Administratorkonten verwalten

ONTAP 9

NetApp
November 16, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/authentication/manage-user-accounts-concept.html on November 16, 2026. Always check docs.netapp.com for the latest.

Inhalt

Administratorkonten verwalten . . . 1
- Informationen zu ONTAP Administratorkonten . . . 1
- Einem ONTAP Administratorkonto einen öffentlichen Schlüssel zuordnen . . . 1
- SSH Public Keys und X.509-Zertifikate für ONTAP Administratoren verwalten . . . 2
  - Einem Administratorkonto werden ein öffentlicher Schlüssel und ein X.509-Zertifikat zugeordnet. . . . 2
  - Die Zertifikatszuordnung vom öffentlichen SSH-Schlüssel für ein Administratorkonto entfernen . . . 3
  - Die Zuordnung des öffentlichen Schlüssels und des Zertifikats von einem Administratorkonto entfernen . . . 4
- Cisco Duo 2FA für ONTAP SSH-Anmeldungen konfigurieren . . . 4
  - Cisco Duo konfigurieren . . . 5
  - Cisco Duo Konfiguration ändern . . . 5
  - Cisco Duo Konfiguration entfernen . . . 6
  - Cisco Duo Konfiguration anzeigen . . . 6
  - Eine Duo Gruppe erstellen . . . 7
  - Duo Gruppen anzeigen . . . 7
  - Eine Duo Gruppe entfernen . . . 8
  - Duo Authentifizierung für Benutzer umgehen . . . 8
- Ein von einer Zertifizierungsstelle signiertes Serverzertifikat in ONTAP generieren und installieren . . . 9
  - Generieren einer Certificate Signing Request . . . 10
  - Ein von einer Zertifizierungsstelle signiertes Serverzertifikat installieren . . . 11
- ONTAP Zertifikate mit System Manager verwalten . . . 12
  - Zertifikatsinformationen anzeigen . . . 12
  - Benachrichtigungen zum Zertifikatsablauf ändern . . . 13
  - Generieren einer Certificate Signing Request . . . 14
  - Eine vertrauenswürdige Zertifizierungsstelle installieren (hinzufügen) . . . 14
  - Eine vertrauenswürdige Zertifizierungsstelle löschen . . . 15
  - Eine vertrauenswürdige Zertifizierungsstelle erneuern . . . 15
  - Ein Client-/Serverzertifikat installieren (hinzufügen) . . . 15
  - Ein selbstsigniertes Client-/Serverzertifikat generieren (hinzufügen) . . . 15
  - Löschen eines Client/Server-Zertifikats . . . 16
  - Ein Client-/Serverzertifikat erneuern . . . 16
  - Eine neue lokale Zertifizierungsstelle erstellen . . . 16
  - Ein Zertifikat mit einer lokalen Zertifizierungsstelle signieren . . . 17
  - Lokale Zertifizierungsstelle löschen . . . 17
  - Eine lokale Zertifizierungsstelle erneuern . . . 17
- Konfigurieren des Zugriffs auf Active Directory-Domänencontroller in ONTAP . . . 17
  - Einen Authentifizierungstunnel konfigurieren . . . 18
  - Ein SVM-Computerkonto in der Domäne erstellen . . . 19
- LDAP- oder NIS-Serverzugriff in ONTAP konfigurieren . . . 20
  - LDAP Serverzugriff konfigurieren . . . 20
  - NIS Serverzugriff konfigurieren . . . 22
  - Einen Namensdienstschalter erstellen . . . 22
- Ändern eines ONTAP Administratorpassworts . . . 23

Konfiguration von ONTAP Benachrichtigungen zum Ablauf von ONTAP Benutzerpasswörtern in System Manager . . . 24
Sperren und Entsperren eines ONTAP Administratorkontos . . . 25
Fehlgeschlagene Anmeldeversuche in ONTAP verwalten . . . 26
Woran Sie erkennen, dass Anmeldeversuche fehlgeschlagen sind . . . 26
Was zu tun ist, wenn wiederholte Anmeldeversuche fehlschlagen . . . 26
SHA-2 für Passwörter von ONTAP Administratorenkonten erzwingen . . . 26
Diagnose und Behebung von ONTAP Dateizugriffsproblemen mit System Manager . . . 27

Administratorkonten verwalten

Informationen zu ONTAP Administratorkonten

Je nachdem, wie Sie den Kontozugriff aktiviert haben, kann es erforderlich sein, einen öffentlichen Schlüssel mit einem lokalen Konto zu verknüpfen, ein von einer Zertifizierungsstelle signiertes Server-Digitalzertifikat zu installieren oder den Zugriff auf AD, LDAP oder NIS zu konfigurieren. Alle diese Aufgaben können vor oder nach der Aktivierung des Kontozugriffs ausgeführt werden.

Einem ONTAP Administratorkonto einen öffentlichen Schlüssel zuordnen

Für die SSH Public Key Authentifizierung muss der öffentliche Schlüssel einem Administratorkonto zugeordnet werden, bevor das Konto auf die SVM zugreifen kann. Mit dem `security login publickey create` Befehl kann ein Schlüssel einem Administratorkonto zugeordnet werden.

Über diese Aufgabe

Wenn ein Konto über SSH sowohl mit einem Passwort als auch mit einem öffentlichen SSH-Schlüssel authentifiziert wird, erfolgt die Authentifizierung des Kontos zuerst mit dem öffentlichen Schlüssel.

Bevor Sie beginnen

- Der SSH-Schlüssel muss generiert worden sein.
- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Einem Administratorkonto wird ein öffentlicher Schlüssel zugeordnet:

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-comment` *`comment`*

   Weitere Informationen zu `security login publickey create` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Änderung kann durch Anzeigen des öffentlichen Schlüssels überprüft werden:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

   Weitere Informationen zu `security login publickey show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiel

Der folgende Befehl verknüpft einen öffentlichen Schlüssel mit dem SVM-Administratorkonto `svmadmin1` für die SVM `engData1`. Dem öffentlichen Schlüssel wird die Indexnummer 5 zugewiesen.

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

SSH Public Keys und X.509-Zertifikate für ONTAP Administratoren verwalten

Für erhöhte Sicherheit bei der SSH-Authentifizierung mit Administratorkonten kann das `security login publickey` Befehlssatz verwendet werden, um den öffentlichen SSH-Schlüssel und dessen Zuordnung zu X.509-Zertifikaten zu verwalten.

Einem Administratorkonto werden ein öffentlicher Schlüssel und ein X.509-Zertifikat zugeordnet.

Ab ONTAP 9.13.1 kann ein X.509-Zertifikat mit dem öffentlichen Schlüssel verknüpft werden, der dem Administratorkonto zugeordnet ist. Dadurch ergibt sich zusätzliche Sicherheit, da bei der SSH-Anmeldung für dieses Konto eine Überprüfung auf Zertifikatsablauf oder -sperrung erfolgt.

Über diese Aufgabe

Wenn ein Konto über SSH sowohl mit einem öffentlichen SSH-Schlüssel als auch mit einem X.509-Zertifikat authentifiziert wird, prüft ONTAP die Gültigkeit des X.509-Zertifikats, bevor die Authentifizierung mit dem öffentlichen SSH-Schlüssel erfolgt. Die SSH-Anmeldung wird verweigert, wenn das Zertifikat abgelaufen oder widerrufen ist, und der öffentliche Schlüssel wird automatisch deaktiviert.

Bevor Sie beginnen

- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.
- Der SSH-Schlüssel muss generiert worden sein.
- Wenn lediglich das X.509-Zertifikat auf Ablauf überprüft werden soll, kann ein selbstsigniertes Zertifikat verwendet werden.
- Falls das X.509-Zertifikat auf Ablauf und Widerruf überprüft werden soll:
  - Sie müssen das Zertifikat von einer Zertifizierungsstelle (CA) erhalten haben.
  - Sie müssen die Zertifikatskette (Zwischen- und Stammzertifizierungsstellenzertifikate) mit `security certificate install` Befehlen installieren. Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".
  - Sie müssen OCSP für SSH aktivieren. Weitere Anweisungen sind unter "Die Gültigkeit digitaler Zertifikate wird mithilfe von OCSP überprüft." zu finden.

