



管理者認証と**RBAC**の管理

ONTAP 9

NetApp
February 12, 2026

目次

管理者認証とRBACの管理	1
ONTAPの管理者認証とRBACについて学ぶ	1
ONTAP管理者認証とRBACワークフロー	1
ONTAP管理者認証とRBAC設定のためのワークシート	2
ログイン アカountの作成または変更	2
Cisco Duoセキュリティ情報の設定	5
カスタム ロールの定義	8
ユーザ アカountへの公開鍵の関連付け	10
動的許可グローバル設定の構成	11
CA署名済みサーバ デジタル証明書のインストール	13
Active Directoryドメイン コントローラ アクセスの設定	14
LDAPサーバまたはNISサーバのアクセスの設定	15
SAMLアクセスの設定	17
ログイン アカountの作成	18
ONTAPログイン アカountの作成について学ぶ	18
ローカル アカount アクセスの有効化	19
Active Directory ONTAPアカountアクセスを有効にする	31
LDAPまたはNIS ONTAPアカountアクセスを有効にする	33
アクセス制御ロールの管理	35
ONTAPアクセス制御ロールの管理について学ぶ	35
ONTAP管理者に割り当てられたロールを変更する	35
ONTAP管理者のカスタムロールを定義する	36
ONTAPクラスタ管理者向けの定義済みロール	37
ONTAP SVM管理者向けの定義済みロール	40
System ManagerでONTAP管理者アクセスを管理する	41
ONTAPでのJITアクセス権限昇格	42
ONTAPでのジャストインタイム権限昇格の設定	43
管理者アカountの管理	48
ONTAP管理者アカountの管理について学ぶ	49
公開キーをONTAP管理者アカountに関連付ける	49
ONTAP管理者のSSH公開鍵とX.509証明書を管理する	50
ONTAP SSH ログイン用に Cisco Duo 2FA を設定する	52
ONTAPでCA署名付きサーバ証明書を生成してインストールする	57
System ManagerでONTAP証明書を管理する	61
ONTAPでActive Directoryドメイン コントローラ アクセスを設定する	65
ONTAPでLDAPサーバまたはNISサーバ アクセスを設定	68
ONTAP管理者パスワードを変更する	71
ONTAP管理者アカountのロックとロック解除	72
ONTAPでログイン試行の失敗を管理する	73

ONTAP管理者アカウントのパスワードにSHA-2を適用する	74
System Manager を使用して ONTAP ファイル アクセスの問題を診断および修正する	75
マルチ管理者認証の管理	75
ONTAPマルチ管理者検証について学ぶ	75
MAVのONTAP管理者承認グループを管理する	92
ONTAPでマルチ管理者検証を有効または無効にする	95
ONTAPで保護された操作のマルチ管理者検証ルールを管理する	99
ONTAPでMAV保護された操作の実行をリクエストする	101
ONTAPでMAV保護操作リクエストを管理する	104
動的許可の管理	109
ONTAP動的認証について学ぶ	109
ONTAPでの動的認可の有効化または無効化	110
ONTAPでの動的認可のカスタマイズ	112

管理者認証とRBACの管理

ONTAPの管理者認証とRBACについて学ぶ

ONTAPのクラスタ管理者およびStorage Virtual Machine (SVM) 管理者のログイン アカウントを有効にすることができます。管理者が実行できる機能をロールベース アクセス制御 (RBAC) を使用して定義することもできます。

ローカルの管理者アカウントには、次の種類の認証を使用した管理Storage Virtual Machine (SVM) またはデータSVMへのアクセスを許可できます。

- "パスワード"
- "SSH公開鍵"
- "SSL証明書"
- "SSH多要素認証 (MFA) "

ONTAP 9.3以降では、パスワードと公開鍵による認証がサポートされています。

リモートの管理者アカウントには、次の種類の認証を使用した管理SVMまたはデータSVMへのアクセスを許可できます。

- "Active Directory"

ONTAP 9.13.1以降では、Active Directoryユーザのプライマリ認証方式またはセカンダリ認証方式としてSSH公開キーを使用できます。

- "SAML認証 (管理SVMのみ) "

ONTAP 9.3以降では、Service Processor Infrastructure、ONTAP API、またはSystem Managerのいずれかのwebサービスを使用して管理SVMにアクセスするために、Security Assertion Markup Language (SAML) 認証を使用できます。

- "LDAP または NIS"

ONTAP 9.4以降では、LDAPサーバまたはNISサーバ上のリモート ユーザにSSH MFAを使用できます。nsswitchと公開鍵による認証がサポートされます。

ONTAP管理者認証とRBACワークフロー

ローカルまたはリモートの管理者アカウントに対して認証を有効にすることができます。ローカル アカウントのアカウント情報はストレージ システムに、リモート アカウントのアカウント情報はストレージ システム以外の場所に格納されます。それぞれのアカウントに事前定義またはカスタムのロールを割り当てることができます。

1

構成ワークシートに記入する

ログイン アカウントを作成し、ロールベースアクセス制御（RBAC）を設定する前に、**"設定ワークシート"**内の各項目に関する情報を収集する必要があります。

2

管理者アカウントがローカルかリモートかを判断する

- ローカルの場合：**"password"**、**"SSH"**、**"SSH MFA"**、または**"SSL"**アクセスを有効にします。
- リモートの場合： リモートアクセスの種類を決定します。アクセスの種類に応じて、**"Active Directory アクセスを有効にする"**、**"LDAPまたはNISアクセスを有効にする"**、または**"SAML認証を構成する（admin SVMのみ）"**。

3

ロールベースアクセスを設定する

管理者に割り当てられたロールによって、管理者がアクセスできるコマンドが決まります。ロールは管理者アカウントの作成時に割り当てられ、**"modified"**することができます。**"cluster"**および**"SVM"**管理者用の事前定義されたロールを使用するか、必要に応じて**"カスタムロールを定義する"**することができます。

4

管理者アカウントを管理する

アカウントアクセスの有効化方法によっては、**"ローカルアカウントの公開鍵"**の関連付け、**"公開鍵とX.509証明書"**の管理、**"SSHログイン用のCisco Duo 2FA"**の設定、**"CA署名付きサーバ デジタル証明書"**のインストール、または**"Active Directory"**、**"LDAPまたはNIS"**アクセスの設定が必要になる場合があります。これらのタスクは、アカウントアクセスの有効化前でも有効化後でも実行できます。

5

追加のセキュリティ機能を設定する

- "マルチ管理者認証の管理"**特定の操作に指定された管理者からの承認が必要であることを確認したい場合。
- "動的許可の管理"**ユーザーの信頼レベルに基づいて追加の認可チェックを動的に適用する場合。
- "タイミングよく（JIT） 権限昇格を構成する"**ユーザーが特定のタスクを実行するために一時的に昇格された権限にアクセスできるようにする場合。

ONTAP管理者認証とRBAC設定のためのワークシート

ログイン アカウントを作成してロールベース アクセス制御（RBAC）を設定する前に、設定ワークシートの各項目について情報を収集しておく必要があります。

この手順で説明されているコマンドの詳細については、**"ONTAPコマンド リファレンス"**を参照してください。

ログイン アカウントの作成または変更

ストレージVMにアクセスするログインアカウントを有効にする際に、``security login create`` コマンドでこれらの値を指定します。**"ONTAPコマンド リファレンス"**の ``security login create``の詳細を確認してください。

`security login modify`コマンドでアカウントのストレージ VMへのアクセス方法を変更する場合も、同じ値を指定します。link:<https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html>["ONTAPコマンド リファレンス"^]の`security login modify`の詳細をご覧ください。

フィールド	概要	あなたの価値
-vserver	アカウントがアクセスするStorage VMの名前。デフォルト値はクラスタの管理Storage VMの名前です。	
-user-or-group-name	アカウントのユーザ名またはグループ名。グループ名を指定した場合、そのグループ内の各ユーザのアクセスが有効になります。1つのユーザ名またはグループ名を複数のアプリケーションに関連付けることができます。	
-application	Storage VMへのアクセスに使用するアプリケーション。 <ul style="list-style-type: none">• http• ontapi• snmp• ssh	

-authmethod	<p>アカウントの認証に使用する認証方式。</p> <ul style="list-style-type: none"> • `cert` SSL証明書認証用 • domain Active Directory認証用 • nsswitch LDAP または NIS 認証用 • `password` ユーザーパスワード認証用 • `publickey` 公開鍵認証用 • community SNMP コミュニティ文字列用 • usm SNMP ユーザーセキュリティモデル用 • saml for Security Assertion Markup Language (SAML) 認証 	
-remote-switch-ipaddress	<p>リモートスイッチのIPアドレス。リモートスイッチは、クラスタスイッチヘルスマニタ (CSHM) によって監視されるクラスタスイッチ、またはMetroClusterヘルスマニタ (MCC-HM) によって監視されるファイバチャネル (FC) スイッチです。このオプションは、アプリケーションが `snmp` で、認証方法が `usm` の場合にのみ適用されます。</p>	
-role	<p>アカウントに割り当てられているアクセス制御ロール。</p> <ul style="list-style-type: none"> • クラスタ (管理ストレージ VM) の場合、デフォルト値は `admin` です。 • データ ストレージ VM の場合、デフォルト値は `vsadmin` です。 	
-comment	<p>(オプション) アカウントについての説明。テキストを二重引用符 (") で囲む必要があります。</p>	

-is-ns-switch-group	アカウントがLDAP グループアカウントであるか、NIS グループアカウントであるか(yes または no)。	
-second-authentication-method	<p>多要素認証を使用する場合の、第2の認証方式。</p> <ul style="list-style-type: none"> • none 多要素認証を使用しない場合はデフォルト値 • publickey 公開鍵認証の場合、authmethod が password または nsswitch のとき • password authmethod が公開鍵の場合のユーザーパスワード認証用 • nsswitch authmethod が publickey の場合のユーザーパスワード認証用 <p>認証の順序は、常に公開鍵が先でパスワードがあとです。</p>	
-is-ldap-fastbind	<p>ONTAP 9.11.1 以降、true に設定すると nsswitch 認証のための LDAP ファストバインドが有効になります。デフォルトは false です。LDAP ファストバインドを使用するには、-authentication-method 値を nsswitch に設定する必要があります。"ONTAP NFS SVMのnsswitch認証にLDAP高速バインドを使用する"。</p>	

Cisco Duoセキュリティ情報の設定

ストレージVMのSSHログインでCisco Duoの2要素認証を有効にする際に、security login duo create コマンドでこれらの値を指定します。["ONTAPコマンド リファレンス"](#)の security login duo create の詳細をご覧ください。

フィールド	概要	あなたの価値
-vserver	Duo認証設定を適用するStorage VM (ONTAP CLIではvserver)。	
-integration-key	DuoにSSHアプリケーションを登録するときに取得した統合キー。	

-secret-key	DuoにSSHアプリケーションを登録するときに取得したシークレットキー。	
-api-host	<p>SSHアプリケーションをDuoに登録する際に取得したAPIホスト名。 例：</p> <pre>api- <HOSTNAME>.duosecurity.com</pre>	
-fail-mode	<p>Duo認証を妨げるサービス エラーまたは設定エラーが発生した場合、fail safe（アクセスを許可）または secure（アクセスを拒否）します。デフォルトは`safe`で、Duo APIサーバにアクセスできないなどのエラーによりDuo認証が失敗した場合、Duo認証はバイパスされます。</p>	
-http-proxy	<p>指定されたHTTPプロキシを使用します。HTTPプロキシで認証が必要な場合は、プロキシURLに認証情報を含めます。例：</p> <pre>http- proxy=http://username :password@proxy.example.org:8080</pre>	

-autopush

`true`または
`false`。デフォルトは
`false`です。
`true`の場合、Duoは自動
的にユーザーの携帯電話にプ
ッシュログインリクエストを
送信し、プッシュが利用でき
ない場合は通話に戻ります。
これにより、パスコード認証
が実質的に無効になることに
注意してください。
`false`の場合、ユーザー
は認証方法を選択するよう求
められます。

`autopush` =
`true`で設定する場合は、
`max-prompts` =
`1`を設定することをお勧め
します。

-max-prompts	<p>ユーザーが2要素認証に失敗した場合、Duoはユーザーに再度認証を求めます。このオプションは、アクセスを拒否する前にDuoが表示するプロンプトの最大数を設定します。1、2、または`3`である必要があります。デフォルト値は`1`です。</p> <p>たとえば、`max-prompts = 1`の場合、ユーザーは最初のプロンプトで正常に認証される必要がありますが、`max-prompts = 2`の場合、ユーザーが最初のプロンプトで誤った情報を入力すると、再度認証するように求められます。</p> <div data-bbox="591 688 1029 940" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <pre>`autopush = true`で設定する場合は、 `max-prompts = 1`を設定することをお勧め します。</pre> </div> <p>最適なエクスペリエンスを得るには、公開鍵認証のみを使用するユーザーは常に`max-prompts`を`1`に設定します。</p>	
-enabled	<p>Duo 2要素認証を有効にします。デフォルトでは`true`に設定されています。有効にすると、SSHログイン時に設定されたパラメータに従ってDuo 2要素認証が強制されます。Duoが無効（`false`に設定）の場合、Duo認証は無視されます。</p>	
-pushinfo	<p>アクセスしているアプリケーションやサービスの名前など、プッシュ通知に追加情報を提供するためのオプションです。これにより、ユーザは正しいサービスにログインしていることを確認でき、セキュリティを強化できます。</p>	

カスタム ロールの定義

カスタム ロールを定義する際に、`security login role create` コマンドでこれらの値を指定します。["ONTAP コマンド リファレンス"](#)の`security login role create`の詳細を確認してください。

フィールド	概要	あなたの価値
-vserver	(オプション) ロールに関連付けられているStorage VM (ONTAP CLIではvserver) の名前。	
-role	ロールの名前。	
-cmddirname	ロールがアクセスを許可するコマンドまたはコマンド ディレクトリ。コマンド サブディレクトリ名は二重引用符 (") で囲む必要があります。例: "volume snapshot" すべてのコマンド ディレクトリを指定するには、`DEFAULT` と入力する必要があります。	
-access	<p>(オプション) ロールのアクセスレベル。コマンド ディレクトリの場合:</p> <ul style="list-style-type: none"> • none (カスタム ロールのデフォルト値) は、コマンド ディレクトリ内のコマンドへのアクセスを拒否します • `readonly` は、`show` コマンド ディレクトリとそのサブディレクトリ内のコマンドへのアクセスを許可します • `all` コマンド ディレクトリとそのサブディレクトリ内のすべてのコマンドへのアクセスを許可します <p>非固有コマンド (create、modify、delete、または `show` で終わらないコマンド) の場合:</p> <ul style="list-style-type: none"> • none (カスタム ロールのデフォルト値) は、コマンドへのアクセスを拒否します • `readonly` は該当なし • `all` コマンドへのアクセスを許可します <p>組み込みコマンドへのアクセスを許可または拒否するには、コマンド ディレクトリを指定する必要があります。</p>	

-query	(オプション) アクセスレベルをフィルタリングするために使用されるクエリ オブジェクト。コマンドまたはコマンド ディレクトリ内のコマンドの有効なオプションの形式で指定されます。クエリ オブジェクトは二重引用符 (") で囲む必要があります。たとえば、コマンド ディレクトリが `volume` の場合、クエリ オブジェクト <code>"-aggr aggr0"</code> は <code>aggr0</code> アグリゲートへのアクセスのみを有効にします。	
--------	--	--

ユーザ アカウントへの公開鍵の関連付け

``security login publickey create`` コマンドでSSH公開鍵をユーザ アカウントに関連付ける際に、これらの値を指定します。link:<https://docs.netapp.com/us-en/ontap-cli/security-login-publickey-create.html>["ONTAP コマンド リファレンス"]の ``security login publickey create`` の詳細を確認してください。

フィールド	概要	あなたの価値
-vserver	(オプション) アカウントがアクセスするStorage VMの名前。	
-username	アカウントのユーザー名。デフォルト値 (admin) は、クラスタ管理者のデフォルト名です。	
-index	公開鍵のインデックス番号。デフォルト値は、アカウントに対して最初に作成された鍵では0、それ以外の場合は既存の一番大きいインデックス番号に1を加えた値です。	
-publickey	OpenSSH公開鍵。鍵は二重引用符 (") で囲む必要があります。	
-role	アカウントに割り当てられているアクセス制御ロール。	
-comment	(オプション) 公開鍵についての説明。テキストを二重引用符 (") で囲む必要があります。	

-x509-certificate	<p>(オプション) ONTAP 9.13.1以降では、X.509証明書とSSH公開鍵の関連付けを管理できます。</p> <p>X.509証明書をSSH公開鍵に関連付けると、証明書が有効かどうかをSSHログイン時にONTAPがチェックします。証明書の有効期限が切れている、または証明書が失効している場合、ログインは許可されず、関連付けられているSSH公開鍵は無効になります。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> • <code>install</code>：指定されたPEMエンコードされたX.509証明書をインストールし、SSH公開鍵に関連付けます。インストールする証明書の全文を含めてください。 • <code>modify</code>：既存のPEMエンコードされたX.509証明書を指定された証明書に更新し、SSH公開鍵に関連付けます。新しい証明書の全文を含めてください。 • <code>delete</code>：SSH公開キーと関連付けられた既存のX.509証明書を削除します。 	
-------------------	---	--

動的許可グローバル設定の構成

ONTAP 9.15.1以降では、`security dynamic-authorization modify` コマンドでこれらの値を指定します。["ONTAPコマンド リファレンス"](#)の`security dynamic-authorization modify`の詳細を確認してください。

フィールド	概要	あなたの価値
-vserver	信頼スコア設定を変更するストレージVMの名前。このパラメータを省略すると、クラスターレベルの設定が使用されます。	

-state	<p>動的認証モード。可能な値：</p> <ul style="list-style-type: none"> • disabled：（デフォルト）動的認証は無効です。 • visibility：このモードは、動的な認可のテストに役立ちます。このモードでは、制限されたアクティビティごとに信頼スコアがチェックされますが、強制はされません。ただし、拒否されるか追加の認証チャレンジの対象となるアクティビティはすべてログに記録されます。 • enforced：`visibility`モードでのテストを完了した後に使用してください。このモードでは、制限されたアクティビティごとに信頼スコアがチェックされ、制限条件が満たされた場合にアクティビティ制限が適用されます。また、抑制間隔も適用され、指定された間隔内で追加の認証チャレンジが防止されます。 	
-suppression-interval	<p>指定された間隔内で追加の認証チャレンジを防止します。間隔はISO-8601形式で、1分から1時間までの値を指定できます。0に設定すると、抑制間隔は無効になり、必要な場合は常にユーザーに認証チャレンジが求められます。</p>	
-lower-challenge-boundary	<p>多要素認証（MFA）チャレンジの下限パーセンテージです。有効範囲は0～99です。値100は、すべてのリクエストが拒否されるため無効です。デフォルト値は0です。</p>	
-upper-challenge-boundary	<p>MFAチャレンジの上限パーセンテージです。有効範囲は0～100です。下限値以上である必要があります。100を指定すると、すべてのリクエストが拒否されるか、追加の認証チャレンジが課されます。チャレンジなしで許可されるリクエストはありません。デフォルト値は90です。</p>	

CA署名済みサーバ デジタル証明書のインストール

``security certificate generate-csr`` コマンドでストレージVMをSSLサーバとして認証する際に使用するデジタル証明書署名要求 (CSR) を生成する際に、これらの値を指定します。link:<https://docs.netapp.com/us-en/ontap-cli/security-certificate-generate-csr.html> ["ONTAP コマンド リファレンス"] の ``security certificate generate-csr`` の詳細を確認してください。

