認証とアクセス制御
ONTAP 9

NetApp
February 12, 2026

目次

認証とアクセス制御

認証およびアクセス制御の概要

ONTAP WebサービスのONTAPクラスタ認証およびアクセス制御を管理できます。

System ManagerまたはCLIを使用して、クライアントや管理者によるクラスタおよびストレージへのアクセスを制御します。

クラシック System Manager （ ONTAP 9.7 以前でのみ使用可能）を使用している場合は、 "System Manager Classic（ONTAP 9.0～9.7）"を参照してください。

クライアント認証と許可

ONTAPは、信頼できるソースを使用してクライアントマシンとユーザーのIDを検証することで、それらを認証します。ONTAPは、ユーザーの認証情報とファイルまたはディレクトリに設定されている権限を比較することで、ユーザーにファイルまたはディレクトリへのアクセスを許可します。

管理者認証と**RBAC**

管理者は、ローカルまたはリモートのログイン アカウントを使用してクラスタおよびStorage VMへの認証を行います。管理者がアクセスできるコマンドは、ロールベース アクセス制御（RBAC）に基づいて決まります。

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。 • `http` • `ontapi` • `snmp` • `ssh`	
`-authmethod`	アカウントの認証に使用する認証方式。 • `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`	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モニタ（CSHM）によって監視されるクラスタスイッチ、またはMetroClusterヘルスモニタ（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。	

`-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。 • クラスター（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`	（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。	
`-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`	多要素認証を使用する場合の、第2の認証方式。 • `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 認証の順序は、常に公開鍵が先でパスワードがあとです。	
`-is-ldap-fastbind`	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"。	

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`	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： `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	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。	
`-http-proxy`	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： `http-proxy=http://username:password@proxy.example.org:8080`	

-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`	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。 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。 `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。 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。	
`-enabled`	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。	
`-pushinfo`	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。	

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`	（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： • `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 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： • `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 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。	

-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 `"-aggr aggr0"`は `aggr0`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`	（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。 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。 • `install`：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。 • `modify`：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。 • `delete`：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 レベルの設定が使用されます。	

`-state`	動的認証モード。可能な値： • `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`	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。	
`-lower-challenge-boundary`	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。	
`-upper-challenge-boundary`	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。	

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
-common-name	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。	
-size	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。	
-country	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。	
-state	Storage VMが設置されている都道府県。	
-locality	Storage VMが設置されている市区町村。	
-organization	Storage VMを管理している組織。	
-unit	Storage VMを管理している組織内の部門。	
-email-addr	Storage VMの管理担当者のEメール アドレス。	
-hash-function	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 SHA256`です。指定できる値は `SHA1、 SHA256、 `MD5`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。 • `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`	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`）。 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。	

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`	ネーム サービス データベース。 • `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`	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）。 • `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["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

1. 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
   svmadmin1 -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

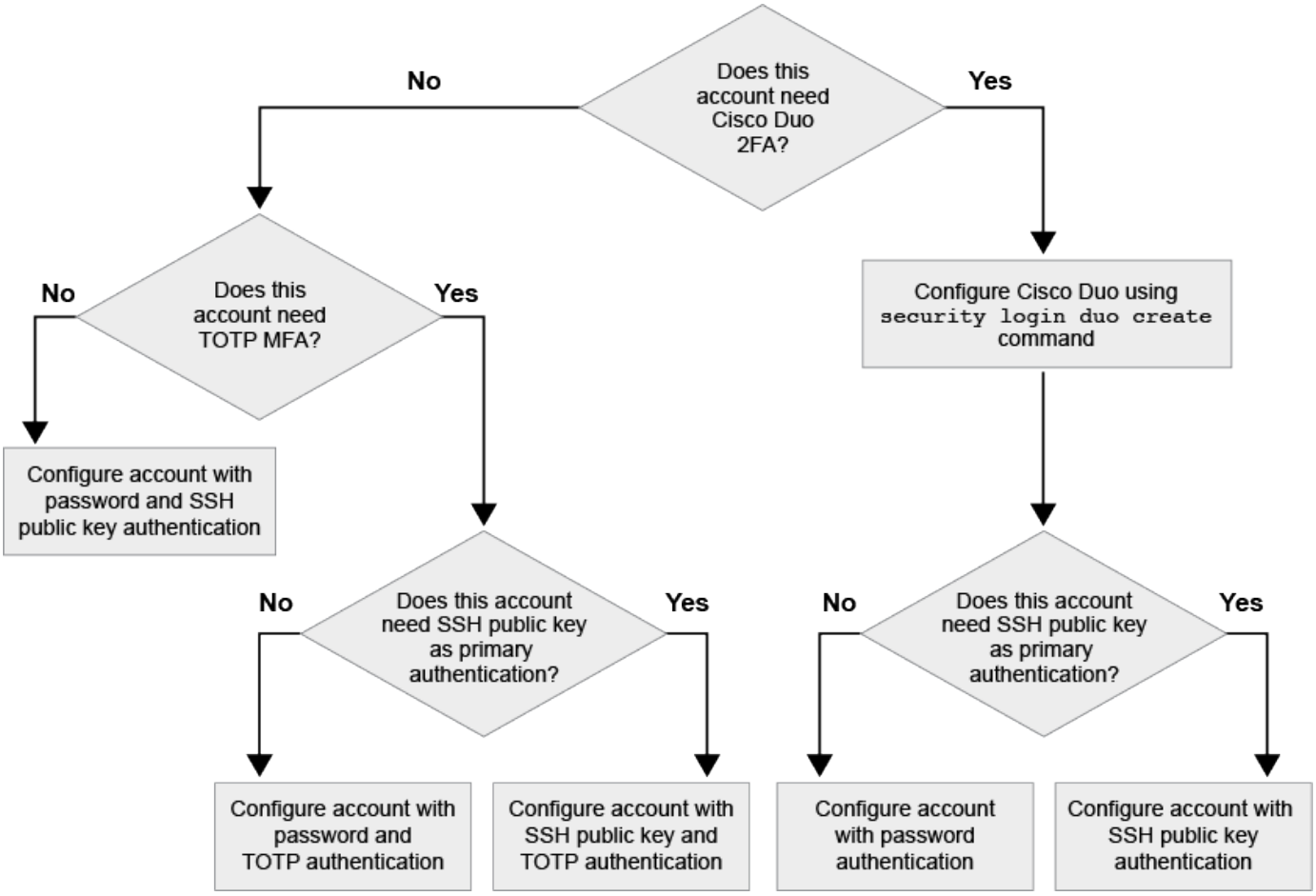
ONTAP多要素認証について学ぶ

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）を組み合わせて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["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["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["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	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

9.13.1以降	ドメイン	公開鍵	新規ユーザー向け
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			既存ユーザーの場合
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

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	`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]`

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	`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]`

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

1. 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SVM`engCluster`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。

2. 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["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	• 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	• 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
• set • system node autosupport	なし	その他のすべてのコマンドディレクトリ(DEFAULT)

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(`DEFAULT`)	readonly	all
• `security login password` 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 • `set`	• 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(`DEFAULT`)	snaplock
all	• `set` • `volume create` • `volume modify` • `volume move` • `volume show`	なし
• `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(`DEFAULT`)
なし	なし	すべてのコマンドディレクトリ(`DEFAULT`)

`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"

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	• 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	• 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	• 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 インターフェイスの監視 • SVMの健全性の監視
vsadmin-backup	• 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	• 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 インターフェイスの監視
vsadmin-readonly	• 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 インターフェイスの監視 • 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生じ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	• `security login create` • `security login delete`	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	• `security certificate create` • `security certificate install`	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	• `security login create -application ssh`	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	• `system license add` • `system license delete`	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	• `system node image update` • `system node upgrade-revert`	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	• `security login role create` • `security login role modify`	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	• `cluster add-node` • `cluster remove-node` • `cluster modify`	クラスターの拡張または再構成のために昇格します。
SVMの管理	• `vserver create` • `vserver delete` • `vserver modify`	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	• `volume create` • `volume delete` • `volume modify`	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	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	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	• `network interface create` • `network port vlan create`	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	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	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	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	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	• `qos policy-group create` • `qos policy-group modify`	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	• `security audit log show`	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	• `event notification create` • `event notification modify`	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	• `volume show` • `security audit log show`	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	• `security login show` • `security login role show`	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

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["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 `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["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["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 `<STORAGE_VM_NAME>`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ベールに所在する、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。

`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署名付きサーバー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	• [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	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]

ローカル証明書機関	• [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. + Add 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["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、SVM`vs1.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より前のリリースへリバートする際に、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。
   a. すべての MD5 管理者アカウントを期限切れにします： `security login expire-password -vserver * -username * -hash-function md5`

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

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

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操作用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 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 delete` [3]
- `security anti-ransomware volume attack clear-suspect` [1]
- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume event-log modify` [2]
- `security anti-ransomware volume pause` [1]
- `security anti-ransomware vserver event-log modify` [2]
- `security audit modify` [3]
- `security ipsec config modify` [3]
- `security ipsec policy create` [3]
- `security ipsec policy delete` [3]
- `security ipsec policy modify` [3]
- `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-passphrase` [3]
- `security saml-sp create` [3]

- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete [4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]

- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume rename [5]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- 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 rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]

- 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 delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- 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-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete [4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]

- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]
- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- 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 rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- 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]

9.15.1

- 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 delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- 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-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume file privileged-delete [3]

- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- 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 rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- 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 options [3]
- vserver peer delete
- vserver security file-directory apply [3]

- vserver security file-directory remove-slag [3]
- 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]

9.14.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- 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 modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- 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 create [2]
- vserver modify [2]
- vserver peer delete

9.13.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume pause [1]
- 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 modify [1]
- 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。

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り、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	`security login show`
現在の管理者の認証情報を変更する	`security login modify <parameters>`
新しい管理者アカウントを作成する	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

`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	`security multi-admin-verify approval-group modify [parameters]`
メンバーを追加または削除する	`security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2…]][-approvers-to-remove approver1[,approver2…]]`
グループを削除する	`security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name`

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

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. 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。
   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。
   c. + 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。
   d. 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	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`
	
	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。
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	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

MAV 構成を変更する（MAV の承認が必要）	`security multi-admin-verify approval-group modify [-approval-groups group1[,group2…]] [-required-approvers nn ] [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`

MAV機能を確認する	`security multi-admin-verify show`
	
	例：
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution Approval Approval`
	`Enabled Approvers Expiry Expiry Groups`
	`------- --------- --------- --------- -----------`
	`true 2 1h 1h mav-grp1`

MAV 機能を無効にする（MAV の承認が必要）	`security multi-admin-verify modify -enabled false`

関連情報

- "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-vsim20::> 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。	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

現在の管理者の認証情報を変更する	`security login modify <parameters>`
	
	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。
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

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	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
ルールを削除します。	`security multi-admin-verify rule delete -operation "protected_operation"`
ルールを表示	`security multi-admin-verify rule show`

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 vol1
             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 vol1 -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	`security multi-admin-verify request approve` *`nn`*
リクエストを拒否する	`security multi-admin-verify request veto` *`nn`*
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	`security multi-admin-verify request { show

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。管理者はルールの作成、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["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["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["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
```

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ー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
```

カスタム信頼スコア プロバイダ タグの設定

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 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 "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

OAuth 2.0を使用した認証と許可

ONTAP OAuth 2.0導入の概要

ONTAP 9.14以降では、Open Authorization（OAuth 2.0）フレームワークを使用して、ONTAPクラスタへのアクセスを制御するオプションがあります。この機能を有効にする際には、ONTAP CLI、System Manager、REST APIなどの任意のONTAP管理インターフェイスを使用します。ただし、OAuth 2.0による許可とアクセス制御は、クライアントがREST APIを使用してONTAPにアクセスする場合のみ適用できます。

OAuth 2.0のサポートはONTAP 9.14.0で初めて導入されました。そのため、ご利用のONTAPリリースに応じて利用可能かどうかが異なります。詳細については、 "ONTAPリリース ノート" をご覧ください。

機能とメリット

ここでは、ONTAPに導入されたOAuth 2.0の主な機能とメリットについて解説します。

OAuth 2.0標準のサポート

OAuth 2.0は、業界標準の許可フレームワークです。保護されたリソースへのアクセスを制限したり、制御したりするために使用するもので、署名付きアクセス トークンを使用します。OAuth 2.0を使用するメリットには、次のようなものがあります。

- 豊富な許可設定オプション
- パスワードなどクライアントのクレデンシャルが露出する可能性がない
- 設定に基づいてトークンの有効期限を設定可能
- REST APIと組み合わせての使用に最適

一般的な許可サーバでテスト済み

ONTAP OAuth 2.0の実装は、次のようにONTAPリリースに基づいたいくつかの一般的なサーバまたはサービスでテストされています。

- ONTAP 9.16.1（グループUUIDと名前のマッピングおよび外部ロールのサポート）：
  - Microsoft Entra ID
- ONTAP 9.14.1（OAuth 2.0の標準機能のサポート）
  - Auth0
  - Active Directoryフェデレーション サービス（ADFS）
  - Keycloak

各ONTAPリリースで利用できる機能の詳細については、"許可サーバとアクセス トークン"を参照してください。

複数の許可サーバの同時接続をサポート

1つのONTAPクラスタに対して、最大8台の許可サーバを定義できます。これにより、多様なセキュリティ環境のニーズを柔軟に満たせます。

RESTロールとの統合

ONTAPでの許可の判定は、最終的にはユーザまたはグループに割り当てられたRESTロールに基づいて行われます。これらのロールは、自己完結型スコープとしてアクセス トークン内で伝送されるか、Active Directoryグループまたは LDAPグループに沿ったローカルONTAP定義に基づきます。

送信者限定アクセス トークンを使用可能

ONTAPと許可サーバを、Mutual Transport Layer Security（mTLS）を使用するように設定して、クライアント認証を強化できます。これにより、OAuth 2.0アクセス トークンを使用できるのが、その発行を受けたクライアントに限定されます。この機能は、FAPIやMITREによって規定されるものを含む、いくつかの一般的なセキュリティ推奨事項に沿ったものであり、それらへの準拠をサポートします。

導入と設定

OAuth 2.0の導入と設定に着手する際に考慮するべき点は、大きく分けていくつかあります。

ONTAP内のOAuth 2.0エンティティ

OAuth 2.0の許可フレームワークでは各種のエンティティが定義されています。いずれも、データセンターまたはネットワーク内の実在する要素または仮想的な要素に対応させることができます。次の表は、OAuth 2.0のエンティティと、ONTAPでそれぞれに対応する概念をまとめたものです。

OAuth 2.0のエンティティ	概要
リソース	内部 ONTAP コマンドを通じて ONTAP リソースへのアクセスを提供する REST API エンドポイント。
リソース オーナー	保護されたリソースを作成した、またはデフォルトでそのリソースを所有しているONTAPクラスタ ユーザです。
リソース サーバ	保護されているリソースのホスト（ONTAPクラスタ）です。
クライアント	リソース オーナーに代わって、またはリソース オーナーから権限を付与されて、REST APIエンドポイントへのアクセスを要求するアプリケーションです。
許可サーバ	通常はアクセス トークンの発行と管理ポリシーの適用を担当する専用サーバです。

ONTAPのコア設定

OAuth 2.0を有効にして使用するように、ONTAPクラスタを設定する必要があります。これには、許可サーバへの接続を確立することや、必要なONTAP許可設定を定義することが含まれます。この設定には、次のいずれかの管理インターフェイスを使用できます。

- ONTAPコマンドライン インターフェイス
- System Manager
- ONTAP REST API

環境とサポート サービス

ONTAPの定義に加えて、許可サーバの設定も必要です。グループとロールのマッピングを使用している場合は、Active DirectoryグループかLDAPに相当するものの設定も必要です。

サポートされるONTAPクライアント

ONTAP 9.14以降、REST APIクライアントはOAuth 2.0を使用してONTAPにアクセスできます。REST API呼び出しを発行する前に、認可サーバからアクセストークンを取得する必要があります。クライアントは、HTTP認可リクエストヘッダーを使用して、このトークンを_ベアラートークン_としてONTAPクラスタに渡します。必要なセキュリティレベルに応じて、クライアント側で証明書を作成してインストールし、mTLSに基づく送信者制約トークンを使用することもできます。

