Habilitar contas de autenticação multifator (MFA)

ONTAP 9

NetApp
January 17, 2025

Índice

Habilitar contas de autenticação multifator (MFA)

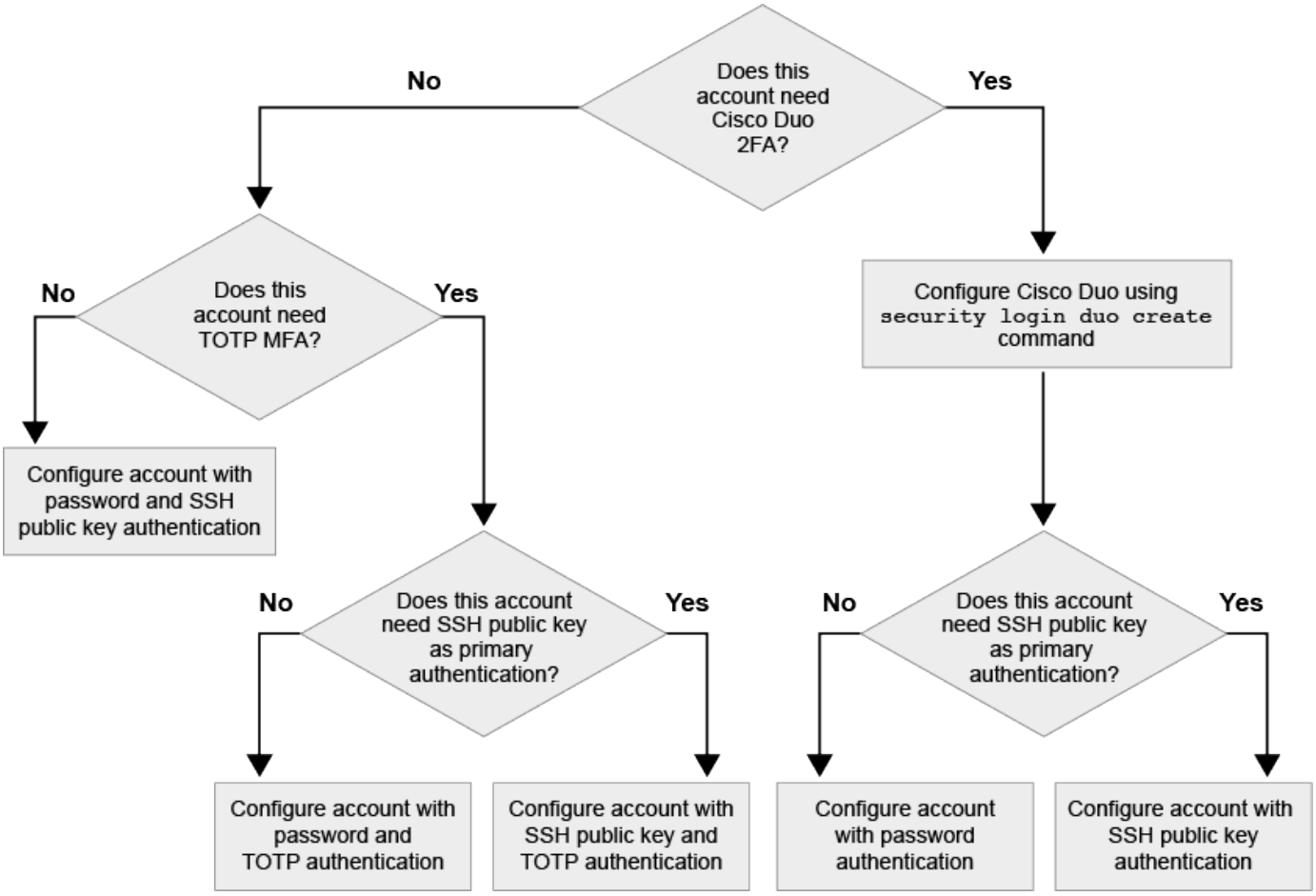
Visão geral da autenticação multifator

A autenticação multifator (MFA) permite aprimorar a segurança, exigindo que os usuários forneçam dois métodos de autenticação para fazer login em um administrador ou uma VM de storage de dados.

Dependendo da sua versão do ONTAP, você pode usar uma combinação de uma chave pública SSH, uma senha de usuário e uma senha única baseada em tempo (TOTP) para autenticação multifator. Quando você ativa e configura o Cisco Duo (ONTAP 9.14,1 e posterior), ele serve como um método de autenticação adicional, complementando os métodos existentes para todos os usuários.

Disponível a partir de…	Primeiro método de autenticação	Segundo método de autenticação
ONTAP 9.14,1	Chave pública SSH	TOTP
	Palavra-passe do utilizador	TOTP
	Chave pública SSH	Cisco Duo
	Palavra-passe do utilizador	Cisco Duo
ONTAP 9.13,1	Chave pública SSH	TOTP
	Palavra-passe do utilizador	TOTP
ONTAP 9,3	Chave pública SSH	Palavra-passe do utilizador

Se o MFA estiver configurado, o administrador do cluster deve primeiro habilitar a conta de usuário local e, em seguida, a conta deve ser configurada pelo usuário local.



Ativar a autenticação multifator

Com a autenticação multifator (MFA), você aumenta a segurança, exigindo que os usuários forneçam dois métodos de autenticação para fazer login em um administrador ou SVM de dados.

Sobre esta tarefa

- Você deve ser um administrador de cluster para executar esta tarefa.
- Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, use o `security login modify` comando para adicionar a função mais tarde.

  "Modificação da função atribuída a um administrador"

- Se você estiver usando uma chave pública para autenticação, associe a chave pública à conta antes que a conta possa acessar o SVM.

