Erstellen von Anmeldekonten

ONTAP 9

NetApp
February 12, 2026

Inhalt

Erstellen von Anmeldekonten

Erfahren Sie mehr über das Erstellen von ONTAP-Anmeldekonten

Sie können lokale oder Remote-Cluster und SVM-Administratorkonten aktivieren. Bei einem lokalen Konto handelt es sich um ein Konto, in dem die Kontoinformationen, der öffentliche Schlüssel oder das Sicherheitszertifikat im Speichersystem gespeichert sind. INFORMATIONEN zu ANZEIGENKONTOKONTEN werden auf einem Domänencontroller gespeichert. LDAP- und NIS-Konten befinden sich auf LDAP- und NIS-Servern.

Cluster- und SVM-Administratoren

Ein_Cluster-Administrator_ greift auf die Admin-SVM für das Cluster zu. `admin`Beim Einrichten des Clusters werden automatisch die Admin-SVM und ein Cluster-Administrator mit dem reservierten Namen erstellt.

Ein Cluster-Administrator mit der Standardrolle `admin` kann den gesamten Cluster und seine Ressourcen verwalten. Der Cluster-Administrator kann bei Bedarf weitere Cluster-Administratoren mit unterschiedlichen Rollen erstellen.

Ein *SVM-Administrator* greift auf eine Daten-SVM zu. Je nach Bedarf erstellt der Cluster-Administrator Daten-SVMs und SVM-Administratoren.

SVM-Administratoren wird die `vsadmin` Rolle standardmäßig zugewiesen. Der Cluster-Administrator kann je nach Bedarf SVM-Administratoren verschiedene Rollen zuweisen.

Namenskonventionen

Die folgenden allgemeinen Namen können nicht für Remote-Cluster- und SVM-Administratorkonten verwendet werden:

- „adm“
- „Bin“
- „cli“
- „Daemon“
- „ftp“
- „Spiele“
- „Anhalten“
- „lp“
- „E-Mail“
- „Mann“
- „Naroot“
- NetApp
- „news“

- „Niemand“
- „Operator“
- „Root“
- „Herunterfahren“
- „Sshd“
- „Synchronisieren“
- „Sys“
- „uucp“
- „Www“

Zusammengeführte Rollen

Wenn Sie mehrere Remote-Konten für denselben Benutzer aktivieren, wird dem Benutzer die Zuordnung aller für die Konten angegebenen Rollen zugewiesen. Das heißt, wenn ein LDAP- oder NIS-Konto die `vsadmin` Rolle zugewiesen `vsadmin-volume` `vsadmin` ist und dem AD-Gruppenkonto für denselben Benutzer die Rolle zugewiesen ist, meldet sich der AD-Benutzer mit den umfassenderen Funktionen an. Die Rollen sollen *fusioniert werden*.

Aktivieren Sie den Zugriff auf lokales Konto

Hier erfahren Sie, wie Sie den Zugriff auf ein lokales ONTAP-Konto aktivieren

Bei einem lokalen Konto handelt es sich um ein Konto, in dem die Kontoinformationen, der öffentliche Schlüssel oder das Sicherheitszertifikat im Speichersystem gespeichert sind. Mit dem `security login create` Befehl können Sie lokale Konten für den Zugriff auf einen Administrator oder eine Daten-SVM aktivieren.

Verwandte Informationen

- "Sicherheits-Login erstellen"

Aktivieren Sie den Zugriff auf das Kennwort des ONTAP-Kontos

Mit dem `security login create` Befehl können Sie Administratorkonten für den Zugriff auf einen Admin oder eine Daten-SVM mit einem Passwort aktivieren. Nachdem Sie den Befehl eingegeben haben, werden Sie zur Eingabe des Passworts aufgefordert.

Über diese Aufgabe

Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, können Sie `security login modify` die Rolle später mit dem Befehl hinzufügen.

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

Bevor Sie beginnen

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

Schritt

1. Ermöglichen Sie lokalen Administratorkonten den Zugriff auf eine SVM über ein Passwort:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   Mit dem folgenden Befehl `admin1 backup` kann das Cluster-Administratorkonto mit der vordefinierten Rolle mit`engCluster` einem Passwort auf die Admin-SVM zugreifen. Nachdem Sie den Befehl eingegeben haben, werden Sie zur Eingabe des Passworts aufgefordert.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

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

Aktivieren Sie den SSH-Zugriff auf den öffentlichen Schlüssel des ONTAP-Kontos

Sie können mit dem `security login create` Befehl Administratorkonten für den Zugriff auf einen Admin oder eine Daten-SVM mit einem öffentlichen SSH-Schlüssel aktivieren.

