Erstellen von Anmeldekonten

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

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.

> Die folgenden allgemeinen Namen können nicht für Remote-Cluster- und SVM-Administratorkonten verwendet werden: „adm“, „bin“, „cli“, „Daemon“, „ftp“, „Spiele“, „Halt“, „lp“, „Mail“, „man“, „Naroot“, „netapp“, „Nachrichten“, „niemand“, „Betreiber“, „Root“, „Shutdown“, „sshd“, „Sync“, „sys“, „uucp“ und „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.

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 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-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 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 SVM`engData1` 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 SVM`engData2` 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.

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.

Was Sie benötigen

- 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.

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 9.11.1 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` Und `ontapi` Applikationen unterstützt.

Schritt

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

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod domain -role role -comment comment [-is-
   ldap-fastbind true]
   ```

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   "Erstellen oder Ändern von Anmeldekonten"

   Mit dem folgenden Befehl wird das AD-Cluster-Administratorkonto aktiviert `DOMAIN1\guest1` Mit dem vordefinierten `backup` Rolle für den Zugriff auf die Administrator-SVM`engCluster`.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
DOMAIN1\guest1 -application ssh -authmethod domain -role backup
```

Mit dem folgenden Befehl werden die SVM-Administratorkonten im AD-Gruppenkonto aktiviert `DOMAIN1\adgroup` Mit dem vordefinierten `vsadmin-volume` Rolle für den Zugriff auf die SVM`engData`.

```
cluster1::>security login create -vserver engData -user-or-group-name
DOMAIN1\adgroup -application ssh -authmethod domain -role vsadmin-volume
```

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.

Was Sie benötigen

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

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.

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 Anmeldekonten"

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

   ```
   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

Konfigurieren Sie die SAML-Authentifizierung

Ab ONTAP 9.3 können Sie die SAML-Authentifizierung (Security Assertion Markup Language) für Webservices konfigurieren. Wenn die SAML-Authentifizierung konfiguriert und aktiviert ist, werden Benutzer von einem externen Identitäts-Provider (IdP) anstelle von Verzeichnisdienstanbietern wie Active Directory und LDAP authentifiziert.

Was Sie benötigen

- Sie müssen das IdP für SAML-Authentifizierung konfiguriert haben.
- Sie müssen über die IdP-URI verfügen.

Über diese Aufgabe

- SAML-Authentifizierung gilt nur für das `http` Und `ontapi` Applikationen unterstützt.

  Der `http` Und `ontapi` Applikationen werden von folgenden Web-Services verwendet: Service Processor Infrastructure, ONTAP APIs oder System Manager.

- SAML-Authentifizierung ist nur für den Zugriff auf die Administrator-SVM anwendbar.

Schritte

1. SAML-Konfiguration für den Zugriff von ONTAP auf die IdP-Metadaten erstellen:

   `security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name`

   `idp_uri` Ist die FTP- oder HTTP-Adresse des IdP-Hosts, von dem die IdP-Metadaten heruntergeladen werden können.

   `ontap_host_name` Ist der Hostname oder die IP-Adresse des Host des SAML-Service-Providers, was in diesem Fall das ONTAP-System ist. Standardmäßig wird die IP-Adresse der Cluster-Management-LIF verwendet.

   Optional können Sie die Zertifikatsinformationen für den ONTAP-Server angeben. Standardmäßig werden die Zertifikatinformationen des ONTAP-Webservers verwendet.

   ```
   cluster_12::> security saml-sp create -idp-uri
   https://scspr0235321001.gdl.englab.netapp.com/idp/shibboleth -verify
   -metadata-server false

   Warning: This restarts the web server. Any HTTP/S connections that are
   active
            will be disrupted.
   Do you want to continue? {y|n}: y
   [Job 179] Job succeeded: Access the SAML SP metadata using the URL:
   https://10.63.56.150/saml-sp/Metadata

   Configure the IdP and Data ONTAP users for the same directory server
   domain to ensure that users are the same for different authentication
   methods. See the "security login show" command for the Data ONTAP user
   configuration.
   ```

   Die URL für den Zugriff auf die ONTAP-Hostmetadaten wird angezeigt.

2. Konfigurieren Sie vom IdP-Host aus das IdP mit den ONTAP-Host-Metadaten.

   Weitere Informationen zum Konfigurieren des IdP finden Sie in der IdP-Dokumentation.

3. SAML-Konfiguration aktivieren:

```
security saml-sp modify -is-enabled true
```

Alle bestehenden Benutzer, die auf das zugreifen `http` Oder `ontapi` Die Applikation wird automatisch für die SAML-Authentifizierung konfiguriert.

4. Wenn Sie Benutzer für das erstellen möchten `http` Oder `ontapi` Anwendung, nachdem SAML konfiguriert wurde, geben Sie SAML als Authentifizierungsmethode für die neuen Benutzer an.

   a. Anmeldemethode für neue Benutzer mit SAML-Authentifizierung erstellen: `security login create -user-or-group-name user_name -application [http | ontapi] -authentication -method saml -vserver svm_name`

   ```
   cluster_12::> security login create -user-or-group-name admin1
   -application http -authentication-method saml -vserver  cluster_12
   ```

   b. Überprüfen Sie, ob der Benutzereintrag erstellt wurde:
   `security login show`

   ```
   cluster_12::> security login show

   Vserver: cluster_12

   Second
   User/Group                 Authentication                 Acct
   Authentication
   Name            Application Method        Role Name        Locked
   Method
   -------------- ----------- ------------- ---------------- ------
   --------------
   admin           console     password      admin            no     none
   admin           http        password      admin            no     none
   admin           http        saml          admin            -      none
   admin           ontapi      password      admin            no     none
   admin           ontapi      saml          admin            -      none
   admin           service-processor
                               password      admin            no     none
   admin           ssh         password      admin            no     none
   admin1          http        password      backup           no     none
   **admin1          http        saml          backup           -
   none**
   ```