SnapCenter 소프트웨어 설명서

SnapCenter Software 4.9

NetApp
March 20, 2024

목차

SnapCenter 소프트웨어 설명서 1
릴리스 정보 2
개념 3
SnapCenter 개요 3
보안 기능 9
SnapCenter 역할 기반 액세스 제어(RBAC) 11
SnapCenter 재해 복구 17
리소스, 리소스 그룹 및 정책 18
사전 스크립트 및 포스트스크립트 19
REST API를 사용하여 SnapCenter 자동화 20
SnapCenter 서버 설치 22
설치 워크플로우 22
SnapCenter 서버 설치를 준비합니다 22
SnapCenter 서버를 설치합니다 42
RBAC 승인을 사용하여 SnapCenter에 로그인합니다 43
CA 인증서를 구성합니다 47
양방향 SSL 통신을 구성하고 사용하도록 설정합니다 50
인증서 기반 인증을 구성합니다 54
Active Directory, LDAP 및 LDAPS를 구성합니다 57
고가용성을 구성합니다 59
역할 기반 액세스 제어(RBAC) 구성 63
감사 로그 설정을 구성합니다 79
스토리지 시스템을 추가합니다 80
SnapCenter 표준 컨트롤러 기반 라이센스를 추가합니다 83
SnapCenter 표준 용량 기반 라이센스 추가 88
스토리지 시스템을 프로비저닝합니다 92
SnapCenter 서버로 보안 MySQL 연결을 구성합니다 109
설치 중에 Windows 호스트에서 활성화된 기능입니다 115
Microsoft SQL Server 데이터베이스 보호 119
Microsoft SQL Server용 SnapCenter 플러그인 119
Microsoft SQL Server용 SnapCenter 플러그인 설치를 빠르게 시작합니다 137
Microsoft SQL Server용 SnapCenter 플러그인 설치를 준비합니다 141
VMware vSphere용 SnapCenter 플러그인을 설치합니다 159
데이터 보호를 준비합니다 160
SQL Server 데이터베이스, 인스턴스 또는 가용성 그룹을 백업합니다 161
SQL Server 리소스를 복구합니다 186
SQL Server 데이터베이스 리소스의 클론을 생성합니다 197
SAP HANA 데이터베이스 보호 211
SAP HANA 데이터베이스용 SnapCenter 플러그인 211

SAP HANA 데이터베이스용 SnapCenter 플러그인 설치를 준비합니다 221
VMware vSphere용 SnapCenter 플러그인을 설치합니다 241
데이터 보호를 준비합니다 242
SAP HANA 리소스 백업 243
SAP HANA 데이터베이스 복원 268
SAP HANA 리소스 백업의 클론을 생성합니다 279
Oracle 데이터베이스 보호 287
Oracle 데이터베이스용 SnapCenter 플러그인 개요 287
Oracle 데이터베이스용 SnapCenter 플러그인을 설치합니다 293
VMware vSphere용 SnapCenter 플러그인을 설치합니다 321
Oracle 데이터베이스 보호를 위한 준비 321
Oracle 데이터베이스를 백업합니다 323
데이터베이스 백업을 마운트 및 마운트 해제합니다 352
Oracle 데이터베이스 복원 및 복구 354
Oracle 데이터베이스 클론 생성 371
애플리케이션 볼륨 관리 392
Windows 파일 시스템 보호 397
Microsoft Windows용 SnapCenter 플러그인 개념 397
Microsoft Windows용 SnapCenter 플러그인을 설치합니다 406
VMware vSphere용 SnapCenter 플러그인을 설치합니다 420
Windows 파일 시스템을 백업합니다 420
Windows 파일 시스템을 복구합니다 437
Windows 파일 시스템의 클론을 생성합니다 442
Microsoft Exchange Server 데이터베이스 보호 451
Microsoft Exchange Server용 SnapCenter 플러그인 개념 451
Microsoft Exchange Server용 SnapCenter 플러그인을 설치합니다 459
VMware vSphere용 SnapCenter 플러그인을 설치합니다 478
데이터 보호를 준비합니다 478
Exchange 리소스를 백업합니다 480
Exchange 리소스를 복구합니다 500
사용자 정의 응용 프로그램 보호 510
SnapCenter 맞춤형 플러그인 510
응용 프로그램용 플러그인을 개발합니다 517
SnapCenter 사용자 지정 플러그인 설치를 준비합니다 540
데이터 보호를 준비합니다 562
사용자 지정 플러그인 리소스를 백업합니다 563
사용자 지정 플러그인 리소스를 복원합니다 582
사용자 지정 플러그인 리소스 백업의 클론을 생성합니다 587
SnapCenter 서버 및 플러그인 관리 595
대시보드 보기 595
RBAC 관리 600

호스트를 관리합니다 601
리소스 페이지에서 지원되는 작업입니다 605
정책 관리 606
자원 그룹을 관리합니다 607
백업 관리 608
클론 삭제 610
작업, 일정, 이벤트 및 로그를 모니터링합니다 610
SnapCenter 보고 기능 개요 613
SnapCenter 서버 리포지토리를 관리합니다 616
신뢰할 수 없는 도메인의 리소스를 관리합니다 619
스토리지 시스템을 관리합니다 620
EMS Data 수집 관리 624
SnapCenter 서버 및 플러그인 업그레이드 626
사용 가능한 업데이트를 확인하도록 SnapCenter를 구성합니다 626
워크플로우 업그레이드 626
SnapCenter 서버를 업그레이드합니다 627
플러그인 패키지를 업그레이드합니다 629
SnapCenter 서버 및 플러그인을 제거합니다 631
SnapCenter 플러그인 패키지를 제거합니다 631
SnapCenter 서버를 제거합니다 635
REST API를 사용하여 자동화 636
REST API 개요 636
SnapCenter REST API에 기본적으로 액세스하는 방법 636
REST 웹 서비스 기반 636
기본 작동 특성 637
API 요청을 제어하는 입력 변수입니다 639
API 응답 해석 642
REST API 지원 644
Swagger API 웹 페이지를 사용하여 REST API에 액세스하는 방법 654
REST API를 시작합니다 655
법적 고지 656
저작권 656
상표 656
특허 656
개인 정보 보호 정책 656
오픈 소스 656

SnapCenter 소프트웨어 설명서

릴리스 정보

해결된 문제, 알려진 문제, 주의 및 제한 사항을 포함하여 SnapCenter 서버 및 SnapCenter 플러그인 패키지의 이 릴리스에 대한 중요 정보를 제공합니다.

자세한 내용은 를 참조하십시오 "SnapCenter 소프트웨어 4.9 릴리스 정보".

개념

SnapCenter 개요

SnapCenter 소프트웨어는 하이브리드 클라우드 어디서나 ONTAP 시스템에서 실행되는 애플리케이션, 데이터베이스, 호스트 파일 시스템 및 VM에 대해 애플리케이션 정합성을 보장하는 데이터 보호 기능을 제공하는 단순하고 확장 가능한 중앙 집중식 플랫폼입니다.

SnapCenter는 NetApp Snapshot, SnapRestore, FlexClone, SnapMirror 및 SnapVault 기술을 활용하여 다음을 제공합니다.

- 빠르고 공간 효율적이며 애플리케이션 정합성이 보장되는 디스크 기반 백업
- 신속하고 세부적인 복원 및 애플리케이션 정합성 보장 복구
- 빠르고 공간 효율적인 클론 복제

SnapCenter에는 SnapCenter 서버와 개별 경량 플러그인이 모두 포함되어 있습니다. 원격 애플리케이션 호스트에 플러그인을 자동으로 구축하고, 백업, 검증 및 클론 작업을 예약하고, 모든 데이터 보호 작업을 모니터링할 수 있습니다.

SnapCenter는 다음과 같은 방법으로 구축할 수 있습니다.

- 다음을 보호하기 위한 온프레미스:
  - ONTAP FAS, AFF 또는 ASA(All SAN Array) 운영 시스템에 있고 ONTAP FAS, AFF 또는 ASA 2차 시스템에 복제된 데이터입니다
  - ONTAP Select 운영 시스템에 있는 데이터
  - ONTAP FAS, AFF 또는 ASA 운영 및 2차 시스템에 있으며 로컬 StorageGRID 오브젝트 스토리지로 보호되는 데이터
- 하이브리드 클라우드의 사내 로 다음을 보호:
  - ONTAP FAS, AFF 또는 ASA 기본 시스템에 있고 Cloud Volumes ONTAP에 복제된 데이터입니다
  - ONTAP FAS, AFF 또는 ASA 운영 및 2차 시스템에 있고 클라우드의 오브젝트 및 아카이브 스토리지로 보호되는 데이터(BlueXP 백업 및 복구 통합 사용)
- 퍼블릭 클라우드에서 다음을 보호합니다.
  - Cloud Volumes ONTAP(이전의 ONTAP 클라우드) 운영 시스템에 있는 데이터
  - ONTAP용 Amazon FSX에 있는 데이터입니다

SnapCenter에는 다음과 같은 주요 기능이 포함되어 있습니다.

- 애플리케이션 정합성이 보장되는 중앙 집중식 데이터 보호

  ONTAP 시스템에서 실행되는 Microsoft Exchange Server, Microsoft SQL Server, Linux 또는 AIX 기반 Oracle 데이터베이스, SAP HANA 데이터베이스 및 Windows 호스트 파일 시스템에 대해 데이터 보호가 지원됩니다.

  사용자 정의 SnapCenter 플러그인을 만들 수 있는 프레임워크를 제공하여 다른 표준 또는 사용자 지정 애플리케이션 및 데이터베이스에서도 데이터 보호가 지원됩니다. 따라서 동일한 단일 창에서 다른 애플리케이션과 데이터베이스의 데이터를 보호할 수 있습니다. NetApp은 이 프레임워크를 활용하여 NetApp 자동화 스토어에서 IBM DB2, MongoDB, MySQL용 SnapCenter 맞춤형 플러그인을 출시했습니다.

"NetApp 스토리지 자동화 스토어"

- 정책 기반 백업

  정책 기반 백업은 NetApp Snapshot 복사본 기술을 활용하여 빠르고 공간 효율적이며 애플리케이션 정합성을 보장하는 디스크 기반 백업을 생성합니다. 필요에 따라 기존 보호 관계를 업데이트하여 보조 스토리지에 대한 이러한 백업을 자동으로 보호할 수 있습니다.

- 여러 리소스를 백업합니다

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

- 복원 및 복구

  SnapCenter는 백업 및 애플리케이션 정합성이 보장되는 시간 기반 복구를 빠르고 세부적으로 복구합니다. 하이브리드 클라우드의 모든 대상에서 복원할 수 있습니다.

- 클론 복제

  SnapCenter는 빠르고 공간 효율적이며 애플리케이션 정합성이 보장되는 클론 복제를 제공하여 소프트웨어를 신속하게 개발할 수 있도록 지원합니다. 하이브리드 클라우드의 모든 대상에서 복제할 수 있습니다.

- 단일 사용자 관리 그래픽 사용자 인터페이스(GUI)

  SnapCenter GUI는 하이브리드 클라우드의 모든 대상에서 리소스의 백업과 클론을 관리할 수 있는 원스톱 인터페이스를 제공합니다.

- REST API, Windows cmdlet, UNIX 명령

  SnapCenter에는 모든 오케스트레이션 소프트웨어와 통합할 수 있는 대부분의 기능, Windows PowerShell cmdlet 및 명령줄 인터페이스 사용을 위한 REST API가 포함되어 있습니다.

  REST API에 대한 자세한 내용은 를 참조하십시오 "REST API 개요".

  Windows cmdlet에 대한 자세한 내용은 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

  UNIX 명령에 대한 자세한 내용은 을 참조하십시오 "SnapCenter 소프트웨어 명령 참조 가이드".

- 중앙 집중식 데이터 보호 대시보드 및 보고
- 보안 및 위임을 위한 역할 기반 액세스 제어(RBAC).
- 고가용성 저장소 데이터베이스

  SnapCenter는 모든 백업 메타데이터를 저장할 수 있는 고가용성 저장소 데이터베이스를 제공합니다.

- 플러그인의 자동 푸시 설치

  SnapCenter 서버 호스트에서 애플리케이션 호스트에 이르는 SnapCenter 플러그인의 원격 푸시를 자동화할 수 있습니다.

- 고가용성

SnapCenter의 고가용성은 외부 로드 밸런서(F5)를 사용하여 설정됩니다. 동일한 데이터 센터 내에서 최대 2개의 노드가 지원됩니다.

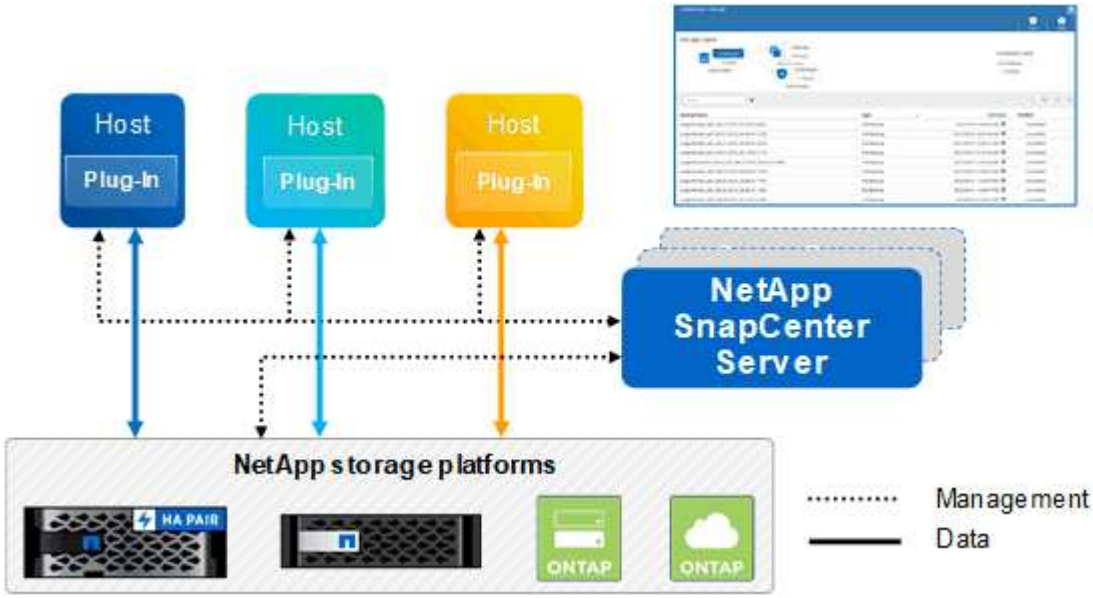
- DR(재해 복구)

  리소스 손상 또는 서버 충돌과 같은 재해 발생 시 SnapCenter 서버를 복구할 수 있습니다.

SnapCenter 아키텍처

SnapCenter 플랫폼은 중앙 집중식 관리 서버(SnapCenter 서버) 및 SnapCenter 플러그인 호스트를 포함하는 다계층 아키텍처를 기반으로 합니다.

SnapCenter는 멀티 사이트 데이터 센터를 지원합니다. SnapCenter 서버와 플러그인 호스트는 서로 다른 지리적 위치에 있을 수 있습니다.



SnapCenter 구성 요소

SnapCenter는 SnapCenter 서버 및 SnapCenter 플러그인으로 구성됩니다. 보호할 데이터에 적합한 플러그인만 설치해야 합니다.

- SnapCenter 서버
- Windows용 SnapCenter 플러그인 패키지로, 다음 플러그인이 포함되어 있습니다.
  - Microsoft SQL Server용 SnapCenter 플러그인
  - Microsoft Windows용 SnapCenter 플러그인
  - Microsoft Exchange Server용 SnapCenter 플러그인
  - SAP HANA 데이터베이스용 SnapCenter 플러그인
- Linux용 SnapCenter 플러그인 패키지, 다음 플러그인 포함:
  - Oracle 데이터베이스용 SnapCenter 플러그인
  - SAP HANA 데이터베이스용 SnapCenter 플러그인

- UNIX용 SnapCenter 플러그인

> UNIX용 SnapCenter 플러그인은 독립 실행형 플러그인이 아니며 독립적으로 설치할 수 없습니다. 이 플러그인은 Oracle 데이터베이스용 SnapCenter 플러그인 또는 SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치할 때 자동으로 설치됩니다.

- AIX용 SnapCenter 플러그인 패키지, 다음 플러그인 포함:
  - Oracle 데이터베이스용 SnapCenter 플러그인
  - UNIX용 SnapCenter 플러그인

> UNIX용 SnapCenter 플러그인은 독립 실행형 플러그인이 아니며 독립적으로 설치할 수 없습니다. 이 플러그인은 Oracle 데이터베이스용 SnapCenter 플러그인을 설치하면 자동으로 설치됩니다.

- SnapCenter 맞춤형 플러그인

  사용자 지정 플러그인은 커뮤니티에서 지원되며 에서 다운로드할 수 있습니다 "NetApp 스토리지 자동화 스토어".

SnapCenter Plug-in for VMware vSphere(이전의 NetApp Data Broker)는 가상화된 데이터베이스 및 파일 시스템에서 SnapCenter 데이터 보호 작업을 지원하는 독립 실행형 가상 어플라이언스입니다.

SnapCenter 서버

SnapCenter 서버에는 웹 서버, 중앙 집중식 HTML5 기반 사용자 인터페이스, PowerShell cmdlet, REST API 및 SnapCenter 저장소가 포함됩니다.

SnapCenter는 단일 사용자 인터페이스 내에서 여러 SnapCenter Server 간에 고가용성 및 수평 확장을 지원합니다. 외부 로드 밸런서(F5)를 사용하여 고가용성을 수행할 수 있습니다. 수천 개의 호스트가 있는 대규모 환경의 경우 여러 SnapCenter 서버를 추가하면 로드 밸런싱에 도움이 됩니다.

- Windows용 SnapCenter 플러그인 패키지를 사용하는 경우 호스트 에이전트는 SnapCenter 서버 및 Windows 플러그인 호스트에서 실행됩니다. Host Agent는 원격 Windows 호스트 또는 Microsoft SQL Server에서 기본적으로 스케줄을 실행하므로 로컬 SQL 인스턴스에서 스케줄이 실행됩니다.

  SnapCenter 서버는 호스트 에이전트를 통해 Windows 플러그인과 통신합니다.

- Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 사용하는 경우 SnapCenter 서버에서 Windows 작업 스케줄로 스케줄이 실행됩니다.
  - Oracle 데이터베이스용 SnapCenter 플러그인의 경우 SnapCenter 서버 호스트에서 실행되는 호스트 에이전트는 Linux 또는 AIX 호스트에서 실행되는 SnapCenter SPL(플러그인 로더)과 통신하여 서로 다른 데이터 보호 작업을 수행합니다.
  - SAP HANA 데이터베이스용 SnapCenter 플러그인 및 SnapCenter 맞춤형 플러그인의 경우 SnapCenter 서버는 호스트에서 실행되는 SCCore 에이전트를 통해 이러한 플러그인과 통신합니다.

SnapCenter 서버 및 플러그인은 HTTPS를 사용하여 호스트 에이전트와 통신합니다. SnapCenter 작업에 대한 정보는 SnapCenter 저장소에 저장됩니다.

SnapCenter는 Windows 호스트에 대해 비결합 네임스페이스를 지원합니다. 비결합 네임스페이스를 사용할 때 문제가 발생하면 을 참조하십시오 "분리된 네임스페이스를 사용할 때 SnapCenter에서 리소스를 검색할 수 없습니다".

SnapCenter 플러그인

각 SnapCenter 플러그인은 특정 환경, 데이터베이스 및 애플리케이션을 지원합니다.

플러그인 이름입니다	설치 패키지에 포함되어 있습니다	다른 플러그인이 필요합니다	호스트에 설치되어 있습니다	지원되는 플랫폼
SQL Server용 플러그인	Windows용 플러그인 패키지	Windows용 플러그인	SQL Server 호스트	Windows
Windows용 플러그인	Windows용 플러그인 패키지		Windows 호스트	Windows
Exchange용 플러그인	Windows용 플러그인 패키지	Windows용 플러그인	Exchange Server 호스트입니다	Windows
Oracle 데이터베이스용 플러그인	Linux용 플러그인 패키지 및 AIX용 플러그인 패키지	UNIX용 플러그인	Oracle 호스트	Linux 또는 AIX
SAP HANA 데이터베이스용 플러그인	Linux용 플러그인 패키지 및 Windows용 플러그인 패키지	UNIX용 플러그인 또는 Windows용 플러그인	HDBSQL 클라이언트 호스트입니다	Linux 또는 Windows
맞춤형 플러그인	"NetApp 스토리지 자동화 스토어"	파일 시스템 백업의 경우 Windows용 플러그인	사용자 지정 애플리케이션 호스트입니다	Linux 또는 Windows

VMware vSphere용 SnapCenter 플러그인은 가상 머신(VM), 데이터 저장소 및 가상 머신 디스크(VMDK)에 대해 충돌 시에도 정합성이 보장되고 VM 정합성이 보장되는 백업 및 복원 작업을 지원하며, SnapCenter 애플리케이션별 플러그인을 지원하여 가상화된 데이터베이스 및 파일 시스템에 대한 애플리케이션 정합성이 보장되는 백업 및 복구 작업을 보호합니다.

SnapCenter 4.1.1 사용자의 경우 VMware vSphere 4.1.1 용 SnapCenter 플러그인 설명서에 가상화 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 나와 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 VMware vSphere용 SnapCenter 플러그인을 사용하여 가상화된 데이터베이스 및 파일 시스템을 보호하는 방법에 대한 정보가 수록되어 있습니다. SnapCenter 4.3 이상을 사용하는 사용자의 경우 를 참조하십시오 "VMware vSphere용 SnapCenter 플러그인 설명서" 에는 VMware vSphere 가상 어플라이언스용 Linux 기반 SnapCenter 플러그인(오픈 가상 어플라이언스 형식)을 사용하여 가상화된 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 있습니다.

Microsoft SQL Server용 SnapCenter 플러그인 기능

- SnapCenter 환경에서 Microsoft SQL Server 데이터베이스의 애플리케이션 인식 백업, 복원 및 클론 복제 작업을

자동화합니다.

- VMware vSphere용 SnapCenter 플러그인을 구축하고 SnapCenter에 플러그인을 등록할 때 VMDK 및 RDM(Raw Device Mapping) LUN에서 Microsoft SQL Server 데이터베이스를 지원합니다
- SMB 공유만 프로비저닝을 지원합니다. SMB 공유에서 SQL Server 데이터베이스 백업에 대한 지원은 제공되지 않습니다.
- SnapManager for Microsoft SQL Server에서 SnapCenter로 백업 가져오기를 지원합니다.

Microsoft Windows용 **SnapCenter** 플러그인 기능

- SnapCenter 환경의 Windows 호스트에서 실행 중인 다른 플러그인에 대해 애플리케이션 인식 데이터 보호 지원
- SnapCenter 환경에서 Microsoft 파일 시스템에 대한 애플리케이션 인식 백업, 복원 및 클론 복제 작업을 자동화합니다
- Windows 호스트에 대한 스토리지 프로비저닝, 스냅샷 복사본 정합성 보장 및 공간 재확보를 지원합니다

Windows용 플러그인은 물리적 및 RDM LUN에 SMB 공유 및 Windows 파일 시스템을 프로비저닝하지만 SMB 공유에서 Windows 파일 시스템에 대한 백업 작업은 지원하지 않습니다.

Microsoft Exchange Server용 **SnapCenter** 플러그인 기능

- SnapCenter 환경에서 Microsoft Exchange Server 데이터베이스 및 DAG(데이터베이스 가용성 그룹)에 대한 애플리케이션 인식 백업 및 복원 작업을 자동화합니다
- VMware vSphere용 SnapCenter 플러그인을 구축할 때 RDM LUN에서 가상화된 Exchange Server를 지원하고 SnapCenter에 플러그인을 등록합니다

Oracle 데이터베이스용 **SnapCenter** 플러그인 기능

- 애플리케이션 인식 백업, 복원, 복구, 확인, 마운트, SnapCenter 환경에서 Oracle 데이터베이스의 마운트 해제 및 클론 작업
- SAP용 Oracle 데이터베이스를 지원하지만 SAP BR * Tools 통합은 제공되지 않습니다

UNIX용 **SnapCenter** 플러그인 기능

- Linux 또는 AIX 시스템에서 기본 호스트 스토리지 스택을 처리함으로써 Oracle 데이터베이스용 플러그인이 Oracle 데이터베이스에서 데이터 보호 작업을 수행할 수 있습니다
- ONTAP를 실행하는 스토리지 시스템에서 NFS(Network File System) 및 SAN(Storage Area Network) 프로토콜을 지원합니다.
- Linux 시스템의 경우 VMware vSphere용 SnapCenter 플러그인을 구축하고 SnapCenter에 플러그인을 등록하면 VMDK 및 RDM LUN의 Oracle 데이터베이스가 지원됩니다.
- SAN 파일 시스템 및 LVM 레이아웃에서 AIX용 Mount Guard를 지원합니다.
- SAN 파일 시스템에 대한 인라인 로깅과 AIX 시스템에 대한 LVM 레이아웃으로 JFS2(Enhanced Journaled File System)를 지원합니다.

  SAN 디바이스에 구축된 SAN 네이티브 디바이스, 파일 시스템 및 LVM 레이아웃이 지원됩니다.

SAP HANA 데이터베이스용 **SnapCenter** 플러그인 기능

- SnapCenter 환경에서 SAP HANA 데이터베이스의 애플리케이션 인식 백업, 복원, 클론 복제를 자동화합니다

SnapCenter 맞춤형 플러그인 기능

- 사용자 지정 플러그인을 지원하여 다른 SnapCenter 플러그인에서 지원하지 않는 애플리케이션 또는 데이터베이스를 관리할 수 있습니다. SnapCenter 설치의 일부로 사용자 지정 플러그인이 제공되지 않습니다.
- 다른 볼륨에 백업 세트의 미러 복제본을 생성하고 D2D 백업 복제를 수행할 수 있습니다.
- Windows 환경과 Linux 환경을 모두 지원합니다. Windows 환경에서 사용자 지정 플러그인을 통한 사용자 지정 애플리케이션은 필요에 따라 Microsoft Windows용 SnapCenter 플러그인을 사용하여 파일 시스템의 일관된 백업을 수행할 수 있습니다.

SnapCenter 소프트웨어용 MySQL, DB2 및 MongoDB 맞춤형 플러그인 샘플은 에서 다운로드할 수 있습니다 "NetApp 스토리지 자동화 스토어".

MySQL, DB2 및 MongoDB 맞춤형 플러그인은 NetApp 커뮤니티를 통해서만 지원됩니다.

NetApp은 맞춤형 플러그인을 생성 및 사용할 수 있는 기능을 지원하지만 생성하는 맞춤형 플러그인은 NetApp에서 지원하지 않습니다.

자세한 내용은 을 참조하십시오 "응용 프로그램용 플러그인을 개발합니다"

SnapCenter 리포지토리

NSM 데이터베이스라고도 하는 SnapCenter 저장소는 모든 SnapCenter 작업에 대한 정보와 메타데이터를 저장합니다.

SnapCenter 서버를 설치할 때 MySQL Server 리포지토리 데이터베이스가 기본적으로 설치됩니다. MySQL Server가 이미 설치되어 있고 SnapCenter Server를 새로 설치하는 경우 MySQL Server를 제거해야 합니다.

SnapCenter는 SnapCenter 리포지토리 데이터베이스로 MySQL Server 5.7.25 이상을 지원합니다. 이전 버전의 MySQL Server를 이전 버전의 SnapCenter와 함께 사용하는 경우 SnapCenter 업그레이드 중에 MySQL Server가 5.7.25 이상으로 업그레이드됩니다.

SnapCenter 리포지토리는 다음 정보와 메타데이터를 저장합니다.

- 백업, 클론, 복원 및 검증 메타데이터
- 보고, 작업 및 이벤트 정보
- 호스트 및 플러그인 정보
- 역할, 사용자 및 권한 세부 정보
- 스토리지 시스템 접속 정보입니다

보안 기능

SnapCenter는 엄격한 보안 및 인증 기능을 사용하여 데이터를 안전하게 보호합니다.

SnapCenter에는 다음과 같은 보안 기능이 포함되어 있습니다.

- SnapCenter에 대한 모든 통신은 HTTP over SSL(HTTPS)을 사용합니다.
- SnapCenter의 모든 자격 증명은 AES(고급 암호화 표준) 암호화를 사용하여 보호됩니다.
- SnapCenter는 FIPS(Federal Information Processing Standard)를 준수하는 보안 알고리즘을 사용합니다.
- SnapCenter는 고객이 제공한 인증 CA 인증서 사용을 지원합니다.
- SnapCenter 4.1.1 이상은 ONTAP와의 TLS(전송 계층 보안) 1.2 통신을 지원합니다. 클라이언트와 서버 간에 TLS 1.2 통신을 사용할 수도 있습니다.
- SnapCenter는 특정 SSL 암호화 제품군을 지원하여 네트워크 통신 전반에 보안을 제공합니다.

  자세한 내용은 을 참조하십시오 "지원되는 SSL 암호화 제품군을 구성하는 방법".
- SnapCenter는 회사의 방화벽 내부에 설치되어 SnapCenter 서버에 액세스하고 SnapCenter 서버와 플러그인 간의 통신을 지원합니다.
- SnapCenter API 및 작업 액세스는 24시간 후에 만료되는 AES 암호화로 암호화된 토큰을 사용합니다.
- SnapCenter는 Windows Active Directory와 통합되어 로그인 및 액세스 권한을 제어하는 역할 기반 액세스 제어(RBAC)를 사용합니다.
- IPsec은 Windows 및 Linux 호스트 시스템용 ONTAP의 SnapCenter에서 지원됩니다. "자세한 정보".
- SnapCenter PowerShell cmdlet은 세션 보안입니다.
- 기본 15분 동안 비활성 상태가 지속되면 SnapCenter에서 5분 후에 로그아웃된다는 경고 메시지를 표시합니다. 20분 동안 사용하지 않으면 SnapCenter에서 로그아웃하고 다시 로그인해야 합니다. 로그아웃 기간을 수정할 수 있습니다.
- 5회 이상의 잘못된 로그인 시도 후에 로그인이 일시적으로 비활성화됩니다.
- SnapCenter 서버와 ONTAP 간의 CA 인증서 인증을 지원합니다. "자세한 정보".
- 무결성 검증 도구는 SnapCenter 서버 및 플러그인에 추가되며 새로 설치 및 업그레이드 작업을 수행하는 동안 제공된 모든 바이너리의 유효성을 검사합니다.

CA 인증서 개요

SnapCenter 서버 설치 프로그램을 사용하면 설치하는 동안 중앙 집중식 SSL 인증서 지원을 사용할 수 있습니다.
서버와 플러그인 간의 보안 통신을 강화하기 위해 SnapCenter는 고객이 제공한 인증 CA 인증서 사용을 지원합니다.

SnapCenter 서버 및 해당 플러그인을 설치한 후 CA 인증서를 배포해야 합니다.
자세한 내용은 을 참조하십시오 "CA 인증서 CSR 파일을 생성합니다".

VMware vSphere용 SnapCenter 플러그인용 CA 인증서를 구축할 수도 있습니다. 자세한 내용은 을 참조하십시오 "인증서를 만들고 가져옵니다".

양방향 SSL 통신

양방향 SSL 통신은 SnapCenter 서버와 플러그인 간의 상호 통신을 보호합니다.

인증서 기반 인증 개요

인증서 기반 인증은 SnapCenter 플러그인 호스트에 액세스하려고 하는 각 사용자의 인증을 확인합니다. 사용자는 개인 키 없이 SnapCenter 서버 인증서를 내보내고 플러그인 호스트 신뢰할 수 있는 저장소에 가져와야 합니다. 인증서 기반 인증은 양방향 SSL 기능이 활성화된 경우에만 작동합니다.

멀티팩터 인증(MFA)

MFA는 SAML(Security Assertion Markup Language)을 통해 타사 ID 공급자(IDP)를 사용하여 사용자 세션을 관리합니다. 이 기능은 TOTP, 생체 인식, 푸시 알림 등과 같은 여러 요소를 기존 사용자 이름 및 암호와 함께 사용할 수 있는 옵션을 제공하므로 인증 보안이 향상됩니다. 또한 고객은 자신의 사용자 ID 공급자를 사용하여 포트폴리오 전체에서 통합 사용자 로그인(SSO)을 얻을 수 있습니다.

MFA는 SnapCenter 서버 UI 로그인에만 적용됩니다. 로그인은 IDP AD FS(Active Directory Federation Services)를 통해 인증됩니다. AD FS에서 다양한 인증 요소를 구성할 수 있습니다. SnapCenter는 서비스 공급자이며 AD FS에서 SnapCenter를 기반 공급업체로 구성해야 합니다. SnapCenter에서 MFA를 사용하려면 AD FS 메타데이터가 필요합니다.

MFA를 사용하는 방법에 대한 자세한 내용은 을 참조하십시오 "다중 요소 인증을 활성화합니다".

SnapCenter 역할 기반 액세스 제어(RBAC)

RBAC 유형

ONTAP RBAC(역할 기반 액세스 제어) 및 SnapCenter 권한을 사용하여 SnapCenter 관리자는 SnapCenter 리소스에 대한 제어 권한을 다른 사용자 또는 사용자 그룹에 위임할 수 있습니다. 이러한 중앙 관리형 액세스를 통해 애플리케이션 관리자는 위임된 환경 내에서 안전하게 작업할 수 있습니다.

언제든지 역할을 만들고 수정할 수 있으며 사용자에게 리소스 액세스 권한을 추가할 수 있지만 SnapCenter를 처음 설정할 때는 최소한 역할에 Active Directory 사용자 또는 그룹을 추가한 다음 이러한 사용자 또는 그룹에 리소스 액세스 권한을 추가해야 합니다.

SnapCenter를 사용하여 사용자 또는 그룹 계정을 만들 수 없습니다. 운영 체제 또는 데이터베이스의 Active Directory에서 사용자 또는 그룹 계정을 만들어야 합니다.

SnapCenter는 다음과 같은 유형의 역할 기반 액세스 제어를 사용합니다.

- SnapCenter RBAC
- SnapCenter 플러그인 RBAC(일부 플러그인의 경우)
- 애플리케이션 레벨 RBAC
- ONTAP 권한

SnapCenter RBAC

역할 및 권한

SnapCenter에는 권한이 이미 할당된 미리 정의된 역할이 제공됩니다. 이러한 역할에 사용자 또는 사용자 그룹을 할당할 수 있습니다. 새 역할을 만들고 사용 권한 및 사용자를 관리할 수도 있습니다.

- 사용자 또는 그룹에 권한 할당 *

사용자 또는 그룹에 권한을 할당하여 호스트, 스토리지 접속 및 리소스 그룹과 같은 SnapCenter 객체를 액세스할 수 있습니다. SnapCenterAdmin 역할의 권한은 변경할 수 없습니다.

동일한 포리스트 내의 사용자와 그룹 및 다른 포리스트에 속한 사용자에게 RBAC 권한을 할당할 수 있습니다. 포리스트 전체의 중첩된 그룹에 속하는 사용자에게는 RBAC 권한을 할당할 수 없습니다.

사용자 지정 역할을 만드는 경우 SnapCenter 관리자 역할의 모든 권한이 있어야 합니다. 호스트 추가 또는 호스트 제거 등의 일부 권한만 복사하는 경우에는 해당 작업을 수행할 수 없습니다.

인증

사용자는 로그인 시 그래픽 사용자 인터페이스(GUI) 또는 PowerShell cmdlet을 사용하여 인증을 제공해야 합니다. 사용자가 둘 이상의 역할의 구성원인 경우 로그인 자격 증명을 입력한 후 사용할 역할을 지정하라는 메시지가 표시됩니다. 또한 사용자는 API를 실행하기 위한 인증을 제공해야 합니다.

애플리케이션 레벨 **RBAC**

SnapCenter는 자격 증명을 사용하여 권한이 있는 SnapCenter 사용자에게 응용 프로그램 수준 권한도 있는지 확인합니다.

예를 들어 SQL Server 환경에서 스냅샷 복사본 및 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 스냅샷 복사본 및 데이터 보호 작업을 수행하려면 SnapCenter 관리자 역할에 Windows 호스트에 대한 관리자 권한이 있어야 합니다.

마찬가지로 Oracle 데이터베이스에서 데이터 보호 작업을 수행하고 데이터베이스 호스트에서 운영 체제(OS) 인증을 사용하지 않도록 설정한 경우 Oracle 데이터베이스 또는 Oracle ASM 자격 증명을 사용하여 자격 증명을 설정해야 합니다. SnapCenter 서버는 작업에 따라 이러한 방법 중 하나를 사용하여 설정된 자격 증명을 인증합니다.

VMware vSphere용 **SnapCenter** 플러그인 **RBAC**

VM 일관성 있는 데이터 보호를 위해 SnapCenter VMware 플러그인을 사용하는 경우 vCenter Server는 추가 RBAC 수준을 제공합니다. SnapCenter VMware 플러그인은 vCenter Server RBAC와 Data ONTAP RBAC를 모두 지원합니다.

자세한 내용은 을 참조하십시오 "VMware vSphere용 SnapCenter 플러그인 RBAC"

ONTAP 권한

스토리지 시스템에 액세스하는 데 필요한 권한이 있는 vsadmin 계정을 생성해야 합니다.

계정을 만들고 권한을 할당하는 방법에 대한 자세한 내용은 을 참조하십시오 "최소 권한으로 ONTAP 클러스터 역할을 생성합니다"

RBAC 권한 및 역할

SnapCenter RBAC(역할 기반 액세스 제어)를 사용하여 역할을 만들고 해당 역할에 권한을 할당한 다음 사용자 또는 사용자 그룹을 역할에 할당할 수 있습니다. 따라서 SnapCenter 관리자는 중앙에서 관리되는 환경을 만들 수 있고, 애플리케이션 관리자는 데이터 보호 작업을 관리할 수 있습니다. SnapCenter에는 몇 가지 미리 정의된 역할 및 권한이 제공됩니다.

SnapCenter 역할

SnapCenter에는 다음과 같은 사전 정의된 역할이 제공됩니다. 이러한 역할에 사용자와 그룹을 할당하거나 새 역할을

만들 수 있습니다.

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

- 애플리케이션 백업 및 클론 관리
- 백업 및 클론 뷰어
- 인프라 관리자
- SnapCenter서버

VMware vSphere 역할용 **SnapCenter** 플러그인

VM, VMDK 및 데이터 저장소의 VM 일관성 있는 데이터 보호를 관리하기 위해 VMware vSphere용 SnapCenter 플러그인을 통해 vCenter에서 다음 역할이 생성됩니다.

- SCV 관리자
- SCV 보기
- SCV 백업
- SCV 복원
- SCV 게스트 파일 복원

자세한 내용은 을 참조하십시오 "VMware vSphere 사용자를 위한 SnapCenter 플러그인의 RBAC 유형"

* 모범 사례: * VMware vSphere 운영을 위한 SnapCenter 플러그인에 대해 하나의 ONTAP 역할을 생성한 후 필요한 모든 권한을 할당하는 것이 좋습니다.

SnapCenter 권한

SnapCenter는 다음과 같은 권한을 제공합니다.

- 리소스 그룹
- 정책
- 백업
- 호스트
- 스토리지 연결
- 복제
- 프로비저닝(Microsoft SQL 데이터베이스에만 해당)
- 대시보드
- 보고서
- 복원
  - 전체 볼륨 복원(사용자 지정 플러그인에만 해당)
- 리소스

관리자가 아닌 경우 리소스 검색 작업을 수행하려면 관리자에게 플러그인 권한이 필요합니다.

- 플러그인 설치 또는 제거

  플러그인 설치 권한을 활성화할 경우 읽기 및 업데이트를 사용하도록 호스트 권한도 수정해야 합니다.

- 마이그레이션
- 마운트(Oracle 데이터베이스에만 해당)
- 마운트 해제(Oracle 데이터베이스에만 해당)
- 작업 모니터

  작업 모니터 권한을 사용하면 다른 역할의 구성원이 할당된 모든 개체에 대한 작업을 볼 수 있습니다.

사전 정의된 **SnapCenter** 역할 및 권한

SnapCenter에는 미리 정의된 역할이 제공되며 각 역할에는 이미 설정된 사용 권한이 있습니다. 역할 기반 액세스 제어(RBAC)를 설정 및 관리할 때 이러한 사전 정의된 역할을 사용하거나 새 역할을 생성할 수 있습니다.

SnapCenter에는 다음과 같은 사전 정의된 역할이 포함되어 있습니다.

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

사용자를 역할에 추가할 때는 스토리지 가상 시스템(SVM) 통신을 지원하기 위해 StorageConnection 권한을 할당하거나 SVM을 사용할 수 있도록 SVM을 사용자에게 할당해야 합니다. 스토리지 연결 권한을 사용하면 SVM 연결을 생성할 수 있습니다.

예를 들어, SnapCenter 관리자 역할을 가진 사용자는 SVM 연결을 생성하여 앱 백업 및 클론 관리 역할을 가진 사용자에게 할당할 수 있습니다. 이 역할은 기본적으로 SVM 연결을 생성하거나 편집할 권한이 없습니다. SVM이 연결되지 않으면 사용자는 백업, 클론 복제 또는 복원 작업을 완료할 수 없습니다.

SnapCenter 관리자 역할

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

앱 백업 및 클론 관리자 역할

App Backup and Clone Admin 역할에는 애플리케이션 백업 및 클론 관련 작업에 대한 관리 작업을 수행하는 데 필요한 권한이 있습니다. 이 역할에는 호스트 관리, 프로비저닝, 스토리지 접속 관리 또는 원격 설치에 대한 권한이 없습니다.

권한	활성화됨	생성	읽기	업데이트	삭제
리소스 그룹	해당 없음	예	예	예	예
정책	해당 없음	예	예	예	예
백업	해당 없음	예	예	예	예
호스트	해당 없음	예	예	예	예
스토리지 연결	해당 없음	아니요	예	아니요	아니요
복제	해당 없음	예	예	예	예
프로비저닝	해당 없음	아니요	예	아니요	아니요
대시보드	예	해당 없음	해당 없음	해당 없음	해당 없음
보고서	예	해당 없음	해당 없음	해당 없음	해당 없음
복원	예	해당 없음	해당 없음	해당 없음	해당 없음
리소스	예	예	예	예	예
플러그인 설치 /제거	아니요	해당 없음		해당 없음	해당 없음
마이그레이션	아니요	해당 없음	해당 없음	해당 없음	해당 없음
마운트	예	예	해당 없음	해당 없음	해당 없음
마운트 해제하다	예	예	해당 없음	해당 없음	해당 없음
전체 볼륨 복원	아니요	아니요	해당 없음	해당 없음	해당 없음
작업 모니터	예	해당 없음	해당 없음	해당 없음	해당 없음

백업 및 클론 뷰어 역할

백업 및 클론 뷰어 역할에는 모든 권한에 대한 읽기 전용 보기가 있습니다. 또한 이 역할에는 대시보드 검색, 보고 및 액세스에 대한 사용 권한이 설정되어 있습니다.

권한	활성화됨	생성	읽기	업데이트	삭제
리소스 그룹	해당 없음	아니요	예	아니요	아니요
정책	해당 없음	아니요	예	아니요	아니요
백업	해당 없음	아니요	예	아니요	아니요
호스트	해당 없음	아니요	예	아니요	아니요
스토리지 연결	해당 없음	아니요	예	아니요	아니요
복제	해당 없음	아니요	예	아니요	아니요
프로비저닝	해당 없음	아니요	예	아니요	아니요
대시보드	예	해당 없음	해당 없음	해당 없음	해당 없음
보고서	예	해당 없음	해당 없음	해당 없음	해당 없음
복원	아니요	아니요	해당 없음	해당 없음	해당 없음
리소스	아니요	아니요	예	예	아니요
플러그인 설치 /제거	아니요	해당 없음	해당 없음	해당 없음	해당 없음
마이그레이션	아니요	해당 없음	해당 없음	해당 없음	해당 없음
마운트	예	해당 없음	해당 없음	해당 없음	해당 없음
마운트 해제하다	예	해당 없음	해당 없음	해당 없음	해당 없음
전체 볼륨 복원	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, 대시보드에 액세스합니다.

권한	활성화됨	생성	읽기	업데이트	삭제
리소스 그룹	해당 없음	예	예	예	예
정책	해당 없음	아니요	예	예	예
백업	해당 없음	예	예	예	예
호스트	해당 없음	예	예	예	예
스토리지 연결	해당 없음	예	예	예	예
복제	해당 없음	아니요	예	아니요	아니요
프로비저닝	해당 없음	예	예	예	예
대시보드	예	해당 없음	해당 없음	해당 없음	해당 없음
보고서	예	해당 없음	해당 없음	해당 없음	해당 없음
복원	예	해당 없음	해당 없음	해당 없음	해당 없음
리소스	예	예	예	예	예
플러그인 설치 /제거	예	해당 없음	해당 없음	해당 없음	해당 없음
마이그레이션	아니요	해당 없음	해당 없음	해당 없음	해당 없음
마운트	아니요	해당 없음	해당 없음	해당 없음	해당 없음
마운트 해제하다	아니요	해당 없음	해당 없음	해당 없음	해당 없음
전체 볼륨 복원	아니요	아니요	해당 없음	해당 없음	해당 없음
작업 모니터	예	해당 없음	해당 없음	해당 없음	해당 없음

SnapCenter 재해 복구

SnapCenter 재해 복구(DR) 기능을 사용하여 리소스 손상 또는 서버 충돌과 같은 재해 발생 시 SnapCenter 서버를 복구할 수 있습니다. SnapCenter 리포지토리, 서버 일정 및 서버 구성 요소를 복구할 수 있습니다. SQL Server용 SnapCenter 플러그인 및 SQL Server용 SnapCenter 플러그인을 복구할 수도 있습니다.

이 섹션에서는 SnapCenter의 두 가지 DR(재해 복구) 유형에 대해 설명합니다.

SnapCenter 서버 **DR**

- SnapCenter 서버 데이터는 백업되며 SnapCenter 서버에 플러그인을 추가하거나 관리하지 않고도 복구할 수 있습니다.
- 보조 SnapCenter 서버는 운영 SnapCenter 서버와 동일한 설치 디렉토리 및 포트에 설치해야 합니다.
- MFA(다중 인증)의 경우 SnapCenter 서버 DR 중에 모든 브라우저 탭을 닫고 브라우저를 다시 열어 다시 로그인해야 합니다. 이렇게 하면 기존 또는 활성 세션 쿠키가 지워 올바른 구성 데이터가 업데이트됩니다.
- SnapCenter 재해 복구 기능은 REST API를 사용하여 SnapCenter 서버를 백업합니다. 을 참조하십시오 "SnapCenter 서버의 재해 복구를 위한 REST API 워크플로우".
- 감사 설정 관련 구성 파일은 DR 백업 및 복구 작업 후 DR 서버 둘 다 백업되지 않습니다. 감사 로그 설정을 수동으로 반복해야 합니다.

SnapCenter 플러그인 및 스토리지 **DR**

DR은 SQL Server용 SnapCenter 플러그인에만 지원됩니다. SQL Server용 SnapCenter 플러그인이 다운된 경우 다른 SQL 호스트로 전환하고 몇 가지 단계를 수행하여 데이터를 복구합니다. 을 참조하십시오 "SQL Server용 SnapCenter 플러그인의 재해 복구".

SnapCenter는 ONTAP SnapMirror 기술을 사용하여 데이터를 복제합니다. 데이터를 2차 사이트로 복제하여 DR에 사용하고 동기화 상태로 유지할 수 있습니다. SnapMirror의 복제 관계를 끊어 페일오버를 시작할 수 있습니다. 페일백 중에 동기화를 취소할 수 있으며 DR 사이트의 데이터를 기본 위치로 다시 복제할 수 있습니다.

리소스, 리소스 그룹 및 정책

SnapCenter를 사용하기 전에 수행할 백업, 클론 및 복원 작업과 관련된 기본 개념을 이해하는 것이 좋습니다. 서로 다른 작업을 위해 리소스, 리소스 그룹 및 정책과 상호 작용합니다.

- * 리소스 * 는 일반적으로 SnapCenter를 통해 백업 또는 클론 복제하는 데이터베이스, Windows 파일 시스템 또는 파일 공유입니다.

  하지만 사용자 환경에 따라 데이터베이스 인스턴스, Microsoft SQL Server 가용성 그룹, Oracle 데이터베이스, Oracle RAC 데이터베이스, Windows 파일 시스템 또는 사용자 지정 애플리케이션 그룹이 리소스가 될 수 있습니다.

- 리소스 그룹 * 은 호스트 또는 클러스터의 리소스 모음입니다. 리소스 그룹에는 여러 호스트 및 여러 클러스터의 리소스가 포함될 수도 있습니다.

  자원 그룹에 대해 작업을 수행할 때 자원 그룹에 지정한 일정에 따라 자원 그룹에 정의된 모든 자원에 대해 해당 작업을 수행합니다.

  필요에 따라 단일 리소스 또는 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 구성할 수도 있습니다.

  > 공유 리소스 그룹의 호스트 중 하나를 유지 관리 모드로 설정하고 동일한 공유 리소스 그룹에 연결된 스케줄이 있는 경우 모든 예약된 작업이 공유 리소스 그룹의 다른 모든 호스트에 대해 일시 중지됩니다.

  데이터베이스 플러그인을 사용하여 데이터베이스, 파일 시스템을 백업할 파일 시스템 플러그인, VMware

vSphere용 SnapCenter 플러그인을 사용하여 VM 및 데이터 저장소를 백업해야 합니다.

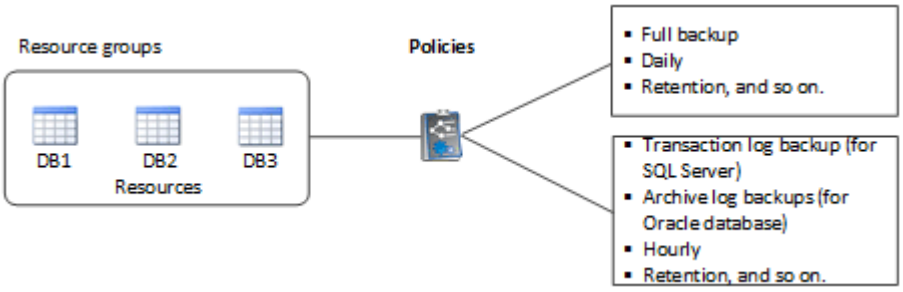
- * 정책 * 백업 빈도, 복제 보존, 복제, 스크립트 및 기타 데이터 보호 작업의 특성을 지정합니다.

  자원 그룹을 만들 때 해당 그룹에 대해 하나 이상의 정책을 선택합니다. 필요 시 백업을 수행할 때 정책을 선택할 수도 있습니다.

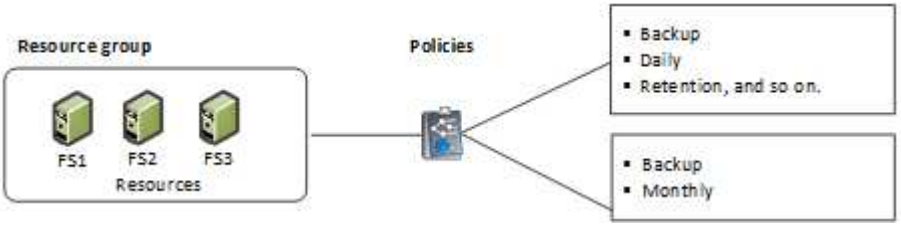
보호하려는_대상_과 이를 보호할 시기를 요일과 시간으로 정의하는 자원 그룹을 생각해 보십시오. 정책을 정의하는 _ 방법 _ 을(를) 보호하려는 것으로 생각해 보십시오. 예를 들어 모든 데이터베이스를 백업하거나 호스트의 모든 파일 시스템을 백업하는 경우 모든 데이터베이스나 호스트의 모든 파일 시스템을 포함하는 리소스 그룹을 생성할 수 있습니다. 그런 다음 리소스 그룹에 일별 정책과 시간별 정책이라는 두 가지 정책을 연결할 수 있습니다.

리소스 그룹을 생성하고 정책을 연결할 때 매일 전체 백업을 수행하고 로그 백업을 매시간 수행하는 다른 일정을 수행하도록 리소스 그룹을 구성할 수 있습니다.

다음 그림에서는 데이터베이스 리소스, 리소스 그룹 및 정책 간의 관계를 보여 줍니다.



다음 그림에서는 Windows 파일 시스템에 대한 리소스, 리소스 그룹 및 정책 간의 관계를 보여 줍니다.



사전 스크립트 및 포스트스크립트

데이터 보호 작업의 일부로 사용자 지정 처방과 사후 스크립트를 사용할 수 있습니다. 이러한 스크립트를 사용하면 데이터 보호 작업 전 또는 이후에 자동화를 수행할 수 있습니다. 예를 들어 데이터 보호 작업 장애 또는 경고를 자동으로 알리는 스크립트를 포함할 수 있습니다. 처방전과 소인을 설정하기 전에 이러한 스크립트를 만들기 위한 몇 가지 요구 사항을 이해해야 합니다.

지원되는 스크립트 유형입니다

Windows에서 지원되는 스크립트 유형은 다음과 같습니다.

- 배치 파일
- PowerShell 스크립트
- Perl 스크립트

UNIX에서 지원되는 스크립트 유형은 다음과 같습니다.

- Perl 스크립트
- Python 스크립트
- 쉘 스크립트

> 기본 bash shell과 함께 sh-shell, k-shell 및 c-shell과 같은 다른 쉘도 지원됩니다.

스크립트 경로

가상화되지 않은 스토리지 시스템과 가상화된 스토리지 시스템에서 SnapCenter 작업의 일부로 실행되는 모든 처방과 사후 스크립트는 플러그인 호스트에서 실행됩니다.

- Windows 스크립트는 플러그인 호스트에 있어야 합니다.

> 처방자 또는 사후 스크립트 경로에는 드라이브 또는 공유가 포함되어서는 안 됩니다. 경로는 scripts_path에 상대해야 합니다.

- UNIX 스크립트는 플러그인 호스트에 있어야 합니다.

> 스크립트 경로는 실행 시 검증됩니다.

스크립트 지정 위치

스크립트는 백업 정책에 지정됩니다. 백업 작업이 시작되면 정책은 자동으로 스크립트를 백업 중인 리소스와 연결합니다. 백업 정책을 만들 때 처방과 PS 인수를 지정할 수 있습니다.

> 여러 스크립트를 지정할 수 없습니다.

스크립트 시간 초과

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

스크립트 출력

Windows prescpts 및 postscripts 출력 파일의 기본 디렉터리는 Windows\System32입니다.

UNIX 처방과 postscript에 대한 기본 위치는 없습니다. 원하는 위치로 출력 파일을 리디렉션할 수 있습니다.

REST API를 사용하여 SnapCenter 자동화

REST API를 사용하여 몇 가지 SnapCenter 관리 작업을 수행할 수 있습니다. REST API는 Swagger 웹 페이지를 통해 표시됩니다. Swagger 웹 페이지에 액세스하여 REST API 설명서를 표시하고 API 호출을 수동으로 실행할 수 있습니다. REST API를 사용하여 SnapCenter 서버 또는 SnapCenter vSphere 호스트를 관리할 수 있습니다.

나머지 **API**는…	위치…
SnapCenter 서버	https:// <SnapCenter_IP_address_or_name>: <SnapCenter_port>/swagger/
VMware vSphere용 SnapCenter 플러그인	https://<OVA_IP_address_or_host_name>: <scv_plugin_port>/API/swagger-ui.html#을 참조하십시오

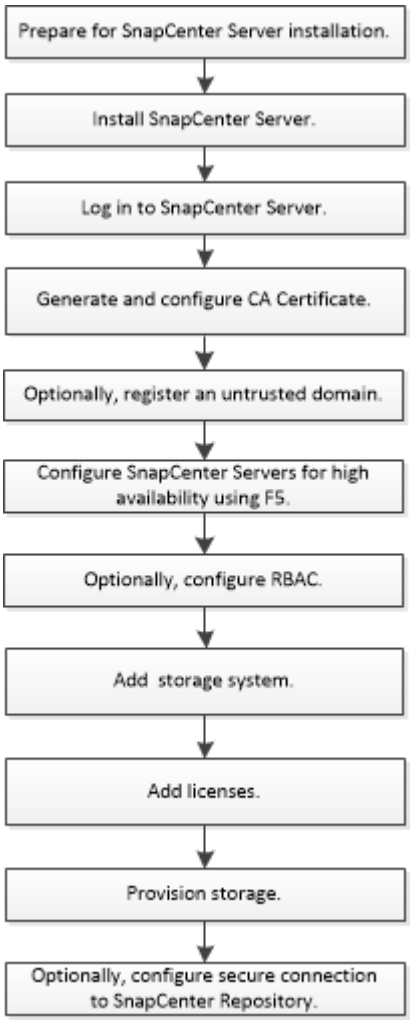
SnapCenter REST API에 대한 자세한 내용은 를 참조하십시오 "REST API 개요"

VMware vSphere REST API용 SnapCenter 플러그인에 대한 자세한 내용은 을 참조하십시오 "VMware vSphere REST API용 SnapCenter 플러그인"

SnapCenter 서버 설치

설치 워크플로우

워크플로우는 SnapCenter 서버를 설치하고 구성하는 데 필요한 여러 작업을 보여 줍니다.



SnapCenter 서버 설치를 준비합니다

도메인 및 작업 그룹 요구 사항

SnapCenter 서버는 도메인 또는 작업 그룹에 있는 시스템에 설치할 수 있습니다. 설치에 사용되는 사용자는 작업 그룹과 도메인 모두에 대해 컴퓨터에 대한 관리자 권한을 가져야 합니다.

Windows 호스트에 SnapCenter 서버 및 SnapCenter 플러그인을 설치하려면 다음 중 하나를 사용해야 합니다.

- * Active Directory 도메인 *

  로컬 관리자 권한이 있는 도메인 사용자를 사용해야 합니다. 도메인 사용자는 Windows 호스트에 있는 로컬 관리자 그룹의 구성원이어야 합니다.

- * 작업 그룹 *

  로컬 관리자 권한이 있는 로컬 계정을 사용해야 합니다.

도메인 트러스트, 다중 도메인 포리스트 및 교차 도메인 트러스트가 지원되지만 교차 포리스트 도메인은 지원되지 않습니다. Active Directory 도메인 및 트러스트에 대한 Microsoft 설명서에 자세한 내용이 나와 있습니다.

SnapCenter 서버를 설치한 후에는 SnapCenter 호스트가 있는 도메인을 변경해서는 안 됩니다. SnapCenter 서버를 설치할 때 있던 도메인에서 SnapCenter 서버 호스트를 제거한 다음 SnapCenter 서버를 제거하려고 하면 제거 작업이 실패합니다.

요구사항을 충족해야 합니다

SnapCenter 서버를 설치하기 전에 공간 및 크기 조정 요구 사항을 숙지해야 합니다. 사용 가능한 시스템 및 보안 업데이트도 적용해야 합니다.

항목	요구 사항
운영 체제	Microsoft Windows 운영 체제의 영어, 독일어, 일본어 및 중국어 간체 버전만 지원됩니다. 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
최소 CPU 수입니다	4코어
최소 RAM	8GB MySQL Server 버퍼 풀은 전체 RAM의 20%를 사용합니다.
SnapCenter 서버 소프트웨어 및 로그의 최소 하드 드라이브 공간	4GB SnapCenter 서버가 설치된 동일한 드라이브에 SnapCenter 저장소가 있는 경우 10GB를 사용하는 것이 좋습니다.
SnapCenter 리포지토리에 대한 최소 하드 드라이브 공간입니다	6GB 참고: SnapCenter 저장소가 설치된 동일한 드라이브에 SnapCenter 서버가 있는 경우 10GB를 사용하는 것이 좋습니다.

항목	요구 사항
필요한 소프트웨어 패키지	• Microsoft .NET Framework 4.7.2 이상 • WMF(Windows Management Framework) 4.0 이상 • PowerShell 4.0 이상 NET 관련 문제 해결에 대한 자세한 내용은 을 참조하십시오 "인터넷에 연결되지 않은 기존 시스템의 경우 SnapCenter 업그레이드 또는 설치가 실패합니다".

SAN 호스트 요구 사항

SnapCenter 호스트가 FC/iSCSI 환경의 일부인 경우 ONTAP 스토리지에 액세스할 수 있도록 시스템에 추가 소프트웨어를 설치해야 할 수 있습니다.

SnapCenter에는 호스트 유틸리티 또는 DSM이 포함되어 있지 않습니다. SnapCenter 호스트가 SAN 환경의 일부인 경우 다음 소프트웨어를 설치하고 구성해야 할 수 있습니다.

- Host Utilities(호스트 유틸리티)

  호스트 유틸리티는 FC와 iSCSI를 지원하며 Windows Server에서 MPIO를 사용할 수 있도록 합니다. 자세한 내용은 을 참조하십시오 "Host Utilities 설명서".

- Windows MPIO용 Microsoft DSM

  이 소프트웨어는 Windows MPIO 드라이버와 함께 작동하여 NetApp과 Windows 호스트 컴퓨터 간의 여러 경로를 관리합니다.

  고가용성 구성을 위해서는 DSM이 필요합니다.

  ⓘ ONTAP DSM을 사용하는 경우 Microsoft DSM으로 마이그레이션해야 합니다. 자세한 내용은 을 참조하십시오 "ONTAP DSM에서 Microsoft DSM으로 마이그레이션하는 방법".

지원되는 스토리지 시스템 및 애플리케이션

지원되는 스토리지 시스템, 애플리케이션 및 데이터베이스를 알아야 합니다.

- SnapCenter는 데이터를 보호하기 위해 ONTAP 8.3.0 이상을 지원합니다.
- SnapCenter는 ONTAP 소프트웨어 4.5 P1 패치 릴리즈로부터 데이터를 보호하기 위해 NetApp SnapCenter용 Amazon FSx를 지원합니다.

  NetApp ONTAP용 Amazon FSx를 사용하는 경우 데이터 보호 작업을 수행하기 위해 SnapCenter 서버 호스트 플러그인이 4.5 P1 이상으로 업그레이드되었는지 확인합니다.

  NetApp ONTAP용 Amazon FSx에 대한 자세한 내용은 를 참조하십시오 "NetApp ONTAP용 Amazon FSx 문서".

- SnapCenter는 다양한 애플리케이션 및 데이터베이스의 보호를 지원합니다.

지원되는 응용 프로그램 및 데이터베이스에 대한 자세한 내용은 을 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

- SnapCenter 4.9 P1 이상은 AWS(Amazon Web Services) 기반 VMware Cloud 환경에서 Oracle 및 Microsoft SQL 워크로드 보호를 지원합니다.

  자세한 내용은 을 참조하십시오
  "AWS SDDC 환경의 VMware Cloud에서 NetApp SnapCenter를 사용하여 Oracle, MS SQL 워크로드를 보호하십시오".

지원되는 브라우저

SnapCenter 소프트웨어는 여러 브라우저에서 사용할 수 있습니다.

- 크롬

  v66을 사용하는 경우 SnapCenter GUI를 시작하지 못할 수 있습니다.

- Internet Explorer 를 참조하십시오

  IE 10 또는 이전 버전을 사용하는 경우 SnapCenter UI가 제대로 로드되지 않습니다. IE 11로 업그레이드해야 합니다.

  - 기본 수준 보안만 지원됩니다.

    Internet Explorer 보안 설정을 변경하면 상당한 브라우저 표시 문제가 발생합니다.

  - Internet Explorer 호환성 보기를 비활성화해야 합니다.

- Microsoft Edge를 참조하십시오

지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

연결 및 포트 요구 사항

SnapCenter 서버 및 응용 프로그램 또는 데이터베이스 플러그인을 설치하기 전에 연결 및 포트 요구 사항이 충족되었는지 확인해야 합니다.

- 응용 프로그램이 포트를 공유할 수 없습니다.

  각 포트는 해당 애플리케이션 전용으로 사용되어야 합니다.

- 사용자 지정 가능한 포트의 경우 기본 포트를 사용하지 않으려는 경우 설치 중에 사용자 지정 포트를 선택할 수 있습니다.

  설치 후 호스트 수정 마법사를 사용하여 플러그인 포트를 변경할 수 있습니다.

- 고정 포트의 경우 기본 포트 번호를 그대로 사용해야 합니다.
- 방화벽

  - 방화벽, 프록시 또는 기타 네트워크 장치가 연결을 방해해서는 안 됩니다.

- SnapCenter를 설치할 때 사용자 지정 포트를 지정하는 경우 SnapCenter 플러그인 로더의 해당 포트에 대한 방화벽 규칙을 플러그인 호스트에 추가해야 합니다.

다음 표에는 여러 포트와 해당 기본값이 나와 있습니다.

포트의 유형입니다	기본 포트입니다
SnapCenter 포트	8146(HTTPS), 양방향, 사용자 지정 가능(URL_\https://server:8146_) SnapCenter 클라이언트(SnapCenter 사용자)와 SnapCenter 서버 간의 통신에 사용됩니다. 플러그인 호스트에서 SnapCenter 서버로의 통신에도 사용됩니다. 포트를 사용자 정의하려면 를 참조하십시오 "설치 마법사를 사용하여 SnapCenter 서버를 설치합니다."
SnapCenter SMCore 통신 포트입니다	8145(HTTPS), 양방향, 사용자 지정 가능 이 포트는 SnapCenter 서버와 SnapCenter 플러그인이 설치된 호스트 간의 통신에 사용됩니다. 포트를 사용자 정의하려면 를 참조하십시오 "설치 마법사를 사용하여 SnapCenter 서버를 설치합니다."
MySQL 포트	3306(HTTPS), 양방향 이 포트는 SnapCenter 및 MySQL 리포지토리 데이터베이스 간의 통신에 사용됩니다. SnapCenter 서버에서 MySQL 서버로 보안 연결을 생성할 수 있습니다. "자세한 정보" 포트를 사용자 정의하려면 를 참조하십시오 "설치 마법사를 사용하여 SnapCenter 서버를 설치합니다."

포트의 유형입니다	기본 포트입니다
Windows 플러그인 호스트	135, 445(TCP) 135번 및 445번 포트 외에도 Microsoft에서 지정한 동적 포트 범위도 열려 있어야 합니다. 원격 설치 작업은 이 포트 범위를 동적으로 검색하는 WMI(Windows Management Instrumentation) 서비스를 사용합니다. 지원되는 동적 포트 범위에 대한 자세한 내용은 을 참조하십시오 "Windows에 대한 서비스 개요 및 네트워크 포트 요구 사항" 이 포트는 SnapCenter 서버와 플러그인이 설치되는 호스트 간의 통신에 사용됩니다. 플러그인 패키지 바이너리를 Windows 플러그인 호스트에 푸시하려면 포트가 플러그인 호스트에서만 열려 있어야 하며 설치 후 닫을 수 있습니다.
Linux 또는 AIX 플러그인 호스트	22(SSH) 포트는 SnapCenter 서버와 플러그인이 설치되는 호스트 간의 통신에 사용됩니다. 이 포트는 SnapCenter에서 플러그인 패키지 바이너리를 Linux 또는 AIX 플러그인 호스트에 복사하는 데 사용되며 방화벽 또는 iptables에서 열거나 제외해야 합니다.
Windows용 SnapCenter 플러그인 패키지, Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지	8145(HTTPS), 양방향, 사용자 지정 가능 이 포트는 플러그인 패키지가 설치된 SMCore와 호스트 간의 통신에 사용됩니다. 또한 SVM 관리 LIF와 SnapCenter 서버 간에 통신 경로를 개방해야 합니다. 포트를 사용자 정의하려면 를 참조하십시오 "호스트를 추가하고 Microsoft Windows용 SnapCenter 플러그인을 설치합니다" 또는 "호스트를 추가하고 Linux 또는 AIX용 SnapCenter 플러그인 패키지를 설치합니다."
Oracle 데이터베이스용 SnapCenter 플러그인	27216, 사용자 지정 가능 기본 JDBC 포트는 Oracle용 플러그인에서 Oracle 데이터베이스에 연결하는 데 사용됩니다. 포트를 사용자 정의하려면 를 참조하십시오 "호스트를 추가하고 Linux 또는 AIX용 SnapCenter 플러그인 패키지를 설치합니다."

포트의 유형입니다	기본 포트입니다
SnapCenter용 맞춤형 플러그인	9090(HTTPS), 고정 사용자 지정 플러그인 호스트에서만 사용되는 내부 포트입니다. 방화벽 예외가 필요하지 않습니다. SnapCenter 서버와 사용자 지정 플러그인 간의 통신은 포트 8145를 통해 라우팅됩니다.
ONTAP 클러스터 또는 SVM 통신 포트	443(HTTPS), 양방향 80(HTTP), 양방향 이 포트는 SnapCenter Server를 실행하는 호스트와 SVM 간 통신에 SAL(Storage Abstraction Layer)에서 사용됩니다. 이 포트는 현재 SnapCenter 플러그인 호스트와 SVM 간 통신에 SnapCenter의 SAL에서 사용됩니다.
SAP HANA 데이터베이스 vCode용 SnapCenter 플러그인 맞춤법 검사기	3instance_number13 또는 3instance_number15, HTTP 또는 HTTPS, 양방향 및 사용자 지정 가능 MDC(멀티테넌트 데이터베이스 컨테이너) 단일 테넌트의 경우 포트 번호는 13으로 끝나며 MDC가 아닌 경우 포트 번호는 15로 끝납니다. 예를 들어, 32013은 인스턴스 20의 포트 번호이고 31015는 인스턴스 10의 포트 번호입니다. 포트를 사용자 정의하려면 를 참조하십시오 "호스트를 추가하고 원격 호스트에 플러그인 패키지를 설치합니다."
도메인 컨트롤러 통신 포트입니다	인증이 제대로 작동하기 위해 도메인 컨트롤러의 방화벽에서 열어야 하는 포트를 확인하려면 Microsoft 설명서를 참조하십시오. SnapCenter 서버, 플러그인 호스트 또는 다른 Windows 클라이언트가 사용자를 인증할 수 있도록 도메인 컨트롤러에서 Microsoft 필수 포트를 열어야 합니다.

포트 세부 정보를 수정하려면 을 참조하십시오 "플러그인 호스트를 수정합니다".

SnapCenter 라이센스

SnapCenter에는 애플리케이션, 데이터베이스, 파일 시스템 및 가상 머신의 데이터 보호를 위해 몇 가지 라이센스가 필요합니다. 설치하는 SnapCenter 라이센스 유형은 스토리지 환경과 사용하려는 기능에 따라 다릅니다.

라이센스	필요한 경우
SnapCenter 표준 컨트롤러 기반	FAS, AFF, All SAN 어레이(ASA)에 필요 SnapCenter 표준 라이센스는 컨트롤러 기반 라이센스이며 프리미엄 번들의 일부로 포함됩니다. SnapManager 제품군 라이센스가 있는 경우 SnapCenter 표준 라이센스 사용 권한도 제공됩니다. FAS, AFF 또는 ASA 스토리지를 사용하여 평가판을 통해 SnapCenter를 설치하려는 경우, 세일즈 담당자에게 문의하여 프리미엄 번들 평가 라이센스를 얻을 수 있습니다. SnapCenter는 데이터 보호 번들의 일부로 제공됩니다. A400 이상을 구입한 경우 데이터 보호 번들을 구입해야 합니다.
SnapCenter 표준 용량 기반	ONTAP Select 및 Cloud Volumes ONTAP에 필요합니다 Cloud Volumes ONTAP 또는 ONTAP Select 고객인 경우 SnapCenter에서 관리하는 데이터를 기준으로 TB당 용량 기반 라이센스를 구입해야 합니다. 기본적으로 SnapCenter는 90일 100TB SnapCenter 표준 용량 기반 평가판 라이센스를 기본 제공합니다. 자세한 내용은 세일즈 담당자에게 문의하십시오.
SnapMirror 또는 SnapVault	ONTAP SnapCenter에서 복제를 사용하는 경우 SnapMirror 또는 SnapVault 라이센스가 필요합니다.
SnapRestore	백업을 복원 및 확인하는 데 필요합니다. 지원합니다 • SnapVault 대상 시스템에서 원격 검증을 수행하고 백업에서 복원하는 데 필요합니다. • SnapMirror 대상 시스템에서 원격 검증을 수행하는 데 필요합니다.
플랙스클론	데이터베이스 클론 생성 및 검증 작업에 필요합니다. 지원합니다 • SnapVault 대상 시스템에서 보조 볼트 백업에서 클론을 생성하는 데 필요합니다. • SnapMirror 대상 시스템에서 보조 SnapMirror 백업에서 클론을 생성해야 합니다.

라이센스	필요한 경우
프로토콜	• LUN에 대한 iSCSI 또는 FC 라이센스 • SMB 공유용 CIFS 라이센스 • NFS 유형 VMDK에 대한 NFS 라이센스 • VMFS 유형 VMDK에 대한 iSCSI 또는 FC 라이센스 소스 볼륨을 사용할 수 없는 경우 데이터를 제공하는 SnapMirror 대상 시스템에 필요합니다.
SnapCenter 표준 라이센스(선택 사항)	보조 대상 SnapCenter 표준 라이센스를 보조 대상에 추가하는 것이 좋지만 필수는 아닙니다. 보조 대상에서 SnapCenter 표준 라이센스가 활성화되어 있지 않으면 페일오버 작업을 수행한 후 SnapCenter를 사용하여 보조 대상의 리소스를 백업할 수 없습니다. 그러나 복제 및 검증 작업을 수행하려면 보조 대상에 FlexClone 라이센스가 필요합니다.

SnapCenter 고급 및 SnapCenter NAS 파일 서비스 라이센스는 더 이상 사용되지 않으며 더 이상 사용할 수 없습니다.

하나 이상의 SnapCenter 라이센스를 설치해야 합니다. 라이센스를 추가하는 방법에 대한 자세한 내용은 을 참조하십시오 "SnapCenter 표준 컨트롤러 기반 라이센스를 추가합니다" 또는 "SnapCenter 표준 용량 기반 라이센스 추가".

SMBR(Single Mailbox Recovery) 라이센스

Exchange용 SnapCenter 플러그인을 사용하여 Microsoft Exchange Server 데이터베이스 및 SMBR(Single Mailbox Recovery)을 관리하는 경우 사용자 메일박스를 기준으로 별도로 구입해야 하는 SMBR용 추가 라이센스가 필요합니다.

NetApp ® Single Mailbox Recovery는 2023년 5월 12일 EOA(End of Availability)로 제공됩니다. 자세한 내용은 을 참조하십시오 "CPC-00507". NetApp은 2020년 6월 24일에 출시된 마케팅 부품 번호를 통해 지원 자격 기간 동안 메일박스 용량, 유지보수, 지원을 구매한 고객을 계속 지원할 예정입니다.

NetApp Single Mailbox Recovery는 Ontrack에서 제공하는 파트너 제품입니다. OnTrack PowerControls는 NetApp Single Mailbox Recovery와 유사한 기능을 제공합니다. 고객은 2023년 5월 12일 EOA 날짜 이후에 세분화된 메일박스 복구를 위해 Ontrack(licensingteam@ontrack.com 통해 Ontrack PowerControls 소프트웨어 라이센스와 Ontrack PowerControls 유지 관리 및 지원 갱신을 조달할 수 있습니다.

자격 증명에 대한 인증 방법입니다

자격 증명은 응용 프로그램이나 환경에 따라 다른 인증 방법을 사용합니다. 자격 증명은 SnapCenter 작업을 수행할 수 있도록 사용자를 인증합니다. 플러그인 설치를 위한 자격 증명 세트와 데이터 보호 작업을 위한 다른 자격 증명 세트를 생성해야 합니다.

Windows 인증

Windows 인증 방법은 Active Directory에 대해 인증합니다. Windows 인증의 경우 Active Directory는 SnapCenter 외부에서 설정됩니다. SnapCenter는 추가 구성 없이 인증합니다. 호스트 추가, 플러그인 패키지 설치 및 작업 예약 등의 작업을 수행하려면 Windows 자격 증명이 필요합니다.

신뢰할 수 없는 도메인 인증입니다

SnapCenter를 사용하면 신뢰할 수 없는 도메인에 속하는 사용자 및 그룹을 사용하여 Windows 자격 증명을 만들 수 있습니다. 인증에 성공하려면 신뢰할 수 없는 도메인을 SnapCenter에 등록해야 합니다.

로컬 워크그룹 인증

SnapCenter를 사용하면 로컬 작업 그룹 사용자 및 그룹을 사용하여 Windows 자격 증명을 생성할 수 있습니다. 로컬 작업 그룹 사용자 및 그룹에 대한 Windows 인증은 Windows 자격 증명 생성 시 수행되지 않지만 호스트 등록 및 기타 호스트 작업이 수행될 때까지 지연됩니다.

SQL Server 인증

SQL 인증 메서드는 SQL Server 인스턴스에 대해 인증합니다. 즉, SnapCenter에서 SQL Server 인스턴스를 검색한 다음 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.

Linux 인증

Linux 인증 방법은 Linux 호스트에 대해 인증합니다. Linux 호스트를 추가하고 SnapCenter GUI에서 Linux용 SnapCenter 플러그인 패키지를 원격으로 설치하는 초기 단계 동안 Linux 인증이 필요합니다.

AIX 인증

AIX 인증 방법은 AIX 호스트에 대해 인증합니다. AIX 호스트를 추가하고 SnapCenter GUI에서 AIX용 SnapCenter 플러그인 패키지를 원격으로 설치하는 초기 단계 동안 AIX 인증이 필요합니다.

Oracle 데이터베이스 인증

Oracle 데이터베이스 인증 방법은 Oracle 데이터베이스에 대해 인증합니다. 데이터베이스 호스트에서 운영 체제(OS) 인증이 비활성화되어 있는 경우 Oracle 데이터베이스에서 작업을 수행하려면 Oracle 데이터베이스 인증이 필요합니다. 따라서 Oracle 데이터베이스 자격 증명을 추가하기 전에 sysdba 권한을 사용하여 Oracle 데이터베이스에 Oracle 사용자를 생성해야 합니다.

Oracle ASM 인증

Oracle ASM 인증 방법은 Oracle ASM(Automatic Storage Management) 인스턴스에 대해 인증합니다. Oracle ASM 인스턴스에 액세스해야 하고 데이터베이스 호스트에서 운영 체제(OS) 인증이 비활성화된 경우 Oracle ASM 인증이 필요합니다. 따라서 Oracle ASM 자격 증명을 추가하기 전에 ASM 인스턴스에서 sysasm 권한을 가진 Oracle 사용자를 생성해야 합니다.

RMAN 카탈로그 인증

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

추가해야 합니다.

스토리지 접속 및 자격 증명

데이터 보호 작업을 수행하기 전에 스토리지 접속을 설정하고 SnapCenter 서버 및 SnapCenter 플러그인에서 사용할 자격 증명을 추가해야 합니다.

- * 스토리지 연결 *

  스토리지 접속을 통해 SnapCenter 서버 및 SnapCenter 플러그인이 ONTAP 스토리지를 액세스할 수 있습니다. 이러한 연결을 설정하려면 AutoSupport 및 이벤트 관리 시스템(EMS) 기능도 구성해야 합니다.

- 자격 증명 *

  - 도메인 관리자 또는 관리자 그룹의 구성원

    SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹의 구성원을 지정합니다. 사용자 이름 필드에 유효한 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 제공 로컬 관리자를 지정합니다. 사용자 계정에 상승된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다.

  사용자 이름 필드의 올바른 형식은 _ 사용자 이름 _ 입니다

  - 개별 리소스 그룹에 대한 자격 증명

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

멀티팩터 인증(MFA)

멀티팩터 인증(MFA) 관리

AD FS(Active Directory Federation Service) 서버 및 SnapCenter 서버에서 MFA(Multi-Factor Authentication) 기능을 관리할 수 있습니다.

멀티팩터 인증(MFA) 활성화

PowerShell 명령을 사용하여 SnapCenter Server에 MFA 기능을 사용하도록 설정할 수 있습니다.

이 작업에 대해

- SnapCenter는 다른 애플리케이션이 동일한 AD FS에 구성되어 있을 때 SSO 기반 로그인을 지원합니다. 특정 AD FS 구성에서 SnapCenter는 AD FS 세션 지속성에 따라 보안상의 이유로 사용자 인증을 요구할 수 있습니다.

- cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 를 실행하여 얻을 수 있습니다 `Get-Help command_name`. 또는 를 볼 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

시작하기 전에

- Windows AD FS(Active Directory Federation Service)가 해당 도메인에서 실행 중이어야 합니다.
- Azure MFA, Cisco Duo 등과 같은 AD FS 지원 다중 요소 인증 서비스가 있어야 합니다.
- SnapCenter 및 AD FS 서버 타임 스탬프는 시간대와 상관없이 동일해야 합니다.
- SnapCenter 서버에 대해 승인된 CA 인증서를 조달하고 구성합니다.

  CA 인증서는 다음과 같은 이유로 필수입니다.

  - 자체 서명된 인증서가 노드 수준에서 고유하므로 ADFS-F5 통신이 끊어지지 않도록 합니다.
  - 독립 실행형 또는 고가용성 구성에서 업그레이드, 복구 또는 재해 복구(DR) 중에 자체 서명된 인증서가 다시 만들어지지 않으므로 MFA 재구성이 방지됩니다.
  - IP-FQDN 해상도를 확인합니다.

    CA 인증서에 대한 자세한 내용은 을 참조하십시오 "CA 인증서 CSR 파일을 생성합니다".

단계

1. AD FS(Active Directory Federation Services) 호스트에 연결합니다.
2. 에서 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 관리자로 SnapCenter 서버에 로그인합니다.
5. PowerShell 세션을 사용하여 _New-SmMultactorAuthenticationMetadata-path_cmdlet을 사용하여 SnapCenter MFA 메타데이터 파일을 생성합니다.

   path 매개 변수는 SnapCenter 서버 호스트에 MFA 메타데이터 파일을 저장할 경로를 지정합니다.
6. 생성된 파일을 AD FS 호스트에 복사하여 SnapCenter를 클라이언트 엔터티로 구성합니다.
7. 를 사용하여 SnapCenter 서버에 대해 MFA를 활성화합니다 `Set-SmMultiFactorAuthentication` cmdlet.
8. (선택 사항) 를 사용하여 MFA 구성 상태 및 설정을 확인합니다 `Get-SmMultiFactorAuthentication` cmdlet.
9. MMC(Microsoft Management Console)로 이동하여 다음 단계를 수행하십시오.
   a. 파일 * > * Snapin 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. SnapCenter에 바인딩된 CA 인증서를 마우스 오른쪽 단추로 클릭한 다음 * 모든 작업 * > * 개인 키 관리 * 를 선택합니다.
   f. 권한 마법사에서 다음 단계를 수행합니다.

i. 추가 * 를 클릭합니다.

ii. Locations * 를 클릭하고 관련 호스트(계층 구조의 맨 위)를 선택합니다.

iii. Locations * (위치 *) 팝업 창에서 * OK * (확인 *)를 클릭합니다.

iv. 개체 이름 필드에 'IIS_IUSRS'를 입력하고 * 이름 확인 * 을 클릭한 다음 * 확인 * 을 클릭합니다.

검사가 성공적으로 완료되면 * OK * 를 클릭합니다.

10. AD FS 호스트에서 AD FS 관리 마법사를 열고 다음 단계를 수행합니다.
    a. '신뢰할 수 있는 당사자'를 마우스 오른쪽 버튼으로 클릭 * > * '신뢰할 수 있는 당사자 신뢰 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 기본 설정으로 설정을 선택합니다.
    f. 마침 * 을 클릭합니다.

    SnapCenter는 이제 제공된 표시 이름을 가진 의존자로 반영됩니다.

11. 이름을 선택하고 다음 단계를 수행하십시오.
    a. 청구 발급 정책 편집 * 을 클릭합니다.
    b. 규칙 추가 * 를 클릭하고 * 다음 * 을 클릭합니다.
    c. 청구 규칙의 이름을 지정합니다.
    d. 속성 저장소로 * Active Directory * 를 선택합니다.
    e. 속성을 * User-Principal-Name * 으로 선택하고 발신 클레임 유형을 * Name-ID * 로 선택합니다.
    f. 마침 * 을 클릭합니다.
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. 메타데이터를 성공적으로 가져왔는지 확인하려면 다음 단계를 수행하십시오.
    a. 신뢰할 수 있는 상대 신뢰를 마우스 오른쪽 단추로 클릭하고 * 속성 * 을 선택합니다.
    b. 끝점, 식별자 및 서명 필드가 채워져 있는지 확인합니다.
14. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성 세션 쿠키를 지우고 다시 로그인합니다.

SnapCenter MFA 기능은 REST API를 사용하여 활성화할 수도 있습니다.

문제 해결에 대한 자세한 내용은 을 참조하십시오 "여러 탭에서 동시 로그인 시도 시 MFA 오류가 표시됩니다".

AD FS MFA 메타데이터를 업데이트합니다

AD FS 서버에 업그레이드, CA 인증서 갱신, DR 등과 같은 수정 사항이 있을 때마다 SnapCenter에서 AD FS MFA 메타데이터를 업데이트해야 합니다.

단계

1. 에서 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 SnapCenter에서 AD FS 메타데이터를 업데이트합니다.

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

4. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성 세션 쿠키를 지우고 다시 로그인합니다.

SnapCenter MFA 메타데이터를 업데이트합니다

복구, CA 인증서 갱신, DR 등과 같은 ADFS 서버에 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. 사용 당사자 신뢰 * 를 클릭합니다.
   b. SnapCenter에 대해 만든 기반 당사자 신뢰를 마우스 오른쪽 단추로 클릭하고 * 삭제 * 를 클릭합니다.

      신뢰할 수 있는 사용자의 사용자 정의 이름이 표시됩니다.

   c. MFA(Multi-factor Authentication)를 활성화합니다.

      을 참조하십시오 "다중 요소 인증을 활성화합니다".
2. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성 세션 쿠키를 지우고 다시 로그인합니다.

MFA(Multi-Factor Authentication) 비활성화

단계

1. MFA를 비활성화하고 를 사용하여 MFA를 활성화했을 때 생성된 구성 파일을 정리합니다 `Set-SmMultiFactorAuthentication` cmdlet.
2. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성 세션 쿠키를 지우고 다시 로그인합니다.

REST API, PowerShell 및 SCCLI를 사용하여 MFA(Multi-Factor Authentication)를 관리합니다

MFA 로그인은 브라우저, REST API, PowerShell 및 SCCLI에서 지원됩니다. MFA는 AD FS ID 관리자를 통해 지원됩니다. GUI, REST API, PowerShell 및 SCCLI에서 MFA를 사용하도록 설정하고 MFA를 사용하지 않도록 설정하고 MFA를 구성할 수 있습니다.

AD FS를 **OAuth/OIDC**로 설정합니다

- 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 단추로 클릭합니다.
     b. 응용 프로그램 그룹 추가 * 를 선택하고 * 응용 프로그램 이름 * 을 입력합니다.
     c. 서버 응용 프로그램 * 을 선택합니다.
     d. 다음 * 을 클릭합니다.
  3. 복사 * 클라이언트 식별자 *.

     클라이언트 ID입니다.
     … 리디렉션 URL에 콜백 URL(SnapCenter 서버 URL)을 추가합니다.
     … 다음 * 을 클릭합니다.
  4. 공유 암호 생성 * 을 선택합니다.

     암호 값을 복사합니다. 클라이언트의 비밀입니다.
     … 다음 * 을 클릭합니다.
  5. 요약 * 페이지에서 * 다음 * 을 클릭합니다.
     a. 완료 * 페이지에서 * 닫기 * 를 클릭합니다.
  6. 새로 추가된 * 응용 프로그램 그룹 * 을 마우스 오른쪽 단추로 클릭하고 * 속성 * 을 선택합니다.
  7. 앱 속성에서 * 응용 프로그램 추가 * 를 선택합니다.
  8. 응용 프로그램 추가 * 를 클릭합니다.

     웹 API를 선택하고 * 다음 * 을 클릭합니다.
  9. 웹 API 구성 페이지에서 이전 단계에서 만든 SnapCenter 서버 URL 및 클라이언트 식별자를 식별자 섹션에 입력합니다.
     a. 추가 * 를 클릭합니다.
     b. 다음 * 을 클릭합니다.
  10. 액세스 제어 정책 선택 * 페이지에서 요구 사항에 따라 제어 정책(예: 모든 사용자 허용 및 MFA 필요)을 선택하고 * 다음 * 을 클릭합니다.
  11. 응용 프로그램 권한 구성 * 페이지에서 기본적으로 OpenID가 범위로 선택되어 있으면 * 다음 * 을 클릭합니다.
  12. 요약 * 페이지에서 * 다음 * 을 클릭합니다.

      완료 * 페이지에서 * 닫기 * 를 클릭합니다.
  13. 샘플 응용 프로그램 속성 * 페이지에서 * 확인 * 을 클릭합니다.
  14. 인증 서버(AD FS)에서 발급하고 리소스에서 사용하도록 의도된 JWT 토큰입니다.

      이 토큰의 'AUD' 또는 청중의 주장은 리소스 또는 웹 API의 식별자와 일치해야 합니다.

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

    OpenID Connect를 구성하여 사용자 이름을 클레임으로 제공합니다.

16. 서버 관리자 오른쪽 상단의 * 도구 * 메뉴 아래에 있는 * AD FS 관리 * 도구를 엽니다.
    a. 왼쪽 사이드바에서 * Application Groups * 폴더를 선택합니다.
    b. 웹 API를 선택하고 * edit * 를 클릭합니다.
    c. 발행 변환 규칙 탭으로 이동합니다

17. 규칙 추가 * 를 클릭합니다.
    a. 클레임 규칙 템플릿 드롭다운에서 * 청구로 LDAP 속성 보내기 * 를 선택합니다.
    b. 다음 * 을 클릭합니다.

18. 청구 규칙 * 이름을 입력합니다.
    a. 특성 저장소 드롭다운에서 * Active Directory * 를 선택합니다.
    b. LDAP 속성 * 드롭다운에서 * 사용자 - 기본 - 이름 * 을 선택하고 O * uting Claim Type * 드롭다운에서 * UPN * 을 선택합니다.
    c. 마침 * 을 클릭합니다.

PowerShell 명령을 사용하여 애플리케이션 그룹을 생성합니다

PowerShell 명령을 사용하여 애플리케이션 그룹인 웹 API를 생성하고 범위와 청구서를 추가할 수 있습니다. 이러한 명령은 자동화된 스크립트 형식으로 사용할 수 있습니다. 자세한 내용은 <link to KB article> 를 참조하십시오.

1. 다음 comamnd를 사용하여 AD FS에서 새 애플리케이션 그룹을 생성합니다.

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

   `ClientRoleIdentifier` 애플리케이션 그룹의 이름입니다

   `redirectURL` 인증 후 리디렉션에 대한 유효한 URL입니다

2. AD FS 서버 응용 프로그램을 생성하고 클라이언트 암호를 생성합니다.

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

3. ADFS 웹 API 응용 프로그램을 만들고 사용할 정책 이름을 구성합니다.

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

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

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

4. 클라이언트 ID와 클라이언트 암호는 한 번만 표시되므로 다음 명령의 출력에서 가져옵니다.

```
"client_id = $identifier"

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

5. AD FS 응용 프로그램에 allat클레임 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. 웹 API 응용 프로그램의 이름을 지정하고 외부 파일을 사용하여 발급 변환 규칙을 정의합니다.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

액세스 토큰 만료 시간을 업데이트합니다

PowerShell 명령을 사용하여 액세스 토큰 만료 시간을 업데이트할 수 있습니다.

- 이 작업에 대한 정보 *
- 액세스 토큰은 사용자, 클라이언트 및 리소스의 특정 조합에 대해서만 사용할 수 있습니다. 액세스 토큰은 해지할 수 없으며 만료까지 유효합니다.

- 기본적으로 액세스 토큰의 만료 시간은 60분입니다. 이 최소 만료 시간은 충분하고 크기가 조정됩니다. 지속적으로 발생하는 비즈니스 크리티컬 작업을 방지할 수 있는 충분한 가치를 제공해야 합니다.
- 단계 *

애플리케이션 그룹 WebAPI에 대한 액세스 토큰 만료 시간을 업데이트하려면 AD FS 서버에서 다음 명령을 사용하십시오.

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

AD FS에서 베어러 토큰을 가져옵니다

REST 클라이언트(예: Postman)에서 아래에 언급된 매개 변수를 입력해야 하며 사용자 자격 증명을 입력하라는 메시지가 표시됩니다. 또한, 베어러 토큰을 얻으려면 2차 인증 요소(보유 중인 인증 및 대상 인증)를 입력해야 합니다.

를 누릅니다
베어러 토큰의 유효성은 애플리케이션당 AD FS 서버에서 구성할 수 있으며, 기본 유효 기간은 60분입니다.

필드에 입력합니다	값
허가 유형	인증 코드
콜백 URL	콜백 URL이 없는 경우 응용 프로그램의 기본 URL을 입력합니다.
인증 URL	[ADFS-DOMAIN-NAME]/ADFS/OAuth2/authorize
액세스 토큰 URL	[ADFS-DOMAIN-NAME]/ADFS/OAuth2/TOKEN
클라이언트 ID입니다	AD FS 클라이언트 ID를 입력합니다
클라이언트 암호	AD FS 클라이언트 암호를 입력합니다
범위	OpenID를 선택합니다
클라이언트 인증	기본 AUTH 헤더로 보냅니다
리소스	고급 옵션* 탭에서 JWT 토큰에 "AUD" 값으로 제공되는 콜백 URL과 동일한 값을 가진 자원 필드를 추가합니다.

SnapCenter 서버에서 **PowerShell, SCCLI** 및 **REST API**를 사용하여 **MFA**를 구성합니다

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

SnapCenter MFA CLI 인증

PowerShell 및 SCCLI에서 베어러 토큰을 사용하여 사용자를 인증하는 데 "AccessToken"이라는 필드가 하나 더 있는 기존 cmdlet(Open-SmConnection)이 확장됩니다.

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

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

SnapCenter MFA REST API 인증

SnapCenter로부터 성공적인 응답을 얻으려면 _Authorization=Bearer <access token>_in REST API 클라이언트(예: Postman 또는 swagger)의 형식으로 베어러 토큰을 사용하고 헤더에 사용자 RoleName을 언급하십시오.

MFA REST API 워크플로우

MFA가 AD FS로 구성된 경우 액세스(베어러) 토큰을 사용하여 인증하여 REST API를 통해 SnapCenter 애플리케이션에 액세스해야 합니다.

- 이 작업에 대한 정보 *
- Postman, Swagger UI 또는 FireCamp와 같은 REST 클라이언트를 사용할 수 있습니다.
- 액세스 토큰을 가져와 후속 요청(SnapCenter REST API)을 인증하여 작업을 수행합니다.
- 단계 *
- AD FS MFA * 를 통해 인증합니다

1. 액세스 토큰을 얻기 위해 AD FS 끝점을 호출하도록 REST 클라이언트를 구성합니다.

   버튼을 눌러 응용 프로그램의 액세스 토큰을 가져오는 경우 AD FS SSO 페이지로 리디렉션됩니다. 이 페이지에서 AD 자격 증명을 제공하고 MFA로 인증해야 합니다.
   AD FS SSO 페이지에서 사용자 이름 텍스트 상자에 사용자 이름 또는 이메일을 입력합니다.

를 누릅니다
사용자 이름은 user@domain 또는 domain\user 형식으로 지정해야 합니다.

1. 암호 텍스트 상자에 암호를 입력합니다.
2. 로그인 * 을 클릭합니다.
3. 로그인 옵션 * 섹션에서 인증 옵션을 선택하고 인증(구성에 따라 다름)을 수행합니다.
   - 푸시: 휴대폰에 전송되는 푸시 알림을 승인합니다.
   - QR 코드: AUTH Point 모바일 앱을 사용하여 QR 코드를 스캔한 다음 앱에 표시된 검증 코드를 입력합니다
   - 일회용 암호: 토큰의 일회용 암호를 입력합니다.
4. 인증에 성공하면 액세스, ID 및 토큰 새로 고침이 포함된 팝업이 열립니다.

   액세스 토큰을 복사하고 SnapCenter REST API에서 사용하여 작업을 수행합니다.

5. REST API에서는 헤더 섹션에서 액세스 토큰 및 역할 이름을 전달해야 합니다.
6. SnapCenter는 AD FS에서 이 액세스 토큰을 검증합니다.

유효한 토큰인 경우 SnapCenter는 해당 토큰을 디코딩하고 사용자 이름을 가져옵니다.

7. SnapCenter는 사용자 이름과 역할 이름을 사용하여 API 실행을 위해 사용자를 인증합니다.

   인증에 성공하면 SnapCenter가 결과를 반환하고 그렇지 않으면 오류 메시지가 표시됩니다.

REST API, CLI 및 **GUI**에 대해 **SnapCenter MFA** 기능을 사용하거나 사용하지 않도록 설정합니다

- GUI *
- 단계 *
  1. SnapCenter 서버에 SnapCenter 관리자로 로그인합니다.
  2. 설정 * > * 글로벌 설정 * > * 멀티팩터인증(MFA) 설정 * 을 클릭합니다
  3. 인터페이스(GUI/RST API/CLI)를 선택하여 MFA 로그인을 활성화하거나 비활성화합니다.
- PowerShell 인터페이스 *
- 단계 *
  1. GUI, REST API, PowerShell 및 SCCLI에 대해 MFA를 사용하도록 PowerShell 또는 CLI 명령을 실행합니다.

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

     path 매개 변수는 AD FS MFA 메타데이터 XML 파일의 위치를 지정합니다.

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

  1. 를 사용하여 MFA 구성 상태 및 설정을 확인합니다 `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 대해 MFA를 사용하도록 다음 POST API를 실행합니다.

매개 변수	값
요청된 URL입니다	/api/4.9/settings/multipactorauthentication을 참조하십시오
HTTP 메소드	게시

요청 본문	{
	"IsGuiMFAEnabled": false,
	"IsRestApiMFAEnabled": 참,
	"IsCliMFAEnabled": false,
	"ADFSConfigFilePath":"C:\\ADFS_METADATA\\abc.xml"
	}

응답 본문	{
	"MFAConfiguration":{을 참조하십시오
	"IsGuiMFAEnabled": false,
	"ADFSConfigFilePath":"C:\\ADFS_METADATA\\abc.xml",
	"SCConfigFilePath": null,
	"IsRestApiMFAEnabled": 참,
	"IsCliMFAEnabled": false,
	"ADFSHostName":"win-adfs-sc49.winscedom2.com"
	}
	}

2. 다음 API를 사용하여 MFA 구성 상태 및 설정을 확인합니다.

매개 변수	값
요청된 URL입니다	/api/4.9/settings/multipactorauthentication을 참조하십시오
HTTP 메소드	가져오기

응답 본문	{
	"MFAConfiguration":{을 참조하십시오
	"IsGuiMFAEnabled": false,
	"ADFSConfigFilePath":"C:\\ADFS_METADATA\\abc.xml",
	"SCConfigFilePath": null,
	"IsRestApiMFAEnabled": 참,
	"IsCliMFAEnabled": false,
	"ADFSHostName":"win-adfs-sc49.winscedom2.com"
	}
	}

SnapCenter 서버를 설치합니다

SnapCenter 서버 설치 관리자 실행 파일을 실행하여 SnapCenter 서버를 설치할 수 있습니다.

필요에 따라 PowerShell cmdlet을 사용하여 몇 가지 설치 및 구성 절차를 수행할 수 있습니다.

명령줄에서 SnapCenter 서버를 자동 설치하는 것은 지원되지 않습니다.

시작하기 전에

- SnapCenter 서버 호스트는 시스템 재시작을 보류하지 않고 Windows 업데이트를 최신 상태로 유지해야 합니다.
- SnapCenter 서버를 설치하려는 호스트에 MySQL Server가 설치되어 있지 않은지 확인해야 합니다.
- Windows 설치 관리자 디버깅을 사용하도록 설정해야 합니다.

  활성화에 대한 자세한 내용은 Microsoft 웹 사이트를 참조하십시오 "Windows 설치 관리자 로깅".

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

- 단계 *

1. 에서 SnapCenter 서버 설치 패키지를 다운로드합니다 "NetApp Support 사이트".
2. 다운로드한 .exe 파일을 두 번 클릭하여 SnapCenter 서버 설치를 시작합니다.

   설치를 시작한 후 모든 사전 점검을 수행하고 최소 요구사항을 충족하지 못할 경우 적절한 오류 또는 경고 메시지가 표시됩니다.

   경고 메시지를 무시하고 설치를 진행할 수 있지만 오류를 수정해야 합니다.

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

   MySQL Server 리포지토리 데이터베이스의 암호를 지정할 필요가 없습니다. SnapCenter 서버 설치 중에 암호는 자동으로 생성됩니다.

   특수 문자 ""%" is not supported in the custom path for the repository database. If you include "%"" 경로에서 설치에 실패했습니다.

4. 지금 설치 * 를 클릭합니다.

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

   Cancel * 버튼을 클릭하면 실행 중인 단계가 완료된 후 롤백 작업을 시작합니다. SnapCenter 서버가 호스트에서 완전히 제거됩니다.

   그러나 "SnapCenter 서버 사이트 재시작" 또는 "SnapCenter 서버 시작 대기 중" 작업이 수행 중일 때 * 취소 * 를 클릭하면 작업을 취소하지 않고 설치가 진행됩니다.

로그 파일은 항상 관리자 사용자의 %temp% 폴더에 (가장 오래된 파일 먼저) 나열됩니다. 로그 위치를 리디렉션하려면 다음을 실행하여 명령 프롬프트에서 SnapCenter 서버 설치를 시작합니다 .`C:\installer_location\installer_name.exe /log"C:\"`

RBAC 승인을 사용하여 SnapCenter에 로그인합니다

SnapCenter는 역할 기반 액세스 제어(RBAC)를 지원합니다. SnapCenter 관리자는

SnapCenter RBAC를 통해 역할 및 리소스를 작업 그룹 또는 Active Directory의 사용자 또는 Active Directory의 그룹에 할당합니다. 이제 RBAC 사용자는 할당된 역할을 사용하여 SnapCenter에 로그인할 수 있습니다.

시작하기 전에

- Windows Server Manager에서 WAS(Windows Process Activation Service)를 활성화해야 합니다.
- Internet Explorer를 브라우저로 사용하여 SnapCenter 서버에 로그인하려면 Internet Explorer의 보호 모드가 비활성화되어 있어야 합니다.
- 이 작업에 대한 정보 *

설치 중에 SnapCenter 서버 설치 마법사가 바로 가기를 만들어 SnapCenter가 설치된 호스트의 바탕 화면과 시작 메뉴에 배치합니다. 또한 설치 완료 시 설치 마법사는 설치 중에 제공한 정보를 기반으로 SnapCenter URL을 표시하며, 원격 시스템에서 로그인하려는 경우 이 URL을 복사할 수 있습니다.

웹 브라우저에 여러 개의 탭이 열려 있는 경우 SnapCenter 브라우저 탭을 닫아도 SnapCenter에서 로그아웃되지 않습니다. SnapCenter와의 연결을 종료하려면 * 로그아웃 * 단추를 클릭하거나 전체 웹 브라우저를 닫아 SnapCenter에서 로그아웃해야 합니다.

모범 사례**:** 보안상의 이유로 브라우저에서 SnapCenter 암호를 저장하지 않는 것이 좋습니다.

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

HA(고가용성) 구축을 위해서는 가상 클러스터 IP_\https://Virtual_Cluster_IP_or_FQDN:8146_.를 사용하여 SnapCenter에 액세스해야 합니다 Internet Explorer(IE)에서 _\https://Virtual_Cluster_IP_or_FQDN:8146_로 이동할 때 SnapCenter UI가 표시되지 않으면 각 플러그인 호스트의 IE에 가상 클러스터 IP 주소 또는 FQDN을 신뢰할 수 있는 사이트로 추가하거나 각 플러그인 호스트에서 IE 고급 보안을 해제해야 합니다.
자세한 내용은 을 참조하십시오 "외부 네트워크에서 클러스터 IP 주소에 액세스할 수 없습니다".

SnapCenter GUI 사용 외에도 PowerShell cmdlet을 사용하여 스크립트를 생성하여 구성, 백업 및 복원 작업을 수행할 수 있습니다. 일부 cmdlet은 SnapCenter 릴리즈마다 변경될 수 있습니다. 를 클릭합니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드" 세부 정보가 있습니다.

SnapCenter에 처음 로그인하는 경우 설치 프로세스 중에 제공한 자격 증명을 사용하여 로그인해야 합니다.

- 단계 *

1. 로컬 호스트 데스크톱에 있는 바로 가기나 설치 마지막에 제공된 URL 또는 SnapCenter 관리자가 제공한 URL에서 SnapCenter를 실행합니다.
2. 사용자 자격 증명을 입력합니다.

다음을 지정하려면...	다음 형식 중 하나를 사용합니다...
도메인 관리자	• NetBIOS\사용자 이름입니다 • 사용자 이름@UPN 접미사 예: username@netapp.com • 도메인 FQDN\사용자 이름입니다
로컬 관리자	사용자 이름

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

   로그인한 후 현재 사용자 및 관련 역할이 SnapCenter의 오른쪽 상단에 표시됩니다.

결과 *

대시보드 페이지가 표시됩니다.

사이트에 연결할 수 없다는 오류로 인해 로깅이 실패하는 경우 SSL 인증서를 SnapCenter에 매핑해야 합니다. "자세한 정보"

- 완료 후 *

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

SnapCenter에서 지원할 신뢰할 수 없는 Active Directory 도메인이 있는 경우 신뢰할 수 없는 도메인의 사용자에 대한 역할을 구성하기 전에 해당 도메인을 SnapCenter에 등록해야 합니다. "자세한 정보"

멀티팩터 인증(MFA)을 사용하여 SnapCenter에 로그인

SnapCenter 서버는 Active Directory의 일부인 도메인 계정에 대해 MFA를 지원합니다.

시작하기 전에

- MFA를 활성화해야 합니다.

  MFA를 사용하는 방법에 대한 자세한 내용은 을 참조하십시오 "다중 요소 인증을 활성화합니다"

- 이 작업에 대한 정보 *
- FQDN만 지원됩니다
- 작업 그룹 및 도메인 간 사용자는 MFA를 사용하여 로그인할 수 없습니다
- 단계 *

1. 로컬 호스트 데스크톱에 있는 바로 가기나 설치 마지막에 제공된 URL 또는 SnapCenter 관리자가 제공한 URL에서 SnapCenter를 실행합니다.
2. AD FS 로그인 페이지에서 사용자 이름 및 암호 를 입력합니다.

   AD FS 페이지에 잘못된 사용자 이름 또는 암호 오류 메시지가 표시되면 다음을 확인해야 합니다.

- 사용자 이름 또는 암호가 유효한지 여부를 나타냅니다

  사용자 계정이 AD(Active Directory)에 있어야 합니다.

- AD에 설정된 최대 허용 시도 횟수를 초과했는지 여부
- AD 및 AD FS의 가동 및 실행 여부를 나타냅니다

SnapCenter 기본 GUI 세션 시간 초과를 수정합니다

SnapCenter GUI 세션 제한 시간을 기본 제한 시간 20분 이하로 수정할 수 있습니다.

SnapCenter는 기본 15분 동안 비활성 상태가 지속되면 GUI 세션에서 5분 후에 로그아웃된다는 경고 메시지를 보안 기능으로 표시합니다. 기본적으로 SnapCenter는 20분 동안 비활성 상태가 지속되면 GUI 세션에서 로그아웃하고 다시 로그인해야 합니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 설정 * > * 글로벌 설정 * 을 클릭합니다.
  2. 전역 설정 페이지에서 * 구성 설정 * 을 클릭합니다.
  3. Session Timeout(세션 시간 초과) 필드에 새 세션 시간 제한을 분 단위로 입력한 다음 * Save * (저장 *)를 클릭합니다.

SSL 3.0을 비활성화하여 SnapCenter 웹 서버를 보호합니다

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

SSL 3.0 프로토콜에 결함이 있어 공격자가 연결 장애를 일으키거나 중간자 공격을 수행하여 웹 사이트와 방문자 사이의 암호화 트래픽을 관찰할 수 있습니다.

- 단계 *
  1. SnapCenter 웹 서버 호스트에서 레지스트리 편집기를 시작하려면 * 시작 * > * 실행 * 을 클릭하고 regedit를 입력합니다.
  2. 레지스트리 편집기에서 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols\SSL 3.0\로 이동합니다.
     - 서버 키가 이미 있는 경우:
       i. 사용 DWORD를 선택한 다음 * 편집 * > * 수정 * 을 클릭합니다.
       ii. 값을 0으로 변경한 다음 * 확인 * 을 클릭합니다.
     - 서버 키가 없는 경우:
       i. 편집 * > * 새로 만들기 * > * 키 * 를 클릭한 다음 키 서버의 이름을 지정합니다.
       ii. 새 서버 키를 선택한 상태에서 * 편집 * > * 새로 만들기 * > * DWORD * 를 클릭합니다.
       iii. 새 DWORD Enabled의 이름을 지정한 다음 0을 값으로 입력합니다.
  3. 레지스트리 편집기를 닫습니다.

CA 인증서를 구성합니다

CA 인증서 CSR 파일을 생성합니다

CSR(인증서 서명 요청)을 생성하고 생성된 CSR을 사용하여 CA(인증 기관)에서 가져올 수 있는 인증서를 가져올 수 있습니다. 인증서에 연결된 개인 키가 있습니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.

CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 자세한 내용은 을 참조하십시오 "CA 인증서 CSR 파일을 생성하는 방법".

도메인(* .domain.company.com) 또는 시스템(machine1.domain.company.com CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter를 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN) 및 해당 호스트 이름을 CA 인증서에 언급해야 합니다. 인증서를 조달하기 전에 SAN(Subject Alternative Name) 필드를 채워 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(* .domain.company.com)의 경우 인증서에 도메인의 모든 호스트 이름이 암시적으로 포함됩니다.

CA 인증서를 가져옵니다

MMC(Microsoft Management Console)를 사용하여 CA 인증서를 SnapCenter 서버 및 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 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 단추로 클릭한 다음 * 모든 작업 * > * 가져오기 * 를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료합니다.

이 마법사 창에서...	다음을 수행합니다.
개인 키를 가져옵니다	예 * 옵션을 선택하고 개인 키를 가져온 다음 * 다음 * 을 클릭합니다.
파일 형식 가져오기	변경하지 않고 * 다음 * 을 클릭합니다.
보안	내보낸 인증서에 사용할 새 암호를 지정하고 * 다음 * 을 클릭합니다.

이 마법사 창에서...	다음을 수행합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

인증서 가져오기는 개인 키와 함께 번들로 제공됩니다(지원되는 형식은 *.pfx, *.p12 및 *.p7b 입니다).

7. "개인" 폴더에 대해 5단계를 반복합니다.

CA 인증서 지문을 받습니다

인증서 thumbprint는 인증서를 식별하는 16진수 문자열입니다. 썸프린트는 썸프린트 알고리즘을 사용하여 인증서 컨텐츠에서 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.
   a. 인증서를 두 번 클릭합니다.
   b. 인증서 대화 상자에서 * 세부 정보 * 탭을 클릭합니다.
   c. 필드 목록을 스크롤하여 * Thumbprint * 를 클릭합니다.
   d. 상자에서 16진수 문자를 복사합니다.
   e. 16진수 사이의 공백을 제거합니다.

      예를 들어, 썸프린트가 "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 0d 42 77 A3 2a 7b"인 경우 공백을 제거한 후 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.
   a. 다음 명령을 실행하여 설치된 인증서의 엄지손가락 지문을 나열하고 최근 설치된 인증서를 주체 이름으로 식별합니다.

      Get-ChildItem-Path 인증:*LocalMachine\My*

   b. 엄지손가락 지문을 복사합니다.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서를 구성합니다

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스를 사용하여 CA 인증서를 구성해야 합니다.

SnapCenter 서버 및 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하여 기존 인증서 바인딩을 제거합니다.

```
> netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
```

예를 들면 다음과 같습니다.

```
 > netsh http delete sslcert ipport=0.0.0.0:8145
```

. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스와 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 들면 다음과 같습니다.

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

SnapCenter 사이트를 사용하여 CA 인증서를 구성합니다

Windows 호스트에서 SnapCenter 사이트를 사용하여 CA 인증서를 구성해야 합니다.

- 단계 *
  1. SnapCenter가 설치된 Windows 서버에서 IIS 관리자를 엽니다.
  2. 왼쪽 탐색 창에서 * 연결 * 을 클릭합니다.
  3. 서버 이름과 * 사이트 * 를 확장합니다.
  4. SSL 인증서를 설치할 SnapCenter 웹 사이트를 선택합니다.
  5. 작업 * > * 사이트 편집 * 으로 이동하여 * 바인딩 * 을 클릭합니다.
  6. 바인딩 페이지에서 https*에 대한 * 바인딩을 선택합니다.
  7. 편집 * 을 클릭합니다.
  8. SSL 인증서 드롭다운 목록에서 최근에 가져온 SSL 인증서를 선택합니다.
  9. 확인 * 을 클릭합니다.

최근에 배포된 CA 인증서가 드롭다운 메뉴에 나열되지 않으면 CA 인증서가 개인 키와 연결되어 있는지 확인합니다.

다음 경로를 사용하여 인증서를 추가해야 합니다. * 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > 인증서 *.

SnapCenter에 대해 CA 인증서를 활성화합니다

CA 인증서를 구성하고 SnapCenter 서버에 대해 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 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 를 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

- 단계 *
  1. 설정 페이지에서 * 설정 * > * 글로벌 설정 * > * CA 인증서 설정 * 으로 이동합니다.
  2. 인증서 유효성 검사 사용 * 을 선택합니다.
  3. 적용 * 을 클릭합니다.
- 완료 후 *

관리 호스트 탭 호스트에는 자물쇠가 표시되고 자물쇠 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- 는 활성화된 CA 인증서가 없거나 플러그인 호스트에 할당되어 있지 않음을 나타냅니다.
- CA 인증서의 유효성을 확인했음을 나타냅니다.
- CA 인증서의 유효성을 확인할 수 없음을 나타냅니다.
- 연결 정보를 검색할 수 없음을 나타냅니다.

상태가 노란색 또는 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

양방향 SSL 통신을 구성하고 사용하도록 설정합니다

양방향 SSL 통신을 구성합니다

SnapCenter 서버와 플러그인 간의 상호 통신을 보호하려면 양방향 SSL 통신을 구성해야 합니다.

- 시작하기 전에 *
- 지원되는 최소 키 길이가 3072인 CA 인증서 CSR 파일을 생성해야 합니다.
- CA 인증서는 서버 인증 및 클라이언트 인증을 지원해야 합니다.
- 개인 키와 지문 세부 정보가 포함된 CA 인증서가 있어야 합니다.
- 단방향 SSL 구성을 활성화해야 합니다.

  자세한 내용은 을 참조하십시오 "CA 인증서 구성 섹션을 참조하십시오."

- 모든 플러그인 호스트와 SnapCenter 서버에서 양방향 SSL 통신을 활성화해야 합니다.

일부 호스트 또는 서버가 양방향 SSL 통신에 사용되지 않는 환경은 지원되지 않습니다.

- 단계 *

1. 포트를 바인딩하려면 SnapCenter IIS 웹 서버 포트 8146(기본값)용 SnapCenter 서버 호스트에서 다음 단계를 수행하고 PowerShell 명령을 사용하여 SMCore 포트 8145(기본값)에 대해 다시 한 번 수행합니다.

   a. 다음 PowerShell 명령을 사용하여 기존 SnapCenter 자체 서명된 인증서 포트 바인딩을 제거합니다.

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
      ```

      예를 들면, 다음과 같습니다.

      ```
      > 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 서버 및 SMCore 포트와 바인딩합니다.

      ```
      > $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 들면, 다음과 같습니다.

      ```
      > $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 조달된 CA 인증서에 액세스하여 인증서 권한 목록에 SnapCenter의 기본 IIS 웹 서버 사용자 "* IIS AppPool\SnapCenter*"를 추가합니다.

   a. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * SnapIn 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 선택합니다.

f. 사용자 추가\권한 마법사를 시작하려면 CA 인증서를 마우스 오른쪽 버튼으로 클릭하고 * 모든 작업 * > * 개인 키 관리 * 를 선택합니다.

g. 추가 * 를 클릭하고 사용자 및 그룹 선택 마법사에서 위치를 로컬 컴퓨터 이름으로 변경합니다(계층 구조에서 맨 위).

h. IIS AppPool\SnapCenter 사용자를 추가하고 모든 제어 권한을 제공합니다.

3. CA 인증서 IIS 권한*의 경우 다음 경로에서 SnapCenter 서버의 새 DWORD 레지스트리 키 항목을 추가합니다.

   Windows 레지스트리 편집기에서 아래 경로로 이동합니다.

   ```
   HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv
   ders\SCHANNEL
   ```

4. SChannel 레지스트리 구성의 컨텍스트에서 새 DWORD 레지스트리 키 항목을 만듭니다.

   ```
   SendTrustedIssuerList = 0

ClientAuthTrustMode = 2
   ```

양방향 **SSL** 통신을 위해 **SnapCenter Windows** 플러그인을 구성합니다

PowerShell 명령을 사용하여 양방향 SSL 통신을 위해 SnapCenter Windows 플러그인을 구성해야 합니다.

- 시작하기 전에 *

CA 인증서 지문을 사용할 수 있는지 확인합니다.

- 단계 *

1. 포트를 바인딩하려면 Windows 플러그인 호스트에서 SMCore 포트 8145(기본값)에 대해 다음 작업을 수행합니다.

   a. 다음 PowerShell 명령을 사용하여 기존 SnapCenter 자체 서명된 인증서 포트 바인딩을 제거합니다.

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
      ```

      예를 들면, 다음과 같습니다.

      ```
      > netsh http delete sslcert ipport=0.0.0.0:8145
      ```

   b. 새로 조달한 CA 인증서를 SMCore 포트와 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 들면, 다음과 같습니다.

```
> $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
```

양방향 **SSL** 통신을 활성화합니다

양방향 SSL 통신을 사용하여 PowerShell 명령을 사용하여 SnapCenter 서버와 플러그인 간의 상호 통신을 보호할 수 있습니다.

- 시작하기 전에 *

모든 플러그인 및 SMCore 에이전트에 대한 명령을 먼저 실행한 다음 서버에 대해 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"}
```

1. 다음 명령을 사용하여 IIS SnapCenter 응용 프로그램 풀 재활용 작업을 수행합니다.
   `> Restart-WebAppPool -Name "SnapCenter"`
2. Windows 플러그인의 경우 다음 PowerShell 명령을 실행하여 SMCore 서비스를 다시 시작합니다.

```
> Restart-Service -Name SnapManagerCoreService
```

양방향 **SSL** 통신을 비활성화합니다

PowerShell 명령을 사용하여 양방향 SSL 통신을 사용하지 않도록 설정할 수 있습니다.

- 이 작업에 대한 정보 *

- 모든 플러그인 및 SMCore 에이전트에 대한 명령을 먼저 실행한 다음 서버에 대해 명령을 실행합니다.
- 양방향 SSL 통신을 비활성화하면 CA 인증서와 해당 구성이 제거되지 않습니다.
- SnapCenter 서버에 새 호스트를 추가하려면 모든 플러그인 호스트에 대해 양방향 SSL을 비활성화해야 합니다.
- NLB 및 F5는 지원되지 않습니다.
- 단계 *

1. 양방향 SSL 통신을 비활성화하려면 모든 플러그인 호스트 및 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"}
```

1. 다음 명령을 사용하여 IIS SnapCenter 응용 프로그램 풀 재활용 작업을 수행합니다.
   `> Restart-WebAppPool -Name "SnapCenter"`
2. Windows 플러그인의 경우 다음 PowerShell 명령을 실행하여 SMCore 서비스를 다시 시작합니다.

```
> Restart-Service -Name SnapManagerCoreService
```

인증서 기반 인증을 구성합니다

SnapCenter 서버에서 **CA(**인증 기관**)** 인증서를 내보냅니다

MMC(Microsoft Management Console)를 사용하여 SnapCenter 서버에서 플러그인 호스트로 CA 인증서를 내보내야 합니다.

시작하기 전에

양방향 SSL을 구성해야 합니다.

- 단계 *

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 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 서버에 사용되는 조달된 CA 인증서를 마우스 오른쪽 단추로 클릭한 다음 * 모든 작업 * > * 내보내기 * 를 선택하여 내보내기 마법사를 시작합니다.
6. 마법사에서 다음 작업을 수행합니다.

이 옵션의 경우...	다음을 수행합니다.
개인 키를 내보냅니다	아니오, 개인 키를 내보내지 않습니다 * 를 선택한 후 * 다음 * 을 클릭합니다.
파일 형식 내보내기	다음 * 을 클릭합니다.
파일 이름	찾아보기 * 를 클릭하고 인증서를 저장할 파일 경로를 지정한 후 * 다음 * 을 클릭합니다.
인증서 내보내기 마법사를 완료합니다	요약을 검토한 후 * Finish * 를 클릭하여 내보내기를 시작합니다.

SnapCenter HA 구성 및 VMware vSphere용 SnapCenter 플러그인에는 인증서 기반 인증이 지원되지 않습니다.

CA(인증 기관) 인증서를 Windows 플러그인 호스트로 가져옵니다

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

- 단계 *
  1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 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 단추로 클릭한 다음 * 모든 작업 * > * 가져오기 * 를 선택하여 가져오기 마법사를 시작합니다.
  6. 마법사에서 다음 작업을 수행합니다.

이 옵션의 경우...	다음을 수행합니다.
매장 위치	다음 * 을 클릭합니다.
가져올 파일	cer 확장자로 끝나는 SnapCenter 서버 인증서를 선택합니다.
인증서 저장소	다음 * 을 클릭합니다.
인증서 내보내기 마법사를 완료합니다	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

CA 인증서를 UNIX 호스트 플러그인으로 가져오고 SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성합니다

CA 인증서를 UNIX 플러그인 호스트로 가져옵니다

CA 인증서를 UNIX 플러그인 호스트로 가져와야 합니다.

- 이 작업에 대한 정보 *
- SPL 키 저장소의 암호 및 사용 중인 CA 서명 키 쌍의 별칭을 관리할 수 있습니다.
- SPL 키 저장소 및 개인 키의 모든 관련 별칭 암호에 대한 암호는 동일해야 합니다.
- 단계 *
  1. SPL 속성 파일에서 SPL 키 저장소 기본 암호를 검색할 수 있습니다. 키에 해당하는 값입니다 `SPL_KEYSTORE_PASS`.
  2. 키 저장소 암호를 변경합니다.
     `$ keytool -storepasswd -keystore keystore.jks`
  3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 암호를 키 저장소에 사용되는 동일한 암호로 변경합니다.
     `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
  4. SPL_keystore_pass in 키에 대해서도 동일하게 업데이트하십시오 `spl.properties` 파일.
  5. 암호를 변경한 후 서비스를 다시 시작합니다.

SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성합니다

루트 또는 중간 인증서를 SPL 신뢰 저장소에 구성해야 합니다. 루트 CA 인증서와 중간 CA 인증서를 추가해야 합니다.

- 단계 *
  1. SPL 키 저장소가 포함된 폴더로 이동합니다. `/var/opt/snapcenter/spl/etc`.
  2. 파일을 찾습니다 `keystore.jks`.
  3. 키 저장소에 추가된 인증서를 나열합니다.
     `$ keytool -list -v -keystore keystore.jks`
  4. 루트 또는 중간 인증서 추가:
     `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
  5. SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.

CA 서명 키 쌍을 SPL 신뢰 저장소에 구성합니다

CA 서명된 키 쌍을 SPL 신뢰 저장소에 구성해야 합니다.

- 단계 *
  1. SPL의 키 저장소가 포함된 폴더로 이동합니다 `/var/opt/snapcenter/spl/etc`.
  2. 파일을 찾습니다 `keystore.jks`.

3. 키 저장소에 추가된 인증서를 나열합니다.
   `$ keytool -list -v -keystore keystore.jks`
4. 개인 키와 공개 키를 모두 사용하는 CA 인증서를 추가합니다.
   `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. 키 저장소에 추가된 인증서를 나열합니다.
   `$ keytool -list -v -keystore keystore.jks`
6. keystore에 keystore에 추가된 새 CA 인증서에 해당하는 별칭이 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 암호를 키 저장소 암호로 변경합니다.

   기본 SPL 키 저장소 암호는 SPL_keystore_pass in 키의 값입니다 `spl.properties` 파일.

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
```

1. CA 인증서의 별칭 이름이 길고 공백 또는 특수 문자("*",",")가 포함된 경우 별칭 이름을 단순 이름으로 변경합니다.
   `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
2. 에 있는 키 저장소에서 별칭 이름을 구성합니다 `spl.properties` 파일.
   이 값을 SPL_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.
3. CA 서명 키 쌍을 SPL 신뢰 저장소에 구성한 후 서비스를 다시 시작합니다.

인증서 기반 인증을 사용합니다

SnapCenter 서버 및 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 사용하려면 다음을 따르십시오.

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

- 클라이언트 인증서 기반 인증을 사용하지 않도록 설정하려면 다음을 따르십시오.

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

Active Directory, LDAP 및 LDAPS를 구성합니다

신뢰할 수 없는 **Active Directory** 도메인을 등록합니다

신뢰할 수 없는 여러 Active Directory 도메인의 호스트, 사용자 및 그룹을 관리하려면 Active Directory를 SnapCenter 서버에 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 설정해야 합니다.
- DNS 확인은 SnapCenter 서버에서 플러그인 호스트로, 또는 그 반대로 설정해야 합니다.
- LDAP 프로토콜 *
- FQDN(정규화된 도메인 이름)은 SnapCenter 서버에서 확인할 수 있어야 합니다.

  FQDN을 사용하여 신뢰할 수 없는 도메인을 등록할 수 있습니다. SnapCenter 서버에서 FQDN을 확인할 수 없는 경우 도메인 컨트롤러 IP 주소로 등록할 수 있으며 SnapCenter 서버에서 확인할 수 있습니다.

LDAPS 프로토콜 *

- LDAPS가 Active Directory 통신 중에 종단 간 암호화를 제공하려면 CA 인증서가 필요합니다.

  "LDAPS에 대한 CA 클라이언트 인증서를 구성합니다"

- SnapCenter 서버에서 도메인 컨트롤러 호스트 이름(DCHostName)에 연결할 수 있어야 합니다.
- 이 작업에 대한 정보 *
- 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 * 글로벌 설정 * 을 클릭합니다.
  3. 글로벌 설정 페이지에서 * 도메인 설정 * 을 클릭합니다.
  4. 을 클릭합니다 + 새 도메인을 등록합니다.
  5. 새 도메인 등록 페이지에서 * LDAP * 또는 * LDAPS * 를 선택합니다.
     a. LDAP * 를 선택한 경우 LDAP에 대해 신뢰할 수 없는 도메인을 등록하는 데 필요한 정보를 지정합니다.

이 필드의 내용...	수행할 작업...
도메인 이름	도메인의 NetBIOS 이름을 지정합니다.
도메인 FQDN	FQDN을 지정하고 * Resolve * 를 클릭합니다.
도메인 컨트롤러 IP 주소입니다	SnapCenter 서버에서 도메인 FQDN을 확인할 수 없는 경우 하나 이상의 도메인 컨트롤러 IP 주소를 지정합니다. 자세한 내용은 을 참조하십시오 "GUI에서 신뢰할 수 없는 도메인에 대한 도메인 컨트롤러 IP를 추가합니다".

b. LDAPS * 를 선택한 경우 LDAPS에 대해 신뢰할 수 없는 도메인을 등록하는 데 필요한 정보를 지정합니다.

이 필드의 내용...	수행할 작업...
도메인 이름	도메인의 NetBIOS 이름을 지정합니다.
도메인 FQDN	FQDN을 지정합니다.
도메인 컨트롤러 이름입니다	하나 이상의 도메인 컨트롤러 이름을 지정하고 * Resolve * 를 클릭합니다.
도메인 컨트롤러 IP 주소입니다	SnapCenter 서버에서 도메인 컨트롤러 이름을 확인할 수 없는 경우 DNS 해상도를 수정해야 합니다.

6. 확인 * 을 클릭합니다.

LDAPS에 대한 CA 클라이언트 인증서를 구성합니다

Windows Active Directory LDAPS가 CA 인증서와 함께 구성된 경우 SnapCenter 서버에서 LDAPS에 대한 CA 클라이언트 인증서를 구성해야 합니다.

- 단계 *

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 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 단추로 클릭한 다음 * 모든 작업 * > * 가져오기 * 를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료합니다.

이 마법사 창에서...	다음을 수행합니다.
를 클릭합니다	찾아보기 * 를 클릭하고 _Root Certificate_를 선택한 후 * 다음 * 을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

7. 중간 인증서에 대해 5단계와 6단계를 반복합니다.

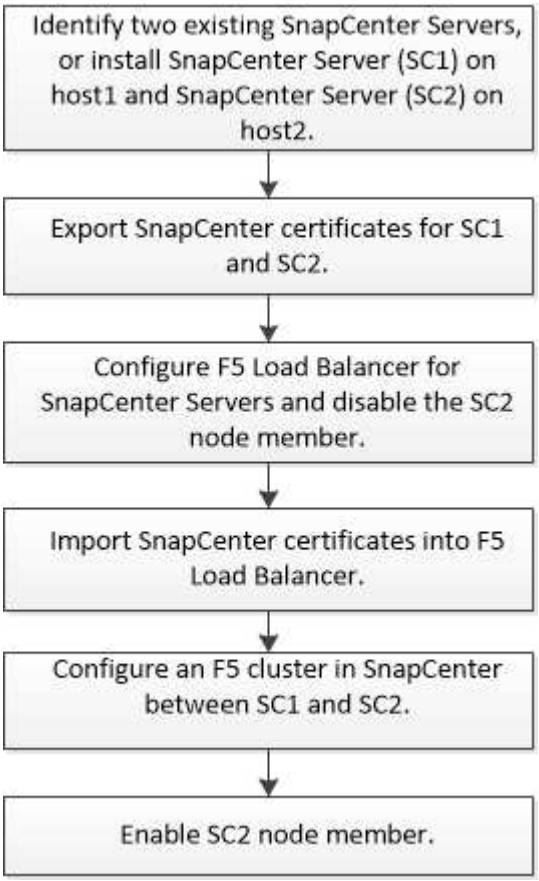
고가용성을 구성합니다

F5를 사용하여 고가용성을 위해 SnapCenter 서버를 구성합니다

SnapCenter에서 HA(고가용성)를 지원하기 위해 F5 로드 밸런서를 설치할 수 있습니다. F5를 사용하면 SnapCenter 서버가 동일한 위치에 있는 최대 2개의 호스트에서 액티브-패시브 구성을 지원할 수 있습니다. SnapCenter에서 F5 로드 밸런서를 사용하려면 SnapCenter 서버를 구성하고 F5 로드 밸런서를 구성해야 합니다.

SnapCenter 4.2.x에서 업그레이드한 후 이전에 네트워크 로드 밸런싱(NLB)을 사용한 경우 해당 구성을 계속 사용하거나 F5 로 전환할 수 있습니다.

워크플로 이미지에는 F5 로드 밸런서를 사용하여 고가용성을 위해 SnapCenter 서버를 구성하는 단계가 나와 있습니다. 자세한 지침은 을 참조하십시오 "F5 로드 밸런서를 사용하여 고가용성을 위해 SnapCenter 서버를 구성하는 방법".



다음 cmdlet을 사용하여 F5 클러스터를 추가 및 제거하려면 SnapCenter Server의 로컬 관리자 그룹 구성원이어야 합니다(스냅센터 관리자 역할에 할당되는 것 외에).

- Add-SmServerCluster를 선택합니다
- Add-SmServer 를 클릭합니다
- 제거 - SmServerCluster

  자세한 내용은 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

추가 **F5** 구성 정보

- 고가용성을 위해 SnapCenter를 설치하고 구성한 후 F5 클러스터 IP를 가리키도록 SnapCenter 바탕 화면 바로 가기를 편집합니다.
- SnapCenter 서버 간에 페일오버가 발생하고 기존 SnapCenter 세션도 있는 경우 브라우저를 닫고 SnapCenter에 다시 로그온해야 합니다.
- NLB 또는 F5(Load Balancer Setup)에서 NLB 또는 F5 노드에 의해 부분적으로 확인된 노드를 추가하고 SnapCenter 노드가 이 노드에 연결할 수 없는 경우 SnapCenter 호스트 페이지는 호스트 다운과 실행 상태 사이를 자주 전환합니다. 이 문제를 해결하려면 두 SnapCenter 노드가 모두 NLB 또는 F5 노드의 호스트를 해결할 수 있는지 확인해야 합니다.
- MFA 설정에 대한 SnapCenter 명령은 모든 노드에서 실행되어야 합니다. AD FS(Active Directory Federation Services) 서버에서 F5 클러스터 세부 정보를 사용하여 기반 당사자 구성을 수행해야 합니다. MFA를 사용하도록 설정하면 노드 레벨 SnapCenter UI 액세스가 차단됩니다.
- 페일오버 중에 감사 로그 설정은 두 번째 노드에 반영되지 않습니다. 따라서 F5 패시브 노드가 활성화될 때 감사 로그 설정을 수동으로 반복해야 합니다.

Microsoft 네트워크 로드 밸런서를 수동으로 구성합니다

Microsoft NLB(네트워크 로드 밸런싱)를 구성하여 SnapCenter 고가용성을 설정할 수 있습니다. SnapCenter 4.2에서는 고가용성을 위해 SnapCenter 설치 외부에서 NLB를 수동으로 구성해야 합니다.

SnapCenter를 사용하여 NLB(네트워크 로드 밸런싱)를 구성하는 방법에 대한 자세한 내용은 을 참조하십시오 "SnapCenter를 사용하여 NLB를 구성하는 방법".

SnapCenter 4.1.1 또는 이전 버전에서 SnapCenter를 설치하는 동안 NLB(네트워크 로드 밸런싱)를 지원했습니다.

고가용성을 위해 **NLB**에서 **F5**로 전환합니다

SnapCenter HA 구성을 NLB(네트워크 로드 밸런싱)에서 F5 로드 밸런서를 사용하도록 변경할 수 있습니다.

- 단계 *
  1. F5를 사용하여 고가용성을 위해 SnapCenter 서버를 구성합니다. "자세한 정보".
  2. SnapCenter 서버 호스트에서 PowerShell을 실행합니다.
  3. Open-SmConnection cmdlet을 사용하여 세션을 시작한 다음 자격 증명을 입력합니다.
  4. Update-SmServerCluster cmdlet을 사용하여 F5 클러스터 IP 주소를 가리키도록 SnapCenter 서버를 업데이트합니다.

     cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

SnapCenter MySQL 리포지토리의 고가용성

MySQL 복제는 하나의 MySQL 데이터베이스 서버(마스터)에서 다른 MySQL 데이터베이스 서버(슬레이브)로 데이터를 복제할 수 있는 MySQL Server의 기능입니다. SnapCenter는 2개의 NLB 지원(Network Load Balancing-enabled) 노드에서만 고가용성을 위해 MySQL 복제를 지원합니다.

SnapCenter는 마스터 리포지토리에서 읽기 또는 쓰기 작업을 수행하고 마스터 리포지토리에 오류가 있을 때 슬레이브 리포지토리에 대한 연결을 라우팅합니다. 그러면 슬레이브 리포지토리가 마스터 리포지토리가 됩니다. SnapCenter는 페일오버 중에만 사용되는 역방향 복제도 지원합니다.

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

SnapCenter는 MySQL 복제를 관리하기 위해 _get-SmrepositoryConfig_and_Set-SmrepositoryConfig_PowerShell cmdlet을 제공합니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

MySQL HA 기능과 관련된 제한 사항을 알고 있어야 합니다.

- NLB와 MySQL HA는 두 노드 이상으로 지원되지 않습니다.
- SnapCenter 독립 실행형 설치에서 NLB 설치로 또는 그 반대로 전환하고 MySQL 독립 실행형 설정에서 MySQL HA로 전환하는 것은 지원되지 않습니다.
- 슬레이브 리포지토리 데이터가 마스터 저장소 데이터와 동기화되지 않은 경우 자동 장애 조치가 지원되지 않습니다.

  _Set-SmRepositoryConfig_cmdlet을 사용하여 강제 대체 작동을 시작할 수 있습니다.

- 페일오버가 시작되면 실행 중인 작업이 실패할 수 있습니다.

  MySQL Server 또는 SnapCenter Server가 다운되어 페일오버가 발생하면 실행 중인 작업이 실패할 수 있습니다. 두 번째 노드로 페일오버한 후 이후의 모든 작업이 성공적으로 실행됩니다.

고가용성 구성에 대한 자세한 내용은 을 참조하십시오 "SnapCenter를 사용하여 NLB 및 ARR을 구성하는 방법".

SnapCenter 인증서를 내보냅니다

- 단계 *
  1. MMC(Microsoft Management Console)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 고유 이름이 있는 인증서를 마우스 오른쪽 단추로 클릭한 다음 * 모든 작업 * > * 내보내기 * 를 선택하여 내보내기 마법사를 시작합니다.
  6. 다음과 같이 마법사를 완료합니다.

이 마법사 창에서...	다음을 수행합니다.
개인 키를 내보냅니다	Yes, export the private key * 옵션을 선택한 후 * Next * 를 클릭합니다.
파일 형식 내보내기	변경하지 않고 * 다음 * 을 클릭합니다.
보안	내보낸 인증서에 사용할 새 암호를 지정하고 * 다음 * 을 클릭합니다.
내보낼 파일	내보낸 인증서의 파일 이름을 지정하고(.pfx 사용) * 다음 * 을 클릭합니다.
인증서 내보내기 마법사를 완료합니다	요약을 검토한 후 * Finish * 를 클릭하여 내보내기를 시작합니다.

결과 *

인증서는 .pfx 형식으로 내보내집니다.

역할 기반 액세스 제어(RBAC) 구성

사용자 또는 그룹을 추가하고 역할 및 자산을 할당합니다

SnapCenter 사용자에 대한 역할 기반 액세스 제어를 구성하려면 사용자 또는 그룹을 추가하고 역할을 할당할 수 있습니다. 역할에 따라 SnapCenter 사용자가 액세스할 수 있는 옵션이 결정됩니다.

시작하기 전에

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

> SnapCenter 4.5에서는 공백(), 하이픈(-), 밑줄(_) 및 콜론(:)과 같은 특수 문자만 사용자 이름과 그룹 이름에 포함할 수 있습니다.
> 이러한 특수 문자로 SnapCenter의 이전 릴리스에서 만든 역할을 사용하려면 SnapCenter WebApp이 설치된 web.config 파일에서 'disableSQLInjectionValidation' 매개 변수의 값을 true 로 변경하여 역할 이름의 유효성 검사를 비활성화할 수 있습니다. 값을 수정한 후에는 서비스를 다시 시작할 필요가 없습니다.

- SnapCenter에는 몇 가지 사전 정의된 역할이 포함되어 있습니다.

  이러한 역할을 사용자에게 할당하거나 새 역할을 만들 수 있습니다.

- SnapCenter RBAC에 추가되는 AD 사용자 및 AD 그룹은 Active Directory의 사용자 컨테이너 및 컴퓨터 컨테이너에 대한 읽기 권한을 가지고 있어야 합니다.

- 적절한 권한이 포함된 사용자 또는 그룹에 역할을 할당한 후에는 호스트 및 스토리지 연결과 같은 SnapCenter 자산에 대한 사용자 액세스를 할당해야 합니다.

  따라서 사용자는 자신에게 할당된 자산에 대한 사용 권한이 있는 작업을 수행할 수 있습니다.

- RBAC 사용 권한 및 효율성을 활용하려면 특정 시점에 사용자나 그룹에 역할을 할당해야 합니다.
- 호스트, 리소스 그룹, 정책, 스토리지 연결, 플러그인, 사용자 또는 그룹을 생성하는 동안 사용자에게 자격 증명을 제공합니다.
- 특정 작업을 수행하기 위해 사용자를 할당해야 하는 최소 자산은 다음과 같습니다.

작동	자산 할당
리소스 보호	호스트, 정책
백업	호스트, 리소스 그룹, 정책
복원	호스트, 리소스 그룹
복제	호스트, 리소스 그룹, 정책
클론 라이프사이클	호스트
리소스 그룹을 만듭니다	호스트

- 새 노드가 Windows 클러스터 또는 DAG(Exchange Server Database Availability Group) 자산에 추가되고 이 새 노드가 사용자에게 할당된 경우 사용자나 그룹에 새 노드를 포함하도록 자산을 재할당해야 합니다.

  RBAC 사용자 또는 그룹을 클러스터 또는 DAG에 재할당하여 RBAC 사용자 또는 그룹에 새 노드를 포함해야 합니다. 예를 들어, 2노드 클러스터가 있고 RBAC 사용자 또는 그룹을 클러스터에 할당했습니다. 클러스터에 다른 노드를 추가하는 경우 RBAC 사용자 또는 그룹을 클러스터에 재할당하여 RBAC 사용자 또는 그룹의 새 노드를 포함해야 합니다.

- 스냅샷 복사본을 복제할 계획인 경우 작업을 수행하는 사용자에게 소스 및 타겟 볼륨 모두에 대한 스토리지 연결을 할당해야 합니다.

  사용자에게 액세스 권한을 할당하기 전에 자산을 추가해야 합니다.

VMware vSphere용 SnapCenter 플러그인 기능을 사용하여 VM, VMDK 또는 데이터 저장소를 보호하는 경우 VMware vSphere GUI를 사용하여 vCenter 사용자를 VMware vSphere용 SnapCenter 플러그인 역할에 추가해야 합니다. VMware vSphere 역할에 대한 자세한 내용은 를 참조하십시오 "VMware vSphere용 SnapCenter 플러그인과 함께 패키지로 제공되는 사전 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 다음을 수행합니다.

이 필드의 내용...	수행할 작업...
액세스 유형	도메인 또는 작업 그룹을 선택합니다 도메인 인증 유형의 경우 사용자를 역할에 추가할 사용자 또는 그룹의 도메인 이름을 지정해야 합니다. 기본적으로 로그인한 도메인 이름으로 미리 채워집니다. 신뢰할 수 없는 도메인은 * 설정 * > * 글로벌 설정 * > * 도메인 설정 * 페이지에서 등록해야 합니다.
유형	사용자 또는 그룹을 선택합니다 SnapCenter는 메일 그룹이 아닌 보안 그룹만 지원합니다.
사용자 이름	a. 부분 사용자 이름을 입력한 다음 * 추가 * 를 클릭합니다. 사용자 이름은 대소문자를 구분합니다. b. 검색 목록에서 사용자 이름을 선택합니다. 다른 도메인 또는 신뢰할 수 없는 도메인의 사용자를 추가할 때는 도메인 간 사용자에 대한 검색 목록이 없으므로 사용자 이름을 완전히 입력해야 합니다. 선택한 역할에 다른 사용자 또는 그룹을 추가하려면 이 단계를 반복합니다.
역할	사용자를 추가할 역할을 선택합니다.

4. Assign * 을 클릭한 다음 Assign Assets 페이지에서 다음을 수행합니다.
   a. 자산 * 드롭다운 목록에서 자산 유형을 선택합니다.
   b. [자산] 테이블에서 자산을 선택합니다.

      사용자가 자산을 SnapCenter에 추가한 경우에만 자산이 나열됩니다.

   c. 필요한 모든 자산에 대해 이 절차를 반복합니다.

d. 저장 * 을 클릭합니다.

5. 제출 * 을 클릭합니다.

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

역할을 생성합니다

기존 SnapCenter 역할을 사용하는 것 외에도 고유한 역할을 만들고 사용 권한을 사용자 지정할 수 있습니다.

"SnapCenterAdmin" 역할로 로그인해야 합니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
2. 설정 페이지에서 * 역할 * 을 클릭합니다.
3. 을 클릭합니다 .
4. 역할 추가 페이지에서 새 역할의 이름과 설명을 지정합니다.

SnapCenter 4.5에서는 공백(), 하이픈(-), 밑줄(_) 및 콜론(:)과 같은 특수 문자만 사용자 이름과 그룹 이름에 포함할 수 있습니다.
이러한 특수 문자로 SnapCenter의 이전 릴리스에서 만든 역할을 사용하려면 SnapCenter WebApp이 설치된 web.config 파일에서 'disableSQLInjectionValidation' 매개 변수의 값을 true 로 변경하여 역할 이름의 유효성 검사를 비활성화할 수 있습니다. 값을 수정한 후에는 서비스를 다시 시작할 필요가 없습니다.

5. 이 역할의 모든 구성원은 다른 구성원의 개체를 볼 수 있습니다 * 를 선택하여 역할의 다른 구성원이 리소스 목록을 새로 고친 후 볼륨 및 호스트와 같은 리소스를 볼 수 있도록 합니다.

이 역할의 구성원이 다른 구성원이 할당된 개체를 보지 못하도록 하려면 이 옵션을 선택 취소해야 합니다.

이 옵션을 사용하면 개체 또는 리소스를 만든 사용자와 동일한 역할에 속한 사용자는 개체 또는 리소스에 대한 사용자 액세스를 할당할 필요가 없습니다.

1. 사용 권한 페이지에서 역할에 할당할 사용 권한을 선택하거나 * 모두 선택 * 을 클릭하여 역할에 모든 사용 권한을 부여합니다.
2. 제출 * 을 클릭합니다.

보안 로그인 명령을 사용하여 **ONTAP RBAC** 역할을 추가합니다

스토리지 시스템에서 clustered ONTAP을 실행 중인 경우 보안 로그인 명령을 사용하여 ONTAP RBAC 역할을 추가할 수 있습니다.

시작하기 전에

- Clustered ONTAP을 실행 중인 스토리지 시스템에 대해 ONTAP RBAC 역할을 생성하기 전에 다음을 확인해야 합니다.

- 수행할 작업(또는 작업)입니다
- 이러한 작업을 수행하는 데 필요한 권한입니다

- RBAC 역할을 구성하려면 다음 작업을 수행해야 합니다.
  - 명령 및/또는 명령 디렉터리에 권한을 부여합니다.

    명령 /command 디렉토리에는 모두 액세스 및 읽기 전용이라는 두 가지 액세스 레벨이 있습니다.

  항상 먼저 모든 액세스 권한을 할당해야 합니다.

  - 사용자에게 역할을 할당합니다.
  - SnapCenter 플러그인이 전체 클러스터의 클러스터 관리자 IP에 연결되어 있는지, 아니면 클러스터 내의 SVM에 직접 연결되어 있는지 여부에 따라 구성을 다양하게 변경할 수 있습니다.

- 이 작업에 대한 정보 *

스토리지 시스템에서 이러한 역할을 간단히 구성하기 위해 NetApp 커뮤니티 포럼에 게시된 RBAC 사용자 작성자 for Data ONTAP 툴을 사용할 수 있습니다.

이 도구는 자동으로 ONTAP 권한 설정을 올바르게 처리합니다. 예를 들어, RBAC Data ONTAP용 사용자 작성 도구 는 모든 액세스 권한이 먼저 나타나도록 올바른 순서로 권한을 자동으로 추가합니다. 읽기 전용 권한을 먼저 추가한 다음 모든 액세스 권한을 추가하면 ONTAP에서 모든 액세스 권한을 중복으로 표시하고 무시합니다.

나중에 SnapCenter 또는 ONTAP를 업그레이드할 경우 RBAC 사용자 생성기 for Data ONTAP 도구를 다시 실행하여 이전에 만든 사용자 역할을 업데이트해야 합니다. 이전 버전의 SnapCenter 또는 ONTAP에 대해 만든 사용자 역할은 업그레이드된 버전에서 제대로 작동하지 않습니다. 이 도구를 다시 실행하면 자동으로 업그레이드를 처리합니다. 역할을 다시 생성할 필요는 없습니다.

ONTAP RBAC 역할 설정에 대한 자세한 내용은 을 참조하십시오 "ONTAP 9 관리자 인증 및 RBAC 전원 가이드".

일관성을 위해 SnapCenter 문서는 사용 권한을 사용하는 역할을 나타냅니다. OnCommand 시스템 관리자 GUI는 *privilege* 대신 _attribute_라는 용어를 사용합니다. ONTAP RBAC 역할을 설정할 때 이 두 용어는 모두 동일합니다.

- 단계 *

1. 스토리지 시스템에서 다음 명령을 입력하여 새 역할을 생성합니다.

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

   - SVM_NAME은 SVM의 이름입니다. 이 필드를 비워 두면 기본적으로 클러스터 관리자가 됩니다.
   - role_name 은 역할에 대해 지정하는 이름입니다.
   - 명령은 ONTAP 기능입니다.

     각 권한에 대해 이 명령을 반복해야 합니다. 모든 액세스 명령은 읽기 전용 명령 앞에 나열되어야 합니다.

   사용 권한 목록에 대한 자세한 내용은 을 참조하십시오 "역할을 생성하고 권한을 할당하는 ONTAP CLI

명령입니다".

2. 다음 명령을 입력하여 사용자 이름을 생성합니다.

```
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 만들고 있는 사용자의 이름입니다.
   - password>는 사용자의 암호입니다. 암호를 지정하지 않으면 시스템에 암호를 입력하라는 메시지가 표시됩니다.
   - 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 만든 사용자의 이름입니다. 이 명령을 사용하면 사용자를 수정하여 역할에 연결할 수 있습니다.
   - svm_name>은 SVM의 이름입니다.
   - role_name>은 1단계에서 만든 역할의 이름입니다.
   - password>는 사용자의 암호입니다. 암호를 지정하지 않으면 시스템에 암호를 입력하라는 메시지가 표시됩니다.

4. 다음 명령을 입력하여 사용자가 올바르게 생성되었는지 확인합니다.

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

user_name 은 3단계에서 만든 사용자의 이름입니다.

최소 권한으로 **SVM** 역할 생성

ONTAP에서 새 SVM 사용자의 역할을 생성할 때 실행해야 하는 ONTAP CLI 명령은 여러 가지가 있습니다. ONTAP에서 SnapCenter와 함께 사용하도록 SVM을 구성하고 vsadmin 역할을 사용하지 않으려는 경우 이 역할이 필요합니다.

- 단계 *

1. 스토리지 시스템에서 역할을 생성하고 역할에 모든 권한을 할당합니다.

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

   각 권한에 대해 이 명령을 반복해야 합니다.

1. 사용자를 생성하고 해당 사용자에게 역할을 할당합니다.

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

2. 사용자 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 몇 가지 ONTAP CLI 명령을 실행해야 합니다.

- `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 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 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 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`

최소 권한으로 **ONTAP** 클러스터 역할을 생성합니다

SnapCenter에서 작업을 수행하기 위해 ONTAP 관리자 역할을 사용할 필요가 없도록 최소 권한으로 ONTAP 클러스터 역할을 생성해야 합니다. 여러 ONTAP CLI 명령을 실행하여 ONTAP 클러스터 역할을 생성하고 최소 권한을 할당할 수 있습니다.

- 단계 *

1. 스토리지 시스템에서 역할을 생성하고 역할에 모든 권한을 할당합니다.

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

   각 권한에 대해 이 명령을 반복해야 합니다.

1. 사용자를 생성하고 해당 사용자에게 역할을 할당합니다.

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

2. 사용자 잠금을 해제합니다.

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

클러스터 역할을 생성하고 권한을 할당하는 **ONTAP CLI** 명령입니다

클러스터 역할을 생성하고 권한을 할당하려면 몇 가지 ONTAP CLI 명령을 실행해야 합니다.

- `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 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 "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 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 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

Active Directory 읽기 권한을 사용하도록 **IIS** 응용 프로그램 풀을 구성합니다

SnapCenter에 대해 Active Directory 읽기 권한을 설정해야 할 때 사용자 지정 응용 프로그램 풀 계정을 만들도록 Windows Server에서 IIS(인터넷 정보 서비스)를 구성할 수 있습니다.

- 단계 *
  1. SnapCenter가 설치된 Windows 서버에서 IIS 관리자를 엽니다.
  2. 왼쪽 탐색 창에서 * 응용 프로그램 풀 * 을 클릭합니다.
  3. 응용 프로그램 풀 목록에서 SnapCenter를 선택한 다음 작업 창에서 * 고급 설정 * 을 클릭합니다.
  4. ID를 선택한 다음 *… * 를 클릭하여 SnapCenter 응용 프로그램 풀 ID를 편집합니다.
  5. 사용자 지정 계정 필드에 Active Directory 읽기 권한이 있는 도메인 사용자 또는 도메인 관리자 계정 이름을 입력합니다.
  6. 확인 을 클릭합니다.

     사용자 지정 계정은 SnapCenter 응용 프로그램 풀의 기본 제공 ApplicationPoolIdentity 계정을 대체합니다.

감사 로그 설정을 구성합니다

감사 로그는 SnapCenter 서버의 모든 작업에 대해 생성됩니다. 기본적으로 감사 로그는 기본적으로 설치된 위치인 _C:\Program Files\NetApp\SnapCenter WebApp\audit_에 보호됩니다.

감사 로그는 각 감사 이벤트에 대해 디지털 서명된 다이제스트를 생성하여 무단 수정으로부터 보호합니다. 생성된 다이제스트는 별도의 감사 체크섬 파일에 보관되며, 컨텐츠의 무결성을 보장하기 위해 정기적인 무결성 검사를 수행합니다.

"SnapCenterAdmin" 역할로 로그인해야 합니다.

- 이 작업에 대한 정보 *
- 경고는 다음과 같은 경우에 전송됩니다.
  - 감사 로그 무결성 검사 스케줄 또는 Syslog 서버가 활성화 또는 비활성화되어 있습니다
  - 감사 로그 무결성 검사, 감사 로그 또는 Syslog 서버 로그 실패
  - 디스크 공간이 부족합니다
- 무결성 검사가 실패한 경우에만 이메일이 전송됩니다.
- 감사 로그 디렉토리와 감사 체크섬 로그 디렉토리 경로를 함께 수정해야 합니다. 이 중 하나만 수정할 수 없습니다.
- 감사 로그 디렉토리 및 감사 체크섬 로그 디렉토리 경로가 수정되면 이전 위치에 있는 감사 로그에 대한 무결성 검사를 수행할 수 없습니다.
- 감사 로그 디렉토리 및 감사 체크섬 로그 디렉토리 경로는 SnapCenter 서버의 로컬 드라이브에 있어야 합니다.

  공유 또는 네트워크 마운트 드라이브는 지원되지 않습니다.

- Syslog 서버 설정에서 UDP 프로토콜을 사용하는 경우 포트가 중단되었거나 사용할 수 없어 발생한 오류는 SnapCenter에서 오류 또는 경고로 캡처될 수 없습니다.
- Set-SmAuditSettings 및 Get-SmAuditSettings 명령을 사용하여 감사 로그를 구성할 수 있습니다.

  cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 Get-Help command_name을 실행하여 얻을 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

- 단계 *

1. 설정 * 페이지에서 * 설정 * > * 글로벌 설정 * > * 감사 로그 설정 * 으로 이동합니다.
2. Audit log(감사 로그) 섹션에서 세부 정보를 입력합니다.
3. 감사 로그 디렉토리 * 및 * 감사 체크섬 로그 디렉토리 * 를 입력합니다
   a. 최대 파일 크기를 입력합니다
   b. 최대 로그 파일을 입력합니다
   c. 경고를 보낼 디스크 공간 사용 비율을 입력합니다
4. (선택 사항) * Log UTC Time * 을 활성화합니다.
5. (선택 사항) * 감사 로그 무결성 검사 일정 * 을 활성화하고 * 무결성 검사 시작 * 을 클릭하여 필요 시 무결성 검사를 수행합니다.

또한 * Start-SmAuditIntegrityCheck * 명령을 실행하여 요청 시 무결성 검사를 시작할 수도 있습니다.

6. (선택 사항) 전달된 감사 로그를 원격 syslog 서버로 활성화하고 Syslog Server 세부 정보를 입력합니다.

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

   a. Syslog 서버 호스트를 입력합니다
   b. Syslog 서버 포트를 입력합니다
   c. Syslog Server Protocol을 입력합니다
   d. RFC 형식을 입력합니다
7. 저장 * 을 클릭합니다.
8. 모니터 * > * 작업 * 을 클릭하면 감사 무결성 검사 및 디스크 공간 검사를 볼 수 있습니다.

스토리지 시스템을 추가합니다

데이터 보호 및 프로비저닝 작업을 수행하려면 SnapCenter 스토리지에 대한 ONTAP 액세스 권한을 제공하는 스토리지 시스템이나 NetApp ONTAP용 Amazon FSx를 설정해야 합니다.

독립 실행형 SVM이나 여러 SVM으로 구성된 클러스터를 추가할 수 있습니다. NetApp ONTAP용 Amazon FSx를 사용하는 경우 fsxadmin 계정을 사용하여 여러 SVM으로 구성된 FSx 관리 LIF를 추가하거나 SnapCenter에서 FSx SVM을 추가할 수 있습니다.

시작하기 전에

- 스토리지 접속을 생성하려면 인프라스트럭처 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

  호스트 캐시가 업데이트되지 않고 데이터베이스 상태가 SnapCenter GUI에 ""백업을 위해 사용할 수 없음"" 또는 ""NetApp 스토리지에 없음""으로 표시될 수 있으므로 스토리지 시스템 접속을 추가하는 동안 호스트 플러그인 설치가 진행되어서는 안 됩니다.

- 스토리지 시스템 이름은 고유해야 합니다.

  SnapCenter는 서로 다른 클러스터에서 동일한 이름의 여러 스토리지 시스템을 지원하지 않습니다. SnapCenter에서 지원하는 각 스토리지 시스템은 고유한 이름과 고유한 데이터 LIF IP 주소를 가져야 합니다.

- 이 작업에 대한 정보 *
- 스토리지 시스템을 구성할 때 EMS(이벤트 관리 시스템) 및 AutoSupport 기능을 활성화할 수도 있습니다. AutoSupport 툴은 시스템 상태에 대한 데이터를 수집하고 데이터를 NetApp 기술 지원 팀에 자동으로 전송하여 시스템에서 문제를 해결할 수 있도록 합니다.

  이러한 기능을 설정하면 SnapCenter는 리소스가 보호되거나, 복구 또는 클론 작업이 성공적으로 완료되거나, 작업이 실패할 때 AutoSupport 정보를 스토리지 시스템 syslog로 보내고, EMS 메시지를 스토리지 시스템 syslog에 보냅니다.

- SnapMirror 타겟 또는 SnapVault 타겟으로 스냅샷 복사본을 복제할 계획이라면, 소스 SVM 또는 클러스터뿐만 아니라 타겟 SVM 또는 클러스터에 대한 스토리지 시스템 연결을 설정해야 합니다.

스토리지 시스템 암호, 예약된 작업, 필요 시 백업 및 복원 작업을 변경하는 경우 작업이 실패할 수 있습니다. 스토리지 시스템 암호를 변경한 후 스토리지 탭에서 * 수정 * 을 클릭하여 암호를 업데이트할 수 있습니다.

- 단계 *

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

이 필드의 내용...	수행할 작업...
스토리지 시스템	스토리지 시스템 이름 또는 IP 주소를 입력합니다. 도메인 이름을 제외한 스토리지 시스템 이름은 15자 이하여야 하며 이름을 확인할 수 있어야 합니다. 이름이 15자를 초과하는 스토리지 시스템 접속을 생성하려면 Add-SmStorageConnectionPowerShell cmdlet을 사용합니다. MCC(MetroCluster Configuration)가 있는 스토리지 시스템의 경우 무중단 운영을 위해 로컬 클러스터와 피어 클러스터를 모두 등록하는 것이 좋습니다. SnapCenter은 서로 다른 클러스터에서 동일한 이름의 여러 SVM을 지원하지 않습니다. SnapCenter에서 지원하는 각 SVM에는 고유한 이름이 있어야 합니다. SnapCenter에 스토리지 연결을 추가한 후에는 ONTAP를 사용하여 SVM 또는 클러스터의 이름을 변경해서는 안 됩니다. 짧은 이름 또는 FQDN으로 SVM을 추가하는 경우 SnapCenter 및 플러그인 호스트 모두에서 확인할 수 있어야 합니다.
사용자 이름/암호	스토리지 시스템을 액세스하는 데 필요한 권한이 있는 스토리지 사용자의 자격 증명을 입력합니다.

이 필드의 내용...	수행할 작업...
이벤트 관리 시스템(EMS) 및 AutoSupport 설정	EMS 메시지를 스토리지 시스템 syslog에 보내거나, 적용된 보호, 완료된 복원 작업 또는 실패한 작업을 위해 스토리지 시스템으로 AutoSupport 메시지를 보내려면 해당 확인란을 선택합니다. 스토리지 시스템에 실패한 작업에 대한 * AutoSupport 알림 전송 * 확인란을 선택하면 AutoSupport 알림을 활성화하기 위해 EMS 메시징이 필요하기 때문에 * SnapCenter 서버 이벤트를 syslog * 에 기록 확인란도 선택됩니다.

4. 플랫폼, 프로토콜, 포트 및 시간 초과에 할당된 기본값을 수정하려면 * 추가 옵션 * 을 클릭합니다.
   a. 플랫폼 의 드롭다운 목록에서 옵션 중 하나를 선택합니다.

      SVM이 백업 관계의 2차 스토리지 시스템인 경우 * 2차 * 확인란을 선택합니다. Secondary * 옵션을 선택하면 SnapCenter에서 즉시 라이센스 검사를 수행하지 않습니다.

SnapCenter에서 SVM을 추가한 경우 사용자는 드롭다운에서 수동으로 플랫폼 유형을 선택해야 합니다.

   a. 프로토콜에서 SVM 또는 클러스터 설정 중에 구성된 프로토콜(일반적으로 HTTPS)을 선택합니다.
   b. 스토리지 시스템에서 허용하는 포트를 입력합니다.

      기본 포트 443은 일반적으로 작동합니다.

   c. 통신 시도가 중지되기 전에 경과되어야 하는 시간(초)을 입력합니다.

      기본값은 60초입니다.

   d. SVM에 관리 인터페이스가 여러 개 있는 경우 * Preferred IP * 확인란을 선택한 다음 SVM 연결을 위한 기본 IP 주소를 입력합니다.
   e. 저장 * 을 클릭합니다.
      1. 제출 * 을 클릭합니다.

결과 *

스토리지 시스템 페이지의 * 유형 * 드롭다운에서 다음 작업 중 하나를 수행합니다.

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

  FSx SVM을 추가한 경우 여기에 FSx SVM이 나열됩니다.

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

  fsxadmin을 사용하여 FSx 클러스터를 추가한 경우 FSx 클러스터가 여기에 나열됩니다.

  클러스터 이름을 클릭하면 클러스터에 포함된 모든 SVM이 스토리지 가상 시스템 섹션에 표시됩니다.

  ONTAP GUI를 사용하여 ONTAP 클러스터에 새 SVM을 추가할 경우 * 재발견 * 을 클릭하여 새로 추가된 SVM을

확인하십시오.

FAS 또는 AFF 스토리지 시스템을 모든 SAN 어레이(ASA)로 업그레이드한 경우, SnapCenter 서버의 스토리지 접속을 새로 고쳐서 SnapCenter의 새 스토리지 유형을 반영해야 합니다.

- 완료 후 *

클러스터 관리자는 스토리지 시스템 명령줄에서 다음 명령을 실행하여 SnapCenter가 액세스할 수 있는 모든 스토리지 시스템에서 e-메일 알림을 보내도록 각 스토리지 시스템 노드에서 AutoSupport를 설정해야 합니다.

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

SVM(스토리지 가상 시스템) 관리자는 AutoSupport에 액세스할 수 없습니다.

SnapCenter 표준 컨트롤러 기반 라이센스를 추가합니다

FAS, AFF 또는 모든 SAN 어레이(ASA) 스토리지 컨트롤러를 사용하는 경우 SnapCenter 표준 컨트롤러 기반 라이센스가 필요합니다.

컨트롤러 기반 라이센스는 다음과 같은 특성을 가지고 있습니다.

- 프리미엄 또는 플래시 번들 구매 시 SnapCenter 표준 자격 포함(기본 팩 제외)
- 무제한 저장소 사용
- ONTAP 시스템 관리자 또는 스토리지 클러스터 명령줄을 사용하여 FAS, AFF 또는 ASA 스토리지 컨트롤러에 직접 추가하여 사용 가능

  SnapCenter 컨트롤러 기반 라이센스의 경우 SnapCenter GUI에 라이센스 정보를 입력하지 않습니다.

- 컨트롤러의 일련 번호에 잠금 상태입니다

필요한 라이센스에 대한 자세한 내용은 를 참조하십시오 "SnapCenter 라이센스".

1단계: SnapManager 제품군 라이센스가 설치되었는지 확인합니다

SnapCenter GUI를 사용하면 SnapManager 제품군 라이센스가 FAS, AFF 또는 ASA 운영 스토리지 시스템에 설치되어 있는지 여부를 확인하고 SnapManager 제품군 라이센스가 필요할 수 있는 스토리지 시스템을 식별할 수 있습니다. SnapManager 제품군 라이센스는 FAS, AFF, ASA SVM 또는 운영 스토리지 시스템의 클러스터에만 적용됩니다.

컨트롤러에 SnapManager Suite 라이센스가 이미 있는 경우 SnapCenter 표준 컨트롤러 기반 라이센스 권한이 자동으로 제공됩니다. SnapManager 라이센스 및 SnapCenter 표준 컨트롤러 기반 라이센스 이름은 서로 바꿔서 사용되지만 동일한 라이센스를 나타냅니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 시스템 * 을 선택합니다.

2. 스토리지 시스템 페이지의 * 유형 * 드롭다운에서 추가된 모든 SVM 또는 클러스터를 표시할지 여부를 선택합니다.
   - 추가된 모든 SVM을 보려면 * ONTAP SVM * 을 선택합니다.
   - 추가된 모든 클러스터를 보려면 * ONTAP 클러스터 * 를 선택합니다.

     클러스터 이름을 선택하면 클러스터에 포함된 모든 SVM이 스토리지 가상 시스템 섹션에 표시됩니다.
3. Storage Connections 목록에서 Controller License 열을 찾습니다.

   컨트롤러 라이센스 열에는 다음 상태가 표시됩니다.

   -  SnapManager 제품군 라이센스가 FAS, AFF 또는 ASA 운영 스토리지 시스템에 설치되어 있음을 나타냅니다.
   -  SnapManager 제품군 라이센스가 FAS, AFF 또는 ASA 운영 스토리지 시스템에 설치되어 있지 않음을 나타냅니다.
   - 해당 없음 은 스토리지 컨트롤러가 Cloud Volumes ONTAP, ONTAP Select 또는 보조 스토리지 플랫폼에 있기 때문에 SnapManager Suite 라이센스가 적용되지 않음을 나타냅니다.

2단계: 컨트롤러에 설치된 라이센스를 식별합니다

ONTAP 명령줄을 사용하여 컨트롤러에 설치된 모든 라이센스를 볼 수 있습니다. FAS, AFF 또는 ASA 시스템의 클러스터 관리자여야 합니다.

SnapCenter 표준 컨트롤러 기반 라이센스는 컨트롤러에 SnapManagerSuite 라이센스로 표시됩니다.

단계

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

예제 출력

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

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

Serial Number: 1-81-00000000000000000000000xx
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 예제에서는 SnapManagerSuite 라이센스가 설치되어 있으므로 추가 SnapCenter 라이센스 작업이 필요하지 않습니다.

3단계: 컨트롤러의 일련 번호를 검색합니다

컨트롤러 기반 라이센스의 일련 번호를 검색하려면 컨트롤러 일련 번호가 필요합니다. ONTAP 명령줄을 사용하여 컨트롤러 일련 번호를 검색할 수 있습니다. FAS, AFF 또는 ASA 시스템의 클러스터 관리자여야 합니다.

단계

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

예제 출력

```
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: xxxxxxxxx
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: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. 일련 번호를 기록합니다.