用語の説明

ONTAP で OAuth 2.0 の導入を検討し始める際には、いくつかの用語を理解しておくと役立ちます。OAuth 2.0 に関する詳細情報へのリンクについては、"その他のリソース"をご覧ください。

アクセス トークン

許可サーバによって発行され、保護されたリソースへのアクセス要求を行うためにOAuth 2.0クライアントアプリケーションによって使用されるトークンです。

JSON Webトークン

アクセス トークンのフォーマットに使用される標準です。JSONは、OAuth 2.0のクレームを3つの主要セクションで構成されるコンパクトな形式で表現するために使用されます。

送信者限定アクセス トークン

Mutual Transport Layer Security（mTLS）プロトコルをベースとする、オプションの機能です。トークンで追加の確認クレームを使用することにより、アクセス トークンを、その発行を受けたクライアントしか使用できなくなります。

JSON Webキー セット

JWKSは、クライアントから提示されたJWTトークンを検証するためにONTAPで使用される公開鍵の集合です。キー セットは、通常、専用のURIを介して許可サーバで使用できます。

Scope

スコープは、ONTAP REST APIなどの保護されたリソースへのアプリケーションのアクセスを制限または制御する手段のひとつです。アクセス トークン内の文字列として表されます。

ONTAP RESTロール

ONTAP 9.6で導入されたRESTロールは、ONTAP RBACフレームワークの核となる要素です。これらのロールは、ONTAPで引き続きサポートされている、従来からあるロールとは異なります。ONTAPに導入されたOAuth 2.0では、RESTロールのみがサポートされています。

HTTP許可ヘッダー

REST API呼び出しの一環として、クライアントと関連する権限を識別するためにHTTPリクエストに含まれるヘッダー。認証と認可の実行方法に応じて、いくつかのフレーバーまたは実装が利用可能です。OAuth 2.0アクセストークンをONTAPに提示する場合、そのトークンは_ベアラートークン_として識別されます。

HTTP基本認証

初期のHTTP認証技術は、依然としてONTAPでサポートされています。プレーンテキストのクレデンシャル（ユーザ名とパスワード）は、コロンで連結され、Base64でエンコードされます。文字列は許可要求ヘッダーに配置され、サーバに送信されます。

FAPI

OpenID Foundationのワーキング グループによって、金融業界向けのプロトコル、データ スキーマ、セキュリティに関する推奨事項が提供されています。このAPIは、もともとFinancial Grade APIとして知られていました。

MITRE

米国空軍と米国政府に技術的ガイダンスや安全保障上のガイダンスを提供している、民間の非営利団体です。

その他のリソース

参考資料をいくつか紹介します。OAuth 2.0や関連する規格の詳細については、これらのサイトを参照してください。

プロトコルと標準

- "RFC 6749：OAuth 2.0 認可フレームワーク"
- "RFC 7519：JSON Web Tokens（JWT）"
- "RFC 7523：OAuth 2.0 クライアント認証および認可付与のための JSON Web Token（JWT）プロファイル"
- "RFC 7662：OAuth 2.0 トークンイントロスペクション"
- "RFC 7800：JWTの所有証明キー"
- "RFC 8705：OAuth 2.0 相互TLSクライアント認証と証明書バインドアクセストークン"

組織

- "OpenID Foundation"
- "FAPIワーキンググループ"
- "MITRE"
- "IANA - JWT"

製品とサービス

- "Auth0"
- "Entra ID"
- "ADFSの概要"
- "Keycloak"

その他のツールとユーティリティ

- "Auth0によるJWT"
- "OpenSSL"

NetAppのドキュメントとリソース

- "ONTAP自動化ドキュメント"

概念

ONTAPにおける**OAuth 2.0**認可サーバーとアクセストークン

許可サーバは、OAuth 2.0許可フレームワークの中心的なコンポーネントとして、いくつかの重要な機能を担っています。

OAuth 2.0許可サーバ

許可サーバは、主にアクセス トークンの作成と署名を行います。このアクセス トークンには、クライアント アプリケーションが保護されたリソースに選択的にアクセスするためのIDと許可情報が格納されます。許可サーバは通常、相互に隔離されています。また、スタンドアロンの専用サーバとして導入したり、IDおよびアクセス管理製品の一部として導入したりと、その導入形式はさまざまです。

認可サーバーには、特にOAuth 2.0の機能がより大規模なIDおよびアクセス管理製品やソリューションに組み込まれている場合、異なる用語が使用されることがあります。例えば、*アイデンティティプロバイダー（IdP）*という用語は、*認可サーバー*と同義語として使用されることがよくあります。

管理

アクセス トークンの発行に加えて、許可サーバは、関連する管理サービスも提供します。これは通常、Web ユーザ インターフェイスを介して行われます。たとえば、次のようなことを定義したり管理したりできます。

- ユーザとユーザ認証
- スコープ
- テナントとRealmを通じた管理分離
- ポリシーの適用
- さまざまな外部サービスへの接続
- その他のIDプロトコル（SAMLなど）のサポート

ONTAPは、OAuth 2.0標準に準拠した許可サーバと互換性があります。

ONTAPへの定義

1台以上の許可サーバをONTAPに定義する必要があります。ONTAPは、各サーバとのセキュアな通信を通じてトークンを検証したり、その他の関連タスクを実行したりして、クライアント アプリケーションを支援します。

ONTAPの設定の主な側面を以下に示します。詳細については、"OAuth 2.0の導入シナリオ"も参照してください。

アクセス トークンの検証方法と検証場所

アクセス トークンの検証には、2つのオプションがあります。

- ローカル検証

  ONTAPは、トークンを発行した許可サーバから提供された情報に基づいて、アクセス トークンをローカルで検証できます。許可サーバから取得した情報は、ONTAPによってキャッシュされ、定期的に更新されます。

- リモート イントロスペクション

  リモート イントロスペクションを使用して、許可サーバでトークンを検証することもできます。イントロスペクションは、許可された当事者がアクセス トークンについて許可サーバに問い合わせることを可能にするプロトコルです。イントロスペクションを使えば、ONTAPでアクセス トークンから特定のメタデータを抽出し、トークンを検証することができます。ONTAPは、パフォーマンス上の理由から一部のデータをキャッシュします。

ネットワークの位置

ONTAPは、ファイアウォールの内側にある可能性があります。この場合は、設定の際にプロキシを指定する必要があります。

許可サーバを定義する方法

CLI、System Manager、REST API などの管理インターフェイスを使用して、ONTAP に認証サーバーを定義できます。例えば、CLI ではコマンド `security oauth2 client create`を使用します。

`security oauth2 client create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-oauth2-client-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

許可サーバの数

1つのONTAPクラスタに対して、最大8台の許可サーバを定義できます。発行者または発行者 / オーディエンスのクレームが一意である限り、同じ許可サーバを同じONTAPクラスタに複数回定義できます。たとえば、Keycloakで異なるRealmを使用する場合は、常にこれが該当します。

ONTAPでサポートされるOAuth 2.0の機能

OAuth 2.0のサポートは、最初にONTAP 9.14.1で利用可能になりましたが、その後のリリースで引き続き強化されています。ONTAPでサポートされているOAuth 2.0の機能を以下に説明します。

特定のONTAPリリースで導入された機能は、以降のリリースでも引き継がれます。

ONTAP 9.16.1

ONTAP 9.16.1では、OAuth 2.0の標準機能が拡張され、ネイティブのEntra IDグループ用のEntra ID固有の拡張機能が追加されています。これにより、アクセス トークンで名前の代わりにGUIDを使用できます。さらに、このリリースでは、アクセス トークンの「roles」フィールドを使用してネイティブ アイデンティティ プロバイダのロールをONTAPのロールにマッピングできる外部ロール マッピングのサポートが追加されています。

ONTAP 9.14.1

ONTAP 9.14.1以降では、次のOAuth 2.0の標準機能を通じて、以下を使用しているアプリケーションに対して許可サーバがサポートされます。

- "RFC6749：OAuth 2.0 認可フレームワーク"および "RFC 7519: JSON Web Token（JWT）"に記載されている「iss」、「aud」、「exp」などの標準フィールドを備えたOAuth 2.0。これには、アクセストークン内の「upn」、「appid」、「sub」、「username」、「preferred_username」などのフィールドを通じてユーザーを一意に識別する機能も含まれています。
- 「group」フィールドを使用したグループ名用のADFSベンダー固有の拡張機能。
- 「group」フィールドを使用したグループUUID用のAzureベンダー固有の拡張機能。
- OAuth 2.0のアクセス トークン スコープ内の自己完結型および指定ロールを使用して許可をサポートするONTAPの拡張機能。これには、「scope」フィールドと「scp」フィールド、およびスコープ内のグループ名が含まれます。

OAuth 2.0アクセス トークンの用途

許可サーバによって発行されたOAuth 2.0アクセス トークンは、ONTAPによって検証され、REST APIクライアント要求のロールベースのアクセス制御に使用されます。

アクセス トークンを取得する

アクセス トークンは、REST APIを使用するONTAPクラスタに定義されている許可サーバから取得する必要があります。トークンを取得するには、許可サーバと直接やり取りする必要があります。

ONTAPがアクセス トークンを発行したり、クライアントからの要求を許可サーバにリダイレクトしたりすることはありません。

トークンを要求する方法は、次のようないくつかの要因によって異なります。

- 許可サーバとその設定オプション
- OAuth 2.0のグラント タイプ
- 要求の発行に使用するクライアントやソフトウェア ツール

グラント タイプ

grant とは、OAuth 2.0 アクセストークンをリクエストおよび取得するために用いられる、ネットワークフローのセットを含む明確に定義されたプロセスです。クライアント、環境、セキュリティ要件に応じて、複数の異なるタイプの grant を使用できます。一般的な grant タイプのリストを下の表に示します。

グラント タイプ	概要
クライアント クレデンシャル	一般的なグラント タイプで、クレデンシャル（IDや共有秘密鍵など）のみを使用します。クライアントがリソースのオーナーと密接な信頼関係にあることが想定されています。
パスワード	リソース オーナー パスワード クレデンシャルは、リソース オーナーがクライアントとの信頼関係を確立している場合に使用できるグラント タイプです。また、レガシーHTTPクライアントからOAuth 2.0に移行する場合にも役立ちます。
許可コード	機密クライアントに最適なグラント タイプで、リダイレクトベースのフローに基づいています。アクセス トークンとリフレッシュ トークンのどちらを取得するためにも使用できます。

JWTのコンテンツ

OAuth 2.0アクセス トークンは、JWT形式です。そのコンテンツは、設定に基づいて許可サーバによって作成されます。ただし、クライアント アプリケーションはトークンを解読できません。クライアントには、トークンを検査したり、そのコンテンツを認識したりする理由がありません。

各JWTアクセス トークンには、一連のクレームが格納されています。クレームには、許可サーバの管理定義に基づいて発行者と許可の特性が記述されています。次の表は、標準に登録されているクレームの一部をまとめたものです。すべての文字列で、大文字と小文字が区別されます。

クレーム	キーワード	概要
Issuer	iss	トークンを発行したプリンシパルを特定します。クレームの処理はアプリケーションにより異なります。
Subject	sub	トークンのサブジェクトまたはユーザです。クレーム名は、グローバルまたはローカルで一意のものに限定されます。

クレーム	キーワード	概要
Audience	aud	目的とするトークンの受信者です。文字列の配列として記述されます。
Expiration	exp	トークンが期限切れになり、拒否されるまでの期間です。

詳細については、 "RFC 7519：JSON Web Tokens"を参照してください。

クライアント許可

ONTAPクライアント許可の概要とオプション

ONTAP OAuth 2.0の実装は、柔軟性と堅牢性を考慮した設計になっていて、ONTAP環境の保護に必要な機能を提供します。これには、同時に指定できない設定オプションがいくつかあります。許可の決定は、最終的にはOAuth 2.0のアクセス トークンに含まれている、またはアクセス トークンから導き出されたONTAP RESTロールに基づいて行われます。

OAuth 2.0の認証を設定する場合にのみ"ONTAP RESTロール"を使用できます。以前のONTAPの従来のロールはサポートされていません。

ONTAPは、設定に基づいて最も適切な単一の認証オプションを適用します。ONTAPがクライアントアクセスを決定する方法の詳細については、"ONTAPによるアクセスの制御方法"を参照してください。

OAuth 2.0の自己完結型スコープ

これらのスコープには、1つ以上のカスタムRESTロールが含まれており、それぞれがアクセストークン内の単一の文字列にカプセル化されています。これらはONTAPロール定義とは独立しています。スコープ文字列は認可サーバで設定する必要があります。詳細については、"自己完結型OAuth 2.0スコープ"を参照してください。

ローカル**ONTAP REST**ロール

組み込みまたはカスタムの単一の名前付きRESTロールを使用できます。名前付きロールのスコープ構文は**ontap-role-**<URL-encoded-ONTAP-role-name>です。例えば、ONTAPロールが `admin`の場合、スコープ文字列は `ontap-role-admin`になります。

ユーザ

アプリケーション「http」へのアクセスが定義されたアクセス トークン内のユーザ名を使用できます。ユーザは、定義された認証方法に基づいて、password、domain（Active Directory）、nsswitch（LDAP）の順にテストされます。

グループ

許可にONTAPグループを使用するように許可サーバを設定できます。ローカルONTAPの定義を調べてもアクセスの可否を判定できない場合は、Active Directory（「domain」）グループかLDAP（「nsswitch」）グループが使用されます。グループ情報は、次の2つの方法のいずれかで指定できます。

- OAuth 2.0のスコープ文字列

  グループメンバーシップを持つユーザーが存在しないクライアント資格情報フローを使用した機密アプリケーションをサポートします。スコープ名は **ontap-group-**<URL-encoded-ONTAP-group-name> とする必要があります。例えば、グループが「development」の場合、スコープ文字列は「ontap-group-

development」になります。

- 「グループ」のクレーム

  これは、リソース オーナー（パスワード グラント）フローを使用してADFSによって発行されるアクセストークンが対象です。

詳細については、"ONTAP で OAuth 2.0 または SAML IdP グループを使用する"を参照してください。

ONTAPの自己完結型OAuth 2.0スコープ

自己完結型スコープは、アクセス トークンで伝送される文字列です。それぞれが完結したカスタム ロール定義であり、ONTAPがアクセスの可否を判定するために必要なものがすべて含まれています。スコープは、ONTAP内で定義されているRESTロールとは別の、独立したものです。

スコープ文字列のフォーマット

基本的に、スコープは連続した文字列で表され、コロンで区切られた6つの値で構成されます。ここでは、スコープ文字列で使用されるパラメータについて説明します。

ONTAPリテラル

スコープは、小文字のリテラル値 `ontap`で始まる必要があります。これにより、スコープがONTAPに固有であることが識別されます。

クラスタ

スコープが適用されるONTAPクラスタを定義します。指定できる値は、次のとおりです。

- クラスタUUID

  単一のクラスタを特定します。

- アスタリスク（*）

  スコープをすべてのクラスタに適用することを意味します。

ONTAP CLIコマンド `cluster identity show`を使用して、クラスタのUUIDを表示できます。指定しない場合は、スコープがすべてのクラスタに適用されます。"ONTAPコマンド リファレンス"の `cluster identity show`の詳細をご覧ください。

ロール

自己完結型スコープに含まれるRESTロールの名前です。この値は、ONTAPで確認されたり、ONTAPに定義されている既存のRESTロールと照合されたりすることはありません。この名前は、ロギングに使用されます。

アクセス レベル

この値は、スコープ内でAPIエンドポイントを使用する場合にクライアント アプリケーションに適用されるアクセス レベルを表します。次の表に、設定できる6つの値をまとめておきます。

アクセス レベル	概要
なし	指定したエンドポイントへのアクセスをすべて拒否します。
readonly	GETを使用した読み取りアクセスのみを許可します。
read_create	読み取りアクセスと、POSTを使用した新しいリソース インスタンスの作成を許可します。
read_modify	読み取りアクセスと、PATCHを使用した既存のリソースの更新を許可します。
read_create_modify	削除以外のアクセスをすべて許可します。許可される処理は、GET（読み取り）、POST（作成）、PATCH（更新）です。
all	フル アクセスを許可します。

