NetApp HCI のドキュメント

HCI

NetApp
December 22, 2023

目次

NetApp HCI のドキュメント 1
NetApp HCI ソリューション 2
リリースノート 3
NetApp HCI の新機能 3
その他のリリース情報 4
概念 7
NetApp HCI 製品の概要 7
ユーザアカウント 8
データ保護 10
クラスタ 14
ノード 16
ストレージ 18
NetApp HCI ライセンス 22
NetApp Hybrid Cloud Control の最大構成数 23
NetApp HCI セキュリティ 23
パフォーマンスと QoS 25
要件と導入前のタスク 29
NetApp HCI 導入の要件の概要 29
管理ノードの要件 29
ネットワークポートの要件 29
ネットワークとスイッチの要件 34
ネットワークケーブルの要件 36
IP アドレスの要件 36
ネットワーク構成： 38
DNS とタイムキーパー機能の要件 46
環境要件 46
保護ドメイン 47
2 ノードストレージクラスタの場合は、監視ノードのリソース要件が必要です 47
NetApp HCI の利用を開始しましょう 49
NetApp HCI のインストールと導入の概要 49
H シリーズハードウェアを設置 56
ストレージパフォーマンスを最適化するために LACP を設定します 72
Active IQ Config Advisor で環境を検証 73
各ノードに IPMI を設定します 76
NetApp HCI を導入します 79
NetApp Deployment Engine にアクセスします 79
導入を開始 82
インストールプロファイルをインポートします 83
VMware vSphere を設定します 83

NetApp HCI クレデンシャルを設定する 86
ネットワークトポロジを選択してください 87
在庫の選択 88
ネットワークの設定を行います 90
構成を確認し、導入します 97
導入後のタスク 99
NetApp HCI を管理します 113
NetApp HCI の管理の概要 113
完全修飾ドメイン名 Web UI アクセスを設定します 113
NetApp HCI と NetApp SolidFire でクレデンシャルを変更 118
vCenter および ESXi のクレデンシャルを更新します 122
NetApp HCI ストレージを管理します 124
管理ノードを操作します 148
NetApp HCI システムの電源をオフまたはオンにします 200
NetApp Hybrid Cloud Control を使用して NetApp HCI システムを監視します 204
Hybrid Cloud Control でストレージリソースとコンピューティングリソースを監視します ダッシュボード 204
ノードページでインベントリを表示します 210
ベースボード管理コントローラの接続情報を編集します 212
ストレージクラスタのボリュームを監視する 216
SolidFire Active IQ を使用して、パフォーマンス、容量、クラスタの健全性を監視できます 217
トラブルシューティング用にログを収集する 219
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 223
アップグレード手順の概要 223
システムのアップグレード手順 225
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 312
NetApp HCI システムを拡張します 314
拡張の概要 314
NetApp HCI ストレージリソースを展開します 315
NetApp HCI コンピューティングリソースを展開します 317
NetApp HCI のストレージリソースとコンピューティングリソースも同時に拡張します 時間 319
クラスタの拡張後に監視ノードを削除します 323
NetApp HCI で Rancher を使用します 325
NetApp HCI の Rancher の概要 325
NetApp HCI の概念に関する Rancher 327
NetApp HCI の Rancher の要件 328
NetApp HCI に Rancher を導入します 331
導入後のタスク 335
ユーザクラスタとアプリケーションを導入 340
NetApp HCI でランチ元を管理します 341

NetApp HCI 実装の Rancher を監視する 342
NetApp HCI の Rancher をアップグレードします 343
NetApp HCI でランチツールをインストールした場合は、取り外します 349
H シリーズハードウェアのメンテナンス 352
H シリーズハードウェアのメンテナンスの概要 352
2U H シリーズシャーシを交換 352
H615C および H610S ノードの DC 電源装置を交換してください 359
コンピューティングノードの DIMM を交換します 362
ストレージノードのドライブを交換 371
H410C ノードを交換してください 376
H410S ノードを交換します 404
H610C ノードと H615C ノードを交換してください 411
H610S ノードを交換してください 417
電源装置を交換してください 420
SN2010 、 SN2100 、および SN2700 の各スイッチを交換してください 422
2 ノードクラスタのストレージノードを交換 430
以前のバージョンの NetApp HCI ドキュメント 432
法的通知 433
著作権 433
商標 433
特許 433
プライバシーポリシー 433
オープンソース 433

NetApp HCI のドキュメント

NetApp HCI ソリューション

NetApp HCI ソリューションは、複数のワークロードを同じインフラに配置することで、摩擦のない大規模なパフォーマンスを実現します。

NetApp HCI を使用すると、複数のパブリッククラウドプロバイダとオンプレミスに クラウド サービス を導入できます。NetApp HCI を使用すると、クラウドプロバイダと同様のサービスをIT部門のサポートなしでセルフサービスモードで導入できます。

NetApp HCI ソリューションの詳細については、を参照してください "NetApp HCI ソリューションのドキュメント"。

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"

リリースノート

NetApp HCI の新機能

ネットアップでは、 NetApp HCI を定期的に更新して、新機能、拡張機能、およびバグ修正を提供しています。NetApp HCI 1.9P1には、ストレージクラスタ用のNetApp Element ソフトウェア12.3.1が含まれます。

> Element 12.3.2には、Apache log4jの脆弱性に対するElementソフトウェアの影響を軽減する機能が含まれています。Virtual Volumes （ VVol ）機能が有効になっている NetApp SolidFire ストレージクラスタは、この脆弱性の影響を受けやすくなっています。
>
> ストレージクラスタがElement 12.3.1で、VVol機能が有効になっている場合は、Elementソフトウェア12.3.2にアップグレードする必要があります。
>
> ストレージクラスタがElement 12.3.1で、VVol機能が無効になっている場合、Elementソフトウェア12.3.2へのアップグレードはオプションです。
>
> アップグレードの実行中を除き、クラスタ内でElementのバージョンを混在させることは推奨されません。

- 。 NetApp HCI 1.9P1 セクションでは、 NetApp HCI バージョン 1.9P1 の新機能とアップデートについて説明します。
- 。 Element 12.3.1 ここでは、 NetApp Element 12..1 の新機能とアップデートについて説明します。

NetApp HCI 1.9P1

NetApp HCI 1.9P1 では、セキュリティと安定性が向上しています。

Element 12.3.1

NetApp HCI 1.9P1 にはストレージクラスタ用の Element 12.3.1 が含まれます。

ストレージファームウェアバンドル **2.99.2**

Element 12.3.1 リリースには、ストレージファームウェアバンドルバージョン 2.99.2 が含まれています。ストレージクラスタがすでに Element 12.3 にある場合は、新しい 2.99.2 ファームウェアバンドルをインストールするだけで済みます。

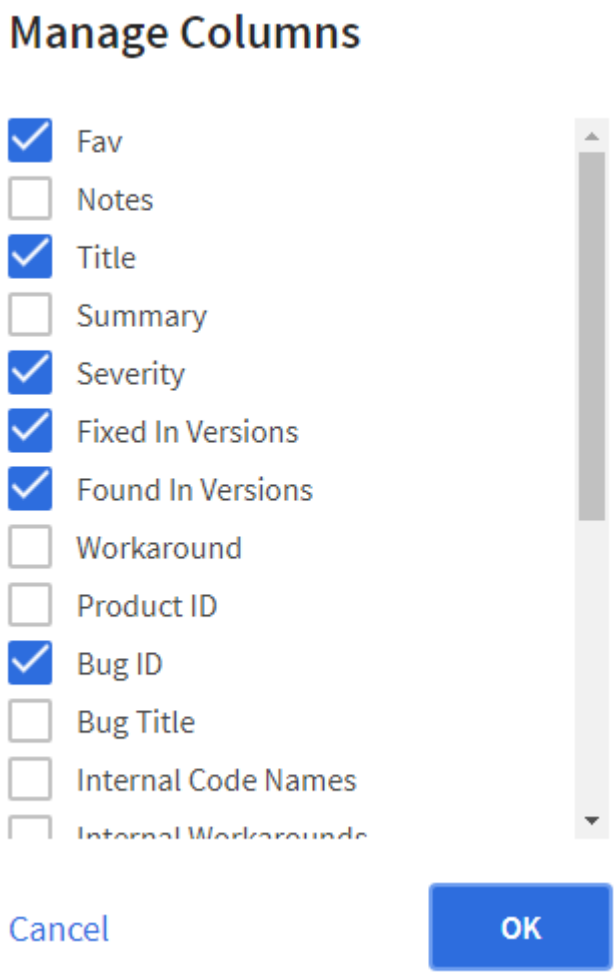
NetApp Bugs Online には、既知の問題と解決済みの問題があります

既知の問題と解決済みの問題の一覧については、 NetApp Bugs Online ツールを参照してください。これらの問題は Element およびその他の製品で参照できます から "NetApp Bugs Online では"。