4단계: 컨트롤러 기반 라이센스의 일련 번호를 검색합니다

FAS 또는 AFF 스토리지를 사용하는 경우 ONTAP 명령줄을 사용하여 설치하기 전에 NetApp Support 사이트에서 SnapCenter 컨트롤러 기반 라이센스를 검색할 수 있습니다.

시작하기 전에

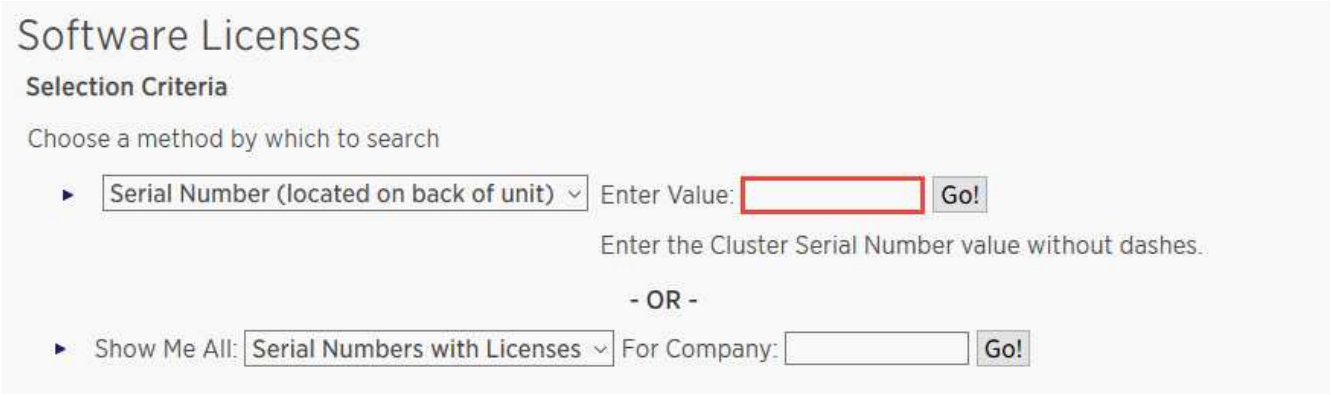
- 유효한 NetApp Support 사이트 로그인 자격 증명이 있어야 합니다.

유효한 자격 증명을 입력하지 않으면 검색에 대한 정보가 반환되지 않습니다.

- 컨트롤러의 일련 번호가 있어야 합니다.

단계

1. 에 로그인합니다 "NetApp Support 사이트".
2. 시스템 * > * 소프트웨어 라이센스 * 로 이동합니다.
3. 선택 기준 영역에서 일련 번호(장치 뒷면에 있음)가 선택되었는지 확인하고 컨트롤러 일련 번호를 입력한 다음 * Go! * 를 선택합니다.



지정된 컨트롤러의 라이센스 목록이 표시됩니다.

4. SnapCenter Standard 또는 SnapManagerSuite 라이센스를 찾아서 기록합니다.

5단계: 컨트롤러 기반 라이센스 추가

FAS, AFF 또는 ASA 시스템을 사용 중이고 SnapCenter Standard 또는 SnapManagerSuite 라이센스가 있는 경우 ONTAP 명령줄을 사용하여 SnapCenter 컨트롤러 기반 라이센스를 추가할 수 있습니다.

시작하기 전에

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

이 작업에 대해

FAS, AFF 또는 SnapCenter ASA 스토리지를 사용해 평가판을 설치하려면 컨트롤러에 설치할 Premium 번들 평가 라이센스를 받아야 합니다.

평가판을 통해 SnapCenter를 설치하려면 세일즈 담당자에게 문의하여 컨트롤러에 설치할 프리미엄 번들 평가 라이센스를 받아야 합니다.

단계

1. ONTAP 명령줄을 사용하여 NetApp 클러스터에 로그인합니다.
2. SnapManagerSuite 라이센스 키 추가:

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

이 명령은 admin 권한 수준에서 사용할 수 있습니다.

3. SnapManagerSuite 라이센스가 설치되었는지 확인합니다.

```
license show
```

6단계: 평가판 라이센스를 제거합니다

컨트롤러 기반 SnapCenter 표준 라이센스를 사용하고 있으며 용량 기반 평가판 라이센스(일련 번호가 ""50"으로 끝나는 번호)를 제거해야 하는 경우 MySQL 명령을 사용하여 평가판 라이센스를 수동으로 제거해야 합니다. 평가판 라이센스는 SnapCenter GUI를 사용하여 삭제할 수 없습니다.

SnapCenter 표준 컨트롤러 기반 라이센스를 사용하는 경우에만 평가판 라이센스를 수동으로 제거해야 합니다. SnapCenter 표준 용량 기반 라이센스를 조달하여 SnapCenter GUI에 추가하면 평가판 라이센스가 자동으로 덮어쓰여집니다.

단계

1. SnapCenter 서버에서 PowerShell 창을 열어 MySQL 암호를 재설정합니다.
   a. Open-SmConnection cmdlet을 실행하여 SnapCenter 서버에서 SnapCenterAdmin 계정에 대한 연결 세션을 시작합니다.
   b. Set-SmRepositoryPassword를 실행하여 MySQL 암호를 재설정합니다.

      cmdlet에 대한 자세한 내용은 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

2. 명령 프롬프트를 열고 MySQL -u root -p 를 실행하여 MySQL에 로그인합니다.

   MySQL에서 암호를 묻는 메시지를 표시합니다. 암호를 재설정하는 동안 제공한 자격 증명을 입력합니다.

3. 데이터베이스에서 평가판 라이센스를 제거합니다.

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

SnapCenter 표준 용량 기반 라이센스 추가

SnapCenter 표준 용량 라이센스를 사용하여 ONTAP Select 및 Cloud Volumes ONTAP 플랫폼의 데이터를 보호할 수 있습니다.

용량 라이센스의 특징은 다음과 같습니다.

- 51xxxxxxx 형식의 9자리 일련 번호로 구성됩니다

  라이센스 일련 번호 및 유효한 NetApp Support 사이트 로그인 자격 증명을 사용하여 SnapCenter GUI를 통해 라이센스를 활성화합니다.

- 사용된 스토리지 용량 또는 보호할 데이터의 크기 중 더 낮은 것을 기준으로 비용을 설정하고 SnapCenter에서 데이터를 관리하는 별도의 영구 라이센스로 사용할 수 있습니다
- 테라바이트당 가용성

  예를 들어, 1TB, 2TB, 4TB 등에 대한 용량 기반 라이센스를 얻을 수 있습니다.

- 100TB 용량 사용 권한이 있는 90일 평가판 라이센스로 제공됩니다

  필요한 라이센스에 대한 자세한 내용은 를 참조하십시오 "SnapCenter 라이센스".

SnapCenter는 Cloud Volumes ONTAP 및 관리하는 ONTAP Select 스토리지에서 매일 자정에 용량 사용량을 자동으로 계산합니다. 표준 용량 라이센스를 사용하는 경우 SnapCenter는 총 라이센스 용량에서 모든 볼륨에 사용된 용량을 추론하여 사용하지 않은 용량을 계산합니다. 사용된 용량이 라이센스 용량을 초과하면 SnapCenter 대시보드에 초과 사용 경고가 표시됩니다. SnapCenter에서 용량 임계값 및 알림을 구성한 경우 사용된 용량이 지정한 임계값에 도달하면 이메일이 전송됩니다.

1단계**:** 용량 요구 사항 계산

SnapCenter 용량 기반 라이센스를 얻기 전에 SnapCenter에서 관리할 호스트의 용량을 계산해야 합니다.

Cloud Volumes ONTAP 또는 ONTAP Select 시스템에서 클러스터 관리자여야 합니다.

이 작업에 대해

SnapCenter는 사용된 실제 용량을 계산합니다. 파일 시스템 또는 데이터베이스의 크기가 1TB이지만 500GB의 공간만 사용되는 경우 SnapCenter는 500GB의 사용된 용량을 계산합니다. 볼륨 용량은 중복제거 및 압축 후 계산되며 전체 볼륨의 사용된 용량을 기준으로 계산됩니다.

단계

1. ONTAP 명령줄을 사용하여 NetApp 컨트롤러에 로그인합니다.
2. 사용된 볼륨 용량을 보려면 명령을 입력합니다.

```
select::> vol show -fields used -volume Engineering,Marketing
vserver volume       used
------- ------       ------
VS1     Engineering  2.13TB
VS1     Marketing    2.62TB

2   entries were displayed.
```

두 볼륨의 사용된 총 용량은 5TB 미만입니다. 따라서 모든 5TB 데이터를 보호하려면 최소 SnapCenter 용량 기반 라이센스 요구사항이 5TB 이상입니다.

그러나 총 사용 용량 5TB의 2TB만 보호하려면 2TB 용량 기반 라이센스를 얻을 수 있습니다.

2단계**:** 용량 기반 라이센스의 일련 번호를 검색합니다

SnapCenter 용량 기반 라이센스 일련 번호는 주문 확인 또는 문서 패키지에서 사용할 수 있습니다. 하지만 이 일련 번호가 없는 경우 NetApp Support 사이트에서 검색할 수 있습니다.

유효한 NetApp Support 사이트 로그인 자격 증명이 있어야 합니다.

단계

1. 에 로그인합니다 "NetApp Support 사이트".

2. 시스템 * > * 소프트웨어 라이센스 * 로 이동합니다.
3. 선택 기준 영역의 모두 표시: 일련 번호 및 라이센스 드롭다운 메뉴에서 * SC_STANDARD * 를 선택합니다.

4. 회사 이름을 입력한 다음 * Go! * 를 선택합니다.

   51xxxxxxx 형식의 9자리 SnapCenter 라이센스 일련 번호가 표시됩니다.

5. 일련 번호를 기록합니다.

3단계**: NetApp** 라이센스 파일을 생성합니다

SnapCenter GUI에 NetApp Support 사이트 자격 증명과 SnapCenter 라이센스 일련 번호를 입력하지 못하거나 SnapCenter에서 NetApp Support 사이트에 인터넷에 액세스할 수 없는 경우 NetApp 라이센스 파일(NLF)을 생성할 수 있습니다. 그런 다음 SnapCenter 호스트에서 액세스할 수 있는 위치에 파일을 다운로드하여 저장할 수 있습니다.

시작하기 전에

- ONTAP Select를 SnapCenter 또는 Cloud Volumes ONTAP와 함께 사용해야 합니다.
- 유효한 NetApp Support 사이트 로그인 자격 증명이 있어야 합니다.
- 51xxxxxxx 형식의 라이센스 일련 번호는 9자리 숫자여야 합니다.

단계

1. 로 이동합니다 "NetApp 라이센스 파일 생성기".
2. 필요한 정보를 입력합니다.
3. 제품 라인 필드의 풀다운 메뉴에서 * SnapCenter 표준(용량 기반) * 을 선택합니다.
4. 제품 일련 번호 필드에 SnapCenter 라이센스 일련 번호를 입력합니다
5. NetApp 데이터 개인 정보 보호 정책을 읽고 동의한 다음 * 제출 * 을 선택합니다.
6. 라이센스 파일을 저장한 다음 파일 위치를 기록합니다.

4단계**:** 용량 기반 라이센스 추가

ONTAP Select 또는 Cloud Volumes ONTAP 플랫폼과 함께 SnapCenter를 사용하는 경우 SnapCenter 용량 기반 라이센스를 하나 이상 설치해야 합니다.

시작하기 전에

- SnapCenter 관리자로 로그인해야 합니다.

- 유효한 NetApp Support 사이트 로그인 자격 증명이 있어야 합니다.
- 51xxxxxxx 형식의 라이센스 일련 번호는 9자리 숫자여야 합니다.

  NetApp 라이센스 파일(NLF)을 사용하여 라이센스를 추가하는 경우 라이센스 파일의 위치를 알아야 합니다.

이 작업에 대해

설정 페이지에서 다음 작업을 수행할 수 있습니다.

- 라이센스를 추가합니다.
- 라이센스 세부 정보를 보고 각 라이센스에 대한 정보를 빠르게 찾습니다.
- 라이센스 용량을 업데이트하거나 임계값 알림 설정을 변경하는 등 기존 라이센스를 대체하려는 경우 라이센스를 수정합니다.
- 기존 라이센스를 교체하려는 경우 또는 라이센스가 더 이상 필요하지 않은 경우 라이센스를 삭제합니다.

> 평가판 라이센스(일련 번호가 50으로 끝나는 번호)는 SnapCenter GUI를 사용하여 삭제할 수 없습니다. 조달된 SnapCenter 표준 용량 기반 라이센스를 추가하면 평가판 라이센스가 자동으로 덮어쓰여집니다.

단계

1. 왼쪽 탐색 창에서 * 설정 * 을 선택합니다.
2. 설정 페이지에서 * 소프트웨어 * 를 선택합니다.
3. 소프트웨어 페이지의 라이센스 섹션에서 * 추가 * (+)를 클릭합니다.
4. SnapCenter 라이센스 추가 마법사에서 다음 방법 중 하나를 선택하여 추가할 라이센스를 가져옵니다.

이 필드의 내용...	수행할 작업...
NSS(NetApp Support Site) 로그인 자격 증명을 입력하여 라이센스를 가져옵니다	a. NSS 사용자 이름을 입력합니다. b. NSS 암호를 입력합니다. c. 컨트롤러 기반 라이센스의 일련 번호를 입력합니다.
NetApp 라이센스 파일	a. 라이센스 파일의 위치를 찾은 다음 선택합니다. b. 열기 * 를 선택합니다.

5. 알림 페이지에서 SnapCenter에서 이메일, EMS 및 AutoSupport 알림을 보내는 용량 임계값을 입력합니다.

   기본 임계값은 90%입니다.

6. 이메일 알림에 맞게 SMTP 서버를 구성하려면 * 설정 * > * 글로벌 설정 * > * 알림 서버 설정 * 을 선택한 후 다음 세부 정보를 입력합니다.

이 필드의 내용...	수행할 작업...
이메일 기본 설정	Always * 또는 * Never * 중에서 선택합니다.
이메일 설정을 제공합니다	Always * 를 선택한 경우 다음을 지정합니다. • 보낸 사람 이메일 주소입니다 • 수신자 이메일 주소입니다 • 선택 사항: 기본 제목 줄을 편집합니다 기본 제목은 "SnapCenter 라이센스 용량 알림 "입니다.

7. 스토리지 시스템 syslog에 EMS(이벤트 관리 시스템) 메시지를 보내거나 스토리지 시스템에 실패한 작업을 위한 AutoSupport 메시지를 보내려면 적절한 확인란을 선택합니다. 발생할 수 있는 문제를 해결하려면 AutoSupport를 활성화하는 것이 좋습니다.
8. 다음 * 을 선택합니다.
9. 요약을 검토한 후 * Finish * 를 선택합니다.

스토리지 시스템을 프로비저닝합니다

Windows 호스트에서 스토리지 용량 할당

LUN 스토리지를 구성합니다

SnapCenter를 사용하여 FC 연결 또는 iSCSI 연결 LUN을 구성할 수 있습니다. SnapCenter를 사용하여 기존 LUN을 Windows 호스트에 연결할 수도 있습니다.

LUN은 SAN 구성의 기본 스토리지 단위입니다. Windows 호스트는 시스템의 LUN을 가상 디스크로 인식합니다. 자세한 내용은 을 참조하십시오 "ONTAP 9 SAN 구성 가이드".

iSCSI 세션을 설정합니다

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

- 시작하기 전에 *
- 스토리지 시스템 노드를 iSCSI 타겟으로 정의해야 합니다.
- 스토리지 시스템에서 iSCSI 서비스를 시작해야 합니다. "자세한 정보"
- 이 작업에 대한 정보 *

IPv6에서 IPv6로 또는 IPv4에서 IPv4로 동일한 IP 버전 간에만 iSCSI 세션을 설정할 수 있습니다.

iSCSI 세션 관리 및 호스트와 타겟 간의 통신에는 둘 다 동일한 서브넷에 있는 경우에만 링크 로컬 IPv6 주소를 사용할 수 있습니다.

iSCSI 이니시에이터의 이름을 변경하면 iSCSI 대상에 대한 액세스가 영향을 받습니다. 이름을 변경한 후에는 이니시에이터가 새 이름을 인식할 수 있도록 타겟을 재구성해야 할 수 있습니다. iSCSI 이니시에이터의 이름을 변경한 후 호스트를 다시 시작해야 합니다.

호스트에 둘 이상의 iSCSI 인터페이스가 있는 경우 첫 번째 인터페이스의 IP 주소를 사용하여 SnapCenter에 iSCSI 세션을 설정한 후에는 다른 IP 주소를 가진 다른 인터페이스에서 iSCSI 세션을 설정할 수 없습니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
  2. 호스트 페이지에서 * iSCSI 세션 * 을 클릭합니다.
  3. Storage Virtual Machine * 드롭다운 목록에서 iSCSI 타겟의 SVM(스토리지 가상 머신)을 선택합니다.
  4. Host * (호스트 *) 드롭다운 목록에서 세션의 호스트를 선택합니다.
  5. 세션 설정 * 을 클릭합니다.

     세션 설정 마법사가 표시됩니다.

  6. 세션 설정 마법사에서 타겟을 식별합니다.

이 필드에서...	입력...
타겟 노드 이름입니다	iSCSI 타겟의 노드 이름입니다 기존 타겟 노드 이름이 있는 경우 해당 이름이 읽기 전용 형식으로 표시됩니다.
대상 포털 주소입니다	대상 네트워크 포털의 IP 주소입니다
대상 포털 포트입니다	대상 네트워크 포털의 TCP 포트입니다
이니시에이터 포털 주소입니다	이니시에이터 네트워크 포털의 IP 주소입니다

  7. 입력한 내용에 만족하면 * 연결 * 을 클릭합니다.

     SnapCenter가 iSCSI 세션을 설정합니다.

  8. 이 절차를 반복하여 각 타겟에 대한 세션을 설정합니다.

iSCSI 세션 연결을 해제합니다

경우에 따라 여러 세션이 있는 대상에서 iSCSI 세션의 연결을 끊어야 할 수 있습니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
  2. 호스트 페이지에서 * iSCSI 세션 * 을 클릭합니다.
  3. Storage Virtual Machine * 드롭다운 목록에서 iSCSI 타겟의 SVM(스토리지 가상 머신)을 선택합니다.
  4. Host * (호스트 *) 드롭다운 목록에서 세션의 호스트를 선택합니다.

5. iSCSI 세션 목록에서 연결을 끊을 세션을 선택하고 * 세션 연결 끊기 * 를 클릭합니다.
6. 세션 연결 끊기 대화 상자에서 * 확인 * 을 클릭합니다.

   SnapCenter는 iSCSI 세션의 연결을 끊습니다.

Igroup 생성 및 관리

이니시에이터 그룹(igroup)을 생성하여 스토리지 시스템에서 특정 LUN에 액세스할 수 있는 호스트를 지정합니다. SnapCenter를 사용하여 Windows 호스트에서 igroup을 생성, 이름 바꾸기, 수정 또는 삭제할 수 있습니다.

igroup 작성

SnapCenter를 사용하여 Windows 호스트에서 igroup을 생성할 수 있습니다. igroup을 LUN에 매핑할 때 디스크 생성 또는 디스크 연결 마법사에서 해당 igroup을 사용할 수 있습니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
  2. 호스트 페이지에서 * iGroup * 을 클릭합니다.
  3. 이니시에이터 그룹 페이지에서 * 신규 * 를 클릭합니다.
  4. Create iGroup 대화 상자에서 igroup을 정의합니다.

이 필드에서...	수행할 작업...
스토리지 시스템	igroup에 매핑할 LUN의 SVM을 선택합니다.
호스트	igroup을 생성할 호스트를 선택합니다.
Igroup 이름입니다	igroup의 이름을 입력합니다.
이니시에이터	이니시에이터를 선택합니다.
유형	이니시에이터 유형, iSCSI, FCP 또는 혼합(FCP 및 iSCSI)을 선택합니다.

  5. 입력한 내용에 만족하면 * 확인 * 을 클릭합니다.

     SnapCenter이 스토리지 시스템에서 igroup을 생성합니다.

igroup의 이름을 바꿉니다

SnapCenter를 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 바꿀 igroup에 사용할 SVM을 선택합니다.
4. SVM의 igroup 목록에서 이름을 바꿀 igroup을 선택하고 * 이름 바꾸기 * 를 클릭합니다.
5. igroup 이름 바꾸기 대화 상자에서 igroup의 새 이름을 입력하고 * 이름 바꾸기 * 를 클릭합니다.

igroup을 수정합니다

SnapCenter를 사용하여 igroup 이니시에이터를 기존 igroup에 추가할 수 있습니다. igroup을 작성하는 동안 하나의 호스트만 추가할 수 있습니다. 클러스터에 대한 igroup을 작성하려는 경우 igroup을 수정하여 해당 igroup에 다른 노드를 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, 수정할 igroup에 사용할 SVM을 선택합니다.
  4. igroup 목록에서 igroup을 선택하고 * igroup에 이니시에이터 추가 * 를 클릭합니다.
  5. 호스트를 선택합니다.
  6. 이니시에이터를 선택하고 * OK * 를 클릭합니다.

igroup을 삭제합니다

더 이상 필요하지 않은 경우 SnapCenter를 사용하여 igroup을 삭제할 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, 삭제할 igroup에 사용할 SVM을 선택합니다.
  4. SVM의 igroup 목록에서 삭제할 igroup을 선택하고 * Delete * 를 클릭합니다.
  5. Delete igroup (그룹 삭제) 대화 상자에서 * OK * (확인 *)를 클릭합니다.

     SnapCenter이 igroup을 삭제합니다.

디스크를 생성하고 관리합니다

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

- SnapCenter는 기본 디스크만 지원합니다. 동적 디스크는 지원되지 않습니다.
- GPT의 경우 하나의 데이터 파티션 및 MBR의 경우 NTFS 또는 CSVFS로 포맷된 하나의 볼륨이 있고 하나의 마운트 경로가 있는 하나의 기본 파티션이 허용됩니다.

- 지원되는 파티션 스타일: GPT, MBR; VMware UEFI VM에서는 iSCSI 디스크만 지원됩니다

> SnapCenter에서는 디스크 이름을 변경할 수 없습니다. SnapCenter에서 관리하는 디스크의 이름을 바꾸면 SnapCenter 작업이 실패합니다.

호스트의 디스크를 봅니다

SnapCenter로 관리하는 각 Windows 호스트에서 디스크를 볼 수 있습니다.

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

     디스크가 나열됩니다.

클러스터링된 디스크를 봅니다

SnapCenter로 관리하는 클러스터에서 클러스터링된 디스크를 볼 수 있습니다. 클러스터 디스크는 호스트 드롭다운에서 클러스터를 선택한 경우에만 표시됩니다.

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

     디스크가 나열됩니다.

FC 연결 또는 **iSCSI** 연결 **LUN** 또는 디스크를 생성합니다

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

SnapCenter 외부에서 디스크를 생성하고 포맷하려면 NTFS 및 CVFS 파일 시스템만 지원됩니다.

시작하기 전에

- 스토리지 시스템에서 LUN에 대한 볼륨을 생성해야 합니다.

  볼륨에는 LUN만 있어야 하며 SnapCenter를 사용하여 생성한 LUN만 포함해야 합니다.

  > 클론이 이미 분할되어 있지 않으면 SnapCenter에서 생성한 클론 볼륨에 LUN을 생성할 수 없습니다.

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

- 이 작업에 대한 정보 *
- Windows Server 페일오버 클러스터의 호스트에서 LUN을 공유하지 않는 한 LUN을 둘 이상의 호스트에 연결할 수 없습니다.
- CSV(Cluster Shared Volumes)를 사용하는 Windows Server 페일오버 클러스터의 호스트가 LUN을 공유하는 경우 클러스터 그룹을 소유하는 호스트에 디스크를 생성해야 합니다.
- 단계 *
  1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
  2. 호스트 페이지에서 * 디스크 * 를 클릭합니다.
  3. 호스트 * 드롭다운 목록에서 호스트를 선택합니다.
  4. 새로 만들기 * 를 클릭합니다.

     디스크 생성 마법사가 열립니다.

  5. LUN 이름 페이지에서 LUN을 확인합니다.

이 필드에서...	수행할 작업...
스토리지 시스템	LUN의 SVM을 선택합니다.
LUN 경로입니다	찾아보기 * 를 클릭하여 LUN이 포함된 폴더의 전체 경로를 선택합니다.
LUN 이름입니다	LUN의 이름을 입력합니다.
클러스터 크기	클러스터의 LUN 블록 할당 크기를 선택합니다. 클러스터 크기는 운영 체제 및 애플리케이션에 따라 다릅니다.
LUN 레이블입니다	선택적으로 LUN에 대한 설명 텍스트를 입력합니다.

  6. 디스크 유형 페이지에서 디스크 유형을 선택합니다.

선택...	만약...
전용 디스크	LUN은 하나의 호스트만 액세스할 수 있습니다. 리소스 그룹 * 필드는 무시하십시오.
공유 디스크	LUN은 Windows Server 페일오버 클러스터의 호스트에서 공유됩니다. 리소스 그룹 * 필드에 클러스터 리소스 그룹의 이름을 입력합니다. 페일오버 클러스터의 한 호스트에만 디스크를 생성해야 합니다.

선택...	만약...
CSV(클러스터 공유 볼륨)	LUN은 CSV를 사용하는 Windows Server 페일오버 클러스터의 호스트에서 공유됩니다. 리소스 그룹 * 필드에 클러스터 리소스 그룹의 이름을 입력합니다. 디스크를 생성할 호스트가 클러스터 그룹의 소유자인지 확인합니다.

7. 드라이브 속성 페이지에서 드라이브 속성을 지정합니다.

속성	설명
마운트 지점을 자동으로 할당합니다	SnapCenter는 시스템 드라이브에 따라 볼륨 마운트 지점을 자동으로 할당합니다. 예를 들어, 시스템 드라이브가 C:인 경우 자동 할당은 C: 드라이브(C:\scmnpt\) 아래에 볼륨 마운트 지점을 생성합니다. 공유 디스크에는 자동 할당이 지원되지 않습니다.
드라이브 문자를 할당합니다	인접한 드롭다운 목록에서 선택한 드라이브에 디스크를 마운트합니다.
볼륨 마운트 지점을 사용합니다	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 선택합니다.
LUN 크기입니다	최소 150MB의 LUN 크기를 지정합니다. 인접 드롭다운 목록에서 MB, GB 또는 TB를 선택합니다.
이 LUN을 호스팅하는 볼륨에 씬 프로비저닝을 사용합니다	씬 LUN을 프로비저닝합니다. 씬 프로비저닝은 필요한 만큼의 스토리지 공간만 한 번에 할당하므로 LUN이 최대 가용 용량까지 효율적으로 성장할 수 있습니다. 필요한 모든 LUN 스토리지를 수용할 수 있는 충분한 공간이 볼륨에 있는지 확인하십시오.

속성	설명
파티션 유형을 선택합니다	GUID 파티션 테이블의 GPT 파티션 또는 마스터 부트 레코드의 MBR 파티션을 선택합니다. MBR 파티션은 Windows Server 장애 조치 클러스터에서 정렬 불량 문제를 일으킬 수 있습니다. UEFI(Unified Extensible Firmware Interface) 파티션 디스크는 지원되지 않습니다.

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

이 필드에서...	수행할 작업...
호스트	클러스터 그룹 이름을 두 번 클릭하여 클러스터에 속한 호스트를 보여 주는 드롭다운 목록을 표시한 다음, 이니시에이터의 호스트를 선택합니다. 이 필드는 LUN이 Windows Server 페일오버 클러스터의 호스트에서 공유되는 경우에만 표시됩니다.
호스트 이니시에이터를 선택합니다	파이버 채널 * 또는 * iSCSI * 를 선택한 다음 호스트에서 이니시에이터를 선택합니다. 다중 경로 I/O(MPIO)와 함께 FC를 사용하는 경우 여러 FC 이니시에이터를 선택할 수 있습니다.

9. 그룹 유형 페이지에서 기존 igroup을 LUN에 매핑할지 또는 새 igroup을 생성할지를 지정합니다.

선택...	만약...
선택한 이니시에이터에 대해 새 igroup을 생성합니다	선택한 이니시에이터에 대해 새 igroup을 생성하려고 합니다.
기존 igroup을 선택하거나 선택한 이니시에이터에 대한 새 igroup을 지정합니다	선택한 이니시에이터에 대해 기존 igroup을 지정하거나 지정한 이름의 새 igroup을 생성합니다. igroup 이름 * 필드에 igroup 이름을 입력합니다. 기존 igroup 이름의 처음 몇 글자를 입력하여 필드를 자동으로 작성합니다.

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

    SnapCenter는 LUN을 생성하여 호스트의 지정된 드라이브 또는 드라이브 경로에 연결합니다.

디스크 크기를 조정합니다

스토리지 시스템 요구사항의 변화에 따라 디스크 크기를 늘리거나 줄일 수 있습니다.

- 이 작업에 대한 정보 *
- 씬 프로비저닝된 LUN의 경우 ONTAP LUN 지오메트리 크기가 최대 크기로 표시됩니다.
- 일반 프로비저닝된 LUN의 경우 확장 가능한 크기(볼륨에서 사용 가능한 크기)가 최대 크기로 표시됩니다.
- MBR 스타일 파티션이 있는 LUN의 크기는 2TB로 제한됩니다.
- GPT 스타일 파티션이 있는 LUN의 스토리지 시스템 크기는 16TB로 제한됩니다.
- LUN 크기를 조정하기 전에 스냅샷 복사본을 만드는 것이 좋습니다.
- LUN의 크기를 변경하기 전에 생성된 스냅샷 복사본에서 LUN을 복원해야 하는 경우 SnapCenter에서는 자동으로 LUN 크기를 스냅샷 복사본 크기로 조정합니다.

  복원 작업 후 크기 조정된 후 LUN에 추가된 데이터는 크기 조정된 후에 만들어진 스냅샷 복사본에서 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 조정할 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 단추가 적절하게 활성화되기 전에 크기 필드 바깥쪽을 클릭해야 합니다. 또한 MB, GB 또는 TB를 클릭하여 측정 단위를 지정해야 합니다.

6. 입력한 내용에 만족하면 * 축소 * 또는 * 확장 * 을 클릭합니다.

   SnapCenter는 디스크의 크기를 조정합니다.

디스크를 연결합니다

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

시작하기 전에

- 스토리지 시스템에서 FC 또는 iSCSI 서비스를 시작해야 합니다.
- iSCSI를 사용하는 경우 스토리지 시스템과 iSCSI 세션을 설정해야 합니다.
- Windows Server 페일오버 클러스터의 호스트에서 LUN을 공유하지 않는 한 LUN을 둘 이상의 호스트에 연결할 수 없습니다.
- CSV(Cluster Shared Volumes)를 사용하는 Windows Server 페일오버 클러스터의 호스트가 LUN을 공유하는 경우 클러스터 그룹을 소유하는 호스트의 디스크를 연결해야 합니다.

- Windows용 플러그인은 디스크를 연결하는 호스트에만 설치해야 합니다.
- 단계 *
  1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
  2. 호스트 페이지에서 * 디스크 * 를 클릭합니다.
  3. 호스트 * 드롭다운 목록에서 호스트를 선택합니다.
  4. 연결 * 을 클릭합니다.

     디스크 연결 마법사가 열립니다.

  5. LUN 이름 페이지에서 접속할 LUN을 확인합니다.

이 필드에서...	수행할 작업...
스토리지 시스템	LUN의 SVM을 선택합니다.
LUN 경로입니다	찾아보기 * 를 클릭하여 LUN이 포함된 볼륨의 전체 경로를 선택합니다.
LUN 이름입니다	LUN의 이름을 입력합니다.
클러스터 크기	클러스터의 LUN 블록 할당 크기를 선택합니다. 클러스터 크기는 운영 체제 및 애플리케이션에 따라 다릅니다.
LUN 레이블입니다	선택적으로 LUN에 대한 설명 텍스트를 입력합니다.

  6. 디스크 유형 페이지에서 디스크 유형을 선택합니다.

선택...	만약...
전용 디스크	LUN은 하나의 호스트만 액세스할 수 있습니다.
공유 디스크	LUN은 Windows Server 페일오버 클러스터의 호스트에서 공유됩니다. 페일오버 클러스터의 한 호스트에만 디스크를 연결해야 합니다.
CSV(클러스터 공유 볼륨)	LUN은 CSV를 사용하는 Windows Server 페일오버 클러스터의 호스트에서 공유됩니다. 디스크에 접속할 호스트가 클러스터 그룹의 소유자인지 확인합니다.

  7. 드라이브 속성 페이지에서 드라이브 속성을 지정합니다.

속성	설명
자동 할당	SnapCenter에서 시스템 드라이브에 따라 볼륨 마운트 지점을 자동으로 할당합니다. 예를 들어, 시스템 드라이브가 C:인 경우 자동 할당 속성은 C: 드라이브(C:\scmnpt\) 아래에 볼륨 마운트 지점을 만듭니다. 공유 디스크에는 자동 할당 속성이 지원되지 않습니다.
드라이브 문자를 할당합니다	인접 드롭다운 목록에서 선택한 드라이브에 디스크를 마운트합니다.
볼륨 마운트 지점을 사용합니다	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 선택합니다.

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

이 필드에서...	수행할 작업...
호스트	클러스터 그룹 이름을 두 번 클릭하여 클러스터에 속한 호스트를 보여 주는 드롭다운 목록을 표시한 다음, 이니시에이터의 호스트를 선택합니다. 이 필드는 LUN이 Windows Server 페일오버 클러스터의 호스트에서 공유되는 경우에만 표시됩니다.
호스트 이니시에이터를 선택합니다	파이버 채널 * 또는 * iSCSI * 를 선택한 다음 호스트에서 이니시에이터를 선택합니다. MPIO에서 FC를 사용하는 경우 여러 FC 이니시에이터를 선택할 수 있습니다.

9. 그룹 유형 페이지에서 기존 igroup을 LUN에 매핑할지 또는 새 igroup을 생성할지를 지정합니다.

선택...	만약...
선택한 이니시에이터에 대해 새 igroup을 생성합니다	선택한 이니시에이터에 대해 새 igroup을 생성하려고 합니다.

선택...	만약...
기존 igroup을 선택하거나 선택한 이니시에이터에 대한 새 igroup을 지정합니다	선택한 이니시에이터에 대해 기존 igroup을 지정하거나 지정한 이름의 새 igroup을 생성합니다. igroup 이름 * 필드에 igroup 이름을 입력합니다. 기존 igroup 이름의 처음 몇 글자를 입력하여 필드를 자동으로 작성합니다.

10. 요약 페이지에서 선택 사항을 검토하고 * 마침 * 을 클릭합니다.

    SnapCenter는 LUN을 호스트의 지정된 드라이브 또는 드라이브 경로에 연결합니다.

디스크 연결을 해제합니다

LUN의 콘텐츠에 영향을 주지 않고 호스트에서 LUN을 분리할 수 있습니다. 단, 클론을 분리하기 전에 연결을 끊으면 클론의 내용이 손실됩니다.

시작하기 전에

- LUN을 다른 애플리케이션에서 사용하고 있지 않은지 확인합니다.
- 모니터링 소프트웨어를 사용하여 LUN을 모니터링하고 있지 않은지 확인합니다.
- LUN을 공유하는 경우 LUN에서 클러스터 리소스 종속성을 제거하고 클러스터의 모든 노드가 켜져 있고, 제대로 작동하고, SnapCenter에서 사용할 수 있는지 확인합니다.
- 이 작업에 대한 정보 *

SnapCenter에서 생성한 FlexClone 볼륨에서 LUN의 연결을 끊은 후 볼륨의 다른 LUN이 연결되어 있지 않으면 SnapCenter가 해당 볼륨을 삭제합니다. LUN을 분리하기 전에 SnapCenter FlexClone 볼륨이 삭제되었을 수 있다는 경고 메시지가 표시됩니다.

FlexClone 볼륨이 자동으로 삭제되지 않도록 하려면 마지막 LUN을 분리하기 전에 볼륨의 이름을 바꾸어야 합니다. 볼륨의 이름을 바꿀 때는 이름의 마지막 문자보다 여러 문자를 변경해야 합니다.

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

     디스크가 나열됩니다.

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

     SnapCenter가 디스크의 연결을 끊습니다.

디스크를 삭제합니다

디스크가 더 이상 필요하지 않으면 삭제할 수 있습니다. 디스크를 삭제한 후에는 삭제할 수 없습니다.

- 단계 *

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

   디스크가 나열됩니다.

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

   SnapCenter가 디스크를 삭제합니다.

SMB 공유를 생성하고 관리합니다

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

* 모범 사례: * cmdlet을 사용하면 SnapCenter에서 제공하는 템플릿을 활용하여 공유 구성을 자동화할 수 있으므로 사용하는 것이 좋습니다.

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

이렇게 하는 것이 편하다면 제공된 모델에 따라 템플릿을 직접 만들 수 있습니다. 사용자 지정 템플릿을 만들기 전에 cmdlet 설명서의 매개 변수를 검토해야 합니다.

SMB 공유를 생성합니다

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

SnapCenter를 사용하여 SMB 공유의 데이터베이스를 백업할 수 없습니다. SMB 지원은 프로비저닝에만 제한됩니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 호스트 페이지에서 * 공유 * 를 클릭합니다.
3. Storage Virtual Machine * 드롭다운 목록에서 SVM을 선택합니다.
4. 새로 만들기 * 를 클릭합니다.

   새 공유 대화 상자가 열립니다.

5. 새 공유 대화 상자에서 공유를 정의합니다.

이 필드에서...	수행할 작업...
설명	공유에 대한 설명 텍스트를 입력합니다.

이 필드에서...	수행할 작업...
공유 이름	공유 이름(예: test_share)을 입력합니다. 공유에 대해 입력한 이름도 볼륨 이름으로 사용됩니다. 공유 이름: • UTF-8 문자열이어야 합니다. • 0x00 - 0x1F(둘 다 포함), 0x22(큰따옴표) 및 특수 문자는 포함할 수 없습니다 `\ / [ ] : (vertical bar) < > + = ; , ?`
공유 경로	• 필드를 클릭하여 새 파일 시스템 경로(예: /)를 입력합니다. • 필드를 두 번 클릭하여 기존 파일 시스템 경로 목록에서 선택합니다.

6. 입력한 내용에 만족하면 * 확인 * 을 클릭합니다.

   SnapCenter은 SVM에서 SMB 공유를 생성합니다.

SMB 공유를 삭제합니다

SMB 공유가 더 이상 필요하지 않은 경우 삭제할 수 있습니다.

- 단계 *

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

   SnapCenter는 SVM에서 SMB 공유를 삭제합니다.

스토리지 시스템의 공간을 재확보할 수 있습니다

NTFS는 파일이 삭제되거나 수정될 때 LUN에서 사용 가능한 공간을 추적하지만 새 정보를 스토리지 시스템에 보고하지 않습니다. Windows 호스트용 플러그인에서 공간 재확보 PowerShell cmdlet을 실행하여 새로 확보된 블록이 스토리지에서 사용 가능으로 표시되는지 확인할 수 있습니다.

원격 플러그인 호스트에서 cmdlet을 실행하는 경우 SnapCenter 서버에 대한 연결을 열려면 SnapCenterOpen - SMConnection cmdlet을 실행해야 합니다.

시작하기 전에

- 복구 작업을 수행하기 전에 공간 재확보 프로세스가 완료되었는지 확인해야 합니다.
- LUN이 Windows Server 페일오버 클러스터의 호스트에서 공유되는 경우 클러스터 그룹을 소유하는 호스트에서 공간 재확보를 수행해야 합니다.
- 최적의 스토리지 성능을 얻으려면 최대한 자주 공간 재확보를 수행해야 합니다.

  전체 NTFS 파일 시스템이 스캔되었는지 확인해야 합니다.

- 이 작업에 대한 정보 *
- 공간 재확보는 시간이 많이 걸리고 CPU가 많이 필요하므로 스토리지 시스템과 Windows 호스트 사용량이 적은 경우에 작업을 실행하는 것이 좋습니다.
- 공간 재확보는 거의 모든 가용 공간을 재확보하지만 100%는 재확보하지 않습니다.
- 공간 재확보를 수행하는 동안 디스크 조각 모음을 동시에 실행해서는 안 됩니다.

  이렇게 하면 재확보 프로세스가 느려질 수 있습니다.

- 단계 *

애플리케이션 서버 PowerShell 명령 프롬프트에서 다음 명령을 입력합니다.

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

drive_path 는 LUN에 매핑된 드라이브 경로입니다.

PowerShell cmdlet을 사용하여 스토리지 용량 할당

SnapCenter GUI를 사용하여 호스트 프로비저닝 및 공간 재확보 작업을 수행하지 않으려는 경우 Microsoft Windows용 SnapCenter 플러그인에서 제공하는 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 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

서버에서 Windows용 SnapDrive를 제거하여 SnapCenter PowerShell cmdlet이 손상된 경우 을 참조하십시오 "Windows용 SnapDrive를 제거하면 SnapCenter cmdlet이 중단됨".

VMware 환경에서 스토리지 프로비저닝

VMware 환경에서 Microsoft Windows용 SnapCenter 플러그인을 사용하여 LUN을 생성 및 관리하고 스냅샷 복사본을 관리할 수 있습니다.

지원되는 **VMware** 게스트 **OS** 플랫폼

- 지원되는 Windows Server 버전

- Microsoft 클러스터 구성

  Microsoft iSCSI Software Initiator를 사용할 경우 VMware에서 최대 16개의 노드를 지원하거나 FC를 사용하여 최대 2개의 노드를 지원합니다

- RDM LUN입니다

  일반 RDM용 4개의 LSI Logic SCSI 컨트롤러가 있는 최대 56개의 RDM LUN 또는 Windows 구성용 VMware VM MSCS 박스-박스 플러그인에서 3개의 LSI Logic SCSI 컨트롤러가 있는 42개의 RDM LUN을 지원합니다

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

지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

VMware ESXi 서버 관련 제한 사항

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

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

- 클러스터된 모든 노드는 동일한 클러스터된 디스크에 대해 동일한 대상 ID(가상 SCSI 어댑터)를 사용해야 합니다.
- Windows용 플러그인 외부에서 RDM LUN을 생성하는 경우 플러그인 서비스를 다시 시작하여 새로 생성된 디스크를 인식할 수 있도록 설정해야 합니다.
- VMware 게스트 OS에서는 iSCSI 및 FC 이니시에이터를 동시에 사용할 수 없습니다.

SnapCenter RDM 작업에 필요한 최소 vCenter 권한

게스트 OS에서 RDM 작업을 수행하려면 호스트에 대해 다음과 같은 vCenter 권한이 있어야 합니다.

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

이러한 권한은 Virtual Center Server 수준에서 역할에 할당해야 합니다. 이러한 권한을 할당하는 역할은 루트 권한이 없는 사용자에게 할당할 수 없습니다.

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

Microsoft 클러스터에서 FC RDM LUN을 관리합니다

Windows용 플러그인을 사용하여 FC RDM LUN을 사용하여 Microsoft 클러스터를 관리할 수 있지만 먼저 플러그인 외부에서 공유 RDM 쿼럼과 공유 스토리지를 생성한 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 즉시 사용 가능한 지원이 포함되어 있습니다.

요구 사항

Windows용 플러그인은 특정 구성 요구 사항을 충족하는 경우 두 개의 서로 다른 ESX 또는 ESXi 서버에 속하는 두

개의 서로 다른 가상 시스템에서 FC RDM LUN을 사용하는 Microsoft 클러스터를 지원합니다.

- 가상 머신(VM)은 동일한 Windows Server 버전을 실행해야 합니다.
- ESX 또는 ESXi 서버 버전은 각 VMware 상위 호스트에 대해 동일해야 합니다.
- 각 상위 호스트에는 최소한 두 개의 네트워크 어댑터가 있어야 합니다.
- 두 ESX Server 또는 ESXi Server 간에 공유되는 VMware VMFS(Virtual Machine File System) 데이터 저장소가 하나 이상 있어야 합니다.
- 공유 데이터 저장소를 FC SAN에 생성하는 것이 좋습니다.

  필요한 경우 iSCSI를 통해 공유 데이터 저장소를 생성할 수도 있습니다.

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

  공유 스토리지에는 가상 디스크를 사용할 수 없습니다.

- SCSI 컨트롤러는 클러스터의 각 가상 머신에서 물리적 호환성 모드로 구성해야 합니다.

  Windows Server 2008 R2에서는 각 가상 머신에 LSI Logic SAS SCSI 컨트롤러를 구성해야 합니다. 공유 LUN은 유형 중 하나만 있고 이미 C: 드라이브에 연결되어 있는 경우 기존 LSI Logic SAS 컨트롤러를 사용할 수 없습니다.

  반가상화 유형의 SCSI 컨트롤러는 VMware Microsoft 클러스터에서 지원되지 않습니다.

  > 물리적 호환성 모드에서 가상 시스템의 공유 LUN에 SCSI 컨트롤러를 추가하는 경우 VMware Infrastructure Client에서 * Create a new disk * 옵션이 아닌 * RDM(Raw Device Mappings *) 옵션을 선택해야 합니다.

- Microsoft 가상 머신 클러스터는 VMware 클러스터에 포함될 수 없습니다.
- Microsoft 클러스터에 속한 가상 머신에 Windows용 플러그인을 설치할 때는 ESX 또는 ESXi 자격 증명이 아닌 vCenter 자격 증명을 사용해야 합니다.
- Windows용 플러그인은 여러 호스트의 이니시에이터를 포함하는 단일 igroup을 생성할 수 없습니다.

  공유 클러스터 디스크로 사용될 RDM LUN을 생성하기 전에 모든 ESXi 호스트의 이니시에이터를 포함하는 igroup을 스토리지 컨트롤러에서 생성해야 합니다.

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

  RDM LUN을 생성할 때 이니시에이터 그룹은 ALUA를 통해 생성됩니다.

제한 사항

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

> 이 기능은 ESX 5.5i 이전의 릴리즈에서는 지원되지 않습니다.

- Windows용 플러그인은 ESX iSCSI 및 NFS 데이터 저장소의 클러스터를 지원하지 않습니다.

- Windows용 플러그인은 클러스터 환경에서 혼합 이니시에이터를 지원하지 않습니다.

  이니시에이터는 FC 또는 Microsoft iSCSI 중 하나여야 하며 둘 다 사용할 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 시스템에서 MPIO를 지원하지 않습니다.

공유 **FC RDM LUN**을 생성합니다

FC RDM LUN을 사용하여 Microsoft 클러스터의 노드 간에 스토리지를 공유하려면 먼저 공유 쿼럼 디스크와 공유 스토리지 디스크를 생성한 다음 클러스터의 두 가상 머신에 추가해야 합니다.

Windows용 플러그인을 사용하여 공유 디스크가 생성되지 않습니다. 공유 LUN을 생성한 다음 클러스터의 각 가상 머신에 추가해야 합니다.
자세한 내용은 을 참조하십시오 "물리적 호스트에서 가상 시스템을 클러스터링합니다".

SnapCenter 서버로 보안 MySQL 연결을 구성합니다

독립 실행형 구성 또는 NLB(네트워크 로드 밸런싱) 구성에서 SnapCenter 서버와 MySQL 서버 간의 통신을 보호하려는 경우 SSL(Secure Sockets Layer) 인증서 및 키 파일을 생성할 수 있습니다.

독립 실행형 SnapCenter 서버 구성에 대해 보안 MySQL 연결을 구성합니다

SnapCenter 서버와 MySQL 서버 간의 통신을 보호하려면 SSL(Secure Sockets Layer) 인증서와 키 파일을 생성할 수 있습니다. MySQL Server 및 SnapCenter Server에서 인증서 및 키 파일을 구성해야 합니다.

다음 인증서가 생성됩니다.

- CA 인증서
- 서버 공용 인증서 및 개인 키 파일
- 클라이언트 공용 인증서 및 개인 키 파일
- 단계 *

1. openssl 명령을 사용하여 Windows에서 MySQL 서버 및 클라이언트에 대한 SSL 인증서 및 키 파일을 설정합니다.

   자세한 내용은 을 참조하십시오 "MySQL 버전 5.7: openssl을 사용하여 SSL 인증서 및 키 만들기"

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

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

2. SSL 인증서 및 키 파일을 MySQL Data 폴더에 복사합니다.

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

3. MySQL 서버 구성 파일(my.in I)에서 CA 인증서, 서버 공용 인증서, 클라이언트 공용 인증서, 서버 개인 키 및 클라이언트 개인 키 경로를 업데이트합니다.

   기본 MySQL 서버 구성 파일(my.in I) 경로는 입니다 `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.

   MySQL 서버 구성 파일(my.in I)의 [mysqld] 섹션에서 CA 인증서, 서버 공용 인증서 및 서버 개인 키 경로를 지정해야 합니다.

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

   다음 예제에서는 기본 폴더에 있는 my.ini 파일의 [mysqld] 섹션에 복사된 인증서와 키 파일을 보여 줍니다 `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 예제에서는 my.ini 파일의 [client] 섹션에서 업데이트된 경로를 보여 줍니다.

   ```
   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. 인터넷 정보 서버(IIS)에서 SnapCenter 서버 웹 응용 프로그램을 중지합니다.
5. MySQL 서비스를 다시 시작합니다.

6. web.config 파일에서 MySQLProtocol 키 값을 업데이트합니다.

   다음 예제에서는 web.config 파일에서 업데이트된 MySQLProtocol 키의 값을 보여 줍니다.

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

7. my.ini 파일의 [client] 섹션에 제공된 경로로 web.config 파일을 업데이트합니다.

   다음 예제에서는 my.ini 파일의 [client] 섹션에서 업데이트된 경로를 보여 줍니다.

```
<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" />
```

1. IIS에서 SnapCenter 서버 웹 응용 프로그램을 시작합니다.

HA 구성을 위한 보안 MySQL 연결을 구성합니다

SnapCenter 서버와 MySQL 서버 간의 통신을 보호하려면 고가용성(HA) 노드 모두에 대해 SSL(Secure Sockets Layer) 인증서와 키 파일을 생성할 수 있습니다. MySQL 서버 및 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 노드에 대한 서버 공용 인증서 및 서버 개인 키 파일
- 두 HA 노드에 대한 클라이언트 공용 인증서 및 클라이언트 개인 키 파일
- 단계 *

1. 첫 번째 HA 노드의 경우 openssl 명령을 사용하여 Windows에서 MySQL 서버 및 클라이언트에 대한 SSL 인증서 및 키 파일을 설정합니다.

   자세한 내용은 을 참조하십시오 "MySQL 버전 5.7: openssl을 사용하여 SSL 인증서 및 키 만들기"

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

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

2. SSL 인증서 및 키 파일을 MySQL Data 폴더에 복사합니다.

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

3. MySQL 서버 구성 파일(my.in I)에서 CA 인증서, 서버 공용 인증서, 클라이언트 공용 인증서, 서버 개인 키 및 클라이언트 개인 키 경로를 업데이트합니다.

   기본 MySQL 서버 구성 파일(my.in I) 경로는 C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.in 입니다

   MySQL 서버 구성 파일(my.in I)의 [mysqld] 섹션에서 CA 인증서, 서버 공용 인증서 및 서버 개인 키 경로를 지정해야 합니다.

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

   다음 예에서는 기본 폴더 C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data에 있는 my.ini 파일의 [mysqld] 섹션에 복사된 인증서 및 키 파일을 보여 줍니다.

```
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 예제에서는 my.ini 파일의 [client] 섹션에서 업데이트된 경로를 보여 줍니다.

```
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 공용 인증서, 서버 개인 키 파일, 클라이언트 공용 인증서 및 클라이언트 개인 키 파일을 생성합니다. 다음 단계를 수행하십시오.

   a. 첫 번째 HA 노드에서 생성된 CA 인증서를 두 번째 NLB 노드의 MySQL Data 폴더에 복사합니다.

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

      > CA 인증서를 다시 만들 수 없습니다. 서버 공용 인증서, 클라이언트 공용 인증서, 서버 개인 키 파일 및 클라이언트 개인 키 파일만 만들어야 합니다.

   b. 첫 번째 HA 노드의 경우 openssl 명령을 사용하여 Windows에서 MySQL 서버 및 클라이언트에 대한 SSL 인증서 및 키 파일을 설정합니다.

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

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

      서버 인증서의 일반 이름으로 서버 FQDN을 사용하는 것이 좋습니다.

   c. SSL 인증서 및 키 파일을 MySQL Data 폴더에 복사합니다.

   d. MySQL 서버 구성 파일(my.in I)에서 CA 인증서, 서버 공용 인증서, 클라이언트 공용 인증서, 서버 개인 키 및 클라이언트 개인 키 경로를 업데이트합니다.

      > MySQL 서버 구성 파일(my.in I)의 [mysqld] 섹션에서 CA 인증서, 서버 공용 인증서 및 서버 개인 키 경로를 지정해야 합니다.

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

      다음 예에서는 기본 폴더 C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data에 있는 my.ini 파일의 [mysqld] 섹션에 복사된 인증서 및 키 파일을 보여 줍니다.

      ```
      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 예제에서는 my.ini 파일의 [client] 섹션에서 업데이트된 경로를 보여 줍니다.

```
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 노드의 IIS(인터넷 정보 서버)에서 SnapCenter 서버 웹 응용 프로그램을 중지합니다.
6. 두 HA 노드에서 MySQL 서비스를 다시 시작합니다.
7. 두 HA 노드에 대해 web.config 파일에서 MySQLProtocol 키의 값을 업데이트합니다.

   다음 예제에서는 web.config 파일에서 업데이트된 MySQLProtocol 키 값을 보여 줍니다.

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

8. 두 HA 노드에 대해 my.ini 파일의 [client] 섹션에 지정한 경로로 web.config 파일을 업데이트합니다.

   다음 예제에서는 my.ini 파일의 [client] 섹션에서 업데이트된 경로를 보여 줍니다.

```
<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" />
```

1. 두 HA 노드의 IIS에서 SnapCenter 서버 웹 응용 프로그램을 시작합니다.
2. HA 노드 중 하나에서 -Force 옵션과 함께 Set-SmrepositoryConfig-RebuildSlave-Force PowerShell cmdlet을 사용하여 두 HA 노드 모두에 안전한 MySQL 복제를 설정합니다.

   복제 상태가 정상인 경우에도 -Force 옵션을 사용하면 슬레이브 리포지토리를 재구축할 수 있습니다.

설치 중에 **Windows** 호스트에서 활성화된 기능입니다

SnapCenter 서버 설치 프로그램을 사용하면 설치 중에 Windows 호스트에서 Windows 기능 및 역할을 사용할 수 있습니다. 이는 문제 해결 및 호스트 시스템 유지 관리 목적으로 활용할 수 있습니다.

범주	피처
웹 서버	• 인터넷 정보 서비스 • 월드 와이드 웹 서비스 • 공통 HTTP 기능 ◦ 기본 문서 ◦ 디렉터리 검색 ◦ HTTP 오류 ◦ HTTP 리디렉션 ◦ 정적 콘텐츠 ◦ WebDAV 게시 • 상태 및 진단 ◦ 사용자 지정 로깅 ◦ HTTP 로깅 ◦ 로깅 도구 ◦ 모니터 요청 ◦ 추적 • 성능 기능 ◦ 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 권한 부여 ◦ Windows 인증 • 응용 프로그램 개발 기능 ◦ NET 확장성 4.5 ◦ 응용 프로그램 초기화 ◦ ASP.NET 4.7.2 ◦ 서버 측 포함 ◦ WebSocket 프로토콜 관리 도구 IIS 관리 콘솔

범주	피처
IIS 관리 스크립트 및 도구	• IIS 관리 서비스 • 웹 관리 도구
NET Framework 4.7.2 기능+	• NET Framework 4.7.2 • ASP.NET 4.7.2 • WCF(Windows Communication Foundation) HTTP Activation45 ◦ TCP 활성화 ◦ HTTP 활성화 ◦ MSMQ(Message Queuing) 활성화 NET 관련 문제 해결에 대한 자세한 내용은 을 참조하십시오 "인터넷에 연결되지 않은 기존 시스템의 경우 SnapCenter 업그레이드 또는 설치가 실패합니다".
메시지 큐	• 메시지 큐 서비스 SnapCenter가 만들고 관리하는 MSMQ 서비스를 사용하는 다른 응용 프로그램이 없는지 확인합니다. • MSMQ 서버
Windows 프로세스 활성화 서비스	• 프로세스 모델
구성 API	모두

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 클론 작업을 자동화합니다.

SQL Server용 플러그인을 설치하면 SnapCenter와 NetApp SnapMirror 기술을 함께 사용하여 다른 볼륨에 백업 세트의 미러링 복사본을 만들고 NetApp SnapVault 기술을 사용하여 표준 준수 또는 아카이브용으로 D2D 백업 복제를 수행할 수 있습니다.

Microsoft SQL Server용 SnapCenter 플러그인으로 수행할 수 있는 작업

사용자 환경에 Microsoft SQL Server용 SnapCenter 플러그인이 설치되어 있는 경우 SnapCenter를 사용하여 SQL Server 데이터베이스를 백업, 복원 및 복제할 수 있습니다.

SQL Server 데이터베이스 및 데이터베이스 리소스의 백업 작업, 복원 작업 및 클론 작업을 지원하는 다음 작업을 수행할 수 있습니다.

- SQL Server 데이터베이스 및 관련 트랜잭션 로그를 백업합니다

  마스터 및 msdb 시스템 데이터베이스에 대한 로그 백업을 만들 수 없습니다. 그러나 모델 시스템 데이터베이스에 대한 로그 백업을 생성할 수 있습니다.

- 데이터베이스 리소스를 복원합니다
  - 마스터 시스템 데이터베이스, msdb 시스템 데이터베이스 및 모델 시스템 데이터베이스를 복원할 수 있습니다.
  - 여러 데이터베이스, 인스턴스 및 가용성 그룹은 복원할 수 없습니다.
  - 시스템 데이터베이스를 대체 경로로 복원할 수 없습니다.
- 운영 데이터베이스의 시점 복제본을 생성합니다

  tempdb 시스템 데이터베이스에는 백업, 복원, 클론 및 클론 수명주기 작업을 수행할 수 없습니다.

- 백업 작업을 즉시 확인하거나 나중에 확인을 연기할 수 있습니다

  SQL Server 시스템 데이터베이스 확인은 지원되지 않습니다. SnapCenter는 데이터베이스를 복제하여 검증 작업을 수행합니다. SnapCenter는 SQL Server 시스템 데이터베이스를 복제할 수 없으므로 이러한 데이터베이스를 확인할 수 없습니다.

- 백업 작업 및 클론 작업 예약
- 백업 작업, 복원 작업 및 클론 작업을 모니터링합니다

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 Server 및 스토리지 시스템의 NetApp Snapshot 복사본 기술과 통합됩니다. SQL Server용 플러그인으로 작업하려면 SnapCenter 인터페이스를 사용합니다.

SQL Server용 플러그인에는 다음과 같은 주요 기능이 포함되어 있습니다.

- * SnapCenter * 기반 통합 그래픽 사용자 인터페이스

  SnapCenter 인터페이스는 전체 플러그인과 환경에 걸쳐 표준화와 일관성을 제공합니다. SnapCenter 인터페이스를 사용하면 플러그인 전체에 걸쳐 일관된 백업 및 복원 프로세스를 완료하고, 중앙 집중식 보고, 대시보드 뷰 사용량을 한 눈에 확인 하고, RBAC(역할 기반 액세스 제어)를 설정하고, 모든 플러그인에 걸쳐 작업을 모니터링할 수 있습니다. 또한 SnapCenter는 중앙 집중식 스케줄링 및 정책 관리 기능을 제공하여 백업 및 클론 작업을 지원합니다.

- * 자동화된 중앙 관리 *

  일상적인 SQL Server 백업을 예약하고, 정책 기반 백업 보존을 구성하고, 시점 및 최신 복원 작업을 설정할 수 있습니다. 또한 전자 메일 경고를 보내도록 SnapCenter를 구성하여 SQL Server 환경을 사전 예방적으로 모니터링할 수도 있습니다.

- * 무중단 NetApp 스냅샷 복사본 기술 *

  SQL Server용 플러그인은 NetApp Snapshot 복사본 기술을 Microsoft Windows용 SnapCenter 플러그인과 함께 사용합니다. 따라서 SQL Server를 오프라인으로 전환하지 않고도 몇 초 내에 데이터베이스를 백업하고 신속하게 복원할 수 있습니다. 스냅샷 복사본은 최소 스토리지 공간을 사용합니다.

이러한 주요 기능 외에도 SQL Server용 플러그인은 다음과 같은 이점을 제공합니다.

- 백업, 복원, 클론, 검증 워크플로우 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임
- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 공간 효율적인 운영 데이터베이스 시점 복사본 생성

  클론을 보유하는 스토리지 시스템에는 FlexClone 라이센스가 필요합니다.

- 무중단 및 자동화된 백업 검증
- 여러 서버에서 동시에 여러 백업을 실행할 수 있습니다
- 백업, 확인, 복원 및 클론 작업의 스크립팅을 위한 PowerShell cmdlet
- SQL Server의 AGS(AlwaysOn Availability Groups)를 지원하여 AG 설정, 백업 및 복원 작업을 가속화합니다
- SQL Server 2014의 일부로 인메모리 데이터베이스 및 BPE(Buffer Pool Extension)를 지원합니다
- LUN 및 가상 머신 디스크(VMDK)의 백업 지원

- 물리적 인프라와 가상화 인프라 지원
- iSCSI, Fibre Channel, FCoE, RDM(Raw Device Mapping) 및 VMDK over NFS 및 VMFS 지원

  NAS 볼륨은 스토리지 가상 시스템(SVM)에서 기본 엑스포트 정책을 사용해야 합니다.

- SQL Server 독립 실행형 데이터베이스의 FileStream 및 파일 그룹 지원

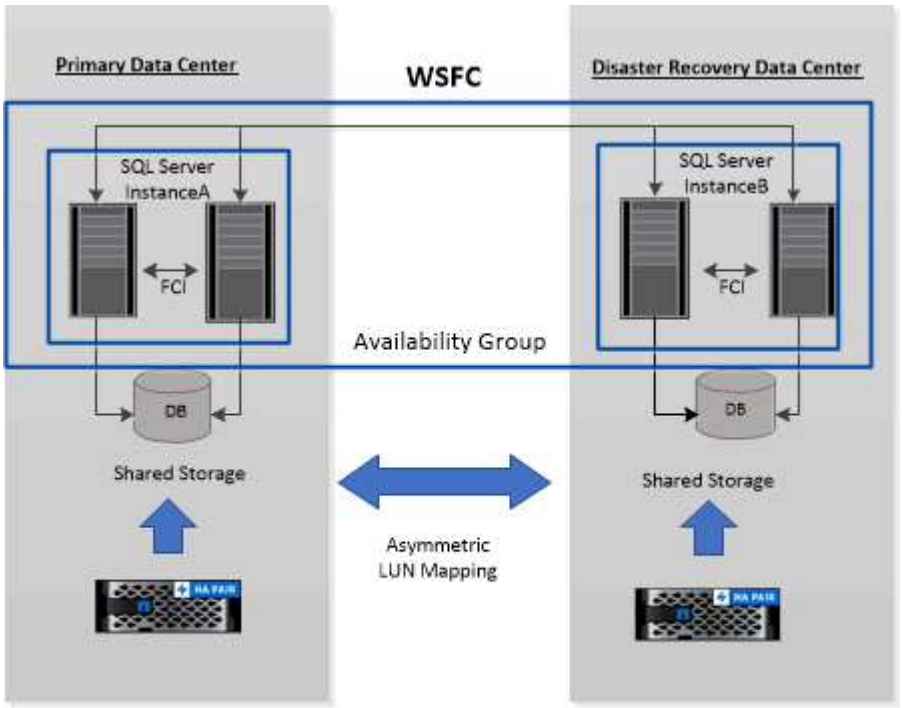
Windows 클러스터에서 비대칭 LUN 매핑 지원

Microsoft SQL Server용 SnapCenter 플러그인은 SQL Server 2012 이상에서 검색, 고가용성을 위한 Asymmetric LUN Mapping(ALM) 구성, 재해 복구를 위한 가용성 그룹을 지원합니다. 리소스를 검색할 때 SnapCenter는 로컬 호스트와 ALM 구성의 원격 호스트에서 데이터베이스를 검색합니다.

ALM 구성은 운영 데이터 센터에 하나 이상의 노드와 재해 복구 센터에 하나 이상의 노드를 포함하는 단일 Windows 서버 장애 조치 클러스터입니다.

다음은 ALM 구성의 예입니다.

- 다중 사이트 데이터 센터에서 두 개의 FCI(장애 조치 클러스터 인스턴스)
- 재해 복구 사이트에서 독립 실행형 인스턴스를 사용하여 재해 복구를 위한 로컬 HA(고가용성) 및 AG(가용성 그룹)용 FCI



WSFC----Windows Server Failover Cluster

운영 데이터 센터의 스토리지는 운영 데이터 센터에 있는 FCI 노드 간에 공유됩니다. 재해 복구 데이터 센터의 스토리지는 재해 복구 데이터 센터에 있는 FCI 노드 간에 공유됩니다.

운영 데이터 센터의 스토리지는 재해 복구 데이터 센터의 노드에 표시되지 않으며 그 반대의 경우도 마찬가지입니다.

ALM 아키텍처는 FCI에서 사용하는 두 개의 공유 스토리지 솔루션과 SQL AG에서 사용하는 비공유 또는 전용 스토리지 솔루션을 결합합니다. AG 솔루션은 데이터 센터 전체에서 공유 디스크 리소스에 동일한 드라이브 문자를 사용합니다. WSFC 내의 노드 하위 집합 간에 클러스터 디스크를 공유하는 이러한 스토리지 배열을 ALM이라고 합니다.

Microsoft Windows용 **SnapCenter** 플러그인 및 **Microsoft SQL Server**용 플러그인이 지원하는 스토리지 유형입니다

SnapCenter는 물리적 시스템과 가상 머신 모두에서 다양한 스토리지 유형을 지원합니다. 호스트에 대한 패키지를 설치하기 전에 스토리지 유형에 대한 지원이 가능한지 확인해야 합니다.

SnapCenter 프로비저닝 및 데이터 보호 지원은 Windows Server에서 제공됩니다. 지원되는 버전에 대한 최신 정보는 를 참조하십시오
"NetApp 상호 운용성 매트릭스 툴".

기계	스토리지 유형입니다	를 사용하여 프로비저닝	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	스토리지 가상 시스템(SVM)에 상주하는 SMB3(CIFS) 공유	SnapCenter GUI 또는 PowerShell cmdlet	프로비저닝만 지원합니다. SnapCenter를 사용하여 SMB 프로토콜을 사용하는 데이터 또는 공유를 백업할 수 없습니다.
VMware VM	FC 또는 iSCSI HBA를 통해 연결된 RDM LUN	PowerShell cmdlet	
VMware VM	iSCSI 이니시에이터가 게스트 시스템에 직접 접속된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	
VMware VM	VMFS(Virtual Machine File Systems) 또는 NFS 데이터 저장소	VMware vSphere를 참조하십시오	
VMware VM	SVM에 상주하는 SMB3 공유에 연결된 게스트 시스템입니다	SnapCenter GUI 또는 PowerShell cmdlet	프로비저닝만 지원합니다. SnapCenter를 사용하여 SMB 프로토콜을 사용하는 데이터 또는 공유를 백업할 수 없습니다.

기계	스토리지 유형입니다	를 사용하여 프로비저닝	지원 노트
Hyper-V VM	가상 Fibre Channel 스위치를 통해 연결된 VFC(가상 FC) LUN입니다	SnapCenter GUI 또는 PowerShell cmdlet	Hyper-V Manager를 사용하여 가상 Fibre Channel 스위치로 연결된 VFC(가상 FC) LUN을 프로비저닝해야 합니다. NetApp 스토리지에 프로비저닝된 Hyper-V는 디스크를 통과하고 VHD(x)에서 데이터베이스를 백업하는 것은 지원되지 않습니다.
Hyper-V VM	iSCSI 이니시에이터가 게스트 시스템에 직접 접속된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	NetApp 스토리지에 프로비저닝된 Hyper-V는 디스크를 통과하고 VHD(x)에서 데이터베이스를 백업하는 것은 지원되지 않습니다.

기계	스토리지 유형입니다	를 사용하여 프로비저닝	지원 노트
Hyper-V VM	SVM에 상주하는 SMB3 공유에 연결된 게스트 시스템입니다	SnapCenter GUI 또는 PowerShell cmdlet	프로비저닝만 지원합니다. SnapCenter를 사용하여 SMB 프로토콜을 사용하는 데이터 또는 공유를 백업할 수 없습니다. NetApp 스토리지에 프로비저닝된 Hyper-V는 디스크를 통과하고 VHD(x)에서 데이터베이스를 백업하는 것은 지원되지 않습니다.

Microsoft SQL Server용 SnapCenter 플러그인의 스토리지 레이아웃 권장 사항

잘 설계된 스토리지 레이아웃을 통해 SnapCenter Server는 복구 목표를 충족하기 위해 데이터베이스를 백업할 수 있습니다. 데이터베이스 크기, 데이터베이스 변경 속도, 백업 수행 빈도 등 스토리지 레이아웃을 정의하는 동안 몇 가지 요소를 고려해야 합니다.

다음 섹션에서는 사용자 환경에 설치된 Microsoft SQL Server용 SnapCenter 플러그인을 사용하여 LUN 및 VMDK(가상 머신 디스크)에 대한 스토리지 레이아웃 권장 사항 및 제한 사항을 정의합니다.

이 경우 LUN에는 게스트에 매핑된 VMware RDM 디스크 및 iSCSI 직접 연결 LUN이 포함될 수 있습니다.

LUN 및 VMDK 요구 사항

선택적으로 전용 LUN 또는 VMDK를 사용하여 다음 데이터베이스의 성능 및 관리를 최적화할 수 있습니다.

- 마스터 및 모델 시스템 데이터베이스
- tempdb
- 사용자 데이터베이스 파일(.mdf 및 .ndf)
- 사용자 데이터베이스 트랜잭션 로그 파일(.ldf)
- 로그 디렉토리

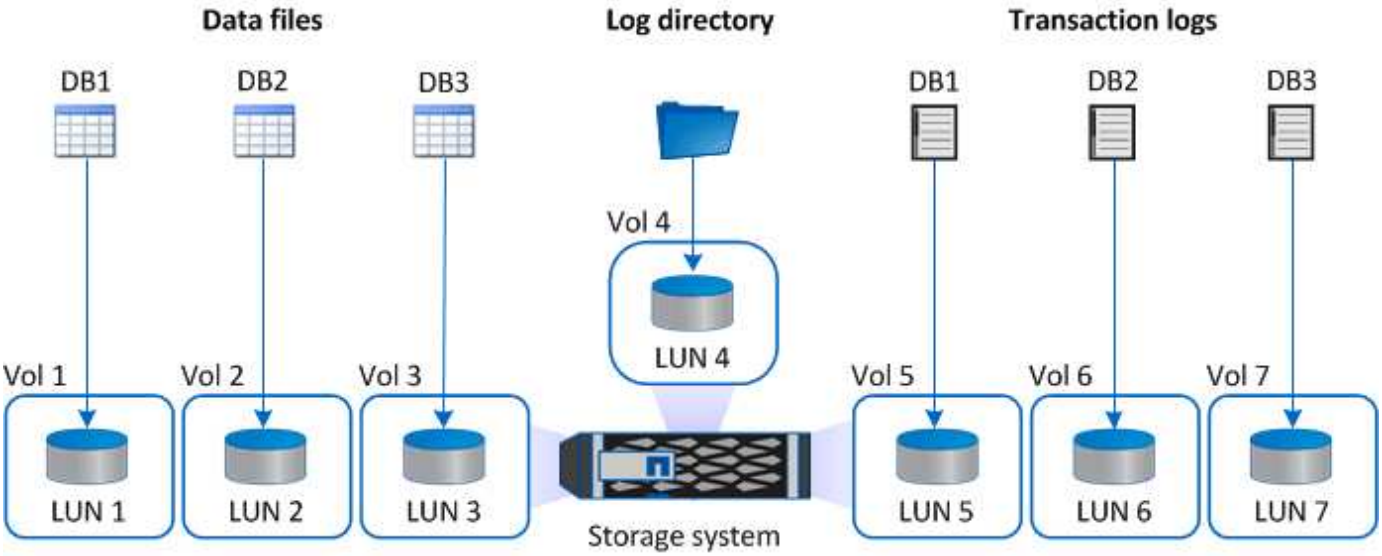
대규모 데이터베이스를 복구하는 모범 사례는 전용 LUN 또는 VMDK를 사용하는 것입니다. 전체 LUN 또는 VMDK를 복원하는 데 걸린 시간이 LUN 또는 VMDK에 저장된 개별 파일을 복원하는 데 걸린 시간보다 작습니다.

로그 디렉토리의 경우 데이터 또는 로그 파일 디스크에 충분한 여유 공간이 있도록 별도의 LUN 또는 VMDK를 생성해야

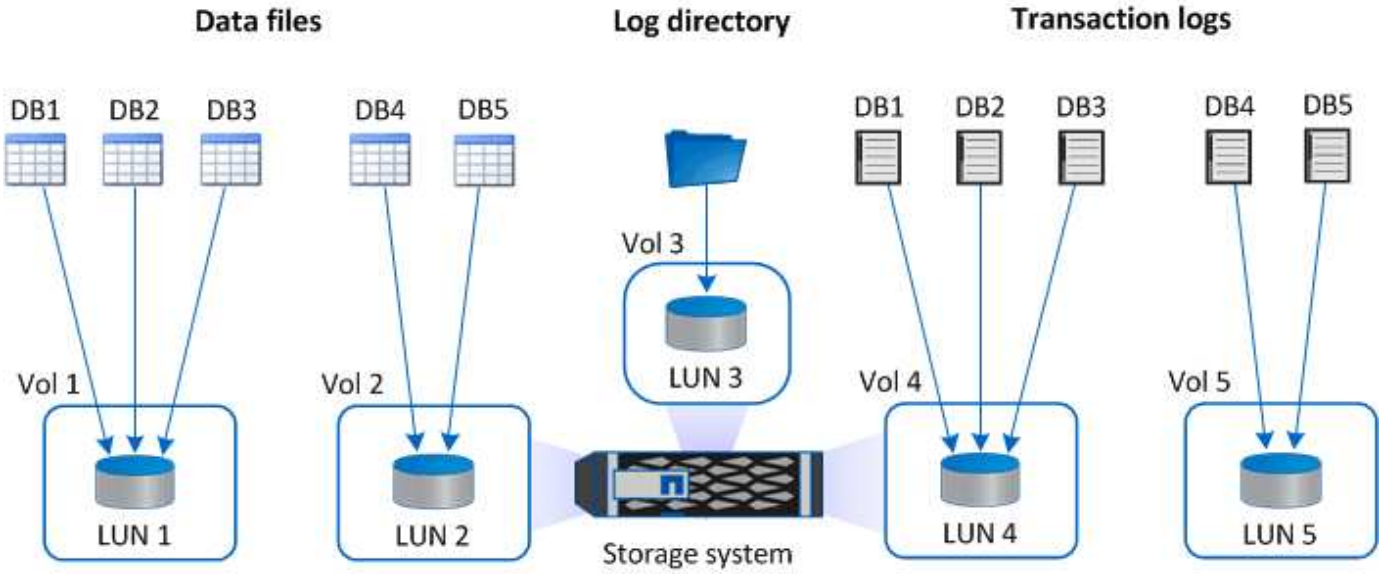
합니다.

LUN 및 **VMDK** 샘플 레이아웃

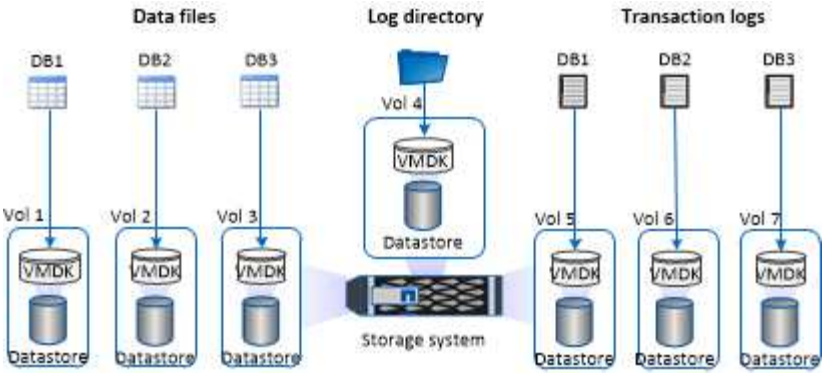
다음 그림에서는 LUN의 대용량 데이터베이스에 대한 스토리지 레이아웃을 구성하는 방법을 보여 줍니다.



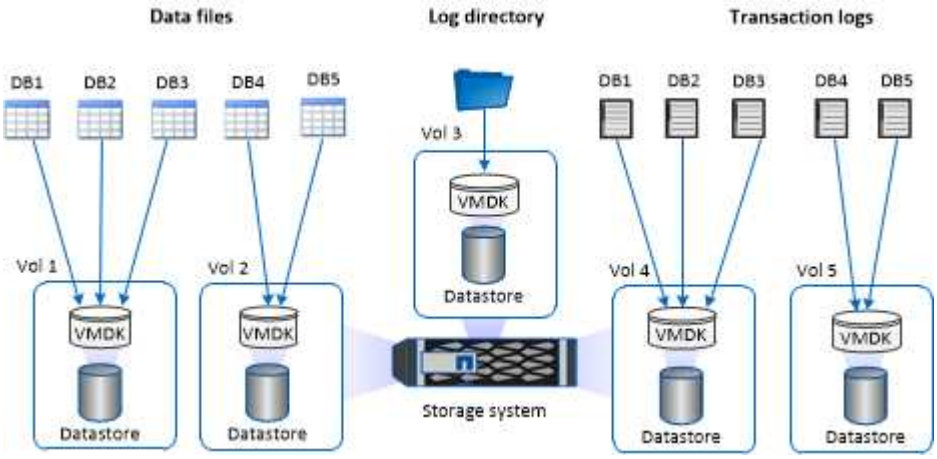
다음 그림에서는 LUN에서 중간 또는 소규모 데이터베이스에 대한 스토리지 레이아웃을 구성하는 방법을 보여 줍니다.



다음 그래픽은 VMDK의 대규모 데이터베이스에 대한 스토리지 레이아웃을 구성하는 방법을 보여 줍니다.



다음 그래픽은 VMDK에서 중간 또는 소규모 데이터베이스의 스토리지 레이아웃을 구성하는 방법을 보여 줍니다.



SQL 플러그인에 필요한 최소 ONTAP 권한

필요한 최소 ONTAP 권한은 데이터 보호를 위해 사용 중인 SnapCenter 플러그인에 따라 다릅니다.

- All-access 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
  - event generate-autosupport-log입니다
  - 작업 기록이 표시됩니다
  - 작업 중지
  - LUN을 클릭합니다
  - LUN 생성
  - LUN을 삭제합니다
  - LUN igroup 추가
  - LUN igroup 작성
  - LUN igroup 삭제
  - LUN igroup의 이름을 바꿉니다
  - LUN igroup 표시
  - LUN 매핑 add-reporting-nodes입니다

- LUN 매핑 생성
- LUN 매핑을 삭제합니다
- LUN 매핑으로 remove-reporting-nodes를 사용할 수 있습니다
- LUN 매핑이 표시됩니다
- LUN 수정
- LUN 이동 - 볼륨
- LUN이 오프라인 상태입니다
- LUN을 온라인 상태로 전환합니다
- LUN 크기 조정
- LUN 일련 번호입니다
- LUN 표시
- SnapMirror 정책 추가 규칙
- SnapMirror 정책 modify-rule을 참조하십시오
- SnapMirror 정책 remove-rule을 참조하십시오
- SnapMirror 정책 쇼
- SnapMirror 복원
- SnapMirror 쇼
- SnapMirror 기록
- SnapMirror 업데이트
- SnapMirror 업데이트 - ls -set
- SnapMirror 목록 - 대상
- 버전
- 볼륨 클론 생성
- 볼륨 클론 표시
- 볼륨 클론 분할 시작이 있습니다
- 볼륨 클론 분할 중지
- 볼륨 생성
- 볼륨 제거
- 볼륨 파일 클론 생성
- 볼륨 파일 show-disk-usage 를 참조하십시오
- 볼륨이 오프라인 상태입니다
- 볼륨을 온라인으로 설정합니다
- 볼륨 수정
- 볼륨 qtree 생성

- 볼륨 qtree 삭제
- 볼륨 qtree 수정
- 볼륨 qtree 표시
- 볼륨 제한
- 볼륨 표시
- 볼륨 스냅샷 생성
- 볼륨 스냅숏 삭제
- 볼륨 스냅숏 수정
- 볼륨 스냅숏 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 - 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- SVM CIFS를 선택합니다
- SVM CIFS 공유 생성
- SVM CIFS 공유 삭제
- SVM CIFS shadowcopy show 를 참조하십시오
- SVM CIFS 공유 표시
- vserver cifs show 를 참조하십시오
- SVM 엑스포트 - 정책
- SVM 엑스포트 정책 생성
- SVM 엑스포트 정책 삭제
- SVM 엑스포트 정책 규칙 생성
- vserver export-policy rule show를 참조하십시오
- vserver export-policy show를 참조하십시오
- SVM iSCSI
- SVM iSCSI 연결이 표시됩니다
- vserver show 를 참조하십시오
- 네트워크 인터페이스
- 네트워크 인터페이스가 표시됩니다
- SVM
- MetroCluster 쇼

SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템을 SQL Server용 플러그인으로 준비합니다

ONTAP 플러그인을 SnapCenter SnapMirror 기술과 함께 사용하여 다른 볼륨에 백업 세트의 미러링 복사본을 만들고 ONTAP SnapVault 기술을 사용하여 표준 준수 및 기타 거버넌스 관련 용도로 D2D 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 타겟 볼륨 간의 데이터 보호 관계를 구성하고 관계를 초기화해야 합니다.

SnapCenter는 스냅샷 복사본 작업이 완료된 후 SnapMirror 및 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행되고, 별도의 ONTAP 일정을 만들지 않습니다.

NetApp SnapManager 제품에서 SnapCenter으로 오고 있으며 구성한 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 운영 스토리지(소스 볼륨)의 데이터를 보조 스토리지(타겟 볼륨)에 복제합니다. 관계를 초기화할 때 ONTAP은 소스 볼륨에서 참조된 데이터 블록을 대상 볼륨으로 전송합니다.

SnapCenter는 SnapMirror와 SnapVault 볼륨(* Primary * > * Mirror * > * Vault *) 간의 계단식 관계를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter는 버전에 상관없이 유연한 SnapMirror 관계의 관리를 지원합니다. 버전에 상관없이 유연한 SnapMirror 관계와 설정 방법에 대한 자세한 내용은 를 참조하십시오 "ONTAP 설명서".

SnapCenter는 * SYNC_MIRROR * 복제를 지원하지 않습니다.

SQL Server 리소스에 대한 백업 전략

SQL Server 리소스에 대한 백업 전략을 정의합니다

백업 작업을 생성하기 전에 백업 전략을 정의하면 데이터베이스를 성공적으로 복원하거나 복제하는 데 필요한 백업이 있는지 확인할 수 있습니다. SLA(서비스 수준 계약), RTO(복구 시간 목표) 및 RPO(복구 시점 목표)에 따라 백업 전략이 크게 결정됩니다.

SLA는 예상되는 서비스 수준을 정의하고 가용성 및 서비스 성능을 비롯한 다양한 서비스 관련 문제를 해결합니다. RTO는 서비스 중단 후 비즈니스 프로세스를 복원해야 하는 시간입니다. RPO는 장애 후 정상적인 작업을 재개하기 위해 백업 스토리지에서 복구해야 하는 파일의 사용 기간에 대한 전략을 정의합니다. SLA, RTO 및 RPO는 백업 전략에 기여합니다.

지원되는 백업 유형입니다

SnapCenter를 사용하여 SQL Server 시스템 및 사용자 데이터베이스를 백업하려면 데이터베이스, SQL Server 인스턴스 및 AG(가용성 그룹)와 같은 리소스 유형을 선택해야 합니다. 스냅샷 복사본 기술은 리소스가 상주하는 볼륨의 온라인 읽기 전용 복사본을 생성하는 데 사용됩니다.

복사 전용 옵션을 선택하여 SQL Server가 트랜잭션 로그를 자르지 않도록 지정할 수 있습니다. 다른 백업 응용 프로그램과 함께 SQL Server를 관리하는 경우에도 이 옵션을 사용해야 합니다. 트랜잭션 로그를 그대로 유지하면 모든 백업 애플리케이션이 시스템 데이터베이스를 복구할 수 있습니다. 복사 전용 백업은 예약된 백업의 시퀀스와 독립적이며

데이터베이스의 백업 및 복원 절차에 영향을 주지 않습니다.

백업 유형	설명	백업 유형이 포함된 복사 전용 옵션입니다
전체 백업 및 로그 백업	시스템 데이터베이스를 백업하고 트랜잭션 로그를 잘라냅니다. SQL Server는 데이터베이스에 이미 커밋된 항목을 제거하여 트랜잭션 로그를 잘라냅니다. 전체 백업이 완료되면 이 옵션은 트랜잭션 정보를 캡처하는 트랜잭션 로그를 생성합니다. 일반적으로 이 옵션을 선택해야 합니다. 그러나 백업 시간이 짧은 경우에는 전체 백업을 사용하여 트랜잭션 로그 백업을 실행하지 않도록 선택할 수 있습니다. 마스터 및 msdb 시스템 데이터베이스에 대한 로그 백업을 만들 수 없습니다. 그러나 모델 시스템 데이터베이스에 대한 로그 백업을 생성할 수 있습니다.	로그를 자르지 않고 시스템 데이터베이스 파일 및 트랜잭션 로그를 백업합니다. 복제 전용 백업은 차등 기본 또는 차등 백업 역할을 할 수 없으며 차등 베이스에 영향을 주지 않습니다. 복사 전용 전체 백업을 복원하는 것은 다른 전체 백업을 복원하는 것과 동일합니다.
전체 데이터베이스 백업	시스템 데이터베이스 파일을 백업합니다. 마스터, 모델 및 msdb 시스템 데이터베이스에 대한 전체 데이터베이스 백업을 만들 수 있습니다.	시스템 데이터베이스 파일을 백업합니다.
트랜잭션 로그 백업	가장 최근의 트랜잭션 로그가 백업된 이후에 커밋된 트랜잭션만 복사하여 잘린 트랜잭션 로그를 백업합니다. 전체 데이터베이스 백업과 함께 트랜잭션 로그 백업을 자주 예약하는 경우 세분화된 복구 지점을 선택할 수 있습니다.	트랜잭션 로그를 잘라내지 않고 백업합니다. 이 백업 유형은 일반 로그 백업의 시퀀싱에 영향을 주지 않습니다. 복사 전용 로그 백업은 온라인 복원 작업을 수행하는 데 유용합니다.

SQL Server용 플러그인 백업 스케줄입니다

백업 빈도(스케줄 유형)는 정책에 지정되며 백업 스케줄은 리소스 그룹 구성에 지정됩니다. 백업 빈도 또는 스케줄을 결정하는 가장 중요한 요소는 리소스의 변경 속도 및 데이터의 중요도입니다. 자주 사용하는 리소스를 매일 한 번씩 백업할 수도 있고, 자주 사용하지 않는 리소스를 하루에 한 번 백업할 수도 있습니다. 기타 요인으로는 조직에 대한 리소스의 중요성, SLA(서비스 수준 계약) 및 RPO(복구 시점 목표)가 있습니다.

SLA는 예상되는 서비스 수준을 정의하고 가용성 및 서비스 성능을 비롯한 다양한 서비스 관련 문제를 해결합니다. RPO는 장애 후 정상적인 작업을 재개하기 위해 백업 스토리지에서 복구해야 하는 파일의 사용 기간에 대한 전략을 정의합니다. SLA 및 RPO는 데이터 보호 전략에 기여합니다.

사용량이 많은 리소스의 경우에도 하루에 한 번 또는 두 번 이상 전체 백업을 실행할 필요가 없습니다. 예를 들어 정기적인 트랜잭션 로그 백업만으로도 필요한 백업이 있는지 확인할 수 있습니다. 데이터베이스를 더 자주 백업할수록 SnapCenter는 복원 시 사용해야 하는 트랜잭션 로그를 더 적게 사용하여 복원 작업을 더 빠르게 수행할 수 있습니다.

백업 스케줄은 다음과 같이 두 부분으로 구성됩니다.

- 백업 빈도

  일부 플러그인에 대해 _schedule type_이라는 백업 빈도(백업 수행 빈도)는 정책 구성의 일부입니다. 정책의 백업 빈도로 시간별, 일별, 주별 또는 월별 을 선택할 수 있습니다. 이러한 빈도 중 하나를 선택하지 않으면 생성된 정책이 온디맨드 전용 정책입니다. 설정 * > * 정책 * 을 클릭하여 정책에 액세스할 수 있습니다.

- 백업 스케줄

  백업 스케줄(백업을 수행할 정확한 시점)은 리소스 그룹 구성의 일부입니다. 예를 들어 주별 백업에 대한 정책이 구성된 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 스케줄을 구성할 수 있습니다. 리소스 그룹 * > * 리소스 그룹 * 을 클릭하여 리소스 그룹 일정에 액세스할 수 있습니다.

데이터베이스에 필요한 백업 작업 수입니다

필요한 백업 작업 수를 결정하는 요인에는 데이터베이스 크기, 사용된 볼륨 수, 데이터베이스 변경 속도 및 SLA(서비스 수준 계약)가 포함됩니다.

데이터베이스 백업의 경우 일반적으로 선택한 백업 작업 수는 데이터베이스를 배치한 볼륨의 수에 따라 달라집니다. 예를 들어, 한 볼륨에 작은 데이터베이스 그룹을 배치하고 다른 볼륨에 큰 데이터베이스를 배치한 경우 작은 데이터베이스에 대해 하나의 백업 작업을 생성하고 큰 데이터베이스에 대해 하나의 백업 작업을 만들 수 있습니다.

SQL Server용 플러그인의 백업 명명 규칙

기본 스냅샷 복사본 명명 규칙을 사용하거나 사용자 지정된 명명 규칙을 사용할 수 있습니다. 기본 백업 명명 규칙은 스냅샷 복사본 이름에 타임 스탬프를 추가하여 복사본이 생성된 시간을 식별하도록 도와줍니다.

스냅샷 복사본은 다음과 같은 기본 명명 규칙을 사용합니다.

```
resourcegroupname_hostname_timestamp
```

다음 예제와 같이 백업 리소스 그룹의 이름을 논리적으로 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예제에서 구문 요소는 다음과 같은 의미를 가집니다.

- _dts1_은(는) 리소스 그룹 이름입니다.
- _mach1x88_은 호스트 이름입니다.

- _03-12-2015_23.17.26_은 날짜 및 타임스탬프입니다.

또는 * Use custom name format for Snapshot copy * 를 선택하여 리소스 또는 리소스 그룹을 보호하면서 스냅샷 복사본 이름 형식을 지정할 수 있습니다. 예를 들어 customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname을 입력합니다. 기본적으로 타임스탬프 접미사가 스냅샷 복사본 이름에 추가됩니다.

SQL Server용 플러그인의 백업 보존 옵션

백업 복사본을 보존할 일 수를 선택하거나 유지할 백업 복사본 수를 최대 255개 사본의 ONTAP로 지정할 수 있습니다. 예를 들어, 조직에서 10일간 백업 복사본 또는 130개의 백업 복사본을 보존해야 할 수도 있습니다.

정책을 생성하는 동안 백업 유형 및 스케줄 유형에 대한 보존 옵션을 지정할 수 있습니다.

SnapMirror 복제를 설정하면 보존 정책이 대상 볼륨에 미러링됩니다.

SnapCenter는 스케줄 유형과 일치하는 보존 레이블이 있는 보존된 백업을 삭제합니다. 리소스 또는 리소스 그룹에 대한 스케줄 유형이 변경된 경우 이전 스케줄 유형 레이블이 있는 백업이 시스템에 남아 있을 수 있습니다.

백업 복사본을 장기간 보존하려면 SnapVault 백업을 사용해야 합니다.

소스 스토리지 시스템에서 트랜잭션 로그 백업을 유지하는 데 걸리는 시간

Microsoft SQL Server용 SnapCenter 플러그인에는 최신 복원 작업을 수행하기 위한 트랜잭션 로그 백업이 필요합니다. 이 작업은 데이터베이스를 두 개의 전체 백업 사이의 시간으로 복원합니다.

예를 들어 SQL Server용 플러그인이 오전 8시에 전체 백업을 수행하는 경우 또한 오후 5시에 최신 트랜잭션 로그 백업을 사용하여 오전 8시 사이에 언제든지 데이터베이스를 복원할 수 있습니다 오후 5시까지 운영됩니다 트랜잭션 로그를 사용할 수 없는 경우 SQL Server용 플러그인은 시점 복원 작업만 수행할 수 있습니다. 그러면 SQL Server용 플러그인이 전체 백업을 완료한 시점으로 데이터베이스를 복원합니다.

일반적으로 하루 또는 이틀 동안만 최신 복원 작업이 필요합니다. 기본적으로 SnapCenter는 최소 2일을 유지합니다.

동일한 볼륨에 여러 개의 데이터베이스가 있습니다

백업 정책에 백업당 최대 데이터베이스(기본값: 100)를 설정하는 옵션이 있으므로 모든 데이터베이스를 동일한 볼륨에 배치할 수 있습니다.

예를 들어, 같은 볼륨에 200개의 데이터베이스가 있는 경우 두 스냅샷 복사본 각각에 100개의 데이터베이스가 있는 2개의 스냅샷 복사본이 생성됩니다.

SQL Server용 플러그인용 기본 또는 보조 스토리지 볼륨을 사용하여 백업 복사본 검증

운영 스토리지 볼륨 또는 SnapMirror 또는 SnapVault 보조 스토리지 볼륨에서 백업 복사본을 확인할 수 있습니다. 보조 스토리지 볼륨을 사용하여 검증하면 운영 스토리지 볼륨의 로드가 감소합니다.

운영 또는 2차 스토리지 볼륨에 있는 백업을 확인하면 모든 운영 및 2차 스냅샷 복사본이 확인됨 으로 표시됩니다.

SnapMirror 및 SnapVault 2차 스토리지 볼륨의 백업 복사본을 확인하려면 SnapRestore 라이센스가 필요합니다.

검증 작업을 예약하는 시기

SnapCenter는 백업을 생성한 후 즉시 백업을 확인할 수 있지만 그렇게 하면 백업 작업을 완료하는 데 필요한 시간이 크게 늘어나고 리소스가 많이 소모됩니다. 따라서 거의 항상 별도의 작업에서 나중에 검증을 예약하는 것이 가장 좋습니다. 예를 들어 오후 5시에 데이터베이스를 백업할 수 있습니다 매일 오후 6시에 1시간 후에 확인을 수행하도록 예약할 수 있습니다

이와 같은 이유로 백업을 수행할 때마다 백업 검증을 실행할 필요는 없습니다. 일반적으로 정기적인 확인 작업을 수행하지만 간격이 짧아 백업의 무결성을 보장할 수 있습니다. 단일 검증 작업으로 여러 백업을 동시에 확인할 수 있습니다.

SQL Server의 복원 전략

SQL Server에 대한 복원 전략을 정의합니다

SQL Server에 대한 복원 전략을 정의하면 데이터베이스를 성공적으로 복원할 수 있습니다.

복구 작업의 소스 및 대상

운영 또는 보조 스토리지의 백업 복사본에서 SQL Server 데이터베이스를 복원할 수 있습니다. 또한 데이터베이스를 원래 위치 외에 다른 대상에 복원할 수 있으므로 요구 사항을 지원하는 대상을 선택할 수 있습니다.

복구 작업의 소스

운영 스토리지 또는 보조 스토리지에서 데이터베이스를 복원할 수 있습니다.

복원 작업의 대상

데이터베이스를 다양한 대상으로 복원할 수 있습니다.

목적지	설명
원래 위치	기본적으로 SnapCenter는 동일한 SQL Server 인스턴스의 동일한 위치에 데이터베이스를 복원합니다.
다른 위치	데이터베이스를 동일한 호스트 내의 모든 SQL Server 인스턴스에서 다른 위치로 복구할 수 있습니다.
다른 데이터베이스 이름을 사용하는 원래 위치 또는 다른 위치	백업이 생성된 동일한 호스트의 SQL Server 인스턴스에 다른 이름으로 데이터베이스를 복구할 수 있습니다.

VMDK(NFS 및 VMFS 데이터 저장소)의 SQL 데이터베이스에 대해 ESX Server 간에 대체 호스트로 복구할 수 없습니다.

SnapCenter에서 지원하는 **SQL Server** 복구 모델

특정 복구 모델은 기본적으로 각 데이터베이스 유형에 할당됩니다. SQL Server 데이터베이스 관리자는 각 데이터베이스를 다른 복구 모델에 다시 할당할 수 있습니다.

SnapCenter는 다음과 같은 세 가지 유형의 SQL Server 복구 모델을 지원합니다.

- 단순한 복구 모델

  단순 복구 모델을 사용하는 경우 트랜잭션 로그를 백업할 수 없습니다.

- 전체 복구 모델

  전체 복구 모델을 사용하는 경우 장애 지점에서 데이터베이스를 이전 상태로 복원할 수 있습니다.

- 대량 로그 복구 모델

  대량 로그 복구 모델을 사용할 경우 대량 로그 작업을 수동으로 다시 실행해야 합니다. 복구 전에 작업의 커밋 레코드가 포함된 트랜잭션 로그가 백업되지 않은 경우 대량 로그 작업을 수행해야 합니다. 대량 로그 작업이 데이터베이스에 1000만 개의 행을 삽입하고 트랜잭션 로그가 백업되기 전에 데이터베이스에 오류가 발생하면 복원된 데이터베이스에 대량 로그 작업에 의해 삽입된 행이 포함되지 않습니다.

복원 작업의 유형입니다

SnapCenter를 사용하여 SQL Server 리소스에 대해 다양한 유형의 복원 작업을 수행할 수 있습니다.

- 최신 상태로 복원합니다
- 이전 시점으로 복원합니다

다음과 같은 경우 최대 1분을 복원하거나 이전 시점으로 복원할 수 있습니다.

- SnapMirror 또는 SnapVault 2차 스토리지에서 복원합니다
- 대체 경로(위치)로 복원

SnapCenter는 볼륨 기반 SnapRestore를 지원하지 않습니다.

최대 **1**분 내에 복원합니다

최신 복원 작업(기본적으로 선택됨)에서는 데이터베이스가 장애 지점까지 복구됩니다. SnapCenter는 다음 시퀀스를 실행하여 이를 수행합니다.

1. 데이터베이스를 복구하기 전에 마지막 활성 트랜잭션 로그를 백업합니다.
2. 선택한 전체 데이터베이스 백업에서 데이터베이스를 복원합니다.
3. 데이터베이스에 커밋되지 않은 모든 트랜잭션 로그를 적용합니다(백업이 생성된 시간부터 최신 시간까지 백업의 트랜잭션 로그 포함).

   트랜잭션 로그가 앞으로 이동되어 선택한 데이터베이스에 적용됩니다.

최신 복원 작업을 수행하려면 일련의 트랜잭션 로그가 필요합니다.

SnapCenter는 로그 전달 백업 파일에서 SQL Server 데이터베이스 트랜잭션 로그를 복원할 수 없으므로(로그 전달을 사용하면 운영 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. 따라서 SnapCenter를 사용하여 SQL Server 데이터베이스 트랜잭션 로그 파일을 백업해야 합니다.

모든 백업에 대해 최신 복원 기능을 유지할 필요가 없는 경우 백업 정책을 통해 시스템의 트랜잭션 로그 백업 보존을 구성할 수 있습니다.

최신 복원 작업의 예

매일 정오와 수요일 오후 4시에 SQL Server 백업을 실행한다고 가정합니다 백업에서 복원해야 합니다. 어떤 이유로 수요일 정오의 백업이 검증에 실패하여 화요일 정오 백업으로부터 복원하기로 결정했습니다. 그런 다음 백업이 복원되면 모든 트랜잭션 로그가 앞으로 이동되어 복구된 데이터베이스에 적용됩니다. 화요일 백업을 생성할 때 커밋되지 않은 로그부터 시작하여 수요일 오후 4시에 작성된 최신 트랜잭션 로그를 계속 진행합니다 (트랜잭션 로그가 백업된 경우)

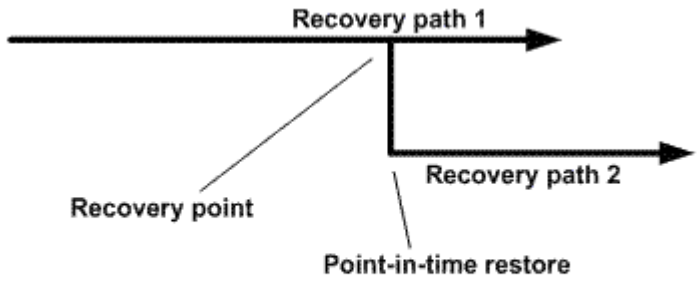
이전 시점으로 복원합니다

시점 복원 작업에서는 데이터베이스가 과거의 특정 시간으로만 복원됩니다. 시점 복원 작업은 다음과 같은 복원 상황에서 수행됩니다.

- 데이터베이스는 백업된 트랜잭션 로그에서 지정된 시간으로 복원됩니다.
- 데이터베이스가 복원되고 백업된 트랜잭션 로그의 하위 집합만 데이터베이스에 적용됩니다.

데이터베이스를 특정 시점으로 복원하면 새 복구 경로가 생성됩니다.

다음 이미지는 시점 복원 작업을 수행할 때의 문제를 보여 줍니다.



이미지에서 복구 경로 1은 전체 백업과 여러 트랜잭션 로그 백업으로 구성됩니다. 데이터베이스를 특정 시점으로 복원합니다. 새 트랜잭션 로그 백업은 시점 복원 작업 후에 생성되며, 이로 인해 복구 경로 2가 생성됩니다. 새 트랜잭션 로그 백업은 새 전체 백업을 생성하지 않고 생성됩니다. 데이터 손상 또는 기타 문제로 인해 새 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 응용 프로그램을 중지할 특정 날짜 및 시간을 지정할 수도 있습니다. 이렇게 하려면 사용 가능한 범위 내에서 날짜 및 시간을 지정하면 SnapCenter에서 해당 시점 이전에 커밋되지 않은 모든 트랜잭션을 제거합니다. 이 방법을 사용하여 손상이 발생하기 전의 시점으로 데이터베이스를 복원하거나 실수로 데이터베이스를 삭제하거나 테이블을 삭제한 경우 복구할 수 있습니다.

자정에 전체 데이터베이스 백업을 한 번, 매시간마다 트랜잭션 로그 백업을 한 번 수행한다고 가정해 보겠습니다. 오전 9시 45분에 데이터베이스가 크래시되지만 오류가 발생한 데이터베이스의 트랜잭션 로그는 여전히 백업되어 있습니다. 다음 시점 복원 시나리오 중 하나를 선택할 수 있습니다.

- 자정에 만든 전체 데이터베이스 백업을 복원하고 이후에 변경된 데이터베이스 내용을 잃게 됩니다. (옵션: 없음)
- 전체 데이터베이스 백업을 복원하고 오전 9시 45분까지 모든 트랜잭션 로그 백업을 적용합니다 (옵션: 로그 종료)
- 전체 데이터베이스 백업을 복원하고 트랜잭션 로그 백업을 적용하여 트랜잭션을 마지막 트랜잭션 로그 백업 세트에서 복원할 시간을 지정합니다. (옵션: 특정 시간별)

이 경우 특정 오류가 보고된 날짜와 시간을 계산합니다. 지정된 날짜 및 시간 이전에 커밋되지 않은 모든 트랜잭션이 제거됩니다.

SQL Server에 대한 클론 생성 전략을 정의합니다

클론 복제 전략을 정의하면 데이터베이스를 성공적으로 복제할 수 있습니다.

1. 클론 작업과 관련된 제한 사항을 검토합니다.
2. 필요한 클론 유형을 결정합니다.

클론 작업의 제한 사항

데이터베이스를 클론 복제하기 전에 클론 작업의 제한 사항을 숙지해야 합니다.

- 11.2.0.4 ~ 12.1.0.1의 Oracle 버전을 사용하는 경우 복제 작업은 에서 수행됩니다 *renamedg* 명령을 실행할 때 중단된 상태입니다. Oracle 패치 19544733을 적용할 수 있습니다 이 문제를 해결하려면 다음을 수행합니다.
- 를 사용하여 호스트에 직접 연결된 LUN에서 데이터베이스 클론 생성 VMDK 또는 동일한 RDM LUN에 대한 Windows 호스트의 Microsoft iSCSI Initiator입니다 Windows 호스트 또는 다른 Windows 호스트는 지원되지 않습니다.
- 볼륨 마운트 지점의 루트 디렉토리는 공유 디렉토리일 수 없습니다.
- 클론이 포함된 LUN을 새 볼륨으로 이동하면 클론을 삭제할 수 없습니다.

클론 작업의 유형입니다

SnapCenter를 사용하여 SQL Server 데이터베이스 백업 또는 운영 데이터베이스를 복제할 수 있습니다.

- 데이터베이스 백업에서 복제합니다

  복제된 데이터베이스는 새 응용 프로그램을 개발하고 격리하는 데 있어 기준 역할을 할 수 있습니다 운영 환경에서 발생하는 애플리케이션 오류입니다. 복제된 데이터베이스도 일 수 있습니다 소프트 데이터베이스 오류로부터 복구하는 데 사용됩니다.

- 클론 라이프사이클

  SnapCenter를 사용하여 운영 시 발생할 반복 클론 작업을 예약할 수 있습니다 데이터베이스가 사용 중이 아닙니다.

Microsoft SQL Server용 SnapCenter 플러그인 설치를 빠르게 시작합니다

SnapCenter 서버 및 플러그인 설치 준비

SnapCenter 서버 및 Microsoft SQL Server용 SnapCenter 플러그인 설치를 위한 준비 지침의 요약 세트를 제공합니다.

도메인 및 작업 그룹 요구 사항

SnapCenter 서버는 도메인 또는 작업 그룹에 있는 시스템에 설치할 수 있습니다.

Active Directory 도메인을 사용하는 경우 로컬 관리자 권한이 있는 도메인 사용자를 사용해야 합니다. 도메인 사용자는 Windows 호스트에 있는 로컬 관리자 그룹의 구성원이어야 합니다.

작업 그룹을 사용하는 경우 로컬 관리자 권한이 있는 로컬 계정을 사용해야 합니다.

라이센스 요구 사항

설치하는 라이센스 유형은 환경에 따라 다릅니다.

라이센스	필요한 경우
SnapCenter 표준 컨트롤러 기반	FAS 또는 AFF 스토리지 컨트롤러에 필요합니다 SnapCenter 표준 라이센스는 컨트롤러 기반 라이센스이며 프리미엄 번들의 일부로 포함됩니다. SnapManager 제품군 라이센스가 있는 경우 SnapCenter 표준 라이센스 사용 권한도 제공됩니다. FAS 또는 AFF 스토리지를 사용하여 평가판을 통해 SnapCenter를 설치하려면 세일즈 담당자에게 연락하여 프리미엄 번들 평가 라이센스를 받으십시오.
SnapCenter 표준 용량 기반	ONTAP Select 및 Cloud Volumes ONTAP에 필요합니다 Cloud Volumes ONTAP 또는 ONTAP Select 고객인 경우 SnapCenter에서 관리하는 데이터를 기준으로 TB당 용량 기반 라이센스를 구입해야 합니다. 기본적으로 SnapCenter는 90일 100TB SnapCenter 표준 용량 기반 평가판 라이센스를 기본 제공합니다. 자세한 내용은 세일즈 담당자에게 문의하십시오.
SnapMirror 또는 SnapVault	ONTAP SnapCenter에서 복제를 사용하는 경우 SnapMirror 또는 SnapVault 라이센스가 필요합니다.
추가 라이센스(선택 사항)	을 참조하십시오 "SnapCenter 라이센스".

라이센스	필요한 경우
SnapCenter 표준 라이센스(선택 사항)	보조 대상 SnapCenter 표준 라이센스를 보조 대상에 추가하는 것이 좋지만 필수는 아닙니다. 보조 대상에서 SnapCenter 표준 라이센스가 활성화되어 있지 않으면 페일오버 작업을 수행한 후 SnapCenter를 사용하여 보조 대상의 리소스를 백업할 수 없습니다. 그러나 복제 및 검증 작업을 수행하려면 보조 대상에 FlexClone 라이센스가 필요합니다.

호스트 및 포트 요구 사항

ONTAP 및 애플리케이션 플러그인 최소 요구 사항은 을 참조하십시오 "상호 운용성 매트릭스 툴".

호스트	최소 요구 사항
운영 체제(64비트)	을 참조하십시오 "상호 운용성 매트릭스 툴"
CPU	• 서버 호스트: 4코어 • 플러그인 호스트: 1 코어
RAM	• 서버 호스트: 8GB • 플러그인 호스트: 1GB
하드 드라이브 공간	서버 호스트: • SnapCenter 서버 소프트웨어 및 로그용 4GB • SnapCenter 리포지토리의 경우 6GB • 각 플러그인 호스트: 플러그인 설치 및 로그의 경우 2GB, 전용 호스트에 플러그인이 설치된 경우에만 필요합니다.
타사 라이브러리	SnapCenter 서버 호스트 및 플러그인 호스트에 필요: • Microsoft .NET Framework 4.7.2 이상 • WMF(Windows Management Framework) 4.0 이상 • PowerShell 4.0 이상
브라우저	Chrome, Internet Explorer 및 Microsoft Edge

포트 유형입니다	기본 포트입니다
SnapCenter 포트	8146(HTTPS), 양방향, 사용자 지정 가능(URL_\https://server:8146_)

포트 유형입니다	기본 포트입니다
SnapCenter SMCore 통신 포트입니다	8145(HTTPS), 양방향, 사용자 지정 가능
리포지토리 데이터베이스	3306(HTTPS), 양방향
Windows 플러그인 호스트	135, 445(TCP) 135번 및 445번 포트 외에도 Microsoft에서 지정한 동적 포트 범위도 열려 있어야 합니다. 원격 설치 작업은 이 포트 범위를 동적으로 검색하는 WMI(Windows Management Instrumentation) 서비스를 사용합니다. 지원되는 동적 포트 범위에 대한 자세한 내용은 을 참조하십시오 "Windows에 대한 서비스 개요 및 네트워크 포트 요구 사항".
Windows용 SnapCenter 플러그인	8145(HTTPS), 양방향, 사용자 지정 가능
ONTAP 클러스터 또는 SVM 통신 포트	443(HTTPS), 양방향, 80(HTTP), 양방향 이 포트는 SnapCenter 서버 호스트, 플러그인 호스트, SVM 또는 ONTAP 클러스터 간의 통신에 사용됩니다.

Microsoft SQL Server용 **SnapCenter** 플러그인 요구 사항

원격 호스트에 대한 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 사용자가 있어야 합니다. 클러스터 노드를 관리하는 경우 클러스터의 모든 노드에 대한 관리 권한이 있는 사용자가 필요합니다.

SQL Server에 대한 sysadmin 권한이 있는 사용자가 있어야 합니다. 플러그인은 Microsoft VDI 프레임워크를 사용하므로 sysadmin 액세스가 필요합니다.

Microsoft SQL Server용 SnapManager를 사용하고 있고 SnapManager for Microsoft SQL Server에서 SnapCenter로 데이터를 가져오려면 를 참조하십시오 "보관된 백업을 가져옵니다"

Microsoft SQL Server용 SnapCenter 서버를 설치합니다

Microsoft SQL Server용 SnapCenter Server를 설치하기 위한 일련의 설치 지침을 제공합니다.

1단계**: SnapCenter** 서버 다운로드 및 설치

1. 에서 SnapCenter 서버 설치 패키지를 다운로드합니다 "NetApp Support 사이트" 그런 다음 exe를 두 번 클릭합니다.

   설치를 시작한 후 모든 사전 점검을 수행하고 최소 요구사항을 충족하지 못할 경우 적절한 오류 또는 경고 메시지가 표시됩니다. 경고 메시지를 무시하고 설치를 진행할 수 있지만 오류를 수정해야 합니다.

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

MySQL Server 리포지토리 데이터베이스의 암호를 지정할 필요가 없습니다. SnapCenter 서버 설치 중에 암호는 자동으로 생성됩니다.

> 특수 문자 "%"는 설치를 위한 사용자 지정 경로에서 지원되지 않습니다. 경로에 "%"를 포함하면 설치가 실패합니다.

3. 지금 설치 * 를 클릭합니다.

2단계**: SnapCenter**에 로그인합니다

1. 호스트 데스크톱의 바로 가기나 설치 시 제공된 URL에서 SnapCenter를 실행합니다(*https://server:8146* SnapCenter 서버가 설치된 기본 포트 8146의 경우 _).
2. 자격 증명을 입력합니다.

   기본 제공 도메인 관리자 사용자 이름 형식의 경우, *NetBIOS*\<사용자 이름> 또는 <사용자 이름>@<도메인> 또는 _<도메인 FQDN>\<사용자 이름>_을 사용합니다.

   기본 제공 로컬 관리자 사용자 이름 형식의 경우 _<사용자 이름>_을(를) 사용합니다.

3. 로그인 * 을 클릭합니다.

3단계**: SnapCenter** 표준 컨트롤러 기반 라이센스 추가

1. ONTAP 명령줄을 사용하여 컨트롤러에 로그인하고 다음을 입력합니다.

   ```
   system license add -license-code <license_key>
   ```

2. 라이센스를 확인합니다.

   ```
   license show
   ```

4단계**: SnapCenter** 용량 기반 라이센스 추가

1. SnapCenter GUI 왼쪽 창에서 * 설정 > 소프트웨어 * 를 클릭한 다음 라이센스 섹션에서 * + * 를 클릭합니다.
2. 라이선스를 얻는 두 가지 방법 중 하나를 선택합니다.
   - 라이센스를 가져오려면 NetApp Support 사이트 로그인 자격 증명을 입력하십시오.
   - NetApp 라이센스 파일의 위치로 이동하여 * Open * 을 클릭합니다.
3. 마법사의 알림 페이지에서 기본 용량 임계값인 90%를 사용합니다.
4. 마침 * 을 클릭합니다.

5단계**:** 스토리지 시스템 접속 설정

1. 왼쪽 창에서 * 스토리지 시스템 > 새로 만들기 * 를 클릭합니다.
2. 스토리지 시스템 추가 페이지에서 다음을 수행합니다.
   a. 스토리지 시스템의 이름 또는 IP 주소를 입력합니다.
   b. 스토리지 시스템을 액세스하는 데 사용되는 자격 증명을 입력합니다.

c. 확인란을 선택하여 EMS(이벤트 관리 시스템) 및 AutoSupport를 활성화합니다.

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

Microsoft SQL Server용 SnapCenter 플러그인을 설치합니다

Microsoft SQL Server용 SnapCenter 플러그인에 대한 일련의 설치 지침을 제공합니다.

1단계**: Run as Credentials**를 설치하여 **Microsoft SQL Server**용 플러그인을 설치합니다

1. 왼쪽 창에서 * 설정 > 자격 증명 > 새로 만들기 * 를 클릭합니다.
2. 자격 증명을 입력합니다.

   기본 제공 도메인 관리자 사용자 이름 형식의 경우, *NetBIOS*\<사용자 이름> 또는 <사용자 이름>@<도메인> 또는 _<도메인 FQDN>\<사용자 이름>_을 사용합니다.

   기본 제공 로컬 관리자 사용자 이름 형식의 경우 _<사용자 이름>_을(를) 사용합니다.

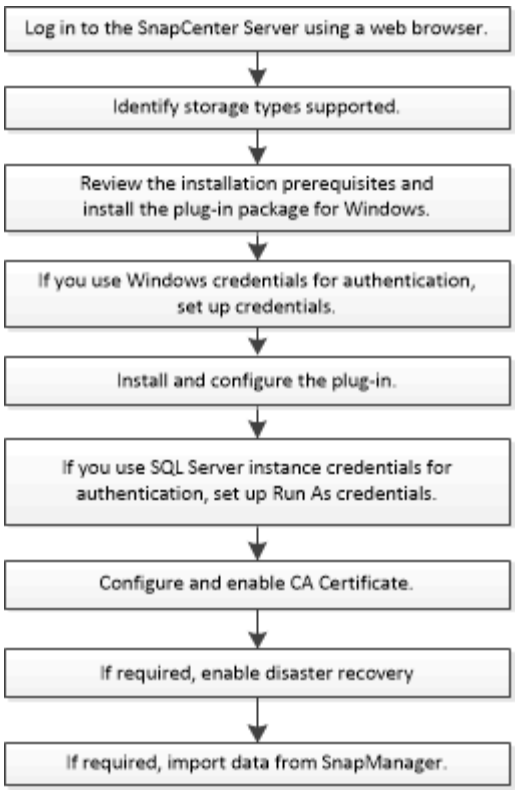
2단계**:** 호스트를 추가하고 **Microsoft SQL Server**용 플러그인을 설치합니다

1. SnapCenter GUI 왼쪽 창에서 * 호스트 > 관리 호스트 > 추가 * 를 클릭합니다.
2. 마법사의 호스트 페이지에서 다음을 수행합니다.
   a. 호스트 유형: Windows 호스트 유형을 선택합니다.
   b. 호스트 이름: SQL 호스트를 사용하거나 전용 Windows 호스트의 FQDN을 지정합니다.
   c. 자격 증명: 생성한 호스트의 유효한 자격 증명 이름을 선택하거나 새 자격 증명을 생성합니다.
3. 설치할 플러그인 선택 섹션에서 * Microsoft SQL Server * 를 선택합니다.
4. 다음 세부 정보를 지정하려면 * 추가 옵션 * 을 클릭합니다.
   a. 포트: 기본 포트 번호를 유지하거나 포트 번호를 지정합니다.
   b. 설치 경로: 기본 경로는 _C:\Program Files\NetApp\SnapCenter_입니다.
   선택적으로 경로를 사용자 지정할 수 있습니다.
   c. 클러스터에 모든 호스트 추가: WSFC에서 SQL을 사용하는 경우 이 확인란을 선택합니다.
   d. 사전 설치 검사 건너뛰기: 플러그인을 수동으로 이미 설치했거나 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.
5. 제출 * 을 클릭합니다.

Microsoft SQL Server용 SnapCenter 플러그인 설치를 준비합니다

Microsoft SQL Server용 SnapCenter 플러그인 설치 워크플로

SQL Server 데이터베이스를 보호하려면 Microsoft SQL Server용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



사전 요구 사항 - 호스트를 추가하고 **Microsoft SQL Server**용 **SnapCenter** 플러그인을 설치합니다

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 완료해야 합니다.

- iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.
- 원격 호스트에 대한 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 사용자가 있어야 합니다.
- SnapCenter에서 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 사용하므로 sysadmin 액세스가 필요합니다.

  "Microsoft 지원 문서 2926557: SQL Server VDI 백업 및 복원 작업에는 sysadmin 권한이 필요합니다"

- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자의 경우 호스트에서 UAC를 비활성화해야 합니다.
- SnapManager for Microsoft SQL Server가 설치된 경우 서비스 및 일정을 중지하거나 사용하지 않아야 합니다.

  백업 또는 클론 작업을 SnapCenter로 가져오려는 경우 SnapManager for Microsoft SQL Server를 제거하지 마십시오.

- 호스트는 서버에서 FQDN(정규화된 도메인 이름)으로 확인할 수 있어야 합니다.

  호스트 파일을 확인할 수 있도록 수정하고 호스트 파일에 짧은 이름과 FQDN이 모두 지정된 경우 SnapCenter hosts 파일에 <IP_address><host_FQDN><host_name> 형식으로 항목을 생성합니다

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항 및 사이징 요구 사항을 숙지해야 합니다.

항목	요구 사항
운영 체제	Microsoft Windows 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	• Microsoft .NET Framework 4.7.2 이상 • WMF(Windows Management Framework) 4.0 이상 • PowerShell 4.0 이상 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴". NET 관련 문제 해결에 대한 자세한 내용은 을 참조하십시오 "인터넷에 연결되지 않은 기존 시스템의 경우 SnapCenter 업그레이드 또는 설치가 실패합니다."

Windows용 SnapCenter 플러그인 패키지에 대한 자격 증명을 설정합니다

SnapCenter는 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다. 데이터베이스 또는 Windows 파일 시스템에서 데이터 보호 작업을 수행하려면 SnapCenter 플러그인 설치를 위한 자격 증명과 추가 자격 증명을 만들어야 합니다.

시작하기 전에

- 플러그인을 설치하기 전에 Windows 자격 증명을 설정해야 합니다.
- 원격 호스트에 대한 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정해야 합니다.
- Windows 호스트에서 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 사용자의 자격 증명을 설정합니다.

SQL 인증 메서드는 SQL Server 인스턴스에 대해 인증합니다. 즉, SnapCenter에서 SQL Server 인스턴스를 검색한 다음 따라서 SQL 자격 증명을 추가하기 전에 호스트를 추가하고 플러그인 패키지를 설치하고 리소스를 새로 고쳐야 합니다. 리소스 예약 또는 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 증명 구성에 필요한 정보를 지정합니다.

이 필드의 내용...	수행할 작업...
자격 증명 이름입니다	자격 증명의 이름을 입력합니다.
사용자 이름/암호	인증에 사용할 사용자 이름과 암호를 입력합니다. • 도메인 관리자 SnapCenter 플러그인을 설치할 시스템에 도메인 관리자를 지정합니다. 사용자 이름 필드에 유효한 형식은 다음과 같습니다. ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우 SnapCenter 플러그인을 설치할 시스템에 기본 제공 로컬 관리자를 지정합니다. 사용자 계정에 상승된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 올바른 형식은 다음과 같습니다. `UserName` 암호에 큰따옴표(") 또는 백틱(')을 사용하지 마십시오. 보다 작음(<) 및 느낌표(!)를 사용해서는 안 됩니다. 암호를 사용한 기호. 예를 들어 LessThan <!10, Lessthan10 <!, backtick'12.

이 필드의 내용...	수행할 작업...
인증 모드	사용할 인증 모드를 선택합니다. 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 페이지의 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

개별 SQL Server 리소스에 대한 자격 증명을 구성합니다

각 사용자에 대해 개별 SQL Server 리소스에 대해 데이터 보호 작업을 수행하도록 자격 증명을 구성할 수 있습니다. 자격 증명을 전역적으로 구성할 수 있지만 특정 리소스에 대해서만 구성할 수 있습니다.

이 작업에 대해

- 인증에 Windows 자격 증명을 사용하는 경우 플러그인을 설치하기 전에 자격 증명을 설정해야 합니다.

  그러나 인증에 SQL Server 인스턴스를 사용하는 경우에는 플러그인을 설치한 후 자격 증명을 추가해야 합니다.

- 자격 증명을 설정하는 동안 SQL 인증을 사용하도록 설정한 경우 검색된 인스턴스 또는 데이터베이스에 빨간색 자물쇠 아이콘이 표시됩니다.

  자물쇠 아이콘이 나타나면 인스턴스 또는 데이터베이스 자격 증명을 지정하여 인스턴스 또는 데이터베이스를 리소스 그룹에 성공적으로 추가해야 합니다.

- 다음 조건이 충족될 경우 sysadmin 액세스 없이 역할 기반 액세스 제어(RBAC) 사용자에게 자격 증명을 할당해야 합니다.
  - 자격 증명이 SQL 인스턴스에 할당됩니다.
  - SQL 인스턴스 또는 호스트는 RBAC 사용자에게 할당됩니다.

    사용자에게 리소스 그룹과 백업 권한이 모두 있어야 합니다.

1단계**:** 자격 증명을 추가 및 구성합니다

1. 왼쪽 탐색 창에서 * 설정 * 을 선택합니다.
2. 설정 페이지에서 * 자격 증명 * 을 선택합니다.
   a. 새 자격 증명을 추가하려면 * New * 를 선택합니다.
   b. 자격 증명 페이지에서 자격 증명을 구성합니다.

이 필드의 내용...	수행할 작업...
자격 증명 이름입니다	자격 증명의 이름을 입력합니다.

이 필드의 내용...	수행할 작업...
사용자 이름	SQL Server 인증에 사용되는 사용자 이름을 입력합니다. • 도메인 관리자 또는 관리자 그룹의 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹의 구성원을 지정합니다. 사용자 이름 * 필드의 올바른 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 제공 로컬 관리자를 지정합니다. 사용자 계정에 상승된 권한이 있거나 사용자가 있는 경우 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다 호스트 시스템에서 액세스 제어 기능이 비활성화되어 있습니다. 사용자 이름 * 필드의 올바른 형식은 _ 사용자 이름 _ 입니다
암호	인증에 사용되는 암호를 입력합니다.
인증 모드	SQL Server 인증 모드를 선택합니다. Windows 사용자에게 SQL Server에 대한 sysadmin 권한이 있는 경우 Windows 인증을 선택할 수도 있습니다.
호스트	호스트를 선택합니다.
SQL Server 인스턴스입니다	SQL Server 인스턴스를 선택합니다.

c. 자격 증명을 추가하려면 * OK * 를 선택합니다.

2단계**:** 인스턴스 구성

1. 왼쪽 탐색 창에서 * 리소스 * 를 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 인스턴스 * 를 선택합니다.
   a. 를 선택합니다 [필터 아이콘]를 클릭한 다음 호스트 이름을 선택하여 인스턴스를 필터링합니다.
   b. 를 선택합니다 [필터 아이콘] 를 눌러 필터 창을 닫습니다.
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 데이터베이스 및 가용성 그룹에는 적용되지 않습니다.

4. 리소스 새로 고침 * 을 선택합니다.

Windows Server 2012 이상에서 GMSA를 구성합니다

Windows Server 2012 이상을 사용하면 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 GMSA(Managed Service Account)를 만들 수 있습니다.

시작하기 전에

- Windows Server 2012 이상의 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2012 이상 호스트가 있어야 합니다.

단계

1. KDS 루트 키를 생성하여 GMSA의 각 개체에 대해 고유한 암호를 생성합니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 Add-KDSRootKey-EffectiveImmediately 명령을 실행합니다
3. GMSA 생성 및 구성:
   a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
 domainName\accountName$
.. 그룹에 컴퓨터 개체를 추가합니다.
.. 방금 생성한 사용자 그룹을 사용하여 GMSA를 생성합니다.
```

   예를 들면, 다음과 같습니다.

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. 실행 `Get-ADServiceAccount` 명령을 사용하여 서비스 계정을 확인합니다.
```

4. 호스트에서 GMSA를 구성합니다.
   a. GMSA 계정을 사용할 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.

      이렇게 하려면 PowerShell에서 다음 명령을 실행합니다.

```
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 확인합니다. `Test-AdServiceAccount <gMSA>`

5. 호스트에서 구성된 GMSA에 관리 권한을 할당합니다.
6. SnapCenter 서버에서 구성된 GMSA 계정을 지정하여 Windows 호스트를 추가합니다.

   SnapCenter 서버는 선택한 플러그인을 호스트에 설치하고 지정된 GMSA는 플러그인 설치 중에 서비스 로그온 계정으로 사용됩니다.

Microsoft SQL Server용 SnapCenter 플러그인을 설치합니다

호스트를 추가하고 Windows용 SnapCenter 플러그인 패키지를 설치합니다

호스트를 추가하고 플러그인 패키지를 설치하려면 SnapCenter * 호스트 추가 * 페이지를 사용해야 합니다. 플러그인은 원격 호스트에 자동으로 설치됩니다.

시작하기 전에

- 플러그인 설치 및 제거 권한이 있는 역할(예: SnapCenter 관리자 역할)에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하면 호스트에서 UAC를 비활성화해야 합니다.
- 메시지 큐 서비스가 실행 중인지 확인해야 합니다.
- 그룹 GMSA(Managed Service Account)를 사용하는 경우 관리자 권한으로 GMSA를 구성해야 합니다.

  "Windows Server 2012 이상에서 그룹 관리 서비스 계정을 SQL용으로 구성합니다"

이 작업에 대해

SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.

호스트를 추가하고 개별 호스트 또는 클러스터에 대한 플러그인 패키지를 설치할 수 있습니다. 클러스터 또는 WSFC(Windows Server Failover Clustering)에 플러그인을 설치하는 경우 클러스터의 모든 노드에 플러그인이 설치됩니다.

호스트 관리에 대한 자세한 내용은 을 참조하십시오 "호스트를 관리합니다".

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 선택합니다.
2. 맨 위에 * Managed Hosts * 탭이 선택되어 있는지 확인합니다.
3. 추가 * 를 선택합니다.
4. 호스트 페이지에서 다음을 수행합니다.

이 필드의 내용...	수행할 작업...
호스트 유형	호스트 유형으로 Windows를 선택합니다. 플러그인이 호스트에 아직 설치되지 않은 경우 SnapCenter 서버가 호스트를 추가한 다음 Windows용 플러그인을 설치합니다. 플러그인 페이지에서 Microsoft SQL Server 옵션을 선택하면 SnapCenter 서버가 SQL Server용 플러그인을 설치합니다.
호스트 이름입니다	FQDN(정규화된 도메인 이름) 또는 호스트의 IP 주소를 입력합니다. IP 주소는 FQDN으로 확인되는 경우에만 신뢰할 수 없는 도메인 호스트에 대해 지원됩니다. SnapCenter는 DNS의 올바른 구성에 따라 달라집니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다. 다음 중 하나의 IP 주소 또는 FQDN을 입력할 수 있습니다. • 독립 실행형 호스트 • WSFC SnapCenter를 사용하여 호스트를 추가하고 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.

이 필드의 내용...	수행할 작업...
자격 증명	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성합니다. 자격 증명에 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하십시오. 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 의해 결정됩니다.

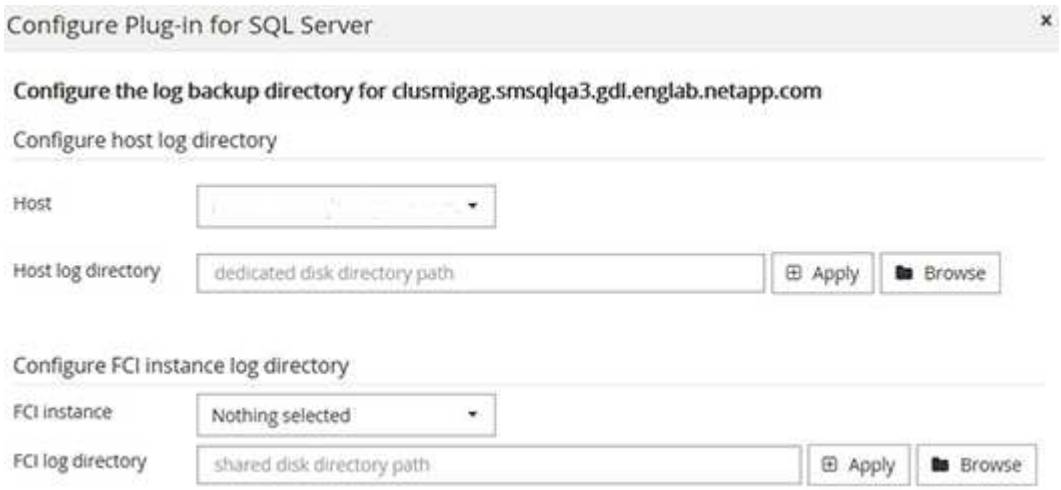
5. 설치할 플러그인 선택 * 섹션에서 설치할 플러그인을 선택합니다.
6. 추가 옵션 * 을 선택합니다.

이 필드의 내용...	수행할 작업...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정합니다. 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 지정할 수 있습니다.
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 검사를 건너뜁니다	플러그인이 이미 수동으로 설치되어 있고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.

이 필드의 내용...	수행할 작업...
그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행합니다	그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행하려면 이 확인란을 선택합니다. GMSA 이름을 domainName\accountName$ 형식으로 제공합니다. GMSA를 사용하여 호스트를 추가하고 GMSA에 로그인 및 sys 관리자 권한이 있는 경우 GMSA를 사용하여 SQL 인스턴스에 연결합니다.

7. 제출 * 을 선택합니다.
8. SQL 플러그인의 경우 로그 디렉토리를 구성할 호스트를 선택합니다.
   a. Configure log directory * 를 선택하고 Configure host log directory 페이지에서 * Browse * 를 선택하고 다음 단계를 완료합니다.

      NetApp LUN(드라이브)만 선택할 수 있습니다. SnapCenter는 호스트 로그 디렉토리를 백업 작업의 일부로 백업 및 복제합니다.



      i. 호스트 로그가 저장될 호스트에서 드라이브 문자 또는 마운트 지점을 선택합니다.
      ii. 필요한 경우 하위 디렉토리를 선택합니다.
      iii. 저장 * 을 선택합니다.
9. 제출 * 을 선택합니다.

   사전 검사 건너뛰기 * 확인란을 선택하지 않은 경우 호스트가 플러그인 설치 요구사항을 충족하는지 여부를 확인합니다. 디스크 공간, RAM, PowerShell 버전, .NET 버전, 위치(Windows 플러그인의 경우) 및 Java 버전(Linux 플러그인의 경우)은 최소 요구 사항에 따라 검증됩니다. 최소 요구 사항이 충족되지 않으면 적절한 오류 또는 경고 메시지가 표시됩니다.

   오류가 디스크 공간 또는 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 파일을 업데이트해야 합니다.

10. 설치 과정을 모니터링합니다.

cmdlet을 사용하여 여러 원격 호스트에 **Microsoft SQL Server**용 **SnapCenter** 플러그인을 설치합니다

Install-SmHostPackage PowerShell cmdlet을 사용하여 Microsoft SQL Server용 SnapCenter 플러그인을 여러 호스트에 동시에 설치할 수 있습니다.

시작하기 전에

플러그인 패키지를 설치할 각 호스트에 대한 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 cmdlet 및 필수 매개 변수를 사용하여 여러 원격 호스트에 Microsoft SQL Server용 SnapCenter 플러그인을 설치합니다.

   cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

   플러그인을 이미 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려는 경우 -skipprecheck 옵션을 사용할 수 있습니다.

4. 원격 설치를 위한 자격 증명을 입력합니다.

명령줄에서 **Microsoft SQL Server**용 **SnapCenter** 플러그인을 자동으로 설치합니다

SnapCenter 사용자 인터페이스 내에서 Microsoft SQL Server용 SnapCenter 플러그인을 설치해야 합니다. 그러나 어떤 이유로 인해 Windows 명령줄에서 자동 모드로 SQL Server용 플러그인 설치 프로그램을 실행할 수 없습니다.

시작하기 전에

- 설치하기 전에 Microsoft SQL Server용 SnapCenter 플러그인의 이전 버전을 삭제해야 합니다.

  자세한 내용은 을 참조하십시오 "플러그인 호스트에서 직접 SnapCenter 플러그인을 설치하는 방법".

단계

1. 플러그인 호스트에 C:\temp 폴더가 있고 로그인한 사용자가 이 폴더에 대한 모든 액세스 권한을 가지고 있는지 확인합니다.
2. C:\ProgramData\NetApp\SnapCenter\Package Repository에서 SQL Server용 플러그인 소프트웨어를 다운로드합니다.

   이 경로는 SnapCenter 서버가 설치된 호스트에서 액세스할 수 있습니다.

3. 플러그인을 설치할 호스트에 설치 파일을 복사합니다.
4. 로컬 호스트의 Windows 명령 프롬프트에서 플러그인 설치 파일을 저장한 디렉토리로 이동합니다.
5. SQL Server용 플러그인 소프트웨어를 설치합니다.

   ```
   "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
   ```

   개체 틀 값을 데이터로 바꿉니다

   - DEBUG_Log_Path는 제품군 설치 프로그램 로그 파일의 이름과 위치입니다.
   - log_Path 는 플러그인 구성 요소(SCW, SCSQL 및 SMCore)의 설치 로그 위치입니다.
   - Num은 SnapCenter이 SMCore와 통신하는 포트입니다
   - install_Directory_Path는 호스트 플러그인 패키지 설치 디렉토리입니다.
   - domain\administrator 는 Microsoft Windows 웹 서비스 계정용 SnapCenter 플러그인입니다.
   - 암호는 Microsoft Windows 웹 서비스 계정용 SnapCenter 플러그인의 암호입니다.
     를 누릅니다
     ```
     "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 Server용 플러그인 설치 중에 전달되는 모든 매개 변수는 대/소문자를 구분합니다.

6. Windows 작업 스케줄러, 기본 설치 로그 파일 C:\Installdebug.log 및 추가 설치 파일을 C:\Temp에서 모니터링합니다.
7. %temp% 디렉터리를 모니터링하여 msiexe.exe 설치 프로그램이 오류 없이 소프트웨어를 설치하고 있는지 확인합니다.

SQL Server용 플러그인을 설치하면 SnapCenter 서버가 아닌 호스트에 플러그인이 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록할 수 있습니다. 호스트가 추가되면 플러그인이 자동으로 검색됩니다.

SQL Server용 플러그인 설치 상태를 모니터링합니다

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행률을 모니터링할 수 있습니다. 설치 진행 상황을 확인하여 설치 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다

- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다

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 클릭합니다.
   b. 선택 사항: 시작 및 종료 날짜를 지정합니다.
   c. 유형 드롭다운 메뉴에서 * 플러그인 설치 * 를 선택합니다.
   d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
   e. 적용 * 을 클릭합니다.
4. 설치 작업을 선택하고 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. Job Details * 페이지에서 * View logs * 를 클릭합니다.

CA 인증서를 구성합니다

CA 인증서 CSR 파일을 생성합니다

CSR(인증서 서명 요청)을 생성하고 생성된 CSR을 사용하여 CA(인증 기관)에서 가져올 수 있는 인증서를 가져올 수 있습니다. 인증서에 연결된 개인 키가 있습니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.

CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 자세한 내용은 을 참조하십시오 "CA 인증서 CSR 파일을 생성하는 방법".

도메인(* .domain.company.com) 또는 시스템(machine1.domain.company.com CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter를 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN) 및 해당 호스트 이름을 CA 인증서에 언급해야 합니다. 인증서를 조달하기 전에 SAN(Subject Alternative Name) 필드를 채워 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(* .domain.company.com)의 경우 인증서에 도메인의 모든 호스트 이름이 암시적으로 포함됩니다.

CA 인증서를 가져옵니다

MMC(Microsoft Management Console)를 사용하여 CA 인증서를 SnapCenter 서버 및 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 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 단추로 클릭한 다음 * 모든 작업 * > * 가져오기 * 를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료합니다.

이 마법사 창에서...	다음을 수행합니다.
개인 키를 가져옵니다	예 * 옵션을 선택하고 개인 키를 가져온 다음 * 다음 * 을 클릭합니다.
파일 형식 가져오기	변경하지 않고 * 다음 * 을 클릭합니다.
보안	내보낸 인증서에 사용할 새 암호를 지정하고 * 다음 * 을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

> 인증서 가져오기는 개인 키와 함께 번들로 제공됩니다(지원되는 형식은 *.pfx, *.p12 및 *.p7b 입니다).

7. "개인" 폴더에 대해 5단계를 반복합니다.

CA 인증서 지문을 받습니다

인증서 thumbprint는 인증서를 식별하는 16진수 문자열입니다. 썸프린트는 썸프린트 알고리즘을 사용하여 인증서 컨텐츠에서 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.
   a. 인증서를 두 번 클릭합니다.
   b. 인증서 대화 상자에서 * 세부 정보 * 탭을 클릭합니다.
   c. 필드 목록을 스크롤하여 * Thumbprint * 를 클릭합니다.
   d. 상자에서 16진수 문자를 복사합니다.
   e. 16진수 사이의 공백을 제거합니다.

      예를 들어, 썸프린트가 "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 0d 42 77 A3 2a 7b"인 경우 공백을 제거한 후 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.
   a. 다음 명령을 실행하여 설치된 인증서의 엄지손가락 지문을 나열하고 최근 설치된 인증서를 주체 이름으로 식별합니다.

      Get-ChildItem-Path 인증:*LocalMachine\My*

   b. 엄지손가락 지문을 복사합니다.

Windows 호스트 플러그인 서비스를 사용하여 **CA** 인증서를 구성합니다

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스를 사용하여 CA 인증서를 구성해야 합니다.

SnapCenter 서버 및 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하여 기존 인증서 바인딩을 제거합니다.

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   예를 들면 다음과 같습니다.

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스와 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 들면 다음과 같습니다.

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

플러그인에 대해 **CA** 인증서를 활성화합니다

CA 인증서를 구성하고 SnapCenter 서버 및 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- run_Set-SmCertificateSettings_cmdlet을 사용하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- _get-SmCertificateSettings_를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 호스트 페이지에서 * 관리되는 호스트 * 를 클릭합니다.
3. 단일 또는 여러 플러그인 호스트를 선택합니다.
4. 추가 옵션 * 을 클릭합니다.
5. 인증서 유효성 검사 사용 * 을 선택합니다.

작업을 마친 후

관리 호스트 탭 호스트에는 자물쇠가 표시되고 자물쇠 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- 는 CA 인증서가 활성화되지 않았으며 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- CA 인증서의 유효성을 확인했음을 나타냅니다.
- CA 인증서의 유효성을 확인할 수 없음을 나타냅니다.
- 연결 정보를 검색할 수 없음을 나타냅니다.

> 상태가 노란색 또는 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

재해 복구 구성

SQL Server용 **SnapCenter** 플러그인의 재해 복구

SQL Server용 SnapCenter 플러그인이 다운된 경우 다음 단계를 사용하여 다른 SQL 호스트로 전환하고 데이터를 복구합니다.

시작하기 전에

- 보조 호스트의 운영 체제, 애플리케이션 및 호스트 이름은 운영 호스트와 동일해야 합니다.
- 호스트 추가 * 또는 * 호스트 수정 * 페이지를 사용하여 대체 호스트로 SnapCenter SQL Server용 플러그인을 푸시합니다. 을 참조하십시오 "호스트를 관리합니다" 를 참조하십시오.

단계

1. SnapCenter Plug-in for SQL Server를 수정하고 설치하려면 * Hosts * 페이지에서 호스트를 선택합니다.
2. (선택 사항) 재해 복구(DR) 백업에서 새 시스템으로 SQL Server용 SnapCenter 플러그인 구성 파일을 교체합니다.
3. DR 백업에서 SnapCenter Plug-in for SQL Server 폴더에서 Windows 및 SQL 일정을 가져옵니다.

관련 정보

를 참조하십시오 "재해 복구 API" 비디오.

SQL Server용 **SnapCenter** 플러그인을 위한 스토리지 재해 복구**(DR**

글로벌 설정 페이지에서 스토리지용 DR 모드를 활성화하여 SQL Server용 SnapCenter 플러그인을 복구할 수 있습니다.

시작하기 전에

- 플러그인이 유지보수 모드인지 확인합니다.
- SnapMirror/SnapVault 연결 끊기.
  "SnapMirror 관계를 더욱 공고히 합니다"
- 2차 LUN의 LUN을 동일한 드라이브 문자로 호스트 시스템에 연결합니다.
- DR 이전에 사용한 드라이브 문자와 동일한 드라이브 문자를 사용하여 모든 디스크가 연결되어 있는지 확인합니다.
- MSSQL 서버 서비스를 다시 시작합니다.
- SQL 리소스가 다시 온라인 상태인지 확인합니다.

이 작업에 대해

DR(재해 복구)은 VMDK 및 RDM 구성에서 지원되지 않습니다.

단계

1. 설정 페이지에서 * 설정 * > * 글로벌 설정 * > * 재해 복구 * 로 이동합니다.
2. 재해 복구 사용 * 을 선택합니다.
3. 적용 * 을 클릭합니다.
4. Monitor * > * Jobs * 를 클릭하여 DR 작업이 활성화되었는지 여부를 확인합니다.

작업을 마친 후

- 페일오버 후에 새 데이터베이스가 생성되면 데이터베이스가 비 DR 모드로 전환됩니다.

  새 데이터베이스는 페일오버 이전과 마찬가지로 계속 작동합니다.

- DR 모드에서 생성된 새 백업은 토폴로지 페이지의 SnapMirror 또는 SnapVault(보조) 아래에 나열됩니다.

  새 백업 옆에 "i" 아이콘이 표시되어 DR 모드 중에 이러한 백업이 생성되었음을 나타냅니다.

- UI 또는 다음 cmdlet을 사용하여 페일오버 중에 생성된 SQL Server 백업용 SnapCenter 플러그인을 삭제할 수 있습니다. `Remove-SmBackup`
- 장애 조치 후 일부 리소스를 DR 모드가 아닌 모드로 설정하려면 다음 cmdlet을 사용합니다. `Remove-SmResourceDRMode`

  자세한 내용은 를 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

- SnapCenter 서버는 DR 또는 비 DR 모드에 있지만 DR 모드 또는 비 DR 모드에 있는 스토리지 리소스가 있는 리소스 그룹이 아닌 개별 스토리지 리소스(SQL 데이터베이스)를 관리합니다.

SnapCenter Plug-in for SQL Server 보조 스토리지에서 운영 스토리지로 페일백

SQL Server 운영 스토리지용 SnapCenter 플러그인이 다시 온라인 상태가 되면 운영 스토리지로 페일백해야 합니다.

시작하기 전에

- 관리 호스트 페이지의 * 유지 관리 * 모드로 SQL Server용 SnapCenter 플러그인을 배치합니다.
- 호스트에서 보조 스토리지를 분리하고 운영 스토리지에서 접속합니다.
- 운영 스토리지로 페일백하려면 역방향 재동기화 작업을 수행하여 페일오버 전의 관계 방향이 그대로 유지되는지 확인합니다.

  역재동기화 작업 후 운영 스토리지와 보조 스토리지의 역할을 유지하려면 역방향 재동기화 작업을 다시 한 번 수행하십시오.

  자세한 내용은 을 참조하십시오 "미러 관계를 역재동기화합니다"

- MSSQL 서버 서비스를 다시 시작합니다.
- SQL 리소스가 다시 온라인 상태인지 확인합니다.

> 플러그인의 페일오버 또는 페일백 중에는 플러그인 전체 상태가 즉시 업데이트되지 않습니다. 호스트 및 플러그인의 전체 상태는 후속 호스트 새로 고침 작업 중에 업데이트됩니다.

단계

1. 설정 페이지에서 * 설정 * > * 글로벌 설정 * > * 재해 복구 * 로 이동합니다.
2. [재해 복구 사용] * 을 선택 취소합니다.
3. 적용 * 을 클릭합니다.
4. Monitor * > * Jobs * 를 클릭하여 DR 작업이 활성화되었는지 여부를 확인합니다.

작업을 마친 후

UI 또는 다음 cmdlet을 사용하여 페일오버 중에 생성된 SQL Server 백업용 SnapCenter 플러그인을 삭제할 수 있습니다. `Remove-SmDRFailoverBackups`

VMware vSphere용 SnapCenter 플러그인을 설치합니다

데이터베이스가 가상 머신(VM)에 저장되어 있거나 VM 및 데이터 저장소를 보호하려는 경우 SnapCenter Plug-in for VMware vSphere 가상 어플라이언스를 구축해야 합니다.

배포에 대한 자세한 내용은 을 참조하십시오 "구축 개요".

CA 인증서를 배포합니다

VMware vSphere용 SnapCenter 플러그인을 사용하여 CA 인증서를 구성하려면 를 참조하십시오 "SSL 인증서를 생성하거나 가져옵니다".

CRL 파일을 구성합니다

VMware vSphere용 SnapCenter 플러그인은 사전 구성된 디렉토리에서 CRL 파일을 찾습니다. VMware vSphere용 SnapCenter 플러그인의 기본 CRL 파일 디렉토리는 */opt/netapp/config/CRL* 입니다.

이 디렉터리에 둘 이상의 CRL 파일을 배치할 수 있습니다. 들어오는 인증서는 각 CRL에 대해 확인됩니다.

데이터 보호를 준비합니다

Microsoft SQL Server용 SnapCenter 플러그인 사용을 위한 사전 요구 사항

SQL Server용 플러그인을 사용하기 전에 SnapCenter 관리자가 SnapCenter Server를 설치 및 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다.
- SnapCenter에 로그인합니다.
- 스토리지 시스템 접속을 추가하거나 할당하고 자격 증명을 생성하여 SnapCenter 환경을 구성합니다.

> SnapCenter은 서로 다른 클러스터에서 동일한 이름의 여러 SVM을 지원하지 않습니다. SnapCenter에서 지원하는 각 SVM에는 고유한 이름이 있어야 합니다.

- 호스트 추가, 플러그인 설치, 리소스 검색(새로 고침) 및 플러그인 구성
- Invoke-SmConfigureResources를 실행하여 로컬 디스크에서 NetApp LUN으로 기존 Microsoft SQL Server 데이터베이스를 이동하거나 그 반대로 이동합니다.

  cmdlet 실행에 대한 자세한 내용은 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드"

- SnapCenter 서버를 사용하여 VMware RDM LUN 또는 VMDK에 상주하는 SQL 데이터베이스를 보호하는 경우 VMware vSphere용 SnapCenter 플러그인을 구축하고 SnapCenter에 플러그인을 등록해야 합니다. 자세한 내용은 VMware vSphere용 SnapCenter 플러그인 설명서를 참조하십시오.

  "VMware vSphere용 SnapCenter 플러그인 설명서"

- Microsoft Windows용 SnapCenter 플러그인을 사용하여 호스트 측 스토리지 프로비저닝을 수행합니다.
- 백업 복제를 원하는 경우 SnapMirror 및 SnapVault 관계를 설정합니다.

자세한 내용은 SnapCenter 설치 정보를 참조하십시오.

SnapCenter 4.1.1 사용자의 경우 VMware vSphere 4.1.1 용 SnapCenter 플러그인 설명서에 가상화 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 나와 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 VMware vSphere용 SnapCenter 플러그인을 사용하여 가상화된 데이터베이스 및 파일 시스템을 보호하는 방법에 대한 정보가 수록되어 있습니다. SnapCenter 4.3.x 사용자의 경우 SnapCenter Plug-in for VMware vSphere 4.3 설명서에는 Linux 기반 SnapCenter Plug-in for VMware vSphere 가상 어플라이언스(오픈 가상 어플라이언스 형식)를 사용하여 가상화된 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 수록되어 있습니다.

"VMware vSphere용 SnapCenter 플러그인 설명서"

리소스, 리소스 그룹 및 정책을 사용하여 SQL Server를 보호하는 방법

SnapCenter를 사용하기 전에 수행할 백업, 클론 및 복원 작업과 관련된 기본 개념을 이해하는 것이 좋습니다. 서로 다른 작업을 위해 리소스, 리소스 그룹 및 정책과 상호 작용합니다.

- 리소스는 일반적으로 SnapCenter을 사용하여 백업 또는 복제하는 데이터베이스, 데이터베이스 인스턴스 또는 Microsoft SQL Server 가용성 그룹입니다.

- SnapCenter 리소스 그룹은 호스트 또는 클러스터의 리소스 모음입니다.

  자원 그룹에 대해 작업을 수행할 때 자원 그룹에 지정한 일정에 따라 자원 그룹에 정의된 자원에 대해 해당 작업을 수행합니다.

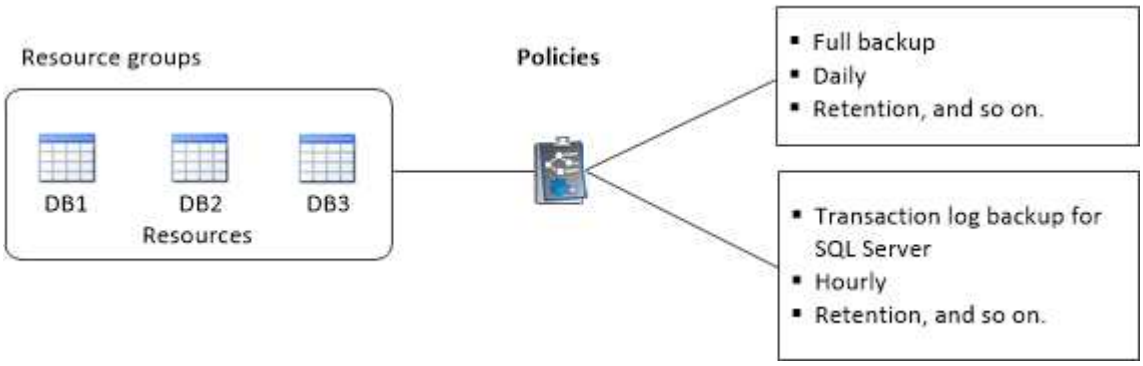
  필요에 따라 단일 리소스 또는 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 수행할 수도 있습니다.

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

  자원 그룹을 만들 때 해당 그룹에 대해 하나 이상의 정책을 선택합니다. 단일 리소스에 대해 필요 시 백업을 수행할 때 정책을 선택할 수도 있습니다.

보호하려는_대상_과 이를 보호할 시기를 요일과 시간으로 정의하는 자원 그룹을 생각해 보십시오. 정책을 정의하는 _ 방법 _ 을(를) 보호하려는 것으로 생각해 보십시오. 예를 들어 모든 데이터베이스를 백업하거나 호스트의 모든 파일 시스템을 백업하는 경우 모든 데이터베이스나 호스트의 모든 파일 시스템을 포함하는 리소스 그룹을 생성할 수 있습니다. 그런 다음 리소스 그룹에 일별 정책과 시간별 정책이라는 두 가지 정책을 연결할 수 있습니다. 리소스 그룹을 생성하고 정책을 연결할 때 매일 전체 백업을 수행하고 로그 백업을 매시간 수행하는 다른 일정을 수행하도록 리소스 그룹을 구성할 수 있습니다.

다음 그림에서는 데이터베이스 리소스, 리소스 그룹 및 정책 간의 관계를 보여 줍니다.



SQL Server 데이터베이스, 인스턴스 또는 가용성 그룹을 백업합니다

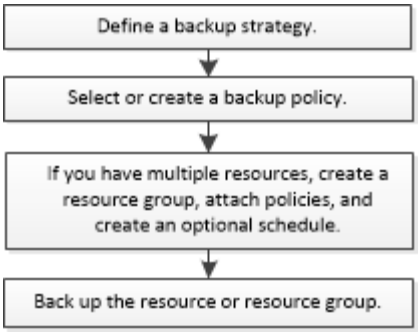
백업 워크플로우

사용자 환경에 Microsoft SQL Server용 SnapCenter 플러그인을 설치하면 SnapCenter를 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 워크플로에서는 백업 작업을 수행해야 하는 순서를 보여 줍니다.



NetApp이 아닌 LUN, 손상된 데이터베이스 또는 복원 중인 데이터베이스를 선택하면 Resources 페이지의 Backup Now, Restore, Manage Backups 및 Clone 옵션이 비활성화됩니다.

PowerShell cmdlet을 수동으로 또는 스크립트에서 사용하여 백업, 복원, 복구, 확인 및 클론 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드"

SnapCenter가 데이터베이스를 백업하는 방법

SnapCenter는 스냅샷 복사본 기술을 사용하여 LUN 또는 VMDK에 상주하는 SQL Server 데이터베이스를 백업합니다. SnapCenter은 데이터베이스의 스냅샷 복사본을 생성하여 백업을 생성합니다.

리소스 페이지에서 전체 데이터베이스 백업에 사용할 데이터베이스를 선택하면 SnapCenter는 동일한 스토리지 볼륨에 상주하는 다른 모든 데이터베이스를 자동으로 선택합니다. LUN 또는 VMDK에서 하나의 데이터베이스만 저장하는 경우 데이터베이스를 개별적으로 선택 또는 다시 선택할 수 있습니다. LUN 또는 VMDK에 여러 데이터베이스가 포함된 경우 데이터베이스를 그룹으로 선택 또는 다시 선택해야 합니다.

단일 볼륨에 상주하는 모든 데이터베이스가 Snapshot 복사본을 사용하여 동시에 백업됩니다. 최대 동시 백업 데이터베이스 수가 35이고 스토리지 볼륨에 데이터베이스가 35개 이상인 경우 생성되는 총 스냅샷 복사본 수는 데이터베이스 수를 35개로 나눈 값과 같습니다.

백업 정책의 각 스냅샷 복사본에 대한 최대 데이터베이스 수를 구성할 수 있습니다.

SnapCenter에서 스냅샷 복사본을 생성하면 전체 스토리지 시스템 볼륨이 스냅샷 복사본에 캡처됩니다. 그러나 백업은 백업이 생성된 SQL 호스트 서버에만 유효합니다.

다른 SQL 호스트 서버의 데이터가 동일한 볼륨에 상주하는 경우 스냅샷 복사본에서 이 데이터를 복원할 수 없습니다.

- 자세한 정보 찾기 *

"PowerShell cmdlet을 사용하여 리소스를 백업합니다"

"리소스 중지 또는 그룹화 작업이 실패했습니다"

리소스를 백업에 사용할 수 있는지 여부를 확인합니다

리소스는 설치한 플러그인에서 유지 관리하는 데이터베이스, 애플리케이션 인스턴스, 가용성 그룹 및 유사한 구성 요소입니다. 이러한 리소스를 리소스 그룹에 추가하여 데이터 보호 작업을 수행할 수 있지만 먼저 사용 가능한 리소스를 확인해야 합니다. 사용 가능한 리소스를 확인하면 플러그인 설치가 성공적으로 완료되었는지 확인할 수도 있습니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 접속 생성, 자격 증명 추가 등의 작업을 이미 완료해야 합니다.
- Microsoft SQL 데이터베이스를 검색하려면 다음 조건 중 하나를 충족해야 합니다.
  - 플러그인 호스트를 SnapCenter 서버에 추가하는 데 사용한 사용자는 Microsoft SQL Server에서 필요한 사용 권한(sysadmin)을 가져야 합니다.
  - 위 조건이 충족되지 않으면 SnapCenter 서버에서 Microsoft SQL Server에 필요한 권한(sysadmin)을 가진 사용자를 구성해야 합니다. 사용자는 Microsoft SQL Server 인스턴스 수준에서 구성해야 하며 사용자는 SQL 또는 Windows 사용자일 수 있습니다.
- Windows 클러스터에서 Microsoft SQL 데이터베이스를 검색하려면 FCI(장애 조치 클러스터 인스턴스) TCP/IP 포트의 차단을 해제해야 합니다.
- 데이터베이스가 VMware RDM LUN 또는 VMDK에 상주하는 경우 VMware vSphere용 SnapCenter 플러그인을 구축하고 SnapCenter에 플러그인을 등록해야 합니다.

  자세한 내용은 을 참조하십시오 "VMware vSphere용 SnapCenter 플러그인 구축"
- GMSA로 호스트를 추가하고 GMSA에 로그인 및 시스템 관리자 권한이 있는 경우 GMSA를 사용하여 SQL 인스턴스에 연결합니다.

이 작업에 대해

Details 페이지의 * Overall Status * 옵션이 Not Available for backup으로 설정되어 있으면 데이터베이스를 백업할 수 없습니다. 다음 중 하나라도 해당하면 * Overall Status *(전체 상태 *) 옵션이 Not Available(백업 불가)로 설정됩니다.

- 데이터베이스가 NetApp LUN에 없습니다.
- 데이터베이스가 정상 상태가 아닙니다.

  데이터베이스가 오프라인 상태, 복원 중, 복구 보류 중, 의심스런 등의 상태일 때 정상 상태가 아닙니다.
- 데이터베이스에 권한이 없습니다.

  예를 들어, 사용자가 데이터베이스에 대한 보기 액세스 권한만 있는 경우 데이터베이스의 파일 및 속성을 식별할 수 없으므로 백업할 수 없습니다.

SQL Server Standard Edition에 가용성 그룹 구성이 있는 경우 SnapCenter는 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 * 또는 * 인스턴스 * 또는 * 가용성 그룹 * 을 선택합니다.

   을 클릭합니다 호스트 이름과 SQL Server 인스턴스를 선택하여 리소스를 필터링합니다. 그런 다음 을 클릭할 수 있습니다 를 눌러 필터 창을 닫습니다.
3. 리소스 새로 고침 * 을 클릭합니다.

   새로 추가, 이름 변경 또는 삭제된 리소스가 SnapCenter 서버 인벤토리로 업데이트됩니다.

데이터베이스가 SnapCenter 외부에서 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

리소스는 리소스 유형, 호스트 또는 클러스터 이름, 관련 리소스 그룹, 백업 유형, 정책 및 전체 상태와 같은 정보와 함께 표시됩니다.

- 데이터베이스가 비 NetApp 스토리지에 있는 경우 `Not available for backup` 이(가) * Overall Status *(전체 상태) 열에 표시됩니다.

  NetApp이 아닌 스토리지에 있는 데이터베이스에는 데이터 보호 작업을 수행할 수 없습니다.

- 데이터베이스가 NetApp 스토리지에 있고 보호되지 않는 경우 `Not protected` 이(가) * Overall Status *(전체 상태) 열에 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되어 있는 경우 사용자 인터페이스가 표시됩니다 `Backup not run` 메시지가 * Overall Status * 열에 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되고 있고 데이터베이스에 대해 백업이 트리거되는 경우 사용자 인터페이스가 표시됩니다 `Backup succeeded` 메시지가 * Overall Status * 열에 표시됩니다.

자격 증명을 설정하는 동안 SQL 인증을 활성화한 경우 검색된 인스턴스 또는 데이터베이스에 빨간색 자물쇠 아이콘이 표시됩니다. 자물쇠 아이콘이 나타나면 인스턴스 또는 데이터베이스 자격 증명을 지정하여 인스턴스 또는 데이터베이스를 리소스 그룹에 성공적으로 추가해야 합니다.

1. SnapCenter 관리자가 RBAC 사용자에게 리소스를 할당한 후에는 RBAC 사용자가 로그인하여 * 자원 새로 고침 * 을 클릭하여 리소스의 최신 * 전체 상태 * 를 확인해야 합니다.

리소스를 **NetApp** 스토리지 시스템으로 마이그레이션

Microsoft Windows용 SnapCenter 플러그인을 사용하여 NetApp 스토리지 시스템을 프로비저닝한 후에는 SnapCenter 그래픽 사용자 인터페이스(GUI) 또는 PowerShell cmdlet을 사용하여 리소스를 NetApp 스토리지 시스템이나 NetApp LUN 간에 마이그레이션할 수 있습니다.

시작하기 전에

- SnapCenter 서버에 스토리지 시스템을 추가해야 합니다.
- SQL Server 리소스를 새로 고친(검색된) 상태여야 합니다.

이 마법사 페이지의 대부분의 필드는 설명이 필요 없습니다. 다음 정보는 안내가 필요할 수 있는 일부 필드에 대해 설명합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 * 데이터베이스 * 또는 * 인스턴스 * 를 선택합니다.
3. 목록에서 데이터베이스 또는 인스턴스를 선택하고 * migrate * 를 클릭합니다.
4. 리소스 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
• 데이터베이스 이름 * (선택 사항)	마이그레이션할 인스턴스를 선택한 경우 * Databases * 드롭다운 목록에서 해당 인스턴스의 데이터베이스를 선택해야 합니다.
• 목적지 선택 *	데이터 및 로그 파일의 타겟 위치를 선택합니다. 데이터 및 로그 파일은 선택한 NetApp 드라이브 아래에 각각 Data 및 Log 폴더로 이동됩니다. 폴더 구조에 폴더가 없으면 폴더가 만들어지고 리소스가 마이그레이션됩니다.
• 데이터베이스 파일 세부 정보 표시 * (선택 사항)	단일 데이터베이스의 여러 파일을 마이그레이션하려는 경우 이 옵션을 선택합니다. 인스턴스 * 리소스를 선택하면 이 옵션이 표시되지 않습니다.
• 옵션 *	소스에서 데이터베이스 복사본을 삭제하려면 * Delete copy of Migrated Database at Original Location * 을 선택합니다. 선택 사항: * 데이터베이스를 분리하기 전에 테이블에 대한 업데이트 통계를 실행합니다 *.

5. 확인 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
• 데이터베이스 일관성 검사 옵션 *	마이그레이션 전에 데이터베이스의 무결성을 확인하려면 * Run Before * 를 선택합니다. 마이그레이션 후 데이터베이스의 무결성을 확인하려면 * Run After * 를 선택합니다.

이 필드의 내용...	수행할 작업...
• DBCC CHECKDB 옵션 *	• 무결성 검사를 데이터베이스의 물리적 구조로 제한하고 데이터베이스에 영향을 미치는 찢어진 페이지, 체크섬 오류 및 일반적인 하드웨어 오류를 감지하려면 * physical_only * 옵션을 선택합니다. • 모든 정보 메시지를 표시하지 않으려면 * no_INFOMSGS * 옵션을 선택합니다. • All_ERRORMSGS * 옵션을 선택하여 객체별로 보고된 모든 오류를 표시합니다. • 클러스터링되지 않은 인덱스를 선택하지 않으려면 * NOINDEX * 옵션을 선택합니다. SQL Server 데이터베이스는 DBCC(Microsoft SQL Server Database Consistency Checker)를 사용하여 데이터베이스 개체의 논리적 무결성 및 물리적 무결성을 검사합니다. ⓘ 이 옵션을 선택하면 실행 시간이 줄어들 수 있습니다. • 내부 데이터베이스 스냅샷 복사본을 사용하는 대신 **TABLOCK** 옵션을 선택하여 검사를 제한하고 잠금을 확보합니다.

6. 요약을 검토한 다음 마침을 클릭합니다.

SQL Server 데이터베이스에 대한 백업 정책을 생성합니다

SnapCenter를 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 및 스토리지 시스템 접속 생성과 같은 작업을 완료하여 데이터 보호를 위한 준비를 갖추어야 합니다.
- 로그 백업을 위해 호스트 로그 디렉토리를 구성해야 합니다.
- SQL Server 리소스를 새로 고친(검색된) 상태여야 합니다.
- 스냅샷 복사본을 미러 또는 볼트에 복제하는 경우 SnapCenter 관리자는 소스 볼륨과 타겟 볼륨 모두에 SVM(스토리지 가상 머신)을 할당해야 합니다.

  관리자가 사용자에게 리소스를 할당하는 방법에 대한 자세한 내용은 SnapCenter 설치 정보를 참조하십시오.

- powershellProcessforScripts 매개 변수의 값을 web.config 파일에서 true 로 설정하여 powerpare 및 postscripts 로 PowerShell 스크립트를 실행해야 합니다.

기본값은 false 입니다.

이 작업에 대해

백업 정책은 백업을 관리 및 유지하는 방법과 리소스 또는 리소스 그룹을 백업하는 빈도를 제어하는 규칙의 집합입니다. 또한 복제 및 스크립트 설정을 지정할 수 있습니다. 정책에 옵션을 지정하면 다른 리소스 그룹에 대한 정책을 다시 사용할 때 시간이 절약됩니다.

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 swagger에서 API:API/4.7/configsettings를 통해 표시할 수 있습니다

Get API를 사용하여 키 값을 표시할 수 있습니다. API 설정은 지원되지 않습니다.

1단계**:** 정책 이름 생성

1. 왼쪽 탐색 창에서 * 설정 * 을 선택합니다.
2. 설정 페이지에서 * 정책 * 을 선택합니다.
3. New * 를 선택합니다.
4. 이름 * 페이지에서 정책 이름과 설명을 입력합니다.

2단계**:** 백업 옵션 구성

1. 백업 유형을 선택합니다

전체 백업 및 로그 백업

데이터베이스 파일 및 트랜잭션 로그를 백업하고 트랜잭션 로그를 잘라냅니다.

1. 전체 백업 및 로그 백업 * 을 선택합니다.
2. 각 스냅샷 복사본에 대해 백업해야 하는 최대 데이터베이스 수를 입력합니다.

여러 백업 작업을 동시에 실행하려면 이 값을 늘려야 합니다.

전체 백업

데이터베이스 파일을 백업합니다.

1. 전체 백업 * 을 선택합니다.
2. 각 스냅샷 복사본에 대해 백업해야 하는 최대 데이터베이스 수를 입력합니다.
기본값은 100입니다

여러 백업 작업을 동시에 실행하려면 이 값을 늘려야 합니다.

로그 백업

트랜잭션 로그를 백업합니다.
. Log backup * 을 선택합니다.

백업만 복사

1. 다른 백업 응용 프로그램을 사용하여 리소스를 백업하는 경우 * 백업만 복사 * 를 선택합니다.

트랜잭션 로그를 그대로 유지하면 모든 백업 애플리케이션이 데이터베이스를 복구할 수 있습니다. 일반적으로 다른 상황에서는 복사 전용 옵션을 사용하지 않아야 합니다.

Microsoft SQL은 보조 스토리지에 대해 * 전체 백업 및 로그 백업 * 옵션과 함께 * 복사 전용 백업 * 옵션을 지원하지 않습니다.

1. 가용성 그룹 설정 섹션에서 다음 작업을 수행합니다.

   a. 기본 백업 복제본에서만 백업합니다.

      기본 백업 복제본에서만 백업하려면 이 옵션을 선택합니다. 기본 백업 복제본은 SQL Server의 AG에 대해 구성된 백업 기본 설정에 따라 결정되며

   b. 백업할 복제본을 선택합니다.

      운영 AG 복제본 또는 보조 AG 복제본을 백업에 선택합니다.

   c. 백업 우선 순위 선택(최소 및 최대 백업 우선 순위)

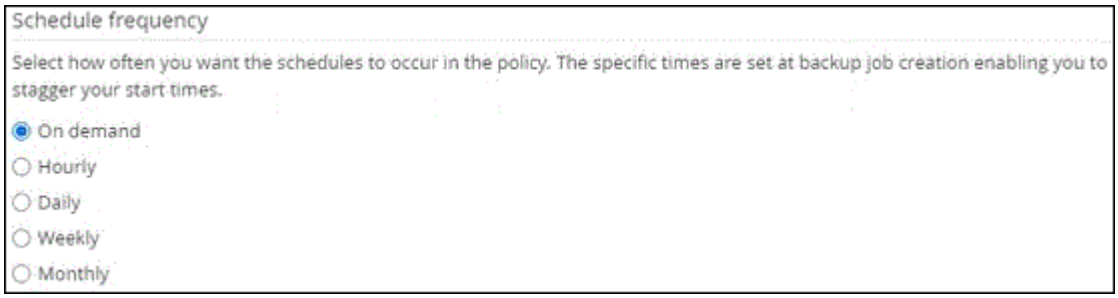
      최소 백업 우선 순위 번호와 백업에 대한 AG 복제본을 결정하는 최대 백업 우선 순위 번호를 지정합니다. 예를 들어 최소 우선 순위는 10이고 최대 우선 순위는 50입니다. 이 경우 우선 순위가 10보다 큰 모든 AG 복제본이 백업에 고려됩니다.

기본적으로 최소 우선 순위는 1이고 최대 우선 순위는 100입니다.

클러스터 구성에서 백업은 정책에 설정된 보존 설정에 따라 클러스터의 각 노드에 유지됩니다. AG의 소유자 노드가 변경되면 보존 설정에 따라 백업이 수행되고 이전 소유자 노드의 백업은 유지됩니다. AG에 대한 보존은 노드 레벨에서만 적용할 수 있습니다.

2. 이 정책의 백업 빈도를 예약합니다. On demand *, * Hourly *, * Daily *, * Weekly * 또는 * Monthly * 를 선택하여 일정 유형을 지정합니다.

   정책에 대해 하나의 일정 유형만 선택할 수 있습니다.



리소스 그룹을 생성하는 동안 백업 작업의 스케줄(시작 날짜, 종료 날짜 및 빈도)을 지정할 수 있습니다. 이렇게 하면 동일한 정책 및 백업 빈도를 공유하는 리소스 그룹을 생성할 수 있지만 각 정책에 서로 다른 백업 스케줄을 할당할 수 있습니다.

오전 2시에 예약된 경우 DST(일광 절약 시간) 중에는 일정이 트리거되지 않습니다.

3단계**:** 보존 설정을 구성합니다

보존 페이지에서 백업 유형 페이지에서 선택한 백업 유형에 따라 다음 작업 중 하나 이상을 수행합니다.

1. 최신 복원 작업에 대한 보존 설정 섹션에서 다음 작업 중 하나를 수행합니다.

특정 사본 수

특정 수의 스냅샷 복사본만 보유합니다.

1. 최근 <number>일 * 에 적용할 수 있는 로그 백업 보존 옵션을 선택하고 보존할 일 수를 지정합니다. 이 제한에 근접하면 이전 복사본을 삭제할 수 있습니다.

특정 일 수입니다

백업 사본을 특정 기간 동안 보관합니다.

1. 마지막 <number>일간의 전체 백업 기간 * 에 적용할 수 있는 로그 백업 보존 옵션을 선택하고 로그 백업 사본을 보관할 일 수를 지정합니다.

1. 필요 시 보존 설정에 대한 * 전체 백업 보존 설정 * 섹션에서 다음 작업을 수행합니다.
   a. 유지할 총 스냅샷 복사본 수를 지정합니다
      i. 유지할 스냅샷 복사본 수를 지정하려면 * 유지할 총 스냅샷 복사본 * 을 선택합니다.

ii. 스냅샷 복사본 수가 지정된 수를 초과하면 가장 오래된 복사본이 먼저 삭제된 후 스냅샷 복사본이 삭제됩니다.

기본적으로 보존 횟수 값은 2로 설정됩니다. 보존 횟수를 1로 설정하면 새 스냅샷 복사본이 타겟으로 복제될 때까지 첫 번째 스냅샷 복사본이 SnapVault 관계의 참조 스냅샷 복사본이므로 보존 작업이 실패할 수 있습니다.

최대 보존 값은 ONTAP 9.4 이상의 리소스에 대해 1018이고, ONTAP 9.3 이전 버전의 리소스에 대해서는 254입니다. 보존이 기본 ONTAP 버전에서 지원하는 값보다 높은 값으로 설정된 경우 백업이 실패합니다.

1. Snapshot 복사본 유지 시간
   a. 스냅샷 복사본을 삭제하기 전에 보관할 일 수를 지정하려면 * 스냅샷 복사본 보관 기간 * 을 선택합니다.
2. 시간별, 일별, 주별 및 월별 보존 설정의 * 전체 백업 보존 설정 * 섹션에서 백업 유형 페이지에서 선택한 스케줄 유형에 대한 보존 설정을 지정합니다.
   a. 유지할 총 스냅샷 복사본 수를 지정합니다
      i. 유지할 스냅샷 복사본 수를 지정하려면 * 유지할 총 스냅샷 복사본 * 을 선택합니다. 스냅샷 복사본 수가 지정된 수를 초과하면 가장 오래된 복사본이 먼저 삭제된 후 스냅샷 복사본이 삭제됩니다.

SnapVault 복제를 설정하려면 보존 수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷 복사본이 타겟으로 복제될 때까지 첫 번째 스냅샷 복사본이 SnapVault 관계의 참조 스냅샷 복사본이므로 보존 작업이 실패할 수 있습니다.

1. Snapshot 복사본 유지 시간
   a. 스냅샷 복사본을 삭제하기 전에 보관할 일 수를 지정하려면 * 스냅샷 복사본 보관 기간 * 을 선택합니다.

로그 스냅샷 복사본의 보존은 기본적으로 7일로 설정됩니다. Set-SmPolicy cmdlet을 사용하여 로그 스냅샷 복사본 보존을 변경합니다.

이 예에서는 로그 스냅샷 복사본 보존을 2로 설정합니다.

예 **1.** 예제 보기

