Gérez les comptes d'administrateur

ONTAP 9

NetApp
September 12, 2024

Sommaire

Gérez les comptes d'administrateur

Gérer la présentation des comptes d'administrateur

Selon la manière dont vous avez activé l'accès au compte, vous devrez peut-être associer une clé publique à un compte local, installer un certificat numérique de serveur signé par une autorité de certification ou configurer l'accès AD, LDAP ou NIS. Vous pouvez effectuer toutes ces tâches avant ou après l'activation de l'accès au compte.

Associer une clé publique à un compte d'administrateur

Pour l'authentification de clé publique SSH, vous devez associer la clé publique à un compte d'administrateur avant que le compte puisse accéder à la SVM. Vous pouvez utiliser le `security login publickey create` commande permettant d'associer une clé à un compte d'administrateur.

Description de la tâche

Si vous authentifiez un compte via SSH avec un mot de passe et une clé publique SSH, le compte est authentifié d'abord par la clé publique.

Avant de commencer

- Vous devez avoir généré la clé SSH.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Associer une clé publique à un compte d'administrateur :

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

   Pour obtenir la syntaxe complète de la commande, reportez-vous à la fiche de référence de "Association d'une clé publique à un compte d'utilisateur".

2. Vérifiez la modification en affichant la clé publique :

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Exemple

La commande suivante associe une clé publique au compte d'administrateur du SVM `svmadmin1` Pour la SVM `engData1`. La clé publique est affectée à l'index numéro 5.

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

Gérer les clés publiques SSH et les certificats X.509 pour un compte d'administrateur

Pour une sécurité accrue de l'authentification SSH avec des comptes d'administrateur, vous pouvez utiliser `security login publickey` Ensemble de commandes pour gérer la clé publique SSH et son association avec les certificats X.509.

Associer une clé publique et un certificat X.509 à un compte d'administrateur

À partir de ONTAP 9.13.1, vous pouvez associer un certificat X.509 à la clé publique que vous associez au compte d'administrateur. Cela vous donne la sécurité supplémentaire des vérifications d'expiration ou de révocation des certificats lors de la connexion SSH à ce compte.

Description de la tâche

Si vous authentifiez un compte via SSH avec une clé publique SSH et un certificat X.509, ONTAP vérifie la validité du certificat X.509 avant de s'authentifier avec la clé publique SSH. La connexion SSH sera refusée si le certificat a expiré ou a été révoqué et la clé publique sera automatiquement désactivée.

Avant de commencer

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Vous devez avoir généré la clé SSH.
- Si vous n'avez besoin que de vérifier l'expiration du certificat X.509, vous pouvez utiliser un certificat auto-signé.
- Si vous avez besoin de vérifier l'expiration et la révocation du certificat X.509 :
  - Vous devez avoir reçu le certificat d'une autorité de certification (CA).
  - Vous devez installer la chaîne de certificats (certificats CA intermédiaire et racine) à l'aide de `security certificate install` commandes.
  - Vous devez activer OCSP pour SSH. Reportez-vous à la section "Vérifiez que les certificats numériques sont valides à l'aide du protocole OCSP" pour obtenir des instructions.

Étapes

1. Associer une clé publique et un certificat X.509 à un compte d'administrateur :

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-x509-certificate install`

   Pour obtenir la syntaxe complète de la commande, reportez-vous à la fiche de référence de "Association d'une clé publique à un compte d'utilisateur".

2. Vérifiez la modification en affichant la clé publique :

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Exemple

La commande suivante associe une clé publique et un certificat X.509 au compte d'administrateur du SVM `svmadmin2` Pour la SVM `engData2`. Le numéro d'index 6 est attribué à la clé publique.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

Supprimez l'association de certificat de la clé publique SSH d'un compte d'administrateur

Vous pouvez supprimer l'association de certificat actuelle de la clé publique SSH du compte, tout en conservant la clé publique.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Supprimez l'association de certificat X.509 d'un compte d'administrateur et conservez la clé publique SSH existante :

   `security login publickey modify -vserver SVM_name -username user_name -index index -x509-certificate delete`

2. Vérifiez la modification en affichant la clé publique :

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Exemple

La commande suivante supprime l'association de certificat X.509 du compte d'administrateur du SVM `svmadmin2` Pour la SVM `engData2` au numéro d'index 6.

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

Supprimez la clé publique et l'association de certificat d'un compte d'administrateur

Vous pouvez supprimer la clé publique actuelle et la configuration de certificat d'un compte.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Supprimez la clé publique et une association de certificat X.509 d'un compte d'administrateur :

   `security login publickey delete -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

2. Vérifiez la modification en affichant la clé publique :

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Exemple

La commande suivante supprime une clé publique et un certificat X.509 du compte d'administrateur du SVM `svmadmin3` Pour la SVM `engData3` au numéro d'index 7.

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

Configurez Cisco Duo 2FA pour les connexions SSH

À partir de ONTAP 9.14.1, vous pouvez configurer ONTAP pour qu'il utilise Cisco Duo pour l'authentification à deux facteurs (2FA) pendant les connexions SSH. Vous configurez Duo au niveau du cluster et il s'applique par défaut à tous les comptes utilisateur. Vous pouvez également configurer Duo au niveau de la machine virtuelle de stockage (anciennement vServer), auquel cas il s'applique uniquement aux utilisateurs de cette machine virtuelle de stockage. Si vous activez et configurez Duo, il sert de méthode d'authentification supplémentaire, en complément des méthodes existantes pour tous les utilisateurs.