手順

1. に進みます "NetApp Bugs Online では"。
2. [キーワードで検索 *] フィールドに、製品名（「要素」など）を入力します。

3. を選択します  をクリックし、 * バージョンで固定 * フィルタを選択し、 * OK * を選択します。



4. [新規検索（ New Search ）] を選択します。
5. [バージョン * で固定] フィールドにリリースバージョンを入力します。

詳細については、こちらをご覧ください

- "『 NetApp Hybrid Cloud Control and Management Services Release Notes 』を参照してください"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"
- "SolidFire および Element ソフトウェアのドキュメント"
- "NetApp HCI でサポートされるファームウェアとESXiドライバのバージョン、NetApp HCI ストレージノードでサポートされるファームウェアのバージョンとファームウェアのバージョン"

その他のリリース情報

ここでは、 NetApp HCI および Element ストレージ環境のさまざまなコンポーネントに

関する最新リリースノートと以前のリリースノートへのリンクを記載します。

ネットアップサポートサイトのクレデンシャルでログインするように求められます。

NetApp HCI

- "NetApp HCI 1.9P1 リリースノート"
- "NetApp HCI 1.9 リリースノート"
- "NetApp HCI 1.8P1 リリースノート"
- "NetApp HCI 1.8 リリースノート"
- "NetApp HCI 1.7P1 リリースノート"

NetApp Element ソフトウェア

- "NetApp Element ソフトウェア 12.3.2 リリースノート"
- "NetApp Element ソフトウェア 12.3.1 リリースノート"
- "NetApp Element ソフトウェア 12.3 リリースノート"
- "NetApp Element ソフトウェア 12.2.1 リリースノート"
- "NetApp Element ソフトウェア 12.2 リリースノート"
- "NetApp Element ソフトウェア 12.0.1 リリースノート"
- "NetApp Element ソフトウェア 12.0 リリースノート"
- "NetApp Element ソフトウェア 11.8 リリースノート"
- "NetApp Element ソフトウェア 11.7 リリースノート"
- "NetApp Element ソフトウェア 11.5.1 リリースノート"
- "NetApp Element ソフトウェア 11.3P1 リリースノート"

管理サービス

- "管理サービスリリースノート"

vCenter Server 向け NetApp Element プラグイン

- "vCenter Plug-in 5.2リリースノート" _ 新規 _
- "vCenter Plug-in 5.1リリースノート"
- "vCenter Plug-in 5.0リリースノート"
- "vCenter Plug-in 4.10リリースノート"
- "vCenter Plug-in 4.9リリースノート"
- "vCenter Plug-in 4.8 リリースノート"
- "vCenter Plug-in 4.7 リリースノート"

- "vCenter Plug-in 4.6 リリースノート"
- "vCenter Plug-in 4.5 リリースノート"
- "『 vCenter Plug-in 4.4 Release Notes 』を参照してください"
- "vCenter Plug-in 4.3 リリースノート"

ファームウェアを計算します

- "Compute Firmware Bundle 2.146 リリースノート"
- "Compute Firmware Bundle 2.76 リリースノート"
- "Compute Firmware Bundle 2.27 リリースノート"
- "Compute Firmware Bundle 12.2.109 リリースノート"
- "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"

ストレージファームウェア

- "ストレージファームウェアバンドル 2.146 リリースノート"
- "ストレージファームウェアバンドル 2.99.2 リリースノート"
- "ストレージファームウェアバンドル 2.76 リリースノート"
- "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"
- "H610S BMC 3.84.07 リリースノート"
- "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"

概念

NetApp HCI 製品の概要

NetApp HCI は、ストレージ、コンピューティング、ネットワーク、ハイパーバイザーを組み合わせたエンタープライズ規模のハイブリッドクラウドインフラ設計であり、パブリッククラウドとプライベートクラウドにまたがる機能を追加します。

ネットアップの分離型ハイブリッドクラウドインフラは、コンピューティングとストレージを個別に拡張し、保証されたパフォーマンスでワークロードに適応させることができます。

- ハイブリッドマルチクラウドのニーズに対応
- コンピューティングとストレージを個別に拡張可能
- ハイブリッドマルチクラウド全体にわたってデータサービスのオーケストレーションを簡易化

NetApp HCI のコンポーネント

次に、 NetApp HCI 環境のさまざまなコンポーネントについて、その概要を示します。

- NetApp HCI は、ストレージリソースとコンピューティングリソースの両方を提供します。NetApp HCI の導入には、 NetApp Deployment Engine * ウィザードを使用します。導入が完了すると、コンピューティングノードが ESXi ホストとして表示され、 VMware vSphere Web Client で管理できるようになります。
- * 管理サービス * またはマイクロサービスには、 Active IQ コレクタ、 vCenter Plug-in 向け QoSSIOC 、 mNode サービスが含まれており、サービスバンドルとして頻繁に更新されます。Element 11.3 リリース以降、 * 管理サービス * は管理ノード上でホストされるようになりました。そのため、メジャーリリースを待つことなく、希望するソフトウェアサービスを更新できます。管理ノード * （ mNode ）は、 Element ソフトウェアベースの 1 つ以上のストレージクラスタと同時に実行される仮想マシンです。このサービスは、アップグレード後にシステムサービスを提供するために使用されます。これには、監視とテレメトリ、クラスタのアセットと設定の管理、システムテストとユーティリティの実行、トラブルシューティング用のネットアップサポートアクセスの有効化などが含まれます。

  の詳細を確認してください "管理サービスのリリース"。

- * NetApp Hybrid Cloud Control * を使用すると、 NetApp HCI を管理できます。NetApp SolidFire Active IQ を使用して、管理サービスのアップグレード、システムの拡張、ログの収集、インストール環境の監視を行うことができます。NetApp Hybrid Cloud Control にログインするには、管理ノードの IP アドレスにアクセスします。
- NetApp Element Plug-in for vCenter Server*は、vSphereのユーザインターフェイス（UI）に統合されたWebベースのツールです。このプラグインは、拡張性と使いやすさを備えた VMware vSphere 用のインターフェイスで、 * NetApp Element ソフトウェア * を実行しているストレージ・クラスタの管理と監視を行うことができます。このプラグインは、 Element UI の代わりに使用できます。プラグインのユーザインターフェイスを使用して、クラスタの検出と設定、ストレージの管理と監視が可能なほか、クラスタ容量からストレージを割り当ててデータストアや仮想データストア（仮想ボリュームの場合）を構成できます。クラスタはネットワーク上では 1 つのローカルグループとして認識され、仮想 IP アドレスによってホストと管理者に示されます。また、クラスタのアクティビティを監視して、さまざまな処理の実行中に発生したイベントのエラーメッセージやアラートメッセージなど、リアルタイムで通知を受け取ることができます。

の詳細を確認してください "vCenter Server 向け NetApp Element プラグイン"。

- デフォルトでは、 NetApp HCI はパフォーマンスとアラートの統計を * NetApp SolidFire Active IQ * サービスに送信します。ネットアップサポートは、通常のサポート契約の一環として、このデータを監視し、パフォーマンスのボトルネックや潜在的なシステムの問題をユーザに警告します。このサービスを利用するにはネットアップサポートアカウントが必要です。まだアカウントを作成していない場合（既存の SolidFire Active IQ アカウントがある場合も含む）は作成する必要があります。

の詳細を確認してください "NetApp SolidFire Active IQ の略"。

NetApp HCI の URL

NetApp HCI で使用する一般的な URL を次に示します。

URL	説明
「ストレージノード上の Bond1G インターフェイスの https://[IPv4 アドレス」	NetApp Deployment Engine ウィザードにアクセスして、 NetApp HCI をインストールおよび設定します。 "詳細はこちら。"
https://<ManagementNodeIP>`	NetApp Hybrid Cloud Control にアクセスして、 NetApp HCI のインストール、拡張、監視、管理サービスの更新を行うことができます。 "詳細はこちら。"
「 https://[IP アドレス」 ： 442`	ノード UI から、ネットワークとクラスタの設定にアクセスし、システムのテストとユーティリティを利用できます。 "詳細はこちら。"
「 https://[management node IP address 」 : 9443	vCenter Plug-in パッケージを vSphere Web Client に登録します。
https://activeiq.solidfire.com`	データを監視し、パフォーマンスのボトルネックや潜在的なシステムの問題に対するアラートを受信します。
https://<ManagementNodeIP>/mnode`	管理ノードから REST API UI を使用して管理サービスを手動で更新します。
https://[storage クラスタ MVIP アドレス '	NetApp Element ソフトウェア UI にアクセスします。

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"

ユーザアカウント

システムのストレージリソースにアクセスするには、ユーザーアカウントを設定する必要があります。

ユーザアカウント管理

ユーザアカウントは、 NetApp Element ソフトウェアベースのネットワーク上のストレージリソースへのアクセスを制御するために使用します。ボリュームを作成するには、ユーザアカウントが少なくとも 1 つ必要です。

ボリュームには、作成時にアカウントが割り当てられます。仮想ボリュームを作成した場合、アカウントはストレージコンテナになります。

その他の考慮事項をいくつか示します。

- アカウントには、そのアカウントに割り当てられているボリュームへのアクセスに必要な CHAP 認証が含まれています。
- アカウントには最大 2 、 000 個のボリュームを割り当てることができますが、 1 つのボリュームが属することのできるアカウントは 1 つだけです。
- ユーザアカウントは、 NetApp Element Management 拡張ポイントで管理できます。

