管理ノードを操作します

Element Software

NetApp
November 12, 2025

目次

管理ノードを操作します 1
- 管理ノードの概要 1
- 管理ノードをインストールまたはリカバリします 2
  - 管理ノードをインストール 2
  - vCenter で NetApp HCC ロールを作成します 9
  - 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 14
  - 管理ノードをリカバリ 16
- 管理ノードにアクセスします 21
  - 管理ノードのノード UI にアクセスします 21
  - 管理ノードの REST API UI にアクセスします 22
- 管理ノードのデフォルトSSL証明書を変更します 23
  - 詳細については、こちらをご覧ください 24
- 管理ノード UI の操作 24
  - 管理ノード UI の概要 24
  - アラートの監視を設定 25
  - 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 25
  - 管理ノードからシステムユーティリティを実行します 27
- 管理ノード REST API の操作 28
  - 管理ノードの REST API UI の概要 28
  - REST API を使用するための許可を取得する 29
  - Active IQ とネットアップによる監視を有効にします 30
  - NetApp Hybrid Cloud Control を複数の vCenter に設定する 33
  - 管理ノードにコントローラアセットを追加します 34
  - ストレージクラスタアセットを作成および管理する 36
  - 既存のコントローラアセットを表示または編集する 41
  - プロキシサーバを設定します 42
  - 管理ノードの OS とサービスのバージョンを確認 44
  - 管理サービスからログを取得しています 45
- サポート接続を管理します 46
  - 基本的なトラブルシューティングのためにSSHを使用してストレージノードにアクセスする 47
  - 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 51
  - 管理ノードで SSH 機能を管理します 52

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。

ベストプラクティスとして、 1 つの管理ノードを 1 つの VMware vCenter インスタンスに関連付けるだけで、同じストレージリソースおよびコンピューティングリソースまたは vCenter インスタンスを複数の管理ノードに定義することは避けてください。

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') を使用すると ' 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 」）を使用すると、プロキシサーバの設定、サービスレベルの更新、アセット管理など、管理ノード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。

- "基本的なトラブルシューティングのためにSSHを使用してストレージノードにアクセスする"
  - "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"

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

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 SolidFire オールフラッシュストレージ管理者を対象としています。

作業を開始する前に

- 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。
- 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。

- ネットアップサポートサイト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 の略	.iso
VMware vSphere の場合	.iso 、 .ova のいずれかです
Citrix XenServer	.iso
OpenStack の機能を使用	.iso

- （管理ノード 12.0 以降にプロキシサーバを使用） NetApp Hybrid Cloud Control を管理サービスバージョン 2.16 に更新してから、プロキシサーバを設定しておきます。

このタスクについて

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をダウンロードしてVMを導入する

NetAppサポートサイトから適切なISOまたはOVAをダウンロードし、VMをインストールします。

手順

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"Element ソフトウェア"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へル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
      - （オプション）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。

手順**2**：管理ノードの管理者を作成してネットワークを設定する

VMのインストールが完了したら、管理ノードのadminユーザを作成し、管理ノードのネットワークを設定します。

手順

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 NIC を追加する必要がある場合は、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"。

ステップ**3**：時刻同期を設定する

管理ノードをセットアップする前に、管理ノードとストレージクラスタの時間を同期してください。

手順

1. NTPを使用して管理ノードとストレージクラスタの時間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：

```
sudo service ntpd stop
```

3. NTP 構成ファイル /etc/ntp.conf を編集します

a. 各サーバの前に # を追加して ' デフォルト・サーバ（サーバ 0.gentoo.pool.ntp.org ）をコメントアウトします

b. 追加したいデフォルトのタイムサーバー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ーは、ストレージクラスターで使用するNTPサーバー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 [ゲスト時刻をホストと同期する] チェックボックスがオフになっていることを確認します。

> 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。

時刻同期の設定が完了したら、NTPを編集しないでください。これは、実行時にNTPに影響します。 Setup コマンド 管理ノード上。

手順**4**：管理ノードをセットアップする

コマンドを使用して管理ノードを設定し `setup-mnode`ます。

手順

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 クラスターの管理仮想 IP アドレス (MVIP)。管理ノードを、インストール時に使用したのと同じストレージクラスターで構成します。 NTP サーバの設定。
      - *--storage_username(-su)[username] * ：「 --storage_mvip 」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。
      - * --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_volume_account (-pVA) [account_name]**:`--use_persistent_volumes が true に設定されている場合 ' 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 '--proxy_port' の入力を求めるプロンプトが表示されます
- **--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 (--proxy_hostname_or_ip`) の入力を求めるプロンプトが表示されます
- * --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. 「 etup-mnode 」コマンドを実行します。

手順**5**：コントローラアセットを設定する

インストールIDを確認し、vCenterコントローラアセットを追加します。

手順

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 にアクセスしてログインします。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 を「 m node-client 」として入力します。
      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 の応答本文から 'id' をコピーして保存し ' 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 Hybrid Cloud Control の vCenter コントローラアセットを管理ノードの既知のアセットに追加します。

