 용량 풀을 사용하는 경우 지정된 QOS 값은 무시됩니다.

7. 스크립트 페이지에서 다음 단계를 수행합니다.
 - a. 복제 작업 전이나 후에 실행해야 하는 사전 복제 또는 사후 복제에 대한 명령을 각각 입력합니다.
 - b. 호스트에 파일 시스템을 마운트하려면 mount 명령을 입력하세요.

소스 HANA 시스템이 자동으로 검색되고 복제 대상 호스트 플러그인이 SAP HANA 호스트에 설치된 경우 SnapCenter 복제 대상 호스트에 있는 기존 HANA 데이터 볼륨을 자동으로 마운트 해제하고 새로 복제된 HANA 데이터 볼륨을 마운트합니다.

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.
9. 요약을 검토한 후 *마침*을 클릭하세요.
10. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.



ANF 클론은 이미 선택된 스냅샷에서 생성된 독립 볼륨이기 때문에 ANF 클론의 경우 클론 분할이 비활성화됩니다.

Microsoft SQL Server 데이터베이스 보호

호스트를 추가하고 **SQL Server** 데이터베이스용 **SnapCenter** 플러그인을 설치합니다.

SnapCenter Azure NetApp Files 의 SMB 공유에 있는 SQL 인스턴스의 데이터 보호를 지원합니다. 독립 실행형 및 가용성 그룹(AG) 구성이 지원됩니다.

SnapCenter 호스트 추가 페이지를 사용하여 호스트를 추가한 다음 플러그인 패키지를 설치해야 합니다. 플러그인은 원격 호스트에 자동으로 설치됩니다.

시작하기 전에

- SnapCenter 관리자 역할과 같이 플러그인 설치 및 제거 권한이 있는 역할에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속하는 경우 호스트에서 UAC를 비활성화해야 합니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 선택합니다.
2. 상단에 관리되는 호스트 탭이 선택되어 있는지 확인하세요.
3. *추가*를 선택하세요.
4. 호스트 페이지에서 다음을 수행합니다.
 - a. 호스트 유형 필드에서 호스트 유형을 선택합니다.
 - b. 호스트 이름 필드에 호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력합니다.
 - c. 자격 증명 필드에 귀하가 만든 자격 증명을 입력합니다.
5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.
6. (선택 사항) *추가 옵션*을 클릭하고 세부 정보를 지정합니다.
7. *제출*을 선택하세요.
8. *로그 디렉터리 구성*을 선택하고 호스트 로그 디렉터리 구성 페이지에서 호스트 로그 디렉터리의 SMB 경로를 입력한 다음 *저장*을 클릭합니다.
9. *제출*을 클릭하고 설치 진행 상황을 모니터링하세요.

SQL Server 데이터베이스에 대한 백업 정책 만들기

SnapCenter 사용하여 SQL Server 리소스를 백업하기 전에 리소스 또는 리소스 그룹에 대한 백업 정책을 만들거나, 리소스 그룹을 만들거나 단일 리소스를 백업할 때 백업 정책을 만들 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.

2. 설정 페이지에서 *정책*을 클릭합니다.
3. *새로 만들기*를 클릭합니다.
4. 이름 페이지에서 정책 이름과 설명을 입력합니다.
5. 정책 유형 페이지에서 다음 단계를 수행합니다.
 - a. 저장소 유형으로 *Azure NetApp Files*를 선택합니다.
 - b. 백업 유형을 선택하세요.
 - i. 데이터베이스 파일과 트랜잭션 로그를 백업하려면 *전체 백업 및 로그 백업*을 선택하세요.
 - ii. 데이터베이스 파일만 백업하려면 *전체 백업*을 선택하세요.
 - iii. 트랜잭션 로그만 백업하려면 *로그 백업*을 선택하세요.
 - iv. 다른 애플리케이션을 사용하여 리소스를 백업하려면 *복사 전용 백업*을 선택하세요.
 - c. 가용성 그룹 설정 섹션에서 다음 작업을 수행합니다.
 - i. 복제본에만 백업하려면 선호하는 백업 복제본에서 백업을 선택하세요.
 - ii. 백업을 위해 기본 AG 복제본이나 보조 AG 복제본을 선택합니다.
 - iii. 백업 우선순위를 선택하세요.
6. 스냅샷 및 백업 페이지에서 다음 단계를 수행합니다.
 - a. 예약된 백업의 빈도를 선택하세요.
 - b. 선택한 백업 유형에 따라 보존 설정을 지정합니다.
 - c. Azure NetApp Files 백업을 활성화하려면 *백업 활성화*를 선택하고 보존 설정을 지정합니다.
7. 확인 페이지에서 다음 단계를 수행하세요.
 - a. 다음 백업 일정에 대한 검증 실행 섹션에서 일정 빈도를 선택합니다.
 - b. 데이터베이스 일관성 검사 옵션 섹션에서 다음 작업을 수행합니다.
 - i. 무결성 검사를 데이터베이스의 물리적 구조로 제한하고 찢어진 페이지, 체크섬 오류, 데이터베이스에 영향을 미치는 일반적인 하드웨어 오류를 감지하려면 *데이터베이스의 물리적 구조로 무결성 구조 제한(PHYSICAL_ONLY)*을 선택합니다.
 - ii. 모든 정보 메시지를 표시하지 않으려면 *모든 정보 메시지 표시 안 함(NO_INFOMSGS)*을 선택하세요.

기본적으로 선택됨.
 - iii. 보고된 모든 오류를 개체별로 표시하려면 *개체별로 보고된 모든 오류 메시지 표시 (ALL_ERRORMSG)*을 선택합니다.
 - iv. 비클러스터형 인덱스를 검사하지 않으려면 *비클러스터형 인덱스를 검사하지 않음(NOINDEX)*을 선택합니다.

SQL Server 데이터베이스는 Microsoft SQL Server 데이터베이스 일관성 검사기(DBCC)를 사용하여 데이터베이스에 있는 개체의 논리적 및 물리적 무결성을 검사합니다.
 - v. 내부 데이터베이스 스냅샷을 사용하는 대신 검사를 제한하고 잠금을 획득하려면 *검사를 제한하고 내부 데이터베이스 스냅샷 복사본을 사용하는 대신 잠금을 획득(TABLOCK)*을 선택합니다.
 - c. 로그 백업 섹션에서 *완료 시 로그 백업 확인*을 선택하여 완료 시 로그 백업을 확인합니다.

- d. 확인 스크립트 설정 섹션에서는 각각 확인 작업 전이나 후에 실행해야 하는 프리스크립트나 포스트스크립트의 경로와 인수를 입력합니다.

8. 요약을 검토하고 *마침*을 클릭하세요.

리소스 그룹을 만들고 SQL 백업 정책을 첨부합니다.

리소스 그룹은 백업하고 보호하려는 리소스를 추가해야 하는 컨테이너입니다.

리소스 그룹을 사용하면 주어진 애플리케이션과 관련된 모든 데이터를 동시에 백업할 수 있습니다. 모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한, 수행하려는 데이터 보호 작업 유형을 정의하려면 리소스 그룹에 하나 이상의 정책을 연결해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	리소스 그룹의 이름을 입력하세요.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력하세요.
스냅샷 복사에 사용자 정의 이름 형식 사용	이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

4. 리소스 페이지에서 호스트 드롭다운 목록에서 호스트 이름을 선택하고 리소스 유형 드롭다운 목록에서 리소스 유형을 선택합니다.
5. 사용 가능한 리소스 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 클릭하여 선택한 리소스 섹션으로 이동합니다.
6. 정책 페이지에서 다음 단계를 수행합니다.
 - a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.
 - b. 일정 구성 열에서 *를 클릭합니다.  * 구성하려는 정책에 대해.
 - c. 정책 _policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 클릭합니다.
 - d. Microsoft SQL Server 스케줄러를 선택합니다.
7. 확인 페이지에서 다음 단계를 수행하세요.
 - a. 검증 서버를 선택하세요.
 - b. 확인 일정을 구성하려는 정책을 선택한 다음 *를 클릭합니다.  *.
 - c. 백업 후 검증 실행 또는 *예약된 검증 실행*을 선택하세요.
 - d. *확인*을 클릭합니다.

8. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

9. 요약을 검토한 후 *마침*을 클릭하세요.

Azure NetApp Files 에서 실행되는 SQL Server 데이터베이스 백업

리소스가 아직 어떤 리소스 그룹에도 속하지 않은 경우 리소스 페이지에서 리소스를 백업할 수 있습니다.

시작하기 전에

Azure Windows 장애 조치(Failover) 클러스터에 클러스터 IP가 할당되지 않았거나 SnapCenter 에서 연결할 수 없는 경우 부하 분산 장치를 만들어야 합니다. 로드 밸런서의 IP는 구성되어야 하며 SnapCenter 서버에서 접근 가능해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 드롭다운 목록에서 데이터베이스, 인스턴스 또는 *가용성 그룹*을 선택합니다.
3. 리소스 페이지에서 *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택한 다음 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.
4. 정책 페이지에서 다음 단계를 수행합니다.
 - a. 드롭다운 목록에서 하나 이상의 정책을 선택하세요.
 - b. 선택하다 *  * 일정을 구성하려는 정책에 대한 일정 구성 열에 있습니다.
 - c. 정책 _policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 선택합니다.
_policy_name_은 선택한 정책의 이름입니다.
 - d. **Microsoft SQL Server** 스케줄러 사용*을 선택한 다음, 스케줄링 정책과 연결된 *스케줄러 인스턴스 드롭다운 목록에서 스케줄러 인스턴스를 선택합니다.
5. 확인 페이지에서 다음 단계를 수행하세요.
 - a. 검증 서버를 선택하세요.
 - b. 확인 일정을 구성하려는 정책을 선택한 다음 *  *.
 - c. 백업 후 검증 실행 또는 *예약된 검증 실행*을 선택하세요.
 - d. OK를 클릭합니다.
6. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.
7. 요약을 검토한 후 *마침*을 클릭하세요.
8. *지금 백업*을 선택하세요.
9. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스에 여러 정책이 연결되어 있는 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.
 - b. *백업 후 확인*을 선택하세요.
 - c. *백업*을 선택하세요.

10. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

SQL Server 리소스 그룹 백업

여러 개의 리소스로 구성된 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 대한 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.
3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음, *지금 백업*을 선택합니다.
4. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스 그룹과 여러 정책이 연관된 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.
 - b. 백업 후, *확인*을 선택하여 주문형 백업을 확인하세요.
 - c. *백업*을 선택하세요.
5. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

SQL Server 데이터베이스 복원 및 복구

SnapCenter 사용하면 백업된 SQL Server 데이터베이스를 복원할 수 있습니다. 데이터베이스 복원은 지정된 SQL Server 백업에서 모든 데이터와 로그 페이지를 지정된 데이터베이스로 복사하는 다단계 프로세스입니다.

이 작업에 관하여

복원할 대상 인스턴스가 SMB ADactive directory 도메인에 속하고 파일 권한을 적절히 설정할 수 있는 권한이 있는 Active Directory 사용자로 구성되어 있는지 확인해야 합니다. SnapCenter 에서 인스턴스 수준에서 자격 증명을 구성해야 합니다.

SMB 구성에서는 대상 인스턴스에 대한 SQL 인증이 지원되지 않습니다. 대상 인스턴스는 필요한 권한이 있는 Active Directory 사용자로 SnapCenter 에 구성되어야 합니다.

SnapCenter 플러그인 서비스 계정이 Active Directory 사용자가 아닌 경우 대체 호스트로 복원을 수행하는 동안 소스 볼륨에 대한 전체 제어 권한이 있는 사용자가 필요하여 가장하여 필요한 작업을 수행할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 목록에서 데이터베이스나 리소스 그룹을 선택하세요.
4. 사본 관리 보기에서 스토리지 시스템의 *백업*을 선택합니다.
5. 테이블에서 백업을 선택한 다음 클릭하십시오.  상.
6. 복원 범위 페이지에서 다음 옵션 중 하나를 선택하세요.
 - a. 백업이 생성된 동일한 SQL 서버로 데이터베이스를 복원하려면 *백업이 생성된 동일한 호스트로 데이터베이스

복원*을 선택합니다.

- b. 백업이 수행된 동일 호스트 또는 다른 호스트의 다른 SQL 서버로 데이터베이스를 복원하려면 *데이터베이스를 대체 호스트로 복원*을 선택합니다.

7. 복구 범위 페이지에서 다음 옵션 중 하나를 선택하세요.

- a. 로그 없이 전체 백업만 복원해야 하는 경우 *없음*을 선택합니다.
- b. 전체 백업 후 사용 가능한 모든 로그 백업을 복원하려면 모든 로그 백업 최신 백업 복원 작업을 선택합니다.
- c. *로그 백업 기준*을 선택하면 특정 날짜의 백업 로그를 기준으로 데이터베이스를 복원하는 지정 시간 복원 작업이 수행됩니다.
- d. 복원된 데이터베이스에 트랜잭션 로그가 적용되지 않는 날짜와 시간을 지정하려면 *특정 날짜까지*를 선택합니다.
- e. 모든 로그 백업, 로그 백업 기준 또는 *특정 날짜 기준*을 선택했고 로그가 사용자 지정 위치에 있는 경우, *사용자 지정 로그 디렉터리 사용*을 선택한 다음 로그 위치를 지정합니다.

8. 수술 전 및 수술 후 페이지에서 필요한 세부 정보를 지정하세요.

9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

10. 요약을 검토한 후 *마침*을 클릭하세요.

11. 모니터 > 작업 페이지를 사용하여 복원 프로세스를 모니터링합니다.

SQL Server 데이터베이스 백업 복제

SnapCenter 사용하면 데이터베이스 백업을 사용하여 SQL 데이터베이스를 복제할 수 있습니다. 생성된 복제본은 두꺼운 복제본이며 부모 용량 풀에 생성됩니다.

이 작업에 관하여

복제 대상 인스턴스가 SMB ADactive directory 도메인에 속하고 파일 권한을 적절히 설정할 수 있는 권한이 있는 Active Directory 사용자로 구성되었는지 확인해야 합니다. SnapCenter 에서 인스턴스 수준의 자격 증명을 구성해야 합니다.

SMB 구성에서는 대상 인스턴스에 대한 SQL 인증이 지원되지 않습니다. 대상 인스턴스는 필요한 권한이 있는 Active Directory 사용자로 SnapCenter 에 구성되어야 합니다.

SnapCenter 플러그인 서비스 계정이 활성 디렉토리 사용자가 아닌 경우 복제를 수행하는 동안 소스 볼륨에 대한 전체 제어 권한이 있는 사용자가 필요하여 가장하여 필요한 작업을 수행할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 데이터베이스 또는 리소스 그룹을 선택하세요.
4. 사본 관리 보기 페이지에서 기본 스토리지 시스템의 백업을 선택합니다.
5. 백업을 선택한 후 *를 선택하세요  *.
6. 복제 옵션 페이지에서 필요한 모든 세부 정보를 제공합니다.
7. 위치 페이지에서 복제본을 만들 저장 위치를 선택합니다.

SQL Server 데이터베이스 ANF 볼륨이 수동 QOS 용량 풀에 구성된 경우 복제된 볼륨에 대한 QOS를 지정합니다.

복제된 볼륨의 QOS가 지정되지 않으면 소스 볼륨의 QOS가 사용됩니다. 자동 QOS 용량 풀을 사용하는 경우 지정된 QOS 값은 무시됩니다.

8. 로그 페이지에서 다음 옵션 중 하나를 선택하세요.
 - a. 로그 없이 전체 백업만 복제하려면 *없음*을 선택하세요.
 - b. 전체 백업 이후의 모든 사용 가능한 로그 백업을 복제하려면 *모든 로그 백업*을 선택합니다.
 - c. 선택한 날짜의 백업 로그까지 생성된 백업 로그를 기준으로 데이터베이스를 복제하려면 *로그 백업 기준*을 선택합니다.
 - d. 지정된 날짜 및 시간 이후에는 거래 로그를 적용하지 않으려면 *특정 날짜까지*를 선택하세요.
9. 스크립트 페이지에서 복제 작업 전이나 후에 실행해야 하는 스크립트 시간 초과, 경로, 프리스크립트 또는 포스트스크립트의 인수를 각각 입력합니다.
10. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.
11. 요약을 검토한 후 *마침*을 선택하세요.
12. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

복제 수명 주기 수행

SnapCenter 사용하면 리소스 그룹이나 데이터베이스에서 복제본을 만들 수 있습니다. 주문형 복제를 수행하거나 리소스 그룹이나 데이터베이스의 반복 복제 작업을 예약할 수 있습니다. 백업을 주기적으로 복제하면 복제본을 사용하여 애플리케이션을 개발하고, 데이터를 채우거나, 데이터를 복구할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 데이터베이스 또는 리소스 그룹을 선택하세요.
4. 사본 관리 보기 페이지에서 기본 스토리지 시스템의 백업을 선택합니다.
5. 백업을 선택한 후 *를 선택하세요  *.
6. 복제 옵션 페이지에서 필요한 모든 세부 정보를 제공합니다.
7. 위치 페이지에서 복제본을 만들 저장 위치를 선택합니다.

SQL Server 데이터베이스 ANF 볼륨이 수동 QOS 용량 풀에 구성된 경우 복제된 볼륨에 대한 QOS를 지정합니다.

복제된 볼륨의 QOS가 지정되지 않으면 소스 볼륨의 QOS가 사용됩니다. 자동 QOS 용량 풀을 사용하는 경우 지정된 QOS 값은 무시됩니다.

8. 스크립트 페이지에서 복제 작업 전이나 후에 실행해야 하는 스크립트 시간 초과, 경로, 프리스크립트 또는 포스트스크립트의 인수를 각각 입력합니다.
9. 일정 페이지에서 다음 작업 중 하나를 수행합니다.
 - 복제 작업을 즉시 실행하려면 *지금 실행*을 선택하세요.
 - 복제 작업이 얼마나 자주 발생해야 하는지, 복제 일정을 언제 시작해야 하는지, 복제 작업이 어느 요일에 발생해야 하는지, 일정이 언제 만료되어야 하는지, 일정이 만료된 후 복제본을 삭제해야 하는지 여부를

결정하려면 *일정 구성*을 선택합니다.

- 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.
- 요약을 검토한 후 *마침*을 선택하세요.
- 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

Oracle 데이터베이스 보호

호스트를 추가하고 **Oracle** 데이터베이스용 **SnapCenter** 플러그인을 설치합니다.

호스트 추가 페이지를 사용하여 호스트를 추가한 다음 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치할 수 있습니다. 플러그인은 원격 호스트에 자동으로 설치됩니다.

개별 호스트나 클러스터에 대해 호스트를 추가하고 플러그인 패키지를 설치할 수 있습니다. 클러스터(Oracle RAC)에 플러그인을 설치하는 경우 플러그인은 클러스터의 모든 노드에 설치됩니다. Oracle RAC One Node의 경우 액티브 노드와 패시브 노드 모두에 플러그인을 설치해야 합니다.

단계

- 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
- 관리되는 호스트 탭이 선택되어 있는지 확인하세요.
- *추가*를 클릭하세요.
- 호스트 페이지에서 다음 작업을 수행합니다.
 - 호스트 유형 필드에서 호스트 유형을 선택합니다.
 - 호스트 이름 필드에 호스트의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력합니다.
 - 자격 증명 필드에 귀하가 만든 자격 증명을 입력합니다.
- 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.
- (선택 사항) *추가 옵션*을 클릭하고 세부 정보를 지정합니다.
- *제출*을 클릭하세요.
- 지문을 확인한 후 *확인 및 제출*을 클릭하세요.

클러스터 설정에서는 클러스터의 각 노드의 지문을 확인해야 합니다.

- 설치 진행 상황을 모니터링합니다.

Oracle 데이터베이스에 대한 백업 정책 생성

SnapCenter 사용하여 Oracle 데이터베이스 리소스를 백업하기 전에 백업하려는 리소스 또는 리소스 그룹에 대한 백업 정책을 만들어야 합니다.

단계

- 왼쪽 탐색 창에서 *설정*을 클릭합니다.
- 설정 페이지에서 *정책*을 클릭합니다.

3. 드롭다운 목록에서 Oracle Database를 선택합니다.
4. *새로 만들기*를 클릭합니다.
5. 이름 페이지에서 정책 이름과 설명을 입력합니다.
6. 정책 유형 페이지에서 다음 단계를 수행합니다.
 - a. 저장소 유형으로 *Azure NetApp Files*를 선택합니다.
 - b. 백업 유형을 온라인 또는 오프라인 백업으로 선택하세요.
 - c. Oracle Recovery Manager(RMAN)를 사용하여 백업을 카탈로그화하려면 *Oracle Recovery Manager(RMAN)를 사용하여 백업 카탈로그화*를 선택하세요.
 - d. 백업 후 보관 로그를 정리하려면 *백업 후 보관 로그 정리*를 선택하세요.
 - e. 보관 로그 삭제 설정을 지정합니다.
7. 스냅샷 및 백업 페이지에서 다음 단계를 수행합니다.
 - a. 예약된 백업의 빈도를 선택하세요.
 - b. 보존 설정을 지정합니다.
 - c. Azure NetApp Files 백업을 활성화하려면 *백업 활성화*를 선택하고 보존 설정을 지정합니다.
8. 스크립트 페이지에서 백업 작업 전이나 후에 실행할 프리스크립트나 포스트스크립트의 경로와 인수를 각각 입력합니다.
9. 검증 페이지에서 검증 작업을 수행할 백업 일정을 선택하고 검증 작업 전이나 후에 실행할 사전 스크립트 또는 사후 스크립트의 경로와 인수를 입력합니다.
10. 요약을 검토하고 *마침*을 클릭하세요.

리소스 그룹을 생성하고 **Oracle** 백업 정책을 첨부합니다.

리소스 그룹은 백업하고 보호하려는 리소스를 추가해야 하는 컨테이너입니다.

리소스 그룹을 사용하면 주어진 애플리케이션과 관련된 모든 데이터를 동시에 백업할 수 있습니다. 모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한, 수행하려는 데이터 보호 작업 유형을 정의하려면 리소스 그룹에 하나 이상의 정책을 연결해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 *새 리소스 그룹*을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.

이 분야에서는...	이렇게 하세요...
이름	리소스 그룹의 이름을 입력하세요.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력하세요.

이 분야에서는...	이렇게 하세요...
스냅샷 복사에 사용자 정의 이름 형식 사용	이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.
아카이브 로그 파일 대상	보관 로그 파일의 대상을 지정합니다.

- 리소스 페이지에서 호스트 드롭다운 목록에서 호스트 이름을 선택하고 리소스 유형 드롭다운 목록에서 리소스 유형을 선택합니다.
- 사용 가능한 리소스 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 클릭하여 선택한 리소스 섹션으로 이동합니다.
- 정책 페이지에서 다음 단계를 수행합니다.
 - 드롭다운 목록에서 하나 이상의 정책을 선택하세요.
 - 일정 구성 열에서 *를 클릭합니다.  * 구성하려는 정책에 대해.
 - 정책 _policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 클릭합니다.
- 확인 페이지에서 다음 단계를 수행하세요.
 - 검증 서버를 선택하세요.
 - 확인 일정을 구성하려는 정책을 선택한 다음 *를 클릭합니다.  .
 - 백업 후 검증 실행 또는 *예약된 검증 실행*을 선택하세요.
 - *확인*을 클릭합니다.
- 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.
- 요약을 검토한 후 *마침*을 클릭하세요.

Azure NetApp Files 에서 실행되는 Oracle 데이터베이스 백업

리소스가 아직 어떤 리소스 그룹에도 속하지 않은 경우 리소스 페이지에서 리소스를 백업할 수 있습니다.

단계

- 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
- 리소스 페이지의 보기 드롭다운 목록에서 *데이터베이스*를 선택합니다.
- 리소스 페이지에서 *스냅샷 복사에 사용자 지정 이름 형식 사용*을 선택한 다음 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다.
- 정책 페이지에서 다음 단계를 수행합니다.
 - 드롭다운 목록에서 하나 이상의 정책을 선택하세요.
 - 선택하다 *  * 일정을 구성하려는 정책에 대한 일정 구성 열에 있습니다.
 - 정책 _policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 *확인*을 선택합니다.
- 확인 페이지에서 다음 단계를 수행하세요.

- a. 검증 서버를 선택하세요.
 - b. 확인 일정을 구성하려는 정책을 선택한 다음  *.
 - c. 백업 후 검증 실행 또는 *예약된 검증 실행*을 선택하세요.
 - d. OK를 클릭합니다.
6. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.
 7. 요약을 검토한 후 *마침*을 클릭하세요.
 8. *지금 백업*을 선택하세요.
 9. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스에 여러 정책이 연결되어 있는 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.
 - b. *백업*을 클릭하세요.
 10. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

Oracle 리소스 그룹 백업

여러 개의 리소스로 구성된 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 대한 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.
3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음, *지금 백업*을 선택합니다.
4. 백업 페이지에서 다음 단계를 수행합니다.
 - a. 리소스 그룹과 여러 정책이 연관된 경우, 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.
 - b. *백업*을 선택하세요.
5. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

Oracle 데이터베이스 복원 및 복구

데이터 손실이 발생한 경우 SnapCenter 사용하여 하나 이상의 백업에서 데이터를 활성 파일 시스템으로 복원한 다음 데이터베이스를 복구할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 목록에서 데이터베이스나 리소스 그룹을 선택하세요.
4. 복사본 관리 보기에서 기본 스토리지 시스템의 *백업*을 선택합니다.
5. 테이블에서 백업을 선택한 후  *.

