NetApp HCI システムのバージョン 1.9 または 1.9P1 をアップグレードします

HCI

NetApp
December 22, 2023

目次

NetApp HCI システムのバージョン 1.9 または 1.9P1 をアップグレードします

アップグレード手順の概要

導入後は、すべての NetApp HCI ソフトウェアコンポーネントを順番にアップグレードすることで、 NetApp HCI システムを最新の状態に保つことができます。

これらのコンポーネントには、管理サービス、 HealthTools 、 NetApp Hybrid Cloud Control 、 Element ソフトウェア、管理ノード、コンピューティングファームウェア、コンピューティングドライバ、 and the Element Plug-in for vCenter Server.関係 グループ

> 2023年11月以降、署名キー証明書（プライベートおよびパブリック）の有効期限が2023年11月5日に切れたため、NetApp Hybrid Cloud ControlまたはREST APIを使用してコンポーネントのアップグレードを開始することはできません。この問題を解決するには、ナレッジベースの記事に記載されている回避策を参照してください。 "アップグレードパッケージのアップロードエラーが原因でSolidFireとHCIのアップグレードを開始できない"。

。 システムのアップグレード順序 コンテンツでは、 NetApp HCI システムのアップグレードを完了するために必要な作業について説明します。これらの手順は、単独でででではなく、大規模なアップグレードシーケンスの一部として実行することを推奨します。コンポーネントベースのアップグレードまたは更新が必要な場合は、手順の前提条件を参照して、さらに複雑な作業が対処されるようにしてください。

。 vSphere のアップグレード順序 Element Plug-in for vCenter Server のコンテンツでは、 Element Plug-in for vCenter Server を再インストールするために必要な、アップグレード前とアップグレード後の追加の手順について説明します。

必要なもの

- 管理ノード 11.3 以降が実行されていることを確認します。新しいバージョンの管理ノードには、個々のサービスを提供するモジュラアーキテクチャが採用されています。

  > バージョンを確認するには、管理ノードにログインし、ログインバナーに表示される Element のバージョン番号を確認します。11.3 を使用していない場合は、を参照してください "管理ノードをアップグレードします"。

- 管理サービスをバージョン 2.1.326 以上にアップグレードしておきます。

  NetApp Hybrid Cloud Control を使用したアップグレードは、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。

- すべてのノードのシステム時間が同期され、 NTP がストレージクラスタとノードに対して正しく設定されていることを確認しておきます。各ノードには、ノード Web UI （「 https://[IP address 」： 442 ）に DNS ネームサーバを設定する必要があります。時刻のずれに関連する未解決のクラスタ障害はありません。

[sys_upgrade_seq]システムアップグレードシーケンス

NetApp HCI システムをアップグレードするには、次の順序で操作します。

手順

1. "Hybrid Cloud Control から管理サービスを更新します"。

> 管理サービスをバージョン 2.16 以降に更新する場合、管理ノード 11.3 から 11.8 を実行しているときは、管理サービスを更新する前に管理ノード VM の RAM を増やす必要があります。

> Element ソフトウェアをアップグレードする前に、最新の管理サービスバンドルに更新する必要があります。

2. "（オプション）最新の HealthTools にアップグレードします"。

> HealthTools のアップグレードは、実行している管理ノードと Element ソフトウェアが 11.1 以前の場合にのみ必要です。NetApp Hybrid Cloud Control を使用した Element のアップグレードには HealthTools は必要ありません。

3. "ストレージをアップグレードする前に、 Element ストレージの健全性チェックを実行します"。
4. "Element ソフトウェアとストレージファームウェアをアップグレードします"。
5. "（オプション） Element ストレージファームウェアのみをアップグレードします"。

> このタスクは、メジャーリリース以外で新しいストレージファームウェアアップグレードがリリースされたときに実行することができます。

6. "（オプション）管理ノードをアップグレードします"。

> ストレージクラスタ上の Element ソフトウェアをアップグレードするために、管理ノードのオペレーティングシステムをアップグレードする必要がなくなりました。管理ノードのバージョンが 11.3 以降である場合は、 NetApp Hybrid Cloud Control を使用して管理サービスを最新バージョンにアップグレードするだけで Element をアップグレードできます。管理ノードのオペレーティングシステムをアップグレードする理由がほかにもある場合は、セキュリティの修正など、管理ノードのアップグレード手順に従ってください。

7. "Element Plug-in for vCenter Server をアップグレードします"。
8. "コンピューティングノードの健全性チェックは、コンピューティングファームウェアをアップグレードする前に実行します"。
9. "コンピューティングノードのドライバを更新します"。
10. "NetApp Hybrid Cloud Control を使用してコンピューティングノードのファームウェアを更新します" または "Ansible でコンピューティングファームウェアのアップグレードを自動化できます"。

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 のリソースページ"
- "NetApp SolidFire オールフラッシュストレージシステムをアップグレード"

システムのアップグレード手順

管理サービスを更新

管理ノード 11.3 以降をインストールしたら、管理サービスを最新のバンドルバージョンに更新できます。

Element 11.3 以降の管理ノードリリースでは、個々のサービスを提供する新しいモジュラアーキテクチャに基づいて管理ノードの設計が変更されました。これらのモジュラ型サービスは、 NetApp HCI システムの一元管理機能と拡張管理機能を提供します。管理サービスには、システム計測、ロギング、更新のサービス、Element Plug-in for vCenter Server の QoSSIOC サービス、 NetApp Hybrid Cloud Control などがあります。

このタスクについて

- Element ソフトウェアをアップグレードする前に、最新の管理サービスバンドルにアップグレードする必要があります。

> - 管理サービス2.22.7には、リモートプラグインを含むElement Plug-in for vCenter Server 5.0が含まれています。Elementプラグインを使用する場合は、ローカルプラグインのサポートを削除するVMwareの指示に従って、管理サービス2.22.7以降にアップグレードする必要があります。 "詳細はこちら。"。
> - 各サービスバンドルの主要なサービス、新機能、バグ修正、および対処方法について説明した最新の管理サービスリリースノートについては、を参照してください "管理サービスのリリースノート"

必要なもの

管理サービス2.20.69以降では、NetApp Hybrid Cloud ControlのUIまたはAPIを使用して管理サービスをアップグレードする前に、エンドユーザライセンス契約（EULA）に同意して保存する必要があります。

1. Webブラウザで管理ノードのIPアドレスを開きます。

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

2. 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。
3. インターフェイスの右上にある [* Upgrade] を選択します。
4. EULAがポップアップ表示されます。下にスクロールして、[現在および今後のすべての更新を許可する*] を選択し、[保存*]を選択します。

オプションを更新します

管理サービスは、 NetApp Hybrid Cloud Control の UI または管理ノードの REST API を使用して更新できます。

- Hybrid Cloud Control を使用して管理サービスを更新します （推奨方法）
- 管理ノード API を使用して管理サービスを更新する

Hybrid Cloud Control を使用して管理サービスを更新します

NetApp Hybrid Cloud Control を使用してネットアップの管理サービスを更新できます。

管理サービスバンドルは、メジャーリリースに含まれていない機能の強化とインストールに対する修正を提供します。

作業を開始する前に

- 管理ノード 11.3 以降が実行されていることを確認します。
- 管理サービスをバージョン 2.16 以降に更新する場合、管理ノード 11.3 から 11.8 を実行しているときは、管理サービスを更新する前に管理ノード VM の RAM を増やす必要があります。
  a. 管理ノード VM の電源をオフにします。
  b. 管理ノード VM の RAM を 12GB から 24GB RAM に変更します。
  c. 管理ノード VM の電源をオンにします。
- 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。
- 管理サービスをバージョン 2.1.326 以上にアップグレードしておきます。NetApp Hybrid Cloud Control のアップグレードは、それよりも前のサービスバンドルでは利用できません。

> 各サービスバンドルバージョンで使用可能なサービスのリストについては、を参照してください "管理サービスリリースノート"。

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。

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

2. 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。
3. インターフェイスの右上にある [* Upgrade] を選択します。
4. アップグレードページで、 * 管理サービス * タブを選択します。
5. ページの指示に従って、管理サービスのアップグレードパッケージをダウンロードし、コンピュータに保存します。
6. 「 * 参照 * 」を選択して、保存したパッケージを検索し、アップロードします。

   パッケージをアップロードすると、アップグレードが自動的に開始されます。

   アップグレードの開始後は、このページにアップグレードのステータスが表示されます。アップグレードの実行中に NetApp Hybrid Cloud Control との接続が失われ、ログインし直さないとアップグレードの結果が表示されないことがあります。

管理ノード API を使用して管理サービスを更新する

管理サービスの更新は、 NetApp Hybrid Cloud Control から実行することを推奨します。ただし、 REST API を使用して、管理サービスのサービスバンドルの更新を管理ノードに手動でアップロード、展開、および導入

することができます。管理ノード用の REST API UI から各コマンドを実行できます。

作業を開始する前に

- NetApp Element ソフトウェア管理ノード 11.3 以降を導入しておきます。
- 管理サービスをバージョン 2.16 以降に更新する場合、管理ノード 11.3 から 11.8 を実行しているときは、管理サービスを更新する前に管理ノード VM の RAM を増やす必要があります。
  a. 管理ノード VM の電源をオフにします。
  b. 管理ノード VM の RAM を 12GB から 24GB RAM に変更します。
  c. 管理ノード VM の電源をオンにします。
- 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。
- 管理サービスをバージョン 2.1.326 以上にアップグレードしておきます。NetApp Hybrid Cloud Control のアップグレードは、それよりも前のサービスバンドルでは利用できません。

> 各サービスバンドルバージョンで使用可能なサービスのリストについては、を参照してください "管理サービスリリースノート"。

手順

1. 管理ノードで REST API UI を開きます 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. 値がまだ入力されていない場合は、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. 管理ノードにサービスバンドルをアップロードして展開するには 'put/services/upload' コマンドを使用します
4. 管理ノードに管理サービスを配備します :PUT /services/deploy
5. 更新のステータスを監視します。「 get/services/update/status 」

   更新が成功すると、次の例のような結果が返されます。

```
{
"current_version": "2.10.29",
"details": "Updated to version 2.17.52",
"status": "success"
}
```

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 のリソースページ"

最新の **HealthTools** にアップグレードします

Element ストレージのアップグレードを 11.1 以前から開始する前に、 HealthTools スイートをアップグレードする必要があります。HealthTools のアップグレードは、実行している管理ノードと Element ソフトウェアが 11.1 以前の場合にのみ必要です。には HealthTools は必要ありません "NetApp Hybrid Cloud Control を使用して Element をアップグレードする"。

> Element ソフトウェア 12.3.2 は、 NetApp HealthTools を使用してにアップグレードできる最終バージョンです。Element ソフトウェア 11.3 以降を実行している場合は、 NetApp Hybrid Cloud Control を使用して Element ソフトウェアをアップグレードする必要があります。Element バージョン 11.1 以前は、 NetApp HealthTools を使用してアップグレードできます。

必要なもの

- 実行されている管理ノードは 11.0 、 11.1 、またはそれ以降です。
- 管理サービスをバージョン 2.1.326 以上にアップグレードしておきます。

  NetApp Hybrid Cloud Control のアップグレードは、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。

- 最新バージョンのをダウンロードしておきます "HealthTools" インストールファイルを管理ノードにコピーしておきます。

  > ローカルにインストールされている HealthTools のバージョンを確認するには 'sfcupdate-healthtools -v コマンドを実行します

- ダークサイトで HealthTools を使用するには、次の追加手順を実行する必要があります。
  - をダウンロードします "JSON ファイル" 管理ノードではないコンピュータのネットアップサポートサイトから、「 metadats.json 」に名前を変更します。
  - 管理ノードをダークサイトで起動して実行します。

このタスクについて

HealthTools スイートのコマンドを実行するには権限を昇格する必要があります。コマンドの先頭に「 sudo 」を付けるか、ユーザを root 権限に昇格させます。

> 使用する HealthTools のバージョンが、以下の入力例と応答よりも新しい場合があります。

手順

1. 「 sfcupdate-healthtools <path to install file>` 」コマンドを実行して、新しい HealthTools ソフトウェアをインストールします。

   入力例：

   ```
   sfupdate-healthtools /tmp/solidfire-healthtools-2020.03.01.09.tgz
   ```

回答例：

```
Checking key signature for file /tmp/solidfirehealthtools-
2020.03.01.09/components.tgz
installing command sfupdate-healthtools
Restarting on version 2020.03.01.09
sfupdate-healthtools /sf/bin/sfupdate-healthtools -r 2020.03.01.09
installing command sfupgradecheck
installing command sfinstall
installing command sfresetupgrade
```

2. 「 fupdate-healthtools -v 」コマンドを実行して、インストールされたバージョンがアップグレードされたことを確認します。

   回答例：

```
Currently installed version of HealthTools:
2020.03.01.09
```

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 のリソースページ"

ストレージをアップグレードする前に、 **Element** ストレージの健全性チェックを実行します

Element ストレージをアップグレードする前に健全性チェックを実行して、クラスタ内のすべてのストレージノードで次回の Element ストレージアップグレードの準備ができていることを確認する必要があります。

必要なもの

- 管理サービス：最新の管理サービスバンドル（2.10.27以降）に更新しました。

> Element ソフトウェアをアップグレードする前に、最新の管理サービスバンドルにアップグレードする必要があります。

- 管理ノード：管理ノード11.3以降を実行していることを確認します。
- * Elementソフトウェア*：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る必要があります。
- エンドユーザライセンス契約（**EULA**）：管理サービス2.20.69以降では、NetApp Hybrid Cloud ControlのUIまたはAPIを使用してElementストレージの健全性チェックを実行する前に、EULAに同意して保存する必要があります。
  a. Webブラウザで管理ノードのIPアドレスを開きます。

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

b. 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。

c. インターフェイスの右上にある [* Upgrade] を選択します。

d. EULAがポップアップ表示されます。下にスクロールして、[現在および今後のすべての更新を許可する*]を選択し、[保存*]を選択します。

健全性チェックのオプション

健全性チェックは、 NetApp Hybrid Cloud Control （ HCC ） UI 、 HCC API 、または HealthTools スイートを使用して実行できます。

- NetApp Hybrid Cloud Control を使用して Element ストレージの健全性を実行します ストレージをアップグレードする前にチェックします （推奨方法）
- API を使用して、実行前に Element ストレージの健全性チェックを実行 ストレージをアップグレードする
- 前に HealthTools を使用して Element ストレージの健全性チェックを実行してください ストレージをアップグレードする

サービスで実行されるストレージ健全性チェックの詳細についても確認できます。

- [サービスによるストレージの健全性チェック]

NetApp Hybrid Cloud Control を使用して **Element** ストレージの健全性を実行します ストレージをアップグレードする前にチェックします

NetApp Hybrid Cloud Control （ HCC ）を使用して、ストレージクラスタをアップグレードする準備が完了していることを確認できます。

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。

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

2. 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。
3. インターフェイスの右上にある [* Upgrade] を選択します。
4. [アップグレード * （ Upgrades * ）] ページで、 [* ストレージ * （ Storage * ）] タブを選択します。
5. 健全性チェックを選択します アップグレードの準備状況を確認するクラスタ
6. [* ストレージヘルスチェック *] ページで、 [* ヘルスチェックの実行 *] を選択します。
7. 問題がある場合は、次の手順を実行します。

   a. 各問題について記載されている特定の技術情報アーティクルに移動するか、指定された対処方法を実行します。

b. KB を指定した場合は、関連する技術情報アーティクルに記載されているプロセスを完了します。

c. クラスタの問題を解決したら、「 * Re-Run Health Check * 」を選択します。

健全性チェックの完了後、エラーは発生しません。ストレージクラスタをアップグレードする準備は完了しています。ストレージノードのアップグレードを参照してください "手順" 続行してください。

API を使用して、実行前に **Element** ストレージの健全性チェックを実行 ストレージをアップグレードする

REST API を使用して、ストレージクラスタをアップグレードする準備が完了していることを確認できます。健全性チェックでは、保留中のノード、ディスクスペースの問題、クラスタ障害など、アップグレードが必要な障害がないことを確認します。

手順

1. ストレージクラスタ ID を確認します。

   a. 管理ノードで管理ノード 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. 値がまだ入力されていない場合は、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. 承認ウィンドウを閉じます。

   c. REST API UI から 'get/assets' 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. 応答から ' アップグレードの準備状況を確認するクラスタのストレージセクションから 'id' をコピーします

   このセクションの「親」の値は、ストレージクラスタの ID ではなく、管理ノードの ID であるため使用しないでください。

```
"config": {},
"credentialid": "12bbb2b2-f1be-123b-1234-12c3d4bc123e",
"host_name": "SF_DEMO",
"id": "12cc3a45-e6e7-8d91-a2bb-0bdb3456b789",
"ip": "10.123.12.12",
"parent": "d123ec42-456e-8912-ad3e-4bd56f4a789a",
"sshcredentialid": null,
"ssl_certificate": null
```

2. ストレージクラスタで健全性チェックを実行します。

   a. 管理ノードでストレージ REST API UI を開きます。

   ```
   https://<ManagementNodeIP>/storage/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. 値がまだ入力されていない場合は、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. 承認ウィンドウを閉じます。

   c. [* POST/Health-Checks （ POST / ヘルスチェック）] を選択します。

   d. [* 試してみてください *] を選択します。

   e. パラメータフィールドに、手順 1 で取得したストレージクラスタ ID を入力します。

   ```
   {
     "config": {},
     "storageId": "123a45b6-1a2b-12a3-1234-1a2b34c567d8"
   }
   ```

   f. 指定したストレージクラスタでヘルスチェックを実行するには、 * Execute * を選択します。

   応答は ' ステータスを初期化中と表示する必要があります

```
{
  "_links": {
    "collection": "https://10.117.149.231/storage/1/health-checks",
    "log": "https://10.117.149.231/storage/1/health-checks/358f073f-
896e-4751-ab7b-ccbb5f61f9fc/log",
    "self": "https://10.117.149.231/storage/1/health-checks/358f073f-
896e-4751-ab7b-ccbb5f61f9fc"
  },
  "config": {},
  "dateCompleted": null,
  "dateCreated": "2020-02-21T22:11:15.476937+00:00",
  "healthCheckId": "358f073f-896e-4751-ab7b-ccbb5f61f9fc",
  "state": "initializing",
  "status": null,
  "storageId": "c6d124b2-396a-4417-8a47-df10d647f4ab",
  "taskId": "73f4df64-bda5-42c1-9074-b4e7843dbb77"
}
```

a. 応答の一部である「 healthCheckID 」をコピーします。

3. 健全性チェックの結果を確認します。

   a. [* 一時的なもの / 正常性チェックの一時的なもの / ｛ healthCheckId ｝ *] を選択します。

   b. [* 試してみてください *] を選択します。

   c. パラメータフィールドにヘルスチェック ID を入力します。

   d. [* Execute] を選択します。

   e. 応答の本文の一番下までスクロールします。

      すべての健全性チェックが成功した場合の出力例を次に示します。

```
"message": "All checks completed successfully.",
"percent": 100,
"timestamp": "2020-03-06T00:03:16.321621Z"
```

4. 「メッセージ」が「クラスタの正常性」に問題があることを示している場合は、次の手順を実行します。

   a. [* Get Singges/health-checksSries/ ｛ healthCheckId}/log*] を選択します

   b. [* 試してみてください *] を選択します。

   c. パラメータフィールドにヘルスチェック ID を入力します。

   d. [* Execute] を選択します。

   e. 特定のエラーを確認し、関連する KB 記事のリンクを取得します。

   f. 各問題について記載されている特定の技術情報アーティクルに移動するか、指定された対処方法を実行します。

   g. KB を指定した場合は、関連する技術情報アーティクルに記載されているプロセスを完了します。

   h. クラスタの問題を解決したら、 * Get Sedges/health-checksRunges/ ｛ healthCheckId ｝ /log * を再度実行します。

前に **HealthTools** を使用して **Element** ストレージの健全性チェックを実行してください ストレージをアップグレードする

「 fupgradecheck 」コマンドを使用して、ストレージクラスタをアップグレードする準備が完了していることを確認できます。このコマンドは、保留中のノード、ディスクスペース、クラスタ障害などの情報を検証します。

管理ノードが外部に接続されていないダークサイトにある場合、アップグレードの準備状況を確認するには、ダウンロードした「 metadats.json 」ファイルが必要です "HealthTools のアップグレード" を実行してください。

このタスクについて

ここでは、次のいずれかの結果をもたらすアップグレードチェックに対処する方法について説明します。

- 「 fupgradecheck 」コマンドを実行すると、正常に実行されます。クラスタをアップグレードする準備は完了しています。

- 「アップグレードチェック」ツールでのチェックが失敗し、エラーメッセージが表示される。クラスタをアップグレードする準備が完了しておらず、追加の手順が必要です。
- アップグレードチェックが失敗し、 HealthTools が最新バージョンでないというエラーメッセージが表示される。
- 管理ノードがダークサイトにあるため、アップグレードチェックが失敗する。

手順

1. 「 fupgradecheck 」コマンドを実行します。

```
sfupgradecheck -u <cluster-user-name> MVIP
```

> パスワードに特殊文字が含まれる場合は、各特殊文字の前にバックスラッシュ（「 \ 」）を追加します。たとえば、「 mypass ！ @1 」は「 'm ypass\ ！ \@1 」と入力する必要があります。

サンプルの入力コマンド。エラーは表示されず、アップグレードの準備ができている場合の出力例です。

```
sfupgradecheck -u admin 10.117.78.244
```

```
check_pending_nodes:
Test Description: Verify no pending nodes in cluster
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltOQAQ/pendingnodes
check_cluster_faults:
Test Description: Report any cluster faults
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/
SolidFire-Disk-space-error
check_mnode_connectivity:
Test Description: Verify storage nodes can communicate with management
node
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltYQAQ/mNodeconnecti
vity
check_files:
Test Description: Verify options file exists
Passed node IDs: 1, 2, 3
check_cores:
Test Description: Verify no core or dump files exists
Passed node IDs: 1, 2, 3
check_upload_speed:
Test Description: Measure the upload speed between the storage node and
the
management node
Node ID: 1 Upload speed: 90063.90 KBs/sec
Node ID: 3 Upload speed: 106511.44 KBs/sec
Node ID: 2 Upload speed: 85038.75 KBs/sec
```

2. エラーが発生した場合は、追加の操作が必要です。詳細については、次のサブセクションを参照してください。

クラスタをアップグレードする準備が完了していません

いずれかの健全性チェックに関連するエラーメッセージが表示された場合は、次の手順を実行します。

1. 「 fupgradecheck 」エラーメッセージを確認します。

   回答例：

