



Gerenciar contas de administrador

ONTAP 9

NetApp
January 17, 2025

Índice

Gerenciar contas de administrador	1
Visão geral das contas de administrador	1
Associar uma chave pública a uma conta de administrador	1
Gerenciar chaves públicas SSH e certificados X,509 para uma conta de administrador	2
Configure o Cisco Duo 2FA para logins SSH com o ONTAP	4
Gere e instale uma visão geral do certificado de servidor assinado pela CA	9
Gerencie certificados com o System Manager	13
Configure a visão geral do acesso do controlador de domínio do active Directory	18
Configure a visão geral do acesso ao servidor LDAP ou NIS	20
Altere uma senha de administrador no ONTAP	23
Bloquear e desbloquear uma conta de administrador	24
Gerir tentativas de início de sessão falhadas	24
Aplicar SHA-2 em senhas de conta de administrador	25
Diagnosticar e corrigir problemas de acesso a arquivos	26

Gerenciar contas de administrador

Visão geral das contas de administrador

Dependendo de como você ativou o acesso à conta, talvez seja necessário associar uma chave pública a uma conta local, instalar um certificado digital de servidor assinado pela CA ou configurar o acesso AD, LDAP ou NIS. Você pode executar todas essas tarefas antes ou depois de ativar o acesso à conta.

Associar uma chave pública a uma conta de administrador

Para autenticação de chave pública SSH, você deve associar a chave pública a uma conta de administrador antes que a conta possa acessar o SVM. Você pode usar o `security login publickey create` comando para associar uma chave a uma conta de administrador.

Sobre esta tarefa

Se você autenticar uma conta via SSH com uma senha e uma chave pública SSH, a conta será autenticada primeiro com a chave pública.

Antes de começar

- Você deve ter gerado a chave SSH.
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Associar uma chave pública a uma conta de administrador:

```
security login publickey create -vserver SVM_name -username user_name -index
index -publickey certificate -comment comment
```

Para obter a sintaxe de comando completa, consulte a referência de Planilha para ["Associar uma chave pública a uma conta de utilizador"](#).

2. Verifique a alteração visualizando a chave pública:

```
security login publickey show -vserver SVM_name -username user_name -index
index
```

Exemplo

O comando a seguir associa uma chave pública à conta de administrador do SVM `svmadmin1` para o `engData1` SVM. A chave pública recebe o número de índice 5.

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

Gerenciar chaves públicas SSH e certificados X,509 para uma conta de administrador

Para maior segurança de autenticação SSH com contas de administrador, você pode usar o `security login publickey` conjunto de comandos para gerenciar a chave pública SSH e sua associação com certificados X,509.

Associar uma chave pública e um certificado X,509 a uma conta de administrador

A partir do ONTAP 9.13.1, é possível associar um certificado X,509 à chave pública associada à conta de administrador. Isso dá a você a segurança adicional de verificações de expiração ou revogação de certificados no login SSH para essa conta.

Sobre esta tarefa

Se você autenticar uma conta via SSH com uma chave pública SSH e um certificado X,509, o ONTAP verifica a validade do certificado X,509 antes de autenticar com a chave pública SSH. O login SSH será recusado se esse certificado estiver expirado ou revogado, e a chave pública será automaticamente desativada.

Antes de começar

- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- Você deve ter gerado a chave SSH.
- Se você precisar apenas do certificado X,509 para ser verificado para a expiração, você pode usar um certificado autoassinado.
- Se você precisar que o certificado X,509 seja verificado quanto à expiração e revogação:
 - Você deve ter recebido o certificado de uma autoridade de certificação (CA).
 - Você deve instalar a cadeia de certificados (certificados de CA intermediária e raiz) usando `security certificate install` comandos.
 - Você precisa ativar o OCSP para SSH. ["Verifique se os certificados digitais são válidos usando OCSP"](#) Consulte para obter instruções.

Passos

1. Associar uma chave pública e um certificado X,509 a uma conta de administrador:

```
security login publickey create -vserver SVM_name -username user_name -index index -publickey certificate -x509-certificate install
```

Para obter a sintaxe de comando completa, consulte a referência de Planilha para ["Associar uma chave pública a uma conta de utilizador"](#).

2. Verifique a alteração visualizando a chave pública:

```
security login publickey show -vserver SVM_name -username user_name -index index
```

Exemplo

O comando a seguir associa uma chave pública e um certificado X,509 à conta de administrador do SVM `svmadmin2` para o `engData2` SVM. A chave pública recebe o número de índice 6.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

Remova a associação de certificados da chave pública SSH para uma conta de administrador

Você pode remover a associação de certificados atual da chave pública SSH da conta, mantendo a chave pública.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Remova a associação de certificados X,509 de uma conta de administrador e guarde a chave pública SSH existente:

```
security login publickey modify -vserver SVM_name -username user_name -index
index -x509-certificate delete
```

2. Verifique a alteração visualizando a chave pública:

```
security login publickey show -vserver SVM_name -username user_name -index
index
```

Exemplo

O comando a seguir remove a associação de certificado X,509 da conta de administrador SVM `svmadmin2` para SVM `engData2` no índice 6.

