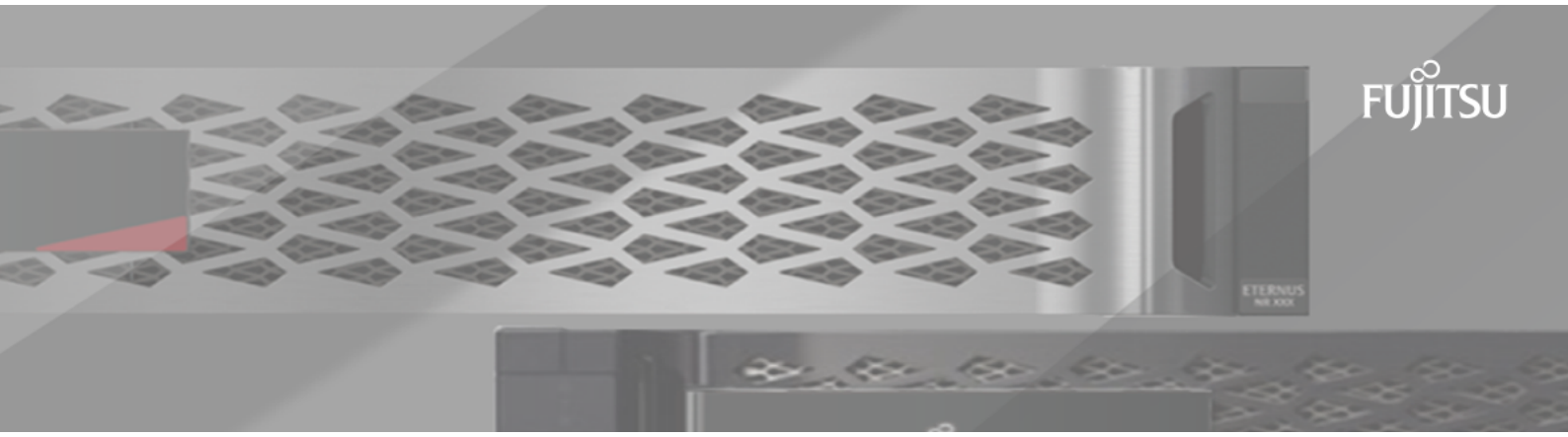
A3CA08733-A605-03



FUJITSU Storage ETERNUS AX/HX Series

管理者認証とRBACパワー ガイド

目次

管理者認証とRBACパワー ガイドの対象者

本書では、ONTAPのクラスタ管理者およびStorage Virtual Machine（SVM）管理者のログイン アカウントを有効にする方法について説明します。また、管理者が実行できる機能をロールベース アクセス制御（RBAC）を使用して定義する方法についても説明しています。

このマニュアルは、ログイン アカウントとRBACを有効にする場合に使用します。想定している状況は次のとおりです。

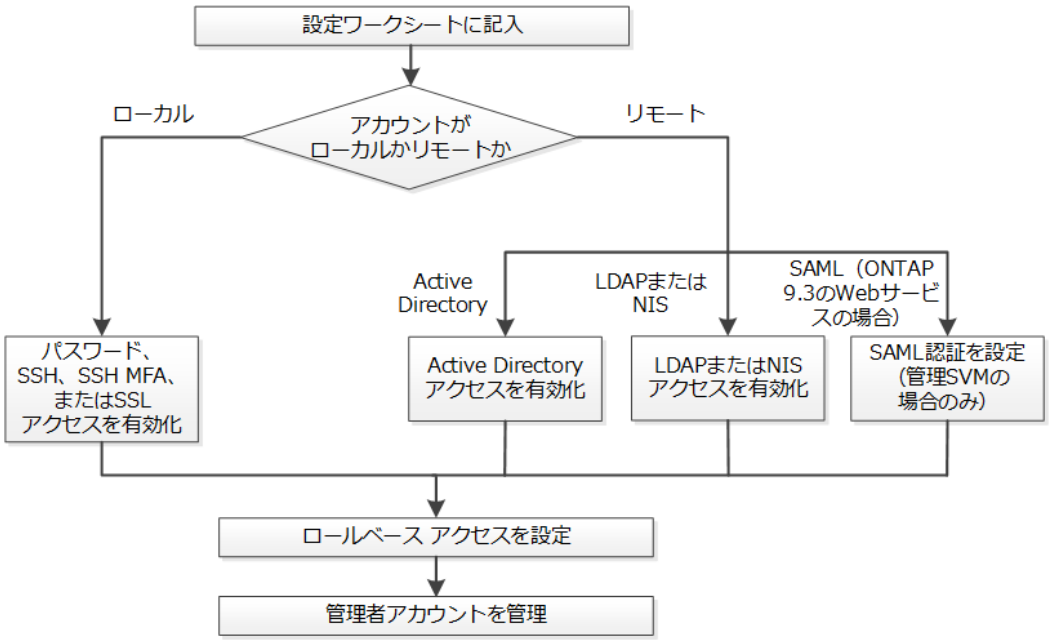
- ONTAP System Managerや自動スクリプト ツールではなく、ONTAPコマンドライン インターフェイス（CLI）を使用する必要がある。
- すべての選択肢について検討するのではなく、ベストプラクティスに従う。
- 背景にある概念について詳しく確認する必要はない。
- クラスタについての情報の収集にSNMPを使用しない。