```
The following tests failed:
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Severity: ERROR
Failed node IDs: 2
Remedy: Remove unneeded files from root drive
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/SolidFire-
Disk-space-error
check_pending_nodes:
Test Description: Verify no pending nodes in cluster
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltOQAQ/pendingnodes
check_cluster_faults:
Test Description: Report any cluster faults
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Passed node IDs: 1, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/SolidFire-
Disk-space-error
check_mnode_connectivity:
Test Description: Verify storage nodes can communicate with management
node
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltYQAQ/mNodeconnectivi
ty
check_files:
Test Description: Verify options file exists
Passed node IDs: 1, 2, 3
check_cores:
Test Description: Verify no core or dump files exists
Passed node IDs: 1, 2, 3
check_upload_speed:
Test Description: Measure the upload speed between the storage node and
the management node
Node ID: 1 Upload speed: 86518.82 KBs/sec
Node ID: 3 Upload speed: 84112.79 KBs/sec
Node ID: 2 Upload speed: 93498.94 KBs/sec
```

この例では、ノード 1 のディスクスペースが少なくなっています。詳細については、を参照してください "ナレッジベース" （ KB ）エラーメッセージに記載されている記事。

HealthTools が最新バージョンではありません

HealthTools が最新バージョンではないことを示すエラーメッセージが表示された場合は、次の手順に従います。

1. アップグレードチェックが失敗したことをエラーメッセージで確認します。

   回答例：

   ```
   sfupgradecheck failed: HealthTools is out of date:
   installed version: 2018.02.01.200
   latest version: 2020.03.01.09.
   The latest version of the HealthTools can be downloaded from:
   https://mysupport.netapp.com/NOW/cgi-bin/software/
   Or rerun with the -n option
   ```

2. 応答に記載されている手順に従います。

管理ノードがダークサイトにあります

1. アップグレードチェックが失敗したことをメッセージで確認します。

   回答例：

   ```
   sfupgradecheck failed: Unable to verify latest available version of
   healthtools.
   ```

2. をダウンロードします "JSON ファイル" 管理ノードではないコンピュータのネットアップサポートサイトから、「 metadats.json 」に名前を変更します。
3. 次のコマンドを実行します。

   ```
   sfupgradecheck -l --metadata=<path-to-metadata-json>
   ```

4. 詳細については、「追加」を参照してください "HealthTools のアップグレード" ダークサイトの情報。
5. 次のコマンドを実行して、 HealthTools スイートが最新バージョンであることを確認します。

   ```
   sfupgradecheck -u <cluster-user-name> -p <cluster-password> MVIP
   ```

サービスによるストレージの健全性チェック

ストレージの健全性チェックでは、クラスタごとに以下のチェックが行われます。

[名前（ **Name** ）] を	ノード / クラスタ	説明
check_async 結果	クラスタ	データベースの非同期結果の数がしきい値を下回っていることを検証します。
check_cluster_faults	クラスタ	（ Element ソースで定義された）アップグレードがブロックされているクラスタエラーがないことを確認します。
check_upload_speed	ノード	ストレージノードと管理ノードの間のアップロード速度を測定します。
connection_speed_check	ノード	ノードがアップグレードパッケージを提供する管理ノードに接続されていることを確認し、接続速度を推定します。
コアをチェックします	ノード	ノード上のカーネルクラッシュダンプファイルとコアファイルをチェックします。直近の期間（しきい値 7 日）にクラッシュが発生した場合、チェックは失敗します。
check_root_disk_space を選択します	ノード	ルートファイルシステムにアップグレードを実行するための十分な空きスペースがあることを確認します。
var_log_disk_space を確認します	ノード	/var/log の空き領域が、空きしきい値のパーセンテージを満たしていることを確認します。サポートされていない場合は、しきい値を下回るために、古いログがローテーションされてパージされます。十分な空きスペースの作成に失敗した場合、チェックは失敗します。
check_pending_nodes	クラスタ	クラスタに保留状態のノードがないことを確認します。

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"
- "NetApp HCI のリソースページ"

Element ソフトウェアをアップグレードします

NetApp Element ソフトウェアをアップグレードするには、 NetApp Hybrid Cloud Control UI 、 REST API 、または HealthTools ツールスイートを使用します。Element ソフトウェアのアップグレードの実行中は、ノードの追加と削除、ドライブの追加と削除、イニシエータ、ボリュームアクセスグループ、仮想ネットワークに関連するコマンドなど、一部の処理は実行できません。

必要なもの

- * admin 権限 * ：アップグレードを実行する権限がストレージクラスタ管理者に付与されています。
- * 有効なアップグレードパス * ：アップグレード先の Element バージョンのアップグレードパス情報を確認し、アップグレードパスが有効であることを確認しておきます。https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Element_Software/What_is_the_upgrade_matrix_for_storage_clusters_running_NetApp_Element_software%3F["ネットアップの技術情報： NetApp Element ソフトウェアを実行するストレージクラスタのアップグレードマトリックス"^]
- * システム時間の同期 * ：すべてのノードのシステム時間が同期されており、 NTP がストレージクラスタとノードに対して正しく設定されていることを確認しておきます。各ノードには、ノード Web UI （「 https://[IP address 」： 442 ）に DNS ネームサーバを設定する必要があります。時刻のずれに関連する未解決のクラスタ障害はありません。
- * システムポート * ： NetApp Hybrid Cloud Control をアップグレードに使用している場合は、必要なポートが開いていることを確認しておきます。を参照してください "ネットワークポート" を参照してください。
- * 管理ノード * ： NetApp Hybrid Cloud Control の UI および API では、環境内の管理ノードはバージョン 11.3 を実行しています。
- * 管理サービス * ：管理サービスバンドルを最新バージョンに更新しました。

> Element ソフトウェアをバージョン 12.3.x にアップグレードする前に、最新の管理サービスバンドルにアップグレードする必要がありますElement ソフトウェアをバージョン 12.3.x に更新する場合は、管理サービス 2.14.60 以降が必要です。

- * クラスタの健全性 * ：クラスタをアップグレードする準備が完了していることを確認しました。を参照してください "ストレージをアップグレードする前に、 Element ストレージの健全性チェックを実行します"。
- * H610S ノードの BMC を更新 * ： H610S ノードの BMC バージョンをアップグレードしました。を参照してください "リリースノートおよびアップグレード手順"。
- エンドユーザライセンス契約（**EULA**）：管理サービス2.20.69以降では、NetApp Hybrid Cloud Control UIまたはAPIを使用してElementソフトウェアをアップグレードする前に、EULAに同意して保存する必要があります。
  a. Webブラウザで管理ノードのIPアドレスを開きます。

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

  b. 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。
  c. インターフェイスの右上にある [* Upgrade] を選択します。
  d. EULAがポップアップ表示されます。下にスクロールして、[現在および今後のすべての更新を許可する*]を選択し、[保存*]を選択します。

アップグレードオプション

次のいずれかの Element ソフトウェアアップグレードオプションを選択します。

- NetApp Hybrid Cloud Control UI を使用して Element ストレージをアップグレードします

- NetApp Hybrid Cloud Control API を使用して Element ストレージをアップグレードします
- HealthTools を使用して接続されているサイトで Element ソフトウェアをアップグレードします
- HealthTools を使用してダークサイトで Element ソフトウェアをアップグレードします

> H610S シリーズノードを Element 12.3.x にアップグレードする場合、ノードで 11.8 よりも前のバージョンの Element が実行されているときは、追加のアップグレード手順（）を実行する必要がありますフェーズ 2.）をクリックします。Element 11.8 以降を実行している場合は、追加のアップグレード手順（フェーズ 2 ）は必要ありません。

NetApp Hybrid Cloud Control UI を使用して **Element** ストレージをアップグレードします

NetApp Hybrid Cloud Control の UI を使用して、ストレージクラスタをアップグレードできます。

> NetApp Hybrid Cloud Control を使用してストレージクラスタをアップグレードする際の潜在的な問題とその対処方法については、を参照してください "こちらの技術情報アーティクル"。

> H610S 以外のプラットフォームでは、ノードあたりのアップグレードプロセスに約 30 分かかります。

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。

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

2. 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。
3. インターフェイスの右上にある [* Upgrade] を選択します。
4. [* Upgrades] ページで、 [* Storage] を選択します。

   [* ストレージ *] タブには、インストールの一部であるストレージクラスタが一覧表示されます。NetApp Hybrid Cloud Control からクラスタにアクセスできない場合は、 * Upgrades * ページに表示されません。

5. 次のオプションを選択し、クラスタに該当する一連の手順を実行します。

オプション	手順
Element 11.8以降を実行しているすべてのクラスタ	a. [* Browse] を選択して、ダウンロードしたアップグレード・パッケージをアップロードします。 b. アップロードが完了するまで待ちます。進捗バーにアップロードのステータスが表示されます。 ブラウザウィンドウから別の場所に移動すると、ファイルのアップロードが失われます。 ファイルのアップロードと検証が完了すると、画面にメッセージが表示されます。検証には数分かかることがあります。この段階でブラウザウィンドウから移動しても、ファイルのアップロードは維持されます。 c. [* アップグレードの開始 *] を選択します。 アップグレード中は、アップグレードステータス * が変更され、プロセスのステータスが反映されます。また、アップグレードの一時停止など、実行する操作に応じて変更が加えられたか、またはアップグレードでエラーが返された場合も変更されます。を参照してください [アップグレードステータスが変わります]。 アップグレードの実行中は、ページを離れてあとから表示し、進捗状況の監視を続行できます。クラスタの行が折りたたまれている場合、ページではステータスと現在のバージョンは動的に更新されません。表を更新するには、クラスタの行を展開する必要があります。また、ページを更新することもできます。 アップグレードの完了後にログをダウンロードできます。

オプション	手順
Element 11.8 より前のバージョンを実行している H610S クラスタをアップグレードしています。	a. アップグレードするクラスタの横にあるドロップダウン矢印を選択し、アップグレード可能なバージョンから選択します。 b. [* アップグレードの開始 *] を選択します。アップグレードが完了すると、プロセスのフェーズ 2 を実行するよう求める画面が表示されます。 c. で必要な追加手順（フェーズ 2 ）を実行します "こちらの技術情報アーティクル"をクリックし、フェーズ 2 が完了したことを UI で確認します。 アップグレードの完了後にログをダウンロードできます。アップグレードステータスのさまざまな変更については、を参照してください [アップグレードステータスが変わります]。

アップグレードステータスが変わります

アップグレードプロセスの実行前、実行中、実行後に、 UI の * アップグレードステータス * 列に表示されるさまざまな状態を以下に示します。

アップグレードの状態	説明
最新	クラスタが最新の Element バージョンにアップグレードされました。
使用可能なバージョン	Element / ストレージファームウェアの新しいバージョンをアップグレードできます。
実行中です	アップグレードを実行中です。進行状況バーにアップグレードステータスが表示されます。画面にはノードレベルの障害も表示され、アップグレードの進行に伴いクラスタ内の各ノードのノード ID も表示されます。各ノードのステータスは、 Element UI または NetApp Element Plug-in for vCenter Server UI を使用して監視できます。
Pausing をアップグレードします	アップグレードを一時停止することもできます。アップグレードプロセスの状態によっては、一時停止処理が成功するか失敗するかが決まります。一時停止処理の確認を求める UI プロンプトが表示されます。アップグレードを一時停止する前にクラスタが安全な場所にあることを確認するには、アップグレード処理が完全に一時停止されるまでに最大 2 時間かかることがあります。アップグレードを再開するには、 * Resume * （続行）を選択します。
一時停止中	アップグレードを一時停止した。[* Resume （続行）] を選択して、プロセスを再開します。

アップグレードの状態	説明
エラー	アップグレード中にエラーが発生しました。エラーログをダウンロードして、ネットアップサポートに送信できます。エラーを解決したら、ページに戻って * Resume *（続行）を選択します。アップグレードを再開すると、システムが健全性チェックを実行してアップグレードの現在の状態を確認している間、進捗状況バーが数分間後方に移動します。
フォローアップを完了します	H610S ノードを 11.8 より前のバージョンからアップグレードした場合のみアップグレードプロセスのフェーズ 1 が完了すると、アップグレードのフェーズ 2 を実行するように求められます（を参照） "こちらの技術情報アーティクル"）。フェーズ 2 を完了し、完了したことを確認すると、ステータスが「 * 最新 * 」に変わります。

NetApp Hybrid Cloud Control API を使用して **Element** ストレージをアップグレードします

API を使用して、クラスタ内のストレージノードを最新バージョンの Element ソフトウェアにアップグレードできます。API の実行には、任意の自動化ツールを使用できます。ここで説明する API ワークフローでは、例として管理ノードで使用可能な REST API UI を使用します。

手順

1. 管理ノードからアクセス可能なデバイスにストレージアップグレードパッケージをダウンロードします。NetApp HCI ソフトウェアにアクセスします "ページをダウンロードします" して最新のストレージノードのイメージをダウンロードしてください。
2. ストレージアップグレードパッケージを管理ノードにアップロードします。
   a. 管理ノードで管理ノード REST API UI を開きます。

      ```
      https://<ManagementNodeIP>/package-repository/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. 承認ウィンドウを閉じます。
   c. REST API UI から * POST/packages * を選択します。
   d. [* 試してみてください *] を選択します。
   e. [* Browse] を選択して、アップグレード・パッケージを選択します。
   f. 「 * Execute * 」を選択してアップロードを開始します。
   g. 応答から ' 後の手順で使用するためにパッケージ ID (`id"') をコピーして保存します
3. アップロードのステータスを確認します。

a. REST API UI から、 * GEGET 処理対象 / パッケージ間の一時的なグループ / ｛ id ｝ 一時的なグループ / ステータス * を選択します。
b. [* 試してみてください *] を選択します。
c. 前の手順でコピーしたパッケージ ID を * id * で入力します。
d. ステータス要求を開始するには、 * Execute * を選択します。

   応答が完了すると、「アクセス」として表示されます。

4. ストレージクラスタ ID を確認します。
   a. 管理ノードで管理ノード 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. 承認ウィンドウを閉じます。
   c. REST API UI から、 * GET / Installations * 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. 応答から、インストールアセット ID （「 id 」）をコピーします。
   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 ' 後の手順で使用できるようにアップグレードするクラスタのストレージ・クラスタ ID （ ID ）をコピーして保存します
5. ストレージのアップグレードを実行します。
   a. 管理ノードでストレージ REST API UI を開きます。

```
https://<ManagementNodeIP>/storage/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. 承認ウィンドウを閉じます。

c. [**POST/upgrade**] を選択します。

d. [* 試してみてください *] を選択します。

e. パラメータフィールドにアップグレードパッケージ ID を入力します。

f. パラメータフィールドにストレージクラスタ ID を入力します。

ペイロードは次の例のようになります。

```
{
  "config": {},
  "packageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4",
  "storageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4"
}
```

g. アップグレードを開始するには、 * Execute * を選択します。

応答は状態を「 initializing 」と示します。

```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1",
    "log": https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1/log
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055`-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
      "string"
    ],
    "message": "string",
    "nodeDetails": [
      {
        "message": "string",
        "step": "NodePreStart",
        "nodeID": 0,
        "numAttempt": 0
      }
    ],
```

```
    "percent": 0,
    "step": "ClusterPreStart",
    "timestamp": "2020-04-21T22:10:57.057Z",
    "failedHealthChecks": [
      {
        "checkID": 0,
        "name": "string",
        "displayName": "string",
        "passed": true,
        "kb": "string",
        "description": "string",
        "remedy": "string",
        "severity": "string",
        "data": {},
        "nodeID": 0
      }
    ]
  },
  "taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",
  "dateCompleted": "2020-04-21T22:10:57.057Z",
  "dateCreated": "2020-04-21T22:10:57.057Z"
}
```


a. 応答の一部であるアップグレード ID （「 upgradeId 」）をコピーします。

6. アップグレードの進捗状況と結果を確認します。

a. Get Sebring/upgrades/｛upgradeId｝ * を選択します。

b. [* 試してみてください *] を選択します。

c. アップグレード ID は、前の手順のアップグレード ID として * upgradeId * と入力します。

d. [* Execute] を選択します。

e. アップグレード中に問題または特別な要件が発生した場合は、次のいずれかを実行します。

オプション	手順
応答の本文に「 failedHealthCheckks 」というメッセージが表示されているため、クラスタのヘルスの問題を修正する必要があります。	i. 各問題について記載されている特定の技術情報アーティクルに移動するか、指定された対処方法を実行します。 ii. KB を指定した場合は、関連する技術情報アーティクルに記載されているプロセスを完了します。 iii. クラスタの問題を解決したら、必要に応じて再認証し、 * PUT 処理の際に必要な数 / アップグレード / ｛ upgradeId ｝ * を選択します。 iv. [* 試してみてください *] を選択します。 v. アップグレード ID は、前の手順のアップグレード ID として * upgradeId * と入力します。 vi. リクエスト本文に「 action 」 : 「 resume 」と入力します。 `{ "action": "resume" }` vii. [* Execute] を選択します。
メンテナンス時間が終了しているか別の理由で、アップグレードを一時停止する必要があります。	i. 必要に応じて再認証し、 * PUT に成功 / アップグレード / ｛ upgradeId ｝ * を選択します。 ii. [* 試してみてください *] を選択します。 iii. アップグレード ID は、前の手順のアップグレード ID として * upgradeId * と入力します。 iv. リクエスト本文に「 action 」 : 「 pause 」と入力します。 `{ "action": "pause" }` v. [* Execute] を選択します。

オプション	手順
11.8 より前のバージョンの Element を実行している H610S クラスタをアップグレードする場合は、応答の本文に状態「 finishedNeedsAck 」が表示されます。H610S ストレージノードごとに、追加のアップグレード手順（フェーズ 2 ）を実行する必要があります。	i. を参照してください [Upgrading H610S storage nodes to Element 12.3.x or later (phase 2)] をクリックし、各ノードでプロセスを完了します。 ii. 必要に応じて再認証し、 * PUT に成功 / アップグレード / ｛ upgradeId ｝ * を選択します。 iii. [* 試してみてください *] を選択します。 iv. アップグレード ID は、前の手順のアップグレード ID として * upgradeId * と入力します。 v. リクエスト本文に「 action 」：「 acknowledge 」と入力します。 `{ "action": "acknowledge" }` vi. [* Execute] を選択します。

f. 必要に応じて、処理が完了するまで * Get Theple/upgrades/ ｛ upgradeId ｝ * API を複数回実行します。

   アップグレード中、エラーが発生しなかった場合、「ステータス」は「実行中」を示します。各ノードがアップグレードされると 'tep' の値が NodeFinished に変わります

アップグレードが正常に終了したのは 'percent` の値が '100' で 'tate' が 'finished' である場合です

NetApp Hybrid Cloud を使用してアップグレードに失敗した場合の動作 制御

アップグレード中にドライブまたはノードで障害が発生した場合は、 Element UI にクラスタエラーが表示されます。アップグレードプロセスは次のノードに進まず、クラスタの障害が解決するまで待機します。UI の進捗状況バーには、アップグレードがクラスタの障害の解決を待機していることが表示されます。アップグレードはクラスタが正常に完了するまで待機するため、この段階で UI で * Pause * を選択することはできません。障害の調査に役立てるには、ネットアップサポートに問い合わせる必要があります。

NetApp Hybrid Cloud Control には 3 時間の待機時間があらかじめ設定されています。この時間内に、次のいずれかの状況が発生する可能性があります。

- クラスタの障害は 3 時間以内に解決され、アップグレードが再開されます。このシナリオでは対処は必要ありません。
- 問題は 3 時間後も解消されず、アップグレードのステータスが「 Error 」（エラー）と赤のバナーを表示します。問題が解決したら、「 * Resume 」（続行）を選択してアップグレードを再開できます。
- 3 時間以内に対処するために、アップグレードを一時的に中止する必要があることがネットアップサポートによって確認されました。サポートは API を使用してアップグレードを中止します。

ノードの更新中にクラスタのアップグレードを中止すると、そのノードからドライブが強制的に削除されることがあります。ドライブが強制的に削除された場合、ネットアップサポートに依頼して手動でドライブを元に戻す処理がアップグレード時に必要になります。ノードでファームウェアの更新や更新後の同期処理に時間がかかる可能性があります。アップグレードが停止していると思われる場合は、ネットアップサポートにお問い合わせください。

HealthTools を使用して接続されているサイトで **Element** ソフトウェアをアップグレードします

手順

1. ストレージアップグレードパッケージをダウンロードします。 NetApp HCI ソフトウェアにアクセスします "ページをダウンロードします" をクリックし、管理ノードではないデバイスに最新のストレージノードイメージをダウンロードします。

   Element ストレージソフトウェアをアップグレードするには、最新バージョンの HealthTools が必要です。

2. ISO ファイルを、 /tmp などのアクセス可能な場所にある管理ノードにコピーします。

   ISO ファイルをアップロードする際には、ファイル名が変更されないようにしてください。変更されていると以降の手順が失敗します。

3. * オプション * ：アップグレードの前に、管理ノードからクラスタノードに ISO をダウンロードします。

   この手順は、ストレージノードに ISO を事前にステージングし、内部チェックを実行してクラスタがアップグレードに適した状態であることを確認することで、アップグレード時間を短縮します。この処理を実行しても、クラスタが「アップグレード」モードになることも、クラスタ処理が制限されることもありません。

   ```
   sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO> --stage
   ```

   コマンドラインからパスワードを省略して 'fsinstall' が情報を入力するようにしますパスワードに特殊文字が含まれる場合は、各特殊文字の前にバックスラッシュ（「 \ 」）を追加します。たとえば、「 mypass ！ @1 」は「 'm ypass\ ！ \@1 」と入力する必要があります。

   - 例 * 次のサンプル入力を参照してください。

     ```
     sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfisodium-
     11.0.0.345.iso --stage
     ```

     サンプルの出力は 'fsinstall が 'fsinstall' の新しいバージョンが利用可能かどうかを確認しようとすることを示しています

```
sfinstall 10.117.0.244 -u admin
/tmp/solidfire-rtfisodium-11.0.0.345.iso 2018-10-01 16:52:15:
Newer version of sfinstall available.
This version: 2018.09.01.130, latest version: 2018.06.05.901.
The latest version of the HealthTools can be downloaded from:
https:// mysupport.netapp.com/NOW/cgi-bin/software/
or rerun with --skip-version-check
```

