Verwalten von Administratorkonten

ONTAP 9

NetApp
February 12, 2026

Inhalt

Verwalten von Administratorkonten

Erfahren Sie mehr über das Managen von ONTAP-Administratorkonten

Je nachdem, wie Sie den Kontozugriff aktiviert haben, müssen Sie möglicherweise einen öffentlichen Schlüssel mit einem lokalen Konto verknüpfen, ein digitales Zertifikat für einen CA-signierten Server installieren oder AD-, LDAP- oder NIS-Zugriff konfigurieren. Sie können alle diese Aufgaben vor oder nach der Aktivierung des Kontozugriffs ausführen.

Verknüpfen Sie einen öffentlichen Schlüssel mit einem ONTAP-Administratorkonto

Bei der SSH-Authentifizierung für den öffentlichen Schlüssel müssen Sie den öffentlichen Schlüssel einem Administratorkonto zuweisen, bevor das Konto auf die SVM zugreifen kann. Mit dem `security login publickey create` Befehl können Sie einen Schlüssel mit einem Administratorkonto verknüpfen.

Über diese Aufgabe

Wenn Sie ein Konto über SSH sowohl mit einem Passwort als auch mit einem öffentlichen SSH-Schlüssel authentifizieren, wird das Konto zunächst mit dem öffentlichen Schlüssel authentifiziert.

Bevor Sie beginnen

- Sie müssen den SSH-Schlüssel generiert haben.
- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

1. Einen öffentlichen Schlüssel einem Administratorkonto zuordnen:

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

   Erfahren Sie mehr über `security login publickey create` in der "ONTAP-Befehlsreferenz".

2. Überprüfen Sie die Änderung, indem Sie den öffentlichen Schlüssel anzeigen:

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

   Erfahren Sie mehr über `security login publickey show` in der "ONTAP-Befehlsreferenz".

Beispiel

Mit dem folgenden Befehl wird ein öffentlicher Schlüssel mit dem SVM-Administratorkonto `svmadmin1` für die SVM verknüpft `engData1`. Der öffentliche Schlüssel wird mit der Indexnummer 5 belegt.

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

Verwalten von öffentlichen SSH-Schlüsseln und X.509-Zertifikaten für ONTAP-Administratoren

Um die SSH-Authentifizierungssicherheit mit Administratorkonten zu erhöhen, können Sie `security login publickey` den öffentlichen SSH-Schlüssel und seine Zuordnung zu X.509-Zertifikaten mit dem Befehlssatz verwalten.

Verknüpfen Sie einen öffentlichen Schlüssel und ein X.509-Zertifikat mit einem Administratorkonto

Ab ONTAP 9.13.1 können Sie ein X.509-Zertifikat mit dem öffentlichen Schlüssel verknüpfen, den Sie mit dem Administratorkonto verknüpfen. Dadurch erhalten Sie die zusätzliche Sicherheit bei der Überprüfung des Zertifikatablaufs oder des Widerrufs bei der SSH-Anmeldung für dieses Konto.

Über diese Aufgabe

Wenn Sie ein Konto über SSH sowohl mit einem öffentlichen SSH-Schlüssel als auch mit einem X.509-Zertifikat authentifizieren, überprüft ONTAP die Gültigkeit des X.509-Zertifikats, bevor es sich mit dem öffentlichen SSH-Schlüssel authentifiziert. Die SSH-Anmeldung wird abgelehnt, wenn das Zertifikat abgelaufen ist oder widerrufen wurde, und der öffentliche Schlüssel wird automatisch deaktiviert.

Bevor Sie beginnen

- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- Sie müssen den SSH-Schlüssel generiert haben.
- Wenn Sie nur das X.509-Zertifikat auf Gültigkeit prüfen müssen, können Sie ein selbstsigniertes Zertifikat verwenden.
- Wenn Sie das X.509-Zertifikat auf Ablaufdatum und Widerruf prüfen müssen:
  - Sie müssen das Zertifikat von einer Zertifizierungsstelle erhalten haben.
  - Sie müssen die Zertifikatskette (Zwischen- und Stammzertifizierungsstellen) mithilfe von `security certificate install` Befehlen installieren. Erfahren Sie mehr über `security certificate install` in der "ONTAP-Befehlsreferenz".
  - Sie müssen OCSP für SSH aktivieren. Anweisungen hierzu finden Sie unter "Überprüfen Sie, ob digitale Zertifikate mit OCSP gültig sind" .

Schritte

1. Einen öffentlichen Schlüssel und ein X.509-Zertifikat einem Administratorkonto zuordnen:

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

   Erfahren Sie mehr über `security login publickey create` in der "ONTAP-Befehlsreferenz".

2. Überprüfen Sie die Änderung, indem Sie den öffentlichen Schlüssel anzeigen:

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

Erfahren Sie mehr über `security login publickey show` in der "ONTAP-Befehlsreferenz".

Beispiel

Mit dem folgenden Befehl werden ein öffentlicher Schlüssel und ein X.509-Zertifikat dem SVM-Administratorkonto `svmadmin2` für die SVM zugeordnet `engData2`. Der öffentliche Schlüssel wird mit der Indexnummer 6 belegt.

```
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>
```

Entfernen Sie die Zertifikatszuordnung aus dem öffentlichen SSH-Schlüssel für ein Administratorkonto

Sie können die aktuelle Zertifikatzuordnung aus dem öffentlichen SSH-Schlüssel des Kontos entfernen und dabei den öffentlichen Schlüssel beibehalten.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

1. Entfernen Sie die X.509-Zertifikatszuordnung aus einem Administratorkonto, und behalten Sie den vorhandenen öffentlichen SSH-Schlüssel bei:

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

   Erfahren Sie mehr über `security login publickey modify` in der "ONTAP-Befehlsreferenz".

2. Überprüfen Sie die Änderung, indem Sie den öffentlichen Schlüssel anzeigen:

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

Beispiel

Mit dem folgenden Befehl wird die X.509-Zertifikatzuordnung aus dem SVM-Administratorkonto `svmadmin2` für die SVM `engData2` unter Indexnummer 6 entfernt.

