管理者アカウントの管理
ONTAP 9

NetApp
December 20, 2024

目次

管理者アカウントの管理 . . . 1
- 管理者アカウントの管理の概要 . . . 1
- 管理者アカウントに公開鍵を関連付ける . . . 1
- 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。 . . . 2
- ONTAPを使用したSSHログイン用のCisco Duo 2FAの設定 . . . 4
- CA署名済みサーバ証明書の生成とインストールの概要 . . . 9
- System Managerを使用した証明書の管理 . . . 13
- Active Directoryドメインコントローラアクセスの設定の概要 . . . 18
- LDAPサーバまたはNISサーバのアクセス設定の概要 . . . 20
- ONTAPでの管理者パスワードの変更 . . . 23
- 管理者アカウントのロックとロック解除 . . . 24
- 失敗したログインを管理します。 . . . 25
- 管理者アカウントパスワードに対するSHA-2の適用 . . . 25
- ファイルアクセスの問題を診断して修正する . . . 26

管理者アカウントの管理

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る

SSH公開鍵認証を使用する場合、アカウントがSVMにアクセスする前に、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。管理者アカウントにキーを関連付けるには、コマンドを使用し `security login publickey create`ます。

タスクの内容

パスワードとSSH公開鍵の両方を使用してSSH経由でアカウントを認証する場合、アカウントは最初に公開鍵で認証されます。

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の `engData1`SVM管理者アカウントに公開鍵を関連付け `svmadmin1`ます。公開鍵にはインデックス番号5が割り当てられます。

```
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ために、一連のコマンドを使用して、SSH公開鍵とそのX.509証明書との関連付けを管理でき `security login publickey`ます。

公開鍵とX.509証明書を管理者アカウントに関連付ける

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。

タスクの内容

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。

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。
  - 証明書チェーン（中間およびルートのCA証明書）は、コマンドを使用してインストールする必要があります `security certificate install`。
  - SSHに対してOCSPを有効にする必要があります。手順については、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する" 。

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の `engData2`SVM管理者アカウントに関連付け `svmadmin2`ます。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する

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。

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、インデックス番号6のSVMのSVM `engData2`管理者アカウントから`X.509`証明書の関連付けを削除します `svmadmin2`。

```
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する

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。

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、インデックス番号7のSVMの `engData3`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。

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

ONTAPを使用した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、デフォルトですべてのユーザアカウントに適用されます。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を参照して"登録に関するドキュメント"ください。

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

コマンドを使用して、クラスタ全体または特定のStorage VM（ONTAP CLIではVserver）に対してCisco Duo構成を作成できます[`security login duo create`。これにより、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。リンクhttps://docsの詳細については、『ONTAPコマンドリファレンス』を参照してください。NetApp .com /us-en/ ONTAP -CLI// security-login-duo-create.html[`security login duo create`^]コマンドを参照してください。

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、環境からの情報を角かっこ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>
```

コマンドの詳細については、を"カンリシヤニンシヨウトRBACセツテイヨウノワアクシイト"参照してください。

Cisco Duo設定の変更

Cisco Duoがユーザーを認証する方法を変更できます(たとえば、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)。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、コマンドを使用できます[`security login duo modify`。リンクhttps://docsの詳細については、『ONTAPコマンドリファレンス』を参照してください。NetApp .com /us-en/ ONTAP -CLI// security-login-duo-modify.html[`security login duo modify`^]コマンドを参照してください。

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設定を変更し、環境で更新された情報を角かっこ内の値に置き換えます。

```
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、ログイン時にSSHユーザが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と表示されます）のCisco Duo設定を削除するには、コマンドを使用し[security login duo delete`ます。リンクhttps://docsの詳細については、『ONTAPコマンドリファレンス』を参照してください。NetApp .com /us-en/ ONTAP -CLI// security-login-duo-delete.html[`security login duo delete^]コマンドを参照してください。

