



Ative o acesso à conta local

ONTAP 9

NetApp
January 17, 2025

Índice

- Ative o acesso à conta local 1
 - Ative a visão geral do acesso à conta local 1
 - Ativar acesso à conta de palavra-passe 1
 - Ativar contas de chave pública SSH 1
 - Habilitar contas de autenticação multifator (MFA) 3
 - Ativar contas de certificado SSL 9

Ative o acesso à conta local

Ative a visão geral do acesso à conta local

Uma conta local é aquela em que as informações da conta, a chave pública ou o certificado de segurança residem no sistema de armazenamento. Você pode usar o `security login create` comando para habilitar contas locais para acessar um administrador ou um SVM de dados.

Ativar acesso à conta de palavra-passe

Você pode usar o `security login create` comando para habilitar contas de administrador para acessar um administrador ou data SVM com uma senha. Você será solicitado a digitar a senha depois de digitar o comando.

Sobre 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.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Ative as contas de administrador locais para acessar um SVM usando uma senha:

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

Para obter a sintaxe de comando completa, consulte ["folha de trabalho"](#).

O comando a seguir habilita a conta de administrador de cluster `admin1` com a função predefinida `backup` para acessar o SVM de `administradorengCluster` usando uma senha. Você será solicitado a digitar a senha depois de digitar o comando.

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

Ativar contas de chave pública SSH

Você pode usar o `security login create` comando para habilitar contas de administrador para acessar um administrador ou SVM de dados com uma chave pública SSH.

Sobre esta tarefa

- Você deve associar 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.

- 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.

Se quiser ativar o modo FIPS no cluster, as contas de chave pública SSH existentes sem os algoritmos de chave suportados devem ser reconfiguradas com um tipo de chave suportado. As contas devem ser reconfiguradas antes de ativar o FIPS ou a autenticação do administrador falhar.

A tabela a seguir indica algoritmos de tipo de chave de host compatíveis com conexões SSH ONTAP. Esses tipos de chave não se aplicam à configuração da autenticação pública SSH.

Lançamento do ONTAP	Tipos de chave compatíveis no modo FIPS	Tipos de chave compatíveis no modo não FIPS
9.11.1 e mais tarde	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 e rsa-sha2-512 e rsa-sha2-256 e ssh-ed25519 e ssh-dss e ssh-rsa
9.10.1 e anteriores	ecdsa-sha2-nistp256 e ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss e ssh-rsa



O suporte para o algoritmo de chave de host ssh-ed25519 é removido a partir de ONTAP 9.11,1.

Para obter mais informações, "[Configurar a segurança da rede usando o FIPS](#)" consulte .

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Habilite as contas de administrador local para acessar um SVM usando uma chave pública SSH:

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

Para obter a sintaxe de comando completa, consulte "[folha de trabalho](#)".

O comando a seguir permite que a conta de administrador SVM `svmadmin1` com a função predefinida `vsadmin-volume` acesse o `SVMengData1` usando uma chave pública SSH:

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

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](#)

Habilitar contas de autenticação multifator (MFA)