Si vous activez l'authentification Duo pour les connexions SSH, les utilisateurs devront inscrire un périphérique lors de leur prochaine connexion à l'aide de SSH. Pour plus d'informations sur l'inscription, reportez-vous au Cisco Duo "documentation d'inscription".

Vous pouvez utiliser l'interface de ligne de commande ONTAP pour effectuer les tâches suivantes avec Cisco Duo :

- Configurez Cisco Duo
- Modifier la configuration Cisco Duo
- Supprimez la configuration Cisco Duo
- Afficher la configuration Cisco Duo
- Supprimer un groupe Duo
- Afficher les groupes Duo
- Contourner l'authentification Duo pour les utilisateurs

Configurez Cisco Duo

Vous pouvez créer une configuration Cisco Duo pour l'ensemble du cluster ou pour une VM de stockage spécifique (appelée vServer dans l'interface de ligne de commande ONTAP) à l'aide de `security login duo create` commande. Dans ce cas, Cisco Duo est activé pour les connexions SSH pour ce cluster ou cette machine virtuelle de stockage.

Étapes

1. Connectez-vous au panneau d'administration Cisco Duo.
2. Accédez à **applications > application UNIX**.
3. Enregistrez votre clé d'intégration, votre clé secrète et le nom d'hôte de l'API.
4. Connectez-vous à votre compte ONTAP à l'aide de SSH.
5. Activez l'authentification Cisco Duo pour cette machine virtuelle de stockage, en remplaçant les informations de votre environnement par les valeurs entre parenthèses :

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

Pour plus d'informations sur les paramètres requis et facultatifs pour cette commande, reportez-vous à la section "Feuilles de calcul pour l'authentification de l'administrateur et la configuration du RBAC".

Modifier la configuration Cisco Duo

Vous pouvez modifier la façon dont Cisco Duo authentifie les utilisateurs (par exemple, le nombre d'invites d'authentification données ou le proxy HTTP utilisé). Si vous devez modifier la configuration Cisco Duo pour une machine virtuelle de stockage (appelée vServer dans l'interface de ligne de commande ONTAP), vous pouvez utiliser `security login duo modify` commande.

Étapes

1. Connectez-vous au panneau d'administration Cisco Duo.
2. Accédez à **applications > application UNIX**.
3. Enregistrez votre clé d'intégration, votre clé secrète et le nom d'hôte de l'API.
4. Connectez-vous à votre compte ONTAP à l'aide de SSH.
5. Modifiez la configuration Cisco Duo pour cette machine virtuelle de stockage en remplaçant les informations mises à jour de votre environnement par les valeurs entre parenthèses :

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-prompts 1|2|3 \
-max-unenrolled-logins <NUM_LOGINS> \
-is-enabled true|false \
-fail-mode safe|secure
```

Supprimez la configuration Cisco Duo

Vous pouvez supprimer la configuration Cisco Duo, ce qui supprime la nécessité pour les utilisateurs SSH de s'authentifier à l'aide de Duo lors de la connexion. Pour supprimer la configuration Cisco Duo d'une machine virtuelle de stockage (appelée vServer dans l'interface de ligne de commande ONTAP), vous pouvez utiliser `security login duo delete` commande.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Supprimez la configuration Cisco Duo pour cette machine virtuelle de stockage, en remplaçant le nom de votre machine virtuelle de stockage par `<STORAGE_VM_NAME>`:

   ```
   security login duo delete  -vserver <STORAGE_VM_NAME>
   ```

   Cette opération supprime définitivement la configuration Cisco Duo pour cette machine virtuelle de stockage.

Afficher la configuration Cisco Duo

Vous pouvez afficher la configuration Cisco Duo existante pour une machine virtuelle de stockage (appelée vServer dans l'interface de ligne de commande ONTAP) à l'aide de `security login duo show` commande.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Affiche la configuration Cisco Duo pour cette machine virtuelle de stockage. Si vous le souhaitez, vous pouvez utiliser le `vserver` Paramètre permettant de spécifier une machine virtuelle de stockage, en remplaçant le nom de la machine virtuelle de stockage par `<STORAGE_VM_NAME>`:

   ```
   security login duo show -vserver <STORAGE_VM_NAME>
   ```

   Vous devez voir les résultats similaires à ce qui suit :

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

Créez un groupe Duo

Vous pouvez demander à Cisco Duo d'inclure uniquement les utilisateurs d'un certain groupe d'utilisateurs Active Directory, LDAP ou local dans le processus d'authentification Duo. Si vous créez un groupe Duo, seuls les utilisateurs de ce groupe sont invités à s'authentifier Duo. Vous pouvez créer un groupe Duo à l'aide du `security login duo group create` commande. Lorsque vous créez un groupe, vous pouvez exclure certains utilisateurs de ce groupe du processus d'authentification Duo.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Créez le groupe Duo en remplaçant les informations de votre environnement par les valeurs entre parenthèses. Si vous omettez le `-vserver` le groupe est créé au niveau du cluster :

   ```
   security login duo group create -vserver <STORAGE_VM_NAME> -group-name
   <GROUP_NAME> -exclude-users <USER1, USER2>
   ```

   Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local. Utilisateurs que vous spécifiez avec le facultatif `-exclude-users` Le paramètre ne sera pas inclus dans le processus d'authentification Duo.

Afficher les groupes Duo

Vous pouvez afficher les entrées de groupe Cisco Duo existantes à l'aide du `security login duo group show` commande.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Affichez les entrées du groupe Duo, en remplaçant les informations de votre environnement par les valeurs entre parenthèses. Si vous omettez le `-vserver` paramètre, le groupe s'affiche au niveau du cluster :

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local. Utilisateurs que vous spécifiez avec le facultatif `-exclude-users` le paramètre ne s'affiche pas.

Supprimer un groupe Duo

Vous pouvez supprimer une entrée de groupe Duo à l'aide du `security login duo group delete` commande. Si vous supprimez un groupe, les utilisateurs de ce groupe ne sont plus inclus dans le processus d'authentification Duo.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Supprimez l'entrée de groupe Duo, en remplaçant les informations de votre environnement par les valeurs entre parenthèses. Si vous omettez le `-vserver` paramètre, le groupe est supprimé au niveau du cluster :

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME>
```

Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local.

Contourner l'authentification Duo pour les utilisateurs

Vous pouvez exclure tous les utilisateurs ou des utilisateurs spécifiques du processus d'authentification Duo SSH.

Exclure tous les utilisateurs Duo

Vous pouvez désactiver l'authentification SSH Cisco Duo pour tous les utilisateurs.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.
2. Désactivez l'authentification Cisco Duo pour les utilisateurs SSH en remplaçant le nom du vServer par `<STORAGE_VM_NAME>`:

```
security login duo -vserver <STORAGE_VM_NAME> -is-duo-enabled-false
```

Exclure les utilisateurs du groupe Duo

Vous pouvez exclure certains utilisateurs faisant partie d'un groupe Duo du processus d'authentification Duo SSH.

Étapes

1. Connectez-vous à votre compte ONTAP à l'aide de SSH.

2. Désactivez l'authentification Cisco Duo pour des utilisateurs spécifiques d'un groupe. Remplacez le nom du groupe et la liste des utilisateurs à exclure par les valeurs entre parenthèses :

```
security login group modify -group-name <GROUP_NAME> -exclude-users
<USER1, USER2>
```

Le nom du groupe Duo doit correspondre à un groupe Active Directory, LDAP ou local. Utilisateurs que vous spécifiez avec `-exclude-users` Le paramètre ne sera pas inclus dans le processus d'authentification Duo.

Exclure les utilisateurs Duo locaux

Vous pouvez exclure certains utilisateurs locaux de l'authentification Duo à l'aide du panneau d'administration Cisco Duo. Pour obtenir des instructions, reportez-vous au "Documentation Cisco Duo".

Générer et installer un certificat de serveur signé par une autorité de certification

Sur les systèmes de production, il est recommandé d'installer un certificat numérique signé par une autorité de certification pour l'authentification du cluster ou d'un SVM en tant que serveur SSL. Vous pouvez utiliser le `security certificate generate-csr` Commande pour générer une requête de signature de certificat (CSR) et le `security certificate install` commande permettant d'installer le certificat que vous recevez de l'autorité de certification.

Générer une demande de signature de certificat

Vous pouvez utiliser le `security certificate generate-csr` Commande pour générer une requête de signature de certificat (CSR). Après le traitement de votre demande, l'autorité de certification vous envoie le certificat numérique signé.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Générer une RSC :

```
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
```

La commande suivante crée une CSR avec une clé privée 2048 bits générée par la fonction de hachage « `S ra256' » à l'usage du groupe « logiciels » dans le département « IT » d'une entreprise dont le nom commun personnalisé est « `erver1.companyname.com`" », situé à Sunnyvale, en Californie, aux États-Unis. L'adresse e-mail de l'administrateur du contact du SVM est « web@example.com ». Le système affiche la RSC et la clé privée dans la sortie.

Exemple de création d'une RSC

```
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. Copiez la demande de certificat à partir de la sortie CSR et envoyez-la sous forme électronique (par exemple un courriel) à une autorité de certification tierce approuvée pour signature.

   Après le traitement de votre demande, l'AC vous envoie le certificat numérique signé. Vous devez conserver une copie de la clé privée et du certificat numérique signé par l'autorité de certification.

Installez un certificat de serveur signé par une autorité de certification

Vous pouvez utiliser le `security certificate install` Commande permettant d'installer un certificat de serveur signé par une autorité de certification sur un SVM. ONTAP vous invite à entrer les certificats racine et intermédiaire de l'autorité de certification (CA) qui forment la chaîne de certificats du certificat du serveur.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étape

1. Installer un certificat de serveur signé par une autorité de certification :

   ```
   security certificate install -vserver SVM_name -type certificate_type
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous au "feuille de calcul".

   > ONTAP vous invite à entrer les certificats racine et intermédiaire de l'autorité de certification qui constituent la chaîne de certificats du certificat du serveur. La chaîne commence par le certificat de l'autorité de certification qui a émis le certificat du serveur et peut atteindre le certificat racine de l'autorité de certification. Tout certificat intermédiaire manquant entraîne l'échec de l'installation du certificat du serveur.

   La commande suivante installe le certificat de serveur signé par l'autorité de certification et les certificats intermédiaires sur SVM « engData2 ».

