SnapCenter 서버 설치

SnapCenter Software 5.0

NetApp
October 15, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/snapcenter-50/install/install_workflow.html on October 15, 2025. Always check docs.netapp.com for the latest.

목차

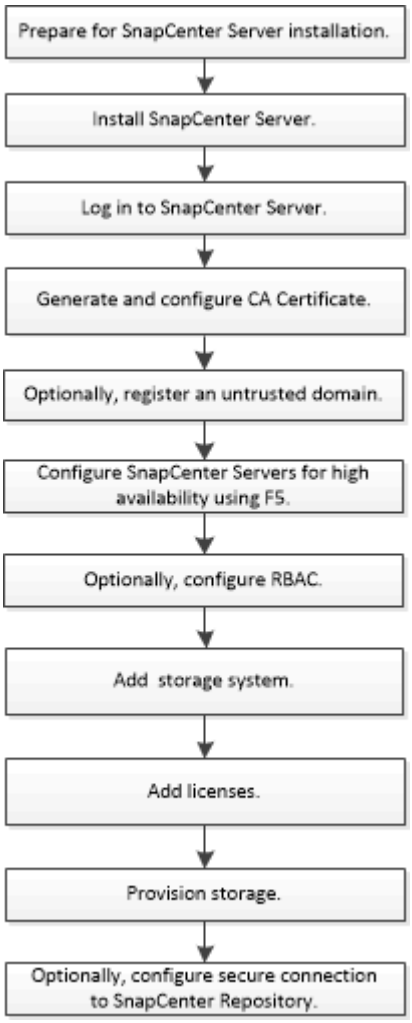
SnapCenter 서버 설치 1
- 설치 워크플로우 1
- SnapCenter 서버 설치를 준비합니다 1
  - 도메인 및 작업 그룹 요구 사항 1
  - 요구사항을 충족해야 합니다 2
  - SAN 호스트 요구 사항 3
  - 지원되는 스토리지 시스템 및 애플리케이션 3
  - 지원되는 브라우저 4
  - 연결 및 포트 요구 사항 4
  - SnapCenter 라이센스 7
  - 자격 증명에 대한 인증 방법입니다 9
  - 스토리지 접속 및 자격 증명 10
  - 멀티팩터 인증(MFA) 11
- SnapCenter 서버를 설치합니다 21
- RBAC 승인을 사용하여 SnapCenter에 로그인합니다 22
  - 멀티팩터 인증(MFA)을 사용하여 SnapCenter에 로그인 23
  - SnapCenter 기본 GUI 세션 시간 초과를 수정합니다 24
  - SSL 3.0을 비활성화하여 SnapCenter 웹 서버를 보호합니다 24
- CA 인증서를 구성합니다 25
  - CA 인증서 CSR 파일을 생성합니다 25
  - CA 인증서를 가져옵니다 25
  - CA 인증서 지문을 받습니다 26
  - Windows 호스트 플러그인 서비스를 사용하여 CA 인증서를 구성합니다 26
  - SnapCenter 사이트를 사용하여 CA 인증서를 구성합니다 27
  - SnapCenter에 대해 CA 인증서를 활성화합니다 28
- 양방향 SSL 통신을 구성하고 사용하도록 설정합니다 28
  - 양방향 SSL 통신을 구성합니다 28
  - 양방향 SSL 통신을 활성화합니다 31
- 인증서 기반 인증을 구성합니다 32
  - SnapCenter 서버에서 CA(인증 기관) 인증서를 내보냅니다 32
  - CA(인증 기관) 인증서를 Windows 플러그인 호스트로 가져옵니다 33
  - CA 인증서를 UNIX 호스트 플러그인으로 가져오고 SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성합니다 34
  - 인증서 기반 인증을 사용합니다 35
- Active Directory, LDAP 및 LDAPS를 구성합니다 36
  - 신뢰할 수 없는 Active Directory 도메인을 등록합니다 36
  - LDAPS에 대한 CA 클라이언트 인증서를 구성합니다 37
- 고가용성을 구성합니다 38
  - F5를 사용하여 고가용성을 위해 SnapCenter 서버를 구성합니다 38
  - Microsoft 네트워크 로드 밸런서를 수동으로 구성합니다 40

고가용성을 위해 NLB에서 F5로 전환합니다 . . . 40
SnapCenter MySQL 리포지토리의 고가용성 . . . 40
SnapCenter 인증서를 내보냅니다 . . . 41
역할 기반 액세스 제어(RBAC) 구성 . . . 42
사용자 또는 그룹을 추가하고 역할 및 자산을 할당합니다 . . . 42
역할을 생성합니다 . . . 44
보안 로그인 명령을 사용하여 ONTAP RBAC 역할을 추가합니다 . . . 45
최소 권한으로 SVM 역할 생성 . . . 47
최소 권한으로 ONTAP 클러스터 역할을 생성합니다 . . . 51
Active Directory 읽기 권한을 사용하도록 IIS 응용 프로그램 풀을 구성합니다 . . . 57
감사 로그 설정을 구성합니다 . . . 57
스토리지 시스템을 추가합니다 . . . 59
SnapCenter 표준 컨트롤러 기반 라이센스를 추가합니다 . . . 62
1단계: SnapManager 제품군 라이센스가 설치되었는지 확인합니다 . . . 62
2단계: 컨트롤러에 설치된 라이센스를 식별합니다 . . . 63
3단계: 컨트롤러의 일련 번호를 검색합니다 . . . 64
4단계: 컨트롤러 기반 라이센스의 일련 번호를 검색합니다 . . . 65
5단계: 컨트롤러 기반 라이센스 추가 . . . 66
6단계: 평가판 라이센스를 제거합니다 . . . 67
SnapCenter 표준 용량 기반 라이센스 추가 . . . 67
스토리지 시스템을 프로비저닝합니다 . . . 71
Windows 호스트에서 스토리지 용량 할당 . . . 71
VMware 환경에서 스토리지 프로비저닝 . . . 85
SnapCenter 서버로 보안 MySQL 연결을 구성합니다 . . . 88
독립 실행형 SnapCenter 서버 구성에 대해 보안 MySQL 연결을 구성합니다 . . . 88
HA 구성을 위한 보안 MySQL 연결을 구성합니다 . . . 90
설치 중에 Windows 호스트에서 활성화된 기능입니다 . . . 94

SnapCenter 서버 설치

설치 워크플로우

워크플로우는 SnapCenter 서버를 설치하고 구성하는 데 필요한 여러 작업을 보여 줍니다.



SnapCenter 서버 설치를 준비합니다

도메인 및 작업 그룹 요구 사항

SnapCenter 서버는 도메인 또는 작업 그룹에 있는 시스템에 설치할 수 있습니다. 설치에 사용되는 사용자는 작업 그룹과 도메인 모두에 대해 컴퓨터에 대한 관리자 권한을 가져야 합니다.

Windows 호스트에 SnapCenter 서버 및 SnapCenter 플러그인을 설치하려면 다음 중 하나를 사용해야 합니다.

- * Active Directory 도메인 *

  로컬 관리자 권한이 있는 도메인 사용자를 사용해야 합니다. 도메인 사용자는 Windows 호스트에 있는 로컬 관리자 그룹의 구성원이어야 합니다.

- * 작업 그룹 *

  로컬 관리자 권한이 있는 로컬 계정을 사용해야 합니다.

도메인 트러스트, 다중 도메인 포리스트 및 교차 도메인 트러스트가 지원되지만 교차 포리스트 도메인은 지원되지 않습니다. Active Directory 도메인 및 트러스트에 대한 Microsoft 설명서에 자세한 내용이 나와 있습니다.

SnapCenter 서버를 설치한 후에는 SnapCenter 호스트가 있는 도메인을 변경해서는 안 됩니다. SnapCenter 서버를 설치할 때 있던 도메인에서 SnapCenter 서버 호스트를 제거한 다음 SnapCenter 서버를 제거하려고 하면 제거 작업이 실패합니다.

요구사항을 충족해야 합니다

SnapCenter 서버를 설치하기 전에 공간 및 크기 조정 요구 사항을 숙지해야 합니다. 사용 가능한 시스템 및 보안 업데이트도 적용해야 합니다.

항목	요구 사항
운영 체제	Microsoft Windows 운영 체제의 영어, 독일어, 일본어 및 중국어 간체 버전만 지원됩니다. 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
최소 CPU 수입니다	4개 코어
최소 RAM	8 GB MySQL Server 버퍼 풀은 전체 RAM의 20%를 사용합니다.
SnapCenter 서버 소프트웨어 및 로그의 최소 하드 드라이브 공간	4 GB SnapCenter 서버가 설치된 동일한 드라이브에 SnapCenter 저장소가 있는 경우 10GB를 사용하는 것이 좋습니다.
SnapCenter 리포지토리에 대한 최소 하드 드라이브 공간입니다	6 GB 참고: SnapCenter 저장소가 설치된 동일한 드라이브에 SnapCenter 서버가 있는 경우 10GB를 사용하는 것이 좋습니다.

항목	요구 사항
필요한 소프트웨어 패키지	• Microsoft .NET Framework 4.7.2 이상 • WMF(Windows Management Framework) 4.0 이상 • PowerShell 4.0 이상 의 경우. 자세한 문제 해결 정보는 을 참조하십시오 "인터넷에 연결되지 않은 기존 시스템의 경우 SnapCenter 업그레이드 또는 설치가 실패합니다".

SAN 호스트 요구 사항

SnapCenter 호스트가 FC/iSCSI 환경의 일부인 경우 ONTAP 스토리지에 액세스할 수 있도록 시스템에 추가 소프트웨어를 설치해야 할 수 있습니다.

SnapCenter에는 호스트 유틸리티 또는 DSM이 포함되어 있지 않습니다. SnapCenter 호스트가 SAN 환경의 일부인 경우 다음 소프트웨어를 설치하고 구성해야 할 수 있습니다.

- Host Utilities(호스트 유틸리티)

  호스트 유틸리티는 FC와 iSCSI를 지원하며 Windows Server에서 MPIO를 사용할 수 있도록 합니다. 자세한 내용은 을 "Host Utilities 설명서"참조하십시오.

- Windows MPIO용 Microsoft DSM

  이 소프트웨어는 Windows MPIO 드라이버와 함께 작동하여 NetApp과 Windows 호스트 컴퓨터 간의 여러 경로를 관리합니다.

  고가용성 구성을 위해서는 DSM이 필요합니다.

  ⓘ ONTAP DSM을 사용하는 경우 Microsoft DSM으로 마이그레이션해야 합니다. 자세한 내용은 을 "ONTAP DSM에서 Microsoft DSM으로 마이그레이션하는 방법"참조하십시오.

지원되는 스토리지 시스템 및 애플리케이션

지원되는 스토리지 시스템, 애플리케이션 및 데이터베이스를 알아야 합니다.

- SnapCenter는 ONTAP 9 .8 이상을 지원하여 데이터를 보호합니다.
- SnapCenter는 ONTAP 소프트웨어 4.5 P1 패치 릴리즈로부터 데이터를 보호하기 위해 NetApp SnapCenter용 Amazon FSx를 지원합니다.

  NetApp ONTAP용 Amazon FSx를 사용하는 경우 데이터 보호 작업을 수행하기 위해 SnapCenter 서버 호스트 플러그인이 4.5 P1 이상으로 업그레이드되었는지 확인합니다.

  Amazon FSx for NetApp ONTAP에 대한 자세한 내용은 을 참조하십시오 "NetApp ONTAP용 Amazon FSx 문서".

- SnapCenter는 다양한 애플리케이션 및 데이터베이스의 보호를 지원합니다.

  지원되는 응용 프로그램 및 데이터베이스에 대한 자세한 내용은 을 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

- SnapCenter 4.9 P1 이상은 AWS(Amazon Web Services) 기반 VMware Cloud 환경에서 Oracle 및 Microsoft SQL 워크로드 보호를 지원합니다.

  자세한 내용은 을 "AWS SDDC 환경의 VMware Cloud에서 NetApp SnapCenter를 사용하여 Oracle, MS SQL 워크로드를 보호하십시오"참조하십시오.

지원되는 브라우저

SnapCenter 소프트웨어는 여러 브라우저에서 사용할 수 있습니다.

- 크롬

  v66을 사용하는 경우 SnapCenter GUI를 시작하지 못할 수 있습니다.

- Microsoft Edge 110.0.1587.17 이상

지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

연결 및 포트 요구 사항

SnapCenter 서버 및 응용 프로그램 또는 데이터베이스 플러그인을 설치하기 전에 연결 및 포트 요구 사항이 충족되었는지 확인해야 합니다.

- 응용 프로그램이 포트를 공유할 수 없습니다.

  각 포트는 해당 애플리케이션 전용으로 사용되어야 합니다.

- 사용자 지정 가능한 포트의 경우 기본 포트를 사용하지 않으려는 경우 설치 중에 사용자 지정 포트를 선택할 수 있습니다.

  설치 후 호스트 수정 마법사를 사용하여 플러그인 포트를 변경할 수 있습니다.

- 고정 포트의 경우 기본 포트 번호를 그대로 사용해야 합니다.
- 방화벽
  - 방화벽, 프록시 또는 기타 네트워크 장치가 연결을 방해해서는 안 됩니다.
  - SnapCenter를 설치할 때 사용자 지정 포트를 지정하는 경우 SnapCenter 플러그인 로더의 해당 포트에 대한 방화벽 규칙을 플러그인 호스트에 추가해야 합니다.

다음 표에는 여러 포트와 해당 기본값이 나와 있습니다.

포트의 유형입니다	기본 포트입니다
SnapCenter 웹 포트	8146(HTTPS), 양방향, 사용자 지정 가능(URL_\https://server:8146_) SnapCenter 클라이언트(SnapCenter 사용자)와 SnapCenter 서버 간의 통신에 사용됩니다. 플러그인 호스트에서 SnapCenter 서버로의 통신에도 사용됩니다. 포트를 사용자 지정하려면 을 참조하십시오 "설치 마법사를 사용하여 SnapCenter 서버를 설치합니다."
SnapCenter SMCore 통신 포트입니다	8145(HTTPS), 양방향, 사용자 지정 가능 이 포트는 SnapCenter 서버와 SnapCenter 플러그인이 설치된 호스트 간의 통신에 사용됩니다. 포트를 사용자 지정하려면 을 참조하십시오 "설치 마법사를 사용하여 SnapCenter 서버를 설치합니다."
MySQL 포트	3306(HTTPS), 양방향 이 포트는 SnapCenter 및 MySQL 리포지토리 데이터베이스 간의 통신에 사용됩니다. SnapCenter 서버에서 MySQL 서버로의 보안 연결을 만들 수 있습니다. "자세한 정보" 포트를 사용자 지정하려면 을 참조하십시오 "설치 마법사를 사용하여 SnapCenter 서버를 설치합니다."
Windows 플러그인 호스트	135, 445(TCP) 135번 및 445번 포트 외에도 Microsoft에서 지정한 동적 포트 범위도 열려 있어야 합니다. 원격 설치 작업은 이 포트 범위를 동적으로 검색하는 WMI(Windows Management Instrumentation) 서비스를 사용합니다. 지원되는 동적 포트 범위에 대한 자세한 내용은 을 참조하십시오 "Windows에 대한 서비스 개요 및 네트워크 포트 요구 사항" 이 포트는 SnapCenter 서버와 플러그인이 설치되는 호스트 간의 통신에 사용됩니다. 플러그인 패키지 바이너리를 Windows 플러그인 호스트에 푸시하려면 포트가 플러그인 호스트에서만 열려 있어야 하며 설치 후 닫을 수 있습니다.