NetApp Hybrid Cloud Control を使用して、次のタイプのアカウントを作成および管理できます。

- ストレージクラスタの管理者ユーザアカウント
- 権限のあるユーザアカウント
- ボリュームアカウント。ボリュームを作成したストレージクラスタのみに固有です。

ストレージクラスタ管理者アカウント

NetApp Element ソフトウェアを実行するストレージクラスタには、次の 2 種類の管理者アカウントがあります。

- * プライマリクラスタ管理者アカウント * ：この管理者アカウントは、クラスタ作成時に作成されます。このアカウントは、クラスタへの最高レベルのアクセス権を持つプライマリの管理アカウントです。このアカウントは、 Linux システムの root ユーザに相当します。この管理者アカウントのパスワードを変更できます。
- * クラスタ管理者アカウント * ：クラスタ管理者アカウントには、クラスタ内で特定のタスクを実行するための限定的な管理アクセスを付与できます。各クラスタ管理者アカウントに割り当てられたクレデンシャルを使用して、ストレージシステム内での API や Element UI の要求が認証されます。

> ノード UI からクラスタ内のアクティブノードにアクセスするには、ローカル（ LDAP 以外）のクラスタ管理者アカウントが必要です。まだクラスタに含まれていないノードにアクセスする場合、アカウントのクレデンシャルは必要ありません。

クラスタ管理者アカウントの管理では、クラスタ管理者アカウントの作成、削除、編集、クラスタ管理者パスワードの変更、およびユーザのシステムアクセスを管理するための LDAP の設定を行うことができます。

権限のあるユーザアカウント

権限のあるユーザアカウントは、ノードおよびクラスタの NetApp Hybrid Cloud Control インスタンスに関連付けられているどのストレージアセットに対しても認証できます。このアカウントを使用すると、すべてのクラスタのボリューム、アカウント、アクセスグループなどを管理できます。

権限のあるユーザアカウントは、 NetApp Hybrid Cloud Control の右上のメニューでユーザ管理オプションを使用して管理しています。

。 "信頼できるストレージクラスタです" は、 NetApp Hybrid Cloud Control がユーザの認証に使用するストレージクラスタです。

信頼できるストレージクラスタで作成されたすべてのユーザが、 NetApp Hybrid Cloud Control にログインできます。他のストレージクラスタで作成されたユーザは、 Hybrid Cloud Control にログインできません。

- 管理ノードにストレージクラスタが 1 つしかない場合は、信頼できるクラスタになります。
- 管理ノードに複数のストレージクラスタがある場合は、それらのクラスタのいずれかが権限のあるクラスタとして割り当てられ、そのクラスタのユーザのみが NetApp Hybrid Cloud Control にログインできます。

NetApp Hybrid Cloud Control の多くの機能は複数のストレージクラスタで使用できますが、認証と許可には制限事項があります。認証と許可に関する制限事項として、信頼できるクラスタのユーザは、他のストレージクラスタのユーザでなくても、 NetApp Hybrid Cloud Control に関連付けられている他のクラスタに対しても操作を実行できます。複数のストレージクラスタの管理を開始する前に、権限のあるクラスタで定義されているユーザが同じ権限を持つ他のすべてのストレージクラスタに定義されていることを確認してください。NetApp Hybrid Cloud Control からユーザを管理できます。

ボリュームアカウント

ボリューム固有のアカウントは、アカウントを作成したストレージクラスタにのみ固有です。これらのアカウントには、ネットワーク全体で特定のボリュームに対する権限を設定できますが、設定したボリューム以外に影響はありません。

ボリュームアカウントは、 NetApp Hybrid Cloud Control Volumes の表で管理されます。

詳細については、こちらをご覧ください

- "ユーザアカウントを管理する"
- "クラスタについて学習する"
- "NetApp HCI のリソースページ"
- "vCenter Server 向け NetApp Element プラグイン"

データ保護

NetApp HCI データ保護の用語には、さまざまな種類のリモートレプリケーション、ボリューム Snapshot 、ボリュームクローニング、保護ドメイン、 Double Helix テクノロジによる高可用性が含まれます。

NetApp HCI データ保護の概念は次のとおりです。

- [リモートレプリケーションの種類]
- データ保護用のボリューム Snapshot
- [ボリュームクローン]

- SolidFire ストレージのバックアップとリストアのプロセスの概要
- [保護ドメイン]
- Double Helix の高可用性

リモートレプリケーションの種類

データのリモートレプリケーションには、次の形式を使用できます。

- [クラスタ間の同期レプリケーションと非同期レプリケーション]
- Snapshot のみのレプリケーション
- SnapMirror を使用した Element クラスタと ONTAP クラスタ間のレプリケーション

を参照してください "TR-4741 ：『 NetApp Element Software Remote Replication 』"。

クラスタ間の同期レプリケーションと非同期レプリケーション

NetApp Element ソフトウェアを実行するクラスタでは、リアルタイムレプリケーションを使用してボリュームデータのリモートコピーを迅速に作成できます。

1 つのストレージクラスタを最大 4 つの他のストレージクラスタとペアリングすることができます。フェイルオーバーやフェイルバックの際には、クラスタペアのどちらかのクラスタからボリュームのデータを同期または非同期でレプリケートできます。

同期レプリケーション

同期レプリケーションでは、ソースクラスタからターゲットクラスタにデータが継続的にレプリケートされ、レイテンシ、パケット損失、ジッター、帯域幅に影響します。

同期レプリケーションは、次のような状況に適しています。

- 複数のシステムを短距離でレプリケート
- に対して地理的にローカルなディザスタリカバリサイト 出典
- 時間の影響を受けやすいアプリケーションとデータベースの保護
- セカンダリサイトを必要とするビジネス継続性アプリケーション プライマリサイトが停止しているときにプライマリサイトとして使用する

非同期レプリケーション

非同期レプリケーションでは、ターゲットクラスタからの確認応答を待たずに、ソースクラスタからターゲットクラスタにデータが継続的にレプリケートされます。非同期レプリケーションでは、書き込みがソースクラスタでコミットされたあとに、クライアント（アプリケーション）に通知されます。

非同期レプリケーションは、次のような状況に適しています。

- ディザスタリカバリサイトはソースから離れており、アプリケーションはネットワークによるレイテンシを許容しません。
- ソースクラスタとターゲットクラスタを接続するネットワークには帯域幅の制限があります。

Snapshot のみのレプリケーション

Snapshot のみのデータ保護では、特定の時点における変更済みのデータをリモートクラスタにレプリケートします。ソースクラスタで作成された Snapshot だけがレプリケートされます。ソースボリュームのアクティブな書き込みはレプリケートされません。

Snapshot レプリケーションの頻度を設定できます。

Snapshot レプリケーションは、非同期レプリケーションまたは同期レプリケーションには影響しません。

SnapMirror を使用した **Element** クラスタと **ONTAP** クラスタ間のレプリケーション

NetApp SnapMirror テクノロジを使用すると、ディザスタリカバリを目的として、 NetApp Element ソフトウェアを使用して作成された Snapshot を ONTAP にレプリケートできます。SnapMirror 関係では、 Element が一方のエンドポイントで、 ONTAP がもう一方のエンドポイントです。

SnapMirror は、地理的に離れたサイトのプライマリストレージからセカンダリストレージへのフェイルオーバー用に設計された、 NetApp Snapshot ™レプリケーションテクノロジです。SnapMirror テクノロジは、セカンダリストレージにある作業データのレプリカまたはミラーを作成します。これにより、プライマリサイトで障害が発生した場合でも、引き続きデータを提供できます。データのミラーリングはボリュームレベルで行われます。

プライマリストレージのソースボリュームとセカンダリストレージのデスティネーションボリュームの関係を、データ保護関係と呼びます。クラスタは、ボリュームが配置されているエンドポイントと呼ばれ、レプリケートされたデータを含むボリュームがピアリングされている必要があります。ピア関係にあることで、クラスタとボリュームの間でデータをセキュアにやり取りできます。

SnapMirror は、 NetApp ONTAP コントローラにあらかじめ搭載されており、 NetApp HCI クラスタと SolidFire クラスタで実行される Element に統合されています。SnapMirror を制御するロジックは ONTAP ソフトウェアにあるため、連携して機能するには、すべての SnapMirror 関係に少なくとも 1 つ ONTAP システムが含まれている必要があります。ユーザは主に Element UI から Element クラスタと ONTAP クラスタの間の関係を管理しますが、一部の管理タスクは NetApp ONTAP System Manager で実行します。また、 ONTAP と Element の両方で使用できる CLI と API を使用して SnapMirror を管理することもできます。

を参照してください "TR-4651 ：『 NetApp SolidFire SnapMirror Architecture and Configuration 』" （ログインが必要です）。

Element ソフトウェアを使用して、クラスタレベルで SnapMirror 機能を手動で有効にする必要があります。SnapMirror 機能はデフォルトでは無効になっており、新規インストール時やアップグレード時に自動的に有効になることはありません。