Exemple d'installation de certificats intermédiaires de certificat de serveur signés par une autorité de certification

```
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.
```

Gérer les certificats avec System Manager

Depuis ONTAP 9.10.1, vous pouvez utiliser System Manager pour gérer les autorités de certification de confiance, les certificats client/serveur et les autorités de certification locales (intégrées).

Avec System Manager, vous pouvez gérer les certificats reçus d'autres applications afin de pouvoir authentifier les communications de ces applications. Vous pouvez également gérer vos propres certificats qui identifient votre système à d'autres applications.

Afficher les informations sur le certificat

System Manager vous permet d'afficher les autorités de certification approuvées, les certificats client/serveur et les autorités de certification locales stockées sur le cluster.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Faites défiler jusqu'à la zone **sécurité**.
   Dans la section **certificats**, les détails suivants sont affichés :
   - Le nombre d'autorités de certification stockées approuvées.
   - Nombre de certificats client/serveur stockés.
   - Le nombre d'autorités de certification locales stockées.
3. Sélectionnez n'importe quel nombre pour afficher les détails d'une catégorie de certificats, ou sélectionnez → pour ouvrir la page **certificats**, qui contient des informations sur toutes les catégories. La liste affiche les informations relatives à l'ensemble du cluster. Pour afficher les informations relatives à une seule machine virtuelle de stockage spécifique, effectuez les opérations suivantes :

a. Sélectionnez **stockage > machines virtuelles de stockage**.
b. Sélectionnez la VM de stockage.
c. Passez à l'onglet **Paramètres**.
d. Sélectionnez un numéro affiché dans la section **certificat**.

Que faire ensuite

- À partir de la page **certificats**, vous pouvez Générer une demande de signature de certificat.
- Les informations de certificat sont séparées en trois onglets, un pour chaque catégorie. Vous pouvez effectuer les tâches suivantes à partir de chaque onglet :

Dans cet onglet…	Vous pouvez effectuer ces procédures…
Autorités de certification approuvées	• [install-trusted-cert] • Supprimer une autorité de certification approuvée • Renouvelez une autorité de certification approuvée
Certificats client/serveur	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
Autorités locales de certification	• Créez une autorité de certification locale • Signer un certificat à l'aide d'une autorité de certification locale • Supprimer une autorité de certification locale • Renouvelez une autorité de certification locale

Générer une demande de signature de certificat

Vous pouvez générer une demande de signature de certificat (CSR) avec System Manager à partir de n'importe quel onglet de la page **certificats**. Une clé privée et une RSC correspondante sont générées, qui peuvent être signées à l'aide d'une autorité de certification pour générer un certificat public.

Étapes

1. Consultez la page **certificats**. Voir Afficher les informations sur le certificat.
2. Sélectionnez **+Generate CSR**.
3. Renseignez les informations relatives au nom du sujet :
   a. Saisissez un **nom commun**.
   b. Sélectionnez un **pays**.
   c. Saisissez une **organisation**.
   d. Entrez une **unité d'organisation**.
4. Si vous souhaitez remplacer les valeurs par défaut, sélectionnez **plus d'options** et fournissez des informations supplémentaires.

Installez (ajoutez) une autorité de certification approuvée

Vous pouvez installer des autorités de certification approuvées supplémentaires dans System Manager.

Étapes

1. Affichez l'onglet **autorités de certification approuvées**. Voir Afficher les informations sur le certificat.
2. Sélectionnez + Add .
3. Dans le panneau **Ajouter une autorité de certification approuvée**, effectuez les opérations suivantes :
   - Saisissez un **nom**.
   - Pour le **scope**, sélectionnez une VM de stockage.
   - Saisissez un **nom commun**.
   - Sélectionnez un **type**.
   - Entrez ou importez **détails du certificat**.

Supprimer une autorité de certification approuvée

Avec System Manager, vous pouvez supprimer une autorité de certification approuvée.

> Vous ne pouvez pas supprimer les autorités de certification approuvées préinstallées avec ONTAP.

Étapes

1. Affichez l'onglet **autorités de certification approuvées**. Voir Afficher les informations sur le certificat.
2. Sélectionnez le nom de l'autorité de certification approuvée.
3. Sélectionnez ⋮ en regard du nom, puis sélectionnez **Supprimer**.

Renouvelez une autorité de certification approuvée

Avec System Manager, vous pouvez renouveler une autorité de certification de confiance qui a expiré ou est sur le point d'expirer.

Étapes

1. Affichez l'onglet **autorités de certification approuvées**. Voir Afficher les informations sur le certificat.
2. Sélectionnez le nom de l'autorité de certification approuvée.
3. Sélectionnez ⋮ en regard du nom du certificat, puis **Renew**.

Installez (ajoutez) un certificat client/serveur

System Manager vous permet d'installer des certificats client/serveur supplémentaires.

Étapes

1. Afficher l'onglet **certificats client/serveur**. Voir Afficher les informations sur le certificat.
2. Sélectionnez + Add .
3. Sur le panneau **Ajouter un certificat client/serveur**, effectuez les opérations suivantes :

- Saisissez un **nom de certificat**.
- Pour le **scope**, sélectionnez une VM de stockage.
- Saisissez un **nom commun**.
- Sélectionnez un **type**.
- Entrez ou importez **détails du certificat**.
  Vous pouvez écrire ou copier et coller les détails du certificat à partir d'un fichier texte ou importer le texte d'un fichier de certificat en cliquant sur **Importer**.
- Entrez la **clé privée**.
  Vous pouvez écrire ou copier et coller la clé privée à partir d'un fichier texte ou importer le texte d'un fichier de clé privée en cliquant sur **Importer**.

