



# **S3** 및 **Swift** 클라이언트 연결 구성 StorageGRID

NetApp  
October 03, 2025

# 목차

S3 및 Swift 클라이언트 연결 구성	1
요약: 클라이언트 연결을 위한 IP 주소 및 포트	1
로드 밸런싱 관리	4
로드 밸런싱 작동 방식 - 로드 밸런서 서비스	4
부하 분산 장치 엔드포인트 구성	5
로드 균형 조정 작동 방식 - CLB 서비스	13
신뢰할 수 없는 클라이언트 네트워크 관리	14
예 1: 게이트웨이 노드는 HTTPS S3 요청만 허용합니다	14
예 2: 스토리지 노드가 S3 플랫폼 서비스 요청을 전송합니다	14
노드의 클라이언트 네트워크를 지정하는 것은 신뢰할 수 없습니다	14
고가용성 그룹 관리	16
HA 그룹이란	16
HA 그룹 사용 방법	17
HA 그룹에 대한 구성 옵션	18
고가용성 그룹 생성	20
고가용성 그룹 편집	24
고가용성 그룹을 제거하는 중입니다	27
S3 API 엔드포인트 도메인 이름 구성	28
클라이언트 통신을 위해 HTTP 활성화	30
허용되는 클라이언트 작업을 제어합니다	31

# S3 및 Swift 클라이언트 연결 구성

그리드 관리자는 S3 및 Swift 테넌트가 클라이언트 애플리케이션을 StorageGRID 시스템에 연결하여 데이터를 저장 및 검색하는 방법을 제어하는 구성 옵션을 관리합니다. 다양한 클라이언트 및 테넌트 요구 사항을 충족하는 여러 가지 옵션이 있습니다.

클라이언트 응용 프로그램은 다음 중 하나를 연결하여 개체를 저장하거나 검색할 수 있습니다.

- 관리 노드 또는 게이트웨이 노드의 부하 분산 서비스 또는 선택적으로 관리 노드 또는 게이트웨이 노드의 고가용성(HA) 그룹의 가상 IP 주소입니다
- 게이트웨이 노드의 CLB 서비스 또는 게이트웨이 노드의 고가용성 그룹의 가상 IP 주소(선택 사항)입니다



CLB 서비스는 더 이상 사용되지 않습니다. StorageGRID 11.3 릴리스 전에 구성된 클라이언트는 게이트웨이 노드에서 CLB 서비스를 계속 사용할 수 있습니다. 로드 밸런싱을 제공하기 위해 StorageGRID에 의존하는 다른 모든 클라이언트 애플리케이션은 로드 밸런서 서비스를 사용하여 연결해야 합니다.

- 외부 로드 밸런서가 있거나 없는 스토리지 노드

StorageGRID 시스템에서 다음 기능을 선택적으로 구성할 수 있습니다.

- \* 로드 밸런서 서비스 \*: 클라이언트가 클라이언트 연결을 위한 로드 밸런서 끝점을 만들어 로드 밸런서 서비스를 사용할 수 있도록 합니다. 로드 밸런서 끝점을 만들 때 끝점에서 HTTP 또는 HTTPS 연결을 허용하는지 여부, 끝점을 사용할 클라이언트 유형(S3 또는 Swift) 및 HTTPS 연결에 사용할 인증서(해당하는 경우)를 포트 번호로 지정합니다.
- \* 신뢰할 수 없는 클라이언트 네트워크 \*: 클라이언트 네트워크를 신뢰할 수 없으므로 구성하여 보안을 강화할 수 있습니다. 클라이언트 네트워크를 신뢰할 수 없는 경우 클라이언트는 로드 밸런서 끝점만 사용하여 연결할 수 있습니다.
- \* 고가용성 그룹 \*: 게이트웨이 노드 또는 관리 노드의 HA 그룹을 생성하여 액티브 백업 구성을 생성하거나 라운드 로빈 DNS 또는 타사 로드 밸런서 및 여러 HA 그룹을 사용하여 액티브-액티브 구성을 수행할 수 있습니다. HA 그룹의 가상 IP 주소를 사용하여 클라이언트 연결이 이루어집니다.

또한 StorageGRID에 직접 연결하는 클라이언트나 CLB 서비스(사용되지 않음)를 사용하는 클라이언트에 대해 HTTP를 사용하도록 설정할 수 있으며 S3 클라이언트에 대해 S3 API 엔드포인트 도메인 이름을 구성할 수 있습니다.

## 요약: 클라이언트 연결을 위한 IP 주소 및 포트

클라이언트 애플리케이션은 그리드 노드의 IP 주소와 해당 노드에 있는 서비스의 포트 번호를 사용하여 StorageGRID에 연결할 수 있습니다. HA(고가용성) 그룹이 구성되어 있는 경우 클라이언트 애플리케이션은 HA 그룹의 가상 IP 주소를 사용하여 연결할 수 있습니다.

이 작업에 대해

이 표에는 클라이언트가 StorageGRID에 연결할 수 있는 다양한 방법과 각 연결 유형에 사용되는 IP 주소 및 포트가 요약되어 있습니다. 이 지침은 로드 밸런서 끝점과 HA(고가용성) 그룹이 이미 구성되어 있는 경우 그리드 관리자에서 이 정보를 찾는 방법을 설명합니다.

연결 위치	클라이언트가 연결하는 서비스입니다	IP 주소입니다	포트
HA 그룹	로드 밸런서	HA 그룹의 가상 IP 주소입니다	<ul style="list-style-type: none"> <li>로드 밸런서 엔드포인트 포트</li> </ul>
HA 그룹	CLB <ul style="list-style-type: none"> <li>참고: * CLB 서비스는 더 이상 사용되지 않습니다.</li> </ul>	HA 그룹의 가상 IP 주소입니다	기본 S3 포트: <ul style="list-style-type: none"> <li>HTTPS: 8082</li> <li>HTTP: 8084</li> </ul> 기본 Swift 포트: <ul style="list-style-type: none"> <li>HTTPS: 8083</li> <li>HTTP: 8085</li> </ul>
관리자 노드	로드 밸런서	관리 노드의 IP 주소입니다	<ul style="list-style-type: none"> <li>로드 밸런서 엔드포인트 포트</li> </ul>
게이트웨이 노드	로드 밸런서	게이트웨이 노드의 IP 주소입니다	<ul style="list-style-type: none"> <li>로드 밸런서 엔드포인트 포트</li> </ul>
게이트웨이 노드	CLB <ul style="list-style-type: none"> <li>참고: * CLB 서비스는 더 이상 사용되지 않습니다.</li> </ul>	게이트웨이 노드의 IP 주소입니다 <ul style="list-style-type: none"> <li>참고: * 기본적으로 CLB 및 LDR용 HTTP 포트는 사용되지 않습니다.</li> </ul>	기본 S3 포트: <ul style="list-style-type: none"> <li>HTTPS: 8082</li> <li>HTTP: 8084</li> </ul> 기본 Swift 포트: <ul style="list-style-type: none"> <li>HTTPS: 8083</li> <li>HTTP: 8085</li> </ul>
스토리지 노드	LDR	스토리지 노드의 IP 주소입니다	기본 S3 포트: <ul style="list-style-type: none"> <li>HTTPS: 18082</li> <li>HTTP: 18084</li> </ul> 기본 Swift 포트: <ul style="list-style-type: none"> <li>HTTPS: 18083</li> <li>HTTP: 18085</li> </ul>

예

S3 클라이언트를 게이트웨이 노드 HA 그룹의 로드 밸런서 끝점에 연결하려면 아래와 같이 구조화된 URL을 사용합니다.

- `https://VIP-of-HA-group:LB-endpoint-port`

예를 들어 HA 그룹의 가상 IP 주소가 192.0.2.5이고 S3 로드 밸런서 끝점의 포트 번호가 10443인 경우 S3 클라이언트는 다음 URL을 사용하여 StorageGRID에 연결할 수 있습니다.

- `https://192.0.2.5:10443`

Swift 클라이언트를 게이트웨이 노드 HA 그룹의 로드 밸런서 끝점에 연결하려면 아래와 같이 구조화된 URL을 사용합니다.

