SnapCenter 서버 구성

SnapCenter software

NetApp
November 06, 2025

목차

SnapCenter 서버 구성

스토리지 시스템 추가 및 프로비저닝

스토리지 시스템 추가

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

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

시작하기 전에

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

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

- 저장 시스템 이름은 고유해야 합니다.

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

이 작업에 관하여

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

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

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

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

단계

1. 왼쪽 탐색 창에서 *저장 시스템*을 클릭합니다.
2. 스토리지 시스템 페이지에서 *새로 만들기*를 클릭합니다.

3. 스토리지 시스템 추가 페이지에서 다음 정보를 제공합니다.

이 분야에서는...	이렇게 하세요...
저장 시스템	저장 시스템 이름이나 IP 주소를 입력하세요. 도메인 이름을 제외한 스토리지 시스템 이름은 15자 이하여야 하며, 이름을 확인할 수 있어야 합니다. 이름이 15자 이상인 스토리지 시스템 연결을 만들려면 Add-SmStorageConnectionPowerShell cmdlet을 사용할 수 있습니다. MetroCluster 구성(MCC)을 사용하는 스토리지 시스템의 경우 중단 없는 작업을 위해 로컬 클러스터와 피어 클러스터를 모두 등록하는 것이 좋습니다. SnapCenter 서로 다른 클러스터에서 동일한 이름을 가진 여러 SVM을 지원하지 않습니다. SnapCenter 에서 지원하는 각 SVM에는 고유한 이름이 있어야 합니다. SnapCenter 에 스토리지 연결을 추가한 후에는 ONTAP 사용하여 SVM이나 클러스터의 이름을 바꾸면 안 됩니다. SVM이 짧은 이름이나 FQDN으로 추가된 경우 SnapCenter 와 플러그인 호스트 모두에서 확인할 수 있어야 합니다.
사용자 이름/비밀번호	스토리지 시스템에 액세스하는 데 필요한 권한이 있는 스토리지 사용자의 자격 증명을 입력하세요.
이벤트 관리 시스템(EMS) 및 AutoSupport 설정	스토리지 시스템 syslog에 EMS 메시지를 보내거나 적용된 보호, 완료된 복원 작업 또는 실패한 작업에 대해 스토리지 시스템에 AutoSupport 메시지를 보내려면 해당 확인란을 선택합니다. 실패한 작업에 대한 **AutoSupport** 알림을 스토리지 시스템에 보내기 확인란을 선택하면 AutoSupport 알림을 활성화하려면 EMS 메시징이 필요하므로 * SnapCenter 서버 이벤트를 syslog에 기록* 확인란도 선택됩니다.

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

a. 플랫폼에서 드롭다운 목록에서 옵션 중 하나를 선택합니다.

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

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

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

   일반적으로 기본 포트 443이 작동합니다.

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

   기본값은 60초입니다.

d. SVM에 여러 관리 인터페이스가 있는 경우 기본 **IP** 확인란을 선택한 다음 SVM 연결에 대한 기본 IP 주소를 입력합니다.
e. *저장*을 클릭하세요.

5. *제출*을 클릭하세요.

결과

스토리지 시스템 페이지의 유형 드롭다운에서 다음 작업 중 하나를 수행합니다.

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

  FSx SVM을 추가한 경우 FSx SVM이 여기에 나열됩니다.

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

  fsxadmin을 사용하여 FSx 클러스터를 추가한 경우 FSx 클러스터가 여기에 나열됩니다.

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

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

끝난 후

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

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

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

저장소 연결 및 자격 증명

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

저장소 연결

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

신임장

- 도메인 관리자 또는 관리자 그룹의 모든 구성원

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

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

- 로컬 관리자(작업 그룹에만 해당)

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

  사용자 이름 필드의 유효한 형식은 다음과 같습니다. *UserName*

- 개별 리소스 그룹에 대한 자격 증명

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

Windows 호스트에 스토리지 프로비저닝

igroups를 만들고 관리하세요

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

igroup 만들기

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

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.

2. 호스트 페이지에서 *Igroup*을 클릭합니다.
3. 개시자 그룹 페이지에서 *새로 만들기*를 클릭합니다.
4. Igroup 만들기 대화 상자에서 igroup을 정의합니다.