Schritte

1. Einem Administratorkonto werden ein öffentlicher Schlüssel und ein X.509-Zertifikat zugeordnet:

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-x509-certificate install`

   Weitere Informationen zu `security login publickey create` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Änderung kann durch Anzeigen des öffentlichen Schlüssels überprüft werden:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

   Weitere Informationen zu `security login publickey show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiel

Der folgende Befehl verknüpft einen öffentlichen Schlüssel und ein X.509-Zertifikat mit dem SVM-Administratorkonto `svmadmin2` für die SVM `engData2`. Dem öffentlichen Schlüssel wird die Indexnummer 6 zugewiesen.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

Die Zertifikatszuordnung vom öffentlichen SSH-Schlüssel für ein Administratorkonto entfernen

Sie können die aktuelle Zertifikatszuordnung vom öffentlichen SSH-Schlüssel des Kontos entfernen, während der öffentliche Schlüssel beibehalten wird.

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Die X.509-Zertifikatszuordnung von einem Administratorkonto entfernen und den vorhandenen SSH-öffentlichen Schlüssel beibehalten:

   `security login publickey modify -vserver SVM_name -username user_name -index index -x509-certificate delete`

   Weitere Informationen zu `security login publickey modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Änderung kann durch Anzeigen des öffentlichen Schlüssels überprüft werden:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Beispiel

Der folgende Befehl entfernt die X.509-Zertifikatszuordnung vom SVM-Administratorkonto `svmadmin2` für die SVM `engData2` mit der Indexnummer 6.

```
cluster1::> security login publickey modify -vserver engData2 -username
```

```
svmadmin2 -index 6 -x509-certificate delete
```

Die Zuordnung des öffentlichen Schlüssels und des Zertifikats von einem Administratorkonto entfernen

Sie können die aktuelle Konfiguration des öffentlichen Schlüssels und des Zertifikats aus einem Konto entfernen.

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Den öffentlichen Schlüssel und die Zuordnung eines X.509-Zertifikats von einem Administratorkonto entfernen:

   `security login publickey delete -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

   Weitere Informationen zu `security login publickey delete` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Änderung kann durch Anzeigen des öffentlichen Schlüssels überprüft werden:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Beispiel

Der folgende Befehl entfernt einen öffentlichen Schlüssel und ein X.509-Zertifikat vom SVM-Administratorkonto `svmadmin3` für die SVM `engData3` mit der Indexnummer 7.

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

Verwandte Informationen

- "security login publickey"

Cisco Duo 2FA für ONTAP SSH-Anmeldungen konfigurieren

Ab ONTAP 9.14.1 kann ONTAP so konfiguriert werden, dass Cisco Duo für die Zwei-Faktor-Authentifizierung (2FA) bei SSH-Anmeldungen verwendet wird. Duo wird auf Clusterebene konfiguriert und gilt standardmäßig für alle Benutzerkonten. Alternativ kann Duo auf Ebene der Storage VM (früher als vserver bezeichnet) konfiguriert werden, wobei es dann nur für Benutzer dieser Storage VM gilt. Wenn Duo aktiviert und konfiguriert ist, dient es als zusätzliches Authentifizierungsverfahren und ergänzt die bestehenden Methoden für alle Benutzer.

Wenn Sie die Duo Authentifizierung für SSH-Anmeldungen aktivieren, müssen Benutzer beim nächsten Anmelden per SSH ein Gerät registrieren. Informationen zur Registrierung enthält die Cisco Duo

"Einschreibungsdokumentation".

Mit der ONTAP-Befehlszeilenschnittstelle können die folgenden Aufgaben mit Cisco Duo durchgeführt werden:

- Cisco Duo konfigurieren
- Cisco Duo Konfiguration ändern
- Cisco Duo Konfiguration entfernen
- Cisco Duo Konfiguration anzeigen
- Eine Duo Gruppe entfernen
- Duo Gruppen anzeigen
- Duo Authentifizierung für Benutzer umgehen

Cisco Duo konfigurieren

Sie können eine Cisco Duo Konfiguration entweder für den gesamten Cluster oder für eine bestimmte Storage VM (in der ONTAP CLI als vserver bezeichnet) mit dem `security login duo create` Befehl erstellen. In diesem Fall ist Cisco Duo für SSH-Anmeldungen für diesen Cluster oder diese Storage VM aktiviert. Weitere Informationen zu `security login duo create` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Im Cisco Duo Admin Panel anmelden.
2. Zu **Anwendungen > UNIX Application** wechseln.
3. Notieren Sie Ihren Integrationsschlüssel, Ihren geheimen Schlüssel und Ihren API-Hostnamen.
4. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
5. Cisco Duo Authentifizierung für diese Storage-VM aktivieren, wobei die Informationen aus Ihrer Umgebung anstelle der Werte in Klammern einzusetzen sind:

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

Cisco Duo Konfiguration ändern

Sie können die Art und Weise ändern, wie Cisco Duo Benutzer authentifiziert (zum Beispiel wie viele Authentifizierungsaufforderungen gestellt werden oder welcher HTTP-Proxy verwendet wird). Wenn die Cisco Duo-Konfiguration für eine Storage-VM (in der ONTAP CLI als vserver bezeichnet) geändert werden muss, kann der `security login duo modify` Befehl verwendet werden. Weitere Informationen zu `security login duo modify` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Im Cisco Duo Admin Panel anmelden.
2. Zu **Anwendungen > UNIX Application** wechseln.
3. Notieren Sie Ihren Integrationsschlüssel, Ihren geheimen Schlüssel und Ihren API-Hostnamen.

4. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
5. Die Cisco Duo Konfiguration für diese Storage-VM kann angepasst werden, indem die Werte in Klammern durch die aktualisierten Informationen aus Ihrer Umgebung ersetzt werden:

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-max-prompts 1|2|3 \
-is-enabled true|false \
-fail-mode safe|secure
```

Cisco Duo Konfiguration entfernen

Sie können die Cisco Duo Konfiguration entfernen, wodurch die Notwendigkeit entfällt, dass sich SSH-Benutzer bei der Anmeldung mit Duo authentifizieren. Zum Entfernen der Cisco Duo Konfiguration für eine Storage VM (in der ONTAP CLI als vserver bezeichnet) kann der `security login duo delete` Befehl verwendet werden. Weitere Informationen zu `security login duo delete` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Entfernen Sie die Cisco Duo Konfiguration für diese Storage-VM, wobei Sie den Namen Ihrer Storage-VM für `<STORAGE_VM_NAME>` einsetzen:

```
security login duo delete  -vserver <STORAGE_VM_NAME>
```

Dadurch wird die Cisco Duo Konfiguration für diese Storage-VM dauerhaft gelöscht.

Cisco Duo Konfiguration anzeigen

Die bestehende Cisco Duo Konfiguration für eine Storage VM (in der ONTAP CLI als vserver bezeichnet) lässt sich mit dem `security login duo show` Befehl anzeigen. Weitere Informationen zu `security login duo show` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Die Cisco Duo Konfiguration für diese Storage-VM anzeigen. Optional kann der `vserver` Parameter verwendet werden, um eine Storage-VM anzugeben, wobei der Name der Storage-VM für `<STORAGE_VM_NAME>` eingesetzt wird:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

Sie sollten eine Ausgabe ähnlich der folgenden sehen:

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

Eine Duo Gruppe erstellen

Es ist möglich, Cisco Duo so zu konfigurieren, dass nur die Benutzer einer bestimmten Active Directory-, LDAP- oder lokalen Nutzergruppe in den Duo-Authentifizierungsprozess einbezogen werden. Wenn eine Duo-Gruppe erstellt wird, werden nur die Benutzer dieser Gruppe zur Duo-Authentifizierung aufgefordert. Eine Duo-Gruppe kann mit dem `security login duo group create` Befehl erstellt werden. Beim Erstellen einer Gruppe besteht optional die Möglichkeit, bestimmte Benutzer dieser Gruppe vom Duo-Authentifizierungsprozess auszuschließen. Weitere Informationen zu `security login duo group create` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Die Duo-Gruppe wird erstellt, wobei die Informationen aus Ihrer Umgebung anstelle der Werte in Klammern eingesetzt werden. Wenn der `-vserver` Parameter weggelassen wird, erfolgt die Erstellung der Gruppe auf Clusterebene:

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

Der Name der Duo-Gruppe muss mit einer Active Directory-, LDAP- oder lokalen Gruppe übereinstimmen. Benutzer, die mit dem optionalen `-excluded-users` Parameter angegeben werden, sind nicht in den Duo-Authentifizierungsprozess einbezogen.

Duo Gruppen anzeigen

Vorhandene Cisco Duo Gruppeneinträge lassen sich mit dem `security login duo group show` Befehl

anzeigen. Weitere Informationen zu `security login duo group show` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Die Duo-Gruppeneinträge werden angezeigt, wobei die Werte in Klammern durch Informationen aus Ihrer Umgebung ersetzt werden. Wenn der `-vserver` Parameter weggelassen wird, erscheint die Gruppe auf Clusterebene:

   ```
   security login duo group show -vserver <STORAGE_VM_NAME> -group-name
   <GROUP_NAME> -excluded-users <USER1, USER2>
   ```

   Der Name der Duo-Gruppe muss mit einer Active Directory-, LDAP- oder lokalen Gruppe übereinstimmen. Benutzer, die mit dem optionalen `-excluded-users` Parameter angegeben werden, werden nicht angezeigt.

Eine Duo Gruppe entfernen

Ein Duo-Gruppeneintrag kann mit dem `security login duo group delete` Befehl entfernt werden. Wenn eine Gruppe entfernt wird, sind die Benutzer dieser Gruppe nicht mehr im Duo Authentifizierungsprozess enthalten. Weitere Informationen zu `security login duo group delete` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Der Duo-Gruppeneintrag wird entfernt, wobei die Werte in Klammern durch Informationen aus Ihrer Umgebung ersetzt werden. Wenn der `-vserver` Parameter weggelassen wird, erfolgt die Entfernung der Gruppe auf Clusterebene.

   ```
   security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
   <GROUP_NAME>
   ```

   Der Name der Duo-Gruppe muss mit einer Active Directory-, LDAP- oder lokalen Gruppe übereinstimmen.

Duo Authentifizierung für Benutzer umgehen

Es besteht die Möglichkeit, alle Benutzer oder bestimmte Benutzer vom Duo SSH-Authentifizierungsprozess auszuschließen.

Alle Duo Nutzer ausschließen

Die Cisco Duo SSH-Authentifizierung kann für alle Benutzer deaktiviert werden.

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Cisco Duo Authentifizierung für SSH-Benutzer deaktivieren, wobei der Vserver-Name durch `<STORAGE_VM_NAME>` ersetzt wird:

```
security login duo modify -vserver <STORAGE_VM_NAME> -is-enabled false
```

Diese Einstellung `-is-enabled false` deaktiviert die Duo Authentifizierung, entfernt die Duo-Konfiguration jedoch nicht aus dem SSH-Anmeldepfad. In manchen Umgebungen kann für SSH-Anmeldungen weiterhin ein interaktiver Authentifizierungsablauf erforderlich sein, was nicht-interaktive SSH-Anmeldungen verhindern kann. Zur Wiederherstellung des nicht-interaktiven SSH-Anmeldeverhaltens ist die Duo-Konfiguration vollständig mit `security login duo delete -vserver <STORAGE_VM_NAME>` zu entfernen.

Duo Gruppenbenutzer ausschließen

Bestimmte Benutzer, die Teil einer Duo-Gruppe sind, können vom Duo SSH-Authentifizierungsprozess ausgeschlossen werden.

Schritte

1. Melden Sie sich mit SSH bei Ihrem ONTAP Konto an.
2. Cisco Duo Authentifizierung für bestimmte Benutzer in einer Gruppe deaktivieren. Der Gruppenname und die Liste der auszuschließenden Benutzer sind anstelle der Werte in Klammern einzusetzen:

   ```
   security login duo group modify -group-name <GROUP_NAME> -excluded-users
   <USER1, USER2>
   ```

   Der Name der Duo-Gruppe muss mit einer Active Directory-, LDAP- oder lokalen Gruppe übereinstimmen. Benutzer, die mit dem `-excluded-users` Parameter angegeben werden, sind nicht in den Duo-Authentifizierungsprozess einbezogen.

   Weitere Informationen zu `security login duo group modify` finden sich in der "ONTAP-Befehlsreferenz".

Lokale Duo Nutzer ausschließen

Bestimmte lokale Nutzer können von der Nutzung der Duo Authentifizierung ausgeschlossen werden, indem das Cisco Duo Admin Panel verwendet wird. Anleitungen finden sich in der "Cisco Duo Dokumentation".

Ein von einer Zertifizierungsstelle signiertes Serverzertifikat in ONTAP generieren und installieren

Auf Produktionssystemen empfiehlt es sich, zur Authentifizierung des Clusters oder der SVM als SSL-Server ein von einer Zertifizierungsstelle signiertes digitales Zertifikat zu installieren. Sie können den `security certificate generate-csr`Befehl verwenden, um eine Zertifikatsignierungsanforderung (CSR) zu generieren, und den `security certificate install`Befehl, um das von der Zertifizierungsstelle erhaltene Zertifikat zu installieren. Weitere Informationen zu `security certificate generate-csr` und `security certificate install` finden Sie in der "ONTAP-

Befehlsreferenz".

Generieren einer Certificate Signing Request

Mit dem `security certificate generate-csr` Befehl lässt sich eine Zertifikatsignierungsanforderung (CSR) generieren. Nach der Bearbeitung Ihrer Anforderung sendet die Zertifizierungsstelle (CA) das signierte digitale Zertifikat.

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Eine CSR generieren:

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

Der folgende Befehl erstellt eine CSR mit einem 2048-Bit-Privatschlüssel, der von der `SHA256` Hash-Funktion generiert wird. Die CSR ist für die Verwendung durch die `Software` Gruppe in der `IT` Abteilung eines Unternehmens mit Sitz in Sunnyvale, California, USA bestimmt. Der benutzerdefinierte Common Name des Unternehmens lautet `server1.companyname.com`. Die E-Mail-Adresse des SVM Kontaktadministrators lautet `web@example.com`. Das System zeigt die CSR und den Privatschlüssel in der Ausgabe an.

▼ **Beispiel für das Erstellen eines CSR**

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

NOTE: Keep a copy of your certificate request and private key for
future reference.
```

2. Die Zertifikatsanforderung aus der CSR-Ausgabe kopieren und in elektronischer Form (z. B. per E-Mail) zur Signierung an eine vertrauenswürdige Drittzertifizierungsstelle senden.

   Die Zertifizierungsstelle muss das signierte Zertifikat im Base64-kodierten PEM- oder PKCS12-Format zurückgeben.

   Nach Bearbeitung Ihres Antrags sendet Ihnen die Zertifizierungsstelle das signierte digitale Zertifikat. Eine Kopie des privaten Schlüssels und des von der Zertifizierungsstelle signierten digitalen Zertifikats sollte aufbewahrt werden.