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

Remova a associação de chave pública e certificado de uma conta de administrador

Você pode remover a chave pública atual e a configuração de certificado de uma conta.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Remova a chave pública e uma associação de certificado X,509 de uma conta de administrador:

```
security login publickey delete -vserver SVM_name -username user_name -index
index
```

2. Verifique a alteração visualizando a chave pública:

```
security login publickey show -vserver SVM_name -username user_name -index index
```

Exemplo

O comando a seguir remove uma chave pública e um certificado X,509 da conta de administrador do SVM svmadmin3 para o SVM engData3 no índice 7.

```
cluster1::> security login publickey delete -vserver engData3 -username svmadmin3 -index 7
```

Configure o Cisco Duo 2FA para logins SSH com o ONTAP

A partir do ONTAP 9.14.1, você pode configurar o ONTAP para usar o Cisco Duo para autenticação de dois fatores (2FA) durante logins SSH. Você configura o Duo no nível do cluster e se aplica a todas as contas de usuário por padrão. Como alternativa, você pode configurar o Duo no nível da VM de armazenamento (anteriormente chamado de vserver), caso em que ele se aplica apenas aos usuários dessa VM de armazenamento. Se você ativar e configurar o Duo, ele serve como um método de autenticação adicional, complementando os métodos existentes para todos os usuários.

Se você ativar a autenticação Duo para logins SSH, os usuários precisarão Registrar um dispositivo na próxima vez que fizerem login usando SSH. Para obter informações sobre a inscrição, consulte o Cisco ["documentação de inscrição" Duo](#) .

Você pode usar a interface de linha de comando ONTAP para executar as seguintes tarefas com o Cisco Duo:

- [Configure o Cisco Duo](#)
- [Altere a configuração do Cisco Duo](#)
- [Remova a configuração do Cisco Duo](#)
- [Veja a configuração do Cisco Duo](#)
- [Remova um grupo Duo](#)
- [Ver grupos Duo](#)
- [Ignorar a autenticação Duo para usuários](#)

Configure o Cisco Duo

Você pode criar uma configuração do Cisco Duo para todo o cluster ou para uma VM de armazenamento específica (chamada de vserver na CLI do ONTAP) usando o `[security login duo create` comando. Quando você faz isso, o Cisco Duo é habilitado para logins SSH para esse cluster ou VM de armazenamento. Saiba mais sobre o `[security login duo create` comando ONTAP na referência de comando.

Passos

1. Inicie sessão no Painel de Administração do Cisco Duo.

2. Acesse a **aplicações > aplicação UNIX**.
3. Registre sua chave de integração, chave secreta e nome de host da API.
4. Faça login na sua conta ONTAP usando SSH.
5. Ative a autenticação do Cisco Duo para esta VM de armazenamento, substituindo as informações do seu ambiente pelos valores entre parênteses:

```
security login duo create \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME>
```

Altere a configuração do Cisco Duo

Você pode alterar a maneira como o Cisco Duo autentica os usuários (por exemplo, quantos prompts de autenticação são fornecidos ou qual proxy HTTP é usado). Se você precisar alterar a configuração do Cisco Duo para uma VM de armazenamento (chamada de vserver na CLI do ONTAP), use o `security login duo modify` comando. Saiba mais sobre o `security login duo modify` comando ONTAP na referência de comando.

Passos

1. Inicie sessão no Painel de Administração do Cisco Duo.
2. Acesse a **aplicações > aplicação UNIX**.
3. Registre sua chave de integração, chave secreta e nome de host da API.
4. Faça login na sua conta ONTAP usando SSH.
5. Altere a configuração do Cisco Duo para esta VM de armazenamento, substituindo as informações atualizadas do seu ambiente pelos valores entre parênteses:

```
security login duo modify \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME> \  
-pushinfo true|false \  
-http-proxy <HTTP_PROXY_URL> \  
-autopush true|false \  
-max-prompts 1|2|3 \  
-is-enabled true|false \  
-fail-mode safe|secure
```

Remova a configuração do Cisco Duo

Você pode remover a configuração do Cisco Duo, que removerá a necessidade de os usuários SSH se

autenticarem usando o Duo no início de sessão. Para remover a configuração do Cisco Duo para uma VM de armazenamento (conhecida como vserver na CLI do ONTAP), você pode usar o `security login duo delete` comando. Saiba mais sobre o `security login duo delete` comando ONTAP na referência de comando.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Remova a configuração do Cisco Duo para esta VM de armazenamento, substituindo o nome da VM de armazenamento por `<STORAGE_VM_NAME>`:

```
security login duo delete -vserver <STORAGE_VM_NAME>
```

Isso exclui permanentemente a configuração do Cisco Duo para essa VM de armazenamento.

Veja a configuração do Cisco Duo

Você pode exibir a configuração existente do Cisco Duo para uma VM de armazenamento (chamada de vserver na CLI do ONTAP) usando o `security login duo show` comando. Saiba mais sobre o `security login duo show` comando ONTAP na referência de comando.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Mostrar a configuração do Cisco Duo para esta VM de armazenamento. Opcionalmente, você pode usar o `vserver` parâmetro para especificar uma VM de armazenamento, substituindo o nome da VM de armazenamento por `<STORAGE_VM_NAME>`:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

Você deve ver saída semelhante ao seguinte:

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```


Crie um grupo Duo

Você pode instruir o Cisco Duo a incluir somente os usuários em um determinado ativo Directory, LDAP ou grupo de usuários local no processo de autenticação Duo. Se você criar um grupo Duo, somente os usuários desse grupo serão solicitados a autenticação Duo. Você pode criar um grupo Duo usando o `security login duo group create` comando. Quando você cria um grupo, você pode excluir usuários específicos desse grupo do processo de autenticação Duo. Saiba mais sobre o `security login duo group create` comando ONTAP na referência de comando.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Crie o grupo Duo, substituindo as informações do seu ambiente pelos valores entre parênteses. Se você omitir o `-vserver` parâmetro, o grupo será criado no nível do cluster:

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME> -excluded-users <USER1, USER2>
```

O nome do grupo Duo tem de corresponder a um grupo ativo Directory, LDAP ou local. Os usuários que você especificar com o parâmetro opcional `-excluded-users` não serão incluídos no processo de autenticação Duo.

Ver grupos Duo

Você pode exibir entradas de grupo existentes do Cisco Duo usando o `security login duo group show` comando. Saiba mais sobre o `security login duo group show` comando ONTAP na referência de comando.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Mostre as entradas do grupo Duo, substituindo as informações do seu ambiente pelos valores entre parênteses. Se você omitir o `-vserver` parâmetro, o grupo será mostrado no nível do cluster:

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME> -excluded-users <USER1, USER2>
```

O nome do grupo Duo tem de corresponder a um grupo ativo Directory, LDAP ou local. Os usuários que você especificar com o parâmetro opcional `-excluded-users` não serão exibidos.

Remova um grupo Duo

Você pode remover uma entrada de grupo Duo usando o `security login duo group delete` comando. Se você remover um grupo, os usuários desse grupo não serão mais incluídos no processo de autenticação Duo. Saiba mais sobre o `security login duo group delete` comando ONTAP na referência de comando.

Passos

1. Faça login na sua conta ONTAP usando SSH.

2. Remova a entrada do grupo Duo, substituindo as informações do ambiente pelos valores entre parênteses. Se você omitir o `-vserver` parâmetro, o grupo será removido no nível do cluster:

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name <GROUP_NAME>
```

O nome do grupo Duo tem de corresponder a um grupo ativo Directory, LDAP ou local.

Ignorar a autenticação Duo para usuários

Você pode excluir todos os usuários ou usuários específicos do processo de autenticação Duo SSH.

Excluir todos os usuários Duo

Você pode desativar a autenticação SSH do Cisco Duo para todos os usuários.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Desative a autenticação Cisco Duo para usuários SSH, substituindo o nome do SVM para `<STORAGE_VM_NAME>`:

```
security login duo modify -vserver <STORAGE_VM_NAME> -is-enabled false
```

Excluir usuários do grupo Duo

Você pode excluir certos usuários que fazem parte de um grupo Duo do processo de autenticação Duo SSH.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Desative a autenticação Cisco Duo para usuários específicos em um grupo. Substitua o nome do grupo e a lista de usuários para excluir pelos valores entre parênteses:

```
security login duo group modify -group-name <GROUP_NAME> -excluded-users <USER1, USER2>
```

O nome do grupo Duo tem de corresponder a um grupo ativo Directory, LDAP ou local. Os usuários que você especificar com o `-excluded-users` parâmetro não serão incluídos no processo de autenticação Duo.

Excluir usuários locais Duo

Você pode excluir usuários locais específicos do uso da autenticação Duo usando o Painel de Administração do Cisco Duo. Para obter instruções, consulte ["Documentação do Cisco Duo"](#) a .

Gere e instale uma visão geral do certificado de servidor assinado pela CA

Em sistemas de produção, é uma prática recomendada instalar um certificado digital assinado pela CA para uso na autenticação do cluster ou SVM como um servidor SSL. Você pode usar o `security certificate generate-csr` comando para gerar uma solicitação de assinatura de certificado (CSR) e o `security certificate install` comando para instalar o certificado recebido de volta da autoridade de certificação.

Gerar uma solicitação de assinatura de certificado

Você pode usar o `security certificate generate-csr` comando para gerar uma solicitação de assinatura de certificado (CSR). Depois de processar sua solicitação, a autoridade de certificação (CA) envia o certificado digital assinado.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Gerar um CSR:

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

O comando a seguir cria uma CSR com uma chave privada de 2048 bits gerada pela função de hash "SHA256" para uso pelo grupo "Software" no departamento de TI de uma empresa cujo nome comum personalizado é "erver1.companyname.com", localizado em Sunnyvale, Califórnia, EUA. O endereço de e-mail do administrador de Contato da SVM é "web@example.com". O sistema apresenta a CSR e a chave privada na saída.

Exemplo de criação de uma CSR

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
```

Certificate Signing Request :

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMakGA1UEBhMCVVMx
CTAHBgNVBAgtADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Private Key :

```
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+jlhrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
```

NOTE: Keep a copy of your certificate request and private key for future reference.

2. Copie a solicitação de certificado da saída CSR e envie-a em formato eletrônico (como e-mail) para uma CA de terceiros confiável para assinatura.

Após processar sua solicitação, a CA envia o certificado digital assinado. Você deve manter uma cópia da chave privada e do certificado digital assinado pela CA.

Instale um certificado de servidor assinado pela CA

Você pode usar o `security certificate install` comando para instalar um certificado de servidor assinado pela CA em um SVM. O ONTAP solicita os certificados raiz e intermediário da autoridade de certificação (CA) que formam a cadeia de certificados do certificado do servidor.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passo

1. Instale um certificado de servidor assinado pela CA:

```
security certificate install -vserver SVM_name -type certificate_type
```

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



O ONTAP solicita os certificados raiz e intermediários da CA que formam a cadeia de certificados do certificado do servidor. A cadeia começa com o certificado da CA que emitiu o certificado do servidor e pode variar até o certificado raiz da CA. Qualquer certificado intermediário ausente resulta na falha da instalação do certificado do servidor.

