



서버 인증서를 구성하는 중입니다

StorageGRID 11.5

NetApp
April 11, 2024

목차

서버 인증서를 구성하는 중입니다	1
지원되는 유형의 사용자 지정 서버 인증서	1
로드 밸런서 끝점용 인증서	1
Grid Manager 및 테넌트 관리자에 대한 사용자 지정 서버 인증서 구성	1
Grid Manager 및 Tenant Manager에 대한 기본 서버 인증서 복원	2
스토리지 노드 또는 CLB 서비스에 연결하기 위한 사용자 지정 서버 인증서 구성	3
S3 및 Swift REST API 엔드포인트에 대한 기본 서버 인증서 복원	4
StorageGRID 시스템의 CA 인증서를 복사하는 중입니다	4
FabricPool용 StorageGRID 인증서 구성	5
관리 인터페이스에 대해 자체 서명된 서버 인증서를 생성하는 중입니다	6

서버 인증서를 구성하는 중입니다

StorageGRID 시스템에서 사용하는 서버 인증서를 사용자 지정할 수 있습니다.

StorageGRID 시스템은 다음과 같은 여러 가지 목적으로 보안 인증서를 사용합니다.

- 관리 인터페이스 서버 인증서: 그리드 관리자, 테넌트 관리자, 그리드 관리 API 및 테넌트 관리 API에 대한 액세스를 보호하는 데 사용됩니다.
- 스토리지 API 서버 인증서: API 클라이언트 애플리케이션이 객체 데이터를 업로드 및 다운로드하는 데 사용하는 스토리지 노드 및 게이트웨이 노드에 대한 액세스를 보호하는 데 사용됩니다.

설치 중에 생성된 기본 인증서를 사용하거나 이러한 기본 인증서 유형 중 하나 또는 둘 다를 사용자 지정 인증서로 바꿀 수 있습니다.

지원되는 유형의 사용자 지정 서버 인증서

StorageGRID 시스템은 RSA 또는 ECDSA(Elliptic Curve Digital Signature Algorithm)로 암호화된 사용자 지정 서버 인증서를 지원합니다.

StorageGRID가 REST API용 클라이언트 연결을 보호하는 방법에 대한 자세한 내용은 S3 또는 Swift 구현 가이드를 참조하십시오.

로드 밸런서 끝점용 인증서

StorageGRID는 로드 밸런서 끝점에 사용되는 인증서를 별도로 관리합니다. 로드 밸런서 인증서를 구성하려면 로드 밸런서 끝점을 구성하는 지침을 참조하십시오.

관련 정보

["S3을 사용합니다"](#)

["Swift를 사용합니다"](#)

["부하 분산 장치 엔드포인트 구성"](#)

Grid Manager 및 테넌트 관리자에 대한 사용자 지정 서버 인증서 구성

기본 StorageGRID 서버 인증서를 단일 사용자 지정 서버 인증서로 교체하여 보안 경고가 발생하지 않고 사용자가 그리드 관리자 및 테넌트 관리자에 액세스할 수 있도록 할 수 있습니다.

이 작업에 대해

기본적으로 모든 관리 노드에는 그리드 CA에서 서명한 인증서가 발급됩니다. 이러한 CA 서명 인증서는 하나의 공통 사용자 지정 서버 인증서 및 해당 개인 키로 대체할 수 있습니다.

단일 사용자 지정 서버 인증서가 모든 관리 노드에 사용되므로 클라이언트가 Grid Manager 및 Tenant Manager에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 사용자 지정 인증서를 정의하여 그리드의 모든 관리 노드와 일치시킵니다.

서버에서 구성을 완료해야 하며 사용 중인 루트 CA(인증 기관)에 따라 사용자가 그리드 관리자 및 테넌트 관리자에 액세스하는 데 사용할 웹 브라우저에 루트 CA 인증서를 설치해야 할 수도 있습니다.



실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 이 서버 인증서가 만료될 때 * Management Interface * 용 서버 인증서 만료 알림과 레거시 관리 인터페이스 인증서 만료(MCEP) 경보가 모두 트리거됩니다. 필요에 따라 * 지원 * > * 도구 * > * 그리드 토폴로지 * 를 선택하여 현재 서비스 인증서가 만료될 때까지 일 수를 확인할 수 있습니다. 그런 다음 *기본 관리 노드 * > * CMN * > * 리소스 * 를 선택합니다.



