



# **ONTAP Tools for VMware vSphereの設定**

## **ONTAP tools for VMware vSphere 10**

NetApp  
November 17, 2025

# 目次

|                                                                |    |
|----------------------------------------------------------------|----|
| ONTAP Tools for VMware vSphereの設定 .....                        | 1  |
| vCenter Serverインスタンスの追加 .....                                  | 1  |
| VASA ProviderをvCenter Serverインスタンスに登録する .....                  | 1  |
| NFS VAAIプラグインをインストールする .....                                   | 2  |
| ESXiホストの設定 .....                                               | 3  |
| ESXiサーバのマルチパスとタイムアウトの設定 .....                                  | 3  |
| ESXiホストの値の設定 .....                                             | 4  |
| ONTAPユーザのロールと権限の設定 .....                                       | 5  |
| SVMアグリゲートのマッピングの要件 .....                                       | 6  |
| ONTAPのユーザとロールを手動で作成する .....                                    | 6  |
| ONTAP tools for VMware vSphere 10.1ユーザから10.3ユーザへのアップグレード ..... | 14 |
| ストレージバックエンドを追加します .....                                        | 16 |
| ストレージバックエンドとvCenter Serverインスタンスの関連付け .....                    | 17 |
| ネットワークアクセスの設定 .....                                            | 18 |
| データストアを作成 .....                                                | 18 |

# ONTAP Tools for VMware vSphereの設定

## vCenter Serverインスタンスの追加

vCenter ServerインスタンスをONTAP tools for VMware vSphereに追加して、vCenter Server環境内の仮想データストアを設定、管理、保護します。複数の vCenter Server インスタンスを追加する場合、ONTAP ツールと各 vCenter Server 間の安全な通信にはカスタム CA 証明書が必要です。

- このタスクについて \*

ONTAP toolsをvCenterと統合することで、プロビジョニング、Snapshot、データ保護などのストレージタスクをvSphere Clientから直接実行できるため、別のストレージ管理コンソールに切り替える必要がありません。

### 手順

1. Webブラウザを開き、次のURLに移動します。  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャルを使用してログインします。
3. vCenter Serverインスタンスをオンボードするには、\* vCenters > Add \*を選択します。vCenterのIPアドレスまたはホスト名、ユーザ名、パスワード、およびポートの詳細を入力します。



vCenterインスタンスをONTAP toolsに追加するために管理者アカウントは必要ありません。権限が制限された管理者アカウントなしでカスタムロールを作成できます。詳細については、を参照してください ["vCenter Server RBACとONTAP Tools for VMware vSphere 10の使用"](#)。

vCenter ServerインスタンスをONTAP toolsに追加すると、次の処理が自動的にトリガーされます。

- vCenter Clientプラグインがリモートプラグインとして登録されます。
- プラグインとAPIのカスタムPrivilegesがvCenter Serverインスタンスに適用されます。
- ユーザを管理するためのカスタムロールが作成されます。
- プラグインは、vSphereユーザインターフェイスにショートカットとして表示されます。

## VASA ProviderをvCenter Serverインスタンスに登録する

VASA Providerは、ONTAP tools for VMware vSphereを使用してvCenter Serverインスタンスに登録できます。[VASA Providerの設定]セクションに、選択したvCenter ServerのVASA Providerの登録ステータスが表示されます。マルチ vCenter 展開では、各 vCenter Server インスタンスにカスタム CA 証明書があることを確認します。

### 手順

1. vSphere Clientにログインします。
2. プラグインセクションで\*ショートカット\*>\* NetApp ONTAP tools \*を選択します。

3. >[VASA Provider設定]\*を選択します。VASA Providerの登録ステータスは「Not Registered」と表示されます。
4. [登録]\*ボタンを選択してVASA Providerを登録します。
5. VASA Providerの名前を入力し、ONTAP tools for VMware vSphereアプリケーションのユーザクレデンシャルを指定して、\*[登録]\*を選択します。
6. 登録が完了してページが更新されると、登録されているVASA Providerのステータス、名前、バージョンが表示されます。登録後、登録解除アクションがアクティブになります。

。終了後 \*

vCenterクライアントからオンボードしたVASA Providerが[VASA Provider]の下に表示されていることを確認します。

#### 手順

1. vCenter Serverインスタンスに移動します。
2. 管理者のクレデンシャルでログインします。
3. >[設定]\*を選択します。オンボードしたVASA Providerが正しく表示されていることを確認します。

## NFS VAAIプラグインをインストールする

NFS vStorage API for Array Integration (NFS VAAI) プラグインは、VMware vSphere とNFSストレージレイを統合するソフトウェアコンポーネントです。ONTAP tools for VMware vSphereを使用してNFS VAAIプラグインをインストールし、NFSストレージレイの高度な機能を活用して、特定のストレージ関連処理をESXiホストからストレージアレイ自体にオフロードします。