以下は、事前ステージング処理に成功した場合の出力例です。

> ステージングが完了すると、アップグレードイベントの後に「 Storage Node Upgrade Staging Successful 」というメッセージが表示されます。

```
flabv0004 ~ # sfinstall -u admin
10.117.0.87 solidfire-rtfi-sodium-patch3-11.3.0.14171.iso --stage
2019-04-03 13:19:58: sfinstall Release Version: 2019.01.01.49
Management Node Platform:
Ember Revision: 26b042c3e15a Build date: 2019-03-12 18:45
2019-04-03 13:19:58: Checking connectivity to MVIP 10.117.0.87
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.86
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.87
...
2019-04-03 13:19:58: Successfully connected to cluster and all nodes
...
2019-04-03 13:20:00: Do you want to continue? ['Yes', 'No']: Yes
...
2019-04-03 13:20:55: Staging install pack on cluster nodes
2019-04-03 13:20:55: newVersion: 11.3.0.14171
2019-04-03 13:21:01: nodeToStage: nlabp2814, nlabp2815, nlabp2816,
nlabp2813
2019-04-03 13:21:02: Staging Node nlabp2815 mip=[10.117.0.87]
nodeID=[2] (1 of 4 nodes)
2019-04-03 13:21:02: Node Upgrade serving image at
http://10.117.0.204/rtfi/solidfire-rtfisodium-
patch3-11.3.0.14171/filesystem.squashfs
...
2019-04-03 13:25:40: Staging finished. Repeat the upgrade command
without the --stage option to start the upgrade.
```

ステージングされた ISO は、アップグレードの完了後に自動的に削除されます。ただし、アップグレードが開始されておらず、再スケジュールが必要な場合は、次のコマンドを使用して ISO のステージングを手動で解除できます。

`finstall <MVIP> -u <cluster_username> — destage `

アップグレードの開始後は、デステージオプションは使用できなくなります。

4. 'fsinstall' コマンドと ISO ファイルへのパスを使用して ' アップグレードを開始します

```
finstall <MVIP> -u <cluster_username><path-to-install-file-ISO>
```

◦ 例 *

入力コマンドの例を次に示します。

```
sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-
11.0.0.345.iso
```

サンプルの出力は 'fsinstall が 'fsinstall' の新しいバージョンが利用可能かどうかを確認しようとすることを示しています

```
sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-
11.0.0.345.iso
2018-10-01 16:52:15: Newer version of sfinstall available.
This version: 2018.09.01.130, latest version: 2018.06.05.901.
The latest version of the HealthTools can be downloaded from:
https://mysupport.netapp.com/NOW/cgi-bin/software/ or rerun with
--skip-version-check
```

以下は、アップグレードに成功した場合の出力例です。アップグレードイベントを使用して、アップグレードの進捗状況を監視できます。

```
# sfinstall 10.117.0.161 -u admin solidfire-rtfi-sodium-11.0.0.761.iso
2018-10-11 18:28
Checking connectivity to MVIP 10.117.0.161
Checking connectivity to node 10.117.0.23
Checking connectivity to node 10.117.0.24
...
Successfully connected to cluster and all nodes
##################################################################
You are about to start a new upgrade
10.117.0.161
10.3.0.161
solidfire-rtfi-sodium-11.0.0.761.iso
Nodes:
10.117.0.23 nlabp1023 SF3010 10.3.0.161
10.117.0.24 nlabp1025 SF3010 10.3.0.161
10.117.0.26 nlabp1027 SF3010 10.3.0.161
10.117.0.28 nlabp1028 SF3010 10.3.0.161
##################################################################
```

```
Do you want to continue? ['Yes', 'No']: yes
...
Watching for new network faults. Existing fault IDs are set([]).
Checking for legacy network interface names that need renaming
Upgrading from 10.3.0.161 to 11.0.0.761 upgrade method=rtfi
Waiting 300 seconds for cluster faults to clear
Waiting for caches to fall below threshold
...
Installing mip=[10.117.0.23] nodeID=[1] (1 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[7] away from mip[10.117.0.23] nodeID[1] ssid[11]
to new ssid[15]
Moving primary slice=[12] away from mip[10.117.0.23] nodeID[1] ssid[11]
to new ssid[15]
...
Installing mip=[10.117.114.24] nodeID=[2] (2 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[5] away from mip[10.117.114.24] nodeID[2] ssid[7]
to new ssid[11]
...
Install of solidfire-rtfi-sodium-11.0.0.761 complete.
Removing old software
No staged builds present on nodeID=[1]
No staged builds present on nodeID=[2]
...
Starting light cluster block service check
```

> H610S シリーズノードを Element 12.3.x にアップグレードする場合、ノードで 11.8 よりも前のバージョンの Element が実行されているときは、追加のアップグレード手順（）を実行する必要がありますフェーズ 2.）をクリックします。Element 11.8 以降を実行している場合は、追加のアップグレード手順（フェーズ 2 ）は必要ありません。

HealthTools を使用してダークサイトで **Element** ソフトウェアをアップグレードします

HealthTools ツールスイートを使用して、外部接続がないダークサイトで NetApp Element ソフトウェアを更新できます。

必要なもの

1. NetApp HCI ソフトウェアにアクセスします "ページをダウンロードします"。
2. 適切なソフトウェアリリースを選択し、管理ノードではないコンピュータに最新のストレージノードイメージをダウンロードします。

Element ストレージソフトウェアをアップグレードするには、最新バージョンの HealthTools が必要です。

3. こちらをダウンロードしてください "JSON ファイル" 管理ノードではないコンピュータのネットアップサポートサイトから、「 metadats.json 」に名前を変更します。
4. ISO ファイルを '/tmp のようなアクセス可能な場所にある管理ノードにコピーします

これは SCP などを使用して実行できます。ISO ファイルをアップロードする際には、ファイル名が変更されないようにしてください。変更されていると以降の手順が失敗します。

手順

1. 次のコマンドを実行します。

```
sfupdate-healthtools <path-to-healthtools-package>
```

2. インストールされているバージョンを確認します。

```
sfupdate-healthtools -v
```

3. 最新バージョンをメタデータ JSON ファイルと照合します。

```
sfupdate-healthtools -l --metadata=<path-to-metadata-json>
```

4. クラスタの準備が完了していることを確認します。

```
sudo sfupgradecheck -u <cluster_username> -p <cluster_password> MVIP
--metadata=<path-to-metadata-json>
```

5. ISO ファイルとメタデータ JSON ファイルへのパスを指定して 'fsinstall コマンドを実行します

```
sfinstall -u <cluster_username> <MVIP> <path-toinstall-file-ISO>
--metadata=<path-to-metadata-json-file>
```

入力コマンドの例を次に示します。

```
sfinstall -u admin 10.117.78.244 /tmp/solidfire-rtfi-11.3.0.345.iso
--metadata=/tmp/metadata.json
```

- オプション * --stage フラグを 'sfcinstall コマンドに追加して ' アップグレードを事前にステージングすることができます

> H610S シリーズノードを Element 12.3.x にアップグレードする場合、ノードで 11.8 よりも前のバージョンの Element が実行されているときは、追加のアップグレード手順（）を実行する必要がありますフェーズ 2.）をクリックします。Element 11.8 以降を実行している場合は、追加のアップグレード手順（フェーズ 2 ）は必要ありません。

HealthTools を使用してアップグレードに失敗した場合の動作

ソフトウェアのアップグレードに失敗した場合は、アップグレードを一時停止できます。

> アップグレードの一時停止には必ず Ctrl-C を使用してくださいこれにより、システムが自動的にクリーンアップされます。

「 finstall 」がクラスタ障害がクリアされるのを待機しているときに障害が発生すると ' 次のノードに進むことはありません

手順

1. Ctrl+C で 'sfcinstall' を停止する必要があります
2. ネットアップサポートに問い合わせて、エラーの調査を依頼します。
3. 同じ 'finstall' コマンドを使用してアップグレードを再開します
4. Ctrl+C でアップグレードを一時停止した場合、アップグレード中にノードがアップグレードされているときは、次のいずれかのオプションを選択します。
   - * wait * ：クラスタ定数をリセットする前に、現在アップグレード中のノードの終了を許可します。
   - * 続行 * ：アップグレードを続行します。これにより一時停止がキャンセルされます。
   - * 中止 * ：クラスタ定数をリセットし、アップグレードをただちに中止します。

> ノードの更新中にクラスタのアップグレードを中止すると、そのノードからドライブが強制的に削除されることがあります。ドライブが強制的に削除された場合、ネットアップサポートに依頼して手動でドライブを元に戻す処理がアップグレード時に必要になります。ノードでファームウェアの更新や更新後の同期処理に時間がかかる可能性があります。アップグレードが停止していると思われる場合は、ネットアップサポートにお問い合わせください。

H610S ストレージノードの **Element 12.3.x** へのアップグレード（フェーズ **2** ）

H610S シリーズノードを Element 12.3.x にアップグレードする場合、ノードで 11.8 よりも前のバージョンの Element が実行されていると、アップグレードプロセスは 2 つのフェーズで構成されます。

最初に実行するフェーズ 1 では、 Element 12.3.x への標準アップグレードプロセスと同じ手順を実行します。Element ソフトウェアと 5 つすべてのファームウェアの更新を、クラスタ内で一度に 1 つのノードずつローリング形式でインストールします。ファームウェアのペイロードが原因で、 H610S ノードあたりの所要時間は約 1.5 ~ 2 時間と推定されます。これには、各ノードのアップグレード終了時のコールドブートサイクルが 1 回含まれます。

フェーズ 2 では、ノード全体を実行するための手順を実行します H610S ノードごとに、シャットダウンと電源切断を行います を参照してください "KB"。このフェーズには、 H610S ノード 1 つにつき約 1 時間かかると推定されます。

フェーズ 1 が完了すると、各 H610S ノードのコールドブート時に 5 つのファームウェア更新のうち 4 つがアクティブになります。ただし、 Complex Programmable Logic Device （ CPLD ；複合プログラマブルロジックデバイス）ファームウェアを完全にインストールするには、完全な電源切断と再接続が必要です。CPLD ファームウェア・アップデートは、再起動または電源再投入時に NVDIMM の障害やメタデータ・ドライブの削除から保護します。この電源リセットには、 H610S ノード 1 つにつき約 1 時間かかると推定されます。ノードをシャットダウンし、電源ケーブルを取り外すか、スマート PDU を介して電源を切断し、約 3 分待ってから電源を再接続する必要があります。

作業を開始する前に

- H610S のアップグレードプロセスのフェーズ 1 が完了し、 Element ストレージの標準のアップグレード手順を使用してストレージノードをアップグレードしておきます。

フェーズ 2 にはオンサイトの担当者が必要です。

手順

1. （フェーズ 2 ）クラスタ内の H610S ノードごとに、電源リセットプロセスを完了します。

H610S 以外のノードもクラスタに含まれている場合、これらの H610S 以外のノードはフェーズ 2 から除外されるため、シャットダウンしたり電源を切断したりする必要はありません。

1. このアップグレードのサポートやスケジュールについては、ネットアップサポートにお問い合わせください。
2. このフェーズ 2 のアップグレード手順に従います "KB" 各 H610S ノードをアップグレードするには、この操作が必要です。

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 のリソースページ"

ストレージファームウェアをアップグレードします

Element 12.0 以降および管理サービスバージョン 2.14 以降では、 NetApp Hybrid Cloud Control の UI と REST API を使用して、ストレージノードでファームウェアのみのアップグレードを実行できます。この手順では、 Element ソフトウェアはアップグレードされず、 Element のメジャーリリース以外のバージョンのストレージファームウェアもアップグレードできます。

必要なもの

- * admin 権限 * ：アップグレードを実行する権限がストレージクラスタ管理者に付与されています。
- * システム時間の同期 * ：すべてのノードのシステム時間が同期されており、 NTP がストレージクラスタとノードに対して正しく設定されていることを確認しておきます。各ノードには、ノード Web UI （「 https://[IP address 」： 442 ）に DNS ネームサーバを設定する必要があります。時刻のずれに関連する未解決のクラスタ障害はありません。
- * システムポート * ： NetApp Hybrid Cloud Control をアップグレードに使用している場合は、必要なポートが開いていることを確認しておきます。を参照してください "ネットワークポート" を参照してくださ

い。

- * 管理ノード * ： NetApp Hybrid Cloud Control の UI および API では、環境内の管理ノードはバージョン 11.3 を実行しています。
- * 管理サービス * ：管理サービスバンドルを最新バージョンに更新しました。

> Element ソフトウェアバージョン 12.0 を実行している H610S ストレージノードについては、ストレージファームウェアバンドル 2.27 にアップグレードする前に「 D パッチ」「 St-909 」を適用する必要があります。アップグレード前に、ネットアップサポートに問い合わせて D パッチを入手します。を参照してください "ストレージファームウェアバンドル 2.27 リリースノート"。

> ストレージノードのファームウェアをアップグレードする前に、最新の管理サービスバンドルにアップグレードする必要があります。Element ソフトウェアをバージョン 12.2 以降に更新する場合は、管理サービス 2.14.60 以降が必要です。

> iDRAC / BIOS ファームウェアを更新するには、ネットアップサポートにお問い合わせください。追加情報の場合は、を参照してください "こちらの技術情報アーティクル"。

- * クラスタの健全性 * ：健全性チェックを実行しました。を参照してください "ストレージをアップグレードする前に、 Element ストレージの健全性チェックを実行します"。
- * H610S ノードの BMC を更新 * ： H610S ノードの BMC バージョンをアップグレードしました。を参照してください "リリースノートおよびアップグレード手順"。

> ご使用のハードウェアのファームウェアとドライバのファームウェアの一覧については、を参照してください "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"。

- エンドユーザライセンス契約（**EULA**）：管理サービス2.20.69以降では、NetApp Hybrid Cloud Control UIまたはAPIを使用してストレージファームウェアをアップグレードする前に、EULAに同意して保存する必要があります。
  a. Webブラウザで管理ノードのIPアドレスを開きます。

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

  b. 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。
  c. インターフェイスの右上にある [* Upgrade] を選択します。
  d. EULAがポップアップ表示されます。下にスクロールして、[現在および今後のすべての更新を許可する*]を選択し、[保存*]を選択します。

アップグレードオプション

次のいずれかのストレージファームウェアアップグレードオプションを選択します。

- NetApp Hybrid Cloud Control UI を使用してストレージファームウェアをアップグレードします
- NetApp Hybrid Cloud Control API を使用してストレージファームウェアをアップグレードします

NetApp Hybrid Cloud Control UI を使用してストレージファームウェアをアップグレードします

NetApp Hybrid Cloud Control の UI を使用して、クラスタ内のストレージノードのファームウェアをアップグレードできます。

必要なもの

管理ノードがインターネットに接続されていない場合は、を使用します "NetApp HCI ストレージクラスタのストレージファームウェアパッケージをダウンロードします"。

NetApp Hybrid Cloud Control を使用してストレージクラスタをアップグレードする際の潜在的な問題とその対処方法については、を参照してください "こちらの技術情報アーティクル"。

アップグレードプロセスは、ストレージノードあたり約 30 分かかります。Element ストレージクラスタをバージョン 2.76 よりも新しいストレージファームウェアにアップグレードする場合、ノードに新しいファームウェアが書き込まれたときのみ、個々のストレージノードがアップグレード中にリブートされます。

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。

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

2. 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。
3. インターフェイスの右上にある [* Upgrade] を選択します。
4. [* Upgrades] ページで、 [* Storage] を選択します。

[* ストレージ *] タブには、インストールの一部であるストレージクラスタが一覧表示されます。NetApp Hybrid Cloud Control からクラスタにアクセスできない場合は、 * Upgrades * ページに表示されません。Element 12.0 以降を実行しているクラスタでは、これらのクラスタの現在のファームウェアバンドルバージョンが表示されます。1 つのクラスタ内のノードでファームウェアバージョンが異なる場合やアップグレードが進むにつれて、「 * Current Firmware Bundle Version * 」列に「 * Multiple * 」と表示されます。「 * multiple * 」を選択すると、「 * Nodes * 」ページに移動してファームウェアバージョンを比較できます。すべてのクラスタで 12.0 よりも前のバージョンの Element を実行している場合、ファームウェアバンドルのバージョン番号に関する情報は表示されません。この情報は、 * Nodes * ページでも確認できます。を参照してください "インベントリを表示します"。

クラスタが最新の状態であり、アップグレードパッケージがない場合は、「 * Element * 」タブと「 * Firmware only * 」タブは表示されません。これらのタブは、アップグレードの実行中は表示されません。[* 要素 *] タブが表示されているが、 [* ファームウェアのみ *] タブが表示されていない場合は、ファームウェアパッケージは利用できません。

5. アップグレードするクラスタの横にあるドロップダウン矢印を選択します。
6. [* Browse] を選択して、ダウンロードしたアップグレード・パッケージをアップロードします。
7. アップロードが完了するまで待ちます。進捗バーにアップロードのステータスが表示されます。

ブラウザウィンドウから別の場所に移動すると、ファイルのアップロードが失われます。

ファイルのアップロードと検証が完了すると、画面にメッセージが表示されます。検証には数分かかることがあります。この段階でブラウザウィンドウから移動しても、ファイルのアップロードは維持されます。

8. 「 * ファームウェアのみ * 」を選択し、利用可能なアップグレードバージョンから選択します。
9. [* アップグレードの開始 *] を選択します。

アップグレード中は、アップグレードステータス * が変更され、プロセスのステータスが反映されます。また、アップグレードの一時停止など、実行する操作に応じて変更が加えられたか、またはアップグレードでエラーが返された場合も変更されます。を参照してください [アップグレードステータスが変わります]。

アップグレードの実行中は、ページを離れてあとから表示し、進捗状況の監視を続行できます。クラスタの行が折りたたまれている場合、ページではステータスと現在のバージョンは動的に更新されません。表を更新するには、クラスタの行を展開する必要があります。また、ページを更新することもできます。

アップグレードの完了後にログをダウンロードできます。

アップグレードステータスが変わります

アップグレードプロセスの実行前、実行中、実行後に、 UI の * アップグレードステータス * 列に表示されるさまざまな状態を以下に示します。

アップグレードの状態	説明
最新	クラスタが最新の Element バージョンにアップグレードされたか、ファームウェアが最新バージョンにアップグレードされました。
検出できません	このステータスは、ストレージサービスAPIがアップグレードステータスの一覧に含まれていないアップグレードステータスを返した場合に表示されます。
使用可能なバージョン	Element / ストレージファームウェアの新しいバージョンをアップグレードできます。
実行中です	アップグレードを実行中です。進行状況バーにアップグレードステータスが表示されます。画面にはノードレベルの障害も表示され、アップグレードの進行に伴いクラスタ内の各ノードのノード ID も表示されます。各ノードのステータスは、 Element UI または NetApp Element Plug-in for vCenter Server UI を使用して監視できます。

アップグレードの状態	説明
Pausing をアップグレードします	アップグレードを一時停止することもできます。アップグレードプロセスの状態によっては、一時停止処理が成功するか失敗するかが決まります。一時停止処理の確認を求める UI プロンプトが表示されます。アップグレードを一時停止する前にクラスタが安全な場所にあることを確認するには、アップグレード処理が完全に一時停止されるまでに最大 2 時間かかることがあります。アップグレードを再開するには、 * Resume * （続行）を選択します。
一時停止中	アップグレードを一時停止した。[* Resume （続行）] を選択して、プロセスを再開します。
エラー	アップグレード中にエラーが発生しました。エラーログをダウンロードして、ネットアップサポートに送信できます。エラーを解決したら、ページに戻って * Resume * （続行）を選択します。アップグレードを再開すると、システムが健全性チェックを実行してアップグレードの現在の状態を確認している間、進捗状況バーが数分間後方に移動します。

NetApp Hybrid Cloud を使用してアップグレードに失敗した場合の動作 制御

アップグレード中にドライブまたはノードで障害が発生した場合は、 Element UI にクラスタエラーが表示されます。アップグレードプロセスは次のノードに進まず、クラスタの障害が解決するまで待機します。UI の進捗状況バーには、アップグレードがクラスタの障害の解決を待機していることが表示されます。アップグレードはクラスタが正常に完了するまで待機するため、この段階で UI で * Pause * を選択することはできません。障害の調査に役立てるには、ネットアップサポートに問い合わせる必要があります。

NetApp Hybrid Cloud Control には 3 時間の待機時間があらかじめ設定されています。この時間内に、次のいずれかの状況が発生する可能性があります。

- クラスタの障害は 3 時間以内に解決され、アップグレードが再開されます。このシナリオでは対処は必要ありません。
- 問題は 3 時間後も解消されず、アップグレードのステータスが「 Error 」（エラー）と赤のバナーを表示します。問題が解決したら、「 * Resume 」（続行）を選択してアップグレードを再開できます。
- 3 時間以内に対処するために、アップグレードを一時的に中止する必要があることがネットアップサポートによって確認されました。サポートは API を使用してアップグレードを中止します。

> ノードの更新中にクラスタのアップグレードを中止すると、そのノードからドライブが強制的に削除されることがあります。ドライブが強制的に削除された場合、ネットアップサポートに依頼して手動でドライブを元に戻す処理がアップグレード時に必要になります。ノードでファームウェアの更新や更新後の同期処理に時間がかかる可能性があります。アップグレードが停止していると思われる場合は、ネットアップサポートにお問い合わせください。

NetApp Hybrid Cloud Control API を使用してストレージファームウェアをアップグレードします

API を使用して、クラスタ内のストレージノードを最新バージョンの Element ソフトウェアにアップグレードできます。API の実行には、任意の自動化ツールを使用できます。ここで説明する API ワークフローでは、例として管理ノードで使用可能な REST API UI を使用します。

手順

1. 管理ノードからアクセス可能なデバイスに最新のストレージファームウェアアップグレードパッケージをダウンロードします。にアクセスします "Element ソフトウェアストレージファームウェアのバンドルページ" 最新のストレージファームウェアイメージをダウンロードできます。
2. ストレージファームウェアのアップグレードパッケージを管理ノードにアップロードします。
   a. 管理ノードで管理ノード REST API UI を開きます。

      ```
      https://<ManagementNodeIP>/package-repository/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. 承認ウィンドウを閉じます。
   c. REST API UI から * POST/packages * を選択します。
   d. [* 試してみてください *] を選択します。
   e. [* Browse] を選択して、アップグレード・パッケージを選択します。
   f. 「 * Execute * 」を選択してアップロードを開始します。
   g. 応答から ' 後の手順で使用するためにパッケージ ID (`id"') をコピーして保存します
3. アップロードのステータスを確認します。
   a. REST API UI から、 * GEGET 処理対象 / パッケージ間の一時的なグループ / ｛ id ｝ 一時的なグループ / ステータス * を選択します。
   b. [* 試してみてください *] を選択します。
   c. 前の手順でコピーしたファームウェアパッケージ ID を * id * で入力します。
   d. ステータス要求を開始するには、 * Execute * を選択します。

