



NetApp HCIの管理

HCI

NetApp
October 11, 2024

目次

NetApp HCIの管理	1
NetApp HCI の管理の概要	1
vCenter および ESXi のクレデンシャルを更新します	1
NetApp HCI ストレージを管理します	4
管理ノードを操作します	28
NetApp HCI システムの電源をオフまたはオンにします	79

NetApp HCIの管理

NetApp HCI の管理の概要

NetApp HCI、ユーザアカウント、ストレージクラスタ、ボリューム、ボリュームアクセスグループ、イニシエータ、ボリューム QoS ポリシー、および管理ノードのクレデンシヤルを管理できます。

使用できる項目は次のとおりです。

- ["vCenter および ESXi のクレデンシヤルを更新します"](#)
- ["NetApp HCI ストレージアセットを管理します"](#)
- ["管理ノードを操作します"](#)
- ["NetApp HCI システムの電源をオフまたはオンにします"](#)

詳細情報

- ["NetApp HCI のリソースページ"](#)

vCenter および ESXi のクレデンシヤルを更新します

NetApp HCI 環境向けに NetApp Hybrid Cloud Control の全機能を維持するために、vCenter および ESXi ホストでクレデンシヤルを変更した場合は、管理ノードのアセットサービスでそれらのクレデンシヤルも更新する必要があります。

タスクの内容

NetApp Hybrid Cloud Control は、VMware vSphere ESXi を実行している vCenter および個々のコンピューティングノードと通信し、ダッシュボードの情報を取得して、ファームウェア、ソフトウェア、ドライバのローリングアップグレードを支援します。NetApp Hybrid Cloud Control および管理ノード上の関連サービスでは、クレデンシヤル（ユーザ名とパスワード）を使用して VMware vCenter および ESXi に対して認証されません。

これらのコンポーネント間の通信に障害が発生すると、NetApp Hybrid Cloud Control と vCenter で認証の問題が発生したときにエラーメッセージが表示されます。NetApp HCI 環境の関連付けられた VMware vCenter インスタンスと通信できない場合、NetApp Hybrid Cloud Control に赤色のエラーバナーが表示されます。VMware vCenter では、NetApp Hybrid Cloud Control の使用時に古いクレデンシヤルを使用して個々の ESXi ホストの ESXi アカウントロックアウトメッセージが表示されます。

NetApp HCI の管理ノードは、次の名前を使用してこれらのコンポーネントを参照します。

- 「コントローラアセット」は、NetApp HCI 環境に関連付けられている vCenter インスタンスです。
- 「コンピューティングノードアセット」は、NetApp HCI 環境の ESXi ホストです。

NetApp Deployment Engine を使用した NetApp HCI の初回インストール時には、vCenter で指定した管理ユーザのクレデンシヤルと ESXi サーバの「root」アカウントのパスワードが管理ノードに保存されます。

管理ノードの **REST API** を使用して **vCenter** のパスワードを更新します

手順に従ってコントローラアセットを更新します。を参照して "[既存のコントローラアセットを表示または編集する](#)"

管理ノード **REST** を使用して **ESXi** のパスワードを更新します **API**

手順

1. 管理ノードのREST APIユーザインターフェイスの概要については、を参照して"[管理ノードの REST API ユーザインターフェイスの概要](#)"ください。
2. 管理ノードの管理サービスの REST API UI にアクセスします。

```
https://<ManagementNodeIP>/mnode
```

management node IP> は、 NetApp HCI 用の管理ネットワーク上の管理ノードの IPv4 アドレスです。

3. 「 * Authorize * (認証) 」または任意のロックアイコンを選択し、次の手順を実行します。
 - a. NetApp SolidFire クラスタの管理ユーザ名とパスワードを入力します。
 - b. クライアントIDにと入力し `mnode-client` ます。
 - c. セッションを開始するには、 * Authorize * を選択します。
 - d. ウィンドウを閉じます。
4. REST API UI から、 * get /assets/compute_nodes * を選択します。

管理ノードに格納されているコンピューティングノードアセットのレコードが取得されます。

UI からこの API に直接アクセスするには、次のリンクを使用します。

```
https://<ManagementNodeIP>/mnode/#/assets/routes.v1.assets_api.get_compute_nodes
```

5. [[* 試してみてください *](#)] を選択します。
6. [[* Execute](#)] を選択します。
7. 応答の本文から、クレデンシャルの更新が必要なコンピューティングノードのアセットレコードを特定します。「ip」プロパティと「host_name」プロパティを使用して、正しい ESXi ホストレコードを検索できます。

```
"config": { },
"credentialid": <credential_id>,
"hardware_tag": <tag>,
"host_name": <host_name>,
"id": <id>,
"ip": <ip>,
"parent": <parent>,
"type": ESXi Host
```



次の手順では、コンピューティングアセットレコードの「親」フィールドと「id」フィールドを使用して、更新するレコードを参照します。

8. コンピューティングノードのアセットを設定します。

- a. PUT /assets/ {asset_id} /compute-nodes/ {compute_id} *を選択します。

UI の API への直接リンクを次に示します。

```
https://<ManagementNodeIP>/mnode/#/assets/routes.v1.assets_api.put_asset_s_compute_id
```

- a. [* 試してみてください *] を選択します。
- b. 「parent」情報を指定して「asset_id」を入力します。
- c. "id" 情報を入力して、"compute_id" を入力します。
- d. ユーザーインターフェイスの要求の本文を変更して、コンピューティングアセットレコードのパスワードとユーザー名のパラメータのみを更新します。

```
{
  "password": "<password>",
  "username": "<username>"
}
```

- e. [* Execute] を選択します。
- f. 応答が HTTP 200 であることを確認します。HTTP 200 は、参照先のコンピューティングアセットレコードに新しいクレデンシャルが格納されたことを示します
9. 新しいパスワードで更新する必要があるその他のコンピューティングノードアセットについて、前述の 2 つの手順を繰り返します。
10. に移動します https://<mNode_ip>/inventory/1/。
- a. 「* Authorize * (認証)」または任意のロックアイコンを選択し、次の手順を実行します。
- i. NetApp SolidFire クラスタの管理ユーザ名とパスワードを入力します。

- ii. クライアントIDに入力し `mnode-client` ます。
 - iii. セッションを開始するには、 * Authorize * を選択します。
 - iv. ウィンドウを閉じます。
 - b. REST API UI から、 * GET / Installations * を選択します。
 - c. [* 試してみてください *] を選択します。
 - d. [Refresh 概要 (更新の設定)] ドロップダウンリストから [* True] を選択します。
 - e. [* Execute] を選択します。
 - f. 応答が HTTP 200 であることを確認します。
11. vCenter のアカウントロックアウトメッセージが表示されなくなるまで約 15 分待ちます。

詳細情報

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

NetApp HCI ストレージを管理します

Manage NetApp HCI storage の概要を参照してください

NetApp HCI では、 NetApp Hybrid Cloud Control を使用してこれらのストレージアセットを管理できます。

- ["ユーザアカウントを作成および管理します"](#)
- ["ストレージクラスタを追加および管理する"](#)
- ["ボリュームの作成と管理"](#)
- ["ボリュームアクセスグループを作成および管理します"](#)
- ["イニシエータを作成および管理する"](#)
- ["ボリュームの QoS ポリシーの作成と管理"](#)

詳細情報

- ["SolidFireおよびElement 12.2ドキュメントセンター"](#)
- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

ネットアップハイブリッドクラウドを使用してユーザアカウントを作成、管理します 制御

Element ベースのストレージシステムでは、「管理者」または「読み取り専用」のユーザに付与する権限に応じて、権限のあるクラスタユーザを作成して NetApp Hybrid Cloud Control へのログインアクセスを有効にすることができます。クラスタユーザに加

えてボリュームアカウントもあり、クライアントはこのアカウントを使用してストレージノード上のボリュームに接続できます。

次のタイプのアカウントを管理します。

- [\[権限のあるクラスタアカウントを管理します\]](#)
- [\[ボリュームアカウントを管理する\]](#)

LDAPを有効にする

任意のユーザアカウントで LDAP を使用するには、最初に LDAP を有効にする必要があります。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで右上のオプションアイコンを選択し、*ユーザー管理*を選択します。
3. [ユーザー] ページで、**Configure LDAP** を選択します。
4. LDAP 設定を定義します。
5. 検索とバインドまたは直接バインドの認証タイプを選択します。
6. 変更を保存する前に、ページ上部の「*LDAP ログインのテスト*」を選択し、存在するユーザーのユーザー名とパスワードを入力して、「*テスト*」を選択します。
7. [保存 (Save)] を選択します。

権限のあるクラスタアカウントを管理します

"[権限のあるユーザアカウント](#)"NetAppハイブリッドクラウドコントロールの右上のメニュー[User Management]オプションで管理します。このタイプのアカウントでは、ノードおよびクラスタの NetApp Hybrid Cloud Control インスタンスに関連付けられているストレージセットに対して認証を行うことができます。このアカウントを使用すると、すべてのクラスタのボリューム、アカウント、アクセスグループなどを管理できます。

権限のあるクラスタアカウントを作成してください

NetApp Hybrid Cloud Control を使用してアカウントを作成できます。

このアカウントを使用して、Hybrid Cloud Control、クラスタのノード UI、および NetApp Element ソフトウェアのストレージクラスタにログインできます。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで、右上の[オプション]アイコンを選択し、*[ユーザー管理]*を選択します。
3. [Create User] を選択します。
4. クラスタまたは LDAP の認証タイプを選択します。
5. 次のいずれかを実行します。

- LDAP を選択した場合は、DN を入力します。



LDAP を使用するには、最初に LDAP または LDAPS を有効にする必要があります。を参照して [LDAPを有効にする](#)

- Auth Type として Cluster を選択した場合は、新しいアカウントの名前とパスワードを入力します。

6. 管理者権限または読み取り専用権限のいずれかを選択します。



NetApp Element ソフトウェアからアクセス許可を表示するには、[従来のアクセス許可を表示する *] を選択します。これらの権限のサブセットを選択すると、そのアカウントには読み取り専用権限が割り当てられます。すべてのレガシー権限を選択した場合、そのアカウントには管理者権限が割り当てられます。



グループのすべての子が権限を継承するようにするには、LDAP サーバで DN 組織管理者グループを作成します。そのグループのすべての子アカウントは、これらの権限を継承します。

7. 「ネットアップのエンドユーザライセンス契約を読んで同意します」というボックスをオンにします。

8. [Create User] を選択します。

権限のあるクラスタアカウントを編集してください

NetApp Hybrid Cloud Control を使用して、ユーザアカウントの権限またはパスワードを変更できます。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで右上のアイコンを選択し、* ユーザー管理 * を選択します。
3. 必要に応じて、* Cluster *、* LDAP *、または * IDP * を選択して、ユーザアカウントのリストをフィルタリングします。

ストレージクラスタのユーザにLDAPを設定している場合、それらのアカウントのユーザタイプは「ldap」と表示されます。ストレージクラスタでIDPを使用してユーザを設定した場合、それらのアカウントの[User Type]は「IdP」と表示されます。

4. テーブルの * アクション * 列で、アカウントのメニューを展開し、* 編集 * を選択します。
5. 必要に応じて変更します。
6. [保存 (Save)] を選択します。
7. NetApp Hybrid Cloud Control からログアウトします。
8. ["クレデンシャルを更新します"](#)NetAppハイブリッドクラウドコントロールAPIを使用して、信頼できるクラスタアセットにアクセスします。



NetApp Hybrid Cloud Control の UI でインベントリの更新に最大 15 分かかる場合があります。インベントリを手動で更新するには、REST API UIインベントリサービスにアクセスし [https://<ManagementNodeIP>/inventory/1/`てクラスタに対してを実行します`GET /installations/{id}。`](https://<ManagementNodeIP>/inventory/1/`てクラスタに対してを実行します`GET /installations/{id}。)

9. NetApp Hybrid Cloud Control にログインします。

権限のあるユーザアカウントを削除します

不要になったアカウントを削除できます。LDAP ユーザアカウントを削除できます。

権限のあるクラスタのプライマリ管理者ユーザアカウントを削除することはできません。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで右上のアイコンを選択し、* ユーザー管理 * を選択します。
3. ユーザーテーブルの * アクション * 列で、アカウントのメニューを展開し、* 削除 * を選択します。
4. [はい] を選択して、削除を確認します。

ボリュームアカウントを管理する

"**ボリュームアカウント**" NetApp Hybrid Cloud Control Volumes のテーブルで管理されます。これらのアカウントは、アカウントを作成したストレージクラスタにのみ固有です。これらのタイプのアカウントでは、ネットワーク上のボリュームにアクセス許可を設定できますが、設定したボリューム以外には影響しません。

ボリュームアカウントには、そのボリュームにアクセスするために必要な CHAP 認証が含まれています。

ボリュームアカウントを作成します

このボリュームに固有のアカウントを作成します。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで、* ストレージ * > * ボリューム * を選択します。
3. 「* アカウント *」タブを選択します。
4. 「* アカウントの作成 *」ボタンを選択します。
5. 新しいアカウントの名前を入力します。
6. CHAP Settings (CHAP 設定) セクションで、次の情報を入力します。
 - CHAP ノードセッション認証用のイニシエータシークレット
 - Target Secret : CHAP ノードセッション認証



いずれかのパスワードを自動生成する場合は、クレデンシャルのフィールドを空白のままにします。

7. 「* アカウントの作成 *」を選択します。

ボリュームアカウントを編集します

CHAP 情報を変更し、アカウントがアクティブであるかロックされているかを変更できます。



管理ノードに関連付けられているアカウントを削除またはロックすると、管理ノードにアクセスできなくなります。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで、 * ストレージ * > * ボリューム * を選択します。
3. 「 * アカウント * 」 タブを選択します。
4. テーブルの * アクション * 列で、アカウントのメニューを展開し、 * 編集 * を選択します。
5. 必要に応じて変更します。
6. 「 * はい * 」 を選択して変更を確定します。

ボリュームアカウントを削除します

不要になったアカウントを削除します。

ボリュームアカウントを削除する前に、そのアカウントに関連付けられているボリュームを削除およびパーージします。



管理ノードに関連付けられているアカウントを削除またはロックすると、管理ノードにアクセスできなくなります。



管理サービスに関連付けられた永続ボリュームは、インストールまたはアップグレード時に新しいアカウントに割り当てられます。永続ボリュームを使用している場合は、ボリュームや関連付けられているアカウントを変更または削除しないでください。これらのアカウントを削除すると、管理ノードが使用できなくなる可能性があります。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで、 * ストレージ * > * ボリューム * を選択します。
3. 「 * アカウント * 」 タブを選択します。
4. テーブルの * アクション * 列で、アカウントのメニューを展開し、 * 削除 * を選択します。
5. [はい] を選択して、削除を確認します。

詳細情報

- ["アカウントの詳細を確認します"](#)
- ["ユーザアカウントを操作する"](#)
- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

NetApp Hybrid Cloud Control を使用してストレージクラスタを追加および管理します

ストレージクラスタを管理ノードアセットインベントリに追加すると、NetApp Hybrid Cloud Control (HCC) を使用して管理できるようになります。システムセットアップ時に最初に追加されたストレージクラスタがデフォルト"[信頼できるストレージクラスタ](#)です"ですが、クラスタを追加するにはHCC UIを使用します。

ストレージクラスタを追加したあと、クラスタのパフォーマンスの監視、管理対象アセットのストレージクラスタクREDENTIALの変更、または HCC を使用して管理する必要がなくなった場合に管理ノードのアセットインベントリからストレージクラスタを削除できます。

Element 12.2以降では、機能オプションを使用して、ストレージクラスタノードのメンテナンスモードを有効または無効にでき"[メンテナンスモト](#)ます。

必要なもの

- クラスタ管理者の権限：で管理者としての権限があります"[信頼できるストレージクラスタ](#)です"。信頼できるクラスタとは、システムのセットアップ時に管理ノードインベントリに最初に追加されるクラスタです。
- * Element ソフトウェア * : ストレージクラスタで NetApp Element ソフトウェア 11.3 以降を実行している必要があります。
- * 管理ノード * : バージョン 11.3 以降を実行する管理ノードを導入しておきます。
- * 管理サービス * : 管理サービスのバンドルをバージョン 2.17 以降に更新しました。

オプション

- [\[ストレージクラスタを追加\]](#)
- [\[ストレージクラスタのステータスを確認\]](#)
- [\[ストレージクラスタクREDENTIALを編集します\]](#)
- [\[ストレージクラスタを削除\]](#)
- [\[メンテナンスモードを有効または無効にします\]](#)

ストレージクラスタを追加

NetApp Hybrid Cloud Control を使用して、管理ノードアセットインベントリにストレージクラスタを追加できます。これにより、HCC UI を使用してクラスタを管理および監視できます。

手順

1. ストレージクラスタ管理者の正規のクREDENTIALを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで右上のオプションメニューを選択し、* 構成 * を選択します。
3. Storage Clusters * ペインで、* Storage Cluster Details * を選択します。
4. Add Storage Cluster (ストレージクラスタの追加) * を選択します。
5. 次の情報を入力します。
 - ストレージクラスタ管理仮想 IP アドレス



追加できるのは、管理ノードで現在管理されていないリモートストレージクラスタだけです。

- ストレージクラスタのユーザ名とパスワード

6. 「* 追加」を選択します。



ストレージクラスタを追加したあとにクラスタのインベントリが更新されて新しい追加が表示されるまでに最大 15 分かかることがあります。変更を反映するには、ブラウザでページの更新が必要になる場合があります。

7. Element ESDS クラスタを追加する場合は、SSH 秘密鍵と SSH ユーザアカウントを入力またはアップロードします。

ストレージクラスタのステータスを確認

NetApp Hybrid Cloud Control の UI を使用して、ストレージクラスタアセットの接続ステータスを監視できます。

手順

1. ストレージクラスタ管理者の正規のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで右上のオプションメニューを選択し、* 構成 * を選択します。
3. インベントリでのストレージクラスタのステータスを確認します。
4. Storage Clusters * ペインで、詳細を表示する * Storage Cluster Details * を選択します。

ストレージクラスタクレデンシャルを編集します

NetApp Hybrid Cloud Control の UI を使用して、ストレージクラスタ管理者のユーザ名とパスワードを編集できます。

手順

1. ストレージクラスタ管理者の正規のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで右上のオプションメニューを選択し、* 構成 * を選択します。
3. Storage Clusters * ペインで、* Storage Cluster Details * を選択します。
4. クラスタの * Actions * メニューを選択し、* Edit Cluster Credentials * を選択します。
5. ストレージクラスタのユーザ名とパスワードを更新します。
6. [保存 (Save)] を選択します。

