Microsoft Exchange Server 데이터베이스 보호

SnapCenter Software 4.5

NetApp
January 18, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/snapcenter-45/protect-sce/concept_snapcenter_plug_in_for_exchange_server_overview.html on January 18, 2024. Always check docs.netapp.com for the latest.

목차

Microsoft Exchange Server 데이터베이스 보호 1
Microsoft Exchange Server용 SnapCenter 플러그인 개념 1
Microsoft Exchange Server용 SnapCenter 플러그인을 설치합니다 11
VMware vSphere용 SnapCenter 플러그인을 설치합니다 29
데이터 보호를 준비합니다 29
Exchange 리소스를 백업합니다 31
Exchange 리소스를 복구합니다 51

Microsoft Exchange Server 데이터베이스 보호

Microsoft Exchange Server용 SnapCenter 플러그인 개념

Microsoft Exchange Server용 SnapCenter 플러그인 개요

Microsoft Exchange Server용 SnapCenter 플러그인은 Exchange 데이터베이스의 애플리케이션 인식 데이터 보호 관리를 지원하는 NetApp SnapCenter 소프트웨어의 호스트 측 구성 요소입니다. Exchange용 플러그인은 SnapCenter 환경에서 Exchange 데이터베이스의 백업 및 복원을 자동화합니다.

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

전체 Exchange 데이터베이스 대신 메일 또는 편지함을 복원 및 복구하려면 SMBR(Single Mailbox Recovery) 소프트웨어를 사용하십시오. NetApp ® Single Mailbox Recovery는 2023년 5월 12일 EOA(End of Availability)로 제공됩니다. NetApp은 2020년 6월 24일에 출시된 마케팅 부품 번호를 통해 지원 자격 기간 동안 메일박스 용량, 유지보수, 지원을 구매한 고객을 계속 지원할 예정입니다.

NetApp Single Mailbox Recovery는 Ontrack에서 제공하는 파트너 제품입니다. OnTrack PowerControls는 NetApp Single Mailbox Recovery와 유사한 기능을 제공합니다. 고객은 세분화된 메일박스 복구를 위해 Ontrack PowerControls 소프트웨어 라이센스와 Ontrack PowerControls 유지보수 및 지원 갱신을 licensingteam@ontrack.com 통해 구매할 수 있습니다.

Microsoft Exchange Server용 SnapCenter 플러그인으로 수행할 수 있는 작업

Exchange용 플러그인을 사용하여 Exchange Server 데이터베이스를 백업 및 복원할 수 있습니다.

- Exchange DAG(데이터베이스 가용성 그룹), 데이터베이스 및 복제 세트의 활성 인벤토리를 보고 관리합니다
- 백업 자동화를 위한 보호 설정을 제공하는 정책을 정의합니다
- 리소스 그룹에 정책을 할당합니다
- 개별 DAG 및 데이터베이스 보호
- 기본 및 보조 Exchange 메일박스 데이터베이스를 백업합니다
- 기본 및 보조 백업에서 데이터베이스를 복원합니다

Microsoft Windows용 SnapCenter 플러그인 및 Microsoft Exchange Server에서 지원하는 스토리지 유형입니다

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

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

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

기계	스토리지 유형입니다	를 사용하여 프로비저닝	지원 노트
Hyper-V VM	iSCSI 이니시에이터가 게스트 시스템에 직접 접속된 iSCSI LUN	SnapCenter GUI 또는 PowerShell cmdlet	ⓘ NetApp 스토리지에 프로비저닝된 Hyper-V는 디스크를 통과하고 VHD(x)에서 데이터베이스를 백업하는 것은 지원되지 않습니다.

최소 **ONTAP** 권한이 필요합니다

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

모든 액세스 명령: **ONTAP 8.2.***x* 이상에 필요한 최소 권한
event generate-autosupport-log입니다
작업 기록이 표시됩니다 작업 중지

모든 액세스 명령: **ONTAP 8.2.*x*** 이상에 필요한 최소 권한
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 persistent - 예약 지우기 LUN 크기 조정 LUN 일련 번호입니다 LUN 표시

모든 액세스 명령: **ONTAP 8.2.*x*** 이상에 필요한 최소 권한
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

모든 액세스 명령: **ONTAP 8.2.*x*** 이상에 필요한 최소 권한
볼륨 클론 생성 볼륨 클론 표시 볼륨 클론 분할 시작이 있습니다 볼륨 클론 분할 중지 볼륨 생성 볼륨 제거 볼륨 파일 클론 생성 볼륨 파일 show-disk-usage 를 참조하십시오 볼륨이 오프라인 상태입니다 볼륨을 온라인으로 설정합니다 볼륨 수정 볼륨 qtree 생성 볼륨 qtree 삭제 볼륨 qtree 수정 볼륨 qtree 표시 볼륨 제한 볼륨 표시 볼륨 스냅샷 생성 볼륨 스냅숏 삭제 볼륨 스냅숏 수정 볼륨 스냅숏 이름 바꾸기 볼륨 스냅샷 복원 볼륨 스냅샷 복원 - 파일 볼륨 스냅샷 표시 볼륨 마운트 해제

모든 액세스 명령: **ONTAP 8.2.*x*** 이상에 필요한 최소 권한
SVM CIFS를 선택합니다 SVM CIFS 공유 생성 SVM CIFS 공유 삭제 SVM CIFS shadowcopy show 를 참조하십시오 SVM CIFS 공유 표시 vserver cifs show 를 참조하십시오 SVM 엑스포트 - 정책 SVM 엑스포트 정책 생성 SVM 엑스포트 정책 삭제 SVM 엑스포트 정책 규칙 생성 vserver export-policy rule show를 참조하십시오 vserver export-policy show를 참조하십시오 SVM iSCSI SVM iSCSI 연결이 표시됩니다 vserver show 를 참조하십시오

읽기 전용 명령: **ONTAP 8.2.*x*** 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.

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

데이터 보호 관계는 운영 스토리지(소스 볼륨)의 데이터를 보조 스토리지(타겟 볼륨)에 복제합니다. 관계를 초기화할 때

ONTAP은 소스 볼륨에서 참조된 데이터 블록을 대상 볼륨으로 전송합니다.

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

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

Exchange Server 리소스에 대한 백업 전략 정의

백업 작업을 생성하기 전에 백업 전략을 정의하면 데이터베이스를 성공적으로 복원하는 데 필요한 백업이 있는지 확인하는 데 도움이 됩니다. SLA(서비스 수준 계약), RTO(복구 시간 목표) 및 RPO(복구 시점 목표)에 따라 백업 전략이 크게 결정됩니다.

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

Exchange 데이터베이스에 대해 지원되는 백업 유형입니다

SnapCenter를 사용하여 Exchange 메일박스를 백업하려면 데이터베이스 및 DAG(데이터베이스 가용성 그룹)와 같은 리소스 유형을 선택해야 합니다. 스냅샷 복사본 기술은 리소스가 상주하는 볼륨의 온라인 읽기 전용 복사본을 생성하는 데 사용됩니다.

백업 유형	설명
전체 및 로그 백업	잘린 로그를 포함하여 데이터베이스와 모든 트랜잭션 로그를 백업합니다. 전체 백업이 완료되면 Exchange Server는 데이터베이스에 이미 커밋된 트랜잭션 로그를 잘라냅니다. 일반적으로 이 옵션을 선택해야 합니다. 그러나 백업 시간이 짧은 경우에는 전체 백업을 사용하여 트랜잭션 로그 백업을 실행하지 않도록 선택할 수 있습니다.
전체 백업	데이터베이스 및 트랜잭션 로그를 백업합니다. 잘린 트랜잭션 로그는 백업되지 않습니다.
로그 백업	모든 트랜잭션 로그를 백업합니다. 데이터베이스에 이미 커밋된 잘린 로그는 백업되지 않습니다. 전체 데이터베이스 백업 간에 트랜잭션 로그 백업을 자주 예약하는 경우 세분화된 복구 지점을 선택할 수 있습니다.

데이터베이스 플러그인에 대한 백업 스케줄입니다

백업 빈도(스케줄 유형)는 정책에 지정되며 백업 스케줄은 리소스 그룹 구성에 지정됩니다. 백업 빈도 또는 스케줄을 결정하는 가장 중요한 요소는 리소스의 변경 속도 및 데이터의 중요도입니다. 자주 사용하는 리소스를 매일 한 번씩 백업할 수도 있고, 자주 사용하지 않는 리소스를 하루에 한 번 백업할 수도 있습니다. 기타 요인으로는 조직에 대한 리소스의 중요성, SLA(서비스 수준 계약) 및 RPO(복구 시점 목표)가 있습니다.

SLA는 예상되는 서비스 수준을 정의하고 가용성 및 서비스 성능을 비롯한 다양한 서비스 관련 문제를 해결합니다. RPO는 장애 후 정상적인 작업을 재개하기 위해 백업 스토리지에서 복구해야 하는 파일의 사용 기간에 대한 전략을 정의합니다. SLA 및 RPO는 데이터 보호 전략에 기여합니다.

사용량이 많은 리소스의 경우에도 하루에 한 번 또는 두 번 이상 전체 백업을 실행할 필요가 없습니다. 예를 들어 정기적인 트랜잭션 로그 백업만으로도 필요한 백업이 있는지 확인할 수 있습니다. 데이터베이스를 더 자주 백업할수록 SnapCenter는 복원 시 사용해야 하는 트랜잭션 로그를 더 적게 사용하여 복원 작업을 더 빠르게 수행할 수 있습니다.

백업 스케줄은 다음과 같이 두 부분으로 구성됩니다.

- 백업 빈도

  일부 플러그인에 대해 _schedule type_이라는 백업 빈도(백업 수행 빈도)는 정책 구성의 일부입니다. 정책의 백업 빈도로 시간별, 일별, 주별 또는 월별 을 선택할 수 있습니다. 이러한 빈도 중 하나를 선택하지 않으면 생성된 정책이 온디맨드 전용 정책입니다. 설정 * > * 정책 * 을 클릭하여 정책에 액세스할 수 있습니다.

- 백업 스케줄

  백업 스케줄(백업을 수행할 정확한 시점)은 리소스 그룹 구성의 일부입니다. 예를 들어 주별 백업에 대한 정책이 구성된 리소스 그룹이 있는 경우 매주 목요일 오후 10시에 백업하도록 스케줄을 구성할 수 있습니다. 리소스 그룹 * > * 리소스 그룹 * 을 클릭하여 리소스 그룹 일정에 액세스할 수 있습니다.

데이터베이스에 필요한 백업 작업 수입니다

필요한 백업 작업 수를 결정하는 요인에는 리소스 크기, 사용된 볼륨 수, 리소스 변경 속도 및 SLA(서비스 수준 계약)가 포함됩니다.

백업 명명 규칙

기본 스냅샷 복사본 명명 규칙을 사용하거나 사용자 지정된 명명 규칙을 사용할 수 있습니다. 기본 백업 명명 규칙은 스냅샷 복사본 이름에 타임 스탬프를 추가하여 복사본이 생성된 시간을 식별하도록 도와줍니다.

스냅샷 복사본은 다음과 같은 기본 명명 규칙을 사용합니다.

'resourcegroupname_hostname_timestamp'

다음 예제와 같이 백업 리소스 그룹의 이름을 논리적으로 지정해야 합니다.

```
dts1_mach1x88_03-12-2015_23.17.26
```

이 예제에서 구문 요소는 다음과 같은 의미를 가집니다.

- _dts1_은(는) 리소스 그룹 이름입니다.

- _mach1x88_은 호스트 이름입니다.
- _03-12-2015_23.17.26_은 날짜 및 타임스탬프입니다.

또는 * Use custom name format for Snapshot copy * 를 선택하여 리소스 또는 리소스 그룹을 보호하면서 스냅샷 복사본 이름 형식을 지정할 수 있습니다. 예를 들어 customtext_resourcegroup_policy_hostname 또는 resourcegroup_hostname을 입력합니다. 기본적으로 타임스탬프 접미사가 스냅샷 복사본 이름에 추가됩니다.

백업 보존 옵션

백업 복사본을 보존할 일 수를 선택하거나 유지할 백업 복사본 수를 최대 255개 사본의 ONTAP로 지정할 수 있습니다. 예를 들어, 조직에서 10일간 백업 복사본 또는 130개의 백업 복사본을 보존해야 할 수도 있습니다.

정책을 생성하는 동안 백업 유형 및 스케줄 유형에 대한 보존 옵션을 지정할 수 있습니다.

SnapMirror 복제를 설정하면 보존 정책이 대상 볼륨에 미러링됩니다.

SnapCenter는 스케줄 유형과 일치하는 보존 레이블이 있는 보존된 백업을 삭제합니다. 리소스 또는 리소스 그룹에 대한 스케줄 유형이 변경된 경우 이전 스케줄 유형 레이블이 있는 백업이 시스템에 남아 있을 수 있습니다.

> 백업 복사본을 장기간 보존하려면 SnapVault 백업을 사용해야 합니다.

Exchange Server의 소스 스토리지 볼륨에 트랜잭션 로그 백업을 유지하는 기간

Microsoft Exchange Server용 SnapCenter 플러그인에는 최신 복원 작업을 수행하기 위한 트랜잭션 로그 백업이 필요합니다. 이 작업은 데이터베이스를 두 개의 전체 백업 사이의 시간으로 복원합니다.

예를 들어 Exchange용 플러그인이 오전 8시에 전체 및 트랜잭션 로그 백업을 수행하는 경우 또한 오후 5시에 전체 및 트랜잭션 로그 백업을 추가로 수행하면 최신 트랜잭션 로그 백업을 사용하여 오전 8시 사이에 언제든지 데이터베이스를 복원할 수 있습니다 오후 5시까지 운영됩니다 트랜잭션 로그를 사용할 수 없는 경우 Exchange용 플러그인은 시점 복원 작업만 수행할 수 있습니다. 그러면 Exchange용 플러그인에서 전체 백업을 완료한 시점으로 데이터베이스를 복원할 수 있습니다.

일반적으로 하루 또는 이틀 동안만 최신 복원 작업이 필요합니다. 기본적으로 SnapCenter는 최소 2일을 유지합니다.

Exchange 데이터베이스에 대한 복구 전략 정의

Exchange Server에 대한 복원 전략을 정의하면 데이터베이스를 성공적으로 복원할 수 있습니다.