IP 주소 대신 도메인 이름을 사용하여 Grid Manager 또는 Tenant Manager에 액세스하는 경우, 다음 중 하나가 발생할 경우 브라우저에 인증서 오류가 표시되지 않고 무시하도록 옵션이 표시되지 않습니다.

- 사용자 지정 관리 인터페이스 서버 인증서가 만료됩니다.
- 사용자 지정 관리 인터페이스 서버 인증서를 기본 서버 인증서로 되돌립니다.

단계

1. 구성 * > * 네트워크 설정 * > * 서버 인증서 * 를 선택합니다.
2. 관리 인터페이스 서버 인증서 섹션에서 * 사용자 정의 인증서 설치 * 를 클릭합니다.
3. 필요한 서버 인증서 파일을 업로드합니다.
 - * 서버 인증서 *: 사용자 정의 서버 인증서 파일 (.crt)를 클릭합니다.
 - * 서버 인증서 개인 키 *: 사용자 지정 서버 인증서 개인 키 파일입니다 (.key)를 클릭합니다.



EC 개인 키는 224비트 이상이어야 합니다. RSA 개인 키는 2048비트 이상이어야 합니다.

- * CA 번들 *: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.
4. 저장 * 을 클릭합니다.

사용자 지정 서버 인증서는 이후의 모든 새 클라이언트 연결에 사용됩니다.

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



새 인증서를 업로드한 후 관련 인증서 만료 알림(또는 레거시 알림)이 지워지도록 최대 1일을 허용합니다.

5. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

Grid Manager 및 Tenant Manager에 대한 기본 서버 인증서 복원

Grid Manager 및 Tenant Manager에 대한 기본 서버 인증서를 사용하도록 되돌릴 수 있습니다.

단계

1. 구성 * > * 네트워크 설정 * > * 서버 인증서 * 를 선택합니다.
2. 인터페이스 서버 인증서 관리 섹션에서 * 기본 인증서 사용 * 을 클릭합니다.

3. 확인 대화 상자에서 * 확인 * 을 클릭합니다.

기본 서버 인증서를 복원하면 구성된 사용자 지정 서버 인증서 파일이 삭제되고 시스템에서 복구할 수 없습니다. 이후의 모든 새 클라이언트 연결에 기본 서버 인증서가 사용됩니다.

4. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

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

스토리지 노드에 대한 S3 또는 Swift 클라이언트 연결에 사용되는 서버 인증서 또는 게이트웨이 노드의 CLB 서비스(더 이상 사용되지 않음)를 교체할 수 있습니다. 교체 사용자 지정 서버 인증서는 조직에 따라 다릅니다.

이 작업에 대해

기본적으로 모든 스토리지 노드에는 그리드 CA에서 서명한 X.509 서버 인증서가 발급됩니다. 이러한 CA 서명 인증서는 하나의 공통 사용자 지정 서버 인증서 및 해당 개인 키로 대체할 수 있습니다.

단일 사용자 지정 서버 인증서가 모든 스토리지 노드에 사용되므로 클라이언트가 스토리지 끝점에 연결할 때 호스트 이름을 확인해야 하는 경우 인증서를 와일드카드 또는 다중 도메인 인증서로 지정해야 합니다. 사용자 지정 인증서를 정의하여 그리드의 모든 스토리지 노드와 일치시킵니다.

서버에서 구성을 완료한 후 사용하는 루트 CA(인증 기관)에 따라 시스템에 액세스하는 데 사용할 S3 또는 Swift API 클라이언트에 루트 CA 인증서를 설치해야 할 수도 있습니다.



실패한 서버 인증서로 인해 작업이 중단되지 않도록 하려면 * Storage API Endpoints * 용 서버 인증서 만료 알림과 레거시 Storage API Service Endpoints 인증서 만료(SCEP) 경보가 모두 루트 서버 인증서가 만료될 때 트리거됩니다. 필요에 따라 * Support *** Tools ** Grid Topology * 를 선택하여 현재 서비스 인증서가 만료될 때까지 일 수를 확인할 수 있습니다. 그런 다음 *기본 관리 노드 ** CMN * 리소스 * 를 선택합니다.