フィールド	概要	あなたの価値
<code>-common-name</code>	証明書の名前。完全修飾ドメイン名 (FQDN) またはカスタム共通名を指定できます。	
<code>-size</code>	秘密鍵のビット数。値が大きいほど、鍵のセキュリティは高くなります。デフォルト値は 2048 です。指定できる値は `512`、`1024`、`1536`、`2048` です。	
<code>-country</code>	ストレージVMの国名 (2文字コード)。デフォルト値は `US` です。コードの一覧については、" ONTAP コマンド リファレンス "を参照してください。	
<code>-state</code>	Storage VMが設置されている都道府県。	
<code>-locality</code>	Storage VMが設置されている市区町村。	
<code>-organization</code>	Storage VMを管理している組織。	
<code>-unit</code>	Storage VMを管理している組織内の部門。	
<code>-email-addr</code>	Storage VMの管理担当者のEメール アドレス。	
<code>-hash-function</code>	証明書に署名するための暗号ハッシュ関数。デフォルト値は <code>SHA256`</code> です。指定できる値は <code>`SHA1`</code> 、 <code>SHA256`</code> 、 <code>`MD5`</code> です。	

```
`security certificate
install`コマンドでこれらの値を指定します。このコマンドは、クラスタまたはストレージVMをSSLサーバとして認証するために使用するCA署名デジタル証明書をインストールする際に使用します。次の表には、アカウント設定に関連するオプションのみが表示されています。link:https://docs.netapp.com/us-en/ontap-cli/security-certificate-install.html["ONTAPコマンド リファレンス"]の`security certificate install`の詳細を確認してください。
```

フィールド	概要	あなたの価値
-vserver	証明書をインストールするStorage VMの名前。	
-type	証明書のタイプ。 <ul style="list-style-type: none"> • `server`サーバ証明書および中間証明書用 • `client-ca`SSLクライアントのルートCAの公開鍵証明書用 • `server-ca`ONTAPがクライアントとなっているSSLサーバのルートCAの公開鍵証明書 • `client`ONTAPをSSLクライアントとして使用するための自己署名またはCA署名のデジタル証明書と秘密鍵 	

Active Directoryドメイン コントローラ アクセスの設定

データ ストレージVM用のSMBサーバをすでに設定しており、Active Directoryドメイン コントローラからクラスタへのアクセスのゲートウェイまたはトンネルとしてストレージVMを設定する場合は、`security login domain-tunnel create`コマンドでこれらの値を指定します。["ONTAPコマンド リファレンス"](#)の`security login domain-tunnel create`の詳細を確認してください。

フィールド	概要	あなたの価値
-vserver	SMBサーバが設定されているStorage VMの名前。	

SMBサーバを設定しておらず、Active Directoryドメインにストレージ VMコンピュータ アカウントを作成する場合は、`vserver active-directory create`コマンドでこれらの値を指定します。["ONTAPコマンド リファレンス"](#)の`vserver active-directory create`の詳細を確認してください。

フィールド	概要	あなたの価値
-------	----	--------

-vserver	Active Directoryコンピュータ アカウントを作成するStorage VMの名前。	
-account-name	コンピュータ アカウントのNetBIOS名。	
-domain	完全修飾ドメイン名 (FQDN) 。	
-ou	ドメイン内の組織単位。デフォルト値は `CN=Computers` です。ONTAPはこの値をドメイン名に追加して、Active Directory識別名を生成します。	

LDAPサーバまたはNISサーバのアクセスの設定

ストレージVMのLDAPクライアント構成を作成する際に、`vserver services name-service ldap client create` コマンドでこれらの値を指定します。["ONTAPコマンド リファレンス"](#)の `vserver services name-service ldap client create` の詳細を確認してください。

次の表には、アカウント設定に関連するオプションのみを記載します。

フィールド	概要	あなたの価値
-vserver	クライアント設定のStorage VMの名前。	
-client-config	クライアント設定の名前。	
-ldap-servers	クライアントが接続するLDAPサーバのIPアドレスおよびホスト名をカンマで区切ったリスト。	
-schema	クライアントがLDAPクエリの作成に使用するスキーマ。	

-use-start-tls	<p>クライアントが Start TLS を使用して LDAP サーバとの通信を暗号化するかどうか (true または false)。</p>	
	<div>  <p>Start TLSは、データStorage VMへのアクセスでのみサポートされます。管理Storage VMへのアクセスではサポートされません。</p> </div>	

これらの値は、LDAPクライアント構成をストレージVMに関連付ける際に、`vserver services name-service ldap create` コマンドで指定します。["ONTAPコマンド リファレンス"](#)の `vserver services name-service ldap create` の詳細を参照してください。

フィールド	概要	あなたの価値
-vserver	クライアント設定を関連付けるStorage VMの名前。	
-client-config	クライアント設定の名前。	
-client-enabled	ストレージVMがLDAPクライアント構成を使用できるかどうか (true または false)。	

ストレージVM上にNISドメイン構成を作成する際に、`vserver services name-service nis-domain create` コマンドでこれらの値を指定します。["ONTAPコマンド リファレンス"](#)の `vserver services name-service nis-domain create` の詳細を確認してください。

フィールド	概要	あなたの価値
-vserver	ドメイン設定を作成するStorage VMの名前。	
-domain	ドメインの名前。	
-nis-servers	ドメイン設定で使用するNISサーバのIPアドレスおよびホスト名をカンマで区切ったリスト。	

ネーム サービス ソースの検索順序を指定する際に、`vserver services name-service ns-switch create` コマンドでこれらの値を指定します。`vserver services name-service ns-switch create` 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。

フィールド	概要	あなたの価値
-vserver	ネーム サービスの参照順序を設定するStorage VMの名前。	
-database	<p>ネーム サービス データベース。</p> <ul style="list-style-type: none"> • `hosts` ファイルおよびDNSネーム サービス用 • `group` ファイル、LDAP、NISネーム サービス用 • `passwd` ファイル、LDAP、NISネーム サービス用 • `netgroup` ファイル、LDAP、NISネーム サービス用 • `namemap` ファイルおよびLDAPネーム サービス用 	
-sources	<p>ネーム サービス ソースを参照する順序（カンマで区切ったリスト）。</p> <ul style="list-style-type: none"> • files • dns • ldap • nis 	

SAMLアクセスの設定

ONTAP 9.3以降では、`security saml-sp create` コマンドでこれらの値を指定してSAML認証を設定します。
`security saml-sp create` 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。

フィールド	概要	あなたの価値
-idp-uri	アイデンティティ プロバイダ (IdP) メタデータをダウンロード可能な、IdPホストのFTPまたはHTTPアドレス。	
-sp-host	SAMLサービス プロバイダ ホスト (ONTAPシステム) のホスト名またはIPアドレス。デフォルトでは、クラスタ管理LIFのIPアドレスが使用されます。	

-cert-ca`および`-cert-serial、または-cert-common-name	サービス プロバイダ ホスト（ONTAPシステム）のサーバ証明書の詳細。サービス プロバイダの証明書の発行元認証局（CA）と証明書のシリアル番号、またはサーバ証明書を入力できます。	
-verify-metadata-server	IdP メタデータ サーバーの ID を検証する必要があるかどうか（true`または`false）。ベストプラクティスとしては、この値を常に`true`に設定します。	

ログイン アカウントの作成

ONTAPログイン アカウントの作成について学ぶ

ローカルまたはリモートのクラスタおよびSVM管理者アカウントを有効にできます。ローカル アカウントとは、アカウント情報、公開鍵、またはセキュリティ証明書がストレージ システム上に保存されているアカウントです。ADアカウント情報はドメイン コントローラに保存されます。LDAPおよびNISアカウントは、LDAPおよびNISサーバに保存されます。

クラスタ管理者とSVM管理者

`_クラスタ管理者_`は、クラスタの管理SVMにアクセスします。管理SVMと予約名`admin`を持つクラスタ管理者は、クラスタのセットアップ時に自動的に作成されます。

デフォルトの`admin`ロールを持つクラスタ管理者は、クラスタ全体とそのリソースを管理できます。クラスタ管理者は、必要に応じて、異なるロールを持つ追加のクラスタ管理者を作成できます。

`_SVM管理者_`はデータSVMにアクセスします。クラスタ管理者は必要に応じてデータSVMとSVM管理者を作成します。

SVM管理者には、デフォルトで`vsadmin`ロールが割り当てられます。クラスタ管理者は、必要に応じてSVM管理者に異なるロールを割り当てることができます。

命名規則

リモート クラスタおよびSVMの管理者アカウントに次の汎用的な名前は使用できません。

- 「adm」
- 「bin」
- 「cli」
- 「daemon」
- 「ftp」

- 「games」
- 「halt」
- 「lp」
- 「mail」
- 「man」
- 「naroot」
- 「netapp」
- 「news」
- 「nobody」
- 「operator」
- 「root」
- 「shutdown」
- 「sshd」
- 「sync」
- "sys"
- 「uucp」
- 「www」

マージされたロール

同じユーザーに対して複数のリモートアカウントを有効にすると、そのユーザーには、アカウントに指定されているすべてのロールの和集合が割り当てられます。つまり、LDAPまたはNISアカウントに `vsadmin` ロールが割り当てられ、同じユーザーのADグループアカウントに `vsadmin-volume` ロールが割り当てられている場合、ADユーザーはより包括的な `vsadmin` 権限でログインします。これらのロールは_マージされている_と呼ばれます。

ローカル アカウント アクセスの有効化

ローカル**ONTAP**アカウント アクセスを有効にする方法について学習します

ローカル アカウントとは、アカウント情報、公開鍵、またはセキュリティ証明書がストレージ システム上に存在するアカウントです。`security login create` コマンドを使用すると、ローカル アカウントが管理SVMまたはデータSVMにアクセスできるようになります。

関連情報

- ["security login create"](#)

ONTAPアカウントのパスワードアクセスを有効にする

```
`security login
```

create`コマンドを使用すると、管理者アカウントがパスワードを使用して管理SVMまたはデータSVMにアクセスできるようになります。コマンドを入力すると、パスワードの入力を求められます。

タスク概要

ログイン アカウントに割り当てるアクセス制御ロールが不明な場合は、`security login modify` コマンドを使用して後でロールを追加できます。

`security login modify`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html>["ONTAPコマンド リファレンス"]を参照してください。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. ローカル管理者アカウントがパスワードを使用してSVMにアクセスできるようにします：

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

次のコマンドは、事前定義された`backup`ロールを持つクラスタ管理者アカウント`admin1`が、パスワードを使用して管理SVMengClusterにアクセスできるようにします。コマンドを入力すると、パスワードの入力を求められます。

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

`security login create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-create.html>["ONTAPコマンド リファレンス"]をご覧ください。

ONTAPアカウントのSSH公開鍵アクセスを有効にする

`security login create`コマンドを使用すると、管理者アカウントがSSH公開キーを使用して管理SVMまたはデータSVMにアクセスできるようになります。

タスク概要

- ・ アカウントがSVMにアクセスするためには、アカウントに公開鍵を関連付けておく必要があります。

ユーザ アカウントへの公開鍵の関連付け

このタスクは、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。

- ログイン アカウントに割り当てるアクセス制御ロールが不明な場合は、`security login modify` コマンドを使用して後でロールを追加できます。

``security login modify``の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html](https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html)["ONTAPコマンド リファレンス"]を参照してください。

クラスタでFIPSモードを有効にする場合は、サポートされているキー アルゴリズムが使用されていない既存のSSH公開鍵アカウントを、サポートされているキー タイプで再設定する必要があります。アカウントの再設定は、FIPを有効にする前に行う必要があります。そうしないと、管理者認証は失敗します。

次の表に、ONTAP SSH接続でサポートされるホスト キー タイプ アルゴリズムを示します。これらのキー タイプは、SSH公開認証の設定には適用されません。

ONTAPリリース	FIPSモードでサポートされるキー タイプ	非FIPSモードでサポートされるキーの種類
9.11.1以降	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 + rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1以前	ecdsa-sha2-nistp256 + ssh-ed25519	ecdsa-sha2-nistp256 + ssh-ed25519 + ssh-dss + ssh-rsa



ONTAP 9.11.1以降では、ssh-ed25519ホスト キー アルゴリズムのサポートが廃止されました。

詳細については、"[FIPSを使用してネットワークセキュリティを設定する](#)"を参照してください。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

- ローカル管理者アカウントがSSH公開鍵を使用してSVMにアクセスできるようにします。

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

次のコマンドは、事前定義された ``vsadmin-volume`` ロールを持つSVM管理者アカウント ``svmadmin1`` が、SSH公開キーを使用してSVMengData1にアクセスできるようにします：

```
cluster1::>security login create -vserver engData1 -user-or-group-name  
svmin1 -application ssh -authmethod publickey -role vsadmin-volume
```

`security login create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-create.html>["ONTAPコマンド リファレンス"]をご覧ください。

終了後の操作

管理者アカウントに公開鍵が関連付けられていない場合、アカウントがSVMにアクセスする前に関連付けておく必要があります。

ユーザ アカウントへの公開鍵の関連付け

多要素認証（MFA）アカウントの有効化

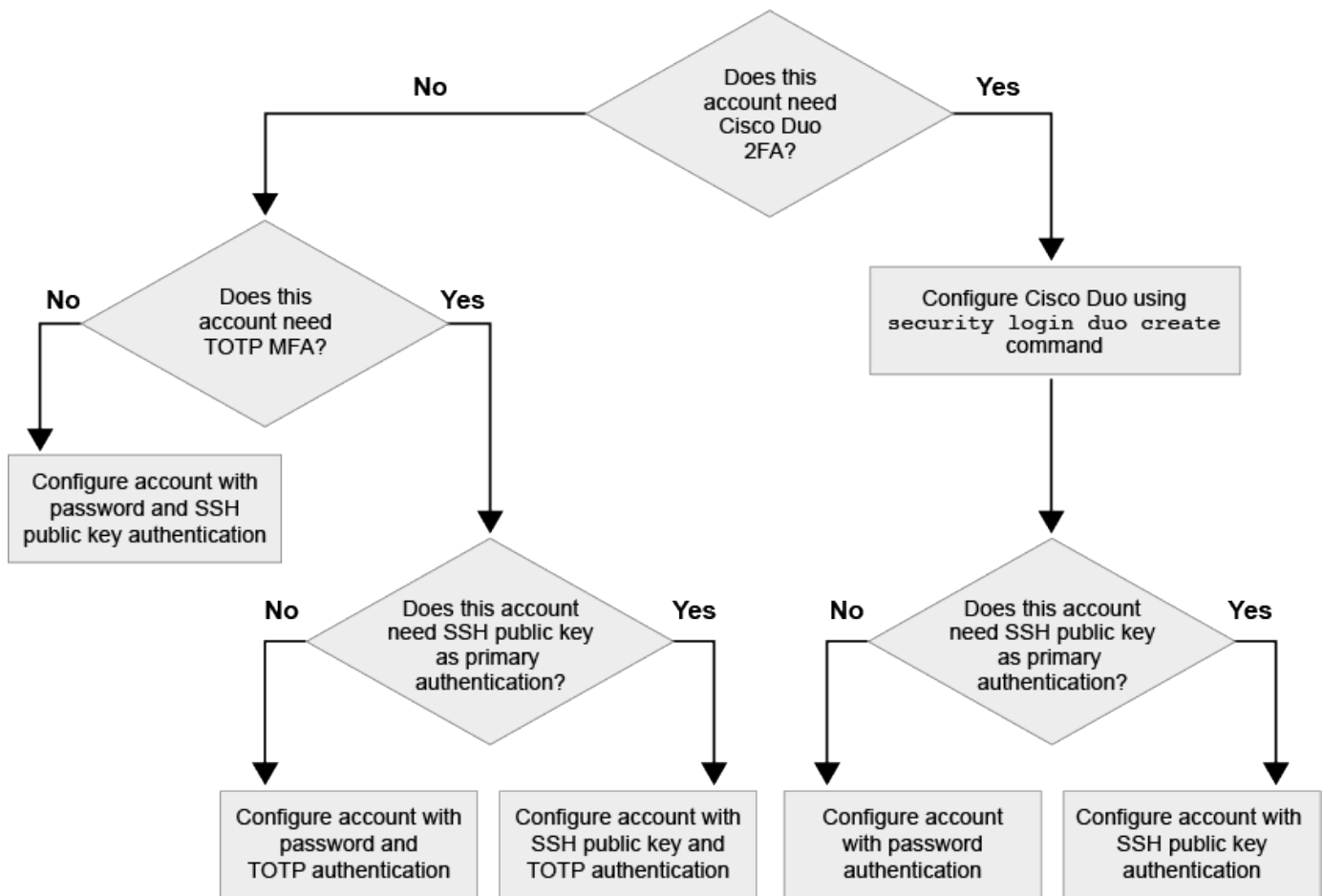
ONTAP多要素認証について学ぶ

多要素認証（MFA）では、管理VMやデータStorage VMにログインする際にユーザに2つの認証方式を要求することで、セキュリティを強化できます。

ONTAPのバージョンに応じて、SSH公開鍵、ユーザ パスワード、Time-based One-Time Password（TOTP）を組み合わせることで多要素認証を行えます。Cisco Duoを有効にして設定すると（ONTAP 9.14.1以降）、すべてのユーザの既存の方式を補完する追加の認証方式として機能します。

追加されたリリース	第1の認証方式	第2の認証方式
ONTAP 9.14.1	SSH公開鍵	TOTP
	ユーザ パスワード	TOTP
	SSH公開鍵	Cisco Duo
	ユーザ パスワード	Cisco Duo
ONTAP 9.13.1	SSH公開鍵	TOTP
	ユーザ パスワード	TOTP
ONTAP 9.3	SSH公開鍵	ユーザ パスワード

MFAが設定されている場合は、最初にクラスタ管理者がローカル ユーザ アカウントを有効にしてから、ローカル ユーザがアカウントを設定する必要があります。



SSHとTOTPを使用してONTAP多要素認証を有効にする

多要素認証（MFA）では、管理SVMやデータSVMにログインする際にユーザに2つの認証方式を要求することで、セキュリティを強化できます。

タスク概要

- 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。
- ログイン アカウントに割り当てるアクセス制御ロールが不明な場合は、`security login modify` コマンドを使用して後でロールを追加できます。

`security login modify`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html](https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html) ["ONTAPコマンド リファレンス"]を参照してください。

"管理者に割り当てられているロールの変更"

- 認証に公開鍵を使用している場合、アカウントがSVMにアクセスするためには、アカウントに公開鍵を関連付けておく必要があります。

"ユーザ アカウントへの公開鍵の関連付け"

このタスクは、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。

- ONTAP 9.12.1以降では、FIDO2（Fast Identity Online）またはPIV（Personal Identity Verification）認証標準を使用して、SSHクライアントMFAにYubikeyハードウェア認証デバイスを使用できます。

SSH公開鍵とユーザ パスワードを使用するMFAの有効化

ONTAP 9.3以降、クラスタ管理者は、SSH公開鍵とユーザ パスワードを使用してMFAでログインするようにローカル ユーザ アカウントを設定できます。

1. ローカル ユーザ アカウントに対して、SSH公開鍵とユーザパスワードを使用するMFAを有効化します。

```
security login create -vserver <svm_name> -user-or-group-name  
<user_name> -application ssh -authentication-method <password|publickey>  
-role admin -second-authentication-method <password|publickey>
```

次のコマンドでは、事前定義された `admin` ロールを持つ SVM 管理者アカウント `admin2` が SSH 公開キーとユーザーパスワードの両方を使用して SVMengData1にログインする必要があります：

```
cluster-1::> security login create -vserver engData1 -user-or-group-name  
admin2 -application ssh -authentication-method publickey -role admin  
-second-authentication-method password
```

Please enter a password for user 'admin2':

Please enter it again:

Warning: To use public-key authentication, you must create a public key
for user "admin2".