Exchange Server의 복구 작업에 대한 소스

기본 스토리지의 백업 복사본에서 Exchange Server 데이터베이스를 복원할 수 있습니다.

운영 스토리지에서만 데이터베이스를 복원할 수 있습니다.

Exchange Server에 대해 지원되는 복구 작업 유형입니다

SnapCenter를 사용하여 Exchange 리소스에 대해 다양한 유형의 복구 작업을 수행할 수 있습니다.

- 최신 상태로 복원합니다

- 이전 시점으로 복원합니다

최대 **1**분 내에 복원합니다

최신 복원 작업에서 데이터베이스는 장애 지점까지 복구됩니다. SnapCenter는 다음 시퀀스를 실행하여 이를 수행합니다.

1. 선택한 전체 데이터베이스 백업에서 데이터베이스를 복원합니다.
2. 백업된 모든 트랜잭션 로그와 가장 최근 백업 이후에 생성된 새 로그를 적용합니다.

   트랜잭션 로그가 앞으로 이동되어 선택한 데이터베이스에 적용됩니다.

   복구가 완료된 후 Exchange에서 새 로그 체인을 생성합니다.

   * 모범 사례: * 복원이 완료된 후 새 전체 및 로그 백업을 수행하는 것이 좋습니다.

   최신 복원 작업을 수행하려면 일련의 트랜잭션 로그가 필요합니다.

   최신 복원을 수행한 후에는 복구에 사용한 백업을 시점 복원 작업에만 사용할 수 있습니다.

   모든 백업에 대해 최신 복원 기능을 유지할 필요가 없는 경우 백업 정책을 통해 시스템의 트랜잭션 로그 백업 보존을 구성할 수 있습니다.

이전 시점으로 복원합니다

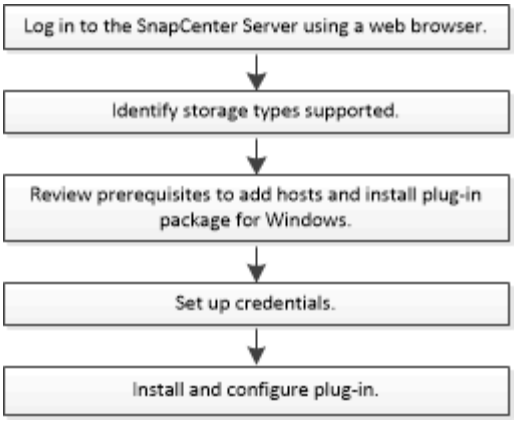
시점 복원 작업에서는 데이터베이스가 과거의 특정 시간으로만 복원됩니다. 시점 복원 작업은 다음과 같은 복원 상황에서 수행됩니다.

- 데이터베이스는 백업된 트랜잭션 로그에서 지정된 시간으로 복원됩니다.
- 데이터베이스가 복원되고 백업된 트랜잭션 로그의 하위 집합만 데이터베이스에 적용됩니다.

Microsoft Exchange Server용 SnapCenter 플러그인을 설치합니다

Microsoft Exchange Server용 SnapCenter 플러그인 설치 워크플로우

Exchange 데이터베이스를 보호하려면 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



호스트를 추가하고 **Microsoft Exchange Server**용 **SnapCenter** 플러그인을 설치하기 위한 사전 요구 사항

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 완료해야 합니다.

- iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.
- 원격 호스트에 대한 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 도메인 사용자가 있어야 합니다.
- 독립 실행형 및 데이터베이스 가용성 그룹 구성에 Microsoft Exchange Server 2013, 2016 또는 2019를 사용해야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자의 경우 호스트에서 UAC를 비활성화해야 합니다.
- SnapCenter에서 클러스터 노드를 관리하는 경우 클러스터의 모든 노드에 대한 관리 권한이 있는 사용자가 있어야 합니다.
- Exchange Server에 대한 관리 권한이 있는 사용자가 있어야 합니다.
- SnapManager for Microsoft Exchange Server 및 SnapDrive for Windows가 이미 설치되어 있는 경우, 동일한 Exchange Server에 Exchange용 플러그인을 설치하기 전에 SnapDrive for Windows에서 사용하는 VSS 하드웨어 공급자를 등록 취소해야 SnapCenter를 사용하여 데이터를 성공적으로 보호할 수 있습니다.
- Microsoft Exchange Server용 SnapManager와 Exchange용 플러그인이 동일한 서버에 설치되어 있는 경우 Windows 스케줄러에서 Microsoft Exchange Server용 SnapManager가 생성한 모든 스케줄을 일시 중지하거나 삭제해야 합니다.
- 호스트는 서버에서 FQDN(정규화된 도메인 이름)으로 확인할 수 있어야 합니다. 호스트 파일을 확인할 수 있도록 수정하고 호스트 파일에 짧은 이름과 FQDN이 모두 지정된 경우 *<IP_address><host_FQDN><host_name>* 형식으로 SnapCenter hosts 파일에 항목을 생성합니다.
- 방화벽에서 다음 포트가 차단되지 않았는지 확인합니다. 차단되지 않으면 호스트 추가 작업이 실패합니다. 이 문제를 해결하려면 동적 포트 범위를 구성해야 합니다. 자세한 내용은 을 참조하십시오 "Microsoft 설명서".
  - Windows 2016 및 Exchange 2016의 경우 포트 범위 50000 - 51000
  - Windows 2012 R2 및 Exchange 2013의 경우 포트 범위는 6000-6500입니다
  - Windows 2019의 경우 포트 범위 49152-65536

포트 범위를 식별하려면 다음 명령을 실행합니다.

- netsh int ipv4 show dynamicport tcp
- netsh int ipv4 show dynamicport udp
- netsh int ipv6 show dynamicport tcp
- netsh int ipv6 show dynamicport UDP

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항 및 사이징 요구 사항을 숙지해야 합니다.

항목	요구 사항
운영 체제	Microsoft Windows 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	• Microsoft .NET Framework 4.5.2 이상 • WMF(Windows Management Framework) 4.0 이상 • PowerShell 4.0 이상 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

Exchange Server 권한이 필요합니다

SnapCenter에서 Exchange Server 또는 DAG를 추가하고 호스트 또는 DAG에 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하려면 최소 권한 및 권한 세트가 있는 사용자에 대한 자격 증명을 사용하여 SnapCenter를 구성해야 합니다.

로컬 관리자 권한이 있는 도메인 사용자와 원격 Exchange 호스트에 대한 로컬 로그인 권한, DAG의 모든 노드에 대한 관리 권한이 있어야 합니다. 도메인 사용자에게는 다음과 같은 최소 권한이 필요합니다.

- Add-MailboxDatabaseCopy 를 선택합니다
- 마운트 해제 - 데이터베이스
- 가져오기 - AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer를 선택합니다
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus 를 참조하십시오
- Get-MailboxServer 를 참조하십시오
- Get-MailboxStatistics를 참조하십시오
- Get-PublicFolderDatabase를 참조하십시오
- Move-ActiveMailboxDatabase(ActiveMailboxDatabase 이동)
- move-DatabasePath-ConfigurationOnly:$true입니다
- 마운트 - 데이터베이스
- New - MailboxDatabase
- 새 기능 - PublicFolderDatabase
- remove - MailboxDatabase(메일 사서함 데이터베이스)
- remove-MailboxDatabaseCopy 를 선택합니다
- 제거 - PublicFolderDatabase
- Resume - MailboxDatabaseCopy
- 설정 - AdServerSettings
- Set-MailboxDatabase -allowfilerestore:$true입니다
- Set-MailboxDatabaseCopy 를 선택합니다
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy 를 선택합니다
- 업데이트 - MailboxDatabaseCopy

Windows Server 2012 이상에서 **GMSA**를 구성합니다

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항 및 사이징 요구 사항을 숙지해야 합니다.

항목	요구 사항
운영 체제	Microsoft Windows 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB

항목	요구 사항
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	• Microsoft .NET Framework 4.5.2 이상 • WMF(Windows Management Framework) 4.0 이상 • PowerShell 4.0 이상 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

Windows용 SnapCenter 플러그인의 자격 증명을 설정합니다

SnapCenter는 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다. 플러그인 패키지를 설치하기 위한 자격 증명과 데이터베이스에서 데이터 보호 작업을 수행하기 위한 추가 자격 증명을 만들어야 합니다.

- 이 작업에 대한 정보 *

Windows 호스트에 플러그인을 설치하기 위한 자격 증명을 설정해야 합니다. 호스트를 구축하고 플러그인을 설치한 후 Windows에 대한 자격 증명을 생성할 수 있지만, 호스트를 구축하고 플러그인을 설치하기 전에 SVM을 추가한 후에 자격 증명을 생성하는 것이 가장 좋습니다.

원격 호스트에 대한 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정합니다.

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

- 단계 *
  1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
  2. 설정 페이지에서 * 자격 증명 * 을 클릭합니다.
  3. 새로 만들기 * 를 클릭합니다.

     자격 증명 창이 표시됩니다.

  4. 자격 증명 페이지에서 다음을 실행합니다.

이 필드의 내용...	수행할 작업...
자격 증명 이름입니다	자격 증명의 이름을 입력합니다.
사용자 이름	인증에 사용되는 사용자 이름을 입력합니다. • 도메인 관리자 또는 관리자 그룹의 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹의 구성원을 지정합니다. 사용자 이름 필드에 유효한 형식은 다음과 같습니다. ◦ 'NetBIOS\사용자 이름' ◦ Domain FQDN\username'입니다 • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우 SnapCenter 플러그인을 설치할 시스템에 기본 제공 로컬 관리자를 지정합니다. 사용자 계정에 상승된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 올바른 형식은 '사용자 이름 '입니다
암호	인증에 사용되는 암호를 입력합니다.
인증	인증 모드로 Windows를 선택합니다.

5. 확인 * 을 클릭합니다.

Windows Server 2012 이상에서 GMSA를 구성합니다

Windows Server 2012 이상을 사용하면 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 GMSA(Managed Service Account)를 만들 수 있습니다.

- 필요한 것 *
- 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 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

      1. 호스트에서 구성된 GMSA에 관리 권한을 할당합니다.

      2. SnapCenter 서버에서 구성된 GMSA 계정을 지정하여 Windows 호스트를 추가합니다.

SnapCenter 서버는 선택한 플러그인을 호스트에 설치하고 지정된 GMSA는 플러그인 설치 중에 서비스 로그온 계정으로 사용됩니다.

호스트를 추가하고 **Exchange**용 플러그인을 설치합니다

SnapCenter * 호스트 추가 * 페이지를 사용하여 Windows 호스트를 추가할 수 있습니다. Exchange용 플러그인은 지정된 호스트에 자동으로 설치됩니다. 이는 플러그인을 설치하는 데 권장되는 방법입니다. 호스트를 추가하고 개별 호스트 또는 클러스터에 대한 플러그인을 설치할 수 있습니다.

- 필요한 것 *
- 플러그인 설치 및 제거 권한이 있는 역할(예: SnapCenter 관리자)에 할당된 사용자여야 합니다
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에 속한 경우 호스트에서 UAC를 비활성화해야 합니다.
- 메시지 큐 서비스가 실행되고 있어야 합니다.
- 그룹 GMSA(Managed Service Account)를 사용하는 경우 관리자 권한으로 GMSA를 구성해야 합니다. 자세한 내용은 을 참조하십시오"Windows Server 2012 이상에서 그룹 관리 서비스 계정을 구성합니다".
- 이 작업에 대한 정보 *

SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.

호스트를 추가하고 개별 호스트 또는 클러스터에 대한 플러그인 패키지를 설치할 수 있습니다. 클러스터(Exchange DAG)에 플러그인을 설치하는 경우 일부 노드에 NetApp LUN에 데이터베이스가 없는 경우에도 클러스터의 모든 노드에 플러그인이 설치됩니다.

Exchange용 플러그인은 Windows용 SnapCenter 플러그인 패키지에 따라 다르며 버전이 같아야 합니다. Exchange용 플러그인 설치 중에 Windows용 SnapCenter 플러그인 패키지가 기본적으로 선택되어 있으며 VSS 하드웨어 공급자와 함께 설치됩니다.

Microsoft Exchange Server용 SnapManager와 Windows용 SnapDrive가 이미 설치되어 있는 경우 Exchange용 플러그인을 동일한 Exchange Server에 설치하려면 Exchange용 플러그인 및 Windows용 SnapCenter 플러그인 패키지와 함께 설치된 VSS 하드웨어 공급자와 호환되지 않으므로 Windows용 SnapDrive에서 사용하는 VSS 하드웨어 공급자를 등록 취소해야 합니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 맨 위에 * Managed Hosts * 가 선택되어 있는지 확인합니다.
3. 추가 * 를 클릭합니다.
4. 호스트 * 페이지에서 다음을 수행합니다.

이 필드의 내용...	수행할 작업...
호스트 유형	호스트 유형으로 * Windows * 를 선택합니다. SnapCenter 서버는 호스트를 추가한 다음 호스트에 Windows용 플러그인 및 Exchange용 플러그인이 설치되어 있지 않은 경우 호스트에 설치합니다. Windows용 플러그인과 Exchange용 플러그인은 동일한 버전이어야 합니다. 다른 버전의 Windows용 플러그인이 이전에 설치된 경우 SnapCenter는 설치 과정에서 버전을 업데이트합니다.
호스트 이름입니다	FQDN(정규화된 도메인 이름) 또는 호스트의 IP 주소를 입력합니다. SnapCenter는 DNS의 올바른 구성에 따라 달라집니다. 따라서 가장 좋은 방법은 FQDN(정규화된 도메인 이름)을 입력하는 것입니다. IP 주소는 FQDN으로 확인되는 경우에만 신뢰할 수 없는 도메인 호스트에 대해 지원됩니다. 다음 중 하나의 IP 주소 또는 FQDN을 입력할 수 있습니다. • 독립 실행형 호스트 • Exchange DAG SnapCenter를 사용하여 호스트를 추가하고 이 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다. DAG 클러스터 노드 중 하나의 IP 주소 또는 FQDN을 제공하여 IP 리스 DAG 클러스터를 추가할 수도 있습니다.
자격 증명	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성합니다. 자격 증명에 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 만들기에 대한 정보를 참조하십시오. 지정한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다. ⓘ 자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 의해 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

   Exchange용 플러그인을 선택하면 Microsoft SQL Server용 SnapCenter 플러그인 선택이 자동으로 취소됩니다. 사용된 메모리 양과 Exchange에 필요한 기타 리소스 사용 때문에 SQL Server와 Exchange Server를 동일한 시스템에 설치하지 않는 것이 좋습니다.

