管理者アカウントを管理する
ONTAP 9

NetApp
September 12, 2024

目次

管理者アカウントを管理する

管理者アカウントの管理の概要

アカウントアクセスを有効にした方法によっては、ローカルアカウントへの公開鍵の関連付け、 CA 署名済みサーバデジタル証明書のインストール、 AD 、 LDAP 、 NIS のアクセスの設定などが必要になる場合があります。これらのタスクはすべて、アカウントアクセスを有効にする前後どちらでも実行できます。

管理者アカウントに公開鍵を関連付けます

SSH 公開鍵認証を使用する場合、アカウントが SVM にアクセスするためには、管理者アカウントに公開鍵を関連付ける必要があります。を使用できます `security login publickey create` 管理者アカウントにキーを関連付けるコマンド。

このタスクについて

SSH でのアカウントの認証にパスワードと SSH 公開鍵の両方を使用する場合、アカウントはまず公開鍵を使用して認証されます。

作業を開始する前に

- SSH キーを生成しておく必要があります。
- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

手順

1. 管理者アカウントに公開鍵を関連付けます。

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

   コマンド構文全体については、のワークシートリファレンスを参照してください "ユーザアカウントへの公開鍵の関連付け"。

2. 公開鍵を表示して変更を確認します。

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

例

次のコマンドは、SVM管理者アカウントに公開鍵を関連付けます `svmadmin1` SVM用 `engData1`。公開鍵のインデックス番号は 5 です。

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

管理者アカウントのSSH公開鍵とX.509証明書を管理します

管理者アカウントによるSSH認証のセキュリティを強化するには、を使用します `security login publickey` SSH公開鍵およびそのX.509証明書との関連付けを管理するための一連のコマンド。

公開鍵とX.509証明書を管理者アカウントに関連付けます

ONTAP 9.13.1以降では、管理者アカウントに関連付けた公開鍵にX.509証明書を関連付けることができます。これにより、そのアカウントのSSHログイン時の証明書の有効期限または失効チェックのセキュリティが強化されます。

このタスクについて

SSH公開鍵とX.509証明書の両方を使用してSSH経由でアカウントを認証する場合、ONTAPは、SSH公開鍵を使用して認証する前にX.509証明書の有効性をチェックします。証明書の有効期限が切れているか失効している場合、SSHログインは拒否され、公開鍵は自動的に無効になります。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。
- SSH キーを生成しておく必要があります。
- X.509証明書の有効期限のみを確認する必要がある場合は、自己署名証明書を使用できます。
- X.509証明書の有効期限と失効を確認する必要がある場合は、次の手順を実行します。
  - 認証局（CA）から証明書を受け取っておく必要があります。
  - を使用して証明書チェーン（中間およびルートのCA証明書）をインストールする必要があります `security certificate install` コマンド
  - SSHに対してOCSPを有効にする必要があります。を参照してください "OCSP を使用してデジタル証明書が有効であることを確認します" 手順については、を参照し

手順

1. 公開鍵とX.509証明書を管理者アカウントに関連付けます。

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

   コマンド構文全体については、のワークシートリファレンスを参照してください "ユーザアカウントへの公開鍵の関連付け"。

2. 公開鍵を表示して変更を確認します。

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

例

次のコマンドは、公開鍵とX.509証明書をSVM管理者アカウントに関連付けます `svmadmin2` SVM用 `engData2`。公開鍵にはインデックス番号6が割り当てられます。

```
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>
```

管理者アカウントの**SSH**公開鍵から証明書の関連付けを削除します

公開鍵を保持したまま、アカウントのSSH公開鍵から現在の証明書の関連付けを削除できます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

手順

1. 管理者アカウントからX.509証明書の関連付けを削除し、既存のSSH公開鍵を保持します。

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

2. 公開鍵を表示して変更を確認します。

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

例

次のコマンドは、X.509証明書の関連付けをSVM管理者アカウントから削除します `svmadmin2` SVM用 `engData2` インデックス番号6です。

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

管理者アカウントから公開鍵と証明書の関連付けを削除します

アカウントから現在の公開鍵と証明書の設定を削除できます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

手順

1. 管理者アカウントから公開鍵とX.509証明書の関連付けを削除します。

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

2. 公開鍵を表示して変更を確認します。

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

例

次のコマンドは、SVM管理者アカウントから公開鍵とX.509証明書を削除します `svmadmin3` SVM用 `engData3` インデックス番号7です。

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

SSHログイン用のCisco Duo 2FAの設定

ONTAP 9.14.1以降では、SSHログイン時に2要素認証（2FA）にCisco Duoを使用するようにONTAPを設定できます。Duoはクラスタレベルで設定し、IT環境はデフォルトですべてのユーザーアカウントを設定します。また、Storage VM（旧称Vserver）のレベルでDuoを設定することもできます。その場合は、そのStorage VMのユーザにのみ適用されます。Duoを有効にして設定すると、追加の認証方式として機能し、すべてのユーザの既存の方式を補完します。

