



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 1
 - 多因素身份验证概述 1
 - 启用多因素身份验证 2
 - 使用TOTP配置MFA的本地用户帐户 5
 - 重置TOTP机密密钥 6
 - 禁用本地帐户的TOTP机密密钥 7

启用多因素身份验证(MFA)帐户

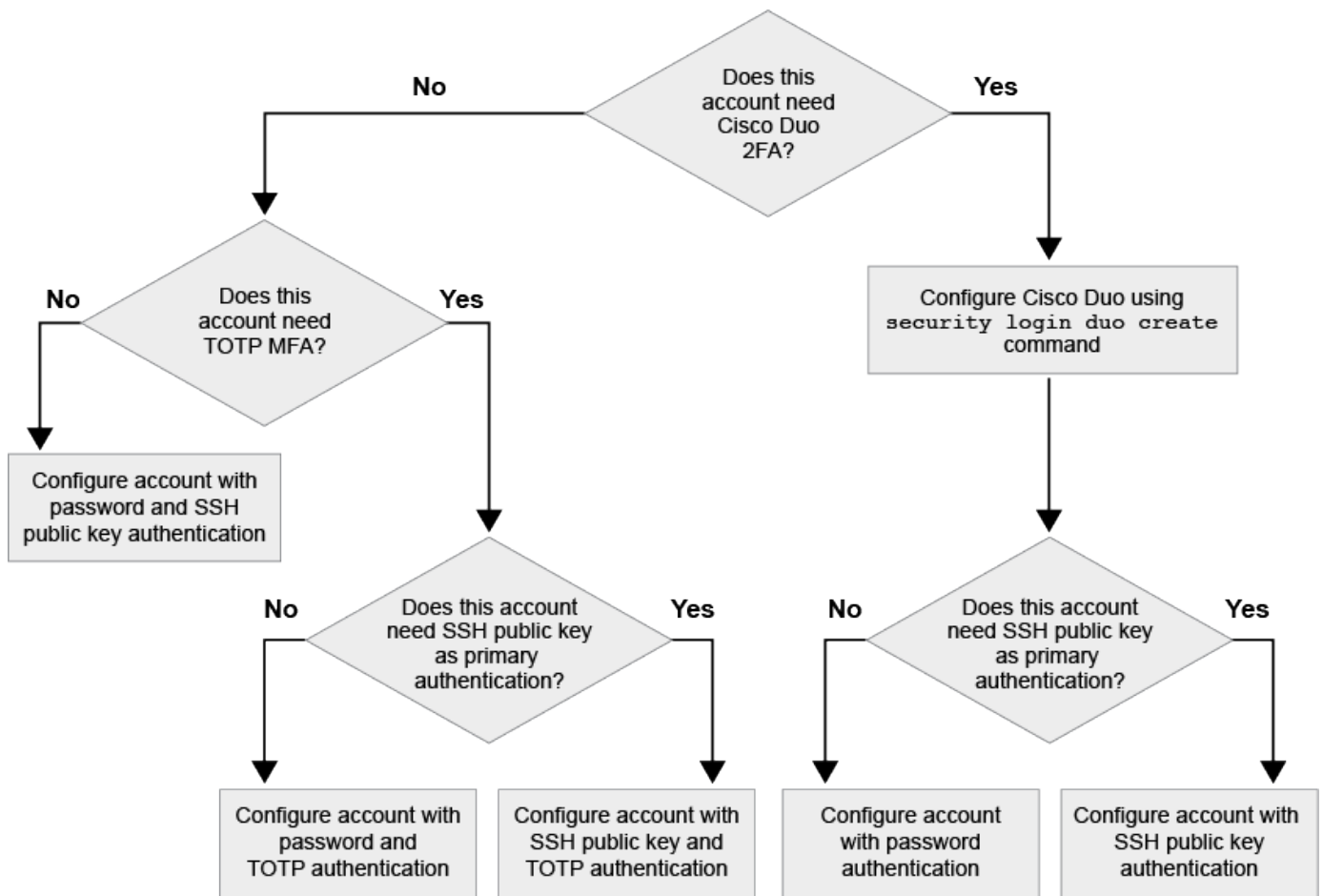
多因素身份验证概述

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FIDO2 (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>"
```

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。