6. (선택 사항) * 추가 옵션 * 을 클릭합니다.

이 필드의 내용...	수행할 작업...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정합니다. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트로 표시됩니다. 플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.
설치 경로	기본 경로는 'C:\Program Files\NetApp\SnapCenter'입니다. 선택적으로 경로를 사용자 지정할 수 있습니다.
DAG의 모든 호스트를 추가합니다	DAG를 추가할 때 이 확인란을 선택합니다.
사전 설치 검사를 건너뜁니다	플러그인이 이미 수동으로 설치되어 있고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.
그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행합니다	그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행하려면 이 확인란을 선택합니다. GMSA 이름을 *domainName\accountName$* 형식으로 제공합니다. GMSA는 SnapCenter Plug-in for Windows 서비스에 대해서만 로그온 서비스 계정으로 사용됩니다.

7. 제출 * 을 클릭합니다.

   사전 검사 건너뛰기 확인란을 선택하지 않은 경우 호스트가 플러그인을 설치하기 위한 요구사항을 충족하는지 여부를 확인합니다. 최소 요구 사항이 충족되지 않으면 적절한 오류 또는 경고 메시지가 표시됩니다.

   이 오류가 디스크 공간 또는 RAM과 관련된 경우 'C:\Program Files\NetApp\SnapCenter' WebApp에 있는

web.config 파일을 업데이트하여 기본값을 수정할 수 있습니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.

> HA 설정에서 web.config 파일을 업데이트하는 경우 두 노드에서 파일을 업데이트해야 합니다.

1. 설치 과정을 모니터링합니다.

PowerShell cmdlet을 사용하여 SnapCenter Server 호스트에서 Exchange용 플러그인을 설치합니다

SnapCenter GUI에서 Exchange용 플러그인을 설치해야 합니다. GUI를 사용하지 않으려는 경우 SnapCenter 서버 호스트 또는 원격 호스트에서 PowerShell cmdlet을 사용할 수 있습니다.

- 필요한 것 *
- SnapCenter 서버가 설치 및 구성되어 있어야 합니다.
- 호스트 또는 관리 권한이 있는 사용자의 로컬 관리자여야 합니다.
- 플러그인, 설치 및 제거 권한이 있는 역할(예: SnapCenter 관리자)에 할당된 사용자여야 합니다
- Exchange용 플러그인을 설치하기 전에 설치 요구 사항 및 지원되는 구성 유형을 검토해야 합니다.
- Exchange용 플러그인을 설치할 호스트는 Windows 호스트여야 합니다.
- 단계 *

  1. SnapCenter 서버 호스트에서 _Open-SmConnection_cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
  2. 필요한 매개 변수와 함께 _Add-SmHost_cmdlet을 사용하여 Exchange용 플러그인을 설치할 호스트를 추가합니다.

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

호스트는 독립 실행형 호스트 또는 DAG일 수 있습니다. DAG를 지정하는 경우 _-IsDAG_매개 변수가 필요합니다.

1. 필요한 매개 변수와 함께 _Install-SmHostPackage_cmdlet을 사용하여 Exchange용 플러그인을 설치합니다.

   이 명령은 지정된 호스트에 Exchange용 플러그인을 설치한 다음 SnapCenter에 플러그인을 등록합니다.

명령줄에서 Exchange용 SnapCenter 플러그인을 자동으로 설치합니다

SnapCenter 사용자 인터페이스 내에서 Exchange용 플러그인을 설치해야 합니다. 그러나 어떤 이유로 인해 Windows 명령줄에서 자동 모드로 Exchange용 플러그인 설치 프로그램을 실행할 수 없습니다.

- 필요한 것 *
- Microsoft Exchange Server 리소스를 백업해야 합니다.
- SnapCenter 플러그인 패키지를 설치해야 합니다.

- 설치하기 전에 Microsoft SQL Server용 SnapCenter 플러그인의 이전 릴리즈를 삭제해야 합니다.

  자세한 내용은 을 참조하십시오 "플러그인 호스트에서 직접 SnapCenter 플러그인을 설치하는 방법".

- 단계 *

  1. 플러그인 호스트에 _C:\temp_folder가 있고 로그인한 사용자가 이 폴더에 대한 모든 액세스 권한을 가지고 있는지 확인합니다.
  2. C:\ProgramData\NetApp\SnapCenter\Package_Repository에서 Microsoft Windows용 SnapCenter 플러그인을 다운로드하십시오.

     이 경로는 SnapCenter 서버가 설치된 호스트에서 액세스할 수 있습니다.

  3. 플러그인을 설치할 호스트에 설치 파일을 복사합니다.
  4. 로컬 호스트의 Windows 명령 프롬프트에서 플러그인 설치 파일을 저장한 디렉토리로 이동합니다.
  5. 다음 명령을 입력하여 변수가 데이터로 교체되도록 설치합니다.

     _snapcenter_windows_host_plugin.exe" /silent/debuglog"<Debug_Log_Path>"/log"<Log_Path>"BI_SNAPCENTER_PORT=<Num>Suite_INSTALLDIR="<Install_Directory_Path>"BI_ServiceAccount=<domain\administrator>BI_SERVICEPSCE=<설치 암호>

     예를 들면 다음과 같습니다.

     _C:\ProgramData\NetApp\SnapCenter\Package Repository\snapcenter_windows_host_plugin.exe" /silent/debuglog "C:\HPPW_SCSQL_Install.log" /log" C:\temp "BI_SNAPCENTER_port=8145 Suite_INSTALLDIR="C:\Program Files\NetApp\SCVICE_PVICE.PCEWE_PCEBI 관리자, PVICE_PVICE_PCEWESTRW=PCEBI_PCEPCEPCEWE_PSHI=설치

     ⓘ Exchange용 플러그인을 설치하는 동안 전달되는 모든 매개 변수는 대/소문자를 구분합니다.

     a. _/silent/debuglog "C:\Installdebug.log" /log "C:\temp" BI_SNAPCENTER_PORT=8145 Suite_INSTALLDIR="C:\Program Files" BI_ServiceAccount=demo\administrator BI_SERVICEPWD=Netapp1! ISFeatureInstall = HPPW, SCW _

        변수에 대해 다음 값을 입력합니다.

변수	값
_ /debuglog "<Debug_Log_Path> _	다음 예제와 같이 제품군 설치 관리자 로그 파일의 이름과 위치를 지정합니다. *Setup.exe /debuglog "C:\PathToLog\setupexe.log*
Bi_SNAPCENTER_PORT	SnapCenter가 SMCore와 통신하는 포트를 지정합니다.
Suite_INSTALLDIR	호스트 플러그인 패키지 설치 디렉토리를 지정합니다.

변수	값
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.

1. Windows 작업 스케줄러, 기본 설치 로그 파일 *C:\Installdebug.log* 및 추가 설치 파일을 _C:\Temp_에서 모니터링합니다.
2. %temp%_ 디렉토리를 모니터링하여 _msiexe.exe_설치 프로그램이 오류 없이 소프트웨어를 설치하고 있는지 확인합니다.

> Exchange용 플러그인을 설치하면 SnapCenter 서버가 아닌 호스트에 플러그인이 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록할 수 있습니다. 호스트가 추가되면 플러그인이 자동으로 검색됩니다.

SnapCenter 플러그인 패키지 설치 상태를 모니터링합니다

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행률을 모니터링할 수 있습니다. 설치 진행 상황을 확인하여 설치 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

- 이 작업에 대한 정보 *

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. 플러그인 설치 작업만 나열되도록 * 작업 * 페이지에서 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.

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.

이 마법사 창에서...	다음을 수행합니다.
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, *.p7b).

7. "개인" 폴더에 대해 5단계를 반복합니다.

CA 인증서 지문을 받습니다

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

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

        예를 들어, 썸프린트가 "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 0d 42 77 A3 2a 7b"인 경우 공백을 제거한 후 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.
  2. PowerShell에서 다음을 수행합니다.
     a. 다음 명령을 실행하여 설치된 인증서의 엄지손가락 지문을 나열하고 최근 설치된 인증서를 주체 이름으로 식별합니다.

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

     b. 엄지손가락 지문을 복사합니다.

Windows 호스트 플러그인 서비스를 사용하여 **CA** 인증서를 구성합니다

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

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

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

     ">netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>"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"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$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.

- 필요한 것 *
- run_Set-SmCertificateSettings_cmdlet을 사용하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- _get-SmCertificateSettings_를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

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

- 단계 *
  1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
  2. 호스트 페이지에서 * 관리되는 호스트 * 를 클릭합니다.
  3. 단일 또는 여러 플러그인 호스트를 선택합니다.
  4. 추가 옵션 * 을 클릭합니다.
  5. 인증서 유효성 검사 사용 * 을 선택합니다.
- 완료 후 *

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

- 🔒 는 CA 인증서가 활성화되지 않았으며 플러그인 호스트에 할당되지 않았음을 나타냅니다.

- CA 인증서의 유효성을 확인했음을 나타냅니다.
- CA 인증서의 유효성을 확인할 수 없음을 나타냅니다.
- 연결 정보를 검색할 수 없음을 나타냅니다.

> 상태가 노란색 또는 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

Exchange 및 **SnapCenter**에 대해 **SnapManager 7.x**가 공존하도록 구성합니다

Microsoft Exchange Server용 SnapCenter 플러그인을 Microsoft Exchange Server용 SnapManager와 함께 사용하려면 Microsoft Exchange Server용 SnapManager가 설치된 동일한 Exchange Server에 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하고 Exchange 일정에 대해 SnapManager를 사용하지 않도록 설정해야 합니다. 및 Microsoft Exchange Server용 SnapCenter 플러그인을 사용하여 새 일정 및 백업을 구성합니다.

- 필요한 것 *
- Microsoft Exchange Server용 SnapManager와 Windows용 SnapDrive가 이미 설치되어 있고 Microsoft Exchange Server용 SnapManager 백업이 시스템과 SnapInfo 디렉토리에 있습니다.
- 더 이상 필요하지 않은 Microsoft Exchange Server용 SnapManager에서 생성한 백업을 삭제하거나 회수해야 합니다.
- Windows 스케줄러에서 Microsoft Exchange Server용 SnapManager가 만든 모든 일정을 일시 중단하거나 삭제해야 합니다.
- Microsoft Exchange Server용 SnapCenter 플러그인과 Microsoft Exchange Server용 SnapManager가 동일한 Exchange Server에 공존할 수 있지만 기존 Microsoft Exchange Server용 SnapManager 설치를 SnapCenter로 업그레이드할 수는 없습니다.

  SnapCenter는 업그레이드 옵션을 제공하지 않습니다.

- SnapCenter는 SnapManager for Microsoft Exchange Server 백업에서 Exchange 데이터베이스 복원을 지원하지 않습니다.

  Microsoft Exchange Server용 SnapCenter 플러그인 설치 후 Microsoft Exchange Server용 SnapManager를 제거하지 않고 나중에 Microsoft Exchange Server용 SnapManager 백업을 복원하려면 추가 단계를 수행해야 합니다.

- 단계 *

  1. 모든 DAG 노드에서 PowerShell을 사용하여 SnapDrive for Windows VSS Hardware Provider가 등록되었는지 여부를 확인합니다. _ vssadmin list providers _

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
   Provider type: Hardware
   Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
   Version: 7. 1. 4. 6845
```

2. SnapDrive 디렉토리에서 SnapDrive for Windows에서 VSS 하드웨어 공급자 등록을 취소합니다. *navssprv.exe -r service –u*
3. VSS Hardware Provider가 제거되었는지 확인합니다. _ vssadmin list providers _
4. SnapCenter에 Exchange 호스트를 추가한 다음 Microsoft Windows용 SnapCenter 플러그인 및 Microsoft Exchange Server용 SnapCenter 플러그인을 설치합니다.
5. 모든 DAG 노드의 Microsoft Windows용 SnapCenter 플러그인 디렉토리에서 VSS 하드웨어 공급자가 등록되었는지 확인합니다. *vssadmin list providers*

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
   Provider type: Hardware
   Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
   Version: 7. 0. 0. 5561
```

6. Microsoft Exchange Server 백업 일정에 대한 SnapManager를 중지합니다.
7. SnapCenter GUI를 사용하여 필요 시 백업을 생성하고, 예약된 백업을 구성하고, 보존 설정을 구성합니다.
8. Microsoft Exchange Server용 SnapManager를 제거합니다.

   Microsoft Exchange Server용 SnapManager를 지금 제거하지 않고 나중에 Microsoft Exchange Server용 SnapManager 백업을 복원하려는 경우:

   a. 모든 DAG 노드에서 Microsoft Exchange Server용 SnapCenter 플러그인 등록 취소: _navssprv.exe -r service -u _

   ```
   C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for
   Microsoft Windows>navssprv.exe -r service -u
   ```

   b. C:\Program Files\NetApp\SnapDrive_ 디렉토리에서 모든 DAG 노드에 SnapDrive for Windows를 등록합니다. _navssprv.exe -r service -a hostname \\username -p password _

VMware vSphere용 SnapCenter 플러그인을 설치합니다

데이터베이스가 가상 머신(VM)에 저장되어 있거나 VM 및 데이터 저장소를 보호하려는 경우 SnapCenter Plug-in for VMware vSphere 가상 어플라이언스를 구축해야 합니다.

배포에 대한 자세한 내용은 을 참조하십시오 "구축 개요".

CA 인증서를 배포합니다

VMware vSphere용 SnapCenter 플러그인을 사용하여 CA 인증서를 구성하려면 를 참조하십시오 "SSL 인증서를 생성하거나 가져옵니다".

CRL 파일을 구성합니다

VMware vSphere용 SnapCenter 플러그인은 사전 구성된 디렉토리에서 CRL 파일을 찾습니다. VMware vSphere용 SnapCenter 플러그인의 기본 CRL 파일 디렉토리는 */opt/netapp/config/CRL* 입니다.

이 디렉터리에 둘 이상의 CRL 파일을 배치할 수 있습니다. 들어오는 인증서는 각 CRL에 대해 확인됩니다.

