認証とアクセス制御
ONTAP 9

NetApp
April 24, 2024

目次

認証とアクセス制御

ニンシヨウトアクセスセイキヨノカイヨウ

ONTAPクラスタの認証とONTAP Webサービスへの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やストレージへのアクセスを制御し、保護することができます。

従来の System Manager （ ONTAP 9.7 以前でのみ使用可能）を使用している場合は、を参照してください "System Manager Classic （ ONTAP 9.0 から 9.7 ）"

クライアントの認証と許可

ONTAP では、信頼できるソースで ID を検証してクライアントマシンおよびユーザを認証します。ONTAP は、ユーザのクレデンシャルとファイルまたはディレクトリに対して設定されている権限を比較して、ユーザ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 に対して自身を認証します。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

管理者認証と **RBAC** の概要については、 **CLI** を使用してください

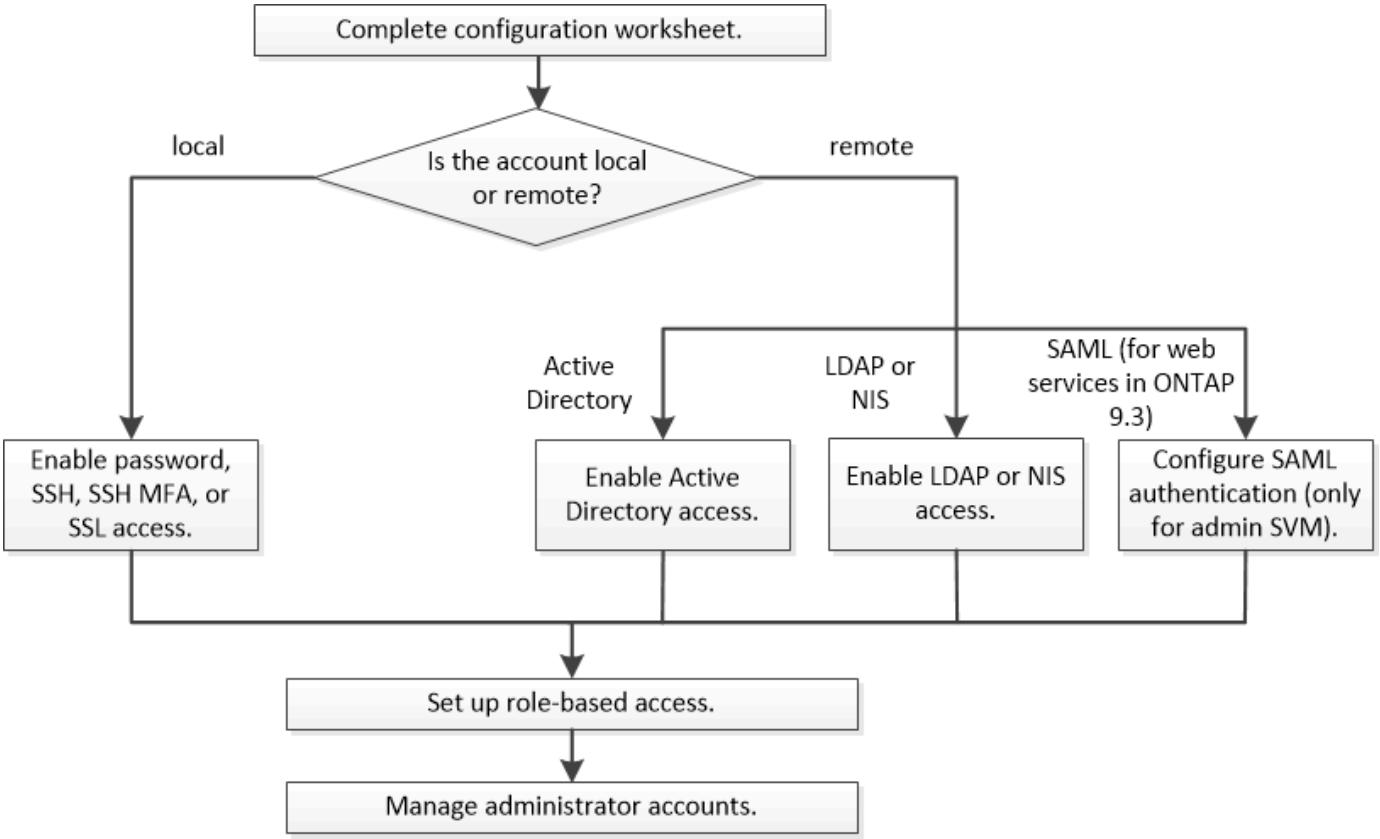
ONTAP クラスタ管理者および Storage Virtual Machine （ SVM ）管理者のログインアカウントを有効にすることができます。管理者が実行できる機能は、ロールベースアクセス制御（ RBAC ）を使用して定義することもできます。

ログインアカウントと RBAC は次の方法で有効にします。

- System Manager や自動スクリプトツールではなく、 ONTAP コマンドラインインターフェイス（ CLI ）を使用する必要がある。
- すべての選択肢について検討するのではなく、ベストプラクティスに従う。
- クラスタに関する情報の収集に SNMP を使用しない。

管理者認証と **RBAC** のワークフロー

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。各アカウントには、事前定義された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。



ローカル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
- 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 サービスを使用することで、管理 SVM へのアクセスに Security Assertion Markup Language （ SAML ）認証を使用できます。

- 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。

管理者認証と **RBAC** 設定用のワークシートです

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。

ログインアカウントを作成または変更します

次の値はで指定します `security login create` コマンドは、ログインアカウントによるStorage VMへのアクセスを有効にする場合に使用します。にも同じ値を指定します `security login modify` コマンドは、アカウントによるStorage VMへのアクセス方法を変更するときに使用します。

フィールド	説明	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。グループ名を指定すると、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。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され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方法。 • cert SSL証明書認証用 • domain Active Directory認証用 • nsswitch LDAPまたはNIS認証に使用します • password ユーザパスワード認証用 • publickey 公開鍵認証用 • community （SNMPコミュニティストリング） • usm SNMPユーザセキュリティモデルの場合 • saml Security Assertion Markup Language（SAML）認証に使用します	
-remote-switch-ipaddress	リモートスイッチの IP アドレスです。リモートスイッチは、クラスタスイッチヘルスモニタ（ CSHM ）で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 ）で監視される Fibre Channel （ FC ）スイッチです。このオプションは、アプリケーションがの場合にのみ適用されます snmp 認証方法はです usm。	
-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（管理Storage VM）のデフォルト値はです。 admin。 • データStorage VMの場合、デフォルト値はです。 vsadmin。	
-comment	（オプション）アカウントの説明。テキストは二重引用符（ " ）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かNISグループアカウントか（`yes` または `no`）。	
`-second-authentication-method`	多要素認証の場合の2番目の認証方式： • `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` は、passwordまたはnsswitchです • `password` でのユーザパスワード認証に使用します `authmethod` は公開鍵です • `nsswitch` authmethodがpublickeyの場合のユーザパスワード認証用 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以降では、trueに設定すると、nsswitch認証に対して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高速バインドを使用するには、を使用します `-authentication-method` 値はに設定する必要があります `nsswitch`。 "nsswitch認証のLDAP fastbindについて説明します。"	

Cisco Duoセキュリティ情報の設定

次の値はで指定します `security login duo create` コマンドは、Storage VMに対してSSHログインを使用したCisco Duoツーファクタ認証を有効にする場合に使用します。

フィールド	説明	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秘密キー。	
`-api-host`	SSHアプリケーションをDuoに登録するときに取得されるAPIホスト名。例： `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	Duo認証を妨げるサービスまたは構成エラーの場合は、失敗します。 `safe` （アクセスを許可）または `secure` （アクセスを拒否）。デフォルトはです `safe`これは、Duo APIサーバーにアクセスできないなどのエラーが原因で失敗した場合、Duo認証がバイパスされることを意味します。	
`-http-proxy`	指定した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にクレデンシャルを含めます。例： `http-proxy=http://username:password@proxy.example.org:8080`	
`-autopush`	または `true` または `false`。デフォルトはです `false`。状況 `true`Duoは、プッシュログイン要求をユーザーの電話に自動的に送信し、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ります。状況 `false`を選択すると、認証方法を選択するように求められます。 セツテイシタシヨウコウ `autopush = true`を設定することをお勧めします `max-prompts = 1`。	

-max-prompts	ユーザーが2番目のファクターで認証に失敗した場合、Duoはユーザーに再度認証を求めるプロンプトを表示します。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。でなければなりません 1、 2`または `3。デフォルト値はです 1。 例えば、`max-prompts = 1`ユーザ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、次の場合は`max-prompts = 2`ユーザが最初のプロンプトで誤った情報を入力すると、再度認証を求めるプロンプトが表示されます。 セツテイシタシヨウコウ autopush = true`を設定することをお勧めします `max-prompts = 1。 最高のエクスペリエンスを得るために、公開鍵認証のみを使用するユーザには、常に max-prompts をに設定します 1。	
-enabled	Duo 2要素認証を有効にします。をに設定します true デフォルトでは有効にすると、設定されているパラメータに従って、SSHログイン時にDuo 2要素認証が実行されます。Duoが無効になっている場合（ false)、Duo認証は無視されます。	

カスタムロールを定義する

次の値はで指定します security login role create コマンドは、カスタムロールを定義するときに使用します。

フィールド	説明	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と表示されます）の名前。	
-role	ロールの名前。	

-cmddirname	ロールでアクセスでき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の名前は二重引用符（"）で囲む必要があります。例："volume snapshot"。入る必要があります DEFAULT すべてのコマンドディレクトリを指定します。	
-access	（任意）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 へのアクセスを許可します 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 • 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 for_nonintrinsic commands_（末尾がでないコマンド create、modify、 delete`または `show）： • 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 は適用されません • 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	（任意）アクセスレベルのフィルタリングに使用されるクエリーオブジェクト。コマンドの有効なオプションまたはコマンドディレクトリ内のコマンドの形式で指定します。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の場合などです volume、クエリーオブジェクト "-aggr aggr0" のアクセスを有効にします aggr0 アグリゲートのみ：	

ユーザアカウントに公開鍵を関連付けます

次の値はで指定します security login publickey create コマンドは、SSH公開鍵をユーザアカウントに関連付けるときに使用します。

フィールド	説明	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名。デフォルト値 `admin`に変更します。これは、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キーの場合は 0 です。それ以外の場合、デフォルト値は、そのアカウントに対して既存の最も大きいインデックス番号の 1 つ以上になります。	
-publickey	OpenSSH 公開鍵。キーは二重引用符（"）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。テキストは二重引用符（"）で囲む必要があります。	

`-x509-certificate`	（任意）ONTAP 9.13.1以降では、SSH公開鍵とのX.509証明書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、ONTAPはSSHログイン時にこの証明書が有効かどうかを確認します。有効期限が切れているか失効している場合、ログインは許可されず、関連するSSH公開鍵は無効になります。有効な値は次のとおり • `install`：指定したPEMでエンコードされた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ます。 • `modify`：PEMでエンコードされた既存の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ます。 • `delete`：既存のX.509証明書とSSH公開鍵の関連付けを削除します。	

CA 署名済みサーバデジタル証明書をインストールする。

次の値はで指定します `security certificate generate-csr` Storage VMをSSLサーバとして認証するために使用するデジタル証明書署名要求（CSR）を生成するときにコマンドを実行します。

フィールド	説明	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、キーのセキュリティは向上します。デフォルト値はです `2048`。指定できる値はです `512`、 `1024`、`1536``および `2048`。	
`-country`	Storage VMの国（2文字のコード）。デフォルト値はです `US`。コードの一覧については、マニュアルページを参照してください。	

`-state`	Storage VMの都道府県。	
`-locality`	Storage VMの局所性。	
`-organization`	Storage VMの組織。	
`-unit`	Storage VMの組織内の単位。	
`-email-addr`	Storage VMの管理者連絡先のEメールアドレス。	
`-hash-function`	証明書の署名に使用する暗号化ハッシュ関数。デフォルト値はです `SHA256`。指定できる値はです `SHA1`、 `SHA256``および `MD5`。	

次の値はで指定します `security certificate install` コマンドは、クラスタまたはStorage VMをSSLサーバとして認証するためにCA署名デジタル証明書をインストールするときに使用します。次の表には、アカウント設定に関連するオプションのみを示します。

フィールド	説明	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` （サーバ証明書と中間証明書） • `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 がクライアントであるSSLサーバのルートCAの公開鍵証明書用 • `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および秘密鍵	

Active Directory ドメインコントローラアクセスを設定する

次の値はで指定します `security login domain-tunnel create` コマンドは、データStorage VM用のSMBサーバがすでに設定されていて、Storage VMをゲートウェイまたは_tunnel_（Active Directoryドメインコントローラによるクラスタへのアクセスの場合）として設定する場合に使用します。

フィールド	説明	あなたの価値

`-vserver`	SMBサーバが設定されているStorage VMの名前。	

次の値はで指定します `vserver active-directory create` コマンドは、SMBサーバを設定しておらず、Active DirectoryドメインにStorage VMコンピュータアカウントを作成する場合に使用します。

フィールド	説明	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。デフォルト値はです `CN=Computers` 。ONTAP はこの値をドメイン名に付加して、 Active Directory 識別名を生成します。	

LDAP サーバまたは **NIS** サーバのアクセスを設定

次の値はで指定します `vserver services name-service ldap client create` コマンドは、Storage VMのLDAPクライアント設定を作成するときに使用します。

次の表には、アカウント設定に関連するオプションのみを示します。

フィールド	説明	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`	クライアントの接続先LDAPサーバのIPアドレスと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ていません。	

次の値はで指定します `vserver services name-service ldap create` コマンドは、LDAPクライアント設定をStorage VMに関連付けるときに使用します。

フィールド	説明	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`	Storage VMでLDAPクライアント設定を使用できるかどうか (`true` または `false`）。	

次の値はで指定します `vserver services name-service nis-domain create` コマンドは、Storage VMにNISドメイン設定を作成するときに使用します。

フィールド	説明	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。	
`-active`	ドメインがアクティブかどうか (`true` または `false`）。	
`-servers`	• ONTAP 9.0 、 9.1 * ：ドメイン設定で使用される NIS サーバの IP アドレスをカンマで区切って指定します。	

-nis-servers	ドメイン設定で使用されるNISサーバのIPアドレスとホスト名をカンマで区切ったリスト。	

次の値はで指定します vserver services name-service ns-switch create コマンドは、ネームサービスソースの参照順序を指定するときに使用します。

フィールド	説明	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） • group （ファイル、LDAP、およびNISの各ネームサービス） • passwd （ファイル、LDAP、およびNISの各ネームサービス） • netgroup （ファイル、LDAP、およびNISの各ネームサービス） • namemap フアイルトLDAPネエムサアヒス	
-sources	ネームサービスソースを検索する順序（カンマで区切ったリスト）。 • files • dns • ldap • nis	

SAML アクセスを設定する

ONTAP 9.3以降では、で次の値を指定します security saml-sp create SAML認証を設定するコマンド。

フィールド	説明	あなたの価値

`-idp-uri`	アイデンティティプロバイダ（ IdP ）メタデータのダウンロード元である IdP ホストの FTP アドレスまたは 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発行認証局（CA）と証明書のシリアル番号、またはサーバ証明書の共通名を入力できます。	
`-verify-metadata-server`	IdPメタデータサーバのIDを検証するかどうか `true` または `false` ）。この値は常にに設定することを推奨します `true`。	

ログインアカウントを作成します

ログインアカウントの作成の概要

クラスタおよび SVM の管理者アカウントは、ローカルまたはリモートのいずれかとして有効にできます。ローカルアカウントでは、アカウント情報、公開鍵、セキュリティ証明書がストレージシステムに格納されます。AD アカウント情報はドメインコントローラに格納されます。LDAP および NIS アカウントは LDAP サーバおよび NIS サーバ上に存在します。