사용자 지정 인증서는 클라이언트가 게이트웨이 노드에서 더 이상 사용되지 않는 CLB 서비스를 사용하여 StorageGRID에 연결하거나 스토리지 노드에 직접 연결하는 경우에만 사용됩니다. 관리 노드 또는 게이트웨이 노드에서 로드 밸런서 서비스를 사용하여 StorageGRID에 연결하는 S3 또는 Swift 클라이언트는 로드 밸런서 끝점에 대해 구성된 인증서를 사용합니다.



곧 만료되는 로드 밸런서 끝점에 대해 * 로드 밸런서 끝점 인증서 만료 * 경고가 트리거됩니다.

단계

1. 구성 * > * 네트워크 설정 * > * 서버 인증서 * 를 선택합니다.
2. 개체 스토리지 API 서비스 끝점 서버 인증서 섹션에서 * 사용자 지정 인증서 설치 * 를 클릭합니다.
3. 필요한 서버 인증서 파일을 업로드합니다.
 - * 서버 인증서 *: 사용자 정의 서버 인증서 파일 (.crt)를 클릭합니다.
 - * 서버 인증서 개인 키 *: 사용자 지정 서버 인증서 개인 키 파일입니다 (.key)를 클릭합니다.



EC 개인 키는 224비트 이상이어야 합니다. RSA 개인 키는 2048비트 이상이어야 합니다.

- * CA 번들 *: 각 중간 발급 CA(인증 기관)의 인증서를 포함하는 단일 파일입니다. 파일에는 인증서 체인 순서에 연결된 PEM 인코딩된 CA 인증서 파일이 각각 포함되어야 합니다.

4. 저장 * 을 클릭합니다.

사용자 지정 서버 인증서는 이후의 모든 새 API 클라이언트 연결에 사용됩니다.

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



새 인증서를 업로드한 후 관련 인증서 만료 알림(또는 레거시 알림)이 지워지도록 최대 1일을 허용합니다.

5. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

관련 정보

["S3을 사용합니다"](#)

["Swift를 사용합니다"](#)

["S3 API 엔드포인트 도메인 이름 구성"](#)

S3 및 Swift REST API 엔드포인트에 대한 기본 서버 인증서 복원

S3 및 Swift REST API 엔드포인트에 대한 기본 서버 인증서를 사용하여 로 되돌릴 수 있습니다.

단계

1. 구성 * > * 네트워크 설정 * > * 서버 인증서 * 를 선택합니다.
2. 개체 스토리지 API 서비스 끝점 서버 인증서 섹션에서 * 기본 인증서 사용 * 을 클릭합니다.
3. 확인 대화 상자에서 * 확인 * 을 클릭합니다.

객체 저장소 API 끝점에 대한 기본 서버 인증서를 복원하면 구성한 사용자 지정 서버 인증서 파일이 삭제되고 시스템에서 복구할 수 없습니다. 이후의 모든 새 API 클라이언트 연결에 기본 서버 인증서가 사용됩니다.

4. 페이지를 새로 고쳐 웹 브라우저가 업데이트되도록 합니다.

StorageGRID 시스템의 CA 인증서를 복사하는 중입니다

StorageGRID는 내부 CA(인증 기관)를 사용하여 내부 트래픽을 보호합니다. 인증서를 업로드해도 이 인증서는 변경되지 않습니다.

필요한 것

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

이 작업에 대해

사용자 지정 서버 인증서가 구성된 경우 클라이언트 응용 프로그램은 사용자 지정 서버 인증서를 사용하여 서버를

확인해야 합니다. StorageGRID 시스템에서 CA 인증서를 복사해서는 안 됩니다.

