



ONTAP Tools for VMware vSphereの設定

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

目次

| | |
|--|----|
| ONTAP Tools for VMware vSphereの設定 | 1 |
| vCenter Serverインスタンスを追加する | 1 |
| VASA プロバイダを vCenter Server インスタンスに登録する | 1 |
| NFS VAAIプラグインのインストール | 2 |
| ESXiホスト設定を構成する | 3 |
| ESXi サーバーのマルチパスとタイムアウト設定を構成する | 3 |
| ESXiホストの値を設定する | 4 |
| ONTAPユーザーの役割と権限を構成する | 5 |
| SVM集約マッピング要件 | 6 |
| ONTAPユーザーとロールを手動で作成する | 6 |
| ONTAP tools for VMware vSphereを10.3 ユーザーにアップグレードする | 14 |
| ONTAP tools for VMware vSphereを10.4 ユーザー向けにアップグレードする | 16 |
| ストレージバックエンドを追加する | 16 |
| ストレージ バックエンドを vCenter Server インスタンスに関連付ける | 18 |
| ネットワークアクセスを構成する | 19 |
| データストアを作成する | 19 |

ONTAP Tools for VMware vSphereの設定

vCenter Serverインスタンスを追加する

ONTAP tools for VMware vSphereに vCenter Server インスタンスを追加して、vCenter Server 環境内の仮想データストアを構成、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ツールを vCenter と統合すると、プロビジョニング、スナップショット、データ保護などのストレージ タスクを vSphere クライアントから直接実行できるようになり、別のストレージ管理コンソールに切り替える必要がなくなります。

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管理者認証情報を使用してログインします。
3. **vCenter** > **追加** を選択して、vCenter Server インスタンスをオンボードします。vCenter の IP アドレスまたはホスト名、ユーザー名、パスワード、ポートの詳細を入力します。



ONTAPツールに vCenter インスタンスを追加するには、管理者アカウントは必要ありません。管理者アカウントなしで、権限が制限されたカスタム ロールを作成できます。参照["ONTAP tools for VMware vSphereで vCenter Server RBAC を使用する"](#)詳細については。

ONTAPツールに vCenter Server インスタンスを追加すると、次のアクションが自動的にトリガーされます。

- vCenter クライアント プラグインはリモート プラグインとして登録されます。
- プラグインと API のカスタム権限が vCenter Server インスタンスに適用されます。
- ユーザーを管理するためにカスタム ロールが作成されます。
- プラグインは、vSphere ユーザー 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 プロバイダを vCenter Server インスタンスに登録する

ONTAP tools for VMware vSphereを使用して、VASA プロバイダーを vCenter Server インスタンスに登録できます。VASA プロバイダ設定セクションには、選択した vCenter Server の VASA プロバイダ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 クライアントにログインします。
2. プラグイン セクションで、[ショートカット] > [* NetApp ONTAPツール*] を選択します。

3. 設定 > *VASA プロバイダー設定*を選択します。VASA プロバイダーの登録ステータスは未登録として表示されます。
4. *登録*ボタンを選択して、VASA プロバイダーを登録します。
5. VASA プロバイダーの名前と資格情報を入力します。ユーザー名には文字、数字、アンダースコアのみを含めることができます。パスワードの長さは 8 ～ 256 文字にする必要があります。
6. *登録*を選択します。
7. 登録が正常に完了し、ページが更新されると、登録された VASA プロバイダーのステータス、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。

次の手順

オンボードされた VASA プロバイダーが vCenter クライアントの VASA プロバイダーの下にリスト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. 管理者の資格情報を使用してログインします。
3. ストレージ プロバイダー > 構成 を選択します。オンボードされた VASA プロバイダーが正しくリストされていることを確認します。

NFS VAAIプラグインのインストール

NFS vStorage API for Array Integration (NFS VAAI) プラグインは、VMware vSphere と NFS ストレージ ア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 アレイの高度な機能を活用して、特定のストレージ関連の操作を 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