#### 開始する前に

- インストールパッケージをダウンロードし ["NetApp NFS Plug-in for VMware VAAI"](#) ます。
- ESXiホストとvSphere 7.0U3の最新のパッチ以降のバージョンとONTAP 9.14.1以降のバージョンがあることを確認します。
- NFSデータストアをマウント

#### 手順

1. vSphere Clientにログインします。
2. プラグインセクションで\*ショートカット\*>\* NetApp ONTAP tools \*を選択します。
3. >[NFS VAAIツール]\*を選択します。
4. VAAIプラグインをvCenter Serverにアップロードしたら、\* Existing version セクションで Change を選択します。**VAAI**プラグインが**vCenter Server**にアップロードされていない場合は、[アップロード]\*ボタンを選択します。
5. ファイルを参照して選択し .vib、\*アップロード\*を選択してファイルをONTAPツールにアップロードします。
6. を選択し、**NFS VAAI**プラグインをインストールする**ESXi**ホストを選択して、[インストール]\*を選択します。

プラグインのインストールに適したESXiホストのみが表示されます。インストールの進捗状況は、vSphere Web Clientの[Recent tasks]セクションで監視できます。

#### 7. インストール後にESXiホストを手動で再起動します。

VMware管理者がESXiホストを再起動すると、ONTAP Tools for VMware vSphereによってNFS VAAIプラグインが自動的に検出されて有効になります。

#### 次の手順

NFS VAAIプラグインをインストールしてESXiホストをリブートしたら、VAAIコピーオフロード用の正しいNFSエクスポートポリシーを設定する必要があります。NFS環境でVAAIを設定する場合は、次の要件を考慮してエクスポートポリシールールを設定します。

- 関連するONTAPボリュームでNFSv4呼び出しを許可する必要があります。
- rootユーザはrootのままにし、すべてのジャンクションの親ボリュームでNFSv4が許可されている必要があります。
- 該当するNFSサーバでVAAIサポートのオプションを設定する必要があります。

手順の詳細については ["VAAIコピーオフロードの正しいNFSエクスポートポリシーを設定する"](#)、技術情報アーティクルを参照してください。

#### 関連情報

["VMware vStorage over NFSのサポート"](#)

["NFSv4.0を有効または無効にする"](#)

["NFSv4 4.2 の ONTAP サポート"](#)

## ESXiホストの設定

ESXiサーバのマルチパスとタイムアウトを設定すると、プライマリパスに障害が発生した場合にバックアップストレージパスにシームレスに切り替えることができるため、高可用性とデータの整合性が確保されます。

### ESXiサーバのマルチパスとタイムアウトの設定

ONTAP tools for VMware vSphereは、NetAppストレージシステムに最適なESXiホストのマルチパス設定とHBAタイムアウト設定を確認して設定します。

- このタスクについて \*

構成とシステムの負荷によっては、このプロセスに時間がかかることがあります。タスクの進行状況は、[最近のタスク]パネルに表示されます。

#### 手順

1. VMware vSphere Web Clientのホームページで、\*[ホストおよびクラスター]\*を選択します。
2. ホストを右クリックし、\* NetApp ONTAP tools > Update host data \*を選択します。

3. VMware vSphere Web Clientのショートカットページで、[plug-ins]セクションで\* NetApp ONTAP tools \*を選択します。
4. ONTAP Tools for VMware vSphereプラグインの概要（ダッシュボード）にある\* ESXiホストコンプライアンス\*カードに移動します。
5. [推奨設定の適用]\*リンクを選択します。
6. ウィンドウで、**NetApp**の推奨設定に準拠するように更新するホストを選択し、[次へ]\*を選択します。



ESXiホストを展開すると、現在の値を確認できます。

7. 設定ページで、必要に応じて推奨値を選択します。
8. 概要ペインで値を確認し、\*[完了]\*を選択します。進捗状況は、最近のタスクパネルで追跡できます。

## ESXiホストの値の設定

ONTAP tools for VMware vSphereを使用すると、ESXiホストでタイムアウトなどの値を設定して、最適なパフォーマンスが確保され、フェイルオーバーが正常に実行されるようにすることができます。ONTAP tools for VMware vSphereが設定する値は、社内のNetAppテストに基づいています。

ESXiホストで設定できる値は次のとおりです。

### HBA / CNAアダプタ設定

次のパラメータをデフォルト値に設定します。

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Emulex FC HBAタイムアウト
- QLogic FC HBAタイムアウト

### MPIO設定

MPIO設定では、NetAppストレージシステムの優先パスを定義します。また、使用可能なパスのうちどのパスが最適化されているか（インターコネクトケーブルを経由する非最適化パスではなく）が判断され、そのいずれかのパスに優先パスが設定されます。

