ONTAP Tools for VMware vSphereの設定

ONTAP tools for VMware vSphere 10

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/ontap-tools-vmware-vsphere-10/configure/add-vcenter.html on September 29, 2025. Always check docs.netapp.com for the latest.

目次

ONTAP Tools for VMware vSphereの設定 . . . 1
ONTAPツールにvCenter Serverインスタンスを追加する . . . 1
ONTAPツールを使用して VASA プロバイダを vCenter Server インスタンスに登録する . . . 1
ONTAPツールを使用して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
ONTAP tools for VMware vSphere 10.3ユーザから10.4ユーザへのアップグレード . . . 16
ONTAPツールにストレージバックエンドを追加する . . . 17
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 . . . 19
ネットワークアクセスの設定 . . . 19
データストアを作成 . . . 20

ONTAP Tools for VMware vSphereの設定

ONTAPツールにvCenter Serverインスタンスを追加する

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。

タスクの内容

ONTAPツールは vCenter Server と統合され、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します。

手順

1. Web ブラウザを開き、次の URL にアクセスします。
   `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。
4. 詳細オプションで、vCenter Server 証明書を自動的に取得 (承認) するか、手動でアップロードします。

> 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。

- ONTAPツールは、vCenter クライアント プラグインをリモート プラグインとして登録します。
- 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。

ONTAPツールを使用して 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します。これにより、ストレージ ポリシー ベースの管理、 vVolsサポート、 ONTAPシステム上の VMware Live Site Recovery アプライアンスとの統合が可能になります。

VASA プロバイダ設定には、選択した vCenter Server の登録ステータスが表示されます。

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. 設定 > *VASA プロバイダー設定*を選択します。 ONTAPツールでは、VASA プロバイダの登録ステータスが未登録として表示されます。
4. [登録]*ボタンを選択してVASA Providerを登録します。
5. VASA 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。パスワードの長さを 8 文字から 256 文字の間で設定します。
6. [*Register] 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、 ONTAPツールには登録済みの 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。

次の手順

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。

ONTAPツールを使用して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 を NFS ストレージ アレイに接続します。 ONTAP tools for VMware vSphereを使用してVAAIプラグインをインストールします。これにより、ESXiホストの代わりにNFSストレージアレイが特定のストレージ操作を処理できるようになります。

作業を開始する前に

- 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 にすでにアップロードしている場合は、*既存のバージョン*で*変更*を選択します。まだアップロードしていない場合は、[アップロード] 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。

   vSphere Web Client には、プラグインをインストールできる ESXi ホストのみが表示されます。インストールの進行状況は「最近のタスク」セクションで確認できます。

7. インストール後にESXiホストを手動で再起動します。

   ESXi ホストを再起動すると、 ONTAP tools for VMware vSphereNFS VAAI プラグインが自動的に検出され、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、ESXi ホストを再起動した後、VAAI コピー オフロードの NFS エクスポート ポリシーを構成します。エクスポート ポリシー ルールが次の要件を満たしていることを確認します。

- 関連するONTAPボリュームは NFSv4 呼び出しを許可します。
- ルート ユーザーはルートのままとなり、すべてのジャンクション親ボリュームで NFSv4 が許可されます。
- VAAI サポートのオプションは、関連する NFS サーバーで設定されます。

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" KB 記事。

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 サーバーのマルチパスとタイムアウト設定を構成すると、データの可用性と整合性を維持するのに役立ちます。プライマリ パスが使用できなくなった場合に、バックアップ ストレージ パスへの自動フェイルオーバーが可能になります。

ESXiサーバのマルチパスとタイムアウトの設定

VMware vSphere 用の ONTAP ツールは、 ESXi ホストのマルチパス設定と HBA タイムアウト設定をチェックし、ネットアップストレージシステムに最も適した設定を行います。

タスクの内容

設定とシステム負荷によっては、このプロセスに時間がかかる場合があります。 「最近のタスク」パネルで進行状況を確認できます。

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]*を選択します。

2. 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。
3. 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。
4. [推奨設定の適用]*リンクを選択します。
5. 推奨ホスト設定の適用 ウィンドウで、 NetApp推奨設定を使用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。

6. 設定ページで、必要に応じて推奨値を選択します。
7. 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を使用して、ESXi ホストのタイムアウトやその他の値を設定し、最適なパフォーマンスとフェイルオーバーを実現します。これらの値はNetAppテストに基づいて設定されます。