a. 管理ノードの mNode サービス API UI にアクセスします。管理ノードの IP アドレスに「 /mnode 」を続けて入力します。

```
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 を「 m node-client 」として入力します。

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ロールを作成する必要があります。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。を参照してください "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「 vcenter 」タイプと「 vcenter 」クレデンシャルタイプで入力します。

g. [* Execute] を選択します。

詳細はこちら

- "永続ボリューム"
- "管理ノードにコントローラ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"
- "SolidFire および Element ソフトウェアのドキュメント"

vCenter で NetApp HCC ロールを作成します

vCenterでNetApp HCCロールを作成して、インストール後にvCenterアセット（コントローラ）を管理ノードに手動で追加したり、既存のコントローラを変更したりする必要があります。

この NetApp HCC ロールは、管理ノードのサービスビューをネットアップ専用のアセットに制限します。

このタスクについて

- この手順では、 vSphere 6.7 の場合の手順を説明しています。インストールされている vSphere のバージョンによっては、 vSphere のユーザインターフェイスが多少異なる場合があります。詳細については、 VMware vCenter のドキュメントを参照してください。
- 終了： "新しい NetApp HCC ロールを作成します"では、最初に vCenter で新しいユーザアカウントを設定し、 NetApp HCC ロールを作成してからユーザ権限を割り当てます。
- ネットアップ ESXi ホスト構成の場合は、 NDE で作成されたユーザアカウントを新しいネットアップ HCC ロールに更新する必要があります。
  - 使用 "このオプションを選択します" NetApp ESXi ホストが vCenter ホストクラスタ内に存在しない場合
  - 使用 "このオプションを選択します" NetApp ESXi ホストが vCenter ホストクラスタ内に存在する場合
- 可能です "コントローラアセットを設定します" 管理ノードにはすでに存在します。
- 新しい NetApp HCC ロールを使用してください "アセットを追加します" を管理ノードに追加します。

新しい NetApp HCC ロールを作成します

vCenter で新しいユーザアカウントをセットアップし、 NetApp HCC ロールを作成してユーザ権限を割り当てます。

vCenter で新しいユーザアカウントを設定します

vCenter で新しいユーザアカウントを設定するには、次の手順を実行します。

手順

1. vSphere Web Client に「 administrator@vsphere.loca l 」または同等の名前でログインします。
2. メニューから * 管理 * を選択します。
3. [* シングルサインオン *] セクションで、 [* ユーザー *] および [* グループ *] を選択します。
4. [**Domain**] リストで、 [vsphere] または LDAP ドメインを選択します。
5. [ユーザーの追加] を選択します。
6. ［ * ユーザーの追加 * ］ フォームに入力します。

vCenter で新しい NetApp HCC ロールを作成します

vCenter で新しい NetApp HCC ロールを作成するには、次の手順を実行します。

手順

1. [役割の編集] を選択し、必要な権限を割り当てます。

2. 左側のナビゲーションペインで、 * グローバル * を選択します。
3. [Diagnostics （診断）] と [License （ライセンス）] を選択します。
4. 左側のナビゲーションペインで、 **Hosts** を選択します。
5. [* Maintenance * （メンテナンス）] 、 [* Power * （電源）] 、 [* Storage partition configuration （ * ストレージパーティションの構成）] 、 [* Firmware * （ファームウェア * ）]
6. 「 NetApp Role 」として保存します。

vCenter にユーザ権限を割り当てます

次の手順を実行して、 vCenter の新しい NetApp HCC ロールにユーザ権限を割り当てます。

手順

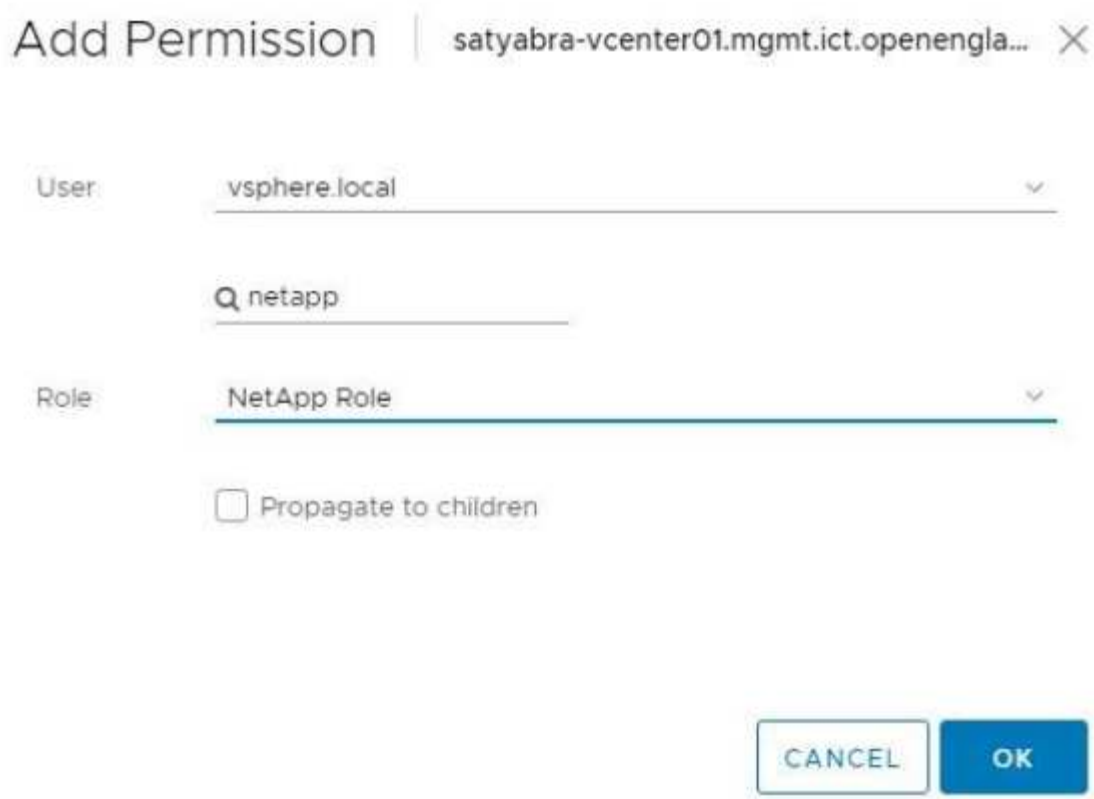
1. メニューから、 * Hosts * および * Clusters * を選択します。
2. 左側のナビゲーションペインで、次のいずれかのオプションを選択します。
   - 最上位の vCenter 。
   - リンクモードの場合は、必要な vCenter を選択します。

   - NetApp Element Plug-in for vCenter Server 5.0以降では、を使用します "vCenter リンクモード"NetApp SolidFire ストレージクラスタを管理するvCenter Serverごとに、Element Plug-inを別々の管理ノードから登録します（推奨）。
   - NetApp Element Plug-in for vCenter Server 4.10以前を使用して、他のvCenter Serverのクラスタリソースを管理する "vCenter リンクモード" はローカルストレージクラスタのみに制限されます。
3. 右のナビゲーションペインで、 * 権限 * を選択します。
4. 新しいユーザを追加するには、「 * + * 」アイコンを選択します。

   [権限の追加 *] ウィンドウに次の詳細を追加します。

   a. 「 vSphered.local 」または LDAP ドメインを選択します
   b. 検索を使用して、で作成した新しいユーザを検索します vCenter で新しいユーザアカウントを設定します。
   c. ［ NetApp Role ］ を選択します。

      Do * not * select * Propagate to children * を選択します。



データセンターにユーザ権限を割り当てます

vCenter のデータセンターにユーザ権限を割り当てるには、次の手順を実行します。

手順

1. 左側のペインで、 * Datacenter * を選択します。
2. 右のナビゲーションペインで、 * 権限 * を選択します。
3. 新しいユーザを追加するには、「 * + * 」アイコンを選択します。

   [権限の追加 *] ウィンドウに次の詳細を追加します。

   a. 「 vSphered.local 」または LDAP ドメインを選択します。
   b. で作成した新しい HCC ユーザを検索するには、検索を使用します vCenter で新しいユーザアカウントを設定します。
   c. 「 ReadOnly ロール」を選択します。

   Do * not * select * Propagate to children * を選択します。

NetApp HCI データストアにユーザ権限を割り当てます

vCenter で NetApp HCI データストアにユーザ権限を割り当てるには、次の手順を実行します。

手順

1. 左側のペインで、 * Datacenter * を選択します。

2. 新しいストレージフォルダを作成します。[**Datacenter**] を右クリックし、 **[*Create storage folder**] を選択します。
3. すべての NetApp HCI データストアをストレージクラスタからローカルにコンピューティングノードに転送し、新しいストレージフォルダに移動します。
4. 新しいストレージフォルダを選択します。
5. 右のナビゲーションペインで、 * 権限 * を選択します。
6. 新しいユーザを追加するには、「 * + * 」アイコンを選択します。

   [権限の追加 *] ウィンドウに次の詳細を追加します。

   a. 「 vSphered.local 」または LDAP ドメインを選択します。
   b. で作成した新しい HCC ユーザを検索するには、検索を使用します vCenter で新しいユーザアカウントを設定します。
   c. 「管理者ロール」を選択します
   d. * 子に伝播 * を選択する。

ネットアップホストクラスタにユーザ権限を割り当てます

vCenter でネットアップホストクラスタにユーザ権限を割り当てるには、次の手順を実行します。

手順

