



Aktivieren Sie den Zugriff auf lokales Konto

ONTAP 9

NetApp
March 24, 2023

Inhaltsverzeichnis

- Aktivieren Sie den Zugriff auf lokales Konto 1
 - Lokalen Kontozugriff aktivieren – Übersicht 1
 - Aktivieren Sie den Zugriff auf das Passwort-Konto 1
 - Aktivieren Sie SSH-Konten für öffentliche Schlüssel 1
 - Multi-Faktor-SSH-Authentifizierung (MFA) aktivieren 3
 - Aktivieren Sie SSL-Zertifikatkonten 4

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.

Was Sie benötigen

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

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.

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 Befehlsyntax 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-SVM `engCluster` 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

Was Sie benötigen

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

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 ssh-ed25519 Host Key Algorithmus wurde in 9.11.1 entfernt

Weitere Informationen finden Sie unter "[Konfiguration der Netzwerksicherheit mit FIPS](#)".

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 Befehlsyntax finden Sie im "[Arbeitsblatt](#)".

Mit dem folgenden Befehl wird das SVM-Administratorkonto aktiviert `svmin1` 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](#)

Multi-Faktor-SSH-Authentifizierung (MFA) aktivieren

Ab ONTAP 9.3 können Sie den verwenden `security login create` Um die Sicherheit zu verbessern, müssen sich Administratoren bei einem Administrator oder einer Daten-SVM sowohl mit einem öffentlichen SSH-Schlüssel als auch mit einem Benutzerpasswort einloggen.

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.

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

Bevor Sie beginnen

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

Über diese Aufgabe

- Sie müssen 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.

- 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 Benutzer wird immer mit Authentifizierung des öffentlichen Schlüssels und der Kennwortauthentifizierung authentifiziert.

Schritt

1. Lokale Administratorkonten erforderlich, um über SSH MFA auf eine SVM zuzugreifen:

```
security login create -vserver SVM -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".

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 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

Was Sie benötigen

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

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](#)



Für Cluster-Administratorkonten wird die Zertifikatauthentifizierung nur mit unterstützt `http` Und `ontapi` Applikationen unterstützt. Bei SVM-Administratorkonten wird die Zertifikatauthentifizierung nur von unterstützt `ontapi` Applikation.

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

Eine 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](#)

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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.