- `https://VIP-of-HA-group:LB-endpoint-port`

예를 들어 HA 그룹의 가상 IP 주소가 192.0.2.6이고 Swift 로드 밸런서 끝점의 포트 번호가 10444인 경우 Swift 클라이언트는 다음 URL을 사용하여 StorageGRID에 연결할 수 있습니다.

- `https://192.0.2.6:10444`

클라이언트가 StorageGRID에 연결하는 데 사용하는 IP 주소에 대한 DNS 이름을 구성할 수 있습니다. 로컬 네트워크 관리자에게 문의하십시오.

## 단계

1. 지원되는 브라우저를 사용하여 Grid Manager에 로그인합니다.
2. 그리드 노드의 IP 주소를 찾으려면
  - a. 노드 \* 를 선택합니다.
  - b. 연결할 관리 노드, 게이트웨이 노드 또는 스토리지 노드를 선택합니다.
  - c. 개요 \* 탭을 선택합니다.
  - d. 노드 정보 섹션에서 노드의 IP 주소를 확인합니다.
  - e. IPv6 주소 및 인터페이스 매핑을 보려면 \* 더 보기 \* 를 클릭합니다.

클라이언트 응용 프로그램에서 목록의 IP 주소로의 연결을 설정할 수 있습니다.

- `eth0`: \* 그리드 네트워크
- \* `eth1`: \* 관리 네트워크(옵션)
- \* `eth2`: \* 클라이언트 네트워크(옵션)



관리 노드 또는 게이트웨이 노드를 보고 있고고가용성 그룹의 활성 노드인 경우 HA 그룹의 가상 IP 주소가 `eth2`에 표시됩니다.

- 3.고가용성 그룹의 가상 IP 주소를 찾으려면 다음을 수행합니다.
  - a. 구성 \* > \* 네트워크 설정 \* > \*고가용성 그룹 \* 을 선택합니다.
  - b. 표에서 HA 그룹의 가상 IP 주소를 확인합니다.
4. 로드 밸런서 끝점의 포트 번호를 찾으려면 다음을 수행합니다.
  - a. 구성 \* > \* 네트워크 설정 \* > \* 로드 밸런서 엔드포인트 \* 를 선택합니다.

로드 밸런서 끝점 페이지가 나타나고 이미 구성된 끝점 목록이 표시됩니다.

- b. 끝점을 선택하고 \* 끝점 편집 \* 을 클릭합니다.

끝점 편집 창이 열리고 끝점에 대한 추가 세부 정보가 표시됩니다.

- c. 선택한 끝점이 올바른 프로토콜(S3 또는 Swift)과 함께 사용하도록 구성되었는지 확인한 후 \* Cancel \* (취소 \*)을 클릭합니다.
- d. 클라이언트 연결에 사용할 끝점의 포트 번호를 확인합니다.



포트 번호가 80 또는 443이면 해당 포트가 관리 노드에 예약되므로 끝점이 게이트웨이 노드에서만 구성됩니다. 다른 모든 포트는 게이트웨이 노드와 관리 노드 모두에서 구성됩니다.

## 로드 밸런싱 관리

StorageGRID 로드 밸런싱 기능을 사용하여 S3 및 Swift 클라이언트에서 수집 및 검색 워크로드를 처리할 수 있습니다. 로드 밸런싱은 여러 스토리지 노드에 워크로드와 연결을 분산하여 속도와 연결 용량을 극대화합니다.

다음과 같은 방법으로 StorageGRID 시스템에서 로드 밸런싱을 수행할 수 있습니다.

- 관리 노드 및 게이트웨이 노드에 설치된 로드 밸런서 서비스를 사용합니다. 로드 밸런서 서비스는 계층 7 로드 밸런싱을 제공하고 클라이언트 요청에 대한 TLS 종료를 수행하고 요청을 검사하며 스토리지 노드에 대한 새로운 보안 연결을 설정합니다. 이것은 권장되는 로드 밸런싱 메커니즘입니다.
- 게이트웨이 노드에만 설치된 CLB(연결 로드 밸런서) 서비스를 사용합니다. CLB 서비스는 계층 4 로드 밸런싱을 제공하고 링크 비용을 지원합니다.



CLB 서비스는 더 이상 사용되지 않습니다.

- 타사 로드 밸런서를 통합합니다. 자세한 내용은 NetApp 어카운트 담당자에게 문의하십시오.

### 로드 밸런싱 작동 방식 - 로드 밸런서 서비스

로드 밸런서 서비스는 들어오는 네트워크 연결을 클라이언트 애플리케이션에서 스토리지 노드로 배포합니다. 로드 밸런싱을 사용하려면 Grid Manager를 사용하여 부하 분산 엔드포인트를 구성해야 합니다.

이러한 노드 유형에는 로드 밸런서 서비스가 포함되어 있으므로 관리 노드 또는 게이트웨이 노드에 대해서만 로드 밸런서 끝점을 구성할 수 있습니다. 스토리지 노드 또는 아카이브 노드의 끝점은 구성할 수 없습니다.

각 로드 밸런서 끝점은 포트, 프로토콜(HTTP 또는 HTTPS), 서비스 유형(S3 또는 Swift) 및 바인딩 모드를 지정합니다. HTTPS 엔드포인트에는 서버 인증서가 필요합니다. 바인딩 모드를 사용하면 엔드포인트 포트의 액세스를 다음과 같이 제한할 수 있습니다.

- 특정 HA(고가용성) 가상 IP 주소(VIP)
- 특정 노드의 특정 네트워크 인터페이스

### 포트 고려 사항

클라이언트는 로드 밸런서 서비스를 실행하는 노드에서 구성한 모든 끝점에 액세스할 수 있습니다. 단, 포트 80과 443은 관리 노드에 예약되므로 이러한 포트에 구성된 끝점은 게이트웨이 노드에서만 로드 밸런싱 작업을 지원합니다.

포트를 다시 매핑한 경우 동일한 포트를 사용하여 로드 밸런서 끝점을 구성할 수 없습니다. 다시 매핑된 포트를 사용하여 끝점을 만들 수 있지만 이러한 끝점은 로드 밸런서 서비스가 아닌 원래 CLB 포트 및 서비스에 다시 매핑됩니다. 포트 재매핑을 제거하기 위한 복구 및 유지 관리 지침의 단계를 따릅니다.



CLB 서비스는 더 이상 사용되지 않습니다.

## CPU 가용성

각 관리 노드와 게이트웨이 노드의 로드 밸런서 서비스는 S3 또는 Swift 트래픽을 스토리지 노드로 전달할 때 독립적으로 작동합니다. 로드 밸런서 서비스는 가중 프로세스를 통해 더 많은 요청을 CPU 가용성이 높은 스토리지 노드로 라우팅합니다. 노드 CPU 로드 정보는 몇 분마다 업데이트되지만 가중치는 더 자주 업데이트될 수 있습니다. 모든 스토리지 노드에는 최소 기본 가중치 값이 할당됩니다. 이는 노드에서 100% 사용률을 보고하거나 사용률을 보고하지 않는 경우에도 마찬가지입니다.

경우에 따라 CPU 가용성에 대한 정보는 로드 밸런서 서비스가 있는 사이트로 제한됩니다.

관련 정보

["유지 및 복구"](#)

## 부하 분산 장치 엔드포인트 구성

부하 분산 엔드포인트를 생성, 편집 및 제거할 수 있습니다.

로드 밸런서 끝점을 만듭니다

각 로드 밸런서 끝점은 포트, 네트워크 프로토콜(HTTP 또는 HTTPS) 및 서비스 유형(S3 또는 Swift)을 지정합니다. HTTPS 끝점을 만드는 경우 서버 인증서를 업로드하거나 생성해야 합니다.

필요한 것

- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 로드 밸런서 서비스에 사용할 포트를 이전에 다시 매핑한 경우 리매핑을 제거해야 합니다.



포트를 다시 매핑한 경우 동일한 포트를 사용하여 로드 밸런서 끝점을 구성할 수 없습니다. 다시 매핑된 포트를 사용하여 끝점을 만들 수 있지만 이러한 끝점은 로드 밸런서 서비스가 아닌 원래 CLB 포트 및 서비스에 다시 매핑됩니다. 포트 재매핑을 제거하기 위한 복구 및 유지 관리 지침의 단계를 따릅니다.



