



# VMware vSphere용 ONTAP 툴에 대한 보안 강화 가이드

## Enterprise applications

NetApp  
May 19, 2024

# 목차

VMware vSphere용 ONTAP 톨에 대한 보안 강화 가이드 .....	1
VMware vSphere용 ONTAP 톨에 대한 보안 강화 가이드 .....	1
VMware vSphere 설치 패키지용 ONTAP 톨의 무결성 검증 .....	1
포트 및 프로토콜 .....	3
VMware vSphere 액세스 지점용 ONTAP 톨(사용자) .....	4
상호 TLS(인증서 기반 인증) .....	5
ONTAP 도구 HTTPS 인증서 .....	11
로그인 배너 .....	11
비활성 시간 초과 .....	12
사용자당 최대 동시 요청 수(네트워크 보안 보호::DOS 공격) .....	12
NTP(Network Time Protocol) 구성 .....	13
암호 정책 .....	13

# VMware vSphere용 ONTAP 툴에 대한 보안 강화 가이드

## VMware vSphere용 ONTAP 툴에 대한 보안 강화 가이드

VMware vSphere용 ONTAP 툴에 대한 보안 강화 가이드에서는 가장 안전한 설정을 구성하기 위한 포괄적인 지침을 제공합니다.

이 가이드는 어플라이언스 자체의 애플리케이션과 게스트 OS 모두에 적용됩니다.

## VMware vSphere 설치 패키지용 ONTAP 툴의 무결성 검증

고객은 두 가지 방법으로 ONTAP 도구 설치 패키지의 무결성을 확인할 수 있습니다.

1. 체크섬 확인
2. 서명을 확인하는 중입니다

체크섬은 OTV 설치 패키지의 다운로드 페이지에 제공됩니다. 사용자는 다운로드 페이지에 제공된 체크섬과 비교하여 다운로드한 패키지의 체크섬을 확인해야 합니다.

### ONTAP 도구 OVA의 서명 확인

vApp 설치 패키지는 타볼 형태로 제공됩니다. 이 타볼에는 README 파일 및 OVA 패키지와 함께 가상 어플라이언스에 대한 중간 및 루트 인증서가 포함되어 있습니다. README 파일은 사용자에게 vApp OVA 패키지의 무결성을 확인하는 방법을 안내합니다.

또한 vCenter 버전 7.0U3E 이상에서 제공된 루트 및 중간 인증서를 업로드해야 합니다. 7.0.1 및 7.0.U3E 사이의 vCenter 버전의 경우 인증서 확인 기능은 VMware에서 지원되지 않습니다. 고객은 vCenter 버전 6.x에 대한 인증서를 업로드할 필요가 없습니다

신뢰할 수 있는 루트 인증서를 **vCenter**에 업로드하는 중입니다

1. VMware vSphere Client를 사용하여 vCenter Server에 로그인합니다.
2. [administrator@vsphere.local](mailto:administrator@vsphere.local) | 또는 vCenter Single Sign-On Administrators 그룹의 다른 구성원에 대한 사용자 이름과 암호를 지정합니다. 설치 중에 다른 도메인을 지정한 경우 administrator@mydomain으로 로그인합니다.
3. 인증서 관리 사용자 인터페이스로 이동합니다. a. 홈 메뉴에서 관리 를 선택합니다. b. 인증서에서 인증서 관리를 클릭합니다.
4. 메시지가 표시되면 vCenter Server의 자격 증명을 입력합니다.
5. 신뢰할 수 있는 루트 인증서에서 추가를 클릭합니다.
6. 찾아보기 를 클릭하고 certificate.pem 파일(OTV\_OVA\_INTER\_ROOT\_CERT\_CHAIN.pem)의 위치를 선택합니다.
7. 추가 를 클릭합니다. 인증서가 저장소에 추가됩니다.

을 참조하십시오 **"인증서 저장소에 신뢰할 수 있는 루트 인증서를 추가합니다"** 를 참조하십시오. OVA 파일을 사용하여 vApp을 구축하는 동안 vApp 패키지의 디지털 서명을 'Review details' 페이지에서 확인할 수 있습니다. 다운로드한

vApp 패키지가 정품이면 '게시자' 옆에 '신뢰할 수 있는 인증서'가 표시됩니다(다음 스크린샷 참조).

### Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details**
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

**Review details**  
Verify the template details.

Publisher	Entrust Code Signing CA - OVCS2 (Trusted certificate)
Product	Virtual Appliance - NetApp Inc. ONTAP tools for VMware vSphere
Version	See appliance for version
Vendor	NetApp Inc.
Description	Virtual Appliance - NetApp Inc. ONTAP tools for VMware vSphere for netapp storage systems. For more information or support please visit <a href="https://www.netapp.com/">https://www.netapp.com/</a>
Download size	2.2 GB
Size on disk	3.9 GB (thin provisioned) 53.0 GB (thick provisioned)

Activate  
Go to Sys

CANCEL BACK NEXT

## ONTAP 도구 ISO 및 SRA tar.gz 서명 확인

NetApp는 OTV-iso 및 SRA.tgz용 제품 zip 파일과 함께 제품 다운로드 페이지의 고객과 코드 서명 인증서를 공유합니다.

코드 서명 인증서에서 사용자는 다음과 같이 공개 키를 추출할 수 있습니다.

```
#> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-key name>
```

그런 다음 공개 키를 사용하여 아래와 같이 ISO 및 tgz 제품 zip의 서명을 확인해야 합니다.

```
#> openssl dgst -sha256 -verify <public-key> -signature <signature-file> <binary-name>
```

예:

```
#> openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > OTV_ISO.pub
#> openssl dgst -sha256 -verify OTV_ISO.pub -signature netapp-ontap-tools-
for-vmware-vsphere-9.12-upgrade-iso.sig netapp-ontap-tools-for-vmware-
vsphere-9.12-upgrade.iso
Verified OK => response
```

## 포트 및 프로토콜

이 슬라이드에는 VMware vSphere 서버용 ONTAP 툴과 관리 스토리지 시스템, 서버 및 기타 구성 요소 등의 기타 엔터티 간의 통신을 지원하는 데 필요한 포트와 프로토콜이 나와 있습니다.

### ONTV에 필요한 인바운드 및 아웃바운드 포트

아래 표에 ONTAP 도구의 올바른 작동에 필요한 인바운드 및 아웃바운드 포트가 나열되어 있습니다. 표에 나와 있는 포트만 원격 컴퓨터에서 연결할 수 있도록 열려 있고 다른 모든 포트는 원격 컴퓨터에서 연결할 수 있도록 차단해야 합니다. 이렇게 하면 시스템의 보안 및 안전을 보장할 수 있습니다.

다음 표에서는 열려 있는 포트의 세부 정보를 설명합니다.

* TCP v4/v6 포트 # *	* 방향 *	* 기능 *
8143	인바운드	REST API용 HTTPS 연결
8043을 참조하십시오	인바운드	HTTPS 연결
9060입니다	인바운드	HTTPS 연결 HTTPS 연결을 통한 SOAP+에 사용됩니다 클라이언트가 ONTAP 도구 API 서버에 연결할 수 있도록 하려면 이 포트를 열어야 합니다.
22	인바운드	SSH(기본적으로 비활성화됨)
9080입니다	인바운드	HTTPS 연결 - VP 및 SRA - 루프백에서만 내부 연결
9083	인바운드	HTTPS 연결 - VP 및 SRA+ HTTPS 연결을 통한 SOAP에 사용됩니다
1162	인바운드	VP SNMP 트랩 패킷입니다
8443	인바운드	원격 플러그인
1527년	내부 전용	Derby 데이터베이스 포트, 이 컴퓨터와 자체 사이에서만 외부 연결이 허용되지 않음 - 내부 연결만 해당
8150입니다	내부 전용	로그 무결성 서비스가 포트에서 실행됩니다
443	양방향	ONTAP 클러스터에 연결하는 데 사용됩니다

### Derby 데이터베이스에 대한 원격 액세스 제어

관리자는 다음 명령을 사용하여 derby 데이터베이스에 액세스할 수 있습니다. ONTAP 도구 로컬 VM 및 원격 서버를

통해 다음 단계에 따라 액세스할 수 있습니다.

```
java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;  
connect 'jdbc:derby://<OTV-  
IP>:1527//opt/netapp/vpserver/vvoldb;user=<user>;password=<password>';
```

\*example: \*

```
root@UnifiedVSC:~# java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;  
ij version 10.15  
ij> connect 'jdbc:derby://localhost:1527//opt/netapp/vpserver/vvoldb;user=app;password=██████████';  
ij> show tables;  
TABLE_SCHEM | TABLE_NAME | REMARKS  
-----  
SYS | SYSALIASES |  
SYS | SYSCHECKS |  
SYS | SYSCOLPERMS |  
SYS | SYSCOLUMNS |  
SYS | SYSCONGLOMERATES |  
SYS | SYSCONSTRAINTS |  
SYS | SYSDEPENDS |  
SYS | SYSFILES |  
SYS | SYSFORIGNKEYS |  
SYS | SYSKEYS |  
SYS | SYSPERMS |
```

## VMware vSphere 액세스 지점용 ONTAP 툴(사용자)

VMware vSphere용 ONTAP 툴은 세 가지 유형의 사용자를 생성하고 사용합니다.