O comando a seguir instala o certificado de servidor assinado pela CA e os certificados intermediários na SVM "engData2".

Exemplo de instalação de certificados intermediários de certificado de servidor assinado pela CA

```
cluster1::>security certificate install -vserver engData2 -type  
server
```

```
Please enter Certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBGNVBAoTAAEJMAcGA1UECzMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBGNVBAoTAAEJMAcGA1UECzMAMQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAAkEAyXrK2sry
```

```
-----END CERTIFICATE-----
```

```
Please enter Private Key: Press <Enter> when done
```

```
-----BEGIN RSA PRIVATE KEY-----
```

```
MIIBPAIBAAJBAM16ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvFC61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT PFnnZnbVcXVM70tbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJz7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrFYC8KwE9k7A0y1RzBLdUwK9AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIgaEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
```

```
-----END RSA PRIVATE KEY-----
```

```
Do you want to continue entering root and/or intermediate  
certificates {y|n}: y
```

```
Please enter Intermediate Certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIE+zCCBGSGAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBACGTG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEh0dHRwOi8vd3d3LnZhbG1kYXRpb24gIDAE BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoXDTI0MDYyOTE3MDYyMFOwYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFFRoZSBHbyBEYWRkeSBHcm91cCwgSW5jLjExMC8GA1UECXMOR28gRGFkZkZkkgQ2xhc3MgMiBDZXJ0
```

```
-----END CERTIFICATE-----
```

```
Do you want to continue entering root and/or intermediate  
certificates {y|n}: y
```

```
Please enter Intermediate Certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwbgsxJDAiBgNVBACtG1ZhbG1DZXJ0
IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbG1DZXJ0IENsYXNzIDIgUG9saWN5IFZhbG1kYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDEzhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBACtG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbG1DZXJ0IENs
YXNzIDIgUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEzhodHRw
-----END CERTIFICATE-----
```

```
Do you want to continue entering root and/or intermediate
certificates {y|n}: n
```

```
You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

Gerencie certificados com o System Manager

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para gerenciar autoridades de certificação confiáveis, certificados de cliente/servidor e autoridades de certificação locais (integradas).

Com o System Manager, você pode gerenciar os certificados recebidos de outros aplicativos para que você possa autenticar as comunicações desses aplicativos. Você também pode gerenciar seus próprios certificados que identificam seu sistema para outros aplicativos.

Exibir informações do certificado

Com o System Manager, é possível exibir autoridades de certificação confiáveis, certificados de cliente/servidor e autoridades de certificação locais armazenadas no cluster.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Role até a área **Segurança**. Na seção **certificados**, os seguintes detalhes são exibidos:
 - O número de autoridades de certificação confiáveis armazenadas.
 - O número de certificados de cliente/servidor armazenados.
 - O número de autoridades locais de certificação armazenadas.
3. Selecione qualquer número para ver detalhes sobre uma categoria de certificados ou [→](#) selecione para abrir a página **certificados**, que contém informações sobre todas as categorias. A lista exibe as informações de todo o cluster. Se você quiser exibir informações apenas para uma VM de armazenamento específica, execute as seguintes etapas:
 - a. Selecione **Storage > Storage VMs**.
 - b. Selecione a VM de armazenamento.

- c. Mude para o separador **Settings**.
- d. Selecione um número mostrado na seção **certificado**.

O que fazer a seguir

- Na página **certificados**, você pode [Gerar uma solicitação de assinatura de certificado](#).
- As informações do certificado são separadas em três guias, uma para cada categoria. Você pode executar as seguintes tarefas em cada guia:

Neste separador...	Pode executar estes procedimentos...
Autoridades de certificação confiáveis	<ul style="list-style-type: none"> • [install-trusted-cert] • Excluir uma autoridade de certificação confiável • Renove uma autoridade de certificação confiável
Certificados de cliente/servidor	<ul style="list-style-type: none"> • [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
<ul style="list-style-type: none"> • Autoridades de certificação locais* 	<ul style="list-style-type: none"> • Crie uma nova autoridade de certificação local • Assine um certificado usando uma autoridade de certificação local • Eliminar uma autoridade de certificação local • Renove uma autoridade de certificação local

Gerar uma solicitação de assinatura de certificado

Você pode gerar uma solicitação de assinatura de certificado (CSR) com o System Manager a partir de qualquer guia da página **certificados**. Uma chave privada e uma CSR correspondente são geradas, que podem ser assinadas usando uma autoridade de certificação para gerar um certificado público.

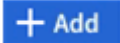
Passos

1. Veja a página **certificados**. [Exibir informações do certificado](#)Consulte .
2. Selecione * gerar CSR*.
3. Preencha as informações para o nome do assunto:
 - a. Introduza um **nome comum**.
 - b. Selecione um **país**.
 - c. Introduza uma **organização**.
 - d. Introduza uma **unidade organizacional**.
4. Se você quiser substituir os padrões, selecione **mais opções** e forneça informações adicionais.

Instale (adicione) uma autoridade de certificação confiável

Você pode instalar autoridades de certificação confiáveis adicionais no System Manager.

Passos

1. Veja a guia **autoridades de certificados confiáveis**. [Exibir informações do certificado](#)Consulte .
2.  Selecione .
3. No painel **Adicionar autoridade de certificação confiável**, execute o seguinte:
 - Introduza um **nome**.
 - Para o **Escopo**, selecione uma VM de armazenamento.
 - Introduza um **nome comum**.
 - Selecione um **tipo**.
 - Introduza ou importe **detalhes do certificado**.


Excluir uma autoridade de certificação confiável

Com o System Manager, você pode excluir uma autoridade de certificação confiável.



Não é possível excluir autoridades de certificado confiáveis pré-instaladas com o ONTAP.


Passos

1. Veja a guia **autoridades de certificados confiáveis**. [Exibir informações do certificado](#)Consulte .
2. Selecione o nome da autoridade de certificação fidedigna.
3. Selecione  ao lado do nome e selecione **Excluir**.

Renove uma autoridade de certificação confiável

Com o System Manager, você pode renovar uma autoridade de certificação confiável que expirou ou está prestes a expirar.


Passos

1. Veja a guia **autoridades de certificados confiáveis**. [Exibir informações do certificado](#)Consulte .
2. Selecione o nome da autoridade de certificação fidedigna.
3. Selecione  ao lado do nome do certificado e depois **Renew**.

Instale (adicione) um certificado cliente/servidor

Com o System Manager, você pode instalar certificados de cliente/servidor adicionais.

Passos

1. Veja a guia **certificados de cliente/servidor**. [Exibir informações do certificado](#)Consulte .