SnapMirror を有効にしたあと、 Element ソフトウェアの Data Protection タブで SnapMirror 関係を作成できます。

データ保護用のボリューム **Snapshot**

ボリューム Snapshot はボリュームのポイントインタイムコピーであり、あとでその時点にボリュームをリストアする際に使用できます。

Snapshot はボリュームクローンに似ていますが、 Snapshot はボリュームメタデータの単なるレプリカであるため、マウントや書き込みはできません。ボリューム Snapshot の作成には少量のシステムリソースとスペースしか使用されないため、クローニングよりも短い時間で完了します。

Snapshot をリモートのクラスタにレプリケートして、ボリュームのバックアップコピーとして使用できます。レプリケートした Snapshot を使用して、ボリュームを特定の時点にロールバックできます。また、レプリケートした Snapshot からボリュームのクローンを作成できます。

Snapshot は、 SolidFire クラスタから外部のオブジェクトストア、または別の SolidFire クラスタにバックアップできます。Snapshot を外部のオブジェクトストアにバックアップする場合は、オブジェクトストアに接続していて、読み取り / 書き込み処理が許可されている必要があります。

データ保護用に、個々のボリュームまたは複数の Snapshot を作成できます。

ボリュームクローン

単一のボリュームまたは複数のボリュームのクローンは、データのポイントインタイムコピーです。ボリュームをクローニングすると、ボリュームの Snapshot が作成され、次にその Snapshot が参照しているデータのコピーが作成されます。

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

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

SolidFire ストレージのバックアップとリストアのプロセスの概要

他の SolidFire ストレージ、および Amazon S3 または OpenStack Swift と互換性のあるセカンダリオブジェクトストアに対して、ボリュームのバックアップとリストアを実行できます。

ボリュームは次の場所にバックアップできます。

- SolidFire ストレージクラスタ
- Amazon S3 オブジェクトストア
- OpenStack Swift オブジェクトストア

OpenStack Swift または Amazon S3 からボリュームをリストアするときは、元のバックアッププロセスのマニフェスト情報が必要です。SolidFire ストレージシステムにバックアップされているボリュームをリストアする場合は、マニフェスト情報は不要です。

保護ドメイン

保護ドメインとは、ノードまたはノードセットをグループ化したもので、データの可用性を維持したまま、一部または全部で障害が発生する可能性があります。保護ドメインを使用すると、ストレージクラスタをシャーシ（シャーシアフィニティ）またはドメイン全体（シャーシのグループ）の損失から自動的に修復できます。

保護ドメインのレイアウトによって、各ノードが特定の保護ドメインに割り当てられます。

保護ドメインレベルと呼ばれる 2 種類の保護ドメインレイアウトがサポートされます。

- ノードレベルでは、各ノードがそれぞれ独自の保護ドメインに属します。
- シャーシレベルでは、 1 つのシャーシを共有するノードのみが同じ保護ドメインに属します。

- シャーシレベルのレイアウトは、ノードをクラスタに追加するときにハードウェアから自動的に決定されます。
- 各ノードが別々のシャーシに配置されたクラスタでは、この 2 つのレベルは機能的に同じです。

手動で実行できます "保護ドメインの監視を有効にします" NetApp Element Plug-in for vCenter Server を使用する。ノードドメインまたはシャーシドメインに基づいて保護ドメインのしきい値を選択できます。

新しいクラスタの作成時に共有シャーシにあるストレージノードを使用する場合は、保護ドメイン機能を使用してシャーシレベルの障害から保護することを検討してください。

カスタムの保護ドメインレイアウトを定義できます。このレイアウトでは、各ノードが 1 つだけのカスタム保護ドメインに関連付けられます。デフォルトでは、各ノードは同じデフォルトのカスタム保護ドメインに割り当てられます。

Double Helix の高可用性

Double Helix データ保護は、システム内のすべてのドライブに、少なくとも 2 つのデータの冗長コピーを分散するレプリケーション方法です。「 RAID レス」アプローチにより、システムは、ストレージシステムのあらゆるレベルで同時に発生する複数の障害を吸収し、迅速に修復することができます。

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

クラスタ

クラスタとは、ストレージリソースまたはコンピューティングリソースを提供する複数のノードの集まりです。NetApp HCI 1.8 以降では、 2 ノードのストレージクラスタを構成できます。ストレージクラスタは、ネットワーク上では 1 つの論理グループとして認識され、ブロックストレージとしてアクセスできます。

NetApp HCI のストレージレイヤは NetApp Element ソフトウェアで提供され、管理レイヤは NetApp Element Plug-in for vCenter Server で提供されます。ストレージノードは、 Bond10G ネットワークインターフェイスを通じて相互に通信する一連のドライブを搭載したサーバです。各ストレージノードはストレージと管理の 2 つのネットワークに接続され、それぞれに 2 つの独立したリンクを使用して冗長性とパフォーマンスを確保します。各ノードには各ネットワークの IP アドレスが必要です。新しいストレージノードで構成されるクラスタを作成したり、既存のクラスタにストレージノードを追加してストレージの容量とパフォーマンスを拡張したりできます。

信頼できるストレージクラスタです

信頼できるストレージクラスタとは、 NetApp Hybrid Cloud Control でユーザの認証に使用するストレージクラスタです。

管理ノードにストレージクラスタが 1 つしかない場合は、信頼できるクラスタになります。管理ノードに複数のストレージクラスタがある場合は、それらのクラスタのいずれかが権限のあるクラスタとして割り当てられ、そのクラスタのユーザのみが NetApp Hybrid Cloud Control にログインできます。権限のあるクラスタを確認するには、「 get/mnode/about 」 API を使用します。応答では、「 token_url 」フィールドの IP アドレ

スは、権限のあるストレージクラスタの管理仮想 IP アドレス（ MVIP ）です。信頼できるクラスタにないユーザとして NetApp Hybrid Cloud Control にログインしようとすると、ログインに失敗します。

NetApp Hybrid Cloud Control の多くの機能は複数のストレージクラスタを使用するように設計されていますが、認証と許可には制限があります。認証と許可に関する制限事項として、信頼できるクラスタのユーザが、他のストレージクラスタのユーザでなくても、 NetApp Hybrid Cloud Control に関連付けられている他のクラスタに対して操作を実行できることがあります。複数のストレージクラスタの管理を開始する前に、権限のあるクラスタで定義されているユーザが同じ権限を持つ他のすべてのストレージクラスタに定義されていることを確認してください。

NetApp Hybrid Cloud Control を使用してユーザを管理できます。

複数のストレージクラスタの管理を開始する前に、権限のあるクラスタで定義されているユーザが同じ権限を持つ他のすべてのストレージクラスタに定義されていることを確認してください。を参照してください "ストレージクラスタアセットを作成および管理する" 管理ノードのストレージクラスタアセットの使用の詳細については、を参照してください。

有効利用されない容量

新しく追加したノードがクラスタの合計容量の 50% を超えると、容量のルールに準拠するためにこのノードの一部の容量が使用できなくなります（「未使用」）。これは、ストレージ容量が追加されるまで有効です。容量のルールにも違反するような大規模なノードを追加すると、それまでに孤立していたノードは孤立しなくなり、新たに追加したノードが孤立する状態になります。この問題を回避するには、容量を常にペアで追加する必要があります。ノードが孤立すると、該当するクラスタエラーがスローされます。

2 ノードストレージクラスタ

NetApp HCI 1.8 以降では、 2 つのストレージノードでストレージクラスタをセットアップできます。

- 特定のタイプのノードを使用して、 2 ノードストレージクラスタを形成できます。を参照してください "NetApp HCI 1.8 リリースノート"。

  2 ノードクラスタの場合、ストレージノードのモデルは 480GB と 960GB のドライブで構成されるノードに制限され、ノードのモデルタイプは同じである必要があります。

- 2 ノードストレージクラスタは、大容量とハイパフォーマンスの要件に左右されないワークロードを使用する小規模な環境に最適です。
- 2 つのストレージノードに加えて、 2 ノードのストレージクラスタには、 NetApp HCI 監視ノード * が 2 つ含まれています。

  の詳細を確認してください "監視ノード："

- 2 ノードストレージクラスタを 3 ノードストレージクラスタに拡張することができます。3 ノードクラスタでは、ストレージノードの障害から自動で修復できるため、耐障害性が向上します。
- 2 ノードストレージクラスタには、従来の 4 ノードストレージクラスタと同じセキュリティ機能が備わっています。
- 2 ノードストレージクラスタでは、 4 ノードストレージクラスタと同じネットワークが使用されます。ネットワークは、 NetApp HCI の導入時に NetApp Deployment Engine ウィザードを使用してセットアップします。

ストレージクラスタのクォーラム

Element ソフトウェアは、選択したノードからストレージクラスタを作成します。これにより、クラスタ構成のレプリケートされたデータベースが保持されます。クラスタの耐障害性を維持するために、クラスタアンサンブルに参加するには、少なくとも 3 つのノードが必要です。2 ノードクラスタの監視ノードを使用して、有効なアンサンブルクォーラムを形成できるだけの十分なストレージノードがあることを確認します。アンサンブルの作成については、監視ノードよりもストレージノードが推奨されます。2 ノードストレージクラスタに関連する 3 ノード以上のアンサンブルでは、 2 つのストレージノードと 1 つの監視ノードが使用されます。