上記の想定条件に該当しない場合は、本書の代わりに次のドキュメントを参照してください。

- ONTAP System Managerを使用したクラスタの管理

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。それぞれのアカウントに事前定義またはカスタムのロールを割り当てることができます。



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

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

  パスワードと公開鍵による認証がサポートされています。

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

- Active Directory
- SAML認証（管理SVMのみ）

  Service Processor Infrastructure、ONTAP API、またはONTAP System Managerのいずれかのウェブ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。
- 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

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 アカウントの作成または変更

次の値は、`security login create`コマンドでログイン アカウントによるStorage Virtual Machine（SVM）へのアクセスを有効にするときに指定します。同じ値は、`security login modify`コマンドでアカウントによるSVMへのアクセスを変更するときにも指定します。

表 1 :

フィールド	説明	収集/決定する情報
-vserver	アカウントがアクセスするSVMの名前。デフォルト値はクラスタの管理SVMの名前です。	
-user-or-group-name	アカウントのユーザ名またはグループ名。グループ名を指定した場合、そのグループ内の各ユーザのアクセスが有効になります。 1つのユーザ名またはグループ名を複数のアプリケーションに関連付けることができます。	
-application	SVMへのアクセスに使用するアプリケーション。 • `http` • `ontapi` • `snmp` • `ssh`	
-authmethod	アカウントの認証に使用する認証方式。 • `cert` - SSL証明書認証 • `domain` - Active Directory認証 • `nsswitch` - LDAP認証またはNIS認証 • `password` - ユーザ パスワード認証 • `publickey` - 公開鍵認証 • `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 • `saml` - Security Assertion Markup Language（SAML）認証	
-remote-switch-ipaddress	リモート スイッチのIPアドレス。リモート スイッチは、クラスタ スイッチ ヘルス モニタ（CSHM）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`snmp`で、認証方法が`usm`の場合にのみ使用できます。	

フィールド	説明	収集/決定する情報
-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SVM）の場合、デフォルト値はadminです。 • データSVMの場合、デフォルト値はvsadminです。	
-comment	任意。アカウントについての説明。テキストを二重引用符（「"」）で囲む必要があります。	
-is-ns-switch-group	アカウントがLDAPグループ アカウントか、またはNISグループ アカウントか（yesまたはno）。	
-second-authentication-method	• none - 多要素認証を使用しない（デフォルト値） • publickey - 公開鍵認証（authmethodがpasswordまたはnsswitchの場合） • password - ユーザ パスワード認証（authmethodが公開鍵の場合） • nsswitch - ユーザ パスワード認証（authmethodがpublickeyの場合） **注：** nsswitchは、**ONTAP 9.7**以降でサポートされます。 認証の順序は、常に公開鍵が先でパスワードがあとです。	

カスタム ロールの定義

次の値は、security login role createコマンドでカスタム ロールを定義するときに指定します。

表 2：

フィールド	説明	収集/決定する情報
-vserver	任意。ロールに関連付けられているSVM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」。 すべてのコマンド ディレクトリを指定する場合は、DEFAULTと入力する必要があります。	

フィールド	説明	収集/決定する情報
-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） - コマンド ディレクトリに含まれるコマンドへのアクセスを拒否します。 • readonly - コマンド ディレクトリとそのサブディレクトリに含まれるshowコマンドへのアクセスを許可します。 • all - コマンド ディレクトリとそのサブディレクトリに含まれるすべてのコマンドへのアクセスを許可します。 非組み込みコマンド（末尾がcreate、modify、delete、show以外のコマンド）の場合： • none（カスタム ロールのデフォルト値） - コマンドへのアクセスを拒否します。 • readonly - 指定できません。 • 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するクエリ オブジェクト。コマンドまたはコマンド ディレクトリ内のコマンドの有効なオプションの形式で指定します。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volumeの場合、「-aggr aggr0」というクエリ オブジェクトを指定すると、aggr0アグリゲートについてのみアクセスが許可されます。	

ユーザ アカウントへの公開鍵の関連付け

次の値は、security login publickey createコマンドでユーザ アカウントにSSH公開鍵を関連付けるときに指定します。

表 3 :

フィールド	説明	収集/決定する情報
-vserver	任意。アカウントがアクセスするSVMの名前。	
-username	アカウントのユーザ名。デフォルト値は、クラスタ管理者のデフォルト名であるadminです。	

