



# ARP 활성화

## ONTAP 9

NetApp  
February 12, 2026

# 목차

ARP 활성화 .....	1
볼륨에서 ONTAP 자율형 랜섬웨어 보호 기능을 활성화합니다 .....	1
NAS FlexVol 볼륨에서 ARP 활성화 .....	2
NAS FlexGroup 볼륨에서 ARP 활성화 .....	4
SAN 볼륨에서 ARP 활성화 .....	7
관련 정보 .....	8
새 볼륨에서 ONTAP 자율적 랜섬웨어 방어 기능을 기본적으로 활성화합니다 .....	8
ONTAP 자율형 랜섬웨어 보호 기능의 기본 활성화를 해제합니다 .....	11

# ARP 활성화

## 볼륨에서 **ONTAP** 자율형 랜섬웨어 보호 기능을 활성화합니다

ONTAP 9.10.1부터 기존 볼륨에서 ARP(자율적 랜섬웨어 방어)를 활성화하거나 새 볼륨을 생성한 후 처음부터 ARP를 활성화할 수 있습니다.

이 작업에 대해

ARP를 활성화하려면 환경에 맞는 절차를 따르십시오. [귀하의 환경이 특정 요구 사항을 충족하는지 확인하십시오.](#) :

- [FlexVol 볼륨이 있는 NAS](#)
- [FlexGroup 볼륨이 있는 NAS](#)
- [SAN 볼륨](#)

ARP를 활성화한 후 환경과 ONTAP 버전에 따라 ARP가 전환 기간에 들어갈 수 있습니다.

볼륨 유형입니다	ONTAP 버전입니다	활성화 후의 동작
NAS FlexGroup	ONTAP 9.18.1 이상	ARP/AI는 학습 기간 없이 즉시 활성화됩니다.
	ONTAP 9.13.1부터 9.17.1까지	ARP는 30일 동안 학습 모드로 시작됩니다.
NAS FlexVol	ONTAP 9.16.1 이상	ARP/AI는 학습 기간 없이 즉시 활성화됩니다.
	ONTAP 9.10.1부터 9.15.1까지	ARP는 30일 동안 학습 모드로 시작됩니다.
SAN 볼륨	ONTAP 9.17.1 이상	ARP/AI는 즉시 활성화되어 초기 보수적 임계값에서 전환하기 전에 적절한 경고 임계값을 설정하기 위한 평가 기간을 시작합니다.

시작하기 전에

ARP를 활성화하기 전에 환경에 다음 사항이 있는지 확인하세요.

### NAS 특정 요구 사항

- NFS 또는 SMB(또는 둘 다) 프로토콜이 활성화된 스토리지 VM(SVM)입니다.
- 클라이언트가 구성된 NAS 작업 부하.
- 활동적인 ["접합 경로"](#) 볼륨을 위해서.

### SAN 특정 요구 사항

- iSCSI, FC 또는 NVMe 프로토콜이 활성화된 스토리지 VM(SVM).
- 클라이언트가 구성된 SAN 워크로드.

일반 요구 사항

- 그만큼 [올바른 라이선스입니다](#) ONTAP 버전용입니다.
- (권장) 다중 관리자 검증(MAV)이 활성화되어 있습니다(ONTAP 9.13.1 이상). 보다 ["다중 관리 검증을 활성화합니다"](#) .

## NAS FlexVol 볼륨에서 **ARP** 활성화

System Manager나 ONTAP CLI를 사용하여 NAS FlexVol 볼륨에서 ARP를 활성화할 수 있습니다. 해당 프로세스는 ONTAP 버전에 따라 다릅니다.

### ONTAP 9.16.1 이상

ONTAP 9.16.1부터 ARP/AI는 학습 기간 없이 즉시 활성화됩니다.

시스템 관리자

1. 스토리지 > 볼륨 \* 을 선택한 다음 보호할 볼륨을 선택합니다.
2. 볼륨 \* 개요의 \* 보안 \* 탭에서 \* 상태 \* 를 선택하여 비활성화에서 활성화로 전환합니다.
3. 랜섬웨어 방지 상자에서 볼륨의 ARP 상태를 확인하세요.

모든 볼륨에 대한 ARP 상태를 표시하려면 \* Volumes \* 창에서 \* Show/Hide \* 를 선택한 다음 \* Anti-Ransomware \* 상태가 선택되어 있는지 확인합니다.