1. 左側のナビゲーションペインで、ネットアップホストクラスタを選択します。
2. 右のナビゲーションペインで、 * 権限 * を選択します。
3. 新しいユーザを追加するには、「 * + * 」アイコンを選択します。

   [権限の追加 *] ウィンドウに次の詳細を追加します。

   a. 「 vSphered.local 」または LDAP ドメインを選択します。
   b. で作成した新しい HCC ユーザを検索するには、検索を使用します vCenter で新しいユーザアカウントを設定します。
   c. 「 NetApp Role 」または「 Administrator 」を選択します。
   d. * 子に伝播 * を選択する。

NetApp ESXi ホスト構成

ネットアップ ESXi ホスト構成の場合は、 NDE で作成されたユーザアカウントを新しいネットアップ HCC ロールに更新する必要があります。

NetApp ESXi ホストが **vCenter** ホストクラスタに存在しません

NetApp ESXi ホストが vCenter ホストクラスタ内にない場合は、次の手順を使用して vCenter でネットアップ HCC ロールとユーザ権限を割り当てることができます。

手順

1. メニューから、 * Hosts * および * Clusters * を選択します。

2. 左側のナビゲーションペインで、 NetApp ESXi ホストを選択します。
3. 右のナビゲーションペインで、 * 権限 * を選択します。
4. 新しいユーザを追加するには、「 * + * 」アイコンを選択します。

   [権限の追加 *] ウィンドウに次の詳細を追加します。

   a. 「 vSphered.local 」または LDAP ドメインを選択します。
   b. 検索を使用して、で作成した新しいユーザを検索します vCenter で新しいユーザアカウントを設定します。
   c. 「 NetApp Role 」または「 Administrator 」を選択します。
5. * 子に伝播 * を選択する。

NetApp ESXi ホストが vCenter ホストクラスタに存在する

ネットアップ ESXi ホストが他のベンダーの ESXi ホストを含む vCenter ホストクラスタ内にある場合は、次の手順を使用してネットアップの HCC ロールとユーザ権限を vCenter で割り当てることができます。

1. メニューから、 * Hosts * および * Clusters * を選択します。
2. 左側のナビゲーションペインで、目的のホストクラスタを展開します。
3. 右のナビゲーションペインで、 * 権限 * を選択します。
4. 新しいユーザを追加するには、「 * + * 」アイコンを選択します。

   [権限の追加 *] ウィンドウに次の詳細を追加します。

   a. 「 vSphered.local 」または LDAP ドメインを選択します。
   b. 検索を使用して、で作成した新しいユーザを検索します vCenter で新しいユーザアカウントを設定します。
   c. ［ NetApp Role ］ を選択します。

      Do * not * select * Propagate to children * を選択します。
5. 左側のナビゲーションペインで、 NetApp ESXi ホストを選択します。
6. 右のナビゲーションペインで、 * 権限 * を選択します。
7. 新しいユーザを追加するには、「 * + * 」アイコンを選択します。

   [権限の追加 *] ウィンドウに次の詳細を追加します。

   a. 「 vSphered.local 」または LDAP ドメインを選択します。
   b. 検索を使用して、で作成した新しいユーザを検索します vCenter で新しいユーザアカウントを設定します。
   c. 「 NetApp Role 」または「 Administrator 」を選択します。
   d. * 子に伝播 * を選択する。
8. ホストクラスタ内の残りの NetApp ESXi ホストに対して同じ手順を繰り返します。

管理ノードにはすでにコントローラアセットが存在します

コントローラアセットが管理ノードにすでに存在する場合は、次の手順を実行して、「 PUT /assets/{asset_id }/controllers /{controller_id } 」を使用してコントローラを設定します。

手順

1. 管理ノードの mNode サービス API UI にアクセスします。

   https://<ManagementNodeIP>/mnode`

2. 「 * Authorize * 」を選択し、 API 呼び出しにアクセスするためのクレデンシャルを入力します。
3. [get/assets] を選択して、親 ID を取得します。
4. 'put/assets/{asset_id }/controllers /{controller_id }' を選択します
   a. アカウントセットアップで作成したクレデンシャルを要求の本文に入力します。

管理ノードにアセットを追加します

インストール後に新しいアセットを手動で追加する必要がある場合は、で作成した新しい HCC ユーザアカウントを使用します vCenter で新しいユーザアカウントを設定します。詳細については、を参照してください "管理ノードにコントローラアセットを追加します"。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

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。

作業を開始する前に

- eth0 の IP アドレスを確認しておきます。
- クラスタで NetApp Element ソフトウェア 11.3 以降を実行している必要があります。
- 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・インターフェイスに必要なパラメータごとに値は「 $ 」で表されます。次のテンプレート内の 'cluster' 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`-- 非セキュアなオプションや '-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・インターフェイスに必要なパラメータごとに値は「 $ 」で表されます。次のテンプレート内の 'cluster' 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`-- 非セキュアなオプションや '-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

- "管理ノードにコントローラアセットを追加します"
- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

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を実行していた 11.3 以降 "永続ボリューム" 機能が関与している。
- 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。
- 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。
- ネットアップサポートサイト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 の略	.iso
VMware vSphere の場合	.iso 、 .ova のいずれかです
Citrix XenServer	.iso
OpenStack の機能を使用	.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. から、インストール環境に対応した OVA または ISO をダウンロードします "Element ソフトウェア" ネットアップサポートサイトのページを参照してください。
   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へル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 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
- （ SolidFire オールフラッシュストレージの場合はオプション）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 NIC を追加する必要がある場合は、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時間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以降の場合は、に進みます サブステップ (f) 時刻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：