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とクラスタ管理者（予約された名前）`admin` は、クラスタのセットアップ時に自動的に作成されます。

デフォルトを持つクラスタ管理者 `admin` ロールは、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、必要に応じて別のロールを割り当てた別のクラスタ管理者を作成することができます。

SVM administrator 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、が割り当てられます `vsadmin` デフォルトではロール。クラスタ管理者は、必要に応じて SVM 管理者に別の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は、次の汎用名は使用できません。

- "adm"
- "ビン"
- "CLI"
- "デーモン"
- "ftp"
- "ゲーム"
- "停止"
- "LP"
- "メール"
- "男"
- "naroot"
- " NetApp "
- "ニュース"
- "誰もいない"
- "演算子"
- "ルート"
- "シャットダウン"
- "sshd"
- "同期"
- "sys"
- " uucp"
- "WWW"

マージされたロール

同じユーザに対して複数のリモートアカウントを有効にすると、そのユーザには各アカウントに対して指定されたロールがすべて割り当てられます。つまり、LDAPまたはNISアカウントにが割り当てられている場合です `vsadmin` ロールが割り当てられ、同じユーザのADグループアカウントにが割り当てられます `vsadmin-volume` ロール。ADユーザは、より包括的なを使用してログインします `vsadmin` 機能：ロールは、 _ merged__ と呼ばれます。

ローカルアカウントアクセスを有効にします

ローカルアカウントアクセスの有効化の概要

ローカルアカウントでは、アカウント情報、公開鍵、セキュリティ証明書がストレージシステムに格納されます。を使用できます `security login create` コマンドを使用して、ローカルアカウントが管理またはデータSVMにアクセスできるようにします。

パスワードアカウントアクセスを有効にします

を使用できます `security login create` コマンドを使用して、管理者アカウントがパスワードを使用して管理またはデータSVM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。

このタスクについて

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、を使用します `security login modify` コマンドを使用してあとでロールを追加します。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

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`*

   コマンド構文全体については、を参照してください "ワークシート"。

   次のコマンドは、クラスタ管理者アカウントを有効にします `admin1` を使用します `backup` 管理SVMにアクセスするためのロール`engCluster` パスワードを使用する。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
   ```

SSH 公開鍵アカウントを有効にします

を使用できます `security login create` コマンドを使用して、管理者アカウントがSSH公開鍵を使用して管理またはデータSVMにアクセスできるようにします。

このタスクについて

- 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、を使用します `security login modify` コマンドを使用してあとでロールを追加します。

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のない既存のSSH公開鍵アカウントを、サポートされるキータイプで再設定する必要があります。 FIPSを有効にする前にアカウントを再設定する必要があります。そうしないと、管理者認証が失敗します。

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	FIPS以外のモードでサポートされるキータイプ
9.11.1以降	ECDSA - sha2 - nistp256	ECDSA-sha2-nistp256+ rsa-sha2-512+ rsa-sha2-256+ SSH-ed25519以降 SSH-DSS+ SSH-RSA
9.10.1以前	ECDSA-sha2-nistp256+ SSH-ed25519	ECDSA-sha2-nistp256+ SSH-ed25519以降 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、を参照してください "FIPS を使用してネットワークセキュリティを設定する"。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

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`*

   コマンド構文全体については、を参照してください "ワークシート"。

   次のコマンドは、SVM管理者アカウントを有効にします `svmadmin1` を使用します `vsadmin-volume` SVMにアクセスするためのロール`engData1` SSH公開鍵の使用：

   ```
   cluster1::>security login create -vserver engData1 -user-or-group-name
   svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
   ```

完了後

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は、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

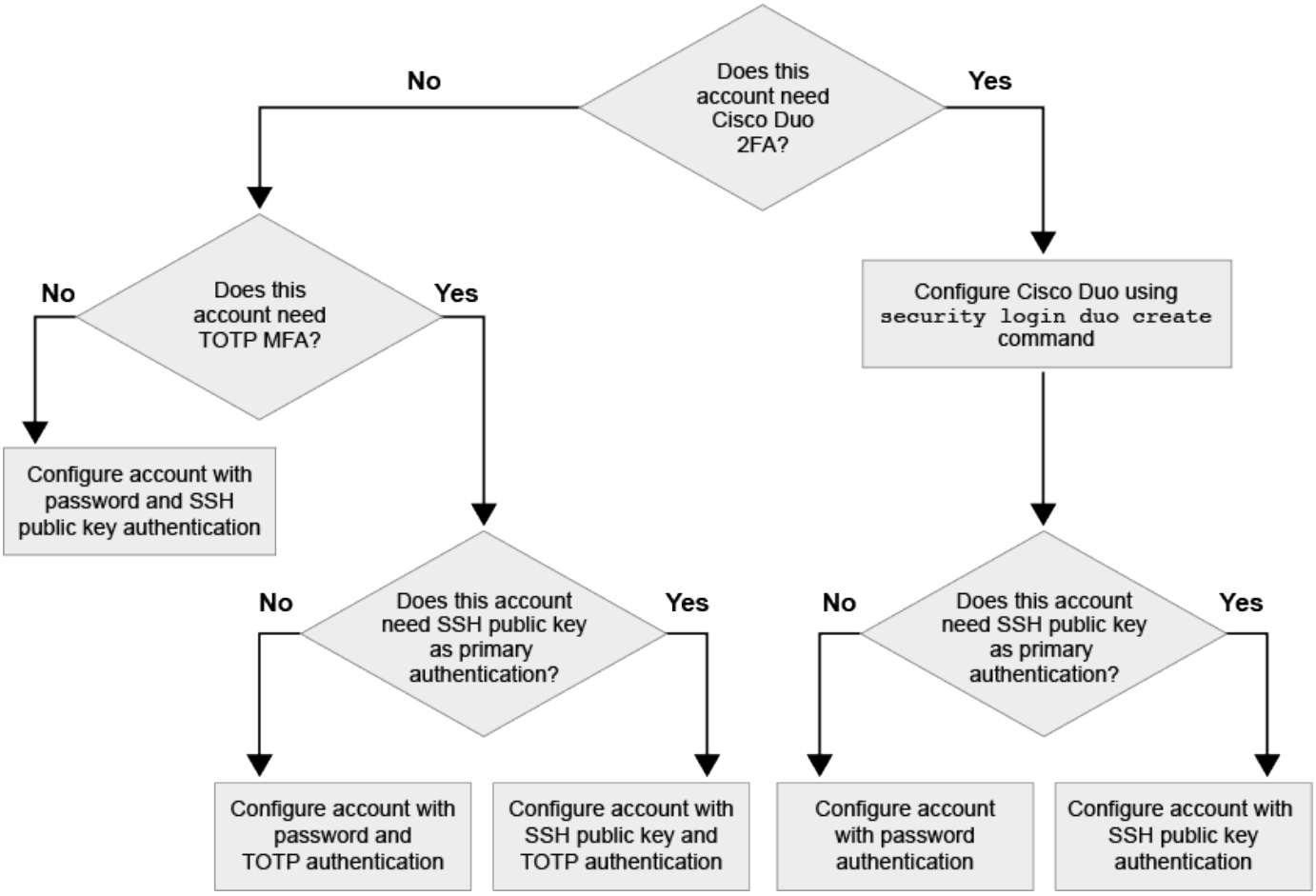
多要素認証の概要

多要素認証（MFA）を使用すると、ユーザが管理Storage VMまたはデータStorage VMにログインする際に2つの認証方式を指定する必要があるため、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、および時間ベースのワンタイムパスワード（TOTP）を組み合わせて多要素認証に使用できます。Cisco Duo（ONTAP 9.14.1以降）をイネーブルにして設定すると、追加の認証方式として機能し、すべてのユーザの既存の方式を補完します。

使用可能なバージョン	最初の認証方法	**2**番目の認証方法
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、クラスタ管理者が最初に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。



多要素認証を有効にします

多要素認証（MFA）を使用すると、管理SVMまたはデータSVMにログインする際にユーザに2つの認証方式の指定を要求することで、セキュリティを強化できます。

このタスクについて

- 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、を使用します `security login modify` コマンドを使用してあとでロールを追加します。

  "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は、アカウントがSVMにアクセスする前にアカウントに公開鍵を関連付ける必要があります。

  "ユーザアカウントに公開鍵を関連付けます"

  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して**MFA**を有効にします

ONTAP 9.3以降では、クラスタ管理者がSSH公開鍵とユーザパスワードを使用してMFAを使用してログインするための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でSSH公開鍵とユーザパスワードを使用してMFAを有効にします。

```
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>
```

次のコマンドを実行するには、SVM管理者アカウントが必要です `admin2` を使用します `admin` SVMにログインするためのロール`engData1` SSH公開鍵とユーザパスワードの両方を使用して、次の手順を実行します。

```
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".
```

TOTPで**MFA**を有効にする

ONTAP 9.13.1以降では、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）の両方を使用してローカルユーザに管理SVMまたはデータSVMへのログインを要求することで、セキュリティを強化できます。TOTPを使用してMFAのアカウントを有効にしたあと、ローカルユーザはにログインする必要があります "設定を完了します"。

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を使用する場合は、常にSSH公開鍵またはユーザパスワードに続く2番目の認証形式になります。

作業を開始する前に

これらのタスクを実行するには、ストレージ管理者である必要があります。

手順

最初の認証方法としてユーザパスワードまたはSSH公開鍵を使用し、2番目の認証方法としてTOTPを使用してMFAを設定できます。

ユーザパスワードと**TOTP**で**MFA**を有効にします

1. ユーザパスワードとTOTPを使用して、ユーザアカウントで多要素認証を有効にします。

   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を使用した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**を使用して**MFA**を有効にします

1. SSH公開鍵とTOTPを使用した多要素認証のユーザアカウントを有効にします。

   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>
   ```

2. TOTPを使用したMFAが有効になっていることを確認します。

```
security login show
```

完了後

- 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は、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"

- TOTPを使用したMFAの設定を完了するには、ローカルユーザがログインする必要があります。

  "TOTPを使用してMFA用のローカルユーザアカウントを設定します"

関連情報

の詳細を確認してください "ONTAP 9での多要素認証（TR-4647）"。

TOTPを使用して**MFA**用のローカルユーザアカウントを設定します

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）を使用して多要素認証（MFA）でユーザアカウントを設定できます。

作業を開始する前に

- ストレージ管理者が必要です "TOTPでMFAを有効にする" ユーザーアカウントの2番目の認証方法として。
- プライマリユーザアカウントの認証方法は、ユーザパスワードまたは公開SSHキーである必要があります。
- スマートフォンと連携するようにTOTPアプリを設定し、TOTPシークレットキーを作成する必要があります。

  TOTPは、Google Authenticatorなどのさまざまな認証アプリでサポートされています。

手順

1. 現在の認証方法でユーザー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. アカウントで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>"
```

TOTPシークレットキーをリセットします

アカウントのセキュリティを保護するために、TOTPシークレットキーが侵害されたり紛失したりした場合は、それ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。

キーが侵害された場合はTOTPをリセットします

TOTPシークレットキーが侵害されたにもかかわらず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>
```

キーを紛失した場合はTOTPをリセットします

TOTPシークレットキーが失われた場合は、ストレージ管理者にに問い合わせてください "キーを無効にします"。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。

作業を開始する前に

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。
ストレージ管理者アカウントがない場合は、ストレージ管理者に連絡してキーを無効にしてください。

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、プライマリの認証方法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>
```

ローカルアカウントの**TOTP**シークレットキーを無効にします

ローカルユーザの時間ベースのワンタイムパスワード（TOTP）シークレットキーが失われた場合、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。

このタスクについて

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。

ステップ

1. TOTPシークレットキーを無効にします。

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

SSL 証明書アカウントを有効にします

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

このタスクについて

- 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を生成し、インストールする

  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、を使用してあとでロールを追加できます `security login modify` コマンドを実行します

  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、証明書認証はでサポートされます。 `http`、 `ontapi`および `rest` アプリケーション：SVM管理者アカウントの場合、でのみ証明書認証がサポートされます `ontapi` および `rest` アプリケーション：

ステップ

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
   ```

   コマンド構文全体については、を参照してください "ONTAP のマニュアルページ - リリース別"。

   次のコマンドは、SVM管理者アカウントを有効にします `svmadmin2` デフォルトで設定されています `vsadmin` SVMにアクセスするためのロール`engData2` SSLデジタル証明書を使用する。

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

完了後

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を生成し、インストールする

Active Directory アカウントアクセスを有効にします

を使用できます `security login create` コマンドを使用して、Active Directory（AD）ユーザまたはグループアカウントが管理またはデータSVMにアクセスできるようにします。AD グループのすべてのユーザは、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。

このタスクについて

- 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を設定しています

  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ユーザパスワードを使用して、SSH公開鍵をプライマリまたはセカンダリの認証方式として使用できます。

  SSH公開鍵をプライマリ認証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、を使用できます "nsswitch認証のためのLDAP高速バインド" AD LDAPサーバでサポートされている場合。

- 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、を使用します `security login modify` コマンドを使用してあとでロールを追加します。

  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へのアクセスは、でのみサポートされます `SSH`、 `ontapi`および `rest` アプリケーション：ADグループは、多要素認証に一般的に使用されるSSH公開鍵認証ではサポートされません。

作業を開始する前に

- クラスタ時間と AD 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。

ステップ

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ユーザの場合：*

ONTAPバージョン	プライマリ認証	セカンダリ認証	コマンドを実行します
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>`

ONTAPバージョン	プライマリ認証	セカンダリ認証	コマンドを実行します

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

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バージョン	プライマリ認証	セカンダリ認証	コマンドを実行します
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]`

+
コマンド構文全体については、を参照してください "管理者認証およびRBAC設定用のワークシート"

完了後

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を設定しています

LDAP または **NIS** アカウントアクセスを有効にします

を使用できます `security login create` LDAPまたはNISのユーザアカウントが管理またはデータSVMにアクセスできるようにするコマンド。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。

このタスクについて

- 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 サーバのアクセスを設定する

  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、を使用します `security login modify` コマンドを使用してあとでロールを追加します。

  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、を使用できます "nsswitch認証のためのLDAP高速バインド" LDAPサーバでサポートされている場合。
- LDAP問題 は既知のものであるため、は使用しないでください `':'` LDAPユーザアカウント情報の任意のフィールドの（コロン）文字（例： `gecos`、 `userPassword`など）。そうしないと、そのユーザの検索操作が失敗します。

作業を開始する前に

このタスクを実行するには、クラスタ管理者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]
   ```

   コマンド構文全体については、を参照してください "ワークシート"。

   "ログインアカウントを作成または変更する"

次のコマンドは、LDAPまたはNISのクラスタ管理者アカウントを有効にします `guest2` を使用します `backup` 管理SVMにアクセスするためのロール`engCluster`。

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

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
   ```

   認証方法はと指定できます `publickey` および2番目の認証方法をに設定します `nsswitch`。

   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"
   ```

完了後

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 サーバのアクセスを設定する

アクセス制御ロールを管理します

アクセス制御ロールの概要

管理者がアクセスできるコマンドは、管理者に割り当てられたロールで決まります。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。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できます。

管理者に割り当てられているロールを変更します

を使用できます `security login modify` コマンドを使用して、クラスタ管理者アカウントまたはSVM管理者アカウントのロールを変更します。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。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. クラスタ管理者または 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
```

コマンド構文全体については、を参照してください "ワークシート"。

"ログインアカウントを作成または変更する"

