



Erstellen von Anmeldekonten

ONTAP 9

NetApp
September 12, 2024

Inhalt

- Erstellen von Anmeldekontoen 1
 - Erstellen Sie die Übersicht über Login-Konten 1
 - Aktivieren Sie den Zugriff auf lokales Konto 2
 - Aktivieren Sie den Zugriff auf Active Directory-Konten 12
 - Aktivieren Sie den LDAP- oder NIS-Kontozugriff 15

Erstellen von Anmeldekonten

Erstellen Sie die Übersicht über Login-Konten

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. Der Administrator-SVM und ein Cluster-Administrator mit dem reservierten Namen `admin` Werden automatisch erstellt, wenn das Cluster eingerichtet ist.

Ein Clusteradministrator mit dem Standardwert `admin` Rolle 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.

Den werden SVM-Administratoren zugewiesen `vsadmin` Rolle standardmäßig. 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 einem LDAP- oder NIS-Konto das zugewiesen ist `vsadmin` Rolle und das AD-Gruppenkonto für denselben Benutzer wird der zugewiesen `vsadmin-volume` Rolle, der AD-Benutzer meldet sich mit dem Inklusiveren an `vsadmin` Sorgen. Die Rollen sollen *fusioniert werden*.

Aktivieren Sie den Zugriff auf lokales Konto

Lokalen Kontozugriff aktivieren – Übersicht

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

Aktivieren Sie den Zugriff auf das Passwort-Konto

Sie können das verwenden `security login create` Befehl zum Aktivieren von Administratorkonten für den Zugriff auf einen Administrator oder Daten-SVM mit einem Passwort Nachdem Sie den Befehl eingegeben haben, werden Sie zur Eingabe des Passworts aufgefordert.

Über diese Aufgabe

Wenn Sie sich nicht sicher sind, welche Rolle bei der Zugriffssteuerung Sie dem Login-Konto zuweisen möchten, können Sie das verwenden `security login modify` Befehl, um die Rolle später hinzuzufügen.

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

Eine vollständige Befehlssyntax finden Sie im ["Arbeitsblatt"](#).

Mit dem folgenden Befehl wird das Cluster-Administratorkonto aktiviert `admin1` Mit dem vordefinierten `backup` Rolle für den Zugriff auf die Administrator-SVMengCluster Mit einem Passwort. 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
```

Aktivieren Sie SSH-Konten für öffentliche Schlüssel

Sie können das verwenden `security login create` Befehl zum Aktivieren von Administratorkonten für den Zugriff auf eine Admin- oder Daten-SVM mit einem öffentlichen SSH-Schlüssel

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 Rolle bei der Zugriffssteuerung Sie dem Login-Konto zuweisen möchten, können Sie das verwenden `security login modify` Befehl, um die Rolle später hinzuzufügen.

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
```

Eine vollständige Befehlssyntax finden Sie im ["Arbeitsblatt"](#).

Mit dem folgenden Befehl wird das SVM-Administratorkonto aktiviert `svmadmin1` Mit dem vordefinierten `vsadmin-volume` Rolle für den Zugriff auf die `SVMengData1` Verwenden eines öffentlichen SSH-Schlüssels:

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

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)

