



# Windows 파일 시스템 보호

## SnapCenter Software 5.0

NetApp  
October 15, 2025

# 목차

Windows 파일 시스템 보호	1
Microsoft Windows용 SnapCenter 플러그인 개념	1
Microsoft Windows용 SnapCenter 플러그인 개요	1
Microsoft Windows용 SnapCenter 플러그인으로 수행할 수 있는 작업	1
Windows용 SnapCenter 플러그인 기능	1
SnapCenter가 Windows 파일 시스템을 백업하는 방법	2
Microsoft Windows용 SnapCenter 플러그인에서 지원하는 스토리지 유형입니다	2
Windows 플러그인에 필요한 최소 ONTAP 권한	5
SnapMirror 및 SnapVault 복제를 위한 스토리지 시스템 준비	7
Windows 파일 시스템에 대한 백업 전략 정의	8
Windows 파일 시스템의 클론 소스 및 대상	10
Microsoft Windows용 SnapCenter 플러그인을 설치합니다	10
Microsoft Windows용 SnapCenter 플러그인 설치 워크플로	10
Microsoft Windows용 SnapCenter 플러그인 설치 요구 사항	10
호스트를 추가하고 Microsoft Windows용 SnapCenter 플러그인을 설치합니다	14
PowerShell cmdlet을 사용하여 여러 원격 호스트에 Microsoft Windows용 SnapCenter 플러그인을 설치합니다	18
명령줄에서 Microsoft Windows용 SnapCenter 플러그인을 자동으로 설치합니다	18
SnapCenter 플러그인 패키지 설치 상태를 모니터링합니다	20
CA 인증서를 구성합니다	20
VMware vSphere용 SnapCenter 플러그인을 설치합니다	24
CA 인증서를 배포합니다	24
CRL 파일을 구성합니다	24
Windows 파일 시스템을 백업합니다	24
Windows 파일 시스템을 백업합니다	24
Windows 파일 시스템에 대한 리소스 가용성을 확인합니다	25
Windows 파일 시스템에 대한 백업 정책을 생성합니다	26
Windows 파일 시스템에 대한 리소스 그룹을 생성합니다	29
필요 시 Windows 파일 시스템에 대한 단일 리소스를 백업합니다	31
Windows 파일 시스템에 대한 리소스 그룹을 백업합니다	33
PowerShell cmdlet을 사용하여 스토리지 시스템 연결과 자격 증명을 생성합니다	34
PowerShell cmdlet을 사용하여 리소스를 백업합니다	35
백업 작업을 모니터링합니다	37
백업 작업을 취소합니다	38
토폴로지 페이지에서 관련 백업 및 클론 보기	39
PowerShell cmdlet을 사용하여 백업을 제거합니다	41
PowerShell cmdlet을 사용하여 보조 백업 수를 정리합니다	42
Windows 파일 시스템을 복구합니다	42
Windows 파일 시스템 백업을 복구합니다	42

PowerShell cmdlet을 사용하여 리소스 복원 .....	44
복구 작업을 모니터링합니다 .....	46
복원 작업을 취소합니다 .....	47
Windows 파일 시스템의 클론을 생성합니다 .....	48
Windows 파일 시스템 백업에서 클론을 생성합니다 .....	48
PowerShell cmdlet을 사용하여 백업 클론 생성 .....	49
클론 작업을 모니터링합니다 .....	53
클론 작업을 취소합니다 .....	54
클론 분할 .....	55

# 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 대한 스토리지 프로비저닝, 스냅샷 일관성 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 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 확인하고, 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 기술 \*

Windows용 플러그인은 NetApp 스냅샷 기술을 사용합니다. 따라서 몇 초 내에 파일 시스템을 백업하고 호스트를 오프라인으로 전환하지 않고도 신속하게 복구할 수 있습니다. 스냅샷은 최소한의 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 라이선스에 대한 내용은 를 참조하십시오 "[SnapCenter 라이선스](#)".
- 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 기술을 사용하여 LUN에 상주하는 Windows 파일 시스템 리소스, CSV(클러스터 공유 볼륨), RDM(원시 장치 매핑) 볼륨, Windows 클러스터의 ALM(비대칭 LUN 매핑) 및 VMFS/NFS 기반 VMDK(NFS를 사용하는 VMware 가상 머신 파일 시스템) 등을 백업합니다.

