



# 관리 노드로 작업

## Element Software

NetApp  
November 12, 2025

# 목차

관리 노드로 작업	1
관리 노드 개요	1
관리 노드 설치 또는 복구	2
관리 노드 설치	2
vCenter에서 NetApp HCC 역할 생성	8
스토리지 네트워크 인터페이스 컨트롤러(NIC) 구성	13
관리 노드 복구	15
관리 노드에 접근	20
관리 노드별 UI에 액세스	20
관리 노드 REST API UI에 액세스합니다.	21
관리 노드 기본 SSL 인증서 변경	22
더 많은 정보를 찾아보세요	23
관리 노드 UI 작업	23
관리 노드 UI 개요	23
알림 모니터링 구성	24
관리 노드 네트워크, 클러스터 및 시스템 설정을 수정하고 테스트합니다.	24
관리 노드에서 시스템 유틸리티 실행	26
관리 노드 REST API로 작업	27
관리 노드 REST API UI 개요	27
REST API 사용 권한 얻기	28
Active IQ 및 NetApp 모니터링 활성화	29
여러 vCenter에 대한 NetApp Hybrid Cloud Control 구성	31
관리 노드에 컨트롤러 자산 추가	32
스토리지 클러스터 자산 생성 및 관리	34
기존 컨트롤러 자산 보기 또는 편집	39
프록시 서버 구성	41
관리 노드 OS 및 서비스 버전 확인	42
관리 서비스에서 로그 가져오기	43
지원 연결 관리	45
기본 문제 해결을 위해 SSH를 사용하여 스토리지 노드에 액세스	45
원격 NetApp 지원 세션 시작	49
관리 노드에서 SSH 기능 관리	50

# 관리 노드로 작업

## 관리 노드 개요

관리 노드(mNode)를 사용하면 시스템 서비스를 사용하고, 클러스터 자산과 설정을 관리하고, 시스템 테스트와 유틸리티를 실행하고, 시스템 모니터링을 위해 Active IQ 구성하고, 문제 해결을 위해 NetApp 지원 액세스를 활성화할 수 있습니다.



모범 사례로, 하나의 관리 노드만 하나의 VMware vCenter 인스턴스에 연결하고, 여러 관리 노드에서 동일한 스토리지 및 컴퓨팅 리소스나 vCenter 인스턴스를 정의하지 마세요.

Element 소프트웨어 버전 11.3 이상을 실행하는 클러스터의 경우 다음 두 인터페이스 중 하나를 사용하여 관리 노드로 작업할 수 있습니다.

- 관리 노드 UI를 사용하여([https://\[mNode IP\]:442](https://[mNode IP]:442)), 네트워크 및 클러스터 설정을 변경하고, 시스템 테스트를 실행하거나 시스템 유틸리티를 사용할 수 있습니다.
- 내장된 REST API UI를 사용하여([https://\[mNode IP\]/mnode](https://[mNode IP]/mnode)), 프록시 서버 구성, 서비스 수준 업데이트 또는 자산 관리를 포함하여 관리 노드 서비스와 관련된 API를 실행하거나 이해할 수 있습니다.

관리 노드 설치 또는 복구:

- ["관리 노드 설치"](#)
- ["스토리지 네트워크 인터페이스 컨트롤러\(NIC\) 구성"](#)
- ["관리 노드 복구"](#)

관리 노드에 접근하세요:

- ["관리 노드\(UI 또는 REST API\)에 액세스합니다."](#)

기본 SSL 인증서를 변경합니다.

- ["관리 노드 기본 SSL 인증서 변경"](#)

관리 노드 UI로 작업 수행:

- ["관리 노드 UI 개요"](#)

관리 노드 REST API를 사용하여 작업 수행:

- ["관리 노드 REST API UI 개요"](#)

NetApp 지원팀과 원격 SSH 기능을 비활성화하거나 활성화하거나 원격 지원 터널 세션을 시작하여 문제 해결을 도와주세요.

- ["기본 문제 해결을 위해 SSH를 사용하여 스토리지 노드에 액세스"](#)
  - ["원격 NetApp 지원 연결 활성화"](#)
  - ["관리 노드에서 SSH 기능 관리"](#)

더 많은 정보를 찾아보세요

- ["vCenter Server용 NetApp Element 플러그인"](#)
- ["SolidFire 및 Element 소프트웨어 문서"](#)

## 관리 노드 설치 또는 복구

### 관리 노드 설치

구성에 적합한 이미지를 사용하여 NetApp Element 소프트웨어를 실행하는 클러스터에 대한 관리 노드를 수동으로 설치할 수 있습니다.

이 수동 프로세스는 관리 노드 설치에 NetApp 배포 엔진을 사용하지 않는 SolidFire 올플래시 스토리지 관리자를 대상으로 합니다.

시작하기 전에

- 귀하의 클러스터 버전은 NetApp Element 소프트웨어 11.3 이상을 실행하고 있습니다.
- 귀하의 설치에는 IPv4를 사용합니다. 관리 노드 11.3은 IPv6를 지원하지 않습니다.



IPv6 지원이 필요한 경우 관리 노드 11.1을 사용할 수 있습니다.

- NetApp 지원 사이트에서 소프트웨어를 다운로드할 수 있는 권한이 있습니다.
- 플랫폼에 맞는 관리 노드 이미지 유형을 식별했습니다.

플랫폼	설치 이미지 유형
마이크로소프트 하이퍼-V	.iso
케이비엠	.iso
VMware vSphere	.iso, .ova
시트릭스 젠서버	.iso
오픈스택	.iso

- (프록시 서버가 있는 관리 노드 12.0 이상) 프록시 서버를 구성하기 전에 NetApp Hybrid Cloud Control을 관리 서비스 버전 2.16으로 업데이트했습니다.

이 작업에 관하여

Element 12.2 관리 노드는 선택적 업그레이드입니다. 기존 배포에는 필요하지 않습니다.

이 절차를 따르기 전에 다음 사항을 이해해야 합니다. "영구 볼륨" 그리고 그것을 사용할 것인지의 여부. 영구 볼륨은 선택 사항이지만 가상 머신(VM) 손실 시 관리 노드 구성 데이터 복구에 권장됩니다.

**1단계: ISO 또는 OVA를 다운로드하고 VM을 배포합니다.**

NetApp 지원 사이트에서 적절한 ISO 또는 OVA를 다운로드하여 VM을 설치합니다.

단계

1. 설치를 위해 OVA 또는 ISO를 다운로드하세요. "엘리먼트 소프트웨어" NetApp 지원 사이트의 페이지입니다.
  - a. \*최신 릴리스 다운로드\*를 선택하고 EULA에 동의하세요.
  - b. 다운로드할 관리 노드 이미지를 선택하세요.
2. OVA를 다운로드한 경우 다음 단계를 따르세요.
  - a. OVA를 배포합니다.
  - b. 스토리지 클러스터가 관리 노드(eth0)와 별도의 서브넷에 있고 영구 볼륨을 사용하려는 경우 스토리지 서브넷 (예: eth1)의 VM에 두 번째 네트워크 인터페이스 컨트롤러(NIC)를 추가하거나 관리 네트워크가 스토리지 네트워크로 라우팅될 수 있는지 확인하세요.

3. ISO를 다운로드한 경우 다음 단계를 따르세요.
  - a. 다음 구성을 사용하여 하이퍼바이저에서 새 64비트 VM을 만듭니다.
    - 6개의 가상 CPU
    - 24GB 램
    - 저장 어댑터 유형이 LSI Logic Parallel로 설정됨



관리 노드의 기본값은 LSI Logic SAS일 수 있습니다. 새 가상 머신 창에서 하드웨어 사용자 지정 > \*가상 하드웨어\*를 선택하여 스토리지 어댑터 구성을 확인합니다. 필요한 경우 LSI Logic SAS를 \*LSI Logic Parallel\*로 변경합니다.

- 400GB 가상 디스크, 썸 프로비저닝
- 인터넷 접속과 스토리지 MVIP 접속이 가능한 하나의 가상 네트워크 인터페이스.
- (선택 사항) 스토리지 클러스터에 대한 관리 네트워크 액세스가 가능한 하나의 가상 네트워크 인터페이스. 스토리지 클러스터가 관리 노드(eth0)와 별도의 서브넷에 있고 영구 볼륨을 사용하려는 경우 스토리지 서브넷(eth1)의 VM에 두 번째 네트워크 인터페이스 컨트롤러(NIC)를 추가하거나 관리 네트워크가 스토리지 네트워크로 라우팅될 수 있는지 확인하세요.



이 절차의 뒷부분에서 지시하는 단계 이전에는 VM의 전원을 켜지 마십시오.

- b. ISO를 VM에 연결하고 .iso 설치 이미지로 부팅합니다.



이미지를 사용하여 관리 노드를 설치하면 시작 화면이 나타나기 전에 30초의 지연이 발생할 수 있습니다.

4. 설치가 완료되면 관리 노드의 VM 전원을 켵니다.

**2단계: 관리 노드 관리자를 생성하고 네트워크를 구성합니다.**

VM 설치가 완료되면 관리 노드 관리자 사용자를 만들고 관리 노드 네트워크를 구성합니다.

**단계**

1. 터미널 사용자 인터페이스(TUI)를 사용하여 관리 노드 관리자 사용자를 만듭니다.



메뉴 옵션 사이를 이동하려면 위쪽 또는 아래쪽 화살표 키를 누르세요. 버튼 사이를 이동하려면 Tab 키를 누르세요. 버튼에서 필드로 이동하려면 Tab 키를 누르세요. 필드 사이를 이동하려면 위쪽 또는 아래쪽 화살표 키를 누르세요.

2. 네트워크에 최대 전송 단위(MTU)가 1500바이트 미만인 IP를 할당하는 DHCP(동적 호스트 구성 프로토콜) 서버가 있는 경우 다음 단계를 수행해야 합니다.

- a. DHCP가 없는 vSphere 네트워크(예: iSCSI)에 관리 노드를 임시로 배치합니다.
- b. VM을 재부팅하거나 VM 네트워크를 다시 시작합니다.
- c. TUI를 사용하여 관리 네트워크에서 1500바이트 이상의 MTU로 올바른 IP를 구성합니다.
- d. VM에 올바른 VM 네트워크를 다시 할당합니다.



MTU가 1500바이트 미만인 IP를 할당하는 DHCP로 인해 관리 노드 네트워크를 구성하거나 관리 노드 UI를 사용할 수 없습니다.

3. 관리 노드 네트워크(eth0)를 구성합니다.



스토리지 트래픽을 분리하기 위해 추가 NIC가 필요한 경우 다른 NIC 구성에 대한 지침을 참조하세요. ["스토리지 네트워크 인터페이스 컨트롤러\(NIC\) 구성"](#).

### 3단계: 시간 동기화 구성

관리 노드를 설정하기 전에 관리 노드와 스토리지 클러스터 간의 시간을 동기화하세요.

단계

1. NTP를 사용하여 관리 노드와 스토리지 클러스터 간의 시간이 동기화되었는지 확인하세요.



요소 12.3.1부터 하위 단계 (a)부터 (e)까지는 자동으로 수행됩니다. 관리 노드 12.3.1의 경우 다음으로 진행하세요. [하위 단계 \(f\)](#) 시간 동기화 구성을 완료합니다.

1. SSH나 하이퍼바이저가 제공하는 콘솔을 사용하여 관리 노드에 로그인합니다.

2. NTPD 중지:

```
sudo service ntpd stop
```

3. NTP 구성 파일 편집 /etc/ntp.conf :

- a. 기본 서버를 주석 처리합니다.(`server 0.gentoo.pool.ntp.org`)을 추가하여 # 각각의 앞에.
- b. 추가하려는 각 기본 시간 서버에 대해 새 줄을 추가합니다. 기본 시간 서버는 스토리지 클러스터에서 사용되는 NTP 서버와 동일해야 합니다. [나중 단계](#).

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time server>
```

c. 완료되면 구성 파일을 저장합니다.

4. 새로 추가된 서버와 NTP 동기화를 강제로 실행합니다.

```
sudo ntpd -gq
```

5. NTPD를 다시 시작합니다.

```
sudo service ntpd start
```

6. 하이퍼바이저를 통해 호스트와의 시간 동기화를 비활성화합니다(다음은 VMware 예시입니다):



예를 들어 Openstack 환경의 .iso 이미지에서와 같이 VMware가 아닌 다른 하이퍼바이저 환경에 mNode를 배포하는 경우 해당 명령에 대한 하이퍼바이저 설명서를 참조하세요.

a. 주기적 시간 동기화 비활성화:

```
vmware-toolbox-cmd timesync disable
```

b. 서비스의 현재 상태를 표시하고 확인합니다.

```
vmware-toolbox-cmd timesync status
```

c. vSphere에서 다음을 확인하십시오. Synchronize guest time with host VM 옵션에서 상자가 선택 취소되어 있습니다.



나중에 VM을 변경하는 경우 이 옵션을 활성화하지 마세요.



시간 동기화 구성을 완료한 후에는 NTP를 편집하지 마십시오. 편집하면 NTP가 실행될 때 영향을 받습니다. [설치 명령](#) 관리 노드에서.

#### 4단계: 관리 노드 설정

다음을 사용하여 관리 노드를 구성합니다. `setup-mnode` 명령.

단계

1. 관리 노드 설정 명령을 구성하고 실행합니다.



보안 프롬프트에서 비밀번호를 입력하라는 메시지가 표시됩니다. 클러스터가 프록시 서버 뒤에 있는 경우 공용 네트워크에 접속할 수 있도록 프록시 설정을 구성해야 합니다.

