



LDAP를 사용합니다

ONTAP 9

NetApp
April 24, 2024

목차

| | |
|---------------------------------------|---|
| LDAP를 사용합니다..... | 1 |
| LDAP 사용 개요..... | 1 |
| 새 LDAP 클라이언트 스키마를 생성합니다 | 2 |
| LDAP 클라이언트 구성을 생성합니다 | 3 |
| LDAP 클라이언트 구성을 SVM과 연결합니다 | 7 |
| 이름 서비스 스위치 테이블에서 LDAP 소스를 확인합니다 | 8 |

LDAP를 사용합니다

LDAP 사용 개요

환경에서 LDAP를 네임 서비스로 사용하는 경우 LDAP 관리자와 협력하여 요구사항 및 적절한 스토리지 시스템 구성을 결정한 다음 SVM을 LDAP 클라이언트로 설정해야 합니다.

ONTAP 9.10.1부터 LDAP 채널 바인딩은 Active Directory 및 이름 서비스 LDAP 연결에 대해 기본적으로 지원됩니다. ONTAP는 시작 TLS 또는 LDAPS가 활성화되고 세션 보안이 서명 또는 봉인으로 설정된 경우에만 LDAP 연결을 사용하여 채널 바인딩을 시도합니다. 이름 서버에서 LDAP 채널 바인딩을 비활성화하거나 다시 활성화하려면 LDAP 클라이언트 modify 명령에 'try-channel-binding' 매개 변수를 사용합니다.

자세한 내용은 을 참조하십시오 "[Windows의 2020 LDAP 채널 바인딩 및 LDAP 서명 요구 사항](#)".

- ONTAP용 LDAP를 구성하기 전에 사이트 배포가 LDAP 서버 및 클라이언트 구성에 대한 모범 사례를 충족하는지 확인해야 합니다. 특히 다음 조건을 충족해야 합니다.
 - LDAP 서버의 도메인 이름이 LDAP 클라이언트의 항목과 일치해야 합니다.
 - LDAP 서버에서 지원하는 LDAP 사용자 암호 해시 유형에는 ONTAP에서 지원하는 해시 유형이 포함되어야 합니다.
 - 암호화(모든 유형) 및 SHA-1(SHA, SSHA).
 - ONTAP 9.8부터 SHA-2 해시(SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, SSHA-512)도 지원됩니다.
 - LDAP 서버에 세션 보안 조치가 필요한 경우 LDAP 클라이언트에서 이를 구성해야 합니다.

다음 세션 보안 옵션을 사용할 수 있습니다.

- LDAP 서명(데이터 무결성 검사 제공) 및 LDAP 서명 및 봉인(데이터 무결성 검사 및 암호화 제공)
- TLS를 시작합니다
- LDAPS(TLS 또는 SSL을 통한 LDAP)
- 서명되고 봉인된 LDAP 쿼리를 사용하려면 다음 서비스를 구성해야 합니다.
 - LDAP 서버는 GSSAPI(Kerberos) SASL 메커니즘을 지원해야 합니다.
 - LDAP 서버에는 DNS 서버에 설정된 PTR 레코드와 DNS A/AAAA 레코드가 있어야 합니다.
 - Kerberos 서버는 DNS 서버에 SRV 레코드가 있어야 합니다.
- 시작 TLS 또는 LDAPS를 활성화하려면 다음 사항을 고려해야 합니다.
 - LDAPS 대신 Start TLS를 사용하는 것이 NetApp 모범 사례입니다.
 - LDAPS를 사용하는 경우 ONTAP 9.5 이상에서 TLS 또는 SSL에 대해 LDAP 서버를 활성화해야 합니다. SSL은 ONTAP 9.0-9.4에서 지원되지 않습니다.
 - 도메인에 인증서 서버가 이미 구성되어 있어야 합니다.
- ONTAP 9.5 이상에서 LDAP 조회 추적을 활성화하려면 다음 조건을 충족해야 합니다.
 - 두 도메인은 다음 신뢰 관계 중 하나로 구성해야 합니다.