SnapCenter는 파일 시스템의 스냅샷을 생성하여 백업을 생성합니다. 볼륨에 여러 호스트의 LUN이 포함된 통합 백업은 각 개별 LUN의 백업보다 더 빠르고 효율적입니다. 각 파일 시스템의 개별 스냅샷에 비해 볼륨 스냅샷이 하나만 생성되기 때문입니다.

SnapCenter이 스냅샷을 생성하면 전체 스토리지 시스템 볼륨이 스냅샷에 캡처됩니다. 그러나 백업은 백업이 생성된 호스트 서버에만 유효합니다.

다른 호스트 서버의 데이터가 동일한 볼륨에 상주하는 경우 이 데이터는 스냅샷에서 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 정보를  
 를 "[NetApp 상호 운용성 매트릭스 툴](#)"참조하십시오.

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	<p>Hyper-V Manager를 사용하여 가상 Fibre Channel 스위치로 연결된 VFC(가상 FC) LUN을 프로비저닝해야 합니다.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>NetApp 스토리지에 프로비저닝된 Hyper-V는 디스크를 통과하고 VHD(x)에서 데이터베이스를 백업하는 것은 지원되지 않습니다.</p> </div>
Hyper-V VM	iSCSI 이니시에이터가 게스트 시스템에 직접 접속된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	<div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>NetApp 스토리지에 프로비저닝된 Hyper-V는 디스크를 통과하고 VHD(x)에서 데이터베이스를 백업하는 것은 지원되지 않습니다.</p> </div>

기계	스토리지 유형입니다	를 사용하여 프로비저닝	지원 노트
Hyper-V VM	SVM에 상주하는 SMB3 공유에 연결된 게스트 시스템입니다	SnapCenter GUI 또는 PowerShell cmdlet	<p>프로비저닝만 지원합니다.</p> <p>SnapCenter를 사용하여 SMB 프로토콜을 사용하는 데이터 또는 공유를 백업할 수 없습니다.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>NetApp 스토리지에 프로비저닝된 Hyper-V는 디스크를 통과하고 VHD(x)에서 데이터베이스를 백업하는 것은 지원되지 않습니다.</p> </div>

## 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 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
- 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
- SVM iSCSI 연결이 표시됩니다
- vservers 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.

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 관계 및 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 매주 백업에 대해 구성된 정책이 있는 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 일정을 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 백업에서는 기본 스냅샷 명명 규칙을 사용합니다. 기본 백업 명명 규칙은 복사본이 생성된 시기를 식별할 수 있도록 스냅샷 이름에 타임스탬프를 추가합니다.

스냅샷은 다음과 같은 기본 명명 규칙을 사용합니다. resourceegropname\_hostname\_timestamp

다음 예제와 같이 백업 리소스 그룹의 이름을 논리적으로 지정해야 합니다.

```
dtst1_mach1x88_03-12-2015_23.17.26
```

이 예제에서 구문 요소는 다음과 같은 의미를 가집니다.

- dtst1 리소스 그룹 이름입니다.
- mach1x88 호스트 이름입니다.
- 03-12-2016\_23.17.26 날짜 및 타임스탬프입니다.

백업을 생성할 때 백업을 식별하는 데 도움이 되는 설명 태그를 추가할 수도 있습니다. 반면, 사용자 지정 백업 명명 규칙을 사용하려면 백업 작업이 완료된 후 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.