> 3 ノードのアンサンブルに 2 つのストレージノードと 1 つの監視ノードがある場合、 1 つのストレージノードがオフラインになると、クラスタはデグレード状態になります。2 つの監視ノードのうち、アンサンブルでアクティブにできる監視ノードは 1 つだけです。2 つ目の監視ノードは、バックアップロールを実行するため、アンサンブルに追加できません。オフラインのストレージノードがオンライン状態に戻るか、交換用ノードがクラスタに追加されるまで、クラスタはデグレード状態のままです。

監視ノードで障害が発生した場合は、残りの監視ノードがアンサンブルに参加して、 3 ノードのアンサンブルを形成します。障害が発生した監視ノードの代わりに新しい監視ノードを導入できます。

2 ノードストレージクラスタでの自動修復と障害処理

従来のクラスタの一部であるノードでハードウェアコンポーネントに障害が発生した場合、クラスタ内の他の使用可能なノードに障害が発生したコンポーネント上のデータがリバランシングされます。2 ノードストレージクラスタでは自動修復機能を使用できません。少なくとも 3 つの物理ストレージノードがクラスタで自動的に修復可能である必要があるためです。2 ノードクラスタの 1 つのノードで障害が発生した場合、 2 ノードクラスタではデータのコピーをもう 1 つ作成する必要はありません。残りのアクティブストレージノードでは、ブロックデータに対する新しい書き込みがレプリケートされます。障害が発生したノードを交換してクラスタに追加すると、 2 つの物理ストレージノード間でデータがリバランシングされます。

3 つ以上のノードを含むストレージクラスタ

2 つのストレージノードから 3 つのストレージノードに拡張することで、ノードとドライブの障害時に自動修復が可能になり、クラスタの耐障害性が向上します。ただし、追加の容量は提供されません。を使用してを展開できます "NetApp Hybrid Cloud Control の UI"。2 ノードクラスタから 3 ノードクラスタに拡張する場合は、容量が孤立する可能性があります（を参照） [有効利用されない容量]）。インストール前に未使用の容量に関する警告が表示されます。1 つの監視ノードを使用して、ストレージノードに障害が発生した場合にアンサンブルクォーラムを維持することもできます。スタンバイ側の監視ノードも同様です。3 ノードストレージクラスタを 4 ノードクラスタに拡張すると、容量とパフォーマンスが向上します。4 ノードクラスタでは、監視ノードがクラスタクォーラムを形成する必要がなくなります。コンピューティングノードは最大 64 個、ストレージノードは 40 個まで拡張できます。

詳細については、こちらをご覧ください

- "NetApp HCI 2 ノードストレージクラスタ | TR-4823"
- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire と Element ソフトウェアドキュメントセンター"

ノード

ノードは、ブロックストレージとコンピューティング機能を提供するためにクラスタに

グループ化されたハードウェアリソースまたは仮想リソースです。

NetApp HCI および Element ソフトウェアでは、クラスタのさまざまなノードロールが定義されています。ノードのロールには、 * 管理ノード * 、 * ストレージノード * 、 * コンピューティングノード * 、 * NetApp HCI 監視ノード * の 4 種類があります。

管理ノード

管理ノード（ mNode とも呼ばれます）は、ストレージクラスタと通信して管理操作を実行しますが、ストレージクラスタのメンバーではありません。管理ノードは、 API 呼び出しを使用してクラスタに関する情報を定期的に収集し、この情報を Active IQ に報告してリモート監視（有効な場合）に利用します。管理ノードでは、クラスタノードのソフトウェアアップグレードの調整も担当します。

管理ノードは、 Element ソフトウェアベースの 1 つ以上のストレージクラスタと同時に実行される仮想マシン（ VM ）です。アップグレードに加え、監視と計測などのシステムサービスの提供、クラスタのアセットと設定の管理、システムテストとユーティリティの実行、ネットアップサポートによるトラブルシューティングアクセスの有効化にも使用されます。Element 11.3 リリース以降、管理ノードはマイクロサービスホストとして機能するようになりました。そのため、メジャーリリースを待つことなく、希望するソフトウェアサービスを更新できます。これらのマイクロサービスまたは管理サービス（ Active IQ コレクタ、 vCenter Plug-in 用の QoSSIOC 、管理ノードサービスなど）は、サービスバンドルとして頻繁に更新されます。

ストレージノード

NetApp HCI ストレージノードは、 NetApp HCI システムのストレージリソースを提供するハードウェアです。ノード内のドライブには、データの格納用と管理用にブロックスペースとメタデータスペースが確保されます。各ノードには、 NetApp Element ソフトウェアの工場出荷時のイメージが含まれています。NetApp HCI ストレージノードは、 NetApp Element Management 拡張ポイントを使用して管理できます。

コンピューティングノード

NetApp HCI コンピューティングノードは、 NetApp HCI 環境での仮想化に必要な、 CPU 、メモリ、ネットワークなどのコンピューティングリソースを提供するハードウェアです。各サーバは VMware ESXi を実行するため、 vSphere のホストおよびクラスタメニューにあるプラグイン以外で NetApp HCI コンピューティングノードの管理（ホストの追加または削除）を行う必要があります。コンピューティングノードは、 4 ノードストレージクラスタと 2 ノードストレージクラスタのどちらであるかに関係なく、 NetApp HCI 環境では最低 2 つの数が維持されます。

監視ノード

NetApp HCI 監視ノードは、 Element ソフトウェアベースのストレージクラスタと並行してコンピューティングノードで実行される VM です。監視ノードでは、スライスサービスまたはブロックサービスがホストされません。監視ノードを使用すると、ストレージノードに障害が発生した場合のストレージクラスタの可用性を確保できます。監視ノードは、他のストレージノードと同じ方法で管理およびアップグレードできます。ストレージクラスタには、最大 4 つの監視ノードを含めることができます。主な目的は、有効なアンサンブルクォーラムを形成できるだけの十分な数のクラスタノードが存在することを確認することです。

- ベストプラクティス：監視ノードの VM でコンピューティングノードのローカルデータストアを使用するように設定する（ NDE のデフォルト設定）。 SolidFire ストレージボリュームなどの共有ストレージには設定しないでください。VM が自動的に移行されないようにするには、監視ノード VM の Distributed Resource Scheduler （ DRS ）自動化レベルを「 * Disabled 」に設定します。これにより、両方の監視ノードが同じコンピューティングノードで実行されないようにし、非ハイアベイラビリティ（ HA ）ペア構成を作成することができます。

の詳細を確認してください "監視ノードのリソース要件" および "監視ノードの IP アドレスの要件"。

2 ノードストレージクラスタでは、監視ノードに障害が発生した場合の冗長性を確保するために、最低 2 つの監視ノードが導入されます。NetApp HCI のインストールプロセスで監視ノードがインストールされると、 VM テンプレートが VMware vCenter に格納されます。これを使用して、誤って削除された場合、失われた場合、または破損した場合に監視ノードを再導入できます。また、監視ノードをホストしていた障害コンピューティングノードと交換する必要がある場合は、テンプレートを使用して監視ノードを再導入することもできます。手順については、 2 ノードおよび 3 ノードのストレージクラスタに対する監視ノードの再導入 * を参照してください "こちらをご覧ください"。

詳細については、こちらをご覧ください

- "NetApp HCI 2 ノードストレージクラスタ | TR-4823"
- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire と Element ソフトウェアドキュメントセンター"

ストレージ

メンテナンスモード

ソフトウェアのアップグレードやホストの修復などのメンテナンスのためにストレージノードをオフラインにする必要がある場合は、そのノードのメンテナンスモードを有効にすることで、ストレージクラスタの残りの部分への I/O の影響を最小限に抑えることができます。メンテナンスモードは、アプライアンスノードと SolidFire エンタープライズ SDS ノードの両方で使用できます。

ストレージノードの電源をオフにすると、 HCC のストレージページのノードステータス列に「使用不可」と表示されます。これは、クラスタ側から見たノードのステータスを示します。ノードの電源オフステータスは、ノードのホスト名の横にある * オフライン * アイコンで示されます。

ストレージノードを保守モードに移行できるのは、ノードが正常で（クラスタエラーがブロックされていない）、かつストレージクラスタが単一ノード障害に対応している場合のみです。正常なトレラントノードに対してメンテナンスモードをイネーブルにすると、ノードはすぐには移行されません。このノードは、次の条件が満たされるまで監視されます。

- ノードでホストされているすべてのボリュームがフェイルオーバーされました

- ノードはのプライマリではなくなりました 任意のボリューム
- 一時スタンバイノードは、対象のすべてのボリュームに割り当てられます フェイルオーバーしました

これらの条件を満たすと、ノードは保守モードに移行します。5 分以内に上記の条件が満たされないと、ノードは保守モードになりません。

ストレージノードのメンテナンスモードを無効にすると、次の条件が満たされるまでノードが監視されます。

- すべてのデータがノードに完全にレプリケートされます
- ブロックしているクラスタのすべての障害が解決されます
- ホストされているボリュームに対する一時的なスタンバイノードの割り当て ノードが非アクティブ化されました

これらの条件を満たしている場合、ノードはメンテナンスモードから移行されます。1 時間以内に上記の条件を満たしていないと、ノードのメンテナンスモードからの移行が失敗します。