Übersicht über Multi-Faktor-Authentifizierung

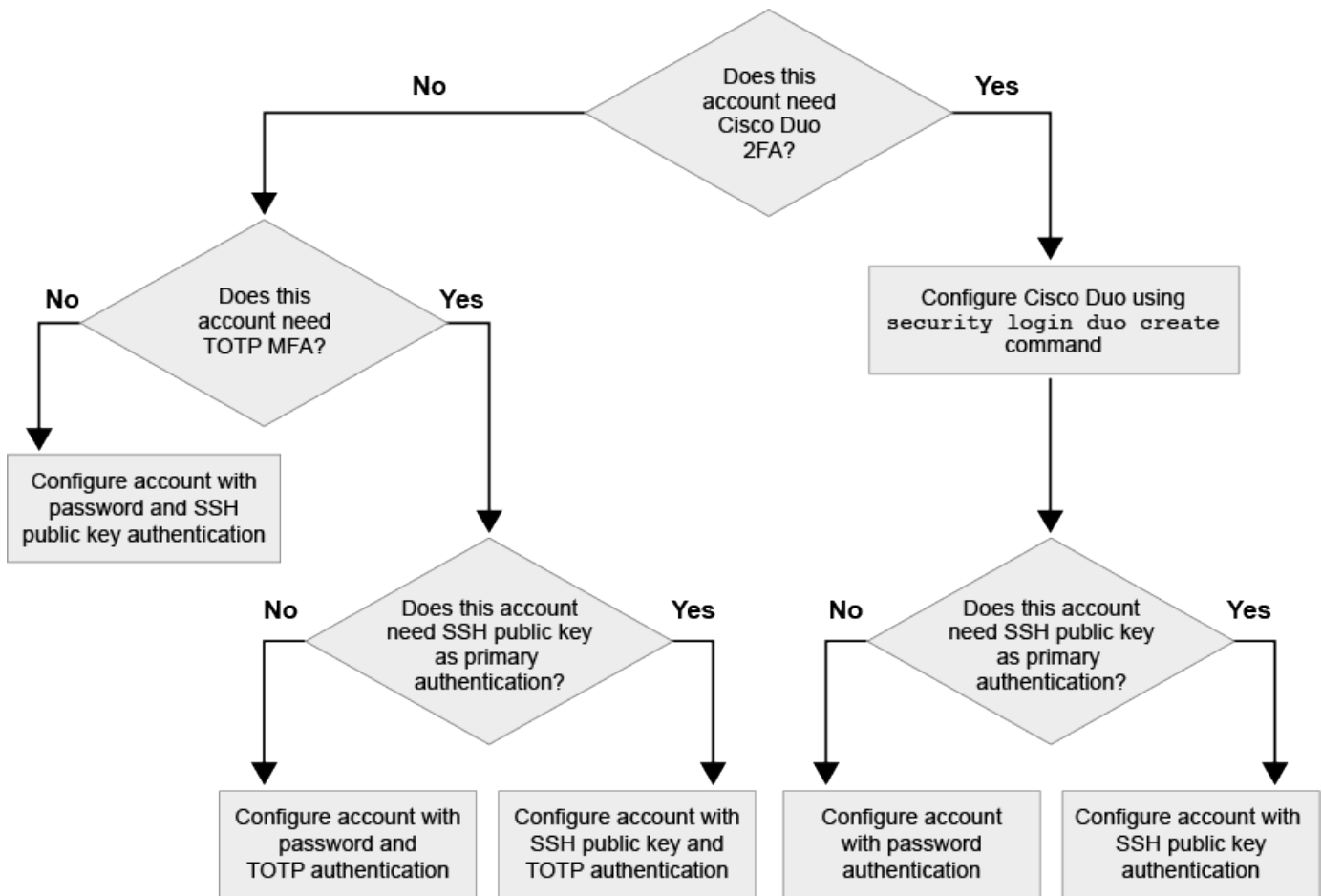
Dank der Multi-Faktor-Authentifizierung (MFA) können Sie die Sicherheit erhöhen, da Benutzer zur Anmeldung bei einem Administrator oder einer Storage-VM zwei Authentifizierungsmethoden bereitstellen müssen.

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

Verfügbar ab...	Erste Authentifizierungsmethode	Zweite Authentifizierungsmethode
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.



Aktivieren Sie Multi-Faktor-Authentifizierung

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 Rolle bei der Zugriffssteuerung Sie dem Login-Konto zuweisen möchten, können Sie das verwenden `security login modify` Befehl, um die Rolle später hinzuzufügen.

["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>
```

Der folgende Befehl erfordert das SVM-Administratorkonto `admin2` Mit dem vordefinierten `admin` Rolle zum Anmelden bei der SVM `engData1` Sowohl mit einem öffentlichen SSH-Schlüssel als auch mit einem Benutzerpasswort:

```
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".

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>
```

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

```
security login show
```

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

Weitere Informationen zu ["Mehrstufige Authentifizierung in ONTAP 9 \(TR-4647\)"](#).

Konfigurieren Sie das lokale Benutzerkonto 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.
- 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.

TOTP wird von verschiedenen Authentifikator-Apps wie Google Authenticator 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>"
```

TOTP-Schlüssel zurücksetzen

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>
```

Deaktivieren Sie den geheimen TOTP-Schlüssel für das lokale Konto

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 delete -vserver "<svm_name>" -username  
"<account_username>"
```

Aktivieren Sie SSL-Zertifikatkonten

Sie können das verwenden `security login create` Befehl zum Aktivieren von Administratorkonten für den Zugriff auf einen Administrator oder eine Daten-SVM mit einem SSL-Zertifikat

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 Rolle die Zugriffskontrolle Sie dem Login-Konto zuweisen möchten, können Sie die Rolle später mit dem hinzufügen `security login modify` Befehl.