SVM

スコープが適用されるクラスター内のSVMの名前。すべてのSVMを指定するには、*（アスタリスク）を使用します。

この機能はONTAP 9.14.1では完全にはサポートされていません。SVMパラメータは無視し、プレースホルダとしてアスタリスクを使用できます。 "ONTAPリリース ノート"を確認して、今後のSVMサポートについてチェックしてください。

REST API URI

リソースまたは関連リソースセットへの完全パスまたは部分パス。文字列は `/api`で始まる必要があります。値を指定しない場合、スコープはONTAPクラスタのすべてのAPIエンドポイントに適用されます。

スコープの例

自己完結型スコープの例を、いくつか紹介します。

ontap:*:joes-role:read_create_modify:*:/api/cluster

このロールを割り当てられたユーザーに `/cluster`エンドポイントへの読み取り、作成、および変更アクセス権を付与します。

CLI管理ツール

自己完結型スコープの管理を容易にし、エラーの発生を抑えるために、ONTAP は `security oauth2 scope`入力パラメータに基づいてスコープ文字列を生成する CLI コマンドを提供しています。

このコマンド `security oauth2 scope`には、入力内容に基づいて2つの使用例があります：

- CLIパラメータからスコープ文字列を生成

  このバージョンのコマンドを使用すると、入力したパラメータに基づいてスコープ文字列を生成できます。

- スコープ文字列からCLIパラメータを生成

  このバージョンのコマンドを使用すると、入力したスコープ文字列に基づいてコマンド パラメータを生成できます。

例

次の例は、スコープ文字列を生成するものです。コマンド例に続いて、出力結果も掲載しています。定義は、すべてのクラスタに適用されます。

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

`security oauth2 scope`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+oauth2+scope["ONTAPコマンドリファレンス"^]をご覧ください。

ONTAP での OAuth 2.0 外部ロールマッピング

外部ロールは、ONTAPで使用するように設定されたアイデンティティ プロバイダで定義されます。ONTAP CLIを使用して、これらの外部ロールとONTAPロールのマッピング関係を作成および管理できます。

ONTAP REST APIを使用して外部ロールマッピング機能を設定することもできます。詳細については、 "ONTAP自動化ドキュメント"をご覧ください。

アクセス トークン内の外部ロール

以下は、2つの外部ロールを含むJSONアクセス トークンの一部です。

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

構成

外部ロール マッピング機能は、ONTAPコマンドライン インターフェイスを使用して管理できます。

作成

`security login external-role-mapping create`コマンドを使用して、ロールマッピング設定を定義できます。このコマンドおよび関連オプションを実行するには、ONTAPの*admin*権限レベルが必要です。

パラメータ

グループ マッピングの作成に使用するパラメータを以下に示します。

パラメータ	概要
external-role	外部のアイデンティティ プロバイダで定義されているロールの名前。
provider	アイデンティティ プロバイダの名前。これはシステムの識別子である必要があります。
ontap-role	外部ロールがマッピングされている既存のONTAPロールを示します。

例

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

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

その他のCLI処理

このコマンドでは、次のような追加の処理がサポートされます。

- 表示
- 変更
- 削除

関連情報

- "ONTAPコマンド リファレンス"

ONTAPによるクライアント アクセスの制御方法

OAuth 2.0を適切に設計、導入するには、ONTAPがどのように許可設定を使用してクラ

イアントのアクセス可否を判定しているのかを理解しておく必要があります。ここでは、アクセスを制御するために使用する主な手順をONTAPリリース別に紹介します。

ONTAP 9.15.1では、OAuth 2.0の重要な更新はありませんでした。9.15.1リリースを使用している場合は、ONTAP 9.14.1の説明を参照してください。

関連情報

- "ONTAPでサポートされるOAuth 2.0の機能"

ONTAP 9.16.1

ONTAP 9.16.1では、OAuth 2.0の標準のサポートが拡張され、ネイティブのEntra IDグループ用のMicrosoft Entra ID固有の拡張機能と外部のロール マッピングが追加されています。

ONTAP 9.16.1のクライアント アクセスの制御

ステップ**1**：自己完結型スコープ

アクセス トークンに自己完結型のスコープが含まれている場合、ONTAPは最初にそれらのスコープを調べます。自己完結型スコープがない場合は、手順2に進みます。

1つ以上の自己完結型スコープが存在する場合、ONTAPは明示的な*ALLOW*または*DENY*の決定が下されるまで各スコープを適用します。明示的な決定が下されると、処理は終了します。

ONTAPが明示的にアクセスの可否を判定できない場合は、手順2に進みます。

ステップ**2**：ローカルロールフラグを確認する

ONTAPはブールパラメータ `use-local-roles-if-present`を調べます。このフラグの値は、ONTAPに定義された各認証サーバーに対して個別に設定されます。

- 値が `true`の場合は、手順 3 に進みます。
- 値が `false`の場合、処理は終了し、アクセスは拒否されます。

ステップ**3**：名前付き**ONTAP REST**ロール

アクセストークンの `scope`または `scp`フィールド、あるいはクレームとして名前付きRESTロールが含まれている場合、ONTAPはそのロールを使用してアクセス決定を行います。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。

指定RESTロールがない場合、またはロールが見つからない場合は、手順4に進みます。

ステップ**4**：ユーザー

アクセス トークンからユーザ名が抽出され、アプリケーション「http」にアクセスできるユーザとの照合が試みられます。ユーザは、認証方法に基づいて次の順序で検証されます。

- password
- domain（Active Directory）
- nsswitch（LDAP）

一致するユーザーが見つかった場合、ONTAPはそのユーザーに定義されたロールを使用してアクセスを決定します。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。

一致するユーザがいない場合、またはアクセス トークンにユーザ名が含まれていない場合は、手順5に進みます。

ステップ**5**：グループ

1つ以上のグループが含まれている場合、フォーマットが検査されます。グループがUUIDで表現されている場合は、内部グループマッピングテーブルが検索されます。一致するグループと関連付けられたロールがある場合、ONTAPはグループに定義されているロールを使用してアクセスを決定します。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。詳細については、"ONTAP で OAuth 2.0 または SAML IdP グループを使用する"をご覧ください。

グループが名前で表現され、ドメインまたはnsswitch認証が設定されている場合、ONTAPはそれぞれActive DirectoryまたはLDAPグループとの照合を試みます。グループが一致する場合、ONTAPはグループに定義されているロールを使用してアクセス判定を行います。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。

一致するグループがない場合、またはアクセス トークンにグループが含まれていない場合、アクセスは拒否され、処理は終了します。

ONTAP 9.14.1

サポートされている初期のOAuth 2.0は、OAuth 2.0の標準機能に基づいて、ONTAP 9.14.1で導入されました。

ONTAP 9.14.1のクライアント アクセスの制御

ステップ**1**：自己完結型スコープ

アクセス トークンに自己完結型のスコープが含まれている場合、ONTAPは最初にそれらのスコープを調べます。自己完結型スコープがない場合は、手順2に進みます。

1つ以上の自己完結型スコープが存在する場合、ONTAPは明示的な*ALLOW*または*DENY*の決定が下されるまで各スコープを適用します。明示的な決定が下されると、処理は終了します。

ONTAPが明示的にアクセスの可否を判定できない場合は、手順2に進みます。

ステップ**2**：ローカルロールフラグを確認する

ONTAPはブールパラメータ `use-local-roles-if-present`を調べます。このフラグの値は、ONTAPに定義された各認証サーバーに対して個別に設定されます。

- 値が `true`の場合は、手順 3 に進みます。
- 値が `false`の場合、処理は終了し、アクセスは拒否されます。

ステップ**3**：名前付き**ONTAP REST**ロール

アクセストークンの `scope`または `scp`フィールドに名前付きREST roleが含まれている場合、ONTAPはそのロールを使用してアクセスを決定します。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。

指定RESTロールがない場合、またはロールが見つからない場合は、手順4に進みます。

ステップ**4**：ユーザー

アクセス トークンからユーザ名が抽出され、アプリケーション「http」にアクセスできるユーザとの照合が試みられます。ユーザは、認証方法に基づいて次の順序で検証されます。

- password
- domain（Active Directory）
- nsswitch（LDAP）

一致するユーザーが見つかった場合、ONTAPはそのユーザーに定義されたロールを使用してアクセスを決定します。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。

一致するユーザがいない場合、またはアクセス トークンにユーザ名が含まれていない場合は、手順5に進みます。

ステップ**5**：グループ

1つ以上のグループが含まれていて、domainまたはnsswitchの許可が設定されている場合、ONTAPはそれらのグループとそれぞれActive DirectoryまたはLDAPグループとの照合を試みます。

グループが一致する場合、ONTAPはグループに定義されたロールを使用してアクセスを決定します。その結果は常に*ALLOW*または*DENY*となり、処理は終了します。

一致するグループがない場合、またはアクセス トークンにグループが含まれていない場合、アクセスは拒否され、処理は終了します。

ONTAPに許可サーバを定義する際には、いくつかの設定オプションが用意されています。これらのオプションに基づいて、複数ある導入シナリオのいずれかを使用して、環境に適した許可サーバを定義できます。

設定パラメータの概要

ONTAPに許可サーバを定義する際には、いくつかの設定パラメータを使用できます。これらのパラメータは、通常はどの管理インターフェイスでもサポートされています。

> 個々のパラメータまたはフィールドに使用される名前は、ONTAP管理インターフェイスによって異なる場合があります。管理インターフェイスの違いに対応するために、表内の各パラメータには単一の汎用名が使用されています。文脈に応じて、特定のインターフェイスで使用される正確な名前に読み替えてください。

パラメータ	概要
Name	ONTAPで認識される許可サーバの名前です。
Application	定義が適用されるONTAP内部アプリケーション。これは*http*である必要があります。
Issuer URI	トークンを発行するサイトまたは組織を特定するパスを含むFQDNです。
Provider JWKS URI	ONTAPがアクセス トークンの検証に使用するJSON Webキー セットを取得するパスとファイル名を含むFQDNです。
JWKS refresh interval	ONTAPがプロバイダのJWKS URIから証明書情報を更新する頻度を定めた時間間隔です。値は、ISO-8601形式で指定します。
Introspection endpoint	ONTAPがイントロスペクションを通じたリモート トークン検証に使用するパスを含むFQDNです。
Client ID	許可サーバで定義されているクライアントの名前です。この値を含める場合は、インターフェイスに基づいて関連付けられたクライアント シークレットも指定する必要があります。
Outgoing proxy	ONTAPがファイアウォールの内側にある場合に、許可サーバへのアクセスを提供するために指定します。URIはcurl形式にする必要があります。
Use local roles if present	指定RESTロールやローカル ユーザなど、ローカルのONTAP定義が使用されているかどうかを判定するブール値フラグです。
Remote user claim	ONTAPがローカルユーザを照合するために使用する代替名。アクセストークン内の `sub`フィールドを使用して、ローカルユーザ名と照合します。
Audience	このフィールドは、アクセス トークンを使用できるエンドポイントを定義します。

導入シナリオ

以下に、一般的な導入シナリオをいくつか示します。トークン検証がONTAPによってローカルで実行されるか、認可サーバによってリモートで実行されるかに基づいて整理されています。各シナリオには、必要な設定オプションのリストが含まれています。設定コマンドの例については、"ONTAPでのOAuth 2.0の導入"を参照してください。

認可サーバを定義したら、ONTAP管理インターフェイスからその設定を表示できます。たとえば、ONTAP CLIで `security oauth2 client show`コマンドを使用します。

ローカル検証

次の導入シナリオは、トークン検証がONTAPによってローカルで実行されるものです。

自己完結型スコープを使用（プロキシなし）

OAuth 2.0の自己完結型スコープのみを使用する、最もシンプルな導入シナリオです。ローカルのONTAP ID定義は使用しません。指定が必要なパラメータは次のとおりです。

- Name
- Application（http）
- Provider JWKS URI
- Issuer URI

また、許可サーバにスコープを追加する必要があります。

自己完結型スコープを使用（プロキシあり）

この導入シナリオでは、OAuth 2.0の自己完結型スコープを使用します。ローカルのONTAP ID定義は使用しません。ただし、許可サーバがファイアウォールの内側にあるため、プロキシを設定する必要があります。指定が必要なパラメータは次のとおりです。

- Name
- Application（http）
- Provider JWKS URI
- Outgoing proxy
- Issuer URI
- Audience

また、許可サーバにスコープを追加する必要があります。

ローカル ユーザのロールとデフォルト ユーザ名のマッピングを使用（プロキシあり）

このデプロイメントシナリオでは、デフォルトの名前マッピングを持つローカルユーザーロールを使用します。リモートユーザークレームはデフォルト値 `sub`を使用するため、アクセストークンのこのフィールドはローカルユーザー名との照合に使用されます。ユーザー名は40文字以下である必要があります。認可サーバーはファイアウォールの背後にあるため、プロキシも設定する必要があります。以下のパラメータを含める必要があります：

- Name
- Application（http）
- Provider JWKS URI
- 存在する場合はローカルロールを使用する(`true`
- Outgoing proxy
- Issuer

ローカル ユーザがONTAPに定義されていることを確認する必要があります。

ローカル ユーザのロールと代替ユーザ名マッピングを使用（プロキシあり）

この導入シナリオでは、ローカル ユーザのロールと、ローカルONTAPユーザの照合に使用される代替ユーザ名を使用します。許可サーバがファイアウォールの内側にあるため、プロキシを設定する必要があります。指定が必要なパラメータは次のとおりです。

- Name
- Application（http）
- Provider JWKS URI
- 存在する場合はローカルロールを使用する(`true`
- Remote user claim
- Outgoing proxy
- Issuer URI
- Audience

ローカル ユーザがONTAPに定義されていることを確認する必要があります。

リモート イントロスペクション

次の導入設定は、ONTAPがイントロスペクションを介してリモートでトークン検証を実行する場合のものです。

自己完結型スコープを使用（プロキシなし）

OAuth 2.0の自己完結型スコープを使用する、シンプルな導入シナリオです。ONTAP ID定義は使用しません。次のパラメータを含める必要があります。

- Name
- Application（http）
- Introspection endpoint
- Client ID
- Issuer URI

スコープのほかに、許可サーバでクライアントとクライアント シークレットを定義する必要があります。

関連情報

- "セキュリティ oauth2 クライアント表示"

OAuth 2.0 相互 **TLS** を使用した **ONTAP** クライアント認証

セキュリティ上のニーズに応じて、オプションで相互TLS（mTLS）を設定して強力なクライアント認証を導入できます。OAuth 2.0環境の一部としてONTAPでmTLSを使用すると、アクセス トークンが、その発行を受けたクライアントしか使用できなくなります。

相互TLSとOAuth 2.0

Transport Layer Security（TLS）は、2つのアプリケーション（通常はクライアント ブラウザとWebサーバ）の間にセキュアな通信チャネルを確立するために使用されます。相互TLSは、クライアント証明書を通じた強力なクライアント識別を実現することにより、これを拡張したものです。OAuth 2.0を導入したONTAPクラスタで使用すると、送信者限定アクセス トークンを作成および使用できるので、基本的なmTLS機能が拡張されます。

送信者制約アクセストークンは、元々発行されたクライアントのみが使用できます。この機能をサポートするために、新しい確認クレーム(`cnf`がトークンに挿入されます。このフィールドには、アクセストークンの要求時に使用されたクライアント証明書のダイジェストを保持するプロパティ `x5t#S256`が含まれます。この値は、トークン検証の一環としてONTAPによって検証されます。送信者制約のない認可サーバによって発行されたアクセストークンには、追加の確認クレームは含まれません。

認証サーバごとにmTLSを使用するようにONTAPを設定する必要があります。たとえば、CLIコマンド `security oauth2 client`には、以下の表に示す3つの値に基づいてmTLS処理を制御するパラメータ `use-mutual-tls`が含まれています。

それぞれの設定で、結果とONTAPによって実行されるアクションは、設定パラメータの値、アクセス トークンの内容、クライアント証明書によって異なります。表内のパラメータは、制限が最も緩いものから最も厳しいものの順に並んでいます。

