



NetApp 지원 플러그인을 사용하여 애플리케이션 보호

SnapCenter Software 6.0

NetApp
December 19, 2024

목차

NetApp 지원 플러그인을 사용하여 애플리케이션 보호	1
NetApp 지원 플러그인	1
NetApp 지원 플러그인 설치 준비	8
데이터 보호를 준비합니다	30
NetApp에서 지원하는 플러그인 리소스를 백업합니다	32
NetApp 지원 플러그인 리소스를 복원합니다	54
클론 NetApp 지원 플러그인 리소스 백업	60

NetApp 지원 플러그인을 사용하여 애플리케이션 보호

NetApp 지원 플러그인

NetApp 지원 플러그인 개요

사용하는 애플리케이션에 MongoDB, ORASCPM(Oracle Applications), SAP ASE, SAP MaxDB 및 스토리지 플러그인과 같은 NetApp 지원 플러그인을 사용한 다음, SnapCenter을 사용하여 이러한 애플리케이션을 백업, 복원 또는 클론 복제할 수 있습니다. NetApp 지원 플러그인은 NetApp SnapCenter 소프트웨어의 호스트측 구성 요소로 작동하여 애플리케이션 인식 데이터 보호 및 리소스 관리를 지원합니다.

NetApp 지원 플러그인을 설치하면 SnapCenter와 NetApp SnapMirror 기술을 함께 사용하여 다른 볼륨에 있는 백업 세트의 미러 복사본을 생성하고 NetApp SnapVault 기술을 사용하여 D2D 백업 복제를 수행할 수 있습니다. NetApp 지원 플러그인은 Windows 환경과 Linux 환경 모두에서 사용할 수 있습니다.



SnapCenterCLI는 NetApp에서 지원되는 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 NetApp 지원 플러그인을 설치할 수 있습니다.

"호스트를 추가하고 원격 호스트에 플러그인 패키지를 설치합니다."



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.

NetApp 지원 플러그인으로 할 수 있는 작업

MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB, 스토리지 플러그인과 같은 NetApp 지원 플러그인을 데이터 보호 작업에 사용할 수 있습니다.

- 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.

데이터 보호 작업에 NetApp 지원 플러그인을 사용할 수 있습니다.

- ONTAP 클러스터에서 스토리지 볼륨의 정합성 보장 그룹 스냅샷을 생성합니다.
- 내장된 사전 및 사후 스크립팅 프레임워크를 사용하여 사용자 지정 애플리케이션을 백업합니다

ONTAP 볼륨, LUN 또는 Qtree를 백업할 수 있습니다.

- SnapCenter 정책을 사용하여 기존 복제 관계(SnapVault/SnapMirror/통합 복제)를 활용하여 운영 환경에서 생성된 스냅샷을 ONTAP 2차 스토리지로 업데이트합니다

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.

NetApp에서 지원하는 플러그인 기능

SnapCenter는 플러그인 애플리케이션 및 스토리지 시스템의 NetApp 기술과 통합됩니다. MongoDB, ORASCPM(Oracle Applications), SAP ASE, SAP MaxDB 및 스토리지 플러그인과 같은 NetApp 지원 플러그인을 사용하려면 SnapCenter 그래픽 사용자 인터페이스를 사용해야 합니다.

- * 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 기술 *

SnapCenter는 NetApp Snapshot 기술을 NetApp 지원 플러그인과 함께 사용하여 리소스를 백업합니다. 스냅샷은 최소한의 스토리지 공간을 사용합니다.

NetApp 지원 플러그인은 다음과 같은 이점을 제공합니다.

- 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 라이선스가 필요합니다.

- 백업을 생성할 때 ONTAP의 일관성 그룹(CG) 스냅샷 기능 지원
- 여러 리소스 호스트에서 동시에 여러 백업을 실행할 수 있습니다

단일 작업에서 단일 호스트의 리소스가 동일한 볼륨을 공유하는 경우 스냅샷이 통합됩니다.

- 외부 명령을 사용하여 스냅샷을 생성하는 기능.
- Windows 환경에서 파일 시스템 정합성이 보장되는 스냅샷을 생성하는 기능

NetApp 지원 플러그인에서 지원되는 스토리지 유형

SnapCenter는 물리적 시스템과 가상 머신 모두에서 다양한 스토리지 유형을 지원합니다. NetApp 지원 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
VMware ESXi	NFS와 SAN 모두에서 VVOL 데이터 저장소 VVOL 데이터 저장소는 VMware vSphere용 ONTAP 톨로만 프로비저닝할 수 있습니다.

NetApp 지원 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 스냅샷 삭제
 - 볼륨 스냅샷 수정
 - 볼륨 스냅샷 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
 - vservers cifs show 를 참조하십시오
 - SVM 익스포트 정책 생성
 - SVM 익스포트 정책 삭제
 - SVM 익스포트 정책 규칙 생성
 - vservers export-policy rule show를 참조하십시오
 - vservers export-policy show를 참조하십시오
 - SVM iSCSI 연결이 표시됩니다
 - vservers show 를 참조하십시오
- 읽기 전용 명령: ONTAP 8.3.0 이상에 필요한 최소 권한

NetApp 지원 플러그인을 위한 SnapMirror 및 SnapVault 복제용 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.

SnapCenter은 스냅샷 작업이 완료된 후에 SnapMirror 및 SnapVault 업데이트를 수행합니다. SnapMirror 및 SnapVault 업데이트는 SnapCenter 작업의 일부로 수행되고, 별도의 ONTAP 일정을 만들지 않습니다.



NetApp SnapManager 제품에서 SnapCenter으로 오고 있으며 구성된 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 [참조하십시오 "ONTAP 설명서"](#).

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. 정합성 보장 그룹 스냅샷을 사용할지 결정하고 정합성 보장 그룹 스냅샷을 삭제하기 위한 적절한 옵션을 결정합니다.
5. 복제에 NetApp SnapMirror 기술을 사용할지, 장기 보존에 NetApp SnapVault 기술을 사용할지 여부를 결정합니다.
6. 소스 스토리지 시스템 및 SnapMirror 대상에서 스냅샷의 보존 기간을 결정합니다.

7. 백업 작업 전후에 명령을 실행할지 여부를 결정하고 처방이나 PS를 제공합니다.

NetApp 지원 플러그인에 대한 백업 전략

NetApp 지원 플러그인 리소스의 백업 일정

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 추가된 NetApp 지원 플러그인 리소스에 지원되는 복구 전략 유형

SnapCenter를 사용하여 복원 작업을 성공적으로 수행하려면 먼저 전략을 정의해야 합니다. 수동으로 추가된 NetApp 지원 플러그인 리소스에 대한 복구 전략에는 두 가지 유형이 있습니다.



수동으로 추가한 NetApp 지원 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 복원을 위해 선택된 스냅샷 이후에 생성된 스냅샷은 삭제되며 복구할 수 없습니다. 또한 동일한 볼륨 또는 qtree에서 다른 리소스가 호스트되는 경우 해당 리소스도 삭제됩니다.

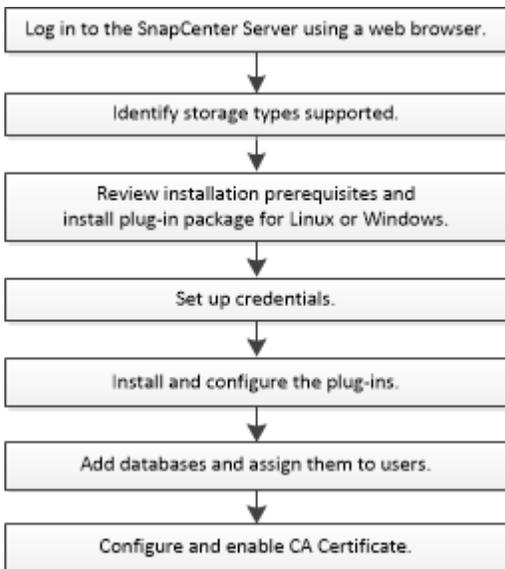
파일 레벨 복구

- 볼륨, qtree 또는 디렉토리에서 파일을 복원합니다
- 선택한 LUN만 복구합니다

NetApp 지원 플러그인 설치 준비

SnapCenter NetApp 지원 플러그인의 설치 워크플로우

NetApp 지원 플러그인 리소스를 보호하려면 SnapCenter NetApp 지원 플러그인을 설치하고 설정해야 합니다.



