Verwalten von Administratorkonten

ONTAP 9

NetApp
March 21, 2023

Inhaltsverzeichnis

Verwalten von Administratorkonten

Administratorkonten verwalten – Übersicht

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

Einem Administratorkonto einen öffentlichen Schlüssel zuordnen

Bei der SSH-Authentifizierung für den öffentlichen Schlüssel müssen Sie den öffentlichen Schlüssel einem Administratorkonto zuweisen, bevor das Konto auf die SVM zugreifen kann. Sie können das verwenden `security login publickey create` Befehl zum Zuordnen eines Schlüssels zu einem Administratorkonto.

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritt

1. Einen öffentlichen Schlüssel einem Administratorkonto zuordnen:

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

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   "Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto"

   Der folgende Befehl ordnet dem SVM-Administratorkonto einen öffentlichen Schlüssel zu `svmadmin1` Für die SVM `engData1`. Dem öffentlichen Schlüssel wird die Indexnummer 5 zugewiesen.

   ```
   cluster1::>security login publickey create -vserver engData1 -username
   svmadmin1 -index 5 -publickey
   "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J
   /vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIza
   FciDy7hgnmdj9eNGedGr/JNrftQbLD1hZybX+72DpQB0tYWBhe6eDJ1oPLob
   ZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
   ```

Erstellen und Installieren eines CA-signierten Serverzertifikats

Erstellen und installieren Sie eine Übersicht über ein CA-signiertes Serverzertifikat

Auf Produktionssystemen ist es eine Best Practice, ein von CA signiertes digitales Zertifikat zur Authentifizierung des Clusters oder der SVM als SSL-Server zu installieren. Sie können das verwenden `security certificate generate-csr` Befehl zum Generieren einer Zertifikatsignierungsanforderung (CSR) und des `security certificate install` Befehl zum Installieren des Zertifikats, das Sie von der Zertifizierungsstelle erhalten.

Generieren Sie eine Anforderung zum Signieren eines Zertifikats

Sie können das verwenden `security certificate generate-csr` Befehl zum Generieren einer Zertifikatsignierungsanforderung (CSR). Nach Bearbeitung Ihrer Anfrage sendet Ihnen die Zertifizierungsstelle (CA) das signierte digitale Zertifikat.

Was Sie benötigen

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

Schritte

1. CSR erstellen:

   ```
   security certificate generate-csr -common-name FQDN_or_common_name -size
   512|1024|1536|2048 -country country -state state -locality locality
   -organization organization -unit unit -email-addr email_of_contact -hash
   -function SHA1|SHA256|MD5
   ```

   Mit dem folgenden Befehl wird eine CSR mit A erstellt `2048`-Bit privater Schlüssel generiert durch die `SHA256` Hashing-Funktion für den Einsatz durch `Software` Gruppe in der `IT` Abteilung eines Unternehmens, dessen eigener gemeinsamer Name ist `server1.companyname.com`, Befindet sich in `Sunnyvale`, `California`, `USA`. Die E-Mail-Adresse des SVM-Kontaktadministrators lautet `web@example.com`. Das System zeigt den CSR und den privaten Schlüssel in der Ausgabe an.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----

Note: Please keep a copy of your certificate request and private key for
future reference.
```

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

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

Installieren Sie ein CA-signiertes Serverzertifikat

Sie können das verwenden `security certificate install` Befehl zum Installieren eines CA-signierten Serverzertifikats auf einer SVM. ONTAP fordert Sie auf, die Stammzertifikate und Zwischenzertifikate der Zertifizierungsstelle (CA) anzugeben, die die Zertifikatskette des Serverzertifikats bilden.

Was Sie benötigen

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

Schritt

1. Installieren eines CA-signierten Serverzertifikats: `security certificate install -vserver SVM_name -type certificate_type`

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   > ONTAP fordert Sie zur Eingabe der CA-Stammzertifikate und der Zwischenzertifikate auf, die die Zertifikatskette des Serverzertifikats bilden. Die Kette beginnt mit dem Zertifikat der Zertifizierungsstelle, die das Serverzertifikat ausgestellt hat, und kann bis zum Stammzertifikat der Zertifizierungsstelle reichen. Fehlende Zwischenzertifikate führen zum Ausfall der Serverzertifikatinstallation.

   Mit dem folgenden Befehl wird das CA-signierte installiert `server` Zertifikat und Zwischenzertifikate auf der SVM`engData2`.