```
sudo service ntpd stop
```

3. NTP 構成ファイル /etc/ntp.conf を編集します

   a. 各サーバの前に # を追加して ' デフォルト・サーバ（サーバ 0.gentoo.pool.ntp.org ）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、同じ NTP サーバである必要があります で使用するストレージクラスタで使用します A "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 [ゲスト時刻をホストと同期する] チェックボックスがオフになっていることを確認します。

> 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。

の実行時は NTP に影響するため、時刻の同期設定の完了後は NTP を編集しないでください 再導入コマンド 管理ノード。

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以前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、「 /sf/mnode 」ディレクトリに保存します。
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. 生成されたファイルを '/sf/mnode -archive' ディレクトリに解凍します

```
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。同じストレージクラスタを使用して管理ノードを設定します の間に使用しました "NTP サーバの設定"。
      - * [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。

1. 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. 「 redeploy -mnode 」コマンドを実行します。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 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、 "管理ノードの認証を再設定します"。

提供する 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" 管理サービス 2.18 以降を実行する管理ノードでは、はデフォルトで無効になっています。以前に管理ノードで SSH 機能を有効にしていた場合は、が必要になることがあります "SSH を再度無効にします" リカバリされた管理ノード。

詳細はこちら

- "永続ボリューム"
- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

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 」）を使用して、プロキシサーバの設定、サービスレベルの更新、アセット管理などの管理ノード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。