포트의 유형입니다	기본 포트입니다
Linux 또는 AIX 플러그인 호스트	22(SSH) 포트는 SnapCenter 서버와 플러그인이 설치되는 호스트 간의 통신에 사용됩니다. 이 포트는 SnapCenter에서 플러그인 패키지 바이너리를 Linux 또는 AIX 플러그인 호스트에 복사하는 데 사용되며 방화벽 또는 iptables에서 열거나 제외해야 합니다.
Windows용 SnapCenter 플러그인 패키지, Linux용 SnapCenter 플러그인 패키지 또는 AIX용 SnapCenter 플러그인 패키지	8145(HTTPS), 양방향, 사용자 지정 가능 이 포트는 플러그인 패키지가 설치된 SMCore와 호스트 간의 통신에 사용됩니다. 또한 SVM 관리 LIF와 SnapCenter 서버 간에 통신 경로를 개방해야 합니다. 포트를 사용자 지정하려면 또는 을 참조하십시오 "호스트를 추가하고 Microsoft Windows용 SnapCenter 플러그인을 설치합니다" "호스트를 추가하고 Linux 또는 AIX용 SnapCenter 플러그인 패키지를 설치합니다."
Oracle 데이터베이스용 SnapCenter 플러그인	27216, 사용자 지정 가능 기본 JDBC 포트는 Oracle용 플러그인에서 Oracle 데이터베이스에 연결하는 데 사용됩니다. 포트를 사용자 지정하려면 을 참조하십시오 "호스트를 추가하고 Linux 또는 AIX용 SnapCenter 플러그인 패키지를 설치합니다."
SnapCenter용 맞춤형 플러그인	9090(HTTPS), 고정 사용자 지정 플러그인 호스트에서만 사용되는 내부 포트입니다. 방화벽 예외가 필요하지 않습니다. SnapCenter 서버와 사용자 지정 플러그인 간의 통신은 포트 8145를 통해 라우팅됩니다.
ONTAP 클러스터 또는 SVM 통신 포트	443(HTTPS), 양방향 80(HTTP), 양방향 이 포트는 SnapCenter Server를 실행하는 호스트와 SVM 간 통신에 SAL(Storage Abstraction Layer)에서 사용됩니다. 이 포트는 현재 SnapCenter 플러그인 호스트와 SVM 간 통신에 SnapCenter의 SAL에서 사용됩니다.

포트의 유형입니다	기본 포트입니다
SAP HANA 데이터베이스 vCode용 SnapCenter 플러그인 맞춤법 검사기	3instance_number13 또는 3instance_number15, HTTP 또는 HTTPS, 양방향 및 사용자 지정 가능 MDC(멀티테넌트 데이터베이스 컨테이너) 단일 테넌트의 경우 포트 번호는 13으로 끝나며 MDC가 아닌 경우 포트 번호는 15로 끝납니다. 예를 들어, 32013은 인스턴스 20의 포트 번호이고 31015는 인스턴스 10의 포트 번호입니다. 포트를 사용자 지정하려면 을 참조하십시오 "호스트를 추가하고 원격 호스트에 플러그인 패키지를 설치합니다."
도메인 컨트롤러 통신 포트입니다	인증이 제대로 작동하기 위해 도메인 컨트롤러의 방화벽에서 열어야 하는 포트를 확인하려면 Microsoft 설명서를 참조하십시오. SnapCenter 서버, 플러그인 호스트 또는 다른 Windows 클라이언트가 사용자를 인증할 수 있도록 도메인 컨트롤러에서 Microsoft 필수 포트를 열어야 합니다.

포트 세부 정보를 수정하려면 을 참조하십시오 "플러그인 호스트를 수정합니다".

SnapCenter 라이센스

SnapCenter에는 애플리케이션, 데이터베이스, 파일 시스템 및 가상 머신의 데이터 보호를 위해 몇 가지 라이센스가 필요합니다. 설치하는 SnapCenter 라이센스 유형은 스토리지 환경과 사용하려는 기능에 따라 다릅니다.

라이센스	필요한 경우
SnapCenter 표준 컨트롤러 기반	FAS, AFF, All SAN 어레이(ASA)에 필요 SnapCenter 표준 라이센스는 컨트롤러 기반 라이센스이며 프리미엄 번들의 일부로 포함됩니다. SnapManager 제품군 라이센스가 있는 경우 SnapCenter 표준 라이센스 사용 권한도 제공됩니다. FAS, AFF 또는 ASA 스토리지를 사용하여 평가판을 통해 SnapCenter를 설치하려는 경우, 세일즈 담당자에게 문의하여 프리미엄 번들 평가 라이센스를 얻을 수 있습니다. SnapCenter는 데이터 보호 번들의 일부로 제공됩니다. A400 이상을 구입한 경우 데이터 보호 번들을 구입해야 합니다.

라이센스	필요한 경우
SnapCenter 표준 용량 기반	ONTAP Select 및 Cloud Volumes ONTAP에 필요합니다 Cloud Volumes ONTAP 또는 ONTAP Select 고객인 경우 SnapCenter에서 관리하는 데이터를 기준으로 TB당 용량 기반 라이센스를 구입해야 합니다. 기본적으로 SnapCenter는 90일 100TB SnapCenter 표준 용량 기반 평가판 라이센스를 기본 제공합니다. 자세한 내용은 세일즈 담당자에게 문의하십시오.
SnapMirror 또는 SnapVault	ONTAP SnapCenter에서 복제를 사용하는 경우 SnapMirror 또는 SnapVault 라이센스가 필요합니다.
SnapRestore	백업을 복원 및 확인하는 데 필요합니다. 지원합니다 • SnapVault 대상 시스템에서 원격 검증을 수행하고 백업에서 복원하는 데 필요합니다. • SnapMirror 대상 시스템에서 원격 검증을 수행하는 데 필요합니다.
플랙스클론	데이터베이스 클론 생성 및 검증 작업에 필요합니다. 지원합니다 • SnapVault 대상 시스템에서 보조 볼트 백업에서 클론을 생성하는 데 필요합니다. • SnapMirror 대상 시스템에서 보조 SnapMirror 백업에서 클론을 생성해야 합니다.
프로토콜	• LUN에 대한 iSCSI 또는 FC 라이센스 • SMB 공유용 CIFS 라이센스 • NFS 유형 VMDK에 대한 NFS 라이센스 • VMFS 유형 VMDK에 대한 iSCSI 또는 FC 라이센스 소스 볼륨을 사용할 수 없는 경우 데이터를 제공하는 SnapMirror 대상 시스템에 필요합니다.

라이센스	필요한 경우
SnapCenter 표준 라이센스(선택 사항)	보조 대상 SnapCenter 표준 라이센스를 보조 대상에 추가하는 것이 좋지만 필수는 아닙니다. 보조 대상에서 SnapCenter 표준 라이센스가 활성화되어 있지 않으면 페일오버 작업을 수행한 후 SnapCenter를 사용하여 보조 대상의 리소스를 백업할 수 없습니다. 그러나 복제 및 검증 작업을 수행하려면 보조 대상에 FlexClone 라이센스가 필요합니다.

SnapCenter 고급 및 SnapCenter NAS 파일 서비스 라이센스는 더 이상 사용되지 않으며 더 이상 사용할 수 없습니다.

하나 이상의 SnapCenter 라이센스를 설치해야 합니다. 라이센스를 추가하는 방법에 대한 자세한 내용은 또는 를 "SnapCenter 표준 컨트롤러 기반 라이센스를 추가합니다" "SnapCenter 표준 용량 기반 라이센스 추가"참조하십시오.

SMBR(Single Mailbox Recovery) 라이센스

Exchange용 SnapCenter 플러그인을 사용하여 Microsoft Exchange Server 데이터베이스 및 SMBR(Single Mailbox Recovery)을 관리하는 경우 사용자 메일박스를 기준으로 별도로 구입해야 하는 SMBR용 추가 라이센스가 필요합니다.

NetApp ® Single Mailbox Recovery는 2023년 5월 12일 EOA(End of Availability)로 제공됩니다. 자세한 내용은 을 "CPC-00507를 참조하십시오"참조하십시오. NetApp은 2020년 6월 24일에 출시된 마케팅 부품 번호를 통해 지원 자격 기간 동안 메일박스 용량, 유지보수, 지원을 구매한 고객을 계속 지원할 예정입니다.

NetApp Single Mailbox Recovery는 Ontrack에서 제공하는 파트너 제품입니다. OnTrack PowerControls는 NetApp Single Mailbox Recovery와 유사한 기능을 제공합니다. 고객은 2023년 5월 12일 EOA 날짜 이후에 세분화된 메일박스 복구를 위해 Ontrack(licensingteam@ontrack.com 통해 Ontrack PowerControls 소프트웨어 라이센스와 Ontrack PowerControls 유지 관리 및 지원 갱신을 조달할 수 있습니다.

자격 증명에 대한 인증 방법입니다

자격 증명은 응용 프로그램이나 환경에 따라 다른 인증 방법을 사용합니다. 자격 증명은 SnapCenter 작업을 수행할 수 있도록 사용자를 인증합니다. 플러그인 설치를 위한 자격 증명 세트와 데이터 보호 작업을 위한 다른 자격 증명 세트를 생성해야 합니다.

Windows 인증

Windows 인증 방법은 Active Directory에 대해 인증합니다. Windows 인증의 경우 Active Directory는 SnapCenter 외부에서 설정됩니다. SnapCenter는 추가 구성 없이 인증합니다. 호스트 추가, 플러그인 패키지 설치 및 작업 예약 등의 작업을 수행하려면 Windows 자격 증명이 필요합니다.

신뢰할 수 없는 도메인 인증입니다

SnapCenter를 사용하면 신뢰할 수 없는 도메인에 속하는 사용자 및 그룹을 사용하여 Windows 자격 증명을 만들 수 있습니다. 인증에 성공하려면 신뢰할 수 없는 도메인을 SnapCenter에 등록해야 합니다.

로컬 워크그룹 인증

SnapCenter를 사용하면 로컬 작업 그룹 사용자 및 그룹을 사용하여 Windows 자격 증명을 생성할 수 있습니다. 로컬 작업 그룹 사용자 및 그룹에 대한 Windows 인증은 Windows 자격 증명 생성 시 수행되지 않지만 호스트 등록 및 기타 호스트 작업이 수행될 때까지 지연됩니다.

SQL Server 인증

SQL 인증 메서드는 SQL Server 인스턴스에 대해 인증합니다. 즉, SnapCenter에서 SQL Server 인스턴스를 검색한 다음 따라서 SQL 자격 증명을 추가하기 전에 호스트를 추가하고 플러그인 패키지를 설치하고 리소스를 새로 고쳐야 합니다. SQL Server에서 일정을 예약하거나 리소스를 검색하는 등의 작업을 수행하려면 SQL Server 인증이 필요합니다.

Linux 인증

Linux 인증 방법은 Linux 호스트에 대해 인증합니다. Linux 호스트를 추가하고 SnapCenter GUI에서 Linux용 SnapCenter 플러그인 패키지를 원격으로 설치하는 초기 단계 동안 Linux 인증이 필요합니다.

AIX 인증

AIX 인증 방법은 AIX 호스트에 대해 인증합니다. AIX 호스트를 추가하고 SnapCenter GUI에서 AIX용 SnapCenter 플러그인 패키지를 원격으로 설치하는 초기 단계 동안 AIX 인증이 필요합니다.

Oracle 데이터베이스 인증

Oracle 데이터베이스 인증 방법은 Oracle 데이터베이스에 대해 인증합니다. 데이터베이스 호스트에서 운영 체제(OS) 인증이 비활성화되어 있는 경우 Oracle 데이터베이스에서 작업을 수행하려면 Oracle 데이터베이스 인증이 필요합니다. 따라서 Oracle 데이터베이스 자격 증명을 추가하기 전에 sysdba 권한을 사용하여 Oracle 데이터베이스에 Oracle 사용자를 생성해야 합니다.

Oracle ASM 인증

Oracle ASM 인증 방법은 Oracle ASM(Automatic Storage Management) 인스턴스에 대해 인증합니다. Oracle ASM 인스턴스에 액세스해야 하고 데이터베이스 호스트에서 운영 체제(OS) 인증이 비활성화된 경우 Oracle ASM 인증이 필요합니다. 따라서 Oracle ASM 자격 증명을 추가하기 전에 ASM 인스턴스에서 sysasm 권한을 가진 Oracle 사용자를 생성해야 합니다.

RMAN 카탈로그 인증

RMAN 카탈로그 인증 방법은 Oracle RMAN(Recovery Manager) 카탈로그 데이터베이스에 대해 인증합니다. 외부 카탈로그 메커니즘을 구성하고 데이터베이스를 카탈로그 데이터베이스에 등록한 경우 RMAN 카탈로그 인증을 추가해야 합니다.

스토리지 접속 및 자격 증명

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

- * 스토리지 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 시스템에서 도메인 관리자 또는 관리자 그룹의 구성원을 지정합니다. 사용자 이름 필드의 유효한 형식은 다음과 같습니다.

    - _NetBIOS\사용자 이름 _
    - _도메인 FQDN\사용자 이름 _
    - 사용자 이름@*UPN*
  - 로컬 관리자(작업 그룹에만 해당)

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

  사용자 이름 필드의 올바른 형식은 _ 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.

멀티팩터 인증(MFA)

멀티팩터 인증(MFA) 관리

AD FS(Active Directory Federation Service) 서버 및 SnapCenter 서버에서 MFA(Multi-Factor Authentication) 기능을 관리할 수 있습니다.

멀티팩터 인증(MFA) 활성화

PowerShell 명령을 사용하여 SnapCenter Server에 MFA 기능을 사용하도록 설정할 수 있습니다.

이 작업에 대해

- SnapCenter는 다른 애플리케이션이 동일한 AD FS에 구성되어 있을 때 SSO 기반 로그인을 지원합니다. 특정 AD FS 구성에서 SnapCenter는 AD FS 세션 지속성에 따라 보안상의 이유로 사용자 인증을 요구할 수 있습니다.
- cmdlet과 함께 사용할 수 있는 매개 변수 및 해당 설명은 를 실행하여 확인할 수 `Get-Help command_name`있습니다. 또는 을 참조하십시오 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

시작하기 전에

- Windows AD FS(Active Directory Federation Service)가 해당 도메인에서 실행 중이어야 합니다.
- Azure MFA, Cisco Duo 등과 같은 AD FS 지원 다중 요소 인증 서비스가 있어야 합니다.
- SnapCenter 및 AD FS 서버 타임 스탬프는 시간대와 상관없이 동일해야 합니다.
- SnapCenter 서버에 대해 승인된 CA 인증서를 조달하고 구성합니다.

  CA 인증서는 다음과 같은 이유로 필수입니다.

- 자체 서명된 인증서가 노드 수준에서 고유하므로 ADFS-F5 통신이 끊어지지 않도록 합니다.
- 독립 실행형 또는 고가용성 구성에서 업그레이드, 복구 또는 재해 복구(DR) 중에 자체 서명된 인증서가 다시 만들어지지 않으므로 MFA 재구성이 방지됩니다.
- IP-FQDN 해상도를 확인합니다.

  CA 인증서에 대한 자세한 내용은 를 "CA 인증서 CSR 파일을 생성합니다"참조하십시오.

단계

1. AD FS(Active Directory Federation Services) 호스트에 연결합니다.
2. FQDN > /FederationMetadata/2007-06/FederationMetadata.xml에서 AD FS 페더레이션 메타데이터 파일을 "https://<host 다운로드합니다."
3. 다운로드한 파일을 SnapCenter 서버에 복사하여 MFA 기능을 활성화합니다.
4. PowerShell을 통해 SnapCenter 관리자로 SnapCenter 서버에 로그인합니다.
5. PowerShell 세션을 사용하여 _New-SmMultactorAuthenticationMetadata-path_cmdlet을 사용하여 SnapCenter MFA 메타데이터 파일을 생성합니다.

   path 매개 변수는 SnapCenter 서버 호스트에 MFA 메타데이터 파일을 저장할 경로를 지정합니다.
6. 생성된 파일을 AD FS 호스트에 복사하여 SnapCenter를 클라이언트 엔터티로 구성합니다.
7. cmdlet을 사용하여 SnapCenter Server용 MFA를 사용하도록 `Set-SmMultiFactorAuthentication` 설정합니다.
8. (선택 사항) cmdlet을 사용하여 MFA 구성 상태 및 설정을 `Get-SmMultiFactorAuthentication` 확인합니다.
9. MMC(Microsoft Management Console)로 이동하여 다음 단계를 수행하십시오.
   a. 파일 * > * Snapin 추가/제거 * 를 클릭합니다.
   b. 스냅인 추가/제거 창에서 * 인증서 * 를 선택한 다음 * 추가 * 를 클릭합니다.
   c. 인증서 스냅인 창에서 * 컴퓨터 계정 * 옵션을 선택한 다음 * 마침 * 을 클릭합니다.
   d. 콘솔 루트 * > * 인증서 – 로컬 컴퓨터 * > * 개인 * > * 인증서 * 를 클릭합니다.
   e. SnapCenter에 바인딩된 CA 인증서를 마우스 오른쪽 단추로 클릭한 다음 * 모든 작업 * > * 개인 키 관리 * 를 선택합니다.
   f. 권한 마법사에서 다음 단계를 수행합니다.
      i. 추가 * 를 클릭합니다.
      ii. Locations * 를 클릭하고 관련 호스트(계층 구조의 맨 위)를 선택합니다.
      iii. Locations * (위치 *) 팝업 창에서 * OK * (확인 *)를 클릭합니다.
      iv. 개체 이름 필드에 'IIS_IUSRS'를 입력하고 * 이름 확인 * 을 클릭한 다음 * 확인 * 을 클릭합니다.