Générer (ajouter) un certificat client/serveur auto-signé

System Manager vous permet de générer des certificats client/serveur autosignés supplémentaires.

Étapes

1. Afficher l'onglet **certificats client/serveur**. Voir Afficher les informations sur le certificat.
2. Sélectionnez **+générer un certificat auto-signé**.
3. Dans le panneau **générer un certificat auto-signé**, effectuez les opérations suivantes :
   - Saisissez un **nom de certificat**.
   - Pour le **scope**, sélectionnez une VM de stockage.
   - Saisissez un **nom commun**.
   - Sélectionnez un **type**.
   - Sélectionnez une fonction **hachage**.
   - Sélectionnez un **taille de clé**.
   - Sélectionnez une **VM de stockage**.

Supprimer un certificat client/serveur

Avec System Manager, vous pouvez supprimer les certificats client/serveur.

Étapes

1. Afficher l'onglet **certificats client/serveur**. Voir Afficher les informations sur le certificat.
2. Sélectionnez le nom du certificat client/serveur.
3. Sélectionnez ⋮ en regard du nom, puis cliquez sur **Supprimer**.

Renouveler un certificat client/serveur

Avec System Manager, vous pouvez renouveler un certificat client/serveur qui a expiré ou est sur le point d'expirer.

Étapes

1. Afficher l'onglet **certificats client/serveur**. Voir Afficher les informations sur le certificat.
2. Sélectionnez le nom du certificat client/serveur.

3. Sélectionnez ⋮ en regard du nom, puis cliquez sur **Renew**.

Créez une autorité de certification locale

Avec System Manager, vous pouvez créer une nouvelle autorité de certification locale.

Étapes

1. Affichez l'onglet **autorités locales de certification**. Voir Afficher les informations sur le certificat.
2. Sélectionnez + Add .
3. Dans le panneau **Ajouter une autorité de certification locale**, effectuez les opérations suivantes :
   - Saisissez un **nom**.
   - Pour le **scope**, sélectionnez une VM de stockage.
   - Saisissez un **nom commun**.
4. Si vous souhaitez remplacer les valeurs par défaut, sélectionnez **plus d'options** et fournissez des informations supplémentaires.

Signer un certificat à l'aide d'une autorité de certification locale

Dans System Manager, vous pouvez signer un certificat à l'aide d'une autorité de certification locale.

Étapes

1. Affichez l'onglet **autorités locales de certification**. Voir Afficher les informations sur le certificat.
2. Sélectionnez le nom de l'autorité de certification locale.
3. Sélectionnez ⋮ en regard du nom, puis **signer un certificat**.
4. Remplissez le formulaire **signer une demande de signature de certificat**.
   - Vous pouvez coller le contenu de la signature de certificat ou importer un fichier de demande de signature de certificat en cliquant sur **Importer**.
   - Indiquez le nombre de jours pendant lesquels le certificat sera valide.

Supprimer une autorité de certification locale

Avec System Manager, vous pouvez supprimer une autorité de certification locale.

Étapes

1. Affichez l'onglet **local Certificate Authority**. Voir Afficher les informations sur le certificat.
2. Sélectionnez le nom de l'autorité de certification locale.
3. Sélectionnez ⋮ en regard du nom, puis **Supprimer**.

Renouvelez une autorité de certification locale

Avec System Manager, vous pouvez renouveler une autorité de certification locale qui a expiré ou est sur le point d'expirer.

Étapes

1. Affichez l'onglet **local Certificate Authority**. Voir Afficher les informations sur le certificat.

2. Sélectionnez le nom de l'autorité de certification locale.
3. Sélectionnez ⋮ en regard du nom, puis cliquez sur **Renew**.

Présentation de la configuration de l'accès au contrôleur de domaine Active Directory

Vous devez configurer l'accès du contrôleur AD domain au cluster ou au SVM avant qu'un compte AD ne puisse accéder au SVM. Si vous avez déjà configuré un serveur SMB pour un SVM de données, vous pouvez configurer le SVM en tant que passerelle, ou *tunnel*, pour l'accès AD au cluster. Si vous n'avez pas configuré de serveur SMB, vous pouvez créer un compte ordinateur pour le SVM sur le domaine AD.

ONTAP prend en charge les services d'authentification de contrôleur de domaine suivants :

- Kerberos
- LDAP
- NETLOGON
- Autorité de sécurité locale (LSA)

ONTAP prend en charge les algorithmes de clé de session suivants pour les connexions Netlogon sécurisées :

Algorithme de clé de session	Disponible à partir de…
HMAC-SHA256, basé sur la norme AES (Advanced Encryption Standard) Si votre cluster exécute ONTAP 9.9.1 ou une version antérieure et que votre contrôleur de domaine applique AES pour des services Netlogon sécurisés, la connexion échoue. Dans ce cas, vous devez reconfigurer votre contrôleur de domaine pour accepter les connexions par clé forte avec ONTAP.	ONTAP 9.10.1
DES et HMAC-MD5 (lorsque la clé est réglée)	Toutes les versions d'ONTAP 9

Si vous souhaitez utiliser les clés de session AES lors de l'établissement d'un canal sécurisé Netlogon, vous devez vérifier que AES est activé sur votre SVM.