パラメータ	概要
なし	OAuth 2.0の相互TLS認証が、許可サーバで完全に無効になります。ONTAPは、トークンに確認クレームが含まれている場合や、TLS接続でクライアント証明書が提供されている場合であっても、mTLSクライアント証明書認証を実行しません。
request	OAuth 2.0 相互 TLS 認証は、クライアントが送信者制約アクセストークンを提示した場合に強制されます。つまり、アクセストークン内に確認クレーム（プロパティ `x5t#S256`を含む）が存在する場合にのみ mTLS が強制されます。これがデフォルト設定です。
必須	許可サーバによって発行されたすべてのアクセス トークンについて、OAuth 2.0の相互TLS認証が実行されます。したがって、すべてのアクセス トークンが送信者限定である必要があります。アクセス トークンに確認クレームが存在しない場合や、無効なクライアント証明書がある場合、認証とREST API要求は失敗します。

導入フローの概要

ONTAP環境でmTLSとOAuth 2.0を使用する際の一般的な手順を以下に示します。詳細については、 "RFC 8705：OAuth 2.0 相互TLSクライアント認証と証明書バインドアクセストークン"を参照してください。

ステップ1：クライアント証明書を作成してインストールする

クライアントIDの確立は、クライアントの秘密鍵を知っていることの証明がベースになります。対応する公開鍵は、クライアントから提示された署名付きX.509証明書に配置されます。クライアント証明書の大まかな作成手順は、次のとおりです。

1. 公開鍵と秘密鍵のペアを生成する
2. 証明書署名要求を生成する
3. CSRファイルを既知のCAに送信する

4. CAが要求を検証して署名済み証明書を発行する

クライアント証明書は通常、ローカルのオペレーティング システムにインストールしたり、curlなどの一般的なユーティリティで直接使用したりできます。

ステップ**2**：**mTLS**を使用するように**ONTAP**を設定する

ONTAPでmTLSを使用するには、設定が必要です。この設定は認証サーバごとに個別に行います。例えば、CLIでは、コマンド `security oauth2 client`にオプションパラメータ `use-mutual-tls`を指定します。詳細については、"ONTAPでのOAuth 2.0の導入"を参照してください。

ステップ**3**：クライアントがアクセストークンを要求する

クライアントは、ONTAPに設定された許可サーバにアクセス トークンを要求する必要があります。クライアント アプリケーションは、手順1で作成してインストールした証明書でmTLSを使用する必要があります。

ステップ**4**：認可サーバーがアクセストークンを生成する

認可サーバーはクライアントリクエストを検証し、アクセストークンを生成します。この一環として、クライアント証明書のメッセージダイジェストを作成し、確認クレーム（フィールド `cnf`）としてトークンに含めます。

ステップ**5**：クライアントアプリケーションがアクセストークンを**ONTAP**に提示

クライアントアプリケーションはONTAPクラスタに対してREST API呼び出しを行い、アクセストークンを*ベアラートークン*として認可リクエストヘッダーに含めます。クライアントは、アクセストークンのリクエストに使用したのと同じ証明書を使用してmTLSを使用する必要があります。

ステップ **6**：**ONTAP** がクライアントとトークンを検証します。

ONTAPは、HTTPリクエスト内のアクセストークンと、mTLS処理の一部として使用されるクライアント証明書を受け取ります。ONTAPは、まずアクセストークン内の署名を検証します。設定に基づいて、ONTAPはクライアント証明書のメッセージダイジェストを生成し、トークン内の確認クレーム*cnf*と比較します。2つの値が一致する場合、ONTAPは、APIリクエストを発行しているクライアントが、アクセストークンが最初に発行されたクライアントと同じであることを確認したことになります。

関連情報

- "セキュリティ OAuth2 クライアント"

設定と導入

ONTAPでの**OAuth 2.0**の導入準備

ONTAP環境でOAuth 2.0を設定する前に、導入の準備をする必要があります。ここでは、主なタスクと決定が必要な事項の概要を説明します。セクションは、一般に望ましいと考えられる順序で並んでいます。大半の環境にはこれで対応できますが、必要があれば環境に応じて調整してご利用ください。このほか、正式な導入計画の作成も検討してください。

環境に応じて、ONTAPに定義された認可サーバーの設定を選択できます。これには、導入タイプごとに指定する必要があるパラメータ値が含まれます。詳細については、"OAuth 2.0の導入シナリオ"を参照してください。

保護されたリソースとクライアント アプリケーション

OAuth 2.0は、保護されたリソースへのアクセスを制御するための許可フレームワークです。そこで、導入に際してまずは使用可能なリソースと、それらにアクセスする必要があるクライアントを特定することが、重要な最初の手順になります。

クライアント アプリケーションの特定

REST API呼び出しを発行する際にOAuth 2.0を使用するクライアントと、それらのクライアントのアクセス先になるAPIエンドポイントを決定する必要があります。

既存の**ONTAP REST**ロールとローカル ユーザの確認

RESTロールやローカル ユーザなど、既存のONTAP IDの定義を確認する必要があります。OAuth 2.0の設定方法によっては、これらの定義を使用してアクセスを制御できます。

OAuth 2.0へのグローバルな移行

OAuth 2.0許可は段階的に導入することもできますが、各許可サーバにグローバル フラグを設定することで、すべてのREST APIクライアントを一気にOAuth 2.0に移行することもできます。これにより、自己完結型スコープを作成しなくても、ONTAPの既存の設定に基づいてアクセスを制御できます。

許可サーバ

許可サーバは、OAuth 2.0環境において、アクセス トークンを発行し、管理ポリシーを適用するという重要な役割を果たします。

許可サーバの選択とインストール

1つ以上の許可サーバを選択し、インストールする必要があります。スコープの定義方法など、アイデンティティ プロバイダの設定オプションと手順を理解しておくことが重要です。Microsoft Entra IDなど、一部の許可サーバは、名前ではなく、UUIDを使用してグループを表します。

許可ルート**CA**証明書をインストールする必要性の判断

ONTAPは、許可サーバの証明書を使用して、クライアントから提示された署名済みアクセス トークンを検証します。そのためにONTAPに必要なのが、ルートCA証明書と中間証明書です。これらの証明書は、事前にONTAPにインストールされている可能性があります。インストールされていない場合には、インストールする必要があります。

ネットワークの位置の評価と設定

許可サーバがファイアウォールの内側にある場合は、プロキシ サーバを使用するようにONTAPを設定する必要があります。

クライアント認証と許可

クライアントの認証と許可には、考慮すべき側面がいくつかあります。

自己完結型スコープかローカル**ONTAP ID**定義か

大きく分けて、許可サーバで自己完結型スコープを定義する方法と、ロールやユーザを含む既存のローカルONTAP ID定義を使用する方法があります

ローカル**ONTAP**処理に関するオプション

ONTAP ID定義を使用する場合は、次のどれを適用するのかを決定する必要があります。

- 指定RESTロール

- ローカル ユーザの照合
- Active Directoryグループまたは LDAPグループ

ローカル検証とリモート イントロスペクション

アクセス トークンがONTAPによってローカルで検証されるか、イントロスペクションによって許可サーバで検証されるかを決定する必要があります。また、更新間隔など、いくつかの関連する値についても検討する必要があります。

送信者限定アクセス トークン

高度なセキュリティが必要な環境には、mTLSベースの送信者限定アクセス トークンを使用できます。この場合、クライアントごとに証明書が必要です。

UUIDとしてのグループおよび**ID**マッピング

UUIDを使用してグループを表す許可サーバを使用している場合は、これらをグループ名に、場合によっては関連付けられているロールにもマッピングする方法を計画する必要があります。

管理インターフェイス

OAuth 2.0は、次のいずれかのONTAPインターフェイスを通じて管理できます。

- コマンドライン インターフェイス
- System Manager
- REST API

クライアントによるアクセス トークン要求の方法

クライアント アプリケーションは、許可サーバに直接アクセス トークンを要求しなければなりません。グラント タイプを含めて、これをどのように行うかを決定する必要があります。

ONTAPの設定

ONTAPで、いくつかの設定タスクを実行する必要があります。

RESTロールとローカル ユーザの定義

許可の設定に基づいて、ローカルのONTAP識別処理を使用できます。その場合は、RESTロールとユーザ定義を確認および定義する必要があります。また、許可サーバによっては、UUID値に基づいたグループの管理も含まれる場合があります。

コア設定

ONTAPのコア設定を行うには、主に次の3つの手順が必要です。

- 必要に応じて、許可サーバの証明書に署名したCAのルート証明書を（ある場合は中間証明書も）インストールします。
- 許可サーバを定義します。
- クラスタのOAuth 2.0処理を有効にします。

ONTAPでの**OAuth 2.0**の導入

OAuth 2.0のコア機能の導入には、主に3つの手順があります。

開始する前に

ONTAPを設定する前に、OAuth 2.0の導入準備を行う必要があります。例えば、証明書の署名方法やファイアウォールの背後にあるかどうかなど、認可サーバを評価する必要があります。詳細については、"ONTAPでのOAuth 2.0の導入準備"をご覧ください。

ステップ**1**：認証サーバーのルート**CA**証明書をインストールする

ONTAPには、豊富なルートCA証明書が事前にインストールされています。そのため多くの場合、許可サーバの証明書は、追加の設定をしなくてもONTAPによってすぐに認識されます。ただし、許可サーバ証明書の署名方法によっては、ルートCA証明書と中間証明書のインストールが必要になる場合があります。

必要な場合は、次の手順に従って証明書をインストールします。必要な証明書は、すべてクラスタ レベルでインストールする必要があります。

ONTAPへのアクセス方法に対応した手順に従ってください。

例 **1.** 手順

System Manager

1. System Managerで、クラスター > *設定*を選択します。
2. *セキュリティ*セクションまで下にスクロールします。
3. 証明書*の横にある→*をクリックします。
4. *信頼された証明機関*タブで*追加*をクリックします。
5. *Import*をクリックし、証明書ファイルを選択します。
6. 環境に合わせて、パラメータの設定を完了します。
7. *[追加]*をクリックします。

CLI

1. インストールを開始します。

   ```
   security certificate install -type server-ca
   ```

2. 次のコンソール メッセージを探します。

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

3. テキスト エディタで証明書ファイルを開きます。
4. 次の行を含めて、証明書全体をコピーします。

   ```
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

5. コマンド プロンプトの末尾に証明書を貼り付けます。
6. **Enter** を押してインストールを完了します。
7. 次のいずれかを使用して、証明書がインストールされたことを確認します。

   ```
   security certificate show-user-installed
   ```

   ```
   security certificate show
   ```

ステップ**2**：認可サーバーを構成する

ONTAPに少なくとも1つの認証サーバーを定義する必要があります。パラメータ値は、設定と導入計画に基づいて選択してください。"OAuth2の導入シナリオ"を確認して、設定に必要な正確なパラメータを決定してください。

許可サーバの定義を変更するために、既存の定義を削除して新しい定義を作成することもできます。

以下に示す例は、"ローカル検証"の最初の単純なデプロイメントシナリオに基づいています。自己完結型スコープはプロキシなしで使用されます。

ONTAPへのアクセス方法に対応した手順に従ってください。CLIの手順では記号変数が使われているので、コマンドを実行する前に置き換える必要があります。

例 **2.** 手順

System Manager

1. System Managerで、クラスター > *設定*を選択します。
2. *セキュリティ*セクションまで下にスクロールします。
3. **OAuth 2.0 authorization***の横にある+*をクリックします。
4. *その他のオプション*を選択します。
5. 環境に必要な値を指定します。例は次のとおりです。
   - Name
   - Application（http）
   - Provider JWKS URI
   - Issuer URI
6. *[追加]*をクリックします。

CLI

1. 改めて定義を作成します。

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

例：

```
security oauth2 client create \
-config-name auth0 \
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
realm/protocol/openid-connect/certs \
-application http \
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

```
`security oauth2 client create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-
cli/security-oauth2-client-create.html["ONTAPコマンド リファレンス
"^]をご覧ください。
```

ステップ**3**：**OAuth 2.0**を有効にする

最後に、OAuth 2.0を有効にします。これはONTAPクラスタのグローバル設定です。

> ONTAP、許可サーバ、サポート サービスがすべて正しく設定されていることを確認できるまで、OAuth 2.0の処理を有効にしないでください。

ONTAPへのアクセス方法に対応した手順に従ってください。

例 **3.** 手順

System Manager

1. System Managerで、クラスター > *設定*を選択します。
2. *Security セクション*まで下にスクロールします。
3. **OAuth 2.0 authorization***の横にある→*をクリックします。
4. **OAuth 2.0** 認証 を有効にします。

CLI

1. OAuth.2.0を有効にします。

   ```
   security oauth2 modify -enabled true
   ```

2. OAuth 2.0が有効になっていることを確認します。

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

関連情報

- "security certificate install"
- "セキュリティ証明書の表示"
- "セキュリティ oauth2 修正"
- "security oauth2 show"

OAuth 2.0を使用して**ONTAP REST API**呼び出しを発行する

ONTAPに導入したOAuth 2.0では、REST APIクライアント アプリケーションがサポートされます。curlを使用して簡単なREST API呼び出しを発行し、OAuth 2.0の使用を開始できます。ここでは、ONTAPクラスタのバージョンを取得する例を紹介します。

開始する前に

ONTAPクラスタにOAuth 2.0の機能を設定して有効にする必要があります。これには、許可サーバの定義が含まれます。

ステップ**1**：アクセストークンを取得する

REST API呼び出しで使用するアクセス トークンを取得する必要があります。トークンの要求はONTAPの外部で実行され、正確な手順は許可サーバとその設定によって異なります。Webブラウザ、curlコマンド、またはプログラミング言語を通じてトークンを要求できます。

参考までに、curlを使用してKeycloakからアクセス トークンを要求する方法を掲載します。

Keycloakの例

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

返されたトークンは、コピーして保存する必要があります。

ステップ**2**：**REST API**呼び出しを発行する

有効なアクセス トークンを取得したら、curlコマンドとアクセス トークンを使用してREST API呼び出しを発行できます。

パラメータと変数

次の表は、curlの例にある2つの変数についての解説です。

変数	概要
$FQDN_IP	ONTAP管理LIFの完全修飾ドメイン名またはIPアドレスです。
$ACCESS_TOKEN	許可サーバによって発行されたOAuth 2.0アクセス トークンです。

curlの例を実行する前に、Bashシェル環境でこれらの変数を設定する必要があります。たとえば、Linux CLIで次のコマンドを入力して、FQDN変数を設定および表示します。

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

ローカルのBashシェルで両方の変数を定義したら、curlコマンドをコピーしてCLIに貼り付けます。*Enter*キーを押して変数を置き換え、コマンドを実行します。