```
cluster1::>security certificate install -vserver engData2 -type server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECxMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuSl8U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEAr1mnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate certificates
{y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
```

```
BgkqhkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate certificates
{y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate certificates
{y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

Konfigurieren Sie den Active Directory-Domänencontroller-Zugriff

Konfigurieren Sie die Active Directory-Domänencontroller-Zugriffsübersicht

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

ONTAP unterstützt die folgenden Authentifizierungsservices für Domänencontroller:

- Kerberos
- LDAP
- Netzanmeldung

- Lokale Sicherheitsbehörde (LSA)

ONTAP unterstützt die folgenden Sitzungsschlüsselalgorithmen für sichere Netlogon-Verbindungen:

Sitzungsschlüsselalgorithmus	Verfügbar in…
HMAC-SHA256, basierend auf dem Advanced Encryption Standard (AES)	ONTAP 9.10.1 und höher
DES und HMAC-MD5 (bei festem Schlüssel)	Alle ONTAP 9 Versionen

Wenn Sie AES-Sitzungsschlüssel während der Einrichtung des sicheren Netzwerklogon-Kanals in ONTAP 9.10.1 und höher verwenden möchten, müssen Sie diese mit dem folgenden Befehl aktivieren:

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

Die Standardeinstellung lautet `false`.

In ONTAP-Versionen vor 9.10.1, wenn der Domain-Controller AES für sichere Netlogon-Dienste erzwingt, schlägt die Verbindung fehl. Der Domain-Controller muss so konfiguriert sein, dass er in diesen Versionen starke Schlüsselverbindungen mit ONTAP akzeptiert.

Konfigurieren Sie einen Authentifizierungstunnel

Falls Sie bereits einen SMB-Server für eine Daten-SVM konfiguriert haben, können Sie den verwenden `security login domain-tunnel create` Befehl zum Konfigurieren der SVM als Gateway, oder *Tunnel*, für AD-Zugriff auf das Cluster.

Was Sie benötigen

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

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

HINWEIS

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

Schritt

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

   ```
   security login domain-tunnel create -vserver SVM_name
   ```

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

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

Die SMB-fähige Daten-SVM wird mit dem folgenden Befehl konfiguriert`engData` Als Authentifizierungstunnel.

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

Erstellen Sie ein SVM-Computerkonto in der Domäne

Falls Sie noch keinen SMB-Server für eine Daten-SVM konfiguriert haben, können Sie den verwenden `vserver active-directory create` Befehl zum Erstellen eines Computerkontos für die SVM in der Domäne.

Was Sie benötigen

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

Über diese Aufgabe

Nach der Eingabe des `vserver active-directory create` Befehl, Sie werden aufgefordert, die Anmeldeinformationen für ein AD-Benutzerkonto mit ausreichenden Berechtigungen bereitzustellen, um der angegebenen Organisationseinheit in der Domäne Computer hinzuzufügen. Das Passwort des Kontos darf nicht leer sein.

Schritt

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

   `vserver active-directory create -vserver` *`SVM_name`* `-account-name` *`NetBIOS_account_name`* `-domain` *`domain`* `-ou` *`organizational_unit`*

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

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

   ```
   cluster1::>vserver active-directory create -vserver engData -account
   -name ADSERVER1 -domain example.com

   In order to create an Active Directory machine account, you must supply
   the name and password of a Windows account with sufficient privileges to
   add computers to the "CN=Computers" container within the "example.com"
   domain.

   Enter the user name: Administrator

   Enter the password:
   ```

Konfigurieren Sie den LDAP- oder NIS-Serverzugriff

Konfigurieren Sie die Übersicht über den Zugriff auf LDAP- oder NIS-Server

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

Konfigurieren Sie den LDAP-Serverzugriff

Sie müssen den LDAP-Serverzugriff auf eine SVM konfigurieren, bevor LDAP-Konten auf die SVM zugreifen können. Sie können das verwenden `vserver services name-service ldap client create` Befehl zum Erstellen einer LDAP-Client-Konfiguration auf der SVM. Anschließend können Sie die verwenden `vserver services name-service ldap create` Befehl zum Zuordnen der LDAP-Client-Konfiguration zur SVM.