```
sudo /sf/packages/mnode/setup-mnode --mnode_admin_user [username]
--storage_mvip [mvip] --storage_username [username] --telemetry_active
[true]
```

a. 다음 필수 매개변수 각각에 대해 [ ] 괄호(괄호 포함) 안의 값을 바꾸세요.



명령어 이름의 약어는 괄호( )로 표시되며, 전체 이름으로 대체될 수 있습니다.

- **--mnode\_admin\_user (-mu) [사용자 이름]:** 관리 노드 관리자 계정의 사용자 이름입니다. 이는 관리 노드에 로그인하는 데 사용한 사용자 계정의 사용자 이름일 가능성이 높습니다.
- **--storage\_mvip (-sm) [MVIP 주소]:** Element 소프트웨어를 실행하는 스토리지 클러스터의 관리 가상 IP 주소(MVIP)입니다. 이전에 사용했던 것과 동일한 스토리지 클러스터로 관리 노드를 구성합니다. [NTP 서버 구성](#).
- **--storage\_username (-su) [사용자 이름]:** 지정된 클러스터에 대한 스토리지 클러스터 관리자 사용자 이름 --storage\_mvip 매개변수.
- **--telemetry\_active (-t) [true]:** Active IQ 에서 분석을 위한 데이터 수집을 활성화하는 true 값을 유지합니다.

b. (선택 사항): 명령에 Active IQ 엔드포인트 매개변수를 추가합니다.

- **--remote\_host (-rh) [AIQ\_endpoint]:** Active IQ 원격 측정 데이터가 처리되도록 전송되는 엔드포인트입니다. 매개변수가 포함되지 않으면 기본 엔드포인트가 사용됩니다.

c. (권장): 다음 영구 볼륨 매개변수를 추가합니다. 영구 볼륨 기능을 위해 생성된 계정 및 볼륨을 수정하거나 삭제하지 마십시오. 그렇지 않으면 관리 기능이 손실됩니다.

- **--use\_persistent\_volumes (-pv) [true/false, 기본값: false]:** 영구 볼륨을 활성화하거나 비활성화합니다. 영구 볼륨 기능을 활성화하려면 true 값을 입력하세요.
- **--persistent\_volumes\_account (-pva) [계정\_이름]:** 만약 --use\_persistent\_volumes true로 설정된 경우 이 매개변수를 사용하고 영구 볼륨에 사용될 스토리지 계정 이름을 입력합니다.



클러스터의 기존 계정 이름과 다른, 영구 볼륨에 고유한 계정 이름을 사용합니다. 영구 볼륨 계정을 나머지 환경과 분리해 두는 것이 매우 중요합니다.

- **--persistent\_volumes\_mvip (-pvm) [mvip]:** 영구 볼륨과 함께 사용될 Element 소프트웨어를 실행하는 스토리지 클러스터의 관리 가상 IP 주소(MVIP)를 입력합니다. 이는 관리 노드에서 여러 스토리지 클러스터를 관리하는 경우에만 필요합니다. 여러 클러스터를 관리하지 않으면 기본 클러스터 MVIP가 사용됩니다.

d. 프록시 서버를 구성하세요:

- **--use\_proxy (-up) [true/false, 기본값: false]:** 프록시 사용을 활성화하거나 비활성화합니다. 이 매개변수는 프록시 서버를 구성하는 데 필요합니다.
- **--proxy\_hostname\_or\_ip (-pi) [호스트]:** 프록시 호스트 이름 또는 IP. 프록시를 사용하려면 이 작업이 필요합니다. 이것을 지정하면 입력하라는 메시지가 표시됩니다. --proxy\_port .
- **--proxy\_username (-pu) [사용자 이름]:** 프록시 사용자 이름. 이 매개변수는 선택 사항입니다.
- **--proxy\_password (-pp) [비밀번호]:** 프록시 비밀번호. 이 매개변수는 선택 사항입니다.
- **--proxy\_port (-pq) [포트, 기본값: 0]:** 프록시 포트. 이것을 지정하면 프록시 호스트 이름이나 IP를

입력하라는 메시지가 표시됩니다.(--proxy\_hostname\_or\_ip).

- **--proxy\_ssh\_port (-ps)** [포트, 기본값: 443]: SSH 프록시 포트. 기본적으로 포트는 443입니다.

e. (선택 사항) 각 매개변수에 대한 추가 정보가 필요한 경우 매개변수 도움말을 사용하세요.

- **--help (-h)**: 각 매개변수에 대한 정보를 반환합니다. 매개변수는 초기 배포에 따라 필수 또는 선택 사항으로 정의됩니다. 업그레이드 및 재배포 매개변수 요구 사항은 다를 수 있습니다.

f. 실행하다 `setup-mnode` 명령.

## 5단계: 컨트롤러 자산 구성

설치 ID를 찾아 vCenter 컨트롤러 자산을 추가합니다.

단계

1. 설치 ID를 찾으세요.

- 브라우저에서 관리 노드 REST API UI에 로그인합니다.
- 저장소 MVIP로 이동하여 로그인합니다. 이렇게 하면 다음 단계에서 인증서가 승인됩니다.
- 관리 노드에서 인벤토리 서비스 REST API UI를 엽니다.

```
https://<ManagementNodeIP>/inventory/1/
```

- \*승인\*을 선택하고 다음을 완료하세요.
  - 클러스터 사용자 이름과 비밀번호를 입력하세요.
  - 클라이언트 ID를 다음과 같이 입력하세요. `mnode-client`.
  - 세션을 시작하려면 \*승인\*을 선택하세요.
- REST API UI에서 \*GET /installations\*를 선택합니다.
- \*시도해보기\*를 선택하세요.
- \*실행\*을 선택하세요.
- 코드 200 응답 본문에서 복사하여 저장하세요. `id` 이후 단계에서 사용하기 위한 설치용입니다.

설치에는 설치 또는 업그레이드 중에 생성된 기본 자산 구성이 있습니다.

2. NetApp Hybrid Cloud Control에 대한 vCenter 컨트롤러 자산을 관리 노드 알려진 자산에 추가합니다.

- 관리 노드에서 관리 노드 IP 주소를 입력한 다음 `mnode` 서비스 API UI에 액세스합니다. `/mnode` :

```
https://<ManagementNodeIP>/mnode
```

- 승인 또는 잠금 아이콘을 선택하고 다음을 완료하세요.
  - 클러스터 사용자 이름과 비밀번호를 입력하세요.
  - 클라이언트 ID를 다음과 같이 입력하세요. `mnode-client`.
  - 세션을 시작하려면 \*승인\*을 선택하세요.

iv. 창을 닫으세요.

c. 컨트롤러 하위 자산을 추가하려면 \*POST /assets/{asset\_id}/controllers\*를 선택하세요.



컨트롤러 하위 자산을 추가하려면 vCenter에서 새로운 NetApp HCC 역할을 만들어야 합니다. 이 새로운 NetApp HCC 역할은 관리 노드 서비스 보기를 NetApp 자산으로만 제한합니다. 보다"[vCenter에서 NetApp HCC 역할 생성](#)".

d. \*시도해보기\*를 선택하세요.

e. 클립보드에 복사한 부모 기반 자산 ID를 **asset\_id** 필드에 입력합니다.

f. 필요한 페이로드 값을 유형으로 입력하세요. vCenter 및 vCenter 자격 증명.

g. \*실행\*을 선택하세요.

더 많은 정보를 찾아보세요

- "[영구 볼륨](#)"
- "[관리 노드에 컨트롤러 자산 추가](#)"
- "[스토리지 NIC 구성](#)"
- "[vCenter Server용 NetApp Element 플러그인](#)"
- "[SolidFire 및 Element 소프트웨어 문서](#)"

## vCenter에서 NetApp HCC 역할 생성

vCenter 자산(컨트롤러)을 설치 후 관리 노드에 수동으로 추가하거나 기존 컨트롤러를 수정하려면 vCenter에서 NetApp HCC 역할을 만들어야 합니다.

이 NetApp HCC 역할은 관리 노드 서비스 보기를 NetApp 자산으로만 제한합니다.

이 작업에 관하여

- 이 절차에서는 vSphere 6.7 버전에서 사용할 수 있는 단계를 설명합니다. 설치된 vSphere 버전에 따라 vSphere 사용자 인터페이스가 설명된 내용과 약간 다를 수 있습니다. 추가 도움말은 VMware vCenter 설명서를 참조하세요.
- 예게"[새로운 NetApp HCC 역할 생성](#)" 먼저 vCenter에서 새 사용자 계정을 설정하고 NetApp HCC 역할을 만든 다음 사용자 권한을 할당합니다.
- NetApp ESXi 호스트 구성의 경우 NDE에서 생성된 사용자 계정을 새 NetApp HCC 역할로 업데이트해야 합니다.
  - 사용"[이 옵션](#)" vCenter 호스트 클러스터 내에 NetApp ESXi 호스트가 없는 경우
  - 사용"[이 옵션](#)" NetApp ESXi 호스트가 vCenter 호스트 클러스터 내에 있는 경우
- 당신은 할 수 있습니다"[컨트롤러 자산 구성](#)" 관리 노드에 이미 존재합니다.
- 새로운 NetApp HCC 역할을 사용하여"[자산 추가](#)" 관리 노드로.

## 새로운 NetApp HCC 역할 만들기

vCenter에서 새 사용자 계정을 설정하고 NetApp HCC 역할을 만든 다음 사용자 권한을 할당합니다.

## vCenter에서 새 사용자 계정 설정

vCenter에서 새 사용자 계정을 설정하려면 다음 단계를 수행하세요.

### 단계

1. vSphere Web Client에 로그인합니다. administrator@vsphere.local 또는 이에 상응하는 것.
2. 메뉴에서 \*관리\*를 선택하세요.
3. **Single Sign On** 섹션에서 \*사용자\*와 \*그룹\*을 선택합니다.
4. 도메인 목록에서 다음을 선택하세요. vsphere.local 또는 LDAP 도메인.
5. \*사용자 추가\*를 선택하세요.
6. 사용자 추가 양식을 작성하세요.

## vCenter에서 새로운 NetApp HCC 역할 생성

vCenter에서 새로운 NetApp HCC 역할을 생성하려면 다음 단계를 수행하세요.

### 단계

1. \*역할 편집\*을 선택하고 필요한 권한을 할당합니다.
2. 왼쪽 탐색 창에서 \*글로벌\*을 선택합니다.
3. \*진단\*과 \*라이선스\*를 선택하세요.
4. 왼쪽 탐색 창에서 \*호스트\*를 선택합니다.
5. 유지관리, 전원, 저장소 파티션 구성, \*펌웨어\*를 선택합니다.
6. 다른 이름으로 저장 NetApp Role .

## vCenter에 사용자 권한 할당

vCenter에서 새 NetApp HCC 역할에 사용자 권한을 할당하려면 다음 단계를 수행합니다.

### 단계

1. 메뉴에서 \*호스트\*와 \*클러스터\*를 선택합니다.
2. 왼쪽 탐색 창에서 다음 옵션 중 하나를 선택하세요.
  - 최상위 vCenter.
  - 연결 모드에 있는 경우 원하는 vCenter입니다.



- vCenter Server 5.0용 NetApp Element 플러그인을 사용하여 시작하려면 "[vCenter 연결 모드](#)" NetApp SolidFire 스토리지 클러스터를 관리하는 각 vCenter Server에 대해 별도의 관리 노드에서 Element 플러그인을 등록합니다(권장).
- vCenter Server 4.10 이하 버전용 NetApp Element 플러그인을 사용하여 다른 vCenter Server에서 클러스터 리소스를 관리합니다. "[vCenter 연결 모드](#)" 로컬 스토리지 클러스터에만 제한됩니다.

3. 오른쪽 탐색 창에서 \*권한\*을 선택합니다.
4. 새로운 사용자를 추가하려면 + 아이콘을 선택하세요.

권한 추가 창에 다음 세부 정보를 추가합니다.

- a. 선택하다 `vsphere.local` 또는 LDAP 도메인
- b. 검색을 사용하여 생성한 새 사용자를 찾으세요. [vCenter에서 새 사용자 계정 설정](#).
- c. 선택하다 NetApp Role.



\*자녀에게 전파\*를 선택하지 마십시오.

Add Permission | satyabra-vcen... X

User: vsphere.local

Q netapp

Role: NetApp Role

Propagate to children

CANCEL OK

데이터 센터에 사용자 권한 할당

vCenter에서 데이터 센터에 대한 사용자 권한을 할당하려면 다음 단계를 수행하세요.

단계

- 1. 왼쪽 창에서 \*데이터 센터\*를 선택합니다.
- 2. 오른쪽 탐색 창에서 \*권한\*을 선택합니다.
- 3. 새로운 사용자를 추가하려면 + 아이콘을 선택하세요.

권한 추가 창에 다음 세부 정보를 추가합니다.

- a. 선택하다 `vsphere.local` 또는 LDAP 도메인.
- b. 검색을 사용하여 생성한 새 HCC 사용자를 찾으세요. [vCenter에서 새 사용자 계정 설정](#).
- c. 선택하다 `ReadOnly role`.



\*자녀에게 전파\*를 선택하지 마십시오.

### NetApp HCI 데이터 저장소에 사용자 권한 할당

vCenter의 NetApp HCI 데이터 저장소에 대한 사용자 권한을 할당하려면 다음 단계를 수행하세요.

단계

1. 왼쪽 창에서 \*데이터 센터\*를 선택합니다.
2. 새로운 저장 폴더를 만듭니다. \*데이터 센터\*를 마우스 오른쪽 버튼으로 클릭하고 \*저장 폴더 만들기\*를 선택합니다.
3. 스토리지 클러스터와 로컬 컴퓨팅 노드의 모든 NetApp HCI 데이터 저장소를 새 스토리지 폴더로 전송합니다.
4. 새로운 저장 폴더를 선택하세요.
5. 오른쪽 탐색 창에서 \*권한\*을 선택합니다.
6. 새로운 사용자를 추가하려면 + 아이콘을 선택하세요.

권한 추가 창에 다음 세부 정보를 추가합니다.

- a. 선택하다 `vsphere.local` 또는 LDAP 도메인.
- b. 검색을 사용하여 생성한 새 HCC 사용자를 찾으세요. [vCenter에서 새 사용자 계정 설정](#) .
- c. 선택하다 Administrator role
- d. \*자녀에게 전파\*를 선택하세요.

### NetApp 호스트 클러스터에 사용자 권한 할당

vCenter에서 NetApp 호스트 클러스터에 대한 사용자 권한을 할당하려면 다음 단계를 수행합니다.

단계

1. 왼쪽 탐색 창에서 NetApp 호스트 클러스터를 선택합니다.
2. 오른쪽 탐색 창에서 \*권한\*을 선택합니다.
3. 새로운 사용자를 추가하려면 + 아이콘을 선택하세요.

권한 추가 창에 다음 세부 정보를 추가합니다.

- a. 선택하다 `vsphere.local` 또는 LDAP 도메인.
- b. 검색을 사용하여 생성한 새 HCC 사용자를 찾으세요. [vCenter에서 새 사용자 계정 설정](#) .
- c. 선택하다 NetApp Role 또는 Administrator .
- d. \*자녀에게 전파\*를 선택하세요.

### NetApp ESXi 호스트 구성

NetApp ESXi 호스트 구성의 경우 NDE에서 생성된 사용자 계정을 새 NetApp HCC 역할로 업데이트해야 합니다.

vCenter 호스트 클러스터에 NetApp ESXi 호스트가 없습니다.

NetApp ESXi 호스트가 vCenter 호스트 클러스터 내에 없는 경우 다음 절차를 사용하여 vCenter에서 NetApp HCC 역할과 사용자 권한을 할당할 수 있습니다.

단계

1. 메뉴에서 \*호스트\*와 \*클러스터\*를 선택합니다.
2. 왼쪽 탐색 창에서 NetApp ESXi 호스트를 선택합니다.
3. 오른쪽 탐색 창에서 \*권한\*을 선택합니다.
4. 새로운 사용자를 추가하려면 + 아이콘을 선택하세요.

권한 추가 창에 다음 세부 정보를 추가합니다.

- a. 선택하다 vsphere.local 또는 LDAP 도메인.
  - b. 검색을 사용하여 생성한 새 사용자를 찾으세요.vCenter에서 새 사용자 계정 설정 .
  - c. 선택하다 NetApp Role 또는 Administrator .
5. \*자녀에게 전파\*를 선택하세요.

NetApp ESXi 호스트가 vCenter 호스트 클러스터에 있습니다.

NetApp ESXi 호스트가 다른 공급업체 ESXi 호스트와 함께 vCenter 호스트 클러스터 내에 있는 경우, 다음 절차를 사용하여 vCenter에서 NetApp HCC 역할과 사용자 권한을 할당할 수 있습니다.

1. 메뉴에서 \*호스트\*와 \*클러스터\*를 선택합니다.
2. 왼쪽 탐색 창에서 원하는 호스트 클러스터를 확장합니다.
3. 오른쪽 탐색 창에서 \*권한\*을 선택합니다.
4. 새로운 사용자를 추가하려면 + 아이콘을 선택하세요.

권한 추가 창에 다음 세부 정보를 추가합니다.

- a. 선택하다 vsphere.local 또는 LDAP 도메인.
- b. 검색을 사용하여 생성한 새 사용자를 찾으세요.vCenter에서 새 사용자 계정 설정 .
- c. 선택하다 NetApp Role .



\*자녀에게 전파\*를 선택하지 마십시오.

5. 왼쪽 탐색 창에서 NetApp ESXi 호스트를 선택합니다.
6. 오른쪽 탐색 창에서 \*권한\*을 선택합니다.
7. 새로운 사용자를 추가하려면 + 아이콘을 선택하세요.

권한 추가 창에 다음 세부 정보를 추가합니다.

- a. 선택하다 vsphere.local 또는 LDAP 도메인.
- b. 검색을 사용하여 생성한 새 사용자를 찾으세요.vCenter에서 새 사용자 계정 설정 .

c. 선택하다 NetApp Role 또는 Administrator .

d. \*자녀에게 전파\*를 선택하세요.

8. 호스트 클러스터의 나머지 NetApp ESXi 호스트에 대해 반복합니다.

컨트롤러 자산이 관리 노드에 이미 존재합니다.

관리 노드에 컨트롤러 자산이 이미 있는 경우 다음 단계를 수행하여 컨트롤러를 구성합니다. PUT /assets /{asset\_id} /controllers /{controller\_id} .

단계

1. 관리 노드에서 mnode 서비스 API UI에 액세스합니다.

<https://<ManagementNodeIP>/mnode>

2. \*인증\*을 선택하고 API 호출에 액세스하기 위한 자격 증명을 입력합니다.

3. 선택하다 GET /assets 부모 ID를 받으세요.

4. 선택하다 PUT /assets /{asset\_id} /controllers /{controller\_id} .

a. 계정 설정에서 생성된 자격 증명을 요청 본문에 입력하세요.

관리 노드에 자산 추가

설치 후 새 자산을 수동으로 추가해야 하는 경우 HCC에서 만든 새 사용자 계정을 사용하세요.vCenter에서 새 사용자 계정 설정 . 자세한 내용은 다음을 참조하세요. "[관리 노드에 컨트롤러 자산 추가](#)".

더 많은 정보를 찾아보세요

- "[vCenter Server용 NetApp Element 플러그인](#)"
- "[SolidFire 및 Element 소프트웨어 문서](#)"

## 스토리지 네트워크 인터페이스 컨트롤러(NIC) 구성

스토리지용으로 추가 NIC를 사용하는 경우 관리 노드에 SSH를 통해 접속하거나 vCenter 콘솔을 사용하여 curl 명령을 실행하여 태그가 지정되거나 지정되지 않은 네트워크 인터페이스를 설정할 수 있습니다.

시작하기 전에

- eth0 IP 주소를 알고 계시죠.
- 귀하의 클러스터 버전은 NetApp Element 소프트웨어 11.3 이상을 실행하고 있습니다.
- 관리 노드 11.3 이상을 배포했습니다.

구성 옵션

귀하의 환경에 적합한 옵션을 선택하세요.

- [태그가 지정되지 않은 네트워크 인터페이스에 대한 스토리지 네트워크 인터페이스 컨트롤러\(NIC\) 구성](#)
- [태그가 지정된 네트워크 인터페이스에 대한 스토리지 네트워크 인터페이스 컨트롤러\(NIC\) 구성](#)

## 태그가 지정되지 않은 네트워크 인터페이스에 대한 스토리지 네트워크 인터페이스 컨트롤러(NIC) 구성

### 단계

1. SSH 또는 vCenter 콘솔을 엽니다.
2. 다음 명령 템플릿의 값을 바꾸고 명령을 실행합니다.



값은 다음으로 표현됩니다. \$ 새로운 스토리지 네트워크 인터페이스에 필요한 각 매개변수에 대해. 그만큼 cluster 다음 템플릿의 객체는 필수이며 관리 노드 호스트 이름 변경에 사용할 수 있습니다. --insecure 또는 -k 옵션은 프로덕션 환경에서 사용하면 안 됩니다.

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
  "params": {
    "network": {
      "$eth1": {
        "#default" : false,
        "address" : "$storage_IP",
        "auto" : true,
        "family" : "inet",
        "method" : "static",
        "mtu" : "9000",
        "netmask" : "$subnet_mask",
        "status" : "Up"
      }
    },
    "cluster": {
      "name": "$mnode_host_name"
    }
  },
  "method": "SetConfig"
}
```