ハイパフォーマンス環境や、単一のLUNデータストアでパフォーマンスをテストする場合は、ラウンドロビン（VMW\_PSP\_RR）パス選択ポリシー（PSP）の負荷分散設定をデフォルトのIOPS設定である1000から1に変更することを検討してください。



MPIO 設定は、NVMe、NVMe/FC、NVMe/TCP プロトコルには適用されません。

### NFS設定

| パラメータ             | 設定する値   |
|-------------------|---------|
| Net.TcpipHeapSize | 32      |
| Net.TcpipHeapMax  | 1024 MB |

|                          |       |
|--------------------------|-------|
| NFS.MaxVolumes           | 256   |
| NFS41.MaxVolumes         | 256   |
| NFS.MaxQueueDepth        | 128以上 |
| NFS.HeartbeatMaxFailures | 10    |
| NFS.HeartbeatFrequency   | 12    |
| NFS.HeartbeatTimeout     | 5     |

## ONTAPユーザのロールと権限の設定

ストレージバックエンドの管理に使用する新しいユーザロールと権限を設定するには、ONTAP tools for VMware vSphereおよびONTAP System Managerに付属のJSONファイルを使用します。

開始する前に

- ONTAP PrivilegesファイルをONTAP tools for VMware vSphereから、`_ \ https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip`を使用してダウンロードしておく必要があります。
- を使用して、ONTAP toolsからONTAP Privilegesファイルをダウンロードしておく必要があります  
`https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip`



ユーザは、クラスタレベルまたはStorage Virtual Machine (SVM) レベルで直接作成できません。user\_roles.jsonファイルを使用せずにユーザを作成することもできます。作成した場合は、SVMレベルの最小限の権限セットが必要になります。

- ストレージバックエンドの管理者権限でログインしている必要があります。

手順

1. ダウンロードした `_ \ https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip` を展開します。
2. クラスタのクラスタ管理IPアドレスを使用してONTAP System Managerにアクセスします。
3. 管理Privilegesでクラスタにログインします。ユーザを設定するには、次の手順を実行します。
  - a. クラスタのONTAP toolsユーザを設定するには、[クラスタ]>[ユーザとロール]\*ペインを選択します。
  - b. SVM ONTAP toolsのユーザを設定するには、[ストレージSVM]>[ユーザとロール]\*ペインを選択します。
  - c. [Users]で[Add]\*を選択します。
  - d. [ユーザーの追加]\*ダイアログボックスで、[仮想化製品]\*を選択します。
  - e. \*参照\*をクリックして、ONTAP Privileges JSONファイルを選択してアップロードします。

[Product]フィールドには自動的に値が入力されます。

- f. 製品機能ドロップダウンメニューから必要な機能を選択します。

[ロール]\*フィールドには、選択した製品機能に基づいて自動的に値が入力されます。

- g. 必要なユーザ名とパスワードを入力します。
- h. ユーザに必要なPrivileges（検出、ストレージの作成、ストレージの変更、ストレージの削除、NAS/SANロール）を選択し、\*[追加]\*を選択します。

新しいロールとユーザが追加され、設定したロールの詳細な権限が表示されます。

## SVMアグリゲートのマッピングの要件

データストアのプロビジョニングにSVMのユーザクレデンシャルを使用するために、内部的にONTAP tools for VMware vSphereは、データストアのPOST APIで指定されたアグリゲートにボリュームを作成します。ONTAPでは、SVMユーザクレデンシャルを使用して、マッピングされていないアグリゲートにボリュームを作成することはできません。この問題を解決するには、ここで説明するONTAP REST APIまたはCLIを使用してSVMとアグリゲートをマッピングする必要があります。

REST API：

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

ONTAP CLI：

```
still15_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver      Aggregate      State      Size Type      SnapLock
Type-----
-----svm_test      still15_vsim_ucs630f_aggr1
online      10.11GB vmdisk  non-snaplock
```

## ONTAPのユーザとロールを手動で作成する

このセクションの手順に従って、JSONファイルを使用せずにユーザとロールを手動で作成します。

1. クラスタのクラスタ管理IPアドレスを使用してONTAP System Managerにアクセスします。
2. 管理Privilegesでクラスタにログインします。
  - a. クラスタのONTAP toolsのロールを設定するには、[クラスタ]>\*[ユーザとロール]\*ペインを選択します。
  - b. クラスタSVM ONTAP toolsのロールを設定するには、[ストレージ**SVM**]>\*[ユーザとロール]\*ペインを選択します。
3. ロールの作成：
  - a. テーブルの\*[追加]\*を選択します。
  - b. [ロール名]\*および[ロール属性]\*の詳細を入力します。  
  
