



## 방화벽을 제어합니다

### StorageGRID 11.8

NetApp  
May 17, 2024

# 목차

방화벽을 제어합니다.....	1
외부 방화벽에서 액세스를 제어합니다.....	1
내부 방화벽 제어를 관리합니다.....	2
내부 방화벽을 구성합니다.....	5

# 방화벽을 제어합니다

## 외부 방화벽에서 액세스를 제어합니다

외부 방화벽에서 특정 포트를 열거나 닫을 수 있습니다.

외부 방화벽에서 특정 포트를 열거나 닫아 StorageGRID 관리 노드의 사용자 인터페이스 및 API에 대한 액세스를 제어할 수 있습니다. 예를 들어, 테넌트가 다른 방법을 사용하여 시스템 액세스를 제어하는 것 외에도 방화벽에서 Grid Manager에 연결할 수 없도록 할 수 있습니다.

StorageGRID 내부 방화벽을 구성하려면 를 참조하십시오 ["내부 방화벽을 구성합니다"](#).

포트	설명	포트가 열려 있는 경우...
443	관리 노드의 기본 HTTPS 포트	웹 브라우저 및 관리 API 클라이언트는 Grid Manager, Grid Management API, Tenant Manager 및 Tenant Management API에 액세스할 수 있습니다.  • 참고: * 포트 443은 일부 내부 트래픽에도 사용됩니다.
8443	관리 노드의 제한된 그리드 관리자 포트	• 웹 브라우저 및 관리 API 클라이언트는 HTTPS를 사용하여 그리드 관리자 및 그리드 관리 API에 액세스할 수 있습니다. • 웹 브라우저 및 관리 API 클라이언트는 테넌트 관리자 또는 테넌트 관리 API에 액세스할 수 없습니다. • 내부 콘텐츠 요청은 거부됩니다.
9443	관리 노드의 제한된 테넌트 관리자 포트	• 웹 브라우저 및 관리 API 클라이언트는 HTTPS를 사용하여 테넌트 관리자 및 테넌트 관리 API에 액세스할 수 있습니다. • 웹 브라우저 및 관리 API 클라이언트는 그리드 관리자 또는 그리드 관리 API에 액세스할 수 없습니다. • 내부 콘텐츠 요청은 거부됩니다.



제한된 Grid Manager 또는 테넌트 관리자 포트에서는 SSO(Single Sign-On)를 사용할 수 없습니다. 사용자가 SSO(Single Sign-On)로 인증하도록 하려면 기본 HTTPS 포트(443)를 사용해야 합니다.

### 관련 정보

- ["Grid Manager에 로그인합니다"](#)
- ["테넌트 계정을 생성합니다"](#)
- ["외부 통신"](#)

# 내부 방화벽 제어를 관리합니다

StorageGRID에는 노드에 대한 네트워크 액세스를 제어할 수 있도록 함으로써 그리드의 보안을 강화하는 각 노드에 대한 내부 방화벽이 포함되어 있습니다. 방화벽을 사용하여 특정 그리드 구축에 필요한 포트를 제외한 모든 포트의 네트워크 액세스를 방지합니다. 방화벽 제어 페이지에서 변경한 구성은 각 노드에 배포됩니다.

방화벽 제어 페이지의 세 가지 탭을 사용하여 그리드에 필요한 액세스를 사용자 지정합니다.

- \* 특별 권한 주소 목록 \*: 이 탭을 사용하면 닫힌 포트에 대한 선택된 액세스를 허용할 수 있습니다. 외부 액세스 관리 탭을 사용하여 닫은 포트에 액세스할 수 있는 IP 주소 또는 서브넷을 CIDR 표시법으로 추가할 수 있습니다.
- \* 외부 액세스 관리 \*: 이 탭을 사용하여 기본적으로 열려 있는 포트를 닫거나 이전에 닫은 포트를 다시 열 수 있습니다.
- \* 신뢰할 수 없는 클라이언트 네트워크 \*: 노드가 클라이언트 네트워크의 인바운드 트래픽을 신뢰하는지 여부를 지정하려면 이 탭을 사용합니다.