Curlの例

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

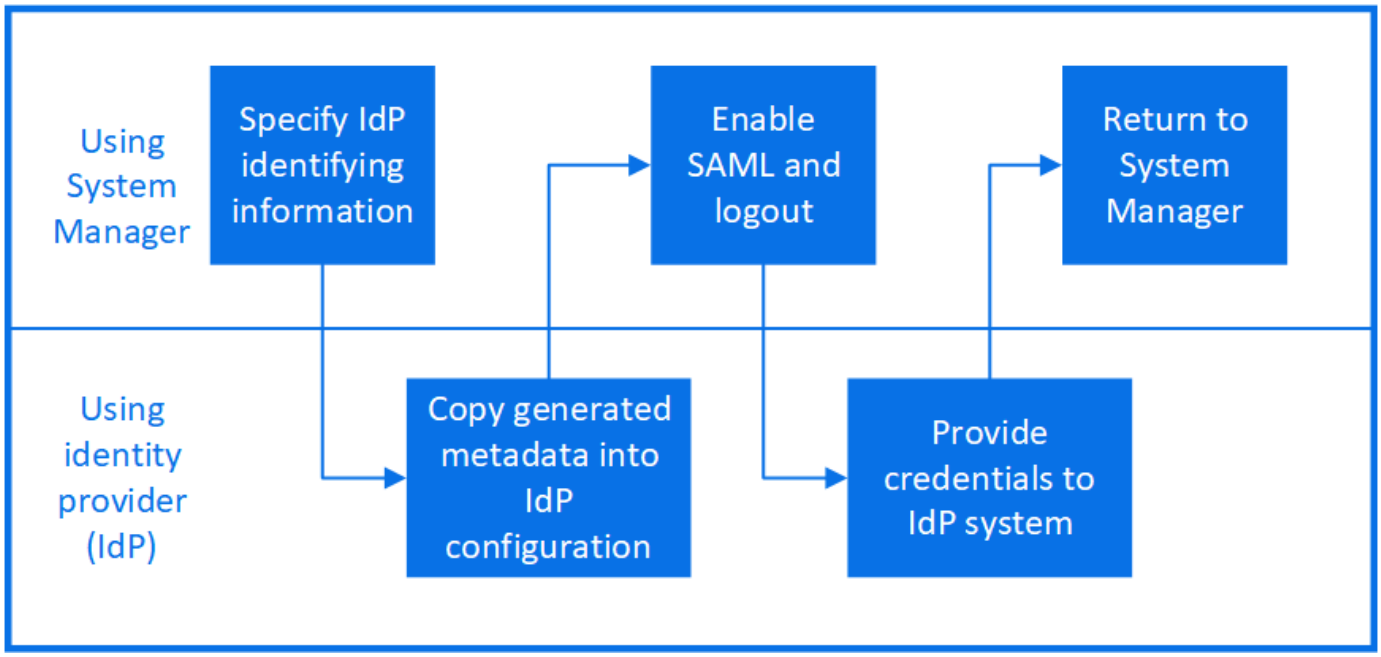
リモートONTAPユーザのSAML認証を設定する

ONTAP 9.3以降では、WebサービスにSecurity Assertion Markup Language（SAML）認証を設定できます。SAML認証を設定して有効にすると、Active DirectoryやLDAPなどのディレクトリ サービス プロバイダではなく、外部のアイデンティティ プロバイダ（IdP）によってユーザが認証されます。SAML認証が無効な場合は、Active DirectoryやLDAPなどの設定済みのディレクトリ サービス プロバイダが認証に使用されます。

SAML認証の有効化

System ManagerまたはCLIを使用してSAML認証を有効にするには、次の手順を実行します。クラスタでONTAP 9.7以前が実行されている場合は、System Managerで実行する手順が異なります。使用しているシステムで利用可能なSystem Managerのオンライン ヘルプを参照してください。

SAML認証を有効にすると、SAML認証が設定されているリモートユーザーのみがSystem Manager GUIにアクセスできるようになります。SAML認証を有効にすると、ローカルユーザーはSystem Manager GUIにアクセスできなくなります。



タスク概要

- SAML認証は、ONTAP `http`アプリケーションと `ontapi`アプリケーションにのみ適用されます。

`http`および `ontapi`アプリケーションは、Service Processor Infrastructure、ONTAP API、およびSystem Managerの各Webサービスによって使用されます。

- SAML認証は、管理SVMへのアクセス時にのみ適用できます。
- ONTAP 9.17.1以降では、IdPが提供するグループ情報をONTAPロールにマッピングできるようになりました。これにより、IdPで定義されたグループに基づいてユーザにロールを割り当てることができます。詳細については、"ONTAP で OAuth 2.0 または SAML IdP グループを使用する"を参照してください。

System Managerでは、次のIdPが検証済みです。

- Microsoft Entra ID（ONTAP 9.17.1以降で検証済み）
- Active Directoryフェデレーション サービス
- Cisco Duo（次のONTAPバージョンで検証済み：）
  - 9.7P21 以降の 9.7 リリース（ "System Manager Classicドキュメント"を参照）
  - 9.8P17以降の9.8パッチリリース
  - 9.9.1P13以降の9.9.1パッチリリース
  - 9.10.1P9以降の9.10.1パッチリリース
  - 9.11.1P4以降の9.11.1パッチリリース
  - 9.12.1以降のリリース
- Shibboleth

開始する前に

- リモート認証に使用するIdPは設定済みである必要があります。IdPのURIが必要です。IdP URIは、ONTAPが認証要求を送信し、応答を受信するWebアドレスです。
- ONTAPクラスタとIdPの間でポート443が開いている必要があります。
- ONTAPクラスタとIdPは、それぞれ相手の完全修飾ドメイン名にpingを実行できる必要があります。DNSが正しく設定され、クラスタ証明書の有効期限が切れていないことを確認してください。
- 必要に応じて、IdPの信頼できる証明機関（CA）をONTAPに追加します。"System ManagerでONTAP証明書を管理する"できます。IdPでONTAPクラスタ証明書を設定する必要がある場合があります。
- ONTAPクラスタの"サービス プロセッサ（SP）"コンソールにアクセスできる必要があります。SAMLの設定が間違っている場合は、SPコンソールからSAMLを無効にする必要があります。
- Entra ID（ONTAP 9.17.1以降で検証済み）を使用している場合は、ONTAP SAML設定を作成する前に、ONTAPメタデータでEntra IDを設定する必要があります。Entra IDは、ONTAPメタデータで設定されるまでIdP URIを提供しません。IdP URIは、ONTAP SAML設定を作成するために必要です。
  - System Managerを使用してSAMLを設定する場合は、System ManagerがONTAPメタデータを提供するまで、IdP URIフィールドを空白のままにしておきます。ONTAPメタデータを使用してEntra IDを設定し、SAML設定を有効にする前にIdP URIをSystem Managerにコピーしてください。
  - ONTAP CLIを使用してSAMLを設定する場合は、ONTAP SAML設定を有効にする前にONTAPメタデータを生成する必要があります。ONTAPメタデータファイルは、以下のコマンドで生成できます：

```
security saml-sp default-metadata create -sp-host <ontap_host_name>
```

`ontap_host_name`は、SAMLサービスプロバイダホスト（この場合はONTAPシステム）のホスト名またはIPアドレスです。デフォルトでは、クラスタ管理IPアドレスが使用されます。オプションでONTAPサーバ証明書情報を指定できます。デフォルトでは、ONTAPWebサーバ証明書情報が使用されます。

提供されたメタデータを使用してEntra IDを設定してください。ONTAP SAML設定を作成する前に、Entra IDを設定する必要があります。Entraの設定が完了したら、以下のCLI手順に進んでください。

- クラスタ内のすべてのノードがバージョン9.17.1になるまで、Entra IDのONTAPメタデータを生成することはできません。

手順

環境に応じて、次の手順を実行します。

System Manager

1. *[クラスタ] > [設定]*をクリックします。
2. *SAML 認証*の横にある⚙をクリックします。
3. *SAML認証を有効にする*チェックボックスがオンになっていることを確認します。
4. IdP URIのURL（"https://"を含む）を入力してください。Entra IDをご利用の場合は、この手順をスキップしてください。
5. 必要に応じてホストシステムのアドレスを変更します。これは、認証後にIdPが接続するアドレスです。デフォルトはクラスタ管理IPアドレスです。
6. 正しい証明書が使用されていることを確認します。
   - システムに「サーバ」タイプの証明書が1つだけ適用されている場合、その証明書はデフォルトとみなされ、画面には表示されません。
   - システムに「サーバー」タイプの証明書が複数マッピングされている場合、そのうちの1つが表示されます。別の証明書を選択するには、*Change*をクリックしてください。
7. *Save*をクリックします。確認ウィンドウにメタデータ情報が表示され、クリップボードに自動的にコピーされます。
8. 指定したIdPシステムにアクセスし、クリップボードからメタデータをコピーしてシステムメタデータを更新します。Entra IDを使用している場合は、システムメタデータを使用してEntra IDを設定した後、IdP URIをONTAPにコピーしてください。
9. 確認ウィンドウ（System Manager内）に戻り、*ホスト URI またはメタデータを使用して IdP を構成しました*のチェックボックスをオンにします。
10. SAMLベースの認証を有効にするには、*ログアウト*をクリックします。IdPシステムに認証画面が表示されます。
11. IdPサインオンページで、SAMLベースの認証情報を入力します。認証情報が検証されると、System Managerのホームページに移動します。

CLI

1. SAMLの設定を作成して、ONTAPがIdPメタデータにアクセスできるようにします。

   ```
   security saml-sp create -idp-uri <idp_uri> -sp-host <ontap_host_name>
   ```

   `idp_uri`は、IdP メタデータをダウンロードできる IdP ホストの FTP または HTTP アドレスです。

   > ⓘ 一部のURLには疑問符（?）が含まれています。疑問符はONTAPコマンドラインのアクティブヘルプを起動します。疑問符を含むURLを入力するには、まずコマンド `set -active-help false`でアクティブヘルプを無効にする必要があります。アクティブヘルプは、後でコマンド `set -active-help true`で再度有効にすることができます。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。

   `ontap_host_name`は、SAMLサービスプロバイダホスト（この場合はONTAPシステム）のホスト名またはIPアドレスです。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。

   必要に応じて、ONTAPサーバ証明書の情報を指定できます。デフォルトでは、ONTAP Webサーバ証明書の情報が使用されます。

```
cluster_12::> security saml-sp create -idp-uri
https://example.url.net/idp/shibboleth

Warning: This restarts the web server. Any HTTP/S connections that
are active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and ONTAP users for the same directory server
domain to ensure that users are the same for different
authentication methods. See the "security login show" command for
the ONTAP user configuration.
```

ONTAPホスト メタデータにアクセスするためのURLが表示されます。

2. IdPホストから、ONTAPホストのメタデータを使用して IdPを設定する を実行します。Entra IDを使用している場合は、この手順はすでに完了しています。
3. IdP が設定されたら、SAML 設定を有効にします：

```
security saml-sp modify -is-enabled true
```

> `http`または `ontapi`アプリケーションにアクセスする既存のユーザは、SAML認証用に自動的に設定されます。

4. SAMLの設定後に `http`または `ontapi`アプリケーションのユーザを作成する場合は、新規ユーザの認証方法としてSAMLを指定してください。ONTAP 9.17.1より前のバージョンでは、SAMLを有効にすると、既存の `http`または `ontapi`ユーザに対してSAMLログインが自動的に作成されます。新規ユーザはSAML用に設定する必要があります。ONTAP 9.17.1以降では、 `password`、domain、または `nsswitch`認証方法で作成されたすべてのユーザは、SAMLを有効にするとIdPに対して自動的に認証されます。

   a. SAML認証を使用した新規ユーザーのログイン方法を作成します。 `user_name`は、IdPで設定されたユーザー名と一致する必要があります。

> この `user_name`値は大文字と小文字が区別されます。Entra IDを使用していない場合は、ユーザー名のみを含め、ドメインの部分は含めないでください。Entra IDを使用している場合は、ドメインを含むユーザー名を作成できます（例：*user_name@domain.com*）。

```
security login create -user-or-group-name <user_name> -application [http
| ontapi] -authentication-method saml -vserver <svm_name>
```

例：

```
cluster_12::> security login create -user-or-group-name admin1
-application http -authentication-method saml -vserver cluster_12
```

b. ユーザ エントリが作成されたことを確認します。

```
security login show
```

例：

```
cluster_12::> security login show

Vserver: cluster_12

Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked
Method
-------------- ----------- ------------- ---------------- ------
--------------
admin          console     password      admin            no
none
admin          http        password      admin            no
none
admin          http        saml          admin            -
none
admin          ontapi      password      admin            no
none
admin          ontapi      saml          admin            -
none
admin          service-processor
                           password      admin            no
none
admin          ssh         password      admin            no
none
admin1         http        password      backup           no
none
admin1         http        saml          backup           -
none
```

+
`security login 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。

SAML認証の無効化

外部Identity Provider（IdP）によるリモートSystem Managerユーザの認証を停止したい場合は、SAML認証を無効にすることができます。SAML認証を無効にすると、ローカルユーザ認証、またはActive DirectoryやLDAPなどの設定済みディレクトリサービスプロバイダがユーザ認証に使用されます。

環境に応じて、次の手順を実行します。

例 **4.** 手順

System Manager

1. *[クラスタ] > [設定]*をクリックします。
2. *SAML認証*で、*有効*トグルボタンをクリックします。
3. オプション：*SAML 認証*の横にある をクリックし、*SAML 認証を有効にする*チェックボックスをオフにすることもできます。

CLI

1. SAML認証を無効にします。

   ```
   security saml-sp modify -is-enabled false
   ```

2. SAML認証を使用しなくなった場合やIdPを変更する場合は、SAMLの設定を削除します。

   ```
   security saml-sp delete
   ```

サードパーティのIdPを構成する

タスク概要

ONTAPで認証するには、IdPの設定を変更する必要がある場合があります。次のセクションでは、サポートされているIdPsの設定情報について説明します。

Entra ID

Entra IDを設定する際は、新しいアプリケーションを作成し、ONTAPから提供されたメタデータを使用してSAMLサインオンを設定します。アプリケーションの作成後、アプリケーションのSAML設定の「属性とクレーム」セクションを以下の内容に合わせて編集します：

設定	**Value**
Name	urn:oid:0.9.2342.19200300.100.1.1
ネームスペース	空白のまま
名前の形式	URI
ソース	属性
ソース属性	user.userprincipalname

Entra ID でグループを使用する場合は、次の設定でグループ要求を追加します：

設定	**Value**
Name	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
ネームスペース	空白のまま
ソース属性	グループID

Entra IDはUUID形式でグループ情報を提供します。Entra IDでグループを使用する方法の詳細については、"UUIDでグループを管理する"をご覧ください。

アプリケーションSAML設定の「SAML証明書」セクションで提供される_App Federation Metadata URL_は、ONTAPに入力するIdP URIです。

Entra ID 多要素認証の設定方法については、"Microsoft Entra多要素認証の展開を計画する"を参照してください。

詳細については、"Entra IDドキュメント"を参照してください。

Active Directoryフェデレーション サービス

Active Directory フェデレーションサービス（AD FS）を設定する際は、ONTAPが提供するサービスプロバイダメタデータを使用して、新しいクレーム対応証明書利用者信頼を追加する必要があります。証明書利用者信頼を作成したら、「LDAP属性をクレームとして送信」テンプレートを使用して、証明書利用者信頼のクレーム発行ポリシーに以下のクレームルールを追加します：

属性ストア	**LDAP**属性	送信クレームタイプ
Active Directory	SAM-account-name	Name ID
Active Directory	SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Active Directory	名前の形式	urn:oasis:names:tc:SAML:2.0:attrname-format:uri
Active Directory	トークングループ - ドメイン名で修飾	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
Active Directory	sAMAccountName	urn:oid:1.2.840.113556.1.4.221

AD FS はグループ情報を名前形式で提供します。AD FS でのグループの使用に関する詳細については、"名前でグループを管理する"を参照してください。

詳細については、"AD FS ドキュメント"を参照してください。

Cisco Duo

設定情報については"Cisco Duo ドキュメント"を参照してください。

Shibboleth

Shibboleth IdP を構成する前に、LDAPサーバを構成しておく必要があります。

ONTAPでSAMLを有効にする場合は、提供されたホストメタデータXMLを保存します。Shibbolethがインストールされているホストで、 `metadata/sp-metadata.xml`の内容を、Shibboleth IdPホームディレクトリ内のホストメタデータXMLに置き換えます。

詳細については、"Shibboleth"を参照してください。

SAMLの設定に関する問題のトラブルシューティング

Security Assertion Markup Language（SAML）認証の設定に失敗した場合は、SAMLの設定に失敗した各ノードを手動で修復して、障害からリカバリできます。修復プロセスの際は、Webサーバが再起動され、アクティブなHTTP接続またはHTTPS接続が中断されます。

タスク概要

SAML認証の設定時に、ONTAPはSAMLの設定をノード単位で適用します。SAML認証を有効にすると、ONTAPは設定の問題がある場合に自動的に各ノードを修復しようとします。いずれかのノードでSAMLの設定に関する問題がある場合は、SAML認証を無効にしてから再度有効にすることができます。SAML認証を再度有効にしたあとでも、1つ以上のノードにSAMLの設定を適用できない場合があります。SAMLの設定に失敗したノードを特定し、そのノードを手動で修復できます。