## 태그가 지정된 네트워크 인터페이스에 대한 스토리지 네트워크 인터페이스 컨트롤러(NIC) 구성

### 단계

1. SSH 또는 vCenter 콘솔을 엽니다.
2. 다음 명령 템플릿의 값을 바꾸고 명령을 실행합니다.



값은 다음으로 표현됩니다. \$ 새로운 스토리지 네트워크 인터페이스에 필요한 각 매개변수에 대해. 그만큼 cluster 다음 템플릿의 객체는 필수이며 관리 노드 호스트 이름 변경에 사용할 수 있습니다. --insecure 또는 -k 옵션은 프로덕션 환경에서 사용하면 안 됩니다.

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
    "params": {
        "network": {
            "$eth1": {
                "#default" : false,
                "address" : "$storage_IP",
                "auto" : true,
                "family" : "inet",
                "method" : "static",
                "mtu" : "9000",
                "netmask" : "$subnet_mask",
                "status" : "Up",
                "virtualNetworkTag" : "$vlan_id"
            }
        },
        "cluster": {
            "name": "$mnode_host_name",
            "cipi": "$eth1.$vlan_id",
            "sipi": "$eth1.$vlan_id"
        }
    },
    "method": "SetConfig"
}
```

더 많은 정보를 찾아보세요

- ["관리 노드에 컨트롤러 자산 추가"](#)
- ["vCenter Server용 NetApp Element 플러그인"](#)
- ["SolidFire 및 Element 소프트웨어 문서"](#)

## 관리 노드 복구

이전 관리 노드에서 영구 볼륨을 사용한 경우 NetApp Element 소프트웨어를 실행하는 클러스터의 관리 노드를 수동으로 복구하고 다시 배포할 수 있습니다.

새로운 OVA를 배포하고 재배포 스크립트를 실행하여 버전 11.3 이상을 실행하는 이전에 설치된 관리 노드에서 구성 데이터를 가져올 수 있습니다.

#### 필요한 것

- 이전 관리 노드는 NetApp Element 소프트웨어 버전 11.3 이상을 실행하고 있었습니다."영구 볼륨" 기능이 활성화되었습니다.
- 영구 볼륨이 포함된 클러스터의 MVIP와 SVIP를 알고 있습니다.
- 귀하의 클러스터 버전은 NetApp Element 소프트웨어 11.3 이상을 실행하고 있습니다.
- 귀하의 설치에 IPv4를 사용합니다. 관리 노드 11.3은 IPv6를 지원하지 않습니다.
- NetApp 지원 사이트에서 소프트웨어를 다운로드할 수 있는 권한이 있습니다.
- 플랫폼에 맞는 관리 노드 이미지 유형을 식별했습니다.

플랫폼	설치 이미지 유형
마이크로소프트 하이퍼-V	.iso
케이비엠	.iso
VMware vSphere	.iso, .ova
시트릭스 젠서버	.iso
오픈스택	.iso

#### 단계

1. ISO 또는 OVA를 다운로드하고 VM을 배포합니다.
2. 네트워크 구성
3. 시간 동기화 구성
4. 관리 노드 구성

#### ISO 또는 OVA를 다운로드하고 VM을 배포합니다.

1. 설치에 필요한 OVA 또는 ISO를 다운로드하세요. "엘리먼트 소프트웨어" NetApp 지원 사이트의 페이지입니다.
  - a. \*최신 릴리스 다운로드\*를 선택하고 EULA에 동의하세요.
  - b. 다운로드할 관리 노드 이미지를 선택하세요.
2. OVA를 다운로드한 경우 다음 단계를 따르세요.
  - a. OVA를 배포합니다.
  - b. 스토리지 클러스터가 관리 노드(eth0)와 별도의 서브넷에 있고 영구 볼륨을 사용하려는 경우 스토리지 서브넷 (예: eth1)의 VM에 두 번째 네트워크 인터페이스 컨트롤러(NIC)를 추가하거나 관리 네트워크가 스토리지 네트워크로 라우팅될 수 있는지 확인하세요.
3. ISO를 다운로드한 경우 다음 단계를 따르세요.
  - a. 다음 구성을 사용하여 하이퍼바이저에서 새로운 64비트 가상 머신을 만듭니다.
    - 6개의 가상 CPU
    - 24GB 램

- 400GB 가상 디스크, 씬 프로비저닝
- 인터넷 접속과 스토리지 MVIP 접속이 가능한 하나의 가상 네트워크 인터페이스.
- ( SolidFire 올플래시 스토리지의 경우 선택 사항) 스토리지 클러스터에 대한 관리 네트워크 액세스를 제공하는 하나의 가상 네트워크 인터페이스입니다. 스토리지 클러스터가 관리 노드(eth0)와 별도의 서브넷에 있고 영구 볼륨을 사용하려는 경우 스토리지 서브넷(eth1)의 VM에 두 번째 네트워크 인터페이스 컨트롤러(NIC)를 추가하거나 관리 네트워크가 스토리지 네트워크로 라우팅될 수 있는지 확인하세요.



이 절차의 뒷부분에서 언급된 단계 이전에는 가상 머신의 전원을 켜지 마십시오.

b. ISO를 가상 머신에 연결하고 .iso 설치 이미지로 부팅합니다.



이미지를 사용하여 관리 노드를 설치하면 시작 화면이 나타나기 전에 30초의 지연이 발생할 수 있습니다.

4. 설치가 완료되면 관리 노드의 가상 머신의 전원을 켵니다.

## 네트워크 구성

1. 터미널 사용자 인터페이스(TUI)를 사용하여 관리 노드 관리자 사용자를 만듭니다.



메뉴 옵션 사이를 이동하려면 위쪽 또는 아래쪽 화살표 키를 누르세요. 버튼 사이를 이동하려면 Tab 키를 누르세요. 버튼에서 필드로 이동하려면 Tab 키를 누르세요. 필드 사이를 이동하려면 위쪽 또는 아래쪽 화살표 키를 누르세요.

2. 관리 노드 네트워크(eth0)를 구성합니다.



스토리지 트래픽을 분리하기 위해 추가 NIC가 필요한 경우 다른 NIC 구성에 대한 지침을 참조하세요. ["스토리지 네트워크 인터페이스 컨트롤러\(NIC\) 구성"](#).

## 시간 동기화 구성

1. NTP를 사용하여 관리 노드와 스토리지 클러스터 간의 시간이 동기화되었는지 확인하세요.



요소 12.3.1부터 하위 단계 (a)부터 (e)까지는 자동으로 수행됩니다. 관리 노드 12.3.1 이상의 경우 다음으로 진행하세요. [하위 단계 \(f\)](#) 시간 동기화 구성을 완료합니다.

1. SSH나 하이퍼바이저가 제공하는 콘솔을 사용하여 관리 노드에 로그인합니다.

2. NTPD 중지:

```
sudo service ntpd stop
```

3. NTP 구성 파일 편집 /etc/ntp.conf :

- 기본 서버를 주석 처리합니다.(server 0.gentoo.pool.ntp.org)을 추가하여 # 각각의 앞에.
- 추가하려는 각 기본 시간 서버에 대해 새 줄을 추가합니다. 기본 시간 서버는 스토리지 클러스터에서 사용되는 NTP 서버와 동일해야 합니다. ["나중 단계"](#).

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time server>
```

c. 완료되면 구성 파일을 저장합니다.

4. 새로 추가된 서버와 NTP 동기화를 강제로 실행합니다.

```
sudo ntpd -gq
```

5. NTPD를 다시 시작합니다.

```
sudo service ntpd start
```

6. 하이퍼바이저를 통해 호스트와의 시간 동기화를 비활성화합니다(다음은 VMware 예시입니다).



예를 들어 Openstack 환경의 .iso 이미지에서와 같이 VMware가 아닌 다른 하이퍼바이저 환경에 mNode를 배포하는 경우 해당 명령에 대한 하이퍼바이저 설명서를 참조하세요.

a. 주기적 시간 동기화 비활성화:

```
vmware-toolbox-cmd timesync disable
```

b. 서비스의 현재 상태를 표시하고 확인합니다.

```
vmware-toolbox-cmd timesync status
```

c. vSphere에서 다음을 확인하십시오. Synchronize guest time with host VM 옵션에서 상자가 선택 취소되어 있습니다.



나중에 VM을 변경하는 경우 이 옵션을 활성화하지 마세요.



시간 동기화 구성을 완료한 후에는 NTP를 편집하지 마십시오. 편집하면 NTP가 실행될 때 영향을 받습니다. [재배포 명령](#) 관리 노드에서.

## 관리 노드 구성

1. 관리 서비스 번들 콘텐츠에 대한 임시 대상 디렉토리를 만듭니다.

```
mkdir -p /sf/etc/mnode/mnode-archive
```

2. 기존 관리 노드에 이전에 설치된 관리 서비스 번들(버전 2.15.28 이상)을 다운로드하여 저장합니다.  
/sf/etc/mnode/ 예배 규칙서.
3. 다음 명령을 사용하여 다운로드한 번들을 추출하고 [ ] 괄호(괄호 포함) 안의 값을 번들 파일의 이름으로 바꿉니다.

```
tar -C /sf/etc/mnode -xvf /sf/etc/mnode/[management services bundle file]
```

4. 결과 파일을 추출합니다. /sf/etc/mnode-archive 예배 규칙서:

```
tar -C /sf/etc/mnode/mnode-archive -xvf /sf/etc/mnode/services_deploy_bundle.tar.gz
```

5. 계정 및 볼륨에 대한 구성 파일을 만듭니다.

```
echo '{"trident": true, "mvip": "[mvip IP address]", "account_name": "[persistent volume account name]"}' | sudo tee /sf/etc/mnode/mnode-archive/management-services-metadata.json
```

- a. 다음 필수 매개변수 각각에 대해 [ ] 괄호(괄호 포함) 안의 값을 바꾸세요.