Was Sie benötigen

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

Über diese Aufgabe

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

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

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

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

Schritte

1. LDAP-Client-Konfiguration auf einer SVM erstellen: `vserver services name-service ldap client create -vserver SVM_name -client-config client_configuration -servers LDAP_server_IPs -schema schema -use-start-tls true|false`

   > Start TLS wird nur für den Zugriff auf Data SVMs unterstützt. Der Zugriff auf Admin-SVMs wird nicht unterstützt.

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   Mit dem folgenden Befehl wird eine LDAP-Client-Konfiguration mit dem Namen erstellt `corp` Auf der SVM`engData`. Der Client macht anonyme Bindungen mit den LDAP-Servern mit den IP-Adressen `172.160.0.100` Und `172.16.0.101`. Der Client verwendet das `RFC-2307` Schema zum Erstellen von

LDAP-Abfragen. Die Kommunikation zwischen Client und Server wird über Start TLS verschlüsselt.

```
cluster1::>vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```

Ab ONTAP 9.2 Field Portal `-ldap-servers` Ersetzt das Feld `-servers`. Dieses neue Feld kann entweder einen Hostnamen oder eine IP-Adresse für den LDAP-Server verwenden.

2. Verbinden Sie die LDAP-Client-Konfiguration mit der SVM: `vserver services name-service ldap create -vserver SVM_name -client-config client_configuration -client-enabled true|false`

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   Mit dem folgenden Befehl wird die LDAP-Client-Konfiguration zugeordnet `corp` Mit der SVM`engData`, Und aktiviert den LDAP-Client auf der SVM.

   ```
   cluster1::>vserver services name-service ldap create -vserver engData
   -client-config corp -client-enabled true
   ```

   Ab ONTAP 9.2 beginnt der `vserver services name-service ldap create` Der Befehl führt eine automatische Konfigurationsvalidierung durch und meldet eine Fehlermeldung, wenn ONTAP den Namensserver nicht kontaktieren kann.

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

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

   ```
   cluster1::> vserver services name-service ldap check -vserver vs0

   | Vserver: vs0                                                |
   | Client Configuration Name: c1                               |
   | LDAP Status: up                                             |
   | LDAP Status Details: Successfully connected to LDAP server
   "10.11.12.13".                                              |
   ```

   Der Befehl Name Service Check ist ab ONTAP 9.2 verfügbar.

Konfigurieren Sie den NIS-Serverzugriff

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

auf einer SVM.

Was Sie benötigen

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

Über diese Aufgabe

Sie können mehrere NIS-Domänen erstellen. Es kann nur eine NIS-Domäne festgelegt werden `active` Zu einer Zeit.

Schritt

1. Erstellen einer NIS-Domänenkonfiguration auf einer SVM: `vserver services name-service nis-domain create -vserver SVM_name -domain client_configuration -active true|false -nis-servers NIS_server_IPs`

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   > Ab ONTAP 9.2 Field Portal `-nis-servers` Ersetzt das Feld `-servers`. Dieses neue Feld kann entweder einen Hostnamen oder eine IP-Adresse für den NIS-Server enthalten.

   Mit dem folgenden Befehl wird eine NIS-Domänenkonfiguration auf der SVM erstellt `engData`. Die NIS-Domäne `nisdomain` Ist bei der Erstellung aktiv und kommuniziert mit einem NIS-Server mit der IP-Adresse `192.0.2.180`.