フィールド	説明	収集/決定する情報
-index	公開鍵のインデックス番号。デフォルト値は、アカウントに対して最初に作成された鍵では0、それ以外の場合は既存の一番大きいインデックス番号に1を加えた値です。	
-publickey	OpenSSH公開鍵。鍵は二重引用符（「"」）で囲む必要があります。	
-role	アカウントに割り当てられているアクセス制御ロール。	
-comment	任意。公開鍵についての説明。テキストを二重引用符（「"」）で囲む必要があります。	

CA署名済みサーバ デジタル証明書のインストール

次の値は、`security certificate generate-csr`コマンドで、SVMをSSLサーバとして認証する際に使用する証明書署名要求（CSR）を生成するときに指定します。

表 4 :

フィールド	説明	収集/決定する情報
-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。この値が高いほど、鍵のセキュリティは向上します。デフォルト値は`2048`です。有効な値は、`512`、`1024`、`1536`、および`2048`です。	
-country	SVMが設置されている国の2文字のコード。デフォルト値はUSです。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	SVMが設置されている都道府県。	
-locality	SVMが設置されている市区町村。	
-organization	SVMを管理している組織。	
-unit	SVMを管理している組織内の部門。	
-email-addr	SVMの管理担当者の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`SHA256`です。有効な値は、`SHA1`、`SHA256`、および`MD5`です。	

次の値は、`security certificate install`コマンドで、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署名済みデジタル証明書をインストールするときに指定します。次の表には、このガイドに関連するオプションのみを記載します。

表 5 :

フィールド	説明	収集/決定する情報
-vserver	証明書をインストールするSVMの名前。	
-type	証明書のタイプ。 • `server` - サーバ証明書および中間証明書 • `client-ca` - SSLクライアントのルートCAの公開鍵証明書 • `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 • `client` - ONTAPをSSLクライアントとして使用するための自己署名またはCA署名のデジタル証明書と秘密鍵	

Active Directoryドメイン コントローラ アクセスの設定

次の値は、データSVM用のCIFSサーバを設定済みで、`security login domain-tunnel create`コマンドで、Active Directoryドメイン コントローラからクラスタへのアクセス用にSVMをゲートウェイまたはトンネルとして設定するときに指定します。

表 6 :

フィールド	説明	収集/決定する情報
-vserver	CIFSサーバが設定されているSVMの名前。	

次の値は、CIFSサーバを設定していない場合に、`vserver active-directory create`コマンドで、Active DirectoryドメインにSVMコンピュータ アカウントを作成するときに指定します。

表 7 :

フィールド	説明	収集/決定する情報
-vserver	Active Directoryコンピュータ アカウントを作成するSVMの名前。	
-account-name	コンピュータ アカウントのNetBIOS名。	
-domain	完全修飾ドメイン名（FQDN）。	
-ou	ドメイン内の組織単位。デフォルト値は`CN=Computers`です。この値がドメイン名に付加されて、Active Directory識別名が生成されます。	

LDAPサーバまたはNISサーバのアクセスの設定

次の値は、`vserver services name-service ldap client create`コマンドでSVMのLDAPクライアント設定を作成するときに指定します。

注： -serversフィールドが-ldap-serversフィールドに置き換えられています。この新しいフィールドには、LDAPサーバの値としてホスト名またはIPアドレスを指定できます。

次の表には、このガイドに関連するオプションのみを記載します。

表 8：

フィールド	説明	収集/決定する情報
-vserver	クライアント設定のSVMの名前。	
-client-config	クライアント設定の名前。	
-servers	クライアントが接続するLDAPサーバのIPアドレスをカンマで区切ったリスト。	
-ldap-servers	クライアントが接続するLDAPサーバのIPアドレスおよびホスト名をカンマで区切ったリスト。	
-schema	クライアントがLDAPクエリの作成に使用するスキーマ。	
-use-start-tls	クライアントがLDAPサーバとの通信をStart TLSを使用して暗号化するかどうか（`true`または`false`）。 **注：** 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。	

次の値は、`vserver services name-service ldap create`コマンドでLDAPクライアント設定をSVMに関連付けるときに指定します。

表 9：

フィールド	説明	収集/決定する情報
-vserver	クライアント設定を関連付けるSVMの名前。	
-client-config	クライアント設定の名前。	
-client-enabled	SVMが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、`vserver services name-service nis-domain create`コマンドでSVMでNISドメイン設定を作成するときに指定します。

注： -serversフィールドが-nis-serversフィールドに置き換えられています。この新しいフィールドには、NISサーバの値としてホスト名またはIPアドレスを指定できます。

表 10 :

フィールド	説明	収集/決定する情報
-vserver	ドメイン設定を作成するSVM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	ドメイン設定で使用するNISサーバのIPアドレスをカンマで区切ったリスト。	
-nis-servers	ドメイン設定で使用するNISサーバのIPアドレスおよびホスト名をカンマで区切ったリスト。	