ストレージクラスタを削除

NetApp Hybrid Cloud Control からストレージクラスタを削除すると、管理ノードインベントリからクラスタが削除されます。ストレージクラスタを削除すると、そのクラスタは HCC で管理できなくなり、クラスタの管理 IP アドレスに直接移動する場合にのみアクセスできます。



信頼できるクラスタをインベントリから削除することはできません。権限のあるクラスタを確認するには、* User Management > Users * に移動します。権限のあるクラスタが「* users *」という見出しの横に表示されています。

手順

1. ストレージクラスタ管理者の正規のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで右上のオプションメニューを選択し、* 構成 * を選択します。
3. Storage Clusters * ペインで、* Storage Cluster Details * を選択します。
4. クラスタの * Actions * メニューを選択し、* Remove Storage Cluster * を選択します。



「* Yes * next」を選択すると、クラスタがインストールから削除されます。

5. 「* はい *」を選択します。

メンテナンスモードを有効または無効にします

この"[メンテナンスモード](#)"機能オプションでは、ストレージクラスタノードの機能と無効化メンテナンスモードを使用できます[可能にする](#)。

必要なもの

- * Element ソフトウェア * : ストレージクラスタで NetApp Element ソフトウェア 12.2 以降を実行している必要があります。
- * 管理ノード * : バージョン 12.2 以降を実行する管理ノードを導入しておきます。
- * 管理サービス * : 管理サービスのバンドルをバージョン 2.19 以降に更新しました。
- 管理者レベルでログインするためのアクセス権があります。

メンテナンスモードを有効にします

次の手順を使用して、ストレージクラスタノードのメンテナンスモードを有効にすることができます。



保守モードにできるノードは一度に 1 つだけです。

手順

1. Webブラウザで管理ノードのIPアドレスを開きます。例：

```
https://<ManagementNodeIP>
```

2. NetApp HCI ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。



メンテナンスモード機能のオプションは、読み取り専用レベルでは無効になります。

3. 左側のナビゲーション青いボックスで、NetApp HCI のインストールを選択します。

4. 左側のナビゲーションペインで、* ノード * を選択します。
5. ストレージインベントリ情報を表示するには、「* ストレージ *」を選択します。
6. ストレージノードでメンテナンスモードを有効にします。



ストレージノードのテーブルは、ユーザが開始した操作以外では2分ごとに自動的に更新されます。処理の前に、nodes テーブルの右上にある更新アイコンを使用して nodes テーブルを更新し、最新の状態に更新します。

[メンテナンスモードを有効にします]

- a. [* アクション *]で、[* メンテナンスモードを有効にする *]を選択します。

メンテナンスモード * を有効にしている間は、選択したノードおよび同じクラスタ上の他のすべてのノードでメンテナンスモードの操作を実行することはできません。

メンテナンスモードを有効にする * が完了すると、* Node Status * 列にレンチアイコンと、メンテナンスモードになっているノードの「* Maintenance Mode *」というテキストが表示されます。

メンテナンスモードを無効にします

ノードがメンテナンスモードになると、このノードで * メンテナンスモードを無効にする * アクションを使用できるようになります。メンテナンス中のノードでメンテナンスモードが無効になるまで、他のノードに対する処理は実行できません。

手順

1. 保守モードのノードの場合は、* アクション * で * メンテナンスモードを無効にする * を選択します。

メンテナンスモード * を無効にしている間は、選択したノードおよび同じクラスタ上の他のすべてのノードでメンテナンスモードの操作を実行することはできません。

メンテナンスモードを無効にする * 完了後、* Node Status * 列に * Active * と表示されます。



ノードが保守モードのときは新しいデータは受け入れられません。そのため、メンテナンスモードを終了する前にノードのデータをバックアップしておく必要があるため、メンテナンスモードを無効にするまでに時間がかかることがあります。保守モードでの作業時間が長くなるほど、保守モードを無効にするためにかかる時間が長くなります。

トラブルシューティング

メンテナンスモードを有効または無効にしているときにエラーが発生した場合は、nodes テーブルの上部にバナーエラーが表示されます。エラーの詳細については、バナーに表示される「* 詳細を表示 *」リンクを選択して、API が返す内容を確認できます。

詳細情報

- ["ストレージクラスタアセットを作成および管理する"](#)
- ["NetApp HCI のリソースページ"](#)

NetApp Hybrid Cloud Control を使用してボリュームを作成および管理する

ボリュームを作成して、指定したアカウントに関連付けることができます。アカウントにボリュームを関連付けると、アカウントは iSCSI イニシエータおよび CHAP クレデンシャルを使用してボリュームにアクセスできるようになります。

作成中に、ボリュームの QoS 設定を指定できます。

NetApp Hybrid Cloud Control では、次の方法でボリュームを管理できます。

- [\[ボリュームの作成\]](#)
- [ボリュームに QoS ポリシーを適用します](#)
- [\[ボリュームの編集\]](#)
- [\[クローンボリューム\]](#)
- [\[ボリュームを削除する\]](#)
- [\[削除したボリュームをリストアします\]](#)
- [\[削除したボリュームをパーズします\]](#)

ボリュームの作成

NetApp Hybrid Cloud Control を使用してストレージボリュームを作成できます。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. [* Volumes (ボリューム) > Overview (概要) *] タブを選択します。

[HCC Volumes (HCC ボリューム) ページ > Overview (概要) タブの画像] |

4. [Create Volume] を選択します。
5. 新しいボリュームの名前を入力します。
6. ボリュームの合計サイズを入力します。



デフォルトで選択されているボリュームサイズの単位は GB です。ボリュームは、GB または GiB 単位のサイズを使用して作成できます。1GB = 1 000 000 000 バイト 1GiB = 1 073 741 824 バイト

7. ボリュームのブロックサイズを選択します。
8. アカ운trリストから、ボリュームへのアクセスを許可するアカウントを選択します。

アカウントが存在しない場合は、「* 新規アカウントの作成 *」を選択し、新しいアカウント名を入力して「* 作成 *」を選択します。アカウントが作成され、新しいボリュームに関連付けられます。



アカウント数が 50 個を超える場合、リストは表示されません。名前の先頭部分を入力すると、オートコンプリート機能によって、選択可能な値が表示されます。

9. QoS を設定するには、次のいずれかを実行します。
 - a. 既存の QoS ポリシーを選択してください。
 - b. QoS 設定で、IOPS の最小値、最大値、バースト値をカスタマイズするか、デフォルトの QoS 値を使用します。

最大 IOPS またはバースト IOPS の値が 20、000 IOPS を超える場合、単一のボリュームでこのレベルの IOPS を実現するには、キュー深度を深くするか、複数のセッションが必要になる場合があります。

10. [Create Volume] を選択します。

ボリュームに **QoS** ポリシーを適用します

NetApp Hybrid Cloud Control を使用して、既存のストレージボリュームに QoS ポリシーを適用できます。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. 「* Volumes * > * Overview *」を選択します。
4. Volumes (ボリューム) テーブルの * Actions (アクション) * 列で、ボリュームのメニューを展開し、* Edit (編集) * を選択します。
5. 次のいずれかを実行して QoS を変更します。
 - a. 既存のポリシーを選択してください。
 - b. Custom Settings で、IOPS の最小値、最大値、バースト値を設定するか、またはデフォルト値を使用します。



ボリュームで QoS ポリシーを使用している場合は、カスタム QoS を設定して、ボリュームとの QoS ポリシーの所属を削除できます。カスタム QoS は、ボリュームの QoS 設定で QoS ポリシーの値を上書きします。



IOPS の値を変更する場合は、10 または 100 単位で増分します。入力値には有効な整数を指定する必要があります。ボリュームのバースト値はできるだけ高くします。バースト値を非常に高く設定することで、たまに発生する大規模ブロックのシーケンシャルワークロードを迅速に処理できる一方で、平常時の IOPS は引き続き抑制することができます。

6. [保存 (Save)] を選択します。

ボリュームの編集

NetApp Hybrid Cloud Control を使用して、QoS 値、ボリュームのサイズ、バイト値の計算単位などのボリューム属性を編集できます。レプリケーションで使用するため、またはボリュームへのアクセスを制限するために、アカウントアクセスを変更することもできます。

タスクの内容

次の状況下でクラスタに十分なスペースがある場合は、ボリュームのサイズを変更できます。

- 正常な動作状態。
- ボリュームのエラーまたは障害が報告されている。
- ボリュームをクローニングしています。
- ボリュームの再同期中。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. 「 * Volumes * > * Overview * 」を選択します。
4. Volumes (ボリューム) テーブルの * Actions (アクション) * 列で、ボリュームのメニューを展開し、 * Edit (編集) * を選択します。
5. 必要に応じて変更を加えます。
 - a. ボリュームの合計サイズを変更します。



ボリュームのサイズは、増やすことはできますが、減らすことはできません。1 回の処理でサイズ変更できるのは、1 つのボリュームのみです。ガベージコレクションやソフトウェアのアップグレードを実行しても、サイズ変更処理は中断されません。



レプリケーション用にボリュームサイズを調整する場合は、最初にレプリケーションターゲットとして割り当てられているボリュームのサイズを拡張します。次に、ソースボリュームのサイズを変更します。ターゲットボリュームのサイズは、ソースボリュームと同じかそれ以上のサイズにすることはできますが、ソースボリュームより小さくすることはできません。



デフォルトで選択されているボリュームサイズの単位は GB です。ボリュームは、GB または GiB 単位のサイズを使用して作成できます。1GB = 1 000 000 000 バイト 1GiB = 1 073 741 824 バイト

b. 別のアカウントアクセスレベルを選択します。

- 読み取り専用
- 読み取り / 書き込み
- ロック済み
- レプリケーションターゲット

c. ボリュームへのアクセスを許可するアカウントを選択します。

名前の先頭部分を入力すると、オートコンプリート機能によって、候補が表示されます。

アカウントが存在しない場合は、「* 新規アカウントの作成 *」を選択し、新しいアカウント名を入力して「* 作成 *」を選択します。アカウントが作成され、既存のボリュームに関連付けられます。

d. 次のいずれかを実行して QoS を変更します。

- i. 既存のポリシーを選択してください。
- ii. Custom Settings で、IOPS の最小値、最大値、バースト値を設定するか、またはデフォルト値を使用します。



ボリュームで QoS ポリシーを使用している場合は、カスタム QoS を設定して、ボリュームとの QoS ポリシーの所属を削除できます。カスタム QoS は、ボリュームの QoS 設定の QoS ポリシー値を上書きします。



IOPS の値は、10 または 100 単位で増減する必要があります。入力値には有効な整数を指定する必要があります。ボリュームのバースト値はできるだけ高くします。バースト値を非常に高く設定することで、たまに発生する大規模ブロックのシーケンシャルワークロードを迅速に処理できる一方で、平常時の IOPS は引き続き抑制することができます。

6. [保存 (Save)] を選択します。

クローンボリューム

単一のストレージボリュームのクローンを作成したり、ボリュームのグループをクローニングしてデータのポイントインタイムコピーを作成したりできます。ボリュームをクローニングすると、ボリュームの Snapshot が作成され、次にその Snapshot が参照しているデータのコピーが作成されます。

必要なもの

- クラスタが少なくとも 1 つ追加されて実行されている必要があります。
- 少なくとも 1 つのボリュームが作成されている必要があります。
- ユーザアカウントが作成されている必要があります。
- ボリュームのサイズと同じかそれ以上のプロビジョニングされていない利用可能なスペースが必要です。

タスクの内容

クラスタでは、ボリュームあたり一度に実行できるクローン要求は最大 2 つ、アクティブなボリュームのクローン処理は最大 8 件までサポートされます。これらの制限を超える要求はキューに登録され、あとで処理されます。

ボリュームクローニングは非同期のプロセスであり、クローニングするボリュームのサイズおよび現在のクラスタの負荷によって所要時間が異なります。



クローンボリュームには、ソースボリュームのボリュームアクセスグループメンバーシップは継承されません。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. [* Volumes (ボリューム) > Overview (概要) *] タブを選択します。
4. クローニングする各ボリュームを選択し、表示される*[クローン]*ボタンを選択します。
5. 次のいずれかを実行します。
 - 単一のボリュームをクローニングするには、次の手順を実行します。
 - i. [* Clone Volume * (* クローンボリューム *)] ダイアログボックスで、ボリュームクローンのボリューム名を入力します。



わかりやすい名前のベストプラクティスを使用してください。これは、環境で複数のクラスタや vCenter Server を使用している場合に特に重要です。

- ii. アカウントアクセスレベルを選択します。
 - 読み取り専用
 - 読み取り / 書き込み
 - ロック済み
 - レプリケーションターゲット
- iii. ボリュームクローンのサイズ (GB または GiB) を選択します。



クローンのボリュームサイズを拡張すると、末尾に空きスペースが追加された新しいボリュームが作成されます。ボリュームの使用方法によっては、新しい空きスペースを使用するために、空きスペースでパーティションの拡張または新しいパーティションの作成が必要になる場合があります。

- iv. ボリュームクローンに関連付けるアカウントを選択します。

アカウントが存在しない場合は、「* 新規アカウントの作成 *」を選択し、新しいアカウント名を入力して「* 作成 *」を選択します。アカウントが作成され、ボリュームに関連付けられます。

- v. [* Clone Volumes] を選択します。

- 複数のボリュームをクローニングするには、次の手順を実行します。
 - i. [* Clone Volumes] ダイアログ・ボックスで [* New Volume Name Prefix] フィールドに 'ボリューム

ム・クローンの任意のプレフィックスを入力します

- ii. ボリュームクローンの新しいアクセスタイプを選択するか、アクティブボリュームからアクセスタイプをコピーします。
- iii. ボリュームクローンに関連付ける新しいアカウントを選択するか、アクティブボリュームからアカウントの関連付けをコピーします。
- iv. [* Clone Volumes] を選択します。



クローニング処理が完了するまでの時間は、ボリュームサイズおよび現在のクラスタの負荷によって異なります。クローンボリュームがボリュームリストに表示されない場合は、ページを更新してください。

ボリュームを削除する

Element ストレージクラスタから 1 つ以上のボリュームを削除できます。

タスクの内容

削除されたボリュームはすぐにパージされるわけではなく、約 8 時間使用可能な状態のままになります。8 時間が経過すると消去され、利用できなくなります。パージされる前にボリュームをリストアすると、ボリュームはオンラインに戻り、iSCSI接続がリストアされます。

Snapshot の作成に使用されたボリュームを削除すると、関連付けられている Snapshot は非アクティブになります。削除したソースボリュームがパージされると、関連する非アクティブな Snapshot もシステムから削除されます。



管理サービスに関連付けられた永続ボリュームが作成され、インストールまたはアップグレード時に新しいアカウントに割り当てられます。永続ボリュームを使用している場合は、ボリュームや関連付けられているアカウントを変更または削除しないでください。これらのボリュームを削除すると、管理ノードが使用できなくなる可能性があります。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. 「* Volumes * > * Overview *」を選択します。
4. 削除するボリュームを 1 つ以上選択します。
5. 次のいずれかを実行します。
 - 複数のボリュームを選択した場合は、テーブル上部の*[Delete]*クイックフィルタを選択します。
 - 単一のボリュームを選択した場合は、Volumes (ボリューム) テーブルの * Actions (アクション) * 列で、ボリュームのメニューを展開し、* Delete (削除) * を選択します。
6. 「* はい *」を選択して削除を確認します。

削除したボリュームをリストアします

削除したストレージボリュームは、削除後 8 時間以内にリストア可能です。

削除されたボリュームはすぐにパージされるわけではなく、約 8 時間使用可能な状態のままになります。8 時

間が経過すると消去され、利用できなくなります。パーズされる前にボリュームをリストアすると、ボリュームはオンラインに戻り、iSCSI接続がリストアされます。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. 「* Volumes * > * Overview *」を選択します。
4. 「削除済み」を選択します。
5. Volumes (ボリューム) テーブルの * Actions (アクション) * 列で、ボリュームのメニューを展開し、* Restore (リストア) * を選択します。
6. [はい] を選択してプロセスを確認します。

削除したボリュームをパーズします

削除したストレージボリュームは、約 8 時間は引き続き使用できます。8 時間が経過すると自動的にパーズされ、使用できなくなります。8 時間待つ必要がない場合は、を削除します

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. 「* Volumes * > * Overview *」を選択します。
4. 「削除済み」を選択します。
5. パーズするボリュームを 1 つ以上選択します。
6. 次のいずれかを実行します。
 - 複数のボリュームを選択した場合は、テーブルの上部にある * Purge * クイック・フィルタを選択します。
 - 1 つのボリュームを選択した場合は、Volumes (ボリューム) テーブルの * Actions (アクション) * 列で、ボリュームのメニューを展開し、* Purge * を選択します。
7. Volumes (ボリューム) テーブルの * Actions (アクション) * 列で、ボリュームのメニューを展開し、* Purge * を選択します。
8. [はい] を選択してプロセスを確認します。

詳細情報

- ["ボリュームについて学習する"](#)
- ["ボリュームを操作します"](#)
- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

ボリュームアクセスグループを作成および管理します

NetApp Hybrid Cloud Control を使用して、新しいボリュームアクセスグループを作成したり、名前、関連付けられているイニシエータ、またはアクセスグループの関連付けられているボリュームを変更したり、既存のボリュームアクセスグループを削除したりできます。

必要なもの

- この NetApp HCI システムの管理者クレデンシャルが必要です。
- 管理サービスをバージョン 2.15.28 以上にアップグレードしておきます。NetApp Hybrid Cloud Control のストレージ管理は、それよりも前のバージョンのサービスバンドルでは利用できません。
- ボリュームアクセスグループの論理的な命名規則があることを確認します。

ボリュームアクセスグループを追加

NetApp Hybrid Cloud Control を使用して、ストレージクラスタにボリュームアクセスグループを追加できます。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. [* Volumes (ボリューム)] を選択します
4. [* アクセスグループ *] タブを選択します。
5. [アクセスグループの作成 *] ボタンを選択します。
6. 表示されたダイアログで、新しいボリュームアクセスグループの名前を入力します。
7. (オプション) 「* Initiators *」セクションで、新しいボリュームアクセスグループに関連付けるイニシエータを 1 つ以上選択します。

イニシエータをボリュームアクセスグループに関連付けると、そのイニシエータはグループ内の各ボリュームに認証なしでアクセスできます。

8. (オプション) * Volumes * セクションで、このボリュームアクセスグループに含めるボリュームを 1 つ以上選択します。
9. [アクセスグループの作成 *] を選択します。

ボリュームアクセスグループを編集します

NetApp Hybrid Cloud Control を使用して、既存のボリュームアクセスグループのプロパティを編集できます。アクセスグループの名前、関連付けられているイニシエータ、または関連付けられているボリュームを変更できます。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。