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、Storage VM名をに置き換えて `<STORAGE_VM_NAME>`ください：

```
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設定を表示するには、コマンドを使用し[security login duo show`ます。リンクhttps://docsの詳細については、『ONTAPコマンドリファレンス』を参照してください。NetApp .com /us-en/ ONTAP -CLI// security-login-duo-show.html[`security login duo show^]コマンドを参照してください。

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、パラメータを使用してStorage VMを指定できます vserver。Storage VM名はに置き換えてください。 <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ーグループのユーザーのみを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グループは、コマンドを使用して作成できます[`security login duo group create`。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。リンクhttps://docsの詳細については、『ONTAPコマンドリファレンス』を参照してください。NetApp .com /us-en/ ONTAP -CLI// security-login-duo-group-create.html[`security login duo group create`^]コマンドを参照してください。

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。パラメータを省略する `-vserver`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。オプションのパラメータで指定したユーザは `-exclude-users`、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、コマンドを使用し[`security login duo group show`ます。リンクhttps://docsの詳細については、『ONTAPコマンドリファレンス』を参照してください。NetApp .com /us-en/ ONTAP -CLI// security-login-duo-group-show.html[`security login duo group show`^]コマンドを参照してください。

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。パラメータを省略すると、 `-vserver`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。オプションのパラメータで指定したユーザ `-exclude-users`は表示されません。

Duoグループの削除

Duoグループエントリを削除するには、コマンドを使用し[`security login duo group delete`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。リンクhttps://docsの詳細については、『ONTAPコマンドリファレンス』を参照してください。NetApp .com /us-en/ ONTAP -CLI// security-login-duo-group-delete.html[`security login duo group delete^]コマンドを参照してください。

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。パラメータを省略すると、 `-vserver`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認証を無効に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. SSHユーザのCisco Duo認証を無効にし、SVM名をに置き換え `<STORAGE_VM_NAME>`ます。

```
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ーに対してCisco Duo認証を無効にします。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。パラメータで指定したユーザは `-exclude-users`、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ーを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 "Cisco Duoマニュアル"ください。

CA署名済みサーバ証明書の生成とインストールの概要

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。コマンドを使用してCertificate Signing Request（CSR；証明書署名要求）を生成し、 `security certificate install`コマンドを使用して認証局から返された証明書をインストールできます `security certificate generate-csr`。

証明書署名要求を生成する

証明書署名要求（CSR）は、コマンドを使用して生成できます `security certificate generate-csr`。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。

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「server1.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。出力にCSRと秘密鍵が表示されます。

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

2. CSR出力の証明書要求を電子形式（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を保管しておく必要があります。

CA署名済みサーバ証明書のインストール

CA署名済みサーバ証明書は、コマンドを使用してSVMにインストールできます `security certificate install`。ONTAPでは、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

書の入力を求められます。

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は、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の範囲があります。中間証明書が不足していると、サーバ証明書のインストールが失敗します。

   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を使用した証明書の管理

System.10.1以降では、ONTAP 9 Managerを使用して、信頼された認証局、クライアント/サーバ証明書、およびローカル（オンボード）の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け取っ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。また、他のアプリケーションに対してシステムを識別する独自の証明書を管理することもできます。

証明書情報の表示

System Managerでは、クラスタに格納されている信頼された認証局、クライアント/サーバ証明書、および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を選択します。

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。

次の手順

- [証明書]ページでは、次のことができます[証明書署名要求を生成する]。
- 証明書情報は、カテゴリごとに1つずつ、3つのタブに分かれています。各タブから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。] • [信頼された認証局の更新]
• 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。] • [ローカル認証局を使用して証明書に署名する] • [ローカル認証局を削除します。] • [ローカル認証局の更新]

証明書署名要求を生成する

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、認証局を使用して署名して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 [証明書情報の表示]
2. [+ CSRの生成]*を選択します。
3. サブジェクト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。

信頼された認証局のインストール（追加）

信頼された追加の認証局をSystem Managerに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 [証明書情報の表示]
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では、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 [証明書情報の表示]
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。

信頼された認証局の更新

System Managerでは、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 [証明書情報の表示]
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/サーバ証明書のインストール（追加）

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 [証明書情報の表示]
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）する

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 [証明書情報の表示]
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する

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 [証明書情報の表示]
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/サーバ証明書の更新

System Managerでは、期限切れまたはまもなく期限切れになるクライアント/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 [証明書情報の表示]
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では、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 [証明書情報の表示]
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。

ローカル認証局を使用して証明書に署名する

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 [証明書情報の表示]
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。
   - 証明書が有効にな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 [証明書情報の表示]
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。

ローカル認証局の更新

System Managerでは、有効期限が切れている、または有効期限が近づいているローカル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 [証明書情報の表示]
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設定の概要

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
- Local Security Authority（LSA）

ONTAPでは、セキュアなNetlogon接続を実現するために次のセッション キー アルゴリズムがサポートされます。

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以前を実行していて、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）	すべてのONTAP 9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。

- 14.1以降では、ONTAP 9の作成時にデフォルトでAESが有効になり、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。

認証トンネルの設定

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

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 アカウントにクラスタの管理SVMへのアクセスを許可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。

10.1以降では、**AD**アクセス用のゲートウェイ（ドメイントンネル）がある場合、**AD**ドメインで**ONTAP 9**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認証で**Kerberos**は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使用できます。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。失敗した場合は、NTLM認証が試行されます。