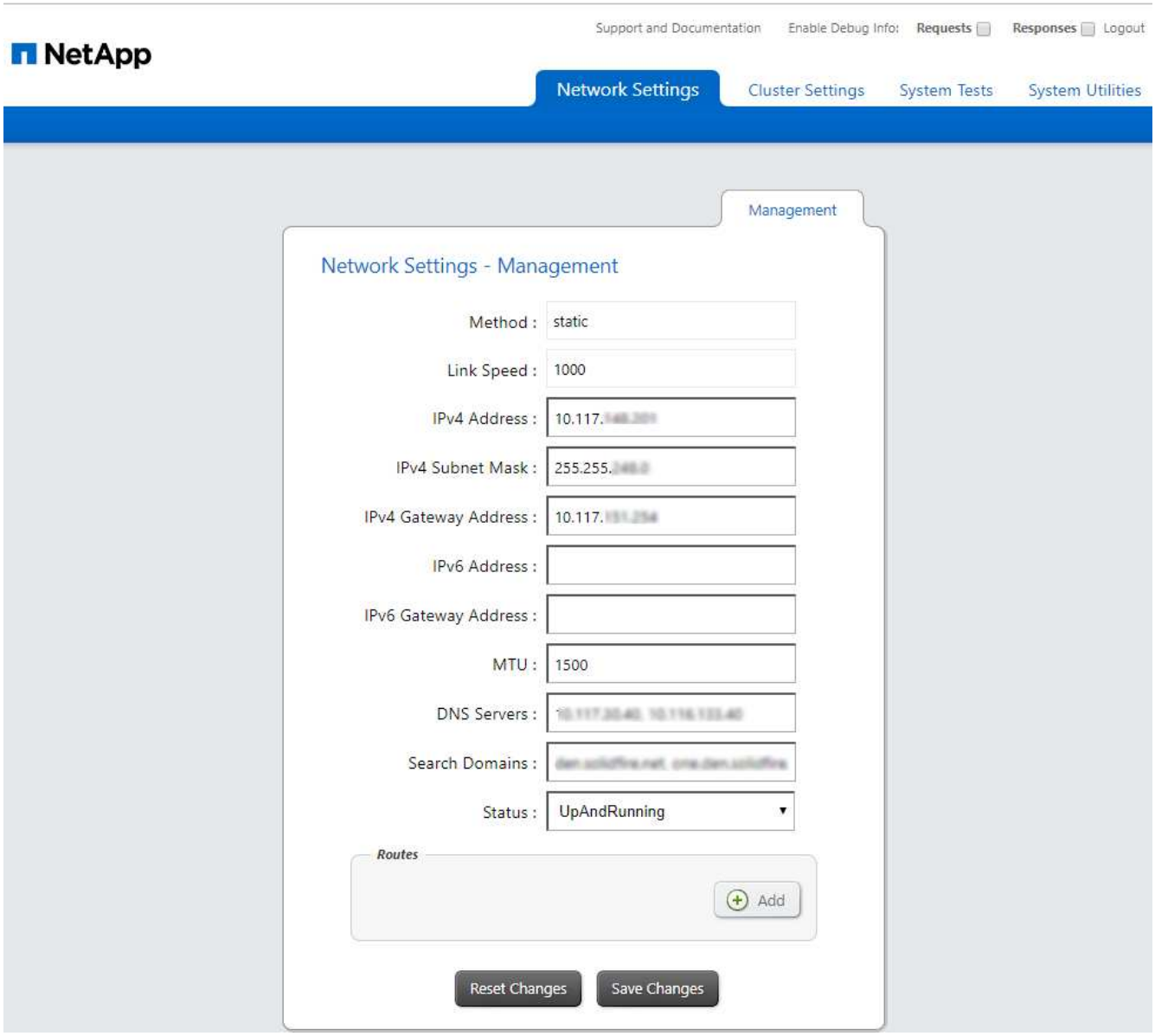
管理ノードのノード **UI** にアクセスします

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
```



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。

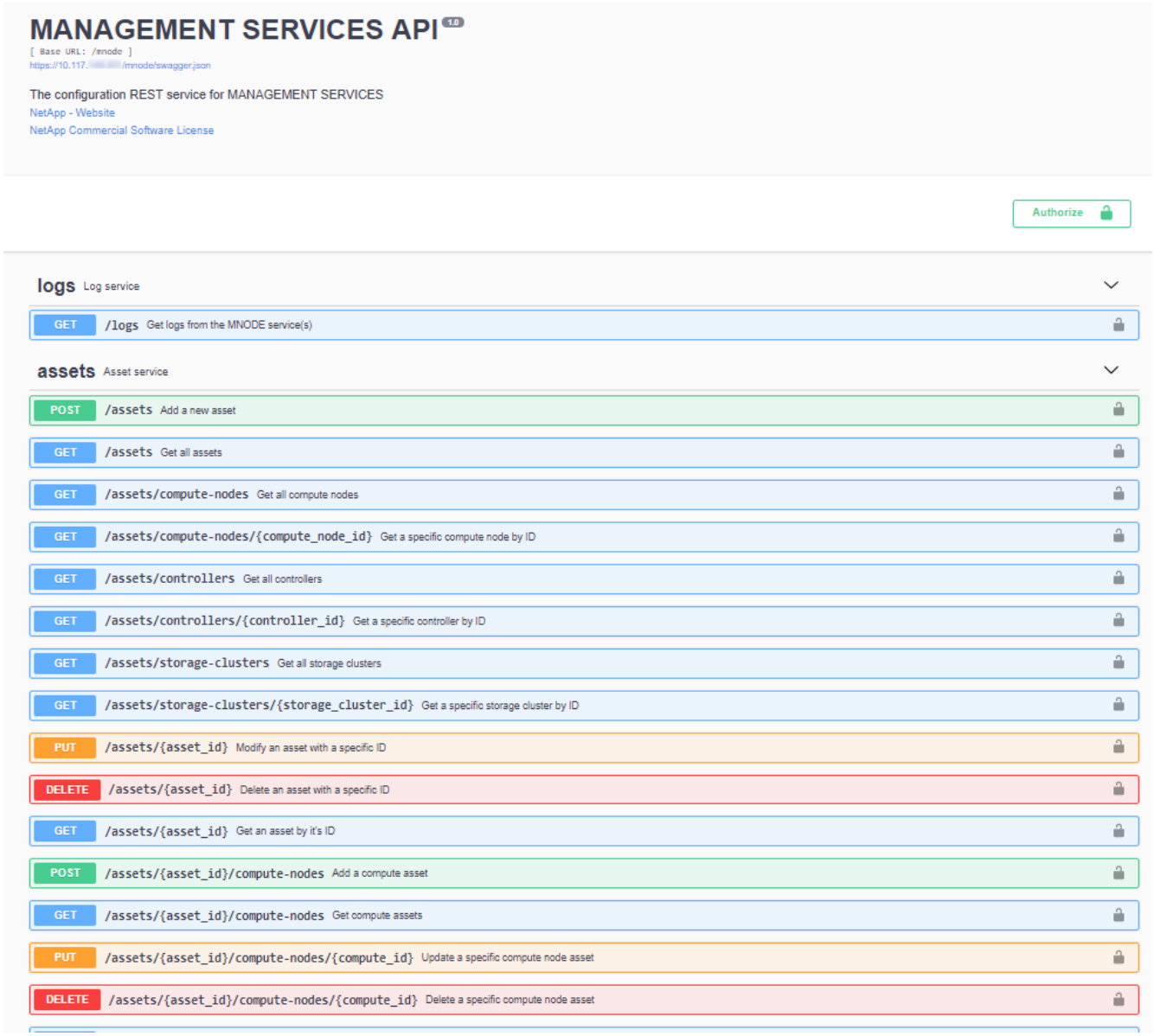
管理ノードの **REST API UI** にアクセスします

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「 /mnode 」を続けて入力します。

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



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 とネットアップによる監視を有効にします"
- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

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 *

  を使用できます "GetNodeSSLCertificateメソッド" 現在インストールされているSSL証明書に関する情報（すべての証明書の詳細を含む）を取得します。

- * SetNodeSSLCertificate *

  を使用できます "SetNodeSSLCertificateメソッド" 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します。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 "RemoveNodeSSLCertificateメソッド" 現在インストールされているSSL証明書と秘密鍵を削除します。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。

詳細については、こちらをご覧ください

- "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` ）を使用すると、ネットワークおよび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。

- "アラートの監視を設定"
- "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"

詳細については、こちらをご覧ください

- "管理ノードにアクセスします"
- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

アラートの監視を設定

アラート監視ツールは、 NetApp HCI のアラート監視用に設定されています。これらのツールは、 SolidFire オールフラッシュストレージには設定も使用もされません。これらのクラスタに対してツールを実行すると、「 webUIParseError ： Invalid response from server 」のような 405 エラーが表示されますが、これは想定される設定です。405`

NetApp HCI のアラート監視を設定する方法の詳細については、を参照してください "アラートの監視を設定"

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場合に使用します。
      - 「手動」：デフォルトで設定が行われないインターフェイスを定義する場合に使用します。
      - `d hop`: DHCP を介して IP アドレスを取得するために使用します。
      - 'tatic ：静的に割り当てられた IPv4 アドレスを持つ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 」
- 「所有」
- 「上」

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。有効な値は「管理」です。
   - * 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"
- "SolidFire および Element ソフトウェアのドキュメント"

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「再起動」と「停止」 (電源オフ) が含まれます。
      - * 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 's_make _support_bundle' スクリプトに渡されますこのパラメータは、ネットアップサポートから指示され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。詳細が必要な場合は、ネットアップサポートにお問い合わせください。

> 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"
- "SolidFire および Element ソフトウェアのドキュメント"

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` ）を使用すると、プロキシサーバの設定、サービスレベルの更新、アセット管理などの管理ノード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。

REST API で実行できるタスクは次のとおりです。

承認

- "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 とネットアップによる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"
- "管理ノードにコントローラアセットを追加します"

- "ストレージクラスタアセットを作成および管理する"

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"
- "ストレージクラスタアセットを作成および管理する"
- "REST API を使用して Element システムログを収集します"
- "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"

詳細については、こちらをご覧ください

- "管理ノードにアクセスします"
- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

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す。

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。

作業を開始する前に

- 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. サービスの REST API UI にアクセスするには、管理ノードの IP アドレスのあとにサービス名を入力します。例：「 /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 を「 m node-client 」として入力します。
   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。

   トークンの期限が切れた後にコマンドを実行しようとすると、「 401 Error: Unauthorized 」という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。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

Active IQ とネットアップによる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、有効にすることができます。SolidFire オールフラッシュストレージシステムのインストール時に SolidFire Active IQ をセットアップしなかった場合は、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 SolidFire Active IQ に転送します。ネットアップ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。

作業を開始する前に

- Quality of Service（QoS；サービス品質）などのActive IQ の一部の機能を正しく機能させるには、Element 11.3以降が必要です。Active IQ のすべての機能を使用できることを確認するために、次のことを推奨します。
  - 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。外部接続のないダークサイトからは、 Active IQ コレクタサービスを使用できません。

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 を「 m node-client 」として入力します。

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 の応答本文から ' インストールの ID をコピーします