- **[mvip IP 주소]:** 스토리지 클러스터의 관리 가상 IP 주소입니다. 이전에 사용했던 것과 동일한 스토리지 클러스터로 관리 노드를 구성합니다. ["NTP 서버 구성"](#).
- **[영구 볼륨 계정 이름]:** 이 스토리지 클러스터의 모든 영구 볼륨과 연결된 계정의 이름입니다.

1. 클러스터에 호스팅된 영구 볼륨에 연결하고 이전 관리 노드 구성 데이터로 서비스를 시작하려면 관리 노드 재배포 명령을 구성하고 실행하세요.



보안 프롬프트에서 비밀번호를 입력하라는 메시지가 표시됩니다. 클러스터가 프록시 서버 뒤에 있는 경우 공용 네트워크에 접속할 수 있도록 프록시 설정을 구성해야 합니다.

```
sudo /sf/packages/mnode/redeploy-mnode --mnode_admin_user [username]
```

- a. [ ] 괄호(괄호 포함) 안의 값을 관리 노드 관리자 계정의 사용자 이름으로 바꾸세요. 이는 관리 노드에 로그인하는데 사용한 사용자 계정의 사용자 이름일 가능성이 높습니다.



사용자 이름을 추가하거나 스크립트에서 정보를 입력하라는 메시지를 표시하도록 할 수 있습니다.

- b. 실행하다 `redeploy-mnode` 명령. 재배포가 완료되면 스크립트는 성공 메시지를 표시합니다.
- c. 시스템의 FQDN(정규화된 도메인 이름)을 사용하여 Element 웹 인터페이스(관리 노드 또는 NetApp Hybrid Cloud Control 등에 액세스하는 경우 "[관리 노드에 대한 인증을 재구성합니다.](#)").



제공하는 SSH 기능 "[NetApp 지원 원격 지원 터널\(RST\) 세션 액세스](#)" 관리 서비스 2.18 이상을 실행하는 관리 노드에서는 기본적으로 비활성화됩니다. 이전에 관리 노드에서 SSH 기능을 활성화한 경우 다음이 필요할 수 있습니다. "[SSH를 다시 비활성화하세요](#)" 복구된 관리 노드에서.

더 많은 정보를 찾아보세요

- "[영구 볼륨](#)"
- "[vCenter Server용 NetApp Element 플러그인](#)"
- "[SolidFire 및 Element 소프트웨어 문서](#)"

## 관리 노드에 접근

NetApp Element 소프트웨어 버전 11.3부터 관리 노드에는 두 개의 UI가 포함됩니다. REST 기반 서비스를 관리하는 UI와 네트워크 및 클러스터 설정, 운영 체제 테스트 및 유틸리티를 관리하는 노드별 UI입니다.

Element 소프트웨어 버전 11.3 이상을 실행하는 클러스터의 경우 다음 두 인터페이스 중 하나를 사용할 수 있습니다.

- 관리 노드 UI를 사용하여([https:// \[mNode IP\]:442](https://[mNode IP]:442)), 네트워크 및 클러스터 설정을 변경하고, 시스템 테스트를 실행하거나 시스템 유틸리티를 사용할 수 있습니다.
- 내장된 REST API UI를 사용하여([https://\[mNode IP\]/mnode](https://[mNode IP]/mnode)), 프록시 서버 구성, 서비스 수준 업데이트 또는 자산 관리를 포함하여 관리 노드 서비스와 관련된 API를 실행하거나 이해할 수 있습니다.

### 관리 노드별 UI에 액세스

노드별 UI에서 네트워크 및 클러스터 설정에 액세스하고 시스템 테스트와 유틸리티를 활용할 수 있습니다.

단계

1. 관리 노드의 노드별 UI에 액세스하려면 관리 노드 IP 주소 다음에 :442를 입력합니다.

```
https://[IP address]:442
```

Management

### Network Settings - Management

Method :

Link Speed :

IPv4 Address :

IPv4 Subnet Mask :

IPv4 Gateway Address :

IPv6 Address :

IPv6 Gateway Address :

MTU :

DNS Servers :

Search Domains :

Status :  ▼

**Routes**

2. 메시지가 표시되면 관리 노드 사용자 이름과 비밀번호를 입력하세요.

관리 노드 **REST API UI**에 액세스합니다.

REST API UI에서 관리 노드의 관리 서비스를 제어하는 서비스 관련 API 메뉴에 액세스할 수 있습니다.

단계

1. 관리 서비스에 대한 REST API UI에 액세스하려면 관리 노드 IP 주소를 입력한 다음 다음을 입력하십시오. /mnode :

```
https://[IP address]/mnode
```

# MANAGEMENT SERVICES API<sup>1.0</sup>

[ Base URL: /mnode ]  
https://10.117.1.100/mnode/swagger/json

The configuration REST service for MANAGEMENT SERVICES

NetApp - Website

NetApp Commercial Software License

Authorize 

## logs Log service

GET /logs Get logs from the MNODE service(s)

## assets Asset service

POST /assets Add a new asset

GET /assets Get all assets

GET /assets/compute-nodes Get all compute nodes

GET /assets/compute-nodes/{compute\_node\_id} Get a specific compute node by ID

GET /assets/controllers Get all controllers

GET /assets/controllers/{controller\_id} Get a specific controller by ID

GET /assets/storage-clusters Get all storage clusters

GET /assets/storage-clusters/{storage\_cluster\_id} Get a specific storage cluster by ID

PUT /assets/{asset\_id} Modify an asset with a specific ID

DELETE /assets/{asset\_id} Delete an asset with a specific ID

GET /assets/{asset\_id} Get an asset by it's ID

POST /assets/{asset\_id}/compute-nodes Add a compute asset

GET /assets/{asset\_id}/compute-nodes Get compute assets

PUT /assets/{asset\_id}/compute-nodes/{compute\_id} Update a specific compute node asset

DELETE /assets/{asset\_id}/compute-nodes/{compute\_id} Delete a specific compute node asset

2. 인증 또는 잠금 아이콘을 선택하고 API 사용 권한을 위한 클러스터 관리자 자격 증명을 입력합니다.

더 많은 정보를 찾아보세요

- ["Active IQ 및 NetApp 모니터링 활성화"](#)
- ["vCenter Server용 NetApp Element 플러그인"](#)
- ["SolidFire 및 Element 소프트웨어 문서"](#)

## 관리 노드 기본 SSL 인증서 변경

NetApp Element API를 사용하여 관리 노드의 기본 SSL 인증서와 개인 키를 변경할 수 있습니다.

관리 노드를 구성하면 Element UI, 노드별 UI 또는 API를 통한 모든 HTTPS 통신에 사용되는 고유한 자체 서명 SSL(Secure Sockets Layer) 인증서와 개인 키가 생성됩니다. Element 소프트웨어는 자체 서명 인증서는 물론 신뢰할

수 있는 인증 기관(CA)에서 발급하고 검증한 인증서도 지원합니다.

다음 API 메서드를 사용하면 기본 SSL 인증서에 대한 자세한 정보를 얻고 변경할 수 있습니다.

- **노드SSL인증서 가져오기**

당신은 사용할 수 있습니다"[GetNodeSSLCertificate 메서드](#)" 모든 인증서 세부 정보를 포함하여 현재 설치된 SSL 인증서에 대한 정보를 검색합니다.

- **SetNodeSSLCertificate**

당신은 사용할 수 있습니다"[SetNodeSSLCertificate 메서드](#)" 클러스터 및 노드별 SSL 인증서를 사용자가 제공한 인증서와 개인 키로 설정합니다. 시스템은 잘못된 인증서가 적용되는 것을 방지하기 위해 인증서와 개인 키를 검증합니다.

- **노드SSL인증서 제거**

이것"[RemoveNodeSSLCertificate 메서드](#)" 현재 설치된 SSL 인증서와 개인 키를 제거합니다. 그러면 클러스터는 새로운 자체 서명 인증서와 개인 키를 생성합니다.

더 많은 정보를 찾아보세요

- "[Element 소프트웨어 기본 SSL 인증서 변경](#)"
- "[Element Software에서 사용자 정의 SSL 인증서를 설정하는 데 필요한 요구 사항은 무엇입니까?](#)"
- "[SolidFire 및 Element 소프트웨어 문서](#)"
- "[vCenter Server용 NetApp Element 플러그인](#)"

## 관리 노드 UI 작업

관리 노드 UI 개요

관리 노드 UI를 사용하여(<https://<ManagementNodeIP>:442>), 네트워크 및 클러스터 설정을 변경하고, 시스템 테스트를 실행하거나 시스템 유틸리티를 사용할 수 있습니다.

관리 노드 UI로 수행할 수 있는 작업:

- "[알림 모니터링 구성](#)"
- "[관리 노드 네트워크, 클러스터 및 시스템 설정을 수정하고 테스트합니다.](#)"
- "[관리 노드에서 시스템 유틸리티 실행](#)"

더 많은 정보를 찾아보세요

- "[관리 노드에 접근](#)"
- "[vCenter Server용 NetApp Element 플러그인](#)"
- "[SolidFire 및 Element 소프트웨어 문서](#)"

## 알림 모니터링 구성

알림 모니터링 도구는 NetApp HCI 알림 모니터링을 위해 구성됩니다. 이러한 도구는 SolidFire 올플래시 스토리지에 대해 구성되거나 사용되지 않습니다. 이러한 클러스터에 대한 도구를 실행하면 다음과 같은 405 오류가 발생합니다. 이는 구성을 고려할 때 예상되는 오류입니다.

```
webUIParseError : Invalid response from server. 405
```

NetApp HCI 에 대한 알림 모니터링 구성에 대한 자세한 내용은 다음을 참조하세요. "[알림 모니터링 구성](#)"

관리 노드 네트워크, 클러스터 및 시스템 설정을 수정하고 테스트합니다.

관리 노드 네트워크, 클러스터 및 시스템 설정을 수정하고 테스트할 수 있습니다.

- [관리 노드 네트워크 설정 업데이트](#)
- [관리 노드 클러스터 설정 업데이트](#)
- [관리 노드 설정 테스트](#)

### 관리 노드 네트워크 설정 업데이트

노드별 관리 노드 UI의 네트워크 설정 탭에서 관리 노드 네트워크 인터페이스 필드를 수정할 수 있습니다.

1. 노드별 관리 노드 UI를 엽니다.
2. 네트워크 설정 탭을 선택합니다.
3. 다음 정보를 보거나 입력하세요.
  - a. 방법: 다음 방법 중 하나를 선택하여 인터페이스를 구성합니다.
    - **loopback**: IPv4 루프백 인터페이스를 정의하는 데 사용됩니다.
    - **manual**: 기본적으로 구성이 수행되지 않는 인터페이스를 정의하는 데 사용됩니다.
    - **dhop**: DHCP를 통해 IP 주소를 얻는 데 사용됩니다.
    - **static**: 정적으로 할당된 IPv4 주소로 이더넷 인터페이스를 정의하는 데 사용됩니다.
  - b. 링크 속도: 가상 NIC에서 협상되는 속도입니다.
  - c. **IPv4** 주소: eth0 네트워크의 IPv4 주소입니다.
  - d. **IPv4** 서브넷 마스크: IPv4 네트워크의 하위 구분을 나타냅니다.
  - e. **IPv4** 게이트웨이 주소: 로컬 네트워크에서 패킷을 전송하는 라우터 네트워크 주소입니다.
  - f. **IPv6** 주소: eth0 네트워크의 IPv6 주소입니다.
  - g. **IPv6** 게이트웨이 주소: 로컬 네트워크에서 패킷을 전송하는 라우터 네트워크 주소입니다.



IPv6 옵션은 11.3 이상 버전의 관리 노드에서는 지원되지 않습니다.

- h. **MTU**: 네트워크 프로토콜이 전송할 수 있는 최대 패킷 크기. 1500 이상이어야 합니다. 두 번째 스토리지 NIC를 추가하는 경우 값은 9000이어야 합니다.
- i. **DNS** 서버: 클러스터 통신에 사용되는 네트워크 인터페이스입니다.

j. 도메인 검색: 시스템에서 사용 가능한 추가 MAC 주소를 검색합니다.

k. 상태: 가능한 값:

- UpAndRunning
- Down
- Up

l. 경로: 경로가 사용하도록 구성된 관련 인터페이스를 통해 특정 호스트 또는 네트워크에 대한 정적 경로입니다.

#### 관리 노드 클러스터 설정 업데이트

관리 노드의 노드별 UI에 있는 클러스터 설정 탭에서 노드가 사용 가능, 보류 중, 보류 중 활성화 및 활성화 상태일 때 클러스터 인터페이스 필드를 수정할 수 있습니다.

1. 노드별 관리 노드 UI를 엽니다.
2. 클러스터 설정 탭을 선택합니다.
3. 다음 정보를 보거나 입력하세요.
  - 역할: 클러스터에서 관리 노드가 갖는 역할입니다. 가능한 값: Management .
  - 버전: 클러스터에서 실행되는 요소 소프트웨어 버전입니다.
  - 기본 인터페이스: Element 소프트웨어를 실행하는 클러스터와 관리 노드 통신에 사용되는 기본 네트워크 인터페이스입니다.

#### 관리 노드 설정 테스트

관리 노드에 대한 관리 및 네트워크 설정을 변경하고 변경 사항을 커밋한 후에는 테스트를 실행하여 변경 사항을 검증할 수 있습니다.

1. 노드별 관리 노드 UI를 엽니다.
2. 관리 노드 UI에서 \*시스템 테스트\*를 선택합니다.
3. 다음 중 하나를 완료하세요.
  - a. 구성된 네트워크 설정이 시스템에 유효한지 확인하려면 \*네트워크 구성 테스트\*를 선택하세요.
  - b. ICMP 패킷을 사용하여 1G 및 10G 인터페이스에서 클러스터의 모든 노드에 대한 네트워크 연결을 테스트하려면 \*Ping 테스트\*를 선택합니다.
4. 다음을 보거나 입력하세요:
  - 호스트: ping을 실행할 장치의 주소나 호스트 이름을 심표로 구분하여 지정합니다.
  - 시도: 시스템이 테스트 ping을 반복해야 하는 횟수를 지정합니다. 기본값: 5.
  - 패킷 크기: 각 IP로 전송되는 ICMP 패킷에 포함할 바이트 수를 지정합니다. 바이트 수는 네트워크 구성에 지정된 최대 MTU보다 작아야 합니다.
  - 시간 초과(mSec): 각 개별 ping 응답을 기다리는 시간(밀리초)을 지정합니다. 기본값: 500ms.
  - 총 시간 초과 초: 다음 ping 시도를 하거나 프로세스를 종료하기 전에 ping이 시스템 응답을 기다려야 하는 시간(초)을 지정합니다. 기본값: 5.
  - 분할 금지: ICMP 패킷에 대해 DF(분할 금지) 플래그를 활성화합니다.

더 많은 정보를 찾아보세요

- ["vCenter Server용 NetApp Element 플러그인"](#)
- ["SolidFire 및 Element 소프트웨어 문서"](#)

## 관리 노드에서 시스템 유틸리티 실행

관리 노드의 노드별 UI를 사용하여 클러스터 지원 번들을 생성하거나 삭제하고, 노드 구성 설정을 재설정하거나 네트워크를 다시 시작할 수 있습니다.