      검사가 성공적으로 완료되면 * OK * 를 클릭합니다.
10. AD FS 호스트에서 AD FS 관리 마법사를 열고 다음 단계를 수행합니다.
    a. '신뢰할 수 있는 당사자'를 마우스 오른쪽 버튼으로 클릭 * > * '신뢰할 수 있는 당사자 신뢰 추가' * > * 시작 * 을 클릭합니다.

b. 두 번째 옵션을 선택하고 SnapCenter MFA 메타데이터 파일을 찾은 후 * 다음 * 을 클릭합니다.

c. 표시 이름을 지정하고 * 다음 * 을 클릭합니다.

d. 필요에 따라 액세스 제어 정책을 선택하고 * 다음 * 을 클릭합니다.

e. 다음 탭에서 기본 설정으로 설정을 선택합니다.

f. 마침 * 을 클릭합니다.

SnapCenter는 이제 제공된 표시 이름을 가진 의존자로 반영됩니다.

11. 이름을 선택하고 다음 단계를 수행하십시오.

a. 청구 발급 정책 편집 * 을 클릭합니다.

b. 규칙 추가 * 를 클릭하고 * 다음 * 을 클릭합니다.

c. 청구 규칙의 이름을 지정합니다.

d. 속성 저장소로 * Active Directory * 를 선택합니다.

e. 속성을 * User-Principal-Name * 으로 선택하고 발신 클레임 유형을 * Name-ID * 로 선택합니다.

f. 마침 * 을 클릭합니다.

12. ADFS 서버에서 다음 PowerShell 명령을 실행합니다.

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-SigningCertificateRevocationCheck None

Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-EncryptionCertificateRevocationCheck None
```

13. 메타데이터를 성공적으로 가져왔는지 확인하려면 다음 단계를 수행하십시오.

a. 신뢰할 수 있는 상대 신뢰를 마우스 오른쪽 단추로 클릭하고 * 속성 * 을 선택합니다.

b. 끝점, 식별자 및 서명 필드가 채워져 있는지 확인합니다.

14. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성 세션 쿠키를 지우고 다시 로그인합니다.

SnapCenter MFA 기능은 REST API를 사용하여 활성화할 수도 있습니다.

문제 해결 정보는 을 "여러 탭에서 동시 로그인 시도 시 MFA 오류가 표시됩니다"참조하십시오.

AD FS MFA 메타데이터를 업데이트합니다

AD FS 서버에 업그레이드, CA 인증서 갱신, DR 등과 같은 수정 사항이 있을 때마다 SnapCenter에서 AD FS MFA 메타데이터를 업데이트해야 합니다.

단계

1. FQDN > /FederationMetadata/2007-06/FederationMetadata.xml에서 AD FS 페더레이션 메타데이터 파일 다운로드 "https://<host "

2. 다운로드한 파일을 SnapCenter 서버에 복사하여 MFA 구성을 업데이트합니다.

3. 다음 cmdlet을 실행하여 SnapCenter에서 AD FS 메타데이터를 업데이트합니다.

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성 세션 쿠키를 지우고 다시 로그인합니다.

SnapCenter MFA 메타데이터를 업데이트합니다

복구, CA 인증서 갱신, DR 등과 같은 ADFS 서버에 수정 사항이 있을 때마다 AD FS에서 SnapCenter MFA 메타데이터를 업데이트해야 합니다.

단계

1. AD FS 호스트에서 AD FS 관리 마법사를 열고 다음 단계를 수행합니다.
   a. 사용 당사자 신뢰 * 를 클릭합니다.
   b. SnapCenter에 대해 만든 기반 당사자 신뢰를 마우스 오른쪽 단추로 클릭하고 * 삭제 * 를 클릭합니다.

      신뢰할 수 있는 사용자의 사용자 정의 이름이 표시됩니다.

   c. MFA(Multi-factor Authentication)를 활성화합니다.

      을 "다중 요소 인증을 활성화합니다"참조하십시오.

2. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성 세션 쿠키를 지우고 다시 로그인합니다.

MFA(Multi-Factor Authentication) 비활성화

단계

1. MFA를 사용하지 않도록 설정하고 cmdlet을 사용하여 MFA를 사용할 때 생성된 구성 파일을 정리합니다. `Set-SmMultiFactorAuthentication`
2. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성 세션 쿠키를 지우고 다시 로그인합니다.

REST API, PowerShell 및 SCCLI를 사용하여 MFA(Multi-Factor Authentication)를 관리합니다

MFA 로그인은 브라우저, REST API, PowerShell 및 SCCLI에서 지원됩니다. MFA는 AD FS ID 관리자를 통해 지원됩니다. GUI, REST API, PowerShell 및 SCCLI에서 MFA를 사용하도록 설정하고 MFA를 사용하지 않도록 설정하고 MFA를 구성할 수 있습니다.

AD FS를 OAuth/OIDC로 설정합니다

- Windows GUI 마법사를 사용하여 AD FS 구성 *
  1. 서버 관리자 대시보드 * > * 도구 * > * ADFS 관리 * 로 이동합니다.
  2. ADFS * > * 응용 프로그램 그룹 * 으로 이동합니다.
     a. 응용 프로그램 그룹 * 을 마우스 오른쪽 단추로 클릭합니다.
     b. 응용 프로그램 그룹 추가 * 를 선택하고 * 응용 프로그램 이름 * 을 입력합니다.
     c. 서버 응용 프로그램 * 을 선택합니다.
     d. 다음 * 을 클릭합니다.
  3. 복사 * 클라이언트 식별자 *.

     클라이언트 ID입니다. … 리디렉션 URL에 콜백 URL(SnapCenter 서버 URL)을 추가합니다. … 다음 * 을 클릭합니다.

4. 공유 암호 생성 * 을 선택합니다.

   암호 값을 복사합니다. 클라이언트의 비밀입니다. … 다음 * 을 클릭합니다.

5. 요약 * 페이지에서 * 다음 * 을 클릭합니다.

   a. 완료 * 페이지에서 * 닫기 * 를 클릭합니다.

6. 새로 추가된 * 응용 프로그램 그룹 * 을 마우스 오른쪽 단추로 클릭하고 * 속성 * 을 선택합니다.
7. 앱 속성에서 * 응용 프로그램 추가 * 를 선택합니다.
8. 응용 프로그램 추가 * 를 클릭합니다.

   웹 API를 선택하고 * 다음 * 을 클릭합니다.

9. 웹 API 구성 페이지에서 이전 단계에서 만든 SnapCenter 서버 URL 및 클라이언트 식별자를 식별자 섹션에 입력합니다.

   a. 추가 * 를 클릭합니다.

   b. 다음 * 을 클릭합니다.

10. 액세스 제어 정책 선택 * 페이지에서 요구 사항에 따라 제어 정책(예: 모든 사용자 허용 및 MFA 필요)을 선택하고 * 다음 * 을 클릭합니다.
11. 응용 프로그램 권한 구성 * 페이지에서 기본적으로 OpenID가 범위로 선택되어 있으면 * 다음 * 을 클릭합니다.
12. 요약 * 페이지에서 * 다음 * 을 클릭합니다.

    완료 * 페이지에서 * 닫기 * 를 클릭합니다.

13. 샘플 응용 프로그램 속성 * 페이지에서 * 확인 * 을 클릭합니다.
14. 인증 서버(AD FS)에서 발급하고 리소스에서 사용하도록 의도된 JWT 토큰입니다.

    이 토큰의 'AUD' 또는 청중의 주장은 리소스 또는 웹 API의 식별자와 일치해야 합니다.

15. 선택한 WebAPI를 편집하고 콜백 URL(SnapCenter 서버 URL)과 클라이언트 식별자가 올바르게 추가되었는지 확인합니다.

    OpenID Connect를 구성하여 사용자 이름을 클레임으로 제공합니다.

16. 서버 관리자 오른쪽 상단의 * 도구 * 메뉴 아래에 있는 * AD FS 관리 * 도구를 엽니다.

    a. 왼쪽 사이드바에서 * Application Groups * 폴더를 선택합니다.

    b. 웹 API를 선택하고 * edit * 를 클릭합니다.

    c. 발행 변환 규칙 탭으로 이동합니다

17. 규칙 추가 * 를 클릭합니다.

    a. 클레임 규칙 템플릿 드롭다운에서 * 청구로 LDAP 속성 보내기 * 를 선택합니다.

    b. 다음 * 을 클릭합니다.

18. 청구 규칙 * 이름을 입력합니다.

    a. 특성 저장소 드롭다운에서 * Active Directory * 를 선택합니다.

b. LDAP 속성 * 드롭다운에서 * 사용자 - 기본 - 이름 * 을 선택하고 O * uting Claim Type * 드롭다운에서 * UPN * 을 선택합니다.

c. 마침 * 을 클릭합니다.

PowerShell 명령을 사용하여 애플리케이션 그룹을 생성합니다

PowerShell 명령을 사용하여 애플리케이션 그룹인 웹 API를 생성하고 범위와 청구서를 추가할 수 있습니다. 이러한 명령은 자동화된 스크립트 형식으로 사용할 수 있습니다. 자세한 내용은 <link to KB article> 를 참조하십시오.

1. 다음 comamnd를 사용하여 AD FS에서 새 애플리케이션 그룹을 생성합니다.

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier
-ApplicationGroupIdentifier $ClientRoleIdentifier
```

`ClientRoleIdentifier` 응용 프로그램 그룹의 이름입니다

`redirectURL` 인증 후 리디렉션에 대한 올바른 URL입니다

2. AD FS 서버 응용 프로그램을 생성하고 클라이언트 암호를 생성합니다.

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
-ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL
-Identifier $identifier -GenerateClientSecret
```

3. ADFS 웹 API 응용 프로그램을 만들고 사용할 정책 이름을 구성합니다.

```
$identifier = (New-Guid).Guid

Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
-Name "App Web API"

-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

4. 클라이언트 ID와 클라이언트 암호는 한 번만 표시되므로 다음 명령의 출력에서 가져옵니다.

```
"client_id = $identifier"

"client_secret: "$($ADFSApp.ClientSecret)
```

5. AD FS 응용 프로그램에 allat클레임 및 OpenID 권한을 부여합니다.

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
-ServerRoleIdentifier $identifier -ScopeNames @('openid')

$transformrule = @"

@RuleTemplate = "LdapClaims"

@RuleName = "AD User properties and Groups"

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
```

```
Issuer ==

"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. 변환 규칙 파일을 작성합니다.

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii $relativePath = Get-Item .\issueancetransformrules.tmp
```

7. 웹 API 응용 프로그램의 이름을 지정하고 외부 파일을 사용하여 발급 변환 규칙을 정의합니다.

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

액세스 토큰 만료 시간을 업데이트합니다

PowerShell 명령을 사용하여 액세스 토큰 만료 시간을 업데이트할 수 있습니다.

- 이 작업에 대한 정보 *
- 액세스 토큰은 사용자, 클라이언트 및 리소스의 특정 조합에 대해서만 사용할 수 있습니다. 액세스 토큰은 해지할 수 없으며 만료까지 유효합니다.
- 기본적으로 액세스 토큰의 만료 시간은 60분입니다. 이 최소 만료 시간은 충분하고 크기가 조정됩니다. 지속적으로 발생하는 비즈니스 크리티컬 작업을 방지할 수 있는 충분한 가치를 제공해야 합니다.
- 단계 *

애플리케이션 그룹 WebAPI에 대한 액세스 토큰 만료 시간을 업데이트하려면 AD FS 서버에서 다음 명령을 사용하십시오.

+ `Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"`

AD FS에서 베어러 토큰을 가져옵니다

REST 클라이언트(예: Postman)에서 아래에 언급된 매개 변수를 입력해야 하며 사용자 자격 증명을 입력하라는 메시지가 표시됩니다. 또한 2단계 인증(보유 항목 및 현재 항목)을 입력하여 베어러 토큰을 얻어야 합니다.

+ 베어러 토큰의 유효 기간은 애플리케이션별로 AD FS 서버에서 구성할 수 있으며 기본 유효 기간은 60분입니다.

필드에 입력합니다	값
허가 유형	인증 코드

콜백 URL	콜백 URL이 없는 경우 응용 프로그램의 기본 URL을 입력합니다.
인증 URL	[ADFS-DOMAIN-NAME]/ADFS/OAuth2/authorize
액세스 토큰 URL	[ADFS-DOMAIN-NAME]/ADFS/OAuth2/TOKEN
클라이언트 ID입니다	AD FS 클라이언트 ID를 입력합니다
클라이언트 암호	AD FS 클라이언트 암호를 입력합니다
범위	OpenID를 선택합니다
클라이언트 인증	기본 AUTH 헤더로 보냅니다
리소스	고급 옵션* 탭에서 JWT 토큰에 "AUD" 값으로 제공되는 콜백 URL과 동일한 값을 가진 자원 필드를 추가합니다.

SnapCenter 서버에서 **PowerShell, SCCLI** 및 **REST API**를 사용하여 **MFA**를 구성합니다

SnapCenter 서버에서 PowerShell, SCCLI 및 REST API를 사용하여 MFA를 구성할 수 있습니다.

SnapCenter MFA CLI 인증

PowerShell 및 SCCLI에서 베어러 토큰을 사용하여 사용자를 인증하는 데 "AccessToken"이라는 필드가 하나 더 있는 기존 cmdlet(Open-SmConnection)이 확장됩니다.

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port
<String>] [-RoleName <String>] [ -AccessToken <string>]
```

위의 cmdlet을 실행한 후 해당 사용자가 추가 SnapCenter cmdlet을 실행할 수 있도록 세션이 생성됩니다.

SnapCenter MFA REST API 인증

SnapCenter로부터 성공적인 응답을 얻으려면 _Authorization=Bearer <access token>_in REST API 클라이언트(예: Postman 또는 swagger)의 형식으로 베어러 토큰을 사용하고 헤더에 사용자 RoleName을 언급하십시오.

MFA REST API 워크플로우

MFA가 AD FS로 구성된 경우 액세스(베어러) 토큰을 사용하여 인증하여 REST API를 통해 SnapCenter 애플리케이션에 액세스해야 합니다.

- 이 작업에 대한 정보 *
- Postman, Swagger UI 또는 FireCamp와 같은 REST 클라이언트를 사용할 수 있습니다.
- 액세스 토큰을 가져와 후속 요청(SnapCenter REST API)을 인증하여 작업을 수행합니다.

- 단계 *
- AD FS MFA * 를 통해 인증합니다

1. 액세스 토큰을 얻기 위해 AD FS 끝점을 호출하도록 REST 클라이언트를 구성합니다.

   버튼을 눌러 응용 프로그램의 액세스 토큰을 가져오는 경우 AD FS SSO 페이지로 리디렉션됩니다. 이 페이지에서 AD 자격 증명을 제공하고 MFA로 인증해야 합니다. 1. AD FS SSO 페이지의 사용자 이름 텍스트 상자에 사용자 이름 또는 이메일을 입력합니다.

+사용자 이름은 user@domain 또는 domain\user로 지정해야 합니다.

1. 암호 텍스트 상자에 암호를 입력합니다.
2. 로그인 * 을 클릭합니다.
3. 로그인 옵션 * 섹션에서 인증 옵션을 선택하고 인증(구성에 따라 다름)을 수행합니다.
   - 푸시: 휴대폰에 전송되는 푸시 알림을 승인합니다.
   - QR 코드: AUTH Point 모바일 앱을 사용하여 QR 코드를 스캔한 다음 앱에 표시된 검증 코드를 입력합니다
   - 일회용 암호: 토큰의 일회용 암호를 입력합니다.
4. 인증에 성공하면 액세스, ID 및 토큰 새로 고침이 포함된 팝업이 열립니다.

