



SnapCenter 서버 구성

SnapCenter software

NetApp
January 09, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/snapcenter/install/task_add_storage_systems.html on January 09, 2026. Always check docs.netapp.com for the latest.

목차

SnapCenter 서버 구성	1
스토리지 시스템 추가 및 프로비저닝	1
스토리지 시스템을 추가합니다	1
스토리지 접속 및 자격 증명	4
Windows 호스트에서 스토리지 용량 할당	4
VMware 환경에서 스토리지 프로비저닝	18
SnapCenter 표준 컨트롤러 기반 라이센스를 추가합니다	21
1단계: SnapManager 제품군 라이센스가 설치되었는지 확인합니다	21
2단계: 컨트롤러에 설치된 라이센스를 식별합니다	22
3단계: 컨트롤러의 일련 번호를 검색합니다	23
4단계: 컨트롤러 기반 라이센스의 일련 번호를 검색합니다	24
5단계: 컨트롤러 기반 라이센스 추가	24
6단계: 평가판 라이센스를 제거합니다	25
고가용성을 구성합니다	25
고가용성을 위해 SnapCenter 서버를 구성합니다	25
SnapCenter MySQL 리포지토리의 고가용성	29
역할 기반 액세스 제어(RBAC) 구성	30
역할을 생성합니다	30
보안 로그인 명령을 사용하여 NetApp ONTAP RBAC 역할을 추가합니다	31
최소 권한으로 SVM 역할 생성	32
ASA R2 시스템에 대한 SVM 역할을 생성합니다	37
최소 권한으로 ONTAP 클러스터 역할을 생성합니다	42
ASA R2 시스템에 대한 ONTAP 클러스터 역할을 생성합니다	48
사용자 또는 그룹을 추가하고 역할 및 자산을 할당합니다	54
감사 로그 설정을 구성합니다	56
SnapCenter 서버로 보안 MySQL 연결을 구성합니다	58
독립 실행형 SnapCenter 서버 구성에 대해 보안 MySQL 연결을 구성합니다	58
HA 구성을 위한 보안 MySQL 연결을 구성합니다	60

SnapCenter 서버 구성

스토리지 시스템 추가 및 프로비저닝

스토리지 시스템을 추가합니다

데이터 보호 및 프로비저닝 작업을 수행할 수 있도록 ONTAP 스토리지, ASA R2 시스템 또는 Amazon FSx for NetApp ONTAP에 대한 SnapCenter 액세스를 제공하는 스토리지 시스템을 설정해야 합니다.

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

시작하기 전에

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

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

- 스토리지 시스템 이름은 고유해야 합니다.

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

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

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

- 스냅샷을 SnapMirror 타겟 또는 SnapVault 대상에 복제하려는 경우, 소스 SVM 또는 클러스터뿐만 아니라, 대상 SVM 또는 클러스터에 대한 스토리지 시스템 연결을 설정해야 합니다.



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

- 단계 *

- 왼쪽 탐색 창에서 * 스토리지 시스템 * 을 클릭합니다.
- 스토리지 시스템 페이지에서 * 신규 * 를 클릭합니다.

3. 스토리지 시스템 추가 페이지에서 다음 정보를 제공합니다.

이 필드의 내용...	수행할 작업...
스토리지 시스템	<p>스토리지 시스템 이름 또는 IP 주소를 입력합니다.</p> <p> 도메인 이름을 제외한 스토리지 시스템 이름은 15자 이하여야 하며 이름을 확인할 수 있어야 합니다. 이름이 15자를 초과하는 스토리지 시스템 접속을 생성하려면 <code>Add-SmStorageConnection</code> PowerShell cmdlet을 사용합니다.</p> <p> MCC(MetroCluster Configuration)가 있는 스토리지 시스템의 경우 무중단 운영을 위해 로컬 클러스터와 피어 클러스터를 모두 등록하는 것이 좋습니다.</p> <p> SnapCenter은 서로 다른 클러스터에서 동일한 이름의 여러 SVM을 지원하지 않습니다. SnapCenter에서 지원하는 각 SVM에는 고유한 이름이 있어야 합니다.</p> <p> SnapCenter에 스토리지 연결을 추가한 후에는 ONTAP를 사용하여 SVM 또는 클러스터의 이름을 변경해서는 안 됩니다.</p> <p> 짧은 이름 또는 FQDN으로 SVM을 추가하는 경우 SnapCenter 및 플러그인 호스트 모두에서 확인할 수 있어야 합니다.</p>
사용자 이름/암호	스토리지 시스템을 액세스하는 데 필요한 권한이 있는 스토리지 사용자의 자격 증명을 입력합니다.
이벤트 관리 시스템(EMS) 및 AutoSupport 설정	<p>EMS 메시지를 스토리지 시스템 syslog에 보내거나, 적용된 보호, 완료된 복원 작업 또는 실패한 작업을 위해 스토리지 시스템으로 AutoSupport 메시지를 보내려면 해당 확인란을 선택합니다.</p> <p>스토리지 시스템에 실패한 작업에 대한 * AutoSupport 알림 전송 * 확인란을 선택하면 AutoSupport 알림을 활성화하기 위해 EMS 메시징이 필요하기 때문에 * SnapCenter 서버 이벤트를 syslog *에 기록 확인란도 선택됩니다.</p>

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

a. 플랫폼의 드롭다운 목록에서 옵션 중 하나를 선택합니다.

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

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

a. 프로토콜에서 SVM 또는 클러스터 설정 중에 구성된 프로토콜(일반적으로 HTTPS)을 선택합니다.

b. 스토리지 시스템에서 허용하는 포트를 입력합니다.

기본 포트 443은 일반적으로 작동합니다.

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

기본값은 60초입니다.

d. SVM에 관리 인터페이스가 여러 개 있는 경우 * Preferred IP * 확인란을 선택한 다음 SVM 연결을 위한 기본 IP 주소를 입력합니다.

e. 저장 * 을 클릭합니다.

1. 제출 * 을 클릭합니다.

결과 *

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

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

FSx SVM을 추가한 경우 여기에 FSx SVM이 나열됩니다.

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

fsxadmin을 사용하여 FSx 클러스터를 추가한 경우 FSx 클러스터가 여기에 나열됩니다.

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

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

- 완료 후 *

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

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



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

스토리지 접속 및 자격 증명

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

저장소 연결

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

자격 증명

- 도메인 관리자 또는 관리자 그룹의 구성원

SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹의 구성원을 지정합니다. 사용자 이름 필드에 유효한 형식은 다음과 같습니다.