```
Set-SmPolicy-PolicyName 'newpol' - PolicyType 'Backup' - PluginPolicyType 'CSQL' - sqlbackuptype
'FullBackupAndLogBackup' - RetenionSettings@{BackupType='DATA'; ScheduleType='Hourly';
RetentionCount = 2}, @{BackupenetSnapshot'; ScheduleType = 'ScheduleReturetEnretionCount'
```

"SnapCenter은 데이터베이스의 스냅샷 복사본을 유지합니다"

4단계**:** 복제 설정을 구성합니다

1. 복제 페이지에서 보조 스토리지 시스템에 대한 복제를 지정합니다.

SnapMirror를 업데이트합니다

로컬 스냅샷 복사본을 생성한 후 SnapMirror를 업데이트합니다.

1. 다른 볼륨(SnapMirror)에 백업 세트의 미러 복사본을 생성하려면 이 옵션을 선택합니다.

SnapVault를 업데이트합니다

스냅샷 복사본을 생성한 후 SnapVault를 업데이트합니다.

1. 디스크 간 백업 복제를 수행하려면 이 옵션을 선택합니다.

보조 정책 레이블

1. 스냅샷 레이블을 선택합니다.

선택한 스냅샷 복사본 레이블에 따라 ONTAP에서는 해당 레이블과 일치하는 2차 스냅샷 복사본 보존 정책을 적용합니다.

로컬 스냅샷 복사본 * 을 생성한 후 SnapMirror 업데이트 * 를 선택한 경우, 선택적으로 보조 정책 레이블을 지정할 수 있습니다. 그러나 로컬 스냅샷 복사본 * 을 생성한 후 * SnapVault 업데이트 * 를 선택한 경우에는 보조 정책 레이블을 지정해야 합니다.

오류 재시도 횟수

1. 프로세스가 중지되기 전에 수행해야 하는 복제 시도 횟수를 입력합니다.

5단계**:** 스크립트 설정을 구성합니다

1. 스크립트 페이지에서 백업 작업 전후에 실행해야 하는 처방인 또는 PS의 경로와 인수를 각각 입력합니다.

   예를 들어 스크립트를 실행하여 SNMP 트랩을 업데이트하고, 경고를 자동화하고, 로그를 보낼 수 있습니다.

처방자 또는 사후 스크립트 경로에는 드라이브 또는 공유가 포함되어서는 안 됩니다. 경로는 scripts_path에 상대해야 합니다.

보조 스토리지가 스냅샷 복사본의 최대 제한에 도달하지 않도록 ONTAP에서 SnapMirror 보존 정책을 구성해야 합니다.

6단계**:** 확인 설정 구성

확인 페이지에서 다음 단계를 수행하십시오.

1. 다음 백업 스케줄에 대한 확인 실행 섹션에서 스케줄 빈도를 선택합니다.
2. 데이터베이스 일관성 검사 옵션 섹션에서 다음 작업을 수행합니다.
   a. 무결성 구조를 데이터베이스의 물리적 구조로 제한(physical_only)
      i. 무결성 검사를 데이터베이스의 물리적 구조로 제한하고 데이터베이스에 영향을 미치는 찢어진 페이지, 체크섬 오류 및 일반적인 하드웨어 오류를 검색하려면 * 데이터베이스의 물리적 구조로 무결성 구조를 제한합니다(physical_only) * 를 선택합니다.

b. 모든 정보 메시지 표시 안 함(INFOMSGS 없음)

   i. 모든 정보 메시지를 표시하지 않으려면 * 모든 정보 메시지 억제(no_INFOMSGS) * 를 선택합니다. 기본적으로 선택되어 있습니다.

c. 객체별 보고된 모든 오류 메시지 표시(ALL_ERRORMSGS)

   i. 객체별로 보고된 모든 오류 메시지 표시(ALL_ERRORMSGS) * 를 선택하여 객체별로 보고된 모든 오류를 표시합니다.

d. 클러스터링되지 않은 인덱스(NOINDEX) 확인 안 함

   i. 클러스터링되지 않은 인덱스를 선택하지 않으려면 * 클러스터링되지 않은 인덱스(NOINDEX) * 를 선택합니다. SQL Server 데이터베이스는 DBCC(Microsoft SQL Server Database Consistency Checker)를 사용하여 데이터베이스 개체의 논리적 무결성 및 물리적 무결성을 검사합니다.

e. 내부 데이터베이스 스냅샷 복사본(TABLOCK)을 사용하지 않고 검사를 제한하고 잠금을 확보합니다.

   i. 내부 데이터베이스 Snapshot 복사본(TABLOCK) * 을 사용하여 검사를 제한하고 내부 데이터베이스 Snapshot 복사본을 사용하지 않고 잠금을 가져오는 대신 * Limit the checks and obtain the lock 을 선택합니다.

3. 로그 백업 * 섹션에서 * 완료 시 로그 백업 확인 * 을 선택하여 완료 시 로그 백업을 확인합니다.
4. 검증 스크립트 설정 * 섹션에서 검증 작업 전후에 실행해야 하는 처방인 또는 PS의 경로와 인수를 각각 입력합니다.

> 처방자 또는 사후 스크립트 경로에는 드라이브 또는 공유가 포함되어서는 안 됩니다. 경로는 scripts_path에 상대해야 합니다.

7단계**:** 요약 검토

1. 요약을 검토한 후 * Finish * 를 선택합니다.

리소스 그룹을 만들고 **SQL Server**에 대한 정책을 연결합니다

리소스 그룹은 함께 백업 및 보호할 리소스를 추가하는 컨테이너입니다. 리소스 그룹을 사용하면 지정된 애플리케이션과 연결된 모든 데이터를 동시에 백업할 수 있습니다. 모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한 수행할 데이터 보호 작업의 유형을 정의하려면 하나 이상의 정책을 리소스 그룹에 연결해야 합니다.

새 자원 그룹을 만들지 않고도 자원을 개별적으로 보호할 수 있습니다. 보호된 리소스에서 백업을 수행할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 데이터베이스 * 를 선택합니다.

> 최근에 SnapCenter에 리소스를 추가한 경우 * 리소스 새로 고침 * 을 클릭하여 새로 추가된 리소스를 확인합니다.

3. 새 리소스 그룹 * 을 클릭합니다.
4. 이름 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
이름	자원 그룹 이름을 입력합니다. 리소스 그룹 이름은 250자를 초과할 수 없습니다.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력합니다. 예를 들어 HR을 여러 자원 그룹에 태그로 추가하면 나중에 HR 태그와 연결된 모든 자원 그룹을 찾을 수 있습니다.
스냅샷 복사본에 대해 사용자 지정 이름 형식을 사용합니다	선택 사항: 사용자 지정 스냅샷 복사본의 이름 및 형식을 입력합니다. 예를 들어 customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname을 입력합니다. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.

5. 리소스 페이지에서 다음 단계를 수행하십시오.
   a. 드롭다운 목록에서 호스트 이름, 리소스 유형 및 SQL Server 인스턴스를 선택하여 리소스 목록을 필터링합니다.

      최근에 추가한 자원은 자원 목록을 새로 고친 후에만 사용 가능한 자원 목록에 나타납니다.

   b. 사용 가능한 리소스* 섹션에서 선택한 리소스 섹션으로 리소스를 이동하려면 다음 단계 중 하나를 수행하십시오.
      - 동일한 스토리지 볼륨에 있는 모든 리소스를 선택한 리소스 섹션으로 이동하려면 * 동일한 스토리지 볼륨에 있는 모든 리소스를 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 선택합니다.

      * 를 클릭하여 정책을 생성할 수도 있습니다 + *.

      선택한 정책에 대한 스케줄 구성 섹션에 선택한 정책이 나열됩니다.

   b. 선택한 정책에 대한 일정 구성 섹션에서 * 를 클릭합니다 + 일정을 구성하려는 정책에 대한 스케줄 구성 열의
   c. policy_policy_name_schedules 추가 대화 상자에서 시작 날짜, 만료 날짜 및 빈도를 지정하여 스케줄을 구성한 다음 * 확인 * 을 클릭합니다.

      정책에 나열된 각 빈도에 대해 이 작업을 수행해야 합니다. 구성된 스케줄은 * 선택한 정책에 대한 스케줄 구성 * 섹션의 적용된 스케줄 열에 나열됩니다.

   d. Microsoft SQL Server 스케줄러를 선택합니다.

스케줄링 정책과 연결할 스케줄러 인스턴스도 선택해야 합니다.

Microsoft SQL Server 스케줄러를 선택하지 않으면 기본값은 Microsoft Windows 스케줄러입니다.

타사 백업 스케줄은 SnapCenter 백업 스케줄과 겹치는 경우 지원되지 않습니다. 스케줄을 수정하고 Windows 스케줄러 또는 SQL Server 에이전트에서 생성된 백업 작업의 이름을 변경해서는 안 됩니다.

7. 확인 페이지에서 다음 단계를 수행하십시오.

   a. 검증 서버 * 드롭다운 목록에서 검증 서버를 선택합니다.

      목록에는 SnapCenter에 추가된 모든 SQL Server가 포함됩니다. 여러 검증 서버(로컬 호스트 또는 원격 호스트)를 선택할 수 있습니다.

      검증 서버 버전은 기본 데이터베이스를 호스팅하는 SQL Server의 버전 및 버전과 일치해야 합니다.

   a. Load locators * 를 클릭하여 SnapMirror 및 SnapVault 볼륨을 로드하여 보조 스토리지에 대한 검증을 수행합니다.

   b. 확인 일정을 구성할 정책을 선택한 다음 * 를 클릭합니다  *.

   c. Add Verification Schedules policy_name 대화 상자에서 다음 작업을 수행합니다.

원하는 작업	수행할 작업...
백업 후 확인을 실행합니다	백업 후 검증 실행 * 을 선택합니다.
검증 예약	Run scheduled verification * 을 선택합니다.

   d. 확인 * 을 클릭합니다.

      구성된 일정이 Applied Schedules 열에 나열됩니다. * 를 클릭하여 검토 후 편집할 수 있습니다  * 또는 * 를 클릭하여 삭제합니다  *.

8. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 자원 그룹에서 수행된 작업의 보고서를 첨부하려면 * 작업 보고서 첨부 * 를 선택합니다.

   이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmtpServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

9. 요약을 검토하고 * Finish * 를 클릭합니다.

관련 정보

"SQL Server 데이터베이스에 대한 백업 정책을 생성합니다"

SQL 리소스 백업 요구 사항

SQL 리소스를 백업하기 전에 몇 가지 요구 사항이 충족되었는지 확인해야 합니다.

- 비 NetApp 스토리지 시스템에서 NetApp 스토리지 시스템으로 리소스를 마이그레이션해야 합니다.
- 백업 정책을 만들어야 합니다.
- 보조 스토리지와 SnapMirror 관계가 있는 리소스를 백업하려면 스토리지 사용자에게 할당된 ONTAP 역할에 "'스냅샷 전체' 권한이 있어야 합니다. 그러나 "vsadmin" 역할을 사용하는 경우에는 "napmirror all" 권한이 필요하지 않습니다.
- SQL 인스턴스 자격 증명이 AD 사용자 또는 그룹에 할당되지 않으면 AD(Active Directory) 사용자가 시작한 백업 작업이 실패합니다. 설정 * > * 사용자 액세스 * 페이지에서 AD 사용자 또는 그룹에 SQL 인스턴스 자격 증명을 할당해야 합니다.
- 정책이 연결된 리소스 그룹을 만들어야 합니다.
- 리소스 그룹에 서로 다른 호스트의 데이터베이스가 여러 개 있는 경우 네트워크 문제로 인해 일부 호스트의 백업 작업이 늦게 트리거될 수 있습니다. Set-SmConfigSettings PS cmdlet을 사용하여 web.config에서 FMaxRetryForUninitializedHosts 의 값을 구성해야 합니다.

SQL 리소스를 백업합니다

자원이 아직 자원 그룹에 속하지 않은 경우 자원 페이지에서 자원을 백업할 수 있습니다.

이 작업에 대해

- Windows 자격 증명 인증의 경우 플러그인을 설치하기 전에 자격 증명을 설정해야 합니다.
- SQL Server 인스턴스 인증의 경우 플러그인을 설치한 후 자격 증명을 추가해야 합니다.
- GMSA 인증의 경우, GMSA를 활성화 및 사용하려면 SnapCenter에 호스트를 등록하는 동안 * 호스트 추가 * 또는 * 호스트 수정 * 페이지에서 GMSA를 설정해야 합니다.
- GMSA로 호스트를 추가하고 GMSA에 로그인 및 시스템 관리자 권한이 있는 경우 GMSA를 사용하여 SQL 인스턴스에 연결합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 * 데이터베이스 * 또는 * 인스턴스 * 또는 * 가용성 그룹 * 을 선택합니다.

    a. 백업하려는 데이터베이스, 인스턴스 또는 가용성 그룹을 선택합니다.

        인스턴스 백업을 수행할 때 마지막 백업 상태 또는 해당 인스턴스의 타임스탬프에 대한 정보는 리소스 페이지에서 사용할 수 없습니다.

    토폴로지 보기에서는 백업 상태, 타임스탬프 또는 백업이 인스턴스 또는 데이터베이스에 대한 것인지 구분할 수 없습니다.

3. 리소스 페이지에서 * 스냅샷 복사본의 * 사용자 지정 이름 형식 확인란을 선택한 다음 스냅샷 복사본 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

    예를 들어 customtext_policy_hostname 또는 resource_hostname을 입력합니다. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.

4. 정책 페이지에서 다음 작업을 수행합니다.

   a. 정책 섹션의 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

      - 를 선택하여 정책을 생성할 수 있습니다 + 를 눌러 정책 마법사를 시작합니다.

      선택한 정책에 대한 일정 구성 * 섹션에 선택한 정책이 나열됩니다.

   b. 를 선택합니다 + 일정을 구성하려는 정책에 대한 스케줄 구성 열의

   c. 에 정책 * 에 대한 스케줄 추가 * 가 있습니다 `policy_name` 대화 상자에서 스케줄을 구성한 다음 * OK * 를 선택합니다.

      여기 `policy_name` 선택한 정책의 이름입니다.

   구성된 스케줄은 * Applied Schedules * 열에 나열됩니다.

   a. Microsoft SQL Server 스케줄러 사용 * 을 선택한 다음 일정 관리 정책과 연결된 * 스케줄러 인스턴스 * 드롭다운 목록에서 스케줄러 인스턴스를 선택합니다.

5. 확인 페이지에서 다음 단계를 수행하십시오.

   a. 검증 서버 * 드롭다운 목록에서 검증 서버를 선택합니다.

      여러 검증 서버(로컬 호스트 또는 원격 호스트)를 선택할 수 있습니다.

      검증 서버 버전은 기본 데이터베이스를 호스팅하는 SQL Server 버전의 버전과 같거나 그 이상이어야 합니다.

   a. 보조 스토리지 시스템의 백업을 확인하려면 * 보조 로케이터 로드 * 를 선택합니다.

   b. 확인 일정을 구성할 정책을 선택한 다음 * 를 선택합니다 + *.

   c. Add Verification Schedules_policy_name_대화 상자에서 다음 작업을 수행합니다.

원하는 작업	수행할 작업...
백업 후 확인을 실행합니다	백업 후 검증 실행 * 을 선택합니다.
검증 예약	Run scheduled verification * 을 선택합니다.

      검증 서버에 스토리지 접속이 없는 경우 디스크 마운트 실패 오류가 발생하면서 확인 작업이 실패합니다.

   d. OK * 를 선택합니다.

      구성된 일정이 Applied Schedules 열에 나열됩니다.

6. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 자원 그룹에서 수행된 작업의 보고서를 첨부하려면 * 작업 보고서 첨부 * 를 선택합니다.

> 이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmtpServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

7. 요약을 검토한 후 * Finish * 를 선택합니다.

   데이터베이스 토폴로지 페이지가 표시됩니다.

8. 지금 백업 * 을 선택합니다.
9. 백업 페이지에서 다음 단계를 수행하십시오.

   a. 리소스에 여러 정책을 적용한 경우 * 정책 * 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

      필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

   b. 백업 후 확인 * 을 선택하여 백업을 확인합니다.

   c. 백업 * 을 선택합니다.

      > Windows 스케줄러 또는 SQL Server 에이전트에서 생성된 백업 작업의 이름은 바꾸지 않아야 합니다.

      필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

   암시적 리소스 그룹이 만들어집니다. 사용자 액세스 페이지에서 해당 사용자 또는 그룹을 선택하여 이 정보를 볼 수 있습니다. 암시적 리소스 그룹 유형은 "리소스"입니다.

10. Monitor * > * Jobs * 를 선택하여 작업 진행 상황을 모니터링합니다.

작업을 마친 후

- MetroCluster 구성에서 SnapCenter는 페일오버 후 보호 관계를 감지하지 못할 수 있습니다.

  "MetroCluster 페일오버 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다"

- VMDK에서 애플리케이션 데이터를 백업하고 VMware vSphere용 SnapCenter 플러그인의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다. Java 힙 크기를 늘리려면 스크립트 파일 /opt/netapp/init_scripts/scvservice를 찾습니다. 이 스크립트에서 은 입니다 `do_start method` Command SnapCenter VMware 플러그인 서비스를 시작합니다. 다음 명령을 업데이트합니다. `Java -jar -Xmx8192M -Xms4096M`.

관련 정보

"SQL Server 데이터베이스에 대한 백업 정책을 생성합니다"

"PowerShell cmdlet을 사용하여 리소스를 백업합니다"

"TCP_TIMEOUT의 지연으로 인해 MySQL 연결 오류로 인해 백업 작업이 실패합니다"

"Windows 스케줄러 오류로 인해 백업이 실패합니다"

"리소스 중지 또는 그룹화 작업이 실패했습니다"

SQL Server 리소스 그룹을 백업합니다

리소스 페이지에서 필요 시 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 연결되어 있고 스케줄이 구성되어 있는 경우 스케줄에 따라 백업이 자동으로 수행됩니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 리소스 그룹 * 을 선택합니다.

   검색 상자에 리소스 그룹 이름을 입력하거나 * 를 선택하여 리소스 그룹을 검색할 수 있습니다[필터 아이콘]를 누른 다음 태그를 선택합니다. 그런 다음 * 를 선택할 수 있습니다[필터 아이콘]를 눌러 필터 창을 닫습니다.

3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음 * 지금 백업 * 을 선택합니다.
4. 백업 페이지에서 다음 단계를 수행하십시오.
   a. 여러 정책을 리소스 그룹에 연결한 경우 * Policy * 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

      필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

   b. 백업 후 * Verify * 를 선택하여 필요 시 백업을 확인합니다.

      정책의 * Verify * 옵션은 예약된 작업에만 적용됩니다.

   c. 백업 * 을 선택합니다.
5. Monitor * > * Jobs * 를 선택하여 작업 진행 상황을 모니터링합니다.

관련 정보

"SQL Server 데이터베이스에 대한 백업 정책을 생성합니다"

"리소스 그룹을 만들고 SQL Server에 대한 정책을 연결합니다"

"PowerShell cmdlet을 사용하여 리소스를 백업합니다"

"TCP_TIMEOUT의 지연으로 인해 MySQL 연결 오류로 인해 백업 작업이 실패합니다"

"Windows 스케줄러 오류로 인해 백업이 실패합니다"

백업 작업을 모니터링합니다

SnapCenter 작업 페이지에서 **SQL** 리소스 백업 작업을 모니터링합니다

SnapCenterJobs 페이지를 사용하여 여러 백업 작업의 진행률을 모니터링할 수 있습니다. 진행 상황을 확인하여 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

다음 아이콘이 작업 페이지에 나타나고 작업의 해당 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨

단계

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 모니터 페이지에서 * 작업 * 을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행하십시오.
   a. 을 클릭합니다 백업 작업만 나열되도록 목록을 필터링합니다.
   b. 시작 및 종료 날짜를 지정합니다.
   c. Type * 드롭다운 목록에서 * Backup * 을 선택합니다.
   d. Status * (상태 *) 드롭다운에서 백업 상태를 선택합니다.
   e. 작업이 성공적으로 완료되었는지 보려면 * Apply * 를 클릭합니다.
4. 백업 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.

   백업 작업 상태가 표시됩니다 작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 기호로 표시되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 * 로그 보기 * 를 클릭합니다.

   로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

작업 창에서 **SQL** 리소스에 대한 데이터 보호 작업을 모니터링합니다

작업 창에는 가장 최근에 수행한 작업 5개가 표시됩니다. 작업 창은 작업이 시작된 시점과 작업의 상태도 표시합니다.

작업 창에는 백업, 복원, 클론 및 예약된 백업 작업에 대한 정보가 표시됩니다. SQL Server용 플러그인 또는 Exchange Server용 플러그인을 사용하는 경우 작업 창에 다시 시드된 작업에 대한 정보도 표시됩니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 을 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다.

   작업 중 하나를 클릭하면 작업 세부 정보가 * 작업 세부 정보 * 페이지에 나열됩니다.

PowerShell cmdlet을 사용하여 스토리지 시스템 연결과 자격 증명을 생성합니다

PowerShell cmdlet을 사용하여 데이터 보호 작업을 수행하기 전에 SVM(Storage Virtual Machine) 연결과 자격 증명을 생성해야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행할 수 있도록 PowerShell 환경을 준비해야 합니다.
- 스토리지 접속을 생성하려면 인프라스트럭처 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

  호스트 캐시가 업데이트되지 않고 데이터베이스 상태가 SnapCenter GUI에 ""백업을 위해 사용할 수 없음"" 또는 ""NetApp 스토리지에 없음""으로 표시될 수 있으므로 스토리지 시스템 접속을 추가하는 동안 호스트 플러그인 설치가 진행되어서는 안 됩니다.

- 스토리지 시스템 이름은 고유해야 합니다.

  SnapCenter는 서로 다른 클러스터에서 동일한 이름의 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 연결 세션을 시작합니다.

   이 예제에서는 PowerShell 세션을 엽니다.

   ```
   PS C:\> Open-SmConnection
   ```

2. Add-SmStorageConnection cmdlet을 사용하여 스토리지 시스템에 대한 새 접속을 생성합니다.

   이 예에서는 새 스토리지 시스템 접속을 생성합니다.

   ```
   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 FinanceAdmin 이라는 새 자격 증명을 만듭니다.

   ```
   PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
   -Credential sddev\administrator
   ```

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

PowerShell cmdlet을 사용하여 리소스를 백업합니다

PowerShell cmdlet을 사용하여 SQL Server 데이터베이스 또는 Windows 파일 시스템을 백업할 수 있습니다. 여기에는 SQL Server 데이터베이스 또는 Windows 파일 시스템 백업에는 SnapCenter Server와의 연결 설정, SQL Server 데이터베이스 인스턴스 또는 Windows 파일 시스템 검색, 정책 추가, 백업 리소스 그룹 생성, 백업 및 백업 확인이 포함됩니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 스토리지 시스템 접속을 추가하고 자격 증명을 생성해야 합니다.
- 호스트 및 검색된 리소스를 추가해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

   사용자 이름 및 암호 프롬프트가 표시됩니다.

2. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.

   이 예제에서는 SQL 백업 유형이 FullBackup인 새 백업 정책을 만듭니다.

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

   이 예에서는 Windows 파일 시스템 백업 유형이 Crash일관성(crash일관성)인 새 백업 정책을 생성합니다.

```
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 시스템에 대한 리소스를 검색합니다.

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. 추가 SmResourceGroup cmdlet을 사용하여 SnapCenter에 새 리소스 그룹을 추가합니다.

   이 예제에서는 지정된 정책 및 리소스를 사용하여 새 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 예에서는 지정된 정책 및 리소스를 사용하여 새 Windows 파일 시스템 백업 리소스 그룹을 생성합니다.

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. New-SmBackup cmdlet을 사용하여 새 백업 작업을 시작합니다.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Get-SmBackupReport cmdlet을 사용하여 백업 작업의 상태를 봅니다.

   이 예는 지정된 날짜에 실행된 모든 작업의 작업 요약 보고서를 표시합니다.

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

Microsoft SQL Server 백업 작업에 대한 SnapCenter 플러그인을 취소합니다

실행 중이거나 대기 중이거나 응답하지 않는 백업 작업을 취소할 수 있습니다. 백업 작업을 취소하면 생성된 백업이 SnapCenter 서버에 등록되지 않은 경우 SnapCenter 서버가 작업을 중지하고 스토리지에서 모든 스냅샷 복사본을 제거합니다. 백업이 이미 SnapCenter 서버에 등록되어 있는 경우 취소가 트리거된 후에도 이미 생성된 스냅샷 복사본이 롤백되지 않습니다.

시작하기 전에

- 복원 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 대기열에 있거나 실행 중인 로그 또는 전체 백업 작업만 취소할 수 있습니다.
- 확인이 시작된 후에는 작업을 취소할 수 없습니다.

  확인 전에 작업을 취소하면 작업이 취소되고 확인 작업이 수행되지 않습니다.

- 모니터 페이지 또는 작업 창에서 백업 작업을 취소할 수 있습니다.
- SnapCenter GUI를 사용하는 것 외에도 PowerShell cmdlet을 사용하여 작업을 취소할 수 있습니다.
- 취소할 수 없는 작업에 대해 * 작업 취소 * 버튼이 비활성화됩니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 사용자\그룹 페이지에서 다른 구성원 개체를 보고 작동할 수 있음 * 을 선택한 경우 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 백업 작업을 취소할 수 있습니다.

단계

다음 작업 중 하나를 수행합니다.

시작...	조치
모니터 페이지	1. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 선택합니다. 2. 작업을 선택하고 * 작업 취소 * 를 선택합니다.
작업 창	1. 백업 작업을 시작한 후 을 선택합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다. 2. 작업을 선택합니다. 3. 작업 세부 정보 페이지에서 * 작업 취소 * 를 선택합니다.

결과

작업이 취소되고 리소스가 이전 상태로 돌아갑니다. 취소한 작업이 취소 또는 실행 상태에서 응답하지 않는 경우 를 실행해야 합니다 `Cancel-SmJob -JobID <int> -Force` 백업 작업을 강제로 중지하는 cmdlet.

토폴로지 페이지에서 SQL Server 백업 및 클론 보기

리소스를 백업 또는 복제할 때 운영 스토리지와 보조 스토리지의 모든 백업 및 클론을 그래픽으로 표시하는 것이 유용할 수 있습니다.

이 작업에 대해

토폴로지 페이지에서 선택한 리소스 또는 리소스 그룹에 사용할 수 있는 모든 백업 및 클론을 볼 수 있습니다. 이러한 백업 및 클론의 세부 정보를 확인한 다음 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

Manage Copies * 보기에서 다음 아이콘을 검토하여 운영 스토리지 또는 보조 스토리지(미러 복사본 또는 볼트 사본)에서 백업 및 클론을 사용할 수 있는지 여부를 확인할 수 있습니다.

- 기본 스토리지에서 사용할 수 있는 백업 및 클론 수를 표시합니다.

-  SnapMirror 기술을 사용하여 보조 스토리지에 미러링된 백업 및 클론 수를 표시합니다.
-  SnapVault 기술을 사용하여 보조 스토리지에 복제된 백업 및 클론 수를 표시합니다.
  - 표시된 백업 수에는 보조 스토리지에서 삭제된 백업이 포함됩니다.

    예를 들어 정책을 사용하여 6개의 백업을 생성하여 4개의 백업만 보존한 경우 표시되는 백업 수는 6입니다.

미러 볼트 유형 볼륨에 있는 버전에 따라 유연한 미러 백업의 클론은 토폴로지 뷰에 표시되지만 토폴로지 뷰에 있는 미러 백업 횟수에는 버전에 따라 유연하게 백업할 수 있는 백업이 포함되지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 자원 세부 정보 보기 또는 자원 그룹 세부 정보 보기에서 자원을 선택합니다.

   선택한 리소스가 복제된 데이터베이스인 경우 클론 생성된 데이터베이스를 보호합니다. 그러면 클론의 소스가 토폴로지 페이지에 표시됩니다. 복제에 사용된 백업을 보려면 * Details * 를 클릭합니다.

   리소스가 보호되는 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. Summary 카드를 검토하여 운영 스토리지와 보조 스토리지에서 사용할 수 있는 백업 및 클론 수를 요약합니다.

   요약 카드 * 섹션에는 총 백업 및 클론 수가 표시됩니다.

   Refresh * 버튼을 클릭하면 스토리지 쿼리가 시작되어 정확한 카운트를 표시합니다.

5. 복사본 관리 * 보기에서 기본 또는 보조 스토리지에서 * 백업 * 또는 * 클론 * 을 클릭하여 백업 또는 클론의 세부 정보를 확인합니다.

   백업 및 클론의 세부 정보가 표 형식으로 표시됩니다.

6. 테이블에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 클론 복제, 이름 바꾸기 및 삭제 작업을 수행합니다.

   보조 스토리지에 있는 백업의 이름을 바꾸거나 백업을 삭제할 수 없습니다.

7. 테이블에서 클론을 선택하고 * Clone Split * 을 클릭합니다.
8. 클론을 삭제하려면 표에서 클론을 선택한 다음 을 클릭합니다  .

PowerShell cmdlet을 사용하여 백업을 제거합니다

다른 데이터 보호 작업에 더 이상 필요하지 않은 경우 Remove-SmBackup cmdlet을 사용하여 백업을 삭제할 수 있습니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Remove-SmBackup cmdlet을 사용하여 하나 이상의 백업을 삭제합니다.

   이 예에서는 백업 ID를 사용하여 두 개의 백업을 삭제합니다.

```
Remove-SmBackup -BackupIds 3,4
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"):
```

PowerShell cmdlet을 사용하여 보조 백업 수를 정리합니다

Remove-SmBackup cmdlet을 사용하여 스냅샷 복사본이 없는 보조 백업의 백업 수를 정리할 수 있습니다. 복사본 관리 토폴로지에 표시된 총 스냅샷 복사본이 보조 스토리지 스냅샷 복사본 보존 설정과 일치하지 않을 때 이 cmdlet을 사용할 수 있습니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. CleanupSecondaryBackups 매개 변수를 사용하여 보조 백업 수를 정리합니다.

   이 예에서는 스냅샷 복사본 없이 2차 백업의 백업 수를 정리합니다.

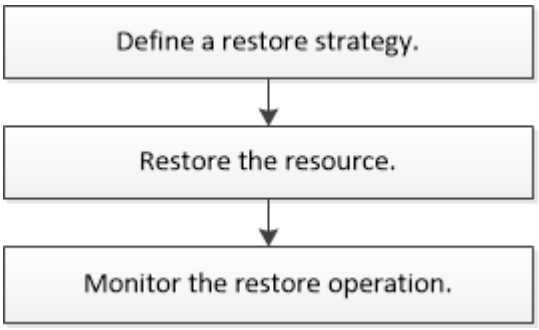
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

SQL Server 리소스를 복구합니다

워크플로를 복원합니다

SnapCenter를 사용하여 하나 이상의 백업에서 액티브 파일 시스템으로 데이터를 복구한 다음 데이터베이스를 복구하여 SQL Server 데이터베이스를 복원할 수 있습니다. 가용성 그룹에 있는 데이터베이스를 복구한 다음 복원된 데이터베이스를 가용성 그룹에 추가할 수도 있습니다. SQL Server 데이터베이스를 복원하기 전에 몇 가지 준비 작업을 수행해야 합니다.

다음 워크플로에서는 데이터베이스 복원 작업을 수행해야 하는 순서를 보여 줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트에서 사용하여 백업, 복원, 복구, 확인 및 클론 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드"

- 자세한 정보 찾기 *

"보조 스토리지에서 SQL Server 데이터베이스를 복구합니다"

"PowerShell cmdlet을 사용하여 리소스 복원 및 복구"

"Windows 2008 R2에서 복원 작업이 실패할 수 있습니다"

데이터베이스 복원 요구 사항

Microsoft SQL Server 백업용 SnapCenter 플러그인에서 SQL Server 데이터베이스를 복원하기 전에 몇 가지 요구 사항이 충족되는지 확인해야 합니다.

- 데이터베이스를 복구하려면 대상 SQL Server 인스턴스가 온라인 상태이고 실행 중이어야 합니다.

  이는 사용자 데이터베이스 복원 작업과 시스템 데이터베이스 복원 작업 모두에 적용됩니다.

- 원격 관리 또는 원격 검증 서버에서 예약된 작업을 포함하여 복원하려는 SQL Server 데이터에 대해 실행되도록 예약된 SnapCenter 작업을 비활성화해야 합니다.
- 시스템 데이터베이스가 작동하지 않는 경우 먼저 SQL Server 유틸리티를 사용하여 시스템 데이터베이스를 재구성해야 합니다.
- 플러그인을 설치하는 경우 다른 역할에 대한 사용 권한을 부여하여 AG(Availability Group) 백업을 복원해야 합니다.

다음 조건 중 하나가 충족되면 AG 복원이 실패합니다.

- RBAC 사용자가 플러그인을 설치하고 관리자가 AG 백업을 복원하려고 할 경우
- 관리자가 플러그인을 설치하고 RBAC 사용자가 AG 백업을 복원하려고 하면

- 사용자 지정 로그 디렉토리 백업을 대체 호스트로 복원하는 경우 SnapCenter 서버 및 플러그인 호스트에 동일한 SnapCenter 버전이 설치되어 있어야 합니다.
- Microsoft 핫픽스 KB2887595를 설치해야 합니다. KB2887595에 대한 자세한 내용은 Microsoft 지원 사이트 를 참조하십시오.

  "Microsoft 지원 문서 2887595: Windows RT 8.1, Windows 8.1, Windows Server 2012 R2 업데이트 롤업: 2013년 11월"

- 리소스 그룹 또는 데이터베이스를 백업해야 합니다.
- 스냅샷 복사본을 미러 또는 볼트에 복제하는 경우 SnapCenter 관리자는 소스 볼륨과 타겟 볼륨 모두에 SVM(스토리지 가상 머신)을 할당해야 합니다.

  관리자가 사용자에게 리소스를 할당하는 방법에 대한 자세한 내용은 SnapCenter 설치 정보를 참조하십시오.

- 데이터베이스를 복구하기 전에 모든 백업 및 클론 작업을 중지해야 합니다.
- 데이터베이스 크기가 테라바이트(TB)인 경우 복원 작업 시간이 초과될 수 있습니다.

  Set-SmConfigSettings-Agent-configSettings@{"RESTTimeout"="20000000"} 명령을 실행하여 SnapCenter 서버의 RESTTimeout 매개 변수 값을 20000000 ms로 늘려야 합니다. 데이터베이스 크기에 따라 시간 초과 값을 변경할 수 있으며 설정할 수 있는 최대값은 86400,000ms입니다.

데이터베이스가 온라인 상태일 때 복원하려면 복원 페이지에서 온라인 복원 옵션을 활성화해야 합니다.

SQL Server 데이터베이스 백업을 복원합니다

SnapCenter를 사용하여 백업된 SQL Server 데이터베이스를 복원할 수 있습니다. 데이터베이스 복원은 모든 데이터와 로그 페이지를 지정된 SQL Server 백업에서 지정된 데이터베이스로 복사하는 다단계 프로세스입니다.

이 작업에 대해

- 백업된 SQL Server 데이터베이스를 백업이 생성된 동일한 호스트의 다른 SQL Server 인스턴스로 복원할 수 있습니다.

  SnapCenter를 사용하여 백업된 SQL Server 데이터베이스를 대체 경로로 복원하여 운영 버전을 교체하지 않을 수 있습니다.

- SnapCenter는 SQL Server 클러스터 그룹을 오프라인으로 전환하지 않고도 Windows 클러스터에서 데이터베이스를 복원할 수 있습니다.
- 복구 작업 중에 클러스터 장애(예: 리소스를 소유한 노드가 다운된 경우)가 발생하면 SQL Server 인스턴스에 다시 연결한 다음 복원 작업을 다시 시작해야 합니다.
- 사용자 또는 SQL Server 에이전트 작업이 데이터베이스에 액세스하는 경우에는 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 swagger에서 API:API/4.7/configsettings를 통해 표시할 수 있습니다

  Get API를 사용하여 키 값을 표시할 수 있습니다. API 설정은 지원되지 않습니다.

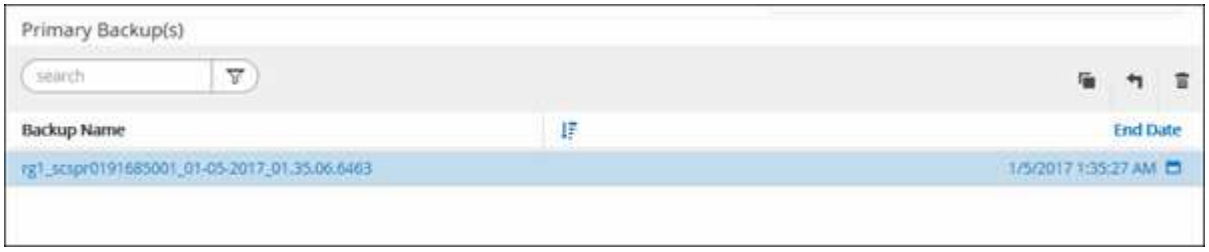
- 복원 마법사 페이지의 대부분의 필드는 설명이 필요 없습니다. 다음 정보는 지침이 필요한 필드에 대해 설명합니다.

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 데이터베이스 또는 리소스 그룹을 선택합니다.

   토폴로지 페이지가 표시됩니다.

4. Manage Copies 보기의 스토리지 시스템에서 * Backups * 를 선택합니다.
5. 테이블에서 백업을 선택한 다음 를 클릭합니다  아이콘을 클릭합니다.



6. 복원 범위 페이지에서 다음 옵션 중 하나를 선택합니다.

옵션을 선택합니다	설명
백업을 생성한 동일한 호스트에 데이터베이스를 복구합니다	백업을 수행한 동일한 SQL Server에 데이터베이스를 복원하려면 이 옵션을 선택합니다.

옵션을 선택합니다	설명
데이터베이스를 대체 호스트로 복구합니다	백업을 수행하는 동일한 호스트 또는 다른 호스트에 있는 다른 SQL Server로 데이터베이스를 복구하려는 경우 이 옵션을 선택합니다. 호스트 이름을 선택하고 데이터베이스 이름(선택 사항)을 입력한 다음 인스턴스를 선택하고 복구 경로를 지정합니다. 대체 경로에 제공된 파일 확장자는 원본 데이터베이스 파일의 파일 확장명과 동일해야 합니다. Restore Scope 페이지에 * Restore the database to an alternate host * 옵션이 표시되지 않으면 브라우저 캐시를 지웁니다.
기존 데이터베이스 파일을 사용하여 데이터베이스를 복원합니다	백업을 수행하는 동일한 호스트 또는 다른 호스트에 있는 대체 SQL Server로 데이터베이스를 복구하려는 경우 이 옵션을 선택합니다. 데이터베이스 파일은 지정된 기존 파일 경로에 이미 있어야 합니다. 호스트 이름을 선택하고 데이터베이스 이름(선택 사항)을 입력한 다음 인스턴스를 선택하고 복구 경로를 지정합니다.

7. 복구 범위 페이지에서 다음 옵션 중 하나를 선택합니다.

옵션을 선택합니다	설명
없음	로그 없이 전체 백업만 복원해야 하는 경우 * 없음 * 을 선택합니다.
모든 로그 백업	전체 백업 후 사용 가능한 모든 로그 백업을 복원하려면 * All log backups * up-to-the-minute backup restore operation(모든 로그 백업 * 최신 백업 복원 작업)을 선택합니다.
까지 로그 백업을 통해	Bby log backups * 를 선택하여 선택한 날짜의 백업 로그까지 백업 로그를 기반으로 데이터베이스를 복원하는 시점 복원 작업을 수행합니다.
특정 날짜 기준 종료	복원된 데이터베이스에 트랜잭션 로그가 적용되지 않는 날짜 및 시간을 지정하려면 특정 날짜별 * 를 선택합니다. 이 시점 복원 작업은 지정된 날짜 및 시간 이후에 기록된 트랜잭션 로그 항목의 복원을 중지합니다.

옵션을 선택합니다	설명
사용자 지정 로그 디렉터리를 사용합니다	모든 로그 백업 *, * 로그 백업 * 또는 * 특정 날짜별 * 을 선택하고 로그가 사용자 정의 위치에 있는 경우 * 사용자 정의 로그 디렉토리 사용 * 을 선택한 다음 로그 위치를 지정합니다. 사용자 정의 로그 디렉토리 사용 * 옵션은 * 대체 호스트로 데이터베이스 복원 * 또는 * 기존 데이터베이스 파일을 사용하여 데이터베이스 복원 * 을 선택한 경우에만 사용할 수 있습니다. 공유 경로를 사용할 수도 있지만 SQL 사용자가 경로에 액세스할 수 있는지 확인할 수도 있습니다. 사용자 지정 로그 디렉터리는 가용성 그룹 데이터베이스에서 지원되지 않습니다.

8. Pre Ops 페이지에서 다음 단계를 수행합니다.

   a. 복원 전 옵션 페이지에서 다음 옵션 중 하나를 선택합니다.

      - 같은 이름으로 데이터베이스를 복원하려면 * 복원 중에 같은 이름으로 데이터베이스 덮어쓰기 * 를 선택합니다.
      - 데이터베이스를 복원하고 기존 복제 설정을 유지하려면 * SQL 데이터베이스 복제 설정 유지 * 를 선택합니다.
      - 복원 작업을 시작하기 전에 트랜잭션 로그를 생성하려면 * 복원 전에 트랜잭션 로그 백업 생성 * 을 선택합니다.
      - 트랜잭션 로그 백업이 실패할 경우 복원 실패 * 전에 트랜잭션 로그 백업이 실패하면 복원 종료 * 를 선택하여 복원 작업을 중단합니다.

   b. 복구 작업을 수행하기 전에 실행할 선택적 스크립트를 지정합니다.

      예를 들어, 스크립트를 실행하여 SNMP 트랩을 업데이트하고, 경고를 자동화하고, 로그를 보내는 등의 작업을 수행할 수 있습니다.

      처방자 또는 사후 스크립트 경로에는 드라이브 또는 공유가 포함되어서는 안 됩니다. 경로는 scripts_path에 상대해야 합니다.

9. Post Ops 페이지에서 다음 단계를 수행하십시오.

   a. 복원 완료 후 데이터베이스 상태 선택 섹션에서 다음 옵션 중 하나를 선택합니다.

      - 지금 필요한 모든 백업을 복원하는 경우 * 운영, 추가 트랜잭션 로그를 복원할 수 없음 * 을 선택하십시오.

        이는 기본 동작으로, 커밋되지 않은 트랜잭션을 롤백하여 데이터베이스를 사용할 수 있도록 합니다. 백업을 생성할 때까지 추가 트랜잭션 로그를 복원할 수 없습니다.

      - 작동하지 않지만 추가 트랜잭션 로그를 복원하는 데 사용할 수 있음 * 을 선택하면 커밋되지 않은 트랜잭션을 롤백하지 않고 데이터베이스가 작동하지 않습니다.

추가 트랜잭션 로그를 복원할 수 있습니다. 데이터베이스가 복구될 때까지 데이터베이스를 사용할 수 없습니다.

- 데이터베이스를 읽기 전용 모드로 두려면 * 읽기 전용 모드, 추가 트랜잭션 로그 복구에 사용 가능 * 을 선택합니다.

  이 옵션은 커밋되지 않은 트랜잭션을 수행하지 않지만 복구 효과를 되돌릴 수 있도록 실행 취소된 작업을 대기 파일에 저장합니다.

Undo directory(디렉터리 실행 취소) 옵션이 활성화된 경우 더 많은 트랜잭션 로그가 복원됩니다. 트랜잭션 로그의 복원 작업이 실패한 경우 변경 내용을 롤백할 수 있습니다. 자세한 내용은 SQL Server 설명서를 참조하십시오.

b. 복구 작업을 수행한 후 실행할 선택적 스크립트를 지정합니다.

예를 들어, 스크립트를 실행하여 SNMP 트랩을 업데이트하고, 경고를 자동화하고, 로그를 보내는 등의 작업을 수행할 수 있습니다.

처방자 또는 사후 스크립트 경로에는 드라이브 또는 공유가 포함되어서는 안 됩니다. 경로는 scripts_path에 상대해야 합니다.

10. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

    또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다.

11. 요약을 검토하고 * Finish * 를 클릭합니다.
12. 모니터 * > * 작업 * 페이지를 사용하여 복원 프로세스를 모니터링합니다.

관련 정보

"PowerShell cmdlet을 사용하여 리소스 복원 및 복구"

"보조 스토리지에서 SQL Server 데이터베이스를 복구합니다"

보조 스토리지에서 **SQL Server** 데이터베이스를 복구합니다

보조 스토리지 시스템의 물리적 LUN(RDM, iSCSI 또는 FCP)에서 백업된 SQL Server 데이터베이스를 복원할 수 있습니다. 복구 기능은 보조 스토리지 시스템에 상주하는 지정된 SQL Server 백업에서 지정된 데이터베이스로 모든 데이터와 로그 페이지를 복사하는 다중 위상 프로세스입니다.

시작하기 전에

- 1차 스토리지 시스템에서 2차 스토리지 시스템으로 스냅샷 복사본을 복제해야 합니다.
- SnapCenter 서버와 플러그인 호스트가 보조 스토리지 시스템에 접속할 수 있는지 확인해야 합니다.
- 복원 마법사 페이지의 대부분의 필드는 기본 복원 프로세스에 설명되어 있습니다. 다음 정보는 지침이 필요한 일부 필드에 대해 설명합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 * SnapCenter Plug-in for SQL Server * 를 선택합니다.

2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 * 데이터베이스 * 또는 * 리소스 그룹 * 을 선택합니다.
3. 데이터베이스 또는 리소스 그룹을 선택합니다.

   데이터베이스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 섹션에서 보조 스토리지 시스템(미러링 또는 볼트)에서 * 백업 * 을 선택합니다.
5. 목록에서 백업을 선택한 다음 을 클릭합니다  .
6. 위치 페이지에서 선택한 리소스를 복원할 대상 볼륨을 선택합니다.
7. 복원 마법사를 완료하고 요약을 검토한 다음 * 마침 * 을 클릭합니다.

데이터베이스를 다른 데이터베이스에서 공유하는 다른 경로로 복원한 경우 전체 백업 및 백업 검증을 수행하여 복구된 데이터베이스에 물리적 레벨의 손상이 없는지 확인해야 합니다.

가용성 그룹 데이터베이스를 다시 시딩합니다

다시 시딩은 AG(Availability Group) 데이터베이스를 복원하는 옵션입니다. 보조 데이터베이스가 AG의 기본 데이터베이스와 동기화되지 않으면 보조 데이터베이스를 다시 시드할 수 있습니다.

시작하기 전에

- 복원할 보조 AG 데이터베이스의 백업을 만들어야 합니다.
- SnapCenter 서버와 플러그인 호스트의 SnapCenter 버전이 동일해야 합니다.

이 작업에 대해

- 운영 데이터베이스에서 재시딩된 작업은 수행할 수 없습니다.
- 복제본 데이터베이스가 가용성 그룹에서 제거된 경우에는 다시 시드 작업을 수행할 수 없습니다. 복제본이 제거되면 재시딩이 실패합니다.
- SQL 가용성 그룹 데이터베이스에서 다시 시딩된 작업을 실행하는 동안 해당 가용성 그룹 데이터베이스의 복제본 데이터베이스에서 로그 백업을 트리거하지 않아야 합니다. 다시 시딩된 작업 중에 로그 백업을 트리거하면 미러 데이터베이스, "database_name"에 트랜잭션 로그 데이터가 부족하여 기본 데이터베이스 오류 메시지의 로그 백업 체인을 보존할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 * SnapCenter Plug-in for SQL Server * 를 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 데이터베이스 * 를 선택합니다.
3. 목록에서 Secondary AG 데이터베이스를 선택합니다.
4. 다시 시딩된 * 을 클릭합니다.
5. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

PowerShell cmdlet을 사용하여 리소스 복원

리소스 백업 복원에는 SnapCenter 서버와의 연결 세션 시작, 백업 목록 표시 및 백업 정보 검색, 백업 복구가 포함됩니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

   이 예에서는 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 예는 2015년 1월 29일부터 2015년 2월 3일까지 백업에 대한 자세한 정보를 표시합니다.

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"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.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.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 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

SQL 리소스 복구 작업을 모니터링합니다

작업 페이지를 사용하여 여러 SnapCenter 복원 작업의 진행률을 모니터링할 수 있습니다. 작업 진행률을 확인하여 작업이 언제 완료되는지 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

복원 후 상태는 복원 작업 후 리소스의 상태와 수행할 수 있는 추가 복원 작업에 대해 설명합니다.

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다

- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨

단계

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 모니터 * 페이지에서 * 작업 * 을 클릭합니다.
3. Jobs * 페이지에서 다음 단계를 수행하십시오.
   a. 을 클릭합니다 복원 작업만 나열되도록 목록을 필터링하려면
   b. 시작 및 종료 날짜를 지정합니다.
   c. Type * 드롭다운 목록에서 * Restore * 를 선택합니다.
   d. Status * (상태 *) 드롭다운 목록에서 복원 상태를 선택합니다.
   e. 성공적으로 완료된 작업을 보려면 * 적용 * 을 클릭합니다.
4. 복원 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. Job Details * 페이지에서 * View logs * 를 클릭합니다.

   로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

볼륨 기반 복원 작업 후에는 백업 메타데이터가 SnapCenter 저장소에서 삭제되지만 백업 카탈로그 항목은 SAP HANA 카탈로그에 남아 있습니다. 복원 작업 상태가 표시됩니다 작업 세부 정보를 클릭하여 일부 하위 작업의 경고 표시를 확인해야 합니다. 경고 표지를 클릭하고 표시된 백업 카탈로그 항목을 삭제합니다.

SQL 리소스 복원 작업을 취소합니다

대기열에 있는 복원 작업을 취소할 수 있습니다.

복원 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

이 작업에 대해

- Monitor* 페이지 또는 * Activity* 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 작업에는 * 작업 취소 * 버튼이 비활성화됩니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 사용자\그룹 페이지의 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.

시작...	조치
모니터 페이지	1. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 클릭합니다. 2. 작업을 선택하고 * 작업 취소 * 를 클릭합니다.
작업 창	1. 복원 작업을 시작한 후 을 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다. 2. 작업을 선택합니다. 3. 작업 세부 정보 페이지에서 * 작업 취소 * 를 클릭합니다.

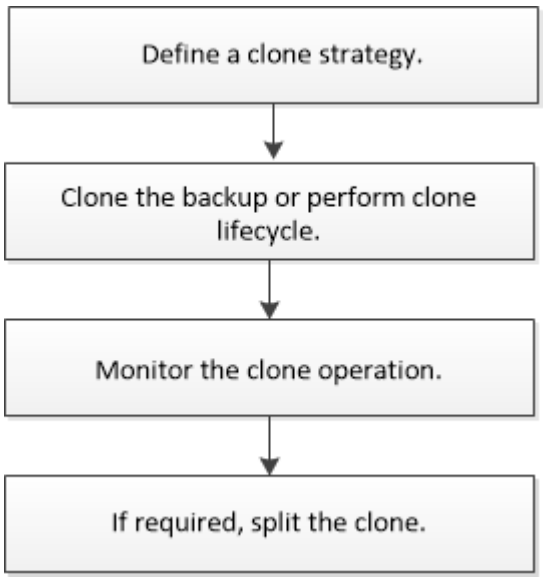
SQL Server 데이터베이스 리소스의 클론을 생성합니다

클론 복제 워크플로우

백업에서 데이터베이스 리소스를 클론 복제하기 전에 SnapCenter Server를 사용하여 몇 가지 작업을 수행해야 합니다. 데이터베이스 클론 복제는 운영 데이터베이스 또는 해당 백업 세트의 시점 복사본을 생성하는 프로세스입니다. 응용 프로그램 개발 주기 동안 현재 데이터베이스 구조 및 콘텐츠를 사용하여 구현해야 하는 기능을 테스트하거나 데이터 웨어하우스를 채울 때 데이터 추출 및 조작 도구를 사용하거나 실수로 삭제 또는 변경된 데이터를 복구하기 위해 데이터베이스를 복제할 수 있습니다.

데이터베이스 클론 생성 작업은 작업 ID를 기반으로 보고서를 생성합니다.

다음 워크플로에서는 클론 생성 작업을 수행해야 하는 순서를 보여 줍니다.



PowerShell cmdlet을 수동으로 또는 스크립트에서 사용하여 백업, 복원, 복구, 확인 및 클론 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드"

- 자세한 정보 찾기 *

"SQL Server 데이터베이스 백업에서 복제합니다"

"클론 수명주기 수행"

"클론 작업이 실패하거나 기본 TCP_TIMEOUT 값으로 완료하는 데 시간이 더 오래 걸릴 수 있습니다"

SQL Server 데이터베이스 백업에서 복제합니다

SnapCenter를 사용하여 SQL Server 데이터베이스 백업을 복제할 수 있습니다. 이전 버전의 데이터에 액세스하거나 복원하려는 경우 필요에 따라 데이터베이스 백업을 클론 복제할 수 있습니다.

시작하기 전에

- 호스트 추가, 리소스 식별 및 스토리지 시스템 접속 생성과 같은 작업을 완료하여 데이터 보호를 준비할 수 있어야 합니다.
- 데이터베이스 또는 리소스 그룹을 백업해야 합니다.
- 데이터 LUN 및 로그 LUN의 미러, 볼트 또는 미러 볼트 같은 보호 유형은 로그 백업을 사용하여 대체 호스트에 클론 생성 시 보조 로케이터를 검색하는 데 동일해야 합니다.
- SnapCenter 클론 작업 중에 마운트된 클론 드라이브를 찾을 수 없는 경우 SnapCenter 서버의 CloneRetryTimeout 매개 변수를 300으로 변경해야 합니다.
- 볼륨을 호스팅하는 애그리게이트는 SVM(스토리지 가상 머신)의 할당된 애그리게이트 목록에 있어야 합니다.

이 작업에 대해

- 독립 실행형 데이터베이스 인스턴스에 클론을 생성하는 동안 마운트 지점 경로가 있고 전용 디스크인지 확인합니다.
- FCI(장애 조치 클러스터 인스턴스)에 클론을 생성하는 동안 마운트 지점이 존재하고, 공유 디스크이며, 경로와 FCI가 동일한 SQL 리소스 그룹에 속해야 합니다.
- 각 호스트에 하나의 VFC 또는 FC 이니시에이터만 연결되어 있는지 확인합니다. 이는 SnapCenter가 호스트당 하나의 이니시에이터만 지원하기 때문입니다.
- 소스 데이터베이스 또는 타겟 인스턴스가 클러스터 공유 볼륨(CSV)에 있으면 복제된 데이터베이스가 CSV에 있게 됩니다.
- 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 swagger에서 API:API/4.7/configsettings를 통해 표시할 수 있습니다

  Get API를 사용하여 키 값을 표시할 수 있습니다. API 설정은 지원되지 않습니다.

가상 환경(VMDK/RDM)의 경우 마운트 지점이 전용 디스크인지 확인합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 선택한 다음 목록에서 * SnapCenter Plug-in for SQL Server * 를 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 데이터베이스 * 또는 * 리소스 그룹 * 을 선택합니다.

   인스턴스 백업 클론 생성은 지원되지 않습니다.

3. 데이터베이스 또는 리소스 그룹을 선택합니다.
4. Manage Copies * (복사본 관리 *) 보기 페이지에서 기본 또는 보조(미러링 또는 보관된) 스토리지 시스템에서 백업을 선택합니다.
5. 백업을 선택한 다음 * 를 선택합니다 *.
6. 클론 옵션 * 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
클론 서버	클론을 생성할 호스트를 선택합니다.
클론 인스턴스	데이터베이스 백업을 복제할 클론 인스턴스를 선택합니다. 이 SQL 인스턴스는 지정된 클론 서버에 있어야 합니다.
접미사 복제	클론 파일 이름에 추가될 접미사를 입력하여 데이터베이스가 클론임을 나타냅니다. 예: *db1_clone*. 원본 데이터베이스와 같은 위치에 클론을 생성하는 경우 복제된 데이터베이스를 원본 데이터베이스와 구분할 수 있도록 접미사를 제공해야 합니다. 그렇지 않으면 작업이 실패합니다.
마운트 지점을 자동으로 할당하거나 경로 아래에 볼륨 마운트 지점을 자동으로 할당합니다	경로 아래에 마운트 지점을 자동으로 할당할지, 볼륨 마운트 지점을 자동으로 할당할지 여부를 선택합니다. 경로 아래의 볼륨 마운트 지점 자동 할당: 경로 아래의 마운트 지점을 사용하여 특정 디렉토리를 제공할 수 있습니다. 마운트 지점은 해당 디렉토리 내에 생성됩니다. 이 옵션을 선택하기 전에 디렉토리가 비어 있는지 확인해야 합니다. 디렉토리에 데이터베이스가 있으면 마운트 작업 후 데이터베이스가 잘못된 상태가 됩니다.

7. 로그 페이지에서 다음 옵션 중 하나를 선택합니다.

이 필드의 내용...	수행할 작업...
없음	로그 없이 전체 백업만 클론하려면 이 옵션을 선택합니다.

이 필드의 내용...	수행할 작업...
모든 로그 백업	전체 백업 이후에 사용 가능한 모든 로그 백업을 클론하려면 이 옵션을 선택합니다.
까지 로그 백업을 통해	선택한 날짜를 사용하여 백업 로그까지 생성된 백업 로그를 기반으로 데이터베이스를 복제하려면 이 옵션을 선택합니다.
특정 날짜 기준 종료	트랜잭션 로그가 복제된 데이터베이스에 적용되지 않는 날짜 및 시간을 지정합니다. 이 시점 클론은 지정된 날짜 및 시간 이후에 기록된 트랜잭션 로그 항목의 클론을 중단합니다.

8. Script * 페이지에서 각각 클론 작업 전후에 실행해야 하는 ppt 또는 postscript의 스크립트 시간 제한, 경로 및 인수를 입력합니다.

   예를 들어, 스크립트를 실행하여 SNMP 트랩을 업데이트하고, 경고를 자동화하고, 로그를 보내는 등의 작업을 수행할 수 있습니다.

   > 처방자 또는 사후 스크립트 경로에는 드라이브 또는 공유가 포함되어서는 안 됩니다. 경로는 scripts_path에 상대해야 합니다.

   기본 스크립트 시간 초과는 60초입니다.

9. 알림 * 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 수행된 클론 작업의 보고서를 첨부하려면 * 작업 보고서 연결 * 을 선택합니다.

   > 이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmtpServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

   EMS의 경우 를 참조할 수 있습니다 "EMS Data 수집 관리"

10. 요약을 검토한 후 * Finish * 를 선택합니다.
11. Monitor * > * Jobs * 를 선택하여 작업 진행 상황을 모니터링합니다.

작업을 마친 후

클론이 생성된 후에는 이름을 바꿀 수 없습니다.

관련 정보

"SQL Server 데이터베이스, 인스턴스 또는 가용성 그룹을 백업합니다"

"PowerShell cmdlet을 사용하여 백업 클론 생성"

"클론 작업이 실패하거나 기본 TCP_TIMEOUT 값으로 완료하는 데 시간이 더 오래 걸릴 수 있습니다"

"장애 조치 클러스터 인스턴스 데이터베이스 클론에 장애가 발생합니다"

PowerShell cmdlet을 사용하여 백업 클론 생성

클론 워크플로우에는 계획, 클론 작업 수행 및 작업 모니터링이 포함됩니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Get-SmBackup 또는 Get-SmResourceGroup cmdlet을 사용하여 클론을 생성할 수 있는 백업을 나열합니다.

   이 예에서는 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     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

   이 예제에서는 지정된 리소스 그룹, 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 클론 작업을 시작합니다.

   이 예에서는 모든 로그를 사용하여 지정된 백업에서 클론을 생성합니다.

```
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 클론을 생성합니다.

```
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 클론 작업의 상태를 봅니다.

   이 예에서는 지정된 작업 ID에 대한 클론 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 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

클론 수명주기 수행

SnapCenter를 사용하면 리소스 그룹 또는 데이터베이스에서 클론을 생성할 수 있습니다. 필요 시 클론을 수행하거나 리소스 그룹 또는 데이터베이스의 반복적인 클론 작업을 예약할 수 있습니다. 주기적으로 백업을 클론하는 경우 클론을 사용하여 애플리케이션을 개발하거나 데이터를 채우거나 데이터를 복구할 수 있습니다.

SnapCenter를 사용하면 여러 서버에서 동시에 여러 클론 작업을 실행하도록 예약할 수 있습니다.

시작하기 전에

- 독립 실행형 데이터베이스 인스턴스에 클론을 생성하는 동안 마운트 지점 경로가 있고 전용 디스크인지 확인합니다.
- FCI(장애 조치 클러스터 인스턴스)에 클론을 생성하는 동안 마운트 지점이 존재하고, 공유 디스크이며, 경로와 FCI가 동일한 SQL 리소스 그룹에 속해야 합니다.
- 소스 데이터베이스 또는 타겟 인스턴스가 클러스터 공유 볼륨(CSV)에 있으면 복제된 데이터베이스가 CSV에 있게 됩니다.

가상 환경(VMDK/RDM)의 경우 마운트 지점이 전용 디스크인지 확인합니다.

이 작업에 대해

- 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 swagger에서 API:API/4.7/configsettings를 통해 표시할 수 있습니다

Get API를 사용하여 키 값을 표시할 수 있습니다. API 설정은 지원되지 않습니다.

- 클론 수명주기 마법사 페이지의 대부분의 필드는 별도의 설명이 필요 없습니다. 다음 정보는 지침이 필요한 필드에 대해 설명합니다.

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. 리소스 그룹 또는 데이터베이스를 선택한 다음 * Clone Lifecycle * 을 클릭합니다.
4. 옵션 페이지에서 다음 작업을 수행합니다.

이 필드의 내용…	수행할 작업…
클론 작업 이름입니다	클론 라이프사이클 작업을 모니터링하고 수정하는 데 도움이 되는 클론 라이프사이클 작업 이름을 지정합니다.
클론 서버	클론을 배치할 호스트를 선택합니다.
클론 인스턴스	데이터베이스를 복제할 클론 인스턴스를 선택합니다. 이 SQL 인스턴스는 지정된 클론 서버에 있어야 합니다.
접미사 복제	클론 데이터베이스에 추가될 접미사를 입력하여 해당 접미사가 클론임을 나타냅니다. 클론 리소스 그룹을 생성하는 데 사용되는 각 SQL 인스턴스에는 고유한 데이터베이스 이름이 있어야 합니다. 예를 들어, 클론 리소스 그룹에 SQL 인스턴스 인스턴스 인스턴스 "inst1"의 소스 데이터베이스 "dB1"이 포함되어 있고 "dB1"이 "inst1"로 복제되는 경우 클론 데이터베이스 이름은 "dB1*clone*"이어야 합니다. "clone""은 데이터베이스가 동일한 인스턴스에 복제되기 때문에 필수 사용자 정의 접미부입니다. "dB1"이 SQL 인스턴스 "inst2"에 복제되면 데이터베이스가 다른 인스턴스로 복제되므로 클론 데이터베이스 이름은 "dB1"(접미사는 선택 사항)으로 유지될 수 있습니다.

이 필드의 내용...	수행할 작업...
마운트 지점을 자동으로 할당하거나 경로 아래에 볼륨 마운트 지점을 자동으로 할당합니다	경로 아래에 마운트 지점 또는 볼륨 마운트 지점을 자동으로 할당할지 여부를 선택합니다. 경로 아래에 있는 볼륨 마운트 지점을 자동 할당하도록 선택하면 특정 디렉토리를 제공할 수 있습니다. 마운트 지점은 해당 디렉토리 내에 생성됩니다. 이 옵션을 선택하기 전에 디렉토리가 비어 있는지 확인해야 합니다. 디렉토리에 데이터베이스가 있으면 마운트 작업 후 데이터베이스가 잘못된 상태가 됩니다.

5. Location 페이지에서 클론을 생성할 스토리지 위치를 선택합니다.
6. 스크립트 페이지에서 복제 작업 전후에 실행해야 하는 처방인 또는 PS의 경로와 인수를 각각 입력합니다.

   예를 들어, 스크립트를 실행하여 SNMP 트랩을 업데이트하고, 경고를 자동화하고, 로그를 보내는 등의 작업을 수행할 수 있습니다.

   > 처방자 또는 사후 스크립트 경로에는 드라이브 또는 공유가 포함되어서는 안 됩니다. 경로는 scripts_path에 상대해야 합니다.

   기본 스크립트 시간 초과는 60초입니다.

7. 스케줄 페이지에서 다음 작업 중 하나를 수행합니다.
   - 클론 작업을 즉시 실행하려면 * 지금 실행 * 을 선택합니다.
   - 클론 작업이 수행되는 빈도, 클론 스케줄이 시작되는 시간, 클론 작업이 발생하는 날짜, 스케줄이 만료되는 날짜 및 스케줄이 만료된 후에 클론을 삭제해야 하는지 여부를 결정하려면 * Configure schedule * 을 선택합니다.
8. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 수행된 클론 작업의 보고서를 첨부하려면 * 작업 보고서 연결 * 을 선택합니다.

   > 이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmtpServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

   EMS의 경우 를 참조할 수 있습니다 "EMS Data 수집 관리"

9. 요약을 검토하고 * Finish * 를 클릭합니다.

모니터 * > * 작업 * 페이지를 사용하여 복제 프로세스를 모니터링해야 합니다.

SQL 데이터베이스 클론 작업을 모니터링합니다

작업 페이지를 사용하여 SnapCenter 클론 작업의 진행률을 모니터링할 수 있습니다. 작업 진행률을 확인하여 작업이 언제 완료되는지 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨
- 단계 *
  1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
  2. 모니터 * 페이지에서 * 작업 * 을 클릭합니다.
  3. Jobs * 페이지에서 다음 단계를 수행하십시오.
     a. 을 클릭합니다 클론 작업만 나열되도록 목록을 필터링합니다.
     b. 시작 및 종료 날짜를 지정합니다.
     c. Type * 드롭다운 목록에서 * Clone * 을 선택합니다.
     d. Status * (상태 *) 드롭다운 목록에서 클론 상태를 선택합니다.
     e. 성공적으로 완료된 작업을 보려면 * 적용 * 을 클릭합니다.
  4. 클론 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
  5. 작업 세부 정보 페이지에서 * 로그 보기 * 를 클릭합니다.

SQL 리소스 클론 작업을 취소합니다

대기열에 있는 클론 작업을 취소할 수 있습니다.

클론 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

이 작업에 대해

- Monitor * 페이지 또는 * Activity * 창에서 대기 중인 클론 작업을 취소할 수 있습니다.
- 실행 중인 클론 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 대기 중인 클론 작업을 취소할 수 있습니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 다른 구성원 개체 * 를 볼 수 있고 사용자\그룹 페이지에서 작동할 수 있는 경우 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 클론 작업을 취소할 수 있습니다.

단계

다음 작업 중 하나를 수행합니다.

시작...	조치
모니터 페이지	1. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 클릭합니다. 2. 작업을 선택하고 * 작업 취소 * 를 클릭합니다.

시작...	조치
작업 창	1. 클론 작업을 시작한 후 을 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다. 2. 작업을 선택합니다. 3. 작업 세부 정보 * 페이지에서 * 작업 취소 * 를 클릭합니다.

클론 분할

SnapCenter를 사용하여 상위 리소스에서 복제된 리소스를 분할할 수 있습니다. 분할되는 클론은 상위 리소스와 독립적입니다.

이 작업에 대해

- 중간 클론에는 클론 분할 작업을 수행할 수 없습니다.

  예를 들어 데이터베이스 백업에서 clone1을 생성한 후 clone1의 백업을 생성한 다음 이 백업(clone2)을 클론 복제할 수 있습니다. clone2를 생성한 후에는 clone1이 중간 클론이며 clone1에서 클론 분할 작업을 수행할 수 없습니다. 그러나 clone2에서 클론 분할 작업을 수행할 수 있습니다.

  clone2를 분할한 후에는 clone1이 더 이상 중간 클론이 아니기 때문에 clone1에서 클론 분할 작업을 수행할 수 있습니다.

- 클론을 분할하면 클론의 백업 복사본 및 클론 작업이 삭제됩니다.
- 클론 분할 작업 제한에 대한 자세한 내용은 을 참조하십시오 "ONTAP 9 논리적 스토리지 관리 가이드".
- 스토리지 시스템의 볼륨 또는 애그리게이트는 온라인 상태인지 확인합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. Resources * 페이지의 View 목록에서 적절한 옵션을 선택합니다.

옵션을 선택합니다	설명
성능을 대폭 향상	보기 목록에서 * 데이터베이스 * 를 선택합니다.
파일 시스템의 경우	보기 목록에서 * 경로 * 를 선택합니다.

3. 목록에서 적절한 리소스를 선택합니다.

   리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 * 보기에서 복제된 리소스(예: 데이터베이스 또는 LUN)를 선택한 다음 * 를 클릭합니다 *.
5. 분할할 클론의 예상 크기와 애그리게이트에서 사용할 수 있는 필수 공간을 검토한 다음 * 시작 * 을 클릭합니다.
6. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

SMCore 서비스가 다시 시작되면 클론 분할 작업이 응답하지 않습니다. Stop-SmJob cmdlet을 실행하여 클론 분할 작업을 중지한 다음 클론 분할 작업을 다시 시도해야 합니다.

폴링 시간을 더 오래 설정하거나 폴링 시간을 짧게 하여 클론이 분할되었는지 여부를 확인하려면 _SMCoreServiceHost.exe.config_file에서 _CloneSplitStatusCheckPollTime_parameter 값을 변경하여 SMCore가 클론 분할 작업의 상태를 폴링할 시간 간격을 설정할 수 있습니다. 값은 밀리초이고 기본값은 5분입니다.

예를 들면 다음과 같습니다.

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

백업, 복원 또는 다른 클론 분할이 진행 중인 경우 클론 분할 시작 작업이 실패합니다. 실행 중인 작업이 완료된 후에만 클론 분할 작업을 다시 시작해야 합니다.

관련 정보

"Aggregate가 존재하지 않으면 SnapCenter 클론 또는 검증에 실패합니다"

SAP HANA 데이터베이스 보호

SAP HANA 데이터베이스용 SnapCenter 플러그인

SAP HANA 데이터베이스용 SnapCenter 플러그인 개요

SAP HANA 데이터베이스용 SnapCenter 플러그인은 SAP HANA 데이터베이스의 애플리케이션 인식 데이터 보호 관리를 지원하는 NetApp SnapCenter 소프트웨어의 호스트 측 구성 요소입니다. SAP HANA 데이터베이스용 플러그인은 SnapCenter 환경에서 SAP HANA 데이터베이스의 백업, 복원 및 클론 복제를 자동화합니다.

SnapCenter는 단일 컨테이너 및 MDC(멀티테넌트 데이터베이스 컨테이너)를 지원합니다. Windows 및 Linux 환경 모두에서 SAP HANA 데이터베이스용 플러그인을 사용할 수 있습니다. HANA 데이터베이스 호스트에 설치되어 있지 않은 플러그인을 중앙 집중식 호스트 플러그인이라고 합니다. 중앙 집중식 호스트 플러그인을 사용하면 다양한 호스트에 걸쳐 여러 HANA 데이터베이스를 관리할 수 있습니다.

SAP HANA 데이터베이스용 플러그인이 설치되어 있는 경우 SnapCenter와 NetApp SnapMirror 기술을 함께 사용하여 다른 볼륨에 백업 세트의 미러링 복사본을 생성할 수 있습니다. 또한 NetApp SnapVault 기술의 플러그인을 사용하여 표준 준수를 위한 D2D 백업 복제를 수행할 수 있습니다.

SAP HANA 데이터베이스용 SnapCenter 플러그인을 사용하여 수행할 수 있는 작업

귀사 환경에 SAP HANA 데이터베이스용 플러그인을 설치하면 SnapCenter를 사용하여 SAP HANA 데이터베이스와 관련 리소스를 백업, 복원 및 클론 복제할 수 있습니다. 이러한 작업을 지원하는 작업을 수행할 수도 있습니다.

- 데이터베이스를 추가합니다.
- 백업을 생성합니다.
- 백업에서 복원합니다.
- 클론 백업.
- 백업 작업을 예약합니다.
- 백업, 복원 및 클론 작업을 모니터링합니다.
- 백업, 복원 및 클론 작업에 대한 보고서를 봅니다.

SAP HANA 데이터베이스용 SnapCenter 플러그인 기능

SnapCenter는 플러그인 애플리케이션 및 스토리지 시스템의 NetApp 기술과 통합됩니다. SAP HANA 데이터베이스용 플러그인과 함께 사용하려면 SnapCenter 그래픽 사용자 인터페이스를 사용해야 합니다.

- * 통합 그래픽 사용자 인터페이스 *

  SnapCenter 인터페이스는 플러그인과 환경 전반에서 표준화와 일관성을 제공합니다. SnapCenter 인터페이스를 사용하면 플러그인 전반에서 일관된 백업, 복원, 클론 복제 작업을 완료하고, 중앙 집중식 보고, 대시보드 뷰를 사용하고, RBAC(역할 기반 액세스 제어)를 설정하고, 모든 플러그인에 걸쳐 작업을 모니터링할 수 있습니다.

- * 자동화된 중앙 관리 *

  백업 작업을 예약하고, 정책 기반 백업 보존을 구성하고, 복구 작업을 수행할 수 있습니다. 또한 SnapCenter에서 이메일 경고를 보내도록 구성하여 환경을 사전에 모니터링할 수도 있습니다.

- * 무중단 NetApp 스냅샷 복사본 기술 *

  SnapCenter은 SAP HANA 데이터베이스용 플러그인과 NetApp 스냅샷 복사본 기술을 사용하여 리소스를 백업합니다.

또한 SAP HANA 데이터베이스용 플러그인을 사용하면 다음과 같은 이점을 얻을 수 있습니다.

- 백업, 복원 및 클론 워크플로우 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임

  권한이 있는 SnapCenter 사용자가 응용 프로그램 수준 권한을 갖도록 자격 증명을 설정할 수도 있습니다.

- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 공간 효율적인 특정 시점 리소스 복사본 생성

  클론을 생성하려는 스토리지 시스템에는 FlexClone 라이센스가 필요합니다.

- 백업을 생성하는 과정에서 ONTAP의 일관성 그룹(CG) 스냅샷 복사본 기능이 지원됩니다.
- 여러 리소스 호스트에서 동시에 여러 백업을 실행할 수 있습니다

  단일 호스트에서 단일 호스트의 리소스가 동일한 볼륨을 공유할 경우 스냅샷 복사본이 통합됩니다.

- 외부 명령을 사용하여 스냅샷 복사본을 생성하는 기능
- 파일 기반 백업 지원:
- XFS 파일 시스템에서 Linux LVM 지원

SAP HANA 데이터베이스용 **SnapCenter** 플러그인이 지원하는 스토리지 유형입니다

SnapCenter는 물리적 시스템과 가상 머신(VM) 모두에서 다양한 스토리지 유형을 지원합니다. SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치하기 전에 스토리지 유형에 대한 지원을 확인해야 합니다.

기계	스토리지 유형입니다
물리적 서버와 가상 서버	FC 연결 LUN
물리적 서버	iSCSI로 연결된 LUN
물리적 서버와 가상 서버	NFS 연결 볼륨

SAP HANA 플러그인에 필요한 최소 **ONTAP** 권한

필요한 최소 ONTAP 권한은 데이터 보호를 위해 사용 중인 SnapCenter 플러그인에 따라

다릅니다.

- All-access 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
  - event generate-autosupport-log입니다
  - 작업 기록이 표시됩니다
  - 작업 중지
  - LUN을 클릭합니다
  - LUN 생성
  - LUN 생성
  - LUN 생성
  - LUN을 삭제합니다
  - LUN igroup 추가
  - LUN igroup 작성
  - LUN igroup 삭제
  - LUN igroup의 이름을 바꿉니다
  - LUN igroup의 이름을 바꿉니다
  - LUN igroup 표시
  - LUN 매핑 add-reporting-nodes입니다
  - LUN 매핑 생성
  - LUN 매핑을 삭제합니다
  - LUN 매핑으로 remove-reporting-nodes를 사용할 수 있습니다
  - LUN 매핑이 표시됩니다
  - LUN 수정
  - LUN 이동 - 볼륨
  - LUN이 오프라인 상태입니다
  - LUN을 온라인 상태로 전환합니다
  - LUN persistent - 예약 지우기
  - LUN 크기 조정
  - LUN 일련 번호입니다
  - LUN 표시
  - SnapMirror 정책 추가 규칙
  - SnapMirror 정책 modify-rule을 참조하십시오
  - SnapMirror 정책 remove-rule을 참조하십시오
  - SnapMirror 정책 쇼
  - SnapMirror 복원

- SnapMirror 쇼
- SnapMirror 기록
- SnapMirror 업데이트
- SnapMirror 업데이트 - ls -set
- SnapMirror 목록 - 대상
- 버전
- 볼륨 클론 생성
- 볼륨 클론 표시
- 볼륨 클론 분할 시작이 있습니다
- 볼륨 클론 분할 중지
- 볼륨 생성
- 볼륨 제거
- 볼륨 파일 클론 생성
- 볼륨 파일 show-disk-usage 를 참조하십시오
- 볼륨이 오프라인 상태입니다
- 볼륨을 온라인으로 설정합니다
- 볼륨 수정
- 볼륨 qtree 생성
- 볼륨 qtree 삭제
- 볼륨 qtree 수정
- 볼륨 qtree 표시
- 볼륨 제한
- 볼륨 표시
- 볼륨 스냅샷 생성
- 볼륨 스냅숏 삭제
- 볼륨 스냅숏 수정
- 볼륨 스냅숏 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 - 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- SVM CIFS를 선택합니다
- SVM CIFS 공유 생성
- SVM CIFS 공유 삭제

- SVM CIFS shadowcopy show 를 참조하십시오
- SVM CIFS 공유 표시
- vserver cifs show 를 참조하십시오
- SVM 엑스포트 - 정책
- SVM 엑스포트 정책 생성
- SVM 엑스포트 정책 삭제
- SVM 엑스포트 정책 규칙 생성
- vserver export-policy rule show를 참조하십시오
- vserver export-policy show를 참조하십시오
- SVM iSCSI
- SVM iSCSI 연결이 표시됩니다
- vserver show 를 참조하십시오

- 읽기 전용 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
  - 네트워크 인터페이스
  - 네트워크 인터페이스가 표시됩니다
  - SVM

SAP HANA 데이터베이스용 **SnapMirror** 및 **SnapVault** 복제를 위한 스토리지 시스템을 준비하십시오

ONTAP 플러그인을 SnapCenter SnapMirror 기술과 함께 사용하여 다른 볼륨에 백업 세트의 미러링 복사본을 만들고 ONTAP SnapVault 기술을 사용하여 표준 준수 및 기타 거버넌스 관련 용도로 D2D 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 타겟 볼륨 간의 데이터 보호 관계를 구성하고 관계를 초기화해야 합니다.

SnapCenter는 스냅샷 복사본 작업이 완료된 후 SnapMirror 및 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행되고, 별도의 ONTAP 일정을 만들지 않습니다.

NetApp SnapManager 제품에서 SnapCenter으로 오고 있으며 구성한 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 운영 스토리지(소스 볼륨)의 데이터를 보조 스토리지(타겟 볼륨)에 복제합니다. 관계를 초기화할 때 ONTAP은 소스 볼륨에서 참조된 데이터 블록을 대상 볼륨으로 전송합니다.

SnapCenter는 SnapMirror와 SnapVault 볼륨(* Primary * > * Mirror * > * Vault *) 간의 계단식 관계를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter는 버전에 상관없이 유연한 SnapMirror 관계의 관리를 지원합니다. 버전에 상관없이 유연한 SnapMirror 관계와 설정 방법에 대한 자세한 내용은 를 참조하십시오 "ONTAP 설명서".

SnapCenter는 * SYNC_MIRROR * 복제를 지원하지 않습니다.

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 만들 수 있습니다. SLA(서비스 수준 계약), RTO(복구 시간 목표) 및 RPO(복구 시점 목표)에 따라 백업 전략이 주로 결정됩니다.

이 작업에 대해

SLA는 예상되는 서비스 수준을 정의하고 서비스의 가용성 및 성능을 비롯한 다양한 서비스 관련 문제를 해결합니다. RTO는 서비스 중단 후 비즈니스 프로세스를 복원해야 하는 시간입니다. RPO는 장애 후 정상적인 작업을 재개하기 위해 백업 스토리지에서 복구해야 하는 파일의 사용 기간에 대한 전략을 정의합니다. SLA, RTO 및 RPO는 데이터 보호 전략에 기여합니다.

단계

1. 자원을 언제 백업해야 하는지 결정합니다.
2. 필요한 백업 작업 수를 결정합니다.
3. 백업 이름을 지정하는 방법을 결정합니다.
4. 스냅샷 복사본 기반 정책을 생성하여 데이터베이스의 애플리케이션 정합성을 보장하는 스냅샷 복사본을 백업할지 결정합니다.
5. 데이터베이스의 무결성을 검증할지 여부를 결정합니다.
6. 복제에 NetApp SnapMirror 기술을 사용할지, 장기간 보존에 NetApp SnapVault 기술을 사용할지 여부를 결정합니다.
7. 소스 스토리지 시스템과 SnapMirror 대상에 있는 스냅샷 복사본의 보존 기간을 결정합니다.
8. 백업 작업 전후에 명령을 실행할지 여부를 결정하고 처방이나 PS를 제공합니다.

Linux 호스트에서 리소스 자동 검색

리소스는 SnapCenter에서 관리하는 Linux 호스트의 SAP HANA 데이터베이스 및 비 데이터 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 설치 또는 업그레이드한 후 중앙 집중식 호스트 플러그인에 있는 단일 컨테이너 리소스는 수동으로 리소스를 추가해도 계속 유지됩니다.

  플러그인을 설치 또는 업그레이드한 후에는 SnapCenter에 직접 등록된 SAP HANA Linux 호스트에서만 SAP HANA 데이터베이스가 자동으로 검색됩니다.

- 멀티테넌트 데이터베이스 컨테이너(MDC)

  플러그인을 설치 또는 업그레이드한 후에는 수동으로 추가한 리소스로 중앙 집중식 호스트 플러그인에 있는 MDC 리소스가 계속됩니다.

SnapCenter 4.3으로 업그레이드한 후 중앙 집중식 호스트 플러그인에서 MDC 리소스를 수동으로 추가해야 합니다.

SnapCenter에 직접 등록된 SAP HANA Linux 호스트의 경우 플러그인을 설치 또는 업그레이드하면 호스트의 리소스에 대한 자동 검색이 트리거됩니다. 플러그인을 업그레이드한 후 플러그인 호스트에 있는 모든 MDC 리소스에 대해 다른 GUID 형식으로 다른 MDC 리소스가 자동으로 검색되어 SnapCenter에 등록됩니다. 새 리소스가 잠김 상태가 됩니다.

예를 들어 SnapCenter 4.2에서 E90 MDC 리소스가 플러그인 호스트에 있고 수동으로 등록된 경우 SnapCenter 4.3으로 업그레이드한 후 다른 GUID를 가진 다른 E90 MDC 리소스가 SnapCenter에 검색되어 등록됩니다.

다음 구성에서는 자동 검색이 지원되지 않습니다.

- RDM 및 VMDK 레이아웃

  위의 리소스가 검색되는 경우 이러한 리소스에서 데이터 보호 작업이 지원되지 않습니다.

- HANA 다중 호스트 구성
- 동일한 호스트에 여러 인스턴스가 있습니다
- 다중 계층 스케일아웃 HANA 시스템 복제
- 시스템 복제 모드의 다중 구간 복제 환경

지원되는 백업 유형입니다

백업 유형은 생성할 백업 유형을 지정합니다. SnapCenter는 SAP HANA 데이터베이스용 파일 기반 백업 및 스냅샷 복사본 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. SnapCenter에서는 파일 기반 백업을 복원 및 클론 복제할 수 없습니다.

스냅샷 복사본 기반 백업

스냅샷 복사본 기반 백업은 NetApp Snapshot 복사본 기술을 활용하여 SAP HANA 데이터베이스가 상주하는 볼륨의 온라인 읽기 전용 복사본을 생성합니다.

SAP HANA 데이터베이스용 **SnapCenter** 플러그인이 정합성 보장 그룹 스냅샷 복사본을 사용하는 방법

플러그인을 사용하여 리소스 그룹의 일관성 그룹 스냅샷 복사본을 생성할 수 있습니다. 일관성 그룹은 여러 볼륨을 포함하는 컨테이너로, 이를 단일 엔터티로 관리할 수 있습니다. 일관성 그룹은 여러 볼륨의 동시 스냅샷 복사본으로 볼륨 그룹의 일관된 복사본을 제공합니다.

스토리지 컨트롤러가 스냅샷 복사본을 일관되게 그룹화할 때까지 대기 시간을 지정할 수도 있습니다. 사용 가능한 대기 시간 옵션은 * 긴급 *, * 보통 * 및 * 완화된 * 입니다. 또한 일관된 그룹 스냅샷 복사본 작업 중에 WAFL(Write Anywhere File Layout) 동기화를 활성화 또는 비활성화할 수 있습니다. WAFL 동기화는 일관성 그룹 스냅샷 복사본의 성능을 향상시킵니다.

SnapCenter에서 로그 및 데이터 백업의 관리 방법

SnapCenter는 스토리지 시스템과 파일 시스템 레벨, SAP HANA 백업 카탈로그 내에서 로그 및 데이터 백업의 하우스키핑을 관리합니다.

운영 또는 2차 스토리지의 스냅샷 복사본과 SAP HANA 카탈로그의 해당 항목이 보존 설정에 따라 삭제됩니다. 백업 및 리소스 그룹을 삭제하는 동안 SAP HANA 카탈로그 항목도 삭제됩니다.

SAP HANA 데이터베이스의 백업 일정을 결정할 때 고려할 사항

백업 스케줄을 결정할 때 가장 중요한 요소는 리소스의 변경 속도입니다. 자주 사용하는 리소스를 매일 한 번씩 백업할 수도 있고, 자주 사용하지 않는 리소스를 하루에 한 번 백업할 수도 있습니다. 기타 요인으로는 조직에 리소스의 중요성, SLA(서비스 수준 계약) 및 RPO(복구 지점 목표)가 있습니다.

백업 스케줄은 다음과 같이 두 부분으로 구성됩니다.

- 백업 빈도(백업 수행 빈도)

  일부 플러그인의 스케줄 유형이라고도 하는 백업 빈도는 정책 구성의 일부입니다. 예를 들어 백업 빈도를 매시간, 일별, 주별 또는 월별로 구성할 수 있습니다.

- 백업 일정(백업을 수행할 정확한 시기

  백업 스케줄은 리소스 또는 리소스 그룹 구성의 일부입니다. 예를 들어 주별 백업에 대한 정책이 구성된 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 스케줄을 구성할 수 있습니다

SAP HANA 데이터베이스에 필요한 백업 작업 수입니다

필요한 백업 작업 수를 결정하는 요인에는 리소스 크기, 사용된 볼륨 수, 리소스 변경 속도 및 SLA(서비스 수준 계약)가 포함됩니다.

SAP HANA 데이터베이스용 플러그인의 백업 명명 규칙

기본 스냅샷 복사본 명명 규칙을 사용하거나 사용자 지정된 명명 규칙을 사용할 수 있습니다. 기본 백업 명명 규칙은 스냅샷 복사본 이름에 타임 스탬프를 추가하여 복사본이 생성된 시간을 식별하도록 도와줍니다.

스냅샷 복사본은 다음과 같은 기본 명명 규칙을 사용합니다.

```
resourcegroupname_hostname_timestamp
```

다음 예제와 같이 백업 리소스 그룹의 이름을 논리적으로 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예제에서 구문 요소는 다음과 같은 의미를 가집니다.

- _dts1_은(는) 리소스 그룹 이름입니다.
- _mach1x88_은 호스트 이름입니다.
- _03-12-2015_23.17.26_은 날짜 및 타임스탬프입니다.

또는 * Use custom name format for Snapshot copy * 를 선택하여 리소스 또는 리소스 그룹을 보호하면서 스냅샷 복사본 이름 형식을 지정할 수 있습니다. 예를 들어 customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname을 입력합니다. 기본적으로 타임스탬프 접미사가 스냅샷 복사본 이름에 추가됩니다.

SAP HANA 데이터베이스용 복원 및 복구 전략

SAP HANA 리소스에 대한 복원 및 복구 전략 정의

복구 및 복구 작업을 성공적으로 수행하려면 데이터베이스를 복원 및 복구하기 전에 전략을 정의해야 합니다.

단계

1. 수동으로 추가한 SAP HANA 리소스에 대해 지원되는 복원 전략을 결정합니다
2. 자동 검색된 SAP HANA 데이터베이스에 대해 지원되는 복구 전략을 결정합니다
3. 수행할 복구 작업 유형을 결정합니다.

수동으로 추가한 SAP HANA 리소스에 대해 지원되는 복원 전략의 유형입니다

SnapCenter를 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다. 수동으로 SAP HANA 리소스를 추가하는 두 가지 유형의 복원 전략이 있습니다. 수동으로 추가한 SAP HANA 리소스는 복구할 수 없습니다.

수동으로 추가한 SAP HANA 리소스는 복구할 수 없습니다.

리소스 복원을 완료합니다

- 리소스의 모든 볼륨, qtree 및 LUN을 복원합니다

리소스에 볼륨 또는 qtree가 포함된 경우, 해당 볼륨 또는 qtree에서 복원하도록 선택된 Snapshot 복사본 이후에 생성된 스냅샷 복사본은 삭제되고 복구할 수 없습니다. 또한 동일한 볼륨 또는 qtree에서 다른 리소스가 호스트되는 경우 해당 리소스도 삭제됩니다.

파일 레벨 복구

- 볼륨, qtree 또는 디렉토리에서 파일을 복원합니다
- 선택한 LUN만 복구합니다

자동으로 검색된 SAP HANA 데이터베이스에 대해 지원되는 복원 전략의 유형입니다

SnapCenter를 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다. 자동으로 검색된 SAP HANA 데이터베이스에는 두 가지 유형의 복원 전략이 있습니다.

리소스 복원을 완료합니다

- 리소스의 모든 볼륨, qtree 및 LUN을 복원합니다
  - 전체 볼륨을 복원하려면 * Volume Revert * 옵션을 선택해야 합니다.

> 리소스에 볼륨 또는 qtree가 포함된 경우, 해당 볼륨 또는 qtree에서 복원하도록 선택된 Snapshot 복사본 이후에 생성된 스냅샷 복사본은 삭제되고 복구할 수 없습니다. 또한 동일한 볼륨 또는 qtree에서 다른 리소스가 호스트되는 경우 해당 리소스도 삭제됩니다.

테넌트 데이터베이스

- 테넌트 데이터베이스를 복원합니다

Tenant Database * 옵션을 선택한 경우 SnapCenter 외부의 HANA Studio 또는 HANA 복구 스크립트를 사용하여 복구 작업을 수행해야 합니다.

자동 검색된 **SAP HANA** 데이터베이스의 복원 작업 유형

SnapCenter는 자동으로 검색된 SAP HANA 데이터베이스에 대해 VBSR(볼륨 기반 SnapRestore), 단일 파일 SnapRestore 및 연결 및 복사본 복원 유형을 지원합니다.

VBSR(볼륨 기반 **SnapRestore)**은 **NFS** 환경에서 다음 시나리오에 대해 수행됩니다**.**

- 복원용으로 선택한 백업이 SnapCenter 4.3 이전의 릴리즈에서 수행되었으며 전체 리소스 옵션을 선택한 경우에만 수행됩니다
- 복원을 위해 선택한 백업이 SnapCenter 4.3에서 수행되고 * 볼륨 복원 * 옵션이 선택된 경우

단일 파일 **SnapRestore**는 **NFS** 환경에서 다음 시나리오에 대해 수행됩니다**.**

- 복원을 위해 선택한 백업이 SnapCenter 4.3에서 수행된 경우, * Complete Resource * 옵션만 선택한 경우
- MDC(멀티테넌트 데이터베이스 컨테이너)의 경우, 복원을 위해 선택한 백업이 SnapCenter 4.3에서 수행되고 * 테넌트 데이터베이스 * 옵션이 선택된 경우
- SnapMirror 또는 SnapVault 보조 위치에서 백업을 선택하고 * Complete Resource * 옵션을 선택한 경우

단일 파일 **SnapRestore**는 **SAN** 환경에서 다음 시나리오에 대해 수행됩니다**.**

- SnapCenter 4.3 이전 릴리즈에서 백업을 수행하고 * Complete Resource * 옵션을 선택한 경우에만 백업이 수행됩니다
- SnapCenter 4.3에서 백업을 수행하고 * Complete Resource * 옵션을 선택한 경우에만 백업이 수행됩니다
- SnapMirror 또는 SnapVault 보조 위치에서 백업을 선택하고 * Complete Resource * 옵션을 선택하면

연결 및 복사 기반 복원은 **SAN** 환경에서 다음 시나리오에 대해 수행됩니다**.**

- MDC의 경우, 복원을 위해 선택된 백업이 SnapCenter 4.3에서 수행되고 * Tenant Database * 옵션이 선택된 경우

> 복원 범위 페이지에서 * 전체 리소스 *, * 볼륨 복원 * 및 * 테넌트 데이터베이스 * 옵션을 사용할 수 있습니다.

SAP HANA 데이터베이스에 지원되는 복구 작업의 유형입니다

SnapCenter를 사용하면 SAP HANA 데이터베이스에 대해 다양한 유형의 복구 작업을 수행할 수 있습니다.

- 데이터베이스를 최신 상태로 복구합니다
- 데이터베이스를 특정 시점으로 복구합니다

  복구할 날짜와 시간을 지정해야 합니다.

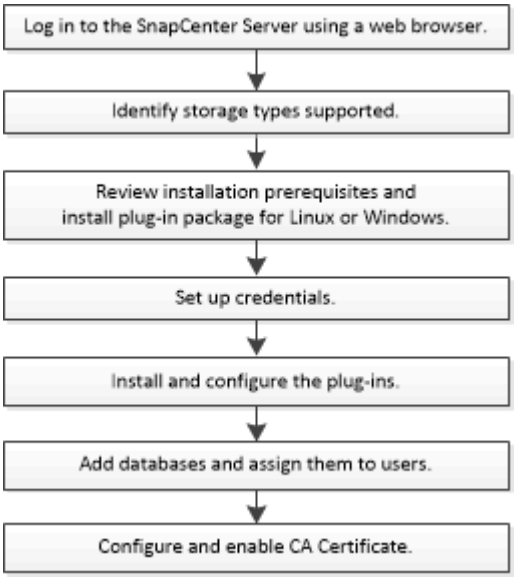
- 데이터베이스를 특정 데이터 백업까지 복구합니다

또한 SnapCenter는 SAP HANA 데이터베이스에 대해 복구 안 함 옵션을 제공합니다.

SAP HANA 데이터베이스용 **SnapCenter** 플러그인 설치를 준비합니다

SAP HANA 데이터베이스용 **SnapCenter** 플러그인 설치 워크플로우

SAP HANA 데이터베이스를 보호하려면 SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



호스트를 추가하고 **SAP HANA** 데이터베이스용 **SnapCenter** 플러그인을 설치하기 위한 사전 요구사항

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 완료해야 합니다. SAP HANA 데이터베이스용 SnapCenter 플러그인은 Windows 및 Linux 환경 모두에서 사용할 수 있습니다.

- 호스트에 Java 1.8 64비트를 설치해야 합니다.

IBM Java는 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 데이터베이스용 플러그인이 도메인 관리자로 설치된 경우 기본 동작입니다.
- Windows의 경우 사용자 저장소 키를 시스템 사용자로 만들어야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자의 경우 호스트에서 UAC를 비활성화해야 합니다. Microsoft Windows용 SnapCenter 플러그인은 기본적으로 Windows 호스트에 SAP HANA 플러그인을 사용하여 구축됩니다.
- Linux 호스트의 경우 HDB Secure User Store 키는 HDBSQL OS 사용자로 액세스됩니다.
- SnapCenter 서버는 SAP HANA 데이터베이스 호스트용 플러그인의 8145 또는 맞춤형 포트에 액세스할 수 있어야 합니다.

Windows 호스트

- 원격 호스트에 대한 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 루트 이외의 사용자에 대해 암호 기반 SSH 연결을 활성화해야 합니다.
- Windows 호스트에 Java 1.8 64비트를 설치해야 합니다.

  "모든 운영 체제에 대한 Java 다운로드"

  "NetApp 상호 운용성 매트릭스 툴"

Linux 호스트

- 루트 또는 루트 이외의 사용자에 대해 암호 기반 SSH 연결을 활성화해야 합니다.
- Linux 호스트에 Java 1.8 64비트를 설치해야 합니다.

  "모든 운영 체제에 대한 Java 다운로드"

  "NetApp 상호 운용성 매트릭스 툴"

- Linux 호스트에서 실행되는 SAP HANA 데이터베이스의 경우 SAP HANA 데이터베이스용 플러그인을 설치하는 동안 UNIX용 SnapCenter 플러그인은 자동으로 설치됩니다.
- 플러그인 설치를 위한 기본 셸은 * bash * 이어야 합니다.

보조 명령

SAP HANA용 SnapCenter 플러그인에서 보조 명령을 실행하려면 에 해당 명령을 포함해야 합니다 `allowed_commands.config` 파일.

`allowed_commands.config` 파일은 SnapCenter Plug-in for SAP HANA 디렉토리의 "etc" 하위 디렉토리에 있습니다.

Windows 호스트

기본값: `C:\Program Files\NetApp\SnapCenter\HANA\etc\allowed_commands.config`

사용자 지정 경로:
`<Custome_Directory>\NetApp\SnapCenter\HANA\etc\allowed_commands.config`
Windows 호스트:

Linux 호스트

기본값: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`

사용자 지정 경로: `<Custome_Directory>/NetApp/snapcenter/scc/etc/allowed_commands.config`

플러그인 호스트에서 추가 명령을 허용하려면 을 엽니다 `allowed_commands.config` 편집기의 파일. 각 명령을 별도의 줄에 입력합니다. 이름은 대소문자를 구분하지 않습니다.
예를 들면, 다음과 같습니다.

명령: mount

명령: 마운트 해제

정규화된 경로 이름을 지정해야 합니다. 공백이 포함된 경우, 경로 이름은 따옴표(")로 묶어야 합니다.
예를 들면, 다음과 같습니다.

명령: "C:\Program Files\NetApp\SnapCreator Commands\sdcli.exe"

명령: myscript.bat

를 누릅니다 `allowed_commands.config` 파일이 없거나 명령 또는 스크립트 실행이 차단되고 워크플로가 실패하고 다음 오류가 발생합니다.

"[/mnt/mount -a] 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여하십시오."

명령 또는 스크립트가 에 없는 경우 `allowed_commands.config`, 명령 또는 스크립트 실행이 차단되고 워크플로가 실패하고 다음 오류가 발생합니다.

"[/mnt/mount -a] 실행이 허용되지 않습니다. 플러그인 호스트의 %s 파일에 명령을 추가하여 권한을 부여하십시오."

와일드카드 항목(*)을 사용하여 모든 명령을 허용해서는 안 됩니다.

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항 및 사이징 요구 사항을 숙지해야 합니다.

항목	요구 사항
운영 체제	Microsoft Windows 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

항목	요구 사항
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	• Microsoft .NET Framework 4.7.2 이상 • WMF(Windows Management Framework) 4.0 이상 • PowerShell 4.0 이상 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴". NET 관련 문제 해결에 대한 자세한 내용은 을 참조하십시오 "인터넷에 연결되지 않은 기존 시스템의 경우 SnapCenter 업그레이드 또는 설치가 실패합니다."

Linux용 SnapCenter 플러그인 패키지 설치를 위한 호스트 요구 사항

Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 및 사이징 요구 사항을 숙지해야 합니다.

항목	요구 사항
운영 체제	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server(SLES) 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB

항목	요구 사항
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	Java 1.8.x(64비트) Oracle Java 및 OpenJDK의 기능 Java를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties 에 있는 java_home 옵션이 올바른 Java 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다. 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

SAP HANA 데이터베이스용 SnapCenter 플러그인에 대한 자격 증명 설정

SnapCenter는 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다. 데이터베이스 또는 Windows 파일 시스템에서 데이터 보호 작업을 수행하려면 SnapCenter 플러그인 설치를 위한 자격 증명과 추가 자격 증명을 만들어야 합니다.

이 작업에 대해

- Linux 호스트

  Linux 호스트에 플러그인을 설치하기 위한 자격 증명을 설정해야 합니다.

  플러그인 프로세스를 설치 및 시작할 수 있는 sudo 권한이 있는 루트 사용자 또는 루트 이외의 사용자에 대한 자격 증명을 설정해야 합니다.

  * 모범 사례: * 호스트를 구축하고 플러그인을 설치한 후 Linux에 대한 자격 증명을 생성할 수 있지만, 모범 사례는 호스트를 구축하고 플러그인을 설치하기 전에 SVM을 추가한 후 자격 증명을 생성하는 것입니다.

- Windows 호스트

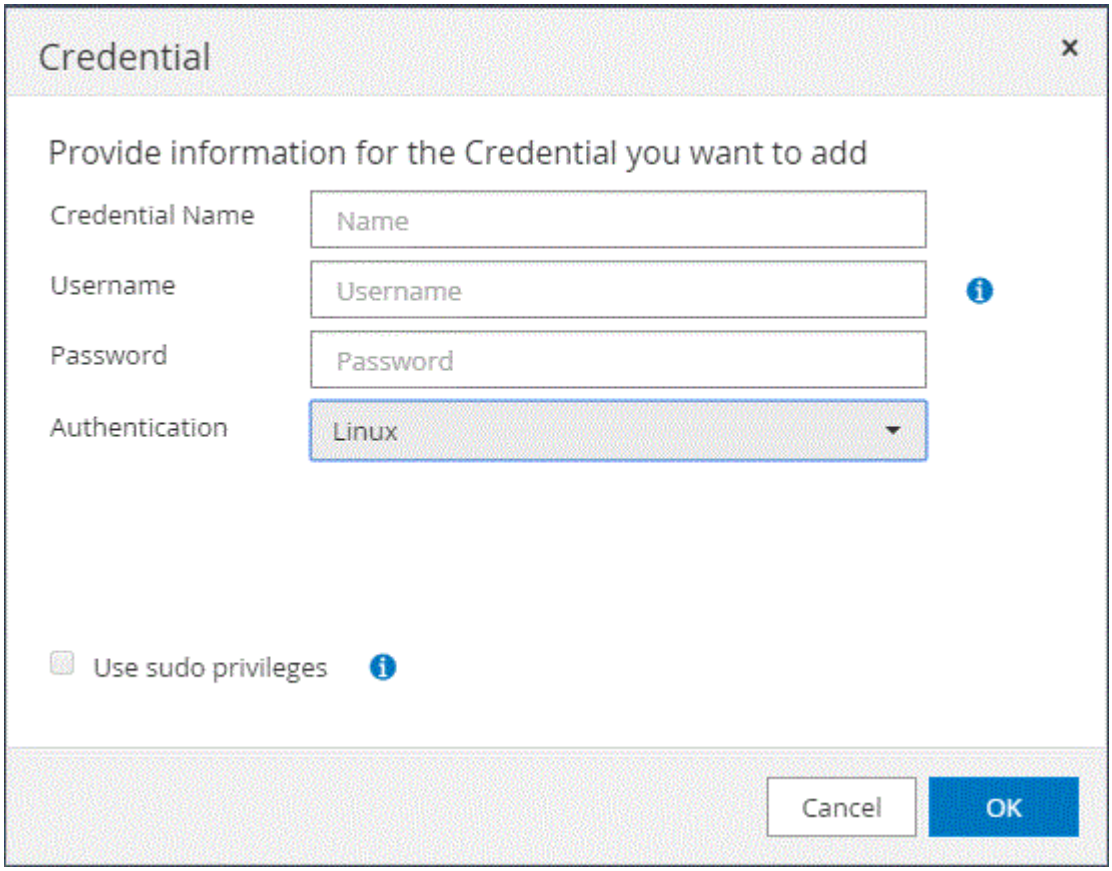
  플러그인을 설치하기 전에 Windows 자격 증명을 설정해야 합니다.

  원격 호스트에 대한 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정해야 합니다.

개별 리소스 그룹에 대한 자격 증명을 설정했고 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 증명 구성에 필요한 정보를 지정합니다.

이 필드의 내용...	수행할 작업...
자격 증명 이름입니다	자격 증명의 이름을 입력합니다.

이 필드의 내용...	수행할 작업...
사용자 이름입니다	인증에 사용할 사용자 이름과 암호를 입력합니다. • 도메인 관리자 또는 관리자 그룹의 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹의 구성원을 지정합니다. 사용자 이름 필드에 유효한 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 제공 로컬 관리자를 지정합니다. 사용자 계정에 상승된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 올바른 형식은 _ 사용자 이름 _ 입니다 암호에 큰따옴표(") 또는 백틱(')을 사용하지 마십시오. 보다 작음(<) 및 느낌표(!)를 사용해서는 안 됩니다. 암호를 사용한 기호. 예를 들어 LessThan <!10, Lessthan10 <!, backtick'12.
암호	인증에 사용되는 암호를 입력합니다.
인증 모드	사용할 인증 모드를 선택합니다.
sudo 권한을 사용합니다	루트가 아닌 사용자에 대한 자격 증명을 생성하는 경우 * sudo 권한 사용 * 확인란을 선택합니다. Linux 사용자에게만 적용됩니다.

5. 확인 * 을 클릭합니다.

자격 증명 설정을 마친 후 사용자 및 액세스 페이지의 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

Windows Server 2012 이상에서 GMSA를 구성합니다

Windows Server 2012 이상을 사용하면 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 GMSA(Managed Service Account)를 만들 수 있습니다.

시작하기 전에

- Windows Server 2012 이상의 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2012 이상 호스트가 있어야 합니다.

단계

1. KDS 루트 키를 생성하여 GMSA의 각 개체에 대해 고유한 암호를 생성합니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 Add-KDSRootKey-EffectiveImmediately 명령을 실행합니다
3. GMSA 생성 및 구성:
   a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
 domainName\accountName$
.. 그룹에 컴퓨터 개체를 추가합니다.
.. 방금 생성한 사용자 그룹을 사용하여 GMSA를 생성합니다.
```

   예를 들면, 다음과 같습니다.

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. 실행 `Get-ADServiceAccount` 명령을 사용하여 서비스 계정을 확인합니다.
```

4. 호스트에서 GMSA를 구성합니다.
   a. GMSA 계정을 사용할 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.

      이렇게 하려면 PowerShell에서 다음 명령을 실행합니다.

```
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 확인합니다. `Test-AdServiceAccount <gMSA>`

5. 호스트에서 구성된 GMSA에 관리 권한을 할당합니다.
6. SnapCenter 서버에서 구성된 GMSA 계정을 지정하여 Windows 호스트를 추가합니다.

   SnapCenter 서버는 선택한 플러그인을 호스트에 설치하고 지정된 GMSA는 플러그인 설치 중에 서비스 로그온 계정으로 사용됩니다.

SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치합니다

호스트를 추가하고 원격 호스트에 플러그인 패키지를 설치합니다

SnapCenter 호스트 추가 페이지를 사용하여 호스트를 추가한 다음 플러그인 패키지를 설치해야 합니다. 플러그인은 원격 호스트에 자동으로 설치됩니다. 호스트를 추가하고 개별 호스트 또는 클러스터에 대한 플러그인 패키지를 설치할 수 있습니다.

시작하기 전에

- 플러그인 설치 및 제거 권한이 있는 역할(예: SnapCenter 관리자 역할)에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에 속한 경우 호스트에서 UAC를 비활성화해야 합니다.
- 메시지 큐 서비스가 실행 중인지 확인해야 합니다.
- 관리 설명서에는 호스트 관리에 대한 정보가 포함되어 있습니다.
- 그룹 GMSA(Managed Service Account)를 사용하는 경우 관리자 권한으로 GMSA를 구성해야 합니다.

  "SAP HANA용 Windows Server 2012 이상에서 그룹 관리 서비스 계정을 구성합니다"

이 작업에 대해

- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.
- SAP HANA 시스템 복제의 경우 운영 시스템과 보조 시스템 모두에서 리소스를 검색하려면 root 또는 sudo 사용자를 사용하여 운영 시스템과 보조 시스템을 모두 추가하는 것이 좋습니다.

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 맨 위에 * Managed Hosts * 탭이 선택되어 있는지 확인합니다.
3. 추가 * 를 클릭합니다.
4. 호스트 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
호스트 유형	호스트 유형을 선택합니다. • Windows • 리눅스 SAP HANA용 플러그인은 HDBSQL 클라이언트 호스트에 설치되며, 이 호스트는 Windows 시스템 또는 Linux 시스템에 있을 수 있습니다.
호스트 이름입니다	통신 호스트 이름을 입력합니다. FQDN(정규화된 도메인 이름) 또는 호스트의 IP 주소를 입력합니다. SnapCenter는 DNS의 올바른 구성에 따라 달라집니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다. 이 호스트에서 HDBSQL 클라이언트 및 HDBUserStore를 구성해야 합니다.
자격 증명	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성합니다. 자격 증명에 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하십시오. 입력한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다. 자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 의해 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.
6. (선택 사항) * 추가 옵션 * 을 클릭합니다.

이 필드의 내용...	수행할 작업...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정합니다. 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.

이 필드의 내용...	수행할 작업...
설치 경로	SAP HANA용 플러그인은 HDBSQL 클라이언트 호스트에 설치되며, 이 호스트는 Windows 시스템 또는 Linux 시스템에 있을 수 있습니다. • Windows용 SnapCenter 플러그인 패키지의 경우 기본 경로는 C:\Program Files\NetApp\SnapCenter입니다. 선택적으로 경로를 사용자 지정할 수 있습니다. • Linux용 SnapCenter 플러그인 패키지의 경우 기본 경로는 /opt/netapp/snapcenter입니다. 선택적으로 경로를 사용자 지정할 수 있습니다.
사전 설치 검사를 건너뜁니다	플러그인이 이미 수동으로 설치되어 있고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.
그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행합니다	Windows 호스트의 경우 그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행하려면 이 확인란을 선택합니다. GMSA 이름을 domainName\accountName$ 형식으로 제공합니다. GMSA는 SnapCenter Plug-in for Windows 서비스에 대해서만 로그온 서비스 계정으로 사용됩니다.

7. 제출 * 을 클릭합니다.

   사전 검사 건너뛰기 확인란을 선택하지 않은 경우 호스트가 플러그인 설치 요구사항을 충족하는지 여부를 확인합니다. 디스크 공간, RAM, PowerShell 버전, .NET 버전, 위치(Windows 플러그인의 경우) 및 Java 버전(Linux 플러그인의 경우)은 최소 요구 사항에 따라 검증됩니다. 최소 요구 사항이 충족되지 않으면 적절한 오류 또는 경고 메시지가 표시됩니다.

   오류가 디스크 공간 또는 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 파일을 업데이트해야 합니다.

8. 호스트 유형이 Linux인 경우 지문을 확인한 다음 * 확인 및 제출 * 을 클릭합니다.

   클러스터 설정에서 클러스터의 각 노드에 대한 지문을 확인해야 합니다.

   동일한 호스트가 SnapCenter에 이전에 추가되었고 지문이 확인되었더라도 지문 확인은 필수입니다.

9. 설치 과정을 모니터링합니다.

   설치 관련 로그 파일은 /custom_location/snapcenter/logs에 있습니다.

cmdlet을 사용하여 여러 원격 호스트에 **Linux** 또는 **Windows**용 **SnapCenter** 플러그인 패키지를 설치합니다

설치-SmHostPackage PowerShell cmdlet을 사용하여 Linux 또는 Windows용 SnapCenter 플러그인 패키지를 여러 호스트에 동시에 설치할 수 있습니다.

시작하기 전에

플러그인 패키지를 설치할 각 호스트에 대한 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 cmdlet 및 필수 매개 변수를 사용하여 여러 호스트에 플러그인을 설치합니다.

   cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

   플러그인을 수동으로 설치했으며 호스트가 플러그인을 설치하는 데 필요한 요구 사항을 충족하는지 확인하지 않으려는 경우 -skipprecheck 옵션을 사용할 수 있습니다.

4. 원격 설치를 위한 자격 증명을 입력합니다.

명령줄 인터페이스를 사용하여 **Linux** 호스트에 **SAP HANA** 데이터베이스용 **SnapCenter** 플러그인을 설치합니다

SnapCenter UI(사용자 인터페이스)를 사용하여 SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치해야 합니다. 사용 환경에서 SnapCenter UI에서 플러그인을 원격으로 설치할 수 없는 경우 CLI(Command-Line Interface)를 사용하여 콘솔 모드 또는 자동 모드로 SAP HANA 데이터베이스용 플러그인을 설치할 수 있습니다.

시작하기 전에

- HDBSQL 클라이언트가 상주하는 각 Linux 호스트에 SAP HANA 데이터베이스용 플러그인을 설치해야 합니다.
- SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치하려는 Linux 호스트는 종속 소프트웨어, 데이터베이스 및 운영 체제 요구사항을 충족해야 합니다.

  상호 운용성 매트릭스 툴(IMT): 지원되는 구성에 대한 최신 정보를 제공합니다.

  "NetApp 상호 운용성 매트릭스 툴"

- SAP HANA 데이터베이스용 SnapCenter 플러그인은 Linux용 SnapCenter 플러그인 패키지의 일부입니다. Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 Windows 호스트에 SnapCenter가 이미 설치되어 있어야 합니다.

단계

1. Linux용 SnapCenter 플러그인 패키지 설치 파일(snapcenter_linux_host_plugin.bin)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. 플러그인 설치: `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 매개 변수를 추가합니다.
5. Add-Smhost cmdlet 및 필수 매개 변수를 사용하여 SnapCenter 서버에 호스트를 추가합니다.

   명령에 사용할 수 있는 매개 변수와 해당 설명에 대한 정보는 _get-Help command_name_을 실행하여 얻을 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

SAP HANA용 플러그인 설치 상태를 모니터링합니다

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행률을 모니터링할 수 있습니다. 설치 진행 상황을 확인하여 설치 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다

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 클릭합니다.
   b. 선택 사항: 시작 및 종료 날짜를 지정합니다.
   c. 유형 드롭다운 메뉴에서 * 플러그인 설치 * 를 선택합니다.
   d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
   e. 적용 * 을 클릭합니다.
4. 설치 작업을 선택하고 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. Job Details * 페이지에서 * View logs * 를 클릭합니다.

CA 인증서를 구성합니다

CA 인증서 CSR 파일을 생성합니다

CSR(인증서 서명 요청)을 생성하고 생성된 CSR을 사용하여 CA(인증 기관)에서 가져올 수 있는 인증서를 가져올 수 있습니다. 인증서에 연결된 개인 키가 있습니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.

CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 자세한 내용은 을 참조하십시오 "CA 인증서 CSR 파일을 생성하는 방법".

도메인(* .domain.company.com) 또는 시스템(machine1.domain.company.com CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter를 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN) 및 해당 호스트 이름을 CA 인증서에 언급해야 합니다. 인증서를 조달하기 전에 SAN(Subject Alternative Name) 필드를 채워 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(* .domain.company.com)의 경우 인증서에 도메인의 모든 호스트 이름이 암시적으로 포함됩니다.

CA 인증서를 가져옵니다

MMC(Microsoft Management Console)를 사용하여 CA 인증서를 SnapCenter 서버 및 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 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 단추로 클릭한 다음 * 모든 작업 * > * 가져오기 * 를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료합니다.

이 마법사 창에서...	다음을 수행합니다.
개인 키를 가져옵니다	예 * 옵션을 선택하고 개인 키를 가져온 다음 * 다음 * 을 클릭합니다.
파일 형식 가져오기	변경하지 않고 * 다음 * 을 클릭합니다.
보안	내보낸 인증서에 사용할 새 암호를 지정하고 * 다음 * 을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

인증서 가져오기는 개인 키와 함께 번들로 제공됩니다(지원되는 형식은 *.pfx, *.p12 및 *.p7b 입니다).

7. "개인" 폴더에 대해 5단계를 반복합니다.

CA 인증서 지문을 받습니다

인증서 thumbprint는 인증서를 식별하는 16진수 문자열입니다. 썸프린트는 썸프린트 알고리즘을 사용하여 인증서 컨텐츠에서 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.
   a. 인증서를 두 번 클릭합니다.
   b. 인증서 대화 상자에서 * 세부 정보 * 탭을 클릭합니다.
   c. 필드 목록을 스크롤하여 * Thumbprint * 를 클릭합니다.
   d. 상자에서 16진수 문자를 복사합니다.
   e. 16진수 사이의 공백을 제거합니다.

      예를 들어, 썸프린트가 "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 0d 42 77 A3 2a 7b"인 경우 공백을 제거한 후 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.
   a. 다음 명령을 실행하여 설치된 인증서의 엄지손가락 지문을 나열하고 최근 설치된 인증서를 주체 이름으로 식별합니다.

      Get-ChildItem-Path 인증:*LocalMachine\My*

   b. 엄지손가락 지문을 복사합니다.

Windows 호스트 플러그인 서비스를 사용하여 **CA** 인증서를 구성합니다

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스를 사용하여 CA 인증서를 구성해야 합니다.

SnapCenter 서버 및 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하여 기존 인증서 바인딩을 제거합니다.

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   예를 들면 다음과 같습니다.

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스와 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 들면 다음과 같습니다.

   ```
   > $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** 인증서를 구성합니다

사용자 지정 플러그인 키 저장소 및 인증서의 암호를 관리하고, CA 인증서를 구성하고, 사용자 지정 플러그인 트러스트 저장소에 대한 루트 또는 중간 인증서를 구성하고, SnapCenter 사용자 지정 플러그인 서비스를 사용하여 사용자 지정 플러그인 트러스트 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

사용자 지정 플러그인은 _/opt/netapp/snapcenter/SCC/etc_에 있는 'keystore.jks' 파일을 신뢰 저장소 및 키 저장소로 사용합니다.

사용자 지정 플러그인 키 저장소 및 사용 중인 **CA** 서명 키 쌍의 별칭에 대한 암호를 관리합니다

단계

1. 사용자 지정 플러그인 에이전트 속성 파일에서 사용자 지정 플러그인 키 저장소 기본 암호를 검색할 수 있습니다.

'keystore_pass' 키에 해당하는 값입니다.

2. 키 저장소 암호를 변경합니다.

```
 keytool -storepasswd -keystore keystore.jks
. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 암호를 키 저장소에 사용되는 동일한 암호로 변경합니다.
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

agent.properties 파일의 keystore_pass 키에 대해서도 동일한 업데이트를 하십시오.

3. 암호를 변경한 후 서비스를 다시 시작합니다.

사용자 지정 플러그인 키 저장소 및 개인 키의 모든 관련 별칭 암호에 대한 암호는 동일해야 합니다.

사용자 지정 플러그인 트러스트 저장소에 루트 또는 중간 인증서를 구성합니다

사용자 지정 플러그인 트러스트 저장소에 대한 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 사용자 지정 플러그인 키 저장소가 포함된 폴더로 이동합니다. /opt/netapp/snapcenter/SCC 등
2. 'keystore.jks' 파일을 찾습니다.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 루트 또는 중간 인증서 추가:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. 루트 또는 중간 인증서를 사용자 지정 플러그인 트러스트 저장소에 구성한 후 서비스를 다시 시작합니다.
```

루트 CA 인증서와 중간 CA 인증서를 추가해야 합니다.

사용자 지정 플러그인 트러스트 저장소에 **CA** 서명 키 쌍을 구성합니다

CA 서명 키 쌍을 사용자 지정 플러그인 트러스트 저장소에 구성해야 합니다.

단계

1. 사용자 지정 플러그인 키 저장소/opt/NetApp/snapcenter/SCC 등이 포함된 폴더로 이동합니다
2. 'keystore.jks' 파일을 찾습니다.

3. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

4. 개인 키와 공개 키를 모두 사용하는 CA 인증서를 추가합니다.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 키 저장소에 추가된 인증서를 나열합니다.

```
keytool -list -v -keystore keystore.jks
```

6. keystore에 keystore에 추가된 새 CA 인증서에 해당하는 별칭이 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 암호를 키 저장소 암호로 변경합니다.

   기본 사용자 지정 플러그인 키 저장소 암호는 agent.properties 파일의 keystore_pass 키 값입니다.

```
 keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. CA 인증서의 별칭 이름이 길고 공백 또는 특수 문자("*",",")가 포함된 경우 별칭 이름을
단순 이름으로 변경합니다.
```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. agent.properties 파일의 CA 인증서에서 별칭 이름을 구성합니다.
```

   이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

8. CA 서명 키 쌍을 사용자 지정 플러그인 트러스트 저장소에 구성한 후 서비스를 다시 시작합니다.

SnapCenter 사용자 지정 플러그인에 대한 **CRL(**인증서 해지 목록**)**을 구성합니다

이 작업에 대해

- SnapCenter 사용자 지정 플러그인은 사전 구성된 디렉터리에서 CRL 파일을 검색합니다.
- SnapCenter 사용자 지정 플러그인에 대한 CRL 파일의 기본 디렉토리는 'opt/netapp/snapcenter/SCC/etc/CRL'입니다.

단계

1. agent.properties 파일의 기본 디렉터리를 수정하여 CRL_path 키에 맞게 업데이트할 수 있습니다.

   이 디렉터리에 둘 이상의 CRL 파일을 배치할 수 있습니다. 들어오는 인증서는 각 CRL에 대해 확인됩니다.

Windows 호스트에서 **SnapCenter SAP HANA** 플러그인 서비스에 대한 **CA** 인증서를 구성합니다

사용자 지정 플러그인 키 저장소 및 인증서의 암호를 관리하고, CA 인증서를 구성하고, 사용자

지정 플러그인 트러스트 저장소에 대한 루트 또는 중간 인증서를 구성하고, SnapCenter 사용자 지정 플러그인 서비스를 사용하여 사용자 지정 플러그인 트러스트 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

사용자 지정 플러그인은 _C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_에 있는 file_keystore.jks_를 신뢰 저장소 및 키 저장소로 사용합니다.

사용자 지정 플러그인 키 저장소 및 사용 중인 **CA** 서명 키 쌍의 별칭에 대한 암호를 관리합니다

단계

1. 사용자 지정 플러그인 에이전트 속성 파일에서 사용자 지정 플러그인 키 저장소 기본 암호를 검색할 수 있습니다.

   key_keystore_pass_에 해당하는 값입니다.

2. 키 저장소 암호를 변경합니다.

   _keytool - storepasswd - keystore keystore.jks _

   > Windows 명령 프롬프트에서 "keytool" 명령을 인식할 수 없는 경우 keytool 명령을 전체 경로로 바꿉니다.

   _C:\Program Files\Java\<JDK_VERSION>\bin\keytool.exe" - storepasswd -keystore keystore .jks _

3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 암호를 키 저장소에 사용되는 동일한 암호로 변경합니다.

   _keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks _

   agent.properties 파일의 keystore_pass 키에 대해서도 동일한 업데이트를 하십시오.

4. 암호를 변경한 후 서비스를 다시 시작합니다.

   > 사용자 지정 플러그인 키 저장소 및 개인 키의 모든 관련 별칭 암호에 대한 암호는 동일해야 합니다.

사용자 지정 플러그인 트러스트 저장소에 루트 또는 중간 인증서를 구성합니다

사용자 지정 플러그인 트러스트 저장소에 대한 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 사용자 지정 플러그인 keystore_C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_가 포함된 폴더로 이동합니다
2. 'keystore.jks' 파일을 찾습니다.
3. 키 저장소에 추가된 인증서를 나열합니다.

   keytool -list -v -keystore keystore.jks

4. 루트 또는 중간 인증서 추가:

   _keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks _

5. 루트 또는 중간 인증서를 사용자 지정 플러그인 트러스트 저장소에 구성한 후 서비스를 다시 시작합니다.

루트 CA 인증서와 중간 CA 인증서를 추가해야 합니다.

사용자 지정 플러그인 트러스트 저장소에 **CA** 서명 키 쌍을 구성합니다

CA 서명 키 쌍을 사용자 지정 플러그인 트러스트 저장소에 구성해야 합니다.

단계

1. 사용자 지정 플러그인 keystore_C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_가 포함된 폴더로 이동합니다
2. *keystore.jks* 파일을 찾습니다.
3. 키 저장소에 추가된 인증서를 나열합니다.

   keytool -list -v -keystore keystore.jks

4. 개인 키와 공개 키를 모두 사용하는 CA 인증서를 추가합니다.

   _keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype jks _

5. 키 저장소에 추가된 인증서를 나열합니다.

   keytool -list -v -keystore keystore.jks

6. keystore에 keystore에 추가된 새 CA 인증서에 해당하는 별칭이 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 암호를 키 저장소 암호로 변경합니다.

   기본 사용자 지정 플러그인 키 저장소 암호는 agent.properties 파일의 keystore_pass 키 값입니다.

   _keytool -keykeyasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks _

8. *agent.properties* 파일의 CA 인증서에서 별칭 이름을 구성합니다.

   이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

9. CA 서명 키 쌍을 사용자 지정 플러그인 트러스트 저장소에 구성한 후 서비스를 다시 시작합니다.

SnapCenter 사용자 지정 플러그인에 대한 **CRL(**인증서 해지 목록**)**을 구성합니다

이 작업에 대해

- 관련 CA 인증서에 대한 최신 CRL 파일을 다운로드하려면 를 참조하십시오 "SnapCenter CA 인증서에서 인증서 해지 목록 파일을 업데이트하는 방법".
- SnapCenter 사용자 지정 플러그인은 사전 구성된 디렉터리에서 CRL 파일을 검색합니다.
- SnapCenter 사용자 지정 플러그인에 대한 CRL 파일의 기본 디렉토리는 _'C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\CRL'_입니다.

단계

1. *agent.properties* 파일의 기본 디렉터리를 수정하여 CRL_path 키에 맞게 업데이트할 수 있습니다.

2. 이 디렉터리에 둘 이상의 CRL 파일을 배치할 수 있습니다.

   들어오는 인증서는 각 CRL에 대해 확인됩니다.

플러그인에 대해 **CA** 인증서를 활성화합니다

CA 인증서를 구성하고 SnapCenter 서버 및 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- run_Set-SmCertificateSettings_cmdlet을 사용하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- _get-SmCertificateSettings_를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 호스트 페이지에서 * 관리되는 호스트 * 를 클릭합니다.
3. 단일 또는 여러 플러그인 호스트를 선택합니다.
4. 추가 옵션 * 을 클릭합니다.
5. 인증서 유효성 검사 사용 * 을 선택합니다.

작업을 마친 후

관리 호스트 탭 호스트에는 자물쇠가 표시되고 자물쇠 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- 는 CA 인증서가 활성화되지 않았으며 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- CA 인증서의 유효성을 확인했음을 나타냅니다.
- CA 인증서의 유효성을 확인할 수 없음을 나타냅니다.
- 연결 정보를 검색할 수 없음을 나타냅니다.

  상태가 노란색 또는 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

VMware vSphere용 SnapCenter 플러그인을 설치합니다

데이터베이스가 가상 머신(VM)에 저장되어 있거나 VM 및 데이터 저장소를 보호하려는 경우 SnapCenter Plug-in for VMware vSphere 가상 어플라이언스를 구축해야 합니다.

배포에 대한 자세한 내용은 을 참조하십시오 "구축 개요".

CA 인증서를 배포합니다

VMware vSphere용 SnapCenter 플러그인을 사용하여 CA 인증서를 구성하려면 를 참조하십시오 "SSL 인증서를 생성하거나 가져옵니다".

CRL 파일을 구성합니다

VMware vSphere용 SnapCenter 플러그인은 사전 구성된 디렉토리에서 CRL 파일을 찾습니다. VMware vSphere용 SnapCenter 플러그인의 기본 CRL 파일 디렉토리는 */opt/netapp/config/CRL* 입니다.

이 디렉터리에 둘 이상의 CRL 파일을 배치할 수 있습니다. 들어오는 인증서는 각 CRL에 대해 확인됩니다.

데이터 보호를 준비합니다

SAP HANA 데이터베이스용 SnapCenter 플러그인을 사용하기 위한 사전 요구사항

SAP HANA 데이터베이스용 SnapCenter 플러그인을 사용하려면 먼저 SnapCenter 관리자가 SnapCenter 서버를 설치 및 구성하고 사전 요구 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다.
- SnapCenter 서버에 로그인합니다.
- 스토리지 시스템 접속을 추가하고 해당하는 경우 자격 증명을 생성하여 SnapCenter 환경을 구성합니다.
- Linux 또는 Windows 호스트에 Java 1.7 또는 Java 1.8을 설치합니다.

  호스트 시스템의 환경 경로 변수에서 Java 경로를 설정해야 합니다.

- 백업 복제를 원하는 경우 SnapMirror 및 SnapVault를 설정합니다.
- 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 클론 작업을 수행할 수 있는 다음과 같은 권한이 있는지 확인하십시오.
  - 백업 관리자
  - 카탈로그 읽기
  - 데이터베이스 백업 관리자
  - 데이터베이스 복구 운영자

SAP HANA 데이터베이스 보호에 리소스, 리소스 그룹 및 정책을 사용하는 방법

SnapCenter를 사용하기 전에 수행할 백업, 클론 및 복원 작업과 관련된 기본 개념을 이해하는 것이 좋습니다. 서로 다른 작업을 위해 리소스, 리소스 그룹 및 정책과 상호 작용합니다.

- 리소스는 일반적으로 SnapCenter를 통해 백업 또는 클론 복제하는 SAP HANA 데이터베이스입니다.
- SnapCenter 리소스 그룹은 호스트의 리소스 모음입니다.

자원 그룹에 대해 작업을 수행할 때 자원 그룹에 지정한 일정에 따라 자원 그룹에 정의된 자원에 대해 해당 작업을 수행합니다.

필요에 따라 단일 리소스 또는 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 수행할 수도 있습니다.

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

  자원 그룹을 만들 때 해당 그룹에 대해 하나 이상의 정책을 선택합니다. 단일 리소스에 대해 필요 시 백업을 수행할 때 정책을 선택할 수도 있습니다.

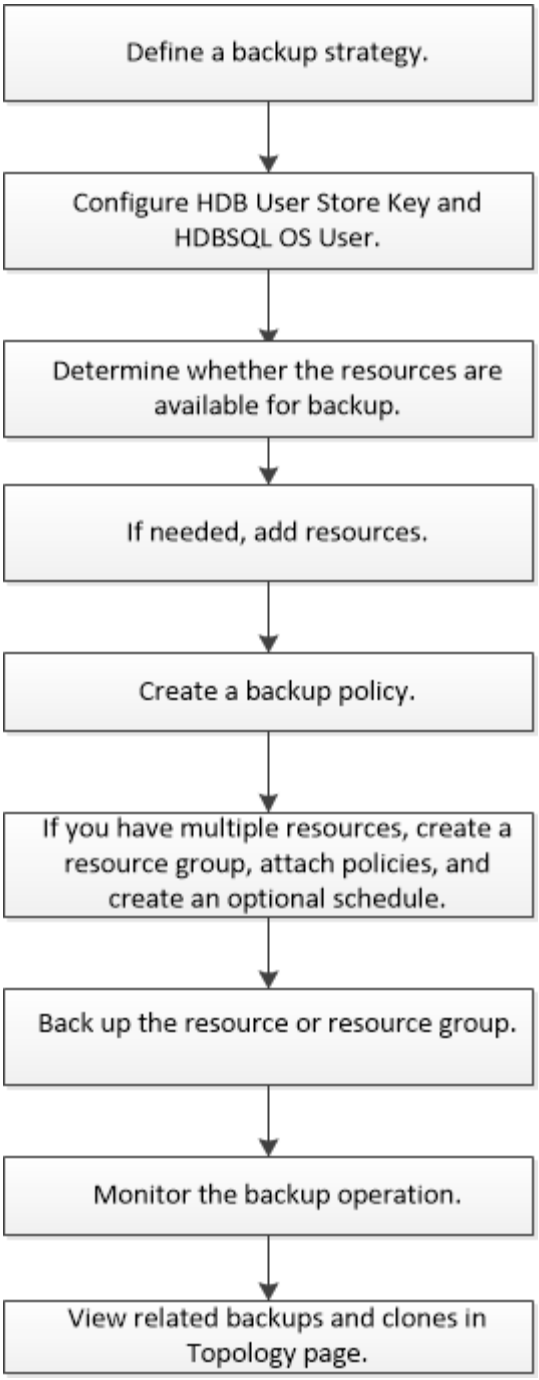
리소스 그룹은 보호할 내용과 시간을 일 및 시간 측면에서 보호할 시기를 정의하는 것으로 생각합니다. 정책을 보호할 방법을 정의하는 것으로 생각해 보십시오. 예를 들어 모든 데이터베이스를 백업하는 경우 호스트에 있는 모든 데이터베이스를 포함하는 리소스 그룹을 생성할 수 있습니다. 그런 다음 리소스 그룹에 일별 정책과 시간별 정책이라는 두 가지 정책을 연결할 수 있습니다. 리소스 그룹을 생성하고 정책을 연결할 때 매일 전체 백업을 수행하도록 리소스 그룹을 구성할 수 있습니다.

SAP HANA 리소스 백업

SAP HANA 리소스 백업

리소스(데이터베이스) 또는 리소스 그룹의 백업을 생성할 수 있습니다. 백업 워크플로우에는 계획, 백업용 데이터베이스 식별, 백업 정책 관리, 리소스 그룹 생성 및 정책 연결, 백업 생성 및 작업 모니터링이 포함됩니다.

다음 워크플로에서는 백업 작업을 수행해야 하는 순서를 보여 줍니다.



PowerShell cmdlet을 수동으로 사용하거나 스크립트에서 사용하여 백업, 복원 및 클론 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말 및 cmdlet 참조 정보에 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다. "SnapCenter 소프트웨어 cmdlet 참조 가이드".

SAP HANA 데이터베이스용 HDB 사용자 저장소 키 및 HDBSQL OS 사용자를 구성합니다

SAP HANA 데이터베이스에서 데이터 보호 작업을 수행하려면 HDB 사용자 저장소 키 및 HDBSQL OS 사용자를 구성해야 합니다.

시작하기 전에

- SAP HANA 데이터베이스에 HDB Secure User Store Key 및 HDB SQL OS User가 구성되어 있지 않은 경우, 자동으로 검색된 리소스에 대해서만 빨간색 자물쇠 아이콘이 나타납니다. 후속 검색 작업 중에 구성된 HDB 보안

사용자 저장소 키가 올바르지 않거나 데이터베이스 자체에 대한 액세스를 제공하지 않으면 빨간색 자물쇠 아이콘이 다시 나타납니다.

- 데이터베이스를 보호하거나 리소스 그룹에 추가하여 데이터 보호 작업을 수행하려면 HDB 보안 사용자 저장소 키 및 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 SnapCenter Plug-in for SAP HANA Database 를 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 리소스 유형을 선택합니다.
3. (선택 사항) 을 클릭합니다 호스트 이름을 선택합니다.

   그런 다음 을 클릭할 수 있습니다 를 눌러 필터 창을 닫습니다.
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 채워집니다.
6. 확인 * 을 클릭합니다.

토폴로지 페이지에서 데이터베이스 구성을 수정할 수 있습니다.

리소스를 검색하고 데이터 보호를 위한 멀티테넌트 데이터베이스 컨테이너를 준비합니다

데이터베이스를 자동으로 검색합니다

리소스는 SnapCenter에서 관리하는 Linux 호스트의 SAP HANA 데이터베이스 및 비 데이터 볼륨입니다. 사용 가능한 SAP HANA 데이터베이스를 검색하고 나면 이러한 리소스를 리소스 그룹에 추가하여 데이터 보호 작업을 수행할 수 있습니다.

시작하기 전에

- SnapCenter 서버 설치, HDB 사용자 저장소 키 추가, 호스트 추가 및 스토리지 시스템 접속 설정과 같은 작업을 이미 완료해야 합니다.
- Linux 호스트에서 HDB 보안 사용자 저장소 키 및 HDB SQL OS 사용자를 구성해야 합니다.
  - HDB 사용자 저장소 키를 SID adm 사용자로 구성해야 합니다. 예를 들어, SID가 A22인 HANA 시스템의 경우 HDB 사용자 저장소 키는 a22adm 으로 구성해야 합니다.
- SAP HANA 데이터베이스용 SnapCenter 플러그인은 RDM/VMDK 가상 환경에 상주하는 리소스의 자동 검색을 지원하지 않습니다. 데이터베이스를 수동으로 추가하는 동시에 가상 환경에 대한 스토리지 정보를 제공해야 합니다.

이 작업에 대해

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. 자원 페이지의 보기 목록에서 자원 유형을 선택합니다.
3. (선택 사항) * 를 클릭합니다  를 누른 다음 호스트 이름을 선택합니다.

   그런 다음 * 를 클릭할 수 있습니다  를 눌러 필터 창을 닫습니다.

4. 리소스 새로 고침 * 을 클릭하여 호스트에서 사용 가능한 리소스를 검색합니다.

   리소스는 리소스 유형, 호스트 이름, 관련 리소스 그룹, 백업 유형, 정책 및 전체 상태와 같은 정보와 함께 표시됩니다.

   - 데이터베이스가 NetApp 스토리지에 있고 보호되지 않는 경우 Overall Status 열에 Not protected가 표시됩니다.
   - 데이터베이스가 NetApp 스토리지 시스템에 있으며 보호되었고 백업 작업이 수행되지 않은 경우 전체 상태 열에 백업 실행 안 됨 이 표시됩니다. 그렇지 않으면 마지막 백업 상태에 따라 상태가 백업 실패 또는 백업 성공 으로 변경됩니다.

SAP HANA 데이터베이스에 HDB Secure User Store Key가 구성되어 있지 않으면 리소스 옆에 빨간색 자물쇠 아이콘이 나타납니다. 후속 검색 작업 중에 구성된 HDB 보안 사용자 저장소 키가 올바르지 않거나 데이터베이스 자체에 대한 액세스를 제공하지 않으면 빨간색 자물쇠 아이콘이 다시 나타납니다.

데이터베이스가 SnapCenter 외부에서 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

작업을 마친 후

데이터베이스를 보호하거나 리소스 그룹에 추가하여 데이터 보호 작업을 수행하려면 HDB Secure User Store Key 및 HDBSQL OS User를 구성해야 합니다.

"SAP HANA 데이터베이스용 HDB 사용자 저장소 키 및 HDBSQL OS 사용자를 구성합니다"

데이터 보호를 위한 멀티 테넌트 데이터베이스 컨테이너 준비

SnapCenter에 직접 등록된 SAP HANA 호스트의 경우 SAP HANA 데이터베이스용 SnapCenter 플러그인을 설치 또는 업그레이드하면 호스트에서 리소스를 자동으로 검색할 수 있습니다. 플러그인을 설치 또는 업그레이드한 후 플러그인 호스트에 있는 모든 MDC(멀티테넌트 데이터베이스 컨테이너) 리소스에 대해 다른 GUID 형식으로 다른 MDC 리소스가 자동으로 검색되어 SnapCenter에 등록됩니다. 새 자원은 "잠김" 상태가 됩니다.

이 작업에 대해

예를 들어 SnapCenter 4.2에서 E90 MDC 리소스가 플러그인 호스트에 있고 수동으로 등록된 경우 SnapCenter 4.3으로 업그레이드한 후 다른 GUID를 가진 다른 E90 MDC 리소스가 SnapCenter에 검색되어 등록됩니다.