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

Entfernen Sie den öffentlichen Schlüssel und die Zertifikatzuordnung aus einem Administratorkonto

Sie können den aktuellen öffentlichen Schlüssel und die Zertifikatkonfiguration aus einem Konto entfernen.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

1. Entfernen Sie den öffentlichen Schlüssel und eine X.509-Zertifikatzuordnung aus einem Administratorkonto:

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

   Erfahren Sie mehr über `security login publickey delete` in der "ONTAP-Befehlsreferenz".

2. Überprüfen Sie die Änderung, indem Sie den öffentlichen Schlüssel anzeigen:

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

Beispiel

Mit dem folgenden Befehl werden ein öffentlicher Schlüssel und ein X.509-Zertifikat aus dem SVM `svmadmin3` `engData3`-Administratorkonto für die SVM unter Indexnummer 7 entfernt.

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

Verwandte Informationen

- "Sicherheits-Login-Publickey"

Konfigurieren Sie Cisco Duo 2FA für ONTAP-SSH-Anmeldungen

Ab ONTAP 9.14.1 können Sie ONTAP während der SSH-Anmeldung für die zwei-Faktor-Authentifizierung (2FA) konfigurieren. Sie konfigurieren Duo auf Cluster-Ebene und dies gilt standardmäßig für alle Benutzerkonten. Alternativ können Sie Duo auf der Ebene der Storage-VM (früher als vServer bezeichnet) konfigurieren. In diesem Fall gilt dies nur für Benutzer dieser Storage-VM. Wenn Sie Duo aktivieren und konfigurieren, dient es als zusätzliche Authentifizierungsmethode, die die bestehenden Methoden für alle Benutzer ergänzt.

Wenn Sie die Duo-Authentifizierung für SSH-Anmeldungen aktivieren, müssen Benutzer ein Gerät registrieren, wenn sie sich das nächste Mal über SSH anmelden. Informationen zur Anmeldung finden Sie im Cisco Duo "Dokumentation der Anmeldung".

Über die ONTAP-Befehlszeilenschnittstelle können Sie mit Cisco Duo die folgenden Aufgaben ausführen:

- Konfigurieren Sie Cisco Duo
- Ändern Sie die Cisco Duo-Konfiguration
- Entfernen Sie die Cisco Duo-Konfiguration
- Cisco Duo-Konfiguration anzeigen
- Entfernen Sie eine Duo-Gruppe
- Zeigen Sie Duo-Gruppen an
- Umgehen Sie die Duo-Authentifizierung für Benutzer

Konfigurieren Sie Cisco Duo

Sie können mit dem `security login duo create` Befehl eine Cisco Duo-Konfiguration für das gesamte Cluster oder für eine bestimmte Storage-VM (in der ONTAP-CLI als vServer bezeichnet) erstellen. Wenn Sie dies tun, ist Cisco Duo für SSH-Anmeldungen für dieses Cluster oder diese Storage-VM aktiviert. Erfahren Sie mehr über `security login duo create` in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich beim Cisco Duo-Administratorbereich an.
2. Gehen Sie zu **Anwendungen > UNIX-Anwendung**.
3. Notieren Sie den Integrationsschlüssel, den geheimen Schlüssel und den API-Hostnamen.
4. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
5. Aktivieren Sie die Cisco Duo-Authentifizierung für diese Storage-VM und ersetzen Sie die Informationen aus Ihrer Umgebung durch die Werte in Klammern:

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

Ändern Sie die Cisco Duo-Konfiguration

Sie können die Art und Weise ändern, wie Cisco Duo Benutzer authentifiziert (z. B. wie viele Authentifizierungsaufforderungen angegeben werden oder welcher HTTP-Proxy verwendet wird). Wenn Sie die Cisco Duo-Konfiguration für eine Speicher-VM ändern müssen (in der ONTAP-CLI als vserver bezeichnet), können Sie den `security login duo modify` Befehl verwenden. Erfahren Sie mehr über `security login duo modify` in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich beim Cisco Duo-Administratorbereich an.
2. Gehen Sie zu **Anwendungen > UNIX-Anwendung**.
3. Notieren Sie den Integrationsschlüssel, den geheimen Schlüssel und den API-Hostnamen.
4. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
5. Ändern Sie die Cisco Duo-Konfiguration für diese Speicher-VM, indem Sie aktualisierte Informationen aus Ihrer Umgebung durch die Werte in Klammern ersetzen:

```
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
```

Entfernen Sie die Cisco Duo-Konfiguration

Sie können die Cisco Duo-Konfiguration entfernen, sodass SSH-Benutzer sich bei der Anmeldung nicht mehr mit Duo authentifizieren müssen. Um die Cisco Duo-Konfiguration für eine Speicher-VM zu entfernen (in der ONTAP-CLI als vServer bezeichnet), können Sie den `security login duo delete` Befehl verwenden. Erfahren Sie mehr über `security login duo delete` in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Entfernen Sie die Cisco Duo-Konfiguration für diese Speicher-VM und ersetzen Sie Ihren Speicher-VM-Namen durch `<STORAGE_VM_NAME>`:

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

   Dadurch wird die Cisco Duo-Konfiguration für diese Speicher-VM endgültig gelöscht.