```
{
  "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 mNode サービス API UI にアクセスします。管理ノードの IP アドレスに「 /mnode 」を続けて入力します。

```
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 を「 m node-client 」として入力します。

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. NetApp Hybrid Cloud Control の vCenter コントローラアセットをまだ追加していない場合は、管理ノードの既知のアセットに追加します。

ネットアップ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「 type 」に「 vcenter 」、 vCenter クレデンシャルを指定して入力します。

```
{
"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。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"

- "SolidFire および Element ソフトウェアのドキュメント"

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. 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 2 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 を「 m node-client 」として入力します。
      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. 更新を「 True 」に設定します。
   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。
3. 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。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

管理ノードにコントローラアセットを追加します

REST API UI を使用して、管理ノードの設定に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きます。
- vCenter で新しい NetApp HCC ロールを作成して、管理ノードのサービス表示をネットアップ専用のアセットに制限します。を参照してください "vCenter で NetApp HCC ロールを作成します"

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 を「 m node-client 」として入力します。
      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 の応答本文から ' インストールの ID をコピーします

```
{
  "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、後の手順で使用するために、クラスタコントローラ ID （「 ControllerID 」）をコピーして保存します。

2. 既存のベースアセットにコントローラサブアセットを追加する場合は、以下を選択します。

```
POST /assets/{asset_id}/controllers
```

a. 管理ノードで mNode サービス REST API UI を開きます。

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

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 を「 m node-client 」として入力します。
   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. 「 * POST /assets/ ｛ asset_id ｝ /controllers * 」を選択します。
d. [* 試してみてください *] を選択します。
e. 親ベースアセット ID を「 * asset_id * 」フィールドに入力します。
f. 必要な値をペイロードに追加します。

g. [* Execute] を選択します。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

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「 /inventory/1/` 」を入力して、インベントリサービスの REST API UI にアクセスします。

```
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 を「 m node-client 」として入力します。
   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/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 の応答本文から ' インストールのリストにある 'id' フィールドに値を保存しますこれはインストール ID です。例：

```
"installations": [
    {
      "id": "1234a678-12ab-35dc-7b4a-1234a5b6a7ba",
      "name": "my-sf-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「 /storage/1/` 」を入力して、ストレージサービスの REST API UI にアクセスします。

```
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 を「 m node-client 」として入力します。
   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。
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 'installationId' パラメータに入力します
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 の応答本文から、正しいストレージクラスタを探して、クラスタの「 torageId 」フィールドに値を保存します。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

- をコピーしました ストレージクラスタ ID とインストール ID をクリックします。
- 複数のストレージノードを追加する場合は、の制限を確認しておく必要があります "権限のあるクラスタです" 複数のストレージクラスタをサポート

> 信頼できるクラスタで定義されたすべてのユーザは、 NetApp 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「 /storage/1/` 」を入力して、ストレージサービスの REST API UI にアクセスします。

```
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 を「 m node-client 」として入力します。
   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. [* 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	を入力します	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 」と入力します	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。

パラメータ	を入力します	説明
「 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。

の手順に従っていることを確認します 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 続行する前に。

手順

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

   ```
   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 を「 m node-client 」として入力します。
   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. PUT / clusters/ ｛ storageId ｝ * を選択します。
4. [* 試してみてください *] を選択します。
5. 以前にコピーしたストレージクラスタ ID を「 torageId 」パラメータに貼り付けます。
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	を入力します	説明
「 password 」と入力します	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。

の手順に従っていることを確認します 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 続行する前に。

手順

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

```
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 を「 m node-client 」として入力します。
   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. DELETE /clusters/ ｛ storageId ｝ * を選択します。
4. [* 試してみてください *] を選択します。
5. 「 torageId 」パラメータに、前の手順でコピーしたストレージクラスタ ID を入力します。
6. [* Execute] を選択します。

   成功すると、 API は空の応答を返します。

詳細については、こちらをご覧ください

- "権限のあるクラスタです"
- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

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 SolidFire 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。

作業を開始する前に

- 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「 /vCenter/1/` 」を入力して、管理サービスの REST API UI にアクセスします。

   ```
   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 を「 m node-client 」として入力します。
   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。

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 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を取得する場合は ' そのコントローラの [id] フィールドからコントローラ ID をクリップボードにコピーし ' 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. 以前にコピーしたコントローラ ID を 'controller_id パラメータに入力します
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 'controller_id パラメータに入力します
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	を入力します	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 」と入力します	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。

詳細については、こちらをご覧ください

- "管理ノードにコントローラアセットを追加します"
- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

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 、ネットアップ監視サービス、およびネットアップサポート用リバーストンネルなど、管理ノードにインストールされている Element ソフトウェアのその他のユーティリティで使用されます。

作業を開始する前に

- 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 以降）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「 /mnode 」を続けて入力し、管理ノードの REST API UI にアクセスします。

   ```
   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 を「 m node-client 」として入力します。
   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. 「 * 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 'use_proxy' を true に設定する必要があります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、管理ノードのリブートが必要になることがあります。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

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（ **Options** ）

- 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: ${TOKEN}"
```

API コマンドで使用されるベアラー '$ ｛ token ｝ ' を検索できます "許可します"。ベアラー '$ ｛ token ｝ ' は curl 応答に含まれています。