SnapCenter 4.2 및 이전 버전의 리소스와 연결된 백업은 보존 기간이 만료될 때까지 보존되어야 합니다. 보존 기간이 만료된 후에는 이전 MDC 리소스를 삭제하고 자동으로 검색된 새 MDC 리소스를 계속 관리할 수 있습니다.

`Old MDC resource` 는 SnapCenter 4.2 이전 릴리즈에서 수동으로 추가한 플러그인 호스트의 MDC 리소스입니다.

다음 단계를 수행하여 SnapCenter 4.3에서 검색된 새 리소스를 데이터 보호 작업에 사용할 수 있습니다.

단계

1. 리소스 페이지에서 이전 SnapCenter 릴리스에 추가된 백업이 있는 이전 MDC 리소스를 선택하고 토폴로지 페이지에서 "유지 관리 모드"로 배치합니다.

   자원이 자원 그룹의 일부인 경우 자원 그룹을 "유지보수 모드"로 설정합니다.

2. 리소스 페이지에서 새 리소스를 선택하여 SnapCenter 4.3으로 업그레이드한 후 검색된 새 MDC 리소스를 구성합니다.

   "'새 MDC 리소스'는 SnapCenter 서버와 플러그인 호스트를 4.3으로 업그레이드한 후 새로 발견된 MDC 리소스입니다. 새 MDC 리소스는 기존 MDC 리소스와 동일한 SID를 가진 리소스로 식별될 수 있으며, 지정된 호스트의 경우 빨간색 자물쇠 아이콘이 리소스 페이지에 표시됩니다.

3. 보호 정책, 일정 및 알림 설정을 선택하여 SnapCenter 4.3으로 업그레이드한 후 발견된 새 MDC 리소스를 보호합니다.
4. 보존 설정을 기반으로 SnapCenter 4.2 이전 릴리즈에서 수행한 백업을 삭제합니다.
5. 토폴로지 페이지에서 리소스 그룹을 삭제합니다.
6. 리소스 페이지에서 이전 MDC 리소스를 삭제합니다.

   예를 들어 기본 스냅샷 복사본의 보존 기간이 7일이고 보조 스냅샷 복사본의 보존 기간이 45일이고 45일이 지난 후 모든 백업을 삭제한 경우 리소스 그룹과 이전 MDC 리소스를 삭제해야 합니다.

관련 정보

"SAP HANA 데이터베이스용 HDB 사용자 저장소 키 및 HDBSQL OS 사용자를 구성합니다"

"토폴로지 페이지에서 SAP HANA 데이터베이스 백업 및 클론 보기"

플러그인 호스트에 수동으로 리소스를 추가합니다

특정 HANA 인스턴스에는 자동 검색이 지원되지 않습니다. 이러한 리소스를 수동으로 추가해야 합니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 접속 설정, HDB 사용자 저장소 키 추가 등의 작업을 완료해야 합니다.
- SAP HANA 시스템 복제의 경우 해당 HANA 시스템의 모든 리소스를 하나의 리소스 그룹에 추가하고 리소스 그룹 백업을 수행하는 것이 좋습니다. 이렇게 하면 Takeover-failback 모드 중에 원활한 백업이 보장됩니다.

"리소스 그룹을 생성하고 정책을 연결합니다".

이 작업에 대해

다음 구성에서는 자동 검색이 지원되지 않습니다.

- RDM 및 VMDK 레이아웃

  위의 리소스가 검색되는 경우 이러한 리소스에서 데이터 보호 작업이 지원되지 않습니다.

- HANA 다중 호스트 구성
- 동일한 호스트에 여러 인스턴스가 있습니다
- 다중 계층 스케일아웃 HANA 시스템 복제
- 시스템 복제 모드의 다중 구간 복제 환경

단계

1. 왼쪽 탐색 창의 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 필드의 내용...	수행할 작업...
리소스 유형	리소스 유형을 입력합니다. 리소스 유형은 단일 컨테이너, 다중 테넌트 데이터베이스 컨테이너(MDC) 및 비 데이터 볼륨입니다.
HANA 시스템 이름	SAP HANA 시스템을 설명하는 이름을 입력합니다. 이 옵션은 단일 컨테이너 또는 MDC 리소스 유형을 선택한 경우에만 사용할 수 있습니다.
SID	SID(시스템 ID)를 입력합니다. 설치된 SAP HANA 시스템은 단일 SID로 식별됩니다.
플러그인 호스트	플러그인 호스트를 선택합니다.
HDB 보안 사용자 저장소 키	SAP HANA 시스템에 연결할 키를 입력합니다. 이 키에는 데이터베이스에 연결할 로그인 정보가 포함되어 있습니다. SAP HANA 시스템 복제의 경우 2차 사용자 키의 유효성이 검사되지 않습니다. 이는 테이크오버 중에 사용됩니다.
HDBSQL OS 사용자	HDB 보안 사용자 저장소 키가 구성된 사용자 이름을 입력합니다. Windows의 경우 HDBSQL OS 사용자가 시스템 사용자여야 합니다. 따라서 시스템 사용자에 대해 HDB 보안 사용자 저장소 키를 구성해야 합니다.

4. 스토리지 설치 공간 제공 페이지에서 스토리지 시스템을 선택하고 하나 이상의 볼륨, LUN 및 qtree를 선택한 다음 * 저장 * 을 클릭합니다.

   선택 사항: * 를 클릭할 수 있습니다 + 다른 스토리지 시스템에서 볼륨, LUN 및 qtree를 더 추가하는 아이콘

5. 요약을 검토하고 * Finish * 를 클릭합니다.

데이터베이스는 SID, 플러그인 호스트, 관련 리소스 그룹 및 정책, 전체 상태와 같은 정보와 함께 표시됩니다

사용자에게 리소스에 대한 액세스 권한을 제공하려면 사용자에게 리소스를 할당해야 합니다. 따라서 사용자는 자신에게 할당된 자산에 대한 사용 권한이 있는 작업을 수행할 수 있습니다.

"사용자 또는 그룹을 추가하고 역할 및 자산을 할당합니다"

데이터베이스를 추가한 후 SAP HANA 데이터베이스 세부 정보를 수정할 수 있습니다.

SAP HANA 리소스와 연결된 백업이 있는 경우 다음을 수정할 수 없습니다.

- MDC(멀티테넌트 데이터베이스 컨테이너): SID 또는 HDBSQL 클라이언트(플러그인) 호스트
- 단일 컨테이너: SID 또는 HDBSQL 클라이언트(플러그인) 호스트
- 비 데이터 볼륨: 리소스 이름, 연결된 SID 또는 플러그인 호스트

SAP HANA 데이터베이스에 대한 백업 정책을 생성합니다

SnapCenter를 사용하여 SAP HANA 데이터베이스 리소스를 백업하기 전에 백업할 리소스 또는 리소스 그룹에 대한 백업 정책을 만들어야 합니다. 백업 정책은 백업을 관리, 예약 및 유지하는 방법을 제어하는 규칙의 집합입니다.

시작하기 전에

- 백업 전략을 정의해야 합니다.

  자세한 내용은 SAP HANA 데이터베이스의 데이터 보호 전략 정의에 대한 정보를 참조하십시오.

- SnapCenter 설치, 호스트 추가, 스토리지 시스템 접속 설정, 리소스 추가 등의 작업을 완료하여 데이터 보호를 위한 준비가 되어 있어야 합니다.
- 스냅샷 복사본을 미러 또는 볼트로 복제할 경우 SnapCenter 관리자가 소스 및 타겟 볼륨에 대한 SVM을 모두 할당해야 합니다.

  또한 정책에서 복제, 스크립트 및 애플리케이션 설정을 지정할 수 있습니다. 이러한 옵션을 사용하면 다른 리소스 그룹에 대해 정책을 다시 사용할 때 시간을 절약할 수 있습니다.

이 작업에 대해

- SAP HANA 시스템 복제
  - 운영 SAP HANA 시스템을 보호할 수 있으며 모든 데이터 보호 작업을 수행할 수 있습니다.
  - 2차 SAP HANA 시스템을 보호할 수 있지만 백업을 생성할 수는 없습니다.

    페일오버 후에는 보조 SAP HANA 시스템이 기본 SAP HANA 시스템으로 전환되므로 모든 데이터 보호 작업을 수행할 수 있습니다.

  SAP HANA 데이터 볼륨에 대한 백업을 생성할 수는 없지만 SnapCenter은 NDV(Non-Data Volumes)를 계속 보호합니다.

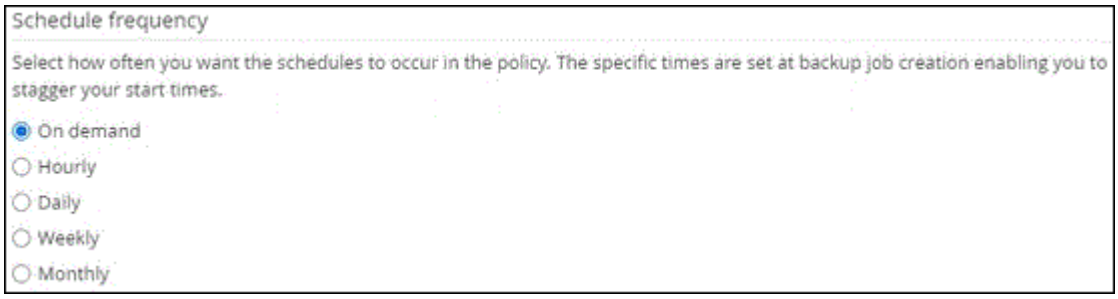
단계

1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
2. 설정 페이지에서 * 정책 * 을 클릭합니다.
3. 새로 만들기 * 를 클릭합니다.
4. 이름 페이지에 정책 이름과 설명을 입력합니다.
5. 설정 페이지에서 다음 단계를 수행하십시오.
   - 백업 유형 선택:

원하는 작업	수행할 작업...
데이터베이스의 무결성 검사를 수행합니다	파일 기반 백업 * 을 선택합니다. 활성 테넌트만 백업됩니다.
스냅샷 복사본 기술을 사용하여 백업을 생성합니다	스냅샷 기반 * 을 선택합니다.

   - On demand *, * Hourly *, * Daily *, * Weekly * 또는 * Monthly * 를 선택하여 일정 유형을 지정합니다.

> 리소스 그룹을 생성하는 동안 백업 작업의 스케줄(시작 날짜, 종료 날짜 및 빈도)을 지정할 수 있습니다. 따라서 동일한 정책 및 백업 빈도를 공유하는 리소스 그룹을 생성할 수 있을 뿐 아니라 각 정책에 서로 다른 백업 스케줄을 할당할 수도 있습니다.



> 오전 2시에 예약된 경우 DST(일광 절약 시간) 중에는 일정이 트리거되지 않습니다.

   - 사용자 지정 백업 설정 * 섹션에서 플러그인에 전달할 특정 백업 설정을 키 값 형식으로 제공합니다.

     플러그인으로 전달할 여러 키 값을 제공할 수 있습니다.

6. 보존 페이지에서 백업 유형에 대한 보존 설정과 백업 유형 페이지에서 선택한 스케줄 유형을 지정합니다.

원하는 작업	그러면...
일정 수의 스냅샷 복사본을 유지합니다	유지할 총 스냅샷 복사본 * 을 선택하고 유지할 스냅샷 복사본 수를 지정합니다. 스냅샷 복사본 수가 지정된 수를 초과하면 가장 오래된 복사본이 먼저 삭제된 후 스냅샷 복사본이 삭제됩니다. 최대 보존 값은 ONTAP 9.4 이상의 리소스에 대해 1018이고, ONTAP 9.3 이전 버전의 리소스에 대해서는 254입니다. 보존이 기본 ONTAP 버전에서 지원하는 값보다 높은 값으로 설정된 경우 백업이 실패합니다. 스냅샷 복사본 기반 백업의 경우 SnapVault 복제를 사용하도록 설정하려는 경우 보존 수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷 복사본이 타겟으로 복제될 때까지 첫 번째 스냅샷 복사본이 SnapVault 관계의 참조 스냅샷 복사본이므로 보존 작업이 실패할 수 있습니다. SAP HANA 시스템 복제의 경우 SAP HANA 시스템의 모든 리소스를 하나의 리소스 그룹에 추가하는 것이 좋습니다. 이렇게 하면 올바른 수의 백업이 유지됩니다. SAP HANA 시스템 복제의 경우, 생성된 총 스냅샷 복사본은 리소스 그룹에 대한 보존 세트와 같습니다. 가장 오래된 스냅샷 복사본을 제거할 때는 가장 오래된 스냅샷 복사본이 있는 노드를 기반으로 합니다. 예를 들어, SAP HANA 시스템 복제 운영 및 SAP HANA 시스템 복제 보조 서버가 있는 리소스 그룹의 경우 보존 기간이 7로 설정됩니다. SAP HANA 시스템 복제 운영 및 SAP HANA 시스템 복제 2차 복제를 포함하여 한 번에 최대 7개의 스냅샷 복사본을 생성할 수 있습니다.
Snapshot 복사본을 일정 일 동안 유지합니다	스냅샷 복사본 보관 * 을 선택한 다음, 스냅샷 복사본을 삭제하기 전에 유지할 일 수를 지정합니다.

7. 스냅샷 복사본 기반 백업의 경우 복제 페이지에서 복제 설정을 지정합니다.

이 필드의 내용...	수행할 작업...
• 로컬 스냅샷 복사본을 생성한 후 SnapMirror 업데이트 * 를 참조하십시오	다른 볼륨에 백업 세트의 미러 복사본을 생성하려면 이 필드를 선택합니다(SnapMirror 복제). ONTAP의 보호 관계가 미러와 볼트 유형이고 이 옵션만 선택한 경우, 운영 스토리지에 생성된 스냅샷 복사본이 대상으로 전송되지 않고 대상에 나열됩니다. 복원 작업을 수행하기 위해 대상에서 이 스냅샷 복사본을 선택하면 선택한 볼트된/미러된 백업 오류 메시지에 대해 보조 위치를 사용할 수 없습니다. 라는 메시지가 표시됩니다.
• 로컬 스냅샷 복사본을 생성한 후 SnapVault 업데이트 * 를 클릭합니다	디스크 간 백업 복제(SnapVault 백업)를 수행하려면 이 옵션을 선택합니다.
• 보조 정책 레이블 *	스냅샷 레이블을 선택합니다. 선택한 스냅샷 복사본 레이블에 따라 ONTAP에서는 해당 레이블과 일치하는 2차 스냅샷 복사본 보존 정책을 적용합니다. 로컬 스냅샷 복사본 * 을 생성한 후 SnapMirror 업데이트 * 를 선택한 경우, 선택적으로 보조 정책 레이블을 지정할 수 있습니다. 그러나 로컬 스냅샷 복사본 * 을 생성한 후 * SnapVault 업데이트 * 를 선택한 경우에는 보조 정책 레이블을 지정해야 합니다.
• 오류 재시도 횟수 *	작업이 중지되기 전에 허용되는 최대 복제 시도 횟수를 입력합니다.

보조 스토리지에 대한 ONTAP의 SnapMirror 보존 정책을 구성하면 보조 스토리지에서 스냅샷 복사본의 최대 제한에 도달하지 않도록 해야 합니다.

8. 요약을 검토하고 * Finish * 를 클릭합니다.

리소스 그룹을 생성하고 정책을 연결합니다

리소스 그룹은 백업 및 보호할 리소스를 추가해야 하는 컨테이너입니다. 리소스 그룹을 사용하면 지정된 애플리케이션과 연결된 모든 데이터를 동시에 백업할 수 있습니다. 모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한 수행할 데이터 보호 작업의 유형을 정의하려면 하나 이상의 정책을 리소스 그룹에 연결해야 합니다.

이 작업에 대해

SAP HANA 시스템 복제 백업을 생성하려면 SAP HANA 시스템의 모든 리소스를 하나의 리소스 그룹에 추가하는 것이 좋습니다. 이렇게 하면 Takeover-failback 모드 중에 원활한 백업이 보장됩니다.

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 필드의 내용...	수행할 작업...
이름	자원 그룹의 이름을 입력합니다. 리소스 그룹 이름은 250자를 초과할 수 없습니다.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력합니다. 예를 들어 HR을 여러 자원 그룹에 태그로 추가하면 나중에 HR 태그와 연결된 모든 자원 그룹을 찾을 수 있습니다.
스냅샷 복사본에 대해 사용자 지정 이름 형식을 사용합니다	이 확인란을 선택하고 스냅샷 복사본 이름에 사용할 사용자 지정 이름 형식을 입력합니다. 예를 들어 customtext_resource group_policy_hostname 또는 resource group_hostname을 입력합니다. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.

4. 리소스 페이지의 * 호스트 * 드롭다운 목록에서 호스트 이름을 선택하고 * 리소스 유형 * 드롭다운 목록에서 리소스 유형을 선택합니다.

   그러면 화면의 정보를 필터링하는 데 도움이 됩니다.

5. 사용 가능한 리소스 * 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 클릭하여 * 선택한 리소스 * 섹션으로 이동합니다.
6. 응용 프로그램 설정 페이지에서 다음을 실행합니다.

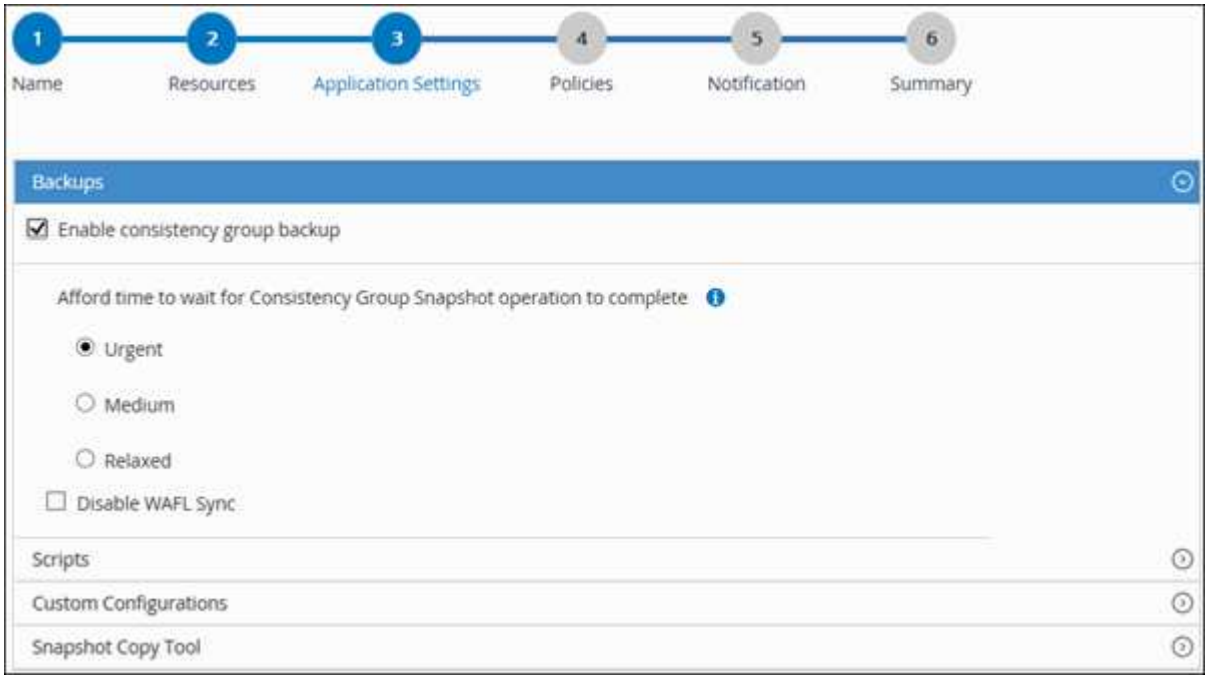
   a. 백업 * 화살표를 클릭하여 추가 백업 옵션을 설정합니다.

      정합성 보장 그룹 백업을 설정하고 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
정합성 보장 그룹 스냅샷 작업이 완료될 때까지 기다릴 여유가 없습니다	스냅샷 복사 작업이 완료될 때까지 대기 시간을 지정하려면 * 긴급 *, * 중간 * 또는 * 완화된 * 을 선택합니다. 긴급 = 5초, 중간 = 7초, 휴식 = 20초

이 필드의 내용...	수행할 작업...
WAFL 동기화를 비활성화합니다	WAFL 정합성 보장 지점을 강제로 사용하지 않으려면 이 옵션을 선택합니다.

+



a. 스크립트 * 화살표를 클릭하고 일시 중지, 스냅샷 복사 및 정지 해제 작업에 대한 사전 및 사후 명령을 입력합니다. 장애 발생 시 종료하기 전에 실행할 사전 명령을 입력할 수도 있습니다.

b. 사용자 지정 구성 * 화살표를 클릭하고 이 리소스를 사용하는 모든 데이터 보호 작업에 필요한 사용자 지정 키 값 쌍을 입력합니다.

매개 변수	설정	설명
archive_log_enable입니다	(예/아니요)	아카이브 로그 관리를 활성화합니다 아카이브 로그를 삭제합니다.
archive_log_retention 을 선택합니다	일 수	에서 일 수를 지정합니다 아카이브 로그가 보존됩니다. 이 설정입니다 보다 크거나 같아야 합니다 NTAP_스냅샷 _ 보존.
archive_log_DIR입니다	change_info_directory/logs	디렉토리의 경로를 지정합니다 아카이브 로그를 포함합니다.

매개 변수	설정	설명
archive_log_EXT	file_extension을 선택합니다	아카이브 로그 파일을 지정합니다 연장 길이. 예를 들어, 가 인 경우 보관 로그는 입니다 log_backup_0_0_0_0.16151855 1942 9 및 file_extension 값이 5인 경우 그러면 로그 확장이 이루어집니다 16151인 5자리 숫자를 유지합니다.
archive_log_recursive_se 를 선택합니다 아키텍처	(예/아니요)	아카이브 관리를 활성화합니다 하위 디렉터리 내의 로그 여러분 가 있는 경우 이 매개변수를 사용해야 합니다 아카이브 로그는 에 있습니다 하위 디렉터리.

SAP HANA Linux 플러그인 시스템에서는 맞춤형 키 값 쌍이 지원되며, 중앙 집중식 Windows 플러그인으로 등록된 SAP HANA 데이터베이스는 지원되지 않습니다.

c. 스냅샷 복사본 툴 * 화살표를 클릭하여 스냅샷 복사본을 생성할 툴을 선택합니다.

원하는 작업	그러면...
SnapCenter - Windows용 플러그인을 사용하고 스냅샷 복사본을 생성하기 전에 파일 시스템을 일관된 상태로 둡니다. Linux 리소스의 경우 이 옵션을 적용할 수 없습니다.	파일 시스템 정합성 보장 * 이 있는 SnapCenter를 선택합니다. 이 옵션은 SAP HANA 데이터베이스용 SnapCenter 플러그인에는 적용되지 않습니다.
SnapCenter를 사용하여 스토리지 레벨의 스냅샷 복사본을 생성합니다	파일 시스템 일관성 없이 SnapCenter * 를 선택합니다.
호스트에서 실행할 명령을 입력하여 스냅샷 복사본을 생성합니다.	기타 * 를 선택한 다음 호스트에서 실행할 명령을 입력하여 스냅샷 복사본을 생성합니다.

7. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

* 를 클릭하여 정책을 생성할 수도 있습니다 + *.

선택한 정책에 대한 스케줄 구성 섹션에 정책이 나열됩니다.

b. Configure Schedules 열에서 * 를 클릭합니다 + 구성할 정책에 대해 * 를 선택합니다.

c. policy_policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 * 확인 * 을 클릭합니다.

여기서 policy_name은 선택한 정책의 이름입니다.

구성된 스케줄은 * Applied Schedules * 열에 나열됩니다.

타사 백업 스케줄은 SnapCenter 백업 스케줄과 겹치는 경우 지원되지 않습니다.

8. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. SMTP 서버는 * 설정 * > * 글로벌 설정 * 에서 구성해야 합니다.

9. 요약을 검토하고 * Finish * 를 클릭합니다.

SAP HANA 데이터베이스 백업

자원이 아직 자원 그룹에 속하지 않은 경우 자원 페이지에서 자원을 백업할 수 있습니다.

시작하기 전에

- 백업 정책을 만들어야 합니다.
- 보조 스토리지와 SnapMirror 관계가 있는 리소스를 백업하려면 스토리지 사용자에게 할당된 ONTAP 역할에 "'스냅샷 전체' 권한이 있어야 합니다. 그러나 "vsadmin" 역할을 사용하는 경우에는 "napmirror all" 권한이 필요하지 않습니다.
- 스냅샷 복사본 기반 백업 작업의 경우 모든 테넌트 데이터베이스가 유효하고 활성 상태인지 확인합니다.
- SAP HANA 시스템 복제 백업을 생성하려면 SAP HANA 시스템의 모든 리소스를 하나의 리소스 그룹에 추가하는 것이 좋습니다. 이렇게 하면 Takeover-failback 모드 중에 원활한 백업이 보장됩니다.

  "리소스 그룹을 생성하고 정책을 연결합니다".

  "리소스 그룹을 백업합니다"

- 하나 이상의 테넌트 데이터베이스가 다운될 때 파일 기반 백업을 생성하려면 을 사용하여 HANA 속성 파일에서 allow_file_based_backup_IFINACTIVE_Tenants_present 매개 변수를 * Yes * 로 설정합니다 `Set-SmConfigSettings` cmdlet.

  cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 get-Help_command_name_을 실행하여 얻을 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드"

- 일시 중지, 스냅샷 복사 및 정지 해제 작업에 대한 사전 및 사후 명령의 경우 플러그인 호스트에서 사용할 수 있는 명령 목록에 다음 경로의 명령이 있는지 확인해야 합니다.

  Windows의 경우:_C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt_

  Linux의 경우: */var/opt/snapcenter/SCC/allowed_commands_list.txt*

명령이 명령 목록에 없으면 작업이 실패합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 유형에 따라 리소스를 필터링합니다.

   를 선택합니다 를 선택한 다음 호스트 이름과 리소스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 을 선택할 수 있습니다 를 눌러 필터 창을 닫습니다.
3. 백업할 리소스를 선택합니다.
4. 리소스 페이지에서 * 스냅샷 복사본에 대해 사용자 지정 이름 형식 사용 * 을 선택한 다음 스냅샷 복사본 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

   예: *customtext_policy_hostname_or_resource_hostname*. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.
5. 응용 프로그램 설정 페이지에서 다음을 실행합니다.
   - 백업 * 화살표를 선택하여 추가 백업 옵션을 설정합니다.

     필요한 경우 정합성 보장 그룹 백업을 설정하고 다음 작업을 수행합니다.

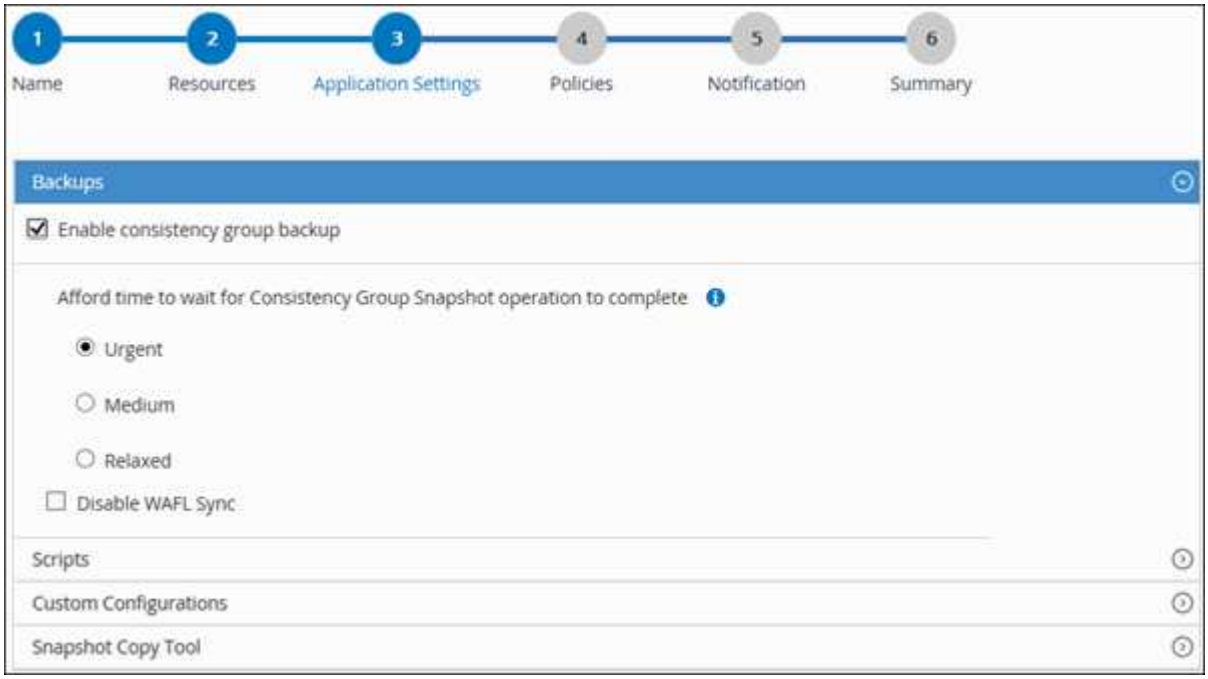
이 필드의 내용...	수행할 작업...
"정합성 보장 그룹 스냅샷" 작업이 완료될 때까지 기다릴 여유가 없습니다	스냅샷 복사 작업이 완료될 때까지 대기 시간을 지정하려면 * 긴급 *, * 중간 * 또는 * 완화된 * 을 선택합니다. 긴급 = 5초, 중간 = 7초, 휴식 = 20초
WAFL 동기화를 비활성화합니다	WAFL 정합성 보장 지점을 강제로 사용하지 않으려면 이 옵션을 선택합니다.

   - Quiesce, Snapshot copy 및 unquiesce 작업에 대한 사전 및 사후 명령을 실행하려면 * Scripts * 화살표를 선택합니다.

     백업 작업을 종료하기 전에 사전 명령을 실행할 수도 있습니다. 사전 스크립트 및 사후 스크립트는 SnapCenter 서버에서 실행됩니다.
   - 사용자 정의 구성** 화살표를 선택한 다음 이 자원을 사용하는 모든 작업에 필요한 사용자 정의 값 쌍을 입력합니다.
   - 스냅샷 복사본을 생성할 툴을 선택하려면 * 스냅샷 복사본 툴 * 화살표를 선택하십시오.

원하는 작업	그러면...
SnapCenter 를 사용하여 스토리지 수준의 스냅샷 복사본을 생성합니다	파일 시스템 일관성 없이 SnapCenter * 를 선택합니다.

원하는 작업	그러면...
SnapCenter: Windows용 플러그인을 사용하여 파일 시스템을 일관된 상태로 전환한 다음 스냅샷 복사본을 생성합니다	파일 시스템 정합성 보장 * 이 있는 SnapCenter를 선택합니다.
명령을 입력하여 스냅샷 복사본을 생성합니다	기타 * 를 선택한 다음 명령을 입력하여 스냅샷 복사본을 생성합니다.



6. 정책 페이지에서 다음 단계를 수행합니다.

   a. 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

      * 를 클릭하여 정책을 생성할 수도 있습니다 + *.

      선택한 정책에 대한 스케줄 구성 섹션에 선택한 정책이 나열됩니다.

   b. 를 선택합니다 + 일정을 구성하려는 정책에 대한 스케줄 구성 열의

   c. policy_policy_name_에 대한 스케줄 추가 대화 상자에서 스케줄을 구성한 다음 * OK * 를 선택합니다.

      _policy_name_은 선택한 정책의 이름입니다.

   구성된 일정이 Applied Schedules 열에 나열됩니다.

7. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. SMTP는 * 설정 * > * 글로벌 설정 * 에서도 구성해야 합니다.

8. 요약을 검토한 후 * Finish * 를 선택합니다.

   리소스 토폴로지 페이지가 표시됩니다.

9. 지금 백업 * 을 선택합니다.
10. 백업 페이지에서 다음 단계를 수행하십시오.
    a. 리소스에 여러 정책을 적용한 경우 * 정책 * 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

       필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

    b. 백업 * 을 선택합니다.
11. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.
    - MetroCluster 구성에서 SnapCenter는 페일오버 후 보호 관계를 감지하지 못할 수 있습니다.

      자세한 내용은 다음을 참조하십시오. "MetroCluster 페일오버 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다"

    - VMDK에서 애플리케이션 데이터를 백업하고 VMware vSphere용 SnapCenter 플러그인의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다.

      Java 힙 크기를 늘리려면 스크립트 파일 _/opt/netapp/init_scripts/scvservice_를 찾습니다. 이 스크립트에서 _do_start method_command는 SnapCenter VMware 플러그인 서비스를 시작합니다. 이 명령을 _java-jar-Xmx8192M-Xms4096M_로 업데이트합니다

리소스 그룹을 백업합니다

리소스 그룹은 호스트의 리소스 모음입니다. 리소스 그룹에 대한 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다.

시작하기 전에

- 정책이 연결된 리소스 그룹을 만들어야 합니다.
- 보조 스토리지와 SnapMirror 관계가 있는 리소스를 백업하려면 스토리지 사용자에게 할당된 ONTAP 역할에 "'스냅샷 전체' 권한이 있어야 합니다. 그러나 "vsadmin" 역할을 사용하는 경우에는 "napmirror all" 권한이 필요하지 않습니다.

이 작업에 대해

리소스 페이지에서 필요 시 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 연결되어 있고 스케줄이 구성되어 있는 경우 스케줄에 따라 백업이 자동으로 수행됩니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 리소스 그룹 * 을 선택합니다.

   검색 상자에 리소스 그룹 이름을 입력하거나 를 선택하여 리소스 그룹을 검색할 수 있습니다 을 클릭한 다음 태그를 선택합니다. 그런 다음 을 선택할 수 있습니다 를 눌러 필터 창을 닫습니다.

3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음 * 지금 백업 * 을 선택합니다.
4. 백업 페이지에서 다음 단계를 수행하십시오.
   a. 여러 정책을 리소스 그룹에 연결한 경우 * Policy * 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

      필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

   b. 백업 * 을 선택합니다.
5. Monitor * > * Jobs * 를 선택하여 작업 진행 상황을 모니터링합니다.

SAP HANA 데이터베이스용 PowerShell cmdlet을 사용하여 스토리지 시스템 연결과 자격 증명을 생성합니다

PowerShell cmdlet을 사용하여 SAP HANA 데이터베이스를 백업, 복원 또는 클론 복제하기 전에 SVM(Storage Virtual Machine) 연결과 자격 증명을 생성해야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행할 수 있도록 PowerShell 환경을 준비해야 합니다.
- 스토리지 접속을 생성하려면 인프라스트럭처 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

  호스트 캐시가 업데이트되지 않고 데이터베이스 상태가 SnapCenter GUI에 ""백업을 위해 사용할 수 없음"" 또는 ""NetApp 스토리지에 없음""으로 표시될 수 있으므로 스토리지 시스템 접속을 추가하는 동안 호스트 플러그인 설치가 진행되어서는 안 됩니다.

- 스토리지 시스템 이름은 고유해야 합니다.

  SnapCenter는 서로 다른 클러스터에서 동일한 이름의 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 접속을 생성합니다.

```
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 FinanceAdmin 이라는 새 자격 증명을 만드는 방법을 보여 줍니다.

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. SnapCenter Server에 SAP HANA 통신 호스트를 추가합니다.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode hana
```

5. 패키지 및 SAP HANA 데이터베이스용 SnapCenter 플러그인을 호스트에 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 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

PowerShell cmdlet을 사용하여 데이터베이스를 백업합니다

데이터베이스 백업에는 SnapCenter 서버와의 연결 설정, 리소스 추가, 정책 추가, 백업 리소스

그룹 생성 및 백업이 포함됩니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 스토리지 시스템 접속을 추가하고 자격 증명을 생성해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146\
```

사용자 이름 및 암호 프롬프트가 표시됩니다.

2. Add-SmResources cmdlet을 사용하여 리소스를 추가합니다.

이 예제에서는 SingleContainer 형식의 SAP HANA 데이터베이스를 추가하는 방법을 보여 줍니다.

```
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 MultipleContainer 유형의 SAP HANA 데이터베이스를 추가하는 방법을 보여 줍니다.

```
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.netapp.
com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType 'MultiTenant'
```

이 예에서는 비 데이터 볼륨 리소스를 생성하는 방법을 보여 줍니다.

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sccore.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 예에서는 스냅샷 복사본 기반 백업에 대한 백업 정책을 생성합니다.

```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType Backup
-PluginPolicyType hana -BackupType SnapShotBasedBackup
```

이 예에서는 파일 기반 백업에 대한 백업 정책을 생성합니다.

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
-PluginPolicyType hana -BackupType FileBasedBackup
```

4. 추가 SmResourceGroup cmdlet을 사용하여 리소스를 보호하거나 SnapCenter에 새 리소스 그룹을 추가합니다.

이 예에서는 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 예에서는 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 정책 및 리소스를 사용하여 새 리소스 그룹을 만듭니다.

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sccore.test.com";"Uid"="SID"},@{"Host"="sccore
linux62.sccore.test.com";"Uid"="MDC\SID"})
  -Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency  -plugincode 'HANA'
```

이 예에서는 데이터 볼륨이 아닌 리소스 그룹을 생성합니다.

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="H11";"PluginName"="han
a"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="MDC\H31";"PluginName
"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="NonDataVolume\
S10\NonDataVolume";"PluginName"="hana"}) -Policies hanaprimary
```

5. New-SmBackup cmdlet을 사용하여 새 백업 작업을 시작합니다.

   이 예제에서는 리소스 그룹을 백업하는 방법을 보여 줍니다.

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

   다음 예에서는 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 백업 ID, 백업 이름과 같은 백업 작업 세부 정보를 모니터링하여 복원 또는 클론 작업을 수행합니다.

```
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 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

백업 작업을 모니터링합니다

SAP HANA 데이터베이스 백업 작업 모니터링

SnapCenterJobs 페이지를 사용하여 여러 백업 작업의 진행률을 모니터링할 수 있습니다. 진행 상황을 확인하여 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

다음 아이콘이 작업 페이지에 나타나고 작업의 해당 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다

- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨

단계

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 모니터 페이지에서 * 작업 * 을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행하십시오.
   a. 을 클릭합니다 백업 작업만 나열되도록 목록을 필터링합니다.
   b. 시작 및 종료 날짜를 지정합니다.
   c. Type * 드롭다운 목록에서 * Backup * 을 선택합니다.
   d. Status * (상태 *) 드롭다운에서 백업 상태를 선택합니다.
   e. 작업이 성공적으로 완료되었는지 보려면 * Apply * 를 클릭합니다.
4. 백업 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.

   백업 작업 상태가 표시됩니다 작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 기호로 표시되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 * 로그 보기 * 를 클릭합니다.

   로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

활동 창에서 **SAP HANA** 데이터베이스의 데이터 보호 작업을 모니터링합니다

작업 창에는 가장 최근에 수행한 작업 5개가 표시됩니다. 작업 창은 작업이 시작된 시점과 작업의 상태도 표시합니다.

작업 창에는 백업, 복원, 클론 및 예약된 백업 작업에 대한 정보가 표시됩니다. SQL Server용 플러그인 또는 Exchange Server용 플러그인을 사용하는 경우 작업 창에 다시 시드된 작업에 대한 정보도 표시됩니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 을 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다.

   작업 중 하나를 클릭하면 작업 세부 정보가 * 작업 세부 정보 * 페이지에 나열됩니다.

SAP HANA의 백업 작업을 취소합니다

대기열에 있는 백업 작업을 취소할 수 있습니다.

- 필요한 것 *
- 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

- 모니터 * 페이지 또는 * 작업 * 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 작업에 대해 * 작업 취소 * 버튼이 비활성화됩니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 사용자\그룹 페이지에서 다른 구성원 개체를 보고 작동할 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.

시작...	조치
모니터 페이지	a. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 클릭합니다. b. 작업을 선택한 다음 * 작업 취소 * 를 클릭합니다.
작업 창	a. 백업 작업을 시작한 후 * 를 클릭합니다 * 를 클릭합니다. b. 작업을 선택합니다. c. 작업 세부 정보 페이지에서 * 작업 취소 * 를 클릭합니다.

작업이 취소되고 리소스가 이전 상태로 돌아갑니다.

토폴로지 페이지에서 **SAP HANA** 데이터베이스 백업 및 클론 보기

리소스를 백업 또는 복제할 때 운영 스토리지와 보조 스토리지의 모든 백업 및 클론을 그래픽으로 표시하는 것이 유용할 수 있습니다.

이 작업에 대해

복제본 관리 보기에서 다음 아이콘을 검토하여 운영 스토리지 또는 보조 스토리지(미러 복사본 또는 볼트 복제본)에서 백업과 클론을 사용할 수 있는지 확인할 수 있습니다.

-  기본 스토리지에서 사용할 수 있는 백업 및 클론 수를 표시합니다.
-  SnapMirror 기술을 사용하여 보조 스토리지에 미러링된 백업 및 클론 수를 표시합니다.
-  SnapVault 기술을 사용하여 보조 스토리지에 복제된 백업 및 클론 수를 표시합니다.

표시된 백업 수에는 보조 스토리지에서 삭제된 백업이 포함됩니다. 예를 들어 정책을 사용하여 6개의 백업을 생성하여 4개의 백업만 보존한 경우 표시되는 백업 수는 6입니다.

미러 볼트 유형 볼륨에 있는 버전에 따라 유연한 미러 백업의 클론은 토폴로지 뷰에 표시되지만 토폴로지 뷰에 있는 미러 백업 횟수에는 버전에 따라 유연하게 백업할 수 있는 백업이 포함되지 않습니다.

SAP HANA 시스템 복제 운영 리소스의 경우 복원 및 삭제 작업이 지원되며 2차 리소스의 경우 클론 작업이 지원됩니다.

토폴로지 페이지에서 선택한 리소스 또는 리소스 그룹에 사용할 수 있는 모든 백업 및 클론을 볼 수 있습니다. 이러한 백업 및 클론의 세부 정보를 확인한 다음 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 자원 세부 정보 보기 또는 자원 그룹 세부 정보 보기에서 자원을 선택합니다.

   리소스가 보호되는 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. 요약 카드 * 를 검토하여 기본 및 보조 스토리지에서 사용할 수 있는 백업 및 클론 수를 요약합니다.

   요약 카드 * 섹션에는 파일 기반 백업, 스냅샷 복사본 백업 및 클론의 총 수가 표시됩니다.

   Refresh * 버튼을 클릭하면 스토리지 쿼리가 시작되어 정확한 카운트를 표시합니다.

5. 복사본 관리 보기에서 기본 또는 보조 스토리지에서 * 백업 * 또는 * 클론 * 을 클릭하여 백업 또는 클론의 세부 정보를 확인합니다.

   백업 및 클론의 세부 정보가 표 형식으로 표시됩니다.

6. 테이블에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 클론 복제 및 삭제 작업을 수행합니다.

   보조 스토리지에 있는 백업의 이름을 바꾸거나 백업을 삭제할 수 없습니다.

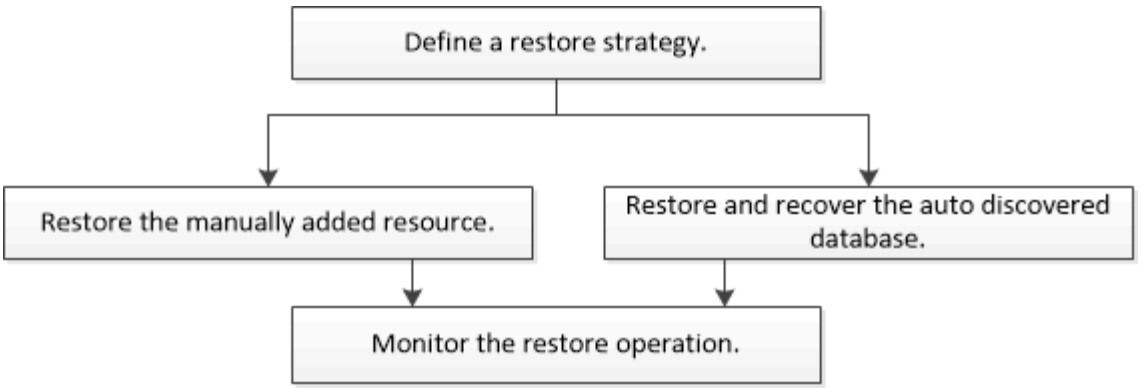
7. 클론을 삭제하려면 표에서 클론을 선택한 다음 을 클릭합니다  .
8. 클론을 분할하려면 테이블에서 클론을 선택한 다음 을 클릭합니다  .

SAP HANA 데이터베이스 복원

워크플로를 복원합니다

복원 및 복구 워크플로에는 계획, 복원 작업 수행 및 작업 모니터링이 포함됩니다.

다음 워크플로에서는 복원 작업을 수행해야 하는 순서를 보여 줍니다.



PowerShell cmdlet을 수동으로 사용하거나 스크립트에서 사용하여 백업, 복원 및 클론 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말 및 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

"SnapCenter 소프트웨어 cmdlet 참조 가이드".

수동으로 추가한 리소스 백업을 복원 및 복구합니다

SnapCenter를 사용하여 하나 이상의 백업에서 데이터를 복원 및 복구할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 복원할 리소스 또는 리소스 그룹에 대해 현재 진행 중인 백업 작업을 취소해야 합니다.
- 사전 복원, 사후 복원, 마운트 및 마운트 해제 명령의 경우 다음 경로에서 플러그인 호스트에서 사용할 수 있는 명령 목록에 명령이 있는지 확인해야 합니다.

  Windows의 경우:_C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt_

  Linux의 경우: */var/opt/snapcenter/SCC/allowed_commands_list.txt*

  명령이 명령 목록에 없으면 작업이 실패합니다.

이 작업에 대해

- SnapCenter에서 파일 기반 백업 복사본을 복원할 수 없습니다.
- SnapCenter 4.3으로 업그레이드한 후 SnapCenter 4.2에서 수행된 백업을 복원할 수 있지만 복구할 수는 없습니다. SnapCenter 4.2에서 수행된 백업을 복구하려면 SnapCenter 외부에 있는 HANA Studio 또는 HANA 복구 스크립트를 사용해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 유형에 따라 리소스를 필터링합니다.

   리소스는 유형, 호스트, 관련 리소스 그룹 및 정책, 상태와 함께 표시됩니다.

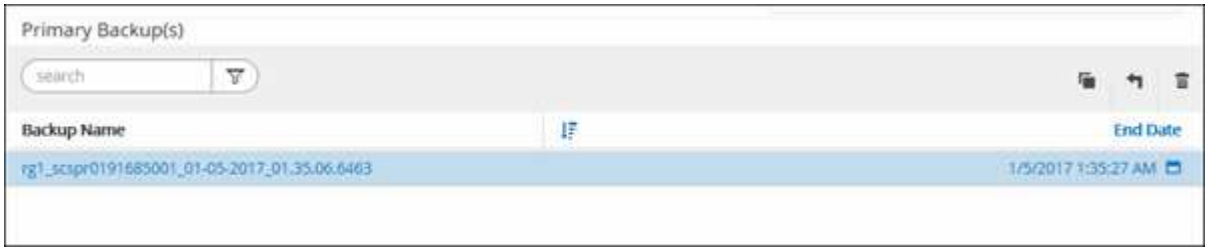
   백업이 리소스 그룹에 대한 것일 수도 있지만 복원할 때 복원할 개별 리소스를 선택해야 합니다.

자원이 보호되지 않으면 전체 상태 열에 "보호되지 않음"이 표시됩니다. 이는 리소스가 보호되지 않거나 다른 사용자가 리소스를 백업했다는 것을 의미할 수 있습니다.

3. 자원을 선택하거나 자원 그룹을 선택한 다음 해당 그룹에서 자원을 선택합니다.

   리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 보관된) 스토리지 시스템에서 * 백업 * 을 선택합니다.
5. 기본 백업 테이블에서 복원할 백업을 선택한 다음 * 를 클릭합니다 *.



6. 복원 범위 페이지에서 * 전체 리소스 * 또는 * 파일 수준 * 을 선택합니다.

   a. Complete Resource * 를 선택하면 SAP HANA 데이터베이스의 구성된 모든 데이터 볼륨이 복원됩니다.

      리소스에 볼륨 또는 qtree가 포함된 경우, 해당 볼륨 또는 qtree에서 복원하도록 선택된 Snapshot 복사본 이후에 생성된 스냅샷 복사본은 삭제되고 복구할 수 없습니다. 또한 동일한 볼륨 또는 qtree에서 다른 리소스가 호스트되는 경우 해당 리소스도 삭제됩니다.

   b. 파일 수준 * 을 선택한 경우 * 모두 * 를 선택하거나 특정 볼륨 또는 qtree를 선택한 다음 해당 볼륨 또는 qtree와 관련된 경로를 쉼표로 구분하여 입력할 수 있습니다

      - 여러 볼륨 및 qtree를 선택할 수 있습니다.
      - 리소스 유형이 LUN이면 전체 LUN이 복구됩니다.

        여러 LUN을 선택할 수 있습니다.

   All * 을 선택하면 볼륨, Qtree 또는 LUN의 모든 파일이 복원됩니다.

7. 복구 작업을 수행하기 전에 Pre restore 및 unmount 명령을 Pre ops 페이지에 입력합니다.

   자동 검색 리소스에 대해서는 마운트 해제 명령을 사용할 수 없습니다.

8. 작업 게시 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.

   자동 검색 리소스에 대해서는 마운트 명령을 사용할 수 없습니다.

9. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. SMTP는 * 설정 * > * 글로벌 설정 * 페이지에서도 구성해야 합니다.

10. 요약을 검토하고 * Finish * 를 클릭합니다.
11. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

자동 검색된 데이터베이스 백업을 복원 및 복구합니다

SnapCenter를 사용하여 하나 이상의 백업에서 데이터를 복원 및 복구할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 복원할 리소스 또는 리소스 그룹에 대해 현재 진행 중인 백업 작업을 취소해야 합니다.
- 사전 복원, 사후 복원, 마운트 및 마운트 해제 명령의 경우 다음 경로에서 플러그인 호스트에서 사용할 수 있는 명령 목록에 명령이 있는지 확인해야 합니다.

  Windows의 경우:_C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt_

  Linux의 경우: */var/opt/snapcenter/SCC/allowed_commands_list.txt*

  명령이 명령 목록에 없으면 작업이 실패합니다.

이 작업에 대해

- SnapCenter에서 파일 기반 백업 복사본을 복원할 수 없습니다.
- SnapCenter 4.3으로 업그레이드한 후 SnapCenter 4.2에서 수행된 백업을 복원할 수 있지만 복구할 수는 없습니다. SnapCenter 4.2에서 수행된 백업을 복구하려면 SnapCenter 외부에 있는 HANA Studio 또는 HANA 복구 스크립트를 사용해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 유형에 따라 리소스를 필터링합니다.

   리소스는 유형, 호스트, 관련 리소스 그룹 및 정책, 상태와 함께 표시됩니다.

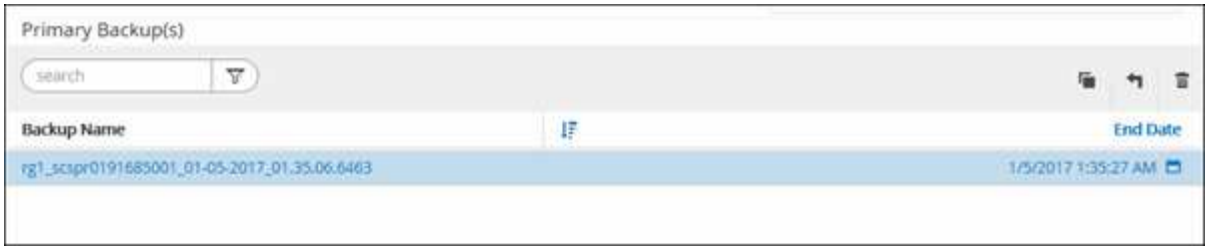
   백업이 리소스 그룹에 대한 것일 수도 있지만 복원할 때 복원할 개별 리소스를 선택해야 합니다.

   자원이 보호되지 않으면 전체 상태 열에 "보호되지 않음"이 표시됩니다. 이는 리소스가 보호되지 않거나 다른 사용자가 리소스를 백업했다는 것을 의미할 수 있습니다.

3. 자원을 선택하거나 자원 그룹을 선택한 다음 해당 그룹에서 자원을 선택합니다.

   리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 보관된) 스토리지 시스템에서 * 백업 * 을 선택합니다.
5. 기본 백업 테이블에서 복원할 백업을 선택한 다음 * 를 클릭합니다 *.



6. 복구 범위 페이지에서 * Complete Resource * 를 선택하여 SAP HANA 데이터베이스의 구성된 데이터 볼륨을 복원합니다.

   전체 리소스 * (볼륨 복원 * 포함 또는 제외) 또는 * 테넌트 데이터베이스 * 를 선택할 수 있습니다.

   사용자가 * 테넌트 데이터베이스 * 또는 * 전체 복원 * 옵션을 선택하면 여러 테넌트의 경우 SnapCenter 서버가 복구 작업을 지원하지 않습니다. 복구 작업을 수행하려면 HANA Studio 또는 HANA Python 스크립트를 사용해야 합니다.

   a. 전체 볼륨을 복원하려면 * Volume Revert * 를 선택합니다.

      이 옵션은 NFS 환경의 SnapCenter 4.3에서 수행된 백업에 사용할 수 있습니다.

      리소스에 볼륨 또는 qtree가 포함된 경우, 해당 볼륨 또는 qtree에서 복원하도록 선택된 Snapshot 복사본 이후에 생성된 스냅샷 복사본은 삭제되고 복구할 수 없습니다. 또한 동일한 볼륨 또는 qtree에서 다른 리소스가 호스트되는 경우 해당 리소스도 삭제됩니다. 이 옵션은 * 볼륨 복원 * 옵션이 있는 * 전체 리소스 * 가 복원용으로 선택된 경우에 적용됩니다.

   b. Tenant Database * 를 선택합니다.

      이 옵션은 MDC 리소스에 대해서만 사용할 수 있습니다.

      복구 작업을 수행하기 전에 테넌트 데이터베이스를 중지해야 합니다.

   테넌트 데이터베이스 * 옵션을 선택한 경우 HANA Studio를 사용하거나 SnapCenter 외부의 HANA 복구 스크립트를 사용하여 복구 작업을 수행해야 합니다.

7. 복구 범위 페이지에서 다음 옵션 중 하나를 선택합니다.

만약...	수행할 작업...
현재 시간에 최대한 가깝게 복구하기를 원합니다	Recover to Most Recent state * 를 선택합니다. 단일 컨테이너 리소스의 경우 하나 이상의 로그 및 카탈로그 백업 위치를 지정합니다. MDC(멀티테넌트 데이터베이스 컨테이너) 리소스의 경우 하나 이상의 로그 백업 위치와 백업 카탈로그 위치를 지정합니다. MDC 리소스의 경우 경로에 시스템 데이터베이스와 테넌트 데이터베이스 로그가 모두 포함되어야 합니다.

만약...	수행할 작업...
지정된 시점으로 복구하려는 경우	시점으로 복구 * 를 선택합니다. a. 시간대를 선택합니다. 브라우저 시간대는 기본적으로 채워집니다. 입력 시간과 함께 선택한 시간대가 절대 GMT로 변환됩니다. b. 날짜 및 시간을 입력합니다. 예를 들어, HANA Linux 호스트는 Sunnyvale, CA에 있고, Raleigh, NC 사용자는 SnapCenter에 대한 로그를 복구하는 중입니다. 이 두 위치 간의 시간 차이는 3시간이며 사용자가 NC Raleigh에서 로그인했기 때문에 GUI에서 선택되는 기본 브라우저 시간대는 GMT-04:00입니다. 사용자가 5 a.m.Sunnyvale, CA로 복구를 수행하려는 경우 사용자는 브라우저 시간대를 HANA Linux 호스트 표준 시간대로 설정해야 합니다(GMT-07:00). 날짜와 시간은 오전 5시로 지정합니다 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 경로에 시스템 데이터베이스와 테넌트 데이터베이스 로그가 모두 포함되어야 합니다.
특정 데이터 백업으로 복구하려는 경우	지정된 데이터 백업으로 복구 * 를 선택합니다.
복구하기를 원하지 않습니다	No recovery * 를 선택합니다. HANA Studio에서 수동으로 복구 작업을 수행해야 합니다.

호스트와 플러그인이 모두 SnapCenter 4.3으로 업그레이드되고, 복구용으로 선택한 백업이 리소스를 변환 또는 자동 검색 리소스로 검색된 후에 수행된다는 전제 하에 SnapCenter 4.3으로 업그레이드한 후 수행된 백업만 복구할 수 있습니다.

8. 복구 작업을 수행하기 전에 Pre restore 및 unmount 명령을 Pre ops 페이지에 입력합니다.

   자동 검색 리소스에 대해서는 마운트 해제 명령을 사용할 수 없습니다.

9. 작업 게시 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.

자동 검색 리소스에 대해서는 마운트 명령을 사용할 수 없습니다.

10. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

    또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. SMTP는 * 설정 * > * 글로벌 설정 * 페이지에서도 구성해야 합니다.

11. 요약을 검토하고 * Finish * 를 클릭합니다.
12. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

PowerShell cmdlet을 사용하여 SAP HANA 데이터베이스를 복원합니다

SAP HANA 데이터베이스 백업을 복구하려면 SnapCenter 서버와의 연결 세션 시작, 백업 목록 표시 및 백업 정보 검색, 백업 복구가 포함됩니다.

시작하기 전에

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원할 백업을 식별합니다.

   이 예에서는 복구에 사용할 수 있는 두 개의 백업이 있음을 보여 줍니다.

```
 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 예는 2015년 1월 29일부터 2015년 2월 3일까지 백업에 대한 자세한 정보를 표시합니다.

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"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. HANA Studio에서 복구 프로세스를 시작합니다.

   데이터베이스가 종료됩니다.

4. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.

   AppObjectId는 "Host\Plugin\UID"입니다. 여기서 UID=SID는 단일 컨테이너 유형 리소스에 대한 것으로, UID=MDC\SID는 여러 컨테이너 리소스에 대한 것입니다. get-smResources cmdlet에서 ResourceID를 가져올 수 있습니다.

```
Get-smResources  -HostName cn24.sccore.test.com  -PluginCode HANA
```

이 예에서는 운영 스토리지에서 데이터베이스를 복구하는 방법을 보여 줍니다.

```
Restore-SmBackup -PluginCode HANA -AppObjectId
cn24.sccore.test.com\hana\H10 -BackupId 3
```

이 예에서는 보조 스토리지에서 데이터베이스를 복구하는 방법을 보여 줍니다.

```
Restore-SmBackup -PluginCode 'HANA' -AppObjectId
cn24.sccore.test.com\hana\H10 -BackupId 399 -Confirm:$false  -Archive @(
@{"Primary"="<Primary Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
Vserver>:<SecondaryVolume>"})
```

백업은 HANA Studio에서 복구에 사용할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

PowerShell cmdlet을 사용하여 리소스 복원

리소스 백업 복원에는 SnapCenter 서버와의 연결 세션 시작, 백업 목록 표시 및 백업 정보 검색, 백업 복구가 포함됩니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

   이 예에서는 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 예는 2015년 1월 29일부터 2015년 2월 3일까지 백업에 대한 자세한 정보를 표시합니다.

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"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.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                 : Restore
'scc54.sccore.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 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

SAP HANA 데이터베이스 복원 작업을 모니터링합니다

작업 페이지를 사용하여 여러 SnapCenter 복원 작업의 진행률을 모니터링할 수 있습니다. 작업 진행률을 확인하여 작업이 언제 완료되는지 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

복원 후 상태는 복원 작업 후 리소스의 상태와 수행할 수 있는 추가 복원 작업에 대해 설명합니다.

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다

- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨

단계

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 모니터 * 페이지에서 * 작업 * 을 클릭합니다.
3. Jobs * 페이지에서 다음 단계를 수행하십시오.
   a. 을 클릭합니다 복원 작업만 나열되도록 목록을 필터링하려면
   b. 시작 및 종료 날짜를 지정합니다.
   c. Type * 드롭다운 목록에서 * Restore * 를 선택합니다.
   d. Status * (상태 *) 드롭다운 목록에서 복원 상태를 선택합니다.
   e. 성공적으로 완료된 작업을 보려면 * 적용 * 을 클릭합니다.
4. 복원 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. Job Details * 페이지에서 * View logs * 를 클릭합니다.

   로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

볼륨 기반 복원 작업 후에는 백업 메타데이터가 SnapCenter 저장소에서 삭제되지만 백업 카탈로그 항목은 SAP HANA 카탈로그에 남아 있습니다. 복원 작업 상태가 표시됩니다 작업 세부 정보를 클릭하여 일부 하위 작업의 경고 표시를 확인해야 합니다. 경고 표지를 클릭하고 표시된 백업 카탈로그 항목을 삭제합니다.

SAP HANA 리소스 백업의 클론을 생성합니다

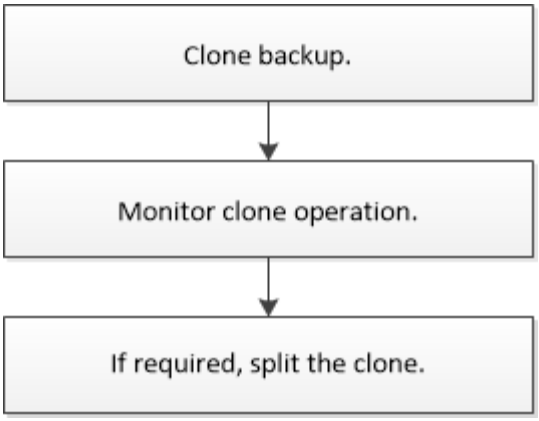
클론 복제 워크플로우

클론 워크플로우에는 클론 작업 수행 및 작업 모니터링이 포함됩니다.

이 작업에 대해

- 소스 SAP HANA 서버에서 클론을 생성할 수 있습니다.
- 다음과 같은 이유로 리소스 백업을 복제할 수 있습니다.
  - 응용 프로그램 개발 주기 동안 현재 리소스 구조 및 콘텐츠를 사용하여 구현해야 하는 기능을 테스트합니다
  - 데이터 웨어하우스를 채울 때 데이터 추출 및 조작 도구를 위한 것입니다
  - 실수로 삭제 또는 변경된 데이터를 복구합니다

다음 워크플로에서는 클론 작업을 수행해야 하는 순서를 보여 줍니다.



PowerShell cmdlet을 수동으로 사용하거나 스크립트에서 사용하여 백업, 복원 및 클론 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말 및 cmdlet 참조 정보에는 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

SAP HANA 데이터베이스 백업의 클론을 생성합니다

SnapCenter를 사용하여 백업을 복제할 수 있습니다. 기본 또는 보조 백업에서 클론을 생성할 수 있습니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 볼륨을 호스팅하는 애그리게이트는 SVM(스토리지 가상 머신)의 할당된 애그리게이트 목록에 있어야 합니다.
- 파일 기반 백업의 클론은 생성할 수 없습니다.
- 타겟 클론 서버에는 타겟 클론 SID 필드에 제공되는 것과 동일한 SAP HANA 인스턴스 SID가 있어야 합니다.
- 사전 클론 생성 또는 사후 클론 명령의 경우 플러그인 호스트에서 사용할 수 있는 명령 목록에 다음 경로의 명령이 있는지 확인해야 합니다.

  Windows의 경우:_C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt_

  Linux의 경우: */var/opt/snapcenter/SCC/allowed_commands_list.txt*

  명령이 명령 목록에 없으면 작업이 실패합니다.

이 작업에 대해

클론 분할 작업 제한에 대한 자세한 내용은 을 참조하십시오 "ONTAP 9 논리적 스토리지 관리 가이드".

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 유형에 따라 리소스를 필터링합니다.

   리소스는 유형, 호스트, 관련 리소스 그룹 및 정책, 상태와 같은 정보와 함께 표시됩니다.

3. 자원 또는 자원 그룹을 선택합니다.

   자원 그룹을 선택한 경우 자원을 선택해야 합니다.

리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 보관된) 스토리지 시스템에서 * 백업 * 을 선택합니다.
5. 테이블에서 데이터 백업을 선택한 다음 을 클릭합니다  .
6. 위치 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
플러그인 호스트입니다	클론을 마운트할 호스트와 플러그인이 설치된 호스트를 선택합니다.
타겟 클론 SID	기존 백업에서 복제할 SAP HANA 인스턴스 ID를 입력합니다.
NFS 내보내기 IP 주소입니다	복제된 볼륨을 내보낼 IP 주소 또는 호스트 이름을 입력합니다.
iSCSI 초기자	LUN을 내보낼 호스트의 iSCSI 이니시에이터 이름을 입력합니다. 이 옵션은 LUN 리소스 유형을 선택한 경우에만 사용할 수 있습니다.
프로토콜	LUN 프로토콜을 입력합니다. 이 옵션은 LUN 리소스 유형을 선택한 경우에만 사용할 수 있습니다.

선택한 리소스가 LUN이고 2차 백업에서 클론을 생성하는 경우 타겟 볼륨이 나열됩니다. 단일 소스에 여러 대상 볼륨이 있을 수 있습니다.

클론 복제 전에 iSCSI 이니시에이터 또는 FCP가 존재하고 대체 호스트에 구성 및 로그인되어 있는지 확인해야 합니다.

7. 스크립트 페이지에서 다음 단계를 수행합니다.

이 스크립트는 플러그인 호스트에서 실행됩니다.

a. 클론 작업 전후에 각각 실행해야 하는 사전 클론 또는 사후 클론 명령을 입력합니다.
   - Pre clone 명령: 이름이 같은 기존 데이터베이스를 삭제합니다
   - 사후 복제 명령: 데이터베이스를 확인하거나 데이터베이스를 시작합니다.

b. mount 명령을 입력하여 호스트에 파일 시스템을 마운트합니다.

   Linux 시스템의 볼륨 또는 qtree에 대한 마운트 명령:

   NFS의 예:

```
mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt
```

8. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다.

9. 요약을 검토하고 * Finish * 를 클릭합니다.
10. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

PowerShell cmdlet을 사용하여 SAP HANA 데이터베이스 백업 클론 생성

클론 워크플로우에는 계획, 클론 작업 수행 및 작업 모니터링이 포함됩니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Get-SmBackup cmdlet을 사용하여 클론 작업을 수행할 백업을 검색합니다.

   이 예에서는 클론 복제에 두 개의 백업을 사용할 수 있음을 보여 줍니다.

```
 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 클론 작업을 시작하고 클론 볼륨을 내보낼 NFS 엑스포트 IP 주소를 지정합니다.

   이 예에서는 클론할 백업에 10.232.206.169의 NFSExportIP 주소가 있음을 보여 줍니다.

```
New-SmClone -AppPluginCode hana -BackupName
scsccore1_sccore_test_com_hana_H73_scsccore1_06-07-2017_02.54.29.3817
-Resources @{"Host"="scsccore1.sccore.test.com";"Uid"="H73"}
-CloneToInstance shivscc4.sccore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data' -preclonecreatecommands
'/home/scripts/scpre_clone.sh' -postclonecreatecommands
'/home/scripts/scpost_clone.sh'
```

NFSExportIP가 지정되지 않으면 기본값이 클론 타겟 호스트로 내보내집니다.

4. Get-SmCloneReport cmdlet을 사용하여 클론 작업 세부 정보를 확인하여 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 클론 작업을 모니터링합니다

작업 페이지를 사용하여 SnapCenter 클론 작업의 진행률을 모니터링할 수 있습니다. 작업 진행률을 확인하여 작업이 언제 완료되는지 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨
- 단계 *

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 모니터 * 페이지에서 * 작업 * 을 클릭합니다.
3. Jobs * 페이지에서 다음 단계를 수행하십시오.
   a. 을 클릭합니다 클론 작업만 나열되도록 목록을 필터링합니다.
   b. 시작 및 종료 날짜를 지정합니다.
   c. Type * 드롭다운 목록에서 * Clone * 을 선택합니다.
   d. Status * (상태 *) 드롭다운 목록에서 클론 상태를 선택합니다.
   e. 성공적으로 완료된 작업을 보려면 * 적용 * 을 클릭합니다.
4. 클론 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. 작업 세부 정보 페이지에서 * 로그 보기 * 를 클릭합니다.

클론 분할

SnapCenter를 사용하여 상위 리소스에서 복제된 리소스를 분할할 수 있습니다. 분할되는 클론은 상위 리소스와 독립적입니다.

이 작업에 대해

- 중간 클론에는 클론 분할 작업을 수행할 수 없습니다.

  예를 들어 데이터베이스 백업에서 clone1을 생성한 후 clone1의 백업을 생성한 다음 이 백업(clone2)을 클론 복제할 수 있습니다. clone2를 생성한 후에는 clone1이 중간 클론이며 clone1에서 클론 분할 작업을 수행할 수 없습니다. 그러나 clone2에서 클론 분할 작업을 수행할 수 있습니다.

  clone2를 분할한 후에는 clone1이 더 이상 중간 클론이 아니기 때문에 clone1에서 클론 분할 작업을 수행할 수 있습니다.

- 클론을 분할하면 클론의 백업 복사본 및 클론 작업이 삭제됩니다.
- 클론 분할 작업 제한에 대한 자세한 내용은 을 참조하십시오 "ONTAP 9 논리적 스토리지 관리 가이드".
- 스토리지 시스템의 볼륨 또는 애그리게이트는 온라인 상태인지 확인합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. Resources * 페이지의 View 목록에서 적절한 옵션을 선택합니다.

옵션을 선택합니다	설명
성능을 대폭 향상	보기 목록에서 * 데이터베이스 * 를 선택합니다.
파일 시스템의 경우	보기 목록에서 * 경로 * 를 선택합니다.

3. 목록에서 적절한 리소스를 선택합니다.

   리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 * 보기에서 복제된 리소스(예: 데이터베이스 또는 LUN)를 선택한 다음 * 를 클릭합니다 *.
5. 분할할 클론의 예상 크기와 애그리게이트에서 사용할 수 있는 필수 공간을 검토한 다음 * 시작 * 을 클릭합니다.
6. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

   SMCore 서비스가 다시 시작되면 클론 분할 작업이 응답하지 않습니다. Stop-SmJob cmdlet을 실행하여 클론 분할 작업을 중지한 다음 클론 분할 작업을 다시 시도해야 합니다.

   폴링 시간을 더 오래 설정하거나 폴링 시간을 짧게 하여 클론이 분할되었는지 여부를 확인하려면 _SMCoreServiceHost.exe.config_file에서 _CloneSplitStatusCheckPollTime_parameter 값을 변경하여 SMCore가 클론 분할 작업의 상태를 폴링할 시간 간격을 설정할 수 있습니다. 값은 밀리초이고 기본값은 5분입니다.

   예를 들면 다음과 같습니다.

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

   백업, 복원 또는 다른 클론 분할이 진행 중인 경우 클론 분할 시작 작업이 실패합니다. 실행 중인 작업이 완료된 후에만 클론 분할 작업을 다시 시작해야 합니다.

관련 정보

"Aggregate가 존재하지 않으면 SnapCenter 클론 또는 검증에 실패합니다"

SnapCenter를 업그레이드한 후 SAP HANA 데이터베이스 복제본을 삭제하거나 분할합니다

SnapCenter 4.3으로 업그레이드한 후 더 이상 클론이 표시되지 않습니다. 클론을 생성한 리소스의 토폴로지 페이지에서 클론을 삭제하거나 클론을 분할할 수 있습니다.

이 작업에 대해

숨겨진 클론의 스토리지 공간을 찾으려면 다음 명령을 실행합니다. `Get-SmClone -ListStorageFootprint`

단계

1. remove-smbackup 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. 자원 페이지에서 상위 자원을 선택합니다.

   리소스 토폴로지 페이지가 표시됩니다.

5. Manage Copies 보기의 운영 또는 2차(미러링 또는 복제) 스토리지 시스템에서 클론을 선택합니다.
6. 클론을 선택한 다음 을 클릭합니다  를 클릭하여 클론을 삭제하거나 을 클릭합니다  를 눌러 클론을 분할합니다.
7. 확인 * 을 클릭합니다.

Oracle 데이터베이스 보호

Oracle 데이터베이스용 SnapCenter 플러그인 개요

Oracle 데이터베이스용 플러그인을 사용하여 수행할 수 있는 작업

Oracle 데이터베이스용 SnapCenter 플러그인은 Oracle 데이터베이스의 애플리케이션 인식 데이터 보호 관리를 지원하는 NetApp SnapCenter 소프트웨어의 호스트 측 구성 요소입니다.

Oracle Database용 플러그인은 Oracle RMAN(Recovery Manager), 검증, 마운트, 마운트 해제, 복구, SnapCenter 환경에서 Oracle 데이터베이스의 복구 및 클론 복제
Oracle 데이터베이스용 플러그인은 모든 데이터 보호 작업을 수행하기 위해 UNIX용 SnapCenter 플러그인을 설치합니다.

Oracle 데이터베이스용 플러그인을 사용하여 SAP 애플리케이션을 실행하는 Oracle 데이터베이스의 백업을 관리할 수 있습니다. 그러나 SAP BR * Tools 통합은 지원되지 않습니다.

- 데이터 파일, 제어 파일, 아카이브 로그 파일을 백업합니다.

  백업은 컨테이너 데이터베이스(CDB) 레벨에서만 지원됩니다.

- 데이터베이스, CDB 및 플러그형 데이터베이스(PDB)의 복원 및 복구

  PDB의 불완전한 복구는 지원되지 않습니다.

- 운영 데이터베이스의 클론을 최대 특정 시점까지 생성합니다.

  클론 복제는 CDB 레벨에서만 지원됩니다.

- 즉시 백업을 확인합니다.
- 복구 작업을 위해 데이터 및 로그 백업을 마운트 및 마운트 해제합니다.
- 백업 및 검증 작업 예약
- 모든 작업을 모니터링합니다.
- 백업, 복원 및 클론 작업에 대한 보고서를 봅니다.

Oracle Database용 플러그인의 기능

Oracle 데이터베이스용 플러그인은 Linux 또는 AIX 호스트의 Oracle 데이터베이스 및 스토리지 시스템의 NetApp 기술과 통합됩니다.

- 통합 그래픽 사용자 인터페이스

  SnapCenter 인터페이스는 플러그인과 환경 전반에서 표준화와 일관성을 제공합니다. SnapCenter 인터페이스를 사용하면 플러그인 전체에서 일관된 백업, 복원, 복구, 클론 작업을 완료하고, 중앙 집중식 보고 기능을 사용하고, 대시보드 뷰를 한눈에 보고, RBAC(역할 기반 액세스 제어)를 설정하고, 모든 플러그인에 걸쳐 작업을 모니터링할 수 있습니다.

- 자동화된 중앙 관리

  백업 및 클론 작업을 예약하고, 정책 기반 백업 보존을 구성하고, 복원 작업을 수행할 수 있습니다. 또한 SnapCenter에서 이메일 경고를 보내도록 구성하여 환경을 사전에 모니터링할 수도 있습니다.

- 무중단 NetApp 스냅샷 복사본 기술

  SnapCenter은 Oracle 데이터베이스용 플러그인과 UNIX용 플러그인을 통해 NetApp Snapshot 복사본 기술을 사용하여 데이터베이스를 백업합니다. 스냅샷 복사본은 최소 스토리지 공간을 사용합니다.

Oracle Database용 플러그인은 다음과 같은 이점도 제공합니다.

- 백업, 복원, 클론, 마운트, 마운트 해제, 검증 워크플로우를 활용해 보십시오
- 호스트에 구성된 Oracle 데이터베이스 자동 검색
- Oracle RMAN(Recovery Manager)을 사용하여 카탈로그 작성 및 카탈로그 작성 취소 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임

  권한이 있는 SnapCenter 사용자가 응용 프로그램 수준 권한을 갖도록 자격 증명을 설정할 수도 있습니다.

- 복원 및 클론 작업을 위한 ALM(Archive Log Management) 지원
- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 공간 효율적인 프로덕션 데이터베이스 시점 복사본 생성

  클론을 생성하려는 스토리지 시스템에는 FlexClone 라이센스가 필요합니다.

- SAN 및 ASM 환경에서 백업을 생성하는 과정에서 ONTAP의 일관성 그룹(CG) 기능 지원
- 무중단 및 자동화된 백업 검증
- 여러 데이터베이스 호스트에서 동시에 여러 백업을 실행할 수 있습니다

  단일 작업으로 단일 호스트의 데이터베이스가 동일한 볼륨을 공유할 때 스냅샷 복사본이 통합됩니다.

- 물리적 인프라와 가상화 인프라 지원
- NFS, iSCSI, FC(Fibre Channel), RDM, VMDK over NFS 및 VMFS, ASM over NFS, SAN, RDM, VMDK를 지원합니다
- ONTAP의 선택적 LUN 맵(SLM) 기능 지원

  기본적으로 설정된 SLM 기능은 최적화된 경로가 없는 LUN을 주기적으로 검색하여 수정합니다. /var/opt/snapcenter/SCU 등에 있는 scu.properties 파일에서 매개변수를 수정하여 SLM을 구성할 수 있습니다

  - enable_lunPATH_monitoring 매개변수 값을 false로 설정하여 이 기능을 비활성화할 수 있습니다.
  - LUNPATH_MONITORING_INTERVAL 매개변수에 값(시간)을 할당하여 LUN 경로가 자동으로 수정되는 빈도를 지정할 수 있습니다.
    SLM에 대한 자세한 내용은 을 참조하십시오 "ONTAP 9 SAN 관리 가이드 를 참조하십시오".

- Linux에서 비휘발성 메모리 익스프레스(NVMe) 지원
  - NVMe util이 호스트에 설치되어 있어야 합니다.

    대체 호스트에 클론 또는 마운트하려면 NVMe util을 설치해야 합니다.

◦ 백업, 복원, 클론, 마운트, 마운트 해제, VMDK 및 RDM과 같은 가상화된 환경을 제외하고 NVMe 하드웨어에서 카탈로그, 카탈로그 해제 및 검증 작업이 지원됩니다.

위의 작업은 파티션이 없거나 단일 파티션이 있는 장치에서 지원됩니다.

커널에서 기본 다중 경로 옵션을 설정하여 NVMe 장치에 대한 다중 경로 솔루션을 구성할 수 있습니다. 장치 매퍼(DM) 다중 경로가 지원되지 않습니다.

- Oracle 및 그리드 대신 기본이 아닌 모든 사용자를 지원합니다.

  기본값이 아닌 사용자를 지원하려면 _FILE/var/opt/snapcenter/sSCO/etc/_에 있는 * sco.properties* 파일에서 매개 변수 값을 수정하여 기본값이 아닌 사용자를 설정해야 합니다.

  매개 변수의 기본값은 Oracle 및 GRID로 설정됩니다.

  ◦ db_user=oracle입니다
  ◦ db_group=oinstall을 선택합니다
  ◦ gi_user = 그리드
  ◦ GI_GROUP = oinstall.(Gi_group = 설치

Oracle Database용 플러그인에서 지원하는 스토리지 유형입니다

SnapCenter는 물리적 시스템과 가상 머신 모두에서 다양한 스토리지 유형을 지원합니다. Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치하기 전에 스토리지 유형에 대한 지원을 확인해야 합니다.

SnapCenter는 Linux 및 AIX용 스토리지 프로비저닝을 지원하지 않습니다.

Linux에서 지원되는 스토리지 유형입니다

다음 표에는 Linux에서 지원되는 스토리지 유형이 나와 있습니다.

기계	스토리지 유형입니다
물리적 서버	• FC 연결 LUN • iSCSI로 연결된 LUN • NFS 연결 볼륨

기계	스토리지 유형입니다
VMware ESXi	• FC 또는 iSCSI ESXi HBA(호스트 버스 어댑터)에 의해 연결된 RDM LUN SnapCenter는 호스트에 있는 모든 호스트 버스 어댑터를 검사하므로 완료하는 데 시간이 오래 걸릴 수 있습니다. hba_driver_names에 나열된 HBA만 재검색하려면 _/opt/netapp/snapcenter/spL/plugins/SCU/scucore/modules/SCU/Config _ 에 있는 * LinuxConfig.pm * 파일을 편집하여 * scsi_hosts_optimized_rescan * 매개 변수의 값을 1로 설정합니다. • iSCSI 이니시에이터가 게스트 시스템에 직접 접속된 iSCSI LUN • VMFS 또는 NFS 데이터 저장소의 VMDK입니다 • 게스트 시스템에 직접 연결된 NFS 볼륨입니다

AIX에서 지원되는 스토리지 유형입니다

다음 표에는 AIX에서 지원되는 스토리지 유형이 나와 있습니다.

기계	스토리지 유형입니다
물리적 서버	• FC 연결 및 iSCSI 연결 LUN SAN 환경에서는 ASM, LVM 및 SAN 파일 시스템이 지원됩니다. ⓘ AIX 및 파일 시스템의 NFS는 지원되지 않습니다. • 향상된 저널 파일 시스템(JFS2) SAN 파일 시스템 및 LVM 레이아웃에 대한 인라인 로깅을 지원합니다.

를 클릭합니다 "NetApp 상호 운용성 매트릭스 툴" 지원되는 버전에 대한 최신 정보를 제공합니다.

Oracle용 플러그인을 위한 **SnapMirror** 및 **SnapVault** 복제를 위한 스토리지 시스템을 준비합니다

ONTAP 플러그인을 SnapCenter SnapMirror 기술과 함께 사용하여 다른 볼륨에 백업 세트의 미러링 복사본을 만들고 ONTAP SnapVault 기술을 사용하여 표준 준수 및 기타 거버넌스 관련 용도로 D2D 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 타겟 볼륨 간의 데이터 보호 관계를 구성하고 관계를 초기화해야 합니다.

SnapCenter는 스냅샷 복사본 작업이 완료된 후 SnapMirror 및 SnapVault에 대한 업데이트를 수행합니다.

SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행되고, 별도의 ONTAP 일정을 만들지 않습니다.

NetApp SnapManager 제품에서 SnapCenter으로 오고 있으며 구성한 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 운영 스토리지(소스 볼륨)의 데이터를 보조 스토리지(타겟 볼륨)에 복제합니다. 관계를 초기화할 때 ONTAP은 소스 볼륨에서 참조된 데이터 블록을 대상 볼륨으로 전송합니다.

SnapCenter는 SnapMirror와 SnapVault 볼륨(* Primary * > * Mirror * > * Vault *) 간의 계단식 관계를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter는 버전에 상관없이 유연한 SnapMirror 관계의 관리를 지원합니다. 버전에 상관없이 유연한 SnapMirror 관계와 설정 방법에 대한 자세한 내용은 를 참조하십시오 "ONTAP 설명서".

SnapCenter는 * SYNC_MIRROR * 복제를 지원하지 않습니다.

Oracle용 플러그인에 필요한 최소 ONTAP 권한

필요한 최소 ONTAP 권한은 데이터 보호를 위해 사용 중인 SnapCenter 플러그인에 따라 다릅니다.

- All-access 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
  - event generate-autosupport-log입니다
  - 작업 기록이 표시됩니다
  - 작업 중지
  - LUN을 클릭합니다
  - LUN 속성이 표시됩니다
  - LUN 생성
  - LUN을 삭제합니다
  - LUN 형태
  - LUN igroup 추가
  - LUN igroup 작성
  - LUN igroup 삭제
  - LUN igroup의 이름을 바꿉니다
  - LUN igroup 표시
  - LUN 매핑 add-reporting-nodes입니다
  - LUN 매핑 생성
  - LUN 매핑을 삭제합니다
  - LUN 매핑으로 remove-reporting-nodes를 사용할 수 있습니다
  - LUN 매핑이 표시됩니다

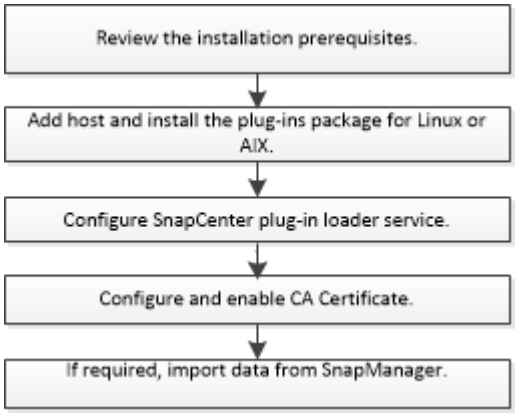
- LUN 수정
- LUN 이동 - 볼륨
- LUN이 오프라인 상태입니다
- LUN을 온라인 상태로 전환합니다
- LUN persistent - 예약 지우기
- LUN 크기 조정
- LUN 일련 번호입니다
- LUN 표시
- SnapMirror 정책 추가 규칙
- SnapMirror 정책 modify-rule을 참조하십시오
- SnapMirror 정책 remove-rule을 참조하십시오
- SnapMirror 정책 쇼
- SnapMirror 복원
- SnapMirror 쇼
- SnapMirror 기록
- SnapMirror 업데이트
- SnapMirror 업데이트 - ls -set
- SnapMirror 목록 - 대상
- 버전
- 볼륨 클론 생성
- 볼륨 클론 표시
- 볼륨 클론 분할 시작이 있습니다
- 볼륨 클론 분할 중지
- 볼륨 생성
- 볼륨 제거
- 볼륨 파일 클론 생성
- 볼륨 파일 show-disk-usage 를 참조하십시오
- 볼륨이 오프라인 상태입니다
- 볼륨을 온라인으로 설정합니다
- 볼륨 수정
- 볼륨 qtree 생성
- 볼륨 qtree 삭제
- 볼륨 qtree 수정
- 볼륨 qtree 표시

- 볼륨 제한
- 볼륨 표시
- 볼륨 스냅샷 생성
- 볼륨 스냅숏 삭제
- 볼륨 스냅숏 수정
- 볼륨 스냅숏 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 - 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- SVM
- SVM CIFS를 선택합니다
- SVM CIFS shadowcopy show 를 참조하십시오
- vserver show 를 참조하십시오
- 네트워크 인터페이스
- 네트워크 인터페이스가 표시됩니다
- MetroCluster 쇼

Oracle 데이터베이스용 SnapCenter 플러그인을 설치합니다

Oracle 데이터베이스용 SnapCenter 플러그인 설치 워크플로우

Oracle 데이터베이스를 보호하려면 Oracle 데이터베이스용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



호스트를 추가하고 Linux 또는 AIX용 플러그인 패키지를 설치하기 위한 사전 요구 사항

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 완료해야 합니다.

- iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.
- 루트 또는 루트 이외의 사용자에 대해 암호 기반 SSH 연결을 활성화해야 합니다.

  Oracle 데이터베이스용 SnapCenter 플러그인은 루트가 아닌 사용자가 설치할 수 있습니다. 그러나 비루트 사용자에 대한 sudo 권한을 구성하여 플러그인 프로세스를 설치하고 시작해야 합니다. 플러그인을 설치하면 프로세스가 루트가 아닌 효과적인 사용자로 실행됩니다.

- AIX 호스트에 AIX용 SnapCenter 플러그인 패키지를 설치하는 경우 디렉토리 레벨 심볼 링크를 수동으로 해결해야 합니다.

  AIX용 SnapCenter 플러그인 패키지는 파일 레벨 심볼 링크를 자동으로 확인하지만 java_home 절대 경로를 얻기 위한 디렉토리 레벨 심볼 링크는 확인하지는 않습니다.

- 설치 사용자에 대해 인증 모드를 Linux 또는 AIX로 사용하여 자격 증명을 작성합니다.
- Linux 또는 AIX 호스트에 Java 1.8.x 또는 Java 11, 64비트를 설치해야 합니다.

  Linux 호스트에 Java 11의 인증된 버전만을 설치했는지 확인합니다.

  Java를 다운로드하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

  - "모든 운영 체제에 대한 Java 다운로드"
  - "AIX용 IBM Java"

- Linux 또는 AIX 호스트에서 실행 중인 Oracle 데이터베이스의 경우 Oracle 데이터베이스용 SnapCenter 플러그인과 UNIX용 SnapCenter 플러그인을 모두 설치해야 합니다.

  Oracle Database용 플러그인을 사용하여 SAP용 Oracle 데이터베이스도 관리할 수 있습니다. 그러나 SAP BR * Tools 통합은 지원되지 않습니다.

- Oracle 데이터베이스 11.2.0.3 이상을 사용하는 경우 13366202 Oracle 패치를 설치해야 합니다.

SnapCenter에서는 /etc/fstab 파일의 UUID 매핑을 지원하지 않습니다.

- 플러그인 설치를 위한 기본 셸은 * bash * 이어야 합니다.

Linux 호스트 요구 사항

Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 호스트가 요구 사항을 충족하는지 확인해야 합니다.

항목	요구 사항
운영 체제	• Red Hat Enterprise Linux • Oracle Linux Oracle Linux 또는 Red Hat Enterprise Linux 6.6 또는 7.0 운영 체제의 LVM에서 Oracle 데이터베이스를 사용하는 경우 최신 버전의 LVM(Logical Volume Manager)을 설치해야 합니다. • SUSE Linux Enterprise Server(SLES)
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	2GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	• Java 1.8.x(64비트) Oracle Java 및 OpenJDK의 기능 • Java 11(64비트) Oracle Java 및 OpenJDK의 기능 Linux 호스트에 Java 11의 인증된 버전만을 설치했는지 확인합니다. Java를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties 에 있는 java_home 옵션이 올바른 Java 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다.

지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

Linux 호스트에 대해 루트가 아닌 사용자에 대한 sudo 권한을 구성합니다

SnapCenter 2.0 이상 버전에서는 루트가 아닌 사용자가 Linux용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 효과적인 비루트 사용자로 실행됩니다. 여러 경로에 대한 액세스를 제공하려면 루트가 아닌 사용자에 대해 sudo 권한을 구성해야 합니다.

- 필요한 것 *
- sudo 버전 1.8.7 이상

- MAC HMAC-SHA2-256 및 MAC HMAC-SHA2-512의 메시지 인증 코드 알고리즘을 구성하려면 _/etc/ssh/sshd_config_file을 편집합니다.

  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 대한 정보 *

루트가 아닌 사용자에 대해 sudo 권한을 구성하여 다음 경로에 대한 액세스를 제공해야 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/SPL입니다
- 단계 *
  1. Linux용 SnapCenter 플러그인 패키지를 설치할 Linux 호스트에 로그인합니다.
  2. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 행을 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/Con
fig_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 !visiblepw
Defaults: LINUX_USER !requiretty
```

다른 허용 명령과 함께 RAC 설정을 사용하는 경우 다음을 /etc/sudoers 파일에 추가해야 합니다. '/<crs_home>/bin/olsnodes'

*/etc/oracle/OLR.loc_file*에서 *_CRS_HOME* 값을 가져올 수 있습니다.

_linux_user_는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

_C:\ProgramData\NetApp\SnapCenter\Package Repository_에 있는 * Oracle_checksum.txt * 파일에서 _checksum_value_를 가져올 수 있습니다.

사용자 지정 위치를 지정한 경우 위치는 _CUSTOM_PATH\NetApp\SnapCenter\Package Repository_입니다.

이 예제는 고유한 데이터를 만들기 위한 참조로만 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.

항목	요구 사항
운영 체제	AIX 6.1 이상
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	4GB

항목	요구 사항
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	• Java 1.8.x(64비트) IBM Java • Java 11(64비트) IBM Java Java를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties 에 있는 java_home 옵션이 올바른 Java 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다.

지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

AIX 호스트에 대한 루트가 아닌 사용자에 대한 sudo 권한을 구성합니다

SnapCenter 4.4 이상에서는 루트가 아닌 사용자가 AIX용 SnapCenter 플러그인 패키지를 설치하고 플러그인 프로세스를 시작할 수 있습니다. 플러그인 프로세스는 효과적인 비루트 사용자로 실행됩니다. 여러 경로에 대한 액세스를 제공하려면 루트가 아닌 사용자에 대해 sudo 권한을 구성해야 합니다.

- 필요한 것 *
- sudo 버전 1.8.7 이상
- MAC HMAC-SHA2-256 및 MAC HMAC-SHA2-512의 메시지 인증 코드 알고리즘을 구성하려면 _/etc/ssh/sshd_config_file을 편집합니다.

  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 대한 정보 *

루트가 아닌 사용자에 대해 sudo 권한을 구성하여 다음 경로에 대한 액세스를 제공해야 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/SPL입니다
- 단계 *
  1. AIX용 SnapCenter 플러그인 패키지를 설치할 AIX 호스트에 로그인합니다.
  2. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 행을 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/Con
fig_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: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

> 다른 허용 명령과 함께 RAC 설정을 사용하는 경우 다음을 /etc/sudoers 파일에 추가해야 합니다. '/<crs_home>/bin/olsnodes'

*/etc/oracle/OLR.loc_file*에서 *_CRS_HOME* 값을 가져올 수 있습니다.

_AIX_USER_는 사용자가 작성한 루트가 아닌 사용자의 이름입니다.

_C:\ProgramData\NetApp\SnapCenter\Package Repository_에 있는 * Oracle_checksum.txt * 파일에서 _checksum_value_를 가져올 수 있습니다.

사용자 지정 위치를 지정한 경우 위치는 _CUSTOM_PATH\NetApp\SnapCenter\Package Repository_입니다.

이 예제는 고유한 데이터를 만들기 위한 참조로만 사용해야 합니다.

자격 증명을 설정합니다

SnapCenter는 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다. Linux 또는 AIX 호스트에 플러그인 패키지를 설치하기 위한 자격 증명을 작성해야 합니다.

- 이 작업에 대한 정보 *

이 자격 증명은 루트 사용자 또는 sudo 권한이 있는 비루트 사용자에 대해 생성되어 플러그인 프로세스를 설치 및 시작할 수 있습니다.

자세한 내용은 다음을 참조하십시오. Linux 호스트에 대해 루트가 아닌 사용자에 대한 sudo 권한을 구성합니다 또는 AIX 호스트에 대한 루트가 아닌 사용자에 대한 sudo 권한을 구성합니다

* 모범 사례: * 호스트를 구축하고 플러그인을 설치한 후에는 자격 증명을 생성할 수 있지만, 호스트를 구축하고 플러그인을 설치하기 전에 SVM을 추가한 후 자격 증명을 생성하는 것이 가장 좋습니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
2. 설정 페이지에서 * 자격 증명 * 을 클릭합니다.
3. 새로 만들기 * 를 클릭합니다.
4. 자격 증명 페이지에 자격 증명 정보를 입력합니다.

이 필드의 내용...	수행할 작업...
자격 증명 이름입니다	자격 증명의 이름을 입력합니다.

이 필드의 내용...	수행할 작업...
사용자 이름/암호	인증에 사용할 사용자 이름과 암호를 입력합니다. • 도메인 관리자 SnapCenter 플러그인을 설치할 시스템에 도메인 관리자를 지정합니다. 사용자 이름 필드에 유효한 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 제공 로컬 관리자를 지정합니다. 사용자 계정에 상승된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 올바른 형식은 _ 사용자 이름 _ 입니다
인증 모드	사용할 인증 모드를 선택합니다. 플러그인 호스트의 운영 체제에 따라 Linux 또는 AIX를 선택합니다.
sudo 권한을 사용합니다	루트가 아닌 사용자에 대한 자격 증명을 생성하는 경우 * sudo 권한 사용 * 확인란을 선택합니다.

5. 확인 * 을 클릭합니다.

자격 증명 설정을 마친 후 * 사용자 및 액세스 * 페이지에서 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

Oracle 데이터베이스에 대한 자격 증명을 구성합니다

Oracle 데이터베이스에서 데이터 보호 작업을 수행하는 데 사용되는 자격 증명을 구성해야 합니다.

- 이 작업에 대한 정보 *

Oracle 데이터베이스에 지원되는 다양한 인증 방법을 검토해야 합니다. 자세한 내용은 을 참조하십시오 "자격 증명에 대한 인증 방법입니다".

개별 리소스 그룹에 대한 자격 증명을 설정하고 사용자 이름에 전체 관리자 권한이 없는 경우 사용자 이름에 적어도 리소스 그룹 및 백업 권한이 있어야 합니다.

Oracle 데이터베이스 인증을 사용하도록 설정한 경우 리소스 보기에 빨간색 자물쇠 아이콘이 표시됩니다. 데이터베이스를 보호하거나 리소스 그룹에 데이터베이스 자격 증명을 추가하여 데이터 보호 작업을 수행하려면

데이터베이스 자격 증명을 구성해야 합니다.

자격 증명을 생성하는 동안 잘못된 세부 정보를 지정하면 오류 메시지가 표시됩니다. 취소 * 를 클릭한 다음 다시 시도해야 합니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 데이터베이스 * 를 선택합니다.
3. 을 클릭합니다 호스트 이름과 데이터베이스 유형을 선택하여 리소스를 필터링합니다.

   그런 다음 을 클릭할 수 있습니다 를 눌러 필터 창을 닫습니다.
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 권한을 가지고 있어야 합니다.

   을 클릭하여 자격 증명을 생성할 수도 있습니다 .
6. Configure ASM settings 섹션의 * Use Existing Credential * 드롭다운 목록에서 ASM 인스턴스에서 데이터 보호 작업을 수행하는 데 사용할 자격 증명을 선택합니다.

   ASM 사용자는 sysasm 권한을 가지고 있어야 합니다.

   을 클릭하여 자격 증명을 생성할 수도 있습니다 .
7. RMAN 카탈로그 설정 구성 섹션의 * 기존 자격 증명 사용 * 드롭다운 목록에서 Oracle RMAN(Recovery Manager) 카탈로그 데이터베이스에서 데이터 보호 작업을 수행하는 데 사용할 자격 증명을 선택합니다.

   을 클릭하여 자격 증명을 생성할 수도 있습니다 .

   TNSName* 필드에 SnapCenter 서버가 데이터베이스와 통신하는 데 사용할 투명 네트워크 기질(TNS) 파일 이름을 입력합니다.
8. Preferred RAC Nodes * 필드에서 백업에 사용할 RAC(Real Application Cluster) 노드를 지정합니다.

   선호하는 노드는 RAC 데이터베이스 인스턴스가 있는 하나 또는 모든 클러스터 노드일 수 있습니다. 백업 작업은 기본 설정 순서대로 이러한 기본 설정 노드에서만 트리거됩니다.

   RAC One Node에서는 하나의 노드만 기본 노드에 나열되고 이 기본 설정 노드는 데이터베이스가 현재 호스팅되는 노드입니다.

   RAC One Node 데이터베이스의 페일오버 또는 재배치 후 SnapCenter 리소스 페이지에서 리소스를 새로 고치면 데이터베이스가 이전에 호스팅되었던 * 선호 RAC 노드 * 목록에서 호스트가 제거됩니다.
   데이터베이스가 재배치된 RAC 노드는 * RAC 노드 * 에 나열되며 기본 RAC 노드로 수동으로 구성해야 합니다.

자세한 내용은 을 참조하십시오 "RAC 설정의 1차 노드".

1. 확인 * 을 클릭합니다.

GUI를 사용하여 Linux 또는 AIX용 플러그인 패키지를 설치하고 호스트를 추가합니다

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 대한 정보 *

호스트를 추가하고 개별 호스트 또는 클러스터에 대한 플러그인 패키지를 설치할 수 있습니다. 클러스터(Oracle RAC)에 플러그인을 설치하는 경우 클러스터의 모든 노드에 플러그인이 설치됩니다. Oracle RAC One Node의 경우 액티브 노드와 패시브 노드 모두에 플러그인을 설치해야 합니다.

플러그인 설치 및 제거 권한이 있는 역할(예: SnapCenter 관리자 역할)에 할당되어야 합니다.

SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 맨 위에 * Managed Hosts * 탭이 선택되어 있는지 확인합니다.
3. 추가 * 를 클릭합니다.
4. 호스트 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
호스트 유형	호스트 유형으로 * Linux * 또는 * AIX * 를 선택합니다. SnapCenter 서버는 호스트를 추가한 다음 호스트에 플러그인이 설치되어 있지 않은 경우 Oracle 데이터베이스용 플러그인과 UNIX용 플러그인을 설치합니다.

이 필드의 내용...	수행할 작업...
호스트 이름입니다	FQDN(정규화된 도메인 이름) 또는 호스트의 IP 주소를 입력합니다. SnapCenter는 DNS의 올바른 구성에 따라 달라집니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다. 다음 중 하나의 IP 주소 또는 FQDN을 입력할 수 있습니다. • 독립 실행형 호스트 • Oracle RAC(Real Application Clusters) 환경의 모든 노드 노드 VIP 또는 스캔 IP는 지원되지 않습니다 SnapCenter를 사용하여 호스트를 추가하고 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.
자격 증명	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성합니다. 자격 증명에 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하십시오. 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 의해 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.
6. (선택 사항) * 추가 옵션 * 을 클릭합니다.

이 필드의 내용...	수행할 작업...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정합니다. 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 _/opt/netapp/snapcenter_입니다. 선택적으로 경로를 사용자 지정할 수 있습니다.
Oracle RAC에 모든 호스트를 추가합니다	Oracle RAC의 모든 클러스터 노드를 추가하려면 이 확인란을 선택합니다. Flex ASM 설정에서 허브 또는 리프 노드인지 여부와 관계없이 모든 노드가 추가됩니다.
선택적 사전 설치 검사를 건너뜁니다	이미 플러그인을 수동으로 설치했고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.

7. 제출 * 을 클릭합니다.

   사전 검사 건너뛰기 확인란을 선택하지 않은 경우 호스트가 플러그인 설치 요구사항을 충족하는지 여부를 확인합니다.

   사전 확인 스크립트는 방화벽 거부 규칙에 지정된 플러그인 포트 방화벽 상태의 유효성을 검사하지 않습니다.

   최소 요구 사항이 충족되지 않으면 적절한 오류 또는 경고 메시지가 표시됩니다. 오류가 디스크 공간 또는 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 파일을 업데이트해야 합니다.

8. 지문을 확인한 다음 * 확인 및 제출 * 을 클릭합니다.

   클러스터 설정에서 클러스터의 각 노드에 대한 지문을 확인해야 합니다.

   SnapCenter는 ECDSA 알고리즘을 지원하지 않습니다.

동일한 호스트가 SnapCenter에 이전에 추가되었고 지문이 확인되었더라도 지문 확인은 필수입니다.

1. 설치 과정을 모니터링합니다.

   설치별 로그 파일은 _/custom_location/snapcenter/logs_에 있습니다.

결과 *

호스트의 모든 데이터베이스가 자동으로 검색되어 리소스 페이지에 표시됩니다. 아무 것도 표시되지 않으면 * 리소스 새로 고침 * 을 클릭합니다.

설치 상태를 모니터링합니다

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행률을 모니터링할 수 있습니다. 설치 진행 상황을 확인하여 설치 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다

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 클릭합니다.
   b. 선택 사항: 시작 및 종료 날짜를 지정합니다.
   c. 유형 드롭다운 메뉴에서 * 플러그인 설치 * 를 선택합니다.
   d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
   e. 적용 * 을 클릭합니다.
4. 설치 작업을 선택하고 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. Job Details * 페이지에서 * View logs * 를 클릭합니다.

Linux 또는 AIX용 플러그인 패키지를 설치하는 다른 방법

cmdlet 또는 CLI를 사용하여 Linux 또는 AIX용 플러그인 패키지를 수동으로 설치할 수도 있습니다.

플러그인을 수동으로 설치하기 전에 _C:\ProgramData\NetApp\SnapCenter\Package Repository_에 있는 * snapcenter_public_key.pub * 및 * snapcenter_linux_host_plugin.bin.SIG * 키를 사용하여 바이너리 패키지의 서명을 확인해야 합니다.

플러그인을 설치할 호스트에 * OpenSSL 1.0.2g * 가 설치되어 있는지 확인합니다.

다음 명령을 실행하여 바이너리 패키지의 서명을 확인합니다.

- 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_linux_host_plugin.bsx.sig snapcenter_linux_host_plugin.bsx`

cmdlet을 사용하여 여러 원격 호스트에 설치합니다

여러 호스트에 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치하려면 _Install-SmHostPackage_PowerShell cmdlet을 사용해야 합니다.

- 필요한 것 *

플러그인 패키지를 설치하려는 각 호스트에 대한 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_cmdlet 및 필수 매개 변수를 사용하여 Linux 또는 AIX용 SnapCenter 플러그인 패키지용 SnapCenter 플러그인 패키지를 설치합니다.

   플러그인을 이미 수동으로 설치했고 호스트가 플러그인을 설치하는 데 필요한 요구 사항을 충족하는지 여부를 확인하지 않으려는 경우 _-skipprecheck_옵션을 사용할 수 있습니다.

   사전 확인 스크립트는 방화벽 거부 규칙에 지정된 플러그인 포트 방화벽 상태의 유효성을 검사하지 않습니다.

1. 원격 설치를 위한 자격 증명을 입력합니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

클러스터 호스트에 설치합니다

클러스터 호스트의 두 노드에 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치해야 합니다.

클러스터 호스트의 각 노드에는 2개의 IP가 있습니다. IP 중 하나는 각 노드의 공용 IP이고, 두 번째 IP는 두 노드 간에 공유되는 클러스터 IP입니다.

- 단계 *

1. 클러스터 호스트의 두 노드에 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치합니다.
2. SNAPCENTER_SERVER_HOST, SPL_PORT, SNAPCENTER_SERVER_PORT 및 SPL_ENABLED_PACGISLICATIONES 매개변수에 대한 올바른 값이 _/var/opt/snapcenter/SPL/etc/_에 있는 spl.properties 파일에 지정되어 있는지 확인합니다.

   SPL_ENABLED_PACNEWNES가 spl.properties 에 지정되지 않은 경우 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 매개 변수를 사용하여 노드의 기본 설정 IP를 설정합니다.
5. SnapCenter 서버 호스트에서 클러스터 IP에 대한 항목과 해당 DNS 이름을 _C:\Windows\System32\drivers\etc\hosts_에 추가합니다.
6. 호스트 이름에 대한 클러스터 IP를 지정하여 _Add-SmHost_cmdlet을 사용하여 SnapCenter 서버에 노드를 추가합니다.

노드 1에서 Oracle 데이터베이스를 검색하고(클러스터 IP가 노드 1에서 호스팅된다고 가정) 데이터베이스의 백업을 생성합니다. 페일오버가 발생하면 노드 1에서 생성된 백업을 사용하여 노드 2에서 데이터베이스를 복원할 수 있습니다. 노드 1에 생성된 백업을 사용하여 노드 2에 클론을 생성할 수도 있습니다.

다른 SnapCenter 작업이 실행 중인 동안 페일오버가 발생하면 오래된 볼륨, 디렉토리 및 잠금 파일이 있습니다.

Linux용 플러그인 패키지를 자동 모드로 설치합니다

CLI(명령줄 인터페이스)를 사용하여 Linux용 SnapCenter 플러그인 패키지를 자동 모드로 설치할 수 있습니다.

- 필요한 것 *
- 플러그인 패키지를 설치하기 위한 사전 요구 사항을 검토해야 합니다.
- 디스플레이 환경 변수가 설정되어 있지 않은지 확인해야 합니다.

  디스플레이 환경 변수가 설정된 경우 설정되지 않은 디스플레이를 실행한 다음 플러그인을 수동으로 설치해야 합니다.

- 이 작업에 대한 정보 *

콘솔 모드로 설치하는 동안 필요한 설치 정보를 제공해야 하지만 자동 모드 설치에서는 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 액세스할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 다운로드한 디렉토리로 이동합니다.
3. 실행

```
./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. spL_enabled_plugins=SCO, SCU를 추가한 다음 SnapCenter 플러그인 로더 서비스를 다시 시작하려면 _/var/opt/snapcenter/spl/etc/_에 있는 spl.properties 파일을 편집합니다.

> 플러그인 패키지를 설치하면 SnapCenter 서버가 아닌 호스트에 플러그인이 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록해야 합니다. 호스트를 추가하는 동안 자격 증명으로 "없음"을 선택합니다. 호스트가 추가되면 설치된 플러그인이 자동으로 검색됩니다.

AIX용 플러그인 패키지를 자동 모드로 설치합니다

CLI(명령줄 인터페이스)를 사용하여 AIX용 SnapCenter 플러그인 패키지를 자동 모드로 설치할 수 있습니다.

- 필요한 것 *
- 플러그인 패키지를 설치하기 위한 사전 요구 사항을 검토해야 합니다.
- 디스플레이 환경 변수가 설정되어 있지 않은지 확인해야 합니다.

  디스플레이 환경 변수가 설정된 경우 설정되지 않은 디스플레이를 실행한 다음 플러그인을 수동으로 설치해야 합니다.

- 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 액세스할 수 있습니다.

  2. 명령 프롬프트에서 설치 파일을 다운로드한 디렉토리로 이동합니다.
  3. 실행

```
./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. spL_enabled_plugins=SCO, SCU를 추가한 다음 SnapCenter 플러그인 로더 서비스를 다시 시작하려면 _/var/opt/snapcenter/spl/etc/_에 있는 spl.properties 파일을 편집합니다.

> 플러그인 패키지를 설치하면 SnapCenter 서버가 아닌 호스트에 플러그인이 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록해야 합니다. 호스트를 추가하는 동안 자격 증명으로 "없음"을 선택합니다. 호스트가 추가되면 설치된 플러그인이 자동으로 검색됩니다.

SnapCenter 플러그인 로더 서비스를 구성합니다

SnapCenter 플러그인 로더 서비스는 Linux 또는 AIX용 플러그인 패키지를 로드하여 SnapCenter 서버와 상호 작용합니다. SnapCenter 플러그인 로더 서비스는 SnapCenter용 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치할 때 설치됩니다.

- 이 작업에 대한 정보 *

Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 설치한 후 SnapCenter 플러그인 로더 서비스가 자동으로 시작됩니다. SnapCenter 플러그인 로더 서비스가 자동으로 시작되지 않는 경우 다음을 수행해야 합니다.

- 플러그인이 작동하는 디렉토리가 삭제되지 않았는지 확인합니다
- Java Virtual Machine에 할당된 메모리 공간을 늘립니다

spl.properties 파일은 _/custom_location/NetApp/snapcenter/SPL/etc/_에 있으며 다음 매개 변수를 포함합니다. 기본값은 이러한 매개 변수에 할당됩니다.

매개 변수 이름입니다	설명
log_level 을 선택합니다	지원되는 로그 수준을 표시합니다. 가능한 값은 추적, 디버그, 정보, 경고, 오류, 치명적입니다.
SPL_protocol(프로토콜)	SnapCenter 플러그인 로더에서 지원하는 프로토콜을 표시합니다. HTTPS 프로토콜만 지원됩니다. 기본값이 없는 경우 값을 추가할 수 있습니다.
SNAPCENTER_SERVER_PROTOCOL	SnapCenter 서버에서 지원하는 프로토콜을 표시합니다. HTTPS 프로토콜만 지원됩니다. 기본값이 없는 경우 값을 추가할 수 있습니다.
skip_jAVHOME_update 를 선택합니다	기본적으로 SPL 서비스는 Java 경로를 감지하고 java_home 매개 변수를 업데이트합니다. 따라서 기본값은 false 로 설정됩니다. 기본 동작을 비활성화하고 Java 경로를 수동으로 수정하려면 TRUE로 설정할 수 있습니다.
SPL_keystore_pass입니다	키 저장소 파일의 암호를 표시합니다. 암호를 변경하거나 새 키 저장소 파일을 만드는 경우에만 이 값을 변경할 수 있습니다.

매개 변수 이름입니다	설명
SPL_PORT	SnapCenter 플러그인 로더 서비스가 실행 중인 포트 번호를 표시합니다. 기본값이 없는 경우 값을 추가할 수 있습니다. 플러그인을 설치한 후에는 값을 변경해서는 안 됩니다.
SNAPCENTER_SERVER_HOST	SnapCenter 서버의 IP 주소 또는 호스트 이름을 표시합니다.
SPL_keystore_path를 입력합니다	키 저장소 파일의 절대 경로를 표시합니다.
SNAPCENTER_SERVER_PORT	SnapCenter 서버가 실행 중인 포트 번호를 표시합니다.
logs_MAX_count	_/custom_location/snapcenter/SPL/logs_folder에 유지되는 SnapCenter 플러그인 로더 로그 파일의 수를 표시합니다. 기본값은 5000으로 설정됩니다. 카운트가 지정된 값보다 큰 경우 마지막으로 수정된 5000개의 파일이 유지됩니다. SnapCenter 플러그인 로더 서비스가 시작된 후 24시간마다 파일 수 검사가 자동으로 수행됩니다. spl.properties 파일을 수동으로 삭제하면 보존할 파일 수가 9999로 설정됩니다.
java_home입니다	SPL 서비스를 시작하는 데 사용되는 java_home의 절대 디렉토리 경로를 표시합니다. 이 경로는 설치 중에 그리고 SPL 시작 시 결정됩니다.
Log_MAX_SIZE(로그 최대 크기)	작업 로그 파일의 최대 크기를 표시합니다. 최대 크기에 도달하면 로그 파일이 압축되고 로그가 해당 작업의 새 파일에 기록됩니다.
최근 _ 일 _ 의 _ 로그 유지	로그가 유지되는 최대 일 수를 표시합니다.
certificate_validation을 활성화합니다	호스트에 대해 CA 인증서 유효성 검사가 활성화되면 true를 표시합니다. spl.properties 를 편집하거나 SnapCenter GUI 또는 cmdlet을 사용하여 이 매개 변수를 활성화 또는 비활성화할 수 있습니다.

이러한 매개 변수 중 하나라도 기본값에 할당되지 않거나 값을 할당하거나 변경하려는 경우 spl.properties 파일을 수정할 수 있습니다. 또한 spl.properties 파일을 확인하고 파일을 편집하여 매개 변수에 할당된 값과 관련된 문제를 해결할 수도 있습니다. spl.properties 파일을 수정한 후 SnapCenter 플러그인 로더 서비스를 다시 시작해야 합니다.

- 단계 *

1. 필요에 따라 다음 작업 중 하나를 수행합니다.
   - 루트 사용자로 SnapCenter 플러그인 로더 서비스를 시작합니다.

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl start`
** SnapCenter 플러그인 로더 서비스를 중지합니다.
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl stop`
```

> stop 명령에 -force 옵션을 사용하면 SnapCenter 플러그인 로더 서비스를 강제로 중지할 수 있습니다. 그러나 기존 작업도 종료되므로 이 작업을 수행하기 전에 주의해야 합니다.

   - SnapCenter 플러그인 로더 서비스를 다시 시작합니다.

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
** SnapCenter 플러그인 로더 서비스의 상태를 찾습니다.
```

```
 `/custom_location/NetApp/snapcenter/spl/bin/spl status`
** SnapCenter 플러그인 로더 서비스에서 변경 사항을 찾습니다.
```

```
`/custom_location/NetApp/snapcenter/spl/bin/spl change`
```

Linux 호스트에서 SnapCenter SPL(Plug-in Loader) 서비스를 사용하여 CA 인증서를 구성합니다

SPL 키 저장소 및 해당 인증서의 암호를 관리하고, CA 인증서를 구성하고, SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성하고, 설치된 디지털 인증서를 활성화하려면 SnapCenter 플러그인 로더 서비스를 사용하여 CA 서명 키 쌍을 SPL 신뢰 저장소에 구성해야 합니다.

> SPL은 '/var/opt/snapcenter/spl/etc'에 있는 'keystore.jks' 파일을 신뢰 저장소 및 키 저장소로 사용합니다.

SPL 키 저장소의 암호 및 사용 중인 CA 서명된 키 쌍의 별칭을 관리합니다

- 단계 *

1. SPL 속성 파일에서 SPL 키 저장소 기본 암호를 검색할 수 있습니다.

   'PL_keystore_pass' 키에 해당하는 값입니다.

2. 키 저장소 암호를 변경합니다.

   ```
    keytool -storepasswd -keystore keystore.jks
   . 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 암호를 키 저장소에 사용되는 동일한 암호로 변경합니다.
   ```

   ```
   keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
   ```

   spl.properties 파일의 SPL_keystore_pass 키에 대해서도 동일하게 업데이트하십시오.

3. 암호를 변경한 후 서비스를 다시 시작합니다.

SPL 키 저장소 및 개인 키의 모든 관련 별칭 암호에 대한 암호는 동일해야 합니다.

SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성합니다

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 찾습니다.
  3. 키 저장소에 추가된 인증서를 나열합니다.

     ```
      keytool -list -v -keystore keystore.jks
     . 루트 또는 중간 인증서 추가:
     ```

     ```
      keytool -import -trustcacerts -alias
     <AliasNameForCerticateToBeImported> -file /<CertificatePath>
     -keystore keystore.jks
     . SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.
     ```

루트 CA 인증서와 중간 CA 인증서를 추가해야 합니다.

CA 서명 키 쌍을 **SPL** 신뢰 저장소에 구성합니다

CA 서명된 키 쌍을 SPL 신뢰 저장소에 구성해야 합니다.

- 단계 *

1. SPL의 keystore/var/opt/snapcenter/SPL 등이 포함된 폴더로 이동합니다
2. 'keystore.jks' 파일을 찾습니다.
3. 키 저장소에 추가된 인증서를 나열합니다.

```
 keytool -list -v -keystore keystore.jks
. 개인 키와 공개 키를 모두 사용하는 CA 인증서를 추가합니다.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. 키 저장소에 추가된 인증서를 나열합니다.
```

```
 keytool -list -v -keystore keystore.jks
. keystore에 keystore에 추가된 새 CA 인증서에 해당하는 별칭이 포함되어 있는지 확인합니다.
. CA 인증서에 추가된 개인 키 암호를 키 저장소 암호로 변경합니다.
```

기본 SPL 키 저장소 암호는 spl.properties 파일의 SPL_keystore_pass 키 값입니다.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>"
-keystore keystore.jks
. CA 인증서의 별칭 이름이 길고 공백 또는 특수 문자("*",",")가 포함된 경우 별칭 이름을 단순 이름으로 변경합니다.
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. spl.properties 파일에 있는 키 저장소에서 별칭 이름을 구성합니다.
```

이 값을 SPL_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

4. CA 서명 키 쌍을 SPL 신뢰 저장소에 구성한 후 서비스를 다시 시작합니다.

SPL에 대한 **CRL(**인증서 해지 목록**)**을 구성합니다

SPL에 대해 CRL을 구성해야 합니다

- 이 작업에 대한 정보 *
- SPL은 사전 구성된 디렉터리에서 CRL 파일을 찾습니다.
- SPL에 대한 CRL 파일의 기본 디렉토리는 _ /var/opt/snapcenter/spl/etc/CRL_ 입니다.

- 단계 *

1. spl.properties 파일의 기본 디렉터리를 SPL_CRL_PATH 키에 맞게 수정 및 업데이트할 수 있습니다.
2. 이 디렉터리에 둘 이상의 CRL 파일을 배치할 수 있습니다.

   들어오는 인증서는 각 CRL에 대해 확인됩니다.

플러그인에 대해 **CA** 인증서를 활성화합니다

CA 인증서를 구성하고 SnapCenter 서버 및 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- run_Set-SmCertificateSettings_cmdlet을 사용하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- _get-SmCertificateSettings_를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 호스트 페이지에서 * 관리되는 호스트 * 를 클릭합니다.
3. 단일 또는 여러 플러그인 호스트를 선택합니다.
4. 추가 옵션 * 을 클릭합니다.
5. 인증서 유효성 검사 사용 * 을 선택합니다.

작업을 마친 후

관리 호스트 탭 호스트에는 자물쇠가 표시되고 자물쇠 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- 는 CA 인증서가 활성화되지 않았으며 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- CA 인증서의 유효성을 확인했음을 나타냅니다.
- CA 인증서의 유효성을 확인할 수 없음을 나타냅니다.
- 연결 정보를 검색할 수 없음을 나타냅니다.

> 상태가 노란색 또는 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

SnapManager for Oracle 및 **SnapManager for SAP**에서 **SnapCenter**로 데이터를 가져옵니다

SnapManager for Oracle 및 SnapManager for SAP에서 SnapCenter로 데이터를 가져오면 이전 버전의 데이터를 계속 사용할 수 있습니다.

명령줄 인터페이스(Linux 호스트 CLI)에서 가져오기 도구를 실행하여 SnapManager for Oracle 및 SnapManager for

SAP에서 SnapCenter로 데이터를 가져올 수 있습니다.

가져오기 도구는 SnapCenter에 정책 및 리소스 그룹을 만듭니다. SnapCenter에서 생성된 정책 및 리소스 그룹은 SnapManager for Oracle 및 SnapManager for SAP에서 이러한 프로파일을 사용하여 수행된 프로필과 작업에 해당합니다. SnapCenter 가져오기 도구는 SnapManager for Oracle 및 SnapManager for SAP 리포지토리 데이터베이스 및 가져올 데이터베이스와 상호 작용합니다.

- 프로파일을 사용하여 수행된 모든 프로파일, 스케줄 및 작업을 검색합니다.
- 프로필에 연결된 각 고유 작업 및 각 스케줄에 대한 SnapCenter 백업 정책을 생성합니다.
- 각 타겟 데이터베이스에 대한 리소스 그룹을 생성합니다.

가져오기 도구는 _/opt/NetApp/snapcenter/SPL/bin_에 있는 SC-migrate 스크립트를 실행하여 실행할 수 있습니다. 가져올 데이터베이스 호스트에 Linux용 SnapCenter 플러그인 패키지를 설치하면 SC-마이그레이션 스크립트가 _/opt/netapp/snapcenter/SPL/bin_에 복사됩니다.

SnapCenter 그래픽 사용자 인터페이스(GUI)에서는 데이터 가져오기가 지원되지 않습니다.

SnapCenter는 7-Mode에서 작동하는 Data ONTAP를 지원하지 않습니다. 7-Mode 전환 툴을 사용하면 7-Mode에서 운영되는 Data ONTAP을 실행하는 시스템에 저장된 데이터와 구성을 ONTAP 시스템으로 마이그레이션할 수 있습니다.

데이터 가져오기에 지원되는 구성입니다

Oracle용 SnapManager 3.4.x 및 SAP용 SnapManager 3.4.x에서 SnapCenter로 데이터를 가져오기 전에 Oracle 데이터베이스용 SnapCenter 플러그인에서 지원되는 구성을 알고 있어야 합니다.

Oracle 데이터베이스용 SnapCenter 플러그인에서 지원되는 구성은 에 나와 있습니다 "NetApp 상호 운용성 매트릭스 툴".

SnapCenter로 가져온 항목

프로파일을 사용하여 수행한 프로파일, 일정 및 작업을 가져올 수 있습니다.

SnapManager for Oracle 및 **SnapManager for SAP**에서	**SnapCenter**로
작업 및 일정이 없는 프로파일	정책은 기본 백업 유형을 온라인 으로, 백업 범위를 전체 로 하여 생성됩니다.
하나 이상의 작업이 있는 프로파일	여러 정책은 해당 프로파일을 사용하여 수행된 프로파일과 작업의 고유한 조합을 기반으로 생성됩니다. SnapCenter에서 생성된 정책에는 프로파일 및 해당 작업에서 가져온 아카이브 로그 잘라내기 및 보존 세부 정보가 포함됩니다.

SnapManager for Oracle 및 **SnapManager for SAP**에서	**SnapCenter**로
Oracle RMAN(Recovery Manager) 구성을 사용한 프로파일	정책은 * Oracle Recovery Manager * 옵션을 활성화한 상태에서 * Catalog Backup을 사용하여 생성됩니다. SnapManager에서 외부 RMAN 카탈로그를 사용한 경우 SnapCenter에서 RMAN 카탈로그 설정을 구성해야 합니다. 기존 자격 증명을 선택하거나 새 자격 증명을 생성할 수 있습니다. RMAN이 SnapManager의 제어 파일을 통해 구성된 경우 SnapCenter에서 RMAN을 구성할 필요가 없습니다.
프로필에 연결된 스케줄입니다	스케줄에 대한 정책이 생성됩니다.
데이터베이스	가져온 각 데이터베이스에 대해 리소스 그룹이 만들어집니다. RAC(Real Application Clusters) 설정에서는 가져오기 도구를 실행하는 노드가 가져오기 후 기본 설정 노드가 되고 해당 노드에 대한 리소스 그룹이 생성됩니다.

프로필을 가져오면 백업 정책과 함께 검증 정책이 생성됩니다.

Oracle용 SnapManager와 SnapManager SAP 프로필, 일정 및 프로필을 사용하여 수행한 작업을 SnapCenter로 가져오는 경우 다른 매개 변수 값도 가져옵니다.

SnapManager for Oracle 및 **SnapManager for SAP** 매개 변수 및 값	**SnapCenter** 매개 변수 및 값	참고
백업 범위 • 가득 참 • 데이터 • 로그	백업 범위 • 가득 참 • 데이터 • 로그	
백업 모드 • 자동 • 온라인 • 오프라인	백업 유형 • 온라인 • 오프라인 종료	백업 모드가 자동인 경우 가져오기 도구는 작업이 수행될 때 데이터베이스 상태를 확인하고 백업 유형을 온라인 또는 오프라인 종료로 적절하게 설정합니다.

SnapManager for Oracle 및 **SnapManager for SAP** 매개 변수 및 값	**SnapCenter** 매개 변수 및 값	참고
보존 • 일 • 카운트	보존 • 일 • 카운트	Oracle용 SnapManager와 SAP용 SnapManager는 일 및 수 모두를 사용하여 보존을 설정합니다. SnapCenter에는 days_or_Counts가 있습니다. 따라서 Oracle의 경우 SnapManager, SAP의 경우 SnapManager에서 일 수가 더 우선하기 때문에 일 수에 따라 보존 기간이 설정됩니다.
일정에 대한 정리 • 모두 • 시스템 변경 번호(SCN) • 날짜 • 지정된 시간, 일, 주 및 월 이전에 생성된 로그입니다	일정에 대한 정리 • 모두 • 지정된 시간 및 일 이전에 생성된 로그입니다	SnapCenter는 SCN, 날짜, 주 및 월을 기준으로 한 가지치기를 지원하지 않습니다.
통지 • 성공적인 작업을 위해 보낸 이메일입니다 • 실패한 작업에 대해서만 이메일이 전송되었습니다 • 성공 및 실패한 작업을 위해 전송된 이메일입니다	통지 • 항상 • 실패 시 • 경고 • 오류	이메일 알림을 가져옵니다. 그러나 SnapCenter GUI를 사용하여 SMTP 서버를 수동으로 업데이트해야 합니다. 이메일 제목은 구성할 수 있도록 비어 있습니다.

SnapCenter로 가져올 수 없는 항목

불러오기 도구는 모든 것을 SnapCenter로 불러오지 않습니다.

다음을 SnapCenter로 가져올 수 없습니다.

- 메타데이터 백업
- 부분 백업
- RDM(Raw Device Mapping) 및 VSC(Virtual Storage Console) 관련 백업
- Oracle용 SnapManager 및 SAP용 SnapManager 리포지토리에서 사용할 수 있는 역할 또는 자격 증명
- 검증, 복원 및 클론 작업과 관련된 데이터
- 작업을 위한 잘라내기
- SnapManager for Oracle 및 SnapManager for SAP 프로필에 지정된 복제 세부 정보입니다

가져온 후에는 SnapCenter에서 생성한 해당 정책을 수동으로 편집하여 복제 세부 정보를 포함해야 합니다.

- 카탈로그 작성된 백업 정보

데이터 가져오기를 준비합니다

데이터를 SnapCenter로 가져오기 전에 가져오기 작업을 성공적으로 실행하기 위해 특정 작업을 수행해야 합니다.

- 단계 *

1. 가져올 데이터베이스를 식별합니다.
2. SnapCenter를 사용하여 데이터베이스 호스트를 추가하고 Linux용 SnapCenter 플러그인 패키지를 설치합니다.
3. SnapCenter를 사용하여 호스트의 데이터베이스에서 사용되는 SVM(스토리지 가상 머신)의 연결을 설정합니다.
4. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
5. 리소스 페이지에서 가져올 데이터베이스가 검색되어 표시되는지 확인합니다.

   가져오기 도구를 실행하려면 데이터베이스에 액세스할 수 있어야 하며 그렇지 않으면 리소스 그룹을 만들 수 없습니다.

   데이터베이스에 자격 증명이 구성되어 있는 경우 SnapCenter에서 해당 자격 증명을 생성하고 데이터베이스에 자격 증명을 할당한 다음 데이터베이스 검색을 다시 실행해야 합니다. 데이터베이스가 ASM(Automatic Storage Management)에 있는 경우 ASM 인스턴스에 대한 자격 증명을 생성하고 자격 증명을 데이터베이스에 할당해야 합니다.

6. 가져오기 도구를 실행하는 사용자가 SnapManager SnapManager for Oracle 또는 SnapManager for SAP CLI 명령(예: 예약 일시 중지 명령)을 실행할 수 있는 충분한 권한을 가지고 있는지 확인합니다 SnapManager.
7. Oracle용 SnapManager 또는 SAP용 SnapManager 호스트에서 다음 명령을 실행하여 스케줄을 일시 중지합니다.
   a. SnapManager for Oracle 호스트에서 스케줄을 일시 중지하려면 다음을 실행합니다.
      - `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 자격 증명 세트 명령을 실행해야 합니다.

   b. SnapManager for SAP 호스트의 스케줄을 일시 중지하려면 다음을 실행합니다.
      - `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 집합 명령을 실행해야 합니다.

1. 호스트 이름 -F를 실행할 때 데이터베이스 호스트의 FQDN(정규화된 도메인 이름)이 표시되는지 확인합니다

   FQDN이 표시되지 않으면 /etc/hosts를 수정하여 호스트의 FQDN을 지정해야 합니다.

데이터를 가져옵니다

데이터베이스 호스트에서 가져오기 도구를 실행하여 데이터를 가져올 수 있습니다.

- 이 작업에 대한 정보 *

가져온 후 생성되는 SnapCenter 백업 정책의 명명 형식은 다음과 같습니다.

- 작업 및 일정 없이 프로파일에 대해 생성된 정책에는 SM_profileName_online_full_default_m마이그레이션된 형식이 있습니다.

  프로파일을 사용하여 작업을 수행하지 않으면 해당 정책은 기본 백업 유형을 온라인 및 백업 범위를 전체 로 사용하여 생성됩니다.

- 하나 이상의 작업으로 프로파일에 대해 생성된 정책에는 SM_profileName_BACKUPMODE_BACKUPSCOPE_Migrated 형식이 있습니다.
- 프로필에 연결된 일정에 대해 생성된 정책에는 SM_profileName_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_Migrated 형식이 있습니다.
- 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 이름 및 암호를 입력합니다.

     자격 증명의 유효성을 검사한 후 SnapCenter와 연결이 설정됩니다.

  4. SnapManager for Oracle 또는 SnapManager for SAP 리포지토리 데이터베이스 세부 정보를 입력합니다.

     저장소 데이터베이스에는 호스트에서 사용할 수 있는 데이터베이스가 나열됩니다.

  5. 대상 데이터베이스 세부 정보를 입력합니다.

     호스트의 모든 데이터베이스를 가져오려면 All 을 입력합니다.

  6. 시스템 로그를 생성하거나 실패한 작업에 대한 ASUP 메시지를 보내려면 *Add-SmStorageConnection* 또는 *Set-SmStorageConnection* 명령을 실행하여 해당 로그를 활성화해야 합니다.

     가져오기 도구를 실행하는 동안 또는 가져온 후에 가져오기 작업을 취소하려면 가져오기 작업의 일부로 만든 SnapCenter 정책, 자격 증명 및 리소스 그룹을 수동으로 삭제해야 합니다.

- 결과 *

SnapCenter 백업 정책은 프로파일을 사용하여 수행하는 프로파일, 스케줄 및 작업에 대해 생성됩니다. 각 타겟 데이터베이스에 대해 리소스 그룹도 만들어집니다.

데이터를 성공적으로 가져오면 가져온 데이터베이스와 연결된 스케줄이 SnapManager for Oracle 및 SnapManager for SAP에서 일시 중단됩니다.

가져온 데이터베이스 또는 파일 시스템을 SnapCenter를 사용하여 관리해야 합니다.

가져오기 도구의 모든 실행에 대한 로그는 SPL_migration_timestamp.log라는 이름의 _/var/opt/snapcenter/SPL/logs_directory에 저장됩니다. 이 로그를 참조하여 가져오기 오류를 검토하고 문제를 해결할 수 있습니다.

VMware vSphere용 SnapCenter 플러그인을 설치합니다

데이터베이스가 가상 머신(VM)에 저장되어 있거나 VM 및 데이터 저장소를 보호하려는 경우 SnapCenter Plug-in for VMware vSphere 가상 어플라이언스를 구축해야 합니다.

배포에 대한 자세한 내용은 을 참조하십시오 "구축 개요".

CA 인증서를 배포합니다

VMware vSphere용 SnapCenter 플러그인을 사용하여 CA 인증서를 구성하려면 를 참조하십시오 "SSL 인증서를 생성하거나 가져옵니다".

CRL 파일을 구성합니다

VMware vSphere용 SnapCenter 플러그인은 사전 구성된 디렉토리에서 CRL 파일을 찾습니다. VMware vSphere용 SnapCenter 플러그인의 기본 CRL 파일 디렉토리는 */opt/netapp/config/CRL* 입니다.

이 디렉터리에 둘 이상의 CRL 파일을 배치할 수 있습니다. 들어오는 인증서는 각 CRL에 대해 확인됩니다.

Oracle 데이터베이스 보호를 위한 준비

백업, 클론 복제 또는 복원 작업과 같은 데이터 보호 작업을 수행하기 전에 전략을 정의하고 환경을 설정해야 합니다. SnapVault 서버에서 SnapMirror 및 SnapCenter 기술을 사용하도록 설정할 수도 있습니다.

SnapVault 및 SnapMirror 기술을 활용하려면 스토리지 장치의 소스 볼륨과 타겟 볼륨 간의 데이터 보호 관계를 구성하고 초기화해야 합니다. NetAppSystem Manager를 사용하거나 스토리지 콘솔 명령줄을 사용하여 이러한 작업을 수행할 수 있습니다.

Oracle 데이터베이스용 플러그인을 사용하기 전에 SnapCenter 관리자는 SnapCenter 서버를 설치 및 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다. "자세한 정보"
- 스토리지 시스템 접속을 추가하여 SnapCenter 환경을 구성합니다. "자세한 정보"

SnapCenter은 서로 다른 클러스터에서 동일한 이름의 여러 SVM을 지원하지 않습니다. SVM 등록 또는 클러스터 등록을 사용하여 SnapCenter에 등록된 각 SVM은 고유해야 합니다.

- 설치 사용자에 대해 인증 모드를 Linux 또는 AIX로 사용하여 자격 증명을 작성합니다. "자세한 정보"
- 호스트를 추가하고 플러그인을 설치한 다음 리소스를 검색합니다.
- SnapCenter 서버를 사용하여 VMware RDM LUN 또는 VMDK에 상주하는 Oracle 데이터베이스를 보호하는 경우 VMware vSphere용 SnapCenter 플러그인을 구축하고 SnapCenter에 플러그인을 등록해야 합니다.
- Linux 또는 AIX 호스트에 Java를 설치합니다.

  을 참조하십시오 "Linux 호스트 요구 사항" 또는 "AIX 호스트 요구 사항" 를 참조하십시오.

- 애플리케이션 방화벽의 시간 초과 값을 3시간 이상으로 설정해야 합니다.
- NFS 환경에 Oracle 데이터베이스가 있는 경우 마운트, 클론, 검증 및 복원 작업을 수행하려면 운영 스토리지 또는 2차 스토리지에 대해 NFS 데이터 LIF를 하나 이상 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 주소가 클론 복제된 볼륨에 대한 SVM(Storage Virtual Machine)의 NFS 스토리지 엑스포트 정책에 추가됩니다. 특정 IP 주소를 사용하거나 IP 주소의 하위 집합으로 제한하려면 Set-PreferredHostIPsInStorageExportPolicy CLI를 실행합니다.
  - SVM에 여러 데이터 경로(LIF)가 있을 경우 SnapCenter은 NFS 클론 복제된 볼륨을 마운트하기 위해 적절한 데이터 경로(LIF)를 선택합니다. 그러나 특정 데이터 경로(LIF)를 지정하려면 Set-SvmPreferredDataPath CLI를 실행해야 합니다.
    자세한 내용은 명령 참조 가이드를 참조하십시오.
- SAN 환경에 Oracle 데이터베이스가 있는 경우 다음 가이드에 설명된 권장 사항에 따라 SAN 환경을 구성해야 합니다.
  - "Linux Unified Host Utilities의 권장 호스트 설정"
  - "ONTAP 스토리지에 Linux 호스트 사용"
  - "AIX 호스트 유틸리티의 영향을 받는 호스트 설정"
- Oracle Linux 또는 RHEL 운영 체제의 LVM에 Oracle 데이터베이스가 있는 경우 최신 버전의 LVM(Logical Volume Management)을 설치합니다.
- Oracle용 SnapManager를 사용하고 있고 Oracle 데이터베이스용 SnapCenter 플러그인으로 마이그레이션하려는 경우 sccli 명령 sc-migrate 를 사용하여 프로필을 SnapCenter의 정책 및 리소스 그룹으로 마이그레이션할 수 있습니다.
- 백업 복제를 원하는 경우 ONTAP에서 SnapMirror 및 SnapVault를 구성합니다

SnapCenter 4.1.1 사용자의 경우 VMware vSphere 4.1.1 용 SnapCenter 플러그인 설명서에 가상화 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 나와 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 VMware vSphere용 SnapCenter 플러그인을 사용하여 가상화된 데이터베이스 및 파일 시스템을 보호하는 방법에 대한 정보가 수록되어 있습니다. SnapCenter 4.3.x 사용자의 경우 SnapCenter Plug-in for VMware vSphere 4.3 설명서에는 Linux 기반 SnapCenter Plug-in for VMware vSphere 가상 어플라이언스(오픈 가상 어플라이언스 형식)를 사용하여 가상화된 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 수록되어 있습니다.

- 자세한 정보 찾기 *

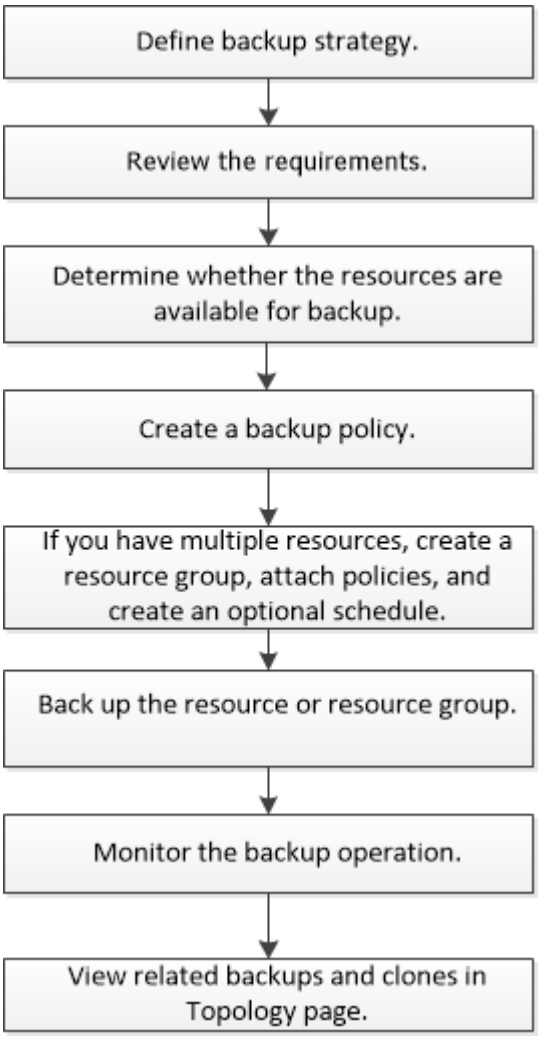
- "상호 운용성 매트릭스 툴"
- "VMware vSphere용 SnapCenter 플러그인 설명서"
- "RHEL 7 이상의 비 다중 경로 환경에서 데이터 보호 작업이 실패합니다"

Oracle 데이터베이스를 백업합니다

백업 절차 개요

리소스(데이터베이스) 또는 리소스 그룹의 백업을 생성할 수 있습니다. 백업 절차에는 계획 수립, 백업을 위한 리소스 식별, 백업 정책 생성, 리소스 그룹 생성 및 정책 연결, 백업 생성 및 작업 모니터링이 포함됩니다.

다음 워크플로에서는 백업 작업을 수행해야 하는 순서를 보여 줍니다.



Oracle 데이터베이스에 대한 백업을 생성하는 동안 데이터베이스에서 여러 작업이 실행되지 않도록 Oracle 데이터베이스 호스트의 */var/opt/snapcenter/sSCO/lock_directory*에 운영 잠금 파일(.sm_lock_dbsid_)이 생성됩니다. 데이터베이스가 백업되면 운영 잠금 파일이 자동으로 제거됩니다.

그러나 이전 백업이 경고와 함께 완료된 경우 운영 잠금 파일이 삭제되지 않고 다음 백업 작업이 대기 큐로 들어갑니다. sm_lock_dbsid * 파일이 삭제되지 않으면 결국 취소될 수 있습니다. 이러한 경우 다음 단계를 수행하여 운영 잠금

파일을 수동으로 삭제해야 합니다.

1. 명령 프롬프트에서 _ /var/opt/snapcenter/sSCO/lock_ 로 이동합니다.
2. 작동 잠금을 삭제합니다.`rm -rf .sm_lock_dbsid.`

백업 구성 정보

백업에 지원되는 **Oracle** 데이터베이스 구성

SnapCenter는 서로 다른 Oracle 데이터베이스 구성의 백업을 지원합니다.

- Oracle 독립형
- Oracle RAC(Real Application Clusters)
- Oracle 독립형 레거시
- Oracle CDB(Standalone Container Database)
- Oracle Data Guard 대기

  Data Guard 대기 데이터베이스의 오프라인 마운트 백업만 생성할 수 있습니다. 오프라인 종료 백업, 아카이브 로그만 백업 및 전체 백업은 지원되지 않습니다.

- Oracle Active Data Guard 대기

  Active Data Guard 대기 데이터베이스의 온라인 백업만 생성할 수 있습니다. 아카이브 로그 전용 백업 및 전체 백업은 지원되지 않습니다.

  Data Guard 대기 또는 Active Data Guard 대기 데이터베이스의 백업을 생성하기 전에 관리 복구 프로세스(MRP)가 중지되고 백업이 생성되면 MRP가 시작됩니다.

- 자동 스토리지 관리(ASM)
  - 가상 머신 디스크(VMDK)의 ASM 독립 실행형 및 ASM RAC

    Oracle 데이터베이스에 지원되는 모든 복원 방법 중에서 VMDK에서 ASM RAC 데이터베이스의 연결 및 복사 복원만 수행할 수 있습니다.

  - ASM 독립 실행형 및 RDM(ASM RAC on Raw Device Mapping)
    를 누릅니다
    ASMLib를 사용하거나 사용하지 않고 ASM의 Oracle 데이터베이스에 대해 백업, 복원 및 복제 작업을 수행할 수 있습니다.
  - Oracle ASM 필터 드라이버(ASMFD)

    PDB 마이그레이션 및 PDB 복제 작업은 지원되지 않습니다.

  - Oracle Flex ASM

지원되는 Oracle 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

Oracle 데이터베이스에 지원되는 백업 유형입니다

백업 유형은 생성할 백업 유형을 지정합니다. SnapCenter는 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 데이터베이스 백업을 생성할 수 있습니다.

온라인 백업의 일부로 다음 파일의 백업을 생성할 수 있습니다.

- 데이터 파일 및 제어 파일만
- 보관 로그 파일만(이 시나리오에서는 데이터베이스가 백업 모드로 전환되지 않음)
- 데이터 파일, 제어 파일 및 아카이브 로그 파일을 포함하는 전체 데이터베이스입니다

오프라인 백업

데이터베이스가 마운트되었거나 종료 상태일 때 생성된 백업을 오프라인 백업이라고 합니다. 오프라인 백업을 콜드 백업이라고도 합니다. 데이터 파일만 포함하고 오프라인 백업에는 제어 파일을 포함할 수 있습니다. 오프라인 마운트 또는 오프라인 종료 백업을 생성할 수 있습니다.

- 오프라인 마운트 백업을 생성할 때는 데이터베이스가 마운트된 상태인지 확인해야 합니다.

  데이터베이스가 다른 상태인 경우 백업 작업이 실패합니다.

- 오프라인 종료 백업을 생성할 때 데이터베이스는 아무 상태에나 있을 수 있습니다.

  백업을 생성하기 위해 데이터베이스 상태가 필수 상태로 변경됩니다. 백업을 생성한 후 데이터베이스 상태가 원래 상태로 되돌아갑니다.

SnapCenter가 **Oracle** 데이터베이스를 검색하는 방법

리소스는 SnapCenter에서 유지 관리하는 호스트의 Oracle 데이터베이스입니다. 사용 가능한 데이터베이스를 발견한 후 이러한 데이터베이스를 리소스 그룹에 추가하여 데이터 보호 작업을 수행할 수 있습니다.

다음 섹션에서는 SnapCenter가 다양한 유형의 Oracle 데이터베이스를 검색하는 데 사용하는 프로세스에 대해 설명합니다.

Oracle 버전 **11***g*_ ~ *12***c__R1**

RAC 데이터베이스

RAC 데이터베이스는 /etc/oratab 항목을 기준으로 검색됩니다. /etc/oratab 파일에 데이터베이스 항목이 있어야 합니다.

독립 실행형

독립 실행형 데이터베이스는 /etc/oratab 항목을 기준으로 검색됩니다.

ASM

ASM 인스턴스 항목은 /etc/oratab 파일에서 사용할 수 있어야 합니다.

RAC One Node

RAC One Node 데이터베이스는 /etc/oratab 항목을 기준으로 검색됩니다.
데이터베이스는 nomount, mount 또는 open 상태여야 합니다. /etc/oratab 파일에 데이터베이스 항목이 있어야 합니다.

데이터베이스가 이미 검색되고 백업이 데이터베이스에 연결되어 있는 경우 RAC One Node 데이터베이스 상태가 이름 변경 또는 삭제됨으로 표시됩니다.

데이터베이스가 재배치되면 다음 단계를 수행해야 합니다.

1. 페일오버된 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 현재 데이터베이스를 호스팅하는 RAC 노드에 기본 클러스터 노드를 설정하도록 데이터베이스를 구성합니다.
5. SnapCenter 작업을 수행합니다.
6. 한 노드에서 다른 노드로 데이터베이스를 재배치하고 이전 노드의 oratab 항목이 삭제되지 않은 경우 동일한 데이터베이스가 두 번 표시되지 않도록 oratab 항목을 수동으로 삭제하십시오.

Oracle 버전 **12cR2 ~ 18C**의 경우

RAC 데이터베이스

srvctl config 명령을 사용하여 RAC 데이터베이스를 검색할 수 있습니다.
/etc/oratab 파일에 데이터베이스 항목이 있어야 합니다.

독립 실행형

독립 실행형 데이터베이스는 /etc/oratab 파일의 항목과 srvctl config 명령의 출력을 기반으로 검색됩니다.

ASM

ASM 인스턴스 항목은 /etc/oratab 파일에 있을 필요가 없습니다.

RAC One Node

srvctl config 명령만 사용하여 RAC One Node 데이터베이스를 검색할 수 있습니다.
데이터베이스는 nomount, mount 또는 open 상태여야 합니다. 데이터베이스가 이미 검색되고 백업이 데이터베이스에 연결되어 있는 경우 RAC One Node 데이터베이스 상태가 이름 변경 또는 삭제됨으로 표시됩니다.

데이터베이스가 재배치되면 다음 단계를 수행해야 합니다.
. 리소스를 수동으로 새로 고칩니다.
. 리소스 페이지에서 RAC One Node 데이터베이스를 선택한 다음 데이터베이스 설정을 클릭합니다.
. 데이터베이스를 현재 데이터베이스를 호스팅하는 RAC 노드에 기본 클러스터 노드를 설정하도록 데이터베이스를 구성합니다.
. SnapCenter 작업을 수행합니다.

/etc/oratab 파일에 Oracle 12*c*r2 및 18*c*database 항목이 있고 동일한 데이터베이스가 srvctl config 명령에 등록되어 있는 경우 SnapCenter는 중복 데이터베이스 항목을 제거합니다.
오래된 데이터베이스 항목이 있으면 데이터베이스가 검색되지만 데이터베이스에 연결할 수 없으며 상태가 오프라인 상태가 됩니다.

RAC 설정의 1차 노드

Oracle RAC(Real Application Clusters) 설정에서 SnapCenter가 백업 작업을 수행하는 데 사용하는 기본 노드를 지정할 수 있습니다. 기본 설정 노드를 지정하지 않으면 SnapCenter가 노드를 기본 설정 노드로 자동 할당하고 해당 노드에 백업이 생성됩니다.

선호하는 노드는 RAC 데이터베이스 인스턴스가 있는 클러스터 노드 중 하나 또는 모두가 될 수 있습니다. 백업 작업은 기본 설정 순서대로 이러한 기본 설정 노드에서만 트리거됩니다.

예

RAC 데이터베이스 cdbrac에는 node1의 cdbrac1, node2의 cdbrac2, node3의 cdbrac3 등 세 가지 인스턴스가 있습니다.

노드 1과 노드 2 인스턴스는 노드 2가 첫 번째 기본 설정이고 노드 1이 두 번째 기본 설정인 기본 노드로 구성됩니다. 백업 작업을 수행할 때 노드 2가 첫 번째 기본 설정 노드이므로 이 작업이 먼저 시도됩니다.

플러그인 에이전트가 호스트에서 실행되고 있지 않은 등의 여러 가지 이유로 인해 노드 2가 백업할 상태가 아닌 경우 호스트의 데이터베이스 인스턴스가 지정된 백업 유형에 대해 필요한 상태가 아닌 경우 또는 FlexASM 구성에서 노드 2의 데이터베이스 인스턴스를 로컬 ASM 인스턴스에서 제공하지 않으면 노드 1에서 작업을 시도합니다.

노드 3은 기본 노드 목록에 없으므로 백업에 사용되지 않습니다.

Flex ASM 설정

Flex ASM 설정에서 카디널리티가 RAC 클러스터의 노드 수보다 적은 경우 Leaf 노드가 기본 노드로 표시되지 않습니다. Flex ASM 클러스터 노드 역할이 변경된 경우 원하는 노드가 새로 고쳐지도록 수동으로 검색해야 합니다.

필요한 데이터베이스 상태입니다

기본 노드의 RAC 데이터베이스 인스턴스가 백업을 성공적으로 완료하려면 필수 상태여야 합니다.

- 구성된 기본 노드의 RAC 데이터베이스 인스턴스 중 하나가 열려 있어야 온라인 백업을 생성할 수 있습니다.
- 구성된 기본 노드의 RAC 데이터베이스 인스턴스 중 하나는 마운트 상태여야 하며, 다른 기본 노드를 비롯한 다른 모든 인스턴스는 마운트 상태 또는 그 아래에 있어야 오프라인 마운트 백업을 생성할 수 있습니다.
- RAC 데이터베이스 인스턴스는 임의의 상태에 있을 수 있지만 오프라인 종료 백업을 생성하려면 기본 노드를 지정해야 합니다.

Oracle Recovery Manager를 사용하여 백업을 카탈로그로 만드는 방법

Oracle RMAN(Recovery Manager)을 사용하여 Oracle 데이터베이스 백업의 카탈로그를 만들어 Oracle RMAN 저장소에 백업 정보를 저장할 수 있습니다.

나중에 블록 레벨 복구 또는 테이블스페이스 시점 복구 작업에 카탈로그 작성된 백업을 사용할 수 있습니다. 이러한 카탈로그 작성된 백업이 필요하지 않은 경우 카탈로그 정보를 제거할 수 있습니다.

카탈로그를 작성하려면 데이터베이스가 마운트됨 또는 상위 상태여야 합니다. 데이터 백업, 아카이브 로그 백업 및 전체 백업에 대한 카탈로그를 작성할 수 있습니다. 여러 데이터베이스가 있는 리소스 그룹의 백업에 대해 카탈로그 작성을 사용하는 경우 각 데이터베이스에 대해 카탈로그가 수행됩니다. Oracle RAC 데이터베이스의 경우 데이터베이스가 마운트된 상태 이상인 기본 노드에서 카탈로그가 수행됩니다.

RAC 데이터베이스의 백업을 카탈로그로 만들려는 경우 해당 데이터베이스에 대해 실행 중인 다른 작업이 없는지

확인합니다. 다른 작업이 실행 중인 경우, 카탈로그 작성 작업이 대기열에 있는 것이 아니라 실패합니다.

외부 카탈로그 데이터베이스

기본적으로 대상 데이터베이스 컨트롤 파일은 카탈로그로 사용됩니다. 외부 카탈로그 데이터베이스를 추가하려면 SnapCenter 그래픽 사용자 인터페이스(GUI)의 데이터베이스 설정 마법사를 사용하여 외부 카탈로그의 자격 증명 및 TNS(투명 네트워크 기판) 이름을 지정하여 데이터베이스를 구성할 수 있습니다. 또한 CLI에서 -OracleRmanCatalogCredentialName 및 -OracleRmanCatalogTnsName 옵션과 함께 Configure-SmOracleDatabase 명령을 실행하여 외부 카탈로그 데이터베이스를 구성할 수도 있습니다.

RMAN 명령

SnapCenter GUI에서 Oracle 백업 정책을 생성하는 동안 카탈로그 작성 옵션을 활성화한 경우, 백업 작업의 일부로 Oracle RMAN을 사용하여 백업 카탈로그를 작성합니다. 를 실행하여 지연된 백업 카탈로그를 수행할 수도 있습니다 `Catalog-SmBackupWithOracleRMAN` 명령.

백업을 카탈로그로 작성한 후 을 실행할 수 있습니다 `Get-SmBackupDetails` 카탈로그 작성된 데이터 파일의 태그, 제어 파일 카탈로그 경로, 카탈로그 작성된 아카이브 로그 위치 등과 같은 카탈로그 작성된 백업 정보를 얻는 명령입니다.

이름 지정 형식입니다

SnapCenter 3.0에서 ASM 디스크 그룹 이름이 16자 이상인 경우 백업에 사용되는 명명 형식은 SC_HASHCODEofDISKGROUP_DBSID_BACKUPID입니다. 그러나 디스크 그룹 이름이 16자 미만인 경우 백업에 사용되는 명명 형식은 DISKGROUPNAME_DBSID_BACKUPID이며, 이는 SnapCenter 2.0에서 사용되는 것과 동일한 형식입니다.

HASHCODEofDISKGROUP은 각 ASM 디스크 그룹에 대해 자동으로 생성되는 번호(2 ~ 10자리)입니다.

크로스체크 작업

교차 검사를 수행하여 리포지토리 레코드가 물리적 상태와 일치하지 않는 백업에 대한 오래된 RMAN 리포지토리 정보를 업데이트할 수 있습니다. 예를 들어, 사용자가 운영 체제 명령을 사용하여 디스크에서 아카이빙된 로그를 제거할 경우, 제어 파일은 로그가 디스크에 있음을 계속 표시합니다(실제로는 그렇지 않음).

crosscheck 작업을 사용하면 제어 파일을 정보로 업데이트할 수 있습니다. Set-SmConfigSettings 명령을 실행하고 enable_crosscheck 매개 변수에 true 값을 할당하여 크로스검사를 활성화할 수 있습니다. 기본값은 false 로 설정됩니다.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

카탈로그 정보를 제거합니다

Uncatalog-SmBackupWithOracleRMAN 명령을 실행하여 카탈로그 정보를 제거할 수 있습니다. SnapCenter GUI를 사용하여 카탈로그 정보를 제거할 수 없습니다. 그러나 백업을 삭제하거나 카탈로그 작성된 백업과 관련된 보존 및 리소스 그룹을 삭제하는 동안 카탈로그 작성된 백업 정보가 제거됩니다.

> SnapCenter 호스트를 강제로 삭제하면 해당 호스트와 연결된 카탈로그 작성된 백업 정보가 제거되지 않습니다. 호스트를 강제로 삭제하기 전에 해당 호스트에 대한 모든 카탈로그 작성된 백업의 정보를 제거해야 합니다.