メンテナンスモードで作業する際のメンテナンスモード処理の状態は、 Element API で確認できます。

- * 無効 *: メンテナンスが要求されていません。
- * FailedToRecover * ：ノードのメンテナンスからのリカバリに失敗しました。
- *RecoveringFromMaintenance *: ノードはメンテナンスからリカバリ中です
- *PreparingForMaintenance *: ノードのメンテナンスを実行できるようにするためのアクションが実行されています。
- * ReadyForMaintenance * ：ノードはメンテナンスの準備ができています。

詳細については、こちらをご覧ください

- "Element API のメンテナンスモードを有効にします"
- "Element API のメンテナンスモードを無効にします"
- "NetApp Element API ドキュメント"
- "NetApp HCI のリソースページ"
- "vCenter Server 向け NetApp Element プラグイン"

個のボリューム

ストレージは、 NetApp Element システムではボリュームとしてプロビジョニングされます。ボリュームは、 iSCSI または Fibre Channel クライアントを使用してネットワーク経由でアクセスされるブロックデバイスです。

NetApp Element Plug-in for vCenter Server では、ユーザアカウントのボリュームを作成、表示、編集、削除、クローニング、バックアップ、リストアすることができます。また、クラスタ上の各ボリュームの管理や、ボリュームアクセスグループのボリュームの追加と削除も可能です。

永続ボリューム

永続ボリュームを使用すると、管理ノードの設定データをローカルな VM ではなく指定したストレージクラスタに格納できるため、管理ノードが失われた場合や削除された場合でもデータを保持することができます。永続ボリュームは、オプションでありながら推奨される管理ノード設定です。

NetApp Deployment Engine を使用して NetApp HCI の管理ノードを導入する場合、永続ボリュームは自動的に有効化されて設定されます。

永続ボリュームを有効にするオプションは、新しい管理ノードの導入時のインストールスクリプトとアップグレードスクリプトに含まれています。永続ボリュームは Element ソフトウェアベースのストレージクラスタ上のボリュームであり、ホスト管理ノード VM のノード設定情報が VM が使用されなくなったあとも格納されます。管理ノードが失われた場合は、交換用の管理ノード VM を再接続して失われた VM の設定データをリカバリできます。

インストールまたはアップグレード時に永続ボリューム機能を有効にすると、割り当てられたクラスタ上の名前に適用された名前の付いた複数のボリュームが自動的に作成されます。これらのボリュームは、 Element ソフトウェアベースのボリュームと同様に、 Element ソフトウェア Web UI 、 NetApp Element Plug-in for vCenter Server 、または API を使用して表示できます。リカバリに使用できる現在の設定データを保持するためには、永続ボリュームが管理ノードに iSCSI 接続された状態で稼働している必要があります。

> 管理サービスに関連付けられた永続ボリュームが作成され、インストールまたはアップグレード時に新しいアカウントに割り当てられます。永続ボリュームを使用している場合は、ボリュームや関連付けられているアカウントを変更または削除しないでください

詳細については、こちらをご覧ください

- "ボリュームを管理します"
- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire と Element ソフトウェアドキュメントセンター"

ボリュームアクセスグループ

ボリュームアクセスグループは、ユーザが iSCSI イニシエータまたは Fibre Channel イニシエータを使用してアクセスできるボリュームの集まりです。

ボリュームアクセスグループを作成して使用することで、一連のボリュームへのアクセスを制御できます。一連のボリュームと一連のイニシエータをボリュームアクセスグループに関連付けると、アクセスグループはそれらのイニシエータにそのボリュームセットへのアクセスを許可します。

ボリュームアクセスグループには次の制限があります。

- ボリュームアクセスグループあたり最大 128 個のイニシエータ
- ボリュームあたり最大 64 個のアクセスグループ。
- 1 つのアクセスグループに含めることができるボリュームは最大 2 、 000 個です。
- 1 つの IQN または WWPN が属することのできるボリュームアクセスグループは 1 つだけです。

詳細については、こちらをご覧ください

- "ボリュームアクセスグループを管理します"
- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire と Element ソフトウェアドキュメントセンター"

イニシエータ

イニシエータはクライアントとボリューム間の通信のエントリポイントとして機能し、外部クライアントからクラスタ内のボリュームへのアクセスを可能にします。ストレージボリュームへのアカウントベースのアクセスではなく、 CHAP ベースのアクセスにイニシエータを使用できます。1 つのイニシエータをボリュームアクセスグループに追加すると、ボリュームアクセスグループのメンバーは認証なしでグループに追加されたすべてのストレージボリュームにアクセスできるようになります。1 つのイニシエータは 1 つのアクセスグループにのみ属することができます。

詳細については、こちらをご覧ください

- "イニシエータを管理する"
- "ボリュームアクセスグループ"
- "ボリュームアクセスグループを管理します"
- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire と Element ソフトウェアドキュメントセンター"

カスタムの保護ドメイン

カスタムの保護ドメインレイアウトを定義できます。このレイアウトでは、各ノードが 1 つだけのカスタム保護ドメインに関連付けられます。デフォルトでは、各ノードは同じデフォルトのカスタム保護ドメインに割り当てられます。

カスタムの保護ドメインが割り当てられていない場合：

- クラスタ処理には影響はありません。
- カスタムレベルは、トレラントでも耐障害性でもありません。

複数のカスタム保護ドメインが割り当てられている場合、各サブシステムは重複を別々のカスタム保護ドメインに割り当てます。これができない場合は、重複したデータが別のノードに割り当てられます。各サブシステム（ビン、スライス、プロトコルエンドポイントプロバイダ、アンサンブルなど）は、それぞれ独立して機能します。

> カスタム保護ドメインを使用すると、ノードがシャーシを共有しないことが前提になります。

次の Element API メソッドは、これらの新しい保護ドメインを公開します。

- GetProtectionDomainLayout - 各ノードのシャーシとカスタム保護ドメインを表示します。

- SetProtectionDomainLayout - 各ノードにカスタム保護ドメインを割り当てることができます。

カスタム保護ドメインの使用の詳細については、ネットアップサポートにお問い合わせください。

詳細については、こちらをご覧ください

"Element API を使用してストレージを管理します"

NetApp HCI ライセンス

NetApp HCI を使用する場合、使用する内容によっては追加のライセンスが必要になることがあります。

NetApp HCI と VMware vSphere のライセンス

VMware vSphere のライセンスは、構成によって異なります。

ネットワークオプション	ライセンス
オプション A ：ケーブル 2 本で VLAN タギングを使用（すべてのコンピューティングノード）	vSphere Distributed Switch を使用する必要があります。これには VMware vSphere Enterprise Plus ライセンスが必要です。
オプション B ：タグ付き VLAN を使用するコンピューティングノード用ケーブル 6 本（ H410C 2RU 4 ノードコンピューティングノード）	この構成では、 vSphere Standard Switch がデフォルトとして使用されます。vSphere Distributed Switch をオプションで使用するには、 VMware Enterprise Plus ライセンスが必要です。
オプション C ：ネイティブ VLAN とタグ付き VLAN を使用するコンピューティングノード用ケーブル × 6 （ H410C 、 2RU 、 4 ノードコンピューティングノード）	この構成では、 vSphere Standard Switch がデフォルトとして使用されます。vSphere Distributed Switch をオプションで使用するには、 VMware Enterprise Plus ライセンスが必要です。

NetApp HCI と ONTAP Select のライセンス

購入した NetApp HCI システムと組み合わせて使用する ONTAP Select のバージョンを提供している場合は、次の制限事項が追加で適用されます。

- NetApp HCI システム販売にバンドルされている ONTAP Select ライセンスは、 NetApp HCI コンピューティングノードと組み合わせてのみ使用できます。
- 対象となる ONTAP Select インスタンスのストレージは、 NetApp HCI ストレージノード上にのみ存在する必要があります。
- サードパーティ製コンピューティングノードやサードパーティ製ストレージノードの使用は禁止されています。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "SolidFire と Element ソフトウェアドキュメントセンター"

NetApp Hybrid Cloud Control の最大構成数

NetApp HCI には、コンピューティングのライフサイクルとストレージ管理を簡易化する NetApp Hybrid Cloud Control が搭載されています。NetApp HCI および NetApp SolidFire ストレージクラスタのストレージノードでの Element ソフトウェアのアップグレードや、 NetApp HCI の NetApp HCI コンピューティングノードでのファームウェアのアップグレードがサポートされます。NetApp HCI の管理ノードではデフォルトで使用できます。

ネットアップが提供する NetApp HCI 環境内のハードウェアコンポーネントとソフトウェアコンポーネントの通信に加えて、 NetApp Hybrid Cloud Control は、 VMware vCenter などのお客様の環境内のサードパーティコンポーネントと通信します。ネットアップは、 NetApp Hybrid Cloud Control の機能およびお客様の環境でこれらのサードパーティコンポーネントとの連動性を、特定の規模で認定します。NetApp Hybrid Cloud Control の運用を最適化するために、構成の最大数には範囲内で設定することを推奨します。

この最大数を超えると、低速のユーザインターフェイスや API 応答、機能の利用不可など、 NetApp Hybrid Cloud Control で問題が発生する可能性があります。構成の上限を超えて設定されている環境で NetApp Hybrid Cloud Control とネットアップの製品サポートを契約された場合は、構成の最大数がドキュメントに記載されている範囲内に収まるように設定を変更するように求められます。