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

5. 입력한 내용이 마음에 들면 *확인*을 클릭하세요.

   SnapCenter 스토리지 시스템에 igroup을 생성합니다.

igroup 이름 바꾸기

SnapCenter 사용하여 기존 igroup의 이름을 바꿀 수 있습니다.

단계

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

igroup 수정

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

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.
2. 호스트 페이지에서 *Igroup*을 클릭합니다.
3. 이니시에이터 그룹 페이지에서 스토리지 가상 머신 필드를 클릭하여 사용 가능한 SVM의 드롭다운 목록을 표시한 다음, 수정하려는 igroup의 SVM을 선택합니다.

4. igroup 목록에서 igroup을 선택하고 *igroup에 시작자 추가*를 클릭합니다.
5. 호스트를 선택하세요.
6. 시작 프로그램을 선택하고 *확인*을 클릭합니다.

igroup 삭제

더 이상 필요하지 않은 igroup을 삭제하려면 SnapCenter 사용하면 됩니다.

단계

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

   SnapCenter igroup을 삭제합니다.

디스크 생성 및 관리

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

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

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

호스트의 디스크 보기

SnapCenter 사용하여 관리하는 각 Windows 호스트의 디스크를 볼 수 있습니다.

단계

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

   디스크가 나열됩니다.

클러스터된 디스크 보기

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

단계

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

   디스크가 나열됩니다.

iSCSI 세션을 설정합니다

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

시작하기 전에

- 스토리지 시스템 노드를 iSCSI 대상으로 정의해야 합니다.
- 스토리지 시스템에서 iSCSI 서비스를 시작했어야 합니다. "자세히 알아보기"

이 작업에 관하여

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

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

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

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

단계

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

   세션 설정 마법사가 표시됩니다.

6. 세션 설정 마법사에서 대상을 식별합니다.

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

7. 입력한 내용이 마음에 들면 *연결*을 클릭하세요.

   SnapCenter iSCSI 세션을 설정합니다.

8. 각 대상에 대한 세션을 설정하려면 이 절차를 반복합니다.

FC 연결 또는 iSCSI 연결 LUN 또는 디스크 생성

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

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

시작하기 전에

- 스토리지 시스템에서 LUN에 대한 볼륨을 생성했어야 합니다.

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

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

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

이 작업에 관하여

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

단계

1. 왼쪽 탐색 창에서 *호스트*를 클릭합니다.

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

   디스크 생성 마법사가 열립니다.

5. LUN 이름 페이지에서 LUN을 식별합니다.

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

6. 디스크 유형 페이지에서 디스크 유형을 선택합니다.

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

7. 드라이브 속성 페이지에서 드라이브 속성을 지정합니다.

재산	설명
마운트 지점 자동 할당	SnapCenter 시스템 드라이브를 기반으로 볼륨 마운트 지점을 자동으로 할당합니다. 예를 들어, 시스템 드라이브가 C:인 경우 자동 할당은 C: 드라이브 아래에 볼륨 마운트 지점(C:\scmnpt\)을 생성합니다. 공유 디스크에는 자동 할당이 지원되지 않습니다.
드라이브 문자 할당	인접한 드롭다운 목록에서 선택한 드라이브에 디스크를 마운트합니다.
볼륨 마운트 지점 사용	인접 필드에 지정한 드라이브 경로에 디스크를 마운트합니다. 볼륨 마운트 지점의 루트는 디스크를 생성하는 호스트가 소유해야 합니다.
드라이브 문자 또는 볼륨 마운트 지점을 할당하지 마십시오.	Windows에서 디스크를 수동으로 마운트하려면 이 옵션을 선택하세요.
LUN 크기	LUN 크기를 지정하세요. 최소 150MB. 옆의 드롭다운 목록에서 MB, GB 또는 TB를 선택하세요.
이 LUN을 호스팅하는 볼륨에 씬 프로비저닝을 사용합니다.	LUN을 씬 프로비저닝합니다. 씬 프로비저닝은 한 번에 필요한 만큼의 저장 공간만 할당하므로 LUN이 사용 가능한 최대 용량까지 효율적으로 확장될 수 있습니다. 필요한 모든 LUN 스토리지를 수용할 수 있을 만큼 볼륨에 충분한 공간이 있는지 확인하세요.
파티션 유형을 선택하세요	GUID 파티션 테이블의 경우 GPT 파티션을 선택하고, 마스터 부트 레코드의 경우 MBR 파티션을 선택합니다. MBR 파티션은 Windows Server 장애 조치(failover) 클러스터에서 정렬 오류 문제를 일으킬 수 있습니다. 통합 확장 가능 펌웨어 인터페이스(UEFI) 파티션 디스크는 지원되지 않습니다.