Über diese Aufgabe

- Sie müssen den öffentlichen Schlüssel dem Konto zuordnen, bevor das Konto auf die SVM zugreifen kann.

  Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto

  Sie können diese Aufgabe vor oder nach dem Aktivieren des Kontozugriffs ausführen.

- Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, können Sie `security login modify` die Rolle später mit dem Befehl hinzufügen.

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

Wenn Sie den FIPS-Modus auf dem Cluster aktivieren möchten, müssen vorhandene öffentliche SSH-Schlüsselkonten ohne die unterstützten Schlüsselalgorithmen mit einem unterstützten Schlüsseltyp neu konfiguriert werden. Die Konten sollten neu konfiguriert werden, bevor Sie FIPS aktivieren, sonst schlägt die Administratorauthentifizierung fehl.

Die folgende Tabelle gibt Algorithmen des Host-Schlüsseltyps an, die für ONTAP-SSH-Verbindungen unterstützt werden. Diese Schlüsseltypen gelten nicht für die Konfiguration der öffentlichen SSH-Authentifizierung.

Version von ONTAP	Im FIPS-Modus unterstützte Schlüsseltypen	Im nicht-FIPS-Modus unterstützte Schlüsseltypen
9.11.1 und höher	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 + rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa

9.10.1 und früher	ecdsa-sha2-nistp256 + ssh-ed25519	ecdsa-sha2-nistp256 + ssh-ed25519 + ssh-dss + ssh-rsa

Die Unterstützung für den Host Key Algorithmus ssh-ed25519 wird ab ONTAP 9.11.1 entfernt.

Weitere Informationen finden Sie unter "Konfiguration der Netzwerksicherheit mit FIPS".

Bevor Sie beginnen

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

Schritt

1. Lokale Administratorkonten können mithilfe eines öffentlichen SSH-Schlüssels auf eine SVM zugreifen:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name user_or_group_name -application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   Mit dem folgenden Befehl kann das SVM-Administratorkonto `svmadmin1` mit der vordefinierten `vsadmin-volume` Rolle`engData1` über einen öffentlichen SSH-Schlüssel auf die SVM zugreifen:

   ```
   cluster1::>security login create -vserver engData1 -user-or-group-name
   svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
   ```

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

Nachdem Sie fertig sind

Falls Sie dem Administratorkonto keinen öffentlichen Schlüssel zugeordnet haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto

Aktivieren Sie Multi-Faktor-Authentifizierungskonten (MFA)