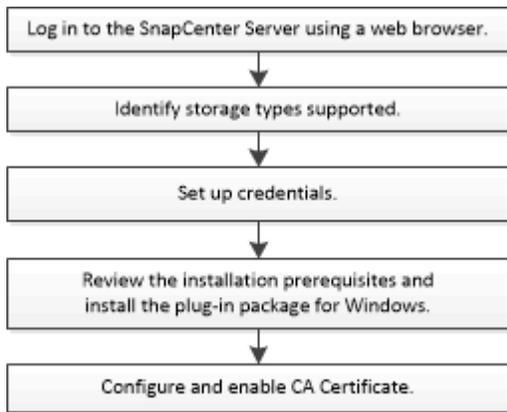
클론 대상	설명
원본, 원본, 위치	기본적으로 SnapCenter는 클론을 생성할 백업과 동일한 위치에 클론을 저장합니다.
위치가 다릅니다	동일한 호스트 또는 다른 호스트의 다른 위치에 클론을 저장할 수 있습니다. 호스트에 SVM(스토리지 가상 시스템)에 대한 연결이 구성되어 있어야 합니다.

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 <a href="#">"NetApp 상호 운용성 매트릭스 툴"</a> 참조하십시오.
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1 GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5 GB   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"> <li>• Microsoft .NET Framework 4.7.2 이상</li> <li>• WMF(Windows Management Framework) 4.0 이상</li> <li>• PowerShell 4.0 이상</li> </ul> <p>지원되는 버전에 대한 최신 정보는 를 <a href="#">"NetApp 상호 운용성 매트릭스 툴"</a>참조하십시오.</p> <p>의 경우. 자세한 문제 해결 정보는 을 참조하십시오 <a href="#">"인터넷에 연결되지 않은 기존 시스템의 경우 SnapCenter 업그레이드 또는 설치가 실패합니다."</a></p>

### 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	<p>인증에 사용되는 사용자 이름과 암호를 입력합니다.</p> <ul style="list-style-type: none"> <li>• 도메인 관리자 또는 관리자 그룹의 구성원</li> </ul> <p>SnapCenter 플러그인을 설치할 시스템에서 도메인 관리자 또는 관리자 그룹의 구성원을 지정합니다. 사용자 이름 필드의 올바른 형식은 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>◦ NetBIOS\UserName</li> <li>◦ Domain FQDN\UserName</li> <li>◦ UserName@upn</li> </ul> <ul style="list-style-type: none"> <li>• 로컬 관리자(작업 그룹에만 해당)</li> </ul> <p>작업 그룹에 속하는 시스템의 경우 SnapCenter 플러그인을 설치할 시스템의 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</p> <p>암호에 큰따옴표(") 또는 백틱(`)을 사용하지 마십시오. 보다 작음(&lt;) 및 느낌표(!)를 사용해서는 안 됩니다. 암호를 사용한 기호. 예를 들어 LessThan &lt;!10, Lessthan10 &lt;!, backtick'12.</p>
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,...>  
.. `Get-ADServiceAccount` 명령을 실행하여 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 로그인 계정으로 사용됩니다.

## 호스트를 추가하고 Microsoft Windows용 SnapCenter 플러그인을 설치합니다

SnapCenter 호스트 추가 페이지를 사용하여 Windows 호스트를 추가할 수 있습니다. Microsoft Windows용 SnapCenter 플러그인은 지정된 호스트에 자동으로 설치됩니다. 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 로그인" 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...
<p>호스트 이름입니다</p>	<p>FQDN(정규화된 도메인 이름) 또는 호스트의 IP 주소를 입력합니다.</p> <p>SnapCenter는 DNS의 올바른 구성에 따라 달라집니다. 따라서 가장 좋은 방법은 FQDN(정규화된 도메인 이름)을 입력하는 것입니다.</p> <p>다음 중 하나의 IP 주소 또는 FQDN을 입력할 수 있습니다.</p> <ul style="list-style-type: none"> <li>• 독립 실행형 호스트</li> <li>• WSFC(Windows Server Failover Clustering)</li> </ul> <p>SnapCenter를 사용하여 호스트를 추가하고 이 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다.</p>
<p>자격 증명</p>	<p>생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성합니다.</p> <p>자격 증명에 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 만들기에 대한 정보를 참조하십시오.</p> <p>사용자 이름, 도메인 및 호스트 유형을 비롯한 자격 증명에 대한 자세한 내용은 입력한 자격 증명 이름 위에 커서를 올려 놓으면 표시됩니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p style="margin: 0;">인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 따라 결정됩니다.</p> </div>