6. 복원 범위 페이지에서 다음 작업을 수행합니다.

- a. RAC 환경에서 데이터베이스 백업을 선택한 경우 RAC를 선택합니다.
- b. 다음 작업을 수행하세요.
 - i. 데이터베이스 파일만 복원하려면 *모든 데이터 파일*을 선택합니다.
 - ii. 테이블스페이스만 복원하려면 *테이블스페이스*를 선택합니다.
 - iii. Data Guard 대기 또는 Active Data Guard 대기 데이터베이스의 리두 로그 파일을 복원하려면 *리두 로그 파일*을 선택합니다.
 - iv. *플러그형 데이터베이스*를 선택하고 복원하려는 PDB를 지정합니다.
 - v. *플러그형 데이터베이스(PDB) 테이블스페이스*를 선택한 다음 복원하려는 PDB와 해당 PDB의 테이블스페이스를 지정합니다.
 - vi. 백업이 생성된 동일한 SQL 서버로 데이터베이스를 복원하려면 *백업이 생성된 동일한 호스트로 데이터베이스 복원*을 선택합니다.
 - vii. 백업이 수행된 동일 호스트 또는 다른 호스트의 다른 SQL 서버로 데이터베이스를 복원하려면 *데이터베이스를 대체 호스트로 복원*을 선택합니다.
 - viii. 복원 및 복구에 필요한 경우 데이터베이스 상태 변경을 선택하여 복원 및 복구 작업을 수행하는 데 필요한 상태로 데이터베이스 상태를 변경합니다.
 - ix. 백업 후 새 데이터 파일이 추가되거나 LUN이 LVM 디스크 그룹에 추가, 삭제 또는 다시 생성되는 경우 제자리 복원을 수행하려면 *강제 제자리 복원*을 선택합니다.

7. 복구 범위 페이지에서 다음 옵션 중 하나를 선택하세요.

- a. 마지막 거래까지 복구하려면 *모든 로그*를 선택하세요.
- b. 특정 SCN으로 복구하려면 *SCN(시스템 변경 번호)까지*를 선택하세요.
- c. 특정 날짜와 시간으로 복구하려면 *날짜 및 시간*을 선택하세요.
- d. 복구를 원하지 않으면 *복구 안 함*을 선택하세요.
- e. 외부 보관 로그 파일의 위치를 지정하려면 *외부 보관 로그 위치 지정*을 선택합니다.

8. 수술 전 및 수술 후 페이지에서 필요한 세부 정보를 지정하세요.

9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

10. 요약을 검토한 후 *마침*을 클릭하세요.

11. 모니터 > *작업*을 클릭하여 작업 진행 상황을 모니터링하세요.

지정 시점 복구를 사용하여 테이블스페이스 복원 및 복구

데이터베이스의 다른 테이블스페이스에 영향을 주지 않고 손상되거나 삭제된 테이블스페이스 하위 집합을 복원할 수 있습니다. SnapCenter RMAN을 사용하여 테이블스페이스의 PITR(지정 시점 복구)을 수행합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 단일 인스턴스(멀티테넌트) 유형의 데이터베이스를 선택합니다.
4. 사본 관리 보기에서 스토리지 시스템의 *백업*을 선택합니다.

백업이 카탈로그화되어 있지 않으면 백업을 선택하고 *카탈로그*를 클릭해야 합니다.

5. 카탈로그화된 백업을 선택한 후 *를 클릭합니다.  *.
6. 복원 범위 페이지에서 다음 작업을 수행합니다.
 - a. RAC 환경에서 데이터베이스 백업을 선택한 경우 *RAC*를 선택합니다.
 - b. 테이블스페이스만 복원하려면 *테이블스페이스*를 선택합니다.
 - c. 복원 및 복구에 필요한 경우 데이터베이스 상태 변경을 선택하여 복원 및 복구 작업을 수행하는 데 필요한 상태로 데이터베이스 상태를 변경합니다.
7. 복구 범위 페이지에서 다음 옵션 중 하나를 선택하세요.
 - a. 특정 SCN으로 복구하려면 *SCN(시스템 변경 번호)까지*를 선택하세요.
 - b. 특정 날짜와 시간으로 복구하려면 *날짜 및 시간*을 선택하세요.
8. 수술 전 및 수술 후 페이지에서 필요한 세부 정보를 지정하세요.
9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.
10. 요약 검토 후 *마침*을 클릭하세요.
11. 모니터 > 작업 페이지를 사용하여 복원 프로세스를 모니터링합니다.

특정 시점 복구를 사용하여 플러그형 데이터베이스를 복원하고 복구합니다.

컨테이너 데이터베이스(CDB)의 다른 PDB에 영향을 주지 않고 손상되거나 삭제된 플러그형 데이터베이스(PDB)를 복원하고 복구할 수 있습니다. SnapCenter RMAN을 사용하여 PDB의 PITR(지정 시점 복구)을 수행합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 단일 인스턴스(멀티테넌트) 유형의 데이터베이스를 선택합니다.
4. 사본 관리 보기에서 스토리지 시스템의 *백업*을 선택합니다.

백업이 카탈로그화되어 있지 않으면 백업을 선택하고 *카탈로그*를 클릭해야 합니다.

5. 카탈로그화된 백업을 선택한 후 *를 클릭합니다.  *.
6. 복원 범위 페이지에서 다음 작업을 수행합니다.
 - a. RAC 환경에서 데이터베이스 백업을 선택한 경우 *RAC*를 선택합니다.
 - b. PDB를 복원할지, 아니면 PDB의 테이블스페이스를 복원할지에 따라 다음 작업 중 하나를 수행합니다.
 - PDB를 복원하려면 *플러그형 데이터베이스(PDB)*를 선택합니다.
 - PDB에서 테이블스페이스를 복원하려면 *플러그형 데이터베이스(PDB) 테이블스페이스*를 선택합니다.
7. 복구 범위 페이지에서 다음 옵션 중 하나를 선택하세요.
 - a. 특정 SCN으로 복구하려면 *SCN(시스템 변경 번호)까지*를 선택하세요.
 - b. 특정 날짜와 시간으로 복구하려면 *날짜 및 시간*을 선택하세요.

8. 수술 전 및 수술 후 페이지에서 필요한 세부 정보를 지정하세요.
9. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.
10. 요약을 검토한 후 *마침*을 클릭하세요.
11. 모니터 > 작업 페이지를 사용하여 복원 프로세스를 모니터링합니다.

Oracle 데이터베이스 백업 복제

SnapCenter 사용하면 데이터베이스 백업을 사용하여 Oracle 데이터베이스를 복제할 수 있습니다. 생성된 복제본은 두꺼운 복제본이며 부모 용량 풀에 생성됩니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 데이터베이스를 선택하세요.
4. 복사본 관리 보기 페이지에서 기본 스토리지 시스템의 백업을 선택합니다.
5. 데이터 백업을 선택한 후 *를 클릭하세요.  *.
6. 이름 페이지에서 데이터베이스(CDB 또는 비 CDB)를 복제할지, 아니면 플러그형 데이터베이스(PDB)를 복제할지 선택합니다.
7. 위치 페이지에서 필요한 세부 정보를 지정하세요.

Oracle 데이터베이스 ANF 볼륨이 수동 QOS 용량 풀에 구성된 경우 복제된 볼륨에 대한 QOS를 지정합니다.

복제된 볼륨의 QOS가 지정되지 않으면 소스 볼륨의 QOS가 사용됩니다. 자동 QOS 용량 풀을 사용하는 경우 지정된 QOS 값은 무시됩니다.

8. 자격 증명 페이지에서 다음 중 하나를 수행합니다.
 - a. 시스템 사용자의 자격 증명 이름에 대해 복제 데이터베이스의 시스템 사용자 암호를 정의하는 데 사용할 자격 증명을 선택합니다.
 - b. 복제 호스트의 ASM 인스턴스에 연결하기 위해 OS 인증이 활성화된 경우 ASM 인스턴스 자격 증명 이름의 경우 *없음*을 선택합니다.

그렇지 않은 경우 "sys" 사용자 또는 복제 호스트에 적용 가능한 "sysasm" 권한이 있는 사용자로 구성된 Oracle ASM 자격 증명을 선택합니다.

9. 사전 작업 페이지에서 사전 스크립트의 경로와 인수를 지정하고 데이터베이스 매개변수 설정 섹션에서 데이터베이스를 초기화하는 데 사용되는 미리 채워진 데이터베이스 매개변수의 값을 수정합니다.
10. 작업 후 페이지에서는 복제된 데이터베이스를 복구하기 위해 기본적으로 데이터베이스 복구 및 *취소 시까지*가 선택되어 있습니다.
 - a. *취소 시까지*를 선택하면 SnapCenter 복제를 위해 선택된 데이터 백업 이후의 아카이브 로그의 연속된 시퀀스를 갖는 최신 로그 백업을 마운트하여 복구를 수행합니다.
 - b. *날짜 및 시간*을 선택하면 SnapCenter 지정된 날짜와 시간까지 데이터베이스를 복구합니다.
 - c. *SCN까지*를 선택하면 SnapCenter 지정된 SCN까지 데이터베이스를 복구합니다.

- d. *외부 보관 로그 위치 지정*을 선택하면 SnapCenter 지정된 SCN 또는 선택한 날짜와 시간을 기준으로 최적의 로그 백업 수를 식별하고 마운트합니다.
- e. 기본적으로 새 **DBID** 만들기 확인란이 선택되어 복제된 데이터베이스에 대한 고유 번호(DBID)를 생성하여 원본 데이터베이스와 구별합니다.

복제된 데이터베이스에 소스 데이터베이스의 DBID를 할당하려면 확인란의 선택을 취소합니다. 이 시나리오에서 소스 데이터베이스가 이미 등록된 외부 RMAN 카탈로그에 복제된 데이터베이스를 등록하려는 경우 작업이 실패합니다.

- f. 복제된 데이터베이스의 기본 임시 테이블스페이스에 대한 임시 파일을 생성하려면 임시 테이블스페이스에 대한 임시 파일 생성 확인란을 선택합니다.
- g. *복제본 생성 시 적용할 SQL 항목 입력*에서 복제본이 생성될 때 적용할 SQL 항목을 추가합니다.
- h. *복제 작업 후 실행할 스크립트 입력*에서 복제 작업 후 실행할 포스트스크립트의 경로와 인수를 지정합니다.

11. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

12. 요약을 검토한 후 *마침*을 선택하세요.

13. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

플러그형 데이터베이스 복제

동일한 호스트 또는 대체 호스트의 다른 또는 동일한 대상 CDB에 플러그형 데이터베이스(PDB)를 복제할 수 있습니다. 복제된 PDB를 원하는 SCN이나 날짜 및 시간으로 복구할 수도 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 데이터베이스 또는 *리소스 그룹*을 선택합니다.
3. 단일 인스턴스(멀티테넌트) 유형의 데이터베이스를 선택합니다.
4. 복사본 관리 보기 페이지에서 기본 스토리지 시스템의 백업을 선택합니다.
5. 백업을 선택한 후 **를 클릭하세요.
6. 이름 페이지에서 *PDB 복제*를 선택하고 다른 세부 정보를 지정합니다.
7. 위치 페이지에서 필요한 세부 정보를 지정하세요.
8. 사전 작업 페이지에서 사전 스크립트의 경로와 인수를 지정하고 데이터베이스 매개변수 설정 섹션에서 데이터베이스를 초기화하는 데 사용되는 미리 채워진 데이터베이스 매개변수의 값을 수정합니다.
9. 작업 후 페이지에서는 복제된 데이터베이스를 복구하기 위해 기본적으로 *취소할 때까지*가 선택되어 있습니다.
 - a. *취소 시까지*를 선택하면 SnapCenter 복제를 위해 선택된 데이터 백업 이후의 아카이브 로그의 연속된 시퀀스를 갖는 최신 로그 백업을 마운트하여 복구를 수행합니다.
 - b. *날짜 및 시간*을 선택하면 SnapCenter 지정된 날짜와 시간까지 데이터베이스를 복구합니다.
 - c. *외부 보관 로그 위치 지정*을 선택하면 SnapCenter 지정된 SCN 또는 선택한 날짜와 시간을 기준으로 최적의 로그 백업 수를 식별하고 마운트합니다.
 - d. 기본적으로 새 **DBID** 만들기 확인란이 선택되어 복제된 데이터베이스에 대한 고유 번호(DBID)를 생성하여 원본 데이터베이스와 구별합니다.

복제된 데이터베이스에 소스 데이터베이스의 DBID를 할당하려면 확인란의 선택을 취소합니다. 이

시나리오에서 소스 데이터베이스가 이미 등록된 외부 RMAN 카탈로그에 복제된 데이터베이스를 등록하려는 경우 작업이 실패합니다.

e. 복제된 데이터베이스의 기본 임시 테이블스페이스에 대한 임시 파일을 생성하려면 임시 테이블스페이스에 대한 임시 파일 생성 확인란을 선택합니다.

f. *복제본 생성 시 적용할 SQL 항목 입력*에서 복제본이 생성될 때 적용할 SQL 항목을 추가합니다.

g. *복제 작업 후 실행할 스크립트 입력*에서 복제 작업 후 실행할 포스트스크립트의 경로와 인수를 지정합니다.

10. 알림 페이지의 이메일 환경 설정 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

11. 요약을 검토한 후 *마침*을 선택하세요.

12. 모니터 > *작업*을 선택하여 작업 진행 상황을 모니터링합니다.

SnapCenter 서버 및 플러그인 관리

대시보드 보기

대시보드 개요

SnapCenter 왼쪽 탐색 창에서 대시보드를 통해 최근 작업 활동, 알림, 보호 요약, 스토리지 효율성 및 사용량, SnapCenter 작업 상태(백업, 복제, 복원), 독립 실행형 및 Windows 클러스터 호스트의 구성 상태, SnapCenter 에서 관리하는 스토리지 가상 머신(SVM) 수, 라이선스 용량 등 시스템 상태를 한눈에 볼 수 있습니다.

대시보드 보기에 표시되는 정보는 현재 SnapCenter 에 로그인한 사용자에게 할당된 역할에 따라 달라집니다. 사용자에게 해당 정보를 볼 권한이 없으면 일부 콘텐츠가 표시되지 않을 수 있습니다.

많은 경우, *i*에 마우스를 올리면 디스플레이에 대한 자세한 정보를 볼 수 있습니다. 어떤 경우에는 대시보드 표시의 정보가 SnapCenter GUI 페이지(리소스, 모니터, 보고서 등)의 자세한 소스 정보에 연결됩니다.

최근 직무 활동

최근 작업 활동 타일은 사용자가 액세스할 수 있는 모든 백업, 복원 및 복제 작업의 최신 작업 활동을 표시합니다. 이 디스플레이의 작업은 완료, 경고, 실패, 실행 중, 대기 중, 취소 중 하나의 상태를 갖습니다.

일자리 위에 마우스를 올리면 자세한 정보가 표시됩니다. 특정 작업 번호를 클릭하면 모니터 페이지로 이동하여 추가 작업 정보를 볼 수 있습니다. 여기에서 작업 세부 정보나 로그 정보를 얻고, 해당 작업에 대한 구체적인 보고서를 생성할 수 있습니다.

*모두 보기*를 클릭하면 모든 SnapCenter 작업의 기록을 볼 수 있습니다.

알림

알림 타일은 호스트와 SnapCenter 서버에 대한 최신의 해결되지 않은 중요 및 경고 알림을 표시합니다.

위험 및 경고 범주 알림의 총 개수가 화면 상단에 표시됩니다. 중요 또는 경고 총계를 클릭하면 알림 페이지에 특정 필터가 적용된 알림 페이지로 이동합니다.

특정 알림을 클릭하면 해당 알림에 대한 자세한 내용을 볼 수 있는 알림 페이지로 이동합니다. 화면 하단의 *모두 보기*를 클릭하면 모든 알림 목록이 있는 알림 페이지로 이동합니다.

최신 보호 요약

최신 보호 요약 타일은 사용자가 액세스할 수 있는 모든 엔터티의 보호 상태를 알려줍니다. 기본적으로 디스플레이는 모든 플러그인의 상태를 제공하도록 설정되어 있습니다. 스냅샷으로 기본 저장소에 백업된 리소스와 SnapMirror 및 SnapVault 기술을 사용하여 보조 저장소에 백업된 리소스에 대한 상태 정보가 제공됩니다. 보조 저장소에 대한 보호 상태 정보의 가용성은 선택한 플러그인 유형에 따라 달라집니다.



미러 볼트 보호 정책을 사용하는 경우 보호 요약에 대한 카운터는 SnapVault 차트가 아닌 SnapMirror 요약 차트에 표시됩니다.

개별 플러그인의 보호 상태는 드롭다운 메뉴에서 플러그인을 선택하여 확인할 수 있습니다. 도넛형 차트는 선택한

플러그인의 보호된 리소스 비율을 보여줍니다. 도넛형 조각을 클릭하면 보고서 > 플러그인 페이지로 이동하여 지정된 플러그인의 모든 기본 및 보조 스토리지 활동에 대한 상세 보고서를 제공합니다.



보조 저장소에 대한 보고서는 SnapVault에만 적용되며 SnapMirror 보고서는 지원되지 않습니다.



SAP HANA는 스냅샷의 기본 및 보조 스토리지에 대한 보호 상태 정보를 제공합니다. 파일 기반 백업에는 기본 저장소 보호 상태만 사용할 수 있습니다.

보호 상태	1차 저장소	2차 저장소
실패한	리소스 그룹이 백업을 실행했지만 백업이 실패한 경우, 리소스 그룹에 속한 엔터티의 수입입니다.	보조 대상으로 전송하지 못한 백업이 있는 엔터티의 수입입니다.
성공적인	리소스 그룹이 성공적으로 백업된 리소스 그룹의 엔터티 수입입니다.	백업이 보조 대상으로 성공적으로 전송된 엔터티의 수입입니다.
구성되지 않음	리소스 그룹에 속하지 않고 백업되지 않은 엔터티의 수입입니다.	백업을 보조 대상으로 전송하도록 구성되지 않은 하나 이상의 리소스 그룹에 속하는 엔터티의 수입입니다.
시작되지 않음	리소스 그룹에 속하지만 백업이 실행되지 않은 엔터티의 수입입니다.	해당 없음.



SnapCenter Server 4.2와 이전 버전의 플러그인(4.2 이전 버전)을 사용하여 백업을 생성하는 경우, 최신 보호 요약 타일에는 이러한 백업의 SnapMirror 보호 상태가 표시되지 않습니다.

일자리

작업 타일은 사용자가 액세스할 수 있는 백업, 복원 및 복제 작업에 대한 요약을 제공합니다. 드롭다운 메뉴를 사용하여 보고서의 기간을 사용자 지정할 수 있습니다. 기간 옵션은 최근 24시간, 최근 7일, 최근 30일로 고정됩니다. 기본 보고서에는 지난 7일 동안 실행된 데이터 보호 작업이 표시됩니다.

백업, 복원 및 복제 작업 정보는 도넛 차트로 표시됩니다. 도넛 조각을 클릭하면 선택 항목에 작업 필터가 미리 적용된 모니터 페이지로 이동합니다.

작업 상태	설명
실패한	실패한 작업의 수.
경고	오류가 발생한 작업의 수입입니다.
성공적인	성공적으로 완료된 작업의 수입입니다.
달리기	현재 실행 중인 작업의 수입입니다.

스토리지

저장소 타일은 90일 동안 보호 작업에 사용된 기본 및 보조 저장소를 표시하고, 소비 추세를 그래픽으로 표현하며, 기본 저장소 절감액을 계산합니다. 저장 정보는 24시간마다 오전 12시에 업데이트됩니다.

SnapCenter 에서 사용 가능한 백업의 총 수와 이러한 백업이 차지하는 크기를 포함하는 하루 총 사용량이 화면 상단에 표시됩니다. 백업에는 여러 개의 스냅샷이 연관될 수 있으며 개수도 동일하게 반영됩니다. 이는 기본 및 보조 스냅샷 모두에 적용됩니다. 예를 들어, 10개의 백업을 생성했는데, 그 중 2개는 정책 기반 백업 보존으로 인해 삭제되었고 1개는 사용자가 명시적으로 삭제한 백업입니다. 따라서 7개의 백업이 차지하는 크기와 함께 7개의 백업 수가 표시됩니다.

기본 스토리지의 스토리지 절약 계수는 논리적 용량(복제본 및 스냅샷 절약과 소비된 스토리지)과 기본 스토리지의 물리적 용량의 비율입니다. 막대형 차트는 저장 공간 절약 효과를 보여줍니다.

선형 그래프는 90일 동안의 일별 1차 및 2차 저장소 소비량을 별도로 표시합니다. 차트 위에 마우스를 올리면 일별 자세한 결과가 표시됩니다.



SnapCenter Server 4.2와 이전 버전의 플러그인(4.2 이전 버전)을 사용하여 백업을 생성하는 경우, 저장소 타일에는 백업 수, 백업에 사용된 저장 공간, 스냅샷 절약량, 복제본 절약량 및 스냅샷 크기가 표시되지 않습니다.

구성

구성 타일은 SnapCenter 관리하고 사용자가 액세스할 수 있는 모든 활성 독립형 및 Windows 클러스터 호스트에 대한 통합 상태 정보를 제공합니다. 여기에는 해당 호스트와 관련된 플러그인 상태 정보가 포함됩니다.

호스트 옆에 있는 숫자를 클릭하면 호스트 페이지의 관리 호스트 섹션으로 이동합니다. 여기에서 선택한 호스트에 대한 자세한 정보를 얻을 수 있습니다.

또한 이 디스플레이는 SnapCenter 에서 관리하고 사용자가 액세스할 수 있는 Standalone ONTAP SVM과 Cluster ONTAP SVM의 합계를 보여줍니다. SVM 옆에 있는 숫자를 클릭하면 스토리지 시스템 페이지로 이동합니다. 여기에서 선택한 SVM에 대한 자세한 정보를 얻을 수 있습니다.

호스트 구성 상태는 빨간색(중요), 노란색(경고), 녹색(활성)으로 표시되며 각 상태에 있는 호스트 수도 함께 표시됩니다. 각 상태에 대한 상태 메시지가 제공됩니다.

구성 상태	설명
업그레이드 필수	지원되지 않는 플러그인을 실행하고 업그레이드가 필요한 호스트의 수입입니다. 지원되지 않는 플러그인은 이 버전의 SnapCenter 와 호환되지 않습니다.
이주 필수	지원되지 않는 플러그인을 실행 중이고 마이그레이션이 필요한 호스트의 수입입니다. 지원되지 않는 플러그인은 이 버전의 SnapCenter 와 호환되지 않습니다.
플러그인이 설치되지 않았습니다	플러그인을 설치해야 하거나 플러그인 설치에 실패했지만 성공적으로 추가된 호스트 수입입니다.
정지된	일정이 중단되어 유지 관리 중인 호스트 수입입니다.

구성 상태	설명
멈췄다	플러그인 서비스가 실행되지 않지만 작동 중인 호스트의 수입입니다.
호스트 다운	다운되었거나 접속할 수 없는 호스트의 수입입니다.
업그레이드 가능(선택 사항)	플러그인 패키지의 최신 버전을 업그레이드할 수 있는 호스트 수입입니다.
마이그레이션 가능(선택 사항)	플러그인의 최신 버전을 마이그레이션할 수 있는 호스트 수입입니다.
로그 디렉토리 구성	SCSqli 트랜잭션 로그 백업을 수행하기 위해 로그 디렉토리를 구성해야 하는 호스트 수입입니다.
VMware 플러그인 구성	SnapCenter Plug-in for VMware vSphere 추가해야 하는 호스트 수입입니다.
알려지지 않은	등록되었지만 설치가 아직 시작되지 않은 호스트의 수입입니다.
달리기	작동 중인 호스트 수와 플러그인이 실행 중인 호스트 수입입니다. 그리고 SCSQL 플러그인의 경우, 로그 디렉토리와 하이퍼바이저가 구성됩니다.
플러그인 설치/제거	플러그인 설치 또는 제거가 진행 중인 호스트의 수입입니다.

대시보드에서 정보를 보는 방법

SnapCenter 왼쪽 탐색 창에서 다양한 대시보드 타일이나 디스플레이를 관련 시스템 세부 정보와 함께 볼 수 있습니다. 대시보드에서 사용할 수 있는 디스플레이의 수는 고정되어 있으며 변경할 수 없습니다. 각 디스플레이에 제공되는 콘텐츠는 역할 기반 액세스 제어(RBAC)에 따라 달라집니다.

단계

1. 왼쪽 탐색 창에서 *대시보드*를 클릭합니다.
2. 각 디스플레이의 활성 영역을 클릭하면 추가 정보를 얻을 수 있습니다.

예를 들어, *작업*에서 도넛형 차트를 클릭하면 선택 사항에 대한 자세한 정보를 볼 수 있는 모니터 페이지로 이동합니다. *보호 요약*에서 도넛형 차트를 클릭하면 보고서 페이지로 이동하여 선택 사항에 대한 자세한 정보를 확인할 수 있습니다.