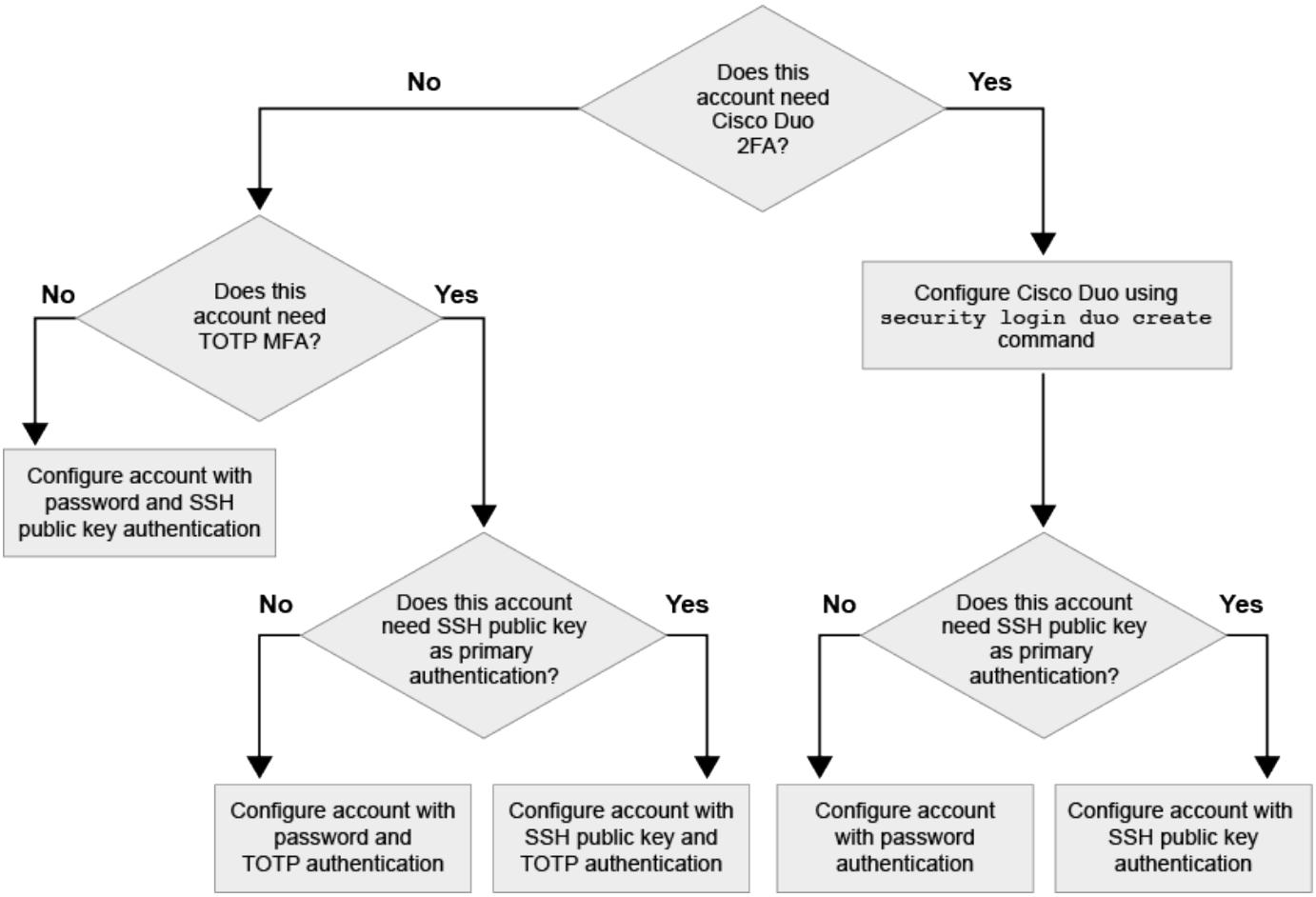
Informieren Sie sich über die ONTAP-Multi-Faktor-Authentifizierung

Dank der Multi-Faktor-Authentifizierung (MFA) können Sie die Sicherheit erhöhen, da Benutzer zur Anmeldung bei einem Administrator oder einer Storage-VM zwei Authentifizierungsmethoden bereitstellen müssen.

Je nach Ihrer Version von ONTAP können Sie eine Kombination aus einem öffentlichen SSH-Schlüssel, einem Benutzerpasswort und einem zeitbasierten Einmalpasswort (TOTP) zur mehrstufigen Authentifizierung verwenden. Wenn Sie Cisco Duo (ONTAP 9.14.1 und höher) aktivieren und konfigurieren, dient es als zusätzliche Authentifizierungsmethode, die die bestehenden Methoden für alle Benutzer ergänzt.

Verfügbar ab…	Erste Authentifizierungsmethode	Zweite Authentifizierungsmethode
ONTAP 9.14.1	Öffentlicher SSH-Schlüssel	TOTP
	Benutzerkennwort	TOTP
	Öffentlicher SSH-Schlüssel	Cisco Duo
	Benutzerpasswort	Cisco Duo
ONTAP 9.13.1	Öffentlicher SSH-Schlüssel	TOTP
	Benutzerpasswort	TOTP
ONTAP 9,3	Öffentlicher SSH-Schlüssel	Benutzerpasswort

Wenn MFA konfiguriert ist, muss der Clusteradministrator zuerst das lokale Benutzerkonto aktivieren, dann muss das Konto vom lokalen Benutzer konfiguriert werden.



Multifaktor-Authentifizierung mit ONTAP über SSH und TOTP

Dank der Multi-Faktor-Authentifizierung (MFA) können Sie die Sicherheit erhöhen, da Benutzer zur Anmeldung bei einem Administrator oder einer Daten-SVM zwei Authentifizierungsmethoden bereitstellen müssen.

Über diese Aufgabe

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, können Sie `security login modify` die Rolle später mit dem Befehl hinzufügen.