次のコマンドは、ADクラスタ管理者アカウントのロールを変更します `DOMAIN1\guest1` に移動します `readonly` ロール。

```
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のSVM管理者アカウントのロールを変更します `DOMAIN1\adgroup` カスタムに `vol_role` ロール。

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

カスタムロールを定義する

を使用できます `security login role create` カスタムロールを定義するコマンド。このコマンドを必要な回数だけ実行して、ロールに関連付ける機能の正確な組み合わせを実現できます。

このタスクについて

- 事前定義かカスタムかにかかわらず、ロールは ONTAP コマンドまたはコマンドディレクトリへのアクセスを許可または拒否します。

  コマンドディレクトリ (`volume`など）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に含まれる各コマンドへのアクセスが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。

> でのみ使用可能なコマンドやコマンドディレクトリへのアクセスを許可するロールをSVM管理者に割り当てることはできません `admin` クラスタ管理者（例：） `security` コマンドディレクトリ。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

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
   ```

   コマンド構文全体については、を参照してください "ワークシート"。

   次のコマンドは、を許可します `vol_role` ロールに内のコマンドへのフルアクセス権が付与されます `volume` コマンドディレクトリ、および内のコマンドへの読み取り専用アクセス `volume snapshot` サブディレクトリ。

   ```
   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、を許可します `SVM_storage` ロール内のコマンドへの読み取り専用アクセス `storage` コマンドディレクトリ。内のコマンドにはアクセスできません `storage encryption` サブディレクトリにアクセスし、へのフルアクセスを許可します `storage aggregate plex offline` 非組み込みコマンド。

   ```
   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
   ```

クラスタ管理者の事前定義されたロール

ほとんどの場合、クラスタ管理者用に事前定義されたロールで十分です。必要に応じて、カスタムロールを作成することができます。デフォルトでは、クラスタ管理者には事前定義されたが割り当てられます `admin` ロール。

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。

ロール	アクセスレベル	コマンドまたはコマンドディレクトリに移動します

管理	すべて	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
読み取り専用です	• 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	すべて
• set • system node autosupport	なし	その他すべてのコマンドディレクトリ (DEFAULT)
バックアップ	すべて	vserver services ndmp
• 読み取り専用	volume	なし

その他すべてのコマンドディレクトリ (DEFAULT)	• 読み取り専用	すべて
• security login password 自身のユーザアカウントのローカルパスワードとキー情報のみを管理する場合 • set	なし	security
• 読み取り専用	その他すべてのコマンドディレクトリ (DEFAULT)	なし

。 autosupport ロールは事前定義されたに割り当てられます autosupport AutoSupport OnDemandで使用されるアカウント。ONTAP では、を変更または削除することはできません autosupport アカウント：また、ONTAP ではを割り当てることもできません autosupport 他のユーザアカウントへのロール。

SVM 管理者の事前定義されたロール

SVM 管理者用に、ほとんどのニーズに合わせて事前定義されたロールが用意されています。必要に応じて、カスタムロールを作成することができます。デフォルトでは、SVM 管理者には事前定義されたが割り当てられます vsadmin ロール。

次の表に、 SVM 管理者用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のローカルパスワードとキー情報を管理します • ボリューム移動を除くボリュームの管理 • クォータ、 qtree 、 Snapshot コピー、およびファイルの管理 • LUN の管理 • privileged delete を除く SnapLock 処理の実行 • プロトコルの設定：NFS、SMB、iSCSI、FC 、FCoE、 NVMe/FCとNVMe/TCP • サービスの設定： DNS 、 LDAP 、 NIS • ジョブの監視 • ネットワーク接続およびネットワークインターフェイスの監視 • SVM の健常性を監視

vsadmin-volume	• 自身のユーザアカウントのローカルパスワードとキー情報を管理します • ボリュームの移動を含む、ボリュームの管理 • クォータ、 qtree 、 Snapshot コピー、およびファイルの管理 • LUN の管理 • プロトコルの設定：NFS、SMB、iSCSI、FC 、FCoE、 NVMe/FCと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 の健常性を監視
vsadmin-protocol のいずれかです	• 自身のユーザアカウントのローカルパスワードとキー情報を管理します • プロトコルの設定：NFS、SMB、iSCSI、FC 、FCoE、 NVMe/FCと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 の健常性を監視
vsadmin-backup のストレージシステムで	• 自身のユーザアカウントのローカルパスワードとキー情報を管理します • NDMP 処理の管理 • リストアしたボリュームを読み取り / 書き込み可能にします • SnapMirror 関係と Snapshot コピーの管理 • 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のローカルパスワードとキー情報を管理します • ボリューム移動を除くボリュームの管理 • クォータ、 qtree 、 Snapshot コピー、およびファイルの管理 • privileged delete などの SnapLock 処理の実行 • 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 • ネットワーク接続およびネットワークインターフェイスの監視
vsadmin-readonly （読み取り専用	• 自身のユーザアカウントのローカルパスワードとキー情報を管理します • SVM の健常性を監視 • ネットワークインターフェイスの監視 • ボリュームと LUN を表示します • サービスとプロトコルの表示

管理者アクセスの制御

管理者に割り当てるロールによって、 System Manager で実行できる機能が決まります。クラスタ管理者と Storage VM 管理者の事前定義されたロールは System Manager から提供されます。 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るか、後で別のロールを割り当てることができます。

アカウントアクセスを有効にした方法によっては、次のいずれかを実行する必要があります。

- ローカルアカウントに公開鍵を関連付けます。
- CA 署名済み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

これらのタスクは、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。

管理者にロールを割り当てます

次のように、管理者にロールを割り当てます。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. 選択するオプション → をクリックします。

3. 選択するオプション + Add [* ユーザー *] の下。
4. ユーザー名を指定し、 * 役割 * のドロップダウンメニューで役割を選択します。
5. ユーザのログイン方法およびパスワードを指定します。

管理者のロールを変更する

管理者のロールを次のように変更します。

手順

1. **[Cluster] > [Settings]** の順にクリックします。
2. ロールを変更するユーザの名前を選択し、をクリックします ⋮ ユーザ名の横に表示されます。
3. [編集（ Edit ）] をクリックします。
4. [*Role] のドロップダウンメニューで、ロールを選択します。

管理者アカウントを管理する

管理者アカウントの管理の概要

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

管理者アカウントに公開鍵を関連付けます

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

このタスクについて

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

作業を開始する前に

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

手順

1. 管理者アカウントに公開鍵を関連付けます。

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

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

2. 公開鍵を表示して変更を確認します。

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

例

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

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

管理者アカウントの**SSH**公開鍵と**X.509**証明書を管理します

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

公開鍵と**X.509**証明書を管理者アカウントに関連付けます

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

このタスクについて

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

作業を開始する前に

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

手順

1. 公開鍵とX.509証明書を管理者アカウントに関連付けます。

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

index -publickey *certificate* -x509-certificate install

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

2. 公開鍵を表示して変更を確認します。

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

例

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

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

管理者アカウントのSSH公開鍵から証明書の関連付けを削除します

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

作業を開始する前に

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

手順

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

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

2. 公開鍵を表示して変更を確認します。

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

例

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

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

管理者アカウントから公開鍵と証明書の関連付けを削除します

アカウントから現在の公開鍵と証明書の設定を削除できます。

作業を開始する前に

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

手順

1. 管理者アカウントから公開鍵とX.509証明書の関連付けを削除します。

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

2. 公開鍵を表示して変更を確認します。

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

例

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

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

SSHログイン用の**Cisco Duo 2FA**の設定

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

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

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

- Cisco Duoの設定
- Cisco Duo設定の変更
- Cisco Duo設定の削除
- Cisco Duo設定の表示
- Duoグループの削除
- Duoグループの表示

- ユーザーのDuo認証をバイパスする

Cisco Duoの設定

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

手順

1. Cisco Duo管理パネルにログインします。
2. [アプリケーション]>[UNIXアプリケーション]*に移動します。
3. 統合キー、シークレットキー、およびAPIホスト名を記録します。
4. SSHを使用してONTAPアカウントにログインします。
5. このStorage VMに対してCisco Duo認証を有効にし、環境の情報を括弧内の値に置き換えます。

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

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

Cisco Duo設定の変更

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

手順

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

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

Cisco Duo設定の削除

Cisco Duo設定を削除すると、SSHユーザがログイン時にDuoを使用して認証する必要がなくなります。Storage VM（ONTAP CLIではVserverと呼ばれます）のCisco Duo設定を削除するには、 `security login duo delete` コマンドを実行します

手順

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

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

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

Cisco Duo設定の表示

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

手順

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

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

   次のような出力が表示されます。

```
Vserver: testcluster
Enabled: true

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

Duoグループの作成

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

手順

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

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

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

Duoグループの表示

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

手順

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

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

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

Duoグループの削除

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

手順

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

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

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

ユーザーのDuo認証をバイパスする

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

すべてのDuoユーザーを除外

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

手順

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

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

Duoグループユーザーを除外

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

手順

1. SSHを使用してONTAPアカウントにログインします。

2. グループ内の特定のユーザに対してCisco Duo認証をディセーブルにします。括弧内の値は、除外するグループ名とユーザのリストに置き換えてください。

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

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

ローカル**Duo**ユーザを除外

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

CA 署名済みサーバ証明書の概要を生成してインストールする

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

証明書署名要求を生成します

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

作業を開始する前に

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

手順

1. CSR を生成します

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

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

CSRの作成例

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

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----


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

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

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

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

CA 署名済みサーバ証明書をインストールします

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

作業を開始する前に

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

ステップ

1. CA署名済みサーバ証明書をインストールします。

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

   コマンド構文全体については、を参照してください "ワークシート"。

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

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

CA署名済みサーバ証明書中間証明書のインストール例

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


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

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

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----


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

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

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----END CERTIFICATE-----


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

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

System Manager を使用して証明書を管理します

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

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

証明書情報を表示します

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

手順

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

c. [設定]タブに切り替えます。

d. [証明書]セクションに表示されている番号を選択します。

次に何をするか

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

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

証明書署名要求を生成します

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

手順

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

信頼できる認証局をインストール（追加）します

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

手順

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

信頼された認証局を削除します

System Manager を使用して、信頼された認証局を削除できます。

> ONTAPがプリインストールされている信頼された認証局は削除できません。

手順

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

信頼された認証局を更新してください

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

手順

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

クライアント / サーバ証明書をインストール（追加）します

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

手順

1. クライアント / サーバ証明書 * タブを表示します。 を参照してください [証明書情報を表示します]。
2. 選択するオプション + Add 。
3. [Add Client/Server Certificate] パネルで、次の手順を実行します。

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

自己署名クライアント / サーバ証明書を生成（追加）します

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

手順

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

クライアント / サーバ証明書を削除します

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

手順

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

クライアント / サーバ証明書を更新します

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

手順

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

2. クライアント/サーバ証明書の名前を選択します。
3. 選択するオプション ⋮ 名前の横にある * Renew * （更新）をクリックします。

新しいローカル認証局を作成します

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

手順

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

ローカルの認証局を使用して証明書に署名します

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

手順

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

ローカル認証局を削除します

System Manager では、ローカルの認証局を削除できます。

手順

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

ローカルの認証局を更新してください

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

手順

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

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

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

ONTAP は、次のドメインコントローラ認証サービスをサポートしています。

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

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

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

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

- ONTAP 9.14.1以降では、SVMの作成時にAESがデフォルトで有効になり、ネットログオンでのセキュアチャネルの確立時にAESセッションキーを使用するようにSVMのセキュリティ設定を変更する必要はありません。
- ONTAP 9.10.1~9.13.1では、SVMの作成時にAESがデフォルトで無効になります。次のコマンドを使用してAESを有効にする必要があります。