- Depuis ONTAP 9.14.1, AES est activé par défaut lorsque vous créez un SVM, et vous n'avez pas besoin de modifier les paramètres de sécurité de votre SVM pour utiliser des clés de session AES lors de l'établissement de canaux sécurisés Netlogon.
- Dans ONTAP 9.10.1 à 9.13.1, AES est désactivé par défaut lors de la création d'un SVM. Vous devez activer AES à l'aide de la commande suivante :

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

> Lorsque vous effectuez une mise à niveau vers ONTAP 9.14.1 ou une version ultérieure, le paramètre AES des SVM existants créés avec les anciennes versions de ONTAP ne changera pas automatiquement. Vous devez toujours mettre à jour la valeur de ce paramètre pour activer les AES sur ces SVM.

Configurer un tunnel d'authentification

Si vous avez déjà configuré un serveur SMB pour un SVM de données, vous pouvez utiliser le `security login domain-tunnel create` Commande permettant de configurer le SVM en tant que passerelle ou *tunnel*, pour l'accès AD au cluster.

Avant de commencer

- Un serveur SMB doit être configuré pour un SVM de données.
- Vous devez avoir activé un compte utilisateur AD domain pour accéder au SVM admin pour le cluster.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.

Depuis ONTAP 9.10.1, si vous disposez d'une passerelle SVM (tunnel du domaine) pour l'accès AD, vous pouvez utiliser Kerberos pour l'authentification admin si vous avez désactivé NTLM dans votre domaine AD. Dans les versions précédentes, Kerberos n'était pas pris en charge par l'authentification admin pour les passerelles SVM. Cette fonctionnalité est disponible par défaut ; aucune configuration n'est requise.

> L'authentification Kerberos a toujours été tentée en premier. En cas d'échec, l'authentification NTLM est alors tentée.

Étape

1. Configurer un SVM de données compatible SMB en tant que tunnel d'authentification pour l'accès au contrôleur de domaine AD au cluster :

   `security login domain-tunnel create -vserver` *`svm_name`*

   Pour connaître la syntaxe complète de la commande, reportez-vous au "feuille de calcul".

   > Le SVM doit être exécuté pour que l'utilisateur puisse être authentifié.

   La commande suivante configure le SVM de données SMB « engData » comme un tunnel d'authentification.

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

Créer un compte SVM Computer sur le domaine

Si vous n'avez pas configuré de serveur SMB pour un SVM de données, vous pouvez utiliser le `vserver active-directory create` Commande pour créer un compte ordinateur pour le SVM sur le domaine.

Description de la tâche

Une fois que vous avez saisi le `vserver active-directory create` Vous êtes invité à fournir les informations d'identification d'un compte utilisateur AD avec suffisamment de privilèges pour ajouter des ordinateurs à l'unité organisationnelle spécifiée dans le domaine. Le mot de passe du compte ne peut pas être

vide.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étape

1. Créer un compte ordinateur pour un SVM sur le domaine AD :

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

   Pour connaître la syntaxe complète de la commande, reportez-vous au "feuille de calcul".

   La commande suivante crée un compte ordinateur nommé « ADSERVER1 » sur le domaine « example.com`" pour SVM « engData ». Une fois la commande saisie, vous êtes invité à saisir les informations d'identification du compte utilisateur AD.

```
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:
```

Configuration de la présentation de l'accès aux serveurs LDAP ou NIS

Vous devez configurer l'accès des serveurs LDAP ou NIS à un SVM pour que les comptes LDAP ou NIS puissent accéder au SVM. La fonction de commutation vous permet d'utiliser LDAP ou NIS comme sources de service de noms alternatifs.

Configurez l'accès au serveur LDAP

Vous devez configurer l'accès des serveurs LDAP à une SVM avant que les comptes LDAP ne puissent accéder à la SVM. Vous pouvez utiliser le `vserver services name-service ldap client create` Commande permettant de créer une configuration client LDAP sur le SVM. Vous pouvez ensuite utiliser le `vserver services name-service ldap create` Commande permettant d'associer la configuration client LDAP à la SVM.

Description de la tâche

La plupart des serveurs LDAP peuvent utiliser les schémas par défaut fournis par ONTAP :

- MS-AD-BIS (schéma préféré pour la plupart des serveurs AD Windows 2012 et versions ultérieures)

- AD-IDMU (serveurs AD Windows 2008, Windows 2016 et versions ultérieures)
- AD-SFU (serveurs AD Windows 2003 et versions antérieures)
- RFC-2307 (SERVEURS LDAP UNIX)

Il est préférable d'utiliser les schémas par défaut à moins qu'il n'y ait une obligation de faire autrement. Si c'est le cas, vous pouvez créer votre propre schéma en copiant un schéma par défaut et en modifiant la copie. Pour plus d'informations, voir :

- "Configuration NFS"
- "Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP"

Avant de commencer

- Vous devez avoir installé un "Certificat numérique de serveur signé CA" Sur le SVM.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Créer une configuration client LDAP sur un SVM :

   `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`

   > Le démarrage de TLS est pris en charge uniquement pour l'accès aux SVM de données. Il n'est pas pris en charge pour l'accès aux SVM d'administration.