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

  "Ändern der Rolle, die einem Administrator zugewiesen ist"

- Wenn Sie einen öffentlichen Schlüssel für die Authentifizierung verwenden, müssen Sie den öffentlichen Schlüssel dem Konto zuordnen, bevor das Konto auf die SVM zugreifen kann.

  "Einem Benutzerkonto einen öffentlichen Schlüssel zuordnen"

  Sie können diese Aufgabe vor oder nach dem Aktivieren des Kontozugriffs ausführen.

- Ab ONTAP 9.12.1 können Sie Yubikey-Hardware-Authentifizierungsgeräte für SSH-Client MFA verwenden, indem Sie die Authentifizierungsstandards FIDO2 (Fast Identity Online) oder PIV (Personal Identity Verification) verwenden.

Aktivieren Sie MFA mit öffentlichem SSH-Schlüssel und Benutzerpasswort

Ab ONTAP 9.3 kann ein Cluster-Administrator lokale Benutzerkonten für die Anmeldung mit einem öffentlichen SSH-Schlüssel und einem Benutzerpasswort einrichten.

1. Aktivieren Sie MFA auf einem lokalen Benutzerkonto mit öffentlichem SSH-Schlüssel und Benutzerpasswort:

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_name> -application ssh -authentication-method <password|publickey>
   -role admin -second-authentication-method <password|publickey>
   ```

   ```
   `admin2` `admin```engData1``Mit dem folgenden Befehl muss sich das SVM-
   Administratorkonto mit der vordefinierten Rolle mit einem öffentlichen
   SSH-Schlüssel und einem Benutzerpasswort bei der SVM anmelden:
   ```

   ```
   cluster-1::> security login create -vserver engData1 -user-or-group-name
   admin2 -application ssh -authentication-method publickey -role admin
   -second-authentication-method password

   Please enter a password for user 'admin2':
   Please enter it again:
   Warning: To use public-key authentication, you must create a public key
   for user "admin2".
   ```

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

Aktivieren Sie MFA mit TOTP

Ab ONTAP 9.13.1 können Sie die Sicherheit erhöhen, indem Sie lokale Benutzer über einen öffentlichen SSH-Schlüssel oder ein Benutzerkennwort und ein zeitbasiertes Einmalpasswort (TOTP) bei einem Administrator oder einer Daten-SVM einloggen müssen. Nachdem das Konto für MFA mit TOTP aktiviert wurde, muss sich der lokale Benutzer bei anmelden"Schließen Sie die Konfiguration ab".

TOTP ist ein Computeralgorithmus, der die aktuelle Zeit verwendet, um ein Einmalpasswort zu generieren. Wenn TOTP verwendet wird, ist es immer die zweite Form der Authentifizierung nach dem öffentlichen SSH-Schlüssel oder dem Benutzerpasswort.

Bevor Sie beginnen

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

Schritte

Sie können MFA für mit einem Benutzerpasswort oder einem öffentlichen SSH-Schlüssel als erste Authentifizierungsmethode und TOTP als zweite Authentifizierungsmethode einrichten.

Aktivieren Sie MFA mit Benutzerpasswort und TOTP

1. Aktivieren Sie ein Benutzerkonto für Multi-Faktor-Authentifizierung mit einem Benutzerpasswort und einem TOTP.

   Für neue Benutzerkonten

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Für bestehende Benutzerkonten

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Vergewissern Sie sich, dass MFA mit TOTP aktiviert ist:

   ```
   security login show
   ```

Aktivieren Sie MFA mit öffentlichem SSH-Schlüssel und TOTP

1. Aktivieren Sie ein Benutzerkonto für Multi-Faktor-Authentifizierung mit einem öffentlichen SSH-Schlüssel und TOTP.

   Für neue Benutzerkonten

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Für bestehende Benutzerkonten

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

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

2. Vergewissern Sie sich, dass MFA mit TOTP aktiviert ist:

```
security login show
```

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

Nachdem Sie fertig sind

- Falls Sie dem Administratorkonto keinen öffentlichen Schlüssel zugeordnet haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

  "Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto"

- Der lokale Benutzer muss sich anmelden, um die MFA-Konfiguration mit TOTP abzuschließen.

  "Konfigurieren Sie das lokale Benutzerkonto für MFA mit TOTP"

Verwandte Informationen

- "Mehrstufige Authentifizierung in ONTAP 9 (TR-4647)"
- "ONTAP-Befehlsreferenz"

Konfigurieren Sie lokale ONTAP-Benutzerkonten für MFA mit TOTP

Ab ONTAP 9.13.1 können Benutzerkonten mit Multi-Faktor-Authentifizierung (MFA) unter Verwendung eines zeitbasierten Einmalpassworts (TOTP) konfiguriert werden.

Bevor Sie beginnen

- Der Storage-Administrator muss "Aktivieren Sie MFA mit TOTP" als zweite Authentifizierungsmethode für Ihr Benutzerkonto verwendet werden.
- Die primäre Authentifizierungsmethode für das Benutzerkonto sollte ein Benutzerpasswort oder ein öffentlicher SSH-Schlüssel sein.
- Sie müssen Ihre TOTP-App so konfigurieren, dass sie mit Ihrem Smartphone funktioniert und Ihren TOTP-Schlüssel erstellt.

  Microsoft Authenticator, Google Authenticator, Authy und jeder andere TOTP-kompatible Authenticator wird unterstützt.

Schritte

1. Melden Sie sich mit Ihrer aktuellen Authentifizierungsmethode bei Ihrem Benutzerkonto an.

   Die aktuelle Authentifizierungsmethode sollte ein Benutzerpasswort oder ein öffentlicher SSH-Schlüssel sein.

2. Erstellen Sie die TOTP-Konfiguration für Ihr Konto:

```
security login totp create -vserver "<svm_name>" -username
"<account_username >"
```

3. Überprüfen Sie, ob die TOTP-Konfiguration für Ihr Konto aktiviert ist:

```
security login totp show -vserver "<svm_name>" -username
"<account_username>"
```

Verwandte Informationen

- "Sicherheits-Login totp erstellen"
- "Sicherheits-Login-TOTP-Show"

Setzen Sie den geheimen TOTP-Schlüssel für ein ONTAP-Benutzerkonto zurück

Um die Sicherheit deines Kontos zu schützen, solltest du den TOTP-Schlüssel deaktivieren und einen neuen erstellen, wenn er kompromittiert oder verloren ist.

Setzen Sie TOTP zurück, wenn Ihr Schlüssel kompromittiert ist

Wenn Ihr TOTP-Schlüssel kompromittiert ist, Sie aber trotzdem Zugriff darauf haben, können Sie den kompromittierten Schlüssel entfernen und einen neuen erstellen.

1. Melden Sie sich mit Ihrem Benutzerkennwort oder dem öffentlichen SSH-Schlüssel und Ihrem kompromittierten TOTP-Schlüssel bei Ihrem Benutzerkonto an.
2. Entfernen Sie den kompromittierten TOTP-Schlüssel:

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. Neuen TOTP-Schlüssel erstellen:

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. Überprüfen Sie, ob die TOTP-Konfiguration für Ihr Konto aktiviert ist:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Setzen Sie TOTP zurück, wenn Ihr Schlüssel verloren geht

Wenn Ihr TOTP-Geheimschlüssel verloren geht, wenden Sie sich an Ihren Speicheradministrator"Lassen Sie den Schlüssel deaktiviert". Nachdem der Schlüssel deaktiviert wurde, können Sie sich mit Ihrer ersten Authentifizierungsmethode anmelden und ein neues TOTP konfigurieren.

Bevor Sie beginnen

Der TOTP-Schlüssel muss von einem Speicheradministrator deaktiviert werden. Wenn Sie kein Storage-

Administratorkonto haben, wenden Sie sich an Ihren Storage-Administrator, um den Schlüssel zu deaktivieren.

Schritte

1. Nachdem der TOTP-Schlüssel von einem Speicheradministrator deaktiviert wurde, melden Sie sich mit Ihrer primären Authentifizierungsmethode bei Ihrem lokalen Konto an.
2. Neuen TOTP-Schlüssel erstellen:

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. Überprüfen Sie, ob die TOTP-Konfiguration für Ihr Konto aktiviert ist:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Verwandte Informationen

- "Sicherheits-Login totp erstellen"
- "Sicherheits-Login-Topp löschen"
- "Sicherheits-Login-TOTP-Show"

Deaktivieren Sie den geheimen TOTP-Schlüssel für ein ONTAP-Benutzerkonto

Wenn der zeitbasierte TOTP-Schlüssel (One-Time Password) eines lokalen Benutzers verloren geht, muss der verlorene Schlüssel von einem Speicheradministrator deaktiviert werden, bevor der Benutzer einen neuen TOTP-Schlüssel erstellen kann.

Über diese Aufgabe

Diese Aufgabe kann nur über ein Cluster-Administratorkonto ausgeführt werden.

Schritt

1. Deaktivieren Sie den geheimen TOTP-Schlüssel:

```
security login totp modify -vserver <svm_name> -username
<account_username> -enabled false
```

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

Aktivieren Sie den Zugriff auf das ONTAP-Konto des SSL-Zertifikats

Mit dem `security login create` Befehl können Sie Administratorkonten für den Zugriff auf einen Admin oder eine Daten-SVM mit einem SSL-Zertifikat aktivieren.

Über diese Aufgabe

- Sie müssen ein digitales Zertifikat für einen CA-signierten Server installieren, bevor das Konto auf die SVM zugreifen kann.

  Erstellen und Installieren eines CA-signierten Serverzertifikats

  Sie können diese Aufgabe vor oder nach dem Aktivieren des Kontozugriffs ausführen.

- Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, können Sie die Rolle später mit dem `security login modify` Befehl hinzufügen.

  Ändern der Rolle, die einem Administrator zugewiesen ist

> Für Clusteradministratorkonten wird die Zertifikatauthentifizierung mit den `http` `ontapi` `rest` Anwendungen , und unterstützt. Bei SVM-Administratorkonten wird die Zertifikatauthentifizierung nur mit den `ontapi` und `rest`-Applikationen unterstützt.

Schritt

1. Aktivieren Sie lokale Administratorkonten für den Zugriff auf eine SVM mithilfe eines SSL-Zertifikats:

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   Mit dem folgenden Befehl `svmadmin2` `vsadmin` kann das SVM-Administratorkonto mit der Standardrolle`engData2` über ein digitales SSL-Zertifikat auf die SVM zugreifen.

   ```
   cluster1::>security login create -vserver engData2 -user-or-group-name
   svmadmin2 -application ontapi -authmethod cert
   ```

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

Nachdem Sie fertig sind

Wenn Sie kein digitales Zertifikat für einen CA-signierten Server installiert haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

Erstellen und Installieren eines CA-signierten Serverzertifikats

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Aktivieren Sie den Zugriff auf das Active Directory-ONTAP-Konto

Sie können mit dem `security login create` Befehl Active Directory (AD) Benutzer- oder Gruppenkonten für den Zugriff auf einen Administrator oder eine Daten-SVM aktivieren. Jeder Benutzer der AD-Gruppe kann mit der Rolle, die der Gruppe zugewiesen ist, auf die SVM zugreifen.

Über diese Aufgabe

- Sie müssen AD-Domänencontroller-Zugriff auf das Cluster oder SVM konfigurieren, bevor das Konto auf die SVM zugreifen kann.

  Active Directory-Domänencontroller-Zugriff wird konfiguriert

  Sie können diese Aufgabe vor oder nach dem Aktivieren des Kontozugriffs ausführen.

- Ab ONTAP 9.13.1 können Sie einen öffentlichen SSH-Schlüssel als primäre oder sekundäre Authentifizierungsmethode mit einem AD-Benutzerpasswort verwenden.

  Wenn Sie einen öffentlichen SSH-Schlüssel als primäre Authentifizierung verwenden, findet keine AD-Authentifizierung statt.

- Ab ONTAP 9.11.1 können Sie verwenden"Verwenden Sie LDAP Fast Bind für die NSswitch-Authentifizierung für ONTAP NFS SVMs", wenn es vom AD-LDAP-Server unterstützt wird.
- Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, können Sie `security login modify` die Rolle später mit dem Befehl hinzufügen.

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

  Ändern der Rolle, die einem Administrator zugewiesen ist

> DER Zugriff auf das Konto `SSH ontapi rest` für ANZEIGENGRUPPEN wird nur mit den Anwendungen , und unterstützt. AD-Gruppen werden mit der SSH-Authentifizierung für öffentliche Schlüssel, die häufig für Multi-Faktor-Authentifizierung verwendet wird, nicht unterstützt.

Bevor Sie beginnen

- Die Cluster-Zeit muss innerhalb von fünf Minuten nach der Zeit auf dem AD Domain Controller synchronisiert werden.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritt

1. Aktivieren Sie AD-Benutzer- oder Gruppenadministratorkonten für den Zugriff auf eine SVM:

   Für AD-Nutzer:

ONTAP-Version	Primäre Authentifizierung	Sekundäre Authentifizierung	Befehl
