ONTAP Tools for VMware vSphereの設定

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目次

ONTAP Tools for VMware vSphereの設定

vCenter Server インスタンスを ONTAP tools に追加する

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 tools と各 vCenter Server 間のセキュアな通信にはカスタム CA 証明書が必要です。

タスク概要

ONATAPツールはvCenter Serverと統合されており、vSphereクライアントから直接、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実行できます。

vCenter Server インスタンスを ONTAP tools に追加すると、以下のアクションが自動的にトリガーされます：

- ONTAP tools 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 は、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ースのショートカットとして表示されます。

開始する前に

- vCenter Server証明書に、DNSとIPアドレスの両方のエントリを含む有効なサブジェクト代替名（SAN）拡張が含まれていることを確認してください。次に例を示します。

```
X509v3 extensions:
    X509v3 Subject Alternative Name:
        DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
```

  証明書にSAN拡張が含まれていない場合、またはSAN拡張に正しいDNSまたはIPアドレス値が含まれていない場合、証明書検証エラーのため、ONTAP tools for VMware vSphereの操作が失敗する可能性があります。

- vCenter Server のプライマリネットワーク識別子（PNID）を SAN の詳細に含める必要があります。PNID と DNS 名は同一であり、DNS で解決可能である必要があります。
- vCenter Server は完全修飾ドメイン名（FQDN）を使用して導入することを推奨します。証明書の SAN に DNS Name=machine_FQDN が含まれるようにすることで、最適な互換性とサポートを実現します。
- 詳細については、VMware のドキュメントを参照してください：
  - "異なる解決策パスのvSphere証明書の要件"
  - "vCenter マシン SSL 証明書をカスタム認証局署名証明書に置き換える"
  - "エラー：Subject Alternate Name（SAN）フィールドにPNIDが含まれていません。有効な証明書を提供してください"

FQDN が使用できない場合は、PNID を IP アドレスに設定し、IP アドレスを SAN に含めることができます。ただし、これは VMware では推奨されていません。

手順

1. ウェブブラウザを開き、次のURLにアクセスしてください：
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. **vCenters** > 追加 を選択して、vCenter サーバー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、およびポートの詳細を入力してください。
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。管理者アカウントがなくても、権限を制限したカスタムロールを作成できます。詳細については、"vCenter Server RBAC と ONTAP tools for VMware vSphere 10 を使用" を参照してください。

ONTAP tools で VASA Provider 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、ONTAP システムでのストレージ ポリシーベース管理、vVols サポート、および VMware Live Site Recovery アプライアンスとの統合が可能になります。

VASA プロバイダー設定には、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 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」>「**NetApp ONTAP tools**」を選択します。
3. 設定 ＞ **VASA Provider**設定 を選択します。ONTAP toolsは、VASA Providerの登録ステータスを「未登録」と表示します。
4. VASAプロバイダーを登録するには、*Register*ボタンを選択してください。
5. VASA Providerの名前とクレデンシャルを入力します。ユーザ名には、英字、数字、アンダースコアのみを使用できます。パスワードは8~256文字にする必要があります。
6. 「登録」を選択します。
7. 登録とページ更新が成功すると、ONTAP tools には、登録済みの VASA Provider のステータス、名前、およびバージョンが表示されます。

次の手順

オンボーディングされた 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表示されていることを確認してください：

手順

1. vCenter Server インスタンスに移動します。
2. 管理者の資格情報でログインしてください。
3. **Storage Providers** > **Configure** を選択します。登録済みの 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てください。

ONTAP tools を使用して NFS VAAI プラグイン をインストールする

NFS vStorage Array Integration用API（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。

開始する前に

- "NetApp NFS Plug-in for VMware VAAI"インストールパッケージをダウンロードします。
- ESXi ホストがvSphere 7.0 U3（最新パッチ以降）および ONTAP 9.14.1 以降であ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 セクションの「ショートカット」>「**NetApp ONTAP tools**」を選択します。
3. 設定 ＞ **NFS VAAI Tools** を選択します。
4. VAAI プラグインをすでに vCenter Server にアップロード済みの場合は、「既存バージョン」の「変更」を選択してください。まだアップロードしていない場合は、「アップロード」を選択してください。
5. ファイルを参照して選択し、 `.vib`ファイルを選択して、*アップロード*を選択してファイルをONTAP tools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。

   vSphere Web クライアントには、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、ESXiホストを手動で再起動してください。