단계

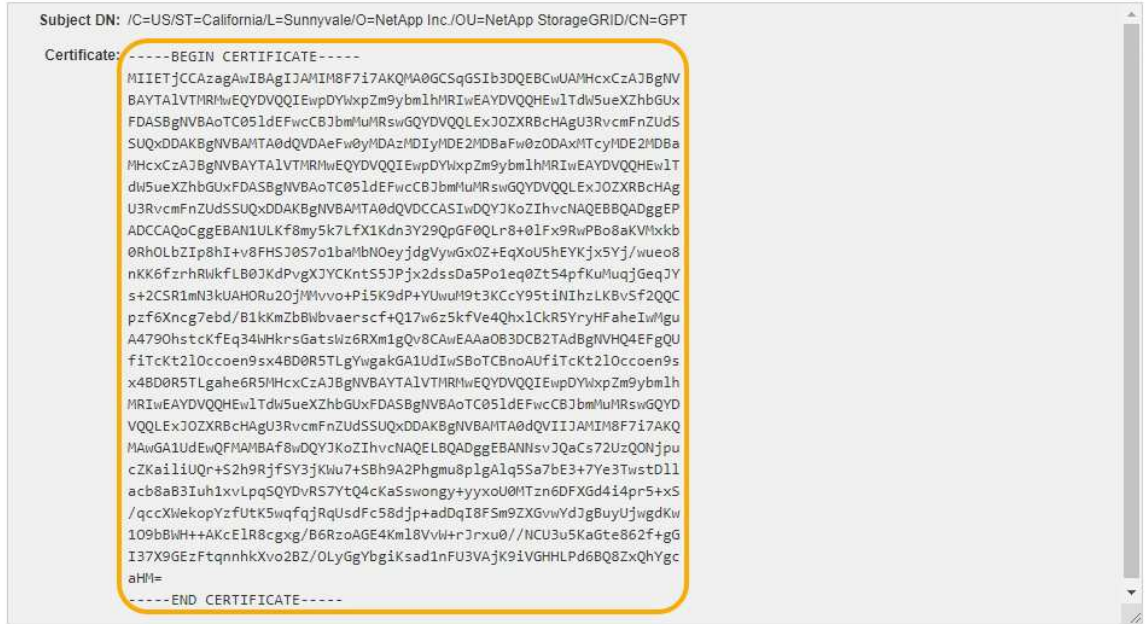
1. 구성 * > * 네트워크 설정 * > * 서버 인증서 * 를 선택합니다.
2. 내부 CA 인증서 * 섹션에서 모든 인증서 텍스트를 선택합니다.

반드시 포함해야 합니다 -----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 선택합니다.

Internal CA Certificate

StorageGRID uses an internal Certificate Authority (CA) to secure internal traffic. This certificate does not change if you upload your own certificates.

To export the internal CA certificate, copy all of the certificate text (starting with -----BEGIN CERTIFICATE and ending with END CERTIFICATE-----), and save it as a .pem file.



3. 선택한 텍스트를 마우스 오른쪽 단추로 클릭하고 * 복사 * 를 선택합니다.
4. 복사한 인증서를 텍스트 편집기에 붙여 넣습니다.
5. 파일을 확장자로 저장합니다 .pem.

예를 들면 다음과 같습니다. storagegrid_certificate.pem

FabricPool용 StorageGRID 인증서 구성

엄격한 호스트 이름 유효성 검사를 수행하고 FabricPool를 사용하는 ONTAP 클라이언트와 같은 엄격한 호스트 이름 유효성 검사를 사용하지 않는 S3 클라이언트의 경우 로드 밸런서 끝점을 구성할 때 서버 인증서를 생성하거나 업로드할 수 있습니다.

필요한 것

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

이 작업에 대해

로드 밸런서 끝점을 만들 때 자체 서명된 서버 인증서를 생성하거나 알려진 CA(인증 기관)에서 서명한 인증서를 업로드할 수 있습니다. 프로덕션 환경에서는 알려진 CA가 서명한 인증서를 사용해야 합니다. CA에서 서명한 인증서는 중단 없이 회전할 수 있습니다. 또한 중간자 공격에 대한 보호 기능이 강화되어 보안이 더욱 강화되고 있습니다.

다음 단계에서는 FabricPool을 사용하는 S3 클라이언트에 대한 일반 지침을 제공합니다. 자세한 내용과 절차는 StorageGRID for FabricPool 구성 지침을 참조하십시오.



게이트웨이 노드의 별도의 CLB(연결 로드 밸런서) 서비스는 더 이상 사용되지 않으며 FabricPool에서 더 이상 사용하지 않는 것이 좋습니다.