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...
<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 포트 번호로 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>
<p>설치 경로</p>	<p>기본 경로는 C:\Program Files\NetApp\SnapCenter입니다.</p> <p>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.</p>
<p>클러스터의 모든 호스트를 추가합니다</p>	<p>WSFC에서 모든 클러스터 노드를 추가하려면 이 확인란을 선택합니다.</p>
<p>사전 설치 검사를 건너뛸니다</p>	<p>플러그인이 이미 수동으로 설치되어 있고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.</p>
<p>그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행합니다</p>	<p>그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행하려면 이 확인란을 선택합니다.</p> <p>GMSA 이름을 <i>domainName\accountName\$</i> 형식으로 제공합니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>GMSA는 SnapCenter Plug-in for Windows 서비스에 대해서만 로그인 서비스 계정으로 사용됩니다.</p> </div>

7. 제출 \* 을 클릭합니다.

Skip prechecks \* 확인란을 선택하지 않은 경우 호스트는 플러그인 설치 요구 사항을 충족하는지 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 WebApp에 있는 web.config 파일을 업데이트하여 기본값을 수정할 수 C:\Program Files\NetApp\SnapCenter 있습니다. 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

SnapCenter Plug-in for Microsoft Windows를 한 번에 여러 호스트에 설치하려면 PowerShell cmdlet을 사용하여 설치할 수 Install-SmHostPackage 있습니다.

플러그인을 설치할 각 호스트에 대한 로컬 관리자 권한이 있는 도메인 사용자로 SnapCenter에 로그인해야 합니다.

단계

1. PowerShell을 실행합니다.
2. SnapCenter 서버 호스트에서 cmdlet을 사용하여 세션을 설정한 Open-SmConnection 다음 자격 증명을 입력합니다.
3. cmdlet 및 필요한 매개 변수를 사용하여 독립 실행형 호스트 또는 클러스터를 SnapCenter에 Add-SmHost 추가합니다.

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.

4. cmdlet 및 필요한 매개 변수를 사용하여 여러 호스트에 플러그인을 Install-SmHostPackage 설치합니다.

플러그인을 수동으로 설치했지만 호스트가 플러그인 설치 요구 사항을 충족하는지 여부를 확인하지 않으려는 경우 이 옵션을 사용할 수 -skipprecheck 있습니다.

## 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 중
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기 중입니다

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 ["CA 인증서 CSR 파일을 생성하는 방법"](#)참조하십시오.



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. 셸프린트는 셸프린트 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, 셸프린트가 "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 ["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 활성화되거나 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- ✅ \*\* CA 인증서의 유효성 검사가 성공적으로 완료되었음을 나타냅니다.
- 🚫 \*\* 는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- 🚫 \*\* 는 연결 정보를 검색할 수 없음을 나타냅니다.



상태가 노란색 또는 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

# VMware vSphere용 SnapCenter 플러그인을 설치합니다

데이터베이스 또는 파일 시스템이 가상 머신(VM)에 저장되어 있거나 VM 및 데이터 저장소를 보호하려는 경우 VMware vSphere 가상 어플라이언스용 SnapCenter 플러그인을 구축해야 합니다.

배포에 대한 자세한 내용은 을 ["구축 개요"](#)참조하십시오.