SSHログインでDuo認証を有効にした場合、ユーザは次回SSHを使用してログインするときにデバイスを登録する必要があります。登録情報については、『Cisco Duo "登録に関するドキュメント"。

Cisco Duoでは、ONTAPコマンドラインインターフェイスを使用して次のタスクを実行できます。

- Cisco Duoの設定
- Cisco Duo設定の変更
- Cisco Duo設定の削除
- Cisco Duo設定の表示
- Duoグループの削除
- Duoグループの表示
- ユーザーのDuo認証をバイパスする

Cisco Duoの設定

Cisco Duo構成は、クラスタ全体または特定のStorage VM（ONTAP CLIではVserverと呼ばれます）に対して、次のコマンドを使用して作成できます。 `security login duo create` コマンドを実行しますこれを行うと、このクラスタまたはStorage VMのSSHログインでCisco Duoが有効になります。

手順

1. Cisco Duo管理パネルにログインします。
2. [アプリケーション]>[UNIXアプリケーション]*に移動します。
3. 統合キー、シークレットキー、およびAPIホスト名を記録します。

4. SSHを使用してONTAPアカウントにログインします。
5. このStorage VMに対してCisco Duo認証を有効にし、環境の情報を括弧内の値に置き換えます。

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

このコマンドの必須パラメータおよびオプションパラメータの詳細については、を参照してください。 "管理者認証と RBAC 設定用のワークシートです"。

Cisco Duo設定の変更

Cisco Duoがユーザを認証する方法（指定される認証プロンプトの数、使用されるHTTPプロキシなど）を変更できます。Storage VM（ONTAP CLIではVserver）のCisco Duo設定を変更する必要がある場合は、`security login duo modify` コマンドを実行します

手順

1. Cisco Duo管理パネルにログインします。
2. [アプリケーション]>[UNIXアプリケーション]*に移動します。
3. 統合キー、シークレットキー、およびAPIホスト名を記録します。
4. SSHを使用してONTAPアカウントにログインします。
5. このStorage VMのCisco Duo構成を変更します。括弧内の値は、環境から更新された情報に置き換えてください。

```
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 \
-prompts 1|2|3 \
-max-unenrolled-logins <NUM_LOGINS> \
-is-enabled true|false \
-fail-mode safe|secure
```

Cisco Duo設定の削除

Cisco Duo設定を削除すると、SSHユーザがログイン時にDuoを使用して認証する必要がなくなりま

す。Storage VM（ONTAP CLIではVserverと呼ばれます）のCisco Duo設定を削除するには、 `security login duo delete` コマンドを実行します

手順

1. SSHを使用してONTAPアカウントにログインします。
2. このStorage VMのCisco Duo設定を削除します。Storage VM名は `<STORAGE_VM_NAME>`：

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

これにより、このStorage VMのCisco Duo設定が完全に削除されます。

Cisco Duo設定の表示

Storage VM（ONTAP CLIではVserverと表示されます）の既存のCisco Duo構成を表示するには、 `security login duo show` コマンドを実行します

手順

1. SSHを使用してONTAPアカウントにログインします。
2. このStorage VMのCisco Duo設定を表示します。必要に応じて、を使用できます `vserver` Storage VMを指定するパラメータ。Storage VM名は `<STORAGE_VM_NAME>`：

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

次のような出力が表示されます。

```
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: -
```

Duoグループの作成

Cisco Duoでは、特定のActive Directory、LDAP、またはローカルユーザグループのユーザだけをDuo認証プロセスに含めるように設定できます。Duoグループを作成すると、そのグループ内のユーザーのみがDuo認証を求められます。Duoグループを作成するには、 `security login duo group create` コマンドを実行しますグループを作成するときに、必要に応じて、そのグループ内の特定のユーザーをDuo認証プロセスから除外することができます。

手順

1. SSHを使用してONTAPアカウントにログインします。
2. Duoグループを作成し、環境の情報を括弧内の値に置き換えます。を省略した場合は、 `-vserver` パラメータを指定すると、グループはクラスタレベルで作成されます。

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

   Duoグループの名前は、Active Directory、LDAP、またはローカルグループと一致している必要があります。オプションで指定するユーザ `-exclude-users` パラメータはDuo認証プロセスに含まれません。

Duoグループの表示

既存のCisco Duoグループエントリを表示するには、 `security login duo group show` コマンドを実行します

手順

1. SSHを使用してONTAPアカウントにログインします。
2. Duoグループのエントリを表示します。括弧内の値は、環境の情報に置き換えてください。を省略した場合は、 `-vserver` パラメータを指定すると、グループはクラスタレベルで表示されます。