작업 시간이 ORACLE_PLUGIN_RMAN_catalog_timeout 매개 변수에 지정된 시간 초과 값을 초과했기 때문에

카탈로그 작성 및 카탈로그 작성 취소에 실패한 경우 다음 명령을 실행하여 매개 변수 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"
```

매개 변수 값을 수정한 후 다음 명령을 실행하여 SnapCenter SPL(Plug-in Loader) 서비스를 다시 시작합니다.

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

명령에 사용할 수 있는 매개 변수와 이에 대한 설명은 get-help command_name 을 실행하여 얻을 수 있습니다. 또는 를 참조할 수도 있습니다 "SnapCenter 소프트웨어 명령 참조 가이드".

백업 특정 처방과 **PS**에 대한 사전 정의된 환경 변수입니다

SnapCenter를 사용하면 백업 정책을 생성하는 동안 처방과 PS를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다. 이 기능은 VMDK를 제외한 모든 Oracle 구성에서 지원됩니다.

SnapCenter는 셸 스크립트가 실행되는 환경에서 직접 액세스할 수 있는 매개 변수의 값을 미리 정의합니다. 스크립트를 실행할 때 이러한 매개 변수의 값을 수동으로 지정할 필요는 없습니다.

백업 정책 생성을 위해 지원되는 사전 정의된 환경 변수입니다

- * SC_JOB_ID * 는 작업의 작업 ID를 지정합니다.

  예: 256

- * SC_ORACLE_SID * 는 데이터베이스의 시스템 식별자를 지정합니다.

  작업에 여러 데이터베이스가 포함된 경우 매개 변수는 파이프로 분리된 데이터베이스 이름을 포함합니다.

  이 매개 변수는 애플리케이션 볼륨에 대해 채워집니다.

  예: NFSB32 | NFSB31

- * sc_host * 는 데이터베이스의 호스트 이름을 지정합니다.

  RAC의 경우 호스트 이름은 백업이 수행되는 호스트의 이름입니다.

  이 매개 변수는 애플리케이션 볼륨에 대해 채워집니다.

  예: scsmohost2.gdl.englabe.netapp.com

- * SC_OS_USER * 는 데이터베이스의 운영 체제 소유자를 지정합니다.

  데이터는 <db1>@<osuser1>|<DB2>@<osuser2>로 포맷됩니다.

  예: NFSB31@ Oracle | NFSB32@ Oracle

- * SC_OS_GROUP * 은 데이터베이스의 운영 체제 그룹을 지정합니다.

  데이터는 <db1>@<osgroup1> | <db2>@<osgroup2> 형식으로 지정됩니다.

예: NFSB31@ 설치 | NFSB32@ oinstall

- * sc_backup_type * "은 백업 유형을 지정합니다(온라인 전체, 온라인 데이터, 온라인 로그, 오프라인 종료, 오프라인 마운트).

  예:

  - 전체 백업의 경우: ONLINEFULL
  - 데이터 전용 백업: ONLINEDATA
  - 로그 전용 백업: ONLINELOG
- * SC_BACKUP_NAME * 은 백업 이름을 지정합니다.

  이 매개 변수는 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 매개 변수는 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: hourly | data@days:3 | log@count:4
  - 필요 시 데이터 백업 전용: OnDemand | data@count:2
  - 필요 시 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 SVM과 데이터 파일 디렉토리의 볼륨 간 스토리지 매핑을 지정합니다. LUN 및 qtree에 대한 상위 볼륨의 이름이 됩니다.

  데이터는 <db1>@<SVM1:volume1>|<DB2>@<SVM2:volume2>로 포맷됩니다.

예:

- 동일한 리소스 그룹에 있는 2개의 데이터베이스: NFSB32@b 벅:/vol/scspr2417819002_NFS_CDB_NFSB32_data | NFSB31@ 벅:/vol/scs42417819002_NFS_CDB_NFSB31_data
- 데이터 파일이 있는 단일 데이터베이스가 여러 볼륨에 분산되어 있는 경우: b 벅:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA, herculus:/vol/scspr2417819002_NFS

- * SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH * 는 SVM과 로그 파일 디렉토리의 볼륨 간 스토리지 매핑을 지정합니다. LUN 및 qtree에 대한 상위 볼륨의 이름이 됩니다.

  예:

  - 단일 데이터베이스 인스턴스의 경우: 벅:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
  - 여러 데이터베이스 인스턴스의 경우: NFSB31@ 벅:/vol/sspr2417819002_NFS_CDB_NFSB31_REDO|NFSB32@벅:/vol/sscspr2417819002_NFS_CDB_NFSB32_REDO

- * sc_primary_full_snapshot_name_for_tag * 는 스토리지 시스템 이름과 볼륨 이름이 포함된 스냅샷의 목록을 지정합니다.

  예:

  - 단일 데이터베이스 인스턴스의 경우: b 벅:/vol/scspr2417819002_nfs_cdb_NFSB32_data/RG2_scspr2417819002_07-21-2021-221_02.28.26.3973_0, 벅:/vol/scspr2417819002_nfs_cdb_nfs_redo_r2032_sprsd-28.07226873_228228228721-2267_2327_02.07_02.73_02.
  - 다중 데이터베이스 인스턴스의 경우: NFSB32@ 벅:/vol/scspr2417819002_nfs_cdb_NFSB32_data/RG2_scspr2417819002_07_07-21-2021-2021_02.28.28.26.3973_0, /vol/scsprec2417819002_sprdl_sprec282282dl_sprdl_sCDB_sprdl_s2021.22.1722.172282dl_sCDB_sCDB_sCDB_sCDB_sprdcdb_sCDB_s20122.1722.07_sCDB_22822.07_sCDB_22.1722.07_sCDB_sCDB_s2022_sCDB_S22.07_S22.1722822_22822_27.07_27.07_27.07_27.07_27.

- * 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
  - 2개의 볼륨이 포함된 정합성 보장 그룹 스냅샷: CG3_R80404CBEF5V1_04-05-2021_03.08.08.4945_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 마운트되어 있으며 백업 중인 파일의 직접적인 부모가 아닌 디렉토리가 포함됩니다. ASM 구성의 경우 디스크 그룹의 이름입니다.

  데이터는 <db1>@<mountpoint1, mountpoint2>|<DB2>@<mountpoint1, mountpoint2>로 포맷됩니다.

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
- ASM: + 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_07-2323_2mnt_323_2n32

* * sc_ARCHIVELOGS_locations * 는 아카이브 로그 디렉토리의 위치를 지정합니다.

  디렉토리 이름은 아카이브 로그 파일의 직접적인 부모가 됩니다. 아카이브 로그가 둘 이상의 위치에 있으면 모든 위치가 캡처됩니다. 여기에는 FRA 시나리오도 포함됩니다. 디렉토리에 대해 소프트링크가 사용되는 경우 동일한 파일이 채워집니다.

  예:

  - NFS:/mnt/nfsdb2_log의 단일 데이터베이스
  - NFS의 여러 데이터베이스와 두 개의 다른 위치에 배치된 NFSB31@/mnt/nfsdb31_log1, /mnt/nfsdb31_log2|NFSB32@/mnt/nfsdb32_log의 경우
  - ASM:+LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15용

* * sc_redo_logs_locations * 는 redo 로그 디렉토리의 위치를 지정합니다.

  디렉토리 이름은 redo 로그 파일의 바로 상위 항목이 됩니다. 디렉토리에 대해 소프트링크가 사용되는 경우 동일한 파일이 채워집니다.

  예:

  - NFS:/mnt/nfsdb2_data/newdb1의 단일 데이터베이스
  - NFS에 있는 여러 데이터베이스의 경우: NFSB31@/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/newdb32
  - ASM:+LOG2DG/ASMDB2/ONLINELOG의 경우

* * sc_control_files_locations * 는 제어 파일 디렉토리의 위치를 지정합니다.

  디렉터리 이름은 제어 파일의 바로 상위 항목이 됩니다. 디렉토리에 대해 소프트링크가 사용되는 경우 동일한 파일이 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/nfsdb32, /mnt/nfsdb32_data/ndb32
- ASM:+LOG2DG/ASMDB2/controlfile의 경우

- * sc_data_files_locations * "는 데이터 파일 디렉토리의 위치를 지정합니다.

  디렉터리 이름은 데이터 파일의 바로 상위 항목이 됩니다. 디렉토리에 대해 소프트링크가 사용되는 경우 동일한 파일이 채워집니다.

  예:

  - NFS:/mnt/nfsdb3_data1, /mnt/nfsdb3_data/NEWDB3/datafile의 단일 데이터베이스
  - NFS:NFSB31@/mnt/nfsdb31_data1, /mnt/nfsdb31_data/NEWDB31/datafile|NFSB32@/mnt/nfsdb32_data1, /mnt/nfsdb32_data/NEWDB32/datafile의 여러 데이터베이스에 대해
  - ASM:+DATA2DG/ASMDB2/데이터 파일, +DATA2DG/ASMDB2/TEMPFILE

- * sc_snapshot_label * 은 보조 레이블의 이름을 지정합니다.

  예: 시간별, 일별, 주별, 월별 또는 사용자 지정 레이블

지원되는 구분 기호

- *: * 은 SVM 이름과 볼륨 이름을 구분하는 데 사용됩니다

  예: buck:/vol/scspr2417819002_nfs_cdb_NFSB32_data/RG2_scspr24178002_07-21-2021_02.28.26.3973_0, b 벅:/vol/sprspr2417819002_nfs_cdb_NFSB32_redo/RG2_scspr2417819002_28.07_02.73_22.73_02.07_02.73_02.73_02.73_02.73_

- * @ * 는 데이터를 데이터베이스 이름과 분리하고 해당 키와 값을 구분하는 데 사용됩니다.

  예:

  - NFSB32@b벅:/vol/scspr24178002_nfs_cdb_NFSB32_data/RG2_scprsprs2417819002_07_07-21-2021-2021_02.28.28.26.3973_0_sprdl: /vol/sprec1782.172262282dl_sCDB_sprdl_n22.1722.1722.1722.172dl_ndl_22.1722.1722.172dl_n22.1722.172dl_ndcdb_n22.1722.1722.1722.172dl_ndcdb_22.172dl_22.07_ndl_ndcdb_ndl_22.1722.1722.07_ndcdb_n22.1782.1722.1722.1722.1722.07_2
  - NFSB31@Oracle|NFSB32@Oracle

- * | * 는 서로 다른 두 데이터베이스 간에 데이터를 분리하고 SC_BACKUP_ID, SC_BACKUP_RETENTION 및 SC_BACKUP_NAME 매개 변수에 대해 서로 다른 두 엔터티 간에 데이터를 분리하는 데 사용됩니다.

  예:

  - Data @ 203 | log @ 205
  - hourly | data@days:3 | log@count:4
  - DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0 | LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1

- * / * 는 SC_PRIMARY_SNACSHOT_NAME 및 SC_PRIMARY_FULL_SNSHOT_NAME_FOR_TAG 매개변수에 대한 스냅숏에서 볼륨 이름을 구분하는 데 사용됩니다.

  예: NFSB32@벅:/vol/scspr2417819002_nfs_cdb_NFSB32_data/RG2_scspr2417819002_07-21-2021-2021_02.28.26.3973_0, 벅:/vol/sprspr2417819002_nfs_cdb_nfs_redo_rredo/RG2_sc2822.17226722_327_2021-282327_327_sprec2021-282327_

- *, * 는 동일한 DB에 대한 변수 세트를 구분하는 데 사용됩니다.

  예: -NFSB32@벅:/vol/scspr24178002_nfs_cdb_NFSB32_data/RG2_scsprspr2417819002_07_07-21-2021-2021_02.28.28.28.26.3973_0, duck: /vol/scsprec17819002_sprecdl_n22.1727.21_sprdl_sprdcdb_22.1722.1722.07_27.21_sCDB_ndl_s2021_sCDB_ndl_sprdl_22.1722.1722.1722.1722.1722.17228002_ndl_sCDB_sCDB_228002_sCDB_228228002_sCDB_sCDB_228002_228002_s20127.21_27.07_27.07_s

백업 보존 옵션

백업 복사본을 보존할 일 수를 선택하거나 유지할 백업 복사본 수를 최대 255개 사본의 ONTAP로 지정할 수 있습니다. 예를 들어, 조직에서 10일간 백업 복사본 또는 130개의 백업 복사본을 보존해야 할 수도 있습니다.

정책을 생성하는 동안 백업 유형 및 스케줄 유형에 대한 보존 옵션을 지정할 수 있습니다.

SnapMirror 복제를 설정하면 보존 정책이 대상 볼륨에 미러링됩니다.

SnapCenter는 스케줄 유형과 일치하는 보존 레이블이 있는 보존된 백업을 삭제합니다. 리소스 또는 리소스 그룹에 대한 스케줄 유형이 변경된 경우 이전 스케줄 유형 레이블이 있는 백업이 시스템에 남아 있을 수 있습니다.

백업 복사본을 장기간 보존하려면 SnapVault 백업을 사용해야 합니다.

백업 스케줄

백업 빈도(스케줄 유형)는 정책에 지정되며 백업 스케줄은 리소스 그룹 구성에 지정됩니다. 백업 빈도 또는 스케줄을 결정하는 가장 중요한 요소는 리소스의 변경 속도 및 데이터의 중요도입니다. 자주 사용하는 리소스를 매일 한 번씩 백업할 수도 있고, 자주 사용하지 않는 리소스를 하루에 한 번 백업할 수도 있습니다. 기타 요인으로는 조직에 대한 리소스의 중요성, SLA(서비스 수준 계약) 및 RPO(복구 시점 목표)가 있습니다.

SLA는 예상되는 서비스 수준을 정의하고 가용성 및 서비스 성능을 비롯한 다양한 서비스 관련 문제를 해결합니다. RPO는 장애 후 정상적인 작업을 재개하기 위해 백업 스토리지에서 복구해야 하는 파일의 사용 기간에 대한 전략을 정의합니다. SLA 및 RPO는 데이터 보호 전략에 기여합니다.

사용량이 많은 리소스의 경우에도 하루에 한 번 또는 두 번 이상 전체 백업을 실행할 필요가 없습니다. 예를 들어 정기적인 트랜잭션 로그 백업만으로도 필요한 백업이 있는지 확인할 수 있습니다. 데이터베이스를 더 자주 백업할수록 SnapCenter는 복원 시 사용해야 하는 트랜잭션 로그를 더 적게 사용하여 복원 작업을 더 빠르게 수행할 수 있습니다.

백업 스케줄은 다음과 같이 두 부분으로 구성됩니다.

- 백업 빈도

일부 플러그인에 대해 _schedule type_이라는 백업 빈도(백업 수행 빈도)는 정책 구성의 일부입니다. 정책의 백업 빈도로 시간별, 일별, 주별 또는 월별 을 선택할 수 있습니다. 이러한 빈도 중 하나를 선택하지 않으면 생성된 정책이 온디맨드 전용 정책입니다. 설정 * > * 정책 * 을 클릭하여 정책에 액세스할 수 있습니다.

- 백업 스케줄

  백업 스케줄(백업을 수행할 정확한 시점)은 리소스 그룹 구성의 일부입니다. 예를 들어 주별 백업에 대한 정책이 구성된 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 스케줄을 구성할 수 있습니다. 리소스 그룹 * > * 리소스 그룹 * 을 클릭하여 리소스 그룹 일정에 액세스할 수 있습니다.

백업 명명 규칙

기본 스냅샷 복사본 명명 규칙을 사용하거나 사용자 지정된 명명 규칙을 사용할 수 있습니다. 기본 백업 명명 규칙은 스냅샷 복사본 이름에 타임 스탬프를 추가하여 복사본이 생성된 시간을 식별하도록 도와줍니다.

스냅샷 복사본은 다음과 같은 기본 명명 규칙을 사용합니다.

```
resourcegroupname_hostname_timestamp
```

다음 예제와 같이 백업 리소스 그룹의 이름을 논리적으로 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예제에서 구문 요소는 다음과 같은 의미를 가집니다.

- _dts1_은(는) 리소스 그룹 이름입니다.
- _mach1x88_은 호스트 이름입니다.
- _03-12-2015_23.17.26_은 날짜 및 타임스탬프입니다.

또는 * Use custom name format for Snapshot copy * 를 선택하여 리소스 또는 리소스 그룹을 보호하면서 스냅샷 복사본 이름 형식을 지정할 수 있습니다. 예를 들어 customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname을 입력합니다. 기본적으로 타임스탬프 접미사가 스냅샷 복사본 이름에 추가됩니다.

Oracle 데이터베이스 백업 요구 사항

Oracle 데이터베이스를 백업하기 전에 사전 요구 사항이 완료되었는지 확인해야 합니다.

- 정책이 연결된 리소스 그룹을 만들어야 합니다.
- 보조 스토리지와 SnapMirror 관계가 있는 리소스를 백업하려면 스토리지 사용자에게 할당된 ONTAP 역할에 "'스냅샷 전체' 권한이 있어야 합니다. 그러나 "vsadmin" 역할을 사용하는 경우에는 "napmirror all" 권한이 필요하지 않습니다.
- 백업 작업에 사용 중인 애그리게이트를 데이터베이스가 사용하는 스토리지 가상 시스템(SVM)에 할당해야 합니다.
- 해당 데이터베이스에 대해 보조 보호가 설정된 경우 데이터베이스에 속한 모든 데이터 볼륨과 아카이브 로그 볼륨이 보호되는지 확인해야 합니다.
- Oracle DBVERIFY 유틸리티를 사용하여 백업을 확인하려면 ASM 디스크 그룹에 파일이 있는 데이터베이스가

""마운트" 또는 ""열기"" 상태에 있어야 합니다.

- 볼륨 마운트 지점 길이가 240자를 초과하지 않는지 확인해야 합니다.
- 백업 중인 데이터베이스가 큰 경우 SnapCenter 서버 호스트의 _C:\Program Files\NetApp\SMCore\SMCoreServiceHost.exe.config_file에서 RESTTimeout 값을 86400,000ms로 늘려야 합니다(TB 단위 크기).

  값을 수정하는 동안 실행 중인 작업이 없는지 확인하고 값을 늘린 후 SnapCenter SMCore 서비스를 다시 시작합니다.

백업에 사용할 수 있는 **Oracle** 데이터베이스에 대해 알아보십시오

리소스는 SnapCenter에서 관리하는 호스트의 Oracle 데이터베이스입니다. 사용 가능한 데이터베이스를 발견한 후 이러한 데이터베이스를 리소스 그룹에 추가하여 데이터 보호 작업을 수행할 수 있습니다.

- 필요한 것 *
- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 접속 생성, 자격 증명 추가 등의 작업을 완료해야 합니다.
- 데이터베이스가 가상 머신 디스크(VMDK) 또는 원시 디바이스 매핑(RDM)에 상주하는 경우 VMware vSphere용 SnapCenter 플러그인을 구축하고 SnapCenter에 플러그인을 등록해야 합니다.

  자세한 내용은 을 참조하십시오 "VMware vSphere용 SnapCenter 플러그인 구축".
- 데이터베이스가 VMDK 파일 시스템에 있는 경우 vCenter에 로그인하고 * VM 옵션 * > * 고급 * > * 구성 편집 * 으로 이동하여 _disk.enableUUID_의 값을 VM에 대해 TRUE로 설정해야 합니다.
- SnapCenter가 수행하는 프로세스를 검토하여 다양한 유형의 Oracle 데이터베이스를 검색해야 합니다.

1단계**: SnapCenter**가 비데이터베이스 항목을 검색하지 못하도록 합니다

SnapCenter가 oratab 파일에 추가된 비데이터베이스 항목을 검색하지 못하도록 할 수 있습니다.

- 단계 *

1. Oracle용 플러그인을 설치한 후 루트 사용자는 _ /var/opt/snapcenter/sSCO/etc/_ 디렉터리 아래에 * sc_oratab.config * 파일을 만들어야 합니다.

   나중에 파일을 유지 관리할 수 있도록 Oracle 바이너리 소유자 및 그룹에 쓰기 권한을 부여합니다.

2. 데이터베이스 관리자는 * sc_oratab.config * 파일에 비데이터베이스 항목을 추가해야 합니다.

   /etc/oratab_file의 비데이터베이스 항목에 대해 정의된 형식을 동일하게 유지하는 것이 좋습니다. 그렇지 않을 경우 사용자가 비데이터베이스 엔터티 문자열만 추가할 수 있습니다.

   문자열은 대/소문자를 구분합니다. 앞에 #이 있는 텍스트는 주석으로 처리됩니다. 설명은 뒤에 추가할 수 있습니다
   비 데이터베이스 이름입니다.

```
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
-----------------------------------------------
```

1. 리소스를 검색합니다.

   SC_oratab.config * 에 추가된 비데이터베이스 항목은 리소스 페이지에 나열되지 않습니다.

SnapCenter 플러그인을 업그레이드하기 전에 항상 SC_oratab.config 파일을 백업하는 것이 좋습니다.

2단계**:** 리소스를 검색합니다

플러그인을 설치하면 해당 호스트의 모든 데이터베이스가 자동으로 검색되어 리소스 페이지에 표시됩니다.

데이터베이스가 성공적으로 검색되도록 하려면 데이터베이스가 마운트된 상태 이상이어야 합니다. Oracle RAC(Real Application Clusters) 환경에서 검색을 수행하는 호스트의 RAC 데이터베이스 인스턴스는 데이터베이스 인스턴스를 성공적으로 검색하려면 마운트 상태 이상이어야 합니다. 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.

   을 클릭합니다 호스트 이름과 데이터베이스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 를 클릭할 수 있습니다 아이콘을 클릭하여 필터 창을 닫습니다.

3. 리소스 새로 고침 * 을 클릭합니다.

   RAC One Node 시나리오에서는 데이터베이스가 현재 호스팅되는 노드의 RAC 데이터베이스로 검색됩니다.

- 결과 *

데이터베이스는 데이터베이스 유형, 호스트 또는 클러스터 이름, 관련 리소스 그룹 및 정책, 상태와 같은 정보와 함께 표시됩니다.

데이터베이스가 SnapCenter 외부에서 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

- 데이터베이스가 비NetApp 스토리지 시스템에 있는 경우 사용자 인터페이스에 Overall Status 열에 Not Available

for Backup 메시지가 표시됩니다.

NetApp이 아닌 스토리지 시스템에 있는 데이터베이스에는 데이터 보호 작업을 수행할 수 없습니다.

- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되지 않은 경우 사용자 인터페이스에 Overall Status 열에 보호되지 않는 메시지가 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되어 있는 경우 사용자 인터페이스에 Overall Status 열에 사용 가능한 백업 메시지가 표시됩니다.

Oracle 데이터베이스 인증을 활성화한 경우 리소스 보기에 빨간색 자물쇠 아이콘이 표시됩니다. 데이터베이스를 보호하거나 리소스 그룹에 데이터베이스 자격 증명을 추가하여 데이터 보호 작업을 수행하려면 데이터베이스 자격 증명을 구성해야 합니다.

Oracle 데이터베이스에 대한 백업 정책을 생성합니다

SnapCenter를 사용하여 Oracle 데이터베이스 리소스를 백업하기 전에 백업하려는 리소스 또는 리소스 그룹에 대한 백업 정책을 만들어야 합니다. 백업 정책은 백업을 관리, 예약 및 유지하는 방법을 제어하는 규칙의 집합입니다. 복제, 스크립트 및 백업 유형 설정을 지정할 수도 있습니다. 정책을 만들면 다른 리소스 또는 리소스 그룹에서 정책을 다시 사용하려는 시간이 절약됩니다.

- 시작하기 전에 *
- 백업 전략을 정의해야 합니다.
- SnapCenter 설치, 호스트 추가, 데이터베이스 검색 및 스토리지 시스템 접속 생성과 같은 작업을 완료하여 데이터 보호를 위한 준비를 갖추어야 합니다.
- 스냅샷 복사본을 미러 또는 소산 보조 스토리지에 복제하는 경우 SnapCenter 관리자는 소스 및 대상 볼륨 모두에 대해 SVM을 할당한 상태여야 합니다.
- 플러그인을 비루트 사용자로 설치한 경우, prescpt 및 PostScript 디렉토리에 실행 권한을 수동으로 할당해야 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 페이지에 정책 이름과 설명을 입력합니다.
6. 백업 유형 페이지에서 다음 단계를 수행하십시오.

    - 온라인 백업 * 을 만들려면 * 온라인 백업 * 을 선택합니다.

      모든 데이터 파일, 제어 파일, 아카이브 로그 파일을 백업할지, 데이터 파일과 제어 파일만 백업할지, 아카이브 로그 파일만 백업할지를 지정해야 합니다.

    - 오프라인 백업 * 을 만들려면 * 오프라인 백업 * 을 선택한 후 다음 옵션 중 하나를 선택합니다.
        - 데이터베이스가 마운트된 상태일 때 오프라인 백업을 생성하려면 * Mount * 를 선택합니다.

- 데이터베이스를 종료 상태로 변경하여 오프라인 종료 백업을 만들려면 * 종료 * 를 선택합니다.

  플러깅 지원 데이터베이스(PDB)가 있고 백업을 생성하기 전에 PDB의 상태를 저장하려면 * Save state of PDB * 를 선택해야 합니다. 이렇게 하면 백업을 생성한 후 PDB를 원래 상태로 가져올 수 있습니다.

- On demand *, * Hourly *, * Daily *, * Weekly * 또는 * Monthly * 를 선택하여 일정 빈도를 지정합니다.

  리소스 그룹을 생성하는 동안 백업 작업의 스케줄(시작 날짜 및 종료 날짜)을 지정할 수 있습니다. 따라서 동일한 정책 및 백업 빈도를 공유하는 리소스 그룹을 생성할 수 있지만, 각 정책에 서로 다른 백업 스케줄을 할당할 수 있습니다.

  오전 2시에 예약된 경우 DST(일광 절약 시간) 중에는 일정이 트리거되지 않습니다.

- Oracle RMAN(Recovery Manager)을 사용하여 백업 카탈로그를 작성하려면 * Oracle RMAN(Recovery Manager)을 사용한 카탈로그 백업 * 을 선택합니다.

  GUI를 사용하거나 SnapCenter CLI 명령 Catalog-SmBackupWithOracleRMAN을 사용하여 한 번에 한 백업의 지연된 카탈로그를 수행할 수 있습니다.

  RAC 데이터베이스의 백업을 카탈로그로 만들려는 경우 해당 데이터베이스에 대해 실행 중인 다른 작업이 없는지 확인합니다. 다른 작업이 실행 중인 경우, 카탈로그 작성 작업이 대기열에 있는 것이 아니라 실패합니다.

- 백업 후 아카이브 로그를 정리하려면 * 백업 후 아카이브 로그 푸네 * 를 선택합니다.

  데이터베이스에 구성되지 않은 아카이브 로그 대상에서 아카이브 로그 잘라내기 작업이 건너뜁니다.

  Oracle Standard Edition을 사용하는 경우 아카이브 로그 백업을 수행하는 동안 log_archive_DEST 및 log_archive_duplex_DEST 매개 변수를 사용할 수 있습니다.

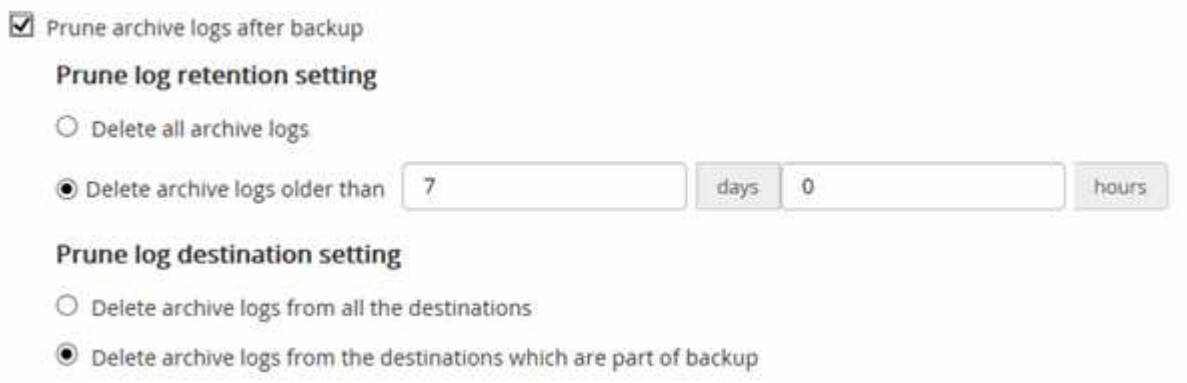
- 아카이브 로그 파일을 백업의 일부로 선택한 경우에만 아카이브 로그를 삭제할 수 있습니다.

  삭제 작업을 성공적으로 수행하려면 RAC 환경의 모든 노드가 모든 아카이브 로그 위치에 액세스할 수 있는지 확인해야 합니다.

원하는 작업	그러면...
모든 아카이브 로그를 삭제합니다	Delete all archive logs * 를 선택합니다.
오래된 아카이브 로그를 삭제합니다	Delete archive logs older than * 을 선택한 다음 일 및 시간 내에 삭제할 아카이브 로그의 기간을 지정합니다.
모든 대상에서 아카이브 로그를 삭제합니다	모든 대상에서 * 아카이브 로그 삭제 * 를 선택합니다.

원하는 작업	그러면...
백업의 일부인 로그 대상에서 아카이브 로그를 삭제합니다	백업에 포함된 대상에서 * 아카이브 로그 삭제 * 를 선택합니다.

+



7. 보존 페이지에서 백업 유형에 대한 보존 설정과 백업 유형 페이지에서 선택한 스케줄 유형을 지정합니다.

원하는 작업	그러면…
일정 수의 스냅샷 복사본을 유지합니다	유지할 총 스냅샷 복사본 * 을 선택하고 유지할 스냅샷 복사본 수를 지정합니다. 스냅샷 복사본 수가 지정된 수를 초과하면 가장 오래된 복사본이 먼저 삭제된 후 스냅샷 복사본이 삭제됩니다. ⓘ 최대 보존 값은 ONTAP 9.4 이상의 리소스에 대해 1018이고, ONTAP 9.3 이전 버전의 리소스에 대해서는 254입니다. 보존이 기본 ONTAP 버전에서 지원하는 값보다 높은 값으로 설정된 경우 백업이 실패합니다. ⓘ SnapVault 복제를 설정하려면 보존 수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷 복사본이 타겟으로 복제될 때까지 첫 번째 스냅샷 복사본이 SnapVault 관계의 참조 스냅샷 복사본이므로 보존 작업이 실패할 수 있습니다.
Snapshot 복사본을 일정 일 동안 유지합니다	스냅샷 복사본 보관 * 을 선택한 다음, 스냅샷 복사본을 삭제하기 전에 유지할 일 수를 지정합니다.

ⓘ 백업의 일부로 아카이브 로그 파일을 선택한 경우에만 아카이브 로그 백업을 보존할 수 있습니다.

8. 복제 페이지에서 복제 설정을 지정합니다.

이 필드의 내용...	수행할 작업...
로컬 스냅샷 복사본을 생성한 후 SnapMirror를 업데이트합니다	다른 볼륨에 백업 세트의 미러 복사본을 생성하려면 이 필드를 선택합니다(SnapMirror 복제).
로컬 스냅샷 복사본을 생성한 후 SnapVault를 업데이트합니다	디스크 간 백업 복제(SnapVault 백업)를 수행하려면 이 옵션을 선택합니다.
보조 정책 레이블입니다	스냅샷 레이블을 선택합니다. 선택한 스냅샷 복사본 레이블에 따라 ONTAP에서는 해당 레이블과 일치하는 2차 스냅샷 복사본 보존 정책을 적용합니다. 로컬 스냅샷 복사본 * 을 생성한 후 SnapMirror 업데이트 * 를 선택한 경우, 선택적으로 보조 정책 레이블을 지정할 수 있습니다. 그러나 로컬 스냅샷 복사본 * 을 생성한 후 * SnapVault 업데이트 * 를 선택한 경우에는 보조 정책 레이블을 지정해야 합니다.
오류 재시도 횟수입니다	작업이 중지되기 전에 허용되는 최대 복제 시도 횟수를 입력합니다.

보조 스토리지에 대한 ONTAP의 SnapMirror 보존 정책을 구성하면 보조 스토리지에서 스냅샷 복사본의 최대 제한에 도달하지 않도록 해야 합니다.

9. 스크립트 페이지에서 백업 작업 전후에 실행할 처방인 또는 PS의 경로와 인수를 각각 입력합니다.

   처방과 소인을 _ /var/opt/snapcenter/spl/scripts_ 또는 이 경로 내의 폴더에 저장해야 합니다. 기본적으로 _/var/opt/snapcenter/SPL/scripts_path가 채워집니다. 스크립트를 저장하기 위해 이 경로 내에 폴더를 만든 경우 경로에 해당 폴더를 지정해야 합니다.

   스크립트 시간 초과 값을 지정할 수도 있습니다. 기본값은 60초입니다.

   SnapCenter에서는 처방과 PS를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다. "자세한 정보"

10. 확인 페이지에서 다음 단계를 수행하십시오.
    a. 검증 작업을 수행할 백업 스케줄을 선택합니다.
    b. 검증 스크립트 명령 섹션에서 검증 작업 전후에 실행할 처방인 또는 PS의 경로와 인수를 각각 입력합니다.

       처방과 소인을 _ /var/opt/snapcenter/spl/scripts_ 또는 이 경로 내의 폴더에 저장해야 합니다. 기본적으로 _/var/opt/snapcenter/SPL/scripts_path가 채워집니다. 스크립트를 저장하기 위해 이 경로 내에 폴더를 만든 경우 경로에 해당 폴더를 지정해야 합니다.

스크립트 시간 초과 값을 지정할 수도 있습니다. 기본값은 60초입니다.

1. 요약을 검토하고 * Finish * 를 클릭합니다.

리소스 그룹을 생성하고 **Oracle** 데이터베이스에 대한 정책을 연결합니다

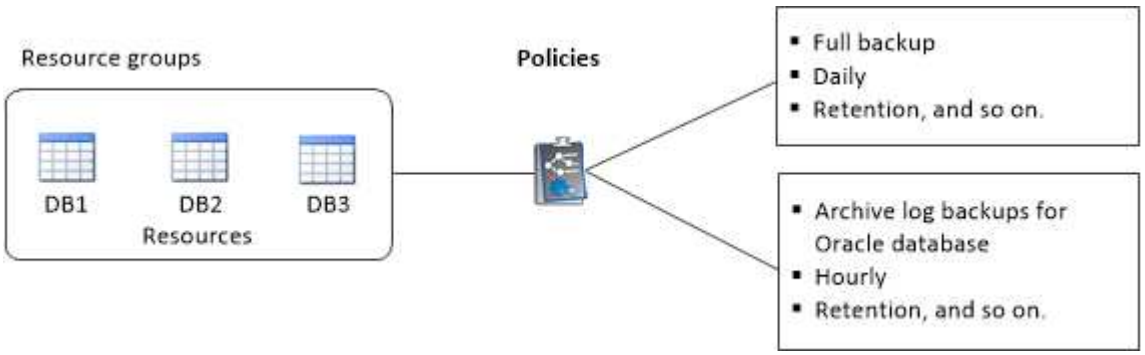
리소스 그룹은 백업 및 보호할 리소스를 추가하는 컨테이너입니다. 리소스 그룹을 사용하면 지정된 애플리케이션과 연결된 모든 데이터를 동시에 백업할 수 있습니다.

이 작업에 대해

Oracle DBVERIFY 유틸리티를 사용하여 백업을 확인하려면 ASM 디스크 그룹에 파일이 있는 데이터베이스가 "마운트" 또는 "열기" 상태여야 합니다.

하나 이상의 정책을 리소스 그룹에 연결하여 수행할 데이터 보호 작업의 유형을 정의합니다.

다음 그림에서는 데이터베이스 리소스, 리소스 그룹 및 정책 간의 관계를 보여 줍니다.



단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 선택하고 목록에서 해당 플러그인을 선택합니다.
2. 리소스 페이지에서 * 새 리소스 그룹 * 을 클릭합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.
   a. 이름 필드에 자원 그룹의 이름을 입력합니다.

      리소스 그룹 이름은 250자를 초과할 수 없습니다.

   b. 나중에 리소스 그룹을 검색할 수 있도록 태그 필드에 하나 이상의 레이블을 입력합니다.

      예를 들어 HR을 여러 자원 그룹에 태그로 추가하면 나중에 HR 태그와 연결된 모든 자원 그룹을 찾을 수 있습니다.

   c. 이 확인란을 선택하고 스냅샷 복사본 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

      예를 들어 customtext_resource group_policy_hostname 또는 resource group_hostname을 입력합니다. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.

   d. 백업하지 않을 아카이브 로그 파일의 대상을 지정합니다.
4. 리소스 페이지의 * 호스트 * 드롭다운 목록에서 Oracle 데이터베이스 호스트 이름을 선택합니다.

리소스가 성공적으로 검색된 경우에만 사용 가능한 리소스 섹션에 리소스가 나열됩니다. 최근에 추가한 자원은 자원 목록을 새로 고친 후에만 사용 가능한 자원 목록에 나타납니다.

5. 사용 가능한 리소스 섹션에서 리소스를 선택하고 선택한 리소스 섹션으로 이동합니다.

   단일 리소스 그룹의 Linux 및 AIX 호스트 모두에서 데이터베이스를 추가할 수 있습니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

   a. 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

      을 클릭하여 정책을 생성할 수도 있습니다 + .

      선택한 정책에 대한 스케줄 구성 섹션에 선택한 정책이 나열됩니다.

   b. 을 클릭합니다 + 스케줄을 구성할 정책에 대한 Configure Schedules 열에서

   c. policy_policy_name_에 대한 스케줄 추가 창에서 스케줄을 구성한 다음 * 확인 * 을 클릭합니다.

      여기서, _policy_name_은 선택한 정책의 이름입니다.

      구성된 일정이 Applied Schedules 열에 나열됩니다.

   타사 백업 스케줄은 SnapCenter 백업 스케줄과 겹치는 경우 지원되지 않습니다.

7. 확인 페이지에서 다음 단계를 수행하십시오.

   a. Load locators * 를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 스토리지에 대한 검증을 수행합니다.

   b. 을 클릭합니다 + Configure Schedules 열에서 정책의 모든 스케줄 유형에 대한 검증 스케줄을 구성합니다.

   c. Add Verification Schedules policy_name 대화 상자에서 다음 작업을 수행합니다.

원하는 작업	수행할 작업...
백업 후 확인을 실행합니다	백업 후 검증 실행 * 을 선택합니다.
검증 예약	Run scheduled verification * 을 선택한 다음 드롭다운 목록에서 일정 유형을 선택합니다.

   d. 2차 스토리지 시스템에서 백업을 확인하려면 * 2차 위치에서 확인 * 을 선택합니다.

   e. 확인 * 을 클릭합니다.

      구성된 검증 일정이 Applied Schedules 열에 나열됩니다.

8. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 자원 그룹에서 수행된 작업의

보고서를 첨부하려면 * 작업 보고서 첨부 * 를 선택합니다.

이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmtpServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

9. 요약을 검토하고 * Finish * 를 클릭합니다.

Oracle 리소스를 백업합니다

자원이 자원 그룹에 속하지 않은 경우 자원 페이지에서 자원을 백업할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 선택하고 목록에서 해당 플러그인을 선택합니다.
2. 리소스 페이지의 보기 목록에서 * 데이터베이스 * 를 선택합니다.
3. 을 클릭합니다 호스트 이름과 데이터베이스 유형을 선택하여 리소스를 필터링합니다.

   그런 다음 을 클릭할 수 있습니다 를 눌러 필터 창을 닫습니다.

4. 백업할 데이터베이스를 선택합니다.

   데이터베이스 보호 페이지가 표시됩니다.

5. 리소스 페이지에서 다음 단계를 수행할 수 있습니다.
   a. 확인란을 선택하고 스냅샷 복사본 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

      예를 들면, 다음과 같습니다. `customtext_policy_hostname` 또는 `resource_hostname`. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.

   b. 백업하지 않을 아카이브 로그 파일의 대상을 지정합니다.
6. 정책 페이지에서 다음 단계를 수행합니다.
   a. 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

      을 클릭하여 정책을 생성할 수 있습니다 .

      선택한 정책에 대한 스케줄 구성 섹션에 선택한 정책이 나열됩니다.

   b. 을 클릭합니다 스케줄 구성 열에서 원하는 정책에 대한 스케줄을 구성합니다.
   c. 정책_정책_이름_에 대한 스케줄 추가 창에서 스케줄을 구성한 다음 을 선택합니다 `OK`.

      _policy_name_은 선택한 정책의 이름입니다.

   구성된 일정이 Applied Schedules 열에 나열됩니다.
7. 확인 페이지에서 다음 단계를 수행하십시오.
   a. Load locators * 를 클릭하여 SnapMirror 또는 SnapVault 볼륨을 로드하여 보조 스토리지를 확인합니다.

b. 을 클릭합니다 Configure Schedules 열에서 정책의 모든 스케줄 유형에 대한 검증 스케줄을 구성합니다. 를 누릅니다
Add Verification Schedules_policy_name_대화 상자에서 다음 단계를 수행할 수 있습니다.

c. 백업 후 검증 실행 * 을 선택합니다.

d. Run scheduled verification * 을 선택하고 드롭다운 목록에서 일정 유형을 선택합니다.

Flex ASM 설정에서 카디널리티가 RAC 클러스터의 노드 수보다 적은 경우 Leaf 노드에서 검증 작업을 수행할 수 없습니다.

e. 보조 스토리지에서 백업을 확인하려면 * 2차 위치에서 확인 * 을 선택합니다.

f. 확인 * 을 클릭합니다.

구성된 검증 일정이 Applied Schedules 열에 나열됩니다.

8. 알림 페이지에서 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목을 지정해야 합니다. 리소스에 대해 수행된 백업 작업의 보고서를 첨부하려면 * 작업 보고서 연결 * 을 선택합니다.

이메일 알림의 경우 GUI 또는 PowerShell 명령을 사용하여 SMTP 서버 세부 정보를 지정해야 합니다 `Set-SmSmtpServer`.

9. 요약을 검토하고 * Finish * 를 클릭합니다.

데이터베이스 토폴로지 페이지가 표시됩니다.

10. 지금 백업 * 을 클릭합니다.

11. 백업 페이지에서 다음 단계를 수행하십시오.

a. 리소스에 여러 정책을 적용한 경우 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

b. 백업 * 을 클릭합니다.

12. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

작업을 마친 후

- AIX 설정에서 를 사용할 수 있습니다 `lkdev` 명령을 사용하여 및 를 잠급니다 `rendev` 백업한 데이터베이스가 있는 디스크의 이름을 바꾸는 명령입니다.

해당 백업을 사용하여 복원할 때 장치의 잠금 또는 이름 바꾸기는 복원 작업에 영향을 주지 않습니다.

- 데이터베이스 쿼리 실행 시간이 시간 초과 값을 초과하여 백업 작업이 실패하면 를 실행하여 Oracle_SQL_QUERY_TIMEOUT 및 ORACLE_PLUGIN_SQL_QUERY_TIMEOUT 매개 변수의 값을 변경해야 합니다 `Set-SmConfigSettings` cmdlet:

매개 변수 값을 수정한 후 다음 명령을 실행하여 SnapCenter SPL(Plug-in Loader) 서비스를 다시 시작합니다

`/opt/NetApp/snapcenter/spl/bin/spl restart`

- 파일을 액세스할 수 없고 확인 프로세스 중에 마운트 지점을 사용할 수 없는 경우 오류 코드 DBV-00100 지정된 파일로 인해 작업이 실패할 수 있습니다. sco.properties 에서 verification_delay 및 verification_retry_count 매개 변수의 값을 수정해야 합니다.

  매개 변수 값을 수정한 후 다음 명령을 실행하여 SnapCenter SPL(Plug-in Loader) 서비스를 다시 시작합니다 `/opt/NetApp/snapcenter/spl/bin/spl restart`

- MetroCluster 구성에서 SnapCenter는 페일오버 후 보호 관계를 감지하지 못할 수 있습니다.
- VMDK에서 애플리케이션 데이터를 백업하고 VMware vSphere용 SnapCenter 플러그인의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다.

  Java 힙 크기를 늘리려면 스크립트 파일 _/opt/netapp/init_scripts/scvservice_를 찾습니다. 이 스크립트에서 은 입니다 `do_start method` Command SnapCenter VMware 플러그인 서비스를 시작합니다. 다음 명령을 업데이트합니다. `Java -jar -Xmx8192M -Xms4096M`.

자세한 내용을 확인하십시오

- "MetroCluster 페일오버 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다"
- "SnapCenter 작업을 수행하기 위해 Oracle RAC One Node 데이터베이스를 건너뜁니다"
- "Oracle 12c ASM 데이터베이스의 상태를 변경하지 못했습니다"
- "AIX 시스템의 백업, 복원 및 클론 작업에 대한 사용자 정의 가능한 매개 변수" (로그인 필요)

Oracle 데이터베이스 리소스 그룹을 백업합니다

리소스 그룹은 호스트 또는 클러스터의 리소스 모음입니다. 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다.

리소스 페이지에서 필요 시 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 연결되어 있고 스케줄이 구성되어 있는 경우 스케줄에 따라 백업이 생성됩니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 선택하고 목록에서 해당 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 리소스 그룹 * 을 선택합니다.
3. 검색 상자에 리소스 그룹 이름을 입력하거나 를 클릭합니다 을 클릭하고 태그를 선택합니다.

   을 클릭합니다 를 눌러 필터 창을 닫습니다.

4. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택합니다.

   두 개의 데이터베이스를 사용하는 통합 리소스 그룹이 있고 그 중 하나에 타사 스토리지에 대한 데이터가 있는 경우, 다른 데이터베이스가 NetApp 스토리지에 있더라도 백업 작업이 중단됩니다.

5. 백업 페이지에서 다음 단계를 수행하십시오.
   a. 리소스 그룹에 연결된 정책이 여러 개인 경우 * 정책 * 드롭다운 목록에서 사용할 백업 정책을 선택합니다.

      필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시

백업이 유지됩니다.

b. 백업 * 을 선택합니다.

6. 모니터 > 작업 * 을 선택하여 진행 상황을 모니터링합니다.

작업을 마친 후

- AIX 설정에서 를 사용할 수 있습니다 `lkdev` 명령을 사용하여 및 를 잠급니다 `rendev` 백업한 데이터베이스가 있는 디스크의 이름을 바꾸는 명령입니다.

  해당 백업을 사용하여 복원할 때 장치의 잠금 또는 이름 바꾸기는 복원 작업에 영향을 주지 않습니다.

- 데이터베이스 쿼리 실행 시간이 시간 초과 값을 초과하여 백업 작업이 실패하면 를 실행하여 Oracle_SQL_QUERY_TIMEOUT 및 ORACLE_PLUGIN_SQL_QUERY_TIMEOUT 매개 변수의 값을 변경해야 합니다 `Set-SmConfigSettings` cmdlet:

  매개 변수 값을 수정한 후 다음 명령을 실행하여 SnapCenter SPL(Plug-in Loader) 서비스를 다시 시작합니다 `/opt/NetApp/snapcenter/spl/bin/spl restart`

- 파일을 액세스할 수 없고 확인 프로세스 중에 마운트 지점을 사용할 수 없는 경우 오류 코드 DBV-00100 지정된 파일로 인해 작업이 실패할 수 있습니다. sco.properties 에서 verification_delay_와 verification_retry_count 매개 변수의 값을 수정해야 합니다.

  매개 변수 값을 수정한 후 다음 명령을 실행하여 SnapCenter SPL(Plug-in Loader) 서비스를 다시 시작합니다 `/opt/NetApp/snapcenter/spl/bin/spl restart`

Oracle 데이터베이스 백업을 모니터링합니다

백업 작업 및 데이터 보호 작업의 진행률을 모니터링하는 방법에 대해 알아봅니다.

Oracle 데이터베이스 백업 작업을 모니터링합니다

SnapCenterJobs 페이지를 사용하여 여러 백업 작업의 진행률을 모니터링할 수 있습니다. 진행 상황을 확인하여 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

다음 아이콘이 작업 페이지에 나타나고 작업의 해당 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨

단계

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.

2. 모니터 페이지에서 * 작업 * 을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행하십시오.
   a. 을 클릭합니다 백업 작업만 나열되도록 목록을 필터링합니다.
   b. 시작 및 종료 날짜를 지정합니다.
   c. Type * 드롭다운 목록에서 * Backup * 을 선택합니다.
   d. Status * (상태 *) 드롭다운에서 백업 상태를 선택합니다.
   e. 작업이 성공적으로 완료되었는지 보려면 * Apply * 를 클릭합니다.
4. 백업 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.

   백업 작업 상태가 표시됩니다 작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 기호로 표시되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 * 로그 보기 * 를 클릭합니다.

   로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

Activity 창에서 데이터 보호 작업을 모니터링합니다

작업 창에는 가장 최근에 수행한 작업 5개가 표시됩니다. 작업 창은 작업이 시작된 시점과 작업의 상태도 표시합니다.

작업 창에는 백업, 복원, 클론 및 예약된 백업 작업에 대한 정보가 표시됩니다. SQL Server용 플러그인 또는 Exchange Server용 플러그인을 사용하는 경우 작업 창에 다시 시드된 작업에 대한 정보도 표시됩니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 을 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다.

   작업 중 하나를 클릭하면 작업 세부 정보가 * 작업 세부 정보 * 페이지에 나열됩니다.

기타 백업 작업

UNIX 명령을 사용하여 **Oracle** 데이터베이스를 백업합니다

백업 워크플로우에는 계획, 백업용 리소스 식별, 백업 정책 생성, 리소스 그룹 생성 및 정책 연결, 백업 생성 및 작업 모니터링이 포함됩니다.

- 필요한 것 *
- 스토리지 시스템 접속을 추가하고 *Add-SmStorageConnection* 및 *Add-SmCredential* 명령을 사용하여 자격 증명을 생성해야 합니다.
- *Open-SmConnection* 명령을 사용하여 SnapCenter 서버와의 연결 세션을 설정해야 합니다.

  SnapCenter 계정 로그인 세션은 하나만 가질 수 있으며 사용자 홈 디렉토리에 토큰이 저장됩니다.

연결 세션은 24시간 동안만 유효합니다. 그러나 토큰 네버엑셀 옵션을 사용하여 토큰을 만들어 만료되지 않고 세션이 항상 유효하게 만들 수 있습니다.

- 이 작업에 대한 정보 *

다음 명령을 실행하여 SnapCenter 서버와의 연결을 설정하고, Oracle 데이터베이스 인스턴스를 검색하고, 정책 및 리소스 그룹을 추가하고, 백업을 백업 및 확인해야 합니다.

명령에 사용할 수 있는 매개 변수 및 해당 설명에 대한 정보는 get-Help_command_name_을 실행하여 얻을 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 명령 참조 가이드".

- 단계 *

1. 지정된 사용자에 대해 SnapCenter 서버와 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. _ 구성 - SmOracleDatabase _
4. 백업 정책 생성:_Add-SmPolicy _
5. 보조(SnapVault 또는 SnapMirror) 스토리지 위치에 대한 정보를 검색합니다. _get-SmSecondaryDetails _

   이 명령은 지정된 리소스의 운영 스토리지 및 보조 스토리지 매핑 세부 정보를 검색합니다. 매핑 세부 정보를 사용하여 백업 리소스 그룹을 생성하는 동안 보조 검증 설정을 구성할 수 있습니다.

6. SnapCenter:_Add-SmResourceGroup_에 리소스 그룹을 추가합니다
7. 백업을 생성합니다:_New-SmBackup_

   WaitForCompletion 옵션을 사용하여 작업을 폴링할 수 있습니다. 이 옵션을 지정하면 명령은 백업 작업이 완료될 때까지 서버를 계속 폴링합니다.

8. SnapCenter:_Get-SmLogs_에서 로그를 검색합니다

Oracle 데이터베이스의 백업 작업을 취소합니다

실행 중이거나 대기 중이거나 응답하지 않는 백업 작업을 취소할 수 있습니다.

백업 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

- 이 작업에 대한 정보 *

백업 작업을 취소하면 생성된 백업이 SnapCenter 서버에 등록되지 않은 경우 SnapCenter 서버가 작업을 중지하고 스토리지에서 모든 스냅샷 복사본을 제거합니다. 백업이 이미 SnapCenter 서버에 등록되어 있는 경우 취소가 트리거된 후에도 이미 생성된 스냅샷 복사본이 롤백되지 않습니다.

- 대기열에 있거나 실행 중인 로그 또는 전체 백업 작업만 취소할 수 있습니다.
- 확인이 시작된 후에는 작업을 취소할 수 없습니다.

  확인 전에 작업을 취소하면 작업이 취소되고 확인 작업이 수행되지 않습니다.

- 카탈로그 작업이 시작된 후에는 백업 작업을 취소할 수 없습니다.

- 모니터 페이지 또는 작업 창에서 백업 작업을 취소할 수 있습니다.
- SnapCenter GUI를 사용하는 것 외에도 CLI 명령을 사용하여 작업을 취소할 수 있습니다.
- 취소할 수 없는 작업에 대해 * 작업 취소 * 버튼이 비활성화됩니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 사용자\그룹 페이지에서 다른 구성원 개체를 보고 작동할 수 있음 * 을 선택한 경우 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 백업 작업을 취소할 수 있습니다.
- 단계 *

다음 작업 중 하나를 수행합니다.

시작...	조치
모니터 페이지	1. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 클릭합니다. 2. 작업을 선택하고 * 작업 취소 * 를 클릭합니다.
작업 창	1. 백업 작업을 시작한 후 를 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다. 2. 작업을 선택합니다. 3. 작업 세부 정보 페이지에서 * 작업 취소 * 를 클릭합니다.

- 결과 *

작업이 취소되고 리소스가 원래 상태로 돌아갑니다.

취소한 작업이 취소 또는 실행 상태에서 응답하지 않는 경우 Cancel-SmJob-jobid <int>-Force 를 실행하여 백업 작업을 강제로 중지해야 합니다.

토폴로지 페이지에서 **Oracle** 데이터베이스 백업 및 클론 보기

리소스를 백업 또는 복제할 때 운영 스토리지와 보조 스토리지의 모든 백업 및 클론을 그래픽으로 표시하는 것이 유용할 수 있습니다.

- 이 작업에 대한 정보 *

토폴로지 페이지에서 선택한 리소스 또는 리소스 그룹에 사용할 수 있는 모든 백업 및 클론을 볼 수 있습니다. 이러한 백업 및 클론의 세부 정보를 확인한 다음 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

복제본 관리 보기에서 다음 아이콘을 검토하여 운영 스토리지 또는 보조 스토리지(미러 복사본 또는 볼트 복제본)에서 백업과 클론을 사용할 수 있는지 확인할 수 있습니다.

- 기본 스토리지에서 사용할 수 있는 백업 및 클론 수를 표시합니다.
- SnapMirror 기술을 사용하여 보조 스토리지에 미러링된 백업 및 클론 수를 표시합니다.

-  SnapVault 기술을 사용하여 보조 스토리지에 복제된 백업 및 클론 수를 표시합니다.

  표시된 백업 수에는 보조 스토리지에서 삭제된 백업이 포함됩니다. 예를 들어 정책을 사용하여 6개의 백업을 생성하여 4개의 백업만 보존한 경우 표시되는 백업 수는 6입니다.

   미러 볼트 유형 볼륨에 있는 버전에 따라 유연한 미러 백업의 클론은 토폴로지 뷰에 표시되지만 토폴로지 뷰에 있는 미러 백업 횟수에는 버전에 따라 유연하게 백업할 수 있는 백업이 포함되지 않습니다.

- 단계 *

  1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
  2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
  3. 자원 세부 정보 보기 또는 자원 그룹 세부 정보 보기에서 자원을 선택합니다.

     리소스가 보호되는 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

  4. Summary 카드를 검토하여 운영 스토리지와 보조 스토리지에서 사용할 수 있는 백업 및 클론 수를 요약합니다.

     요약 카드 섹션에는 총 백업 및 클론 수와 총 로그 백업 수가 표시됩니다.

     Refresh * 버튼을 클릭하면 스토리지 쿼리가 시작되어 정확한 카운트를 표시합니다.

  5. 복사본 관리 보기에서 기본 또는 보조 스토리지에서 * 백업 * 또는 * 클론 * 을 클릭하여 백업 또는 클론의 세부 정보를 확인합니다.

     백업 및 클론의 세부 정보가 표 형식으로 표시됩니다.

  6. 테이블에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복구, 클론, 마운트, 마운트 해제, 이름 바꾸기, 카탈로그, 카탈로그 해제 및 삭제 작업.

      보조 스토리지에 있는 백업의 이름을 바꾸거나 백업을 삭제할 수 없습니다.

     - 로그 백업을 선택한 경우 이름 바꾸기, 마운트, 마운트 해제, 카탈로그, 카탈로그 해제 작업만 수행할 수 있습니다. 삭제 작업을 수행할 수 있습니다.
     - Oracle RMAN(Recovery Manager)을 사용하여 백업 카탈로그를 작성한 경우에는 이러한 카탈로그 작성된 백업의 이름을 바꿀 수 없습니다.

  7. 클론을 삭제하려면 표에서 클론을 선택한 다음 을 클릭합니다  .

Snap미러orStatusUpdateWaitTime 에 할당된 값이 적으면 데이터 및 로그 볼륨이 성공적으로 보호되더라도 미러 및 볼트 백업 복사본이 토폴로지 페이지에 나열되지 않습니다. _Set-SmConfigSettings_PowerShell cmdlet을 사용하여 Snap미러또는 StatusUpdateWaitTime에 할당된 값을 늘려야 합니다.

명령에 사용할 수 있는 매개 변수 및 해당 설명에 대한 정보는 get-Help_command_name_을 실행하여 얻을 수 있습니다.

또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 명령 참조 가이드" 또는 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

데이터베이스 백업을 마운트 및 마운트 해제합니다

백업의 파일에 액세스하려는 경우 하나 또는 여러 개의 데이터와 로그 전용 백업을 마운트할 수 있습니다. 백업을 생성된 동일한 호스트에 마운트하거나 Oracle 및 호스트 구성이 동일한 원격 호스트에 마운트할 수 있습니다. 백업을 수동으로 마운트한 경우 작업을 완료한 후 백업을 수동으로 마운트 해제해야 합니다. 특정 인스턴스에서 데이터베이스 백업을 호스트 중 하나에 마운트할 수 있습니다. 작업을 수행하는 동안 단일 백업만 마운트할 수 있습니다.

Flex ASM 설정에서 카디널리티가 RAC 클러스터의 노드 수보다 적은 경우 Leaf 노드에서 마운트 작업을 수행할 수 없습니다.

데이터베이스 백업을 마운트합니다

백업의 파일에 액세스하려는 경우 데이터베이스 백업을 수동으로 마운트해야 합니다.

- 필요한 것 *
- NFS 환경에 ASM(Automatic Storage Management) 데이터베이스 인스턴스가 있고 ASM 백업을 마운트하려는 경우 ASM 디스크 경로 */var/opt/snapcenter/sSCO/backup* * /_ * _ * /___을(를) ASM_diskstring 매개 변수에 정의된 기존 경로에 추가해야 합니다.
- NFS 환경에 ASM 데이터베이스 인스턴스가 있고 복구 작업의 일부로 ASM 로그 백업을 마운트하려면 ASM 디스크 경로 _ /var/opt/snapcenter/SCU/clones/_ */ * _를 ASM_diskstring 매개 변수에 정의된 기존 경로에 추가해야 합니다.
- ASM_diskstring 매개 변수에서 ASMFD 또는 configure_ORCL: *_을 사용하는 경우 ASMlib를 사용하는 경우 _AFD: *_를 구성해야 합니다.

ASM_diskstring 매개 변수를 편집하는 방법에 대한 자세한 내용은 을 참조하십시오 "ASM_diskstring에 디스크 경로를 추가하는 방법".

- 백업을 마운트하는 동안 소스 데이터베이스 호스트의 자격 증명과 ASM 포트가 다른 경우 ASM 자격 증명 및 ASM 포트를 구성해야 합니다.
- 대체 호스트에 마운트하려면 대체 호스트가 다음 요구 사항을 충족하는지 확인해야 합니다.
  - 원래 호스트의 UID 및 GID와 동일합니다
  - 원래 호스트의 Oracle 버전과 동일합니다
  - 원래 호스트의 OS 배포 및 버전과 동일합니다
  - NVMe의 경우 NVMe util을 설치해야 합니다
- 혼합 프로토콜 iSCSI 및 FC로 구성된 iGroup을 사용하여 LUN이 AIX 호스트에 매핑되지 않았는지 확인해야 합니다. 자세한 내용은 을 참조하십시오 "LUN에 대한 디바이스를 검색할 수 없어 작업이 실패합니다".
- 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. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 데이터베이스를 선택합니다.

데이터베이스 토폴로지 페이지가 표시됩니다.

4. Manage Copies 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템에서 * Backups * 를 선택합니다.
5. 테이블에서 백업을 선택한 다음 을 클릭합니다  .
6. Mount Backups 페이지의 * Choose the host to mount the backup * 드롭다운 목록에서 백업을 마운트할 호스트를 선택합니다.

   마운트 경로 _/var/opt/snapcenter/sSCO/backup_mount/backup_name/database_name_이 표시됩니다.

ASM 데이터베이스의 백업을 마운트하는 경우 마운트 경로 + diskgroupname_SID_backupid가 표시됩니다.

1. Mount * 를 클릭합니다.

- 완료 후 *
- 다음 명령을 실행하여 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-Smbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
```

- 백업 ID를 검색하려면 다음 명령을 실행합니다.

```
./sccli Get-Smbackup-BackupNamebackup_name
```

명령에 사용할 수 있는 매개 변수 및 해당 설명에 대한 정보는 get-Help_command_name_을 실행하여 얻을 수 있습니다.
또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 명령 참조 가이드".

데이터베이스 백업을 마운트 해제합니다

백업의 파일에 더 이상 액세스하지 않으려는 경우 마운트된 데이터베이스 백업을 수동으로 마운트 해제할 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. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 데이터베이스를 선택합니다.

   데이터베이스 토폴로지 페이지가 표시됩니다.

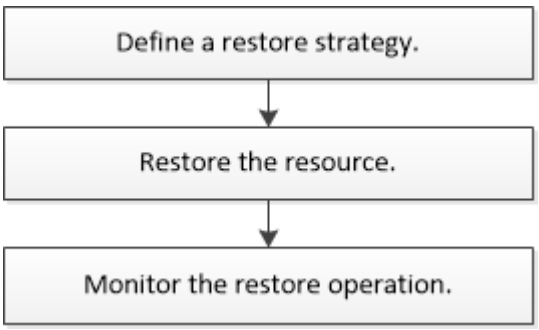
4. 마운트된 백업을 선택한 다음 을 클릭합니다  .
5. 확인 * 을 클릭합니다.

Oracle 데이터베이스 복원 및 복구

워크플로를 복원합니다

복원 워크플로에는 계획, 복원 작업 수행 및 작업 모니터링이 포함됩니다.

다음 워크플로에서는 복원 작업을 수행해야 하는 순서를 보여 줍니다.



Oracle 데이터베이스에 대한 복구 및 복구 전략 정의

복구 및 복구 작업을 성공적으로 수행하려면 데이터베이스를 복원 및 복구하기 전에 전략을 정의해야 합니다.

복구 및 복구 작업에 지원되는 백업 유형입니다

SnapCenter는 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 SnapCenter는 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 데이터베이스 복구는 수행할 수 없습니다.

- 온라인 데이터 백업, 온라인 전체 백업, 오프라인 마운트 백업 및 RAC(Real Application Clusters) 구성의 오프라인 종료 백업
- 온라인 데이터 백업, 온라인 전체 백업, 오프라인 마운트 백업 및 ASM(Automatic Storage Management) 구성에서 오프라인 종료 백업

Oracle 데이터베이스에 지원되는 복원 방법의 유형입니다

SnapCenter는 Oracle 데이터베이스에 대한 연결 및 복사 또는 이동 없는 복원을 지원합니다. 복구 작업 중에 SnapCenter는 데이터 손실 없이 복구에 사용할 파일 시스템에 적합한 복구 방법을 결정합니다.

SnapCenter는 볼륨 기반 SnapRestore를 지원하지 않습니다.

연결 및 복사 복원

데이터베이스 레이아웃이 백업과 다르거나 백업 생성 후 새 파일이 있는 경우 연결 및 복사 복원이 수행됩니다. 연결 및 복사 복원 방법에서는 다음 작업이 수행됩니다.

- 단계 *
  1. 볼륨은 스냅샷 복사본에서 클론 복제되며, 파일 시스템 스택은 클론 복제된 LUN 또는 볼륨을 사용하여 호스트에 구축됩니다.
  2. 파일은 클론 생성된 파일 시스템에서 원래 파일 시스템으로 복제됩니다.
  3. 그런 다음 클론된 파일 시스템이 호스트에서 마운트 해제되고 클론된 볼륨이 ONTAP에서 삭제됩니다.

Flex ASM 설정(카디널리티가 RAC 클러스터의 노드 수보다 적은 경우) 또는 VMDK 또는 RDM의 ASM RAC 데이터베이스의 경우 연결 및 복제 복원 방법만 지원됩니다.

데이터 이동 없이 강제로 복원한 경우에도 SnapCenter는 다음과 같은 경우에 연결 및 복사 복원을 수행합니다.

- 보조 스토리지 시스템에서 복원하고 Data ONTAP이 8.3 이전 버전인 경우
- 데이터베이스 인스턴스가 구성되지 않은 Oracle RAC 설정의 노드에 있는 ASM 디스크 그룹의 복원
- Oracle RAC 설정에서 ASM 인스턴스 또는 클러스터 인스턴스가 실행되고 있지 않거나 피어 노드가 다운된 경우 피어 노드에서
- 제어 파일만 복원합니다
- ASM 디스크 그룹에 상주하는 테이블스페이스의 하위 집합을 복원합니다
- 디스크 그룹은 데이터 파일, SP 파일 및 암호 파일 간에 공유됩니다
- SnapCenter SPL(Plug-in Loader) 서비스가 RAC 환경의 원격 노드에서 설치되지 않았거나 실행되지 않습니다
- Oracle RAC에 새 노드가 추가되고 SnapCenter 서버가 새로 추가된 노드를 인식하지 못합니다

데이터 이동 없이 복원

데이터베이스 레이아웃이 백업과 유사하고 스토리지 및 데이터베이스 스택에서 구성 변경을 수행하지 않은 경우, 데이터 이동 없이 복원이 수행되며, 이 경우 ONTAP에서 파일 또는 LUN 복원이 수행됩니다. SnapCenter는 현재 위치 복원 방법의 일부로 SFSR(Single File SnapRestore)만 지원합니다.

Data ONTAP 8.3 이상은 보조 위치에서 데이터 이동 없이 복원을 지원합니다.

데이터베이스에서 데이터 이동 없이 복원을 수행하려면 ASM 디스크 그룹에 데이터 파일만 있어야 합니다. ASM 디스크 그룹 또는 데이터베이스의 물리적 구조를 변경한 후에는 백업을 생성해야 합니다. 데이터 이동 없이 복원을 수행한 후 디스크 그룹은 백업 시와 동일한 수의 데이터 파일을 포함합니다.

디스크 그룹 또는 마운트 지점이 다음 기준과 일치할 경우 현재 위치 복원이 자동으로 적용됩니다.

- 백업 후 새 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 그룹(LVM 디스크 그룹 구조 변경 확인)에 LUN을 추가, 삭제 또는 재생성할 수 없음

GUI, SnapCenter CLI 또는 PowerShell cmdlet을 사용하여 데이터 이동 없이 강제로 복원할 수 있으며 외부 파일 검사 및 LVM 디스크 그룹 구조 변경 검사를 재정의할 수 있습니다.

ASM RAC에서 데이터 이동 없이 복원 수행

SnapCenter에서 복구를 수행하는 노드를 기본 노드라고 하며 ASM 디스크 그룹이 상주하는 RAC의 다른 모든 노드를 피어 노드라고 합니다. SnapCenter는 ASM 디스크 그룹의 상태를 변경하여 스토리지 복구 작업을 수행하기 전에 ASM 디스크 그룹이 마운트 상태에 있는 모든 노드에서 마운트 해제합니다. 스토리지 복원이 완료된 후 SnapCenter는 복구 작업 전의 ASM 디스크 그룹 상태를 변경합니다.

SAN 환경에서는 SnapCenter가 모든 피어 노드에서 디바이스를 제거하고 스토리지 복구 작업 전에 LUN 매핑 해제 작업을 수행합니다. 스토리지 복구 작업 후 SnapCenter는 LUN 맵 작업을 수행하고 모든 피어 노드에 디바이스를 구성합니다. SAN 환경에서 Oracle RAC ASM 레이아웃이 LUN에 있는 경우 SnapCenter를 복구하는 동안 ASM 디스크 그룹이 상주하는 RAC 클러스터의 모든 노드에서 LUN 매핑 해제, LUN 복원 및 LUN 맵 작업을 수행합니다. LUN에 RAC 노드의 모든 이니시에이터가 사용되지 않은 경우에도 복원하기 전에 SnapCenter을 복원하면 모든 RAC 노드의 모든 이니시에이터가 포함된 새 iGroup이 생성됩니다.

- 피어 노드에서 PreRestore 작업 중에 오류가 발생한 경우 SnapCenter는 PreRestore 작업이 성공한 피어 노드에서 복원을 수행하기 전에 ASM 디스크 그룹 상태를 그대로 자동으로 롤백합니다. 롤백은 작업이 실패한 기본 노드 및 피어 노드에 대해 지원되지 않습니다. 다른 복구를 시도하기 전에 피어 노드의 문제를 수동으로 해결하고 기본 노드의 ASM 디스크 그룹을 마운트 상태로 되돌리시어야 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 되돌리시어야 합니다.
- 피어 노드에서 PostRestore 작업 중에 오류가 발생하면 SnapCenter는 다른 피어 노드에서 복구 작업을 계속합니다. 피어 노드에서 사후 복원 문제를 수동으로 해결해야 합니다.

Oracle 데이터베이스에 지원되는 복원 작업의 유형입니다

SnapCenter를 사용하면 Oracle 데이터베이스에 대해 다양한 유형의 복원 작업을 수행할 수 있습니다.

데이터베이스를 복구하기 전에 실제 데이터베이스 파일과 비교하여 누락된 파일이 있는지 여부를 확인하기 위해 백업을 검증합니다.

전체 복원

- 데이터 파일만 복구합니다
- 제어 파일만 복원합니다
- 데이터 파일 및 제어 파일을 복원합니다
- Data Guard 대기 및 Active Data Guard 대기 데이터베이스에서 데이터 파일, 제어 파일 및 재실행 로그 파일을 복구합니다

부분 복원

- 선택한 테이블스페이서만 복구합니다

- 선택한 플러깅 지원 데이터베이스(PDB)만 복원합니다.
- PDB에서 선택한 테이블스페이서만 복구합니다

Oracle 데이터베이스에 지원되는 복구 작업의 유형입니다

SnapCenter를 사용하면 Oracle 데이터베이스에 대해 다양한 유형의 복구 작업을 수행할 수 있습니다.

- 마지막 트랜잭션까지의 데이터베이스(모든 로그)
- 데이터베이스를 특정 SCN(시스템 변경 번호)까지
- 데이터베이스를 특정 날짜 및 시간까지 설정합니다

  데이터베이스 호스트의 표준 시간대를 기준으로 복구 날짜와 시간을 지정해야 합니다.

  또한 SnapCenter는 Oracle 데이터베이스에 대해 복구 안 함 옵션을 제공합니다.

> ⓘ 데이터베이스 역할을 대기 상태로 사용하여 만든 백업을 사용하여 복원한 경우 Oracle 데이터베이스용 플러그인은 복구를 지원하지 않습니다. 물리적 대기 데이터베이스에 대해 항상 수동 복구를 수행해야 합니다.

Oracle 데이터베이스 복원 및 복구와 관련된 제한 사항

복구 및 복구 작업을 수행하기 전에 제한 사항을 숙지해야 합니다.

11.2.0.4 ~ 12.1.0.1의 Oracle 버전을 사용하는 경우 _renamedg_command를 실행하면 복원 작업이 멈춤 상태가 됩니다. Oracle 패치 19544733을 적용하여 이 문제를 해결할 수 있습니다.

다음 복원 및 복구 작업은 지원되지 않습니다.

- 루트 컨테이너 데이터베이스(CDB)의 테이블스페이스 복구 및 복구
- PDB와 연결된 임시 테이블스페이스 및 임시 테이블스페이스의 복구
- 여러 PDB에서 테이블스페이스를 동시에 복원 및 복구합니다
- 로그 백업 복구
- 백업을 다른 위치로 복구합니다
- Data Guard 대기 또는 Active Data Guard 대기 데이터베이스 이외의 모든 구성에서 REDO 로그 파일 복원
- SPFILE 및 암호 파일 복원
- 동일한 호스트에서 기존 데이터베이스 이름을 사용하여 다시 생성된 데이터베이스에 대해 복구 작업을 수행하고, SnapCenter에서 관리하며, 유효한 백업을 가지고 있는 경우, 복구 작업은 DBID가 서로 다르지만 새로 생성된 데이터베이스 파일을 덮어씁니다.

  다음 작업 중 하나를 수행하면 이 문제를 방지할 수 있습니다.

  - 데이터베이스를 다시 만든 후 SnapCenter 리소스를 검색합니다
  - 다시 생성된 데이터베이스의 백업을 생성합니다

테이블스페이스의 시점 복구와 관련된 제한 사항

- 시스템, SYSAUX 및 실행 취소 테이블스페이스의 PITR(시점 복구)은 지원되지 않습니다
- 테이블스페이스의 PITR은 다른 유형의 복원과 함께 수행할 수 없습니다
- 테이블스페이스의 이름이 바뀌었고 이름을 바꾸기 전에 테이블스페이스를 특정 지점으로 복구하려면 테이블스페이스의 이전 이름을 지정해야 합니다
- 한 테이블스페이스에 있는 테이블에 대한 제약 조건이 다른 테이블스페이스에 포함되어 있는 경우 두 테이블스페이스를 모두 복구해야 합니다
- 테이블과 해당 인덱스가 다른 테이블스페이스에 저장된 경우 PITR을 수행하기 전에 인덱스를 삭제해야 합니다
- PITR은 현재 기본 테이블스페이스를 복구하는 데 사용할 수 없습니다
- PITR은 다음 객체를 포함하는 테이블스페이스를 복구하는 데 사용할 수 없습니다.
    - 모든 내부 또는 포함된 개체가 복구 집합에 없는 경우 기본 개체(예: 구체화된 뷰) 또는 포함된 개체(예: 분할된 테이블)가 있는 개체입니다

      또한 분할된 테이블의 파티션이 서로 다른 테이블스페이스에 저장된 경우 PITR을 수행하기 전에 테이블을 놓거나 PITR을 수행하기 전에 모든 파티션을 동일한 테이블스페이스로 이동해야 합니다.

    - 세그먼트 실행 취소 또는 롤백
    - 여러 수신인이 있는 Oracle 8 호환 고급 대기열
    - SYS 사용자가 소유하는 객체입니다

      이러한 유형의 오브젝트의 예로는 PL/SQL, Java 클래스, 프로그램 호출, 보기, 동의어, 사용자, 권한, 차원, 디렉터리 및 시퀀스

Oracle 데이터베이스 복원을 위한 소스 및 대상

운영 스토리지 또는 보조 스토리지의 백업 복사본에서 Oracle 데이터베이스를 복원할 수 있습니다. 데이터베이스를 동일한 데이터베이스 인스턴스의 동일한 위치로만 복원할 수 있습니다. 그러나 RAC(Real Application Cluster) 설정에서는 데이터베이스를 다른 노드로 복원할 수 있습니다.

복구 작업을 위한 소스

운영 스토리지 또는 보조 스토리지의 백업에서 데이터베이스를 복원할 수 있습니다. 여러 미러 구성의 보조 스토리지에 있는 백업에서 복구하려면 보조 스토리지 미러를 소스로 선택할 수 있습니다.

복원 작업의 대상

데이터베이스를 동일한 데이터베이스 인스턴스의 동일한 위치로만 복원할 수 있습니다.

RAC 설정에서는 클러스터의 모든 노드에서 RAC 데이터베이스를 복원할 수 있습니다.

특정 처방과 **PS**를 복원하기 위한 사전 정의된 환경 변수입니다

SnapCenter를 사용하면 데이터베이스를 복원하는 동안 처방과 PS를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다.

- 데이터베이스 복원을 위해 지원되는 미리 정의된 환경 변수 *

- * SC_JOB_ID * 는 작업의 작업 ID를 지정합니다.

  예: 257

- * SC_ORACLE_SID * 는 데이터베이스의 시스템 식별자를 지정합니다.

  작업에 여러 데이터베이스가 포함된 경우 파이프로 구분된 데이터베이스 이름이 포함됩니다.

  예: NFSB31

- * sc_host * 는 데이터베이스의 호스트 이름을 지정합니다.

  이 매개 변수는 애플리케이션 볼륨에 대해 채워집니다.

  예: scsmohost2.gdl.englabe.netapp.com

- * SC_OS_USER * 는 데이터베이스의 운영 체제 소유자를 지정합니다.

  예: Oracle

- * SC_OS_GROUP * 은 데이터베이스의 운영 체제 그룹을 지정합니다.

  예: oinstall

- * SC_BACKUP_NAME * 은 백업 이름을 지정합니다.

  이 매개 변수는 애플리케이션 볼륨에 대해 채워집니다.

  예:

  - 데이터베이스가 ARCHIVELOG 모드에서 실행되고 있지 않은 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 실행 중인 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 매개 변수는 애플리케이션 볼륨에 대해 채워집니다.

  예:

  - 데이터베이스가 ARCHIVELOG 모드에서 실행되지 않는 경우: data@203|log@205
  - 데이터베이스가 ARCHIVELOG 모드에서 실행 중인 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 복구할 파일과 복구 범위를 지정합니다.

  예:
  RESTORESCOPE:usingBackupControlfile=false|RECOVERYSCOPE:allLogs=true,nLogs=false,untiltime=false,untilscn=false입니다.

구분 기호에 대한 자세한 내용은 을 참조하십시오 "지원되는 구분 기호".

Oracle 데이터베이스 복구 요구 사항

Oracle 데이터베이스를 복구하기 전에 사전 요구 사항이 완료되었는지 확인해야 합니다.

- 복원 및 복구 전략을 정의해야 합니다.
- 스냅샷 복사본을 미러 또는 볼트로 복제할 경우 SnapCenter 관리자가 소스 볼륨과 타겟 볼륨 모두에 SVM(스토리지 가상 머신)을 할당해야 합니다.
- 아카이브 로그가 백업의 일부로 정리된 경우 필요한 아카이브 로그 백업을 수동으로 마운트해야 합니다.
- VMDK(Virtual Machine Disk)에 상주하는 Oracle 데이터베이스를 복원하려면 게스트 시스템에 복제된 VMDK를 할당하는 데 필요한 가용 슬롯 수가 있는지 확인해야 합니다.
- 해당 데이터베이스에 대해 보조 보호가 설정된 경우 데이터베이스에 속한 모든 데이터 볼륨과 아카이브 로그 볼륨이 보호되는지 확인해야 합니다.
- 제어 파일 또는 전체 데이터베이스 복구를 수행하려면 RAC One Node 데이터베이스가 "nomount" 상태여야 합니다.
- NFS 환경에 ASM 데이터베이스 인스턴스가 있는 경우 ASM 로그 백업을 복구 작업의 일부로 성공적으로 마운트하기 위해 ASM 디스크 경로 _/var/opt/snapcenter/SCU/clones/ */ *_를 ASM_diskstring 매개 변수에 정의된 기존 경로에 추가해야 합니다.
- ASM_diskstring 매개 변수에서 ASMFD 또는 configure_ORCL: *_을 사용하는 경우 ASMlib를 사용하는 경우 _AFD: *_를 구성해야 합니다.

  ASM_diskstring 매개 변수를 편집하는 방법에 대한 자세한 내용은 을 참조하십시오 "ASM_diskstring에 디스크 경로를 추가하는 방법"

- 비 ASM 데이터베이스의 경우 _$oracle_home/network/admin_에서 사용할 수 있는 * listener.ora * 파일의 정적 수신기를 구성하고, Oracle 데이터베이스의 경우 OS 인증을 사용하지 않고 Oracle 데이터베이스 인증을 활성화한 경우 ASM 데이터베이스의 경우 _$grid_home/network/admin_에서 해당 데이터베이스의 데이터 파일 및 제어 파일을 복원해야 합니다.
- 데이터베이스 크기가 테라바이트(TB)인 경우 Set-SmConfigSettings 명령을 실행하여 ScCORestoreTimeout 매개 변수의 값을 늘려야 합니다.
- vCenter에 필요한 모든 라이센스가 설치되어 있고 최신 상태인지 확인해야 합니다.

  라이센스가 설치되지 않았거나 최신 상태인 경우 경고 메시지가 표시됩니다. 경고를 무시하고 계속하면 RDM에서 복구가 실패합니다.

- 혼합 프로토콜 iSCSI 및 FC로 구성된 iGroup을 사용하여 LUN이 AIX 호스트에 매핑되지 않았는지 확인해야 합니다. 자세한 내용은 을 참조하십시오 "LUN에 대한 디바이스를 검색할 수 없어 작업이 실패합니다".

Oracle 데이터베이스 복원 및 복구

데이터가 손실된 경우 SnapCenter를 사용하여 하나 이상의 백업에서 액티브 파일 시스템으로 데이터를 복구한 다음 데이터베이스를 복구할 수 있습니다.

- 시작하기 전에 *

플러그인을 비루트 사용자로 설치한 경우, prescpt 및 PostScript 디렉토리에 실행 권한을 수동으로 할당해야 합니다.

- 이 작업에 대한 정보 *

복구는 구성된 아카이브 로그 위치에서 사용할 수 있는 아카이브 로그를 사용하여 수행됩니다. 데이터베이스가 ARCHIVELOG 모드에서 실행 중인 경우 Oracle 데이터베이스는 채워진 REDO 로그 파일 그룹을 하나 이상의 오프라인 대상(집합적으로 아카이빙된 REDO 로그라고 함)에 저장합니다. SnapCenter는 지정된 SCN, 선택한 날짜 및 시간 또는 모든 로그 옵션을 기반으로 최적의 로그 백업 수를 식별하고 마운트합니다.
복구에 필요한 아카이브 로그를 구성된 위치에서 사용할 수 없는 경우 로그를 포함하는 스냅샷 복사본을 마운트하고 경로를 외부 아카이브 로그로 지정해야 합니다.

ASMlib에서 ASMFD로 ASM 데이터베이스를 마이그레이션할 경우 ASMlib를 통해 생성된 백업을 사용하여 데이터베이스를 복원할 수 없습니다. ASMFD 구성에서 백업을 생성하고 이 백업을 사용하여 복원해야 합니다. 마찬가지로 ASM 데이터베이스가 ASMFD에서 ASMlib로 마이그레이션될 경우 ASMlib 구성에서 백업을 생성하여 복원해야 합니다.

데이터베이스를 복구할 때 데이터베이스에서 여러 작업이 실행되지 않도록 Oracle 데이터베이스 호스트의 _/var/opt/snapcenter/sSCO/lock_directory에 운영 잠금 파일(.sm_lock_dbsid)이 생성됩니다. 데이터베이스가 복원되면 운영 잠금 파일이 자동으로 제거됩니다.

SPFILE 및 암호 파일의 복원은 지원되지 않습니다.

- 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. 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 시스템에서 * 백업 * 을 선택합니다.
5. 테이블에서 백업을 선택한 다음 * 를 클릭합니다  *.
6. 복구 범위 페이지에서 다음 작업을 수행합니다.

   a. RAC(Real Application Clusters) 환경에서 데이터베이스 백업을 선택한 경우 RAC 노드를 선택합니다.
   b. 대칭 복사 또는 볼트 데이터 선택 시:
      - 미러 또는 볼트에 로그 백업이 없으면 아무것도 선택되지 않고 로케이터가 비어 있습니다.
      - 로그 백업이 미러 또는 볼트에 있으면 최신 로그 백업이 선택되고 해당 로케이터가 표시됩니다.

        선택한 로그 백업이 미러와 볼트 위치에 모두 있으면 두 로케이터가 모두 표시됩니다.

c. 다음 작업을 수행합니다.

복원하려는 경우...	수행할 작업...
데이터베이스의 모든 데이터 파일	모든 데이터 파일 * 을 선택합니다. 데이터베이스의 데이터 파일만 복원됩니다. 제어 파일, 아카이브 로그 또는 재실행 로그 파일은 복원되지 않습니다.
테이블스페이스	Tablespaces * 를 선택합니다. 복원할 테이블스페이스를 지정할 수 있습니다.
제어 파일	제어 파일 * 을 선택합니다. 제어 파일을 복원하는 동안 복원 프로세스를 통해 파일을 대상 위치로 복사할 수 있도록 디렉터리 구조가 있는지 또는 올바른 사용자 및 그룹 소유로 만들어야 하는지 확인합니다. 디렉토리가 없으면 복원 작업이 실패합니다.
로그 파일을 다시 실행합니다	로그 파일 다시 실행 * 을 선택합니다. 이 옵션은 Data Guard 대기 또는 Active Data Guard 대기 데이터베이스에만 사용할 수 있습니다. REDO 로그 파일은 비 Data Guard 데이터베이스에 대해 백업되지 않습니다. Data Guard가 아닌 데이터베이스의 경우 아카이브 로그를 사용하여 복구가 수행됩니다.
플러그형 데이터베이스(PDB)	Pluggable databases * 를 선택한 다음 복원할 PDB를 지정합니다.
플러깅 지원 데이터베이스(PDB) 테이블스페이스	PDB(Pluggable database) 테이블스페이스 * 를 선택한 다음 복원할 PDB와 해당 PDB의 테이블스페이스를 지정합니다. 이 옵션은 복원을 위해 PDB를 선택한 경우에만 사용할 수 있습니다.

d. 복원 및 복구에 필요한 경우 * 데이터베이스 상태 변경 * 을 선택하여 복원 및 복구 작업을 수행하는 데 필요한 상태로 데이터베이스의 상태를 변경합니다.

   상위 데이터베이스에서 하위 데이터베이스까지의 다양한 상태는 열기, 마운트, 시작 및 종료입니다.

데이터베이스가 더 높은 상태에 있지만 복원 작업을 수행하려면 상태를 더 낮은 상태로 변경해야 하는 경우 이 확인란을 선택해야 합니다. 데이터베이스가 더 낮은 상태에 있지만 복원 작업을 수행하려면 상태를 더 높은 상태로 변경해야 하는 경우 확인란을 선택하지 않아도 데이터베이스 상태가 자동으로 변경됩니다.

데이터베이스가 열려 있는 상태이고 복구를 위해 데이터베이스가 마운트된 상태여야 하는 경우 이 확인란을 선택한 경우에만 데이터베이스 상태가 변경됩니다.

a. 백업 후 새 데이터 파일이 추가되거나 LUN이 LVM 디스크 그룹에 추가, 삭제 또는 재생성될 때 데이터 파일을 데이터 이동 없이 복원하려면 * 강제 복원 * 을 선택합니다.

7. 복구 범위 페이지에서 다음 작업을 수행합니다.

만약...	수행할 작업...
마지막 트랜잭션으로 복구하려고 합니다	모든 로그 * 를 선택합니다.
특정 SCN(시스템 변경 번호)으로 복구하려는 경우	SCN(시스템 변경 번호) * 까지 * 를 선택합니다.
특정 데이터 및 시간으로 복구하려는 경우	날짜 및 시간 * 을 선택합니다. 데이터베이스 호스트의 표준 시간대의 날짜 및 시간을 지정해야 합니다.
복구하기를 원하지 않습니다	No recovery * 를 선택합니다.
외부 아카이브 로그 위치를 지정하려는 경우	데이터베이스가 ARCHIVELOG 모드에서 실행 중인 경우 SnapCenter는 지정된 SCN, 선택한 날짜 및 시간 또는 모든 로그 옵션을 기반으로 최적의 로그 백업 수를 식별하고 마운트합니다. 외부 아카이브 로그 파일의 위치를 계속 지정하려면 * 외부 아카이브 로그 위치 지정 * 을 선택합니다. 아카이브 로그가 백업의 일부로 정리되고 필요한 아카이브 로그 백업을 수동으로 마운트한 경우 마운트된 백업 경로를 복구를 위한 외부 아카이브 로그 위치로 지정해야 합니다. 마운트 경로의 경로와 컨텐츠를 외부 로그 위치로 나열하기 전에 확인해야 합니다. • "NetApp 기술 보고서 4591: 데이터베이스 데이터 보호 백업, 복구, 복제 및 DR" • "ORA-00308 오류로 인해 작업이 실패합니다"

아카이브 로그 볼륨이 보호되지 않지만 데이터 볼륨이 보호되는 경우 보조 백업에서 복구하여 복구를 수행할 수 없습니다. 복구 없음 * 을 선택하여 복원할 수 있습니다.

열린 데이터베이스 옵션을 선택한 상태에서 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 복구 작업 전에 실행할 처방전의 경로와 인수를 입력합니다.

   처방된 내용을 _/var/opt/snapcenter/SPL/scripts_path 또는 이 경로 내의 폴더에 저장해야 합니다. 기본적으로 _/var/opt/snapcenter/SPL/scripts_path가 채워집니다. 스크립트를 저장하기 위해 이 경로 내에 폴더를 만든 경우 경로에 해당 폴더를 지정해야 합니다.

   스크립트 시간 초과 값을 지정할 수도 있습니다. 기본값은 60초입니다.

   SnapCenter에서는 처방과 PS를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다. "자세한 정보"

9. PostOps 페이지에서 다음 단계를 수행하십시오.

   a. 복원 작업 후에 실행할 PostScript의 경로와 인수를 입력합니다.

      postscripts는 */var/opt/snapcenter/SPL/scripts* 또는 이 경로 내의 폴더에 저장해야 합니다. 기본적으로 _/var/opt/snapcenter/SPL/scripts_path가 채워집니다. 스크립트를 저장하기 위해 이 경로 내에 폴더를 만든 경우 경로에 해당 폴더를 지정해야 합니다.

      복원 작업이 실패하면 사후 스크립트가 실행되지 않고 정리 작업이 직접 트리거됩니다.

   b. 복구 후 데이터베이스를 열려면 이 확인란을 선택합니다.

      제어 파일을 사용하거나 사용하지 않고 컨테이너 데이터베이스(CDB)를 복구하거나 CDB 제어 파일만 복구한 후 데이터베이스를 열도록 지정한 경우 해당 CDB에서 플러깅 지원 데이터베이스(PDB)가 아닌 CDB만 열립니다.

      RAC 설정에서는 복구에 사용되는 RAC 인스턴스만 복구 후 열립니다.

      제어 파일, 제어 파일이 있거나 없는 시스템 테이블스페이스 또는 제어 파일이 있거나 없는 PDB를 사용하여 사용자 테이블스페이스를 복구한 후에는 복구 작업과 관련된 PDB 상태만 원래 상태로 변경됩니다. 복구에 사용되지 않은 다른 PDB의 상태는 해당 PDB의 상태가 저장되지 않았기 때문에 원래 상태로 변경되지 않습니다. 복구에 사용되지 않은 PDB의 상태를 수동으로 변경해야 합니다.

10. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일 알림을 보낼 시나리오를 선택합니다.

    또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 수행된 복원 작업의 보고서를 첨부하려면 * 작업 보고서 연결 * 을 선택해야 합니다.

    이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmtpServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

1. 요약을 검토하고 * Finish * 를 클릭합니다.
2. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

- 자세한 정보 *

- "SnapCenter 작업을 수행하기 위해 Oracle RAC One Node 데이터베이스를 건너뜁니다"
- "보조 SnapMirror 또는 SnapVault 위치에서 복원하지 못했습니다"
- "고아 성육신의 백업에서 복원하지 못했습니다"
- "AIX 시스템의 백업, 복원 및 클론 작업에 대한 사용자 정의 가능한 매개 변수"

시점 복구를 사용하여 테이블스페이스를 복구 및 복구합니다

데이터베이스의 다른 테이블스페이스에 영향을 주지 않고 손상되거나 삭제된 테이블스페이스의 하위 집합을 복원할 수 있습니다. SnapCenter는 RMAN을 사용하여 테이블스페이스의 시점 복구(PITR)를 수행합니다.

- 시작하기 전에 *
- 테이블스페이스의 PITR을 수행하는 데 필요한 백업은 카탈로그로 작성되어 마운트되어야 합니다.
- 플러그인을 비루트 사용자로 설치한 경우, prescpt 및 PostScript 디렉토리에 실행 권한을 수동으로 할당해야 합니다.
- 이 작업에 대한 정보 *

PITR 작동 중에 RMAN은 지정된 보조 대상에서 보조 인스턴스를 만듭니다. 보조 대상은 마운트 지점 또는 ASM 디스크 그룹일 수 있습니다. 마운트된 위치에 공간이 충분한 경우 전용 마운트 지점 대신 마운트된 위치 중 하나를 다시 사용할 수 있습니다.

날짜 및 시간 또는 SCN을 지정해야 하며 테이블스페이스가 소스 데이터베이스에 복구됩니다.

ASM, NFS 및 SAN 환경에 상주하는 여러 테이블스페이스를 선택하고 복구할 수 있습니다. 예를 들어 테이블스페이스 TS2 및 TS3가 NFS에 상주하고 TS4가 SAN에 상주하는 경우 단일 PITR 작업을 수행하여 모든 테이블스페이스를 복원할 수 있습니다.

RAC 설정에서 RAC의 모든 노드에서 테이블스페이스의 PITR을 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. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 단일 인스턴스 유형(멀티 테넌트) 데이터베이스를 선택합니다.

   데이터베이스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템에서 * 백업 * 을 선택합니다.

   백업이 카탈로그에 기재되지 않은 경우 백업을 선택하고 * Catalog * 를 클릭해야 합니다.

5. 카탈로그 작성된 백업을 선택하고 * 를 클릭합니다  *.
6. 복구 범위 페이지에서 다음 작업을 수행합니다.
   a. RAC(Real Application Clusters) 환경에서 데이터베이스 백업을 선택한 경우 RAC 노드를 선택합니다.

b. Tablespaces * 를 선택한 다음 복원할 테이블스페이스를 지정합니다.

SYSAUX, 시스템 및 실행 취소 테이블스페이스에서 PITR을 수행할 수 없습니다.

c. 복원 및 복구에 필요한 경우 * 데이터베이스 상태 변경 * 을 선택하여 복원 및 복구 작업을 수행하는 데 필요한 상태로 데이터베이스의 상태를 변경합니다.

7. 복구 범위 페이지에서 다음 작업 중 하나를 수행합니다.
   - 특정 SCN(시스템 변경 번호)으로 복구하려면 SCN * 이 될 때까지 * 를 선택하고 SCN 및 보조 대상을 지정합니다.
   - 특정 날짜 및 시간으로 복구하려면 * 날짜 및 시간 * 을 선택하고 날짜 및 시간과 보조 대상을 지정합니다.

     SnapCenter는 지정된 SCN 또는 선택한 날짜 및 시간을 기반으로 PITR을 수행하는 데 필요한 최적의 데이터 및 로그 백업 수를 식별하고 카탈로그로 작성합니다.

8. PreOps 페이지에서 복구 작업 전에 실행할 처방전의 경로와 인수를 입력합니다.

   처방된 내용을 /var/opt/snapcenter/spl/scripts 경로 또는 이 경로 내의 폴더에 저장해야 합니다. 기본적으로 /var/opt/snapcenter/SPL/scripts 경로가 채워집니다. 스크립트를 저장하기 위해 이 경로 내에 폴더를 만든 경우 경로에 해당 폴더를 지정해야 합니다.

   스크립트 시간 초과 값을 지정할 수도 있습니다. 기본값은 60초입니다.

SnapCenter에서는 처방과 PS를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다. "자세한 정보"

1. PostOps 페이지에서 다음 단계를 수행하십시오.
   a. 복원 작업 후에 실행할 PostScript의 경로와 인수를 입력합니다.

   복원 작업이 실패하면 사후 스크립트가 실행되지 않고 정리 작업이 직접 트리거됩니다.

   b. 복구 후 데이터베이스를 열려면 이 확인란을 선택합니다.
2. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일 알림을 보낼 시나리오를 선택합니다.
3. 요약을 검토하고 * Finish * 를 클릭합니다.
4. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

시점 복구를 사용하여 플러그형 데이터베이스를 복원 및 복구합니다

컨테이너 데이터베이스(CDB)의 다른 PDB에 영향을 주지 않고 손상되거나 삭제된 플러그형 데이터베이스(PDB)를 복원 및 복구할 수 있습니다. SnapCenter는 RMAN을 사용하여 PDB의 시점 복구(PITR)를 수행합니다.

- 시작하기 전에 *
- PDB의 PITR을 수행하는 데 필요한 백업은 카탈로그로 작성되어 마운트되어야 합니다.

RAC 설정에서 RAC 설정의 모든 노드에서 PDB를 수동으로 닫아야 합니다(상태를 마운트된 상태로 변경).

- 플러그인을 비루트 사용자로 설치한 경우, prescpt 및 PostScript 디렉토리에 실행 권한을 수동으로 할당해야 합니다.
- 이 작업에 대한 정보 *

PITR 작동 중에 RMAN은 지정된 보조 대상에서 보조 인스턴스를 만듭니다. 보조 대상은 마운트 지점 또는 ASM 디스크 그룹일 수 있습니다. 마운트된 위치에 공간이 충분한 경우 전용 마운트 지점 대신 마운트된 위치 중 하나를 다시 사용할 수 있습니다.

PDB의 PITR을 수행하려면 날짜 및 시간 또는 SCN을 지정해야 합니다. RMAN은 데이터 파일을 포함하여 읽기 쓰기, 읽기 전용 또는 손실된 PDB를 복구할 수 있습니다.

다음 경우에만 복원 및 복구할 수 있습니다.

- 한 번에 PDB 한 개
- PDB의 테이블스페이스 하나
- 동일한 PDB의 여러 테이블스페이스입니다

RAC 설정에서 RAC의 모든 노드에서 테이블스페이스의 PITR을 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. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 단일 인스턴스 유형(멀티 테넌트) 데이터베이스를 선택합니다.

   데이터베이스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 복제) 스토리지 시스템에서 * 백업 * 을 선택합니다.

   백업이 카탈로그에 기재되지 않은 경우 백업을 선택하고 * Catalog * 를 클릭해야 합니다.

5. 카탈로그 작성된 백업을 선택하고 * 를 클릭합니다 *.
6. 복구 범위 페이지에서 다음 작업을 수행합니다.
   a. RAC(Real Application Clusters) 환경에서 데이터베이스 백업을 선택한 경우 RAC 노드를 선택합니다.
   b. PDB의 PDB 또는 테이블스페이스를 복원할지 여부에 따라 다음 작업 중 하나를 수행합니다.

원하는 작업	단계…
PDB를 복원합니다	i. Pluggable databases (PDB) * 를 선택합니다. ii. 복원할 PDB를 지정합니다. PDB$ 시드 데이터베이스에서 PITR을 수행할 수 없습니다.

PDB에서 테이블스페이스를 복구합니다	i. Pluggable database (PDB) 테이블스페이스 * 를 선택합니다. ii. PDB를 지정합니다. iii. 복원할 단일 테이블스페이스 또는 여러 테이블스페이스를 지정합니다. SYSAUX, 시스템 및 실행 취소 테이블스페이스에서 PITR을 수행할 수 없습니다.

c. 복원 및 복구에 필요한 경우 * 데이터베이스 상태 변경 * 을 선택하여 복원 및 복구 작업을 수행하는 데 필요한 상태로 데이터베이스의 상태를 변경합니다.

7. 복구 범위 페이지에서 다음 작업 중 하나를 수행합니다.
   - 특정 SCN(시스템 변경 번호)으로 복구하려면 SCN * 이 될 때까지 * 를 선택하고 SCN 및 보조 대상을 지정합니다.
   - 특정 날짜 및 시간으로 복구하려면 * 날짜 및 시간 * 을 선택하고 날짜 및 시간과 보조 대상을 지정합니다.

     SnapCenter는 지정된 SCN 또는 선택한 날짜 및 시간을 기반으로 PITR을 수행하는 데 필요한 최적의 데이터 및 로그 백업 수를 식별하고 카탈로그로 작성합니다.

8. PreOps 페이지에서 복구 작업 전에 실행할 처방전의 경로와 인수를 입력합니다.

   처방된 내용을 /var/opt/snapcenter/spl/scripts 경로 또는 이 경로 내의 폴더에 저장해야 합니다. 기본적으로 /var/opt/snapcenter/SPL/scripts 경로가 채워집니다. 스크립트를 저장하기 위해 이 경로 내에 폴더를 만든 경우 경로에 해당 폴더를 지정해야 합니다.

   스크립트 시간 초과 값을 지정할 수도 있습니다. 기본값은 60초입니다.

SnapCenter에서는 처방과 PS를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다. "자세한 정보"

1. PostOps 페이지에서 다음 단계를 수행하십시오.
   a. 복원 작업 후에 실행할 PostScript의 경로와 인수를 입력합니다.

      복원 작업이 실패하면 사후 스크립트가 실행되지 않고 정리 작업이 직접 트리거됩니다.

   b. 복구 후 데이터베이스를 열려면 이 확인란을 선택합니다.

      RAC 설정에서는 데이터베이스가 복구된 노드에서만 PDB가 열립니다. RAC 설정의 다른 모든 노드에서 복구된 PDB를 수동으로 열어야 합니다.

2. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일 알림을 보낼 시나리오를 선택합니다.
3. 요약을 검토하고 * Finish * 를 클릭합니다.
4. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

UNIX 명령을 사용하여 Oracle 데이터베이스를 복구 및 복구합니다

복원 및 복구 워크플로에는 계획, 복원 및 복구 작업 수행 및 작업 모니터링이 포함됩니다.

- 이 작업에 대한 정보 *

다음 명령을 실행하여 SnapCenter 서버와의 연결을 설정하고, 백업을 나열하고, 해당 정보를 검색하고, 백업을 복원해야 합니다.

명령에 사용할 수 있는 매개 변수 및 해당 설명에 대한 정보는 get-Help_command_name_을 실행하여 얻을 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 명령 참조 가이드".

- 단계 *

1. 지정된 사용자에 대해 SnapCenter 서버와 연결 세션을 시작합니다. _ Open - SmConnection _
2. 복원하려는 백업에 대한 정보를 검색합니다. *get-SmBackup*
3. 지정된 백업에 대한 자세한 정보(*Get-SmBackupDetails*)를 검색합니다

   이 명령은 지정된 백업 ID를 사용하여 지정된 리소스 백업에 대한 자세한 정보를 검색합니다. 이 정보에는 데이터베이스 이름, 버전, 홈, 시작 및 종료 SCN, 테이블스페이스, 플러깅 지원 데이터베이스 및 테이블스페이스가 포함됩니다.

4. 백업에서 데이터를 복원합니다:_Restore-SmBackup_

Oracle 데이터베이스 복원 작업을 모니터링합니다

작업 페이지를 사용하여 여러 SnapCenter 복원 작업의 진행률을 모니터링할 수 있습니다. 작업 진행률을 확인하여 작업이 언제 완료되는지 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

복원 후 상태는 복원 작업 후 리소스의 상태와 수행할 수 있는 추가 복원 작업에 대해 설명합니다.

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨

단계

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 모니터 * 페이지에서 * 작업 * 을 클릭합니다.
3. Jobs * 페이지에서 다음 단계를 수행하십시오.

a. 을 클릭합니다 복원 작업만 나열되도록 목록을 필터링하려면
b. 시작 및 종료 날짜를 지정합니다.
c. Type * 드롭다운 목록에서 * Restore * 를 선택합니다.
d. Status * (상태 *) 드롭다운 목록에서 복원 상태를 선택합니다.
e. 성공적으로 완료된 작업을 보려면 * 적용 * 을 클릭합니다.

4. 복원 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. Job Details * 페이지에서 * View logs * 를 클릭합니다.

로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

볼륨 기반 복원 작업 후에는 백업 메타데이터가 SnapCenter 저장소에서 삭제되지만 백업 카탈로그 항목은 SAP HANA 카탈로그에 남아 있습니다. 복원 작업 상태가 표시됩니다 작업 세부 정보를 클릭하여 일부 하위 작업의 경고 표시를 확인해야 합니다. 경고 표지를 클릭하고 표시된 백업 카탈로그 항목을 삭제합니다.

Oracle 데이터베이스 복원 작업을 취소합니다

대기열에 있는 복원 작업을 취소할 수 있습니다.

복원 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

이 작업에 대해

- Monitor* 페이지 또는 * Activity* 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 작업에는 * 작업 취소 * 버튼이 비활성화됩니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 사용자\그룹 페이지의 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.

시작...	조치
모니터 페이지	1. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 클릭합니다. 2. 작업을 선택하고 * 작업 취소 * 를 클릭합니다.
작업 창	1. 복원 작업을 시작한 후 을 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다. 2. 작업을 선택합니다. 3. 작업 세부 정보 페이지에서 * 작업 취소 * 를 클릭합니다.

Oracle 데이터베이스 클론 생성

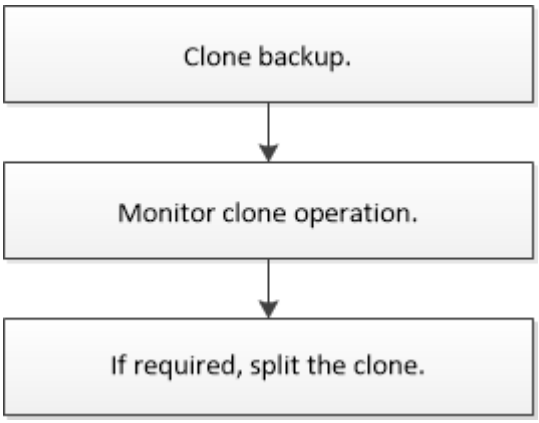
클론 복제 워크플로우

클론 워크플로우에는 계획, 클론 작업 수행 및 작업 모니터링이 포함됩니다.

다음과 같은 이유로 데이터베이스를 복제할 수 있습니다.

- 응용 프로그램 개발 주기 동안 현재 데이터베이스 구조 및 콘텐츠를 사용하여 구현해야 하는 기능을 테스트합니다.
- 데이터 추출 및 조작 도구를 사용하여 데이터 웨어하우스를 채웁니다.
- 실수로 삭제 또는 변경된 데이터를 복구합니다.

다음 워크플로에서는 클론 작업을 수행해야 하는 순서를 보여 줍니다.



Oracle 데이터베이스에 대한 클론 전략 정의

데이터베이스를 복제하기 전에 전략을 정의하면 클론 생성 작업이 성공적으로 수행됩니다.

클론 생성에 지원되는 백업 유형입니다

SnapCenter는 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
- 온라인 데이터 백업, 온라인 전체 백업, 오프라인 마운트 백업 및 RAC(Real Application Clusters) 구성의 오프라인 종료 백업
- 온라인 데이터 백업, 온라인 전체 백업, 오프라인 마운트 백업 및 ASM(Automatic Storage Management) 구성에서 오프라인 종료 백업

다중 경로 구성 파일의 user_friendly_names 옵션이 yes로 설정되어 있으면 SAN 구성이 지원되지 않습니다.

아카이브 로그 백업의 클론 생성은 지원되지 않습니다.

Oracle 데이터베이스에 지원되는 클론 생성 유형입니다

Oracle 데이터베이스 환경에서 SnapCenter은 데이터베이스 백업의 복제를 지원합니다. 기본 및 보조 스토리지 시스템에서 백업을 복제할 수 있습니다.

SnapCenter 서버는 NetApp FlexClone 기술을 사용하여 백업을 복제합니다.

"Refresh-SmClone" 명령을 실행하여 클론을 새로 고칠 수 있습니다. 이 명령은 데이터베이스의 백업을 생성하고 기존 클론을 삭제한 다음 같은 이름의 클론을 생성합니다.

클론 새로 고침 작업은 UNIX 명령을 통해서만 수행할 수 있습니다.

Oracle 데이터베이스에 대한 클론 명명 규칙

SnapCenter 3.0에서는 파일 시스템의 클론에 사용되는 명명 규칙이 ASM 디스크 그룹의 클론과 다릅니다.

- SAN 또는 NFS 파일 시스템의 명명 규칙은 FileSystemNameofsourcedatabase_CLONEID입니다.
- ASM 디스크 그룹의 명명 규칙은 SC_HASHCODEofDISKGROUP_CLONEID입니다.

  HASHCODEofDISKGROUP은 ASM 디스크 그룹마다 고유한 자동 생성 번호(2 ~ 10자리)입니다.

Oracle 데이터베이스 복제의 제한 사항

데이터베이스를 클론 복제하기 전에 클론 작업의 제한 사항을 숙지해야 합니다.

- 11.2.0.4 ~ 12.1.0.1의 Oracle 버전을 사용하는 경우 *renamedg* 명령을 실행하면 클론 작업이 멈춤 상태가 됩니다. Oracle 패치 19544733을 적용하여 이 문제를 해결할 수 있습니다.
- 호스트에 직접 연결된 LUN(예: Windows 호스트의 Microsoft iSCSI Initiator 사용)에서 동일한 Windows 호스트의 VMDK 또는 RDM LUN에 또는 다른 Windows 호스트의 RDM LUN에 대한 데이터베이스 클론 생성은 지원되지 않습니다.
- 볼륨 마운트 지점의 루트 디렉토리는 공유 디렉토리일 수 없습니다.
- 클론이 포함된 LUN을 새 볼륨으로 이동하면 클론을 삭제할 수 없습니다.

클론별 정의 정의 지정 지정 지정 및 **PostScript**에 대한 사전 정의된 환경 변수입니다

SnapCenter를 사용하면 데이터베이스를 복제하는 동안 처방과 PS를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다.

- 데이터베이스 복제를 위해 미리 정의된 환경 변수 지원 *
- * sc_original_SID * 는 소스 데이터베이스의 SID를 지정합니다.

이 매개 변수는 애플리케이션 볼륨에 대해 채워집니다.

예: NFSB32

- * sc_original_host * 는 소스 호스트의 이름을 지정합니다.

  이 매개 변수는 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 백업 이름을 지정합니다.

  이 매개 변수는 애플리케이션 볼륨에 대해 채워집니다.

  예:

  ◦ 데이터베이스가 ARCHIVELOG 모드에서 실행되고 있지 않은 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 실행 중인 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_16.7_16.7_16.7_07-22

- * SC_AV_NAME * 은 애플리케이션 볼륨의 이름을 지정합니다.

  예: AV1 | AV2

- * sc_original_OS_user * 는 소스 데이터베이스의 운영 체제 소유자를 지정합니다.

  예: Oracle

- * sc_original_OS_group * 은 소스 데이터베이스의 운영 체제 그룹을 지정합니다.

  예: oinstall

- "SC_TARGET_SID * "는 복제된 데이터베이스의 SID를 지정합니다.

  PDB 복제 워크플로우의 경우 이 매개 변수의 값은 사전 정의되지 않습니다.

  이 매개 변수는 애플리케이션 볼륨에 대해 채워집니다.

  예: clonedb

- * SC_TARGET_HOST * 는 데이터베이스를 복제할 호스트의 이름을 지정합니다.

  이 매개 변수는 애플리케이션 볼륨에 대해 채워집니다.

  예: asmrac1.gdl.englab.netapp.com

- * SC_TARGET_OS_USER * 는 복제된 데이터베이스의 운영 체제 소유자를 지정합니다.

  PDB 복제 워크플로우의 경우 이 매개 변수의 값은 사전 정의되지 않습니다.

  예: Oracle

- * SC_TARGET_OS_GROUP * 은 복제된 데이터베이스의 운영 체제 그룹을 지정합니다.

  PDB 복제 워크플로우의 경우 이 매개 변수의 값은 사전 정의되지 않습니다.

  예: oinstall

- * SC_TARGET_DB_PORT * 는 복제된 데이터베이스의 데이터베이스 포트를 지정합니다.

  PDB 복제 워크플로우의 경우 이 매개 변수의 값은 사전 정의되지 않습니다.

  예: 1521

구분 기호에 대한 자세한 내용은 을 참조하십시오 "지원되는 구분 기호".

Oracle 데이터베이스 클론 생성 요구 사항

Oracle 데이터베이스를 복제하기 전에 필수 구성 요소가 완료되었는지 확인해야 합니다.

- SnapCenter를 사용하여 데이터베이스 백업을 만들어야 합니다.

  클론 생성 작업을 성공적으로 수행하려면 온라인 데이터 및 로그 백업 또는 오프라인(마운트 또는 종료) 백업을 성공적으로 생성해야 합니다.

- 제어 파일 또는 redo 로그 파일 경로를 사용자 지정하려면 필요한 파일 시스템 또는 ASM(Automatic Storage Management) 디스크 그룹을 미리 프로비저닝해야 합니다.

  기본적으로 클론 데이터베이스의 재실행 로그 및 제어 파일은 ASM 디스크 그룹 또는 SnapCenter이 클론 데이터베이스의 데이터 파일에 대해 프로비저닝한 파일 시스템에 생성됩니다.

- ASM over NFS를 사용하는 경우 ASM_diskstring 매개 변수에 정의된 기존 경로에 _/var/opt/snapcenter/SCU/clones/ */ *_를 추가해야 합니다.
- ASM_diskstring 매개 변수에서 ASMFD 또는 configure_ORCL: *_을 사용하는 경우 ASMlib를 사용하는 경우 _AFD: *_를 구성해야 합니다.

  ASM_diskstring 매개 변수를 편집하는 방법에 대한 자세한 내용은 을 참조하십시오 "ASM_diskstring에 디스크 경로를 추가하는 방법".

- 대체 호스트에서 클론을 생성하는 경우 대체 호스트는 다음 요구 사항을 충족해야 합니다.
  - Oracle 데이터베이스용 SnapCenter 플러그인을 대체 호스트에 설치해야 합니다.
  - 클론 호스트는 운영 스토리지 또는 보조 스토리지에서 LUN을 검색할 수 있어야 합니다.
    - 운영 스토리지 또는 보조(볼트 또는 미러) 스토리지에서 대체 호스트로 클론을 생성하는 경우 iSCSI 세션이 보조 스토리지와 대체 호스트 간에 설정되거나 FC에 대해 적절하게 조닝(Zoning)되었는지 확인합니다.
    - Vault 또는 Mirror 스토리지에서 동일한 호스트로 클론을 생성하는 경우, iSCSI 세션이 Vault 또는 Mirror

스토리지와 호스트 간에 설정되어 있는지 또는 FC에 맞게 조닝(zoning)되어 있는지 확인합니다.

- 가상화 환경에서 클론을 생성하는 경우 iSCSI 세션이 운영 스토리지 또는 보조 스토리지와 대체 호스트를 호스팅하는 ESX 서버 간에 설정되어 있는지 또는 FC에 대해 적절하게 조닝(zoning)되어 있는지 확인합니다.

  자세한 내용은 을 참조하십시오 "호스트 유틸리티 설명서".

- 소스 데이터베이스가 ASM 데이터베이스인 경우:
  - ASM 인스턴스는 클론이 수행될 호스트에서 실행 중이어야 합니다.
  - 클론 데이터베이스의 아카이브 로그 파일을 전용 ASM 디스크 그룹에 배치하려면 클론 작업 전에 ASM 디스크 그룹을 프로비저닝해야 합니다.
  - 데이터 디스크 그룹의 이름은 구성할 수 있지만 클론이 수행될 호스트의 다른 ASM 디스크 그룹에서 해당 이름을 사용하지 않도록 해야 합니다.

    ASM 디스크 그룹에 상주하는 데이터 파일은 SnapCenter 클론 워크플로우의 일부로 프로비저닝됩니다.

- NVMe의 경우 NVMe util을 설치해야 합니다

- 로그 백업을 사용하여 대체 호스트에 클론을 생성하는 동안 보조 로케이터를 검색하려면 데이터 LUN과 미러, 볼트 또는 미러 볼트와 같은 로그 LUN에 대한 보호 유형이 동일해야 합니다.
- 소스 데이터베이스 매개 변수 파일에서 exclude_seed_cdb_view의 값을 false로 설정하여 12_c_database의 백업 복제를 위한 시드 PDB 관련 정보를 검색해야 합니다.

  시드 PDB는 CDB가 PDB를 생성하는 데 사용할 수 있는 시스템 제공 템플릿입니다. 시드 PDB의 이름은 PDB$seed입니다. PDB$ 시드에 대한 자세한 내용은 Oracle Doc ID 1940806.1을 참조하십시오.

  12_c_database를 백업하기 전에 값을 설정해야 합니다.

- SnapCenter는 autofs 서브시스템에서 관리하는 파일 시스템의 백업을 지원합니다. 데이터베이스를 복제하는 경우 플러그인 호스트의 루트 사용자에게 autofs 마운트 지점의 루트 아래에 디렉토리를 생성할 권한이 없으므로 데이터 마운트 지점이 autofs 마운트 지점의 루트 아래에 있지 않은지 확인합니다.

  제어 및 재실행 로그 파일이 데이터 마운트 지점에 있는 경우 제어 파일 경로를 수정한 다음 그에 따라 로그 파일 경로를 다시 실행해야 합니다.

  새로 클론된 마운트 지점을 autofs 하위 시스템에 수동으로 등록할 수 있습니다. 새로 클론된 마운트 지점은 자동으로 등록되지 않습니다.

- TDE(자동 로그인)가 있고 동일한 호스트 또는 대체 호스트에서 데이터베이스를 복제하려는 경우 소스 데이터베이스에서 복제된 데이터베이스로 _ /etc/oracle/wallet/$oracle_SID_ 아래의 Wallet(키 파일)을 복사해야 합니다.
- use_lvmetad = 0 in_/etc/lvm/lvm.conf_의 값을 설정하고 lvm2-lvmetad 서비스를 중지하여 Oracle Linux 7 이상 또는 Red Hat Enterprise Linux(RHEL) 7 이상의 SAN 환경에서 클론을 성공적으로 수행해야 합니다.
- Oracle 데이터베이스 11.2.0.3 이상을 사용하고 보조 인스턴스의 데이터베이스 ID가 NID 스크립트를 사용하여 변경된 경우 13366202 Oracle 패치를 설치해야 합니다.
- 볼륨을 호스팅하는 애그리게이트는 SVM(스토리지 가상 머신)의 할당된 애그리게이트 목록에 있어야 합니다.
- NVMe의 경우 대상 포트를 연결에 제외해야 하는 경우 /var/opt/snapcenter/scu/etc/NVMe.conf 파일에 타겟 노드 이름과 포트 이름을 추가해야 합니다.

파일이 없는 경우 아래 예와 같이 파일을 작성해야 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>
}
```

- 혼합 프로토콜 iSCSI 및 FC로 구성된 iGroup을 사용하여 LUN이 AIX 호스트에 매핑되지 않았는지 확인해야 합니다. 자세한 내용은 을 참조하십시오 "LUN에 대한 디바이스를 검색할 수 없어 작업이 실패합니다".

Oracle 데이터베이스 백업의 클론을 생성합니다

SnapCenter를 사용하여 데이터베이스 백업을 사용하여 Oracle 데이터베이스를 복제할 수 있습니다.

- 시작하기 전에 *

플러그인을 비루트 사용자로 설치한 경우, prescpt 및 PostScript 디렉토리에 실행 권한을 수동으로 할당해야 합니다.

- 이 작업에 대한 정보 *

클론 생성 작업을 수행하면 데이터베이스 데이터 파일의 복사본이 생성되고 새 온라인 redo 로그 파일과 제어 파일이 생성됩니다. 지정된 복구 옵션에 따라 데이터베이스를 지정된 시간으로 선택적으로 복구할 수 있습니다.

Linux 호스트에서 생성된 백업을 AIX 호스트에 복제하거나 그 반대로 복제하려고 하면 클론 생성이 실패합니다.

SnapCenter는 Oracle RAC 데이터베이스 백업에서 클론 복제할 때 독립 실행형 데이터베이스를 생성합니다. SnapCenter는 Data Guard 대기 및 Active Data Guard 대기 데이터베이스 백업에서 클론을 생성할 수 있도록 지원합니다.

클론 생성 중에 SnapCenter는 복구 작업에 대한 SCN 또는 데이터 및 시간을 기준으로 최적의 로그 백업 수를 마운트합니다. 복구 후 로그 백업이 마운트 해제됩니다. 이러한 모든 클론은 */var/opt/snapcenter/SCU/clones/* 아래에 마운트됩니다. ASM over NFS를 사용하는 경우 ASM_diskstring 매개 변수에 정의된 기존 경로에 _/var/opt/snapcenter/SCU/clones/ */ *_를 추가해야 합니다.

SAN 환경에서 ASM 데이터베이스의 백업을 복제하는 동안 복제된 호스트 디바이스에 대한 udev 규칙이 _ /etc/udev/rules.d/999-scu-netapp.rules_ 에 생성됩니다. 클론 생성된 호스트 디바이스와 연결된 이러한 udev 규칙은 클론을 삭제할 때 삭제됩니다.

Flex ASM 설정에서 카디널리티가 RAC 클러스터의 노드 수보다 적은 경우 Leaf 노드에서 클론 작업을 수행할 수 없습니다.

- 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. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 데이터베이스를 선택합니다.

데이터베이스 토폴로지 페이지가 표시됩니다.

4. Manage Copies 보기에서 Local copies (primary), Mirror copies (secondary) 또는 Vault copies (secondary) 중에서 백업을 선택합니다.
5. 테이블에서 데이터 백업을 선택한 다음 * 를 클릭합니다  *.
6. 이름 페이지에서 다음 작업 중 하나를 수행합니다.

원하는 작업	단계...
데이터베이스 클론 생성(CDB 또는 비 CDB)	a. 클론의 SID를 지정합니다. 클론 SID는 기본적으로 사용할 수 없으며 SID의 최대 길이는 8자입니다. 클론을 생성할 호스트에 동일한 SID의 데이터베이스가 없는지 확인해야 합니다.
플러깅 지원 데이터베이스(PDB) 클론 생성	a. PDB 복제 * 를 선택합니다. b. 복제할 PDB를 지정합니다. c. 복제된 PDB의 이름을 지정합니다. PDB를 복제하는 자세한 단계는 를 참조하십시오 "플러그형 데이터베이스의 클론 복제".

대칭 복사 또는 볼트 데이터 선택 시:

- 미러 또는 볼트에 로그 백업이 없으면 아무것도 선택되지 않고 로케이터가 비어 있습니다.
- 로그 백업이 미러 또는 볼트에 있으면 최신 로그 백업이 선택되고 해당 로케이터가 표시됩니다.

선택한 로그 백업이 미러와 볼트 위치에 모두 있으면 두 로케이터가 모두 표시됩니다.

7. 위치 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
호스트 복제	기본적으로 소스 데이터베이스 호스트는 채워집니다. 대체 호스트에서 클론을 생성하려면 소스 데이터베이스 호스트의 버전과 Oracle 및 OS 버전이 동일한 호스트를 선택합니다.

이 필드의 내용...	수행할 작업...
데이터 파일 위치	기본적으로 데이터 파일 위치는 채워집니다. SAN 또는 NFS 파일 시스템에 대한 SnapCenter 기본 명명 규칙은 FileSystemNameofsourcedatabase_CLONEID입니다. ASM 디스크 그룹에 대한 SnapCenter 기본 명명 규칙은 SC_HASHCODEofDISKGROUP_CLONEID입니다. HASHCODEofDISKGROUP은 ASM 디스크 그룹마다 고유한 자동 생성 번호(2 ~ 10자리)입니다. ⓘ ASM 디스크 그룹 이름을 사용자 지정하는 경우 이름 길이가 Oracle에서 지원하는 최대 길이를 따르는지 확인합니다. 다른 경로를 지정하려면 클론 데이터베이스의 데이터 파일 마운트 지점 또는 ASM 디스크 그룹 이름을 입력해야 합니다. 데이터 파일 경로를 사용자 지정할 때는 데이터 파일에 사용된 것과 동일한 이름 또는 기존 ASM 디스크 그룹 또는 파일 시스템으로 제어 파일과 redo 로그 파일 ASM 디스크 그룹 이름 또는 파일 시스템을 변경해야 합니다.
제어 파일	기본적으로 제어 파일 경로가 채워집니다. 제어 파일은 데이터 파일과 동일한 ASM 디스크 그룹 또는 파일 시스템에 배치됩니다. 제어 파일 경로를 재정의하려면 다른 제어 파일 경로를 제공할 수 있습니다. ⓘ 파일 시스템 또는 ASM 디스크 그룹이 호스트에 있어야 합니다. 기본적으로 컨트롤 파일 수는 소스 데이터베이스의 수와 동일합니다. 제어 파일 수는 수정할 수 있지만 데이터베이스를 복제하려면 최소한 하나의 제어 파일이 필요합니다. 제어 파일 경로를 소스 데이터베이스와 다른 파일 시스템(기존 파일)으로 사용자 지정할 수 있습니다.

이 필드의 내용...	수행할 작업...
다시 실행 로그	기본적으로 redo 로그 파일 그룹, 경로 및 크기가 채워집니다. 재실행 로그는 클론 데이터베이스의 데이터 파일과 동일한 ASM 디스크 그룹 또는 파일 시스템에 배치됩니다. 재실행 로그 파일 경로를 재정의하려면 redo 로그 파일 경로를 소스 데이터베이스와 다른 파일 시스템으로 사용자 지정할 수 있습니다. ⓘ 새 파일 시스템 또는 ASM 디스크 그룹이 호스트에 있어야 합니다. 기본적으로 redo 로그 그룹 수, redo 로그 파일 및 해당 크기는 소스 데이터베이스와 동일합니다. 다음 매개변수를 수정할 수 있습니다. • redo 로그 그룹의 수입니다 ⓘ 데이터베이스를 복제하려면 최소 2개의 REDO 로그 그룹이 필요합니다. • 각 그룹 및 해당 경로의 로그 파일을 다시 실행합니다 redo 로그 파일 경로를 소스 데이터베이스와 다른 파일 시스템(기존 파일)으로 사용자 지정할 수 있습니다. ⓘ 데이터베이스를 복제하려면 redo 로그 그룹에 최소 하나의 redo 로그 파일이 필요합니다. • redo 로그 파일의 크기입니다

8. 자격 증명 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
sys 사용자의 자격 증명 이름입니다	클론 데이터베이스의 sys 사용자 암호를 정의하는 데 사용할 자격 증명을 선택합니다. 대상 호스트의 sqlnet.ora 파일에 SQLNET.authentication_services가 none으로 설정되어 있으면 SnapCenter GUI에서 자격 증명으로 * 없음 * 을 선택하지 않아야 합니다.

이 필드의 내용...	수행할 작업...
ASM 인스턴스 자격 증명 이름입니다	클론 호스트의 ASM 인스턴스에 연결할 수 있도록 OS 인증이 활성화된 경우 * 없음 * 을 선택합니다. 그렇지 않으면 "sys" 사용자로 구성된 Oracle ASM 자격 증명 또는 클론 호스트에 적용할 수 있는 "sysasm" 권한이 있는 사용자를 선택합니다.

Oracle 홈, 사용자 이름 및 그룹 세부 정보는 소스 데이터베이스에서 자동으로 채워집니다. 클론을 생성할 호스트의 Oracle 환경에 따라 값을 변경할 수 있습니다.

9. PreOps 페이지에서 다음 단계를 수행하십시오.

   a. 클론 작업 전에 실행할 처방전의 경로와 인수를 입력합니다.

      처방된 내용을 */var/opt/snapcenter/SPL/scripts* 또는 이 경로 내의 폴더에 저장해야 합니다. 기본적으로 _/var/opt/snapcenter/SPL/scripts_path가 채워집니다. 이 경로 내의 폴더에 스크립트를 배치한 경우 스크립트가 있는 폴더까지 전체 경로를 제공해야 합니다.

      SnapCenter에서는 처방과 PS를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다. "자세한 정보"

   b. 데이터베이스 매개 변수 설정 섹션에서 데이터베이스를 초기화하는 데 사용되는 미리 채워진 데이터베이스 매개 변수의 값을 수정합니다.

      를 클릭하여 추가 매개 변수를 추가할 수 있습니다 + *.

      Oracle Standard Edition을 사용 중이고 데이터베이스가 아카이브 로그 모드에서 실행 중이거나 아카이브 redo 로그에서 데이터베이스를 복원하려면 매개 변수를 추가하고 경로를 지정합니다.

      - LOG_ARCHIVE_DEST
      - log_archive_duplex_DEST

      FRA(Fast Recovery Area)가 미리 채워진 데이터베이스 매개 변수에 정의되지 않았습니다. 관련 매개변수를 추가하여 FRA를 구성할 수 있습니다.

      log_archive_dest_1의 기본값은 $ORACLE_HOME/clone_sid이며 복제된 데이터베이스의 아카이브 로그가 이 위치에 생성됩니다. log_archive_dest_1 매개 변수를 삭제한 경우 아카이브 로그 위치는 Oracle에서 결정합니다. log_archive_dest_1을 편집하여 아카이브 로그의 새 위치를 정의할 수 있지만 파일 시스템 또는 디스크 그룹이 기존 상태여야 하며 호스트에서 사용할 수 있어야 합니다.

   a. 기본 데이터베이스 매개 변수 설정을 가져오려면 * Reset * (재설정 *)을 클릭합니다.

10. PostOps 페이지에서 * Recover database * 및 * until Cancel * 이 기본적으로 선택되어 복제된 데이터베이스의 복구를 수행합니다.

    SnapCenter는 클론 생성을 위해 선택한 데이터 백업 이후에 연속되지 않은 아카이브 로그가 있는 최신 로그 백업을 마운트하여 복구를 수행합니다. 운영 스토리지에서 클론을 수행하려면 로그 및 데이터 백업이 운영 스토리지에 있어야 하고 보조 스토리지에서 클론을 수행하려면 로그 및 데이터 백업이 보조 스토리지에 있어야 합니다.

SnapCenter가 적절한 로그 백업을 찾지 못할 경우 * 데이터베이스 복구 * 및 * 취소 시까지 * 옵션이 선택되지 않습니다. 로그 백업을 사용할 수 없는 경우 * 외부 아카이브 로그 위치 지정 * 에서 외부 아카이브 로그 위치를 제공할 수 있습니다. 여러 로그 위치를 지정할 수 있습니다.

FRA(Flash Recovery Area) 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 또는 Active Data Guard 대기 데이터베이스인 경우 PostOps 페이지가 표시되지 않습니다. Data Guard 대기 또는 Active Data Guard 대기 데이터베이스의 경우 SnapCenter는 SnapCenter GUI에서 복구 유형을 선택할 수 있는 옵션을 제공하지 않지만 로그를 적용하지 않고 복구 유형 취소를 통해 데이터베이스를 복구합니다.

필드 이름입니다	설명
를 눌러 취소 로 이동합니다	SnapCenter는 클론 생성을 위해 선택한 데이터 백업 이후에 연속되지 않은 아카이브 로그가 있는 최신 로그 백업을 마운트하여 복구를 수행합니다. 로그 파일이 없거나 손상될 때까지 복제된 데이터베이스가 복구됩니다.
날짜 및 시간	SnapCenter는 데이터베이스를 지정된 날짜 및 시간까지 복구합니다. 허용되는 형식은 mm/dd/yyyy hh:mm:ss입니다. 시간은 24시간 형식으로 지정할 수 있습니다.
SCN(시스템 변경 번호)까지	SnapCenter는 데이터베이스를 지정된 SCN(시스템 변경 번호)까지 복구합니다.
외부 아카이브 로그 위치를 지정합니다	데이터베이스가 ARCHIVELOG 모드에서 실행 중인 경우 SnapCenter는 지정된 SCN 또는 선택한 날짜 및 시간을 기반으로 최적의 로그 백업 수를 식별하고 마운트합니다. 외부 아카이브 로그 위치를 지정할 수도 있습니다. 취소 전까지 선택한 경우 SnapCenter는 로그 백업을 자동으로 식별하고 마운트하지 않습니다.

필드 이름입니다	설명
새 DBID를 생성합니다	기본적으로 * Create new DBID * (새 DBID 생성 *) 확인란이 선택되어 복제된 데이터베이스에 대한 고유 번호(DBID)가 소스 데이터베이스와 구별됩니다. 원본 데이터베이스의 DBID를 복제된 데이터베이스에 할당하려면 이 확인란의 선택을 취소합니다. 이 시나리오에서는 소스 데이터베이스가 이미 등록된 외부 RMAN 카탈로그에 클론 생성된 데이터베이스를 등록하려는 경우 작업이 실패합니다.
임시 테이블스페이스에 대한 tempfile을 생성합니다	클론된 데이터베이스의 기본 임시 테이블스페이스에 대한 tempfile을 생성하려면 이 확인란을 선택합니다. 이 확인란을 선택하지 않으면 tempfile 없이 데이터베이스 클론이 생성됩니다.
클론이 생성될 때 적용할 SQL 항목을 입력합니다	클론이 생성될 때 적용할 SQL 항목을 추가합니다.
클론 작업 후 실행할 스크립트를 입력합니다	클론 작업 후에 실행할 PostScript의 경로와 인수를 지정합니다. PostScript는 */var/opt/snapcenter/SPL/scripts* 또는 이 경로 내의 모든 폴더에 저장해야 합니다. 기본적으로 _/var/opt/snapcenter/SPL/scripts_path가 채워집니다. 이 경로 내의 폴더에 스크립트를 배치한 경우 스크립트가 있는 폴더까지 전체 경로를 제공해야 합니다. ⓘ 클론 작업이 실패하면 사후 스크립트가 실행되지 않고 정리 작업이 직접 트리거됩니다.

11. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

    또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 수행된 클론 작업의 보고서를 첨부하려면 * 작업 보고서 연결 * 을 선택합니다.

    ⓘ 이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmtpServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

1. 요약을 검토하고 * Finish * 를 클릭합니다.

클론 생성 작업의 일부로 복구를 수행하는 동안 복구에 실패하더라도 클론이 경고와 함께 생성됩니다. 이 클론에 대해 수동 복구를 수행하여 클론 데이터베이스를 정합성 보장 상태로 만들 수 있습니다.

2. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

결과 *

데이터베이스를 클론 생성한 후 리소스 페이지를 새로 고쳐 복제된 데이터베이스를 백업에 사용할 수 있는 리소스 중 하나로 나열할 수 있습니다. 클론 생성된 데이터베이스는 표준 백업 워크플로우를 사용하는 다른 데이터베이스와 마찬가지로 보호되거나 새로 생성되거나 기존 리소스 그룹에 포함될 수 있습니다. 클론 복제된 데이터베이스를 추가로 클론 복제할 수 있습니다(클론 복제).

클론 생성 후에는 복제된 데이터베이스의 이름을 변경해서는 안 됩니다.

클론 생성 중에 복구를 수행하지 않은 경우 부적절한 복구 때문에 복제된 데이터베이스의 백업이 실패할 수 있으며 수동 복구를 수행해야 할 수 있습니다. 아카이브 로그에 대해 채워진 기본 위치가 NetApp이 아닌 스토리지에 있거나 스토리지 시스템이 SnapCenter로 구성되지 않은 경우에도 로그 백업이 실패할 수 있습니다.

AIX 설정에서 lkdev 명령을 사용하여 잠그고 rendev 명령을 사용하여 클론 데이터베이스가 상주하는 디스크의 이름을 바꿀 수 있습니다.

디바이스 잠금 또는 이름 변경은 클론 삭제 작업에 영향을 주지 않습니다. SAN 장치에 구축된 AIX LVM 레이아웃의 경우 복제된 SAN 디바이스에 대해 디바이스 이름 바꾸기가 지원되지 않습니다.

- 자세한 정보 찾기 *
- "ORA-00308 오류 메시지와 함께 복구 또는 클론 생성이 실패합니다"
- "복제된 데이터베이스를 복구하지 못했습니다"
- "AIX 시스템의 백업, 복원 및 클론 작업에 대한 사용자 정의 가능한 매개 변수"

플러그형 데이터베이스의 클론 복제

PDB(Pluggable Database)를 동일한 호스트 또는 대체 호스트의 다른 또는 동일한 타겟 CDB에 복제할 수 있습니다. 복제된 PDB를 원하는 SCN 또는 날짜 및 시간으로 복구할 수도 있습니다.

- 시작하기 전에 *

플러그인을 비루트 사용자로 설치한 경우, prescpt 및 PostScript 디렉토리에 실행 권한을 수동으로 할당해야 합니다.

- 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. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 단일 인스턴스 유형(멀티 테넌트) 데이터베이스를 선택합니다.

   데이터베이스 토폴로지 페이지가 표시됩니다.

4. Manage Copies 보기에서 Local copies (primary), Mirror copies (secondary) 또는 Vault copies (secondary) 중에서 백업을 선택합니다.
5. 테이블에서 백업을 선택한 다음 * 를 클릭합니다  *.
6. 이름 페이지에서 다음 작업을 수행합니다.
   a. PDB 복제 * 를 선택합니다.
   b. 복제할 PDB를 지정합니다.

      PDB는 한 번에 하나만 복제할 수 있습니다.

   c. PDB 복제 이름을 지정합니다.
7. 위치 페이지에서 다음 작업을 수행합니다.

이 필드의 내용…	수행할 작업…
호스트 복제	기본적으로 소스 데이터베이스 호스트는 채워집니다. 대체 호스트에서 클론을 생성하려면 소스 데이터베이스 호스트의 버전과 Oracle 및 OS 버전이 동일한 호스트를 선택합니다.
타겟 CDB	복제된 PDB를 포함할 CDB를 선택합니다. 타겟 CDB가 실행되고 있는지 확인해야 합니다.
데이터베이스 상태	PDB를 읽기-쓰기 모드로 열려면 * Open the Cloned PDB in read-write mode * 확인란을 선택합니다.

데이터 파일 위치	기본적으로 데이터 파일 위치는 채워집니다. SAN 또는 NFS 파일 시스템에 대한 SnapCenter 기본 명명 규칙은 FileSystemNameofsourcedatabase_SCJOBID입니다. ASM 디스크 그룹에 대한 SnapCenter 기본 명명 규칙은 SC_HASHCODEofDISKGROUP_SCJOBID입니다. HASHCODEofDISKGROUP은 ASM 디스크 그룹마다 고유한 자동 생성 번호(2 ~ 10자리)입니다. ⓘ ASM 디스크 그룹 이름을 사용자 지정하는 경우 이름 길이가 Oracle에서 지원하는 최대 길이를 따르는지 확인합니다. 다른 경로를 지정하려면 클론 데이터베이스의 데이터 파일 마운트 지점 또는 ASM 디스크 그룹 이름을 입력해야 합니다.

Oracle 홈, 사용자 이름 및 그룹 세부 정보는 소스 데이터베이스에서 자동으로 채워집니다. 클론을 생성할 호스트의 Oracle 환경에 따라 값을 변경할 수 있습니다.

8. PreOps 페이지에서 다음 단계를 수행하십시오.

   a. 클론 작업 전에 실행할 처방전의 경로와 인수를 입력합니다.

      처방된 내용을 /var/opt/snapcenter/spl/scripts 또는 이 경로 내의 폴더에 저장해야 합니다. 기본적으로 /var/opt/snapcenter/SPL/scripts 경로가 채워집니다. 이 경로 내의 폴더에 스크립트를 배치한 경우 스크립트가 있는 폴더까지 전체 경로를 제공해야 합니다.

   SnapCenter에서는 처방과 PS를 실행할 때 미리 정의된 환경 변수를 사용할 수 있습니다. "자세한 정보"

   a. 보조 CDB 클론 데이터베이스 매개 변수 설정 섹션에서 데이터베이스를 초기화하는 데 사용되는 미리 채워진 데이터베이스 매개 변수의 값을 수정합니다.

9. 기본 데이터베이스 매개 변수 설정을 가져오려면 * Reset * (재설정 *)을 클릭합니다.
10. PostOps 페이지에서 * until Cancel * 이 기본적으로 선택되어 복제된 데이터베이스의 복구를 수행합니다.

    SnapCenter가 적절한 로그 백업을 찾지 못할 경우 * until Cancel * 옵션을 선택하지 않습니다. 로그 백업을 사용할 수 없는 경우 * 외부 아카이브 로그 위치 지정 * 에서 외부 아카이브 로그 위치를 제공할 수 있습니다. 여러 로그 위치를 지정할 수 있습니다.

    ⓘ FRA(Flash Recovery Area) 및 OMF(Oracle Managed Files)를 지원하도록 구성된 소스 데이터베이스를 복제하려는 경우 복구를 위한 로그 대상도 OMF 디렉토리 구조를 준수해야 합니다.

필드 이름입니다	설명
를 눌러 취소 로 이동합니다	SnapCenter는 클론 생성을 위해 선택한 데이터 백업 이후에 연속되지 않은 아카이브 로그가 있는 최신 로그 백업을 마운트하여 복구를 수행합니다. 운영 스토리지에서 클론을 수행하려면 로그 및 데이터 백업이 운영 스토리지에 있어야 하고 보조 스토리지에서 클론을 수행하려면 로그 및 데이터 백업이 보조 스토리지에 있어야 합니다. 로그 파일이 없거나 손상될 때까지 복제된 데이터베이스가 복구됩니다.
날짜 및 시간	SnapCenter는 데이터베이스를 지정된 날짜 및 시간까지 복구합니다. 시간은 24시간 형식으로 지정할 수 있습니다.
SCN(시스템 변경 번호)까지	SnapCenter는 데이터베이스를 지정된 SCN(시스템 변경 번호)까지 복구합니다.
외부 아카이브 로그 위치를 지정합니다	외부 아카이브 로그 위치를 지정합니다.
새 DBID를 생성합니다	기본적으로 * 보조 클론 데이터베이스에 대해 새 DBID * 생성 확인란이 선택되지 않습니다. 보조 클론 데이터베이스의 고유 번호(DBID)를 생성하여 원본 데이터베이스와 구별하려면 이 확인란을 선택합니다.
임시 테이블스페이스에 대한 tempfile을 생성합니다	클론된 데이터베이스의 기본 임시 테이블스페이스에 대한 tempfile을 생성하려면 이 확인란을 선택합니다. 이 확인란을 선택하지 않으면 tempfile 없이 데이터베이스 클론이 생성됩니다.
클론이 생성될 때 적용할 SQL 항목을 입력합니다	클론이 생성될 때 적용할 SQL 항목을 추가합니다.

필드 이름입니다	설명
클론 작업 후 실행할 스크립트를 입력합니다	클론 작업 후에 실행할 PostScript의 경로와 인수를 지정합니다. PostScript는 */var/opt/snapcenter/SPL/scripts* 또는 이 경로 내의 모든 폴더에 저장해야 합니다. 기본적으로 _/var/opt/snapcenter/SPL/scripts_path가 채워집니다. 이 경로 내의 폴더에 스크립트를 배치한 경우 스크립트가 있는 폴더까지 전체 경로를 제공해야 합니다. ⓘ 클론 작업이 실패하면 사후 스크립트가 실행되지 않고 정리 작업이 직접 트리거됩니다.

11. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

    또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 수행된 클론 작업의 보고서를 첨부하려면 * 작업 보고서 연결 * 을 선택합니다.

ⓘ 이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmtpServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

1. 요약을 검토하고 * Finish * 를 클릭합니다.
2. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

- 완료 후 *

복제된 PDB의 백업을 생성하려면 복제된 PDB만 백업할 수 없기 때문에 PDB가 복제되는 대상 CDB를 백업해야 합니다. 2차 관계를 사용하여 백업을 생성하려면 타겟 CDB에 대한 2차 관계를 생성해야 합니다.

RAC 설정에서 복제된 PDB의 스토리지는 PDB 클론이 수행된 노드에만 연결됩니다. RAC의 다른 노드에 있는 PDB가 마운트 상태입니다. 다른 노드에서 복제된 PDB에 액세스할 수 있도록 하려면 스토리지를 다른 노드에 수동으로 연결해야 합니다.

- 자세한 정보 찾기 *
- "ORA-00308 오류 메시지와 함께 복구 또는 클론 생성이 실패합니다"
- "AIX 시스템의 백업, 복원 및 클론 작업에 대한 사용자 정의 가능한 매개 변수"

UNIX 명령을 사용하여 Oracle 데이터베이스 백업의 클론을 생성합니다

클론 워크플로우에는 계획, 클론 작업 수행 및 작업 모니터링이 포함됩니다.

- 이 작업에 대한 정보 *

다음 명령을 실행하여 Oracle 데이터베이스 클론 사양 파일을 생성하고 클론 작업을 시작해야 합니다.

명령에 사용할 수 있는 매개 변수 및 해당 설명에 대한 정보는 get-Help_command_name_을 실행하여 얻을 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 명령 참조 가이드".

- 단계 *

1. 지정된 백업에서 Oracle 데이터베이스 클론 사양을 생성합니다.*New-SmOracleCloneSpecification*

   보조 데이터 보호 정책이 통합 미러 볼트이면 -IncludeSecondaryDetails만 지정합니다. SecondaryStorageType 을 지정할 필요가 없습니다.

   이 명령은 지정된 소스 데이터베이스 및 해당 백업에 대한 Oracle 데이터베이스 클론 사양 파일을 자동으로 생성합니다. 또한 생성할 클론 데이터베이스에 대해 생성된 지정 파일에 자동으로 생성된 값이 있도록 클론 데이터베이스 SID를 제공해야 합니다.

   클론 사양 파일은 _/var/opt/snapcenter/sSCO/clone_spec_에서 생성됩니다.

2. 클론 리소스 그룹 또는 기존 백업에서 클론 작업을 시작합니다. _ New - SmClone _

   이 명령은 클론 작업을 시작합니다. 또한 클론 작업을 위한 Oracle 클론 사양 파일 경로를 제공해야 합니다. 복구 옵션, 클론 작업을 수행할 호스트, 처방점, 사후 스크립트 및 기타 세부 정보를 지정할 수도 있습니다.

기본적으로 클론 데이터베이스의 아카이브 로그 대상 파일은 _$ORACLE_HOME/clone_SID_에 자동으로 채워집니다.

Oracle 데이터베이스 클론을 분할합니다

SnapCenter를 사용하여 상위 리소스에서 복제된 리소스를 분할할 수 있습니다. 분할되는 클론은 상위 리소스와 독립적입니다.

- 이 작업에 대한 정보 *
- 중간 클론에는 클론 분할 작업을 수행할 수 없습니다.

  예를 들어 데이터베이스 백업에서 clone1을 생성한 후 clone1의 백업을 생성한 다음 이 백업(clone2)을 클론 복제할 수 있습니다. clone2를 생성한 후에는 clone1이 중간 클론이며 clone1에서 클론 분할 작업을 수행할 수 없습니다. 그러나 clone2에서 클론 분할 작업을 수행할 수 있습니다.

  clone2를 분할한 후에는 clone1이 더 이상 중간 클론이 아니기 때문에 clone1에서 클론 분할 작업을 수행할 수 있습니다.

- 클론을 분할하면 클론의 백업 복사본이 삭제됩니다.
- 클론 분할 작업 제한에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 논리적 스토리지 관리 가이드".
- 스토리지 시스템의 볼륨 또는 애그리게이트는 온라인 상태인지 확인합니다.
- 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 을 클릭합니다  .

4. 분할할 클론의 예상 크기와 애그리게이트에서 사용할 수 있는 필수 공간을 검토한 다음 * 시작 * 을 클릭합니다.
5. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

   SMCore 서비스가 다시 시작되고 클론 분할 작업이 수행된 데이터베이스가 리소스 페이지에 클론으로 나열되면 클론 분할 작업이 응답하지 않습니다. 클론 분할 작업을 중지하려면 _Stop-SmJob_cmdlet을 실행한 다음 클론 분할 작업을 다시 시도해야 합니다.

   폴링 시간을 더 오래 설정하거나 폴링 시간을 짧게 하여 클론이 분할되었는지 여부를 확인하려면 SMCoreServiceHost.exe.config 파일에서 CloneSplitStatusCheckPollTime 매개 변수의 값을 변경하여 SMCore가 클론 분할 작업의 상태를 폴링할 시간 간격을 설정할 수 있습니다. 값은 밀리초이고 기본값은 5분입니다.

   예를 들면, 다음과 같습니다.

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

백업, 복원 또는 다른 클론 분할이 진행 중인 경우 클론 분할 시작 작업이 실패합니다. 실행 중인 작업이 완료된 후에만 클론 분할 작업을 다시 시작해야 합니다.

플러그형 데이터베이스의 클론 분할

SnapCenter를 사용하여 복제된 PDB(플러그형 데이터베이스)를 분할할 수 있습니다.

- 이 작업에 대한 정보 *

PDB가 복제되는 대상 CDB의 백업을 생성한 경우 PDB 클론을 분할하면 복제된 PDB가 복제된 PDB가 포함된 대상 CDB의 모든 백업에서도 제거됩니다.

PDB 클론은 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. Manage Copies 뷰에서 운영 또는 2차(미러링 또는 복제) 스토리지 시스템에서 * Clones * 를 선택합니다.
4. PDB 클론(targetCDB:PDBClone)을 선택한 다음 을 클릭합니다  .
5. 분할할 클론의 예상 크기와 애그리게이트에서 사용할 수 있는 필수 공간을 검토한 다음 * 시작 * 을 클릭합니다.
6. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

Oracle 데이터베이스 클론 작업을 모니터링합니다

작업 페이지를 사용하여 SnapCenter 클론 작업의 진행률을 모니터링할 수 있습니다. 작업 진행률을 확인하여 작업이 언제 완료되는지 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨
- 단계 *

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 모니터 * 페이지에서 * 작업 * 을 클릭합니다.
3. Jobs * 페이지에서 다음 단계를 수행하십시오.
   a. 을 클릭합니다 클론 작업만 나열되도록 목록을 필터링합니다.
   b. 시작 및 종료 날짜를 지정합니다.
   c. Type * 드롭다운 목록에서 * Clone * 을 선택합니다.
   d. Status * (상태 *) 드롭다운 목록에서 클론 상태를 선택합니다.
   e. 성공적으로 완료된 작업을 보려면 * 적용 * 을 클릭합니다.
4. 클론 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. 작업 세부 정보 페이지에서 * 로그 보기 * 를 클릭합니다.

클론을 새로 고칩니다

새로 고침 - SmClone_ 명령을 실행하여 클론을 새로 고칠 수 있습니다. 이 명령은 데이터베이스의 백업을 생성하고 기존 클론을 삭제한 다음 같은 이름의 클론을 생성합니다.

PDB 클론은 새로 고칠 수 없습니다.

- 필요한 것 *
- 예약된 백업을 사용하지 않고 온라인 전체 백업 또는 오프라인 데이터 백업 정책을 생성합니다.
- 정책에서 백업 장애에 대해서만 e-메일 알림을 구성합니다.
- 필요 시 백업의 보존 수를 적절하게 정의하여 원치 않는 백업이 없도록 합니다.
- 클론 새로 고침 작업을 위해 식별된 리소스 그룹에 온라인 전체 백업 또는 오프라인 데이터 백업 정책만 연결되어 있는지 확인합니다.
- 하나의 데이터베이스만 사용하여 리소스 그룹을 생성합니다.
- 클론 새로 고침 명령에 대해 cron 작업이 생성된 경우 SnapCenter 스케줄과 cron 일정이 데이터베이스 리소스 그룹에 대해 겹치지 않도록 해야 합니다.

  클론 새로 고침 명령에 대해 생성된 cron 작업의 경우 24시간마다 Open-SmConnection을 실행해야 합니다.

- 클론 SID가 호스트에 대해 고유한지 확인합니다.

  여러 번의 클론 새로 고침 작업에서 동일한 클론 사양 파일을 사용하거나 클론 SID가 동일한 클론 지정 파일을 사용하는 경우 호스트에서 SID가 있는 기존 클론이 삭제되고 클론이 생성됩니다.

- 보조 보호 기능을 사용하여 백업 정책을 설정하고 ""-IncludeSecondaryDetails""를 사용하여 클론 사양 파일을 만들어 보조 백업을 사용하여 클론을 생성해야 합니다.
  - 기본 클론 사양 파일이 지정되었지만 정책에 보조 업데이트 옵션이 선택된 경우 백업이 생성되고 업데이트가 보조 로 전송됩니다. 그러나 클론은 기본 백업에서 생성됩니다.
  - 기본 클론 사양 파일이 지정되고 정책에 보조 업데이트 옵션이 선택되지 않은 경우 백업이 운영 사이트에서 생성되고 운영 사이트에서 클론이 생성됩니다.

- 단계 *

  1. 지정된 사용자에 대해 SnapCenter 서버와 연결 세션을 시작합니다. _ Open - SmConnection _
  2. 지정된 백업에서 Oracle 데이터베이스 클론 사양을 생성합니다.*New-SmOracleCloneSpecification*

     보조 데이터 보호 정책이 통합 미러 볼트이면 -IncludeSecondaryDetails만 지정합니다. SecondaryStorageType 을 지정할 필요가 없습니다.

     이 명령은 지정된 소스 데이터베이스 및 해당 백업에 대한 Oracle 데이터베이스 클론 사양 파일을 자동으로 생성합니다. 또한 생성할 클론 데이터베이스에 대해 생성된 지정 파일에 자동으로 생성된 값이 있도록 클론 데이터베이스 SID를 제공해야 합니다.

     클론 사양 파일은 _/var/opt/snapcenter/sSCO/clone_spec_에서 생성됩니다.

  3. Run_Refresh-SmClone _ 을(를) 실행합니다.

     "PL-SCO-20032: canExecute 작업이 실패하고 다음 오류가 발생할 경우: PL-SCO-30031: Redo 로그 파일 + SC_2959770772_clmdb/clmdb/redolog/redo01_01.log exists" 오류 메시지가 나타나면 _-WaitToTriggerClone_에 대해 더 높은 값을 지정하십시오.

UNIX 명령에 대한 자세한 내용은 를 참조하십시오 "SnapCenter 소프트웨어 명령 참조 가이드".

플러그형 데이터베이스의 클론을 삭제합니다

더 이상 필요하지 않은 경우 플러그형 데이터베이스(PDB)의 클론을 삭제할 수 있습니다.

PDB가 복제되는 대상 CDB의 백업을 생성한 경우 PDB 클론을 삭제하면 복제된 PDB도 대상 CDB 백업에서 제거됩니다.

PDB 클론은 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. Manage Copies 뷰에서 운영 또는 2차(미러링 또는 복제) 스토리지 시스템에서 * Clones * 를 선택합니다.

4. PDB 클론(targetCDB:PDBClone)을 선택한 다음 을 클릭합니다 .
5. 확인 * 을 클릭합니다.

애플리케이션 볼륨 관리

애플리케이션 볼륨 추가

SnapCenter는 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 * Resources * 를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
  2. 응용 프로그램 볼륨 추가 * 를 클릭합니다.
  3. 이름 페이지에서 다음 작업을 수행합니다.
     - Name(이름) 필드에 애플리케이션 볼륨의 이름을 입력합니다.
     - 호스트 이름 필드에 호스트 이름을 입력합니다.
  4. Storage Footprint 페이지에서 스토리지 시스템 이름을 입력하고 하나 또는 볼륨을 선택한 다음 연결된 LUN 또는 qtree를 지정합니다.

     여러 스토리지 시스템을 추가할 수 있습니다.
  5. 요약을 검토하고 * Finish * 를 클릭합니다.
  6. 리소스 페이지의 * 보기 * 목록에서 * 응용 프로그램 볼륨 * 을 선택하여 추가한 모든 응용 프로그램 볼륨을 봅니다.

애플리케이션 볼륨을 수정합니다

백업이 생성되지 않은 경우 애플리케이션 볼륨을 추가하는 동안 지정한 모든 값을 수정할 수 있습니다. 백업이 생성된 경우 스토리지 시스템 세부 정보만 수정할 수 있습니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * Resources * 를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
  2. 리소스 페이지의 * 보기 * 목록에서 * 응용 프로그램 볼륨 * 을 선택합니다.
  3. 을 클릭합니다  를 눌러 값을 수정합니다.

응용 프로그램 볼륨을 삭제합니다

응용 프로그램 볼륨을 삭제할 때 응용 프로그램 볼륨과 연결된 백업이 있으면 응용 프로그램 볼륨은 유지 관리 모드로 전환되고 새 백업이 생성되지 않으며 이전 백업은 보존되지 않습니다. 연결된 백업이 없으면 모든 메타데이터가 삭제됩니다.

필요한 경우 SnapCenter를 사용하여 삭제 작업을 실행 취소할 수 있습니다.

- 단계 *

1. 왼쪽 탐색 창에서 * Resources * 를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 응용 프로그램 볼륨 * 을 선택합니다.
3. 을 클릭합니다 를 눌러 값을 수정합니다.

애플리케이션 볼륨 백업

애플리케이션 볼륨을 백업합니다

애플리케이션 볼륨이 리소스 그룹에 속하지 않은 경우 리소스 페이지에서 애플리케이션 볼륨을 백업할 수 있습니다.

- 이 작업에 대한 정보 *

기본적으로 일관성 그룹(CG) 백업이 생성됩니다. 볼륨 기반 백업을 생성하려면 _web.config_file에서 * EnableOracleNdvVolumeBasedBackup * 의 값을 true 로 설정해야 합니다.

- 단계 *

1. 왼쪽 탐색 창에서 * Resources * 를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 응용 프로그램 볼륨 * 을 선택합니다.
3. 를 클릭합니다를 누른 다음 호스트 이름과 데이터베이스 유형을 선택하여 리소스를 필터링합니다.

   그런 다음 * 를 클릭할 수 있습니다를 눌러 필터 창을 닫습니다.

4. 백업할 애플리케이션 볼륨을 선택합니다.

   Application volume-protect(애플리케이션 볼륨 보호) 페이지가 표시됩니다.

5. 리소스 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
스냅샷 복사본에 대해 사용자 지정 이름 형식을 사용합니다	이 확인란을 선택한 다음 스냅샷 복사본 이름에 사용할 사용자 지정 이름 형식을 입력합니다. 예를 들어 customtext__policy_hostname 또는 resource_hostname을 입력합니다. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.
백업에서 아카이브 로그 대상을 제외합니다	백업하지 않을 아카이브 로그 파일의 대상을 지정합니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

   a. 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

* 를 클릭하여 정책을 생성할 수도 있습니다 + *.

선택한 정책에 대한 스케줄 구성 섹션에 선택한 정책이 나열됩니다.

b. 을 클릭합니다 + 스케줄을 구성할 정책에 대한 Configure Schedules 열에서

c. policy_policy_name_에 대한 스케줄 추가 창에서 스케줄을 구성한 다음 * 확인 * 을 클릭합니다.

_policy_name_은 선택한 정책의 이름입니다.

구성된 일정이 Applied Schedules 열에 나열됩니다.

7. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 리소스에 수행된 백업 작업의 보고서를 첨부하려면 * 작업 보고서 첨부 * 를 선택합니다.

이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmtpServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

1. 요약을 검토하고 * Finish * 를 클릭합니다.

애플리케이션 볼륨 토폴로지 페이지가 표시됩니다.

2. 지금 백업 * 을 클릭합니다.
3. 백업 페이지에서 다음 단계를 수행하십시오.
   a. 리소스에 여러 정책을 적용한 경우 * 정책 * 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.
   b. 백업 * 을 클릭합니다.
4. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

애플리케이션 볼륨 리소스 그룹을 백업합니다

애플리케이션 볼륨만 포함하거나 애플리케이션 볼륨과 데이터베이스를 혼합하여 포함하는 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 대한 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다.

리소스 그룹에 여러 애플리케이션 볼륨이 있는 경우 모든 애플리케이션 볼륨에 SnapMirror 또는 SnapVault 복제 정책이 있어야 합니다.

- 이 작업에 대한 정보 *

기본적으로 일관성 그룹(CG) 백업이 생성됩니다. 볼륨 기반 백업을 생성하려면 _web.config_file에서 * EnableOracleNdvVolumeBasedBackup * 의 값을 true 로 설정해야 합니다.

- 단계 *

1. 왼쪽 탐색 창에서 * Resources * 를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.

2. 리소스 페이지의 * 보기 * 목록에서 * 리소스 그룹 * 을 선택합니다.

   검색 상자에 리소스 그룹 이름을 입력하거나 * 를 클릭하여 리소스 그룹을 검색할 수 있습니다  를 누른 다음 태그를 선택합니다. 그런 다음 * 를 클릭할 수 있습니다  를 눌러 필터 창을 닫습니다.

3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음 * 지금 백업 * 을 클릭합니다.
4. 백업 페이지에서 다음 단계를 수행하십시오.
   a. 여러 정책을 리소스 그룹에 연결한 경우 * Policy * 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

      필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

   b. 백업 * 을 클릭합니다.
5. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

   검증 작업은 애플리케이션 볼륨이 아닌 데이터베이스에 대해서만 수행됩니다.

클론 애플리케이션 볼륨 백업

SnapCenter를 사용하여 애플리케이션 볼륨 백업을 복제할 수 있습니다.

- 시작하기 전에 *

플러그인을 비루트 사용자로 설치한 경우, prescpt 및 PostScript 디렉토리에 실행 권한을 수동으로 할당해야 합니다.

- 단계 *

1. 왼쪽 탐색 창에서 * Resources * 를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 응용 프로그램 볼륨 * 을 선택합니다.
3. 애플리케이션 볼륨 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 애플리케이션 볼륨을 선택합니다.

   애플리케이션 볼륨 토폴로지 페이지가 표시됩니다.

4. Manage Copies 보기에서 Local copies (primary), Mirror copies (secondary) 또는 Vault copies (secondary) 중에서 백업을 선택합니다.
5. 테이블에서 백업을 선택한 다음 * 를 클릭합니다  *.
6. 위치 페이지에서 다음 작업을 수행합니다.

이 필드의 내용…	수행할 작업…
플러그인 호스트입니다	클론을 생성할 호스트를 선택합니다.
대상 리소스 이름입니다	자원 이름을 지정합니다.

7. 스크립트 페이지에서 클론 생성 전에 실행할 스크립트의 이름, 파일 시스템을 마운트하는 명령 및 클론 생성 후 실행할 스크립트의 이름을 지정합니다.

8. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 수행된 클론 작업의 보고서를 첨부하려면 * 작업 보고서 연결 * 을 선택합니다.

   이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmtpServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

1. 요약을 검토하고 * Finish * 를 클릭합니다.

애플리케이션 볼륨 클론을 분할합니다

SnapCenter를 사용하여 상위 리소스에서 복제된 리소스를 분할할 수 있습니다. 분할되는 클론은 상위 리소스와 독립적입니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * Resources * 를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
  2. 리소스 페이지의 * 보기 * 목록에서 * 응용 프로그램 볼륨 * 을 선택합니다.
  3. 클론 생성된 리소스를 선택하고 을 클릭합니다  .
  4. 분할할 클론의 예상 크기와 애그리게이트에서 사용할 수 있는 필수 공간을 검토한 다음 * 시작 * 을 클릭합니다.
  5. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

애플리케이션 볼륨 클론을 삭제합니다

더 이상 필요하지 않은 클론은 삭제할 수 있습니다. 다른 클론의 소스와 같은 역할을 하는 클론은 삭제할 수 없습니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * Resources * 를 클릭한 다음 목록에서 Oracle Database 플러그인을 선택합니다.
  2. 리소스 페이지의 * 보기 * 목록에서 * 응용 프로그램 볼륨 * 을 선택합니다.
  3. 목록에서 리소스 또는 리소스 그룹을 선택합니다.

     리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

  4. Manage Copies 뷰에서 운영 또는 2차(미러링 또는 복제) 스토리지 시스템에서 * Clones * 를 선택합니다.
  5. 클론을 선택한 다음 을 클릭합니다  .
  6. 클론 삭제 페이지에서 다음 작업을 수행합니다.
     a. Pre clone delete * 필드에 클론을 삭제하기 전에 실행할 스크립트의 이름을 입력합니다.
     b. 클론을 삭제하기 전에 * Unmount * 필드에 클론을 마운트 해제하는 명령을 입력합니다.
  7. 확인 * 을 클릭합니다.

Windows 파일 시스템 보호

Microsoft Windows용 SnapCenter 플러그인 개념

Microsoft Windows용 SnapCenter 플러그인 개요

Microsoft Windows용 SnapCenter 플러그인은 Microsoft 파일 시스템 리소스에 대한 애플리케이션 인식 데이터 보호 관리를 지원하는 NetApp SnapCenter 소프트웨어의 호스트 측 구성 요소입니다. 또한 Windows 파일 시스템에 스토리지 프로비저닝, 스냅샷 복사본 정합성 보장 및 공간 재확보 기능을 제공합니다. Windows용 플러그인은 SnapCenter 환경에서 파일 시스템 백업, 복원 및 클론 복제 작업을 자동화합니다.

Windows용 플러그인을 설치하면 SnapCenter와 NetApp SnapMirror 기술을 함께 사용하여 다른 볼륨에 백업 세트의 미러링 복사본을 만들고 NetApp SnapVault 기술을 사용하여 아카이브 또는 표준 준수를 위한 D2D 백업 복제를 수행할 수 있습니다.

Microsoft Windows용 SnapCenter 플러그인으로 수행할 수 있는 작업

사용자 환경에 Windows용 플러그인이 설치되어 있는 경우 SnapCenter를 사용하여 Windows 파일 시스템을 백업, 복원 및 클론 복제할 수 있습니다. 이러한 작업을 지원하는 작업을 수행할 수도 있습니다.

- 리소스를 검색합니다
- Windows 파일 시스템을 백업합니다
- 백업 작업을 예약합니다
- 파일 시스템 백업을 복구합니다
- 클론 파일 시스템 백업
- 백업, 복원 및 클론 작업을 모니터링합니다

Windows용 플러그인은 SMB 공유에서 파일 시스템의 백업 및 복원을 지원하지 않습니다.

Windows용 SnapCenter 플러그인 기능

Windows용 플러그인은 스토리지 시스템의 NetApp Snapshot 복사본 기술과 통합됩니다. Windows용 플러그인으로 작업하려면 SnapCenter 인터페이스를 사용합니다.

Windows용 플러그인에는 다음과 같은 주요 기능이 포함되어 있습니다.

- * SnapCenter * 기반 통합 그래픽 사용자 인터페이스

  SnapCenter 인터페이스는 전체 플러그인과 환경에 걸쳐 표준화와 일관성을 제공합니다. SnapCenter 인터페이스를 사용하면 플러그인 전체에 걸쳐 일관된 백업 및 복원 프로세스를 완료하고, 중앙 집중식 보고, 대시보드 뷰 사용량을 한 눈에 확인 하고, RBAC(역할 기반 액세스 제어)를 설정하고, 모든 플러그인에 걸쳐 작업을 모니터링할 수 있습니다. 또한 SnapCenter는 중앙 집중식 스케줄링 및 정책 관리 기능을 제공하여 백업 및 클론 작업을 지원합니다.

- * 자동화된 중앙 관리 *

  일상적인 파일 시스템 백업을 예약하고, 정책 기반 백업 보존을 구성하고, 복구 작업을 설정할 수 있습니다. 또한 e-메일 알림을 보내도록 SnapCenter를 구성하여 파일 시스템 환경을 사전 예방적으로 모니터링할 수도 있습니다.

- * 무중단 NetApp 스냅샷 복사본 기술 *

  Windows용 플러그인에서는 NetApp Snapshot 복사본 기술을 사용합니다. 따라서 몇 초 내에 파일 시스템을 백업하고 호스트를 오프라인으로 전환하지 않고도 신속하게 복구할 수 있습니다. 스냅샷 복사본은 최소 스토리지 공간을 사용합니다.

이러한 주요 기능 외에도 Windows용 플러그인은 다음과 같은 이점을 제공합니다.

- 백업, 복원 및 클론 워크플로우 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임
- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 공간 효율적인 운영 파일 시스템 복사본 생성

  FlexClone 라이센스에 대한 자세한 내용은 을 참조하십시오 "SnapCenter 라이센스".

- 여러 서버에서 동시에 여러 백업을 실행할 수 있습니다
- 백업, 복원 및 클론 작업의 스크립팅을 위한 PowerShell cmdlet
- 파일 시스템 및 가상 시스템 디스크(VMDK)의 백업 지원
- 물리적 인프라와 가상화 인프라 지원
- iSCSI, Fibre Channel, FCoE, RDM(Raw Device Mapping), ALM(Asymmetric LUN Mapping), NFS 및 VMFS를 통한 VMDK 및 가상 FC 지원

SnapCenter가 Windows 파일 시스템을 백업하는 방법

SnapCenter는 스냅샷 복제 기술을 사용하여 LUN, CSV(클러스터 공유 볼륨), RDM(원시 디바이스 매핑) 볼륨, Windows 클러스터의 ALM(비대칭 LUN 매핑) 및 VMFS/NFS(NFS를 사용하는 VMware 가상 머신 파일 시스템)에 기반한 VMDK에 상주하는 Windows 파일 시스템 리소스를 백업합니다.

SnapCenter는 파일 시스템의 스냅샷 복사본을 생성하여 백업을 생성합니다. 볼륨이 여러 호스트의 LUN을 포함하는 통합 백업은 각 파일 시스템의 개별 스냅샷과 비교하여 하나의 볼륨 스냅샷 복사본만 생성되므로 각 개별 LUN의 백업보다 더 빠르고 효율적입니다.

SnapCenter에서 스냅샷 복사본을 생성하면 전체 스토리지 시스템 볼륨이 스냅샷 복사본에 캡처됩니다. 그러나 백업은 백업이 생성된 호스트 서버에만 유효합니다.

다른 호스트 서버의 데이터가 동일한 볼륨에 상주하는 경우 스냅샷 복사본에서 이 데이터를 복원할 수 없습니다.

Windows 파일 시스템에 데이터베이스가 포함된 경우 파일 시스템 백업은 데이터베이스 백업과 동일하지 않습니다. 데이터베이스를 백업하려면 데이터베이스 플러그인 중 하나를 사용해야 합니다.

Microsoft Windows용 SnapCenter 플러그인에서 지원하는 스토리지 유형입니다

SnapCenter는 물리적 시스템과 가상 머신 모두에서 다양한 스토리지 유형을 지원합니다. 호스트에 대한 패키지를 설치하기 전에 스토리지 유형에 대한 지원이 가능한지 확인해야 합니다.

SnapCenter 프로비저닝 및 데이터 보호 지원은 Windows Server에서 제공됩니다. 지원되는 버전에 대한 최신 정보는 를 참조하십시오
"NetApp 상호 운용성 매트릭스 툴".

기계	스토리지 유형입니다	를 사용하여 프로비저닝	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	스토리지 가상 시스템(SVM)에 상주하는 SMB3(CIFS) 공유	SnapCenter GUI 또는 PowerShell cmdlet	프로비저닝만 지원합니다. SnapCenter를 사용하여 SMB 프로토콜을 사용하는 데이터 또는 공유를 백업할 수 없습니다.
VMware VM	FC 또는 iSCSI HBA를 통해 연결된 RDM LUN	PowerShell cmdlet	
VMware VM	iSCSI 이니시에이터가 게스트 시스템에 직접 접속된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	
VMware VM	VMFS(Virtual Machine File Systems) 또는 NFS 데이터 저장소	VMware vSphere를 참조하십시오	
VMware VM	SVM에 상주하는 SMB3 공유에 연결된 게스트 시스템입니다	SnapCenter GUI 또는 PowerShell cmdlet	프로비저닝만 지원합니다. SnapCenter를 사용하여 SMB 프로토콜을 사용하는 데이터 또는 공유를 백업할 수 없습니다.

기계	스토리지 유형입니다	를 사용하여 프로비저닝	지원 노트
Hyper-V VM	가상 Fibre Channel 스위치를 통해 연결된 VFC(가상 FC) LUN입니다	SnapCenter GUI 또는 PowerShell cmdlet	Hyper-V Manager를 사용하여 가상 Fibre Channel 스위치로 연결된 VFC(가상 FC) LUN을 프로비저닝해야 합니다. NetApp 스토리지에 프로비저닝된 Hyper-V는 디스크를 통과하고 VHD(x)에서 데이터베이스를 백업하는 것은 지원되지 않습니다.
Hyper-V VM	iSCSI 이니시에이터가 게스트 시스템에 직접 접속된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	NetApp 스토리지에 프로비저닝된 Hyper-V는 디스크를 통과하고 VHD(x)에서 데이터베이스를 백업하는 것은 지원되지 않습니다.

기계	스토리지 유형입니다	를 사용하여 프로비저닝	지원 노트
Hyper-V VM	SVM에 상주하는 SMB3 공유에 연결된 게스트 시스템입니다	SnapCenter GUI 또는 PowerShell cmdlet	프로비저닝만 지원합니다. SnapCenter를 사용하여 SMB 프로토콜을 사용하는 데이터 또는 공유를 백업할 수 없습니다. NetApp 스토리지에 프로비저닝된 Hyper-V는 디스크를 통과하고 VHD(x)에서 데이터베이스를 백업하는 것은 지원되지 않습니다.

Windows 플러그인에 필요한 최소 ONTAP 권한

필요한 최소 ONTAP 권한은 데이터 보호를 위해 사용 중인 SnapCenter 플러그인에 따라 다릅니다.

- All-access 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
  - event generate-autosupport-log입니다
  - 작업 기록이 표시됩니다
  - 작업 중지
  - LUN을 클릭합니다
  - LUN 생성
  - LUN을 삭제합니다
  - LUN igroup 추가
  - LUN igroup 작성
  - LUN igroup 삭제
  - LUN igroup의 이름을 바꿉니다
  - LUN igroup 표시
  - LUN 매핑 add-reporting-nodes입니다
  - LUN 매핑 생성

- LUN 매핑을 삭제합니다
- LUN 매핑으로 remove-reporting-nodes를 사용할 수 있습니다
- LUN 매핑이 표시됩니다
- LUN 수정
- LUN 이동 - 볼륨
- LUN이 오프라인 상태입니다
- LUN을 온라인 상태로 전환합니다
- LUN 크기 조정
- LUN 일련 번호입니다
- LUN 표시
- SnapMirror 정책 추가 규칙
- SnapMirror 정책 modify-rule을 참조하십시오
- SnapMirror 정책 remove-rule을 참조하십시오
- SnapMirror 정책 쇼
- SnapMirror 복원
- SnapMirror 쇼
- SnapMirror 기록
- SnapMirror 업데이트
- SnapMirror 업데이트 - ls -set
- SnapMirror 목록 - 대상
- 버전
- 볼륨 클론 생성
- 볼륨 클론 표시
- 볼륨 클론 분할 시작이 있습니다
- 볼륨 클론 분할 중지
- 볼륨 생성
- 볼륨 제거
- 볼륨 파일 클론 생성
- 볼륨 파일 show-disk-usage 를 참조하십시오
- 볼륨이 오프라인 상태입니다
- 볼륨을 온라인으로 설정합니다
- 볼륨 수정
- 볼륨 qtree 생성
- 볼륨 qtree 삭제

- 볼륨 qtree 수정
- 볼륨 qtree 표시
- 볼륨 제한
- 볼륨 표시
- 볼륨 스냅샷 생성
- 볼륨 스냅숏 삭제
- 볼륨 스냅숏 수정
- 볼륨 스냅숏 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 - 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- SVM CIFS를 선택합니다
- SVM CIFS 공유 생성
- SVM CIFS 공유 삭제
- SVM CIFS shadowcopy show 를 참조하십시오
- SVM CIFS 공유 표시
- vserver cifs show 를 참조하십시오
- SVM 엑스포트 - 정책
- SVM 엑스포트 정책 생성
- SVM 엑스포트 정책 삭제
- SVM 엑스포트 정책 규칙 생성
- vserver export-policy rule show를 참조하십시오
- vserver export-policy show를 참조하십시오
- SVM iSCSI
- SVM iSCSI 연결이 표시됩니다
- vserver show 를 참조하십시오

- 읽기 전용 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
  - 네트워크 인터페이스
  - 네트워크 인터페이스가 표시됩니다
  - SVM

SnapMirror 및 **SnapVault** 복제를 위한 스토리지 시스템 준비

ONTAP 플러그인을 SnapCenter SnapMirror 기술과 함께 사용하여 다른 볼륨에 백업 세트의 미러링 복사본을 만들고 ONTAP SnapVault 기술을 사용하여 표준 준수 및 기타 거버넌스 관련

용도로 D2D 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 타겟 볼륨 간의 데이터 보호 관계를 구성하고 관계를 초기화해야 합니다.

SnapCenter는 스냅샷 복사본 작업이 완료된 후 SnapMirror 및 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행되고, 별도의 ONTAP 일정을 만들지 않습니다.

NetApp SnapManager 제품에서 SnapCenter으로 오고 있으며 구성한 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 운영 스토리지(소스 볼륨)의 데이터를 보조 스토리지(타겟 볼륨)에 복제합니다. 관계를 초기화할 때 ONTAP은 소스 볼륨에서 참조된 데이터 블록을 대상 볼륨으로 전송합니다.

SnapCenter는 SnapMirror와 SnapVault 볼륨(* Primary * > * Mirror * > * Vault *) 간의 계단식 관계를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter는 버전에 상관없이 유연한 SnapMirror 관계의 관리를 지원합니다. 버전에 상관없이 유연한 SnapMirror 관계와 설정 방법에 대한 자세한 내용은 를 참조하십시오 "ONTAP 설명서".

SnapCenter는 * SYNC_MIRROR * 복제를 지원하지 않습니다.

Windows 파일 시스템에 대한 백업 전략 정의

백업을 생성하기 전에 백업 전략을 정의하면 파일 시스템을 성공적으로 복원하거나 복제하는 데 필요한 백업을 얻을 수 있습니다. SLA(서비스 수준 계약), RTO(복구 시간 목표) 및 RPO(복구 시점 목표)에 따라 백업 전략이 주로 결정됩니다.

SLA는 예상되는 서비스 수준을 정의하고 서비스의 가용성 및 성능을 비롯한 다양한 서비스 관련 문제를 해결합니다. RTO는 서비스 중단 후 비즈니스 프로세스를 복원해야 하는 시간입니다. RPO는 장애 후 정상적인 작업을 재개하기 위해 백업 스토리지에서 복구해야 하는 파일의 사용 기간에 대한 전략을 정의합니다. SLA, RTO 및 RPO는 데이터 보호 전략에 기여합니다.

Windows 파일 시스템에 대한 백업 스케줄입니다

백업 빈도는 정책에 지정되며 백업 스케줄은 리소스 그룹 구성에 지정됩니다. 백업 빈도 또는 스케줄을 결정하는 가장 중요한 요소는 리소스의 변경 속도 및 데이터의 중요도입니다. 자주 사용하는 리소스를 매일 한 번씩 백업할 수도 있고, 자주 사용하지 않는 리소스를 하루에 한 번 백업할 수도 있습니다. 기타 요인으로는 조직에 대한 리소스의 중요성, SLA(서비스 수준 계약) 및 RPO(복구 시점 목표)가 있습니다.

SLA는 예상되는 서비스 수준을 정의하고 가용성 및 서비스 성능을 비롯한 다양한 서비스 관련 문제를 해결합니다. RPO는 장애 후 정상적인 작업을 재개하기 위해 백업 스토리지에서 복구해야 하는 파일의 사용 기간에 대한 전략을 정의합니다. SLA 및 RPO는 데이터 보호 전략에 기여합니다.

사용량이 많은 리소스의 경우에도 하루에 한 번 또는 두 번 이상 전체 백업을 실행할 필요가 없습니다.

백업 스케줄은 다음과 같이 두 부분으로 구성됩니다.

- 백업 빈도

  일부 플러그인에 대해 _schedule type_이라는 백업 빈도(백업 수행 빈도)는 정책 구성의 일부입니다. 예를 들어 백업 빈도를 매시간, 일별, 주별 또는 월별로 구성하거나, 해당 정책을 주문형 전용 정책으로 만드는 * 없음 * 을

지정할 수 있습니다. 설정 * > * 정책 * 을 클릭하여 정책에 액세스할 수 있습니다.

- 백업 스케줄

  백업 스케줄(백업을 수행할 정확한 시점)은 리소스 그룹 구성의 일부입니다. 예를 들어 주별 백업에 대한 정책이 구성된 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 스케줄을 구성할 수 있습니다. 리소스 그룹 * > * 리소스 그룹 * 을 클릭하여 리소스 그룹 일정에 액세스할 수 있습니다.

Windows 파일 시스템에 필요한 백업 수입니다

필요한 백업 수를 결정하는 요소에는 Windows 파일 시스템의 크기, 사용된 볼륨 수, 파일 시스템의 변경 속도 및 SLA(서비스 수준 계약)가 포함됩니다.

Windows 파일 시스템의 백업 명명 규칙

Windows 파일 시스템 백업에는 기본 스냅샷 복사본 명명 규칙이 사용됩니다. 기본 백업 명명 규칙은 스냅샷 복사본 이름에 타임 스탬프를 추가하여 복사본이 생성된 시간을 식별하도록 도와줍니다.

스냅샷 복사본은 resourcegroupname_hostname_timestamp라는 기본 명명 규칙을 사용합니다

다음 예제와 같이 백업 리소스 그룹의 이름을 논리적으로 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예제에서 구문 요소는 다음과 같은 의미를 가집니다.

- `dts1` 은(는) 리소스 그룹 이름입니다.
- `mach1x88` 호스트 이름입니다.
- `03-12-2016_23.17.26` 날짜 및 타임 스탬프입니다.

백업을 생성할 때 백업을 식별하는 데 도움이 되는 설명 태그를 추가할 수도 있습니다. 반면, 사용자 지정 백업 명명 규칙을 사용하려면 백업 작업이 완료된 후 백업 이름을 변경해야 합니다.

백업 보존 옵션

백업 복사본을 보존할 일 수를 선택하거나 유지할 백업 복사본 수를 최대 255개 사본의 ONTAP로 지정할 수 있습니다. 예를 들어, 조직에서 10일간 백업 복사본 또는 130개의 백업 복사본을 보존해야 할 수도 있습니다.

정책을 생성하는 동안 백업 유형 및 스케줄 유형에 대한 보존 옵션을 지정할 수 있습니다.

SnapMirror 복제를 설정하면 보존 정책이 대상 볼륨에 미러링됩니다.

SnapCenter는 스케줄 유형과 일치하는 보존 레이블이 있는 보존된 백업을 삭제합니다. 리소스 또는 리소스 그룹에 대한 스케줄 유형이 변경된 경우 이전 스케줄 유형 레이블이 있는 백업이 시스템에 남아 있을 수 있습니다.

백업 복사본을 장기간 보존하려면 SnapVault 백업을 사용해야 합니다.

Windows 파일 시스템의 클론 소스 및 대상

운영 스토리지 또는 보조 스토리지에서 파일 시스템 백업을 클론 복제할 수 있습니다. 또한 요구 사항을 지원하는 대상을 선택할 수도 있습니다. 즉, 원래 백업 위치나 동일한 호스트의 다른 대상 또는 다른 호스트의 대상이 될 수 있습니다. 대상은 클론 소스 백업과 동일한 볼륨에 있어야 합니다.

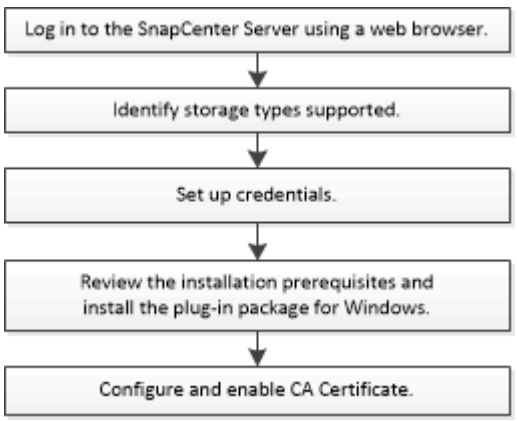
클론 대상	설명
원본, 원본, 위치	기본적으로 SnapCenter는 클론을 생성할 백업과 동일한 위치에 클론을 저장합니다.
위치가 다릅니다	동일한 호스트 또는 다른 호스트의 다른 위치에 클론을 저장할 수 있습니다. 호스트에 SVM(스토리지 가상 시스템)에 대한 연결이 구성되어 있어야 합니다.

클론 작업이 완료된 후 클론의 이름을 바꿀 수 있습니다.

Microsoft Windows용 SnapCenter 플러그인을 설치합니다

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 알고 있어야 합니다.

Windows용 플러그인을 사용하려면 먼저 SnapCenter 관리자가 SnapCenter 서버를 설치 및 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 사용자의 경우 호스트에서 UAC를 비활성화해야 합니다.
- 백업 복제를 원하면 SnapMirror 및 SnapVault를 설정해야 합니다.

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항 및 사이징 요구 사항을 숙지해야 합니다.

항목	요구 사항
운영 체제	Microsoft Windows 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	• Microsoft .NET Framework 4.7.2 이상 • WMF(Windows Management Framework) 4.0 이상 • PowerShell 4.0 이상 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴". NET 관련 문제 해결에 대한 자세한 내용은 을 참조하십시오 "인터넷에 연결되지 않은 기존 시스템의 경우 SnapCenter 업그레이드 또는 설치가 실패합니다."

Windows용 플러그인의 자격 증명을 설정합니다

SnapCenter는 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 비롯한 관리자 권한으로 자격 증명을 설정해야 합니다.
- 개별 리소스 그룹에 대한 자격 증명을 설정했고 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 실행합니다.

이 필드의 내용...	수행할 작업...
자격 증명 이름입니다	자격 증명의 이름을 입력합니다.
사용자 이름/암호	인증에 사용되는 사용자 이름과 암호를 입력합니다. • 도메인 관리자 또는 관리자 그룹의 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹의 구성원을 지정합니다. 사용자 이름 필드의 올바른 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 제공 로컬 관리자를 지정합니다. 사용자 계정에 상승된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 올바른 형식은 다음과 같습니다. `UserName` 암호에 큰따옴표(") 또는 백틱(')을 사용하지 마십시오. 보다 작음(<) 및 느낌표(!)를 사용해서는 안 됩니다. 암호를 사용한 기호. 예를 들어 LessThan <!10, Lessthan10 <!, backtick'12.
암호	인증에 사용되는 암호를 입력합니다.

  5. 확인 * 을 클릭합니다.

자격 증명 설정을 마친 후 사용자 및 액세스 페이지의 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

Windows Server 2012 이상에서 GMSA를 구성합니다

Windows Server 2012 이상을 사용하면 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 GMSA(Managed Service Account)를 만들 수 있습니다.

시작하기 전에

- Windows Server 2012 이상의 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2012 이상 호스트가 있어야 합니다.

단계

1. KDS 루트 키를 생성하여 GMSA의 각 개체에 대해 고유한 암호를 생성합니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 Add-KDSRootKey-EffectiveImmediately 명령을 실행합니다
3. GMSA 생성 및 구성:
   a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
 domainName\accountName$
.. 그룹에 컴퓨터 개체를 추가합니다.
.. 방금 생성한 사용자 그룹을 사용하여 GMSA를 생성합니다.
```

   예를 들면, 다음과 같습니다.