[REST API Path]\*と該当するアクセスをドロップダウンから追加します。
  - c. 必要なAPIをすべて追加し、変更を保存します。

#### 4. ユーザの作成：

- a. Users テーブルの Add \*を選択します。
- b. [ユーザの追加]ダイアログボックスで、\*[System Manager]\*を選択します。
- c. [Username]\*を入力します。
- d. 上記の\*ロールの作成\*ステップで作成したオプションから\*ロール\*を選択します。
- e. アクセスを許可するアプリケーションと認証方法を入力します。ONTAPIとHTTPが必要なアプリケーションで、認証タイプは\* Password \*です。
- f. ユーザーの\*パスワード\*とユーザーの\*保存\*を設定します。

#### 管理者以外のグローバルを対象としたクラスタユーザに必要な最小権限のリスト

このセクションには、users JSONファイルを使用せずに作成した管理者以外のグローバル対象のクラスタユーザに必要な最小権限を記載します。クラスタをローカルスコープで追加する場合は、JSONファイルを使用してユーザを作成することを推奨します。ONTAP tools for VMware vSphereでは、ONTAPでのプロビジョニングに読み取り権限だけでは不十分なためです。

#### APIの使用：

| API                                             | アクセスレベル    | 使用目的                                          |
|-------------------------------------------------|------------|-----------------------------------------------|
| /api/クラスタ                                       | 読み取り専用     | クラスタ構成の検出                                     |
| /api/cluster/licensing/licenses                 | 読み取り専用     | プロトコル固有のライセンスのライセンスチェック                       |
| /API /クラスタ/ノード                                  | 読み取り専用     | プラットフォームタイプの検出                                |
| /api/security/accounts<br>(/api/security/アカウント) | 読み取り専用     | 権限の検出                                         |
| /api/security/rolesのように入力します                    | 読み取り専用     | 権限の検出                                         |
| / API /ストレージ/アグリゲート                             | 読み取り専用     | データストア/ボリュームプロビジョニング時のアグリゲートスペースの確認           |
| / API /ストレージ/クラスタ                               | 読み取り専用     | クラスタレベルのスペースと削減率のデータを取得するには                   |
| /API/ストレージ/ディスク                                 | 読み取り専用     | アグリゲートに関連付けられているディスクを取得するには                   |
| /api/storage/qos/policies                       | 読み取り/作成/変更 | QoSとVMポリシーの管理                                 |
| /api/SVM/SVMs                                   | 読み取り専用     | クラスタがローカルに追加された場合にSVMの設定を取得するには、次の手順を実行します。   |
| /api/network/ip/interfaces                      | 読み取り専用     | ストレージバックエンドの追加-管理LIFの範囲がクラスタ/ SVMであることを確認します。 |

## クラスタを対象としたONTAP Tools for VMware vSphere ONTAP APIベースのユーザを作成する



データストアで障害が発生した場合にパッチ処理や自動ロールバックを実行するには、Privilegesの検出、作成、変更、削除が必要です。これらのPrivilegesがすべて揃っていないと、ワークフローの中断やクリーンアップの問題が発生します。

検出、ストレージの作成、ストレージの変更、ストレージの削除を伴うONTAP tools for VMware vSphere ONTAP APIベースのユーザの作成Privilegesを使用すると、検出の開始とONTAP toolsのワークフローの管理が可能になります。

上記のすべてのPrivilegesを使用してクラスタを対象としたユーザを作成するには、次のコマンドを実行します。

```
security login rest-role create -role <role-name> -api  
/api/application/consistency-groups -access all  
  
security login rest-role create -role <role-name> -api  
/api/private/cli/snapmirror -access all  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nfs/export-policies -access all  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystem-maps -access all  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystems -access all  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/igroups -access all  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/lun-maps -access all  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/vvol-bindings -access all  
  
security login rest-role create -role <role-name> -api  
/api/snapmirror/relationships -access all  
  
security login rest-role create -role <role-name> -api  
/api/storage/volumes -access all  
  
security login rest-role create -role <role-name> -api  
"/api/storage/volumes/*/snapshots" -access all  
  
security login rest-role create -role <role-name> -api /api/storage/luns
```