   Pour connaître la syntaxe complète de la commande, reportez-vous au "feuille de calcul".

   La commande suivante crée une configuration client LDAP nommée « corp » sur le SVM « engData ». Le client établit des liaisons anonymes vers les serveurs LDAP avec les adresses IP 172.160.0.100 et 172.16.0.101. Le client utilise le schéma RFC-2307 pour effectuer des requêtes LDAP. La communication entre le client et le serveur est cryptée à l'aide de Start TLS.

   ```
   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
   ```

   > À partir de ONTAP 9.2, le champ `-ldap-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur LDAP.

2. Associer la configuration client LDAP au SVM : `vserver services name-service ldap create -vserver` *`SVM_name`* `-client-config` *`client_configuration`* `-client-enabled true|false`

   Pour connaître la syntaxe complète de la commande, reportez-vous au "feuille de calcul".

   La commande suivante associe la configuration du client LDAP `corp` Avec la SVM `engData`, Et active le client LDAP sur la SVM.

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

> À partir de ONTAP 9.2, le `vserver services name-service ldap create` Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP n'est pas en mesure de contacter le serveur de noms.

3. Valider le statut des serveurs name en utilisant la commande vserver services name-service ldap check.

   La commande suivante valide les serveurs LDAP sur le SVM vs 0.

```
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".                                              |
```

   La commande name service check est disponible à partir de ONTAP 9.2.

Configurer l'accès au serveur NIS

Vous devez configurer l'accès du serveur NIS à un SVM pour que les comptes NIS puissent accéder au SVM. Vous pouvez utiliser le `vserver services name-service nis-domain create` Commande permettant de créer une configuration de domaine NIS sur un SVM

Description de la tâche

Vous pouvez créer plusieurs domaines NIS. Un seul domaine NIS peut être défini sur `active` à la fois.

Avant de commencer

- Tous les serveurs configurés doivent être disponibles et accessibles avant de configurer le domaine NIS sur le SVM.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étape

1. Créer une configuration de domaine NIS sur un SVM :

   `vserver services name-service nis-domain create -vserver` *`SVM_name`* `-domain client_configuration -active true|false -nis-servers` *`NIS_server_IPs`*

   Pour connaître la syntaxe complète de la commande, reportez-vous au "feuille de calcul".

   > À partir de ONTAP 9.2, le champ `-nis-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur NIS.

La commande suivante crée une configuration de domaine NIS sur SVM « engData ». Domaine NIS `nisdomain` Est actif lors de la création et communique avec un serveur NIS avec l'adresse IP 192.0.2.180.

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

Créer un commutateur de service de nom

La fonction de changement de service de noms vous permet d'utiliser LDAP ou NIS comme sources de service de noms alternatifs. Vous pouvez utiliser le `vserver services name-service ns-switch modify` commande permettant de spécifier l'ordre de recherche des sources de service de noms.

Avant de commencer

- Vous devez avoir configuré l'accès aux serveurs LDAP et NIS.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou un administrateur SVM.

Étape

1. Spécifiez l'ordre de recherche des sources de service de noms :

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

   Pour connaître la syntaxe complète de la commande, reportez-vous au "feuille de calcul".

   La commande suivante spécifie l'ordre de recherche des sources de service de noms LDAP et NIS pour la base de données « passwd » sur SVM « engData ».

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

Modifier un mot de passe administrateur

Vous devez modifier votre mot de passe initial immédiatement après la première connexion au système. Si vous êtes un administrateur de SVM, vous pouvez utiliser `security login password` commande permettant de modifier votre propre mot de passe. Si vous êtes administrateur de cluster, vous pouvez utiliser `security login password` pour modifier le mot de passe d'un administrateur.

Description de la tâche

Le nouveau mot de passe doit respecter les règles suivantes :

- Il ne peut pas contenir le nom d'utilisateur
- Elle doit comporter au moins huit caractères
- Il doit contenir au moins une lettre et un chiffre

- Il ne peut pas être le même que les six derniers mots de passe

> Vous pouvez utiliser le `security login role config modify` commande permettant de modifier les règles de mot de passe des comptes associés à un rôle donné. Pour plus d'informations, reportez-vous à la section "référence de commande".

Avant de commencer

- Vous devez être un administrateur de cluster ou de SVM pour modifier votre propre mot de passe.
- Vous devez être un administrateur de cluster pour modifier le mot de passe d'un autre administrateur.

Étape

1. Modifier un mot de passe d'administrateur : `security login password -vserver` *`svm_name`* `-username` *`user_name`*

   La commande suivante permet de modifier le mot de passe de l'administrateur `admin1` Pour la SVM`vs1.example.com`. Vous êtes invité à saisir le mot de passe actuel, puis à saisir de nouveau le nouveau mot de passe.

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

Verrouiller et déverrouiller un compte administrateur

Vous pouvez utiliser le `security login lock` commande permettant de verrouiller un compte d'administrateur, et le `security login unlock` commande pour déverrouiller le compte.

Avant de commencer

Pour effectuer ces tâches, vous devez être un administrateur de cluster.