   액세스 토큰을 복사하고 SnapCenter REST API에서 사용하여 작업을 수행합니다.

5. REST API에서는 헤더 섹션에서 액세스 토큰 및 역할 이름을 전달해야 합니다.
6. SnapCenter는 AD FS에서 이 액세스 토큰을 검증합니다.

   유효한 토큰인 경우 SnapCenter는 해당 토큰을 디코딩하고 사용자 이름을 가져옵니다.

7. SnapCenter는 사용자 이름과 역할 이름을 사용하여 API 실행을 위해 사용자를 인증합니다.

   인증에 성공하면 SnapCenter가 결과를 반환하고 그렇지 않으면 오류 메시지가 표시됩니다.

REST API, CLI 및 **GUI**에 대해 **SnapCenter MFA** 기능을 사용하거나 사용하지 않도록 설정합니다

- GUI *
- 단계 *

1. SnapCenter 서버에 SnapCenter 관리자로 로그인합니다.
2. 설정 * > * 글로벌 설정 * > * 멀티팩터인증(MFA) 설정 * 을 클릭합니다
3. 인터페이스(GUI/RST API/CLI)를 선택하여 MFA 로그인을 활성화하거나 비활성화합니다.

- PowerShell 인터페이스 *
- 단계 *

1. GUI, REST API, PowerShell 및 SCCLI에 대해 MFA를 사용하도록 PowerShell 또는 CLI 명령을 실행합니다.

```
Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled
-IsCliMFAEnabled -Path
```

path 매개 변수는 AD FS MFA 메타데이터 XML 파일의 위치를 지정합니다.

지정된 AD FS 메타데이터 파일 경로로 구성된 SnapCenter GUI, REST API, PowerShell 및 SCCLI에 대한 MFA를 활성화합니다.

1. cmdlet을 사용하여 MFA 구성 상태 및 설정을 `Get-SmMultiFactorAuthentication` 확인합니다.

SCCLI 인터페이스 *

- 단계 *
  1. `# sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path "C:\ADFS_metadata\abc.xml"`
  2. `# sccli Get-SmMultiFactorAuthentication`
- REST API *
  1. GUI, REST API, PowerShell 및 SCCLI에 대해 MFA를 사용하도록 다음 POST API를 실행합니다.

매개 변수	값
요청된 URL입니다	/api/4.9/settings/multipactorauthentication을 참조하십시오
HTTP 메소드	게시
요청 본문	{"IsGuiMFAEnabled":false, "IsRestApiMFAEnabled":true, "IsCliMFAEnabled":false, "ADFSConfigFilePath":"C:\\ADFS_METADATA\\abc.xml"}
응답 본문	{"MFAConfiguration":{"IsGuiMFAEnabled":FALSE, "ADFSConfigFilePath":"C:\\ADFS_METADATA\\abc.xml", "SCConfigFilePath": null, "IsRestApiMFAEnabled": true, "IsCliMFAEnabled": false, "ADFSHostName":"win-adfs-sc49.winscedom2.com"}

  2. 다음 API를 사용하여 MFA 구성 상태 및 설정을 확인합니다.

매개 변수	값
요청된 URL입니다	/api/4.9/settings/multipactorauthentication을 참조하십시오
HTTP 메소드	가져오기

응답 본문	{"MFAConfiguration":{"IsGuiMFAEnabled":FALSE, "ADFSConfigFilePath":"C:\\ADFS_METADATA\\abc.xml", "SCConfigFilePath": null, "IsRestApiMFAEnabled": true, "IsCliMFAEnabled": false, "ADFSHostName":"win-adfs-sc49.winscedom2.com"}

SnapCenter 서버를 설치합니다

SnapCenter 서버 설치 관리자 실행 파일을 실행하여 SnapCenter 서버를 설치할 수 있습니다.

필요에 따라 PowerShell cmdlet을 사용하여 몇 가지 설치 및 구성 절차를 수행할 수 있습니다.

명령줄에서 SnapCenter 서버를 자동 설치하는 것은 지원되지 않습니다.

시작하기 전에

- SnapCenter 서버 호스트는 시스템 재시작을 보류하지 않고 Windows 업데이트를 최신 상태로 유지해야 합니다.
- SnapCenter 서버를 설치하려는 호스트에 MySQL Server가 설치되어 있지 않은지 확인해야 합니다.
- Windows 설치 관리자 디버깅을 사용하도록 설정해야 합니다.

  사용 방법에 대한 자세한 내용은 Microsoft 웹 사이트를 "Windows 설치 관리자 로깅"참조하십시오.

  Microsoft Exchange Server, Active Directory 또는 도메인 이름 서버가 있는 호스트에 SnapCenter 서버를 설치하면 안 됩니다.

- 단계 *

1. 에서 SnapCenter 서버 설치 패키지를 "NetApp Support 사이트"다운로드합니다.
2. 다운로드한 .exe 파일을 두 번 클릭하여 SnapCenter 서버 설치를 시작합니다.

   설치를 시작한 후 모든 사전 점검을 수행하고 최소 요구사항을 충족하지 못할 경우 적절한 오류 또는 경고 메시지가 표시됩니다.

   경고 메시지를 무시하고 설치를 진행할 수 있지만 오류를 수정해야 합니다.

3. SnapCenter 서버 설치에 필요한 미리 채워진 값을 검토하고 필요한 경우 수정합니다.

   MySQL Server 리포지토리 데이터베이스의 암호를 지정할 필요가 없습니다. SnapCenter 서버 설치 중에 암호는 자동으로 생성됩니다.

   경로에 특수 문자 "%`" is not supported in the custom path for the repository database. If you include "`"%", 설치가 실패합니다.

4. 지금 설치 * 를 클릭합니다.

   잘못된 값을 지정한 경우 해당 오류 메시지가 표시됩니다. 값을 다시 입력한 다음 설치를 시작해야 합니다.

Cancel * 버튼을 클릭하면 실행 중인 단계가 완료된 후 롤백 작업을 시작합니다. SnapCenter 서버가 호스트에서 완전히 제거됩니다.

그러나 "SnapCenter 서버 사이트 재시작" 또는 "SnapCenter 서버 시작 대기 중" 작업이 수행 중일 때 * 취소 * 를 클릭하면 작업을 취소하지 않고 설치가 진행됩니다.

로그 파일은 항상 관리자 사용자의 %temp% 폴더에 (가장 오래된 파일 먼저) 나열됩니다. 로그 위치를 리디렉션하려면 다음을 실행하여 명령 프롬프트에서 SnapCenter 서버 설치를 시작합니다 `.C:\installer_location\installer_name.exe /log"C:\"`

RBAC 승인을 사용하여 SnapCenter에 로그인합니다

SnapCenter는 역할 기반 액세스 제어(RBAC)를 지원합니다. SnapCenter 관리자는 SnapCenter RBAC를 통해 역할 및 리소스를 작업 그룹 또는 Active Directory의 사용자 또는 Active Directory의 그룹에 할당합니다. 이제 RBAC 사용자는 할당된 역할을 사용하여 SnapCenter에 로그인할 수 있습니다.

시작하기 전에

- Windows Server Manager에서 WAS(Windows Process Activation Service)를 활성화해야 합니다.
- Internet Explorer를 브라우저로 사용하여 SnapCenter 서버에 로그인하려면 Internet Explorer의 보호 모드가 비활성화되어 있어야 합니다.
- 이 작업에 대한 정보 *

설치 중에 SnapCenter 서버 설치 마법사가 바로 가기를 만들어 SnapCenter가 설치된 호스트의 바탕 화면과 시작 메뉴에 배치합니다. 또한 설치 완료 시 설치 마법사는 설치 중에 제공한 정보를 기반으로 SnapCenter URL을 표시하며, 원격 시스템에서 로그인하려는 경우 이 URL을 복사할 수 있습니다.

웹 브라우저에 여러 개의 탭이 열려 있는 경우 SnapCenter 브라우저 탭을 닫아도 SnapCenter에서 로그아웃되지 않습니다. SnapCenter와의 연결을 종료하려면 * 로그아웃 * 단추를 클릭하거나 전체 웹 브라우저를 닫아 SnapCenter에서 로그아웃해야 합니다.

모범 사례**:** 보안상의 이유로 브라우저에서 SnapCenter 암호를 저장하지 않는 것이 좋습니다.

기본 GUI URL은 SnapCenter 서버가 설치된 서버의 기본 포트 8146에 대한 보안 연결입니다(*https://server:8146*).) SnapCenter 설치 중에 다른 서버 포트를 제공한 경우 해당 포트가 대신 사용됩니다.

HA(고가용성) 구축을 위해서는 가상 클러스터 IP_\https://Virtual_Cluster_IP_or_FQDN:8146_.를 사용하여 SnapCenter에 액세스해야 합니다 Internet Explorer(IE)에서 _\https://Virtual_Cluster_IP_or_FQDN:8146_로 이동할 때 SnapCenter UI가 표시되지 않으면 각 플러그인 호스트의 IE에 가상 클러스터 IP 주소 또는 FQDN을 신뢰할 수 있는 사이트로 추가하거나 각 플러그인 호스트에서 IE 고급 보안을 해제해야 합니다. 자세한 내용은 을 "외부 네트워크에서 클러스터 IP 주소에 액세스할 수 없습니다"참조하십시오.

SnapCenter GUI 사용 외에도 PowerShell cmdlet을 사용하여 스크립트를 생성하여 구성, 백업 및 복원 작업을 수행할 수 있습니다. 일부 cmdlet은 SnapCenter 릴리즈마다 변경될 수 있습니다. 에 "SnapCenter 소프트웨어 cmdlet 참조 가이드" 자세한 내용이 있습니다.

SnapCenter에 처음 로그인하는 경우 설치 프로세스 중에 제공한 자격 증명을 사용하여 로그인해야 합니다.

- 단계 *

1. 로컬 호스트 데스크톱에 있는 바로 가기나 설치 마지막에 제공된 URL 또는 SnapCenter 관리자가 제공한 URL에서 SnapCenter를 실행합니다.
2. 사용자 자격 증명을 입력합니다.

다음을 지정하려면...	다음 형식 중 하나를 사용합니다...
도메인 관리자	• NetBIOS\사용자 이름입니다 • 사용자 이름@UPN 접미사 예: username@netapp.com • 도메인 FQDN\사용자 이름입니다
로컬 관리자	사용자 이름

3. 둘 이상의 역할이 할당된 경우 역할 상자에서 이 로그인 세션에 사용할 역할을 선택합니다.

   로그인한 후 현재 사용자 및 관련 역할이 SnapCenter의 오른쪽 상단에 표시됩니다.

결과 *

대시보드 페이지가 표시됩니다.

사이트에 연결할 수 없다는 오류로 인해 로깅이 실패하는 경우 SSL 인증서를 SnapCenter에 매핑해야 합니다. "자세한 정보"

- 완료 후 *

SnapCenter 서버에 RBAC 사용자로 처음으로 로그인한 후 리소스 목록을 새로 고칩니다.

SnapCenter에서 지원할 신뢰할 수 없는 Active Directory 도메인이 있는 경우 신뢰할 수 없는 도메인의 사용자에 대한 역할을 구성하기 전에 해당 도메인을 SnapCenter에 등록해야 합니다. "자세한 정보"

멀티팩터 인증(MFA)을 사용하여 SnapCenter에 로그인

SnapCenter 서버는 Active Directory의 일부인 도메인 계정에 대해 MFA를 지원합니다.

시작하기 전에

- MFA를 활성화해야 합니다.

  MFA를 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오 "다중 요소 인증을 활성화합니다"

- 이 작업에 대한 정보 *

- FQDN만 지원됩니다
- 작업 그룹 및 도메인 간 사용자는 MFA를 사용하여 로그인할 수 없습니다
- 단계 *
  1. 로컬 호스트 데스크톱에 있는 바로 가기나 설치 마지막에 제공된 URL 또는 SnapCenter 관리자가 제공한 URL에서 SnapCenter를 실행합니다.
  2. AD FS 로그인 페이지에서 사용자 이름 및 암호 를 입력합니다.

     AD FS 페이지에 잘못된 사용자 이름 또는 암호 오류 메시지가 표시되면 다음을 확인해야 합니다.

     - 사용자 이름 또는 암호가 유효한지 여부를 나타냅니다

       사용자 계정이 AD(Active Directory)에 있어야 합니다.

     - AD에 설정된 최대 허용 시도 횟수를 초과했는지 여부
     - AD 및 AD FS의 가동 및 실행 여부를 나타냅니다

SnapCenter 기본 GUI 세션 시간 초과를 수정합니다

SnapCenter GUI 세션 제한 시간을 기본 제한 시간 20분 이하로 수정할 수 있습니다.

SnapCenter는 기본 15분 동안 비활성 상태가 지속되면 GUI 세션에서 5분 후에 로그아웃된다는 경고 메시지를 보안 기능으로 표시합니다. 기본적으로 SnapCenter는 20분 동안 비활성 상태가 지속되면 GUI 세션에서 로그아웃하고 다시 로그인해야 합니다.

- 단계 *
  1. 왼쪽 탐색 창에서 * 설정 * > * 글로벌 설정 * 을 클릭합니다.
  2. 전역 설정 페이지에서 * 구성 설정 * 을 클릭합니다.
  3. Session Timeout(세션 시간 초과) 필드에 새 세션 시간 제한을 분 단위로 입력한 다음 * Save * (저장 *)를 클릭합니다.

SSL 3.0을 비활성화하여 SnapCenter 웹 서버를 보호합니다

보안을 위해 SnapCenter 웹 서버에서 SSL(Secure Socket Layer) 3.0 프로토콜을 사용하는 경우 Microsoft IIS에서 SSL(Secure Socket Layer) 3.0 프로토콜을 비활성화해야 합니다.

SSL 3.0 프로토콜에 결함이 있어 공격자가 연결 장애를 일으키거나 중간자 공격을 수행하여 웹 사이트와 방문자 사이의 암호화 트래픽을 관찰할 수 있습니다.

- 단계 *
  1. SnapCenter 웹 서버 호스트에서 레지스트리 편집기를 시작하려면 * 시작 * > * 실행 * 을 클릭하고 regedit를 입력합니다.
  2. 레지스트리 편집기에서 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols\SSL 3.0\로 이동합니다.
     - 서버 키가 이미 있는 경우:
       i. 사용 DWORD를 선택한 다음 * 편집 * > * 수정 * 을 클릭합니다.

ii. 값을 0으로 변경한 다음 * 확인 * 을 클릭합니다.

- 서버 키가 없는 경우:
  i. 편집 * > * 새로 만들기 * > * 키 * 를 클릭한 다음 키 서버의 이름을 지정합니다.
  ii. 새 서버 키를 선택한 상태에서 * 편집 * > * 새로 만들기 * > * DWORD * 를 클릭합니다.
  iii. 새 DWORD Enabled의 이름을 지정한 다음 0을 값으로 입력합니다.

3. 레지스트리 편집기를 닫습니다.

CA 인증서를 구성합니다

CA 인증서 CSR 파일을 생성합니다

CSR(인증서 서명 요청)을 생성하고 생성된 CSR을 사용하여 CA(인증 기관)에서 가져올 수 있는 인증서를 가져올 수 있습니다. 인증서에 연결된 개인 키가 있습니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.

CA 인증서 RSA 키 길이는 최소 3072비트여야 합니다.

CSR 생성에 대한 자세한 내용은 을 "CA 인증서 CSR 파일을 생성하는 방법"참조하십시오.

도메인(* .domain.company.com) 또는 시스템(machine1.domain.company.com CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter를 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN) 및 해당 호스트 이름을 CA 인증서에 언급해야 합니다. 인증서를 조달하기 전에 SAN(Subject Alternative Name) 필드를 채워 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(* .domain.company.com)의 경우 인증서에 도메인의 모든 호스트 이름이 암시적으로 포함됩니다.

CA 인증서를 가져옵니다

MMC(Microsoft Management Console)를 사용하여 CA 인증서를 SnapCenter 서버 및 Windows 호스트 플러그인으로 가져와야 합니다.