데이터 보호를 준비합니다

백업, 클론 복제 또는 복원 작업과 같은 데이터 보호 작업을 수행하기 전에 전략을 정의하고 환경을 설정해야 합니다. SnapVault 서버에서 SnapMirror 및 SnapCenter 기술을 사용하도록 설정할 수도 있습니다.

SnapVault 및 SnapMirror 기술을 활용하려면 스토리지 장치의 소스 볼륨과 타겟 볼륨 간의 데이터 보호 관계를 구성하고 초기화해야 합니다. NetAppSystem Manager를 사용하거나 스토리지 콘솔 명령줄을 사용하여 이러한 작업을 수행할 수 있습니다.

- 자세한 정보 찾기 *

"REST API 시작하기"

Microsoft Exchange Server용 SnapCenter 플러그인 사용을 위한 사전 요구 사항

Exchange용 플러그인을 사용하기 전에 SnapCenter 관리자가 SnapCenter 서버를 설치 및 구성하고 필수 작업을 수행해야 합니다.

- SnapCenter 서버를 설치하고 구성합니다.
- SnapCenter에 로그인합니다.
- 스토리지 시스템 접속을 추가하거나 할당하고 자격 증명을 생성하여 SnapCenter 환경을 구성합니다.

> SnapCenter은 서로 다른 클러스터에서 동일한 이름의 여러 SVM을 지원하지 않습니다. SnapCenter에서 지원하는 각 SVM에는 고유한 이름이 있어야 합니다.

- 호스트를 추가하고, Microsoft Windows용 SnapCenter 플러그인 및 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하고, 리소스를 검색(새로 고침)합니다.
- Microsoft Windows용 SnapCenter 플러그인을 사용하여 호스트 측 스토리지 프로비저닝을 수행합니다.

- SnapCenter 서버를 사용하여 VMware RDM LUN에 상주하는 Exchange 데이터베이스를 보호하는 경우 VMware vSphere용 SnapCenter 플러그인을 구축하고 SnapCenter에 플러그인을 등록해야 합니다. 자세한 내용은 VMware vSphere용 SnapCenter 플러그인 설명서를 참조하십시오.

  VMDK는 지원되지 않습니다.

- Microsoft Exchange 도구를 사용하여 로컬 디스크에서 지원되는 스토리지로 기존 Microsoft Exchange Server 데이터베이스를 이동합니다.
- 백업 복제를 원하는 경우 SnapMirror 및 SnapVault 관계를 설정합니다.

SnapCenter 4.1.1 사용자의 경우 VMware vSphere 4.1.1 용 SnapCenter 플러그인 설명서에 가상화 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 나와 있습니다. SnapCenter 4.2.x 사용자, NetApp Data Broker 1.0 및 1.0.1의 경우, Linux 기반 NetApp Data Broker 가상 어플라이언스(Open Virtual Appliance 형식)에서 제공하는 VMware vSphere용 SnapCenter 플러그인을 사용하여 가상화된 데이터베이스 및 파일 시스템을 보호하는 방법에 대한 정보가 수록되어 있습니다. SnapCenter 4.3.x 사용자의 경우 SnapCenter Plug-in for VMware vSphere 4.3 설명서에는 Linux 기반 SnapCenter Plug-in for VMware vSphere 가상 어플라이언스(오픈 가상 어플라이언스 형식)를 사용하여 가상화된 데이터베이스와 파일 시스템을 보호하는 방법에 대한 정보가 수록되어 있습니다.

"VMware vSphere용 SnapCenter 플러그인 설명서"

리소스, 리소스 그룹 및 정책을 사용하여 **Exchange Server**를 보호하는 방법

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

- 리소스는 일반적으로 SnapCenter를 사용하여 백업하는 메일박스 데이터베이스 또는 Microsoft Exchange DAG(데이터베이스 가용성 그룹)입니다.
- SnapCenter 리소스 그룹은 호스트 또는 Exchange DAG의 리소스 모음이며 리소스 그룹에는 전체 DAG 또는 개별 데이터베이스가 포함될 수 있습니다.

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

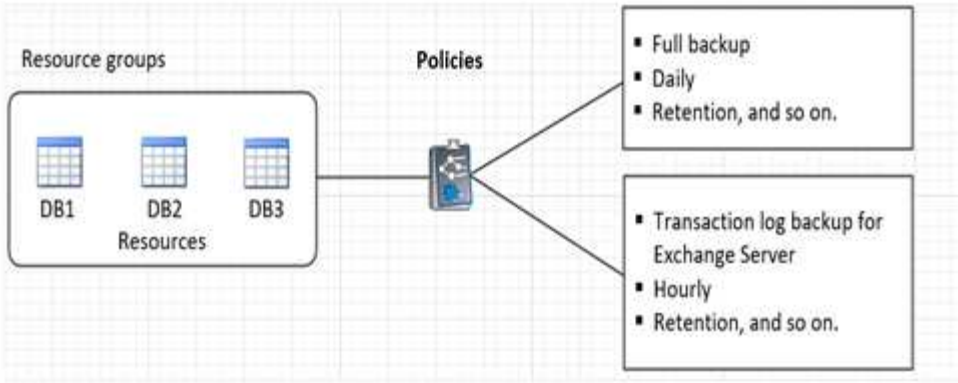
  필요에 따라 단일 리소스 또는 리소스 그룹을 백업할 수 있습니다. 단일 리소스 및 리소스 그룹에 대해 예약된 백업을 수행할 수도 있습니다.

  리소스 그룹은 이전에 데이터 세트라고 했습니다.

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

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

보호하려는_대상_과 이를 보호할 시기를 요일과 시간으로 정의하는 자원 그룹을 생각해 보십시오. 정책을 정의하는 _ 방법 _ 을(를) 보호하려는 것으로 생각해 보십시오. 예를 들어, 호스트의 모든 데이터베이스를 백업하는 경우 호스트의 모든 데이터베이스를 포함하는 리소스 그룹을 생성할 수 있습니다. 그런 다음 리소스 그룹에 일별 정책과 시간별 정책이라는 두 가지 정책을 연결할 수 있습니다. 리소스 그룹을 생성하고 정책을 연결할 때 매일 전체 백업을 수행하고 로그 백업을 매시간 수행하는 다른 일정을 수행하도록 리소스 그룹을 구성할 수 있습니다. 다음 그림에서는 데이터베이스 리소스, 리소스 그룹 및 정책 간의 관계를 보여 줍니다.



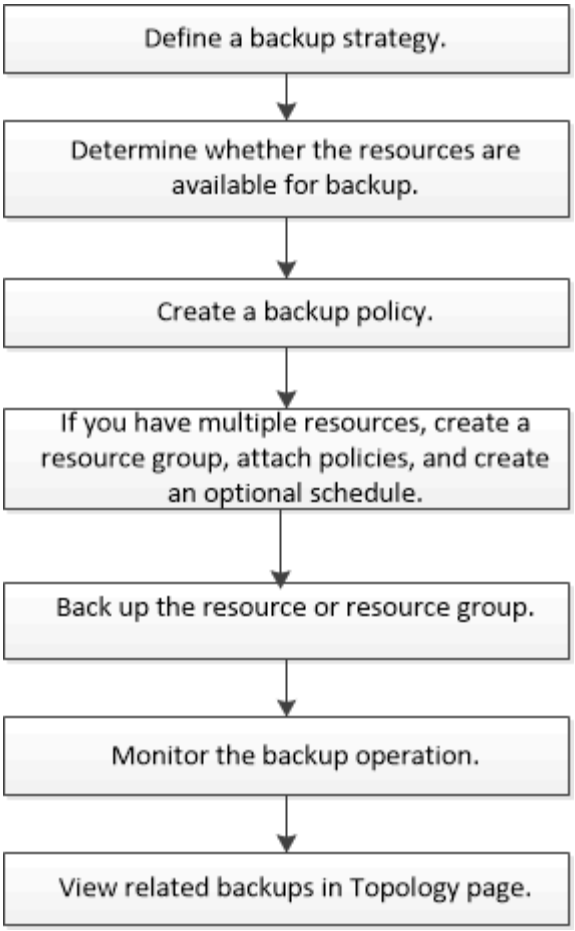
Exchange 리소스를 백업합니다

백업 워크플로우

사용자 환경에 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하면 SnapCenter를 사용하여 Exchange 리소스를 백업할 수 있습니다.

여러 서버에서 동시에 실행되도록 여러 백업을 예약할 수 있습니다. 동일한 리소스에서 백업 및 복원 작업을 동시에 수행할 수 없습니다. 동일한 볼륨의 액티브 및 패시브 백업 복사본은 지원되지 않습니다.

다음 워크플로에서는 백업 작업을 수행해야 하는 순서를 보여 줍니다.



Exchange 데이터베이스 및 백업 검증

Microsoft Exchange Server용 SnapCenter 플러그인은 백업 검증을 제공하지 않지만 Exchange와 함께 제공되는 Eseutil 도구를 사용하여 Exchange 데이터베이스 및 백업을 확인할 수 있습니다.

Microsoft Exchange Eseutil 도구는 Exchange 서버에 포함된 명령줄 유틸리티입니다. 이 유틸리티를 사용하면 정합성 검사를 수행하여 Exchange 데이터베이스 및 백업의 무결성을 확인할 수 있습니다.

* 모범 사례: * 적어도 두 개 이상의 복제본이 있는 DAG(데이터베이스 가용성 그룹) 구성의 일부인 데이터베이스에 대해 일관성 검사를 수행할 필요는 없습니다.

자세한 내용은 을 참조하십시오 "Microsoft Exchange Server 설명서를 참조하십시오".

Exchange 리소스를 백업에 사용할 수 있는지 여부를 확인합니다

리소스는 사용자가 설치한 플러그인에서 유지 관리하는 데이터베이스, Exchange 데이터베이스 가용성 그룹입니다. 이러한 리소스를 리소스 그룹에 추가하여 데이터 보호 작업을 수행할 수 있지만 먼저 사용 가능한 리소스를 확인해야 합니다. 사용 가능한 리소스를 확인하면 플러그인 설치가 성공적으로 완료되었는지 확인할 수도 있습니다.

- 필요한 것 *

- SnapCenter 서버 설치, 호스트 추가, 스토리지 시스템 접속 생성, 자격 증명 추가 및 Exchange용 플러그인 설치와 같은 작업을 이미 완료해야 합니다.
- Single Mailbox Recovery 소프트웨어 기능을 사용하려면 Single Mailbox Recovery 소프트웨어가 설치된 Exchange Server에 활성 데이터베이스를 설치해야 합니다.
- 데이터베이스가 VMware RDM LUN에 상주하는 경우 VMware vSphere용 SnapCenter 플러그인을 구축하고 SnapCenter에 플러그인을 등록해야 합니다. 를 클릭합니다 "VMware vSphere용 SnapCenter 플러그인 설명서" 자세한 정보가 있습니다.
- 이 작업에 대한 정보 *
- Details 페이지의 * Overall Status * 옵션이 Not Available for backup으로 설정되어 있으면 데이터베이스를 백업할 수 없습니다. 다음 중 하나라도 해당하면 * Overall Status *(전체 상태 *) 옵션이 Not Available(백업 불가)로 설정됩니다.
  - 데이터베이스가 NetApp LUN에 없습니다.
  - 데이터베이스가 정상 상태가 아닙니다.

    데이터베이스가 마운트, 마운트 해제, 다시 시드되거나 복구 보류 상태인 경우 정상 상태가 아닙니다.
- DAG(Database Availability Group)가 있는 경우 DAG에서 백업 작업을 실행하여 그룹의 모든 데이터베이스를 백업할 수 있습니다.
- 단계 *

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 리소스 페이지의 왼쪽 위 모서리에 있는 플러그인 드롭다운 목록에서 * Microsoft Exchange Server * 를 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 * 데이터베이스 * 또는 * 데이터베이스 가용성 그룹 * 또는 * 리소스 그룹 * 을 선택합니다.

   을 클릭합니다 호스트 이름과 Exchange Server를 선택하여 리소스를 필터링합니다. 그런 다음 을 클릭할 수 있습니다 를 눌러 필터 창을 닫습니다.
3. 리소스 새로 고침 * 을 클릭합니다.

   새로 추가, 이름 변경 또는 삭제된 리소스가 SnapCenter 서버 인벤토리로 업데이트됩니다.

   리소스는 리소스 이름, 데이터베이스 가용성 그룹 이름, 데이터베이스가 현재 활성 상태인 서버, 복제본이 있는 서버, 마지막 백업 시간 및 전체 상태 등의 정보와 함께 표시됩니다.

   - 데이터베이스가 비 NetApp 스토리지에 있는 경우 백업을 사용할 수 없음 이 전체 상태 열에 표시됩니다.

     DAG에서 액티브 데이터베이스 복제본이 타사 스토리지에 있고 하나 이상의 패시브 데이터베이스 복제본이 NetApp 스토리지에 있는 경우 보호되지 않음 이 * Overall Status * 열에 표시됩니다.

NetApp이 아닌 스토리지 유형에 있는 데이터베이스에는 데이터 보호 작업을 수행할 수 없습니다.

- 데이터베이스가 NetApp 스토리지에 있고 보호되지 않는 경우 * Overall Status * 열에 보호되지 않음 이 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있고 보호되어 있는 경우 사용자 인터페이스에 **Overall Status** 열에 Backup not run 메시지가 표시됩니다.
- 데이터베이스가 NetApp 스토리지 시스템에 있으며 보호되어 있고 데이터베이스에 대한 백업이 트리거된 경우 사용자 인터페이스에 * Overall Status * 열에 Backup Succeeded 메시지가 표시됩니다.

Exchange Server 데이터베이스에 대한 백업 정책을 생성합니다

SnapCenter를 사용하여 Microsoft Exchange Server 리소스를 백업하기 전에 Exchange 리소스 또는 리소스 그룹에 대한 백업 정책을 만들거나 리소스 그룹을 만들거나 단일 리소스를 백업할 때 백업 정책을 만들 수 있습니다.

- 필요한 것 *
- 데이터 보호 전략을 정의해야 합니다.

  자세한 내용은 Exchange 데이터베이스에 대한 데이터 보호 전략 정의에 대한 정보를 참조하십시오.