CLI를 참조하십시오

기존 볼륨에서 **ARP** 활성화:

```
security anti-ransomware volume enable -volume <vol_name> -vserver  
<svm_name>
```

**ARP**가 활성화된 새 볼륨을 만듭니다.

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate  
<aggr_name> -size <nn> -anti-ransomware-state enabled -junction-path  
</path_name>
```

**ARP** 상태 확인:

```
security anti-ransomware volume show
```

에 대한 자세한 내용은 `security anti-ransomware volume show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

### ONTAP 9.10.1부터 9.15.1까지

ONTAP 9.10.1~9.15.1의 경우 처음에 ARP를 활성화해야 합니다. **"학습 모드"** (또는 "테스트 실행" 상태). 시스템은 작업 부하를 분석하여 정상적인 동작을 특성화합니다. 활성 모드에서 시작하면 과도한 오탐지 보고가 발생할 수 있습니다.

ARP를 최소 30일 동안 학습 모드로 실행하는 것이 좋습니다. ONTAP 9.13.1부터 ARP는 최적의 학습 기간 간격을 자동으로 결정하고 전환을 자동화하며, 이는 30일 전에 실행될 수 있습니다.

시스템 관리자

1. 스토리지 > 볼륨 \* 을 선택한 다음 보호할 볼륨을 선택합니다.
2. 볼륨 \* 개요의 \* 보안 \* 탭에서 \* 상태 \* 를 선택하여 비활성화에서 활성화로 전환합니다.
3. 랜섬웨어 방지 상자에서 \*학습 모드에서 활성화\*를 선택합니다.



당신은 할 수 있습니다"연관된 스토리지 VM에서 자동 학습을 활성 모드로 전환하는 것을 비활성화합니다." 학습 모드에서 활성 모드로의 전환을 수동으로 제어하려는 경우.



기존 볼륨에서 학습 및 활성 모드는 볼륨의 기존 데이터가 아닌 새로 기록된 데이터에만 적용됩니다. ARP에 대해 볼륨이 활성화된 후 새 데이터를 기반으로 이전 일반 데이터 트래픽의 특성이 가정되기 때문에 기존 데이터는 스캔되고 분석되지 않습니다.

#### 4. 랜섬웨어 방지 상자에서 볼륨의 ARP 상태를 확인하세요.

모든 볼륨에 대한 ARP 상태를 표시하려면 \* Volumes \* 창에서 \* Show/Hide \* 를 선택한 다음 \* Anti-Ransomware \* 상태가 선택되어 있는지 확인합니다.

#### CLI를 참조하십시오

기존 볼륨에서 **ARP** 활성화:

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver
<svm_name>
```

에 대한 자세한 내용은 security anti-ransomware volume dry-run "ONTAP 명령 참조입니다"을 참조하십시오.

**ARP**가 활성화된 새 볼륨을 만듭니다.

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state dry-run -junction-path
</path_name>
```

자동 전환 비활성화(선택 사항):

ONTAP 9.13.1부터 ONTAP 9.15.1까지 업그레이드하고 연관된 모든 볼륨에 대해 학습 모드에서 활성 모드로의 전환을 수동으로 제어하려는 경우 SVM에서 다음 작업을 수행할 수 있습니다.

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

**ARP** 상태 확인:

```
security anti-ransomware volume show
```

## NAS FlexGroup 볼륨에서 **ARP** 활성화

System Manager나 ONTAP CLI를 사용하여 NAS FlexGroup 볼륨에서 ARP를 활성화할 수 있습니다. 해당

프로세스는 ONTAP 버전에 따라 다릅니다.

### ONTAP 9.18.1 이상

ONTAP 9.18.1부터 ARP/AI는 학습 기간이 필요 없이 FlexGroup 볼륨에 대해 즉시 활성화됩니다.

시스템 관리자

1. \*저장소 > 볼륨\*을 선택한 다음 보호하려는 FlexGroup 볼륨을 선택합니다.
2. 볼륨 \* 개요의 \* 보안 \* 탭에서 \* 상태 \* 를 선택하여 비활성화에서 활성화로 전환합니다.
3. 랜섬웨어 방지 상자에서 볼륨의 ARP 상태를 확인하세요.

모든 볼륨에 대한 ARP 상태를 표시하려면 \* Volumes \* 창에서 \* Show/Hide \* 를 선택한 다음 \* Anti-Ransomware \* 상태가 선택되어 있는지 확인합니다.

CLI를 참조하십시오

기존 **FlexGroup** 볼륨에서 **ARP** 활성화:

```
security anti-ransomware volume enable -volume <vol_name> -vserver  
<svm_name>
```

**ARP**가 활성화된 새로운 **FlexGroup** 볼륨을 만듭니다.

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list  
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti  
-ransomware-state enabled -junction-path </path_name>
```

**ARP** 상태 확인:

```
security anti-ransomware volume show
```

### ONTAP 9.13.1부터 9.17.1까지

ONTAP 9.13.1~9.17.1의 경우 FlexGroup 볼륨은 다음에서 시작됩니다. **"학습 모드"**. 시스템은 작업 부하를 분석하여 정상적인 동작을 특성화합니다.

ARP를 최소 30일 동안 학습 모드로 실행하는 것이 좋습니다. ARP는 최적의 학습 기간 간격을 자동으로 결정하고 30일 전에 전환이 자동화될 수 있습니다.

시스템 관리자

1. \*저장소 > 볼륨\*을 선택한 다음 보호하려는 FlexGroup 볼륨을 선택합니다.
2. 볼륨 \* 개요의 \* 보안 \* 탭에서 \* 상태 \* 를 선택하여 비활성화에서 활성화로 전환합니다.
3. 랜섬웨어 방지 상자에서 \*학습 모드에서 활성화\*를 선택합니다.



당신은 할 수 있습니다 **"자동 학습에서 활성 모드로의 전환 비활성화"** 학습 모드에서 활성 모드로의 전환을 수동으로 제어하려는 경우.



#### 4. 랜섬웨어 방지 상자에서 볼륨의 ARP 상태를 확인하세요.

CLI를 참조하십시오

기존 **FlexGroup** 볼륨에서 **ARP** 활성화:

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver  
<svm_name>
```

**ARP**가 활성화된 새로운 **FlexGroup** 볼륨을 만듭니다.

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list  
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti  
-ransomware-state dry-run -junction-path </path_name>
```

자동 전환 비활성화(선택 사항):

학습 모드에서 활성 모드로의 전환을 수동으로 제어하려면 다음을 수행하세요.

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to  
-enabled false
```

**ARP** 상태 확인:

```
security anti-ransomware volume show
```

## SAN 볼륨에서 **ARP** 활성화

ONTAP 9.17.1부터 SAN 볼륨에서 ARP를 활성화할 수 있습니다. ARP/AI 기능은 자동으로 활성화되며 SAN 볼륨을 적극적으로 모니터링하고 보호하기 시작합니다. "평가 기간" 동시에 워크로드가 ARP에 적합한지 확인하고 감지를 위한 최적의 암호화 임계값을 설정합니다.

System Manager나 ONTAP CLI를 사용하여 SAN 볼륨에서 ARP를 활성화할 수 있습니다.

시스템 관리자

단계

1. \*저장소 > 볼륨\*을 선택한 다음 보호하려는 SAN 볼륨을 선택합니다.
2. 볼륨 \* 개요의 \* 보안 \* 탭에서 \* 상태 \* 를 선택하여 비활성화에서 활성화로 전환합니다.
3. ARP/AI는 자동으로 평가 기간에 들어갑니다.
4. 랜섬웨어 방지 상자에서 ARP 상태와 평가 상태를 확인하세요.

모든 볼륨에 대한 ARP 상태를 표시하려면 \* Volumes \* 창에서 \* Show/Hide \* 를 선택한 다음 \* Anti-Ransomware \* 상태가 선택되어 있는지 확인합니다.

CLI를 참조하십시오

기존 **SAN** 볼륨에서 **ARP** 활성화:

```
security anti-ransomware volume enable -volume <vol_name> -vserver  
<svm_name>
```

**ARP**가 활성화된 새 **SAN** 볼륨을 만듭니다.

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate  
<aggr_name> -size <nn> -anti-ransomware-state enabled
```

**ARP** 상태 및 평가 상태 확인:

```
security anti-ransomware volume show
```

확인하다 Block device detection status 평가 기간 진행 상황을 모니터링하는 필드입니다.

