Activez les comptes d'authentification multifacteur (MFA)

ONTAP 9

NetApp
April 16, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/authentication/mfa-overview.html on April 16, 2024. Always check docs.netapp.com for the latest.

Sommaire

Activez les comptes d’authentification multifacteur (MFA) 1
Présentation de l’authentification multifacteur 1
Activez l’authentification multifacteur 2
Configurer le compte utilisateur local pour MFA avec TOTP 5
Réinitialiser la clé secrète TOTP 6
Désactiver la clé secrète TOTP pour le compte local 7

Activez les comptes d’authentification multifacteur (MFA)

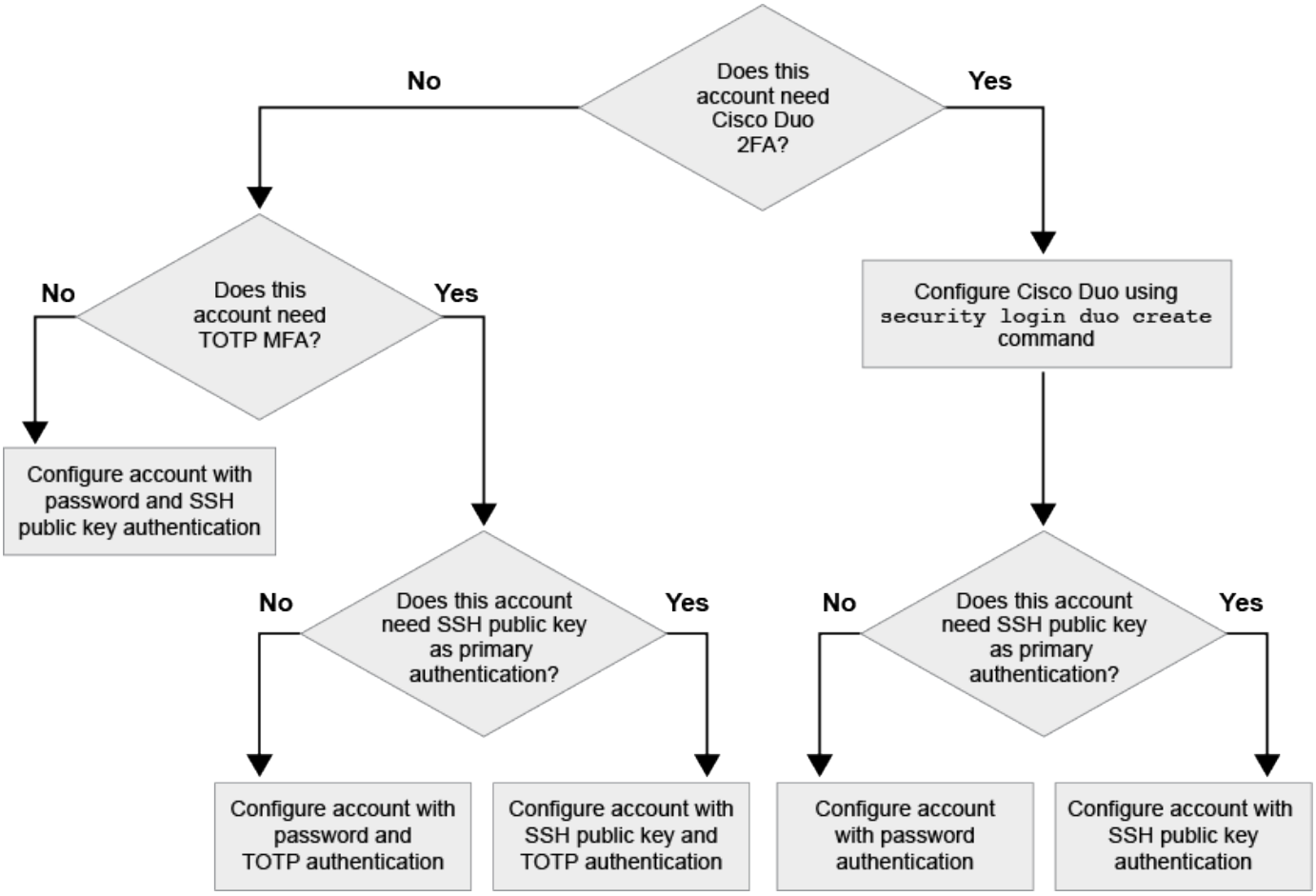
Présentation de l’authentification multifacteur

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>"
```

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.