단계

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 추가/제거 * 를 클릭합니다.
2. 스냅인 추가/제거 창에서 * 인증서 * 를 선택한 다음 * 추가 * 를 클릭합니다.
3. 인증서 스냅인 창에서 * 컴퓨터 계정 * 옵션을 선택한 다음 * 마침 * 을 클릭합니다.
4. 콘솔 루트 * > * 인증서 – 로컬 컴퓨터 * > * 신뢰할 수 있는 루트 인증 기관 * > * 인증서 * 를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 단추로 클릭한 다음 * 모든 작업 * > * 가져오기 * 를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료합니다.

이 마법사 창에서...	다음을 수행합니다.
개인 키를 가져옵니다	예 * 옵션을 선택하고 개인 키를 가져온 다음 * 다음 * 을 클릭합니다.
파일 형식 가져오기	변경하지 않고 * 다음 * 을 클릭합니다.
보안	내보낸 인증서에 사용할 새 암호를 지정하고 * 다음 * 을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

인증서 가져오기는 개인 키와 함께 번들로 제공됩니다(지원되는 형식은 *.pfx, *.p12 및 *.p7b 입니다).

7. "개인" 폴더에 대해 5단계를 반복합니다.

CA 인증서 지문을 받습니다

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

단계

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

      예를 들어, 썸프린트가 "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 0d 42 77 A3 2a 7b"인 경우 공백을 제거한 후 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.
   a. 다음 명령을 실행하여 설치된 인증서의 엄지손가락 지문을 나열하고 최근 설치된 인증서를 주체 이름으로 식별합니다.

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

   b. 엄지손가락 지문을 복사합니다.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서를 구성합니다

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스를 사용하여 CA

인증서를 구성해야 합니다.

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

단계

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

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   예를 들면 다음과 같습니다.

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스와 바인딩합니다.
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   예를 들면 다음과 같습니다.

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

SnapCenter 사이트를 사용하여 **CA** 인증서를 구성합니다

Windows 호스트에서 SnapCenter 사이트를 사용하여 CA 인증서를 구성해야 합니다.

- 단계 *
  1. SnapCenter가 설치된 Windows 서버에서 IIS 관리자를 엽니다.
  2. 왼쪽 탐색 창에서 * 연결 * 을 클릭합니다.
  3. 서버 이름과 * 사이트 * 를 확장합니다.
  4. SSL 인증서를 설치할 SnapCenter 웹 사이트를 선택합니다.
  5. 작업 * > * 사이트 편집 * 으로 이동하여 * 바인딩 * 을 클릭합니다.
  6. 바인딩 페이지에서 https*에 대한 * 바인딩을 선택합니다.
  7. 편집 * 을 클릭합니다.
  8. SSL 인증서 드롭다운 목록에서 최근에 가져온 SSL 인증서를 선택합니다.

9. 확인 * 을 클릭합니다.

최근에 배포된 CA 인증서가 드롭다운 메뉴에 나열되지 않으면 CA 인증서가 개인 키와 연결되어 있는지 확인합니다.

다음 경로를 사용하여 인증서를 추가해야 합니다. * 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 신뢰할 수 있는 루트 인증 기관 > 인증서 *.

SnapCenter에 대해 CA 인증서를 활성화합니다

CA 인증서를 구성하고 SnapCenter 서버에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

시작하기 전에

- Set-SmCertificateSettings cmdlet을 사용하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- Get-SmCertificateSettings cmdlet을 사용하여 SnapCenter 서버의 인증서 상태를 표시할 수 있습니다.

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

- 단계 *
  1. 설정 페이지에서 * 설정 * > * 글로벌 설정 * > * CA 인증서 설정 * 으로 이동합니다.
  2. 인증서 유효성 검사 사용 * 을 선택합니다.
  3. 적용 * 을 클릭합니다.
- 완료 후 *

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

- * * 플러그인 호스트에 활성화되거나 할당된 CA 인증서가 없음을 나타냅니다.
- * * CA 인증서의 유효성 검사가 성공적으로 완료되었음을 나타냅니다.
- * * 는 CA 인증서의 유효성을 검사할 수 없음을 나타냅니다.
- * * 는 연결 정보를 검색할 수 없음을 나타냅니다.

상태가 노란색 또는 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

양방향 SSL 통신을 구성하고 사용하도록 설정합니다

양방향 SSL 통신을 구성합니다

SnapCenter 서버와 플러그인 간의 상호 통신을 보호하려면 양방향 SSL 통신을 구성해야 합니다.

- 시작하기 전에 *

- 지원되는 최소 키 길이가 3072인 CA 인증서 CSR 파일을 생성해야 합니다.
- CA 인증서는 서버 인증 및 클라이언트 인증을 지원해야 합니다.
- 개인 키와 지문 세부 정보가 포함된 CA 인증서가 있어야 합니다.
- 단방향 SSL 구성을 활성화해야 합니다.

  자세한 내용은 을 참조하십시오 "CA 인증서 구성 섹션을 참조하십시오."

- 모든 플러그인 호스트와 SnapCenter 서버에서 양방향 SSL 통신을 활성화해야 합니다.

  일부 호스트 또는 서버가 양방향 SSL 통신에 사용되지 않는 환경은 지원되지 않습니다.

- 단계 *

1. 포트를 바인딩하려면 SnapCenter IIS 웹 서버 포트 8146(기본값)용 SnapCenter 서버 호스트에서 다음 단계를 수행하고 PowerShell 명령을 사용하여 SMCore 포트 8145(기본값)에 대해 다시 한 번 수행합니다.

   a. 다음 PowerShell 명령을 사용하여 기존 SnapCenter 자체 서명된 인증서 포트 바인딩을 제거합니다.

   ```
   > netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
   ```

   예를 들면, 다음과 같습니다.

   ```
   > netsh http delete sslcert ipport=0.0.0.0:8145

   > netsh http delete sslcert ipport=0.0.0.0:8146
   ```

   b. 새로 조달한 CA 인증서를 SnapCenter 서버 및 SMCore 포트와 바인딩합니다.

   ```
   > $cert = “<CA_certificate thumbprint>”

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>
   certhash=$cert appid="$guid" clientcertnegotiation=enable
   verifyclientcertrevocation=disable

   > netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
   ```

   예를 들면, 다음과 같습니다.

   ```
   > $cert = “abc123abc123abc123abc123”

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
   clientcertnegotiation=enable verifyclientcertrevocation=disable

   > $guid = [guid]::NewGuid().ToString("B")

   > netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
   clientcertnegotiation=enable verifyclientcertrevocation=disable
   ```

```
> netsh http show sslcert ipport=0.0.0.0:8146
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

2. CA 인증서에 대한 권한에 액세스하려면 다음 단계를 수행하여 새로 조달된 CA 인증서에 액세스하여 인증서 권한 목록에 SnapCenter의 기본 IIS 웹 서버 사용자 "* IIS AppPool\SnapCenter*"를 추가합니다.
   a. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * SnapIn 추가/제거 * 를 클릭합니다.
   b. 스냅인 추가/제거 창에서 * 인증서 * 를 선택한 다음 * 추가 * 를 클릭합니다.
   c. 인증서 스냅인 창에서 * 컴퓨터 계정 * 옵션을 선택한 다음 * 마침 * 을 클릭합니다.
   d. 콘솔 루트 * > * 인증서 – 로컬 컴퓨터 * > * 개인 * > * 인증서 * 를 클릭합니다.
   e. SnapCenter 인증서를 선택합니다.
   f. 사용자 추가\권한 마법사를 시작하려면 CA 인증서를 마우스 오른쪽 버튼으로 클릭하고 * 모든 작업 * > * 개인 키 관리 * 를 선택합니다.
   g. Add * 를 클릭하고 Select users and groups(사용자 및 그룹 선택) 마법사에서 위치를 local computer name(계층의 맨 위)으로 변경합니다.
   h. IIS AppPool\SnapCenter 사용자를 추가하고 모든 제어 권한을 제공합니다.
3. CA 인증서 IIS 권한*의 경우 다음 경로에서 SnapCenter 서버의 새 DWORD 레지스트리 키 항목을 추가합니다.

   Windows 레지스트리 편집기에서 아래 경로로 이동합니다.

   ```
   HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv
   ders\SCHANNEL
   ```

4. SChannel 레지스트리 구성의 컨텍스트에서 새 DWORD 레지스트리 키 항목을 만듭니다.

   ```
   SendTrustedIssuerList = 0
   ```

```
ClientAuthTrustMode = 2
```

양방향 **SSL** 통신을 위해 **SnapCenter Windows** 플러그인을 구성합니다

PowerShell 명령을 사용하여 양방향 SSL 통신을 위해 SnapCenter Windows 플러그인을 구성해야 합니다.

- 시작하기 전에 *

CA 인증서 지문을 사용할 수 있는지 확인합니다.

- 단계 *

1. 포트를 바인딩하려면 Windows 플러그인 호스트에서 SMCore 포트 8145(기본값)에 대해 다음 작업을 수행합니다.
   a. 다음 PowerShell 명령을 사용하여 기존 SnapCenter 자체 서명된 인증서 포트 바인딩을 제거합니다.

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
      ```

예를 들면, 다음과 같습니다.

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

b. 새로 조달한 CA 인증서를 SMCore 포트와 바인딩합니다.

```
> $cert = "<CA_certificate thumbprint>"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
appid="$guid" clientcertnegotiation=enable
verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:<SMCore Port>
```

예를 들면, 다음과 같습니다.

```
> $cert = "abc123abc123abc123abc123"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8145
```

양방향 **SSL** 통신을 활성화합니다

양방향 SSL 통신을 사용하여 PowerShell 명령을 사용하여 SnapCenter 서버와 플러그인 간의 상호 통신을 보호할 수 있습니다.

- 시작하기 전에 *

모든 플러그인 및 SMCore 에이전트에 대한 명령을 먼저 실행한 다음 서버에 대해 명령을 실행합니다.

- 단계 *

1. 양방향 SSL 통신을 활성화하려면 플러그인, 서버 및 양방향 SSL 통신이 필요한 각 에이전트에 대해 SnapCenter 서버에서 다음 명령을 실행합니다.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName <Plugin_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

1. 다음 명령을 사용하여 IIS SnapCenter 응용 프로그램 풀 재활용 작업을 수행합니다. `> Restart-WebAppPool -Name "SnapCenter"`

2. Windows 플러그인의 경우 다음 PowerShell 명령을 실행하여 SMCore 서비스를 다시 시작합니다.

```
> Restart-Service -Name SnapManagerCoreService
```

양방향 **SSL** 통신을 비활성화합니다

PowerShell 명령을 사용하여 양방향 SSL 통신을 사용하지 않도록 설정할 수 있습니다.

- 이 작업에 대한 정보 *
- 모든 플러그인 및 SMCore 에이전트에 대한 명령을 먼저 실행한 다음 서버에 대해 명령을 실행합니다.
- 양방향 SSL 통신을 비활성화하면 CA 인증서와 해당 구성이 제거되지 않습니다.
- SnapCenter 서버에 새 호스트를 추가하려면 모든 플러그인 호스트에 대해 양방향 SSL을 비활성화해야 합니다.
- NLB 및 F5는 지원되지 않습니다.
- 단계 *

1. 양방향 SSL 통신을 비활성화하려면 모든 플러그인 호스트 및 SnapCenter 호스트에 대해 SnapCenter 서버에서 다음 명령을 실행합니다.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName <Agent_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

1. 다음 명령을 사용하여 IIS SnapCenter 응용 프로그램 풀 재활용 작업을 수행합니다. `> Restart-WebAppPool -Name "SnapCenter"`
2. Windows 플러그인의 경우 다음 PowerShell 명령을 실행하여 SMCore 서비스를 다시 시작합니다.

```
> Restart-Service -Name SnapManagerCoreService
```

인증서 기반 인증을 구성합니다

SnapCenter 서버에서 **CA(**인증 기관**)** 인증서를 내보냅니다

MMC(Microsoft Management Console)를 사용하여 SnapCenter 서버에서 플러그인 호스트로 CA 인증서를 내보내야 합니다.

시작하기 전에

양방향 SSL을 구성해야 합니다.

- 단계 *

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 추가/제거 * 를 클릭합니다.
2. 스냅인 추가/제거 창에서 * 인증서 * 를 선택한 다음 * 추가 * 를 클릭합니다.

3. 인증서 스냅인 창에서 * 컴퓨터 계정 * 옵션을 선택한 다음 * 마침 * 을 클릭합니다.
4. 콘솔 루트 * > * 인증서 - 로컬 컴퓨터 * > * 개인 * > * 인증서 * 를 클릭합니다.
5. SnapCenter 서버에 사용되는 조달된 CA 인증서를 마우스 오른쪽 단추로 클릭한 다음 * 모든 작업 * > * 내보내기 * 를 선택하여 내보내기 마법사를 시작합니다.
6. 마법사에서 다음 작업을 수행합니다.

이 옵션의 경우...	다음을 수행합니다.
개인 키를 내보냅니다	아니오, 개인 키를 내보내지 않습니다 * 를 선택한 후 * 다음 * 을 클릭합니다.
파일 형식 내보내기	다음 * 을 클릭합니다.
파일 이름	찾아보기 * 를 클릭하고 인증서를 저장할 파일 경로를 지정한 후 * 다음 * 을 클릭합니다.
인증서 내보내기 마법사를 완료합니다	요약을 검토한 후 * Finish * 를 클릭하여 내보내기를 시작합니다.

SnapCenter HA 구성 및 VMware vSphere용 SnapCenter 플러그인에는 인증서 기반 인증이 지원되지 않습니다.

CA(인증 기관) 인증서를 Windows 플러그인 호스트로 가져옵니다

내보낸 SnapCenter 서버 CA 인증서를 사용하려면 Microsoft 관리 콘솔(MMC)을 사용하여 관련 인증서를 SnapCenter Windows 플러그인 호스트로 가져와야 합니다.

- 단계 *

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 추가/제거 * 를 클릭합니다.
2. 스냅인 추가/제거 창에서 * 인증서 * 를 선택한 다음 * 추가 * 를 클릭합니다.
3. 인증서 스냅인 창에서 * 컴퓨터 계정 * 옵션을 선택한 다음 * 마침 * 을 클릭합니다.
4. 콘솔 루트 * > * 인증서 - 로컬 컴퓨터 * > * 개인 * > * 인증서 * 를 클릭합니다.
5. "개인" 폴더를 마우스 오른쪽 단추로 클릭한 다음 * 모든 작업 * > * 가져오기 * 를 선택하여 가져오기 마법사를 시작합니다.
6. 마법사에서 다음 작업을 수행합니다.

이 옵션의 경우...	다음을 수행합니다.
매장 위치	다음 * 을 클릭합니다.
가져올 파일	cer 확장자로 끝나는 SnapCenter 서버 인증서를 선택합니다.

이 옵션의 경우...	다음을 수행합니다.
인증서 저장소	다음 * 을 클릭합니다.
인증서 내보내기 마법사를 완료합니다	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

CA 인증서를 UNIX 호스트 플러그인으로 가져오고 SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성합니다

CA 인증서를 UNIX 플러그인 호스트로 가져옵니다

CA 인증서를 UNIX 플러그인 호스트로 가져와야 합니다.

- 이 작업에 대한 정보 *
- SPL 키 저장소의 암호 및 사용 중인 CA 서명 키 쌍의 별칭을 관리할 수 있습니다.
- SPL 키 저장소 및 개인 키의 모든 관련 별칭 암호에 대한 암호는 동일해야 합니다.
- 단계 *
  1. SPL 속성 파일에서 SPL 키 저장소 기본 암호를 검색할 수 있습니다. 키에 해당하는 `SPL_KEYSTORE_PASS`값입니다.
  2. 키 저장소 암호 변경: `$ keytool -storepasswd -keystore keystore.jks`
  3. 키 저장소에 있는 개인 키 항목의 모든 별칭에 대한 암호를 키 저장소에 사용된 것과 동일한 암호로 변경합니다. `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
  4. 파일에서 SPL_keystore_pass 키에 대해 동일하게 `spl.properties` 업데이트합니다.
  5. 암호를 변경한 후 서비스를 다시 시작합니다.

SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성합니다

루트 또는 중간 인증서를 SPL 신뢰 저장소에 구성해야 합니다. 루트 CA 인증서와 중간 CA 인증서를 추가해야 합니다.

- 단계 *
  1. SPL 키 저장소가 있는 폴더로 이동합니다 `/var/opt/snapcenter/spl/etc`.
  2. 파일을 찾습니다 `keystore.jks`.
  3. 키 저장소에 추가된 인증서를 나열합니다. `$ keytool -list -v -keystore keystore.jks`
  4. 루트 또는 중간 인증서 추가: `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
  5. SPL 신뢰 저장소에 루트 또는 중간 인증서를 구성한 후 서비스를 다시 시작합니다.

CA 서명 키 쌍을 **SPL** 신뢰 저장소에 구성합니다

CA 서명된 키 쌍을 SPL 신뢰 저장소에 구성해야 합니다.

- 단계 *

1. SPL의 키 저장소가 있는 폴더로 `/var/opt/snapcenter/spl/etc`이동합니다.
2. 파일을 찾습니다 `keystore.jks`.
3. 키 저장소에 추가된 인증서를 나열합니다. `$ keytool -list -v -keystore keystore.jks`
4. 개인 키와 공개 키가 모두 있는 CA 인증서를 추가합니다. `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. 키 저장소에 추가된 인증서를 나열합니다. `$ keytool -list -v -keystore keystore.jks`
6. keystore에 keystore에 추가된 새 CA 인증서에 해당하는 별칭이 포함되어 있는지 확인합니다.
7. CA 인증서에 추가된 개인 키 암호를 키 저장소 암호로 변경합니다.

   기본 SPL 키 저장소 암호는 파일의 키 SPL_keystore_pass `spl.properties` 값입니다.

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
```

1. CA 인증서의 별칭 이름이 길고 공백이나 특수 문자("*",",")가 포함된 경우 별칭 이름을 간단한 이름으로 변경합니다. `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
2. 파일에 있는 키 저장소에서 별칭 이름을 `spl.properties` 구성합니다. 이 값을 SPL_CERTIFICATE_ALIAS 키에 대해 업데이트합니다.
3. CA 서명 키 쌍을 SPL 신뢰 저장소에 구성한 후 서비스를 다시 시작합니다.