- ダウンロード ["NetApp NFS Plug-in for VMware VAAI"](#) インストール パッケージ。
- ESXi ホストと vSphere 7.0U3 の最新パッチ以降のバージョン、およびONTAP 9.14.1 以降のバージョンがインストールされていることを確認してください。
- NFS データストアをマウントします。

手順

1. vSphere クライアントにログインします。
2. プラグイン セクションで、[ショートカット] > [* NetApp ONTAPツール*] を選択します。
3. 設定 > **NFS VAAI ツール** を選択します。
4. VAAI プラグインが vCenter Server にアップロードされたら、[既存のバージョン] セクションで [変更] 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. 参照して選択 `vib` ファイルを選択し、[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. **ESXi** ホストにインストール 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。vSphere Web Client の最近のタスク セクションでインストールの進行状況を監視できます。

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はNFS VAAI プラグインを自動的に検出し、有効にします。

次の手順

NFS VAAI プラグインをインストールし、ESXi ホストを再起動した後、VAAI コピー オフロード用の正しい NFS エクスポート ポリシーを構成する必要があります。NFS 環境で VAAI を構成する場合は、次の要件を考慮してエクスポート ポリシー ルールを構成します。

- 関連するONTAPボリュームは NFSv4 呼び出しを許可する必要があります。
- ルート ユーザーはルートのままにし、すべてのジャンクション 親ボリュームで NFSv4 を許可する必要があります。
- 関連する NFS サーバーで 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コピーオフロード用の適切なNFSエクスポートポリシーを構成する](#)" KB 記事。

関連情報

["VMware vStorage over NFSのサポート"](#)

["NFSv4.0の有効化または無効化"](#)

["ONTAPでのNFSv4.2のサポート"](#)

ESXiホスト設定を構成する

ESXi サーバーのマルチパスとタイムアウト設定を構成すると、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 サーバーのマルチパスとタイムアウト設定を構成する

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

構成とシステム負荷によっては、このプロセスに長い時間がかかる場合があります。タスクの進捗状況は[Recent Tasks]パネルに表示されます。

手順

1. VMware vSphere Web クライアントのホームページから、*ホストとクラスタ*を選択します。
2. ホストを右クリックし、* NetApp ONTAPツール* > ホスト データの更新 を選択します。

3. VMware vSphere Web クライアントのショートカット ページで、プラグイン セクションの * NetApp ONTAPツール* 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. *推奨設定を適用*リンクを選択します。
6. 推奨ホスト設定の適用 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 ホストを展開して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。最近のタスク パネルで進行状況を追跡できます。

ESXiホストの値を設定する

ONTAP tools for VMware vSphereを使用して、ESXi ホスト上でタイムアウトやその他の値を設定することで、最高のパフォーマンスとフェイルオーバーの成功を確保できます。ONTAP tools for VMware vSphereが設定する値は、NetApp の内部テストに基づいています。

次に示すESXiホストの値を設定できます。

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 設定は、NetAppストレージ システムの優先パスを定義します。利用可能なパスのうちどれが最適化されているか (相互接続ケーブルを通過する最適化されていないパスとは対照的) を決定し、優先パスをそれらのパスの 1 つに設定します。

高パフォーマンス環境の場合、または単一の LUN データストアでパフォーマンスをテストしている場合は、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 設定の 1000 から値 1 に変更することを検討してください。



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

NFS設定

| パラメータ | この値を次のように設定します... |
|-------------------|-------------------|
| 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ユーザーの役割と権限を構成する

ONTAP tools for VMware vSphereおよびONTAP System Manager 用の ONTAP ツールに付属の JSON ファイルを使用して、ストレージ バックエンドを管理するための新しいユーザー ロールと権限を設定できます。

開始する前に

- https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip を使用して、ONTAP tools for VMware vSphereからONTAP権限ファイルをダウンロードしておく必要があります。
- ONTAPツールからONTAPPrivilegesファイルをダウンロードしておく必要があります。
https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip。



ユーザーは、クラスターで作成することも、ストレージ仮想マシン (SVM) レベルで直接作成することもできます。user_roles.json ファイルを使用せずにユーザーを作成することもできますが、その場合は SVM レベルで最小限の権限セットが必要です。