Ein von einer Zertifizierungsstelle signiertes Serverzertifikat installieren

Sie können den `security certificate install` Befehl verwenden, um ein von einer Zertifizierungsstelle (CA) signiertes Serverzertifikat auf einer SVM zu installieren. ONTAP fordert Sie zur Eingabe der Root- und Zwischenzertifikate der Zertifizierungsstelle (CA) auf, die die Zertifikatskette des Serverzertifikats bilden. Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Ein von einer Zertifizierungsstelle signiertes Serverzertifikat installieren:

```
security certificate install -vserver SVM_name -type certificate_type
```

   ONTAP fordert Sie zur Eingabe der Stamm- und Zwischenzertifikate der Zertifizierungsstelle auf, die die Zertifikatskette des Serverzertifikats bilden. Die Kette beginnt mit dem Zertifikat der Zertifizierungsstelle, die das Serverzertifikat ausgestellt hat, und kann bis zum Stammzertifikat der Zertifizierungsstelle reichen. Fehlende Zwischenzertifikate führen dazu, dass die Installation des Serverzertifikats fehlschlägt.

   Der folgende Befehl installiert das CA-signierte Serverzertifikat und die Zwischenzertifikate auf SVM `engData2`.

   ▼ Beispiel für die Installation eines CA-signierten Serverzertifikats und von Zwischenzertifikaten

```
cluster1::>security certificate install -vserver engData2 -type server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
```

```
Do you want to continue entering root and/or intermediate certificates
{y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate certificates
{y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate certificates
{y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

Verwandte Informationen

- "security certificate generate-csr"

ONTAP Zertifikate mit System Manager verwalten

Ab ONTAP 9.10.1 kann mit System Manager die Verwaltung von vertrauenswürdigen Zertifizierungsstellen, Client-/Server-Zertifikaten und lokalen (Onboard) Zertifizierungsstellen erfolgen.

Mit System Manager können Sie die von anderen Anwendungen empfangenen Zertifikate verwalten, sodass die Kommunikation dieser Anwendungen authentifiziert werden kann. Auch die eigenen Zertifikate, die Ihr System gegenüber anderen Anwendungen identifizieren, lassen sich verwalten.

Zertifikatsinformationen anzeigen

Mit System Manager lassen sich vertrauenswürdige Zertifizierungsstellen, Client-/Serverzertifikate und lokale Zertifizierungsstellen anzeigen, die auf dem Cluster gespeichert sind.

Schritte

1. Im System Manager **Cluster > Einstellungen** auswählen.
2. Scrollen Sie zum Bereich **Sicherheit**. Im Abschnitt **Zertifikate** werden folgende Details angezeigt:
    - Die Anzahl der gespeicherten vertrauenswürdigen Zertifizierungsstellen.

- Die Anzahl der gespeicherten Client-/Serverzertifikate.
- Die Anzahl der gespeicherten lokalen Zertifizierungsstellen.

3. Wählen Sie eine beliebige Zahl aus, um Details zu einer Zertifikatskategorie anzuzeigen, oder wählen Sie → aus, um die Seite **Zertifikate** zu öffnen, die Informationen zu allen Kategorien enthält. Die Liste zeigt die Informationen für den gesamten Cluster an. Um Informationen nur für eine bestimmte Storage-VM anzuzeigen, sind die folgenden Schritte erforderlich:
   a. Wählen Sie **Speicher > Speicher-VMs**.
   b. Die Storage-VM auswählen.
   c. Zur Registerkarte **Einstellungen** wechseln.
   d. Wählen Sie eine Nummer im Abschnitt **Zertifikat** aus.

Nächste Schritte

- Auf der Seite **Zertifikate** können Sie Generieren einer Certificate Signing Request.
- Die Zertifikatsinformationen sind in drei Registerkarten unterteilt, eine für jede Kategorie. Von jeder Registerkarte aus lassen sich die folgenden Aufgaben durchführen:

Auf dieser Registerkarte…	Sie können diese Verfahren durchführen…
Vertrauenswürdige Zertifizierungsstellen	• Eine vertrauenswürdige Zertifizierungsstelle installieren (hinzufügen) • Eine vertrauenswürdige Zertifizierungsstelle löschen • Eine vertrauenswürdige Zertifizierungsstelle erneuern
Client/Server-Zertifikate	• Ein Client-/Serverzertifikat installieren (hinzufügen) • [gen-cs-cert] • Löschen eines Client/Server-Zertifikats • Benachrichtigungen zum Zertifikatsablauf ändern (beginnend mit ONTAP 9.20.1) • Ein Client-/Serverzertifikat erneuern
Lokale Zertifizierungsstellen	• Eine neue lokale Zertifizierungsstelle erstellen • Ein Zertifikat mit einer lokalen Zertifizierungsstelle signieren • Lokale Zertifizierungsstelle löschen • Eine lokale Zertifizierungsstelle erneuern

Benachrichtigungen zum Zertifikatsablauf ändern

Ab ONTAP 9.20.1 zeigt System Manager 30 Tage vor Ablauf eines Zertifikats für einen Cluster oder eine Storage Virtual Machine (SVM) eine Dashboard-Systemstatuswarnung an. Die Warnung wird täglich aktualisiert, um die Anzahl der verbleibenden Tage bis zum Ablauf anzuzeigen.

Sie können den standardmäßigen Warnschwellenwert von 30 Tagen auf eine beliebige Anzahl von Tagen zwischen 0 und 90 ändern. Sie können die Benachrichtigung auch deaktivieren, sodass sie nicht angezeigt wird, oder Benachrichtigungen für bereits abgelaufene Zertifikate unterdrücken, während Sie weiterhin Benachrichtigungen für bevorstehende Abläufe erhalten.

Schritte

1. Im System Manager **Cluster > Einstellungen** auswählen.

2. Unter **Zertifikate** erfolgt die Auswahl von → und anschließend von **Zertifikateinstellungen**.
3. Aktualisierung des Schwellenwerts für die Ablaufwarnung sowie Deaktivierung oder Unterdrückung der Warnung:
   - Eine Aktualisierung des **Warnschwellenwerts** auf eine beliebige Anzahl von Tagen zwischen 0 und 90 ist möglich.
   - Mit **Ablaufwarnungen deaktivieren** lässt sich die Warnung deaktivieren.
   - Mit **Benachrichtigungen über abgelaufene Zertifikate unterdrücken** werden Benachrichtigungen für bereits abgelaufene Zertifikate ausgeblendet, während Benachrichtigungen für bevorstehende Ablaufdaten weiterhin empfangen werden.

Generieren einer Certificate Signing Request

Sie können mit System Manager auf jeder Registerkarte der Seite **Zertifikate** eine Zertifikatsignierungsanforderung (CSR) generieren. Ein privater Schlüssel und eine zugehörige CSR werden generiert, die von einer Zertifizierungsstelle signiert werden können, um ein öffentliches Zertifikat zu erstellen.

Schritte

1. Die Seite **Zertifikate** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. **+CSR generieren** auswählen.
3. Vervollständigen Sie die Angaben zum Betreffnamen:
   a. Einen **allgemeinen Namen** eingeben.
   b. Ein **Land** auswählen.
   c. Eine **Organisation** eingeben.
   d. Eine **Organisationseinheit** eingeben.
4. Wenn Sie die Standardeinstellungen überschreiben möchten, wählen Sie **Weitere Optionen** und geben zusätzliche Informationen an.

Eine vertrauenswürdige Zertifizierungsstelle installieren (hinzufügen)

Im System Manager lassen sich zusätzliche vertrauenswürdige Zertifizierungsstellen installieren.

Schritte

1. Die Registerkarte **Vertrauenswürdige Zertifizierungsstellen** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie + Add .
3. Im Fenster **Vertrauenswürdige Zertifizierungsstelle hinzufügen** sind die folgenden Schritte auszuführen:
   - Einen **Namen** eingeben.
   - Für den **Bereich** eine Storage-VM auswählen.
   - Einen **allgemeinen Namen** eingeben.
   - Einen **Typ** auswählen.
   - Geben Sie die **Zertifikatsdetails** ein oder importieren Sie diese.

Eine vertrauenswürdige Zertifizierungsstelle löschen

Mit System Manager kann eine vertrauenswürdige Zertifizierungsstelle gelöscht werden.

> Vorinstallierte vertrauenswürdige Zertifizierungsstellen mit ONTAP können nicht gelöscht werden.

Schritte

1. Die Registerkarte **Vertrauenswürdige Zertifizierungsstellen** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie den Namen der vertrauenswürdigen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ neben dem Namen und dann **Löschen** aus.

Eine vertrauenswürdige Zertifizierungsstelle erneuern

Mit System Manager ist es möglich, eine vertrauenswürdige Zertifizierungsstelle zu erneuern, deren Gültigkeit abgelaufen ist oder demnächst abläuft.

Schritte