Windows, Linux 또는 AIX용 호스트 추가 및 플러그인 패키지 설치를 위한 사전 요구 사항

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 완료해야 합니다. NetApp 지원 플러그인은 Windows, Linux 및 AIX 환경에서 지원됩니다.



스토리지 및 Oracle 애플리케이션은 AIX에서 지원됩니다.

- Linux, Windows 또는 AIX 호스트에 Java 11을 설치해야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에게 속한 경우 호스트에서 UAC를 비활성화해야 합니다.

- 호스트 추가 작업이 수행되는 클라이언트 호스트에서 MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB, 스토리지 플러그인과 같은 NetApp 지원 플러그인을 사용할 수 있어야 합니다.

일반

iSCSI를 사용하는 경우 iSCSI 서비스가 실행되고 있어야 합니다.

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.
- Microsoft Windows용 SnapCenter 플러그인을 수동으로 선택해야 합니다.

Linux 및 AIX 호스트



스토리지 및 Oracle 애플리케이션은 AIX에서 지원됩니다.

- 루트 또는 루트 이외의 사용자에게 대해 암호 기반 SSH 연결을 활성화해야 합니다.
- Linux 호스트에 Java 11을 설치해야 합니다.

SnapCenter 서버 호스트에 대해 Windows Server 2019 또는 Windows Server 2016을 사용하는 경우 Java 11을 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 사용자에게 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 SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```

_linux_user_는 사용자가 생성한 루트가 아닌 사용자의 이름입니다.

다음 위치에 있는 * SC_UNIX_plugins_checksum.txt * 파일에서 _checksum_value_를 가져올 수 있습니다.

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\SC_UNIX_plugins_checksum.txt` SnapCenter 서버가 Windows 호스트에 설치된 경우
- `/opt/netapp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` if SnapCenter 서버가 Linux 호스트에 설치되어 있는 경우.



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.



스토리지 및 Oracle 애플리케이션은 AIX에서 지원됩니다.



AIX용 SnapCenter 플러그인 패키지의 일부인 UNIX용 SnapCenter 플러그인은 동시 볼륨 그룹을 지원하지 않습니다.

항목	요구 사항
운영 체제	AIX 7.1 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	자바 11 IBM 자바 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 ["NetApp 상호 운용성 매트릭스 툴"](#) 참조하십시오.

AIX 호스트에 대한 루트가 아닌 사용자에게 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 사용자에게 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_file`을 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 사용자에게 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_file에서 `_CRS_HOME` 값을 가져올 수 있습니다.

`_AIX_USER` 는 사용자가 작성한 루트가 아닌 사용자의 이름입니다.

다음 위치에 있는 * `SC_UNIX_plugins_checksum.txt` * 파일에서 `_checksum_value` 를 가져올 수 있습니다.

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\SC_UNIX_plugins_checksum.txt_SnapCenter` 서버가 Windows 호스트에 설치된 경우
- `/opt/netapp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt_if SnapCenter` 서버가 Linux 호스트에 설치되어 있는 경우.



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 "NetApp 상호 운용성 매트릭스 툴" 참조하십시오.
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	<ul style="list-style-type: none"> • 버전 8.0.5부터 시작하여 이후의 모든 .NET 8 패치를 포함하는 .NET Core • PowerShell 코어 7.4.2 • Java 11 Oracle Java 및 OpenJDK <p>지원되는 버전에 대한 최신 정보는 를 "NetApp 상호 운용성 매트릭스 툴"참조하십시오.</p> <p>NET 관련 문제 해결에 대한 자세한 내용은 을 참조하십시오 "인터넷에 연결되지 않은 기존 시스템의 경우 SnapCenter 업그레이드 또는 설치가 실패합니다."</p>

Linux 및 AIX용 SnapCenter 플러그인 패키지 설치를 위한 호스트 요구 사항입니다

Linux 또는 AIX용 SnapCenter 플러그인 패키지를 설치하기 전에 호스트가 요구 사항을 충족하는지 확인해야 합니다.



스토리지 및 Oracle 애플리케이션은 AIX에서 지원됩니다.

항목	요구 사항
운영 체제	<ul style="list-style-type: none"> • 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 <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>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.</p> </div>
필요한 소프트웨어 패키지	Java 11 Oracle Java 또는 OpenJDK <p>Java를 최신 버전으로 업그레이드한 경우 <code>/var/opt/snapcenter/spl/etc/spl.properties</code> 에 있는 <code>java_home</code> 옵션이 올바른 Java 버전과 올바른 경로로 설정되어 있는지 확인해야 합니다.</p>

지원되는 버전에 대한 최신 정보는 를 참조하십시오 "[NetApp 상호 운용성 매트릭스 툴](#)"

NetApp 지원 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 또는 AIX 호스트

Linux 또는 AIX 호스트에 플러그인을 설치하기 위한 자격 증명을 설정해야 합니다.

플러그인 프로세스를 설치 및 시작할 수 있는 sudo 권한이 있는 루트 사용자 또는 루트 이외의 사용자에게 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.

• NetApp 지원 플러그인 응용 프로그램

플러그인은 리소스를 추가하는 동안 선택 또는 생성된 자격 증명을 사용합니다. 데이터 보호 작업 중에 리소스에 자격 증명 없이 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	<p>인증에 사용할 사용자 이름과 암호를 입력합니다.</p> <ul style="list-style-type: none"> • 도메인 관리자 또는 관리자 그룹의 구성원 <p>SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹의 구성원을 지정합니다. 사용자 이름 필드에 유효한 형식은 다음과 같습니다.</p> <ul style="list-style-type: none"> ◦ _NetBIOS\사용자 이름 _ ◦ _도메인 FQDN\사용자 이름 _ <ul style="list-style-type: none"> • 로컬 관리자(작업 그룹에만 해당) <p>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</p>
암호	인증에 사용되는 암호를 입력합니다.
인증 유형	사용할 인증 유형을 선택합니다.

이 필드의 내용...	수행할 작업...
sudo 권한을 사용합니다	루트가 아닌 사용자에게 자격 증명을 생성하는 경우 * sudo 권한 사용 * 확인란을 선택합니다.  Linux 및 AIX 사용자에게만 적용됩니다.

5. 확인 * 을 클릭합니다.

자격 증명 설정을 마친 후 사용자 및 액세스 페이지의 사용자 또는 사용자 그룹에 자격 증명 유지 관리를 할당할 수 있습니다.

Windows Server 2016 이상에서 GMSA를 구성합니다

Windows Server 2016 이상을 사용하면 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 GMSA(Managed Service Account)를 만들 수 있습니다.