대시보드에서 작업 상태 보고서 요청

대시보드 페이지에서 백업, 복원 및 복제 작업에 대한 보고서를 요청할 수 있습니다. 이 기능은 SnapCenter 환경에서 성공한 작업과 실패한 작업의 총 수를 파악하려는 경우에 유용합니다.

단계

1. 왼쪽 탐색 창에서 *대시보드*를 클릭하세요.
2. 대시보드에서 작업 타일을 찾은 다음, 백업, 복원 또는 *복제*를 선택합니다.
3. 풀다운 메뉴를 사용하여 작업 정보를 원하는 기간(24시간, 7일 또는 30일)을 선택합니다.

시스템은 데이터를 덮는 도넛형 차트를 표시합니다.

4. 보고서를 원하는 작업 정보를 나타내는 도넛 조각을 클릭합니다.

도넛형 차트를 클릭하면 대시보드 페이지에서 모니터 페이지로 이동합니다. 모니터 페이지에는 도넛 차트에서 선택한 상태의 작업이 표시됩니다.

5. 모니터 페이지 목록에서 특정 작업을 클릭하여 선택합니다.
6. 모니터 페이지 상단에서 *보고서*를 클릭합니다.

결과

보고서에는 선택한 작업에 대한 정보만 표시됩니다. 보고서를 검토하거나 로컬 시스템에 다운로드할 수 있습니다.

대시보드에서 보호 상태 보고서 요청

대시보드를 사용하여 특정 플러그인이 관리하는 리소스에 대한 보호 세부 정보를 요청할 수 있습니다. 데이터 보호 요약에는 데이터 백업만 고려됩니다.

단계

1. 왼쪽 탐색 창에서 *대시보드*를 클릭합니다.
2. 대시보드에서 최신 보호 요약 타일을 찾아 풀다운 메뉴를 사용하여 플러그인을 선택하세요.

대시보드는 기본 저장소에 백업된 리소스에 대한 도넛형 차트를 표시하고, 플러그인에 적용 가능한 경우 보조 저장소에 백업된 리소스에 대한 도넛형 차트를 표시합니다.



데이터 보호 보고서는 특정 플러그인 유형에만 사용할 수 있습니다. *모든 플러그인*을 지정하는 것은 지원되지 않습니다.

3. 보고서를 원하는 상태를 나타내는 도넛 조각을 클릭합니다.

도넛형 차트를 클릭하면 대시보드 페이지에서 보고서로 이동한 다음 플러그인 페이지로 이동합니다. 보고서에는 선택한 플러그인의 상태만 표시됩니다. 보고서를 검토하거나 로컬 시스템에 다운로드할 수 있습니다.



SnapMirror 도넛 차트 및 파일 기반 SAP HANA 백업에 대한 보고서 페이지로의 리디렉션은 지원되지 않습니다.

RBAC 관리

SnapCenter 사용하면 역할, 사용자, 그룹을 수정할 수 있습니다.

역할 수정

SnapCenter 역할을 수정하여 사용자 또는 그룹을 제거하고 해당 역할과 관련된 권한을 변경할 수 있습니다. 전체 역할에서 사용되는 권한을 변경하거나 제거하려는 경우 역할을 수정하는 것이 특히 유용합니다.

시작하기 전에

"SnapCenterAdmin" 역할로 로그인해야 합니다.



SnapCenterAdmin 역할에 대한 권한은 수정하거나 제거할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *역할*을 클릭합니다.
3. 역할 이름 필드에서 수정하려는 역할을 클릭합니다.
4. *이 역할의 모든 구성원은 다른 구성원의 개체를 볼 수 있음*을 선택하면 해당 역할의 다른 구성원이 리소스 목록을 새로 고친 후 볼륨 및 호스트와 같은 리소스를 볼 수 있습니다.

이 역할의 멤버가 다른 멤버에게 할당된 개체를 보지 못하도록 하려면 이 옵션의 선택을 해제합니다.



이 옵션을 활성화하면 사용자가 개체나 리소스를 만든 사용자와 동일한 역할에 속해 있는 경우 개체나 리소스에 대한 액세스 권한을 사용자에게 할당할 필요가 없습니다.

5. 역할 세부 정보 페이지에서 필요에 따라 권한을 변경하거나 멤버 할당을 해제합니다.
6. *제출*을 클릭하세요.

사용자 및 그룹 수정

SnapCenter 사용자 또는 그룹을 수정하여 해당 역할과 자산을 변경할 수 있습니다.

시작하기 전에

SnapCenter 관리자로 로그인해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *사용자 및 액세스*를 클릭합니다.
3. 사용자 또는 그룹 이름 목록에서 수정하려는 사용자 또는 그룹을 클릭합니다.
4. 사용자 또는 그룹 세부 정보 페이지에서 역할과 자산을 변경합니다.
5. *제출*을 클릭하세요.

호스트 관리

호스트를 추가하고 SnapCenter 플러그인 패키지를 설치하고, 검증 서버를 추가하고, 호스트를 제거하고, 백업 작업을 마이그레이션하고, 호스트를 업데이트하여 플러그인 패키지를 업그레이드하거나 새로운 플러그인 패키지를 추가할 수 있습니다. 사용하는 플러그인에 따라 디스크 프로비저닝, SMB 공유 관리, 이니시에이터 그룹(igroup) 관리, iSCSI 세션 관리, 데이터 마이그레이션 등의 작업을 수행할 수도 있습니다.

다음 작업을 수행할 수 있습니다 ...	Microsoft Exchange Server의 경우	Microsoft SQL Server의 경우	Microsoft Windows의 경우	Oracle 데이터베이스의 경우	SAP HANA 데이터베이스용	NetApp 지원 플러그인의 경우	Db2의 경우	PostgreSQL의 경우	MySQL의 경우
호스트 추가 및 플러그인 패키지 설치	예	예	예	예	예	예	예	예	예
호스트에 대한 ESXi 정보 업데이트	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
일정을 일시 중단하고 호스트를 유지 관리 모드로 전환합니다.	예	예	예	예	예	예	예	예	예
플러그인을 추가, 업그레이드 또는 제거하여 호스트를 수정합니다.	예	예	예	예	예	예	예	예	예
SnapCenter 에서 호스트 제거	예	예	예	예	예	예	예	예	예

다음 작업을 수행할 수 있습니다 ...	Microsoft Exchange Server의 경우	Microsoft SQL Server의 경우	Microsoft Windows의 경우	Oracle 데이터베이스의 경우	SAP HANA 데이터베이스용	NetApp 지원 플러그인의 경우	Db2의 경우	PostgreSQL의 경우	MySQL의 경우
플러그인 서비스 시작(Windows 호스트에서 실행되는 플러그인에만 적용 가능)	예	예	예	아니요	예	예	예	예	예
디스크 프로비저닝	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
SMB 주식 관리	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
iGroups 관리	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
iSCSI 세션 관리	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요

가상 머신 정보 새로 고침

VMware vCenter 자격 증명이 변경되거나 데이터베이스 또는 파일 시스템 호스트가 다시 시작되면 가상 머신 정보를 새로 고쳐야 합니다. SnapCenter 에서 가상 머신 정보를 새로 고치면 VMware vSphere vCenter와 통신이 시작되고 vCenter 자격 증명을 얻습니다.



RDM 기반 디스크는 데이터베이스 호스트에 설치된 Microsoft Windows용 SnapCenter 플러그인을 통해 관리됩니다. RDM을 관리하기 위해 Microsoft Windows용 SnapCenter 플러그인은 데이터베이스 호스트를 관리하는 vCenter 서버와 통신합니다.

단계

1. SnapCenter 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 관리 호스트 페이지에서 업데이트할 호스트를 선택합니다.
4. *VM 새로 고침*을 클릭합니다.

플러그인 호스트 수정

플러그인을 설치한 후, 필요한 경우 플러그인 호스트 세부 정보를 수정할 수 있습니다. Microsoft SQL Server용 SnapCenter 플러그인의 자격 증명, 설치 경로, 플러그인, 로그 디렉토리 세부 정보, 그룹 관리 서비스 계정(gMSA) 및 플러그인 포트를 수정할 수 있습니다.



플러그인 버전이 SnapCenter Server 버전과 동일한지 확인하세요.

이 작업에 관하여

- 플러그인을 설치한 후에만 플러그인 포트를 수정할 수 있습니다.

업그레이드 작업이 진행되는 동안에는 플러그인 포트를 수정할 수 없습니다.

- 플러그인 포트를 수정할 때 다음과 같은 포트 롤백 시나리오를 알고 있어야 합니다.
 - 독립 실행형 설정에서 SnapCenter 구성 요소 중 하나의 포트를 변경하지 못하면 작업이 실패하고 모든 구성 요소에 대해 이전 포트가 유지됩니다.

모든 구성 요소에 대한 포트가 변경되었지만 구성 요소 중 하나가 새 포트로 시작하지 못하는 경우 모든 구성 요소에 대해 이전 포트가 유지됩니다. 예를 들어, 독립형 호스트에서 두 개의 플러그인에 대한 포트를 변경하려고 하는데 SnapCenter 플러그인 중 하나에 새 포트를 적용하지 못하면 해당 작업은 실패하고(해당 오류 메시지와 함께) 두 플러그인 모두에 대해 이전 포트가 유지됩니다.

- 클러스터링 설정에서 SnapCenter 노드 중 하나에 설치된 플러그인의 포트를 변경하지 못하면 작업이 실패하고 모든 노드에서 이전 포트가 유지됩니다.

예를 들어, 클러스터링 설정에서 플러그인이 4개의 노드에 설치되고 노드 중 하나의 포트가 변경되지 않으면 모든 노드에서 기존 포트가 유지됩니다.

gMSA와 함께 플러그인을 설치하면 추가 옵션 창에서 수정할 수 있습니다. gMSA 없이 플러그인을 설치한 경우 gMSA 계정을 지정하여 플러그인 서비스 계정으로 사용할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 맨 위에 *관리되는 호스트*가 선택되어 있는지 확인하세요.
3. 수정하려는 호스트를 선택하고 필드 하나를 수정합니다.

한 번에 한 개의 필드만 수정할 수 있습니다.

4. *제출*을 클릭하세요.

결과

호스트가 검증되어 SnapCenter 서버에 추가됩니다.

플러그인 서비스 시작 또는 재시작

SnapCenter 플러그인 서비스를 시작하면 서비스가 실행 중이 아니면 서비스를 시작하고, 실행 중이면 서비스를 다시 시작할 수 있습니다. 유지관리가 수행된 후 서비스를 다시 시작하는 것이 좋습니다.

서비스를 다시 시작할 때 실행 중인 작업이 없는지 확인해야 합니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 관리 호스트 페이지에서 시작하려는 호스트를 선택합니다.
4. 딸깍 하는 소리  아이콘을 클릭하고 서비스 시작 또는 *서비스 다시 시작*을 클릭합니다.

여러 호스트의 서비스를 동시에 시작하거나 다시 시작할 수 있습니다.

호스트 유지 관리를 위한 일정을 일시 중단합니다.

호스트가 SnapCenter 예약 작업을 실행하지 못하도록 하려면 호스트를 유지 관리 모드로 전환하면 됩니다. 플러그인을 업그레이드하기 전이나 호스트에서 유지 관리 작업을 수행하는 경우 이 작업을 수행해야 합니다.



SnapCenter 해당 호스트와 통신할 수 없기 때문에 다운된 호스트의 일정을 일시 중단할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 관리 호스트 페이지에서 일시 중단하려는 호스트를 선택합니다.
4. 클릭  아이콘을 클릭한 다음 *일정 일시 중단*을 클릭하여 이 플러그인의 호스트를 유지 관리 모드로 전환합니다.

여러 호스트의 일정을 동시에 일시 중지할 수 있습니다.



먼저 플러그인 서비스를 중지할 필요는 없습니다. 플러그인 서비스는 실행 중이거나 중지된 상태일 수 있습니다.

결과

호스트에서 일정을 일시 중단한 후 관리 호스트 페이지에서 해당 호스트의 전체 상태 필드에 *일시 중단*이 표시됩니다.

호스트 유지 관리를 완료한 후 *일정 활성화*를 클릭하면 호스트를 유지 관리 모드에서 해제할 수 있습니다. 여러 호스트의 일정을 동시에 활성화할 수 있습니다.

리소스 페이지에서 지원되는 작업

리소스 페이지에서 리소스를 검색하고 데이터 보호 작업을 수행할 수 있습니다. 리소스를 관리하는 데 사용하는 플러그인에 따라 수행할 수 있는 작업이 달라집니다.

리소스 페이지에서 다음 작업을 수행할 수 있습니다.

다음 작업을 수행할 수 있습니다...	Microsoft Exchange Server의 경우	Microsoft SQL Server의 경우	Microsoft Windows의 경우	Oracle 데이터베이스의 경우	SAP HANA 데이터베이스용
백업에 사용할 수 있는 리소스가 있는지 확인하세요	예	예	예	예	예
리소스의 주문형 백업 수행	예	예	예	예	예
백업에서 복원	예	예	예	예	예
백업 복제	아니요	예	예	예	예
백업 관리	예	예	예	예	예
클론 관리	아니요	예	예	예	예
정책 관리	예	예	예	예	예
저장소 연결 관리	예	예	예	예	예
백업 마운트	아니요	아니요	아니요	예	아니요
백업 마운트 해제	아니요	아니요	아니요	예	아니요
자세한 내용 보기	예	예	예	예	예

정책 관리

리소스 또는 리소스 그룹에서 정책을 분리하고, 수정, 삭제, 보기 및 복사할 수 있습니다.

정책 수정

정책이 리소스 또는 리소스 그룹에 연결되어 있는 동안 복제 옵션, 스냅샷 보존 설정, 오류 재시도 횟수 또는 스크립트 정보를 수정할 수 있습니다. 정책을 분리한 후에만 일정 유형(빈도)을 수정할 수 있습니다.

이 작업에 관하여

정책에서 일정 유형을 수정하려면 추가 단계가 필요합니다. SnapCenter 서버는 정책이 리소스나 리소스 그룹에 연결될 때만 일정 유형을 등록하기 때문입니다.

만약 당신이 원한다면...	그 다음에...
추가 일정 유형 추가	새로운 정책을 만들어 필요한 리소스나 리소스 그룹에 연결합니다. 예를 들어, 리소스 그룹 정책이 매시간 백업만 지정하고 매일 백업도 추가하려는 경우, 매일 일정 유형으로 정책을 만들어 리소스 그룹에 추가할 수 있습니다. 그러면 리소스 그룹에는 시간별 정책과 일별 정책이라는 두 가지 정책이 생깁니다.
일정 유형 제거 또는 변경	다음을 수행하세요. 1. 해당 정책을 사용하는 모든 리소스와 리소스 그룹에서 정책을 분리합니다. 2. 일정 유형을 수정합니다. 3. 모든 리소스와 리소스 그룹에 정책을 다시 연결합니다. 예를 들어, 정책에서 매시간 백업을 지정하고 이를 매일 백업으로 변경하려는 경우 먼저 해당 정책을 분리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *정책*을 클릭합니다.
3. 정책을 선택한 다음 *수정*을 클릭합니다.
4. 정보를 수정한 후 *마침*을 클릭합니다.

정책 분리

더 이상 해당 정책으로 리소스의 데이터 보호를 관리하고 싶지 않으면 언제든지 리소스 또는 리소스 그룹에서 정책을 분리할 수 있습니다. 정책을 삭제하거나 일정 유형을 수정하려면 먼저 정책을 분리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.
3. 리소스 그룹을 선택한 다음 *리소스 그룹 수정*을 클릭합니다.
4. 리소스 그룹 수정 마법사의 정책 페이지에서 드롭다운 목록에서 분리하려는 정책 옆에 있는 확인 표시를 지웁니다.
5. 마법사의 나머지 부분에서 리소스 그룹에 대한 추가 수정 사항을 적용한 다음 *마침*을 클릭합니다.

정책 삭제

더 이상 정책이 필요하지 않은 경우 정책을 삭제하는 것이 좋습니다.

시작하기 전에

정책이 리소스 또는 리소스 그룹과 연결되어 있는 경우 해당 정책을 리소스 또는 리소스 그룹에서 분리해야 합니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *정책*을 클릭합니다.
3. 정책을 선택한 다음 *삭제*를 클릭합니다.
4. *예*를 클릭하세요.

리소스 그룹 관리

리소스 그룹에서 다양한 작업을 수행할 수 있습니다.

리소스 그룹과 관련된 다음 작업을 수행할 수 있습니다.

- 리소스 그룹을 선택하고 *리소스 그룹 수정*을 클릭하여 리소스 그룹을 수정하면 리소스 그룹을 만들 때 제공한 정보를 편집할 수 있습니다.



리소스 그룹을 수정하는 동안 일정을 변경할 수 있습니다. 하지만 일정 유형을 변경하려면 정책을 수정해야 합니다.



리소스 그룹에서 리소스를 제거하는 경우 리소스 그룹에 현재 연결된 정책에 정의된 백업 보존 설정은 제거된 리소스에 계속 적용됩니다.

- 리소스 그룹의 백업을 만듭니다.
- 백업의 복제본을 만듭니다.

기존 SQL, Oracle, Windows 파일 시스템, 사용자 정의 애플리케이션, SAP HANA 데이터베이스 리소스 또는 리소스 그룹의 백업에서 복제할 수 있습니다.

- 리소스 그룹의 복제본을 만듭니다.

이 작업은 SQL 리소스 그룹(데이터베이스만 포함)에 대해서만 지원됩니다. 리소스 그룹 복제 일정(복제 수명 주기)을 구성할 수 있습니다.

- 리소스 그룹에서 예약된 작업이 시작되지 않도록 합니다.
- 리소스 그룹을 삭제합니다.

리소스 그룹에서 작업 중지 및 재개

리소스 그룹에서 예약된 작업이 시작되지 않도록 일시적으로 비활성화할 수 있습니다. 나중에 원할 때 해당 작업을 활성화할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.

2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.
3. 리소스 그룹을 선택하고 *유지 관리*를 클릭합니다.
4. *확인*을 클릭합니다.

유지 관리 모드로 전환한 리소스 그룹에서 작업을 재개하려면 리소스 그룹을 선택하고 *프로덕션*을 클릭하세요.

리소스 그룹 삭제

리소스 그룹의 리소스를 더 이상 보호할 필요가 없으면 리소스 그룹을 삭제할 수 있습니다. SnapCenter 에서 플러그인을 제거하기 전에 리소스 그룹이 삭제되었는지 확인해야 합니다.

이 작업에 관하여

리소스 그룹의 모든 리소스에 대해 생성된 모든 복제본을 수동으로 삭제해야 합니다. 선택적으로 리소스 그룹과 연관된 모든 백업, 메타데이터, 정책 및 스냅샷을 강제로 삭제할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 목록에서 *리소스 그룹*을 선택합니다.
3. 리소스 그룹을 선택한 다음 *삭제*를 클릭합니다.
4. 선택 사항: 리소스 그룹과 연관된 모든 백업, 메타데이터, 정책 및 스냅샷을 제거하려면 이 리소스 그룹과 연관된 백업 삭제 및 정책 분리 확인란을 선택합니다.
5. *확인*을 클릭합니다.

백업 관리

백업의 이름을 바꾸고 삭제할 수 있습니다. 여러 백업을 동시에 삭제할 수도 있습니다.

백업 이름 바꾸기

검색성을 높이기 위해 더 나은 이름을 지정하려면 백업의 이름을 바꿀 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 목록에서 리소스 또는 리소스 그룹을 선택합니다.

리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다. 리소스 또는 리소스 그룹이 데이터 보호용으로 구성되지 않은 경우 토폴로지 페이지 대신 보호 마법사가 표시됩니다.

4. 사본 관리 보기에서 기본 스토리지 시스템의 *백업*을 선택합니다.

보조 저장 시스템에 있는 백업의 이름을 바꿀 수 없습니다.

Oracle Recovery Manager(RMAN)를 사용하여 Oracle 데이터베이스 백업을 카탈로그화한 경우 카탈로그화된

백업의 이름을 바꿀 수 없습니다.

5. 백업을 선택한 후 클릭하세요. .
6. 백업 이름 바꾸기 필드에 새 이름을 입력하고 *확인*을 클릭합니다.

백업 삭제

다른 데이터 보호 작업에 더 이상 백업이 필요하지 않으면 백업을 삭제할 수 있습니다.

시작하기 전에

백업을 삭제하기 전에 연관된 복제본을 삭제해야 합니다.



백업이 복제된 리소스와 연결되어 있는 경우 백업을 삭제할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 목록에서 리소스 또는 리소스 그룹을 선택합니다.

리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. 사본 관리 보기에서 기본 스토리지 시스템의 *백업*을 선택합니다.

보조 저장 시스템에 있는 백업은 삭제할 수 없습니다.

5. 백업을 선택한 후 클릭하세요. .

SAP HANA 데이터베이스 백업을 삭제하는 경우 해당 백업의 연관된 SAP HANA 카탈로그도 삭제됩니다.



마지막으로 남아 있는 백업이 삭제되면 연관된 HANA 카탈로그 항목을 삭제할 수 없습니다.

6. *확인*을 클릭합니다.



SnapCenter 에 오래된 데이터베이스 백업이 있고 스토리지 시스템에 해당 백업이 없는 경우 remove-smbbackup 명령을 사용하여 이러한 오래된 백업 항목을 정리해야 합니다. 오래된 백업이 카탈로그화된 경우 복구 카탈로그 데이터베이스에서 카탈로그에서 제거됩니다.

보호 제거

보호 제거는 모든 백업을 삭제하고 모든 정책을 분리합니다. 보호를 제거하기 전에 백업이 마운트되지 않았고 백업과 연결된 복제본이 없는지 확인해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.

3. 목록에서 리소스 또는 리소스 그룹을 선택합니다.

리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. 백업을 선택하고 *보호 제거*를 클릭합니다.

클론 삭제

더 이상 필요하지 않은 복제본은 삭제할 수 있습니다.

이 작업에 관하여

다른 클론의 소스 역할을 하는 클론은 삭제할 수 없습니다.

예를 들어, 프로덕션 데이터베이스가 db1인 경우 데이터베이스 clone1은 db1의 백업에서 복제되고 이후 clone1은 보호됩니다. 데이터베이스 clone2는 clone1의 백업에서 복제되었습니다. clone1을 삭제하기로 결정한 경우 먼저 clone2를 삭제한 다음 clone1을 삭제해야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 보기 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 목록에서 리소스 또는 리소스 그룹을 선택합니다.

리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템의 *복제본*을 선택합니다.
5. 복제본을 선택한 다음 클릭하세요. .

SAP HANA 데이터베이스 복제본을 삭제하는 경우 복제본 삭제 페이지에서 다음 작업을 수행합니다.

- a. 사전 복제 삭제 필드에 복제본을 삭제하기 전에 실행해야 하는 명령을 입력합니다.
 - b. 언마운트 필드에 클론을 삭제하기 전에 클론을 언마운트하는 명령을 입력합니다.
6. *확인*을 클릭합니다.

끝난 후

때로는 파일 시스템이 삭제되지 않는 경우가 있습니다. 다음 명령을 실행하여 CLONE_DELETE_DELAY 매개변수의 값을 늘려야 합니다..`./sccli Set-SmConfigSettings`



CLONE_DELETE_DELAY 매개변수는 애플리케이션 복제본 삭제가 완료된 후 파일 시스템 삭제를 시작하기 전까지 기다리는 시간(초)을 지정합니다.

매개변수 값을 수정한 후 SnapCenter 플러그인 Loader (SPL) 서비스를 다시 시작합니다.

작업, 일정, 이벤트 및 로그를 모니터링합니다.

모니터 페이지에서 작업 진행 상황을 모니터링하고, 예약된 작업에 대한 정보를 얻고, 이벤트와 로그를 검토할 수 있습니다.

작업 모니터링

SnapCenter 백업, 복제, 복원 및 검증 작업에 대한 정보를 볼 수 있습니다. 시작 및 종료 날짜, 작업 유형, 리소스 그룹, 정책 또는 SnapCenter 플러그인을 기준으로 이 보기를 필터링할 수 있습니다. 또한, 지정된 작업에 대한 추가 세부 정보와 로그 파일을 확인할 수도 있습니다.

SnapMirror 및 SnapVault 작업과 관련된 작업도 모니터링할 수 있습니다.



SnapCenter 관리자 또는 다른 슈퍼 유저 역할이 할당되지 않은 한, 본인이 생성하고 본인과 관련된 작업만 모니터링할 수 있습니다.

작업 모니터링과 관련된 다음 작업을 수행할 수 있습니다.

- 백업, 복제, 복원 및 검증 작업을 모니터링합니다.
- 작업 세부 정보와 보고서를 확인하세요.
- 예약된 작업을 중지합니다.

예약된 백업 작업 관리

SnapCenter 6.0.1 릴리스부터 새로운 매개변수 `*JobConcurrencyThreshold*`가 도입되어 주어진 시간에 실행될 수 있는 예약된 작업 수에 대한 임계값을 설정합니다. 이를 통해 시스템 하드웨어 구성에 따라 실행하려는 백업 수를 제어할 수 있습니다.