Cisco Duo-Konfiguration anzeigen

Sie können die bestehende Cisco Duo-Konfiguration für eine Storage-VM (in der ONTAP-CLI als vserver bezeichnet) mit dem `security login duo show` Befehl anzeigen. Erfahren Sie mehr über `security login duo show` in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Zeigen Sie die Cisco Duo-Konfiguration für diese Storage-VM. Optional können Sie mit dem `vserver` Parameter eine Storage-VM angeben und den Namen der Storage-VM ersetzen für `<STORAGE_VM_NAME>`:

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

   Sie sollten eine Ausgabe wie die folgende 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: -
```

Erstellen Sie eine Duo-Gruppe

Sie können Cisco Duo anweisen, nur die Benutzer in einem bestimmten Active Directory, LDAP oder einer lokalen Benutzergruppe in den Duo-Authentifizierungsprozess einzubeziehen. Wenn Sie eine Duo-Gruppe erstellen, werden nur die Benutzer dieser Gruppe zur Duo-Authentifizierung aufgefordert. Sie können eine Duo-Gruppe mit dem `security login duo group create` Befehl erstellen. Wenn Sie eine Gruppe erstellen, können Sie optional bestimmte Benutzer dieser Gruppe aus dem Duo-Authentifizierungsprozess ausschließen. Erfahren Sie mehr über `security login duo group create` in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Erstellen Sie die Duo-Gruppe, indem Sie Informationen aus Ihrer Umgebung durch die Werte in Klammern ersetzen. Wenn Sie den `-vserver` Parameter nicht angeben, wird die Gruppe auf Cluster-Ebene erstellt:

```
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 Sie mit dem optionalen `-excluded-users` Parameter angeben, werden nicht in den Duo-Authentifizierungsprozess einbezogen.

Zeigen Sie Duo-Gruppen an

Sie können vorhandene Cisco Duo-Gruppeneinträge mit dem `security login duo group show` Befehl anzeigen. Erfahren Sie mehr über `security login duo group show` in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Zeigen Sie die Gruppeneinträge der Duo-Gruppe an und ersetzen Sie die Informationen aus Ihrer

Umgebung durch die Werte in Klammern. Wenn Sie den `-vserver` Parameter nicht angeben, wird die Gruppe auf Cluster-Ebene angezeigt:

```
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 Sie mit dem optionalen `-excluded-users` Parameter angeben, werden nicht angezeigt.

Entfernen Sie eine Duo-Gruppe

Sie können einen Duo-Gruppeneintrag mit dem `security login duo group delete` Befehl entfernen. Wenn Sie eine Gruppe entfernen, werden die Benutzer dieser Gruppe nicht mehr in den Duo-Authentifizierungsprozess einbezogen. Erfahren Sie mehr über `security login duo group delete` in der "ONTAP-Befehlsreferenz".

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Entfernen Sie den Gruppeneintrag Duo, und ersetzen Sie die Informationen aus Ihrer Umgebung durch die Werte in Klammern. Wenn Sie den `-vserver` Parameter nicht angeben, wird die Gruppe auf Cluster-Ebene entfernt:

```
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.

Umgehen Sie die Duo-Authentifizierung für Benutzer

Sie können alle Benutzer oder bestimmte Benutzer von der Duo SSH-Authentifizierung ausschließen.

Alle Duo-Benutzer ausschließen

Sie können die Cisco Duo SSH-Authentifizierung für alle Benutzer deaktivieren.

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Deaktivieren Sie die Cisco Duo-Authentifizierung für SSH-Benutzer, indem Sie den vServer-Namen durch `<STORAGE_VM_NAME>` folgende ersetzen:

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

Benutzer der Duo-Gruppe ausschließen

Sie können bestimmte Benutzer, die Teil einer Duo-Gruppe sind, aus dem Duo SSH-Authentifizierungsprozess

ausschließen.

Schritte

1. Melden Sie sich über SSH bei Ihrem ONTAP-Konto an.
2. Deaktivieren Sie die Cisco Duo-Authentifizierung für bestimmte Benutzer in einer Gruppe. Ersetzen Sie den Gruppennamen und die Liste der auszuschließenden Benutzer durch die Werte in Klammern:

   ```
   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 Sie mit dem `-excluded-users` Parameter angeben, werden nicht in den Duo-Authentifizierungsprozess einbezogen.

   Erfahren Sie mehr über `security login duo group modify` in der "ONTAP-Befehlsreferenz".

Lokale Duo-Benutzer ausschließen

Sie können bestimmte lokale Benutzer von der Duo-Authentifizierung ausschließen, indem Sie das Cisco Duo-Administratorfenster verwenden. Anweisungen hierzu finden Sie im "Cisco Duo-Dokumentation".

Erstellen und installieren Sie ein CA-signiertes Serverzertifikat in ONTAP

Auf Produktionssystemen ist es eine Best Practice, ein von CA signiertes digitales Zertifikat zur Authentifizierung des Clusters oder der SVM als SSL-Server zu installieren. Sie können mit dem `security certificate generate-csr` Befehl eine Zertifikatsignierungsanforderung (CSR) generieren und mit dem `security certificate install` Befehl das Zertifikat installieren, das Sie von der Zertifizierungsstelle zurückerhalten. Erfahren Sie mehr über `security certificate generate-csr` und `security certificate install` in der "ONTAP-Befehlsreferenz".

Generieren Sie eine Anforderung zum Signieren eines Zertifikats

Mit dem `security certificate generate-csr` Befehl können Sie eine Zertifikatsignierungsanforderung (CSR) generieren. Nach Bearbeitung Ihrer Anfrage sendet Ihnen die Zertifizierungsstelle (CA) das signierte digitale Zertifikat.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

1. CSR erstellen:

```
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
```

Mit dem folgenden Befehl wird ein CSR mit einem 2048-Bit privaten Schlüssel erstellt, der durch die Hashing-Funktion erzeugt `SHA256` wird, um von der Gruppe in der `IT` Abteilung eines Unternehmens verwendet `Software` zu werden, dessen benutzerdefinierter gemeinsamer Name `server1.companyname.com` in Sunnyvale, Kalifornien, USA liegt. Die E-Mail-Adresse des SVM-Kontaktadministrators lautet `web@example.com`. Das System zeigt den CSR und den privaten Schlüssel in der Ausgabe an.

Beispiel für das Erstellen einer 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. Kopieren Sie die Zertifikatsanforderung aus der CSR-Ausgabe, und senden Sie sie in elektronischer Form (z. B. E-Mail) an eine vertrauenswürdige Drittanbieter-CA zum Signieren.

   Nach Bearbeitung Ihrer Anfrage sendet Ihnen die CA das signierte digitale Zertifikat. Sie sollten eine Kopie des privaten Schlüssels und des CA-signierten digitalen Zertifikats aufbewahren.

Installieren Sie ein CA-signiertes Serverzertifikat

Sie können mit dem `security certificate install` Befehl ein CA-signiertes Serverzertifikat auf einer SVM installieren. ONTAP fordert Sie auf, die Stammzertifikate und Zwischenzertifikate der Zertifizierungsstelle (CA) anzugeben, die die Zertifikatskette des Serverzertifikats bilden. Erfahren Sie mehr über `security certificate install` in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritt

1. Installieren eines CA-signierten Serverzertifikats:

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

> ONTAP fordert Sie zur Eingabe der CA-Stammzertifikate und der Zwischenzertifikate 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 zum Ausfall der Serverzertifikatinstallation.

Mit dem folgenden Befehl werden das CA-signierte Serverzertifikat und die Zwischenzertifikate auf SVM installiert `engData2`.

Beispiel für die Installation eines CA-signierten Server-Zertifikats für Zwischenzertifikate