시작하기 전에

- Windows Server 2016 이상의 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2016 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,...>
.. Get-ADServiceAccount 명령을 실행하여 서비스 계정을 확인한다.
```

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 'Install-AdServiceAccount<GMSA>'를 실행하여 호스트에 GMSA를 설치합니다
 - c. 'Test-AdServiceAccount <GMSA>' 명령을 실행하여 GMSA 계정을 확인합니다
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.

NetApp 지원 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.
- 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 2016 이상에서 그룹 관리 서비스 계정을 구성합니다"](#)

- Windows 호스트의 경우 SnapCenter Plug-in for Windows를 선택해야 합니다.

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...
<p>호스트 유형</p>	<p>호스트 유형을 선택합니다.</p> <ul style="list-style-type: none"> • Windows • 리눅스 • AIX <p> NetApp 지원 플러그인은 Windows, Linux 및 AIX 환경에서 사용할 수 있습니다.</p> <p> 스토리지 및 Oracle 애플리케이션은 AIX에서 지원됩니다.</p>
<p>호스트 이름입니다</p>	<p>FQDN(정규화된 도메인 이름) 또는 호스트의 IP 주소를 입력합니다.</p> <p>SnapCenter는 DNS의 올바른 구성에 따라 달라집니다. 따라서 FQDN을 입력하는 것이 가장 좋습니다.</p> <p>Windows 환경의 경우 IP 주소는 FQDN으로 확인되는 경우에만 신뢰할 수 없는 도메인 호스트에 대해 지원됩니다.</p> <p>독립 실행형 호스트의 IP 주소 또는 FQDN을 입력할 수 있습니다.</p> <p>SnapCenter를 사용하여 호스트를 추가하고 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.</p>

이 필드의 내용...	수행할 작업...
<p>자격 증명</p>	<p>생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성합니다.</p> <p>자격 증명에는 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 생성에 대한 정보를 참조하십시오.</p> <p>지정한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 의해 결정됩니다.</p> </div>

5. 설치할 플러그인 선택 * 섹션에서 설치할 플러그인을 선택합니다.

목록에서 다음 플러그인을 설치할 수 있습니다.

- MongoDB
- ORASCPM(Oracle Applications로 표시됨)
- SAP ASE를 참조하십시오
- SAP MaxDB입니다
- 스토리지

6. (선택 사항) * 추가 옵션 * 을 선택하여 다른 플러그인을 설치합니다.

이 필드의 내용...	수행할 작업...
<p>포트</p>	<p>기본 포트 번호를 유지하거나 포트 번호를 지정합니다.</p> <p>기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트로 표시됩니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.</p> </div>

이 필드의 내용...	수행할 작업...
설치 경로	<p>NetApp 지원 플러그인은 Windows 시스템 또는 Linux 시스템에 설치할 수 있습니다.</p> <ul style="list-style-type: none"> • Windows용 SnapCenter 플러그인 패키지의 경우 기본 경로는 C:\Program Files\NetApp\SnapCenter입니다. <p>선택적으로 경로를 사용자 지정할 수 있습니다.</p> <ul style="list-style-type: none"> • Linux용 SnapCenter 플러그인 패키지 및 AIX용 SnapCenter 플러그인 패키지의 경우 기본 경로는 /opt/NetApp/snapcenter. <p>선택적으로 경로를 사용자 지정할 수 있습니다.</p>
사전 설치 검사를 건너뛰니다	<p>플러그인이 이미 수동으로 설치되어 있고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.</p>
그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행합니다	<p>Windows 호스트의 경우 그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행하려면 이 확인란을 선택합니다.</p> <div style="display: flex; flex-direction: column; gap: 10px;"> <div data-bbox="873 1045 928 1108">  <p>GMSA 이름을 domainName\accountName\$ 형식으로 제공합니다.</p> </div> <div data-bbox="873 1213 928 1276">  <p>GMSA는 SnapCenter Plug-in for Windows 서비스에 대해서만 로그인 서비스 계정으로 사용됩니다.</p> </div> </div>

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 에 있는 web.config 파일을 업데이트하여 기본값을 수정할 수 C:\Program Files\NetApp\SnapCenter WebApp 있습니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.



HA 설정에서 SnapManager.Web.UI.dll.config를 업데이트하는 경우 두 노드에서 파일을 업데이트하고 SnapCenter 앱 풀을 다시 시작해야 합니다.

Windows 기본 경로는 입니다 C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config

Linux 기본 경로는 입니다

/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config

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, Windows** 또는 **AIX용 SnapCenter** 플러그인 패키지를 설치합니다

Install-SmHostPackage PowerShell cmdlet을 사용하여 여러 호스트에 Linux, Windows 또는 AIX용 SnapCenter 플러그인 패키지를 동시에 설치할 수 있습니다.

시작하기 전에

호스트를 추가하는 사용자는 호스트에 대한 관리 권한이 있어야 합니다.



스토리지 및 Oracle 애플리케이션은 AIX에서 지원됩니다.

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 "[SnapCenter 소프트웨어 cmdlet 참조 가이드](#)" 있습니다.

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 **NetApp** 지원 플러그인을 설치합니다

SnapCenter UI(사용자 인터페이스)를 사용하여 NetApp 지원 플러그인을 설치해야 합니다. 환경에서 SnapCenter UI에서 플러그인의 원격 설치를 허용하지 않는 경우 CLI(명령줄 인터페이스)를 사용하여 콘솔 모드나 자동 모드로 NetApp 지원 플러그인을 설치할 수 있습니다.

단계

1. C:\ProgramData\NetApp\SnapCenter\Package Repository에서 NetApp 지원 플러그인을 설치하려는 호스트로 Linux 설치 파일(snapcenter_linux_host_plugin.bin)을 SnapCenter 복사합니다.

SnapCenter 서버가 설치된 호스트에서 이 경로에 액세스할 수 있습니다.

- 명령 프롬프트에서 설치 파일을 복사한 디렉토리로 이동합니다.
- 플러그인 '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'를 설치합니다

- -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
```

- 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 ["SnapCenter 소프트웨어 cmdlet 참조 가이드"](#) 있습니다.

- SnapCenter에 로그인하고 UI 또는 PowerShell cmdlet을 사용하여 NetApp 지원 플러그인을 업로드합니다.

섹션을 참조하여 UI에서 NetApp 지원 플러그인을 업로드할 수 ["호스트를 추가하고 원격 호스트에 플러그인 패키지를 설치합니다"](#) 있습니다.

SnapCenter cmdlet 도움말 및 cmdlet 참조 정보에 PowerShell cmdlet에 대한 자세한 정보가 포함되어 있습니다.

["SnapCenter 소프트웨어 cmdlet 참조 가이드"](#)..

NetApp 지원 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 콘텐츠에서 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>"를 선택합니다

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 **NetApp** 지원 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.

키툴-리스트-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.

```
키툴-리스트-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.

```
키툴-리스트-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 NetApp 지원 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 ["SnapCenter 소프트웨어 cmdlet 참조 가이드"](#) 있습니다.

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

NetApp 지원 플러그인을 사용하기 위한 사전 요구사항

SnapCenter NetApp 지원 플러그인을 사용하려면 먼저 SnapCenter 관리자가 SnapCenter Server를 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 11을 설치합니다.
- 여러 데이터 경로(LIF) 또는 dNFS 구성이 있는 경우 데이터베이스 호스트에서 SnapCenter CLI를 사용하여 다음을 수행할 수 있습니다.
 - 기본적으로 데이터베이스 호스트의 모든 IP 주소가 클론 복제된 볼륨에 대한 SVM(Storage Virtual Machine)의 NFS 스토리지 익스포트 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 "[SnapCenter 소프트웨어 명령 참조 가이드](#)" 있습니다.
- 백업 복제를 원하는 경우 SnapMirror 및 SnapVault를 설정합니다.
- 호스트의 다른 애플리케이션에서 포트 9090을 사용하지 않는지 확인합니다.

포트 9090은 SnapCenter에 필요한 다른 포트 외에 NetApp 지원 플러그인에서 사용하도록 예약해야 합니다.

리소스, 리소스 그룹 및 정책을 사용하여 NetApp 지원 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.

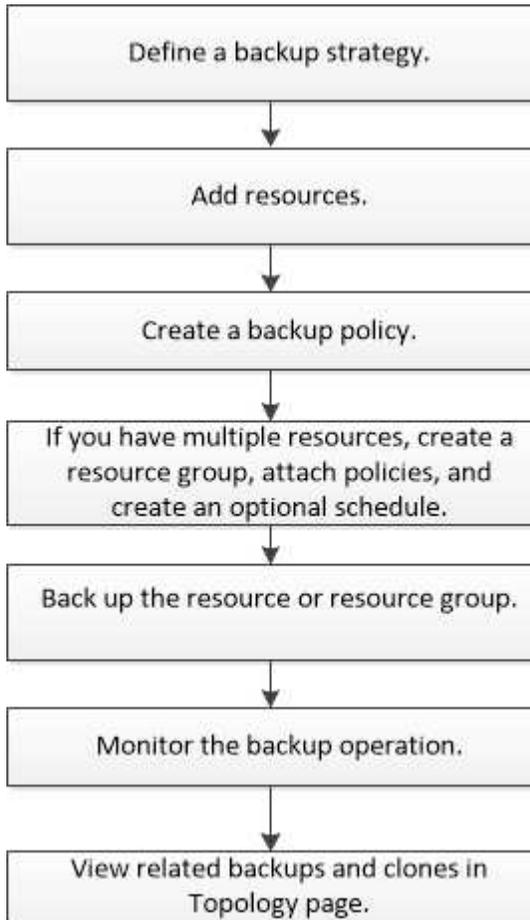
보호하려는 `_대상_`과 이를 보호할 시기를 요일과 시간으로 정의하는 자원 그룹을 생각해 보십시오. 정책을 정의하는 `_방법_`(를) 보호하려는 것으로 생각해 보십시오. 예를 들어 모든 데이터베이스를 백업하거나 호스트의 모든 파일 시스템을 백업하는 경우 모든 데이터베이스나 호스트의 모든 파일 시스템을 포함하는 리소스 그룹을 생성할 수 있습니다. 그런 다음 리소스 그룹에 일별 정책과 시간별 정책이라는 두 가지 정책을 연결할 수 있습니다. 리소스 그룹을 생성하고 정책을 연결할 때 매일 파일 기반 백업을 수행하고 시간 단위로 스냅샷 기반 백업을 수행하는 다른 일정을 수행하도록 리소스 그룹을 구성할 수 있습니다.