- 양방향
- 원웨이 - 프라이머리(primary)가 추천 도메인을 신뢰하는 곳입니다
- 부모-자식
- DNS는 참조된 모든 서버 이름을 확인하도록 구성되어야 합니다.
- 도메인 암호는 -bind-as-cifs-server가 true로 설정된 경우 인증하기 위해 동일해야 합니다.

LDAP 조회 추적에는 다음 구성이 지원되지 않습니다.



- 모든 ONTAP 버전:
 - 관리 SVM의 LDAP 클라이언트
- ONTAP 9.8 및 이전 버전(9.9.1 이상에서 지원됨):
 - LDAP 서명 및 봉인('-session-security' 옵션)
 - 암호화된 TLS 연결('-use-start-tls' 옵션)
 - LDAPS 포트 636을 통한 통신('-use-ldaps-for-ad-ldap' 옵션)

- SVM에서 LDAP 클라이언트를 구성할 때 LDAP 스키마를 입력해야 합니다.

대부분의 경우 기본 ONTAP 스키마 중 하나가 적합합니다. 그러나 사용자 환경의 LDAP 스키마가 이러한 스키마와 다른 경우 LDAP 클라이언트를 생성하기 전에 ONTAP에 대한 새 LDAP 클라이언트 스키마를 만들어야 합니다. 사용자 환경의 요구 사항에 대해서는 LDAP 관리자에게 문의하십시오.

- 호스트 이름 확인에 LDAP를 사용하는 것은 지원되지 않습니다.

를 참조하십시오

- ["NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법"](#)
- ["SVM에 자체 서명된 루트 CA 인증서를 설치합니다"](#)

새 LDAP 클라이언트 스키마를 생성합니다

사용자 환경의 LDAP 스키마가 ONTAP 기본값과 다른 경우 LDAP 클라이언트 구성을 생성하기 전에 ONTAP에 대한 새 LDAP 클라이언트 스키마를 만들어야 합니다.

이 작업에 대해

대부분의 LDAP 서버는 ONTAP에서 제공하는 기본 스키마를 사용할 수 있습니다.

- MS-AD-BIS(대부분의 Windows 2012 이상 AD 서버에 대한 기본 스키마)
- AD-IDMU(Windows 2008, Windows 2012 이상 AD 서버)
- AD-SFU(Windows 2003 및 이전 AD 서버)
- RFC-2307(UNIX LDAP 서버)

기본값이 아닌 LDAP 스키마를 사용해야 하는 경우 LDAP 클라이언트 구성을 생성하기 전에 만들어야 합니다. 새 스키마를 만들기 전에 LDAP 관리자에게 문의하십시오.

ONTAP에서 제공하는 기본 LDAP 스키마는 수정할 수 없습니다. 새 스키마를 만들려면 복사본을 만든 다음 복사본을 적절하게 수정합니다.

단계

1. 기존 LDAP 클라이언트 스키마 템플릿을 표시하여 복사할 템플릿을 식별합니다.

'vserver services name-service ldap client schema show'를 참조하십시오

2. 권한 수준을 고급으로 설정합니다.

세트 프리빌리지 고급

3. 기존 LDAP 클라이언트 스키마의 복사본을 만듭니다.

'vserver services name-service LDAP 클라이언트 스키마 복사 - vservice_vservice_name_-
schema_existing_schema_name_-new-schema-name_new_schema_name_'

4. 새 스키마를 수정하고 사용자 환경에 맞게 사용자 지정합니다.

'vserver services name-service LDAP 클라이언트 스키마 수정

5. 관리자 권한 레벨로 돌아갑니다.

'Set-Privilege admin'입니다

LDAP 클라이언트 구성을 생성합니다

ONTAP가 사용자 환경의 외부 LDAP 또는 Active Directory 서비스에 액세스하도록 하려면 먼저 스토리지 시스템에서 LDAP 클라이언트를 설정해야 합니다.