```
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

- "Sicherheitszertifikat generieren-csr"

Managen Sie ONTAP Zertifikate mit System Manager

Ab ONTAP 9.10.1 können Sie mit System Manager vertrauenswürdige Zertifizierungsstellen, Client-/Serverzertifikate und lokale (Onboard-)Zertifizierungsstellen verwalten.

Mit System Manager können Sie die von anderen Anwendungen erhaltenen Zertifikate verwalten, sodass Sie die Kommunikation von diesen Anwendungen authentifizieren können. Sie können auch Ihre eigenen Zertifikate verwalten, die Ihr System für andere Anwendungen identifizieren.

Zeigen Sie Zertifikatinformationen an

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

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Blättern Sie zum Bereich **Sicherheit**. Im Abschnitt **Zertifikate** werden die folgenden Details angezeigt:
   - Die Anzahl der gespeicherten vertrauenswürdigen Zertifizierungsstellen.
   - Die Anzahl der gespeicherten Client/Server-Zertifikate.
   - Die Anzahl der gespeicherten lokalen Zertifikatbehörden.
3. Wählen Sie eine beliebige Nummer aus, um Details zu einer Zertifikatkategorie anzuzeigen, oder wählen Sie aus → , um die Seite **Zertifikate** zu öffnen, die Informationen zu allen Kategorien enthält. In der Liste werden die Informationen für den gesamten Cluster angezeigt. Wenn Sie Informationen nur für eine bestimmte Storage-VM anzeigen möchten, führen Sie die folgenden Schritte aus:
   a. Wählen Sie **Storage > Storage VMs**.
   b. Wählen Sie die Storage-VM aus.
   c. Wechseln Sie zur Registerkarte **Einstellungen**.
   d. Wählen Sie eine Zahl aus, die im Abschnitt **Zertifikat** angezeigt wird.

Nächste Schritte

- Auf der Seite **Zertifikate** können Sie Generieren Sie eine Anforderung zum Signieren eines Zertifikats.
- Die Zertifikatinformation ist in drei Registerkarten unterteilt, eine für jede Kategorie. Sie können auf jeder Registerkarte die folgenden Aufgaben ausführen:

Auf dieser Registerkarte…	Sie können folgende Verfahren durchführen…
• Vertrauenswürdige Zertifizierungsstellen*	• [install-trusted-cert] • Löschen einer vertrauenswürdigen Zertifizierungsstelle • Eine vertrauenswürdige Zertifizierungsstelle erneuern

Client/Server-Zertifikate	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
Lokale Zertifikatbehörden	• Erstellen Sie eine neue lokale Zertifizierungsstelle • Unterzeichnen Sie ein Zertifikat mithilfe einer lokalen Zertifizierungsstelle • Lokale Zertifizierungsstelle löschen • Erneuern Sie eine lokale Zertifizierungsstelle

Generieren Sie eine Anforderung zum Signieren eines Zertifikats

Sie können eine Zertifikatsignierungsanforderung (CSR) mit System Manager auf einer beliebigen Registerkarte der Seite **Certificates** generieren. Es werden ein privater Schlüssel und ein entsprechender CSR erzeugt, der mit einer Zertifizierungsstelle signiert werden kann, um ein öffentliches Zertifikat zu generieren.

Schritte

1. Öffnen Sie die Seite **Zertifikate**. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie **+CSR erstellen**.
3. Geben Sie die Informationen für den Betreff ein:
   a. Geben Sie einen **gemeinsamen Namen** ein.
   b. Wählen Sie ein **Land** aus.
   c. Geben Sie eine **Organisation** ein.
   d. Geben Sie eine **Organisationseinheit** ein.
4. Wenn Sie die Standardeinstellungen überschreiben möchten, wählen Sie **Weitere Optionen** und geben Sie zusätzliche Informationen ein.

Installieren Sie eine vertrauenswürdige Zertifizierungsstelle (Hinzufügen)

Sie können weitere vertrauenswürdige Zertifizierungsstellen in System Manager installieren.

Schritte

1. Öffnen Sie die Registerkarte * Trusted Certificate Authorities*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie + Add .
3. Führen Sie im Fenster * Vertrauenswürdige Zertifizierungsstelle hinzufügen* folgende Schritte aus:
   - Geben Sie einen **Namen** ein.
   - Wählen Sie für den **Scope** eine Storage-VM aus.
   - Geben Sie einen **gemeinsamen Namen** ein.
   - Wählen Sie einen **Typ** aus.
   - Geben Sie **Zertifikatdetails** ein oder importieren Sie sie.

Löschen einer vertrauenswürdigen Zertifizierungsstelle

Mit System Manager können Sie eine vertrauenswürdige Zertifizierungsstelle löschen.

> Sie können keine vertrauenswürdigen Zertifizierungsstellen löschen, die mit ONTAP vorinstalliert sind.

Schritte

1. Öffnen Sie die Registerkarte * Trusted Certificate Authorities*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen der vertrauenswürdigen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ neben dem Namen, und wählen Sie dann **Löschen**.