NetApp에서 지원하는 플러그인 리소스를 백업합니다

NetApp에서 지원하는 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"](#)

NetApp 지원 플러그인에 리소스 추가

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.
- SnapCenter 서버에 플러그인을 업로드해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지에서 * 리소스 추가 * 를 선택합니다.
3. 리소스 세부 정보 제공 페이지에서 다음 작업을 수행합니다.

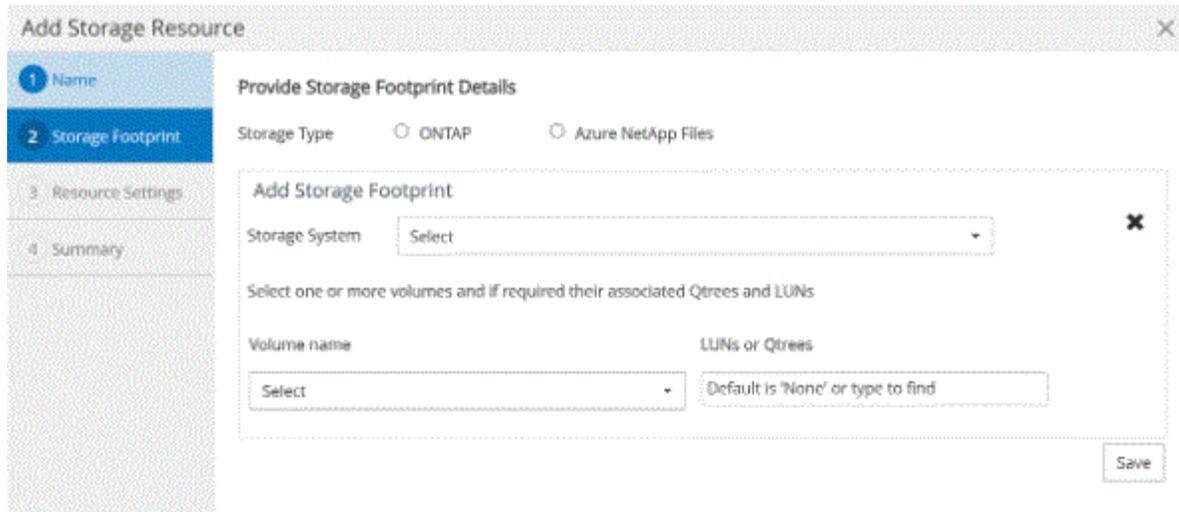
이 필드의 내용...	수행할 작업...
이름	리소스의 이름을 입력합니다.
호스트 이름입니다	호스트를 선택합니다.
유형	유형을 선택합니다. 유형은 플러그인 설명 파일에 따라 사용자가 정의합니다. 예를 들어, 데이터베이스와 인스턴스 등이 있습니다. 선택한 유형에 부모가 있는 경우 상위 항목의 세부 정보를 입력합니다. 예를 들어, 형식이 Database 이고 모체가 instance인 경우 인스턴스의 세부 정보를 입력합니다.
자격 증명 이름입니다	자격 증명을 선택하거나 새 자격 증명을 생성합니다.
마운트 경로	리소스가 마운트된 마운트 경로를 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.



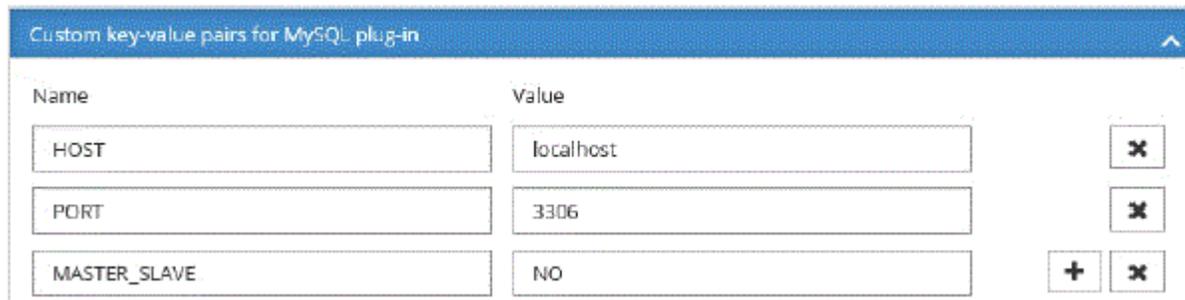
NetApp 지원 플러그인은 리소스의 자동 검색을 지원하지 않습니다. 물리적 환경과 가상 환경의 스토리지 세부 정보도 자동으로 검색되지 않습니다. 리소스를 생성하는 동안 물리적 환경과 가상 환경에 대한 스토리지 정보를 제공해야 합니다.



5. 리소스 설정 페이지에서 리소스에 대한 사용자 지정 키 값 쌍을 제공합니다.

 사용자 정의 키 이름이 대문자인지 확인합니다.

Resource settings



각 플러그인 매개변수는 을 참조하십시오 "[리소스를 구성하는 매개 변수입니다](#)"

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. NetApp 지원 플러그인 리소스에 연결된 백업이 있는 경우 리소스 이름, 리소스 유형 및 호스트 이름 필드를 수정할 수 없습니다.

리소스를 구성하는 매개 변수입니다

플러그인을 수동으로 추가하는 경우 다음 매개 변수를 사용하여 리소스 설정 페이지에서 리소스를 구성할 수 있습니다.

MongoDB용 플러그인

리소스 설정:

- `mongodb_app_server`=(공유 클러스터로서의 리소스 유형) 또는 `mongodb_REPLICASET_server`=(replicaset으로 사용되는 리소스 유형)
- `oplog_path` = (MongoDB.propertiesfile 에서 제공된 경우 선택적 매개 변수)
- `mongodb_authentication_type` = (LDAP 인증의 경우 일반, 기타 인증의 경우 없음)

MongoDB.properties 파일을 제공해야 하는 매개 변수는 다음과 같습니다.

- `DISABLE_STARTING_STARTING_SERVICES`=
 - n 플러그인에서 Start/Stop 서비스를 수행하는 경우
 - 사용자가 start/** stop 서비스를 수행하는 경우 y
 - 기본값으로서의 선택적 매개 변수는 N으로 설정됩니다
- `oplog_path_`=(SnapCenter에 사용자 지정 키-값 쌍으로 이미 제공된 경우 선택적 매개 변수입니다.)

MaxDB용 플러그인

리소스 설정:

- `XUSER_ENABLE` (Y|N) 데이터베이스 사용자에게 암호가 필요하지 않도록 MaxDB에 대한 xuser 사용을 활성화 또는 비활성화합니다.
- `Handle_LOGWRITER` (Y|N) 일시 중지 로그라이터(N) 또는 다시 시작 로그라이터(Y) 작업을 실행합니다.
- `DBMCLICMD(PATH_TO_dbmcli_cmd)`는 MaxDB dbmcli 명령의 경로를 지정합니다. 설정하지 않으면 검색 경로에 dbmcli가 사용됩니다.



Windows 환경의 경우 경로는 큰따옴표("...") 안에 있어야 합니다.

- `SQLCLICMD(PATH_TO_sqlcli_cmd)` MaxDB sqlcli 명령의 경로를 지정합니다. 경로를 설정하지 않으면 sqlcli 가 검색 경로에 사용됩니다.
- `MAXDB_UPDATE_HIST_LOG` (Y|N) 는 MaxDB 백업 프로그램이 MaxDB 이력 로그를 업데이트해야 하는지 여부를 지시합니다.
- `MAXDB_CHECK_snapshot_DIR`: example, SID1: directory [, directoary...];[SID2: directoary[, directory...]] Snap Creator 스냅샷 복제 작업이 성공적인지 확인하고 스냅샷이 생성되었는지 확인합니다.