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

   Duoグループの名前は、Active Directory、LDAP、またはローカルグループと一致している必要があります。オプションで指定するユーザ `-exclude-users` パラメータは表示されません。

Duoグループの削除

Duoグループのエントリを削除するには、 `security login duo group delete` コマンドを実行しますグループを削除すると、そのグループのユーザはDuo認証プロセスに含まれなくなります。

手順

1. SSHを使用してONTAPアカウントにログインします。
2. Duoグループエントリを削除し、環境内の情報を括弧内の値に置き換えます。を省略した場合は、 `-vserver` パラメータを指定すると、グループはクラスタレベルで削除されます。

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

Duoグループの名前は、Active Directory、LDAP、またはローカルグループと一致している必要があります。

ユーザーのDuo認証をバイパスする

すべてのユーザーまたは特定のユーザーをDuo SSH認証プロセスから除外できます。

すべてのDuoユーザーを除外

すべてのユーザに対してCisco Duo SSH認証をディセーブルにできます。

手順

1. SSHを使用してONTAPアカウントにログインします。
2. SSHユーザに対してCisco Duo認証を無効にします（SVM名をに置き換えてください）。`<STORAGE_VM_NAME>`：

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

Duoグループユーザーを除外

Duoグループの一部である特定のユーザーを、Duo SSH認証プロセスから除外できます。

手順

1. SSHを使用してONTAPアカウントにログインします。
2. グループ内の特定のユーザに対してCisco Duo認証をディセーブルにします。括弧内の値は、除外するグループ名とユーザのリストに置き換えてください。

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

Duoグループの名前は、Active Directory、LDAP、またはローカルグループと一致している必要があります。で指定するユーザ `-exclude-users` パラメータはDuo認証プロセスに含まれません。

ローカルDuoユーザを除外

Cisco Duo管理パネルを使用すると、特定のローカルユーザをDuo認証の使用から除外できます。手順については、を参照してください "Cisco Duoマニュアル"。

CA 署名済みサーバ証明書の概要を生成してインストールする

本番用システムでは、クラスタまたは SVM を SSL サーバとして認証する際に使用する CA 署名デジタル証明書をインストールすることを推奨します。を使用できます `security certificate generate-csr` 証明書署名要求（CSR）を生成するコマンドと `security certificate install` 認証局から返された証明書をインストールするコマンド。

証明書署名要求を生成します

を使用できます `security certificate generate-csr` 証明書署名要求（CSR）を生成するコマンド。要求が処理されると、署名済みのデジタル証明書が認証局（ CA ）から送信されます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

手順

1. CSR を生成します

   ```
   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
   ```

   次のコマンドでは、米国カリフォルニア州サニーベールにある企業（カスタム共通名「s erver1.companyname.com`"」）の「IT」部門の「ソフトウェア」グループが使用する、「SHA256」ハッシュ関数で生成される2、048ビット秘密鍵を使用してCSRを作成します。SVM担当管理者のEメールアドレスは「web@example.com」です。CSR と秘密鍵が出力に表示されます。

CSRの作成例

```
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
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----

Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. CSR 出力の証明書要求をデジタル形式（ E メールなど）で信頼できるサードパーティの CA に送信し、署名を求めます。

   要求が処理されると、署名済みのデジタル証明書が CA から送信されます。秘密鍵と CA 署名デジタル証明書のコピーは保管する必要があります。

CA 署名済みサーバ証明書をインストールします

を使用できます `security certificate install` CA署名済みサーバ証明書をSVMにインストールするコマンドONTAP は、サーバ証明書の証明書チェーンを形成する、認証局（ CA ）のルート証明書と中間証明書の入力を求めます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

ステップ

1. CA署名済みサーバ証明書をインストールします。

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

   コマンド構文全体については、を参照してください "ワークシート"。

   > ONTAP から、サーバ証明書の証明書チェーンを形成する CA ルート証明書と中間証明書の入力を求められます。チェーンは、サーバ証明書を発行した CA の証明書から始まり、 CA のルート証明書まで続く場合があります。中間証明書が 1 つでも抜けていると、サーバ証明書のインストールに失敗します。

   次のコマンドは、CA署名済みサーバ証明書と中間証明書をSVM「engData2」にインストールします。

CA署名済みサーバ証明書中間証明書のインストール例

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECxMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuSl8U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEAr1mnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----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+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3MgMiBDZXJ0
-----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-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----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.
```

System Manager を使用して証明書を管理します

ONTAP 9.10.1 以降では、 System Manager を使用して、信頼される認証局、クライアント / サーバ証明書、ローカル（オンボード）認証局を管理できます。

System Manager では、他のアプリケーションから受信した証明書を管理して、それらのアプリケーションからの通信を認証できます。 システムを他のアプリケーションに識別する独自の証明書を管理することもできます。

