Activez l'accès au compte local

ONTAP 9

NetApp
April 24, 2024

Sommaire

Activez l’accès au compte local

Activer la présentation de l’accès au compte local

Un compte local est un compte dans lequel les informations de compte, la clé publique ou le certificat de sécurité résident sur le système de stockage. Vous pouvez utiliser le `security login create` Commande pour permettre aux comptes locaux d’accéder à un admin ou un SVM de données.

Activer l’accès au compte par mot de passe

Vous pouvez utiliser le `security login create` Commande permettant aux comptes d’administrateur d’accéder à un admin ou un SVM de données avec un mot de passe. Après avoir saisi la commande, vous êtes invité à saisir le mot de passe.

Description de la tâche

Si vous n’êtes pas certain du rôle de contrôle d’accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser le `security login modify` commande permettant d’ajouter le rôle ultérieurement.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étape

1. Activer les comptes d’administrateur local pour accéder à un SVM via un mot de passe :

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

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

   La commande suivante active le compte d’administrateur du cluster `admin1` avec le prédéfini `backup` Rôle d’accès à la SVM d’admin`engCluster` à l’aide d’un mot de passe. Après avoir saisi la commande, vous êtes invité à saisir le mot de passe.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

Activez les comptes de clé publique SSH

Vous pouvez utiliser le `security login create` Commande permettant aux comptes d’administrateur d’accéder à un SVM de données ou admin avec une clé publique SSH.

Description de la tâche

- Vous devez associer la clé publique au compte avant que le compte puisse accéder à la SVM.

Association d'une clé publique à un compte d'utilisateur

Vous pouvez effectuer cette tâche avant ou après avoir activé l'accès au compte.

- Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser le `security login modify` commande permettant d'ajouter le rôle ultérieurement.

Si vous souhaitez activer le mode FIPS sur votre cluster, vous devez reconfigurer les comptes de clés publiques SSH existants sans les algorithmes de clé pris en charge avec un type de clé pris en charge. Les comptes doivent être reconfigurés avant l'activation de FIPS, sinon l'authentification de l'administrateur échouera.

Le tableau suivant indique les algorithmes de type de clé hôte pris en charge pour les connexions ONTAP SSH. Ces types de clés ne s'appliquent pas à la configuration de l'authentification publique SSH.

Version de ONTAP	Types de clés pris en charge en mode FIPS	Types de clés pris en charge en mode non FIPS
9.11.1 et versions ultérieures	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 et versions antérieures	ecdsa-sha2-nistp256 ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa

La prise en charge de l'algorithme de clé hôte ssh-ed25519 a été supprimée à partir de ONTAP 9.11.1.

Pour plus d'informations, voir "Configurez la sécurité réseau à l'aide de FIPS".

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étape

1. Activer les comptes d'administrateur local pour accéder à un SVM à l'aide d'une clé publique SSH :

   `security login create -vserver` *`SVM_name`* `-user-or-group-name user_or_group_name -application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

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

   La commande suivante active le compte d'administrateur du SVM `svmadmin1` avec le prédéfini `vsadmin-volume` Rôle d'accès à la SVM`engData1` Utilisation d'une clé publique SSH :

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

Une fois que vous avez terminé

Si vous n'avez pas associé de clé publique au compte administrateur, vous devez le faire avant que le compte puisse accéder à la SVM.

Association d'une clé publique à un compte d'utilisateur

Activez les comptes d'authentification multifacteur (MFA)