이는 NFS에만 적용됩니다. 디렉토리는 .snapshot 디렉토리가 포함된 위치를 가리켜야 합니다. 쉼표로 구분된 목록에 여러 디렉토리를 포함할 수 있습니다.

MaxDB 7.8 이상 버전에서는 데이터베이스 백업 요청이 백업 기록에서 Failed(실패) 로 표시됩니다.

- `MAXDB_BACKUP_TEMPLATES`: 각 데이터베이스에 대한 백업 템플릿을 지정합니다.

템플릿이 있어야 하며 외부 유형의 백업 템플릿이어야 합니다. MaxDB 7.8 이상에 대한 스냅샷 통합을 활성화하려면 MaxDB 백그라운드 서버 기능이 있어야 하며 외부 유형의 MaxDB 백업 템플릿을 이미 구성해야 합니다.

- MAXDB_BG_SERVER_PREFIX: 백그라운드 서버 이름의 접두사를 지정합니다.

MAXDB_BACKUP_templates 매개 변수가 설정된 경우 MAXDB_BG_SERVER_PREFIX 매개 변수도 설정해야 합니다. 접두사를 설정하지 않으면 기본값 na_bg_가 사용됩니다.

SAP ASE용 플러그인

리소스 설정:

- SYBASE_SERVER(DATA_SERVER_NAME)는 Sybase 데이터 서버 이름(isql 명령의 -S 옵션)을 지정합니다. 예: p_test.
- SYBASE_DATABASE_EXCLUDE(db_name)는 "ALL" 구문을 사용하는 경우 데이터베이스를 제외할 수 있도록 허용합니다.

세미콜론으로 구분된 목록을 사용하여 여러 데이터베이스를 지정할 수 있습니다. 예: pubs2; test_db1.

- SYBASE_USER:USER_NAME은 isql 명령을 실행할 수 있는 운영 체제 사용자를 지정합니다.

UNIX에 필요합니다. 이 매개 변수는 Snap Creator Agent 시작 및 중지 명령을 실행하는 사용자(일반적으로 루트 사용자)와 isql 명령을 실행하는 사용자가 다른 경우에 필요합니다.

- SYBASE_TRAN_Dump db_name:DIRECTORY_PATH 스냅샷을 생성한 후 Sybase 트랜잭션 덤프를 수행할 수 있습니다. 예를 들어 pubs2:/sybasedumps/pubs2 를 입력합니다

트랜잭션 덤프가 필요한 각 데이터베이스를 지정해야 합니다.

- Sybase_Tran_dump_compress (Y|N) 기본 Sybase 트랜잭션 덤프 압축을 설정하거나 해제합니다.
- SYBASE_ISQL_CMD(예: /opt/Sybase/OCS-15_0/bin/isql)는 isql 명령의 경로를 정의합니다.
- SYBASE_EXCLUDE_TEMPdb(Y|N)를 사용하면 사용자가 생성한 임시 데이터베이스를 자동으로 제외할 수 있습니다.

Oracle 애플리케이션용 플러그인(ORASCPM)

리소스 설정:

- SQLPlus_CMD는 SQLPlus에 대한 경로를 지정합니다.
- Oracle_databases는 백업할 Oracle 데이터베이스와 해당 사용자(database:user)를 나열합니다.
- cntl_file_backup_DIR은 제어 파일 백업을 위한 디렉토리를 지정합니다.
- Ora_TEMP는 임시 파일의 디렉토리를 지정합니다.
- oracle_home은 Oracle 소프트웨어가 설치된 디렉토리를 지정합니다.
- ARCHIVE_LOG_ONLY 아카이브 로그를 백업할지 여부를 지정합니다.
- ORACLE_BACKUP_MODE는 온라인 또는 오프라인 백업을 수행할지 여부를 지정합니다.

NetApp 지원 플러그인 리소스에 대한 정책을 생성합니다

SnapCenter를 사용하여 NetApp 지원 플러그인 특정 리소스를 백업하기 전에 백업하려는 리소스 또는 리소스 그룹에 대한 백업 정책을 생성해야 합니다.

시작하기 전에

- 백업 전략을 정의해야 합니다.

자세한 내용은 NetApp 지원 플러그인에 대한 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 미리 또는 소산 작업에 할당해야 합니다.

미리 또는 볼트에 스냅샷을 복제하는 경우 SnapCenter 관리자가 소스 볼륨과 타겟 볼륨 모두에 SVM을 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.
- SnapLock
 - '특정 기간 동안 백업 복사본 유지' 옵션을 선택한 경우 SnapLock 보존 기간은 언급된 보존 일수보다 작거나 같아야 합니다.
 - 스냅샷 잠금 기간을 지정하면 보존 기간이 만료될 때까지 스냅샷이 삭제되지 않습니다. 이로 인해 정책에 지정된 개수보다 많은 수의 스냅샷이 보존될 수 있습니다.
 - ONTAP 9.12.1 이하 버전의 경우, 복원 과정에서 SnapLock 볼트 스냅샷에서 생성된 클론은 SnapLock 볼트 만료 시간을 상속합니다. 스토리지 관리자는 SnapLock 만료 시간 이후 클론을 수동으로 정리해야 합니다.



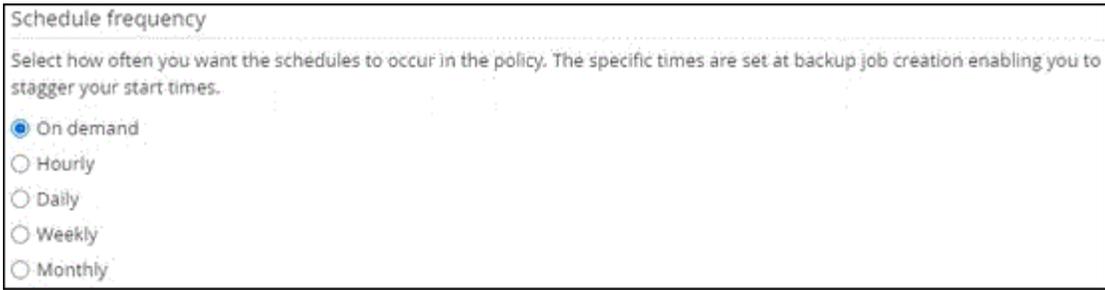
기본 SnapLock 설정은 SnapCenter 백업 정책에서 관리하고 보조 SnapLock 설정은 ONTAP에서 관리합니다.

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...
특정 수의 스냅샷을 유지합니다	<p>유지할 스냅샷 복사본 합계 * 를 선택한 다음 보관할 스냅샷 수를 지정합니다.</p> <p>스냅샷 수가 지정된 수를 초과하면 가장 오래된 복제본이 먼저 삭제되고 스냅샷이 삭제됩니다.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> SnapVault 복제를 설정하려면 보존 수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷이 타겟으로 복제될 때까지 첫 번째 스냅샷이 SnapVault 관계에 대한 참조 스냅샷이기 때문에 보존 작업이 실패할 수 있습니다.</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> 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.</p> </div>
스냅샷을 특정 기간 동안 보관합니다	스냅샷 복사본 유지 * 를 선택한 다음 스냅샷을 삭제하기 전에 보존할 일 수를 지정합니다.
스냅샷 복사본 잠금 기간	<p>Snapshot locking period(스냅샷 잠금 기간) 를 선택하고 일, 월 또는 년을 선택합니다.</p> <p>SnapLock 보존 기간은 100년 미만이어야 합니다.</p>