- SnapCenter 설치, 호스트 추가, 리소스 식별 및 스토리지 시스템 접속 생성과 같은 작업을 완료하여 데이터 보호를 위한 준비를 갖추어야 합니다.
- Exchange Server 리소스를 새로 고친(검색된) 상태여야 합니다.
- 스냅샷 복사본을 미러 또는 볼트에 복제하는 경우 SnapCenter 관리자는 소스 볼륨과 타겟 볼륨 모두에 SVM(스토리지 가상 머신)을 할당해야 합니다.
- powershell 스크립트를 p규정된 ppts 및 postscripts로 실행하려면 web.config 파일에서 usePowershellProcessforScripts 매개 변수의 값을 true로 설정해야 합니다.

  기본값은 false 입니다

- 이 작업에 대한 정보 *

백업 정책은 백업을 관리 및 유지하는 방법과 리소스 또는 리소스 그룹을 백업하는 빈도를 제어하는 규칙의 집합입니다. 또한 스크립트 설정을 지정할 수도 있습니다. 정책에 옵션을 지정하면 다른 리소스 그룹에 대한 정책을 다시 사용할 때 시간이 절약됩니다.

전체 백업 보존은 특정 정책에 따라 다릅니다. 정책 A를 사용하여 전체 백업 보존 기간이 4인 데이터베이스 또는 리소스는 전체 백업 4개를 보유하며 동일한 데이터베이스 또는 리소스에 대해 정책 B에 영향을 미치지 않습니다. 이 경우 3개의 전체 백업을 유지하기 위해 보존 기간이 3일 수 있습니다.

로그 백업 보존은 정책에 따라 효과적이며 데이터베이스 또는 리소스의 모든 로그 백업에 적용됩니다. 따라서 정책 B를 사용하여 전체 백업을 수행할 경우 로그 보존 설정은 정책 A가 동일한 데이터베이스 또는 리소스에 생성한 로그 백업에 영향을 줍니다. 마찬가지로 정책 A의 로그 보존 설정은 정책 B가 동일한 데이터베이스의 로그 백업에 영향을 줍니다.

* 모범 사례: * 보존하려는 전체 및 로그 백업 수에 따라 보조 보존 정책을 구성하는 것이 좋습니다. 2차 보존 정책을 구성할 때는 데이터베이스와 로그가 서로 다른 볼륨에 있을 때 각 백업마다 3개의 스냅샷 복사본을 가질 수 있고 데이터베이스와 로그가 같은 볼륨에 있을 때는 각 백업마다 2개의 스냅샷 복사본을 가질 수 있다는 점을 유의해야 합니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
  2. 설정 페이지에서 * 정책 * 을 클릭합니다.
  3. 새로 만들기 * 를 클릭합니다.
  4. 이름 페이지에서 정책 이름 및 설명을 입력합니다.
  5. 백업 유형 페이지에서 다음 단계를 수행하십시오.

a. 백업 유형 선택:

원하는 작업	수행할 작업...
데이터베이스 파일 및 필요한 트랜잭션 로그를 백업합니다	전체 백업 및 로그 백업 * 을 선택합니다. 데이터베이스는 로그 잘라내기를 통해 백업되며 잘린 로그를 포함하여 모든 로그가 백업됩니다. ⓘ 권장되는 백업 유형입니다.
데이터베이스 파일 및 커밋되지 않은 트랜잭션 로그를 백업합니다	전체 백업 * 을 선택합니다. 데이터베이스는 로그 잘라내기를 통해 백업되며 잘린 로그는 백업되지 않습니다.
모든 트랜잭션 로그를 백업합니다	Log backup * 을 선택합니다. 활성 파일 시스템의 모든 트랜잭션 로그가 백업되며 로그 잘라내기가 없습니다. _scebackupinfo_directory가 라이브 로그와 동일한 디스크에 생성됩니다. 이 디렉토리에는 Exchange 데이터베이스의 증가분 변경 사항에 대한 포인터가 포함되어 있으며 전체 로그 파일과 동일하지는 않습니다.
트랜잭션 로그 파일을 자르지 않고 모든 데이터베이스 파일 및 트랜잭션 로그를 백업합니다	백업 복사 * 를 선택합니다. 모든 데이터베이스 및 모든 로그가 백업되며 로그 잘라내기가 없습니다. 일반적으로 이 백업 유형을 사용하여 복제본을 다시 시드하거나 문제를 테스트 또는 진단할 수 있습니다.

ⓘ UTM(최신) 보존이 아닌 전체 백업 보존을 기준으로 로그 백업에 필요한 공간을 정의해야 합니다.

ⓘ Exchange 볼륨(LUN)을 처리할 때 로그 및 데이터베이스에 대해 별도의 볼트 정책을 생성하고 동일한 레이블을 사용하여 로그 정책의 유지(보존)를 데이터베이스 정책으로 각 레이블에 대해 두 배로 설정합니다. 자세한 내용은 다음을 참조하십시오. "Exchange 백업용 SnapCenter는 볼트 대상 로그 볼륨에 스냅샷의 절반만 유지합니다".

b. 데이터베이스 사용 가능 그룹 설정 섹션에서 작업을 선택합니다.

이 필드의 내용...	수행할 작업...
활성 복사본을 백업합니다	선택한 데이터베이스의 활성 사본만 백업하려면 이 옵션을 선택합니다. DAG(데이터베이스 가용성 그룹)의 경우 이 옵션은 DAG에 있는 모든 데이터베이스의 액티브 복제본만 백업합니다. 패시브 복사본은 백업되지 않습니다.
백업 작업 생성 시 선택할 서버의 복사본을 백업합니다	활성 서버와 수동 서버 모두에서 선택한 서버의 데이터베이스 복사본을 백업하려면 이 옵션을 선택합니다. DAG의 경우 이 옵션은 선택한 서버에 있는 모든 데이터베이스의 액티브 복제본과 패시브 복제본을 모두 백업합니다.

클러스터 구성에서 백업은 정책에 설정된 보존 설정에 따라 클러스터의 각 노드에 유지됩니다. 클러스터의 소유자 노드가 변경되면 이전 소유자 노드의 백업이 유지됩니다. 보존은 노드 레벨에서만 적용됩니다.

c. 일정 빈도 섹션에서 * On demand *, * Hourly *, * Daily *, * Weekly *, * Monthly * 등의 빈도 유형을 하나 이상 선택합니다.

리소스 그룹을 생성하는 동안 백업 작업의 스케줄(시작 날짜, 종료 날짜)을 지정할 수 있습니다. 이렇게 하면 동일한 정책 및 백업 빈도를 공유하는 리소스 그룹을 생성할 수 있지만 각 정책에 서로 다른 백업 스케줄을 할당할 수 있습니다.

오전 2시에 예약된 경우 DST(일광 절약 시간) 중에는 일정이 트리거되지 않습니다.

6. 보존 페이지에서 보존 설정을 구성합니다.

표시되는 옵션은 이전에 선택한 백업 유형 및 빈도 유형에 따라 달라집니다.

최대 보존 값은 ONTAP 9.4 이상의 리소스에 대해 1018이고, ONTAP 9.3 이전 버전의 리소스에 대해서는 254입니다. 보존이 기본 ONTAP 버전에서 지원하는 값보다 높은 값으로 설정된 경우 백업이 실패합니다.

SnapVault 복제를 설정하려면 보존 수를 2 이상으로 설정해야 합니다. 보존 횟수를 1로 설정하면 새 스냅샷 복사본이 타겟으로 복제될 때까지 첫 번째 스냅샷 복사본이 SnapVault 관계의 참조 스냅샷 복사본이므로 보존 작업이 실패할 수 있습니다.

a. 로그 백업 보존 설정 섹션에서 다음 중 하나를 선택합니다.

원하는 작업	수행할 작업...
특정 수의 로그 백업만 유지합니다	로그가 유지되는 전체 백업 수 * 를 선택하고 최신 복원 기능을 원하는 전체 백업 수를 지정합니다. UTM(최신) 보존은 전체 또는 로그 백업을 통해 생성된 로그 백업에 적용됩니다. 예를 들어, UTM 보존 설정이 마지막 5개의 전체 백업의 로그 백업을 유지하도록 구성된 경우 마지막 5개의 전체 백업의 로그 백업이 보존됩니다. 전체 및 로그 백업의 일부로 생성된 로그 폴더는 UTM의 일부로 자동으로 삭제됩니다. 로그 폴더는 수동으로 삭제할 수 없습니다. 예를 들어 전체 또는 전체 및 로그 백업의 보존 설정이 1개월로 설정되고 UTM 보존이 10일로 설정된 경우, UTM에 따라 이러한 백업의 일부로 생성된 로그 폴더가 삭제됩니다. 따라서 10일 로그 폴더만 있고 다른 모든 백업은 시점 복원으로 표시됩니다. 최신 복원을 수행하지 않으려는 경우 UTM 보존 값을 0으로 설정할 수 있습니다. 그러면 시점 복원 작업이 활성화됩니다. • 모범 사례: * 전체 백업 보존 설정 섹션의 전체 스냅샷 복사본(전체 백업) 설정과 같은 설정을 사용하는 것이 좋습니다. 이렇게 하면 각 전체 백업에 대해 로그 파일이 유지됩니다.
백업 사본을 특정 기간 동안 보관합니다	Keep log backups for Last * 옵션을 선택하고 로그 백업 사본을 보관할 일 수를 지정합니다. 전체 백업 일수까지 로그 백업이 보존됩니다.

백업 유형으로 * 로그 백업 * 을 선택한 경우 로그 백업은 전체 백업에 대한 최신 보존 설정의 일부로 보존됩니다.

b. 전체 백업 보존 설정 섹션에서 필요 시 백업에 대해 다음 중 하나를 선택한 다음 전체 백업에 대해 하나를 선택합니다.

이 필드의 내용...	수행할 작업...
특정 수의 스냅샷 복사본만 보유합니다	유지할 전체 백업 수를 지정하려면 * 유지할 총 스냅샷 복사본 * 옵션을 선택하고 유지할 스냅샷 복사본(전체 백업) 수를 지정합니다. 전체 백업 수가 지정된 수를 초과하면 지정된 수를 초과하는 전체 백업이 삭제되며 가장 오래된 복제본이 먼저 삭제됩니다.

이 필드의 내용...	수행할 작업...
특정 기간 동안 전체 백업을 보존합니다	스냅샷 복사본 보관 * 옵션을 선택하고 스냅샷 복사본을 보관할 일 수(전체 백업)를 지정합니다.

> DAG 구성에서 호스트에 대한 전체 백업이 없는 로그 백업만 있는 데이터베이스가 있는 경우 로그 백업은 다음과 같은 방식으로 유지됩니다.

- 기본적으로 SnapCenter는 DAG의 다른 모든 호스트에서 이 데이터베이스에 대해 가장 오래된 전체 백업을 찾고 전체 백업 전에 이 호스트에서 수행된 모든 로그 백업을 삭제합니다.
- DAG의 호스트에 있는 데이터베이스의 기본 보존 동작은 _C:\Program Files\NetApp\SnapCenter WebApp\web.config_file에 * MaxLogBackupOnlyWithoutFullBackup * 키를 추가하여 로그 백업만 사용하여 재정의할 수 있습니다.

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

이 예에서 값 10은 호스트에 최대 10개의 로그 백업을 유지하는 것을 의미합니다.

7. 복제 페이지에서 다음 보조 복제 옵션 중 하나 또는 둘 다를 선택합니다.

이 필드의 내용...	수행할 작업...
로컬 스냅샷 복사본을 생성한 후 SnapMirror를 업데이트합니다	백업 세트의 미러 복사본을 다른 볼륨(SnapMirror)에 유지하려면 이 옵션을 선택합니다.
로컬 스냅샷 복사본을 생성한 후 SnapVault를 업데이트합니다	디스크 간 백업 복제를 수행하려면 이 옵션을 선택합니다.
보조 정책 레이블입니다	스냅샷 레이블을 선택합니다. 선택한 스냅샷 복사본 레이블에 따라 ONTAP에서는 해당 레이블과 일치하는 2차 스냅샷 복사본 보존 정책을 적용합니다. 로컬 스냅샷 복사본 * 을 생성한 후 SnapMirror 업데이트 * 를 선택한 경우, 선택적으로 보조 정책 레이블을 지정할 수 있습니다. 그러나 로컬 스냅샷 복사본 * 을 생성한 후 * SnapVault 업데이트 * 를 선택한 경우에는 보조 정책 레이블을 지정해야 합니다.
오류 재시도 횟수입니다	프로세스가 중지되기 전에 수행해야 하는 복제 시도 횟수를 입력합니다.

> 보조 스토리지에 대한 ONTAP의 SnapMirror 보존 정책을 구성하면 보조 스토리지에서 스냅샷 복사본의 최대 제한에 도달하지 않도록 해야 합니다.

8. 스크립트 페이지에서 백업 작업 전후에 실행해야 하는 ppt 또는 postscript의 경로와 인수를 각각 입력합니다.
   - Prescript 백업 인수에는 ""$Database" 및 ""$ServerInstance" 가 포함됩니다.
   - 포스트스크립트 백업 인수에는 ""$Database", "$ServerInstance", "$BackupName", "$LogDirectory" 및 "$LogSnapshot""이 포함됩니다.

     스크립트를 실행하여 SNMP 트랩을 업데이트하고, 경고를 자동화하고, 로그를 보내는 등의 작업을 수행할 수 있습니다.
9. 요약을 검토하고 * Finish * 를 클릭합니다.

리소스 그룹을 생성하고 **Exchange Server**에 대한 정책을 연결합니다

모든 데이터 보호 작업에는 리소스 그룹이 필요합니다. 또한 수행할 데이터 보호 작업의 유형과 보호 스케줄을 정의하려면 하나 이상의 정책을 리소스 그룹에 연결해야 합니다.

- 단계 *

1. 왼쪽 탐색 창에서 * Resources * 를 클릭한 다음 목록에서 Microsoft Exchange Server 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 데이터베이스 * 를 선택합니다.

   > 최근에 SnapCenter에 리소스를 추가한 경우 * 리소스 새로 고침 * 을 클릭하여 새로 추가된 리소스를 확인합니다.

3. 새 리소스 그룹 * 을 클릭합니다.
4. 이름 페이지에서 다음 작업을 수행합니다.