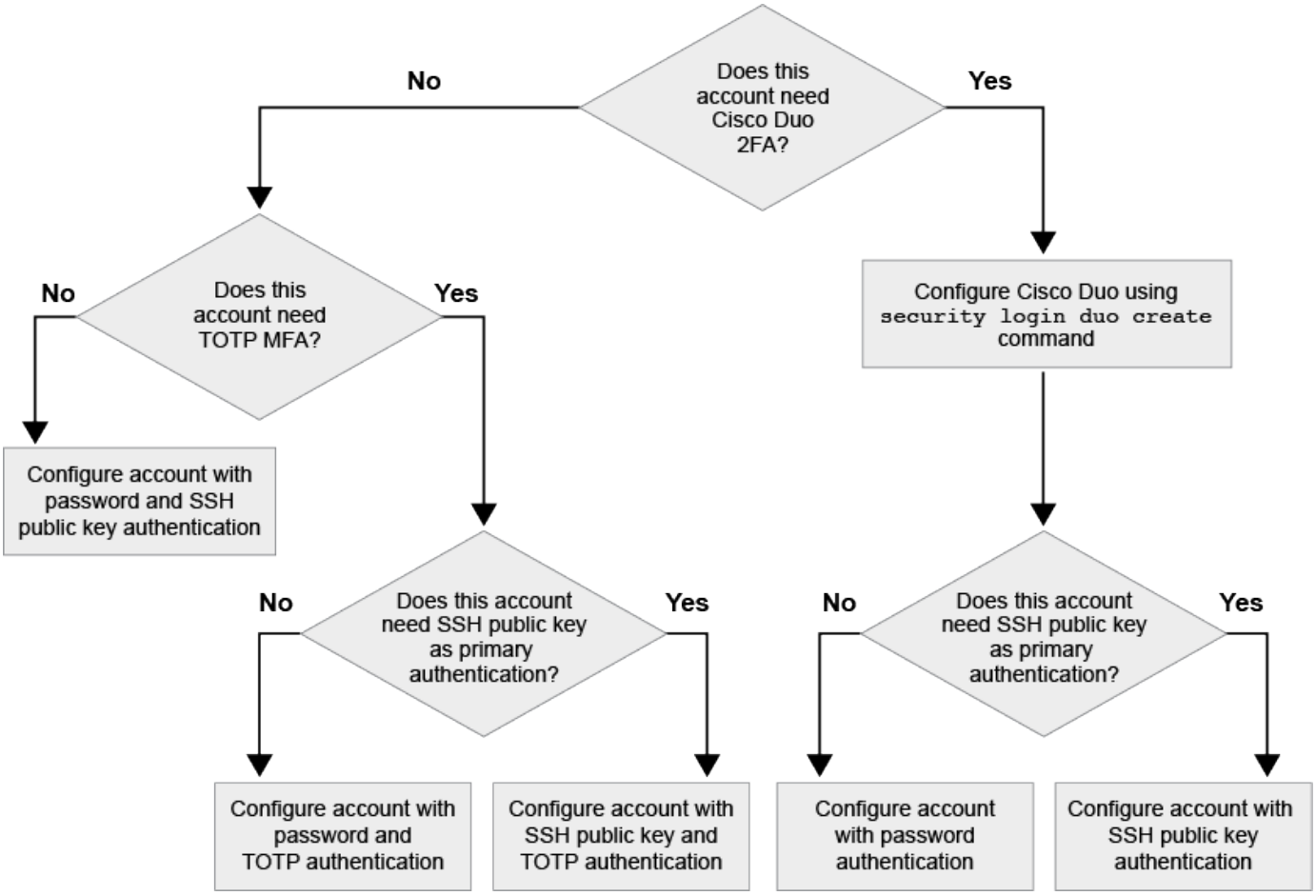
Présentation de l'authentification multifacteur

L'authentification multifacteur (MFA) vous permet d'améliorer la sécurité en exigeant que les utilisateurs fournissent deux méthodes d'authentification pour se connecter à un administrateur ou à une VM de stockage des données.

Selon votre version de ONTAP, vous pouvez utiliser une clé publique SSH, un mot de passe utilisateur et un mot de passe à usage unique (TOTP) pour l'authentification multifacteur. Lorsque vous activez et configurez Cisco Duo (ONTAP 9.14.1 et versions ultérieures), il sert de méthode d'authentification supplémentaire, en complément des méthodes existantes pour tous les utilisateurs.

Disponible à partir de…	Première méthode d'authentification	Deuxième méthode d'authentification
ONTAP 9.14.1	Clé publique SSH	TOTP
	Mot de passe utilisateur	TOTP
	Clé publique SSH	Duo Cisco
	Mot de passe utilisateur	Duo Cisco
ONTAP 9.13.1	Clé publique SSH	TOTP
	Mot de passe utilisateur	TOTP
ONTAP 9.3	Clé publique SSH	Mot de passe utilisateur

Si l'authentification multifacteur est configurée, l'administrateur du cluster doit d'abord activer le compte utilisateur local. Le compte doit alors être configuré par l'utilisateur local.



Activez l'authentification multifacteur

L'authentification multifacteur (MFA) vous permet d'améliorer la sécurité en exigeant que les utilisateurs fournissent deux méthodes d'authentification pour se connecter à un administrateur ou à un SVM de données.