手順

1. advanced権限レベルにログインします。

   ```
   set -privilege advanced
   ```

2. SAMLの設定に失敗したノードを特定します。

   ```
   security saml-sp status show -instance
   ```

   例：

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                Update Status: config-failed
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

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

3. 障害が発生したノードでSAMLの設定を修復します。

   ```
   security saml-sp repair -node <node_name>
   ```

   例：

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

   Webサーバが再起動され、アクティブなHTTP接続またはHTTPS接続が中断されます。

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

4. すべてのノードでSAMLが正常に設定されたことを確認します。

   `security saml-sp status show -instance`

   例：

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                 Update Status: config-success
                Database Epoch: 9
    Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
         ID of SAML Config Job: 179

                          Node: node2
                 Update Status: config-success
                Database Epoch: 9
    Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
         ID of SAML Config Job: 180
2 entries were displayed.
```

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

関連情報

- "ONTAPコマンド リファレンス"
- "セキュリティ SAML-SP"
- "security login create"

ONTAP で OAuth 2.0 または SAML IdP グループを使用する

ONTAPは、OAuth 2.0認証サーバーまたはSAMLアイデンティティプロバイダー（IdP）に基づいてグループを設定するための複数のオプションを提供しています。その後、グ

ループはONTAPがアクセスを決定するために使用するロールにマッピングされます。

ONTAP 9.17.1以降、SAML IdPが提供するグループ情報をONTAPロールにマッピングできます。これにより、IdPで定義されたグループに基づいてユーザーにロールを割り当てることができます。詳細については、"SAML 認証の設定"を参照してください。ONTAP 9.14.1以降、ONTAPはOAuth 2.0のグループ名認証をサポートしています。ONTAP 9.16.1以降、ONTAPはOAuth 2.0のグループUUID認証とロールマッピングをサポートしています。詳細については、"ONTAP OAuth 2.0導入の概要"を参照してください。

グループの識別方法

認可サーバまたはSAML IdPでグループを設定すると、名前またはUUIDを使用してOAuth 2.0アクセストークンまたはSAMLアサーションで識別され、送信されます。ONTAPを設定する前に、認可サーバまたはSAML IdPがグループをどのように処理するかを把握しておく必要があります。

アクセス トークンに複数のグループが含まれている場合、ONTAPは一致するまで各グループの使用を試みます。

グループ名

Active Directory フェデレーションサービス（ADFS）をはじめとする多くの認可サーバーと SAML IdPsは、グループを名前で識別・表現します。以下は、ADFS によって生成された、複数のグループを含む JSON OAuth 2.0 アクセストークンの一部です。詳細については、[名前でグループを管理する]をご覧ください。

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

グループ**UUID**

Microsoft Entra IDなどの一部の認可サーバーとSAML IdPsは、UUIDを使用してグループを識別および表現します。以下は、Entra IDによって生成された、複数のグループを含むOAuth 2.0アクセストークンの一部です。詳細については、UUIDでグループを管理するをご覧ください。

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

名前でグループを管理する

認可サーバーまたはSAML IdPがグループを識別するために名前を使用している場合は、各グループがONTAPクラスタに定義されていることを確認する必要があります。セキュリティ環境によっては、グループが既に定義されている場合があります。

ONTAPグループを定義するCLIコマンドの例を以下に示します。サンプルアクセストークンから取得した名前付きグループを使用していることに注意してください。このコマンドを実行するには、ONTAPの*admin*権限レベルが必要です。

例

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

SAML IdP および OAuth 2.0 認証サーバー グループには `-authentication-method` `domain`または`nsswitch`を使用します。

ONTAP REST APIを使用してこの機能を設定することもできます。 "ONTAP自動化ドキュメント"で詳細をご覧ください。

UUIDでグループを管理する

認可サーバまたはSAML IdPがUUID値を使用してグループを表す場合、グループを使用する前に2段階の設定を行う必要があります。ONTAP 9.16.1以降では、2つのマッピング機能が利用可能になり、Entra IDでテストされています。OAuth 2.0用のEntra IDはONTAP 9.16.1以降、SAML用のEntra IDはONTAP 9.17.1以降でサポートされています。CLIコマンドを実行するには、ONTAPの*admin*権限レベルである必要があります。

これらの機能は、ONTAP REST APIを使用して設定することもできます。詳細については、"ONTAP自動化ドキュメント"をご覧ください。

グループ**UUID**をグループ名にマッピングする

UUID値を使用してグループを表す認証サーバまたはSAML IdPを使用している場合は、グループUUIDをグループ名にマッピングする必要があります。主なONTAP CLI操作については以下で説明します。

作成

`security login group create`コマンドを使用して、新しいグループマッピング設定を定義できます。グループのUUIDと名前は、認可サーバーまたはSAML IdPの設定と一致する必要があります。link:https://docs.netapp.com/us-en/ontap-cli/security-login-group-create.html["ONTAPコマンド リファレンス"^]での`security login group create`の詳細をご覧ください。

パラメータ

グループ マッピングの作成に使用するパラメータを以下に示します。

パラメータ	概要
vserver	必要に応じて、グループを関連付けるStorage Virtual Machine（SVM）の名前を指定します。省略すると、グループはONTAPクラスタに関連付けられます。
name	ONTAPが使用するグループの一意の名前。
type	この値は、グループのソースであるアイデンティティ プロバイダを示します。
uuid	認可サーバーまたは SAML IdP によって提供されるグループのユニバーサル一意識別子を指定します。

ONTAP のグループを定義する CLI コマンドの例を次に示します。サンプルアクセストークンの UUID グループを使用していることに注意してください。

例

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

グループを作成すると、グループに対して一意の読み取り専用の整数の識別子が生成されます。

その他のCLI処理

このコマンドでは、次のような追加の処理がサポートされます。

- 表示
- 変更
- 削除

`show`オプションを使用して、グループに対して生成された一意のグループIDを取得できます。link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=show["ONTAPコマンド リファレンス"^]の`show`の詳細をご覧ください。

グループ**UUID**をロールにマッピングする

UUID値を使用してグループを表す認可サーバまたはSAML IdPを使用している場合は、グループをロールにマッピングできます。ONTAPにおけるロールベースアクセス制御の詳細については、"ONTAPアクセス制御ロールの管理について学ぶ"を参照してください。主なONTAP CLI操作については以下で説明します。コマンドを実行するには、ONTAPの*admin*権限レベルである必要があります。

> まずグループUUIDをグループ名にマッピングする、グループに対して生成された一意の整数IDを取得する必要があります。このIDは、グループをロールにマッピングするために必要になります。

作成

`security login group role-mapping create`コマンドを使用して、新しいロールマッピングを定義できます。link:https://docs.netapp.com/us-en/ontap-cli/security-login-group-role-mapping-create.html["ONTAPコマンド リファレンス"^]の `security login group role-mapping create`の詳細をご覧ください。

パラメータ

グループをロールにマッピングするために使用するパラメータを以下に示します。

パラメータ	概要
group-id	コマンド `security login group create`を使用してグループに対して生成された一意の ID を指定します。
role	グループのマッピング先のONTAPロールの名前。

例

```
security login group role-mapping create -group-id 1 -role admin
```

その他の**CLI**処理

このコマンドでは、次のような追加の処理がサポートされます。

- 表示
- 変更
- 削除

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。

関連情報

- "外部ロール マッピング"

WebAuthn MFAを使用した認証と許可

ONTAP System Managerユーザー向けのWebAuthn多要素認証について学ぶ

ONTAP 9.16.1以降では、管理者は、System Managerにログインするユーザに対してWebAuthn多要素認証（MFA）を有効にすることができます。これにより、第2の認証方法としてFIDO2キー（YubiKeyなど）を使用したSystem Managerログインが有効になります。デフォルトでは、新規および既存のONTAPユーザに対してWebAuthn MFAは無効になっています。

WebAuthn MFAは、第1の認証方法に次のタイプの認証を使用するユーザおよびグループでサポートされます。

- ユーザ：password、domain、またはnsswitch
- グループ：domainまたはnsswitch

ユーザの第2の認証方法としてWebAuthn MFAを有効にすると、そのユーザはSystem Managerにログインしたときにハードウェア認証コードの登録を求められます。登録後、秘密鍵は認証コードに格納され、公開鍵はONTAPに格納されます。

ONTAPは、ユーザ1人につき1つのWebAuthnクレデンシャルをサポートします。ユーザが認証コードを紛失し、認証コードを交換する必要がある場合、ONTAP管理者はそのユーザのWebAuthnクレデンシャルを削除して、ユーザが次回のログイン時に新しい認証コードを登録できるようにする必要があります。

> WebAuthn MFAを2つ目の認証方法として有効にしているユーザーは、System Managerにアクセスする際に、IPアドレス（例："https://192.168.100.200"）ではなくFQDN（例："https://myontap.example.com"）を使用する必要があります。WebAuthn MFAが有効になっているユーザーの場合、IPアドレスを使用してSystem Managerにログインしようとすると拒否されます。

ONTAP System Managerのユーザまたはグループに対してWebAuthn MFAを有効にする

ONTAP管理者は、WebAuthn MFAオプションを有効にして新しいユーザまたはグループを追加するか、既存のユーザまたはグループに対してそのオプションを有効にすることで、System Managerのユーザまたはグループに対してWebAuthn MFAを有効にできます。

> ユーザまたはグループの第2の認証方法としてWebAuthn MFAを有効にすると、ユーザ（またはそのグループ内のすべてのユーザ）はSystem Managerに次回ログインしたときにハードウェアFIDO2デバイスの登録を求められます。この登録はユーザのローカル オペレーティング システムによって処理され、通常はセキュリティ キーの挿入、パスキーの作成、セキュリティ キーのタッチ（サポートされている場合）で構成されます。

新しいユーザまたはグループの作成時にWebAuthn MFAを有効にする

System ManagerまたはONTAP CLIを使用して、WebAuthn MFAが有効な新しいユーザまたはグループを作成できます。

System Manager

1. *Cluster > Settings*を選択します。
2. *Users and Roles*の横にある矢印アイコンを選択します。
3. *ユーザー*で*追加*を選択します。
4. ユーザー名またはグループ名を指定し、*Role*のドロップダウン メニューでロールを選択します。
5. ユーザまたはグループのログイン方法とパスワードを指定します。

   WebAuthn MFAでは、ログイン方法として、ユーザの場合は「password」、「domain」、または「nsswitch」、グループの場合は「domain」または「nsswitch」をサポートしています。

6. **HTTP** の **MFA** 列で、有効 を選択します。
7. *保存*を選択します。

CLI

1. WebAuthn MFAが有効な新しいユーザまたはグループを作成します。

   次の例では、第2の認証方法として「publickey」を選択してWebAuthn MFAを有効にしています。

```
security login create -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

`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。

既存のユーザまたはグループに対して**WebAuthn MFA**を有効にする

既存のユーザまたはグループに対してWebAuthn MFAを有効にすることができます。

System Manager

1. *Cluster > Settings*を選択します。
2. *Users and Roles*の横にある矢印アイコンを選択します。
3. ユーザとグループのリストで、編集するユーザまたはグループのオプション メニューを選択します。

   WebAuthn MFAでは、ログイン方法として、ユーザの場合は「password」、「domain」、または「nsswitch」、グループの場合は「domain」または「nsswitch」をサポートしています。
4. そのユーザーの **HTTP** の **MFA** 列で、有効 を選択します。
5. *保存*を選択します。

CLI

1. 既存のユーザまたはグループを変更して、そのユーザまたはグループに対してWebAuthn MFAを有効にします。

   次の例では、第2の認証方法として「publickey」を選択してWebAuthn MFAを有効にしています。

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

`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。

ONTAP System Managerユーザに対して**WebAuthn MFA**を無効にする

ONTAP管理者は、System ManagerまたはONTAP CLIでユーザまたはグループを編集することで、ユーザまたはグループに対してWebAuthn MFAを無効にできます。

既存のユーザまたはグループに対して**WebAuthn MFA**を無効にする

既存のユーザまたはグループに対してWebAuthn MFAをいつでも無効にできます。

登録済みクレデンシャルを無効にしても、クレデンシャルは保持されます。あとでクレデンシャルを再度有効にした場合、同じクレデンシャルが使用されるため、ユーザがログイン時に再登録する必要はありません。

System Manager

1. *Cluster > Settings*を選択します。
2. *Users and Roles*の横にある矢印アイコンを選択します。
3. ユーザとグループのリストで、編集するユーザまたはグループを選択します。
4. そのユーザーの **HTTP** の **MFA** 列で、無効 を選択します。
5. *保存*を選択します。

CLI

1. 既存のユーザまたはグループを変更して、そのユーザまたはグループに対してWebAuthn MFAを無効にします。

   次の例では、第2の認証方法として「none」を選択してWebAuthn MFAを無効にしています。

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method none \
                      -application http \
                      -role admin
```

`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。

ONTAP WebAuthn MFA設定の表示とクレデンシャルの管理

ONTAP管理者は、クラスタ全体のWebAuthn MFA設定を表示し、WebAuthn MFAのユーザおよびグループのクレデンシャルを管理できます。

WebAuthn MFAのクラスタ設定の表示

ONTAP CLIを使用して、WebAuthn MFAのクラスタ設定を表示できます。

手順

1. WebAuthn MFA のクラスター設定を表示します。オプションで、 `vserver` 引数を使用してストレージ VM を指定することもできます。

```
security webauthn show -vserver <storage_vm_name>
```

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

サポートされている**WebAuthn MFA**の公開鍵アルゴリズムの表示

Storage VMまたはクラスタでサポートされているWebAuthn MFAの公開鍵アルゴリズムを表示できます。

手順

1. サポートされている公開鍵WebAuthn MFAアルゴリズムを一覧表示します。オプションで、 `vserver`引数を使用してストレージVMを指定することもできます：

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

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

登録済み**WebAuthn MFA**クレデンシャルの表示

ONTAP管理者は、すべてのユーザの登録済みWebAuthnクレデンシャルを表示できます。管理者以外のユーザは、この手順を使用して、自分の登録済みWebAuthnクレデンシャルのみを表示できます。

手順

1. 登録済みWebAuthn MFAクレデンシャルを表示します。

```
security webauthn credentials show
```

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

登録済み**WebAuthn MFA**クレデンシャルの削除

登録済みWebAuthn MFAクレデンシャルを削除できます。これは、ユーザのハードウェア キーが紛失したり、盗まれたり、使用されなくなったりした場合に便利です。また、ユーザが元のハードウェア認証コードを持っているものの、新しいものに交換したい場合にも、登録済みクレデンシャルを削除することができます。クレデンシャルを削除すると、ユーザは交換用認証コードの登録を求められます。

ユーザーの登録済みの認証情報を削除しても、そのユーザーのWebAuthn MFAは無効になりません。ユーザーがハードウェア認証デバイスを紛失し、交換前にログインする必要がある場合は、以下の手順に従って認証情報を削除し、"WebAuthn MFAの無効化"ユーザーに対しても実行する必要があります。

System Manager

1. *Cluster > Settings*を選択します。
2. *Users and Roles*の横にある矢印アイコンを選択します。
3. ユーザとグループのリストで、クレデンシャルを削除するユーザまたはグループのオプション メニューを選択します。
4. **HTTP** 資格情報の **MFA** を削除 を選択します。
5. *削除*を選択します。

CLI

1. 登録済みクレデンシャルを削除します。次の点に注意してください。
   - 必要に応じて、ユーザのStorage VMを指定できます。省略すると、クラスタ レベルでクレデンシャルが削除されます。
   - 必要に応じて、クレデンシャルを削除するユーザのユーザ名を指定できます。省略すると、現在のユーザのクレデンシャルが削除されます。