次の値は、vserver services name-service ns-switch createコマンドでネーム サービス ソースの参照順序を指定するときに指定します。

表 11 :

フィールド	説明	収集/決定する情報
-vserver	ネーム サービスの参照順序を設定するSVM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の各ネーム 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 - ファイルおよびLDAPの各ネーム サービス	
-sources	ネーム サービス ソースを参照する順序（カンマで区切ったリスト）。 • file • dns • ldap • nis	

SAMLアクセスの設定

次の値は、security saml-sp createコマンドでONTAP 9.7以降でSAML認証を設定するときに指定します。

表 12 :

フィールド	説明	収集/決定する情報
-idp-uri	アイデンティティ プロバイダ（IdP）メタデータをダウンロード可能な、IdPホストのFTPまたはHTTPアドレス。	
-sp-host	SAMLサービス プロバイダ ホスト（ETERNUS AX/HXシリーズ）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]と[-cert-serial]または[-cert-common-name]	サービス プロバイダ ホスト（ETERNUS AX/HXシリーズ）のサーバ証明書の詳細。	
-verify-metadata-server	IdPメタデータ サーバのアイデンティティを検証するかどうか（`true`または`false`）。この値は常に`true`に設定することを推奨します。	

ログイン アカウントの作成

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アカウントの情報はドメイン コントローラに格納されます。LDAPおよびNISのアカウントはLDAPサーバおよびNISサーバで管理されます。

クラスタ管理者とSVM管理者

クラスタ管理者は、クラスタの管理SVMにアクセスします。管理SVMとクラスタ管理者（予約名`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。

デフォルトの`admin`ロールが割り当てられたクラスタ管理者は、クラスタとそのリソースをすべて管理できます。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*管理者は、データSVMにアクセスします。データSVMとSVM管理者は、クラスタ管理者が必要に応じて作成します。

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

注： リモート クラスタおよびSVMの管理者アカウントに次の汎用的な名前は使用できません：「adm」、「bin」、「cli」、「daemon」、「ftp」、「games」、「halt」、「lp」、「mail」、「man」、「naroot」、「fujitsu」、「news」、「nobody」、「operator」、「root」、「shutdown」、「sshd」、「sync」、「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。たとえば、あるLDAPまたはNISアカウントに`vsadmin`ロールが割り当てられ、同じユーザのADグループ アカウントに`vsadmin-volume`ロールが割り当てられている場合、そのADユーザはより権限の広い`vsadmin`の機能でログインします。このような場合、ロールがマージされたと表現します。

ローカル アカウント アクセスの有効化

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。`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することができます。

パスワード アカウント アクセスの有効化

`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することができます。この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。

始める前に

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。

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確定していない場合は、あとで`security login modify`コマンドを使用してロールを追加できます。

管理者に割り当てられているロールの変更（20ページ）

手順

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、ワークシートを参照してください。

ログイン アカウントの作成または変更（5ページ）

次のコマンドは、事前定義のbackupロールが割り当てられたクラスタ管理者アカウントadmin1が、管理SVMengClusterにパスワードを使用してアクセスできるようにします。この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公開鍵アカウントの有効化

`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することができます。

始める前に

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。

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確定していない場合は、あとで`security login modify`コマンドを使用してロールを追加できます。

  管理者に割り当てられているロールの変更（20ページ）

手順

ローカル管理者アカウントがSSH公開鍵を使用してSVMにアクセスできるようにします。 `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

コマンド構文全体については、ワークシートを参照してください。

ログイン アカウントの作成または変更（5ページ）

次のコマンドは、事前定義のvsadmin-volumeロールが割り当てられたSVM管理者アカウントsvmadmin1が、SVMengData1にSSH公開鍵を使用してアクセスできるようにします。

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

次のタスク

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

ユーザ アカウントへの公開鍵の関連付け（7ページ）

SSH多要素認証（MFA）の有効化

`security login create`コマンドを使用して、管理者による管理SVMまたはデータSVMへのログインにSSH公開鍵とユーザ パスワードの両方を要求することで、セキュリティを強化できます。

始める前に

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。

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確定していない場合は、あとで`security login modify`コマンドを使用してロールを追加できます。

  管理者に割り当てられているロールの変更（20ページ）
- ユーザは最初に公開鍵認証で認証され、続いてパスワード認証で認証されます。

手順

ローカル管理者アカウントに対し、SSH MFAを使用してSVMにアクセスすることを要求します。`security login create -vserver` *`SVM`* `-user-or-group-name` *`user_name`* `-application ssh -authentication-method password|publickey -role admin -second-authentication-method password|publickey`

次のコマンドでは、事前定義された`admin`ロールのSVM管理者アカウント`admin2`に対し、SSH公開鍵とユーザ パスワードの両方を使用して`SVMengData1`にログインすることを要求します。

```
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".
```