9.13.1 und höher	Öffentlicher Schlüssel	Keine	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

ONTAP-Version	Primäre Authentifizierung	Sekundäre Authentifizierung	Befehl

9.13.1 und höher	Domäne	Öffentlicher Schlüssel	**Für einen neuen Benutzer**
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			Für einen bestehenden Benutzer
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

9.0 und höher	Domäne	Keine	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

Für AD-Gruppen:

ONTAP-Version	Primäre Authentifizierung	Sekundäre Authentifizierung	Befehl
9.0 und höher	Domäne	Keine	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

Nachdem Sie fertig sind

Falls Sie keinen Zugriff von AD-Domänen-Controllern auf das Cluster oder SVM konfiguriert haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

Active Directory-Domänencontroller-Zugriff wird konfiguriert

Verwandte Informationen

- "Sicherheits-Login erstellen"

Aktivieren Sie den Zugriff auf das LDAP- oder NIS-ONTAP-Konto

Sie können den `security login create` Befehl verwenden, um LDAP- oder NIS-Benutzerkonten für den Zugriff auf einen Administrator oder eine Daten-SVM zu aktivieren. Wenn Sie keinen LDAP- oder NIS-Serverzugriff auf die SVM konfiguriert haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

Über diese Aufgabe

- Gruppenkonten werden nicht unterstützt.
- Sie müssen LDAP- oder NIS-Serverzugriff auf die SVM konfigurieren, bevor das Konto auf die SVM zugreifen kann.

  Konfigurieren des LDAP- oder NIS-Serverzugriffs

  Sie können diese Aufgabe vor oder nach dem Aktivieren des Kontozugriffs ausführen.

- Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, können Sie `security login modify` die Rolle später mit dem Befehl hinzufügen.

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

  Ändern der Rolle, die einem Administrator zugewiesen ist

- Ab ONTAP 9.4 wird Multi-Faktor-Authentifizierung (MFA) für Remote-Benutzer über LDAP- oder NIS-Server unterstützt.
- Ab ONTAP 9.11.1 können Sie verwenden"Verwenden Sie LDAP Fast Bind für die NSswitch-Authentifizierung für ONTAP NFS SVMs", wenn es vom LDAP-Server unterstützt wird.
- Aufgrund eines bekannten LDAP-Problems sollten Sie das `':'` Zeichen (Doppelpunkt) nicht in einem Feld von LDAP-Benutzerkontoinformationen verwenden (z. B. `gecos` , `userPassword` usw.). Andernfalls schlägt die Suche für diesen Benutzer fehl.

Bevor Sie beginnen

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

Schritte

1. Aktivieren Sie LDAP- oder NIS-Benutzer- oder Gruppenkonten für den Zugriff auf eine SVM:

   ```
   security login create -vserver SVM_name -user-or-group-name user_name
   -application application -authmethod nsswitch -role role -comment comment -is
   -ns-switch-group yes|no [-is-ldap-fastbind true]
   ```

"Erstellen oder Ändern von Anmeldekonten"

Mit dem folgenden Befehl wird das LDAP- oder NIS-Clusteradministratorkonto `guest2` mit der vordefinierten `backup` Rolle aktiviert, um auf die Admin-SVM zuzugreifen`engCluster`.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
guest2 -application ssh -authmethod nsswitch -role backup
```

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

2. MFA-Anmeldung für LDAP- oder NIS-Benutzer aktivieren:

```
security login modify -user-or-group-name rem_usr1 -application ssh
-authentication-method nsswitch -role admin -is-ns-switch-group no -second
-authentication-method publickey
```

Die Authentifizierungsmethode kann als `publickey` und zweite Authentifizierungsmethode als angegeben werden `nsswitch`.

Im folgenden Beispiel wird die MFA-Authentifizierung aktiviert:

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

Nachdem Sie fertig sind

Wenn Sie keinen LDAP- oder NIS-Serverzugriff auf die SVM konfiguriert haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

Konfigurieren des LDAP- oder NIS-Serverzugriffs

Verwandte Informationen

- "Sicherheitsanmeldung"