CLB 서비스는 더 이상 사용되지 않습니다.

단계

1. 구성 \* > \* 네트워크 설정 \* > \* 로드 밸런서 엔드포인트 \* 를 선택합니다.

부하 분산 엔드포인트 페이지가 나타납니다.

## Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

**i** Changes to endpoints can take up to 15 minutes to be applied to all nodes.

**+** Add endpoint port   **✎** Edit endpoint   **✕** Remove endpoint port

Display name

Port

Using HTTPS

*No endpoints configured.*

2. 끝점 추가 \* 를 선택합니다.

끝점 만들기 대화 상자가 나타납니다.

### Create Endpoint

Display Name

Port 10443

Protocol  HTTP  HTTPS

Endpoint Binding Mode  Global  HA Group VIPs  Node Interfaces

Cancel

Save

3. 로드 밸런서 끝점 페이지의 목록에 표시될 끝점의 표시 이름을 입력합니다.

4. 포트 번호를 입력하거나 미리 채워진 포트 번호를 그대로 둡니다.

포트 번호 80 또는 443을 입력하면 엔드포인트는 게이트웨이 노드에서만 구성됩니다. 이러한 포트는 관리 노드에 예약되기 때문입니다.



다른 그리드 서비스에서 사용하는 포트는 허용되지 않습니다. 내부 및 외부 통신에 사용되는 포트 목록은 네트워킹 지침을 참조하십시오.

5. 이 끝점의 네트워크 프로토콜을 지정하려면 \* HTTP \* 또는 \* HTTPS \* 를 선택합니다.

6. 끝점 바인딩 모드를 선택합니다.

- \* 글로벌 \* (기본값): 엔드포인트는 지정된 포트 번호의 모든 게이트웨이 노드 및 관리 노드에서 액세스할 수 있습니다.

## Create Endpoint

Display Name

Port

Protocol  HTTP  HTTPS

Endpoint Binding Mode  Global  HA Group VIPs  Node Interfaces

**i** This endpoint is currently bound globally. All nodes will use this endpoint unless an endpoint with an overriding binding mode exists for a specific port.

Cancel Save

- \* HA 그룹 VIP \*: 끝점은 선택한 HA 그룹에 대해 정의된 가상 IP 주소를 통해서만 액세스할 수 있습니다. 이 모드에서 정의된 엔드포인트는 해당 엔드포인트에서 정의된 HA 그룹이 서로 겹치지 않는 한 동일한 포트 번호를 재사용할 수 있습니다.

끝점을 표시할 가상 IP 주소가 있는 HA 그룹을 선택합니다.

## Create Endpoint

Display Name

Port

Protocol  HTTP  HTTPS

Endpoint Binding Mode  Global  HA Group VIPs  Node Interfaces

Name	Description	Virtual IP Addresses	Interfaces
<input type="checkbox"/> Group1		192.168.5.163	CO-REF-DC1-ADM1:eth0 (preferred Master)
<input type="checkbox"/> Group2		47.47.5.162	CO-REF-DC1-ADM1:eth2 (preferred Master)

Displaying 2 HA groups.

**⚠** No HA groups selected. You must select one or more HA Groups; otherwise, this endpoint will act as a globally bound endpoint.

Cancel Save

- \* 노드 인터페이스 \*: 끝점은 지정된 노드와 네트워크 인터페이스에서만 액세스할 수 있습니다. 이 모드에서 정의된 끝점은 인터페이스가 서로 겹치지 않는 한 동일한 포트 번호를 다시 사용할 수 있습니다.

끝점을 표시할 노드 인터페이스를 선택합니다.

## Create Endpoint

Display Name

Port

Protocol  HTTP  HTTPS

Endpoint Binding Mode  Global  HA Group VIPs  Node Interfaces

Node	Interface
<input type="checkbox"/> CO-REF-DC1-ADM1	eth0
<input type="checkbox"/> CO-REF-DC1-ADM1	eth1
<input type="checkbox"/> CO-REF-DC1-ADM1	eth2
<input type="checkbox"/> CO-REF-DC1-GW1	eth0
<input type="checkbox"/> CO-REF-DC2-ADM1	eth0
<input type="checkbox"/> CO-REF-DC2-GW1	eth0

 No node interfaces selected. You must select one or more node interfaces; otherwise, this endpoint will act as a globally bound endpoint.

7. 저장 \* 을 선택합니다.

끝점 편집 대화 상자가 나타납니다.

8. S3 \* 또는 \* Swift \* 를 선택하여 이 끝점에서 지원하는 트래픽 유형을 지정합니다.

## Edit Endpoint Unsecured Port A (port 10449)

### Endpoint Service Configuration

Endpoint service type  S3  Swift

9. HTTP \* 를 선택한 경우 \* Save \* 를 선택합니다.

보안되지 않은 끝점이 만들어집니다. 부하 분산 끝점 페이지의 표에는 끝점의 표시 이름, 포트 번호, 프로토콜 및 끝점 ID가 나열됩니다.

10. HTTPS \* 를 선택하고 인증서를 업로드하려면 \* 인증서 업로드 \* 를 선택합니다.

## Load Certificate

Upload the PEM-encoded custom certificate, private key, and CA bundle files.

Server Certificate

Certificate Private Key

CA Bundle

Cancel

Save

- a. 서버 인증서와 인증서 개인 키를 찾습니다.

S3 클라이언트가 S3 API 엔드포인트 도메인 이름을 사용하여 연결할 수 있도록 하려면 클라이언트가 그리드에 연결하는 데 사용할 수 있는 모든 도메인 이름과 일치하는 다중 도메인 또는 와일드카드 인증서를 사용합니다. 예를 들어 서버 인증서에서 도메인 이름을 사용할 수 있습니다 \*.example.com.

### "S3 API 엔드포인트 도메인 이름 구성"

- a. 선택적으로 CA 번들을 찾습니다.
- b. 저장 \* 을 선택합니다.

끝점에 대한 PEM 인코딩된 인증서 데이터가 나타납니다.

11. HTTPS \* 를 선택하고 인증서를 생성하려면 \* 인증서 생성 \* 을 선택합니다.

## Generate Certificate

Domain 1  +

IP 1  +

Subject

Days valid

Cancel

Generate

- a. 도메인 이름 또는 IP 주소를 입력합니다.

와일드카드를 사용하여 로드 밸런서 서비스를 실행하는 모든 관리 노드 및 게이트웨이 노드의 정규화된 도메인 이름을 나타낼 수 있습니다. 예를 들면, 다음과 같습니다. \*.sgws.foo.com 와일드카드를 사용하여 나타냅니다 gn1.sgws.foo.com 및 gn2.sgws.foo.com.

## "S3 API 엔드포인트 도메인 이름 구성"

a. 를 선택합니다 + 다른 도메인 이름 또는 IP 주소를 추가합니다.

HA(고가용성) 그룹을 사용하는 경우 HA 가상 IP의 도메인 이름 및 IP 주소를 추가합니다.

b. 필요한 경우 인증서를 소유하는 사용자를 식별하기 위해 DN(고유 이름)이라고도 하는 X.509 제목을 입력합니다.

c. 원하는 경우 인증서가 유효한 일 수를 선택합니다. 기본값은 730일입니다.

d. Generate \* 를 선택합니다.

끝점에 대한 인증서 메타데이터 및 PEM 인코딩된 인증서 데이터가 나타납니다.

12. 저장 \* 을 클릭합니다.

끝점이 작성됩니다. 부하 분산 끝점 페이지의 표에는 끝점의 표시 이름, 포트 번호, 프로토콜 및 끝점 ID가 나열됩니다.

관련 정보

["유지 및 복구"](#)

["네트워크 지침"](#)

["고가용성 그룹 관리"](#)

["신뢰할 수 없는 클라이언트 네트워크 관리"](#)

로드 밸런서 끝점 편집

비보안(HTTP) 끝점의 경우 S3 및 Swift 간에 끝점 서비스 유형을 변경할 수 있습니다. 보안(HTTPS) 엔드포인트의 경우 엔드포인트 서비스 유형을 편집하고 보안 인증서를 보거나 변경할 수 있습니다.