`*JobConcurrencyThreshold*`에 할당된 기본값은 0이며 비활성화되어 있습니다. 예약된 백업 창 동안 성능 저하가 관찰되면 값을 할당하여 활성화할 수 있습니다.



`*JobConcurrencyThreshold*`를 활성화하여 동시 작업을 관리하는 경우 SnapCenter 백업 순서를 제어할 수 없으며 일정에 지정된 동시에 백업이 트리거되지 않을 수 있습니다.

단계

1. `C:\Program Files\NetApp\ SnapCenter WebApp\ SnapManager.Web.UI.dll.config`에 있는 `_JobConcurrencyThreshold` 매개변수의 값을 설정합니다.
2. IIS > 애플리케이션 풀 > SnapCenter > 다시 시작을 클릭하여 SnapCenter 애플리케이션 풀을 재할용합니다.
3. IIS > 사이트 > SnapCenter > 다시 시작을 클릭하여 SnapCenter 웹 서비스를 다시 시작합니다.

오래된 작업 관리

오래된 작업은 SnapCenter 의 중단이나 부적절한 작업 업데이트로 인해 생성됩니다. SnapCenter 6.0.1 릴리스부터 72시간 이상 멈춰 있는 오래된 작업을 정리하기 위한 사전 정의된 일정이 도입되었습니다. 구성 가능한 매개변수 `*CleanUpStaleJobsIntervalHours*`를 편집하여 일정 빈도를 변경할 수 있습니다.

모니터 > 일정 > `*SnapCenter_StaleJobCleanUp*`에서 일정을 실행하여 필요에 따라 정리를 트리거할 수 있습니다.

단계

1. C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config_에 있는 _CleanUpStaleJobsIntervalHours 매개변수의 값을 설정합니다.
2. IIS > 애플리케이션 풀 > SnapCenter > 다시 시작을 클릭하여 SnapCenter 애플리케이션 풀을 재활용합니다.
3. IIS > 사이트 > SnapCenter > 다시 시작을 클릭하여 SnapCenter 웹 서비스를 다시 시작합니다.

일정을 모니터링하세요

작업이 시작되는 시점, 마지막 실행 시점, 다음에 실행되는 시점을 확인하려면 현재 일정을 확인하는 것이 좋습니다. 또한 작업이 실행되는 호스트와 작업의 리소스 그룹 및 정책 정보를 확인할 수도 있습니다.

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *일정*을 클릭합니다.
3. 리소스 그룹과 일정 유형을 선택하세요.
4. 예정된 작업 목록을 확인하세요.

이벤트 모니터링

사용자가 리소스 그룹을 생성하거나 시스템이 예약된 백업을 생성하는 등의 활동을 시작할 때 등 시스템에서 SnapCenter 이벤트 목록을 볼 수 있습니다. 백업이나 복원 작업과 같은 작업이 현재 진행 중인지 확인하기 위해 이벤트를 보고 싶을 수도 있습니다.

이 작업에 관하여

모든 채용 정보는 이벤트 페이지에 표시됩니다. 예를 들어, 백업 작업이 시작되면 “backup start” 이벤트가 나타납니다. 백업이 완료되면 “백업 완료” 이벤트가 나타납니다.

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 모니터 페이지에서 *이벤트*를 클릭합니다.
3. (선택 사항) 필터 상자에서 시작 또는 종료 날짜, 이벤트 범주(예: 백업, 리소스 그룹 또는 정책), 심각도 수준을 입력하고 *적용*을 클릭합니다. 또는 검색창에 문자를 입력하세요.
4. 이벤트 목록을 확인하세요.

로그 모니터링

SnapCenter 서버 로그, SnapCenter 호스트 에이전트 로그, 플러그인 로그를 보고 다운로드할 수 있습니다. 문제 해결에 도움이 되도록 로그를 확인하는 것이 좋습니다.

이 작업에 관하여

로그를 필터링하여 특정 로그 심각도 수준만 표시할 수 있습니다.

- 디버그

- 정보
- 경고하다
- 오류
- 치명적인

또한 작업 수준 로그를 얻을 수도 있습니다. 예를 들어, 백업 작업 실패 이유를 해결하는 데 도움이 되는 로그입니다. 작업 수준 로그의 경우 모니터 > 작업 옵션을 사용하세요.

단계

1. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
2. 작업 페이지에서 작업을 선택하고 로그 다운로드를 클릭합니다.

다운로드한 압축 폴더에는 작업 로그와 일반 로그가 들어 있습니다. 압축된 폴더 이름에는 선택한 작업 ID와 작업 유형이 포함되어 있습니다.

3. 모니터 페이지에서 *로그*를 클릭합니다.
4. 로그 유형, 호스트, 인스턴스를 선택하세요.

로그 유형을 *플러그인*으로 선택하면 호스트 또는 SnapCenter 플러그인을 선택할 수 있습니다. 로그 유형이 *서버*인 경우에는 이 작업을 수행할 수 없습니다.

5. 특정 소스, 메시지 또는 로그 수준별로 로그를 필터링하려면 열 제목 상단에 있는 필터 아이콘을 클릭합니다.

모든 로그를 표시하려면 *크거나 같음*을 선택하십시오. Debug 수준.

6. *새로고침*을 클릭하세요.
7. 로그 목록을 확인하세요.
8. *다운로드*를 클릭하여 로그를 다운로드하세요.

다운로드한 압축 폴더에는 작업 로그와 일반 로그가 들어 있습니다. 압축된 폴더 이름에는 선택한 작업 ID와 작업 유형이 포함되어 있습니다.

최적의 성능을 위해 대규모 구성에서는 PowerShell cmdlet을 사용하여 SnapCenter 의 로그 설정을 최소 수준으로 설정해야 합니다.

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10
-JobLogsMaxFileSize 10MB -Server
```



장애 조치 작업이 완료된 후 상태 또는 구성 정보에 액세스하려면 cmdlet을 실행하세요. Get-SmRepositoryConfig.

SnapCenter 에서 작업 및 로그 제거

SnapCenter 에서 백업, 복원, 복제 및 검증 작업과 로그를 제거할 수 있습니다. SnapCenter 사용자가 삭제하지 않는 한 성공한 작업 로그와 실패한 작업 로그를 무기한 저장합니다. 저장 공간을 보충하려면 제거하는 것이 좋습니다.

이 작업에 관하여

현재 운영 중인 일자리가 없어야 합니다. 작업 ID를 제공하여 특정 작업을 제거할 수도 있고, 지정된 기간 내에 작업을 제거할 수도 있습니다.

작업을 제거하기 위해 호스트를 유지 관리 모드로 전환할 필요는 없습니다.

단계

1. PowerShell을 실행합니다.
2. 명령 프롬프트에서 다음을 입력합니다. `Open-SMConnection`
3. 명령 프롬프트에서 다음을 입력합니다. `Remove-SmJobs`
4. 왼쪽 탐색 창에서 *모니터*를 클릭합니다.
5. 모니터 페이지에서 *작업*을 클릭합니다.
6. 작업 페이지에서 작업 상태를 검토하세요.

관련 정보

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. ["SnapCenter 소프트웨어 Cmdlet 참조 가이드"](#).

SnapCenter 보고 기능 개요

SnapCenter 시스템 상태와 운영 성공 여부를 모니터링하고 관리할 수 있는 다양한 보고 옵션을 제공합니다.

보고서 유형	설명
백업 보고서	백업 보고서는 SnapCenter 환경의 백업 추세, 백업 성공률, 지정된 시간 동안 수행된 각 백업에 대한 일부 정보에 대한 전반적인 데이터를 제공합니다. 백업이 삭제되면 보고서에는 삭제된 백업에 대한 상태 정보가 표시되지 않습니다. 백업 세부 정보 보고서는 지정된 백업 작업에 대한 자세한 정보를 제공하고 성공적으로 백업된 리소스와 실패한 리소스를 나열합니다.
복제 보고서	클론 보고서는 SnapCenter 환경의 클론 추세, 클론 성공률, 지정된 시간 동안 수행된 각 클론 작업에 대한 일부 정보에 대한 전반적인 데이터를 제공합니다. 복제본이 삭제되면 보고서에는 삭제된 복제본에 대한 상태 정보가 표시되지 않습니다. 복제 세부 정보 보고서는 지정된 복제, 복제 호스트 및 복제 작업 상태에 대한 세부 정보를 제공합니다. 작업이 실패하면 복제 세부 정보 보고서에 실패에 대한 정보가 표시됩니다.

보고서 유형	설명
보고서 복원	복원 보고서는 복원 작업에 대한 전반적인 정보를 제공합니다. 복원 세부 정보 보고서는 호스트 이름, 백업 이름, 작업 시작 및 기간, 개별 작업의 상태를 포함하여 지정된 복원 작업에 대한 세부 정보를 제공합니다. 작업이 실패하면 복원 세부 정보 보고서에 실패에 대한 정보가 표시됩니다.
보호 보고서	이러한 보고서는 모든 SnapCenter 플러그인 인스턴스에서 관리하는 리소스에 대한 보호 세부 정보를 제공합니다. 이 보고서는 모든 플러그인 인스턴스에서 관리하는 리소스에 대한 보호 세부 정보를 제공합니다. 보고서가 생성될 때 백업되지 않은 리소스, 보호되지 않은 리소스, 백업 작업이 실패한 리소스 그룹의 리소스, SnapVault 상태 등에 대한 개요, 세부 정보를 볼 수 있습니다.
예정된 보고서	이러한 보고서는 매일, 매주 또는 매월 등 주기적으로 실행되도록 예약되어 있습니다. 보고서는 지정된 날짜와 시간에 자동으로 생성되며, 해당 보고서는 이메일을 통해 해당 담당자에게 전송됩니다. 일정을 활성화, 비활성화, 수정 또는 삭제할 수 있습니다. 활성화된 일정은 지금 실행 버튼을 클릭하여 필요에 따라 실행할 수 있습니다. 관리자는 모든 일정을 실행할 수 있지만, 생성된 보고서에는 일정을 만든 사용자가 제공한 권한에 따라 데이터가 포함됩니다. 관리자 외의 다른 사용자는 자신의 권한에 따라 일정을 보거나 수정할 수 있습니다. 역할 추가 페이지에서 이 역할의 모든 구성원이 다른 구성원의 객체를 볼 수 있음 옵션이 선택된 경우, 해당 역할의 다른 구성원이 보고 수정할 수 있습니다.

액세스 보고서

SnapCenter 대시보드를 사용하면 시스템 상태를 빠르게 파악할 수 있습니다. 대시보드에서 더 자세한 내용을 확인할 수 있습니다. 혹은 자세한 보고서에 직접 접근할 수도 있습니다.

다음 방법 중 하나를 사용하여 보고서에 액세스할 수 있습니다.

- 왼쪽 탐색 창에서 대시보드*를 클릭한 다음 *마지막 보호 요약 원형 차트를 클릭하면 보고서 페이지에서 자세한 내용을 볼 수 있습니다.
- 왼쪽 탐색 창에서 *보고서*를 클릭합니다.

보고서 필터링

필요한 정보의 세부 수준과 기간 등에 따라 다양한 매개변수에 따라 보고서 데이터를 필터링할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *보고서*를 클릭합니다.
2. 매개변수 보기가 표시되지 않으면 보고서 도구 모음에서 매개변수 영역 전환 아이콘을 클릭합니다.
3. 보고서를 실행할 시간 범위를 지정하세요. + 종료 날짜를 생략하면 사용 가능한 모든 정보가 검색됩니다.
4. 다음 기준에 따라 보고서 정보를 필터링합니다.
 - 리소스 그룹
 - 주인
 - 정책
 - 의지
 - 상태
 - 플러그인 이름
5. *적용*을 클릭하세요.

보고서 내보내기 또는 인쇄

SnapCenter 보고서를 내보내면 다양한 대체 형식으로 보고서를 볼 수 있습니다. 보고서를 인쇄할 수도 있습니다.

단계

1. 왼쪽 탐색 창에서 *보고서*를 클릭합니다.
2. 보고서 도구 모음에서 다음 중 하나를 수행합니다.
 - 인쇄 가능한 보고서를 미리 보려면 인쇄 미리보기 전환 아이콘을 클릭하세요.
 - 보고서를 다른 형식으로 내보내려면 내보내기 아이콘 드롭다운 목록에서 형식을 선택하세요.
3. 보고서를 인쇄하려면 인쇄 아이콘을 클릭하세요.
4. 특정 보고서 요약을 보려면 보고서의 해당 섹션으로 스크롤하세요.

이메일 알림을 위한 SMTP 서버 설정

데이터 보호 작업 보고서를 자신 또는 다른 사람에게 보내는 데 사용할 SMTP 서버를 지정할 수 있습니다. 구성을 확인하기 위해 테스트 이메일을 보낼 수도 있습니다. 해당 설정은 이메일 알림을 구성하는 모든 SnapCenter 작업에 전역적으로 적용됩니다.

이 옵션은 모든 데이터 보호 작업 보고서를 보내기 위한 SMTP 서버를 구성합니다. 그러나 특정 리소스에 대한 정기적인 SnapCenter 데이터 보호 작업 업데이트를 자신이나 다른 사람에게 전송하여 해당 업데이트 상태를 모니터링하려는 경우, 리소스 그룹을 생성할 때 SnapCenter 보고서를 이메일로 전송하는 옵션을 구성할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *전역 설정*을 클릭합니다.
3. SMTP 서버를 입력하고 *저장*을 클릭합니다.
4. 테스트 이메일을 보내려면 이메일을 보낼 발신자 및 수신자 이메일 주소를 입력하고, 제목을 입력한 후 *보내기*를 클릭하세요.

이메일로 보고서를 보내는 옵션을 구성하세요

정기적인 SnapCenter 데이터 보호 작업 업데이트를 자신이나 다른 사람에게 전송하여 해당 업데이트 상태를 모니터링하려는 경우, 리소스 그룹을 생성할 때 SnapCenter 보고서를 이메일로 전송하는 옵션을 구성할 수 있습니다.

시작하기 전에

설정 아래의 글로벌 설정 페이지에서 SMTP 서버를 구성했어야 합니다.

단계

1. 왼쪽 탐색 창에서 *리소스*를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 보고 싶은 리소스 유형을 선택하고 *새 리소스 그룹*을 클릭하거나, 기존 리소스 그룹을 선택하고 *수정*을 클릭하여 기존 리소스 그룹에 대한 이메일 보고서를 구성합니다.
3. 새 리소스 그룹 마법사의 알림 패널에서 풀다운 메뉴에서 항상 보고서를 받을지, 실패 시 보고서를 받을지, 실패 또는 경고 시 보고서를 받을지 선택합니다.
4. 이메일이 발송된 주소, 이메일이 발송된 주소, 이메일 제목을 입력하세요.

SnapCenter 서버 저장소 관리

SnapCenter 에서 수행되는 다양한 작업과 관련된 정보는 SnapCenter 서버 데이터베이스 저장소에 저장됩니다. SnapCenter 서버를 데이터 손실로부터 보호하려면 저장소의 백업을 만들어야 합니다.

SnapCenter 서버 저장소는 때때로 NSM 데이터베이스라고도 합니다.

SnapCenter 저장소 보호를 위한 전제 조건

SnapCenter 저장소를 보호하려면 환경이 특정 전제 조건을 충족해야 합니다.

- 스토리지 가상 머신(SVM) 연결 관리

저장소 자격 증명을 구성해야 합니다.

- 호스트 프로비저닝

SnapCenter 저장소 호스트에는 최소한 하나의 NetApp 스토리지 디스크가 있어야 합니다. SnapCenter 저장소 호스트에 NetApp 디스크가 없으면 디스크를 하나 만들어야 합니다.

호스트 추가, SVM 연결 설정, 호스트 프로비저닝에 대한 자세한 내용은 설치 지침을 참조하세요.

- iSCSI LUN 또는 VMDK 프로비저닝

고가용성(HA) 구성의 경우 SnapCenter 서버 중 하나에서 iSCSI LUN이나 VMDK를 프로비저닝할 수 있습니다.

SnapCenter 저장소 백업

SnapCenter 서버 저장소를 백업하면 데이터 손실로부터 보호하는 데 도움이 됩니다. *Protect-SmRepository* cmdlet을 실행하여 저장소를 백업할 수 있습니다.

이 작업에 관하여

Protect-SmRepository cmdlet은 다음 작업을 수행합니다.

- 리소스 그룹과 정책을 생성합니다.
- SnapCenter 저장소에 대한 백업 일정을 생성합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 *Open-SmConnection* cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
3. *Protect-SmRepository* cmdlet과 필요한 매개변수를 사용하여 저장소를 백업합니다.

SnapCenter 저장소의 백업 보기

Get-SmRepositoryBackups cmdlet을 실행하면 SnapCenter Server 데이터베이스 저장소 백업 목록을 표시할 수 있습니다.

저장소 백업은 *Protect-SmRepository* cmdlet에 지정된 일정에 따라 생성됩니다.

단계

1. PowerShell을 실행합니다.
2. 명령 프롬프트에서 다음 cmdlet을 입력한 다음 SnapCenter 서버에 연결하기 위한 자격 증명을 제공합니다. *Open-SMConnection*
3. *Get-SmRepositoryBackups* cmdlet을 사용하여 사용 가능한 모든 SnapCenter 데이터베이스 백업을 나열합니다.

SnapCenter 데이터베이스 저장소 복원

Restore-SmRepositoryBackup cmdlet을 실행하여 SnapCenter 저장소를 복원할 수 있습니다.

SnapCenter 저장소를 복원하는 경우, 복원 작업 중에는 저장소 데이터베이스에 액세스할 수 없으므로 실행 중인 다른 SnapCenter 작업에 영향을 미칩니다.

단계

1. PowerShell을 실행합니다.
2. 명령 프롬프트에서 다음 cmdlet을 입력한 다음 SnapCenter 서버에 연결하기 위한 자격 증명을 제공합니다. *Open-SMConnection*
3. *Restore-SmRepositoryBackup* cmdlet을 사용하여 저장소 백업을 복원합니다.

다음 cmdlet은 iSCSI LUN이나 VMDK에 있는 백업에서 SnapCenter MySQL 데이터베이스 저장소를 복원합니다.

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mvax3550-s09_09-15-2016_10.32.00.4445
```

다음 cmdlet은 iSCSI LUN에서 백업 파일이 실수로 삭제된 경우 SnapCenter MySQL 데이터베이스를 복원합니다. VMDK의 경우 ONTAP 스냅샷에서 백업을 수동으로 복원합니다.

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
```



복원 작업을 수행한 후 저장소 백업을 검색하면 저장소 복원 작업을 수행하는 데 사용된 백업은 나열되지 않습니다.

SnapCenter 저장소 마이그레이션

SnapCenter Server 데이터베이스 저장소를 기본 위치에서 다른 디스크로 마이그레이션할 수 있습니다. 더 많은 공간이 있는 디스크로 저장소를 옮기고 싶을 때 저장소를 마이그레이션할 수 있습니다.

단계

1. Windows에서 MYSQL57 서비스를 중지합니다.
2. MySQL 데이터 디렉토리를 찾습니다.

일반적으로 데이터 디렉터리는 C:\ProgramData\MySQL\MySQL Server 5.7\Data에서 찾을 수 있습니다.

3. MySQL 데이터 디렉토리를 새 위치(예: E:\Data\nsm)로 복사합니다.
4. 새 디렉토리를 마우스 오른쪽 버튼으로 클릭한 다음 속성 > *보안*을 선택하여 네트워크 서비스 로컬 서버 계정을 새 디렉토리에 추가한 다음 해당 계정에 모든 권한을 할당합니다.
5. 원래 데이터베이스 디렉토리의 이름을 nsm_copy로 바꿉니다.
6. Windows 명령 프롬프트에서 *mklink* 명령을 사용하여 심볼릭 디렉토리 링크를 만듭니다.

```
"mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
```

7. Windows에서 MYSQL57 서비스를 시작합니다.
8. SnapCenter 에 로그인하여 저장소 항목을 확인하거나 MySQL 유틸리티에 로그인하여 새 저장소에 연결하여 데이터베이스 위치가 변경되었는지 확인합니다.
9. 원래의 이름이 바뀐 데이터베이스 저장소 디렉토리(nsm_copy)를 삭제합니다.

SnapCenter 저장소 비밀번호 재설정

MySQL 서버 저장소 데이터베이스 비밀번호는 SnapCenter 4.2에서 SnapCenter 서버를 설치하는 동안 자동으로 생성됩니다. 이 자동 생성된 비밀번호는 SnapCenter 사용자에게 어떤 시점에서도 알려지지 않습니다. 저장소 데이터베이스에 접근하려면 비밀번호를 재설정해야 합니다.

시작하기 전에

비밀번호를 재설정하려면 SnapCenter 관리자 권한이 있어야 합니다.

단계

1. PowerShell을 실행합니다.

2. 명령 프롬프트에서 다음 명령을 입력한 다음 SnapCenter 서버에 연결하기 위한 자격 증명을 제공하세요: *Open-SMConnection*
3. 저장소 비밀번호 재설정: *Set-SmRepositoryPassword*

다음 명령은 저장소 비밀번호를 재설정합니다.

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: *****
ConfirmPassword: *****
Successfully updated the MySQL server password.
```

관련 정보

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

신뢰할 수 없는 도메인의 리소스 관리

SnapCenter Active Directory(AD) 신뢰할 수 있는 도메인의 호스트를 관리하는 것 외에도 여러 AD 신뢰할 수 없는 도메인의 호스트도 관리합니다. 신뢰할 수 없는 AD 도메인은 SnapCenter 서버에 등록되어야 합니다. SnapCenter 여러 개의 신뢰할 수 없는 AD 도메인의 사용자와 그룹을 지원합니다.

도메인이나 작업 그룹에 속한 컴퓨터에 SnapCenter 서버를 설치할 수 있습니다. SnapCenter 서버를 설치하려면 해당 컴퓨터가 도메인에 있는 경우 도메인 자격 증명을 지정해야 하고, 해당 컴퓨터가 작업 그룹에 있는 경우 로컬 관리자 자격 증명을 지정해야 합니다.

SnapCenter 서버에 등록되지 않은 도메인에 속한 Active Directory(AD) 그룹은 지원되지 않습니다. 이러한 AD 그룹으로 SnapCenter 역할을 생성할 수는 있지만 SnapCenter 서버에 로그인하면 다음 오류 메시지가 나타나며 실패합니다. 로그인하려는 사용자는 어떤 역할에도 속하지 않습니다. 관리자에게 문의하세요.

신뢰할 수 없는 도메인 수정

도메인 컨트롤러 IP 주소나 정규화된 도메인 이름(FQDN)을 업데이트하려는 경우 신뢰할 수 없는 도메인을 수정할 수 있습니다.

이 작업에 관하여

FQDN을 수정한 후에는 연관된 자산(호스트, 사용자, 그룹)이 예상대로 작동하지 않을 수 있습니다.

신뢰할 수 없는 도메인을 수정하려면 SnapCenter 사용자 인터페이스나 PowerShell cmdlet을 사용할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 ***설정***을 클릭합니다.
2. 설정 페이지에서 ***전역 설정***을 클릭합니다.

3. 글로벌 설정 페이지에서 *도메인 설정*을 클릭합니다.

4.

딸깍 하는 소리  , 그리고 다음 세부 정보를 제공하세요.

이 분야에서는...	이렇게 하세요...
도메인 FQDN	FQDN을 지정하고 *확인*을 클릭합니다.
도메인 컨트롤러 IP 주소	도메인 FQDN을 확인할 수 없는 경우 하나 이상의 도메인 컨트롤러 IP 주소를 지정하세요.

5. *확인*을 클릭합니다.

신뢰할 수 없는 Active Directory 도메인 등록 취소

해당 도메인에 연결된 자산을 사용하지 않으려면 신뢰할 수 없는 Active Directory 도메인의 등록을 취소할 수 있습니다.

시작하기 전에

신뢰할 수 없는 도메인과 연결된 호스트, 사용자, 그룹 및 자격 증명을 제거해야 합니다.

이 작업에 관하여

- 도메인이 SnapCenter 서버에서 등록 해제되면 해당 도메인의 사용자는 SnapCenter 서버에 액세스할 수 없습니다.
- 연관된 자산(호스트, 사용자, 그룹)이 있는 경우 도메인 등록을 취소하면 해당 자산은 작동하지 않습니다.
- 신뢰할 수 없는 도메인의 등록을 취소하려면 SnapCenter 사용자 인터페이스나 PowerShell cmdlet을 사용할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *전역 설정*을 클릭합니다.
3. 글로벌 설정 페이지에서 *도메인 설정*을 클릭합니다.
4. 도메인 목록에서 등록을 취소하려는 도메인을 선택합니다.
5. 딸깍 하는 소리  을 클릭한 다음 *확인*을 클릭합니다.

저장 시스템 관리

스토리지 시스템을 추가한 후에는 스토리지 시스템 구성과 연결을 수정하거나 스토리지 시스템을 삭제할 수 있습니다.

스토리지 시스템 구성 수정

사용자 이름, 비밀번호, 플랫폼, 포트, 프로토콜, 시간 초과 기간, 기본 IP 주소 또는 메시징 옵션을 변경하려는 경우 SnapCenter 사용하여 스토리지 시스템 구성을 수정할 수 있습니다.