2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. [* Volumes (ボリューム)] を選択します
4. [* アクセスグループ*] タブを選択します。
5. アクセスグループテーブルの *Actions* 列で、編集する必要があるアクセスグループのオプションメニューを展開します。
6. オプションメニューで、* 編集 * を選択します。
7. 名前、関連付けられているイニシエータ、または関連付けられているボリュームに必要な変更を加えます。
8. [保存 (Save)] を選択して変更を確認します。
9. **Access Groups** テーブルで、アクセスグループに変更が反映されていることを確認します。

ボリュームアクセスグループを削除する

NetApp Hybrid Cloud Control を使用してボリュームアクセスグループを削除し、同時にこのアクセスグループに関連付けられているイニシエータをシステムから削除することができます。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. [* Volumes (ボリューム)] を選択します
4. [* アクセスグループ*] タブを選択します。
5. アクセスグループテーブルの *Actions* 列で、削除するアクセスグループのオプションメニューを展開します。
6. オプションメニューで、* 削除 * を選択します。
7. アクセスグループに関連付けられているイニシエータを削除しない場合は、「* このアクセスグループ内のイニシエータを削除する *」チェックボックスの選択を解除します。
8. [はい] を選択して、削除操作を確認します。

詳細情報

- ["ボリュームアクセスグループについて学習する"](#)
- ["ボリュームアクセスグループにイニシエータを追加します"](#)
- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

イニシエータを作成および管理する

ボリュームへのアカウントベースではなくCHAPベースのアクセスにを使用できます"[イニシエータ](#)"。イニシエータを作成および削除したり、管理やボリュームアクセスを簡単にするためにわかりやすいエイリアスを指定したりできます。ボリュームアクセスグループに追加されたイニシエータは、グループ内のすべてのボリュームにアクセスできる

ようになります。

必要なもの

- クラスタ管理者のクレデンシャルが必要です。
- 管理サービスをバージョン 2.17 以上にアップグレードしておきます。NetApp Hybrid Cloud Control のイニシエータ管理は、それよりも前のバージョンのサービスバンドルでは使用できません。

オプション

- [\[イニシエータを作成します\]](#)
- [\[ボリュームアクセスグループにイニシエータを追加します\]](#)
- [\[イニシエータエイリアスを変更します\]](#)
- [\[イニシエータを削除する\]](#)

イニシエータを作成します

iSCSI イニシエータまたは Fibre Channel イニシエータを作成し、オプションでエイリアスを割り当てることができます。

タスクの内容

イニシエータIQNの有効な形式は、です。 `iqn.yyyy-mm`y`とmは数字で、続けて任意の文字列を指定します。使用できる文字は、数字、小文字のアルファベット、ピリオド (.)、コロン (:)、ダッシュ (-) です。形式の例を次に示します。`

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

Fibre ChannelイニシエータWWPNの有効な形式は `:Aa:bB:CC:dd:11:22:33:44`、または ``AabBCCdd11223344`` です。形式の例を次に示します。

```
5f:47:ac:c0:5c:74:d4:02
```

手順

1. Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. `[* Volumes (ボリューム)]` を選択します
4. イニシエータ * タブを選択します。
5. イニシエータの作成 * ボタンを選択します。

オプション	手順
1つ以上のイニシエータを作成します	<ul style="list-style-type: none"> a. IQN または WWPN * フィールドにイニシエータの IQN または WWPN を入力します。 b. [* エイリアス] フィールドにイニシエータのフレンドリ名を入力します。 c. (オプション) Add Initiator * を選択して新しいイニシエータフィールドを開くか、代わりに bulk create オプションを使用します。 d. イニシエータの作成 * を選択します。
イニシエータを一括作成します	<ul style="list-style-type: none"> a. 「 * Bulk Add IQs/WWPN * 」を選択します。 b. IQN または WWPN のリストをテキストボックスに入力します。各 IQN または WWPN は、カンマまたはスペースで区切って指定するか、または独自の行に入力する必要があります。 c. [* IQN / WWPN の追加 *] を選択します。 d. (オプション) 各イニシエータに一意的エイリアスを追加します。 e. インストール環境にすでに存在する可能性のあるイニシエータをリストから削除します。 f. イニシエータの作成 * を選択します。

ボリュームアクセスグループにイニシエータを追加します

ボリュームアクセスグループにイニシエータを追加できます。イニシエータをボリュームアクセスグループに追加すると、そのイニシエータはそのボリュームアクセスグループ内のすべてのボリュームにアクセスできるようになります。

手順

1. Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. [* Volumes (ボリューム)] を選択します
4. イニシエータ * タブを選択します。
5. 追加するイニシエータを 1 つ以上選択します。
6. [* アクション] > [アクセスグループに追加 *] を選択します。
7. アクセスグループを選択します。
8. [イニシエータの追加] を選択して変更を確認します。

イニシエータエイリアスを変更します

既存のイニシエータのエイリアスを変更するか、既存のエイリアスがない場合はエイリアスを追加できます。

手順

1. Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. [* Volumes (ボリューム)] を選択します
4. イニシエータ * タブを選択します。
5. [*Actions] 列で、イニシエータのオプション・メニューを展開します。
6. 「* 編集 *」を選択します。
7. エイリアスに必要な変更を加えるか、新しいエイリアスを追加します。
8. [保存 (Save)] を選択します。

イニシエータを削除する

1 つ以上のイニシエータを削除できます。イニシエータを削除すると、関連付けられているすべてのボリュームアクセスグループから削除されます。イニシエータを使用した接続は、接続をリセットするまでは有効なままです。

手順

1. Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. [* Volumes (ボリューム)] を選択します
4. イニシエータ * タブを選択します。
5. 1 つ以上のイニシエータを削除します。
 - a. 削除するイニシエータを 1 つ以上選択します。
 - b. [* アクション > 削除 (* Actions > Delete *)] を選択
 - c. 削除操作を確定し、* はい * を選択します。

詳細情報

- ["イニシエータについて学習する"](#)
- ["ボリュームアクセスグループについて学習する"](#)
- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

ボリュームの QoS ポリシーの作成と管理

標準的なサービス品質設定を QoS ポリシーとして作成および保存して、複数のボリューム

ムに適用することができます。QoS ポリシーを使用するには、Element 10.0 以降のクラスタを選択する必要があります。10.0 より前のクラスタでは QoS ポリシーを使用できません。



個々のボリュームではなくを使用する方法の詳細については、「NetApp HCIの概念」のコンテンツを参照してください"[QoSポリシー](#)"["QoS"](#)。

NetApp Hybrid Cloud Control を使用すると、次のタスクを実行して QoS ポリシーを作成および管理できます。

- [QoS ポリシーを作成する](#)
- [ボリュームに QoS ポリシーを適用します](#)
- [ボリュームの QoS ポリシーの割り当てを変更します](#)
- [QoS ポリシーを編集する](#)
- [QoS ポリシーを削除する](#)

QoS ポリシーを作成する

QoS ポリシーを作成し、同等のパフォーマンスが必要なボリュームに適用することができます。



QoS ポリシーを使用している場合は、ボリュームでカスタム QoS を使用しないでください。カスタム QoS は、ボリュームの QoS 設定に対して QoS ポリシーの値を上書きして調整します。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで、ストレージクラスタのメニューを展開します。
3. Storage > Volumes (ストレージ) を選択します。
4. [* QoS Policies] タブを選択します。
5. [* ポリシーの作成 *] を選択します。
6. 「* ポリシー名 *」を入力します。



わかりやすい名前のベストプラクティスを使用してください。これは、環境で複数のクラスタや vCenter Server を使用している場合に特に重要です。

7. 最小 IOPS、最大 IOPS、バースト IOPS の値を入力します。
8. [Create QoS Policy] を選択します。

ポリシーのシステム ID が生成され、そのポリシーが割り当てられた QoS 値を含む QoS ポリシーページに表示されます。

ボリュームに **QoS** ポリシーを適用します

NetApp Hybrid Cloud Control を使用して、既存の QoS ポリシーをボリュームに割り当てることができます。

必要なもの

割り当てる QoS ポリシーを選択しておき **作成済み** ます。

タスクの内容

このタスクでは、設定を変更して個々のボリュームに QoS ポリシーを割り当てる方法について説明します。最新バージョンの NetApp Hybrid Cloud Control では、複数のボリュームに一括割り当てオプションはありません。一括割り当てする機能が今後のリリースで提供されるまでは、Element Web UI または vCenter Plug-in UI を使用して QoS ポリシーを一括で割り当てることができます。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで、ストレージクラスタのメニューを展開します。
3. Storage > Volumes (ストレージ) を選択します。
4. 変更するボリュームの横にある * Actions * (アクション) メニューを選択します。
5. 表示されたメニューで、「* 編集 *」を選択します。
6. ダイアログボックスで、* QoS ポリシーの割り当て * を有効にし、選択したボリュームに適用する QoS ポリシーをドロップダウンリストから選択します。



QoS を割り当てると、以前に適用されていた個々のボリュームの QoS 値は上書きされま
す。

7. [保存 (Save)] を選択します。

更新されたボリュームが割り当てられた QoS ポリシーで概要ページに表示されます。

ボリュームの **QoS** ポリシーの割り当てを変更します

ボリュームから QoS ポリシーの割り当てを解除したり、別の QoS ポリシーやカスタム QoS を選択したりで
きます。

必要なもの

変更するボリュームが QoS ポリシーである **割り当て済み**。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで、ストレージクラスタのメニューを展開します。
3. Storage > Volumes (ストレージ) を選択します。
4. 変更するボリュームの横にある * Actions * (アクション) メニューを選択します。
5. 表示されたメニューで、「* 編集 *」を選択します。

6. ダイアログボックスで、次のいずれかを実行します。

- QoS ポリシーの割り当てを無効にし、個々のボリュームの QoS の最小 IOPS *、最大 IOPS *、バースト IOPS * の値を変更します。



QoS ポリシーが無効な場合、特に変更されていないかぎり、ボリュームはデフォルトの QoS IOPS 値を使用します。

- 選択したボリュームに適用する別の QoS ポリシーをドロップダウンリストから選択してください。

7. [保存 (Save)] を選択します。

更新されたボリュームが概要ページに表示されます。

QoS ポリシーを編集する

既存の QoS ポリシーの名前を変更したり、ポリシーに関連付けられている値を編集したりできます。QoS ポリシーのパフォーマンス値を変更すると、そのポリシーに関連付けられているすべてのボリュームの QoS に影響します。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで、ストレージクラスタのメニューを展開します。
3. Storage > Volumes (ストレージ) を選択します。
4. [* QoS Policies] タブを選択します。
5. 変更する QoS ポリシーの横にある * Actions * メニューを選択します。
6. 「* 編集 *」を選択します。
7. [Edit QoS Policy] ダイアログボックスで、次の 1 つ以上を変更します。
 - * Name * : QoS ポリシーのユーザ定義名。
 - * Min IOPS * : ボリュームに対して保証されている最小 IOPS 。デフォルト値は 50 です。
 - * Max IOPS * : ボリュームで許可されている最大 IOPS 。デフォルト値は15,000です。
 - * Burst IOPS * : ボリュームに対して短期間で許可されている最大 IOPS 。デフォルト値は15,000です。
8. [保存 (Save)] を選択します。

更新された QoS ポリシーが [QoS Policies] ページに表示されます。



ポリシーの*[アクティブボリューム]*列でリンクを選択すると、そのポリシーに割り当てられているボリュームだけでフィルタリングされたリストを表示できます。

QoS ポリシーを削除する

不要になった QoS ポリシーを削除できます。QoS ポリシーを削除しても、そのポリシーが割り当てられたすべてのボリュームで、それまでにそのポリシーで定義されていた QoS 値が個々のボリュームの QoS 値とし

て維持されます。削除された QoS ポリシーとの関連付けがすべて削除されます。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで、ストレージクラスタのメニューを展開します。
3. Storage > Volumes (ストレージ) を選択します。
4. [* QoS Policies] タブを選択します。
5. 変更する QoS ポリシーの横にある * Actions * メニューを選択します。
6. 「* 削除」を選択します。
7. 操作を確定します。

詳細情報

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp SolidFire and Element ドキュメントセンター \(ドキュメントセンターのバージョン\) "](#)

管理ノードを操作します

管理ノードの概要

管理ノード (mNode) は、システムサービスの使用、クラスタのアセットと設定の管理、システムのテストとユーティリティの実行、システム監視用の Active IQ の設定、トラブルシューティング用のネットアップサポートアクセスの有効化に使用できます。

Element ソフトウェアバージョン 11.3 以降を実行するクラスタでは、次のいずれかのインターフェイスを使用して管理ノードを操作できます。

- 管理ノードUI('https:// [mNode IP]:442'を使用) では、ネットワークとクラスタの設定を変更したり、システムテストを実行したり、システムユーティリティを使用したりできます。
- 組み込みのREST API UI('https://[mNode IP]/mnode'を使用) を使用して、プロキシサーバの設定、サービスレベルの更新、資産管理など、管理ノードのサービスに関連するAPIを実行したり理解したりできます。

管理ノードをインストールまたはリカバリします。

- ["管理ノードをインストール"](#)
- ["ストレージネットワークインターフェイスコントローラ \(NIC\) の設定"](#)
- ["管理ノードをリカバリ"](#)

管理ノードにアクセスします。

- ["管理ノード \(UI または REST API\) へのアクセス"](#)

デフォルトのSSL証明書を変更します。

- ["管理ノードのデフォルトSSL証明書を変更します"](#)

管理ノード UI を使用してタスクを実行します。

- ["管理ノード UI の概要"](#)

管理ノード REST API を使用してタスクを実行します。

- ["管理ノードの REST API UI の概要"](#)

リモート SSH 機能を無効または有効にするか、ネットアップサポートとのリモートサポートトンネルセッションを開始して、トラブルシューティングに役立ててください。

- ["ネットアップサポートによるリモート接続を有効にする"](#)
- ["管理ノードで SSH 機能を管理します"](#)

詳細情報

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

管理ノードをインストールまたはリカバリします

管理ノードをインストール

NetApp Element ソフトウェアを実行しているクラスタの管理ノードは、構成に応じたイメージを使用して手動でインストールできます。

この手動プロセスは、管理ノードのインストールに NetApp Deployment Engine を使用していない NetApp HCI 管理者を対象としています。

必要なもの

- クラスタバージョンで NetApp Element ソフトウェア 11.3 以降が実行されています。
- インストール環境では IPv4 を使用します。管理ノード 11.3 では IPv6 がサポートされません。



IPv6 のサポートが必要な場合は、管理ノード 11.1 を使用してください。

- NetApp Support Site からソフトウェアをダウンロードする権限が必要です。
- 使用するプラットフォームに適した管理ノードイメージのタイプを特定しておきます。

プラットフォーム	インストールイメージのタイプ
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso 、 .ova のいずれかです
Citrix XenServer	.iso

プラットフォーム	インストールイメージのタイプ
OpenStack	.iso

- (管理ノード 12.0 および 12.2 でプロキシサーバを使用) プロキシサーバを設定する前に、NetApp Hybrid Cloud Control を管理サービスバージョン 2.16 に更新しました。

タスクの内容

Element 12.2管理ノードはオプションのアップグレードです。既存の環境では必要ありません。

この手順を実行する前に、これらの手順を理解し、使用するかどうかを判断しておく必要があります"永続ボリューム"。永続ボリュームはオプションですが、仮想マシン (VM) が失われた場合の管理ノードの設定データのリカバリには推奨されます。

手順

1. ISO または OVA をダウンロードし、VM を導入します
2. [管理ノード管理者を作成し、ネットワークを設定]
3. [時刻同期を設定します]
4. [管理ノードをセットアップ]
5. [コントローラアセットを設定する]
6. (NetApp HCI のみ) コンピューティングノードアセットを設定します

ISO または OVA をダウンロードし、VM を導入します

1. NetAppサポートサイトのページから、インストールに対応したOVAまたはISOをダウンロードし "NetApp HCI" ます。
 - a. Download Latest Release * を選択し、EULA に同意します。
 - b. ダウンロードする管理ノードのイメージを選択します。
2. OVA をダウンロードした場合は、次の手順を実行します。
 - a. OVA を導入します。
 - b. ストレージクラスが管理ノード (eth0) とは別のサブネット上にある環境で永続ボリュームを使用する場合は、ストレージサブネット (eth1 など) 上の VM に 2 つ目のネットワークインターフェイスコントローラ (NIC) を追加するか、管理ネットワークからストレージネットワークヘルパーティング可能なことを確認します。
3. ISO をダウンロードした場合は、次の手順を実行します。
 - a. 次の構成でハイパーバイザーから新しい 64 ビットの VM を作成します。
 - 仮想 CPU × 6
 - 24GBのRAM
 - ストレージアダプタのタイプが LSI Logic Parallel に設定されています



管理ノードのデフォルトは LSI Logic SAS になる場合があります。[* 新しい仮想マシン*] ウィンドウで、[* ハードウェアのカスタマイズ* > * 仮想ハードウェア*] を選択して、ストレージ・アダプターの構成を確認します。必要に応じて、LSI Logic SAS を * LSI Logic Parallel * に変更します。

- 400GB の仮想ディスク、シンプロビジョニング
- インターネットアクセスとストレージ MVIP へのアクセスが可能な仮想ネットワークインターフェイス × 1
- ストレージクラスタへの管理ネットワークアクセスが可能な仮想ネットワークインターフェイス × 1。ストレージクラスタが管理ノード（eth0）とは別のサブネット上にある環境で永続ボリュームを使用する場合は、ストレージサブネット（eth1）上の VM に 2 つ目のネットワークインターフェイスコントローラ（NIC）を追加するか、管理ネットワークからストレージネットワークへルーティング可能なことを確認します。



この手順の以降の手順で指示があるまでは、VM の電源をオンにしないでください。

b. ISO を VM に接続し、.iso インストールイメージでブートします。



イメージを使用して管理ノードをインストールすると、スプラッシュ画面が表示されるまでに 30 秒程度かかることがあります。

4. インストールが完了したら、管理ノードの VM の電源をオンにします。

管理ノード管理者を作成し、ネットワークを設定

1. ターミナルユーザインターフェイス（TUI）を使用して、管理ノードの管理ユーザを作成します。



メニューオプションを移動するには、上矢印キーまたは下矢印キーを押します。ボタン間を移動するには、Tab キーを押します。ボタンからフィールドに移動するには、Tab キーを押します。フィールド間を移動するには、上矢印キーまたは下矢印キーを押します。

2. ネットワーク上に、最大伝送ユニット（MTU）が 1500 バイト未満の IP を割り当てる Dynamic Host Configuration Protocol（DHCP；動的ホスト構成プロトコル）サーバがある場合は、次の手順を実行する必要があります。

- a. iSCSI などの DHCP を使用しないで、一時的に管理ノードを vSphere ネットワークに配置します。
- b. VM をリブートするか、VM ネットワークを再起動します。
- c. TUI を使用して、管理ネットワークの正しい IP を 1500 バイト以上の MTU で設定します。
- d. VM に正しい VM ネットワークを再割り当てします。