## 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.

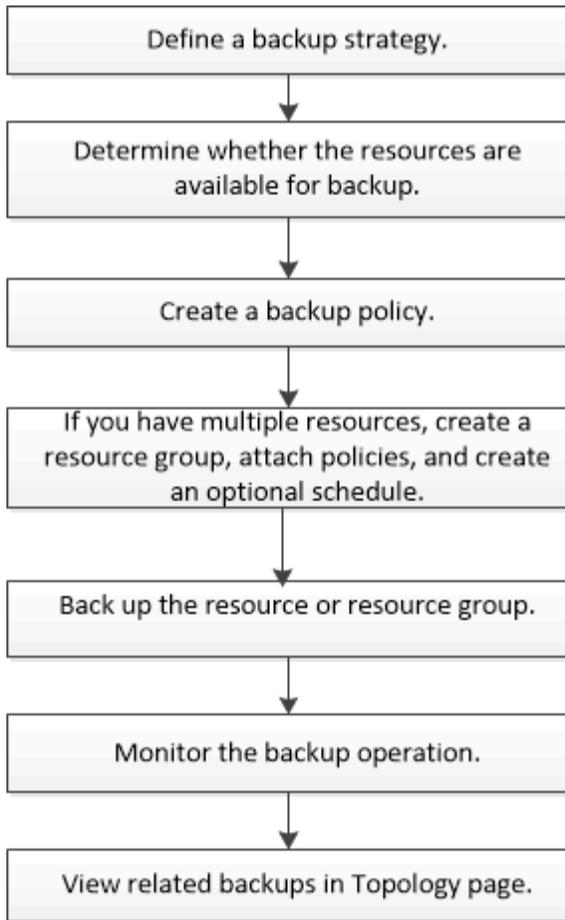
# Windows 파일 시스템을 백업합니다

## 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. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말 또는 [에 "SnapCenter 소프트웨어 cmdlet 참조 가이드"](#) 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 ["VMware vSphere용 SnapCenter 플러그인 설명서"](#) 참조하십시오.

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.

- 미리 또는 소산 2차 스토리지에 스냅샷을 복제하는 경우, SnapCenter 관리자가 소스 볼륨과 타겟 볼륨 모두에 대해 SVM을 할당해야 합니다.
- powershellProcessforScripts 매개 변수의 값을 web.config 파일에서 true 로 설정하여 powerpare 및 postscripts 로 PowerShell 스크립트를 실행해야 합니다.

기본값은 false 입니다

- SnapMirror Business Continuity(SM-BC)의 경우 사전 요구사항 및 제한사항에 대한 자세한 내용은 을 참조하십시오 "[SnapMirror 비즈니스 연속성에 대한 오브젝트 제한](#)".

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.

- 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. 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 2시를 예약한 경우 DST(일광 절약 시간제) 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	스냅샷을 자동으로 삭제하기 전에 SnapCenter 저장소 수를 지정하려면 이 옵션을 선택합니다.
다음보다 오래된 스냅샷 복사본을 삭제합니다	SnapCenter에서 백업 복사본을 삭제하기 전에 보존할 일 수를 지정하려면 이 옵션을 선택합니다.

옵션을 선택합니다	설명
스냅샷 복사본 잠금 기간	Snapshot locking period(스냅샷 잠금 기간) 를 선택하고 일, 월 또는 년을 선택합니다.  SnapLock 보존 기간은 100년 미만이어야 합니다.



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...
<ul style="list-style-type: none"> <li>로컬 스냅샷 복사본을 생성한 후 SnapMirror 업데이트 * 를 참조하십시오</li> </ul>	<p>다른 볼륨(SnapMirror)에 백업 세트의 미러 복사본을 생성하려면 이 옵션을 선택합니다.</p> <p>이 옵션은 SnapMirror Business Continuity(SM-BC)에 대해 활성화되어야 합니다.</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>을 <a href="#">"토폴로지 페이지에서 관련 백업 및 클론 보기"</a> 참조하십시오.</p>
스냅샷 복사본을 생성한 후 SnapVault를 업데이트합니다	<p>디스크 간 백업 복제를 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 운영 SnapLock 만료 시간이 새로 고쳐집니다.</p> <p>SnapLock가 SnapLock 볼트라고 하는 ONTAP의 보조 버전에만 설정된 경우, 토폴로지 페이지에서 새로 고침 버튼을 클릭하면 ONTAP에서 검색된 보조 시스템의 잠금 기간이 새로 고쳐집니다.</p> <p>SnapLock 볼트에 대한 자세한 내용은 을 참조하십시오 <a href="#">"볼트 대상에서 WORM에 스냅샷 복사본을 커밋합니다"</a></p>