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

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

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

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

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

    SnapCenter LUN을 생성하고 호스트의 지정된 드라이브 또는 드라이브 경로에 연결합니다.

디스크 크기 조정

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

이 작업에 관하여

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

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

단계

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

   디스크가 나열됩니다.

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

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

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

   SnapCenter 디스크 크기를 조정합니다.

디스크 연결

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

시작하기 전에

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

단계

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

   디스크 연결 마법사가 열립니다.

5. LUN 이름 페이지에서 연결할 LUN을 식별합니다.

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

6. 디스크 유형 페이지에서 디스크 유형을 선택합니다.

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

7. 드라이브 속성 페이지에서 드라이브 속성을 지정합니다.

재산	설명
자동 할당	SnapCenter 시스템 드라이브를 기반으로 볼륨 마운트 지점을 자동으로 할당하도록 합니다. 예를 들어, 시스템 드라이브가 C:인 경우 자동 할당 속성은 C: 드라이브 아래에 볼륨 마운트 지점(C:\scmnpt\)을 만듭니다. 공유 디스크에서는 자동 할당 속성이 지원되지 않습니다.

재산	설명
드라이브 문자 할당	옆의 드롭다운 목록에서 선택한 드라이브에 디스크를 마운트합니다.
볼륨 마운트 지점 사용	인접한 필드에 지정한 드라이브 경로에 디스크를 마운트합니다. 볼륨 마운트 지점의 루트는 디스크를 생성하는 호스트가 소유해야 합니다.
드라이브 문자 또는 볼륨 마운트 지점을 할당하지 마십시오.	Windows에서 디스크를 수동으로 마운트하려면 이 옵션을 선택하세요.

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

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

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

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

10. 요약 페이지에서 선택 사항을 검토하고 *마침*을 클릭합니다.

    SnapCenter LUN을 호스트의 지정된 드라이브 또는 드라이브 경로에 연결합니다.

디스크 연결 해제

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

시작하기 전에

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

이 작업에 관하여

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

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

단계

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

   디스크가 나열됩니다.

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

   SnapCenter 가 디스크 연결을 끊습니다.

디스크 삭제

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

단계

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

   디스크가 나열됩니다.

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

SnapCenter 디스크를 삭제합니다.

SMB 공유 생성 및 관리

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

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

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

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

SMB 공유 만들기

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

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

단계

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

   새 공유 대화 상자가 열립니다.

5. 새 공유 대화 상자에서 공유를 정의합니다.

이 분야에서는...	이렇게 하세요...
설명	공유에 대한 설명 텍스트를 입력하세요.

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

6. 입력한 내용이 마음에 들면 *확인*을 클릭하세요.

   SnapCenter SVM에 SMB 공유를 생성합니다.

SMB 공유 삭제

더 이상 필요하지 않은 SMB 공유를 삭제할 수 있습니다.

단계

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

   SnapCenter SVM에서 SMB 공유를 삭제합니다.

저장 시스템에서 공간 확보

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

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

시작하기 전에

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

  전체 NTFS 파일 시스템이 검사되었는지 확인해야 합니다.

이 작업에 관하여

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

  그렇게 하면 회수 과정이 느려질 수 있습니다.

단계

애플리케이션 서버 PowerShell 명령 프롬프트에서 다음 명령을 입력합니다.

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

drive_path는 LUN에 매핑된 드라이브 경로입니다.

PowerShell cmdlet을 사용하여 스토리지 프로비저닝

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

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

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 _Get-Help command_name_을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "SnapCenter 소프트웨어 Cmdlet 참조 가이드" .