필요한 것

- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

단계

1. 구성 \* > \* 네트워크 설정 \* > \* 로드 밸런서 엔드포인트 \* 를 선택합니다.

부하 분산 엔드포인트 페이지가 나타납니다. 기존 끝점이 테이블에 나열됩니다.

인증서가 곧 만료되는 끝점이 표에 나와 있습니다.



- 끝점 바인딩 모드를 변경합니다. 보안(HTTPS) 엔드포인트의 경우 다음을 수행할 수 있습니다.
- S3 및 Swift 간에 엔드포인트 서비스 유형을 변경합니다.
- 끝점 바인딩 모드를 변경합니다.
- 보안 인증서를 봅니다.
- 현재 인증서가 만료되거나 만료될 때 새 보안 인증서를 업로드하거나 생성합니다.

기본 StorageGRID 서버 인증서 또는 업로드된 CA 서명 인증서에 대한 자세한 정보를 표시하려면 탭을 선택합니다.



예를 들어, HTTP에서 HTTPS로 같은 기존 끝점의 프로토콜을 변경하려면 새 끝점을 만들어야 합니다. 로드 밸런서 끝점을 만들기 위한 지침에 따라 원하는 프로토콜을 선택합니다.

5. 저장 \* 을 클릭합니다.

관련 정보

[로드 밸런서 끝점을 만듭니다](#)

로드 밸런서 끝점을 제거하는 중입니다

로드 밸런서 끝점이 더 이상 필요하지 않으면 제거할 수 있습니다.

필요한 것

- 루트 액세스 권한이 있어야 합니다.
- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

단계

1. 구성 \* > \* 네트워크 설정 \* > \* 로드 밸런서 엔드포인트 \* 를 선택합니다.

부하 분산 엔드포인트 페이지가 나타납니다. 기존 끝점이 테이블에 나열됩니다.

### Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

<input type="button" value="+ Add endpoint"/> <input type="button" value="✎ Edit endpoint"/> <input type="button" value="✕ Remove endpoint"/>			
	Display name	Port	Using HTTPS
<input type="radio"/>	Unsecured Endpoint 5	10444	No
<input checked="" type="radio"/>	Secured Endpoint 1	10443	Yes

Displaying 2 endpoints.

2. 제거할 끝점 왼쪽에 있는 라디오 단추를 선택합니다.

3. 끝점 제거 \* 를 클릭합니다.

확인 대화 상자가 나타납니다.

## Warning

Remove Endpoint

Are you sure you want to remove endpoint 'Secured Endpoint 1'?

Cancel

OK

4. 확인 \* 을 클릭합니다.

끝점이 제거됩니다.

## 로드 균형 조정 작동 방식 - CLB 서비스

게이트웨이 노드의 CLB(연결 로드 밸런서) 서비스는 더 이상 사용되지 않습니다. 이제 로드 밸런서 서비스가 권장되는 로드 밸런싱 메커니즘입니다.

CLB 서비스는 Layer 4 로드 밸런싱을 사용하여 클라이언트 응용 프로그램에서 들어오는 TCP 네트워크 연결을 가용성, 시스템 로드 및 관리자 구성 링크 비용에 따라 최적의 스토리지 노드로 배포합니다. 최적의 스토리지 노드를 선택하면 CLB 서비스는 양방향 네트워크 연결을 설정하고 선택한 노드로 트래픽을 전달합니다. CLB는 들어오는 네트워크 연결을 연결할 때 그리드 네트워크 구성을 고려하지 않습니다.

CLB 서비스에 대한 정보를 보려면 \* 지원 \* > \* 도구 \* > \* 그리드 토폴로지 \* 를 선택한 다음 \* CLB \* 와 그 아래 옵션을 선택할 수 있을 때까지 게이트웨이 노드를 확장합니다.

The screenshot shows the StorageGRID WebScale Deployment interface. On the left, the 'Grid Topology' tree is visible, with 'DC1-G1-98-161' selected and highlighted in blue. The main panel displays the 'Overview: Summary - DC1-G1-98-161' page, which includes a 'Storage Capacity' section with the following data:

Storage Capacity	Value	Icon
Storage Nodes Installed:	N/A	🔍
Storage Nodes Readable:	N/A	🔍
Storage Nodes Writable:	N/A	🔍
Installed Storage Capacity:	N/A	🔍
Used Storage Capacity:	N/A	🔍
Used Storage Capacity for Data:	N/A	🔍
Used Storage Capacity for Metadata:	N/A	🔍
Usable Storage Capacity:	N/A	🔍

CLB 서비스를 사용하도록 선택한 경우 StorageGRID 시스템에 대한 링크 비용을 구성하는 것이 좋습니다.

관련 정보

"링크 비용은 얼마입니까"

"링크 비용을 업데이트하는 중입니다"

# 신뢰할 수 없는 클라이언트 네트워크 관리

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 사용 가능한 모든 외부 포트의 각 그리드 노드에 대한 인바운드 연결을 신뢰합니다(네트워크 지침의 외부 통신 정보 참조).

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.

## 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. 로드 밸런서 엔드포인트 페이지에서 포트 443에서 HTTPS를 통해 S3에 대한 로드 밸런서 끝점을 구성합니다.
2. 신뢰할 수 없는 클라이언트 네트워크 페이지에서 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.

- 신뢰할 수 없는 클라이언트 네트워크 페이지에서 스토리지 노드의 클라이언트 네트워크를 신뢰할 수 없음을 나타냅니다.

구성을 저장한 후 스토리지 노드는 더 이상 클라이언트 네트워크에서 들어오는 트래픽을 허용하지 않지만 Amazon Web Services에 대한 아웃바운드 요청은 계속 허용합니다.

관련 정보

["네트워크 지침"](#)

["부하 분산 장치 엔드포인트 구성"](#)

노드의 클라이언트 네트워크를 지정하는 것은 신뢰할 수 없습니다

클라이언트 네트워크를 사용하는 경우 각 노드의 클라이언트 네트워크를 신뢰할 수 있는지 신뢰할 수 없는지 여부를 지정할 수 있습니다. 또한 확장에 추가된 새 노드의 기본 설정을 지정할 수도 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.

- 루트 액세스 권한이 있어야 합니다.
- 관리자 노드 또는 게이트웨이 노드가 명시적으로 구성된 끝점에서만 인바운드 트래픽을 수락하도록 하려면 로드 밸런서 끝점을 정의해야 합니다.



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

## 단계

1. 구성 \* \* 네트워크 설정 \* 신뢰할 수 없는 클라이언트 네트워크 \* 를 선택합니다.

신뢰할 수 없는 클라이언트 네트워크 페이지가 나타납니다.

이 페이지에는 StorageGRID 시스템의 모든 노드가 나열됩니다. 노드의 클라이언트 네트워크를 신뢰할 수 있어야 하는 경우 사용할 수 없는 이유 열에 항목이 포함됩니다.

### Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

#### Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network     Trusted  
 Default                       Untrusted

#### Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	

Client Network untrusted on 0 nodes.

Save

2. 새 노드 기본값 설정 \* 섹션에서 확장 절차에서 그리드에 새 노드를 추가할 때 기본 설정을 지정합니다.

- \* 신뢰 \*: 확장 시 노드가 추가되면 해당 클라이언트 네트워크를 신뢰할 수 있습니다.
- \* 신뢰할 수 없음 \*: 확장 시 노드가 추가되면 해당 클라이언트 네트워크를 신뢰할 수 없습니다. 필요에 따라 이 페이지로 돌아가 특정 새 노드의 설정을 변경할 수 있습니다.



이 설정은 StorageGRID 시스템의 기존 노드에는 영향을 주지 않습니다.

3. 신뢰할 수 없는 클라이언트 네트워크 노드 선택 \* 섹션에서 명시적으로 구성된 로드 밸런서 끝점에서만 클라이언트 연결을 허용할 노드를 선택합니다.

제목에서 확인란을 선택하거나 선택 취소하여 모든 노드를 선택하거나 선택 취소할 수 있습니다.

4. 저장 \* 을 클릭합니다.

새 방화벽 규칙이 즉시 추가되고 적용됩니다. 로드 밸런서 끝점이 구성되지 않은 경우 기존 클라이언트 연결이 실패할 수 있습니다.