設定の最大数

NetApp Hybrid Cloud Control では、最大 500 個のネットアップコンピューティングノードを含む VMware vSphere 環境がサポートされます。NetApp Element ソフトウェアベースのストレージクラスタを 20 個までサポートし、クラスタあたり 40 個のストレージノードで構成されます。

NetApp HCI セキュリティ

NetApp HCI を使用すると、業界標準のセキュリティプロトコルでデータが保護されます。

ストレージノードの保存データの暗号化

NetApp HCI では、ストレージクラスタに格納されているすべてのデータを暗号化できます。

ストレージノード内の暗号化に対応したすべてのドライブで、ドライブレベルの AES 256 ビット暗号化が使用されます。各ドライブには、ドライブが最初に初期化されたときに作成される、専用の暗号化キーがあります。暗号化機能を有効にすると、ストレージクラスタ全体のパスワードが作成され、複数のチャンクとしてクラスタ内のすべてのノードに配信されます。どのノードにもパスワード全体が格納されることはありません。このパスワードを使用して、ドライブへのすべてのアクセスが保護されます。ドライブのロックを解除するにはパスワードが必要です。ドライブがすべてのデータを暗号化しているため、データのセキュリティは常に確保されます。

保存データの暗号化を有効にしても、ストレージクラスタのパフォーマンスと効率には影響はありません。また、 Element API または Element UI を使用して暗号化が有効なドライブまたはノードをストレージクラスタ

から削除すると、保存データの暗号化がドライブで無効になり、ドライブは安全に消去されて、これらのドライブに格納されていたデータが保護されます。ドライブを取り外した後、「 SecureEraseDrives 」 API メソッドを使用してドライブを安全に消去できます。ストレージクラスタからドライブまたはノードを強制的に削除した場合は、データはクラスタ全体のパスワードおよびドライブごとの暗号化キーによって引き続き保護されます。

保存データの暗号化を有効または無効にする方法については、を参照してください "クラスタで暗号化を有効または無効にします" SolidFire and Element ドキュメントセンターを参照してください。

保存データのソフトウェア暗号化

保存データのソフトウェア暗号化を使用すると、ストレージクラスタ内の SSD に書き込まれるすべてのデータを暗号化できます。これにより、自己暗号化ドライブ（ SED ）を搭載していない SolidFire エンタープライズ SDS ノードで、暗号化の第一層が実現します。

外部キー管理

サードパーティの KMIP 準拠キー管理サービス（ KMS ）を使用してストレージクラスタの暗号化キーを管理するように Element ソフトウェアを設定できます。この機能を有効にすると、ストレージクラスタ全体のドライブアクセスパスワード暗号化キーが KMS によって指定した値で管理されます。Element では、次のキー管理サービスを使用できます。

- Gemalto SafeNet KeySecure の各コマンドを入力します
- SafeNet at KeySecure の指定
- HyTrust KeyControl の略
- Vormetric データセキュリティ Manager の略
- IBM Security Key Lifecycle Manager の略

外部キー管理の設定の詳細については、を参照してください "外部キー管理の開始" SolidFire and Element ドキュメントセンターを参照してください。

多要素認証

多要素認証（ MFA ）を使用することで、ログイン時に NetApp Element Web UI またはストレージノード UI で認証するためのさまざまな種類の証拠をユーザに提示する必要があります。既存のユーザ管理システムおよびアイデンティティプロバイダと統合されたログインに対して多要素認証のみを受け入れるように Element を設定できます。Element を既存の SAML 2.0 アイデンティティプロバイダと統合するように設定できます。これにより、パスワードとテキストメッセージ、パスワードと E メールメッセージ、その他の方法など、複数の認証方式を適用できます。

多要素認証を、 Microsoft Active Directory Federation Services （ADFS ）や Shibboleth など、 SAML 2.0 対応の一般的なアイデンティティプロバイダ（ IdP ）とペアリングできます。

MFA を設定するには、を参照してください "多要素認証の有効化" SolidFire and Element ドキュメントセンターを参照してください。

HTTPS 向けの FIPS 140-2 と保存データ暗号化

NetApp SolidFire ストレージクラスタおよび NetApp HCI システムでは、暗号モジュールに関する Federal Information Processing Standard （ FIPS ；連邦情報処理標準） 140-2 の要件に準拠した暗号化がサポートさ

れています。SolidFire または NetApp HCI クラスタで、 HTTPS 通信とドライブ暗号化の両方に対して FIPS 140-2 準拠を有効にすることができます。

クラスタで FIPS 140-2 動作モードを有効にすると、クラスタは NetApp Cryptographic Security Module （ NCSM ）をアクティブ化し、 NetApp Element UI および API との HTTPS を介したすべての通信に FIPS 140-2 レベル 1 認定の暗号化を利用します。FIPS 140-2 HTTPS 暗号化をイネーブルにするには 'EnableFeature` Element API を 'fips' パラメータとともに使用しますFIPS 対応ハードウェアを搭載したストレージクラスタでは、「 EnableFeature` Element API 」パラメータを「 FipsDrives 」パラメータとともに使用して、保存データの FIPS ドライブ暗号化を有効にすることもできます。

新しいストレージクラスタでの FIPS 140-2 暗号化の準備の詳細については、を参照してください "FIPS ドライブをサポートするクラスタを作成する"。

既存の準備が完了したクラスタで FIPS 140-2 を有効にする方法の詳細については、を参照してください "EnableFeature Element API"。

パフォーマンスと QoS

SolidFire ストレージクラスタでは、サービス品質（ QoS ）パラメータをボリューム単位で指定できます。QoS を定義する 3 つの設定可能なパラメータである Min IOPS 、 Max IOPS 、および Burst IOPS を使用して、 IOPS （ 1 秒あたりの入出力）で測定されるクラスタパフォーマンスを保証することができます。

> SolidFire Active IQ には、最適な設定と QoS 設定に関するアドバイスを提供する QoS 推奨ページがあります。

QoS パラメータ

IOPS パラメータは、次のように定義します。

- * 最小 IOPS * - ストレージクラスタがボリュームに提供する平常時の最小 IOPS 。ボリュームに設定された Min IOPS は、そのボリュームに対して最低限保証されるパフォーマンスレベルです。パフォーマンスがこのレベルを下回ることはありません。
- * 最大 IOPS * - ストレージクラスタがボリュームに提供する平常時の最大 IOPS 。クラスタの IOPS レベルが非常に高い場合も、 IOPS パフォーマンスはこのレベル以下に抑えられます。
- * Burst IOPS * - 短時間のバースト時に許容される最大 IOPS 。ボリュームが Max IOPS 未満で動作している間は、バーストクレジットが蓄積されます。パフォーマンスレベルが非常に高くなって最大レベルに達した場合、ボリュームで IOPS の短時間のバーストが許容されます。

  Element ソフトウェアでは、 IOPS 使用率が低い状態でクラスタが稼働しているときに Burst IOPS が使用されます。

  個々のボリュームは、蓄積したバーストクレジットを使用して、一定の「バースト期間」中は Max IOPS を最大で Burst IOPS レベルまで一時的に超過することができます。 ボリュームのバースト時間は最大で 60 秒です。クラスタの容量にバーストに対応できるだけの余力があることが条件になります。ボリュームは、 Max IOPS 未満で動作している 1 秒ごとに、 1 秒分のバーストクレジットを蓄積します（最大 60 秒）。

  Burst IOPS には 2 つの制限があります。

- ボリュームは、蓄積したバーストクレジット数と同じ秒数だけ Max IOPS を超過できます。
- ボリュームが Max IOPS の設定を超えた場合は、 Burst IOPS の設定によって制限されます。つまり、バースト時の IOPS がボリュームの Burst IOPS の設定を超えることはありません。

* Effective Max Bandwidth * - 最大帯域幅は、（ QoS 曲線に基づく） IOPS に IO サイズを掛けて計算されます。

例： QoS パラメータを Min IOPS = 100 、 Max IOPS = 1000 、 Burst IOPS = 1500 に設定した場合、パフォーマンスの品質は次のようになります。

- 各ワークロードは、クラスタで IOPS に対するワークロードの競合が発生するまでは、最大で 1000 IOPS を持続的に使用することができます。競合が発生すると、すべてのボリュームの IOPS が指定の QoS 範囲内に戻ってパフォーマンスの競合が解消されるまで、 IOPS が少しずつ引き下げられます。
- すべてのボリュームのパフォーマンスは、最大で Min IOPS の 100 まで引き下げられます。Min IOPS である 100 を下回ることはなく、ワークロードの競合が解消されれば 100 IOPS よりも高いレベルにとどまることが可能です。
- パフォーマンスは長期間にわたって 1000 IOPS を超えることも、 100 IOPS を下回ることもありません。1500 IOPS （ Burst IOPS ）のパフォーマンスは、 Max IOPS 未満で動作することでバーストクレジットを蓄積したボリュームに対して短時間の間のみ許容されます。バーストレベルが持続することはありません。