2.  Selecione .
3. No painel **Adicionar certificado de cliente/servidor**, execute o seguinte:
 - Introduza um **nome de certificado**.
 - Para o **Escopo**, selecione uma VM de armazenamento.
 - Introduza um **nome comum**.
 - Selecione um **tipo**.

- Introduza ou importe **detalhes do certificado**. Você pode escrever ou copiar e colar os detalhes do certificado de um arquivo de texto ou importar o texto de um arquivo de certificado clicando em **Importar**.
- Introduza a **chave privada**. Você pode escrever ou copiar e colar na chave privada de um arquivo de texto ou pode importar o texto de um arquivo de chave privada clicando em **Importar**.

Gerar (adicionar) um certificado cliente/servidor autoassinado

Com o System Manager, você pode gerar certificados de cliente/servidor autoassinados adicionais.


Passos

1. Veja a guia **certificados de cliente/servidor**. [Exibir informações do certificado](#)Consulte .
2. Selecione * gerar certificado autoassinado*.
3. No painel **Generate Self-signed Certificate** (gerar certificado autoassinado), execute o seguinte procedimento:
 - Introduza um **nome de certificado**.
 - Para o **Escopo**, selecione uma VM de armazenamento.
 - Introduza um **nome comum**.
 - Selecione um **tipo**.
 - Selecione uma função **hash**.
 - Selecione um **tamanho da chave**.
 - Selecione uma **VM de armazenamento**.

Excluir um certificado cliente/servidor

Com o System Manager, pode eliminar certificados de cliente/servidor.


Passos

1. Veja a guia **certificados de cliente/servidor**. [Exibir informações do certificado](#)Consulte .
2. Selecione o nome do certificado cliente/servidor.
3. Selecione  ao lado do nome e clique em **Excluir**.

Renove um certificado cliente/servidor

Com o System Manager, você pode renovar um certificado cliente/servidor que expirou ou está prestes a expirar.

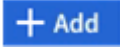
Passos

1. Veja a guia **certificados de cliente/servidor**. [Exibir informações do certificado](#)Consulte .
2. Selecione o nome do certificado cliente/servidor.
3. Selecione  ao lado do nome e, em seguida, clique em **Renew**.

Crie uma nova autoridade de certificação local

Com o System Manager, você pode criar uma nova autoridade de certificação local.


Passos

1. Veja a guia **autoridades de certificados locais**. [Exibir informações do certificado](#)Consulte .
2.  Selecione .
3. No painel **Add local Certificate Authority** (Adicionar autoridade de certificação local), execute o seguinte procedimento:
 - Introduza um **nome**.
 - Para o **Escopo**, selecione uma VM de armazenamento.
 - Introduza um **nome comum**.
4. Se você quiser substituir os padrões, selecione **mais opções** e forneça informações adicionais.

Assine um certificado usando uma autoridade de certificação local

No System Manager, você pode usar uma autoridade de certificação local para assinar um certificado.


Passos

1. Veja a guia **autoridades de certificados locais**. [Exibir informações do certificado](#)Consulte .
2. Selecione o nome da autoridade de certificação local.
3. Selecione  ao lado do nome e depois **assinar um certificado**.
4. Preencha o formulário **assinar um pedido de assinatura de certificado**.
 - Você pode colar no conteúdo de assinatura de certificado ou importar um arquivo de solicitação de assinatura de certificado clicando em **Importar**.
 - Especifique o número de dias para os quais o certificado será válido.

Eliminar uma autoridade de certificação local

Com o System Manager, pode eliminar uma autoridade de certificação local.


Passos

1. Veja a guia **Autoridade de Certificação local**. [Exibir informações do certificado](#)Consulte .
2. Selecione o nome da autoridade de certificação local.
3. Selecione  ao lado do nome e, em seguida, **Excluir**.

Renove uma autoridade de certificação local

Com o System Manager, você pode renovar uma autoridade de certificação local que expirou ou está prestes a expirar.

Passos

1. Veja a guia **Autoridade de Certificação local**. [Exibir informações do certificado](#)Consulte .
2. Selecione o nome da autoridade de certificação local.
3. Selecione  ao lado do nome e, em seguida, clique em **Renew**.

Configure a visão geral do acesso do controlador de domínio do ativo Directory

Você deve configurar o acesso do controlador de domínio do AD ao cluster ou SVM antes que uma conta do AD possa acessar o SVM. Se você já tiver configurado um servidor SMB para um SVM de dados, poderá configurar o SVM como um gateway, ou *tunnel*, para acesso AD ao cluster. Se você não tiver configurado um servidor SMB, poderá criar uma conta de computador para o SVM no domínio AD.

O ONTAP oferece suporte aos seguintes serviços de autenticação de controlador de domínio:

- Kerberos
- LDAP
- NETLOGON
- Autoridade de Segurança local (LSA)

O ONTAP suporta os seguintes algoritmos de chave de sessão para conexões seguras de Netlogon:

Algoritmo da chave de sessão	Disponível a partir de...
HMAC-SHA256, com base no padrão de criptografia avançada (AES) se o cluster estiver executando o ONTAP 9.9,1 ou anterior e o controlador de domínio forçar o AES para serviços de Netlogon seguros, a conexão falhará. Nesse caso, você precisa reconfigurar seu controlador de domínio para aceitar conexões de chave forte com o ONTAP.	ONTAP 9.10,1
DES e HMAC-MD5 (quando a chave forte está definida)	Todos os lançamentos do ONTAP 9

Se você quiser usar chaves de sessão AES durante o estabelecimento de canal seguro Netlogon, você precisa verificar se o AES está habilitado no SVM.

- A partir do ONTAP 9.14,1, o AES é ativado por padrão quando você cria um SVM e não precisa modificar as configurações de segurança do seu SVM para usar chaves de sessão AES durante o estabelecimento de canal seguro Netlogon.
- No ONTAP 9.10,1 a 9.13.1, o AES é desativado por padrão quando você cria um SVM. Você precisa ativar o AES usando o seguinte comando:

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```



Quando você atualiza para o ONTAP 9.14,1 ou posterior, a configuração AES para SVMs existentes que foram criadas com versões mais antigas do ONTAP não será alterada automaticamente. Você ainda precisa atualizar o valor dessa configuração para ativar o AES nesses SVMs.

Configurar um túnel de autenticação

Se você já tiver configurado um servidor SMB para um SVM de dados, poderá usar o `security login domain-tunnel create` comando para configurar o SVM como um gateway, ou *tunnel*, para acesso AD ao cluster.

Antes de começar

- Você precisa ter configurado um servidor SMB para um data SVM.
- Você deve ter habilitado uma conta de usuário de domínio do AD para acessar o SVM do administrador do cluster.
- Você deve ser um administrador de cluster para executar esta tarefa.

A partir do ONTAP 9.10.1, se você tiver um gateway SVM (túnel de domínio) para acesso AD, você poderá usar o Kerberos para autenticação de administrador se tiver desabilitado o NTLM no domínio do AD. Em versões anteriores, o Kerberos não era compatível com autenticação de administrador para gateways SVM. Esta funcionalidade está disponível por padrão; nenhuma configuração é necessária.



A autenticação Kerberos é sempre tentada primeiro. Em caso de falha, a autenticação NTLM é então tentada.

Passo

1. Configure um SVM de dados habilitado para SMB como um túnel de autenticação para acesso do controlador de domínio do AD ao cluster:

```
security login domain-tunnel create -vserver svm_name
```

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



O SVM deve estar em execução para que o usuário seja autenticado.

O comando a seguir configura o SVM de dados habilitado para SMB "engData" como um túnel de autenticação.

```
cluster1::>security login domain-tunnel create -vserver engData
```

Crie uma conta de computador SVM no domínio

Se você não tiver configurado um servidor SMB para um SVM de dados, poderá usar o `vserver active-directory create` comando para criar uma conta de computador para o SVM no domínio.

Sobre esta tarefa

Depois de inserir o `vserver active-directory create` comando, você será solicitado a fornecer as credenciais para uma conta de usuário do AD com Privileges suficiente para adicionar computadores à unidade organizacional especificada no domínio. A senha da conta não pode estar vazia.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passo

1. Crie uma conta de computador para um SVM no domínio AD:

```
vserver active-directory create -vserver SVM_name -account-name  
NetBIOS_account_name -domain domain -ou organizational_unit
```

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

O comando a seguir cria uma conta de computador chamada "ADSERVER1" no domínio "example.com" para SVM "engData". Você será solicitado a inserir as credenciais da conta de usuário do AD depois de inserir o comando.

```
cluster1::>vserver active-directory create -vserver engData -account  
-name ADSERVER1 -domain example.com
```

In order to create an Active Directory machine account, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "example.com" domain.

Enter the user name: Administrator

Enter the password:

Configure a visão geral do acesso ao servidor LDAP ou NIS

Você deve configurar o acesso de servidor LDAP ou NIS a um SVM antes que as contas LDAP ou NIS possam acessar o SVM. O recurso de switch permite que você use LDAP ou NIS como fontes alternativas de serviço de nomes.

Configurar o acesso ao servidor LDAP

Você deve configurar o acesso do servidor LDAP a um SVM antes que as contas LDAP possam acessar o SVM. Você pode usar o `vserver services name-service ldap client create` comando para criar uma configuração de cliente LDAP no SVM. Em seguida, você pode usar o `vserver services name-service ldap create` comando para associar a configuração do cliente LDAP ao SVM.

Sobre esta tarefa

A maioria dos servidores LDAP pode usar os esquemas padrão fornecidos pelo ONTAP:

- MS-AD-BIS (o esquema preferido para a maioria dos servidores AD do Windows 2012 e posteriores)
- Ad-IDMU (Windows 2008, Windows 2016 e servidores AD posteriores)
- Ad-SFU (Windows 2003 e servidores AD anteriores)
- RFC-2307 (SERVIDORES LDAP UNIX)

É melhor usar os esquemas padrão, a menos que haja um requisito para fazer o contrário. Nesse caso, você pode criar seu próprio esquema copiando um esquema padrão e modificando a cópia. Para obter mais informações, consulte:

- "Configuração NFS"
- "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"

Antes de começar

- Você precisa ter instalado a "Certificado digital do servidor assinado pela CA" no SVM.
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Criar uma configuração de cliente LDAP em uma SVM:

```
vserver services name-service ldap client create -vserver <SVM_name> -client
-config <client_configuration> -servers <LDAP_server_IPs> -schema <schema>
-use-start-tls <true|false>
```



Iniciar TLS é compatível apenas para acesso a SVMs de dados. Ele não é compatível com acesso a SVMs administrativas.

Para obter a sintaxe de comando completa, consulte "folha de trabalho".

O comando a seguir cria uma configuração de cliente LDAP chamada `corp` em SVM `engData`. O cliente faz ligações anônimas aos servidores LDAP com os endereços IP 172.160.0.100 e 172.16.0.101. O cliente usa o esquema RFC-2307 para fazer consultas LDAP. A comunicação entre o cliente e o servidor é criptografada usando Iniciar TLS.

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```



A partir de ONTAP 9.2, o campo `-ldap-servers` substitui o `-servers` campo. Este novo campo pode ter um nome de host ou um endereço IP para o servidor LDAP.

2. Associe a configuração do cliente LDAP à SVM: `vserver services name-service ldap create -vserver <SVM_name> -client-config <client_configuration> -client-enabled <true|false>`

Para obter a sintaxe de comando completa, consulte "folha de trabalho".

O comando a seguir associa a configuração do cliente LDAP `corp` ao SVM `engData` e habilita o cliente LDAP no SVM.

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```



A partir do ONTAP 9.2, o `vserver services name-service ldap create` comando executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não conseguir entrar em Contato com o servidor de nomes.

3. Valide o status dos servidores de nomes usando o comando de verificação ldap do serviço de nomes dos serviços vserver.

O comando a seguir valida servidores LDAP no SVM vs0.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
| "10.11.12.13". |
```

O comando name Service check está disponível a partir de ONTAP 9.2.

Configurar o acesso ao servidor NIS

Você deve configurar o acesso do servidor NIS a um SVM antes que as contas NIS possam acessar o SVM. Você pode usar o `vserver services name-service nis-domain create` comando para criar uma configuração de domínio NIS em um SVM.

Antes de começar

- Todos os servidores configurados devem estar disponíveis e acessíveis antes de configurar o domínio NIS no SVM.
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passo

1. Crie uma configuração de domínio NIS em uma SVM:

```
vserver services name-service nis-domain create -vserver <SVM_name> -domain <client_configuration> -nis-servers <NIS_server_IPs>
```

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



A partir de ONTAP 9.2, o campo `-nis-servers` substitui o `-servers` campo. Este novo campo pode ter um nome de host ou um endereço IP para o servidor NIS.

O comando a seguir cria uma configuração de domínio NIS no SVM `engData`. O domínio NIS `nisdomain` comunica com um servidor NIS com o endereço IP `192.0.2.180`.

```
cluster1::>vserver services name-service nis-domain create -vserver engData -domain nisdomain -nis-servers 192.0.2.180
```

Crie um switch de serviço de nomes

O recurso de switch de serviço de nomes permite que você use LDAP ou NIS como fontes alternativas de

serviço de nomes. Você pode usar o `vserver services name-service ns-switch modify` comando para especificar a ordem de pesquisa para fontes de serviço de nome.

Antes de começar

- Tem de ter configurado o acesso ao servidor LDAP e NIS.
- Você deve ser um administrador de cluster ou um administrador de SVM para executar essa tarefa.

Passo

1. Especifique a ordem de pesquisa para fontes do serviço de nomes:

```
vserver services name-service ns-switch modify -vserver <SVM_name> -database <name_service_switch_database> -sources <name_service_source_order>
```

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

O comando a seguir especifica a ordem de pesquisa das fontes de serviço de nomes LDAP e NIS para o `passwd` banco de dados no SVM `engData`.

```
cluster1::>vserver services name-service ns-switch  
modify -vserver engData -database passwd -source files ldap,nis
```

Altere uma senha de administrador no ONTAP

Você deve alterar sua senha inicial imediatamente após fazer login no sistema pela primeira vez. Se você for um administrador SVM, poderá usar o `security login password` comando para alterar sua própria senha. Se for um administrador de cluster, pode utilizar o `security login password` comando para alterar a palavra-passe de qualquer administrador.

Sobre esta tarefa

A nova palavra-passe deve respeitar as seguintes regras:

- Não pode conter o nome de utilizador
- Deve ter pelo menos oito caracteres
- Deve conter pelo menos uma letra e um número
- Não pode ser o mesmo que as últimas seis senhas



Você pode usar o `security login role config modify` comando para modificar as regras de senha para contas associadas a uma determinada função. Saiba mais sobre o comando link:<https://docs.NetApp.com/US-en/ONTAP-cli/security-login-role-config-modify.html> `security login role config modify` em referência de comando ONTAP.

Antes de começar

- Você deve ser um administrador de cluster ou SVM para alterar sua própria senha.
- Você deve ser um administrador de cluster para alterar a senha de outro administrador.