에 대한 자세한 내용은 security anti-ransomware volume show ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

## 관련 정보

- ["학습 기간 후 활성화 모드로 전환합니다"](#)

## 새 볼륨에서 **ONTAP** 자율적 랜섬웨어 방어 기능을 기본적으로 활성화합니다

ONTAP 9.10.1부터 스토리지 VM(SVM)을 구성하여 새 볼륨이 Autonomous Ransomware Protection(ARP)으로 기본적으로 설정되도록 할 수 있습니다. System Manager 또는 ONTAP CLI를 사용하여 이 설정을 수정할 수 있습니다.

ONTAP 9.18.1부터 클러스터 업그레이드 또는 새 설치 후 12시간의 유예 기간이 지나면 "지원되는 시스템"에 대해 클러스터 수준에서 모든 새 볼륨에 대해 ARP가 기본적으로 활성화됩니다. 클러스터 수준에서 ARP의 자동 기본 활성화를 비활성화하더라도 SVM 수준에서 모든 새 볼륨에 대해 ARP를 수동으로 기본적으로 활성화하도록 선택할 수 있습니다.

ONTAP 9.17.1 이하 버전에서는 SVM 수준에서 구성하는 것이 새 볼륨에서 ARP를 기본적으로 활성화하는 유일한 방법입니다.

이 작업에 대해

기본적으로 새 볼륨은 ARP 기능이 비활성화된 상태로 생성됩니다. SVM에서 생성된 새 볼륨에서 기본적으로 ARP 기능을 활성화하고 활성화되도록 설정해야 합니다.

ARP가 활성화되지 않은 기존 볼륨은 SVM의 기본값을 변경해도 ARP 활성화 상태가 자동으로 변경되지 않습니다. 이 절차에 설명된 SVM 설정 변경 사항은 새 볼륨에만 영향을 미칩니다. 방법을 배우십시오 "[기존 볼륨에 대해 ARP를 활성화합니다](#)".

ARP를 활성화한 후 환경과 ONTAP 버전에 따라 ARP가 전환 기간에 들어갈 수 있습니다.

볼륨 유형입니다	ONTAP 버전입니다	활성화 후의 동작
NAS FlexGroup	ONTAP 9.18.1 이상	ARP/AI는 학습 기간 없이 즉시 활성화됩니다.
	ONTAP 9.13.1부터 9.17.1까지	ARP는 30일 동안 학습 모드로 시작됩니다.
NAS FlexVol	ONTAP 9.16.1 이상	ARP/AI는 학습 기간 없이 즉시 활성화됩니다.
	ONTAP 9.10.1부터 9.15.1까지	ARP는 30일 동안 학습 모드로 시작됩니다.
SAN 볼륨	ONTAP 9.17.1 이상	ARP/AI는 즉시 활성화되어 초기 보수적 임계값에서 전환하기 전에 적절한 경고 임계값을 설정하기 위한 평가 기간을 시작합니다.

시작하기 전에

ARP를 활성화하기 전에 환경에 다음 사항이 있는지 확인하세요.

#### NAS 특정 요구 사항

- NFS 또는 SMB(또는 둘 다) 프로토콜이 활성화된 스토리지 VM(SVM)입니다.
- 활동적인 "[접합 경로](#)" 볼륨을 위해서.

#### SAN 특정 요구 사항

- iSCSI, FC 또는 NVMe 프로토콜이 활성화된 스토리지 VM(SVM).


일반 요구 사항

- 그만큼 "[올바른 라이선스입니다](#)" ONTAP 버전용입니다.
- (권장) 다중 관리자 검증(MAV)이 활성화되었습니다(ONTAP 9.13.1+). 보다 "[다중 관리 검증을 활성화합니다](#)".

단계

시스템 관리자 또는 ONTAP CLI를 사용하여 새 볼륨에 대해 기본적으로 ARP를 활성화할 수 있습니다.

## 시스템 관리자

1. 환경에 따라 저장소 또는 \*클러스터\*를 선택하고, \*저장소 VM\*을 선택한 다음 ARP로 보호하려는 볼륨이 포함된 저장소 VM을 선택합니다.
2. 설정 탭으로 이동합니다. 보안\*에서 \*랜섬웨어 방지 타일을 찾아 선택합니다.  .
3. 랜섬웨어 방지(ARP)를 활성화하려면 확인란을 선택하세요. 스토리지 VM의 모든 적격 볼륨에서 ARP를 활성화하려면 추가 확인란을 선택하세요.
4. 권장 학습 기간이 있는 ONTAP 버전의 경우, \*충분한 학습 후 학습 모드에서 활성 모드로 자동 전환\*을 선택하세요. 이를 통해 ARP가 최적의 학습 기간 간격을 결정하고 활성 모드로 자동 전환할 수 있습니다.