단계

1. 관리 노드 관리자 자격 증명을 사용하여 노드별 관리 노드 UI를 엽니다.
2. \*시스템 유틸리티\*를 선택하세요.
3. 실행하려는 유틸리티의 버튼을 선택하세요.
  - a. 전원 제어: 노드를 재부팅, 전원 주기 또는 종료합니다. 다음 옵션 중 하나를 지정하세요.



이 작업으로 인해 네트워크 연결이 일시적으로 끊어집니다.

- 작업: 옵션은 다음과 같습니다. Restart 그리고 Halt (전원 끄기).
  - 웨이크업 지연: 노드가 다시 온라인 상태가 되기 전까지의 추가 시간입니다.
- b. 클러스터 지원 번들 생성: 클러스터의 하나 이상의 노드에 대한 NetApp 지원 진단 평가를 지원하기 위해 클러스터 지원 번들을 생성합니다. 다음 옵션을 지정하세요.
    - 번들 이름: 생성된 각 지원 번들에 대한 고유한 이름입니다. 이름이 제공되지 않으면 "supportbundle"과 노드 이름이 파일 이름으로 사용됩니다.
    - **Mvip**: 클러스터의 MVIP입니다. 번들은 클러스터의 모든 노드에서 수집됩니다. Nodes 매개변수가 지정되지 않은 경우 이 매개변수가 필요합니다.
    - 노드: 번들을 수집할 노드의 IP 주소입니다. 번들을 수집할 노드를 지정하려면 Nodes 또는 Mvip 중 하나만 사용하지만, 둘 다 사용하지는 마세요. Mvip가 지정되지 않은 경우 이 매개변수가 필요합니다.
    - 사용자 이름: 클러스터 관리자 사용자 이름입니다.
    - 비밀번호: 클러스터 관리자 비밀번호입니다.
    - 미완료 허용: 하나 이상의 노드에서 번들을 수집할 수 없는 경우 스크립트가 계속 실행되도록 허용합니다.
    - 추가 인수: 이 매개변수는 다음에 공급됩니다. sf\_make\_support\_bundle 스크립트. 이 매개변수는 NetApp 지원팀의 요청에 의해서만 사용되어야 합니다.
  - c. 모든 지원 번들 삭제: 관리 노드에 있는 현재 지원 번들을 모두 삭제합니다.
  - d. 노드 재설정: 관리 노드를 새 설치 이미지로 재설정합니다. 이렇게 하면 네트워크 구성을 제외한 모든 설정이 기본 상태로 변경됩니다. 다음 옵션을 지정하세요.
    - 빌드: 노드가 재설정될 원격 Element 소프트웨어 이미지의 URL입니다.
    - 옵션: 재설정 작업을 실행하기 위한 사양입니다. 자세한 내용은 필요한 경우 NetApp 지원팀에서 제공해 드립니다.



이 작업으로 인해 네트워크 연결이 일시적으로 끊어집니다.

e. 네트워킹 재시작: 관리 노드에서 모든 네트워크 서비스를 재시작합니다.



이 작업으로 인해 네트워크 연결이 일시적으로 끊어집니다.

더 많은 정보를 찾아보세요

- "vCenter Server용 NetApp Element 플러그인"
- "SolidFire 및 Element 소프트웨어 문서"

## 관리 노드 REST API로 작업

### 관리 노드 REST API UI 개요

내장된 REST API UI를 사용하여(<https://<ManagementNodeIP>/mnode>), 프록시 서버 구성, 서비스 수준 업데이트 또는 자산 관리를 포함하여 관리 노드 서비스와 관련된 API를 실행하거나 이해할 수 있습니다.

REST API로 수행할 수 있는 작업:

#### 권한 부여

- "REST API 사용 권한 얻기"

#### 자산 구성

- "Active IQ 및 NetApp 모니터링 활성화"
- "관리 노드에 대한 프록시 서버 구성"
- "여러 vCenter에 대한 NetApp Hybrid Cloud Control 구성"
- "관리 노드에 컨트롤러 자산 추가"
- "스토리지 클러스터 자산 생성 및 관리"

#### 자산 관리

- "기존 컨트롤러 자산 보기 또는 편집"
- "스토리지 클러스터 자산 생성 및 관리"
- "REST API를 사용하여 Element 시스템 로그를 수집합니다."
- "관리 노드 OS 및 서비스 버전 확인"
- "관리 서비스에서 로그 가져오기"

더 많은 정보를 찾아보세요

- "관리 노드에 접근"
- "vCenter Server용 NetApp Element 플러그인"

## REST API 사용 권한 얻기

REST API UI에서 관리 서비스용 API를 사용하려면 먼저 권한을 부여해야 합니다. 액세스 토큰을 얻어서 이를 수행합니다.

토큰을 얻으려면 클러스터 관리자 자격 증명과 클라이언트 ID를 제공해야 합니다. 각 토큰은 약 10분 동안 지속됩니다. 토큰이 만료된 후에는 새로운 액세스 토큰을 다시 인증할 수 있습니다.

관리 노드 설치 및 배포 중에 인증 기능이 설정됩니다. 토큰 서비스는 설정 중에 정의한 스토리지 클러스터를 기반으로 합니다.

시작하기 전에

- 클러스터 버전에서는 NetApp Element 소프트웨어 11.3 이상을 실행해야 합니다.
- 버전 11.3 이상을 실행하는 관리 노드를 배포했어야 합니다.

### API 명령

```
TOKEN=`curl -k -X POST https://MVIP/auth/connect/token -F client_id=mnode-client -F grant_type=password -F username=CLUSTER_ADMIN -F password=CLUSTER_PASSWORD|awk -F':' '{print $2}'|awk -F',' '{print $1}'|sed s/\"//g`
```

### REST API UI 단계

1. 예를 들어 관리 노드 IP 주소 다음에 서비스 이름을 입력하여 서비스에 대한 REST API UI에 액세스합니다.  
/mnode/ :

```
https://<ManagementNodeIP>/mnode/
```

2. \*승인\*을 선택하세요.



또는 서비스 API 옆에 있는 잠금 아이콘을 선택할 수도 있습니다.

3. 다음을 완료하세요.

- a. 클러스터 사용자 이름과 비밀번호를 입력하세요.
- b. 클라이언트 ID를 다음과 같이 입력하세요. mnode-client .
- c. 클라이언트 비밀번호에 값을 입력하지 마세요.
- d. 세션을 시작하려면 \*승인\*을 선택하세요.

4. 사용 가능한 권한 대화 상자를 닫습니다.



토큰이 만료된 후에 명령을 실행하려고 하면 401 Error: UNAUTHORIZED 메시지가 나타납니다. 이 메시지가 표시되면 다시 승인하세요.

더 많은 정보를 찾아보세요

- ["vCenter Server용 NetApp Element 플러그인"](#)
- ["SolidFire 및 Element 소프트웨어 문서"](#)

## Active IQ 및 NetApp 모니터링 활성화

설치 또는 업그레이드 중에 Active IQ 스토리지 모니터링을 아직 활성화하지 않았다면 이제 활성화할 수 있습니다. SolidFire 올플래시 스토리지 시스템을 설치하는 동안 SolidFire Active IQ 설정하지 않은 경우 이 절차를 사용해야 할 수도 있습니다.

Active IQ 수집기 서비스는 구성 데이터와 Element 소프트웨어 기반 클러스터 성능 측정 항목을 SolidFire Active IQ 로 전달하여 과거 보고 및 실시간에 가까운 성능 모니터링을 수행합니다. NetApp 모니터링 서비스를 사용하면 스토리지 클러스터 오류를 vCenter로 전달하여 경고 알림을 받을 수 있습니다.

시작하기 전에

- 예를 들어 Active IQ 의 일부 기능(서비스 품질(QoS))을 사용하려면 Element 11.3 이상이 필요합니다. 모든 Active IQ 기능을 사용할 수 있는 능력이 있는지 확인하기 위해 NetApp 다음을 권장합니다.
  - 스토리지 클러스터에서 NetApp Element 소프트웨어 11.3 이상이 실행되고 있습니다.
  - 버전 11.3 이상을 실행하는 관리 노드를 배포했습니다.
- 인터넷에 접속할 수 있습니다. Active IQ 수집기 서비스는 외부 연결이 없는 다크 사이트에서는 사용할 수 없습니다.

단계

1. 설치에 대한 기본 자산 ID를 가져옵니다.

- a. 관리 노드에서 인벤토리 서비스 REST API UI를 엽니다.

```
https://<ManagementNodeIP>/inventory/1/
```

b. \*승인\*을 선택하고 다음을 완료하세요.

- i. 클러스터 사용자 이름과 비밀번호를 입력하세요.
- ii. 클라이언트 ID를 다음과 같이 입력하세요. `mnode-client`.
- iii. 세션을 시작하려면 \*승인\*을 선택하세요.
- iv. 창을 닫으세요.

c. REST API UI에서 \*GET /installations\*를 선택합니다.

d. \*시도해보기\*를 선택하세요.

e. \*실행\*을 선택하세요.

f. 코드 200 응답 본문에서 다음을 복사합니다. id 설치를 위해서.

```
{
  "installations": [
    {
      "_links": {
        "collection":
"https://10.111.211.111/inventory/1/installations",
        "self":
"https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-
91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
    }
  ]
}
```



설치에는 설치 또는 업그레이드 중에 생성된 기본 자산 구성이 있습니다.

## 2. 원격 측정 활성화:

- a. 관리 노드에서 관리 노드 IP 주소를 입력한 다음 mnode 서비스 API UI에 액세스합니다. /mnode :

```
https://<ManagementNodeIP>/mnode
```

- b. 승인 또는 잠금 아이콘을 선택하고 다음을 완료하세요.

- i. 클러스터 사용자 이름과 비밀번호를 입력하세요.
- ii. 클라이언트 ID를 다음과 같이 입력하세요. mnode-client .
- iii. 세션을 시작하려면 \*승인\*을 선택하세요.
- iv. 창을 닫으세요.

- c. 기본 자산을 구성합니다.

- i. \*PUT /assets/{asset\_id}\*를 선택하세요.
- ii. \*시도해보기\*를 선택하세요.
- iii. JSON 페이로드에 다음을 입력하세요.

```
{
  "telemetry_active": true
  "config": {}
}
```

- iv. 이전 단계의 기본 ID를 \*asset\_ID\*에 입력합니다.

- v. \*실행\*을 선택하세요.

Active IQ 서비스는 자산이 변경될 때마다 자동으로 다시 시작됩니다. 자산을 수정하면 설정이 적용되기 전에 약간의 지연이 발생합니다.

3. 아직 수행하지 않았다면 NetApp Hybrid Cloud Control에 대한 vCenter 컨트롤러 자산을 관리 노드 알려진 자산에 추가합니다.



NetApp 모니터링 서비스에는 컨트롤러 자산이 필요합니다.

- 컨트롤러 하위 자산을 추가하려면 \*POST /assets/{asset\_id}/controllers\*를 선택하세요.
- \*시도해보기\*를 선택하세요.
- 클립보드에 복사한 부모 기반 자산 ID를 **asset\_id** 필드에 입력합니다.
- 필요한 페이로드 값을 입력하세요. type ~처럼 vCenter 및 vCenter 자격 증명.

```
{
  "username": "string",
  "password": "string",
  "ip": "string",
  "type": "vCenter",
  "host_name": "string",
  "config": {}
}
```



`ip`vCenter IP 주소입니다.

- \*실행\*을 선택하세요.

더 많은 정보를 찾아보세요

- ["vCenter Server용 NetApp Element 플러그인"](#)
- ["SolidFire 및 Element 소프트웨어 문서"](#)

## 여러 vCenter에 대한 NetApp Hybrid Cloud Control 구성

연결 모드를 사용하지 않는 두 개 이상의 vCenter에서 자산을 관리하도록 NetApp Hybrid Cloud Control을 구성할 수 있습니다.

최근에 확장된 설치에 자산을 추가해야 하거나 새 자산이 구성에 자동으로 추가되지 않은 경우 초기 설치 후에 이 프로세스를 사용해야 합니다. 이러한 API를 사용하여 설치에 최근 추가된 자산을 추가하세요.

필요한 것

- 귀하의 클러스터 버전은 NetApp Element 소프트웨어 11.3 이상을 실행하고 있습니다.
- 버전 11.3 이상을 실행하는 관리 노드를 배포했습니다.

단계

- ["새 vCenter를 컨트롤러 자산으로 추가"](#)관리 노드 구성으로.
- 관리 노드에서 인벤토리 서비스 API를 새로 고칩니다.

https://<ManagementNodeIP>/inventory/1/



또는 NetApp Hybrid Cloud Control UI에서 인벤토리가 업데이트될 때까지 2분간 기다릴 수 있습니다.

- a. \*승인\*을 선택하고 다음을 완료하세요.
    - i. 클러스터 사용자 이름과 비밀번호를 입력하세요.
    - ii. 클라이언트 ID를 다음과 같이 입력하세요. `mnode-client`.
    - iii. 세션을 시작하려면 \*승인\*을 선택하세요.
    - iv. 창을 닫으세요.
  - b. REST API UI에서 \*GET /installations\*를 선택합니다.
  - c. \*시도해보기\*를 선택하세요.
  - d. \*실행\*을 선택하세요.
  - e. 응답에서 설치 자산 ID를 복사합니다. ("id").
  - f. REST API UI에서 \*GET /installations/{id}\*를 선택합니다.
  - g. \*시도해보기\*를 선택하세요.
  - h. 새로 고침을 설정하세요 `True`.
  - i. 설치 자산 ID를 `id` 필드에 붙여넣습니다.
  - j. \*실행\*을 선택하세요.
3. NetApp Hybrid Cloud Control 브라우저를 새로 고쳐 변경 사항을 확인하세요.

더 많은 정보를 찾아보세요

- ["vCenter Server용 NetApp Element 플러그인"](#)
- ["SolidFire 및 Element 소프트웨어 문서"](#)

## 관리 노드에 컨트롤러 자산 추가

REST API UI를 사용하여 관리 노드 구성에 컨트롤러 자산을 추가할 수 있습니다.

최근에 설치를 확장했고 새 자산이 구성에 자동으로 추가되지 않은 경우 자산을 추가해야 할 수도 있습니다. 이러한 API를 사용하여 설치에 최근 추가된 자산을 추가하세요.

필요한 것

- 귀하의 클러스터 버전은 NetApp Element 소프트웨어 11.3 이상을 실행하고 있습니다.
- 버전 11.3 이상을 실행하는 관리 노드를 배포했습니다.
- vCenter에서 새로운 NetApp HCC 역할을 생성하여 관리 노드 서비스 보기를 NetApp 전용 자산으로 제한했습니다. 보다 ["vCenter에서 NetApp HCC 역할 생성"](#)

단계

1. 설치에 대한 기본 자산 ID를 가져옵니다.

- a. 관리 노드에서 인벤토리 서비스 REST API UI를 엽니다.

```
https://<ManagementNodeIP>/inventory/1/
```

- b. \*승인\*을 선택하고 다음을 완료하세요.