証明書情報を表示します

System Manager を使用すると、信頼された認証局、クライアント / サーバ証明書、およびクラスタに格納されているローカルの認証局を表示できます。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. [* セキュリティ * （ * Security * ）] 領域までスクロールします。
   ［ * 証明書 * ］ セクションには、次の詳細が表示されます。
   - 保存されている信頼された認証局の数。
   - 保存されているクライアント / サーバ証明書の数。
   - 保存されているローカル認証局の数。
3. 任意の数を選択して証明書のカテゴリの詳細を表示するか、 → すべてのカテゴリに関する情報を含む*証明書*ページを開きます。リストには、クラスタ全体の情報が表示されます。特定のStorage VMの情報のみを表示する場合は、次の手順を実行します。
   a. [ストレージ]>[Storage VM]*を選択します。
   b. Storage VM を選択してください。

c. [設定]タブに切り替えます。

d. [証明書]セクションに表示されている番号を選択します。

次に何をするか

- ［ * 証明書 * ］ ページでは、次の操作を実行できます [証明書署名要求を生成します]。
- 証明書の情報は、カテゴリごとに 1 つずつ、 3 つのタブに分けられます。 各タブでは、次のタスクを実行できます。

タブ	実行できる手順
• 信頼された認証機関 *	• [install-trusted-cert] • [信頼された認証局を削除します] • [信頼された認証局を更新してください]
• クライアント / サーバ証明書 *	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
• ローカル認証局 *	• [新しいローカル認証局を作成します] • [ローカルの認証局を使用して証明書に署名します] • [ローカル認証局を削除します] • [ローカルの認証局を更新してください]

証明書署名要求を生成します

証明書署名要求（ CSR ）は、 Certificate * ページの任意のタブから System Manager で生成できます。秘密鍵と対応する CSR が生成されます。これには認証局を使用して署名し、パブリック証明書を生成できます。

手順

1. ［ * 証明書 * ］ ページを表示します。 を参照してください [証明書情報を表示します]。
2. [+ CSRの生成]*を選択します。
3. 件名の情報を入力します。
   a. * 共通名 * を入力します。
   b. * 国 * を選択します。
   c. * 組織 * を入力します。
   d. * 組織単位 * を入力します。
4. デフォルト値を上書きする場合は、 * その他のオプション * を選択して追加情報を指定します。

信頼できる認証局をインストール（追加）します

System Manager に信頼された追加の認証局をインストールできます。

手順

1. [**Trusted Certificate Authorities**] タブを表示します。 を参照してください [証明書情報を表示します]。
2. を選択します + Add 。
3. [Add Trusted Certificate Authority*] パネルで、次の手順を実行します。
   - * 名 * を入力します。
   - スコープ * には、 Storage VM を選択します。
   - * 共通名 * を入力します。
   - * タイプ * を選択します。
   - 証明書の詳細を入力またはインポートします。 *

信頼された認証局を削除します

System Manager を使用して、信頼された認証局を削除できます。

ONTAPがプリインストールされている信頼された認証局は削除できません。

手順

1. [**Trusted Certificate Authorities**] タブを表示します。を参照してください [証明書情報を表示します]。
2. 信頼された認証局の名前を選択します。
3. 名前の横にあるを選択し ⋮ 、*[削除]*を選択します。

信頼された認証局を更新してください

System Manager を使用すると、有効期限が切れている、または有効期限が近づいている信頼された認証局を更新できます。

手順

1. [**Trusted Certificate Authorities**] タブを表示します。を参照してください [証明書情報を表示します]。
2. 信頼された認証局の名前を選択します。
3. 証明書名の横にあるを選択し、*更新*を選択します ⋮ 。

クライアント / サーバ証明書をインストール（追加）します

System Manager では、追加のクライアント / サーバ証明書をインストールできます。

手順

1. クライアント / サーバ証明書 * タブを表示します。 を参照してください [証明書情報を表示します]。
2. を選択します + Add 。

3. [Add Client/Server Certificate] パネルで、次の手順を実行します。
    - * 証明書名 * を入力します。
    - スコープ * には、 Storage VM を選択します。
    - * 共通名 * を入力します。
    - * タイプ * を選択します。
    - 証明書の詳細を入力またはインポートします。 *
      テキストファイルから証明書の詳細を入力またはコピーして貼り付けることも、 * Import * をクリックして証明書ファイルからテキストをインポートすることもできます。
    - 秘密鍵*を入力します。
      テキストファイルから秘密キーを入力するか、コピーして貼り付けるか、 * インポート * をクリックして秘密キーファイルからテキストをインポートすることができます。