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

이 필드의 내용...	수행할 작업...
스냅샷 복사본에 대해 사용자 지정 이름 형식을 사용합니다	선택 사항: 사용자 지정 스냅샷 복사본의 이름 및 형식을 입력합니다. 예를 들어, _customtext_resourcegroup_policy_hostname_or_resourcegroup_hostname_입니다. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.

5. 리소스 페이지에서 다음 단계를 수행하십시오.

   a. 사용 가능한 리소스 목록을 필터링하려면 리소스 유형과 드롭다운 목록에서 데이터베이스 사용 가능 그룹을 선택합니다.

   > 최근에 추가한 자원은 자원 목록을 새로 고친 후에만 사용 가능한 자원 목록에 나타납니다.

   Available Resources and Selected Resources 섹션에 호스트 이름과 함께 데이터베이스 이름이 표시됩니다. 이 호스트 이름은 데이터베이스가 특정 호스트에서 활성화되어 있으며 이 호스트에서 백업을 수행할 수 없음을 나타냅니다. 정책에서 백업 작업 생성 시 선택할 * 서버의 백업 복사본 * 옵션을 선택한 경우 백업할 서버 선택 옵션에서 하나 이상의 백업 서버를 선택해야 합니다.

   a. 검색 텍스트 상자에 리소스 이름을 입력하거나 스크롤하여 리소스를 찾습니다.

   b. 사용 가능한 리소스 섹션에서 선택한 리소스 섹션으로 리소스를 이동하려면 다음 단계 중 하나를 수행합니다.

      - 동일한 스토리지 볼륨에 있는 모든 리소스를 선택한 리소스 섹션으로 이동하려면 * 동일한 스토리지 볼륨에 있는 모든 리소스를 자동 선택 * 을 선택합니다.
      - 사용 가능한 리소스 섹션에서 리소스를 선택한 다음 오른쪽 화살표를 클릭하여 선택한 리소스 섹션으로 이동합니다.

        Microsoft Exchange Server용 SnapCenter의 리소스 그룹은 스냅샷 복사본당 30개 이상의 데이터베이스를 가질 수 없습니다. 하나의 리소스 그룹에 30개 이상의 데이터베이스가 있는 경우 추가 데이터베이스를 위해 두 번째 스냅샷 복사본이 생성됩니다. 따라서 기본 백업 작업 아래에 2개의 하위 작업이 생성됩니다. 보조 복제가 있는 백업의 경우 SnapMirror 또는 SnapVault 업데이트가 진행 중일 때 두 하위 작업의 업데이트가 겹치는 시나리오가 있을 수 있습니다. 로그가 작업이 완료되었음을 나타내더라도 기본 백업 작업은 계속 계속 실행됩니다.

6. 정책 페이지에서 다음 단계를 수행합니다.

   a. 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

   > * 를 클릭하여 정책을 생성할 수도 있습니다 + *.

   > 백업 작업 생성 시 선택할 서버에 대한 * 백업 복사본 * 옵션이 정책에 포함된 경우 하나 이상의 서버를 선택할 수 있는 서버 선택 옵션이 표시됩니다. 서버 선택 옵션에는 선택한 데이터베이스가 NetApp 스토리지에 있는 서버만 나열됩니다.

   선택한 정책에 대한 스케줄 구성 섹션에 선택한 정책이 나열됩니다.

b. 선택한 정책에 대한 일정 구성 섹션에서 * 를 클릭합니다 + 일정을 구성하려는 정책에 대한 * 스케줄 구성 * 열에 있습니다.

c. policy_policy_name_schedules 추가 대화 상자에서 시작 날짜, 만료 날짜 및 빈도를 지정하여 스케줄을 구성한 다음 * 확인 * 을 클릭합니다.

   정책에 나열된 각 빈도에 대해 이 작업을 수행해야 합니다. 구성된 스케줄은 선택한 정책에 대한 스케줄 구성 섹션의 * Applied Schedules * 열에 나열됩니다.

타사 백업 스케줄은 SnapCenter 백업 스케줄과 겹치는 경우 지원되지 않습니다.

7. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 자원 그룹에서 수행된 작업의 보고서를 첨부하려면 * 작업 보고서 첨부 * 를 선택합니다.

   이메일 알림의 경우, GUI 또는 PowerShell 명령 'Set-SmtpServer'를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

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

1. 요약을 검토하고 * Finish * 를 클릭합니다.

Exchange 데이터베이스를 백업합니다

데이터베이스가 리소스 그룹에 속하지 않은 경우 리소스 페이지에서 데이터베이스 또는 데이터베이스 가용성 그룹을 백업할 수 있습니다.

- 필요한 것 *
- 백업 정책을 만들어야 합니다.
- 백업 작업에서 사용 중인 애그리게이트를 데이터베이스에서 사용하는 SVM에 할당해야 합니다.
- 2차 스토리지와 SnapMirror 관계가 있는 리소스를 백업하려면 스토리지 사용자에게 할당된 역할에 "'스냅샷 전체' 권한이 있어야 합니다. 그러나 "vsadmin" 역할을 사용하는 경우에는 "napmirror all" 권한이 필요하지 않습니다.
- NetApp 및 비 NetApp 스토리지에 액티브/패시브 데이터베이스 복사본이 있는 데이터베이스 또는 데이터베이스 가용성 그룹의 백업을 수행하려면 정책에서 백업 작업 생성 시간 * 동안 선택할 서버의 활성 복사본 * 백업 * 또는 * 백업 복사본 * 옵션을 선택한 경우 백업 작업이 경고 상태로 전환됩니다. 백업이 NetApp 스토리지의 액티브/패시브 데이터베이스 복사본에 대해 성공하고 NetApp이 아닌 타사 스토리지의 액티브/패시브 데이터베이스 복사본에 대해서는 백업이 실패합니다.

  * 모범 사례: * 활성 및 수동 데이터베이스의 백업을 동시에 실행하지 마십시오. 경쟁 조건이 발생할 수 있으며 백업 중 하나가 실패할 수 있습니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 * Microsoft Exchange Server 플러그인 * 을 선택합니다.
2. 리소스 페이지의 * 보기 * 목록에서 * 데이터베이스 * 또는 * 데이터베이스 가용성 그룹 * 을 선택합니다.

리소스 페이지에서 을(를) 클릭합니다 아이콘은 데이터베이스가 비NetApp 스토리지에 있음을 나타냅니다.

> DAG에서 액티브 데이터베이스 복제본이 타사 스토리지에 있고 하나 이상의 패시브 데이터베이스 복제본이 NetApp 스토리지에 상주하는 경우 데이터베이스를 보호할 수 있습니다.

를 클릭합니다를 누른 다음 호스트 이름과 데이터베이스 유형을 선택하여 리소스를 필터링합니다. 그런 다음 * 를 클릭할 수 있습니다를 눌러 필터 창을 닫습니다.

- 데이터베이스를 백업하려면 데이터베이스 이름을 클릭합니다.
  i. 토폴로지 뷰가 표시되면 * 보호 * 를 클릭합니다.
  ii. 데이터베이스 보호 리소스 마법사가 표시되면 3단계를 계속 진행합니다.
- 데이터베이스 가용성 그룹을 백업하려면 데이터베이스 가용성 그룹 이름을 클릭합니다.

3. 사용자 지정 스냅샷 복사본 이름을 지정하려면 리소스 페이지에서 * 스냅샷 복사본에 사용자 지정 이름 형식 사용 * 확인란을 선택한 다음 스냅샷 복사본 이름에 사용할 사용자 지정 이름 형식을 입력합니다.

   예: *customtext_policy_hostname_or_resource_hostname*. 기본적으로 스냅샷 복사본 이름에 타임스탬프가 추가됩니다.

4. 정책 페이지에서 다음 단계를 수행합니다.

   a. 드롭다운 목록에서 하나 이상의 정책을 선택합니다.

   > * 를 클릭하여 정책을 생성할 수도 있습니다 *.

   > 백업 작업 생성 시 선택할 서버에 대한 * 백업 복사본 * 옵션이 정책에 포함된 경우 하나 이상의 서버를 선택할 수 있는 서버 선택 옵션이 표시됩니다. 서버 선택 옵션에는 선택한 데이터베이스가 NetApp 스토리지에 있는 서버만 나열됩니다.

   선택한 정책에 대한 스케줄 구성 섹션에 선택한 정책이 나열됩니다.

   b. 를 클릭합니다 일정을 구성하려는 정책에 대한 스케줄 구성 열의

   c. policy_policy_name_에 대한 스케줄 추가 창에서 스케줄을 구성한 다음 * 확인 * 을 클릭합니다.

   여기서, _policy_name_은 선택한 정책의 이름입니다.

   구성된 일정이 Applied Schedules 열에 나열됩니다.

5. 알림 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다. 리소스에 대해 수행된 백업 작업의 보고서를 첨부하려면 * 작업 보고서 연결 * 을 선택합니다.

> 이메일 알림의 경우 GUI 또는 PowerShell 명령 Set-SmtpServer를 사용하여 SMTP 서버 세부 정보를 지정해야 합니다.

1. 요약을 검토하고 * Finish * 를 클릭합니다.

   데이터베이스 토폴로지 페이지가 표시됩니다.

2. 지금 백업 * 을 클릭합니다.
3. 백업 페이지에서 다음 단계를 수행하십시오.
   a. 리소스에 여러 정책을 적용한 경우 * 정책 * 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

      필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

   b. 백업 * 을 클릭합니다.
4. 페이지 하단의 작업 창에서 작업을 두 번 클릭하여 작업 세부 정보 페이지를 표시하여 백업 진행 상황을 모니터링합니다.
   - MetroCluster 구성에서 SnapCenter는 페일오버 후 보호 관계를 감지하지 못할 수 있습니다.

     자세한 내용은 다음을 참조하십시오. "MetroCluster 페일오버 후 SnapMirror 또는 SnapVault 관계를 감지할 수 없습니다"

   - VMDK에서 애플리케이션 데이터를 백업하고 VMware vSphere용 SnapCenter 플러그인의 Java 힙 크기가 충분히 크지 않으면 백업이 실패할 수 있습니다.

     Java 힙 크기를 늘리려면 스크립트 파일 _/opt/netapp/init_scripts/scvservice_를 찾습니다. 이 스크립트에서 _do_start method_command는 SnapCenter VMware 플러그인 서비스를 시작합니다. 이 명령을 _java-jar-Xmx8192M-Xms4096M_로 업데이트합니다

Exchange 리소스 그룹을 백업합니다

리소스 그룹은 호스트 또는 Exchange DAG의 리소스 모음이며 리소스 그룹에는 전체 DAG 또는 개별 데이터베이스가 포함될 수 있습니다. 리소스 페이지에서 리소스 그룹을 백업할 수 있습니다.

- 필요한 것 *
- 정책이 연결된 리소스 그룹을 만들어야 합니다.
- 백업 작업에 사용 중인 애그리게이트를 데이터베이스가 사용하는 스토리지 가상 시스템(SVM)에 할당해야 합니다.
- 2차 스토리지와 SnapMirror 관계가 있는 리소스를 백업하려면 스토리지 사용자에게 할당된 역할에 "'스냅샷 전체' 권한이 있어야 합니다. 그러나 "vsadmin" 역할을 사용하는 경우에는 "napmirror all" 권한이 필요하지 않습니다.
- 리소스 그룹에 서로 다른 호스트의 데이터베이스가 여러 개 있는 경우 네트워크 문제로 인해 일부 호스트의 백업 작업이 늦게 시작될 수 있습니다. et-SmConfigSettings PowerShell cmdlet을 사용하여 web.config에서 MaxRetryForUninitializedHosts 의 값을 구성해야 합니다.
- 리소스 그룹에 NetApp 및 비 NetApp 스토리지에 액티브/패시브 데이터베이스 복사본이 있는 데이터베이스 또는 데이터베이스 가용성 그룹이 포함되어 있고, 백업 작업 생성 시 선택할 서버의 액티브 복제본 * 또는 * 백업 복제본 * 옵션을 선택한 경우 그런 다음 백업 작업이 경고 상태가 됩니다.

  백업이 NetApp 스토리지의 액티브/패시브 데이터베이스 복사본에 대해 성공하고 NetApp이 아닌 타사 스토리지의 액티브/패시브 데이터베이스 복사본에 대해서는 백업이 실패합니다.

- 이 작업에 대한 정보 *

리소스 페이지에서 필요 시 리소스 그룹을 백업할 수 있습니다. 리소스 그룹에 정책이 연결되어 있고 스케줄이 구성되어 있는 경우 스케줄에 따라 백업이 자동으로 수행됩니다.

- 단계 *

  1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 * Microsoft Exchange Server 플러그인 * 을 선택합니다.
  2. 리소스 페이지의 * 보기 * 목록에서 * 리소스 그룹 * 을 선택합니다.

     검색 상자에 리소스 그룹 이름을 입력하거나 * 를 클릭하여 리소스 그룹을 검색할 수 있습니다를 누른 다음 태그를 선택합니다. 그런 다음 * 를 클릭할 수 있습니다를 눌러 필터 창을 닫습니다.
  3. 리소스 그룹 페이지에서 백업할 리소스 그룹을 선택한 다음 * 지금 백업 * 을 클릭합니다.
  4. 백업 페이지에서 다음 단계를 수행하십시오.

     a. 여러 정책을 리소스 그룹에 연결한 경우 * Policy * 드롭다운 목록에서 백업에 사용할 정책을 선택합니다.

        필요 시 백업에 대해 선택한 정책이 백업 스케줄과 연결된 경우 스케줄 유형에 지정된 보존 설정에 따라 필요 시 백업이 유지됩니다.

     b. 백업 * 을 클릭합니다.
  5. 페이지 하단의 작업 창에서 작업을 두 번 클릭하여 작업 세부 정보 페이지를 표시하여 백업 진행 상황을 모니터링합니다.

Exchange Server용 **PowerShell cmdlet**을 사용하여 스토리지 시스템 연결과 자격 증명을 생성합니다

PowerShell cmdlet을 사용하여 백업 및 복원하기 전에 SVM(Storage Virtual Machine) 연결과 자격 증명을 생성해야 합니다.

- 필요한 것 *
- PowerShell cmdlet을 실행할 수 있도록 PowerShell 환경을 준비해야 합니다.
- 스토리지 접속을 생성하려면 인프라스트럭처 관리자 역할에 필요한 권한이 있어야 합니다.
- 플러그인 설치가 진행 중이 아닌지 확인해야 합니다.