-access all

```
security login rest-role create -role <role-name> -api  
/api/storage/namespaces -access all
```

```
security login rest-role create -role <role-name> -api  
/api/storage/qos/policies -access all
```

```
security login rest-role create -role <role-name> -api  
/api/cluster/schedules -access read_create
```

```
security login rest-role create -role <role-name> -api  
/api/snapmirror/policies -access read_create
```

```
security login rest-role create -role <role-name> -api  
/api/storage/file/clone -access read_create
```

```
security login rest-role create -role <role-name> -api  
/api/storage/file/copy -access read_create
```

```
security login rest-role create -role <role-name> -api  
/api/support/ems/application-logs -access read_create
```

```
security login rest-role create -role <role-name> -api  
/api/protocols/nfs/services -access read_modify
```

```
security login rest-role create -role <role-name> -api /api/cluster  
-access readonly
```

```
security login rest-role create -role <role-name> -api /api/cluster/jobs  
-access readonly
```

```
security login rest-role create -role <role-name> -api  
/api/cluster/licensing/licenses -access readonly
```

```
security login rest-role create -role <role-name> -api /api/cluster/nodes  
-access readonly
```

```
security login rest-role create -role <role-name> -api /api/cluster/peers  
-access readonly
```

```
security login rest-role create -role <role-name> -api /api/name-  
services/name-mappings -access readonly
```

```
security login rest-role create -role <role-name> -api  
/api/network/ethernet/ports -access readonly
```

```
security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly
```

```
security login rest-role create -role <role-name> -api /api/svm/peers  
-access readonly  
  
security login rest-role create -role <role-name> -api /api/svm/svms  
-access readonly
```

また、ONTAPバージョン9.16.0以降の場合は、次のコマンドを実行します。

```
security login rest-role create -role <role-name> -api  
/api/storage/storage-units -access all
```

### ONTAP tools for VMware vSphere ONTAP APIベースのSVMを対象としたユーザを作成する

すべてのPrivilegesを使用してSVMを対象としたユーザを作成するには、次のコマンドを実行します。

```
security login rest-role create -role <role-name> -api  
/api/application/consistency-groups -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/private/cli/snapmirror -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/igroups -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/lun-maps -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/snapmirror/relationships -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/storage/volumes -access all -vserver <vserver-name>
```

```

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/luns
-access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

```

```

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>

```

また、ONTAPバージョン9.16.0以降の場合は、次のコマンドを実行します。

```

security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>

```

上記で作成したAPIベースのロールを使用して新しいAPIベースのユーザを作成するには、次のコマンドを実行します。

```
security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>
```

例：

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_sti160-cluster_
```

アカウントのロックを解除するには、次のコマンドを実行して管理インターフェイスへのアクセスを有効にします。

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

例：

```
security login unlock -username testvpsraall -vserver C1_sti160-cluster
```

## ONTAP tools for VMware vSphere 10.1ユーザから10.3ユーザへのアップグレード

ONTAP tools for VMware vSphere 10.1ユーザが、JSONファイルを使用して作成されたクラスタスコープのユーザである場合は、ONTAP CLIでadminユーザを使用して次のコマンドを実行し、10.3リリースにアップグレードします。

製品機能の場合：

- VSC
- VSCとVASA Provider
- VSCとSRA
- VSC、VASA Provider、SRA：

クラスタPrivileges：

```
security login role create -role <existing-role-name>-cmddirname "vserver nvme namespace show"-access all
```

```
security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem show"-access all
```

```
security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem host show"-access all
```

*security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem map show"-access all*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme show -interface"-access read*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem host add"-access all*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem map add"-access all*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme namespace delete"-access all*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem delete"-access all*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem host remove"-access all*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem map remove"-access all*

ONTAP tools for VMware vSphere 10.1ユーザが、JSONファイルを使用して作成されたSVMスコープのユーザである場合は、ONTAP CLIでadminユーザを使用して次のコマンドを実行し、10.3リリースにアップグレードします。

SVM Privileges :

*security login role create -role <existing-role-name>-cmddirname "vserver nvme namespace show"-access all -vserver <vserver-name>*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem show"-access all -vserver <vserver-name>*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem host show"-access all -vserver <vserver-name>*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem map show"-access all -vserver <vserver-name>*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme show-interface"-access read -vserver <vserver-name>*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem host add"-access all -vserver <vserver-name>*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem map add"-access all -vserver <vserver-name>*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme namespace delete"-access all -vserver <vserver-name>*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem delete"-access all -vserver <vserver-name>*

*security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem host remove"-access all -vserver <vserver-name>*

```
security login role create -role <existing-role-name>-cmddirname "vserver nvme subsystem map remove"-  
access all -vserver <vserver-name>
```

command\_vserver nvme namespace show\_and\_vserver nvme subsystem show\_を既存のロールに追加すると、次のコマンドが追加されます。