서버에서 Windows용 SnapDrive 제거하여 SnapCenter PowerShell cmdlet이 손상된 경우 다음을 참조하세요. "Windows용 SnapDrive 제거하면 SnapCenter cmdlet이 손상됨" .

VMware 환경에서 스토리지 프로비저닝

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

지원되는 **VMware** 게스트 **OS** 플랫폼

- 지원되는 Windows Server 버전

- Microsoft 클러스터 구성

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

- RDM LUN

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

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

지원되는 버전에 대한 최신 정보는 다음을 참조하세요. "NetApp 상호 운용성 매트릭스 도구" .

VMware ESXi 서버 관련 제한 사항

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

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

- 모든 클러스터 노드는 동일한 클러스터 디스크에 대해 동일한 대상 ID(가상 SCSI 어댑터에서)를 사용해야 합니다.
- Windows용 플러그인 외부에서 RDM LUN을 생성하는 경우 플러그인 서비스를 다시 시작해야 새로 생성된 디스크를 인식할 수 있습니다.
- VMware 게스트 OS에서는 iSCSI와 FC 이니시에이터를 동시에 사용할 수 없습니다.

SnapCenter RDM 작업에 필요한 최소 **vCenter** 권한

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

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

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

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

Microsoft 클러스터에서 **FC RDM LUN** 관리

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

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

요구 사항

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

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

  필요한 경우 공유 데이터 저장소를 iSCSI를 통해 생성할 수도 있습니다.

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

  공유 스토리지에는 가상 디스크를 사용할 수 없습니다.

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

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

  준가상화 유형의 SCSI 컨트롤러는 VMware Microsoft 클러스터에서 지원되지 않습니다.

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

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

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

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

  RDM LUN을 생성하면 ALUA를 사용하여 이니시에이터 그룹이 생성됩니다.

제한 사항

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

이 기능은 ESX 5.5i 이전 릴리스에서는 지원되지 않습니다.

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

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

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

공유 **FC RDM LUN** 생성

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

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

SnapCenter Standard 컨트롤러 기반 라이선스 추가

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

컨트롤러 기반 라이선스에는 다음과 같은 특징이 있습니다.

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

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

- 컨트롤러의 일련번호에 고정됨

필요한 라이센스에 대한 정보는 다음을 참조하세요."SnapCenter 라이센스" .

1단계: SnapManager Suite 라이선스가 설치되었는지 확인

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

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

단계

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

     클러스터 이름을 선택하면 클러스터에 속한 모든 SVM이 스토리지 가상 머신 섹션에 표시됩니다.
3. 저장소 연결 목록에서 컨트롤러 라이선스 열을 찾으세요.

   컨트롤러 라이선스 열에는 다음 상태가 표시됩니다.

   -  SnapManager Suite 라이선스가 FAS, AFF 또는 ASA 기본 스토리지 시스템에 설치되었음을 나타냅니다.
   -  SnapManager Suite 라이선스가 FAS, AFF 또는 ASA 기본 스토리지 시스템에 설치되지 않았음을 나타냅니다.
   - 해당 없음은 스토리지 컨트롤러가 Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select 또는 보조 스토리지 플랫폼에 있기 때문에 SnapManager Suite 라이선스가 적용되지 않음을 나타냅니다.

2단계: 컨트롤러에 설치된 라이센스 식별

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

컨트롤러는 SnapManagerSuite 라이선스로 SnapCenter Standard 컨트롤러 기반 라이선스를 표시합니다.

단계

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

출력 예

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

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

Serial Number: 1-81-00000000000000000000000xx
Owner: cluster1-01
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
NFS               license  NFS License              -
CIFS              license  CIFS License             -
iSCSI             license  iSCSI License            -
FCP               license  FCP License              -
SnapRestore       license  SnapRestore License      -
SnapMirror        license  SnapMirror License       -
FlexClone         license  FlexClone License        -
SnapVault         license  SnapVault License        -
SnapManagerSuite  license  SnapManagerSuite License -
```

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

3단계: 컨트롤러 일련 번호 검색

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

단계

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

출력 예

```
cluster1::> system show -instance

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

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

3. 일련번호를 기록하세요.