次のタスク

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

ユーザ アカウントへの公開鍵の関連付け（7ページ）

SSL証明書アカウントの有効化

`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することができます。

始める前に

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。

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の生成とインストール（25ページ）

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確定していない場合は、あとでsecurity login modifyコマンドを使用してロールを追加できます。

  管理者に割り当てられているロールの変更（20ページ）

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

手順

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、ワークシートを参照してください。

ログイン アカウントの作成または変更（5ページ）

次のコマンドは、デフォルトのvsadminロールが割り当てられたSVM管理者アカウントsvmadmin2が、SVMengData2にSSLデジタル証明書を使用してアクセスできるようにします。

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

次のタスク

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

CA署名済みサーバ証明書の生成とインストール（25ページ）

Active Directoryアカウント アクセスの有効化

`security login create`コマンドを使用して、Active Directory（AD）のユーザ アカウントまたはグループ 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することができます。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。

始める前に

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

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 アクセスの設定（28ページ）

  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確定していない場合は、あとでsecurity login modifyコマンドを使用してロールを追加できます。

  管理者に割り当てられているロールの変更（20ページ）

注： ADグループ アカウントによるアクセスは、SSHアプリケーションとontapiアプリケーションでのみサポートされます。

手順

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

コマンド構文全体については、ワークシートを参照してください。

ログイン アカウントの作成または変更（5ページ）

次のコマンドは、事前定義のbackupロールが割り当てられたADのクラスタ管理者アカウントDOMAIN1\guest1が、管理SVMengClusterにアクセスできるようにします。

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

次のコマンドは、事前定義のvsadmin-volumeロールが割り当てられたADグループ アカウントDOMAIN1\adgroupのSVM管理者アカウントが、SVMengDataにアクセスできるようにします。

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

次のタスク

ADドメイン コントローラからクラスタまたはSVMへのアクセスを設定していない場合は、アカウントがSVMにアクセスする前に設定しておく必要があります。

Active Directoryドメイン コントローラ アクセスの設定（28ページ）

LDAPまたはNISアカウント アクセスの有効化

`security login create`コマンドを使用して、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ことができます。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。

始める前に

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。

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サーバのアクセスの設定（29ページ）

  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確定していない場合は、あとで`security login modify`コマンドを使用してロールを追加できます。

  管理者に割り当てられているロールの変更（20ページ）
- 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。
- LDAPの既知の問題のため、LDAPユーザ アカウント情報のフィールド（gecosやuserPasswordなど）にはコロン（':'）を使用しないでください。コロンを使用すると、そのユーザを検索できなくなります。

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`

   コマンド構文全体については、ワークシートを参照してください。

   ログイン アカウントの作成または変更（5ページ）

   次のコマンドは、事前定義のbackupロールが割り当てられたLDAPまたはNISのクラスタ管理者アカウントguest2が、管理SVMengClusterにアクセスできるようにします。

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

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`

   認証方式にはpublickeyを、第2の認証方式にはnsswitchを指定できます。

   次の例ではMFA認証を有効にしています。

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

次のタスク

LDAPサーバまたはNISサーバからSVMへのアクセスを設定していない場合は、アカウントがSVMにアクセスする前に設定しておく必要があります。

LDAPサーバまたはNISサーバのアクセスの設定（29ページ）

SAML認証の設定

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。

始める前に

- SAML認証用のIdPを設定しておく必要があります。
- IdP URIが必要です。

このタスクについて

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

  httpアプリケーションとontapiアプリケーションは、Webサービス（Service Processor Infrastructure、ONTAP API、またはONTAP System Manager）によって使用されます。
- SAML認証は、管理SVMへのアクセス時にのみ適用できます。

手順

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である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（ここではETERNUS AX/HXシリーズ）のホストのホスト名または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://
scspr0235321001.gdl.englab.fujitsu.com/idp/shibboleth -verify-metadata-
server false

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://10.63.56.150/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`

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

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

   a) SAML認証を使用して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
   ```

アクセス制御ロールの管理

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。

関連概念

クラスタ管理者の事前定義されたロール（21ページ）
SVM管理者の事前定義されたロール（22ページ）

関連タスク

管理者に割り当てられているロールの変更（20ページ）
カスタム ロールの定義（20ページ）

管理者に割り当てられているロールの変更

`security login modify`コマンドを使用して、クラスタやSVMの管理者アカウントのロールを変更できます。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。

始める前に

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

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、ワークシートを参照してください。

ログイン アカウントの作成または変更（5ページ）

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

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

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

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

カスタム ロールの定義

カスタム ロールは、`security login role create`コマンドを使用して定義できます。このコマンドを必要な回数だけ実行し、希望する機能を自由に組み合わせてロールに関連付けることができます。

始める前に

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。

このタスクについて

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

  コマンド ディレクトリ（volumeなど）は、関連するコマンドとそのサブディレクトリで構成されるグループです。この手順で別途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対して指定したアクセス レベルが親のアクセス レベルよりも優先されます。

注： SVM管理者に、adminクラスタ管理者のみが使用できるコマンドやコマンド ディレクトリ（securityコマンド ディレクトリなど）へのアクセスを付与するロールを割り当てることはできません。

手順

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、ワークシートを参照してください。

カスタム ロールの定義（6ページ）

次のコマンドは、vol_roleロールに対して、volumeコマンド ディレクトリのコマンドへのフル アクセスとvolume snapshotサブディレクトリのコマンドへの読み取り専用アクセスを許可します。

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

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

次のコマンドは、SVM_storageロールに対して、storageコマンド ディレクトリのコマンドへの読み取りアクセスを許可し、storage encryptionサブディレクトリのコマンドへのアクセスを拒否し、storage aggregate plex offline非組み込みコマンドへのフル アクセスを許可します。