1. 시스템 사용자: 루트 사용자 계정입니다
2. 애플리케이션 사용자: 관리자 사용자, 유지보수 사용자 및 DB 사용자 계정
3. 지원 사용자: diag 사용자 계정입니다

### 1. 시스템 사용자

시스템 (루트) 사용자는 기본 운영 체제 (데비안)에 ONTAP 도구 설치로 생성됩니다.

- 기본 시스템 사용자 "root"는 ONTAP 도구 설치로 데비안에 생성됩니다. 기본값은 비활성화되며 '이전' 콘솔을 통해 애드혹 방식으로 활성화할 수 있습니다.

### 응용 프로그램 사용자

응용 프로그램 사용자의 이름은 ONTAP 도구에서 로컬 사용자로 지정됩니다. ONTAP 도구 응용 프로그램에서 만든 사용자입니다. 아래 표에는 애플리케이션 사용자 유형이 나와 있습니다.

* 사용자 *	* 설명 *
관리자 사용자	ONTAP 도구를 설치하는 동안 생성되며 사용자가 ONTAP 도구를 배포하는 동안 자격 증명을 제공합니다. 사용자는 '이전' 콘솔에서 '암호'를 변경할 수 있습니다. 암호는 90일 후에 만료되며 사용자는 동일하게 변경해야 합니다.

* 사용자 *	* 설명 *
유지보수 사용자	ONTAP 도구를 설치하는 동안 생성되며 사용자가 ONTAP 도구를 배포하는 동안 자격 증명을 제공합니다. 사용자는 '이전' 콘솔에서 '암호'를 변경할 수 있습니다. 이 사용자는 유지 관리 사용자이며 유지 관리 콘솔 작업을 실행하기 위해 생성됩니다.
데이터베이스 사용자	ONTAP 도구를 설치하는 동안 생성되며 사용자가 ONTAP 도구를 배포하는 동안 자격 증명을 제공합니다. 사용자는 '이전' 콘솔에서 '암호'를 변경할 수 있습니다. 암호는 90일 후에 만료되며 사용자는 동일하게 변경해야 합니다.

## 사용자 지원(diag 사용자)

ONTAP 도구를 설치하는 동안 지원 사용자가 생성됩니다. 이 사용자는 서버의 문제나 중단이 발생할 경우 ONTAP 도구에 액세스하고 로그를 수집하는 데 사용할 수 있습니다. 기본적으로 이 사용자는 비활성화되어 있지만 '이전' 콘솔을 통해 애드혹 방식으로 활성화할 수 있습니다. 이 사용자는 특정 시간이 지나면 자동으로 비활성화됩니다.

## 상호 TLS(인증서 기반 인증)

ONTAP 버전 9.7 이상에서는 상호 TLS 통신을 지원합니다. VMware 및 vSphere 9.12용 ONTAP 툴부터 상호 TLS는 새로 추가된 클러스터와의 통신에 사용됩니다(ONTAP 버전에 따라 다름).

## ONTAP

이전에 추가한 모든 스토리지 시스템에 대해 업그레이드 중에 추가된 모든 스토리지 시스템이 자동으로 신뢰되고 인증서 기반 인증 메커니즘이 구성됩니다.

아래 스크린샷과 같이 클러스터 설정 페이지에는 각 클러스터에 대해 구성된 상호 TLS(인증서 기반 인증) 상태가 표시됩니다.

Name	Type	IP Address	ONTAP Release	Status	Capacity	NFS VAAI	Supported Protocols
Cl_sti21-vs1m-ucs58im_1678878260	Cluster	10.234.85.142	9.12.0	Normal	20.42%		

### \* 클러스터 추가 \*

클러스터 추가 워크플로우 중에 추가되는 클러스터가 MTLS를 지원하는 경우 MTLS는 기본적으로 구성됩니다. 사용자는 이에 대해 구성을 수행할 필요가 없습니다. 아래 스크린샷은 클러스터 추가 중 사용자에게 표시되는 화면을 보여 줍니다.

## Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server 10.224.58.52 ▼

Name or IP address:

\_\_\_\_\_

Username:

\_\_\_\_\_

Password:

\_\_\_\_\_

Port:

443

Advanced options ▲

ONTAP Cluster  
Certificate:

Automatically fetch  Manually upload

CANCEL

ADD



## Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server	10.224.58.52 
Name or IP address:	10.234.85.142
Username:	admin
Password:	.....
Port:	443
Advanced options	

CANCEL

ADD

## Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

10.234.85.52

### Authorize Cluster Certificate

Host 10.234.85.142 has identified itself with a self-signed certificate.