      応答が完了すると、「アクセス」として表示されます。

4. インストールアセット ID を確認します。
   a. 管理ノードで管理ノード 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. 承認ウィンドウを閉じます。

c. REST API UI から、 * GET / Installations * 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. 応答から ' インストール資産 ID (id`) をコピーします

```
"id": "abcd01e2-xx00-4ccf-11ee-11f111xx9a0b",
"management": {
  "errors": [],
  "inventory": {
    "authoritativeClusterMvip": "10.111.111.111",
    "bundleVersion": "2.14.19",
    "managementIp": "10.111.111.111",
    "version": "1.4.12"
```

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 ' 後の手順で使用できるようにアップグレードするクラスタのストレージ・クラスタ ID （ ID ）をコピーして保存します

```
"storage": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterUuid": "a1bd1111-4f1e-46zz-ab6f-0a1111b1111x",
        "id": "a1bd1111-4f1e-46zz-ab6f-a1a1a111b012",
```

5. ストレージファームウェアのアップグレードを実行します。

a. 管理ノードでストレージ REST API UI を開きます。

```
https://<ManagementNodeIP>/storage/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. [**POST/upgrade**] を選択します。

d. [* 試してみてください *] を選択します。

e. パラメータフィールドにアップグレードパッケージ ID を入力します。

f. パラメータフィールドにストレージクラスタ ID を入力します。

g. アップグレードを開始するには、 * Execute * を選択します。

応答は ' ステータスを初期化中と表示する必要があります


```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1",
    "log": https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1/log
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
      "string"
    ],
    "message": "string",
    "nodeDetails": [
      {
        "message": "string",
        "step": "NodePreStart",
        "nodeID": 0,
        "numAttempt": 0
      }
    ],
    "percent": 0,
    "step": "ClusterPreStart",
    "timestamp": "2020-04-21T22:10:57.057Z",
    "failedHealthChecks": [
      {
        "checkID": 0,
        "name": "string",
        "displayName": "string",
        "passed": true,
        "kb": "string",
        "description": "string",
```

```
        "remedy": "string",
        "severity": "string",
        "data": {},
        "nodeID": 0
      }
    ]
  },
  "taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",
  "dateCompleted": "2020-04-21T22:10:57.057Z",
  "dateCreated": "2020-04-21T22:10:57.057Z"
}
```


a. 応答の一部であるアップグレード ID （「 upgradeId 」）をコピーします。

6. アップグレードの進捗状況と結果を確認します。

   a. Get Sebring/upgrades/｛upgradeId｝ * を選択します。
   b. [* 試してみてください *] を選択します。
   c. アップグレード ID は、前の手順のアップグレード ID として * upgradeId * と入力します。
   d. [* Execute] を選択します。
   e. アップグレード中に問題または特別な要件が発生した場合は、次のいずれかを実行します。

オプション	手順
応答の本文に「 failedHealthCheckks 」というメッセージが表示されているため、クラスタのヘルスの問題を修正する必要があります。	i. 各問題について記載されている特定の技術情報アーティクルに移動するか、指定された対処方法を実行します。 ii. KB を指定した場合は、関連する技術情報アーティクルに記載されているプロセスを完了します。 iii. クラスタの問題を解決したら、必要に応じて再認証し、 * PUT 処理の際に必要な数 / アップグレード / ｛ upgradeId ｝ * を選択します。 iv. [* 試してみてください *] を選択します。 v. アップグレード ID は、前の手順のアップグレード ID として * upgradeId * と入力します。 vi. リクエスト本文に「 action 」 : 「 resume 」と入力します。 `{ "action": "resume" }` vii. [* Execute] を選択します。
メンテナンス時間が終了しているか別の理由で、アップグレードを一時停止する必要があります。	i. 必要に応じて再認証し、 * PUT に成功 / アップグレード / ｛ upgradeId ｝ * を選択します。 ii. [* 試してみてください *] を選択します。 iii. アップグレード ID は、前の手順のアップグレード ID として * upgradeId * と入力します。 iv. リクエスト本文に「 action 」 : 「 pause 」と入力します。 `{ "action": "pause" }` v. [* Execute] を選択します。

f. 必要に応じて、処理が完了するまで * Get Theple/upgrades/ ｛ upgradeId ｝ * API を複数回実行します。

アップグレード中、エラーが発生しなかった場合、「ステータス」は「実行中」を示します。各ノードがアップグレードされると 'tep' の値が NodeFinished に変わります

アップグレードが正常に終了したのは 'percent` の値が '100' で 'tate' が 'finished' である場合です

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 のリソースページ"

管理ノードをアップグレードします

管理ノードをバージョン 11.0 以降からバージョン 12.3.x にアップグレードできます。

ストレージクラスタ上の Element ソフトウェアをアップグレードするために、管理ノードのオペレーティングシステムをアップグレードする必要がなくなりました。管理ノードがバージョン 11.3 以降である場合は、NetApp Hybrid Cloud Control を使用して管理サービスを最新バージョンにアップグレードするだけで Element をアップグレードできます。管理ノードのオペレーティングシステムをアップグレードする理由がほかにもある場合は、セキュリティの修正など、管理ノードのアップグレード手順に従ってください。

> vCenter Plug-in 4.4 以降では、モジュラアーキテクチャで作成された管理ノード 11.3 以降が必要であり、個々のサービスを提供します。

アップグレードオプション

次のいずれかの管理ノードアップグレードオプションを選択します。

> - 管理ノード 12.3.2 には、 Virtual Volumes （ VVol ）機能が有効になっている場合に、ストレージクラスタのセキュリティを軽減する機能が含まれています。ストレージクラスタがすでにElement 12.3にあり、VVol機能が有効になっている場合は、12.3.2にアップグレードする必要があります。
> - 管理ノード 12..1 では、機能の変更やバグの修正は行われていません。管理ノード 12.3 をすでに実行している場合は、これを 12.3.1 にアップグレードする必要はありません。

- 管理ノード 12.3 からアップグレードする場合：管理ノード 12..1 には、追加の機能変更やバグ修正はありません。管理ノード 12.3 をすでに実行している場合は、これを 12.3.1 にアップグレードする必要はありません。

> NDE を使用して導入した管理ノード 12.3 でアップグレードを続行するように選択すると、12.3.x へのアップグレードが完了します。ただし、アップグレードの再開時にエラーが発生する場合があります。この場合は、管理ノードをリブートして、 12.3.x が正しく表示されるようにします

- 管理ノード 12.2 からアップグレードする場合は、次の手順を実行します。12.2 から管理ノードをバージョン 12.3.x にアップグレードします
- 管理ノード 12.0 からアップグレードする場合は、次の手順を実行します。バージョン 12.0 から管理ノードをバージョン 12.3.x にアップグレードします
- 管理ノード 11.3 、 11.5 、 11.7 、または 11.8 からアップグレードする場合は、次の手順を実行します。管理ノードをバージョン 11.3 から 11.8 にアップグレードします

- 管理ノード 11.0 または 11.1 からアップグレードする場合は、次の手順を実行します。管理ノードをバージョン 12.3.x にアップグレードします。 11.1 または 11.0 からアップグレードします
- 管理ノードバージョン 10.x からアップグレードする場合は、次の手順を実行します。管理ノードバージョン 10.x から 11.x への移行

管理サービスのバージョンがシーケンシャルに * 更新されている（1）場合、および（2） Element ストレージのバージョンが既存の管理ノードを * 保持する場合は、次のオプションを選択します。

> 管理サービスと Element ストレージを順番に更新しないと、この手順で再認証を再設定することはできません。代わりに、該当するアップグレード手順を実行してください。

- 既存の管理ノードを保持する場合：管理ノード REST API を使用して認証を再設定します

12.2 から管理ノードをバージョン **12.3.x** にアップグレードします

新しい管理ノード仮想マシンをプロビジョニングすることなく、バージョン 12.2 からバージョン 12.3.x への管理ノードのインプレースアップグレードを実行できます。

> Element 12.3.x 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。

必要なもの

- 管理ノード VM の RAM は 24GB です。
- アップグレードする管理ノードのバージョンが 12.0 で、 IPv4 ネットワークを使用している。管理ノードバージョン 12.3.x は IPv6 をサポートしていません。

> 管理ノードのバージョンを確認するには、管理ノードにログインし、ログインバナーに表示される Element のバージョン番号を確認します。

- NetApp Hybrid Cloud Control （HCC）を使用して管理サービスバンドルを最新バージョンに更新しておく必要があります。HCC には、次の IP アドレスからアクセスできます。 https://<ManagementNodeIP>`
- 管理ノードをバージョン 12.3.x に更新する場合は、続行するには管理サービス 2.14.60 以降が必要です。
- 追加のネットワークアダプタを設定しておきます（必要な場合）。 の手順に従ってください "追加のストレージ NIC の設定"。

> eth0 を SVIP にルーティングできない場合は、永続ボリュームに追加のネットワークアダプタが必要になることがあります。永続ボリュームを設定できるように、 iSCSI ストレージネットワークに新しいネットワークアダプタを設定してください。

- ストレージノードで Element 11.3 以降が実行されていることを確認します。

手順

1. SSH またはコンソールアクセスを使用して管理ノード仮想マシンにログインします。
2. をダウンロードします "管理ノード ISO" NetApp HCI の場合は、ネットアップサポートサイトから管理ノード仮想マシンへ。

> ISO の名前は 'olidfire-fdva-<Element release>-patchX-XXX.X.XXXX.iso' と似ています

3. ダウンロードしたファイルに対して md5sum を実行し、その出力を、ネットアップサポートサイトにある NetApp HCI または Element ソフトウェア用の md5sum と比較することで、ダウンロードの整合性を確認します。

   「 sudo md5sum -b 」 <path to ISO>/solidfire-fdva-<Element release > -patchX-XXX.X.XXXX.iso 」を参照してください

4. 次のコマンドを使用して、管理ノードの ISO イメージをマウントし、ファイルシステムに内容をコピーします。

```
sudo mkdir -p /upgrade
```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso>
/mnt
```

```
sudo cp -r /mnt/* /upgrade
```

5. ホーム・ディレクトリに移動し 'ISO ファイルを /mnt/' からアンマウントします

```
sudo umount /mnt
```

6. 管理ノードのスペースを節約するために ISO を削除します。

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

7. アップグレードする管理ノードで次のコマンドを実行して管理ノードの OS バージョンをアップグレードします。Active IQ コレクタやプロキシの設定など、必要な設定ファイルはすべてアップグレード後も保持されます。

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

   アップグレードプロセスが完了すると、管理ノードが新しい OS でリブートします。

   > この手順で説明した sudo コマンドを実行すると、 SSH セッションが強制終了されます。継続的な監視を行うには、コンソールアクセスが必要です。アップグレードの実行中にコンソールにアクセスできない場合は、 SSH ログインを再試行し、 15~30 分後に接続を確認します。ログイン後、アップグレードが正常に完了したことを示す SSH バナーで新しい OS バージョンを確認できます。

8. 管理ノードで「 redeploy -mnode 」スクリプトを実行して、以前の管理サービスの設定を保持します。

設定に応じて、 Active IQ コレクタサービス、コントローラ（ vCenter ）、プロキシなどの以前の管理サービスの設定が適用されます。

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

管理ノードで SSH 機能を無効にしていた場合は、が必要です "SSH を再度無効にします" リカバリされた管理ノード。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" 管理ノードではデフォルトで有効になっています。

バージョン **12.0** から管理ノードをバージョン **12.3.x** にアップグレードします

新しい管理ノード仮想マシンをプロビジョニングすることなく、管理ノードバージョン 12.0 からバージョン 12.3.x へのインプレースアップグレードを実行できます。

Element 12.3.x 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。

必要なもの

- アップグレードする管理ノードのバージョンが 12.0 で、 IPv4 ネットワークを使用している。管理ノードバージョン 12.3.x は IPv6 をサポートしていません。

  管理ノードのバージョンを確認するには、管理ノードにログインし、ログインバナーに表示される Element のバージョン番号を確認します。

- NetApp Hybrid Cloud Control （ HCC ）を使用して管理サービスバンドルを最新バージョンに更新しておく必要があります。HCC には、次の IP アドレスからアクセスできます。 https://<ManagementNodeIP>`
- 管理ノードをバージョン 12.3.x に更新する場合は、続行するには管理サービス 2.14.60 以降が必要です。
- 追加のネットワークアダプタを設定しておきます（必要な場合）。 の手順に従ってください "追加のストレージ NIC の設定"。

  eth0 を SVIP にルーティングできない場合は、永続ボリュームに追加のネットワークアダプタが必要になることがあります。永続ボリュームを設定できるように、 iSCSI ストレージネットワークに新しいネットワークアダプタを設定してください。

- ストレージノードで Element 11.3 以降が実行されていることを確認します。

手順

1. 管理ノードの VM RAM を設定します。
   a. 管理ノード VM の電源をオフにします。
   b. 管理ノード VM の RAM を 12GB から 24GB RAM に変更します。
   c. 管理ノード VM の電源をオンにします。
2. SSH またはコンソールアクセスを使用して管理ノード仮想マシンにログインします。
3. をダウンロードします "管理ノード ISO" NetApp HCI の場合は、ネットアップサポートサイトから管理ノ

ード仮想マシンへ。

> ISO の名前は 'olidfire-fdva-<Element release>-patchX-XXX.X.XXXX.iso' と似ています

4. ダウンロードしたファイルに対して md5sum を実行し、その出力を、ネットアップサポートサイトにある NetApp HCI または Element ソフトウェア用の md5sum と比較することで、ダウンロードの整合性を確認します。

   「 sudo md5sum -b 」 <path to ISO>/solidfire-fdva-<Element release > -patchX-XXX.X.XXXX.iso 」を参照してください

5. 次のコマンドを使用して、管理ノードの ISO イメージをマウントし、ファイルシステムに内容をコピーします。

```
sudo mkdir -p /upgrade
```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso>
/mnt
```

```
sudo cp -r /mnt/* /upgrade
```

6. ホーム・ディレクトリに移動し 'ISO ファイルを /mnt/' からアンマウントします

```
sudo umount /mnt
```

7. 管理ノードのスペースを節約するために ISO を削除します。

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

8. アップグレードする管理ノードで次のコマンドを実行して管理ノードの OS バージョンをアップグレードします。Active IQ コレクタやプロキシの設定など、必要な設定ファイルはすべてアップグレード後も保持されます。

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

   アップグレードプロセスが完了すると、管理ノードが新しい OS でリブートします。

この手順で説明した sudo コマンドを実行すると、 SSH セッションが強制終了されます。継続的な監視を行うには、コンソールアクセスが必要です。アップグレードの実行中にコンソールにアクセスできない場合は、 SSH ログインを再試行し、 15~30 分後に接続を確認します。ログイン後、アップグレードが正常に完了したことを示す SSH バナーで新しい OS バージョンを確認できます。

9. 管理ノードで「 redeploy -mnode 」スクリプトを実行して、以前の管理サービスの設定を保持します。

設定に応じて、 Active IQ コレクタサービス、コントローラ（ vCenter ）、プロキシなどの以前の管理サービスの設定が適用されます。

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

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" をクリックします。

管理ノードをバージョン **11.3** から **11.8** にアップグレードします

新しい管理ノード仮想マシンをプロビジョニングすることなく、管理ノードバージョン 11.3 、 11.5 、 11.7 、または 11.8 からバージョン 12.3.x へのインプレースアップグレードを実行できます。

Element 12.3.x 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。

必要なもの

- アップグレードする管理ノードのバージョンが 11.3 、 11.5 、 11.7 、または 11.8 で、 IPv4 ネットワークを使用していることを確認します。管理ノードバージョン 12.3.x は IPv6 をサポートしていません。

管理ノードのバージョンを確認するには、管理ノードにログインし、ログインバナーに表示される Element のバージョン番号を確認します。

- NetApp Hybrid Cloud Control （ HCC ）を使用して管理サービスバンドルを最新バージョンに更新しておく必要があります。HCC には、次の IP アドレスからアクセスできます。 https://<ManagementNodeIP>`
- 管理ノードをバージョン 12.3.x に更新する場合は、続行するには管理サービス 2.14.60 以降が必要です。
- 追加のネットワークアダプタを設定しておきます（必要な場合）。 の手順に従ってください "追加のストレージ NIC の設定"。

eth0 を SVIP にルーティングできない場合は、永続ボリュームに追加のネットワークアダプタが必要になることがあります。永続ボリュームを設定できるように、 iSCSI ストレージネットワークに新しいネットワークアダプタを設定してください。

- ストレージノードで Element 11.3 以降が実行されていることを確認します。

手順

1. 管理ノードの VM RAM を設定します。
   a. 管理ノード VM の電源をオフにします。
   b. 管理ノード VM の RAM を 12GB から 24GB RAM に変更します。
   c. 管理ノード VM の電源をオンにします。
2. SSH またはコンソールアクセスを使用して管理ノード仮想マシンにログインします。
3. をダウンロードします "管理ノード ISO" NetApp HCI の場合は、ネットアップサポートサイトから管理ノード仮想マシンへ。

   ISO の名前は 'olidfire-fdva-<Element release>-patchX-XXX.X.XXXX.iso' と似ています

4. ダウンロードしたファイルに対して md5sum を実行し、その出力を、ネットアップサポートサイトにある NetApp HCI または Element ソフトウェア用の md5sum と比較することで、ダウンロードの整合性を確認します。

   「 sudo md5sum -b 」 <path to ISO>/solidfire-fdva-<Element release > -patchX-XXX.X.XXXX.iso 」を参照してください

5. 次のコマンドを使用して、管理ノードの ISO イメージをマウントし、ファイルシステムに内容をコピーします。

```
sudo mkdir -p /upgrade
```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso>
/mnt
```

```
sudo cp -r /mnt/* /upgrade
```

6. ホーム・ディレクトリに移動し 'ISO ファイルを /mnt/' からアンマウントします

```
sudo umount /mnt
```

7. 管理ノードのスペースを節約するために ISO を削除します。

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

8. 11.3 、 11.5 、 11.7 、または 11.8 の管理ノードで、次のコマンドを実行して管理ノードの OS バージョンをアップグレードします。Active IQ コレクタやプロキシの設定など、必要な設定ファイルはすべてアップグレード後も保持されます。

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

アップグレードプロセスが完了すると、管理ノードが新しい OS でリブートします。

> この手順で説明した sudo コマンドを実行すると、 SSH セッションが強制終了されます。継続的な監視を行うには、コンソールアクセスが必要です。アップグレードの実行中にコンソールにアクセスできない場合は、 SSH ログインを再試行し、 15~30 分後に接続を確認します。ログイン後、アップグレードが正常に完了したことを示す SSH バナーで新しい OS バージョンを確認できます。

9. 管理ノードで「 redeploy -mnode 」スクリプトを実行して、以前の管理サービスの設定を保持します。

> 設定に応じて、 Active IQ コレクタサービス、コントローラ（ vCenter ）、プロキシなどの以前の管理サービスの設定が適用されます。

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

> 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" をクリックします。

管理ノードをバージョン **12.3.x** にアップグレードします。 **11.1** または **11.0** からアップグレードします

新しい管理ノード仮想マシンをプロビジョニングすることなく、管理ノード 11.0 または 11.1 からバージョン 12.3.x へのインプレースアップグレードを実行できます。

必要なもの

- ストレージノードで Element 11.3 以降が実行されていることを確認します。

  > 最新の HealthTools を使用して Element ソフトウェアをアップグレードしてください。

- アップグレードする管理ノードのバージョンが 11.0 または 11.1 で、 IPv4 ネットワークを使用していることを確認します。管理ノードバージョン 12.3.x は IPv6 をサポートしていません。

  > 管理ノードのバージョンを確認するには、管理ノードにログインし、ログインバナーに表示される Element のバージョン番号を確認します。

- 管理ノード 11.0 の場合、 VM メモリを手動で 12GB に増やす必要があります。
- 必要に応じて、管理ノードユーザガイドに記載されているストレージ NIC （ eth1 ）の設定手順に従って追加のネットワークアダプタを設定しておきます。

> eth0 を SVIP にルーティングできない場合は、永続ボリュームに追加のネットワークアダプタが必要になることがあります。永続ボリュームを設定できるように、 iSCSI ストレージネットワークに新しいネットワークアダプタを設定してください。

手順

1. 管理ノードの VM RAM を設定します。
   a. 管理ノード VM の電源をオフにします。
   b. 管理ノード VM の RAM を 12GB から 24GB RAM に変更します。
   c. 管理ノード VM の電源をオンにします。
2. SSH またはコンソールアクセスを使用して管理ノード仮想マシンにログインします。
3. をダウンロードします "管理ノード ISO" NetApp HCI の場合は、ネットアップサポートサイトから管理ノード仮想マシンへ。

   > ISO の名前は 'olidfire-fdva-<Element release>-patchX-XXX.X.XXXX.iso' と似ています

4. ダウンロードしたファイルに対して md5sum を実行し、その出力を、ネットアップサポートサイトにある NetApp HCI または Element ソフトウェア用の md5sum と比較することで、ダウンロードの整合性を確認します。