ESXi ホストでは、次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 システムに最適なパスを選択します。 MPIO 設定では最適なパスを選択して使用します。

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) の負荷分散設定を調整してパフォーマンスを向上させます。デフォルトの IOPS 値を 1000 から 1 に設定します。

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だ
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

ONTAP tools for VMware vSphereおよびONTAP System Manager 用の ONTAP ツールの JSON ファイルを使用して、ストレージ バックエンドのユーザー ロールと権限を構成します。

作業を開始する前に

- *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* を使用して、 ONTAP tools for VMware vSphereからONTAPPrivilegesファイルをダウンロードします。 zip ファイルをダウンロードすると、2 つの JSON ファイルが見つかります。 ASA r2 システムを構成するときは、 ASA r2 固有の JSON ファイルを使用します。

> ユーザーは、クラスター レベルまたはストレージ仮想マシン (SVM) レベルで直接作成できます。 user_roles.json ファイルを使用しない場合は、ユーザーに必要な最小限の SVM 権限があることを確認してください。

- ストレージ バックエンドの管理者権限でログインします。

手順

1. ダウンロードした *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* ファイルを抽出します。
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:
   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。
   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*して、 ONTAPPrivilegesJSON ファイルを選択してアップロードします。 ASA r2 以外のシステムの場合は users_roles.json ファイルを選択し、 ASA r2 システムの場合は users_roles_ASAr2.json ファイルを選択します。

      ONTAPツールは、製品フィールドに自動的に入力します。

   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。

ONTAPツールは、選択した製品の機能に基づいて **Role** フィールドに自動的に入力します。

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。

ONTAPツールは新しいロールとユーザーを追加します。設定したロールの権限を表示できます。

SVMアグリゲートのマッピングの要件

SVM ユーザー認証情報を使用してデータストアをプロビジョニングする場合、 ONTAP tools for VMware vSphereは、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 ユーザーが SVM にマップされていないアグリゲート上にボリュームを作成できないようにします。ボリュームを作成する前に、 ONTAP REST API または CLI を使用して SVM を必要なアグリゲートにマッピングします。

REST API：

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

ONTAP CLI：

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver        Aggregate      State         Size Type    SnapLock
Type-------------- -------------- ------- ---------- -------
--------------svm_test       sti115_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

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 を選択します。
   b. クラスター 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 を選択します。
3. ロールを作成します。
   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 パス を追加し、ドロップダウン リストからアクセスを選択します。

c. 必要なAPIをすべて追加し、変更を保存します。

4. ユーザーを作成します:

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

このセクションでは、JSON ファイルのない管理者以外のグローバル スコープのクラスター ユーザーに必要な最小限の権限を示します。クラスタがローカル スコープ内にある場合、 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なため、JSON ファイルを使用してユーザを作成します。

API を使用して機能にアクセスできます。

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（/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/ボリュームのプロビジョニング中の集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/policies	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	クラスターがローカルに追加されたときに SVM 構成を取得します。
/api/network/ip/interfaces	読み取り専用	ストレージバックエンドを追加 - 管理LIFスコープがクラスタ/SVMであることを確認する

/api/ストレージ/アベイラビリティゾーン	読み取り専用	SAZ発見。 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。
/api/cluster/メトロクラスタ	読み取り専用	MetroCluster のステータスと構成の詳細を取得します。

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

> データストアでの PATCH 操作と自動ロールバックには、検出、作成、変更、および破棄の権限が必要です。権限がないと、ワークフローやクリーンアップの問題が発生する可能性があります。

検出、作成、変更、および破棄の権限を持つONTAP API ベースのユーザーは、 ONTAPツールのワークフローを管理できます。

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

security login rest-role create -role <role-name> -api
/api/cluster/metrocluster -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バージョン9.16.1以降のASA R2システムでは、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
```

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>
```

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_
```

次のコマンドを実行して、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

JSONファイルを使用して作成されたクラスタを対象としたユーザのONTAP tools for VMware vSphere 10.1ユーザの場合は、次のONTAP CLIコマンドをユーザadmin Privilegesで使用して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

JSONファイルを使用して作成されたSVMを対象としたユーザを持つONTAP tools for VMware vSphere 10.1ユーザの場合は、管理ユーザPrivilegesを指定してONTAP CLIコマンドを使用し、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>

次のコマンドを有効にするには、コマンド *vserver nvme namespace show* と *vserver nvme subsystem show* を既存のロールに追加します。

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

ONTAP tools for VMware vSphere 10.3ユーザから10.4ユーザへのアップグレード

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ファイルおよびONTAPバージョン9.16.1以降を使用して作成されたクラスタを対象としたユーザを含むONTAP tools for VMware vSphere 10.3ユーザの場合は、管理者ユーザPrivilegesを指定してONTAP CLIコマンドを使用し、10.4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 "storage
availability-zone show" -access all
```