Description de la tâche

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez utiliser le `security login modify` commande permettant d'ajouter le rôle ultérieurement.

  "Modification du rôle attribué à un administrateur"

- Si vous utilisez une clé publique pour l'authentification, vous devez associer la clé publique au compte avant que le compte puisse accéder à la SVM.

  "Associer une clé publique à un compte d'utilisateur"

  Vous pouvez effectuer cette tâche avant ou après avoir activé l'accès au compte.

- À partir de ONTAP 9.12.1, vous pouvez utiliser les périphériques d'authentification matérielle Yubikey pour le client SSH MFA en utilisant les normes d'authentification FIDO2 (Fast Identity Online) ou PIV (Personal Identity Verification).

Activez MFA avec la clé publique SSH et le mot de passe utilisateur

Depuis la version ONTAP 9.3, l'administrateur du cluster peut configurer des comptes utilisateurs locaux pour se connecter à MFA à l'aide d'une clé publique SSH et d'un mot de passe utilisateur.

1. Activer MFA sur le compte utilisateur local avec la clé publique SSH et le mot de passe utilisateur :

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_name> -application ssh -authentication-method <password|publickey>
   -role admin -second-authentication-method <password|publickey>
   ```

   La commande suivante nécessite un compte d'administrateur du SVM `admin2` avec le prédéfini `admin` Rôle de connexion à la SVM`engData1` Avec une clé publique SSH et un mot de passe utilisateur :

   ```
   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".
   ```

Activez MFA avec TOTP

À partir de ONTAP 9.13.1, vous pouvez améliorer la sécurité en exigeant des utilisateurs locaux qu'ils se connectent à un administrateur ou à un SVM de données à l'aide d'une clé publique SSH ou d'un mot de passe utilisateur et d'un mot de passe à usage unique (TOTP) basé sur le temps. Une fois le compte activé pour MFA avec TOTP, l'utilisateur local doit se connecter à "terminez la configuration".

TOTP est un algorithme informatique qui utilise l'heure actuelle pour générer un mot de passe à usage unique. Si TOTP est utilisé, il s'agit toujours de la deuxième forme d'authentification après la clé publique SSH ou le mot de passe utilisateur.

Avant de commencer

Vous devez être administrateur du stockage pour effectuer ces tâches.

Étapes

Vous pouvez configurer MFA avec un mot de passe utilisateur ou une clé publique SSH comme première méthode d'authentification et TOTP comme deuxième méthode d'authentification.

Activer MFA avec mot de passe utilisateur et TOTP

1. Activez un compte utilisateur pour l'authentification multifacteur avec un mot de passe utilisateur et un TOTP.

   Pour les nouveaux comptes utilisateur

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Pour les comptes utilisateur existants

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Vérifier que MFA avec TOTP est activé :

   ```
   security login show
   ```

Activez MFA avec clé publique SSH et TOTP

1. Activez un compte utilisateur pour l'authentification multifacteur avec une clé publique SSH et un TOTP.

   Pour les nouveaux comptes utilisateur

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Pour les comptes utilisateur existants

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Vérifier que MFA avec TOTP est activé :