Passo

1. Alterar uma palavra-passe de administrador: `security login password -vserver svm_name -username user_name`

O comando a seguir altera a senha do administrador `admin1` do SVM `vs1.example.com`. É-lhe pedido que introduza a palavra-passe atual e, em seguida, introduza e volte a introduzir a nova palavra-passe.

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

Bloquear e desbloquear uma conta de administrador

Você pode usar o `security login lock` comando para bloquear uma conta de administrador e o `security login unlock` comando para desbloquear a conta.

Antes de começar

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

Passos

1. Bloquear uma conta de administrador:

```
security login lock -vserver SVM_name -username user_name
```

O comando a seguir bloqueia a conta de administrador `admin1` do SVM `vs1.example.com`:

```
cluster1::>security login lock -vserver engData -username admin1
```

2. Desbloquear uma conta de administrador:

```
security login unlock -vserver SVM_name -username user_name
```

O comando a seguir desbloqueia a conta de administrador `admin1` do SVM `vs1.example.com`:

```
cluster1::>security login unlock -vserver engData -username admin1
```

Gerir tentativas de início de sessão falhadas

Tentativas repetidas de login falhadas às vezes indicam que um intruso está tentando acessar o sistema de armazenamento. Você pode executar várias etapas para garantir que não ocorra uma intrusão.

Como você saberá que as tentativas de login falharam

O sistema de Gestão de Eventos (EMS) notifica-o sobre tentativas falhadas de início de sessão a cada hora. Pode encontrar um registo de tentativas de início de sessão falhadas `audit.log` no ficheiro.

O que fazer se tentativas repetidas de login falharem

A curto prazo, você pode executar várias etapas para evitar uma intrusão:

- Exigir que as senhas sejam compostas por um número mínimo de caracteres maiúsculos, minúsculos, caracteres especiais e/ou dígitos
- Impor um atraso após uma tentativa de início de sessão com falha
- Limite o número de tentativas de início de sessão falhadas permitidas e bloqueie os utilizadores após o número especificado de tentativas falhadas
- Expire e bloqueie contas que estejam inativas por um determinado número de dias

Você pode usar o `security login role config modify` comando para executar essas tarefas.

A longo prazo, você pode seguir estes passos adicionais:

- Use o `security ssh modify` comando para limitar o número de tentativas de login falhadas para todos os SVMs recém-criados.
- Migre contas de algoritmo MD5 existentes para o algoritmo SHA-512 mais seguro, exigindo que os usuários alterem suas senhas.

Aplicar SHA-2 em senhas de conta de administrador

As contas de administrador criadas antes do ONTAP 9.0 continuam a usar senhas MD5 após a atualização, até que as senhas sejam alteradas manualmente. O MD5 é menos seguro do que o SHA-2. Portanto, após a atualização, você deve solicitar aos usuários de contas MD5 que alterem suas senhas para usar a função hash SHA-512 padrão.

Sobre esta tarefa

A funcionalidade hash de senha permite que você faça o seguinte:

- Exibir contas de usuário que correspondem à função hash especificada.
- Expire contas que usam uma função hash especificada (por exemplo, MD5), forçando os usuários a alterar suas senhas em seu próximo login.
- Bloquear contas cujas senhas usam a função hash especificada.
- Ao reverter para uma versão anterior ao ONTAP 9, redefina a própria senha do administrador do cluster para que ela seja compatível com a função hash (MD5) que é suportada pela versão anterior.

O ONTAP aceita senhas SHA-2 pré-hash somente usando o SDK de gerenciamento do NetApp (`security-login-create`e`security-login-modify-password`o`).

Passos

1. Migre as contas de administrador do MD5 para a função hash de senha SHA-512:
 - a. Expire todas as contas de administrador do MD5: `security login expire-password -vserver`

```
* -username * -hash-function md5
```

Isso força os usuários de conta do MD5 a alterar suas senhas no próximo login.

- b. Peça aos usuários de contas do MD5 para fazer login por meio de um console ou sessão SSH.

O sistema detecta que as contas estão expiradas e solicita aos usuários que alterem suas senhas. Sha-512 é usado por padrão para as senhas alteradas.

2. Para contas do MD5 cujos usuários não fazem login para alterar suas senhas dentro de um período de tempo, force a migração da conta:

- a. Bloquear contas que ainda usam a função hash MD5 (nível de privilégio avançado):

```
security login expire-password -vserver * -username * -hash-function md5 -lock-after integer
```


Após o número de dias especificado pelo `-lock-after`, os usuários não podem acessar suas contas do MD5.

- b. Desbloqueie as contas quando os usuários estiverem prontos para alterar suas senhas:


```
security login unlock -vserver svm_name -username user_name
```
- c. Faça com que os usuários façam login em suas contas por meio de uma sessão de console ou SSH e alterem suas senhas quando o sistema solicitar que façam isso.

Diagnosticar e corrigir problemas de acesso a arquivos

Passos

1. No System Manager, selecione **Storage > Storage VMs**.
2. Selecione a VM de armazenamento na qual você deseja executar um rastreamento.
3. Clique  em **mais**.
4. Clique em **Trace File Access**.
5. Forneça o nome de usuário e o endereço IP do cliente e clique em **Iniciar rastreamento**.

Os resultados do rastreio são apresentados numa tabela. A coluna **razões** fornece o motivo pelo qual um arquivo não pôde ser acessado.

6. Clique  na coluna esquerda da tabela de resultados para visualizar as permissões de acesso ao arquivo.

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 INTERRUPTÃO 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.