ステップ

1. SMB対応のデータ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する

データSVM用のSMBサーバを設定していない場合は、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できます `vserver active-directory create`。

タスクの内容

コマンドを入力すると `vserver active-directory create`、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Privileges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を空にすることはできません。

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サーバのアクセス設定の概要

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 アクセスの設定

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。コマンドを使用すると、SVMにLDAPクライアント設定を作成できます `vserver services name-service ldap client create`。その後、コマンドを使用し `vserver services name-service ldap create`て、LDAPクライアント設定をSVMに関連付けます。

タスクの内容

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

- MS-AD-BIS（Windows Server 2012以降のほとんどの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 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ないかぎり、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、デフォルトのスキーマをコピーしてコピーを変更することで、独自のスキーマを作成できます。詳細については、次を参照してください。

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

開始する前に

- SVMにをインストールしておく必要があり"CA 署名済みサーバデジタル証明書"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。

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に `engData`という名前のLDAPクライアント設定を作成し `corp`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、 `-ldap-servers`フィールドがフィールドに置き換わります `-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SVMに `engData`関連付け `corp`、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`、コマンドによって設定の自動検証が実行され、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が報告されます。

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。SVMにNISドメイン設定を作成するには、コマンドを使用し `vserver services name-service nis-domain create`ます。

開始する前に

- SVMにNISドメインを設定するには、設定済みのすべてのサーバが使用可能でアクセス可能である必要があります。
- 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> -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、 `-nis-servers`フィールドがフィールドに置き換わります `-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にNISドメイン設定を作成し `engData`ます。`NIS`ドメインは `nisdomain`、IPアドレスを使用してNISサーバと通信し `192.0.2.180`ます。

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

ネームサービススイッチを作成する

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。コマンドを使用すると、ネームサービスソースの参照順序を指定できます `vserver services name-service ns-switch modify`。

開始する前に

- LDAPサーバと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検索順序を指定します。

   ```
   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上のデータベース `engData`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 `passwd`。

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

ONTAPでの管理者パスワードの変更

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、コマンドを使用して自分のパスワードを変更できます `security login password`。クラスタ管理者は、コマンドを使用して管理者のパスワードを変更できます `security login password`。

タスクの内容

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。
- 英文字と数字がそれぞれ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。

> コマンドを使用すると、指定したロールに関連付けられたアカウントのパスワードルールを変更できます[`security login role config modify`。リンクhttps://docsの詳細については、ONTAPコマンドリファレンスを参照してください。NetApp .com /us-en/ ONTAP -CLI/security-login-role-config-modify.html[`security login role config modify`^]コマンドを参照してください。

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`*

   次のコマンドは、SVMの`vs1.example.com`管理者のパスワードを変更し `admin1`ます。プロンプトが表示されたら、現在のパスワードを入力し、新しいパスワードを入力して再入力します。

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

管理者アカウントのロックとロック解除

コマンドを使用して管理者アカウントをロックし、 `security login unlock`コマンドを使用してアカウントのロックを解除でき `security login lock`ます。

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、SVMの管理者アカウントをロックし `admin1`` vs1.example.com`ます。

   ```
   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、SVMの管理者アカウントのロックを解除し `admin1`vs1.example.comます。

```
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ファイルで確認できます `audit.log`。

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

これらのタスクは、コマンドを使用して実行できます `security login role config modify`。

長期的に見て、次の手順を実行することもできます。

- 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するには、コマンドを使用し `security ssh modify`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。

管理者アカウントパスワードに対する**SHA-2**の適用

ONTAP 9 .0より前に作成した管理者アカウントは、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パスワードを使用します。MD5はSHA-2より安全ではありません。そのため、アップグレード後は、MD5アカウントのユーザに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に指示する必要があります。

タスクの内容

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します。
- 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、ユーザが次回ログイン時にパスワードを変更するように強制します。
- 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よりも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および `security-login-modify-password`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(`security-login-create`ます）。

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アカウントユーザは次回ログイン時にパスワードを変更する必要があります。

   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に依頼します。

      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プロンプトが表示されます。変更されたパスワードには、デフォルトでSHA-512が使用されます。

2. 一定時間内にユーザがログインしてパスワードを変更しないMD5アカウントの場合は、アカウントを強制的に移行します。
   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する `-lock-after`と、ユーザはMD5アカウントにアクセスできなくなります。

   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、プロンプトが表示されたらパスワードを変更してもらいます。

ファイルアクセスの問題を診断して修正する

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を選択します。
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。

著作権に関する情報

商標に関する情報