4단계: 컨트롤러 기반 라이센스의 일련 번호 검색

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

시작하기 전에

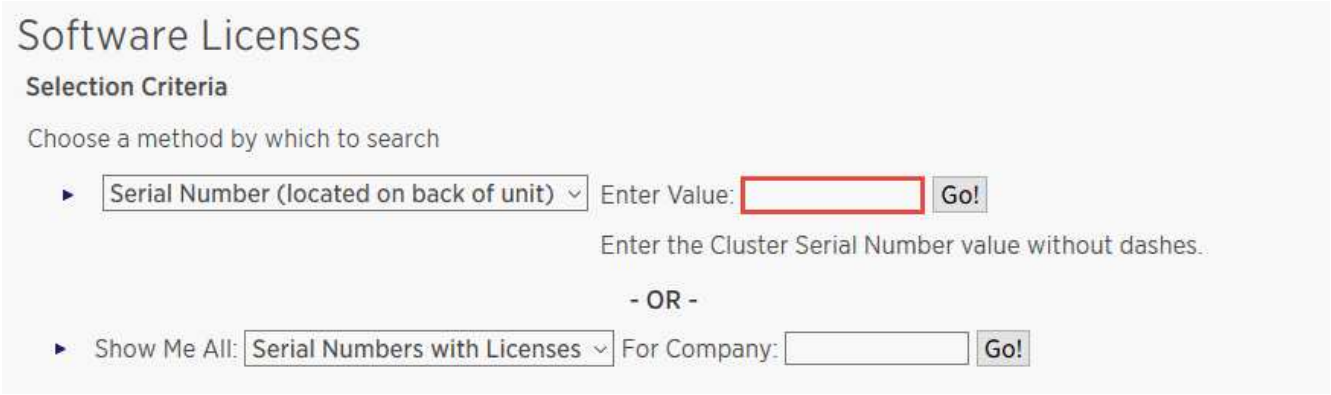
- 유효한 NetApp 지원 사이트 로그인 자격 증명이 있어야 합니다.

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

- 컨트롤러 일련번호가 있어야 합니다.

단계

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



지정된 컨트롤러에 대한 라이센스 목록이 표시됩니다.

4. SnapCenter Standard 또는 SnapManagerSuite 라이선스를 찾아 기록합니다.

5단계: 컨트롤러 기반 라이선스 추가

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

시작하기 전에

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

이 작업에 관하여

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

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

단계

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

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

이 명령은 관리자 권한 수준에서 사용할 수 있습니다.

3. SnapManagerSuite 라이선스가 설치되었는지 확인하세요.

```
license show
```

6단계: 평가판 라이센스 제거

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

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

단계

1. SnapCenter 서버에서 PowerShell 창을 열어 MySQL 비밀번호를 재설정합니다.
   a. SnapCenterAdmin 계정에 대한 SnapCenter 서버와의 연결을 설정하려면 Open-SmConnection cmdlet을 실행합니다.
   b. Set-SmRepositoryPassword를 실행하여 MySQL 비밀번호를 재설정합니다.

      cmdlet에 대한 정보는 다음을 참조하세요. "SnapCenter 소프트웨어 Cmdlet 참조 가이드" .
2. 명령 프롬프트를 열고 mysql -u root -p를 실행하여 MySQL에 로그인합니다.

   MySQL에서 비밀번호를 입력하라는 메시지가 표시됩니다. 비밀번호를 재설정할 때 제공한 자격 증명을 입력하세요.
3. 데이터베이스에서 평가판 라이센스를 제거합니다.

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

고가용성 구성

고가용성을 위한 SnapCenter 서버 구성

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

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

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

F5를 사용하여 고가용성 구성

F5 로드 밸런서를 사용하여 고가용성을 위해 SnapCenter 서버를 구성하는 방법에 대한 지침은 다음을 참조하세요. "F5 로드 밸런서를 사용하여 고가용성을 위해 SnapCenter 서버를 구성하는 방법" .

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

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

  자세한 내용은 다음을 참조하세요. "SnapCenter 소프트웨어 Cmdlet 참조 가이드" .