MTU が 1、500 バイト未満の DHCP を割り当てると、管理ノードネットワークの設定や管理ノード UI の使用ができなくなる可能性があります。

3. 管理ノードネットワーク（eth0）を設定します。



ストレージトラフィックを分離するために追加のNICが必要な場合は、別のNICの設定手順を参照してください。["ストレージネットワークインターフェイスコントローラ（NIC）の設定"](#)

時刻同期を設定します

1. NTP を使用して管理ノードとストレージクラスタの間で時刻が同期されていることを確認します。



Element 12..1 以降では、手順 (a) ~ (e) が自動的に実行されます。管理ノード12.3.1の場合は、に進み、サブステップ (f)時間の同期の設定を完了します。

1. SSH またはハイパーバイザーが提供するコンソールを使用して、管理ノードにログインします。
2. NTPDを停止します。

```
sudo service ntpd stop
```

3. NTP構成ファイルを編集し `etc/ntp.conf` ます。

- a. 各サーバの前に(server 0.gentoo.pool.ntp.org`を追加して、デフォルトサーバをコメントアウトします `#。
- b. 追加するデフォルトのタイムサーバごとに新しい行を追加します。デフォルトのタイムサーバは、で使用するストレージクラスタで使用されているNTPサーバと同じである必要があります"後の手順"。

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time server>
```

- c. 完了したら構成ファイルを保存します。

4. 新しく追加したサーバと NTP 同期を強制します。

```
sudo ntpd -gq
```

5. NTPD を再起動します。

```
sudo service ntpd start
```

6. [[ハイパーバイザーを介したホストとの時間同期を無効にします (VMware の例を次に示します) 。



OpenStack 環境の .iso イメージなどで、VMware 以外のハイパーバイザー環境に mNode を導入する場合は、同等のコマンドについてハイパーバイザーのドキュメントを参照してください。

- a. 定期的な時刻同期を無効にします。

```
vmware-toolbox-cmd timesync disable
```

- b. サービスの現在のステータスを表示して確認します。

```
vmware-toolbox-cmd timesync status
```

- c. vSphereで、VMオプションのチェックボックスがオフになっていることを確認し `Synchronize guest time with host` ます。



今後 VM を変更する場合は、このオプションを有効にしないでください。



時刻の同期設定が完了したらNTPを編集しないでください。管理ノードで実行するとNTPに影響するためです。"[Setup コマンド](#)"

管理ノードをセットアップ

1. 管理ノードのセットアップコマンドを設定して実行します。



セキュアプロンプトにパスワードを入力するように求められます。クラスタがプロキシサーバーの背後にある場合、パブリックネットワークに接続できるようにプロキシを設定する必要があります。

```
sudo /sf/packages/mnode/setup-mnode --mnode_admin_user [username]
--storage_mvip [mvip] --storage_username [username] --telemetry_active
[true]
```

- a. 次の各必須パラメータについて、[] ブラケット（ブラケットを含む）の値を置き換えます。



内はコマンドの省略名で、正式な名前の代わりに使用できます。


- * `--mnode_admin_user (-mu) [username]` * : 管理ノードの管理者アカウントのユーザ名。一般には、管理ノードへのログインに使用したユーザアカウントのユーザ名です。
- * `--storage_mvip (-SM) [MVIP アドレス]` * : Element ソフトウェアを実行しているストレージクラスタの管理仮想 IP アドレス (MVIP)。で使用したストレージクラスタを使用して管理ノードを設定し "[NTP サーバの設定](#)" ます。
- `--storage_username (-su) [username]` : パラメータで指定したクラスタのストレージクラスタ管理者のユーザ名 `--storage_mvip`。
- * `--metal_active (-t) [true]` * : Active IQ による分析のためのデータ収集を有効にする値を true のままにします。

- b. (オプション) : Active IQ エンドポイントのパラメータをコマンドに追加します。

- * `--remote_host (-RH) [AIQ_endpoint]` * : Active IQ のテレメトリデータの処理が行われるエンドポイント。このパラメータを指定しない場合は、デフォルトのエンドポイントが使用されま

す。

- c. (推奨) : 永続ボリュームに関する以下のパラメータを追加します。永続ボリューム機能用に作成されたアカウントとボリュームを変更または削除しないでください。変更または削除すると、管理機能が失われます。
 - * `--use_persistent_volumes (-pv) [true/false、デフォルト: false]*` : 永続ボリュームを有効または無効にします。永続ボリューム機能を有効にするには、`true` を入力します。
 - `--persistent_volumes_account (-pva) [account_name]` : が `true` に設定されている場合、`--use_persistent_volumes` は、このパラメータを使用して、永続ボリュームに使用するストレージアカウント名を入力します。

 永続ボリュームには、クラスタ上の既存のアカウント名とは異なる一意のアカウント名を使用してください。永続ボリュームのアカウントを他の環境から切り離すことが非常に重要です。

- * `- persistent_volumes_mvip (-pvm) [mvip]*` : 永続ボリュームで使用する Element ソフトウェアを実行しているストレージクラスタの管理仮想 IP アドレス (MVIP) を入力します。このパラメータは、管理ノードで複数のストレージクラスタが管理されている場合にのみ必要です。複数のクラスタを管理していない場合は、デフォルトのクラスタ MVIP が使用されます。
- d. プロキシサーバを設定します。
 - * `--use_proxy (-up) [true/false、default: false]*` : プロキシの使用を有効または無効にします。このパラメータは、プロキシサーバを設定する場合に必要です。
 - * `--proxy_hostname_or_IP (-pi) [-host]*` : プロキシのホスト名または IP。プロキシを使用する場合は必須です。これを指定すると、入力を求めるプロンプトが表示され `--proxy_port` ます。
 - `--proxy_username (-pu) [username]` : プロキシユーザ名。このパラメータはオプションです。
 - `--proxy_password (-pp)[password]` : プロキシパスワード。このパラメータはオプションです。
 - * `--proxy_port (-pq) [port、default: 0]*` : プロキシポート。これを指定すると、プロキシホスト名または IP を入力するように求められ (`--proxy_hostname_or_ip` ます)。
 - * `--proxy_ssh_port (-ps) [port、default: 443]*` : SSH プロキシポート。デフォルト値はポート 443 です。
- e. (オプション) 各パラメータに関する追加情報が必要な場合は、`help` パラメータを使用します。
 - `--help(-h)` : 各パラメータに関する情報を返します。パラメータは、初期導入時に必須またはオプションとして定義します。アップグレードと再導入ではパラメータの要件が異なる場合があります。
- f. コマンドを実行します `setup-mnode`。

コントローラアセットを設定する

1. インストール ID を確認します。
 - a. ブラウザから、管理ノードの REST API UI にログインします。
 - b. ストレージの MVIP に移動してログインします。この操作を実行すると、次の手順で証明書が承認されます。
 - c. 管理ノードでインベントリサービス REST API UI を開きます。

```
https://<ManagementNodeIP>/inventory/1/
```

- d. 「* Authorize *」（認証）を選択して、次の手順を実行
 - i. クラスタのユーザ名とパスワードを入力します。
 - ii. クライアントIDにと入力し `mnode-client` ます。
 - iii. セッションを開始するには、* Authorize * を選択します。
- e. REST API UI で、* 一部のユーザに一時的な処理を開始 / インストール * を選択します。
- f. [* 試してみてください *] を選択します。
- g. [* Execute] を選択します。
- h. コード200応答本文からをコピーして保存し、`id`後の手順で使用できるようにします。

インストール環境には、インストールまたはアップグレード時に作成されたベースアセットの構成が含まれています。

2. （NetApp HCI のみ）vSphere でコンピューティングノードのハードウェアタグを確認します。
 - a. vSphere Web Client ナビゲータでホストを選択します。
 - b. **[Monitor]** タブを選択し、**[Hardware Health]** を選択します。
 - c. ノードの BIOS のメーカーとモデル番号が表示されます。値をコピーして保存し、`tag`後の手順で使用します。
3. 管理ノードの既知のアセットに、NetApp HCI 監視用の vCenter コントローラアセット（NetApp HCI 環境のみ）と Hybrid Cloud Control（すべての環境）を追加します。
 - a. 管理ノードのIPアドレスに続けて次のように入力し、管理ノードのmnodeサービスAPI UIにアクセスし `mnode` ます。

```
https://<ManagementNodeIP>/mnode
```

- b. 「* Authorize *（認証）」または任意のロックアイコンを選択し、次の手順を実行します。
 - i. クラスタのユーザ名とパスワードを入力します。
 - ii. クライアントIDにと入力し `mnode-client` ます。
 - iii. セッションを開始するには、* Authorize * を選択します。
 - iv. ウィンドウを閉じます。
- c. コントローラサブアセットを追加する場合は、「* POST /assets/ { asset_id } /controllers *」を選択します。



コントローラサブアセットを追加する場合は、vCenter で新しい NetApp HCC ロールを作成することを推奨します。この新しい NetApp HCC ロールにより、管理ノードのサービス表示がネットアップ専用のアセットに制限されます。を参照して ["vCenter で NetApp HCC ロールを作成します"](#)

- d. [* 試してみてください *] を選択します。

- e. クリップボードにコピーした親ベースアセットの ID を * asset_id * フィールドに入力します。
- f. 必要なペイロード値をタイプとvCenterクレデンシャルとともに入力し `vCenter` ます。
- g. [* Execute] を選択します。

(NetApp HCI のみ) コンピューティングノードアセットを設定します

1. (NetApp HCI のみ) 管理ノードの既知のアセットにコンピューティングノードのアセットを追加します。
 - a. コンピューティングノードアセットのクレデンシャルを使用してコンピューティングノードサブアセットを追加する場合は、「* POST/assets/ { asset_id } /compute-nodes 」を選択します。
 - b. [* 試してみてください*]を選択します。
 - c. クリップボードにコピーした親ベースアセットの ID を * asset_id * フィールドに入力します。
 - d. ペイロードで、 Model タブで定義されているとおりに必要なペイロード値を入力します。と入力し ESXi Host type、の前の手順で保存したハードウェアタグを入力し `hardware_tag` ます。
 - e. [* Execute] を選択します。

詳細はこちら

- ["永続ボリューム"](#)
- ["管理ノードにアセットを追加します"](#)
- ["ストレージ NIC を設定します"](#)
- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

ストレージネットワークインターフェイスコントローラ (NIC) の設定

ストレージに追加の NIC を使用している場合は、SSH で管理ノードに接続するか、vCenter コンソールを使用して curl コマンドを実行し、タグ付きまたはタグなしのネットワークインターフェイスをセットアップできます。

必要なもの

- eth0 の IP アドレスを確認しておきます。
- クラスタバージョンで NetApp Element ソフトウェア 11.3 以降が実行されています。
- 管理ノード 11.3 以降を導入しておきます。

設定オプション

環境に適したオプションを選択します。

- [タグなしのストレージネットワークインターフェイスコントローラ \(NIC \) を設定します ネットワークインターフェイス](#)
- [タグ付きのストレージネットワークインターフェイスコントローラ \(NIC \) を設定します ネットワークインターフェイス](#)

タグなしのストレージネットワークインターフェイスコントローラ（NIC）を設定します ネットワークインターフェイス

手順

1. SSH または vCenter コンソールを開きます。
2. 次のコマンドテンプレートの値を置き換え、コマンドを実行します。



新しいストレージネットワークインターフェイスの各必須パラメータの値は、で示されま
す \$。`cluster` 次のテンプレート内のオブジェクトは必須であり、管理ノードのホスト名
の変更で使用できません。`--insecure` または `-k` オプションは本番環境では使用しないでくだ
さい。

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \  
https://$mnode_IP:442/json-rpc/10.0 \  
-H 'Content-Type: application/json' \  
-H 'cache-control: no-cache' \  
-d ' {  
    "params": {  
        "network": {  
            "$eth1": {  
                "#default" : false,  
                "address" : "$storage_IP",  
                "auto" : true,  
                "family" : "inet",  
                "method" : "static",  
                "mtu" : "9000",  
                "netmask" : "$subnet_mask",  
                "status" : "Up"  
            }  
        },  
        "cluster": {  
            "name": "$mnode_host_name"  
        }  
    },  
    "method": "SetConfig"  
}'
```

タグ付きのストレージネットワークインターフェイスコントローラ（NIC）を設定します ネットワークインターフェイス

手順

1. SSH または vCenter コンソールを開きます。
2. 次のコマンドテンプレートの値を置き換え、コマンドを実行します。



新しいストレージネットワークインターフェースの各必須パラメータの値は、で示されます。`cluster` 次のテンプレート内のオブジェクトは必須であり、管理ノードのホスト名の変更に使用できます。`--insecure` または `-k` オプションは本番環境では使用しないでください。

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
    "params": {
        "network": {
            "$eth1": {
                "#default" : false,
                "address" : "$storage_IP",
                "auto" : true,
                "family" : "inet",
                "method" : "static",
                "mtu" : "9000",
                "netmask" : "$subnet_mask",
                "status" : "Up",
                "virtualNetworkTag" : "$vlan_id"
            }
        },
        "cluster": {
            "name": "$mnode_host_name",
            "cipi": "$eth1.$vlan_id",
            "sipi": "$eth1.$vlan_id"
        }
    },
    "method": "SetConfig"
}
```

詳細はこちら

- ["管理ノードにアセットを追加します"](#)
- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

管理ノードをリカバリ

以前の管理ノードで永続ボリュームを使用していた場合は、NetApp Element ソフトウェアを実行しているクラスタの管理ノードを手動でリカバリして再導入できます。

新しい OVA を導入して再導入スクリプトを実行すると、バージョン 11.3 以降を実行していた以前の管理ノードから設定データを取得することができます。

必要なもの

- 以前の管理ノードで NetApp Element ソフトウェアバージョン 11.3 以降を実行しており、機能を使用していました "永続ボリューム"。
- 永続ボリュームを含むクラスタの MVIP と SVIP が必要です。
- クラスタバージョンで NetApp Element ソフトウェア 11.3 以降が実行されています。
- インストール環境では IPv4 を使用します。管理ノード 11.3 では IPv6 がサポートされません。
- NetApp Support Site からソフトウェアをダウンロードする権限が必要です。
- 使用するプラットフォームに適した管理ノードイメージのタイプを特定しておきます。

プラットフォーム	インストールイメージのタイプ
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso 、 .ova のいずれかです
Citrix XenServer	.iso
OpenStack	.iso

手順

1. ISO または OVA をダウンロードし、VM を導入します
2. [ネットワークを設定します]
3. [時刻同期を設定します]
4. [管理ノードを設定]

ISO または OVA をダウンロードし、VM を導入します

1. NetApp サポートサイトのページから、インストールに対応した OVA または ISO をダウンロードし "NetApp HCI" ます。
 - a. Download Latest Release * を選択し、EULA に同意します。
 - b. ダウンロードする管理ノードのイメージを選択します。
2. OVA をダウンロードした場合は、次の手順を実行します。
 - a. OVA を導入します。
 - b. ストレージクラスタが管理ノード (eth0) とは別のサブネット上にある環境で永続ボリュームを使用する場合は、ストレージサブネット (eth1 など) 上の VM に 2 つ目のネットワークインターフェイスコントローラ (NIC) を追加するか、管理ネットワークからストレージネットワークヘルパーティング可能なことを確認します。
3. ISO をダウンロードした場合は、次の手順を実行します。
 - a. 以下の構成でハイパーバイザーから新しい 64 ビットの仮想マシンを作成します。
 - 仮想 CPU × 6

- 24GBのRAM
- 400GB の仮想ディスク、シンプロビジョニング
- インターネットアクセスとストレージ MVIIP へのアクセスが可能な仮想ネットワークインターフェイス × 1
- ストレージクラスタへの管理ネットワークアクセスが可能な仮想ネットワークインターフェイス × 1。ストレージクラスタが管理ノード（eth0）とは別のサブネット上にある環境で永続ボリュームを使用する場合は、ストレージサブネット（eth1）上の VM に 2 つ目のネットワークインターフェイスコントローラ（NIC）を追加するか、管理ネットワークからストレージネットワークヘルテイング可能なことを確認します。



このあとの手順で指示があるまでは、仮想マシンの電源をオンにしないでください。

b. 仮想マシンに ISO を接続し、.iso インストールイメージでブートします。



イメージを使用して管理ノードをインストールすると、スプラッシュ画面が表示されるまでに 30 秒程度かかることがあります。

4. インストールが完了したら、管理ノードの仮想マシンの電源をオンにします。

ネットワークを設定します

1. ターミナルユーザインターフェイス（TUI）を使用して、管理ノードの管理ユーザを作成します。



メニューオプションを移動するには、上矢印キーまたは下矢印キーを押します。ボタン間を移動するには、Tab キーを押します。ボタンからフィールドに移動するには、Tab キーを押します。フィールド間を移動するには、上矢印キーまたは下矢印キーを押します。

2. 管理ノードネットワーク（eth0）を設定します。



ストレージトラフィックを分離するために追加のNICが必要な場合は、別のNICの設定手順を参照してください。["ストレージネットワークインターフェイスコントローラ（NIC）の設定"](#)

時刻同期を設定します

1. NTP を使用して管理ノードとストレージクラスタの間で時刻が同期されていることを確認します。



Element 12..1 以降では、手順（a）～（e）が自動的に実行されます。管理ノード12.3.1の場合は、に進み、[サブステップ \(f\)](#)時間の同期の設定を完了します。

1. SSH またはハイパーバイザーが提供するコンソールを使用して、管理ノードにログインします。

2. NTPDを停止します。

```
sudo service ntpd stop
```

3. NTP構成ファイルを編集し`/etc/ntp.conf`ます。

- a. 各サーバの前に(server 0.gentoo.pool.ntp.org`を追加して、デフォルトサーバをコメントアウトします`#。
- b. 追加するデフォルトのタイムサーバごとに新しい行を追加します。デフォルトのタイムサーバは、で使用するストレージクラスタで使用されているNTPサーバと同じである必要があります"後の手順"。

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time server>
```

- c. 完了したら構成ファイルを保存します。

4. 新しく追加したサーバと NTP 同期を強制します。

```
sudo ntpd -gq
```

5. NTPD を再起動します。

```
sudo service ntpd start
```

6. [[ハイパーバイザーを使用したホストとの時間同期を無効にします（VMware の例を次に示します）。



OpenStack 環境の .iso イメージなどで、VMware 以外のハイパーバイザー環境に mNode を導入する場合は、同等のコマンドについてハイパーバイザーのドキュメントを参照してください。

- a. 定期的な時刻同期を無効にします。

```
vmware-toolbox-cmd timesync disable
```

- b. サービスの現在のステータスを表示して確認します。

```
vmware-toolbox-cmd timesync status
```

- c. vSphereで、VMオプションのチェックボックスがオフになっていることを確認し`Synchronize guest time with host`ます。