- _NetBIOS\사용자 이름 _
- _도메인 FQDN\사용자 이름 _
- 사용자 이름@UPN

- 로컬 관리자(작업 그룹에만 해당)

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

사용자 이름 필드의 올바른 형식은 _ 사용자 이름 _ 입니다

- 개별 리소스 그룹에 대한 자격 증명

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

Windows 호스트에서 스토리지 용량 할당

igroup 생성 및 관리

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

igroup 작성

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

- 단계 *
- 1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.

2. 호스트 페이지에서 * iGroup * 을 클릭합니다.
3. 이니시에이터 그룹 페이지에서 * 신규 * 를 클릭합니다.
4. Create iGroup 대화 상자에서 igrup을 정의합니다.

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

5. 입력한 내용에 만족하면 * 확인 * 을 클릭합니다.

SnapCenter이 스토리지 시스템에서 igrup을 생성합니다.

igroup의 이름을 바꿉니다

SnapCenter를 사용하여 기존 igrup의 이름을 바꿀 수 있습니다.

- 단계 *
1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
 2. 호스트 페이지에서 * iGroup * 을 클릭합니다.
 3. 이니시에이터 그룹 페이지에서 * 스토리지 가상 머신 * 필드를 클릭하여 사용 가능한 SVM 목록을 표시한 다음, 이름을 바꿀 igrup에 사용할 SVM을 선택합니다.
 4. SVM의 igrup 목록에서 이름을 바꿀 igrup을 선택하고 * 이름 바꾸기 * 를 클릭합니다.
 5. igrup 이름 바꾸기 대화 상자에서 igrup의 새 이름을 입력하고 * 이름 바꾸기 * 를 클릭합니다.

igroup을 수정합니다

SnapCenter를 사용하여 igrup 이니시에이터를 기존 igrup에 추가할 수 있습니다. igrup을 작성하는 동안 하나의 호스트만 추가할 수 있습니다. 클러스터에 대한 igrup을 작성하려는 경우 igrup을 수정하여 해당 igrup에 다른 노드를 추가할 수 있습니다.

- 단계 *
1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
 2. 호스트 페이지에서 * iGroup * 을 클릭합니다.
 3. 이니시에이터 그룹 페이지에서 * 스토리지 가상 머신 * 필드를 클릭하여 사용 가능한 SVM의 드롭다운 목록을 표시한 다음, 수정할 igrup에 사용할 SVM을 선택합니다.

4. igrup 목록에서 igrup을 선택하고 * igrup에 이니시에이터 추가 * 를 클릭합니다.
5. 호스트를 선택합니다.
6. 이니시에이터를 선택하고 * OK * 를 클릭합니다.

igroup을 삭제합니다

더 이상 필요하지 않은 경우 SnapCenter를 사용하여 igrup을 삭제할 수 있습니다.

- 단계 *
1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
 2. 호스트 페이지에서 * iGroup * 을 클릭합니다.
 3. 이니시에이터 그룹 페이지에서 * 스토리지 가상 머신 * 필드를 클릭하여 사용 가능한 SVM의 드롭다운 목록을 표시한 다음, 삭제할 igrup에 사용할 SVM을 선택합니다.
 4. SVM의 igrup 목록에서 삭제할 igrup을 선택하고 * Delete * 를 클릭합니다.
 5. Delete igrup (그룹 삭제) 대화 상자에서 * OK * (확인 *)를 클릭합니다.

SnapCenter이 igrup을 삭제합니다.

디스크를 생성하고 관리합니다

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

- SnapCenter는 기본 디스크만 지원합니다. 동적 디스크는 지원되지 않습니다.
- GPT의 경우 하나의 데이터 파티션 및 MBR의 경우 NTFS 또는 CSVFS로 포맷된 하나의 볼륨이 있고 하나의 마운트 경로가 있는 하나의 기본 파티션이 허용됩니다.
- 지원되는 파티션 스타일: GPT, MBR; VMware UEFI VM에서는 iSCSI 디스크만 지원됩니다



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

호스트의 디스크를 봅니다

SnapCenter로 관리하는 각 Windows 호스트에서 디스크를 볼 수 있습니다.

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

디스크가 나열됩니다.

클러스터링된 디스크를 봅니다

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

- 단계 *

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

디스크가 나열됩니다.

iSCSI 세션을 설정합니다

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

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

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

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

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

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

- 단계 *

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

세션 설정 마법사가 표시됩니다.

6. 세션 설정 마법사에서 타겟을 식별합니다.

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

7. 입력한 내용에 만족하면 * 연결 * 을 클릭합니다.

SnapCenter가 iSCSI 세션을 설정합니다.

8. 이 절차를 반복하여 각 타겟에 대한 세션을 설정합니다.

FC 연결 또는 iSCSI 연결 LUN 또는 디스크를 생성합니다

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

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

시작하기 전에

- 스토리지 시스템에서 LUN에 대한 볼륨을 생성해야 합니다.

볼륨에는 LUN만 있어야 하며 SnapCenter를 사용하여 생성한 LUN만 포함해야 합니다.



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

- 스토리지 시스템에서 FC 또는 iSCSI 서비스를 시작해야 합니다.
- iSCSI를 사용하는 경우 스토리지 시스템과 iSCSI 세션을 설정해야 합니다.
- Windows용 SnapCenter 플러그인 패키지는 디스크를 생성하는 호스트에만 설치해야 합니다.
- 이 작업에 대한 정보 *
- Windows Server 페일오버 클러스터의 호스트에서 LUN을 공유하지 않는 한 LUN을 둘 이상의 호스트에 연결할 수 없습니다.
- CSV(Cluster Shared Volumes)를 사용하는 Windows Server 페일오버 클러스터의 호스트가 LUN을 공유하는 경우 클러스터 그룹을 소유하는 호스트에 디스크를 생성해야 합니다.
- 단계 *
 - 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
 - 호스트 페이지에서 * 디스크 * 를 클릭합니다.

3. 호스트 * 드롭다운 목록에서 호스트를 선택합니다.

4. 새로 만들기 * 를 클릭합니다.

디스크 생성 마법사가 열립니다.

5. LUN 이름 페이지에서 LUN을 확인합니다.

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

6. 디스크 유형 페이지에서 디스크 유형을 선택합니다.

선택...	만약...
전용 디스크	LUN은 하나의 호스트만 액세스할 수 있습니다. 리소스 그룹 * 필드는 무시하십시오.
공유 디스크	LUN은 Windows Server 페일오버 클러스터의 호스트에서 공유됩니다. 리소스 그룹 * 필드에 클러스터 리소스 그룹의 이름을 입력합니다. 페일오버 클러스터의 한 호스트에만 디스크를 생성해야 합니다.
CSV(클러스터 공유 볼륨)	LUN은 CSV를 사용하는 Windows Server 페일오버 클러스터의 호스트에서 공유됩니다. 리소스 그룹 * 필드에 클러스터 리소스 그룹의 이름을 입력합니다. 디스크를 생성할 호스트가 클러스터 그룹의 소유자인지 확인합니다.