`security login create`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html](https://docs.netapp.com/us-en/ontap-cli/security-login-create.html) ["ONTAPコマンド リファレンス"]をご覧ください。

TOTPを使用するMFAの有効化

ONTAP 9.13.1以降では、ローカルユーザにSSH公開鍵またはユーザパスワードと時間ベースのワンタイムパスワード（TOTP）の両方を使用して管理SVMまたはデータSVMにログインすることを要求することで、セキュリティを強化できます。アカウントでTOTPを使用したMFAが有効になった後、ローカルユーザは["設定を完了する"](#)にログインする必要があります。

TOTPは、現在の時刻を使用してワンタイム パスワードを生成するコンピュータ アルゴリズムです。TOTPは、必ずSSH公開鍵またはユーザ パスワードに続く第2の認証方式として使用します。

開始する前に

これらのタスクを実行するには、ストレージ管理者である必要があります。

手順

第1の認証方式にユーザ パスワードまたはSSH公開鍵を使用し、第2の認証方式にTOTPを使用するよう

にMFAを設定できます。

ユーザ パスワードとTOTPを使用するMFAの有効化

1. ユーザ アカウントに対して、ユーザ パスワードとTOTPを使用する多要素認証を有効化します。

新規ユーザーアカウントの場合

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

既存のユーザーアカウントの場合

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

2. TOTPを使用するMFAが有効になっていることを確認します。

```
security login show
```

SSH公開鍵とTOTPを使用するMFAの有効化

1. SSH公開鍵とTOTPを使用する多要素認証を有効化します。

新規ユーザーアカウントの場合

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

既存のユーザーアカウントの場合

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

```
`security login modify`
```

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html>["ONTAP コマンド リファレンス"]を参照してください。

2. TOTPを使用するMFAが有効になっていることを確認します。

```
security login show
```

`security login show`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-show.html>["ONTAP コマンド リファレンス"]を参照してください。

終了後の操作

- 管理者アカウントに公開鍵が関連付けられていない場合、アカウントがSVMにアクセスする前に関連付けておく必要があります。

"ユーザ アカウントへの公開鍵の関連付け"

- ローカル ユーザがログインし、TOTPを使用するMFAの設定を完了する必要があります。

"ローカル ユーザ アカウントでのTOTPを使用するMFAの設定"

関連情報

- "ONTAP 9 における多要素認証 (TR-4647) "
- "ONTAP コマンド リファレンス"

TOTPを使用したMFA用のローカルONTAPユーザーアカウントを構成する

ONTAP 9.13.1以降では、時間ベースのワンタイムパスワード (TOTP) を使用した多要素認証 (MFA) でユーザーアカウントを設定できます。

開始する前に

- ストレージ管理者は、ユーザーアカウントの2番目の認証方法として"[TOTPでMFAを有効にする](#)"を設定する必要があります。
- ユーザ アカウントの第1の認証方式が、ユーザ パスワードまたはSSH公開鍵である必要があります。
- スマートフォンにTOTPアプリを設定し、TOTPシークレット キーを作成しておく必要があります。

Microsoft Authenticator、Google Authenticator / Google認証システム、AuthyなどのTOTP互換認証コードがサポートされています。

手順

1. 現在の認証方法でユーザ アカウントにログインします。

現在の認証方法は、ユーザ パスワードまたはSSH公開鍵である必要があります。

2. アカウントにTOTP設定を作成します。

```
security login totp create -vserver "<svm_name>" -username  
"<account_username >"
```

3. アカウントでTOTP設定が有効になっていることを確認します。

```
security login totp show -vserver "<svm_name>" -username  
"<account_username>"
```

関連情報

- ["セキュリティログイン TOTP 作成"](#)
- ["security login totp show"](#)

ONTAPユーザーアカウントの**TOTP**秘密キーをリセットします

アカウントのセキュリティを確保するために、TOTPシークレット キーが侵害されたり、キーを紛失した場合、既存のキーを無効にして新しいシークレット キーを作成する必要があります。

キー侵害時の**TOTP**のリセット

TOTPシークレット キーが侵害されたが引き続きアクセスできる場合は、侵害されたキーを削除して新しいキーを作成できます。

1. ユーザ パスワードまたはSSH公開鍵と、侵害されたTOTPシークレット キーを使用して、ユーザ アカウントにログインします。
2. 侵害されたTOTPシークレット キーを削除します。

```
security login totp delete -vserver <svm_name> -username  
<account_username>
```

3. 新しいTOTPシークレット キーを作成します。

```
security login totp create -vserver <svm_name> -username  
<account_username>
```

4. アカウントでTOTP設定が有効になっていることを確認します。

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

キー紛失時のTOTPのリセット

TOTP 秘密キーを紛失した場合は、ストレージ管理者に連絡して"[キーが無効になっている](#)"してください。キーが無効になったら、最初の認証方法を使用してログインし、新しい TOTP を設定できます。

開始する前に

ストレージ管理者が、TOTPシークレット キーを無効にする必要があります。ストレージ管理者でない場合は、ストレージ管理者にキーの無効化を依頼してください。

手順

1. ストレージ管理者がTOTPシークレットを無効にしたら、第1の認証方式を使用してローカル アカウントにログインします。
2. 新しいTOTPシークレット キーを作成します。

```
security login totp create -vserver <svm_name> -username  
<account_username >
```

3. アカウントでTOTP設定が有効になっていることを確認します。

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

関連情報

- "[セキュリティログイン TOTP 作成](#)"
- "[セキュリティログイン TOTP 削除](#)"
- "[security login totp show](#)"

ONTAPユーザーアカウントのTOTPシークレットキーを無効にする

ローカル ユーザのTime-based One-Time Password (TOTP) シークレット キーが失われた場合は、失われたキーをストレージ管理者が無効にしてから、ユーザが新しいTOTPシークレット キーを作成する必要があります。

タスク概要

このタスクは、クラスタ管理者アカウントからのみ実行できます。

手順

1. TOTPシークレット キーを無効にします。

```
security login totp modify -vserver <svm_name> -username  
<account_username> -enabled false
```

```
`security login totp modify`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-login-totp-modify.html](https://docs.netapp.com/us-en/ontap-cli/security-login-totp-modify.html)["ONTAPコマンド リファレンス"]を参照してください。

SSL証明書のONTAPアカウントアクセスを有効にする

`security login create`コマンドを使用すると、管理者アカウントがSSL証明書を使用して管理SVMまたはデータSVMにアクセスできるようになります。

タスク概要

- アカウントがSVMにアクセスするためには、CA署名済みサーバ デジタル証明書をインストールしておく必要があります。

CA署名済みサーバ証明書の生成とインストール

このタスクは、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。

- ログイン アカウントに割り当てるアクセス制御ロールが不明な場合は、後で `security login modify` コマンドを使用してロールを追加できます。

管理者に割り当てられているロールの変更



クラスタ管理者アカウントの場合、証明書認証は http、ontapi、および `rest` アプリケーションでサポートされます。SVM管理者アカウントの場合、証明書認証は `ontapi` および `rest` アプリケーションでのみサポートされます。

手順

1. ローカル管理者アカウントがSSL証明書を使用してSVMにアクセスできるようにします。

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

次のコマンドは、デフォルトの `vsadmin` ロールを持つSVM管理者アカウント `svmadmin2` が、SSLデジタル証明書を使用してSVMengData2にアクセスできるようにします。

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

``security login create``の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-create.html>["ONTAPコマンド リファレンス"]をご覧ください。

終了後の操作

CA署名済みサーバ デジタル証明書がインストールされていない場合は、アカウントがSVMにアクセスする前にインストールしておく必要があります。

CA署名済みサーバ証明書の生成とインストール

この手順で説明されているコマンドの詳細については、"[ONTAPコマンド リファレンス](#)"を参照してください。

Active Directory ONTAPアカウントアクセスを有効にする

``security login create``コマンドを使用すると、Active Directory (AD) のユーザーまたはグループアカウントが管理SVMまたはデータSVMにアクセスできるようになります。ADグループ内のすべてのユーザーは、グループに割り当てられたロールを使用してSVMにアクセスできます。

タスク概要

- アカウントが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。

Active Directoryドメイン コントローラ アクセスの設定

このタスクは、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。

- ONTAP 9.13.1以降では、ADユーザ パスワードと組み合わせる第1または第2の認証方式として、SSH公開鍵を使用できます。

SSH公開鍵を第1の認証方式として使用することを選択した場合、AD認証は行われません。

- ONTAP 9.11.1以降では、AD LDAPサーバでサポートされている場合は"[ONTAP NFS SVMのnsswitch認証にLDAP高速バインドを使用する](#)"を使用できます。
- ログイン アカウントに割り当てるアクセス制御ロールが不明な場合は、`security login modify` コマンドを使用して後でロールを追加できます。

``security login modify``の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html>["ONTAPコマンド リファレンス"]を参照してください。

管理者に割り当てられているロールの変更



ADグループアカウントアクセスは、SSH、ontapi、および`rest`アプリケーションでのみサポートされます。ADグループは、多要素認証で一般的に使用されるSSH公開キー認証ではサポートされません。

開始する前に

- クラスタ時間とActive Directoryドメイン コントローラの時刻を、誤差が5分以内となるように同期する必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. ADのユーザまたはグループ管理者アカウントがSVMにアクセスできるようにします。

ADユーザーの場合：

ONTAPバージョン	第1の認証方式	第2の認証方式	コマンド
9.13.1以降	公開鍵	なし	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role></pre>
9.13.1以降	ドメイン	公開鍵	<p>新規ユーザー向け</p> <pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre> <p>既存ユーザーの場合</p> <pre>security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre>

ONTAPバージョン	第1の認証方式	第2の認証方式	コマンド
9.0以降	ドメイン	なし	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap- fastbind true]</pre>

ADグループの場合：

ONTAPのバージョン	第1の認証方式	第2の認証方式	コマンド
9.0以降	ドメイン	なし	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap- fastbind true]</pre>

終了後の操作

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いない場合は、アカウントがSVMにアクセスする前に設定しておく必要があります。

Active Directoryドメイン コントローラ アクセスの設定

関連情報

- ["security login create"](#)

LDAPまたはNIS ONTAPアカウントアクセスを有効にする

`security login create`コマンドを使用すると、LDAPまたはNISユーザアカウントが管理SVMまたはデータSVMにアクセスできるようになります。SVMへのLDAPまたはNISサーバアクセスを設定していない場合は、アカウントがSVMにアクセスできるようにする前に設定する必要があります。

タスク概要

- グループ アカウントはサポートされていません。
- アカウントが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。

LDAPサーバまたはNISサーバのアクセスの設定

このタスクは、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。

- ログイン アカウントに割り当てるアクセス制御ロールが不明な場合は、`security login modify` コマンドを使用して後でロールを追加できます。

``security login modify``の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html>["ONTAPコマンド リファレンス"]を参照してください。

管理者に割り当てられているロールの変更

- ONTAP 9.4以降では、LDAPサーバまたはNISサーバを経由するリモート ユーザに対して多要素認証 (MFA) がサポートされます。
- ONTAP 9.11.1以降では、LDAPサーバでサポートされている場合は["ONTAP NFS SVMのnsswitch認証にLDAP高速バインドを使用する"](#)を使用できます。
- 既知のLDAPの問題のため、LDAPユーザーアカウント情報のどのフィールドでも ':' (コロン) 文字を使用しないでください (例: `gecos`、``userPassword`` など)。そうしないと、そのユーザーの検索操作が失敗します。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

- LDAPまたはNISのユーザ アカウントまたはグループ アカウントがSVMにアクセスできるようにします。

```
security login create -vserver SVM_name -user-or-group-name user_name
-application application -authmethod nsswitch -role role -comment comment -is
-ns-switch-group yes|no [-is-ldap-fastbind true]
```

"ログイン アカウントの作成または変更"

次のコマンドは、事前定義された ``backup`` ロールを持つLDAPまたはNISクラスタ管理者アカウント ``guest2`` が管理SVMengClusterにアクセスできるようにします。

```
cluster1::>security login create -vserver engCluster -user-or-group-name
guest2 -application ssh -authmethod nsswitch -role backup
```

``security login create``の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-create.html>["ONTAPコマンド リファレンス"]をご覧ください。

- LDAPユーザまたはNISユーザに対してMFAログインを有効にします。

```
security login modify -user-or-group-name rem_usr1 -application ssh
-authentication-method nsswitch -role admin -is-ns-switch-group no -second
-authentication-method publickey
```

認証方法は `publickey` として指定でき、2 番目の認証方法は `nsswitch` として指定できます。

次の例ではMFA認証を有効にしています。

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

終了後の操作

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いない場合は、アカウントがSVMにアクセスする前に設定しておく必要があります。

LDAPサーバまたはNISサーバのアクセスの設定

関連情報

- ["セキュリティログイン"](#)

アクセス制御ロールの管理

ONTAPアクセス制御ロールの管理について学ぶ

管理者に割り当てられたロールによって、管理者がアクセスできるコマンドが決まります。ロールは管理者アカウントの作成時に割り当てます。必要に応じて、別のロールを割り当てたり、カスタムロールを定義したりすることもできます。

ONTAP管理者に割り当てられたロールを変更する

`security login modify` コマンドを使用して、クラスタまたはSVM管理者アカウントのロールを変更できます。定義済みロールまたはカスタムロールを割り当てることができます。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタまたは SVM 管理者のロールを変更します：

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

"ログイン アカウントの作成または変更"

次のコマンドは、AD クラスタ管理者アカウント `DOMAIN1\guest1` のロールを事前定義済み `readonly` ロールに変更します。

```
cluster1::>security login modify -vserver engCluster -user-or-group-name  
DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
```

次のコマンドは、AD グループ アカウント `DOMAIN1\adgroup` 内の SVM 管理者アカウントのロールをカスタム `vol_role` ロールに変更します。

```
cluster1::>security login modify -vserver engData -user-or-group-name  
DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
```

`security login modify`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html](https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html)["ONTAP コマンド リファレンス"]を参照してください。

ONTAP 管理者のカスタムロールを定義する

`security login role create` コマンドを使用してカスタムロールを定義できます。ロールに関連付ける機能の正確な組み合わせを実現するために、必要な回数だけコマンドを実行できます。

タスク概要

- ONTAP のコマンドやコマンド ディレクトリへのアクセスは、ロール（事前定義済みまたはカスタム）に基づいて許可または拒否されます。

コマンド ディレクトリ(`volume` は、関連するコマンドとコマンド サブディレクトリのグループです。この手順で説明されている場合を除き、コマンド ディレクトリへのアクセスを許可または拒否すると、ディレクトリとそのサブディレクトリ内の各コマンドへのアクセスも許可または拒否されます。

- 特定のコマンドまたはサブディレクトリへのアクセスは、親ディレクトリへのアクセスよりも優先されます。

あるロールにコマンド ディレクトリを定義し、そのあとに親ディレクトリの特定のコマンドまたはサブディレクトリに対して異なるアクセス レベルを定義した場合、そのコマンドまたはサブディレクトリに対して指定したアクセス レベルが親のアクセス レベルよりも優先されます。



`admin` クラスタ管理者のみが使用できるコマンドまたはコマンド ディレクトリ（`security` コマンド ディレクトリなど）へのアクセス権を付与するロールを SVM 管理者に割り当て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、クラスタ管理者である必要があります。

手順

1. カスタム ロールを定義します。

```
security login role create -vserver SVM_name -role role -cmddirname  
command_or_directory_name -access access_level -query query
```

次のコマンドは、`vol_role`ロールに`volume`コマンド ディレクトリ内のコマンドへのフル アクセスと、`volume snapshot`サブディレクトリ内のコマンドへの読み取り専用アクセスを付与します。

```
cluster1::>security login role create -role vol_role -cmddirname  
"volume" -access all  
  
cluster1::>security login role create -role vol_role -cmddirname "volume  
snapshot" -access readonly
```

次のコマンドは、`SVM_storage`ロールに`storage`コマンド ディレクトリ内のコマンドへの読み取り専用アクセスを許可し、`storage encryption`サブディレクトリ内のコマンドへのアクセスを許可せず、`storage aggregate plex offline`非組み込みコマンドへのフル アクセスを許可します。

```
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage" -access readonly  
  
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage encryption" -access none  
  
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage aggregate plex offline" -access all
```

```
`security login role create`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-  
login-role-create.html["ONTAPコマンド リファレンス"^]を参照してください。
```

関連情報

- ["security login role create"](#)
- ["storage aggregate plex offline"](#)
- ["ストレージ暗号化"](#)

ONTAPクラスタ管理者向けの定義済みロール

クラスタ管理者向けの事前定義されたロールは、ほとんどのニーズを満たすはずです。必要に応じてカスタムロールを作成することもできます。デフォルトでは、クラスタ管

理者には事前定義された `admin` ロールが割り当てられています。

次の表に、クラスタ管理者用の事前定義されたロールを示します。

この役割...	このレベルのアクセス権を持っています...	次のコマンドまたはコマンドディレクトリ
admin	all	すべてのコマンドディレクトリ (DEFAULT)
admin-no-fsa (ONTAP 9.12.1以降で利用可能)	読み取り / 書き込み	<ul style="list-style-type: none">• すべてのコマンドディレクトリ (DEFAULT)• security login rest-role• security login role
読み取り専用	<ul style="list-style-type: none">• security login rest-role create• security login rest-role delete• security login rest-role modify• security login rest-role show• security login role create• security login role create• security login role delete• security login role modify• security login role show• volume activity-tracking• volume analytics	なし
volume file show-disk-usage	autosupport	all

<ul style="list-style-type: none"> • set • system node autosupport 	なし	その他のすべてのコマンドディレクトリ(DEFAULTT)
バックアップ	all	vserver services ndmp
readonly	volume	なし
その他のすべてのコマンドディレクトリ(DEFAULTT)	readonly	all
<ul style="list-style-type: none"> • security login password <p>自身のユーザ アカウント、ローカル パスワード、キー情報を管理する場合のみ</p> <ul style="list-style-type: none"> • set 	<ul style="list-style-type: none"> • ONTAP 9.8以降、読み取り専用 • ONTAP 9.8より前は、なし 	security
readonly	その他のすべてのコマンドディレクトリ(DEFAULTT)	snaplock
all	<ul style="list-style-type: none"> • set • volume create • volume modify • volume move • volume show 	なし
<ul style="list-style-type: none"> • volume move governor • volume move recommend 	なし	その他のすべてのコマンドディレクトリ(DEFAULTT)
なし	なし	すべてのコマンドディレクトリ(DEFAULTT)



`autosupport` ロールは、AutoSupport OnDemandによって使用される事前定義済みの `autosupport` アカウントに割り当てられます。ONTAPでは、`autosupport` アカウントの変更または削除はできません。ONTAPでは、`autosupport` ロールを他のユーザーアカウントに割り当てることもできません。

関連情報

- ["セキュリティログイン"](#)
- ["設定"](#)
- ["ボリューム"](#)

- "vserver services ndmp"

ONTAP SVM管理者向けの定義済みロール

SVM管理者向けの事前定義されたロールは、ほとんどのニーズを満たすはずです。必要に応じてカスタムロールを作成することもできます。デフォルトでは、SVM管理者には事前定義された`vsadmin`ロールが割り当てられています。

次の表に、SVM管理者向けの事前定義されたロールを示します。

ロール名	機能
vsadmin	<ul style="list-style-type: none"> • 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshot、ファイルの管理 • LUNの管理 • SnapLock処理の実行（privileged deleteを除く） • プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、NVMe/FC、NVMe/TCP • サービスの設定：DNS、LDAP、NIS • ジョブの監視 • ネットワーク接続とネットワーク インターフェイスの監視 • SVMの健全性の監視
vsadmin-volume	<ul style="list-style-type: none"> • 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshot、ファイルの管理 • LUNの管理 • プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、NVMe/FC、NVMe/TCP • サービスの設定：DNS、LDAP、NIS • ネットワーク インターフェイスの監視 • SVMの健全性の監視

vsadmin-protocol	<ul style="list-style-type: none"> • 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、NVMe/FC、NVMe/TCP • サービスの設定：DNS、LDAP、NIS • LUNの管理 • ネットワーク インターフェ이스の監視 • SVMの健全性の監視
vsadmin-backup	<ul style="list-style-type: none"> • 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • NDMP処理の管理 • リストアしたボリュームの読み取り / 書き込み許可 • SnapMirror関係とスナップショットの管理 • ボリュームとネットワーク情報の表示
vsadmin-snaplock	<ul style="list-style-type: none"> • 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshot、ファイルの管理 • SnapLock処理の実行（privileged deleteも含む） • プロトコルの設定：NFS と SMB • サービスの設定：DNS、LDAP、NIS • ジョブの監視 • ネットワーク接続とネットワーク インターフェ이스の監視
vsadmin-readonly	<ul style="list-style-type: none"> • 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • SVMの健全性の監視 • ネットワーク インターフェ이스の監視 • ボリュームとLUNの表示 • サービスとプロトコルの表示

System ManagerでONTAP管理者アクセスを管理する

管理者がSystem Managerで実行できる機能は、管理者に割り当てられたロールで決まります。System Managerには、クラスタ管理者およびStorage VM管理者向けの事前定義

されたロールが用意されています。ロールは管理者のアカウントを作成するときに割り当てますが、あとで別のロールを割り当てることもできます。

アカウント アクセスを有効にした方法に応じて、次のいずれかの作業が必要になることがあります。

- 公開鍵をローカル アカウントに関連付ける。
- CAが署名したサーバ デジタル証明書をインストールする。
- AD、LDAP、またはNISアクセスを設定する。

これらの作業は、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。

管理者へのロールの割り当て

管理者にロールを割り当てる手順は次のとおりです。

手順

1. *Cluster > Settings*を選択します。
2. *ユーザーとロール*の横にある ➔ を選択します。
3. *ユーザー*の下の **+ Add** を選択します。
4. ユーザー名を指定し、*Role*のドロップダウン メニューでロールを選択します。
5. ユーザのログイン方法とパスワードを指定します。

管理者のロールの変更

管理者のロールを変更する手順は次のとおりです。

手順

1. *[クラスタ] > [設定]*をクリックします。
2. 役割を変更するユーザーの名前を選択し、ユーザー名の横に表示される ⋮ をクリックします。
3. *編集*をクリックします。
4. *Role*のドロップダウンメニューで役割を選択します。

ONTAPでのJITアクセス権限昇格

ONTAP 9.17.1以降、クラスタ管理者は**"タイミングよく（JIT）権限昇格を設定する"**ONTAPユーザーが特定のタスクを実行するために一時的に権限を昇格することを許可できます。ユーザーにJITが設定されている場合、ユーザーはタスクを実行するために必要な権限を持つロールに一時的に権限を昇格できます。セッションの有効期限が切れると、ユーザーは元のアクセス レベルに戻ります。

クラスタ管理者は、ユーザがJIT昇格にアクセスできる期間を設定できます。たとえば、クラスタ管理者は、30日間（JIT有効期間）にわたり、セッションごとに30分（セッション有効期間）のJIT昇格アクセス制限を設定できます。30日間の期間中、ユーザは必要に応じて何度でも権限を昇格できますが、各セッションは30分に制限されます。

タスク概要

- JIT権限の昇格は、SSHを使用してONTAPにアクセスするユーザーのみが利用できます。権限の昇格は現在のSSHセッション内でのみ可能ですが、必要に応じて任意の数の同時SSHセッション内で権限を昇格できます。
- JIT 権限の昇格は、パスワード、nsswitch、またはドメイン認証を使用してログインするユーザーに対してのみサポートされます。多要素認証（MFA）は JIT 権限の昇格ではサポートされていません。
- 構成されたセッションまたはJITの有効期間が経過した場合、またはクラスタ管理者がユーザのJITアクセスを取り消した場合、ユーザのJITセッションは終了します。

開始する前に

- JIT権限の昇格を利用するには、クラスタ管理者がアカウントのJITアクセスを設定する必要があります。クラスタ管理者は、権限を昇格できるロールと、昇格した権限にアクセスできる期間を決定します。

手順

1. 構成されたロールに権限を一時的に昇格します：