이 작업에 관하여

개별 사용자 또는 그룹에 대한 저장소 연결을 수정할 수 있습니다. 동일한 스토리지 시스템에 대한 권한이 있는 하나 이상의 그룹에 속해 있는 경우 스토리지 연결 이름은 스토리지 시스템에 대한 권한이 있는 각 그룹마다 한 번씩, 스토리지 연결 목록에 여러 번 표시됩니다.

단계

1. 왼쪽 탐색 창에서 *저장 시스템*을 클릭합니다.
2. 스토리지 시스템 페이지의 유형 드롭다운에서 다음 작업 중 하나를 수행합니다.

선택하다...	단계...
ONTAP SVM	추가된 모든 스토리지 가상 머신(SVM)을 보고, 필요한 SVM 구성을 수정합니다. a. 저장소 연결 페이지에서 적절한 SVM 이름을 클릭합니다. b. 다음 작업 중 하나를 수행합니다. ◦ SVM이 어떤 클러스터에도 속하지 않은 경우 스토리지 시스템 수정 페이지에서 사용자 이름, 비밀번호, EMS 및 AutoSupport 설정, 플랫폼, 프로토콜, 포트, 시간 초과, 기본 IP 등의 구성을 수정합니다. ◦ SVM이 클러스터의 일부인 경우 스토리지 시스템 수정 페이지에서 *SVM을 독립적으로 관리*를 선택하고 사용자 이름, 비밀번호, EMS 및 AutoSupport 설정, 플랫폼, 프로토콜, 포트, 시간 초과, 기본 IP 등의 구성을 수정합니다. SVM을 독립적으로 관리하도록 수정한 후, 클러스터를 통해 관리하기로 결정한 경우 SVM을 삭제한 후 *재검색*을 클릭해야 합니다. SVM이 ONTAP 클러스터에 추가됩니다.  SnapCenter GUI에서 스토리지 시스템 비밀번호가 업데이트되면 해당 플러그인이나 서버 호스트의 SMCORE 서비스를 다시 시작해야 합니다. 업데이트된 비밀번호가 SMCORE에 반영되지 않아 백업 작업이 잘못된 자격 증명 오류로 실패하게 됩니다.

선택하다...	단계...
ONTAP 클러스터	추가된 모든 클러스터를 보고 필요한 클러스터 구성을 수정합니다. a. 저장소 연결 페이지에서 클러스터 이름을 클릭합니다. b. 스토리지 시스템 수정 페이지에서 사용자 이름 옆에 있는 편집 아이콘을 클릭하고 사용자 이름과 비밀번호를 수정합니다. c. EMS 및 AutoSupport 설정을 선택하거나 선택 취소합니다. d. *추가 옵션*을 클릭하고 플랫폼, 프로토콜, 포트, 시간 초과, 기본 IP 등의 다른 구성을 수정합니다.

3. *제출*을 클릭하세요.

저장 시스템 삭제

SnapCenter 사용하면 사용하지 않는 저장 시스템을 삭제할 수 있습니다.

이 작업에 관하여

개별 사용자 또는 그룹의 저장소 연결을 삭제할 수 있습니다. 동일한 스토리지 시스템에 대한 권한이 있는 하나 이상의 그룹에 속해 있는 경우 스토리지 시스템 이름은 스토리지 연결 목록에 여러 번 표시되며, 스토리지 시스템에 대한 권한이 있는 각 그룹마다 한 번씩 표시됩니다.



스토리지 시스템을 삭제하면 해당 스토리지 시스템에서 수행 중인 모든 작업이 실패합니다.

단계

1. 왼쪽 탐색 창에서 *저장 시스템*을 클릭합니다.
2. 스토리지 시스템 페이지의 유형 드롭다운에서 *ONTAP SVM* 또는 *ONTAP 클러스터*를 선택합니다.
3. 저장소 연결 페이지에서 SVM 옆에 있는 확인란을 선택하거나 삭제하려는 클러스터를 선택합니다.



클러스터의 일부인 SVM을 선택할 수 없습니다.

4. *삭제*를 클릭하세요.
5. 저장소 시스템 연결 설정 삭제 페이지에서 *확인*을 클릭합니다.



ONTAP GUI를 사용하여 ONTAP 클러스터에서 SVM을 삭제한 경우 SnapCenter GUI에서 *재검색*을 클릭하여 SVM 목록을 업데이트합니다.

REST API 지원

ONTAP 에 대한 모든 ASA, AFF 또는 FAS 시스템 연결은 기본적으로 ZAPI를 통해 이루어집니다. REST API는 특정

ONTAP 버전에 대해 활성화될 수 있습니다.

SnapCenter ZAPI를 지원하지 않는 ASA r2 시스템에서 모든 작업을 수행하기 위해 REST API를 활용합니다.

다음 구성 파일에서 구성 키를 수정할 수 있습니다.

- 저장소 연결에 대한 휴식이 활성화되어 있습니까?

기본값은 false입니다.

- REST를 사용하는 MinOntapVersion

기본값은 9.13.1입니다.

REST API를 통한 연결 활성화

1. IsRestEnabledForStorageConnection을 true로 설정합니다.
2. 서버와 Windows 플러그인 호스트 모두의 SMCoreServiceHost.dll.config와 SnapDriveService.dll.config에 키를 추가합니다.

```
<키="IsRestEnabledForStorageConnection" 값="true" /> 추가
```

REST API를 통한 연결을 ONTAP의 특정 버전으로 제한합니다.

1. 구성 매개변수 MinOntapVersionToUseREST를 true로 설정합니다.
2. 서버와 Windows 플러그인 호스트 모두의 SMCoreServiceHost.dll.config와 SnapDriveService.dll.config에 키를 추가합니다.

```
<키="MinOntapVersionToUseREST" 값="9.13.1" /> 추가
```

3. 서버에서 SmCore 서비스를 다시 시작하고 플러그인 머신에서 플러그인과 SnapDrive 서비스를 다시 시작합니다.

EMS 데이터 수집 관리

PowerShell cmdlet을 사용하여 이벤트 관리 시스템(EMS) 데이터 수집을 예약하고 관리할 수 있습니다. EMS 데이터 수집에는 SnapCenter 서버, 설치된 SnapCenter 플러그인 패키지, 호스트 및 이와 유사한 정보에 대한 세부 정보를 수집한 다음 이를 지정된 ONTAP 스토리지 가상 머신(SVM)으로 전송하는 작업이 포함됩니다.



데이터 수집 작업이 진행 중일 때는 시스템 CPU 사용률이 높습니다. 작업이 진행되는 동안에는 데이터 크기에 관계없이 CPU 사용률이 높게 유지됩니다.

EMS 데이터 수집 중지

EMS 데이터 수집은 기본적으로 활성화되어 있으며 설치일로부터 7일마다 실행됩니다. PowerShell cmdlet _Disable-SmDataCollectionEMS_를 사용하면 언제든지 데이터 수집을 비활성화할 수 있습니다.

단계

1. PowerShell 명령줄에서 _Open-SmConnection_을 입력하여 SnapCenter 와 세션을 설정합니다.

2. `_Disable-SmDataCollectionEms_`를 입력하여 EMS 데이터 수집을 비활성화합니다.

EMS 데이터 수집 시작

EMS 데이터 수집은 기본적으로 활성화되어 있으며 설치 날짜로부터 7일마다 실행되도록 예약되어 있습니다. 비활성화한 경우 `Enable-SmDataCollectionEMS` cmdlet을 사용하여 EMS 데이터 수집을 다시 시작할 수 있습니다.

NetApp ONTAP 이벤트 `generate-autosupport-log` 권한이 SVM(스토리지 가상 머신) 사용자에게 부여되었습니다.

단계

1. PowerShell 명령줄에서 `_Open-SmConnection_`을 입력하여 SnapCenter 와 세션을 설정합니다.
2. `_Enable-SmDataCollectionEMS_`를 입력하여 EMS 데이터 수집을 활성화합니다.

EMS 데이터 수집 일정 및 대상 SVM 변경

PowerShell cmdlet을 사용하여 EMS 데이터 수집 일정이나 대상 스토리지 가상 머신(SVM)을 변경할 수 있습니다.

단계

1. PowerShell 명령줄에서 SnapCenter 와 세션을 설정하려면 `Open-SmConnection` cmdlet을 입력합니다.
2. EMS 데이터 수집 대상을 변경하려면 `Set-SmDataCollectionEmsTarget` cmdlet을 입력합니다.
3. EMS 데이터 수집 일정을 변경하려면 `Set-SmDataCollectionEmsSchedule` cmdlet을 입력합니다.

EMS 데이터 수집 상태 모니터링

여러 PowerShell cmdlet을 사용하여 EMS 데이터 수집 상태를 모니터링할 수 있습니다. 일정, 스토리지 가상 머신(SVM) 대상 및 상태에 대한 정보를 얻을 수 있습니다.

단계

1. PowerShell 명령줄에서 `_Open-SmConnection_`을 입력하여 SnapCenter 와 세션을 설정합니다.
2. `_Get-SmDataCollectionEmsSchedule_`을 입력하여 EMS 데이터 수집 일정에 대한 정보를 검색합니다.
3. `_Get-SmDataCollectionEmsStatus_`를 입력하여 EMS 데이터 수집 상태에 대한 정보를 검색합니다.
4. `_Get-SmDataCollectionEmsTarget_`을 입력하여 EMS 데이터 수집 대상에 대한 정보를 검색합니다.

관련 정보

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

SnapCenter 서버 및 플러그인 업그레이드

사용 가능한 업데이트를 확인하기 위해 **SnapCenter** 구성합니다.

SnapCenter NetApp 지원 사이트와 주기적으로 통신하여 사용 가능한 소프트웨어 업데이트를 알려드립니다. 또한, 사용 가능한 업데이트에 대한 정보를 받을 간격을 지정하기 위해 일정을 만들 수도 있습니다.

단계

1. 왼쪽 탐색 창에서 *설정*을 클릭합니다.
2. 설정 페이지에서 *소프트웨어*를 클릭합니다.

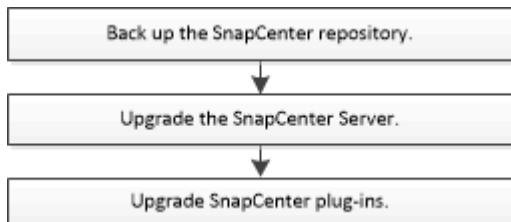
사용 가능한 소프트웨어 페이지에는 사용 가능한 플러그인 패키지, 사용 가능한 버전 및 설치 상태가 표시됩니다.

3. *업데이트 확인*을 클릭하여 최신 버전의 플러그인 패키지가 있는지 확인하세요.
4. *업데이트 일정*을 클릭하면 사용 가능한 업데이트에 대한 정보를 받을 간격을 지정하는 일정을 만들 수 있습니다.
 - a. *업데이트 확인*에서 간격을 선택하세요.
 - b. SnapCenter 서버 관리자 Windows 자격 증명을 선택하고 *확인*을 클릭합니다.

업그레이드 워크플로

SnapCenter 의 각 릴리스에는 업데이트된 SnapCenter 서버와 플러그인 패키지가 포함되어 있습니다. 플러그인 패키지 업데이트는 SnapCenter 설치 프로그램과 함께 배포됩니다. SnapCenter 구성하여 사용 가능한 업데이트를 확인할 수 있습니다.

워크플로는 SnapCenter 서버와 플러그인 패키지를 업그레이드하는 데 필요한 다양한 작업을 보여줍니다.



지원되는 업그레이드 경로

업그레이드 경로를 통해 SnapCenter 의 이전 버전 중에서 최신 버전의 SnapCenter 로 업그레이드할 수 있는 버전과 지원되는 플러그인 버전을 파악하는 데 도움이 됩니다.

SnapCenter 서버 버전을 사용 중이라면...	SnapCenter 서버를 직접 업그레이드할 수 있습니다...	지원되는 플러그인 버전
5.0	6.0	• 5.0 • 6.0
	6.0.1	• 6.0.1
	6.1	• 6.1
6.0	6.0.1	• 6.0 • 6.0.1
	6.1	• 6.1
6.0.1	6.1	• 6.0.1 • 6.1

SnapCenter Plug-in for VMware vSphere 업그레이드에 대한 정보는 다음을 참조하세요. ["SnapCenter Plug-in for VMware vSphere 업그레이드"](#).

Windows 호스트에서 SnapCenter 서버 업그레이드

최신 버전에서 제공되는 최신 기능과 향상된 기능을 사용하려면 SnapCenter 서버를 업그레이드해야 합니다.

시작하기 전에

- SnapCenter 서버 호스트를 최신 Windows 업데이트로 업데이트하고 보류 중인 시스템 재시작이 없는지 확인하세요.
- 업그레이드를 시작하기 전에 다른 작업이 실행되고 있지 않은지 확인하세요.
- ASP.NET Core Runtime 8.0.12(및 모든 후속 8.0.x 패치) 호스팅 번들과 PowerShell 7.4.2 이상을 설치합니다.
- 작업이 실행되고 있지 않은지 확인한 후 SnapCenter 저장소(MySQL) 데이터베이스를 백업합니다. SnapCenter Server와 Exchange 플러그인을 업그레이드하기 전에 이 작업을 수행하는 것이 좋습니다.

자세한 내용은 다음을 참조하세요. ["SnapCenter 저장소 백업"](#).

- SnapCenter 서버 호스트나 플러그인 호스트에서 수정한 모든 SnapCenter 구성 파일을 백업하세요.

SnapCenter 구성 파일의 예: SnapDriveService.exe.config, SMCoreServiceHost.exe.config 등.

- SnapCenter 5.0에 여러 버전의 사용자 지정 플러그인을 설치한 경우 6.0 이상으로 업그레이드하기 전에 PowerShell cmdlet을 실행하여 SnapCenter 저장소(NSM 데이터베이스)에서 최신 버전을 제외한 모든 이전 버전의 사용자 지정 플러그인을 제거해야 합니다.
 - 달리다 Open-SmConnection SnapCenterAdmin 역할 자격 증명을 사용하여 로그인합니다.
 - 달리다 Remove-SmPluginPackage -PluginName M<plug-in name> -PluginVersion

<version number>

자세한 내용은 다음을 참조하세요. "[SnapCenter 6.0 이상으로 업그레이드가 실패합니다.](#)".

이 작업에 관하여

- 업그레이드하는 동안 SnapCenter SQL 스크립트를 실행하여 NSM 데이터베이스의 Exchange 데이터를 업데이트하고 DAG 및 호스트 약어를 FQDN으로 변환합니다. 이는 Exchange 플러그인과 함께 SnapCenter Server를 사용하는 경우에만 적용됩니다.
- 서버 호스트를 수동으로 유지 관리 모드로 전환한 경우 업그레이드 후 호스트 > *일정 활성화*를 선택하여 서버 호스트를 유지 관리 모드에서 해제합니다.
- 정책에서 사전 스크립트와 사후 스크립트가 활성화된 기존 백업 및 검증 일정의 경우, 업그레이드 후에도 백업 작업이 계속 작동합니다.

작업 세부 정보 페이지에서 경고 메시지는 고객에게 스크립트를 SCRIPTS_PATH에 복사하고 정책을 편집하여 SCRIPTS_PATH에 상대적인 경로를 제공하도록 권장합니다. 복제 수명 주기 작업의 경우 경고 메시지는 하위 작업 수준에서 나타납니다.

단계

1. NetApp 지원 사이트에서 SnapCenter 서버 설치 패키지를 다운로드하세요.

<https://mysupport.netapp.com/site/products/all/details/snapcenter/downloads-tab>

2. C:\Program Files\ NetApp\ SnapCenter WebApp에 있는 web.config의 복사본을 만듭니다.
3. 업그레이드에 실패할 경우 Windows 작업 스케줄러에서 SnapCenter 플러그인 호스트 일정을 내보내 복원할 수 있습니다.

```
md d:\\SCBackup\\schtasks /query /xml /TN taskname >>
"D:\\SCBackup\\taskname.xml"
```

4. 저장소 백업이 구성되지 않은 경우 SnapCenter MySQL 데이터베이스 덤프를 만듭니다.

```
md d:\\SCBackup\\mysqldump --all-databases --single-transaction --add-drop
-database --triggers --routines --events -u root -p >
D:\\SCBackup\\SCRepoBackup.dmp
```

메시지가 나타나면 비밀번호를 입력하세요.

5. 다운로드한 .exe 파일을 두 번 클릭하여 SnapCenter 서버 업그레이드를 시작합니다.

업그레이드를 시작하면 SnapCenter 사전 검사를 실행합니다. 시스템이 최소 요구 사항을 충족하지 못하면 SnapCenter 오류 또는 경고 메시지가 표시됩니다. 경고를 무시하고 설치를 계속할 수 있지만, 오류는 반드시 수정해야 합니다.



SnapCenter 이전 버전의 SnapCenter Server를 설치하는 동안 제공된 기존 MySQL Server 저장소 데이터베이스 비밀번호를 계속 사용합니다.

6. *업그레이드*를 선택하세요.

어느 단계에서든 *취소*를 선택하면 SnapCenter 업그레이드를 중지합니다. SnapCenter 서버를 이전 상태로

롤백하지 않습니다.

모범 사례: 로그아웃했다가 다시 로그인하거나 새 브라우저를 열어 SnapCenter 사용자 인터페이스에 액세스하세요.

당신이 완료한 후

- sudo 사용자를 사용하여 플러그인을 설치한 경우 `C:\ProgramData\NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`에 있는 sha224 키를 복사하여 `_etc/sudoers` 파일을 업데이트해야 합니다.
- 서버 호스트에서 리소스를 새로 검색해야 합니다.

SnapCenter 서버 호스트 상태가 중지됨으로 표시되면 잠시 기다렸다가 새로 검색을 수행합니다.
HostRefreshInterval 매개변수 값(기본값은 3600초)을 10분 이상의 값으로 변경할 수도 있습니다.

- 업그레이드가 실패하면 실패한 설치를 정리하고 이전 버전의 SnapCenter 다시 설치하고 NSM 데이터베이스를 이전 상태로 복원합니다.
- 서버 호스트를 업그레이드한 후에는 스토리지 시스템을 추가하기 전에 플러그인도 업그레이드해야 합니다.

Linux 호스트에서 SnapCenter 서버 업그레이드

SnapCenter Server 설치 프로그램 파일을 사용하여 SnapCenter Server를 업그레이드할 수 있습니다.

단계

1. SnapCenter Server를 업그레이드하려면 다음 작업 중 하나를 수행하세요.

공연을 하고 싶다면...	이렇게 하세요...
비대화형 업그레이드	<pre>sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DUPGRADE=<value> -DINSTALL_LOG_NAME=<filename></pre> 예: <code>sudo ./snapcenter_linux_server.bin -i silent</code> <code>-DUPGRADE=1</code> <code>-DINSTALL_LOG_NAME=InstallerLog.log</code> 로그는 <code>_var/opt/snapcenter/logs_</code>에 저장됩니다. 업그레이드를 위해 전달되는 매개변수: • <code>DINSTALL_LOG_NAME</code>: 설치 로그가 저장될 로그 파일 이름입니다. • <code>DUPGRADE</code>: 기본값은 0입니다. SnapCenter 서버를 업그레이드하려면 이 매개변수와 값을 0이 아닌 정수로 지정하세요.

공연을 하고 싶다면...	이렇게 하세요...
대화형 설치	<pre>./snapcenter-linux-server- (e18/e19/sles15).bin</pre> 업그레이드 확인 메시지가 표시됩니다. SnapCenter 서버 업그레이드를 확인하려면 0이 아닌 다른 값을 입력하세요.



SnapCenter 에서 로그아웃한 다음 로그인하거나, 브라우저를 닫은 다음 새 브라우저를 열어 SnapCenter GUI에 액세스하세요.

플러그인 패키지를 업그레이드하세요

플러그인 패키지는 SnapCenter 업그레이드의 일부로 배포됩니다.

업그레이드하려는 각 플러그인 호스트를 수동으로 유지 관리 모드로 전환할 필요는 없습니다. 업그레이드 절차를 통해 Windows, Linux 또는 AIX 플러그인 호스트가 유지 관리 모드로 전환되기 때문입니다. 유지 관리 모드에서는 업그레이드 중에 플러그인 호스트에서 예약된 작업이 실행되는 것을 방지합니다.

시작하기 전에

- Linux 시스템에 액세스할 수 있는 루트가 아닌 사용자인 경우 업그레이드 작업을 수행하기 전에 `/etc/sudoers` 파일을 최신 체크섬 값으로 업데이트해야 합니다.
- 기본적으로 SnapCenter 환경에서 JAVA_HOME을 감지합니다. 고정된 JAVA_HOME을 사용하고 Linux 호스트에서 플러그인을 업그레이드하려는 경우 `/var/opt/snapcenter/spl/etc/`에 있는 `_spl.properties` 파일에 `SKIP_JAVAHOME_UPDATE` 매개변수를 수동으로 추가하고 값을 TRUE로 설정해야 합니다.

플러그인이 업그레이드되거나 SnapCenter 플러그인 로더(SPL) 서비스가 다시 시작되면 JAVA_HOME 값이 업데이트됩니다. SPL을 업그레이드하거나 다시 시작하기 전에 `SKIP_JAVAHOME_UPDATE` 매개변수를 추가하고 값을 TRUE로 설정하면 JAVA_HOME 값이 업데이트되지 않습니다.

- SnapCenter 서버 호스트나 플러그인 호스트에서 수정한 모든 SnapCenter 구성 파일을 백업했어야 합니다.

SnapCenter 구성 파일의 예: `SnapDriveService.exe.config`, `SMCoreServiceHost.exe.config` 등.

이 작업에 관하여

- Microsoft SQL Server용 SnapCenter 플러그인, Microsoft Exchange Server용 SnapCenter 플러그인, Microsoft Windows용 SnapCenter 플러그인의 경우 `SCRIPTS_PATH`를 실행하려면 서버와 플러그인 호스트를 모두 최신 버전으로 업그레이드하는 것이 좋습니다.

정책에서 사전 스크립트와 사후 스크립트가 활성화된 기존 백업 및 검증 일정의 경우, 업그레이드 후에도 백업 작업이 계속 작동합니다.

작업 세부 정보 페이지에서 경고 메시지는 고객에게 스크립트를 `SCRIPTS_PATH`에 복사하고 정책을 편집하여 `SCRIPTS_PATH`에 상대적인 경로를 제공하도록 권장합니다. 복제 수명 주기 작업의 경우 경고 메시지는 하위 작업 수준에서 나타납니다.

단계

1. 왼쪽 탐색 창에서 호스트 > *관리 호스트*를 클릭합니다.

2. 다음 작업 중 하나를 수행하여 호스트를 업그레이드합니다.

◦ 플러그인 호스트 중 하나에 대해 전체 상태 옆에 "업그레이드 가능"이 표시되면 플러그인 호스트 이름을 클릭하고 다음을 수행합니다.

i. *추가 옵션*을 클릭하세요.

ii. 플러그인 호스트가 플러그인 업그레이드 요구 사항을 충족하는지 여부를 검증하지 않으려면 *사전 검사 건너뛰기*를 선택합니다.

iii. *업그레이드*를 클릭하세요.

◦ 여러 호스트를 업그레이드하려면 모든 호스트를 선택하고 다음을 클릭합니다.  을 클릭한 다음 업그레이드 > *확인*을 클릭합니다.

플러그인 업그레이드 중에 모든 관련 서비스가 다시 시작됩니다.



패키지의 모든 플러그인이 선택되지만, 이전 버전의 SnapCenter 와 함께 설치된 플러그인만 업그레이드되고 나머지 플러그인은 설치되지 않습니다. 새로운 플러그인을 설치하려면 플러그인 추가 옵션을 사용해야 합니다.

사전 검사 건너뛰기 확인란을 선택하지 않은 경우, 플러그인 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하기 위해 유효성 검사가 진행됩니다. 최소 요구 사항을 충족하지 못할 경우, 해당 오류 또는 경고 메시지가 표시됩니다. 문제를 해결한 후 *업그레이드*를 클릭하세요.



오류가 디스크 공간이나 RAM과 관련된 경우 C:\Program Files\ NetApp\ SnapCenter WebApp에 있는 web.config나 C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ SnapCenter\에 있는 PowerShell 구성 파일을 업데이트하여 기본값을 수정할 수 있습니다. 오류가 나머지 매개변수와 관련된 경우 문제를 해결한 다음 요구 사항을 다시 검증해야 합니다.

기술 업데이트

SnapCenter 서버 호스트의 기술 업데이트

SnapCenter 서버 호스트를 새로 고쳐야 하는 경우, 새 호스트에 동일한 버전의 SnapCenter 서버를 설치한 다음 API를 실행하여 이전 서버에서 SnapCenter 백업하고 새 서버에서 복원할 수 있습니다.

단계

1. 새로운 호스트를 배포하고 다음 작업을 수행합니다.
 - a. SnapCenter Server의 동일한 버전을 설치합니다.
 - b. (선택 사항) CA 인증서를 구성하고 양방향 SSL을 활성화합니다. 자세한 내용은 다음을 참조하세요. "[CA 인증서 구성](#)" 그리고 "[양방향 SSL 구성 및 활성화](#)".
 - c. (선택 사항) 다중 요소 인증을 구성합니다. 자세한 내용은 다음을 참조하세요. "[다중 요소 인증 활성화](#)".
2. SnapCenter 관리자 사용자로 로그인합니다.
3. API를 사용하여 이전 호스트에 SnapCenter 서버의 백업을 만듭니다.
`/<snapcenter_version>/server/backup` 또는 cmdlet: *New-SmServerBackup*.