관련 정보

["부하 분산 장치 엔드포인트 구성"](#)

## 고가용성 그룹 관리

고가용성(HA) 그룹을 사용하여 S3 및 Swift 클라이언트에 고가용성 데이터 연결을 제공할 수 있습니다. HA 그룹을 사용하여 Grid Manager 및 Tenant Manager에 대한 고가용성 연결을 제공할 수도 있습니다.

- ["HA 그룹이란"](#)
- ["HA 그룹 사용 방법"](#)
- ["HA 그룹에 대한 구성 옵션"](#)
- ["고가용성 그룹 생성"](#)
- ["고가용성 그룹 편집"](#)
- ["고가용성 그룹을 제거하는 중입니다"](#)

### HA 그룹이란

고가용성 그룹은 가상 IP 주소(VIP)를 사용하여 게이트웨이 노드 또는 관리 노드 서비스에 대한 액티브 백업 액세스를 제공합니다.

HA 그룹은 관리 노드 및 게이트웨이 노드에 있는 하나 이상의 네트워크 인터페이스로 구성됩니다. HA 그룹을 생성할 때 Grid Network(eth0) 또는 Client Network(eth2)에 속하는 네트워크 인터페이스를 선택합니다. HA 그룹의 모든 인터페이스는 동일한 네트워크 서브넷 내에 있어야 합니다.

HA 그룹은 그룹의 활성 인터페이스에 추가된 하나 이상의 가상 IP 주소를 유지합니다. 활성 인터페이스를 사용할 수 없게 되면 가상 IP 주소가 다른 인터페이스로 이동합니다. 이 장애 조치 프로세스는 일반적으로 몇 초 밖에 걸리지 않으며 클라이언트 응용 프로그램에 거의 영향을 주지 않고 정상적인 재시도 동작에 의존하여 작업을 계속할 수 있을 정도로 빠릅니다.

HA 그룹의 활성 인터페이스가 Master로 지정됩니다. 다른 모든 인터페이스는 백업으로 지정됩니다. 이러한 지정을 보려면 \* 노드 \* > \*노드 \* > \* 개요 \* 를 선택합니다.

Overview

Hardware

Network

Storage

Load Balancer

Events

Tasks

Node Information 

Name	DC1-ADM1
Type	Admin Node
ID	711b7b9b-8d24-4d9f-877a-be3fa3ac27e8
Connection State	 Connected
Software Version	11.4.0 (build 20200515.2346.8edcbbf)
HA Groups	Fabric Pools, Master
IP Addresses	192.168.2.208, 10.224.2.208, 47.47.2.208, 47.47.4.219 <a href="#">Show more</a> 

HA 그룹을 생성할 때 기본 마스터가 될 인터페이스를 하나 지정합니다. 장애가 발생하여 VIP 주소가 백업 인터페이스에 재할당되지 않는 한 기본 마스터는 활성 인터페이스입니다. 장애가 해결되면 VIP 주소가 자동으로 기본 마스터로 다시 이동됩니다.

페일오버는 다음과 같은 이유로 트리거될 수 있습니다.

- 인터페이스가 구성된 노드가 다운됩니다.
- 인터페이스가 구성된 노드는 다른 모든 노드와의 연결이 2분 이상 끊어집니다
- 활성 인터페이스가 다운됩니다.
- 로드 밸런서 서비스가 중지됩니다.
- High Availability 서비스가 중지됩니다.



활성 인터페이스를 호스팅하는 노드 외부의 네트워크 장애로 인해 페일오버가 트리거되지 않을 수 있습니다. 마찬가지로, 페일오버는 CLB 서비스 장애(더 이상 사용되지 않음) 또는 Grid Manager 또는 테넌트 관리자에 대한 서비스에 의해 트리거되지 않습니다.

HA 그룹에 2개 이상의 노드의 인터페이스가 포함된 경우 페일오버 중에 액티브 인터페이스가 다른 노드의 인터페이스로 이동할 수 있습니다.

## HA 그룹 사용 방법

여러 가지 이유로 고가용성(HA) 그룹을 사용할 수 있습니다.

- HA 그룹은 Grid Manager 또는 Tenant Manager에 대한 고가용성 관리 연결을 제공할 수 있습니다.
- HA 그룹은 S3 및 Swift 클라이언트에 고가용성 데이터 연결을 제공할 수 있습니다.
- 인터페이스가 하나만 포함된 HA 그룹을 사용하면 많은 VIP 주소를 제공하고 IPv6 주소를 명시적으로 설정할 수 있습니다.

그룹에 포함된 모든 노드가 동일한 서비스를 제공하는 경우에만 HA 그룹이 고가용성을 제공할 수 있습니다. HA 그룹을

생성할 때 필요한 서비스를 제공하는 노드 유형의 인터페이스를 추가합니다.

- \* 관리 노드 \*: 로드 밸런서 서비스를 포함하고 그리드 관리자 또는 테넌트 관리자에 대한 액세스를 활성화합니다.
- \* 게이트웨이 노드 \*: 로드 밸런서 서비스 및 CLB 서비스(더 이상 사용되지 않음)를 포함합니다.

HA 그룹의 용도	이 유형의 노드를 HA 그룹에 추가합니다
Grid Manager에 액세스합니다	<ul style="list-style-type: none"> <li>• 기본 관리자 노드(* 기본 마스터 *)</li> <li>• 운영 관리자 노드가 아닌 노드</li> <li>• 참고: * 기본 관리 노드는 기본 마스터여야 합니다. 일부 유지 보수 절차는 기본 관리 노드에서만 수행할 수 있습니다.</li> </ul>
테넌트 관리자에 대한 액세스만 가능합니다	<ul style="list-style-type: none"> <li>• 운영 또는 비운영 관리 노드</li> </ul>
S3 또는 Swift 클라이언트 액세스 — 로드 밸런서 서비스	<ul style="list-style-type: none"> <li>• 관리자 노드</li> <li>• 게이트웨이 노드</li> </ul>
S3 또는 Swift 클라이언트 액세스 — CLB 서비스  • 참고: * CLB 서비스는 더 이상 사용되지 않습니다.	<ul style="list-style-type: none"> <li>• 게이트웨이 노드</li> </ul>

### Grid Manager 또는 Tenant Manager에 HA 그룹을 사용할 때의 제한 사항

Grid Manager 또는 테넌트 관리자에 대한 서비스 장애가 HA 그룹 내에서 페일오버를 트리거하지 않습니다.

페일오버가 발생했을 때 Grid Manager 또는 Tenant Manager에 로그인한 경우, 로그아웃되며 작업을 재개하려면 다시 로그인해야 합니다.

기본 관리 노드를 사용할 수 없는 경우 일부 유지 관리 절차를 수행할 수 없습니다. 장애 조치 중에 그리드 관리자를 사용하여 StorageGRID 시스템을 모니터링할 수 있습니다.