7. 드라이브 속성 페이지에서 드라이브 속성을 지정합니다.

속성	설명
마운트 지점을 자동으로 할당합니다	<p>SnapCenter는 시스템 드라이브에 따라 볼륨 마운트 지점을 자동으로 할당합니다.</p> <p>예를 들어, 시스템 드라이브가 C:인 경우 자동 할당은 C: 드라이브(C:\scmnpt) 아래에 볼륨 마운트 지점을 생성합니다. 공유 디스크에는 자동 할당이 지원되지 않습니다.</p>
드라이브 문자를 할당합니다	인접한 드롭다운 목록에서 선택한 드라이브에 디스크를 마운트합니다.
볼륨 마운트 지점을 사용합니다	<p>인접한 필드에 지정한 드라이브 경로에 디스크를 마운트합니다.</p> <p>볼륨 마운트 지점의 루트는 디스크를 생성하는 호스트가 소유해야 합니다.</p>
드라이브 문자 또는 볼륨 마운트 지점을 할당하지 마십시오	Windows에서 디스크를 수동으로 마운트하려면 이 옵션을 선택합니다.
LUN 크기입니다	<p>최소 150MB의 LUN 크기를 지정합니다.</p> <p>인접 드롭다운 목록에서 MB, GB 또는 TB를 선택합니다.</p>
이 LUN을 호스팅하는 볼륨에 쓴 프로비저닝을 사용합니다	<p>쓴 LUN을 프로비저닝합니다.</p> <p>쓴 프로비저닝은 필요한 만큼의 스토리지 공간만 한 번에 할당하므로 LUN이 최대 가용 용량까지 효율적으로 성장할 수 있습니다.</p> <p>필요한 모든 LUN 스토리지를 수용할 수 있는 충분한 공간이 볼륨에 있는지 확인하십시오.</p>
파티션 유형을 선택합니다	<p>GUID 파티션 테이블의 GPT 파티션 또는 마스터 부트 레코드의 MBR 파티션을 선택합니다.</p> <p>MBR 파티션은 Windows Server 장애 조치 클러스터에서 정렬 불량 문제를 일으킬 수 있습니다.</p> <p> UEFI(Unified Extensible Firmware Interface) 파티션 디스크는 지원되지 않습니다.</p>

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

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

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

선택...	만약...
선택한 이니시에이터에 대해 새 igrup을 생성합니다	선택한 이니시에이터에 대해 새 igrup을 생성하려고 합니다.
기존 igrup을 선택하거나 선택한 이니시에이터에 대한 새 igrup을 지정합니다	<p>선택한 이니시에이터에 대해 기존 igrup을 지정하거나 지정한 이름의 새 igrup을 생성합니다.</p> <p>igrup 이름 * 필드에 igrup 이름을 입력합니다. 기존 igrup 이름의 처음 몇 글자를 입력하여 필드를 자동으로 작성합니다.</p>

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

SnapCenter는 LUN을 생성하여 호스트의 지정된 드라이브 또는 드라이브 경로에 연결합니다.

디스크 크기를 조정합니다

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

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

복원 작업 후 LUN 크기가 조정된 후 LUN에 추가된 데이터는 크기가 조정된 후 생성된 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 조정할 디스크를 선택한 다음 * 크기 조정 * 을 클릭합니다.
5. 디스크 크기 조정 대화 상자에서 슬라이더 도구를 사용하여 디스크의 새 크기를 지정하거나 크기 필드에 새 크기를 입력합니다.



크기를 수동으로 입력하는 경우 축소 또는 확장 단추가 적절하게 활성화되기 전에 크기 필드 바깥쪽을 클릭해야 합니다. 또한 MB, GB 또는 TB를 클릭하여 측정 단위를 지정해야 합니다.

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

SnapCenter는 디스크의 크기를 조정합니다.

디스크를 연결합니다

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

시작하기 전에

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

- 단계 *

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

디스크 연결 마법사가 열립니다.

5. LUN 이름 페이지에서 접속할 LUN을 확인합니다.

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

6. 디스크 유형 페이지에서 디스크 유형을 선택합니다.

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

7. 드라이브 속성 페이지에서 드라이브 속성을 지정합니다.

속성	설명
자동 할당	SnapCenter에서 시스템 드라이브에 따라 볼륨 마운트 지점을 자동으로 할당합니다. 예를 들어, 시스템 드라이브가 C:인 경우 자동 할당 속성은 C: 드라이브(C:\scmnpt) 아래에 볼륨 마운트 지점을 만듭니다. 공유 디스크에는 자동 할당 속성이 지원되지 않습니다.

속성	설명
드라이브 문자를 할당합니다	인접 드롭다운 목록에서 선택한 드라이브에 디스크를 마운트합니다.
볼륨 마운트 지점을 사용합니다	인접 필드에 지정한 드라이브 경로에 디스크를 마운트합니다. 볼륨 마운트 지점의 루트는 디스크를 생성하는 호스트가 소유해야 합니다.
드라이브 문자 또는 볼륨 마운트 지점을 할당하지 마십시오	Windows에서 디스크를 수동으로 마운트하려면 이 옵션을 선택합니다.

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

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

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

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

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

SnapCenter는 LUN을 호스트의 지정된 드라이브 또는 드라이브 경로에 연결합니다.

디스크 연결을 해제합니다

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

시작하기 전에

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

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

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

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

디스크가 나열됩니다.

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

SnapCenter가 디스크의 연결을 끊습니다.

디스크를 삭제합니다

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

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

디스크가 나열됩니다.

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

SnapCenter가 디스크를 삭제합니다.

SMB 공유를 생성하고 관리합니다

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

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

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



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

SMB 공유를 생성합니다

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

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

- 단계 *

- 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
- 호스트 페이지에서 * 공유 * 를 클릭합니다.
- Storage Virtual Machine * 드롭다운 목록에서 SVM을 선택합니다.
- 새로 만들기 * 를 클릭합니다.

새 공유 대화 상자가 열립니다.

- 새 공유 대화 상자에서 공유를 정의합니다.