[Ändern der Rolle, die einem Administrator zugewiesen ist](#)



Bei Clusteradministratorkonten wird die Zertifikatauthentifizierung mit unterstützt `http`, `ontapi`, und `rest` Applikationen unterstützt. Bei SVM-Administratorkonten wird die Zertifikatauthentifizierung nur von unterstützt `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
```

Vollständige Befehlssyntax finden Sie im ["ONTAP-man-Pages nach Release"](#).

Mit dem folgenden Befehl wird das SVM-Administratorkonto aktiviert `svmadmin2` Mit der Standardeinstellung `vsadmin` Rolle für den Zugriff auf die `SVMengData2` Verwenden eines digitalen SSL-Zertifikats.

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

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](#)

Aktivieren Sie den Zugriff auf Active Directory-Konten

Sie können das verwenden `security login create` Befehl zum Aktivieren von Active Directory-Benutzer- oder Gruppenkonten für den Zugriff auf einen Administrator oder eine Daten-SVM 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 dies nutzen ["LDAP fast bind für nsswitch-Authentifizierung"](#) Wenn es vom AD LDAP-Server unterstützt wird.

- Wenn Sie sich nicht sicher sind, welche Rolle bei der Zugriffssteuerung Sie dem Login-Konto zuweisen möchten, können Sie das verwenden `security login modify` Befehl, um die Rolle später hinzuzufügen.

Ändern der Rolle, die einem Administrator zugewiesen ist



Der Zugriff auf das Konto FÜR DIE ANZEIGENGRUPPE wird nur mit dem unterstützt SSH, ontapi, und rest Applikationen 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	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role></pre>

ONTAP-Version	Primäre Authentifizierung	Sekundäre Authentifizierung	Befehl
9.13.1 und höher	Domäne	Öffentlicher Schlüssel	<p>Für einen neuen Benutzer</p> <pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre> <p>Für einen bestehenden Benutzer</p> <pre>security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre>
9.0 und höher	Domäne	Keine	<pre>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]</pre>

Für AD-Gruppen:

ONTAP-Version	Primäre Authentifizierung	Sekundäre Authentifizierung	Befehl
9.0 und höher	Domäne	Keine	<pre>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]</pre>

Eine vollständige Befehlssyntax finden Sie unter "[Worksheets zur Administratorauthentifizierung und RBAC-Konfiguration](#)"

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](#)

Aktivieren Sie den LDAP- oder NIS-Kontozugriff

Sie können das verwenden `security login create` Befehl zum Aktivieren von LDAP- oder NIS-Benutzerkonten für den Zugriff auf Admin oder Daten-SVMs. 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 Rolle bei der Zugriffssteuerung Sie dem Login-Konto zuweisen möchten, können Sie das verwenden `security login modify` Befehl, um die Rolle später hinzuzufügen.

[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 dies nutzen "[LDAP fast bind für nsswitch-Authentifizierung](#)" Wenn es vom LDAP-Server unterstützt wird.
- Aufgrund eines bekannten LDAP-Problems sollten Sie das nicht verwenden ' : ' (Doppelpunkt) Zeichen in einem beliebigen Feld von LDAP-Benutzerkontoinformationen (z. B. `gecos`, `userPassword`, Und so weiter). 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]
```

Eine vollständige Befehlssyntax finden Sie im "[Arbeitsblatt](#)".

"Erstellen oder Ändern von Anmeldekonto"

Mit dem folgenden Befehl wird das LDAP- oder NIS-Cluster-Administratorkonto aktiviert `guest2` Mit dem vordefinierten `backup` Rolle für den Zugriff auf die `Administrator-SVMengCluster`.

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

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 angegeben werden `publickey` Und zweite Authentifizierungsmethode als `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

Copyright-Informationen

Copyright © 2024 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 IRGEND EINER 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.