REST API の UI の手順

1. 管理ノードの IP アドレスのあとに「 /mnode/ 」を入力して、サービスの REST API UI にアクセスします。

```
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。

     管理サービスのバンドルバージョン（「 mnode_bundle_version 」）、管理ノードの OS バージョン（「 os_version 」）、および管理ノードの API バージョン（「 version 」）が応答の本文に示されます。
   - 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。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

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 」：ログから返される行数を入力します。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。

   - [`ince] ：サービスログの開始時点の ISO-8601 タイムスタンプを追加します。

     より広いタイムパンのログを収集する場合は、妥当な「 ince」 パラメータを使用してください。

   - 「 service-name 」：サービス名を入力します。

     管理ノード上のサービスを一覧表示するには 'get/services' コマンドを使用します

   - 'setp` ：停止したサービスからログを取得するには 'true' に設定します
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"
- "SolidFire および Element ソフトウェアのドキュメント"

サポート接続を管理します

基本的なトラブルシューティングのためにSSHを使用してストレージノードにアクセスする

Element 12.5以降では、基本的なトラブルシューティングに、ストレージノード上でsfreadonlyシステムアカウントを使用できます。高度なトラブルシューティングのために、ネットアップサポート用のリモートサポートトンネルアクセスを有効にして開くこともできます。

sfreadonlyシステムアカウントを使用すると、基本的なLinuxシステムおよびネットワークトラブルシューティングコマンド(pingコマンドを含む)を実行できます。

> ネットアップサポートから指示されないかぎり、このシステムに対する変更はサポートされず、サポート契約にも取り消し、データのアクセスが不安定になったり、アクセスできなくなる場合があります。

作業を開始する前に

- 書き込み許可：現在の作業ディレクトリに対する書き込み許可があることを確認します。
- (オプション)独自のキーペアを生成: Windows 10、MacOS、またはLinuxディストリビューションから「ssh-keygen」を実行します。これは、ユーザキーペアを作成する1回限りのアクションで、今後のトラブルシューティングセッションで再利用できます。このモデルでは、従業員アカウントに関連付けられた証明書を使用することもできます。
- 管理ノードでSSH機能を有効にする：管理モードでリモートアクセス機能を有効にするには、を参照してください "このトピック"。管理サービス 2.18 以降では、管理ノードでリモートアクセス機能がデフォルトで無効になっています。
- ストレージクラスタでSSH機能を有効にする：ストレージクラスタノードでリモートアクセス機能を有効にするには、を参照してください "このトピック"。
- ファイアウォールの設定：管理ノードがプロキシサーバの背後にある場合は、sshd.configファイルで次のTCPポートを設定しておく必要があります。

TCP ポート	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に 管理ノード

トラブルシューティングのオプション

- [クラスタノードのトラブルシューティングを行う]
- [ネットアップサポートでクラスタノードのトラブルシューティングを行います]
- [クラスタに属していないノードのトラブルシューティングを行う]

クラスタノードのトラブルシューティングを行う

sfreadonlyシステムアカウントを使用した基本的なトラブルシューティングを実行できます。

手順

1. 管理ノードVMのインストール時に選択したアカウントのログインクレデンシャルを使用して、管理ノードにSSH接続します。
2. 管理ノードで'/sf/bin'に移動します
3. ご使用のシステムに適したスクリプトを検索します。
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

   SignSshKeys.ps1はPowerShell 7以降に依存し、SignSshKeys.pyはPython 3.6.0以降およびに依存しています "モジュールを要求します"。

   「SignSshKeys」スクリプトは、「user」、「user.pub」、および「user-cert.pub」ファイルを現在の作業ディレクトリに書き込みます。これらのファイルはあとで「ssh」コマンドで使用されます。ただし、公開鍵ファイルがスクリプトに提供されると、ディレクトリに書き込まれるのは「<public_key>」ファイル（「<public_key>」で置き換えられた「公開鍵ファイル」の接頭辞）のみです。

4. 管理ノードでスクリプトを実行して、SSHキーチェーンを生成します。スクリプトでは、クラスタ内のすべてのノードに対して、sfreadonlyシステムアカウントを使用したSSHアクセスを有効にしています。

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--publickey [public key path]
```

   a. 次の各パラメータについて、[]括弧内の値（括弧を含む）を置き換えます。

      省略形またはフル形式のパラメータを使用できます。

      - **--ip|-i [IP address]**：APIの実行対象となるターゲットノードのIPアドレス。
      - **--user|-u [username]**：API呼び出しの実行に使用するクラスタユーザ。
      - （任意）**--duration|-d[hours]**：符号付きキーの有効期間は、時間単位の整数として保持する必要があります。デフォルトは 24 時間です。
      - （任意）**-publickey |-k [**公開鍵のパス**]**：ユーザが公開鍵を指定した場合のパス。

   b. 入力内容を次のコマンド例と比較します。この例では'10.116.139.195'はストレージ・ノードのIPで'admin'はクラスタ・ユーザ名で'キーの有効期間は2時間です

```
sh /sf/bin/SignSshKeys.sh --ip 10.116.139.195 --user admin --duration
2
```

c. コマンドを実行します。

5. ノードIPへのSSH接続：

```
ssh -i user sfreadonly@[node_ip]
```

基本的なLinuxシステムおよびネットワークのトラブルシューティングコマンド(pingコマンドなど)やその他の読み取り専用コマンドを実行できます。

6. （任意）ディセーブルにします "リモートアクセス機能" トラブルシューティングが完了したら、もう一度実行します。

SSHを無効にしないと、管理ノードでSSHが有効なままになります。SSH を有効にした設定は、手動で無効にするまで、更新やアップグレードを通じて管理ノードで維持されます。

ネットアップサポートでクラスタノードのトラブルシューティングを行います

ネットアップサポートは、技術者がより詳細なElement診断を実行できるようにするシステムアカウントを使用して、高度なトラブルシューティングを実行できます。

手順

1. 管理ノードVMのインストール時に選択したアカウントのログインクレデンシャルを使用して、管理ノードにSSH接続します。
2. ネットアップサポートから送信されたポート番号を指定してrstコマンドを実行し、サポートトンネルを開きます。

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

   ネットアップサポートは、サポートトンネルを使用して管理ノードにログインします。

3. 管理ノードで'/sf/bin'に移動します
4. ご使用のシステムに適したスクリプトを検索します。
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