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

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

認証トンネルを設定します

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

作業を開始する前に

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

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

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

ステップ

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

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

   コマンド構文全体については、を参照してください "ワークシート"。

   ユーザを認証するには、 SVM が実行されている必要があります。

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

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

ドメインに **SVM** コンピュータアカウントを作成します

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

このタスクについて

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

作業を開始する前に

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

ステップ

1. AD ドメインに SVM 用のコンピュータアカウントを作成します。

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

   コマンド構文全体については、を参照してください "ワークシート"。

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

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

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

Enter the user name: Administrator

Enter the password:
```

LDAP サーバまたは **NIS** サーバのアクセスの概要を設定

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

LDAP サーバアクセスを設定する

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

このタスクについて

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

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

- AD-SFU （ Windows Server 2003 以前の AD サーバ）
- RFC-2307 （ UNIX LDAP サーバ）

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

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

作業を開始する前に

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

手順

1. SVMにLDAPクライアント設定を作成します。

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

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

   コマンド構文全体については、を参照してください "ワークシート"。

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

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

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

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

   コマンド構文全体については、を参照してください "ワークシート"。

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

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

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

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

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

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

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

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

NIS サーバアクセスの設定

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

このタスクについて

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

作業を開始する前に

- SVM に NIS ドメインを設定するためには、設定済みのすべてのサーバが使用可能でアクセスできる状態になっている必要があります。
- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。

ステップ

1. SVMにNISドメイン設定を作成します。

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

   コマンド構文全体については、を参照してください "ワークシート"。

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

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

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

ネームサービススイッチを作成します

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

作業を開始する前に

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

ステップ

1. ネームサービスソースの参照順序を指定します。

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

   コマンド構文全体については、を参照してください "ワークシート"。

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

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

管理者パスワードを変更します

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

このタスクについて

新しいパスワードは次のルールに従う必要があります。

- ユーザ名を含めることはできません

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

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

作業を開始する前に

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

ステップ

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

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

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

管理者アカウントをロックおよびロック解除します

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

作業を開始する前に

これらのタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 管理者アカウントをロックします。

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

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

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

2. 管理者アカウントのロックを解除します。

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

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

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

失敗したログインを管理します

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

失敗したログインを確認する方法

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

ログイン試行が繰り返し失敗する場合の対処方法

侵入を防ぐための短期的な対策としては、次のような方法があります。

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

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

長期的に見て、次の手順を実行することもできます。

- を使用します security ssh modify コマンドを使用して、新しく作成するすべてのSVMに対してログインの失敗回数を制限します。
- ユーザにパスワードの変更を求めることで、既存の MD5 アルゴリズムのアカウントをより安全な SHA-512 アルゴリズムに移行する。

管理者アカウントのパスワードに **SHA-2** を適用します

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

このタスクについて

パスワードハッシュ機能を使用すると、次の操作を実行できます。

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

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

手順

1. MD5 管理者アカウントを SHA-512 パスワードハッシュ関数に移行します。
   a. すべてのMD5管理者アカウントを期限切れにします。 `security login expire-password -vserver * -username * -hash-function md5`

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

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

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

2. ユーザが一定期間ログインしていないためにパスワードが変更されない MD5 アカウントについては、強制的にアカウントを移行します。
   a. まだMD5ハッシュ関数を使用しているアカウントをロックします（advanced権限レベル）。 `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

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

   b. ユーザがパスワードを変更する準備ができたら、アカウントのロックを解除します。 `security login unlock -vserver *svm_name* -username *user_name*`
   c. ユーザに、コンソールまたは SSH セッションからアカウントにログインし、表示される指示に従ってパスワードを変更するよう促します。

ファイルアクセスの問題を診断して修正

手順

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

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

れます。

6. をクリックします ファイルアクセス権限を表示するには、結果テーブルの左側の列を参照してください。

管理者による検証を管理します

マルチ管理者検証の概要

ONTAP 9.11.1以降では、マルチ管理検証（MAV）を使用して、ボリュームやSnapshotコピーの削除などの特定の処理を、指定した管理者からの承認がないと実行できないようにすることができます。これにより、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が、望ましくない変更やデータの削除を行うことを防止でき

マルチ管理者検証の設定は、次のとおりです。

- "1つ以上の管理者承認グループを作成します。"
- "マルチ管理者検証機能の有効化。"
- "ルールを追加または変更する。"

初期設定後、これらの要素はMAV承認グループ（MAV管理者）の管理者のみが変更できます。

マルチ管理者検証を有効にすると、保護されたすべての処理が完了するために次の3つの手順が必要となります。

- ユーザが処理を開始すると、が実行されます "要求が生成されます。"
- 実行する前に、少なくとも1つは必要です "MAV管理者は承認する必要があります。"
- 承認されると、ユーザーは操作を完了します。

複数管理者による検証は、自動化の負荷が大きいボリュームやワークフローでは使用しないことを想定しています。自動化された各タスクを完了するには承認が必要なためです。 オートメーションとMAVを併用する場合は、MAVの特定の操作にクエリを使用することをお勧めします。たとえば、適用できます `volume delete` MAVルールは、自動化が関係しないボリュームにのみ適用され、特定の命名規則を使用して指定できます。

> MAVの管理者の承認なしでマルチ管理者検証機能を無効にする必要がある場合は、ネットアップサポートに連絡して、次の技術情報アーティクルを記載します。 "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"。

マルチ管理者検証の仕組み

マルチ管理者検証は、次の要素で構成されます。

- 承認権限と拒否権を持つ1人以上の管理者のグループ。
- 保護された操作またはコマンドのセット（a_rules table_）
- a_rulesエンジン_保護されたオペレーションの実行を識別および制御します

MAVルールは、Role-Based Access Control（RBAC；ロールベースアクセス制御）ルールのあとに評価されま

す。このため、保護された操作を実行または承認する管理者は、それらの操作に対する最低限のRBAC権限を持っている必要があります。 "RBACの詳細については、こちらをご覧ください。"

システム定義のルール

マルチ管理者検証を有効にすると、システム定義のルール（_guard-rale_rulesとも呼ばれます）によってMAV処理のセットが確立され、MAVプロセス自体が回避されるリスクが含まれます。これらの操作をルールテーブルから削除することはできません。MAVを有効にすると、アスタリスク（）で指定された操作は、実行前に**1**人以上の管理者による承認を必要とします。ただし、 show *コマンドは除きます。

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

  管理者による検証機能の設定を制御します。

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

  管理者による検証クレデンシャルを使用して、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*

  管理者による検証が必要な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。

ルールで保護されたコマンド

マルチ管理者検証を有効にした場合、システム定義のコマンドに加えて次のコマンドもデフォルトで保護されますが、これらのコマンドの保護を解除するようにルールを変更することができます。

- `security login password`
- `security login unlock`
- `set`

ONTAP 9.11.1以降のリリースでは、次のコマンドを保護できます。

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

ONTAP 9.13.1以降では、次のコマンドを保護できます。

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

ONTAP 9.14.1以降では、次のコマンドを保護できます。

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

複数管理者による承認の仕組み

保護された操作がMAV保護されたクラスタで入力されると、操作の実行要求が指定されたMAV管理者グループに送信されます。

次の項目を設定できます。

- 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を持つRBACロールが必要です。

- MAV管理者グループの数。
  - MAVグループは、保護された各操作ルールに割り当てられます。

    - 複数のMAVグループの場合、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。
- 保護された操作を実行するために必要なMAV承認の数。
- MAV管理者が承認要求に応答する必要がある_承認の失効_期間。
- 要求元の管理者が処理を完了する必要がある_実行のexpiry_period。

これらのパラメータを設定したら、MAV承認が必要です。

MAV管理者は、保護された操作を実行するための独自の要求を承認できません。そのため、次の

- 管理者が1人だけのクラスタではMAVを有効にしないでください。
- MAVグループにユーザーが1人しかいない場合、MAV管理者は保護された操作を入力できません。通常の管理者は、これらの操作を入力する必要があり、MAV管理者は承認のみを行えます。
- MAV管理者が保護された操作を実行できるようにするには、MAV管理者の数が、必要な承認数よりも1人大きくなければなりません。
  たとえば、保護された操作に2つの承認が必要で、MAV管理者がそれらを実行する場合、MAV管理者グループには3人の承認が必要です。

MAV管理者は、（EMSを使用して）Eメールアラートで承認要求を受信するか、要求キューを照会できます。リクエストを受け取った場合、次の3つのアクションのいずれかを実行できます。

- 承認します
- 拒否（拒否）
- 無視（操作なし）

MAVルールに関連付けられているすべての承認者に電子メール通知が送信されるのは、次の場合です。

- リクエストが作成されました。
- リクエストが承認または拒否された場合。
- 承認されたリクエストが実行されます。

リクエスト者が同じ承認グループに属している場合は、リクエストが承認されると電子メールが送信されます。

*注：*リクエスト者は、承認グループに属している場合でも、リクエスト者自身のリクエストを承認できません。ただし、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）リクエスタは、電子メール通知を受信しません。

保護された操作の実行の仕組み

保護された操作の実行が承認されると、要求されたユーザーは操作を続行します。処理が拒否された場合、要求元ユーザは処理を続行する前に要求を削除する必要があります。

MAVルールはRBAC権限の後に評価されます。そのため、操作の実行に十分なRBACアクセス許可がないユーザーはMAV要求プロセスを開始できません。

管理者の承認グループを管理します

Multi-Admin Verification（MAV；マルチ管理者検証）を有効にする前に、1人以上の管理

者が承認権限または拒否権限を付与される管理者承認グループを作成する必要があります。マルチ管理者検証を有効にすると、承認グループのメンバーシップを変更した場合には、既存の資格のある管理者の承認が必要になります。

このタスクについて

既存の管理者をMAVグループに追加したり、新しい管理者を作成したりできます。

MAV機能は、既存のロールベースアクセス制御（RBAC）設定に対応しています。MAV管理者は、MAV管理者グループに追加する前に、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の詳細については、こちらをご覧ください。"

MAVを設定して、承認リクエストが保留中であることをMAV管理者に通知できます。そのためには、Eメール通知（特に）を設定する必要があります `Mail From` および `Mail Server` パラメータ—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。MAV管理者は、電子メールアラートを使用しないで、承認キューを手動でチェックする必要があります。

System Manager の手順の略

MAV承認グループを初めて作成する場合は、「System Manager手順 to」を参照してください "マルチ管理者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. 管理者による検証を受ける管理者を特定します。
   a. [**Cluster]>[Settings.**]をクリックします
   b. をクリックします → をクリックします
   c. をクリックします + Add [**Users.**]の下にあります
   d. 必要に応じて名簿を変更します。

      詳細については、を参照してください "管理者アクセスの制御"

2. MAV承認グループを作成または変更します。
   a. [**Cluster]>[Settings.**]をクリックします
   b. をクリックします → 「セキュリティ」セクションの「*マルチ管理者承認」の横。（が表示されます ⚙ アイコン（MAVがまだ設定されていない場合）。
      - Name：グループ名を入力します。
      - 承認者：ユーザーのリストから承認者を選択します。
      - Eメールアドレス：Eメールアドレスを入力します。
      - デフォルトグループ：グループを選択します。

MAVを有効にした後、既存の設定を編集するにはMAV承認が必要です。

CLI 手順の略

1. に値が設定されていることを確認します `Mail From` および `Mail Server` パラメータ入力するコマンド

```
event config show
```

次のような情報が表示されます。

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

次のパラメータを入力して設定します。

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

2. 管理者による検証を受ける管理者を特定します

実行する処理	入力するコマンド
現在の管理者を表示します	`security login show`
現在の管理者のクレデンシャルの変更	`security login modify <parameters>`
新しい管理者アカウントを作成します	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

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。
- `-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つのメンバーと関連付けられたE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。

*注意：*すべての場合、MAV管理者による承認が必要です。

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

マルチ管理者検証を有効または無効にします

Multi-admin Verification（MAV；マルチ管理者検証）は明示的に有効にする必要があります。マルチ管理者検証を有効にした後は、MAV承認グループ（MAV管理者）の管理者による承認が必要になります。

このタスクについて

MAVを有効にすると、MAVを変更または無効にするには、MAV管理者の承認が必要になります。

> MAVの管理者の承認なしでマルチ管理者検証機能を無効にする必要がある場合は、ネットアップサポートに連絡して、次の技術情報アーティクルを記載します。 "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をイネーブルにすると、次のパラメータをグローバルに指定できます。

承認グループ

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とAutonomous Ransomware Protection（ARP）を使用している場合は、ARPの一時停止、無効化、および疑わしい要求のクリアを担当する新規または既存の承認グループを定義します。

必須の承認者

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

必要な承認者の数は、デフォルトの承認グループ内の一意の承認者の総数よりも少なくする必要があります。

承認の有効期限（時間、分、秒）

MAV管理者が承認要求に応答する必要がある期間。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。

実行の有効期限（時間、分、秒）

要求元の管理者が::operationを完了する必要がある期間。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。

特定のパラメータについて、これらのパラメータを上書きすることもできます "操作ルール。"

System Manager の手順の略

1. 管理者による検証を受ける管理者を特定します。
   a. **[Cluster]>[Settings.**]をクリックします
   b. をクリックします → をクリックします
   c. をクリックします + Add **[Users.**]の下にあります
   d. 必要に応じて名簿を変更します。

      詳細については、を参照してください "管理者アクセスの制御"

2. 少なくとも1つの承認グループを作成し、少なくとも1つのルールを追加して、マルチ管理者検証を有効にします。
   a. **[Cluster]>[Settings.**]をクリックします
   b. をクリックします ⚙ 「セキュリティ」セクションの「*マルチ管理者承認」の横。
   c. をクリックします + Add 1つ以上の承認グループを追加します。
      - 名前–グループ名を入力します。
      - 承認者–ユーザーのリストから承認者を選択します。
      - Eメールアドレス–Eメールアドレスを入力します。
      - デフォルトグループ–グループを選択します。
   d. ルールを少なくとも1つ追加してください。
      - 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、特定のルールに別の値を割り当てます。
  - 必要な承認者の数
  - 承認グループ

e. [詳細設定*]をクリックして、デフォルトを表示または変更します。
   - 必要な承認者数（デフォルト：1）
   - 実行要求の有効期限（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*
   - 送信元Eメールアドレス*

     *これらは、「通知管理」で管理されている電子メール設定を更新します。まだ設定されていない場合は、設定を求めるプロンプトが表示されます。

f. Enable（有効）*をクリックしてMAV初期設定を完了します。

初期設定後、現在のMAVステータスが* Multi-Admin Approval *（マルチ管理者承認）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操作
- 保留状態のオープン要求の数

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

マルチ管理者検証を無効にする場合：

1. **[Cluster]>[Settings.**]をクリックします
2. をクリックします ⚙ 「セキュリティ」セクションの「*マルチ管理者承認」の横。
3. [有効]トグルボタンをクリックします。

   この操作を完了するにはMAV承認が必要です。

CLI 手順の略

CLIでMAV機能をイネーブルにする前に、少なくとも1つ "MAV管理者グループ" を作成しておく必要があります。

実行する処理	入力するコマンド

MAV機能を有効にします	`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、MAVを1つの承認グループ、2つの必須承認者、およびデフォルトの有効期限で有効にします。
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	1つ以上を追加して初期設定を完了します "操作ルール。"

MAV設定の変更（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機能を確認します	`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`

保護された操作ルールを管理します

MAV（Multi-admin Verification）ルールを作成して、承認が必要な操作を指定します。操作が開始されるたびに、保護された操作が妨害され、承認の要求が生成されます。

ルールは任意の管理者が適切なRBAC機能を使用してMAVを有効にする前に作成できますが、MAVを有効にすると、ルールセットを変更するにはMAV承認が必要になります。

1回の操作で作成できるMAVルールは1つだけです。たとえば、複数のMAVルールを作成することはできません。 `volume-snapshot-delete` ルール。必要なルール制約は1つのルール内に含める必要があります。

ルールで保護されたコマンド

ONTAP 9.11.1以降では、次のコマンドを保護するルールを作成できます。

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

ONTAP 9.13.1以降では、次のコマンドを保護するルールを作成できます。

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

ONTAP 9.14.1以降では、次のコマンドを保護するルールを作成できます。

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`

- `vserver modify`

MAV system-defaultコマンドのルール `security multi-admin-verify` "コマンド"を変更することはできません。

マルチ管理者検証を有効にした場合、システム定義のコマンドに加えて次のコマンドもデフォルトで保護されますが、これらのコマンドの保護を解除するようにルールを変更することができます。

- `security login password`
- `security login unlock`
- `set`

ルール制約

ルールを作成するときに、オプションでを指定できます `-query` 要求をコマンド機能のサブセットに制限するオプション。。 `-query` オプションを使用すると、SVM、ボリューム、Snapshot名などの構成要素を制限することもできます。

例えば、 `volume snapshot delete` コマンド、 `-query` 次のように設定できます。 `-snapshot !hourly*,!daily*,!weekly*` つまり、hourly、daily、またはweekly属性のプレフィックスが付いたボリュームSnapshotは、MAV保護から除外されます。

```
smci-vsim20::> security multi-admin-verify rule show
                                            Required  Approval
Vserver Operation                           Approvers Groups
------- ------------------------------------ --------- -------------
vs01    volume snapshot delete               -         -
          Query: -snapshot !hourly*,!daily*,!weekly*
```

> 除外された構成要素はMAVによって保護されず、管理者はそれらを削除または名前変更できます。

デフォルトでは、ルールは対応するを指定します `security multi-admin-verify request create` *"protected_operation"* 保護されたオペレーションが入力されると、コマンドが自動的に生成されます。このデフォルトを変更して、が必要になるようにすることができます `request create` コマンドは別 々 に入力します。

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

- 承認者の必要数
- 承認グループ
- 承認の有効期限
- 実行の有効期限

System Manager の手順の略

保護された処理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 "マルチ管理者

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：

1. [* Cluster]>[Settings]（設定）*を選択します。
2. 選択するオプション 「セキュリティ」セクションの「*マルチ管理者承認」の横。
3. 選択するオプション + Add ルールを追加するには、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欄のままにします。グローバル設定を上書きする場合は、特定のルールに別の値を割り当てます。
     - 必要な承認者の数
     - 承認グループ

CLI 手順の略

> すべて `security multi-admin-verify rule` コマンドを実行するには、以外のMAV管理者の承認が必要です `security multi-admin-verify rule show`。

実行する処理	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]`

現在の管理者のクレデンシャルの変更	`security login modify <parameters>`
	
	例：次のルールでは、ルートボリュームの削除が承認されている必要があります。
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

ルールを変更します	`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"`
ルールを表示します	`security multi-admin-verify rule show`

コマンド構文の詳細については、を参照してください `security multi-admin-verify rule` マニュアルページ

保護された操作の実行を要求します

マルチ管理者検証（MAV）が有効になっているクラスタで保護された操作またはコマンドを開始すると、ONTAP は自動的に操作を代行受信し、要求を生成するよう要求します。この要求は、MAV承認グループ（MAV管理者）の1人以上の管理者によって承認される必要があります。または、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、または要求や有効期限を超えた場合は、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設定に対応しています。つまり、管理者ロールには、MAV設定に関係なく、保護された操作を実行するための十分な権限が必要です。 "RBACの詳細については、こちらをご覧ください"。

MAV管理者の場合、保護された操作を実行する要求もMAV管理者によって承認される必要があります。

System Manager の手順の略

ユーザーがメニュー項目をクリックして操作を開始し、操作が保護されると、承認要求が生成され、次のような通知がユーザーに送信されます。

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

[*Multi-Admin Requests]ウィンドウは、MAVが有効な場合に使用できます。このウィンドウには、ユーザのログインIDとMAVロール（承認者または未承認）に基づいて保留中のリクエストが表示されます。保留中の要求ごとに、次のフィールドが表示されます。

- 操作
- インデックス（数値）
- ステータス（［保留中］、［承認済み］、［却下済み］、［実行済み］、または［期限切れ］）

  リクエストが1人の承認者によって却下された場合、それ以上のアクションは実行できません。

- query（要求された処理のパラメータまたは値）
- ユーザーを要求しています
- 要求の有効期限はです
- （の数）保留中の承認者
- （数）承認者の候補

要求が承認されると、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操作を再試行すると、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 手順の略

1. 保護された操作を直接入力するか、MAV requestコマンドを使用します。

   例–ボリュームを削除するには、次のいずれかのコマンドを入力します。

   - `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. リクエストのステータスを確認し、MAV通知に応答します。

   a. 要求が承認されたら、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、または有効期限が過ぎた場合は、要求を削除し、再送信するか、MAV管理者に連絡してください。

   - 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".
```