```
security jit-privilege elevate
```

このコマンドを入力すると、ログインパスワードの入力を求められます。アカウントにJITアクセスが設定されている場合、設定されたセッション期間中、昇格されたアクセス権限が付与されます。セッション期間が終了すると、元のアクセス レベルに戻ります。設定されたJIT有効期間内であれば、必要に応じて何度でも権限を昇格できます。

2. JITセッションの残り時間を表示します：

```
security jit-privilege show-remaining-time
```

現在タイミングよくセッション中の場合、このコマンドは残り時間を表示します。

3. 必要に応じて、JITセッションを早めに終了します：

```
security jit-privilege reset
```

現在JITセッション中の場合、このコマンドはJITセッションを終了し、元のアクセス レベルに戻します。

ONTAP でのジャストインタイム権限昇格の設定

ONTAP 9.17.1以降、クラスタ管理者はジャストインタイム（JIT）権限昇格を設定できるようになりました。ONTAPユーザーは特定のタスクを実行するために一時的に権限を昇格できます。ユーザーにJITを設定すると、"[特権を昇格する](#)"タスクの実行に必要な権限を持つロールに一時的に昇格できます。セッション期間が終了すると、ユーザーは元のアクセス レベルに戻ります。

クラスタ管理者は、ユーザがJIT昇格にアクセスできる期間を設定できます。たとえば、JIT昇格へのユーザ ア

アクセスを、30日間（JIT有効期間）にわたり、1セッションあたり30分（セッション有効期間）に制限するように設定できます。30日間の期間中、ユーザは必要に応じて何度でも権限を昇格できますが、各セッションは30分に制限されます。

JIT 権限昇格は最小権限の原則をサポートしており、ユーザーは昇格された権限を必要とするタスクを、その権限を永続的に付与することなく実行できます。これにより、不正アクセスやシステムへの偶発的な変更のリスクを軽減できます。以下の例は、JIT 権限昇格の一般的なユースケースを示しています（：）

- ``security login create``および``security login delete``コマンドへの一時的なアクセスを許可して、ユーザのオンボーディングとオフボーディングを有効にします。
- 更新ウィンドウ中は、``system node image update``および``system node upgrade-revert``への一時的なアクセスを許可します。更新が完了すると、コマンドへのアクセスは取り消されます。
- `cluster add-node`、`cluster remove-node`、および``cluster modify``への一時的なアクセスを許可して、クラスタの拡張または再構成を可能にします。クラスタの変更が完了すると、コマンド アクセスは取り消されます。
- ``volume snapshot restore``への一時的なアクセスを許可して、リストア処理とバックアップ ターゲットの管理を有効にします。リストアまたは設定が完了すると、コマンド アクセスは取り消されます。
- コンプライアンス チェック中に監査ログの確認とエクスポートを有効にするために、``security audit log show``への一時的なアクセスを許可します。

一般的な just-in-time の使用例のより詳細なリストについては、[JITの一般的なユースケース](#)を参照してください。

クラスタ管理者は ONTAP ユーザの JIT アクセスを設定し、クラスタ全体でグローバルに、または特定の SVM に対してデフォルトの JIT 有効期間を設定できます。

タスク概要

- JIT権限の昇格は、SSHを使用してONTAPにアクセスするユーザーのみが利用できます。昇格された権限はユーザーの現在のSSHセッション内でのみ利用可能ですが、必要に応じて任意の数の同時SSHセッション内で権限を昇格できます。
- JIT 権限の昇格は、パスワード、nsswitch、またはドメイン認証を使用してログインするユーザーに対してのみサポートされます。多要素認証（MFA）は JIT 権限の昇格ではサポートされていません。

開始する前に

- 次のタスクを実行するには、``admin``権限レベルの ONTAP クラスタ管理者である必要があります。

グローバル**just-in-time**設定を変更する

デフォルトのJIT設定はONTAPクラスタ全体、または特定のSVMごとに変更できます。これらの設定により、JITアクセスが設定されているユーザーのデフォルトのセッション有効期間と最大JIT有効期間が決まります。

タスク概要

- デフォルト ``default-session-validity-period`` 値は1時間です。この設定は、ユーザーがJITセッションで昇格された権限にアクセスできる時間（再昇格が必要になるまで）を決定します。
- デフォルト ``max-jit-validity-period`` 値は90日です。この設定は、設定された開始日以降、ユーザがタイミングよく昇格にアクセスできる最大期間を決定します。個々のユーザに対してタイミングよく昇格の有効期間を設定できますが、最大のタイミングよく昇格の有効期間を超えることはできません。

手順

1. 現在の JIT 設定を確認します：

```
security jit-privilege show -vserver <svm_name>
```

`-vserver`はオプションです。SVMを指定しない場合、コマンドはグローバルJIT設定を表示します。

2. JIT 設定をグローバルまたは SVM に対して変更します：

```
security jit-privilege modify -vserver <svm_name> -default-session  
-validity-period <period> -max-jit-validity-period <period>
```

SVMを指定しない場合、コマンドはグローバルJIT設定を変更します。次の例では、SVM `svm1` のデフォルトのJITセッション期間を45分、最大JIT期間を30日に設定します：+

```
`security jit-privilege modify -vserver svm1 -default-session-validity-period  
45m -max-jit-validity-period 30d
```

この例では、ユーザーは一度に 45 分間タイミングよく昇格にアクセスでき、構成された開始日から最大 30 日間タイミングよくセッションを開始できます。

ユーザの JIT 権限昇格アクセスを設定する

ONTAP ユーザーにタイミングよく権限の昇格アクセスを割り当てることができます。

手順

1. ユーザの現在のタイミングよくアクセスを確認します：

```
security jit-privilege user show -username <username>
```

`-username`はオプションです。ユーザ名を指定しない場合、コマンドはすべてのユーザのJITアクセスを表示します。

2. ユーザに新しいタイミングよくアクセスを割り当てます：

```
security jit-privilege create -username <username> -vserver <svm_name>  
-role <rbac_role> -session-validity-period <period> -jit-validity-period  
<period> -start-time <date>
```

- `-vserver`が指定されていない場合、JIT アクセスはクラスタレベルで割り当てられます。
- `-role`は、ユーザーが昇格されるRBACロールです。指定されていない場合、`-role`はデフォルトで`admin`になります。
- `-session-validity-period`は、ユーザーが新しいJITセッションを開始する必要がある前に昇格されたロールにアクセスできる期間です。指定されていない場合は、グローバルまたはSVM `default`

`session-validity-period`が使用されます。

- `-jit-validity-period`は、設定された開始日以降、ユーザーがJITセッションを開始できる最大期間です。指定しない場合は、`session-validity-period`が使用されます。このパラメータは、グローバルまたはSVM `max-jit-validity-period`を超えることはできません。
- `-start-time`は、ユーザーがJITセッションを開始できる日時です。指定されていない場合は、現在の日時が使用されます。

次の例では、`ontap_user`が新しい JIT セッションを開始する前に 1 時間 `admin` ロールにアクセスできるようになります。`ontap_user`は、2025 年 7 月 1 日午後 1 時から 60 日間 JIT セッションを開始できるようになります：+

```
security jit-privilege user create -username ontap_user -role admin
-session-validity-period 1h -jit-validity-period 60d -start-time "7/1/25
13:00:00"
```

3. 必要に応じて、ユーザーの JIT アクセスを取り消します：

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

このコマンドは、ユーザーのJITアクセスを、アクセス期限が切れていない場合でも取り消します。`-vserver`が指定されていない場合、JITアクセスはクラスターレベルで取り消されます。ユーザーがアクティブなJITセッションに参加している場合は、セッションが終了します。

JITの一般的なユースケース

以下の表は、JIT権限昇格の一般的なユースケースを示しています。各ユースケースでは、関連するコマンドへのアクセスを提供するためにRBACロールを設定する必要があります。各コマンドは、コマンドとそのパラメータに関する詳細情報が記載されているONTAPコマンドリファレンスにリンクされています。

ユースケース	コマンド	詳細
ユーザーとロールの管理	<ul style="list-style-type: none">• <code>security login create</code>• <code>security login delete</code>	オンボーディングまたはオフボーディング中に、一時的に昇格してユーザーを追加/削除したり、ロールを変更したりします。
証明書管理	<ul style="list-style-type: none">• <code>security certificate create</code>• <code>security certificate install</code>	証明書のインストールまたは更新のために短期アクセスを許可します。
SSH/CLI アクセス制御	<ul style="list-style-type: none">• <code>security login create -application ssh</code>	トラブルシューティングやベンダーサポートのために、一時的にSSHアクセスを許可します。
ライセンス管理	<ul style="list-style-type: none">• <code>system license add</code>• <code>system license delete</code>	機能のアクティブ化または非アクティブ化中にライセンスを追加または削除する権限を付与します。

ユースケース	コマンド	詳細
システムのアップグレードとパッチ適用	<ul style="list-style-type: none"> • <code>system node image update</code> • <code>system node upgrade-revert</code> 	アップグレードウィンドウの間昇格し、その後取り消します。
ネットワークセキュリティ設定	<ul style="list-style-type: none"> • <code>security login role create</code> • <code>security login role modify</code> 	ネットワーク関連のセキュリティロールへの一時的な変更を許可します。
クラスタ管理	<ul style="list-style-type: none"> • <code>cluster add-node</code> • <code>cluster remove-node</code> • <code>cluster modify</code> 	クラスタの拡張または再構成のために昇格します。
SVMの管理	<ul style="list-style-type: none"> • <code>vserver create</code> • <code>vserver delete</code> • <code>vserver modify</code> 	プロビジョニングまたは廃止のために、SVM 管理者権限を一時的に付与します。
ボリュームの管理	<ul style="list-style-type: none"> • <code>volume create</code> • <code>volume delete</code> • <code>volume modify</code> 	ボリュームのプロビジョニング、サイズ変更、または削除のために昇格します。
Snapshotの管理	<ul style="list-style-type: none"> • <code>volume snapshot create</code> • <code>volume snapshot delete</code> • <code>volume snapshot restore</code> 	リカバリ中のスナップショット削除または復元のために昇格します。
ネットワーク構成	<ul style="list-style-type: none"> • <code>network interface create</code> • <code>network port vlan create</code> 	メンテナンス期間中のネットワーク変更の権限を付与します。
ディスク/アグリゲートの管理	<ul style="list-style-type: none"> • <code>storage disk assign</code> • <code>storage aggregate create</code> • <code>storage aggregate add-disks</code> 	ディスクの追加や削除、あるいはアグリゲートの管理を行うには、権限を昇格してください。

ユースケース	コマンド	詳細
データ保護	<ul style="list-style-type: none"> • <code>snapmirror create</code> • <code>snapmirror modify</code> • <code>snapmirror restore</code> 	SnapMirror関係を構成または復元するために一時的に昇格します。
パフォーマンス調整	<ul style="list-style-type: none"> • <code>qos policy-group create</code> • <code>qos policy-group modify</code> 	パフォーマンスのトラブルシューティングやチューニングのために昇格します。
監査ログへのアクセス	<ul style="list-style-type: none"> • <code>security audit log show</code> 	コンプライアンス チェック中に監査ログの確認またはエクスポートを行うために一時的に昇格します。
イベントとアラートの管理	<ul style="list-style-type: none"> • <code>event notification create</code> • <code>event notification modify</code> 	イベント通知または SNMP トラップを構成またはテストするには、Elevate を使用します。
コンプライアンス主導のデータアクセス	<ul style="list-style-type: none"> • <code>volume show</code> • <code>security audit log show</code> 	監査人が機密データやログを確認できるように、一時的な読み取り専用アクセスを許可します。
特権アクセスのレビュー	<ul style="list-style-type: none"> • <code>security login show</code> • <code>security login role show</code> 	特権アクセスの確認とレポートのために一時的に昇格します。読み取り専用の昇格アクセスを一定期間のみ許可します。

関連情報

- ["cluster"](#)
- ["イベント通知"](#)
- ["network"](#)
- ["qos policy-group"](#)
- ["セキュリティ"](#)
- ["SnapMirror"](#)
- ["storage"](#)
- ["システム"](#)
- ["ボリューム"](#)
- ["SVM"](#)

管理者アカウントの管理

ONTAP管理者アカウントの管理について学ぶ

アカウント アクセスの有効化方法によっては、ローカル アカウントへの公開鍵の関連付け、CA 署名付きサーバー デジタル証明書のインストール、AD、LDAP、または NIS 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 アクセスの有効化前でも有効化後でも実行できます。

公開キーをONTAP管理者アカウントに関連付ける

SSH公開鍵認証の場合、管理者アカウントがSVMにアクセスする前に、公開鍵を管理者アカウントに関連付ける必要があります。`security login publickey create`コマンドを使用して、キーを管理者アカウントに関連付けることができます。

タスク概要

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。

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
```

```
`security login publickey create`
```

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-publickey-create.html>["ONTAPコマンド リファレンス"^]をご覧ください。

2. 公開鍵を表示して変更内容を確認します。

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

```
`security login publickey show`
```

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-publickey-show.html>["ONTAPコマンド リファレンス"^]をご覧ください。

例

次のコマンドは、SVM `engData1` の SVM 管理者アカウント `svmadmin1` に公開鍵を関連付けます。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>"
```

ONTAP管理者のSSH公開鍵とX.509証明書を管理する

管理者アカウントによる SSH 認証セキュリティを強化するために、`security login publickey` コマンド セットを使用して SSH 公開キーと X.509 証明書との関連付けを管理できます。

公開鍵とX.509証明書の管理者アカウントへの関連付け

ONTAP 9.13.1以降では、管理者アカウントに関連付ける公開鍵にX.509証明書を関連付けることができます。これにより、アカウントのSSHログイン時に証明書の期限切れや失効がチェックされ、セキュリティが強化されます。

タスク概要

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公開鍵を使用した認証の前に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、または証明書が失効している場合、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証明書の期限切れのみをチェック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証明書の期限切れと失効をチェック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CA証明書とルートCA証明書）は `security certificate install` コマンドを使用してインストールする必要があります。["ONTAPコマンド リファレンス"](#)の `security certificate install` の詳細をご覧ください。
 - SSH で OCSP を有効にする必要があります。手順については["デジタル証明書が有効であることの確認（OCSPを使用）"](#)を参照してください。

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
```

```
`security login publickey create`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-login-publickey-create.html](https://docs.netapp.com/us-en/ontap-cli/security-login-publickey-create.html)["ONTAPコマンド リファレンス"]をご覧ください。

2. 公開鍵を表示して変更内容を確認します。

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

```
`security login publickey show`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-login-publickey-show.html](https://docs.netapp.com/us-en/ontap-cli/security-login-publickey-show.html)["ONTAPコマンド リファレンス"^]をご覧ください。

例

次のコマンドは、SVM `engData2` の SVM 管理者アカウント `svmadmin2` に公開鍵と X.509 証明書を関連付けます。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します。

公開鍵は保持したまま、アカウントのSSH公開鍵から現在の証明書と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
```

```
`security login publickey modify`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-login-publickey-modify.html](https://docs.netapp.com/us-en/ontap-cli/security-login-publickey-modify.html)["ONTAPコマンド リファレンス"^]をご覧ください。

2. 公開鍵を表示して変更内容を確認します。

```
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 engData2 の SVM 管理者アカウント `svmadmin2` から X.509 証明書の関連付けを削除します。

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

管理者アカウントからの公開鍵と証明書の関連付けの削除

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
```

```
`security login publickey delete`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-login-publickey-delete.html](https://docs.netapp.com/us-en/ontap-cli/security-login-publickey-delete.html)["ONTAPコマンド リファレンス"^]をご覧ください。

2. 公開鍵を表示して変更内容を確認します。

```
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 engData3 の SVM 管理者アカウント `svmadmin3` から公開キーと X.509 証明書を削除します。

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

関連情報

- ["セキュリティログイン公開鍵"](#)

ONTAP SSH ログイン用に Cisco Duo 2FA を設定する

ONTAP 9.14.1以降では、SSHログイン時の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、設定は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。代わりに、DuoをStorage VM（旧称Vserver）レベルで設定することもできます。その場合は、そのStorage VMのユーザのみに適用されます。Duoを有効にして設定すると、すべてのユーザの既存の方式を補完する追加の認証方式として機能します。

SSHログインにDuo認証を有効にすると、ユーザーは次回SSHログイン時にデバイスを登録する必要があります。登録方法については、Cisco Duo ["登録ドキュメント"](#)をご覧ください。

ONTAPのコマンドライン インターフェイスで実行できるCisco Duo関連のタスクは次のとおりです。

- [Cisco Duoの設定](#)
- [Cisco Duoの設定の変更](#)
- [Cisco Duoの設定の削除](#)
- [Cisco Duoの設定の表示](#)
- [Duoグループの削除](#)
- [Duoグループの表示](#)
- [ユーザのDuo認証のバイパス](#)