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

- 스토리지 시스템 이름은 고유해야 합니다.

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

- 단계 *

  1. Open-SmConnection cmdlet을 사용하여 PowerShell 연결 세션을 시작합니다.

     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 -SVM test_vs1 -Protocol Https
-Timeout 60
```

3. Add-Credential cmdlet을 사용하여 Run As 계정을 새로 만듭니다.

   이 예제에서는 Windows 자격 증명을 사용하여 ExchangeAdmin이라는 새 Run As 계정을 만듭니다.

```
PS C:> Add-SmCredential -Name ExchangeAdmin -AuthMode Windows
-Credential sddev\administrator
```

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

PowerShell cmdlet을 사용하여 Exchange 리소스를 백업합니다

Exchange Server 데이터베이스 백업에는 SnapCenter Server와의 연결 설정, Exchange Server 데이터베이스 검색, 정책 추가, 백업 리소스 그룹 생성, 백업 및 백업 상태 보기가 포함됩니다.

- 필요한 것 *
- PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.
- 스토리지 시스템 접속을 추가하고 자격 증명을 생성해야 합니다.
- 호스트 및 검색된 리소스를 추가해야 합니다.

> Exchange용 플러그인은 클론 작업을 지원하지 않으므로 Exchange용 플러그인에서는 추가 SmPolicy cmdlet의 CloneType 매개 변수가 지원되지 않습니다

- 단계 *

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

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

   사용자 이름 및 암호 프롬프트가 표시됩니다.

2. Add-SmPolicy cmdlet을 사용하여 백업 정책을 만듭니다.

   이 예에서는 전체 백업 및 로그 백업을 사용하여 새 백업 정책을 생성합니다. Exchange 백업 유형:

   ```
   C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy
   -PolicyType Backup -PluginPolicytype SCE -SceBackupType
   FullBackupAndLogBackup -BackupActiveCopies
   ```

   이 예에서는 시간별 전체 백업 및 로그 백업을 사용하여 새 백업 정책을 생성합니다. Exchange 백업 유형:

   ```
   C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Hourly_Full_Log_bkp_Policy
   -PolicyType Backup -PluginPolicytype SCE -SceBackupType
   FullBackupAndLogBackup -BackupActiveCopies -ScheduleType Hourly
   -RetentionSettings
   @{'BackupType'='DATA';'ScheduleType'='Hourly';'RetentionCount'='10'}
   ```

   이 예에서는 Exchange 로그만 백업하기 위한 새 백업 정책을 생성합니다.

   ```
   Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup
   -PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
   ```

3. Get-SmResources cmdlet을 사용하여 호스트 리소스를 검색합니다.

   이 예제에서는 지정된 호스트에서 Microsoft Exchange Server 플러그인에 대한 리소스를 검색합니다.

   ```
   C:\PS> Get-SmResources -HostName vise-f6.sddev.mycompany.com
   -PluginCode SCE
   ```

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

   이 예에서는 지정된 정책 및 리소스를 사용하여 새 Exchange Server 데이터베이스 백업 리소스 그룹을 생성합니다.

   ```
   C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
   -Description 'Backup ResourceGroup with Full and Log backup policy'
   -PluginCode SCE -Policies
   SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log
   _bkp_Policy -Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange
   Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-
   w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
   ```

   이 예에서는 지정된 정책 및 리소스를 사용하여 새 Exchange DAG(Database Availability Group) 백업 리소스

그룹을 생성합니다.

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description
'Backup ResourceGroup with Full and Log backup policy' -PluginCode
SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log
_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database
Availability Group";"Names"="DAGSCE0102"}
```

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

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

이 예에서는 보조 스토리지에 새 백업을 생성합니다.

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

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

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

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

이 예는 특정 작업 ID에 대한 작업 요약 보고서를 표시합니다.

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

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

백업 작업을 모니터링합니다

SnapCenterJobs 페이지를 사용하여 여러 백업 작업의 진행률을 모니터링할 수 있습니다. 진행 상황을 확인하여 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

- 이 작업에 대한 정보 *

다음 아이콘이 작업 페이지에 나타나고 작업의 해당 상태를 나타냅니다.

- 진행 중입니다

- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 취소됨
- 단계 *
  1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
  2. 모니터 페이지에서 * 작업 * 을 클릭합니다.
  3. 작업 페이지에서 다음 단계를 수행하십시오.
     a. 을 클릭합니다 백업 작업만 나열되도록 목록을 필터링합니다.
     b. 시작 및 종료 날짜를 지정합니다.
     c. Type * 드롭다운 목록에서 * Backup * 을 선택합니다.
     d. Status * (상태 *) 드롭다운에서 백업 상태를 선택합니다.
     e. 작업이 성공적으로 완료되었는지 보려면 * Apply * 를 클릭합니다.
  4. 백업 작업을 선택한 다음 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.

     백업 작업 상태가 표시됩니다 작업 세부 정보를 클릭하면 백업 작업의 일부 하위 작업이 아직 진행 중이거나 경고 기호로 표시되어 있는 것을 볼 수 있습니다.

  5. 작업 세부 정보 * 페이지에서 * 로그 보기 * 를 클릭합니다.

     로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

Activity 창에서 작업을 모니터링합니다

작업 창에는 가장 최근에 수행한 작업 5개가 표시됩니다. 작업 창은 작업이 시작된 시점과 작업의 상태도 표시합니다.

작업 창에는 백업, 복원, 클론 및 예약된 백업 작업에 대한 정보가 표시됩니다. SQL Server용 플러그인 또는 Exchange Server용 플러그인을 사용하는 경우 작업 창에 다시 시드된 작업에 대한 정보도 표시됩니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
  2. 을 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다.

     작업 중 하나를 클릭하면 작업 세부 정보가 작업 세부 정보 페이지에 나열됩니다.

Exchange 데이터베이스에 대한 백업 작업을 취소합니다

대기열에 있는 백업 작업을 취소할 수 있습니다.

- 필요한 것 *

- 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.
- 모니터 * 페이지 또는 * 작업 * 창에서 백업 작업을 취소할 수 있습니다.
- 실행 중인 백업 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 백업 작업을 취소할 수 있습니다.
- 취소할 수 없는 작업에 대해 * 작업 취소 * 버튼이 비활성화됩니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 사용자\그룹 페이지에서 다른 구성원 개체를 보고 작동할 수 있음 * 을 선택한 경우 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 백업 작업을 취소할 수 있습니다.
- 단계 *
  1. 다음 작업 중 하나를 수행합니다.

시작...	조치
모니터 페이지	a. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 클릭합니다. b. 작업을 선택한 다음 * 작업 취소 * 를 클릭합니다.
작업 창	a. 백업 작업을 시작한 후 * 를 클릭합니다 * 를 클릭합니다. b. 작업을 선택합니다. c. 작업 세부 정보 페이지에서 * 작업 취소 * 를 클릭합니다.

작업이 취소되고 리소스가 이전 상태로 돌아갑니다.

PowerShell cmdlet을 사용하여 Exchange 백업을 제거합니다

다른 데이터 보호 작업에 Exchange 백업이 더 이상 필요하지 않은 경우 Remove-SmBackup cmdlet을 사용하여 Exchange 백업을 삭제할 수 있습니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

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

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

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

  2. 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"):
```

토폴로지 페이지에서 **Exchange** 백업을 봅니다

리소스를 백업할 준비를 할 때 운영 및 보조 스토리지의 모든 백업을 그래픽으로 표시하는 것이 도움이 될 수 있습니다.

- 이 작업에 대한 정보 *

토폴로지 페이지에서 선택한 리소스 또는 리소스 그룹에 사용할 수 있는 모든 백업을 볼 수 있습니다. 이러한 백업의 세부 정보를 확인한 다음 해당 백업을 선택하여 데이터 보호 작업을 수행할 수 있습니다.

복제본 관리 보기에서 다음 아이콘을 검토하여 운영 스토리지 또는 보조 스토리지(미러 복사본 또는 볼트 복제본)에서 백업을 사용할 수 있는지 여부를 확인할 수 있습니다.

- 기본 스토리지에서 사용할 수 있는 백업 수를 표시합니다.
- SnapMirror 기술을 사용하여 보조 스토리지에 미러링되는 백업 수를 표시합니다.
- SnapVault 기술을 사용하여 보조 스토리지에 복제되는 백업 수를 표시합니다.
  - 표시된 백업 수에는 보조 스토리지에서 삭제된 백업이 포함됩니다.

    예를 들어 정책을 사용하여 6개의 백업을 생성하여 4개의 백업만 보존한 경우 표시되는 백업 수는 6입니다.

* 모범 사례: * 정확한 수의 복제된 백업이 표시되도록 토폴로지를 새로 고치는 것이 좋습니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 적절한 플러그인을 선택합니다.
2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 데이터베이스, 리소스 또는 리소스 그룹을 선택합니다.
3. 데이터베이스 세부 정보 보기 또는 리소스 그룹 세부 정보 보기에서 리소스를 선택합니다.

   리소스가 보호되는 경우 선택한 리소스의 토폴로지 페이지가 표시됩니다.

4. Summary card(요약 카드) 섹션을 검토하여 운영 스토리지와 보조 스토리지에서 사용할 수 있는 백업의 수를 요약합니다.

요약 카드 섹션에는 총 백업 수와 총 로그 백업 수가 표시됩니다.

Refresh * 버튼을 클릭하면 스토리지 쿼리가 시작되어 정확한 카운트를 표시합니다.

1. 복사본 관리 보기에서 기본 또는 보조 스토리지에서 * 백업 * 을 클릭하여 백업 세부 정보를 확인합니다.

   백업 세부 정보가 표 형식으로 표시됩니다.

2. 테이블에서 백업을 선택한 다음 데이터 보호 아이콘을 클릭하여 복원, 이름 바꾸기 및 삭제 작업을 수행합니다.

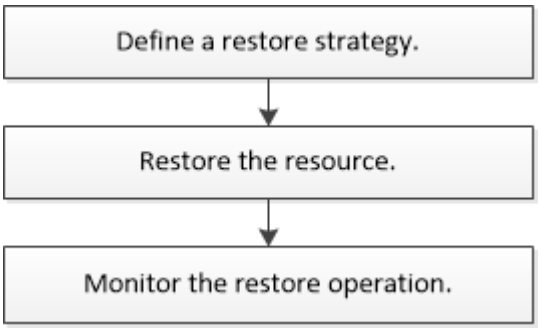
   보조 스토리지에 있는 백업의 이름을 바꾸거나 백업을 삭제할 수 없습니다. 스냅샷 복사본 삭제는 ONTAP 보존 설정에 의해 처리됩니다.

Exchange 리소스를 복구합니다

워크플로를 복원합니다

SnapCenter를 사용하여 하나 이상의 백업을 활성 파일 시스템에 복구함으로써 Exchange 데이터베이스를 복구할 수 있습니다.

다음 워크플로에서는 Exchange 데이터베이스 복원 작업을 수행해야 하는 순서를 보여 줍니다.



PowerShell cmdlet을 수동으로 사용하거나 스크립트에서 사용하여 백업 및 복원 작업을 수행할 수도 있습니다. PowerShell cmdlet에 대한 자세한 내용은 SnapCenter cmdlet 도움말을 사용하거나 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

Exchange 데이터베이스 복구 요구 사항

Microsoft Exchange Server 백업용 SnapCenter 플러그인에서 Exchange Server 데이터베이스를 복구하기 전에 몇 가지 요구 사항이 충족되는지 확인해야 합니다.

- 데이터베이스를 복구하려면 Exchange Server가 온라인 상태이고 실행 중이어야 합니다.
- 데이터베이스는 Exchange Server에 있어야 합니다.

  삭제된 데이터베이스 복원은 지원되지 않습니다.

- 데이터베이스에 대한 SnapCenter 일정을 일시 중지해야 합니다.

- SnapCenter 서버 및 Microsoft Exchange Server용 SnapCenter 플러그인은 복원하려는 백업이 포함된 운영 스토리지 및 보조 스토리지에 연결되어 있어야 합니다.

Exchange 데이터베이스를 복구합니다

SnapCenter를 사용하여 백업된 Exchange 데이터베이스를 복구할 수 있습니다.

- 필요한 것 *
- 리소스 그룹, 데이터베이스 또는 DAG(데이터베이스 가용성 그룹)를 백업해야 합니다.
- Exchange 데이터베이스가 다른 위치로 마이그레이션되면 이전 백업에서 복구 작업이 작동하지 않습니다.
- 스냅샷 복사본을 미러 또는 볼트에 복제하는 경우 SnapCenter 관리자는 소스 볼륨과 타겟 볼륨 모두에 대해 SVM을 할당해야 합니다.
- DAG에서 액티브 데이터베이스 복제본이 타사 스토리지에 있고 NetApp 스토리지에 있는 패시브 데이터베이스 복제본 백업에서 복구하려는 경우 패시브 복제본(NetApp 스토리지)을 액티브 복제본으로 만들고 리소스를 새로 고치고 복구 작업을 수행합니다.

  Move-ActiveMailboxDatabase 명령을 실행하여 수동 데이터베이스 복사본을 활성 데이터베이스 복사본으로 만듭니다.

  를 클릭합니다 "Microsoft 설명서" 이 명령에 대한 정보를 포함합니다.

- 이 작업에 대한 정보 *
- 데이터베이스에서 복구 작업을 수행하면 데이터베이스가 동일한 호스트에 다시 마운트되고 새 볼륨이 생성되지 않습니다.
- DAG 레벨 백업은 개별 데이터베이스에서 복구해야 합니다.
- Exchange 데이터베이스(.edb) 파일 이외의 파일이 있는 경우 전체 디스크 복원이 지원되지 않습니다.

  Exchange용 플러그인은 디스크에 복제에 사용되는 것과 같은 Exchange 파일이 포함되어 있는 경우 디스크에서 전체 복구를 수행하지 않습니다. 전체 복원이 Exchange 기능에 영향을 줄 수 있는 경우 Exchange용 플러그인은 단일 파일 복원 작업을 수행합니다.

- Exchange용 플러그인은 BitLocker로 암호화된 드라이브를 복원할 수 없습니다.
- 단계 *

  1. 왼쪽 탐색 창의 리소스 페이지 왼쪽 위에 있는 * 리소스 * 를 클릭합니다.
  2. 드롭다운 목록에서 Exchange Server 플러그인을 선택합니다.
  3. 리소스 페이지의 보기 목록에서 * 데이터베이스 * 를 선택합니다.
  4. 목록에서 데이터베이스를 선택합니다.
  5. Manage Copies 보기의 Primary Backups 표에서 * Backups * 를 선택한 다음 * 를 클릭합니다 *.
  6. 옵션 페이지에서 다음 로그 백업 옵션 중 하나를 선택합니다.

옵션을 선택합니다	설명
모든 로그 백업	전체 백업 후 사용 가능한 모든 로그 백업을 복원하려면 * 모든 로그 백업 * 을 선택하여 최신 백업 복원 작업을 수행하십시오.
까지 로그 백업을 통해	선택한 로그까지 로그 백업을 기반으로 데이터베이스를 복원하는 시점 복원 작업을 수행하려면 * 까지 로그 백업 * 을 선택합니다. 드롭다운 목록에 표시되는 로그 수는 UTM을 기반으로 합니다. 예를 들어 전체 백업 보존이 5이고 UTM 보존이 3인 경우 사용 가능한 로그 백업 수는 5이지만 드롭다운에서 복구 작업을 수행하기 위해 3개의 로그만 나열됩니다.
특정 날짜 기준 종료	복원된 데이터베이스에 트랜잭션 로그를 적용할 날짜 및 시간을 지정하려면 특정 날짜별 * 를 선택합니다. 이 시점 복원 작업은 지정된 날짜 및 시간에 마지막 백업까지 기록된 트랜잭션 로그 항목을 복원합니다.
없음	로그 백업 없이 전체 백업만 복원해야 하는 경우 * 없음 * 을 선택합니다.

다음 작업 중 하나를 수행할 수 있습니다.

- * 복구 후 데이터베이스 복구 및 마운트 * - 이 옵션은 기본적으로 선택되어 있습니다.
- * 복구하기 전에 백업에서 트랜잭션 로그의 무결성을 확인하지 않음 * - 기본적으로 SnapCenter는 복원 작업을 수행하기 전에 백업에서 트랜잭션 로그의 무결성을 확인합니다.

* 모범 사례: * 이 옵션을 선택해서는 안 됩니다.

7. 스크립트 페이지에서 복원 작업 전후에 실행해야 하는 처방인 또는 PS의 경로와 인수를 각각 입력합니다.

   복구 매개 변수 인수에는 $Database 및 $ServerInstance가 포함됩니다.

   PostScript 인수 복원에는 $Database, $ServerInstance, $BackupName, $LogDirectory 및 $TargetServerInstance가 포함됩니다.

스크립트를 실행하여 SNMP 트랩을 업데이트하고, 경고를 자동화하고, 로그를 보내는 등의 작업을 수행할 수 있습니다.

1. 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.

2. 요약을 검토하고 * Finish * 를 클릭합니다.

3. 페이지 하단의 Activity[활동] 패널을 확장하여 복구 작업의 상태를 볼 수 있습니다.

   모니터 * > * 작업 * 페이지를 사용하여 복원 프로세스를 모니터링해야 합니다.

백업에서 활성 데이터베이스를 복구할 때 복제본과 액티브 데이터베이스 사이에 지연이 있는 경우 수동 데이터베이스가 일시 중단 또는 실패 상태가 될 수 있습니다.

활성 데이터베이스의 로그 체인이 포크되고 복제를 중단시킬 새 분기가 시작될 때 상태 변경이 발생할 수 있습니다. Exchange Server에서 복제본을 수정하려고 시도하지만 복구할 수 없는 경우 복구 후 새 백업을 생성한 다음 복제본을 다시 시드해야 합니다.

메일 및 편지함의 세밀한 복구

SMBR(Single Mailbox Recovery) 소프트웨어를 사용하면 전체 Exchange 데이터베이스 대신 메일 또는 편지함을 복원 및 복구할 수 있습니다.

전체 데이터베이스를 복원하여 단일 메일을 복구하면 많은 시간과 리소스가 소모됩니다. SMBR은 스냅샷의 클론 복제본을 생성한 다음 Microsoft API를 사용하여 SMBR에 메일박스를 마운트하여 메일을 빠르게 복구하는 데 도움이 됩니다. SMBR 사용 방법에 대한 자세한 내용은 을 참조하십시오 "SMBR 관리 가이드".

SMBR에 대한 자세한 내용은 다음을 참조하십시오.

- "SMBR(Ontrack Power Control 복원에도 적용 가능)을 사용하여 단일 항목을 수동으로 복원하는 방법"
- "SnapCenter를 사용하여 SMBR의 보조 스토리지에서 복원하는 방법"
- "SMBR을 사용하여 SnapVault에서 Microsoft Exchange Mail 복구"

보조 스토리지에서 **Exchange Server** 데이터베이스를 복구합니다

보조 스토리지(미러 또는 볼트)에서 백업된 Exchange Server 데이터베이스를 복구할 수 있습니다.

기본 스토리지에서 보조 스토리지로 Snapshot 복사본을 복제해야 합니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 * Microsoft Exchange Server 플러그인 * 을 선택합니다.
  2. 리소스 페이지의 * 보기 * 드롭다운 목록에서 * 데이터베이스 * 또는 * 리소스 그룹 * 을 선택합니다.
  3. 데이터베이스 또는 리소스 그룹을 선택합니다.

     데이터베이스 또는 리소스 그룹 토폴로지 페이지가 표시됩니다.

  4. 복사본 관리 섹션의 보조 스토리지 시스템(미러 또는 볼트)에서 * 백업 * 을 선택합니다.
  5. 목록에서 백업을 선택한 다음 을 클릭합니다 .
  6. 위치 페이지에서 선택한 리소스를 복원할 대상 볼륨을 선택합니다.
  7. 복원 마법사를 완료하고 요약을 검토한 다음 * 마침 * 을 클릭합니다.

PowerShell cmdlet을 사용하여 Exchange 리소스를 복원합니다

Exchange 데이터베이스 복구에는 SnapCenter 서버와의 연결 세션 시작, 백업 목록 표시 및 백업 정보 검색, 백업 복구가 포함됩니다.

PowerShell cmdlet을 실행하려면 PowerShell 환경을 준비해야 합니다.

- 단계 *

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대해 SnapCenter Server와 연결 세션을 시작합니다.

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

2. Get-SmBackup 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
--------                      ----------
----------                    ----------
341                           ResourceGroup_36304978_UTM... 12/8/2017
4:13:24 PM          Full Backup
342                           ResourceGroup_36304978_UTM... 12/8/2017
4:16:23 PM          Full Backup
355                           ResourceGroup_06140588_UTM... 12/8/2017
6:32:36 PM          Log Backup
356                           ResourceGroup_06140588_UTM... 12/8/2017
6:36:20 PM          Full Backup
```