  "Associar uma chave pública a uma conta de utilizador"

  Pode executar esta tarefa antes ou depois de ativar o acesso à conta.

- A partir do ONTAP 9.12,1, você pode usar dispositivos de autenticação de hardware Yubikey para o MFA do cliente SSH usando os padrões de autenticação FIDO2 (identidade rápida on-line) ou Verificação de identidade pessoal (PIV).

Habilite o MFA com chave pública SSH e senha do usuário

A partir do ONTAP 9.3, um administrador de cluster pode configurar contas de usuário locais para fazer login com MFA usando uma chave pública SSH e uma senha de usuário.

1. Habilite o MFA em conta de usuário local com chave pública SSH e senha de usuário:

```
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>
```

O comando a seguir exige que a conta de administrador SVM `admin2` com a função predefinida `admin` efetue login no SVM`engData1` com uma chave pública SSH e uma senha de usuário:

```
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".
```

Habilite MFA com TOTP

A partir do ONTAP 9.13,1, você pode melhorar a segurança, exigindo que os usuários locais façam login em um administrador ou SVM de dados com uma chave pública SSH ou senha de usuário e uma senha única baseada em tempo (TOTP). Depois que a conta estiver habilitada para MFA com TOTP, o usuário local deverá fazer login "conclua a configuração"no .

TOTP é um algoritmo de computador que usa a hora atual para gerar uma senha única. Se o TOTP for usado, é sempre a segunda forma de autenticação após a chave pública SSH ou a senha do usuário.

Antes de começar

Você deve ser um administrador de armazenamento para executar essas tarefas.

Passos

Você pode configurar o MFA para com uma senha de usuário ou uma chave pública SSH como o primeiro método de autenticação e o TOTP como o segundo método de autenticação.

Habilite MFA com senha de usuário e TOTP

1. Ative uma conta de usuário para autenticação multifator com uma senha de usuário e TOTP.

   Para novas contas de usuário

   ```
   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>
   ```

   Para contas de usuário existentes

   ```
   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. Verifique se o MFA com TOTP está ativado:

   ```
   security login show
   ```

Habilite MFA com chave pública SSH e TOTP

1. Ative uma conta de usuário para autenticação multifator com uma chave pública SSH e TOTP.

   Para novas contas de usuário

   ```
   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>
   ```

   Para contas de usuário existentes

   ```
   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. Verifique se o MFA com TOTP está ativado:

```
security login show
```

Depois de terminar

- Se você não tiver associado uma chave pública à conta de administrador, deverá fazê-lo antes que a conta possa acessar o SVM.

  "Associar uma chave pública a uma conta de utilizador"

- O usuário local deve fazer login para concluir a configuração de MFA com TOTP.

  "Configurar conta de usuário local para MFA com TOTP"

Informações relacionadas

Saiba mais "Autenticação multifator no ONTAP 9 (TR-4647)"sobre o .

Configurar conta de usuário local para MFA com TOTP

A partir do ONTAP 9.13,1, as contas de usuário podem ser configuradas com autenticação multifator (MFA) usando uma senha única baseada em tempo (TOTP).

Antes de começar

- O administrador de armazenamento tem de "Habilite MFA com TOTP" ser um segundo método de autenticação para a sua conta de utilizador.
- Seu método de autenticação de conta de usuário principal deve ser uma senha de usuário ou uma chave SSH pública.
- Você deve configurar seu aplicativo TOTP para trabalhar com seu smartphone e criar sua chave secreta TOTP.

  Microsoft Authenticator, Google Authenticator, Authy e qualquer outro autenticador compatível com TOTP são suportados.

Passos

1. Inicie sessão na sua conta de utilizador com o método de autenticação atual.

   Seu método de autenticação atual deve ser uma senha de usuário ou uma chave pública SSH.

2. Crie a configuração TOTP na sua conta:

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

3. Verifique se a configuração TOTP está ativada na sua conta:

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

Repor chave secreta TOTP

Para proteger a segurança da sua conta, se a sua chave secreta TOTP estiver comprometida ou perdida, você deve desativá-la e criar uma nova.

Reponha o TOTP se a sua chave estiver comprometida

Se sua chave secreta TOTP estiver comprometida, mas você ainda tiver acesso a ela, poderá remover a chave comprometida e criar uma nova.

1. Faça login na sua conta de usuário com sua senha de usuário ou chave pública SSH e sua chave secreta TOTP comprometida.
2. Remova a chave secreta TOTP comprometida:

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

3. Crie uma nova chave secreta TOTP:

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

4. Verifique se a configuração TOTP está ativada na sua conta:

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

Reinicie o TOTP se a sua chave for perdida

Se a chave secreta TOTP for perdida, entre em Contato com o administrador de armazenamento para "tenha a chave desativada". Depois que sua chave for desativada, você poderá usar seu primeiro método de autenticação para fazer login e configurar um novo TOTP.

Antes de começar

A chave secreta TOTP deve ser desativada por um administrador de armazenamento. Se não tiver uma conta de administrador de armazenamento, contacte o administrador de armazenamento para desativar a chave.

Passos

1. Depois que o segredo TOTP for desativado por um administrador de armazenamento, use seu método de autenticação principal para fazer login na sua conta local.

2. Crie uma nova chave secreta TOTP:

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

3. Verifique se a configuração TOTP está ativada na sua conta:

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

Desative a chave secreta TOTP para a conta local

Se a chave secreta de uma senha de tempo único (TOTP) de um usuário local for perdida, a chave perdida deve ser desativada por um administrador de armazenamento antes que o usuário possa criar uma nova chave secreta TOTP.

Sobre esta tarefa

Esta tarefa só pode ser executada a partir de uma conta de administrador de cluster.

Passo

1. Desative a chave secreta TOTP:

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

Informações sobre direitos autorais

Informações sobre marcas comerciais