- 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://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip ファイルを解凍します。
2. クラスターのクラスタ管理 IP アドレスを使用してONTAP System Manager にアクセスします。
3. 管理者権限でクラスターにログインします。ユーザーを構成するには、次の手順を実行します。
 - a. クラスタONTAPツール ユーザーを構成するには、[クラスタ] > [設定] > [ユーザーとロール] ペインを選択します。
 - b. SVM ONTAPツール ユーザーを構成するには、[ストレージ **SVM**] > [設定] > [ユーザーとロール] ペインを選択します。
 - c. [ユーザー]の下の[追加]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*して、ONTAPPrivilegesJSON ファイルを選択してアップロードします。

製品フィールドは自動的に入力されます。

- f. ドロップダウンから製品機能として*VSC、VASA プロバイダー、および SRA*を選択します。

役割 フィールドは、選択した製品の機能に基づいて自動的に入力されます。

- g. 必要なユーザ名とパスワードを入力します。
- h. ユーザーに必要な権限 (検出、ストレージの作成、ストレージの変更、ストレージの破棄、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ーが追加され、設定したロールの詳細な権限を確認できます。

SVM集約マッピング要件

データストアのプロビジョニングに SVM ユーザー認証情報を使用するために、ONTAP tools for VMware vSphereは内部的に、データストア POST API で指定されたアグリゲート上にボリュームを作成します。ONTAP、SVM ユーザー認証情報を使用して、SVM 上のマッピングされていないアグリゲート上にボリュームを作成することはできません。これを解決するには、ここで説明するように、ONTAP REST API または CLI を使用して SVM をアグリゲートに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ユーザーとロールを手動で作成する

JSON ファイルを使用せずにユーザーとロールを手動で作成するには、このセクションの指示に従います。

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. 管理者権限でクラスターにログインします。
 - a. クラスタONTAPツールのロールを設定するには、クラスタ > 設定 > ユーザーとロール ペインを選択します。
 - b. クラスタSVM ONTAPツールのロールを設定するには、ストレージ**SVM** > 設定 > *ユーザーとロール* ペインを選択します。
3. ロールの作成:
 - a. *ロール*テーブルの下に*追加*を選択します。
 - b. *ロール名*と*ロール属性*の詳細を入力します。

ドロップダウンから*REST API パス*とそれぞれのアクセスを追加します。

c. 必要な API をすべて追加し、変更を保存します。

4. ユーザーの作成:

- a. *ユーザー*テーブルの下で*追加*を選択します。
- b. *ユーザーの追加*ダイアログボックスで、*システムマネージャ*を選択します。
- c. *ユーザー名*を入力します。
- d. 上記の*ロールの作成*手順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。必要なアプリケーションは ONTAPI と HTTP で、認証タイプは パスワード です。
- f. *ユーザーのパスワード*を設定し、ユーザーを*保存*します。

管理者以外のグローバル スコープのクラスタ ユーザーに必要な最小限の権限のリスト

このセクションでは、ユーザーJSONファイルを使用せずに作成された、管理者以外のグローバルスコープのクラスタユーザーに必要な最小限の権限について説明します。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ーを作成することをお勧めします。これは、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以上の権限が必要になるためです。

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/ライセンス/ライセンス | 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/cluster/nodes | 読み取り専用 | プラットフォームタイプの検出 |
| /api/セキュリティ/アカウント | 読み取り専用 | 特権の発見 |
| /api/セキュリティ/ロール | 読み取り専用 | 特権の発見 |
| /api/ストレージ/集約 | 読み取り専用 | データストア/ボリュームのプロビジョニング中の合計スペースチェック |
| /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効率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たディスクを取得するには |
| /api/storage/qos/ポリシー | 読み取り/作成/変更 | QoSとVMポリシー管理 |
| /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 構成を取得します。 |
| /api/ネットワーク/ip/インターフェース | 読み取り専用 | ストレージバックエンドの追加 - 管理LIFスコープがクラスタ/SVMであることを確認する |
| /api/storage/可用性ゾーン | 読み取り専用 | SAZディスクバリエーション。ONTAP 9.16.1 リリース以降およびASA r2 システムに適用されます。 |