   ESXiホストを再起動すると、ONTAP tools for VMware vSphereがNFS VAAIプラグインを自動的に検出して有効にします。

次の手順

NFS VAAI プラグインをインストールしてESXiホストを再起動した後、VAAI コピー オフロード用のNFSエクスポートポリシーを設定します。エクスポートポリシールールが以下の要件を満たしていることを確認してください：

- 関連する ONTAP ボリュームは NFSv4 呼び出しを許可します。

- rootユーザーはrootのままであり、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 サーバで設定されます。

詳細については、 "VAAI コピー オフロードに適切な NFS エクスポート ポリシーを設定する" KBの記事を参照してください。

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"

ONTAP toolsでESXiホストの設定を構成する

ESXi サーバーのマルチパス設定とタイムアウト設定を構成することで、データの可用性と整合性を維持するのに役立ちます。プライマリパスが利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。

タスク概要

この処理には、お使いのシステム構成や負荷状況によっては時間がかかる場合があります。最近のタスクパネルで進捗状況を確認できます。

手順

1. VMware vSphere Web クライアントのホームページで、「ホストとクラスタ」を選択します。
2. 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 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** ホスト準拠 カードに移動します。
4. 「推奨設定を適用」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てください。
7. 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捗状況を確認できます。

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値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のテストに基づいて設定されます。

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

以下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設定は最適なパスを選択して使用します。

ハイ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 に変更します。

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…に設定してください。
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024 MB
NFS.MaxVolumes	256
NFS41.MaxVolumesを使用したチャンク アップロード署名要求がサポートされるようになりました。	256
NFS.MaxQueueDepth	128以上
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

ONTAP tools用のONTAPユーザーロールと権限を設定する

このセクションでは、ONTAP tools for VMware vSphere および ONTAP System Manager を使用して、ストレージバックエンドの ONTAP ユーザーロールと Privileges

を設定します。提供されている JSON ファイルを使用してロールを割り当てたり、ユーザーとロールを手動で作成したり、管理者以外のアカウントに必要最小限の Privileges を適用したりできます。

開始する前に

- ONTAP tools for VMware vSphere から ONTAP Privileges ファイルを *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* を使用して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 システムを設定する際は、ASA r2 固有の JSON ファイルを使用してください。

> ユーザーは、クラスタ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、ユーザーが最低限必要な SVM 権限を持ってい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てください。

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. 管理者権限でクラスターにログインしてください。ユーザーを設定するには：
   a. クラスター ONTAP tools ユーザーを設定するには、クラスター > 設定 > ユーザーと役割 ペインを選択します。
   b. SVM ONTAP tools ユーザーを設定するには、ストレージ **SVM** > 設定 > ユーザーと役割 ペインを選択します。
   c. 「Users」の下にある「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 ONTAP Privileges JSON 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 tools 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 Provider、SRA」を選択してください。

      ONTAP tools は、選択した製品機能に基づいて「役割」フィールドを自動的に設定します。

   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 Privileges （Discovery、Create Storage、Modify Storage、Destroy Storage、NAS/SAN Role）を選択し、**Add** を選択します。

ONTAP tools は新しいロールとユーザーを追加します。設定したロールに付与されている Privileges を確認できます。

SVMアグリゲートマッピング要件

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、データストアの 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 は、SVM にマッピングされていないアグリゲート上に SVM ユーザーがボリュームを作成することを防止します。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てください。

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 ユーザーとロールを手動で作成する

JSONファイルを使わずに、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. 管理者権限でクラスターにログインします。
   a. クラスター ONTAP tools のロールを設定するには、クラスター > 設定 > *ユーザーとロール*を選択します。
   b. クラスター SVM の ONTAP tools 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. 役割を作成する：
   a. **Roles** テーブルの **Add** を選択します。
   b. *役割名*と*役割属性*の詳細を入力してください。

      *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てください。

   c. 必要なAPIをすべて追加し、変更を保存します。
4. ユーザーを作成する：
   a. ユーザー テーブルの下にある 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、「System Manager」を選択します。
   c. *ユーザー名*を入力してください。

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」を選択してください。

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 は必須の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を設定し、ユーザーを保存します。

管理者権限を持たない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 **Privileges** の一覧

このページでは、JSON ファイルを持たない非管理者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 Privileges を一覧表示します。クラスターがローカルスコープにある場合は、JSON ファイルを使用してユーザーを作成してください。これは、ONTAP tools for VMware vSphere が ONTAP 上でプロビジョニングを行うために、読み取り Privileges 以上の権限を必要とするためです。