今後 VM を変更する場合は、このオプションを有効にしないでください。



時刻の同期設定が完了したらNTPを編集しないでください。管理ノードで実行するとNTPに影響するためです。[再導入コマンド](#)

管理ノードを設定

1. 管理サービスバンドルの内容を保存する一時的なデスティネーションディレクトリを作成します。

```
mkdir -p /sf/etc/mnode/mnode-archive
```

2. 既存の管理ノードにインストールされていた管理サービスバンドル（バージョン2.15.28以降）をダウンロードし、ディレクトリに保存します /sf/etc/mnode/。
3. 次のコマンドを使用して、ダウンロードしたバンドルを展開します。角かっこ内の値をバンドルファイル名に置き換えます。

```
tar -C /sf/etc/mnode -xvf /sf/etc/mnode/[management services bundle file]
```

4. 作成されたファイルをディレクトリに展開し `sf/etc/mnode-archive` ます。

```
tar -C /sf/etc/mnode/mnode-archive -xvf /sf/etc/mnode/services_deploy_bundle.tar.gz
```

5. アカウントとボリュームの構成ファイルを作成します。

```
echo '{"trident": true, "mvip": "[mvip IP address]", "account_name": "[persistent volume account name]"}' | sudo tee /sf/etc/mnode/mnode-archive/management-services-metadata.json
```

- a. 次の各必須パラメータについて、[] ブラケット（ブラケットを含む）の値を置き換えます。

- **[mvip IP address]** : ストレージクラスタの管理仮想 IP アドレス。で使用したストレージクラスタを使用して管理ノードを設定し"[NTP サーバの設定](#)"ます。
- *** [persistent volume account name] *** : このストレージクラスタ内のすべての永続ボリュームに関連付けられたアカウントの名前。

6. クラスタでホストされている永続ボリュームに接続し、以前の管理ノードの設定データを使用してサービスを開始するには、管理ノードの再導入コマンドを設定して実行します。



セキュアプロンプトにパスワードを入力するように求められます。クラスタがプロキシサーバの背後にある場合、パブリックネットワークに接続できるようにプロキシを設定する必要があります。

```
sudo /sf/packages/mnode/redeploy-mnode --mnode_admin_user [username]
```

- a. 角かっこ内の値を、管理ノードの管理者アカウントのユーザ名に置き換えます。一般には、管理ノードへのログインに使用したユーザアカウントのユーザ名です。



ユーザ名を追加するか、または情報の入力を求めるプロンプトをスクリプトに表示することができます。

- b. コマンドを実行します `redeploy-mnode`。再導入が完了すると、成功メッセージが表示されます。
- c. システムのFully Qualified Domain Name (FQDN；完全修飾ドメイン名) を使用してElementまたはNetApp HCIのWebインターフェイス（管理ノードやNetApp Hybrid Cloud Controlなど）にアクセスする場合は、を["管理ノードの認証を再設定します"](#)参照してください。



管理ノードで以前にSSH機能を無効にしていた場合は、リカバリした管理ノードでを実行する必要があります"[SSH を再度無効にします](#)"ます。のSSH機能"[ネットアップサポートの Remote Support Tunnel \(RST\) セッションアクセス](#)"は、管理ノードではデフォルトで有効になっています。

詳細はこちら

- ["永続ボリューム"](#)
- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

管理ノードにアクセスします

NetApp Element ソフトウェアバージョン 11.3 以降、管理ノードには 2 つの UI が装備されています。REST ベースのサービスを管理するための UI と、ネットワーク / クラスタ設定の管理とオペレーティングシステムのテスト / ユーティリティを実行するためのノード UI です。

Element ソフトウェアバージョン 11.3 以降を実行するクラスタでは、次の 2 つのインターフェイスのいずれかを使用できます。

- 管理ノード UI (`https:// [mNode IP]:442` を使用) を使用して、ネットワークとクラスタの設定を変更したり、システムテストを実行したり、システムユーティリティを使用したりできます。
- 組み込みの REST API UI (`https://[mNode IP]/mnode` を使用) を使用して、プロキシサーバの設定、サービスレベルの更新、資産管理など、管理ノードのサービスに関連する API を実行または把握できます。

管理ノードのノード UI にアクセスします

ノード UI からは、ネットワークとクラスタの設定にアクセスし、システムのテストとユーティリティを利用できます。

手順

1. 管理ノードのノード UI にアクセスするには、と入力します 管理ノードの IP アドレスに続けて： 442 を

追加します

```
https://[IP address]:442
```

Support and Documentation Enable Debug Info: Requests Responses Logout

NetApp

Network Settings Cluster Settings System Tests System Utilities

Management

Network Settings - Management

Method: static

Link Speed: 1000

IPv4 Address: 10.117.148.201

IPv4 Subnet Mask: 255.255.255.0

IPv4 Gateway Address: 10.117.151.254

IPv6 Address:

IPv6 Gateway Address:

MTU: 1500

DNS Servers: 10.117.20.40, 10.116.133.40

Search Domains: den.scoloffre.net, org.den.scoloffre

Status: UpAndRunning

Routes

+ Add

Reset Changes Save Changes

2. プロンプトが表示されたら、管理ノードのユーザ名とパスワードを入力します。

管理ノードの **REST API UI** にアクセスします

REST API UI からは、管理ノード上の管理サービスを制御するサービス関連 API のメニューにアクセスできます。

手順

1. 管理サービスのREST API UIにアクセスするには、管理ノードのIPアドレスに続けて次のように入力し`/mnode`ます。

https://[IP address]/mnode

MANAGEMENT SERVICES API^{1.0}

[Base URL: /mnode]
https://10.117.100.100/mnode/swagger.json

The configuration REST service for MANAGEMENT SERVICES
NetApp - Website
NetApp Commercial Software License

Authorize 

logs Log service

GET /logs Get logs from the MNODE service(s)

assets Asset service

POST /assets Add a new asset

GET /assets Get all assets

GET /assets/compute-nodes Get all compute nodes

GET /assets/compute-nodes/{compute_node_id} Get a specific compute node by ID

GET /assets/controllers Get all controllers

GET /assets/controllers/{controller_id} Get a specific controller by ID

GET /assets/storage-clusters Get all storage clusters

GET /assets/storage-clusters/{storage_cluster_id} Get a specific storage cluster by ID

PUT /assets/{asset_id} Modify an asset with a specific ID

DELETE /assets/{asset_id} Delete an asset with a specific ID

GET /assets/{asset_id} Get an asset by it's ID

POST /assets/{asset_id}/compute-nodes Add a compute asset

GET /assets/{asset_id}/compute-nodes Get compute assets

PUT /assets/{asset_id}/compute-nodes/{compute_id} Update a specific compute node asset

DELETE /assets/{asset_id}/compute-nodes/{compute_id} Delete a specific compute node asset

2. 「* Authorize *」またはロックアイコンを選択し、API を使用する権限を付与するクラスタ管理者のクレデンシャルを入力します。

詳細はこちら

- "Active IQ と NetApp HCI の監視を有効にします"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

管理ノードのデフォルト**SSL**証明書を変更します

NetApp Element APIを使用して、管理ノードのデフォルトのSSL証明書と秘密鍵を変更

できます。

管理ノードを設定すると、一意の自己署名Secure Sockets Layer (SSL) 証明書と秘密鍵が作成され、Element UI、ノードUI、またはノードAPIを使用してすべてのHTTPS通信に使用されます。Element ソフトウェアは、自己署名証明書に加え、信頼できる認証局 (CA) が発行して検証する証明書をサポートします。

次の API メソッドを使用して、デフォルトの SSL 証明書に関する詳細情報を取得し、変更を加えることができます。

- * [GetNodeSSLCertificate](#) *

を使用すると、現在インストールされている SSL 証明書に関するすべての証明書の詳細を含む情報を取得できます "[GetNodeSSLCertificateメソッド](#)"。

- * [SetNodeSSLCertificate](#) *

を使用して、クラスタおよびノード単位の SSL 証明書を指定した証明書と秘密鍵に設定できます "[SetNodeSSLCertificateメソッド](#)"。証明書と秘密鍵はシステムで検証されるため、無効な証明書が適用されることはありません。

- * [RemoveNodeSSLCertificate](#) *

これにより、"[RemoveNodeSSLCertificateメソッド](#)"現在インストールされている SSL 証明書と秘密鍵が削除されます。そのあと、クラスタで新しい自己署名証明書と秘密鍵が生成されます。

詳細情報

- "[Element ソフトウェアのデフォルトの SSL 証明書を変更](#)"
- "[Element SoftwareでのカスタムSSL証明書の設定に関する要件を教えてください。](#)"
- "[SolidFire および Element ソフトウェアのドキュメント](#)"
- "[vCenter Server 向け NetApp Element プラグイン](#)"

管理ノード UI の操作

管理ノード UI の概要

管理ノードUI(`https://<ManagementNodeIP>:442`を使用) では、ネットワークとクラスタの設定を変更したり、システムテストを実行したり、システムユーティリティを使用したりできます。

管理ノード UI で実行できるタスクは次のとおりです。

- "[NetApp HCI でアラート監視を設定する](#)"
- "[管理ノードのネットワーク、クラスタ、およびシステムの設定を変更してテストする](#)"
- "[管理ノードからシステムユーティリティを実行します](#)"

詳細情報

- "管理ノードにアクセスします"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

NetApp HCI でアラート監視を設定する



NetApp HCI システムでアラートを監視するように設定を行うことができます。

NetApp HCI のアラート監視は、NetApp HCI ストレージクラスタのシステムアラートを vCenter Server に転送して、vSphere Web Client インターフェイスで NetApp HCI のすべてのアラートを表示できるようにします。

1. ノード管理ノードUIを開き(`https://[IP address]:442`ます)。
2. [Alert Monitor]タブを選択します。
3. アラート監視オプションを設定します。

アラート監視オプション

オプション	製品説明
Alert Monitor テストを実行します	<p>モニタシステムテストを実行して次の項目を確認します。</p> <ul style="list-style-type: none"> • NetApp HCI と VMware vCenter の接続 • データストア情報を使用した NetApp HCI と VMware vCenter のペアリング QoSSIOC サービスによって提供されます • 現在の NetApp HCI アラームと vCenter アラームのリスト
アラートを収集します	<p>NetApp HCI ストレージアラームの vCenter への転送を有効または無効にします。ドロップダウンリストからターゲットのストレージクラスタを選択できます。このオプションのデフォルト設定はです Enabled。</p>
ベストプラクティスアラートを収集	<p>NetApp HCI ストレージのベストプラクティスアラートの vCenter への転送を有効または無効にします。ベストプラクティスアラートは、最適化されていないシステム構成によってトリガーされた障害です。このオプションのデフォルト設定はです Disabled。無効にすると、NetApp HCI ストレージのベストプラクティスアラートは vCenter に表示されません。</p>

オプション	製品説明
サポートデータをAIQに送信	<p>VMware vCenter から NetApp SolidFire Active IQ へのサポートデータと監視データのフローを制御します。</p> <p>オプションは次のとおりです。</p> <ul style="list-style-type: none"> • Enabled : vCenter アラーム、 NetApp HCI ストレージアラーム、 およびサポートデータがすべて NetApp SolidFire Active IQ に送信されます。これにより、 NetAppはNetApp HCIのインストールをプロアクティブにサポートおよび監視できるため、システムに影響を与える前に潜在的な問題を検出して解決できます。 • Disabled : vCenter アラーム、 NetApp HCI ストレージアラーム、 サポートデータはいずれも NetApp SolidFire Active IQ に送信されません。 <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>NetApp Deployment Engineを使用し、*[Send data to AIQ *]オプションをオフにした場合は、このページから管理ノードのREST APIを使用してサービスを設定する必要がある"テレメータを有効にします"があります。</p> </div>
コンピューティングノードのデータを AIQ に送信	<p>コンピューティングノードから NetApp SolidFire Active IQ へのサポートデータと監視データのフローを制御します。</p> <p>オプションは次のとおりです。</p> <ul style="list-style-type: none"> • Enabled : コンピューティングノードに関するサポートデータと監視データが NetApp SolidFire Active IQ に転送されるため、コンピューティングノードのハードウェアをプロアクティブにサポートできます。 • Disabled : コンピューティングノードに関するサポートデータと監視データは NetApp SolidFire Active IQ に転送されません。 <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>NetApp Deployment Engineを使用し、*[Send data to AIQ *]オプションをオフにした場合は、このページから管理ノードのREST APIを使用してサービスを設定する必要がある"テレメータを有効にします"があります。</p> </div>

詳細はこちら

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

管理ノードのネットワーク、クラスタ、およびシステムの設定を変更してテストする

管理ノードのネットワーク、クラスタ、およびシステムの設定を変更してテストすることができます。

- [\[管理ノードのネットワーク設定を更新します\]](#)
- [\[管理ノードのクラスタ設定を更新します\]](#)
- [\[管理ノードの設定をテストします\]](#)

管理ノードのネットワーク設定を更新します

ノード管理ノード UI のネットワーク設定タブで、管理ノードのネットワークインターフェイスフィールドを変更できます。

1. ノード管理ノード UI を開きます。
2. [* ネットワーク設定 *] タブを選択します。
3. 次の情報を表示または入力します。
 - a. * method * : インターフェイスを設定するには、次のいずれかの方法を選択します。
 - `loopback` : IPv4ループバックインターフェイスを定義するために使用します。
 - `manual` : デフォルトで設定されていないインターフェイスを定義する場合に使用します。
 - `dhcp` : DHCP経由でIPアドレスを取得する場合に使用します。
 - `static` : IPv4アドレスが静的に割り当てられたイーサネットインターフェイスを定義する場合に使用します。
 - b. * リンク速度 * : 仮想 NIC によってネゴシエートされた速度。
 - c. **IPv4 Address**: eth0 ネットワークの IPv4 アドレス。
 - d. **IPv4 Subnet Mask**: IPv4 ネットワークのアドレス分割。
 - e. *IPv4 ゲートウェイアドレス *: ローカルネットワークからパケットを送信するためのルータネットワークアドレス。
 - f. **IPv6 Address**: eth0 ネットワークの IPv6 アドレス。
 - g. *IPv6 ゲートウェイアドレス *: ローカルネットワークからパケットを送信するためのルータネットワークアドレス。



IPv6 オプションは、11.3 以降のバージョンの管理ノードではサポートされていません。

- h. **MTU** : ネットワークプロトコルが伝送できる最大パケットサイズ。1500 以上にする必要があります。2 つ目のストレージ NIC を追加する場合は、値を 9000 にする必要があります。
- i. **DNS Servers** : クラスタ通信に使用するネットワーク・インターフェイス。
- j. * 検索ドメイン *: システムで使用可能な追加の MAC アドレスを検索します。

k. * ステータス * : 有効な値は次のとおりです。

- UpAndRunning
- Down
- Up

l. * Routes * : ルートが使用するように設定されている、関連付けられたインターフェイスを介した特定のホストまたはネットワークへのスタティックルート。

管理ノードのクラスタ設定を更新します

管理ノードのノード UI のクラスタ設定タブで、ノードの状態が Available、Pending、PendingActive、または Active であるときにクラスタインターフェイスのフィールドを変更できます。

1. ノード管理ノード UI を開きます。
2. [クラスタ設定 *] タブを選択します。
3. 次の情報を表示または入力します。
 - * ロール * : 管理ノードがクラスタ内に設定するロール。有効な値: Management
 - * バージョン * : クラスタで実行されている Element ソフトウェアのバージョン。
 - * デフォルトインターフェイス * : Element ソフトウェアを実行しているクラスタとの管理ノード通信に使用されるデフォルトのネットワークインターフェイス。

管理ノードの設定をテストします

管理ノードの管理設定とネットワーク設定を変更して変更をコミットしたら、テストを実行して変更を検証できます。

1. ノード管理ノード UI を開きます。
2. 管理ノード UI で、* システムテスト * を選択します。
3. 次のいずれかを実行します。
 - a. 設定したネットワーク設定がシステムに対して有効であることを確認するには、* ネットワーク設定のテスト * を選択します。
 - b. 1G および 10G の両方のインターフェイスで、ICMP パケットを使用してクラスタ内のすべてのノードへのネットワーク接続をテストするには、「* ping のテスト」を選択します。
4. 次の情報を表示または入力します。
 - * Hosts * : ping を実行するデバイスのアドレスまたはホスト名をカンマで区切って指定します。
 - * attempts * : ping テストを繰り返す回数を指定します。デフォルト値は 5 です。
 - * Packet Size * : 各 IP に送信される ICMP パケットで送信するバイト数を指定します。ネットワーク設定で指定されている最大 MTU より小さい値を指定する必要があります。
 - * Timeout msec * : ping 応答ごとに待機するミリ秒数を指定します。デフォルト値は 500 ミリ秒です。
 - * Total Timeout Sec* : ping 試行の実行前またはプロセスの終了前に、ping がシステム応答を待機する時間を秒単位で指定します。デフォルト値は 5 です。
 - * フラグメンテーションの禁止 * : ICMP パケットの DF (Do not fragment) フラグを有効にします。

詳細はこちら

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

管理ノードからシステムユーティリティを実行します

管理ノードのノード UI を使用して、クラスタサポートバンドルの作成または削除、ノード設定のリセット、ネットワークの再起動を実行できます。

手順

1. 管理ノードの管理クレデンシャルを使用して、ノード管理ノード UI を開きます。
2. システムユーティリティ * を選択します。
3. 実行するユーティリティのボタンを選択します。
 - a. * Control Power * : ノードをリブート、電源再投入、またはシャットダウンします。次のいずれかのオプションを指定します。



この処理を実行すると、ネットワーク接続が一時的に失われます。

- アクション: オプションには AND Halt (電源オフ) が含まれます Restart。
 - * Wakeup Delay * : ノードがオンラインに戻るまでの時間。
- b. * クラスタサポートバンドルの作成 * : クラスタ内のノードについてネットアップサポートの診断を受けるためのクラスタサポートバンドルを作成します。次のオプションを指定します。
 - * Bundle Name * : 作成された各サポートバンドルの一意の名前。名前を指定しない場合、「supportbundle」とノード名がファイル名として使用されます。
 - * Mvip * : クラスタの MVIP。バンドルは、クラスタ内のすべてのノードから収集されます。このパラメータは、Nodes パラメータを指定しない場合のみ必要です。
 - * Nodes * : バンドルを収集するノードの IP アドレス。バンドルの収集元のノードを指定するには、Nodes または Mvip のいずれかを使用します。両方を使用することはできません。このパラメータは、Mvip を指定しない場合は必須です。
 - * Username * : クラスタ管理者ユーザ名。
 - * Password * : クラスタ管理者のパスワード。
 - * Allow Incomplete * : 1 つ以上のノードからバンドルを収集できない場合でもスクリプトが引き続き実行されます。
 - * Extra Args * : このパラメータはスクリプトに渡されます sf_make_support_bundle。このパラメータは、NetApp サポートから指示があった場合にのみ使用します。
 - c. * Delete All Support Bundles * : 管理ノードに保存されているすべてのサポートバンドルを削除します。
 - d. * ノードのリセット * : 管理ノードを新しいインストールイメージにリセットします。これにより、ネットワーク設定を除くすべての設定がデフォルトの状態に変更されます。次のオプションを指定します。
 - * Build * : ノードをリセットするリモート Element ソフトウェアイメージの URL。
 - * オプション * : リセット操作を実行するための仕様。詳細は、必要に応じて NetApp サポートから