- i. 클러스터 사용자 이름과 비밀번호를 입력하세요.
- ii. 클라이언트 ID를 다음과 같이 입력하세요. `mnode-client`.
- iii. 세션을 시작하려면 \*승인\*을 선택하세요.
- iv. 창을 닫으세요.

- c. REST API UI에서 \*GET /installations\*를 선택합니다.

- d. \*시도해보기\*를 선택하세요.

- e. \*실행\*을 선택하세요.

- f. 코드 200 응답 본문에서 다음을 복사합니다. id 설치를 위해서.

```
{
  "installations": [
    {
      "_links": {
        "collection":
"https://10.111.211.111/inventory/1/installations",
        "self":
"https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-
91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
    }
  ]
}
```



설치에는 설치 또는 업그레이드 중에 생성된 기본 자산 구성이 있습니다.

- g. REST API UI에서 \*GET /installations/{id}\*를 선택합니다.

- h. \*시도해보기\*를 선택하세요.

- i. 설치 자산 ID를 `id` 필드에 붙여넣습니다.

- j. \*실행\*을 선택하세요.

- k. 응답에서 클러스터 컨트롤러 ID를 복사하여 저장합니다. ("`controllerId`") 을 나중에 사용합니다.

2. 기존 기본 자산에 컨트롤러 하위 자산을 추가하려면 다음을 선택하세요.

```
POST /assets/{asset_id}/controllers
```

- a. 관리 노드에서 mNode 서비스 REST API UI를 엽니다.

```
https://<ManagementNodeIP>/mnode
```

- b. \*승인\*을 선택하고 다음을 완료하세요.
- 클러스터 사용자 이름과 비밀번호를 입력하세요.
  - 클라이언트 ID를 다음과 같이 입력하세요. `mnode-client`.
  - 세션을 시작하려면 \*승인\*을 선택하세요.
  - 창을 닫으세요.
- c. \*POST /assets/{asset\_id}/controllers\*를 선택하세요.
- d. \*시도해보기\*를 선택하세요.
- e. **asset\_id** 필드에 부모 기반 자산 ID를 입력합니다.
- f. 필요한 값을 페이로드에 추가합니다.
- g. \*실행\*을 선택하세요.

더 많은 정보를 찾아보세요

- ["vCenter Server용 NetApp Element 플러그인"](#)
- ["SolidFire 및 Element 소프트웨어 문서"](#)

## 스토리지 클러스터 자산 생성 및 관리

REST API를 사용하여 관리 노드에 새로운 스토리지 클러스터 자산을 추가하고, 알려진 스토리지 클러스터 자산에 대한 저장된 자격 증명을 편집하고, 관리 노드에서 스토리지 클러스터 자산을 삭제할 수 있습니다.

필요한 것

- 스토리지 클러스터 버전에서 NetApp Element 소프트웨어 11.3 이상이 실행되고 있는지 확인하세요.
- 버전 11.3 이상을 실행하는 관리 노드를 배포했는지 확인하세요.

스토리지 클러스터 자산 관리 옵션

다음 옵션 중 하나를 선택하세요.

- [스토리지 클러스터 자산의 설치 ID 및 클러스터 ID를 검색합니다.](#)
- [새로운 스토리지 클러스터 자산 추가](#)
- [스토리지 클러스터 자산에 대한 저장된 자격 증명을 편집합니다.](#)
- [스토리지 클러스터 자산 삭제](#)

스토리지 클러스터 자산의 설치 ID 및 클러스터 ID를 검색합니다.

REST API를 사용하면 설치 ID와 스토리지 클러스터 ID를 얻을 수 있습니다. 새로운 스토리지 클러스터 자산을

추가하려면 설치 ID가 필요하고, 특정 스토리지 클러스터 자산을 수정하거나 삭제하려면 클러스터 ID가 필요합니다.

단계

1. 관리 노드 IP 주소를 입력한 다음 다음을 입력하여 인벤토리 서비스에 대한 REST API UI에 액세스합니다.  
/inventory/1/ :

```
https://<ManagementNodeIP>/inventory/1/
```

2. 승인 또는 잠금 아이콘을 선택하고 다음을 완료하세요.
  - a. 클러스터 사용자 이름과 비밀번호를 입력하세요.
  - b. 클라이언트 ID를 다음과 같이 입력하세요. `mnode-client`.
  - c. 세션을 시작하려면 \*승인\*을 선택하세요.
  - d. 창을 닫으세요.
3. \*GET /installations\*를 선택하세요.
4. \*시도해보기\*를 선택하세요.
5. \*실행\*을 선택하세요.

API는 알려진 모든 설치 목록을 반환합니다.

6. 코드 200 응답 본문에서 값을 저장합니다. `id` 설치 목록에서 찾을 수 있는 필드입니다. 이것은 설치 ID입니다. 예를 들어:

```
"installations": [  
  {  
    "id": "1234a678-12ab-35dc-7b4a-1234a5b6a7ba",  
    "name": "my-sf-installation",  
    "_links": {  
      "collection": "https://localhost/inventory/1/installations",  
      "self": "https://localhost/inventory/1/installations/1234a678-  
12ab-35dc-7b4a-1234a5b6a7ba"  
    }  
  }  
]
```

7. 관리 노드 IP 주소를 입력한 다음 저장 서비스에 대한 REST API UI에 액세스합니다. /storage/1/ :

```
https://<ManagementNodeIP>/storage/1/
```

8. 승인 또는 잠금 아이콘을 선택하고 다음을 완료하세요.
  - a. 클러스터 사용자 이름과 비밀번호를 입력하세요.
  - b. 클라이언트 ID를 다음과 같이 입력하세요. `mnode-client`.

- c. 세션을 시작하려면 \*승인\*을 선택하세요.
  - d. 창을 닫으세요.
9. \*GET /clusters\*를 선택하세요.
  10. \*시도해보기\*를 선택하세요.
  11. 이전에 저장한 설치 ID를 입력하세요. `installationId` 매개변수.
  12. \*실행\*을 선택하세요.

API는 이 설치에서 알려진 모든 스토리지 클러스터 목록을 반환합니다.

13. 코드 200 응답 본문에서 올바른 스토리지 클러스터를 찾아 클러스터의 값을 저장합니다. `storageId` 필드. 이는 스토리지 클러스터 ID입니다.

### 새로운 스토리지 클러스터 자산 추가

REST API를 사용하여 관리 노드 인벤토리에 하나 이상의 새로운 스토리지 클러스터 자산을 추가할 수 있습니다. 새로운 스토리지 클러스터 자산을 추가하면 해당 자산이 자동으로 관리 노드에 등록됩니다.

#### 필요한 것

- 당신은 복사했습니다 [스토리지 클러스터 ID 및 설치 ID](#) 추가하려는 모든 스토리지 클러스터에 대해.
- 두 개 이상의 저장 노드를 추가하는 경우 다음 제한 사항을 읽고 이해해야 합니다. "[권위 있는 클러스터](#)" 다중 스토리지 클러스터 지원.



권한 있는 클러스터에 정의된 모든 사용자는 NetApp Hybrid Cloud Control 인스턴스에 연결된 다른 모든 클러스터의 사용자로 정의됩니다.

#### 단계

1. 관리 노드 IP 주소를 입력한 다음 저장 서비스에 대한 REST API UI에 액세스합니다. `/storage/1/` :

```
https://<ManagementNodeIP>/storage/1/
```

2. 승인 또는 잠금 아이콘을 선택하고 다음을 완료하세요.
  - a. 클러스터 사용자 이름과 비밀번호를 입력하세요.
  - b. 클라이언트 ID를 다음과 같이 입력하세요. `mnode-client`.
  - c. 세션을 시작하려면 \*승인\*을 선택하세요.
  - d. 창을 닫으세요.
3. \*POST /clusters\*를 선택하세요.
4. \*시도해보기\*를 선택하세요.
5. 요청 본문 필드에 다음 매개변수를 사용하여 새 스토리지 클러스터의 정보를 입력합니다.

```
{
  "installationId": "a1b2c34d-e56f-1a2b-c123-1ab2cd345d6e",
  "mvip": "10.0.0.1",
  "password": "admin",
  "userId": "admin"
}
```

매개변수	유형	설명
installationId	끈	새로운 스토리지 클러스터를 추가할 설치입니다. 이전에 저장한 설치 ID를 이 매개변수에 입력하세요.
mvip	끈	스토리지 클러스터의 IPv4 관리 가상 IP 주소(MVIP)입니다.
password	끈	스토리지 클러스터와 통신하는 데 사용되는 비밀번호입니다.
userId	끈	스토리지 클러스터와 통신하는 데 사용되는 사용자 ID입니다(사용자는 관리자 권한이 있어야 함).

6. \*실행\*을 선택하세요.

API는 이름, 버전, IP 주소 정보 등 새로 추가된 스토리지 클러스터 자산에 대한 정보가 포함된 객체를 반환합니다.

스토리지 클러스터 자산에 대한 저장된 자격 증명을 편집합니다.

관리 노드가 스토리지 클러스터에 로그인하는 데 사용하는 저장된 자격 증명을 편집할 수 있습니다. 선택한 사용자에게는 클러스터 관리자 액세스 권한이 있어야 합니다.



다음 단계를 따랐는지 확인하세요. [스토리지 클러스터 자산의 설치 ID 및 클러스터 ID를 검색합니다.](#) 계속하기 전에.

단계

1. 관리 노드 IP 주소를 입력한 다음 저장 서비스에 대한 REST API UI에 액세스합니다. /storage/1/ :

```
https://<ManagementNodeIP>/storage/1/
```

2. 승인 또는 잠금 아이콘을 선택하고 다음을 완료하세요.
  - a. 클러스터 사용자 이름과 비밀번호를 입력하세요.
  - b. 클라이언트 ID를 다음과 같이 입력하세요. mnode-client .
  - c. 세션을 시작하려면 \*승인\*을 선택하세요.
  - d. 창을 닫으세요.
3. \*PUT /clusters/{storageId}\*를 선택합니다.

4. \*시도해보기\*를 선택하세요.
5. 이전에 복사한 스토리지 클러스터 ID를 붙여넣습니다. storageId 매개변수.
6. 요청 본문 필드에서 다음 매개변수 중 하나 또는 둘 다를 변경하세요.

```
{
  "password": "adminadmin",
  "userId": "admin"
}
```

매개변수	유형	설명
password	끈	스토리지 클러스터와 통신하는 데 사용되는 비밀번호입니다.
userId	끈	스토리지 클러스터와 통신하는 데 사용되는 사용자 ID입니다(사용자는 관리자 권한이 있어야 함).

7. \*실행\*을 선택하세요.

#### 스토리지 클러스터 자산 삭제

스토리지 클러스터가 더 이상 서비스되지 않으면 스토리지 클러스터 자산을 삭제할 수 있습니다. 스토리지 클러스터 자산을 제거하면 관리 노드에서 자동으로 등록이 취소됩니다.



다음 단계를 따랐는지 확인하세요. [스토리지 클러스터 자산의 설치 ID 및 클러스터 ID를 검색합니다.](#) 계속하기 전에.

#### 단계

1. 관리 노드 IP 주소를 입력한 다음 저장 서비스에 대한 REST API UI에 액세스합니다. /storage/1/ :

```
https://<ManagementNodeIP>/storage/1/
```

2. 승인 또는 잠금 아이콘을 선택하고 다음을 완료하세요.
  - a. 클러스터 사용자 이름과 비밀번호를 입력하세요.
  - b. 클라이언트 ID를 다음과 같이 입력하세요. mnode-client .
  - c. 세션을 시작하려면 \*승인\*을 선택하세요.
  - d. 창을 닫으세요.
3. \*DELETE /clusters/{storageId}\*를 선택합니다.
4. \*시도해보기\*를 선택하세요.
5. 이전에 복사한 스토리지 클러스터 ID를 입력하세요. storageId 매개변수.
6. \*실행\*을 선택하세요.

성공하면 API는 빈 응답을 반환합니다.

더 많은 정보를 찾아보세요

- ["권위 있는 클러스터"](#)
- ["vCenter Server용 NetApp Element 플러그인"](#)
- ["SolidFire 및 Element 소프트웨어 문서"](#)

## 기존 컨트롤러 자산 보기 또는 편집

REST API를 사용하여 관리 노드 구성에서 VMware vCenter 컨트롤러에 대한 정보를 보고 기존 컨트롤러를 편집할 수 있습니다. 컨트롤러는 NetApp SolidFire 설치에 대한 관리 노드에 등록된 VMware vCenter 인스턴스입니다.

시작하기 전에

- 클러스터 버전에서 NetApp Element 소프트웨어 11.3 이상이 실행되고 있는지 확인하세요.
- 버전 11.3 이상을 실행하는 관리 노드를 배포했는지 확인하세요.

관리 서비스 **REST API**에 액세스하세요

단계

1. 관리 노드 IP 주소를 입력한 다음 관리 서비스에 대한 REST API UI에 액세스합니다. /vcenter/1/ :

```
https://<ManagementNodeIP>/vcenter/1/
```

2. 승인 또는 잠금 아이콘을 선택하고 다음을 완료하세요.
  - a. 클러스터 사용자 이름과 비밀번호를 입력하세요.
  - b. 클라이언트 ID를 다음과 같이 입력하세요. `mnode-client`.
  - c. 세션을 시작하려면 \*승인\*을 선택하세요.
  - d. 창을 닫으세요.

## 기존 컨트롤러에 대한 저장된 정보 보기

REST API를 사용하여 관리 노드에 등록된 기존 vCenter 컨트롤러를 나열하고 해당 컨트롤러에 대한 저장된 정보를 볼 수 있습니다.

단계

1. \*GET /compute/controllers\*를 선택합니다.
2. \*시도해보기\*를 선택하세요.
3. \*실행\*을 선택하세요.

API는 모든 알려진 vCenter 컨트롤러 목록과 함께 각 컨트롤러와 통신하는 데 사용되는 IP 주소, 컨트롤러 ID, 호스트 이름 및 사용자 ID를 반환합니다.

- 특정 컨트롤러의 연결 상태를 알고 싶다면 컨트롤러 ID를 복사하세요. id 해당 컨트롤러의 필드를 클립보드에 복사하여 확인하세요. [기존 컨트롤러의 상태 보기](#).

#### 기존 컨트롤러의 상태 보기

관리 노드에 등록된 기존 vCenter 컨트롤러의 상태를 볼 수 있습니다. API는 NetApp Hybrid Cloud Control이 vCenter 컨트롤러에 연결할 수 있는지 여부를 나타내는 상태와 해당 상태에 대한 이유를 반환합니다.

#### 단계

- \*GET /compute/controllers/{controller\_id}/status\*를 선택합니다.
- \*시도해보기\*를 선택하세요.
- 이전에 복사한 컨트롤러 ID를 입력하세요. controller\_id 매개변수.
- \*실행\*을 선택하세요.

API는 해당 vCenter 컨트롤러의 상태와 해당 상태에 대한 이유를 반환합니다.