自己署名クライアント / サーバ証明書を生成（追加）します

System Manager では、追加の自己署名クライアント / サーバ証明書を生成できます。

手順

1. クライアント / サーバ証明書 * タブを表示します。 を参照してください [証明書情報を表示します]。
2. [+自己署名証明書の生成]*を選択します。
3. 自己署名証明書の生成 * パネルで、次の手順を実行します。
    - * 証明書名 * を入力します。
    - スコープ * には、 Storage VM を選択します。
    - * 共通名 * を入力します。
    - * タイプ * を選択します。
    - * ハッシュ関数 * を選択します。
    - * キーサイズ * を選択します。
    - Storage VM * を選択します。

クライアント / サーバ証明書を削除します

System Manager では、クライアント / サーバ証明書を削除できます。

手順

1. クライアント / サーバ証明書 * タブを表示します。を参照してください [証明書情報を表示します]。
2. クライアント/サーバ証明書の名前を選択します。
3. 名前の横にあるを選択し ⋮ 、*[削除]*をクリックします。

クライアント / サーバ証明書を更新します

System Manager を使用して、有効期限が切れている、または有効期限が近づいているクライアント / サーバ証明書を更新できます。

手順

1. クライアント / サーバ証明書 * タブを表示します。 を参照してください [証明書情報を表示します]。
2. クライアント/サーバ証明書の名前を選択します。
3. 名前の横にあるを選択し ⋮ 、*更新*をクリックします。

新しいローカル認証局を作成します

System Manager を使用して、新しいローカル認証局を作成できます。

手順

1. [ローカル証明機関 *] タブを表示します。 を参照してください [証明書情報を表示します]。
2. を選択します + Add 。
3. [Add Local Certificate Authority*] パネルで、次の手順を実行します。
   - * 名 * を入力します。
   - スコープ * には、 Storage VM を選択します。
   - * 共通名 * を入力します。
4. デフォルト値を上書きする場合は、 * その他のオプション * を選択して追加情報を指定します。

ローカルの認証局を使用して証明書に署名します

System Manager では、ローカルの認証局を使用して証明書に署名できます。

手順

1. [ローカル証明機関 *] タブを表示します。 を参照してください [証明書情報を表示します]。
2. ローカル認証局の名前を選択します。
3. 名前の横にあるを選択し ⋮ 、証明書に署名。
4. [証明書署名要求に署名する *] フォームに入力します。
   - 証明書署名のコンテンツを貼り付けるか、 * Import * をクリックして証明書署名要求ファイルをインポートできます。
   - 証明書を有効にする日数を指定します。

ローカル認証局を削除します

System Manager では、ローカルの認証局を削除できます。

手順

1. [ローカル認証局] タブを表示します。 を参照してください [証明書情報を表示します]。
2. ローカル認証局の名前を選択します。
3. 名前の横にあるを選択し、*[削除]*を選択し ⋮ ます。

ローカルの認証局を更新してください

System Manager を使用して、有効期限が切れた、または有効期限が近づいているローカルの認証局を更新できます。

手順

1. [ローカル認証局] タブを表示します。を参照してください [証明書情報を表示します]。
2. ローカル認証局の名前を選択します。
3. 名前の横にあるを選択し ⋮ 、*更新*をクリックします。

Active Directory ドメインコントローラアクセスの概要を設定する

AD アカウントから SVM にアクセスするためには、 AD ドメインコントローラからクラスタまたは SVM へのアクセスを設定しておく必要があります。データ SVM 用に SMB サーバをすでに設定している場合は、クラスタへの AD アクセス用に SVM をゲートウェイまたは *tunnel* として設定できます。SMB サーバを設定していない場合は、 AD ドメインに SVM 用のコンピュータアカウントを作成できます。

ONTAP は、次のドメインコントローラ認証サービスをサポートしています。

- Kerberos
- LDAP
- Netlogon
- ローカルセキュリティ局（ LSA ）

ONTAP は、次のセッションキーアルゴリズムをサポートしており、セキュアな Netlogon 接続を実現します。

セッションキーアルゴリズム	使用可能なバージョン
HMAC-SHA256 （ Advanced Encryption Standard （ AES ）に基づく） クラスタでONTAP 9.9.1以前が実行されていて、ドメインコントローラでセキュアなネットログオンサービスにAESが適用されている場合は、接続が失敗します。この場合、代わりにONTAPとの強力なキー接続を受け入れるようにドメインコントローラを再設定する必要があります。	ONTAP 9.10.1
DES および HMAC-MD5 （強力なキーが設定されている場合）	ONTAP 9 のすべてのリリース

ネットログオンでのセキュアチャネルの確立中にAESセッションキーを使用する場合は、SVMでAESが有効になっていることを確認する必要があります。

- ONTAP 9.14.1以降では、SVMの作成時にAESがデフォルトで有効になり、ネットログオンでのセキュアチャネルの確立時にAESセッションキーを使用するようにSVMのセキュリティ設定を変更する必要はあり