이 탭의 설정은 외부 액세스 관리 탭의 설정보다 우선합니다.

- 신뢰할 수 없는 클라이언트 네트워크가 있는 노드는 해당 노드에 구성된 로드 밸런서 엔드포인트 포트(글로벌, 노드 인터페이스 및 노드 유형 바운드 엔드포인트)의 연결만 받아들입니다.
- 부하 분산 장치 엔드포인트 포트 \_ 는(는) 신뢰할 수 없는 클라이언트 네트워크에서 외부 네트워크 관리 탭의 설정에 관계없이 열려 있는 유일한 포트입니다.
- 신뢰할 수 있는 경우 외부 액세스 관리 탭에서 열린 모든 포트와 클라이언트 네트워크에 열려 있는 모든 로드 밸런서 끝점에 액세스할 수 있습니다.



한 탭에서 설정한 내용은 다른 탭의 액세스 변경에 영향을 줄 수 있습니다. 모든 탭의 설정을 확인하여 네트워크가 예상한 대로 작동하는지 확인하십시오.

내부 방화벽 제어를 구성하려면 를 참조하십시오 ["방화벽 제어를 구성합니다"](#).

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 을 참조하십시오 ["외부 방화벽에서 액세스를 제어합니다"](#).

## 특별 권한 주소 목록 및 외부 액세스 관리 탭

특별 권한 주소 목록 탭을 사용하면 닫힌 그리드 포트에 대한 액세스 권한이 부여된 하나 이상의 IP 주소를 등록할 수 있습니다. 외부 액세스 관리 탭을 사용하면 선택한 외부 포트 또는 열려 있는 모든 외부 포트에 대한 외부 액세스를 닫을 수 있습니다(외부 포트는 기본적으로 비 그리드 노드가 액세스할 수 있는 포트입니다). 이러한 두 탭을 함께 사용하여 그리드에 필요한 정확한 네트워크 액세스를 사용자 지정할 수 있습니다.



권한이 있는 IP 주소는 기본적으로 내부 그리드 포트 액세스를 갖지 않습니다.

예 1: 유지 보수 작업에 점프 호스트를 사용합니다

네트워크 관리에 점프 호스트(보안 강화 호스트)를 사용하려는 경우를 가정해 보겠습니다. 다음과 같은 일반 단계를 사용할 수 있습니다.

1. 특별 권한 주소 목록 탭을 사용하여 점프 호스트의 IP 주소를 추가합니다.

## 2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단합니다.



포트 443 및 8443을 차단하기 전에 권한이 있는 IP 주소를 추가합니다. 사용자를 포함하여 현재 차단된 포트에 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다.

구성을 저장하면 이동 호스트를 제외한 모든 호스트에 대해 그리드의 관리 노드에 있는 모든 외부 포트가 차단됩니다. 그런 다음 점프 호스트를 사용하여 그리드에 대한 유지 관리 작업을 보다 안전하게 수행할 수 있습니다.

### 예 2: 그리드 관리자 및 테넌트 관리자에 대한 액세스를 제한합니다

보안상의 이유로 Grid Manager 및 Tenant Manager(사전 설정 포트)에 대한 액세스를 제한하려는 경우를 가정해 보겠습니다. 다음과 같은 일반 단계를 사용할 수 있습니다.

1. 외부 액세스 관리 탭의 토글을 사용하여 포트 443을 차단합니다.
2. 외부 액세스 관리 탭의 토글을 사용하여 포트 8443에 대한 액세스를 허용합니다.
3. 포트 9443에 액세스할 수 있도록 하려면 Manage external access(외부 액세스 관리) 탭의 토글을 사용하십시오.

구성을 저장한 후 호스트는 포트 443에 액세스할 수 없지만 포트 8443을 통해 Grid Manager와 포트 9443을 통해 테넌트 관리자를 액세스할 수는 있습니다.