```
vserver nvme namespace create  
  
vserver nvme namespace modify  
  
vserver nvme subsystem create  
  
vserver nvme subsystem modify
```

## ストレージバックエンドを追加します

ストレージバックエンドを追加すると、ONTAPクラスタをオンボードできます。

- このタスクについて \*

マルチテナンシーのセットアップで、vCenterが関連付けられたSVMのテナントとして機能する場合は、ONTAP tools Managerを使用してクラスタを追加します。ストレージバックエンドをvCenter Serverに関連付けて、オンボードされたvCenter Serverインスタンスにグローバルにマッピングします。vCenterテナントは、目的のStorage Virtual Machine (SVM) をオンボードする必要があります。これにより、SVMユーザーはvVolデータストアをプロビジョニングできます。SVMを使用してvCenterにストレージを追加できます。

ONTAP toolsのユーザインターフェイスを使用して、ローカルストレージバックエンドをクラスタまたはSVMのクレデンシャルで追加します。これらのストレージバックエンドは1つのvCenterに限定されます。ローカルでクラスタのクレデンシャルを使用すると、関連付けられたSVMがvCenterに自動的にマッピングされてVVOLまたはVMFSが管理されます。SRAを含むVMFSの管理については、ONTAP toolsではグローバルクラスタを必要とせずにSVMクレデンシャルがサポートされます。

## ONTAP tools Managerの使用



マルチテナントセットアップでは、SVMユーザクレデンシャルを使用するために、ストレージバックエンドクラスタをグローバルに、SVMをローカルに追加できます。

### 手順

1. WebブラウザからONTAP Tools Managerを起動します。  
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャルを使用してログインします。
3. サイドバーから\* Storage backends \*を選択します。
4. ストレージバックエンドを追加し、サーバのIPアドレスまたはFQDN、ユーザ名、およびパスワードの詳細を指定します。



IPv4とIPv6のアドレス管理LIFがサポートされます。

## vSphere Clientユーザインターフェイスを使用



vSphere Clientユーザインターフェイスでストレージバックエンドを設定する場合、VVOLデータストアではSVMユーザを直接追加できない点に注意してください。

1. vSphere Clientにログインします。
2. ショートカットページで、プラグインセクションの\* NetApp ONTAP tools \*を選択します。
3. サイドバーから\* Storage backends \*を選択します。
4. ストレージバックエンドを追加し、サーバのIPアドレス、ユーザ名、パスワード、およびポートの詳細を指定します。



SVMユーザを直接追加するには、クラスタベースのクレデンシャルとIPv4およびIPv6アドレス管理LIFを追加するか、SVM管理LIFにSVMベースのクレデンシャルを指定します。

### 次の手順

リストが更新され、新しく追加されたストレージバックエンドがリストに表示されます。

## ストレージバックエンドとvCenter Serverインスタンスの関連付け

ストレージバックエンドをvCenter Serverに関連付けて、ストレージバックエンドとオンボードされたvCenter Serverインスタンスの間にグローバルなマッピングを作成します。

### 手順

1. WebブラウザからONTAP Tools Managerを起動します。

<https://<ONTAPtoolsIP>:8443/virtualization/ui/>

2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャルを使用してログインします。
3. サイドバーから[vCenter]を選択します。
4. ストレージバックエンドに関連付けるvCenter Serverインスタンスの縦の省略記号を選択します。
5. ドロップダウンからストレージバックエンドを選択して、vCenter Serverインスタンスに必要なストレージバックエンドに関連付けます。

## ネットワークアクセスの設定

ネットワークアクセスを設定していない場合は、ESXiホストで検出されたすべてのIPアドレスがデフォルトでエクスポートポリシーに追加されます。いくつかの特定のIPアドレスをエクスポートポリシーに追加して残りのIPアドレスを除外するように設定できます。ただし、除外したESXiホストでマウント処理を実行すると、処理が失敗します。

### 手順

1. vSphere Clientにログインします。
2. プラグインセクションのショートカットページで\* NetApp ONTAP tools \*を選択します。
3. ONTAPツールの左側のペインで、[設定]>\*[編集]\*に移動します。

複数のIPアドレスを追加するには、リストをカンマ、範囲、Classless Inter-Domain Routing (CIDR ; クラスレスドメイン間ルーティング)、またはこれらの組み合わせで区切ります。

4. [ 保存 ( Save ) ] を選択します。

## データストアを作成

ホストクラスタレベルでデータストアを作成すると、データストアが作成されてデステイネーションのすべてのホストにマウントされます。この操作は、現在のユーザに実行権限がある場合にのみ有効になります。