Eine vertrauenswürdige Zertifizierungsstelle erneuern

Mit System Manager können Sie eine vertrauenswürdige Zertifizierungsstelle erneuern, die abgelaufen ist oder bald abläuft.

Schritte

1. Öffnen Sie die Registerkarte * Trusted Certificate Authorities*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen der vertrauenswürdigen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ neben dem Zertifikatnamen und dann **Renew** aus.

Installieren Sie ein Client-/Serverzertifikat (hinzufügen)

Mit System Manager können Sie zusätzliche Client-/Server-Zertifikate installieren.

Schritte

1. Öffnen Sie die Registerkarte **Client/Server Certificates**. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie + Add .
3. Führen Sie im Fenster **Client/Server-Zertifikat hinzufügen** folgende Schritte aus:
   - Geben Sie einen **Zertifikatnamen** ein.
   - Wählen Sie für den **Scope** eine Storage-VM aus.
   - Geben Sie einen **gemeinsamen Namen** ein.
   - Wählen Sie einen **Typ** aus.
   - Geben Sie **Zertifikatdetails** ein oder importieren Sie sie. Sie können entweder aus einer Textdatei die Zertifikatdetails einschreiben oder kopieren und einfügen oder den Text aus einer Zertifikatdatei importieren, indem Sie auf **Import** klicken.
   - Geben Sie den **privaten Schlüssel** ein. Sie können entweder aus einer Textdatei den privaten Schlüssel einschreiben oder kopieren und einfügen oder den Text aus einer privaten Schlüsseldatei importieren, indem Sie auf **Import** klicken.

Erstellen (Hinzufügen) eines selbstsignierten Client/Server-Zertifikats

Mit System Manager können Sie zusätzliche selbstsignierte Client-/Server-Zertifikate generieren.

Schritte

1. Öffnen Sie die Registerkarte **Client/Server Certificates**. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie **+Selbstsigniertes Zertifikat erstellen**.
3. Führen Sie im Fenster **selbst signiertes Zertifikat generieren** folgende Schritte aus:
   - Geben Sie einen **Zertifikatnamen** ein.
   - Wählen Sie für den **Scope** eine Storage-VM aus.
   - Geben Sie einen **gemeinsamen Namen** ein.
   - Wählen Sie einen **Typ** aus.
   - Wählen Sie eine **Hash-Funktion** aus.
   - Wählen Sie eine * Tastengröße* aus.
   - Wählen Sie eine **Storage-VM** aus.

Löschen Sie ein Client-/Serverzertifikat

Mit System Manager können Sie Client-/Server-Zertifikate löschen.

Schritte

1. Öffnen Sie die Registerkarte **Client/Server Certificates**. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen des Client/Server-Zertifikats aus.
3. Wählen Sie neben dem Namen aus ⋮, und klicken Sie dann auf **Löschen**.

Erneuern eines Client-/Serverzertifikats

Mit System Manager können Sie ein Client-/Serverzertifikat verlängern, das abgelaufen ist oder kurz vor Ablauf steht.

Schritte

1. Öffnen Sie die Registerkarte **Client/Server Certificates**. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen des Client/Server-Zertifikats aus.
3. Wählen Sie ⋮ neben dem Namen, und klicken Sie dann auf **erneuern**.

Erstellen Sie eine neue lokale Zertifizierungsstelle

Mit System Manager können Sie eine neue lokale Zertifizierungsstelle erstellen.

Schritte

1. Öffnen Sie die Registerkarte * Lokale Zertifikatbehörden*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie 

.
3. Führen Sie im Fenster * Lokale Zertifizierungsstelle hinzufügen* folgende Schritte aus:
   - Geben Sie einen **Namen** ein.
   - Wählen Sie für den **Scope** eine Storage-VM aus.
   - Geben Sie einen **gemeinsamen Namen** ein.
4. Wenn Sie die Standardeinstellungen überschreiben möchten, wählen Sie **Weitere Optionen** und geben Sie zusätzliche Informationen ein.

Unterzeichnen Sie ein Zertifikat mithilfe einer lokalen Zertifizierungsstelle

In System Manager können Sie eine lokale Zertifizierungsstelle zum Signieren eines Zertifikats verwenden.

Schritte

1. Öffnen Sie die Registerkarte * Lokale Zertifikatbehörden*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen der lokalen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ neben dem Namen und dann **Zertifikat signieren**.
4. Füllen Sie das Formular **Signieren einer Zertifikatsignierungsanforderung** aus.
   - Sie können entweder den Inhalt der Zertifikatsignierung einfügen oder eine Zertifikatsignierungsanfragedatei importieren, indem Sie auf **Import** klicken.
   - Geben Sie die Anzahl der Tage an, für die das Zertifikat gültig sein soll.

Lokale Zertifizierungsstelle löschen

Mit System Manager können Sie eine lokale Zertifizierungsstelle löschen.

Schritte

1. Öffnen Sie die Registerkarte * Local Certificate Authority*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen der lokalen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ neben dem Namen und dann **Löschen**.

Erneuern Sie eine lokale Zertifizierungsstelle

Mit System Manager können Sie eine lokale Zertifizierungsstelle erneuern, die abgelaufen ist oder bald abläuft.

Schritte

1. Öffnen Sie die Registerkarte * Local Certificate Authority*. Siehe Zeigen Sie Zertifikatinformationen an.
2. Wählen Sie den Namen der lokalen Zertifizierungsstelle aus.
3. Wählen Sie ⋮ neben dem Namen, und klicken Sie dann auf **erneuern**.

Konfigurieren Sie den Zugriff auf den Active Directory-Domänencontroller in ONTAP

Sie müssen AD-Domänencontroller-Zugriff auf das Cluster oder SVM konfigurieren, bevor ein AD-Konto auf die SVM zugreifen kann. Falls Sie bereits einen SMB-Server für eine Daten-SVM konfiguriert haben, können Sie die SVM für einen AD-Zugriff auf das Cluster als Gateway oder „*Tunnel*“ konfigurieren. Wenn Sie keinen SMB-Server konfiguriert haben, können Sie ein Computerkonto für die SVM in der AD-Domäne erstellen.