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-
   XX.X.X.XXXX.iso
   ```

5. 次のコマンドを使用して、管理ノードの ISO イメージをマウントし、ファイルシステムに内容をコピーします。

   ```
   sudo mkdir -p /upgrade
   ```

   ```
   sudo mount solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso /mnt
   ```

   ```
   sudo cp -r /mnt/* /upgrade
   ```

6. ホームディレクトリに移動し、 ISO ファイルを /mnt からアンマウントします。

   ```
   sudo umount /mnt
   ```

7. 管理ノードのスペースを節約するために ISO を削除します。

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

8. 次のいずれかのスクリプトを実行して、管理ノードの OS バージョンをアップグレードします。使用しているバージョンに適したスクリプトのみを実行してください。各スクリプトでは、 Active IQ コレクタやプロキシの設定など、必要な設定ファイルはすべてアップグレード後も保持されます。

   a. 11.1 （ 11.1.0.73 ）の管理ノードの場合は次のコマンドを実行します。

   ```
   sudo /sf/rtfi/bin/sfrtfi_inplace
   file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
   sf_keep_paths="/sf/packages/solidfire-sioc-4.2.3.2288
   /sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc
   /sf/packages/nma"
   ```

   b. 11.1 （ 11.1.0.72 ）の管理ノードの場合は次のコマンドを実行します。

   ```
   sudo /sf/rtfi/bin/sfrtfi_inplace
   file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
   sf_keep_paths="/sf/packages/solidfire-sioc-4.2.1.2281
   /sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc
   /sf/packages/nma"
   ```

   c. 11.0 （ 11.0.0.781 ）の管理ノードの場合は次のコマンドを実行します。

   ```
   sudo /sf/rtfi/bin/sfrtfi_inplace
   file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
   sf_keep_paths="/sf/packages/solidfire-sioc-4.2.0.2253
   /sf/packages/solidfire-nma-1.4.8/conf /sf/packages/sioc
   /sf/packages/nma"
   ```

   アップグレードプロセスが完了すると、管理ノードが新しい OS でリブートします。

   > この手順で説明した sudo コマンドを実行すると、 SSH セッションが強制終了されます。継続的な監視を行うには、コンソールアクセスが必要です。アップグレードの実行中にコンソールにアクセスできない場合は、 SSH ログインを再試行し、 15~30 分後に接続を確認します。ログイン後、アップグレードが正常に完了したことを示す SSH バナーで新しい OS バージョンを確認できます。

9. 12.3.x 管理ノードで、「 upgrade-mnode 」スクリプトを実行して、以前の設定を保持します。

   > 11.0 または 11.1 の管理ノードから移行している場合、 Active IQ コレクタが新しい形式にコピーされます。

a. 既存の管理ノード 11.0 または 11.1 で単一のストレージクラスタを管理しており、永続ボリュームがある場合：

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true -
persistent volume> -pva <persistent volume account name - storage
volume account>
```

b. 既存の管理ノード 11.0 または 11.1 で単一のストレージクラスタを管理しており、永続ボリュームがない場合：

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user>
```

c. 既存の管理ノード 11.0 または 11.1 で複数のストレージクラスタを管理しており、永続ボリュームがある場合：

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true -
persistent volume> -pva <persistent volume account name - storage
volume account> -pvm <persistent volumes mvip>
```

d. 既存の管理ノード 11.0 または 11.1 で複数のストレージクラスタを管理しており、永続ボリュームがない場合（「 -pvm 」フラグでクラスタのいずれかの MVIP アドレスを指定）：

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pvm <mvip for
persistent volumes>
```

10. （ NetApp Element Plug-in for vCenter Server を使用するすべての NetApp HCI インストールの場合）で、の手順に従って、 12.3.x 管理ノードの vCenter Plug-in を更新します "Element Plug-in for vCenter Server をアップグレードします" トピック：
11. 管理ノード API を使用して、インストール環境のアセット 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。
        i. 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。
    b. 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/
```

    c. 「 * 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。

d. 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。

e. [* 試してみてください *] を選択します。

f. [* Execute] を選択します。

g. 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

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。

12. 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。後の手順で使用するために 'tag' の値をコピーして保存します

13. HCI の監視と Hybrid Cloud Control 用の 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. 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「 vcenter 」タイプと「 vcenter 」クレデンシャルタイプで入力します。

e. [* Execute] を選択します。

14. コンピューティングノード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. 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。「タイプ」として「 ESXi ホスト」と入力し、「 hardware_tag 」の前の手順で保存したハードウェアタグを貼り付けます。

e. [* Execute] を選択します。

管理ノードバージョン **10.x** から **11.x** への移行

管理ノードのバージョンが 10.x の場合、 10.x から 11.x にアップグレードすることはできません代わりに、ここに記載する移行手順を使用して、新しく導入した 11.1 の管理ノードに 10.x から設定をコピーします。現在の管理ノードが 11.0 以降の場合は、この手順は省略してください。管理ノード 11.0 または 11.1 とが必要です "最新の HealthTools" Element ソフトウェアを 10.3 以降から 11.x にアップグレードします

手順

1. VMware vSphere インターフェイスで、管理ノード 11.1 OVA を導入し、電源をオンにします。

2. 管理ノードの VM コンソールを開きます。ターミナルユーザインターフェイス（ TUI ）が起動します。

3. TUI を使用して新しい管理者の ID を作成し、パスワードを割り当てます。
4. 管理ノードの TUI で、新しい ID とパスワードを使用して管理ノードにログインし、動作を確認します。
5. vCenter または管理ノードの TUI で、管理ノード 11.1 の IP アドレスを取得し、ポート 9443 でこの IP アドレスにアクセスして管理ノード UI を開きます。

```
https://<mNode 11.1 IP address>:9443
```

6. vSphere で、 * NetApp Element Configuration * > * mNode Settings * の順に選択します。（旧バージョンでは、最上位のメニューは * NetApp SolidFire 構成 * です）。
7. * アクション * > * クリア * を選択します。
8. 確認するには、 * はい * を選択します。mNode Status フィールドに Not Configured と表示されるはずです。

> 最初に「 * mNode Settings * 」タブに移動すると、 mNode の Status フィールドに、想定される「 Up * 」ではなく「 * Not Configured * 」と表示されることがあります。 * Actions * > * Clear * を選択できない場合があります。ブラウザの表示を更新します。mNode の Status フィールドには、最終的に **up** と表示されます。

9. vSphere からログアウトします。
10. Web ブラウザで、管理ノード登録ユーティリティを開き、 * QoSSIOC サービス管理 * を選択します。

```
https://<mNode 11.1 IP address>:9443
```

11. QoSSIOC の新しいパスワードを設定します。

> デフォルトのパスワードは SolidFire ですこのパスワードは、新しいパスワードを設定するために必要です。

12. [* vCenter Plug-in Registration * （ vCenter Plug-in の登録 * ）] タブを選択します。
13. [プラグインの更新] を選択します。
14. 必要な値を入力します。完了したら、 * アップデート * を選択します。
15. vSphere にログインし、 * NetApp Element 構成 * > * mNode 設定 * を選択します。
16. * アクション * > * 設定 * を選択します。
17. 管理ノードの IP アドレス、管理ノードのユーザ ID （ユーザ名は「 admin 」）、登録ユーティリティの「 QoSSIOC サービス管理 * 」タブで設定したパスワード、および vCenter のユーザ ID とパスワードを入力します。

    vSphere で、 mNode 設定 * タブに mNode ステータスが * up * と表示されます。これは、管理ノード 11.1 が vCenter に登録されていることを示します。

18. 管理ノード登録ユーティリティ（「 https://<mNode 11.1 IP アドレス > ： 9443 」）から SIOC サービスを再起動します。

19. 1 分ほど待ってから、「 * NetApp Element Configuration * > * mNode Settings * 」タブを確認します。mNode のステータスが「 * up 」と表示されるはずです。

    ステータスが「 * down 」の場合は、「 /sf/packages/sioc/app.properties` 」の権限を確認します。ファイル所有者には、読み取り、書き込み、および実行の各権限が必要です。正しい権限は次のように表示されます。

    ```
    -rwx------
    ```

20. SIOC プロセスが開始され、 vCenter で mNode のステータスが「 up 」と表示されたら、管理ノードの「 f—hci-nma 」サービスのログを確認します。エラーメッセージは表示されません。

21. （管理ノード 11.1 の場合のみ） root 権限で管理ノードバージョン 11.1 に SSH 接続し、次のコマンドを使用して NMA サービスを開始します。

    ```
    # systemctl enable /sf/packages/nma/systemd/sf-hci-nma.service
    ```

    ```
    # systemctl start sf-hci-nma21
    ```

22. vCenter から、ドライブの削除、ドライブの追加、またはノードのリブートを実行します。これによりストレージアラートがトリガーされ、 vCenter で報告されます。アラートが生成されれば、 NMA システムアラートは想定どおりに機能しています。

23. ONTAP Select が vCenter に設定されている場合、前の管理ノードの「 .ots.properties` 」ファイルを管理ノードバージョン 11.1x/sf/packages/NMA /conf/.ots.properties` ファイルにコピーして NMA で ONTAP Select アラートを設定し、次のコマンドを使用して NMA サービスを再起動します。

    ```
    systemctl restart sf-hci-nma
    ```

24. 次のコマンドを使用してログを表示し、 ONTAP Select が動作していることを確認します。

    ```
    journalctl -f | grep -i ots
    ```

25. 次の手順で Active IQ を設定します。

    a. 管理ノードバージョン 11.1 に SSH 接続し "/sf/packages/collector' ディレクトリに移動します

    b. 次のコマンドを実行します。

    ```
    sudo ./manage-collector.py --set-username netapp --set-password --set
    -mvip <MVIP>
    ```

    c. プロンプトが表示されたら、管理ノード UI のパスワードを入力します。

    d. 次のコマンドを実行します。

```
./manage-collector.py --get-all
```

```
sudo systemctl restart sfcollector
```

e. 「 fcollector 」ログを確認し、正常に動作していることを確認します。

26. vSphere で、 * NetApp Element Configuration * > * mNode Settings * タブに mNode ステータスが * up * と表示される必要があります。
27. NMA からシステムアラートと ONTAP Select アラートが報告されていることを確認します。
28. すべての動作が想定どおりであることを確認したら、管理ノード 10.x の VM をシャットダウンして削除します。

管理ノード **REST API** を使用して認証を再設定します

既存の管理ノードは、（1）管理サービスと（2） Element ストレージを順番にアップグレードした場合でも維持できます。別のアップグレード順序を使用した場合は、インプレース管理ノードのアップグレード手順を参照してください。

作業を開始する前に

- 管理サービスを 2.10.29 以降に更新しておきます。
- ストレージクラスタで Element 12.0 以降が実行されている。
- 管理ノードは 11.3 以降です。
- 管理サービスを順番に更新し、 Element ストレージをアップグレードしておきます。この手順を使用して認証を再設定するには、説明されている順序でアップグレードを完了する必要があります。

手順

1. 管理ノードで管理ノード REST API UI を開きます。

```
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. 値がまだ入力されていない場合は、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。
3. REST API UI から、 * POST /services/reconfigure -auth* を選択します。
4. [* 試してみてください *] を選択します。
5. *LOAD_images * パラメータでは 'TRUE' を選択します
6. [* Execute] を選択します。

   応答の本文は、再設定が正常に完了したことを示します。

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"
- "NetApp HCI のリソースページ"

Element Plug-in for vCenter Server をアップグレードします

既存のvSphere環境にNetApp Element Plug-in for VMware vCenter Serverが登録されている場合は、プラグインサービスが含まれている管理サービスパッケージを最初に更新したあとで、プラグインの登録を更新できます。

登録ユーティリティを使用して、 vCenter Server Virtual Appliance （ vCSA ）または Windows でプラグインの登録を更新できます。vCenter Plug-in の登録変更は、プラグインを使用するすべての vCenter Server で行う必要があります。

> 管理サービス2.22.7には、リモートプラグインを含むElement Plug-in for vCenter Server 5.0が含まれています。Elementプラグインを使用する場合は、ローカルプラグインのサポートを削除するVMwareの指示に従って、管理サービス2.22.7以降にアップグレードする必要があります。 "詳細はこちら。"。

vCenter 5.0以降向けElementプラグイン

このアップグレード手順では、次のアップグレードシナリオについて説明します。

- Element Plug-in for vCenter Server 5.2、5.1、または5.0にアップグレードする。
- HTML5 vSphere Web Client 8.0または7.0にアップグレードする。

> Element Plug-in for vCenter 5.0以降はvCenter Server 6.7および6.5と互換性がありません。

> Element Plug-in for vCenter Server 4.xを5.xにアップグレードすると、vCenterインスタンスからリモートプラグインにデータをコピーできないため、プラグインが設定されているクラスタは失われます。クラスタをリモートプラグインに再度追加する必要があります。これは、ローカルプラグインからリモートプラグインにアップグレードする場合の1回限りのアクティビティです。

vCenter 4.10以前のElementプラグイン

このアップグレード手順では、次のアップグレードシナリオについて説明します。

- Element Plug-in for VMware vCenter Server 4.10、4.9、4.8、4.7、4.6にアップグレードする場合 4.5または4.4。
- 7.0 、 6.7 、または 6.5 の HTML5 vSphere Web Client にアップグレードする。

- このプラグインは、VMware vCenter Server 4.x向けVMware vCenter Server 8.0 for Element Plug-inと互換性がありません
- このプラグインは、VMware vCenter Server 6.5 for Element Plug-in for VMware vCenter Server 4.6、4.7、および4.8とは互換性がありません。

- 6.7 Flash vSphere Web Client にアップグレードする。

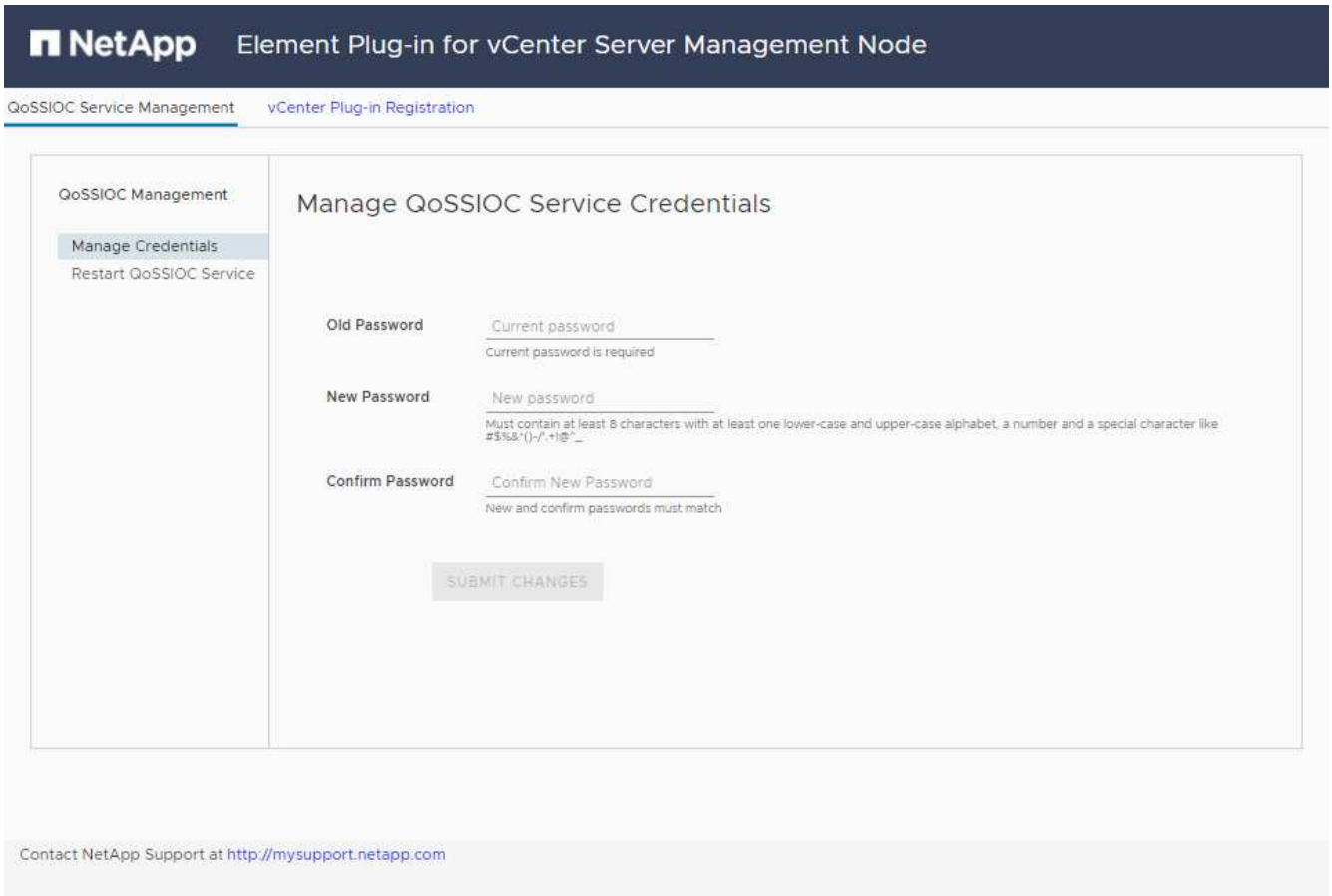
> このプラグインは、 HTML5 vSphere Web Client バージョン 6.7 U2 ビルド 13007421 および更新 2a より前にリリースされたその他の 6.7 U2 ビルド（ビルド 13643870 ）とは互換性がありません。サポートされる vSphere のバージョンの詳細については、のリリースノートを参照してください "プラグインのバージョン"。

必要なもの

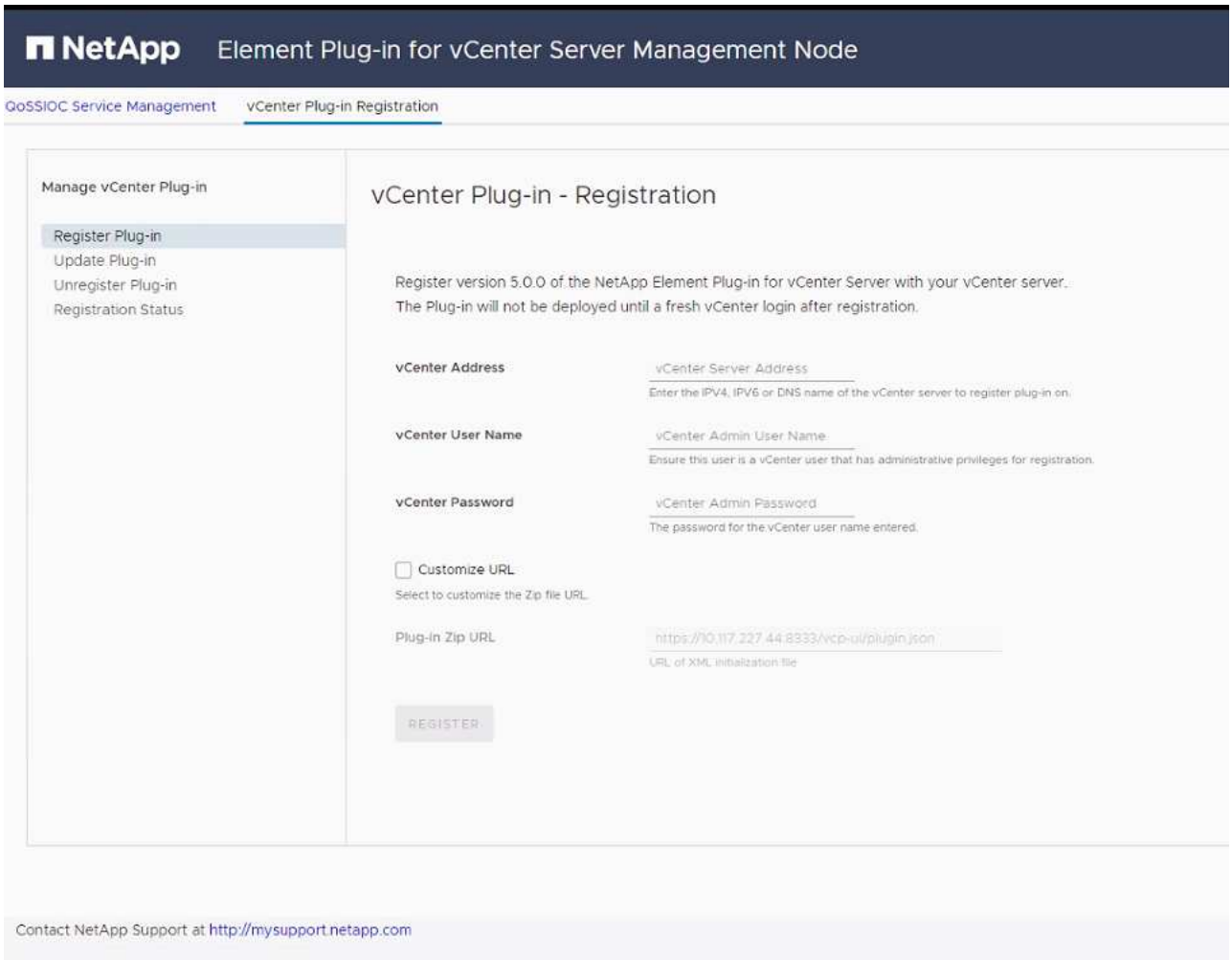
- * 管理者権限 * ：プラグインをインストールするための vCenter Administrator ロールの権限があります。
- * vSphere のアップグレード * ： NetApp Element Plug-in for vCenter Server をアップグレードする前に、必要な vCenter のアップグレードを実行しておきます。以下の手順は、 vCenter のアップグレードが完了していることを前提としています。
- * vCenter Server ：**vCenter Plug-in**バージョン**5.x**または**4.x**が**vCenter Server**に登録されている。登録ユーティリティを使用します (**`https://[management node IP]:9443`**）で、 Registration Status を選択し、必要なフィールドに情報を入力して Check Status *を選択し、vCenter Plug-inがすでに登録されていること、および現在のインストールバージョン番号を確認します。
- * 管理サービスの更新 * ：を更新しました "管理サービスのバンドル" を最新バージョンに更新します。vCenter プラグインの更新は、 NetApp HCI のメジャー製品リリース以外でリリースされた管理サービスの更新を使用して配布されます。
- 管理ノードのアップグレード：
  - Element vCenterプラグイン5.0以降では、これまで管理ノードを実行しています "アップグレード済み" をバージョン12.3.x以降にアップグレードします。
  - Element vCenterプラグイン4.4～4.10では、以前から管理ノードを実行しています "アップグレード済み" バージョン 11.3 以降。vCenter Plug-in 4.4以降では、個別のサービスを提供するモジュラアーキテクチャを備えた11.3以降の管理ノードが必要です。管理ノードの電源をオンにして IP アドレスまたは DHCP アドレスを設定しておく必要があります。
- * Elementストレージのアップグレード*：
  - Element vCenterプラグイン5.0以降では、NetApp Element ソフトウェア12.3.x以降を実行するクラスタが必要です。
  - Element vCenterプラグイン4.10以前では、NetApp Element ソフトウェア11.3以降を実行するクラスタが必要です。
- * vSphere Web Client * ：プラグインのアップグレードを開始する前に vSphere Web Client からログアウトしました。Web Client からログアウトしないと、このプロセスで行ったプラグインへの更新が認識されません。

手順

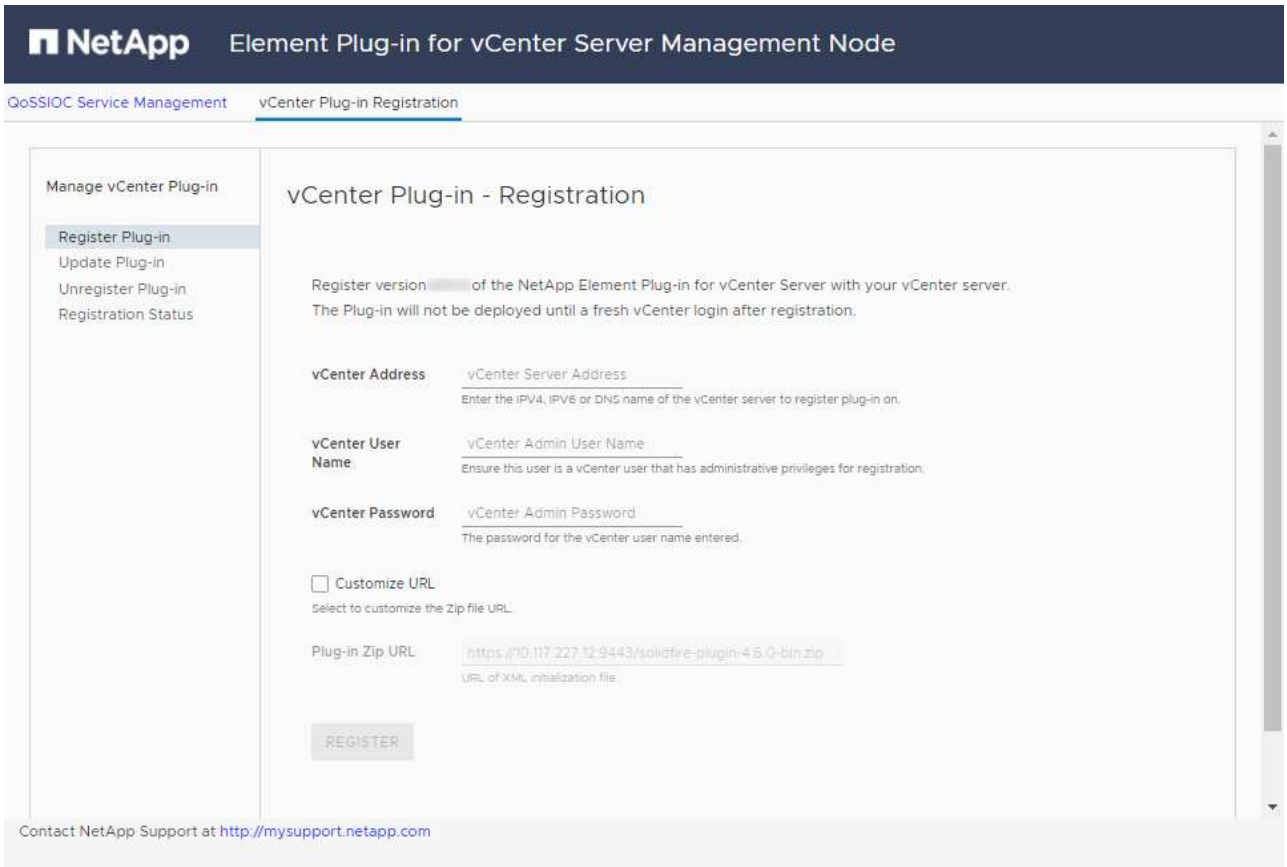
1. ブラウザに管理ノードの IP アドレスを入力します。登録用の TCP ポート「 https://[management node ip 」： 9443 でこのプラグインの登録ユーティリティ UI が開き、「 Manage QoSSIOC Service Credentials * 」ページが表示されます。



2. vCenter Plug-in Registration * を選択します。
   - Element Plug-in for vCenter Server 5.xの[vCenter Plug-in Registration]ページ：



- Element Plug-in for vCenter Server 4.10以前のvCenter Plug-inの登録ページ：



3. Manage vCenter Plug-in * で、 * Update Plug-in * を選択します。
4. 次の情報を確認し、必要に応じて更新します。
   a. プラグインを登録する vCenter サービスの IPv4 アドレスまたは FQDN 。
   b. vCenter Administrator のユーザ名。

      vCenter Administrator ロールの権限を持つユーザのユーザ名とパスワードを入力する必要があります。

   c. vCenter Administrator のパスワード。
   d. （社内サーバ/ダークサイトの場合）Element Plug-in for vCenterのバージョンに応じて、プラグインのJSONファイルまたはプラグインのZIPのカスタムURL：
      i. Element Plug-in for vCenter Server 5.0以降、プラグインのJSONファイルのカスタムURL。

         HTTPまたはHTTPSサーバ（ダークサイト）を使用している場合、またはJSONファイル名やネットワーク設定を変更した場合は、「* Custom URL *」を選択してURLをカスタマイズできます。URL をカスタマイズする場合の追加の設定手順については、社内（ダークサイト）の HTTP サーバの vCenter プロパティの変更に関する Element Plug-in for vCenter Server のドキュメントを参照してください。

      ii. Element Plug-in for vCenter Server 4.10以前の場合は、プラグインのZIPのカスタムURL。

> HTTP または HTTPS サーバ（ダークサイト）を使用している場合、または ZIP ファイル名やネットワーク設定を変更した場合は、「 * Custom URL * 」を選択して URL をカスタマイズできます。URL をカスタマイズする場合の追加の設定手順については、社内（ダークサイト）の HTTP サーバの vCenter プロパティの変更に関する Element Plug-in for vCenter Server のドキュメントを参照してください。

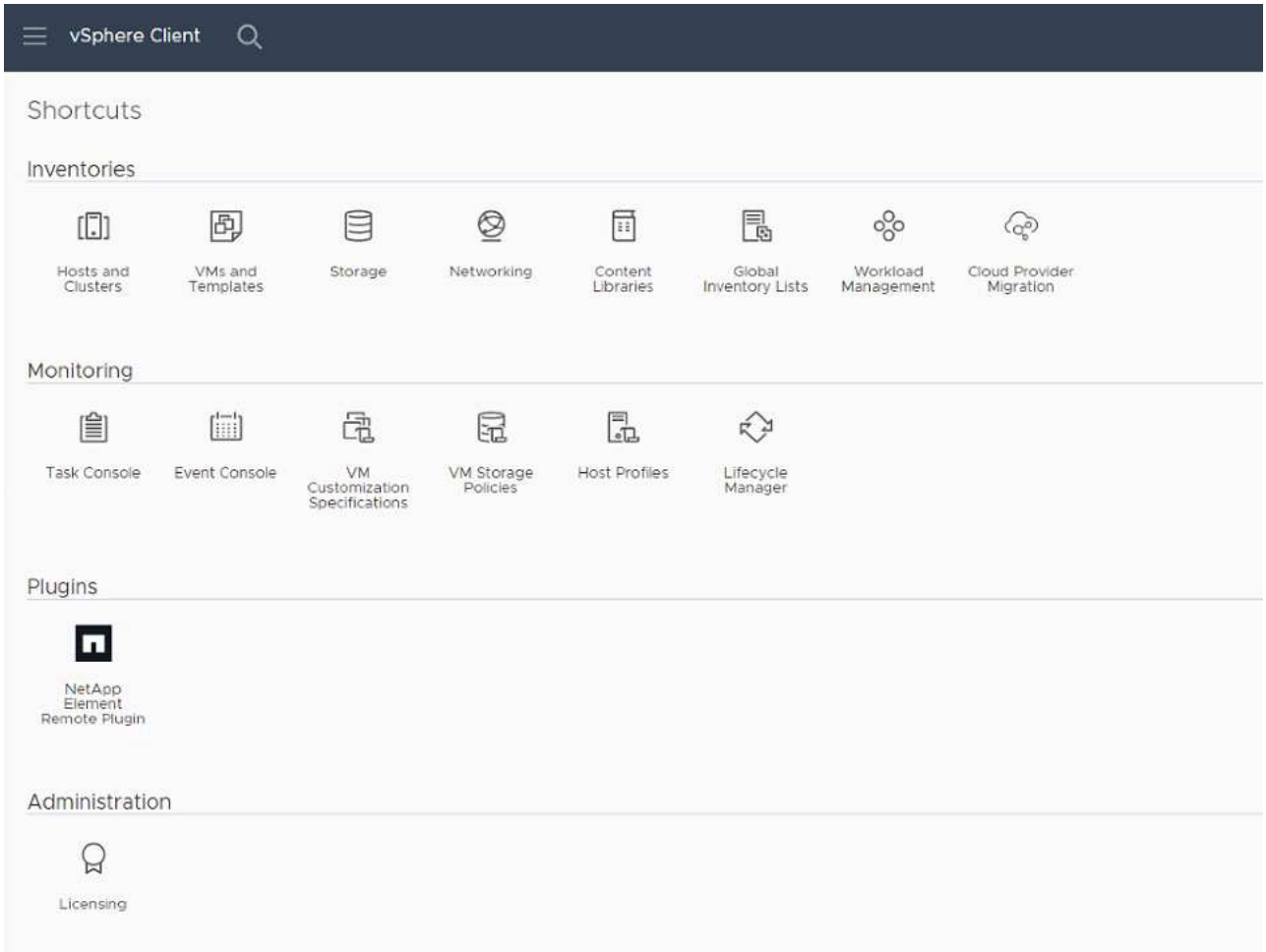
5. 「 * Update * 」を選択します。

   登録が完了すると、登録ユーティリティの UI にバナーが表示されます。

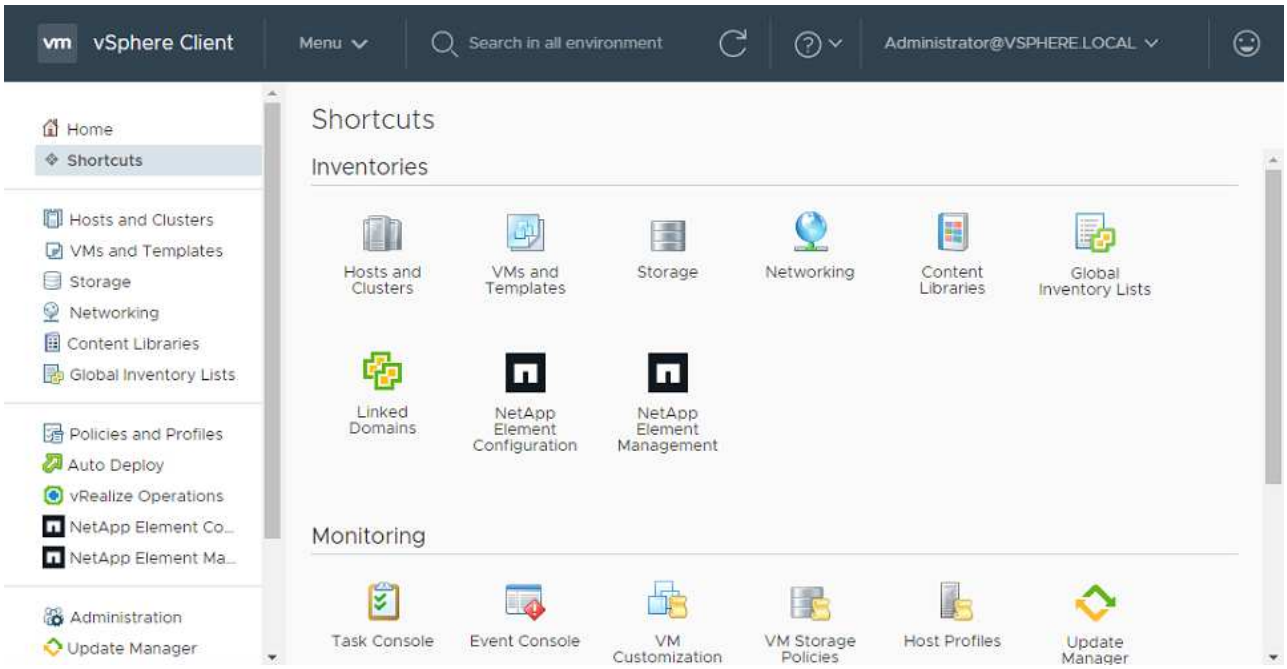
6. vSphere Web Client に vCenter Administrator としてログインします。vSphere Web Client にすでにログインしている場合は、ログアウトし、 2~3 分待ってから再度ログインする必要があります。

   > この操作により、新しいデータベースが作成され、 vSphere Web Client でのインストールが完了します。

7. vSphere Web Client で、タスクモニタで次のタスクが完了していることを確認します。「ダウンロードプラグイン」および「デプロイプラグイン」。
8. vSphere Web Clientの* Shortcuts *タブとサイドパネルにプラグインの拡張ポイントが表示されていることを確認します。
   - Element Plug-in for vCenter Server 5.0以降では、NetApp Element リモートプラグイン拡張ポイントが表示されます。



- Element Plug-in for vCenter Server 4.10以前では、NetApp Element Configuration and Management拡張ポイントが表示されます。



> vCenter Plug-in のアイコンが表示されない場合は、を参照してください "vCenter Server 向け Element プラグイン" プラグインのトラブルシューティングに関するドキュメント。
>
> VMware vCenter Server 6.7U1を使用してNetApp Element Plug-in for vCenter Server 4.8以降にアップグレードしたあとに、ストレージクラスタが表示されないか、NetApp Element構成の「クラスタ」および「QoSSIOC設定*」のセクションにサーバエラーが表示される場合は、を参照してください "vCenter Server 向け Element プラグイン" これらのエラーのトラブルシューティングに関するドキュメント。

9. プラグインの * NetApp Element 構成 * 拡張ポイントの * バージョン情報 * タブでバージョンの変更を確認します。

   次のバージョンの詳細またはより新しいバージョンの詳細が表示されます。

