启用多因素身份验证(MFA)帐户

ONTAP 9

NetApp
April 24, 2024

目录

启用多因素身份验证(MFA)帐户

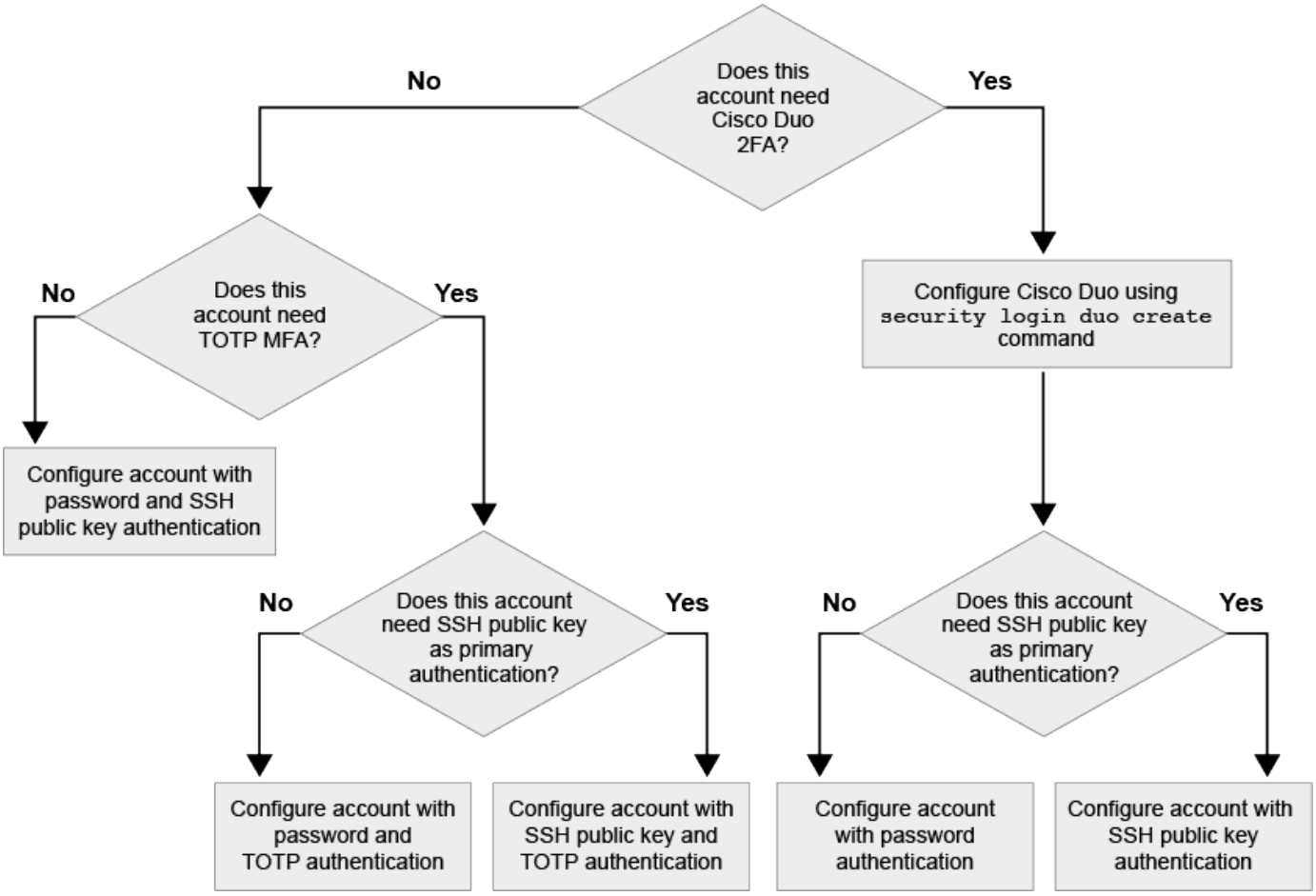
多因素身份验证概述

通过多因素身份验证(MFA)、您可以要求用户提供两种身份验证方法来登录到管理员或数据Storage VM、从而增强安全性。

根据您的ONTAP版本、您可以组合使用SSH公共密钥、用户密码和基于时间的一次性密码(TOTP)进行多因素身份验证。启用并配置Cisco Duo (ONTAP 9.14.1及更高版本)时、它可作为一种附加的身份验证方法、对所有用户的现有方法进行补充。

可用开头为...	第一种身份验证方法	第二种身份验证方法
ONTAP 9.14.1	SSH 公有密钥	TOTP
	用户密码	TOTP
	SSH 公有密钥	Cisco Duo
	User password	Cisco Duo
ONTAP 9.13.1	SSH 公有密钥	TOTP
	User password	TOTP
ONTAP 9.3	SSH 公有密钥	User password

如果配置了MFA、则集群管理员必须先启用本地用户帐户、然后该帐户必须由本地用户配置。



启用多因素身份验证

通过多因素身份验证(MFA)、您可以要求用户提供两种身份验证方法来登录到管理员或数据SVM、从而增强安全性。

关于此任务

- 您必须是集群管理员才能执行此任务。
- 如果您不确定要分配给登录帐户的访问控制角色、可以使用 `security login modify` 命令以稍后添加此角色。