인증서 기반 인증을 사용합니다

SnapCenter 서버 및 Windows 플러그인 호스트에 대한 인증서 기반 인증을 활성화하려면 다음 PowerShell cmdlet을 실행합니다. Linux 플러그인 호스트의 경우 양방향 SSL을 활성화하면 인증서 기반 인증이 활성화됩니다.

- 클라이언트 인증서 기반 인증을 사용하려면 다음을 따르십시오.

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- 클라이언트 인증서 기반 인증을 사용하지 않도록 설정하려면 다음을 따르십시오.

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

Active Directory, LDAP 및 LDAPS를 구성합니다

신뢰할 수 없는 **Active Directory** 도메인을 등록합니다

신뢰할 수 없는 여러 Active Directory 도메인의 호스트, 사용자 및 그룹을 관리하려면 Active Directory를 SnapCenter 서버에 등록해야 합니다.

시작하기 전에

- LDAP 및 LDAPS 프로토콜 *
- LDAP 또는 LDAPS 프로토콜을 사용하여 신뢰할 수 없는 Active Directory 도메인을 등록할 수 있습니다.
- 플러그인 호스트와 SnapCenter 서버 간에 양방향 통신을 설정해야 합니다.
- DNS 확인은 SnapCenter 서버에서 플러그인 호스트로, 또는 그 반대로 설정해야 합니다.

LDAP 프로토콜 *

- FQDN(정규화된 도메인 이름)은 SnapCenter 서버에서 확인할 수 있어야 합니다.

  FQDN을 사용하여 신뢰할 수 없는 도메인을 등록할 수 있습니다. SnapCenter 서버에서 FQDN을 확인할 수 없는 경우 도메인 컨트롤러 IP 주소로 등록할 수 있으며 SnapCenter 서버에서 확인할 수 있습니다.

LDAPS 프로토콜 *

- LDAPS가 Active Directory 통신 중에 종단 간 암호화를 제공하려면 CA 인증서가 필요합니다.

  "LDAPS에 대한 CA 클라이언트 인증서를 구성합니다"

- SnapCenter 서버에서 도메인 컨트롤러 호스트 이름(DCHostName)에 연결할 수 있어야 합니다.
- 이 작업에 대한 정보 *
- SnapCenter 사용자 인터페이스, PowerShell cmdlet 또는 REST API를 사용하여 신뢰할 수 없는 도메인을 등록할 수 있습니다.
- 단계 *
  1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
  2. 설정 페이지에서 * 글로벌 설정 * 을 클릭합니다.
  3. 글로벌 설정 페이지에서 * 도메인 설정 * 을 클릭합니다.
  4. + 새 도메인을 등록하려면 클릭합니다.
  5. 새 도메인 등록 페이지에서 * LDAP * 또는 * LDAPS * 를 선택합니다.
     a. LDAP * 를 선택한 경우 LDAP에 대해 신뢰할 수 없는 도메인을 등록하는 데 필요한 정보를 지정합니다.

이 필드의 내용...	수행할 작업...
도메인 이름	도메인의 NetBIOS 이름을 지정합니다.

이 필드의 내용...	수행할 작업...
도메인 FQDN	FQDN을 지정하고 * Resolve * 를 클릭합니다.
도메인 컨트롤러 IP 주소입니다	SnapCenter 서버에서 도메인 FQDN을 확인할 수 없는 경우 하나 이상의 도메인 컨트롤러 IP 주소를 지정합니다. 자세한 내용은 을 "GUI에서 신뢰할 수 없는 도메인에 대한 도메인 컨트롤러 IP를 추가합니다 "참조하십시오.

b. LDAPS * 를 선택한 경우 LDAPS에 대해 신뢰할 수 없는 도메인을 등록하는 데 필요한 정보를 지정합니다.

이 필드의 내용...	수행할 작업...
도메인 이름	도메인의 NetBIOS 이름을 지정합니다.
도메인 FQDN	FQDN을 지정합니다.
도메인 컨트롤러 이름입니다	하나 이상의 도메인 컨트롤러 이름을 지정하고 * Resolve * 를 클릭합니다.
도메인 컨트롤러 IP 주소입니다	SnapCenter 서버에서 도메인 컨트롤러 이름을 확인할 수 없는 경우 DNS 해상도를 수정해야 합니다.

6. 확인 * 을 클릭합니다.

LDAPS에 대한 CA 클라이언트 인증서를 구성합니다

Windows Active Directory LDAPS가 CA 인증서와 함께 구성된 경우 SnapCenter 서버에서 LDAPS에 대한 CA 클라이언트 인증서를 구성해야 합니다.

- 단계 *

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 추가/제거 * 를 클릭합니다.
2. 스냅인 추가/제거 창에서 * 인증서 * 를 선택한 다음 * 추가 * 를 클릭합니다.
3. 인증서 스냅인 창에서 * 컴퓨터 계정 * 옵션을 선택한 다음 * 마침 * 을 클릭합니다.
4. 콘솔 루트 * > * 인증서 – 로컬 컴퓨터 * > * 신뢰할 수 있는 루트 인증 기관 * > * 인증서 * 를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 단추로 클릭한 다음 * 모든 작업 * > * 가져오기 * 를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료합니다.

이 마법사 창에서...	다음을 수행합니다.
를 클릭합니다	찾아보기 * 를 클릭하고 _Root Certificate_를 선택한 후 * 다음 * 을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

7. 중간 인증서에 대해 5단계와 6단계를 반복합니다.

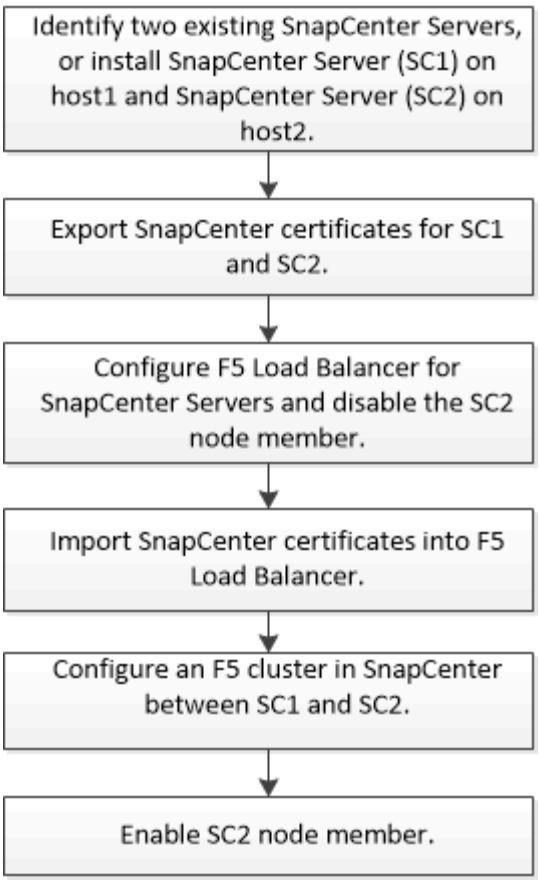
고가용성을 구성합니다

F5를 사용하여 고가용성을 위해 **SnapCenter** 서버를 구성합니다

SnapCenter에서 HA(고가용성)를 지원하기 위해 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.

SnapCenter 4.2.x에서 업그레이드한 후 이전에 네트워크 로드 밸런싱(NLB)을 사용한 경우 해당 구성을 계속 사용하거나 F5 로 전환할 수 있습니다.

워크플로 이미지에는 F5 로드 밸런서를 사용하여 고가용성을 위해 SnapCenter 서버를 구성하는 단계가 나와 있습니다. 자세한 지침은 을 참조하십시오 "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 **F5** 구성 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.
- NLB 또는 F5(Load Balancer Setup)에서 NLB 또는 F5 노드에 의해 부분적으로 확인된 노드를 추가하고 SnapCenter 노드가 이 노드에 연결할 수 없는 경우 SnapCenter 호스트 페이지는 호스트 다운과 실행 상태 사이를 자주 전환합니다. 이 문제를 해결하려면 두 SnapCenter 노드가 모두 NLB 또는 F5 노드의 호스트를 해결할 수 있는지 확인해야 합니다.
- MFA 설정에 대한 SnapCenter 명령은 모든 노드에서 실행되어야 합니다. AD FS(Active Directory Federation Services) 서버에서 F5 클러스터 세부 정보를 사용하여 기반 당사자 구성을 수행해야 합니다. MFA를 사용하도록 설정하면 노드 레벨 SnapCenter UI 액세스가 차단됩니다.
- 페일오버 중에 감사 로그 설정은 두 번째 노드에 반영되지 않습니다. 따라서 F5 패시브 노드가 활성화될 때 감사 로그 설정을 수동으로 반복해야 합니다.

Microsoft 네트워크 로드 밸런서를 수동으로 구성합니다

Microsoft NLB(네트워크 로드 밸런싱)를 구성하여 SnapCenter 고가용성을 설정할 수 있습니다. SnapCenter 4.2에서는 고가용성을 위해 SnapCenter 설치 외부에서 NLB를 수동으로 구성해야 합니다.

SnapCenter를 사용하여 NLB(네트워크 부하 분산)를 구성하는 방법에 대한 자세한 내용은 을 참조하십시오 "SnapCenter를 사용하여 NLB를 구성하는 방법".

SnapCenter 4.1.1 또는 이전 버전에서 SnapCenter를 설치하는 동안 NLB(네트워크 로드 밸런싱)를 지원했습니다.

고가용성을 위해 NLB에서 F5로 전환합니다

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 을 참조할 수도 "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"있습니다.

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_cmdlet을 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 "SnapCenter를 사용하여 NLB 및 ARR을 구성하는 방법"참조하십시오.

SnapCenter 인증서를 내보냅니다

- 단계 *

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * 스냅인 추가/제거 * 를 클릭합니다.
2. 스냅인 추가/제거 창에서 * 인증서 * 를 선택한 다음 * 추가 * 를 클릭합니다.
3. 인증서 스냅인 창에서 * 내 사용자 계정 * 옵션을 선택한 다음 * 마침 * 을 클릭합니다.
4. 콘솔 루트 * > * 인증서 - 현재 사용자 * > * 신뢰할 수 있는 루트 인증 기관 * > * 인증서 * 를 클릭합니다.
5. SnapCenter 고유 이름이 있는 인증서를 마우스 오른쪽 단추로 클릭한 다음 * 모든 작업 * > * 내보내기 * 를 선택하여 내보내기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료합니다.

이 마법사 창에서...	다음을 수행합니다.
개인 키를 내보냅니다	Yes, export the private key * 옵션을 선택한 후 * Next * 를 클릭합니다.
파일 형식 내보내기	변경하지 않고 * 다음 * 을 클릭합니다.
보안	내보낸 인증서에 사용할 새 암호를 지정하고 * 다음 * 을 클릭합니다.
내보낼 파일	내보낸 인증서의 파일 이름을 지정하고(.pfx 사용) * 다음 * 을 클릭합니다.
인증서 내보내기 마법사를 완료합니다	요약을 검토한 후 * Finish * 를 클릭하여 내보내기를 시작합니다.

결과 *

인증서는 .pfx 형식으로 내보내집니다.

역할 기반 액세스 제어(RBAC) 구성

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.

> SnapCenter 4.5에서는 공백(), 하이픈(-), 밑줄(_) 및 콜론(:)과 같은 특수 문자만 사용자 이름과 그룹 이름에 포함할 수 있습니다. 이러한 특수 문자로 SnapCenter의 이전 릴리스에서 만든 역할을 사용하려면 SnapCenter WebApp이 설치된 web.config 파일에서 'disableSQLInjectionValidation' 매개 변수의 값을 true 로 변경하여 역할 이름의 유효성 검사를 비활성화할 수 있습니다. 값을 수정한 후에는 서비스를 다시 시작할 필요가 없습니다.

- 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
복제	호스트, 리소스 그룹, 정책

작동	자산 할당
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 을 참조하십시오 "VMware vSphere용 SnapCenter 플러그인과 함께 패키지로 제공되는 사전 정의된 역할".

- 단계 *

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

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

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

4. Assign * 을 클릭한 다음 Assign Assets 페이지에서 다음을 수행합니다.
   a. 자산 * 드롭다운 목록에서 자산 유형을 선택합니다.
   b. [자산] 테이블에서 자산을 선택합니다.

      사용자가 자산을 SnapCenter에 추가한 경우에만 자산이 나열됩니다.

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

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

역할을 생성합니다

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

"SnapCenterAdmin" 역할로 로그인해야 합니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
2. 설정 페이지에서 * 역할 * 을 클릭합니다.
3. 을 클릭합니다.
4. 역할 추가 페이지에서 새 역할의 이름과 설명을 지정합니다.

   SnapCenter 4.5에서는 공백(), 하이픈(-), 밑줄(_) 및 콜론(:)과 같은 특수 문자만 사용자 이름과 그룹 이름에 포함할 수 있습니다. 이러한 특수 문자로 SnapCenter의 이전 릴리스에서 만든 역할을 사용하려면 SnapCenter WebApp이 설치된 web.config 파일에서 'disableSQLInjectionValidation' 매개 변수의 값을 true 로 변경하여 역할 이름의 유효성 검사를 비활성화할 수 있습니다. 값을 수정한 후에는 서비스를 다시 시작할 필요가 없습니다.

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.

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

보안 로그인 명령을 사용하여 **ONTAP RBAC** 역할을 추가합니다

스토리지 시스템에서 clustered ONTAP을 실행 중인 경우 보안 로그인 명령을 사용하여 ONTAP RBAC 역할을 추가할 수 있습니다.

시작하기 전에

- Clustered ONTAP을 실행 중인 스토리지 시스템에 대해 ONTAP RBAC 역할을 생성하기 전에 다음을 확인해야 합니다.
  - 수행할 작업(또는 작업)입니다
  - 이러한 작업을 수행하는 데 필요한 권한입니다
- RBAC 역할을 구성하려면 다음 작업을 수행해야 합니다.
  - 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 있는지 여부에 따라 구성을 다양하게 변경할 수 있습니다.
- 이 작업에 대한 정보 *

스토리지 시스템에서 이러한 역할을 간단히 구성하기 위해 NetApp 커뮤니티 포럼에 게시된 RBAC 사용자 작성자 for Data ONTAP 툴을 사용할 수 있습니다.