필요한 것

Active Directory 도메인 확인됨 목록의 처음 세 개 서버 중 하나가 작동 중이고 데이터를 제공하고 있어야 합니다. 그렇지 않으면 이 작업이 실패합니다.



여러 대의 서버가 있으며 그 중 어느 시점에서든 3대 이상의 서버가 다운됩니다.

단계

1. "vserver services name-service ldap client create" 명령에 대한 적절한 구성 값을 확인하려면 LDAP 관리자에게 문의하십시오.

- a. LDAP 서버에 대한 도메인 기반 또는 주소 기반 연결을 지정합니다.

AD-DOMAIN과 -SERS 옵션은 상호 배타적입니다.

- Active Directory 도메인에서 LDAP 서버 검색을 설정하려면 '-ad-domain' 옵션을 사용합니다.

- 를 사용할 수 있습니다 -restrict-discovery-to-site LDAP 서버 검색을 지정된 도메인의 CIFS 기본 사이트로 제한하는 옵션입니다. 이 옵션을 사용하는 경우 에서 CIFS 기본 사이트도 지정해야 합니다 -default-site.

- '-preferred-ad-servers' 옵션을 사용하여 심표로 구분된 목록에서 IP 주소로 하나 이상의 기본 Active Directory 서버를 지정할 수 있습니다. 클라이언트를 생성한 후 'vserver services name-service ldap client modify' 명령을 사용하여 이 목록을 수정할 수 있습니다.
- 를 사용합니다 -servers 심표로 구분된 목록의 IP 주소로 하나 이상의 LDAP 서버(Active Directory 또는 UNIX)를 지정하는 옵션입니다.



를 클릭합니다 -servers ONTAP 9.2에서는 이 옵션이 사용되지 않습니다. ONTAP 9.2부터, 는 -ldap-servers 필드가 를 대체합니다 -servers 필드에 입력합니다. 이 필드에는 LDAP 서버의 호스트 이름 또는 IP 주소를 사용할 수 있습니다.

b. 기본 또는 사용자 지정 LDAP 스키마를 지정합니다.

대부분의 LDAP 서버는 ONTAP에서 제공하는 기본 읽기 전용 스키마를 사용할 수 있습니다. 그렇지 않으면 기본 스키마를 사용하는 것이 좋습니다. 이 경우 기본 스키마(읽기 전용)를 복사한 다음 복사본을 수정하여 고유한 스키마를 만들 수 있습니다.

기본 스키마:

- MS-AD-BIS

RFC-2307bis를 기반으로 하는 이 방식은 대부분의 표준 Windows 2012 이상 LDAP 구축에 선호되는 LDAP 스키마입니다.

- AD-IDMU

UNIX용 Active Directory ID 관리를 기반으로 하는 이 스키마는 대부분의 Windows 2008, Windows 2012 이상 AD 서버에 적합합니다.

- AD-SFU

UNIX용 Active Directory 서비스를 기반으로 하는 이 스키마는 대부분의 Windows 2003 및 이전 AD 서버에 적합합니다.

- RFC-2307

RFC-2307(LDAP를 네트워크 정보 서비스로 사용하는 접근 방식)에 따라 이 스키마는 대부분의 UNIX AD 서버에 적합합니다.

c. 바인딩 값을 선택합니다.

- '-min-bind-level{anonymous|simple|sasl}'은 최소 bind authentication level을 지정한다.

기본값은 ' * anonymous * '입니다.

- '-bind-dn_ldap_DN_'은 바인딩 사용자를 지정합니다.

Active Directory 서버의 경우 계정(domain\user) 또는 보안 주체(user@domain.com) 양식에서 사용자를 지정해야 합니다. 그렇지 않으면 고유 이름(CN=user, DC=domain, DC=com) 형식으로 사용자를 지정해야 합니다.

- '-BIND-PASSWORD_PASSWORD_'는 바인딩 암호를 지정합니다.

d. 필요한 경우 세션 보안 옵션을 선택합니다.