  "修改分配给管理员的角色"

- 如果您使用公共密钥进行身份验证、则必须先将此公共密钥与此帐户关联、然后此帐户才能访问SVM。

  "将公有密钥与用户帐户关联"

  您可以在启用帐户访问之前或之后执行此任务。

- 从ONTAP 9.12.1开始、您可以使用FID02 (快速身份联机)或个人身份验证(PIV)身份验证标准对SSH客户端MFA使用优键硬件身份验证设备。

使用SSH公共密钥和用户密码启用MFA

从ONTAP 9.3开始、集群管理员可以设置本地用户帐户、以便使用SSH公共密钥和用户密码登录MFA。

1. 使用SSH公共密钥和用户密码在本地用户帐户上启用MFA：

```
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>
```

以下命令需要SVM管理员帐户 `admin2` 和预定义的 `admin` 用于登录到SVM的角色`engData1` 使用SSH公共密钥和用户密码：

```
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".
```

使用TOTP启用MFA

从ONTAP 9.13.1开始、您可以通过要求本地用户同时使用SSH公共密钥或用户密码以及基于时间的一次性密码(TOTP)登录到管理员或数据SVM来增强安全性。使用TOTP为帐户启用MFA后、本地用户必须登录到 "完成配置"。

TOTP是一种计算机算法、使用当前时间生成一次性密码。 如果使用TOTP、则它始终是继SSH公共密钥或用户密码之后的第二种身份验证形式。

开始之前

您必须是存储管理员才能执行这些任务。

步骤

您可以将MFA设置为、并将用户密码或SSH公共密钥作为第一种身份验证方法、将TOTP作为第二种身份验证方法。

使用用户密码和**TOTP**启用**MFA**

1. 使用用户密码和TOTP为用户帐户启用多因素身份验证。

   新用户帐户

   ```
   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>
   ```

   用于现有用户帐户

   ```
   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. 验证是否已启用具有TOTP的MFA：

   ```
   security login show
   ```

使用**SSH**公共密钥和**TOTP**启用**MFA**

1. 使用SSH公共密钥和TOTP为用户帐户启用多因素身份验证。

   新用户帐户

   ```
   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>
   ```

   用于现有用户帐户

   ```
   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. 验证是否已启用具有TOTP的MFA：

```
security login show
```

完成后

- 如果您尚未将公有密钥与管理员帐户关联，则必须先将其关联，然后该帐户才能访问 SVM 。

  "将公有密钥与用户帐户关联"

- 本地用户必须登录才能使用TOTP完成MFA配置。

  "使用TOTP配置MFA的本地用户帐户"

相关信息

了解更多信息 "ONTAP 9中的多因素身份验证(TR-4647)"。

使用TOTP配置MFA的本地用户帐户

从ONTAP 9.13.1开始、可以使用基于时间的一次性密码(TOTP)为用户帐户配置多因素身份验证(MFA)。

开始之前

- 存储管理员必须执行此操作 "使用TOTP启用MFA" 作为用户帐户的第二种身份验证方法。
- 您的主用户帐户身份验证方法应为用户密码或公共SSH密钥。
- 您必须将TOTP应用程序配置为与智能手机配合使用、并创建TOTP机密密钥。

  各种身份验证程序应用程序(如Google身份验证程序)均支持TOTP。

步骤

1. 使用当前身份验证方法登录到您的用户帐户。

   您当前的身份验证方法应为用户密码或SSH公共密钥。

2. 在您的帐户上创建TOTP配置：

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

3. 验证是否已在您的帐户上启用TOTP配置：

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

重置TOTP机密密钥

为了保护您的帐户安全、如果您的TOTP机密密钥泄露或丢失、您应禁用它并创建一个新密钥。

如果您的密钥已损坏、请重置TOTP

如果您的TOTP机密密钥已泄露、但您仍可访问该密钥、则可以删除此泄露密钥并创建一个新密钥。

1. 使用您的用户密码或SSH公共密钥以及泄露的TOTP机密密钥登录到您的用户帐户。
2. 删除已泄露的TOTP机密密钥：

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

3. 创建新的TOTP密钥：

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

4. 验证是否已在您的帐户上启用TOTP配置：

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

如果密钥丢失、请重置TOTP

如果您的TOTP机密密钥丢失、请与您的存储管理员联系以获取 "禁用密钥"。禁用密钥后、您可以使用第一种身份验证方法登录并配置新的TOTP。

开始之前

存储管理员必须禁用TOTP机密密钥。 如果您没有存储管理员帐户、请与存储管理员联系以禁用此密钥。

步骤

1. 存储管理员禁用TOTP密钥后、使用主身份验证方法登录到本地帐户。
2. 创建新的TOTP密钥：

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

3. 验证是否已在您的帐户上启用TOTP配置：

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

禁用本地帐户的TOTP机密密钥

如果本地用户丢失了基于时间的一次性密码(TOTP)密钥、则存储管理员必须先禁用丢失的密钥、然后用户才能创建新的TOTP密钥。

关于此任务

只能使用集群管理员帐户执行此任务。

步骤

1. 禁用TOTP密钥：

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