#### 컨트롤러의 저장된 속성을 편집합니다.

관리 노드에 등록된 기존 vCenter 컨트롤러에 대해 저장된 사용자 이름이나 비밀번호를 편집할 수 있습니다. 기존 vCenter 컨트롤러의 저장된 IP 주소는 편집할 수 없습니다.

#### 단계

- \*PUT /compute/controllers/{controller\_id}\*를 선택합니다.
- vCenter 컨트롤러의 컨트롤러 ID를 입력하세요. controller\_id 매개변수.
- \*시도해보기\*를 선택하세요.
- 요청 본문 필드에서 다음 매개변수 중 하나를 변경하세요.

매개변수	유형	설명
userId	끈	vCenter 컨트롤러와 통신하는 데 사용되는 사용자 ID를 변경합니다 (사용자는 관리자 권한이 있어야 함).
password	끈	vCenter 컨트롤러와 통신하는 데 사용되는 비밀번호를 변경합니다.

- \*실행\*을 선택하세요.

API는 업데이트된 컨트롤러 정보를 반환합니다.

#### 더 많은 정보를 찾아보세요

- "[관리 노드에 컨트롤러 자산 추가](#)"
- "[vCenter Server용 NetApp Element 플러그인](#)"
- "[SolidFire 및 Element 소프트웨어 문서](#)"

## 프록시 서버 구성

클러스터가 프록시 서버 뒤에 있는 경우 공용 네트워크에 접속할 수 있도록 프록시 설정을 구성해야 합니다.

프록시 서버는 원격 측정 수집기와 역방향 터널 연결에 사용됩니다. 설치 또는 업그레이드 중에 프록시 서버를 구성하지 않은 경우 REST API UI를 사용하여 프록시 서버를 활성화하고 구성할 수 있습니다. 기존 프록시 서버 설정을 수정하거나 프록시 서버를 비활성화할 수도 있습니다.

프록시 서버를 구성하는 명령은 관리 노드의 현재 프록시 설정을 업데이트한 다음 반환합니다. 프록시 설정은 NetApp 모니터링 서비스인 Active IQ 와 NetApp 지원을 위한 역방향 지원 터널을 포함하여 관리 노드에 설치된 기타 Element 소프트웨어 유틸리티에서 사용됩니다.

### 시작하기 전에

- 구성 중인 프록시 서버에 대한 호스트 및 자격 증명 정보를 알아야 합니다.
- 클러스터 버전에서 NetApp Element 소프트웨어 11.3 이상이 실행되고 있는지 확인하세요.
- 버전 11.3 이상을 실행하는 관리 노드를 배포했는지 확인하세요.
- (관리 노드 12.0 이상) 프록시 서버를 구성하기 전에 NetApp Hybrid Cloud Control을 관리 서비스 버전 2.16으로 업데이트했습니다.

### 단계

1. 관리 노드 IP 주소를 입력한 다음 관리 노드에서 REST API UI에 액세스합니다. /mnode :

```
https://<ManagementNodeIP>/mnode
```

2. 승인 또는 잠금 아이콘을 선택하고 다음을 완료하세요.
  - a. 클러스터 사용자 이름과 비밀번호를 입력하세요.
  - b. 클라이언트 ID를 다음과 같이 입력하세요. mnode-client .
  - c. 세션을 시작하려면 \*승인\*을 선택하세요.
  - d. 창을 닫으세요.
3. \*PUT /설정\*을 선택하세요.
4. \*시도해보기\*를 선택하세요.
5. 프록시 서버를 활성화하려면 다음을 설정해야 합니다. use\_proxy 사실입니다. IP 또는 호스트 이름과 프록시 포트 대상을 입력하세요.

프록시 사용자 이름, 프록시 비밀번호, SSH 포트는 선택 사항이므로 사용하지 않을 경우 생략해야 합니다.

```
{
  "proxy_ip_or_hostname": "[IP or name]",
  "use_proxy": [true/false],
  "proxy_username": "[username]",
  "proxy_password": "[password]",
  "proxy_port": [port value],
  "proxy_ssh_port": [port value: default is 443]
}
```

6. \*실행\*을 선택하세요.



환경에 따라 관리 노드를 재부팅해야 할 수도 있습니다.

더 많은 정보를 찾아보세요

- ["vCenter Server용 NetApp Element 플러그인"](#)
- ["SolidFire 및 Element 소프트웨어 문서"](#)

## 관리 노드 OS 및 서비스 버전 확인

관리 노드의 REST API를 사용하여 관리 노드 OS, 관리 서비스 번들 및 관리 노드에서 실행되는 개별 서비스의 버전 번호를 확인할 수 있습니다.

필요한 것

- 클러스터에서 NetApp Element 소프트웨어 11.3 이상이 실행되고 있습니다.
- 버전 11.3 이상을 실행하는 관리 노드를 배포했습니다.

옵션

- [API 명령](#)
- [REST API UI 단계](#)

## API 명령

- 관리 노드에서 실행 중인 관리 노드 OS, 관리 서비스 번들 및 관리 노드 API(mnode-api) 서비스에 대한 버전 정보를 가져옵니다.

```
curl -X GET "https://<ManagementNodeIP>/mnode/about" -H "accept:
application/json"
```

- 관리 노드에서 실행 중인 개별 서비스에 대한 버전 정보를 가져옵니다.

```
curl -X GET "https://<ManagementNodeIP>/mnode/services?status=running"
-H "accept: */*" -H "Authorization: ${TOKEN}"
```



당신은 운반자를 찾을 수 있습니다. `${TOKEN}` API 명령에서 사용됨 "허가하다". 운반자 `${TOKEN}` curl 응답에 있습니다.

## REST API UI 단계

1. 관리 노드 IP 주소를 입력한 다음 다음을 입력하여 서비스에 대한 REST API UI에 액세스합니다. `/mnode/` :

```
https://<ManagementNodeIP>/mnode/
```

2. 다음 중 하나를 수행하세요.

- 관리 노드에서 실행 중인 관리 노드 OS, 관리 서비스 번들 및 관리 노드 API(mnode-api) 서비스에 대한 버전 정보를 가져옵니다.
  - i. \*GET /about\*을 선택하세요.
  - ii. \*시도해보기\*를 선택하세요.
  - iii. \*실행\*을 선택하세요.

관리 서비스 번들 버전("mnode\_bundle\_version"), 관리 노드 OS 버전("os\_version"), 및 관리 노드 API 버전("version")는 응답 본문에 표시됩니다.

- 관리 노드에서 실행 중인 개별 서비스에 대한 버전 정보를 가져옵니다.
  - i. \*GET /services\*를 선택하세요.
  - ii. \*시도해보기\*를 선택하세요.
  - iii. 상태를 \*실행 중\*으로 선택하세요.
  - iv. \*실행\*을 선택하세요.

관리 노드에서 실행 중인 서비스는 응답 본문에 표시됩니다.

더 많은 정보를 찾아보세요

- ["vCenter Server용 NetApp Element 플러그인"](#)
- ["SolidFire 및 Element 소프트웨어 문서"](#)

## 관리 서비스에서 로그 가져오기

REST API를 사용하여 관리 노드에서 실행되는 서비스의 로그를 검색할 수 있습니다. 모든 공개 서비스에서 로그를 가져오거나 특정 서비스를 지정하고 쿼리 매개변수를 사용하여 반환 결과를 더 잘 정의할 수 있습니다.

## 필요한 것

- 귀하의 클러스터 버전은 NetApp Element 소프트웨어 11.3 이상을 실행하고 있습니다.
- 버전 11.3 이상을 실행하는 관리 노드를 배포했습니다.

## 단계

### 1. 관리 노드에서 REST API UI를 엽니다.

- 관리 서비스 2.21.61부터 시작:

```
https://<ManagementNodeIP>/mnode/4/
```

- 관리 서비스 2.20.69 또는 이전 버전의 경우:

```
https://<ManagementNodeIP>/mnode
```

### 2. 승인 또는 잠금 아이콘을 선택하고 다음을 완료하세요.

- a. 클러스터 사용자 이름과 비밀번호를 입력하세요.
- b. 값이 아직 채워지지 않았다면 클라이언트 ID를 mnode-client로 입력하세요.
- c. 세션을 시작하려면 \*승인\*을 선택하세요.
- d. 창을 닫으세요.

### 3. \*GET /logs\*를 선택하세요.

### 4. \*시도해보기\*를 선택하세요.

### 5. 다음 매개변수를 지정하세요.

- `lines`: 로그를 반환할 줄의 수를 입력합니다. 이 매개변수는 기본적으로 1000인 정수입니다.



`lines`를 0으로 설정하여 로그 내용의 전체 기록을 요청하지 않도록 합니다.

- `since`: 서비스 로그 시작 지점에 ISO-8601 타임스탬프를 추가합니다.



합리적인 것을 사용하세요 `since` 더 넓은 시간 범위의 로그를 수집할 때 매개변수를 사용합니다.

- `service-name`: 서비스 이름을 입력하세요.



사용하다 `GET /services` 관리 노드의 서비스를 나열하는 명령입니다.

- `stopped`: 설정 `true` 중지된 서비스에서 로그를 검색합니다.

### 6. \*실행\*을 선택하세요.

### 7. 응답 본문에서 \*다운로드\*를 선택하여 로그 출력을 저장합니다.

더 많은 정보를 찾아보세요

- "vCenter Server용 NetApp Element 플러그인"
- "SolidFire 및 Element 소프트웨어 문서"

## 지원 연결 관리

기본 문제 해결을 위해 **SSH**를 사용하여 스토리지 노드에 액세스

Element 12.5부터 기본적인 문제 해결을 위해 스토리지 노드에서 `sfireadonly` 시스템 계정을 사용할 수 있습니다. 고급 문제 해결을 위해 NetApp 지원에 대한 원격 지원 터널 액세스를 활성화하고 열 수도 있습니다.

`sfireadonly` 시스템 계정을 사용하면 다음을 포함한 기본 Linux 시스템 및 네트워크 문제 해결 명령을 실행할 수 있습니다. `ping`.



NetApp 지원팀의 별도 안내 없이 이 시스템을 변경하는 것은 지원되지 않으며, 지원 계약이 무효화되고 데이터 불안정이나 접근 불가 현상이 발생할 수 있습니다.

시작하기 전에

- 쓰기 권한: 현재 작업 디렉토리에 대한 쓰기 권한이 있는지 확인하세요.
- (선택 사항) 나만의 키 쌍을 생성하세요: 실행 `ssh-keygen` Windows 10, MacOS 또는 Linux 배포판에서. 이는 사용자 키 쌍을 생성하는 일회성 작업이며 향후 문제 해결 세션에 재사용할 수 있습니다. 직원 계정과 연결된 인증서를 사용하면 이 모델에서도 효과적일 수 있습니다.
- 관리 노드에서 **SSH** 기능 활성화: 관리 모드에서 원격 액세스 기능을 활성화하려면 다음을 참조하세요. "[이 주제](#)". 관리 서비스 2.18 이상의 경우, 관리 노드에서 원격 액세스 기능은 기본적으로 비활성화됩니다.
- 저장소 클러스터에서 **SSH** 기능 활성화: 저장소 클러스터 노드에서 원격 액세스 기능을 활성화하려면 다음을 참조하세요. "[이 주제](#)".
- 방화벽 구성: 관리 노드가 프록시 서버 뒤에 있는 경우 `sshd.config` 파일에 다음 TCP 포트가 필요합니다.

TCP 포트	설명	연결 방향
443	웹 UI에 대한 개방형 지원 터널을 통한 역방향 포트 포워딩을 위한 API 호출/HTTPS	관리 노드에서 저장 노드로
22	SSH 로그인 접근	관리 노드에서 스토리지 노드로 또는 스토리지 노드에서 관리 노드로

문제 해결 옵션

- [클러스터 노드 문제 해결](#)
- [NetApp 지원을 통해 클러스터 노드 문제 해결](#)
- [클러스터에 속하지 않는 노드 문제 해결](#)

클러스터 노드 문제 해결

`sfireadonly` 시스템 계정을 사용하여 기본적인 문제 해결을 수행할 수 있습니다.

## 단계

1. 관리 노드 VM을 설치할 때 선택한 계정 로그인 자격 증명을 사용하여 관리 노드에 SSH를 실행합니다.
2. 관리 노드에서 다음으로 이동하세요. `/sf/bin`.
3. 시스템에 적합한 스크립트를 찾으세요.
  - `SignSshKeys.ps1`
  - `SignSshKeys.py`
  - `SignSshKeys.sh`

`SignSshKeys.ps1`은 PowerShell 7 이상에 종속되고 `SignSshKeys.py`는 Python 3.6.0 이상에 종속됩니다. "요청 모듈".



그만큼 `SignSshKeys` 대본을 쓰다 `user`, `user.pub`, 그리고 `user-cert.pub` 현재 작업 디렉토리에 파일을 저장하면 나중에 다음에서 사용됩니다. `ssh` 명령. 그러나 스크립트에 공개 키 파일이 제공되는 경우에는 `<public_key>` 파일(와 함께 `<public_key>` 스크립트에 전달된 공개 키 파일의 접두사로 대체된 내용이 디렉토리에 기록됩니다.

4. 관리 노드에서 스크립트를 실행하여 SSH 키체인을 생성합니다. 이 스크립트는 클러스터의 모든 노드에서 `sftreadonly` 시스템 계정을 사용하여 SSH 액세스를 활성화합니다.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--publickey [public key path]
```

- a. 다음 각 매개변수에 대해 `[]` 괄호(괄호 포함) 안의 값을 바꾸세요.



약어 또는 전체 형식 매개변수를 사용할 수 있습니다.

- `--ip | -i [ip 주소]`: API를 실행할 대상 노드의 IP 주소입니다.
  - `--user | -u [사용자 이름]`: API 호출을 실행하는 데 사용되는 클러스터 사용자입니다.
  - (선택 사항) `--duration | -d [시간]`: 서명된 키가 유효한 상태로 유지되는 기간을 정수로 시간 단위로 지정합니다. 기본값은 24시간입니다.
  - (선택 사항) `--publickey | -k [공개 키 경로]`: 사용자가 공개 키를 제공하기로 선택한 경우 공개 키 경로입니다.
- b. 다음 샘플 명령과 입력 내용을 비교해 보세요. 이 예에서, `10.116.139.195` 저장 노드의 IP입니다. `admin` 클러스터 사용자 이름이고 키 유효 기간은 2시간입니다.

```
sh /sf/bin/SignSshKeys.sh --ip 10.116.139.195 --user admin --duration
2
```

- c. 명령을 실행합니다.

5. 노드 IP에 SSH를 실행합니다.