7. Replication * 페이지에서 복제 설정을 지정합니다.

이 필드의 내용...	수행할 작업...
<ul style="list-style-type: none"> 로컬 스냅샷 복사본을 생성한 후 SnapMirror 업데이트 * 를 참조하십시오 	<p>다른 볼륨에 백업 세트의 미리 복사본을 생성하려면 이 필드를 선택합니다(SnapMirror 복제).</p> <p>ONTAP의 보호 관계가 미리 및 볼트 유형이고 이 옵션만 선택하는 경우, 기본 볼륨에서 생성된 스냅샷은 대상으로 전송되지 않고 대상에 나열됩니다. 복원 작업을 수행하기 위해 대상에서 이 스냅샷을 선택하면 다음 오류 메시지가 표시됩니다. 선택한 볼트 백업/미러링된 백업에 대해 보조 위치를 사용할 수 없습니다.</p> <p>보조 복제 중에 SnapLock 만료 시간에 운영 SnapLock 만료 시간이 로드됩니다.</p> <p>토폴로지 페이지에서 * 새로 고침 * 버튼을 클릭하면 ONTAP에서 검색된 2차 및 1차 SnapLock 만료 시간이 새로 고쳐집니다.</p> <p>을 "토폴로지 페이지에서 NetApp 지원 플러그인 리소스 관련 백업 및 클론을 확인합니다"참조하십시오.</p>
<ul style="list-style-type: none"> 로컬 스냅샷 복사본을 생성한 후 SnapVault 업데이트 * 를 클릭합니다 	<p>디스크 간 백업 복제(SnapVault 백업)를 수행하려면 이 옵션을 선택합니다.</p> <p>보조 복제 중에 SnapLock 만료 시간에 운영 SnapLock 만료 시간이 로드됩니다. 토폴로지 페이지에서 * 새로 고침 * 버튼을 클릭하면 ONTAP에서 검색된 2차 및 1차 SnapLock 만료 시간이 새로 고쳐집니다.</p> <p>SnapLock가 SnapLock 볼트라고 하는 ONTAP의 보조 버전에서만 구성된 경우 토폴로지 페이지에서 * 새로 고침 * 버튼을 클릭하면 ONTAP에서 검색된 보조 시스템의 잠금 기간이 새로 고쳐집니다.</p> <p>SnapLock 볼트에 대한 자세한 내용은 볼트에서 WORM에 스냅샷 커밋 을 참조하십시오 목적지</p> <p>"토폴로지 페이지에서 NetApp 지원 플러그인 리소스 관련 백업 및 클론을 확인합니다"..</p>

이 필드의 내용...	수행할 작업...
<ul style="list-style-type: none"> 보조 정책 레이블 * 	<p>스냅샷 레이블을 선택합니다.</p> <p>선택한 스냅샷 레이블에 따라 ONTAP은 해당 레이블과 일치하는 보조 스냅샷 보존 정책을 적용합니다.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p> 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.</p> </div>
<ul style="list-style-type: none"> 오류 재시도 횟수 * 	<p>작업이 중지되기 전에 허용되는 최대 복제 시도 횟수를 입력합니다.</p>



보조 스토리지의 최대 스냅샷 한도에 도달하지 않도록 ONTAP에서 보조 스토리지의 SnapMirror 보존 정책을 구성해야 합니다.

8. 요약을 검토하고 * Finish * 를 클릭합니다.

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

- 왼쪽 탐색 창에서 * 리소스 * 를 선택한 다음 목록에서 적절한 플러그인을 선택합니다.
- 자원 페이지에서 새 자원 그룹을 선택합니다.
- 이름 페이지에서 다음 작업을 수행합니다.

이 필드의 내용...	수행할 작업...
이름	<p>자원 그룹의 이름을 입력합니다.</p> <p>참고: 리소스 그룹 이름은 250자를 초과할 수 없습니다.</p>
태그	<p>나중에 리소스 그룹을 검색하는 데 도움이 되는 하나 이상의 레이블을 입력합니다.</p> <p>예를 들어 HR을 여러 자원 그룹에 태그로 추가하면 나중에 HR 태그와 연결된 모든 자원 그룹을 찾을 수 있습니다.</p>

이 필드의 내용...	수행할 작업...
스냅샷 복사본에 대해 사용자 지정 이름 형식을 사용합니다	이 확인란을 선택하고 스냅샷 이름에 사용할 사용자 지정 이름 형식을 입력합니다. 예를 들어, <code>_customtext_resource group_policy_hostname</code> 또는 <code>resource group_hostname</code> 과 같이 입력합니다. 기본적으로 타임스탬프는 스냅샷 이름에 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.

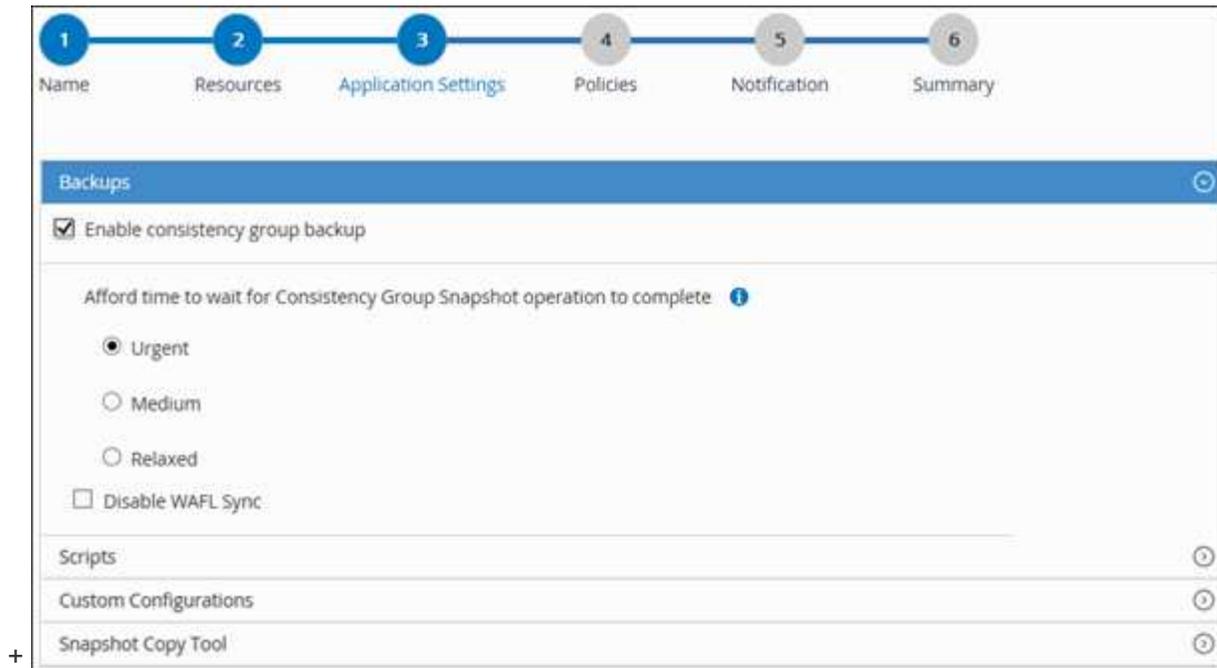
5. 사용 가능한 리소스 * 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 선택하여 * 선택한 리소스 * 섹션으로 이동합니다.

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	Urgent(긴급), Medium(중간) 또는 Relaxed(완화된) 를 선택하여 스냅샷 작업이 완료될 때까지 대기할 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 정지, 스냅샷 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 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	아카이브 로그가 유지되는 일 수를 지정합니다. 이 설정은 ntap_snapshot_retentions보다 크거나 같아야 합니다.
archive_log_DIR입니다	change_info_directory/logs	아카이브 로그를 포함하는 디렉토리의 경로를 지정합니다.
archive_log_EXT	file_extension을 선택합니다	아카이브 로그 파일 확장 길이를 지정합니다. 예를 들어 보관 로그가 log_backup_0_0_0_0.16151855 1942 9이고 file_extension 값이 5이면 로그 확장자는 5자리 (16151)를 유지합니다.

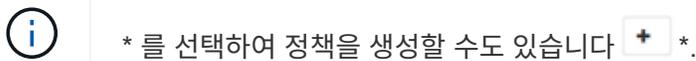
매개 변수	설정	설명
archive_log_recursive_se arch	(예/아니요)	하위 디렉터리 내의 아카이브 로그 관리를 활성화합니다. 아카이브 로그가 하위 디렉토리 아래에 있는 경우 이 매개 변수를 사용해야 합니다.

c. 스냅샷 복사 도구 * 화살표를 선택하여 스냅샷을 생성할 도구를 선택합니다.

원하는 작업	그러면...
SnapCenter - Windows용 플러그인을 사용하고 스냅샷을 생성하기 전에 파일 시스템을 정합성 보장 상태로 전환합니다. 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 레벨 스냅샷을 생성합니다	파일 시스템 일관성 없이 SnapCenter * 를 선택합니다.
호스트에서 실행할 명령을 입력하여 스냅샷을 생성합니다.	기타 * 를 선택한 다음 호스트에서 실행할 명령을 입력하여 스냅샷을 생성합니다.