提供されます。



この処理を実行すると、ネットワーク接続が一時的に失われます。

e. * ネットワークの再起動 * : 管理ノード上のすべてのネットワークサービスを再起動します。



この処理を実行すると、ネットワーク接続が一時的に失われます。

詳細はこちら

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

管理ノード REST API の操作

管理ノードの REST API UI の概要

組み込みの REST API UI (`https://<ManagementNodeIP>/mnode`` を使用) を使用して、プロキシサーバの設定、サービスレベルの更新、資産管理など、管理ノードのサービスに関連する API を実行または把握できます。

REST API で実行できるタスクは次のとおりです。

許可

- ["REST API を使用するための許可を取得する"](#)

アセットの設定

- ["Active IQ と NetApp HCI の監視を有効にします"](#)
- ["管理ノード用のプロキシサーバを設定します"](#)
- ["NetApp Hybrid Cloud Control を複数の vCenter に設定する"](#)
- ["管理ノードにコンピューティングアセットとコントローラアセットを追加します"](#)
- ["ストレージクラスアセットを作成および管理する"](#)

資産管理

- ["既存のコントローラアセットを表示または編集する"](#)
- ["ストレージクラスアセットを作成および管理する"](#)
- ["管理ノードからアセットを削除します"](#)
- ["REST API を使用して NetApp HCI ログを収集します"](#)
- ["管理ノードの OS とサービスのバージョンを確認"](#)
- ["管理サービスからログを取得しています"](#)

詳細情報

- "管理ノードにアクセスします"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

REST API を使用するための許可を取得する

REST API UI で管理サービス用の API を使用するには、事前に承認が必要です。アクセストークンを取得します。

トークンを取得するには、クラスタ管理者のクレデンシャルとクライアント ID を指定します。各トークンの有効期間は約 10 分です。トークンの期限が切れたら、再度承認して新しいアクセストークンを取得できません。

許可機能は管理ノードのインストールおよび導入時に設定します。トークンサービスは、セットアップ時に定義したストレージクラスタに基づいています。

必要なもの

- クラスタで NetApp Element ソフトウェア 11.3 以降を実行している必要があります。
- バージョン 11.3 以降を実行する管理ノードを導入しておく必要があります。

API コマンド

```
TOKEN=`curl -k -X POST https://MVIP/auth/connect/token -F client_id=mnode-client -F grant_type=password -F username=CLUSTER_ADMIN -F password=CLUSTER_PASSWORD|awk -F': ' '{print $2}'|awk -F',' '{print $1}'|sed s/\"//g`
```

REST API の UI の手順

1. 管理ノードの IP アドレスとサービス名を入力して、サービスの REST API UI にアクセスします。次に例を示します。 /mnode/

```
https://<ManagementNodeIP>/mnode/
```

2. 「* Authorize * (認証)」を選択



または、任意のサービス API の横にあるロックアイコンを選択することもできます。

3. 次の手順を実行します。
 - a. クラスタのユーザ名とパスワードを入力します。
 - b. クライアント ID にと入力し `mnode-client` ます。
 - c. クライアントシークレットの値は入力しないでください。
 - d. セッションを開始するには、* Authorize * を選択します。
4. **[Available Authorizations (使用可能な承認)]** ダイアログボックスを閉じます。



トークンの有効期限が切れたあとにコマンドを実行しようとするすると 401 Error: UNAUTHORIZED、メッセージが表示されます。このメッセージが表示された場合は、再度承認してください。

詳細情報

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

Active IQ と NetApp HCI の監視を有効にします

インストールまたはアップグレード時にActive IQ ストレージの監視を有効にしていない場合、NetApp HCI とNetApp HCI のコンピューティング監視を有効にすることができます。NetApp HCI Deployment Engineを使用してテレメトリを無効にした場合、この手順の使用が必要になることがあります。

Active IQ コレクタサービスは、履歴データのレポートおよびほぼリアルタイムのパフォーマンス監視用に、設定データと Element ソフトウェアベースのクラスタパフォーマンス指標を NetApp Active IQ に転送します。NetApp HCI 監視サービスを使用すると、ストレージクラスタのエラーを vCenter に転送してアラート通知を送信できます。

必要なもの

- ストレージクラスタで NetApp Element ソフトウェア 11.3 以降が実行されている必要があります。
- バージョン 11.3 以降を実行する管理ノードを導入しておきます。
- インターネットにアクセスできる。Active IQ コレクタサービスをダークサイトから使用することはできません。

手順

1. インストールのベースアセット ID を取得します。
 - a. 管理ノードでインベントリサービス REST API UI を開きます。

```
https://<ManagementNodeIP>/inventory/1/
```

- b. 「* Authorize *」（認証）を選択して、次の手順を実行
 - i. クラスタのユーザ名とパスワードを入力します。
 - ii. クライアントIDにと入力し `mnode-client` ます。
 - iii. セッションを開始するには、* Authorize * を選択します。
 - iv. ウィンドウを閉じます。
- c. REST API UI で、* 一部のユーザに一時的な処理を開始 / インストール * を選択します。
- d. [* 試してみてください *] を選択します。
- e. [* Execute] を選択します。
- f. コード200応答本文から、インストール用のをコピーします id。


```
{
  "installations": [
    {
      "_links": {
        "collection":
"https://10.111.211.111/inventory/1/installations",
        "self":
"https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-
91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
    }
  ]
}
```



インストール環境には、インストールまたはアップグレード時に作成されたベースアセットの構成が含まれています。

2. テレメータの有効化：

- a. 管理ノードのIPアドレスに続けて次のように入力し、管理ノードのmnodeサービスAPI UIにアクセスし `mnode` ます。

```
https://<ManagementNodeIP>/mnode
```

- b. 「* Authorize * (認証)」または任意のロックアイコンを選択し、次の手順を実行します。
 - i. クラスタのユーザ名とパスワードを入力します。
 - ii. クライアントIDにと入力し `mnode-client` ます。
 - iii. セッションを開始するには、* Authorize * を選択します。
 - iv. ウィンドウを閉じます。
- c. ベースアセットを設定します。
 - i. PUT /assets/ { asset_id } * を選択します。
 - ii. [* 試してみてください *] を選択します。
 - iii. JSON ペイロードに次のコマンドを入力します。

```
{
  "telemetry_active": true
  "config": {}
}
```

- iv. 前の手順のベース ID を * asset_ID * に入力します。
- v. [* Execute] を選択します。

Active IQ サービスは、アセットが変更されるたびに自動的に再起動されます。アセットを変更す

ると、設定が適用されるまで短時間の遅延が発生します。

3. 管理ノードの既知のアセットに、NetApp HCI 監視用の vCenter コントローラアセット（NetApp HCI インストールのみ）と Hybrid Cloud Control 用の vCenter コントローラアセット（すべてのインストール環境）を追加しておきます。



NetApp HCI 監視サービスにはコントローラアセットが必要です。

- a. コントローラサブアセットを追加する場合は、「* POST /assets/ { asset_id } /controllers *」を選択します。
- b. [* 試してみてください *] を選択します。
- c. クリップボードにコピーした親ベースアセットの ID を * asset_id * フィールドに入力します。
- d. 必要なペイロード値を AS `vCenter` および vCenter クレデンシャルとともに入力し `type` ます。

```
{
  "username": "string",
  "password": "string",
  "ip": "string",
  "type": "vCenter",
  "host_name": "string",
  "config": {}
}
```



`ip` は vCenter の IP アドレスです。

- e. [* Execute] を選択します。

詳細情報

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

NetApp Hybrid Cloud Control を複数の vCenter に設定する

リンクモードを使用していない 2 つ以上の vCenter からアセットを管理するように NetApp Hybrid Cloud Control を設定できます。

この手順は、最初のインストール後に、最近拡張した環境のアセットを追加する必要がある場合や、新しいアセットが構成に自動的に追加されない場合に使用してください。これらの API を使用して、最近追加されたアセットを環境に追加します。

必要なもの

- クラスタバージョンで NetApp Element ソフトウェア 11.3 以降が実行されています。
- バージョン 11.3 以降を実行する管理ノードを導入しておきます。

手順

1. "新しい vCenter をコントローラアセットとして追加する"を管理ノードの設定に追加します。
2. "コンピューティングアセットとして新しいコンピューティングノードを追加します"を管理ノードの設定に追加します。



NetAppハイブリッドクラウドコントロールに表示されるまたは`Unable to Detect`エラーの解決`Hardware ID not available`が必要になる場合があります"コンピューティングノードの BMC クレデンシャルを変更します"ます。

3. 管理ノードでインベントリサービス API をリフレッシュします。

```
https://<ManagementNodeIP>/inventory/1/
```



また、 NetApp Hybrid Cloud Control の UI でインベントリが更新されるまで 15 分待つこともできます。

- a. 「* Authorize *」 (認証) を選択して、次の手順を実行
 - i. クラスタのユーザ名とパスワードを入力します。
 - ii. クライアントIDにと入力し`mnode-client`ます。
 - iii. セッションを開始するには、* Authorize * を選択します。
 - iv. ウィンドウを閉じます。
 - b. REST API UI で、* 一部のユーザに一時的な処理を開始 / インストール * を選択します。
 - c. [* 試してみてください *] を選択します。
 - d. [* Execute] を選択します。
 - e. 応答から、インストールアセットID("id"をコピーします)。
 - f. REST API UI から、* GET / Installations / { id } * を選択します。
 - g. [* 試してみてください *] を選択します。
 - h. リフレッシュをに設定します True。
 - i. インストールアセット ID を **id** フィールドに貼り付けます。
 - j. [* Execute] を選択します。
4. NetApp Hybrid Cloud Control のブラウザをリフレッシュして変更を確認します。

詳細情報

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

管理ノードにコンピューティングアセットとコントローラアセットを追加します

REST API UI を使用して、管理ノードの構成にコンピューティングアセットとコントローラアセットを追加できます。

アセットの追加は、環境を拡張したあとに、新しいアセットが構成に自動的に追加されなかった場合などに必要になります。これらの API を使用して、最近追加されたアセットを環境に追加します。

必要なもの

- クラスタバージョンで NetApp Element ソフトウェア 11.3 以降が実行されています。
- バージョン 11.3 以降を実行する管理ノードを導入しておきます。
- "vCenter で新しい NetApp HCC ロールを作成しました"管理ノードのサービスの表示をNetAppのみのアセットに制限する必要があります。
- vCenter の管理 IP アドレスとクレデンシャルが必要です。
- コンピューティングノード（ESXi）の管理 IP アドレスとルートクレデンシャルが必要です。
- ハードウェア（BMC）の管理 IP アドレスと管理者のクレデンシャルが必要です。

タスクの内容

（NetApp HCIのみ）NetApp HCIシステムの拡張後にHybrid Cloud Control（HCC）にコンピューティングノードが表示されない場合は、この手順のを使用してコンピューティングノードを追加できます POST /assets/{asset_id}/compute-nodes。

手順

1. インストールのベースアセット ID を取得します。
 - a. 管理ノードでインベントリサービス REST API UI を開きます。

```
https://<ManagementNodeIP>/inventory/1/
```

- b. 「* Authorize *」（認証）を選択して、次の手順を実行
 - i. クラスタのユーザ名とパスワードを入力します。
 - ii. クライアントIDにと入力し `mnode-client` ます。
 - iii. セッションを開始するには、* Authorize * を選択します。
 - iv. ウィンドウを閉じます。
- c. REST API UI で、* 一部のユーザに一時的な処理を開始 / インストール * を選択します。
- d. [* 試してみてください *] を選択します。
- e. [* Execute] を選択します。
- f. コード200応答本文から、インストール用のをコピーします id。

```
{
  "installations": [
    {
      "_links": {
        "collection":
"https://10.111.211.111/inventory/1/installations",
        "self":
"https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-
91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
    }
  ]
}
```



インストール環境には、インストールまたはアップグレード時に作成されたベースアセットの構成が含まれています。

- g. REST API UI から、* GET / Installations / {id} * を選択します。
 - h. [* 試してみてください *] を選択します。
 - i. インストールアセット ID を **id** フィールドに貼り付けます。
 - j. [* Execute] を選択します。
 - k. 応答から、クラスタコントローラIDをコピーして保存し("controllerId"、あとの手順で使用します。
2. (コンピューティングノードの場合のみ) [コンピューティングノードのハードウェアタグを確認します](#) をvSphereで使用します。
 3. コントローラアセット (vCenter) 、コンピューティングノード (ESXi) 、またはハードウェア (BMC) を既存のベースアセットに追加するには、次のいずれかを選択します。

オプション	製品説明
POST / assets / { asset_id } / コントローラ	<p>a. 管理ノードで mNode サービス REST API UI を開きます。</p> <div data-bbox="760 254 1487 352" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; text-align: center;"> <p>https://<ManagementNodeIP>/mnode</p> </div> <p>i. 「 * Authorize * 」 (認証) を選択して、次の手順を実行</p> <ul style="list-style-type: none"> A. クラスタのユーザ名とパスワードを入力します。 B. クライアントIDにと入力し `mnode-client` ます。 C. セッションを開始するには、 * Authorize * を選択します。 D. ウィンドウを閉じます。 <p>b. 「 * POST / assets / { asset_id } / controllers * 」 を選択します。</p> <p>c. [* 試してみてください *] を選択します。</p> <p>d. 親ベースアセット ID を 「 * asset_id * 」 フィールドに入力します。</p> <p>e. 必要な値をペイロードに追加します。</p> <p>f. [* Execute] を選択します。</p>

オプション	製品説明
POST /assets/ { asset_id } / compute-nodes	<p>a. 管理ノードで mNode サービス REST API UI を開きます。</p> <div data-bbox="760 254 1485 352" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <pre>https://<ManagementNodeIP>/mnode</pre> </div> <p>i. 「* Authorize *」（認証）を選択して、次の手順を実行</p> <ul style="list-style-type: none"> A. クラスタのユーザ名とパスワードを入力します。 B. クライアントIDに入力し `mnode-client` ます。 C. セッションを開始するには、* Authorize * を選択します。 D. ウィンドウを閉じます。 <p>b. 「* POST /assets/ { asset_id } /compute-nodes 」を選択します。</p> <p>c. [* 試してみてください *] を選択します。</p> <p>d. 前の手順でコピーした親ベースアセットの ID を 「* asset_id *」 フィールドに入力します。</p> <p>e. ペイロードで、次の手順を実行します。</p> <ul style="list-style-type: none"> i. フィールドにノードの管理IPを入力し `ip` ます。 ii. には hardwareTag、前の手順で保存したハードウェアタグの値を入力します。 iii. 必要に応じて、他の値を入力します。 <p>f. [* Execute] を選択します。</p>

オプション	製品説明
POST /assets/ { asset_id } /ハードウェアノード	<p>a. 管理ノードで mNode サービス REST API UI を開きます。</p> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0; background-color: #f9f9f9;"> <p>https://<ManagementNodeIP>/mnode</p> </div> <p>i. 「* Authorize *」（認証）を選択して、次の手順を実行</p> <ol style="list-style-type: none"> A. クラスタのユーザ名とパスワードを入力します。 B. クライアントIDにと入力し `mnode-client` ます。 C. セッションを開始するには、* Authorize * を選択します。 D. ウィンドウを閉じます。 <p>b. 「* POST /assets/ { asset_id } /hardware-nodes 」を選択します。</p> <p>c. [* 試してみてください *] を選択します。</p> <p>d. 親ベースアセット ID を 「* asset_id *」 フィールドに入力します。</p> <p>e. 必要な値をペイロードに追加します。</p> <p>f. [* Execute] を選択します。</p>

詳細情報

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

コンピューティングノードのハードウェアタグを確認する方法

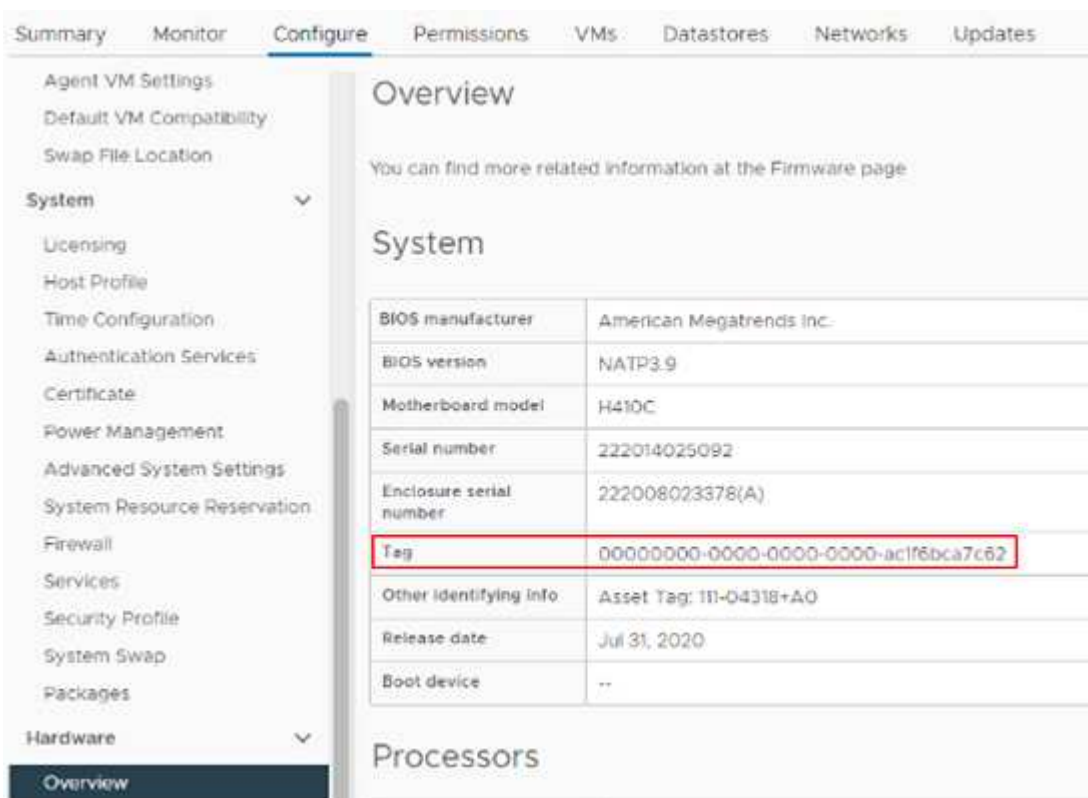
REST API UI を使用してコンピューティングノードアセットを管理ノードの構成に追加するには、ハードウェアタグが必要です。

VMware vSphere 7.0

VMware vSphere Web Client 7.0で、コンピューティングノードのハードウェアタグを探します。

手順

1. vSphere Web Client ナビゲータでホストを選択します。
2. [* 構成 * (Configure *)] タブを選択します。
3. サイドバーから、* Hardware > Overview *を選択します。ハードウェアタグが表に記載されているかどうかを確認します System。



The screenshot shows the VMware vSphere Web Client interface. The 'Configure' tab is selected, and the 'System' section is expanded. The 'Overview' page displays system information in a table. The 'Tag' field is highlighted with a red box.