保護された操作要求を管理します

MAV承認グループ（MAV管理者）の管理者に保留中の操作実行要求が通知された場合、一定の期間（承認期限）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、リクエスト者はリクエストを削除して、別のリクエストを作成する必要があります。

このタスクについて

承認リクエストはインデックス番号で識別されます。インデックス番号は電子メールメッセージに含まれ、リクエストキューの表示にも含まれます。

要求キューからは、次の情報を表示できます。

操作

要求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。

状態

リクエストの現在の状態（保留中、承認済み、却下済み、期限切れ） 実行済み。リクエストが1人の承認者によって却下された場合、それ以上のアクションは実行できません。

必須の承認者

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

保留中の承認者

リクエストを承認済みとしてマークす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。許可されたユーザーは、操作ルールの承認期限を設定できます。承認期限がルールに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

要求元の管理者が処理を完了する必要のある期間。許可された任意のユーザーは、操作ルールの実行有効期限を設定できます。実行有効期限がルールに設定されていない場合は、グローバル設定の実行有効期限が適用されます。

ユーザーが承認しました

リクエストを承認したMAV管理者。

ユーザが拒否しました

リクエストを拒否したMAV管理者。

Storage VM（SVM）

要求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。

ユーザが要求しました

要求を作成したユーザのユーザ名。

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（ **Comment** ）

リクエストに関連付けられているコメント。

ユーザが許可されました

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。状況 `users-permitted` が空の場合、適切な権限を持つすべてのユーザが処理を実行できます。

期限切れの要求または実行された要求は、制限が1000件に達したとき、または期限切れの要求が8時間を超えたときにすべて削除されます。拒否された要求は、期限切れとしてマークされると削除されます。

System Manager の手順の略

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却下するためのリンクが記載された電子メールメッセージを受信します。承認ダイアログにアクセスするには、Eメール内のリンクをクリックするか、System Managerで* Events & Jobs > Requests *（イベントとジョブ>要求）に移動します。

[*Requests]ウィンドウは、マルチ管理者検証がイネーブルの場合に使用でき、ユーザのログインIDおよびMAVロール（アプルーバまたはそれ以外）に基づいて保留中の要求が表示されます。

- 操作
- インデックス（数値）
- ステータス（［保留中］、［承認済み］、［却下済み］、［実行済み］、または［期限切れ］）

  リクエストが1人の承認者によって却下された場合、それ以上のアクションは実行できません。

- query（要求された処理のパラメータまたは値）
- ユーザーを要求しています
- 要求の有効期限はです
- （の数）保留中の承認者
- （数）承認者の候補

MAV管理者は、この画面に追加のコントロールを設定できます。管理者は、個々の操作または操作の選択したグループを承認、拒否、または削除できます。ただし、MAV管理者が要求元ユーザである場合は、独自の要求を承認、拒否、または削除することはできません。

CLI 手順の略

1. 保留中のリクエストが電子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メモします。インデックス番号は、以下の* 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。

実行する処理	入力するコマンド
リクエストを承認します	`security multi-admin-verify request approve nn`
要求を拒否します	`security multi-admin-verify request veto nn`
すべての要求、保留中の要求、または単一の要求を表示します	`security multi-admin-verify request { show

実行する処理	入力するコマンド
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  キュー内のすべての要求を表示することも、保留中の要求だけを表示することもできます。インデックス番号を入力すると、その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を表示するには、を使用します `-fields` パラメータ）またはすべてのフィールドについて（を使用 `-instance` パラメータ）。
リクエストを削除します	`security multi-admin-verify request delete` *`nn`*

例

次のシーケンスでは、MAV管理者がインデックス番号3のリクエストメールを受信した後、リクエストが承認されます。これはすでに1つの承認を持っています。

```
          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

次のシーケンスは、MAV管理者がインデックス番号3の要求メールを受信した後、すでに1つの承認がある要求を拒否します。