[Show certificate](#)

Do you want to trust this certificate?

NO

YES

CANCEL

ADD

## Authorize Cluster Certificate

Host 10.234.85.142 has identified itself with a self-signed certificate.

[Hide certificate](#)

### Certificate Information

This certificate identifies the 10.234.85.142 host.

#### Issued By

**Name (CN or DN):** C1\_sti21-vsimsim-ucs581m\_1678878260

#### Issued To

**Name (CN or DN):** C1\_sti21-vsimsim-ucs581m\_1678878260

#### Validity

**Issued On:** 03/15/2023 11:16:06

**Expires On:** 03/14/2024 11:16:06

#### Fingerprint Information

**SHA-1 Fingerprint:** 2C:38:E3:5C:4B:F3:5D:3F:39:C8:CE:4A:8  
2:C1:A6:EE:34:53:A0:F3

**SHA-256 Fingerprint:** 05:0F:FE:CD:B0:C6:FC:6F:EB:8A:FC:86:F  
7:E3:EF:D4:8D:CA:02:92:9B:E1:A4:70:84:  
52:F8:76:98:64:FA:23

Do you want to trust this certificate?

NO

YES

### 클러스터 편집

클러스터 편집 작업 중에 다음과 같은 두 가지 시나리오가 있습니다.

- ONTAP 인증서가 만료되면 사용자는 새 인증서를 얻고 업로드해야 합니다.
- OTV 인증서가 만료되면 사용자는 확인란을 선택하여 인증서를 다시 생성할 수 있습니다.
  - \_ONTAP에 대한 새 클라이언트 인증서를 생성합니다

# Modify Storage System

Settings   Provisioning Options

IP address or hostname:  ▼

Port:

Username:

Password:

Upload Certificate (Optional)  [BROWSE](#)

Skip monitoring of this storage system

Generate a new client certificate for ONTAP

CANCEL

OK



## ONTAP 도구 HTTPS 인증서

기본적으로 ONTAP 도구는 웹 UI에 대한 HTTPS 액세스를 보호하기 위해 설치 중에 자동으로 만들어진 자체 서명 인증서를 사용합니다. ONTAP 도구는 다음과 같은 기능을 제공합니다.

1. HTTPS 인증서를 다시 생성합니다

ONTAP 도구를 설치하는 동안 HTTPS CA 인증서가 설치되고 인증서가 키 저장소에 저장됩니다. 사용자는 유지 관리 콘솔을 통해 HTTPS 인증서를 다시 생성할 수 있습니다.

위의 옵션은 \_'응용 프로그램 구성' → '인증서 다시 생성'.\_으로 이동하여 \_maint\_console에서 액세스할 수 있습니다

## 로그인 배너

다음 로그인 배너는 사용자가 로그인 프롬프트에 사용자 이름을 입력하면 표시됩니다. SSH는 기본적으로 비활성화되어 있으며 VM 콘솔에서 활성화된 경우 1회 로그인만 허용합니다.

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.
```

사용자가 SSH 채널을 통해 로그인을 완료하면 다음 텍스트가 표시됩니다.

```
Linux UnifiedVSC 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21)
x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

## 비활성 시간 초과

무단 액세스를 방지하기 위해 비활성 시간 제한이 설정되며, 이 시간 제한은 승인된 리소스를 사용하는 동안 특정 기간 동안 비활성 상태인 사용자를 자동으로 로그아웃시킵니다. 이렇게 하면 권한이 있는 사용자만 리소스에 액세스할 수 있으며 보안을 유지하는 데 도움이 됩니다.

- 기본적으로 vSphere Client 세션은 120분 동안 유효 시간이 지나면 닫히므로 사용자가 다시 로그인하여 클라이언트 사용을 재개해야 합니다. `webclient.properties` 파일을 편집하여 시간 초과 값을 변경할 수 있습니다. vSphere Client의 시간 초과를 구성할 수 있습니다 "[vSphere Client Timeout 값을 구성합니다](#)"
- ONTAP 도구의 웹 CLI 세션 로그아웃 시간은 30분입니다.

## 사용자당 최대 동시 요청 수(네트워크 보안 보호::DOS 공격)

기본적으로 사용자당 최대 동시 요청 수는 48개입니다. ONTAP 도구의 루트 사용자는 해당 환경의 요구 사항에 따라 이 값을 변경할 수 있습니다. 이 값은 서비스 거부(DOS) 공격에 대한 메커니즘을 제공하므로 매우 높은 값으로 설정하지 않아야 합니다.