Property	Value
BIOS manufacturer	American Megatrends Inc.
BIOS version	NATP3.9
Motherboard model	H410C
Serial number	222014025092
Enclosure serial number	222008023378(A)
Tag	00000000-0000-0000-0000-ac1f6bca7c62
Other identifying info	Asset Tag: 111-04318+A0
Release date	Jul 31, 2020
Boot device	--

4. *Tag*の値をコピーして保存します。
5. コンピューティングアセットとコントローラアセットを管理ノードに追加します。

VMware vSphere 6.7および6.5

VMware vSphere Web Client 6.7および6.5で、コンピューティングノードのハードウェアタグを確認します。

手順

1. vSphere Web Client ナビゲータでホストを選択します。
2. [Monitor] タブを選択し、[Hardware Health] を選択します。
3. タグが BIOS の製造元とモデル番号で表示されているかどうかを確認します。

The screenshot shows the 'Hardware Health' page. On the left is a navigation menu with categories like 'Issues and Alarms', 'Performance', 'Tasks and Events', and 'Hardware Health'. The main content area displays BIOS details: 'BIOS Manufacturer: , BIOS Version: NA2.1', 'Model: H700E, Serial Number: 000172000247', and 'Tag: 00000000-0000-0000-0000-0cc47ad47cac'. Below this are tabs for 'SENSORS', 'ALERTS AND WARNINGS', and 'SYSTEM EVENT LOG'. A table of sensors is visible at the bottom, with columns for ID, Sensors, Status, Reading, and SI. The first row shows '0.29.1.65', 'Fan Device 1 FAN1', 'Normal', '10300 RPM', and 'C'.

- *Tag*の値をコピーして保存します。
- コンピューティングアセットとコントローラアセットを管理ノードに追加します。

ストレージクラスタアセットを作成および管理する

新しいストレージクラスタアセットを管理ノードに追加したり、既知のストレージクラスタアセット用に格納されているクレデンシャルを編集したり、REST API を使用して管理ノードからストレージクラスタアセットを削除したりできます。

必要なもの

- ストレージクラスタで NetApp Element ソフトウェア 11.3 以降を実行していることを確認します。
- バージョン 11.3 以降を実行する管理ノードを導入しておきます。

ストレージクラスタのアセット管理オプション

次のいずれかのオプションを選択します。

- [ストレージのインストール ID とクラスタ ID を取得します クラスタアセット](#)
- [\[新しいストレージクラスタアセットを追加します\]](#)
- [\[ストレージクラスタアセットに保存されているクレデンシャルを編集します\]](#)
- [\[ストレージクラスタアセットを削除します\]](#)

ストレージのインストール ID とクラスタ ID を取得します クラスタアセット

REST API のインストール ID およびストレージクラスタの ID を取得できます。インストール ID は、新しいストレージクラスタアセットを追加する場合に必要になります。クラスタ ID は、特定のストレージクラスタアセットを変更または削除する場合に必要になります。

手順

1. 管理ノードのIPアドレスに続けて次のように入力し、インベントリサービスのREST API UIにアクセスし `/inventory/1/` ます。

```
https://<ManagementNodeIP>/inventory/1/
```

2. 「* Authorize *（認証）」または任意のロックアイコンを選択し、次の手順を実行します。
 - a. クラスタのユーザ名とパスワードを入力します。
 - b. クライアントIDにと入力し `mnode-client` ます。
 - c. セッションを開始するには、* Authorize * を選択します。
 - d. ウィンドウを閉じます。
3. [*Get/Installations] を選択します。
4. [* 試してみてください *] を選択します。
5. [* Execute] を選択します。

API は、既知のすべてのインストールのリストを返します。

6. コード200応答本文から、インストールのリストにあるフィールドに値を保存します id。これはインストール ID です。例：

```
"installations": [  
  {  
    "id": "1234a678-12ab-35dc-7b4a-1234a5b6a7ba",  
    "name": "my-hci-installation",  
    "_links": {  
      "collection": "https://localhost/inventory/1/installations",  
      "self": "https://localhost/inventory/1/installations/1234a678-  
12ab-35dc-7b4a-1234a5b6a7ba"  
    }  
  }  
]
```

7. 管理ノードのIPアドレスに続けて次のように入力して、ストレージサービスのREST API UIにアクセスし `/storage/1/` ます。

```
https://<ManagementNodeIP>/storage/1/
```

8. 「* Authorize *（認証）」または任意のロックアイコンを選択し、次の手順を実行します。
 - a. クラスタのユーザ名とパスワードを入力します。
 - b. クライアントIDにと入力し `mnode-client` ます。
 - c. セッションを開始するには、* Authorize * を選択します。
 - d. ウィンドウを閉じます。
9. 「* get/clusters *」を選択します。

10. [* 試してみてください *] を選択します。
11. 前の手順で保存したインストールIDをパラメータに入力し `installationId` ます。
12. [* Execute] を選択します。

API は、このインストール環境内のすべての既知のストレージクラスタのリストを返します。

13. コード200の応答本文で、正しいストレージクラスタを探し、その値をクラスタのフィールドに保存します storageId。これはストレージクラスタの ID です。

新しいストレージクラスタアセットを追加します

REST API を使用して、管理ノードインベントリに新しいストレージクラスタアセットを追加できます。新しいストレージクラスタアセットを追加すると、そのアセットが管理ノードに自動的に登録されます。

必要なもの

- 追加するストレージクラスタのをコピーしておき [ストレージクラスタ ID とインストール ID](#) ます。
- 複数のストレージノードを追加する場合は、および複数のストレージクラスタのサポートの制限事項を確認し、理解しておく ["権限のあるクラスタです"](#) 必要があります。



信頼できるクラスタで定義されたすべてのユーザが、Hybrid Cloud Control インスタンスに関連付けられている他のすべてのクラスタのユーザとして定義されています。

手順

1. 管理ノードのIPアドレスに続けて次のように入力して、ストレージサービスのREST API UIにアクセスし `/storage/1/` ます。

```
https://<ManagementNodeIP>/storage/1/
```

2. 「* Authorize * (認証)」または任意のロックアイコンを選択し、次の手順を実行します。
 - a. クラスタのユーザ名とパスワードを入力します。
 - b. クライアントIDにと入力し `mnode-client` ます。
 - c. セッションを開始するには、* Authorize * を選択します。
 - d. ウィンドウを閉じます。
3. [* POST/clusters] を選択します。
4. [* 試してみてください *] を選択します。
5. 「Request body」フィールドに、次のパラメータで新しいストレージクラスタの情報を入力します。

```
{
  "installationId": "a1b2c34d-e56f-1a2b-c123-1ab2cd345d6e",
  "mvip": "10.0.0.1",
  "password": "admin",
  "userId": "admin"
}
```

パラメータ	タイプ	製品説明
installationId	文字列	新しいストレージクラスタを追加するインストール。以前に保存したインストール ID をこのパラメータに入力します。
mvip	文字列	ストレージクラスタの IPv4 管理仮想 IP アドレス (MVIP)。
password	文字列	ストレージクラスタとの通信に使用するパスワード。
userId	文字列	ストレージクラスタとの通信に使用するユーザ ID (ユーザには管理者権限が必要)。

6. [* Execute] を選択します。

API は、新しく追加したストレージクラスタアセットの名前、バージョン、IP アドレスなどの情報を含むオブジェクトを返します。

ストレージクラスタアセットに保存されているクレデンシャルを編集します

管理ノードがストレージクラスタへのログインに使用する、保存されているクレデンシャルを編集できます。選択するユーザにはクラスタ管理者アクセスが必要です。



続行する前に、の手順を実行していることを確認して [ストレージのインストール ID とクラスタ ID を取得します クラスタアセット](#) ください。

手順

1. 管理ノードのIPアドレスに続けて次のように入力して、ストレージサービスのREST API UIにアクセスし `storage/1/` ます。

```
https://<ManagementNodeIP>/storage/1/
```

2. 「* Authorize * (認証)」または任意のロックアイコンを選択し、次の手順を実行します。

- クラスタのユーザ名とパスワードを入力します。
- クライアントIDにと入力し `mnode-client` ます。
- セッションを開始するには、* Authorize * を選択します。

- d. ウィンドウを閉じます。
3. PUT /clusters/ { storageld } * を選択します。
4. [* 試してみてください *] を選択します。
5. 前の手順でコピーしたストレージクラスIDをパラメータに貼り付け `storageld` ます。
6. [Request body] フィールドで、次のパラメータの一方または両方を変更します。

```
{
  "password": "adminadmin",
  "userId": "admin"
}
```

パラメータ	タイプ	製品説明
password	文字列	ストレージクラスタとの通信に使用するパスワード。
userId	文字列	ストレージクラスタとの通信に使用するユーザ ID (ユーザには管理者権限が必要)。

7. [* Execute] を選択します。

ストレージクラスタアセットを削除します

ストレージクラスタが使用停止になっている場合は、ストレージクラスタアセットを削除できます。ストレージクラスタのアセットを削除すると、管理ノードから自動的に登録解除されます。



続行する前に、この手順を実行していることを確認して [ストレージのインストール ID とクラスタ ID を取得します](#) クラスタアセットください。

手順

1. 管理ノードのIPアドレスに続けて次のように入力して、ストレージサービスのREST API UIにアクセスし `storage/1/` ます。

```
https://<ManagementNodeIP>/storage/1/
```

2. 「* Authorize * (認証)」または任意のロックアイコンを選択し、次の手順を実行します。
 - a. クラスタのユーザ名とパスワードを入力します。
 - b. クライアントIDにと入力し `mnode-client` ます。
 - c. セッションを開始するには、* Authorize * を選択します。
 - d. ウィンドウを閉じます。
3. DELETE /clusters/ { storageld } * を選択します。
4. [* 試してみてください *] を選択します。

5. 前の手順でパラメータでコピーしたストレージクラスタIDを入力し `storageId` ます。

6. [* Execute] を選択します。

成功すると、API は空の応答を返します。

詳細情報

- ["権限のあるクラスタです"](#)
- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

既存のコントローラアセットを表示または編集する

REST API を使用して、管理ノード構成内の既存の VMware vCenter コントローラに関する情報を表示および編集することができます。コントローラは、NetApp HCI 環境の管理ノードに登録されている VMware vCenter インスタンスです。

必要なもの

- クラスタで NetApp Element ソフトウェア 11.3 以降を実行していることを確認します。
- バージョン 11.3 以降を実行する管理ノードを導入しておきます。

管理サービス REST API にアクセスします

手順

1. 管理ノードのIPアドレスに続けて次のように入力し、管理サービスのREST API UIにアクセスし `/vcenter/1/` ます。

```
https://<ManagementNodeIP>/vcenter/1/
```

2. 「* Authorize * (認証)」または任意のロックアイコンを選択し、次の手順を実行します。
- a. クラスタのユーザ名とパスワードを入力します。
 - b. クライアントIDにと入力し `mnode-client` ます。
 - c. セッションを開始するには、* Authorize * を選択します。
 - d. ウィンドウを閉じます。

既存のコントローラについて格納されている情報を表示する

管理ノードに登録されている既存の vCenter コントローラをリストし、REST API を使用してそれらのコントローラに関する格納されている情報を表示できます。

手順

1. GET / compute / controllers * を選択します。
2. [* 試してみてください *] を選択します。

3. [* Execute] を選択します。

API は、各コントローラとの通信に使用される IP アドレス、コントローラ ID、ホスト名、およびユーザー ID とともに、認識されているすべての vCenter コントローラのリストを返します。

4. 特定のコントローラの接続ステータスが必要な場合は、そのコントローラのフィールドからクリップボードにコントローラIDをコピーし id、を参照してください。[既存のコントローラのステータスを表示します]

既存のコントローラのステータスを表示します

管理ノードに登録されている既存の vCenter コントローラのステータスを確認できます。この API は、NetApp Hybrid Cloud Control が vCenter コントローラに接続できるかどうか、およびそのステータスの理由を示すステータスを返します。

手順

1. GET / compute / controllers / { controller_id } / status * を選択します。
2. [* 試してみてください *] を選択します。
3. 前の手順でパラメータにコピーしたコントローラIDを入力し `controller_id` ます。
4. [* Execute] を選択します。

API は、この vCenter コントローラのステータスとそのステータスの理由を返します。

コントローラの保存されているプロパティを編集します

管理ノードに登録されている既存のすべての vCenter コントローラについて、格納されているユーザ名とパスワードを編集することができます。既存の vCenter コントローラに格納されている IP アドレスは編集できません。

手順

1. PUT / compute / controllers / { controller_id } * を選択します。
2. vCenter コントローラのコントローラIDをパラメータに入力し `controller_id` ます。
3. [* 試してみてください *] を選択します。
4. [Request body] フィールドで次のいずれかのパラメータを変更します。

パラメータ	タイプ	製品説明
userId	文字列	vCenter コントローラとの通信に使用するユーザ ID を変更します (ユーザには管理者権限が必要です)。
password	文字列	vCenter コントローラとの通信に使用するパスワードを変更します。

5. [* Execute] を選択します。

API から更新されたコントローラ情報が返されます。

詳細情報

- ["管理ノードにアセットを追加します"](#)
- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

管理ノードからアセットを削除します

コンピューティングノードを物理的に交換した場合や NetApp HCI クラスタから削除する必要がある場合は、管理ノード API を使用してコンピューティングノードのアセットを削除する必要があります。

必要なもの

- ストレージクラスタで NetApp Element ソフトウェア 11.3 以降が実行されている必要があります。
- バージョン 11.3 以降を実行する管理ノードを導入しておきます。

手順

1. 管理ノードのIPアドレスに続けて次のように入力し `mnode/1/` ます。

```
https://<ManagementNodeIP>/mnode/1/
```

2. 「* Authorize *」またはロックアイコンを選択し、API を使用する権限を付与するクラスタ管理者のクレデンシャルを入力します。
 - a. クラスタのユーザ名とパスワードを入力します。
 - b. 値が選択されていない場合は、タイプドロップダウンリストから * リクエスト本文 * を選択します。
 - c. クライアントIDは、値がまだ入力されていない場合と同様に入力し `mnode-client` ます。
 - d. クライアントシークレットの値は入力しないでください。
 - e. セッションを開始するには、* Authorize * を選択します。
 - f. ウィンドウを閉じます。
3. **[Available Authorizations (使用可能な承認)]** ダイアログボックスを閉じます。
4. **[*Get/assets]** を選択します。
5. **[* 試してみてください *]** を選択します。
6. **[* Execute]** を選択します。
7. 応答の本文を下にスクロールして**[*Compute]***セクションに移動し、障害が発生したコンピューティングノードの値との `id`` 値をコピーします `parent`。
8. **削除 / アセット / { asset_id } / コンピュートノード / { compute_id } *** を選択します。
9. **[* 試してみてください *]** を選択します。
10. 前の手順でコピーした値と `id` 値を入力し `parent` ます。
11. **[* Execute]** を選択します。

プロキシサーバを設定します

クラスタがプロキシサーバの背後にある場合、パブリックネットワークに接続できるようにプロキシを設定する必要があります。

プロキシサーバは、テレメトリコレクタとリバーストンネル接続に使用されます。インストールまたはアップグレード時にプロキシサーバを設定しなかった場合は、REST API UI を使用してプロキシサーバを有効にして設定することができます。既存のプロキシサーバ設定を変更したり、プロキシサーバを無効にしたりすることもできます。

プロキシサーバの更新を設定するコマンド。管理ノードの現在のプロキシ設定を返します。プロキシ設定は、Active IQ、NetApp Deployment Engine によって導入される NetApp HCI 監視サービス、およびネットアップサポート用のリバースサポートトンネルなど、管理ノードにインストールされるその他の Element ソフトウェアユーティリティで使用されます。

必要なもの

- 設定するプロキシサーバのホストとクレデンシャルの情報を確認しておく必要があります。
- クラスタで NetApp Element ソフトウェア 11.3 以降を実行していることを確認します。
- バージョン 11.3 以降を実行する管理ノードを導入しておきます。
- (管理ノード 12.0 および 12.2) プロキシサーバを設定する前に、NetApp Hybrid Cloud Control を管理サービスバージョン 2.16 に更新しました。

手順

1. 管理ノードのIPアドレスに続けて次のように入力し、管理ノードのREST API UIにアクセスし `mnode` ます。

```
https://<ManagementNodeIP>/mnode
```

2. 「* Authorize * (認証)」または任意のロックアイコンを選択し、次の手順を実行します。
 - a. クラスタのユーザ名とパスワードを入力します。
 - b. クライアントIDに入力し `mnode-client` ます。
 - c. セッションを開始するには、* Authorize * を選択します。
 - d. ウィンドウを閉じます。
3. 「* PUT / SETTINGS *」を選択します。
4. 「[* 試してみてください *]」を選択します。
5. プロキシサーバを有効にするには、をtrueに設定する必要があります use_proxy。IP またはホスト名とプロキシポートの宛先を入力します。

プロキシユーザ名、プロキシパスワード、および SSH ポートはオプションです。使用しない場合は省略してください。

```
{
  "proxy_ip_or_hostname": "[IP or name]",
  "use_proxy": [true/false],
  "proxy_username": "[username]",
  "proxy_password": "[password]",
  "proxy_port": [port value],
  "proxy_ssh_port": [port value: default is 443]
}
```

6. [* Execute] を選択します。



環境によっては、管理ノードのリポートが必要になることがあります。

詳細情報

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

管理ノードの **OS** とサービスのバージョンを確認

管理ノードで REST API を使用して、管理ノードの OS、管理サービスバンドル、および個々のサービスのバージョン番号を確認できます。

必要なもの

- クラスタで NetApp Element ソフトウェア 11.3 以降が実行されている必要があります。
- バージョン 11.3 以降を実行する管理ノードを導入しておきます。

オプション

- [API コマンド](#)
- [REST API の UI の手順](#)