ません。

- ONTAP 9.10.1~9.13.1では、SVMの作成時にAESがデフォルトで無効になります。次のコマンドを使用してAESを有効にする必要があります。

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

> ONTAP 9.14.1以降にアップグレードした場合、以前のリリースのONTAPで作成された既存のSVMのAES設定は自動的には変更されません。これらのSVMでAESを有効にするには、引き続きこの設定の値を更新する必要があります。

認証トンネルを設定します

データSVM用のSMBサーバがすでに設定されている場合は、を使用できます `security login domain-tunnel create` コマンドを使用して、SVMをADによるクラスタへのアクセス用のゲートウェイ（*tunnel*）として設定します。

作業を開始する前に

- データSVM用のSMBサーバを設定しておく必要があります。
- AD ドメインのユーザアカウントによるクラスタの管理 SVM へのアクセスを有効にしておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。

ONTAP 9.10.1 以降では、 AD アクセス用の SVM ゲートウェイ（ドメイントンネル）がある場合に、 AD ドメインで NTLM を無効にしていれば、管理認証に Kerberos を使用できます。以前のリリースでは、 SVM ゲートウェイの管理者認証で Kerberos がサポートされていませんでした。この機能はデフォルトで有効になっており、設定は必要ありません。

> Kerberos 認証は常に最初に試行されます。失敗すると、 NTLM 認証が試行されます。

ステップ

1. SMB 対応データ SVM を AD ドメインコントローラがクラスタにアクセスするための認証トンネルとして設定します。

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

   コマンド構文全体については、を参照してください "ワークシート"。

   > ユーザを認証するには、 SVM が実行されている必要があります。

   次のコマンドは、SMB対応のデータSVM「engData」を認証トンネルとして設定します。

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

ドメインに SVM コンピュータアカウントを作成します

データSVM用のSMBサーバを設定していない場合は、を使用できます `vserver active-directory create` コマンドを使用して、ドメインにSVM用のコンピュータアカウントを作成します。

このタスクについて

を入力した後 `vserver active-directory create` コマンドを実行すると、ドメイン内の指定した組織単位にコンピュータを追加するための十分な権限を持つADユーザアカウントのクレデンシャルを入力するように求められます。アカウントのパスワードは空にできません。

作業を開始する前に

このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

ステップ

1. AD ドメインに SVM 用のコンピュータアカウントを作成します。

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

   コマンド構文全体については、を参照してください "ワークシート"。

   次のコマンドは、SVM「engData」のドメイン「example.com`"」に「ADSERVER1」という名前のコンピュータアカウントを作成します。コマンドを入力すると、 AD ユーザアカウントのクレデンシャルの入力を求められます。

   ```
   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:
   ```

LDAP サーバまたは NIS サーバのアクセスの概要を設定

LDAP アカウントまたは NIS アカウントから SVM にアクセスするためには、 LDAP サーバまたは NIS サーバから SVM へのアクセスを設定しておく必要があります。スイッチ機能を使用すると、 LDAP または NIS を代替ネームサービスソースとして使用できます。

LDAP サーバアクセスを設定する

LDAP アカウントが SVM にアクセスするためには、 LDAP サーバから SVM へのアクセスを設定しておく必要があります。を使用できます `vserver services name-service ldap client create` コマンドを使用してSVMにLDAPクライアント設定を作成します。その後、を使用できます `vserver services name-service ldap create` コマンドを使用してLDAPクライアント設定をSVMに関連付けます。

このタスクについて

ほとんどの LDAP サーバでは、 ONTAP が提供する次のデフォルトスキーマを使用できます。

- MS-AD-BIS （ほとんどの Windows Server 2012 以降の AD サーバで推奨されるスキーマ）
- AD-IDMU（Windows 2008、Windows 2016、およびそれ以降のADサーバ）
- AD-SFU （ Windows Server 2003 以前の AD サーバ）
- RFC-2307 （ UNIX LDAP サーバ）

他のスキーマを使用する必要がある場合を除き、デフォルトのスキーマを使用することを推奨します。その場合は、デフォルトスキーマをコピーし、コピーを変更することによって、独自のスキーマを作成できます。詳細については、を参照してください

- "NFS構成"
- "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"

作業を開始する前に

- をインストールしておく必要があります "CA 署名済みサーバデジタル証明書" 指定します。
- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

手順

1. SVMにLDAPクライアント設定を作成します。

   ```
   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
   ```

   > Start TLS は、データ SVM へのアクセスでのみサポートされます。管理 SVM へのアクセスではサポートされません。

   コマンド構文全体については、を参照してください "ワークシート"。

   次のコマンドは、SVM「engData」上に「corp」という名前のLDAPクライアント設定を作成します。クライアントは、IPアドレスが172.160.0.100および172.16.0.101のLDAPサーバに匿名でバインドします。クライアントはRFC-2307スキーマを使用してLDAPクエリを実行します。クライアントとサーバ間の通信は Start TLS を使用して暗号化されます。