포트 443, 8443 및 9443 은 Grid Manager 및 Tenant Manager에 대해 사전 설정된 포트입니다. 특정 Grid Manager 또는 Tenant 관리자에 대한 액세스를 제한하도록 포트를 전환할 수 있습니다.

### 예 3: 민감한 포트를 잠급니다

중요한 포트와 해당 포트의 서비스(예: 포트 22의 SSH)를 잠그려고 한다고 가정합니다. 다음과 같은 일반 단계를 사용할 수 있습니다.

1. 특별 권한 주소 목록 탭을 사용하여 서비스에 액세스해야 하는 호스트에만 액세스 권한을 부여합니다.
2. 외부 액세스 관리 탭을 사용하여 모든 포트를 차단합니다.



Grid Manager 및 Tenant Manager 액세스에 할당된 포트에 대한 액세스를 차단하기 전에 권한 있는 IP 주소를 추가합니다(사전 설정된 포트는 443 및 8443). 사용자를 포함하여 현재 차단된 포트에 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다.

구성을 저장하면 권한이 있는 주소 목록의 호스트에서 포트 22 및 SSH 서비스를 사용할 수 있습니다. 다른 모든 호스트는 요청이 어떤 인터페이스에서 제공되든 서비스에 대한 액세스가 거부됩니다.

### 예 4: 사용하지 않는 서비스에 대한 액세스를 비활성화합니다

네트워크 수준에서는 사용하지 않을 일부 서비스를 사용하지 않도록 설정할 수 있습니다. 예를 들어, Swift 액세스를 제공하지 않으면 다음과 같은 일반 단계를 수행합니다.

1. 외부 액세스 관리 탭의 토글을 사용하여 포트 18083을 차단합니다.
2. 외부 액세스 관리 탭의 토글을 사용하여 포트 18085를 차단합니다.

구성을 저장한 후에는 스토리지 노드가 더 이상 Swift 연결을 허용하지 않지만, 차단되지 않은 포트에서 다른 서비스에

대한 액세스를 계속 허용합니다.

## 신뢰할 수 없는 클라이언트 네트워크 탭

클라이언트 네트워크를 사용하는 경우 명시적으로 구성된 끝점에서만 인바운드 클라이언트 트래픽을 허용하여 악의적인 공격으로부터 StorageGRID를 보호할 수 있습니다.

기본적으로 각 그리드 노드의 클라이언트 네트워크는 `_trusted_` 입니다. 즉, 기본적으로 StorageGRID는 모든 그리드 노드에 대한 인바운드 연결을 신뢰합니다 ["사용 가능한 외부 포트"](#).

각 노드의 클라이언트 네트워크가 `_untrusted_`로 지정함으로써 StorageGRID 시스템에 대한 악의적인 공격의 위협을 줄일 수 있습니다. 노드의 클라이언트 네트워크를 신뢰할 수 없는 경우 노드는 로드 밸런서 끝점으로 명시적으로 구성된 포트의 인바운드 연결만 허용합니다. 을 참조하십시오 ["로드 밸런서 엔드포인트를 구성합니다"](#) 및 ["방화벽 제어를 구성합니다"](#).

### 예 1: 게이트웨이 노드는 HTTPS S3 요청만 허용합니다

게이트웨이 노드가 HTTPS S3 요청을 제외한 클라이언트 네트워크의 모든 인바운드 트래픽을 거부하도록 한다고 가정합니다. 다음과 같은 일반 단계를 수행합니다.

1. 에서 ["부하 분산 장치 엔드포인트"](#) 페이지에서 포트 443에서 HTTPS를 통해 S3에 대한 로드 밸런서 끝점을 구성합니다.
2. 방화벽 제어 페이지에서 신뢰할 수 없음 을 선택하여 게이트웨이 노드의 클라이언트 네트워크를 신뢰할 수 없도록 지정합니다.