사용자는 `*/opt/netapp/vscserver/etc/dosfilterParams.json` \* 파일에서 최대 동시 세션 및 기타 지원되는 매개 변수의 수를 변경할 수 있습니다.

다음 매개 변수를 사용하여 필터를 구성할 수 있습니다.

- `*delayms*` : 고려되기 전에 속도 제한을 초과하는 모든 요청에 주어진 지연 시간(밀리초)입니다. 요청을 거부하려면 -1을 지정합니다.
- `*thromlems*` : 세마포에 대한 비동기 대기 시간.

- *\*maxRequests\**: 이 요청을 실행할 수 있는 기간입니다.
- *\*ipWhitelist\**: 속도 제한이 없는 침표로 구분된 IP 주소 목록입니다. (vCenter, ESXi 및 SRA IP일 수 있음)
- *\*maxRequestsPerSec\**: 초당 연결의 최대 요청 수입니다.
- *\_dosfilterParams* 파일의 기본값 *\_:*\*

```
{ "delayMs": "-1",
  "throttleMs": "1800000",
  "maxRequestMs": "300000",
  "ipWhitelist": "10.224.58.52",
  "maxRequestsPerSec": "48" }
```

## NTP(Network Time Protocol) 구성

경우에 따라 네트워크 시간 구성의 불일치로 인해 보안 문제가 발생할 수 있습니다. 이러한 문제를 방지하려면 네트워크 내의 모든 장치에 정확한 시간 설정이 있는지 확인하는 것이 중요합니다.

### \* 가상 어플라이언스 \*

가상 어플라이언스의 유지 관리 콘솔에서 NTP 서버를 구성할 수 있습니다. 사용자는 시스템 구성⇒\_새 NTP 서버 추가\_옵션에서 NTP 서버 세부 정보를 추가할 수 있습니다

기본적으로 NTP에 대한 서비스는 ntpd입니다. 이 서비스는 레거시 서비스이며 일부 경우 가상 시스템에서 제대로 작동하지 않습니다.

### \* 데비안 \*

데비안에서 사용자는 /etc/ntp.conf 파일에 액세스하여 NTP 서버 세부 정보를 확인할 수 있습니다.

## 암호 정책

ONTAP 도구를 처음 배포하거나 버전 9.12 이상으로 업그레이드하는 사용자는 관리자와 데이터베이스 사용자 모두에 대해 강력한 암호 정책을 따라야 합니다. 배포 프로세스 중에 새 사용자에게 암호를 입력하라는 메시지가 표시됩니다. 버전 9.12 이상으로 업그레이드하는 Brownfield 사용자의 경우 유지 관리 콘솔에서 강력한 암호 정책을 따르는 옵션을 사용할 수 있습니다.

- 사용자가 유지 관리 콘솔에 로그인하면 복잡한 규칙 집합에 대해 암호가 확인되고, 따르지 않을 경우 사용자에게 동일한 암호를 재설정하라는 메시지가 표시됩니다.
- 암호 기본 유효 기간은 90일이며 75일 후에는 사용자가 암호 변경 알림을 받기 시작합니다.
- 모든 사이클에서 새 암호를 설정해야 합니다. 시스템에서는 마지막 암호를 새 암호로 사용하지 않습니다.
- 사용자가 유지 관리 콘솔에 로그인할 때마다 기본 메뉴를 로드하기 전에 아래 스크린샷과 같은 암호 정책을 확인합니다.

```
Maintenance Console : "Netapp ONTAP tools for VMware vSphere"
Discovered interfaces: eth0 (ENABLED)
validating password policies
```

- 암호 정책 또는 ONTAP tools 9.11 또는 이전 버전에서 업그레이드 설정을 따르지 않는 경우. 그런 다음 사용자가 암호를 재설정하는 다음 화면을 볼 수 있습니다.

```
Your Administrator and Database password is expired or does not match password policy:
-----
1 ) Change 'administrator' user password
2 ) Change database password
x ) Exit
Enter your choice: _
```

- 사용자가 약한 암호를 설정하려고 하거나 마지막 암호를 다시 입력하면 다음 오류가 표시됩니다.

```
Changing password for administrator.
User: administrator
Enter new password:
Retype new password:
Password doesn't matches the password policy.
For security reasons, it is recommended to use a password that is of eight to thirty characters and
contains a minimum of one upper, one lower, one digit, and one special character.
Enter new password:
Retype new password:
Check if new decoder works ?
New decoder worked successfully
08-02/23 13:36:53 Your new password must be different
Error updating sra credential file
Press ENTER to continue._
```



## 저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 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.