백업을 수행하기 전에 예약된 모든 작업을 일시 중단하고 실행 중인 작업이 없는지 확인하세요.



새 도메인에서 실행 중인 SnapCenter 서버에서 백업을 복원하려면 백업을 수행하기 전에 이전 SnapCenter 호스트에 새 도메인 사용자를 추가하고 SnapCenter 관리자 역할을 지정해야 합니다.

4. 이전 호스트에서 새 호스트로 백업을 복사합니다.
5. API를 사용하여 새 호스트에서 SnapCenter 서버의 백업을 복원합니다.
`/<snapcenter_version>/server/restore` 또는 cmdlet: *Restore-SmServerBackup*.

복원을 수행하면 기본적으로 모든 호스트의 새 SnapCenter 서버 URL이 업데이트됩니다. 업데이트를 건너뛰려면 `-SkipSMSURLInHosts` 속성을 사용하고 다음 API를 사용하여 서버 URL을 별도로 업데이트하세요.

`/<snapcenter_version>/server/configureurl` 또는 cmdlet: *Set-SmServerConfig*.



플러그인 호스트가 서버 호스트 이름을 확인할 수 없는 경우 각 플러그인 호스트에 로그인하여 `<New IP> SC_Server_Name` 형식으로 새 IP에 대한 `etc/host` 항목을 추가합니다.



서버 `etc/host` 항목은 복원되지 않습니다. 이전 서버에서 수동으로 복원할 수 있습니다.

새 도메인에서 실행 중인 SnpCenter 서버에서 백업이 복원되었고 이전 도메인 사용자를 계속 사용하려면 새 SnapCenter 서버에서 이전 도메인을 등록해야 합니다.



이전 SnapCenter 호스트에서 `web.config` 파일을 수동으로 업데이트한 경우 업데이트가 새 호스트로 복사되지 않습니다. 새 호스트의 `web.config` 파일에서 동일한 변경 사항을 수동으로 만들어야 합니다.

6. SnapCenter 서버 URL 업데이트를 건너뛰었거나 복원 프로세스 중에 호스트가 다운된 경우 API를 사용하여

SnapCenter 에서 관리하는 모든 호스트 또는 지정된 호스트의 새 서버 이름을 업데이트합니다.
/<snapcenter_version>/server/configureurl 또는 cmdlet: *Set-SmServerConfig*.

7. 새로운 SnapCenter 서버에서 모든 호스트에 예약된 작업을 활성화합니다.

F5 클러스터의 노드 기술 업데이트

F5 클러스터의 모든 노드를 제거하고 새 노드를 추가하여 해당 노드의 기술을 새로 고칠 수 있습니다. 새로 고쳐야 할 노드가 활성 상태인 경우 클러스터의 다른 노드를 활성 상태로 만든 다음 해당 노드를 제거합니다.

F5 클러스터에 노드를 추가하는 방법에 대한 정보는 다음을 참조하세요. "[F5를 사용하여 고가용성을 위한 SnapCenter 서버 구성](#)".



F5 클러스터의 URL이 변경되면 다음 API를 사용하여 모든 호스트에서 URL을 업데이트할 수 있습니다.
/<snapcenter_version>/server/configureurl 또는 cmdlet: *Set-SmServerConfig*.

이전 SnapCenter 서버 호스트 해제

새로운 SnapCenter 서버가 작동 중이고 모든 플러그인 호스트가 새로운 SnapCenter 서버 호스트와 통신할 수 있는지 확인한 후에 이전 SnapCenter 서버 호스트를 제거할 수 있습니다.

이전 SnapCenter 서버 호스트로 롤백

문제가 발생하는 경우 API를 사용하여 모든 호스트의 SnapCenter 서버 URL을 업데이트하여 이전 SnapCenter 서버 호스트를 다시 가져올 수 있습니다. /<snapcenter_version>/server/configureurl 또는 cmdlet: *Set-SmServerConfig*.

재해 복구

독립형 SnapCenter 호스트의 재해 복구

서버 백업을 새 호스트로 복원하여 재해 복구를 수행할 수 있습니다.

시작하기 전에

이전 SnapCenter 서버의 백업이 있는지 확인하세요.

단계

1. 새로운 호스트를 배포하고 다음 작업을 수행합니다.
 - a. SnapCenter Server의 동일한 버전을 설치합니다.
 - b. CA 인증서를 구성하고 양방향 SSL을 활성화합니다. 자세한 내용은 다음을 참조하세요. "[CA 인증서 구성](#)" 그리고 "[양방향 SSL 구성 및 활성화](#)".
2. 이전 SnapCenter 서버 백업을 새 호스트로 복사합니다.
3. SnapCenter 관리자 사용자로 로그인합니다.
4. API를 사용하여 새 호스트에서 SnapCenter 서버의 백업을 복원합니다.
/<snapcenter_version>/server/restore 또는 cmdlet: *Restore-SmServerBackup*.

복원을 수행하면 기본적으로 모든 호스트의 새 SnapCenter 서버 URL이 업데이트됩니다. 업데이트를 건너뛰려면 *-SkipSMSURLInHosts* 속성을 사용하고 다음 API를 사용하여 서버 URL을 별도로 업데이트하세요.

/<snapcenter_version>/server/configureurl 또는 cmdlet: *Set-SmServerConfig*.



플러그인 호스트가 서버 호스트 이름을 확인할 수 없는 경우 각 플러그인 호스트에 로그인하여 <New IP> SC_Server_Name 형식으로 새 IP에 대한 *etc/host* 항목을 추가합니다.



서버 *etc/host* 항목은 복원되지 않습니다. 이전 서버에서 수동으로 복원할 수 있습니다.

5. URL 업데이트를 건너뛰었거나 복원 프로세스 중에 호스트가 다운된 경우 API를 사용하여 SnapCenter 에서 관리하는 모든 호스트 또는 지정된 호스트의 새 서버 이름을 업데이트합니다.

/<snapcenter_version>/server/configureurl 또는 cmdlet: *Set-SmServerConfig*.

SnapCenter F5 클러스터의 재해 복구

서버 백업을 새 호스트로 복원한 다음 독립 실행형 호스트를 클러스터로 변환하여 재해 복구를 수행할 수 있습니다.

시작하기 전에

이전 SnapCenter 서버의 백업이 있는지 확인하세요.

단계

1. 새로운 호스트를 배포하고 다음 작업을 수행합니다.
 - a. SnapCenter Server의 동일한 버전을 설치합니다.
 - b. CA 인증서를 구성하고 양방향 SSL을 활성화합니다. 자세한 내용은 다음을 참조하세요. "[CA 인증서 구성](#)" 그리고 "[양방향 SSL 구성 및 활성화](#)".
2. 이전 SnapCenter 서버 백업을 새 호스트로 복사합니다.
3. SnapCenter 관리자 사용자로 로그인합니다.
4. API를 사용하여 새 호스트에서 SnapCenter 서버의 백업을 복원합니다.

/<snapcenter_version>/server/restore 또는 cmdlet: *Restore-SmServerBackup*.

복원을 수행하면 기본적으로 모든 호스트의 새 SnapCenter 서버 URL이 업데이트됩니다. 업데이트를 건너뛰려면 *-SkipSMSURLInHosts* 속성을 사용하고 다음 API를 사용하여 서버 URL을 별도로 업데이트하세요.

/<snapcenter_version>/server/configureurl 또는 cmdlet: *Set-SmServerConfig*.



플러그인 호스트가 서버 호스트 이름을 확인할 수 없는 경우 각 플러그인 호스트에 로그인하여 <New IP> SC_Server_Name 형식으로 새 IP에 대한 *etc/host* 항목을 추가합니다.



서버 *etc/host* 항목은 복원되지 않습니다. 이전 서버에서 수동으로 복원할 수 있습니다.

5. URL 업데이트를 건너뛰었거나 복원 프로세스 중에 호스트가 다운된 경우 API를 사용하여 SnapCenter 에서 관리하는 모든 호스트 또는 지정된 호스트의 새 서버 이름을 업데이트합니다.

/<snapcenter_version>/server/configureurl 또는 cmdlet: *Set-SmServerConfig*.

6. 독립형 호스트를 F5 클러스터로 변환합니다.

F5 구성 방법에 대한 정보는 다음을 참조하세요. "[F5를 사용하여 고가용성을 위한 SnapCenter 서버 구성](#)".

관련 정보

API에 대한 정보를 보려면 Swagger 페이지에 액세스해야 합니다. "[Swagger API 웹 페이지를 사용하여 REST API에 액세스하는 방법](#)".

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

SnapCenter 플러그인 호스트의 기술 업데이트

SnapCenter 플러그인 호스트를 새로 고쳐야 하는 경우 리소스를 이전 호스트에서 새 호스트로 이동해야 합니다. 새로운 호스트가 SnapCenter에 추가되면 모든 리소스가 검색되지만 새로운 리소스로 처리됩니다.

이 작업에 관하여

이전 호스트 이름과 새 호스트 이름을 입력으로 받고, 이름으로 리소스를 비교하고, 일치하는 리소스의 객체를 이전 호스트에서 새 호스트로 다시 연결하는 API나 cmdlet을 실행해야 합니다. 일치하는 리소스는 보호됨으로 표시됩니다.

- *IsDryRun* 매개변수는 기본적으로 True로 설정되며 이는 이전 호스트와 새 호스트의 일치하는 리소스를 식별합니다.

일치하는 리소스를 확인한 후 *IsDryRun* 매개변수를 False로 설정하여 일치하는 리소스의 객체를 이전 호스트에서 새 호스트로 다시 연결해야 합니다.

- *AutoMigrateManuallyAddedResources* 매개변수는 기본적으로 True로 설정되어 있으며, 이를 통해 수동으로 추가된 리소스가 이전 호스트에서 새 호스트로 자동으로 복사됩니다.

AutoMigrateManuallyAddedResources 매개변수는 Oracle 및 SAP HANA 리소스에만 적용할 수 있습니다.

- 이전 호스트와 새 호스트의 인스턴스 이름이 다른 경우 *SQLInstanceMapping* 매개변수를 사용해야 합니다. 기본 인스턴스인 경우 인스턴스 이름으로 `_default_instance_`를 사용합니다.

다음 SnapCenter 플러그인에 대해 기술 업데이트가 지원됩니다.

- Microsoft SQL Server용 SnapCenter 플러그인
 - SQL 데이터베이스가 인스턴스 수준에서 보호되고 호스트 기술 업데이트의 일부로 일부 리소스만 새 호스트로 이동된 경우 기존 인스턴스 수준 보호는 리소스 그룹 보호로 변환되고 두 호스트의 인스턴스가 리소스 그룹에 추가됩니다.
 - SQL 호스트(예: host1)가 다른 호스트(예: host2)의 리소스에 대한 스케줄러 또는 검증 서버로 사용되는 경우, host1에서 기술 업데이트를 수행하는 동안 스케줄이나 검증 세부 정보는 마이그레이션되지 않고 host1에서 계속 실행됩니다. 수정해야 하는 경우 해당 호스트에서 수동으로 변경해야 합니다.
 - SQL FCI(Failover Cluster Instances) 설정을 사용하는 경우 FCI 클러스터에 새 노드를 추가하고 SnapCenter에서 플러그인 호스트를 새로 고쳐서 기술 업데이트를 수행할 수 있습니다.
 - SQL 가용성 그룹(AG) 설정을 사용하는 경우 기술 업데이트가 필요하지 않습니다. AG에 새로운 노드를 추가하고 SnapCenter에서 호스트를 새로 고칠 수 있습니다.
- Windows용 SnapCenter 플러그인
- Oracle 데이터베이스용 SnapCenter 플러그인

Oracle Real Application Cluster(RAC) 설정을 사용하는 경우 RAC 클러스터에 새 노드를 추가하고 SnapCenter에서 플러그인 호스트를 새로 고쳐서 기술 새로 고침을 수행할 수 있습니다.

- SAP HANA 데이터베이스용 SnapCenter 플러그인

지원되는 사용 사례는 다음과 같습니다.

- 한 호스트에서 다른 호스트로 리소스를 마이그레이션합니다.
- 여러 호스트에서 하나 이하의 호스트로 리소스를 마이그레이션합니다.
- 한 호스트에서 여러 호스트로 리소스를 마이그레이션합니다.

지원되는 시나리오는 다음과 같습니다.

- 새로운 호스트의 이름은 이전 호스트와 다릅니다.
- 기존 호스트의 이름이 변경되었습니다.

시작하기 전에

이 워크플로는 SnapCenter 저장소의 데이터를 수정하므로 SnapCenter 저장소를 백업하는 것이 좋습니다. 데이터 문제가 발생할 경우 SnapCenter 저장소를 백업을 사용하여 이전 상태로 되돌릴 수 있습니다.

자세한 내용은 다음을 참조하세요. "[SnapCenter 저장소 백업](#)".

단계

1. 새로운 호스트를 배포하고 애플리케이션을 설치합니다.
2. 이전 호스트의 일정을 중단합니다.
3. 필요한 리소스를 이전 호스트에서 새 호스트로 이동합니다.
 - a. 동일한 저장소에서 새 호스트에 필요한 데이터베이스를 불러옵니다.
 - 저장소가 이전 호스트와 동일한 드라이브 또는 동일한 마운트 경로에 매핑되었는지 확인하세요. 저장소가 올바르게 매핑되지 않으면 이전 호스트에서 생성된 백업을 복원에 사용할 수 없습니다.



기본적으로 Windows는 사용 가능한 다음 드라이브를 자동으로 할당합니다.

- 스토리지 DR이 활성화된 경우 해당 스토리지를 새 호스트에 마운트해야 합니다.
- b. 애플리케이션 버전이 변경된 경우 호환성을 확인하세요.
 - c. Oracle 플러그인 호스트의 경우에만 Oracle과 해당 그룹 사용자의 UID와 GID가 이전 호스트와 동일한지 확인하세요.

자세한 내용은 다음을 참조하세요.

- "[이전 호스트에서 새 호스트로 SQL 데이터베이스를 마이그레이션하는 방법](#)"
- "[Oracle 데이터베이스를 이전 호스트에서 새 호스트로 마이그레이션하는 방법](#)"
- "[새 호스트에 SAP HANA 데이터베이스를 가져오는 방법](#)"

4. SnapCenter 에 새로운 호스트를 추가합니다.
5. 모든 리소스가 검색되었는지 확인하세요.
6. 호스트 새로 고침 API를 실행합니다. `/<snapcenter_version>/techrefresh/host` 또는 cmdlet: `Invoke-SmTechRefreshHost`.



기본적으로 드라이런이 활성화되어 있으며, 다시 연결할 일치하는 리소스가 식별됩니다. API: `/jobs/{jobid}` 또는 cmdlet `_Get-SmJobSummaryReport_`를 실행하여 리소스를 확인할 수 있습니다.

여러 호스트에서 리소스를 마이그레이션한 경우 모든 호스트에 대해 API나 cmdlet을 실행해야 합니다. 새 호스트의 드라이브 또는 마운트 경로가 이전 호스트와 동일하지 않으면 다음 복원 작업이 실패합니다.

- SQL 내부 복원은 실패합니다. 하지만 RTAL 기능을 활용할 수 있습니다.
- Oracle 및 SAP HANA 데이터베이스 복원이 실패합니다.

여러 호스트로 마이그레이션하려면 모든 호스트에 대해 1단계부터 모든 단계를 수행해야 합니다.



동일한 호스트에서 API나 cmdlet을 여러 번 실행할 수 있으며, 새로운 리소스가 식별된 경우에만 다시 연결됩니다.

7. (선택 사항) SnapCenter 에서 이전 호스트를 제거합니다.

관련 정보

API에 대한 정보를 보려면 Swagger 페이지에 액세스해야 합니다. "[Swagger API 웹 페이지를 사용하여 REST API에 액세스하는 방법](#)".

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

저장 시스템의 기술 업데이트

스토리지 기술적으로 업데이트되면 데이터는 새로운 스토리지로 마이그레이션되고 애플리케이션 호스트는 새로운 스토리지에 마운트됩니다. SnapCenter 백업 워크플로는 새 저장소를 식별하고 새 저장소가 SnapCenter 에 등록되면 스냅샷을 만듭니다.

저장소 새로 고침 후 생성된 새 백업에 대해 복원, 마운트 및 복제를 수행할 수 있습니다. 그러나 저장소 새로 고침 전에 생성된 백업에서 이러한 작업을 수행하면 실패하게 됩니다. 백업에 이전 저장소 세부 정보가 있기 때문입니다.

SnapCenter 의 이전 백업을 새 스토리지 세부 정보로 업데이트하려면 스토리지 기술 새로 고침 API 또는 cmdlet을 실행해야 합니다.

다음 SnapCenter 플러그인에 대해 기술 업데이트가 지원됩니다.

- Microsoft SQL Server용 SnapCenter 플러그인
- Windows용 SnapCenter 플러그인
- Oracle 데이터베이스용 SnapCenter 플러그인
- SAP HANA 데이터베이스용 SnapCenter 플러그인
- Microsoft Exchange Server용 SnapCenter 플러그인

지원되는 사용 사례는 다음과 같습니다.

- 기본 저장소 새로 고침

스토리지 기술 갱신은 기본 스토리지를 새 스토리지로 교체하는 데 지원됩니다. 기존의 보조 저장소를 기본 저장소로 변환할 수 없습니다.

- 보조 저장소 새로 고침

기본 저장소의 백업을 업데이트합니다.

저장소 기술이 업데이트되면 저장소 기술 업데이트 API 또는 cmdlet을 실행하여 SnapCenter 의 이전 백업을 새 저장소 세부 정보로 업데이트해야 합니다.

시작하기 전에

이 워크플로는 SnapCenter 저장소의 데이터를 수정하므로 SnapCenter 저장소를 백업하는 것이 좋습니다. 데이터 문제가 발생할 경우 SnapCenter 저장소를 백업을 사용하여 이전 상태로 되돌릴 수 있습니다.

자세한 내용은 다음을 참조하세요. "[SnapCenter 저장소 백업](#)".

단계

1. 기존 저장소에서 새 저장소로 데이터를 마이그레이션합니다.

마이그레이션 방법에 대한 자세한 내용은 다음을 참조하세요.

- "[데이터를 새 저장소로 마이그레이션하는 방법](#)"
- "[볼륨을 복사하고 모든 스냅샷 사본을 보존하려면 어떻게 해야 하나요?](#)"

2. 호스트를 유지 관리 모드로 전환합니다.
3. 각 호스트에 새로운 스토리지를 마운트하고 데이터베이스를 불러옵니다.

새로운 저장소는 이전과 같은 방식으로 호스트에 연결되어야 합니다. 예를 들어, SAN으로 연결된 경우 SAN으로 연결해야 합니다.

새로운 저장소는 기존 저장소와 동일한 드라이브나 경로에 마운트되어야 합니다.

4. 모든 리소스가 제대로 작동하고 있는지 확인하세요.
5. SnapCenter 에 새로운 저장소를 추가합니다.

SnapCenter 의 클러스터 전체에서 고유한 SVM 이름이 있는지 확인하세요. 새 스토리지에서 동일한 SVM 이름을 사용하고 스토리지 새로 고침을 실행하기 전에 SVM의 모든 볼륨을 마이그레이션할 수 있는 경우, 이전 클러스터에서 SVM을 삭제하고 SnapCenter 에서 이전 클러스터를 다시 검색하여 캐시에서 SVM을 제거하는 것이 좋습니다.

6. 호스트를 프로덕션 모드로 전환합니다.
7. SnapCenter 에서 스토리지가 마이그레이션된 리소스의 백업을 만듭니다. SnapCenter 에서 최신 스토리지 공간을 식별하려면 새로운 백업이 필요하며, 이는 기존 백업의 메타데이터를 업데이트하는 데 사용됩니다.



새로운 LUN이 호스트에 연결될 때마다 새로운 일련 번호가 지정됩니다. Windows 파일 시스템을 검색하는 동안 SnapCenter 모든 고유한 일련 번호를 새 리소스로 처리합니다. 스토리지 기술 새로 고침 중에 새 스토리지의 LUN이 동일한 드라이브 문자 또는 경로로 호스트에 연결되면 SnapCenter 에서 Windows 파일 시스템을 검색하여 동일한 드라이브 문자 또는 경로로 마운트된 경우에도 기존 리소스를 삭제된 것으로 표시하고 새 LUN을 새 리소스로 표시합니다. 리소스가 삭제됨으로 표시되면 SnapCenter 에서 스토리지 기술 새로 고침에 고려되지 않으며 이전 리소스의 모든 백업이 손실됩니다. Windows 파일 시스템 리소스의 경우 저장소 새로 고침이 발생할 때마다 저장소 새로 고침 API 또는 cmdlet을 실행하기 전에 리소스 검색을 수행해서는 안 됩니다.

8. 저장소 새로 고침 API를 실행합니다. `/<snapcenter_version>/techrefresh/primarystorage` 또는 cmdlet: `Invoke-SmTechRefreshPrimaryStorage`.



리소스가 복제가 활성화된 정책으로 구성된 경우, 저장소 새로 고침 후의 최신 백업에는 보조 저장소에 대한 세부 정보가 포함되어야 합니다.

- a. SQL FCI(Failover Cluster Instances) 설정을 사용하는 경우 백업은 클러스터 수준에서 유지 관리됩니다. 스토리지 기술 업데이트에 대한 입력으로 클러스터 이름을 제공해야 합니다.
- b. SQL 가용성 그룹(AG) 설정을 사용하는 경우 백업은 노드 수준에서 유지 관리됩니다. 스토리지 기술 업데이트에 대한 입력으로 노드 이름을 제공해야 합니다.
- c. Oracle Real Application Clusters(RAC) 설정을 사용하는 경우 모든 노드에서 스토리지 기술 새로 고침을 수행할 수 있습니다.

`IsDryRun` 속성은 기본적으로 True로 설정됩니다. 저장소가 새로 고쳐지는 리소스를 식별합니다. API: `'<snapcenter_version>/jobs/{jobid}'` 또는 cmdlet `_Get-SmJobSummaryReport_`를 실행하여 리소스와 변경된 저장소 세부 정보를 볼 수 있습니다.

9. 저장소 세부 정보를 확인한 후 `IsDryRun` 속성을 False로 설정하고 저장소 새로 고침 API를 실행합니다. `/<snapcenter_version>/techrefresh/primarystorage` 또는 cmdlet: `Invoke-SmTechRefreshPrimaryStorage`.

이렇게 하면 이전 백업의 저장 세부 정보가 업데이트됩니다.

동일한 호스트에서 API나 cmdlet을 여러 번 실행할 수 있으며, 저장소가 새로 고쳐진 경우에만 이전 백업의 저장소 세부 정보가 업데이트됩니다.



ONTAP에서는 클론 계층을 마이그레이션할 수 없습니다. 마이그레이션되는 스토리지에 SnapCenter 에 복제 메타데이터가 있는 경우 복제된 리소스는 독립 리소스로 표시됩니다. 복제 메타데이터의 복제본은 재귀적으로 제거됩니다.

10. (선택 사항) 모든 스냅샷이 이전 기본 저장소에서 새 기본 저장소로 이동되지 않은 경우 다음 API를 실행합니다. `/<snapcenter_version>/hosts/primarybackupsexistencecheck` 또는 cmdlet `Invoke-SmPrimaryBackupsExistenceCheck`.

이렇게 하면 새로운 기본 저장소에서 스냅샷 존재 여부 검사가 수행되고 해당 백업을 SnapCenter 에서 어떤 작업에도 사용할 수 없음으로 표시합니다.

보조 저장소의 백업을 업데이트합니다.

저장소 기술이 업데이트되면 저장소 기술 업데이트 API 또는 cmdlet을 실행하여 SnapCenter 의 이전 백업을 새 저장소 세부 정보로 업데이트해야 합니다.

시작하기 전에

이 워크플로는 SnapCenter 저장소의 데이터를 수정하므로 SnapCenter 저장소를 백업하는 것이 좋습니다. 데이터 문제가 발생할 경우 SnapCenter 저장소를 백업을 사용하여 이전 상태로 되돌릴 수 있습니다.

자세한 내용은 다음을 참조하세요. "[SnapCenter 저장소 백업](#)".

단계

1. 기존 저장소에서 새 저장소로 데이터를 마이그레이션합니다.

마이그레이션 방법에 대한 자세한 내용은 다음을 참조하세요.

- "[데이터를 새 저장소로 마이그레이션하는 방법](#)"
- "[볼륨을 복사하고 모든 스냅샷 사본을 보존하려면 어떻게 해야 하나요?](#)"

2. 기본 저장소와 새로운 보조 저장소 사이에 SnapMirror 관계를 설정하고 관계 상태가 양호한지 확인합니다.
3. SnapCenter 에서 스토리지가 마이그레이션된 리소스의 백업을 만듭니다.

SnapCenter 에서 최신 스토리지 공간을 식별하려면 새로운 백업이 필요하며, 이는 기존 백업의 메타데이터를 업데이트하는 데 사용됩니다.