1. Die Registerkarte **Vertrauenswürdige Zertifizierungsstellen** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie den Namen der vertrauenswürdigen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ neben dem Zertifikatsnamen dann **Erneuern**.

Ein Client-/Serverzertifikat installieren (hinzufügen)

Mit System Manager können zusätzliche Client-/Serverzertifikate installiert werden.

Schritte

1. Die Registerkarte **Client/Serverzertifikate** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie + Add.
3. Im Fenster **Client-/Serverzertifikat hinzufügen** sind die folgenden Schritte auszuführen:
   - Einen **Zertifikatsnamen** eingeben.
   - Für den **Bereich** eine Storage-VM auswählen.
   - Einen **allgemeinen Namen** eingeben.
   - Einen **Typ** auswählen.
   - Geben Sie die **Zertifikatsdetails** ein oder importieren Sie diese. Die Zertifikatsdetails können entweder direkt eingegeben oder aus einer Textdatei kopiert und eingefügt werden. Alternativ lässt sich der Text aus einer Zertifikatsdatei durch Klicken auf **Import** importieren.
   - Geben Sie den **privaten Schlüssel** ein. Sie können den privaten Schlüssel entweder direkt eingeben oder aus einer Textdatei kopieren und einfügen oder den Text aus einer privaten Schlüsseldatei importieren, indem Sie auf **Import** klicken.

Ein selbstsigniertes Client-/Serverzertifikat generieren (hinzufügen)

Mit System Manager lassen sich zusätzliche selbstsignierte Client/Server-Zertifikate generieren.

Schritte

1. Die Registerkarte **Client/Serverzertifikate** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. **+Selbstsigniertes Zertifikat generieren** auswählen.
3. Im Fenster **Selbstsigniertes Zertifikat generieren** Folgendes ausführen:
   - Einen **Zertifikatsnamen** eingeben.
   - Für den **Bereich** eine Storage-VM auswählen.
   - Einen **allgemeinen Namen** eingeben.
   - Einen **Typ** auswählen.
   - Eine **Hashfunktion** auswählen.
   - Wählen Sie eine **Schlüssellänge**.
   - Eine **Speicher-VM** auswählen.

Löschen eines Client/Server-Zertifikats

Mit System Manager können Sie Client-/Serverzertifikate löschen.

Schritte

1. Die Registerkarte **Client/Serverzertifikate** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie den Namen des Client/Server-Zertifikats aus.
3. Wählen Sie ⋮ neben dem Namen aus und klicken Sie auf **Löschen**.

Ein Client-/Serverzertifikat erneuern

Mit System Manager kann ein Client/Server-Zertifikat erneuert werden, das abgelaufen ist oder demnächst abläuft.

Schritte

1. Die Registerkarte **Client/Serverzertifikate** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie den Namen des Client/Server-Zertifikats aus.
3. Wählen Sie ⋮ neben dem Namen und klicken Sie auf **Erneuern**.

Eine neue lokale Zertifizierungsstelle erstellen

Mit System Manager kann eine neue lokale Zertifizierungsstelle erstellt werden.

Schritte

1. Den Tab **Lokale Zertifizierungsstellen** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Wählen Sie + Add .
3. Im Fenster **Lokale Zertifizierungsstelle hinzufügen** Folgendes ausführen:
   - Einen **Namen** eingeben.
   - Für den **Bereich** eine Storage-VM auswählen.
   - Einen **allgemeinen Namen** eingeben.
4. Wenn Sie die Standardeinstellungen überschreiben möchten, wählen Sie **Weitere Optionen** und geben

zusätzliche Informationen an.

Ein Zertifikat mit einer lokalen Zertifizierungsstelle signieren

Im System Manager kann eine lokale Zertifizierungsstelle verwendet werden, um ein Zertifikat zu signieren.

Schritte

1. Den Tab **Lokale Zertifizierungsstellen** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Den Namen der lokalen Zertifizierungsstelle auswählen.
3. Wählen Sie ⋮ neben dem Namen dann **Zertifikat signieren**.
4. Das Formular **Antrag auf Unterzeichnung eines Zertifikats** ausfüllen.
   - Sie können entweder den Inhalt der Zertifikatsignierung einfügen oder eine Zertifikatsignierungsanforderungsdatei durch Klicken auf **Import** importieren.
   - Geben Sie die Anzahl der Tage an, für die das Zertifikat gültig ist.

Lokale Zertifizierungsstelle löschen

Mit System Manager kann eine lokale Zertifizierungsstelle gelöscht werden.

Schritte

1. Die Registerkarte **Local Certificate Authority** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Den Namen der lokalen Zertifizierungsstelle auswählen.
3. Wählen Sie ⋮ neben dem Namen und dann **Löschen**.

Eine lokale Zertifizierungsstelle erneuern

Mit System Manager können Sie eine lokale Zertifizierungsstelle erneuern, deren Gültigkeit abgelaufen ist oder demnächst abläuft.

Schritte

1. Die Registerkarte **Local Certificate Authority** anzeigen. Siehe Zertifikatsinformationen anzeigen.
2. Den Namen der lokalen Zertifizierungsstelle auswählen.
3. Wählen Sie ⋮ neben dem Namen und klicken Sie auf **Erneuern**.

Konfigurieren des Zugriffs auf Active Directory-Domänencontroller in ONTAP

Sie müssen den Zugriff des AD-Domänencontrollers auf den Cluster oder die SVM konfigurieren, bevor ein AD-Konto auf die SVM zugreifen kann. Wenn bereits ein SMB-Server für eine Daten-SVM konfiguriert wurde, kann die SVM als Gateway oder Tunnel für den AD-Zugriff auf den Cluster verwendet werden. Wenn kein SMB-Server konfiguriert wurde, kann ein Computerkonto für die SVM in der AD-Domäne erstellt werden.

ONTAP unterstützt die folgenden Domänencontroller-Authentifizierungsdienste:

- Kerberos

- LDAP
- Netlogon
- Lokale Sicherheitsautorität (LSA)

ONTAP unterstützt die folgenden Sitzungsschlüssel-Algorithmen für sichere Netlogon Verbindungen:

Session key Algorithmus	Verfügbar ab…
HMAC-SHA256, basierend auf dem Advanced Encryption Standard (AES). Wenn auf Ihrem Cluster ONTAP 9.9.1 oder einer früheren Version ausgeführt wird und Ihr Domänencontroller AES für sichere Netlogon-Dienste erzwingt, schlägt die Verbindung fehl. In diesem Fall ist der Domänencontroller so zu konfigurieren, dass er stattdessen starke Schlüsselverbindungen mit ONTAP akzeptiert.	ONTAP 9.10.1
DES und HMAC-MD5 (wenn ein starker Schlüssel gesetzt ist)	Alle ONTAP 9 Versionen

Wenn AES-Sitzungsschlüssel während des Aufbaus eines sicheren Netlogon-Kanals verwendet werden sollen, ist zu überprüfen, ob AES auf Ihrer SVM aktiviert ist.

- Ab ONTAP 9.14.1 ist AES standardmäßig aktiviert, wenn eine SVM erstellt wird, und es ist nicht erforderlich, die Sicherheitseinstellungen der SVM zu ändern, um AES-Sitzungsschlüssel während der Herstellung eines sicheren Netlogon-Kanals zu verwenden.
- In ONTAP 9.10.1 bis 9.13.1 ist AES beim Erstellen einer SVM standardmäßig deaktiviert. AES muss mit dem folgenden Befehl aktiviert werden:

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

Beim Upgrade auf ONTAP 9.14.1 oder höher ändert sich die AES-Einstellung für bestehende SVMs, die mit älteren ONTAP-Versionen erstellt wurden, nicht automatisch. Der Wert dieser Einstellung muss weiterhin aktualisiert werden, um AES auf diesen SVMs zu aktivieren.

Einen Authentifizierungstunnel konfigurieren

Wenn Sie bereits einen SMB-Server für eine Daten-SVM konfiguriert haben, kann mit dem `security login domain-tunnel create` Befehl die SVM als Gateway (oder Tunnel) für den AD-Zugriff auf den Cluster konfiguriert werden.

Vor ONTAP 9.16.1 ist ein Authentifizierungstunnel erforderlich, um Cluster-Administratorkonten mit AD zu verwalten.

Bevor Sie beginnen

- Es muss ein SMB-Server für eine Daten-SVM konfiguriert sein.
- Ein AD-Domänenbenutzerkonto muss für den Zugriff auf die Admin-SVM des Clusters aktiviert sein.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Ab ONTAP 9.10.1 ist bei Verwendung eines SVM-Gateways (Domain-Tunnel) für den AD-Zugriff die Nutzung

von Kerberos für die Admin-Authentifizierung möglich, sofern NTLM in Ihrer AD-Domäne deaktiviert ist. In früheren Versionen wurde Kerberos bei der Admin-Authentifizierung für SVM-Gateways nicht unterstützt. Diese Funktionalität ist standardmäßig verfügbar, eine Konfiguration ist nicht erforderlich.

Zuerst wird immer die Kerberos-Authentifizierung versucht. Im Falle eines Fehlschlags wird anschließend die NTLM-Authentifizierung versucht.

Schritte

1. Eine SMB-fähige Daten-SVM als Authentifizierungstunnel für den Zugriff des AD-Domänencontrollers auf den Cluster konfigurieren:

```
security login domain-tunnel create -vserver <svm_name>
```

Weitere Informationen zu `security login domain-tunnel create` finden sich in der "ONTAP-Befehlsreferenz".

Die SVM muss ausgeführt werden, damit der Benutzer authentifiziert wird.

Der folgende Befehl konfiguriert die SMB-fähige Daten-SVM `engData` als Authentifizierungstunnel.

```
cluster1::>security login domain-tunnel create -vserver engData
```

Ein SVM-Computerkonto in der Domäne erstellen

Wenn für eine Daten-SVM kein SMB-Server konfiguriert wurde, kann mit dem `vserver active-directory create` Befehl ein Computerkonto für die SVM in der Domäne erstellt werden.

Über diese Aufgabe

Nach Eingabe des `vserver active-directory create` Befehls werden Sie aufgefordert, die Anmeldeinformationen für ein AD-Benutzerkonto mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit in der Domäne anzugeben. Das Kennwort des Kontos darf nicht leer sein.

Ab ONTAP 9.16.1 lässt sich dieses Verfahren zur Verwaltung von Cluster-Administratorkonten mit AD nutzen.

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Ein Computerkonto für eine SVM in der AD-Domäne erstellen:

```
vserver active-directory create -vserver <SVM_name> -account-name
<NetBIOS_account_name> -domain <domain> -ou <organizational_unit>
```

Ab ONTAP 9.16.1 akzeptiert der `-vserver` Parameter die Admin-SVM. Weitere Informationen zu `vserver active-directory create` finden sich in der "ONTAP-Befehlsreferenz".

Der folgende Befehl erstellt ein Computerkonto mit dem Namen `ADSERVER1` in der Domäne `example.com` für SVM `engData`. Nach Eingabe des Befehls erfolgt eine Aufforderung zur Eingabe der Anmeldeinformationen des AD-Benutzerkontos.

```
cluster1::>vserver active-directory create -vserver engData -account
-name ADSERVER1 -domain example.com

In order to create an Active Directory machine account, you must supply
the name and password of a Windows account with sufficient privileges to
add computers to the "CN=Computers" container within the "example.com"
domain.

Enter the user name: Administrator

Enter the password:
```

LDAP- oder NIS-Serverzugriff in ONTAP konfigurieren

Sie müssen den LDAP- oder NIS-Serverzugriff auf eine SVM konfigurieren, bevor LDAP- oder NIS-Konten auf die SVM zugreifen können. Die Switch-Funktion ermöglicht die Verwendung von LDAP oder NIS als alternative Namensdienstquellen.

LDAP Serverzugriff konfigurieren

Sie müssen den LDAP-Serverzugriff auf eine SVM konfigurieren, bevor LDAP-Konten auf die SVM zugreifen können. Mit dem `vserver services name-service ldap client create` Befehl lässt sich eine LDAP-Client-Konfiguration auf der SVM erstellen. Anschließend kann der `vserver services name-service ldap create` Befehl verwendet werden, um die LDAP-Client-Konfiguration mit der SVM zu verknüpfen.

Über diese Aufgabe

Die meisten LDAP-Server können die von ONTAP bereitgestellten Standardschemas verwenden:

- MS-AD-BIS (das bevorzugte Schema für die meisten Windows 2012 und späteren AD-Server)
- AD-IDMU (Windows 2008, Windows 2016 und spätere AD-Server)
- AD-SFU (Windows 2003 und ältere AD-Server)
- RFC-2307 (UNIX LDAP-Server)

Es empfiehlt sich, die Standardschemata zu verwenden, sofern keine anderen Anforderungen bestehen. Falls dies der Fall ist, kann ein eigenes Schema erstellt werden, indem ein Standardschema kopiert und die Kopie angepasst wird. Weitere Informationen:

- "NFS-Konfiguration"
- "NetApp Technischer Bericht 4835: Konfiguration von LDAP in ONTAP"

Bevor Sie beginnen

- Es muss eine "CA-signiertes digitales Serverzertifikat" auf der SVM installiert sein.

- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Erstellen einer LDAP-Client-Konfiguration auf einer SVM:

   ```
   vserver services name-service ldap client create -vserver <SVM_name> -client
   -config <client_configuration> -servers <LDAP_server_IPs> -schema <schema>
   -use-start-tls <true|false>
   ```

   > Start TLS wird nur für den Zugriff auf Daten-SVMs unterstützt. Für den Zugriff auf Admin-SVMs wird es nicht unterstützt.

   Weitere Informationen zu `vserver services name-service ldap client create` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl erstellt eine LDAP-Client-Konfiguration mit dem Namen `corp` auf SVM `engData`. Der Client stellt anonyme Bindungen zu den LDAP-Servern mit den IP-Adressen 172.160.0.100 und 172.16.0.101 her. Der Client verwendet das RFC-2307-Schema für LDAP-Abfragen. Die Kommunikation zwischen Client und Server wird mit Start TLS verschlüsselt.

   ```
   cluster1::> vserver services name-service ldap client create
   -vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
   -schema RFC-2307 -use-start-tls true
   ```

   > Das `-ldap-servers` Feld ersetzt das `-servers` Feld. Das `-ldap-servers` Feld kann verwendet werden, um entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server anzugeben.

2. Die LDAP-Client-Konfiguration mit der SVM verknüpfen: `vserver services name-service ldap create -vserver <SVM_name> -client-config <client_configuration> -client -enabled <true|false>`

   Weitere Informationen zu `vserver services name-service ldap create` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl verknüpft die LDAP-Client-Konfiguration `corp` mit der SVM `engData` und aktiviert den LDAP-Client auf der SVM.

   ```
   cluster1::>vserver services name-service ldap create -vserver engData
   -client-config corp -client-enabled true
   ```

   > Der `vserver services name-service ldap create` Befehl führt eine automatische Konfigurationsprüfung durch und gibt eine Fehlermeldung aus, wenn ONTAP den Nameserver nicht erreichen kann.

3. Der Status der Nameserver kann mit dem Befehl vserver services name-service ldap check validiert werden.

Der folgende Befehl validiert LDAP-Server auf der SVM vs0.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                    |
```

Mit dem `name service check` Befehl lässt sich der Status der Nameserver validieren.