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. 실행 `Get-ADServiceAccount` 명령을 사용하여 서비스 계정을 확인합니다.
```

4. 호스트에서 GMSA를 구성합니다.
   a. GMSA 계정을 사용할 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.

      이렇게 하려면 PowerShell에서 다음 명령을 실행합니다.

```
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 확인합니다. `Test-AdServiceAccount <gMSA>`

5. 호스트에서 구성된 GMSA에 관리 권한을 할당합니다.
6. SnapCenter 서버에서 구성된 GMSA 계정을 지정하여 Windows 호스트를 추가합니다.

   SnapCenter 서버는 선택한 플러그인을 호스트에 설치하고 지정된 GMSA는 플러그인 설치 중에 서비스 로그온 계정으로 사용됩니다.

호스트를 추가하고 **Microsoft Windows**용 **SnapCenter** 플러그인을 설치합니다

SnapCenter 호스트 추가 페이지를 사용하여 Windows 호스트를 추가할 수 있습니다. Microsoft Windows용 SnapCenter 플러그인은 지정된 호스트에 자동으로 설치됩니다. 이는 플러그인을 설치하는 데 권장되는 방법입니다. 호스트를 추가하고 개별 호스트 또는 클러스터에 대한 플러그인을 설치할 수 있습니다.

시작하기 전에

- 플러그인 설치 및 제거 권한이 있는 역할(예: SnapCenter 관리자 역할)에 할당된 사용자여야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자의 경우 호스트에서 UAC를 비활성화해야 합니다.
- SnapCenter 사용자는 Windows 서버의 "서비스로 로그온" 역할에 추가해야 합니다.
- 메시지 큐 서비스가 실행 중인지 확인해야 합니다.
- 그룹 GMSA(Managed Service Account)를 사용하는 경우 관리자 권한으로 GMSA를 구성해야 합니다.

  "Windows Server 2012 이상에서 Windows 파일 시스템용 그룹 관리 서비스 계정을 구성합니다"

이 작업에 대해

- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.
- Windows 플러그인
  - Microsoft Windows
  - Microsoft Exchange Server를 참조하십시오
  - Microsoft SQL Server를 참조하십시오
  - SAP HANA를 참조하십시오
  - 맞춤형 플러그인
- 클러스터에 플러그인 설치

  클러스터(WSFC, Oracle RAC 또는 Exchange DAG)에 플러그인을 설치하면 클러스터의 모든 노드에 플러그인이 설치됩니다.

- E-Series 스토리지

  E-series 스토리지에 연결된 Windows 호스트에는 Windows용 플러그인을 설치할 수 없습니다.

호스트가 이미 작업 그룹에 속해 있고 다른 도메인으로 변경되었거나 그 반대로 변경된 경우 SnapCenter는 동일한 호스트(플러그인 호스트)를 SnapCenter에 추가할 수 없습니다. 동일한 호스트를 추가하려면 SnapCenter에서 호스트를 제거하고 다시 추가해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 맨 위에 * Managed Hosts * 가 선택되어 있는지 확인합니다.
3. 추가 * 를 클릭합니다.
4. 호스트 페이지에서 다음을 수행합니다.

이 필드의 내용...	수행할 작업...
호스트 유형	Windows * 호스트 유형을 선택합니다. SnapCenter 서버는 호스트를 추가한 다음 호스트에 아직 설치되지 않은 경우 Windows용 플러그인을 설치합니다.

이 필드의 내용...	수행할 작업...
호스트 이름입니다	FQDN(정규화된 도메인 이름) 또는 호스트의 IP 주소를 입력합니다. SnapCenter는 DNS의 올바른 구성에 따라 달라집니다. 따라서 가장 좋은 방법은 FQDN(정규화된 도메인 이름)을 입력하는 것입니다. 다음 중 하나의 IP 주소 또는 FQDN을 입력할 수 있습니다. • 독립 실행형 호스트 • WSFC(Windows Server Failover Clustering) SnapCenter를 사용하여 호스트를 추가하고 이 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.
자격 증명	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성합니다. 자격 증명에 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 만들기에 대한 정보를 참조하십시오. 사용자 이름, 도메인 및 호스트 유형을 비롯한 자격 증명에 대한 자세한 내용은 입력한 자격 증명 이름 위에 커서를 올려 놓으면 표시됩니다. 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 필드의 내용...	수행할 작업...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정합니다. 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 지정할 수 있습니다. Windows용 SnapCenter 플러그인 패키지의 경우 기본 경로는 C:\Program Files\NetApp\SnapCenter입니다. 그러나 원하는 경우 기본 경로를 사용자 지정할 수 있습니다.
클러스터의 모든 호스트를 추가합니다	WSFC에서 모든 클러스터 노드를 추가하려면 이 확인란을 선택합니다.
사전 설치 검사를 건너뜁니다	플러그인이 이미 수동으로 설치되어 있고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.
그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행합니다	그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행하려면 이 확인란을 선택합니다. GMSA 이름을 *domainName\accountName$* 형식으로 제공합니다. GMSA는 SnapCenter Plug-in for Windows 서비스에 대해서만 로그온 서비스 계정으로 사용됩니다.

7. 제출 * 을 클릭합니다.

Skip Prech사전 검사 * 확인란을 선택하지 않은 경우 호스트는 플러그인 설치 요구 사항을 충족하는지 여부를 확인합니다. 디스크 공간, RAM, PowerShell 버전, .NET 버전 및 위치는 최소 요구 사항에 따라 검증됩니다. 최소 요구 사항이 충족되지 않으면 적절한 오류 또는 경고 메시지가 표시됩니다.

오류가 디스크 공간 또는 RAM과 관련된 경우 에 있는 web.config 파일을 업데이트할 수 있습니다 `C:\Program Files\NetApp\SnapCenter` 기본값을 수정하려면 WebApp을 사용합니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.

HA 설정에서 web.config 파일을 업데이트하는 경우 두 노드에서 파일을 업데이트해야 합니다.

8. 설치 과정을 모니터링합니다.

PowerShell cmdlet을 사용하여 여러 원격 호스트에 Microsoft Windows용 SnapCenter 플러그인을 설치합니다

Microsoft Windows용 SnapCenter 플러그인을 한 번에 여러 호스트에 설치하려면 를 사용하십시오 `Install-SmHostPackage` PowerShell cmdlet.

플러그인을 설치할 각 호스트에 대한 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter에 로그인해야 합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 를 사용하여 세션을 설정합니다 `Open-SmConnection` cmdlet을 입력한 다음 자격 증명을 입력합니다.
3. 를 사용하여 독립 실행형 호스트 또는 클러스터를 SnapCenter에 추가합니다 `Add-SmHost` cmdlet 및 필수 매개 변수

   cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

4. 를 사용하여 여러 호스트에 플러그인을 설치합니다 `Install-SmHostPackage` cmdlet 및 필수 매개 변수

   를 사용할 수 있습니다 `-skipprecheck` 옵션을 선택할 수 있습니다. 플러그인을 수동으로 설치했고 호스트가 플러그인을 설치하는 데 필요한 요구 사항을 충족하는지 확인하지 않으려는 경우

명령줄에서 Microsoft Windows용 SnapCenter 플러그인을 자동으로 설치합니다

SnapCenter GUI에서 원격으로 플러그인을 설치할 수 없는 경우 Windows 호스트에 Microsoft Windows용 SnapCenter 플러그인을 로컬로 설치할 수 있습니다. Windows 명령줄에서 Microsoft Windows 설치 프로그램용 SnapCenter 플러그인을 자동 모드로 실행할 수 있습니다.

시작하기 전에

- Microsoft .Net 4.7.2 이상을 설치해야 합니다.
- PowerShell 4.0 이상을 설치해야 합니다.
- Windows 메시지 큐잉을 켜야 합니다.
- 호스트의 로컬 관리자여야 합니다.

단계

1. 설치 위치에서 Microsoft Windows용 SnapCenter 플러그인을 다운로드합니다.

   예를 들어 기본 설치 경로는 C:\ProgramData\NetApp\SnapCenter\Package Repository입니다.

   이 경로는 SnapCenter 서버가 설치된 호스트에서 액세스할 수 있습니다.

2. 플러그인을 설치할 호스트에 설치 파일을 복사합니다.
3. 명령 프롬프트에서 설치 파일을 다운로드한 디렉토리로 이동합니다.
4. 변수를 데이터로 대치하는 다음 명령을 입력합니다.

```
"snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
ISFeatureInstall=SCW
```

예를 들면 다음과 같습니다.

```
`"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 플러그인 설치 중에 전달되는 모든 매개 변수는 대/소문자를 구분합니다.

다음 변수의 값을 입력합니다.

변수	값
_ /debuglog "<Debug_Log_Path> _	Setup.exe /debuglog "C:\PathToLog\setupexe.log" 예제와 같이 제품군 설치 관리자 로그 파일의 이름과 위치를 지정합니다.
Bi_SNAPCENTER_PORT	SnapCenter가 SMCore와 통신하는 포트를 지정합니다.
Suite_INSTALLDIR	호스트 플러그인 패키지 설치 디렉토리를 지정합니다.
BI_서비스 계정	Microsoft Windows 웹 서비스 계정용 SnapCenter 플러그인을 지정합니다.
BI_세비셀	Microsoft Windows 웹 서비스 계정용 SnapCenter 플러그인 암호를 지정합니다.
ISFeatureInstall을 선택합니다	SnapCenter가 원격 호스트에 구축할 솔루션을 지정합니다.

_debuglog_parameter에는 SnapCenter에 대한 로그 파일의 경로가 포함됩니다. 이 로그 파일에 기록하는 것이 문제 해결 정보를 얻는 데 권장되는 방법입니다. 이 파일에는 설치 시 플러그인 사전 요구 사항에 대해 수행한 검사 결과가 포함되어 있기 때문입니다.

필요한 경우 Windows용 SnapCenter 패키지의 로그 파일에서 추가 문제 해결 정보를 찾을 수 있습니다. 패키지의

로그 파일은 *%Temp%* 폴더에 (가장 오래된 파일 먼저) 나열됩니다(예: *C:\temp*).

Windows용 플러그인을 설치하면 SnapCenter 서버가 아닌 호스트에 플러그인이 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록할 수 있습니다. 호스트가 추가되면 플러그인이 자동으로 검색됩니다.

SnapCenter 플러그인 패키지 설치 상태를 모니터링합니다

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행률을 모니터링할 수 있습니다. 설치 진행 상황을 확인하여 설치 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다

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 클릭합니다.
   b. 선택 사항: 시작 및 종료 날짜를 지정합니다.
   c. 유형 드롭다운 메뉴에서 * 플러그인 설치 * 를 선택합니다.
   d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
   e. 적용 * 을 클릭합니다.
4. 설치 작업을 선택하고 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. Job Details * 페이지에서 * View logs * 를 클릭합니다.

CA 인증서를 구성합니다

CA 인증서 CSR 파일을 생성합니다

CSR(인증서 서명 요청)을 생성하고 생성된 CSR을 사용하여 CA(인증 기관)에서 가져올 수 있는 인증서를 가져올 수 있습니다. 인증서에 연결된 개인 키가 있습니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.

CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 자세한 내용은 을 참조하십시오 "CA 인증서 CSR 파일을 생성하는 방법".

도메인(* .domain.company.com) 또는 시스템(machine1.domain.company.com CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter를 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN) 및 해당 호스트 이름을 CA 인증서에 언급해야 합니다. 인증서를 조달하기 전에 SAN(Subject Alternative Name) 필드를 채워 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(* .domain.company.com)의 경우 인증서에 도메인의 모든 호스트 이름이 암시적으로 포함됩니다.

CA 인증서를 가져옵니다

MMC(Microsoft Management Console)를 사용하여 CA 인증서를 SnapCenter 서버 및 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 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 단추로 클릭한 다음 * 모든 작업 * > * 가져오기 * 를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료합니다.

이 마법사 창에서...	다음을 수행합니다.
개인 키를 가져옵니다	예 * 옵션을 선택하고 개인 키를 가져온 다음 * 다음 * 을 클릭합니다.
파일 형식 가져오기	변경하지 않고 * 다음 * 을 클릭합니다.
보안	내보낸 인증서에 사용할 새 암호를 지정하고 * 다음 * 을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

인증서 가져오기는 개인 키와 함께 번들로 제공됩니다(지원되는 형식은 *.pfx, *.p12 및 *.p7b 입니다).

7. "개인" 폴더에 대해 5단계를 반복합니다.

CA 인증서 지문을 받습니다

인증서 thumbprint는 인증서를 식별하는 16진수 문자열입니다. 썸프린트는 썸프린트 알고리즘을 사용하여 인증서 컨텐츠에서 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.
   a. 인증서를 두 번 클릭합니다.
   b. 인증서 대화 상자에서 * 세부 정보 * 탭을 클릭합니다.
   c. 필드 목록을 스크롤하여 * Thumbprint * 를 클릭합니다.
   d. 상자에서 16진수 문자를 복사합니다.
   e. 16진수 사이의 공백을 제거합니다.

      예를 들어, 썸프린트가 "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 0d 42 77 A3 2a 7b"인 경우 공백을 제거한 후 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.
   a. 다음 명령을 실행하여 설치된 인증서의 엄지손가락 지문을 나열하고 최근 설치된 인증서를 주체 이름으로 식별합니다.

      Get-ChildItem-Path 인증:*LocalMachine\My*

   b. 엄지손가락 지문을 복사합니다.

Windows 호스트 플러그인 서비스를 사용하여 **CA** 인증서를 구성합니다

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스를 사용하여 CA 인증서를 구성해야 합니다.

SnapCenter 서버 및 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하여 기존 인증서 바인딩을 제거합니다.

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   예를 들면 다음과 같습니다.

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스와 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 들면 다음과 같습니다.

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

플러그인에 대해 **CA** 인증서를 활성화합니다

CA 인증서를 구성하고 SnapCenter 서버 및 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- run_Set-SmCertificateSettings_cmdlet을 사용하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- _get-SmCertificateSettings_를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 호스트 페이지에서 * 관리되는 호스트 * 를 클릭합니다.
3. 단일 또는 여러 플러그인 호스트를 선택합니다.
4. 추가 옵션 * 을 클릭합니다.
5. 인증서 유효성 검사 사용 * 을 선택합니다.

작업을 마친 후

관리 호스트 탭 호스트에는 자물쇠가 표시되고 자물쇠 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- 는 CA 인증서가 활성화되지 않았으며 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- CA 인증서의 유효성을 확인했음을 나타냅니다.
- CA 인증서의 유효성을 확인할 수 없음을 나타냅니다.
- 연결 정보를 검색할 수 없음을 나타냅니다.

> 상태가 노란색 또는 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

VMware vSphere용 SnapCenter 플러그인을 설치합니다

데이터베이스가 가상 머신(VM)에 저장되어 있거나 VM 및 데이터 저장소를 보호하려는 경우 SnapCenter Plug-in for VMware vSphere 가상 어플라이언스를 구축해야 합니다.

배포에 대한 자세한 내용은 을 참조하십시오 "구축 개요".

CA 인증서를 배포합니다

VMware vSphere용 SnapCenter 플러그인을 사용하여 CA 인증서를 구성하려면 를 참조하십시오 "SSL 인증서를 생성하거나 가져옵니다".

CRL 파일을 구성합니다

VMware vSphere용 SnapCenter 플러그인은 사전 구성된 디렉토리에서 CRL 파일을 찾습니다. VMware vSphere용 SnapCenter 플러그인의 기본 CRL 파일 디렉토리는 */opt/netapp/config/CRL* 입니다.

이 디렉터리에 둘 이상의 CRL 파일을 배치할 수 있습니다. 들어오는 인증서는 각 CRL에 대해 확인됩니다.

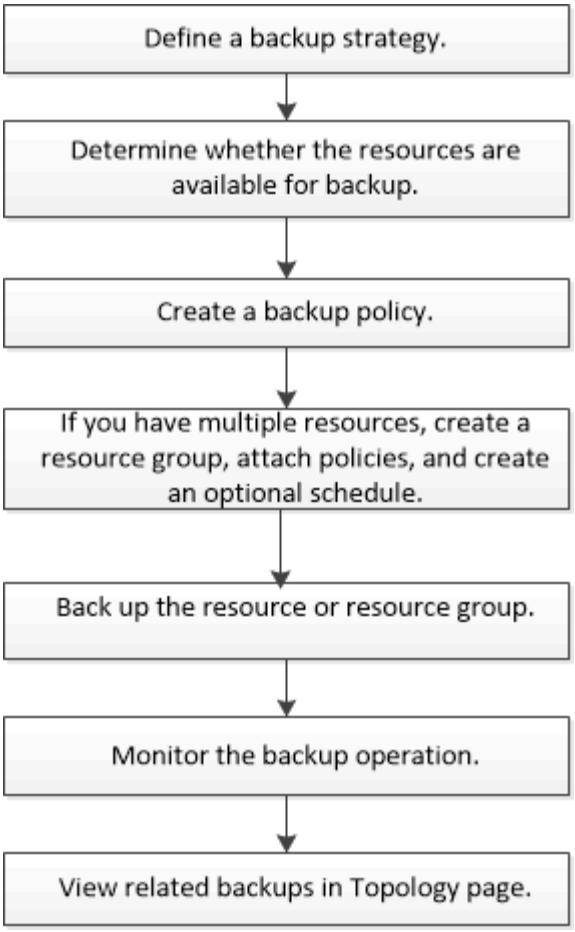
Windows 파일 시스템을 백업합니다

Windows 파일 시스템을 백업합니다

사용자 환경에 Microsoft Windows용 SnapCenter 플러그인을 설치하면 SnapCenter를 사용하여 Windows 파일 시스템을 백업할 수 있습니다. 단일 파일 시스템 또는 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 워크플로에서는 백업 작업을 수행해야 하는 순서를 보여 줍니다.



PowerShell cmdlet을 수동으로 사용하거나 스크립트에서 사용하여 백업, 복원 및 클론 작업을 수행할 수도 있습니다. SnapCenter cmdlet 도움말 또는 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드" PowerShell cmdlet에 대한 자세한 내용은 에 나와 있습니다.

Windows 파일 시스템에 대한 리소스 가용성을 확인합니다

리소스는 사용자가 설치한 플러그인에서 유지 관리하는 파일 시스템의 LUN 및 유사한 구성 요소입니다. 이러한 리소스를 리소스 그룹에 추가하여 여러 리소스에서 데이터 보호 작업을 수행할 수 있지만 먼저 사용 가능한 리소스를 확인해야 합니다. 사용 가능한 리소스를 검색해도 플러그인 설치가 성공적으로 완료되었는지 확인할 수 있습니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, SVM(스토리지 가상 시스템) 연결 생성, 자격 증명 추가 등과 같은 작업을 이미 완료해야 합니다.
- 파일이 VMware RDM LUN 또는 VMDK에 상주하는 경우 VMware vSphere용 SnapCenter 플러그인을 구축하고 SnapCenter에 플러그인을 등록해야 합니다. 자세한 내용은 을 참조하십시오 "VMware vSphere용 SnapCenter 플러그인 설명서".

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 목록에서 * 파일 시스템 * 을 선택합니다.
3. 리소스 목록을 필터링할 호스트를 선택한 다음 * 리소스 새로 고침 * 을 클릭합니다.

새로 추가, 이름 변경 또는 삭제된 파일 시스템이 SnapCenter 서버 인벤토리로 업데이트됩니다.

데이터베이스가 SnapCenter 외부에서 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

Windows 파일 시스템에 대한 백업 정책을 생성합니다

SnapCenter를 사용하여 Windows 파일 시스템을 백업하기 전에 리소스에 대한 새 백업 정책을 만들거나 리소스 그룹을 만들 때 또는 리소스를 백업할 때 새 백업 정책을 만들 수 있습니다.

시작하기 전에

- 백업 전략을 정의해야 합니다. "자세한 정보"
- 데이터 보호를 위한 준비가 되어 있어야 합니다.

  데이터 보호를 준비하려면 SnapCenter 설치, 호스트 추가, 리소스 검색, SVM(스토리지 가상 시스템) 연결 생성 등의 작업을 완료해야 합니다.

- 스냅샷 복사본을 미러 또는 소산 보조 스토리지에 복제하는 경우 SnapCenter 관리자는 소스 및 대상 볼륨 모두에 대해 SVM을 할당한 상태여야 합니다.
- powershellProcessforScripts 매개 변수의 값을 web.config 파일에서 true 로 설정하여 powerpare 및 postscripts 로 PowerShell 스크립트를 실행해야 합니다.

  기본값은 false 입니다

이 작업에 대해

- 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 swagger에서 API:API/4.7/configsettings를 통해 표시할 수 있습니다

  Get API를 사용하여 키 값을 표시할 수 있습니다. API 설정은 지원되지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
2. 설정 페이지에서 * 정책 * 을 클릭합니다.
3. 기존 정책을 사용할 수 있는지 확인하려면 정책 이름을 선택한 다음 * 세부 정보 * 를 클릭합니다.

   기존 정책을 검토한 후 다음 중 하나를 수행할 수 있습니다.

   - 기존 정책을 사용합니다.
   - 기존 정책을 복사하고 정책 구성을 수정합니다.
   - 새 정책을 생성합니다.
4. 새 정책을 만들려면 * New * 를 클릭합니다.

5. 이름 페이지에 정책 이름과 설명을 입력합니다.
6. 백업 옵션 페이지에서 다음 작업을 수행합니다.

   a. 백업 설정을 선택합니다.

옵션을 선택합니다	설명
파일 시스템 정합성 보장 백업	백업 작업이 시작되기 전에 SnapCenter가 파일 시스템이 상주하는 디스크 드라이브를 일시 중지한 다음 백업 작업이 종료된 후 디스크 드라이브를 다시 시작하도록 하려면 이 옵션을 선택합니다.
파일 시스템 충돌 - 정합성 보장 백업	SnapCenter가 파일 시스템이 상주하는 디스크 드라이브를 중지하지 않도록 하려면 이 옵션을 선택합니다.

   b. 스케줄 빈도(정책 유형이라고도 함)를 선택합니다.

   정책은 백업 빈도만 지정합니다. 백업에 대한 특정 보호 스케줄은 리소스 그룹에 정의됩니다. 따라서 둘 이상의 리소스 그룹이 동일한 정책 및 백업 빈도를 공유할 수 있지만 백업 스케줄은 다릅니다.

   오전 2시에 예약된 경우 DST(일광 절약 시간) 중에는 일정이 트리거되지 않습니다.

7. 보존 페이지에서 필요 시 백업 및 선택한 각 스케줄 빈도에 대한 보존 설정을 지정합니다.

옵션을 선택합니다	설명
유지할 총 스냅샷 복사본	SnapCenter에서 자동으로 삭제하기 전에 자동으로 저장되는 스냅샷 복사본의 수를 지정하려면 이 옵션을 선택합니다.
다음보다 오래된 스냅샷 복사본을 삭제합니다	SnapCenter에서 백업 복사본을 삭제하기 전에 보존할 일 수를 지정하려면 이 옵션을 선택합니다.

   보존 카운트를 2 이상으로 설정해야 합니다. 보존 카운트의 최소값은 2입니다.

   최대 보존 값은 ONTAP 9.4 이상의 리소스에 대해 1018이고, ONTAP 9.3 이전 버전의 리소스에 대해서는 254입니다. 보존이 기본 ONTAP 버전에서 지원하는 값보다 높은 값으로 설정된 경우 백업이 실패합니다.

8. 복제 페이지에서 보조 스토리지 시스템에 대한 복제를 지정합니다.

이 필드의 내용...	수행할 작업...
로컬 스냅샷 복사본을 생성한 후 SnapMirror를 업데이트합니다	다른 볼륨(SnapMirror)에 백업 세트의 미러 복사본을 생성하려면 이 옵션을 선택합니다.

이 필드의 내용...	수행할 작업...
스냅샷 복사본을 생성한 후 SnapVault를 업데이트합니다	디스크 간 백업 복제를 수행하려면 이 옵션을 선택합니다.
보조 정책 레이블입니다	스냅샷 레이블을 선택합니다. 선택한 스냅샷 복사본 레이블에 따라 ONTAP에서는 해당 레이블과 일치하는 2차 스냅샷 복사본 보존 정책을 적용합니다. 로컬 스냅샷 복사본 * 을 생성한 후 SnapMirror 업데이트 * 를 선택한 경우, 선택적으로 보조 정책 레이블을 지정할 수 있습니다. 그러나 로컬 스냅샷 복사본 * 을 생성한 후 * SnapVault 업데이트 * 를 선택한 경우에는 보조 정책 레이블을 지정해야 합니다.
오류 재시도 횟수입니다	프로세스가 중지되기 전에 수행해야 하는 복제 시도 횟수를 입력합니다.

보조 스토리지에 대한 ONTAP의 SnapMirror 보존 정책을 구성하면 보조 스토리지에서 스냅샷 복사본의 최대 제한에 도달하지 않도록 해야 합니다.

9. 스크립트 페이지에서 SnapCenter 서버가 백업 작업 전후에 실행할 처방인 경로 또는 PS를 각각 입력하고 SnapCenter가 스크립트가 시간 초과 전에 실행될 때까지 대기하는 시간 제한을 입력합니다.

   예를 들어 스크립트를 실행하여 SNMP 트랩을 업데이트하고, 경고를 자동화하고, 로그를 보낼 수 있습니다.

   처방자 또는 사후 스크립트 경로에는 드라이브 또는 공유가 포함되어서는 안 됩니다. 경로는 scripts_path에 상대해야 합니다.

10. 요약을 검토하고 * Finish * 를 클릭합니다.

Windows 파일 시스템에 대한 리소스 그룹을 생성합니다

리소스 그룹은 보호할 여러 파일 시스템을 추가할 수 있는 컨테이너입니다. 또한 수행할 데이터 보호 작업의 유형을 정의하려면 하나 이상의 정책을 리소스 그룹에 연결한 다음 백업 일정을 지정해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 목록에서 * 파일 시스템 * 을 선택합니다.

   최근에 SnapCenter에 파일 시스템을 추가한 경우 * 리소스 새로 고침 * 을 클릭하여 새로 추가된 리소스를 확인합니다.

3. 새 리소스 그룹 * 을 클릭합니다.
4. 마법사의 이름 페이지에서 다음을 수행합니다.

이 필드의 내용...	수행할 작업...
이름	자원 그룹 이름을 입력합니다. 리소스 그룹 이름은 250자를 초과할 수 없습니다.
스냅샷 복사본에 대해 사용자 지정 이름 형식을 사용합니다	선택 사항: 사용자 지정 스냅샷 복사본의 이름 및 형식을 입력합니다. 예를 들어 customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname을 입력합니다. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.
태그	리소스 그룹을 찾을 때 도움이 되는 설명 태그를 입력합니다.

5. 리소스 페이지에서 다음 작업을 수행합니다.
   a. 리소스 목록을 필터링할 호스트를 선택합니다.

      최근에 추가한 자원은 자원 목록을 새로 고친 후에만 사용 가능한 자원 목록에 나타납니다.

   b. 사용 가능한 리소스 섹션에서 백업할 파일 시스템을 클릭한 다음 오른쪽 화살표를 클릭하여 추가 섹션으로 이동합니다.

      동일한 스토리지 볼륨에서 모든 리소스 자동 선택 * 옵션을 선택하면 동일한 볼륨에 있는 모든 리소스가 선택됩니다. 추가된 섹션으로 이동하면 해당 볼륨의 모든 리소스가 함께 이동합니다.

   단일 파일 시스템을 추가하려면 * 동일한 스토리지 볼륨에서 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 선택합니다.

      기존 정책을 선택하고 * 세부 정보 * 를 클릭하여 해당 정책을 사용할 수 있는지 여부를 확인할 수 있습니다.

      기존 정책이 요구 사항을 충족하지 않는 경우 * 를 클릭하여 새 정책을 생성할 수 있습니다 + 를 눌러 정책 마법사를 시작합니다.

      선택한 정책이 선택한 정책에 대한 스케줄 구성 섹션의 정책 열에 나열됩니다.

   b. 선택한 정책에 대한 일정 구성 섹션에서 * 를 클릭합니다 + 일정을 구성하려는 정책에 대한 스케줄 구성 열의

c. 정책이 여러 일정 유형(빈도)과 연결된 경우 구성할 빈도를 선택합니다.

d. policy_policy_name_schedules 추가 대화 상자에서 시작 날짜, 만료 날짜 및 빈도를 지정하여 스케줄을 구성한 다음 * 마침 * 을 클릭합니다.

구성된 스케줄은 선택한 정책에 대한 스케줄 구성 섹션의 적용된 스케줄 열에 나열됩니다.

타사 백업 스케줄은 SnapCenter 백업 스케줄과 겹치는 경우 지원되지 않습니다. Windows 작업 스케줄러 및 SQL Server Agent에서 일정을 수정하면 안 됩니다.

7. 알림 페이지에서 다음과 같이 알림 정보를 제공합니다.

이 필드의 내용...	수행할 작업...
이메일 기본 설정	백업 리소스 그룹을 만들고 정책을 첨부하고 일정을 구성한 후 수신자에게 이메일을 보내려면 * Always *, * On Failure * 또는 * On failure 또는 Warning * 을 선택합니다. SMTP 서버, 기본 이메일 제목 줄, 받는 사람 및 보낸 사람 이메일 주소를 입력합니다.
보낸 사람	이메일 주소입니다
를 선택합니다	전자 메일 받는 사람 주소
제목	기본 이메일 제목줄

8. 요약을 검토하고 * Finish * 를 클릭합니다.

필요 시 백업을 수행하거나 예약된 백업이 발생할 때까지 기다릴 수 있습니다.

필요 시 **Windows** 파일 시스템에 대한 단일 리소스를 백업합니다

자원이 자원 그룹에 없으면 자원 페이지에서 필요에 따라 자원을 백업할 수 있습니다.

이 작업에 대해

2차 스토리지와 SnapMirror 관계가 있는 리소스를 백업하려면 스토리지 사용자에게 할당된 역할에 "'스냅샷 전체' 권한이 있어야 합니다. 그러나 "vsadmin" 역할을 사용하는 경우에는 "napmirror all" 권한이 필요하지 않습니다.

파일 시스템을 백업할 때 SnapCenter는 백업되는 파일 시스템의 볼륨 마운트 지점(VMP)에 마운트된 LUN을 백업하지 않습니다.

Windows 파일 시스템 컨텍스트에서 작업하는 경우 데이터베이스 파일을 백업하지 마십시오. 이렇게 하면 일관되지 않은 백업이 생성되고 복원할 때 데이터가 손실될 수 있습니다. 데이터베이스 파일을 보호하려면 데이터베이스에 적합한 SnapCenter 플러그인(예: Microsoft SQL Server용 SnapCenter 플러그인, Microsoft Exchange Server용 SnapCenter 플러그인 또는 데이터베이스 파일용 사용자 지정 플러그인)을 사용해야 합니다.

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 스냅샷 복사본에 대한 사용자 지정 이름 형식을 입력합니다.

   예를 들어 customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname을 입력합니다. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.

5. 정책 페이지에서 다음 작업을 수행합니다.

   a. 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

      기존 정책을 선택한 다음 * 세부 정보 * 를 클릭하여 해당 정책을 사용할 수 있는지 여부를 확인할 수 있습니다.

      기존 정책이 요구 사항을 충족하지 않는 경우 기존 정책을 복사하여 수정하거나 를 클릭하여 새 정책을 생성할 수 있습니다  를 클릭하여 정책 마법사를 시작합니다.

      선택한 정책이 선택한 정책에 대한 스케줄 구성 섹션의 정책 열에 나열됩니다.

   b. 선택한 정책에 대한 스케줄 구성 섹션에서 을 클릭합니다  스케줄을 구성할 정책에 대한 Configure Schedules 열에서

   c. policy_policy_name_schedules 추가 대화 상자에서 시작 날짜, 만료 날짜 및 빈도를 지정하여 스케줄을 구성한 다음 * 마침 * 을 클릭합니다.

      구성된 스케줄은 선택한 정책에 대한 스케줄 구성 섹션의 적용된 스케줄 열에 나열됩니다.

   "예약된 작업이 실패할 수 있습니다"

6. 알림 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
이메일 기본 설정	백업 리소스 그룹을 만들고 정책을 첨부하고 일정을 구성한 후 수신자에게 이메일을 보내려면 * Always *, * On Failure * 또는 * On failure 또는 Warning * 을 선택합니다. SMTP 서버 정보, 기본 이메일 제목 줄, ""받는 사람"" 및 " 보내는 사람" 이메일 주소를 입력합니다.
보낸 사람	이메일 주소입니다
를 선택합니다	전자 메일 받는 사람 주소
제목	기본 이메일 제목줄

7. 요약을 검토하고 * Finish * 를 클릭합니다.

   데이터베이스 토폴로지 페이지가 표시됩니다.

8. 지금 백업 * 을 클릭합니다.
9. 백업 페이지에서 다음 단계를 수행하십시오.
   a. 리소스에 여러 정책을 적용한 경우 정책 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

      필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

   b. 백업 * 을 클릭합니다.
10. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

Windows 파일 시스템에 대한 리소스 그룹을 백업합니다

리소스 그룹은 호스트 또는 클러스터의 리소스 모음입니다. 리소스 그룹에 대한 백업 작업은 리소스 그룹에 정의된 모든 리소스에 대해 수행됩니다. 리소스 페이지에서 필요 시 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 연결되어 있고 스케줄이 구성되어 있는 경우 스케줄에 따라 백업이 자동으로 수행됩니다.

시작하기 전에

- 정책이 연결된 리소스 그룹을 만들어야 합니다.
- 2차 스토리지와 SnapMirror 관계가 있는 리소스를 백업하려면 스토리지 사용자에게 할당된 역할에 "'스냅샷 전체' 권한이 있어야 합니다. 그러나 "vsadmin" 역할을 사용하는 경우에는 "napmirror all" 권한이 필요하지 않습니다.
- 리소스 그룹에 서로 다른 호스트의 데이터베이스가 여러 개 있는 경우 일부 호스트의 백업 작업이 네트워크 문제로 인해 늦게 트리거될 수 있습니다. Set-SmConfigSettings PowerShell cmdlet을 사용하여 web.config에서 MaxRetryForUninitializedHosts 의 값을 구성해야 합니다

> 파일 시스템을 백업할 때 SnapCenter는 백업되는 파일 시스템의 볼륨 마운트 지점(VMP)에 마운트된 LUN을 백업하지 않습니다.

> Windows 파일 시스템 컨텍스트에서 작업하는 경우 데이터베이스 파일을 백업하지 마십시오. 이렇게 하면 일관되지 않은 백업이 생성되고 복원할 때 데이터가 손실될 수 있습니다. 데이터베이스 파일을 보호하려면 데이터베이스에 적합한 SnapCenter 플러그인(예: Microsoft SQL Server용 SnapCenter 플러그인, Microsoft Exchange Server용 SnapCenter 플러그인 또는 데이터베이스 파일용 사용자 지정 플러그인)을 사용해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 리소스 그룹 * 을 선택합니다.

   검색 상자에 리소스 그룹 이름을 입력하거나 을 클릭하여 리소스 그룹을 검색할 수 있습니다 태그를 선택합니다. 그런 다음 을 클릭할 수 있습니다 를 눌러 필터 창을 닫습니다.

3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음 * 지금 백업 * 을 클릭합니다.

Oracle 데이터베이스용 SnapCenter 플러그인의 경우 데이터베이스 2개를 사용하는 통합 리소스 그룹이 있고 데이터베이스 중 하나가 타사 스토리지에서 데이터 파일을 사용하는 경우 다른 데이터베이스는 NetApp 스토리지에 있지만 백업 작업은 중단됩니다.

4. 백업 페이지에서 다음 단계를 수행하십시오.
   a. 여러 정책을 리소스 그룹에 연결한 경우 * Policy * 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

      필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

   b. 백업 * 을 클릭합니다.
5. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.
   - MetroCluster 구성에서 SnapCenter는 페일오버 후 보호 관계를 감지하지 못할 수 있습니다.

     "MetroCluster 페일오버 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다"

   - VMDK에서 애플리케이션 데이터를 백업하고 VMware vSphere용 SnapCenter 플러그인의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다. Java 힙 크기를 늘리려면 스크립트 파일을 찾습니다 `/opt/netapp/init_scripts/scvservice`. 이 스크립트에서 은 입니다 `do_start method` Command SnapCenter VMware 플러그인 서비스를 시작합니다. 다음 명령을 업데이트합니다. `Java -jar -Xmx8192M -Xms4096M`.

PowerShell cmdlet을 사용하여 스토리지 시스템 연결과 자격 증명을 생성합니다

PowerShell cmdlet을 사용하여 데이터 보호 작업을 수행하기 전에 SVM(Storage Virtual Machine) 연결과 자격 증명을 생성해야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행할 수 있도록 PowerShell 환경을 준비해야 합니다.
- 스토리지 접속을 생성하려면 인프라스트럭처 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

  호스트 캐시가 업데이트되지 않고 데이터베이스 상태가 SnapCenter GUI에 ""백업을 위해 사용할 수 없음"" 또는 ""NetApp 스토리지에 없음""으로 표시될 수 있으므로 스토리지 시스템 접속을 추가하는 동안 호스트 플러그인 설치가 진행되어서는 안 됩니다.

- 스토리지 시스템 이름은 고유해야 합니다.

  SnapCenter는 서로 다른 클러스터에서 동일한 이름의 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 연결 세션을 시작합니다.

   이 예제에서는 PowerShell 세션을 엽니다.

```
PS C:\> Open-SmConnection
```

2. Add-SmStorageConnection cmdlet을 사용하여 스토리지 시스템에 대한 새 접속을 생성합니다.

   이 예에서는 새 스토리지 시스템 접속을 생성합니다.

```
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 FinanceAdmin 이라는 새 자격 증명을 만듭니다.

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

PowerShell cmdlet을 사용하여 리소스를 백업합니다

PowerShell cmdlet을 사용하여 SQL Server 데이터베이스 또는 Windows 파일 시스템을 백업할 수 있습니다. 여기에는 SQL Server 데이터베이스 또는 Windows 파일 시스템 백업에는 SnapCenter Server와의 연결 설정, SQL Server 데이터베이스 인스턴스 또는 Windows 파일 시스템 검색, 정책 추가, 백업 리소스 그룹 생성, 백업 및 백업 확인이 포함됩니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 스토리지 시스템 접속을 추가하고 자격 증명을 생성해야 합니다.
- 호스트 및 검색된 리소스를 추가해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

   사용자 이름 및 암호 프롬프트가 표시됩니다.

2. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.

   이 예제에서는 SQL 백업 유형이 FullBackup인 새 백업 정책을 만듭니다.

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

이 예에서는 Windows 파일 시스템 백업 유형이 Crash일관성(crash일관성)인 새 백업 정책을 생성합니다.

```
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 시스템에 대한 리소스를 검색합니다.

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. 추가 SmResourceGroup cmdlet을 사용하여 SnapCenter에 새 리소스 그룹을 추가합니다.

   이 예제에서는 지정된 정책 및 리소스를 사용하여 새 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 예에서는 지정된 정책 및 리소스를 사용하여 새 Windows 파일 시스템 백업 리소스 그룹을 생성합니다.

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. New-SmBackup cmdlet을 사용하여 새 백업 작업을 시작합니다.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Get-SmBackupReport cmdlet을 사용하여 백업 작업의 상태를 봅니다.

   이 예는 지정된 날짜에 실행된 모든 작업의 작업 요약 보고서를 표시합니다.

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

백업 작업을 모니터링합니다

SnapCenterJobs 페이지를 사용하여 여러 백업 작업의 진행률을 모니터링할 수 있습니다. 진행 상황을 확인하여 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

다음 아이콘이 작업 페이지에 나타나고 작업의 해당 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨

단계

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 모니터 페이지에서 * 작업 * 을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행하십시오.
   a. 을 클릭합니다 백업 작업만 나열되도록 목록을 필터링합니다.
   b. 시작 및 종료 날짜를 지정합니다.
   c. Type * 드롭다운 목록에서 * Backup * 을 선택합니다.
   d. Status * (상태 *) 드롭다운에서 백업 상태를 선택합니다.
   e. 작업이 성공적으로 완료되었는지 보려면 * Apply * 를 클릭합니다.
4. 백업 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.

백업 작업 상태가 표시됩니다 작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 기호로 표시되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 * 로그 보기 * 를 클릭합니다.

   로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

Activity 창에서 작업을 모니터링합니다

작업 창에는 가장 최근에 수행한 작업 5개가 표시됩니다. 작업 창은 작업이 시작된 시점과 작업의 상태도 표시합니다.

작업 창에는 백업, 복원, 클론 및 예약된 백업 작업에 대한 정보가 표시됩니다. SQL Server용 플러그인 또는 Exchange Server용 플러그인을 사용하는 경우 작업 창에 다시 시드된 작업에 대한 정보도 표시됩니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 을 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다.

   작업 중 하나를 클릭하면 작업 세부 정보가 * 작업 세부 정보 * 페이지에 나열됩니다.

백업 작업을 취소합니다

대기열에 있는 백업 작업을 취소할 수 있습니다.

- 필요한 것 *
- 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 모니터 * 페이지 또는 * 작업 * 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 작업에 대해 * 작업 취소 * 버튼이 비활성화됩니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 사용자\그룹 페이지에서 다른 구성원 개체를 보고 작동할 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.

시작...	조치
모니터 페이지	a. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 클릭합니다. b. 작업을 선택한 다음 * 작업 취소 * 를 클릭합니다.

시작...	조치
작업 창	a. 백업 작업을 시작한 후 * 를 클릭합니다 * 를 클릭합니다. b. 작업을 선택합니다. c. 작업 세부 정보 페이지에서 * 작업 취소 * 를 클릭합니다.

작업이 취소되고 리소스가 이전 상태로 돌아갑니다.

토폴로지 페이지에서 관련 백업 및 클론 보기

리소스를 백업 또는 클론 복제할 때 운영 스토리지와 보조 스토리지의 모든 백업 및 클론을 그래픽으로 표시할 수 있습니다. 토폴로지 페이지에서 선택한 리소스 또는 리소스 그룹에 사용할 수 있는 모든 백업 및 클론을 볼 수 있습니다. 이러한 백업 및 클론의 세부 정보를 확인한 다음 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

이 작업에 대해

복제본 관리 보기에서 다음 아이콘을 검토하여 운영 스토리지 또는 보조 스토리지(미러 복사본 또는 볼트 복제본)에서 백업과 클론을 사용할 수 있는지 확인할 수 있습니다.

- 기본 스토리지에서 사용할 수 있는 백업 및 클론 수를 표시합니다.
- SnapMirror 기술을 사용하여 보조 스토리지에 미러링된 백업 및 클론 수를 표시합니다.

  미러 볼트 유형 볼륨에 있는 버전에 유연한 미러 백업의 클론은 토폴로지 뷰에 표시되지만 토폴로지 뷰에 있는 미러 백업 카운트에 버전에 따라 유연하게 백업할 수 있는 백업이 포함되지 않습니다.

- SnapVault 기술을 사용하여 보조 스토리지에 복제된 백업 및 클론 수를 표시합니다.
  - 표시된 백업 수에는 보조 스토리지에서 삭제된 백업이 포함됩니다. 예를 들어 정책을 사용하여 6개의 백업을 생성하여 4개의 백업만 보존한 경우 표시되는 백업 수는 6입니다.
  - SnapCenter 1.1에서 업그레이드한 경우, 토폴로지 페이지의 미러 복사본 또는 볼트 사본 아래에 보조 복제본(미러 또는 볼트)의 클론이 표시되지 않습니다. SnapCenter 1.1을 사용하여 생성된 모든 클론은 SnapCenter 3.0의 로컬 복제본 아래에 표시됩니다.

미러 볼트 유형 볼륨에 있는 버전에 유연한 미러 백업의 클론은 토폴로지 뷰에 표시되지만 토폴로지 뷰에 있는 미러 백업 카운트에 버전에 따라 유연하게 백업할 수 있는 백업이 포함되지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.

2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 자원 세부 정보 보기 또는 자원 그룹 세부 정보 보기에서 자원을 선택합니다.

   리소스가 보호되는 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. Summary 카드를 검토하여 운영 스토리지와 보조 스토리지에서 사용할 수 있는 백업 및 클론 수를 요약합니다.

   요약 카드 섹션에는 총 백업 및 클론 수가 표시됩니다. Oracle 데이터베이스에만 해당하는 요약 카드 섹션에는 총 로그 백업 수가 표시됩니다.

   새로 고침 버튼을 클릭하면 스토리지 쿼리가 시작되어 정확한 카운트가 표시됩니다.

5. 복사본 관리 보기에서 기본 또는 보조 스토리지에서 * 백업 * 또는 * 클론 * 을 클릭하여 백업 또는 클론의 세부 정보를 확인합니다.

   백업 및 클론의 세부 정보가 표 형식으로 표시됩니다.

6. 테이블에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 클론 복제, 이름 바꾸기 및 삭제 작업을 수행합니다.

   보조 스토리지 시스템에 있는 백업의 이름을 바꾸거나 백업을 삭제할 수 없습니다.

   SnapCenter 사용자 지정 플러그인을 사용하는 경우에는 운영 스토리지 시스템에 있는 백업의 이름을 바꿀 수 없습니다.

   - Oracle 리소스 또는 리소스 그룹의 백업을 선택한 경우 마운트 및 마운트 해제 작업을 수행할 수도 있습니다.
   - Oracle 리소스 또는 리소스 그룹의 로그 백업을 선택한 경우 이름 바꾸기, 마운트, 마운트 해제 및 삭제 작업을 수행할 수 있습니다.
   - Linux용 SnapCenter 플러그인 패키지를 사용하고 있고 Oracle RMAN(복구 관리자)을 사용하여 백업 카탈로그를 작성한 경우에는 이러한 카탈로그 작성된 백업의 이름을 바꿀 수 없습니다.
7. 클론을 삭제하려면 표에서 클론을 선택하고 을 클릭합니다 를 눌러 클론을 삭제합니다.

운영 스토리지의 백업 및 클론을 보여 주는 예

PowerShell cmdlet을 사용하여 백업을 제거합니다

다른 데이터 보호 작업에 더 이상 필요하지 않은 경우 Remove-SmBackup cmdlet을 사용하여 백업을 삭제할 수 있습니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Remove-SmBackup cmdlet을 사용하여 하나 이상의 백업을 삭제합니다.

   이 예에서는 백업 ID를 사용하여 두 개의 백업을 삭제합니다.

```
Remove-SmBackup -BackupIds 3,4
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"):
```

PowerShell cmdlet을 사용하여 보조 백업 수를 정리합니다

Remove-SmBackup cmdlet을 사용하여 스냅샷 복사본이 없는 보조 백업의 백업 수를 정리할 수 있습니다. 복사본 관리 토폴로지에 표시된 총 스냅샷 복사본이 보조 스토리지 스냅샷 복사본 보존 설정과 일치하지 않을 때 이 cmdlet을 사용할 수 있습니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. CleanupSecondaryBackups 매개 변수를 사용하여 보조 백업 수를 정리합니다.

   이 예에서는 스냅샷 복사본 없이 2차 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 시스템을 복구합니다

Windows 파일 시스템 백업을 복구합니다

SnapCenter를 사용하여 파일 시스템 백업을 복구할 수 있습니다. 파일 시스템 복구는 지정된 백업의 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 복구 작업을 시작하기 전에 해당 작업을 취소해야 합니다.
- 파일 시스템 백업은 대체 경로가 아닌 원래 위치로만 복구할 수 있습니다.

  복구된 파일 시스템이 파일 시스템의 원래 위치에 있는 데이터를 덮어쓰므로 백업에서 단일 파일을 복구할 수 없습니다. 파일 시스템 백업에서 단일 파일을 복구하려면 백업을 클론하고 클론의 파일에 액세스해야 합니다.
- 시스템 또는 부팅 볼륨을 복원할 수 없습니다.
- SnapCenter는 클러스터 그룹을 오프라인으로 전환하지 않고도 Windows 클러스터에서 파일 시스템을 복구할 수 있습니다.

이 작업에 대해

- 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 swagger에서 API:API/4.7/configsettings를 통해 표시할 수 있습니다

  Get API를 사용하여 키 값을 표시할 수 있습니다. API 설정은 지원되지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 목록을 필터링하려면 파일 시스템 및 리소스 그룹 옵션을 선택합니다.
3. 목록에서 리소스 그룹을 선택한 다음 * 복원 * 을 클릭합니다.
4. 백업 페이지에서 운영 스토리지 시스템이나 보조 스토리지 시스템에서 복구할지 여부를 선택한 다음 복구할 백업을 선택합니다.

5. 복원 마법사에서 옵션을 선택합니다.
6. 복원 작업 전후에 SnapCenter를 실행할 경로 및 처방된 postscript의 인수를 각각 입력할 수 있습니다.

   예를 들어, 스크립트를 실행하여 SNMP 트랩을 업데이트하고, 경고를 자동화하고, 로그를 보내는 등의 작업을 수행할 수 있습니다.

   처방자 또는 사후 스크립트 경로에는 드라이브 또는 공유가 포함되어서는 안 됩니다. 경로는 scripts_path에 상대해야 합니다.

7. 알림 페이지에서 다음 옵션 중 하나를 선택합니다.

이 필드의 내용...	수행할 작업...
SnapCenter 서버 이벤트를 스토리지 시스템 syslog에 기록합니다	SnapCenter 서버 이벤트를 스토리지 시스템의 syslog에 로깅하려면 이 옵션을 선택합니다.
실패한 작업에 대한 AutoSupport 알림을 스토리지 시스템으로 보냅니다	AutoSupport를 사용하여 실패한 작업에 대한 정보를 NetApp에 보내려면 이 옵션을 선택합니다.
이메일 기본 설정	백업을 복원한 후 수신자에게 이메일 메시지를 보내려면 * Always *, * On Failure * 또는 * On failure 또는 Warning * 을 선택합니다. SMTP 서버, 기본 이메일 제목 줄 및 받는 사람 및 보낸 사람 이메일 주소를 입력합니다.

8. 요약을 검토하고 * Finish * 를 클릭합니다.
9. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

복구된 파일 시스템에 데이터베이스가 포함되어 있는 경우 데이터베이스도 복원해야 합니다. 데이터베이스를 복원하지 않으면 데이터베이스가 잘못된 상태일 수 있습니다. 데이터베이스 복원에 대한 자세한 내용은 해당 데이터베이스의 데이터 보호 가이드 를 참조하십시오.

PowerShell cmdlet을 사용하여 리소스 복원

리소스 백업 복원에는 SnapCenter 서버와의 연결 세션 시작, 백업 목록 표시 및 백업 정보 검색, 백업 복구가 포함됩니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

이 예에서는 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 예는 2015년 1월 29일부터 2015년 2월 3일까지 백업에 대한 자세한 정보를 표시합니다.

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"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.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.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 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

복구 작업을 모니터링합니다

작업 페이지를 사용하여 여러 SnapCenter 복원 작업의 진행률을 모니터링할 수 있습니다. 작업 진행률을 확인하여 작업이 언제 완료되는지 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

복원 후 상태는 복원 작업 후 리소스의 상태와 수행할 수 있는 추가 복원 작업에 대해 설명합니다.

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다

- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨

단계

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 모니터 * 페이지에서 * 작업 * 을 클릭합니다.
3. Jobs * 페이지에서 다음 단계를 수행하십시오.
   a. 을 클릭합니다 복원 작업만 나열되도록 목록을 필터링하려면
   b. 시작 및 종료 날짜를 지정합니다.
   c. Type * 드롭다운 목록에서 * Restore * 를 선택합니다.
   d. Status * (상태 *) 드롭다운 목록에서 복원 상태를 선택합니다.
   e. 성공적으로 완료된 작업을 보려면 * 적용 * 을 클릭합니다.
4. 복원 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. Job Details * 페이지에서 * View logs * 를 클릭합니다.

   로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

볼륨 기반 복원 작업 후에는 백업 메타데이터가 SnapCenter 저장소에서 삭제되지만 백업 카탈로그 항목은 SAP HANA 카탈로그에 남아 있습니다. 복원 작업 상태가 표시됩니다 작업 세부 정보를 클릭하여 일부 하위 작업의 경고 표시를 확인해야 합니다. 경고 표지를 클릭하고 표시된 백업 카탈로그 항목을 삭제합니다.

복원 작업을 취소합니다

대기열에 있는 복원 작업을 취소할 수 있습니다.

복원 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

이 작업에 대해

- Monitor* 페이지 또는 * Activity* 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 작업에는 * 작업 취소 * 버튼이 비활성화됩니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 사용자\그룹 페이지의 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.

시작...	조치
모니터 페이지	1. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 클릭합니다. 2. 작업을 선택하고 * 작업 취소 * 를 클릭합니다.
작업 창	1. 복원 작업을 시작한 후 을 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다. 2. 작업을 선택합니다. 3. 작업 세부 정보 페이지에서 * 작업 취소 * 를 클릭합니다.

Windows 파일 시스템의 클론을 생성합니다

Windows 파일 시스템 백업에서 클론을 생성합니다

SnapCenter를 사용하여 Windows 파일 시스템 백업을 복제할 수 있습니다. 실수로 삭제되거나 변경된 단일 파일의 복제본을 원하는 경우 백업을 복제하고 클론에서 해당 파일에 액세스할 수 있습니다.

시작하기 전에

- 호스트 추가, 리소스 식별 및 SVM(스토리지 가상 머신) 연결 생성과 같은 작업을 완료하여 데이터 보호를 준비할 수 있어야 합니다.
- 파일 시스템의 백업이 있어야 합니다.
- 볼륨을 호스팅하는 애그리게이트는 SVM(스토리지 가상 머신)의 할당된 애그리게이트 목록에 있어야 합니다.
- 리소스 그룹을 복제할 수 없습니다. 개별 파일 시스템 백업만 복제할 수 있습니다.
- 백업이 VMDK 디스크가 있는 가상 시스템에 상주하는 경우 SnapCenter는 백업을 물리적 서버에 복제할 수 없습니다.
- Windows 클러스터(예: 공유 LUN 또는 CSV(클러스터 공유 볼륨) LUN)의 클론을 생성하면 지정한 호스트의 전용 LUN으로 클론이 저장됩니다.
- 클론 생성 작업의 경우 볼륨 마운트 지점의 루트 디렉토리는 공유 디렉토리일 수 없습니다.
- Aggregate의 홈 노드가 아닌 노드에서는 클론을 생성할 수 없습니다.
- Windows 파일 시스템에 대해 반복 클론(클론 라이프사이클) 작업을 예약할 수 없으며 필요 시에만 백업을 클론 복제할 수 있습니다.
- 클론이 포함된 LUN을 새 볼륨으로 이동하면 SnapCenter에서 더 이상 클론을 지원할 수 없습니다. 예를 들어, SnapCenter를 사용하여 해당 클론을 삭제할 수는 없습니다.
- 여러 환경에서 클론을 생성할 수는 없습니다. 예를 들어, 물리적 디스크에서 가상 디스크로 복제하거나 그 반대로 복제할 수 있습니다.

이 작업에 대해

- 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 swagger에서 API:API/4.7/configsettings를 통해 표시할 수 있습니다

Get API를 사용하여 키 값을 표시할 수 있습니다. API 설정은 지원되지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 목록에서 * 파일 시스템 * 을 선택합니다.
3. 호스트를 선택합니다.

   리소스가 보호된 경우 토폴로지 뷰가 자동으로 표시됩니다.

4. 리소스 목록에서 클론 복제할 백업을 선택한 다음 클론 아이콘을 클릭합니다.
5. 옵션 페이지에서 다음을 실행합니다.

이 필드의 내용...	수행할 작업...
클론 서버	클론을 생성할 호스트를 선택합니다.
""마운트 지점 자동 할당"" 또는 ""경로 아래 볼륨 마운트 지점 자동 할당""	경로 아래에 마운트 지점을 자동으로 할당할지, 볼륨 마운트 지점을 자동으로 할당할지 여부를 선택합니다. 경로 아래의 볼륨 마운트 지점 자동 할당: 경로 아래의 마운트 지점을 사용하여 마운트 지점을 생성할 특정 디렉토리를 제공할 수 있습니다. 이 옵션을 선택하기 전에 디렉토리가 비어 있는지 확인해야 합니다. 디렉토리에 백업이 있으면 마운트 작업 후 백업이 잘못된 상태가 됩니다.
보관 위치	보조 백업을 클론하는 경우 아카이브 위치를 선택합니다.

6. 스크립트 페이지에서 실행할 처방이나 소인을 지정합니다.

   처방자 또는 사후 스크립트 경로에는 드라이브 또는 공유가 포함되어서는 안 됩니다. 경로는 scripts_path에 상대해야 합니다.

7. 요약을 검토하고 * Finish * 를 클릭합니다.
8. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

PowerShell cmdlet을 사용하여 백업 클론 생성

클론 워크플로우에는 계획, 클론 작업 수행 및 작업 모니터링이 포함됩니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Get-SmBackup 또는 Get-SmResourceGroup cmdlet을 사용하여 클론을 생성할 수 있는 백업을 나열합니다.

   이 예에서는 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     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

   이 예제에서는 지정된 리소스 그룹, 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 클론 작업을 시작합니다.

   이 예에서는 모든 로그를 사용하여 지정된 백업에서 클론을 생성합니다.

```
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 클론을 생성합니다.

```
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 클론 작업의 상태를 봅니다.

   이 예에서는 지정된 작업 ID에 대한 클론 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 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

클론 작업을 모니터링합니다

작업 페이지를 사용하여 SnapCenter 클론 작업의 진행률을 모니터링할 수 있습니다. 작업 진행률을 확인하여 작업이 언제 완료되는지 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다

- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨
- 단계 *
  1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
  2. 모니터 * 페이지에서 * 작업 * 을 클릭합니다.
  3. Jobs * 페이지에서 다음 단계를 수행하십시오.
     a. 을 클릭합니다 클론 작업만 나열되도록 목록을 필터링합니다.
     b. 시작 및 종료 날짜를 지정합니다.
     c. Type * 드롭다운 목록에서 * Clone * 을 선택합니다.
     d. Status * (상태 *) 드롭다운 목록에서 클론 상태를 선택합니다.
     e. 성공적으로 완료된 작업을 보려면 * 적용 * 을 클릭합니다.
  4. 클론 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
  5. 작업 세부 정보 페이지에서 * 로그 보기 * 를 클릭합니다.

클론 작업을 취소합니다

대기열에 있는 클론 작업을 취소할 수 있습니다.

클론 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

이 작업에 대해

- Monitor * 페이지 또는 * Activity * 창에서 대기 중인 클론 작업을 취소할 수 있습니다.
- 실행 중인 클론 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 대기 중인 클론 작업을 취소할 수 있습니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 다른 구성원 개체 * 를 볼 수 있고 사용자\그룹 페이지에서 작동할 수 있는 경우 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 클론 작업을 취소할 수 있습니다.

단계

다음 작업 중 하나를 수행합니다.

시작...	조치
모니터 페이지	1. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 클릭합니다. 2. 작업을 선택하고 * 작업 취소 * 를 클릭합니다.

시작...	조치
작업 창	1. 클론 작업을 시작한 후 을 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다. 2. 작업을 선택합니다. 3. 작업 세부 정보 * 페이지에서 * 작업 취소 * 를 클릭합니다.

클론 분할

SnapCenter를 사용하여 상위 리소스에서 복제된 리소스를 분할할 수 있습니다. 분할되는 클론은 상위 리소스와 독립적입니다.

이 작업에 대해

- 중간 클론에는 클론 분할 작업을 수행할 수 없습니다.

  예를 들어 데이터베이스 백업에서 clone1을 생성한 후 clone1의 백업을 생성한 다음 이 백업(clone2)을 클론 복제할 수 있습니다. clone2를 생성한 후에는 clone1이 중간 클론이며 clone1에서 클론 분할 작업을 수행할 수 없습니다. 그러나 clone2에서 클론 분할 작업을 수행할 수 있습니다.

  clone2를 분할한 후에는 clone1이 더 이상 중간 클론이 아니기 때문에 clone1에서 클론 분할 작업을 수행할 수 있습니다.

- 클론을 분할하면 클론의 백업 복사본 및 클론 작업이 삭제됩니다.
- 클론 분할 작업 제한에 대한 자세한 내용은 을 참조하십시오 "ONTAP 9 논리적 스토리지 관리 가이드".
- 스토리지 시스템의 볼륨 또는 애그리게이트는 온라인 상태인지 확인합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. Resources * 페이지의 View 목록에서 적절한 옵션을 선택합니다.

옵션을 선택합니다	설명
성능을 대폭 향상	보기 목록에서 * 데이터베이스 * 를 선택합니다.
파일 시스템의 경우	보기 목록에서 * 경로 * 를 선택합니다.

3. 목록에서 적절한 리소스를 선택합니다.

   리소스 토폴로지 페이지가 표시됩니다.

4. 복사본 관리 * 보기에서 복제된 리소스(예: 데이터베이스 또는 LUN)를 선택한 다음 * 를 클릭합니다 *.
5. 분할할 클론의 예상 크기와 애그리게이트에서 사용할 수 있는 필수 공간을 검토한 다음 * 시작 * 을 클릭합니다.
6. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

SMCore 서비스가 다시 시작되면 클론 분할 작업이 응답하지 않습니다. Stop-SmJob cmdlet을 실행하여 클론 분할 작업을 중지한 다음 클론 분할 작업을 다시 시도해야 합니다.

폴링 시간을 더 오래 설정하거나 폴링 시간을 짧게 하여 클론이 분할되었는지 여부를 확인하려면 _SMCoreServiceHost.exe.config_file에서 _CloneSplitStatusCheckPollTime_parameter 값을 변경하여 SMCore가 클론 분할 작업의 상태를 폴링할 시간 간격을 설정할 수 있습니다. 값은 밀리초이고 기본값은 5분입니다.

예를 들면 다음과 같습니다.

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

백업, 복원 또는 다른 클론 분할이 진행 중인 경우 클론 분할 시작 작업이 실패합니다. 실행 중인 작업이 완료된 후에만 클론 분할 작업을 다시 시작해야 합니다.

관련 정보

"Aggregate가 존재하지 않으면 SnapCenter 클론 또는 검증에 실패합니다"

Microsoft Exchange Server 데이터베이스 보호

Microsoft Exchange Server용 SnapCenter 플러그인 개념

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 SnapCenter와 NetApp SnapMirror 기술을 함께 사용하여 다른 볼륨에 백업 세트의 미러링 복사본을 만들고 NetApp SnapVault 기술을 사용하여 표준 준수 또는 아카이브용으로 D2D 백업 복제를 수행할 수 있습니다.

전체 Exchange 데이터베이스 대신 메일 또는 편지함을 복원 및 복구하려면 SMBR(Single Mailbox Recovery) 소프트웨어를 사용하십시오.
NetApp ® Single Mailbox Recovery는 2023년 5월 12일 EOA(End of Availability)로 제공됩니다. NetApp은 2020년 6월 24일에 출시된 마케팅 부품 번호를 통해 지원 자격 기간 동안 메일박스 용량, 유지보수, 지원을 구매한 고객을 계속 지원할 예정입니다.

NetApp Single Mailbox Recovery는 Ontrack에서 제공하는 파트너 제품입니다. OnTrack PowerControls는 NetApp Single Mailbox Recovery와 유사한 기능을 제공합니다. 고객은 세분화된 메일박스 복구를 위해 Ontrack PowerControls 소프트웨어 라이센스와 Ontrack PowerControls 유지보수 및 지원 갱신을 licensingteam@ontrack.com 통해 구매할 수 있습니다.

Microsoft Exchange Server용 SnapCenter 플러그인으로 수행할 수 있는 작업

Exchange용 플러그인을 사용하여 Exchange Server 데이터베이스를 백업 및 복원할 수 있습니다.

- Exchange DAG(데이터베이스 가용성 그룹), 데이터베이스 및 복제 세트의 활성 인벤토리를 보고 관리합니다
- 백업 자동화를 위한 보호 설정을 제공하는 정책을 정의합니다
- 리소스 그룹에 정책을 할당합니다
- 개별 DAG 및 데이터베이스 보호
- 기본 및 보조 Exchange 메일박스 데이터베이스를 백업합니다
- 기본 및 보조 백업에서 데이터베이스를 복원합니다

Microsoft Windows용 SnapCenter 플러그인 및 Microsoft Exchange Server에서 지원하는 스토리지 유형입니다

SnapCenter는 물리적 시스템과 가상 머신 모두에서 다양한 스토리지 유형을 지원합니다. 호스트에 대한 패키지를 설치하기 전에 스토리지 유형에 대한 지원이 가능한지 확인해야 합니다.

SnapCenter 프로비저닝 및 데이터 보호 지원은 Windows Server에서 제공됩니다. 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

기계	스토리지 유형입니다	를 사용하여 프로비저닝	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 HBA를 통해 연결된 RDM LUN	PowerShell cmdlet	물리적 호환성 전용  VMDK는 지원되지 않습니다.
VMware VM	iSCSI 이니시에이터가 게스트 시스템에 직접 접속된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	 VMDK는 지원되지 않습니다.
Hyper-V VM	가상 Fibre Channel 스위치를 통해 연결된 VFC(가상 FC) LUN입니다	SnapCenter GUI 또는 PowerShell cmdlet	Hyper-V Manager를 사용하여 가상 Fibre Channel 스위치로 연결된 VFC(가상 FC) LUN을 프로비저닝해야 합니다.  NetApp 스토리지에 프로비저닝된 Hyper-V는 디스크를 통과하고 VHD(x)에서 데이터베이스를 백업하는 것은 지원되지 않습니다.

기계	스토리지 유형입니다	를 사용하여 프로비저닝	지원 노트
Hyper-V VM	iSCSI 이니시에이터가 게스트 시스템에 직접 접속된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	NetApp 스토리지에 프로비저닝된 Hyper-V는 디스크를 통과하고 VHD(x)에서 데이터베이스를 백업하는 것은 지원되지 않습니다.

Exchange 플러그인에 필요한 최소 ONTAP 권한

필요한 최소 ONTAP 권한은 데이터 보호를 위해 사용 중인 SnapCenter 플러그인에 따라 다릅니다.

- All-access 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
  - event generate-autosupport-log입니다
  - 작업 기록이 표시됩니다
  - 작업 중지
  - LUN을 클릭합니다
  - LUN 생성
  - LUN 생성
  - LUN 생성
  - LUN을 삭제합니다
  - LUN igroup 추가
  - LUN igroup 작성
  - LUN igroup 삭제
  - LUN igroup의 이름을 바꿉니다
  - LUN igroup의 이름을 바꿉니다
  - LUN igroup 표시
  - LUN 매핑 add-reporting-nodes입니다
  - LUN 매핑 생성
  - LUN 매핑을 삭제합니다
  - LUN 매핑으로 remove-reporting-nodes를 사용할 수 있습니다

- LUN 매핑이 표시됩니다
- LUN 수정
- LUN 이동 - 볼륨
- LUN이 오프라인 상태입니다
- LUN을 온라인 상태로 전환합니다
- LUN persistent - 예약 지우기
- LUN 크기 조정
- LUN 일련 번호입니다
- LUN 표시
- SnapMirror 정책 추가 규칙
- SnapMirror 정책 modify-rule을 참조하십시오
- SnapMirror 정책 remove-rule을 참조하십시오
- SnapMirror 정책 쇼
- SnapMirror 복원
- SnapMirror 쇼
- SnapMirror 기록
- SnapMirror 업데이트
- SnapMirror 업데이트 - ls -set
- SnapMirror 목록 - 대상
- 버전
- 볼륨 클론 생성
- 볼륨 클론 표시
- 볼륨 클론 분할 시작이 있습니다
- 볼륨 클론 분할 중지
- 볼륨 생성
- 볼륨 제거
- 볼륨 파일 클론 생성
- 볼륨 파일 show-disk-usage 를 참조하십시오
- 볼륨이 오프라인 상태입니다
- 볼륨을 온라인으로 설정합니다
- 볼륨 수정
- 볼륨 qtree 생성
- 볼륨 qtree 삭제
- 볼륨 qtree 수정

- 볼륨 qtree 표시
- 볼륨 제한
- 볼륨 표시
- 볼륨 스냅샷 생성
- 볼륨 스냅숏 삭제
- 볼륨 스냅숏 수정
- 볼륨 스냅숏 이름 바꾸기
- 볼륨 스냅샷 복원
- 볼륨 스냅샷 복원 - 파일
- 볼륨 스냅샷 표시
- 볼륨 마운트 해제
- SVM CIFS를 선택합니다
- SVM CIFS 공유 생성
- SVM CIFS 공유 삭제
- SVM CIFS shadowcopy show 를 참조하십시오
- SVM CIFS 공유 표시
- vserver cifs show 를 참조하십시오
- SVM 엑스포트 - 정책
- SVM 엑스포트 정책 생성
- SVM 엑스포트 정책 삭제
- SVM 엑스포트 정책 규칙 생성
- vserver export-policy rule show를 참조하십시오
- vserver export-policy show를 참조하십시오
- SVM iSCSI
- SVM iSCSI 연결이 표시됩니다
- vserver show 를 참조하십시오

- 읽기 전용 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
  - 네트워크 인터페이스
  - 네트워크 인터페이스가 표시됩니다
  - SVM

SnapMirror 및 **SnapVault** 복제를 위한 스토리지 시스템 준비

ONTAP 플러그인을 SnapCenter SnapMirror 기술과 함께 사용하여 다른 볼륨에 백업 세트의 미러링 복사본을 만들고 ONTAP SnapVault 기술을 사용하여 표준 준수 및 기타 거버넌스 관련 용도로 D2D 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 타겟

볼륨 간의 데이터 보호 관계를 구성하고 관계를 초기화해야 합니다.

SnapCenter는 스냅샷 복사본 작업이 완료된 후 SnapMirror 및 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행되고, 별도의 ONTAP 일정을 만들지 않습니다.

NetApp SnapManager 제품에서 SnapCenter으로 오고 있으며 구성한 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 운영 스토리지(소스 볼륨)의 데이터를 보조 스토리지(타겟 볼륨)에 복제합니다. 관계를 초기화할 때 ONTAP은 소스 볼륨에서 참조된 데이터 블록을 대상 볼륨으로 전송합니다.

SnapCenter는 SnapMirror와 SnapVault 볼륨(* Primary * > * Mirror * > * Vault *) 간의 계단식 관계를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter는 버전에 상관없이 유연한 SnapMirror 관계의 관리를 지원합니다. 버전에 상관없이 유연한 SnapMirror 관계와 설정 방법에 대한 자세한 내용은 를 참조하십시오 "ONTAP 설명서".

SnapCenter는 * SYNC_MIRROR * 복제를 지원하지 않습니다.

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. SLA(서비스 수준 계약), RTO(복구 시간 목표) 및 RPO(복구 시점 목표)에 따라 백업 전략이 크게 결정됩니다.

SLA는 예상되는 서비스 수준을 정의하고 가용성 및 서비스 성능을 비롯한 다양한 서비스 관련 문제를 해결합니다. RTO는 서비스 중단 후 비즈니스 프로세스를 복원해야 하는 시간입니다. RPO는 장애 후 정상적인 작업을 재개하기 위해 백업 스토리지에서 복구해야 하는 파일의 사용 기간에 대한 전략을 정의합니다. SLA, RTO 및 RPO는 백업 전략에 기여합니다.

Exchange 데이터베이스에 대해 지원되는 백업 유형입니다

SnapCenter를 사용하여 Exchange 메일박스를 백업하려면 데이터베이스 및 DAG(데이터베이스 가용성 그룹)와 같은 리소스 유형을 선택해야 합니다. 스냅샷 복사본 기술은 리소스가 상주하는 볼륨의 온라인 읽기 전용 복사본을 생성하는 데 사용됩니다.

백업 유형	설명
전체 및 로그 백업	잘린 로그를 포함하여 데이터베이스와 모든 트랜잭션 로그를 백업합니다. 전체 백업이 완료되면 Exchange Server는 데이터베이스에 이미 커밋된 트랜잭션 로그를 잘라냅니다. 일반적으로 이 옵션을 선택해야 합니다. 그러나 백업 시간이 짧은 경우에는 전체 백업을 사용하여 트랜잭션 로그 백업을 실행하지 않도록 선택할 수 있습니다.

백업 유형	설명
전체 백업	데이터베이스 및 트랜잭션 로그를 백업합니다. 잘린 트랜잭션 로그는 백업되지 않습니다.
로그 백업	모든 트랜잭션 로그를 백업합니다. 데이터베이스에 이미 커밋된 잘린 로그는 백업되지 않습니다. 전체 데이터베이스 백업 간에 트랜잭션 로그 백업을 자주 예약하는 경우 세분화된 복구 지점을 선택할 수 있습니다.

데이터베이스 플러그인에 대한 백업 스케줄입니다

백업 빈도(스케줄 유형)는 정책에 지정되며 백업 스케줄은 리소스 그룹 구성에 지정됩니다. 백업 빈도 또는 스케줄을 결정하는 가장 중요한 요소는 리소스의 변경 속도 및 데이터의 중요도입니다. 자주 사용하는 리소스를 매일 한 번씩 백업할 수도 있고, 자주 사용하지 않는 리소스를 하루에 한 번 백업할 수도 있습니다. 기타 요인으로는 조직에 대한 리소스의 중요성, SLA(서비스 수준 계약) 및 RPO(복구 시점 목표)가 있습니다.

SLA는 예상되는 서비스 수준을 정의하고 가용성 및 서비스 성능을 비롯한 다양한 서비스 관련 문제를 해결합니다. RPO는 장애 후 정상적인 작업을 재개하기 위해 백업 스토리지에서 복구해야 하는 파일의 사용 기간에 대한 전략을 정의합니다. SLA 및 RPO는 데이터 보호 전략에 기여합니다.

사용량이 많은 리소스의 경우에도 하루에 한 번 또는 두 번 이상 전체 백업을 실행할 필요가 없습니다. 예를 들어 정기적인 트랜잭션 로그 백업만으로도 필요한 백업이 있는지 확인할 수 있습니다. 데이터베이스를 더 자주 백업할수록 SnapCenter는 복원 시 사용해야 하는 트랜잭션 로그를 더 적게 사용하여 복원 작업을 더 빠르게 수행할 수 있습니다.

백업 스케줄은 다음과 같이 두 부분으로 구성됩니다.

- 백업 빈도

  일부 플러그인에 대해 _schedule type_이라는 백업 빈도(백업 수행 빈도)는 정책 구성의 일부입니다. 정책의 백업 빈도로 시간별, 일별, 주별 또는 월별 을 선택할 수 있습니다. 이러한 빈도 중 하나를 선택하지 않으면 생성된 정책이 온디맨드 전용 정책입니다. 설정 * > * 정책 * 을 클릭하여 정책에 액세스할 수 있습니다.

- 백업 스케줄

  백업 스케줄(백업을 수행할 정확한 시점)은 리소스 그룹 구성의 일부입니다. 예를 들어 주별 백업에 대한 정책이 구성된 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 스케줄을 구성할 수 있습니다. 리소스 그룹 * > * 리소스 그룹 * 을 클릭하여 리소스 그룹 일정에 액세스할 수 있습니다.

데이터베이스에 필요한 백업 작업 수입니다

필요한 백업 작업 수를 결정하는 요인에는 리소스 크기, 사용된 볼륨 수, 리소스 변경 속도 및 SLA(서비스 수준 계약)가 포함됩니다.

백업 명명 규칙

기본 스냅샷 복사본 명명 규칙을 사용하거나 사용자 지정된 명명 규칙을 사용할 수 있습니다. 기본 백업 명명 규칙은 스냅샷 복사본 이름에 타임 스탬프를 추가하여 복사본이 생성된 시간을 식별하도록 도와줍니다.

스냅샷 복사본은 다음과 같은 기본 명명 규칙을 사용합니다.

`resourcegroupname_hostname_timestamp`

다음 예제와 같이 백업 리소스 그룹의 이름을 논리적으로 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예제에서 구문 요소는 다음과 같은 의미를 가집니다.

- _dts1_은(는) 리소스 그룹 이름입니다.
- _mach1x88_은 호스트 이름입니다.
- _03-12-2015_23.17.26_은 날짜 및 타임스탬프입니다.

또는 * Use custom name format for Snapshot copy * 를 선택하여 리소스 또는 리소스 그룹을 보호하면서 스냅샷 복사본 이름 형식을 지정할 수 있습니다. 예를 들어 customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname을 입력합니다. 기본적으로 타임스탬프 접미사가 스냅샷 복사본 이름에 추가됩니다.

백업 보존 옵션

백업 복사본을 보존할 일 수를 선택하거나 유지할 백업 복사본 수를 최대 255개 사본의 ONTAP로 지정할 수 있습니다. 예를 들어, 조직에서 10일간 백업 복사본 또는 130개의 백업 복사본을 보존해야 할 수도 있습니다.

정책을 생성하는 동안 백업 유형 및 스케줄 유형에 대한 보존 옵션을 지정할 수 있습니다.

SnapMirror 복제를 설정하면 보존 정책이 대상 볼륨에 미러링됩니다.

SnapCenter는 스케줄 유형과 일치하는 보존 레이블이 있는 보존된 백업을 삭제합니다. 리소스 또는 리소스 그룹에 대한 스케줄 유형이 변경된 경우 이전 스케줄 유형 레이블이 있는 백업이 시스템에 남아 있을 수 있습니다.

백업 복사본을 장기간 보존하려면 SnapVault 백업을 사용해야 합니다.

Exchange Server의 소스 스토리지 볼륨에 트랜잭션 로그 백업을 유지하는 기간

Microsoft Exchange Server용 SnapCenter 플러그인에는 최신 복원 작업을 수행하기 위한 트랜잭션 로그 백업이 필요합니다. 이 작업은 데이터베이스를 두 개의 전체 백업 사이의 시간으로 복원합니다.

예를 들어 Exchange용 플러그인이 오전 8시에 전체 및 트랜잭션 로그 백업을 수행하는 경우 또한 오후 5시에 전체 및 트랜잭션 로그 백업을 추가로 수행하면 최신 트랜잭션 로그 백업을 사용하여 오전 8시 사이에 언제든지 데이터베이스를 복원할 수 있습니다 오후 5시까지 운영됩니다 트랜잭션 로그를 사용할 수 없는 경우 Exchange용 플러그인은 시점 복원 작업만 수행할 수 있습니다. 그러면 Exchange용 플러그인에서 전체 백업을 완료한 시점으로 데이터베이스를 복원할 수 있습니다.

일반적으로 하루 또는 이틀 동안만 최신 복원 작업이 필요합니다. 기본적으로 SnapCenter는 최소 2일을 유지합니다.

Exchange 데이터베이스에 대한 복구 전략 정의

Exchange Server에 대한 복원 전략을 정의하면 데이터베이스를 성공적으로 복원할 수

있습니다.

Exchange Server의 복구 작업에 대한 소스

기본 스토리지의 백업 복사본에서 Exchange Server 데이터베이스를 복원할 수 있습니다.

운영 스토리지에서만 데이터베이스를 복원할 수 있습니다.

Exchange Server에 대해 지원되는 복구 작업 유형입니다

SnapCenter를 사용하여 Exchange 리소스에 대해 다양한 유형의 복구 작업을 수행할 수 있습니다.

- 최신 상태로 복원합니다
- 이전 시점으로 복원합니다

최대 1분 내에 복원합니다

최신 복원 작업에서 데이터베이스는 장애 지점까지 복구됩니다. SnapCenter는 다음 시퀀스를 실행하여 이를 수행합니다.

1. 선택한 전체 데이터베이스 백업에서 데이터베이스를 복원합니다.
2. 백업된 모든 트랜잭션 로그와 가장 최근 백업 이후에 생성된 새 로그를 적용합니다.

   트랜잭션 로그가 앞으로 이동되어 선택한 데이터베이스에 적용됩니다.

   복구가 완료된 후 Exchange에서 새 로그 체인을 생성합니다.

* 모범 사례: * 복원이 완료된 후 새 전체 및 로그 백업을 수행하는 것이 좋습니다.

   최신 복원 작업을 수행하려면 일련의 트랜잭션 로그가 필요합니다.

   최신 복원을 수행한 후에는 복구에 사용한 백업을 시점 복원 작업에만 사용할 수 있습니다.

   모든 백업에 대해 최신 복원 기능을 유지할 필요가 없는 경우 백업 정책을 통해 시스템의 트랜잭션 로그 백업 보존을 구성할 수 있습니다.

이전 시점으로 복원합니다

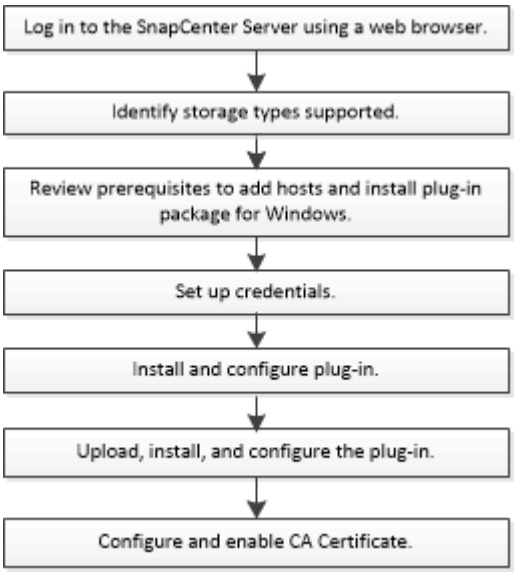
시점 복원 작업에서는 데이터베이스가 과거의 특정 시간으로만 복원됩니다. 시점 복원 작업은 다음과 같은 복원 상황에서 수행됩니다.

- 데이터베이스는 백업된 트랜잭션 로그에서 지정된 시간으로 복원됩니다.
- 데이터베이스가 복원되고 백업된 트랜잭션 로그의 하위 집합만 데이터베이스에 적용됩니다.

Microsoft Exchange Server용 SnapCenter 플러그인을 설치합니다

Microsoft Exchange Server용 SnapCenter 플러그인 설치 워크플로우

Exchange 데이터베이스를 보호하려면 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



호스트를 추가하고 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하기 위한 사전 요구 사항

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 완료해야 합니다.

- iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.
- 원격 호스트에 대한 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 도메인 사용자가 있어야 합니다.
- 독립 실행형 및 데이터베이스 가용성 그룹 구성에 Microsoft Exchange Server 2013, 2016 또는 2019를 사용해야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자의 경우 호스트에서 UAC를 비활성화해야 합니다.
- SnapCenter에서 클러스터 노드를 관리하는 경우 클러스터의 모든 노드에 대한 관리 권한이 있는 사용자가 있어야 합니다.
- Exchange Server에 대한 관리 권한이 있는 사용자가 있어야 합니다.
- SnapManager for Microsoft Exchange Server 및 SnapDrive for Windows가 이미 설치되어 있는 경우, 동일한 Exchange Server에 Exchange용 플러그인을 설치하기 전에 SnapDrive for Windows에서 사용하는 VSS 하드웨어 공급자를 등록 취소해야 SnapCenter를 사용하여 데이터를 성공적으로 보호할 수 있습니다.
- Microsoft Exchange Server용 SnapManager와 Exchange용 플러그인이 동일한 서버에 설치되어 있는 경우 Windows 스케줄러에서 Microsoft Exchange Server용 SnapManager가 생성한 모든 스케줄을 일시 중지하거나 삭제해야 합니다.
- 호스트는 서버에서 FQDN(정규화된 도메인 이름)으로 확인할 수 있어야 합니다. 호스트 파일을 확인할 수 있도록 수정하고 호스트 파일에 짧은 이름과 FQDN이 모두 지정된 경우 *<IP_address><host_FQDN><host_name>* 형식으로 SnapCenter hosts 파일에 항목을 생성합니다.
- 방화벽에서 다음 포트가 차단되지 않았는지 확인합니다. 차단되지 않으면 호스트 추가 작업이 실패합니다. 이 문제를 해결하려면 동적 포트 범위를 구성해야 합니다. 자세한 내용은 을 참조하십시오 "Microsoft 설명서".

- Windows 2016 및 Exchange 2016의 경우 포트 범위 50000 - 51000
- Windows 2012 R2 및 Exchange 2013의 경우 포트 범위는 6000-6500입니다
- Windows 2019의 경우 포트 범위 49152-65536

포트 범위를 식별하려면 다음 명령을 실행합니다.

- 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 사항 및 사이징 요구 사항을 숙지해야 합니다.

항목	요구 사항
운영 체제	Microsoft Windows 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	• Microsoft .NET Framework 4.7.2 이상 • WMF(Windows Management Framework) 4.0 이상 • PowerShell 4.0 이상 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴". NET 관련 문제 해결에 대한 자세한 내용은 을 참조하십시오 "인터넷에 연결되지 않은 기존 시스템의 경우 SnapCenter 업그레이드 또는 설치가 실패합니다."

Exchange Server 권한이 필요합니다

SnapCenter에서 Exchange Server 또는 DAG를 추가하고 호스트 또는 DAG에 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하려면 최소 권한 및 권한 세트가 있는 사용자에 대한 자격 증명을 사용하여 SnapCenter를 구성해야 합니다.

로컬 관리자 권한이 있는 도메인 사용자와 원격 Exchange 호스트에 대한 로컬 로그인 권한, DAG의 모든 노드에 대한 관리 권한이 있어야 합니다. 도메인 사용자에게는 다음과 같은 최소 권한이 필요합니다.

- Add-MailboxDatabaseCopy 를 선택합니다
- 마운트 해제 - 데이터베이스
- 가져오기 - AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer를 선택합니다
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus 를 참조하십시오
- Get-MailboxServer 를 참조하십시오
- Get-MailboxStatistics를 참조하십시오
- Get-PublicFolderDatabase를 참조하십시오
- Move-ActiveMailboxDatabase(ActiveMailboxDatabase 이동)
- move-DatabasePath-ConfigurationOnly:$true입니다
- 마운트 - 데이터베이스
- New - MailboxDatabase
- 새 기능 - PublicFolderDatabase
- remove - MailboxDatabase(메일 사서함 데이터베이스)
- remove-MailboxDatabaseCopy 를 선택합니다
- 제거 - PublicFolderDatabase
- Resume - MailboxDatabaseCopy
- 설정 - AdServerSettings
- Set-MailboxDatabase -allowfilerestore:$true입니다
- Set-MailboxDatabaseCopy 를 선택합니다
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy 를 선택합니다
- 업데이트 - MailboxDatabaseCopy

Windows용 **SnapCenter** 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항 및 사이징 요구 사항을 숙지해야 합니다.

항목	요구 사항
운영 체제	Microsoft Windows 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	• Microsoft .NET Framework 4.7.2 이상 • WMF(Windows Management Framework) 4.0 이상 • PowerShell 4.0 이상 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴". NET 관련 문제 해결에 대한 자세한 내용은 을 참조하십시오 "인터넷에 연결되지 않은 기존 시스템의 경우 SnapCenter 업그레이드 또는 설치가 실패합니다."

Windows용 SnapCenter 플러그인의 자격 증명을 설정합니다

SnapCenter는 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 대해

Windows 호스트에 플러그인을 설치하기 위한 자격 증명을 설정해야 합니다. 호스트를 구축하고 플러그인을 설치한 후 Windows에 대한 자격 증명을 생성할 수 있지만, 호스트를 구축하고 플러그인을 설치하기 전에 SVM을 추가한 후에 자격 증명을 생성하는 것이 가장 좋습니다.

원격 호스트에 대한 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정합니다.

개별 리소스 그룹에 대한 자격 증명을 설정했고 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 실행합니다.

이 필드의 내용...	수행할 작업...
자격 증명 이름입니다	자격 증명의 이름을 입력합니다.
사용자 이름	인증에 사용되는 사용자 이름을 입력합니다. • 도메인 관리자 또는 관리자 그룹의 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹의 구성원을 지정합니다. 사용자 이름 필드에 유효한 형식은 다음과 같습니다. ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우 SnapCenter 플러그인을 설치할 시스템에 기본 제공 로컬 관리자를 지정합니다. 사용자 계정에 상승된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 올바른 형식은 다음과 같습니다. `UserName`
암호	인증에 사용되는 암호를 입력합니다.
인증	인증 모드로 Windows를 선택합니다.

5. 확인 * 을 클릭합니다.

Windows Server 2012 이상에서 GMSA를 구성합니다

Windows Server 2012 이상을 사용하면 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 GMSA(Managed Service Account)를 만들 수 있습니다.

시작하기 전에

- Windows Server 2012 이상의 도메인 컨트롤러가 있어야 합니다.

- 도메인의 구성원인 Windows Server 2012 이상 호스트가 있어야 합니다.

단계

1. KDS 루트 키를 생성하여 GMSA의 각 개체에 대해 고유한 암호를 생성합니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 Add-KDSRootKey-EffectiveImmediately 명령을 실행합니다
3. GMSA 생성 및 구성:
   a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
 domainName\accountName$
.. 그룹에 컴퓨터 개체를 추가합니다.
.. 방금 생성한 사용자 그룹을 사용하여 GMSA를 생성합니다.
```

   예를 들면, 다음과 같습니다.

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. 실행 `Get-ADServiceAccount` 명령을 사용하여 서비스 계정을 확인합니다.
```

4. 호스트에서 GMSA를 구성합니다.
   a. GMSA 계정을 사용할 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.

   이렇게 하려면 PowerShell에서 다음 명령을 실행합니다.

```
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 확인합니다. `Test-AdServiceAccount <gMSA>`

5. 호스트에서 구성된 GMSA에 관리 권한을 할당합니다.
6. SnapCenter 서버에서 구성된 GMSA 계정을 지정하여 Windows 호스트를 추가합니다.

   SnapCenter 서버는 선택한 플러그인을 호스트에 설치하고 지정된 GMSA는 플러그인 설치 중에 서비스 로그온 계정으로 사용됩니다.

호스트를 추가하고 **Exchange**용 플러그인을 설치합니다

SnapCenter 호스트 추가 페이지를 사용하여 Windows 호스트를 추가할 수 있습니다. Exchange용 플러그인은 지정된 호스트에 자동으로 설치됩니다. 이는 플러그인을 설치하는 데 권장되는 방법입니다. 호스트를 추가하고 개별 호스트 또는 클러스터에 대한 플러그인을 설치할 수 있습니다.

시작하기 전에

- 플러그인 설치 및 제거 권한이 있는 역할(예: SnapCenter 관리자)에 할당된 사용자여야 합니다
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에 속한 경우 호스트에서 UAC를 비활성화해야 합니다.
- 메시지 큐 서비스가 실행되고 있어야 합니다.
- 그룹 GMSA(Managed Service Account)를 사용하는 경우 관리자 권한으로 GMSA를 구성해야 합니다. 자세한 내용은 을 참조하십시오
  "Microsoft Exchange Server에 대해 Windows Server 2012 이상에서 그룹 관리 서비스 계정을 구성합니다".

이 작업에 대해

- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.
- 호스트를 추가하고 개별 호스트 또는 클러스터에 대한 플러그인 패키지를 설치할 수 있습니다.
- Exchange 노드가 DAG의 일부인 경우 SnapCenter 서버에 하나의 노드만 추가할 수 없습니다.
- 클러스터(Exchange DAG)에 플러그인을 설치하는 경우 일부 노드에 NetApp LUN에 데이터베이스가 없는 경우에도 클러스터의 모든 노드에 플러그인이 설치됩니다.

SnapCenter 4.6부터 SCE는 멀티 테넌시를 지원하며 다음 방법을 사용하여 호스트를 추가할 수 있습니다.

호스트 작업을 추가합니다	**4.5** 이하	**4.6** 이상
크로스 또는 다른 도메인에 IP-less DAG를 추가합니다	지원되지 않습니다	지원
동일한 도메인 또는 교차 도메인에 있는 고유한 이름의 여러 IP DAG를 추가합니다	지원	지원
도메인 간에 동일한 호스트 이름 및 /또는 DB 이름을 가진 여러 IP 또는 IP가 없는 DAG를 추가합니다	지원되지 않습니다	지원

호스트 작업을 추가합니다	**4.5** 이하	**4.6** 이상
동일한 이름과 도메인 간에 여러 IP/IP 없는 DAG를 추가합니다	지원되지 않습니다	지원
동일한 이름과 도메인 간에 여러 독립 실행형 호스트를 추가합니다	지원되지 않습니다	지원

Exchange용 플러그인은 Windows용 SnapCenter 플러그인 패키지에 따라 다르며 버전이 같아야 합니다. Exchange용 플러그인 설치 중에 Windows용 SnapCenter 플러그인 패키지가 기본적으로 선택되어 있으며 VSS 하드웨어 공급자와 함께 설치됩니다.

Microsoft Exchange Server용 SnapManager와 Windows용 SnapDrive가 이미 설치되어 있는 경우 Exchange용 플러그인을 동일한 Exchange Server에 설치하려면 Exchange용 플러그인 및 Windows용 SnapCenter 플러그인 패키지와 함께 설치된 VSS 하드웨어 공급자와 호환되지 않으므로 Windows용 SnapDrive에서 사용하는 VSS 하드웨어 공급자를 등록 취소해야 합니다. 자세한 내용은 을 참조하십시오 "Data ONTAP VSS 하드웨어 공급자를 수동으로 등록하는 방법".

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 맨 위에 * Managed Hosts * 가 선택되어 있는지 확인합니다.
3. 추가 * 를 클릭합니다.
4. 호스트 페이지에서 다음을 수행합니다.

이 필드의 내용...	수행할 작업...
호스트 유형	호스트 유형으로 * Windows * 를 선택합니다. SnapCenter 서버는 호스트를 추가한 다음 호스트에 Windows용 플러그인 및 Exchange용 플러그인이 설치되어 있지 않은 경우 호스트에 설치합니다. Windows용 플러그인과 Exchange용 플러그인은 동일한 버전이어야 합니다. 다른 버전의 Windows용 플러그인이 이전에 설치된 경우 SnapCenter는 설치 과정에서 버전을 업데이트합니다.

이 필드의 내용...	수행할 작업...
호스트 이름입니다	FQDN(정규화된 도메인 이름) 또는 호스트의 IP 주소를 입력합니다. SnapCenter는 DNS의 올바른 구성에 따라 달라집니다. 따라서 가장 좋은 방법은 FQDN(정규화된 도메인 이름)을 입력하는 것입니다. IP 주소는 FQDN으로 확인되는 경우에만 신뢰할 수 없는 도메인 호스트에 대해 지원됩니다. SnapCenter를 사용하여 호스트를 추가하고 이 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다. 다음 중 하나의 IP 주소 또는 FQDN을 입력할 수 있습니다. • 독립 실행형 호스트 • Exchange DAG 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 주소 또는 FQDN을 제공하여 IP less DAG 클러스터를 추가합니다. ◦ 동일한 도메인 또는 다른 도메인에 상주하는 IP가 적은 DAG를 추가합니다. 이름은 같지만 도메인이 다른 여러 IP/IP가 없는 DAG를 추가할 수도 있습니다. 독립 실행형 호스트 또는 Exchange DAG(도메인 간 또는 동일한 도메인)의 경우 호스트 또는 DAG의 IP 주소 또는 FQDN을 제공하는 것이 좋습니다.

이 필드의 내용...	수행할 작업...
자격 증명	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성합니다. 자격 증명에 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 만들기에 대한 정보를 참조하십시오. 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 의해 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

   Exchange용 플러그인을 선택하면 Microsoft SQL Server용 SnapCenter 플러그인 선택이 자동으로 취소됩니다. 사용된 메모리 양과 Exchange에 필요한 기타 리소스 사용 때문에 SQL Server와 Exchange Server를 동일한 시스템에 설치하지 않는 것이 좋습니다.

6. (선택 사항) * 추가 옵션 * 을 클릭합니다.

이 필드의 내용...	수행할 작업...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정합니다. 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 입니다 `C:\Program Files\NetApp\SnapCenter`. 선택적으로 경로를 사용자 지정할 수 있습니다.
DAG의 모든 호스트를 추가합니다	DAG를 추가할 때 이 확인란을 선택합니다.
사전 설치 검사를 건너뜁니다	플러그인이 이미 수동으로 설치되어 있고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.

이 필드의 내용...	수행할 작업...
그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행합니다	그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행하려면 이 확인란을 선택합니다. GMSA 이름을 *domainName\accountName$* 형식으로 제공합니다. GMSA는 SnapCenter Plug-in for Windows 서비스에 대해서만 로그온 서비스 계정으로 사용됩니다.

7. 제출 * 을 클릭합니다.

   사전 검사 건너뛰기 확인란을 선택하지 않은 경우 호스트가 플러그인을 설치하기 위한 요구사항을 충족하는지 여부를 확인합니다. 최소 요구 사항이 충족되지 않으면 적절한 오류 또는 경고 메시지가 표시됩니다.

   오류가 디스크 공간 또는 RAM과 관련된 경우 에 있는 web.config 파일을 업데이트할 수 있습니다 `C:\Program Files\NetApp\SnapCenter` 기본값을 수정하려면 WebApp을 사용합니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.

   HA 설정에서 web.config 파일을 업데이트하는 경우 두 노드에서 파일을 업데이트해야 합니다.

8. 설치 과정을 모니터링합니다.

PowerShell cmdlet을 사용하여 SnapCenter Server 호스트에서 Exchange용 플러그인을 설치합니다

SnapCenter GUI에서 Exchange용 플러그인을 설치해야 합니다. GUI를 사용하지 않으려는 경우 SnapCenter 서버 호스트 또는 원격 호스트에서 PowerShell cmdlet을 사용할 수 있습니다.

시작하기 전에

- SnapCenter 서버가 설치 및 구성되어 있어야 합니다.
- 호스트 또는 관리 권한이 있는 사용자의 로컬 관리자여야 합니다.
- 플러그인, 설치 및 제거 권한이 있는 역할(예: SnapCenter 관리자)에 할당된 사용자여야 합니다
- Exchange용 플러그인을 설치하기 전에 설치 요구 사항 및 지원되는 구성 유형을 검토해야 합니다.
- Exchange용 플러그인을 설치할 호스트는 Windows 호스트여야 합니다.

단계

1. SnapCenter 서버 호스트에서 _Open-SmConnection_cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
2. 필요한 매개 변수와 함께 _Add-SmHost_cmdlet을 사용하여 Exchange용 플러그인을 설치할 호스트를 추가합니다.

   cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

호스트는 독립 실행형 호스트 또는 DAG일 수 있습니다. DAG를 지정하는 경우 _-IsDAG_매개 변수가 필요합니다.

3. 필요한 매개 변수와 함께 _Install-SmHostPackage_cmdlet을 사용하여 Exchange용 플러그인을 설치합니다.

   이 명령은 지정된 호스트에 Exchange용 플러그인을 설치한 다음 SnapCenter에 플러그인을 등록합니다.

명령줄에서 **Exchange**용 **SnapCenter** 플러그인을 자동으로 설치합니다

SnapCenter 사용자 인터페이스 내에서 Exchange용 플러그인을 설치해야 합니다. 그러나 어떤 이유로 인해 Windows 명령줄에서 자동 모드로 Exchange용 플러그인 설치 프로그램을 실행할 수 없습니다.

시작하기 전에

- Microsoft Exchange Server 리소스를 백업해야 합니다.
- SnapCenter 플러그인 패키지를 설치해야 합니다.
- 설치하기 전에 Microsoft SQL Server용 SnapCenter 플러그인의 이전 릴리즈를 삭제해야 합니다.

  자세한 내용은 을 참조하십시오 "플러그인 호스트에서 직접 SnapCenter 플러그인을 설치하는 방법".

단계

1. 플러그인 호스트에 _C:\temp_folder가 있고 로그인한 사용자가 이 폴더에 대한 모든 액세스 권한을 가지고 있는지 확인합니다.
2. C:\ProgramData\NetApp\SnapCenter\Package_Repository에서 Microsoft Windows용 SnapCenter 플러그인을 다운로드하십시오.

   이 경로는 SnapCenter 서버가 설치된 호스트에서 액세스할 수 있습니다.

3. 플러그인을 설치할 호스트에 설치 파일을 복사합니다.
4. 로컬 호스트의 Windows 명령 프롬프트에서 플러그인 설치 파일을 저장한 디렉토리로 이동합니다.
5. 다음 명령을 입력하여 플러그인을 설치합니다.

   _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_SERVICEPSCE=<설치 암호>

   예를 들면 다음과 같습니다.

   _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\SCVICE_PVICE.PCEWE_PCEBI 관리자, PVICE_PVICE_PCEWESTRW=PCEBI_PCEPCEPCEWE_PSHI=설치

   Exchange용 플러그인을 설치하는 동안 전달되는 모든 매개 변수는 대/소문자를 구분합니다.

   변수에 대해 다음 값을 입력합니다.

변수	값
_ /debuglog "<Debug_Log_Path> _	다음 예제와 같이 제품군 설치 관리자 로그 파일의 이름과 위치를 지정합니다. *Setup.exe /debuglog "C:\PathToLog\setupexe.log*
Bi_SNAPCENTER_PORT	SnapCenter가 SMCore와 통신하는 포트를 지정합니다.
Suite_INSTALLDIR	호스트 플러그인 패키지 설치 디렉토리를 지정합니다.
BI_서비스 계정	Microsoft Windows 웹 서비스 계정용 SnapCenter 플러그인을 지정합니다.
BI_세비셀	Microsoft Windows 웹 서비스 계정용 SnapCenter 플러그인 암호를 지정합니다.
ISFeatureInstall을 선택합니다	SnapCenter가 원격 호스트에 구축할 솔루션을 지정합니다.

6. Windows 작업 스케줄러, 기본 설치 로그 파일 *C:\Installdebug.log* 및 추가 설치 파일을 _C:\Temp_에서 모니터링합니다.
7. %temp%_ 디렉토리를 모니터링하여 _msiexe.exe_설치 프로그램이 오류 없이 소프트웨어를 설치하고 있는지 확인합니다.

Exchange용 플러그인을 설치하면 SnapCenter 서버가 아닌 호스트에 플러그인이 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록할 수 있습니다. 호스트가 추가되면 플러그인이 자동으로 검색됩니다.

SnapCenter 플러그인 패키지 설치 상태를 모니터링합니다

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행률을 모니터링할 수 있습니다. 설치 진행 상황을 확인하여 설치 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다

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 클릭합니다.
   b. 선택 사항: 시작 및 종료 날짜를 지정합니다.
   c. 유형 드롭다운 메뉴에서 * 플러그인 설치 * 를 선택합니다.
   d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
   e. 적용 * 을 클릭합니다.
4. 설치 작업을 선택하고 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. Job Details * 페이지에서 * View logs * 를 클릭합니다.

CA 인증서를 구성합니다

CA 인증서 CSR 파일을 생성합니다

CSR(인증서 서명 요청)을 생성하고 생성된 CSR을 사용하여 CA(인증 기관)에서 가져올 수 있는 인증서를 가져올 수 있습니다. 인증서에 연결된 개인 키가 있습니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.

CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 자세한 내용은 을 참조하십시오 "CA 인증서 CSR 파일을 생성하는 방법".

도메인(* .domain.company.com) 또는 시스템(machine1.domain.company.com CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter를 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN) 및 해당 호스트 이름을 CA 인증서에 언급해야 합니다. 인증서를 조달하기 전에 SAN(Subject Alternative Name) 필드를 채워 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(* .domain.company.com)의 경우 인증서에 도메인의 모든 호스트 이름이 암시적으로 포함됩니다.

CA 인증서를 가져옵니다

MMC(Microsoft Management Console)를 사용하여 CA 인증서를 SnapCenter 서버 및 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 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 단추로 클릭한 다음 * 모든 작업 * > * 가져오기 * 를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료합니다.

이 마법사 창에서...	다음을 수행합니다.
개인 키를 가져옵니다	예 * 옵션을 선택하고 개인 키를 가져온 다음 * 다음 * 을 클릭합니다.
파일 형식 가져오기	변경하지 않고 * 다음 * 을 클릭합니다.
보안	내보낸 인증서에 사용할 새 암호를 지정하고 * 다음 * 을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

인증서 가져오기는 개인 키와 함께 번들로 제공됩니다(지원되는 형식은 *.pfx, *.p12 및 *.p7b 입니다).

7. "개인" 폴더에 대해 5단계를 반복합니다.

CA 인증서 지문을 받습니다

인증서 thumbprint는 인증서를 식별하는 16진수 문자열입니다. 썸프린트는 썸프린트 알고리즘을 사용하여 인증서 컨텐츠에서 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.
   a. 인증서를 두 번 클릭합니다.
   b. 인증서 대화 상자에서 * 세부 정보 * 탭을 클릭합니다.
   c. 필드 목록을 스크롤하여 * Thumbprint * 를 클릭합니다.
   d. 상자에서 16진수 문자를 복사합니다.
   e. 16진수 사이의 공백을 제거합니다.

      예를 들어, 썸프린트가 "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 0d 42 77 A3 2a 7b"인 경우 공백을 제거한 후 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.
   a. 다음 명령을 실행하여 설치된 인증서의 엄지손가락 지문을 나열하고 최근 설치된 인증서를 주체 이름으로 식별합니다.

      Get-ChildItem-Path 인증:*LocalMachine\My*

   b. 엄지손가락 지문을 복사합니다.

Windows 호스트 플러그인 서비스를 사용하여 **CA** 인증서를 구성합니다

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스를 사용하여 CA 인증서를 구성해야 합니다.

SnapCenter 서버 및 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하여 기존 인증서 바인딩을 제거합니다.

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   예를 들면 다음과 같습니다.

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스와 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 들면 다음과 같습니다.

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

플러그인에 대해 **CA** 인증서를 활성화합니다

CA 인증서를 구성하고 SnapCenter 서버 및 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- run_Set-SmCertificateSettings_cmdlet을 사용하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- _get-SmCertificateSettings_를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 호스트 페이지에서 * 관리되는 호스트 * 를 클릭합니다.
3. 단일 또는 여러 플러그인 호스트를 선택합니다.
4. 추가 옵션 * 을 클릭합니다.
5. 인증서 유효성 검사 사용 * 을 선택합니다.

작업을 마친 후

관리 호스트 탭 호스트에는 자물쇠가 표시되고 자물쇠 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- 는 CA 인증서가 활성화되지 않았으며 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- CA 인증서의 유효성을 확인했음을 나타냅니다.
- CA 인증서의 유효성을 확인할 수 없음을 나타냅니다.
- 연결 정보를 검색할 수 없음을 나타냅니다.

상태가 노란색 또는 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

Exchange 및 SnapCenter에 대해 SnapManager 7.x가 공존하도록 구성합니다

Microsoft Exchange Server용 SnapCenter 플러그인을 Microsoft Exchange Server용 SnapManager와 함께 사용하려면 Microsoft Exchange Server용 SnapManager가 설치된 동일한 Exchange Server에 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하고 Exchange 일정에 대해 SnapManager를 사용하지 않도록 설정해야 합니다. 및 Microsoft Exchange Server용 SnapCenter 플러그인을 사용하여 새 일정 및 백업을 구성합니다.

시작하기 전에

- Microsoft Exchange Server용 SnapManager와 Windows용 SnapDrive가 이미 설치되어 있고 Microsoft Exchange Server용 SnapManager 백업이 시스템과 SnapInfo 디렉토리에 있습니다.
- 더 이상 필요하지 않은 Microsoft Exchange Server용 SnapManager에서 생성한 백업을 삭제하거나 회수해야 합니다.
- Windows 스케줄러에서 Microsoft Exchange Server용 SnapManager가 만든 모든 일정을 일시 중단하거나 삭제해야 합니다.
- Microsoft Exchange Server용 SnapCenter 플러그인과 Microsoft Exchange Server용 SnapManager가 동일한 Exchange Server에 공존할 수 있지만 기존 Microsoft Exchange Server용 SnapManager 설치를 SnapCenter로 업그레이드할 수는 없습니다.

  SnapCenter는 업그레이드 옵션을 제공하지 않습니다.

- SnapCenter는 SnapManager for Microsoft Exchange Server 백업에서 Exchange 데이터베이스 복원을 지원하지 않습니다.

  Microsoft Exchange Server용 SnapCenter 플러그인 설치 후 Microsoft Exchange Server용 SnapManager를 제거하지 않고 나중에 Microsoft Exchange Server용 SnapManager 백업을 복원하려면 추가 단계를 수행해야 합니다.

단계

1. 모든 DAG 노드에서 PowerShell을 사용하여 SnapDrive for Windows VSS Hardware Provider가 등록되었는지 여부를 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 SnapDrive for Windows에서 VSS 하드웨어 공급자 등록을 취소합니다. *navssprv.exe -r service –u*
3. VSS Hardware Provider가 제거되었는지 확인합니다. _ vssadmin list providers _
4. SnapCenter에 Exchange 호스트를 추가한 다음 Microsoft Windows용 SnapCenter 플러그인 및 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 SnapManager를 중지합니다.
7. SnapCenter GUI를 사용하여 필요 시 백업을 생성하고, 예약된 백업을 구성하고, 보존 설정을 구성합니다.
8. Microsoft Exchange Server용 SnapManager를 제거합니다.

   Microsoft Exchange Server용 SnapManager를 지금 제거하지 않고 나중에 Microsoft Exchange Server용 SnapManager 백업을 복원하려는 경우:

   a. 모든 DAG 노드에서 Microsoft Exchange Server용 SnapCenter 플러그인 등록 취소: _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 SnapDrive for Windows를 등록합니다. _navssprv.exe -r service -a hostname \\username -p password _

VMware vSphere용 SnapCenter 플러그인을 설치합니다

데이터베이스가 가상 머신(VM)에 저장되어 있거나 VM 및 데이터 저장소를 보호하려는 경우 SnapCenter Plug-in for VMware vSphere 가상 어플라이언스를 구축해야 합니다.

배포에 대한 자세한 내용은 을 참조하십시오 "구축 개요".

CA 인증서를 배포합니다

VMware vSphere용 SnapCenter 플러그인을 사용하여 CA 인증서를 구성하려면 를 참조하십시오 "SSL 인증서를 생성하거나 가져옵니다".

CRL 파일을 구성합니다

VMware vSphere용 SnapCenter 플러그인은 사전 구성된 디렉토리에서 CRL 파일을 찾습니다. VMware vSphere용 SnapCenter 플러그인의 기본 CRL 파일 디렉토리는 */opt/netapp/config/CRL* 입니다.

이 디렉터리에 둘 이상의 CRL 파일을 배치할 수 있습니다. 들어오는 인증서는 각 CRL에 대해 확인됩니다.

데이터 보호를 준비합니다

백업, 클론 복제 또는 복원 작업과 같은 데이터 보호 작업을 수행하기 전에 전략을 정의하고 환경을 설정해야 합니다. SnapVault 서버에서 SnapMirror 및 SnapCenter 기술을 사용하도록 설정할 수도 있습니다.

SnapVault 및 SnapMirror 기술을 활용하려면 스토리지 장치의 소스 볼륨과 타겟 볼륨 간의 데이터 보호 관계를 구성하고 초기화해야 합니다. NetAppSystem Manager를 사용하거나 스토리지 콘솔 명령줄을 사용하여 이러한 작업을 수행할 수 있습니다.

- 자세한 정보 찾기 *

"REST API 시작하기"

Microsoft Exchange Server용 SnapCenter 플러그인 사용을 위한 사전 요구 사항

Exchange용 플러그인을 사용하기 전에 SnapCenter 관리자가 SnapCenter 서버를 설치 및 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다.
- SnapCenter에 로그인합니다.

- 스토리지 시스템 접속을 추가하거나 할당하고 자격 증명을 생성하여 SnapCenter 환경을 구성합니다.

  SnapCenter은 서로 다른 클러스터에서 동일한 이름의 여러 SVM을 지원하지 않습니다. SnapCenter에서 지원하는 각 SVM에는 고유한 이름이 있어야 합니다.

- 호스트를 추가하고, Microsoft Windows용 SnapCenter 플러그인 및 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하고, 리소스를 검색(새로 고침)합니다.
- Microsoft Windows용 SnapCenter 플러그인을 사용하여 호스트 측 스토리지 프로비저닝을 수행합니다.
- SnapCenter 서버를 사용하여 VMware RDM LUN에 상주하는 Exchange 데이터베이스를 보호하는 경우 VMware vSphere용 SnapCenter 플러그인을 구축하고 SnapCenter에 플러그인을 등록해야 합니다. 자세한 내용은 VMware vSphere용 SnapCenter 플러그인 설명서를 참조하십시오.

  VMDK는 지원되지 않습니다.

- Microsoft Exchange 도구를 사용하여 로컬 디스크에서 지원되는 스토리지로 기존 Microsoft Exchange Server 데이터베이스를 이동합니다.
- 백업 복제를 원하는 경우 SnapMirror 및 SnapVault 관계를 설정합니다.

SnapCenter 4.1.1 사용자의 경우 VMware vSphere 4.1.1 용 SnapCenter 플러그인 설명서에 가상화 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 나와 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 VMware vSphere용 SnapCenter 플러그인을 사용하여 가상화된 데이터베이스 및 파일 시스템을 보호하는 방법에 대한 정보가 수록되어 있습니다. SnapCenter 4.3.x 사용자의 경우 SnapCenter Plug-in for VMware vSphere 4.3 설명서에는 Linux 기반 SnapCenter Plug-in for VMware vSphere 가상 어플라이언스(오픈 가상 어플라이언스 형식)를 사용하여 가상화된 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 수록되어 있습니다.

"VMware vSphere용 SnapCenter 플러그인 설명서"

리소스, 리소스 그룹 및 정책을 사용하여 **Exchange Server**를 보호하는 방법

SnapCenter를 사용하기 전에 수행할 백업, 복구 및 재시딩된 작업과 관련된 기본 개념을 이해하는 것이 좋습니다. 서로 다른 작업을 위해 리소스, 리소스 그룹 및 정책과 상호 작용합니다.

- 리소스는 일반적으로 SnapCenter를 사용하여 백업하는 메일박스 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.

  자원 그룹에 대해 작업을 수행할 때 자원 그룹에 지정한 일정에 따라 자원 그룹에 정의된 자원에 대해 해당 작업을 수행합니다.

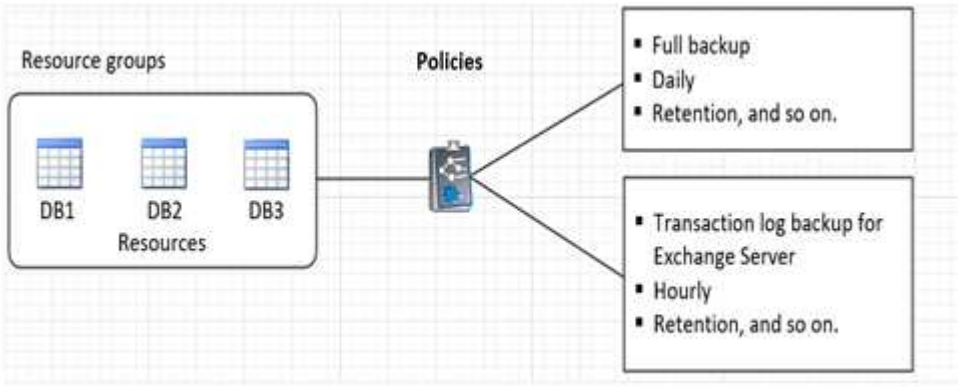
  필요에 따라 단일 리소스 또는 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 수행할 수도 있습니다.

  리소스 그룹은 이전에 데이터 세트라고 했습니다.

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

  자원 그룹을 만들 때 해당 그룹에 대해 하나 이상의 정책을 선택합니다. 단일 리소스에 대해 필요 시 백업을 수행할 때 하나 이상의 정책을 선택할 수도 있습니다.

보호하려는_대상_과 이를 보호할 시기를 요일과 시간으로 정의하는 자원 그룹을 생각해 보십시오. 정책을 정의하는 _ 방법 _ 을(를) 보호하려는 것으로 생각해 보십시오. 예를 들어, 호스트의 모든 데이터베이스를 백업하는 경우 호스트의 모든 데이터베이스를 포함하는 리소스 그룹을 생성할 수 있습니다. 그런 다음 리소스 그룹에 일별 정책과 시간별 정책이라는 두 가지 정책을 연결할 수 있습니다. 리소스 그룹을 생성하고 정책을 연결할 때 매일 전체 백업을 수행하고 로그 백업을 매시간 수행하는 다른 일정을 수행하도록 리소스 그룹을 구성할 수 있습니다. 다음 그림에서는 데이터베이스 리소스, 리소스 그룹 및 정책 간의 관계를 보여 줍니다.



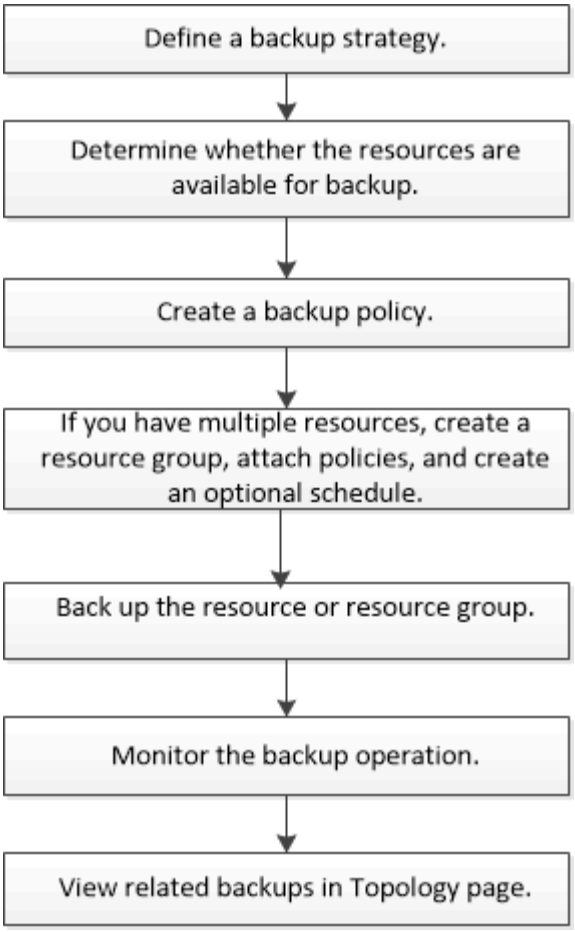
Exchange 리소스를 백업합니다

백업 워크플로우

사용자 환경에 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하면 SnapCenter를 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 볼륨의 액티브 및 패시브 백업 복사본은 지원되지 않습니다.

다음 워크플로에서는 백업 작업을 수행해야 하는 순서를 보여 줍니다.



Exchange 데이터베이스 및 백업 검증

Microsoft Exchange Server용 SnapCenter 플러그인은 백업 검증을 제공하지 않지만 Exchange와 함께 제공되는 Eseutil 도구를 사용하여 Exchange 데이터베이스 및 백업을 확인할 수 있습니다.

Microsoft Exchange Eseutil 도구는 Exchange 서버에 포함된 명령줄 유틸리티입니다. 이 유틸리티를 사용하면 정합성 검사를 수행하여 Exchange 데이터베이스 및 백업의 무결성을 확인할 수 있습니다.

* 모범 사례: * 적어도 두 개 이상의 복제본이 있는 DAG(데이터베이스 가용성 그룹) 구성의 일부인 데이터베이스에 대해 일관성 검사를 수행할 필요는 없습니다.

자세한 내용은 을 참조하십시오 "Microsoft Exchange Server 설명서를 참조하십시오".

Exchange 리소스를 백업에 사용할 수 있는지 여부를 확인합니다

리소스는 사용자가 설치한 플러그인에서 유지 관리하는 데이터베이스, Exchange 데이터베이스 가용성 그룹입니다. 이러한 리소스를 리소스 그룹에 추가하여 데이터 보호 작업을 수행할 수 있지만 먼저 사용 가능한 리소스를 확인해야 합니다. 사용 가능한 리소스를 확인하면 플러그인 설치가 성공적으로 완료되었는지 확인할 수도 있습니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 접속 생성, 자격 증명 추가 및 Exchange용 플러그인 설치와 같은 작업을 이미 완료해야 합니다.
- Single Mailbox Recovery 소프트웨어 기능을 사용하려면 Single Mailbox Recovery 소프트웨어가 설치된 Exchange Server에 활성 데이터베이스를 설치해야 합니다.
- 데이터베이스가 VMware RDM LUN에 상주하는 경우 VMware vSphere용 SnapCenter 플러그인을 구축하고 SnapCenter에 플러그인을 등록해야 합니다. 를 클릭합니다 "VMware vSphere용 SnapCenter 플러그인 설명서" 자세한 정보가 있습니다.

이 작업에 대해

- Details 페이지의 * Overall Status * 옵션이 Not Available for backup으로 설정되어 있으면 데이터베이스를 백업할 수 없습니다. 다음 중 하나라도 해당하면 * Overall Status *(전체 상태 *) 옵션이 Not Available(백업 불가)로 설정됩니다.
  - 데이터베이스가 NetApp LUN에 없습니다.
  - 데이터베이스가 정상 상태가 아닙니다.

    데이터베이스가 마운트, 마운트 해제, 다시 시드되거나 복구 보류 상태인 경우 정상 상태가 아닙니다.
- DAG(Database Availability Group)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 위 모서리에 있는 플러그인 드롭다운 목록에서 * Microsoft Exchange Server * 를 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 * 데이터베이스 * 또는 * 데이터베이스 가용성 그룹 * 또는 * 리소스 그룹 * 을 선택합니다.

   모든 데이터베이스와 DAG는 DAG 또는 호스트 이름과 함께 FQDN 형식으로 표시되므로 여러 데이터베이스를 구별할 수 있습니다.

   을 클릭합니다  호스트 이름과 Exchange Server를 선택하여 리소스를 필터링합니다. 그런 다음 을 클릭할 수 있습니다  를 눌러 필터 창을 닫습니다.
3. 리소스 새로 고침 * 을 클릭합니다.

   새로 추가, 이름 변경 또는 삭제된 리소스가 SnapCenter 서버 인벤토리로 업데이트됩니다.

   데이터베이스가 SnapCenter 외부에서 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

   리소스는 리소스 이름, 데이터베이스 가용성 그룹 이름, 데이터베이스가 현재 활성 상태인 서버, 복제본이 있는 서버, 마지막 백업 시간 및 전체 상태 등의 정보와 함께 표시됩니다.

   - 데이터베이스가 비 NetApp 스토리지에 있는 경우 백업을 사용할 수 없음 이 전체 상태 열에 표시됩니다.

     DAG에서 액티브 데이터베이스 복제본이 타사 스토리지에 있고 하나 이상의 패시브 데이터베이스 복제본이 NetApp 스토리지에 있는 경우 보호되지 않음 이 * Overall Status * 열에 표시됩니다.

   NetApp이 아닌 스토리지 유형에 있는 데이터베이스에는 데이터 보호 작업을 수행할 수 없습니다.

   - 데이터베이스가 NetApp 스토리지에 있고 보호되지 않는 경우 * Overall Status * 열에 보호되지 않음 이

표시됩니다.

- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되어 있는 경우 사용자 인터페이스에 **Overall Status** 열에 Backup not run 메시지가 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있으며 보호되어 있고 데이터베이스에 대한 백업이 트리거된 경우 사용자 인터페이스에 * Overall Status * 열에 Backup Succeeded 메시지가 표시됩니다.

Exchange Server 데이터베이스에 대한 백업 정책을 생성합니다

SnapCenter를 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 참조하십시오.

- SnapCenter 설치, 호스트 추가, 리소스 식별 및 스토리지 시스템 접속 생성과 같은 작업을 완료하여 데이터 보호를 위한 준비를 갖추어야 합니다.
- Exchange Server 리소스를 새로 고친(검색된) 상태여야 합니다.
- 스냅샷 복사본을 미러 또는 볼트에 복제하는 경우 SnapCenter 관리자는 소스 볼륨과 타겟 볼륨 모두에 SVM(스토리지 가상 머신)을 할당해야 합니다.
- powershell 스크립트를 pare pts 및 postscripts로 실행하려면 의 값을 설정해야 합니다 `usePowershellProcessforScripts` 매개 변수는 에서 TRUE로 설정합니다 `web.config` 파일.

  기본값은 false 입니다

이 작업에 대해

- 백업 정책은 백업을 관리 및 유지하는 방법과 리소스 또는 리소스 그룹을 백업하는 빈도를 제어하는 규칙의 집합입니다. 또한 스크립트 설정을 지정할 수도 있습니다. 정책에 옵션을 지정하면 다른 리소스 그룹에 대한 정책을 다시 사용할 때 시간이 절약됩니다.
- 전체 백업 보존은 특정 정책에 따라 다릅니다. 정책 A를 사용하여 전체 백업 보존 기간이 4인 데이터베이스 또는 리소스는 전체 백업 4개를 보유하며 동일한 데이터베이스 또는 리소스에 대해 정책 B에 영향을 미치지 않습니다. 이 경우 3개의 전체 백업을 유지하기 위해 보존 기간이 3일 수 있습니다.
- 로그 백업 보존은 정책에 따라 효과적이며 데이터베이스 또는 리소스의 모든 로그 백업에 적용됩니다. 따라서 정책 B를 사용하여 전체 백업을 수행할 경우 로그 보존 설정은 정책 A가 동일한 데이터베이스 또는 리소스에 생성한 로그 백업에 영향을 줍니다. 마찬가지로 정책 A의 로그 보존 설정은 정책 B가 동일한 데이터베이스의 로그 백업에 영향을 줍니다.
- 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 swagger에서 API:API/4.7/configsettings를 통해 표시할 수 있습니다

  Get API를 사용하여 키 값을 표시할 수 있습니다. API 설정은 지원되지 않습니다.

* 모범 사례: * 보존하려는 전체 및 로그 백업 수에 따라 보조 보존 정책을 구성하는 것이 좋습니다. 2차 보존 정책을 구성할 때는 데이터베이스와 로그가 서로 다른 볼륨에 있을 때 각 백업마다 3개의 스냅샷 복사본을 가질 수 있고 데이터베이스와 로그가 같은 볼륨에 있을 때는 각 백업마다 2개의 스냅샷 복사본을 가질 수 있다는 점을 유의해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
2. 설정 페이지에서 * 정책 * 을 클릭합니다.
3. 새로 만들기 * 를 클릭합니다.
4. 이름 페이지에 정책 이름과 설명을 입력합니다.
5. 백업 유형 페이지에서 다음 단계를 수행하십시오.

    a. 백업 유형 선택:

원하는 작업	수행할 작업...
데이터베이스 파일 및 필요한 트랜잭션 로그를 백업합니다	전체 백업 및 로그 백업 * 을 선택합니다. 데이터베이스는 로그 잘라내기를 통해 백업되며 잘린 로그를 포함하여 모든 로그가 백업됩니다. ⓘ 권장되는 백업 유형입니다.
데이터베이스 파일 및 커밋되지 않은 트랜잭션 로그를 백업합니다	전체 백업 * 을 선택합니다. 데이터베이스는 로그 잘라내기를 통해 백업되며 잘린 로그는 백업되지 않습니다.
모든 트랜잭션 로그를 백업합니다	Log backup * 을 선택합니다. 활성 파일 시스템의 모든 트랜잭션 로그가 백업되며 로그 잘라내기가 없습니다. _scebackupinfo_directory가 라이브 로그와 동일한 디스크에 생성됩니다. 이 디렉토리에는 Exchange 데이터베이스의 증가분 변경 사항에 대한 포인터가 포함되어 있으며 전체 로그 파일과 동일하지는 않습니다.
트랜잭션 로그 파일을 자르지 않고 모든 데이터베이스 파일 및 트랜잭션 로그를 백업합니다	백업 복사 * 를 선택합니다. 모든 데이터베이스 및 모든 로그가 백업되며 로그 잘라내기가 없습니다. 일반적으로 이 백업 유형을 사용하여 복제본을 다시 시드하거나 문제를 테스트 또는 진단할 수 있습니다.

UTM(최신) 보존이 아닌 전체 백업 보존을 기준으로 로그 백업에 필요한 공간을 정의해야 합니다.

Exchange 볼륨(LUN)을 처리할 때 로그 및 데이터베이스에 대해 별도의 볼트 정책을 생성하고 동일한 레이블을 사용하여 로그 정책의 유지(보존)를 데이터베이스 정책으로 각 레이블에 대해 두 배로 설정합니다. 자세한 내용은 다음을 참조하십시오. "Exchange 백업용 SnapCenter는 볼트 대상 로그 볼륨에 스냅샷의 절반만 유지합니다"

b. 데이터베이스 사용 가능 그룹 설정 섹션에서 작업을 선택합니다.

이 필드의 내용...	수행할 작업...
활성 복사본을 백업합니다	선택한 데이터베이스의 활성 사본만 백업하려면 이 옵션을 선택합니다. DAG(데이터베이스 가용성 그룹)의 경우 이 옵션은 DAG에 있는 모든 데이터베이스의 액티브 복제본만 백업합니다. 패시브 복사본은 백업되지 않습니다.
백업 작업 생성 시 선택할 서버의 복사본을 백업합니다	활성 서버와 수동 서버 모두에서 선택한 서버의 데이터베이스 복사본을 백업하려면 이 옵션을 선택합니다. DAG의 경우 이 옵션은 선택한 서버에 있는 모든 데이터베이스의 액티브 복제본과 패시브 복제본을 모두 백업합니다.

클러스터 구성에서 백업은 정책에 설정된 보존 설정에 따라 클러스터의 각 노드에 유지됩니다. 클러스터의 소유자 노드가 변경되면 이전 소유자 노드의 백업이 유지됩니다. 보존은 노드 레벨에서만 적용됩니다.

c. 일정 빈도 섹션에서 * On demand *, * Hourly *, * Daily *, * Weekly *, * Monthly * 등의 빈도 유형을 하나 이상 선택합니다.

리소스 그룹을 생성하는 동안 백업 작업의 스케줄(시작 날짜, 종료 날짜)을 지정할 수 있습니다. 이렇게 하면 동일한 정책 및 백업 빈도를 공유하는 리소스 그룹을 생성할 수 있지만 각 정책에 서로 다른 백업 스케줄을 할당할 수 있습니다.

오전 2시에 예약된 경우 DST(일광 절약 시간) 중에는 일정이 트리거되지 않습니다.

6. 보존 페이지에서 보존 설정을 구성합니다.

표시되는 옵션은 이전에 선택한 백업 유형 및 빈도 유형에 따라 달라집니다.

최대 보존 값은 ONTAP 9.4 이상의 리소스에 대해 1018이고, ONTAP 9.3 이전 버전의 리소스에 대해서는 254입니다. 보존이 기본 ONTAP 버전에서 지원하는 값보다 높은 값으로 설정된 경우 백업이 실패합니다.

SnapVault 복제를 설정하려면 보존 수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷 복사본이 타겟으로 복제될 때까지 첫 번째 스냅샷 복사본이 SnapVault 관계의 참조 스냅샷 복사본이므로 보존 작업이 실패할 수 있습니다.

a. 로그 백업 보존 설정 섹션에서 다음 중 하나를 선택합니다.

원하는 작업	수행할 작업...
특정 수의 로그 백업만 유지합니다	로그가 유지되는 전체 백업 수 * 를 선택하고 최신 복원 기능을 원하는 전체 백업 수를 지정합니다. UTM(최신) 보존은 전체 또는 로그 백업을 통해 생성된 로그 백업에 적용됩니다. 예를 들어, UTM 보존 설정이 마지막 5개의 전체 백업의 로그 백업을 유지하도록 구성된 경우 마지막 5개의 전체 백업의 로그 백업이 보존됩니다. 전체 및 로그 백업의 일부로 생성된 로그 폴더는 UTM의 일부로 자동으로 삭제됩니다. 로그 폴더는 수동으로 삭제할 수 없습니다. 예를 들어 전체 또는 전체 및 로그 백업의 보존 설정이 1개월로 설정되고 UTM 보존이 10일로 설정된 경우, UTM에 따라 이러한 백업의 일부로 생성된 로그 폴더가 삭제됩니다. 따라서 10일 로그 폴더만 있고 다른 모든 백업은 시점 복원으로 표시됩니다. 최신 복원을 수행하지 않으려는 경우 UTM 보존 값을 0으로 설정할 수 있습니다. 그러면 시점 복원 작업이 활성화됩니다. • 모범 사례: * 전체 백업 보존 설정 섹션의 전체 스냅샷 복사본(전체 백업) 설정과 같은 설정을 사용하는 것이 좋습니다. 이렇게 하면 각 전체 백업에 대해 로그 파일이 유지됩니다.
백업 사본을 특정 기간 동안 보관합니다	Keep log backups for Last * 옵션을 선택하고 로그 백업 사본을 보관할 일 수를 지정합니다. 전체 백업 일수까지 로그 백업이 보존됩니다.

백업 유형으로 * 로그 백업 * 을 선택한 경우 로그 백업은 전체 백업에 대한 최신 보존 설정의 일부로 보존됩니다.

b. 전체 백업 보존 설정 섹션에서 필요 시 백업에 대해 다음 중 하나를 선택한 다음 전체 백업에 대해 하나를 선택합니다.

이 필드의 내용...	수행할 작업...
특정 수의 스냅샷 복사본만 보유합니다	유지할 전체 백업 수를 지정하려면 * 유지할 총 스냅샷 복사본 * 옵션을 선택하고 유지할 스냅샷 복사본(전체 백업) 수를 지정합니다. 전체 백업 수가 지정된 수를 초과하면 지정된 수를 초과하는 전체 백업이 삭제되며 가장 오래된 복제본이 먼저 삭제됩니다.
특정 기간 동안 전체 백업을 보존합니다	스냅샷 복사본 보관 * 옵션을 선택하고 스냅샷 복사본을 보관할 일 수(전체 백업)를 지정합니다.

DAG 구성에서 호스트에 대한 전체 백업이 없는 로그 백업만 있는 데이터베이스가 있는 경우 로그 백업은 다음과 같은 방식으로 유지됩니다.

- 기본적으로 SnapCenter는 DAG의 다른 모든 호스트에서 이 데이터베이스에 대해 가장 오래된 전체 백업을 찾고 전체 백업 전에 이 호스트에서 수행된 모든 로그 백업을 삭제합니다.
- DAG의 호스트에 있는 데이터베이스의 기본 보존 동작은 _C:\Program Files\NetApp\SnapCenter WebApp\web.config_file에 * MaxLogBackupOnlyWithoutFullBackup * 키를 추가하여 로그 백업만 사용하여 재정의할 수 있습니다.

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

이 예에서 값 10은 호스트에 최대 10개의 로그 백업을 유지하는 것을 의미합니다.

7. 복제 페이지에서 다음 보조 복제 옵션 중 하나 또는 둘 다를 선택합니다.

이 필드의 내용...	수행할 작업...
로컬 스냅샷 복사본을 생성한 후 SnapMirror를 업데이트합니다	백업 세트의 미러 복사본을 다른 볼륨(SnapMirror)에 유지하려면 이 옵션을 선택합니다.
로컬 스냅샷 복사본을 생성한 후 SnapVault를 업데이트합니다	디스크 간 백업 복제를 수행하려면 이 옵션을 선택합니다.

이 필드의 내용...	수행할 작업...
보조 정책 레이블입니다	스냅샷 레이블을 선택합니다. 선택한 스냅샷 복사본 레이블에 따라 ONTAP에서는 해당 레이블과 일치하는 2차 스냅샷 복사본 보존 정책을 적용합니다. 로컬 스냅샷 복사본 * 을 생성한 후 SnapMirror 업데이트 * 를 선택한 경우, 선택적으로 보조 정책 레이블을 지정할 수 있습니다. 그러나 로컬 스냅샷 복사본 * 을 생성한 후 * SnapVault 업데이트 * 를 선택한 경우에는 보조 정책 레이블을 지정해야 합니다.
오류 재시도 횟수입니다	프로세스가 중지되기 전에 수행해야 하는 복제 시도 횟수를 입력합니다.

보조 스토리지에 대한 ONTAP의 SnapMirror 보존 정책을 구성하면 보조 스토리지에서 스냅샷 복사본의 최대 제한에 도달하지 않도록 해야 합니다.

8. 스크립트 페이지에서 백업 작업 전후에 실행해야 하는 처방인 또는 PS의 경로와 인수를 각각 입력합니다.
   - Prescript 백업 인수에는 ""$Database" 및 ""$ServerInstance" 가 포함됩니다.
   - 포스트스크립트 백업 인수에는 ""$Database", "$ServerInstance", "$BackupName", "$LogDirectory" 및 "$LogSnapshot""이 포함됩니다.

     스크립트를 실행하여 SNMP 트랩을 업데이트하고, 경고를 자동화하고, 로그를 보내는 등의 작업을 수행할 수 있습니다.

     처방자 또는 사후 스크립트 경로에는 드라이브 또는 공유가 포함되어서는 안 됩니다. 경로는 scripts_path에 상대해야 합니다.
9. 요약을 검토하고 * Finish * 를 클릭합니다.

리소스 그룹을 생성하고 **Exchange Server**에 대한 정책을 연결합니다

모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한 수행할 데이터 보호 작업의 유형과 보호 스케줄을 정의하려면 하나 이상의 정책을 리소스 그룹에 연결해야 합니다.

이 작업에 대해

- 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 swagger에서 API:API/4.7/configsettings를 통해 표시할 수 있습니다

Get API를 사용하여 키 값을 표시할 수 있습니다. API 설정은 지원되지 않습니다.

단계

1. 왼쪽 탐색 창에서 * Resources * 를 클릭한 다음 목록에서 Microsoft Exchange Server 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 데이터베이스 * 를 선택합니다.

   최근에 SnapCenter에 리소스를 추가한 경우 * 리소스 새로 고침 * 을 클릭하여 새로 추가된 리소스를 확인합니다.

3. 새 리소스 그룹 * 을 클릭합니다.
4. 이름 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
이름	자원 그룹 이름을 입력합니다. 리소스 그룹 이름은 250자를 초과할 수 없습니다.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력합니다. 예를 들어 HR을 여러 자원 그룹에 태그로 추가하면 나중에 HR 태그와 연결된 모든 자원 그룹을 찾을 수 있습니다.
스냅샷 복사본에 대해 사용자 지정 이름 형식을 사용합니다	선택 사항: 사용자 지정 스냅샷 복사본의 이름 및 형식을 입력합니다. 예를 들어, _customtext_resourcegroup_policy_hostname_or_resourcegroup_hostname_입니다. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.

5. 리소스 페이지에서 다음 단계를 수행하십시오.
   a. 사용 가능한 리소스 목록을 필터링하려면 리소스 유형과 드롭다운 목록에서 데이터베이스 사용 가능 그룹을 선택합니다.

      최근에 추가한 자원은 자원 목록을 새로 고친 후에만 사용 가능한 자원 목록에 나타납니다.

      Available Resources and Selected Resources 섹션에 호스트의 FQDN과 함께 데이터베이스 이름이 표시됩니다. 이 FQDN은 데이터베이스가 특정 호스트에서 활성화되어 있으며 이 호스트에서 백업을 수행할 수 없음을 나타냅니다. 정책에서 백업 작업 생성 시 선택할 * 서버의 백업 복사본 * 옵션을 선택한 경우 백업할 서버 선택 옵션에서 하나 이상의 백업 서버를 선택해야 합니다.

b. 검색 텍스트 상자에 리소스 이름을 입력하거나 스크롤하여 리소스를 찾습니다.

c. 사용 가능한 리소스 섹션에서 선택한 리소스 섹션으로 리소스를 이동하려면 다음 단계 중 하나를 수행합니다.

- 동일한 스토리지 볼륨에 있는 모든 리소스를 선택한 리소스 섹션으로 이동하려면 * 동일한 스토리지 볼륨에 있는 모든 리소스를 자동 선택 * 을 선택합니다.
- 사용 가능한 리소스 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 클릭하여 선택한 리소스 섹션으로 이동합니다.

Microsoft Exchange Server용 SnapCenter의 리소스 그룹은 스냅샷 복사본당 30개 이상의 데이터베이스를 가질 수 없습니다. 하나의 리소스 그룹에 30개 이상의 데이터베이스가 있는 경우 추가 데이터베이스를 위해 두 번째 스냅샷 복사본이 생성됩니다. 따라서 기본 백업 작업 아래에 2개의 하위 작업이 생성됩니다. 보조 복제가 있는 백업의 경우 SnapMirror 또는 SnapVault 업데이트가 진행 중일 때 두 하위 작업의 업데이트가 겹치는 시나리오가 있을 수 있습니다. 로그가 작업이 완료되었음을 나타내더라도 기본 백업 작업은 계속 계속 실행됩니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

* 를 클릭하여 정책을 생성할 수도 있습니다 + *.