```
      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: -
```

OAuth 2.0を使用した認証と許可

ONTAP OAuth 2.0実装の概要

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できます。この機能は、ONTAP CLI、System Manager、REST APIなど、ONTAP管理インターフェイスを使用して設定できます。ただし、OAuth 2.0の承認とアクセス制御の決定は、クライアントがREST APIを使用してONTAPにアクセスする場合にのみ適用できます。

> OAuth 2.0のサポートはONTAP 9.14.0で初めて導入されたため、使用しているONTAPリリースに依存します。を参照してください "ONTAP リリースノート" を参照してください。

機能とメリット

ONTAPでOAuth 2.0を使用する主な機能と利点を以下に説明します。

OAuth 2.0標準のサポート

OAuth 2.0は業界標準の認可フレームワークです。署名付きアクセストークンを使用して、保護されたリソースへのアクセスを制限および制御するために使用されます。OAuth 2.0を使用すると、次のような利点があります。

- 認証設定の多くのオプション
- パスワードを含むクライアントのクレデンシャルは絶対に公開しない
- トークンは構成に基づいて有効期限が切れるように設定できます
- REST APIでの使用に最適

いくつかの一般的な承認サーバーでテスト済み

ONTAPの実装は、OAuth 2.0準拠の認可サーバーと互換性があるように設計されています。次の一般的なサーバまたはサービスでテスト済みです。

- Auth0
- Active Directoryフェデレーションサービス（ADFS）
- キークローク

複数の同時認証サーバのサポート

1つのONTAPクラスタに対して最大8つ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に柔軟に対応できます。

RESTロールトノトウゴウ

ONTAP認証の決定は、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またはLDAPグループとともにローカルONTAP定義に基づいて伝送されます。

送信者に制約されたアクセストークンを使用するオプション

クライアント認証を強化するMutual Transport Layer Security（MTLS）を使用するようにONTAPおよび認可サーバを設定できます。これにより、OAuth 2.0アクセストークンが最初に発行されたクライアントによってのみ使用されることが保証されます。この機能は、FAPIやMITERによって確立されたものを含む、いくつかの一般的なセキュリティ推奨事項をサポートし、それらと一致しています。

実装と構成

大まかに言えば、OAuth 2.0の実装と構成にはいくつかの側面があり、開始時に考慮する必要があります。

ONTAP内のOAuth 2.0エンティティ

OAuth 2.0認証フレームワークは、データセンターまたはネットワーク内の実際の要素または仮想要素にマッピングできる複数のエンティティを定義します。OAuth 2.0エンティティとそのONTAPへの適応を以下の表に示します。

OAuth 2.0エンティティ	説明
リソース	内部ONTAPコマンドを使用して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。
リソース所有者	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。
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）。
クライアント	リソース所有者に代わって、または権限を持って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。
許可サーバ	通常、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。

コア**ONTAP**構成

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、認可サーバへの接続の確立と、必要なONTAP認可設定の定義が含まれます。この設定は、次のいずれかの管理インターフェイスを使用して実行できます。

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

環境およびサポートサービス

ONTAP定義に加えて、認可サーバも設定する必要があります。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グループまたはLDAPに相当するものも設定する必要があります。

サポートされる**ONTAP**クライアント

ONTAP 9.14以降では、REST APIクライアントからOAuth 2.0を使用してONTAPにアクセスできます。REST API呼び出しを実行する前に、認証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。次に、クライアントは、HTTP認証要求ヘッダーを使用して、このトークンを_bearer token_としてONTAPクラスタに渡します。必要なセキュリティのレベルに応じて、クライアントで証明書を作成してインストールし、MTLSに基づいて送信者に制約されたトークンを使用することもできます。

選択した用語

ONTAPを使用したOAuth 2.0デプロイメントの検討を開始する際には、いくつかの用語について理解しておくと役立ちます。を参照してください "その他のリソース" OAuth 2.0に関する詳細情報へのリンクについては、を参照してください。

アクセストークン

認証サーバーによって発行され、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。

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。JSONは、OAuth 2.0の要求を3つの主要セクションに配置したコンパクトな形式で表現するために使用されます。

送信者に制約されたアクセストークン

Mutual Transport Layer Security（MTLS）プロトコルに基づくオプションの機能。トークンで追加の確認要求を使用することで、アクセストークンが最初に発行されたクライアントによってのみ使用されるようになります。

JSON Webキーセット

JWKSは、ONTAPが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使用する公開鍵の集まりです。キーセットは、通常、認証サーバで専用のURIを使用して使用できます。

適用範囲

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を提供します。これらは、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

RESTロールはONTAP 9.6で導入され、ONTAP RBACフレームワークの中核をなす機能です。これらのロールは、ONTAPで引き続きサポートされている以前の従来のロールとは異なります。ONTAPのOAuth 2.0実装では、RESTロールのみがサポートされています。

HTTP認証ヘッダー

REST API呼び出しの一部としてクライアントと関連する権限を識別するためのHTTP要求に含まれるヘッダー。認証と認可の実行方法に応じて、いくつかの種類または実装があります。OAuth 2.0アクセストークンをONTAPに提示する場合、トークンは_bearer token_として識別されます。

HTTPベーシック認証

初期のHTTP認証技術はまだ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。文字列は認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で、金融業界向けにプロトコル、データスキーマ、およびセキュリティに関する推奨事項を提供しています。このAPIは元 々 Financial Grade APIとして知られていた。

マイター

米国空軍と米国政府に技術的および安全保障上のガイダンスを提供する民間の非営利企業。

その他のリソース

いくつかの追加リソースを以下に示します。OAuth 2.0と関連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トークン（JWT）"
- "RFC 7523: OAuth 2.0クライアントの認証と承認のためのJSON Webトークン（JWT）プロファイル"
- "RFC 7662：『OAuth 2.0 Token Introspection』"
- "RFC 7800：『Proof-of-Possession Key for JWT』"
- "RFC 8705：『OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens』"

組織

- "OpenID基盤"
- "FAPIワーキンググループ"
- "マイター"
- "IANA-JWT"

製品とサービス

- "Auth0"
- "ADFSの概要"
- "キークローク"

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の自動化" ドキュメント

概念

認証サーバとアクセストークン

認可サーバーは、OAuth 2.0 Authorizationフレームワーク内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実行します。

OAuth 2.0認可サーバ

認証サーバは、主にアクセストークンの作成と署名を行います。これらのトークンには、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できるように、IDおよび承認情報が含まれています。これらのサーバは通常、相互に分離されており、スタンドアロンの専用サーバとして、またはより大きなIDおよびアクセス管理製品の一部として、いくつかの異なる方法で実装できます。

> OAuth 2.0の機能がより大きなIDおよびアクセス管理製品または解決策内にパッケージ化されている場合は特に、認可サーバーに異なる用語が使用されることがあります。たとえば、*アイデンティティプロバイダ（IdP）*という用語は、*認証サーバ*と同じ意味でよく使用されます。

管理

アクセストークンの発行に加えて、認可サーバーは一般的にWebユーザーインターフェイスを介して関連する管理サービスも提供します。たとえば、次の項目を定義および管理できます。

- ユーザおよびユーザ認証
- スコープ
- テナントとレルムによる管理の分離
- 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標準に準拠した認可サーバーと互換性があります。

ONTAPニテイキ

1つ以上の認可サーバをONTAPに定義する必要があります。ONTAPは、各サーバとセキュアに通信してトークンを検証し、クライアントアプリケーションをサポートするその他の関連タスクを実行します。

ONTAP構成の主な側面を以下に示します。も参照してください "OAuth 2.0の導入シナリオ" を参照してください。

アクセストークンの検証方法と検証場所

アクセストークンを検証するには、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認可サーバー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。認証サーバから取得された情報は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、認証サーバー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認可サーバーに問い合わせることを可能にするプロトコルです。ONTAPは、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方法を提供します。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。

ネットワークの場所

ONTAPはファイアウォールの背後にある可能性があります。この場合は、設定の一部としてプロキシを指定する必要があります。

許可サーバの定義方法

ONTAPに対する認証サーバは、CLI、System Manager、REST APIなどの任意の管理インターフェイスを使用して定義できます。たとえば、CLIでは次のコマンドを使用します。 `security oauth2 client create`。

認証サーバの数

1つのONTAPクラスタに対して最大8つの許可サーバを定義できます。発行者または発行者/オーディエンスの要求が一意である限り、同じ認証サーバを同じONTAPクラスタに複数回定義できます。たとえば、Keycloakでは、異なるレルムを使用する場合は常にこのようになります。

OAuth 2.0アクセストークンの使用

認証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アクセスの決定に使用されます。

アクセストークンの取得

REST APIを使用するONTAPクラスタに定義されている認証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。トークンを取得するには、認可サーバーに直接問い合わせる必要があります。

> ONTAPは、問題アクセストークンを使用したり、クライアントからの要求を認可サーバにリダイレクトしたりすることはありません。

トークンの要求方法は、次のようないくつかの要因によって異なります。

- 認可サーバとその設定オプション
- OAuth 2.0認可タイプ
- 要求の問題に使用するクライアントまたはソフトウェアツール

付与タイプ

a_grant_は、OAuth 2.0アクセストークンの要求と受信に使用される、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、およびセキュリティの要件に応じて、いくつかの異なる権限付与タイプを使用できます。一般的な付与タイプの一覧を以下の表に示します。

許可タイプ	説明
クライアントクレデンシャル	クレデンシャル（IDや共有シークレットなど）のみを使用する一般的な付与タイプ。クライアントは、リソース所有者と密接な信頼関係を持っていると想定されます。
パスワード	リソース所有者パスワード資格情報付与タイプは、リソース所有者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ます。また、レガシーHTTPクライアントをOAuth 2.0に移行する場合にも役立ちます。
認証コード	これは機密クライアントにとって理想的な認可タイプであり、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両方を取得するために使用できます。

JWTの内容

OAuth 2.0アクセストークンはJWT形式です。コンテンツは、設定に基づいて認可サーバによって作成されます。ただし、トークンはクライアントアプリケーションには不透明です。クライアントには、トークンを検査したり、コンテンツを認識したりする理由はありません。

各JWTアクセストークンには、クレームのセットが含まれています。クレームは、発行者の特性と認可サーバーでの管理定義に基づいた認可を記述します。この規格に登録されている請求の一部は、次の表に記載されています。すべての文字列で大文字と小文字が区別されます。

請求	キーワード	説明
発行者	ISS	トークンを発行したプリンシパルを識別します。請求処理はアプリケーション固有です。
件名	サブ	トークンのサブジェクトまたはユーザ。名前のスコープは、グローバルまたはローカルで一意になります。
対象者	豪ドル	トークンの対象となる受信者。文字列の配列として実装されます。

請求	キーワード	説明
有効期限	有効期限	トークンが期限切れになり、拒否されるまでの時間。

を参照してください "RFC 7519：JSON Webトークン" を参照してください。

ONTAPクライアント許可のオプション

ONTAPクライアント許可をカスタマイズするには、いくつかのオプションを使用できます。承認の決定は、最終的には、アクセストークンに含まれるか、アクセストークンから派生したONTAP RESTロールに基づいて行われます。

> 使用できるのは "ONTAP RESTロール" OAuth 2.0の認可を設定する場合。以前のONTAPの従来のロールはサポートされていません。

はじめに

ONTAP内のOAuth 2.0の実装は、柔軟性と堅牢性を考慮して設計されており、ONTAP環境を保護するために必要なオプションを提供します。大まかには、ONTAPクライアント許可を定義するための3つの主要な設定カテゴリがあります。これらの設定オプションを同時に指定することはできません。

ONTAPでは、構成に応じて最適な1つのオプションが適用されます。を参照してください "ONTAPニヨルアクセスノケツテイホウホウ" を参照して、アクセスを決定するためにONTAPで構成定義をどのように処理するかを確認してください。

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1つの文字列にカプセル化されています。ONTAPロールの定義には依存しません。認可サーバーでこれらのスコープ文字列を定義する必要があります。

ローカルの**ONTAP**固有の**REST**ロールとユーザ

設定に基づいて、ローカルONTAP ID定義を使用してアクセスを決定できます。オプションは次のとおりです。

- 単一のネームドRESTロール
- ユーザ名とローカルONTAPユーザの照合

指定したロールのscope構文は、* ontap-role-*<URL-encoded-ONTAP-role-name>です。たとえば、ロールが「admin」の場合、スコープ文字列は「ontap-role-admin」になります。

Active Directoryまたは**LDAP**グループ

ローカルONTAPの定義を調べても、アクセスを決定できない場合は、Active Directory（「domain」）または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スコープ文字列

  グループメンバーシップを持つユーザがいない場合、クライアントのクレデンシャルフローを使用して機密アプリケーションをサポートします。スコープには* ontap-group-*<URL-encoded-ONTAP-group-name>という名前を付けます。たとえば、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」の主張

  これは、リソース所有者(パスワード付与)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を対象としています。

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。各ロールは完全なカスタムロール定義であり、アクセスを決定するためにONTAPが必要とするすべての機能が含まれています。スコープは、ONTAP内で定義されているRESTロールとは別のものです。

スコープ文字列の形式

基本レベルでは、スコープは連続した文字列として表され、コロンで区切られた6つの値で構成されます。スコープ文字列で使用されるパラメータについては、以下で説明します。

ONTAPリテラル

スコープはリテラル値で始まる必要があります `ontap` 小文字で入力します。これにより、範囲がONTAPに固有であることが識別されます。

クラスタ

スコープ環境となるONTAPクラスタを定義します。次の値を指定できます。

- クラスタUUID

  単一のクラスタを識別します。

- アスタリスク(*)

  スコープ環境のすべてのクラスタを示します。

ONTAP CLIコマンドを使用できます。 `cluster identity show` をクリックしてクラスタのUUIDを表示します。指定しない場合は、スコープ環境all clustersになります。

ロール

自己完結型スコープに含まれるRESTロールの名前。この値は、ONTAPで検証されたり、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とき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示します。次の表に示す6つの値があります。

アクセスレベル	説明
なし	指定したエンドポイントへのすべてのアクセスを拒否します。
- 読み取り専用	GETを使用した読み取りアクセスのみを許可します。

アクセスレベル	説明
READ_CREATE	POSTを使用して、読み取りアクセスと新しいリソースインスタンスの作成を許可します。
READ_MODIFY	読み取りアクセスを許可し、PATCHを使用して既存のリソースを更新する機能を許可します。
READ_CREATE _MODIFY	削除以外のすべてのアクセスを許可します。許可される処理は、GET（読み取り）、POST（作成）、およびPATCH（更新）です。
すべて	フルアクセスを許可します。

SVM

クラスタ内のスコープ環境内のSVMの名前。すべてのSVMを示すために、*（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のパラメータは無視して、プレースホルダにアスタリスクを使用できます。を確認します "ONTAP リリースノート" をクリックしてSVMの今後のサポートを確認してください。

REST API URI

リソースまたは関連リソースのセットへの完全パスまたは部分パス。文字列は次で始まる必要があります：`/api`。値を指定しない場合は、スコープ環境All APIエンドポイントがONTAPクラスタで指定されます。

範囲の例

自己完結型スコープの例を以下に示します。

ONTAP：：joes-role：read_create_modify：：/api/cluster

このロールを割り当てられたユーザに、 `/cluster` エンドポイント。

CLI管理ツール

自己完結型スコープの管理を容易にし、エラーが発生しにくくするために、ONTAPにはCLIコマンドが用意されています。 `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します。

コマンド `security oauth2 scope` 入力内容に基づいて、次の2つのユースケースがあります。

- 文字列をスコープするCLIパラメータ

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

- scope string to CLIパラメータ

  このバージョンのコマンドを使用すると、入力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

次の例では、次のコマンド例のあとに出力が含まれたスコープ文字列を生成します。定義は、すべてのクラスタを環境します。

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

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

ONTAPニヨルアクセスノケツテイホウホウ

OAuth 2.0を適切に設計および実装するには、ONTAPが許可設定を使用してクライアントのアクセスを決定する方法を理解する必要があります。

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、ステップ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*決定が行われるまで、各スコープを適用します。明示的な決定が行われた場合、処理は終了します。

ONTAPが明示的にアクセスを決定できない場合は、手順2に進みます。

手順**2**：ローカルロールフラグを確認する

ONTAPがフラグの値を調べる `use-local-roles-if-present`。このフラグの値は、ONTAPに定義された認可サーバーごとに個別に設定されます。

- の場合 `true` 手順3に進みます。
- の場合 `false` 処理が終了し、アクセスが拒否されます。

手順**3**：名前付き**ONTAP REST**ロール

アクセストークンに名前付き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を決定します。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

名前付き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。

手順**4**：ローカル**ONTAP**ユーザ

アクセストークンからユーザ名を抽出し、ローカルONTAPユーザと照合してみます。

ローカルONTAPユーザが一致した場合、ONTAPはそのユーザ用に定義されたロールを使用してアクセスを決定します。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

ローカルONTAPユーザが一致しない場合、またはアクセストークンにユーザ名がない場合は、手順5に進みます。

手順**5**：グループとロールのマッピング

アクセストークンからグループを抽出し、グループと照合してみます。グループは、Active Directoryまたは同等のLDAPサーバを使用して定義します。

一致するグループがある場合、ONTAPはその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。これにより、常に* allow または deny *の決定が行われ、処理が終了します。

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ない場合、アクセスは拒否され、処理は

終了します。

OAuth 2.0の導入シナリオ

ONTAPに認可サーバーを定義するときに使用できる設定オプションはいくつかあります。これらのオプションに基づいて、展開環境に適した承認サーバーを作成できます。

設定パラメータの概要

ONTAPに認可サーバーを定義する際には、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、一般にすべての管理インターフェイスでサポートされています。

パラメータ名は、ONTAP管理インターフェイスによって多少異なります。たとえば、リモートイントロスペクションを設定する場合、エンドポイントはCLIコマンドパラメータを使用して識別されます。`-introspection-endpoint`。ただし、System Managerでは、同等のフィールドは_Authorizationサーバトークンイントロスペクション URI_です。すべてのONTAP管理インターフェイスに対応するために、パラメータの一般的な概要が用意されています。正確なパラメータまたはフィールドは、コンテキストに基づいて明確にする必要があります。

パラメータ	説明
名前	ONTAPで認識されている認可サーバの名前。
アプリケーション	ONTAP内部アプリケーション定義環境。これは* http *である必要があります。
発行者URI	トークンを発行するサイトまたは組織を識別するパスを持つFQDN。
プロバイダ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。
JWKS更新間隔	ONTAPがプロバイダーJWKS URIから証明書情報を更新する頻度を決定する時間間隔。値はISO-8601形式で指定します。
イントロスペクションエンドポイント	ONTAPがイントロスペクションを通じてリモートトークン検証を実行するために使用するパスを持つFQDN。
クライアント ID	認可サーバで定義されているクライアントの名前。この値が含まれている場合は、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。
発信プロキシ	これは、ONTAPがファイアウォールの背後にある場合に、認可サーバへのアクセスを提供するためです。URIはcurl形式で指定する必要があります。
ローカルロールがある場合は使用	ローカルONTAP定義が使用されているかどうかを判断するブーリアンフラグ（名前付きRESTロールとローカルユーザを含む）。
ユーザ要求の削除	ONTAPがローカルユーザとの照合に使用する別名。を使用します `sub` ローカルユーザ名と一致するアクセストークンのフィールド。

導入シナリオ

いくつかの一般的な導入シナリオを次に示します。これらは、トークン検証がONTAPによってローカルで実行されるか、認証サーバによってリモートで実行されるかに基づいて編成されます。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。を参照してください "ONTAPでのOAuth 2.0の導入" コンフィギュレーションコマンドの例については、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を使用してその設定を表示できます。たとえば、次のコマンドを使用します。 `security oauth2 client show` ONTAP CLIを使用します。

ローカル検証

次の導入シナリオは、ローカルでトークン検証を実行するONTAPに基づいています。

プロキシなしで自己完結型スコープを使用する

これは、OAuth 2.0の自己完結型スコープのみを使用する最も単純な展開です。ローカルONTAP ID定義は使用されません。次のパラメータを指定する必要があります。

- 名前
- アプリケーション（http）
- プロバイダJWKS URI
- 発行者URI

また、認可サーバーでスコープを追加する必要があります。

プロキシで自己完結型スコープを使用する

この展開シナリオでは、OAuth 2.0の自己完結型スコープを使用します。ローカルONTAP ID定義は使用されません。ただし、認可サーバは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。次のパラメータを指定する必要があります。

- 名前
- アプリケーション（http）
- プロバイダJWKS URI
- 発信プロキシ
- 発行者URI
- 対象者

また、認可サーバーでスコープを追加する必要があります。

ローカルユーザロールとデフォルトユーザ名のマッピングをプロキシで使用する

この導入シナリオでは、ローカルユーザロールとデフォルトのネームマッピングを使用します。リモートユーザ要求では、のデフォルト値が使用されます。 `sub` 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一致するために使用されます。ユーザ名は40文字以下にする必要があります。認証サーバは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もあります。次のパラメータを指定する必要があります。

- 名前
- アプリケーション（http）
- プロバイダJWKS URI
- ローカルロールがある場合は使用 (`true`)
- 発信プロキシ

- 発行者

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。

ローカルユーザロールと代替ユーザ名マッピングをプロキシで使用する

この導入シナリオでは、ローカルユーザロールと代替ユーザ名を使用して、ローカルONTAPユーザを照合します。認証サーバはファイアウォールの背後にあるため、プロキシを設定する必要があります。次のパラメータを指定する必要があります。

- 名前
- アプリケーション（http）
- プロバイダJWKS URI
- ローカルロールがある場合は使用 (`true`)
- リモートユーザの要求
- 発信プロキシ
- 発行者URI
- 対象者

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

次の展開構成は、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ONTAPに基づいています。

プロキシなしで自己完結型スコープを使用する

これは、OAuth 2.0の自己完結型スコープを使用したシンプルな展開です。ONTAP ID定義は使用されません。次のパラメータを指定する必要があります。

- 名前
- アプリケーション（http）
- イントロスペクションエンドポイント
- クライアント ID
- 発行者URI

認可サーバーでは、スコープ、およびクライアントシークレットを定義する必要があります。

相互**TLS**を使用したクライアント認証

セキュリティのニーズに応じて、オプションでMutual TLS（MTLS）を設定して強力なクライアント認証を実装できます。OAuth 2.0展開の一部としてONTAPで使用される場合、MTLSはアクセストークンが最初に発行されたクライアントによってのみ使用されることを保証します。

OAuth 2.0を使用した相互TLS

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）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介してクライアントを強力に識別できるようにすることで、これを拡張します。OAuth 2.0を使用したONTAPクラスタで使用する場合、送信者に制約されたアクセストークンを作成して使用することで、基本的なMTLS機能が拡張されます。

送信者に制約されたアクセストークンは、最初に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、新しい確認請求 (`cnf`）がトークンに挿入されます。フィールドにプロパティが含まれています `x5t#S256` アクセストークンを要求するときに使用されるクライアント証明書のダイジェストを保持します。この値は、トークンの検証の一環としてONTAPによって検証されます。送信者に制約されていない許可サーバーによって発行されたアクセストークンには、追加の確認要求は含まれません。

認可サーバごとにMTLSを個別に使用するように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` パラメータを含む `use-mutual-tls` 次の表に示す3つの値に基づいてMTLS処理を制御します。

> 各構成で、ONTAPによって実行される結果とアクションは、構成パラメータの値、およびアクセストークンとクライアント証明書の内容によって異なります。テーブル内のパラメータは、最小から最も制限の厳しいものに分類されています。

パラメータ	説明
なし	OAuth 2.0相互TLS認証は、認可サーバーでは完全に無効になっています。ONTAPは、確認要求がトークンに含まれている場合やクライアント証明書がTLS接続で提供されている場合でも、MTLSクライアント証明書認証を実行しません。
リクエスト	OAuth 2.0相互TLS認証は、送信者に制約されたアクセストークンがクライアントによって提示された場合に適用されます。つまり、MTLSは、確認請求（財産を含む）の場合にのみ適用されます。 `x5t#S256`）がアクセストークンに含まれています。これがデフォルト設定です。
必須	OAuth 2.0相互TLS認証は、認可サーバーによって発行されたすべてのアクセストークンに適用されます。したがって、すべてのアクセストークンは送信者に制約される必要があります。アクセストークンに確認要求がない場合、または無効なクライアント証明書がある場合、認証およびREST API要求は失敗します。

導入フローの概要

ONTAP環境でOAuth 2.0でMTLSを使用する場合の一般的な手順を以下に示します。を参照してください "RFC 8705：『OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens』" 詳細：

手順**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に関する知識の証明に基づいています。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作成手順の概要は次のとおりです。

1. 公開鍵と秘密鍵のペアを生成する
2. 証明書署名要求を作成する
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、署名済み証明書を発行

通常、クライアント証明書はローカルのオペレーティングシステムにインストールするか、curlなどの一般的なユーティリティを使用して直接使用できます。

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

MTLSを使用するようにONTAPを設定する必要があります。この設定は、認可サーバごとに個別に行われます。たとえば、CLIでは次のコマンドを使用します。 `security oauth2 client` は、オプションのパラメータとともに使用されます。 `use-mutual-tls`。を参照してください "ONTAPでのOAuth 2.0の導入" を参照してください。

手順**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に設定された認証サーバから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で作成および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:**認証サーバーがアクセストークンを生成する

認可サーバはクライアント要求を検証し、アクセストークンを生成します。この一部として、クライアント証明書のメッセージダイジェストが作成されます。このダイジェストは、トークンに確認要求として含まれます（フィールド `cnf`）。

手順**5**：クライアントアプリケーションが**ONTAP**にアクセストークンを提示する

クライアントアプリケーションは、ONTAPクラスタへのREST API呼び出しを実行し、アクセストークンを* bearerトークン*として承認要求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要求に使用したのと同じ証明書を持つMTLSを使用する必要があります。

ステップ**6: ONTAP**はクライアントとトークンを検証します。

ONTAPは、HTTP要求で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信します。ONTAPは最初にアクセストークン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、トークン内の確認要求* cnf*と比較します。2つの値が一致する場合、ONTAPは、API要求を行う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ました。

構成と導入

ONTAPを使用した**OAuth 2.0**の導入準備

ONTAP環境でOAuth 2.0を構成する前に、展開の準備をする必要があります。主なタスクと決定事項の概要を以下に示します。セクションの配置は、通常、従うべき順序に沿って配置されます。ただし、ほとんどの環境に適用できますが、必要に応じて環境に適応する必要があります。また、正式な導入計画の作成も検討する必要があります。

> 環境に応じて、ONTAPに定義されている認証サーバの設定を選択できます。これには、導入のタイプごとに指定する必要があるパラメータ値も含まれます。を参照してください "OAuth 2.0の導入シナリオ" を参照してください。

リソースとクライアントアプリケーションを保護

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承認フレームワークです。このため、導入

の最初の重要なステップは、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です。

クライアントアプリケーションを特定する

REST API呼び出しを発行するときにOAuth 2.0を使用するクライアントと、アクセスが必要な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決定できます。

OAuth 2.0へのグローバルな移行

OAuth 2.0認証を段階的に実装することもできますが、各認証サーバー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OAuth 2.0にすぐに移動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することなく、既存のONTAP構成に基づいてアクセスを決定できます。

認証サーバ

認証サーバーは、アクセストークンを発行し、管理ポリシーを適用することで、OAuth 2.0の展開において重要な役割を果たします。

認可サーバーを選択してインストールします。

1つ以上の認可サーバーを選択して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することが重要です。

認証ルート**CA**証明書をインストールする必要があるかどうかを判断する

ONTAPでは、認証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。これを行うには、ONTAPにルートCA証明書と中間証明書が必要です。ONTAPがプリインストールされている場合があります。そうでない場合は、インストールする必要があります。

ネットワークの場所と構成の評価

認証サーバがファイアウォールの背後にある場合は、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。

クライアントの認証と許可

クライアントの認証と許可には、いくつかの側面を考慮する必要があります。

自己完結型スコープまたはローカル**ONTAP ID**定義

大まかに言えば、認可サーバーで定義された自己完結型スコープを定義することも、役割やユーザーを含む既存のローカルONTAP ID定義に依存することもできます。

ローカル**ONTAP**処理を使用するオプション

ONTAP ID定義を使用する場合は、適用するものを次のように決定する必要があります。

- ネームドRESTロール
- ローカルユーザの一致
- Active DirectoryまたはLDAPグループ

ローカル検証または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認可サーバー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も考慮する必要があります。

送信者に制約されたアクセストークン

高度なセキュリティが必要な環境では、MTLSに基づいて送信制限付きアクセストークンを使用できます。これには、クライアントごとに証明書が必要です。

管理インターフェイス

OAuth 2.0の管理は、次のいずれかのONTAPインターフェイスを使用して実行できます。

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

クライアントニヨルアクセストークンノヨウキュウホウホウ

クライアントアプリケーションは、許可サーバからアクセストークンを直接要求する必要があります。許可の種類を含め、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の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を定義する

認証設定に基づいて、ローカルのONTAP識別処理を使用できます。この場合は、RESTロールとユーザ定義を確認して定義する必要があります。

コア構成

コアONTAP構成の実行には、主に次の3つの手順が必要です。

- 必要に応じて、認証サーバの証明書に署名したCAのルート証明書（および中間証明書）をインストールします。
- 認可サーバを定義します。
- クラスタに対してOAuth 2.0の処理を有効にします。

ONTAPでのOAuth 2.0の導入

OAuth 2.0のコア機能の展開には、主に3つのステップがあります。

作業を開始する前に

ONTAPを設定する前に、OAuth 2.0の展開を準備する必要があります。たとえば、証明書がどのように署名されたか、ファイアウォールの内側にあるかなど、承認サーバーを評価する必要があります。を参照してください "ONTAPを使用したOAuth 2.0の導入準備" を参照してください。

手順**1**：認証サーバ証明書をインストールする

ONTAPには、多数のルート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、認証サーバの証明書は追加の設定なしで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。

必要に応じて、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基づいて、正しい手順を選択します。

例 **1.** 手順

System Manager の略

1. System Managerで、**[**クラスタ**]>***[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. の横にある→*をクリックします。
4. タブで[追加]*をクリックします。
5. [インポート]*をクリックし、証明書ファイルを選択します。
6. 環境に合わせて設定パラメータを設定します。
7. [追加（ Add ）] をクリックします。

CLI の使用

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確認します。

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

3. 証明書ファイルをテキストエディタで開きます。
4. 次の行を含む証明書全体をコピーします。

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

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

5. コマンドプロンプトの後に証明書を端末に貼り付けます。
6. Enter*キー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ていることを確認します。

   ```
   security certificate show-user-installed