ONTAPツールにストレージバックエンドを追加する

ONTAPツールにストレージ バックエンドを追加すると、vCenter Server から直接データストアをプロビジョニングおよび管理できます。

ストレージ バックエンドをローカルに追加するには、 ONTAPツール インターフェイスでクラスタまたは SVM の認証情報を使用します。これらのストレージ バックエンドは、選択した vCenter Server でのみ使用できます。 ONTAPツールは、 vVolsまたは VMFS データストアの管理のために SVM を vCenter Server にマッピングします。 VMFS データストアおよび SRA ワークフローでは、グローバルにマップされたクラスターを必要とせずに SVM 資格情報を使用できます。

ONTAPツール マネージャーでONTAPクラスター認証情報を使用して、グローバル ストレージ バックエンドを追加できます。グローバル ストレージ バックエンドにより、vVol 管理に必要なクラスター リソースを識別する検出ワークフローが可能になります。マルチテナント設定では、SVM ユーザーをローカルに追加してvVolsデータストアを管理できます。

ONTAPシステムでMetroClusterサポートを有効にする場合は、ソース クラスタと宛先クラスタの両方をローカルまたはグローバル ストレージ バックエンドとしてオンボードします。

作業を開始する前に

証明書に有効なサブジェクト別名 (SAN) フィールドが含まれていることを確認します。 ONTAPシステムは、SAN フィールドを使用してクラスタおよび SVM 管理 LIF を識別します。

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。

5. ONTAPクラスタ証明書を自動的に取得して承認するか、証明書の場所を参照して手動でアップロードします。

   > 必要に応じて、メンテナンス コンソールからサブジェクト別名 (SAN) 検証を無効にすることができます。手順については、"証明書検証フラグを変更する" 。

6. 追加するストレージ バックエンドがMetroCluster構成の一部である場合、 ONTAP Tools Manager はピア クラスタを追加するためのポップアップ メッセージが表示されます。 *追加*を選択し、MetroClusterピア ストレージ バックエンドの詳細を入力します。

   > ONTAPシステムがスイッチオーバーとスイッチバックを実行した後、 ONTAPツールの検出を手動で実行します。

vSphere Clientユーザインターフェイスを使用

> vVolsデータストアは、vSphere クライアント ユーザー インターフェイスを介した SVM ユーザーの直接追加をサポートしていません。

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。

   > IPv4 または IPv6 管理 LIF でクラスターベースの認証情報を使用してストレージ バックエンドを追加できます。 SVM ユーザーを直接追加するには、SVM 管理 LIF とともに SVM ベースの認証情報を指定します。クラスターがすでにオンボードされている場合は、そのクラスターから SVM ユーザーを再度オンボードすることはできません。

5. ONTAPクラスタ証明書を自動的に取得して承認するか、証明書の場所を参照して手動でアップロードします。
6. 追加されたストレージ バックエンドがMetroCluster構成の一部である場合、 ONTAPツールは * MetroClusterピアの追加* 画面を表示します。ピア ストレージ バックエンドを追加するには、[ピアの追加] を選択します。

> ONTAPシステムがスイッチオーバーとスイッチバックを実行した後、 ONTAPツールの検出を手動で実行します。

次の手順

ONTAPツールはリストを更新し、新しいストレージ バックエンドを表示します。

ONTAPツールは、ストレージ バックエンド ページに新しく追加されたストレージ バックエンドをリストします。証明書の有効期限が 30 日以内に切れる場合、 ONTAPツールは証明書の有効期限列に警告を表示します。有効期限が切れると、ストレージ システムに接続できなくなるため、 ONTAPツールはストレージ バックエンドを不明としてマークします。

関連情報

"クラスタをMetroCluster構成に設定"

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

すべての vCenter Server インスタンスのアクセスを有効にするには、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ます。 MetroCluster構成の場合、ストレージ バックエンド クラスタを関連付けるときに、そのピア クラスタも vCenter Server に関連付けるようにしてください。