추가 정보

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

NLB(네트워크 부하 분산)를 사용하여 고가용성 구성

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

SnapCenter 사용하여 NLB(네트워크 부하 분산)를 구성하는 방법에 대한 정보는 다음을 참조하세요. "SnapCenter 로 NLB를 구성하는 방법" .

AWS Elastic Load Balancing(ELB)을 사용하여 고가용성 구성

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

단계

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

- 위치: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
- 키: DisabledComponents
- 유형: REG_DWORD
- 값: 0x20

b. 완전히 정규화된 도메인 이름이 DNS 또는 로컬 호스트 구성을 통해 IPv4 주소로 확인될 수 있는지 확인하세요.

c. 시스템 프록시가 구성되어 있지 않은지 확인하세요.

d. Active Directory가 없는 설정을 사용하고 서버가 하나의 도메인에 속하지 않는 경우 두 Windows Server에서 관리자 암호가 동일한지 확인하세요.

e. 두 Windows 서버에 가상 IP를 추가합니다.

3. SnapCenter 클러스터를 생성합니다.

a. PowerShell을 시작하고 SnapCenter 에 연결합니다. `Open-SmConnection`

b. 클러스터를 생성합니다. `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`

c. 보조 서버를 추가합니다. `Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`

d. 고가용성에 대한 세부 정보를 얻으세요. `Get-SmServerConfig`

4. AWS CloudWatch에서 모니터링하여 가상 사설 IP 엔드포인트를 사용할 수 없게 될 경우 라우팅 테이블을 조정하는 Lamda 함수를 생성합니다. 자세한 내용은 다음을 참조하세요. "람다 함수 만들기" .

5. CloudWatch에서 모니터를 생성하여 SnapCenter 엔드포인트의 가용성을 모니터링합니다. 엔드포인트에 도달할 수 없는 경우 람다 함수를 트리거하도록 알람이 구성됩니다. Lambda 함수는 라우팅 테이블을 조정하여 트래픽을 활성 SnapCenter 서버로 리디렉션합니다. 자세한 내용은 다음을 참조하세요. "합성 카나리아 만들기" .

6. CloudWatch 모니터링의 대안으로 단계 함수를 사용하여 워크플로를 구현하면 장애 조치 시간을 단축할 수 있습니다. 워크플로에는 SnapCenter URL을 테스트하는 Lambda 프로브 함수, 실패 횟수를 저장하는 DynamoDB 테이블, Step 함수 자체가 포함됩니다.

a. SnapCenter URL을 조사하려면 람다 함수를 사용합니다. 자세한 내용은 다음을 참조하세요. "람다 함수 생성" .

b. 두 Step Function 반복 사이의 실패 횟수를 저장하기 위해 DynamoDB 테이블을 만듭니다. 자세한 내용은 다음을 참조하세요. "DynamoDB 테이블 시작하기" .

c. 계단 함수를 만듭니다. 자세한 내용은 다음을 참조하세요. "Step Function 문서" .

d. 단일 단계를 테스트합니다.

e. 전체 기능을 테스트합니다.

f. IAM 역할을 생성하고 Lambda 함수를 실행할 수 있는 권한을 조정합니다.

g. Step Function을 트리거하기 위한 일정을 만듭니다. 자세한 내용은 다음을 참조하세요. "Amazon EventBridge Scheduler를 사용하여 Step Functions 시작하기" .

Azure 부하 분산 장치를 사용하여 고가용성 구성

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

단계

1. Azure Portal을 사용하여 확장 집합에서 가상 머신을 만듭니다. Azure 가상 머신 확장 집합을 사용하면 부하 분산된 가상 머신 그룹을 만들고 관리할 수 있습니다. 가상 머신 인스턴스의 수는 수요나 정의된 일정에 따라 자동으로 늘어나거나 줄어들 수 있습니다. 자세한 내용은 다음을 참조하세요. "Azure Portal을 사용하여 확장 집합에서 가상 머신 만들기" .
2. 가상 머신을 구성한 후 VM 세트의 각 가상 머신에 로그인하고 두 노드 모두에 SnapCenter Server를 설치합니다.
3. 호스트 1에 클러스터를 생성합니다. `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>`
4. 보조 서버를 추가합니다. `Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>`
5. 고가용성 세부 정보를 얻으세요. `Get-SmServerConfig`
6. 필요한 경우 보조 호스트를 다시 빌드합니다. `Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. 두 번째 호스트로 장애 조치합니다. `Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== 고가용성을 위해 NLB에서 F5로 전환

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

단계

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

   cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 _Get-Help command_name_을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "SnapCenter 소프트웨어 Cmdlet 참조 가이드" .