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/cluster	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/cluster/nodes	読み取り専用	プラットフォームタイプの検出
/api/security/accounts	読み取り専用	特権の検出
/api/security/roles	読み取り専用	特権の検出
/api/storage/aggregates	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アグリゲートスペースチェック
/api/storage/cluster	読み取り専用	クラスターレベルのスペースと効率データを取得するには
/api/storage/disks	読み取り専用	集約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およびVMポリシー管理
/api/svm/svms	読み取り専用	クラスターをローカルで追加した際に、SVM構成を取得するため。
/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スコープがクラスター/SVMであることを識別する
/api/storage/availability-zones	読み取り専用	SAZ ディスカバリ。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/metrocluster	読み取り専用	MetroCluster のステータスと設定の詳細を取得します。

VMware vSphere 向け **ONTAP tools** の **ONTAP API** ベースのクラスタスコープユーザーを作成する

データストアに対するPATCH操作および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。権限が不足していると、ワークフローやクリーンアップに問題が発生する可能性があります。

検出、作成、変更、削除の権限を持つ ONTAP API ベースのユーザーは、ONTAP tools のワークフローを管理できます。

上記で述べたすべての権限を持つクラスタスコープ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 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
```

さらに、ONTAPバージョン9.16.0以降では、以下のコマンドを実行してください：

```
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 向け **ONTAP tools** の **ONTAP API** ベースの **SVM** スコープユーザーを作成する

以下のコマンドを実行して、すべての権限を持つSVMスコープのユーザーを作成します。

```
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以降では、以下のコマンドを実行してください：

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

以前に作成した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_sti160-cluster_
```