이 필드의 내용...	수행할 작업...
보조 정책 레이블입니다	<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>
오류 재시도 횟수입니다	프로세스가 중지되기 전에 수행해야 하는 복제 시도 횟수를 입력합니다.



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

- 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.

- 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.

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.
- SM-BC가 없는 새 파일 시스템을 SM-BC가 포함된 리소스가 포함된 기존 리소스 그룹에 추가할 수 없습니다.
- SM-BC의 페일오버 모드에서 기존 리소스 그룹에 새 파일 시스템을 추가할 수 없습니다. 리소스를 일반 또는 페일백 상태에서만 리소스 그룹에 추가할 수 있습니다.

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	<p>자원 그룹 이름을 입력합니다.</p> <p> 리소스 그룹 이름은 250자를 초과할 수 없습니다.</p>
스냅샷 복사본에 대해 사용자 지정 이름 형식을 사용합니다	<p>선택 사항: 사용자 지정 스냅샷 이름 및 형식을 입력합니다.</p> <p>예를 들어 customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname을 입력합니다. 기본적으로 타임스탬프는 스냅샷 이름에 추가됩니다.</p>
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.

요구 사항을 충족하는 기존 정책이 없는 경우 \* + \* 를 클릭하여 새 정책을 생성하여 정책 마법사를 시작할 수

있습니다.

선택한 정책이 선택한 정책에 대한 스케줄 구성 섹션의 정책 열에 나열됩니다.

- b. 선택한 정책에 대한 스케줄 구성 섹션에서 스케줄을 구성할 정책에 대한 스케줄 구성 열에 있는 \* \* \* \* 를 클릭합니다  .
- 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 스냅샷의 사용자 지정 이름 형식을 입력합니다.

예를 들어 customtext\_resourcegroup\_policy\_hostname 또는 resourcegroup\_hostname을 입력합니다. 기본적으로 타임스탬프는 스냅샷 이름에 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.

요구 사항을 충족하는 기존 정책이 없는 경우 기존 정책을 복사하여 수정하거나 를 클릭하여 정책 마법사를 시작하여 새 정책을 생성할 수 있습니다.

선택한 정책이 선택한 정책에 대한 스케줄 구성 섹션의 정책 열에 나열됩니다.

- b. 선택한 정책에 대한 스케줄 구성 섹션에서 스케줄을 구성할 정책에 대한 스케줄 구성 열을 클릭합니다

- 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	<p>백업 리소스 그룹을 만들고 정책을 첨부하고 일정을 구성한 후 수신자에게 이메일을 보내려면 * Always * , * On Failure * 또는 * On failure 또는 Warning * 을 선택합니다.</p> <p>SMTP 서버 정보, 기본 이메일 제목 줄, ""받는 사람"" 및 " 보내는 사람" 이메일 주소를 입력합니다.</p>

이 필드의 내용...	수행할 작업...
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 자원 그룹 이름을 입력하거나 태그를 클릭하고 선택하여 자원 그룹을 검색할 수  있습니다. 그런 다음 을 클릭하여 필터 창을 닫을 수  있습니다.

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 `/opt/netapp/init_scripts/scvservice`` 찾습니다. 이 스크립트에서 ``do_start method` 명령은 SnapCenter VMware 플러그인 서비스를 시작합니다. 해당 명령을 다음과 같이 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 "[SnapCenter 소프트웨어 cmdlet 참조 가이드](#)" 있습니다.

## 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"="vise-f6.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 ["SnapCenter 소프트웨어 cmdlet 참조 가이드"](#) 있습니다.