## vVolデータストアを作成する

ONTAP tools for VMware vSphere 10.3以降では、ASA R2システムにvVolデータストアを作成できます。スペース効率はthin.vvolです。VASA Providerでは、VVOLデータストアの作成時にコンテナと必要なプロトコルエンドポイントが作成されます。このコンテナにはバックアップボリュームはありません。

### 開始する前に

- ルートアグリゲートがSVMにマッピングされていないことを確認してください。
- 選択したvCenterにVASA Providerが登録されていることを確認してください。
- ASA R2ストレージシステムでは、SVMユーザのアグリゲートにSVMをマッピングする必要があります。

### 手順

1. vSphere Clientにログインします。
2. ホストシステム、ホストクラスタ、またはデータセンターを右クリックし、\* NetApp ONTAP tools >[Create Datastore]\*を選択します。
3. [VVols]\*[データストアタイプ]\*を選択します。
4. [Datastore name]\*と[Protocol]\*の情報を入力します。



ASA R2システムでは、VVOLのiSCSIプロトコルとFCプロトコルがサポートされません。

5. データストアを作成するStorage VMを選択します。
6. NFSプロトコルのカスタムエクスポートポリシーを選択するか、iSCSIプロトコルとFCプロトコルのカスタムイニシエータグループ名を\*[アドバンスドオプション]\*で選択します。



ASA R2ストレージシステムタイプがSVMの場合、データストアは単なる論理コンテナであるため、ストレージユニット（LUN /ネームスペース）は作成されません。

7. [ストレージ属性]\*ペインで、新しいボリュームを作成するか、既存のボリュームを使用できます。ただし、これら2種類のボリュームを組み合わせるとVVOLデータストアを作成することはできません。

新しいボリュームを作成するときに、データストアでQoSを有効にすることができます。デフォルトでは、LUNが作成される要求ごとに1つのボリュームが作成されます。この手順は、ASA R2ストレージシステムを使用するvVolデータストアには適用されません。

8. ペインで選択内容を確認し、[完了]\*を選択します。

## NFSデータストアを作成する

VMware Network File System (NFS) データストアは、NFSプロトコルを使用して、ESXiホストをネットワーク経由で共有ストレージデバイスに接続します。NFSデータストアはVMware vSphere環境で一般的に使用され、シンプルさや柔軟性など、いくつかの利点があります。

### 手順

1. vSphere Clientにログインします。
2. ホストシステム、ホストクラスタ、またはデータセンターを右クリックし、\* NetApp ONTAP tools >[データストアの作成]\*を選択します。

3. [データストアの種類]\*フィールドで[NFS]を選択します。
4. ペインに、データストア名、サイズ、およびプロトコルの情報を入力します。詳細オプションで[データストアクラスタ]および[Kerberos認証]\*を選択します。



Kerberos認証は、NFS 4.1プロトコルが選択されている場合にのみ使用できます。

5. [ストレージ]ペインで\*と[Storage VM]\*を選択します。
6. 必要に応じて、アドバンスドオプションで\*[カスタムエクスポートポリシー]\*を選択しますが、推奨されません。使用する場合は、すべてのオブジェクトに対してvCenterで検出を実行してください。



SVMのデフォルト/ルートポリシーを使用してNFSデータストアを作成することはできません。

- アドバンスドオプションの\*[非対称]\*トグルボタンは、プラットフォームのドロップダウンでパフォーマンスまたは容量が選択されている場合にのみ表示されます。
  - プラットフォームのドロップダウンで\*[いずれか]\*オプションを選択すると、プラットフォームフラグまたは非対称フラグに関係なくvCenterに属しているSVMが表示されます。
7. ペインで、ボリューム作成用のアグリゲートを選択します。アドバンスドオプションで、必要に応じて[スペースリザベーション]および[QoSを有効にする]\*を選択します。
  8. ペインで選択内容を確認し、[完了]\*を選択します。

NFSデータストアが作成され、すべてのホストにマウントされます。

#### VMFSデータストアの作成

Virtual Machine File System (VMFS) は、VMware vSphere環境に仮想マシンファイルを格納するクラスタファイルシステムです。VMFSを使用すると、複数のESXiホストから同じ仮想マシンファイルに同時にアクセスできるため、vMotionや高可用性などの機能を利用できます。

保護されているクラスタの場合：

- VMFSデータストアのみを作成できます。VMFSデータストアを保護対象のクラスタに追加すると、データストアは自動的に保護されます。
- 保護されているホストクラスタが1つ以上あるデータセンターにデータストアを作成することはできません。
- 親ホストクラスタが「Automated Failover Duplex policy」タイプ（uniform / non-uniform config）の関係で保護されている場合は、ESXiホストにデータストアを作成できません。
- VMFSデータストアは、非同期関係で保護されているESXiホストにのみ作成できます。「自動フェイルオーバーデュプレックス」ポリシーで保護されているホストクラスタの一部であるESXiホストでは、データストアを作成してマウントすることはできません。

開始する前に

- ONTAPストレージ側で各プロトコルのサービスとLIFを有効にします。
- ASA R2ストレージシステムで、SVMユーザ用のアグリゲートにSVMをマッピングします。
- NVMe/TCPプロトコルを使用している場合はESXiホストを設定します。
  - a. を確認します。 ["VMware Compatibility Guide"](#)