백업 작업 생성 시 선택할 서버에 대한 * 백업 복사본 * 옵션이 정책에 포함된 경우 하나 이상의 서버를 선택할 수 있는 서버 선택 옵션이 표시됩니다. 서버 선택 옵션에는 선택한 데이터베이스가 NetApp 스토리지에 있는 서버만 나열됩니다.

선택한 정책에 대한 스케줄 구성 섹션에 선택한 정책이 나열됩니다.

b. 선택한 정책에 대한 일정 구성 섹션에서 * 를 클릭합니다 + 일정을 구성하려는 정책에 대한 * 스케줄 구성 * 열에 있습니다.

c. policy_policy_name_schedules 추가 대화 상자에서 시작 날짜, 만료 날짜 및 빈도를 지정하여 스케줄을 구성한 다음 * 확인 * 을 클릭합니다.

정책에 나열된 각 빈도에 대해 이 작업을 수행해야 합니다. 구성된 스케줄은 선택한 정책에 대한 스케줄 구성 섹션의 * Applied Schedules * 열에 나열됩니다.

타사 백업 스케줄은 SnapCenter 백업 스케줄과 겹치는 경우 지원되지 않습니다.

7. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 자원 그룹에서 수행된 작업의 보고서를 첨부하려면 * 작업 보고서 첨부 * 를 선택합니다.

이메일 알림의 경우 GUI 또는 PowerShell 명령을 사용하여 SMTP 서버 세부 정보를 지정해야 합니다 `Set-SmSmtpServer`.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

8. 요약을 검토하고 * Finish * 를 클릭합니다.

Exchange 데이터베이스를 백업합니다

데이터베이스가 리소스 그룹에 속하지 않은 경우 리소스 페이지에서 데이터베이스 또는 데이터베이스 가용성 그룹을 백업할 수 있습니다.

시작하기 전에

- 백업 정책을 만들어야 합니다.
- 백업 작업에서 사용 중인 애그리게이트를 데이터베이스에서 사용하는 SVM에 할당해야 합니다.
- 2차 스토리지와 SnapMirror 관계가 있는 리소스를 백업하려면 스토리지 사용자에게 할당된 역할에 "'스냅샷 전체' 권한이 있어야 합니다. 그러나 "vsadmin" 역할을 사용하는 경우에는 "napmirror all" 권한이 필요하지 않습니다.
- NetApp 및 비 NetApp 스토리지에 액티브/패시브 데이터베이스 복사본이 있는 데이터베이스 또는 데이터베이스 가용성 그룹의 백업을 수행하려면 정책에서 백업 작업 생성 시간 * 동안 선택할 서버의 활성 복사본 * 백업 * 또는 * 백업 복사본 * 옵션을 선택한 경우 백업 작업이 경고 상태로 전환됩니다. 백업이 NetApp 스토리지의 액티브/패시브 데이터베이스 복사본에 대해 성공하고 NetApp이 아닌 타사 스토리지의 액티브/패시브 데이터베이스 복사본에 대해서는 백업이 실패합니다.

  * 모범 사례: * 활성 및 수동 데이터베이스의 백업을 동시에 실행하지 마십시오. 경쟁 조건이 발생할 수 있으며 백업 중 하나가 실패할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 * Microsoft Exchange Server 플러그인 * 을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 데이터베이스 * 또는 * 데이터베이스 가용성 그룹 * 을 선택합니다.

   리소스 페이지에서 을(를) 선택합니다  아이콘은 데이터베이스가 비NetApp 스토리지에 있음을 나타냅니다.

   DAG에서 액티브 데이터베이스 복제본이 타사 스토리지에 있고 하나 이상의 패시브 데이터베이스 복제본이 NetApp 스토리지에 상주하는 경우 데이터베이스를 보호할 수 있습니다.

   를 클릭합니다  를 누른 다음 호스트 이름과 데이터베이스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 * 를 클릭할 수 있습니다  를 눌러 필터 창을 닫습니다.

   - 데이터베이스를 백업하려면 데이터베이스 이름을 클릭합니다.
     i. 토폴로지 뷰가 표시되면 * 보호 * 를 클릭합니다.
     ii. 데이터베이스 보호 리소스 마법사가 표시되면 3단계를 계속 진행합니다.
   - 데이터베이스 가용성 그룹을 백업하려면 데이터베이스 가용성 그룹 이름을 클릭합니다.
3. 사용자 지정 스냅샷 복사본 이름을 지정하려면 리소스 페이지에서 * 스냅샷 복사본에 사용자 지정 이름 형식 사용 * 확인란을 선택한 다음 스냅샷 복사본 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

   예: *customtext_policy_hostname_or_resource_hostname*. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.

4. 정책 페이지에서 다음 단계를 수행합니다.

   a. 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

* 를 클릭하여 정책을 생성할 수도 있습니다 + *.

백업 작업 생성 시 선택할 서버에 대한 * 백업 복사본 * 옵션이 정책에 포함된 경우 하나 이상의 서버를 선택할 수 있는 서버 선택 옵션이 표시됩니다. 서버 선택 옵션에는 선택한 데이터베이스가 NetApp 스토리지에 있는 서버만 나열됩니다.

선택한 정책에 대한 스케줄 구성 섹션에 선택한 정책이 나열됩니다.

b. + 를 클릭합니다 일정을 구성하려는 정책에 대한 스케줄 구성 열의

c. policy_policy_name_에 대한 스케줄 추가 창에서 스케줄을 구성한 다음 * 확인 * 을 클릭합니다.

여기서, _policy_name_은 선택한 정책의 이름입니다.

구성된 일정이 Applied Schedules 열에 나열됩니다.

5. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 리소스에 대해 수행된 백업 작업의 보고서를 첨부하려면 * 작업 보고서 연결 * 을 선택합니다.

이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmtpServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

6. 요약을 검토하고 * Finish * 를 클릭합니다.

데이터베이스 토폴로지 페이지가 표시됩니다.

7. 지금 백업 * 을 클릭합니다.
8. 백업 페이지에서 다음 단계를 수행하십시오.
   a. 리소스에 여러 정책을 적용한 경우 * 정책 * 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

   b. 백업 * 을 클릭합니다.
9. 페이지 하단의 작업 창에서 작업을 두 번 클릭하여 작업 세부 정보 페이지를 표시하여 백업 진행 상황을 모니터링합니다.
   - MetroCluster 구성에서 SnapCenter는 페일오버 후 보호 관계를 감지하지 못할 수 있습니다.

자세한 내용은 다음을 참조하십시오. "MetroCluster 페일오버 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다"

   - VMDK에서 애플리케이션 데이터를 백업하고 VMware vSphere용 SnapCenter 플러그인의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다.

Java 힙 크기를 늘리려면 스크립트 파일 _/opt/netapp/init_scripts/scvservice_를 찾습니다. 이 스크립트에서 _do_start method_command는 SnapCenter VMware 플러그인 서비스를 시작합니다. 이 명령을 _java-jar-

Xmx8192M-Xms4096M_로 업데이트합니다

Exchange 리소스 그룹을 백업합니다

리소스 그룹은 호스트 또는 Exchange DAG의 리소스 모음이며 리소스 그룹에는 전체 DAG 또는 개별 데이터베이스가 포함될 수 있습니다. 리소스 페이지에서 리소스 그룹을 백업할 수 있습니다.

시작하기 전에

- 정책이 연결된 리소스 그룹을 만들어야 합니다.
- 백업 작업에 사용 중인 애그리게이트를 데이터베이스가 사용하는 스토리지 가상 시스템(SVM)에 할당해야 합니다.
- 2차 스토리지와 SnapMirror 관계가 있는 리소스를 백업하려면 스토리지 사용자에게 할당된 역할에 "'스냅샷 전체' 권한이 있어야 합니다. 그러나 "vsadmin" 역할을 사용하는 경우에는 "napmirror all" 권한이 필요하지 않습니다.
- 리소스 그룹에 서로 다른 호스트의 데이터베이스가 여러 개 있는 경우 네트워크 문제로 인해 일부 호스트의 백업 작업이 늦게 시작될 수 있습니다. 의 값을 구성해야 합니다 `MaxRetryForUninitializedHosts` 인치 `web.config` 를 사용합니다 `Set-SmConfigSettings` PowerShell cmdlet.
- 리소스 그룹에 NetApp 및 비 NetApp 스토리지에 액티브/패시브 데이터베이스 복사본이 있는 데이터베이스 또는 데이터베이스 가용성 그룹이 포함되어 있고, 백업 작업 생성 시 선택할 서버의 액티브 복제본 * 또는 * 백업 복제본 * 옵션을 선택한 경우 그런 다음 백업 작업이 경고 상태가 됩니다.

  백업이 NetApp 스토리지의 액티브/패시브 데이터베이스 복사본에 대해 성공하고 NetApp이 아닌 타사 스토리지의 액티브/패시브 데이터베이스 복사본에 대해서는 백업이 실패합니다.

이 작업에 대해

리소스 페이지에서 필요 시 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 연결되어 있고 스케줄이 구성되어 있는 경우 스케줄에 따라 백업이 자동으로 수행됩니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 * Microsoft Exchange Server 플러그인 * 을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 리소스 그룹 * 을 선택합니다.

   검색 상자에 리소스 그룹 이름을 입력하거나 * 를 클릭하여 리소스 그룹을 검색할 수 있습니다  를 누른 다음 태그를 선택합니다. 그런 다음 * 를 클릭할 수 있습니다  를 눌러 필터 창을 닫습니다.
3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음 * 지금 백업 * 을 클릭합니다.
4. 백업 페이지에서 다음 단계를 수행하십시오.
   a. 여러 정책을 리소스 그룹에 연결한 경우 * Policy * 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

      필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

   b. 백업 * 을 클릭합니다.
5. 페이지 하단의 작업 창에서 작업을 두 번 클릭하여 작업 세부 정보 페이지를 표시하여 백업 진행 상황을 모니터링합니다.

Exchange Server용 PowerShell cmdlet을 사용하여 스토리지 시스템 연결과 자격 증명을 생성합니다

PowerShell cmdlet을 사용하여 백업 및 복원하기 전에 SVM(Storage Virtual Machine) 연결과 자격 증명을 생성해야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행할 수 있도록 PowerShell 환경을 준비해야 합니다.
- 스토리지 접속을 생성하려면 인프라스트럭처 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

  호스트 캐시가 업데이트되지 않고 데이터베이스 상태가 SnapCenter GUI에 ""백업을 위해 사용할 수 없음"" 또는 ""NetApp 스토리지에 없음""으로 표시될 수 있으므로 스토리지 시스템 접속을 추가하는 동안 호스트 플러그인 설치가 진행되어서는 안 됩니다.

- 스토리지 시스템 이름은 고유해야 합니다.

  SnapCenter는 서로 다른 클러스터에서 동일한 이름의 여러 스토리지 시스템을 지원하지 않습니다. SnapCenter에서 지원하는 각 스토리지 시스템은 고유한 이름과 고유한 데이터 LIF IP 주소를 가져야 합니다.

단계

1. 를 사용하여 PowerShell 연결 세션을 시작합니다 `Open-SmConnection` cmdlet.

   이 예제에서는 PowerShell 세션을 엽니다.

   ```
   PS C:\> Open-SmConnection
   ```

2. 를 사용하여 스토리지 시스템에 대한 새 접속을 생성합니다 `Add-SmStorageConnection` cmdlet.

   이 예에서는 새 스토리지 시스템 접속을 생성합니다.

   ```
   PS C:\> Add-SmStorageConnection -SVM test_vs1 -Protocol Https
   -Timeout 60
   ```

3. 을 사용하여 새 Run As 계정을 만듭니다 `Add-Credential` cmdlet.

   이 예제에서는 Windows 자격 증명을 사용하여 ExchangeAdmin이라는 새 Run As 계정을 만듭니다.

   ```
   PS C:> Add-SmCredential -Name ExchangeAdmin -AuthMode Windows
   -Credential sddev\administrator
   ```

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

PowerShell cmdlet을 사용하여 Exchange 리소스를 백업합니다

Exchange Server 데이터베이스 백업에는 SnapCenter Server와의 연결 설정, Exchange Server 데이터베이스 검색, 정책 추가, 백업 리소스 그룹 생성, 백업 및 백업 상태 보기가 포함됩니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 스토리지 시스템 접속을 추가하고 자격 증명을 생성해야 합니다.
- 호스트 및 검색된 리소스를 추가해야 합니다.

Exchange용 플러그인은 클론 작업을 지원하지 않으므로 Exchange용 플러그인에서는 추가 SmPolicy cmdlet의 CloneType 매개 변수가 지원되지 않습니다

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146/
```

사용자 이름 및 암호 프롬프트가 표시됩니다.

2. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.

이 예에서는 전체 백업 및 로그 백업을 사용하여 새 백업 정책을 생성합니다. Exchange 백업 유형:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies
```

이 예에서는 시간별 전체 백업 및 로그 백업을 사용하여 새 백업 정책을 생성합니다. Exchange 백업 유형:

```
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 예에서는 Exchange 로그만 백업하기 위한 새 백업 정책을 생성합니다.

```
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. 추가 SmResourceGroup cmdlet을 사용하여 SnapCenter에 새 리소스 그룹을 추가합니다.

   이 예에서는 지정된 정책 및 리소스를 사용하여 새 Exchange Server 데이터베이스 백업 리소스 그룹을 생성합니다.

   ```
   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_bk
   p_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 예에서는 지정된 정책 및 리소스를 사용하여 새 Exchange DAG(Database Availability Group) 백업 리소스 그룹을 생성합니다.

   ```
   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_bk
   p_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database Availability
   Group";"Names"="DAGSCE0102"}
   ```

5. New-SmBackup cmdlet을 사용하여 새 백업 작업을 시작합니다.

   ```
   C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
   SCE_w2k12_Full_Log_bkp_Policy
   ```

   이 예에서는 보조 스토리지에 새 백업을 생성합니다.

   ```
   New-SMBackup -DatasetName ResourceGroup1 -Policy
   Secondary_Backup_Policy4
   ```

6. Get-SmBackupReport cmdlet을 사용하여 백업 작업의 상태를 봅니다.

이 예는 지정된 날짜에 실행된 모든 작업의 작업 요약 보고서를 표시합니다.

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

이 예는 특정 작업 ID에 대한 작업 요약 보고서를 표시합니다.

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

백업 작업을 모니터링합니다

SnapCenterJobs 페이지를 사용하여 여러 백업 작업의 진행률을 모니터링할 수 있습니다. 진행 상황을 확인하여 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

다음 아이콘이 작업 페이지에 나타나고 작업의 해당 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨

단계

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 모니터 페이지에서 * 작업 * 을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행하십시오.
   a. 을 클릭합니다 백업 작업만 나열되도록 목록을 필터링합니다.
   b. 시작 및 종료 날짜를 지정합니다.
   c. Type * 드롭다운 목록에서 * Backup * 을 선택합니다.
   d. Status * (상태 *) 드롭다운에서 백업 상태를 선택합니다.
   e. 작업이 성공적으로 완료되었는지 보려면 * Apply * 를 클릭합니다.
4. 백업 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.

> 백업 작업 상태가 표시됩니다 작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 기호로 표시되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 * 로그 보기 * 를 클릭합니다.

   로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

Activity 창에서 작업을 모니터링합니다

작업 창에는 가장 최근에 수행한 작업 5개가 표시됩니다. 작업 창은 작업이 시작된 시점과 작업의 상태도 표시합니다.

작업 창에는 백업, 복원, 클론 및 예약된 백업 작업에 대한 정보가 표시됩니다. SQL Server용 플러그인 또는 Exchange Server용 플러그인을 사용하는 경우 작업 창에 다시 시드된 작업에 대한 정보도 표시됩니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 을 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다.

   작업 중 하나를 클릭하면 작업 세부 정보가 * 작업 세부 정보 * 페이지에 나열됩니다.

Exchange 데이터베이스에 대한 백업 작업을 취소합니다

대기열에 있는 백업 작업을 취소할 수 있습니다.

- 필요한 것 *
- 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 모니터 * 페이지 또는 * 작업 * 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 작업에 대해 * 작업 취소 * 버튼이 비활성화됩니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 사용자\그룹 페이지에서 다른 구성원 개체를 보고 작동할 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.

시작...	조치
모니터 페이지	a. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 클릭합니다. b. 작업을 선택한 다음 * 작업 취소 * 를 클릭합니다.
작업 창	a. 백업 작업을 시작한 후 * 를 클릭합니다 * 를 클릭합니다. b. 작업을 선택합니다. c. 작업 세부 정보 페이지에서 * 작업 취소 * 를 클릭합니다.

작업이 취소되고 리소스가 이전 상태로 돌아갑니다.

PowerShell cmdlet을 사용하여 Exchange 백업을 제거합니다

다른 데이터 보호 작업에 Exchange 백업이 더 이상 필요하지 않은 경우 Remove-SmBackup cmdlet을 사용하여 Exchange 백업을 삭제할 수 있습니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146/
```

2. 를 사용하여 하나 이상의 백업을 삭제합니다 `Remove-SmBackup` cmdlet.

   이 예에서는 백업 ID를 사용하여 두 개의 백업을 삭제합니다.

```
Remove-SmBackup -BackupIds 3,4
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"):
```

토폴로지 페이지에서 Exchange 백업을 봅니다

리소스를 백업할 준비를 할 때 운영 및 보조 스토리지의 모든 백업을 그래픽으로 표시하는 것이 도움이 될 수 있습니다.

이 작업에 대해

토폴로지 페이지에서 선택한 리소스 또는 리소스 그룹에 사용할 수 있는 모든 백업을 볼 수 있습니다. 이러한 백업의 세부 정보를 확인한 다음 해당 백업을 선택하여 데이터 보호 작업을 수행할 수 있습니다.

복제본 관리 보기에서 다음 아이콘을 검토하여 운영 스토리지 또는 보조 스토리지(미러 복사본 또는 볼트 복제본)에서 백업을 사용할 수 있는지 여부를 확인할 수 있습니다.

-  기본 스토리지에서 사용할 수 있는 백업 수를 표시합니다.
-  SnapMirror 기술을 사용하여 보조 스토리지에 미러링되는 백업 수를 표시합니다.

-  SnapVault 기술을 사용하여 보조 스토리지에 복제되는 백업 수를 표시합니다.
  - 표시된 백업 수에는 보조 스토리지에서 삭제된 백업이 포함됩니다.

    예를 들어 정책을 사용하여 6개의 백업을 생성하여 4개의 백업만 보존한 경우 표시되는 백업 수는 6입니다.

* 모범 사례: * 정확한 수의 복제된 백업이 표시되도록 토폴로지를 새로 고치는 것이 좋습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 데이터베이스, 리소스 또는 리소스 그룹을 선택합니다.
3. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 리소스를 선택합니다.

   리소스가 보호되는 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.
4. Summary card(요약 카드) 섹션을 검토하여 운영 스토리지와 보조 스토리지에서 사용할 수 있는 백업의 수를 요약합니다.

   요약 카드 섹션에는 총 백업 수와 총 로그 백업 수가 표시됩니다.

   Refresh * 버튼을 클릭하면 스토리지 쿼리가 시작되어 정확한 카운트를 표시합니다.
5. 복사본 관리 보기에서 기본 또는 보조 스토리지에서 * 백업 * 을 클릭하여 백업 세부 정보를 확인합니다.

   백업 세부 정보가 표 형식으로 표시됩니다.
6. 테이블에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 이름 바꾸기 및 삭제 작업을 수행합니다.

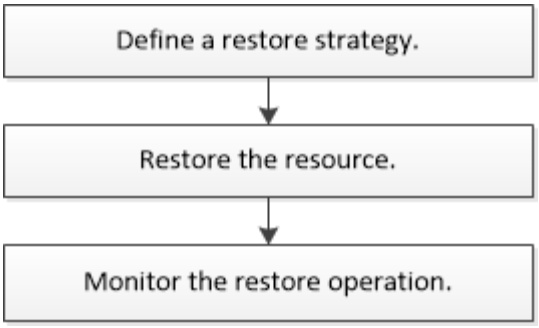
    보조 스토리지에 있는 백업의 이름을 바꾸거나 백업을 삭제할 수 없습니다. 스냅샷 복사본 삭제는 ONTAP 보존 설정에 의해 처리됩니다.

Exchange 리소스를 복구합니다

워크플로를 복원합니다

SnapCenter를 사용하여 하나 이상의 백업을 활성 파일 시스템에 복구함으로써 Exchange 데이터베이스를 복구할 수 있습니다.

다음 워크플로에서는 Exchange 데이터베이스 복원 작업을 수행해야 하는 순서를 보여 줍니다.



PowerShell cmdlet을 수동으로 사용하거나 스크립트에서 사용하여 백업 및 복원 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

Exchange 데이터베이스 복구 요구 사항

Microsoft Exchange Server 백업용 SnapCenter 플러그인에서 Exchange Server 데이터베이스를 복구하기 전에 몇 가지 요구 사항이 충족되는지 확인해야 합니다.

복원 기능을 완전히 사용하려면 SnapCenter Server 및 Exchange 데이터베이스용 SnapCenter 플러그인을 4.6으로 업그레이드해야 합니다.

- 데이터베이스를 복구하려면 Exchange Server가 온라인 상태이고 실행 중이어야 합니다.
- 데이터베이스는 Exchange Server에 있어야 합니다.

  삭제된 데이터베이스 복원은 지원되지 않습니다.

- 데이터베이스에 대한 SnapCenter 일정을 일시 중지해야 합니다.
- SnapCenter 서버 및 Microsoft Exchange Server용 SnapCenter 플러그인은 복원하려는 백업이 포함된 운영 스토리지 및 보조 스토리지에 연결되어 있어야 합니다.

Exchange 데이터베이스를 복구합니다

SnapCenter를 사용하여 백업된 Exchange 데이터베이스를 복구할 수 있습니다.

시작하기 전에

- 리소스 그룹, 데이터베이스 또는 DAG(데이터베이스 가용성 그룹)를 백업해야 합니다.
- Exchange 데이터베이스가 다른 위치로 마이그레이션되면 이전 백업에서 복구 작업이 작동하지 않습니다.
- 스냅샷 복사본을 미러 또는 볼트에 복제하는 경우 SnapCenter 관리자는 소스 볼륨과 타겟 볼륨 모두에 대해 SVM을 할당해야 합니다.
- DAG에서 액티브 데이터베이스 복제본이 타사 스토리지에 있고 NetApp 스토리지에 있는 패시브 데이터베이스 복제본 백업에서 복구하려는 경우 패시브 복제본(NetApp 스토리지)을 액티브 복제본으로 만들고 리소스를 새로 고치고 복구 작업을 수행합니다.

  를 실행합니다 `Move-ActiveMailboxDatabase` 수동 데이터베이스 복사본을 활성 데이터베이스 복사본으로 만드는 명령입니다.

를 클릭합니다 "Microsoft 설명서" 이 명령에 대한 정보를 포함합니다.

이 작업에 대해

- 데이터베이스에서 복구 작업을 수행하면 데이터베이스가 동일한 호스트에 다시 마운트되고 새 볼륨이 생성되지 않습니다.
- DAG 레벨 백업은 개별 데이터베이스에서 복구해야 합니다.
- Exchange 데이터베이스(.edb) 파일 이외의 파일이 있는 경우 전체 디스크 복원이 지원되지 않습니다.

  Exchange용 플러그인은 디스크에 복제에 사용되는 것과 같은 Exchange 파일이 포함되어 있는 경우 디스크에서 전체 복구를 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_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 swagger에서 API:API/4.7/configsettings를 통해 표시할 수 있습니다

  Get API를 사용하여 키 값을 표시할 수 있습니다. API 설정은 지원되지 않습니다.

단계

1. 왼쪽 탐색 창의 리소스 페이지 왼쪽 위에 있는 * 리소스 * 를 클릭합니다.
2. 드롭다운 목록에서 Exchange Server 플러그인을 선택합니다.
3. 리소스 페이지의 보기 목록에서 * 데이터베이스 * 를 선택합니다.
4. 목록에서 데이터베이스를 선택합니다.
5. Manage Copies 보기의 Primary Backups 표에서 * Backups * 를 선택한 다음 * 를 클릭합니다 *.
6. 옵션 페이지에서 다음 로그 백업 옵션 중 하나를 선택합니다.

옵션을 선택합니다	설명
모든 로그 백업	전체 백업 후 사용 가능한 모든 로그 백업을 복원하려면 * 모든 로그 백업 * 을 선택하여 최신 백업 복원 작업을 수행하십시오.

옵션을 선택합니다	설명
까지 로그 백업을 통해	선택한 로그까지 로그 백업을 기반으로 데이터베이스를 복원하는 시점 복원 작업을 수행하려면 * 까지 로그 백업 * 을 선택합니다. 드롭다운 목록에 표시되는 로그 수는 UTM을 기반으로 합니다. 예를 들어 전체 백업 보존이 5이고 UTM 보존이 3인 경우 사용 가능한 로그 백업 수는 5이지만 드롭다운에서 복구 작업을 수행하기 위해 3개의 로그만 나열됩니다.
특정 날짜 기준 종료	복원된 데이터베이스에 트랜잭션 로그를 적용할 날짜 및 시간을 지정하려면 특정 날짜별 * 를 선택합니다. 이 시점 복원 작업은 지정된 날짜 및 시간에 마지막 백업까지 기록된 트랜잭션 로그 항목을 복원합니다.
없음	로그 백업 없이 전체 백업만 복원해야 하는 경우 * 없음 * 을 선택합니다.

다음 작업 중 하나를 수행할 수 있습니다.

- * 복구 후 데이터베이스 복구 및 마운트 * - 이 옵션은 기본적으로 선택되어 있습니다.
- * 복구하기 전에 백업에서 트랜잭션 로그의 무결성을 확인하지 않음 * - 기본적으로 SnapCenter는 복원 작업을 수행하기 전에 백업에서 트랜잭션 로그의 무결성을 확인합니다.

  * 모범 사례: * 이 옵션을 선택해서는 안 됩니다.

7. 스크립트 페이지에서 복원 작업 전후에 실행해야 하는 처방인 또는 PS의 경로와 인수를 각각 입력합니다.

   복구 매개 변수 인수에는 $Database 및 $ServerInstance가 포함됩니다.

   PostScript 인수 복원에는 $Database, $ServerInstance, $BackupName, $LogDirectory 및 $TargetServerInstance가 포함됩니다.

   스크립트를 실행하여 SNMP 트랩을 업데이트하고, 경고를 자동화하고, 로그를 보내는 등의 작업을 수행할 수 있습니다.

   처방자 또는 사후 스크립트 경로에는 드라이브 또는 공유가 포함되어서는 안 됩니다. 경로는 scripts_path에 상대해야 합니다.

8. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다.

9. 요약을 검토하고 * Finish * 를 클릭합니다.
10. 페이지 하단의 Activity[활동] 패널을 확장하여 복구 작업의 상태를 볼 수 있습니다.

모니터 * > * 작업 * 페이지를 사용하여 복원 프로세스를 모니터링해야 합니다.

백업에서 활성 데이터베이스를 복구할 때 복제본과 액티브 데이터베이스 사이에 지연이 있는 경우 수동 데이터베이스가 일시 중단 또는 실패 상태가 될 수 있습니다.

활성 데이터베이스의 로그 체인이 포크되고 복제를 중단시킬 새 분기가 시작될 때 상태 변경이 발생할 수 있습니다. Exchange Server에서 복제본을 수정하려고 시도하지만 복구할 수 없는 경우 복구 후 새 백업을 생성한 다음 복제본을 다시 시드해야 합니다.

메일 및 편지함의 세밀한 복구

SMBR(Single Mailbox Recovery) 소프트웨어를 사용하면 전체 Exchange 데이터베이스 대신 메일 또는 편지함을 복원 및 복구할 수 있습니다.

전체 데이터베이스를 복원하여 단일 메일을 복구하면 많은 시간과 리소스가 소모됩니다. SMBR은 스냅샷의 클론 복제본을 생성한 다음 Microsoft API를 사용하여 SMBR에 메일박스를 마운트하여 메일을 빠르게 복구하는 데 도움이 됩니다.
SMBR 사용 방법에 대한 자세한 내용은 을 참조하십시오 "SMBR 관리 가이드".

SMBR에 대한 자세한 내용은 다음을 참조하십시오.

- "SMBR(Ontrack Power Control 복원에도 적용 가능)을 사용하여 단일 항목을 수동으로 복원하는 방법"
- "SnapCenter를 사용하여 SMBR의 보조 스토리지에서 복원하는 방법"
- "SMBR을 사용하여 SnapVault에서 Microsoft Exchange Mail 복구"

보조 스토리지에서 **Exchange Server** 데이터베이스를 복구합니다

보조 스토리지(미러 또는 볼트)에서 백업된 Exchange Server 데이터베이스를 복구할 수 있습니다.

기본 스토리지에서 보조 스토리지로 Snapshot 복사본을 복제해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 * Microsoft Exchange Server 플러그인 * 을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 * 데이터베이스 * 또는 * 리소스 그룹 * 을 선택합니다.
3. 데이터베이스 또는 리소스 그룹을 선택합니다.

   데이터베이스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.
4. 복사본 관리 섹션의 보조 스토리지 시스템(미러 또는 볼트)에서 * 백업 * 을 선택합니다.
5. 목록에서 백업을 선택한 다음 을 클릭합니다  .
6. 위치 페이지에서 선택한 리소스를 복원할 대상 볼륨을 선택합니다.
7. 복원 마법사를 완료하고 요약을 검토한 다음 * 마침 * 을 클릭합니다.

PowerShell cmdlet을 사용하여 Exchange 리소스를 복원합니다

Exchange 데이터베이스 복구에는 SnapCenter 서버와의 연결 세션 시작, 백업 목록 표시 및 백업 정보 검색, 백업 복구가 포함됩니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

단계

1. 를 사용하여 지정된 사용자에 대해 SnapCenter 서버와의 연결 세션을 시작합니다 `Open-SmConnection` cmdlet.

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146/
```

2. 를 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다 `Get-SmBackup` cmdlet.

   이 예에서는 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. 를 사용하여 백업에서 데이터를 복원합니다 `Restore-SmBackup` cmdlet.

   이 예에서는 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 예에서는 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 예에서는 보조 스토리지의 백업을 1차 사례로 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
```

를 클릭합니다 `-archive` 매개 변수를 사용하면 복원에 사용할 운영 볼륨과 2차 볼륨을 지정할 수 있습니다.

를 클릭합니다 `-IsRecoverMount:$true` 매개 변수를 사용하면 복구 후에 데이터베이스를 마운트할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

패시브 **Exchange** 노드 복제본을 다시 시딩했습니다

복제본이 손상된 경우와 같이 복제본을 재시딩해야 하는 경우 SnapCenter의 재시딩된 기능을 사용하여 최신 백업으로 재시딩할 수 있습니다.

시작하기 전에

- SnapCenter Server 4.1 이상을 사용하고 Exchange 4.1 이상을 위한 플러그인을 사용해야 합니다.

  복제본 재시딩은 4.1 이전 버전의 SnapCenter에서는 지원되지 않습니다.

- 다시 시딩하려는 데이터베이스의 백업을 만들어야 합니다.

* 모범 사례: * 노드 사이의 지연 현상을 방지하려면 재시딩된 작업을 수행하기 전에 새 백업을 생성하거나 최신 백업이 있는 호스트를 선택하는 것이 좋습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 * Microsoft Exchange Server 플러그인 * 을 선택합니다.
2. 리소스 페이지의 보기 목록에서 적절한 옵션을 선택합니다.

옵션을 선택합니다	설명
단일 데이터베이스를 다시 시딩합니다	보기 목록에서 * 데이터베이스 * 를 선택합니다.
DAG에서 데이터베이스를 재시딩하는 경우	보기 목록에서 * 데이터베이스 가용성 그룹 * 을 선택합니다.

3. 다시 시딩할 리소스를 선택합니다.
4. 복사본 관리 페이지에서 * 다시 시딩된 * 을 클릭합니다.
5. 다시 시딩된 마법사의 비정상적인 데이터베이스 복사본 목록에서 다시 시딩할 복제본을 선택하고 * 다음 * 을 클릭합니다.
6. 호스트 창에서 다시 연결할 백업이 있는 호스트를 선택한 후 * 다음 * 을 클릭합니다.
7. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다.

8. 요약을 검토하고 * Finish * 를 클릭합니다.
9. 페이지 하단의 Activity[활동] 패널을 확장하여 작업 상태를 볼 수 있습니다.

패시브 데이터베이스 복사본이 NetApp이 아닌 스토리지에 상주하는 경우 다시 시딩된 작업은 지원되지 않습니다.

Exchange 데이터베이스에 대해 PowerShell cmdlet을 사용하여 복제본을 다시 시딩했습니다

PowerShell cmdlet을 사용하여 동일한 호스트에 있는 가장 최근 복사본 또는 대체 호스트에서 가장 최근 복사본을 사용하여 상태가 불량한 복제본을 복구할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. 를 사용하여 지정된 사용자에 대해 SnapCenter 서버와의 연결 세션을 시작합니다 `Open-SmConnection` cmdlet.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. 를 사용하여 데이터베이스를 다시 시딩했습니다 `reseed-SmDagReplicaCopy` cmdlet.

   이 예에서는 호스트 "mva-rx200.netapp.com" 에서 해당 호스트의 최신 백업을 사용하여 실패한 데이터베이스 복제본을 다시 시딩합니다.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb
```

   이 예제에서는 다른 호스트 "mva-rx201.netapp.com." 데이터베이스의 최신 백업(운영/복제본)을 사용하여 execdb라는 데이터베이스 복제본을 다시 시딩합니다

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb -BackupHost "mva-rx201.netapp.com"
```

복구 작업을 모니터링합니다

작업 페이지를 사용하여 여러 SnapCenter 복원 작업의 진행률을 모니터링할 수 있습니다. 작업 진행률을 확인하여 작업이 언제 완료되는지 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

복원 후 상태는 복원 작업 후 리소스의 상태와 수행할 수 있는 추가 복원 작업에 대해 설명합니다.

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨

단계

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 모니터 * 페이지에서 * 작업 * 을 클릭합니다.
3. Jobs * 페이지에서 다음 단계를 수행하십시오.
   a. 을 클릭합니다 복원 작업만 나열되도록 목록을 필터링하려면
   b. 시작 및 종료 날짜를 지정합니다.
   c. Type * 드롭다운 목록에서 * Restore * 를 선택합니다.
   d. Status * (상태 *) 드롭다운 목록에서 복원 상태를 선택합니다.
   e. 성공적으로 완료된 작업을 보려면 * 적용 * 을 클릭합니다.
4. 복원 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. Job Details * 페이지에서 * View logs * 를 클릭합니다.

   로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

볼륨 기반 복원 작업 후에는 백업 메타데이터가 SnapCenter 저장소에서 삭제되지만 백업 카탈로그 항목은 SAP HANA 카탈로그에 남아 있습니다. 복원 작업 상태가 표시됩니다 작업 세부 정보를 클릭하여 일부 하위 작업의 경고 표시를 확인해야 합니다. 경고 표지를 클릭하고 표시된 백업 카탈로그 항목을 삭제합니다.

Exchange 데이터베이스에 대한 복구 작업을 취소합니다

대기열에 있는 복원 작업을 취소할 수 있습니다.

복원 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

이 작업에 대해

- Monitor* 페이지 또는 * Activity* 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 작업에는 * 작업 취소 * 버튼이 비활성화됩니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 사용자\그룹 페이지의 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.

시작...	조치
모니터 페이지	1. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 클릭합니다. 2. 작업을 선택하고 * 작업 취소 * 를 클릭합니다.
작업 창	1. 복원 작업을 시작한 후 을 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다. 2. 작업을 선택합니다. 3. 작업 세부 정보 페이지에서 * 작업 취소 * 를 클릭합니다.

사용자 정의 응용 프로그램 보호

SnapCenter 맞춤형 플러그인

SnapCenter 맞춤형 플러그인 개요

사용하는 애플리케이션용 맞춤형 플러그인을 개발한 다음 SnapCenter를 사용하여 이러한 애플리케이션을 백업, 복원 또는 복제할 수 있습니다. 다른 SnapCenter 플러그인과 마찬가지로, 사용자 지정 플러그인은 NetApp SnapCenter 소프트웨어의 호스트 측 구성 요소로 작동하여 애플리케이션 인식 데이터 보호 및 리소스 관리를 지원합니다.

사용자 지정 플러그인이 설치된 경우 SnapCenter with NetApp SnapMirror 기술을 사용하여 다른 볼륨에 백업 세트의 미러 복사본을 생성하고 NetApp SnapVault 기술을 사용하여 D2D 백업 복제를 수행할 수 있습니다. 사용자 지정 플러그인은 Windows 및 Linux 환경 모두에서 사용할 수 있습니다.

SnapCenterCLI는 SnapCenter 맞춤형 플러그인 명령을 지원하지 않습니다.

NetApp은 SnapCenter에 내장된 맞춤형 플러그인 프레임워크를 사용하여 ONTAP 스토리지에서 데이터 볼륨의 데이터 보호 작업을 수행할 수 있는 스토리지 플러그인을 제공합니다.

호스트 추가 페이지에서 사용자 지정 플러그인 및 스토리지 플러그인을 설치할 수 있습니다.

"호스트를 추가하고 원격 호스트에 플러그인 패키지를 설치합니다."

NetApp은 또한 MySQL, MAXDB, DB2, Sybase, DPGLUE, MongoDB, ORASCPM 및 PostgreSQL 맞춤형 플러그인 이러한 플러그인은 에서 다운로드할 수 있습니다 "NetApp 스토리지 자동화 스토어".

SnapCenter 지원 정책은 SnapCenter 맞춤형 플러그인 프레임워크, 핵심 엔진 및 관련 API에 대한 지원을 포함합니다. 지원 서비스는 플러그인 소스 코드와 사용자 지정 플러그인 프레임워크에 구축된 관련 스크립트를 지원하지 않습니다.

을 참조하여 사용자 지정 플러그인을 만들 수 있습니다 "응용 프로그램용 플러그인을 개발합니다".

SnapCenter 맞춤형 플러그인 및 스토리지 플러그인으로 수행할 수 있는 작업

데이터 보호 작업에 SnapCenter 맞춤형 플러그인을 사용할 수 있습니다.

- 맞춤형 플러그인 *
- 데이터베이스, 인스턴스, 문서 또는 테이블스페이스와 같은 리소스를 추가합니다.
- 백업을 생성합니다.
- 백업에서 복원합니다.
- 클론 백업.
- 백업 작업을 예약합니다.
- 백업, 복원 및 클론 작업을 모니터링합니다.

- 백업, 복원 및 클론 작업에 대한 보고서를 봅니다.
- 스토리지 플러그인 *

스토리지 플러그인을 사용하여 데이터 보호 작업을 수행할 수 있습니다.

- ONTAP 클러스터에서 스토리지 볼륨의 일관성 그룹 Snapshot 복사본을 생성합니다.
- 내장된 사전 및 사후 스크립팅 프레임워크를 사용하여 사용자 지정 애플리케이션을 백업합니다

  ONTAP 볼륨, LUN 또는 Qtree를 백업할 수 있습니다.

- ONTAP 정책을 사용하여 기본 Snapshot 복사본을 SnapCenter 보조 복사본으로 업데이트하고 기존 복제 관계(SnapVault/SnapMirror/유니파이드 복제)를 활용합니다

  ONTAP Primary 및 Secondary는 ONTAP FAS, AFF, ASA(All SAN Array), Select 또는 Cloud ONTAP가 될 수 있습니다.

- 전체 ONTAP 볼륨, LUN 또는 파일을 복구합니다.

  찾아보기 또는 인덱싱 기능이 제품에 내장되어 있지 않으므로 해당 파일 경로를 수동으로 제공해야 합니다.

  Qtree 또는 디렉토리 복원은 지원되지 않지만, 백업 범위가 Qtree 레벨에서 정의된 경우 Qtree만 클론 복제 및 내보낼 수 있습니다.

SnapCenter 맞춤형 플러그인 기능

SnapCenter는 플러그인 애플리케이션 및 스토리지 시스템의 NetApp 기술과 통합됩니다. 사용자 지정 플러그인으로 작업하려면 SnapCenter 그래픽 사용자 인터페이스를 사용합니다.

- * 통합 그래픽 사용자 인터페이스 *

  SnapCenter 인터페이스는 플러그인과 환경 전반에서 표준화와 일관성을 제공합니다. SnapCenter 인터페이스를 사용하면 플러그인 전체에서 일관된 백업, 복원, 복구, 클론 작업을 완료하고, 중앙 집중식 보고 기능을 사용하고, 대시보드 뷰를 한눈에 보고, RBAC(역할 기반 액세스 제어)를 설정하고, 모든 플러그인에 걸쳐 작업을 모니터링할 수 있습니다.

- * 자동화된 중앙 관리 *

  백업 작업을 예약하고, 정책 기반 백업 보존을 구성하고, 복구 작업을 수행할 수 있습니다. 또한 SnapCenter에서 이메일 경고를 보내도록 구성하여 환경을 사전에 모니터링할 수도 있습니다.

- * 무중단 NetApp 스냅샷 복사본 기술 *

  SnapCenter은 SnapCenter 맞춤형 플러그인과 NetApp 스냅샷 복사본 기술을 사용하여 리소스를 백업합니다. 스냅샷 복사본은 최소 스토리지 공간을 사용합니다.

사용자 지정 플러그인 기능을 사용하면 다음과 같은 이점이 있습니다.

- 백업, 복원 및 클론 워크플로우 지원
- RBAC 지원 보안 및 중앙 집중식 역할 위임

권한이 있는 SnapCenter 사용자가 응용 프로그램 수준 권한을 갖도록 자격 증명을 설정할 수도 있습니다.

- NetApp FlexClone 기술을 사용하여 테스트 또는 데이터 추출을 위한 공간 효율적인 특정 시점 리소스 복사본 생성

  클론을 생성하려는 스토리지 시스템에는 FlexClone 라이센스가 필요합니다.

- 백업을 생성하는 과정에서 ONTAP의 일관성 그룹(CG) 스냅샷 복사본 기능이 지원됩니다.
- 여러 리소스 호스트에서 동시에 여러 백업을 실행할 수 있습니다

  단일 호스트에서 단일 호스트의 리소스가 동일한 볼륨을 공유할 경우 스냅샷 복사본이 통합됩니다.

- 외부 명령을 사용하여 스냅샷 복사본을 생성하는 기능
- Windows 환경에서 파일 시스템의 일관된 Snapshot 복사본을 생성할 수 있는 기능

SnapCenter 사용자 지정 플러그인에서 지원하는 스토리지 유형입니다

SnapCenter는 물리적 시스템과 가상 머신 모두에서 다양한 스토리지 유형을 지원합니다. SnapCenter 사용자 지정 플러그인을 설치하기 전에 스토리지 유형에 대한 지원을 확인해야 합니다.

기계	스토리지 유형입니다
VM 호스트의 물리적 마운트 및 NFS 직접 마운트(VMDK 및 RDM LUN은 지원되지 않음)	FC 연결 LUN
VM 호스트의 물리적 마운트 및 NFS 직접 마운트(VMDK 및 RDM LUN은 지원되지 않음)	iSCSI로 연결된 LUN
VM 호스트의 물리적 마운트 및 NFS 직접 마운트(VMDK 및 RDM LUN은 지원되지 않음)	NFS 연결 볼륨

사용자 지정 플러그인에 필요한 최소 **ONTAP** 권한

필요한 최소 ONTAP 권한은 데이터 보호를 위해 사용 중인 SnapCenter 플러그인에 따라 다릅니다.

- All-access 명령: ONTAP 8.3.0 이상에 필요한 최소 권한
  - event generate-autosupport-log입니다
  - 작업 기록이 표시됩니다
  - 작업 중지
  - LUN 속성이 표시됩니다
  - LUN 생성
  - LUN을 삭제합니다
  - LUN 형태

- LUN igroup 추가
- LUN igroup 작성
- LUN igroup 삭제
- LUN igroup의 이름을 바꿉니다
- LUN igroup 표시
- LUN 매핑 add-reporting-nodes입니다
- LUN 매핑 생성
- LUN 매핑을 삭제합니다
- LUN 매핑으로 remove-reporting-nodes를 사용할 수 있습니다
- LUN 매핑이 표시됩니다
- LUN 수정
- LUN 이동 - 볼륨
- LUN이 오프라인 상태입니다
- LUN을 온라인 상태로 전환합니다
- LUN 크기 조정
- LUN 일련 번호입니다
- LUN 표시
- 네트워크 인터페이스
- SnapMirror 정책 추가 규칙
- SnapMirror 정책 modify-rule을 참조하십시오
- SnapMirror 정책 remove-rule을 참조하십시오
- SnapMirror 정책 쇼
- SnapMirror 복원
- SnapMirror 쇼
- SnapMirror 기록
- SnapMirror 업데이트
- SnapMirror 업데이트 - ls -set
- SnapMirror 목록 - 대상
- 버전
- 볼륨 클론 생성
- 볼륨 클론 표시
- 볼륨 클론 분할 시작이 있습니다
- 볼륨 클론 분할 중지
- 볼륨 생성

    - 볼륨 제거
    - 볼륨 파일 클론 생성
    - 볼륨 파일 show-disk-usage 를 참조하십시오
    - 볼륨이 오프라인 상태입니다
    - 볼륨을 온라인으로 설정합니다
    - 볼륨 수정
    - 볼륨 qtree 생성
    - 볼륨 qtree 삭제
    - 볼륨 qtree 수정
    - 볼륨 qtree 표시
    - 볼륨 제한
    - 볼륨 표시
    - 볼륨 스냅샷 생성
    - 볼륨 스냅숏 삭제
    - 볼륨 스냅숏 수정
    - 볼륨 스냅숏 이름 바꾸기
    - 볼륨 스냅샷 복원
    - 볼륨 스냅샷 복원 - 파일
    - 볼륨 스냅샷 표시
    - 볼륨 마운트 해제
    - SVM CIFS를 선택합니다
    - SVM CIFS 공유 생성
    - SVM CIFS 공유 삭제
    - SVM CIFS shadowcopy show 를 참조하십시오
    - SVM CIFS 공유 표시
    - vserver cifs show 를 참조하십시오
    - SVM 엑스포트 정책 생성
    - SVM 엑스포트 정책 삭제
    - SVM 엑스포트 정책 규칙 생성
    - vserver export-policy rule show를 참조하십시오
    - vserver export-policy show를 참조하십시오
    - SVM iSCSI 연결이 표시됩니다
    - vserver show 를 참조하십시오
- 읽기 전용 명령: ONTAP 8.3.0 이상에 필요한 최소 권한

◦ 네트워크 인터페이스

맞춤형 플러그인을 위한 **SnapMirror** 및 **SnapVault** 복제를 위한 스토리지 시스템 준비

ONTAP 플러그인을 SnapCenter SnapMirror 기술과 함께 사용하여 다른 볼륨에 백업 세트의 미러링 복사본을 만들고 ONTAP SnapVault 기술을 사용하여 표준 준수 및 기타 거버넌스 관련 용도로 D2D 백업 복제를 수행할 수 있습니다. 이러한 작업을 수행하기 전에 소스 볼륨과 타겟 볼륨 간의 데이터 보호 관계를 구성하고 관계를 초기화해야 합니다.

SnapCenter는 스냅샷 복사본 작업이 완료된 후 SnapMirror 및 SnapVault에 대한 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행되고, 별도의 ONTAP 일정을 만들지 않습니다.

NetApp SnapManager 제품에서 SnapCenter으로 오고 있으며 구성한 데이터 보호 관계에 만족하는 경우 이 섹션을 건너뛸 수 있습니다.

데이터 보호 관계는 운영 스토리지(소스 볼륨)의 데이터를 보조 스토리지(타겟 볼륨)에 복제합니다. 관계를 초기화할 때 ONTAP은 소스 볼륨에서 참조된 데이터 블록을 대상 볼륨으로 전송합니다.

SnapCenter는 SnapMirror와 SnapVault 볼륨(* Primary * > * Mirror * > * Vault *) 간의 계단식 관계를 지원하지 않습니다. 팬아웃 관계를 사용해야 합니다.

SnapCenter는 버전에 상관없이 유연한 SnapMirror 관계의 관리를 지원합니다. 버전에 상관없이 유연한 SnapMirror 관계와 설정 방법에 대한 자세한 내용은 를 참조하십시오 "ONTAP 설명서".

SnapCenter는 * SYNC_MIRROR * 복제를 지원하지 않습니다.

백업 전략 정의

백업 작업을 생성하기 전에 백업 전략을 정의하면 리소스를 성공적으로 복원하거나 복제하는 데 필요한 백업을 확보할 수 있습니다. SLA(서비스 수준 계약), RTO(복구 시간 목표) 및 RPO(복구 시점 목표)에 따라 백업 전략이 주로 결정됩니다.

이 작업에 대해

SLA는 예상되는 서비스 수준을 정의하고 서비스의 가용성 및 성능을 비롯한 다양한 서비스 관련 문제를 해결합니다. RTO는 서비스 중단 후 비즈니스 프로세스를 복원해야 하는 시간입니다. RPO는 장애 후 정상적인 작업을 재개하기 위해 백업 스토리지에서 복구해야 하는 파일의 사용 기간에 대한 전략을 정의합니다. SLA, RTO 및 RPO는 데이터 보호 전략에 기여합니다.

단계

1. 자원을 언제 백업해야 하는지 결정합니다.
2. 필요한 백업 작업 수를 결정합니다.
3. 백업 이름을 지정하는 방법을 결정합니다.
4. 일관성 그룹 스냅샷 복사본을 사용할지 결정하고 일관성 그룹 스냅샷 복사본을 삭제할 수 있는 적절한 옵션을 결정합니다.
5. 복제에 NetApp SnapMirror 기술을 사용할지, 장기 보존에 NetApp SnapVault 기술을 사용할지 여부를 결정합니다.

6. 소스 스토리지 시스템과 SnapMirror 대상에 있는 스냅샷 복사본의 보존 기간을 결정합니다.
7. 백업 작업 전후에 명령을 실행할지 여부를 결정하고 처방이나 PS를 제공합니다.

맞춤형 플러그인의 백업 전략

사용자 지정 플러그인 리소스의 백업 스케줄입니다

백업 스케줄을 결정할 때 가장 중요한 요소는 리소스의 변경 속도입니다. 리소스를 더 자주 백업할수록 SnapCenter에서 복원에 사용하는 아카이브 로그가 적어지므로 복원 작업이 더 빨라집니다.

자주 사용하는 리소스를 매일 한 번씩 백업할 수도 있고, 자주 사용하지 않는 리소스를 하루에 한 번 백업할 수도 있습니다. 기타 요인으로는 조직에 리소스의 중요성, SLA(서비스 수준 계약) 및 RPO(복구 지점 목표)가 있습니다.

SLA는 예상되는 서비스 수준을 정의하고 가용성 및 서비스 성능을 비롯한 다양한 서비스 관련 문제를 해결합니다. RPO는 장애 후 정상적인 작업을 재개하기 위해 백업 스토리지에서 복구해야 하는 파일의 사용 기간에 대한 전략을 정의합니다. SLA 및 RPO는 데이터 보호 전략에 기여합니다.

백업 스케줄은 다음과 같이 두 부분으로 구성됩니다.

- 백업 빈도

  일부 플러그인의 스케줄 유형이라고도 하는 백업 빈도(백업 수행 빈도)는 정책 구성의 일부입니다. 예를 들어 백업 빈도를 매시간, 일별, 주별 또는 월별로 구성할 수 있습니다. SnapCenter GUI에서 * 설정 * > * 정책 * 을 클릭하여 정책에 액세스할 수 있습니다.

- 백업 스케줄

  백업 스케줄(백업을 수행할 정확한 시점)은 리소스 또는 리소스 그룹 구성의 일부입니다. 예를 들어 주별 백업에 대한 정책이 구성된 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 스케줄을 구성할 수 있습니다 SnapCenter GUI에서 * 리소스 * 를 클릭한 다음 해당 플러그인을 선택하고 * 보기 * > * 리소스 그룹 * 을 클릭하여 리소스 그룹 일정에 액세스할 수 있습니다.

필요한 백업 작업 수입니다

필요한 백업 작업 수를 결정하는 요인에는 리소스 크기, 사용된 볼륨 수, 리소스 변경 속도 및 SLA(서비스 수준 계약)가 포함됩니다.

일반적으로 선택한 백업 작업 수는 리소스를 배치한 볼륨의 수에 따라 달라집니다. 예를 들어, 한 볼륨에 작은 리소스 그룹을 배치하고 다른 볼륨에 큰 리소스를 배치한 경우 작은 리소스에 대해 하나의 백업 작업을 생성하고 큰 리소스에 대해 하나의 백업 작업을 만들 수 있습니다.

수동으로 추가한 사용자 지정 플러그인 리소스에 대해 지원되는 복원 전략 유형입니다

SnapCenter를 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다. 사용자 지정 플러그인 리소스를 수동으로 추가하기 위한 두 가지 유형의 복원 전략이 있습니다.

수동으로 추가한 사용자 지정 플러그인 리소스는 복구할 수 없습니다.

리소스 복원을 완료합니다

- 리소스의 모든 볼륨, qtree 및 LUN을 복원합니다

> 리소스에 볼륨 또는 qtree가 포함된 경우, 해당 볼륨 또는 qtree에서 복원하도록 선택된 Snapshot 복사본 이후에 생성된 스냅샷 복사본은 삭제되고 복구할 수 없습니다. 또한 동일한 볼륨 또는 qtree에서 다른 리소스가 호스트되는 경우 해당 리소스도 삭제됩니다.

파일 레벨 복구

- 볼륨, qtree 또는 디렉토리에서 파일을 복원합니다
- 선택한 LUN만 복구합니다

응용 프로그램용 플러그인을 개발합니다

개요

SnapCenter 서버를 사용하면 SnapCenter에 대한 플러그인으로 응용 프로그램을 배포 및 관리할 수 있습니다. 원하는 애플리케이션을 SnapCenter 서버에 연결하여 데이터 보호 및 를 수행할 수 있습니다 관리 기능:

SnapCenter를 사용하면 다양한 프로그래밍 언어를 사용하여 사용자 지정 플러그인을 개발할 수 있습니다. 가능합니다 Perl, Java, 배치 또는 기타 스크립팅 언어를 사용하여 사용자 지정 플러그인을 개발합니다.

SnapCenter에서 사용자 지정 플러그인을 사용하려면 다음 작업을 수행해야 합니다.

- 이 가이드의 지침에 따라 응용 프로그램용 플러그인을 만듭니다
- 설명 파일을 만듭니다
- 사용자 지정 플러그인을 내보내어 SnapCenter 호스트에 설치합니다
- 플러그인 zip 파일을 SnapCenter 서버에 업로드합니다

모든 **API** 호출의 일반 플러그인 처리

모든 API 호출에 대해 다음 정보를 사용합니다.

- 플러그인 매개 변수
- 종료 코드
- 오류 메시지를 기록합니다
- 데이터 정합성

플러그인 매개 변수를 사용합니다

매개 변수 집합은 모든 API 호출의 일부로 플러그인으로 전달됩니다. 다음 표에서는 매개 변수에 대한 특정 정보를 보여 줍니다.

매개 변수	목적
조치	워크플로 이름을 결정합니다. 예를 들어, 검색, 백업, fileOrVolRestore 또는 를 입력합니다 클oneVolAndLun
리소스	보호할 리소스를 나열합니다. 리소스는 UID 및 유형으로 식별됩니다. 이 목록은 다음 형식으로 플러그인에 표시됩니다. "<UID>, <type>;<UID>, <type>". 예를 들면, 다음과 같습니다. “인스턴스 인스턴스 인스턴스 인스턴스;Instance2\\DB1, 데이터베이스”
APP_NAME입니다	사용 중인 플러그인을 결정합니다. 예: DB2, MySQL. SnapCenter 서버는 나열된 응용 프로그램에 대한 지원을 기본적으로 제공합니다. 이 매개 변수는 대/소문자를 구분합니다.
app_ignore_error	(Y 또는 N) 응용 프로그램 오류가 발생하면 SnapCenter가 종료되거나 종료되지 않습니다. 이 기능은 여러 데이터베이스를 백업할 때 단일 장애가 발생하는 것을 원하지 않을 때 유용합니다 백업 작업을 중지합니다.
resource_name>__app_instance_username입니다	리소스에 대해 SnapCenter 자격 증명이 설정되었습니다.
resource_name>_app_instance_password	리소스에 대해 SnapCenter 자격 증명이 설정되었습니다.
resource_name>_<custom_pRAM>	모든 자원 수준 사용자 정의 키 값은 입니다 접두사가 붙은 플러그인에서 사용할 수 있습니다 “<RESOURCE_NAME> _”. 예를 들어, 가 인 경우 사용자 정의 키는 리소스의 "master_slave"입니다 이름이 "MySQLDB"인 경우 로 사용할 수 있습니다 MySQLDB_MASTER_SLAVE

종료 코드를 사용합니다

플러그인은 종료 코드를 통해 작업 상태를 호스트로 다시 반환합니다. 각각
코드는 특정 의미를 가집니다. 플러그인은 오른쪽 종료 코드를 사용하여 동일한 것을 나타냅니다.

다음 표에서는 오류 코드와 그 의미를 보여 줍니다.

종료 코드입니다	목적
0	작업이 성공했습니다.

종료 코드입니다	목적
99	요청된 작업이 지원되지 않거나 구현되지 않았습니다.
100	작업이 실패했습니다. 일시 중지 해제를 건너뛰고 를 종료합니다. 일시 중지 해제는 기본적으로 사용됩니다.
101	작업이 실패했습니다. 백업 작업을 계속합니다.
기타	작업이 실패했습니다. 중지 해제를 실행하고 종료합니다.

오류 메시지를 기록합니다

오류 메시지는 플러그인에서 SnapCenter 서버로 전달됩니다. 메시지가 표시됩니다
메시지, 로그 수준 및 타임 스탬프가 포함됩니다.

다음 표에는 레벨 및 그 용도가 나와 있습니다.

매개 변수	목적
정보	정보 메시지입니다
경고	경고 메시지
오류	오류 메시지
디버그	디버그 메시지입니다
트레이스	Trace 메시지

데이터 일관성 유지

사용자 지정 플러그인은 동일한 워크플로우 실행 작업 간 데이터를 보존합니다. 용
예를 들어, 플러그인은 중지 종료 시 데이터를 저장할 수 있으며 일시 중지 해제 중에 사용할 수 있습니다
작동.

보존할 데이터는 플러그인으로 결과 객체의 일부로 설정됩니다. 특정 형식을 따릅니다
및 은 각 플러그인 개발 스타일에 대해 자세히 설명합니다.

Perl 기반 개발

PERL을 사용하여 플러그인을 개발하는 동안 특정 규칙을 따라야 합니다.

- 내용을 읽을 수 있어야 합니다
- 필수 작업 setenv, quiesce 및 unquiesce를 구현해야 합니다
- 결과를 에이전트로 다시 전달하려면 특정 구문을 사용해야 합니다

- 콘텐츠는 <plugin_name>.pm 파일로 저장해야 합니다

사용 가능한 작업은 입니다

- 설정
- 버전
- 정지
- 정지 해제
- clone_pre, clone_post
- restore_pre, 복구하십시오
- 정리

일반적인 플러그인 처리

결과 개체 사용

모든 사용자 지정 플러그인 작업은 결과 개체를 정의해야 합니다. 이 개체는 메시지, 종료 코드, stdout 및 stderr를 다시 호스트 에이전트로 보냅니다.

결과 개체:

```
my $result = {
```

```
      exit_code => 0,
      stdout => "",
      stderr => "",
};
```

결과 객체 반환:

```
return $result;
```

데이터 일관성 유지

정리 작업을 제외한 작업 간 데이터를 동일한 워크플로 실행의 일부로 보존할 수 있습니다. 이 작업은 키 값 쌍을 사용하여 수행됩니다. 데이터의 키 값 쌍은 결과 개체의 일부로 설정되며 동일한 워크플로의 후속 작업에서 사용 가능한 것으로 유지됩니다.

다음 코드 샘플은 보존할 데이터를 설정합니다.

```
my $result = {
  exit_code => 0,
  stdout => "",
  stderr => "",
};
  $result->{env}->{'key1'} = 'value1';
  $result->{env}->{'key2'} = 'value2';
  ….
  return $result
```

위의 코드는 두 개의 키 값 쌍을 설정하며, 이러한 키 값 쌍은 후속 작업에서 입력으로 사용할 수 있습니다. 다음 코드를 사용하여 두 키 값 쌍에 액세스할 수 있습니다.

```
sub setENV {
    my ($self, $config) = @_;
    my $first_value = $config->{'key1'};
    my $second_value = $config->{'key2'};
    …
}
```

```
 === Logging error messages
```

각 작업은 콘텐츠를 표시하고 저장하는 호스트 에이전트로 메시지를 다시 보낼 수 있습니다. 메시지에는 메시지 수준, 타임스탬프 및 메시지 텍스트가 포함됩니다. 여러 줄 메시지가 지원됩니다.

```
Load the SnapCreator::Event Class:
my $msgObj = new SnapCreator::Event();
my @message_a = ();
```

msgObj 를 사용하여 Collect 메서드를 사용하여 메시지를 캡처합니다.

```
$msgObj->collect(\@message_a, INFO, "My INFO Message");
$msgObj->collect(\@message_a, WARN, "My WARN Message");
$msgObj->collect(\@message_a, ERROR, "My ERROR Message");
$msgObj->collect(\@message_a, DEBUG, "My DEBUG Message");
$msgObj->collect(\@message_a, TRACE, "My TRACE Message");
```

결과 객체에 메시지 적용:

```
$result->{message} = \@message_a;
```

플러그인 스텁 사용

사용자 지정 플러그인은 플러그인 스텁을 노출해야 합니다. SnapCenter 서버가 워크플로에 따라 호출하는 메서드입니다.

플러그인 스텁	선택 사항/필수 요소입니다	목적
설정	필수 요소입니다	이 스텁은 환경과 구성 개체를 설정합니다. 모든 환경 구문 분석 또는 처리는 여기에서 수행해야 합니다. 스텁이 호출될 때마다 setenv 스텁이 바로 전에 호출됩니다. PERL 스타일 플러그인에만 필요합니다.
버전	선택 사항	이 스텁은 응용 프로그램 버전을 가져오는 데 사용됩니다.
파악	선택 사항	이 스텁은 에이전트나 호스트에서 호스팅되는 인스턴스 또는 데이터베이스와 같은 애플리케이션 객체를 검색하는 데 사용됩니다. 플러그인은 응답의 일부로 검색된 애플리케이션 객체를 특정 형식으로 반환해야 합니다. 이 스텁은 응용 프로그램이 Unix용 SnapDrive와 통합된 경우에만 사용됩니다. Linux 파일 시스템(Linux 파일 시스템)이 지원됩니다. AIX/Solaris(Unix 유형)는 지원되지 않습니다.

플러그인 스텝	선택 사항/필수 요소입니다	목적
discovery_complete(검색 완료	선택 사항	이 스텝은 에이전트나 호스트에서 호스팅되는 인스턴스 또는 데이터베이스와 같은 애플리케이션 객체를 검색하는 데 사용됩니다. 플러그인은 응답의 일부로 검색된 애플리케이션 객체를 특정 형식으로 반환해야 합니다. 이 스텝은 응용 프로그램이 Unix용 SnapDrive와 통합된 경우에만 사용됩니다. Linux 파일 시스템(Linux 파일 시스템)이 지원됩니다. AIX 및 Solaris(Unix 유형)는 지원되지 않습니다.
정지	필수 요소입니다	이 스텝은 일시 중지를 수행합니다. 즉, 애플리케이션을 스냅샷 복사본을 생성할 수 있는 상태로 전환합니다. 이 이름은 스냅샷 복사본 작업 전에 호출됩니다. 보존할 애플리케이션의 메타데이터는 응답 과정에서 설정되어야 하며, 이 메타데이터는 후속 클론 생성 또는 복구 작업 중에 구성 매개 변수 형태로 해당 스토리지 스냅샷 복사본에 대해 반환됩니다.
정지 해제	필수 요소입니다	이 스텝은 중지 해제를 수행하는 역할을 하며, 이는 애플리케이션을 정상 상태로 전환하는 것을 의미합니다. 이 이름은 스냅샷 복사본을 생성한 후에 호출됩니다.
Clone_pre	선택 사항	이 스텝은 사전 클론 작업을 수행합니다. 기본 제공 SnapCenter 서버 클론 생성 인터페이스를 사용 중이며 클론 작업을 수행할 때 트리거됩니다.
clone_post	선택 사항	이 스텝은 사후 클론 작업을 수행하는 역할을 합니다. 이는 사용자가 기본 제공 SnapCenter 서버 클론 생성 인터페이스를 사용하고 있다고 가정하고 클론 작업을 수행할 때만 트리거됩니다.

플러그인 스텝	선택 사항/필수 요소입니다	목적
restore_pre	선택 사항	이 스텝은 PreRestore 작업을 수행하는 역할을 합니다. 이는 사용자가 기본 제공 SnapCenter 서버 복원 인터페이스를 사용하고 있으며 복원 작업을 수행하는 동안 트리거된다고 가정합니다.
복원	선택 사항	이 스텝은 애플리케이션 복구 작업을 수행하는 역할을 합니다. 이는 사용자가 기본 제공 SnapCenter 서버 복원 인터페이스를 사용하고 있다고 가정하고 복원 작업을 수행할 때만 트리거됩니다.
정리	선택 사항	이 스텝은 백업, 복구 또는 클론 작업 후 정리 작업을 수행합니다. 정리 작업은 정상적인 워크플로 실행 중 또는 워크플로 오류가 발생한 경우에 가능합니다. 백업, cloneVolAndLun 또는 fileOrVolRestore 등의 구성 매개 변수 작업을 참조하여 정리 작업이 호출되는 워크플로 이름을 유추할 수 있습니다. 구성 매개 변수 ERROR_MESSAGE는 워크플로우를 실행하는 동안 오류가 있는지 여부를 나타냅니다. ERROR_MESSAGE가 정의되어 있고 NULL이 아닌 경우 Workflow 장애 실행 중에 정리가 호출됩니다.
APP_VERSION	선택 사항	이 스텝은 SnapCenter에서 응용 프로그램을 가져오는 데 사용됩니다 플러그인에서 관리하는 버전 세부 정보

플러그인 패키지 정보

모든 플러그인에는 다음 정보가 있어야 합니다.

```
package MOCK;
our @ISA = qw(SnapCreator::Mod);
=head1 NAME
MOCK - class which represents a MOCK module.
=cut
=head1 DESCRIPTION
MOCK implements methods which only log requests.
=cut
use strict;
use warnings;
use diagnostics;
use SnapCreator::Util::Generic qw ( trim isEmpty );
use SnapCreator::Util::OS qw ( isWindows isUnix getUid
createTmpFile );
use SnapCreator::Event qw ( INFO ERROR WARN DEBUG COMMENT ASUP
CMD DUMP );
my $msgObj = new SnapCreator::Event();
my %config_h = ();
```

운영

사용자 지정 플러그인에서 지원하는 setenv, Version, Quiesce 및 Unquiesce와 같은 다양한 작업을 코딩할 수 있습니다.

setenv 작동

PERL을 사용하여 만든 플러그인에는 setenv 작업이 필요합니다. ENV를 설정하고 플러그인 매개변수에 쉽게 액세스할 수 있습니다.

```
sub setENV {
    my ($self, $obj) = @_;
    %config_h = %{$obj};
    my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
    };
    return $result;
}
```

버전 작업

버전 작업은 응용 프로그램 버전 정보를 반환합니다.

```
sub version {
  my $version_result = {
    major => 1,
    minor => 2,
    patch => 1,
    build => 0
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::quiesce");
  $version_result->{message} = \@message_a;
  return $version_result;
}
```

중지 작업

Quiesce 작업은 resources 매개 변수에 나열된 리소스에 대해 응용 프로그램 중지 작업을 수행합니다.

```
sub quiesce {
  my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::quiesce");
  $result->{message} = \@message_a;
  return $result;
}
```

작업 중지 해제

응용 프로그램 정지 해제를 위해서는 중지 해제 작업이 필요합니다. 리소스 목록은 resources 매개 변수에서 사용할 수 있습니다.

```
sub unquiesce {
  my $result = {
      exit_code => 0,
      stdout => "",
      stderr => "",
  };
  my @message_a = ();
  $msgObj->collect(\@message_a, INFO, "VOLUMES
$config_h{'VOLUMES'}");
  $msgObj->collect(\@message_a, INFO,
"$config_h{'APP_NAME'}::unquiesce");
  $result->{message} = \@message_a;
  return $result;
}
```

네이티브 스타일

SnapCenter는 플러그인 생성을 위해 비 PERL 프로그래밍 또는 스크립팅 언어를 지원합니다. 이를 스크립트 또는 배치 파일일 수 있는 네이티브 스타일 프로그래밍이라고 합니다.

네이티브 스타일 플러그인은 다음과 같은 특정 규칙을 따라야 합니다.

플러그인은 실행 가능해야 합니다

- Unix 시스템의 경우 에이전트를 실행하는 사용자는 플러그인에 대한 실행 권한이 있어야 합니다
- Windows 시스템의 경우 PowerShell 플러그인에는 접미사 .ps1, 기타 창이 있어야 합니다
  스크립트에는 .cmd 또는 .bat 접미사가 있어야 하며 사용자가 실행할 수 있어야 합니다
- 플러그인은 "-quiesce", "-unquiesce"와 같은 명령줄 인수에 반응해야 합니다.
- 작업 또는 기능이 구현되지 않은 경우 플러그인은 종료 코드 99를 반환해야 합니다
- 플러그인은 특정 구문을 사용하여 결과를 서버로 다시 전달해야 합니다

일반적인 플러그인 처리

오류 메시지를 로깅합니다

각 작업은 콘텐츠를 표시하고 저장하는 서버로 메시지를 다시 보낼 수 있습니다. 메시지에는 메시지 수준, 타임스탬프 및 메시지 텍스트가 포함됩니다. 여러 줄 메시지가 지원됩니다.

형식:

```
SC_MSG#<level>#<timestamp>#<message>
SC_MESSAGE#<level>#<timestamp>#<message>
```

SnapCenter 플러그인은 플러그인 스텁을 구현해야 합니다. SnapCenter 서버가 특정 워크플로를 기반으로 호출하는 메서드입니다.

플러그인 스텁	선택 사항/필수 요소입니다	목적
정지	필수 요소입니다	이 스텁은 정지 작업을 수행합니다. 그러면 가 배치됩니다 Snapshot 복사본을 생성할 수 있는 상태로 애플리케이션 저장 이 작업은 스토리지 스냅샷 복사본 작업 전에 호출됩니다.
정지 해제	필수 요소입니다	이 스텁은 정지 해제를 수행하는 역할을 합니다. 있습니다 정상 상태의 응용 프로그램입니다. 이 이름은 스토리지 후에 호출됩니다 스냅샷 복사본 작업:
Clone_pre	선택 사항	이 스텁은 사전 클론 작업을 수행합니다. 이는 사용자가 기본 제공 SnapCenter 클론 생성 인터페이스를 사용하고 있으며 작업 "clone_vol 또는 clone_lun"을 수행하는 동안에만 트리거된다는 것을 전제로 합니다.
clone_post	선택 사항	이 스텁은 사후 클론 작업을 수행하는 역할을 합니다. 이는 사용자가 기본 제공 SnapCenter 클론 생성 인터페이스를 사용 중이며 "clone_vol 또는 clone_lun" 작업을 수행하는 동안에만 트리거된다고 가정합니다.
restore_pre	선택 사항	이 스텁은 사전 복원 작업을 수행하는 역할을 합니다. 이는 사용자가 기본 제공 SnapCenter 복원 인터페이스를 사용하고 있다고 가정하고 복원 작업을 수행하는 동안에만 트리거됩니다.
복원	선택 사항	이 스텁은 모든 복구 작업을 수행합니다. 여기 기본 제공 복원 인터페이스를 사용하지 않는 것으로 가정합니다. 복구 작업을 수행하는 동안 트리거됩니다.

예

Windows PowerShell

시스템에서 스크립트를 실행할 수 있는지 확인합니다. 스크립트를 실행할 수 없는 경우 스크립트에 대해 Set-ExecutionPolicy bypass를 설정하고 작업을 재시도하십시오.

```
if ($args.length -ne 1) {
  write-warning "You must specify a method";
  break;
}
function log ($level, $message) {
  $d = get-date
  echo "SC_MSG#$level#$d#$message"
}
function quiesce {
  $app_name = (get-item env:APP_NAME).value
  log "INFO" "Quiescing application using script $app_name";
  log "INFO" "Quiescing application finished successfully"
}
function unquiesce {
  $app_name = (get-item env:APP_NAME).value
  log "INFO" "Unquiescing application using script $app_name";
  log "INFO" "Unquiescing application finished successfully"
}
  switch ($args[0]) {
    "-quiesce" {
    quiesce;
}
"-unquiesce" {
    unquiesce;
}
default {
    write-error "Function $args[0] is not implemented";
    exit 99;
  }
}
exit 0;
```

Java 스타일

Java 사용자 지정 플러그인은 데이터베이스, 인스턴스 등과 같은 응용 프로그램과 직접 상호 작용합니다.

제한 사항

Java 프로그래밍 언어를 사용하여 플러그인을 개발하는 동안 알아야 할 몇 가지 제한 사항이 있습니다.

플러그인 특성	**Java** 플러그인
복잡성	낮음-중간
메모리 공간	최대 10-20MB
다른 라이브러리에 대한 종속성	응용 프로그램 통신용 라이브러리
스레드 수입니다	1
스레드 런타임	1시간 미만

Java 제한에 대한 이유

SnapCenter 에이전트의 목표는 지속적이고 안전하고 강력한 애플리케이션 통합을 보장하는 것입니다. Java 플러그인을 지원함으로써 플러그인에서 메모리 누수 및 기타 원치 않는 문제를 일으킬 수 있습니다. 이러한 문제는 해결하기 어려우며, 특히 사용이 간편한 상태를 유지하는 것이 목표일 때 더욱 그렇습니다. 플러그인의 복잡성이 너무 복잡하지 않으면 개발자가 오류를 발생했을 가능성이 훨씬 줄어듭니다. Java 플러그인의 위험은 그들이 이다 SnapCenter 에이전트와 동일한 JVM에서 실행. 플러그인이 충돌하거나 메모리를 누출하면 Agent에도 부정적인 영향을 미칠 수 있습니다.

지원되는 방법

방법	필수 요소입니다	설명	언제 누가 부르는가**?**
버전	예	플러그인 버전을 반환해야 합니다.	SnapCenter 서버 또는 에이전트가 의 버전을 요청합니다 플러그인입니다.
정지	예	응용 프로그램에서 일시 중지를 수행해야 합니다. 대부분의 경우 이는 애플리케이션을 SnapCenter 서버가 백업을 생성할 수 있는 상태(예: 스냅샷 복사본)로 전환하는 것을 의미합니다.	SnapCenter 서버가 스냅샷 복사본을 생성하기 전에 또는 를 선택합니다 일반적으로 백업을 수행합니다.
정지 해제	예	응용 프로그램에서 정지 해제를 수행해야 합니다. 대부분의 경우, 이것은 입니다 응용 프로그램을 다시 정상 작동 상태로 전환하는 것을 의미합니다.	SnapCenter 서버가 스냅샷 복사본을 생성한 후 또는 이(가) 있는 경우 일반적으로 백업을 수행했습니다.

방법	필수 요소입니다	설명	언제 누가 부르는가?
정리	아니요	플러그인에서 청소해야 하는 모든 것을 정리하는 역할을 합니다.	SnapCenter 서버의 워크플로가 완료되면(성공 또는 실패)
ClonePre(사전	아니요	클론 작업을 수행하기 전에 수행해야 하는 작업을 수행해야 합니다.	사용자가 "cloneVol" 또는 "cloneLun" 작업을 트리거하고 내장된 클론 생성 마법사(GUI/CLI)를 사용하는 경우
ClonePost	아니요	클론 작업을 수행한 후 수행해야 하는 작업을 수행해야 합니다.	사용자가 "cloneVol" 또는 "cloneLun" 작업을 트리거하고 내장된 클론 생성 마법사(GUI/CLI)를 사용하는 경우
RestorePre	아니요	복구 작업을 호출하기 전에 수행해야 하는 작업을 수행해야 합니다.	사용자가 복구 작업을 트리거하는 경우
복원	아니요	애플리케이션의 복원/복구를 수행합니다.	사용자가 복구 작업을 트리거하는 경우
AppVersion(애플리케이션 버전)	아니요	플러그인으로 관리되는 응용 프로그램 버전을 검색합니다.	모든 워크플로우에서 백업/복원/클론과 같은 ASUP 데이터 수집의 일부

자습서

이 섹션에서는 Java 프로그래밍 언어를 사용하여 사용자 지정 플러그인을 만드는 방법에 대해 설명합니다.

일식을 설정합니다

1. Eclipse에서 새 Java 프로젝트 "TutorialPlugin"을 만듭니다
2. 마침 * 을 클릭합니다
3. 새 프로젝트 * → * 속성 * → * Java 빌드 경로 * → * 라이브러리 * → * 외부 jar 추가 * 를 마우스 오른쪽 버튼으로 클릭합니다
4. Host Agent의 ../lib/folder로 이동하여 jar scAgent-5.0-core.jar 및 common-5.0.jar 를 선택합니다
5. 프로젝트를 선택하고 * src 폴더 * → * New * → * Package * 를 마우스 오른쪽 단추로 클릭한 다음 com.netapp.snapcreator.agent.plugin.TutorialPlugin 이름의 새 패키지를 만듭니다
6. 새 패키지를 마우스 오른쪽 단추로 클릭하고 새로 만들기 → Java 클래스 를 선택합니다.
   a. 이름을 TutorialPlugin 으로 입력합니다.
   b. 수퍼클래스 찾아보기 단추를 클릭하고 "* AbstractPlugin"을 검색합니다. 하나의 결과만 표시되어야 합니다.

```
 "AbstractPlugin - com.netapp.snapcreator.agent.nextgen.plugin".
.. 마침 * 을 클릭합니다.
.. Java 클래스:
```

```
package com.netapp.snapcreator.agent.plugin.TutorialPlugin;
import
com.netapp.snapcreator.agent.nextgen.common.result.Describe
Result;
import
com.netapp.snapcreator.agent.nextgen.common.result.Result;
import
com.netapp.snapcreator.agent.nextgen.common.result.VersionR
esult;
import
com.netapp.snapcreator.agent.nextgen.context.Context;
import
com.netapp.snapcreator.agent.nextgen.plugin.AbstractPlugin;
public class TutorialPlugin extends AbstractPlugin {
  @Override
  public DescribeResult describe(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public Result quiesce(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public Result unquiesce(Context context) {
    // TODO Auto-generated method stub
    return null;
  }
  @Override
  public VersionResult version() {
    // TODO Auto-generated method stub
    return null;
  }
}
```

필요한 방법을 구현합니다

Quiesce, Unquiesce 및 version은 각 사용자 지정 Java 플러그인이 구현해야 하는 필수 메서드입니다.

다음은 플러그인 버전을 반환하는 버전 방법입니다.

```
@Override
public VersionResult version() {
    VersionResult versionResult = VersionResult.builder()
                                                .withMajor(1)
                                                .withMinor(0)
                                                .withPatch(0)
                                                .withBuild(0)
                                                .build();
    return versionResult;
}
```

```
Below is the implementation of quiesce and unquiesce method. These will be
interacting with   the application, which is being protected by SnapCenter
Server. As this is just a tutorial, the
application part is not explained, and the focus is more on the
functionality that SnapCenter   Agent provides the following to the plug-
in developers:
```

```
@Override
  public Result quiesce(Context context) {
    final Logger logger = context.getLogger();
    /*
      * TODO: Add application interaction here
    */
```

```
logger.error("Something bad happened.");
logger.info("Successfully handled application");
```

```
    Result result = Result.builder()
                    .withExitCode(0)
                    .withMessages(logger.getMessages())
                    .build();
    return result;
}
```

이 메서드는 Context 개체에 전달됩니다. 여기에는 Logger 및 Context Store 같은 여러 도우미뿐만 아니라 현재 작업에 대한 정보(workflow-ID, job-ID)도 포함됩니다. FINAL Logger = CONTEXT.getLogger(); 를 호출하여 로거를 가져올 수 있습니다. Logger 개체는 다른 로깅 프레임워크에서 알려진 유사한 메서드(예: logback)를 제공합니다. 결과 개체에서 종료 코드를 지정할 수도 있습니다. 이 예제에서는 문제가 없으므로 0이 반환됩니다. 다른 종료 코드는 다른

실패 시나리오에 매핑할 수 있습니다.

결과 개체 사용

결과 개체에는 다음 매개 변수가 포함됩니다.

매개 변수	기본값	설명
구성	비어 있습니다 구성	이 매개 변수는 구성 매개 변수를 서버로 다시 보내는 데 사용할 수 있습니다. 바로 그것입니다 플러그인이 업데이트하려는 매개 변수가 될 수 있습니다. 이 변경 사항이 인지 여부 SnapCenter 서버의 구성에 실제로 반영되는 것은 에 따라 다릅니다 config의 app_CONF_persistency=Y 또는 N 매개 변수입니다.
ExitCode를 참조하십시오	0	작업의 상태를 나타냅니다. "0"은 작업이 인 것을 의미합니다 성공적으로 실행되었습니다. 다른 값은 오류 또는 경고를 나타냅니다.
Stdout(스토우아웃)	비어 있습니다 목록	stdout 메시지를 SnapCenter로 다시 전송하는 데 사용할 수 있습니다 서버.
Stderr	비어 있습니다 목록	stderr 메시지를 SnapCenter로 다시 전송하는 데 사용할 수 있습니다 서버.
메시지	비어 있습니다 목록	이 목록에는 플러그인에서 으로 반환하려는 모든 메시지가 포함되어 있습니다 서버. SnapCenter 서버는 이러한 메시지를 CLI 또는 GUI에 표시합니다.

SnapCenter 에이전트는 빌더를 제공합니다 ("작성기 패턴")를 참조하십시오 결과 유형. 따라서 다음과 같이 매우 간단하게 사용할 수 있습니다.

```
Result result = Result.builder()
                    .withExitCode(0)
                    .withStdout(stdout)
                    .withStderr(stderr)
                    .withConfig(config)
                    .withMessages(logger.getMessages())
                    .build()
```

예를 들어, 종료 코드를 0으로 설정하고, stdout 및 stderr에 대한 목록을 설정하고, config 매개 변수를 설정하고, 서버로 다시 전송될 로그 메시지를 추가합니다. 모든 매개 변수가 필요하지 않으면 필요한 매개 변수만 보냅니다. 각 매개 변수에는 기본값이 있으므로 아래 코드에서 .withExitCode(0)를 제거하면 결과는 영향을 받지 않습니다.

```
Result result = Result.builder()
                      .withExitCode(0)
                      .withMessages(logger.getMessages())
                      .build();
```

버전

VersionResult 는 SnapCenter 서버에 플러그인 버전을 알립니다. 상속됩니다
그 결과 구성, exitCode, stdout, stderr 및 메시지 매개 변수가 포함됩니다.

매개 변수	기본값	설명
전공	0	플러그인의 주 버전 필드입니다.
경미합니다	0	플러그인의 부 버전 필드입니다.
패치	0	플러그인의 패치 버전 필드입니다.
빌드	0	플러그인의 빌드 버전 필드입니다.

예를 들면 다음과 같습니다.

```
VersionResult result = VersionResult.builder()
                                    .withMajor(1)
                                    .withMinor(0)
                                    .withPatch(0)
                                    .withBuild(0)
                                    .build();
```

컨텍스트 객체 사용

컨텍스트 개체는 다음 메서드를 제공합니다.

컨텍스트 방법입니다	목적
문자열 getWorkflowId();	에 대해 SnapCenter 서버에서 사용 중인 워크플로 ID를 반환합니다 현재 워크플로.
구성 getconfig();	SnapCenter 서버에서 으로 전송 중인 구성을 반환합니다 에이전트.

Workflow-ID입니다

workflow-ID는 SnapCenter 서버가 실행 중인 특정 를 참조하는 데 사용하는 ID입니다
워크플로우.

구성

이 개체에는 사용자가 의 config에서 설정할 수 있는 매개 변수가 대부분 포함되어 있습니다
SnapCenter 서버. 그러나 보안상의 이유로 이러한 매개 변수 중 일부가 발생할 수 있습니다
서버 측에서 필터링함. 다음은 Config에 액세스하여 검색하는 방법에 대한 예입니다
매개 변수:

```
final Config config = context.getConfig();
String myParameter =
config.getParameter("PLUGIN_MANDATORY_PARAMETER");
```

이제 ""//myParameter"에 SnapCenter 서버의 config에서 읽은 매개 변수가 포함되어 있습니다
config 매개 변수 키가 없으면 빈 String("")이 반환됩니다.

플러그인을 내보내는 중입니다

SnapCenter 호스트에 설치하려면 플러그인을 내보내야 합니다.

Eclipse에서 다음 작업을 수행합니다.

1. 플러그인의 기본 패키지를 마우스 오른쪽 단추로 클릭합니다(이 예에서는)
   com.netapp.snapcreator.agent.plugin.TutorialPlugin 참조하십시오.
2. 내보내기 * → * Java * → * JAR 파일 * 을 선택합니다
3. 다음 * 을 클릭합니다.
4. 다음 창에서 대상 jar 파일 경로를 지정합니다. tutorial_plugin.jar
   플러그인의 기본 클래스는 TutorialPlugin.class 로 명명되며 이 플러그인은 폴더에 추가해야 합니다
   같은 이름을 가진.

플러그인이 추가 라이브러리에 종속된 경우 lib / 폴더를 만들 수 있습니다

플러그인이 종속된 jar 파일을 추가할 수 있습니다(예: 데이터베이스 드라이버). 시기
SnapCenter는 플러그인을 로드하며 이 폴더의 모든 jar 파일을 및 에 자동으로 연결합니다
클래스 경로에 추가합니다.

SnapCenter의 사용자 지정 플러그인

SnapCenter의 사용자 지정 플러그인

Java, PERL 또는 네이티브 스타일을 사용하여 만든 사용자 지정 플러그인은 SnapCenter 서버를 사용하여 호스트에 설치하여 응용 프로그램의 데이터 보호를 활성화할 수 있습니다. 이 자습서에 제공된 절차를 사용하여 SnapCenter 호스트에 설치하려면 플러그인을 내보내야 합니다.

생성된 모든 플러그인에 대해 설명 파일이 있어야 합니다. 설명 파일에는 플러그인의 세부 정보가 설명되어 있습니다. 파일 이름은 Plugin_descriptor.xml이어야 합니다.

플러그인 설명자 파일 특성 및 그 중요성을 사용합니다

속성	설명
이름	플러그인의 이름입니다. 영숫자 문자는 사용할 수 있습니다. 예: DB2, MySQL, MongoDB 네이티브 스타일로 만들어진 플러그인의 경우 파일 확장명을 제공하지 않아야 합니다. 예를 들어 플러그인 이름이 mongodb.sh인 경우 이름을 mongodb로 지정합니다.
버전	플러그인 버전입니다. 주 버전과 부 버전을 모두 포함할 수 있습니다. 예: 1.0, 1.1, 2.0, 2.1
표시 이름	SnapCenter 서버에 표시할 플러그인 이름입니다. 동일한 플러그인의 여러 버전이 기록되는 경우 모든 버전에서 표시 이름이 동일한지 확인하십시오.
PluginType입니다	플러그인을 만드는 데 사용되는 언어입니다. 지원되는 값은 Perl, Java 및 Native입니다. 기본 플러그인 유형에는 Unix/Linux 셸 스크립트, Windows 스크립트, Python 또는 기타 스크립팅 언어가 포함됩니다.
OSNAME	플러그인이 설치된 호스트 OS 이름입니다. 유효한 값은 Windows 및 입니다 리눅스. PERL 유형 플러그인과 같은 여러 OS 유형에서 단일 플러그인을 배포할 수 있습니다.
OSVersion(OS버전)	플러그인이 설치된 호스트 OS 버전입니다.
리소스 이름	플러그인이 지원할 수 있는 리소스 유형의 이름입니다. 예를 들어, 데이터베이스, 인스턴스, 컬렉션.
모체	이 경우 ResourceName 은 다른 리소스 유형에 따라 계층적으로 종속됩니다 Parent 부모 ResourceType 을 결정합니다. 예를 들어, DB2 플러그인에서 ResourceName “Database”에는 부모 “인스턴스”가 있습니다.

속성	설명
RequireFileSystemPlugin	예 또는 아니요 복구 탭이 인지 여부를 결정합니다 복원 마법사에 표시됩니다.
ResourceRequiresAuthentication을 참조하십시오	예 또는 아니요 자동으로 검색되거나 자동으로 검색되지 않은 리소스를 결정합니다 다음 이후에 데이터 보호 작업을 수행하려면 자동 검색의 자격 증명이 필요합니다 스토리지 검색
RequireFileSystemClone 을 참조하십시오	예 또는 아니요 플러그인에 클론을 위한 FileSystem 플러그인 통합이 필요한지 여부를 결정합니다 워크플로우.

사용자 지정 플러그인 DB2에 대한 Plugin_descriptor.xml 파일의 예는 다음과 같습니다.

```
<Plugin>
<SMSServer></SMSServer>
<Name>DB2</Name>
<Version>1.0</Version>
<PluginType>Perl</PluginType>
<DisplayName>Custom DB2 Plugin</DisplayName>
<SupportedOS>
<OS>
<OSName>windows</OSName>
<OSVersion>2012</OSVersion>
</OS>
<OS>
<OSName>Linux</OSName>
<OSVersion>7</OSVersion>
</OS>
</SupportedOS>
<ResourceTypes>
<ResourceType>
<ResourceName>Database</ResourceName>
<Parent>Instance</Parent>
</ResourceType>
<ResourceType>
<ResourceName>Instance</ResourceName>
</ResourceType>
</ResourceTypes>
<RequireFileSystemPlugin>no</RequireFileSystemPlugin>
<ResourceRequiresAuthentication>yes</ResourceRequiresAuthentication>
<SupportsApplicationRecovery>yes</SupportsApplicationRecovery>
</Plugin>
```

ZIP 파일 생성

플러그인을 개발하고 설명자 파일을 만든 후에는 플러그인 파일 및 을 추가해야 합니다
Plugin_descriptor.xml 파일을 폴더로 압축하여 압축합니다.

ZIP 파일을 작성하기 전에 다음 사항을 고려해야 합니다.

- 스크립트 이름은 플러그인 이름과 같아야 합니다.
- PERL 플러그인의 경우 ZIP 폴더에 스크립트 파일과 가 있는 폴더가 있어야 합니다
  설명 파일은 이 폴더 외부에 있어야 합니다. 폴더 이름은 과 같아야 합니다
  플러그인 이름입니다.
- PERL 플러그인 이외의 플러그인의 경우 ZIP 폴더에 설명자와 가 포함되어 있어야 합니다
  스크립트 파일
- OS 버전은 숫자여야 합니다.

예:

- DB2 플러그인: DB2.pm 및 Plugin_descriptor.xml 파일을 “DB2.zip”에 추가합니다.
- Java를 사용하여 개발된 플러그인: jar 파일 추가, 종속 jar 파일 및 Plugin_descriptor.xml 파일을 폴더로 압축하여 압축합니다.

플러그인 **ZIP** 파일을 업로드하는 중입니다

플러그인을 사용할 수 있도록 플러그인 ZIP 파일을 SnapCenter 서버에 업로드해야 합니다 원하는 호스트에 구축

UI 또는 cmdlet을 사용하여 플러그인을 업로드할 수 있습니다.

- UI: *
- 플러그인 ZIP 파일을 * 추가 * 또는 * 호스트 수정 * 워크플로우 마법사의 일부로 업로드합니다
- “사용자 지정 플러그인을 업로드하려면 선택하십시오.” * 를 클릭합니다
- PowerShell: *
- Upload-SmPluginPackage cmdlet

  예를 들어, PS > 업로드 - SmPluginPackage - AbsolutePath c:\DB2_1.zip

  PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말 또는 을 참조하십시오 cmdlet 참조 정보를 참조하십시오.

"SnapCenter 소프트웨어 cmdlet 참조 가이드".

사용자 지정 플러그인 배포

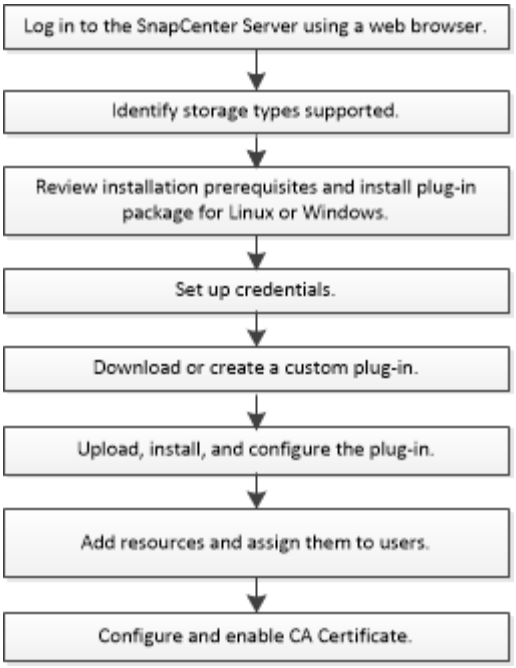
이제 업로드된 사용자 지정 플러그인을 의 일부로 원하는 호스트에 배포할 수 있습니다 * 호스트 추가 * 및 * 호스트 수정 * 워크플로우. 에 여러 버전의 플러그인을 업로드할 수 있습니다 SnapCenter 서버 및 특정 호스트에 배포할 버전을 선택할 수 있습니다.

플러그인을 업로드하는 방법에 대한 자세한 내용은 을 참조하십시오. "호스트를 추가하고 원격 호스트에 플러그인 패키지를 설치합니다"

SnapCenter 사용자 지정 플러그인 설치를 준비합니다

SnapCenter 맞춤형 플러그인의 설치 워크플로우

사용자 지정 플러그인 리소스를 보호하려면 SnapCenter 사용자 지정 플러그인을 설치하고 설정해야 합니다.



"응용 프로그램용 플러그인을 개발합니다"

호스트 추가 및 **SnapCenter** 사용자 지정 플러그인 설치를 위한 사전 요구 사항

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 완료해야 합니다. 사용자 지정 플러그인은 Windows 및 Linux 환경 모두에서 사용할 수 있습니다.

- 사용자 지정 플러그인을 만들어야 합니다. 자세한 내용은 개발자 정보를 참조하십시오.

  "응용 프로그램용 플러그인을 개발합니다"

- MySQL 또는 DB2 애플리케이션을 관리하려면 NetApp에서 제공하는 MySQL 및 DB2 사용자 지정 플러그인을 다운로드해야 합니다.
- Linux 또는 Windows 호스트에 Java 1.8 또는 Java 11(64비트)을 설치해야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에 속한 경우 호스트에서 UAC를 비활성화해야 합니다.
- 호스트 추가 작업이 수행되는 클라이언트 호스트에서 사용자 지정 플러그인을 사용할 수 있어야 합니다.

일반

iSCSI를 사용하는 경우 iSCSI 서비스가 실행되고 있어야 합니다.

SHA512 해시

- NetApp에서 제공하는 사용자 지정 플러그인의 경우 사용자 지정 플러그인 파일의 SHA512 해시를 _CUSTOM_PLUGIN_CHECKSH체크섬_LIST_FILE에 추가해야 합니다.
  - Linux 호스트의 경우 SHA512 해시는 _/var/opt/snapcenter/SCC/custom_plugin_checksum_list.txt_에 있습니다
  - Windows 호스트의 경우 SHA512 해시는 에 있습니다

C:\Program Files\NetApp\SnapCenter Plug-in Creator\etc\custom_plugin_checksum_list.txt

사용자 지정 설치 경로의 경우 SHA512 해시는 _<사용자 지정 경로>\NetApp\SnapCenter\Snapcenter 플러그인 생성자\etc\custom_plugin_checksum_list.txt_에 있습니다

custom_plugin_checksum_list 는 SnapCenter에서 호스트에 설치하는 사용자 지정 플러그인 설치의 일부입니다.

- 응용 프로그램에 대해 생성된 사용자 지정 플러그인의 경우 다음 단계를 수행해야 합니다.

  a. 플러그인 zip 파일의 SHA512 해시를 생성했습니다.

  과 같은 온라인 도구를 사용할 수 있습니다 "SHA512 해시".

  b. 생성된 SHA512 해시를 새 줄에 CUSTOM_PLUGIN_CHECK체크섬_LIST 파일에 추가했습니다.

  주석은 # 기호로 시작하여 해시가 속한 플러그인을 식별합니다.

  다음은 체크섬 파일의 SHA512 해시 항목의 예입니다.

```
#ORASCPM
03721f567a1e4a1cb5569066b9a58af619ee12b1f8713108f81b696cfbdb81c25232fa63
d6e6777a2b2a1ec068bb0a93a59a8ade71587182f8bccbe81f7e0ba6
```

Windows 호스트

- 원격 호스트에 대한 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 도메인 사용자가 있어야 합니다.
- SnapCenter에서 클러스터 노드를 관리하는 경우 클러스터의 모든 노드에 대한 관리 권한이 있는 사용자가 있어야 합니다.

Linux 호스트

- 루트 또는 루트 이외의 사용자에 대해 암호 기반 SSH 연결을 활성화해야 합니다.
- Linux 호스트에 Java 1.8 또는 Java 11(64비트)을 설치해야 합니다.

  SnapCenter 서버 호스트에 Windows Server 2019 또는 Windows Server 2016을 사용하는 경우 Java 1.8 또는 Java 11(64비트)을 설치해야 합니다. 상호 운용성 매트릭스 툴(IMT): 요구사항에 대한 최신 정보를 제공합니다.

  "모든 운영 체제에 대한 Java 다운로드"

  "NetApp 상호 운용성 매트릭스 툴"

- 여러 경로에 대한 액세스를 제공하려면 비루트 사용자에 대해 sudo 권한을 구성해야 합니다. visudo Linux 유틸리티를 사용하여 /etc/sudoers 파일에 다음 행을 추가합니다.

  Sudo 버전 1.8.7 이상을 사용하고 있는지 확인합니다.

```
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 !visiblepw
Defaults: LINUX_USER !requiretty
```

_linux_user_는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

_C:\ProgramData\NetApp\SnapCenter\Package Repository_에 있는 * Oracle_checksum.txt * 파일에서 _checksum_value_를 가져올 수 있습니다.

이 예제는 고유한 데이터를 만들기 위한 참조로만 사용해야 합니다.

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항 및 사이징 요구 사항을 숙지해야 합니다.

항목	요구 사항
운영 체제	Microsoft Windows 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB

항목	요구 사항
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	• Microsoft .NET Framework 4.7.2 이상 • WMF(Windows Management Framework) 4.0 이상 • PowerShell 4.0 이상 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴". NET 관련 문제 해결에 대한 자세한 내용은 을 참조하십시오 "인터넷에 연결되지 않은 기존 시스템의 경우 SnapCenter 업그레이드 또는 설치가 실패합니다."

Linux용 SnapCenter 플러그인 패키지 설치를 위한 호스트 요구 사항

Linux용 SnapCenter 플러그인 패키지를 설치하기 전에 호스트가 요구 사항을 충족하는지 확인해야 합니다.

항목	요구 사항
운영 체제	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server(SLES)
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	2GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.

항목	요구 사항
필요한 소프트웨어 패키지	Java 1.8(64비트) Oracle Java 또는 OpenJDK Flavors Java를 최신 버전으로 업그레이드한 경우 /var/opt/snapcenter/spl/etc/spl.properties 에 있는 java_home 옵션이 올바른 Java 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다.

지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴"

SnapCenter 사용자 지정 플러그인에 대한 자격 증명을 설정합니다

SnapCenter는 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다. 데이터베이스 또는 Windows 파일 시스템에서 데이터 보호 작업을 수행하려면 SnapCenter 플러그인 설치를 위한 자격 증명과 추가 자격 증명을 만들어야 합니다.

시작하기 전에

- Linux 호스트

  Linux 호스트에 플러그인을 설치하기 위한 자격 증명을 설정해야 합니다.

  플러그인 프로세스를 설치 및 시작할 수 있는 sudo 권한이 있는 루트 사용자 또는 루트 이외의 사용자에 대한 자격 증명을 설정해야 합니다.

  * 모범 사례: * 호스트를 구축하고 플러그인을 설치한 후 Linux에 대한 자격 증명을 생성할 수 있지만, 모범 사례는 호스트를 구축하고 플러그인을 설치하기 전에 SVM을 추가한 후 자격 증명을 생성하는 것입니다.

- Windows 호스트

  플러그인을 설치하기 전에 Windows 자격 증명을 설정해야 합니다.

  원격 호스트에 대한 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정해야 합니다.

- 맞춤형 플러그인 애플리케이션

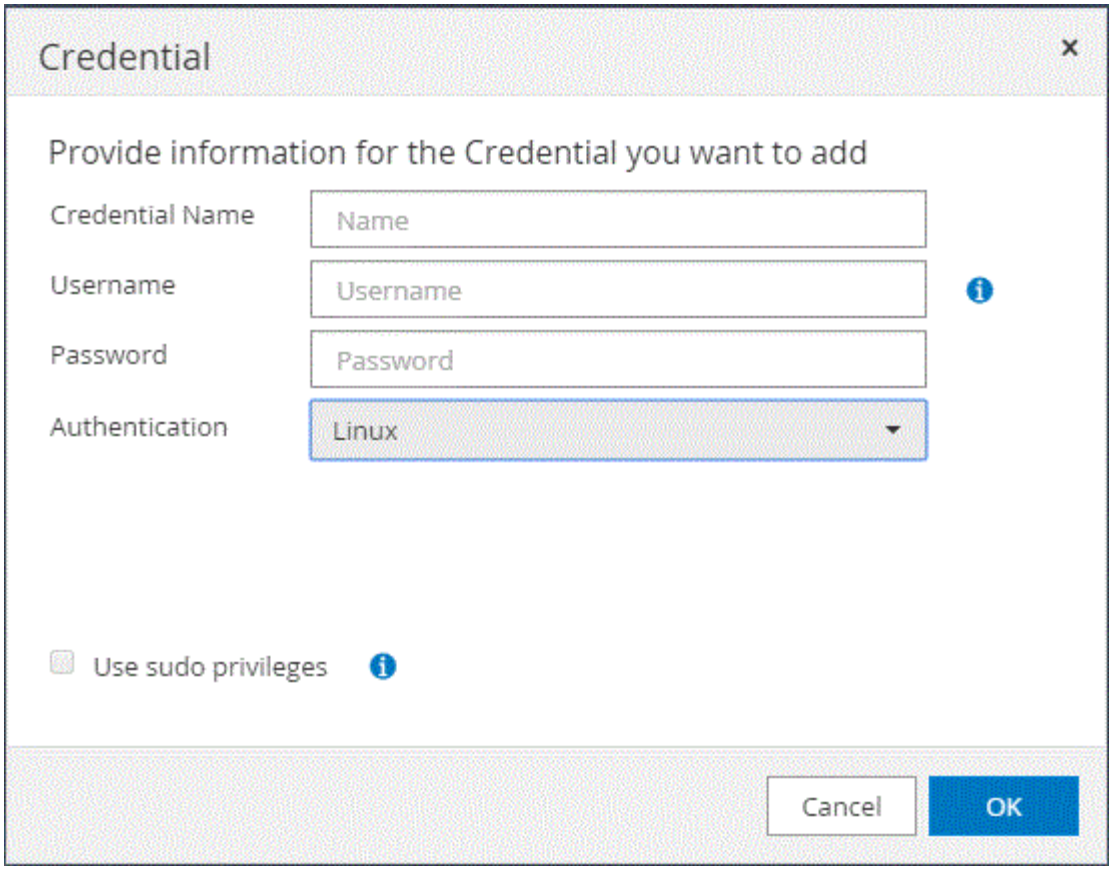
  플러그인은 리소스를 추가하는 동안 선택 또는 생성된 자격 증명을 사용합니다. 데이터 보호 작업 중에 리소스에 자격 증명이 필요하지 않은 경우 자격 증명을 * 없음 * 으로 설정할 수 있습니다.

이 작업에 대해

개별 리소스 그룹에 대한 자격 증명을 설정했고 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 증명 구성에 필요한 정보를 지정합니다.

이 필드의 내용...	수행할 작업...
자격 증명 이름입니다	자격 증명의 이름을 입력합니다.
사용자 이름입니다	인증에 사용할 사용자 이름과 암호를 입력합니다. • 도메인 관리자 또는 관리자 그룹의 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹의 구성원을 지정합니다. 사용자 이름 필드에 유효한 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 제공 로컬 관리자를 지정합니다. 사용자 계정에 상승된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 올바른 형식은 _ 사용자 이름 _ 입니다

이 필드의 내용...	수행할 작업...
암호	인증에 사용되는 암호를 입력합니다.
인증 모드	사용할 인증 모드를 선택합니다.
sudo 권한을 사용합니다	루트가 아닌 사용자에 대한 자격 증명을 생성하는 경우 * sudo 권한 사용 * 확인란을 선택합니다. Linux 사용자에게만 적용됩니다.

5. 확인 * 을 클릭합니다.

자격 증명 설정을 마친 후 사용자 및 액세스 페이지의 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

Windows Server 2012 이상에서 GMSA를 구성합니다

Windows Server 2012 이상을 사용하면 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 GMSA(Managed Service Account)를 만들 수 있습니다.

시작하기 전에

- Windows Server 2012 이상의 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2012 이상 호스트가 있어야 합니다.

단계

1. KDS 루트 키를 생성하여 GMSA의 각 개체에 대해 고유한 암호를 생성합니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 Add-KDSRootKey-EffectiveImmediately 명령을 실행합니다
3. GMSA 생성 및 구성:
   a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
 domainName\accountName$
.. 그룹에 컴퓨터 개체를 추가합니다.
.. 방금 생성한 사용자 그룹을 사용하여 GMSA를 생성합니다.
```

   예를 들면, 다음과 같습니다.

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. 실행 `Get-ADServiceAccount` 명령을 사용하여 서비스 계정을 확인합니다.
```

4. 호스트에서 GMSA를 구성합니다.

   a. GMSA 계정을 사용할 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.

      이렇게 하려면 PowerShell에서 다음 명령을 실행합니다.

```
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 확인합니다. `Test-AdServiceAccount <gMSA>`

5. 호스트에서 구성된 GMSA에 관리 권한을 할당합니다.

6. SnapCenter 서버에서 구성된 GMSA 계정을 지정하여 Windows 호스트를 추가합니다.

   SnapCenter 서버는 선택한 플러그인을 호스트에 설치하고 지정된 GMSA는 플러그인 설치 중에 서비스 로그온 계정으로 사용됩니다.

SnapCenter 사용자 지정 플러그인을 설치합니다

호스트를 추가하고 원격 호스트에 플러그인 패키지를 설치합니다

SnapCenterAdd 호스트 페이지를 사용하여 호스트를 추가한 다음 플러그인 패키지를 설치해야 합니다. 플러그인은 원격 호스트에 자동으로 설치됩니다. 호스트를 추가하고 개별 호스트 또는 클러스터에 대한 플러그인 패키지를 설치할 수 있습니다.

시작하기 전에

- 플러그인 설치 및 제거 권한이 있는 역할(예: SnapCenter 관리자 역할)에 할당된 사용자여야 합니다.
- 메시지 큐 서비스가 실행 중인지 확인해야 합니다.

- 그룹 GMSA(Managed Service Account)를 사용하는 경우 관리자 권한으로 GMSA를 구성해야 합니다.

  "사용자 지정 응용 프로그램에 대해 Windows Server 2012 이상에서 그룹 관리 서비스 계정을 구성합니다"

이 작업에 대해

SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.

WSFC(클러스터에 플러그인)를 설치하면 클러스터의 모든 노드에 플러그인이 설치됩니다.

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 선택합니다.
2. 맨 위에 * Managed Hosts * 탭이 선택되어 있는지 확인합니다.
3. 추가 * 를 선택합니다.
4. 호스트 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
호스트 유형	호스트 유형을 선택합니다. • Windows • 리눅스 사용자 지정 플러그인은 Windows 및 Linux 환경 모두에서 사용할 수 있습니다.
호스트 이름입니다	FQDN(정규화된 도메인 이름) 또는 호스트의 IP 주소를 입력합니다. SnapCenter는 DNS의 올바른 구성에 따라 달라집니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다. Windows 환경의 경우 IP 주소는 FQDN으로 확인되는 경우에만 신뢰할 수 없는 도메인 호스트에 대해 지원됩니다. 독립 실행형 호스트의 IP 주소 또는 FQDN을 입력할 수 있습니다. SnapCenter를 사용하여 호스트를 추가하고 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.

이 필드의 내용...	수행할 작업...
자격 증명	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성합니다. 자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하십시오. 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 의해 결정됩니다.

5. 설치할 플러그인 선택 * 섹션에서 설치할 플러그인을 선택합니다.
6. (선택 사항) * 추가 옵션 * 을 선택합니다.

이 필드의 내용...	수행할 작업...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정합니다. 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.

이 필드의 내용...	수행할 작업...
설치 경로	사용자 지정 플러그인은 Windows 시스템 또는 Linux 시스템에 설치할 수 있습니다. • Windows용 SnapCenter 플러그인 패키지의 경우 기본 경로는 C:\Program Files\NetApp\SnapCenter입니다. 선택적으로 경로를 사용자 지정할 수 있습니다. • Linux용 SnapCenter 플러그인 패키지의 경우 기본 경로는 입니다 `/opt/NetApp/snapcenter`. 선택적으로 경로를 사용자 지정할 수 있습니다. • SnapCenter 맞춤형 플러그인: i. 사용자 지정 플러그인 섹션에서 * 찾아보기 * 를 선택하고 압축된 사용자 지정 플러그인 폴더를 선택합니다. 압축된 폴더에는 사용자 지정 플러그인 코드와 descriptor.xml 파일이 들어 있습니다. 스토리지 플러그인의 경우 로 이동합니다 *`C:\ProgramData\NetApp\SnapCenter\Package Repository`* 를 선택하고 를 선택합니다 `Storage.zip` 폴더. ii. 업로드 * 를 선택합니다. 압축된 사용자 지정 플러그인 폴더의 descriptor.xml 파일은 패키지를 업로드하기 전에 유효성을 검사합니다. SnapCenter 서버에 업로드되는 사용자 지정 플러그인이 나열됩니다. MySQL 또는 DB2 애플리케이션을 관리하려는 경우 NetApp에서 제공하는 MySQL 및 DB2 사용자 지정 플러그인을 사용할 수 있습니다. MySQL 및 DB2 맞춤형 플러그인은 에서 사용할 수 있습니다 "NetApp 자동화 스토어"
사전 설치 검사를 건너뜁니다	플러그인이 이미 수동으로 설치되어 있고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.

이 필드의 내용...	수행할 작업...
그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행합니다	Windows 호스트의 경우 그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행하려면 이 확인란을 선택합니다. GMSA 이름을 domainName\accountName$ 형식으로 제공합니다. GMSA는 SnapCenter Plug-in for Windows 서비스에 대해서만 로그온 서비스 계정으로 사용됩니다.

7. 제출 * 을 선택합니다.

   Skip Prech사전 검사 * 확인란을 선택하지 않은 경우 호스트가 플러그인 설치 요구 사항을 충족하는지 여부를 확인합니다. 디스크 공간, RAM, PowerShell 버전, .NET 버전, 위치(Windows 플러그인의 경우) 및 Java 버전(Linux 플러그인의 경우)은 최소 요구 사항에 따라 검증됩니다. 최소 요구 사항이 충족되지 않으면 적절한 오류 또는 경고 메시지가 표시됩니다.

   오류가 디스크 공간 또는 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 파일을 업데이트해야 합니다.

8. 호스트 유형이 Linux인 경우 지문을 확인한 다음 * 확인 및 제출 * 을 선택합니다.

   동일한 호스트가 SnapCenter에 이전에 추가되었고 지문이 확인되었더라도 지문 확인은 필수입니다.

9. 설치 과정을 모니터링합니다.

   설치별 로그 파일은 에 있습니다 `/custom_location/snapcenter/` 로그.

cmdlet을 사용하여 여러 원격 호스트에 **Linux** 또는 **Windows**용 **SnapCenter** 플러그인 패키지를 설치합니다

설치-SmHostPackage PowerShell cmdlet을 사용하여 Linux 또는 Windows용 SnapCenter 플러그인 패키지를 여러 호스트에 동시에 설치할 수 있습니다.

시작하기 전에

호스트를 추가하는 사용자는 호스트에 대한 관리 권한이 있어야 합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 Open-SmConnection cmdlet을 사용하여 세션을 설정한 다음 자격 증명을

입력합니다.

3. Install-SmHostPackage cmdlet 및 필수 매개 변수를 사용하여 여러 호스트에 플러그인을 설치합니다.

   cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

   플러그인을 수동으로 설치했으며 호스트가 플러그인을 설치하는 데 필요한 요구 사항을 충족하는지 확인하지 않으려는 경우 -skipprecheck 옵션을 사용할 수 있습니다.

4. 원격 설치를 위한 자격 증명을 입력합니다.

명령줄 인터페이스를 사용하여 **Linux** 호스트에 **SnapCenter** 사용자 지정 플러그인을 설치합니다

SnapCenter UI(사용자 인터페이스)를 사용하여 SnapCenter 사용자 지정 플러그인을 설치해야 합니다. 사용자 환경에서 SnapCenter UI에서 플러그인을 원격으로 설치할 수 없는 경우 CLI(Command-Line Interface)를 사용하여 콘솔 모드 또는 자동 모드로 사용자 지정 플러그인을 설치할 수 있습니다.

단계

1. C:\ProgramData\NetApp\SnapCenter\Package Repository에서 Linux 설치 파일(snapcenter_linux_host_plugin.bin)용 SnapCenter 플러그인 패키지를 사용자 지정 플러그인을 설치할 호스트에 복사합니다.

   SnapCenter 서버가 설치된 호스트에서 이 경로에 액세스할 수 있습니다.

2. 명령 프롬프트에서 설치 파일을 복사한 디렉토리로 이동합니다.

3. 플러그인 설치: `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 cmdlet 및 필수 매개 변수를 사용하여 SnapCenter 서버에 호스트를 추가합니다.

   명령에 사용할 수 있는 매개 변수와 해당 설명에 대한 정보는 _get-Help command_name_을 실행하여 얻을 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

5. SnapCenter에 로그인하고 UI에서 또는 PowerShell cmdlet을 사용하여 사용자 지정 플러그인을 업로드합니다.

   을 참조하여 UI에서 사용자 지정 플러그인을 업로드할 수 있습니다 "호스트를 추가하고 원격 호스트에 플러그인 패키지를 설치합니다" 섹션을 참조하십시오.

   SnapCenter cmdlet 도움말 및 cmdlet 참조 정보에 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

   "SnapCenter 소프트웨어 cmdlet 참조 가이드".

사용자 지정 플러그인 설치 상태를 모니터링합니다

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행률을 모니터링할 수 있습니다. 설치 진행 상황을 확인하여 설치 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다

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 클릭합니다.
   b. 선택 사항: 시작 및 종료 날짜를 지정합니다.
   c. 유형 드롭다운 메뉴에서 * 플러그인 설치 * 를 선택합니다.
   d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
   e. 적용 * 을 클릭합니다.
4. 설치 작업을 선택하고 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. Job Details * 페이지에서 * View logs * 를 클릭합니다.

CA 인증서를 구성합니다

CA 인증서 **CSR** 파일을 생성합니다

CSR(인증서 서명 요청)을 생성하고 생성된 CSR을 사용하여 CA(인증 기관)에서 가져올 수 있는 인증서를 가져올 수 있습니다. 인증서에 연결된 개인 키가 있습니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.

CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 자세한 내용은 을 참조하십시오 "CA 인증서 CSR 파일을 생성하는 방법".

도메인(* .domain.company.com) 또는 시스템(machine1.domain.company.com CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter를 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN) 및 해당 호스트 이름을 CA 인증서에 언급해야 합니다. 인증서를 조달하기 전에 SAN(Subject Alternative Name) 필드를 채워 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(* .domain.company.com)의 경우 인증서에 도메인의 모든 호스트 이름이 암시적으로 포함됩니다.

CA 인증서를 가져옵니다

MMC(Microsoft Management Console)를 사용하여 CA 인증서를 SnapCenter 서버 및 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 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 단추로 클릭한 다음 * 모든 작업 * > * 가져오기 * 를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료합니다.

이 마법사 창에서...	다음을 수행합니다.
개인 키를 가져옵니다	예 * 옵션을 선택하고 개인 키를 가져온 다음 * 다음 * 을 클릭합니다.
파일 형식 가져오기	변경하지 않고 * 다음 * 을 클릭합니다.
보안	내보낸 인증서에 사용할 새 암호를 지정하고 * 다음 * 을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

인증서 가져오기는 개인 키와 함께 번들로 제공됩니다(지원되는 형식은 *.pfx, *.p12 및 *.p7b 입니다).

7. "개인" 폴더에 대해 5단계를 반복합니다.

CA 인증서 지문을 받습니다

인증서 thumbprint는 인증서를 식별하는 16진수 문자열입니다. 썸프린트는 썸프린트 알고리즘을 사용하여 인증서 컨텐츠에서 계산됩니다.

단계

1. GUI에서 다음을 수행합니다.
   a. 인증서를 두 번 클릭합니다.
   b. 인증서 대화 상자에서 * 세부 정보 * 탭을 클릭합니다.
   c. 필드 목록을 스크롤하여 * Thumbprint * 를 클릭합니다.
   d. 상자에서 16진수 문자를 복사합니다.
   e. 16진수 사이의 공백을 제거합니다.

      예를 들어, 썸프린트가 "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 0d 42 77 A3 2a 7b"인 경우 공백을 제거한 후 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.
   a. 다음 명령을 실행하여 설치된 인증서의 엄지손가락 지문을 나열하고 최근 설치된 인증서를 주체 이름으로 식별합니다.

      Get-ChildItem-Path 인증:*LocalMachine\My*

   b. 엄지손가락 지문을 복사합니다.

Windows 호스트 플러그인 서비스를 사용하여 **CA** 인증서를 구성합니다

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스를 사용하여 CA 인증서를 구성해야 합니다.

SnapCenter 서버 및 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

단계

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하여 기존 인증서 바인딩을 제거합니다.

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   예를 들면 다음과 같습니다.

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스와 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 들면 다음과 같습니다.

```
> $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** 사용자 지정 플러그인 서비스에 대한 **CA** 인증서를 구성합니다

사용자 지정 플러그인 키 저장소 및 인증서의 암호를 관리하고, CA 인증서를 구성하고, 사용자 지정 플러그인 트러스트 저장소에 대한 루트 또는 중간 인증서를 구성하고, SnapCenter 사용자 지정 플러그인 서비스를 사용하여 사용자 지정 플러그인 트러스트 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

사용자 지정 플러그인은 _/opt/netapp/snapcenter/SCC/etc_에 있는 'keystore.jks' 파일을 신뢰 저장소 및 키 저장소로 사용합니다.

사용자 지정 플러그인 키 저장소 및 사용 중인 **CA** 서명 키 쌍의 별칭에 대한 암호를 관리합니다

단계

1. 사용자 지정 플러그인 에이전트 속성 파일에서 사용자 지정 플러그인 키 저장소 기본 암호를 검색할 수 있습니다.

   'keystore_pass' 키에 해당하는 값입니다.

2. 키 저장소 암호를 변경합니다.

```
 keytool -storepasswd -keystore keystore.jks
. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 암호를 키 저장소에 사용되는 동일한 암호로 변경합니다.
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

   agent.properties 파일의 keystore_pass 키에 대해서도 동일한 업데이트를 하십시오.

3. 암호를 변경한 후 서비스를 다시 시작합니다.

   사용자 지정 플러그인 키 저장소 및 개인 키의 모든 관련 별칭 암호에 대한 암호는 동일해야 합니다.

사용자 지정 플러그인 트러스트 저장소에 루트 또는 중간 인증서를 구성합니다

사용자 지정 플러그인 트러스트 저장소에 대한 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 사용자 지정 플러그인 키 저장소가 포함된 폴더로 이동합니다. /opt/netapp/snapcenter/SCC 등
2. 'keystore.jks' 파일을 찾습니다.
3. 키 저장소에 추가된 인증서를 나열합니다.

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. 루트 또는 중간 인증서 추가:

   ```
    keytool -import -trustcacerts -alias myRootCA -file
   /root/USERTrustRSA_Root.cer -keystore keystore.jks
   ```

   . 루트 또는 중간 인증서를 사용자 지정 플러그인 트러스트 저장소에 구성한 후 서비스를 다시 시작합니다.

ⓘ 루트 CA 인증서와 중간 CA 인증서를 추가해야 합니다.

사용자 지정 플러그인 트러스트 저장소에 **CA** 서명 키 쌍을 구성합니다

CA 서명 키 쌍을 사용자 지정 플러그인 트러스트 저장소에 구성해야 합니다.

단계

1. 사용자 지정 플러그인 키 저장소/opt/NetApp/snapcenter/SCC 등이 포함된 폴더로 이동합니다
2. 'keystore.jks' 파일을 찾습니다.
3. 키 저장소에 추가된 인증서를 나열합니다.

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. 개인 키와 공개 키를 모두 사용하는 CA 인증서를 추가합니다.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. 키 저장소에 추가된 인증서를 나열합니다.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. keystore에 keystore에 추가된 새 CA 인증서에 해당하는 별칭이 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 암호를 키 저장소 암호로 변경합니다.

   기본 사용자 지정 플러그인 키 저장소 암호는 agent.properties 파일의 keystore_pass 키 값입니다.

```
 keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. CA 인증서의 별칭 이름이 길고 공백 또는 특수 문자("*",",")가 포함된 경우 별칭 이름을
단순 이름으로 변경합니다.
```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. agent.properties 파일의 CA 인증서에서 별칭 이름을 구성합니다.
```

이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

8. CA 서명 키 쌍을 사용자 지정 플러그인 트러스트 저장소에 구성한 후 서비스를 다시 시작합니다.

SnapCenter 사용자 지정 플러그인에 대한 CRL(인증서 해지 목록)을 구성합니다

이 작업에 대해

- SnapCenter 사용자 지정 플러그인은 사전 구성된 디렉터리에서 CRL 파일을 검색합니다.
- SnapCenter 사용자 지정 플러그인에 대한 CRL 파일의 기본 디렉토리는 'opt/netapp/snapcenter/SCC/etc/CRL'입니다.

단계

1. agent.properties 파일의 기본 디렉터리를 수정하여 CRL_path 키에 맞게 업데이트할 수 있습니다.

   이 디렉터리에 둘 이상의 CRL 파일을 배치할 수 있습니다. 들어오는 인증서는 각 CRL에 대해 확인됩니다.

Windows 호스트에서 SnapCenter 사용자 지정 플러그인 서비스에 대한 CA 인증서를 구성합니다

사용자 지정 플러그인 키 저장소 및 인증서의 암호를 관리하고, CA 인증서를 구성하고, 사용자 지정 플러그인 트러스트 저장소에 대한 루트 또는 중간 인증서를 구성하고, SnapCenter 사용자 지정 플러그인 서비스를 사용하여 사용자 지정 플러그인 트러스트 저장소에 CA 서명 키 쌍을 구성하여 설치된 디지털 인증서를 활성화해야 합니다.

사용자 지정 플러그인은 _C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_에 있는 file_keystore.jks_를 신뢰 저장소 및 키 저장소로 사용합니다.

사용자 지정 플러그인 키 저장소 및 사용 중인 CA 서명 키 쌍의 별칭에 대한 암호를 관리합니다

단계

1. 사용자 지정 플러그인 에이전트 속성 파일에서 사용자 지정 플러그인 키 저장소 기본 암호를 검색할 수 있습니다.

   key_keystore_pass_에 해당하는 값입니다.

2. 키 저장소 암호를 변경합니다.

   _keytool - storepasswd - keystore keystore.jks _

Windows 명령 프롬프트에서 "keytool" 명령을 인식할 수 없는 경우 keytool 명령을 전체 경로로 바꿉니다.

_C:\Program Files\Java\<JDK_VERSION>\bin\keytool.exe" - storepasswd -keystore keystore .jks _

3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 암호를 키 저장소에 사용되는 동일한 암호로 변경합니다.

   _keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks _

   agent.properties 파일의 keystore_pass 키에 대해서도 동일한 업데이트를 하십시오.

4. 암호를 변경한 후 서비스를 다시 시작합니다.

사용자 지정 플러그인 키 저장소 및 개인 키의 모든 관련 별칭 암호에 대한 암호는 동일해야 합니다.

사용자 지정 플러그인 트러스트 저장소에 루트 또는 중간 인증서를 구성합니다

사용자 지정 플러그인 트러스트 저장소에 대한 개인 키 없이 루트 또는 중간 인증서를 구성해야 합니다.

단계

1. 사용자 지정 플러그인 keystore_C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_가 포함된 폴더로 이동합니다
2. 'keystore.jks' 파일을 찾습니다.
3. 키 저장소에 추가된 인증서를 나열합니다.

   keytool -list -v -keystore keystore.jks

4. 루트 또는 중간 인증서 추가:

   _keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks _

5. 루트 또는 중간 인증서를 사용자 지정 플러그인 트러스트 저장소에 구성한 후 서비스를 다시 시작합니다.

루트 CA 인증서와 중간 CA 인증서를 추가해야 합니다.

사용자 지정 플러그인 트러스트 저장소에 **CA** 서명 키 쌍을 구성합니다

CA 서명 키 쌍을 사용자 지정 플러그인 트러스트 저장소에 구성해야 합니다.

단계

1. 사용자 지정 플러그인 keystore_C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_가 포함된 폴더로 이동합니다
2. *keystore.jks* 파일을 찾습니다.
3. 키 저장소에 추가된 인증서를 나열합니다.

   keytool -list -v -keystore keystore.jks

4. 개인 키와 공개 키를 모두 사용하는 CA 인증서를 추가합니다.

_keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype jks _

5. 키 저장소에 추가된 인증서를 나열합니다.

   keytool -list -v -keystore keystore.jks

6. keystore에 keystore에 추가된 새 CA 인증서에 해당하는 별칭이 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 암호를 키 저장소 암호로 변경합니다.

   기본 사용자 지정 플러그인 키 저장소 암호는 agent.properties 파일의 keystore_pass 키 값입니다.

   _keytool -keykeyasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks _

8. *agent.properties* 파일의 CA 인증서에서 별칭 이름을 구성합니다.

   이 값을 SCC_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.

9. CA 서명 키 쌍을 사용자 지정 플러그인 트러스트 저장소에 구성한 후 서비스를 다시 시작합니다.

SnapCenter 사용자 지정 플러그인에 대한 **CRL(**인증서 해지 목록**)**을 구성합니다

이 작업에 대해

- 관련 CA 인증서에 대한 최신 CRL 파일을 다운로드하려면 를 참조하십시오 "SnapCenter CA 인증서에서 인증서 해지 목록 파일을 업데이트하는 방법".
- SnapCenter 사용자 지정 플러그인은 사전 구성된 디렉터리에서 CRL 파일을 검색합니다.
- SnapCenter 사용자 지정 플러그인에 대한 CRL 파일의 기본 디렉토리는 _'C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\CRL'_입니다.

단계

1. *agent.properties* 파일의 기본 디렉터리를 수정하여 CRL_path 키에 맞게 업데이트할 수 있습니다.
2. 이 디렉터리에 둘 이상의 CRL 파일을 배치할 수 있습니다.

   들어오는 인증서는 각 CRL에 대해 확인됩니다.

플러그인에 대해 **CA** 인증서를 활성화합니다

CA 인증서를 구성하고 SnapCenter 서버 및 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- run_Set-SmCertificateSettings_cmdlet을 사용하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- _get-SmCertificateSettings_를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 호스트 페이지에서 * 관리되는 호스트 * 를 클릭합니다.
3. 단일 또는 여러 플러그인 호스트를 선택합니다.
4. 추가 옵션 * 을 클릭합니다.
5. 인증서 유효성 검사 사용 * 을 선택합니다.

작업을 마친 후

관리 호스트 탭 호스트에는 자물쇠가 표시되고 자물쇠 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- 는 CA 인증서가 활성화되지 않았으며 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- CA 인증서의 유효성을 확인했음을 나타냅니다.
- CA 인증서의 유효성을 확인할 수 없음을 나타냅니다.
- 연결 정보를 검색할 수 없음을 나타냅니다.

상태가 노란색 또는 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

데이터 보호를 준비합니다

SnapCenter 사용자 지정 플러그인 사용을 위한 사전 요구 사항

SnapCenter 사용자 지정 플러그인을 사용하려면 먼저 SnapCenter 관리자가 SnapCenter 서버를 설치 및 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다.
- SnapCenter 서버에 로그인합니다.
- 스토리지 시스템 접속을 추가하고 해당하는 경우 자격 증명을 생성하여 SnapCenter 환경을 구성합니다.
- 호스트를 추가하고 플러그인을 설치 및 업로드합니다.
- 해당하는 경우 플러그인 호스트에 Java 1.7 또는 Java 1.8을 설치합니다.
- 여러 데이터 경로(LIF) 또는 dNFS 구성이 있는 경우 데이터베이스 호스트에서 SnapCenter CLI를 사용하여 다음을 수행할 수 있습니다.
  - 기본적으로 데이터베이스 호스트의 모든 IP 주소가 클론 복제된 볼륨에 대한 SVM(Storage Virtual Machine)의 NFS 스토리지 엑스포트 정책에 추가됩니다. 특정 IP 주소를 사용하거나 IP 주소의 하위 집합으로 제한하려면 Set-PreferredHostIPsInStorageExportPolicy CLI를 실행합니다.
  - SVM에 여러 데이터 경로(LIF)가 있을 경우 SnapCenter은 NFS 클론 복제된 볼륨을 마운트하기 위해 적절한 데이터 경로(LIF)를 선택합니다. 그러나 특정 데이터 경로(LIF)를 지정하려면 Set-SvmPreferredDataPath CLI를 실행해야 합니다.
    명령에 사용할 수 있는 매개 변수와 해당 설명에 대한 정보는 _get-Help command_name_을 실행하여 얻을 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 명령 참조 가이드".
- 백업 복제를 원하는 경우 SnapMirror 및 SnapVault를 설정합니다.
- 호스트의 다른 애플리케이션에서 포트 9090을 사용하지 않는지 확인합니다.

포트 9090은 SnapCenter에 필요한 다른 포트 외에도 SnapCenter 사용자 지정 플러그인에서 사용하도록 예약되어야 합니다.

리소스, 리소스 그룹 및 정책을 사용하여 맞춤형 플러그인 리소스를 보호하는 방법

SnapCenter를 사용하기 전에 수행할 백업, 클론 및 복원 작업과 관련된 기본 개념을 이해하는 것이 좋습니다. 서로 다른 작업을 위해 리소스, 리소스 그룹 및 정책과 상호 작용합니다.

- 리소스는 일반적으로 SnapCenter를 사용하여 백업 또는 클론 복제하는 데이터베이스, Windows 파일 시스템 또는 VM입니다.
- SnapCenter 리소스 그룹은 호스트 또는 클러스터의 리소스 모음입니다.

  자원 그룹에 대해 작업을 수행할 때 자원 그룹에 지정한 일정에 따라 자원 그룹에 정의된 자원에 대해 해당 작업을 수행합니다.

  필요에 따라 단일 리소스 또는 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 수행할 수도 있습니다.

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

  자원 그룹을 만들 때 해당 그룹에 대해 하나 이상의 정책을 선택합니다. 단일 리소스에 대해 필요 시 백업을 수행할 때 정책을 선택할 수도 있습니다.

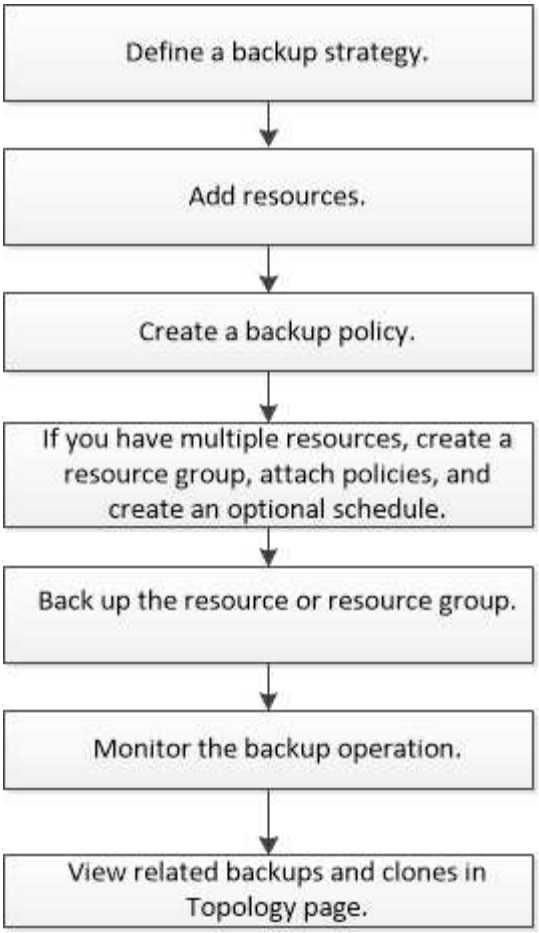
보호하려는_대상_과 이를 보호할 시기를 요일과 시간으로 정의하는 자원 그룹을 생각해 보십시오. 정책을 정의하는 _ 방법 _ 을(를) 보호하려는 것으로 생각해 보십시오. 예를 들어 모든 데이터베이스를 백업하거나 호스트의 모든 파일 시스템을 백업하는 경우 모든 데이터베이스나 호스트의 모든 파일 시스템을 포함하는 리소스 그룹을 생성할 수 있습니다. 그런 다음 리소스 그룹에 일별 정책과 시간별 정책이라는 두 가지 정책을 연결할 수 있습니다. 리소스 그룹을 생성하고 정책을 연결할 때 매일 파일 기반 백업을 수행하고 시간 단위로 스냅샷 기반 백업을 수행하는 다른 일정을 수행하도록 리소스 그룹을 구성할 수 있습니다.

사용자 지정 플러그인 리소스를 백업합니다

사용자 지정 플러그인 리소스를 백업합니다

백업 워크플로우에는 계획, 백업용 리소스 식별, 백업 정책 관리, 리소스 그룹 생성 및 정책 연결, 백업 생성 및 작업 모니터링이 포함됩니다.

다음 워크플로에서는 백업 작업을 수행해야 하는 순서를 보여 줍니다.



PowerShell cmdlet을 수동으로 사용하거나 스크립트에서 사용하여 백업, 복원 및 클론 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드"

SnapCenter 사용자 지정 플러그인에 리소스를 추가합니다

백업하거나 클론 복제할 리소스를 추가해야 합니다. 환경에 따라 백업 또는 복제할 데이터베이스 인스턴스 또는 컬렉션이 리소스가 될 수 있습니다.

시작하기 전에

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 접속 생성, 자격 증명 추가 등의 작업을 완료해야 합니다.
- 이(가) 있어야 합니다 "응용 프로그램에 대한 사용자 지정 플러그인을 만들었습니다".
- SnapCenter 서버에 플러그인을 업로드해야 합니다.

이 작업에 대해

MySQL 및 DB2 애플리케이션에 대한 리소스를 추가할 수도 있습니다. 이러한 플러그인은 에서 다운로드할 수 있습니다 "NetApp 스토리지 자동화 스토어".

단계

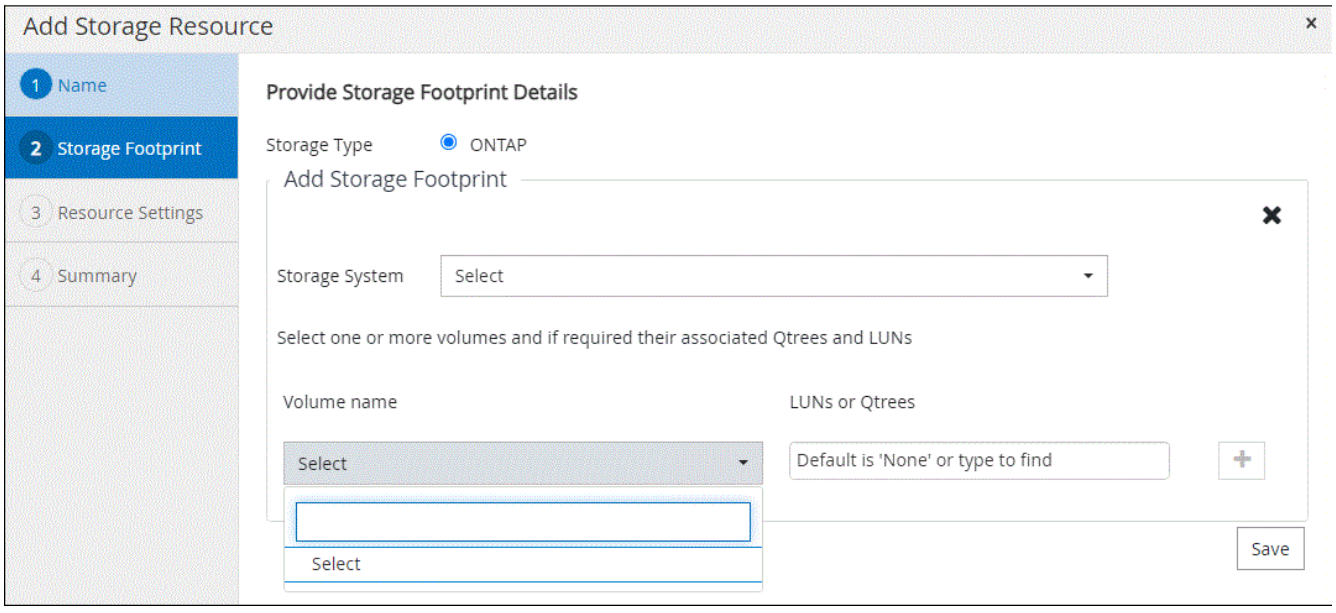
1. 왼쪽 탐색 창에서 * 리소스 * 를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 * 리소스 추가 * 를 선택합니다.
3. 리소스 세부 정보 제공 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
이름	리소스의 이름을 입력합니다.
호스트 이름입니다	호스트를 선택합니다.
유형	유형을 선택합니다. 유형은 플러그인 설명 파일에 따라 사용자가 정의합니다. 예를 들어, 데이터베이스와 인스턴스 등이 있습니다. 선택한 유형에 부모가 있는 경우 상위 항목의 세부 정보를 입력합니다. 예를 들어, 형식이 Database 이고 모체가 instance인 경우 인스턴스의 세부 정보를 입력합니다.
자격 증명 이름입니다	자격 증명을 선택하거나 새 자격 증명을 생성합니다.
마운트 경로	리소스가 마운트된 마운트 경로를 입력합니다. 이는 Windows 호스트에만 적용됩니다.

4. 스토리지 설치 공간 제공 페이지에서 스토리지 시스템을 선택하고 하나 이상의 볼륨, LUN 및 qtree를 선택한 다음 * 저장 * 을 선택합니다.

   선택 사항: 을 선택합니다  아이콘을 클릭하여 다른 스토리지 시스템에서 볼륨, LUN 및 qtree를 더 추가합니다.

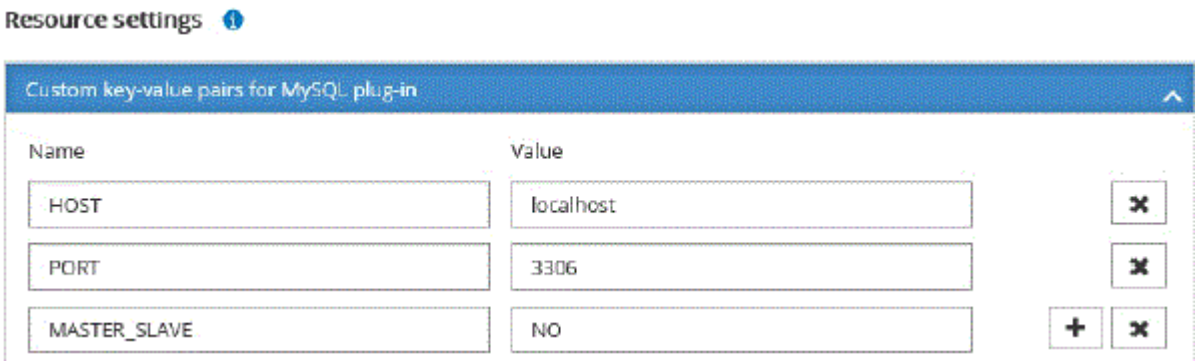
   SnapCenter 사용자 지정 플러그인은 리소스의 자동 검색을 지원하지 않습니다. 물리적 환경과 가상 환경의 스토리지 세부 정보도 자동으로 검색되지 않습니다. 리소스를 생성하는 동안 물리적 환경과 가상 환경에 대한 스토리지 정보를 제공해야 합니다.



5. 리소스 설정 페이지에서 리소스에 대한 사용자 지정 키 값 쌍을 제공합니다.

자원별 정보를 전달하려면 사용자 지정 키 값 쌍을 사용합니다. 예를 들어, MySQL 플러그인을 사용하는 경우 호스트를 host=hostname, port=port-no 로 지정하여 MySQL 및 master-slave 구성에서 master_slave=""Yes"" 또는 ""no"(name은 master_slave, value는 ""Yes"" 또는 ""No")로 지정해야 합니다.

HOST 및 PORT가 대문자로 되어 있는지 확인합니다.



6. 요약을 검토한 후 * Finish * 를 선택합니다.

결과

리소스는 유형, 호스트 또는 클러스터 이름, 관련 리소스 그룹 및 정책, 전체 상태와 같은 정보와 함께 표시됩니다.

데이터베이스가 SnapCenter 외부에서 이름이 변경된 경우 리소스를 새로 고쳐야 합니다.

작업을 마친 후

다른 사용자에게 자산에 대한 액세스 권한을 제공하려면 SnapCenter 관리자가 해당 사용자에게 자산을 할당해야 합니다. 따라서 사용자는 자신에게 할당된 자산에 대한 사용 권한이 있는 작업을 수행할 수 있습니다.

리소스를 추가한 후 리소스 세부 정보를 수정할 수 있습니다. 사용자 지정 플러그인 리소스에 연결된 백업이 있는 경우 리소스 이름, 리소스 유형 및 호스트 이름 등의 필드를 수정할 수 없습니다.

사용자 지정 플러그인 리소스에 대한 정책을 생성합니다

SnapCenter를 사용하여 사용자 지정 플러그인 특정 리소스를 백업하기 전에 백업할 리소스 또는 리소스 그룹에 대한 백업 정책을 만들어야 합니다.

시작하기 전에

- 백업 전략을 정의해야 합니다.

  자세한 내용은 사용자 지정 플러그인의 데이터 보호 전략 정의에 대한 정보를 참조하십시오.

- 데이터 보호를 위한 준비가 되어 있어야 합니다.

  데이터 보호 준비에는 SnapCenter 설치, 호스트 추가, 스토리지 시스템 접속 생성, 리소스 추가 등의 작업이 포함됩니다.

- SVM(스토리지 가상 머신)을 미러 또는 소산 작업에 할당해야 합니다.

  스냅샷 복사본을 미러 또는 볼트로 복제할 경우 SnapCenter 관리자가 소스 및 타겟 볼륨에 대한 SVM을 모두 할당해야 합니다.

- 보호할 리소스를 수동으로 추가해야 합니다.

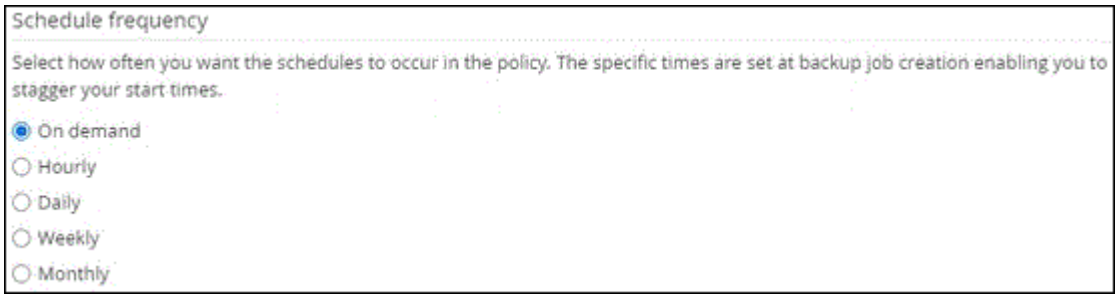
이 작업에 대해

- 백업 정책은 백업을 관리, 예약 및 유지하는 방법을 제어하는 규칙의 집합입니다. 또한 복제, 스크립트 및 애플리케이션 설정을 지정할 수 있습니다.
- 정책에 옵션을 지정하면 다른 리소스 그룹에 대한 정책을 다시 사용할 때 시간이 절약됩니다.

단계

1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
2. 설정 페이지에서 * 정책 * 을 클릭합니다.
3. 새로 만들기 * 를 클릭합니다.
4. 이름 페이지에 정책 이름과 설명을 입력합니다.
5. 설정 페이지에서 다음 단계를 수행하십시오.
   - On demand *, * Hourly *, * Daily *, * Weekly * 또는 * Monthly * 를 선택하여 일정 유형을 지정합니다.

     리소스 그룹을 생성하는 동안 백업 작업의 스케줄(시작 날짜, 종료 날짜 및 빈도)을 지정할 수 있습니다. 따라서 동일한 정책 및 백업 빈도를 공유하는 리소스 그룹을 생성할 수 있지만, 각 정책에 서로 다른 백업 스케줄을 할당할 수 있습니다.

     오전 2시에 예약된 경우 DST(일광 절약 시간) 중에는 일정이 트리거되지 않습니다.

   - 사용자 지정 백업 설정 섹션에서 플러그인으로 전달되어야 하는 특정 백업 설정을 키 값 형식으로 제공합니다. 플러그인으로 전달할 여러 키 값을 제공할 수 있습니다.
6. Retention * 페이지에서 * Backup Type * 페이지에서 선택한 백업 유형 및 스케줄 유형에 대한 보존 설정을 지정합니다.

원하는 작업	그러면...
일정 수의 스냅샷 복사본을 유지합니다	유지할 총 스냅샷 복사본 * 을 선택하고 유지할 스냅샷 복사본 수를 지정합니다. 스냅샷 복사본 수가 지정된 수를 초과하면 가장 오래된 복사본이 먼저 삭제된 후 스냅샷 복사본이 삭제됩니다. SnapVault 복제를 설정하려면 보존 수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷 복사본이 타겟으로 복제될 때까지 첫 번째 스냅샷 복사본이 SnapVault 관계의 참조 스냅샷 복사본이므로 보존 작업이 실패할 수 있습니다. 최대 보존 값은 ONTAP 9.4 이상의 리소스에 대해 1018이고, ONTAP 9.3 이전 버전의 리소스에 대해서는 254입니다. 보존이 기본 ONTAP 버전에서 지원하는 값보다 높은 값으로 설정된 경우 백업이 실패합니다.
Snapshot 복사본을 일정 일 동안 유지합니다	스냅샷 복사본 보관 * 을 선택한 다음, 스냅샷 복사본을 삭제하기 전에 유지할 일 수를 지정합니다.

7. Replication * 페이지에서 복제 설정을 지정합니다.

이 필드의 내용...	수행할 작업...
• 로컬 스냅샷 복사본을 생성한 후 SnapMirror 업데이트 * 를 참조하십시오	다른 볼륨에 백업 세트의 미러 복사본을 생성하려면 이 필드를 선택합니다(SnapMirror 복제). ONTAP의 보호 관계가 미러와 볼트 유형이고 이 옵션만 선택한 경우, 기본 에 생성된 스냅샷 복사본이 대상으로 전송되지 않고 대상에 나열됩니다. 복원 작업을 수행하기 위해 대상에서 이 스냅샷 복사본을 선택한 경우 다음 오류 메시지가 표시됩니다. 보조 위치는 선택한 볼트된 /미러링된 백업에 사용할 수 없습니다.
• 로컬 스냅샷 복사본을 생성한 후 SnapVault 업데이트 * 를 클릭합니다	디스크 간 백업 복제(SnapVault 백업)를 수행하려면 이 옵션을 선택합니다.

이 필드의 내용...	수행할 작업...
• 보조 정책 레이블 *	스냅샷 레이블을 선택합니다. 선택한 스냅샷 복사본 레이블에 따라 ONTAP에서는 해당 레이블과 일치하는 2차 스냅샷 복사본 보존 정책을 적용합니다. 로컬 스냅샷 복사본 * 을 생성한 후 SnapMirror 업데이트 * 를 선택한 경우, 선택적으로 보조 정책 레이블을 지정할 수 있습니다. 그러나 로컬 스냅샷 복사본 * 을 생성한 후 * SnapVault 업데이트 * 를 선택한 경우에는 보조 정책 레이블을 지정해야 합니다.
• 오류 재시도 횟수 *	작업이 중지되기 전에 허용되는 최대 복제 시도 횟수를 입력합니다.

보조 스토리지에 대한 ONTAP의 SnapMirror 보존 정책을 구성하면 보조 스토리지에서 스냅샷 복사본의 최대 제한에 도달하지 않도록 해야 합니다.

8. 요약을 검토하고 * Finish * 를 클릭합니다.

SnapCenter에서 리소스 그룹을 생성하고 정책을 연결합니다

리소스 그룹은 백업 및 보호할 리소스를 추가해야 하는 컨테이너입니다. 이 기능을 사용하면 특정 애플리케이션과 연결된 모든 데이터를 동시에 백업할 수 있습니다. 또한 수행할 데이터 보호 작업의 유형을 정의하려면 하나 이상의 정책을 리소스 그룹에 연결해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 자원 페이지에서 새 자원 그룹을 선택합니다.
3. 이름 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
이름	자원 그룹의 이름을 입력합니다. 참고: 리소스 그룹 이름은 250자를 초과할 수 없습니다.
태그	나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력합니다. 예를 들어 HR을 여러 자원 그룹에 태그로 추가하면 나중에 HR 태그와 연결된 모든 자원 그룹을 찾을 수 있습니다.

이 필드의 내용…	수행할 작업…
스냅샷 복사본에 대해 사용자 지정 이름 형식을 사용합니다	이 확인란을 선택하고 스냅샷 복사본 이름에 사용할 사용자 지정 이름 형식을 입력합니다. 예를 들어, _customtext_resource group_policy_hostname 또는 resource group_hostname_과 같이 입력합니다. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.

4. 선택 사항: 리소스 페이지의 * 호스트 * 드롭다운 목록에서 호스트 이름을 선택하고 * 리소스 유형 * 드롭다운 목록에서 리소스 유형을 선택합니다.

   그러면 화면의 정보를 필터링하는 데 도움이 됩니다.

5. 사용 가능한 리소스 * 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 선택하여 * 선택한 리소스 * 섹션으로 이동합니다.
6. 선택 사항: * 응용 프로그램 설정 * 페이지에서 다음을 수행합니다.

   a. 백업 화살표를 선택하여 추가 백업 옵션을 설정합니다.

      정합성 보장 그룹 백업을 설정하고 다음 작업을 수행합니다.

이 필드의 내용…	수행할 작업…
정합성 보장 그룹 스냅샷 작업이 완료될 때까지 기다릴 여유가 없습니다	긴급, 중간 또는 완해제 를 선택하여 스냅샷 복사 작업이 완료될 때까지 기다리는 시간을 지정합니다. 긴급 = 5초, 중간 = 7초, 휴식 = 20초
WAFL 동기화를 비활성화합니다	WAFL 정합성 보장 지점을 강제로 사용하지 않으려면 이 옵션을 선택합니다.

+

a. 스크립트 화살표를 선택하고 일시 중지, 스냅샷 복사 및 일시 중지 해제 작업에 대한 사전 및 사후 명령을 입력합니다. 장애 발생 시 종료하기 전에 실행할 사전 명령을 입력할 수도 있습니다.

b. 사용자 지정 구성 화살표를 선택하고 이 리소스를 사용하는 모든 데이터 보호 작업에 필요한 사용자 지정 키 값 쌍을 입력합니다.

매개 변수	설정	설명
archive_log_enable입니다	(예/아니요)	아카이브 로그 관리를 활성화하여 아카이브 로그를 삭제합니다.
archive_log_retention 을 선택합니다	일 수	에서 일 수를 지정합니다 아카이브 로그가 보존됩니다. 이 설정입니다 보다 크거나 같아야 합니다 NTAP_스냅샷 _ 보존.
archive_log_DIR입니다	change_info_directory/logs	디렉토리의 경로를 지정합니다 아카이브 로그를 포함합니다.

매개 변수	설정	설명
archive_log_EXT	file_extension을 선택합니다	아카이브 로그 파일을 지정합니다 연장 길이. 예를 들어, 가 인 경우 보관 로그는 입니다 log_backup_0_0_0_0.16151855 1942 9 및 file_extension 값이 5인 경우 그러면 로그 확장이 이루어집니다 16151인 5자리 숫자를 유지합니다.
archive_log_recursive_se 를 선택합니다 아키텍처	(예/아니요)	아카이브 관리를 활성화합니다 하위 디렉터리 내의 로그 여러분 가 있는 경우 이 매개변수를 사용해야 합니다 아카이브 로그는 에 있습니다 하위 디렉터리.

c. 스냅샷 복사본을 생성할 툴을 선택하려면 * 스냅샷 복사본 툴 * 화살표를 선택하십시오.

원하는 작업	그러면...
SnapCenter - Windows용 플러그인을 사용하고 스냅샷 복사본을 생성하기 전에 파일 시스템을 일관된 상태로 둡니다. Linux 리소스의 경우 이 옵션을 적용할 수 없습니다.	SnapCenter with File System Consistency를 선택합니다. 이 옵션은 SAP HANA 데이터베이스용 SnapCenter 플러그인에는 적용되지 않습니다.
SnapCenter를 사용하여 스토리지 레벨의 스냅샷 복사본을 생성합니다	파일 시스템 정합성 보장 없이 SnapCenter를 선택합니다.
호스트에서 실행할 명령을 입력하여 스냅샷 복사본을 생성합니다.	기타를 선택한 다음 호스트에서 실행할 명령을 입력하여 스냅샷 복사본을 생성합니다.

7. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

* 를 선택하여 정책을 생성할 수도 있습니다 + *.

정책은 * 선택한 정책에 대한 일정 구성 * 섹션에 나열됩니다.

b. Configure Schedules * 열에서 * 를 선택합니다 + 구성할 정책에 대해 * 를 선택합니다.

c. policy_policy_name_name에 대한 스케줄 추가 대화 상자에서 스케줄을 구성하고 확인 을 선택합니다.

여기서 policy_name은 선택한 정책의 이름입니다.

구성된 일정이 Applied Schedules 열에 나열됩니다.
타사 백업 스케줄은 SnapCenter 백업 스케줄과 겹치는 경우 지원되지 않습니다.

8. 알림 * 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. SMTP 서버는 * 설정 * > * 글로벌 설정 * 에서 구성해야 합니다.

9. 요약을 검토한 후 * Finish * 를 선택합니다.

개별 맞춤형 플러그인 리소스를 백업합니다

개별 사용자 지정 플러그인 리소스가 리소스 그룹에 포함되어 있지 않은 경우 리소스 페이지에서 리소스를 백업할 수 있습니다. 필요에 따라 리소스를 백업하거나 리소스에 정책이 연결되어 있고 스케줄이 구성된 경우 스케줄에 따라 백업이 자동으로 수행됩니다.

시작하기 전에

- 백업 정책을 만들어야 합니다.
- 보조 스토리지와 SnapMirror 관계가 있는 리소스를 백업하려면 스토리지 사용자에게 할당된 ONTAP 역할에 "'스냅샷 전체' 권한이 있어야 합니다. 그러나 "vsadmin" 역할을 사용하는 경우에는 "napmirror all" 권한이 필요하지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 유형에 따라 리소스를 필터링합니다.

을 클릭합니다 호스트 이름과 리소스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 을 클릭할 수 있습니다 를 눌러 필터 창을 닫습니다.

3. 백업할 리소스를 클릭합니다.
4. 리소스 페이지에서 사용자 지정 이름을 사용하려면 * 스냅샷 복사본에 사용자 지정 이름 형식 사용 * 확인란을 선택한 다음 스냅샷 복사본 이름의 사용자 지정 이름 형식을 입력합니다.

예: *customtext_policy_hostname_or_resource_hostname*. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.

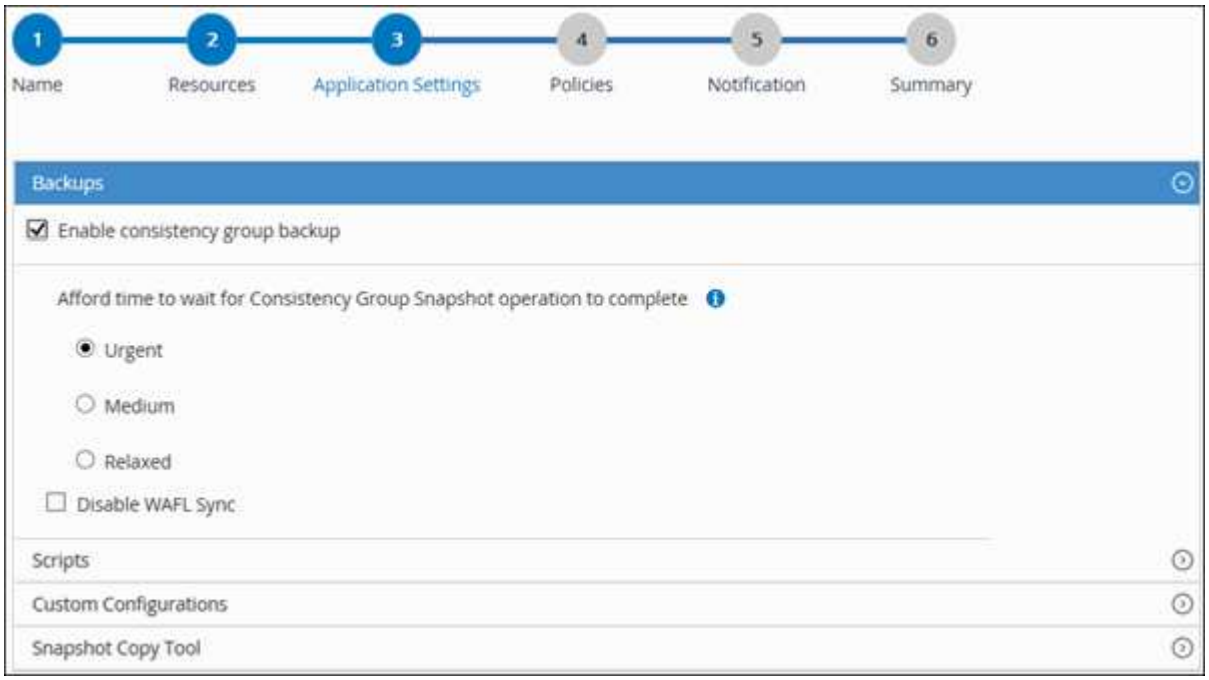
5. 응용 프로그램 설정 페이지에서 다음을 실행합니다.

a. 백업 * 화살표를 클릭하여 추가 백업 옵션을 설정합니다.

필요한 경우 정합성 보장 그룹 백업을 설정하고 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
정합성 보장 그룹 스냅샷 작업이 완료될 때까지 기다릴 여유가 없습니다	긴급, 중간 또는 완해제 를 선택하여 스냅샷 복사 작업이 완료될 때까지 기다리는 시간을 지정합니다. 긴급 = 5초, 중간 = 7초, 휴식 = 20초
WAFL 동기화를 비활성화합니다	WAFL 정합성 보장 지점을 강제로 사용하지 않으려면 이 옵션을 선택합니다.

+



a. Quiesce, Snapshot copy 및 unquiesce 작업에 대한 사전 및 사후 명령을 실행하려면 * Scripts * 화살표를 클릭합니다. 백업 작업을 종료하기 전에 사전 명령을 실행할 수도 있습니다.

   사전 스크립트 및 사후 스크립트는 SnapCenter 서버에서 실행됩니다.

b. 사용자 정의 구성* 화살표를 클릭한 다음 이 자원을 사용하는 모든 작업에 필요한 사용자 정의 값 쌍을 입력합니다.

c. 스냅샷 복사본 툴 * 화살표를 클릭하여 스냅샷 복사본을 생성할 툴을 선택합니다.