3. Restore-SmBackup cmdlet을 사용하여 백업에서 데이터를 복원합니다.

   이 예에서는 최신 백업을 복원합니다.

```
C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341
-IsRecoverMount:$true
```

   이 예에서는 시점 백업을 복원합니다.

```
C:\ PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341
-IsRecoverMount:$true -LogRestoreType ByTransactionLogs -LogCount 2
```

이 예에서는 보조 스토리지의 백업을 1차 사례로 복원합니다.

```
C:\ PS> Restore-SmBackup -PluginCode 'SCE' -AppObjectId 'DB2'
-BackupId 81 -IsRecoverMount:$true -Confirm:$false
-archive @{Primary="paw_vs:vol1";Secondary="paw_vs:vol1_mirror"}
-logrestoretype All
```

'-archive' 매개 변수를 사용하면 복원에 사용할 운영 볼륨과 2차 볼륨을 지정할 수 있습니다.

'-IsRecoverMount:$true' 매개 변수를 사용하면 복구 후에 데이터베이스를 마운트할 수 있습니다.

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

패시브 **Exchange** 노드 복제본을 다시 시딩했습니다

복제본이 손상된 경우와 같이 복제본을 재시딩해야 하는 경우 SnapCenter의 재시딩된 기능을 사용하여 최신 백업으로 재시딩할 수 있습니다.

- SnapCenter Server 4.1 이상을 사용하고 Exchange 4.1 이상을 위한 플러그인을 사용해야 합니다.

  복제본 재시딩은 4.1 이전 버전의 SnapCenter에서는 지원되지 않습니다.

- 다시 시딩하려는 데이터베이스의 백업을 만들어야 합니다.

* 모범 사례: * 노드 사이의 지연 현상을 방지하려면 재시딩된 작업을 수행하기 전에 새 백업을 생성하거나 최신 백업이 있는 호스트를 선택하는 것이 좋습니다.

- 단계 *

  1. 왼쪽 탐색 창에서 * 리소스 * 를 클릭한 다음 목록에서 * Microsoft Exchange Server 플러그인 * 을 선택합니다.
  2. Resources * 페이지의 View 목록에서 적절한 옵션을 선택합니다.

옵션을 선택합니다	설명
단일 데이터베이스를 다시 시딩합니다	보기 목록에서 * 데이터베이스 * 를 선택합니다.
DAG에서 데이터베이스를 재시딩하는 경우	보기 목록에서 * 데이터베이스 가용성 그룹 * 을 선택합니다.

  3. 다시 시딩할 리소스를 선택합니다.

4. 매수 관리 * 페이지에서 * 다시 시딩된 * 을 클릭합니다.
5. 다시 시딩된 마법사의 비정상적인 데이터베이스 복사본 목록에서 다시 시딩할 복제본을 선택하고 * 다음 * 을 클릭합니다.
6. 호스트 창에서 다시 연결할 백업이 있는 호스트를 선택한 후 * 다음 * 을 클릭합니다.
7. Script* 페이지에서 재시딩된 작업 전후에 실행해야 하는 처방인 또는 PS의 경로와 인수를 각각 입력합니다.

   예를 들어, 스크립트를 실행하여 SNMP 트랩을 업데이트하고, 경고를 자동화하고, 로그를 보내는 등의 작업을 수행할 수 있습니다.

8. 알림 * 페이지의 * 이메일 기본 설정 * 드롭다운 목록에서 이메일을 보낼 시나리오를 선택합니다.

   또한 보낸 사람 및 받는 사람 전자 메일 주소와 전자 메일의 제목도 지정해야 합니다.

9. 요약을 검토하고 * Finish * 를 클릭합니다.
10. 페이지 하단의 Activity[활동] 패널을 확장하여 작업 상태를 볼 수 있습니다.

패시브 데이터베이스 복사본이 NetApp이 아닌 스토리지에 상주하는 경우 다시 시딩된 작업은 지원되지 않습니다.

Exchange 데이터베이스에 대해 **PowerShell cmdlet**을 사용하여 복제본을 다시 시딩했습니다

PowerShell cmdlet을 사용하여 동일한 호스트에 있는 가장 최근 복사본 또는 대체 호스트에서 가장 최근 복사본을 사용하여 상태가 불량한 복제본을 복구할 수 있습니다.

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

- 단계 *

1. Open-SmConnection cmdlet을 사용하여 지정된 사용자에 대해 SnapCenter Server와 연결 세션을 시작합니다.

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

2. '시드-SmDagReplicaCopy' cmdlet을 사용하여 데이터베이스를 다시 시딩했습니다.

   이 예에서는 호스트 "mva-rx200.netapp.com" 에서 해당 호스트의 최신 백업을 사용하여 실패한 데이터베이스 복제본을 다시 시딩합니다.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb
```

   이 예제에서는 다른 호스트 "mva-rx201.netapp.com." 데이터베이스의 최신 백업(운영/복제본)을 사용하여 execdb라는 데이터베이스 복제본을 다시 시딩합니다

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb -BackupHost "mva-rx201.netapp.com"
```

복구 작업을 모니터링합니다

작업 페이지를 사용하여 여러 SnapCenter 복원 작업의 진행률을 모니터링할 수 있습니다. 작업 진행률을 확인하여 작업이 언제 완료되는지 또는 문제가 있는지 확인할 수 있습니다.

- 이 작업에 대한 정보 *

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. 작업 * 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. 작업 세부 정보 * 페이지에서 * 로그 보기 * 를 클릭합니다.

   로그 보기 * 버튼은 선택한 작업에 대한 상세 로그를 표시합니다.

> 볼륨 기반 복원 작업 후에는 백업 메타데이터가 SnapCenter 저장소에서 삭제되지만 백업 카탈로그 항목은 SAP HANA 카탈로그에 남아 있습니다. 복원 작업 상태가 표시됩니다 작업 세부 정보를 클릭하여 일부 하위 작업의 경고 표시를 확인해야 합니다. 경고 표지를 클릭하고 표시된 백업 카탈로그 항목을 삭제합니다.

Exchange 데이터베이스에 대한 복구 작업을 취소합니다

대기열에 있는 복원 작업을 취소할 수 있습니다.

복원 작업을 취소하려면 SnapCenter 관리자 또는 작업 소유자로 로그인해야 합니다.

- 이 작업에 대한 정보 *
- 모니터 페이지 또는 작업 창에서 대기 중인 복원 작업을 취소할 수 있습니다.
- 실행 중인 복원 작업은 취소할 수 없습니다.
- SnapCenter GUI, PowerShell cmdlet 또는 CLI 명령을 사용하여 대기 중인 복원 작업을 취소할 수 있습니다.
- 취소할 수 없는 복원 작업에는 * 작업 취소 * 버튼이 비활성화됩니다.
- 역할을 만드는 동안 이 역할의 모든 구성원이 사용자\그룹 페이지의 다른 구성원 개체를 보고 작업할 수 있음 * 을 선택한 경우 해당 역할을 사용하는 동안 다른 구성원의 대기 중인 복원 작업을 취소할 수 있습니다.
- 단계 *

다음 작업 중 하나를 수행합니다.

시작...	조치
모니터 페이지	1. 왼쪽 탐색 창에서 * 모니터 * > * 작업 * 을 클릭합니다. 2. 작업을 선택하고 * 작업 취소 * 를 클릭합니다.
작업 창	1. 복원 작업을 시작한 후 을 클릭합니다 를 클릭하여 가장 최근 작업 5개를 확인합니다. 2. 작업을 선택합니다. 3. 작업 세부 정보 페이지에서 * 작업 취소 * 를 클릭합니다.

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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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