```
security webauthn credentials delete -vserver <storage_vm_name>
-username <username>
```

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

Webサービスの管理

Webサービスの管理 - 概要

クラスタまたはStorage Virtual Machine（SVM）のWebサービスを有効化または無効化したり、Webサービスの設定を表示したり、ロールのユーザーがWebサービスにアクセスできるかどうかを制御したりできます。

クラスタまたはSVMのWebサービスは次の方法で管理できます。

- 特定のWebサービスを有効化または無効化する
- Webサービスへのアクセスを暗号化されたHTTP（SSL）のみに限定するかどうかを指定する

- Webサービスの可用性を表示する
- あるロールのユーザのWebサービスへのアクセスを許可する、または禁止する
- Webサービスへのアクセスが許可されているロールを表示する

ユーザがあるWebサービスへアクセスするには、次の条件をすべて満たしている必要があります。

- 認証されたユーザであること。

  たとえば、Webサービスからユーザ名およびパスワードの入力を求められた場合、ユーザは有効なアカウントの情報を入力する必要があります。

- ユーザに正しいアクセス方法が設定されていること。

  認証は、指定されたWebサービスに対する正しいアクセス方法を持つユーザに対してのみ成功します。ONTAP API Webサービス `ontapi`の場合、ユーザは `ontapi`アクセス方法を持っている必要があります。その他のすべてのWebサービスの場合、ユーザは `http`アクセス方法を持っている必要があります。

> `security login`コマンドを使用して、ユーザーのアクセス方法と認証方法を管理します。

- Webサービスがユーザのアクセス制御ロールを許可するように設定されていること。

> `vserver services web access`コマンドを使用して、ロールのWebサービスへのアクセスを制御します。

ファイアウォールが有効になっている場合は、Webサービスに使用するLIFのファイアウォール ポリシーを設定して、HTTPまたはHTTPSを許可する必要があります。

Webサービスアクセスに HTTPS を使用する場合は、Webサービスを提供するクラスタまたは SVM の SSL も有効にする必要があり、クラスタまたは SVM のデジタル証明書を提供する必要があります。

ONTAP Webサービスへのアクセスを管理する

Webサービスは、HTTPまたはHTTPSを使用してユーザがアクセスできるアプリケーションです。クラスタ管理者はWebプロトコル エンジンをセットアップし、SSLを設定し、Webサービスを有効にし、ロールのユーザがWebサービスにアクセスできるようにします。

ONTAP 9.6以降では、次のWebサービスがサポートされます。

- サービスプロセッサインフラストラクチャ (`spi`)

  このサービスは、クラスタ管理LIFまたはノード管理LIFを介して、ノードのログ、コアダンプ、およびMIBファイルをHTTPまたはHTTPSでアクセスできるようにします。デフォルト設定は `enabled`です。

ノードのログファイルまたはコアダンプファイルへのアクセス要求があると、 `spi`Webサービスは、あるノードから、ファイルが存在する別のノードのルートボリュームへのマウントポイントを自動的に作成します。マウントポイントを手動で作成する必要はありません。

- ONTAP API (`ontapi`)

  このサービスを使用すると、ONTAP APIを実行してリモートプログラムから管理機能を実行できます。デフォルト設定は `enabled`です。

  一部の外部管理ツールにはこのサービスが必要です。たとえば、System Managerを使用する場合は、このサービスを有効にしておく必要があります。

- Data ONTAP検出(`disco`)

  このサービスにより、オフボックス管理アプリケーションがネットワーク内のクラスタを検出できるようになります。デフォルト設定は `enabled`です。

- サポート診断(`supdiag`)

  このサービスは、問題の分析と解決を支援するために、システム上の特権環境へのアクセスを制御します。デフォルト設定は `disabled`です。このサービスは、テクニカルサポートから指示された場合にのみ有効にしてください。

- System Manager(`sysmgr`)

  このサービスは、ONTAPに含まれるSystem Managerの可用性を制御します。デフォルト設定は `enabled`です。このサービスはクラスタでのみサポートされます。

- ファームウェア ベースボード管理コントローラ（BMC）アップデート(`FW_BMC`

  このサービスを使用すると、BMCファームウェアファイルをダウンロードできます。デフォルト設定は `enabled`です。

- ONTAP ドキュメント(`docs`)

  このサービスはONTAPドキュメントへのアクセスを提供します。デフォルト設定は `enabled`です。

- ONTAP RESTful API (`docs_api`)

  このサービスは、ONTAP RESTful APIドキュメントへのアクセスを提供します。デフォルト設定は `enabled`です。

- ファイルのアップロードとダウンロード(`fud`)

  このサービスでは、ファイルのアップロードとダウンロードが可能です。デフォルト設定は `enabled`です。

- ONTAPメッセージング(`ontapmsg`)

  このサービスは、イベントをサブスクライブするためのパブリッシュ/サブスクライブインターフェースをサポートしています。デフォルト設定は `enabled`です。

- ONTAPポータル(`portal`)

このサービスは、ゲートウェイを仮想サーバーに実装します。デフォルト設定は `enabled`です。

- ONTAP Restful Interface(`rest`)

  このサービスは、クラスタインフラストラクチャのすべての要素をリモートで管理するためのRESTfulインターフェースをサポートしています。デフォルト設定は `enabled`です。

- Security Assertion Markup Language（SAML）サービスプロバイダーサポート(`saml`)

  このサービスは、SAMLサービスプロバイダーをサポートするためのリソースを提供します。デフォルト設定は `enabled`です。

- SAML サービスプロバイダー(`saml-sp`)

  このサービスは、SPメタデータやアサーションコンシューマサービスなどのサービスをサービスプロバイダに提供します。デフォルト設定は `enabled`です。

ONTAP 9.7以降では、さらに次のサービスがサポートされます。

- 構成バックアップファイル(`backups`)

  このサービスを使用すると、設定のバックアップファイルをダウンロードできます。デフォルト設定は `enabled`です。

- ONTAP セキュリティ(`security`)

  このサービスは、認証を強化するためにCSRFトークン管理をサポートしています。デフォルト設定は `enabled`です。

ONTAPでWebプロトコルエンジンを管理する

クラスタ上でWebプロトコル エンジンを設定し、Webアクセスを許可するかどうか、およびどのSSLのバージョンが使用可能かを制御できます。また、Webプロトコル エンジンの構成設定を表示することもできます。

Webプロトコル エンジンは、次の方法でクラスタ レベルで管理できます。

- `system services web modify`コマンドに `-external`パラメータを指定することで、リモートクライアントがWebサービスコンテンツにアクセスする際にHTTPまたはHTTPSのどちらを使用できるかを指定できます。
- `security config modify`コマンドを `-supported-protocol`パラメータとともに使用することで、安全なWebアクセスにSSLv3を使用するかどうかを指定できます。デフォルトでは、SSLv3は無効になっています。トランスポート層セキュリティ1.0（TLSv1.0）は有効になっており、必要に応じて無効にすることができます。

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

- クラスタ全体のコントロール プレーンWebサービス インターフェイス用に、Federal Information Processing Standard（FIPS）140-2準拠モードを有効にすることができます。

  FIPS 140-2準拠モードは、デフォルトでは無効になっています。

  - **FIPS 140-2** 準拠モードが無効の場合 `security config modify`コマンドの `is-fips-enabled`パラメータを `true`に設定し、 `security config show`コマンドを使用してオンライン状態を確認することで、FIPS 140-2 準拠モードを有効にできます。
  - **FIPS 140-2**準拠モードが有効になっている場合
    - ONTAP 9.11.1以降、TLSv1、TLSv1.1、SSLv3は無効になり、TSLv1.2とTSLv1.3のみが有効のままになります。これはONTAP 9の内部および外部の他のシステムと通信に影響します。FIPS 140-2準拠モードを有効にしてから無効にした場合、TLSv1、TLSv1.1、SSLv3は無効のままになります。以前の設定に応じて、TLSv1.2またはTLSv1.3のいずれかが有効のままになります。
    - ONTAP 9.11.1より前のバージョンでは、TLSv1とSSLv3の両方が無効になっており、TLSv1.1とTLSv1.2のみが有効のままです。ONTAPでは、FIPS 140-2準拠モードが有効になっている場合、TLSv1とSSLv3の両方を有効にすることはできません。FIPS 140-2準拠モードを有効にしてから無効にした場合、TLSv1とSSLv3は無効のままですが、以前の設定に応じて、TLSv1.2またはTLSv1.1とTLSv1.2の両方が有効になります。
- `system security config show`コマンドを使用して、クラスタ全体のセキュリティの設定を表示できます。

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

ファイアウォールが有効になっている場合は、Webサービスに使用する論理インターフェイス（LIF）のファイアウォール ポリシーを設定して、HTTPまたはHTTPSアクセスを許可する必要があります。

WebサービスアクセスにHTTPSを使用する場合は、Webサービスを提供するクラスタまたはStorage Virtual Machine（SVM）のSSLを有効にし、そのクラスタまたはSVMのデジタル証明書を提供する必要もあります。

MetroCluster構成では、クラスタ上のWebプロトコル エンジンの設定に対する変更内容は、パートナー クラスタにはレプリケートされません。

Webプロトコル エンジンを管理するためのONTAPコマンド

`system services web`コマンドを使用してWebプロトコルエンジンを管理します。 `system services firewall policy create`コマンドと `network interface modify`コマンドを使用して、Webアクセス要求がファイアウォールを通過できるようにします。

状況	使用するコマンド
クラスター レベルでWebプロトコル エンジンを構成します： • クラスターのWebプロトコル エンジンを有効または無効にする • クラスターの SSLv3 を有効または無効にする • セキュア Web サービス（HTTPS）の FIPS 140-2 準拠を有効または無効にする	`system services web modify`
クラスタ レベルでの Web プロトコル エンジンの構成を表示し、クラスタ全体で Web プロトコルが機能しているかどうかを確認し、FIPS 140-2 準拠が有効になっていてオンラインかどうかを表示します	`system services web show`
ノードレベルでのwebプロトコルエンジンの構成と、クラスター内のノードのwebサービス処理のアクティビティを表示します。	`system services web node show`
ファイアウォール ポリシーを作成するか、既存のファイアウォール ポリシーに HTTP または HTTPS プロトコル サービスを追加して、Webアクセス要求がファイアウォールを通過できるようにします。	`system services firewall policy create` `-service`パラメータを `http`または`https`に設定すると、Webアクセス要求がファイアウォールを通過できるようになります。
ファイアウォールポリシーをLIFに関連付ける	`network interface modify` `-firewall-policy`パラメータを使用して、LIFのファイアウォール ポリシーを変更できます。

関連情報

- "network interface modify"

ONTAP Webサービスへのアクセスを設定する

Webサービスへのアクセスを設定すると、許可されたユーザがHTTPまたはHTTPSを使用して、クラスタまたはStorage Virtual Machine（SVM）上のサービスコンテンツにアクセスできるようになります。

手順

1. ファイアウォールが有効になっている場合は、Webサービスに使用されるLIFのファイアウォールポリシ

ーでHTTPまたはHTTPSアクセスが設定されていることを確認します：

> `system services firewall show`コマンドを使用してファイアウォールが有効になっているかどうかを確認できます。

a. ファイアウォール ポリシーで HTTP または HTTPS が設定されていることを確認するには、 `system services firewall policy show` コマンドを使用します。

> `system services firewall policy create`コマンドの `-service`パラメータを `http`または `https`に設定して、ポリシーがWebアクセスをサポートできるようにします。

b. HTTP または HTTPS をサポートするファイアウォール ポリシーが、Web サービスを提供する LIF に関連付けられていることを確認するには、 `-firewall-policy`パラメータを指定した `network interface show`コマンドを使用します。

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

> `network interface modify`コマンドに `-firewall-policy`パラメータを指定して、LIFに対してファイアウォールポリシーを有効にします。

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

2. クラスターレベルのWebプロトコルエンジンを構成し、Webサービスコンテンツにアクセスできるようにするには、 `system services web modify`コマンドを使用します。
3. セキュア Web サービス（HTTPS）を使用する予定の場合は、SSL を有効にし、 `security ssl modify`コマンドを使用してクラスタまたは SVM のデジタル証明書情報を提供します。

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

4. クラスタまたは SVM の Web サービスを有効にするには、 `vserver services web modify`コマンドを使用します。

クラスタまたは SVM に対して有効にするサービスごとに、この手順を繰り返す必要があります。

5. クラスタまたは SVM 上の Web サービスにアクセスするロールを承認するには、 `vserver services web access create` コマンドを使用します。

   アクセスを許可するロールは既に存在している必要があります。 `security login role show`コマンドを使用して既存のロールを表示するか、 `security login role create`コマンドを使用して新しいロールを作成できます。

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

6. Webサービスへのアクセスが許可されているロールの場合は、 `security login show`コマンドの出力をチェックして、そのユーザも正しいアクセス方法で設定されていることを確認します。

   ONTAP API Webサービス `ontapi`にアクセスするには、ユーザに `ontapi`アクセス方法を設定する必要があります。その他のすべてのWebサービスにアクセスするには、ユーザに `http`アクセス方法を設定する必要があります。

   `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。

   `security login create`コマンドを使用して、ユーザのアクセス方法を追加します。link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html["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。

Webサービスを管理するためのONTAPコマンド

`vserver services web`コマンドを使用して、クラスタまたはStorage Virtual Machine（SVM）のWebサービスの可用性を管理します。 `vserver services web access`コマンドを使用して、ロールのWebサービスへのアクセスを制御します。

状況	使用するコマンド
クラスタまたはSVMのWebサービスを次のように設定する • Webサービスを有効または無効にする • WebサービスへのアクセスにHTTPSだけを許可するかどうかを指定する	`vserver services web modify`
クラスタまたはSVMのWebサービスの設定と可用性を表示する	`vserver services web show`
特定のロールに対して、クラスタまたはSVMのWebサービスへのアクセスを許可する	`vserver services web access create`
クラスタまたはSVMのWebサービスへのアクセスが許可されているロールを表示する	`vserver services web access show`
特定のロールに対して、クラスタまたはSVMのWebサービスへのアクセスを禁止する	`vserver services web access delete`

関連情報

"ONTAPコマンド リファレンス"

ONTAPノード上のマウントポイントを管理するためのコマンド

`spi`ウェブサービスは、ノードのログファイルまたはコアファイルへのアクセス要求に応じて、あるノードから別のノードのルートボリュームへのマウントポイントを自動的に作成します。マウントポイントを手動で管理する必要はありませんが、 `system node root-mount`コマンドを使用して管理できます。

状況	使用するコマンド
1つのノードから別のノードのルート ボリュームへのマウント ポイントを手動で作成する	`system node root-mount create`あるノードから別のノードへ存在できるマウント ポイントは 1 つだけです。
クラスタ内のノードにある既存のマウント ポイントとその作成時刻、現在の状態を表示する	`system node root-mount show`
1つのノードから別のノードのルート ボリュームへのマウント ポイントを削除し、そのマウント ポイントへの接続を強制的に切断する	`system node root-mount delete`

関連情報

"ONTAPコマンド リファレンス"

ONTAPでのSSLの管理

`security ssl`コマンドを使用して、クラスタまたはストレージ仮想マシン（SVM）のSSLプロトコルを管理します。SSLプロトコルは、デジタル証明書を使用してWebサーバーとブラウザ間の暗号化された接続を確立することで、Webアクセスのセキュリティを強化します。

クラスタまたはStorage Virtual Machine（SVM）のSSLは次の方法で管理できます。

- SSLを有効にする
- デジタル証明書を生成してインストールし、クラスタまたはSVMと関連付ける
- SSL設定を表示してSSLが有効かどうかを確認し、可能な場合はSSL証明書名を確認する
- クラスタまたはSVMのファイアウォール ポリシーを設定して、Webアクセス要求が通過できるようにする
- 使用できるSSLのバージョンを定義する
- WebサービスのHTTPS要求のみにアクセスを制限する

SSLの管理用コマンド

`security ssl`コマンドを使用して、クラスタまたはStorage Virtual Machine（SVM）のSSLプロトコルを管理します。

状況	使用するコマンド
クラスタまたはSVMのSSLを有効にし、デジタル証明書と関連付ける	`security ssl modify`
クラスタまたはSVMのSSL設定と証明書名を表示する	`security ssl show`

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

ONTAP WebサービスにHSTSを使用する

HTTP Strict Transport Security（HSTS）は、プロトコルダウングレード攻撃やCookieハイジャックといった中間者攻撃からWebサイトを保護するためのWebセキュリティポリシーメカニズムです。HTTPSの使用を強制することで、HSTSはユーザーのブラウザとサーバ間のすべての通信が暗号化されることを保証します。ONTAP 9.17.1以

降、ONTAPはONTAP WebサービスにHTTPS接続を強制できるようになりました。

> HSTSは、ONTAPとの最初のセキュアなHTTPS接続が確立された後にのみ、Webブラウザによって適用されます。ブラウザが最初のセキュアな接続を確立しない場合、HSTSは適用されません。HSTSの管理については、ブラウザのドキュメントを参照してください。

タスク概要

- 9.17.1以降では、新規にインストールされたONTAPクラスタではHSTSがデフォルトで有効になっています。9.17.1にアップグレードすると、HSTSはデフォルトで有効になりません。アップグレード後にHSTSを有効にする必要があります。
- HSTS はすべての"ONTAP Webサービス"でサポートされています。

開始する前に

- 次のタスクには高度な権限が必要です。

HSTS設定を表示

現在の HSTS 構成を表示して、有効になっているかどうかを確認し、最大経過時間の設定を表示できます。

手順

1. `system services web show`コマンドを使用して、HSTS設定を含む現在のWebサービス構成を表示します：