이 필드에서...	수행할 작업...
설명	공유에 대한 설명 텍스트를 입력합니다.
공유 이름	<p>공유 이름(예: test_share)을 입력합니다.</p> <p>공유에 대해 입력한 이름도 볼륨 이름으로 사용됩니다.</p> <p>공유 이름:</p> <ul style="list-style-type: none">UTF-8 문자열이어야 합니다.0x00에서 0x1F(둘 다 포함), 0x22(큰따옴표), 특수 문자 "V[]:(세로 막대) <>+=;?"와 같은 문자는 포함할 수 없습니다

이 필드에서...	수행할 작업...
공유 경로	<ul style="list-style-type: none"> 필드를 클릭하여 새 파일 시스템 경로(예: /)를 입력합니다. 필드를 두 번 클릭하여 기존 파일 시스템 경로 목록에서 선택합니다.

6. 입력한 내용에 만족하면 * 확인 * 을 클릭합니다.

SnapCenter은 SVM에서 SMB 공유를 생성합니다.

SMB 공유를 삭제합니다

SMB 공유가 더 이상 필요하지 않은 경우 삭제할 수 있습니다.

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

SnapCenter는 SVM에서 SMB 공유를 삭제합니다.

스토리지 시스템의 공간을 재확보할 수 있습니다

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

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

시작하기 전에

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

전체 NTFS 파일 시스템이 스캔되었는지 확인해야 합니다.

- 이 작업에 대한 정보 *
- 공간 재확보는 시간이 많이 걸리고 CPU가 많이 필요하므로 스토리지 시스템과 Windows 호스트 사용량이 적은

경우에 작업을 실행하는 것이 좋습니다.

- 공간 재확보는 거의 모든 가용 공간을 재확보하지만 100%는 재확보하지 않습니다.
- 공간 재확보를 수행하는 동안 디스크 조각 모음을 동시에 실행해서는 안 됩니다.

이렇게 하면 재확보 프로세스가 느려질 수 있습니다.

- 단계 *

애플리케이션 서버 PowerShell 명령 프롬프트에서 다음 명령을 입력합니다.

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

drive_path 는 LUN에 매핑된 드라이브 경로입니다.

PowerShell cmdlet을 사용하여 스토리지 용량 할당

SnapCenter GUI를 사용하여 호스트 프로비저닝 및 공간 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 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 참조할 수도 ["SnapCenter 소프트웨어 cmdlet 참조 가이드"](#)입니다.

서버에서 Windows용 SnapDrive를 제거하여 SnapCenter PowerShell cmdlet이 손상된 경우 을 참조하십시오 ["Windows용 SnapDrive를 제거하면 SnapCenter cmdlet이 중단됨"](#).

VMware 환경에서 스토리지 프로비저닝

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

지원되는 **VMware** 게스트 OS 플랫폼

- 지원되는 Windows Server 버전
- Microsoft 클러스터 구성

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

- RDM LUN입니다

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

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

VMware ESXi 서버 관련 제한 사항

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

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

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

SnapCenter RDM 작업에 필요한 최소 vCenter 권한

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

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

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

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

Microsoft 클러스터에서 FC RDM LUN을 관리합니다

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

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

요구 사항

Windows용 플러그인은 특정 구성 요구 사항을 충족하는 경우 두 개의 서로 다른 ESX 또는 ESXi 서버에 속하는 두 개의 서로 다른 가상 시스템에서 FC RDM LUN을 사용하는 Microsoft 클러스터를 지원합니다.

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

필요한 경우 iSCSI를 통해 공유 데이터 저장소를 생성할 수도 있습니다.

- 공유 RDM LUN은 물리적 호환성 모드에 있어야 합니다.

- Windows용 플러그인 외부에서 공유 RDM LUN을 수동으로 생성해야 합니다.

공유 스토리지에는 가상 디스크를 사용할 수 없습니다.

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

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

반가상화 유형의 SCSI 컨트롤러는 VMware Microsoft 클러스터에서 지원되지 않습니다.



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

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

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

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

RDM LUN을 생성할 때 이니시에이터 그룹은 ALUA를 통해 생성됩니다.

제한 사항

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



이 기능은 ESX 5.5i 이전의 릴리즈에서는 지원되지 않습니다.

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

이니시에이터는 FC 또는 Microsoft iSCSI 중 하나여야 하며 둘 다 사용할 수는 없습니다.

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

공유 FC RDM LUN을 생성합니다

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

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

SnapCenter 표준 컨트롤러 기반 라이센스를 추가합니다

FAS, AFF 또는 ASA 스토리지 컨트롤러를 사용하는 경우 SnapCenter 표준 컨트롤러 기반 라이센스가 필요합니다.

컨트롤러 기반 라이센스는 다음과 같은 특성을 가지고 있습니다.

- 프리미엄 또는 플래시 번들 구매 시 SnapCenter 표준 자격 포함(기본 팩 제외)
- 무제한 저장소 사용
- ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 FAS, AFF 또는 ASA 스토리지 컨트롤러에 직접 추가합니다.



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

- 컨트롤러의 일련 번호에 잠금 상태입니다

필요한 라이센스에 대한 자세한 내용은 ["SnapCenter 라이센스"](#) 참조하십시오.

1단계: SnapManager 제품군 라이센스가 설치되었는지 확인합니다

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. SnapManager Suite 라이선스와 SnapCenter Standard 컨트롤러 기반 라이선스라는 이름은 혼용되지만, 동일한 라이선스를 나타냅니다.

단계

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

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

3. Storage Connections 목록에서 Controller License 열을 찾습니다.

컨트롤러 라이센스 열에는 다음 상태가 표시됩니다.

◦

SnapManager 제품군 라이센스가 FAS, AFF 또는 ASA 운영 스토리지 시스템에 설치되어 있음을 나타냅니다.

-  SnapManager 제품군 라이센스가 FAS, AFF 또는 ASA 운영 스토리지 시스템에 설치되어 있지 않음을 나타냅니다.
- 해당 없음은 스토리지 컨트롤러가 Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select 또는 보조 스토리지 플랫폼에 있으므로 SnapManager 제품군 라이센스가 적용되지 않음을 나타냅니다.

2단계: 컨트롤러에 설치된 라이센스를 식별합니다

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



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.

예제 출력

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

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

Serial Number: 1-81-0000000000000000000000000000xx
Owner: cluster1-01
Package          Type      Description          Expiration
-----          -----
NFS              license   NFS License          -
CIFS             license   CIFS License          -
iSCSI            license   iSCSI License          -
FCP              license   FCP License          -
SnapRestore      license   SnapRestore License      -
SnapMirror       license   SnapMirror License      -
FlexClone        license   FlexClone License      -
SnapVault        license   SnapVault License      -
SnapManagerSuite license   SnapManagerSuite License      -
```

이 예제에서는 SnapManagerSuite 라이센스가 설치되어 있으므로 추가 SnapCenter 라이센스 작업이 필요하지 않습니다.

3단계: 컨트롤러의 일련 번호를 검색합니다

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.

예제 출력

```
cluster1::> system show -instance

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

3. 일련 번호를 기록합니다.