   ```
   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
   ```

> ONTAP 9.2以降では、フィールドが表示されます `-ldap-servers` フィールドを置き換えます `-servers`。この新しいフィールドには、 LDAP サーバのホスト名または IP アドレスを指定できます。

2. LDAPクライアント設定をSVMに関連付けます。 `vserver services name-service ldap create -vserver *SVM_name* -client-config *client_configuration* -client-enabled true|false`

   コマンド構文全体については、を参照してください "ワークシート"。

   次のコマンドは、LDAPクライアント設定を関連付けます `corp` SVMを使用します `engData`、SVMでLDAPクライアントを有効にします。

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

> ONTAP 9.2以降では、 `vserver services name-service ldap create` コマンドは設定の自動検証を実行し、ONTAP がネームサーバに接続できない場合はエラーメッセージを報告します。

3. vserver services name-service ldap check コマンドを使用して、ネームサーバのステータスを検証します。

   次のコマンドは、 SVM vs0 上の LDAP サーバを検証します。

```
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".                                              |
```

   ネームサービスのチェックコマンドは ONTAP 9.2 以降で使用できます。

NIS サーバアクセスの設定

NISアカウントがSVMにアクセスするためには、NISサーバからSVMへのアクセスを設定しておく必要があります。を使用できます `vserver services name-service nis-domain create` コマンドを使用してSVMにNISドメイン設定を作成します。

このタスクについて

複数の NIS ドメインを作成できます。に設定できるNISドメインは1つだけです `active` 一度に。

作業を開始する前に

- SVM に NIS ドメインを設定するためには、設定済みのすべてのサーバが使用可能でアクセスできる状態

になっている必要があります。

- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

ステップ

1. SVMにNISドメイン設定を作成します。

   `vserver services name-service nis-domain create -vserver` *`SVM_name`* `-domain client_configuration -active true|false -nis-servers` *`NIS_server_IPs`*

   コマンド構文全体については、を参照してください "ワークシート"。

   > ONTAP 9.2以降では、フィールドが表示されます `-nis-servers` フィールドを置き換えます `-servers`。この新しいフィールドには、NISサーバのホスト名またはIPアドレスを指定できます。

   次のコマンドは、SVM「engData」にNISドメイン設定を作成します。NISドメイン `nisdomain` は作成時にアクティブになり、IPアドレスが192.0.2.180のNISサーバと通信します。

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

ネームサービススイッチを作成します

ネームサービススイッチ機能を使用すると、 LDAP または NIS を代替ネームサービスソースとして使用できます。を使用できます `vserver services name-service ns-switch modify` コマンドを使用して、ネームサービスソースの参照順序を指定します。

作業を開始する前に

- LDAP サーバおよび NIS サーバのアクセスを設定しておく必要があります。
- このタスクを実行するには、クラスタ管理者または SVM 管理者である必要があります。

ステップ

1. ネームサービスソースの参照順序を指定します。

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

   コマンド構文全体については、を参照してください "ワークシート"。

   次のコマンドは、SVM「engData」上の「passwd」データベースのLDAPおよびNISネームサービスソースの検索順序を指定します。

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

管理者パスワードを変更します

初期パスワードは、システムへの初回ログイン後すぐに変更してください。SVM管理者は、を使用できます `security login password` コマンドを使用して自分のパスワードを変更します。クラスタ管理者は、を使用できます `security login password` コマンドを使用して管理者のパスワードを変更します。

このタスクについて

新しいパスワードは次のルールに従う必要があります。

- ユーザ名を含めることはできません
- 8 文字以上である必要があります
- アルファベットと数字がそれぞれ 1 文字以上含まれている必要があります
- 直近の 6 つのパスワードと同じパスワードは使用できません

> を使用できます `security login role config modify` コマンドを使用して、特定のロールに関連付けられているアカウントのパスワードルールを変更します。詳細については、を参照してください "コマンドリファレンス"。

作業を開始する前に

- 自分のパスワードを変更するには、クラスタ管理者または SVM 管理者である必要があります。
- 他の管理者のパスワードを変更するには、クラスタ管理者である必要があります。

ステップ

1. 管理者パスワードを変更します。 `security login password -vserver` *`svm_name`* `-username` *`user_name`*

   管理者のパスワードを変更するコマンドの例を次に示します `admin1` SVM用`vs1.example.com`。現在のパスワードの入力を求められたら、新しいパスワードを入力して、もう一度入力します。

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

管理者アカウントをロックおよびロック解除します

を使用できます `security login lock` 管理者アカウントをロックするコマンド、および `security login unlock` コマンドを使用してアカウントのロックを解除します。