ONTAP unterstützt die folgenden Authentifizierungsservices für Domänencontroller:

- Kerberos
- LDAP
- Netzanmeldung

- Lokale Sicherheitsbehörde (LSA)

ONTAP unterstützt die folgenden Sitzungsschlüsselalgorithmen für sichere Netlogon-Verbindungen:

Sitzungsschlüsselalgorithmus	Verfügbar ab…
HMAC-SHA256, basierend auf dem Advanced Encryption Standard (AES) Wenn Ihr Cluster ONTAP 9.9.1 oder früher ausführt und Ihr Domänencontroller AES für sichere Netlogon-Dienste erzwingt, schlägt die Verbindung fehl. In diesem Fall müssen Sie Ihren Domänencontroller neu konfigurieren, um stattdessen starke Schlüsselverbindungen mit ONTAP zu akzeptieren.	ONTAP 9.10.1
DES und HMAC-MD5 (bei festem Schlüssel)	Alle ONTAP 9 Versionen

Wenn Sie AES-Sitzungsschlüssel während der Einrichtung des sicheren Netlogon-Kanals verwenden möchten, müssen Sie überprüfen, ob AES auf Ihrer SVM aktiviert ist.

- Ab ONTAP 9.14.1 ist AES standardmäßig aktiviert, wenn Sie eine SVM erstellen, und Sie müssen die Sicherheitseinstellungen Ihrer SVM nicht ändern, um AES-Sitzungsschlüssel während der Einrichtung des sicheren Netlogon-Kanals zu verwenden.
- In ONTAP 9.10.1 bis 9.13.1 ist AES beim Erstellen einer SVM standardmäßig deaktiviert. Sie müssen AES mit dem folgenden Befehl aktivieren:

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

Beim Upgrade auf ONTAP 9.14.1 oder höher wird die AES-Einstellung für vorhandene SVMs, die mit älteren ONTAP Versionen erstellt wurden, nicht automatisch geändert. Sie müssen den Wert für diese Einstellung immer noch aktualisieren, um AES für diese SVMs zu aktivieren.

Konfigurieren Sie einen Authentifizierungstunnel

Falls Sie bereits einen SMB-Server für eine Daten-SVM `security login domain-tunnel create` konfiguriert haben, können Sie die SVM mit dem Befehl als Gateway bzw. *Tunnel* für AD-Zugriff auf das Cluster konfigurieren.

Vor ONTAP 9.16.1 müssen Sie einen Authentifizierungstunnel verwenden, um Clusteradministratorkonten mit AD zu managen.

Bevor Sie beginnen

- Sie müssen einen SMB-Server für eine Daten-SVM konfiguriert haben.
- Sie müssen ein AD-Domänenbenutzerkonto aktiviert haben, um auf die Admin-SVM für das Cluster zuzugreifen.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Wenn Sie seit ONTAP 9.10.1 über ein SVM-Gateway (Domain-Tunnel) für AD-Zugriff verfügen, können Sie Kerberos für die Admin-Authentifizierung verwenden, wenn Sie NTLM in Ihrer AD-Domäne deaktiviert haben. In früheren Versionen wurde Kerberos mit der Admin-Authentifizierung für SVM Gateways nicht unterstützt.

Diese Funktion ist standardmäßig verfügbar; keine Konfiguration erforderlich.

> Kerberos-Authentifizierung wird immer zuerst versucht. Bei einem Fehler wird dann versucht, die NTLM-Authentifizierung zu aktivieren.

Schritte

1. Konfigurieren Sie eine SMB-fähige Daten-SVM als Authentifizierungstunnel für AD-Domänencontroller-Zugriff auf das Cluster:

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

   Erfahren Sie mehr über `security login domain-tunnel create` in der "ONTAP-Befehlsreferenz".

   > Die SVM muss ausgeführt werden, damit der Benutzer authentifiziert werden kann.

   Mit dem folgenden Befehl wird die Daten-SVM mit SMB-Aktivierung als Authentifizierungstunnel konfiguriert `engData`.

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

Erstellen Sie ein SVM-Computerkonto in der Domäne

Wenn Sie keinen SMB-Server für eine Daten-SVM konfiguriert haben, können Sie mit dem `vserver active-directory create` Befehl ein Computerkonto für die SVM in der Domäne erstellen.

Über diese Aufgabe

Nachdem Sie den `vserver active-directory create` Befehl eingegeben haben, werden Sie aufgefordert, die Anmeldeinformationen für ein AD-Benutzerkonto mit ausreichender Privileges anzugeben, um der angegebenen Organisationseinheit in der Domäne Computer hinzuzufügen. Das Passwort des Kontos darf nicht leer sein.

Ab ONTAP 9.16.1 können Sie dieses Verfahren verwenden, um Clusteradministratorkonten mit AD zu verwalten.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

1. Erstellen eines Computerkontos für eine SVM in der AD-Domäne:

   ```
   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. Erfahren Sie mehr über `vserver active-directory create` in der "ONTAP-Befehlsreferenz".

Mit dem folgenden Befehl wird ein Computerkonto mit dem Namen in der Domäne `example.com` für SVM `engData` erstellt `ADSERVER1`. Sie werden nach Eingabe des Befehls zur Eingabe der Anmeldedaten für das AD-Benutzerkonto aufgefordert.