Cisco Duoの設定

``security login duo create`` コマンドを使用して、クラスタ全体または特定のストレージ VM (ONTAP CLI では `vserver` と呼ばれます) に対してCisco Duo設定を作成できます。これを行うと、このクラスタまたはストレージVMへのSSHログインでCisco Duoが有効になります。link:<https://docs.netapp.com/us-en/ontap-cli/security-login-duo-create.html>["ONTAPコマンド リファレンス"]の ``security login duo create`` の詳細をご覧ください。

手順

1. Cisco Duo管理パネルにログインします。
2. **Applications > UNIX Application** に移動します。
3. 統合キー、シークレット キー、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認証を有効にします。山括弧内の値は、使用する環境の情報に置き換えてください。

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

Cisco Duoの設定の変更

Cisco Duo によるユーザー認証方法（例えば、認証プロンプトの表示回数や使用する HTTP プロキシなど）を変更できます。ストレージ VM (ONTAP CLI では `vserver` と呼ばれます) の Cisco Duo 設定を変更する必要がある場合は、``security login duo modify`` コマンドを使用できます。["ONTAPコマンド リファレンス"](#)の ``security login duo modify`` の詳細をご覧ください。

手順

1. Cisco Duo管理パネルにログインします。
2. **Applications > UNIX Application** に移動します。
3. 統合キー、シークレット キー、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設定を変更します。山括弧内の値は、使用する環境の新しい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 \  
-max-prompts 1|2|3 \  
-is-enabled true|false \  
-fail-mode safe|secure
```

Cisco Duoの設定の削除

Cisco Duoの設定を削除すると、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。ストレージ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` コマンドを使用します。`security login duo delete`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。

手順

1. SSHを使用して、ONTAPアカウントにログインします。
2. このストレージ VM の Cisco Duo 構成を削除し、次の部分をストレージ VM 名に置き換えます。
<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の設定の表示

ストレージVM（ONTAP CLIではvserverと呼ばれます）の既存のCisco Duo構成は、`security login duo show` コマンドを使用して表示できます。"[ONTAPコマンド リファレンス](#)"の`security login duo show`の詳細をご覧ください。

手順

1. SSHを使用して、ONTAPアカウントにログインします。
2. このストレージVMのCisco Duo設定を表示します。オプションで、`vserver`パラメータを使用してストレージVMを指定することもできます。その場合は、`<STORAGE_VM_NAME>`をストレージVM名に置き換えます。

```
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、そのグループに属するユーザのみが Duo 認証を求められます。Duo グループは `security login duo group create` コマンドを使用して作成できます。グループを作成する際に、オプションでそのグループ内の特定のユーザを Duo 認証プロセスから除外することもできます。["ONTAPコマンド リファレンス"](#)の `security login duo group create` の詳細をご覧ください。

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グループを作成します。括弧内の値は、環境の情報を置き換えてください。`-vserver`パラメータを省略すると、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> -excluded-users <USER1, USER2>
```

Duo グループの名前は、Active Directory、LDAP、またはローカル グループと一致する必要があります。オプションの `-excluded-users`パラメータで指定したユーザは、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 エントリは `security login duo group show` コマンドを使用して表示できます。`security login duo group show` 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。

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、環境から取得した情報に置き換えてください。`-vserver` パラメータを省略すると、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> -excluded-users <USER1, USER2>
```

Duo グループの名前は、Active Directory、LDAP、またはローカル グループと一致する必要があります。オプションの `-excluded-users` パラメータで指定したユーザは表示されません。

Duoグループの削除

`security login duo group delete` コマンドを使用して、Duo グループのエントリを削除できます。グループを削除すると、そのグループに所属するユーザーは Duo 認証プロセスに含まれなくなります。link:<https://docs.netapp.com/us-en/ontap-cli/security-login-duo-group-delete.html> ["ONTAP コマンド リファレンス"] の `security login duo group delete` の詳細をご覧ください。

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削除します。括弧内の値は、環境から取得した情報に置き換えてください。`-vserver` パラメータを省略すると、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 / ローカル グループと一致している必要があります。

ユーザのDuo認証のバイパス

すべてのユーザか特定のユーザを、Duo SSH認証プロセスから除外できます。

すべてのDuoユーザの除外

すべてのユーザについて、Cisco Duo SSH認証を無効にできます。

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 ユーザの Cisco Duo 認証を無効にし、Vserver 名を `` に置き換えます：

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

Duoグループ ユーザの除外

Duoグループに含まれる特定のユーザを、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のCisco Duo認証を無効にします。山括弧内の値は、それぞれ除外するグループ名やユーザ リストに置き換えてください。

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

Duo グループの名前は、Active Directory、LDAP、またはローカル グループと一致する必要があります。
`-excluded-users`パラメータで指定したユーザは、Duo 認証プロセスに含まれません。

```
`security login duo group modify`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-  
login-duo-group-modify.html["ONTAPコマンド リファレンス"]をご覧ください。
```

ローカルDuoユーザの除外

Cisco Duo 管理パネルを使用して、特定のローカル ユーザを Duo 認証から除外できます。手順については、["Cisco Duo ドキュメント"](#)を参照してください。

ONTAPでCA署名付きサーバ証明書を生成してインストールする

本番環境システムでは、クラスタまたはSVMをSSLサーバとして認証するために、CA署名のデジタル証明書をインストールすることを推奨します。`security certificate generate-csr`コマンドを使用して証明書署名要求（CSR）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`および`security certificate install`の詳細については、["ONTAPコマンド リファレンス"](#)をご覧ください。

証明書署名要求の生成

```
`security certificate generate-csr`コマンドを使用して証明書署名要求（  
CSR）を生成できます。要求が処理されると、認証局（CA）が署名されたデジタル証明書を送信し  
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
```

次のコマンドは、米国カリフォルニア州サニーバールに所在する、カスタム共通名が`server1.companyname.com`である企業の`IT`部門の`Software`グループが使用する、`SHA256`ハッシュ関数によって生成された2048ビットの秘密鍵を含むCSRを作成します。SVM連絡先管理者のメールアドレスは`web@example.com`です。システムはCSRと秘密鍵を出力に表示します。

CSRを作成する例

```
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-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

```
Private Key :
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----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を保管する必要があります。

CA署名済みサーバ証明書のインストール

`security certificate install`コマンドを使用して、SVMにCA署名付きサーバ証明書をインストールできます。ONTAPは、サーバ証明書の証明書チェーンを構成する認証局（CA）のルート証明書と中間証明書の入力を求めます。link:<https://docs.netapp.com/us-en/ontap-cli/security-certificate-install.html>["ONTAPコマンドリファレンス"]の `security certificate install` の詳細をご覧ください。

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. 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
```



サーバ証明書の証明書チェーンを形成する、CAのルート証明書と中間証明書の入力を求めるプロンプトが表示されます。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きます。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署名付き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と中間証明書をインストールする例

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----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-----
<certificate_value>
-----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-----
<certificate_value>
-----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.
```

関連情報

- ["セキュリティ証明書 generate-csr"](#)

System ManagerでONTAP証明書を管理する

ONTAP 9.10.1以降では、System 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、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することができます。他のアプリケーションに対してシステムを識別するための独自の証明書も管理できます。

証明書情報の表示

System Managerを使用して、クラスタに保存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、およびローカル認証局を表示できます。

手順

1. System Managerで、*Cluster > Settings*を選択します。
2. *セキュリティ*領域までスクロールします。*証明書*セクションには、以下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. 証明書のカテゴリの詳細を表示するには、任意の番号を選択するか、➡を選択してすべてのカテゴリの情報を含む*証明書*ページを開いてください。リストにはクラスタ全体の情報が表示されます。特定のストレージVMの情報のみを表示するには、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。

次のステップ

- 証明書 ページから、[\[証明書署名要求の生成\]](#)できます。
- 証明書情報は、カテゴリごとに3つのタブに分かれています。各タブで次の作業を実行できます。

このタブでは...	以下の手順を実行できます...
信頼できる認証機関	<ul style="list-style-type: none">• [install-trusted-cert]• [信頼された認証局の削除]• [信頼された認証局の更新]
クライアント/サーバ証明書	<ul style="list-style-type: none">• [install-cs-cert]• [gen-cs-cert]• [delete-cs-cert]• [renew-cs-cert]

ローカル証明書機関	<ul style="list-style-type: none"> • [新しいローカル認証局の作成] • [ローカル認証局を使用した証明書への署名] • [ローカル認証局の削除] • [ローカル認証局の更新]
-----------	--

証明書署名要求の生成

System Managerの*証明書*ページの任意のタブから、証明書署名要求（CSR）を生成できます。秘密鍵と対応するCSRが生成され、証明機関を使用して署名することで公開証明書を生成できます。

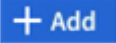
手順

1. *証明書*ページを表示します。[\[証明書情報の表示\]](#)を参照してください。
2. *+Generate CSR*を選択します。
3. サブジェクト名を入力します。
 - a. *共通名*を入力します。
 - b. *国*を選択してください。
 - c. *組織*を入力します。
 - d. *組織単位*を入力します。
4. デフォルトを上書きする場合は、*その他のオプション*を選択し、追加情報を入力します。

信頼された認証局のインストール（追加）

System Managerを使用して、信頼された認証局を追加でインストールできます。

手順

1. *信頼された証明機関*タブを表示します。[\[証明書情報の表示\]](#)を参照してください。
2.  **Add** を選択します。
3. 信頼できる証明機関の追加 パネルで、次の操作を実行します：
 - *名前*を入力してください。
 - **scope** として、ストレージ 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。


信頼された認証局の削除

System Managerを使用して、信頼された認証局を削除できます。



ONTAPにあらかじめ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. *信頼された証明機関*タブを表示します。[\[証明書情報の表示\]](#)を参照してください。
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を使用して、有効期限が切れているか近づいている信頼された認証局を更新できます。

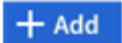
手順

1. *信頼された証明機関*タブを表示します。[\[証明書情報の表示\]](#)を参照してください。
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を使用して、クライアント / サーバ証明書を追加でインストールできます。

手順

1. *クライアント/サーバー証明書*タブを表示します。[\[証明書情報の表示\]](#)を参照してください。
2.  を選択します。
3. *クライアント/サーバー証明書の追加*パネルで、次の操作を実行します：
 - *証明書名*を入力します。
 - **scope** として、ストレージ 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。証明書の詳細を直接入力するか、テキストファイルからコピー&ペーストするか、*インポート*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ができます。
 - *秘密鍵*を入力します。秘密鍵をテキスト ファイルから入力またはコピー アンド ペーストするか、*インポート*をクリックして秘密鍵ファイルからテキストをインポートできます。

自己署名クライアント / サーバ証明書の生成（追加）

System Managerを使用して、自己署名クライアント / サーバ証明書を追加で生成できます。

手順


1. *クライアント/サーバー証明書*タブを表示します。[\[証明書情報の表示\]](#)を参照してください。
2. *+Generate Self-signed Certificate*を選択します。
3. *自己署名証明書の生成*パネルで、次の操作を実行します：
 - *証明書名*を入力します。
 - **scope** として、ストレージ 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。
- ストレージ **VM** を選択します。

クライアント / サーバ証明書の削除

System Managerを使用して、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/サーバー証明書*タブを表示します。[\[証明書情報の表示\]](#)を参照してください。
2. クライアント / サーバ証明書の名前をクリックします。
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を使用して、有効期限が切れているか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/サーバー証明書*タブを表示します。[\[証明書情報の表示\]](#)を参照してください。
2. クライアント / サーバ証明書の名前をクリックします。
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の作成

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。[\[証明書情報の表示\]](#)を参照してください。
2.  **+ Add** を選択します。
3. *ローカル証明機関の追加*パネルで、次の操作を実行します：
 - *名前*を入力してください。
 - **scope** として、ストレージ VM を選択します。
 - *共通名*を入力します。
4. デフォルトを上書きする場合は、*その他のオプション*を選択し、追加情報を入力します。

ローカル認証局を使用した証明書への署名

System Managerで、ローカル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。[\[証明書情報の表示\]](#)を参照してください。
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*を選択します。
4. *証明書署名要求に署名*フォームに記入します。
 - 証明書署名コンテンツを貼り付けるか、*インポート*をクリックして証明書署名要求ファイルをインポートすることができます。
 - 証明書の有効期間を日数で指定します。

ローカル認証局の削除

System Managerを使用して、ローカル認証局を削除できます。


手順

1. *ローカル証明機関*タブを表示します。[\[証明書情報の表示\]](#)を参照してください。
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て、*削除*をクリックします。

ローカル認証局の更新

System Managerを使用して、有効期限が切れているか近づいているローカル認証局を更新できます。

手順

1. *ローカル証明機関*タブを表示します。[\[証明書情報の表示\]](#)を参照してください。
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。

ONTAPでActive Directoryドメイン コントローラ アクセスを設定する

ADアカウントがSVMにアクセスするには、クラスタまたはSVMへのADドメイン コントローラ アクセスを設定する必要があります。データSVM用のSMBサーバをすでに設定している場合は、SVMをクラスタへのADアクセス用のゲートウェイ（トンネル）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ドメイン上にSVM用のコンピュータ アカウントを作成できます。

ONTAPでは、次のドメイン コントローラ認証サービスがサポートされます。

- 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	追加されたリリース
HMAC-SHA256 (Advanced Encryption Standard (AES) ベース) クラスタでONTAP 9.9.1以前が実行されており、ドメイン コントローラがセキュアなNetlogonサービスにAESを適用している場合、接続は失敗します。この場合、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

Netlogonのセキュアなチャネル確立にAESセッション キーを使用する場合は、SVM上で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化されます。そのため、SVMのセキュリティ設定を変更することなく、Netlogonのセキュアなチャネル確立時にAESセッション キーを使用できます。
- ONTAP 9.10.1から9.13.1までは、SVMの作成時にAESがデフォルトで無効化されます。次のコマンドでAESを有効化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でも、それより前のONTAPリリースで作成したSVMのAES設定が自動的に変更されることはありません。これらのSVMでAESを有効化するには、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用にSMBサーバをすでに設定している場合は、`security login domain-tunnel create`コマンドを使用して、SVMをクラスタへのADアクセス用のゲートウェイ、つまり_トンネル_として設定できます。

ONTAP 9.16.1より前では、ADでクラスタ管理者アカウントを管理するには、認証トンネルを使用する必要があります。

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。

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、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認証にKerberosは使用できませんでした。この機能はデフォルトで使用可能であり、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。失敗した場合、次にNTLM認証が試行されます。

手順

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>
```

```
`security login domain-tunnel create`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-  
login-domain-tunnel-create.html ["ONTAP コマンド リファレンス  
"^]を参照してください。
```



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
```

ドメインでの**SVM**コンピュータ アカウントの作成

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

タスク概要

```
`vserver active-directory  
create` コマンドを入力すると、ドメイン内の指定された組織単位にコンピュータを追加するのに  
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の入力を求められます。アカウントのパスワードを空にすることはで  
きません。
```

ONTAP 9.16.1以降では、この手順を使用してADでクラスタ管理者アカウントを管理できます。

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の管理者である必要があります。

手順

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>
```

ONTAP 9.16.1以降、`-vserver` パラメータは管理SVMを受け入れるようになりました。"[ONTAP コマンド](#)

[リファレンス](#)"の `vserver active-directory create` の詳細をご覧ください。

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:

ONTAPでLDAPサーバまたはNISサーバ アクセスを設定

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 ソースとして使用することができます。

LDAPサーバ アクセスの設定

LDAPアカウントがSVMにアクセスするには、SVMへのLDAPサーバ アクセスを設定する必要があります。`vserver services name-service ldap client create` コマンドを使用して、SVM上にLDAPクライアント設定を作成できます。その後、`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に関連付けることができます。

タスク概要

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 (Windows Server 2012以降のほとんどのADサーバで優先されるスキーマ)
- AD-IDMU (Windows Server 2008、Windows Server 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)

特別な要件がある場合を除き、デフォルト スキーマを使用することを推奨します。独自のスキーマが必要な場合は、デフォルト スキーマをコピーし、コピーを変更します。詳細については、以下を参照してください。

- ["NFSの設定"](#)
- ["NetAppテクニカルレポート4835：ONTAPでLDAPを設定する方法"](#)

開始する前に

- SVM に "CA署名付きサーバ デジタル証明書" をインストール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. 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。

```
`vserver services name-service ldap client create`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-  
services-name-service-ldap-client-create.html["ONTAPコマンド  
リファレンス"^]を参照してください。
```

次のコマンドは、SVM `engData` 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172.160.0.100および172.16.0.101を持つLDAPサーバに匿名バインドを行います。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
```



`-ldap-servers`フィールドは`-servers`フィールドを置き換えます。`-ldap-servers`フィールドを使用して、LDAPサーバのホスト名またはIPアドレスのいずれかを指定できます。

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>`

```
`vserver services name-service ldap create`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-  
services-name-service-ldap-create.html["ONTAPコマンド リファレンス  
"^]を参照してください。
```

次のコマンドは、LDAPクライアント設定 `corp` をSVM `engData` に関連付け、SVM上で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
```



`vserver services name-service ldap create` コマンドは自動構成検証を実行し、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". |
```

`name service 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にアクセスするには、SVMへのNISサーバ アクセスを設定する必要があります。
`vserver services name-service nis-domain create` コマンドを使用して、SVM上にNISドメイン設定を作成できます。

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。

手順

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>
```

`vserver services name-service nis-domain create`
の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/vserver-services-name-service-nis-domain-create.html](https://docs.netapp.com/us-en/ontap-cli/vserver-services-name-service-nis-domain-create.html)["ONTAPコマンド リファレンス"]を参照してください。



`-nis-servers`フィールドは`-servers`フィールドを置き換えます。`-nis-servers`フィールドを使用して、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`上にNISドメイン設定を作成します。NISドメイン `nisdomain`は、IPアドレス `192.0.2.180`を持つNISサーバと通信します。

```
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 スイッチの作成

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。`vserver services name-service ns-switch modify`コマンドを使用して、ネーム サービス ソースの検索順序を指定できます。

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。

手順

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>
```

```
`vserver services name-service ns-switch modify`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-services-name-service-ns-switch-modify.html["ONTAPコマンド リファレンス"]を参照してください。
```

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
```

ONTAP管理者パスワードを変更する

システムに初めてログインした後は、すぐに初期パスワードを変更してください。SVM管理者の場合は、`security login password`コマンドを使用して自身のパスワードを変更できます。クラスタ管理者の場合は、`security login password`コマンドを使用して任意の管理者のパスワードを変更できます。