```
cluster1::>security login role create -role SVM_storage -cmddirname "storage" -
access readonly

cluster1::>security login role create -role SVM_storage -cmddirname "storage
 encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname "storage
 aggregate plex offline" -access all
```

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もできます。デフォルトでは、クラスタ管理者には、事前定義されたadminロールが割り当てられます。

次の表に、クラスタ管理者用の事前定義されたロールを示します。

表 13 :

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
admin	all	すべてのコマンド ディレクトリ（デフォルト）
autosupport	all	• `set` • `system node autosupport`
	none	その他のすべてのコマンド ディレクトリ（デフォルト）
backup	all	`vserver services ndmp`
	readonly	`volume`
	none	その他のすべてのコマンド ディレクトリ（デフォルト）
readonly	all	• `security login password` • `set`
	none	`security`
	readonly	その他のすべてのコマンド ディレクトリ（デフォルト）
none	none	すべてのコマンド ディレクトリ（デフォルト）

注 : `autosupport` ロールは、事前定義された`autosupport`アカウントに割り当てられ、AutoSupport OnDemandで使用されます。ONTAPでは、`autosupport`アカウントを変更または削除することはできません。また、`autosupport`ロールを他のユーザ アカウントに割り当てることもできません。

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もできます。デフォルトでは、SVM管理者は、事前定義された`vsadmin`ロールに割り当てられます。

次の表に、SVM管理者向けの事前定義されたロールを示します。

表 14 :

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の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshotコピー、およびファイルの管理 • LUNの管理 • SnapLock処理の実行（privileged deleteを除く） • プロトコルの設定：NFS、CIFS、iSCSI、FC （FCoEを含む） • サービスの設定：DNS、LDAP、NIS • ジョブの監視 • ネットワーク接続とネットワーク インターフェイスの監視 • SVMの健常性の監視
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の管理 • ボリュームの管理（ボリュームの移動も含む） • 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、CIFS、iSCSI、FC（FCoEを含む） • 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の健常性の監視
vsadmin-protocol	• 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管理 • プロトコルの設定：NFS、CIFS、iSCSI、FC（FCoEを含む） • 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の健常性の監視
vsadmin-backup	• 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管理 • NDMP処理の管理 • リストアしたボリュームの読み取り / 書き込み許可 • SnapMirror関係と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の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshotコピー、およびファイルの管理 • SnapLock処理の実行（privileged deleteも含む） • プロトコルの設定：NFS、CIFS • サービスの設定：DNS、LDAP、NIS • ジョブの監視 • ネットワーク接続とネットワーク インターフェイスの監視

ロール名	機能
vsadmin-readonly	• 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管理 • SVMの健常性の監視 • ネットワーク インターフェイスの監視 • ボリュームとLUNの表示 • サービスとプロトコルの表示

管理者アカウントの管理

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ります。これらのタスクはいずれもアカウント アクセスを有効にする前後どちらでも実行できます。

関連概念

CA署名済みサーバ証明書の生成とインストール（25ページ）
Active Directoryドメイン コントローラ アクセスの設定（28ページ）
LDAPサーバまたはNISサーバのアクセスの設定（29ページ）

関連タスク

管理者アカウントへの公開鍵の関連付け（25ページ）
管理者パスワードの変更（31ページ）
管理者アカウントのロックとロック解除（32ページ）

管理者アカウントへの公開鍵の関連付け

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

始める前に

- 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。

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。

手順

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、ワークシート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（7ページ）

次のコマンドは、SVMengData1のSVM管理者アカウントsvmadmin1に公開鍵を関連付けます。公開鍵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
"ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J
/vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIza
FciDy7hgnmdj9eNGedGr/JNrftQbLD1hZybX+72DpQB0tYWBhe6eDJ1oPLob
ZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

CA署名済みサーバ証明書の生成とインストール

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ために、CA署名済みデジタル証明書をインストールすることを推奨します。`security certificate generate-csr`コマンドを

使用して証明書署名要求（CSR）を生成し、認証局から返された証明書をsecurity certificate installコマンドを使用してインストールします。

関連タスク

証明書署名要求の生成（26ページ）
CA署名済みサーバ証明書のインストール（26ページ）

証明書署名要求の生成

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

始める前に

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

手順

1. CSRを生成します。security certificate generate-csr -common-name *FQDN_or_common_name* -size 512|1024|1536|2048 -country *country* -state *state* -locality *locality* -organization *organization* -unit *unit* -email-addr *email_of_contact* -hash-function SHA1|SHA256|MD5

   次のコマンドは、SHA256ハッシュ関数で生成される2048ビット秘密鍵を使用して、CSRを作成します。この証明書は、米国（US）California州のSunnyvaleにある企業（カスタム共通名server1.companyname.com）のIT部門のSoftwareグループが使用します。SVM担当管理者のEメール アドレスはweb@example.comです。出力にはCSRと秘密鍵が表示されます。

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

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
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を保管する必要があります。

CA署名済みサーバ証明書のインストール

CA署名済みサーバ証明書は、security certificate installコマンドを使用してSVMにインストールできます。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るプロンプトが表示されます。

始める前に

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

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、ワークシートを参照してください。

CA署名済みサーバ デジタル証明書のインストール（8ページ）

注： サーバ証明書の証明書チェーンを形成する、CAのルート証明書と中間証明書の入力を求めるプロンプトが表示されます。チェーンは、サーバ証明書を発行したCAの証明書から始まり、CAのルート証明書まで続きます。中間証明書が1つでも抜けていると、サーバ証明書のインストールに失敗します。

次のコマンドは、CA署名済みサーバ証明書と中間証明書をSVMengData2にインストールします。