4단계: 컨트롤러 기반 라이센스의 일련 번호를 검색합니다

FAS, 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 Support 사이트 로그인 자격 증명이 있어야 합니다.

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

- 컨트롤러의 일련 번호가 있어야 합니다.

단계

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

Software Licenses

Selection Criteria

Choose a method by which to search

▶ Enter Value: **Go!**

Enter the Cluster Serial Number value without dashes.

- OR -

▶ Show Me All: For Company: **Go!**

지정된 컨트롤러의 라이센스 목록이 표시됩니다.

4. SnapCenter Standard 또는 SnapManagerSuite 라이센스를 찾아서 기록합니다.

5단계: 컨트롤러 기반 라이센스 추가

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

시작하기 전에

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

이 작업에 대해

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

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

단계

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

'시스템 사용권 추가-사용권 코드 사용권_키'

이 명령은 admin 권한 수준에서 사용할 수 있습니다.

3. SnapManagerSuite 라이센스가 설치되었는지 확인합니다.

'라이선스 쇼'

6단계: 평가판 라이센스를 제거합니다

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



SnapCenter 표준 컨트롤러 기반 라이센스를 사용하는 경우에만 평가판 라이센스를 수동으로 제거해야 합니다.

단계

1. SnapCenter 서버에서 PowerShell 창을 열어 MySQL 암호를 재설정합니다.
 - a. SnapCenterAdmin 계정에 대한 SnapCenter 서버와의 연결을 설정하려면 Open-SmConnection cmdlet을 실행합니다.
 - b. Set-SmRepositoryPassword를 실행하여 MySQL 암호를 재설정합니다.cmdlet에 대한 정보는 다음을 참조하세요. "[SnapCenter 소프트웨어 cmdlet 참조 가이드](#)".
2. 명령 프롬프트를 열고 MySQL -u root -p 를 실행하여 MySQL에 로그인합니다.
MySQL에서 암호를 묻는 메시지를 표시합니다. 암호를 재설정하는 동안 제공한 자격 증명을 입력합니다.
3. 데이터베이스에서 평가판 라이센스를 제거합니다.

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

고가용성을 구성합니다

고가용성을 위해 SnapCenter 서버를 구성합니다

Windows 또는 Linux에서 실행되는 SnapCenter에서 HA(고가용성)를 지원하려면 F5 로드 밸런서를 설치할 수 있습니다. F5를 사용하면 SnapCenter 서버가 동일한 위치에 있는 최대 2개의 호스트에서 액티브-패시브 구성을 지원할 수 있습니다. SnapCenter에서 F5 로드

밸런서를 사용하려면 SnapCenter 서버를 구성하고 F5 로드 밸런서를 구성해야 합니다.

NLB(네트워크 부하 분산)를 구성하여 SnapCenter 고가용성을 설정할 수도 있습니다. 고가용성을 위해 SnapCenter 설치 외부에서 NLB를 수동으로 구성해야 합니다.

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

F5를 사용하여 고가용성을 구성합니다

F5 로드 밸런서를 사용하여 고가용성을 위해 SnapCenter 서버를 구성하는 방법에 대한 지침은 다음을 참조하세요. ["F5 로드 밸런서를 사용하여 고가용성을 위해 SnapCenter 서버를 구성하는 방법"](#).

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

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

자세한 내용은 을 ["SnapCenter 소프트웨어 cmdlet 참조 가이드"](#)참조하십시오.

추가 정보

- 고가용성을 위해 SnapCenter를 설치하고 구성한 후 F5 클러스터 IP를 가리키도록 SnapCenter 바탕 화면 바로 가기를 편집합니다.
- SnapCenter 서버 간에 페일오버가 발생하고 기존 SnapCenter 세션도 있는 경우 브라우저를 닫고 SnapCenter에 다시 로그온해야 합니다.
- 로드 밸런서 설정(NLB 또는 F5)에서 NLB 또는 F5 호스트에 의해 부분적으로 확인된 호스트를 추가하고 SnapCenter 호스트가 이 호스트에 도달할 수 없는 경우 SnapCenter 호스트 페이지는 호스트 중단 및 실행 중 상태로 자주 전환합니다. 이 문제를 해결하려면 두 SnapCenter 호스트가 모두 NLB 또는 F5 호스트에서 호스트를 해결할 수 있는지 확인해야 합니다.
- MFA 설정에 대한 SnapCenter 명령은 모든 호스트에서 실행해야 합니다. AD FS(Active Directory Federation Services) 서버에서 F5 클러스터 세부 정보를 사용하여 일반 당사자 구성을 수행해야 합니다. MFA가 설정된 후에는 호스트 레벨 SnapCenter UI 액세스가 차단됩니다.
- 페일오버 중에는 감사 로그 설정이 두 번째 호스트에 반영되지 않습니다. 따라서 F5 패시브 호스트가 활성화되면 수동으로 감사 로그 설정을 반복해야 합니다.

NLB(Network Load Balancing)를 사용하여 고가용성 구성

NLB(네트워크 부하 분산)를 구성하여 SnapCenter 고가용성을 설정할 수 있습니다. 고가용성을 위해 SnapCenter 설치 외부에서 NLB를 수동으로 구성해야 합니다.

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

AWS ELB(Elastic Load Balancing)를 사용하여 고가용성 구성

AWS(Amazon Web Services)에서 SnapCenter 서버 2대를 별도의 AZ(가용 영역)에 설정하고 자동 장애 조치가 가능하도록 구성하여 고가용성 SnapCenter 환경을 구성할 수 있습니다. 이 아키텍처에는 가상 사설 IP 주소, 라우팅 테이블, 활성 및 대기 MySQL 데이터베이스 간의 동기화가 포함됩니다.