   security certificate show
   ```

手順**2**：認証サーバを設定する

ONTAPに対する認可サーバーを少なくとも1つ定義する必要があります。設定と導入計画に基づいてパラメータ値を選択する必要があります。レビュー "OAuth2導入シナリオ" をクリックして、構成に必要な正確なパラ

メータを決定します。

認可サーバー定義を変更するには、既存の定義を削除して新しい定義を作成します。

次の例は、最初のシンプルな導入シナリオに基づいています。 "ローカル検証"。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基づいて、正しい手順を選択します。CLI手順では、コマンドを実行する前に置き換える必要があるシンボリック変数を使用します。

例 **2.** 手順

System Manager の略

1. System Managerで、**[**クラスタ**]>***[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. 導入に必要な値を次のように指定します。
   - 名前
   - アプリケーション（http）
   - プロバイダJWKS URI
   - 発行者URI
6. [追加（ Add ）] をクリックします。

CLI の使用

1. 定義を再作成します。

```
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
```

手順**3**：**OAuth 2.0**を有効にする

最後のステップは、OAuth 2.0を有効にすることです。これはONTAPクラスタのグローバル設定です。

> ONTAP、認可サーバー、および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するまで、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基づいて、正しい手順を選択します。

例 **3.** 手順

System Manager の略

1. System Managerで、**[**クラスタ**]>***[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. * OAuth 2.0認証*を有効にします。

CLI の使用

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
   ```

OAuth 2.0を使用した**REST API**呼び出しの問題

ONTAPのOAuth 2.0実装では、REST APIクライアントアプリケーションがサポートされています。curlを使用して簡単なREST API呼び出しを問題し、OAuth 2.0の使用を開始できます。次の例は、ONTAPクラスタのバージョンを取得します。

作業を開始する前に

ONTAPクラスタに対してOAuth 2.0機能を設定して有効にする必要があります。これには、認可サーバー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。トークン要求はONTAPの外部で実行され、正確な手順は認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使用してトークンを要求できます。

説明のために、curlを使用してKeycloakからアクセストークンを要求する方法の例を以下に示します。

キークロークの例

```
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'
```

返されたトークンをコピーして保存する必要があります。

手順2：REST API呼び出しを問題する

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呼び出しを問題できます。

パラメータと変数

curlの例の2つの変数について、次の表で説明します。

変数（**Variable**）	説明
$FQDN_IP	ONTAP管理LIFの完全修飾ドメイン名またはIPアドレス。
$access_token	認可サーバーによって発行されたOAuth 2.0アクセストークン。

curlの例を発行する前に、まず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
```

両方の変数をローカルのBashシェルで定義したら、curlコマンドをコピーしてCLIに貼り付けることができます。Enter *を押して変数を置き換え、コマンドを問題します。

カールの例

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

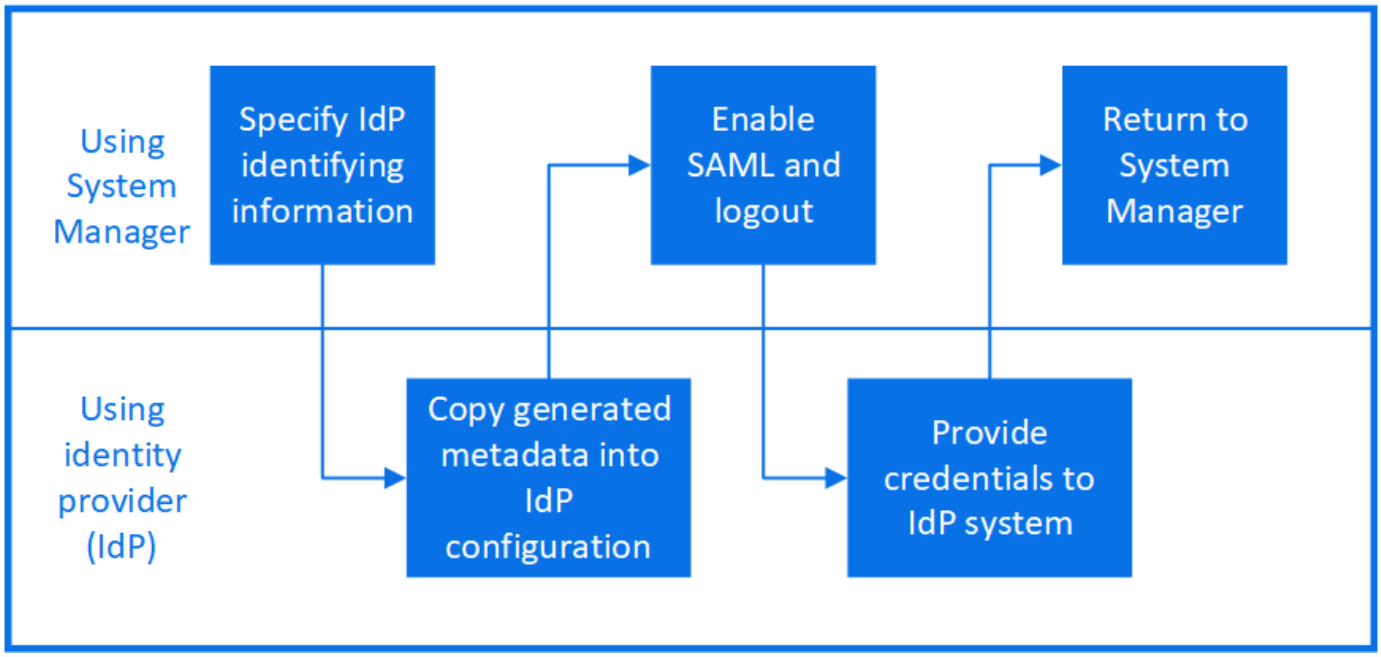
SAML 認証を設定する

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 認証を有効にする

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。ご使用の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、System ManagerのGUIにアクセスできるのはリモートユーザだけになります。ローカルユーザは、 SAML 認証を有効にしたあとで System Manager GUI にアクセスできません。



作業を開始する前に

- リモート認証に使用する IdP を設定する必要があります。

  > 設定済みの IdP から提供されたドキュメントを参照してください。

- IdP の URI が必要です。

このタスクについて

- SAML認証は、にのみ適用されます `http` および `ontapi` アプリケーション：

  。 `http` および `ontapi` アプリケーションは、サービスプロセッサインフラ、ONTAP API、またはSystem ManagerのWebサービスで使用されます。

- SAML 認証は、管理 SVM へのアクセス時にのみ適用できます。

次のIdPがSystem Managerで検証されました。

- 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のクラシックドキュメント"）
  - 9.8P17以降の9.8リリース
  - 9.9.1P13以降の9.9リリース
  - 9.10.1P9以降の9.10リリース
  - 9.11.1P4以降の9.11リリース
  - 9.12.1以降のリリース
- Shibboleth

環境に応じて、次の手順を実行します。

例 **4.** 手順

System Manager の略

1. **[Cluster] > [Settings]** の順にクリックします。
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 （を含む）を入力します "https://"）。
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。
6. 正しい証明書が使用されていることを確認します。
   - タイプが「 server 」の証明書が 1 つだけシステムにマッピングされている場合、その証明書はデフォルトとみなされ、表示されません。
   - システムが「 server 」タイプの複数の証明書にマッピングされている場合は、いずれかの証明書が表示されます。 別の証明書を選択するには、 * Change * をクリックします。
7. [保存（ Save ）] をクリックします。確認ウィンドウには、自動的にクリップボードにコピーされたメタデータ情報が表示されます。
8. 指定した IdP システムに移動し、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。
9. 確認ウィンドウ（ System Manager ）に戻り、チェックボックスをオンにします。 * ホスト URI またはメタデータで IdP を設定しました。 *
10. Logout * をクリックして、 SAML ベースの認証を有効にします。 IdP システムに認証画面が表示されます。
11. IdP システムで、 SAML ベースのクレデンシャルを入力します。クレデンシャルを確認すると、 System Manager のホームページが表示されます。

CLI の使用

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メタデータのダウンロード元のIdPホストのFTPアドレスまたはHTTPアドレスです。

   `ontap_host_name` は、SAMLサービスプロバイダホスト（ここでは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 Data 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 Data 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 ホストメタデータを使用して IdP を設定します。

   IdP の設定の詳細については、 IdP のマニュアルを参照してください。

3. SAML の設定を有効にします。

   security saml-sp modify -is-enabled true

   にアクセスする既存のユーザ `http` または `ontapi` アプリケーションでSAML認証が自動的に設定されます。

4. のユーザを作成する場合 `http` または `ontapi` アプリケーションSAMLの設定後、新しいユーザの認証方式としてSAMLを指定します。

   a. SAML認証を使用する新しいユーザのログイン方法を作成します。
      [+]
      security login create -user-or-group-name *user_name* -application [http | ontapi] -authentication-method saml -vserver *svm_name*

      ```
      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

```
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**
```

SAML 認証を無効にする

外部のアイデンティティプロバイダ（ IdP ）を使用して Web ユーザの認証を停止する場合は、 SAML 認証を無効にすることができます。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。

環境に応じて、次の手順を実行します。

例 **5.** 手順

System Manager の略

1. [**Cluster] > [Settings**] の順にクリックします。
2. [* SAML Authentication* （ SAML 認証）] で、 [* Enabled * （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 [SAML 認証を有効にする *] チェックボックスをオフにします

CLI の使用

1. SAML 認証を無効にする

   ```
   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
   ```

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。修復プロセスの実行中は、 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。

このタスクについて

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
   ```

```
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.
```

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*

```
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。

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