SnapCenter MySQL 저장소의 고가용성

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

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

MySQL 고가용성(HA) 기능을 사용하려면 첫 번째 노드에서 NLB(네트워크 로드 밸런서)를 구성해야 합니다. MySQL

저장소는 설치의 일부로 이 노드에 설치됩니다. 두 번째 노드에 SnapCenter 설치하는 동안 첫 번째 노드의 F5에 가입하고 두 번째 노드에 MySQL 저장소의 복사본을 만들어야 합니다.

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

cmdlet과 함께 사용할 수 있는 매개변수와 해당 설명에 대한 정보는 _Get-Help command_name_을 실행하면 얻을 수 있습니다. 또는 다음을 참조할 수도 있습니다. "SnapCenter 소프트웨어 Cmdlet 참조 가이드" .

MySQL HA 기능과 관련된 제한 사항을 알고 있어야 합니다.

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

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

- 장애 조치가 시작되면 실행 중인 작업이 실패할 수 있습니다.

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

고가용성 구성에 대한 자세한 내용은 다음을 참조하세요. "SnapCenter 사용하여 NLB 및 ARR을 구성하는 방법" .

역할 기반 액세스 제어(RBAC) 구성

역할 만들기

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

자신의 역할을 생성하려면 "SnapCenterAdmin" 역할로 로그인해야 합니다.

단계

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

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

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

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

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

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

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

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

시작하기 전에

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

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

  항상 모든 접근 권한을 먼저 할당해야 합니다.

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

이 작업에 관하여

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

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

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

ONTAP RBAC 역할 설정에 대한 자세한 내용은 다음을 참조하세요. "ONTAP 9 관리자 인증 및 RBAC 전원 가이드" .

단계

1. 스토리지 시스템에서 다음 명령을 입력하여 새 역할을 만듭니다.

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

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

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

권한 목록에 대한 정보는 다음을 참조하세요."역할 생성 및 권한 할당을 위한 ONTAP CLI 명령" .

2. 다음 명령을 입력하여 사용자 이름을 만듭니다.

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

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

3. 다음 명령을 입력하여 사용자에게 역할을 할당합니다.

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

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

4. 다음 명령을 입력하여 사용자가 올바르게 생성되었는지 확인하세요.

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

   user_name은 3단계에서 생성한 사용자의 이름입니다.

최소 권한으로 **SVM** 역할 생성

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

단계

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

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

   각 권한에 대해 이 명령을 반복해야 합니다.

2. 사용자를 만들고 해당 사용자에게 역할을 할당합니다.

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

3. 사용자의 잠금을 해제합니다.

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

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

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

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

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

"version" -access all

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

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

"volume clone split status" -access all

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

ASA r2 시스템에 대한 SVM 역할 생성

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

단계

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

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

   각 권한에 대해 이 명령을 반복해야 합니다.

2. 사용자를 만들고 해당 사용자에게 역할을 할당합니다.

   ```
   security login create -user <user_name\> -vserver <svm_name\> -application
   ```

```
http -authmethod password -role <SVM_Role_Name\>
```

3. 사용자의 잠금을 해제합니다.

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

SVM 역할 생성 및 권한 할당을 위한 ONTAP CLI 명령

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

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

"lun mapping remove-reporting-nodes" -access all

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

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

"volume snapshot rename" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "storage-unit show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "consistency-group" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all`
- `security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name`
- `security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name`

최소 권한으로 **ONTAP** 클러스터 역할 생성

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

단계

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

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

   각 권한에 대해 이 명령을 반복해야 합니다.

2. 사용자를 만들고 해당 사용자에게 역할을 할당합니다.

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

3. 사용자의 잠금을 해제합니다.