タスク概要

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。



`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たアカウントのパスワードルールを変更できます。

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。

手順

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、SVMvs1.example.comの管理者`admin1`のパスワードを変更します。現在のパスワードの入力を求められた後に、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:
```

関連情報

- ["security login role config modify"](#)
- ["security login password"](#)

ONTAP管理者アカウントのロックとロック解除

`security login lock`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 vs1.example.comの管理者アカウント`admin1`をロックします：

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

`security login lock`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-lock.html>["ONTAPコマンド リファレンス"]をご覧ください。

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 vs1.example.comの管理者アカウント`admin1`のロックを解除します：

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

`security login unlock`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-unlock.html>["ONTAPコマンド リファレンス"]をご覧ください。

関連情報

- ["セキュリティログイン"](#)

ONTAP でログイン試行の失敗を管理する

ログイン試行が繰り返し失敗する場合は、侵入者がストレージシステムにアクセスしようとしている可能性があります。侵入を防ぐために、いくつかの対策を講じることができます。

ログイン試行が失敗したことを確認する方法

イベント管理システム（EMS）は、失敗したログイン試行について1時間ごとに通知します。失敗したログイン試行の記録は`audit.log`ファイルで確認できます。

ログインを何度も試みても失敗した場合の対処法

短期的には、侵入を防ぐためにいくつかの手順を実行できます：

- パスワードは、最小数の大文字、小文字、特殊文字、および/または数字で構成される必要があります
- ログイン試行の失敗後に遅延を課す

- ログイン失敗回数を制限し、指定回数の失敗後にユーザーをロック アウトします。
- 指定した日数以上使用されていないアカウントを期限切れにしてロック アウトする

``security login role config modify`` コマンドを使用してこれらのタスクを実行できます。link:<https://docs.netapp.com/us-en/ontap-cli/security-login-role-config-modify.html>["ONTAPコマンド リファレンス"]の ``security login role config modify`` の詳細をご覧ください。

長期的には、次の追加手順を実行できます：

- ``security ssh modify`` コマンドを使用して、新規に作成されたすべてのSVMへのログイン試行失敗回数を制限します。["ONTAPコマンド リファレンス"](#)の ``security ssh modify`` の詳細をご覧ください。
- ユーザーにパスワードの変更を要求することで、既存の MD5 アルゴリズム アカウントをより安全な SHA-512 アルゴリズムに移行します。

ONTAP管理者アカウントのパスワードにSHA-2を適用する

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。

タスク概要

パスワード ハッシュ機能を使用すると次のことが可能です。

- 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、次回ログイン時にユーザにパスワードを変更させる。
- 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より前のリリースヘリバートする際に、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する。

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

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。

- 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、次のログイン時にパスワードの変更が必要になります。

- 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促します。

システムによって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ていない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. MD5ハッシュ関数をまだ使用しているアカウントをロックします（高度な権限レベル）：
`security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`
- ``-lock-after``で指定された日数が経過すると、ユーザーはMD5アカウントにアクセスできなくなります。
- b. ユーザーがパスワードを変更する準備ができたなら、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。


関連情報

- ["セキュリティログイン パスワードの有効期限切れ"](#)
- ["security login unlock"](#)


System Manager を使用して **ONTAP** ファイル アクセスの問題を診断および修正する

ONTAP 9.8 以降では、ファイル アクセスに関する問題をトレースして表示できます。

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. *Trace File Access*をクリックします。
5. ユーザー名とクライアント IP アドレスを入力し、*トレースの開始*をクリックします。

トレース結果は表に表示されます。*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の  をクリックすると、ファイルのアクセス権限が表示されます。

マルチ管理者認証の管理

ONTAP マルチ管理者検証について学ぶ

ONTAP 9.11.1以降では、マルチ管理者検証（MAV）を使用して、ボリュームやSnapshotの削除などの特定の処理を、指定された管理者の承認を得た場合にのみ実行

できるようにすることができます。これにより、セキュリティ侵害を受けた管理者、悪意のある管理者、または経験の浅い管理者による望ましくない変更やデータの削除を防ぐことができます。

マルチ管理者認証を設定するには、次の処理を実行します。

- "管理者承認グループを1つ以上作成する。"
- "マルチ管理者認証機能を有効にする。"
- "ルールを追加または変更する。"

初期設定後にこれらの要素を変更できるのは、MAV承認グループの管理者（MAV管理者）のみです。

マルチ管理者認証が有効な場合、保護対象処理を完了するには次の手順が必要です。

1. ユーザーが操作を開始すると、"リクエストが生成されます。"
2. 操作を実行する前に、少なくとも1つの"MAV 管理者の承認が必要です。"
3. 承認されると、プロンプトが表示され、ユーザは処理を完了します。



MAV 管理者の承認なしに複数管理者検証機能を無効にする必要がある場合は、NetApp サポートに連絡して次のことを伝えてください"[NetApp ナレッジベース：MAV 管理者が利用できない場合にマルチ管理者検証を無効にする方法](#)"。

マルチ管理者による検証は、自動化が高度に絡むボリュームやワークフローには適していません。自動化されたタスクはそれぞれ、操作を完了する前に承認が必要になるためです。自動化とMAVを併用する場合は、特定のMAV操作のクエリを使用することをお勧めします。例えば、`volume delete`自動化が関係しないボリュームにのみMAVルールを適用し、それらのボリュームに特定の命名スキームを指定するといったことが可能です。



Cloud Volumes ONTAPでは、マルチ管理者認証は使用できません。

マルチ管理者認証の仕組み

マルチ管理者認証は次の要素で構成されます。

- 承認権と拒否権を持つ1人以上の管理者のグループ。
- ルール テーブル 内の保護された操作またはコマンドのセット。
- 保護された操作の実行を識別および制御する_ルールエンジン_。

MAVルールは、ロールベース アクセス制御（RBAC）ルールのあとに評価されます。そのため、保護対象処理を実行または承認する管理者は、それらの処理に対する最低限のRBAC権限を保有している必要があります。"[RBAC の詳細](#)"。

システム定義のルール

マルチ管理者認証が有効化されている場合、システム定義ルール（_ガードレール_ルールとも呼ばれます）によって、MAVプロセス自体の回避リスクを抑制するための一連のMAV操作が確立されます。これらの操作はルールテーブルから削除できません。MAVが有効化されると、アスタリスク（*）で指定された操作は、*show*コマンドを除き、実行前に1人以上の管理者の承認が必要になります。

- `security multi-admin-verify modify`操作``*``

マルチ管理者認証機能の設定を制御します。

- `security multi-admin-verify approval-group`操作``*``

マルチ管理者認証のクレデンシャルを有する一連の管理者のメンバーシップを制御します。

- `security multi-admin-verify rule`操作``*``

マルチ管理者認証を必要とする一連のコマンドを制御します。

- `security multi-admin-verify request 操作`

承認プロセスを制御します。

ルール保護コマンド

システム定義の操作に加えて、マルチ管理者検証が有効になっている場合は次のコマンドがデフォルトで保護されますが、ルールを変更してこれらのコマンドの保護を削除できます：

- `"security login password"`
- `"security login unlock"`
- `"設定"`

各ONTAPバージョンでは、マルチ管理者認証ルールで保護できるコマンドが上記以外にも用意されています。保護可能なコマンドの全一覧を確認するには、お使いのONTAPリリースを選択してください。

9.17.1

- cluster date modify³
- cluster log-forwarding create³
- cluster log-forwarding delete³
- cluster log-forwarding modify³
- cluster peer delete
- cluster time-service ntp server create³
- cluster time-service ntp server delete³
- cluster time-service ntp key create³
- cluster time-service ntp key delete³
- cluster time-service ntp key modify³
- cluster time-service ntp server modify³
- event config modify
- event config set-mail-server-password³
- lun delete³
- security anti-ransomware volume attack clear-suspect¹
- security anti-ransomware volume disable¹
- security anti-ransomware volume event-log modify²
- security anti-ransomware volume pause¹
- security anti-ransomware vserver event-log modify²
- security audit modify³
- security ipsec config modify³
- security ipsec policy create³
- security ipsec policy delete³
- security ipsec policy modify³
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- security key-manager onboard update-passphrase³
- security saml-sp create³

- security saml-sp delete³
- security saml-sp modify³
- security webauthn credentials delete⁴
- snaplock legal-hold end³
- storage aggregate delete³
- storage aggregate offline⁴
- storage encryption disk destroy³
- storage encryption disk modify³
- storage encryption disk revert-to-original-state³
- storage encryption disk sanitize³
- system bridge run-cli³
- system controller flash-cache secure-erase run³
- system controller service-event delete³
- system health alert delete³
- system health alert modify³
- system health policy definition modify³
- system node autosupport modify³
- system node autosupport trigger modify³
- system node coredump delete³
- system node coredump delete-all³
- system node hardware nvram-encryption modify³
- system node run
- system node systemshell
- system script delete³
- system service-processor ssh add-allowed-addresses³
- system service-processor ssh remove-allowed-addresses³
- system smtape restore³
- system switch ethernet log disable-collection³
- system switch ethernet log modify³
- timezone³
- volume create³
- volume delete
- volume encryption conversion start⁴
- volume encryption rekey start⁴

- volume file privileged-delete³
- volume flexcache delete
- volume modify³
- volume rename⁵
- volume recovery-queue modify²
- volume recovery-queue purge²
- volume recovery-queue purge-all²
- volume snaplock modify¹
- volume snapshot autodelete modify
- volume snapshot create³
- volume snapshot delete
- volume snapshot modify³
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename³
- volume snapshot restore
- vservers audit create³
- vservers audit delete³
- vservers audit disable³
- vservers audit modify³
- vservers audit rotate-log³
- vservers create²
- vservers consistency-group create⁴
- vservers consistency-group delete⁴
- vservers consistency-group modify⁴
- vservers consistency-group snapshot create⁴
- vservers consistency-group snapshot delete⁴
- vservers delete³
- vservers modify²
- vservers object-store-server audit create³

- `vserver object-store-server audit delete`³
- `vserver object-store-server audit disable`³
- `vserver object-store-server audit modify`³
- `vserver object-store-server audit rotate-log`³
- `vserver object-store-server bucket cors-rule create`⁴
- `vserver object-store-server bucket cors-rule delete`⁴
- `vserver options`³
- `vserver peer delete`
- `vserver security file-directory apply`³
- `vserver security file-directory remove-slag`³
- `vserver stop`⁴
- `vserver vscan disable`³
- `vserver vscan on-access-policy create`³
- `vserver vscan on-access-policy delete`³
- `vserver vscan on-access-policy disable`³
- `vserver vscan on-access-policy modify`³
- `vserver vscan scanner-pool create`³
- `vserver vscan scanner-pool delete`³
- `vserver vscan scanner-pool modify`³

9.16.1

- `cluster date modify`³
- `cluster log-forwarding create`³
- `cluster log-forwarding delete`³
- `cluster log-forwarding modify`³
- `cluster peer delete`
- `cluster time-service ntp server create`³
- `cluster time-service ntp server delete`³
- `cluster time-service ntp key create`³
- `cluster time-service ntp key delete`³
- `cluster time-service ntp key modify`³
- `cluster time-service ntp server modify`³
- `event config modify`
- `event config set-mail-server-password`³

- lun delete³
- security anti-ransomware volume attack clear-suspect¹
- security anti-ransomware volume disable¹
- security anti-ransomware volume event-log modify²
- security anti-ransomware volume pause¹
- security anti-ransomware vsriver event-log modify²
- security audit modify³
- security ipsec config modify³
- security ipsec policy create³
- security ipsec policy delete³
- security ipsec policy modify³
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- security key-manager onboard update-passphrase³
- security saml-sp create³
- security saml-sp delete³
- security saml-sp modify³
- security webauthn credentials delete⁴
- snaplock legal-hold end³
- storage aggregate delete³
- storage aggregate offline⁴
- storage encryption disk destroy³
- storage encryption disk modify³
- storage encryption disk revert-to-original-state³
- storage encryption disk sanitize³
- system bridge run-cli³
- system controller flash-cache secure-erase run³
- system controller service-event delete³
- system health alert delete³
- system health alert modify³

- system health policy definition modify³
- system node autosupport modify³
- system node autosupport trigger modify³
- system node coredump delete³
- system node coredump delete-all³
- system node hardware nvram-encryption modify³
- system node run
- system node systemshell
- system script delete³
- system service-processor ssh add-allowed-addresses³
- system service-processor ssh remove-allowed-addresses³
- system smtape restore³
- system switch ethernet log disable-collection³
- system switch ethernet log modify³
- timezone³
- volume create³
- volume delete
- volume encryption conversion start⁴
- volume encryption rekey start⁴
- volume file privileged-delete³
- volume flexcache delete
- volume modify³
- volume recovery-queue modify²
- volume recovery-queue purge²
- volume recovery-queue purge-all²
- volume snaplock modify¹
- volume snapshot autodelete modify
- volume snapshot create³
- volume snapshot delete
- volume snapshot modify³
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename³
- volume snapshot restore
- vservice audit create³
- vservice audit delete³
- vservice audit disable³
- vservice audit modify³
- vservice audit rotate-log³
- vservice create²
- vservice consistency-group create⁴
- vservice consistency-group delete⁴
- vservice consistency-group modify⁴
- vservice consistency-group snapshot create⁴
- vservice consistency-group snapshot delete⁴
- vservice delete³
- vservice modify²
- vservice object-store-server audit create³
- vservice object-store-server audit delete³
- vservice object-store-server audit disable³
- vservice object-store-server audit modify³
- vservice object-store-server audit rotate-log³
- vservice object-store-server bucket cors-rule create⁴
- vservice object-store-server bucket cors-rule delete⁴
- vservice options³
- vservice peer delete
- vservice security file-directory apply³
- vservice security file-directory remove-slag³
- vservice stop⁴
- vservice vscan disable³
- vservice vscan on-access-policy create³
- vservice vscan on-access-policy delete³
- vservice vscan on-access-policy disable³
- vservice vscan on-access-policy modify³

- vserver vscan scanner-pool create³
- vserver vscan scanner-pool delete³
- vserver vscan scanner-pool modify³

9.15.1

- cluster date modify³
- cluster log-forwarding create³
- cluster log-forwarding delete³
- cluster log-forwarding modify³
- cluster peer delete
- cluster time-service ntp server create³
- cluster time-service ntp server delete³
- cluster time-service ntp key create³
- cluster time-service ntp key delete³
- cluster time-service ntp key modify³
- cluster time-service ntp server modify³
- event config modify
- event config set-mail-server-password³
- lun delete³
- security anti-ransomware volume attack clear-suspect¹
- security anti-ransomware volume disable¹
- security anti-ransomware volume event-log modify²
- security anti-ransomware volume pause¹
- security anti-ransomware vserver event-log modify²
- security audit modify³
- security ipsec config modify³
- security ipsec policy create³
- security ipsec policy delete³
- security ipsec policy modify³
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete

- security login publickey modify
- security key-manager onboard update-passphrase³
- security saml-sp create³
- security saml-sp delete³
- security saml-sp modify³
- snaplock legal-hold end³
- storage aggregate delete³
- storage encryption disk destroy³
- storage encryption disk modify³
- storage encryption disk revert-to-original-state³
- storage encryption disk sanitize³
- system bridge run-cli³
- system controller flash-cache secure-erase run³
- system controller service-event delete³
- system health alert delete³
- system health alert modify³
- system health policy definition modify³
- system node autosupport modify³
- system node autosupport trigger modify³
- system node coredump delete³
- system node coredump delete-all³
- system node hardware nvram-encryption modify³
- system node run
- system node systemshell
- system script delete³
- system service-processor ssh add-allowed-addresses³
- system service-processor ssh remove-allowed-addresses³
- system smtape restore³
- system switch ethernet log disable-collection³
- system switch ethernet log modify³
- timezone³
- volume create³
- volume delete
- volume file privileged-delete³

- volume flexcache delete
- volume modify³
- volume recovery-queue modify²
- volume recovery-queue purge²
- volume recovery-queue purge-all²
- volume snaplock modify¹
- volume snapshot autodelete modify
- volume snapshot create³
- volume snapshot delete
- volume snapshot modify³
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename³
- volume snapshot restore
- vservers audit create³
- vservers audit delete³
- vservers audit disable³
- vservers audit modify³
- vservers audit rotate-log³
- vservers create²
- vservers delete³
- vservers modify²
- vservers object-store-server audit create³
- vservers object-store-server audit delete³
- vservers object-store-server audit disable³
- vservers object-store-server audit modify³
- vservers object-store-server audit rotate-log³
- vservers options³
- vservers peer delete
- vservers security file-directory apply³

- vserver security file-directory remove-slag³
- vserver vscan disable³
- vserver vscan on-access-policy create³
- vserver vscan on-access-policy delete³
- vserver vscan on-access-policy disable³
- vserver vscan on-access-policy modify³
- vserver vscan scanner-pool create³
- vserver vscan scanner-pool delete³
- vserver vscan scanner-pool modify³

9.14.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect¹
- security anti-ransomware volume disable¹
- security anti-ransomware volume event-log modify²
- security anti-ransomware volume pause¹
- security anti-ransomware vserver event-log modify²
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify²
- volume recovery-queue purge²
- volume recovery-queue purge-all²
- volume snaplock modify¹
- volume snapshot autodelete modify
- volume snapshot delete

- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vservice create²
- vservice modify²
- vservice peer delete

9.13.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect¹
- security anti-ransomware volume disable¹
- security anti-ransomware volume pause¹
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snaplock modify¹
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

9.12.1 / 9.11.1

- cluster peer delete
- event config modify
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

1. 9.13.1で新規追加されたルール保護コマンド
2. 9.14.1で新規追加されたルール保護コマンド
3. 9.15.1で新規追加されたルール保護コマンド
4. 9.16.1で新規追加されたルール保護コマンド
5. 9.17.1で新規追加されたルール保護コマンド

*このコマンドはCLIでのみ使用可能であり、一部のリリースではSystem Managerでは使用できません。

マルチ管理者承認の仕組み

保護対象処理がMAVで保護されたクラスタで入力されると、指定されたMAV管理者グループに処理の実行要求が送信されます。

設定できる項目は次のとおりです。

- MAVグループ内の管理者の名前、連絡先情報、および数。

MAV管理者には、クラスタ管理者権限のあるRBACロールが必要です。

- MAV管理者グループの数。
 - 保護対象処理ルールごとにMAVグループが割り当てられます。
 - MAVグループが複数ある場合は、どのMAVグループが特定のルールを承認するかを設定できます。
- 保護対象処理を実行するために必要なMAV承認者の数。
- MAV 管理者が承認リクエストに応答しなければならない_承認有効期限_。
- 要求元の管理者が操作を完了しなければならない_実行有効期限_。

設定後にこれらのパラメータを変更するには、MAVの承認が必要です。

MAV管理者は、自身が要求した保護対象処理の実行を承認することはできません。そのため、次の点に注意してください。

- 管理者が1人しかいないクラスタでは、MAVを有効にしないでください。
- MAVグループのメンバーが1人だけの場合、そのMAV管理者は保護対象処理を開始できません。保護対象処理は一般の管理者が開始する必要がある、MAV管理者は承認のみを行うことができます。
- MAV管理者が保護対象処理を実行できるようにするには、MAV管理者の数が、必要な承認者数よりも1人多くなければなりません。たとえば、ある保護対象処理に2人の承認が必要で、MAV管理者がその処理を実行できるようにするためには、MAV管理者グループに3人のメンバーが必要です。

承認要求は、（EMSを使用して）Eメール アラートでMAV管理者に送信できるほか、管理者が要求キューを照会することもできます。受信した要求に対し、MAV管理者は次の3つのいずれかの対応を取ることができます。

- 承認
- 却下（拒否）
- 無視（対応なし）

次の場合、MAVルールに関連付けられているすべての承認者にEメール通知が送信されます。

- 要求が作成された場合。
- 要求が承認または拒否された場合。
- 承認された要求が実行された場合。

処理の要求者が同じ承認グループに属している場合は、要求が承認された場合もEメールが送信されます。



要求者は、承認グループに属していても自身の要求は承認できません（ただし、自分の要求のEメール通知を受け取ることはできます）。承認グループに属していない（つまり、MAV管理者ではない）要求者には、Eメール通知は送信されません。

保護対象処理が実行される仕組み

保護対象処理の実行が承認された場合、要求元ユーザはプロンプトを確認して処理を続行します。処理が拒否された場合、要求元ユーザは、要求を削除してから次の作業に進む必要があります。

MAVルールはRBACの権限のあとに評価されます。そのため、処理を実行するための十分なRBACの権限がないユーザはMAV要求プロセスを開始できません。

MAVルールは、保護された操作が実行される前に評価されます。つまり、ルールはシステムの現在の状態に基づいて適用されます。例えば、`volume modify`のクエリが`-size 5GB`のMAVルールを作成した場合、`volume modify`を使用して5GBのボリュームを2GBにサイズ変更するにはMAVの承認が必要ですが、2GBのボリュームを5GBにサイズ変更する場合はMAVの承認は必要ありません。

関連情報

- ["cluster"](#)
- ["lun"](#)
- ["セキュリティ"](#)
- ["snaplock リーガルホールド終了"](#)
- ["ストレージアグリゲート"](#)
- ["ストレージ暗号化"](#)
- ["システム"](#)

MAVのONTAP管理者承認グループを管理する

マルチ管理者認証（MAV）を有効にする前に、承認または拒否の権限が付与された1人以上の管理者を含む管理者承認グループを作成する必要があります。マルチ管理者認証を有効にした場合、承認グループのメンバーシップを変更するには、認定された既存のいずれかの管理者の承認が必要です。

タスク概要

既存の管理者をMAVグループに追加するか、または新しい管理者を作成できます。

MAV機能は、既存のロールベースアクセス制御（RBAC）設定を尊重します。MAV管理者候補は、MAV管理者グループに追加される前に、保護された操作を実行するための十分な権限を持っている必要があります。["RBACの詳細をご覧ください。"](#)



MAVを設定して、承認リクエストが保留中であることをMAV管理者に通知することができます。そのためには、メール通知（特に`Mail From`および`Mail Server`パラメータ）を設定する必要があります。または、これらのパラメータをクリアして通知を無効にすることもできます。メールアラートがない場合、MAV管理者は承認キューを手動で確認する必要があります。

ONTAP 9.15.1以降では、Active Directory（AD）ユーザーをMAV管理者として設定できます。ADユーザーは["ONTAP管理者として設定されている"](#)である必要があります。



System Managerの手順

MAV承認グループを初めて作成する場合は、System Managerの手順を参照してください"[複数管理者による検証を有効にします。](#)"

既存の承認グループを変更する、または追加の承認グループを作成するには、次の手順を実行します。

1. マルチ管理者認証の対象となる管理者を特定します。
 - a. *クラスター > 設定*をクリックします。
 - b. *ユーザーとロール*の横にある  をクリックします。
 - c. *ユーザー*の下にある  Add をクリックします。
 - d. 必要に応じて内容を変更します。

詳細については、"[管理者アクセスを制御します。](#)"を参照してください。

2. MAV承認グループを作成または変更します。
 - a. *クラスター > 設定*をクリックします。
 - b. *セキュリティ*セクションの*複数管理者承認*の横にある  をクリックします。（MAVがまだ設定されていない場合は  アイコンが表示されます。）
 - Name：グループ名を入力します。
 - Approvers：ユーザのリストから承認者を選択します。
 - Email address：Eメール アドレスを入力します。
 - Default group：グループを選択します。

MAVを有効にしたあとで既存の設定を編集するには、MAVの承認が必要です。

CLIの手順

1. `Mail From`および `Mail Server`パラメータに値が設定されていることを確認します。次のように入力します：