```
ssh -i user sfreadonly@[node_ip]
```

다음과 같은 기본 Linux 시스템 및 네트워크 문제 해결 명령을 실행할 수 있습니다. ping 및 기타 읽기 전용 명령.

6. (선택 사항) 비활성화"원격 액세스 기능" 문제 해결이 완료된 후에 다시 시도하세요.



SSH를 비활성화하지 않으면 관리 노드에서 SSH가 활성화된 상태로 유지됩니다. SSH가 활성화된 구성은 수동으로 비활성화할 때까지 업데이트 및 업그레이드를 통해 관리 노드에 유지됩니다.

## NetApp 지원을 통해 클러스터 노드 문제 해결

NetApp 지원팀은 기술자가 Element에 대한 심층적인 진단을 실행할 수 있도록 하는 시스템 계정을 사용하여 고급 문제 해결을 수행할 수 있습니다.

### 단계

1. 관리 노드 VM을 설치할 때 선택한 계정 로그인 자격 증명을 사용하여 관리 노드에 SSH를 실행합니다.
2. NetApp 지원팀에서 보낸 포트 번호로 첫 번째 명령을 실행하여 지원 터널을 엽니다.

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

NetApp 지원팀은 지원 터널을 사용하여 관리 노드에 로그인합니다.

3. 관리 노드에서 다음으로 이동하세요. `/sf/bin`.
4. 시스템에 적합한 스크립트를 찾으세요.
  - SignSshKeys.ps1
  - SignSshKeys.py
  - SignSshKeys.sh



SignSshKeys.ps1은 PowerShell 7 이상에 종속되고 SignSshKeys.py는 Python 3.6.0 이상에 종속됩니다. "요청 모듈".

그만큼 SignSshKeys 대본을 쓰다 user , user.pub , 그리고 user-cert.pub 현재 작업 디렉토리에 파일을 저장하면 나중에 다음에서 사용됩니다. ssh 명령. 그러나 스크립트에 공개 키 파일이 제공되는 경우에는 <public\_key> 파일(와 함께 <public\_key> 스크립트에 전달된 공개 키 파일의 접두사로 대체된 내용이 디렉토리에 기록됩니다.

5. SSH 키체인을 생성하려면 스크립트를 실행하세요. `--sfadmin` 깃발. 이 스크립트는 모든 노드에서 SSH를 활성화합니다.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--sfadmin
```

SSH로 `--sfadmin` 클러스터된 노드에 SSH 키체인을 생성하려면 다음을 사용해야 합니다.  
`--user ~`와 함께 `supportAdmin` 클러스터에 대한 액세스.

구성하려면 `supportAdmin` 클러스터 관리자 계정에 대한 액세스를 위해 Element UI 또는 API를 사용할 수 있습니다.



- "Element UI를 사용하여 "supportAdmin" 액세스 구성"
- 구성 `supportAdmin` API를 사용하여 액세스하고 추가 "supportAdmin" 로서 "access" API 요청을 입력하세요:
  - "새 계정에 대한 "supportAdmin" 액세스 구성"
  - "기존 계정에 대한 "supportAdmin" 액세스 구성"

을 얻으려면 `clusterAdminID`, 당신은 사용할 수 있습니다"클러스터 관리자 목록" API.

추가하려면 `supportAdmin` 접근하려면 클러스터 관리자 또는 관리자 권한이 있어야 합니다.

a. 다음 각 매개변수에 대해 [ ] 괄호(괄호 포함) 안의 값을 바꾸세요.



약어 또는 전체 형식 매개변수를 사용할 수 있습니다.

- `--ip | -i [ip 주소]`: API를 실행할 대상 노드의 IP 주소입니다.
- `--user | -u [사용자 이름]`: API 호출을 실행하는 데 사용되는 클러스터 사용자입니다.
- (선택 사항) `--duration | -d [시간]`: 서명된 키가 유효한 상태로 유지되는 기간을 정수로 시간 단위로 지정합니다. 기본값은 24시간입니다.

b. 다음 샘플 명령과 입력 내용을 비교해 보세요. 이 예에서, 192.168.0.1 저장 노드의 IP입니다. `admin` 클러스터 사용자 이름이고 키 유효 기간은 2시간입니다. `--sfadmin` 문제 해결을 위해 NetApp 지원 노드에 액세스할 수 있습니다.

```
sh /sf/bin/SignSshKeys.sh --ip 192.168.0.1 --user admin --duration 2 --sfadmin
```

c. 명령을 실행합니다.

6. 노드 IP에 SSH를 실행합니다.

```
ssh -i user sfadmin@[node_ip]
```

7. 원격 지원 터널을 닫으려면 다음을 입력하세요.

```
rst --killall
```

8. (선택 사항) 비활성화"원격 액세스 기능" 문제 해결이 완료된 후에 다시 시도하세요.



SSH를 비활성화하지 않으면 관리 노드에서 SSH가 활성화된 상태로 유지됩니다. SSH가 활성화된 구성은 수동으로 비활성화할 때까지 업데이트 및 업그레이드를 통해 관리 노드에 유지됩니다.

### 클러스터에 속하지 않는 노드 문제 해결

아직 클러스터에 추가되지 않은 노드의 기본적인 문제 해결을 수행할 수 있습니다. NetApp 지원팀의 도움 여부와 관계없이 sfreadonly 시스템 계정을 이 목적으로 사용할 수 있습니다. 관리 노드가 설정되어 있으면 이를 SSH에 사용하고 이 작업을 위해 제공된 스크립트를 실행할 수 있습니다.

1. SSH 클라이언트가 설치된 Windows, Linux 또는 Mac 컴퓨터에서 NetApp 지원팀에서 제공한 시스템에 적합한 스크립트를 실행합니다.
2. 노드 IP에 SSH를 실행합니다.

```
ssh -i user sfreadonly@[node_ip]
```

3. (선택 사항) 비활성화"[원격 액세스 기능](#)" 문제 해결이 완료된 후에 다시 시도하세요.



SSH를 비활성화하지 않으면 관리 노드에서 SSH가 활성화된 상태로 유지됩니다. SSH가 활성화된 구성은 수동으로 비활성화할 때까지 업데이트 및 업그레이드를 통해 관리 노드에 유지됩니다.

더 많은 정보를 찾아보세요

- "[vCenter Server용 NetApp Element 플러그인](#)"
- "[NetApp HCI 문서](#)"

### 원격 NetApp 지원 세션 시작

SolidFire 올플래시 스토리지 시스템에 대한 기술 지원이 필요한 경우 NetApp 지원팀이 원격으로 시스템에 접속하여 지원을 제공할 수 있습니다. 세션을 시작하고 원격으로 액세스하려면 NetApp 지원팀에서 사용자 환경에 대한 역방향 Secure Shell(SSH) 연결을 열 수 있습니다.

NetApp 지원을 통해 SSH 역방향 터널 연결을 위한 TCP 포트를 열 수 있습니다. 이 연결을 통해 NetApp 지원팀은 관리 노드에 로그인할 수 있습니다.

시작하기 전에

- 관리 서비스 2.18 이상의 경우, 관리 노드에서 원격 액세스 기능은 기본적으로 비활성화됩니다. 원격 액세스 기능을 활성화하려면 다음을 참조하세요. "[관리 노드에서 SSH 기능 관리](#)".
- 관리 노드가 프록시 서버 뒤에 있는 경우 sshd.config 파일에 다음 TCP 포트가 필요합니다.

TCP 포트	설명	연결 방향
443	웹 UI에 대한 개방형 지원 터널을 통한 역방향 포트 포워딩을 위한 API 호출/HTTPS	관리 노드에서 저장 노드로

TCP 포트	설명	연결 방향
22	SSH 로그인 접근	관리 노드에서 스토리지 노드로 또는 스토리지 노드에서 관리 노드로

## 단계

- 관리 노드에 로그인하고 터미널 세션을 엽니다.
- 프롬프트에서 다음을 입력합니다.

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

- 원격 지원 터널을 닫으려면 다음을 입력하세요.

```
rst --killall
```

- (선택 사항) 비활성화 "원격 액세스 기능" 다시.



SSH를 비활성화하지 않으면 관리 노드에서 SSH가 활성화된 상태로 유지됩니다. SSH가 활성화된 구성은 수동으로 비활성화할 때까지 업데이트 및 업그레이드를 통해 관리 노드에 유지됩니다.

더 많은 정보를 찾아보세요

- ["vCenter Server용 NetApp Element 플러그인"](#)
- ["SolidFire 및 Element 소프트웨어 문서"](#)

## 관리 노드에서 SSH 기능 관리

REST API를 사용하여 관리 노드(mNode)에서 SSH 기능을 비활성화, 다시 활성화하거나 해당 기능을 사용하는지 여부를 확인할 수 있습니다. 제공하는 SSH 기능 "[NetApp 지원 원격 지원 터널\(RST\) 세션 액세스](#)" 관리 서비스 2.18 이상을 실행하는 관리 노드에서는 기본적으로 비활성화됩니다.

Management Services 2.20.69부터 NetApp Hybrid Cloud Control UI를 사용하여 관리 노드에서 SSH 기능을 활성화하거나 비활성화할 수 있습니다.

### 필요한 것

- \* NetApp Hybrid Cloud Control 권한\*: 관리자 권한이 있습니다.
- 클러스터 관리자 권한: 스토리지 클러스터에 대한 관리자 권한이 있습니다.
- **Element** 소프트웨어: 클러스터에서 NetApp Element 소프트웨어 11.3 이상이 실행되고 있습니다.
- 관리 노드: 11.3 이상 버전을 실행하는 관리 노드를 배포했습니다.
- 경영 서비스 업데이트:
  - NetApp Hybrid Cloud Control UI를 사용하려면 다음을 업데이트해야 합니다. "[관리 서비스 번들](#)" 버전 2.20.69 이상.
  - REST API UI를 사용하려면 다음을 업데이트해야 합니다. "[관리 서비스 번들](#)" 버전 2.17로.

## 옵션

- [NetApp Hybrid Cloud Control UI](#)를 사용하여 관리 노드에서 SSH 기능을 비활성화하거나 활성화합니다.

다음 작업 중 하나를 수행할 수 있습니다."인증하다" :

- [API](#)를 사용하여 관리 노드에서 SSH 기능을 비활성화하거나 활성화합니다.
- [API](#)를 사용하여 관리 노드의 SSH 기능 상태를 확인합니다.

**NetApp Hybrid Cloud Control UI**를 사용하여 관리 노드에서 **SSH** 기능을 비활성화하거나 활성화합니다.

관리 노드에서 SSH 기능을 비활성화하거나 다시 활성화할 수 있습니다. 제공하는 SSH 기능"[NetApp 지원 원격 지원 터널\(RST\) 세션 액세스](#)" 관리 서비스 2.18 이상을 실행하는 관리 노드에서는 기본적으로 비활성화됩니다. SSH를 비활성화해도 관리 노드에 대한 기존 SSH 클라이언트 세션은 종료되거나 연결이 끊어지지 않습니다. SSH를 비활성화한 후 나중에 다시 활성화하려면 [NetApp Hybrid Cloud Control UI](#)를 사용하면 됩니다.



스토리지 클러스터에 대한 SSH를 사용하여 지원 액세스를 활성화하거나 비활성화하려면 다음을 사용해야 합니다."[Element UI 클러스터 설정 페이지](#)".

## 단계

1. 대시보드에서 오른쪽 상단의 옵션 메뉴를 선택하고 \*구성\*을 선택합니다.
2. 관리 노드에 대한 지원 액세스 화면에서 스위치를 전환하여 관리 노드 SSH를 활성화합니다.
3. 문제 해결을 완료한 후 관리 노드에 대한 지원 액세스 화면에서 스위치를 전환하여 관리 노드 SSH를 비활성화합니다.

**API**를 사용하여 관리 노드에서 **SSH** 기능을 비활성화하거나 활성화합니다.

관리 노드에서 SSH 기능을 비활성화하거나 다시 활성화할 수 있습니다. 제공하는 SSH 기능"[NetApp 지원 원격 지원 터널\(RST\) 세션 액세스](#)" 관리 서비스 2.18 이상을 실행하는 관리 노드에서는 기본적으로 비활성화됩니다. SSH를 비활성화해도 관리 노드에 대한 기존 SSH 클라이언트 세션은 종료되거나 연결이 끊어지지 않습니다. SSH를 비활성화한 후 나중에 다시 활성화하려면 동일한 API를 사용하면 됩니다.

## API 명령

관리 서비스 2.18 이상의 경우:

```
curl -k -X PUT
"https://<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

관리 서비스 2.17 이하 버전의 경우:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



당신은 운반자를 찾을 수 있습니다  $\${TOKEN}$  API 명령에서 사용됨 "허가하다". 운반자  $\${TOKEN}$  curl 응답에 있습니다.

## REST API UI 단계

1. 관리 노드 IP 주소를 입력한 다음 관리 노드 API 서비스에 대한 REST API UI에 액세스합니다. /mnode/ :

```
https://<ManagementNodeIP>/mnode/
```

2. \*승인\*을 선택하고 다음을 완료하세요.
  - a. 클러스터 사용자 이름과 비밀번호를 입력하세요.
  - b. 클라이언트 ID를 다음과 같이 입력하세요. mnode-client .
  - c. 세션을 시작하려면 \*승인\*을 선택하세요.
  - d. 창을 닫으세요.
3. REST API UI에서 \*PUT /settings/ssh\*를 선택합니다.
  - a. \*시도해보기\*를 선택하세요.
  - b. 활성화 매개변수를 다음으로 설정합니다. false SSH를 비활성화하거나 true 이전에 비활성화되었던 SSH 기능을 다시 활성화합니다.
  - c. \*실행\*을 선택하세요.

**API**를 사용하여 관리 노드의 **SSH** 기능 상태를 확인합니다.

관리 노드 서비스 API를 사용하여 관리 노드에서 SSH 기능이 활성화되어 있는지 여부를 확인할 수 있습니다. 관리 서비스 2.18 이상을 실행하는 관리 노드에서는 SSH가 기본적으로 비활성화되어 있습니다.

## API 명령

관리 서비스 2.18 이상의 경우:

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer  $\${TOKEN}$ "
```

관리 서비스 2.17 이하 버전의 경우:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer  $\${TOKEN}$ "
```



당신은 운반자를 찾을 수 있습니다  $\${TOKEN}$  API 명령에서 사용됨 "허가하다". 운반자  $\${TOKEN}$  curl 응답에 있습니다.

## REST API UI 단계

1. 관리 노드 IP 주소를 입력한 다음 관리 노드 API 서비스에 대한 REST API UI에 액세스합니다. /mnode/ :

```
https://<ManagementNodeIP>/mnode/
```

2. \*승인\*을 선택하고 다음을 완료하세요.
  - a. 클러스터 사용자 이름과 비밀번호를 입력하세요.
  - b. 클라이언트 ID를 다음과 같이 입력하세요. `mnode-client`.
  - c. 세션을 시작하려면 \*승인\*을 선택하세요.
  - d. 창을 닫으세요.
3. REST API UI에서 \*GET /settings/ssh\*를 선택합니다.
  - a. \*시도해보기\*를 선택하세요.
  - b. \*실행\*을 선택하세요.

더 많은 정보를 찾아보세요

- ["vCenter Server용 NetApp Element 플러그인"](#)
- ["SolidFire 및 Element 소프트웨어 문서"](#)

## 저작권 정보

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

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

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

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

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

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

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

## 상표 정보

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