```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
```

Erstellen Sie einen Namensdienstschalter

Mit der Namensdienst-Switch-Funktion können Sie LDAP oder NIS als alternative Namensdienstquellen verwenden. Sie können das verwenden `vserver services name-service ns-switch modify` Befehl zum Festlegen der Reihenfolge für Name-Service-Quellen.

Was Sie benötigen

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

Schritt

1. Geben Sie die Suchreihenfolge für Namensdienstquellen an:

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

   Eine vollständige Befehlssyntax finden Sie im "Arbeitsblatt".

   Mit dem folgenden Befehl wird die Suchreihenfolge der LDAP- und NIS-Namensdienstquellen für die

festgelegt `passwd` Datenbank auf dem `engData`SVM:

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

Ändern Sie ein Administratorpasswort

Sie sollten Ihr Anfangspasswort sofort nach der ersten Anmeldung am System ändern. Als SVM-Administrator können Sie die verwenden `security login password` Befehl zum Ändern Ihres eigenen Passworts. Als Cluster-Administrator können Sie das verwenden `security login password` Befehl zum Ändern des Administratorkennworts.

Was Sie benötigen

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

Über diese Aufgabe

Das neue Passwort muss folgende Bedingungen erfüllen:

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

> Sie können das verwenden.`security login role config modify` Befehl zum Ändern der Kennwortregeln für Konten, die einer bestimmten Rolle zugeordnet sind. Weitere Informationen finden Sie auf der man-Page.`security login role config modify`

Schritt

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

   Mit dem folgenden Befehl wird das Passwort des Administrators geändert `admin1` Für die SVM`vs1.example.com`. Sie werden aufgefordert, das aktuelle Passwort einzugeben, dann das neue Passwort einzugeben und erneut einzugeben.

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

Sperren und Entsperren eines Administratorkontos

Sie können das verwenden `security login lock` Befehl zum Sperren eines Administratorkontos und des `security login unlock` Befehl zum Entsperren des Kontos.

Was Sie benötigen

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

Schritte

1. Administratorkonto sperren:

   `security login lock -vserver SVM_name -username user_name`

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

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

2. Administratorkonto entsperren:

   `security login unlock -vserver SVM_name -username user_name`

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

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

Fehlgeschlagene Anmeldeversuche verwalten

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

Wie Sie wissen, dass Anmeldeversuche fehlgeschlagen sind

Das Event Management System (EMS) informiert Sie jede Stunde über fehlgeschlagene Anmeldeversuche. Im finden Sie eine Aufzeichnung fehlgeschlagener Anmeldeversuche `audit.log` Datei:

Was tun, wenn wiederholte Anmeldeversuche fehlschlagen

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

- Kennwörter müssen aus einer Mindestanzahl von Groß-/Kleinschreibung, Kleinbuchstaben, Sonderzeichen und/oder Ziffern bestehen
- Legen Sie nach einem fehlgeschlagenen Anmeldeversuch eine Verzögerung fest

- Begrenzen Sie die Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche und sperren Sie Benutzer nach der angegebenen Anzahl fehlgeschlagener Versuche
- Verfallen und sperren Sie Konten, die für eine bestimmte Anzahl von Tagen inaktiv sind

Sie können das verwenden `security login role config modify` Befehl zum Ausführen dieser Aufgaben.

Langfristig können Sie die folgenden zusätzlichen Schritte einleiten:

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

SHA-2 für Passwörter für Administratorkonten erzwingen

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

Über diese Aufgabe

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

- Zeigt Benutzerkonten an, die mit der angegebenen Hash-Funktion übereinstimmen.
- Verfallen von Konten, die eine angegebene Hash-Funktion verwenden (z. B. MD5), sodass die Benutzer ihre Passwörter bei der nächsten Anmeldung ändern müssen.
- Konten sperren, deren Passwörter die angegebene Hash-Funktion verwenden.
- Wenn Sie auf eine Version vor ONTAP 9 zurücksetzen, setzen Sie das Kennwort des Clusteradministrators zurück, damit es mit der Hash-Funktion (MD5) kompatibel ist, die von der früheren Version unterstützt wird.

ONTAP akzeptiert vorgehackte SHA-2-Passwörter nur mithilfe des NetApp Manageability SDK (Security-Login-create und Security-Login-modify-password).

"Bessere Managebarkeit"

Schritte

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

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

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

      Das System erkennt, dass die Konten abgelaufen sind, und fordert Benutzer auf, ihre Passwörter zu ändern. SHA-512 wird standardmäßig für die geänderten Passwörter verwendet.
2. Bei MD5-Konten, deren Benutzer sich nicht anmelden, um ihre Passwörter innerhalb eines bestimmten

Zeitraums zu ändern, erzwingen Sie die Kontomigration:

a. Konten sperren, die weiterhin die MD5-Hash-Funktion verwenden (erweiterte Berechtigungsebene): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

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

b. Entsperren Sie die Konten, wenn die Benutzer bereit sind, ihre Passwörter zu ändern: `security login unlock -vserver vserver_name -username user_name`

c. Benutzer müssen sich über eine Konsole oder SSH-Sitzung bei ihren Konten anmelden und ihre Passwörter ändern, wenn das System sie dazu auffordert.