アカウントのロックを解除して管理インターフェイ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_sti160-cluster
```

ONTAP tools for VMware vSphere 10.1ユーザーから10.3ユーザー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スコープのユーザーを持つONTAP tools for VMware vSphere 10.1ユーザーは、以下のONTAP CLIコマンドを管理者権限で使用して、10.3リリースにアップグレードしてください。

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。

クラスタ権限：

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 で json ファイルを使用して作成された SVM スコープのユーザーを使用している場合は、管理者権限を持つ 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てください。

SVM権限：

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>

以下のコマンドを有効にするには、既存のロールに *vserver nvme namespace show* および *vserver nvme subsystem show* コマンドを追加します。

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

ONTAP tools for VMware vSphere 10.3ユーザーから10.4ユーザーへのアップグレード

ONTAP 9.16.1 以降、ONTAP tools for VMware vSphere 10.3 ユーザーを 10.4 ユーザーにアップグレードします。

JSON ファイルを使用して作成されたクラスタスコープユーザーおよび ONTAP バージョン 9.16.1 以降を使用している ONTAP tools for VMware vSphere 10.3 のユーザーは、管理者権限を持つ 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てください。

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。

クラスタ権限：

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

ONTAP toolsにストレージバックエンドを追加する

ONTAP tools for VMware vSphere を使用して、ESXi ホストのストレージバックエンドを追加および管理します。クラスターや SVM をオンボーディングし、MetroCluster サポートを有効にして、セキュアな接続のために証明書を検証できます。ストレージバックエンドは、ONTAP tools Manager または vSphere クライアントを使用して構成し、証明書のステータスを監視したり、クラスターの変更後にリソースを手動で再検出したりできます。

ストレージ バックエンドをローカルに追加するには、ONTAP toolsのインターフェイスでクラスターまたはSVMの資格情報を使用します。ローカル 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 toolsは、vVolsまたはVMFSデータストア管理のためにSVMをvCenter Serverにマッピングします。VMFSデータストアおよびSRAのワークフローでは、クラスターをグローバルにマッピングすることなくSVMの資格情報を使用できます。

グローバルストレージバックエンドを追加するには、ONTAP tools Manager で ONTAP クラスターの認証情報を使用します。グローバルストレージバックエンドにより、検出ワークフローが vVol 管理に必要なクラスターリソースを特定できるようになります。マルチテナント環境では、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。

グローバルおよびローカルストレージバックエンドの詳細については、KB記事 "OTV 10：ストレージバックエンドのグローバルスコープとローカルスコープとは"を参照してください。

MetroClusterサポートが ONTAP で有効になっている場合は、ソースクラスターとデスティネーションクラスターの両方を、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。

開始する前に

証明書に有効なサブジェクト代替名（SAN）フィールドが含まれていることを確認してください。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

マルチテナントのセットアップでは、ストレージバックエンドクラスタをグローバルに追加し、SVMをローカルに追加して、SVMユーザーの認証情報を使用できます。

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. デプロイ時に指定した ONTAP tools for VMware vSphere の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、パスワードの詳細を指定してください。

   IPv4およびIPv6アドレス管理LIFがサポートされています。

5. ONTAPクラスタ証明書を自動的に取得して認証するか、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代替名（SAN）の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"を参照してください。

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はピアクラスターを追加するためのポップアップメッセージを表示します。「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てください。

   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 tools の検出を手動で実行してください。

vSphere クライアントユーザーインターフェースの使用

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ースを通じたSVMユーザーの直接追加をサポートしていません。

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にある **NetApp ONTAP tools** 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、ポートの詳細を入力してください。

   IPv4またはIPv6の管理LIFのいずれかを使用して、クラスタベースの認証情報で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ベースの認証情報とSVM管理LIFを指定してください。クラスターがすでにオンボーディングされている場合、そのクラスターからSVMユーザーを再度オンボーディング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認証するか、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 tools は **Add MetroCluster peer** 画面を表示します。**Add peer** を選択して、ピアストレージバックエンドを追加します。

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 tools の検出を手動で実行してください。

ONTAP tools 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一覧表示します。証明書の有効期限が30日以内の場合、ONTAP tools 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、ONTAP tools はストレージシステムに接続できないため、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

"OTV 10：ストレージバックエンドのグローバルスコープとローカルスコープとは"

"クラスタをMetroCluster構成に設定"

ONTAP tools でvCenter Server インスタンスにストレージバックエンドを関連付ける

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て、すべての vCenter Server インスタンスへのアクセスを有効にします。MetroCluster 構成では、ストレージバックエンドクラスタを関連付ける場合、ピアクラスタも vCenter Server に関連付けてください。

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. デプロイ時に指定した ONTAP tools for VMware vSphere の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。

ONTAP tools でネットワーク アクセスを設定する

デフォルトでは、ESXi ホストから検出されたすべての IP アドレスは、ネットワーク アクセスを設定しない限り、エクスポート ポリシーに自動的に追加されます。エクスポート ポリシーを変更することで、特定の IP アドレスからのアクセスのみを許可できます。除外された ESXi ホストがマウント操作を試みた場合、その操作は失敗します。

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 tools** を選択します。
3. ONTAP tools 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）、またはこれら3つの組み合わせで区切ります。

4. 「保存」を選択します。

ONTAP toolsでデータストアを作成する

ホストクラスタレベルでデータストアを作成すると、ONTAP tools はすべての宛先ホストにマウントし、必要な権限がある場合にのみアクションを有効にします。

vCenter Server のネイティブデータストアと **ONTAP tools** が管理するデータストア間の相互運用性

ONTAP tools for VMware vSphere 10.4 以降、ONTAP tools はデータストア用にネストされた igroup を作成します。親 igroup はデータストア固有のもので、子 igroup はホストにマッピングされます。ONTAP System Manager からフラットな igroup を作成し、ONTAP tools を使用せずに VMFS データストアの作成に使用できます。詳細については、 "SANイニシエータとigroupを管理する"を参照してください。

ストレージをオンボーディングしてデータストア検出を実行した後、ONTAP tools はVMFSデータストア内のフラットなigroupをネストされたigroupに変更します。以前のフラットな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 tools の管理インターフェイスまたはREST APIを使用してください。