作業を開始する前に

これらのタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 管理者アカウントをロックします。

   `security login lock -vserver SVM_name -username user_name`

   次のコマンドは、管理者アカウントをロックします `admin1` SVM用 `vs1.example.com`：

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

2. 管理者アカウントのロックを解除します。

   `security login unlock -vserver SVM_name -username user_name`

   次のコマンドは、管理者アカウントのロックを解除します `admin1` SVM用 `vs1.example.com`：

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

失敗したログインを管理します

ログイン試行が繰り返し失敗する場合、侵入者がストレージシステムへのアクセスを試みていることが疑われます。侵入を防ぐためにさまざまな対策を講じることができます。

失敗したログインを確認する方法

イベント管理システム（ EMS ）では 1 時間ごとに失敗したログイン試行を通知します。失敗したログインの記録は、で確認できます `audit.log` ファイル。

ログイン試行が繰り返し失敗する場合の対処方法

侵入を防ぐための短期的な対策としては、次のような方法があります。

- パスワードに大文字、小文字、特殊文字、数字を最低何文字か含めるように要求します
- ログインに失敗したあとに間隔を設定します
- 許容されるログイン失敗回数を制限し、指定した回数を超えたユーザをロックアウトします
- 指定した日数アクティブでないアカウントを期限切れにしてロックアウトします

を使用できます `security login role config modify` コマンドを使用してこれらのタスクを実行します。

長期的に見て、次の手順を実行することもできます。

- を使用します `security ssh modify` コマンドを使用して、新しく作成するすべてのSVMに対してログ

インの失敗回数を制限します。

- ユーザにパスワードの変更を求めることで、既存の MD5 アルゴリズムのアカウントをより安全な SHA-512 アルゴリズムに移行する。

管理者アカウントのパスワードに **SHA-2** を適用します

ONTAP 9.0 より前のバージョンで作成した管理者アカウントでは、パスワードが手動で変更されるまで、アップグレード後も引き続き MD5 パスワードが使用されます。MD5 は SHA-2 よりも安全性が低くなります。そのため、アップグレード後は、 MD5 アカウントのユーザに対してパスワードを変更してデフォルトの SHA-512 ハッシュ関数を使用するよう促す必要があります。

このタスクについて

パスワードハッシュ機能を使用すると、次の操作を実行できます。

- 指定したハッシュ関数に一致するユーザアカウントを表示する。
- 指定したハッシュ関数（ MD5 など）を使用するアカウントを期限切れにして、次回のログイン時にユーザにパスワードの変更を強制します。
- 指定したハッシュ関数を使用するパスワードが指定されたアカウントをロックする。
- ONTAP 9 より前のリリースにリバートする場合は、クラスタ管理者のパスワードを以前のリリースでサポートされているハッシュ関数（ MD5 ）と互換性があるパスワードにリセットします。

ONTAPは、NetApp Manageability SDKを使用する場合にのみ、事前にハッシュされたSHA-2パスワードを受け入れます。（`security-login-create` および `security-login-modify-password`）。

手順

1. MD5 管理者アカウントを SHA-512 パスワードハッシュ関数に移行します。

   a. すべてのMD5管理者アカウントを期限切れにします。 `security login expire-password -vserver * -username * -hash-function md5`

      これにより、 MD5 アカウントのユーザは、次回のログイン時にパスワードの変更が必要になります。

   b. MD5 アカウントのユーザに、コンソールまたは SSH セッションを使用してログインするよう依頼します。

      アカウントの有効期限が切れていることが検出され、ユーザにパスワードの変更を求めるメッセージが表示されます。変更されたパスワードでは、デフォルトで SHA-512 が使用されます。

2. ユーザが一定期間ログインしていないためにパスワードが変更されない MD5 アカウントについては、強制的にアカウントを移行します。

   a. まだMD5ハッシュ関数を使用しているアカウントをロックします（advanced権限レベル）。 `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

      で指定した日数が経過した後 `-lock-after`ユーザーはMD5アカウントにアクセスできません。

   b. ユーザがパスワードを変更する準備ができたら、アカウントのロックを解除します。 `security`

```
login unlock -vserver svm_name -username user_name
```

c. ユーザに、コンソールまたは SSH セッションからアカウントにログインし、表示される指示に従ってパスワードを変更するよう促します。

ファイルアクセスの問題を診断して修正

手順

1. System Manager で、 * Storage > Storage VM* を選択します。
2. トレースを実行する Storage VM を選択してください。
3. [詳細]*をクリックします ⋮ 。
4. ファイルアクセスのトレース * をクリックします。
5. ユーザー名とクライアントの IP アドレスを入力し、 * トレースを開始 * をクリックします。

   トレース結果が表形式で表示されます。 [* 理由] 列には、ファイルにアクセスできなかった理由が表示されます。

6. 結果テーブルの左側の列をクリック ⌄ すると、ファイルアクセス権限が表示されます。