이 도구는 자동으로 ONTAP 권한 설정을 올바르게 처리합니다. 예를 들어, RBAC Data ONTAP용 사용자 작성 도구 는 모든 액세스 권한이 먼저 나타나도록 올바른 순서로 권한을 자동으로 추가합니다. 읽기 전용 권한을 먼저 추가한 다음 모든 액세스 권한을 추가하면 ONTAP에서 모든 액세스 권한을 중복으로 표시하고 무시합니다.

나중에 SnapCenter 또는 ONTAP를 업그레이드할 경우 RBAC 사용자 생성기 for Data ONTAP 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".

일관성을 위해 SnapCenter 문서는 사용 권한을 사용하는 역할을 나타냅니다. OnCommand 시스템 관리자 GUI는 *privilege* 대신 _attribute_라는 용어를 사용합니다. ONTAP RBAC 역할을 설정할 때 이 두 용어는 모두 동일합니다.

- 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 을 참조하십시오 "역할을 생성하고 권한을 할당하는 ONTAP CLI 명령입니다".

2. 다음 명령을 입력하여 사용자 이름을 생성합니다.

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

   - user_name은 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.

   ```
   security login modify username <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.

```
security login role create -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
ontapi -authmethod password -role <SVM_Role_Name\>
```

2. 사용자 잠금을 해제합니다.

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

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

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

SnapCenter 5.0에서는 SVM admin 사용자가 REST API를 통해서만 지원됩니다. 가상 서버 관리자가 아닌 다른 관리자를 사용하여 역할을 생성하려면 ZAPI를 사용해야 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 stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"lun resize" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot 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 unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"vserver cifs share show" -access all

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

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 -authmethod password -role <role_name\>
```

2. 사용자 잠금을 해제합니다.

```
security login unlock -user <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.

SnapCenter 5.0에서는 클러스터 관리자가 REST API를 사용하는 경우에만 지원됩니다. 비 클러스터 관리자를 사용하여 역할을 생성하려면 ZAPI를 사용해야 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 stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all`

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

"security login" -access readonly

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

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume 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 unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all

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

Active Directory 읽기 권한을 사용하도록 **IIS** 응용 프로그램 풀을 구성합니다

SnapCenter에 대해 Active Directory 읽기 권한을 설정해야 할 때 사용자 지정 응용 프로그램 풀 계정을 만들도록 Windows Server에서 IIS(인터넷 정보 서비스)를 구성할 수 있습니다.

- 단계 *
  1. SnapCenter가 설치된 Windows 서버에서 IIS 관리자를 엽니다.
  2. 왼쪽 탐색 창에서 * 응용 프로그램 풀 * 을 클릭합니다.
  3. 응용 프로그램 풀 목록에서 SnapCenter를 선택한 다음 작업 창에서 * 고급 설정 * 을 클릭합니다.
  4. ID를 선택한 다음 *… * 를 클릭하여 SnapCenter 응용 프로그램 풀 ID를 편집합니다.
  5. 사용자 지정 계정 필드에 Active Directory 읽기 권한이 있는 도메인 사용자 또는 도메인 관리자 계정 이름을 입력합니다.
  6. 확인 을 클릭합니다.

     사용자 지정 계정은 SnapCenter 응용 프로그램 풀의 기본 제공 ApplicationPoolIdentity 계정을 대체합니다.

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 대한 정보 *
- 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 *
  1. 설정 * 페이지에서 * 설정 * > * 글로벌 설정 * > * 감사 로그 설정 * 으로 이동합니다.
  2. Audit log(감사 로그) 섹션에서 세부 정보를 입력합니다.
  3. 감사 로그 디렉토리 * 및 * 감사 체크섬 로그 디렉토리 * 를 입력합니다
     a. 최대 파일 크기를 입력합니다
     b. 최대 로그 파일을 입력합니다
     c. 경고를 보낼 디스크 공간 사용 비율을 입력합니다
  4. (선택 사항) * Log UTC Time * 을 활성화합니다.
  5. (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.

  6. (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.

     a. 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.

스토리지 시스템을 추가합니다

데이터 보호 및 프로비저닝 작업을 수행하려면 SnapCenter 스토리지에 대한 ONTAP 액세스 권한을 제공하는 스토리지 시스템이나 NetApp ONTAP용 Amazon FSx를 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 탭에서 * 수정 * 을 클릭하여 암호를 업데이트할 수 있습니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 스토리지 시스템 * 을 클릭합니다.

2. 스토리지 시스템 페이지에서 * 신규 * 를 클릭합니다.
3. 스토리지 시스템 추가 페이지에서 다음 정보를 제공합니다.

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

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

FAS 또는 AFF 스토리지 시스템을 모든 SAN 어레이(ASA)로 업그레이드한 경우, SnapCenter 서버의 스토리지 접속을 새로 고쳐서 SnapCenter의 새 스토리지 유형을 반영해야 합니다.

- 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 -noteto enable
```

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

SnapCenter 표준 컨트롤러 기반 라이센스를 추가합니다

FAS, AFF 또는 모든 SAN 어레이(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 관리자 또는 스토리지 클러스터 명령줄을 사용하여 FAS, AFF 또는 ASA 스토리지 컨트롤러에 직접 추가하여 사용 가능

  SnapCenter 컨트롤러 기반 라이센스의 경우 SnapCenter GUI에 라이센스 정보를 입력하지 않습니다.

- 컨트롤러의 일련 번호에 잠금 상태입니다

필요한 라이센스에 대한 자세한 내용은 을 "SnapCenter 라이센스"참조하십시오.

1단계: SnapManager 제품군 라이센스가 설치되었는지 확인합니다

SnapCenter GUI를 사용하면 SnapManager 제품군 라이센스가 FAS, AFF 또는 ASA 운영 스토리지 시스템에 설치되어 있는지 여부를 확인하고 SnapManager 제품군 라이센스가 필요할 수 있는 스토리지 시스템을 식별할 수 있습니다. SnapManager 제품군 라이센스는 FAS, AFF, ASA SVM 또는 운영 스토리지 시스템의 클러스터에만 적용됩니다.

컨트롤러에 SnapManager Suite 라이센스가 이미 있는 경우 SnapCenter 표준 컨트롤러 기반 라이센스 권한이 자동으로 제공됩니다. SnapManager 라이센스 및 SnapCenter 표준 컨트롤러 기반 라이센스 이름은 서로 바꿔서 사용되지만 동일한 라이센스를 나타냅니다.

단계

1. 왼쪽 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.

   - ✔ FAS, AFF 또는 ASA 운영 스토리지 시스템에 SnapManager 제품군 라이센스가 설치되어 있음을

나타냅니다.

- ⊘ FAS, AFF 또는 ASA 운영 스토리지 시스템에 SnapManager 제품군 라이센스가 설치되어 있지 않음을 나타냅니다.
- 해당 없음 은 스토리지 컨트롤러가 Cloud Volumes ONTAP, ONTAP Select 또는 보조 스토리지 플랫폼에 있기 때문에 SnapManager Suite 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.

ⓘ SnapCenter 표준 컨트롤러 기반 라이센스는 컨트롤러에 SnapManagerSuite 라이센스로 표시됩니다.

단계

1. ONTAP 명령줄을 사용하여 NetApp 컨트롤러에 로그인합니다.
2. license show 명령을 입력한 다음 출력을 확인하여 SnapManagerSuite 라이센스가 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: 1-81-00000000000000000000000xx
Owner: cluster1-01
Package           Type     Description              Expiration
----------------- -------- ---------------------    ---------------
NFS               license  NFS License              -
CIFS              license  CIFS License             -
iSCSI             license  iSCSI License            -
FCP               license  FCP License              -
SnapRestore       license  SnapRestore License      -
SnapMirror        license  SnapMirror License       -
FlexClone         license  FlexClone License        -
SnapVault         license  SnapVault License        -
SnapManagerSuite  license  SnapManagerSuite License -
```

이 예제에서는 SnapManagerSuite 라이센스가 설치되어 있으므로 추가 SnapCenter 라이센스 작업이 필요하지

않습니다.

3단계: 컨트롤러의 일련 번호를 검색합니다

컨트롤러 기반 라이센스의 일련 번호를 검색하려면 컨트롤러 일련 번호가 필요합니다. ONTAP 명령줄을 사용하여 컨트롤러 일련 번호를 검색할 수 있습니다. 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: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

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

3. 일련 번호를 기록합니다.

4단계: 컨트롤러 기반 라이센스의 일련 번호를 검색합니다

FAS 또는 AFF 스토리지를 사용하는 경우 ONTAP 명령줄을 사용하여 설치하기 전에 NetApp Support 사이트에서 SnapCenter 컨트롤러 기반 라이센스를 검색할 수 있습니다.

시작하기 전에

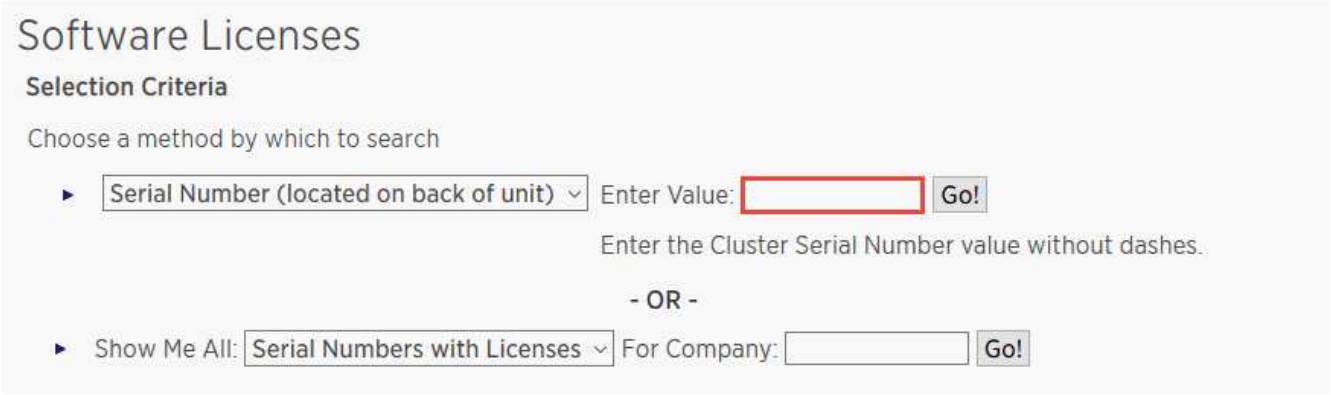
- 유효한 NetApp Support 사이트 로그인 자격 증명이 있어야 합니다.

유효한 자격 증명을 입력하지 않으면 검색에 대한 정보가 반환되지 않습니다.

- 컨트롤러의 일련 번호가 있어야 합니다.

단계

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



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:

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

이 명령은 admin 권한 수준에서 사용할 수 있습니다.

3. SnapManagerSuite 라이센스가 설치되었는지 확인합니다.

   ```
   license show
   ```

6단계: 평가판 라이센스를 제거합니다

컨트롤러 기반 SnapCenter 표준 라이센스를 사용하고 있으며 용량 기반 평가판 라이센스(일련 번호가 ""50"으로 끝나는 번호)를 제거해야 하는 경우 MySQL 명령을 사용하여 평가판 라이센스를 수동으로 제거해야 합니다. 평가판 라이센스는 SnapCenter GUI를 사용하여 삭제할 수 없습니다.

> SnapCenter 표준 컨트롤러 기반 라이센스를 사용하는 경우에만 평가판 라이센스를 수동으로 제거해야 합니다. SnapCenter 표준 용량 기반 라이센스를 조달하여 SnapCenter GUI에 추가하면 평가판 라이센스가 자동으로 덮어쓰여집니다.

단계

1. SnapCenter 서버에서 PowerShell 창을 열어 MySQL 암호를 재설정합니다.
   a. Open-SmConnection cmdlet을 실행하여 SnapCenter 서버에서 SnapCenterAdmin 계정에 대한 연결 세션을 시작합니다.
   b. Set-SmRepositoryPassword를 실행하여 MySQL 암호를 재설정합니다.

      cmdlet에 대한 자세한 내용은 을 "SnapCenter 소프트웨어 cmdlet 참조 가이드"참조하십시오.

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';
   ```

SnapCenter 표준 용량 기반 라이센스 추가

SnapCenter 표준 용량 라이센스를 사용하여 ONTAP Select 및 Cloud Volumes ONTAP 플랫폼의 데이터를 보호할 수 있습니다.

용량 라이센스의 특징은 다음과 같습니다.

- 51xxxxxxx 형식의 9자리 일련 번호로 구성됩니다

  라이센스 일련 번호 및 유효한 NetApp Support 사이트 로그인 자격 증명을 사용하여 SnapCenter GUI를 통해 라이센스를 활성화합니다.

- 사용된 스토리지 용량 또는 보호할 데이터의 크기 중 더 낮은 것을 기준으로 비용을 설정하고 SnapCenter에서 데이터를 관리하는 별도의 영구 라이센스로 사용할 수 있습니다
- 테라바이트당 가용성

  예를 들어, 1TB, 2TB, 4TB 등에 대한 용량 기반 라이센스를 얻을 수 있습니다.

- 100TB 용량 사용 권한이 있는 90일 평가판 라이센스로 제공됩니다

  필요한 라이센스에 대한 자세한 내용은 을 "SnapCenter 라이센스"참조하십시오.

SnapCenter는 Cloud Volumes ONTAP 및 관리하는 ONTAP Select 스토리지에서 매일 자정에 용량 사용량을 자동으로 계산합니다. 표준 용량 라이센스를 사용하는 경우 SnapCenter는 총 라이센스 용량에서 모든 볼륨에 사용된 용량을 추론하여 사용하지 않은 용량을 계산합니다. 사용된 용량이 라이센스 용량을 초과하면 SnapCenter 대시보드에 초과 사용 경고가 표시됩니다. SnapCenter에서 용량 임계값 및 알림을 구성한 경우 사용된 용량이 지정한 임계값에 도달하면 이메일이 전송됩니다.

1단계**:** 용량 요구 사항 계산

SnapCenter 용량 기반 라이센스를 얻기 전에 SnapCenter에서 관리할 호스트의 용량을 계산해야 합니다.

Cloud Volumes ONTAP 또는 ONTAP Select 시스템에서 클러스터 관리자여야 합니다.

이 작업에 대해

SnapCenter는 사용된 실제 용량을 계산합니다. 파일 시스템 또는 데이터베이스의 크기가 1TB이지만 500GB의 공간만 사용되는 경우 SnapCenter는 500GB의 사용된 용량을 계산합니다. 볼륨 용량은 중복제거 및 압축 후 계산되며 전체 볼륨의 사용된 용량을 기준으로 계산됩니다.

단계

1. ONTAP 명령줄을 사용하여 NetApp 컨트롤러에 로그인합니다.
2. 사용된 볼륨 용량을 보려면 명령을 입력합니다.

```
select::> vol show -fields used -volume Engineering,Marketing
vserver volume       used
------- ------       ------
VS1     Engineering  2.13TB
VS1     Marketing    2.62TB

2   entries were displayed.
```

두 볼륨의 사용된 총 용량은 5TB 미만입니다. 따라서 모든 5TB 데이터를 보호하려면 최소 SnapCenter 용량 기반 라이센스 요구사항이 5TB 이상입니다.

그러나 총 사용 용량 5TB의 2TB만 보호하려면 2TB 용량 기반 라이센스를 얻을 수 있습니다.

2단계**:** 용량 기반 라이센스의 일련 번호를 검색합니다

SnapCenter 용량 기반 라이센스 일련 번호는 주문 확인 또는 문서 패키지에서 사용할 수 있습니다. 하지만 이 일련 번호가 없는 경우 NetApp Support 사이트에서 검색할 수 있습니다.

유효한 NetApp Support 사이트 로그인 자격 증명이 있어야 합니다.

단계

1. 에 "NetApp Support 사이트"로그인합니다.

2. 시스템 * > * 소프트웨어 라이센스 * 로 이동합니다.
3. 선택 기준 영역의 모두 표시: 일련 번호 및 라이센스 드롭다운 메뉴에서 * SC_STANDARD * 를 선택합니다.