LDAP 서버에서 필요한 경우 LDAP 서명 및 봉인 또는 TLS를 통한 LDAP를 활성화할 수 있습니다.

- '--세션-보안{none|sign|seal}'

서명('사인', 데이터 무결성), 서명 및 봉인('씰', 데이터 무결성 및 암호화) 또는 둘 다('없음', 서명 또는 봉인 없음)를 사용할 수 있습니다. 기본값은 '없음'입니다.

또한 서명과 봉인 바인딩이 실패할 경우 바인딩 인증을 '* anonymous *' 또는 '* simple *'로 되돌리지 않으려면 '-min-bind-level' {'s ASL'}을 설정해야 합니다.

- '-use-start-tls'{'true'|'false'}

'* true*'로 설정되어 있고 LDAP 서버가 이를 지원하는 경우 LDAP 클라이언트는 서버에 암호화된 TLS 연결을 사용합니다. 기본값은 '* FALSE *'입니다. 이 옵션을 사용하려면 LDAP 서버의 자체 서명된 루트 CA 인증서를 설치해야 합니다.



스토리지 VM에 도메인에 추가된 SMB 서버가 있고 LDAP 서버가 SMB 서버의 홈 도메인의 도메인 컨트롤러 중 하나인 경우 을 수정할 수 있습니다 -session-security-for-ad -ldap 옵션을 선택합니다 vserver cifs security modify 명령.

e. 포트, 쿼리 및 기준 값을 선택합니다.

기본값을 사용하는 것이 좋지만 LDAP 관리자에게 해당 값이 사용자 환경에 적합한지 확인해야 합니다.

- '-port_port_'는 LDAP 서버 포트를 지정합니다.

기본값은 389입니다.

Start TLS를 사용하여 LDAP 연결을 보호하려면 기본 포트 389를 사용해야 합니다. 시작 TLS는 LDAP 기본 포트 389를 통한 일반 텍스트 연결로 시작되고 해당 연결은 TLS로 업그레이드됩니다. 포트를 변경하면 Start TLS가 실패합니다.

- '-query-timeout_integer_'는 쿼리 시간 제한(초)을 지정합니다.

허용 범위는 1 ~ 10초입니다. 기본값은 3초입니다.

- '-base-dn_ldap_dn_'은 기본 DN을 지정합니다.

필요한 경우 여러 값을 입력할 수 있습니다(예: LDAP 조회 추적을 사용하는 경우). 기본값은 ""(root)입니다.

- '-base-scope'{'base'|'onelevel'|'subtree'}는 기본 검색 범위를 지정합니다.

기본값은 'Subtree'입니다.

- '-referral-enabled'{'true'|'false'}는 LDAP 조회 추적 활성화 여부를 지정합니다.

ONTAP 9.5부터 LDAP 조회 응답이 기본 LDAP 서버에 반환되어 원하는 레코드가 참조된 LDAP 서버에 있음을 나타내는 경우 ONTAP LDAP 클라이언트가 다른 LDAP 서버에 조회 요청을 참조할 수 있습니다. 기본값은 '* FALSE *'입니다.

참조된 LDAP 서버에 있는 레코드를 검색하려면 LDAP 클라이언트 구성의 일부로 참조된 레코드의 기본 dn을 기본 dn에 추가해야 합니다.

2. 스토리지 VM에서 LDAP 클라이언트 구성을 생성합니다.

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```



LDAP 클라이언트 구성을 생성할 때 스토리지 VM 이름을 제공해야 합니다.

3. LDAP 클라이언트 구성이 성공적으로 생성되었는지 확인합니다.

```
'vserver services name-service ldap client show-client-config client_config_name'
```

예

다음 명령을 실행하면 스토리지 VM VS1이 LDAP용 Active Directory 서버와 함께 작동하도록 ldap1이라는 새 LDAP 클라이언트 구성이 생성됩니다.