```
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.
```

関連情報

"ONTAP 9コマンド"

Web サービスを管理します

Manage Web Services の概要

クラスタまたは Storage Virtual Machine （ SVM ）の Web サービスを有効または無効にしたり、 Web サービスの設定を表示したり、ロールのユーザが Web サービスにアクセスできるかどうかを管理したりできます。

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 サービスを有効または無効にします
- Web サービスへのアクセスを暗号化された HTTP （ SSL ）のみに制限するかどうかを指定する
- Web サービスの可用性を表示します
- あるロールのユーザに Web サービスへのアクセスを許可するかどうか
- 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 Web サービスにアクセスするには、次の条件をすべて満たしている必要があります。

- ユーザが認証されている必要があります。

  たとえば、 Web サービスからユーザ名とパスワードの入力を求められる場合があります。ユーザの応答は有効なアカウントと一致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。

  指定された Web サービスの正しいアクセス方法が設定されたユーザのみが正常に認証されます。ONTAP API Webサービス用 `ontapi`）を使用する場合は、を使用する必要があります `ontapi` アクセス方法。その他のすべてのWebサービスの場合は、が必要です `http` アクセス方法。

  > を使用します `security login` ユーザのアクセス方法と認証方法を管理するコマンド。

- 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必要があります。

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

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 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。

Web サービスへのアクセスを管理します

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 (`spi`)

  このサービスによって、ノードのログファイル、コアダンプファイル、および MIB ファイルに、クラスタ管理 LIF またはノード管理 LIF から HTTP または HTTPS でアクセスできるようになります。デフォルト設定はです `enabled`。

  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発生すると、が表示されます `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`)

  このサービスでは、 ONTAP API を実行し、リモートプログラムで管理機能を実行できます。デフォルト設定はです `enabled`。

  一部の外部管理ツールではこのサービスが必要になる場合があります。たとえば、 System Manager を使用する場合、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`)

  このサービスは、外部の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します。デフォルト設定はです `enabled`。

- Support Diagnostics（診断）の略 (`supdiag`)

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

- System Manager の略 (`sysmgr`)

  このサービスは、 ONTAP に組み込まれている System Manager の可用性を管理します。デフォルト設定はです `enabled`。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）の更新 (`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。デフォルト設定はです `enabled`。

- ONTAP のドキュメント (`docs`)

  このサービスでは、 ONTAP のドキュメントにアクセスできます。デフォルト設定はです `enabled`。

- ONTAP RESTful API (`docs_api`)

  このサービスを使用すると、 ONTAP RESTful API のドキュメントにアクセスできます。デフォルト設定はです `enabled`。

- ファイルのアップロードとダウンロード (`fud`)

  このサービスは、ファイルのアップロードとダウンロードを提供します。デフォルト設定はです `enabled`。

- ONTAP メッセージング (`ontapmsg`)

  このサービスでは、イベントをサブスクライブできるパブリッシュおよびサブスクライブインターフェイスがサポートされています。デフォルト設定はです `enabled`。

- 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に実装します。デフォルト設定はです `enabled`。

- ONTAP RESTfulインターフェイス (`rest`)

  このサービスは、クラスタインフラのすべての要素をリモートで管理するために使用する RESTful インターフェイスをサポートします。デフォルト設定はです `enabled`。

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

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

- SAMLサービスプロバイダ (`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。デフォルト設定はです `enabled`。

ONTAP 9.7 以降では、次の追加サービスがサポートされます。

- 設定バックアップファイル (`backups`)

  このサービスでは、構成バックアップファイルをダウンロードできます。デフォルト設定はです `enabled`。

- ONTAPのセキュリティ (`security`)

  このサービスでは、 CSRF トークン管理をサポートして認証を強化しています。デフォルト設定はです `enabled`。

Web プロトコルエンジンを管理します

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。Web プロトコルエンジンの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。

- を使用して、リモートクライアントがHTTPまたはHTTPSを使用してWebサービスコンテンツにアクセスできるかどうかを指定できます `system services web modify` コマンドにを指定します `-external` パラメータ
- を使用して、セキュアなWebアクセスにSSLv3を使用するかどうかを指定できます `security config modify` コマンドにを指定します `-supported-protocol` パラメータ
  デフォルトでは、 SSLv3 は無効になっています。Transport Layer Security 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。
- 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に対して、 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 準拠モードが無効な場合 *
    FIPS 140-2準拠モードを有効にするには、 `is-fips-enabled` パラメータの値 `true` をクリックします `security config modify` コマンドを実行し、を使用します `security config show` コマンドを使用してオンラインステータスを確認します。
  - * FIPS 140-2 準拠モードが有効な場合 *
    - ONTAP 9.11.1以降では、TLSv1、TLSv1.1、およびSSLv3は無効になり、TSLv1.2とTSLv1.3のみが有効なままになります。ONTAP 9の内部および外部にある他のシステムや通信に影響します。FIPS 140-2準拠モードを有効にし、その後無効にした場合、TLSv1、TLSv1.1、およびSSLv3は無効のままになります。TLSV.1またはTLSv1 1.3は、前の設定に応じて有効のままになります。
    - 9.11.1より前のバージョンのONTAP では、TLSv1とSSLv3は無効になり、TLSv1.1とTLSv1.2のみが引き続き有効になります。ONTAP では、 FIPS 140-2 準拠モードが有効な場合、 TLSv1 と SSLv3 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、その後無効にした場合、 TLSv1 と SSLv3 は無効なままですが、以前の設定によっては、 TLSv1.2 または TLSv1.1 と

TLSv1.2 の両方が有効になります。

- 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 `system security config show` コマンドを実行します

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コマンド

を使用します `system services web` Webプロトコルエンジンを管理するコマンド。を使用します `system services firewall policy create` および `network interface modify` 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するコマンド。

状況	使用するコマンド
クラスタレベルで Web プロトコルエンジンを設定します。 • クラスタの Web プロトコルエンジンを有効または無効にします • クラスタの SSLv3 を有効または無効にします • セキュアな Web サービス（ HTTPS ）に対する FIPS 140-2 準拠を有効または無効にする	`system services web modify`
クラスタレベルの Web プロトコルエンジンの設定を表示し、 Web プロトコルがクラスタ全体で機能しているかどうかを確認し、 FIPS 140-2 準拠が有効でオンラインになっているかどうかを表示します	`system services web show`
ノードレベルの Web プロトコルエンジンの設定と、クラスタ内のノードに対する 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` を設定します `-service` パラメータの値 `http` または `https` 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
ファイアウォールポリシーを LIF と関連付ける	`network interface modify` を使用できます `-firewall-policy` LIFのファイアウォールポリシーを変更するためのパラメータ。

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ことで、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 ）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 サービスで使用される LIF のファイアウォールポリシーで HTTP または HTTPS のアクセスがセットアップされていることを確認してください。

   ファイアウォールが有効になっているかどうかは、を使用して確認できます `system services firewall show` コマンドを実行します

   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、を使用します `system services firewall policy show` コマンドを実行します

      を設定します `-service` のパラメータ `system services firewall policy create` コマンドをに送信します `http` または `https` ポリシーで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をサポートしてい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、を使用します `network interface show` コマンドにを指定します `-firewall-policy` パラメータ

      を使用します `network interface modify` コマンドにを指定します `-firewall-policy` LIFに対してファイアウォールポリシーを有効にするためのパラメータ。

2. クラスタレベルのWebプロトコルエンジンを設定してWebサービスのコンテンツにアクセスできるようにするには、を使用します `system services web modify` コマンドを実行します
3. セキュアなWebサービス（HTTPS）を使用する場合は、SSLを有効にし、を使用してクラスタまたはSVMのデジタル証明書情報を入力します `security ssl modify` コマンドを実行します
4. クラスタまたはSVMでWebサービスを有効にするには、を使用します `vserver services web modify` コマンドを実行します

   この手順は、クラスタまたは SVM に対して有効にする各サービスについて繰り返す必要があります。

5. 特定のロールにクラスタまたはSVMのWebサービスへのアクセスを許可するには、を使用します `vserver services web access create` コマンドを実行します

   アクセスを許可するロールはすでに存在している必要があります。を使用して、既存のロールを表示できます `security login role show` コマンドを実行するか、を使用して新しいロールを作成します `security login role create` コマンドを実行します

6. Webサービスへのアクセスが許可されているロールについては、の出力を確認して、ユーザにも正しいアクセス方法が設定されていることを確認してください `security login show` コマンドを実行します

   をクリックしてONTAP API Webサービスにアクセスします `ontapi`）を使用してユーザを設定する必要があります `ontapi` アクセス方法。他のすべてのWebサービスにアクセスするには、ユーザがで設定されている必要があります `http` アクセス方法。

   を使用します `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。

Web サービスを管理するためのコマンド

を使用します `vserver services web` クラスタまたはStorage Virtual Machine（SVM）のWebサービスの可用性を管理するためのコマンド。を使用します `vserver services web access` ロールのWebサービスへのアクセスを制御するコマンド。

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します • Web サービスへのアクセスに HTTPS だけを使用できるようにするかどうかを指定します	`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します	`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 9コマンド"

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` Web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、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、を使用して管理できます `system node root-mount` コマンド

状況	使用するコマンド
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します	`system node root-mount create` ノード間で作成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上の既存のマウントポイントを、マウントポイントが作成された時刻と現在の状態を含めて表示します	`system node root-mount show`
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終了します	`system node root-mount delete`

関連情報

"ONTAP 9コマンド"

SSLの管理

SSL プロトコルは、デジタル証明書を使用して Web サーバとブラウザの間に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向上させます。

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 の有効化
- 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 証明書名を表示します
- 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、 Web アクセス要求が通過できるようにします
- 使用できる SSL のバージョンを定義します
- 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

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

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、デジタル証明書を関連付けます	`security ssl modify`
クラスタまたは SVM の SSL 設定と証明書の名前を表示する	`security ssl show`

Web サービスへのアクセスに関する問題のトラブルシューティングを行う

設定エラー原因 Web サービスへのアクセスに関する問題が発生します。このエラーに対応するには、 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、 すべてのユーザアクセス許可が正しく設定されていることを確認します。

次の表は、 Web サービスの設定エラーを特定して対処する際に役立ちます。

アクセスに関する問題	原因となる設定エラー	エラーに対処する方法
Webブラウザからが返されます `unable to connect` または `failure to establish a connection` Webサービスにアクセスしようとするとエラーが発生します。	LIF が正しく設定されていない可能性があります。	Web サービスを配信する LIF に ping を送信できることを確認します。 を使用します `network ping` コマンドを使用してLIFにpingを送信します。ネットワーク設定の詳細については、『ネットワーク管理ガイド』を参照してください。
ファイアウォールが正しく設定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いて、ポリシーが Web サービスを配信する LIF に割り当てられていることを確認します。 を使用します `system services firewall policy` ファイアウォールポリシーを管理するためのコマンド。を使用します `network interface modify` コマンドにを指定します `-firewall -policy` ポリシーをLIFに関連付けるためのパラメータ。	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。

アクセスに関する問題	原因となる設定エラー	エラーに対処する方法
Web プロトコルエンジンが有効になっていて、 Web サービスがアクセス可能であることを確認します。 を使用します `system services web` クラスタのWeb プロトコルエンジンを管理するコマンド。	Webブラウザからが返されます `not found` Webサービスにアクセスしようとするとエラーが発生します。	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。 を使用します `vserver services web modify` Webサービスへのアクセスを有効にするコマンド。	Web ブラウザで、ユーザ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ない。	ユーザを認証できない、アクセス方法が正しくない、またはユーザに Web サービスへのアクセスが許可されていない

アクセスに関する問題	原因となる設定エラー	エラーに対処する方法
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が設定されていることを確認します。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ます。 を使用します `security login` ユーザアカウント、そのアクセス方法、および認証方法を管理するコマンド。ONTAP API Webサービスにアクセスするにはが必要です `ontapi` アクセス方法。他のすべてのWebサービスにアクセスするにはが必要です `http` アクセス方法。を使用します `vserver services web access` ロールのWebサービスへのアクセスを管理するコマンド。	HTTPS を使用して Web サービスに接続すると、接続が中断されたことが Web ブラウザに表示されます。	Web サービスを配信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る
クラスタまたは SVM で SSL が有効になっていて、デジタル証明書が有効であることを確認します。 を使用します `security ssl` HTTPサーバおよびのSSL設定を管理するコマンド `security certificate show` デジタル証明書情報を表示するコマンド。	HTTPS を使用して Web サービスに接続すると、信頼されていない接続であると Web ブラウザに表示されます。	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。

証明書を使用してリモートサーバの **ID** を確認します

証明書の概要を使用してリモートサーバの ID を確認します

ONTAP は、リモートサーバの ID を検証するセキュリティ証明書機能をサポートしています。

ONTAP ソフトウェアでは、次のデジタル証明書機能とプロトコルを使用して安全に接続できます。

- Online Certificate Status Protocol （ OCSP ）は、 SSL 接続と 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は無効になっています。
- ONTAP ソフトウェアには、信頼されたルート証明書のデフォルトセットが付属しています。
- Key Management Interoperability Protocol （ KMIP ）の証明書を使用して、クラスタと KMIP サーバの相互認証を有効にできます。

OCSP を使用してデジタル証明書が有効であることを確認します

ONTAP 9.2 以降では、 Online Certificate Status Protocol （ OCSP ）を有効にすることで、 Transport Layer Security （ TLS ）通信を使用する ONTAP アプリケーションでデジタル証明書のステータスを受信できます。OCSP による証明書のステータスチェックは、特定のアプリケーションに対していつでも有効または無効にできます。デフォルトでは、 OCSP による証明書のステータスチェックは無効になっています。

必要なもの

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。

このタスクについて

OCSP は、次のアプリケーションをサポートしています。

- AutoSupport
- イベント管理システム（ 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 advanced に設定します。 `set -privilege advanced`。
2. 特定の ONTAP 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場合	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場合	使用するコマンド

有効	`security config ocsp enable`
	
	`-app all`

無効	`security config ocsp disable`
	
	`-app all`

有効にすると、指定した証明書が「有効」、「失効」、「不明」のいずれであるかを示す署名済みの応答が、すべてのアプリケーションに送信されます。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場合、または OCSP サーバにアクセスできない場合、アプリケーションは続行できません。

4. を使用します `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.
```

TLS ベースのアプリケーションのデフォルト証明書を表示します

ONTAP 9.2 以降では、 ONTAP に、 Transport Layer Security （ TLS ）を使用する ONTAP アプリケーション用の信頼されたルート証明書のデフォルトセットが付属しています。

必要なもの

デフォルトの証明書は、管理 SVM の作成時、または ONTAP 9.2 へのアップグレード時に、管理 SVM にのみインストールされます。

このタスクについて

現在クライアントとして機能し、証明書の検証が必要なアプリケーションは、 AutoSupport 、 EMS 、 LDAP 、監査ログ、 FabricPool 、 および KMIP を使用できます。

証明書の有効期限が切れると、ユーザに証明書を削除するよう要求する EMS メッセージが起動します。デフォルトの証明書は、 advanced 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 アプリケーションが正常に機能しなくなる場合があります（ AutoSupport 、監査ログなど）。

ステップ

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

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver    Serial Number   Common Name                             Type
---------- --------------- ---------------------------------------
------------
fas2552-2n-abc-3
           01              AAACertificateServices
server-ca
    Certificate Authority: AAA Certificate Services
          Expiration Date: Sun Dec 31 18:59:59 2028
```

クラスタと**KMIP**サーバの相互認証

クラスタと **KMIP** サーバの相互認証の概要

Key Management Interoperability Protocol （ KMIP ）サーバなど、クラスタと外部キー管理ツールを相互認証することで、キー管理ツールが SSL を介した KMIP を使用してクラスタと通信できるようになります。この設定は、特定のアプリケーションや機能（ストレージ暗号化機能など）で、データアクセスの安全性を確保するためにセキュアなキーが必要とされる場合に使用します。

クラスタの証明書署名要求を生成します

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

必要なもの

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

   コマンド構文全体については、マニュアルページを参照してください。

   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 CSR は、米国カリフォルニア州のサニーベールにある server1.companyname.com というカスタム共通名の企業の 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。CSR と秘密鍵が出力に表示されます。

```
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-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

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

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

クラスタの **CA** 署名済みサーバ証明書をインストールします

SSL サーバでクラスタまたは Storage Virtual Machine （ SVM ）を SSL クライアントとして認証するためには、 client タイプのデジタル証明書をクラスタまたは SVM にインストールします。次に、 client-ca 証明書をその SSL サーバの管理者に渡してインストールしてもらいます。

必要なもの

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をインストールしておく必要があります `server-ca` 証明書のタイプ。

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、を使用します `security certificate create` コマンドにを指定します `type client` パラメータ
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. セキュリティ証明書を使用して、証明書署名要求（CSR）を生成します `generate-csr` コマンドを実行します

      証明書要求と秘密鍵を含む CSR 出力が表示され、今後の参照用にファイルにコピーするよう求められます。 ONTAP

   b. 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 CA に送信し、署名を求めます。

      秘密鍵と CA 署名証明書のコピーは今後の参照用として保管しておいてください。

   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. を使用してCA署名証明書をインストールします `security certificate install` コマンドにを指定します `-type client` パラメータ
   b. プロンプトが表示されたら証明書と秘密鍵を入力し、 * 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。

      信頼できるルート CA から発行された SSL 証明書に至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、問題のエンドエンティティのサーバ証明書専用に信頼できるルートから発行される、副次的な証明書です。この結果、信頼できるルート CA から始まり、中間証明書を経て、発行された SSL 証明書で終わる証明書チェーンが形成されます。

3. を指定します `client-ca` クラスタまたはSVMの証明書。サーバにインストールするためのSSLサーバの管理者への証明書。

   security certificate showコマンドとを使用します `-instance` および `-type client-ca` が表示されます `client-ca` 証明書情報。

KMIP サーバの CA 署名済みクライアント証明書をインストールします

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 のタイプと組み合わせて適用され、クラスタと外部キー管理ツール（ KMIP サーバなど）の相互認証に使用される証明書であることを示します。

このタスクについて

KMIP サーバをクラスタに対して SSL サーバとして認証する KMIP 証明書をインストールします。

手順

1. を使用します `security certificate install` コマンドにを指定します `-type server-ca` および `-subtype kmip-cert` KMIPサーバ用のKMIP証明書をインストールするためのパラメータ。

2. プロンプトが表示されたら、証明書を入力して Enter キーを押します。

   今後の参照用として証明書のコピーを保管するように ONTAP から求められます。

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

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----


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

cluster1::>
```