## CLI를 참조하십시오

새 볼륨에서 기본적으로 **ARP**를 활성화하도록 기존 **SVM** 수정

선택하다 dry-run ARP 버전에 다음이 필요한 경우 **학습 기간** . 그렇지 않으면 선택하십시오 enabled .

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume  
-state <dry-run|enabled>
```

새 볼륨에 대해 기본적으로 **ARP**가 활성화된 새 **SVM**을 만듭니다.

선택하다 dry-run ARP 버전에 다음이 필요한 경우 **학습 기간** . 그렇지 않으면 선택하십시오 enabled .

```
vserver create -vserver <svm_name> -anti-ransomware-default-volume  
-state <dry-run|enabled>
```

기존 **SVM**을 수정하여 자동 학습을 활성 모드로 전환하지 않도록 합니다.

ONTAP 9.15.1을 통해 ONTAP 9.13.1로 업그레이드했고 기본 상태가 다음과 같은 경우 dry-run (학습모드)에서는 적응학습이 활성화되어 변경이 가능합니다. enabled 상태(활성 모드)는 자동으로 수행됩니다. 이 자동 스위치를 비활성화하면 연관된 모든 볼륨에 대해 학습 모드에서 활성 모드로의 전환을 수동으로 제어할 수 있습니다.

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to  
-enabled false
```

## ARP 상태 확인

```
security anti-ransomware volume show
```

## 관련 정보

- "학습 기간 후 활성 모드로 전환합니다"
- "보안 랜섬웨어 볼륨 보기"

## ONTAP 자율형 랜섬웨어 보호 기능의 기본 활성화를 해제합니다

ONTAP 9.18.1부터 ARP 라이선스가 설치되어 있는 경우 업그레이드 또는 새로 설치한 후 12시간의 워밍업 기간이 지나면 AFF A-series 및 AFF C-series, ASA, ASA r2 시스템의 모든 새 볼륨에서 ARP(Autonomous Ransomware Protection)가 기본적으로 자동으로 활성화됩니다. System Manager 또는 ONTAP CLI를 사용하여 12시간 유예 기간 중 또는 이후에 이 기본 활성화를 해제할 수 있습니다.



기존 볼륨은 ARP용 "수동으로 활성화됨"이어야 합니다.

이 작업에 대해


이 절차에 대해 선택한 설정은 나중에 변경할 수 있습니다. 유예 기간 이후에는 언제든지 기본 활성화 기능을 켜거나 끌 수 있습니다.

```
security anti-ransomware auto-enable modify -new-volume-auto-enable  
false|true
```

단계

System Manager 또는 ONTAP CLI를 사용하여 ARP 기본 활성화 옵션을 관리할 수 있습니다.

## 시스템 관리자

1. 클러스터 > 설정 \* 을 선택합니다.
2. 다음 중 하나를 수행합니다.
  - 활성화 유예 기간 동안 비활성화:
    - i. 랜섬웨어 방지 섹션에서 ARP가 활성화되기까지 남은 시간을 나타내는 메시지가 표시됩니다. \*활성화 안 함\*을 선택합니다.
    - ii. 다음 대화 상자에서 \*Disable\*을 선택하여 새 볼륨에 대한 기본 ARP 활성화가 해제되었는지 확인하십시오.
  - 유예 기간 후 비활성화:
    - i. 랜섬웨어 방지 섹션에서  를 선택하세요.
    - ii. 확인란을 선택한 다음 \*저장\*을 클릭하여 새 볼륨에 대한 기본 ARP 활성화를 비활성화합니다.

## CLI를 참조하십시오

1. 기본 활성화 상태를 확인합니다.

```
security anti-ransomware auto-enable show
```

2. 새 볼륨에 대한 기본 활성화 비활성화:

```
security anti-ransomware auto-enable modify -new-volume-auto-enable  
false
```

## 관련 정보

- ["개별 볼륨에서 ONTAP 자율형 랜섬웨어 보호 기능을 활성화합니다"](#)

## 저작권 정보

Copyright © 2026 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.