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

다음 명령을 실행하면 스토리지 VM VS1이 Active Directory 서버와 작동하여 서명과 봉인이 필요한 LDAP에 대해 ldap1이라는 새 LDAP 클라이언트 구성이 생성되고 LDAP 서버 검색이 지정된 도메인의 특정 사이트로 제한됩니다.

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

다음 명령을 실행하면 스토리지 VM VS1이 LDAP 조회 추적이 필요한 LDAP용 Active Directory 서버와 작동하도록 ldap1이라는 새 LDAP 클라이언트 구성이 생성됩니다.


```
cluster1::> vservice services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

다음 명령을 실행하면 기본 DN을 지정하여 스토리지 VM VS1에 대해 ldap1이라는 LDAP 클라이언트 구성이 수정됩니다.

```
cluster1::> vservice services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

다음 명령을 실행하면 조회 추적을 활성화하여 스토리지 VM VS1에 대해 ldap1이라는 LDAP 클라이언트 구성이 수정됩니다.

```
cluster1::> vservice services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com" -referral-enabled true
```

LDAP 클라이언트 구성을 SVM과 연결합니다

SVM에서 LDAP를 활성화하려면 "vservice services name-service ldap create" 명령을 사용하여 LDAP 클라이언트 구성을 SVM과 연결해야 합니다.

필요한 것

- LDAP 도메인은 네트워크 내에 이미 존재해야 하며 SVM이 있는 클러스터에서 액세스할 수 있어야 합니다.
- SVM에 LDAP 클라이언트 구성이 있어야 합니다.

단계

1. SVM에서 LDAP 지원:

'vservice services name-service LDAP create-vserver_vserver_name_-client-config_client_config_name_'



ONTAP 9.2부터 'vservice services name-service ldap create' 명령은 자동 구성 검증을 수행하고 ONTAP가 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

다음 명령을 실행하면 "VS1" SVM에서 LDAP를 활성화하고 "ldap1" LDAP 클라이언트 구성을 사용하도록 구성합니다.

```
cluster1::> vservice services name-service ldap create -vserver vs1
-client-config ldap1 -client-enabled true
```

2. `vserver services name-service ldap check` 명령을 사용하여 이름 서버의 상태를 확인합니다.

다음 명령은 SVM VS1 에서 LDAP 서버의 유효성을 검사합니다.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
| "10.11.12.13". |
```

이름 서비스 확인 명령은 ONTAP 9.2부터 사용할 수 있습니다.

이름 서비스 스위치 테이블에서 **LDAP** 소스를 확인합니다

SVM을 위한 네임 서비스 스위치 테이블에 네임 서비스에 대한 LDAP 소스가 올바르게 나열되어 있는지 확인해야 합니다.

단계

1. 현재 이름 서비스 스위치 테이블 내용을 표시합니다.

```
'vserver services name-service ns-switch show -vserver_svm_name_'
```

다음 명령을 실행하면 SVM My_SVM의 결과가 표시됩니다.

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM

Vserver      Database      Source
-----
My_SVM       hosts         files,
              dns
My_SVM       group         files,ldap
My_SVM       passwd        files,ldap
My_SVM       netgroup      files
My_SVM       namemap       files
5 entries were displayed.
```

이름 매핑 정보를 검색할 소스 및 순서를 지정합니다. UNIX 전용 환경에서는 이 항목이 필요하지 않습니다. 이름 매핑은 UNIX와 Windows를 모두 사용하는 혼합 환경에서만 필요합니다.

2. 필요에 따라 ns-switch 항목을 업데이트합니다.

| ns-switch 항목을 업데이트하려면... | 명령 입력... |
|--------------------------|---|
| 사용자 정보 | 'vserver services name-service ns-switch modify -vserver_vserver_name_-database passwd - sources ldap, files' |
| 그룹 정보 | 'vserver services name-service ns-switch modify -vserver_vserver_name_-database group-sources ldap, files' |
| 넷그룹 정보입니다 | 'vserver services name-service ns-switch modify -vserver_vserver_name_-database 넷그룹 - 소스 LDAP, 파일' |

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.