VMware vSphere ONTAP API ベースのクラスター スコープ ユーザー ONTAP tools for VMware vSphereを作成する



データストアで障害が発生した場合に PATCH 操作と自動ロールバックを実行するには、検出、作成、変更、および破棄のPrivilegesが必要です。これらすべての権限が不足すると、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、ストレージの破棄の権限を持つ ONTAP tools for VMware vSphere ONTAP API ベースのユーザー用の ONTAP ツールを作成すると、検出を開始し、ONTAP ツール ワークフローを管理できるようになります。

上記のすべての権限を持つクラスター スコープ ユーザーを作成するには、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
```

さらに、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バージョン 9.16.1 以降のASAr2 システムの場合は、次のコマンドを実行します。

```
security login rest-role create -role <role-name> -api  
/api/storage/availability-zones -access readonly
```

VMware vSphere ONTAP API ベースの SVM スコープ ユーザーONTAP tools for VMware vSphereを作成する

すべての権限を持つ SVM スコープ ユーザーを作成するには、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>

```

さらに、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 ベースのユーザーを作成するには、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_stil60-cluster_
```

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

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

例：

```
security login unlock -username testvpsraall -vserver C1_stil60-cluster
```

ONTAP tools for VMware vSphereを10.3 ユーザーにアップグレードする

JSON ファイルを使用して作成されたクラスター スコープのユーザーを持つONTAP tools for VMware vSphere の場合は、ユーザー管理者権限で次のONTAP CLI コマンドを使用して 10.3 リリースにアップグレードします。

製品の機能について：

- VSC
- VSCおよびVASAプロバイダー
- VSCおよびSRA
- VSC、VASA プロバイダー、および SRA。

クラスター権限：

security login role create -role <既存のロール名> -cmddirname "vserver nvme namespace show" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem show" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem host show" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem map show" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme show-interface" -access read

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem host add" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem map add" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme namespace delete" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem delete" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem host remove" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem map remove" -access all

json ファイルを使用して作成された SVM スコープ ユーザーを持つ ONTAP tools for VMware vSphere の場合は、管理者ユーザー権限で ONTAP CLI コマンドを使用して 10.3 リリースにアップグレードします。

SVM 権限:

security login role create -role <既存のロール名> -cmddirname "vserver nvme namespace show" -access all -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem show" -access all -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem host show" -access all -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem map show" -access all -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme show-interface" -access read -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem host add" -access all -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem map add" -access all -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme namespace delete" -access all

`-vserver <vserver-name>`

`security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem delete" -access all
-vserver <vserver-name>`

`security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem host remove"
-access all -vserver <vserver-name>`

`security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem map remove"
-access all -vserver <vserver-name>`

既存のロールにコマンド `vserver nvme namespace show` と `vserver nvme subsystem show` を追加すると、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
```

ONTAP tools for VMware vSphereを10.4 ユーザー向けにアップグレードする

ONTAP 9.16.1 以降では、ONTAP tools for VMware vSphereを10.4 ユーザーにアップグレードします。

JSON ファイルとONTAPバージョン 9.16.1 以上を使用して作成されたクラスター スコープ ユーザーを持つONTAP tools for VMware vSphereの場合は、管理者ユーザー権限でONTAP CLI コマンドを使用して 10.4 リリースにアップグレードします。

製品の機能について:

- VSC
- VSCおよびVASAプロバイダー
- VSCおよびSRA
- VSC、VASA プロバイダー、および SRA。

クラスター権限:

```
security login role create -role <existing-role-name> -cmddirname "storage  
availability-zone show" -access all
```

ストレージバックエンドを追加する

ストレージ バックエンドを追加すると、ONTAPクラスターをオンボードできるようになります。

このタスクについて

vCenter が関連付けられた SVM を持つテナントとして機能するマルチテナント設定の場合は、ONTAP ツール マネージャ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プします。vCenter テナントは、必要なストレージ仮想マシン (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 vVols データストアをプロビジョニングできるようになります。SVM を使用して vCenter にストレージを追加できます。