4. 회사 이름을 입력한 다음 * Go! * 를 선택합니다.

   51xxxxxxx 형식의 9자리 SnapCenter 라이센스 일련 번호가 표시됩니다.

5. 일련 번호를 기록합니다.

3단계**: NetApp** 라이센스 파일을 생성합니다

SnapCenter GUI에 NetApp Support 사이트 자격 증명과 SnapCenter 라이센스 일련 번호를 입력하지 못하거나 SnapCenter에서 NetApp Support 사이트에 인터넷에 액세스할 수 없는 경우 NetApp 라이센스 파일(NLF)을 생성할 수 있습니다. 그런 다음 SnapCenter 호스트에서 액세스할 수 있는 위치에 파일을 다운로드하여 저장할 수 있습니다.

시작하기 전에

- ONTAP Select를 SnapCenter 또는 Cloud Volumes ONTAP와 함께 사용해야 합니다.
- 유효한 NetApp Support 사이트 로그인 자격 증명이 있어야 합니다.
- 51xxxxxxx 형식의 라이센스 일련 번호는 9자리 숫자여야 합니다.

단계

1. 로 "NetApp 라이센스 파일 생성기"이동합니다.
2. 필요한 정보를 입력합니다.
3. 제품 라인 필드의 풀다운 메뉴에서 * SnapCenter 표준(용량 기반) * 을 선택합니다.
4. 제품 일련 번호 필드에 SnapCenter 라이센스 일련 번호를 입력합니다
5. NetApp 데이터 개인 정보 보호 정책을 읽고 동의한 다음 * 제출 * 을 선택합니다.
6. 라이센스 파일을 저장한 다음 파일 위치를 기록합니다.

4단계**:** 용량 기반 라이센스 추가

ONTAP Select 또는 Cloud Volumes ONTAP 플랫폼과 함께 SnapCenter를 사용하는 경우 SnapCenter 용량 기반 라이센스를 하나 이상 설치해야 합니다.

시작하기 전에

- SnapCenter 관리자로 로그인해야 합니다.

- 유효한 NetApp Support 사이트 로그인 자격 증명이 있어야 합니다.
- 51xxxxxxx 형식의 라이센스 일련 번호는 9자리 숫자여야 합니다.

  NetApp 라이센스 파일(NLF)을 사용하여 라이센스를 추가하는 경우 라이센스 파일의 위치를 알아야 합니다.

이 작업에 대해

설정 페이지에서 다음 작업을 수행할 수 있습니다.

- 라이센스를 추가합니다.
- 라이센스 세부 정보를 보고 각 라이센스에 대한 정보를 빠르게 찾습니다.
- 라이센스 용량을 업데이트하거나 임계값 알림 설정을 변경하는 등 기존 라이센스를 대체하려는 경우 라이센스를 수정합니다.
- 기존 라이센스를 교체하려는 경우 또는 라이센스가 더 이상 필요하지 않은 경우 라이센스를 삭제합니다.

> 평가판 라이센스(일련 번호가 50으로 끝나는 번호)는 SnapCenter GUI를 사용하여 삭제할 수 없습니다. 조달된 SnapCenter 표준 용량 기반 라이센스를 추가하면 평가판 라이센스가 자동으로 덮어쓰여집니다.

단계

1. 왼쪽 탐색 창에서 * 설정 * 을 선택합니다.
2. 설정 페이지에서 * 소프트웨어 * 를 선택합니다.
3. 소프트웨어 페이지의 라이센스 섹션에서 * 추가 * ()를 선택합니다 .
4. SnapCenter 라이센스 추가 마법사에서 다음 방법 중 하나를 선택하여 추가할 라이센스를 가져옵니다.

이 필드의 내용...	수행할 작업...
NSS(NetApp Support Site) 로그인 자격 증명을 입력하여 라이센스를 가져옵니다	a. NSS 사용자 이름을 입력합니다. b. NSS 암호를 입력합니다. c. 컨트롤러 기반 라이센스의 일련 번호를 입력합니다.
NetApp 라이센스 파일	a. 라이센스 파일의 위치를 찾은 다음 선택합니다. b. 열기 * 를 선택합니다.

5. 알림 페이지에서 SnapCenter에서 이메일, EMS 및 AutoSupport 알림을 보내는 용량 임계값을 입력합니다.

   기본 임계값은 90%입니다.

6. 이메일 알림에 맞게 SMTP 서버를 구성하려면 * 설정 * > * 글로벌 설정 * > * 알림 서버 설정 * 을 선택한 후 다음 세부 정보를 입력합니다.

이 필드의 내용...	수행할 작업...
이메일 기본 설정	Always * 또는 * Never * 중에서 선택합니다.
이메일 설정을 제공합니다	Always * 를 선택한 경우 다음을 지정합니다. • 보낸 사람 이메일 주소입니다 • 수신자 이메일 주소입니다 • 선택 사항: 기본 제목 줄을 편집합니다 기본 제목은 "SnapCenter 라이센스 용량 알림 "입니다.

7. 스토리지 시스템 syslog에 EMS(이벤트 관리 시스템) 메시지를 보내거나 스토리지 시스템에 실패한 작업을 위한 AutoSupport 메시지를 보내려면 적절한 확인란을 선택합니다. 발생할 수 있는 문제를 해결하려면 AutoSupport를 활성화하는 것이 좋습니다.
8. 다음 * 을 선택합니다.
9. 요약을 검토한 후 * Finish * 를 선택합니다.

스토리지 시스템을 프로비저닝합니다

Windows 호스트에서 스토리지 용량 할당

LUN 스토리지를 구성합니다

SnapCenter를 사용하여 FC 연결 또는 iSCSI 연결 LUN을 구성할 수 있습니다. SnapCenter를 사용하여 기존 LUN을 Windows 호스트에 연결할 수도 있습니다.

LUN은 SAN 구성의 기본 스토리지 단위입니다. Windows 호스트는 시스템의 LUN을 가상 디스크로 인식합니다. 자세한 내용은 을 "ONTAP 9 SAN 구성 가이드"참조하십시오.

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.

iSCSI 세션 연결을 해제합니다

경우에 따라 여러 세션이 있는 대상에서 iSCSI 세션의 연결을 끊어야 할 수 있습니다.

- 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. iSCSI 세션 목록에서 연결을 끊을 세션을 선택하고 * 세션 연결 끊기 * 를 클릭합니다.
6. 세션 연결 끊기 대화 상자에서 * 확인 * 을 클릭합니다.

   SnapCenter는 iSCSI 세션의 연결을 끊습니다.

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 igroup을 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 igroup을 생성합니다.

igroup의 이름을 바꿉니다

SnapCenter를 사용하여 기존 igroup의 이름을 바꿀 수 있습니다.

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

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

igroup을 수정합니다

SnapCenter를 사용하여 igroup 이니시에이터를 기존 igroup에 추가할 수 있습니다. igroup을 작성하는 동안 하나의 호스트만 추가할 수 있습니다. 클러스터에 대한 igroup을 작성하려는 경우 igroup을 수정하여 해당 igroup에 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 igroup에 사용할 SVM을 선택합니다.
  4. igroup 목록에서 igroup을 선택하고 * igroup에 이니시에이터 추가 * 를 클릭합니다.
  5. 호스트를 선택합니다.
  6. 이니시에이터를 선택하고 * OK * 를 클릭합니다.

igroup을 삭제합니다

더 이상 필요하지 않은 경우 SnapCenter를 사용하여 igroup을 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 igroup에 사용할 SVM을 선택합니다.
  4. SVM의 igroup 목록에서 삭제할 igroup을 선택하고 * Delete * 를 클릭합니다.
  5. Delete igroup (그룹 삭제) 대화 상자에서 * OK * (확인 *)를 클릭합니다.

     SnapCenter이 igroup을 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.

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 *
  1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
  2. 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 경로	찾아보기 * 를 클릭하여 LUN이 포함된 폴더의 전체 경로를 선택합니다.
LUN 이름	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.

선택...	만약...
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	SnapCenter는 시스템 드라이브에 따라 볼륨 마운트 지점을 자동으로 할당합니다. 예를 들어, 시스템 드라이브가 C:인 경우 자동 할당은 C: 드라이브(C:\scmnpt\) 아래에 볼륨 마운트 지점을 생성합니다. 공유 디스크에는 자동 할당이 지원되지 않습니다.
드라이브 문자를 할당합니다	인접한 드롭다운 목록에서 선택한 드라이브에 디스크를 마운트합니다.
볼륨 마운트 지점을 사용합니다	인접한 필드에 지정한 드라이브 경로에 디스크를 마운트합니다. 볼륨 마운트 지점의 루트는 디스크를 생성하는 호스트가 소유해야 합니다.
드라이브 문자 또는 볼륨 마운트 지점을 할당하지 마십시오	Windows에서 디스크를 수동으로 마운트하려면 이 옵션을 선택합니다.
LUN 크기입니다	최소 150MB의 LUN 크기를 지정합니다. 인접 드롭다운 목록에서 MB, GB 또는 TB를 선택합니다.
이 LUN을 호스팅하는 볼륨에 씬 프로비저닝을 사용합니다	씬 LUN을 프로비저닝합니다. 씬 프로비저닝은 필요한 만큼의 스토리지 공간만 한 번에 할당하므로 LUN이 최대 가용 용량까지 효율적으로 성장할 수 있습니다. 필요한 모든 LUN 스토리지를 수용할 수 있는 충분한 공간이 볼륨에 있는지 확인하십시오.

속성	설명
파티션 유형을 선택합니다	GUID 파티션 테이블의 GPT 파티션 또는 마스터 부트 레코드의 MBR 파티션을 선택합니다. MBR 파티션은 Windows Server 장애 조치 클러스터에서 정렬 불량 문제를 일으킬 수 있습니다. UEFI(Unified Extensible Firmware Interface) 파티션 디스크는 지원되지 않습니다.

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. 다중 경로 I/O(MPIO)와 함께 FC를 사용하는 경우 여러 FC 이니시에이터를 선택할 수 있습니다.

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

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

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 경로	찾아보기 * 를 클릭하여 LUN이 포함된 볼륨의 전체 경로를 선택합니다.
LUN 이름	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.
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 igroup을 LUN에 매핑할지 또는 새 igroup을 생성할지를 지정합니다.

선택...	만약...
선택한 이니시에이터에 대해 새 igroup을 생성합니다	선택한 이니시에이터에 대해 새 igroup을 생성하려고 합니다.

선택...	만약...
기존 igroup을 선택하거나 선택한 이니시에이터에 대한 새 igroup을 지정합니다	선택한 이니시에이터에 대해 기존 igroup을 지정하거나 지정한 이름의 새 igroup을 생성합니다. igroup 이름 * 필드에 igroup 이름을 입력합니다. 기존 igroup 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 *

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 호스트 페이지에서 * 공유 * 를 클릭합니다.
3. Storage Virtual Machine * 드롭다운 목록에서 SVM을 선택합니다.
4. 새로 만들기 * 를 클릭합니다.

   새 공유 대화 상자가 열립니다.

5. 새 공유 대화 상자에서 공유를 정의합니다.

이 필드에서...	수행할 작업...
설명	공유에 대한 설명 텍스트를 입력합니다.

이 필드에서...	수행할 작업...
공유 이름	공유 이름(예: test_share)을 입력합니다. 공유에 대해 입력한 이름도 볼륨 이름으로 사용됩니다. 공유 이름: • UTF-8 문자열이어야 합니다. • 0x00에서 0x1F 사이의 제어 문자(모두 포함), 0x22(큰따옴표) 및 특수 문자를 포함하지 않아야 합니다 `\ / [ ] : (vertical bar) < > + = ; , ?`
공유 경로	• 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 재확보 작업을 수행하지 않으려는 경우 Microsoft Windows용 SnapCenter 플러그인에서 제공하는 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 을 참조할 수도 "SnapCenter 소프트웨어 cmdlet 참조 가이드"있습니다.

서버에서 SnapDrive for Windows가 제거되어 SnapCenter PowerShell cmdlet이 끊어진 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.

지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

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 igroup을 생성할 수 없습니다.

  공유 클러스터 디스크로 사용될 RDM LUN을 생성하기 전에 모든 ESXi 호스트의 이니시에이터를 포함하는 igroup을 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 LUN**을 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 을 "물리적 호스트에서 가상 시스템을 클러스터링합니다"참조하십시오.

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.in I)에서 CA 인증서, 서버 공용 인증서, 클라이언트 공용 인증서, 서버 개인 키 및 클라이언트 개인 키 경로를 업데이트합니다.

   기본 MySQL 서버 구성 파일(my.in i) 경로는 `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`입니다.

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

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

   다음 예제는 기본 폴더에 있는 my.ini 파일의 [mysqld] 섹션에 복사된 인증서 및 키 파일을 보여 `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`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. web.config 파일에서 MySQLProtocol 키 값을 업데이트합니다.

   다음 예제에서는 web.config 파일에서 업데이트된 MySQLProtocol 키의 값을 보여 줍니다.

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

7. my.ini 파일의 [client] 섹션에 제공된 경로로 web.config 파일을 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.in I)에서 CA 인증서, 서버 공용 인증서, 클라이언트 공용 인증서, 서버 개인 키 및 클라이언트 개인 키 경로를 업데이트합니다.

   기본 MySQL 서버 구성 파일(my.in I) 경로는 C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.in 입니다

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

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

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

   MySQL 서버 구성 파일(my.in I)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 web.config 파일에서 MySQLProtocol 키의 값을 업데이트합니다.

   다음 예제에서는 web.config 파일에서 업데이트된 MySQLProtocol 키 값을 보여 줍니다.

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

8. 두 HA 노드에 대해 my.ini 파일의 [client] 섹션에 지정한 경로로 web.config 파일을 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.

설치 중에 **Windows** 호스트에서 활성화된 기능입니다

SnapCenter 서버 설치 프로그램을 사용하면 설치 중에 Windows 호스트에서 Windows 기능 및 역할을 사용할 수 있습니다. 이는 문제 해결 및 호스트 시스템 유지 관리 목적으로 활용할 수 있습니다.

범주	피처
웹 서버	• 인터넷 정보 서비스 • 월드 와이드 웹 서비스 • 공통 HTTP 기능 ◦ 기본 문서 ◦ 디렉터리 검색 ◦ HTTP 오류 ◦ HTTP 리디렉션 ◦ 정적 콘텐츠 ◦ WebDAV 게시 • 상태 및 진단 ◦ 사용자 지정 로깅 ◦ HTTP 로깅 ◦ 로깅 도구 ◦ 모니터 요청 ◦ 추적 • 성능 기능 ◦ 정적 콘텐츠 압축 • 보안 ◦ IP 보안 ◦ 기본 인증 ◦ 중앙 집중식 SSL 인증서 지원 ◦ 클라이언트 인증서 매핑 인증 ◦ IIS 클라이언트 인증서 매핑 인증 ◦ IP 및 도메인 제한 ◦ 요청 필터링 ◦ URL 권한 부여 ◦ Windows 인증 • 응용 프로그램 개발 기능 ◦ NET 확장성 4.5 ◦ 응용 프로그램 초기화 ◦ ASP.NET 4.7.2 ◦ 서버 측 포함 ◦ WebSocket 프로토콜 관리 도구 IIS 관리 콘솔

범주	피처
IIS 관리 스크립트 및 도구	• IIS 관리 서비스 • 웹 관리 도구
NET Framework 4.7.2 기능+	• NET Framework 4.7.2 • ASP.NET 4.7.2 • WCF(Windows Communication Foundation) HTTP Activation45 ◦ TCP 활성화 ◦ HTTP 활성화 ◦ MSMQ(Message Queuing) 활성화 의 경우. 자세한 문제 해결 정보는 을 참조하십시오 "인터넷에 연결되지 않은 기존 시스템의 경우 SnapCenter 업그레이드 또는 설치가 실패합니다".
메시지 큐	• 메시지 큐 서비스 SnapCenter가 만들고 관리하는 MSMQ 서비스를 사용하는 다른 응용 프로그램이 없는지 확인합니다. • MSMQ 서버
Windows 프로세스 활성화 서비스	• 프로세스 모델
구성 API	모두

저작권 정보

Copyright © 2025 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 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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