### CLB 서비스에 HA 그룹 사용 제한

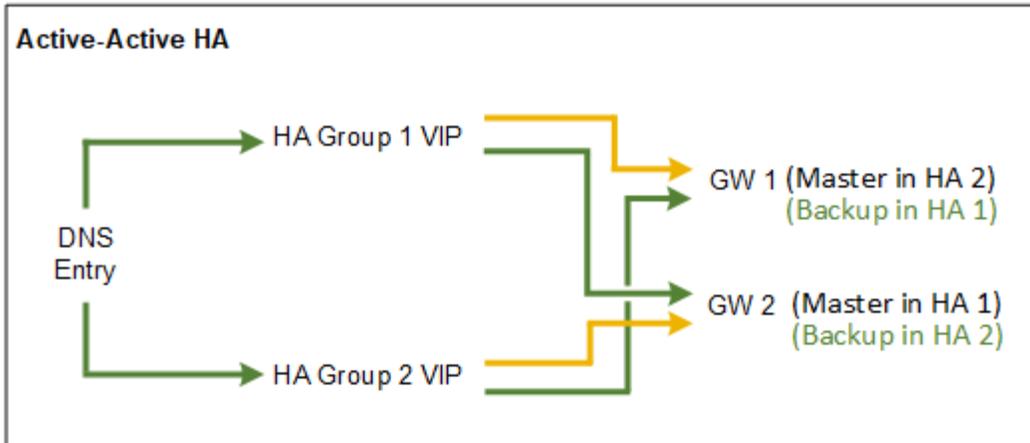
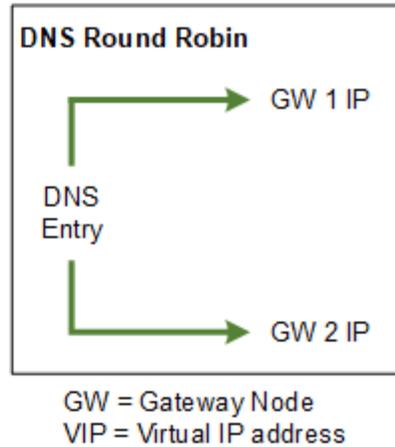
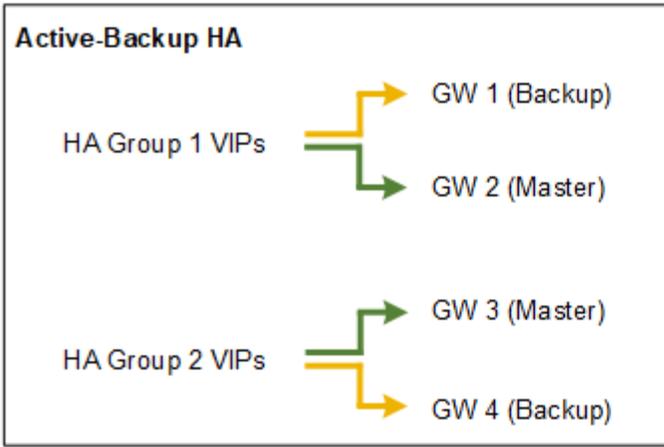
CLB 서비스가 실패해도 HA 그룹 내에서 대체 작동이 트리거되지 않습니다.



CLB 서비스는 더 이상 사용되지 않습니다.

### HA 그룹에 대한 구성 옵션

다음 다이어그램에서는 HA 그룹을 구성할 수 있는 다양한 방법의 예를 제공합니다. 각 옵션에는 장단점이 있습니다.



Active-Active HA 예에서와 같이 여러 개의 중복 HA 그룹을 생성할 때 총 처리량은 노드 수와 HA 그룹으로 확장됩니다. 3개 이상의 노드와 3개 이상의 HA 그룹을 사용하면 노드를 오프라인으로 전환해야 하는 유지보수 절차 중에도 VIP를 사용하여 작업을 계속할 수 있습니다.

이 표에는 다이어그램에 표시된 각 HA 구성의 이점이 요약되어 있습니다.

구성	장점	단점
Active-Backup HA를 참조하십시오	<ul style="list-style-type: none"> <li>외부 종속성 없이 StorageGRID에서 관리</li> <li>빠른 페일오버.</li> </ul>	<ul style="list-style-type: none"> <li>HA 그룹에서 하나의 노드만 활성화됩니다. HA 그룹당 최소 하나의 노드가 유휴 상태가 됩니다.</li> </ul>
DNS 라운드 로빈	<ul style="list-style-type: none"> <li>총 처리량 향상:</li> <li>유휴 호스트가 없습니다.</li> </ul>	<ul style="list-style-type: none"> <li>느린 페일오버 - 클라이언트 동작에 따라 달라질 수 있습니다.</li> <li>StorageGRID 외부에서 하드웨어를 구성해야 합니다.</li> <li>고객이 구현한 상태 점검이 필요합니다.</li> </ul>

구성	장점	단점
액티브-액티브	<ul style="list-style-type: none"> <li>트래픽이 여러 HA 그룹에 분산됩니다.</li> <li>HA 그룹 수에 따라 확장 가능한 높은 애그리게이트 처리량입니다.</li> <li>빠른 페일오버.</li> </ul>	<ul style="list-style-type: none"> <li>구성이 더 복잡합니다.</li> <li>StorageGRID 외부에서 하드웨어를 구성해야 합니다.</li> <li>고객이 구현한 상태 점검이 필요합니다.</li> </ul>

## 고가용성 그룹 생성

하나 이상의 고가용성(HA) 그룹을 생성하여 관리 노드 또는 게이트웨이 노드의 서비스에 대한 고가용성 액세스를 제공할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.

이 작업에 대해

HA 그룹에 포함할 인터페이스는 다음 조건을 충족해야 합니다.

- 인터페이스는 게이트웨이 노드 또는 관리 노드여야 합니다.
- 인터페이스는 Grid Network(eth0) 또는 Client Network(eth2)에 속해야 합니다.
- 인터페이스는 DHCP가 아닌 고정 또는 고정 IP 주소 지정으로 구성해야 합니다.

단계

- 구성 \* > \* 네트워크 설정 \* > \* 고가용성 그룹 \* 을 선택합니다.

High Availability Groups 페이지가 나타납니다.

### High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.



2. Create \* 를 클릭합니다.

High Availability Group 생성 대화 상자가 나타납니다.

3. 이름을 입력하고 원하는 경우 HA 그룹에 대한 설명을 입력합니다.
4. Select Interfaces \* 를 클릭합니다.

High Availability Group에 인터페이스 추가 대화 상자가 나타납니다. 이 표에는 적합한 노드, 인터페이스 및 IPv4 서브넷이 나와 있습니다.

## Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
	g140-g1	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g1	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g3	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g3	eth2	192.168.0.0/21	
	g140-g4	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

Cancel

Apply

DHCP에서 IP 주소를 할당한 경우 인터페이스가 목록에 나타나지 않습니다.

### 5. HA 그룹에 추가 \* 열에서 HA 그룹에 추가할 인터페이스의 확인란을 선택합니다.

인터페이스 선택에 대한 다음 지침을 참조하십시오.

- 인터페이스를 하나 이상 선택해야 합니다.
- 둘 이상의 인터페이스를 선택하는 경우 모든 인터페이스가 그리드 네트워크(eth0) 또는 클라이언트 네트워크(eth2)에 있어야 합니다.
- 모든 인터페이스는 동일한 서브넷 또는 공통 접두사가 있는 서브넷에 있어야 합니다.

IP 주소는 가장 작은 서브넷(접두사가 가장 큰 서브넷)으로 제한됩니다.

- 다른 노드 유형의 인터페이스를 선택하고 페일오버가 발생하는 경우 선택한 노드에 공통되는 서비스만 가상 IP에서 사용할 수 있습니다.
  - Grid Manager 또는 Tenant Manager의 HA 보호를 위해 두 개 이상의 관리 노드를 선택합니다.
  - 로드 밸런서 서비스의 HA 보호를 위해 두 개 이상의 관리 노드, 게이트웨이 노드 또는 둘 다를 선택합니다.
  - CLB 서비스의 HA 보호를 위해 둘 이상의 게이트웨이 노드를 선택합니다.



CLB 서비스는 더 이상 사용되지 않습니다.

## Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
<input checked="" type="checkbox"/>	DC1-ADM1	eth0	10.96.100.0/23	
<input checked="" type="checkbox"/>	DC1-G1	eth0	10.96.100.0/23	
<input checked="" type="checkbox"/>	DC2-ADM1	eth0	10.96.100.0/23	

There are 3 interfaces selected.

**Attention:** You have selected nodes of different types that run different services. If a failover occurs, only the services common to all node types will be available on the virtual IPs.

Cancel

Apply

6. 적용 \* 을 클릭합니다.

선택한 인터페이스가 고가용성 그룹 생성 페이지의 인터페이스 섹션에 나열됩니다. 기본적으로 목록의 첫 번째 인터페이스가 기본 설정 마스터로 선택됩니다.

## Create High Availability Group

### High Availability Group

Name

Description

### Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Select Interfaces

Node Name	Interface	IPv4 Subnet	Preferred Master
g140-g1	eth2	47.47.0.0/21	<input checked="" type="radio"/>
g140-g2	eth2	47.47.0.0/21	<input type="radio"/>

Displaying 2 interfaces.

### Virtual IP Addresses

Virtual IP Subnet: 47.47.0.0/21. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1



Cancel

Save

7. 다른 인터페이스를 기본 마스터로 사용하려면 \* Preferred Master \* 열에서 해당 인터페이스를 선택합니다.