```
event config show
```

次のような出力が表示されます。

```
cluster01::> event config show
                        Mail From:  admin@localhost
                        Mail Server: localhost
                        Proxy URL:   -
                        Proxy User:  -
                        Publish/Subscribe Messaging Enabled: true
```

これらのパラメータを設定するには、次のように入力します。

```
event config modify -mail-from email_address -mail-server server_name
```

`event config show`および `event config modify`
の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/search.html?q=event+config>["ONTAP コマンド リファレンス"]をご覧ください。

2. マルチ管理者認証の対象となる管理者を特定します。

次の操作を行う場合：	入力するコマンド
現在の管理者を表示する	<code>security login show</code>
現在の管理者の認証情報を変更する	<code>security login modify <parameters></code>
新しい管理者アカウントを作成する	<code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code>

`security login show`、 `security login modify`、および `security login create`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+login>["ONTAP コマンド リファレンス"]をご覧ください。

3. MAV承認グループを作成します。

```
security multi-admin-verify approval-group create [ -vserver svm_name] -name  
group_name -approvers approver1[,approver2...] [[-email address1], address1...]
```

- `-vserver` - このリリースでは管理 SVM のみがサポートされます。
- `-name` - MAV グループ名（最大 64 文字）。
- `-approvers` - 1人以上の承認者のリスト。ADユーザーの場合は、`domain\user``という形式を使用します。例： ``mydomain\pavan``。
- `-email` - リクエストが作成、承認、拒否、または実行されたときに通知される1つ以上の電子メールアドレス。

例： 次のコマンドは、2 人のメンバーと関連付けられた電子メール アドレスを持つ MAV グループを作成します。

```
cluster-1::> security multi-admin-verify approval-group create -name  
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. グループの作成とメンバーシップを確認します。

```
security multi-admin-verify approval-group show
```

例：

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name          Approvers          Email
-----  -
svm-1    mav-grp1      pavan,julia        email
pavan@myfirm.com,julia@myfirm.com
```

MAVグループの初期設定を変更するには、次のコマンドを使用します。

注：すべて、実行前に MAV 管理者の承認が必要です。

次の操作を行う場合：	入力するコマンド
グループの特性を変更するか、既存のメンバー情報を変更する	<code>security multi-admin-verify approval-group modify [parameters]</code>
メンバーを追加または削除する	<code>security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2...]] [-approvers-to-remove approver1[,approver2...]]</code>
グループを削除する	<code>security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name</code>

関連情報

- ["セキュリティ多管理者認証"](#)

ONTAPでマルチ管理者検証を有効または無効にする

マルチ管理者認証（MAV）は明示的に有効にする必要があります。有効にしたマルチ管理者認証を削除するには、MAV承認グループ内の管理者（MAV管理者）による承認が必要です。

タスク概要

有効にしたMAVを変更または無効にするには、MAV管理者の承認が必要です。



MAV 管理者の承認なしに複数管理者検証機能を無効にする必要がある場合は、NetApp サポートに連絡して次のことを伝えてください["NetApp ナレッジベース：MAV 管理者が利用できない場合にマルチ管理者検証を無効にする方法"](#)。

MAVを有効にする際には、次のパラメータをグローバルに指定できます。

Approval groups

グローバル承認グループのリスト。MAV機能を有効にするには、少なくとも1つのグループが必要です。



MAVを自律型ランサムウェア対策（ARP）で使用している場合は、ARPの一時停止、無効化、疑わしい要求のクリアを承認する新規または既存の承認グループを定義します。

必要な承認者

保護された操作を実行するために必要な承認者の数。デフォルトおよび最小数は1です。



必要な承認者数は、デフォルトの承認グループ内の承認者の合計数よりも少なくする必要があります。

承認の有効期限（時：分：秒）

MAV管理者が承認リクエストに応答しなければならない期間。デフォルト値は1時間（1h）、サポートされる最小値は1秒（1s）、サポートされる最大値は14日（14d）です。


実行期限（時、分、秒）

要求元の管理者が：：操作を完了しなければならない期間。デフォルト値は1時間（1h）、サポートされる最小値は1秒（1s）、サポートされる最大値は14日（14d）です。

特定の"[操作ルール](#)。"に対して、これらのパラメータのいずれかを上書きすることもできます

System Managerの手順

- マルチ管理者認証の対象となる管理者を特定します。
 - *クラスター > 設定*をクリックします。
 - *ユーザーとロール*の横にある [→](#) をクリックします。
 - *ユーザー*の下にある [+ Add](#) をクリックします。
 - 必要に応じて内容を変更します。

詳細については、"[管理者アクセスを制御します](#)。"を参照してください。
- 承認グループを1つ以上作成し、ルールを1つ以上追加して、マルチ管理者認証を有効にします。
 - *クラスター > 設定*をクリックします。
 - *セキュリティ*セクションの*複数管理者承認*の横にある  をクリックします。
 - [+ Add](#) をクリックして、少なくとも1つの承認グループを追加します。
 - Name – グループ名を入力します。
 - Approvers – ユーザーのリストから承認者を選択します。
 - Email address – Eメール アドレスを入力します。
 - Default group – グループを選択します。
 - ルールを1つ以上追加します。
 - Operation – サポートされているコマンドをリストから選択します。
 - Query – 必要なコマンド オプションと値を入力します。

- オプションのパラメータ：グローバル設定を適用する場合は、空白のままにします。グローバル設定を上書きする場合は、特定のルールに対して別の値を割り当てます。
 - Required number of approvers
 - Approval groups

e. デフォルトを表示または変更するには、*詳細設定*をクリックします。

- 必要な承認者数（デフォルト：1）
- 実行リクエストの有効期限（デフォルト：1時間）
- 承認リクエストの有効期限（デフォルト：1時間）
- メールサーバー*
- 送信元メールアドレス*

*これらは「通知管理」で管理されているメール設定を更新します。まだ設定されていない場合は、設定するように求められます。


f. *有効化*をクリックして、MAV の初期設定を完了します。

初期構成後、現在の MAV ステータスが **Multi-Admin Approval** タイルに表示されます。

- ステータス（有効または無効）
- 承認が必要なアクティブな処理
- 保留状態のオープン要求の数

→をクリックすると、既存の構成を表示できます。既存の構成を編集するには、MAV の承認が必要です。

マルチ管理者認証を無効にするには、次の手順を実行します。

1. *クラスター > 設定*をクリックします。
2. *セキュリティ*セクションの*複数管理者承認*の横にある  をクリックします。
3. [Enabled] トグル ボタンをクリックします。

この処理を完了するには、MAVの承認が必要です。

CLIの手順

CLI で MAV 機能を有効にする前に、少なくとも 1 つの"MAV 管理者グループ"を作成しておく必要があります。

次の操作を行う場合：	入力するコマンド
MAV機能を有効にする	<pre>security multi-admin-verify modify -approval-groups group1[,group2...] [- required-approvers nn] -enabled true [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]</pre> <p>例：次のコマンドは、承認グループ 1 つ、必須承認者 2 人、およびデフォルトの有効期限で MAV を有効にします。</p> <pre>cluster-1::> security multi-admin- verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre> <p>少なくとも1つの"操作ルール。"を追加して初期設定を完了します</p>
MAV 構成を変更する（MAV の承認が必要）	<pre>security multi-admin-verify approval- group modify [-approval-groups group1 [,group2...]] [-required-approvers nn] [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]</pre>
MAV機能を確認する	<pre>security multi-admin-verify show</pre> <p>例：</p> <pre>cluster-1::> security multi-admin- verify show Is Required Execution Approval Approval Enabled Approvers Expiry Expiry Groups ----- true 2 1h 1h mav-grp1</pre>
MAV 機能を無効にする（MAV の承認が必要）	<pre>security multi-admin-verify modify -enabled false</pre>

- "セキュリティ多管理者認証"

ONTAPで保護された操作のマルチ管理者検証ルールを管理する

マルチ管理者認証（MAV）ルールを作成して、承認が必要な処理を指定します。保護対象処理が開始されると、処理が傍受され、承認要求が生成されます。

ルールは、MAVを有効にする前であれば、適切なRBAC機能を持つ任意の管理者が作成できますが、MAVを有効にしたあとにルール セットを変更するにはMAVの承認が必要です。

1つの操作につき1つのMAVルールのみ作成できます。例えば、複数の `volume-snapshot-delete` ルールを作成することはできません。必要なルール制約はすべて、1つのルール内に含める必要があります。

"これらのコマンド"を保護するためのルールを作成できます。コマンドの保護機能が最初に利用可能になったONTAPバージョン以降、各コマンドを保護できます。

MAV システムのデフォルト コマンドのルール（`security multi-admin-verify "コマンド"`）は変更できません。

システム定義の操作に加えて、マルチ管理者検証が有効になっている場合は次のコマンドがデフォルトで保護されますが、ルールを変更してこれらのコマンドの保護を削除できます：

- "security login password"
- "security login unlock"
- "設定"

ルールの制約

ルールを作成する際に、`-query` オプションを任意で指定して、リクエストをコマンド機能のサブセットに制限できます。`-query` オプションは、SVM、ボリューム、Snapshot名などの構成要素を制限するためにも使用できます。

たとえば、`volume snapshot delete` コマンドでは、`-query` を `!snapshot !hourly*,!daily*,!weekly*` に設定できます。これは、時間別、日次、または週次属性がプレフィックスとして付いたボリューム スナップショットが MAV 保護から除外されることを意味します。

```
smci-vs1m20::> security multi-admin-verify rule show
```

		Required	Approval
Vserver	Operation	Approvers	Groups
vs01	volume snapshot delete	-	-
	Query: -snapshot !hourly*,!daily*,!weekly*		



除外された設定要素はMAVによって保護されず、どの管理者も削除したり名前を変更したりすることができます。

デフォルトでは、保護された操作が入力されると、対応する `security multi-admin-verify request create "protected_operation"` コマンドが自動的に生成されるようにルールが規定されています。このデフォルトを変

更して、`request create` コマンドを別途入力するように設定することもできます。


デフォルトでは、ルールは次のグローバルMAV設定を継承しますが、ルール固有の例外を指定できます。

- Required Number of Approvers
- Approval Groups
- Approval Expiry period
- Execution Expiry period

System Managerの手順

保護された操作ルールを初めて追加する場合は、System Managerの手順を参照してください。["複数管理者による検証を有効にします。"](#)

既存のルール セットを変更するには、次の手順を実行します。

1. ***Cluster > Settings***を選択します。
2. ***セキュリティ*セクションの*複数管理者承認***の横にある  を選択します。
3. **+ Add** を選択して、少なくとも 1 つのルールを追加します。既存のルールを変更または削除することもできます。
 - Operation – サポートされているコマンドをリストから選択します。
 - Query – 必要なコマンド オプションと値を入力します。
 - オプションのパラメータ：グローバル設定を適用する場合は、空白のままにします。グローバル設定を上書きする場合は、特定のルールに対して別の値を割り当てます。
 - Required number of approvers
 - Approval groups

CLIの手順



すべての `security multi-admin-verify rule` コマンドは、`security multi-admin-verify rule show` を除き、実行前にMAV管理者の承認が必要です。

次の操作を行う場合：	入力するコマンド
ルールを作成します。	<pre>security multi-admin-verify rule create -operation "protected_operation" [- query operation_subset] [parameters]</pre>
現在の管理者の認証情報を変更する	<pre>security login modify <parameters></pre> <p>例：次のルールでは、ルートボリュームを削除するには承認が必要です。</p> <pre>security multi-admin-verify rule create -operation "volume delete" -query "- vserver vs0"</pre>

次の操作を行う場合：	入力するコマンド
ルールを変更する	<code>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</code>
ルールを削除します。	<code>security multi-admin-verify rule delete -operation "protected_operation"</code>
ルールを表示	<code>security multi-admin-verify rule show</code>

関連情報

- ["セキュリティ多管理者検証ルール"](#)
- ["security login modify"](#)

ONTAPでMAV保護された操作の実行をリクエストする

マルチ管理者認証（MAV）が有効になっているクラスターで保護対象処理またはコマンドを開始すると、ONTAPは自動的に処理を傍受して、要求を生成するよう求めます。生成した要求は、MAV承認グループ内の1人以上の管理者（MAV管理者）によって承認される必要があります。また、ダイアログなしでMAV要求を作成することもできます。

承認された場合は、クエリに応答して、要求の有効期限内に処理を完了する必要があります。拒否された場合、要求数の上限を超えた場合、または有効期限を過ぎた場合は、要求を削除して再送信する必要があります。

MAV機能は、既存のRBAC設定を遵守します。つまり、MAVの設定に関係なく、管理者ロールには、保護対象処理を実行するための十分な権限が必要です。["RBACの詳細"](#)。

MAV管理者が保護対象処理を実行する要求を生成した場合も、その要求は他のMAV管理者によって承認される必要があります。

System Managerの手順

ユーザがメニュー オプションをクリックしてある処理を開始し、その処理が保護されている場合、承認要求が生成され、次のような通知がユーザに送信されます。

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

MAVが有効な場合、*マルチ管理者リクエスト*ウィンドウが利用可能になり、ユーザーのログインIDとMAVロール（承認者かどうか）に基づいて保留中のリクエストが表示されます。保留中のリクエストごとに、以下のフィールドが表示されます：

- 処理
- Index（番号）

- Status (Pending、Approved、Rejected、Executed、Expired)

承認者が1人でも要求を却下した場合、それ以上の操作を行うことはできません。

- Query (要求された処理のパラメータまたは値)
- Requesting User
- Request Expires On
- Pending Approvers (人数)
- Potential Approvers (人数)

要求が承認された場合、要求元ユーザは有効期限内に処理を再試行できます。

ユーザが承認なしで処理を再試行すると、次のような通知が表示されます。

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

CLIの手順

1. 保護対象処理を直接、またはMAV要求コマンドを使用して入力します。

例 – ボリュームを削除するには、次のコマンドのいずれかを入力します：

◦ volume delete

```
cluster-1::*> volume delete -volume vol1 -vserver vs0

Warning: This operation requires multi-admin verification. To create
a
      verification request use "security multi-admin-verify
request
      create".

      Would you like to create a request for this operation?
      {y|n}: y

Error: command failed: The security multi-admin-verify request (index
3) is
      auto-generated and requires approval.
```

◦ security multi-admin-verify request create "volume delete"

```
Error: command failed: The security multi-admin-verify request (index
3)
    requires approval.
```

2. 要求のステータスを確認して、MAV通知に応答します。

a. 要求が承認された場合は、CLIメッセージに応答して処理を完了します。

例：

```
cluster-1::> security multi-admin-verify request show 3
```

```
    Request Index: 3
      Operation: volume delete
        Query: -vserver vs0 -volume vol1
        State: approved
Required Approvers: 1
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
    Approvals: admin2
    User Vetoed: -
      Vserver: cluster-1
  User Requested: admin
    Time Created: 2/25/2022 13:32:03
    Time Approved: 2/25/2022 13:35:36
      Comment: -
  Users Permitted: -
```

```
cluster-1::*> volume delete -volume vol1 -vserver vs0
```

```
Info: Volume "vol1" in Vserver "vs0" will be marked as deleted and
placed in the volume recovery queue. The space used by the volume
will be recovered only after the retention period of 12 hours has
completed. To recover the space immediately, get the volume name
using (privilege:advanced) "volume recovery-queue show vol1_*" and
then "volume recovery-queue purge -vserver vs0 -volume <volume_name>"
command. To recover the volume use the (privilege:advanced) "volume
recovery-queue recover -vserver vs0 -volume <volume_name>"
command.
```

```
Warning: Are you sure you want to delete volume "vol1" in Vserver
"vs0" ?
{y|n}: y
```

- b. 要求が拒否された場合、または有効期限を過ぎた場合は、要求を削除して、再送信するかMAV管理者に問い合わせます。

例：

```
cluster-1::> security multi-admin-verify request show 3

Request Index: 3
Operation: volume delete
Query: -vserver vs0 -volume voll
State: vetoed
Required Approvers: 1
Pending Approvers: 1
Approval Expiry: 2/25/2022 14:38:47
Execution Expiry: -
Approvals: -
User Vetoed: admin2
Vserver: cluster-1
User Requested: admin
Time Created: 2/25/2022 13:38:47
Time Approved: -
Comment: -
Users Permitted: -

cluster-1::*> volume delete -volume voll -vserver vs0

Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

関連情報

- ["セキュリティ多管理者認証"](#)

ONTAPでMAV保護操作リクエストを管理する

MAV承認グループ（MAV管理者）の管理者は、保留中の処理実行要求の通知を受けた場合、一定時間（承認有効期限）内に承認または拒否のメッセージで応答する必要があります。十分な数の承認が得られない場合、要求者は要求を削除して、別の要求を行う必要があります。

タスク概要

承認要求はインデックス番号で識別され、Eメール メッセージおよび要求キューに表示されます。



multi-admin-verify 終了状態のリクエストは自動的に上書きまたは削除される可能性があります。"監査ログ"を使用して以前のリクエストを確認してください。

要求キューには次の情報が表示されます。

処理

リクエストが作成される保護された操作。

クエリ

ユーザーが操作を適用するオブジェクト（複数可）。

状態

リクエストの現在の状態（保留中、承認済み、拒否、期限切れ、実行済み）。リクエストがいずれかの承認者によって拒否された場合、それ以上のアクションは実行できません。

必要な承認者

リクエストを承認するために必要なMAV管理者の数。ユーザーは操作ルールにrequired-approversパラメータを設定できます。ユーザーがルールにrequired-approversを設定していない場合は、グローバル設定のrequired-approversが適用されます。

承認待ちの承認者

リクエストが承認済みとしてマークされるために、リクエストを承認する必要がある MAV 管理者の数。

承認の有効期限

MAV管理者が承認要求に応答する必要がある期間。権限のあるユーザーは、操作ルールの承認期限を設定できます。ルールに承認期限が設定されていない場合は、グローバル設定の承認期限が適用されます。

実行の有効期限

要求元の管理者が操作を完了しなければならない期間。権限のあるユーザーは誰でも操作ルールのexecution-expiryを設定できます。ルールにexecution-expiryが設定されていない場合は、グローバル設定のexecution-expiryが適用されます。