이 작업이 완료될 때까지 기다려야 합니다. 완료 전에 다음 단계로 진행하면 SnapCenter 이전 보조 스냅샷 메타데이터가 완전히 손실됩니다.

4. 호스트의 모든 리소스에 대한 백업을 성공적으로 생성한 후 보조 스토리지 새로 고침 API를 실행합니다.
`/<snapcenter_version>/techrefresh/secondarystorage` 또는 cmdlet: `Invoke-SmTechRefreshSecondaryStorage`.

이렇게 하면 지정된 호스트의 이전 백업에 대한 보조 저장소 세부 정보가 업데이트됩니다.

리소스 수준에서 이를 실행하려면 각 리소스에 대해 *새로 고침*을 클릭하여 보조 저장소 메타데이터를 업데이트합니다.

5. 이전 백업을 성공적으로 업데이트한 후에는 기존 보조 저장소와 기본 저장소의 관계를 끊을 수 있습니다.

SnapCenter 서버 및 플러그인 제거

SnapCenter 플러그인 패키지 제거

호스트 제거를 위한 전제 조건

SnapCenter GUI를 사용하여 호스트를 제거하고 개별 플러그인이나 플러그인 패키지를 제거할 수 있습니다. SnapCenter 서버 호스트에서 명령줄 인터페이스(CLI)를 사용하거나 모든 호스트에서 로컬로 Windows 프로그램 제거 옵션을 사용하여 원격 호스트에서 개별 플러그인이나 플러그인 패키지를 제거할 수도 있습니다.

SnapCenter 서버에서 호스트를 제거하기 전에 필수 조건을 완료해야 합니다.

- 관리자로 로그인해야 합니다.
- 호스트에서 검색 작업이 실행되고 있지 않은지 확인해야 합니다.
- 호스트와 연관된 모든 객체를 제거하려면 필요한 권한이 있는 역할이 할당되어야 합니다. 그렇지 않으면 제거 작업이 실패합니다.
- SnapCenter에 호스트를 추가한 후 SSH 키가 수정된 경우 지문을 확인해야 합니다.
- SnapCenter 호스트가 SnapCenter의 최신 버전으로 업그레이드되었지만 플러그인 호스트가 여전히 이전 버전의 플러그인을 실행 중인 경우 지문을 확인해야 합니다.

역할 기반 액세스 제어를 사용하여 호스트를 제거하기 위한 전제 조건

- 읽기, 호스트 삭제, 플러그인 설치, 제거, 개체 삭제 권한이 있는 RBAC 역할을 사용하여 로그인했어야 합니다.

객체에는 복제, 백업, 리소스 그룹, 스토리지 시스템 등이 있습니다.

- RBAC 사용자를 RBAC 역할에 추가했어야 합니다.
- 삭제하려는 호스트, 플러그인, 자격 증명, 리소스 그룹 및 스토리지 시스템(복제본의 경우)에 RBAC 사용자를 할당해야 합니다.
- SnapCenter에 RBAC 사용자로 로그인했어야 합니다.

복제 수명 주기 작업에서 생성된 복제본이 있는 호스트를 제거하기 위한 전제 조건

- SQL 데이터베이스에 대한 복제 수명 주기 관리를 사용하여 복제 작업을 생성했어야 합니다.
- 복제 읽기 및 삭제, 리소스 읽기 및 삭제, 리소스 그룹 읽기 및 삭제, 스토리지 읽기 및 삭제, 프로비저닝 읽기 및 삭제, 마운트, 마운트 해제, 플러그인 설치 및 설치 제거, 호스트 읽기 및 삭제 권한이 있는 RBAC 역할을 만들어야 합니다.
- RBAC 사용자에게 RBAC 역할을 할당했어야 합니다.
- 호스트, Microsoft SQL Server용 SnapCenter 플러그인, 자격 증명, 복제 수명 주기 리소스 그룹 및 스토리지 시스템에 RBAC 사용자를 할당했어야 합니다.
- SnapCenter에 RBAC 사용자로 로그인했어야 합니다.

SnapCenter Plug-in for VMware vSphere 제거에 대한 자세한 내용은 다음을 참조하세요. ["SnapCenter Plug-in for](#)

호스트 제거

SnapCenter 서버가 호스트를 제거할 때는 먼저 SnapCenter 리소스 페이지에 나열된 해당 호스트에 대한 백업, 복제, 복제 작업, 리소스 그룹 및 리소스를 제거한 다음 호스트에서 플러그인 패키지를 제거합니다.

이 작업에 관하여

- 호스트를 삭제하면 해당 호스트와 연결된 백업, 복제본 및 리소스 그룹도 삭제됩니다.
- 리소스 그룹을 제거하면 연관된 모든 일정도 제거됩니다.
- 호스트에 다른 호스트와 공유되는 리소스 그룹이 있고 해당 호스트를 삭제하면 해당 리소스 그룹도 삭제됩니다.
- 사용이 중단되었거나 접근할 수 없는 플러그인 호스트를 제거하려면 *Remove-SmHost* cmdlet을 사용해야 합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)"

- 호스트를 제거하는 데 필요한 시간은 백업 수와 보존 설정에 따라 달라집니다. 이는 각 컨트롤러에서 스냅샷이 삭제되고 메타데이터가 정리되기 때문입니다.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 제거할 호스트를 선택한 다음 *제거*를 클릭합니다.
4. Oracle RAC 클러스터의 경우 클러스터의 모든 호스트에서 SnapCenter software 제거하려면 *클러스터의 모든 호스트 포함*을 선택합니다.

클러스터의 노드 하나를 제거하면 모든 노드를 하나씩 제거할 수도 있습니다.

5. *확인*을 클릭합니다.



클러스터에서 호스트 플러그인을 제거했다가 다시 설치하면 클러스터 리소스가 자동으로 검색되지 않습니다. 클러스터 호스트 이름을 선택한 다음 *리소스 새로 고침*을 클릭하면 클러스터 리소스를 자동으로 검색합니다.

SnapCenter GUI를 사용하여 플러그인 제거

더 이상 개별 플러그인이나 플러그인 패키지가 필요하지 않다고 판단되면 SnapCenter 인터페이스를 사용하여 제거할 수 있습니다.

시작하기 전에

- 제거하려는 플러그인 패키지의 리소스 그룹을 제거해야 합니다.
- 제거하려는 플러그인 패키지의 리소스 그룹과 연관된 정책을 분리해야 합니다.

이 작업에 관하여

개별 플러그인을 제거할 수 있습니다. 예를 들어, 호스트의 리소스가 부족하여 Microsoft SQL Server용 SnapCenter 플러그인을 더 강력한 호스트로 옮기고 싶을 때 해당 플러그인을 제거해야 할 수 있습니다. 플러그인 패키지 전체를 제거할 수도 있습니다. 예를 들어, Oracle Database용 SnapCenter 플러그인과 UNIX용 SnapCenter 플러그인이 포함된 Linux용 SnapCenter 플러그인 패키지를 제거해야 할 수도 있습니다.

- 호스트를 제거하면 모든 플러그인도 제거됩니다.

SnapCenter 에서 호스트를 제거하면 SnapCenter 호스트를 제거하기 전에 호스트의 모든 플러그인 패키지를 제거합니다.

- SnapCenter GUI는 한 번에 하나의 호스트에서 플러그인을 제거합니다.

SnapCenter GUI를 사용하면 한 번에 하나의 호스트에서만 플러그인을 제거할 수 있습니다. 하지만 여러 개의 설치 제거 작업을 동시에 실행할 수도 있습니다.

Uninstall-SmHostPackage cmdlet과 필요한 매개변수를 사용하여 여러 호스트에서 플러그인을 제거할 수도 있습니다. cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".



SnapCenter 서버가 설치된 호스트에서 Windows용 SnapCenter 플러그인 패키지를 제거하면 SnapCenter 서버 설치가 손상됩니다. SnapCenter 서버가 더 이상 필요하지 않다고 확신하기 전까지는 Windows용 SnapCenter 플러그인 패키지를 제거하지 마세요.

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *관리되는 호스트*를 클릭합니다.
3. 관리 호스트 페이지에서 플러그인이나 플러그인 패키지를 제거할 호스트를 선택합니다.
4. 제거하려는 플러그인 옆의 제거 > *제출*을 클릭합니다.

당신이 완료한 후

해당 호스트에 플러그인을 다시 설치하기 전에 5분 정도 기다려야 합니다. 이 기간은 SnapCenter GUI가 관리 호스트의 상태를 새로 고치는 데 충분합니다. 플러그인을 바로 다시 설치하면 설치에 실패합니다.

Linux용 SnapCenter 플러그인 패키지를 제거하는 경우, 제거 관련 로그 파일은 `_/custom_location/snapcenter/log_`에서 사용할 수 있습니다.

PowerShell cmdlet을 사용하여 Windows 플러그인 제거

SnapCenter 서버 호스트 명령줄 인터페이스에서 *Uninstall-SmHostPackage* cmdlet을 사용하여 하나 이상의 호스트에서 개별 플러그인을 제거하거나 플러그인 패키지를 제거할 수 있습니다.

플러그인을 제거하려는 각 호스트에서 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter 에 로그인해야 합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 `Open-SMConnection -SMSbaseUri https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME` 명령을 입력한 다음 자격 증명을 입력합니다.

3. `Uninstall-SmHostPackage` cmdlet과 필요한 매개변수를 사용하여 Windows 플러그인을 제거합니다.

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 `_Get-Help command_name_`을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

호스트에서 로컬로 플러그인 제거

SnapCenter 서버에서 호스트에 접속할 수 없는 경우 호스트에서 로컬로 SnapCenter 플러그인을 제거할 수 있습니다.

이 작업에 관하여

개별 플러그인이나 플러그인 패키지를 제거하는 가장 좋은 방법은 SnapCenter GUI를 사용하거나 SnapCenter 서버 호스트 명령줄 인터페이스에서 `Uninstall-SmHostPackage` cmdlet을 사용하는 것입니다. 이러한 절차는 SnapCenter 서버가 모든 변경 사항에 맞게 최신 상태를 유지하는 데 도움이 됩니다.

하지만 드물게는 로컬에서 플러그인을 제거해야 할 수도 있습니다. 예를 들어, SnapCenter 서버에서 제거 작업을 실행했지만 작업이 실패했거나 SnapCenter 서버를 제거했는데 고아 플러그인이 호스트에 남아 있을 수 있습니다.



호스트에서 로컬로 플러그인 패키지를 제거해도 호스트와 관련된 데이터(예: 예약된 작업 및 백업 메타데이터)는 삭제되지 않습니다.



제어판에서 Windows용 SnapCenter 플러그인 패키지를 로컬로 제거하려고 시도하지 마세요. SnapCenter GUI를 사용하여 Microsoft Windows용 SnapCenter 플러그인이 제대로 제거되었는지 확인해야 합니다.

단계

1. 호스트 시스템에서 제어판으로 이동하여 *프로그램 제거*를 클릭합니다.
2. 프로그램 목록에서 제거하려는 SnapCenter 플러그인이나 플러그인 패키지를 선택하고 *제거*를 클릭합니다.

Windows는 선택한 패키지의 모든 플러그인을 제거합니다.

CLI를 사용하여 Linux 또는 AIX용 플러그인 패키지 제거

명령줄 인터페이스를 사용하여 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 제거할 수 있습니다.

시작하기 전에

- 예약된 작업을 삭제했는지 확인하세요.
- 실행 중인 모든 작업이 완료되었는지 확인하세요.

단계

제거하려면 `_/custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall_`을 실행하세요.

Windows 호스트에서 SnapCenter 서버 제거

더 이상 SnapCenter Server를 사용하여 데이터 보호 작업을 관리하지 않으려면 SnapCenter

Server 호스트의 프로그램 및 기능 제어판을 사용하여 SnapCenter Server를 제거할 수 있습니다. SnapCenter 서버를 제거하면 모든 구성 요소가 제거됩니다.

시작하기 전에

- SnapCenter 서버가 설치된 드라이브에 최소 2GB의 여유 공간이 있는지 확인하세요.
- SnapCenter 서버가 설치된 도메인이 제거되지 않았는지 확인하세요.

SnapCenter 서버가 설치된 도메인을 제거한 다음 제거를 시도하면 작업이 실패합니다.

- 저장소 데이터베이스는 정리되고 설치 제거되므로 저장소 데이터베이스를 백업했어야 합니다.

단계

1. SnapCenter 서버 호스트에서 제어판으로 이동합니다.
2. 카테고리 보기에 있는지 확인하세요.
3. 프로그램에서 *프로그램 제거*를 클릭합니다.

프로그램 및 기능 창이 열립니다.

4. NetApp SnapCenter Server를 선택한 다음 *제거*를 클릭합니다.

SnapCenter 4.2부터 SnapCenter 서버를 제거하면 MySQL 서버 저장소 데이터베이스를 포함한 모든 구성 요소가 제거됩니다.

- NLB 클러스터에서 NLB 노드를 제거하려면 SnapCenter 서버 호스트를 다시 시작해야 합니다. 호스트를 재시작하지 않으면 SnapCenter 서버를 다시 설치하려고 할 때 오류가 발생할 수 있습니다.
- 설치 제거 중에 제거되지 않은 .NET Framework는 수동으로 제거해야 합니다.

Linux 호스트에서 SnapCenter 서버 제거

더 이상 SnapCenter 서버를 사용하여 데이터 보호 작업을 관리하지 않으려면 SnapCenter 서버를 제거할 수 있습니다. SnapCenter 서버를 제거하면 모든 구성 요소가 제거됩니다.

단계

1. SnapCenter Server를 제거하려면 다음 작업 중 하나를 수행하세요.

공연을 하고 싶다면...	이렇게 하세요...
비대화형 설치 제거	<pre>\$ sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall -i silent -DCONFIRM=1</pre> 예: sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall

공연을 하고 싶다면...	이렇게 하세요...
대화형 제거	<pre data-bbox="842 159 1484 264">\$ sudo <USER_INSTALL_DIR>/NetApp/snapcenter/S napManagerWeb/installation/uninstall</pre> 제거를 확인하려면 확인 입력란에 0이 아닌 다른 값을 입력하세요.

REST API를 사용하여 자동화

REST API를 사용한 SnapCenter 자동화

REST API를 사용하여 다양한 SnapCenter 관리 작업을 수행할 수 있습니다. REST API는 Swagger 웹 페이지를 통해 공개됩니다. REST API 문서를 표시하고 수동으로 API 호출을 실행하려면

`_https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/_`에서 제공되는 Swagger 웹 페이지에 액세스할 수 있습니다.

REST API를 지원하는 플러그인은 다음과 같습니다.

- Microsoft SQL Server용 플러그인
- SAP HANA 데이터베이스용 플러그인
- Oracle 데이터베이스용 플러그인

SnapCenter Plug-in for VMware vSphere에 대한 정보는 다음을 참조하세요. "[SnapCenter Plug-in for VMware vSphere](#)"

SnapCenter REST API에 기본적으로 액세스하는 방법

REST 클라이언트를 지원하는 모든 프로그래밍 언어를 사용하여 SnapCenter REST API에 직접 액세스할 수 있습니다. 인기 있는 언어로는 Python, PowerShell, Java 등이 있습니다.

REST 웹 서비스 기반

REST(Representational State Transfer)는 분산 웹 애플리케이션을 구축하는 스타일입니다. 웹 서비스 API 설계에 적용되면 서버 기반 리소스를 노출하고 상태를 관리하는 데 필요한 기술과 모범 사례를 확립합니다. SnapCenter 관리하기 위한 유연한 기반을 제공하기 위해 주류 프로토콜과 표준을 사용합니다.

자원과 국가 대표

리소스는 웹 기반 시스템의 기본 구성 요소입니다. REST 웹 서비스 애플리케이션을 구축할 때 초기 설계 작업은 다음과 같습니다.

시스템 또는 서버 기반 리소스 식별

모든 시스템은 리소스를 사용하고 유지관리합니다. 리소스는 파일, 비즈니스 트랜잭션, 프로세스 또는 관리 개체일 수 있습니다. REST 웹 서비스 기반 애플리케이션을 설계할 때 가장 먼저 해야 할 작업 중 하나는 리소스를 식별하는 것입니다.

리소스 상태 및 관련 상태 작업의 정의

자원은 항상 유한한 수의 상태 중 하나에 머물러 있습니다. 상태와 상태 변경에 영향을 미치는 관련 작업은 명확하게

정의되어야 합니다.

URI 엔드포인트

모든 REST 리소스는 명확하게 정의된 주소 지정 체계를 사용하여 정의하고 제공해야 합니다. 리소스가 위치하고 식별되는 엔드포인트는 URI(Uniform Resource Identifier)를 사용합니다.

URI는 네트워크의 각 리소스에 고유한 이름을 생성하는 일반적인 프레임워크를 제공합니다. URL(Uniform Resource Locator)은 웹 서비스에서 리소스를 식별하고 액세스하는 데 사용되는 URI 유형입니다. 리소스는 일반적으로 파일 디렉터리와 유사한 계층 구조로 노출됩니다.

HTTP 메시지

HTTP(Hypertext Transfer Protocol)는 웹 서비스 클라이언트와 서버가 리소스에 대한 요청 및 응답 메시지를 교환하는 데 사용하는 프로토콜입니다.

웹 서비스 애플리케이션을 설계하는 과정에서 HTTP 메서드는 리소스와 해당 상태 관리 작업에 매핑됩니다. HTTP는 상태를 저장하지 않습니다. 따라서 관련된 요청과 응답 세트를 하나의 트랜잭션의 일부로 연관시키려면 요청 및 응답 데이터 흐름과 함께 전달되는 HTTP 헤더에 추가 정보를 포함해야 합니다.

JSON 포매팅

웹 서비스 클라이언트와 서버 간에 정보를 구성하고 전송하는 방법은 여러 가지가 있지만, 가장 인기 있는 옵션은 JSON(JavaScript Object Notation)입니다.

JSON은 간단한 데이터 구조를 일반 텍스트로 표현하는 업계 표준이며, 리소스를 설명하는 상태 정보를 전송하는 데 사용됩니다. SnapCenter REST API는 JSON을 사용하여 각 HTTP 요청 및 응답 본문에 포함된 데이터를 형식화합니다.

기본 작동 특성

REST는 공통된 기술과 모범 사례를 제공하지만, 각 API의 세부 사항은 설계 방식에 따라 달라질 수 있습니다.

요청 및 응답 API 트랜잭션

모든 REST API 호출은 SnapCenter 서버 시스템에 대한 HTTP 요청으로 수행되며, 이를 통해 클라이언트에 대한 관련 응답이 생성됩니다. 이 요청과 응답 쌍은 API 트랜잭션으로 간주됩니다.

API를 사용하기 전에 요청을 제어하는 데 사용할 수 있는 입력 변수와 응답 출력의 내용을 잘 알고 있어야 합니다.

CRUD 작업 지원

SnapCenter REST API를 통해 사용 가능한 각 리소스는 CRUD 모델을 기반으로 액세스됩니다.

- 만들다
- 읽다
- 업데이트

- 삭제

일부 리소스의 경우 작업의 하위 집합만 지원됩니다.

객체 식별자

각 리소스 인스턴스 또는 객체는 생성될 때 고유 식별자가 할당됩니다. 대부분의 경우 식별자는 128비트 UUID입니다. 이러한 식별자는 특정 SnapCenter 서버 내에서 전역적으로 고유합니다.

새로운 객체 인스턴스를 생성하는 API 호출을 발행한 후, 연관된 ID가 있는 URL이 HTTP 응답의 위치 헤더에 포함되어 호출자에게 반환됩니다. 식별자를 추출하여 리소스 인스턴스를 참조할 때 후속 호출에서 사용할 수 있습니다.



객체 식별자의 내용과 내부 구조는 언제든지 변경될 수 있습니다. 연관된 객체를 참조할 때 해당 API 호출에서 필요에 따라서는 식별자를 사용해야 합니다.

객체 인스턴스 및 컬렉션

리소스 경로와 HTTP 메서드에 따라 API 호출은 특정 개체 인스턴스나 개체 컬렉션에 적용될 수 있습니다.

동기 및 비동기 작업

SnapCenter 클라이언트로부터 수신한 HTTP 요청을 동기적 또는 비동기적으로 수행합니다.

동기 처리

SnapCenter 요청을 즉시 수행하고 성공하면 HTTP 상태 코드 200 또는 201로 응답합니다.

GET 메서드를 사용하는 모든 요청은 항상 동기적으로 수행됩니다. 또한 POST를 사용하는 요청은 2초 이내에 완료될 것으로 예상되는 경우 동기적으로 실행되도록 설계되었습니다.

비동기 처리

비동기 요청이 유효한 경우 SnapCenter 요청을 처리하기 위한 백그라운드 작업과 작업을 고정하기 위한 작업 객체를 생성합니다. HTTP 상태 코드 202는 작업 객체와 함께 호출자에게 반환됩니다. 성공 또는 실패를 확인하려면 작업 상태를 검색해야 합니다.

POST 및 DELETE 메서드를 사용하는 요청은 완료하는 데 2초 이상 걸릴 것으로 예상되는 경우 비동기적으로 실행되도록 설계되었습니다.

보안

REST API가 제공하는 보안은 주로 SnapCenter 에서 제공하는 기존 보안 기능을 기반으로 합니다. API에서는 다음과 같은 보안을 사용합니다.

전송 계층 보안

SnapCenter 서버와 클라이언트 간 네트워크를 통해 전송되는 모든 트래픽은 일반적으로 SnapCenter 구성 설정에 따라 TLS를 사용하여 암호화됩니다.

HTTP 인증

HTTP 수준에서는 API 트랜잭션에 기본 인증이 사용됩니다. 사용자 이름과 비밀번호를 base64 문자열로 담은 HTTP 헤더가 각 요청에 추가됩니다.

API 요청을 제어하는 입력 변수

HTTP 요청에 설정된 매개변수와 변수를 통해 API 호출이 처리되는 방식을 제어할 수 있습니다.

HTTP 메서드

SnapCenter REST API에서 지원하는 HTTP 메서드는 다음 표에 나와 있습니다.



각 REST 엔드포인트에서 모든 HTTP 메서드를 사용할 수 있는 것은 아닙니다.

HTTP 메서드	설명
얻다	리소스 인스턴스 또는 컬렉션에서 개체 속성을 검색합니다.
우편	제공된 입력을 기반으로 새로운 리소스 인스턴스를 생성합니다.
삭제	기존 리소스 인스턴스를 삭제합니다.
놓다	기존 리소스 인스턴스를 수정합니다.

요청 헤더

HTTP 요청에는 여러 개의 헤더를 포함해야 합니다.

콘텐츠 유형

요청 본문에 JSON이 포함되어 있는 경우 이 헤더를 `_application/json_`으로 설정해야 합니다.

수용하다

이 헤더는 `_application/json_`으로 설정되어야 합니다.

권한 부여

기본 인증은 사용자 이름과 비밀번호를 base64 문자열로 인코딩하여 설정해야 합니다.

요청 본문

요청 본문의 내용은 특정 호출에 따라 다릅니다. HTTP 요청 본문은 다음 중 하나로 구성됩니다.

- 입력 변수가 있는 JSON 객체
- 비어 있는

객체 필터링

GET을 사용하는 API 호출을 실행할 때 반환되는 객체를 속성에 따라 제한하거나 필터링할 수 있습니다. 예를 들어, 일치시킬 정확한 값을 지정할 수 있습니다.

<field>=<query value>

정확한 일치 외에도 다양한 연산자를 사용하여 값 범위에 대한 객체 집합을 반환할 수 있습니다. SnapCenter REST API는 아래 표에 표시된 필터링 연산자를 지원합니다.

연산자	설명
=	동일하다
<	미만
>	보다 크다
←	이하
>=	이상 또는 같음
업데이트	또는
!	같지 않다
*	탐욕스러운 와일드카드

null 키워드나 부정 ***!null***을 쿼리의 일부로 사용하면 특정 필드가 설정되었는지 여부에 따라 개체 컬렉션을 반환할 수도 있습니다.



설정되지 않은 필드는 일반적으로 일치하는 쿼리에서 제외됩니다.

특정 객체 필드 요청

기본적으로 GET을 사용하여 API 호출을 실행하면 객체를 고유하게 식별하는 속성만 반환됩니다. 이 최소 필드 집합은 각 객체의 키 역할을 하며 객체 유형에 따라 달라집니다. 다음을 사용하여 추가 개체 속성을 선택할 수 있습니다. **fields** 다음과 같은 방법으로 쿼리 매개변수를 사용합니다.

공통 또는 표준 필드

가장 일반적으로 사용되는 객체 필드를 검색하려면 **fields=***를 지정합니다. 이러한 필드는 일반적으로 로컬 서버 메모리에 유지되거나 액세스하는 데 거의 처리가 필요하지 않습니다. 이는 URL 경로 키(UUID)와 함께 GET을 사용한 후 객체에 대해 반환되는 속성과 동일합니다.

모든 분야

fields=**를 지정하면 추가 서버 처리가 필요한 필드를 포함하여 모든 개체 필드를 검색합니다.

사용자 정의 필드 선택

원하는 정확한 필드를 지정하려면 ***fields=<field_name>***을 사용하세요. 여러 필드를 요청할 경우, 공백 없이 쉼표로 값을 구분해야 합니다.