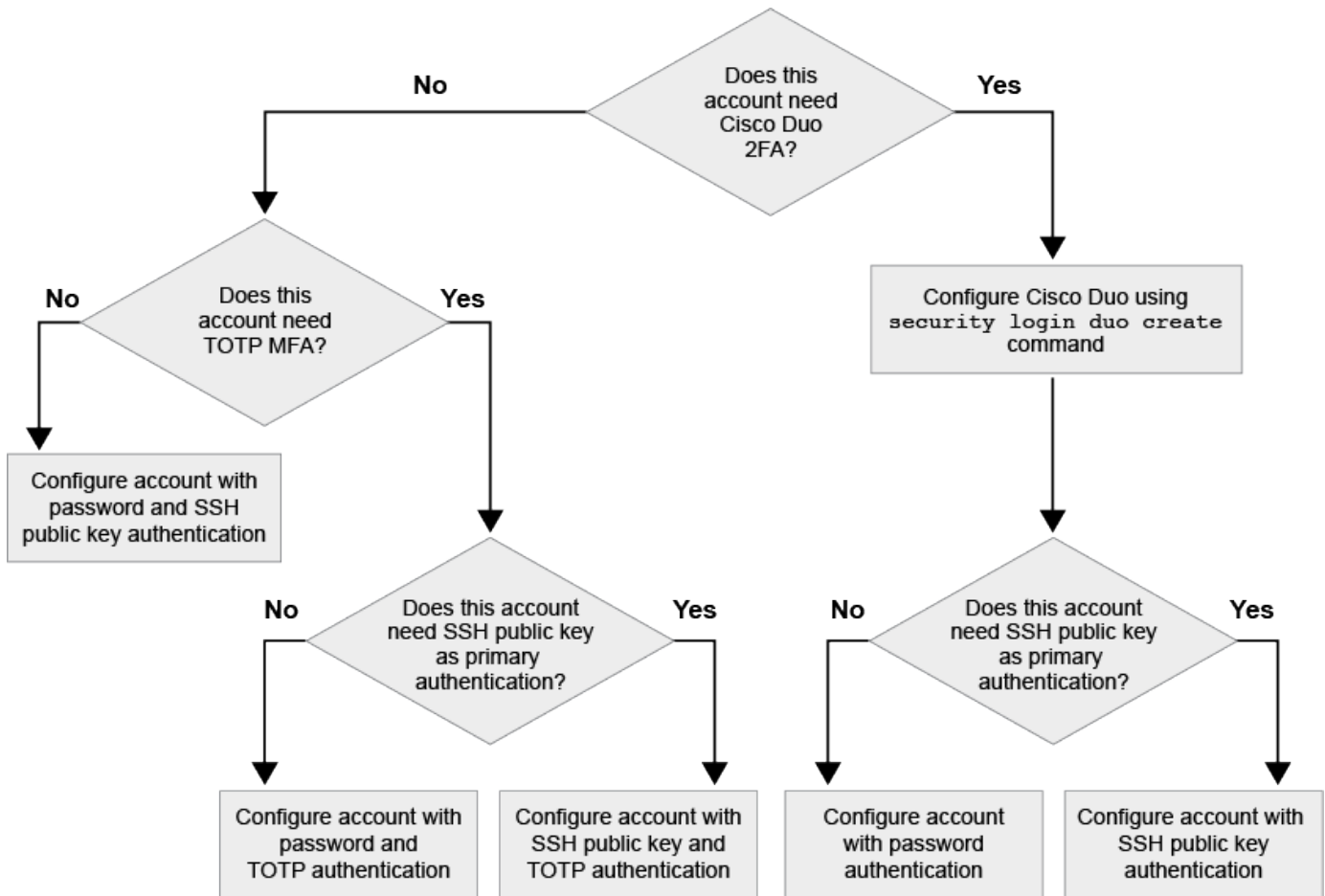
Visão geral da autenticação multifator

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>"
```

Ativar contas de certificado SSL

Você pode usar o `security login create` comando para habilitar contas de administrador para acessar um administrador ou data SVM com um certificado SSL.

Sobre esta tarefa

- Você deve instalar um certificado digital de servidor assinado pela CA antes que a conta possa acessar o SVM.

[Gerando e instalando um certificado de servidor assinado pela CA](#)

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

- Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, poderá adicionar a função mais tarde com o `security login modify` comando.

[Modificação da função atribuída a um administrador](#)



Para contas de administrador de cluster, a autenticação de certificado é suportada com os `http` aplicativos, `ontapi` e `rest`. Para contas de administrador da SVM, a autenticação de certificado é compatível apenas com `ontapi` os aplicativos e `rest`.

Passo

1. Ative as contas de administrador local para acessar um SVM usando um certificado SSL:

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

Para obter a sintaxe de comando completa, consulte ["ONTAP man pages por release"](#).

O comando a seguir permite que a conta de administrador SVM `svmadmin2` com a função padrão `vsadmin` acesse o `SVMengData2` usando um certificado digital SSL.

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

Depois de terminar

Se você não tiver instalado um certificado digital de servidor assinado pela CA, deverá fazê-lo antes que a conta possa acessar o SVM.

[Gerando e instalando um certificado de servidor assinado pela CA](#)

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.