단계

1. AWS에서 가상 전용 오버레이 IP를 구성합니다. 자세한 내용은 을 ["가상 전용 오버레이 IP를 구성합니다"](#) 참조하십시오.
2. Windows 호스트를 준비합니다
 - a. IPv4의 우선 순위를 IPv6보다 높게 지정:

- 위치: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
 - 키: DisabledComponents
 - REG_DWORD 를 입력합니다
 - 값: 0x20
- b. DNS를 통해 또는 IPv4 주소에 대한 로컬 호스트 구성을 통해 정규화된 도메인 이름을 확인할 수 있는지 확인합니다.
- c. 시스템 프록시가 구성되어 있지 않은지 확인합니다.
- d. Active Directory 없이 설치 프로그램을 사용할 때 Windows Server에서 관리자 암호가 동일하고 서버가 한 도메인에 있지 않은지 확인합니다.
- e. 두 Windows Server에 가상 IP를 추가합니다.
3. SnapCenter 클러스터를 생성합니다.
- a. Powershell을 시작하고 SnapCenter에 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. 고가용성 세부 정보를 확인하십시오. Get-SmServerConfig
4. Lamda 기능을 생성하여 AWS CloudWatch에서 모니터링하는 가상 사설 IP 끝점을 사용할 수 없게 될 경우 라우팅 테이블을 조정합니다. 자세한 내용은 ["Lambda 함수를 만듭니다"](#) 참조하십시오.
5. CloudWatch에서 모니터를 만들어 SnapCenter 끝점의 가용성을 모니터링합니다. 종점에 도달할 수 없는 경우 Lambda 기능을 트리거하도록 알람이 구성됩니다. Lambda 기능은 트래픽을 활성 SnapCenter 서버로 리디렉션하도록 라우팅 테이블을 조정합니다. 자세한 내용은 ["합성 캐너리를 만듭니다"](#) 참조하십시오.
6. CloudWatch 모니터링의 대안으로 STEP 기능을 사용하여 워크플로우를 구현하여 페일오버 시간을 줄입니다. 워크플로에는 SnapCenter URL을 테스트하는 Lambda 프로브 기능, 오류 카운트를 저장하기 위한 DynamoDB 테이블 및 Step 함수 자체가 포함됩니다.
- a. SnapCenter URL을 탐색하는 데 lambda 함수를 사용합니다. 자세한 내용은 ["Lambda 함수를 만듭니다"](#) 참조하십시오.
 - b. 2단계 함수 반복 간 실패 횟수를 저장하기 위해 DynamoDB 테이블을 만듭니다. 자세한 내용은 ["DynamoDB 테이블을 사용해 보세요"](#) 참조하십시오.
 - c. 단계 기능을 만듭니다. 자세한 내용은 ["STEP 기능 문서화"](#) 참조하십시오.
 - d. 단일 단계를 테스트합니다.
 - e. 전체 기능을 테스트합니다.
 - f. IAM 역할을 생성하고 Lambda 기능을 실행할 수 있도록 권한을 조정합니다.
 - g. 단계 기능을 트리거하기 위한 스케줄을 생성합니다. 자세한 내용은 ["Amazon EventBridge Scheduler를 사용하여 단계 기능을 시작합니다"](#) 참조하십시오.

Azure 로드 밸런서를 사용하여 고가용성을 구성합니다

Azure 로드 밸런서를 사용하여 고가용성 SnapCenter 환경을 구성할 수 있습니다.

단계

1. Azure Portal을 사용하여 확장 집합으로 가상 머신을 생성합니다. Azure 가상 머신 스케일 세트를 사용하여 로드 밸런싱된 가상 머신 그룹을 만들고 관리할 수 있습니다. 가상 머신 인스턴스의 수는 수요 또는 정의된 일정에 따라 자동으로 증가 또는 감소할 수 있습니다. 자세한 내용은 ["Azure Portal을 사용하여 확장 집합으로 가상 머신을 생성합니다"](#) 참조하십시오.
2. 가상 머신을 구성한 후 VM 세트의 각 가상 머신에 로그인하고 두 노드에 SnapCenter Server를 설치합니다.
3. 호스트 1에서 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 확인합니다. `Get-SmServerConfig`
6. 필요한 경우 보조 호스트를 재구축합니다. `Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. 두 번째 호스트로 페일오버합니다. `Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== NLB에서 F5로 전환하여 고가용성을 보장합니다

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

- 단계 *

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

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

SnapCenter MySQL 리포지토리의 고가용성

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

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

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

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

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

MySQL HA 기능과 관련된 제한 사항을 알고 있어야 합니다.

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

`_Set-SmRepositoryConfig_cmdlet`을 사용하여 강제 대체 작동을 시작할 수 있습니다.

- 페일오버가 시작되면 실행 중인 작업이 실패할 수 있습니다.

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

고가용성 구성에 대한 자세한 내용은 을 참조하십시오 "[SnapCenter를 사용하여 NLB 및 ARR을 구성하는 방법](#)".

역할 기반 액세스 제어(RBAC) 구성

역할을 생성합니다

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

자신의 역할을 생성하려면 "SnapCenterAdmin" 역할로 로그인해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
2. 설정 페이지에서 * 역할 * 을 클릭합니다.
3. 을 클릭합니다 .
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 있습니다 * 를 선택하여 역할의 다른 구성원이 리소스 목록을 새로 고친 후 볼륨 및 호스트와 같은 리소스를 볼 수 있도록 합니다.

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



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

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

보안 로그인 명령을 사용하여 NetApp ONTAP RBAC 역할을 추가합니다

스토리지 시스템에서 clustered ONTAP을 실행 중인 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 디렉터리에 권한을 부여합니다.

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

항상 먼저 모든 액세스 권한을 할당해야 합니다.

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

이 작업에 대해

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

이 도구는 자동으로 ONTAP 권한 설정을 올바르게 처리합니다. 예를 들어 RBAC NetApp ONTAP용 사용자 작성기 도구는 모든 액세스 권한 Privileges가 먼저 표시되도록 Privileges를 올바른 순서로 자동으로 추가합니다. 읽기 전용 권한을 먼저 추가한 다음 모든 액세스 권한을 추가하면 ONTAP에서 모든 액세스 권한을 종복으로 표시하고 무시합니다.

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

ONTAP RBAC 역할 설정에 대한 자세한 내용은 [을 참조하십시오 "ONTAP 9 관리자 인증 및 RBAC 전원 가이드"](#).

단계

1. 스토리지 시스템에서 다음 명령을 입력하여 새 역할을 생성합니다.

```
'Security login role create <role_name> - cmddirname "command" - access all - vserver <svm_name>'
```

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



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

사용 권한 목록에 대한 자세한 내용은 ["역할을 생성하고 권한을 할당하는 ONTAP CLI 명령입니다"](#).

2. 다음 명령을 입력하여 사용자 이름을 생성합니다.

'보안 로그인 생성 - 사용자 이름 <user_name> - 응용 프로그램 ontapi - AuthMethod <password> - 역할 <name_of_role_in_step_1> - vserver <svm_name> - 설명 "user_description"

- user_name은 만들고 있는 사용자의 이름입니다.
- password>는 사용자의 암호입니다. 암호를 지정하지 않으면 시스템에 암호를 입력하라는 메시지가 표시됩니다.
- SVM_NAME은 SVM의 이름입니다.

3. 다음 명령을 입력하여 사용자에게 역할을 할당합니다.