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

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

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

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

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

"network interface create" -access readonly

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all

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

"volume clone split start" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all

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

"vserver export-policy rule modify" -access all

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

ASA r2 시스템에 대한 ONTAP 클러스터 역할 생성

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

단계

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

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

   각 권한에 대해 이 명령을 반복해야 합니다.

2. 사용자를 만들고 해당 사용자에게 역할을 할당합니다.

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

3. 사용자의 잠금을 해제합니다.

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

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

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

- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all

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

"lun mapping show" -access all

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

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

"system license delete" -access all

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

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

"vserver cifs share delete" -access all

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

사용자 또는 그룹을 추가하고 역할과 자산을 할당합니다.

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

시작하기 전에

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

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

- SnapCenter 에는 미리 정의된 역할이 여러 개 포함되어 있습니다.

  사용자에게 이러한 역할을 할당하거나 새로운 역할을 만들 수 있습니다.

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

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

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

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

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

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

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

  사용자에게 액세스 권한을 할당하기 전에 자산을 추가해야 합니다.

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

단계

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

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

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

4. *할당*을 클릭한 다음 자산 할당 페이지에서 다음을 수행합니다.
   a. 자산 드롭다운 목록에서 자산 유형을 선택하세요.
   b. 자산 테이블에서 자산을 선택합니다.

      사용자가 SnapCenter 에 자산을 추가한 경우에만 자산이 나열됩니다.

   c. 필요한 모든 자산에 대해 이 절차를 반복합니다.
   d. *저장*을 클릭하세요.
5. *제출*을 클릭하세요.

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

감사 로그 설정 구성

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

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

"SnapCenterAdmin" 역할로 로그인했어야 합니다.

이 작업에 관하여

- 알림은 다음과 같은 시나리오에서 전송됩니다.

- 감사 로그 무결성 검사 일정 또는 Syslog 서버가 활성화 또는 비활성화되었습니다.
- 감사 로그 무결성 검사, 감사 로그 또는 Syslog 서버 로그 실패
- 디스크 공간 부족

- 무결성 검사에 실패한 경우에만 이메일이 전송됩니다.
- 감사 로그 디렉토리와 감사 체크섬 로그 디렉토리 경로를 함께 수정해야 합니다. 그 중 하나만 수정할 수는 없습니다.
- 감사 로그 디렉토리와 감사 체크섬 로그 디렉토리 경로가 수정되면 이전 위치에 있는 감사 로그에 대한 무결성 검사를 수행할 수 없습니다.
- 감사 로그 디렉토리와 감사 체크섬 로그 디렉토리 경로는 SnapCenter Server의 로컬 드라이브에 있어야 합니다.

  공유 또는 네트워크 마운트 드라이브는 지원되지 않습니다.

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

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

단계

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

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

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

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

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

SnapCenter Server를 사용하여 보안된 MySQL 연결 구성

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

독립형 SnapCenter 서버 구성을 위한 보안 MySQL 연결 구성

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

다음 인증서가 생성됩니다.

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

단계

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

   자세한 내용은 다음을 참조하세요. "MySQL 버전 5.7: openssl을 사용하여 SSL 인증서 및 키 생성"

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

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

2. SSL 인증서와 키 파일을 MySQL 데이터 폴더로 복사합니다.

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

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

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

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

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

   다음 예제는 기본 폴더의 my.ini 파일의 [mysqld] 섹션에 복사된 인증서 및 키 파일을 보여줍니다.
   `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data` .

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. IIS에서 SnapCenter Server 웹 애플리케이션을 시작합니다.

HA 구성을 위한 보안 MySQL 연결 구성

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

다음 인증서가 생성됩니다.

- CA 인증서

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

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

단계

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

   자세한 내용은 다음을 참조하세요. "MySQL 버전 5.7: openssl을 사용하여 SSL 인증서 및 키 생성"

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

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

2. SSL 인증서와 키 파일을 MySQL 데이터 폴더로 복사합니다.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

      서버 인증서의 일반 이름으로 서버 FQDN을 사용하는 것이 좋습니다.

   c. SSL 인증서와 키 파일을 MySQL 데이터 폴더로 복사합니다.

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

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

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

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

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

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

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

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

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

+

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

+

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

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

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

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

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

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

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

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

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

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

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