ONTAP ツールのユーザー インターフェイスを使用して、クラスタまたは SVM 認証情報を持つローカル ストレージ バックエンドを追加します。これらのストレージ バックエンドは、単一の vCenter に制限されます。クラスタ認証情報をローカルで使用する場合、関連付けられた SVM は自動的に vCenter にマッピングされ、vVols または VMFS を管理します。SRA を含む VMFS 管理の場合、ONTAP ツールはグローバル クラスタを必要とせずに SVM 認証情報をサポートします。

ONTAPツールマネージャの使用



マルチテナント設定では、ストレージ バックエンド クラスターをグローバルに追加し、SVM をローカルに追加して、SVM ユーザー資格情報を使用できます。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. サイドバーから*ストレージ バックエンド*を選択します。
4. ストレージ バックエンドを追加し、サーバーの IP アドレスまたは FQDN、ユーザー名、およびパスワードの詳細を指定します。



IPv4 および IPv6 アドレス管理 LIF がサポートされています。

vSphere クライアント ユーザー インターフェイスの使用



vSphere クライアント ユーザー インターフェイスを通じてストレージ バックエンドを構成する場合、vVolsデータストアでは SVM ユーザーの直接追加がサポートされていないことに注意することが重要です。

1. vSphere クライアントにログインします。
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ツール* を選択します。
3. サイドバーから*ストレージ バックエンド*を選択します。
4. ストレージ バックエンドを追加し、サーバーの IP アドレス、ユーザー名、パスワード、ポートの詳細を指定します。



SVM ユーザーを直接追加するには、クラスターベースの認証情報と IPv4 および IPv6 アドレス管理 LIF を追加するか、SVM 管理 LIF を使用して SVM ベースの認証情報を提供します。

次は何？

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 バックエンドを vCenter Server インスタンスに関連付ける

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 インスタンス間のマッピングをグローバルに作成します。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。

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

2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報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 インスタンスに対して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、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を構成する

ネットワーク アクセスを構成していない場合は、ESXi ホストから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。特定の IP アドレスをいくつかエクスポート ポリシーに追加し、残りを除外するように構成できます。ただし、除外された ESXi ホストでマウント操作を実行すると、操作は失敗します。

手順

1. vSphere クライアントにログインします。
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ツール* を選択します。
3. ONTAPツールの左側のペインで、設定 > ネットワーク アクセスの管理 > 編集 に移動します。

複数の IP アドレスを追加するには、リストをコンマ、範囲、クラスレス ドメイン間ルーティング (CIDR)、またはこれら 3 つすべての組み合わせで区切ります。

4. *保存*を選択します。

データストアを作成する

ホスト クラスター レベルでデータストアを作成すると、データストアは宛先のすべてのホストに作成されてマウントされ、現在のユーザーに実行権限がある場合にのみアクションが有効になります。

vCenter Server および**ONTAP**ツールで管理されるデータストアを備えたネイティブ データストア間の相互運用性

ONTAP tools for VMware vSphereは、データストアに固有の親 igroup とホストにマップされた子 igroup を持つ、データストアのネストされた igroup を作成します。ONTAPシステム マネージャからフラット igroup を作成し、それを使用してONTAPツールを使用せずに VMFS データストアを作成できます。参照 ["SANイニシエータとigroupを管理する"](#)詳細についてはこちらをご覧ください。

ストレージがONTAPツールにオンボードされ、データストア検出が実行されると、フラット igroup と VMFS データストアはONTAPツールによって管理され、ネストされた igroup に変換されます。以前のフラット igroup を使用して新しいデータストアを作成することはできません。ネストされた igroup を再利用するには、ONTAPツールのユーザ インターフェイスまたは REST API を使用する必要があります。

vVolsデータストアを作成する

ONTAP tools for VMware vSphere以降では、スペース効率の高い thin.vVol としてASA r2 システム上にvVolsデータストアを作成できます。VASA プロバイダーは、vVol データストアを作成するときに、コンテナと必要なプロトコル エンドポイントを作成します。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 にマップされていないことを確認します。
- 選択した vCenter に VASA プロバイダーが登録されていることを確認します。
- ASA r2 ストレージ システムでは、SVM を SVM ユーザーのアグリゲートにマッピングする必要があります。