```
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.
```

Active Directoryドメイン コントローラ アクセスの設定

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用のCIFSサーバがすでに設定されている場合は、SVMをADのクラスタ アクセス用のゲートウェイ（トンネル）として設定できます。CIFS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。

認証トンネルの設定

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

始める前に

- データSVM用のCIFS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。

手順

CIFS対応のデータSVMをADドメイン コントローラがクラスタにアクセスするための認証トンネルとして設定します。 `security login domain-tunnel create -vserver` *`SVM_name`*

コマンド構文全体については、ワークシートを参照してください。

Active Directoryドメイン コントローラ アクセスの設定（9ページ）

注： 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、CIFS対応のデータSVMengDataを認証トンネルとして設定します。

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

ドメインでのSVMコンピュータ アカウントの作成

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

始める前に

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。

このタスクについて

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

手順

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、ワークシートを参照してください。

Active Directoryドメイン コントローラ アクセスの設定（9ページ）

次のコマンドは、ドメインexample.comにSVMengData用の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設定

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

関連タスク

LDAPサーバ アクセスの設定（29ページ）
NISサーバ アクセスの設定（30ページ）
ネーム サービス スイッチの作成（31ページ）

LDAPサーバ アクセスの設定

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

始める前に

- CA署名済みサーバ デジタル証明書をSVMにインストールしておく必要があります。

  CA署名済みサーバ証明書の生成とインストール（25ページ）
- 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。

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（Windows Server 2012以降のほとんどのADサーバで優先されるスキーマ）
- AD-IDMU（Windows Server 2008、Windows Server 2012、およびそれ以降のADサーバ）
- AD-SFU（Windows Server 2003以前のADサーバ）
- RFC-2307（UNIX LDAPサーバ）

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

- NFS構成パワー ガイド

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`

注： 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、ワークシートを参照してください。

LDAPサーバまたはNISサーバのアクセスの設定（10ページ）

次のコマンドは、SVMengDataにcorpという名前のLDAPクライアント設定を作成します。このクライアントは、IPアドレスが172.160.0.100と172.16.0.101のLDAPサーバに匿名でバインドします。LDAPクエリの作成にはRFC-2307スキーマを使用します。クライアントとサーバの間の通信は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
```

注： フィールド-ldap-serversが、フィールド-serversの代わりに使用されています。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、ワークシートを参照してください。

   LDAPサーバまたはNISサーバのアクセスの設定（10ページ）

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

   注： `vserver services name-service ldap create`コマンドによって設定の自動検証が行われ、ONTAPがネーム サーバに接続できない場合はエラー メッセージが報告されます。

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

   次のコマンドは、SVM vs0のLDAPサーバを検証します。

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

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

   ネーム サービスのチェック コマンドは使用できます。

NISサーバ アクセスの設定

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

始める前に

- 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。

このタスクについて

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

手順

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、ワークシートを参照してください。

LDAPサーバまたはNISサーバのアクセスの設定（10ページ）

注： フィールド-serversがフィールド-nis-serversに置き換えられています。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、SVMengDataにNISドメイン設定を作成します。この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 スイッチの作成

ネーム サービス スイッチ機能を使用すると、LDAPまたはNISを代替ネーム サービス ソースとして使用することができます。ネーム サービス ソースの参照順序は、`vserver services name-service ns-switch modify`コマンドを使用して指定できます。