```
NetApp Element Plug-in Version: 5.2
NetApp Element Plug-in Build Number: 12
```

> vCenter Plug-in には、オンラインヘルプが用意されています。ヘルプの最新のコンテンツが読み込まれるようにするために、プラグインをアップグレードしたあとにブラウザキャッシュをクリアしてください。

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"
- "NetApp HCI のリソースページ"

コンピューティングノードの健全性チェックは、コンピューティングファームウェアをアップグレードする前に実行します

コンピューティングファームウェアをアップグレードする前に健全性チェックを実行して、クラスタ内のすべてのコンピューティングノードをアップグレードする準備ができていることを確認する必要があります。コンピューティングノードの健全性チェックは、管理対象の 1 つ以上の NetApp HCI コンピューティングノードのコンピューティングクラスタに対してのみ実行できます。

必要なもの

- 管理サービス：最新の管理サービスバンドル（2.11以降）に更新しました。
- 管理ノード：管理ノード11.3以降を実行していることを確認します。
- * 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以降が実行されている必要があります。
- エンドユーザライセンス契約（**EULA**）：管理サービス2.20.69以降では、NetApp Hybrid Cloud ControlのUIまたはAPIを使用してコンピューティングノードの健全性チェックを実行する前に、EULAに同意して保存する必要があります。
  a. Webブラウザで管理ノードのIPアドレスを開きます。

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

  b. 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。
  c. インターフェイスの右上にある [* Upgrade] を選択します。
  d. EULAがポップアップ表示されます。下にスクロールして、[現在および今後のすべての更新を許可する*]を選択し、[保存*]を選択します。

健全性チェックのオプション

健全性チェックは、NetApp Hybrid Cloud ControlのUIまたはNetApp Hybrid Cloud ControlのAPIを使用して実行できます。

- NetApp Hybrid Cloud Control を使用して、コンピューティングノードの健全性を実行します ファームウェアをアップグレードする前にチェックします （推奨方法）
- 前にコンピューティングノードの健全性チェックを実行するには、 API を使用します ファームウェアをアップグレード中です

また、サービスで実行されるコンピューティングノードの健全性チェックの詳細も確認できます。

- [コンピューティングノードの健全性チェックはサービスによる機能で]

NetApp Hybrid Cloud Control を使用して、コンピューティングノードの健全性を実行します ファームウェアをアップグレードする前にチェックします

NetApp Hybrid Cloud Controlを使用して、コンピューティングノードでファームウェアをアップグレードする準備ができているかどうかを確認できます。

> 2 ノードのストレージクラスタ構成が複数ある場合は、それぞれ独自の vCenter 内で、監視ノードの健全性チェックで正確なレポートが行われないことがあります。そのため、 ESXi ホストをアップグレードする準備ができたら、アップグレードする ESXi ホスト上の監視ノードのみをシャットダウンする必要があります。別の方法で監視ノードの電源をオフにして、 NetApp HCI 環境で常に 1 つの監視ノードが実行されていることを確認する必要があります。

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。

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

2. 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。
3. インターフェイスの右上にある [* Upgrade] を選択します。
4. [* Upgrades] ページで、 [* Compute firmware*] タブを選択します。
5. 健全性チェックを選択します アップグレードの準備状況を確認するクラスタ
6. [* コンピュートヘルスチェック *] ページで、 [* ヘルスチェックの実行 *] を選択します。
7. 問題がある場合は、ページにレポートが表示されます。次の手順を実行します。
   a. 各問題について記載されている特定の技術情報アーティクルに移動するか、指定された対処方法を実行します。
   b. KB を指定した場合は、関連する技術情報アーティクルに記載されているプロセスを完了します。
   c. クラスタの問題を解決したら、「 * Re-Run Health Check * 」を選択します。

健全性チェックがエラーなく完了すると、クラスタ内のコンピューティングノードをアップグレードする準備が整います。を参照してください "コンピューティングノードのファームウェアを更新します" 続行してください。

前にコンピューティングノードの健全性チェックを実行するには、 **API** を使用します ファームウェアをアップグレード中です

REST API を使用して、クラスタ内のコンピューティングノードをアップグレードする準備ができているかどうかを確認できます。健全性チェックでは、 ESXi ホストの問題や vSphere のその他の問題など、アップグレード時の問題がないことを確認します。環境内の各コンピューティングクラスタについて、コンピューティングノードの健全性チェックを実行する必要があります。

手順

1. コントローラ ID とクラスタ ID を確認します。
   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. 値がまだ入力されていない場合は、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。
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 ' ヘルス・チェックに使用するインストールの "id" をコピーします
g. REST API UI から、 * Get 操作対象の一時リソース / ｛ 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 ID を入力します。
j. [* Execute] を選択します。
k. コード 200 の応答本文から、次のそれぞれの ID をコピーします。
    i. クラスタ ID （「 ClusterId 」）
    ii. コントローラ ID （「 ControllerID 」）

```
{
  "_links": {
    "collection":
"https://10.117.187.199/inventory/1/installations",
    "self":
"https://10.117.187.199/inventory/1/installations/xx94f6f0-12a6-
412f-8b5e-4cf2z58329x0"
  },
  "compute": {
    "errors": [],
    "inventory": {
      "clusters": [
        {
          "clusterId": "domain-1",
          "controllerId": "abc12c3a-aa87-4e33-9f94-xx588c2cdcf6",
          "datacenterName": "NetApp-HCI-Datacenter-01",
          "installationId": "xx94f6f0-12a6-412f-8b5e-
4cf2z58329x0",
          "installationName": "test-nde-mnode",
          "inventoryType": "managed",
          "name": "NetApp-HCI-Cluster-01",
          "summary": {
            "nodeCount": 2,
            "virtualMachineCount": 2
          }
        }
      ],
```

2. クラスタ内のコンピューティングノードで健常性チェックを実行します。
   a. 管理ノードでコンピューティングサービス REST API UI を開きます。

      ```
      https://<ManagementNodeIP>/vcenter/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. 値がまだ入力されていない場合は、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。
   c. [* POST/compute/Patlein/{controller_ID} 一致 / 正常性チェック *] を選択します。
   d. [* 試してみてください *] を選択します。
   e. 前の手順からコピーした「 ControllerID 」を「 * Controller_ID * 」パラメータフィールドに入力します。

f. ペイロードで、前の手順から「 cluster 」の値としてコピーした「 clusterId 」を入力し、「 nodes 」パラメータを削除します。

```
{
  "cluster": "domain-1"
}
```

g. クラスタの健全性チェックを実行するには、 * Execute * を選択します。

コード 200 の応答では ' 状態チェックの結果を確認するために必要なタスク ID が追加された 'resourceLink' URL が提供されます