7. 정책 페이지에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 하나 이상의 정책을 선택합니다.



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. 요약 검토 후 * Finish * 를 선택합니다.

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 Core 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 ["SnapCenter 소프트웨어 cmdlet 참조 가이드"](#) 있습니다.

NetApp에서 지원하는 개별 플러그인 리소스를 백업합니다

개별 NetApp 지원 플러그인 리소스가 리소스 그룹의 일부가 아닌 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.

SnapCenter UI

단계

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 리소스 유형에 따라 리소스를 필터링합니다.

를 클릭한  다음 호스트 이름과 리소스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 을 클릭하여 필터 창을 닫을 수  있습니다.

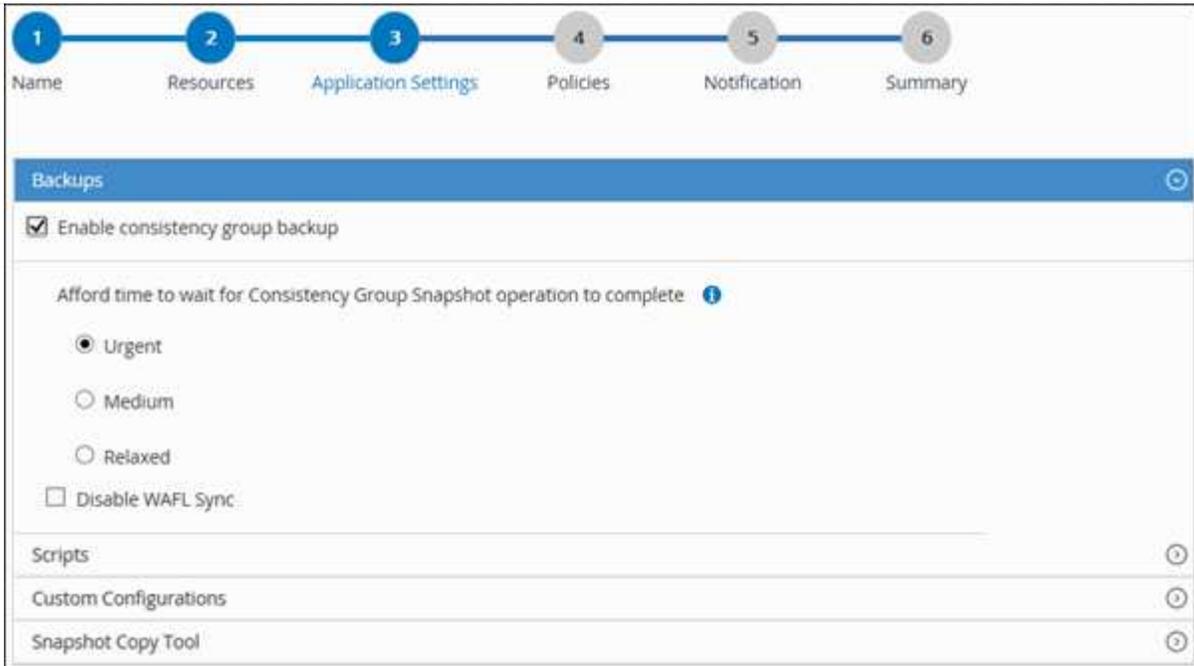
3. 백업할 리소스를 클릭합니다.
4. 사용자 지정 이름을 사용하려면 리소스 페이지에서 * 스냅샷 복사본에 사용자 지정 이름 형식 사용 * 확인란을 선택한 다음 스냅샷 이름에 대한 사용자 지정 이름 형식을 입력합니다.

예: `customtext_policy_hostname_or_resource_hostname`. 기본적으로 타임스탬프는 스냅샷 이름에 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	Urgent(긴급), Medium(중간) 또는 Relaxed(완화된) 를 선택하여 스냅샷 작업이 완료될 때까지 대기할 시간을 지정합니다. 긴급 = 5초, 중간 = 7초, 휴식 = 20초
WAFL 동기화를 비활성화합니다	WAFL 정합성 보장 지점을 강제로 사용하지 않으려면 이 옵션을 선택합니다.



- a. 정지, 스냅샷 및 정지 해제 작업에 대한 사전 및 사후 명령을 실행하려면 스크립트 * 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 복사 도구 * 화살표를 클릭하여 스냅샷을 생성할 도구를 선택합니다.

원하는 작업	그러면...
SnapCenter 를 사용하여 스토리지 수준 스냅샷을 생성합니다	파일 시스템 일관성 없이 SnapCenter * 를 선택합니다.
SnapCenter - Windows용 플러그인을 사용하여 파일 시스템을 일관된 상태로 설정한 다음 스냅샷을 생성합니다	파일 시스템 정합성 보장 * 이 있는 SnapCenter를 선택합니다.
명령을 입력하여 스냅샷을 생성합니다	기타 * 를 선택한 다음 명령을 입력하여 스냅샷을 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.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 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 'scc55.sscore.test.com' -PluginCode
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database
-StorageFootPrint (
@{"VolumeName"="qtree_voll_scc55_sscore_test_com";"QTREE_NAME"="qtree
Vol1";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

3. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.

이 예에서는 새 백업 정책을 생성합니다.

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'  
-PluginPolicyType DummyPlugin -description 'testPolicy'
```

4. 추가 SmResourceGroup cmdlet을 사용하여 SnapCenter에 새 리소스 그룹을 추가합니다.

이 예에서는 지정된 정책 및 리소스를 사용하여 새 리소스 그룹을 만듭니다.

```
Add-SmResourceGroup -ResourceGroupName  
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'  
-Resources  
@(@{"Host"="scc55.sscore.test.com";"Uid"="QTREE2";"PluginName"="Dumm  
yPlugin"},@{"Host"="scc55.sscore.test.com";"Uid"="QTREE";"PluginName  
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'  
-usesnapcenterwithoutfilesystemconsistency
```

5. New-SmBackup cmdlet을 사용하여 새 백업 작업을 시작합니다.

```
New-SMBackup -DatasetName  
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy  
test2
```

6. Get-SmBackupReport cmdlet을 사용하여 백업 작업의 상태를 봅니다.

이 예는 지정된 날짜에 실행된 모든 작업의 작업 요약 보고서를 표시합니다.