원하는 작업	그러면...
SnapCenter를 사용하여 스토리지 레벨의 스냅샷 복사본을 생성할 수 있습니다	파일 시스템 일관성 없이 SnapCenter * 를 선택합니다.
SnapCenter은 Windows용 플러그인을 사용하여 파일 시스템을 일관된 상태로 전환한 다음 스냅샷 복사본을 만듭니다	파일 시스템 정합성 보장 * 이 있는 SnapCenter를 선택합니다.

원하는 작업	그러면...
명령을 입력하여 스냅샷 복사본을 생성합니다	기타 * 를 선택한 다음 명령을 입력하여 스냅샷 복사본을 생성합니다.

6. 정책 페이지에서 다음 단계를 수행합니다.
   a. 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

      을 클릭하여 정책을 생성할 수도 있습니다 + .

      선택한 정책에 대한 스케줄 구성 섹션에 선택한 정책이 나열됩니다.

   b. + 을 클릭합니다 스케줄을 구성할 정책에 대한 Configure Schedules 열에서
   c. policy_policy_name_에 대한 일정 추가 대화 상자에서 일정을 구성한 다음 * 확인 * 을 클릭합니다.

      여기서, _policy_name_은 선택한 정책의 이름입니다.

   구성된 일정이 Applied Schedules 열에 나열됩니다.
7. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. SMTP는 * 설정 * > * 글로벌 설정 * 에서도 구성해야 합니다.
8. 요약을 검토하고 * Finish * 를 클릭합니다.

   리소스 토폴로지 페이지가 표시됩니다.
9. 지금 백업 * 을 클릭합니다.
10. 백업 페이지에서 다음 단계를 수행하십시오.
    a. 리소스에 여러 정책을 적용한 경우 * 정책 * 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

       필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

    b. 백업 * 을 클릭합니다.
11. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

사용자 지정 플러그인 리소스의 리소스 그룹을 백업합니다

리소스 페이지에서 필요 시 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 연결되어 있고 스케줄이 구성되어 있는 경우 스케줄에 따라 백업이 자동으로 수행됩니다.

시작하기 전에

- 정책이 연결된 리소스 그룹을 만들어야 합니다.

- 보조 스토리지와 SnapMirror 관계가 있는 리소스를 백업하려면 스토리지 사용자에게 할당된 ONTAP 역할에 "'스냅샷 전체' 권한이 있어야 합니다. 그러나 "vsadmin" 역할을 사용하는 경우에는 "napmirror all" 권한이 필요하지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 리소스 그룹 * 을 선택합니다.

   검색 상자에 리소스 그룹 이름을 입력하거나 을 클릭하여 리소스 그룹을 검색할 수 있습니다 태그를 선택합니다. 그런 다음 을 클릭할 수 있습니다 를 눌러 필터 창을 닫습니다.
3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음 * 지금 백업 * 을 클릭합니다.
4. 백업 페이지에서 다음 단계를 수행하십시오.
   a. 여러 정책을 리소스 그룹에 연결한 경우 * Policy * 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

      필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

   b. 백업 * 을 클릭합니다.
5. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.
   - MetroCluster 구성에서 SnapCenter는 페일오버 후 보호 관계를 감지하지 못할 수 있습니다.

     "MetroCluster 페일오버 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다"
   - VMDK에서 애플리케이션 데이터를 백업하고 VMware vSphere용 SnapCenter 플러그인의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다. Java 힙 크기를 늘리려면 스크립트 파일 /opt/netapp/init_scripts/scvservice를 찾습니다. 이 스크립트에서 은 입니다 `do_start method` Command SnapCenter VMware 플러그인 서비스를 시작합니다. 다음 명령을 업데이트합니다. `Java -jar -Xmx8192M -Xms4096M`.

PowerShell cmdlet을 사용하여 스토리지 시스템 연결과 자격 증명을 생성합니다

PowerShell cmdlet을 사용하여 데이터 보호 작업을 수행하기 전에 SVM(Storage Virtual Machine) 연결과 자격 증명을 생성해야 합니다.

시작하기 전에

- PowerShell cmdlet을 실행할 수 있도록 PowerShell 환경을 준비해야 합니다.
- 스토리지 접속을 생성하려면 인프라스트럭처 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

  호스트 캐시가 업데이트되지 않고 데이터베이스 상태가 SnapCenter GUI에 ""백업을 위해 사용할 수 없음"" 또는 ""NetApp 스토리지에 없음""으로 표시될 수 있으므로 스토리지 시스템 접속을 추가하는 동안 호스트 플러그인 설치가 진행되어서는 안 됩니다.
- 스토리지 시스템 이름은 고유해야 합니다.

  SnapCenter는 서로 다른 클러스터에서 동일한 이름의 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 연결 세션을 시작합니다.

   이 예제에서는 PowerShell 세션을 엽니다.

   ```
   PS C:\> Open-SmConnection
   ```

2. Add-SmStorageConnection cmdlet을 사용하여 스토리지 시스템에 대한 새 접속을 생성합니다.

   이 예에서는 새 스토리지 시스템 접속을 생성합니다.

   ```
   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 FinanceAdmin 이라는 새 자격 증명을 만듭니다.

   ```
   PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
   -Credential sddev\administrator
   ```

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

PowerShell cmdlet을 사용하여 리소스를 백업합니다

리소스 백업에는 SnapCenter 서버와의 연결 설정, 리소스 추가, 정책 추가, 백업 리소스 그룹 생성 및 백업이 포함됩니다.

시작하기 전에

- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 스토리지 시스템 접속을 추가하고 자격 증명을 생성해야 합니다.

이 작업에 대해

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

   ```
   Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146\
   ```

사용자 이름 및 암호 프롬프트가 표시됩니다.

2. Add-SmResources cmdlet을 사용하여 리소스를 추가합니다.

   이 예제에서는 리소스를 추가합니다.

```
Add-SmResource -HostName '10.232.206.248' -PluginCode 'DB2'
-ResourceName NONREC1 -ResourceType Database -StorageFootPrint ( @
{"VolumeName"="DB2_NONREC1DB";"LunName"="DB2_NONREC1DB";"Vserver"="vserv
er_scauto_secondary"}) -Instance db2inst1
```

3. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.

   이 예에서는 새 백업 정책을 생성합니다.

```
Add-SMPolicy -PolicyName 'db2VolumePolicy' -PolicyType 'Backup'
-PluginPolicyType DB2  -description 'VolumePolicy'
```

4. 추가 SmResourceGroup cmdlet을 사용하여 SnapCenter에 새 리소스 그룹을 추가합니다.

   이 예제에서는 지정된 정책 및 리소스를 사용하여 새 리소스 그룹을 만듭니다.

```
Add-SmResourceGroup -ResourceGroupName
'Verify_ManualBackup_DatabaseLevel_MultipleVolume_unix' -Resources @(@
{"Host"="10.232.206.248";"Uid"="db2inst2\NONREC"},@{"Host"="10.232.206.2
48";"Uid"="db2inst1\NONREC"}) -Policies db2ManualPolicy
```

5. New-SmBackup cmdlet을 사용하여 새 백업 작업을 시작합니다.

```
New-SMBackup -DatasetName
Verify_ManualBackup_DatabaseLevel_MultipleVolume_unix -Policy
db2ManualPolicy
```

6. Get-SmBackupReport cmdlet을 사용하여 백업 작업의 상태를 봅니다.

   이 예는 지정된 날짜에 실행된 모든 작업의 작업 요약 보고서를 표시합니다.

```
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 :
```

맞춤형 플러그인 리소스 백업 작업 모니터링

SnapCenterJobs 페이지를 사용하여 여러 백업 작업의 진행률을 모니터링할 수 있습니다. 진행 상황을 확인하여 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

다음 아이콘이 작업 페이지에 나타나고 작업의 해당 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨

단계

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 모니터 페이지에서 * 작업 * 을 클릭합니다.
3. 작업 페이지에서 다음 단계를 수행하십시오.
   a. 을 클릭합니다 백업 작업만 나열되도록 목록을 필터링합니다.
   b. 시작 및 종료 날짜를 지정합니다.
   c. Type * 드롭다운 목록에서 * Backup * 을 선택합니다.
   d. Status * (상태 *) 드롭다운에서 백업 상태를 선택합니다.
   e. 작업이 성공적으로 완료되었는지 보려면 * Apply * 를 클릭합니다.
4. 백업 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.

   백업 작업 상태가 표시됩니다 작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 기호로 표시되어 있는 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 * 로그 보기 * 를 클릭합니다.

   로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

사용자 지정 플러그인에 대한 백업 작업을 취소합니다

대기열에 있는 백업 작업을 취소할 수 있습니다.

- 필요한 것 *
- 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 모니터 * 페이지 또는 * 작업 * 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 작업에 대해 * 작업 취소 * 버튼이 비활성화됩니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 사용자\그룹 페이지에서 다른 구성원 개체를 보고 작동할 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.

시작...	조치
모니터 페이지	a. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 클릭합니다. b. 작업을 선택한 다음 * 작업 취소 * 를 클릭합니다.

시작...	조치
작업 창	a. 백업 작업을 시작한 후 * 를 클릭합니다 * 를 클릭합니다. b. 작업을 선택합니다. c. 작업 세부 정보 페이지에서 * 작업 취소 * 를 클릭합니다.

작업이 취소되고 리소스가 이전 상태로 돌아갑니다.

Topology 페이지에서 사용자 지정 플러그인 리소스 관련 백업 및 클론을 봅니다

리소스를 백업 또는 복제할 때 운영 스토리지와 보조 스토리지의 모든 백업 및 클론을 그래픽으로 표시하는 것이 유용할 수 있습니다. 토폴로지 페이지에서 선택한 리소스 또는 리소스 그룹에 사용할 수 있는 모든 백업 및 클론을 볼 수 있습니다. 이러한 백업 및 클론의 세부 정보를 확인한 다음 이를 선택하여 데이터 보호 작업을 수행할 수 있습니다.

이 작업에 대해

복제본 관리 보기에서 다음 아이콘을 검토하여 운영 스토리지 또는 보조 스토리지(미러 복사본 또는 볼트 복제본)에서 백업과 클론을 사용할 수 있는지 확인할 수 있습니다.

- 기본 스토리지에서 사용할 수 있는 백업 및 클론 수를 표시합니다.
- SnapMirror 기술을 사용하여 보조 스토리지에 미러링된 백업 및 클론 수를 표시합니다.

  미러 볼트 유형 볼륨에 있는 버전에 유연한 미러 백업의 클론은 토폴로지 뷰에 표시되지만 토폴로지 뷰에 있는 미러 백업 카운트에 버전에 따라 유연하게 백업할 수 있는 백업이 포함되지 않습니다.

- SnapVault 기술을 사용하여 보조 스토리지에 복제된 백업 및 클론 수를 표시합니다.

  표시된 백업 수에는 보조 스토리지에서 삭제된 백업이 포함됩니다. 예를 들어 정책을 사용하여 6개의 백업을 생성하여 4개의 백업만 보존한 경우 표시되는 백업 수는 6입니다.

  미러 볼트 유형 볼륨에 있는 버전에 유연한 미러 백업의 클론은 토폴로지 뷰에 표시되지만 토폴로지 뷰에 있는 미러 백업 카운트에 버전에 따라 유연하게 백업할 수 있는 백업이 포함되지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 자원 세부 정보 보기 또는 자원 그룹 세부 정보 보기에서 자원을 선택합니다.

리소스가 보호되는 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. Summary 카드를 검토하여 운영 스토리지와 보조 스토리지에서 사용할 수 있는 백업 및 클론 수를 요약합니다.

   요약 카드 섹션에는 총 백업 및 클론 수가 표시됩니다.

   새로 고침 버튼을 클릭하면 스토리지 쿼리가 시작되어 정확한 카운트가 표시됩니다.

5. 복사본 관리 보기에서 기본 또는 보조 스토리지에서 * 백업 * 또는 * 클론 * 을 클릭하여 백업 또는 클론의 세부 정보를 확인합니다.

   백업 및 클론의 세부 정보가 표 형식으로 표시됩니다.

6. 테이블에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 클론 복제, 이름 바꾸기 및 삭제 작업을 수행합니다.

   ⓘ 보조 스토리지 시스템에 있는 백업의 이름을 바꾸거나 백업을 삭제할 수 없습니다.

   ⓘ 운영 스토리지 시스템에 있는 백업의 이름은 변경할 수 없습니다.

7. 클론을 삭제하려면 표에서 클론을 선택하고 을 클릭합니다 를 눌러 클론을 삭제합니다.

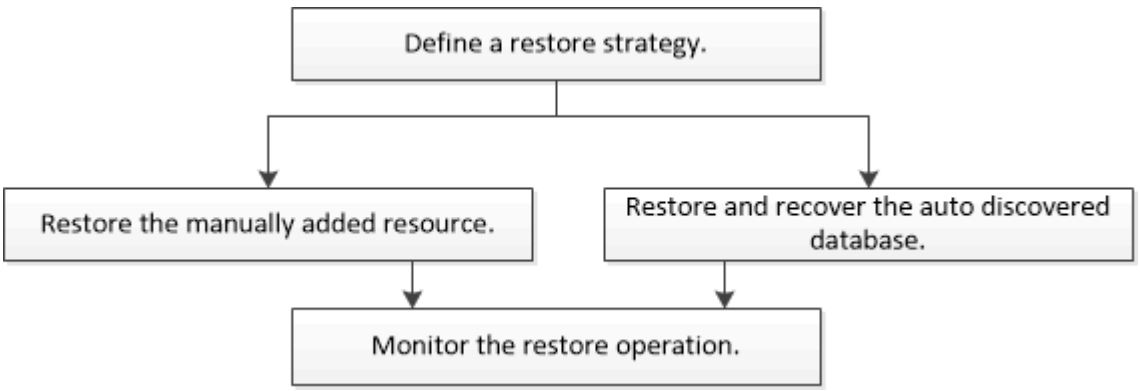
사용자 지정 플러그인 리소스를 복원합니다

사용자 지정 플러그인 리소스를 복원합니다

복원 및 복구 워크플로에는 계획, 복원 작업 수행 및 작업 모니터링이 포함됩니다.

이 작업에 대해

다음 워크플로에서는 복원 작업을 수행해야 하는 순서를 보여 줍니다.



PowerShell cmdlet을 수동으로 사용하거나 스크립트에서 사용하여 백업, 복원 및 클론 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

리소스 백업을 복원합니다

SnapCenter를 사용하여 리소스를 복원할 수 있습니다. 복구 작업의 기능은 사용하는

플러그인에 따라 다릅니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 스냅샷 복사본을 미러 또는 볼트로 복제할 경우 SnapCenter 관리자가 소스 볼륨과 타겟 볼륨 모두에 대해 SVM(스토리지 가상 머신)을 할당해야 합니다.
- 복원할 리소스 또는 리소스 그룹에 대해 현재 진행 중인 백업 작업을 취소해야 합니다.

이 작업에 대해

기본 복구 작업은 스토리지 객체만 복원합니다. 애플리케이션 레벨에서 복구 작업은 사용자 지정 플러그인이 해당 기능을 제공하는 경우에만 수행할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 유형에 따라 리소스를 필터링합니다.

   리소스는 유형, 호스트 또는 클러스터 이름, 관련 리소스 그룹 및 정책, 상태와 같은 정보와 함께 표시됩니다.

   백업이 리소스 그룹에 대한 것일 수도 있지만 복원할 때 복원할 개별 리소스를 선택해야 합니다.

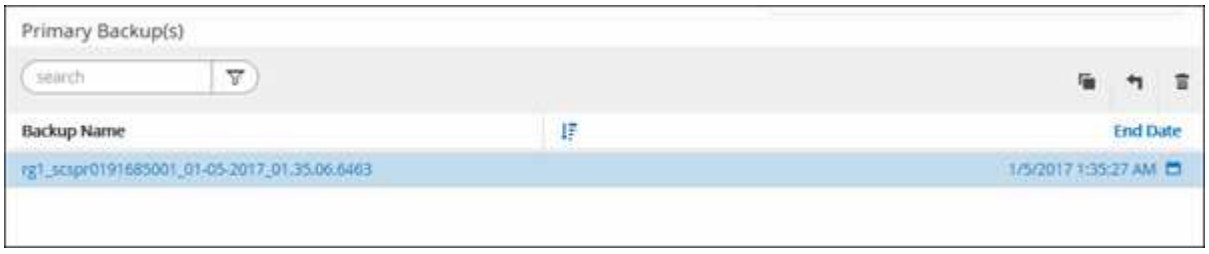
   리소스가 보호되지 않으면 * Overall Status * 열에 _Not protected_가 표시됩니다.

   Overall Status* 열의 status_not protected_는 리소스가 보호되지 않거나 다른 사용자가 리소스를 백업했다는 것을 의미할 수 있습니다.

3. 자원을 선택하거나 자원 그룹을 선택한 다음 해당 그룹에서 자원을 선택합니다.

   리소스 토폴로지 페이지가 표시됩니다.

4. Manage Copies * 뷰에서 기본 또는 보조(미러링 또는 보관된) 스토리지 시스템에서 * Backups * 를 선택합니다.
5. 기본 백업 테이블에서 복원할 백업을 선택한 다음 을 클릭합니다 .



6. 복원 범위 페이지에서 * 전체 리소스 * 또는 * 파일 수준 * 을 선택합니다.
   a. Complete Resource * 를 선택하면 리소스 백업이 복원됩니다.

      리소스에 Storage Footprint로 볼륨 또는 qtree가 포함되어 있는 경우 이러한 볼륨 또는 qtree의 최신 스냅샷 복사본이 삭제되고 복구할 수 없습니다. 또한 동일한 볼륨 또는 qtree에서 다른 리소스가 호스트되는 경우 해당 리소스도 삭제됩니다.

   b. 파일 수준 * 을 선택한 경우 * 모두 * 를 선택하거나 볼륨 또는 qtree를 선택한 다음 선택한 볼륨 또는 qtree와

관련된 경로를 쉼표로 구분하여 입력할 수 있습니다.

- 여러 볼륨 및 qtree를 선택할 수 있습니다.
- 리소스 유형이 LUN이면 전체 LUN이 복구됩니다. 여러 LUN을 선택할 수 있습니다.
  를 누릅니다
  참고: * All * 을 선택하면 볼륨, Qtree 또는 LUN의 모든 파일이 복원됩니다.

7. 복구 유형 * 페이지에서 다음 단계를 수행하십시오. 로그를 적용하려면 옵션을 선택하십시오. 복원 유형을 선택하기 전에 플러그인이 모든 로그 및 로그를 지원하는지 확인하십시오.

원하는 작업	수행할 작업...
모든 로그를 복원합니다	모든 로그 * 를 선택합니다. 플러그인이 * 모든 로그 * 를 지원하는지 확인합니다.
지정된 시간까지 모든 로그를 복원합니다	로그 종료 * 를 선택합니다. 플러그인이 * 까지 * 로그를 지원하는지 확인합니다.
리소스 백업을 복원합니다	없음 * 을 선택합니다.

8. Pre ops * 페이지에서 복구 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 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

    또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. SMTP는 * 설정 * > * 글로벌 설정 * 페이지에서도 구성해야 합니다.

11. 요약을 검토하고 * Finish * 를 클릭합니다.
12. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

PowerShell cmdlet을 사용하여 리소스 복원

리소스 백업 복원에는 SnapCenter 서버와의 연결 세션 시작, 백업 목록 표시 및 백업 정보 검색, 백업 복구가 포함됩니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

    이 예에서는 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 예는 2015년 1월 29일부터 2015년 2월 3일까지 백업에 대한 자세한 정보를 표시합니다.

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"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.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                 : Restore
'scc54.sccore.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 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

맞춤형 플러그인 리소스 복구 작업을 모니터링합니다

작업 페이지를 사용하여 여러 SnapCenter 복원 작업의 진행률을 모니터링할 수 있습니다. 작업 진행률을 확인하여 작업이 언제 완료되는지 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

복원 후 상태는 복원 작업 후 리소스의 상태와 수행할 수 있는 추가 복원 작업에 대해 설명합니다.

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다

- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨

단계

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 모니터 * 페이지에서 * 작업 * 을 클릭합니다.
3. Jobs * 페이지에서 다음 단계를 수행하십시오.
   a. 을 클릭합니다 복원 작업만 나열되도록 목록을 필터링하려면
   b. 시작 및 종료 날짜를 지정합니다.
   c. Type * 드롭다운 목록에서 * Restore * 를 선택합니다.
   d. Status * (상태 *) 드롭다운 목록에서 복원 상태를 선택합니다.
   e. 성공적으로 완료된 작업을 보려면 * 적용 * 을 클릭합니다.
4. 복원 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
5. Job Details * 페이지에서 * View logs * 를 클릭합니다.

   로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

볼륨 기반 복원 작업 후에는 백업 메타데이터가 SnapCenter 저장소에서 삭제되지만 백업 카탈로그 항목은 SAP HANA 카탈로그에 남아 있습니다. 복원 작업 상태가 표시됩니다 작업 세부 정보를 클릭하여 일부 하위 작업의 경고 표시를 확인해야 합니다. 경고 표지를 클릭하고 표시된 백업 카탈로그 항목을 삭제합니다.

사용자 지정 플러그인 리소스 백업의 클론을 생성합니다

사용자 지정 플러그인 리소스 백업의 클론을 생성합니다

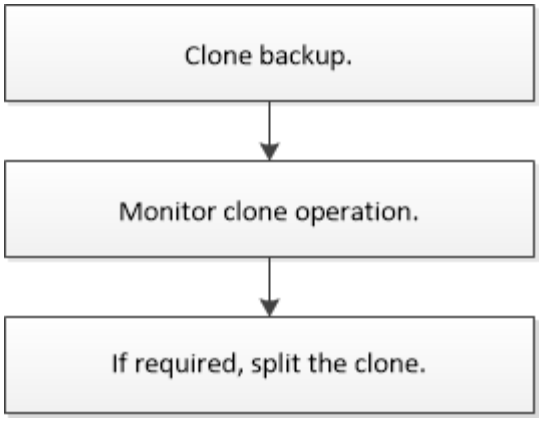
클론 워크플로우에는 클론 작업 수행 및 작업 모니터링이 포함됩니다.

이 작업에 대해

다음과 같은 이유로 리소스 백업을 복제할 수 있습니다.

- 응용 프로그램 개발 주기 동안 현재 리소스 구조 및 콘텐츠를 사용하여 구현해야 하는 기능을 테스트합니다
- 데이터 웨어하우스를 채울 때 데이터 추출 및 조작 도구를 위한 것입니다
- 실수로 삭제 또는 변경된 데이터를 복구합니다

다음 워크플로에서는 클론 작업을 수행해야 하는 순서를 보여 줍니다.



PowerShell cmdlet을 수동으로 사용하거나 스크립트에서 사용하여 백업, 복원 및 클론 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

백업에서 복제합니다

SnapCenter를 사용하여 백업을 복제할 수 있습니다. 기본 또는 보조 백업에서 클론을 생성할 수 있습니다. 클론 작업의 기능은 사용하는 플러그인에 따라 다릅니다.

시작하기 전에

- 리소스 또는 리소스 그룹을 백업해야 합니다.
- 기본 클론 작업에서는 스토리지 오브젝트만 복제합니다. 애플리케이션 레벨에서 클론 작업은 맞춤형 플러그인이 해당 기능을 제공하는 경우에만 수행할 수 있습니다.
- 볼륨을 호스팅하는 애그리게이트는 SVM(스토리지 가상 머신)의 할당된 애그리게이트 목록에 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 * 페이지의 * 보기 * 드롭다운 목록에서 리소스 유형에 따라 리소스를 필터링합니다.

   리소스는 유형, 호스트 또는 클러스터 이름, 관련 리소스 그룹 및 정책, 상태와 같은 정보와 함께 표시됩니다.
3. 자원 또는 자원 그룹을 선택합니다.

   자원 그룹을 선택한 경우 자원을 선택해야 합니다.

   리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.
4. 복사본 관리 보기에서 기본 또는 보조(미러링 또는 보관된) 스토리지 시스템에서 * 백업 * 을 선택합니다.
5. 테이블에서 데이터 백업을 선택한 다음 을 클릭합니다  .
6. 위치 페이지에서 다음을 수행합니다.

이 필드의 내용...	수행할 작업...
클론 서버	기본적으로 소스 호스트는 채워집니다. 다른 호스트를 지정하려면 클론을 마운트해야 하는 호스트를 선택하고 플러그인이 설치된 호스트를 선택합니다.
접미사 복제	클론 대상이 소스와 동일한 경우 이 작업은 필수입니다. 새로 복제된 리소스 이름에 추가할 접미사를 입력합니다. 접미사는 클론된 리소스가 호스트에서 고유하도록 보장합니다. 예: RS1_clone. 원래 리소스와 동일한 호스트에 클론 생성 중인 경우 클론된 리소스를 원래 리소스와 구분할 수 있도록 접미사를 제공해야 합니다. 그렇지 않으면 작업이 실패합니다.

선택한 리소스가 LUN이고 2차 백업에서 클론을 생성하는 경우 타겟 볼륨이 나열됩니다. 단일 소스에 여러 대상 볼륨이 있을 수 있습니다.

7. 설정 * 페이지에서 다음을 수행합니다.

이 필드의 내용...	수행할 작업...
이니시에이터 이름입니다	호스트 이니시에이터 이름, 즉 IQDN 또는 WWPN을 입력합니다.
Igroup 프로토콜	Igroup 프로토콜을 선택합니다.

설정 페이지는 스토리지 유형이 LUN인 경우에만 표시됩니다.

8. 스크립트 페이지에서 클론 작업 전후에 각각 실행해야 하는 사전 클론 또는 사후 클론 명령을 입력합니다. mount 명령을 입력하여 호스트에 파일 시스템을 마운트합니다.

   예를 들면 다음과 같습니다.

   - Pre clone 명령: 이름이 같은 기존 데이터베이스를 삭제합니다
   - 사후 복제 명령: 데이터베이스를 확인하거나 데이터베이스를 시작합니다.

     Linux 시스템의 볼륨 또는 qtree에 대한 마운트 명령: mount <vserver_name>: %<volume_name_Clone/mnt>

9. 알림 * 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다.

10. 요약을 검토하고 * Finish * 를 클릭합니다.

11. 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

PowerShell cmdlet을 사용하여 백업 클론 생성

클론 워크플로우에는 계획, 클론 작업 수행 및 작업 모니터링이 포함됩니다.

시작하기 전에

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Get-SmBackup 또는 Get-SmResourceGroup cmdlet을 사용하여 클론을 생성할 수 있는 백업을 나열합니다.

   이 예에서는 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
```

   다음 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                    : {}
    HostResourceMaping          : {}
    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                    : {}
    HostResourceMaping          : {}
    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 클론 리소스 그룹 또는 기존 백업에서 클론 작업을 시작합니다.

   이 예에서는 모든 로그를 사용하여 지정된 백업에서 클론을 생성합니다.

```
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 클론 작업의 상태를 봅니다.

   이 예에서는 지정된 작업 ID에 대한 클론 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          :
```

사용자 지정 플러그인 리소스 클론 작업을 모니터링합니다

작업 페이지를 사용하여 SnapCenter 클론 작업의 진행률을 모니터링할 수 있습니다. 작업 진행률을 확인하여 작업이 언제 완료되는지 또는 문제가 있는지 확인할 수 있습니다.

이 작업에 대해

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다

- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨

- 단계 *
  1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
  2. 모니터 * 페이지에서 * 작업 * 을 클릭합니다.
  3. Jobs * 페이지에서 다음 단계를 수행하십시오.
     a. 을 클릭합니다 클론 작업만 나열되도록 목록을 필터링합니다.
     b. 시작 및 종료 날짜를 지정합니다.
     c. Type * 드롭다운 목록에서 * Clone * 을 선택합니다.
     d. Status * (상태 *) 드롭다운 목록에서 클론 상태를 선택합니다.
     e. 성공적으로 완료된 작업을 보려면 * 적용 * 을 클릭합니다.
  4. 클론 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
  5. 작업 세부 정보 페이지에서 * 로그 보기 * 를 클릭합니다.

SnapCenter 서버 및 플러그인 관리

대시보드 보기

대시보드 개요

SnapCenter의 왼쪽 탐색 창에서 대시보드에서 최근 작업 활동, 경고, 보호 요약, 스토리지 효율성 및 사용, SnapCenter 작업 상태(백업, 클론, 복원), 독립 실행형 및 Windows 클러스터 호스트의 구성 상태 등을 한눈에 파악할 수 있습니다. SnapCenter에서 관리하는 SVM(스토리지 가상 머신) 수 및 라이센스 용량

대시보드 보기에 표시되는 정보는 현재 SnapCenter에 로그인한 사용자에게 할당된 역할에 따라 달라집니다. 사용자가 해당 정보를 볼 수 있는 권한이 없는 경우 일부 콘텐츠가 표시되지 않을 수 있습니다.

대부분의 경우 * i * 를 마우스 포인터로 가리키면 디스플레이에 대한 자세한 정보를 볼 수 있습니다. 경우에 따라 대시보드 디스플레이의 정보가 리소스, 모니터 및 보고서와 같은 SnapCenter GUI 페이지의 자세한 소스 정보에 링크될 수 있습니다.

최근 작업 활동

최근 작업 활동 타일에는 액세스 권한이 있는 모든 백업, 복원 및 클론 작업의 최신 작업 활동이 표시됩니다. 이 디스플레이의 작업에는 완료, 경고, 실패, 실행 중, 대기 중, 및 취소됨.

작업 위로 마우스를 이동하면 자세한 정보를 볼 수 있습니다. 특정 작업 번호를 클릭하여 추가 작업 정보를 볼 수 있습니다. 이 작업 번호는 Monitor 페이지로 리디렉션됩니다. 여기서 작업 세부 정보 또는 로그 정보를 얻고 해당 작업에 대한 보고서를 생성할 수 있습니다.

모든 SnapCenter 작업의 기록을 보려면 * 모두 보기 * 를 클릭합니다.

경고

Alerts(경고) 타일에는 호스트 및 SnapCenter 서버에 대한 최신 미해결 위험 및 경고 경고가 표시됩니다.

위험 및 경고 범주 경고의 총 개수가 디스플레이 상단에 표시됩니다. 위험 또는 경고 합계를 클릭하면 경고 페이지에 특정 필터가 적용된 경고 페이지로 리디렉션됩니다.

특정 경고를 클릭하면 해당 경고에 대한 자세한 내용을 볼 수 있는 경고 페이지로 리디렉션됩니다. 디스플레이 하단의 * 모두 보기 * 를 클릭하면 경고 페이지로 이동하여 모든 경고 목록을 볼 수 있습니다.

최신 보호 요약

최신 보호 요약 타일은 액세스 권한이 있는 모든 엔티티에 대한 보호 상태를 제공합니다. 기본적으로 디스플레이는 모든 플러그인의 상태를 제공하도록 설정됩니다. 상태 정보는 기본 스토리지에 Snapshot 복사본으로 백업된 리소스 및 SnapMirror 및 SnapVault 기술을 사용하는 보조 스토리지에 제공됩니다. 보조 스토리지에 대한 보호 상태 정보의 가용성은 선택한 플러그인 유형에 따라 달라집니다.

> 미러 소산 보호 정책을 사용하는 경우 보호 요약의 카운터가 SnapMirror 차트가 아니라 SnapVault 요약 차트에 표시됩니다.

개별 플러그인의 보호 상태는 드롭다운 메뉴에서 플러그인을 선택하여 사용할 수 있습니다. 도넛형 차트에는 선택한 플러그인에 대한 보호된 리소스의 백분율이 표시됩니다. 도넛 조각을 클릭하면 * 보고서 * > * 플러그인 * 페이지로 리디렉션되며, 지정된 플러그인에 대한 모든 기본 및 보조 스토리지 작업에 대한 자세한 보고서가 제공됩니다.

보조 스토리지에 대한 보고서는 SnapVault에만 적용되고 SnapMirror 보고서는 지원되지 않습니다.

SAP HANA는 스냅샷 복사본을 위한 운영 스토리지 및 2차 스토리지에 대한 보호 상태 정보를 제공합니다. 파일 기반 백업에는 운영 스토리지 보호 상태만 사용할 수 있습니다.

보호 상태입니다	운영 스토리지	2차 스토리지
실패했습니다	리소스 그룹에 속한 엔터티의 개수로, 리소스 그룹에서 백업을 실행했지만 백업이 실패했습니다.	보조 대상으로 전송하지 못한 백업이 있는 엔터티의 수입니다.
성공했습니다	리소스 그룹이 성공적으로 백업된 리소스 그룹의 엔티티 수입니다.	보조 대상으로 성공적으로 전송된 백업의 엔티티 수입니다.
구성되지 않았습니다	리소스 그룹에 속하지 않고 백업되지 않은 엔터티의 수입니다.	백업을 위해 구성되지 않은 하나 이상의 리소스 그룹에 속한 엔터티가 보조 대상으로 전송될 수 있습니다.
시작되지 않았습니다	리소스 그룹에 속하지만 백업이 실행되지 않은 엔터티의 수입니다.	해당 없음.

백업을 생성하기 위해 SnapCenter 서버 4.2 및 이전 버전의 플러그인(4.2 이전)을 사용하는 경우 * 최신 보호 요약 * 타일에 이러한 백업의 SnapMirror 보호 상태가 표시되지 않습니다.

작업

작업 타일은 액세스할 수 있는 백업, 복원 및 클론 작업의 요약을 제공합니다. 드롭다운 메뉴를 사용하여 보고서의 시간 프레임을 사용자 지정할 수 있습니다. 기간 옵션은 최근 24시간, 지난 7일 및 지난 30일에 고정됩니다. 기본 보고서에는 지난 7일 동안 실행된 데이터 보호 작업이 표시됩니다.

백업, 복원 및 클론 작업 정보가 도넛형 차트에 표시됩니다. 도넛형 조각을 클릭하면 선택 항목에 미리 적용된 작업 필터가 있는 모니터 페이지로 이동합니다.

작업 상태입니다	설명
실패했습니다	실패한 작업 수입니다.
경고	오류가 발생한 작업 수입니다.
성공했습니다	성공적으로 완료된 작업의 수입니다.
실행 중입니다	현재 실행 중인 작업 수입니다.

스토리지

Storage(스토리지) 타일은 90일 동안 보호 작업에서 사용하는 운영 및 보조 스토리지를 표시하고, 소비 추세를 그래픽으로 표시하고, 기본 스토리지 절약 효과를 계산합니다. 스토리지 정보는 24시간마다 오전 12시에 업데이트됩니다

SnapCenter에서 사용할 수 있는 총 백업 수와 이러한 백업이 차지하는 크기로 구성된 일일 총 소모량이 디스플레이 상단에 표시됩니다. 백업에는 여러 스냅샷 복사본이 연결될 수 있으며 이 수에 동일하게 반영됩니다. 이 옵션은 기본 및 보조 스냅샷 복사본에 모두 적용할 수 있습니다. 예를 들어 10개의 백업을 생성했으며, 그 중 2개는 정책 기반 백업 보존으로 인해 삭제되고 1개의 백업은 사용자가 명시적으로 삭제합니다. 따라서 7개의 백업이 차지하는 크기와 함께 7개의 백업이 표시됩니다.

운영 스토리지의 스토리지 절약 비율은 기본 스토리지의 물리적 용량에 대한 논리적 용량(클론 및 스냅샷 복사본 절약 + 스토리지 소비)의 비율입니다. 막대 차트는 스토리지 절약 효과를 보여 줍니다.

선형 그래프는 롤링 90일 동안 1차 및 2차 스토리지 소비를 일 단위로 각각 플롯합니다. 차트 위에 마우스를 놓으면 자세한 일별 결과가 표시됩니다.

백업을 생성하기 위해 SnapCenter 서버 4.2와 이전 버전의 플러그인(4.2 이전)을 사용하는 경우 * 스토리지 * 타일에는 백업 수, 이러한 백업에서 사용되는 스토리지, 스냅샷 절약, 클론 절감 및 스냅샷 크기가 표시되지 않습니다.

구성

구성 타일은 SnapCenter가 관리하고 있고 사용자가 액세스할 수 있는 모든 활성 독립 실행형 및 Windows 클러스터 호스트에 대한 통합 상태 정보를 제공합니다. 여기에는 해당 호스트와 연결된 플러그인 상태 정보가 포함됩니다.

Hosts 옆의 숫자를 클릭하면 Hosts 페이지의 Managed Hosts 섹션으로 이동합니다. 여기서 선택한 호스트에 대한 자세한 정보를 얻을 수 있습니다.

또한 이 디스플레이에 SnapCenter에서 관리하는 독립 실행형 ONTAP SVM과 클러스터 ONTAP SVM의 합계가 표시되고 액세스할 수 있는 가 표시됩니다. SVM 옆의 번호를 클릭하면 스토리지 시스템 페이지로 이동합니다. 여기서 선택한 SVM에 대한 자세한 정보를 얻을 수 있습니다.

호스트 구성 상태는 각 상태의 호스트 수와 함께 빨간색(위험), 노란색(경고) 및 녹색(활성)으로 표시됩니다. 상태 메시지는 각 상태에 대해 제공됩니다.

구성 상태입니다	설명
업그레이드가 필수입니다	지원되지 않는 플러그인을 실행하고 업그레이드가 필요한 호스트의 수입니다. 지원되지 않는 플러그인은 이 버전의 SnapCenter와 호환되지 않습니다.
마이그레이션은 필수입니다	지원되지 않는 플러그인을 실행하고 마이그레이션이 필요한 호스트의 수입니다. 지원되지 않는 플러그인은 이 버전의 SnapCenter와 호환되지 않습니다.
설치된 플러그인이 없습니다	성공적으로 추가되었지만 플러그인을 설치해야 하거나 플러그인 설치에 실패한 호스트의 수입니다.

구성 상태입니다	설명
일시 중단됨	스케줄이 일시 중단되어 유지 보수 중인 호스트의 수입니다.
중지되었습니다	가동되지만 플러그인 서비스가 실행되고 있지 않은 호스트의 수입니다.
호스트가 다운되었습니다	다운되었거나 연결할 수 없는 호스트의 수입니다.
업그레이드 가능(선택 사항)	최신 버전의 플러그인 패키지를 업그레이드할 수 있는 호스트의 수입니다.
마이그레이션 사용 가능(선택 사항)	마이그레이션을 위해 최신 버전의 플러그인을 사용할 수 있는 호스트의 수입니다.
로그 디렉터리를 구성합니다	트랜잭션 로그 백업을 수행하려면 SCSQL에 대해 로그 디렉토리를 구성해야 하는 호스트의 수입니다.
VMware 플러그인을 구성합니다	VMware vSphere용 SnapCenter 플러그인을 추가해야 하는 호스트 수입니다.
알 수 없음	등록되었지만 설치가 아직 트리거되지 않은 호스트의 수입니다.
실행 중입니다	실행 중인 호스트 및 플러그인의 수입니다. SCSQL 플러그인의 경우 로그 디렉토리와 하이퍼바이저가 구성됩니다.
플러그인 설치\ 제거 중	플러그인 설치 또는 제거가 진행 중인 호스트의 수입니다.

라이센스 용량

라이센스 용량 타일은 SnapCenter 표준 용량 기반 라이센스에 대한 라이센스 만료 경고, 사용된 용량, 용량 임계값 경고 및 총 라이센스 용량에 대한 정보를 표시합니다.

이 표시는 Cloud Volumes ONTAP 또는 ONTAP Select 플랫폼에서 SnapCenter 표준 용량 기반 라이센스를 사용하는 경우에만 나타납니다. FAS, AFF 또는 모든 SAN 어레이(ASA) 플랫폼의 경우 SnapCenter 라이센스는 컨트롤러 기반이며 무제한 용량으로 라이센스가 부여되며 용량 라이센스는 필요하지 않습니다.

라이센스 상태입니다	설명
사용 중입니다	현재 사용 중인 용량입니다.

라이센스 상태입니다	설명
알림	용량 임계값 - 알림이 대시보드에 표시되고, 구성된 경우 e-메일 알림이 전송될 때 알림이 표시되는 임계값입니다.
허가되었습니다	라이센스 용량의 양입니다.
않습니다	라이센스 용량을 초과한 용량의 양입니다.

대시보드에서 정보를 보는 방법

SnapCenter 왼쪽 탐색 창에서 다양한 대시보드 타일을 보거나 관련 시스템 세부 정보와 함께 표시할 수 있습니다. 대시보드에서 사용 가능한 디스플레이 수는 고정되어 있으며 변경할 수 없습니다. 각 디스플레이 내에서 제공되는 콘텐츠는 역할 기반 액세스 제어(RBAC)에 따라 달라집니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 대시보드 * 를 클릭합니다.
  2. 추가 정보를 얻으려면 각 디스플레이의 활성 영역을 클릭합니다.

     예를 들어, * 작업 * 에서 도넛형 차트를 클릭하면 선택에 대한 자세한 정보가 모니터 페이지로 리디렉션됩니다. 보호 요약 * 에서 도넛형 차트를 클릭하면 보고서 페이지로 리디렉션되어 선택 사항에 대한 자세한 정보를 볼 수 있습니다.

대시보드에서 작업의 상태 보고서를 요청합니다

대시보드 페이지에서 백업, 복원 및 클론 작업에 대한 보고서를 요청할 수 있습니다. 이 기능은 SnapCenter 환경에서 성공하거나 실패한 작업의 총 수를 확인하려는 경우에 유용합니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 대시보드 * 를 클릭합니다
  2. 대시보드에서 작업 타일을 찾은 다음 * 백업 *, * 복원 * 또는 * 클론 * 을 선택합니다.
  3. 풀다운 메뉴를 사용하여 24시간, 7일 또는 30일 중에서 작업 정보를 원하는 기간을 선택합니다.

     데이터가 포함된 도넛형 차트가 표시됩니다.

  4. 보고서를 작성할 작업 정보를 나타내는 도넛형 조각을 클릭합니다.

     도넛형 차트를 클릭하면 대시보드 페이지에서 모니터 페이지로 리디렉션됩니다. 모니터 페이지에는 도넛형 차트에서 선택한 상태의 작업이 표시됩니다.

  5. Monitor(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 상태에 대한 보고서를 요청합니다

대시보드를 사용하여 특정 플러그인에서 관리하는 리소스에 대한 보호 세부 정보를 요청할 수 있습니다. 데이터 백업은 데이터 보호 요약으로 간주됩니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 대시보드 * 를 클릭합니다.
2. 대시보드에서 최신 보호 요약 타일을 찾아 풀다운 메뉴를 사용하여 플러그인을 선택합니다.

   대시보드에는 운영 스토리지에 백업된 리소스에 대한 도넛형 차트가 표시됩니다. 플러그인에는 보조 스토리지에 백업된 리소스에 대한 도넛형 차트가 표시됩니다.

   데이터 보호 보고서는 특정 플러그인 유형에 대해서만 사용할 수 있습니다. 모든 플러그인*을 지정하는 것은 지원되지 않습니다.

3. 보고서를 만들 상태를 나타내는 도넛형 조각을 클릭합니다.

   도넛형 차트를 클릭하면 대시보드 페이지에서 보고서, 플러그인 페이지로 리디렉션됩니다. 선택한 플러그인의 상태만 보고서에 표시됩니다. 보고서를 검토하거나 로컬 시스템에 다운로드할 수 있습니다.

SnapMirror 도넛 차트 및 파일 기반 SAP HANA 백업에 대한 보고서 페이지로 리디렉션할 수 없습니다.

RBAC 관리

SnapCenter에서는 역할, 사용자 및 그룹을 수정할 수 있습니다.

역할을 수정합니다

SnapCenter 역할을 수정하여 사용자 또는 그룹을 제거하고 역할에 연결된 권한을 변경할 수 있습니다. 전체 역할에 사용되는 권한을 변경하거나 제거하고자 할 때 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 수정할 역할을 클릭합니다.
4. 역할 세부 정보 페이지에서 권한을 변경하거나 필요에 따라 구성원을 할당 해제합니다.

5. 이 역할의 모든 구성원은 다른 구성원의 개체를 볼 수 있습니다 * 를 선택하여 역할의 다른 구성원이 리소스 목록을 새로 고친 후 볼륨 및 호스트와 같은 리소스를 볼 수 있도록 합니다.

   이 역할의 구성원이 다른 구성원이 할당된 개체를 보지 못하도록 하려면 이 옵션을 선택 취소합니다.

   이 옵션을 사용하면 개체 또는 리소스를 만든 사용자와 동일한 역할에 속한 사용자는 개체 또는 리소스에 대한 사용자 액세스를 할당할 필요가 없습니다.

1. 제출 * 을 클릭합니다.

사용자 및 그룹을 수정합니다

SnapCenter 사용자 또는 그룹을 수정하여 역할 및 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 수정할 사용자 또는 그룹을 클릭합니다.
  4. 사용자 또는 그룹 세부 정보 페이지에서 역할 및 자산을 변경합니다.
  5. 제출 * 을 클릭합니다.

호스트를 관리합니다

호스트를 추가하고 SnapCenter 플러그인 패키지를 설치하고, 검증 서버를 추가하고, 호스트를 제거하고, 백업 작업을 마이그레이션하고, 호스트를 업데이트하여 플러그인 패키지를 업그레이드하거나 새 플러그인 패키지를 추가할 수 있습니다. 사용 중인 플러그인에 따라 디스크 프로비저닝, SMB 공유 관리, 이니시에이터 그룹(igroup) 관리, iSCSI 세션 관리 및 데이터 마이그레이션도 가능합니다.

이러한 작업을 수행할 수 있습니다…	**Microsoft Exchange Server**의 경우	**Microsoft SQL Server**의 경우	**Microsoft Windows**의 경우	고성능 솔루션	**SAP HANA** 데이터베이스용	맞춤형 플러그인용
호스트를 추가하고 플러그인 패키지를 설치합니다	예	예	예	예	예	예
호스트의 ESXi 정보를 업데이트합니다	아니요	예	아니요	아니요	아니요	아니요

이러한 작업을 수행할 수 있습니다…	**Microsoft Exchange Server**의 경우	**Microsoft SQL Server**의 경우	**Microsoft Windows**의 경우	고성능 솔루션	**SAP HANA** 데이터베이스용	맞춤형 플러그인용
스케줄을 일시 중지하고 호스트를 유지 보수 모드로 전환합니다	예	예	예	예	예	예
플러그인을 추가, 업그레이드 또는 제거하여 호스트를 수정합니다	예	예	예	예	예	예
SnapCenter에서 호스트를 제거합니다	예	예	예	예	예	예
플러그인 서비스를 시작합니다	예	예	예	예	예	예
디스크 프로비저닝	아니요	아니요	예	아니요	아니요	아니요
SMB 공유를 관리합니다	아니요	아니요	예	아니요	아니요	아니요
iGroup을 관리합니다	아니요	아니요	예	아니요	아니요	아니요
iSCSI 세션을 관리합니다	아니요	아니요	예	아니요	아니요	

가상 머신 정보를 새로 고칩니다

VMware vCenter 자격 증명이 변경되거나 데이터베이스 또는 파일 시스템 호스트가 다시 시작될 때 가상 머신 정보를 새로 고쳐야 합니다. SnapCenter에서 가상 머신 정보를 새로 고치면 VMware vSphere vCenter와의 통신이 시작되고 vCenter 자격 증명이 획득됩니다.

RDM 기반 디스크는 데이터베이스 호스트에 설치된 Microsoft Windows용 SnapCenter 플러그인으로 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. Managed Hosts 페이지에서 업데이트할 호스트를 선택합니다.
4. VM 새로 고침 * 을 클릭합니다.

플러그인 호스트를 수정합니다

플러그인을 설치한 후 필요한 경우 플러그인 호스트 세부 정보를 수정할 수 있습니다. Microsoft SQL Server용 SnapCenter 플러그인, GMSA(그룹 관리 서비스 계정) 및 플러그인 포트에 대한 자격 증명, 설치 경로, 플러그인, 로그 디렉토리 세부 정보를 수정할 수 있습니다.

플러그인 버전이 SnapCenter 서버 버전과 동일한지 확인합니다.

- 이 작업에 대한 정보 *
- 플러그인 포트는 플러그인이 설치된 후에만 수정할 수 있습니다.

  업그레이드 작업이 진행 중인 동안에는 플러그인 포트를 수정할 수 없습니다.

- 플러그인 포트를 수정하는 동안 다음 포트 롤백 시나리오를 알고 있어야 합니다.
  - 독립 실행형 설정에서 SnapCenter가 구성 요소 중 하나의 포트를 변경하지 못하면 작업이 실패하고 모든 구성 요소에 대해 이전 포트가 유지됩니다.

    모든 구성 요소에 대해 포트가 변경되었지만 구성 요소 중 하나가 새 포트로 시작되지 않는 경우 모든 구성 요소에 대해 이전 포트가 유지됩니다. 예를 들어, 독립 실행형 호스트에서 2개의 플러그인에 대한 포트를 변경하려고 할 때 SnapCenter가 새 포트를 플러그인 중 하나에 적용하지 못하면 작업이 실패하고(적절한 오류 메시지가 표시됨) 이전 포트는 두 플러그인에 대해 유지됩니다.

  - 클러스터 설정에서 SnapCenter가 노드 중 하나에 설치된 플러그인의 포트를 변경하지 못할 경우 작업이 실패하고 모든 노드에 대해 이전 포트가 유지됩니다.

    예를 들어, 플러그인이 클러스터 설치의 4개 노드에 설치되고 노드 중 하나에 대해 포트가 변경되지 않은 경우 이전 포트는 모든 노드에 대해 유지됩니다.

GMSA와 함께 플러그인을 설치하면 * 추가 옵션 * 창에서 수정할 수 있습니다. GMSA 없이 플러그인을 설치하는 경우 GMSA 계정을 지정하여 플러그인 서비스 계정으로 사용할 수 있습니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 맨 위에 * Managed Hosts * 가 선택되어 있는지 확인합니다.
3. 수정할 호스트를 선택하고 하나의 필드를 수정합니다.

   한 번에 하나의 필드만 수정할 수 있습니다.

4. 제출 * 을 클릭합니다.

결과 *

호스트가 검증되어 SnapCenter 서버에 추가됩니다.

플러그인 서비스를 시작하거나 다시 시작합니다

SnapCenter 플러그인 서비스를 시작하면 서비스가 실행되고 있지 않은 경우 서비스를 시작하거나 실행 중인 경우 서비스를 다시 시작할 수 있습니다. 유지 관리를 수행한 후 서비스를 다시 시작할 수 있습니다.

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. Managed Hosts 페이지에서 시작할 호스트를 선택합니다.
  4. 을 클릭합니다 아이콘을 클릭하고 * 서비스 시작 * 또는 * 서비스 다시 시작 * 을 클릭합니다.

     여러 호스트의 서비스를 동시에 시작하거나 다시 시작할 수 있습니다.

호스트 유지 관리를 위한 스케줄을 일시 중지합니다

호스트가 SnapCenter 예약 작업을 실행하지 못하도록 하려면 호스트를 유지 관리 모드로 전환할 수 있습니다. 플러그인을 업그레이드하거나 호스트에 대한 유지보수 작업을 수행하기 전에 이 작업을 수행해야 합니다.

SnapCenter가 해당 호스트와 통신할 수 없기 때문에 중단된 호스트의 스케줄을 일시 중지할 수 없습니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
  2. 호스트 페이지에서 * 관리되는 호스트 * 를 클릭합니다.
  3. Managed Hosts 페이지에서 일시 중지할 호스트를 선택합니다.
  4. 를 클릭합니다 아이콘을 클릭한 다음 * Suspend Schedule * 을 클릭하여 이 플러그인의 호스트를 유지 관리 모드로 설정합니다.

     여러 호스트의 스케줄을 동시에 일시 중지할 수 있습니다.

     먼저 플러그인 서비스를 중지할 필요가 없습니다. 플러그인 서비스는 실행 중 또는 중지됨 상태일 수 있습니다.

결과 *

호스트에서 스케줄을 일시 중지한 후 호스트의 전체 상태 필드에 관리 호스트 페이지에 * 일시 중단됨 * 이 표시됩니다.

호스트 유지 관리를 완료한 후 * Activate Schedule * (일정 활성화 *)을 클릭하여 호스트를 유지 관리 모드에서 빠져나올 수 있습니다.
여러 호스트의 스케줄을 동시에 활성화할 수 있습니다.

리소스 페이지에서 지원되는 작업입니다

리소스 페이지에서 리소스를 검색하고 데이터 보호 작업을 수행할 수 있습니다. 수행할 수 있는 작업은 리소스를 관리하는 데 사용하는 플러그인에 따라 다릅니다.

자원 페이지에서 다음 작업을 수행할 수 있습니다.

이러한 작업을 수행할 수 있습니다...	**Microsoft Exchange Server**의 경우	**Microsoft SQL Server**의 경우	**Microsoft Windows**의 경우	고성능 솔루션	**SAP HANA** 데이터베이스용	맞춤형 플러그인용
리소스를 백업에 사용할 수 있는지 여부를 확인합니다	예	예	예	예	예	예
리소스의 필요 시 백업을 수행합니다	예	예	예	예	예	예
백업에서 복원합니다	예	예	예	예	예	예
클론 백업	아니요	예	예	예	예	예
백업 관리	예	예	예	예	예	예
클론 관리	아니요	예	예	예	예	예
정책 관리	예	예	예	예	예	예
스토리지 접속을 관리합니다	예	예	예	예	예	예
백업을 마운트합니다	아니요	아니요	아니요	예	아니요	아니요
백업을 마운트 해제합니다	아니요	아니요	아니요	예	아니요	아니요
세부 정보 보기	예	예	예	예	예	예

정책 관리

리소스 또는 리소스 그룹에서 정책을 분리하고 수정, 삭제, 보기 및 복사할 수 있습니다.

정책을 수정합니다

정책이 리소스 또는 리소스 그룹에 연결되어 있는 동안 복제 옵션, 스냅샷 복사본 보존 설정, 오류 재시도 횟수 또는 스크립트 정보를 수정할 수 있습니다. 정책을 분리한 후에만 스케줄 유형(빈도)을 수정할 수 있습니다.

- 이 작업에 대한 정보 *

SnapCenter 서버는 정책이 리소스 또는 리소스 그룹에 연결될 때만 일정 유형을 등록하므로 정책에서 일정 유형을 수정하려면 추가 단계가 필요합니다.

원하는 작업	그러면...
추가 일정 유형을 추가합니다	새 정책을 만들어 필요한 리소스 또는 리소스 그룹에 연결합니다. 예를 들어 리소스 그룹 정책에서 매시간 백업만 지정하고 일별 백업도 추가하려는 경우 일별 스케줄 유형을 사용하여 정책을 생성한 후 리소스 그룹에 추가할 수 있습니다. 그러면 리소스 그룹에는 매시간 및 매일의 두 가지 정책이 있습니다.
일정 유형을 제거 또는 변경합니다	다음을 수행합니다. 1. 해당 정책을 사용하는 모든 리소스 및 리소스 그룹에서 정책을 분리합니다. 2. 스케줄 유형을 수정합니다. 3. 모든 리소스 및 리소스 그룹에 정책을 다시 연결합니다. 예를 들어, 정책이 시간별 백업을 지정하고 이를 일일 백업으로 변경하려는 경우 먼저 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 다음 * 마침 * 을 클릭합니다.

정책을 분리합니다

이러한 정책이 리소스에 대한 데이터 보호를 더 이상 제어하지 않도록 하려는 경우 언제든지 리소스 또는 리소스 그룹에서 정책을 분리할 수 있습니다. 정책을 삭제하거나 스케줄 유형을 수정하기 전에 먼저 정책을 분리해야 합니다.

- 단계 *

  1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
  2. 리소스 페이지의 * 보기 * 목록에서 * 리소스 그룹 * 을 선택합니다.
  3. 자원 그룹을 선택한 다음 * 자원 그룹 수정 * 을 클릭합니다.
  4. 자원 그룹 수정 마법사의 정책 페이지에 있는 드롭다운 목록에서 분리할 정책 옆에 있는 확인 표시를 지웁니다.
  5. 마법사의 나머지 부분에서 리소스 그룹을 추가로 수정한 후 * Finish * 를 클릭합니다.

정책을 삭제합니다

더 이상 정책이 필요하지 않으면 삭제할 수 있습니다.

시작하기 전에

정책이 리소스 또는 리소스 그룹과 연결된 경우 리소스 또는 리소스 그룹에서 정책을 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 클릭합니다.

자원 그룹을 관리합니다

리소스 그룹에 대해 다양한 작업을 수행할 수 있습니다.

자원 그룹과 관련된 다음 작업을 수행할 수 있습니다.

- 자원 그룹을 만드는 동안 제공한 정보를 편집하려면 자원 그룹을 선택하고 * 자원 그룹 수정 * 을 클릭하여 자원 그룹을 수정합니다.

  자원 그룹을 수정하는 동안 일정을 변경할 수 있습니다. 그러나 스케줄 유형을 변경하려면 정책을 수정해야 합니다.

  리소스 그룹에서 리소스를 제거하면 현재 리소스 그룹에 연결된 정책에 정의된 백업 보존 설정이 제거된 리소스에 계속 적용됩니다.

- 리소스 그룹의 백업을 생성합니다.
- 백업의 클론을 생성합니다.

  SQL, Oracle, Windows 파일 시스템, 맞춤형 애플리케이션, SAP HANA 데이터베이스 리소스 또는 리소스 그룹의 기존 백업에서 클론을 생성할 수 있습니다.

- 리소스 그룹의 클론을 생성합니다.

  이 작업은 SQL 리소스 그룹(데이터베이스만 포함)에만 지원됩니다. 리소스 그룹 클론 생성(클론 라이프사이클)에

대한 스케줄을 구성할 수 있습니다.

- 리소스 그룹에 대한 예약된 작업이 시작되지 않도록 합니다.
- 자원 그룹을 삭제합니다.

리소스 그룹에 대한 작업을 중지하고 다시 시작합니다

자원 그룹에서 예약된 작업을 시작하는 것을 일시적으로 해제할 수 있습니다. 나중에 원하는 경우 이러한 작업을 활성화할 수 있습니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
  2. 리소스 페이지의 * 보기 * 목록에서 * 리소스 그룹 * 을 선택합니다.
  3. 자원 그룹을 선택하고 * 유지보수 * 를 클릭합니다.
  4. 확인 * 을 클릭합니다.

유지보수 모드로 설정한 리소스 그룹에 대한 작업을 재개하려면 리소스 그룹을 선택하고 * 운영 * 을 클릭합니다.

리소스 그룹을 삭제합니다

자원 그룹의 자원을 더 이상 보호할 필요가 없는 경우 자원 그룹을 삭제할 수 있습니다. SnapCenter에서 플러그인을 제거하기 전에 리소스 그룹이 삭제되었는지 확인해야 합니다.

- 이 작업에 대한 정보 *

리소스 그룹의 리소스에 대해 생성된 모든 클론을 수동으로 삭제해야 합니다. 선택적으로 리소스 그룹에 연결된 모든 백업, 메타데이터, 정책 및 스냅샷 복사본을 강제로 삭제할 수 있습니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
  2. 리소스 페이지의 * 보기 * 목록에서 * 리소스 그룹 * 을 선택합니다.
  3. 자원 그룹을 선택한 다음 * 삭제 * 를 클릭합니다.
  4. 선택 사항: 이 리소스 그룹과 연결된 백업 및 분리 정책 * 삭제 확인란을 선택하여 리소스 그룹과 연결된 모든 백업, 메타데이터, 정책 및 스냅샷 복사본을 제거합니다.
  5. 확인 * 을 클릭합니다.

백업 관리

백업의 이름을 바꾸고 삭제할 수 있습니다. 여러 백업을 동시에 삭제할 수도 있습니다.

백업 이름을 바꿉니다

검색 가능성을 향상시키기 위해 더 나은 이름을 제공하려면 백업 이름을 바꿀 수 있습니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 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 보호를 위해 구성되지 않은 경우 토폴로지 페이지 대신 보호 마법사가 표시됩니다.

4. Manage Copies 보기의 기본 스토리지 시스템에서 * Backups * 를 선택합니다.

   보조 스토리지 시스템에 있는 백업의 이름은 변경할 수 없습니다.

Oracle RMAN(Recovery Manager)을 사용하여 Oracle 데이터베이스의 백업을 카탈로그로 작성한 경우 이러한 카탈로그 작성된 백업의 이름을 바꿀 수 없습니다.

1. 백업을 선택한 다음 을 클릭합니다  .
2. 백업 이름 바꾸기 * 필드에 새 이름을 입력하고 * 확인 * 을 클릭합니다.

백업을 삭제합니다

다른 데이터 보호 작업을 위해 더 이상 백업이 필요하지 않은 경우 백업을 삭제할 수 있습니다.

시작하기 전에

백업을 삭제하기 전에 연결된 클론을 삭제해야 합니다.

백업이 클론 생성된 리소스와 연결된 경우 백업을 삭제할 수 없습니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
3. 목록에서 리소스 또는 리소스 그룹을 선택합니다.

   리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

4. Manage Copies 보기의 기본 스토리지 시스템에서 * Backups * 를 선택합니다.

   보조 스토리지 시스템에 있는 백업은 삭제할 수 없습니다.

5. 백업을 선택한 다음 을 클릭합니다  .

   SAP HANA 데이터베이스 백업을 삭제하는 경우 관련된 백업 SAP HANA 카탈로그도 함께 삭제됩니다.

마지막 남은 백업을 삭제하면 관련 HANA 카탈로그 항목을 삭제할 수 없습니다.

1. 확인 * 을 클릭합니다.

SnapCenter에 스토리지 시스템에 해당하는 백업이 없는 오래된 데이터베이스 백업이 있는 경우 remove-smbackup 명령을 사용하여 이러한 오래된 백업 항목을 정리해야 합니다. 오래된 백업이 카탈로그로 작성된 경우 복구 카탈로그 데이터베이스에서 카탈로그가 해제됩니다.

클론 삭제

더 이상 필요하지 않은 클론은 삭제할 수 있습니다.

- 이 작업에 대한 정보 *

다른 클론의 소스와 같은 역할을 하는 클론은 삭제할 수 없습니다.

예를 들어 운영 데이터베이스가 db1인 경우 데이터베이스 clone1이 db1의 백업에서 복제되고 이후에 clone1이 보호됩니다. clone1의 백업에서 데이터베이스 clone2가 복제됩니다. clone1을 삭제하려면 먼저 clone2를 삭제한 다음 clone1을 삭제해야 합니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
  2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 또는 리소스 그룹을 선택합니다.
  3. 목록에서 리소스 또는 리소스 그룹을 선택합니다.

     리소스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.
  4. Manage Copies 뷰에서 운영 또는 2차(미러링 또는 복제) 스토리지 시스템에서 * Clones * 를 선택합니다.
  5. 클론을 선택한 다음 을 클릭합니다 .

     SAP HANA 데이터베이스 클론을 삭제하는 경우 클론 삭제 페이지에서 다음 작업을 수행합니다.

     a. Pre clone delete * 필드에 클론을 삭제하기 전에 실행해야 하는 명령을 입력합니다.
     b. 클론을 삭제하기 전에 * Unmount * 필드에 클론을 마운트 해제하는 명령을 입력합니다.
  6. 확인 * 을 클릭합니다.
- 완료 후 *

파일 시스템이 삭제되지 않는 경우가 있습니다. 다음 명령을 실행하여 clone_delete_delay 매개 변수의 값을 늘려야 합니다.`../sccli Set-SmConfigSettings`

clone_delete_delay 매개 변수는 애플리케이션 클론 삭제를 완료한 후 파일 시스템 삭제를 시작하기 전에 대기할 시간(초)을 지정합니다.

매개 변수 값을 수정한 후 SnapCenter SPL(Plug-in Loader) 서비스를 다시 시작합니다.

작업, 일정, 이벤트 및 로그를 모니터링합니다

작업 진행 상황을 모니터링하고, 예약된 작업에 대한 정보를 얻고, 모니터 페이지에서 이벤트 및 로그를 검토할 수 있습니다.

작업을 모니터링합니다

SnapCenter 백업, 클론, 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 정보 및 로그 파일을 얻을 수 있습니다.

SnapMirror 및 SnapVault 작업과 관련된 작업을 모니터링할 수도 있습니다.

SnapCenter 관리자 또는 다른 수퍼 사용자 역할이 할당되지 않은 경우 사용자가 생성한 작업과 사용자와 관련된 작업만 모니터링할 수 있습니다.

작업 모니터링과 관련된 다음 작업을 수행할 수 있습니다.

- 백업, 클론, 복원 및 검증 작업을 모니터링합니다.
- 작업 세부 정보 및 보고서를 봅니다.
- 예약된 작업을 중지합니다.

일정을 모니터링합니다

현재 스케줄을 확인하여 작업 시작 시간, 마지막 실행 시간 및 다음 실행 시기를 결정할 수 있습니다. 또한 작업이 실행되는 호스트를 작업의 리소스 그룹 및 정책 정보와 함께 확인할 수도 있습니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
  2. 모니터 페이지에서 * 스케줄 * 을 클릭합니다.
  3. 자원 그룹과 일정 유형을 선택합니다.
  4. 예약된 작업 목록을 봅니다.

이벤트를 모니터링합니다

사용자가 리소스 그룹을 만들 때 또는 시스템이 예약된 백업 생성과 같은 작업을 시작할 때와 같이 시스템에서 SnapCenter 이벤트 목록을 볼 수 있습니다. 백업 또는 복구 작업과 같은 작업이 현재 진행 중인지 여부를 확인하기 위해 이벤트를 볼 수 있습니다.

- 이 작업에 대한 정보 *

모든 작업 정보가 이벤트 페이지에 나타납니다. 예를 들어 백업 작업이 시작되면 ""백업 시작"" 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 상자에 시작 또는 종료 날짜, 이벤트 범주(예: 백업, 리소스 그룹 또는 정책) 및 심각도 수준을 입력하고 * 적용 * 을 클릭합니다. 또는 검색 상자에 문자를 입력합니다.
  4. 이벤트 목록을 봅니다.

로그를 모니터링합니다

SnapCenter 서버 로그, SnapCenter 호스트 에이전트 로그 및 플러그인 로그를 보고 다운로드할 수 있습니다. 문제 해결에 도움이 되도록 로그를 볼 수 있습니다.

- 이 작업에 대한 정보 *

로그를 필터링하여 특정 로그 심각도 수준만 표시할 수 있습니다.

- 디버그
- 정보
- 경고
- 오류
- 치명적

백업 작업 실패 원인을 해결하는 데 도움이 되는 로그 등의 작업 수준 로그를 얻을 수도 있습니다. 작업 수준 로그의 경우 * Monitor * > * Jobs * 옵션을 사용합니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
2. 작업 페이지에서 작업을 선택하고 로그 다운로드 를 클릭합니다.

   다운로드된 압축 폴더에는 작업 로그 및 공통 로그가 포함됩니다. 압축된 폴더 이름에는 선택한 작업 ID와 작업 유형이 포함되어 있습니다.
3. 모니터 페이지에서 * 로그 * 를 클릭합니다.
4. 로그 유형, 호스트 및 인스턴스를 선택합니다.

   로그 유형을 * plugin * 으로 선택한 경우 호스트 또는 SnapCenter 플러그인을 선택할 수 있습니다. 로그 유형이 * server * 인 경우 이 작업을 수행할 수 없습니다.
5. 특정 원본, 메시지 또는 로그 수준별로 로그를 필터링하려면 열 머리글 맨 위에 있는 필터 아이콘을 클릭합니다.

   모든 로그를 표시하려면 * 보다 크거나 같음 * 을 으로 선택합니다 `Debug` 레벨.
6. 새로 고침 * 을 클릭합니다.
7. 로그 목록을 봅니다.
8. 로그를 다운로드하려면 * 다운로드 * 를 클릭합니다.

   다운로드된 압축 폴더에는 작업 로그 및 공통 로그가 포함됩니다. 압축된 폴더 이름에는 선택한 작업 ID와 작업 유형이 포함되어 있습니다.

최적의 성능을 위한 대규모 구성에서는 PowerShell cmdlet을 사용하여 SnapCenter의 로그 설정을 최소 수준으로 설정해야 합니다.

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10
-JobLogsMaxFileSize 10MB -Server
```

페일오버 작업이 완료된 후 상태 또는 구성 정보에 액세스하려면 cmdlet을 실행합니다 `Get-SmRepositoryConfig`.

SnapCenter에서 작업 및 로그를 제거합니다

SnapCenter에서 백업, 복원, 클론, 검증 작업 및 로그를 제거할 수 있습니다. SnapCenter는 사용자가 제거하지 않는 한 성공하거나 실패한 작업 로그를 무기한 저장합니다. 스토리지를 보충하기 위해 제거할 수 있습니다.

- 이 작업에 대한 정보 *

현재 작업 중인 작업이 없어야 합니다.
작업 ID를 제공하여 특정 작업을 제거하거나 지정된 기간 내에 작업을 제거할 수 있습니다.

호스트를 유지보수 모드로 전환하여 작업을 제거할 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 작업의 상태를 검토합니다.

관련 정보

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

SnapCenter 보고 기능 개요

SnapCenter는 시스템 상태 및 운영 성공을 모니터링하고 관리할 수 있는 다양한 보고 옵션을 제공합니다.

보고서 유형	설명
백업 보고서	백업 보고서는 SnapCenter 환경의 백업 추세, 백업 성공률 및 지정된 시간 동안 수행된 각 백업에 대한 일부 정보에 대한 전체 데이터를 제공합니다. 백업이 삭제되면 보고서는 삭제된 백업에 대한 상태 정보를 표시하지 않습니다. 백업 세부 정보 보고서는 지정된 백업 작업에 대한 자세한 정보를 제공하고 성공적으로 백업된 리소스 및 실패한 리소스를 나열합니다.

보고서 유형	설명
보고서 복제	클론 보고서는 SnapCenter 환경의 클론 추세, 클론 성공률 및 지정된 시간 동안 수행된 각 클론 작업에 대한 일부 정보에 대한 전체 데이터를 제공합니다. 클론이 삭제되면 삭제된 클론에 대한 상태 정보가 보고서에 표시되지 않습니다. 클론 세부 정보 보고서에는 지정된 클론, 클론 호스트 및 클론 작업 작업 상태에 대한 세부 정보가 나와 있습니다. 작업이 실패하면 클론 세부 정보 보고서에 실패에 대한 정보가 표시됩니다.
보고서 복원	복원 보고서는 복원 작업에 대한 전체 정보를 제공합니다. 복구 세부 정보 보고서는 호스트 이름, 백업 이름, 작업 시작 및 기간, 개별 작업 작업 상태 등 지정된 복구 작업에 대한 세부 정보를 제공합니다. 작업이 실패하면 복구 세부 정보 보고서에 실패에 대한 정보가 표시됩니다.
보호 보고서	이러한 보고서는 모든 SnapCenter 플러그인 인스턴스에서 관리되는 리소스에 대한 보호 세부 정보를 제공합니다. 이 보고서는 모든 플러그인 인스턴스에서 관리되는 리소스에 대한 보호 세부 정보를 제공합니다. 개요, 보호되지 않은 리소스의 세부 정보, 보고서가 생성될 때 백업하지 않은 리소스, 백업 작업이 실패한 리소스 그룹의 리소스, SnapVault 상태를 확인할 수 있습니다.
예약된 보고서	이러한 보고서는 매일, 매주 또는 매월 정기적으로 실행되도록 예약되어 있습니다. 보고서는 지정된 날짜 및 시간에 자동으로 생성되며 전자 메일을 통해 각 사용자에게 전송됩니다 스케줄을 활성화, 비활성화, 수정 또는 삭제할 수 있습니다. 활성화된 스케줄은 * 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 이외의 다른 사용자는 자신의 권한에 따라 일정을 보거나 수정할 수 있습니다. 이 역할의 모든 구성원이 다른 구성원의 개체를 볼 수 있음 옵션이 역할 추가 페이지에서 선택된 경우 역할의 다른 구성원이 보고 수정할 수 있습니다.

보고서에 액세스합니다

SnapCenter 대시보드를 사용하여 시스템 상태를 빠르게 파악할 수 있습니다. 대시보드에서 자세한 정보를 확인할 수 있습니다. 또는 상세 보고서에 직접 액세스할 수도 있습니다.

다음 방법 중 하나를 사용하여 보고서에 액세스할 수 있습니다.

- 왼쪽 탐색 창에서 * 대시보드 * 를 클릭한 다음 * 마지막 보호 요약 * 원형 차트 를 클릭하여 보고서 페이지에서 자세한 내용을 확인합니다.

- 왼쪽 탐색 창에서 * 보고서 * 를 클릭합니다.

보고서를 필터링합니다

필요한 정보의 세부 수준과 시간 범위에 따라 다양한 매개 변수에 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 지정합니다.
     를 누릅니다
     종료 날짜를 생략하면 사용 가능한 모든 정보가 검색됩니다.
  4. 다음 기준에 따라 보고서 정보를 필터링합니다.
     - 리소스 그룹
     - 호스트
     - 정책
     - 리소스
     - 상태
     - 플러그인 이름입니다
  5. 적용 * 을 클릭합니다.

보고서를 내보내거나 인쇄합니다

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 미리 보기 전환 * 아이콘을 클릭합니다.
     - 보고서를 대체 형식으로 내보내려면 * 내보내기 * 아이콘 드롭다운 목록에서 형식을 선택합니다.
  3. 보고서를 인쇄하려면 * 인쇄 * 아이콘을 클릭합니다.
  4. 특정 보고서 요약을 보려면 보고서의 해당 섹션으로 스크롤합니다.

이메일 알림에 대한 **SMTP** 서버를 설정합니다

사용자 자신 또는 다른 사람에게 데이터 보호 작업 보고서를 보내는 데 사용할 SMTP 서버를 지정할 수 있습니다. 테스트 이메일을 보내 구성을 확인할 수도 있습니다. 이 설정은 이메일 알림을 구성하는 모든 SnapCenter 작업에 전체적으로 적용됩니다.

이 옵션은 모든 데이터 보호 작업 보고서를 전송할 SMTP 서버를 구성합니다. 그러나 직접 또는 다른 사용자에게 보내진 특정 리소스에 대해 정기적으로 SnapCenter 데이터 보호 작업을 업데이트하여 해당 업데이트의 상태를 모니터링하려는 경우 리소스 그룹을 만들 때 SnapCenter 보고서를 전자 메일로 보내는 옵션을 구성할 수 있습니다.

- 단계 *

  1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
  2. 설정 페이지에서 * 글로벌 설정 * 을 클릭합니다.
  3. SMTP 서버를 입력하고 * Save * 를 클릭합니다.
  4. 테스트 e-메일을 보내려면 e-메일을 보낼 e-메일 주소를 입력하고 제목을 입력한 다음 * 보내기 * 를 클릭합니다.

보고서를 e-메일로 보내는 옵션을 구성합니다

정기적으로 SnapCenter 데이터 보호 작업 업데이트를 자신 또는 다른 사람에게 보내 해당 업데이트의 상태를 모니터링하려는 경우 리소스 그룹을 만들 때 SnapCenter 보고서를 전자 메일로 보내는 옵션을 구성할 수 있습니다.

시작하기 전에

설정의 글로벌 설정 페이지에서 SMTP 서버를 구성해야 합니다.

- 단계 *

  1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
  2. 보려는 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 보고서를 항상 수신할지, 실패했는지, 아니면 실패했는지 또는 경고인지 선택합니다.
  4. 이메일을 보낼 주소, 이메일을 보낼 주소 및 이메일 제목을 입력합니다.

SnapCenter 서버 리포지토리를 관리합니다

SnapCenter에서 수행되는 다양한 작업과 관련된 정보는 SnapCenter 서버 데이터베이스 저장소에 저장됩니다. SnapCenter 서버가 데이터 손실로부터 보호되도록 리포지토리의 백업을 만들어야 합니다.

SnapCenter 서버 저장소는 NSM 데이터베이스라고도 합니다.

SnapCenter 리포지토리 보호를 위한 사전 요구 사항

SnapCenter 리포지토리를 보호하려면 환경에서 특정 사전 요구 사항을 충족해야 합니다.

- SVM(스토리지 가상 시스템) 연결 관리

  스토리지 자격 증명을 구성해야 합니다.

- 호스트 프로비저닝

  SnapCenter 저장소 호스트에는 하나 이상의 NetApp 저장소 디스크가 있어야 합니다. SnapCenter 저장소 호스트에 NetApp 디스크가 없으면 새로 만들어야 합니다.

  호스트 추가, SVM 연결 설정 및 호스트 프로비저닝에 대한 자세한 내용은 설치 지침을 참조하십시오.

- iSCSI LUN 또는 VMDK를 프로비저닝합니다

고가용성(HA) 구성의 경우 SnapCenter 서버 중 하나에 iSCSI LUN 또는 VMDK를 프로비저닝할 수 있습니다.

SnapCenter 리포지토리를 백업합니다

SnapCenter 서버 리포지토리를 백업하면 데이터 손실로부터 보호할 수 있습니다. _protect-SmRepository_cmdlet을 실행하여 리포지토리를 백업할 수 있습니다.

- 이 작업에 대한 정보 *

Protect-SmRepository_cmdlet은 다음 작업을 수행합니다.

- 리소스 그룹 및 정책을 생성합니다
- SnapCenter 리포지토리에 대한 백업 일정을 만듭니다
- 단계 *
  1. PowerShell을 실행합니다.
  2. SnapCenter 서버 호스트에서 _Open-SmConnection_cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
  3. _protect-SmRepository_cmdlet 및 필수 매개 변수를 사용하여 리포지토리를 백업합니다.

SnapCenter 리포지토리의 백업을 봅니다

get-SmrepositoryBackups_cmdlet을 실행하여 SnapCenter 서버 데이터베이스 저장소 백업 목록을 표시할 수 있습니다.

리포지토리 백업은 _protect-SmRepository_cmdlet에 지정된 일정에 따라 생성됩니다.

- 단계 *
  1. PowerShell을 실행합니다.
  2. 명령 프롬프트에서 다음 cmdlet을 입력한 다음 SnapCenter 서버에 연결할 자격 증명을 입력합니다.*Open - SMConnection*
  3. get-SmrepositoryBackups_cmdlet을 사용하여 사용 가능한 모든 SnapCenter 데이터베이스 백업을 나열합니다.

SnapCenter 데이터베이스 리포지토리를 복구합니다

_Restore-SmRepositoryBackup_cmdlet을 실행하여 SnapCenter 리포지토리를 복원할 수 있습니다.

SnapCenter 리포지토리를 복구하는 경우 복원 작업 중에 리포지토리 데이터베이스에 액세스할 수 없기 때문에 실행 중인 다른 SnapCenter 작업이 영향을 받습니다.

- 단계 *
  1. PowerShell을 실행합니다.
  2. 명령 프롬프트에서 다음 cmdlet을 입력한 다음 SnapCenter 서버에 연결할 자격 증명을 입력합니다.*Open - SMConnection*
  3. _Restore-SmRepositoryBackup_cmdlet을 사용하여 리포지토리 백업을 복원합니다.

다음 cmdlet은 iSCSI LUN 또는 VMDK에 있는 백업에서 SnapCenter MySQL 데이터베이스 리포지토리를 복구합니다.

```
C:\PS>Restore-SmRepositoryBackup -BackupName
MYSQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445
```

다음 cmdlet은 백업 파일이 iSCSI LUN에서 실수로 삭제되었을 때 SnapCenter MySQL 데이터베이스를 복원합니다. VMDK의 경우 ONTAP 스냅샷 복사본에서 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 리포지토리 백업을 검색할 때 리포지토리 복원 작업을 수행하는 데 사용된 백업이 표시되지 않습니다.

SnapCenter 리포지토리를 마이그레이션합니다

SnapCenter 서버 데이터베이스 리포지토리를 기본 위치에서 다른 디스크로 마이그레이션할 수 있습니다. 저장소를 더 많은 공간이 있는 디스크에 재배치하려면 리포지토리를 마이그레이션할 수 있습니다.

- 단계 *
  1. Windows에서 MYSQL57 서비스를 중지합니다.
  2. MySQL DATA 디렉토리를 찾습니다.

     일반적으로 C:\ProgramData\MySQL\MySQL Server 5.7\Data에서 데이터 디렉터리를 찾을 수 있습니다.
  3. MySQL data 디렉토리를 새 위치(예: E:\Data\NSM)로 복사합니다.
  4. 새 디렉터리를 마우스 오른쪽 단추로 클릭한 다음 * 속성 * > * 보안 * 을 선택하여 네트워크 서비스 로컬 서버 계정을 새 디렉터리에 추가한 다음 계정에 전체 권한을 할당합니다.
  5. 원래 데이터베이스 디렉토리의 이름을 NSM_copy와 같이 변경합니다.
  6. Windows 명령 프롬프트에서 _mklink_명령을 사용하여 심볼 디렉토리 링크를 생성합니다.

     ```
     "mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
     ```
  7. Windows에서 MYSQL57 서비스를 시작합니다.
  8. SnapCenter에 로그인하고 리포지토리 항목을 확인하거나 MySQL 유틸리티에 로그인하고 새 리포지토리에 연결하여 데이터베이스 위치 변경이 성공했는지 확인합니다.
  9. 이름이 변경된 원래 데이터베이스 리포지토리 디렉토리(NSM_copy)를 삭제합니다.

SnapCenter 리포지토리 암호를 재설정합니다

MySQL 서버 리포지토리 데이터베이스 암호는 SnapCenter 4.2에서 SnapCenter 서버를 설치하는 동안 자동으로 생성됩니다. SnapCenter 사용자는 이 자동 생성된 암호를 언제든지 알 수 없습니다. 리포지토리 데이터베이스에 액세스하려면 암호를 재설정해야 합니다.

시작하기 전에

비밀번호를 재설정하려면 SnapCenter 관리자 권한이 있어야 합니다.

- 단계 *

1. PowerShell을 실행합니다.
2. 명령 프롬프트에서 다음 명령을 입력한 다음 SnapCenter 서버에 연결할 자격 증명을 입력합니다._Open - SMConnection _
3. 리포지토리 암호 재설정: *Set-SmRepositoryPassword*

   다음 명령을 실행하면 리포지토리 암호가 재설정됩니다.

```
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 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

신뢰할 수 없는 도메인의 리소스를 관리합니다

AD(Active Directory) 신뢰할 수 있는 도메인의 호스트를 관리하는 것 외에도 SnapCenter는 신뢰할 수 없는 여러 AD 도메인의 호스트도 관리합니다. 신뢰할 수 없는 AD 도메인은 SnapCenter 서버에 등록되어 있어야 합니다. SnapCenter는 신뢰할 수 없는 여러 AD 도메인의 사용자 및 그룹을 지원합니다.

도메인 또는 작업 그룹에 있는 컴퓨터에 SnapCenter 서버를 설치할 수 있습니다. SnapCenter 서버를 설치하려면 시스템이 도메인에 있는 경우 도메인 자격 증명을 지정하거나, 컴퓨터가 작업 그룹에 있는 경우 로컬 관리자 자격 증명을 지정해야 합니다.

SnapCenter 서버에 등록되지 않은 도메인에 속하는 AD(Active Directory) 그룹은 지원되지 않습니다. 이러한 AD 그룹을 사용하여 SnapCenter 역할을 생성할 수 있지만 SnapCenter 서버에 로그인하는 데 실패하고 다음 오류 메시지가 표시됩니다. 로그인하려는 사용자가 역할에 속하지 않습니다. 관리자에게 문의하십시오.

신뢰할 수 없는 도메인을 수정합니다

도메인 컨트롤러 IP 주소 또는 FQDN(정규화된 도메인 이름)을 업데이트하려는 경우 신뢰할 수 없는 도메인을 수정할 수 있습니다.

- 이 작업에 대한 정보 *

FQDN을 수정한 후 연결된 자산(호스트, 사용자 및 그룹)이 예상대로 작동하지 않을 수 있습니다.

신뢰할 수 없는 도메인을 수정하려면 SnapCenter 사용자 인터페이스 또는 PowerShell cmdlet을 사용할 수 있습니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
  2. 설정 페이지에서 * 글로벌 설정 * 을 클릭합니다.
  3. 글로벌 설정 페이지에서 * 도메인 설정 * 을 클릭합니다.
  4. 을 클릭합니다  을 클릭한 후 다음 세부 정보를 제공합니다.

이 필드의 내용...	수행할 작업...
도메인 FQDN	FQDN을 지정하고 * Resolve * 를 클릭합니다.
도메인 컨트롤러 IP 주소입니다	도메인 FQDN을 확인할 수 없는 경우 하나 이상의 도메인 컨트롤러 IP 주소를 지정합니다.

  5. 확인 * 을 클릭합니다.

신뢰할 수 없는 **Active Directory** 도메인의 등록을 취소합니다

해당 도메인과 연결된 자산을 사용하지 않으려는 경우 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 대한 정보 *
- SnapCenter 서버에서 도메인을 등록 취소한 후에는 해당 도메인의 사용자가 SnapCenter 서버에 액세스할 수 없습니다.
- 연결된 자산(호스트, 사용자 및 그룹)이 있는 경우 도메인 등록을 취소하면 자산이 작동하지 않습니다.
- 신뢰할 수 없는 도메인의 등록을 취소하려면 SnapCenter 사용자 인터페이스 또는 PowerShell cmdlet을 사용합니다.
- 단계 *
  1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
  2. 설정 페이지에서 * 글로벌 설정 * 을 클릭합니다.
  3. 글로벌 설정 페이지에서 * 도메인 설정 * 을 클릭합니다.
  4. 도메인 목록에서 등록을 취소할 도메인을 선택합니다.
  5. 을 클릭합니다  를 클릭한 다음 * 확인 * 을 클릭합니다.

스토리지 시스템을 관리합니다

스토리지 시스템을 추가한 후 스토리지 시스템 구성 및 접속을 수정하거나 스토리지 시스템을

삭제할 수 있습니다.

스토리지 시스템 구성을 수정합니다

SnapCenter를 사용하여 사용자 이름, 암호, 플랫폼, 포트, 프로토콜 등을 변경하려는 경우 스토리지 시스템 구성을 수정할 수 있습니다. 제한 시간, 기본 IP 주소 또는 메시징 옵션.

- 이 작업에 대한 정보 *

개별 사용자 또는 그룹에 대한 스토리지 접속을 수정할 수 있습니다. 동일한 스토리지 시스템에 대한 사용 권한이 있는 하나 이상의 그룹에 속해 있는 경우 스토리지 접속 이름은 스토리지 시스템에 대한 사용 권한이 있는 각 그룹에 대해 한 번씩 스토리지 접속 목록에 여러 번 표시됩니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 스토리지 시스템 * 을 클릭합니다.
2. 스토리지 시스템 페이지의 * 유형 * 드롭다운에서 다음 작업 중 하나를 수행합니다.

선택...	단계...
ONTAP SVM	추가된 모든 SVM(스토리지 가상 시스템)을 확인하고 필요한 SVM 구성을 수정합니다. a. 스토리지 연결 페이지에서 적절한 SVM 이름을 클릭합니다. b. 다음 작업 중 하나를 수행합니다. ◦ SVM이 클러스터에 속하지 않는 경우 스토리지 시스템 수정 페이지에서 사용자 이름, 암호, EMS 및 AutoSupport 설정, 플랫폼, 프로토콜, 포트, 시간 초과 등의 구성을 수정합니다. 및 기본 IP를 선택합니다. ◦ SVM이 클러스터의 일부인 경우 Modify Storage System 페이지에서 * Manage SVM Independently * 를 선택하고 사용자 이름, 암호, EMS 및 AutoSupport 설정, 플랫폼, 프로토콜, 포트, 시간 초과 등의 구성을 수정합니다. 및 기본 IP를 선택합니다. SVM을 독립적으로 관리되도록 수정한 후 클러스터를 통해 관리하려는 경우 SVM을 삭제하고 * ReDiscover * 를 클릭해야 합니다. SVM이 ONTAP 클러스터에 추가됩니다. SnapCenter GUI에서 스토리지 시스템 암호를 업데이트할 경우 업데이트된 암호가 SMCore에 반영되지 않고 백업 작업이 실패하고 잘못된 자격 증명 오류가 발생하므로 해당 플러그인 또는 서버 호스트의 SMCore 서비스를 다시 시작해야 합니다.

선택...	단계...
ONTAP 클러스터	추가된 모든 클러스터를 확인하고 필요한 클러스터 구성을 수정합니다. a. 스토리지 접속 페이지에서 클러스터 이름을 클릭합니다. b. 스토리지 시스템 수정 페이지에서 사용자 이름 옆에 있는 편집 아이콘을 클릭하고 사용자 이름과 암호를 수정합니다. c. EMS 및 AutoSupport 설정을 선택하거나 지웁니다. d. 추가 옵션 * 을 클릭하고 플랫폼, 프로토콜, 포트, 시간 초과 및 기본 IP와 같은 다른 구성을 수정합니다.

3. 제출 * 을 클릭합니다.

스토리지 시스템을 삭제합니다

SnapCenter를 사용하여 사용하지 않는 스토리지 시스템을 삭제할 수 있습니다.

- 이 작업에 대한 정보 *

개별 사용자 또는 그룹의 스토리지 접속을 삭제할 수 있습니다. 동일한 스토리지 시스템에 대한 사용 권한이 있는 하나 이상의 그룹에 속해 있는 경우 스토리지 시스템 이름은 스토리지 시스템에 대한 사용 권한이 있는 각 그룹에 대해 한 번씩 스토리지 접속 목록에 여러 번 표시됩니다.

ⓘ 스토리지 시스템을 삭제하면 해당 스토리지 시스템에서 수행 중인 모든 작업이 실패합니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 스토리지 시스템 * 을 클릭합니다.
2. 스토리지 시스템 페이지의 * 유형 * 드롭다운에서 * ONTAP SVM * 또는 * ONTAP 클러스터 * 를 선택합니다.
3. 스토리지 연결 페이지에서 SVM 옆의 확인란을 선택하거나 삭제할 클러스터를 선택합니다.

   ⓘ 클러스터의 일부인 SVM은 선택할 수 없습니다.

4. 삭제 * 를 클릭합니다.
5. 스토리지 시스템 접속 설정 삭제 페이지에서 * 확인 * 을 클릭합니다.

   ⓘ ONTAP GUI를 사용하여 ONTAP 클러스터에서 SVM을 삭제한 경우, SnapCenter GUI에서 * 재발견 * 을 클릭하여 SVM 목록을 업데이트하십시오.

EMS Data 수집 관리

PowerShell cmdlet을 사용하여 EMS(Event Management System) 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 지정된 SVM(ONTAP Storage Virtual Machine)으로 전송하는 작업이 포함됩니다.

데이터 수집 작업이 진행 중인 경우 시스템 CPU 사용률이 높습니다. 데이터 크기와 관계없이 작업이 진행되는 동안에는 CPU 사용률이 계속 높습니다.

EMS 데이터 수집을 중지합니다

EMS 데이터 수집은 기본적으로 활성화되어 있으며 설치 날짜로부터 7일마다 실행됩니다. PowerShell cmdlet_Disable-SmDataCollectionEMS_를 사용하여 언제든지 데이터 수집을 비활성화할 수 있습니다.

- 단계 *
  1. PowerShell 명령줄에서 *Open-SmConnection* 을 입력하여 SnapCenter와 세션을 설정합니다.
  2. Disable-SmDataCollectionEms_를 입력하여 EMS 데이터 수집을 비활성화합니다.

EMS 데이터 수집을 시작합니다

EMS 데이터 수집은 기본적으로 활성화되어 있으며 설치 날짜로부터 7일마다 실행되도록 예약되어 있습니다. 이 기능을 사용하지 않도록 설정한 경우 _Enable-SmDataCollectionEMS_cmdlet을 사용하여 EMS 데이터 수집을 다시 시작할 수 있습니다.

Data ONTAP 이벤트 generate-autosupport-log 권한은 SVM(스토리지 가상 시스템) 사용자에게 부여되었습니다.

- 단계 *
  1. PowerShell 명령줄에서 *Open-SmConnection* 을 입력하여 SnapCenter와 세션을 설정합니다.
  2. Enable-SmDataCollectionEMS_를 입력하여 EMS 데이터 수집을 활성화합니다.

EMS Data 수집 일정 및 Target SVM 변경

PowerShell cmdlet을 사용하여 EMS 데이터 수집 스케줄 또는 대상 SVM(Storage Virtual Machine)을 변경할 수 있습니다.

- 단계 *
  1. PowerShell 명령줄에서 SnapCenter를 사용하여 세션을 설정하려면 _Open-SmConnection_cmdlet을 입력합니다.
  2. EMS 데이터 수집 대상을 변경하려면 _Set-SmDataCollectionEmsTarget_cmdlet을 입력합니다.
  3. EMS 데이터 수집 스케줄을 변경하려면 _Set-SmDataCollectionEmsSchedule_cmdlet을 입력합니다.

EMS Data 수집 상태 모니터링

여러 개의 PowerShell cmdlet을 사용하여 EMS 데이터 수집 상태를 모니터링할 수 있습니다. 일정, SVM(스토리지 가상 시스템) 타겟 및 상태에 대한 정보를 얻을 수 있습니다.

- 단계 *

1. PowerShell 명령줄에서 *Open-SmConnection* 을 입력하여 SnapCenter와 세션을 설정합니다.
2. get-SmDataCollectionEmsSchedule_을 입력하여 EMS 데이터 수집 스케줄에 대한 정보를 검색합니다.
3. _get-SmDataCollectionEmsStatus_를 입력하여 EMS 데이터 수집 상태에 대한 정보를 조회한다.
4. get-SmDataCollectionEmsTarget _ 을 입력하여 EMS 데이터 수집 대상에 대한 정보를 검색합니다.

관련 정보

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

SnapCenter 서버 및 플러그인 업그레이드

사용 가능한 업데이트를 확인하도록 SnapCenter를 구성합니다

SnapCenter은 주기적으로 NetApp Support 사이트와 통신하여 사용 가능한 소프트웨어 업데이트를 알려줍니다. 사용 가능한 업데이트에 대한 정보를 받을 간격을 지정하는 일정을 만들 수도 있습니다.

단계

1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
2. 설정 * 페이지에서 * 소프트웨어 * 를 클릭합니다.

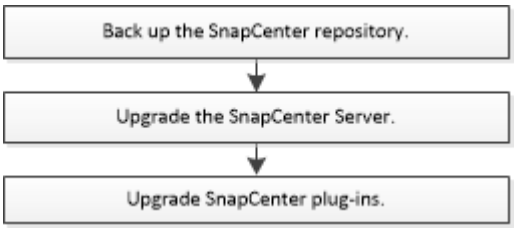
   사용 가능한 소프트웨어 페이지에는 사용 가능한 플러그인 패키지, 사용 가능한 버전 및 설치 상태가 표시됩니다.

3. 최신 버전의 플러그인 패키지를 사용할 수 있는지 확인하려면 * 업데이트 확인 * 을 클릭합니다.
4. 업데이트 예약 * 을 클릭하여 사용 가능한 업데이트에 대한 정보를 수신할 간격을 지정하는 일정을 만듭니다.
   a. 업데이트 확인 * 에서 간격을 선택합니다.
   b. SnapCenter 서버 관리자 Windows 자격 증명을 선택하고 * 확인 * 을 클릭합니다.

워크플로우 업그레이드

SnapCenter의 각 릴리즈에는 업데이트된 SnapCenter 서버 및 플러그인 패키지가 포함되어 있습니다. 플러그인 패키지 업데이트는 SnapCenter 설치 프로그램과 함께 배포됩니다. SnapCenter에서 사용 가능한 업데이트를 확인하도록 구성할 수 있습니다.

워크플로우는 SnapCenter 서버 및 플러그인 패키지를 업그레이드하는 데 필요한 여러 작업을 보여 줍니다.



지원되는 업그레이드 경로

SnapCenter 서버 버전을 사용 중인 경우…	**SnapCenter** 서버를 다음으로 직접 업그레이드할 수 있습니다.	지원되는 플러그인 버전입니다
4.6.x	4.7	• 4.6.x • 4.7
	4.8	• 4.8

SnapCenter 서버 버전을 사용 중인 경우...	**SnapCenter** 서버를 다음으로 직접 업그레이드할 수 있습니다.	지원되는 플러그인 버전입니다
4.7	4.8	• 4.7 • 4.8
	4.9	• 4.9
4.8	4.9	• 4.8 • 4.9

예를 들어 SnapCenter 버전 4.6.x를 사용 중인 경우 4.9로 업그레이드하려면 먼저 4.7로 업그레이드한 다음 4.9로 롤링 업그레이드를 수행해야 합니다.

VMware vSphere용 SnapCenter 플러그인 업그레이드에 대한 자세한 내용은 을 참조하십시오 "VMware vSphere용 SnapCenter 플러그인 업그레이드".

SnapCenter 서버를 업그레이드합니다

SnapCenter 서버 설치 관리자 실행 파일을 사용하여 SnapCenter 서버를 업그레이드할 수 있습니다.

시작하기 전에

- SnapCenter 서버 호스트는 Windows 업데이트와 함께 최신 버전이어야 하며, 보류 중인 시스템 재시작이 없어야 합니다.
- 업그레이드 작업을 시작하기 전에 실행 중인 다른 작업이 없는지 확인해야 합니다.
- 실행 중인 작업이 없는지 확인한 후 SnapCenter 리포지토리(MySQL) 데이터베이스를 백업해야 합니다. SnapCenter 서버 및 Exchange 플러그인을 업그레이드하기 전에 이 방법을 권장합니다.

  자세한 내용은 을 참조하십시오 "SnapCenter 리포지토리를 백업합니다".

- SnapCenter 서버 호스트 또는 플러그인 호스트에서 수정한 모든 SnapCenter 구성 파일을 백업해야 합니다.

  SnapCenter 구성 파일의 예: SnapDriveService.exe.config, SMCoreServiceHost.exe.config 등

이 작업에 대해

- 업그레이드 중에는 호스트가 예약된 작업을 실행하지 못하도록 유지 보수 모드로 자동 전환됩니다. 업그레이드 후 호스트가 자동으로 유지 보수 모드에서 해제됩니다.
- 업그레이드 중에 SQL 스크립트를 실행하여 NSM 데이터베이스에서 Exchange 데이터를 업데이트합니다. 그러면 DAG 및 호스트 단축 이름이 FQDN으로 변환됩니다. 이 기능은 Exchange 플러그인이 있는 SnapCenter 서버를 사용하는 경우에만 적용됩니다.
- 업그레이드 작업을 시작하기 전에 호스트를 유지 관리 모드로 수동으로 배치한 경우 업그레이드 후 * 호스트 * > * 스케줄 활성화 * 를 클릭하여 호스트를 유지 관리 모드에서 수동으로 해제해야 합니다.
- Microsoft SQL Server용 SnapCenter 플러그인, Microsoft Exchange Server용 SnapCenter 플러그인 및

Microsoft Windows용 SnapCenter 플러그인의 경우, 실행할 scripts_path의 서버 및 플러그인 호스트를 4.7 버전으로 업그레이드하는 것이 좋습니다.

정책에서 predpts 및 postscript가 활성화된 기존 백업 및 검증 스케줄의 경우 업그레이드 후에도 백업 작업이 계속 작동합니다.

Job details * 페이지에서 스크립트를 scripts_path에 복사하고 정책을 편집하여 scripts_path와 관련된 경로를 제공하는 것이 좋습니다. 클론 수명주기 작업의 경우 하위 작업 레벨에 경고 메시지가 표시됩니다.

단계

1. NetApp Support 사이트에서 SnapCenter 서버 설치 패키지를 다운로드하십시오.

   https://mysupport.netapp.com/site/products/all/details/snapcenter/downloads-tab

2. C:\Program Files\NetApp\SnapCenter WebApp에 있는 web.config의 복사본을 생성합니다.
3. Windows 작업 스케줄에서 플러그인 호스트와 관련된 SnapCenter 스케줄을 내보내면 업그레이드에 실패할 경우 이를 사용하여 스케줄을 복구할 수 있습니다.

   ```
   md d:\\SCBackup``schtasks /query /xml /TN taskname >>
   "D:\SCBackup\taskname.xml"
   ```

4. 리포지토리 백업이 구성되지 않은 경우 SnapCenter MySQL 데이터베이스 덤프를 생성합니다.

   ```
   md d:\\SCBackup``mysqldump --all-databases --single-transaction --add-drop
   -database --triggers --routines --events -u root -p >
   D:\SCBackup\SCRepoBackup.dmp
   ```

   메시지가 표시되면 암호를 입력합니다.

5. 다운로드한 .exe 파일을 두 번 클릭하여 SnapCenter 서버 업그레이드를 시작합니다.

   업그레이드를 시작하면 모든 사전 점검을 수행하고, 최소 요구사항을 충족하지 않을 경우 적절한 오류 또는 경고 메시지가 표시됩니다. 경고 메시지를 무시하고 설치를 계속할 수 있습니다. 그러나 오류는 수정해야 합니다.

   SnapCenter는 이전 버전의 SnapCenter Server 설치 중에 제공된 기존 MySQL Server 리포지토리 데이터베이스 암호를 계속 사용합니다.

6. 업그레이드 * 를 클릭합니다.

   어느 단계에서든 * 취소 * 버튼을 클릭하면 업그레이드 워크플로우가 취소됩니다. SnapCenter 서버를 이전 상태로 롤백하지 않습니다.

   모범 사례: 로그아웃한 다음 SnapCenter에 로그인하거나, 닫은 다음 새 브라우저를 열어 SnapCenter GUI에 액세스해야 합니다.

작업을 마친 후

- sudo 사용자를 사용하여 플러그인을 설치하는 경우 _C:\ProgramData\NetApp\SnapCenter\Package Repository\Oracle_checksum.txt_에서 사용할 수 있는 sha224 키를 복사하여 _/etc/sudoers_file을 업데이트해야 합니다.

- 호스트에서 리소스를 새로 검색해야 합니다.

  호스트 상태가 중지됨 으로 표시되면 잠시 기다린 후 새 검색을 수행할 수 있습니다. HostRefreshInterval* 매개 변수 값(기본값은 3600초)을 10분 이상의 값으로 변경할 수도 있습니다.

- 업그레이드에 실패하면 실패한 설치를 정리하여 이전 버전의 SnapCenter를 다시 설치한 다음 NSM 데이터베이스를 이전 상태로 복원해야 합니다.
- SnapCenter 서버 호스트를 업그레이드한 후 스토리지 시스템을 추가하기 전에 플러그인도 업그레이드해야 합니다.

플러그인 패키지를 업그레이드합니다

플러그인 패키지는 SnapCenter 업그레이드의 일부로 배포됩니다.

업그레이드 절차에서는 Windows, Linux 또는 AIX 호스트를 "유지 관리" 모드로 전환하여 호스트가 예약된 작업을 실행하지 못하도록 합니다.

시작하기 전에

- Linux 시스템에 액세스할 수 있는 루트가 아닌 사용자인 경우 업그레이드 작업을 수행하기 전에 _/etc/sudoers_file을 최신 체크섬 값으로 업데이트해야 합니다.
- 기본적으로 SnapCenter는 환경에서 java_home을 감지합니다. 고정 java_home을 사용하고 Linux 호스트에서 플러그인을 업그레이드하는 경우 */var/opt/snapcenter/spl/etc/_*에 있는 *_spl.properties* 파일에 skip_jAVAHOME_update 매개 변수를 수동으로 추가하고 값을 true 로 설정해야 합니다.

  플러그인이 업그레이드되거나 SnapCenter 플러그인 로더(SPL) 서비스가 다시 시작되면 java_home의 값이 업데이트됩니다. SPL을 업그레이드하거나 다시 시작하기 전에 skip_jAVAHOME_update 매개 변수를 추가하고 값을 true 로 설정하면 java_home 값이 업데이트되지 않습니다.

- SnapCenter 서버 호스트 또는 플러그인 호스트에서 수정한 모든 SnapCenter 구성 파일을 백업해야 합니다.

  SnapCenter 구성 파일의 예: SnapDriveService.exe.config, SMCoreServiceHost.exe.config 등

이 작업에 대해

- 업그레이드 절차에서는 Windows, Linux 또는 AIX 호스트를 "유지 관리" 모드로 전환하여 호스트가 예약된 작업을 실행하지 못하도록 합니다.
- Microsoft SQL Server용 SnapCenter 플러그인, Microsoft Exchange Server용 SnapCenter 플러그인 및 Microsoft Windows용 SnapCenter 플러그인의 경우 실행할 scripts_path의 최신 버전으로 서버와 플러그인 호스트를 모두 업그레이드하는 것이 좋습니다.

  정책에서 predpts 및 postscript가 활성화된 기존 백업 및 검증 스케줄의 경우 업그레이드 후에도 백업 작업이 계속 작동합니다.

  Job details * 페이지에서 스크립트를 scripts_path에 복사하고 정책을 편집하여 scripts_path와 관련된 경로를 제공하는 것이 좋습니다. 클론 수명주기 작업의 경우 하위 작업 레벨에 경고 메시지가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 * 호스트 * > * 관리 호스트 * 를 클릭합니다.
2. 다음 작업 중 하나를 수행하여 호스트를 업그레이드합니다.

- 호스트 중 하나에 대해 전체 상태 열에 ""업그레이드 가능""이 표시되면 호스트 이름을 클릭하고 다음을 수행합니다.

  i. 추가 옵션 * 을 클릭합니다.

  ii. 호스트가 플러그인을 업그레이드하는 데 필요한 요구사항을 충족하는지 확인하지 않으려면 * 사전 검사 건너뛰기 * 를 선택합니다.

  iii. 업그레이드 * 를 클릭합니다.

- 여러 호스트를 업그레이드하려면 모든 호스트를 선택하고 을 클릭합니다  를 클릭한 다음 * 업그레이드 * > * 확인 * 을 클릭합니다.

  플러그인 업그레이드 중에 모든 관련 서비스가 다시 시작됩니다.

  패키지의 모든 플러그인이 선택되지만 이전 버전의 SnapCenter와 함께 설치된 플러그인만 업그레이드되고 나머지 플러그인은 설치되지 않습니다. 새 플러그인을 설치하려면 * 플러그인 추가 * 옵션을 사용해야 합니다.

  사전 검사 건너뛰기 * 확인란을 선택하지 않은 경우 호스트가 플러그인을 설치하는 데 필요한 요구 사항을 충족하는지 여부를 확인합니다. 최소 요구 사항이 충족되지 않으면 적절한 오류 또는 경고 메시지가 표시됩니다. 문제를 해결한 후 * 업그레이드 * 를 클릭합니다.

  오류가 디스크 공간 또는 RAM과 관련된 경우 C:\Program Files\NetApp\SnapCenter WebApp에 있는 web.config 또는 C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SnapCenter\에 있는 PowerShell config 파일을 업데이트하여 기본값을 수정할 수 있습니다. 오류가 나머지 매개변수와 관련된 경우 문제를 해결한 다음 요구 사항을 다시 확인해야 합니다.

SnapCenter 서버 및 플러그인을 제거합니다

SnapCenter 플러그인 패키지를 제거합니다

호스트 제거를 위한 사전 요구 사항

SnapCenter GUI를 사용하여 호스트를 제거하고 개별 플러그인 또는 플러그인 패키지를 제거할 수 있습니다. 또한 SnapCenter 서버 호스트의 CLI(명령줄 인터페이스)를 사용하거나 Windows*에서 로컬로 프로그램 제거* 옵션을 사용하여 원격 호스트에서 개별 플러그인 또는 플러그인 패키지를 제거할 수 있습니다.

SnapCenter 서버에서 호스트를 제거하기 전에 사전 요구 사항을 완료해야 합니다.

- 관리자로 로그인해야 합니다.
- SnapCenter 사용자 지정 플러그인을 사용하는 경우 호스트와 연결된 SnapCenter에서 모든 클론을 삭제해야 합니다.
- 검색 작업이 호스트에서 실행되고 있지 않은지 확인해야 합니다.
- 호스트와 연결된 모든 객체를 제거하는 데 필요한 권한이 있는 역할이 할당되어야 합니다. 그렇지 않으면 제거 작업이 실패합니다.
- SnapCenter에 호스트를 추가한 후 SSH 키가 수정된 경우 지문을 확인해야 합니다.
- SnapCenter 호스트가 최신 버전의 SnapCenter로 업그레이드되었지만 플러그인 호스트가 여전히 이전 버전의 플러그인을 실행 중인 경우 지문을 확인해야 합니다.

역할 기반 액세스 제어를 사용하여 호스트를 제거하기 위한 사전 요구 사항

- 읽기, 호스트 삭제, 설치, 플러그인 제거 및 개체 삭제 권한이 있는 RBAC 역할을 사용하여 로그인해야 합니다.

  객체는 클론, 백업, 리소스 그룹, 스토리지 시스템 등이 될 수 있습니다.

- RBAC 역할에 RBAC 사용자를 추가해야 합니다.
- 삭제할 호스트, 플러그인, 자격 증명, 리소스 그룹 및 스토리지 시스템(클론용)에 RBAC 사용자를 할당해야 합니다.
- SnapCenter를 RBAC 사용자로 로그인해야 합니다.

사전 요구 사항 **-** 클론 수명주기 작업에서 생성된 클론이 있는 호스트를 제거합니다

- SQL 데이터베이스의 클론 라이프사이클 관리를 사용하여 클론 작업을 생성해야 합니다.
- 클론 읽기 및 삭제, 리소스 읽기 및 삭제, 리소스 그룹 읽기 및 삭제, 스토리지 읽기 및 삭제, 읽기 및 삭제 프로비저닝, 마운트, 마운트 해제, 플러그인 설치 및 제거, 호스트 읽기 및 삭제 권한이 있는 RBAC 역할을 만들어야 합니다.
- RBAC 사용자를 RBAC 역할에 할당해야 합니다.
- RBAC 사용자를 호스트, Microsoft SQL Server용 SnapCenter 플러그인, 자격 증명, 클론 라이프사이클 리소스 그룹 및 스토리지 시스템에 할당해야 합니다.
- SnapCenter를 RBAC 사용자로 로그인해야 합니다.

VMware vSphere용 SnapCenter 플러그인 제거에 대한 자세한 내용은 을 참조하십시오 "VMware vSphere용 SnapCenter 플러그인을 제거합니다".

호스트를 제거합니다

SnapCenter 서버가 호스트를 제거하면 먼저 SnapCenter 리소스 페이지에서 해당 호스트에 대해 나열된 백업, 클론, 클론 작업, 리소스 그룹 및 리소스를 제거한 다음 호스트에서 플러그인 패키지를 제거합니다.

이 작업에 대해

- 호스트를 삭제하면 호스트와 연결된 백업, 클론 및 리소스 그룹도 삭제됩니다.
- 리소스 그룹을 제거하면 연결된 모든 스케줄도 제거됩니다.
- 호스트에 다른 호스트와 공유되는 리소스 그룹이 있고 호스트를 삭제하는 경우 리소스 그룹도 삭제됩니다.
- 사용 중단되거나 연결할 수 없는 플러그인 호스트를 제거하려면 _Remove-SmHost_cmdlet을 사용해야 합니다.

  cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드"

- 호스트를 제거하는 데 필요한 시간은 백업 수와 보존 설정에 따라 달라집니다. 이는 각 컨트롤러에서 스냅샷 복사본이 삭제되고 메타데이터가 정리되기 때문입니다.

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. Hosts * 페이지에서 * Managed Hosts * 를 클릭합니다.
3. 제거할 호스트를 선택한 다음 * 제거 * 를 클릭합니다.
4. Oracle RAC 클러스터의 경우 클러스터의 모든 호스트에서 SnapCenter 소프트웨어를 제거하려면 * 클러스터의 모든 호스트 포함 * 을 선택합니다.

   또한 클러스터의 노드 하나를 제거하여 모든 노드를 하나씩 제거할 수도 있습니다.

5. 확인 * 을 클릭합니다.

> 클러스터에서 호스트 플러그인을 제거하고 다시 설치하면 클러스터 리소스가 자동으로 검색되지 않습니다. 클러스터 호스트 이름을 선택한 다음 * 리소스 새로 고침 * 을 클릭하여 클러스터 리소스를 자동으로 검색합니다.

SnapCenter GUI를 사용하여 플러그인을 제거합니다

개별 플러그인 또는 플러그인 패키지가 더 이상 필요하지 않다고 결정한 경우 SnapCenter 인터페이스를 사용하여 제거할 수 있습니다.

시작하기 전에

- 제거할 플러그인 패키지의 리소스 그룹을 제거해야 합니다.
- 제거할 플러그인 패키지의 리소스 그룹과 연결된 정책을 분리해야 합니다.

이 작업에 대해

개별 플러그인을 제거할 수 있습니다. 예를 들어, 호스트에 리소스가 부족하고 해당 플러그인을 보다 강력한 호스트로 이동하려고 하기 때문에 Microsoft SQL Server용 SnapCenter 플러그인을 제거해야 할 수 있습니다. 전체 플러그인 패키지를 제거할 수도 있습니다. 예를 들어, Oracle 데이터베이스용 SnapCenter 플러그인 및 UNIX용 SnapCenter 플러그인이 포함된 Linux용 SnapCenter 플러그인 패키지를 제거해야 할 수 있습니다.

- 호스트 제거에는 모든 플러그인이 제거됩니다.

  SnapCenter에서 호스트를 제거하면 SnapCenter는 호스트를 제거하기 전에 호스트에 있는 모든 플러그인 패키지를 제거합니다.

- SnapCenter GUI는 한 번에 하나의 호스트에서 플러그인을 제거합니다.

  SnapCenter GUI를 사용하는 경우 한 번에 하나의 호스트에서만 플러그인을 제거할 수 있습니다. 그러나 여러 제거 작업을 동시에 실행할 수 있습니다.

  또한 _Uninstall-SmHostPackage_cmdlet 및 필수 매개 변수를 사용하여 여러 호스트에서 플러그인을 제거할 수도 있습니다. cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 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 않은 경우가 아니면 Windows용 SnapCenter 플러그인 패키지를 제거하지 마십시오.

단계

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 호스트 페이지에서 * 관리되는 호스트 * 를 클릭합니다.
3. 관리 호스트 페이지에서 플러그인 또는 플러그인 패키지를 제거할 호스트를 선택합니다.
4. 제거하려는 플러그인 옆에 있는 * 제거 * > * 제출 * 을 클릭합니다.

작업을 마친 후

해당 호스트에 플러그인을 다시 설치하기 전에 5분 정도 기다려야 합니다. 이 기간은 SnapCenter GUI가 관리 대상 호스트의 상태를 새로 고칠 수 있을 정도로 충분합니다. 플러그인을 즉시 재설치하면 설치가 실패합니다.

Linux용 SnapCenter 플러그인 패키지를 제거하는 경우 설치 제거별 로그 파일은 _/custom_location/snapcenter/log_에서 사용할 수 있습니다.

PowerShell cmdlet을 사용하여 Windows 플러그인을 제거합니다

SnapCenter 서버 호스트 명령줄 인터페이스의 _Uninstall-SmHostPackage_cmdlet을 사용하여 하나 이상의 호스트에서 개별 플러그인을 제거하거나 플러그인 패키지를 제거할 수 있습니다.

플러그인을 제거할 각 호스트에 대한 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter에 로그인해야 합니다.

단계

1. PowerShell을 실행합니다.

2. SnapCenter 서버 호스트에서:_Open-SMConnection-SMSbaseUrl https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME_ 명령을 입력한 다음 자격 증명을 입력합니다.
3. _Uninstall-SmHostPackage_cmdlet 및 필수 매개 변수를 사용하여 Windows 플러그인을 제거합니다.

   cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

호스트에서 플러그인을 로컬로 제거합니다

SnapCenter 서버에서 호스트에 연결할 수 없는 경우 호스트에서 SnapCenter 플러그인을 로컬로 제거할 수 있습니다.

이 작업에 대해

개별 플러그인 또는 플러그인 패키지를 제거하는 가장 좋은 방법은 SnapCenter GUI를 사용하거나 SnapCenter 서버 호스트 명령줄 인터페이스에서 Uninstall-SmHostPackage cmdlet을 사용하는 것입니다. 이러한 절차는 SnapCenter 서버가 변경 사항을 최신 상태로 유지하는 데 도움이 됩니다.

그러나 플러그인을 로컬로 제거해야 하는 경우는 드뭅니다. 예를 들어 SnapCenter 서버에서 제거 작업을 실행했지만 작업이 실패했거나 SnapCenter 서버를 제거했거나 분리된 플러그인은 호스트에 남아 있을 수 있습니다.

ⓘ 호스트에서 플러그인 패키지를 로컬로 제거해도 호스트와 연결된 데이터(예: 예약된 작업 및 백업 메타데이터)는 삭제되지 않습니다.

ⓘ 제어판에서 Windows용 SnapCenter 플러그인 패키지를 로컬로 제거하지 마십시오. SnapCenter GUI를 사용하여 Microsoft Windows용 SnapCenter 플러그인이 제대로 제거되었는지 확인해야 합니다.

단계

1. 호스트 시스템에서 제어판 으로 이동하여 * 프로그램 제거 * 를 클릭합니다.
2. 프로그램 목록에서 제거할 SnapCenter 플러그인 또는 플러그인 패키지를 선택하고 * 제거 * 를 클릭합니다.

   Windows가 선택한 패키지의 모든 플러그인을 제거합니다.

CLI를 사용하여 Linux 또는 AIX용 플러그인 패키지를 제거합니다

명령줄 인터페이스를 사용하여 Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지를 제거할 수 있습니다.

시작하기 전에

- 예약된 작업을 삭제했는지 확인합니다
- 실행 중인 모든 작업이 완료되었는지 확인합니다.

단계

설치 제거하려면 _/custom_location/NetApp/snapcenter/SPL/installation/plugins/uninstall_을 실행합니다.

SnapCenter 서버를 제거합니다

SnapCenter 서버를 사용하여 데이터 보호 작업을 더 이상 관리하지 않으려는 경우 SnapCenter 서버 호스트의 프로그램 및 기능 제어판을 사용하여 SnapCenter 서버를 제거할 수 있습니다. SnapCenter 서버를 제거하면 해당 구성 요소가 모두 제거됩니다.

시작하기 전에

- SnapCenter 서버가 설치된 드라이브에 2GB 이상의 여유 공간이 있는지 확인합니다.
- SnapCenter 서버가 설치된 도메인이 제거되지 않았는지 확인합니다.

  SnapCenter 서버가 설치된 도메인을 제거한 다음 제거를 시도하면 작업이 실패합니다.

- 리포지토리 데이터베이스가 정리 및 제거되므로 리포지토리 데이터베이스를 백업해야 합니다.

단계

1. SnapCenter 서버 호스트에서 제어판으로 이동합니다.
2. 범주 * 보기에 있는지 확인합니다.
3. 프로그램에서 * 프로그램 제거 * 를 클릭합니다.

   프로그램 및 기능 창이 열립니다.

4. NetApp SnapCenter 서버를 선택한 다음 * 제거 * 를 클릭합니다.

   SnapCenter 4.2에서 SnapCenter 서버를 제거하면 MySQL Server 리포지토리 데이터베이스를 포함한 모든 구성 요소가 제거됩니다.

   - NLB 클러스터에서 NLB 노드를 제거하려면 SnapCenter 서버 호스트를 다시 시작해야 합니다. 호스트를 다시 시작하지 않으면 SnapCenter 서버를 다시 설치하려고 할 때 오류가 발생할 수 있습니다.
   - 제거하는 동안 제거되지 않은 .NET Framework를 수동으로 제거해야 합니다.

REST API를 사용하여 자동화

REST API 개요

REST API를 사용하여 몇 가지 SnapCenter 관리 작업을 수행할 수 있습니다. REST API는 Swagger 웹 페이지를 통해 표시됩니다.

Swagger 웹 페이지는 _\https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/_에서 사용할 수 있으며 REST API 설명서를 표시하고 API 호출을 수동으로 실행할 수 있습니다.

REST API를 지원하는 플러그인은 다음과 같습니다.

- Microsoft SQL Server용 플러그인
- SAP HANA 데이터베이스용 플러그인
- 맞춤형 플러그인
- Oracle 데이터베이스용 플러그인

SnapCenter REST API에 기본적으로 액세스하는 방법

REST 클라이언트를 지원하는 모든 프로그래밍 언어를 사용하여 SnapCenter REST API에 직접 액세스할 수 있습니다. Python, PowerShell, Java 등 다양한 언어가 제공됩니다.

REST 웹 서비스 기반

REST(Representational State Transfer)는 분산된 웹 애플리케이션을 만드는 스타일입니다. 웹 서비스 API 설계에 적용할 경우 서버 기반 리소스를 노출하고 상태를 관리하기 위한 일련의 기술과 Best Practice를 수립합니다. 이 솔루션은 메인스트림 프로토콜과 표준을 사용하여 SnapCenter 관리를 위한 유연한 기반을 제공합니다.

리소스 및 상태 표시

리소스는 웹 기반 시스템의 기본 구성 요소입니다. REST 웹 서비스 응용 프로그램을 만들 때 초기 설계 작업은 다음과 같습니다.

시스템 또는 서버 기반 리소스 식별

모든 시스템은 리소스를 사용하고 유지합니다. 리소스는 파일, 비즈니스 트랜잭션, 프로세스 또는 관리 엔티티가 될 수 있습니다. REST 웹 서비스를 기반으로 애플리케이션을 설계하는 첫 번째 작업 중 하나는 리소스를 식별하는 것입니다.

자원 상태 및 연관된 상태 작업의 정의

리소스는 항상 한정된 수의 상태 중 하나에 있습니다. 상태 변경에 영향을 주는 데 사용되는 상태 및 관련 작업을 명확하게 정의해야 합니다.

URI 끝점

모든 REST 리소스는 잘 정의된 주소 지정 체계를 사용하여 정의되고 사용 가능해야 합니다. 리소스가 있고 식별된 끝점은 URI(Uniform Resource Identifier)를 사용합니다.

URI는 네트워크의 각 리소스에 대해 고유한 이름을 만들기 위한 일반 프레임워크를 제공합니다. URL(Uniform Resource Locator)은 리소스를 식별하고 액세스하기 위해 웹 서비스와 함께 사용되는 URI 유형입니다. 일반적으로 리소스는 파일 디렉터리와 비슷한 계층적 구조로 표시됩니다.

HTTP 메시지

HTTP(Hypertext Transfer Protocol)는 웹 서비스 클라이언트 및 서버가 리소스에 대한 요청 및 응답 메시지를 교환하기 위해 사용하는 프로토콜입니다.

웹 서비스 응용 프로그램 설계의 일환으로 HTTP 메서드는 리소스 및 해당 상태 관리 작업에 매핑됩니다. HTTP는 상태 비저장 입니다. 따라서 관련 요청 및 응답 집합을 하나의 트랜잭션으로 연결하려면 요청 및 응답 데이터 플로우와 함께 전달된 HTTP 헤더에 추가 정보가 포함되어야 합니다.

JSON 형식

정보는 여러 가지 방법으로 웹 서비스 클라이언트와 서버 간에 구조화되고 전송될 수 있지만 가장 일반적인 옵션은 JSON(JavaScript Object Notation)입니다.

JSON은 단순 데이터 구조를 일반 텍스트로 나타내는 업계 표준이며 리소스를 설명하는 상태 정보를 전송하는 데 사용됩니다. SnapCenter REST API는 JSON을 사용하여 각 HTTP 요청 및 응답의 본문으로 전송되는 데이터를 포맷합니다.

기본 작동 특성

REST는 일반적인 기술과 모범 사례를 설정하지만 각 API의 세부 사항은 설계 선택에 따라 달라질 수 있습니다.

요청 및 응답 API 트랜잭션

모든 REST API 호출은 클라이언트에 대한 관련 응답을 생성하는 SnapCenter 서버 시스템에 대한 HTTP 요청으로 수행됩니다. 이 요청 및 응답 쌍은 API 트랜잭션으로 간주됩니다.

API를 사용하기 전에 요청 및 응답 출력의 내용을 제어하는 데 사용할 수 있는 입력 변수에 대해 잘 알고 있어야 합니다.

CRUD 작업 지원

SnapCenter REST API를 통해 사용 가능한 각 리소스는 CRUD 모델을 기반으로 액세스됩니다.

- 생성
- 읽기
- 업데이트
- 삭제

일부 리소스의 경우 일부 작업만 지원됩니다.

오브젝트 식별자

각 리소스 인스턴스 또는 개체는 만들 때 고유한 식별자가 할당됩니다. 대부분의 경우 식별자는 128비트 UUID입니다. 이러한 식별자는 특정 SnapCenter 서버 내에서 전역적으로 고유합니다.

새 개체 인스턴스를 만드는 API 호출을 실행하면 연결된 ID가 있는 URL이 HTTP 응답의 위치 헤더에 있는 호출자에게 반환됩니다. 식별자를 추출하여 리소스 인스턴스를 참조할 때 후속 호출에 사용할 수 있습니다.

개체 식별자의 내용 및 내부 구조는 언제든지 변경할 수 있습니다. 관련 객체를 참조할 때는 필요한 경우 해당 API 호출에서만 식별자를 사용해야 합니다.

개체 인스턴스 및 컬렉션

API 호출은 리소스 경로 및 HTTP 메서드에 따라 특정 개체 인스턴스 또는 개체 컬렉션에 적용될 수 있습니다.

동기 및 비동기 작업

SnapCenter는 클라이언트로부터 받은 HTTP 요청을 동기적 또는 비동기적으로 수행합니다.

동기 처리

SnapCenter는 요청을 즉시 수행하고 HTTP 상태 코드가 200 또는 201인 경우 응답한다.

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 SnapCenter는 요청을 처리하기 위한 백그라운드 작업과 작업을 고정하기 위한 작업 개체를 만듭니다. HTTP 상태 코드 202가 작업 객체와 함께 호출자에게 반환됩니다. 작업의 상태를 검색하여 성공 또는 실패를 결정해야 합니다.

POST 및 DELETE 메서드를 사용하는 요청은 완료하는 데 2초 이상 걸릴 것으로 예상되는 경우 비동기적으로 실행되도록 설계되었습니다.

보안

REST API와 함께 제공되는 보안은 주로 SnapCenter에서 사용할 수 있는 기존 보안 기능을 기반으로 합니다. 다음 보안은 API에서 사용됩니다.

전송 계층 보안

SnapCenter 서버와 클라이언트 사이에서 네트워크를 통해 전송되는 모든 트래픽은 일반적으로 SnapCenter 구성 설정에 따라 TLS를 사용하여 암호화됩니다.

HTTP 인증

HTTP 수준에서는 API 트랜잭션에 기본 인증이 사용됩니다. base64 문자열에 사용자 이름과 암호가 있는 HTTP 헤더가 각 요청에 추가됩니다.

API 요청을 제어하는 입력 변수입니다

HTTP 요청에 설정된 매개 변수와 변수를 통해 API 호출이 처리되는 방식을 제어할 수 있습니다.

HTTP 메서드

SnapCenter REST API에서 지원하는 HTTP 메서드는 다음 표에 나와 있습니다.

모든 HTTP 메서드를 각 REST 끝점에서 사용할 수 있는 것은 아닙니다.

HTTP 메소드	설명
가져오기	리소스 인스턴스 또는 컬렉션의 개체 속성을 검색합니다.
게시	제공된 입력을 기반으로 새 리소스 인스턴스를 만듭니다.
삭제	기존 리소스 인스턴스를 삭제합니다.
를 누릅니다	기존 리소스 인스턴스를 수정합니다.

요청 헤더

HTTP 요청에 여러 헤더를 포함해야 합니다.

콘텐츠 유형

요청 본문에 JSON이 포함된 경우 이 헤더를 _application/json_으로 설정해야 합니다.

수락

이 헤더는 _application/json_으로 설정해야 합니다.

권한 부여

기본 인증은 base64 문자열로 인코딩된 사용자 이름과 암호로 설정되어야 합니다.

요청 본문

요청 본문의 내용은 특정 호출에 따라 달라집니다. HTTP 요청 본문은 다음 중 하나로 구성됩니다.

- 입력 변수가 있는 JSON 개체입니다
- 비어 있습니다

오브젝트 필터링

Get을 사용하는 API 호출을 실행할 때 모든 특성에 따라 반환된 객체를 제한하거나 필터링할 수 있습니다. 예를 들어, 다음과 같이 정확하게 일치하는 값을 지정할 수 있습니다.

```
<field>=<query value>
```

정확한 일치 항목 외에도 다른 연산자를 사용하여 값 범위에 있는 개체 집합을 반환할 수 있습니다. SnapCenter REST API는 아래 표에 나와 있는 필터링 연산자를 지원합니다.

운영자	설명
=	같음
를 누릅니다	보다 작음
를 누릅니다	보다 큼
lt;=.(&L	보다 작거나 같음
GT;=.(&T	보다 크거나 같음
업데이트	또는
!	같지 않음
*	greedy 와일드카드

쿼리의 일부로 * null * 키워드 또는 해당 부정 *!null * 을 사용하여 특정 필드가 설정되었는지 여부를 기준으로 개체 컬렉션을 반환할 수도 있습니다.

설정되지 않은 필드는 일반적으로 일치하는 쿼리에서 제외됩니다.

특정 객체 필드를 요청하는 중입니다

기본적으로 Get 을 사용하여 API 호출을 실행하면 개체나 개체를 고유하게 식별하는 특성만 반환됩니다. 이 최소 필드 집합은 각 개체의 키 역할을 하며 개체 유형에 따라 달라집니다. 를 사용하여 추가 개체 속성을 선택할 수 있습니다 `fields` 쿼리 매개 변수는 다음과 같은 방식으로 지정합니다.

공통 또는 표준 필드

가장 일반적으로 사용되는 개체 필드를 검색하려면 * fields=** 를 지정합니다. 이러한 필드는 일반적으로 로컬 서버 메모리에 유지되거나 액세스에 필요한 처리가 거의 필요하지 않습니다. 이 속성은 URL 경로 키(UUID)로 GET을 사용한 후 개체에 대해 반환되는 속성과 동일합니다.

모든 필드

액세스 시 추가 서버 처리가 필요한 필드를 포함하여 모든 오브젝트 필드를 검색하려면 * fields = * 를 지정합니다.

사용자 정의 필드 선택

필드=<field_name>* 를 사용하여 원하는 필드를 정확하게 지정합니다. 여러 필드를 요청할 때는 공백 없이 쉼표를 사용하여 값을 구분해야 합니다.

가장 좋은 방법은 항상 원하는 특정 필드를 식별하는 것입니다. 필요한 경우 공통 필드 또는 모든 필드 집합만 검색해야 합니다. 공통으로 분류되어 _ FACTORS= * _ 로 반환되는 필드는 내부 성능 분석에 따라 NetApp에서 결정합니다. 필드의 분류는 향후 릴리스에서 변경될 수 있습니다.

출력 집합에서 오브젝트 정렬

리소스 컬렉션의 레코드는 개체에서 정의한 기본 순서로 반환됩니다. 를 사용하여 순서를 변경할 수 있습니다

`order_by` 다음과 같이 필드 이름 및 정렬 방향을 가진 쿼리 매개 변수:

```
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 지정하지만 방향을 지정하지 않으면 값이 오름차순으로 정렬됩니다.
- 여러 매개 변수를 포함할 때는 필드를 쉼표로 구분해야 합니다.

컬렉션의 개체를 검색할 때 페이지 매김

Get 을 사용하여 API 호출을 실행하여 같은 형식의 개체 컬렉션에 액세스하면 SnapCenter 는 두 가지 제약 조건에 따라 가능한 한 많은 개체를 반환합니다. 요청에 대한 추가 쿼리 매개 변수를 사용하여 이러한 각 제약 조건을 제어할 수 있습니다. 특정 GET 요청에 대한 첫 번째 제약 조건에 도달하면 요청이 종료되고 반환된 레코드 수가 제한됩니다.

모든 개체를 반복하기 전에 요청이 종료되면 응답에는 다음 레코드 배치를 검색하는 데 필요한 링크가 포함됩니다.

개체 수 제한

기본적으로 SnapCenter 는 GET 요청에 대해 최대 10,000개의 오브젝트를 반환합니다. 이 제한은 _max_records_query 매개 변수를 사용하여 변경할 수 있습니다. 예를 들면 다음과 같습니다.

```
max_records=20
```

실제로 반환되는 개체 수는 관련 시간 제약 조건 및 시스템의 총 개체 수에 따라 실제 최대값보다 작을 수 있습니다.

객체를 검색하는 데 사용되는 시간 제한

기본적으로 SnapCenter 는 GET 요청에 허용된 시간 내에 가능한 한 많은 오브젝트를 반환합니다. 기본 시간 초과는 15초입니다. return_timeout_query 매개 변수를 사용하여 이 제한을 변경할 수 있습니다. 예를 들면 다음과 같습니다.

```
return_timeout=5
```

실제로 반환되는 개체 수는 시스템의 총 개체 수와 개체 수에 대한 관련 제약 조건에 따라 최대 개체수보다 작을 수 있습니다.

결과 집합 축소

필요한 경우 이러한 두 매개 변수를 추가 쿼리 매개 변수와 결합하여 결과 집합의 범위를 좁힐 수 있습니다. 예를 들어, 지정된 시간 이후에 생성된 최대 10개의 EMS 이벤트가 반환됩니다.

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

여러 요청을 발행하여 객체를 통해 페이지를 이동할 수 있습니다. 이후의 각 API 호출은 마지막 결과 집합의 최신 이벤트를 기반으로 새 시간 값을 사용해야 합니다.

크기 속성

일부 API 호출과 특정 쿼리 매개 변수에 사용되는 입력 값은 숫자입니다. 정수(바이트)를 제공하는 대신 다음 표에 나와 있는 접미사를 선택적으로 사용할 수 있습니다.

접미사	설명
KB를 클릭합니다	KB 킬로바이트(1024바이트) 또는 키비바이트
MB	MB 메가바이트(KB x 1024바이트) 또는 메가바이트
GB	GB 기가바이트(MB x 1024바이트) 또는 기비바이트
TB	TB 테라바이트(GB x 1024 byes) 또는 테비바이트
PB	PB 페타바이트(TB x 1024 byes) 또는 페이비바이트

API 응답 해석

각 API 요청은 클라이언트에 대한 응답을 다시 생성합니다. 응답을 검토하여 성공 여부를 확인하고 필요에 따라 추가 데이터를 검색해야 합니다.

HTTP 상태 코드입니다

SnapCenter REST API에서 사용하는 HTTP 상태 코드는 다음과 같다.

코드	설명
200	좋습니다 새 개체를 만들지 않는 호출에 대한 성공 여부를 나타냅니다.
201	작성됨 객체가 성공적으로 생성되었습니다. 응답의 위치 헤더에는 개체의 고유 식별자가 포함됩니다.
202	수락됨 요청을 수행하기 위해 백그라운드 작업이 시작되었지만 아직 완료되지 않았습니다.
400	잘못된 요청입니다 요청 입력이 인식되지 않거나 부적절합니다.
401	권한이 없습니다 사용자 인증에 실패했습니다.
403	금지됨 권한 부여(RBAC) 오류로 인해 액세스가 거부되었습니다.

코드	설명
404	찾을 수 없습니다 요청에서 참조되는 리소스가 없습니다.
405	메서드가 허용되지 않습니다 요청의 HTTP 메서드가 리소스에 대해 지원되지 않습니다.
409	충돌 다른 개체를 먼저 만들어야 하거나 요청된 개체가 이미 있으므로 개체를 만들지 못했습니다.
500입니다	내부 오류입니다 서버에서 일반적인 내부 오류가 발생했습니다.

응답 헤더

SnapCenter에서 생성된 HTTP 응답에는 여러 헤더가 포함되어 있습니다.

위치

개체를 만들 때 위치 머리글에는 개체에 할당된 고유 식별자를 포함하여 새 개체에 대한 전체 URL이 포함됩니다.

콘텐츠 유형

이것은 일반적으로 입니다 `application/json`.

응답 바디

API 요청으로 인한 응답 본문의 내용은 객체, 처리 유형 및 요청의 성공 또는 실패에 따라 달라집니다. 응답은 항상 JSON으로 렌더링됩니다.

단일 개체

요청에 따라 필드 집합과 함께 단일 개체를 반환할 수 있습니다. 예를 들어, 가져오기를 사용하여 고유 식별자를 사용하여 클러스터의 선택된 속성을 검색할 수 있습니다.

여러 개의 개체

리소스 컬렉션의 여러 개체를 반환할 수 있습니다. 어떤 경우든 에는 일관된 형식이 사용됩니다 `num_records` 개체 인스턴스의 배열을 포함하는 레코드 및 레코드 수를 나타냅니다. 예를 들어, 특정 클러스터에 정의된 노드를 검색할 수 있습니다.

작업 객체

API 호출이 비동기적으로 처리되는 경우 백그라운드 작업을 고정하는 Job 개체가 반환됩니다. 예를 들어 클러스터 구성을 업데이트하는 데 사용되는 패치 요청은 비동기적으로 처리되고 작업 개체를 반환합니다.

오류 개체

오류가 발생하면 항상 Error 개체가 반환됩니다. 예를 들어, 클러스터에 대해 정의되지 않은 필드를 변경하려고 하면 오류가 발생합니다.

비어 있습니다

경우에 따라 데이터가 반환되지 않고 응답 본문에 빈 JSON 개체가 포함되는 경우가 있습니다.

오류

오류가 발생하면 응답 본문에 오류 객체가 반환됩니다.

형식

오류 개체의 형식은 다음과 같습니다.

```
"error": {
"message": "<string>",
"code": <integer>[,
"target": "<string>"]
}
```

코드 값을 사용하여 일반 오류 유형 또는 범주를 확인하고 메시지를 사용하여 특정 오류를 확인할 수 있습니다. 사용 가능한 경우 대상 필드에는 오류와 관련된 특정 사용자 입력이 포함됩니다.

일반 오류 코드

일반적인 오류 코드는 다음 표에 설명되어 있습니다. 특정 API 호출에는 추가 오류 코드가 포함될 수 있습니다.

코드	설명
409	동일한 식별자를 가진 객체가 이미 있습니다.
400	필드 값이 잘못되었거나 누락되었거나 추가 필드가 제공되었습니다.
400	작업이 지원되지 않습니다.
405	지정된 식별자가 있는 개체를 찾을 수 없습니다.
403	요청 수행 권한이 거부되었습니다.
409	리소스가 사용 중입니다.

REST API 지원

SnapCenter 서버 및 플러그인에 지원되는 REST API

SnapCenter REST API를 통해 사용 가능한 리소스는 SnapCenter API 설명서 페이지에 표시된 대로 범주로 구성됩니다. 다음은 기본 리소스 경로가 있는 각 리소스에 대한 간략한

설명과 함께 적절한 경우 추가 사용 고려 사항입니다.

인증

이 API를 사용하여 SnapCenter 서버에 로그인할 수 있습니다. 이 API는 후속 요청을 인증하는 데 사용되는 사용자 인증 토큰을 반환합니다.

도메인

API를 사용하여 다른 작업을 수행할 수 있습니다.

- SnapCenter에서 모든 도메인을 검색합니다
- 특정 도메인의 세부 정보를 검색합니다
- 도메인을 등록 또는 등록 취소합니다
- 도메인을 수정합니다

작업

API를 사용하여 다른 작업을 수행할 수 있습니다.

- SnapCenter에서 모든 작업을 검색합니다
- 작업의 상태를 검색합니다
- 작업을 취소하거나 중지합니다

설정

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 자격 증명을 등록, 수정 또는 제거합니다
- SnapCenter 서버에 등록된 자격 증명 정보를 표시합니다
- 알림 설정을 구성합니다
- 이메일 알림을 보내도록 현재 구성된 SMTP 서버에 대한 정보를 검색하고 SMTP 서버의 이름, 받는 사람의 이름 및 보낸 사람의 이름을 표시합니다
- SnapCenter 서버 로그인의 MFA(다중 인증) 구성을 표시합니다
- SnapCenter 서버 로그인에 대해 MFA를 설정 또는 해제하고 구성합니다
- MFA를 설정하는 데 필요한 구성 파일을 생성합니다

호스트

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 모든 SnapCenter 호스트를 쿼리합니다
- SnapCenter에서 하나 이상의 호스트를 제거합니다
- 이름으로 호스트를 검색합니다
- 호스트의 모든 리소스를 검색합니다

- 자원 ID를 사용하여 자원을 조회한다
- 플러그인 구성 세부 정보를 검색합니다
- 플러그인 호스트를 구성합니다
- Microsoft SQL Server 호스트에 대한 플러그인의 모든 리소스를 검색합니다
- Oracle 데이터베이스 호스트에 대한 플러그인의 모든 리소스를 검색합니다
- 사용자 지정 애플리케이션 호스트에 대한 플러그인의 모든 리소스를 검색합니다
- SAP HANA 호스트용 플러그인의 모든 리소스를 검색합니다
- 설치된 플러그인을 검색합니다
- 기존 호스트에 플러그인을 설치합니다
- 호스트 패키지를 업그레이드합니다
- 기존 호스트에서 플러그인을 제거합니다
- 호스트에 플러그인을 추가합니다
- 호스트를 추가하거나 수정합니다
- Linux 호스트의 서명을 받습니다
- Linux 호스트의 서명을 등록합니다
- 호스트를 유지 보수 또는 운영 모드로 전환합니다
- 호스트에서 플러그인 서비스를 시작하거나 다시 시작합니다
- 호스트 이름을 바꿉니다

리소스

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 모든 리소스를 검색합니다
- 자원 ID를 사용하여 자원을 조회한다
- Microsoft SQL Server 호스트에 대한 플러그인의 모든 리소스를 검색합니다
- Oracle 데이터베이스 호스트에 대한 플러그인의 모든 리소스를 검색합니다
- 사용자 지정 애플리케이션 호스트에 대한 플러그인의 모든 리소스를 검색합니다
- SAP HANA 호스트용 플러그인의 모든 리소스를 검색합니다
- 키를 사용하여 Microsoft SQL Server 리소스를 검색합니다
- 키를 사용하여 사용자 지정 리소스를 검색합니다
- 사용자 지정 애플리케이션 호스트에 대한 플러그인 리소스를 수정합니다
- 키를 사용하여 사용자 지정 애플리케이션 호스트의 플러그인 리소스를 제거합니다
- 키를 사용하여 SAP HANA 리소스를 검색합니다
- SAP HANA 호스트에 대한 플러그인 리소스를 수정합니다
- 키를 사용하여 SAP HANA 호스트에 대한 플러그인 리소스를 제거합니다

- 키를 사용하여 Oracle 리소스를 검색합니다
- Oracle 애플리케이션 볼륨 리소스를 생성합니다
- Oracle 애플리케이션 볼륨 리소스를 수정합니다
- 키를 사용하여 Oracle 애플리케이션 볼륨 리소스를 제거합니다
- Oracle 리소스의 보조 세부 정보를 검색합니다
- Microsoft SQL Server용 플러그인을 사용하여 Microsoft SQL Server 리소스를 백업합니다
- Oracle 데이터베이스용 플러그인을 사용하여 Oracle 리소스를 백업합니다
- 사용자 지정 애플리케이션용 플러그인을 사용하여 사용자 지정 리소스를 백업합니다
- SAP HANA 데이터베이스 구성
- Oracle 데이터베이스를 구성합니다
- SQL 데이터베이스 백업을 복원합니다
- Oracle 데이터베이스 백업을 복원합니다
- 사용자 지정 애플리케이션 백업을 복원합니다
- 사용자 지정 플러그인 리소스를 생성합니다
- SAP HANA 리소스를 생성합니다
- 사용자 지정 애플리케이션용 플러그인을 사용하여 사용자 지정 리소스를 보호합니다
- Microsoft SQL Server용 플러그인을 사용하여 Microsoft SQL Server 리소스를 보호합니다
- 보호된 Microsoft SQL Server 리소스를 수정합니다
- Microsoft SQL Server 리소스에 대한 보호를 제거합니다
- Oracle 데이터베이스용 플러그인을 사용하여 Oracle 리소스를 보호합니다
- 보호된 Oracle 리소스를 수정합니다
- Oracle 리소스의 보호 제거
- 사용자 지정 애플리케이션용 플러그인을 사용하여 백업에서 리소스를 클론 복제합니다
- Oracle 데이터베이스용 플러그인을 사용하여 백업에서 Oracle 애플리케이션 볼륨의 클론을 생성합니다
- Microsoft SQL Server용 플러그인을 사용하여 백업에서 Microsoft SQL Server 리소스의 클론을 생성합니다
- Microsoft SQL Server 리소스의 클론 수명 주기를 생성합니다
- Microsoft SQL Server 리소스의 클론 수명 주기를 수정합니다
- Microsoft SQL Server 리소스의 클론 수명 주기를 삭제합니다
- 기존 Microsoft SQL Server 데이터베이스를 로컬 디스크에서 NetApp LUN으로 이동합니다
- Oracle 데이터베이스에 대한 클론 사양 파일을 생성합니다
- Oracle 리소스의 주문형 클론 새로 고침 작업을 시작합니다
- 클론 사양 파일을 사용하여 백업에서 Oracle 리소스를 생성합니다
- 데이터베이스를 보조 복제본으로 복원하고 데이터베이스를 다시 가용성 그룹에 연결합니다
- Oracle 애플리케이션 볼륨 리소스를 생성합니다

백업

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 백업 이름, 유형, 플러그인, 리소스 또는 날짜별로 백업 세부 정보를 검색합니다
- 모든 백업을 검색합니다
- 백업 세부 정보를 검색합니다
- 백업 이름 바꾸기 또는 삭제
- Oracle 백업을 마운트합니다
- Oracle 백업을 마운트 해제합니다
- Oracle 백업 카탈로그 작성
- Oracle 백업의 카탈로그를 해제합니다
- 시점 복구를 수행하기 위해 마운트하는 데 필요한 모든 백업을 가져옵니다

복제

API를 사용하여 다른 작업을 수행할 수 있습니다.

- Oracle 데이터베이스 클론 사양 파일을 생성, 표시, 수정 및 삭제합니다
- Oracle 데이터베이스 클론 계층 구조를 표시합니다
- 클론 세부 정보를 검색합니다
- 모든 클론 검색
- 클론 삭제
- ID별로 클론 세부 정보를 검색합니다
- Oracle 리소스의 주문형 클론 새로 고침 작업을 시작합니다
- 클론 사양 파일을 사용하여 백업에서 Oracle 리소스의 클론을 생성합니다

클론 분할

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 클론 생성된 리소스의 클론 분할 작업을 예측합니다
- 클론 분할 작업의 상태를 검색합니다
- 클론 분할 작업을 시작하거나 중지합니다

리소스 그룹

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 모든 리소스 그룹의 세부 정보를 검색합니다
- 이름별로 자원 그룹을 조회한다
- 사용자 지정 응용 프로그램용 플러그인에 대한 리소스 그룹을 생성합니다

- Microsoft SQL Server용 플러그인에 대한 리소스 그룹을 생성합니다
- Oracle 데이터베이스용 플러그인에 대한 리소스 그룹을 생성합니다
- 사용자 지정 응용 프로그램의 플러그인에 대한 리소스 그룹을 수정합니다
- Microsoft SQL Server용 플러그인의 리소스 그룹을 수정합니다
- Oracle 데이터베이스용 플러그인의 리소스 그룹을 수정합니다
- Microsoft SQL Server용 플러그인에 대한 리소스 그룹의 클론 수명 주기를 생성, 수정 또는 삭제합니다
- 리소스 그룹을 백업합니다
- 리소스 그룹을 유지 관리 또는 운영 모드로 전환합니다
- 자원 그룹을 제거합니다

정책

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 정책 세부 정보를 검색합니다
- 이름별로 정책 세부 정보를 검색합니다
- 정책을 삭제합니다
- 기존 정책의 복사본을 생성합니다
- 사용자 지정 응용 프로그램의 플러그인에 대한 정책을 생성하거나 수정합니다
- Microsoft SQL Server용 플러그인의 정책을 생성하거나 수정합니다
- Oracle 데이터베이스용 플러그인에 대한 정책을 생성하거나 수정합니다
- SAP HANA 데이터베이스용 플러그인에 대한 정책을 생성하거나 수정합니다

스토리지

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 모든 공유를 검색합니다
- 이름으로 공유를 검색합니다
- 공유를 만들거나 삭제합니다
- 저장소 세부 정보를 검색합니다
- 이름별로 저장소 세부 정보를 검색합니다
- 스토리지를 생성, 수정 또는 삭제합니다
- 스토리지 클러스터에서 리소스를 검색합니다
- 스토리지 클러스터의 리소스를 검색합니다

공유

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 공유의 세부 정보를 검색합니다
- 모든 공유의 세부 정보를 가져옵니다
- 스토리지에서 공유를 생성하거나 삭제합니다
- 이름으로 공유를 검색합니다

플러그인

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 호스트의 모든 플러그인을 나열합니다
- 키를 사용하여 Microsoft SQL Server 리소스를 검색합니다
- 키를 사용하여 사용자 지정 리소스를 수정합니다
- 키를 사용하여 사용자 지정 리소스를 제거합니다
- 키를 사용하여 SAP HANA 리소스를 검색합니다
- 키를 사용하여 SAP HANA 리소스를 수정합니다
- 키를 사용하여 SAP HANA 리소스를 제거합니다
- 키를 사용하여 Oracle 리소스를 검색합니다
- 키를 사용하여 Oracle 애플리케이션 볼륨 리소스를 수정합니다
- 키를 사용하여 Oracle 애플리케이션 볼륨 리소스를 제거합니다
- Microsoft SQL Server용 플러그인과 키를 사용하여 Microsoft SQL Server 리소스를 백업합니다
- Oracle 데이터베이스용 플러그인과 키를 사용하여 Oracle 리소스를 백업합니다
- 사용자 지정 애플리케이션 및 키용 플러그인을 사용하여 사용자 지정 애플리케이션 리소스를 백업합니다
- 키를 사용하여 SAP HANA 데이터베이스를 구성합니다
- 키를 사용하여 Oracle 데이터베이스를 구성합니다
- 키를 사용하여 사용자 지정 응용 프로그램 백업을 복원합니다
- 사용자 지정 플러그인 리소스를 생성합니다
- SAP HANA 리소스를 생성합니다
- Oracle 애플리케이션 볼륨 리소스를 생성합니다
- 사용자 지정 애플리케이션용 플러그인을 사용하여 사용자 지정 리소스를 보호합니다
- Microsoft SQL Server용 플러그인을 사용하여 Microsoft SQL Server 리소스를 보호합니다
- 보호된 Microsoft SQL Server 리소스를 수정합니다
- Microsoft SQL Server 리소스에 대한 보호를 제거합니다
- Oracle 데이터베이스용 플러그인을 사용하여 Oracle 리소스를 보호합니다
- 보호된 Oracle 리소스를 수정합니다
- Oracle 리소스의 보호 제거
- 사용자 지정 애플리케이션용 플러그인을 사용하여 백업에서 리소스를 클론 복제합니다

- Oracle 데이터베이스용 플러그인을 사용하여 백업에서 Oracle 애플리케이션 볼륨의 클론을 생성합니다
- Microsoft SQL Server용 플러그인을 사용하여 백업에서 Microsoft SQL Server 리소스의 클론을 생성합니다
- Microsoft SQL Server 리소스의 클론 수명 주기를 생성합니다
- Microsoft SQL Server 리소스의 클론 수명 주기를 수정합니다
- Microsoft SQL Server 리소스의 클론 수명 주기를 삭제합니다
- Oracle 데이터베이스에 대한 클론 사양 파일을 생성합니다
- Oracle 리소스의 온디맨드 클론 수명 주기를 시작합니다
- 클론 사양 파일을 사용하여 백업에서 Oracle 리소스의 클론을 생성합니다

보고서

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 각 플러그인에 대한 백업, 복원 및 클론 작업 보고서를 검색합니다
- 스케줄을 추가, 실행, 삭제 또는 수정합니다
- 예약된 보고서에 대한 데이터를 검색합니다

경고

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 모든 경고를 검색합니다
- ID별로 경고를 검색합니다
- 여러 알림을 삭제하거나 ID별로 알림을 삭제합니다

RBAC

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 사용자, 그룹 및 역할에 대한 세부 정보를 검색합니다
- 사용자 추가 또는 삭제
- 역할에 사용자를 할당합니다
- 역할에서 사용자 할당을 취소합니다
- 역할을 생성, 수정 또는 삭제합니다
- 역할에 그룹을 할당합니다
- 역할에서 그룹 할당을 취소합니다
- 그룹을 추가하거나 삭제합니다
- 기존 역할의 복사본을 만듭니다
- 사용자 또는 그룹에 리소스를 할당하거나 할당 해제합니다

구성

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 구성 설정을 봅니다
- 구성 설정을 수정합니다

인증서 설정

API를 사용하여 다른 작업을 수행할 수 있습니다.

- SnapCenter 서버 또는 플러그인 호스트의 인증서 상태를 봅니다
- SnapCenter 서버 또는 플러그인 호스트의 인증서 설정을 수정합니다

리포지토리

API를 사용하여 다른 작업을 수행할 수 있습니다.

- 리포지토리 백업을 검색합니다
- 리포지토리에 대한 구성 정보를 봅니다
- SnapCenter 리포지토리를 보호하고 복구합니다
- SnapCenter 리포지토리 보호를 해제합니다
- 리포지토리를 재구축하고 페일오버합니다

버전

이 API를 사용하여 SnapCenter 버전을 볼 수 있습니다.

DR(재해 복구) REST API

SnapCenter DR(재해 복구) 기능은 REST API를 사용하여 SnapCenter 서버를 백업합니다. DR REST API를 사용하기 전에 다음 단계를 수행하십시오.

- 단계 *

1. DR 백업 REST API를 사용하여 지정된 서버 DR 백업에서 SnapCenter 서버를 복원하는 새 서버 DR 백업 생성: `/4.5/disasterrecovery/server/backup`
2. 보조 서버 시스템을 불러오지만 보조 서버에 SnapCenter 서버를 설치하기 전에 필수 구성 요소를 완료해야 합니다.
   - 대체 서버 호스트 이름/호스트 FQDN은 기본 서버 호스트 이름과 같아야 하지만 IP 주소는 다를 수 있습니다.
   - 2차 서버 버전은 1차 서버와 동일해야 합니다.
   - 보조 SnapCenter는 운영 포트와 동일한 위치에 동일한 포트에 설치해야 합니다.
3. 서버 DR 복원 작업을 트리거하기 전에 재해 발생 후 DR 백업이 저장되는 경로 또는 대상 경로를 가져와야 합니다.
   - 다음 명령을 사용하여 DR 백업 파일이 새 SnapCenter 서버에 복사되었는지 확인합니다.

```
xcopy <Ssource_Path> \\<Destination_Server_IP>\<Folder_Path> /O /X /E /H
/K {ex : xcopy C:\DRBackup \\10.225.81.114\c$\DRBackup /O /X /E /H /K}
```

4. 보조 시스템에 SnapCenter 서버를 설치합니다.
   - DR 복원 작업을 수행하는 동안 SnapCenter 서버와 관련된 작업이 실행되고 있지 않은지 확인해야 합니다.
5. 보조 SnapCenter 서버를 운영 서버와 동일한 위치에 동일한 포트에 설치합니다.
   - DR 복원 API를 사용하여 서버 DR 복원 작업 수행: `/4.5/disasterrecovery/server/restore`

     플러그인이 서버 호스트 이름을 확인할 수 없는 경우 각 플러그인 호스트에 로그인하고 <New IP> SC_Server_Name 형식으로 새 IP에 대한 etc/host 항목을 추가합니다.
     예를 들면, 다음과 같습니다. `10.225.81.35 SCServer1`

서버 etc/host 항목은 복원되지 않습니다. DR 백업 폴더에서 수동으로 복원할 수 있습니다.

F5 설치의 경우 복원 작업이 독립 실행형으로 수행되며 일련의 명령을 실행하여 F5를 다시 만들어야 합니다. 참조, 링크: "SnapCenter를 다른 서버로 마이그레이션하는 방법"

DR 복구 후 호스트가 추가되지만 플러그인을 수동으로 설치해야 합니다.

Windows용 SnapCenter 플러그인을 설치하고 NetApp LUN을 서버 시스템에 연결한 경우에만 저장소 백업 일정이 복구됩니다.

DLL이 손상된 경우 SnapCenter 서버를 복구하거나 잘못된 설치를 수정할 수 있습니다.

NSM 또는 config 파일이 손상된 경우 동일한 버전으로 SnapCenter 서버를 제거하고 다시 설치할 수 있습니다.

VM이 손상된 경우 같은 이름의 다른 VM 또는 시스템을 가져와 같은 버전의 SnapCenter Server를 설치합니다.

SnapCenter 서버의 재해 복구에 **REST API**가 지원됩니다

REST API를 사용하여 REST API Swagger 페이지에서 다음 작업을 수행할 수 있습니다. Swagger 페이지에 액세스하는 방법은 를 참조하십시오 "swagger API 웹 페이지를 사용하여 REST API에 액세스하는 방법".

시작하기 전에

- SnapCenter 관리자로 로그인해야 합니다.
- DR 복원 API를 실행하려면 SnapCenter 서버가 실행 중이어야 합니다.
- DLL이 손상된 경우 SnapCenter 서버 설치를 복구합니다.
- NSM이 손상되었거나 구성 파일이 손상된 경우 동일한 버전으로 SnapCenter 서버를 제거하고 다시 설치합니다.
- VM이 손상된 경우 이름이 같은 다른 VM을 가져오고 동일한 버전의 SnapCenter Server를 설치합니다.

이 작업에 대해

SnapCenter 서버 DR은 모든 플러그인을 지원합니다.

설명	REST API	HTTP 메소드
기존 SnapCenter 서버 DR 백업을 가져옵니다 DR 백업이 저장되는 타겟 경로를 제공해야 합니다.	`/4.5/disasterrecovery/server/backup?targetpath={path}`	가져오기
새 서버 DR 백업을 생성합니다.	`/4.5/disasterrecovery/server/backup`	게시
지정된 서버 DR 백업에서 SnapCenter 서버를 복원합니다.	`/4.5/disasterrecovery/server/restore`	게시
백업 이름을 기준으로 서버 DR 백업을 삭제합니다.	`/4.5/disasterrecovery/server/backup`	삭제
스토리지 DR을 설정하거나 해제합니다	`/4.5/disasterrecovery/storage`	게시

관련 정보

를 참조하십시오 "재해 복구 API" 비디오.

Swagger API 웹 페이지를 사용하여 REST API에 액세스하는 방법

REST API는 Swagger 웹 페이지를 통해 표시됩니다. Swagger 웹 페이지에 액세스하여 SnapCenter 서버 REST API를 표시하고 API 호출을 수동으로 실행할 수 있습니다. REST API를 사용하여 SnapCenter 서버를 관리하거나 데이터 보호 작업을 수행할 수 있습니다.

REST API를 실행할 SnapCenter 서버의 관리 IP 주소 또는 도메인 이름을 알아야 합니다.

REST API 클라이언트를 실행하는 데 특별한 권한이 필요하지 않습니다. 모든 사용자는 Swagger 웹 페이지에 액세스할 수 있습니다. REST API를 통해 액세스하는 객체에 대한 각 권한은 REST API에 로그인하기 위해 토큰을 생성하는 사용자를 기반으로 합니다.

단계

1. 브라우저에서 Swagger 웹 페이지에 액세스할 URL을 *https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/* 형식으로 입력합니다.

   REST API URL에 +,., %, & 등의 문자가 없는지 확인합니다.

2. Swagger API 문서가 자동으로 표시되지 않으면 * Swagger Explore * 필드에 다음을 입력합니다. _\https:// <SnapCenter_IP_address_or_name>: <SnapCenter_port>/content/swagger/SnapCenter.YAML _
3. Explore * 를 클릭합니다.

   API 리소스 유형 또는 범주 목록이 표시됩니다.

4. API 리소스 유형을 클릭하여 해당 리소스 유형의 API를 표시합니다.

SnapCenter REST API를 실행할 때 예기치 않은 동작이 발생하는 경우 로그 파일을 사용하여 원인을 식별하고 문제를 해결할 수 있습니다.
SnapCenter 사용자 인터페이스에서 * 모니터 * > * 로그 * > * 다운로드 * 를 클릭하여 로그 파일을 다운로드할 수 있습니다.

REST API를 시작합니다

SnapCenter REST API를 사용하여 빠르게 시작할 수 있습니다. API에 액세스하면 실시간 설정에서 보다 복잡한 워크플로 프로세스를 사용하여 API를 사용하기 전에 몇 가지 관점을 제공합니다.

헬로우 월드

시스템에서 간단한 명령을 실행하여 SnapCenter REST API 사용을 시작하고 사용 가능 여부를 확인할 수 있습니다.

시작하기 전에

- 시스템에서 Curl 유틸리티를 사용할 수 있는지 확인합니다.
- SnapCenter 서버의 IP 주소 또는 호스트 이름입니다
- SnapCenter REST API 액세스 권한이 있는 계정의 사용자 이름 및 암호

> 자격 증명에 특수 문자가 포함되어 있는 경우 사용 중인 셸에 따라 Curl에 허용되는 형식으로 형식을 지정해야 합니다. 예를 들어 각 특수 문자 앞에 백슬래시를 삽입하거나 전체 문자를 줄 바꿈할 수 있습니다 `username:password` 문자열을 작은따옴표로 묶습니다.

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

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인 정보 보호 정책

"https://www.netapp.com/company/legal/privacy-policy/"

오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이센스에 대한 정보를 제공합니다.

"SnapCenter 4.9에 대한 고지 사항"