   SignSshKeys.ps1はPowerShell 7以降に依存し、SignSshKeys.pyはPython 3.6.0以降およびに依存しています "モジュールを要求します"。

   「SignSshKeys」スクリプトは、「user」、「user.pub」、および「user-cert.pub」ファイルを現在の作業ディレクトリに書き込みます。これらのファイルはあとで「ssh」コマンドで使用されます。ただし、公開鍵ファイルがスクリプトに提供されると、ディレクトリに書き込まれるのは「<public_key>」ファイル（「<public_key>」で置き換えられた「公開鍵ファイル」の接頭辞）のみです。

5. スクリプトを実行して、「--sfadmin」フラグを付けたSSHキーチェーンを生成します。このスクリプトでは、すべてのノードでSSHを有効にします。

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--sfadmin
```

クラスタノードに—sfadminとしてSSHするには、クラスタ上で「supportAdmin」アクセス権を持つ「--user」を使用してSSHキーチェーンを生成する必要があります。

クラスタ管理者アカウントの「supportAdmin」アクセスを設定するには、Element UIまたはAPIを使用します。

- "Element UIを使用して「supportAdmin」アクセスを設定します"
- APIを使用して「supportAdmin」アクセスを構成し、「supportAdmin」を「access」タイプとしてAPI要求に追加します。
  - "新しいアカウントの「supportAdmin」アクセスを設定します"
  - "既存のアカウントの「supportAdmin」アクセスを設定します"

    'clusterAdminID'を取得するには'を使用します "ListClusterAdmins" API

「supportAdmin」アクセスを追加するには、クラスタ管理者または管理者の権限が必要です。

a. 次の各パラメータについて、[]括弧内の値（括弧を含む）を置き換えます。

   省略形またはフル形式のパラメータを使用できます。

   - **--ip|-i [IP address]**：APIの実行対象となるターゲットノードのIPアドレス。
   - **--user|-u [username]**：API呼び出しの実行に使用するクラスタユーザ。
   - （任意）**--duration|-d[hours]**：符号付きキーの有効期間は、時間単位の整数として保持する必要があります。デフォルトは 24 時間です。

b. 入力内容を次のコマンド例と比較します。この例では'192.168.0.1'はストレージ・ノードのIP 'admin'はクラスタ・ユーザ名'キーの有効期間は2時間'--sfadmin'は'トラブルシューティングのためにNetAppサポート・ノードにアクセスできるようにします

```
sh /sf/bin/SignSshKeys.sh --ip 192.168.0.1 --user admin --duration 2
--sfadmin
```

c. コマンドを実行します。

6. ノードIPへのSSH接続：

```
ssh -i user sfadmin@[node_ip]
```

7. 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

8. （任意）ディセーブルにします "リモートアクセス機能" トラブルシューティングが完了したら、もう一度実行します。

> SSHを無効にしないと、管理ノードでSSHが有効なままになります。SSH を有効にした設定は、手動で無効にするまで、更新やアップグレードを通じて管理ノードで維持されます。

クラスタに属していないノードのトラブルシューティングを行う

クラスタにまだ追加されていないノードについて、基本的なトラブルシューティングを実行できます。sfreadonlyシステムアカウントは、ネットアップサポートの有無に関係なく使用できます。管理ノードを設定している場合は、SSHに使用し、このタスクに提供されたスクリプトを実行できます。

1. SSHクライアントがインストールされているWindows、Linux、またはMacマシンで、ネットアップサポートから提供されたシステムに適したスクリプトを実行します。
2. ノードIPへのSSH接続：

```
ssh -i user sfreadonly@[node_ip]
```

3. （任意）ディセーブルにします "リモートアクセス機能" トラブルシューティングが完了したら、もう一度実行します。

> SSHを無効にしないと、管理ノードでSSHが有効なままになります。SSH を有効にした設定は、手動で無効にするまで、更新やアップグレードを通じて管理ノードで維持されます。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のドキュメント"

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

SolidFire オールフラッシュストレージ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。

ネットアップサポートとの 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。

作業を開始する前に

- 管理サービス 2.18 以降では、管理ノードでリモートアクセス機能がデフォルトで無効になっています。リモートアクセス機能を有効にするには、を参照してください "管理ノードで SSH 機能を管理します"。

- 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	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に 管理ノード

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

- （任意）ディセーブルにします "リモートアクセス機能" をもう一度クリックします

> SSHを無効にしないと、管理ノードでSSHが有効なままになります。SSH を有効にした設定は、手動で無効にするまで、更新やアップグレードを通じて管理ノードで維持されます。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

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。提供する 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" 管理サービス 2.18 以降を実行する管理ノードでは、はデフォルトで無効になっています。

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のUIを使用するために、を更新しておきます "管理サービスのバンドル" をバージョン2.20.69以降にアップグレードします。
  - REST API UIを使用するために、を更新しておきます "管理サービスのバンドル" バージョン 2.17 へ。

オプション（ **Options** ）

- 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

完了後、次のいずれかのタスクを実行できます "認証"：

- 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。提供する 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" 管理サービス 2.18 以降を実行する管理ノードでは、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に対してSSHを使用して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。提供する 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" 管理サービス 2.18 以降を実行する管理ノードでは、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ー '$ ｛ token ｝ ' を検索できます "許可します"。ベアラー '$ ｛ token ｝ ' は curl 応答に含まれています。

REST API の **UI** の手順

1. 管理ノードの IP アドレスのあとに「 /mnode/ 」を入力して、管理ノード API サービスの REST API UI にアクセスします。

   ```
   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 を「 m node-client 」として入力します。
   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. REST API UI から、 * PUT / settingsusel/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 をディセーブルにするには '**enabled** パラメータを 'false' に設定し ' 前にディセーブルにした SSH 機能を再度イネーブルにするには 'true' を設定します
   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。管理サービス 2.18 以降を実行する管理ノードでは、 SSH はデフォルトで無効になっています。

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ー '$ ｛ token ｝ ' を検索できます "許可します"。ベアラー '$ ｛ token ｝ ' は curl 応答に含まれています。

REST API の **UI** の手順

1. 管理ノードの IP アドレスのあとに「 /mnode/ 」を入力して、管理ノード API サービスの REST API UI にアクセスします。

   ```
   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 を「 m node-client 」として入力します。
   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. 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。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire および Element ソフトウェアのドキュメント"

著作権に関する情報

商標に関する情報