vVols データストアを作成する

ONTAP tools for VMware vSphere 10.3以降では、スペース効率をthin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。vVol。VASA Provider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を作成します。VASA Providerは、このコンテナにバッキングボリュームを割り当てません。

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。
- VASAプロバイダーが選択したvCenterに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はSVMユーザーのアグリゲートにマッピングされる必要があります。

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、またはデータセンターを右クリックして、**NetApp ONTAP tools** > *データストアの作成*を選択します。
3. vVolsを*データストア タイプ*として選択します。
4. *データストア名*と*プロトコル*情報を入力してください。

   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を選択してください。
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、すべてのオブジェクトについてvCenterで検出を実行してください。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 プロトコル用に*カスタム イニシエータ 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/namespace）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て 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際に、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のvVolsデータストアについては、この手順をスキップしてください。

8. *概要*ペインで選択内容を確認し、*完了*を選択してください。

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環境で使用されています。

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、またはデータセンターを右クリックして、* 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」を選択してください。
4. 「名前とプロトコル」ペインに、データストア名、サイズ、および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」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、すべてのオブジェクトについて vCenter で検出を実行してください。このオプションは使用しないことをお勧めします。

   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。

   - 詳細オプションでは、プラットフォームのドロップダウンメニューで「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」切り替えボタンが表示されます。
   - プラットフォームのドロップダウンで **Any** オプションを選択すると、vCenter 内のすべての SVM を表示できます。プラットフォームと非対称フラグは表示には影響しません。
7. 「ストレージ属性」ペインで、ボリューム作成に使用するアグリゲートを選択します。詳細設定で、必要に応じて「スペース予約」と「QoSを有効にする」を選択します。
8. 「概要」ペインで選択内容を確認し、「完了」を選択してください。

ONTAP tools はNFSデータストアを作成し、すべてのホストにマウントします。

VMFSデータストアを作成する

VMFSは、仮想マシンファイルを保存するためのクラスタ型ファイルシステムです。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、vMotionおよび高可用性機能をサポートします。

保護されたクラスターの場合：

- VMFSデータストアのみ作成可能です。保護されたクラスタにVMFSデータストアを追加すると、自動的にそのデータストアが保護されます。
- 保護されたホストクラスタが1つ以上存在するデータセンターには、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、非同期関係によって保護されているESXiホスト上でのみ作成できます。「Automated Failover Duplex」ポリシーによって保護されているホストクラスタの一部である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で SVM ユーザーの集約に SVM をマッピングします。

- NVMe/TCPプロトコルを使用する場合は、ESXiホストを設定します。
  a. 確認する "VMware互換性ガイド"

  > VMware vSphere 7.0 U3以降のバージョンはNVMe/TCPプロトコルをサポートしています。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ースカード（NIC）のベンダーが、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てください。
  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リリースを使用する場合は、VMwareサイトの手順に従って "NVMe over TCPアダプタのVMkernelバインディングを設定する"NVMe/TCPポートバインディングを設定してください。VMware vSphere 8リリースを使用する場合は、 "ESXi上でTCP経由のNVMeを構成する"に従ってNVMe/TCPポートバインディングを設定してください。
  e. VMware vSphere 7リリースについては、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を有効にする"NVMe/TCPソフトウェアアダプタを設定してください。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アダプタを追加する"に従ってNVMe/TCPソフトウェアアダプタを設定してください。
  f. ESXiホスト上で"ストレージ システムとホストの検出"アクションを実行します。詳細については、 "vSphere 8.0 Update 1およびONTAP 9.13.1を使用したVMFSデータストア向けNVMe/TCPの設定方法" を参照してください。
- NVME/FCプロトコルを使用している場合は、以下の手順を実行してESXiホストを設定してください。
  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）を有効にしてください。
  b. SCSIのゾーニングを完了してください。
  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てください。

FC プロトコル用に ONTAP SVM を設定するには、 "FC用のSVMの設定"を参照してください。

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、 "ONTAP を使用したESXi 8.x の NVMe-oF ホスト構成"を参照してください。

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 ホスト構成ガイド"および "TR-4684を使用したチャンク アップロード署名要求がサポートされるようになりました。"を参照してください。

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、またはデータセンターを右クリックして、**NetApp ONTAP tools** > *データストアの作成*を選択します。
3. VMFS データストアのタイプを選択します。
4. 「名前とプロトコル」ペインに、データストア名、サイズ、およびプロトコル情報を入力します。既存のVMFSクラスタに新しいデータストアを追加するには、「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. **Storage***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 セクションで カス

タムイニシエータグループ名 を入力してください。データストアには、既存の igroup を選択するか、カスタム名で新しい igroup を作成できます。

NVMe/FCまたはNVMe/TCPプロトコルが選択されると、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 tools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、名前空間サブシステムを作成します。*Storage*ペインの詳細オプションにある*custom namespace subsystem name*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では、ストレージが分離されているため、*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. ONTAP tools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/Namespace）を作成します。

   ONTAP 9.16.1以降、ASA r2ストレージシステムはクラスターあたり最大12ノードをサポートします。

   c. 12ノードSVMを搭載したASA r2ストレージシステム（異種クラスタ）の*パフォーマンスサービスレベル*を選択してください。選択したSVMが同種クラスタである場合、またはSVMユーザーを使用している場合は、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のバランスの取れた配置アルゴリズムを使用してストレージユニットを作成します。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」と「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（LUN/名前空間）の作成には適用されません。そのため、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プロトコルによる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. 「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ー上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のメッセージが表示されます。

結果

ONTAP tools はVMFSデータストアを作成し、すべてのホストにマウントします。

著作権に関する情報

商標に関する情報