NIS Serverzugriff konfigurieren

Sie müssen den NIS-Serverzugriff auf eine SVM konfigurieren, bevor NIS-Konten auf die SVM zugreifen können. Mit dem `vserver services name-service nis-domain create` Befehl lässt sich eine NIS-Domänenkonfiguration auf einer SVM erstellen.

Bevor Sie beginnen

- Alle konfigurierten Server müssen verfügbar und erreichbar sein, bevor die NIS-Domäne auf der SVM konfiguriert wird.
- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Erstellen einer NIS-Domänenkonfiguration auf einer SVM:

   ```
   vserver services name-service nis-domain create -vserver <SVM_name> -domain
   <client_configuration> -nis-servers <NIS_server_IPs>
   ```

   Weitere Informationen zu `vserver services name-service nis-domain create` finden sich in der "ONTAP-Befehlsreferenz".

   > Das `-nis-servers` Feld ersetzt das `-servers` Feld. Das `-nis-servers` Feld kann verwendet werden, um entweder einen Hostnamen oder eine IP-Adresse für den NIS-Server anzugeben.

   Der folgende Befehl erstellt eine NIS-Domänenkonfiguration auf SVM `engData`. Die NIS-Domäne `nisdomain` kommuniziert mit einem NIS-Server mit der IP-Adresse `192.0.2.180`.

   ```
   cluster1::>vserver services name-service nis-domain create
   -vserver engData -domain nisdomain -nis-servers 192.0.2.180
   ```

Einen Namensdienstschalter erstellen

Die Funktion zum Umschalten des Namensdienstes ermöglicht die Verwendung von LDAP oder NIS als alternative Namensdienstquellen. Mit dem `vserver services name-service ns-switch modify` Befehl kann die Reihenfolge der Namensdienstquellen festgelegt werden.

Bevor Sie beginnen

- Der Zugriff auf LDAP- und NIS-Server muss konfiguriert sein.
- Um diese Aufgabe auszuführen, ist die Rolle als Cluster-Administrator oder SVM-Administrator erforderlich.

Schritt

1. Die Suchreihenfolge für Namensdienstquellen angeben:

   ```
   vserver services name-service ns-switch modify -vserver <SVM_name> -database
   <name_service_switch_database> -sources <name_service_source_order>
   ```

   Weitere Informationen zu `vserver services name-service ns-switch modify` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl legt die Suchreihenfolge der Name-Service-Quellen LDAP und NIS für die `passwd` Datenbank auf SVM `engData` fest.

   ```
   cluster1::>vserver services name-service ns-switch
   modify -vserver engData -database passwd -source files ldap,nis
   ```

Ändern eines ONTAP Administratorpassworts

Sie sollten Ihr anfängliches ONTAP Administratorpasswort unmittelbar nach der ersten Anmeldung und anschließend regelmäßig ändern, um die Sicherheit Ihres Clusters zu gewährleisten.

Ab ONTAP 9.20.1 zeigt der System Manager, sofern Ihr Benutzerkonto für Benachrichtigungen zum Passwortablauf konfiguriert ist, 14 Tage vor Ablauf Ihres Passworts eine Warnmeldung an. Die Meldung wird bei jeder Anmeldung aktualisiert und zeigt die verbleibenden Tage an.

Über diese Aufgabe

Das neue Passwort muss folgende Regeln erfüllen:

- Es darf den Benutzernamen nicht enthalten
- Es muss mindestens acht Zeichen lang sein
- Es muss mindestens einen Buchstaben und eine Zahl enthalten
- Es kann nicht dasselbe sein wie die letzten sechs Passwörter

> Der `security login role config modify`Befehl kann verwendet werden, um die Passwortregeln für Konten zu ändern, die einer bestimmten Rolle zugeordnet sind.

Bevor Sie beginnen

- Sie müssen Cluster- oder SVM-Administrator sein, um Ihr eigenes Passwort zu ändern.
- Sie müssen Cluster-Administrator sein, um das Passwort eines anderen Administrators zu ändern.

Schritte

Das Ändern Ihres Passworts ist über System Manager oder die ONTAP Befehlszeilenschnittstelle (CLI)

möglich.

System Manager

1. Im System Manager **Cluster > Einstellungen** auswählen.
2. Unter **Benutzer und Rollen** können Sie **Benutzer** auswählen.
3. Es ist ⋮ neben dem Benutzerkonto auszuwählen, für das das Passwort geändert werden muss, und anschließend **Change password**.
4. Neues Passwort eingeben.
5. Zur Bestätigung wird das neue Passwort erneut eingegeben und anschließend **Speichern** ausgewählt.

CLI

Wenn Sie SVM-Administrator sind, können Sie den `security login password` Befehl verwenden, um Ihr eigenes Passwort zu ändern. Wenn Sie Cluster-Administrator sind, können Sie den `security login password` Befehl verwenden, um das Passwort eines beliebigen Administrators zu ändern.

1. Ändern eines Administratorpassworts: `security login password -vserver` *`svm_name`* `-username` *`user_name`*

   Der folgende Befehl ändert das Kennwort des Administrators `admin1` für die SVM `vs1.example.com`. Danach geben Sie das aktuelle Kennwort sowie das neue Kennwort zur Bestätigung zweimal ein.

   ```
   vs1.example.com::>security login password -vserver engData -username
   admin1
   Please enter your current password:
   Please enter a new password:
   Please enter it again:
   ```

Verwandte Informationen

- "security login role config modify"
- "security login password"

Konfiguration von ONTAP Benachrichtigungen zum Ablauf von ONTAP Benutzerpasswörtern in System Manager

Ab ONTAP 9.20.1 erhält der Benutzer, wenn die einem Benutzerkonto zugeordnete Rolle für Benachrichtigungen zum Passwortablauf konfiguriert ist, direkt nach der Anmeldung in System Manager eine Banner-Benachrichtigung oben auf der Seite, beginnend 14 Tage vor dem Ablauf des Passworts. Die Benachrichtigung wird bei jeder Anmeldung aktualisiert und zeigt die Anzahl der verbleibenden Tage bis zum Ablauf des Passworts an. Sie können Benachrichtigungen zum Passwortablauf beim Hinzufügen oder Bearbeiten einer Administratorrolle konfigurieren.

Schritte

1. **Cluster > Einstellungen** auswählen.
2. Neben **Benutzer und Rollen** → auswählen.
3. Die Benachrichtigungen zum Ablauf von Passwörtern werden beim Hinzufügen oder Bearbeiten einer Benutzerrolle konfiguriert.
   - Für die Konfiguration beim Hinzufügen einer Benutzerrolle ist unter **Rollen** + Add auszuwählen. Anschließend folgen die Eingabe eines Namens für die Rolle sowie die Auswahl der Gültigkeitsdauer des Passworts und einer Benachrichtigung zum Passwortablauf.
   - Bei der Bearbeitung einer Benutzerrolle erfolgt die Konfiguration unter **Rollen** durch Auswahl der Benutzerrolle. Anschließend erfolgt unter **Bearbeiten** die Auswahl des Gültigkeitszeitraums des Passworts.
   - Wählen Sie **Add**.