## 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 중
-  성공적으로 완료되었습니다
-  실패했습니다
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
-  대기 중입니다
-  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.

### 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.

단계

1. 왼쪽 탐색 창에서 \* 리소스 \* 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2.  Activity(활동) 패널을 클릭하여 가장 최근의 5개 작업을 봅니다.

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 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.
작업 창	a. 백업 작업을 시작한 후  Activity(작업) 창을 클릭하여 가장 최근의 5개 작업을 봅니다. 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.

-  운영 스토리지에서 사용 가능한 백업 및 클론 수를 표시합니다.
- 에는 SnapMirror 기술을 사용하여 2차 스토리지에 미러링되는 백업 및 클론의 수가 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.
-  SnapVault 기술을 사용하여 보조 스토리지에 복제된 백업 및 클론의 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.

2차 관계를 SnapMirror Business Continuity(SM-BC)로 사용할 경우 다음과 같은 추가 아이콘을 볼 수 있습니다.

-  는 복제 사이트가 작동 중임을 의미합니다.
-  는 복제 사이트가 다운되었음을 의미합니다.
-  2차 미러 또는 볼트 관계가 다시 설정되지 않았음을 의미합니다.

#### 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.

Refresh \* 버튼을 클릭하면 스토리지 쿼리가 시작되어 정확한 카운트를 표시합니다.

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.

SnapMirror 비즈니스 연속성(SM-BC)의 경우 \* 새로 고침 \* 버튼을 클릭하면 운영 사이트와 복제 사이트 모두를 ONTAP에 쿼리하여 SnapCenter 백업 인벤토리를 업데이트합니다. 또한 주간 스케줄은 SM-BC 관계를 포함하는 모든 데이터베이스에 대해 이 작업을 수행합니다.

- SM-BC의 경우 새 기본 대상에 대한 비동기식 미러, 볼트 또는 MirrorVault 관계는 페일오버 후 수동으로 구성해야 합니다.
- 페일오버 후 SnapCenter에서 페일오버를 인식하려면 백업을 생성해야 합니다. 백업이 생성된 후에만 \* Refresh \* 를 클릭할 수 있습니다.

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.

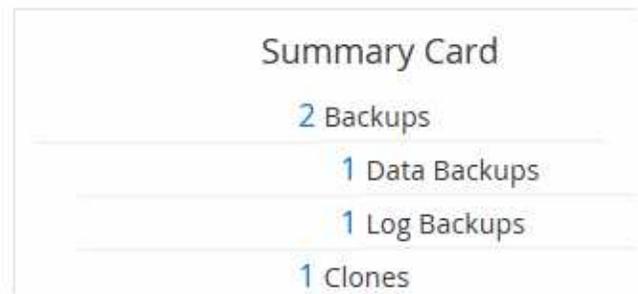
SnapCenter 사용자 지정 플러그인을 사용하는 경우에는 운영 스토리지 시스템에 있는 백업의 이름을 바꿀 수 없습니다.

- 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  클릭하여 클론을 삭제합니다.

운영 스토리지의 백업 및 클론을 보여 주는 예

## Manage Copies



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

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 스냅샷이 없는 보조 백업의 백업 수를 정리할 수 있습니다. 복사본 관리 토폴로지에 표시된 총 스냅샷이 보조 스토리지 스냅샷 보존 설정과 일치하지 않는 경우 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 ["SnapCenter 소프트웨어 cmdlet 참조 가이드"](#) 있습니다.

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 스냅샷이 없는 보조 백업에 대한 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_path`는 플러그인 호스트의 `SMCoreServiceHost.exe.Config` 파일에 있는 `PredefinedWindowsScriptsDirectory` 키를 사용하여 정의됩니다.

필요한 경우 이 경로를 변경하고 SMcore 서비스를 다시 시작할 수 있습니다. 보안을 위해 기본 경로를 사용하는 것이 좋습니다.