장애가 발생하여 VIP 주소가 백업 인터페이스에 재할당되지 않는 한 기본 마스터는 활성 인터페이스입니다.



HA 그룹이 그리드 관리자에 대한 액세스를 제공하는 경우 기본 관리 노드에서 기본 마스터로 사용할 인터페이스를 선택해야 합니다. 일부 유지 보수 절차는 기본 관리 노드에서만 수행할 수 있습니다.

8. 페이지의 가상 IP 주소 섹션에서 HA 그룹에 대한 가상 IP 주소를 1~10개 입력합니다. 더하기 기호(+)

IPv4 주소를 하나 이상 입력해야 합니다. 선택적으로 추가 IPv4 및 IPv6 주소를 지정할 수 있습니다.

IPv4 주소는 모든 멤버 인터페이스에서 공유하는 IPv4 서브넷 내에 있어야 합니다.

9. 저장 \* 을 클릭합니다.

HA 그룹이 생성되고 이제 구성된 가상 IP 주소를 사용할 수 있습니다.

관련 정보

["Red Hat Enterprise Linux 또는 CentOS를 설치합니다"](#)

["VMware를 설치합니다"](#)

["Ubuntu 또는 Debian을 설치합니다"](#)

["로드 밸런싱 관리"](#)

## 고가용성 그룹 편집

HA(고가용성) 그룹을 편집하여 이름과 설명을 변경하거나, 인터페이스를 추가 또는 제거하거나, 가상 IP 주소를 추가 또는 업데이트할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.

이 작업에 대해

HA 그룹을 편집하는 몇 가지 이유는 다음과 같습니다.

- 기존 그룹에 인터페이스 추가 인터페이스 IP 주소는 그룹에 이미 할당된 다른 인터페이스와 동일한 서브넷 내에 있어야 합니다.
- HA 그룹에서 인터페이스 제거 예를 들어 그리드 네트워크 또는 클라이언트 네트워크에 대한 노드의 인터페이스가 HA 그룹에서 사용되는 경우 사이트 또는 노드 서비스 해제 절차를 시작할 수 없습니다.

단계

1. 구성 \* > \* 네트워크 설정 \* > \* 고가용성 그룹 \* 을 선택합니다.

High Availability Groups 페이지가 나타납니다.

### High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

+ Create Edit Remove				
	Name	Description	Virtual IP Addresses	Interfaces
<input type="radio"/>	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
<input type="radio"/>	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

Displaying 2 HA groups.

2. 편집할 HA 그룹을 선택하고 \* 편집 \* 을 클릭합니다.

High Availability Group 편집 대화 상자가 나타납니다.

- 필요에 따라 그룹의 이름 또는 설명을 업데이트합니다.
- 필요에 따라 \* 인터페이스 선택 \* 을 클릭하여 HA 그룹의 인터페이스를 변경합니다.

High Availability Group에 인터페이스 추가 대화 상자가 나타납니다.

### Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
	g140-g1	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g1	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g3	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g3	eth2	192.168.0.0/21	
	g140-g4	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

DHCP에서 IP 주소를 할당한 경우 인터페이스가 목록에 나타나지 않습니다.

- 확인란을 선택하거나 선택 취소하여 인터페이스를 추가하거나 제거합니다.

인터페이스 선택에 대한 다음 지침을 참조하십시오.

- 인터페이스를 하나 이상 선택해야 합니다.
- 둘 이상의 인터페이스를 선택하는 경우 모든 인터페이스가 그리드 네트워크(eth0) 또는 클라이언트 네트워크(eth2)에 있어야 합니다.
- 모든 인터페이스는 동일한 서브넷 또는 공통 접두사가 있는 서브넷에 있어야 합니다.

IP 주소는 가장 작은 서브넷(접두사가 가장 큰 서브넷)으로 제한됩니다.

- 다른 노드 유형의 인터페이스를 선택하고 페일오버가 발생하는 경우 선택한 노드에 공통되는 서비스만 가상 IP에서 사용할 수 있습니다.
  - Grid Manager 또는 Tenant Manager의 HA 보호를 위해 두 개 이상의 관리 노드를 선택합니다.
  - 로드 밸런서 서비스의 HA 보호를 위해 두 개 이상의 관리 노드, 게이트웨이 노드 또는 둘 다를 선택합니다.
  - CLB 서비스의 HA 보호를 위해 둘 이상의 게이트웨이 노드를 선택합니다.



CLB 서비스는 더 이상 사용되지 않습니다.

- 적용 \* 을 클릭합니다.

선택한 인터페이스가 페이지의 인터페이스 섹션에 나열됩니다. 기본적으로 목록의 첫 번째 인터페이스가 기본 설정 마스터로 선택됩니다.

### Edit High Availability Group 'HA Group - Admin Nodes'

---

#### High Availability Group

Name

Description

---

#### Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Select Interfaces

Node Name	Interface	IPv4 Subnet	Preferred Master
DC1-ADM1	eth0	10.96.100.0/23	<input checked="" type="radio"/>
DC2-ADM1	eth0	10.96.100.0/23	<input type="radio"/>

Displaying 2 interfaces.

---

#### Virtual IP Addresses

Virtual IP Subnet: 10.96.100.0/23. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1  +

Cancel
Save

7. 다른 인터페이스를 기본 마스터로 사용하려면 \* Preferred Master \* 열에서 해당 인터페이스를 선택합니다.

장애가 발생하여 VIP 주소가 백업 인터페이스에 재할당되지 않는 한 기본 마스터는 활성 인터페이스입니다.



HA 그룹이 그리드 관리자에 대한 액세스를 제공하는 경우 기본 관리 노드에서 기본 마스터로 사용할 인터페이스를 선택해야 합니다. 일부 유지 보수 절차는 기본 관리 노드에서만 수행할 수 있습니다.

8. 필요에 따라 HA 그룹의 가상 IP 주소를 업데이트합니다.

IPv4 주소를 하나 이상 입력해야 합니다. 선택적으로 추가 IPv4 및 IPv6 주소를 지정할 수 있습니다.

IPv4 주소는 모든 멤버 인터페이스에서 공유하는 IPv4 서브넷 내에 있어야 합니다.

9. 저장 \* 을 클릭합니다.

HA 그룹이 업데이트됩니다.

## 고가용성 그룹을 제거하는 중입니다

더 이상 사용하지 않는 고가용성(HA) 그룹을 제거할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 루트 액세스 권한이 있어야 합니다.

이 작업을 시작합니다

HA 그룹을 제거하면 그룹의 가상 IP 주소 중 하나를 사용하도록 구성된 S3 또는 Swift 클라이언트가 더 이상 StorageGRID에 연결할 수 없습니다. 클라이언트 중단을 방지하려면 HA 그룹을 삭제하기 전에 영향을 받는 모든 S3 또는 Swift 클라이언트 애플리케이션을 업데이트해야 합니다. 다른 IP 주소(예: 다른 HA 그룹의 가상 IP 주소 또는 설치 중 또는 DHCP를 사용하는 동안 인터페이스에 구성된 IP 주소)를 사용하여 연결할 각 클라이언트를 업데이트합니다.

단계

1. 구성 \* > \* 네트워크 설정 \* > \* 고가용성 그룹 \* 을 선택합니다.

High Availability Groups 페이지가 나타납니다.

### High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

	Name	Description	Virtual IP Addresses	Interfaces
<input type="radio"/>	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
<input type="radio"/>	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

Displaying 2 HA groups.

2. 제거할 HA 그룹을 선택하고 \* 제거 \* 를 클릭합니다.

High Availability Group 삭제 경고가 나타납니다.

## ⚠ Warning

### Delete High Availability Group

Are you sure you want to delete High Availability Group 'HA group 1'?

Cancel

OK

3. 확인 \* 을 클릭합니다.

HA 그룹이 제거됩니다.

## S3 API 엔드포인트 도메인 이름 구성

S3 가상 호스팅 스타일 요청을 지원하려면 Grid Manager를 사용하여 S3 클라이언트가 연결하는 끝점 도메인 이름 목록을 구성해야 합니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.
- 그리드 업그레이드가 진행 중이 아닌 것을 확인해야 합니다.