```
security login show
```

Une fois que vous avez terminé

- Si vous n'avez pas associé de clé publique au compte administrateur, vous devez le faire avant que le compte puisse accéder à la SVM.

  "Association d'une clé publique à un compte d'utilisateur"

- L'utilisateur local doit se connecter pour terminer la configuration MFA avec TOTP.

  "Configurer le compte utilisateur local pour MFA avec TOTP"

Informations associées

En savoir plus sur "Authentification multifactorielle dans ONTAP 9 (TR-4647)".

Configurer le compte utilisateur local pour MFA avec TOTP

À partir de la ONTAP 9.13.1, les comptes utilisateur peuvent être configurés avec l'authentification multifacteur (MFA) avec un mot de passe à usage unique (TOTP).

Avant de commencer

- L'administrateur du stockage doit "Activez MFA avec TOTP" comme deuxième méthode d'authentification pour votre compte utilisateur.
- La méthode d'authentification de votre compte utilisateur principal doit être un mot de passe utilisateur ou une clé SSH publique.
- Vous devez configurer votre application TOTP pour qu'elle fonctionne avec votre smartphone et créer votre clé secrète TOTP.

  TOTP est pris en charge par diverses applications d'authentificateur telles que Google Authenticator.

Étapes

1. Connectez-vous à votre compte utilisateur avec votre méthode d'authentification actuelle.

   Votre méthode d'authentification actuelle doit être un mot de passe utilisateur ou une clé publique SSH.

2. Créez la configuration TOTP sur votre compte :

   ```
   security login totp create -vserver "<svm_name>" -username
   "<account_username >"
   ```

3. Vérifiez que la configuration TOTP est activée sur votre compte :

   ```
   security login totp show -vserver "<svm_name>" -username
   "<account_username>"
   ```

Réinitialiser la clé secrète TOTP

Pour protéger la sécurité de votre compte, si votre clé secrète TOTP est compromise ou perdue, vous devez la désactiver et en créer une nouvelle.

Réinitialisez le TOTP si votre clé est compromise

Si votre clé secrète TOTP est compromise, mais que vous y avez toujours accès, vous pouvez supprimer la clé compromise et en créer une nouvelle.

1. Connectez-vous à votre compte utilisateur avec votre mot de passe utilisateur ou votre clé publique SSH et votre clé secrète TOTP compromise.
2. Supprimez la clé secrète TOTP compromise :

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. Créez une nouvelle clé secrète TOTP :

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. Vérifiez que la configuration TOTP est activée sur votre compte :

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Réinitialisez le TOTP en cas de perte de votre clé

Si votre clé secrète TOTP est perdue, contactez votre administrateur de stockage à l'adresse "faites désactiver la clé". Une fois votre clé désactivée, vous pouvez utiliser votre première méthode d'authentification pour vous connecter et configurer un nouveau TOTP.

Avant de commencer

La clé secrète TOTP doit être désactivée par un administrateur de stockage. Si vous ne possédez pas de compte d'administrateur de stockage, contactez votre administrateur de stockage pour que la clé soit désactivée.

Étapes

1. Une fois le secret TOTP désactivé par un administrateur de stockage, utilisez votre méthode d'authentification principale pour vous connecter à votre compte local.
2. Créez une nouvelle clé secrète TOTP :

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. Vérifiez que la configuration TOTP est activée sur votre compte :

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Désactiver la clé secrète TOTP pour le compte local

Si la clé secrète TOTP (Time-based password) d'un utilisateur local est perdue, la clé perdue doit être désactivée par un administrateur de stockage avant que l'utilisateur puisse créer une nouvelle clé secrète TOTP.

Description de la tâche

Cette tâche ne peut être effectuée qu'à partir d'un compte d'administrateur de cluster.

Étape

1. Désactiver la clé secrète TOTP :

```
security login totp delete -vserver "<svm_name>" -username
"<account_username>"
```

Activez les comptes de certificat SSL

Vous pouvez utiliser le `security login create` Commande pour permettre aux comptes d'administrateur d'accéder à un SVM d'administration ou de données avec un certificat SSL.

Description de la tâche

- Vous devez installer un certificat numérique de serveur signé par une autorité de certification pour que le compte puisse accéder à la SVM.

  Génération et installation d'un certificat de serveur signé par une autorité de certification

  Vous pouvez effectuer cette tâche avant ou après avoir activé l'accès au compte.

- Si vous n'êtes pas certain du rôle de contrôle d'accès que vous souhaitez attribuer au compte de connexion, vous pouvez ajouter le rôle ultérieurement avec le `security login modify` commande.

  Modification du rôle attribué à un administrateur

Pour les comptes d'administrateur de cluster, l'authentification par certificat est prise en charge avec `http`, `ontapi`, et `rest` en termes de latence. Pour les comptes d'administrateur SVM, l'authentification par certificat est prise en charge uniquement avec `ontapi` et `rest` en termes de latence.

Étape

1. Activer les comptes d'administrateur local pour accéder à un SVM à l'aide d'un certificat SSL :

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous au "Pages de manuel ONTAP par version".

   La commande suivante active le compte d'administrateur du SVM `svmadmin2` avec la valeur par défaut `vsadmin` Rôle d'accès à la SVM`engData2` Utilisation d'un certificat numérique SSL.

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

Une fois que vous avez terminé

Si vous n'avez pas installé de certificat numérique serveur signé par une autorité de certification, vous devez le faire avant que le compte puisse accéder à la SVM.

Génération et installation d'un certificat de serveur signé par une autorité de certification