Étapes

1. Verrouiller un compte administrateur :

   ```
   security login lock -vserver SVM_name -username user_name
   ```

   La commande suivante verrouille le compte administrateur `admin1` Pour la SVM `vs1.example.com`:

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

2. Déverrouiller un compte administrateur :

   ```
   security login unlock -vserver SVM_name -username user_name
   ```

La commande suivante déverrouille le compte administrateur `admin1` Pour la SVM `vs1.example.com`:

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

La gestion des tentatives de connexion a échoué

Les tentatives répétées de connexion échouées indiquent parfois qu'un intrus tente d'accéder au système de stockage. Vous pouvez prendre plusieurs mesures pour vous assurer qu'une intrusion n'a pas lieu.

Comment savoir que les tentatives de connexion ont échoué

Le système de gestion des événements (EMS) vous informe de l'échec des tentatives de connexion toutes les heures. Vous pouvez trouver un enregistrement des tentatives de connexion échouées dans le `audit.log` fichier.

Que faire en cas d'échec des tentatives de connexion répétées

À court terme, vous pouvez prendre plusieurs mesures pour éviter une intrusion :

- Exiger que les mots de passe soient composés d'un nombre minimum de caractères majuscules, de minuscules, de caractères spéciaux et/ou de chiffres
- Imposer un délai après une tentative de connexion échouée
- Limitez le nombre de tentatives de connexion ayant échoué autorisées et verrouillez les utilisateurs après le nombre spécifié de tentatives ayant échoué
- Expire et verrouille les comptes inactifs pendant un nombre de jours spécifié

Vous pouvez utiliser le `security login role config modify` pour effectuer ces tâches.

Sur le long terme, vous pouvez prendre les mesures suivantes :

- Utilisez le `security ssh modify` Commande pour limiter le nombre de tentatives de connexion ayant échoué pour tous les SVM nouvellement créés.
- Migrez les comptes d'algorithme MD5 existants vers l'algorithme SHA-512 plus sécurisé en exigeant des utilisateurs de modifier leurs mots de passe.

Appliquer SHA-2 sur les mots de passe du compte d'administrateur

Les comptes d'administrateur créés avant ONTAP 9.0 continuent d'utiliser des mots de passe MD5 après la mise à niveau, jusqu'à ce que les mots de passe soient changés manuellement. MD5 est moins sécurisé que SHA-2. Par conséquent, après la mise à niveau, vous devez inviter les utilisateurs de comptes MD5 à modifier leurs mots de passe pour utiliser la fonction de hachage SHA-512 par défaut.

Description de la tâche

La fonctionnalité de hachage du mot de passe vous permet d'effectuer les opérations suivantes :

- Affiche les comptes utilisateur correspondant à la fonction de hachage spécifiée.
- Expire les comptes qui utilisent une fonction de hachage spécifiée (par exemple MD5), forçant les utilisateurs à modifier leurs mots de passe lors de leur prochaine connexion.
- Verrouiller les comptes dont les mots de passe utilisent la fonction de hachage spécifiée.
- Pour revenir à une version antérieure à ONTAP 9, réinitialisez le mot de passe de l'administrateur du cluster afin qu'il soit compatible avec la fonction de hachage (MD5) prise en charge par la version précédente.

ONTAP n'accepte que les mots de passe SHA-2 pré-hachés à l'aide du SDK de gestion NetApp (`security-login-create` et `security-login-modify-password`).

Étapes

1. Migrez les comptes administrateur MD5 vers la fonction de hachage SHA-512 :
   a. Expire tous les comptes administrateur MD5 : `security login expire-password -vserver * -username * -hash-function md5`

      Cela oblige les utilisateurs de compte MD5 à changer leurs mots de passe lors de la prochaine connexion.

   b. Demandez aux utilisateurs de comptes MD5 de se connecter par le biais d'une console ou d'une session SSH.

      Le système détecte que les comptes ont expiré et invite les utilisateurs à modifier leur mot de passe. SHA-512 est utilisé par défaut pour les mots de passe modifiés.

2. Pour les comptes MD5 dont les utilisateurs ne se connectent pas pour modifier leurs mots de passe dans un délai donné, forcez la migration du compte :
   a. Verrouiller les comptes qui utilisent toujours la fonction de hachage MD5 (niveau de privilège avancé) : `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

      Après le nombre de jours spécifié par `-lock-after`, Les utilisateurs ne peuvent pas accéder à leurs comptes MD5.

   b. Déverrouillez les comptes lorsque les utilisateurs sont prêts à modifier leur mot de passe : `security login unlock -vserver` *`svm_name`* `-username` *`user_name`*
   c. Demandez aux utilisateurs de se connecter à leurs comptes via une console ou une session SSH et de modifier leur mot de passe lorsque le système les invite à le faire.

Diagnostiquer et corriger les problèmes d'accès aux fichiers

Étapes

1. Dans System Manager, sélectionnez **stockage > machines virtuelles de stockage**.
2. Sélectionnez la VM de stockage sur laquelle vous souhaitez effectuer un suivi.
3. Cliquez sur ⋮ **plus**.

4. Cliquez sur **Trace File Access**.
5. Indiquez le nom d’utilisateur et l’adresse IP du client, puis cliquez sur **Start Tracing**.

   Les résultats de la trace s’affichent dans un tableau. La colonne **motifs** indique la raison pour laquelle un fichier n’a pas pu être accédé.

6. Cliquez sur ⌄ dans la colonne de gauche du tableau de résultats pour afficher les autorisations d’accès aux fichiers.