키 값은 swagger에서 `API:API/4.7/configsettings`를 통해 표시할 수 있습니다

Get API를 사용하여 키 값을 표시할 수 있습니다. API 설정은 지원되지 않습니다.

- SnapMirror Business Continuity(SM-BC) 복원 작업의 경우 기본 위치에서 백업을 선택해야 합니다.
- 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.

#### 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_path`에 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.

- 요약을 검토하고 \* Finish \* 를 클릭합니다.
- 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

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

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

- 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 -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.

## 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 중
-  성공적으로 완료되었습니다

-  실패했습니다
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
-  대기 중입니다
-  취소됨

단계

1. 왼쪽 탐색 창에서 \* 모니터 \* 를 클릭합니다.
2. 모니터 \* 페이지에서 \* 작업 \* 을 클릭합니다.
3. Jobs \* 페이지에서 다음 단계를 수행하십시오.
  - a. 복원 작업만 나열되도록 목록을 필터링하려면  클릭합니다.
  - 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.

## 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 사용자그룹 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	<ol style="list-style-type: none"> <li>1. 왼쪽 탐색 창에서 * 모니터 * &gt; * 작업 * 을 클릭합니다.</li> <li>2. 작업을 선택하고 * 작업 취소 * 를 클릭합니다.</li> </ol>

시작...	조치
작업 창	<ol style="list-style-type: none"> <li>1. 복구 작업을 시작한 후  Activity(작업) 창을 클릭하여 5개의 가장 최근의 작업을 봅니다.</li> <li>2. 작업을 선택합니다.</li> <li>3. 작업 세부 정보 페이지에서 * 작업 취소 * 를 클릭합니다.</li> </ol>

## 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_path`는 플러그인 호스트의 `SMCoreServiceHost.exe.Config` 파일에 있는 `PredefinedWindowsScriptsDirectory` 키를 사용하여 정의됩니다.

필요한 경우 이 경로를 변경하고 SMcore 서비스를 다시 시작할 수 있습니다. 보안을 위해 기본 경로를 사용하는 것이 좋습니다.

키 값은 swagger에서 `API:API/4.7/configsettings`를 통해 표시할 수 있습니다

Get API를 사용하여 키 값을 표시할 수 있습니다. API 설정은 지원되지 않습니다.

- 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.

#### 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 사용자에게 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	

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}
HostResourceMapping : {}
Configuration : SMCOREContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCOREContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
```

```
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
```

```
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCOREContracts.SmAuth
IsClone : False
```

3. New-SmClone cmdlet을 사용하여 기존 백업에서 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
-B BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-R Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-A AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-S Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

#### 4. Get-SmCloneReport cmdlet을 사용하여 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 ["SnapCenter 소프트웨어 cmdlet 참조 가이드"](#) 있습니다.

### 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 중

-  성공적으로 완료되었습니다
-  실패했습니다
-  경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
-  대기 중입니다
-  취소됨
- 단계 \*
  1. 왼쪽 탐색 창에서 \* 모니터 \* 를 클릭합니다.
  2. 모니터 \* 페이지에서 \* 작업 \* 을 클릭합니다.
  3. Jobs \* 페이지에서 다음 단계를 수행하십시오.
    - a. 클론 작업만 나열되도록 목록을 필터링하려면  클릭합니다.
    - 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 사용자그룹 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	<ol style="list-style-type: none"> <li>1. 왼쪽 탐색 창에서 * 모니터 * &gt; * 작업 * 을 클릭합니다.</li> <li>2. 작업을 선택하고 * 작업 취소 * 를 클릭합니다.</li> </ol>

시작...	조치
작업 창	<ol style="list-style-type: none"> <li>1. 클론 작업을 시작한 후  Activity 창을 클릭하여 가장 최근의 5개 작업을 봅니다.</li> <li>2. 작업을 선택합니다.</li> <li>3. 작업 세부 정보 * 페이지에서 * 작업 취소 * 를 클릭합니다.</li> </ol>

## 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 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. 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"

## 저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

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

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

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

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

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

## 상표 정보

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