'보안 로그인 수정 사용자 이름 <user_name> – vserver <svm_name> - role <role_name> - application ontapi-application console - AuthMethod <password>'

- user_name>은 2단계에서 만든 사용자의 이름입니다. 이 명령을 사용하면 사용자를 수정하여 역할에 연결할 수 있습니다.
- svm_name>은 SVM의 이름입니다.
- role_name>은 1단계에서 만든 역할의 이름입니다.
- password>는 사용자의 암호입니다. 암호를 지정하지 않으면 시스템에 암호를 입력하라는 메시지가 표시됩니다.

4. 다음 명령을 입력하여 사용자가 올바르게 생성되었는지 확인합니다.

'Security login show –vserver <svm_name>-user-or-group-name <user_name>'

user_name 은 3단계에서 만든 사용자의 이름입니다.

최소 권한으로 SVM 역할 생성

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

- 단계 *

1. 스토리지 시스템에서 역할을 생성하고 역할에 모든 권한을 할당합니다.

'보안 로그인 역할 생성 – vserver <svm_name> - role <SVM_Role_Name> - cmddirname <permission>'



각 권한에 대해 이 명령을 반복해야 합니다.

1. 사용자를 생성하고 해당 사용자에게 역할을 할당합니다.

'보안 로그인 생성 - 사용자 <user_name> - vserver <svm_name> - application ontapi - AuthMethod

```
password - role <SVM_Role_Name>'
```

2. 사용자 잠금을 해제합니다.

```
'보안 로그인 잠금 해제 - 사용자 <user_name> - vserver <svm_name>'
```

SVM 역할 생성 및 권한 할당을 위한 ONTAP CLI 명령

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

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- 'Security login role create - vserver SVM_Name - role SVM_Role_Name - cmddirname "job history show" - access all'
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job 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 igrup add" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun igrup create" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun igrup delete" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun igrup rename" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun igrup show" - access all'을 선택합니다
- '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'
- '보안 로그인 역할 생성 - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver export-policy rule show" - access all'을 선택합니다
- '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 역할을 생성합니다

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 생성하고 역할에 모든 권한을 할당합니다.

'보안 로그인 역할 생성 – vserver <svm_name> - role <SVM_Role_Name> - cmddirname <permission>'



각 권한에 대해 이 명령을 반복해야 합니다.

1. 사용자를 생성하고 해당 사용자에게 역할을 할당합니다.

security login create -user <user_name> -vserver <svm_name> -application http -authmethod password -role <SVM_Role_Name>

2. 사용자 잠금을 해제합니다.

'보안 로그인 잠금 해제 - 사용자 <user_name> - vserver <svm_name>'

SVM 역할 생성 및 권한 할당을 위한 ONTAP CLI 명령

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

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- 'Security login role create - vserver SVM_Name - role SVM_Role_Name - cmddirname "job history show" - access all'

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job 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 igrup add" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun igrup create" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun igrup delete" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun igrup rename" - access all'
- 'Security login role create - vserver SVM_name - role SVM_Role_Name - cmddirname "lun igrup show" - access all'을 선택합니다
- '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'
- '보안 로그인 역할 생성 - vserver SVM_name - role SVM_Role_Name - cmddirname "vserver export-policy rule show" - access all'을 선택합니다
 - '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 역할을 생성합니다

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

- 단계 *

1. 스토리지 시스템에서 역할을 생성하고 역할에 모든 권한을 할당합니다.

'Security login role create – vserver <cluster_name> - role <role_name> - cmddirname <permission>'



각 권한에 대해 이 명령을 반복해야 합니다.

1. 사용자를 생성하고 해당 사용자에게 역할을 할당합니다.

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

2. 사용자 잠금을 해제합니다.

'보안 로그인 잠금 해제 - 사용자 <user_name> - vserver <cluster_name>'