```
{
  "resourceLink": "https://10.117.150.84/vcenter/1/compute/tasks/[This
is the task ID for health check task results]",
  "serviceName": "vcenter-v2-svc",
  "taskId": "ab12c345-06f7-42d7-b87c-7x64x56x321x",
  "taskName": "VCenter service health checks"
}
```

a. 「 resourceLink 」 URL のタスク ID 部分をコピーして、タスクの結果を確認します。

3. 健全性チェックの結果を確認します。

a. 管理ノードのコンピューティングサービス REST API UI に戻ります。

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

b. [**Get/computeTole/tasks/{tasks_id}**] を選択します。

c. [* 試してみてください *] を選択します。

d. 「 task_id 」パラメータフィールドに、「 resourceLink 」 URL のタスク ID 部分を *POST/computeTouled/{controller_ID} の一時的なチェック / 正常性チェック *code 200 応答から入力します。

e. [* Execute] を選択します。

f. [ステータス] が表示され、コンピューティングノードの正常性に問題があることが示された場合は、次の手順を実行します。

i. 各問題について記載されている特定の KB 記事 (`KbLink') に移動するか、指定された対処方法を実行します。

ii. KB を指定した場合は、関連する技術情報アーティクルに記載されているプロセスを完了します。

iii. クラスタの問題を解決したら、 * POST /computeates/ ｛ controller_ID ｝ の一時的な不具合 / 健全性チェック * を再度実行します（手順 2 を参照）。

健全性チェックが問題なく完了した場合は、応答コード 200 が成功したことを示します。

コンピューティングノードの健全性チェックはサービスによる機能で

NetApp Hybrid Cloud ControlまたはAPIのどちらのメソッドで実行したかに関係なく、ノードごとに次のチェックを実行します。環境によっては、一部のチェックが省略されることがあります。検出された問題を解決したあとに、健全性チェックを再実行する必要があります。

説明を確認します	ノード / クラスタ	解決に必要なアクション	手順が記載された技術情報アーティクル
DRS は有効で、完全に自動化されているか。	クラスタ	DRS をオンにして、完全に自動化されていることを確認します。	"こちらの技術情報をご覧ください"。注：標準ライセンスを使用している場合は、 ESXi ホストをメンテナンスモードにし、ヘルスチェックのエラーに関する警告を無視してください。
DPM は vSphere で無効になっていますか。	クラスタ	Distributed Power Management をオフにします。	"こちらの技術情報をご覧ください"。
vSphere で HA アドミッション制御が無効になっているか。	クラスタ	HA アドミッション制御をオフにします。	"こちらの技術情報をご覧ください"。
クラスタ内のホストで VM の FT が有効になっているかどうか	ノード	影響を受けるすべての仮想マシンでフォールトトレランスを一時停止します。	"こちらの技術情報をご覧ください"。
クラスタの重要なアラームは vCenter にありますか。	クラスタ	vSphere を起動し、アラートを解決または承認してから処理を進めてください。	問題を解決するために KB は必要ありません。
vCenter には汎用 / グローバル情報アラートがありますか。	クラスタ	vSphere を起動し、アラートを解決または承認してから処理を進めてください。	問題を解決するために KB は必要ありません。
管理サービスは最新ですか？	HCI システム	アップグレードまたはアップグレード前の健全性チェックを実行する前に、管理サービスを更新する必要があります。	問題を解決するために KB は必要ありません。を参照してください "この記事では" を参照してください。
vSphere の現在の ESXi ノードでエラーが発生していますか？	ノード	vSphere を起動し、アラートを解決または承認してから処理を進めてください。	問題を解決するために KB は必要ありません。
仮想メディアがクラスタ内のホスト上の VM にマウントされているか。	ノード	すべての仮想メディアディスク（ CD/DVD またはフロッピー）を VM からアンマウントします。	問題を解決するために KB は必要ありません。

説明を確認します	ノード / クラスタ	解決に必要なアクション	手順が記載された技術情報アーティクル
BMC バージョンは、Redfish でサポートされている最小要件バージョンですか。	ノード	BMC ファームウェアを手動で更新します。	問題を解決するために KB は必要ありません。
ESXi ホストは稼働していますか？	ノード	ESXi ホストを起動します。	問題を解決するために KB は必要ありません。
ローカルの ESXi ストレージに仮想マシンがありますか。	ノード / VM	仮想マシンに接続されたローカルストレージを削除または移行します。	問題を解決するために KB は必要ありません。
BMC は稼働していますか？	ノード	BMC の電源をオンにして、この管理ノードからアクセス可能なネットワークに接続しておきます。	問題を解決するために KB は必要ありません。
利用可能なパートナー ESXi ホストがあるか？	ノード	仮想マシンを移行するには、クラスタ内の 1 つ以上の ESXi ホストを使用可能な状態にします（保守モードではありません）。	問題を解決するために KB は必要ありません。
IPMI プロトコルで BMC に接続できますか？	ノード	ベースボード管理コントローラ（ BMC ）で IPMI プロトコルを有効にします。	問題を解決するために KB は必要ありません。
ESXi ホストがハードウェアホスト（ BMC ）に正しくマッピングされているか。	ノード	ESXi ホストがベースボード管理コントローラ（ BMC ）に正しくマッピングされていません。ESXi ホストとハードウェアホストの間のマッピングを修正します。	問題を解決するために KB は必要ありません。を参照してください "この記事では" を参照してください。
クラスタ内の監視ノードのステータスは何ですか。特定された監視ノードが実行されていません。	ノード	監視ノードは、代替 ESXi ホストでは実行されません。代替 ESXi ホストで監視ノードの電源をオンにし、健全性チェックを再実行します。* HCI 環境では、監視ノードが常に 1 つ実行されている必要があります。 *	"こちらの技術情報をご覧ください"

説明を確認します	ノード / クラスタ	解決に必要なアクション	手順が記載された技術情報アーティクル
クラスタ内の監視ノードのステータスは何ですか。この ESXi ホストで監視ノードが起動して実行されており、代替監視ノードが起動されて実行されていません。	ノード	監視ノードは、代替 ESXi ホストでは実行されません。代替 ESXi ホストで監視ノードの電源をオンにします。この ESXi ホストをアップグレードする準備ができたら、この ESXi ホストで実行されている監視ノードをシャットダウンし、健全性チェックを再実行してください。* HCI 環境では、監視ノードが常に 1 つ実行されている必要があります。 *	"こちらの技術情報をご覧ください"
クラスタ内の監視ノードのステータスは何ですか。監視ノードはこの ESXi ホストで実行されており、代替ノードは稼働しているが、同じ ESXi ホストで実行されている。	ノード	この ESXi ホストで両方の監視ノードが実行されています。1 つの監視ノードを代替 ESXi ホストに再配置します。この ESXi ホストをアップグレードする準備ができたら、この ESXi ホストに残っている監視ノードをシャットダウンして健常性チェックを再実行します。* HCI 環境では、監視ノードが常に 1 つ実行されている必要があります。 *	"こちらの技術情報をご覧ください"
クラスタ内の監視ノードのステータスは何ですか。監視ノードがこの ESXi ホストで実行されており、別の監視ノードが別の ESXi ホストで実行されています。	ノード	監視ノードは、この ESXi ホスト上でローカルに実行されています。この ESXi ホストをアップグレードする準備ができたら、この ESXi ホストでのみ監視ノードをシャットダウンして健常性チェックを再実行してください。* HCI 環境では、監視ノードが常に 1 つ実行されている必要があります。 *	"こちらの技術情報をご覧ください"

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"
- "NetApp HCI のリソースページ"

コンピューティングノードのドライバを更新

H シリーズのコンピューティングノードでは、ノードで使用されているドライバを VMware Update Manager を使用して更新できます。

必要なもの

お使いのハードウェアのファームウェアとドライバのマトリックスを参照してください "サポートされているファームウェアおよびESXiドライバのバージョン"。

このタスクについて

以下の更新処理は一度に 1 つずつ実行します。

ファームウェアのアップグレードを実行する前に、 ESXi ドライバの現在のバージョンを確認する必要があります。ドライバが最新でない場合は、まずドライバをアップグレードします。その後、コンピューティングノードのコンピューティングファームウェアをアップグレードします。

手順

1. を参照します "NetApp HCI ソフトウェアのダウンロード" ページに移動し、正しいバージョンの NetApp HCI のダウンロードリンクを選択します。
2. ドロップダウンリストから * esxi_drivers * を選択します。
3. エンドユーザライセンス契約に同意します。
4. 使用しているノードタイプと ESXi バージョンに対応したドライバパッケージをダウンロードします。
5. ダウンロードしたドライババンドルをローカルコンピュータに展開します。

   ネットアップのドライババンドルには、 VMware オフラインバンドルの ZIP ファイルが 1 つ以上含まれています。これらの ZIP ファイルは展開しないでください。

6. VMware vCenter の * VMware Update Manager * にアクセスします。
7. コンピューティングノードのドライバオフラインバンドルファイルを * パッチリポジトリ * にインポートします。
   - VMware ESXi 7.0 では、 NetApp H610C 、 H615C 、 H410C 、および Hx00E コンピューティングノードとそのビルドインシステムコンポーネントに必要なすべてのドライバが、 VMware ESXi 7.0 の標準のインストール ISO イメージに含まれています。VMware ESXi 7.0 （および更新）を実行する NetApp HCI コンピューティングノードのドライバを追加または更新する必要はありません。
   - VMware ESXi 6.x の場合、次の手順を実行して、ドライバのオフラインバンドルファイルをインポートします。
     i. [* アップデート * （ Updates * ）] タブを選択します。
     ii. 「 * ファイルからアップロード」を選択します。
     iii. 以前にダウンロードしたオフラインバンドルを参照し、 * import * を選択します。
8. コンピューティングノードの新しいホストベースラインを作成します。
9. 名前とタイプに * Host Extension * を選択し、インポートされたすべてのドライバパッケージを新しいベースラインに含めるように選択します。
10. vCenter の * Host and Clusters * メニューで、更新するコンピュートノードを含むクラスタを選択し、 * Update Manager * タブに移動します。

11. [* 修正（ Remediate* ）] を選択し、新しく作成したホストベースラインを選択します。ベースラインに含まれるドライバが選択されていることを確認します。
12. ウィザードの指示に従って、 * Host Remediation Options * に進み、ドライバの更新中に仮想マシンをオンラインの状態に保つために、 * Do Not Change VM Power State * オプションが選択されていることを確認します。

> クラスタで VMware DRS （ Distributed Resource Scheduler ）が有効になっている場合（ NetApp HCI 環境のデフォルト）、仮想マシンはクラスタ内の他のノードに自動的に移行されます。

13. ウィザードの [*Ready to Complete] ページに進み、 [*Finish] を選択します。

    クラスタ内のすべてのコンピューティングノードのドライバが、仮想マシンはオンラインのまま、一度に 1 ノードずつ更新されます。

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 のリソースページ"

コンピューティングノードのファームウェアをアップグレードします

H シリーズコンピューティングノードの場合は、 BMC 、 BIOS 、 NIC などのハードウェアコンポーネントのファームウェアをアップグレードできます。コンピューティングノードのファームウェアをアップグレードするには、 NetApp Hybrid Cloud Control の UI 、 REST API 、最新のファームウェアイメージを含む USB ドライブ、または BMC UI を使用します。

アップグレード後、コンピューティングノードは ESXi でブートされ、以前と同様に動作します。設定は保持されます。

必要なもの

- * コンピューティングドライバ * ：コンピューティングノードのドライバをアップグレードしておきます。コンピューティングノードのドライバが新しいファームウェアと互換性がない場合、アップグレードは開始されません。を参照してください "Interoperability Matrix Tool （ IMT ）" ドライバとファームウェアの互換性情報については、最新のを参照してください "コンピューティングノードのファームウェアリリースノート" 最新のファームウェアやドライバに関する重要な詳細情報を確認できます。
- * admin 権限 * ：アップグレードを実行するには、クラスタ管理者権限と BMC 管理者権限が必要です。
- * システムポート * ： NetApp Hybrid Cloud Control をアップグレードに使用している場合は、必要なポートが開いていることを確認しておきます。を参照してください "ネットワークポート" を参照してください。
- * BMC および BIOS の最小バージョン * ： NetApp Hybrid Cloud Control を使用してアップグレードするノードが、次の最小要件を満たしていることを確認します。

モデル	**BMC** の最小バージョン	**BIOS** の最小バージョン
H410Cでし た	サポートされているすべてのバージョン（アップグレードは不要）に一致しました	サポートされているすべてのバージョン（アップグレードは不要）に一致しました
H610C</Z1> グループ	3.96.07	3B01
H615CFCLSH.(チベ	4.68.07	3B08 。 CO の一酸化

> H615C コンピューティングノードでは、 BMC ファームウェアをバージョン 4.68 に更新する必要があります を使用する "ファームウェアバンドル 2.27 を計算します" NetApp Hybrid Cloud Control で今後のファームウェアアップグレードを実行できるようにするため。

> ご使用のハードウェアのファームウェアとドライバのファームウェアの一覧については、を参照してください "サポートされているファームウェアおよびESXiドライバのバージョン"。

- *BIOS 起動順序 *: 各ノードの BIOS セットアップで起動順序を手動で変更して、起動リストに「 USB CD/DVD」 が表示されるようにします。を参照してください "記事" を参照してください。
- * BMC クレデンシャル * ： NetApp Hybrid Cloud Control がコンピューティングノードの BMC への接続に使用するクレデンシャルを更新します。これは、ネットアップのハイブリッドクラウドを使用して実行できます 制御 "UI" または "API"。アップグレード前に BMC 情報を更新すると、インベントリが更新され、アップグレードの完了に必要なすべてのハードウェアパラメータが管理ノードサービスで認識されるようになります。
- * 接続されているメディア * ：コンピューティングノードのアップグレードを開始する前に、物理 USB または ISO の接続をすべて解除してください。
- * KVM ESXi コンソール * ：コンピューティングノードのアップグレードを開始する前に、 BMC UI で開いているすべての Serial-Over-LAN （ SOL ）セッションとアクティブな KVM セッションを閉じます。
- * 監視ノードの要件 * ： 2 ノードおよび 3 ノードのストレージクラスタでは、 1 つ "監視ノード" 常に NetApp HCI インストール環境で実行しておく必要があります。
- * コンピューティングノードの健全性チェック * ：ノードをアップグレードする準備が完了していることを確認しました。を参照してください "コンピューティングノードの健全性チェックは、コンピューティングファームウェアをアップグレードする前に実行します"。
- エンドユーザライセンス契約（**EULA**）：管理サービス2.20.69以降では、NetApp Hybrid Cloud Control UIまたはAPIを使用してコンピューティングノードのファームウェアをアップグレードする前に、EULAに同意して保存する必要があります。
  a. Webブラウザで管理ノードのIPアドレスを開きます。

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

  b. 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。
  c. インターフェイスの右上にある [* Upgrade] を選択します。
  d. EULAがポップアップ表示されます。下にスクロールして、[現在および今後のすべての更新を許可する*]を選択し、[保存*]を選択します。

このタスクについて

本番環境では、一度に 1 つのコンピューティングノードのファームウェアをアップグレードします。

> ヘルスチェックを実行してファームウェアのアップグレードを開始する前に、 ESXi ホストのロックダウンモードを解除する必要があります。を参照してください "ESXi ホストでロックダウンモードを無効にする方法" および "VMware ロックダウンモードの動作" を参照してください。

NetApp Hybrid Cloud Control の UI または API のアップグレードでは、 DRS 機能と必要なライセンスがある場合、アップグレードプロセス中に ESXi ホストが自動的にメンテナンスモードになります。ノードがリブートされ、アップグレードプロセスが完了すると、 ESXi ホストがメンテナンスモードから除外されます。USB および BMC UI オプションでは、各手順の説明に従って、 ESXi ホストを手動でメンテナンスモードにする必要があります。

> アップグレードする前に、 ESXi ドライバの現在のバージョンを確認してください。ドライバが最新でない場合は、まずドライバをアップグレードします。その後、コンピューティングノードのコンピューティングファームウェアをアップグレードします。

アップグレードオプション

アップグレードシナリオに関連するオプションを選択します。

- NetApp Hybrid Cloud Control の UI を使用してコンピューティングをアップグレードします ノード （推奨）
- NetApp Hybrid Cloud Control API を使用してコンピューティングをアップグレードします ノード
- 最新のコンピューティングファームウェアバンドルでイメージ化されたUSBドライブを使用します
- ベースボード管理コントローラ（ BMC ）のユーザインターフェイス（ UI ）を使用する

NetApp Hybrid Cloud Control の UI を使用してコンピューティングをアップグレードします ノード

管理サービス 2.14 以降では、 NetApp Hybrid Cloud Control の UI を使用してコンピューティングノードをアップグレードできます。ノードのリストから、アップグレードするノードを選択する必要があります。[現行バージョン *] タブには現在のファームウェアバージョンが表示され、 [提案されたバージョン *] タブには利用可能なアップグレードバージョンが表示されます（存在する場合）。

> アップグレードを成功させるには、 vSphere クラスタの健全性チェックが成功していることを確認します。

> 管理ノードと BMC ホスト間のネットワーク接続の速度によっては、 NIC 、 BIOS 、および BMC のアップグレードにノードあたり約 60 分かかることがあります。

> NetApp Hybrid Cloud Control UI を使用して、 H300E 、 H500E 、 H700E の各コンピューティングノードのコンピューティングファームウェアをアップグレードできなくなりました。をアップグレードする場合は、を使用する必要があります USB ドライブ または BMC UI コンピューティングファームウェアバンドルをマウントする。

必要なもの

- 管理ノードがインターネットに接続されていない場合は、からコンピューティングファームウェアバンドルをダウンロードしておきます "ネットアップサポートサイト"。

TAR.GZ`ファイルをTARファイルに抽出し、次にTARファイルをコンピュート・ファームウェア・バンドルに抽出します。

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。

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

2. 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。
3. インターフェイスの右上にある [* Upgrade] を選択します。
4. [アップグレード * （ Upgrades * ）] ページで、 [ファームウェアの計算（ Compute firmware ）] を選択します。
5. アップグレードするクラスタを選択します。

   クラスタ内のノードは、現在のファームウェアバージョンと新しいバージョン（アップグレード可能な場合）に加えてリストに表示されます。

6. からダウンロードしたコンピュートファームウェアバンドルをアップロードするには、* Browse *を選択します "ネットアップサポートサイト"。
7. アップロードが完了するまで待ちます。進捗バーにアップロードのステータスが表示されます。

   ブラウザウィンドウから別の場所に移動すると、ファイルのアップロードがバックグラウンドで実行されます。

   ファイルのアップロードと検証が完了すると、画面にメッセージが表示されます。検証には数分かかることがあります。

8. コンピューティングファームウェアバンドルを選択します。
9. [* アップグレードの開始 *] を選択します。

   [**Begin Upgrade**] を選択すると、ウィンドウに失敗したヘルスチェックがある場合は表示されます。

   アップグレードは開始後に一時停止できません。ファームウェアは、 NIC 、 BIOS 、および BMC の順序で順番に更新されます。アップグレード中は BMC UI にログインしないでください。BMC にログインすると、アップグレードプロセスを監視する Hybrid Cloud Control Serial-Over-LAN （ SOL ）セッションが終了します。

10. クラスタレベルまたはノードレベルでヘルスチェックに警告が渡され、重大な障害がなければ、「 * アップグレードの準備が完了しています * 」と表示されます。[ノードのアップグレード] を選択します。

    アップグレードの実行中は、ページを離れてあとから表示し、進捗状況の監視を続行できます。アップグレードの実行中、アップグレードのステータスに関するさまざまなメッセージが UI に表示されます。

H610CおよびH615Cコンピューティングノードのファームウェアをアップグレードしている間は、BMC Web UIでSerial-Over-LAN（SOL）コンソールを開かないでください。これにより、アップグレードが失敗する場合があります。

アップグレードの完了後に、 UI にメッセージが表示されます。アップグレードの完了後にログをダウンロードできます。アップグレードステータスのさまざまな変更については、を参照してください [アップグレードステータスが変わります]。

アップグレード中に障害が発生した場合は、 NetApp Hybrid Cloud Control がノードをリブートし、ノードをメンテナンスモードから除外して、エラーステータスとエラーログへのリンクを表示します。エラーログをダウンロードして、特定の手順や KB 記事へのリンクを参照し、問題を診断して修正できます。NetApp Hybrid Cloud Control を使用したコンピューティングノードのファームウェアアップグレードの問題の詳細については、こちらを参照してください "KB" 記事。

アップグレードステータスが変わります

アップグレードプロセスの実行前、実行中、実行後に表示されるさまざまな状態を次に示します。

アップグレードの状態	説明
ノードで 1 つ以上の健全性チェックに失敗しました。を展開して詳細を表示します。	1 つ以上の健全性チェックに失敗しました。
エラー	アップグレード中にエラーが発生しました。エラーログをダウンロードして、ネットアップサポートに送信できます。
検出できません	このステータスは、コンピューティングノードアセットにハードウェアタグがないにもかかわらず、NetApp Hybrid Cloud Controlがコンピューティングノードを照会できない場合に表示されます。
アップグレードの準備が完了しました。	すべての健全性チェックにパスし、ノードをアップグレードする準備が完了しました。
アップグレード中にエラーが発生しました。	重大なエラーが発生すると、アップグレードは失敗し、この通知が表示されます。エラーの解決に役立つ [ログのダウンロード] リンクを選択して、ログをダウンロードします。エラーを解決してから、もう一度アップグレードを実行してください。
ノードのアップグレードを実行中です。	アップグレードを実行中です。進行状況バーにアップグレードステータスが表示されます。

NetApp Hybrid Cloud Control API を使用してコンピューティングをアップグレードします ノード

API を使用して、クラスタ内の各コンピューティングノードを最新のファームウェアバージョンにアップグレードできます。API の実行には、任意の自動化ツールを使用できます。ここで説明する API ワークフローでは、例として管理ノードで使用可能な REST API UI を使用します。

NetApp Hybrid Cloud Control UI を使用して、 H300E 、 H500E 、 H700E の各コンピューティングノードのコンピューティングファームウェアをアップグレードできなくなりました。をアップグレードする場合は、を使用する必要があります USB ドライブ または BMC UI コンピューティングファームウェアバンドルをマウントする。

必要なもの

vCenter やハードウェアのアセットなど、コンピューティングノードのアセットを管理ノードのアセットに認識しておく必要があります。インベントリサービス API を使用して、アセットを確認できます (`https://<ManagementNodeIP>/inventory/1/`)。

手順

1. NetApp HCI ソフトウェアにアクセスします "ページをダウンロードします" 管理ノードからアクセス可能なデバイスに最新のコンピューティングファームウェアバンドルをダウンロードします。
2. コンピューティングファームウェアバンドルを管理ノードにアップロードします。
   a. 管理ノードで管理ノード REST API UI を開きます。

   ```
   https://<ManagementNodeIP>/package-repository/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. 承認ウィンドウを閉じます。
   c. REST API UI から * POST/packages * を選択します。
   d. [* 試してみてください *] を選択します。
   e. * Browse（参照）*を選択し、コンピュートファームウェアバンドルを選択します。
   f. 「 * Execute * 」を選択してアップロードを開始します。
   g. 応答から'後の手順で使用するために'コンピュート・ファームウェア・バンドルID（「id」）をコピーして保存します
3. アップロードのステータスを確認します。
   a. REST API UI から、 * GEGET 処理対象 / パッケージ間の一時的なグループ / ｛ id ｝ 一時的なグループ / ステータス * を選択します。
   b. [* 試してみてください *] を選択します。
   c. 前の手順でコピーしたパッケージ ID を * id * で入力します。
   d. ステータス要求を開始するには、 * Execute * を選択します。

      応答が完了すると、「アクセス」として表示されます。

   e. 応答から'後の手順で使用するために'コンピューティング・ファームウェア・バンドル名（名前）とバージョン（バージョン）をコピーして保存します
4. アップグレードするノードのコンピューティングコントローラ ID とノードハードウェア ID を確認しま

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. 承認ウィンドウを閉じます。
c. REST API UI から、 * GET / Installations * 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. 応答から、インストールアセット ID （「 id 」）をコピーします。
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 」）とノードハードウェア ID （「 hardwareId 」）をコピーして保存します。

```
"compute": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterId": "Test-1B",
        "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
```

```
"nodes": [
  {
    "bmcDetails": {
      "bmcAddress": "10.111.0.111",
      "credentialsAvailable": true,
      "credentialsValidated": true
    },
    "chassisSerialNumber": "111930011231",
    "chassisSlot": "D",
    "hardwareId": "123a4567-01b1-1243-a12b-11ab11ab0a15",
    "hardwareTag": "00000000-0000-0000-0000-ab1c2de34f5g",
    "id": "e1111d10-1a1a-12d7-1a23-ab1cde23456f",
    "model": "H410C",
```

5. コンピューティングノードのファームウェアアップグレードを実行します。
   a. 管理ノードでハードウェアサービス REST API UI を開きます。

```
https://<ManagementNodeIP>/hardware/2/
```