VMware vSphere 7.0 U3以降のバージョンでは、NVMe/TCPプロトコルがサポートされます。ただし、VMware vSphere 8.0以降のバージョンを推奨します。

- b. ネットワークインターフェイスカード（NIC）ベンダーがNVMe/TCPプロトコルを使用するESXi NICをサポートしているかどうかを確認します。
  - c. NICベンダーの仕様に従ってESXi NICをNVMe/TCP用に設定します。
  - d. VMware vSphere 7リリースを使用している場合は、VMwareサイトの手順に従って ["NVMe over TCPアダプタ用のVMkernelバインドの設定"](#) NVMe/TCPポートバインドを設定します。VMware vSphere 8リリースを使用している場合は、に従って ["ESXiでのNVMe over TCPの設定"](#) NVMe/TCPポートバインドを設定します。
  - e. VMware vSphere 7リリースの場合は、ページの手順に従って ["NVMe over RDMAまたはNVMe over TCPソフトウェアアダプタの有効化"](#) NVMe/TCPソフトウェアアダプタを設定します。VMware vSphere 8リリースの場合は、に従って ["ソフトウェアNVMe over RDMAまたはNVMe over TCPアダプタの追加"](#) NVMe/TCPソフトウェアアダプタを設定します。
  - f. ["ストレージシステムとホストの検出"](#) ESXiホストでアクションを実行します。詳細については、を参照してください ["VMFSデータストア用にNVMe/TCPをvSphere 8.0 Update 1およびONTAP 9 VMFS.13.1で設定する方法"](#)。
- NVMe/FCプロトコルを使用する場合は、次の手順を実行してESXiホストを設定します。
    - a. ESXiホストでNVMe over Fabrics（NVMe-oF）を有効にします。
    - b. SCSIゾーニングを完了します。
    - c. ESXiホストとONTAPシステムが物理レイヤと論理レイヤで接続されていることを確認します。

ONTAP SVMをFCプロトコル用に設定する方法については、を参照してください ["FC用のSVMの設定"](#)。

VMware vSphere 8.0でNVMe/FCプロトコルを使用する方法の詳細については、を参照してください ["ONTAP を搭載したESXi 8.x向けのNVMe-oFホスト構成"](#)。

VMware vSphere 7.0でNVMe/FCを使用する方法の詳細については ["ONTAP NVMe/FC Host Configuration Guide"](#)、およびを参照して ["TR-4684"](#) ください。

#### 手順

1. vSphere Clientにログインします。
2. ホストシステム、ホストクラスタ、またはデータセンターを右クリックし、\* NetApp ONTAP tools >[Create Datastore]\*を選択します。
3. VMFSデータストアタイプを選択します。
4. [名前とプロトコル]\*ペインで、データストアの名前、サイズ、およびプロトコルの情報を入力します。既存のVMFSデータストアクラスタに新しいデータストアを追加する場合は、[Advanced Options]でデータストアクラスタセクタを選択します。
5. ペインで**Storage VM**を選択します。必要に応じて、[アドバンスドオプション]\*セクションで[カスタムイニシエータグループ名]\*を指定します。データストア用に既存のigroupを選択するか、カスタム名を指定して新しいigroupを作成できます。

NVMe/FCプロトコルまたはNVMe/TCPプロトコルを選択すると、新しいネームスペースサブシステムが作成され、ネームスペースのマッピングに使用されます。ネームスペースサブシステムは、自動生成されたデータストア名を使用して作成されます。[ストレージ]\*ペインの詳細オプションにある\*カスタムネームスペースサブシステム名\*フィールドで、ネームスペースサブシステムの名前を変更

できます。

6. ストレージ属性\*ペインで、次の手順を実行します。

- a. ドロップダウンオプションから\*[アグリゲート]\*を選択します。



ASA R2ストレージシステムでは、ASA R2ストレージは分離型ストレージであるため、\*Aggregate\*オプションは表示されません。ASA R2ストレージシステムタイプのSVMを選択した場合は、ストレージ属性ページにQoSを有効にするためのオプションが表示されます。

- b. 選択したプロトコルに従って、ストレージユニット（LUN/ネームスペース）がシンタイプのスペースリザベーションで作成されます。

- c. 必要に応じて\*、[QoSを有効にする]\*オプションを選択し、詳細を指定します。



ASA R2ストレージタイプでは、ボリュームの作成または選択はストレージユニット（LUN/ネームスペース）の作成には適用されません。したがって、これらのオプションは表示されません。



NVMe/FCまたはNVMe/TCPプロトコルを使用してVMFSデータストアを作成する場合は、既存のボリュームを使用できないため、新しいボリュームを作成する必要があります。

7. ペインでデータストアの詳細を確認し、[終了]\*を選択します。



保護対象のクラスタにデータストアを作成すると、「The datastore is being mounted on a protected Cluster」という読み取り専用メッセージが表示されます。

結果

VMFSデータストアが作成され、すべてのホストにマウントされます。

## 著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

## 商標に関する情報

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