```
cluster-1::system services web*> show

                    External Web Services: true
                                HTTP Port: 80
                               HTTPS Port: 443
                          Protocol Status: online
                       Per Address Limit: 80
                     Wait Queue Capacity: 192
                            HTTP Enabled: true
                  CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                            HSTS Enabled: true
                  HSTS max age (Seconds): 63072000
```

HSTSを有効にして最大期間を設定する

ONTAP 9.17.1以降、新しいONTAPクラスタではHSTSがデフォルトで有効になっています。既存のクラスタを9.17.1以降にアップグレードする場合は、クラスタでHSTSを手動で有効にして、HTTPSの使用を強制する必要があります。HSTSを有効にして最大有効期間を設定できます。HSTSが有効になっている場合は、いつ

でも最大有効期間を変更できます。HSTSを有効にすると、ブラウザは最初のセキュア接続が確立された後にのみ、セキュア接続の強制を開始します。

手順

1. `system services web modify`コマンドを使用して、HSTS を有効にするか、最大経過時間を変更します：

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age`ブラウザがHTTPSの適用を記憶する期間（秒数）を指定します。デフォルト値は63072000秒（2年）です。

HSTSを無効にする

ブラウザは接続ごとにHSTSの最大有効期間設定を保存し、ONTAPでHSTSが無効になっている場合でも、全期間にわたってHSTSを強制適用し続けます。HSTSが無効になった後、ブラウザがHSTSの強制適用を停止するまでには、設定された最大有効期間までかかります。この期間中に安全な接続が不可能になった場合、HSTSを強制適用しているブラウザは、問題が解決されるかブラウザの最大有効期間が切れるまで、ONTAP Webサービスへのアクセスを許可しません。

手順

1. `system services web modify`コマンドを使用して HSTS を無効にします：

```
system services web modify -hsts-enabled false
```

関連情報

"RFC 6797 - HTTP Strict Transport Security（HSTS）"

ONTAP Webサービスアクセスの問題のトラブルシューティング

設定エラーによって、Webサービスへのアクセスに関する問題が発生します。LIF、ファイアウォール ポリシー、Webプロトコル エンジン、Webサービス、デジタル証明書、およびユーザ アクセス認証がすべて正しく設定されていることを確認することで、エラーに対処できます。

次の表は、Webサービスの構成エラーを識別して対処するのに役立ちます：

このアクセスの問題...	この設定エラーが原因で発生します...	エラーを解決するには...
Webサービスにアクセスしようとすると、Webブラウザから `unable to connect`または `failure to establish a connection`エラーが返されます。	LIF が正しく設定されていない可能性があります。	Webサービスを提供するLIFにpingできることを確認します。 LIF を ping するには、 `network ping` コマンドを使用します。
ファイアウォールが正しく構成されていない可能性があります。	HTTP または HTTPS をサポートするようにファイアウォール ポリシーが設定されており、そのポリシーが Web サービスを提供する LIF に割り当てられていることを確認します。 `system services firewall policy`コマンドを使用してファイアウォール ポリシーを管理します。 `network interface modify`コマンドを `-firewall-policy`パラメータとともに使用して、ポリシーをLIFに関連付けます。	Webプロトコル エンジンが無効になっている可能性があります。

このアクセスの問題...	この設定エラーが原因で発生します...	エラーを解決するには...
Webサービスにアクセスできるように、Webプロトコル エンジンが有効になっていることを確認します。  `system services web`コマンドを使用して、クラスタのWebプロトコル エンジンを管理します。	Web サービスにアクセスしようとすると、Web ブラウザから `not found`エラーが返されます。	Webサービスが無効になっている可能性があります。
アクセスを許可する各 Web サービスが個別に有効になっていることを確認します。  `vserver services web modify`コマンドを使用して、Webサービスへのアクセスを有効にします。	Webブラウザは、ユーザーのアカウント名とパスワードを使用してWebサービスにログインできません。	ユーザーを認証できないか、アクセス方法が正しくないか、またはユーザーにWebサービスへのアクセス権限がありません。

このアクセスの問題...	この設定エラーが原因で発生します...	エラーを解決するには...
ユーザ アカウントが存在し、正しいアクセス方法と認証方法で設定されていることを確認してください。また、ユーザのロールにWebサービスへのアクセスが許可されていることを確認してください。 `security login`コマンドを使用して、ユーザアカウントとそのアクセス方法および認証方法を管理します。`ONTAP API Web`サービスにアクセスするには、`ontapi`アクセス方法が必要です。その他のすべての`Web`サービスにアクセスするには、`http`アクセス方法が必要です。`vserver services web access`コマンドを使用して、ロールの`Web`サービスへのアクセスを管理します。	HTTPS を使用して Web サービスに接続すると、Web ブラウザに接続が中断されたことが示されます。	Web サービスを提供するクラスタまたはStorage Virtual Machine（SVM）でSSLが有効になっていない可能性があります。

このアクセスの問題...	この設定エラーが原因で発生します...	エラーを解決するには...
クラスタまたは SVM で SSL が有効になっており、デジタル証明書が有効であることを確認します。 `security ssl`コマンドを使用してHTTPサーバのSSL設定を管理し、`security certificate show`コマンドを使用してデジタル証明書情報を表示します。	HTTPS を使用して Web サービスに接続すると、Web ブラウザには接続が信頼できないと表示されます。	自己署名デジタル証明書を使用している可能性があります。

関連情報

- "ONTAPのネットワーク設定のベストプラクティスとは？"
- "network ping"
- "network interface modify"
- "セキュリティ証明書 generate-csr"
- "security certificate install"
- "セキュリティ証明書の表示"
- "セキュリティ SSL"

証明書を使用したリモート サーバのIDの確認

ONTAPで証明書を使用してリモートサーバーのIDを検証する方法について説明します

ONTAPは、リモート サーバーの ID を確認するためのセキュリティ証明書機能をサポートしています。

ONTAPソフトウェアは、次のデジタル証明書機能とプロトコルを使用して安全な接続を実現します：

- Online Certificate Status Protocol（OCSP）は、SSLおよびTransport Layer Security（TLS）接続を使用して、ONTAPサービスからのデジタル証明書要求のステータスを検証します。この機能はデフォルトで無効になっています。
- ONTAPソフトウェアには、信頼できるルート証明書のデフォルト セットが含まれています。

- Key Management Interoperability Protocol（KMIP）証明書により、クラスターと KMIP サーバーの相互認証が可能になります。

ONTAPでOCSPを使用してデジタル証明書が有効であることを確認する

Online Certificate Status Protocol（OCSP）により、Transport Layer Security（TLS）通信を使用するONTAPアプリケーションは、OCSPが有効になっている場合にデジタル証明書ステータスを受信できます。特定のアプリケーションに対するOCSP証明書ステータスチェックは、いつでも有効または無効にできます。デフォルトでは、OCSP証明書ステータスチェックは無効になっています。

開始する前に

このタスクを実行するには、advanced権限レベルのアクセス権が必要です。

タスク概要

OCSPは、次のアプリケーションでサポートされています。

- AutoSupport
- イベント管理システム（Event Management System（EMS））
- LDAP over TLS
- Key Management Interoperability Protocol（KMIP）
- 監査ログ
- FabricPool
- SSH（ONTAP 9.13.1以降）

手順

1. 権限レベルを詳細に設定します： `set -privilege advanced`
2. 特定のアプリケーションでOCSPによる証明書のステータス チェックを有効または無効にするには、次の該当するコマンドを使用します。

一部のアプリケーションに対して **OCSP** 証明書ステータス チェックを実行する場合は...	使用するコマンド
有効	`security config ocsp enable -app app name`
無効	`security config ocsp disable -app app name`

次のコマンドは、AutoSupportおよびEMSのOCSPサポートを有効にします。

```
cluster::*> security config ocsp enable -app asup,ems
```

OCSPを有効にすると、アプリケーションは次のいずれかの応答を受信します。

- Good - 証明書は有効で、通信可能な状態です。
- Revoked - 証明書は発行元の認証局によって永続的に信頼できないと判断されており、通信不可能な状態です。
- Unknown - サーバが証明書に関するステータス情報を持っていないため、通信不可能な状態です。
- OCSP server information is missing in the certificate - TLS通信は続行していますが、サーバでOCSPが無効であると判断されているため、ステータス チェックは実行されません。
- No response from OCSP server - アプリケーションを実行できない状態です。

3. TLSを使用するすべてのアプリケーションでOCSPによる証明書のステータス チェックを有効または無効にするには、次の該当するコマンドを使用します。

すべてのアプリケーションに対して **OCSP** 証明書ステータス チェックを実行する場合は...	使用するコマンド
有効	`security config ocsp enable -app all`
無効	`security config ocsp disable -app all`

この機能を有効にした場合は、すべてのアプリケーションで証明書のステータス（good、revoked、またはunknown）が署名された応答を受信します。証明書のステータスがrevokedの場合は、アプリケーションは実行できません。アプリケーションがOCSPサーバから応答を受信できない、またはOCSPサーバにアクセスできない場合も、アプリケーションは実行できません。

4. `security config ocsp show`コマンドを使用して、OCSPをサポートするすべてのアプリケーションとそのサポート ステータスを表示します。

```
cluster::*> security config ocsp show
         Application                        OCSP Enabled?
         --------------------               ---------------------
         autosupport                        false
         audit_log                          false
         fabricpool                         false
         ems                                false
         kmip                               false
         ldap_ad                            true
         ldap_nis_namemap                   true
         ssh                                true

         8 entries were displayed.
```

関連情報

- "security config ocsp enable"
- "security config ocsp 無効化"
- "security config ocsp show"

ONTAPのTLSベースアプリケーションのデフォルト証明書を表示する

ONTAPは、トランスポート層セキュリティ（TLS）を使用するONTAPアプリケーションに、信頼できるルート証明書のデフォルト セットを提供します。

開始する前に

デフォルトの証明書は、管理SVMの作成時またはアップグレード時にのみ管理SVMにインストールされます。

タスク概要

現在、クライアントとして機能し、証明書の検証を必要とするアプリケーションはAutoSupport、EMS、LDAP、監査ログ、FabricPool、および KMIP です。

証明書の有効期限が切れると、ユーザーに証明書の削除を要求するEMSメッセージが呼び出されます。デフォルトの証明書は、上級権限レベルでのみ削除できます。

デフォルトの証明書を削除すると、一部のONTAPアプリケーション（AutoSupportや監査ログなど）が期待どおりに機能しなくなる可能性があります。

手順

1. 管理SVMにインストールされているデフォルトの証明書を表示するには、security certificate showコマンドを使用します。

   security certificate show -vserver -type server-ca

```
cluster1::> security certificate show

Vserver    Serial Number   Certificate Name
Type
---------- --------------- ----------------------------------------
---------
vs0        4F4E4D7B         www.example.com
server
    Certificate Authority:  www.example.com
          Expiration Date: Thu Feb 28 16:08:28 2013
```

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

クラスタとKMIPサーバの相互認証

ONTAPクラスタとKMIPサーバの相互認証の概要

クラスタと外部キーマネージャ（Key Management Interoperability Protocol（KMIP）サーバなど）を相互認証することで、キーマネージャはSSL経由のKMIPを使用してクラスタと通信できるようになります。これは、アプリケーションまたは特定の機能（ストレージ暗号化機能など）が、安全なデータアクセスを提供するために安全なキーを必要とする場合に行います。

ONTAP でクラスタの証明書署名要求を生成する

セキュリティ証明書 `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、証明機関（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
```

```
`security certificate generate-csr`
の詳細については、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"^]をご覧ください。
```

次のコマンドは、SHA256ハッシュ関数で生成される2,048ビット秘密鍵を使用して、CSRを作成します。この証明書は、米国カリフォルニア州のサニーベールにある企業（カスタム共通名server1.companyname.com）のIT部門のソフトウェア グループが使用します。SVM担当管理者のEメール アドレスは\web@example.comです。出力にはCSRと秘密鍵が表示されます。

```
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 :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

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

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

ONTAPクラスタ用のCA署名サーバ証明書をインストールする

SSLサーバがクラスタまたはStorage Virtual Machine（SVM）をSSLクライアントとして認証できるようにするには、クラスタまたはSVMにクライアント タイプのデジタル証明書をインストールします。次に、SSLサーバ管理者にclient-ca証明書を提供し、サーバにインストールしてもらいます。

開始する前に

`server-ca`証明書タイプを使用して、クラスタまたはSVMに
SSLサーバのルート証明書がすでにインストールされている必要があります。

手順

1. クライアント認証に自己署名デジタル証明書を使用するには、 `type client`パラメータを指定して `security certificate create`コマンドを使用します。

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

2. クライアント認証にCA署名デジタル証明書を使用するには、次の手順を実行します：

a. security certificate `generate-csr`コマンドを使用して、デジタル証明書署名要求（CSR）を生成します。

   ONTAP は、証明書要求と秘密キーを含む CSR 出力を表示し、将来の参照用に出力をファイルにコピーするように通知します。

b. CSR 出力からの証明書要求を電子形式（電子メールなど）で信頼できる CA に送信し、署名を依頼します。

   将来の参照用に、秘密キーと CA 署名証明書のコピーを保管しておく必要があります。

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。

a. `-type client`パラメータを指定した `security certificate install`コマンドを使用して、CA署名証明書をインストールします。
b. プロンプトが表示されたら証明書と秘密キーを入力し、*Enter*キーを押します。
c. プロンプトが表示されたら追加のルート証明書または中間証明書を入力し、*Enter*キーを押します。

   信頼されたルートCAから始まり、お客様に発行されたSSL証明書で終わる証明書チェーンに中間証明書がない場合は、クラスタまたはSVMに中間証明書をインストールします。中間証明書は、エンドエンティティサーバ証明書を発行するために信頼されたルートCAによって発行される従属証明書です。その結果、信頼されたルートCAから始まり、中間証明書を経由して、お客様に発行されたSSL証明書で終わる証明書チェーンが作成されます。

3. クラスタまたは SVM の `client-ca`証明書を SSL サーバーの管理者に提供し、サーバーにインストールしてもらいます。

   `-instance`および `-type client-ca`パラメータを指定した `security certificate show` コマンドは、 `client-ca`証明書情報を表示します。

関連情報

- "security certificate install"
- "セキュリティ証明書の表示"

ONTAPにKMIPサーバー用のCA署名付きクライアント証明書をインストールする

Key Management Interoperability Protocol（KMIP）の証明書サブタイプ（-subtype kmip-certパラメータ）は、clientおよびserver-caタイプとともに、証明書がクラスタとKMIPサーバなどの外部キー マネージャとの相互認証に使用されることを指定します。

タスク概要

KMIP 証明書をインストールして、KMIP サーバーをクラスタの SSL サーバーとして認証します。

手順

1. `-type server-ca`および `-subtype kmip-cert`パラメータを指定した `security certificate install`コマンドを使用して、KMIPサーバーのKMIP証明書をインストールします。
2. プロンプトが表示されたら、証明書を入力し、Enterキーを押します。

ONTAP は、将来の参照用に証明書のコピーを保管しておくように通知します。

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


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

cluster1::>
```

関連情報

- "security certificate install"