手順

1. vSphere クライアントにログインします。
2. ホスト システム、ホスト クラスター、またはデータ センターを右クリックし、* NetApp ONTAP ツール* > データストアの作成 を選択します。
3. vVols *データストア タイプ*を選択します。
4. *データストア名*と*プロトコル*情報を入力します。



ASA r2 システムは、vVolsの iSCSI および FC プロトコルをサポートしています。

5. データストアを作成するストレージ VM を選択します。
6. 詳細オプション:
 - カスタム エクスポート ポリシー を選択した場合は、すべてのオブジェクトに対して vCenter で検出を実行するようにしてください。このオプションは使用しないことをお勧めします。
 - iSCSI および FC プロトコルに対して カスタム イニシエーター グループ 名を選択できます。



ASA r2 ストレージ システム タイプ SVM では、データストアは論理コンテナにすぎないため、ストレージ ユニット (LUN/名前空間) は作成されません。

7. ストレージ属性 ペインでは、新しいボリュームを作成したり、既存のボリュームを使用したりできます。ただし、これら 2 種類のボリュームを組み合わせるとvVols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 を有効にできます。デフォルトでは、LUN 作成要求ごとに 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vVolsデータストアには適用されません。

8. 概要 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 ネットワーク ファイル システム (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ており、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 クライアントにログインします。
2. ホスト システム、ホスト クラスター、またはデータ センターを右クリックし、* NetApp ONTAP ツール* > * データストアの作成* を選択します。
3. データストア タイプ フィールドで NFS を選択します。
4. 名前とプロトコル ペインにデータストアの名前、サイズ、プロトコル情報を入力します。詳細オプションで*データストア クラスター*と*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 プラットフォーム と ストレージ **VM** を選択します。
6. 詳細オプションで カスタム エクスポート ポリシー を選択した場合は、vCenter ですべてのオブジェクトの検出を実行します。このオプションは使用しないことをお勧めします。



SVM のデフォルト/ルート ボリューム 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。

- 詳細オプションでは、プラットフォーム 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、非対称 トグル ボタンが表示されます。
 - プラットフォーム ドロップダウンで 任意 オプションを選択すると、プラットフォームや非対称フラグに関係なく、vCenter の一部である SVM が表示されます。
7. ストレージ属性 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。詳細オプションで、必要に応じて スペース予約 と **QoS** の有効化 を選択します。
 8. 概要 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 データストアを作成する

仮想マシン ファイル システム (VMFS) は、VMware vSphere 環境で仮想マシン ファイルを保存するクラスター化されたファイル システムです。VMFS を使用すると、複数の ESXi ホストが同じ仮想マシン ファイルに同時にアクセスできるようになり、vMotion や高可用性などの機能が有効になります。

保護されたクラスターの場合:

- VMFS データストアのみを作成できます。保護されたクラスターに VMFS データストアを追加すると、データストアは自動的に保護されます。
- 1 つ以上の保護されたホスト クラスターを持つ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 クラスターが「自動フェイルオーバー デュプレックス ポリシー」タイプ (均一/非均一構成) の関係で保護されている場合、ESXi ホストにデータストアを作成することはできません。
- VMFS データストアは、非同期関係によって保護された ESXi ホスト上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」ポリシーによって保護されているホスト クラスターの一部である ESXi ホスト上に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 システム内の SVM ユーザーのアグリゲートに SVM をマップします。
- NVMe/TCP プロトコルを使用している場合は、ESXi ホストを構成します。
 - a. レビュー ["VMware 互換性ガイド"](#)



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ています。ただし、VMware vSphere 8.0 以降のバージョンが推奨されます。