```
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:
```

Konfigurieren Sie den LDAP- oder NIS-Serverzugriff in ONTAP

Sie müssen den LDAP- oder NIS-Serverzugriff auf eine SVM konfigurieren, bevor LDAP- oder NIS-Konten auf die SVM zugreifen können. Mit der Switch-Funktion können Sie LDAP oder NIS als alternative Namensdienstquellen verwenden.

Konfigurieren Sie den LDAP-Serverzugriff

Sie müssen den LDAP-Serverzugriff auf eine SVM konfigurieren, bevor LDAP-Konten auf die SVM zugreifen können. Sie können den `vserver services name-service ldap client create` Befehl verwenden, um eine LDAP-Client-Konfiguration auf der SVM zu erstellen. Mit dem `vserver services name-service ldap create` Befehl können Sie die LDAP-Client-Konfiguration der SVM zuordnen.

Über diese Aufgabe

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

- MS-AD-bis (das bevorzugte Schema für die meisten Windows 2012- und späteren AD-Server)
- AD-IDMU (AD-Server Windows 2008, Windows 2016 und höher)
- AD-SFU (Windows 2003 und frühere AD-Server)
- RFC-2307 (UNIX LDAP-SERVER)

Es empfiehlt sich, die Standardschemata zu verwenden, es sei denn, es ist eine andere Voraussetzung zu tun. In diesem Fall können Sie ein eigenes Schema erstellen, indem Sie ein Standardschema kopieren und die Kopie ändern. Weitere Informationen finden Sie unter:

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

Bevor Sie beginnen

- Sie müssen eine "DIGITALES Zertifikat für DEN CA-signierten Server" auf der SVM installiert haben.
- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

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

   ```
   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 Data SVMs unterstützt. Der Zugriff auf Admin-SVMs wird nicht unterstützt.

   Erfahren Sie mehr über `vserver services name-service ldap client create` in der "ONTAP-Befehlsreferenz".

   Mit dem folgenden Befehl wird eine LDAP-Client-Konfiguration mit dem Namen auf SVM `engData` erstellt `corp`. Der Client bindet mit den IP-Adressen 172.160.0.100 und 172.16.0.101 anonymisiert an die LDAP-Server. Der Client verwendet das RFC-2307-Schema, um LDAP-Abfragen zu erstellen. Die Kommunikation zwischen Client und Server wird über 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
   ```

   > Der `-ldap-servers` Feld ersetzt das `-servers` Feld. Sie können das `-ldap-servers` , um entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server anzugeben.

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

   Erfahren Sie mehr über `vserver services name-service ldap create` in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl ordnet die LDAP-Client-Konfiguration `corp` der SVM `engData`zu 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` Der Befehl führt eine automatische Konfigurationsvalidierung durch und meldet eine Fehlermeldung, wenn ONTAP den Nameserver nicht kontaktieren kann.

3. Überprüfen Sie den Status der Namensserver mithilfe des LDAP-Prüfbefehls vserver Services Name-Service.

Mit dem folgenden Befehl werden die LDAP-Server auf der SVM vs0 validiert.

```
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".                                                    |
```

Sie können die `name service check` Befehl zum Überprüfen des Status der Nameserver.

Konfigurieren Sie den NIS-Serverzugriff

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

Bevor Sie beginnen

- Alle konfigurierten Server müssen verfügbar und zugänglich sein, bevor Sie die NIS-Domäne auf der SVM konfigurieren.
- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

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>`

   Erfahren Sie mehr über `vserver services name-service nis-domain create` in der "ONTAP-Befehlsreferenz".

   > Der `-nis-servers` Feld ersetzt das `-servers` Feld. Sie können das `-nis-servers` , um entweder einen Hostnamen oder eine IP-Adresse für den NIS-Server anzugeben.

   Mit dem folgenden Befehl wird eine NIS-Domänenkonfiguration auf SVM erstellt `engData`. Die NIS-Domain `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
```

Erstellen Sie einen Namensdienstschalter

Mit der Namensdienst-Switch-Funktion können Sie LDAP oder NIS als alternative Namensdienstquellen verwenden. Sie können den `vserver services name-service ns-switch modify` Befehl verwenden, um die Reihenfolge für Namensdienstquellen festzulegen.

Bevor Sie beginnen

- Sie müssen LDAP- und NIS-Serverzugriff konfiguriert haben.
- Um diese Aufgabe auszuführen, müssen Sie ein Cluster-Administrator oder SVM-Administrator sein.

Schritt

1. Geben Sie die Suchreihenfolge für Namensdienstquellen an:

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

   Erfahren Sie mehr über `vserver services name-service ns-switch modify` in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl gibt die Suchreihenfolge der LDAP- und NIS-Namensservice-Quellen für die `passwd` Datenbank auf SVM an `engData`.

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

Ändern Sie ein ONTAP-Administratorkennwort

Sie sollten Ihr Anfangspasswort sofort nach der ersten Anmeldung am System ändern. Als SVM-Administrator können Sie mit dem `security login password` Befehl Ihr eigenes Passwort ändern. Als Cluster-Administrator können Sie mit dem `security login password` Befehl das Administratorpasswort ändern.

Über diese Aufgabe

Das neue Passwort muss folgende Bedingungen erfüllen:

- Er darf den Benutzernamen nicht enthalten
- Sie muss mindestens acht Zeichen lang sein
- Sie muss mindestens einen Buchstaben und eine Ziffer enthalten
- Es darf nicht mit den letzten sechs Kennwörtern identisch sein

> Mit dem `security login role config modify` Befehl können Sie die Passwortregeln für Konten ändern, die einer bestimmten Rolle zugeordnet sind.

Bevor Sie beginnen

- Zum Ändern des eigenen Passworts müssen Sie ein Cluster- oder SVM-Administrator sein.
- Sie müssen ein Cluster-Administrator sein, um das Passwort eines anderen Administrators zu ändern.