```

Get-SmBackupReport -JobId 149

BackedUpObjects           : {QTREE2, QTREE}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 1
SmJobId                   : 149
StartDateTime             : 1/15/2024 1:35:17 AM
EndDateTime               : 1/15/2024 1:36:19 AM
Duration                  : 00:01:02.4265750
CreatedDateTime           : 1/15/2024 1:35:51 AM
Status                    : Completed
ProtectionGroupName       :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows
SmProtectionGroupId       : 1
PolicyName                 : test2
SmPolicyId                : 4
BackupName                 :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows_scc55_01-
15-2024_01.35.17.4467
VerificationStatus        : NotApplicable
VerificationStatuses      :
SmJobError                 :
BackupType                 : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
PluginCode                 : SCC
PluginName                 : DummyPlugin
PluginDisplayName          : DummyPlugin
JobTypeId                  :
JobHost                    : scc55.sscore.test.com

```

NetApp에서 지원하는 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/scvservice`를 찾습니다. 이 스크립트에서 `do_start method` 명령이 SnapCenter VMware 플러그인 서비스를 시작합니다. 이 명령을 `'java-jar-Xmx8192M-Xms4096M'`으로 업데이트합니다.

NetApp 지원 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. 백업 작업만 나열되도록 목록을 필터링하려면  클릭합니다.
 - 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 표시되지만  작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 기호로 표시된 것을 볼 수 있습니다.

5. 작업 세부 정보 페이지에서 * 로그 보기 * 를 클릭합니다.
 로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

NetApp 지원 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 사용자그룹 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 NetApp 지원 플러그인 리소스 관련 백업 및 클론을 확인합니다

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.

SnapLock 지원 백업을 수행한 경우 * 새로 고침 * 버튼을 클릭하면 ONTAP에서 검색된 운영 및 보조 SnapLock 만료 시간이 새로 고쳐집니다. 주별 스케줄은 ONTAP에서 검색된 운영 및 보조 SnapLock 만료 시간도 새로 고칩니다.

애플리케이션 리소스가 여러 볼륨에 분산되면 백업에 대한 SnapLock 만료 시간이 볼륨의 스냅샷에 대해 설정된 가장 긴 SnapLock 만료 시간이 됩니다. ONTAP에서 가장 긴 SnapLock 만료 시간을 검색합니다.

필요 시 백업 후 * Refresh * 버튼을 클릭하면 백업 또는 클론의 세부 정보가 새로 고쳐집니다.

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.

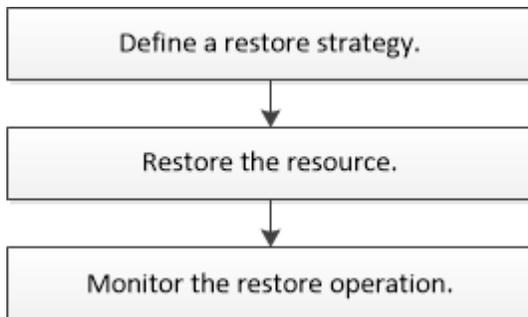
NetApp 지원 플러그인 리소스를 복원합니다

NetApp 지원 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.
- 미러 또는 볼트에 스냅샷을 복제하는 경우, 소스 볼륨과 타겟 볼륨 모두에 대해 SnapCenter 관리자가 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 NetApp 지원 플러그인이 해당 기능을 제공하는 경우에만 수행할 수 있습니다.
- ONTAP 9.12.1 이하 버전의 경우, 복원 과정에서 SnapLock 볼트 스냅샷에서 생성된 클론은 SnapLock 볼트 만료 시간을 상속합니다. 스토리지 관리자는 SnapLock 만료 시간 이후 클론을 수동으로 정리해야 합니다.

SnapCenter UI

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.



Backup Name	End Date
rg1_scapr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. 복원 범위 페이지에서 * 전체 리소스 * 또는 * 파일 수준 * 을 선택합니다.

- a. Complete Resource * 를 선택하면 리소스 백업이 복원됩니다.

리소스에 스토리지 설치 공간으로 볼륨 또는 qtree가 포함되어 있으면 해당 볼륨 또는 qtree의 새로운 스냅샷이 삭제되어 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. 참고: * All * 을 선택하면 볼륨, qtree 또는 LUN의 모든 파일이 복원됩니다.

7. Pre ops * 페이지에서 복구 작업을 수행하기 전에 실행할 사전 복원 및 마운트 해제 명령을 입력합니다.
8. Post ops * 페이지에서 복구 작업을 수행한 후 실행할 mount 및 post restore 명령을 입력합니다.
9. 알림 * 페이지의 * 이메일 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.

PowerShell cmdlet

단계

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대한 SnapCenter Server 연결 세션을 시작합니다.

```
PS C:\> Open-Smconnection
```

2. Get-SmBackup 및 Get-SmBackupReport cmdlet을 사용하여 복원하려는 하나 이상의 백업에 대한 정보를 검색합니다.

이 예에서는 사용 가능한 모든 백업에 대한 정보를 표시합니다.

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

이 예는 2015년 1월 29일부터 2015년 2월 3일까지 백업에 대한 자세한 정보를 표시합니다.

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId         : 2032
StartDateTime   : 2/2/2015 6:57:03 AM
EndDateTime     : 2/2/2015 6:57:11 AM
Duration        : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName      : Vault
SmPolicyId     : 18
BackupName      : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId         : 2183
StartDateTime   : 2/2/2015 1:02:41 PM
EndDateTime     : 2/2/2015 1:02:38 PM
Duration        : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName      : Vault
SmPolicyId     : 18
BackupName      : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 `running_get-Help command_name_`에서 확인할 수 있습니다. 또는 을 참조할 수도 "[SnapCenter 소프트웨어 cmdlet 참조 가이드](#)" 있습니다.

NetApp 지원 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.

클론 NetApp 지원 플러그인 리소스 백업

클론 NetApp 지원 플러그인 리소스 백업

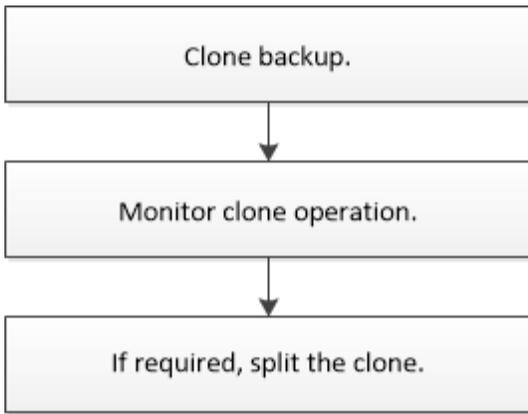
클론 워크플로우에는 클론 작업 수행 및 작업 모니터링이 포함됩니다.

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 NetApp 지원 플러그인이 해당 기능을 제공하는 경우에만 수행할 수 있습니다.
- 볼륨을 호스팅하는 애그리게이트는 SVM(스토리지 가상 머신)의 할당된 애그리게이트 목록에 있어야 합니다.

이 작업에 대해

ONTAP 9.12.1 이하 버전의 경우, 복원 과정에서 SnapLock 볼트 스냅샷에서 생성된 클론은 SnapLock 볼트 만료 시간을 상속합니다. 스토리지 관리자는 SnapLock 만료 시간 이후 클론을 수동으로 정리해야 합니다.

SnapCenter UI

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.

이 필드의 내용...	수행할 작업...
lgroup 프로토콜	lgroup 프로토콜을 선택합니다.



설정 페이지는 스토리지 유형이 LUN인 경우에만 표시됩니다.

- 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>

- 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.

- 요약을 검토하고 * Finish * 를 클릭합니다.

- 모니터 * > * 작업 * 을 클릭하여 작업 진행 상황을 모니터링합니다.

PowerShell cmdlet

단계

- Open-SmConnection cmdlet을 사용하여 지정된 사용자에게 대한 SnapCenter Server 연결 세션을 시작합니다.

```
Open-SmConnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

- 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 : {}  
HostResourceMapping : {}  
Configuration :  
SMCoreContracts.SmCloneConfiguration  
LastBackupStatus : Completed  
VerificationServer :  
EmailBody :  
EmailNotificationPreference : Never  
VerificationServerInfo :  
SchedulerSQLInstance :  
CustomText :  
CustomSnapshotFormat :  
SearchResources : False  
ByPassCredential : False  
IsCustomSnapshot :  
MaintenanceStatus : Production  
PluginProtectionGroupTypes : {SMSQL}  
Tag :
```

```

IsInternal                : False
EnableEmailAttachment    : False
VerificationSettings     : {}
Name                     : NFS_DB
Type                     : Group
Id                       : 2
Host                     :
UserName                 :
Passphrase               :
Deleted                  : False
Auth                     : SMCoreContracts.SmAuth
IsClone                  : False
CloneLevel               : 0
Hosts                    :
StorageName              :
ResourceGroupNames      :
PolicyNames              :

Description               :
CreationTime              : 10/10/2016 4:51:36 PM
ModificationTime         : 10/10/2016 5:27:57 PM
EnableEmail              : False
EmailSMTPServer          :
EmailFrom                :
EmailTo                  :
EmailSubject             :
EnableSysLog             : False
ProtectionGroupType      : Backup
EnableAsupOnFailure      : False
Policies                  : {}
HostResourceMapping      : {}
Configuration            :
SMCoreContracts.SmCloneConfiguration
LastBackupStatus         : Failed
VerificationServer       :
EmailBody                 :
EmailNotificationPreference : Never
VerificationServerInfo   :
SchedulerSQLInstance     :
CustomText                :
CustomSnapshotFormat     :
SearchResources          : False
ByPassRunAs              : False
IsCustomSnapshot         :
MaintenanceStatus        : Production
PluginProtectionGroupTypes : {SMSQL}

```

```

Tag :
IsInternal : False
EnableEmailAttachment : False
VerificationSettings : {}
Name : Test
Type : Group
Id : 3
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
Hosts :
StorageName :
ResourceGroupNames :
PolicyNames :

```

3. New-SmClone cmdlet을 사용하여 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.sscore.test.com";"Uid"="QTREE1"} -
CloneToInstance scc54.sscore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sscore.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           :

```

NetApp 지원 플러그인 리소스 클론 작업 모니터링

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.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.