그리드 업그레이드가 진행 중일 때는 도메인 이름 구성을 변경하지 마십시오.

이 작업에 대해

클라이언트가 S3 엔드 포인트 도메인 이름을 사용하도록 설정하려면 다음 작업을 모두 수행해야 합니다.

- 그리드 관리자를 사용하여 StorageGRID 시스템에 S3 끝점 도메인 이름을 추가합니다.
- 클라이언트가 StorageGRID에 대한 HTTPS 연결에 사용하는 인증서가 클라이언트에 필요한 모든 도메인 이름에 서명되었는지 확인합니다.

예를 들어, 끝점이 인 경우 `s3.company.com`HTTPS 연결에 사용되는 인증서에 가 포함되어 있는지 확인해야 합니다 `s3.company.com 끝점 및 끝점의 와일드카드 주체 대체 이름(SAN): *.s3.company.com.`

- 클라이언트가 사용하는 DNS 서버를 구성합니다. 클라이언트가 연결하는 데 사용하는 IP 주소에 대한 DNS 레코드를 포함하고 와일드카드 이름을 포함하여 레코드가 필요한 모든 끝점 도메인 이름을 참조하는지 확인합니다.



클라이언트는 게이트웨이 노드, 관리 노드 또는 스토리지 노드의 IP 주소를 사용하거나 고가용성 그룹의 가상 IP 주소에 연결하여 StorageGRID에 연결할 수 있습니다. DNS 레코드에 올바른 IP 주소를 포함하도록 클라이언트 응용 프로그램이 그리드에 연결하는 방법을 이해해야 합니다.

클라이언트가 HTTPS 연결에 사용하는 인증서는 클라이언트가 그리드에 연결하는 방식에 따라 달라집니다.

- 클라이언트가 로드 밸런서 서비스를 사용하여 연결하는 경우 이 클라이언트는 특정 로드 밸런서 끝점에 대한

인증서를 사용합니다.



각 로드 밸런서 끝점마다 고유한 인증서가 있으며 각 끝점이 서로 다른 끝점 도메인 이름을 인식하도록 구성할 수 있습니다.

- 클라이언트가 스토리지 노드 또는 게이트웨이 노드의 CLB 서비스에 접속하는 경우 클라이언트는 필요한 모든 끝점 도메인 이름을 포함하도록 업데이트된 그리드 사용자 지정 서버 인증서를 사용합니다.



CLB 서비스는 더 이상 사용되지 않습니다.

단계

1. 구성 > \* 네트워크 설정 > \* 도메인 이름 \* 을 선택합니다.

끝점 도메인 이름 페이지가 나타납니다.

Endpoint Domain Names

#### Virtual Hosted-Style Requests

Enable support of S3 virtual hosted-style requests by specifying API endpoint domain names. Support is disabled if this list is empty. Examples: s3.example.com, s3.example.co.uk, s3-east.example.com

Endpoint 1	<input type="text" value="s3.example.com"/>	✕
Endpoint 2	<input type="text"/>	+ ✕
<input type="button" value="Save"/>		

2. (+) 아이콘을 사용하여 추가 필드를 추가하려면 \* Endpoint \* 필드에 S3 API 끝점 도메인 이름 목록을 입력합니다.

이 목록이 비어 있으면 S3 가상 호스팅 스타일 요청에 대한 지원이 비활성화됩니다.

3. 저장 \* 을 클릭합니다.
4. 클라이언트가 사용하는 서버 인증서가 필요한 끝점 도메인 이름과 일치하는지 확인합니다.
  - 로드 밸런서 서비스를 사용하는 클라이언트의 경우 클라이언트가 연결하는 로드 밸런서 끝점과 연결된 인증서를 업데이트합니다.
  - 스토리지 노드에 직접 접속하거나 게이트웨이 노드에서 CLB 서비스를 사용하는 클라이언트의 경우 그리드의 사용자 지정 서버 인증서를 업데이트합니다.
5. 엔드포인트 도메인 이름 요청을 확인하는 데 필요한 DNS 레코드를 추가합니다.

결과

이제 클라이언트가 끝점을 사용할 때 `bucket.s3.company.com` DNS 서버가 올바른 끝점으로 확인되고 인증서는 끝점을 예상대로 인증합니다.

관련 정보

["S3을 사용합니다"](#)

["IP 주소 보기"](#)

"고가용성 그룹 생성"

"스토리지 노드 또는 CLB 서비스에 연결하기 위한 사용자 지정 서버 인증서 구성"

"부하 분산 장치 엔드포인트 구성"

## 클라이언트 통신을 위해 HTTP 활성화

기본적으로 클라이언트 응용 프로그램은 스토리지 노드에 대한 모든 연결 또는 게이트웨이 노드의 더 이상 사용되지 않는 CLB 서비스에 대해 HTTPS 네트워크 프로토콜을 사용합니다. 비프로덕션 그리드를 테스트할 때와 같이 이러한 연결에 대해 HTTP를 선택적으로 활성화할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

S3 및 Swift 클라이언트가 HTTP를 스토리지 노드 또는 게이트웨이 노드의 더 이상 사용되지 않는 CLB 서비스에 직접 연결해야 하는 경우에만 이 작업을 완료합니다.

HTTPS 연결만 사용하는 클라이언트 또는 로드 밸런서 서비스에 연결된 클라이언트에 대해서는 이 작업을 완료할 필요가 없습니다. 각 로드 밸런서 끝점에서 HTTP 또는 HTTPS를 사용하도록 구성할 수 있기 때문입니다. 자세한 내용은 로드 밸런서 엔드포인트 구성에 대한 정보를 참조하십시오.

을 참조하십시오. "요약: 클라이언트 연결을 위한 IP 주소 및 포트" 스토리지 노드에 연결할 때 또는 HTTP 또는 HTTPS를 사용하여 더 이상 사용되지 않는 CLB 서비스에 연결할 때 사용하는 S3 및 Swift 포트에 대해 알아보십시오



요청이 암호화되지 않은 상태로 전송되므로 프로덕션 그리드에 대해 HTTP를 설정할 때는 주의해야 합니다.

단계

1. 구성 \*\* 시스템 설정 \* 그리드 옵션 \* 을 선택합니다.
2. 네트워크 옵션 섹션에서 \* HTTP 연결 사용 \* 확인란을 선택합니다.

### Network Options



3. 저장 \* 을 클릭합니다.

관련 정보

"부하 분산 장치 엔드포인트 구성"

"S3을 사용합니다"

"Swift를 사용합니다"

## 허용되는 클라이언트 작업을 제어합니다

클라이언트 수정 방지 그리드 옵션을 선택하여 특정 HTTP 클라이언트 작업을 거부할 수 있습니다.

필요한 것

- 지원되는 브라우저를 사용하여 Grid Manager에 로그인해야 합니다.
- 특정 액세스 권한이 있어야 합니다.

이 작업에 대해

클라이언트 수정 방지 는 시스템 전체 설정입니다. 클라이언트 수정 방지 옵션을 선택하면 다음 요청이 거부됩니다.

- \* S3 REST API \*
  - 버킷 요청을 삭제합니다
  - 기존 오브젝트의 데이터, 사용자 정의 메타데이터 또는 S3 오브젝트 태그 지정을 수정하는 요청



이 설정은 버전 관리가 활성화된 버킷에는 적용되지 않습니다. 버전 관리를 사용하면 이미 개체 데이터, 사용자 정의 메타데이터 및 개체 태그 지정을 수정할 수 없습니다.

- \* Swift REST API \*
  - 컨테이너 요청을 삭제합니다
  - 기존 객체 수정 요청. 예를 들어, 덮어쓰기, 삭제, 메타데이터 업데이트 등의 작업이 거부됩니다.

단계

1. 구성 \*\* 시스템 설정 \* 그리드 옵션 \* 을 선택합니다.
2. 네트워크 옵션 섹션에서 \* 클라이언트 수정 방지 \* 확인란을 선택합니다.

### Network Options

Prevent Client Modification

Enable HTTP Connection

Network Transfer Encryption  AES128-SHA  AES256-SHA

3. 저장 \* 을 클릭합니다.

## 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.