API コマンド

- 管理ノードで実行されている管理ノードの OS、管理サービスバンドル、および管理ノードの API (mnode-API) サービスに関するバージョン情報を取得します。

```
curl -X GET "https://<ManagementNodeIP>/mnode/about" -H "accept: application/json"
```

- 管理ノードで実行されている個々のサービスに関するバージョン情報を取得します。

```
curl -X GET "https://<ManagementNodeIP>/mnode/services?status=running" -H "accept: */*" -H "Authorization: Bearer ${TOKEN}"
```



APIコマンドで使用されるベアラを見つけることができます。`\${TOKEN}`"許可する"。ベアラ`\${TOKEN}`はコール応答にあります。

REST API の UI の手順

1. 管理ノードのIPアドレスに続けて次のように入力して、サービスのREST API UIにアクセスし`/mnode/`ます。

```
https://<ManagementNodeIP>/mnode/
```

2. 次のいずれかを実行します。

- 管理ノードで実行されている管理ノードの OS、管理サービスバンドル、および管理ノードの API（mnode-API）サービスに関するバージョン情報を取得します。

- i. **[Get/About]** を選択します。
- ii. **[* 試してみてください *]** を選択します。
- iii. **[* Execute]** を選択します。

("version" 応答の本文には、("mnode_bundle_version" 管理サービスバンドルのバージョン)、 ("os_version" 管理ノードの OSバージョン、 管理ノードの APIバージョン) が表示されます。

- 管理ノードで実行されている個々のサービスに関するバージョン情報を取得します。

- i. **[get/services]** を選択します。
- ii. **[* 試してみてください *]** を選択します。
- iii. ステータスを「* Running *」と選択します。
- iv. **[* Execute]** を選択します。

管理ノードで実行されているサービスは応答の本文に示されます。

詳細情報

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

管理サービスからログを取得しています

REST API を使用して、管理ノードで実行されているサービスからログを取得できます。すべてのパブリックサービスからログを取得したり、特定のサービスを指定したりできます。また、クエリパラメータを使用して、取得する内容を細かく絞り込むこともできます。

必要なもの

- クラスタバージョンで NetApp Element ソフトウェア 11.3 以降が実行されています。
- バージョン 11.3 以降を実行する管理ノードを導入しておきます。

手順

1. 管理ノードでREST API UIを開きます。
 - 管理サービス2.2.1.61以降では、次の処理を実行します。

```
https://<ManagementNodeIP>/mnode/4/
```

- 管理サービス2.20.69以前の場合：

```
https://<ManagementNodeIP>/mnode
```

2. 「* Authorize * (認証)」または任意のロックアイコンを選択し、次の手順を実行します。
 - a. クラスタのユーザ名とパスワードを入力します。
 - b. mnode-client の値がまだ入力されていない場合は、クライアント ID を入力します。
 - c. セッションを開始するには、* Authorize * を選択します。
 - d. ウィンドウを閉じます。
3. 「* get/logs *」を選択します。
4. 「* 試してみてください *」を選択します。
5. 次のパラメータを指定します。
 - Lines:ログが返す行数を入力します。このパラメータは整数で、デフォルトは 1000 です。



Lines を 0 に設定して、ログコンテンツの履歴全体を要求しないでください。

- since:サービスログの開始ポイントにISO-8601タイムスタンプを追加します。



より長い期間のログを収集する場合は、適切なパラメータを使用して `since` ください。

- service-name : サービス名を入力します。



コマンドを使用し `GET /services` で、管理ノード上のサービスを一覧表示します。

- stopped : 停止したサービスからログを取得するには、をに設定します true。

6. 「* Execute」を選択します。
7. 応答の本文から「* Download *」を選択して、ログ出力を保存します。

詳細はこちら

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

サポート接続を管理します

リモートのネットアップサポートセッションを開始します

NetApp HCI システムのテクニカルサポートが必要な場合は、ネットアップサポートがお客様のシステムにリモートで接続できます。セッションを開始してリモートアクセスを確立するために、ネットアップサポートはお客様の環境へのリバース Secure Shell (SSH) 接続を確立します。

タスクの内容

NetAppサポートとのSSHリバーストンネル接続用のTCPポートを開くことができます。この接続を介して、ネットアップサポートはお客様の管理ノードにログインします。管理ノードがプロキシサーバの背後にある場合は、次の TCP ポートを sshd.config ファイルで設定しておく必要があります。

TCP ポート	製品説明	接続方向
443	オープンサポートトンネルを介したリバースポート転送用の API 呼び出し / HTTPS をクリックします	管理ノードからストレージノードへ
22	SSH ログインアクセス	管理ノードからストレージノードへ、またはストレージノードから管理ノード



デフォルトでは、管理ノードでリモートアクセスの機能が有効になっています。リモートアクセス機能を無効にするには、を参照してください"[管理ノードで SSH 機能を管理します](#)"。必要に応じて、リモートアクセス機能を再度有効にすることができます。

手順

- 管理ノードにログインし、ターミナルセッションを開きます。
- プロンプトで、次のように入力します。

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

- リモートサポートトンネルを閉じるには、次のように入力します。

```
rst --killall
```

詳細情報

- "[vCenter Server 向け NetApp Element プラグイン](#)"
- "[NetApp HCI のリソースページ](#)"

管理ノードで SSH 機能を管理します

REST API を使用して、管理ノード (mNode) の SSH 機能の無効化、再有効化、ステータスの確認を行うことができます。のSSH機能"[ネットアップサポートの Remote Support Tunnel \(RST\) セッションアクセス](#)"は、管理ノードではデフォルトで有効になっています。

管理サービス2.20.69以降では、NetApp Hybrid Cloud Control UIを使用して管理ノードのSSH機能を有効または無効にすることができます。

必要なもの

- * NetApp Hybrid Cloud Controlの権限*：管理者の権限が必要です。
- * クラスタ管理者権限 *：ストレージクラスタに対する管理者権限があります。
- * Element ソフトウェア *：クラスタで NetApp Element ソフトウェア 11.3 以降が実行されている必要があります。
- * 管理ノード *：バージョン 11.3 以降を実行する管理ノードを導入しておきます。
- 管理サービスの更新：
 - NetApp Hybrid Cloud Control UIを使用するために、をバージョン2.20.69以降に更新しておき ["管理サービスのバンドル"](#)ます。
 - REST API UIを使用するために、をバージョン2.17に更新しておき ["管理サービスのバンドル"](#)ます。

オプション

- [NetApp Hybrid Cloud ControlのUI](#)を使用して、[管理ノードのSSH機能を無効または有効にします](#)

次のタスクは、実行後に実行でき["認証"](#)ます。

- [APIを使用して、管理ノードのSSH機能を無効または有効にします](#)
- [APIを使用して、管理ノードのSSH機能のステータスを確認します](#)

NetApp Hybrid Cloud ControlのUIを使用して、**管理ノードのSSH機能**を無効または有効にします

管理ノードで SSH 機能を無効にしたり、再度有効にしたりできます。のSSH機能["ネットアップサポートの Remote Support Tunnel \(RST\) セッションアクセス"](#)は、管理サービス2.18以降を実行する管理ノードではデフォルトで無効になっています。SSH を無効にしても、管理ノードへの既存の SSH クライアントセッションは終了せず、切断もされません。SSHを無効にしたあとで再度有効にすることを選択した場合、NetApp Hybrid Cloud ControlのUIを使用して再度有効にすることができます。



ストレージクラスタでSSHを使用したサポートアクセスを有効または無効にするには、を使用する必要があります ["Element UIクラスタ設定ページ"](#)。

手順

1. ダッシュボードで右上のオプションメニューを選択し、* 構成 * を選択します。
2. Support Access for Management Node *画面で、スイッチを切り替えて管理ノードSSHを有効にします。
3. トラブルシューティングが完了したら、* Support Access for Management Node *画面で、スイッチを切り替えて管理ノードSSHを無効にします。

APIを使用して、**管理ノードのSSH機能**を無効または有効にします

管理ノードで SSH 機能を無効にしたり、再度有効にしたりできます。のSSH機能["ネットアップサポートの Remote Support Tunnel \(RST\) セッションアクセス"](#)は、管理ノードではデフォルトで有効になっています。SSH を無効にしても、管理ノードへの既存の SSH クライアントセッションは終了せず、切断もされません。SSH を無効にしたあとで再度有効にすることを選択した場合は、同じ API を使用して再度有効にすることができます。

APIコマンド

管理サービス 2.18 以降の場合：

```
curl -k -X PUT
"https://<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

管理サービス 2.17 以前：

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



APIコマンドで使用されるベアラを見つけることができます `${TOKEN}` "許可する"。ベアラ `${TOKEN}` はカール応答にあります。

REST API の UI の手順

1. 管理ノードのIPアドレスに続けて次のように入力し、管理ノードAPIサービスのREST API UIにアクセスし `/mnode/` ます。

```
https://<ManagementNodeIP>/mnode/
```

2. 「* Authorize *」（認証）を選択して、次の手順を実行
 - a. クラスタのユーザ名とパスワードを入力します。
 - b. クライアントIDにと入力し `mnode-client` ます。
 - c. セッションを開始するには、* Authorize * を選択します。
 - d. ウィンドウを閉じます。
3. REST API UI から、* PUT / settings拘束 / ssh * を選択します。
 - a. [* 試してみてください *] を選択します。
 - b. SSHを無効にするか、以前に無効にしたSSH機能を再度有効にするには `true`、* enabled *パラメータをに設定し `false` ます。
 - c. [* Execute] を選択します。

APIを使用して、管理ノードのSSH機能のステータスを確認します

管理ノードで SSH 機能が有効になっているかどうかは、管理ノードのサービス API を使用して確認できます。管理ノードでは、SSH がデフォルトで有効になっています。

APIコマンド

管理サービス 2.18 以降の場合：


```
curl -k -X PUT
"https://<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

管理サービス 2.17 以前：

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



APIコマンドで使用されるベアラを見つけることができます ` \${TOKEN} ` "許可する"。ベアラ ` \${TOKEN} ` はコール応答にあります。

REST API の UI の手順

1. 管理ノードのIPアドレスに続けて次のように入力し、管理ノードAPIサービスのREST API UIにアクセスし ` /mnode/ ` ます。

```
https://<ManagementNodeIP>/mnode/
```

2. 「 * Authorize * 」 (認証) を選択して、次の手順を実行
 - a. クラスタのユーザ名とパスワードを入力します。
 - b. クライアントIDにと入力し ` mnode-client ` ます。
 - c. セッションを開始するには、 * Authorize * を選択します。
 - d. ウィンドウを閉じます。
3. REST API UI から、 * GET / settings拘束 / ssh * を選択します。
 - a. [* 試してみてください *] を選択します。
 - b. [* Execute] を選択します。

詳細情報

- ["vCenter Server 向け NetApp Element プラグイン"](#)
- ["NetApp HCI のリソースページ"](#)

NetApp HCI システムの電源をオフまたはオンにします

NetApp HCI システムの電源オン / オフを切り替えます

システム停止が予定されている場合、ハードウェアのメンテナンスを実施する必要がある場合、またはシステムの拡張が必要な場合は、NetApp HCI システムの電源をオフにしたり、オンにしたりできます。必要に応じて、次のタスクを実行して、NetApp HCI

システムの電源をオフにしたり、オンにしたりします。

NetApp HCI システムの電源をオフにする状況としては、次のようなケースが考えられます。

- スケジュールされたシステム停止
- シャーシのファンの交換
- ファームウェアのアップグレード
- ストレージリソースまたはコンピューティングリソースの拡張

NetApp HCI システムの電源をオフにするために必要な作業の概要を次に示します。

- VMware vCenter Server (vCSA) を除くすべての仮想マシンの電源をオフにします。
- vCSA をホストしているサーバ以外のすべての ESXi サーバの電源をオフにします。
- vCSA の電源をオフにします。
- NetApp HCI ストレージシステムの電源をオフにします。

NetApp HCI システムの電源をオンにするために必要な作業の概要を次に示します。

- すべての物理ストレージノードの電源をオンにします。
- すべての物理コンピューティングノードの電源をオンにします。
- vCSA の電源をオンにします。
- システムを確認し、追加の仮想マシンの電源をオンにします。

詳細情報

- ["NetApp HCI でサポートされるファームウェアとESXiドライバのバージョン、NetApp HCI ストレージノードでサポートされるファームウェアのバージョンとファームウェアのバージョン"](#)

NetApp HCI システムのコンピューティングリソースの電源をオフにします

NetApp HCI コンピューティングリソースの電源をオフにするには、個々の VMware ESXi ホストおよび VMware vCenter Server Appliance の電源を一定の順序でオフにする必要があります。

手順

1. NetApp HCI システムを制御する vCenter インスタンスにログインし、vCenter Server Virtual Appliance (vCSA) をホストしている ESXi マシンを特定します。
2. vCSA を実行している ESXi ホストを特定したら、次の手順に従って、vCSA 以外のすべての仮想マシンの電源をオフにします。
 - a. 仮想マシンを選択します。
 - b. 右クリックして、* 電源 > ゲスト OS のシャットダウン * を選択します。
3. vCSA を実行している ESXi ホスト以外のすべての ESXi ホストの電源をオフにします。
4. vCSA の電源をオフにします。

電源をオフにするまで vCSA が切断されるため、vCenter セッションが終了します。これで、1 台の ESXi ホストのみを電源オンにした状態ですべての仮想マシンをシャットダウンできます。

5. 実行中の ESXi ホストにログインします。
6. ホスト上のすべての仮想マシンの電源がオフになっていることを確認します。
7. ESXi ホストをシャットダウンします。

NetApp HCI ストレージクラスタに対して開いている iSCSI セッションがすべて切断されます。

詳細情報

- "NetApp HCI でサポートされるファームウェアとESXiドライバのバージョン、NetApp HCI ストレージノードでサポートされるファームウェアのバージョンとファームウェアのバージョン"

NetApp HCI システムのストレージリソースの電源をオフにします

NetApp HCIのストレージリソースの電源をオフにするときは、Element APIメソッドを使用してストレージノードを適切に停止する必要 `Shutdown` があります。

手順

コンピューティングリソースの電源をオフにしたら、Web ブラウザを使用して、NetApp HCI ストレージクラスタのすべてのノードをシャットダウンします。

1. ストレージクラスタにログインし、正しい MVIP に接続していることを確認します。
2. (オプション) ホストからのすべてのI/O処理が停止したことを確認します。
 - a. 使用している1つ以上のハイパーバイザーに適したコマンドを使用して、ホスト側からのI/Oを休止します。
 - b. クラスタUIで、* Reporting > Overview *を選択します。[クラスタの入出力]グラフにアクティビティが表示されていないことを確認します。
 - c. すべてのI/O処理が停止したら、20分待ってからクラスタをシャットダウンします。
3. iSCSI セッション数が 0 であることを確認します。
4. クラスタ > ノード > アクティブ * と進み、クラスタ内のすべてのアクティブノードのノード ID を記録します。
5. NetApp HCIストレージクラスタの電源をオフにするには、Webブラウザを開き、次のURLを使用して電源オフおよび停止の手順を実行します。はNetApp HCIストレージシステムの管理IPアドレスで、nodes=[] `アレイには手順4で記録したノードIDが含まれています` {MVIP}。例：

```
https://{MVIP}/json-rpc/1.0?method=Shutdown&nodes=[1,2,3,4]&option=halt
```



シークレットウィンドウでコマンドを実行すると、保存されているURLから以降の段階でコマンドが実行されないようにすることができます。

6. クラスタ管理者のユーザ名とパスワードを入力します。

- すべてのストレージクラスターノードがAPI結果のセクションに含まれていることを確認して、API呼び出しが正常に返されたことを確認します `successful`。

すべての NetApp HCI ストレージノードの電源がオフになりました。

- [戻る]ボタンを選択しないようにブラウザまたはタブを閉じてAPI呼び出しを繰り返します。

クラスターを再起動するときは、特定の手順に従ってすべてのノードがオンラインになったことを確認する必要があります。

1. 重大度の重大度とクラスターの障害がすべて解決されたことを確認します `volumesOffline`。
2. クラスターが安定するまで10~15分待ちます。
3. データにアクセスするためのホストの起動を開始します。



メンテナンス後にノードの電源をオンにして正常であることを確認する時間を長くしたい場合は、データの同期を遅らせて不要なビンの同期を回避する方法についてテクニカルサポートにお問い合わせください。

詳細情報

- ["NetApp HCI でサポートされるファームウェアとESXiドライバのバージョン、NetApp HCI ストレージノードでサポートされるファームウェアのバージョンとファームウェアのバージョン"](#)

NetApp HCI システムのストレージリソースの電源をオンにします

スケジュールされたシステム停止の終了後、NetApp HCI の電源をオンにできます。

手順

1. 電源ボタンまたは BMC を使用して、すべてのストレージノードの電源をオンにします。
2. BMC を使用している場合は、各ノードにログインし、* Remote Control > Power Control > Power On Server * と進みます。
3. すべてのストレージノードがオンラインになったら、NetApp HCI ストレージシステムにログインし、すべてのノードが動作していることを確認します。

詳細情報

- ["NetApp HCI でサポートされるファームウェアとESXiドライバのバージョン、NetApp HCI ストレージノードでサポートされるファームウェアのバージョンとファームウェアのバージョン"](#)

NetApp HCI システムのコンピューティングリソースの電源をオンにします

スケジュールされたシステム停止の終了後、NetApp HCI システムのコンピューティングリソースの電源をオンにできます。

手順

1. ストレージノードの電源をオンにする場合と同じ手順で、コンピューティングノードの電源をオンにします。

2. すべてのコンピューティングノードが稼働状態になったら、vCSA を実行していた ESXi ホストにログインします。
3. コンピューティングホストにログインし、すべての NetApp HCI データストアが表示されることを確認します。一般的な NetApp HCI システムでは、すべての ESXi ローカルデータストアと、少なくとも次の共有データストアが表示されます。

NetApp-HCI-Datastore-[01,02]

1. すべてのストレージにアクセスできる場合は、次の手順で vCSA とその他必要な仮想マシンの電源をオンにします。
 - a. ナビゲータで仮想マシンを選択し、パワーオンするすべての仮想マシンを選択して、*[パワーオン]*ボタンを選択します。
2. 仮想マシンの電源をオンにしたら、約 5 分待ってから Web ブラウザを使用して vCSA アプリケーションの IP アドレスまたは FQDN に移動します。

この操作が早すぎると、vSphere Client Web サーバが初期化中であることを示すメッセージが表示されます。

3. vSphere Client の初期化が完了したら、ログインして、すべての ESXi ホストと仮想マシンがオンラインであることを確認します。

詳細情報

- ["NetApp HCI でサポートされるファームウェアとESXiドライバのバージョン、NetApp HCI ストレージノードでサポートされるファームウェアのバージョンとファームウェアのバージョン"](#)

著作権に関する情報

Copyright © 2024 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。