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 バックエンドに接続する vCenter Server インスタンスの横にある縦の省略記号を選択します。
5. ドロップダウン メニューから、選択した vCenter Server インスタンスに関連付けるストレージ バックエンドを選択します。

ネットワークアクセスの設定

ネットワーク アクセスが構成されていない限り、ESXi ホストから検出されたすべての IP アドレスはエクスポート ポリシーに自動的に含まれます。特定の IP アドレスのみを許可し、他の IP アドレスを除外するようにポリシーを構成できます。ただし、除外され

た ESXi ホストからマウントしようとすると、操作は失敗します。

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 > 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、 ONTAPツールによってそれがすべての宛先ホストにマウントされ、必要な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とネイティブ データストア間の相互運用性

ONTAP tools for VMware vSphere以降、 ONTAPツールはデータストアにネストされた igroup を作成します。親 igroup はデータストアに固有のもので、子 igroup はホストにマップされます。 ONTAP System Manager 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。

ストレージをオンボードし、データストアの検出を実行すると、 ONTAPツールは VMFS データストア内のフラット igroup をネストされた igroup に変更します。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 インターフェイスまたは REST API を使用します。

vVol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。 VASA プロバイダーは、このコンテナーにバックアップ ボリュームを割り当てません。

作業を開始する前に

- 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 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 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 Client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. [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す。

5. データストアを作成するStorage VMを選択します。
6. 詳細オプション（advanced options）で：
   - 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プロトコルとFCプロトコルには* Custom initiator group * name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、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て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。 ASA r2 ストレージ システム上のvVolsデータストアの場合は、この手順をスキップします。

8. ペインで選択内容を確認し、[完了]*を選択します。

NFSデータストアを作成する

NFS データストアは、NFS プロトコルを使用して ESXi ホストを共有ストレージに接続します。これらはシンプルで柔軟性があり、VMware vSphere 環境で使用されます。

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. 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 のデフォルトまたはルート 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。

   - アドバンストオプションの*[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 ドロップダウンで **Any** オプションを選択すると、vCenter 内のすべての SVM が表示されます。プラットフォームと非対称フラグは可視性に影響しません。
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。アドバンストオプションで、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。

ONTAPツールは NFS データストアを作成し、それをすべてのホストにマウントします。

VMFSデータストアの作成

VMFS は、仮想マシン ファイルを保存するためのクラスター化されたファイル システムです。 vMotion および高可用性機能のために、複数の ESXi ホストが同じ VM ファイルに同時にアクセスできます。

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。保護されたクラスターに VMFS データストアを追加すると、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「自動フェイルオーバー デュプレックス ポリシー」(均一構成または非均一構成) によって保護されている場合、ESXi ホスト上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。

作業を開始する前に

- 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 プロトコルを使用した 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、NVMe/TCP 用に ESXi NIC を設定します。
  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を検出"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. ESXiホストでNVMe over Fabrics（NVMe-oF）が有効になっていない場合は有効にします。
  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 クラスタに追加するには、[詳細オプション] でデータストア クラスタを選択します。
5. ペインで**Storage VM**を選択します。必要に応じて、**[**アドバンストオプション**]***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 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。 ONTAPツールは、データストア名を含む自動生成された名前を使用してネームスペース サブシステムを作成します。 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 システムの場合、ストレージが分散されているため、**Aggregate** オプションは表示されません。ASA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. ONTAPツールは、選択したプロトコルに基づいて、シン スペース リザーブを持つストレージ ユニット (LUN/名前空間) を作成します。

   > ONTAP 9.16.1以降では、ASA R2ストレージシステムでクラスタあたり最大12ノードがサポートされます。

   c. 異機種混在クラスタで12ノードのSVMを使用するASA R2ストレージシステムの場合は、[パフォーマンスサービスレベル]*を選択します。このオプションは、選択したSVMが同種クラスタの場合、またはSVMユーザを使用している場合は使用できません。

      「any」は、パフォーマンスサービスレベル（PSL）のデフォルト値です。この設定では、ONTAPの分散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、パフォーマンスまたは極端なオプションを選択できます。

   d. 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 プロトコルを使用した VMFS データストアを作成することはできません。 VMFS データストア用の新しいボリュームを作成します。

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

ONTAPツールは VMFS データストアを作成し、それをすべてのホストにマウントします。

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権を有し、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権については、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。