Ergebnis

Der Benutzer erhält im System Manager direkt nach der Anmeldung ein Banner mit einer Warnmeldung am oberen Seitenrand, beginnend mit der ausgewählten Anzahl von Tagen vor dem Ablauf des Passworts. Die Benachrichtigung wird bei jeder Anmeldung aktualisiert und zeigt die verbleibenden Tage bis zum Ablauf des Passworts an.

Sperren und Entsperren eines ONTAP Administratorkontos

Sie können den `security login lock`-Befehl verwenden, um ein Administratorkonto zu sperren, und den `security login unlock`-Befehl, um das Konto zu entsperren.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgaben ausführen zu können.

Schritte

1. Administratorkonto sperren:

   ```
   security login lock -vserver SVM_name -username user_name
   ```

   Der folgende Befehl sperrt das Administratorkonto `admin1` für die SVM `vs1.example.com`:

   ```
   cluster1::>security login lock -vserver engData -username admin1
   ```

   Weitere Informationen zu `security login lock` finden sich in der "ONTAP-Befehlsreferenz".

2. Entsperren eines Administratorkontos:

   ```
   security login unlock -vserver SVM_name -username user_name
   ```

   Der folgende Befehl entsperrt das Administratorkonto `admin1` für die SVM `vs1.example.com`:

   ```
   cluster1::>security login unlock -vserver engData -username admin1
   ```

Weitere Informationen zu `security login unlock` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Security Login"

Fehlgeschlagene Anmeldeversuche in ONTAP verwalten

Wiederholte fehlgeschlagene Anmeldeversuche können darauf hindeuten, dass ein Eindringling versucht, auf das Speichersystem zuzugreifen. Es stehen verschiedene Maßnahmen zur Verfügung, um sicherzustellen, dass kein unbefugter Zugriff erfolgt.

Woran Sie erkennen, dass Anmeldeversuche fehlgeschlagen sind

Das Ereignismanagementsystem (EMS) benachrichtigt Sie stündlich über fehlgeschlagene Anmeldeversuche. Ein Protokoll der fehlgeschlagenen Anmeldeversuche befindet sich in der `audit.log` Datei.

Was zu tun ist, wenn wiederholte Anmeldeversuche fehlschlagen

Kurzfristig können Sie eine Reihe von Maßnahmen ergreifen, um einen Einbruch zu verhindern:

- Es wird verlangt, dass Passwörter aus einer Mindestanzahl von Großbuchstaben, Kleinbuchstaben, Sonderzeichen und/oder Ziffern bestehen.
- Nach einem fehlgeschlagenen Anmeldeversuch eine Verzögerung anwenden
- Die Anzahl zulässiger fehlgeschlagener Anmeldeversuche ist begrenzt, und Benutzer werden nach der festgelegten Anzahl fehlgeschlagener Versuche gesperrt.
- Konten, die für eine bestimmte Anzahl von Tagen inaktiv sind, verlieren ihre Gültigkeit und werden gesperrt.

Sie können den `security login role config modify` Befehl verwenden, um diese Aufgaben auszuführen. Weitere Informationen zu `security login role config modify` finden sich in der "ONTAP-Befehlsreferenz".

Langfristig sind folgende zusätzliche Schritte möglich:

- Mit dem `security ssh modify` Befehl lässt sich die Anzahl fehlgeschlagener Anmeldeversuche für alle neu erstellten SVMs begrenzen. Weitere Informationen zu `security ssh modify` finden sich in der "ONTAP-Befehlsreferenz".
- Bestehende MD5-Algorithmus-Konten werden auf den sichereren SHA-512 Algorithmus migriert, indem von den Benutzern verlangt wird, ihre Passwörter zu ändern.

SHA-2 für Passwörter von ONTAP Administratorenkonten erzwingen

Administratorkonten, die vor ONTAP 9.0 erstellt wurden, verwenden nach dem Upgrade weiterhin MD5-Passwörter, bis die Passwörter manuell geändert werden. MD5 ist weniger sicher als SHA-2. Nach dem Upgrade empfiehlt es sich, die Benutzer von MD5-Konten darauf hinzuweisen, ihre Passwörter zu ändern, damit die standardmäßige SHA-512-Hashfunktion verwendet wird.

Über diese Aufgabe

Die Passwort-Hash-Funktion ermöglicht Folgendes:

- Benutzerkonten, die der angegebenen Hash-Funktion entsprechen, werden angezeigt.
- Konten, die eine bestimmte Hash-Funktion verwenden (z. B. MD5), laufen ab, wodurch die Benutzer gezwungen werden, bei ihrem nächsten Login ihr Passwort zu ändern.
- Konten, deren Passwörter die angegebene Hash-Funktion verwenden, werden gesperrt.
- Beim Zurücksetzen auf eine Version vor ONTAP 9 ist das eigene Passwort des Cluster-Administrators zurückzusetzen, damit es mit der von der früheren Version unterstützten Hash-Funktion (MD5) kompatibel ist.

ONTAP akzeptiert vorab gehashte SHA-2-Passwörter nur über das NetApp Manageability SDK (`security-login-create` und `security-login-modify-password`.

Schritte

1. Die MD5-Administratorkonten auf die SHA-512-Passwort-Hash-Funktion migrieren:
   a. Alle MD5-Administratorkonten ablaufen lassen: `security login expire-password -vserver * -username * -hash-function md5`

      Dadurch müssen MD5-Kontobenutzer ihr Passwort beim nächsten Login ändern.

   b. Benutzer von MD5-Konten sollten sich über eine Konsole oder eine SSH-Sitzung anmelden.

      Das System erkennt, dass die Konten abgelaufen sind, und fordert die Benutzer auf, ihre Passwörter zu ändern. SHA-512 wird standardmäßig für die geänderten Passwörter verwendet.

2. Für MD5-Konten, deren Benutzer sich nicht innerhalb eines bestimmten Zeitraums anmelden, um ihr Passwort zu ändern, wird die Kontomigration erzwungen:
   a. Konten sperren, die weiterhin die MD5-Hashfunktion verwenden (erweiterte Berechtigungsstufe): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

      Nach der von `-lock-after`angegebenen Anzahl von Tagen können Benutzer nicht mehr auf ihre MD5-Konten zugreifen.

   b. Die Konten werden entsperrt, wenn die Benutzer bereit sind, ihre Passwörter zu ändern: `security login unlock -vserver` *`svm_name`* `-username` *`user_name`*

   c. Benutzer melden sich über eine Konsole oder eine SSH-Sitzung bei ihren Konten an und ändern ihre Passwörter, wenn das System sie dazu auffordert.

Verwandte Informationen

- "security login expire-password"
- "security login unlock"

Diagnose und Behebung von ONTAP Dateizugriffsproblemen mit System Manager

Ab ONTAP 9.8 lassen sich Bedenken beim Dateizugriff nachverfolgen und anzeigen.

Schritte

1. Im System Manager unter **Storage > Storage-VMs** auswählen.
2. Die Storage-VM auswählen, auf der eine Ablaufverfolgung durchgeführt werden soll.
3. Klicken Sie auf **Mehr**.
4. **Dateizugriff nachverfolgen** auswählen.
5. Den Benutzernamen und die Client-IP-Adresse angeben, anschließend auf **Start Tracing** klicken.

   Die Ergebnisse der Ablaufverfolgung werden in einer Tabelle angezeigt. Die Spalte **Gründe** gibt den Grund an, warum auf eine Datei nicht zugegriffen werden konnte.
6. In der linken Spalte der Ergebnistabelle auf klicken, um die Dateizugriffsberechtigungen anzuzeigen.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.