구성을 저장한 후 게이트웨이 노드의 클라이언트 네트워크의 모든 인바운드 트래픽은 포트 443 및 ICMP 에코(ping) 요청의 HTTPS S3 요청을 제외하고 삭제됩니다.

### 예 2: 스토리지 노드가 S3 플랫폼 서비스 요청을 전송합니다

스토리지 노드에서 아웃바운드 S3 플랫폼 서비스 트래픽을 활성화하되 클라이언트 네트워크의 해당 스토리지 노드에 대한 인바운드 연결을 차단하려는 경우를 가정해 봅니다. 이 일반 단계를 수행합니다.

- 방화벽 제어 페이지의 신뢰할 수 없는 클라이언트 네트워크 탭에서 스토리지 노드의 클라이언트 네트워크를 신뢰할 수 없음을 나타냅니다.

구성을 저장한 후 스토리지 노드는 더 이상 클라이언트 네트워크에서 들어오는 트래픽을 허용하지 않지만 구성된 플랫폼 서비스 대상에 대한 아웃바운드 요청은 계속 허용합니다.

### 예 3: 그리드 관리자에 대한 액세스를 서브넷으로 제한

특정 서브넷에서만 Grid Manager 액세스를 허용한다고 가정합니다. 다음 단계를 수행합니다.

1. 관리 노드의 클라이언트 네트워크를 서브넷에 연결합니다.
2. 신뢰할 수 없는 클라이언트 네트워크 탭을 사용하여 클라이언트 네트워크를 신뢰할 수 없음으로 구성합니다.
3. 관리 인터페이스 로드 밸런서 엔드포인트를 생성할 때 port를 입력하고 포트가 액세스할 관리 인터페이스를 선택합니다.
4. 신뢰할 수 없는 클라이언트 네트워크에 대해 \* 예 \* 를 선택합니다.
5. 외부 액세스 관리 탭을 사용하여 모든 외부 포트(해당 서브넷 외부의 호스트에 대해 설정된 권한이 있는 IP 주소 포함 또는 제외)를 차단합니다.

구성을 저장한 후에는 지정한 서버넷의 호스트만 Grid Manager에 액세스할 수 있습니다. 다른 호스트는 모두 차단됩니다.

## 내부 방화벽을 구성합니다

StorageGRID 노드의 특정 포트에 대한 네트워크 액세스를 제어하도록 StorageGRID 방화벽을 구성할 수 있습니다.

시작하기 전에

- 를 사용하여 그리드 관리자에 로그인했습니다 ["지원되는 웹 브라우저"](#).
- 있습니다 ["특정 액세스 권한"](#).
- 에서 정보를 검토했습니다 ["방화벽 제어 관리"](#) 및 ["네트워킹 지침"](#).
- 관리자 노드 또는 게이트웨이 노드가 명시적으로 구성된 끝점에서만 인바운드 트래픽을 수락하도록 하려면 로드 밸런서 끝점을 정의해야 합니다.



클라이언트 네트워크의 구성을 변경할 때 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

이 작업에 대해

StorageGRID에는 그리드의 노드에서 일부 포트를 열거나 닫을 수 있도록 각 노드에 대한 내부 방화벽이 포함되어 있습니다. 방화벽 제어 탭을 사용하여 그리드 네트워크, 관리자 네트워크 및 클라이언트 네트워크에서 기본적으로 열려 있는 포트를 열거나 닫을 수 있습니다. 닫힌 그리드 포트에 액세스할 수 있는 권한이 있는 IP 주소 목록을 만들 수도 있습니다. 클라이언트 네트워크를 사용하는 경우 노드가 클라이언트 네트워크의 인바운드 트래픽을 신뢰하는지 여부를 지정하고 클라이언트 네트워크의 특정 포트에 대한 액세스를 구성할 수 있습니다.

그리드 외부의 IP 주소에 열려 있는 포트 수를 절대적으로 필요한 포트만으로 제한하면 그리드의 보안이 향상됩니다. 세 개의 방화벽 제어 탭 각각에서 설정을 사용하여 필요한 포트만 열도록 합니다.