의 필요할 때만 공통 필드 세트나 모든 필드를 검색해야 합니다. 어떤 필드가 공통으로 분류되고 `_fields=*`를 사용하여 반환되는지는 NetApp 에서 내부 성능 분석을 기반으로 결정합니다. 필드 분류는 향후 릴리스에서 변경될 수 있습니다.

출력 세트에서 객체 정렬

리소스 컬렉션의 레코드는 객체에 정의된 기본 순서대로 반환됩니다. 다음을 사용하여 순서를 변경할 수 있습니다. `order_by` 필드 이름과 정렬 방향을 포함하는 쿼리 매개변수는 다음과 같습니다.

```
order_by=<field name> asc|desc
```

예를 들어, 유형 필드를 내림차순으로 정렬한 다음 ID를 오름차순으로 정렬할 수 있습니다.

```
order_by=type desc, id asc
```

- 정렬 필드를 지정했지만 방향을 제공하지 않으면 값이 오름차순으로 정렬됩니다.
- 여러 개의 매개변수를 포함하는 경우 필드를 쉼표로 구분해야 합니다.

컬렉션에서 객체를 검색할 때의 페이지 매김

GET을 사용하여 동일한 유형의 객체 컬렉션에 액세스하기 위한 API 호출을 발행할 때 SnapCenter 두 가지 제약 조건에 따라 가능한 한 많은 객체를 반환하려고 시도합니다. 요청에 대한 추가 쿼리 매개변수를 사용하여 이러한 각 제약 조건을 제어할 수 있습니다. 특정 GET 요청에 대해 도달한 첫 번째 제약 조건은 요청을 종료하고 따라서 반환되는 레코드 수를 제한합니다.



모든 객체를 반복하기 전에 요청이 종료되면 응답에는 다음 레코드 배치를 검색하는 데 필요한 링크가 포함됩니다.

객체 수 제한

기본적으로 SnapCenter GET 요청에 대해 최대 10,000개의 객체를 반환합니다. `max_records` 쿼리 매개변수를 사용하여 이 제한을 변경할 수 있습니다. 예를 들어:

```
max_records=20
```

실제로 반환되는 객체의 수는 관련 시간 제약과 시스템의 총 객체 수에 따라 적용되는 최대값보다 적을 수 있습니다.

객체를 검색하는 데 사용되는 시간 제한

기본적으로 SnapCenter GET 요청에 허용된 시간 내에 가능한 한 많은 객체를 반환합니다. 기본 제한 시간은 15초입니다. `return_timeout` 쿼리 매개변수를 사용하여 이 제한을 변경할 수 있습니다. 예를 들어:

```
return_timeout=5
```

실제로 반환되는 객체의 수는 시스템의 객체 수와 관련된 제약 조건 및 객체 총 수에 따라 적용되는 최대값보다 적을 수 있습니다.

결과 집합 줄이기

필요한 경우 이 두 매개변수를 추가 쿼리 매개변수와 결합하여 결과 집합을 줄일 수 있습니다. 예를 들어, 다음은 지정된

시간 이후에 생성된 최대 10개의 EMS 이벤트를 반환합니다.

time⇒ 2018-04-04T15:41:29.140265Z&max_records=10

여러 개의 요청을 발행하여 객체를 탐색할 수 있습니다. 이후의 각 API 호출은 마지막 결과 집합의 최신 이벤트를 기반으로 새로운 시간 값을 사용해야 합니다.

크기 속성

일부 API 호출과 특정 쿼리 매개변수에 사용되는 입력 값은 숫자형입니다. 바이트 단위의 정수를 제공하는 대신 다음 표에 표시된 것처럼 접미사를 사용할 수도 있습니다.

접미사	설명
KB	KB 킬로바이트(1024바이트) 또는 키비바이트
엠비	MB 메가바이트(KB x 1024바이트) 또는 메비바이트
영국	GB 기가바이트(MB x 1024바이트) 또는 기비바이트
결핵	TB 테라바이트(GB x 1024바이트) 또는 테비바이트
피비	PB 페타바이트(TB x 1024바이트) 또는 페비바이트

API 응답 해석

각 API 요청은 클라이언트에게 응답을 생성합니다. 응답을 검토하여 성공했는지 확인하고 필요에 따라 추가 데이터를 검색해야 합니다.

HTTP 상태 코드

SnapCenter REST API에서 사용하는 HTTP 상태 코드는 아래와 같습니다.

암호	설명
200	OK 새로운 객체를 생성하지 않는 호출의 경우 성공을 나타냅니다.
201	생성된 객체가 성공적으로 생성되었습니다. 응답의 위치 헤더에는 객체의 고유 식별자가 포함됩니다.
202	수락된 요청을 수행하기 위한 백그라운드 작업이 시작되었지만 아직 완료되지 않았습니다.
400	잘못된 요청 요청 입력이 인식되지 않거나 부적절합니다.
401	권한이 없는 사용자 인증에 실패했습니다.
403	권한 부여(RBAC) 오류로 인해 금지된 액세스가 거부되었습니다.
404	찾을 수 없음 요청에서 언급한 리소스가 존재하지 않습니다.
405	허용되지 않는 메서드 요청의 HTTP 메서드는 해당 리소스에 대해 지원되지 않습니다.

암호	설명
409	충돌 객체를 생성하려는 시도는 다른 객체를 먼저 생성해야 하거나 요청된 객체가 이미 존재하기 때문에 실패했습니다.
500	내부 오류 서버에서 일반적인 내부 오류가 발생했습니다.

응답 헤더

SnapCenter 에서 생성된 HTTP 응답에는 여러 개의 헤더가 포함됩니다.

위치

객체가 생성되면 위치 헤더에는 객체에 할당된 고유 식별자를 포함하여 새 객체의 전체 URL이 포함됩니다.

콘텐츠 유형

이것은 일반적으로 다음과 같습니다. `application/json`.

대응 기관

API 요청으로 인해 생성되는 응답 본문의 내용은 객체, 처리 유형, 요청의 성공 또는 실패 여부에 따라 달라집니다. 응답은 항상 JSON으로 렌더링됩니다.

단일 객체

요청에 따라 필드 집합이 포함된 단일 객체가 반환될 수 있습니다. 예를 들어, GET을 사용하면 고유 식별자를 사용하여 클러스터의 선택된 속성을 검색할 수 있습니다.

여러 개체

리소스 컬렉션에서 여러 개의 개체가 반환될 수 있습니다. 모든 경우에 일관된 형식이 사용됩니다. `num_records` 레코드 수와 객체 인스턴스 배열을 포함하는 레코드 수를 나타냅니다. 예를 들어, 특정 클러스터에 정의된 노드를 검색할 수 있습니다.

Job 객체

API 호출이 비동기적으로 처리되는 경우 백그라운드 작업을 고정하는 Job 객체가 반환됩니다. 예를 들어, 클러스터 구성을 업데이트하는 데 사용되는 PATCH 요청은 비동기적으로 처리되고 Job 객체를 반환합니다.

오류 객체

오류가 발생하면 항상 Error 객체가 반환됩니다. 예를 들어, 클러스터에 대해 정의되지 않은 필드를 변경하려고 하면 오류가 발생합니다.

비어 있는

어떤 경우에는 데이터가 반환되지 않고 응답 본문에 빈 JSON 개체가 포함됩니다.

오류

오류가 발생하면 응답 본문에 오류 객체가 반환됩니다.

체재

오류 객체의 형식은 다음과 같습니다.

```
"error": {  
  "message": "<string>",  
  "code": <integer>[,  
  "target": "<string>"]  
}
```

코드 값을 사용하여 일반적인 오류 유형이나 범주를 파악하고, 메시지를 사용하여 특정 오류를 파악할 수 있습니다. 가능한 경우 대상 필드에는 오류와 관련된 특정 사용자 입력이 포함됩니다.

일반적인 오류 코드

일반적인 오류 코드는 다음 표에 설명되어 있습니다. 특정 API 호출에는 추가 오류 코드가 포함될 수 있습니다.

암호	설명
409	동일한 식별자를 가진 객체가 이미 존재합니다.
400	필드 값에 잘못된 값이 있거나 값이 누락되었거나 추가 필드가 제공되었습니다.
400	해당 작업은 지원되지 않습니다.
405	지정된 식별자를 가진 객체를 찾을 수 없습니다.
403	요청을 수행할 수 있는 권한이 거부되었습니다.
409	리소스가 사용 중입니다.

SnapCenter 서버 및 플러그인에 지원되는 REST API

SnapCenter REST API를 통해 사용할 수 있는 리소스는 SnapCenter API 문서 페이지에 표시된 대로 범주별로 정리되어 있습니다. 아래에는 기본 리소스 경로를 포함한 각 리소스에 대한 간략한 설명이 나와 있으며, 필요한 경우 추가 사용 고려 사항도 나와 있습니다.

인증

이 API를 사용하여 SnapCenter 서버에 로그인할 수 있습니다. 이 API는 후속 요청을 인증하는 데 사용되는 사용자 인증 토큰을 반환합니다.

도메인

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- SnapCenter 의 모든 도메인을 검색합니다
- 특정 도메인의 세부 정보 검색
- 도메인 등록 또는 등록 취소
- 도메인 수정

일자리

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- SnapCenter 에서 모든 작업 검색
- 작업 상태 검색
- 작업을 취소하거나 중지하다

설정

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 자격 증명을 등록, 수정 또는 제거합니다.
- SnapCenter 서버에 등록된 자격 증명 정보를 표시합니다.
- 알림 설정 구성
- 현재 이메일 알림을 보내도록 구성된 SMTP 서버에 대한 정보를 검색하고 SMTP 서버 이름, 수신자 이름, 발신자 이름을 표시합니다.
- SnapCenter 서버 로그인에 다중 인증 요소(MFA) 구성을 표시합니다.
- SnapCenter 서버 로그인에 대한 MFA를 활성화하거나 비활성화하고 구성합니다.
- MFA 설정에 필요한 구성 파일을 만듭니다.

호스트

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 모든 SnapCenter 호스트 쿼리
- SnapCenter 에서 하나 이상의 호스트 제거
- 이름으로 호스트 검색
- 호스트의 모든 리소스 검색
- 리소스 ID를 사용하여 리소스를 검색합니다.
- 플러그인 구성 세부 정보 검색
- 플러그인 호스트 구성
- Microsoft SQL Server 호스트용 플러그인의 모든 리소스를 검색합니다.
- Oracle 데이터베이스 호스트용 플러그인의 모든 리소스를 검색합니다.
- 사용자 정의 애플리케이션 호스트에 대한 플러그인의 모든 리소스를 검색합니다.

- SAP HANA 호스트용 플러그인의 모든 리소스를 검색합니다.
- 설치된 플러그인을 검색합니다
- 기존 호스트에 플러그인 설치
- 호스트 패키지 업그레이드
- 기존 호스트에서 플러그인 제거
- 호스트에 플러그인 추가
- 호스트 추가 또는 수정
- Linux 호스트의 서명을 가져옵니다
- Linux 호스트의 서명을 등록합니다
- 호스트를 유지 관리 또는 프로덕션 모드로 전환
- 호스트에서 플러그인 서비스를 시작하거나 다시 시작합니다.
- 호스트 이름 바꾸기

리소스

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 모든 리소스 검색
- 리소스 ID를 사용하여 리소스를 검색합니다.
- Microsoft SQL Server 호스트용 플러그인의 모든 리소스를 검색합니다.
- Oracle 데이터베이스 호스트용 플러그인의 모든 리소스를 검색합니다.
- 사용자 정의 애플리케이션 호스트에 대한 플러그인의 모든 리소스를 검색합니다.
- SAP HANA 호스트용 플러그인의 모든 리소스를 검색합니다.
- 키를 사용하여 Microsoft SQL Server 리소스 검색
- 키를 사용하여 사용자 정의 리소스 검색
- 사용자 정의 애플리케이션 호스트에 대한 플러그인 리소스 수정
- 키를 사용하여 사용자 정의 애플리케이션 호스트의 플러그인 리소스를 제거합니다.
- 키를 사용하여 SAP HANA 리소스 검색
- SAP HANA 호스트용 플러그인 리소스 수정
- 키를 사용하여 SAP HANA 호스트용 플러그인 리소스 제거
- 키를 사용하여 Oracle 리소스 검색
- Oracle 애플리케이션 볼륨 리소스 생성
- Oracle 애플리케이션 볼륨 리소스 수정
- 키를 사용하여 Oracle 애플리케이션 볼륨 리소스 제거
- Oracle 리소스의 보조 세부 정보를 검색합니다.
- Microsoft SQL Server용 플러그인을 사용하여 Microsoft SQL Server 리소스 백업

- Oracle 데이터베이스용 플러그인을 사용하여 Oracle 리소스 백업
- 사용자 정의 애플리케이션용 플러그인을 사용하여 사용자 정의 리소스 백업
- SAP HANA 데이터베이스 구성
- Oracle 데이터베이스 구성
- SQL 데이터베이스 백업 복원
- Oracle 데이터베이스 백업 복원
- 사용자 정의 애플리케이션 백업 복원
- SAP HANA 리소스 생성
- 사용자 정의 애플리케이션용 플러그인을 사용하여 사용자 정의 리소스 보호
- Microsoft SQL Server용 플러그인을 사용하여 Microsoft SQL Server 리소스 보호
- 보호된 Microsoft SQL Server 리소스 수정
- Microsoft SQL Server 리소스에 대한 보호 제거
- Oracle 데이터베이스용 플러그인을 사용하여 Oracle 리소스 보호
- 보호된 Oracle 리소스 수정
- Oracle 리소스에서 보호 제거
- 사용자 정의 애플리케이션용 플러그인을 사용하여 백업에서 리소스 복제
- Oracle 데이터베이스용 플러그인을 사용하여 백업에서 Oracle 애플리케이션 볼륨 복제
- Microsoft SQL Server용 플러그인을 사용하여 백업에서 Microsoft SQL Server 리소스를 복제합니다.
- Microsoft SQL Server 리소스의 복제 수명 주기를 만듭니다.
- Microsoft SQL Server 리소스의 복제 수명 주기 수정
- Microsoft SQL Server 리소스의 복제 수명 주기 삭제
- 기존 Microsoft SQL Server 데이터베이스를 로컬 디스크에서 NetApp LUN으로 이동합니다.
- Oracle 데이터베이스에 대한 복제 사양 파일 생성
- Oracle 리소스의 주문형 복제 새로 고침 작업 시작
- 복제 사양 파일을 사용하여 백업에서 Oracle 리소스를 만듭니다.
- 데이터베이스를 보조 복제본으로 복원하고 데이터베이스를 가용성 그룹에 다시 조인합니다.
- Oracle 애플리케이션 볼륨 리소스 생성

백업

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 백업 이름, 유형, 플러그인, 리소스 또는 날짜별로 백업 세부 정보 검색
- 모든 백업 검색
- 백업 세부 정보 검색
- 백업 이름 바꾸기 또는 삭제

- Oracle 백업 마운트
- Oracle 백업 마운트 해제
- Oracle 백업 카탈로그화
- Oracle 백업 카탈로그 해제
- 특정 시점 복구를 수행하기 위해 마운트해야 하는 모든 백업을 가져옵니다.

클론

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- Oracle 데이터베이스 복제 사양 파일을 생성, 표시, 수정 및 삭제합니다.
- Oracle 데이터베이스 복제 계층 표시
- 클론 세부 정보 검색
- 모든 클론을 검색합니다
- 클론 삭제
- ID로 클론 세부 정보 검색
- Oracle 리소스의 주문형 복제 새로 고침 작업 시작
- 복제 사양 파일을 사용하여 백업에서 Oracle 리소스를 복제합니다.

클론 분할

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 복제된 리소스의 복제 분할 작업을 추정합니다.
- 복제 분할 작업의 상태를 검색합니다.
- 클론 분할 작업 시작 또는 중지

리소스 그룹

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 모든 리소스 그룹의 세부 정보 검색
- 이름으로 리소스 그룹을 검색합니다.
- 사용자 정의 애플리케이션용 플러그인에 대한 리소스 그룹을 생성합니다.
- Microsoft SQL Server용 플러그인에 대한 리소스 그룹을 만듭니다.
- Oracle 데이터베이스 플러그인에 대한 리소스 그룹 생성
- 사용자 정의 애플리케이션용 플러그인에 대한 리소스 그룹 수정
- Microsoft SQL Server용 플러그인에 대한 리소스 그룹 수정
- Oracle 데이터베이스 플러그인에 대한 리소스 그룹 수정
- Microsoft SQL Server용 플러그인 리소스 그룹의 복제 수명 주기를 생성, 수정 또는 삭제합니다.

- 리소스 그룹 백업
- 리소스 그룹을 유지 관리 또는 프로덕션 모드로 전환
- 리소스 그룹 제거

정책

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 정책 세부 정보 검색
- 이름으로 정책 세부 정보 검색
- 정책 삭제
- 기존 정책의 사본을 만듭니다
- 사용자 정의 애플리케이션용 플러그인에 대한 정책을 생성하거나 수정합니다.
- Microsoft SQL Server용 플러그인에 대한 정책을 만들거나 수정합니다.
- Oracle 데이터베이스용 플러그인에 대한 정책을 생성하거나 수정합니다.
- SAP HANA 데이터베이스용 플러그인에 대한 정책을 생성하거나 수정합니다.

스토리지

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 모든 주식을 검색합니다
- 이름으로 공유 검색
- 공유 만들기 또는 삭제
- 저장 세부 정보 검색
- 이름으로 저장소 세부 정보 검색
- 저장소 생성, 수정 또는 삭제
- 스토리지 클러스터에서 리소스 검색
- 스토리지 클러스터에서 리소스 검색

공유하다

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 공유 세부 정보를 검색합니다
- 모든 주식의 세부 정보를 검색합니다
- 저장소에서 공유를 생성하거나 삭제합니다.
- 이름으로 공유 검색

플러그인

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 호스트의 모든 플러그인을 나열합니다
- 키를 사용하여 Microsoft SQL Server 리소스 검색
- 키를 사용하여 사용자 정의 리소스 수정
- 키를 사용하여 사용자 정의 리소스 제거
- 키를 사용하여 SAP HANA 리소스 검색
- 키를 사용하여 SAP HANA 리소스 수정
- 키를 사용하여 SAP HANA 리소스 제거
- 키를 사용하여 Oracle 리소스 검색
- 키를 사용하여 Oracle 애플리케이션 볼륨 리소스 수정
- 키를 사용하여 Oracle 애플리케이션 볼륨 리소스 제거
- Microsoft SQL Server용 플러그인과 키를 사용하여 Microsoft SQL Server 리소스를 백업합니다.
- Oracle 데이터베이스용 플러그인과 키를 사용하여 Oracle 리소스를 백업합니다.
- 사용자 정의 애플리케이션용 플러그인과 키를 사용하여 사용자 정의 애플리케이션 리소스를 백업합니다.
- 키를 사용하여 SAP HANA 데이터베이스 구성
- 키를 사용하여 Oracle 데이터베이스 구성
- 키를 사용하여 사용자 정의 애플리케이션 백업 복원
- SAP HANA 리소스 생성
- Oracle 애플리케이션 볼륨 리소스 생성
- 사용자 정의 애플리케이션용 플러그인을 사용하여 사용자 정의 리소스 보호
- Microsoft SQL Server용 플러그인을 사용하여 Microsoft SQL Server 리소스 보호
- 보호된 Microsoft SQL Server 리소스 수정
- Microsoft SQL Server 리소스에 대한 보호 제거
- Oracle 데이터베이스용 플러그인을 사용하여 Oracle 리소스 보호
- 보호된 Oracle 리소스 수정
- Oracle 리소스에서 보호 제거
- 사용자 정의 애플리케이션용 플러그인을 사용하여 백업에서 리소스 복제
- Oracle 데이터베이스용 플러그인을 사용하여 백업에서 Oracle 애플리케이션 볼륨 복제
- Microsoft SQL Server용 플러그인을 사용하여 백업에서 Microsoft SQL Server 리소스를 복제합니다.
- Microsoft SQL Server 리소스의 복제 수명 주기를 만듭니다.
- Microsoft SQL Server 리소스의 복제 수명 주기 수정
- Microsoft SQL Server 리소스의 복제 수명 주기 삭제
- Oracle 데이터베이스에 대한 복제 사양 파일 생성

- Oracle 리소스의 주문형 복제 수명 주기를 시작합니다.
- 복제 사양 파일을 사용하여 백업에서 Oracle 리소스를 복제합니다.

보고서

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 각 플러그인에 대한 백업, 복원 및 복제 작업 보고서를 검색합니다.
- 일정을 추가, 실행, 삭제 또는 수정합니다.
- 예약된 보고서에 대한 데이터 검색

알림

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 모든 알림을 검색합니다
- ID로 알림 검색
- 여러 개의 알림을 삭제하거나 ID로 알림을 삭제합니다.

알박

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 사용자, 그룹 및 역할의 세부 정보를 검색합니다.
- 사용자 추가 또는 삭제
- 사용자에게 역할 할당
- 역할에서 사용자 할당 해제
- 역할 생성, 수정 또는 삭제
- 그룹에 역할 할당
- 역할에서 그룹 할당 해제
- 그룹 추가 또는 삭제
- 기존 역할의 사본을 만듭니다
- 사용자 또는 그룹에 리소스 할당 또는 할당 해제

구성

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 구성 설정 보기
- 구성 설정을 수정하다

인증서 설정

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- SnapCenter 서버 또는 플러그인 호스트의 인증서 상태를 확인합니다.
- SnapCenter 서버 또는 플러그인 호스트에 대한 인증서 설정을 수정합니다.

저장소

API를 사용하여 다양한 작업을 수행할 수 있습니다.

- 저장소 백업을 검색합니다
- 저장소에 대한 구성 정보를 봅니다.
- SnapCenter 저장소를 보호하고 복원합니다.
- SnapCenter 저장소 보호 해제
- 저장소를 다시 빌드하고 장애 조치합니다.

버전

이 API를 사용하면 SnapCenter 버전을 볼 수 있습니다.

Swagger API 웹 페이지를 사용하여 REST API에 액세스하는 방법

REST API는 Swagger 웹 페이지를 통해 공개됩니다. Swagger 웹 페이지에 접속하면 SnapCenter Server REST API를 표시하고 수동으로 API 호출을 실행할 수 있습니다. REST API를 사용하면 SnapCenter 서버를 관리하거나 데이터 보호 작업을 수행하는 데 도움이 됩니다.

REST API를 실행하려는 SnapCenter 서버의 관리 IP 주소 또는 도메인 이름을 알아야 합니다.

REST API 클라이언트를 실행하는 데 특별한 권한이 필요하지 않습니다. 모든 사용자가 Swagger 웹 페이지에 접속할 수 있습니다. REST API를 통해 액세스하는 개체에 대한 각각의 권한은 REST API에 로그인하기 위해 토큰을 생성하는 사용자를 기반으로 합니다.

단계

1. 브라우저에서 Swagger 웹 페이지에 접속하기 위한 URL을 `https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/` 형식으로 입력합니다.



REST API URL에 +, ., %, & 등의 문자가 포함되지 않도록 하세요.

2. **Swagger Explore** 필드에서 Swagger API 설명서가 자동으로 표시되지 않으면 다음을 입력합니다.
`https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/Content/swagger/ SnapCenter.yaml`
3. *탐색*을 클릭하세요.

API 리소스 유형 또는 범주 목록이 표시됩니다.

4. API 리소스 유형을 클릭하면 해당 리소스 유형의 API가 표시됩니다.

SnapCenter REST API를 실행할 때 예기치 않은 동작이 발생하는 경우 로그 파일을 사용하여 원인을 파악하고 문제를 해결할 수 있습니다. SnapCenter 사용자 인터페이스에서 모니터 > 로그 > *다운로드*를 클릭하여 로그 파일을 다운로드할 수 있습니다.

REST API 시작하기

SnapCenter REST API를 사용하면 빠르게 시작할 수 있습니다. API에 액세스하면 라이브 설정에서 보다 복잡한 워크플로 프로세스를 사용하기 전에 어느 정도 관점을 얻을 수 있습니다.

안녕하세요 세상

시스템에서 간단한 명령을 실행하여 SnapCenter REST API를 사용하고 가용성을 확인할 수 있습니다.

시작하기 전에

- Curl 유틸리티가 시스템에서 사용 가능한지 확인하세요.
- SnapCenter 서버의 IP 주소 또는 호스트 이름
- SnapCenter REST API에 액세스할 권한이 있는 계정의 사용자 이름과 비밀번호입니다.



자격 증명에 특수 문자가 포함되어 있는 경우, 사용하는 셸을 기준으로 Curl에서 허용하는 방식으로 형식을 지정해야 합니다. 예를 들어, 각 특수 문자 앞에 백슬래시를 삽입하거나 전체를 래핑할 수 있습니다. `username:password` 작은따옴표로 묶은 문자열.

단계

명령줄 인터페이스에서 다음을 실행하여 플러그인 정보를 검색합니다.

```
curl -X GET -u username:password -k  
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

예:

```
curl -X GET -u admin:password -k  
"'https://10.225.87.97/api/hosts?fields=IncludePluginInfo'"
```

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

공지 파일은 NetApp 소프트웨어에서 사용되는 타사 저작권 및 라이선스에 대한 정보를 제공합니다.

["SnapCenter 6.1에 대한 공지"](#)

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.