   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. 承認ウィンドウを閉じます。
   c. 「 * POST/nodes / ｛ hardware_id ｝ /upgrades * 」を選択します。
   d. [* 試してみてください *] を選択します。
   e. 前の手順で保存したハードウェア・ホストの資産 ID （「 hardwareId 」）をパラメータ・フィールドに入力します。
   f. ペイロード値については、次の手順を実行します。
      i. ノードでヘルスチェックが実行され、 ESXi ホストがメンテナンスモードに設定されるように、値「 force 」： false 」および「 maintenanceMode 」： true 」を保持します。
      ii. クラスタコントローラ ID （前の手順で保存した「 ControllerID 」）を入力します。
      iii. 前の手順で保存したコンピューティングファームウェアのバンドル名とバージョンを入力します。

```
{
  "config": {
    "force": false,
    "maintenanceMode": true
  },
  "controllerId": "a1b23456-c1d2-11e1-1234-a12bcdef123a",
  "packageName": "compute-firmware-12.2.109",
  "packageVersion": "12.2.109"
}
```

g. アップグレードを開始するには、 * Execute * を選択します。

> アップグレードは開始後に一時停止できません。ファームウェアは、 NIC 、 BIOS 、および BMC の順序で順番に更新されます。アップグレード中は BMC UI にログインしないでください。BMC にログインすると、アップグレードプロセスを監視する Hybrid Cloud Control Serial-Over-LAN （ SOL ）セッションが終了します。

h. 応答内のリソースリンク ("resourceLink") URL の一部であるアップグレードタスク ID をコピーします

6. アップグレードの進捗状況と結果を確認します。

a. 「 * get/task/ ｛ task_id ｝ /logs * 」を選択します。

b. [* 試してみてください *] を選択します。

c. 前の手順のタスク ID を * TASK_ID * に入力します。

d. [* Execute] を選択します。

e. アップグレード中に問題または特別な要件が発生した場合は、次のいずれかを実行します。

オプション	手順
応答の本文に「 failedHealthCheckks 」というメッセージが表示されているため、クラスタのヘルスの問題を修正する必要があります。	i. 各問題について記載されている特定の技術情報アーティクルに移動するか、指定された対処方法を実行します。 ii. KB を指定した場合は、関連する技術情報アーティクルに記載されているプロセスを完了します。 iii. クラスタの問題を解決したら、必要に応じて再認証し、 * POST /nodes/ ｛ hardware_id ｝ /upgrades * を選択します。 iv. アップグレード手順で前述した手順を繰り返します。
アップグレードに失敗し、移行後の手順はアップグレードログに記載されていません。	i. を参照してください "こちらの技術情報アーティクル" （ログインが必要です）。

f. 必要に応じて、処理が完了するまで * Get Th量 / タスク / ｛ task_id ｝ / ログ * API を複数回実行しま

す。

アップグレード中、エラーが発生しなかった場合、「ステータス」は「実行中」を示します。各ステップが完了すると、「ステータス」の値が「完了」に変わります。

各ステップのステータスが「 Completed 」で「 percentageCompleted 」の値が「 100 」の場合、アップグレードは正常に終了しました。

7. （オプション）各コンポーネントのアップグレードされたファームウェアバージョンを確認します。
   a. 管理ノードでハードウェアサービス REST API UI を開きます。

      ```
      https://<ManagementNodeIP>/hardware/2/
      ```

   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. 承認ウィンドウを閉じます。
   c. REST API UI から、 * GET 処理対象の新規 / ノード間の処理 / ｛ hardware_id ｝ の一時的な処理 / アップグレード * を選択します。
   d. （オプション）日付とステータスのパラメータを入力して、結果をフィルタリングします。
   e. 前の手順で保存したハードウェア・ホストの資産 ID （「 hardwareId 」）をパラメータ・フィールドに入力します。
   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. すべてのコンポーネントのファームウェアが以前のバージョンから最新のファームウェアに正常にアップグレードされたことを示す応答を確認します。

最新のコンピューティングファームウェアバンドルでイメージ化された**USB**ドライブを使用します

コンピューティングノードのUSBポートにダウンロードした最新のコンピューティングファームウェアバンドルがインストールされたUSBドライブを挿入できます。この手順 に記載されているUSBメモリ方式を使用する代わりに、ベースボード管理コントローラ（BMC）インターフェイスの仮想コンソールで仮想CD/DVDオプションを使用して、コンピューティングノードにコンピューティングファームウェアバンドルをマウントできます。BMC を使用する方法は、 USB メモリを使用する方法よりもかなり時間がかかります。ワークステーションまたはサーバに必要なネットワーク帯域幅があること、および BMC とのブラウザセッションがタイムアウトしないことを確認してください。

必要なもの

- 管理ノードがインターネットに接続されていない場合は、からコンピューティングファームウェアバンドルをダウンロードしておきます "ネットアップサポートサイト"。

> TAR.GZ`ファイルをTARファイルに抽出し、次にTARファイルをコンピュート・ファームウェア・バンドルに抽出します。

手順

1. Etcherユーティリティを使用して、コンピュートファームウェアバンドルをUSBドライブにフラッシュします。
2. VMware vCenter を使用してコンピューティングノードをメンテナンスモードに切り替えて、すべての仮想マシンをホストから退避します。

> クラスタで VMware DRS （ Distributed Resource Scheduler ）が有効になっている場合（ NetApp HCI 環境のデフォルト）、仮想マシンはクラスタ内の他のノードに自動的に移行されます。

3. コンピューティングノードの USB ポートに USB メモリを挿入し、 VMware vCenter を使用してコンピューティングノードをリブートします。
4. コンピューティングノードの POST サイクル中に * F11 * を押して、 Boot Manager を開きます。F11 キーを何度も押さなければならない場合があります。この操作は ' ビデオ / キーボードを接続するか 'BMC' のコンソールを使用して実行できます
5. 表示されたメニューから * One Shot * > * USB Flash Drive * を選択します。USB メモリがメニューに表示されない場合は、 USB フラッシュドライブがシステムの BIOS のレガシー起動順序に含まれていることを確認します。
6. Enter キーを押して、 USB メモリからシステムを起動します。ファームウェアのフラッシュプロセスが開始されます。

   ファームウェアのフラッシュが完了してノードがリブートしたあと、 ESXi の起動に数分かかる場合があります。

7. リブートが完了したら、 vCenter を使用して、アップグレードしたコンピューティングノードでメンテナンスモードを終了します。
8. アップグレードしたコンピューティングノードから USB フラッシュドライブを取り外します。
9. すべてのコンピューティングノードがアップグレードされるまで、 ESXi クラスタ内の他のコンピューティングノードに対してこの手順を繰り返します。

ベースボード管理コントローラ（ **BMC** ）のユーザインターフェイス（ **UI** ）を使用する

アップグレードが正常に完了するように、コンピューティングファームウェアバンドルをロードし、ノードをコンピューティングファームウェアバンドルに対してリブートするには、手順を連続して実行する必要があります。コンピューティングファームウェアバンドルは、Webブラウザをホストしているシステムまたは仮想マシン（VM）に配置する必要があります。プロセスを開始する前に、コンピューティングファームウェアバンドルをダウンロードしたことを確認してください。

> システムまたは VM とノードを同じネットワークに配置することを推奨します。

> BMC UI からのアップグレードには約 25~30 分かかります。

- H410C ノードと H300E / H500E / H700E ノードのファームウェアをアップグレードします
- H610C / H615C ノードのファームウェアをアップグレードします

ノードがクラスタに参加している場合は、アップグレード前にノードをメンテナンスモードにして、アップグレード後にメンテナンスモードを終了する必要があります。

> プロセス中に表示された次の情報メッセージは無視してください。「 Untrusty Debug Firmware Key is used 、 SecureFlash is currently in Debug Mode 」

手順

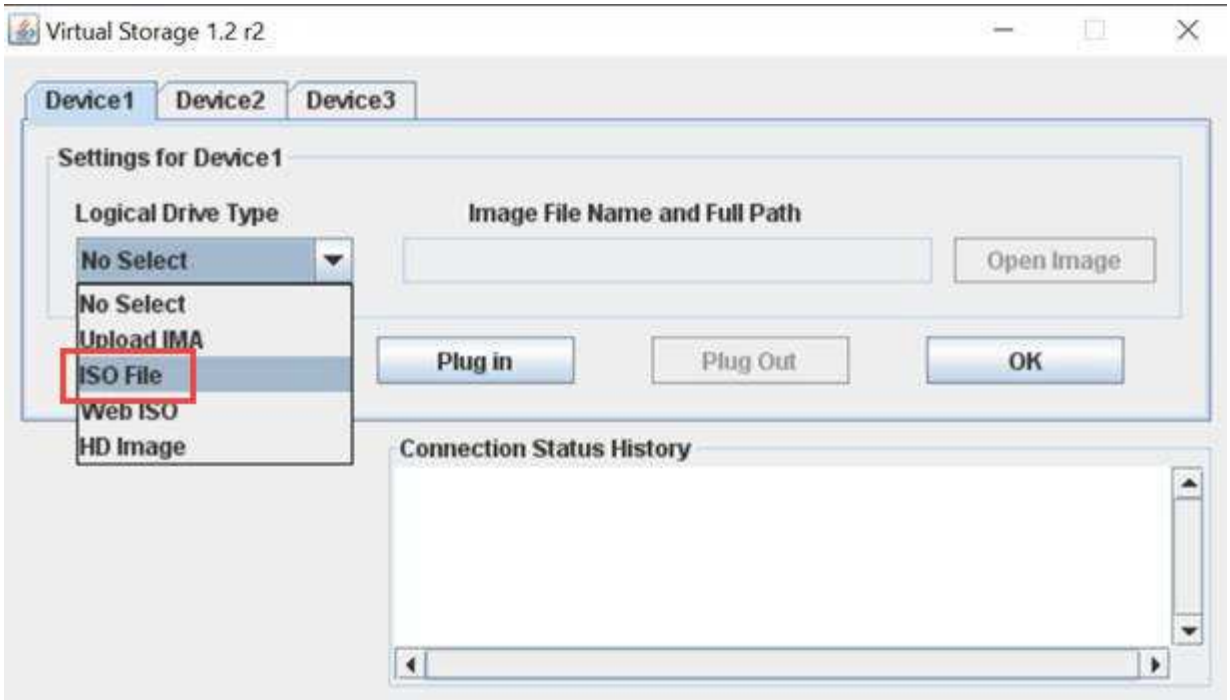
1. ノードがクラスタに参加している場合は、次のように保守モードにします。ない場合は、手順 2 に進みます。
   a. VMware vCenter Web Client にログインします。
   b. ホスト（コンピューティングノード）名を右クリックし、 * メンテナンスモード > メンテナンスモードへの切り替え * を選択します。
   c. 「 * OK 」を選択します。ホスト上の VM は、使用可能な別のホストに移行されます。移行する VM の数によっては、 VM の移行に時間がかかることがあります。

      > 続行する前に、ホスト上のすべての VM が移行されていることを確認してください。

2. BMC UI （ https://BMCIP/#login` ）に移動します。 BMCIP は BMC の IP アドレスです。
3. クレデンシャルを使用してログインします。
4. [* リモートコントロール]>[コンソールリダイレクト *] を選択します。
5. [コンソールの起動 *] を選択します。

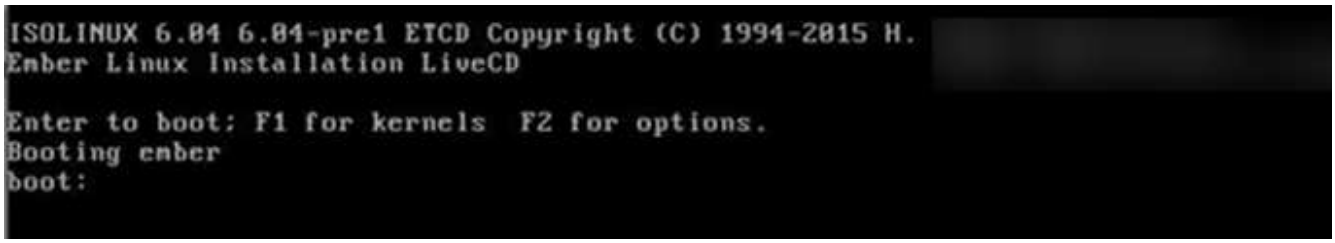
   > Java のインストールまたは更新が必要になる場合があります。

6. コンソールが開いたら、 * バーチャル・メディア > バーチャル・ストレージ * を選択します。
7. Virtual Storage （仮想ストレージ）画面で、 * Logical Drive Type （論理ドライブタイプ） * を選択し、 * ISO File （ ISO ファイル） * を選択します。



8. [Open Image*（イメージを開く）]を選択して、コンピュートファームウェアバンドルファイルをダウンロードしたフォルダを参照し、コンピュートファームウェアバンドルファイルを選択します。
9. [* プラグイン *] を選択します。
10. 接続ステータスに「 Device#:VM Plug-in OK!! 」と表示されたら、「 **OK** 」を選択します。
11. ノードを再起動するには、 * F12 * を押して * Restart * を選択するか、 * Power Control > Set Power Reset * を選択します。
12. リブート中に* F11 *を押してブートオプションを選択し、コンピューティングファームウェアバンドルをロードします。ブートメニューが表示されるまでに F11 キーを何度か押しなければならない場合があります。

    次の画面が表示されます。



13. 上記の画面で、 **Enter** キーを押します。ネットワークによっては、アップグレードを開始するために * Enter キーを押してから数分かかることがあります。

> ファームウェアのアップグレードによっては、コンソールが切断されたり、 BMC のセッションが切断されたりする場合があります。BMC に再度ログインできますが、ファームウェアのアップグレードにより、コンソールなどの一部のサービスを使用できない場合があります。アップグレードが完了すると、ノードのコールドリブートが実行されます。これには約 5 分かかることがあります。

14. BMC UI に再度ログインし、 * System * を選択して、 OS の起動後に BIOS のバージョンとビルド時間を

確認します。アップグレードが正常に完了すると、新しい BIOS と BMC のバージョンが表示されます。

> BIOS のバージョンは、ノードのブートが完了するまでアップグレード後のバージョンを表示しません。

15. ノードがクラスタに含まれている場合は、次の手順を実行します。スタンドアロンノードの場合、これ以上の操作は必要ありません。
    a. VMware vCenter Web Client にログインします。
    b. ホストのメンテナンスモードを解除します。赤色のフラグが外れている可能性があります。すべてのステータスが解消されるまで待ちます。
    c. 電源がオフになっていた残りの VM のいずれかの電源をオンにします。

H610C / H615C ノードのファームウェアをアップグレードします

手順は、ノードがスタンドアロンであるかクラスタの一部であるかによって異なります。手順 の所要時間は約25分で、ノードの電源オフ、コンピューティングファームウェアバンドルのアップロード、デバイスのフラッシュ、アップグレード後のノードの電源のオンとオフが含まれます。

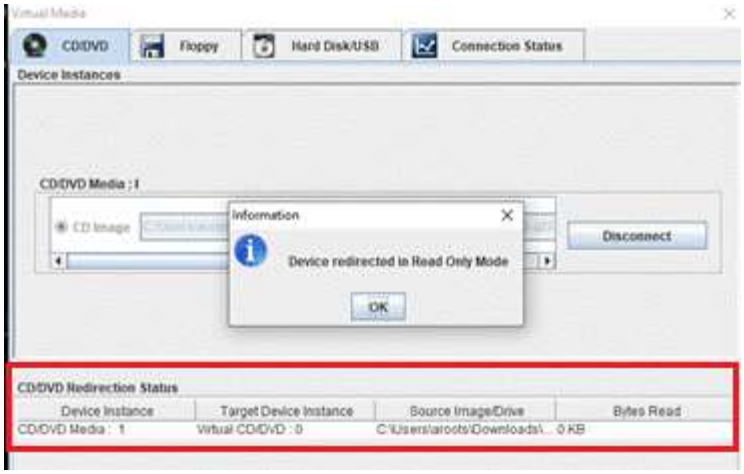
手順

1. ノードがクラスタに参加している場合は、次のように保守モードにします。ない場合は、手順 2 に進みます。
    a. VMware vCenter Web Client にログインします。
    b. ホスト（コンピューティングノード）名を右クリックし、 * メンテナンスモード > メンテナンスモードへの切り替え * を選択します。
    c. 「 * OK 」を選択します。ホスト上の VM は、使用可能な別のホストに移行されます。移行する VM の数によっては、 VM の移行に時間がかかることがあります。

    > 続行する前に、ホスト上のすべての VM が移行されていることを確認してください。

2. BMC UI 「 https://BMCIP/#login` 」に移動します。ここで、 BMC IP は BMC の IP アドレスです。
3. クレデンシャルを使用してログインします。
4. リモート・コントロール > Launch KVM (Java)* を選択します
5. コンソールウィンドウで、 * Media > Virtual Media Wizard* を選択します。

6. [**Browse**] を選択し ' コンピュート・ファームウェアの [.iso （ .iso ）] ファイルを選択します
7. 「 * 接続」を選択します。成功したことを示すポップアップが表示され、パスとデバイスが下部に表示されます。[仮想メディア *] ウィンドウを閉じることができます。



8. ノードを再起動するには、 * F12 * を押して * Restart * を選択するか、 * Power Control > Set Power Reset * を選択します。
9. リブート中に* F11 *を押してブートオプションを選択し、コンピューティングファームウェアバンドルをロードします。
10. 表示されたリストから **AMI Virtual CDROM** * を選択し、 ***Enter** を選択します。リストに AMI Virtual CDROM が表示されない場合は、 BIOS にアクセスして起動リストで有効にします。保存するとノードがリブートします。再起動中に * F11 * を押します。

11. 表示された画面で、 **Enter** を選択します。

> ファームウェアのアップグレードによっては、コンソールが切断されたり、 BMC のセッションが切断されたりする場合があります。BMC に再度ログインできますが、ファームウェアのアップグレードが原因で、コンソールなどの一部のサービスを使用できない場合があります。アップグレードが完了すると、ノードのコールドリブートが実行されます。これには約 5 分かかることがあります。

12. コンソールから切断された場合は、 * Remote Control * を選択して * Launch KVM * または * Launch KVM （ Java ） * を選択し、再接続してノードのブートが完了したことを確認します。ノードが正常にブートしたことを確認するために、複数の再接続が必要になる場合があります。

電源投入プロセス中、約 5 分間、 KVM コンソールに「 * No Signal * （信号なし）」と表示されます。

13. ノードの電源をオンにした後、 * ダッシュボード > デバイス情報 > 詳細情報 * を選択して、 BIOS と BMC のバージョンを確認します。アップグレード後の BIOS と BMC のバージョンが表示されます。アップグレード後のバージョンの BIOS は、ノードが完全にブートするまで表示されません。
14. ノードをメンテナンスモードにした場合は、ノードが ESXi をブートした後、ホスト（コンピューティングノード）名を右クリックし、 * Maintenance Mode > Exit Maintenance Mode * を選択して VM をホストに戻します。
15. vCenter で、ホスト名を選択し、 BIOS のバージョンを設定して確認します。

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"
- "NetApp HCI のリソースページ"

Ansible によるコンピューティングノードのファームウェアアップグレードの自動化

NetApp Hybrid Cloud Control のワークフローを使用して、 NetApp HCI コンピューティングノードのシステムファームウェアを更新できます。これには、 BMC 、 BIOS 、 NIC などのコンポーネントのファームウェアも含まれます。大規模なコンピューティングクラスタを含む環境では、 Ansible を使用してクラスタ全体のローリングアップグレードを実行することでワークフローを自動化できます。

コンピューティングノードのファームウェアアップグレードを自動化する Ansible のロールはネットアップによって提供されますが、自動化は補助コンポーネントとして機能し、追加のセットアップやソフトウェアコンポーネントの実行が必要となります。Ansible 自動化の変更はベストエフォートベースでのみサポートされます。

アップグレード用の Ansible のロールは、 NetApp HCI H シリーズのコンピューティングノードでのみ機能します。サードパーティ製コンピューティングノードのアップグレードにはこのロールを使用できません。

必要なもの

- * ファームウェアのアップグレードの準備と前提条件 * ：の手順に従って、 NetApp HCI のインストール環境でファームウェアのアップグレードの準備ができている必要があります "ファームウェアのアップグレードを実行する"。
- * Ansible コントロールノード * で自動化を実行する準備：物理サーバまたは仮想サーバで Ansible でファームウェア更新の自動化を実行します。

このタスクについて

本番環境では、 NetApp HCI インストール環境のコンピューティングノードを、 1 つずつローリング方式で更新する必要があります。NetApp Hybrid Cloud Control の API は、健全性チェックの実行、コンピューティングノード上の ESXi のメンテナンス、ファームウェアアップグレードを適用するためのコンピューティングノードのリブートなど、コンピューティングノードのファームウェアアップグレードプロセス全体を 1 つのコンピューティングノードに対してオーケストレーションします。Ansible ロールは、コンピューティングノードのグループまたはクラスタ全体に対してファームウェアアップグレードをオーケストレーションするための

オプションを提供します。

ファームウェアのアップグレードの自動化を始めましょう

作業を開始するには、に移動します "GitHub 上の NetApp Ansible リポジトリ" および 'NAR_compute_nodes_firmware_upgrades ロールとドキュメントをダウンロードします

詳細については、こちらをご覧ください

- "NetApp HCI のリソースページ"

を使用して、 NetApp HCI システムの vSphere コンポーネントをアップグレードします vCenter Server 向け Element プラグイン

NetApp HCI 環境の VMware vSphere コンポーネントをアップグレードするときは、Element Plug-in for vCenter Server についていくつかの追加の手順を実行する必要があります。

手順

1. vCSA のアップグレード "クリア" プラグインの QoSSIOC 設定（ * NetApp Element Configuration > QoSSIOC Settings * ）。[**QoSSIOC Status**] フィールドには、プロセスの完了後に「 Not Configured 」と表示されます。
2. vCSA と Windows のアップグレード "登録解除します" 登録ユーティリティを使用してプラグインを関連付けられている vCenter Server からプラグインを削除します。
3. "vCenter Server 、 ESXi 、 VM 、その他の VMware コンポーネントを含む vSphere をアップグレードします"。

> 回避策 を適用せずにVMware vCenter 7.0 Update 3でプラグインを導入できるようにするには、NetApp Element Plug-in for vCenter Server 5.0以降にアップグレードしてください。
>
> Element Plug-in for vCenter Server 4.xでVMware vCenter Server 7.0 Update 3にアップグレードした場合、プラグイン4.xを導入できません。Spring Framework 4を使用してこの問題を解決するには、を参照してください "こちらの技術情報アーティクル"。

> 用のコンピューティングノードの ESXi をアップグレードする場合 "2 ノードクラスタ"では、一度に 1 つのコンピューティングノードのみをアップグレードして、一時的に 1 つの監視ノードのみが使用不能になり、クラスタクォーラムを維持できるようにします。

4. "登録" vCenter で Element Plug-in for vCenter Server を再度実行します。
5. "クラスタを追加" プラグインを使用する。
6. "QoSSIOC を設定します" プラグインを使用する。
7. "QoSSIOC を有効にします" プラグインで制御されているすべてのデータストアが対象です。

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 のリソースページ"
- "NetApp HCI 2 ノードストレージクラスタテクニカルレポート"