예를 포함한 방화벽 컨트롤 사용에 대한 자세한 내용은 을 참조하십시오 ["방화벽 제어 관리"](#).

외부 방화벽 및 네트워크 보안에 대한 자세한 내용은 을 참조하십시오 ["외부 방화벽에서 액세스를 제어합니다"](#).

## 방화벽 컨트롤에 액세스합니다

단계

1. 구성 \* > \* 보안 \* > \* 방화벽 제어 \* 를 선택합니다.

이 페이지의 세 가지 탭은 에 설명되어 있습니다 ["방화벽 제어 관리"](#).

2. 탭을 선택하여 방화벽 컨트롤을 구성합니다.

이러한 탭은 순서에 상관없이 사용할 수 있습니다. 한 탭에서 설정한 구성은 다른 탭에서 수행할 수 있는 작업을 제한하지 않지만 한 탭에서 변경한 구성은 다른 탭에 구성된 포트의 동작을 변경할 수 있습니다.

## 특별 권한 주소 목록

특별 권한 주소 목록 탭을 사용하여 외부 액세스 관리 탭의 설정에 따라 기본적으로 닫히거나 닫힌 포트에 대한 호스트 액세스 권한을 부여할 수 있습니다.

권한이 있는 IP 주소 및 서브넷에는 기본적으로 내부 그리드 액세스가 없습니다. 또한 외부 액세스 관리 탭에서 차단된 경우에도 권한이 있는 주소 목록 탭에서 열린 로드 밸런서 끝점과 추가 포트에 액세스할 수 있습니다.



권한이 있는 주소 목록 탭의 설정은 신뢰할 수 없는 클라이언트 네트워크 탭의 설정을 재정의할 수 없습니다.

### 단계

1. 특별 권한 주소 목록 탭에서 닫힌 포트에 대한 액세스를 허용할 주소 또는 IP 서브넷을 입력합니다.
2. 선택적으로 \* CIDR 표기법 \* 으로 다른 IP 주소 또는 서브넷 추가 를 선택하여 권한이 있는 클라이언트를 추가합니다.



가능한 한 적은 수의 주소를 권한 있는 목록에 추가합니다.

3. 선택적으로 \* 권한이 있는 IP 주소가 StorageGRID 내부 포트에 액세스하도록 허용 \* 을 선택합니다. 을 참조하십시오 ["StorageGRID 내부 포트"](#).



이 옵션은 내부 서비스에 대한 일부 보호를 제거합니다. 가능한 경우 비활성화 상태로 둡니다.

4. 저장 \* 을 선택합니다.

## 외부 액세스를 관리합니다

외부 액세스 관리 탭에서 포트가 닫힌 경우 권한이 있는 주소 목록에 IP 주소를 추가하지 않으면 비 그리드 IP 주소로 포트에 액세스할 수 없습니다. 기본적으로 열려 있는 포트만 닫을 수 있으며 닫은 포트만 열 수 있습니다.



외부 액세스 관리 탭의 설정은 신뢰할 수 없는 클라이언트 네트워크 탭의 설정을 재정의할 수 없습니다. 예를 들어, 노드가 신뢰할 수 없는 경우 외부 액세스 관리 탭에 열려 있어도 클라이언트 네트워크에서 포트 SSH/22가 차단됩니다. 신뢰할 수 없는 클라이언트 네트워크 탭의 설정은 클라이언트 네트워크의 닫힌 포트(예: 443, 8443, 9443)를 재정의합니다.

### 단계

1. 외부 액세스 관리 \* 를 선택합니다. 이 탭에는 그리드의 노드에 대해 모든 외부 포트(기본적으로 비 그리드 노드가 액세스할 수 있는 포트)가 포함된 테이블이 표시됩니다.
2. 다음 옵션을 사용하여 열고 닫을 포트를 구성합니다.
  - 각 포트 옆의 토글을 사용하여 선택한 포트를 열거나 닫습니다.
  - 표시된 모든 포트 열기 \* 를 선택하여 표에 나열된 모든 포트를 엽니다.
  - 표에 나열된 모든 포트를 닫으려면 \* 표시된 모든 포트 닫기 \* 를 선택합니다.