承認されたユーザー

リクエストを承認した MAV 管理者。

ユーザーが拒否しました

リクエストを拒否した MAV 管理者。

ストレージVM（vserver）

リクエストが関連付けられている SVM。このリリースでは、管理 SVM のみがサポートされます。

ユーザーがリクエストした

リクエストを作成したユーザーのユーザー名。

作成時刻

リクエストが作成された時刻。

承認された時間

リクエストの状態が承認済みに変更された時刻。

コメント

リクエストに関連付けられているコメント。

許可されたユーザー

リクエストが承認された保護された操作の実行を許可されているユーザーのリスト。`users-permitted`が空の場合、適切な権限を持つすべてのユーザーが操作を実行できます。

System Manager

MAV管理者は、承認リクエストの詳細、リクエストの有効期限、リクエストを承認または拒否するためのリンクが記載されたメールを受け取ります。メール内のリンクをクリックするか、System Manager の*イベントとジョブ> リクエスト*に移動することで、承認ダイアログにアクセスできます。

Requests ウィンドウは、マルチ管理者検証が有効になっている場合に使用でき、ユーザーのログイン ID と MAV ロール（承認者かどうか）に基づいて保留中のリクエストが表示されます。

- 処理
- Index（番号）
- Status（Pending、Approved、Rejected、Executed、Expired）

承認者が1人でも要求を却下した場合、それ以上の操作を行うことはできません。

- Query（要求された処理のパラメータまたは値）
- Requesting User
- Request Expires On
- Pending Approvers（人数）
- Potential Approvers（人数）

MAV管理者は、このウィンドウで個々の処理または複数の処理を承認、却下、削除できます。ただし、MAV管理者が要求元ユーザである場合、自身の要求を承認、却下、削除することはできません。

CLI

1. 承認待ちのリクエストがメールで通知された場合は、リクエストのインデックス番号と承認期限を必ずご確認ください。インデックス番号は、下記の*show*または*show-pending*オプションを使用して表示することもできます。
2. 要求を承認または拒否します。

次の操作を行う場合：	入力するコマンド
リクエストを承認する	<code>security multi-admin-verify request approve nn</code>
リクエストを拒否する	<code>security multi-admin-verify request veto nn</code>
すべてのリクエスト、保留中のリクエスト、または単一のリクエストを表示します	<code>`security multi-admin-verify request { show</code>

次の操作を行う場合：	入力するコマンド
show-pending } [nn] { -fields field1[,field2...]	[-instance]}` キュー内のすべてのリクエストを表示するか、保留中のリクエストのみを表示できます。インデックス番号を入力すると、その番号の情報のみが表示されます。特定のフィールドに関する情報（`-fields`パラメータを使用）、またはすべてのフィールドに関する情報（`-instance`パラメータを使用）を表示できます。
リクエストを削除する	security multi-admin-verify request delete nn

例：

次の例では、MAV管理者が、インデックス番号3の要求のEメールを受信したあとに要求を承認します。この要求はすでに1件の承認を獲得しています。

```

cluster1::> security multi-admin-verify request show-pending
Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete - pending 1 julia

cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
Operation: volume delete
Query: -
State: approved
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
Approvals: mav-admin2
User Vetoed: -
Vserver: cluster-1
User Requested: julia
Time Created: 2/25/2022 13:32:03
Time Approved: 2/25/2022 13:35:36
Comment: -
Users Permitted: -

```

例：

次の例は、MAV管理者が、インデックス番号3の要求のEメールを受信したあとに要求を拒否します。この要求はすでに1件の承認を獲得しています。

```
cluster1::> security multi-admin-verify request show-pending
Pending
Index Operation      Query State   Approvers Requestor
-----
3 volume delete - pending 1 pavan

cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
Operation: volume delete
Query: -
State: vetoed
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
Approvals: mav-admin1
User Vetoed: mav-admin2
Vserver: cluster-1
User Requested: pavan
Time Created: 2/25/2022 13:32:03
Time Approved: 2/25/2022 13:35:36
Comment: -
Users Permitted: -
```

関連情報

- ["セキュリティ多管理者認証"](#)

動的許可の管理

ONTAP動的認証について学ぶ

ONTAP 9.15.1以降では、管理者は動的許可を設定し有効化することで、ONTAPへのリモート アクセス時のセキュリティを強化するとともに、悪意のあるユーザによる攻撃の被害を軽減できます。ONTAP 9.15.1の動的許可は初期段階のフレームワークであり、ユーザにセキュリティ スコアを割り当て、その行動が不審な場合に追加の許可チェックを実施するか、操作を完全に拒否できます。管理者はルールを作成、信頼スコアの割り当

て、コマンドの制限を行い、ユーザの特定の行動を許可または拒否するタイミングを指定できます。動的許可の有効化は、クラスタ全体または個別のStorage VMに対して行えます。

動的許可の仕組み

動的許可では、信頼スコア システムに基づき、許可ポリシーに応じた各種信頼レベルをユーザに割り当てます。ユーザの信頼レベルに応じて、その操作を許可または拒否するか、追加の認証を求めることができます。

"動的許可のカスタマイズ"を参照して、基準スコアの重みやその他の動的承認属性を構成する方法の詳細を確認してください。

信頼済みのデバイス

動的許可が使用されている場合、信頼済みのデバイスの定義は、ユーザが認証方法の1つとして公開鍵認証を使用してONTAPにログインするために使用するデバイスです。そのデバイスは、そのユーザのみが対応する秘密鍵を所有しているため、信頼されます。

動的許可の例

例として、3名のユーザがボリュームの削除を試みた場合を考えます。各ユーザの操作試行時には、それぞれのリスクが以下のように評価されます。

- 1番目のユーザは、以前に数回だけ認証に失敗した信頼済みのデバイスからログインしました。そのため、リスクは低いと評価され、追加の認証不要で操作が許可されます。
- 2番目のユーザは、以前に認証に失敗した割合が中程度の信頼済みのデバイスからログインしました。そのため、リスクは中程度と評価され、操作の許可前に追加の認証が求められます。
- 3番目のユーザは、以前に認証に失敗した割合が高い、信頼されていないデバイスからログインしました。そのため、リスクは高いと評価され、操作が拒否されます。

次の手順

- "動的許可の有効化と無効化"
- "動的許可のカスタマイズ"

ONTAPでの動的認可の有効化または無効化

ONTAP 9.15.1以降、管理者は動的認証の設定と有効化を、`visibility`設定をテストするモード、または`enforced`SSH経由で接続するCLIユーザ向けに設定をアクティブ化するモードのいずれかで実行できます。動的認証が不要になった場合は、無効にすることができます。動的認証を無効にしても設定はそのまま残り、後で再度有効にする場合に使用できます。

```
`security dynamic-authorization modify`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-modify.html](https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-modify.html)["ONTAPコマンド リファレンス"]を参照してください。

テスト目的での動的許可の有効化

visibilityモードで動的許可を有効化すると、ユーザを誤ってロックアウトする事態を防ぎつつ、機能のテストを行えます。このモードでは、すべての制限対象操作で信頼スコアがチェックされますが、適用はされません。ただし、動的許可の有効時に拒否または追加認証チャレンジの対象となるすべての操作が記録されます。ベストプラクティスとして、目的の設定を適用する前に、このモードでテストすることが推奨されます。



他の動的認証設定をまだ設定していない場合でも、この手順で初めて動的認証を有効化できます。環境に合わせてカスタマイズするためのその他の動的認証設定を設定する手順については、"[動的許可のカスタマイズ](#)"を参照してください。

手順

1. グローバル設定を構成し、機能の状態を `visibility` に変更することで、可視性モードで動的認証を有効にします。`-vserver` パラメータを使用しない場合、コマンドはクラスタレベルで実行されます。括弧内の値<>を環境に合わせて更新してください。太字のパラメータは必須です：

```
security dynamic-authorization modify \  
<strong>-state visibility</strong> \  
-lower-challenge-boundary <percent> \  
-upper-challenge-boundary <percent> \  
-suppression-interval <interval> \  
-vserver <storage_VM_name>
```

2. `show` コマンドを使用してグローバル構成を表示し、結果を確認します：

```
security dynamic-authorization show
```

enforcedモードでの動的許可の有効化

enforcedモードで動的許可を有効化できます。通常、このモードはvisibilityモードでのテスト実施後に使用します。このモードでは、すべての制限対象操作で信頼スコアがチェックされ、制限条件に該当する場合に操作制限が適用されます。抑制間隔も適用されるため、指定した間隔中は追加の認証チャレンジが行われません。



この手順では、以前に `visibility` モードで動的許可を設定して有効にしていることを前提としています。これを強くお勧めします。

手順

1. `enforced` モードで動的認証を有効にするには、状態を `enforced` に変更します。`-vserver` パラメータを使用しない場合、コマンドはクラスタレベルで実行されます。括弧内の値<>を環境に合わせて更新してください。太字のパラメータは必須です：

```
security dynamic-authorization modify \  
<strong>-state enforced</strong> \  
-vserver <storage_VM_name>
```

2. `show` コマンドを使用してグローバル構成を表示し、結果を確認します：

```
security dynamic-authorization show
```

動的許可の無効化

追加した認証セキュリティが不要になった場合、動的許可を無効化できます。

手順

1. 動的認証を無効化するには、状態を `disabled` に変更してください。`-vserver` パラメータを使用しない場合、コマンドはクラスタ レベルで実行されます。括弧内の値<>は環境に合わせて更新してください。太字のパラメータは必須です：

```
security dynamic-authorization modify \  
<strong>-state disabled</strong> \  
-vserver <storage_VM_name>
```

2. `show` コマンドを使用してグローバル構成を表示し、結果を確認します：

```
security dynamic-authorization show
```

```
`security dynamic-authorization show`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-show.html ["ONTAP コマンド リファレンス  
"^] を参照してください。
```

次の手順

(オプション) 環境に応じて、"[動的許可のカスタマイズ](#)"を参照して他の動的認証設定を構成してください。

ONTAPでの動的認可のカスタマイズ

管理者は、動的許可のさまざまな設定をカスタマイズして、自身がONTAPクラスタにリモートでSSH接続する際のセキュリティを高められます。

セキュリティのニーズに応じて、以下の動的許可設定をカスタマイズできます。

- [\[動的許可グローバル設定の構成\]](#)
- [動的許可の信頼スコア コンポーネントの構成](#)
- [カスタム信頼スコア プロバイダの設定](#)
- [\[制限されたコマンドの設定\]](#)

- [\[動的許可グループの設定\]](#)

動的許可グローバル設定の構成

保護対象のStorage VM、認証チャレンジの抑制間隔、信頼スコア設定など、動的許可のグローバル設定を構成できます。

```
`security login domain-tunnel create`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-modify.html](https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-modify.html) ["ONTAPコマンド リファレンス"^]をご覧ください。

手順

1. 動的認証のグローバル設定を構成します。`-vserver`パラメータを使用しない場合、コマンドはクラスタレベルで実行されます。括弧内の値<>を環境に合わせて更新してください：

```
security dynamic-authorization modify \  
-lower-challenge-boundary <percent> \  
-upper-challenge-boundary <percent> \  
-suppression-interval <interval> \  
-vserver <storage_VM_name>
```

2. 変更後の設定を確認します。

```
security dynamic-authorization show
```

制限されたコマンドの設定

動的認証を有効にすると、この機能にはデフォルトで制限コマンドのセットが含まれます。このリストはニーズに合わせて変更できます。制限コマンドのデフォルトリストについては、"[マルチ管理者検証 \(MAV\) のドキュメント](#)"を参照してください。

制限コマンドの追加

動的許可で制限するコマンドのリストにコマンドを追加できます。

```
`security dynamic-authorization rule create`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-rule-create.html](https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-rule-create.html) ["ONTAPコマンド リファレンス"^]をご覧ください。

手順

1. コマンドを追加します。括弧内の値<>を環境に合わせて更新してください。`-vserver`パラメータを使用しない場合、コマンドはクラスタレベルで実行されます。太字のパラメータは必須です：

```
security dynamic-authorization rule create \  
-query <query> \  
<strong>-operation <text></strong> \  
-index <integer> \  
-vserver <storage_VM_name>
```

2. 変更後の制限コマンド リストを確認します。

```
security dynamic-authorization rule show
```

制限コマンドの削除

動的許可で制限するコマンドのリストからコマンドを削除できます。

```
`security dynamic-authorization rule delete`  
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-rule-delete.html ["ONTAPコマンド リファレンス  
"^]をご覧ください。
```

手順

1. コマンドを削除します。括弧内の値<>を環境に合わせて更新します。`-vserver`パラメータを使用しない場合、コマンドはクラスタ レベルで実行されます。太字のパラメータは必須です：

```
security dynamic-authorization rule delete \  
<strong>-operation <text></strong> \  
-vserver <storage_VM_name>
```

2. 変更後の制限コマンド リストを確認します。

```
security dynamic-authorization rule show
```

動的許可グループの設定

デフォルトでは、動的認証は有効にするとすぐにすべてのユーザーとグループに適用されます。ただし、`security dynamic-authorization group create`コマンドを使用してグループを作成し、特定のユーザーにのみ動的認証を適用することもできます。

動的許可グループの追加

動的許可グループを追加できます。

```
`security dynamic-authorization group create`
```

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-group-create.html>["ONTAPコマンド リファレンス"]をご覧ください。

手順

1. グループを作成します。括弧内の値<>を環境に合わせて更新してください。`-vserver`パラメータを使用しない場合、コマンドはクラスタ レベルで実行されます。太字のパラメータは必須です：

```
security dynamic-authorization group create \  
<strong>-name <group-name></strong> \  
-vserver <storage_VM_name> \  
-excluded-usernames <user1,user2,user3...>
```

2. 変更後の動的許可グループを確認します。

```
security dynamic-authorization group show
```

動的許可グループの削除

動的許可グループを削除できます。

```
`security dynamic-authorization group delete`
```

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-group-delete.html>["ONTAPコマンド リファレンス"]をご覧ください。

手順

1. グループを削除します。括弧内の値<>を環境に合わせて更新してください。`-vserver`パラメータを使用しない場合、コマンドはクラスタ レベルで実行されます。太字のパラメータは必須です：

```
security dynamic-authorization group delete \  
<strong>-name <group-name></strong> \  
-vserver <storage_VM_name>
```

2. 変更後の動的許可グループを確認します。

```
security dynamic-authorization group show
```

動的許可の信頼スコア コンポーネントの構成

スコア重みの上限を設定することで、スコア基準の優先度を変更したり、リスク スコアから特定の基準を削除したりできます。



ベストプラクティスとして、デフォルトのスコア重み値は残しておき、必要に応じて調整だけ行うことが推奨されます。

```
`security dynamic-authorization trust-score-component  
modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-  
cli/security-dynamic-authorization-trust-score-component-  
modify.html["ONTAP コマンド リファレンス"^]を参照してください。
```

以下に、変更可能なコンポーネントをデフォルトのスコア重みおよび重み（パーセント）とともに示します。

条件	コンポーネント名	デフォルトの未加工スコアの重み	デフォルトのパーセンテージの重み
デバイスの信頼度	trusted-device	20	50
ユーザのログイン認証履歴	authentication-history	20	50

手順

1. 信頼スコアの構成要素を変更します。括弧内の値<>を環境に合わせて更新してください。`-vserver`パラメータを指定しない場合、コマンドはクラスタレベルで実行されます。太字のパラメータは必須です：

```
security dynamic-authorization trust-score-component modify \  
<strong>-component <component-name></strong> \  
<strong>-weight <integer></strong> \  
-vserver <storage_VM_name>
```

2. 変更後の信頼スコア コンポーネント設定を確認します。

```
security dynamic-authorization trust-score-component show
```

ユーザの信頼スコアのリセット

ユーザがシステム ポリシーによりアクセスを拒否されたものの、その身元を証明可能な場合、管理者はそのユーザの信頼スコアをリセットできます。

```
`security dynamic-authorization user-trust-score reset`
```

の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-dynamic-authorization-user-trust-score-reset.html>["ONTAP コマンド リファレンス"]をご覧ください。

手順

1. コマンドを追加します。リセット可能な信頼スコア コンポーネントのリストについては、[動的許可の信頼スコア コンポーネントの構成](#)を参照してください。括弧<>内の値を環境に合わせて更新してください。
`-vserver`パラメータを使用しない場合、コマンドはクラスタ レベルで実行されます。太字のパラメータは必須です (：)

```
security dynamic-authorization user-trust-score reset \  
<strong>-username <username></strong> \  
<strong>-component <component-name></strong> \  
-vserver <storage_VM_name>
```

信頼スコアの閲覧

ユーザは、ログイン セッションにおける自分の信頼スコアを閲覧できます。

手順

1. 信頼スコアを表示します。

```
security login whoami
```

次のような出力が表示されます。

```
User: admin  
Role: admin  
Trust Score: 50
```

`security login whoami`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/security-login-whoami.html>["ONTAP コマンド リファレンス"]をご覧ください。

カスタム信頼スコア プロバイダの設定

すでに外部の信頼スコア プロバイダからスコア設定方法を受信している場合、動的許可設定にカスタム プロバイダを追加できます。

開始する前に

- カスタム信頼スコア プロバイダはJSON応答を返せなくてはなりません。次の構文要件を満たす必要があります。
 - 信頼スコアを返すフィールドは、配列要素ではなくスカラーである必要があります。
 - 信頼スコアを返すフィールドは、`trust_score.value`などのネストされたフィールドにすることができます。
 - JSON応答に、信頼スコアの数値を返すフィールドが含まれている必要があります。ネイティブでこのフィールドが存在しない場合は、この値を返すラッパー スクリプトを作成できます。
- 提供する値は信頼スコアとリスク スコアのいずれかを指定できます。信頼スコアとリスク スコアの違いは、前者は信頼度が高いほどスコアが高くなるのに対し、後者はその反対であることです。たとえば、スコア範囲が0～100で信頼スコアが90の場合、スコアの信頼度が非常に高いとみなされ、通常は追加チャレンジなしで「許可」されます。反対に、スコア範囲が0～100でリスク スコアが90の場合、リスクが高いとみなされ、通常は追加チャレンジなしで「拒否」されます。
- カスタム信頼スコア プロバイダはONTAP REST API経由でアクセス可能である必要があります。
- カスタム信頼スコア プロバイダは、いずれかのサポート対象パラメータで設定可能である必要があります。サポート対象パラメータ一覧にない設定が必要なカスタム信頼スコア プロバイダは使用できません。

```
`security dynamic-authorization trust-score-component
create`の詳細については、link:https://docs.netapp.com/us-en/ontap-
cli/security-dynamic-authorization-trust-score-component-
create.html["ONTAPコマンド リファレンス"]を参照してください。
```

手順

1. カスタム信頼スコアプロバイダーを追加します。括弧内の値<>を環境に合わせて更新してください。`-vserver`パラメータを使用しない場合、コマンドはクラスタレベルで実行されます。太字のパラメータは必須です：

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. 変更後の信頼スコア プロバイダ設定を確認します。

```
security dynamic-authorization trust-score-component show
```

外部の信頼スコア プロバイダとの通信にタグを使用できます。こうすることで、機密情報を漏えいさせることなく、URLで信頼スコア プロバイダに情報を送信できます。

```
`security dynamic-authorization trust-score-component  
create`の詳細については、link:https://docs.netapp.com/us-en/ontap-  
cli/security-dynamic-authorization-trust-score-component-  
create.html["ONTAPコマンド リファレンス"]を参照してください。
```

手順

1. トラスト スコア プロバイダ タグを有効にします。括弧内の値<>を環境に合わせて更新してください。`vserver`パラメータを使用しない場合、コマンドはクラスターレベルで実行されます。太字のパラメータは必須です：

```
security dynamic-authorization trust-score-component create \  
<strong>-component <component_name></strong> \  
-weight <initial_score_weight> \  
-max-score <max_score_for_provider> \  
<strong>-provider-uri <provider_URI></strong> \  
-score-field <REST_API_score_field> \  
<strong>-secret-access-key "<key_text>"</strong>
```

例：

```
security dynamic-authorization trust-score-component create -component  
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-  
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score  
-field score -access-key "MIIBBjCB rAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。