始める前に

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

手順

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、ワークシートを参照してください。

LDAPサーバまたはNISサーバのアクセスの設定（10ページ）

次のコマンドは、engDataSVMのpasswdデータベースのLDAPおよびNISネーム サービス ソースの参照順序を指定します。

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

管理者パスワードの変更

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

始める前に

- 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。

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。

- 英文字と数字がそれぞれ1文字以上含まれている必要があります。
- 直近の6つのパスワードと同じパスワードは使用できません。

注： `security login role config modify`コマンドを使用して、特定のロールに関連付けられたアカウントに対するパスワード ルールを変更することができます。詳細については、マニュアル ページを参照してください。

`security login role config modify`

手順

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

次のコマンドは、SVMvs1.example.comの管理者であるadmin1のパスワードを変更します。プロンプトで現在のパスワードを入力したあと、新しいパスワードを入力し、確認用に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:
```

管理者アカウントのロックとロック解除

管理者アカウントは`security login lock`コマンドを使用してロックでき、`security login unlock`コマンドを使用してロックを解除できます。

始める前に

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、SVMvs1.example.comの管理者アカウントadmin1をロックします。

   ```
   cluster1::>security login lock -vserver engData -username admin1
   ```
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、SVMvs1.example.comの管理者アカウントadmin1のロックを解除します。

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

失敗したログインの管理

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audit.logファイルで確認できます。

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。

- 大文字、小文字、特殊文字、数字を少なくとも何文字か含めるようにパスワードの要件を設定する。
- ログインに失敗したあとに連続して試行できないように間隔を設定する。
- 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する。
- アクセスしていない期間が指定した日数を超えたアカウントを有効期限切れにしてロックアウトする。

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

さらに、長期的な対策として次のような方法があります。

- `security ssh modify`コマンドを使用して、新規に作成されるすべてのSVMに対してログイン失敗回数の制限を設定する。
- ユーザにパスワードを変更するように要求し、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。

関連タスク

管理者アカウント パスワードでのSHA-2の適用（33ページ）

管理者アカウント パスワードでのSHA-2の適用

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ことが可能です。

- 指定したハッシュ関数に一致するユーザ アカウントを表示する。
- 指定したハッシュ関数（MD5など）を使用するアカウントを期限切れにして、次回ログイン時にユーザにパスワードを変更させる。
- 指定したハッシュ関数を使用するパスワードが指定されたアカウントをロックする。

ONTAPでは、Manageability SDK（security-login-createおよびsecurity-login-modify-password）を使用して、あらかじめハッシュ化したSHA-2パスワードだけを受け入れます。

手順

1. MD5管理者アカウントをSHA-512パスワード ハッシュ関数に移行します。
   a) すべてのMD5管理者アカウントを期限切れにします。`security login expire-password -vserver * -username * -hash-function md5`
      これにより、MD5アカウントのユーザは、次回のログイン時にパスワードの変更が必要になります。
   b) MD5アカウントのユーザに、コンソールまたはSSHセッションを使用してログインするよう促します。
      システムによってアカウントの有効期限が切れていることが検出され、ユーザにパスワードの変更を求めるメッセージが表示されます。変更されたパスワードでは、デフォルトでSHA-512が使用されます。
2. オプション: ユーザが一定期間ログインしていないためにパスワードが変更されていないMD5アカウントについては、強制的にアカウントを移行します。
   a) 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`*
      -lock-afterで指定した日数が経過すると、ユーザはMD5アカウントにアクセスできなくなります。

b) ユーザがパスワードを変更できる状態になったら、アカウントのロックを解除します。`security login unlock -vserver *vserver_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。

詳細情報の入手方法

ONTAPのクラスタ管理者およびSVM管理者のログイン アカウントを有効にしたあと、さらに高度なタスクを実行できます。

- ONTAP System Managerを使用したクラスタの管理

  ONTAP System Managerを使用して管理者認証とRBACに関するタスクを実行する方法について説明します。
- システム アドミニストレーション リファレンス

  ONTAPを実行するストレージ システムの一般的なシステム管理について説明しています。

著作権に関する情報

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

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

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

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

登録商標

富士通、富士通ロゴ、ETERNUSは富士通の登録商標です。会社名、製品名等の固有名詞は、各社の商号、商標または登録商標です。

https://www.fujitsu.com/jp/products/computing/storage/trademark/

マニュアルの更新について

本書の最新版や本装置に関連する最新の情報は、以下のサイトで公開されています。

https://www.fujitsu.com/jp/products/computing/storage/manual/

必要に応じてご使用モデルのマニュアルを参照してください。

FUJITSU Storage ETERNUS AX/HX Series

管理者認証とRBACパワー ガイド

A3CA08733-A605-03

発行日: 2021 年 6 月

発行責任: 富士通株式会社