Grid Manager 포트 443 또는 8443을 닫으면 사용자를 포함하여 차단된 포트에 현재 연결되어 있는 모든 사용자는 권한이 있는 주소 목록에 IP 주소가 추가되지 않으면 Grid Manager에 액세스할 수 없습니다.





테이블 오른쪽에 있는 스크롤 막대를 사용하여 사용 가능한 모든 포트를 확인합니다. 검색 필드를 사용하여 포트 번호를 입력하여 외부 포트의 설정을 찾습니다. 일부 포트 번호를 입력할 수 있습니다. 예를 들어 \* 2 \* 를 입력하면 이름에 문자열 "2"가 포함된 모든 포트가 표시됩니다.

### 3. 저장 \* 을 선택합니다

## 신뢰할 수 없는 클라이언트 네트워크

노드의 클라이언트 네트워크를 신뢰할 수 없는 경우 노드는 로드 밸런서 끝점으로 구성된 포트의 인바운드 트래픽만 허용하고 선택적으로 이 탭에서 선택하는 추가 포트만 허용합니다. 이 탭을 사용하여 확장에 추가된 새 노드의 기본 설정을 지정할 수도 있습니다.



로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

신뢰할 수 없는 클라이언트 네트워크\* 탭에서 변경한 구성은 \* 외부 액세스 관리 \* 탭의 설정보다 우선합니다.

### 단계

1. 신뢰할 수 없는 클라이언트 네트워크 \* 를 선택합니다.
2. 새 노드 기본값 설정 섹션에서 확장 절차에서 그리드에 새 노드를 추가할 때 기본 설정을 지정합니다.

- \* 신뢰 \* (기본값): 확장 시 노드를 추가하면 해당 클라이언트 네트워크가 신뢰됩니다.
- \* 신뢰할 수 없음 \*: 확장 시 노드가 추가되면 해당 클라이언트 네트워크를 신뢰할 수 없습니다.

필요에 따라 이 탭으로 돌아가 특정 새 노드의 설정을 변경할 수 있습니다.



이 설정은 StorageGRID 시스템의 기존 노드에는 영향을 주지 않습니다.

3. 다음 옵션을 사용하여 명시적으로 구성된 로드 밸런싱 장치 엔드포인트 또는 추가 선택 포트에서만 클라이언트 연결을 허용할 노드를 선택합니다.

- 표시된 노드에서 신뢰 해제 \* 를 선택하여 테이블에 표시된 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가합니다.
- 표시된 노드의 신뢰 \* 를 선택하여 신뢰할 수 없는 클라이언트 네트워크 목록에서 표에 표시된 모든 노드를 제거합니다.
- 각 노드 옆의 토글을 사용하여 선택한 노드에 대해 클라이언트 네트워크를 신뢰할 수 있는 또는 신뢰할 수 없는 것으로 설정합니다.

예를 들어 표시된 노드에서 \* 언트러스트 \* 를 선택하여 모든 노드를 신뢰할 수 없는 클라이언트 네트워크 목록에 추가한 다음 개별 노드 옆의 토글을 사용하여 해당 단일 노드를 신뢰할 수 있는 클라이언트 네트워크 목록에 추가할 수 있습니다.



테이블 오른쪽에 있는 스크롤 막대를 사용하여 사용 가능한 모든 노드를 확인합니다. 검색 필드를 사용하여 노드 이름을 입력하여 노드 설정을 찾습니다. 부분 이름을 입력할 수 있습니다. 예를 들어 \* GW \* 를 입력하면 이름에 "GW" 문자열이 포함된 모든 노드가 표시됩니다.

### 4. 저장 \* 을 선택합니다.

새 방화벽 설정이 즉시 적용되고 적용됩니다. 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이

실패할 수 있습니다.

## 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.