- 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 プロトコルを使用した ESXi NIC をサポートしているかどうかを検証します。
 - c. NIC ベンダーの仕様に従って、ESXi NIC を NVMe/TCP 用に構成します。
 - d. VMware vSphere 7リリースを使用する場合は、VMwareサイトの指示に従ってください。 ["NVMe over TCP アダプタの VMkernel バインディングを構成する"](#) NVMe/TCP ポート バインディングを構成します。 VMware vSphere 8リリースを使用する場合は、 ["ESXi での NVMe over TCP の構成"](#)、NVMe/TCP ポート バインディングを構成します。
 - e. VMware vSphere 7リリースの場合は、次のページの手順に従ってください。 ["NVMe over RDMA または NVMe over TCP ソフトウェア アダプターを有効にする"](#) NVMe/TCP ソフトウェア アダプターを構成します。 VMware vSphere 8リリースについては、 ["ソフトウェア NVMe over RDMA または NVMe over TCP アダプターを追加する"](#) NVMe/TCP ソフトウェア アダプターを構成します。
 - f. 走る["ストレージ システムとホストの検出"](#)ESXi ホストでのアクション。 ["vSphere 8.0 Update 1 およびONTAP 9.13.1 を使用して VMFS データストアに NVMe/TCP を構成する方法"](#)。
- NVMe/FC プロトコルを使用している場合は、次の手順を実行して ESXi ホストを構成します。
 - a. まだ有効になっていない場合は、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システムが物理層と論理層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には、 ["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、以下を参照してください。 ["ONTAPを使用した ESXi 8.x 向け 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、以下を参照してください。 ["ONTAP NVMe/FC ホスト構成ガイド"](#)そして ["TR-4684"](#)。

手順

1. vSphere クライアントにログインします。
2. ホスト システム、ホスト クラスター、またはデータ センターを右クリックし、* NetApp ONTAP ツール* > データストアの作成 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 ペインにデータストアの名前、サイズ、プロトコル情報を入力します。新しいデータストアを既存の VMFS データストア クラスターに追加する場合は、[詳細オプション] の下にあるデータストア クラスター セレクタを選択します。
5. ストレージ ペインでストレージ VM を選択します。必要に応じて、[詳細オプション] セクションに

カスタム イニシエーター グループ名 を入力します。データストアに既存の igroup を選択するか、カスタム名で新しい igroup を作成することができます。

NVMe/FC または NVMe/TCP プロトコルを選択すると、新しい名前空間サブシステムが作成され、名前空間マッピングに使用されます。名前空間サブシステムは、データストア名を含む自動生成された名前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の カスタム名前空間サブシステム名 フィールドで、名前空間サブシステムの名前を変更できます。

6. ストレージ属性 ペインから:

- a. ドロップダウン オプションから **Aggregate** を選択します。



ASA r2ストレージシステムの場合、ASA r2ストレージは分散ストレージであるため、「アグリゲート」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を選択すると、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、thin タイプのスペース予約を持つストレージ ユニット (LUN/名前空間) が作成されます。



ONTAP 9.16.1 以降、ASA r2 ストレージ システムはクラスタごとに最大 12 個のノードをサポートします。

- c. 異機種クラスタである 12 ノード SVM を備えたASA r2 ストレージ システムの パフォーマンス サービス レベル を選択します。選択した SVM が同種クラスタであるか、SVM ユーザーを使用している場合、このオプションは使用できません。

「Any」はデフォルトのパフォーマンス サービス レベル (PSL) 値です。この設定では、ONTAP バランス配置アルゴリズムを使用してストレージ ユニットが作成されます。ただし、必要に応じてパフォーマンス オプションまたはエクストリーム オプションを選択できます。

- d. 必要に応じて、「既存のボリュームを使用する」および「QoS を有効にする」オプションを選択し、詳細を入力します。



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 ユニットの作成 (LUN/名前空間) 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。



既存のボリュームを使用して NVMe/FC または NVMe/TCP プロトコルで VMFS 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必要があります。

7. 概要 ペインでデータストアの詳細を確認し、完了 を選択します。



保護されたクラスタ上にデータストアを作成すると、「データストアは保護されたクラスタにマウントされています。」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。