Schritt

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

   Mit dem folgenden Befehl wird das Passwort des Administrators `admin1` für die SVM

geändert`vs1.example.com`. Sie werden aufgefordert, das aktuelle Passwort einzugeben, dann das neue Passwort einzugeben und erneut einzugeben.

```
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

- "Sicherheits-Login-Rollenkonfiguration ändern"
- "Sicherheits-Login-Passwort"

Sperren und Entsperren eines ONTAP-Administratorkontos

Mit dem `security login lock` Befehl können Sie ein Administratorkonto sperren und mit dem `security login unlock` Befehl das Konto entsperren.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgaben auszuführen.

Schritte

1. Administratorkonto sperren:

   `security login lock -vserver SVM_name -username user_name`

   Mit dem folgenden Befehl wird das Administratorkonto `admin1` für die SVM gesperrt`vs1.example.com`:

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

   Erfahren Sie mehr über `security login lock` in der "ONTAP-Befehlsreferenz".

2. Administratorkonto entsperren:

   `security login unlock -vserver SVM_name -username user_name`

   Mit dem folgenden Befehl wird das Administratorkonto `admin1` für die SVM entsperrt`vs1.example.com`:

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

   Erfahren Sie mehr über `security login unlock` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Sicherheitsanmeldung"

Fehlgeschlagene Anmeldeversuche in ONTAP verwalten

Wiederholt fehlgeschlagene Anmeldeversuche weisen manchmal darauf hin, dass ein Eindringling versucht, auf das Speichersystem zuzugreifen. Sie können eine Reihe von Maßnahmen ergreifen, um sicherzustellen, dass kein Einbruch stattfindet.

Wie Sie wissen, dass Anmeldeversuche fehlgeschlagen sind

Das Event Management System (EMS) informiert Sie jede Stunde über fehlgeschlagene Anmeldeversuche. In der `audit.log` Datei finden Sie einen Datensatz mit fehlgeschlagenen Anmeldeversuchen.

Was tun, wenn wiederholte Anmeldeversuche fehlschlagen

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

- Kennwörter müssen aus einer Mindestanzahl von Groß-/Kleinschreibung, Kleinbuchstaben, Sonderzeichen und/oder Ziffern bestehen
- Legen Sie nach einem fehlgeschlagenen Anmeldeversuch eine Verzögerung fest
- Begrenzen Sie die Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche und sperren Sie Benutzer nach der angegebenen Anzahl fehlgeschlagener Versuche
- Verfallen und sperren Sie Konten, die für eine bestimmte Anzahl von Tagen inaktiv sind

Sie können die `security login role config modify` folgenden Aufgaben mit dem Befehl ausführen. Erfahren Sie mehr über `security login role config modify` in der "ONTAP-Befehlsreferenz".

Langfristig können Sie die folgenden zusätzlichen Schritte einleiten:

- Verwenden Sie den `security ssh modify` Befehl, um die Anzahl der fehlgeschlagenen Anmeldeversuche für alle neu erstellten SVMs zu begrenzen. Erfahren Sie mehr über `security ssh modify` in der "ONTAP-Befehlsreferenz".
- Migrieren Sie vorhandene MD5-Algorithmus-Konten in den sichereren SHA-512-Algorithmus, indem Sie Benutzer dazu auffordern, ihre Passwörter zu ändern.

SHA-2 auf ONTAP-Administratorkontokennwörtern erzwingen

Vor ONTAP 9.0 erstellte Administratorkonten verwenden nach dem Upgrade weiterhin MD5-Passwörter, bis die Passwörter manuell geändert werden. MD5 ist weniger sicher als SHA-2. Daher sollten Sie nach dem Upgrade Benutzer von MD5-Konten auffordern, ihre Passwörter zu ändern, um die Standard-SHA-512-Hash-Funktion zu verwenden.

Über diese Aufgabe

Mit der Passwort-Hash-Funktion können Sie Folgendes tun:

- Zeigt Benutzerkonten an, die mit der angegebenen Hash-Funktion übereinstimmen.
- Verfallen von Konten, die eine angegebene Hash-Funktion verwenden (z. B. MD5), sodass die Benutzer ihre Passwörter bei der nächsten Anmeldung ändern müssen.

- Konten sperren, deren Passwörter die angegebene Hash-Funktion verwenden.
- Wenn Sie auf eine Version vor ONTAP 9 zurücksetzen, setzen Sie das Kennwort des Clusteradministrators zurück, damit es mit der Hash-Funktion (MD5) kompatibel ist, die von der früheren Version unterstützt wird.

ONTAP akzeptiert vorgehashte SHA-2-Passwörter nur unter Verwendung von NetApp Manageability SDK (`security-login-create` und `security-login-modify-password`).

Schritte

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

      Dadurch werden MD5-Kontobenutzer gezwungen, ihre Passwörter bei der nächsten Anmeldung zu ändern.

   b. Benutzer von MD5-Konten bitten, sich über eine Konsole oder SSH-Sitzung anzumelden.

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

2. Bei MD5-Konten, deren Benutzer sich nicht anmelden, um ihre Passwörter innerhalb eines bestimmten Zeitraums zu ändern, erzwingen Sie die Kontomigration:
   a. Sperren von Konten, die weiterhin die MD5-Hash-Funktion verwenden (erweiterte Berechtigungsebene): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

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

   b. Entsperren Sie die Konten, wenn die Benutzer bereit sind, ihre Passwörter zu ändern: `security login unlock -vserver` *`svm_name`* `-username` *`user_name`*
   c. Benutzer müssen sich über eine Konsole oder SSH-Sitzung bei ihren Konten anmelden und ihre Passwörter ändern, wenn das System sie dazu auffordert.

Verwandte Informationen

- "Sicherheits-Login-Passwortablauf"
- "Sicherheits-Login entsperren"

Diagnostizieren und korrigieren Sie Probleme mit dem ONTAP-Dateizugriff mit System Manager

Ab ONTAP 9.8 können Sie Probleme mit dem Dateizugriff nachverfolgen und anzeigen.

Schritte

1. Wählen Sie in System Manager **Storage > Storage VMs** aus.
2. Wählen Sie die Speicher-VM aus, auf der Sie eine Ablaufverfolgung durchführen möchten.
3. Klicken Sie Auf ⋮ **Mehr**.
4. Klicken Sie Auf **Trace File Access**.

5. Geben Sie den Benutzernamen und die IP-Adresse des Clients an, und klicken Sie dann auf **Tracing starten**.

   Die Trace-Ergebnisse werden in einer Tabelle angezeigt. Die Spalte **Gründe** gibt den Grund, warum auf eine Datei nicht zugegriffen werden konnte.

6. Klicken Sie in der linken Spalte der Ergebnistabelle auf , um die Zugriffsrechte für die Datei anzuzeigen.