단계

1. 선택적으로 FabricPool에서 사용할 고가용성(HA) 그룹을 구성합니다.
2. FabricPool에서 사용할 S3 로드 밸런서 끝점을 만듭니다.

HTTPS 로드 밸런서 끝점을 만들면 서버 인증서, 인증서 개인 키 및 CA 번들을 업로드하라는 메시지가 표시됩니다.

3. StorageGRID을 ONTAP의 클라우드 계층으로 연결

로드 밸런서 끝점 포트와 업로드한 CA 인증서에 사용된 정규화된 도메인 이름을 지정합니다. 그런 다음 CA 인증서를 제공합니다.



중간 CA에서 StorageGRID 인증서를 발급한 경우 중간 CA 인증서를 제공해야 합니다. StorageGRID 인증서가 루트 CA에서 직접 발급된 경우 루트 CA 인증서를 제공해야 합니다.

관련 정보

["FabricPool용 StorageGRID를 구성합니다"](#)

관리 인터페이스에 대해 자체 서명된 서버 인증서를 생성하는 중입니다

스크립트를 사용하여 엄격한 호스트 이름 확인이 필요한 관리 API 클라이언트용 자체 서명된 서버 인증서를 생성할 수 있습니다.

필요한 것

- 특정 액세스 권한이 있어야 합니다.
- `passwords.txt` 파일이 있어야 합니다.

이 작업에 대해

프로덕션 환경에서는 알려진 CA(인증 기관)에서 서명한 인증서를 사용해야 합니다. CA에서 서명한 인증서는 중단 없이 회전할 수 있습니다. 또한 중간자 공격에 대한 보호 기능이 강화되어 보안이 더욱 강화되고 있습니다.

단계

1. 각 관리 노드의 FQDN(정규화된 도메인 이름)을 얻습니다.
2. 기본 관리자 노드에 로그인합니다.
 - a. 다음 명령을 입력합니다. `ssh admin@primary_Admin_Node_IP`

- b. 에 나열된 암호를 입력합니다 Passwords.txt 파일.
- c. 루트로 전환하려면 다음 명령을 입력합니다. su -
- d. 에 나열된 암호를 입력합니다 Passwords.txt 파일.

루트로 로그인하면 프롬프트가 에서 변경됩니다 \$ 를 선택합니다 #.

3. 자체 서명된 새 인증서를 사용하여 StorageGRID를 구성합니다.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- 용 --domains`에서 와일드카드를 사용하여 모든 관리 노드의 정규화된 도메인 이름을 나타냅니다. 예를 들면, 다음과 같습니다. `*.ui.storagegrid.example.com 와일드카드를 사용하여 나타냅니다 admin1.ui.storagegrid.example.com 및 admin2.ui.storagegrid.example.com.
- 설정 --type 를 선택합니다 management Grid Manager 및 Tenant Manager에서 사용하는 인증서를 구성합니다.
- 기본적으로 생성된 인증서는 1년(365일) 동안 유효하며 만료되기 전에 다시 만들어야 합니다. 를 사용할 수 있습니다 --days 기본 유효 기간을 재정의하는 인수입니다.



인증서의 유효 기간은 언제 시작됩니다 make-certificate 가 실행됩니다. 관리 API 클라이언트가 StorageGRID와 동일한 시간 소스와 동기화되어 있는지 확인해야 합니다. 그렇지 않으면 클라이언트가 인증서를 거부할 수 있습니다.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 365
```

결과 출력에는 관리 API 클라이언트에 필요한 공용 인증서가 포함됩니다.

4. 인증서를 선택하고 복사합니다.

선택 항목에 BEGIN 및 END 태그를 포함합니다.

- 5. 명령 셸에서 로그아웃합니다. \$ exit
- 6. 인증서가 구성되었는지 확인합니다.
 - a. 그리드 관리자에 액세스합니다.
 - b. 구성 ** 서버 인증서 * 관리 인터페이스 서버 인증서 * 를 선택합니다.
- 7. 복사한 공용 인증서를 사용하도록 관리 API 클라이언트를 구성합니다. BEGIN 및 END Tags를 포함합니다.

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.