클러스터 역할을 생성하고 권한을 할당하는 ONTAP CLI 명령입니다

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

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

```
"cluster peer show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"cluster show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"event generate-autosupport-log" -access all
• 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "job history show" - access all'
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
"job 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 igrup add" - access all'
• 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igrup create" - access all'
• 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igrup delete" - access all'
• 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igrup modify" - access all'
• 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igrup rename" - access all'
• 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igrup 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_Name - cmddirname "SnapMirror create" - vserver Cluster_name - access all'
- 'Security login role create - 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 cleanup" - 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'을 참조하십시오
 - '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'을 선택합니다
 - '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'
- '보안 로그인 역할 생성 - 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'
- '보안 로그인 역할 생성 - 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 역할을 생성합니다

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

- 단계 *

1. 스토리지 시스템에서 역할을 생성하고 역할에 모든 권한을 할당합니다.

'Security login role create – vserver <cluster_name> - role <role_name> - cmddirname <permission>'



각 권한에 대해 이 명령을 반복해야 합니다.

1. 사용자를 생성하고 해당 사용자에게 역할을 할당합니다.

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

2. 사용자 잠금을 해제합니다.

'보안 로그인 잠금 해제 - 사용자 <user_name> - vserver <cluster_name>'

클러스터 역할을 생성하고 권한을 할당하는 ONTAP CLI 명령입니다

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

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

- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "job history show" - access all'
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job 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 igrup add" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igrup create" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igrup delete" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igrup modify" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igrup rename" - access all'
- 'Security login role create - vserver Cluster_name - role Role_Name - cmddirname "lun igrup 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_Name - cmddirname "SnapMirror create" - vserver Cluster_name - access all'
- 'Security login role create - 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 cleanup" - 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'을 참조하십시오
- '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'을 선택합니다
- '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'

- 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'
- '보안 로그인 역할 생성 - 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'
- '보안 로그인 역할 생성 - 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 역할 및 자산을 할당합니다

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

시작하기 전에

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



사용자 이름 및 그룹 이름에는 공백(), 하이픈(-), 밑줄(_) 및 콜론(:)과 같은 특수 문자만 포함할 수 있습니다.

- SnapCenter에는 몇 가지 사전 정의된 역할이 포함되어 있습니다.

이러한 역할을 사용자에게 할당하거나 새 역할을 만들 수 있습니다.

- SnapCenter RBAC에 추가되는 AD 사용자 및 AD 그룹은 Active Directory의 사용자 컨테이너 및 컴퓨터 컨테이너에 대한 읽기 권한을 가지고 있어야 합니다.
- 적절한 권한이 포함된 사용자 또는 그룹에 역할을 할당한 후에는 호스트 및 스토리지 연결과 같은 SnapCenter 자산에 대한 사용자 액세스를 할당해야 합니다.

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

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

작동	자산 할당
리소스 보호	호스트, 정책
백업	호스트, 리소스 그룹, 정책
복원	호스트, 리소스 그룹

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

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

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

- 스냅샷을 복제하려는 경우 작업을 수행하는 사용자에게 소스 볼륨과 대상 볼륨에 대한 스토리지 접속을 할당해야 합니다.

사용자에게 액세스 권한을 할당하기 전에 자산을 추가해야 합니다.

 VMware vSphere용 SnapCenter 플러그인 기능을 사용하여 VM, VMDK 또는 데이터 저장소를 보호하는 경우 VMware vSphere GUI를 사용하여 vCenter 사용자를 VMware vSphere용 SnapCenter 플러그인 역할에 추가해야 합니다. VMware vSphere 역할에 대한 자세한 내용은 ["VMware vSphere용 SnapCenter 플러그인과 함께 패키지로 제공되는 사전 정의된 역할"](#)를 참조하십시오.

- 단계 *

- 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
- 설정 페이지에서 * 사용자 및 액세스 * > * 를 클릭합니다 .
- Active Directory 또는 작업 그룹에서 사용자/그룹 추가 페이지에서 다음을 수행합니다.

이 필드의 내용...	수행할 작업...
액세스 유형	<p>도메인 또는 작업 그룹을 선택합니다</p> <p>도메인 인증 유형의 경우 사용자를 역할에 추가할 사용자 또는 그룹의 도메인 이름을 지정해야 합니다.</p> <p>기본적으로 로그인한 도메인 이름으로 미리 채워집니다.</p> <p> 신뢰할 수 없는 도메인은 * 설정 * > * 글로벌 설정 * > * 도메인 설정 * 페이지에서 등록해야 합니다.</p>

이 필드의 내용...	수행할 작업...
유형	<p>사용자 또는 그룹을 선택합니다</p> <p> SnapCenter는 메일 그룹이 아닌 보안 그룹만 지원합니다.</p>
사용자 이름	<p>a. 부분 사용자 이름을 입력한 다음 * 추가 * 를 클릭합니다.</p> <p> 사용자 이름은 대소문자를 구분합니다.</p> <p>b. 검색 목록에서 사용자 이름을 선택합니다.</p> <p> 다른 도메인 또는 신뢰할 수 없는 도메인의 사용자를 추가할 때는 도메인 간 사용자에 대한 검색 목록이 없으므로 사용자 이름을 완전히 입력해야 합니다.</p> <p>선택한 역할에 다른 사용자 또는 그룹을 추가하려면 이 단계를 반복합니다.</p>
역할	사용자를 추가할 역할을 선택합니다.

4. Assign * 을 클릭한 다음 Assign Assets 페이지에서 다음을 수행합니다.

- 자산 * 드롭다운 목록에서 자산 유형을 선택합니다.
- [자산] 테이블에서 자산을 선택합니다.

사용자가 자산을 SnapCenter에 추가한 경우에만 자산이 나열됩니다.

- 필요한 모든 자산에 대해 이 절차를 반복합니다.
- 저장 * 을 클릭합니다.

5. 제출 * 을 클릭합니다.

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

감사 로그 설정을 구성합니다

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

감사 로그는 각 감사 이벤트에 대해 디지털 서명된 다이제스트를 생성하여 무단 수정으로부터 보호합니다. 생성된

다이제스트는 별도의 감사 체크섬 파일에 보관되며, 컨텐츠의 무결성을 보장하기 위해 정기적인 무결성 검사를 수행합니다.

"SnapCenterAdmin" 역할로 로그인해야 합니다.

이 작업에 대해

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

공유 또는 네트워크 마운트 드라이브는 지원되지 않습니다.

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

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 Get-Help command_name을 실행하여 얻을 수 있습니다. 또는 를 참조할 수도 ["SnapCenter 소프트웨어 cmdlet 참조 가이드"](#)있습니다.

단계

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

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

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

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

- Syslog 서버 호스트를 입력합니다

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

SnapCenter 서버로 보안 MySQL 연결을 구성합니다

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

독립 실행형 SnapCenter 서버 구성에 대해 보안 MySQL 연결을 구성합니다

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

다음 인증서가 생성됩니다.

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

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

자세한 내용은 을 참조하십시오 ["MySQL 버전 5.7: openssl을 사용하여 SSL 인증서 및 키 만들기"](#)



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

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

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

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

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

기본 MySQL Server 구성 파일(my.ini) 경로는 'C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini'입니다.



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

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

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

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

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

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

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

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

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

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

4. 인터넷 정보 서버(IIS)에서 SnapCenter 서버 웹 응용 프로그램을 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 키의 값을 보여 줍니다.

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

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

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

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

+

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

+

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

1. IIS에서 SnapCenter 서버 웹 응용 프로그램을 시작합니다.

HA 구성을 위한 보안 MySQL 연결을 구성합니다

SnapCenter 서버와 MySQL 서버 간의 통신을 보호하려면 고가용성(HA) 노드 모두에 대해 SSL(Secure Sockets Layer) 인증서와 키 파일을 생성할 수 있습니다. MySQL 서버 및 HA 노드에서 인증서와 키 파일을 구성해야 합니다.

다음 인증서가 생성됩니다.

- CA 인증서

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

- 두 HA 노드에 대한 서버 공용 인증서 및 서버 개인 키 파일
- 두 HA 노드에 대한 클라이언트 공용 인증서 및 클라이언트 개인 키 파일
- 단계 *

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

자세한 내용은 을 참조하십시오 ["MySQL 버전 5.7: openssl을 사용하여 SSL 인증서 및 키 만들기"](#)



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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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



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

서버 인증서의 일반 이름으로 서버 FQDN을 사용하는 것이 좋습니다.

- c. SSL 인증서 및 키 파일을 MySQL Data 폴더에 복사합니다.
d. MySQL 서버 구성 파일(my.ini)에서 CA 인증서, 서버 공용 인증서, 클라이언트 공용 인증서, 서버 개인 키 및 클라이언트 개인 키 경로를 업데이트합니다.



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

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

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

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

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

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

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

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

+

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

+

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

5. 두 HA 노드의 IIS(인터넷 정보 서버)에서 SnapCenter 서버 웹 응용 프로그램을 중지합니다.
6. 두 HA 노드에서 MySQL 서비스를 다시 시작합니다.
7. 두 HA 노드에 대해 SnapManager.Web.UI.dll.config 파일에서 MySQLProtocol 키 값을 업데이트합니다.

다음 예제에서는 SnapManager.Web.UI.dll.config 파일에서 업데이트된 MySQLProtocol 키의 값을 보여 줍니다.

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

8. SnapManager.Web.UI.dll.config 파일을 두 HA 노드에 대해 my.ini 파일의 [client] 섹션에서 지정한 경로로 업데이트합니다.

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

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

+

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

+

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

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

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

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그레픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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