QoS 値の制限

QoS の最小値と最大値を次に示します。

パラメータ	最小値	デフォルト	**4KB × 4**	**5 8 KB**	**6 、 16KB** です	**262KB**
最小 IOPS	50	50	15,000	9 、 375 *	5556 *	385 *
最大 IOPS	100	15,000	200,000 **	125,000	74,074	5128
バースト IOPS	100	15,000	200,000 **	125,000	74.074	5128

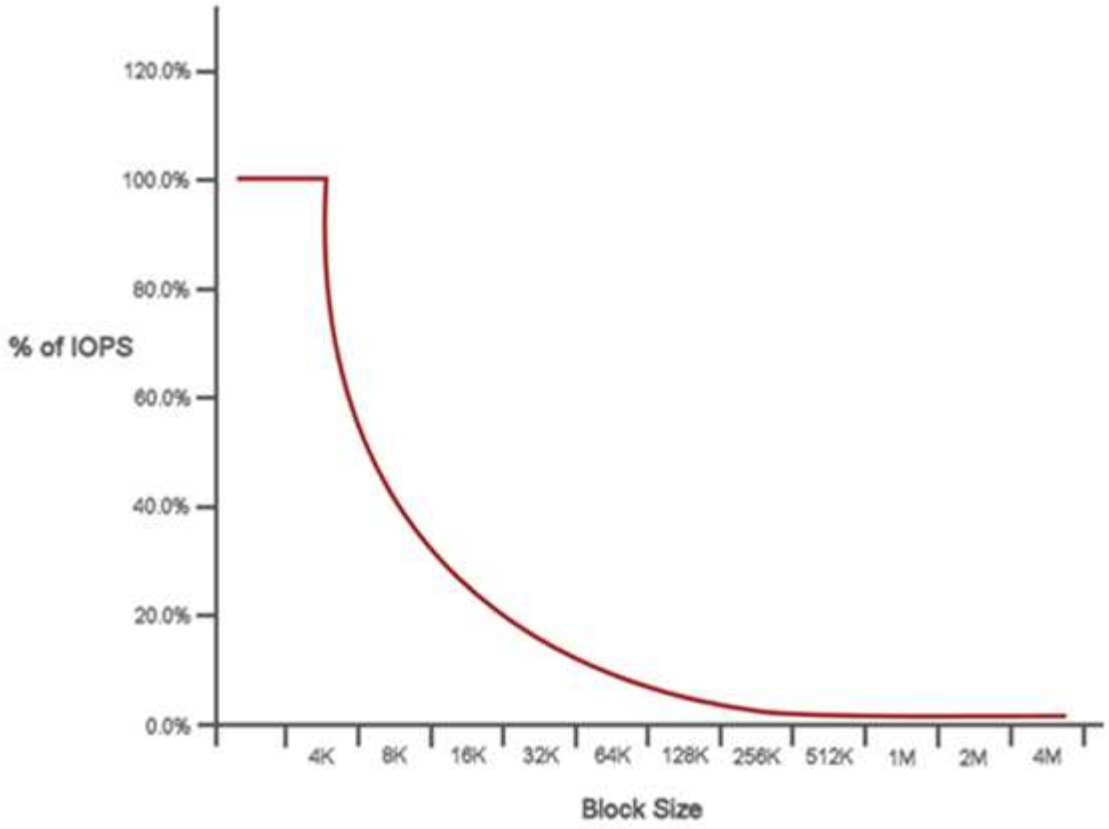
- これらは概算値です。** 最大 IOPS とバースト IOPS は最大 200 、 000 に設定できます。ただし、この設定は、ボリュームのパフォーマンスの制限を意図的に解放する場合にのみ使用できます。実際のボリュームの最大パフォーマンスは、クラスタの使用率とノードごとのパフォーマンスによって制限されます。

QoS パフォーマンス

QoS パフォーマンス曲線は、ブロックサイズと IOPS の割合の関係を示しています。

アプリケーションが取得できる IOPS には、ブロックサイズと帯域幅が直接影響します。Element ソフトウェアは、ブロックサイズを 4k に正規化することで受信したブロックサイズを考慮します。システムは、ワークロードに応じてブロックサイズを増やすことがあります。ブロックサイズが大きくなると、システムはそのブロックサイズを処理するために必要なレベルまで帯域幅を増やします。帯域幅が増えると、システムが処理可能な IOPS は減少します。

QoS パフォーマンス曲線は、ブロックサイズの増大と IOPS の割合の減少の関係を示しています。



たとえば、ブロックサイズが 4k で帯域幅が 4000KBps であれば、 IOPS は 1000 です。ブロックサイズが 8k に増え、帯域幅が 5000KBps に増えると、 IOPS は 625 まで減少します。ブロックサイズを考慮することで、バックアップやハイパーバイザーアクティビティなど、より大きなブロックサイズを使用する優先度の低いワークロードは、より小さいブロックサイズを使用する優先度の高いトラフィックに必要なパフォーマンスをあまり消費しません。

QoS ポリシー

標準的な QoS 設定を QoS ポリシーとして作成および保存して、複数のボリュームに適用することができます。

QoS ポリシーは、データベースサーバ、アプリケーションサーバ、インフラサーバなど、ほとんどリブートされずにストレージへの常時アクセスが必要となるサービス環境に最適です。個々のボリュームの QoS は、仮想デスクトップや専用キオスクタイプの VM など、 1 日に何回か再起動、電源投入、電源オフなどの軽用途の VM に最適です。

QoS ポリシーと QoS ポリシーを一緒に使用しないでください。QoS ポリシーを使用している場合は、ボリュームでカスタム QoS を使用しないでください。カスタム QoS は、ボリュームの QoS 設定に対して QoS ポリシーの値を上書きして調整します。

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

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"

要件と導入前のタスク

NetApp HCI 導入の要件の概要

NetApp HCI には、データセンターで適切に運用するための物理的要件とネットワーク要件があります。導入を開始する前に、以下に示す要件および推奨事項を満たしていることを確認してください。

NetApp HCI ハードウェアが届く前に、ネットアッププロフェッショナルサービスが提供する導入前ワークブックのチェック項目を必ず実施しておいてください。本ドキュメントには、 NetApp HCI の導入を成功させるためにネットワークと環境を準備するために必要な作業の包括的なリストが記載されています。

要件と導入前タスクへのリンクを次に示します。

- "ネットワークポートの要件"
- "ネットワークとスイッチの要件"
- "ネットワークケーブルの要件"
- "IP アドレスの要件"
- "ネットワーク構成："
- "DNS とタイムキーパー機能の要件"
- "環境要件"
- "保護ドメイン"
- "2 ノードストレージクラスタの場合は、監視ノードのリソース要件が必要です"

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

管理ノードの要件

ベストプラクティスとして、 1 つの管理ノードを 1 つの VMware vCenter インスタンスに関連付けるだけで、同じストレージリソースおよびコンピューティングリソースまたは vCenter インスタンスを複数の管理ノードに定義することは避けてください。複数の管理ノードで同じリソースを定義していると、ネットアップ ActiveIQ で誤ったリソースレポートなど、原因の問題が発生する可能性があります。

ネットワークポートの要件

システムをリモートで管理し、データセンター外部のクライアントがリソースに接続できるようにし、内部サービスが正常に機能するようにするために、データセンターのエッジファイアウォールで次のポートを許可する必要があります。システムの使用方法に

よっては、これらのポート、 URL 、または IP アドレスの一部は不要な場合もあります。

特に記載がないかぎり、すべてのポートがTCPであり、NetAppサポートサーバ、管理ノード、およびElementソフトウェアを実行するノードの間の3ウェイハンドシェイク通信がすべてサポートされている必要があります。たとえば、管理ノードのソースのホストはTCPポート443を介してストレージクラスタのMVIPデスティネーションのホストと通信し、デスティネーションホストは任意のポートを介してソースホストと通信します。

この表では次の略語を使用します。

- mip ：管理 IP アドレス。ノードごとのアドレスです
- sip ：ストレージ IP アドレス。ノードごとのアドレスです
- MVIP ：管理仮想 IP アドレス
- SVIP ：ストレージ仮想 IP アドレス

ソース	宛先	ポート	説明
コンピューティングノードの BMC / IPMI	管理ノード	111 TCP/UDP	NetApp Hybrid Cloud Control の API 通信
コンピューティングノードの BMC / IPMI	管理ノード	137-138 UDP	NetApp Hybrid Cloud Control の API 通信
コンピューティングノードの BMC / IPMI	管理ノード	445	NetApp Hybrid Cloud Control の API 通信
コンピューティングノードの BMC / IPMI	管理ノード	623 UDP	Remote Management Control Protocol （ RMCP ）ポート。NetApp Hybrid Cloud Control 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する場合は必須です。
コンピューティングノードの BMC / IPMI	管理ノード	2049 TCP/UDP	NetApp Hybrid Cloud Control の API 通信
iSCSI クライアント	ストレージクラスタの MVIP	443	（オプション） UI および API アクセス
iSCSI クライアント	ストレージクラスタの SVIP	3260	クライアント iSCSI 通信
iSCSI クライアント	ストレージノードの SIP	3260	クライアント iSCSI 通信
管理ノード	「 fsupport.solidfire.com 」	22	サポートアクセス用リバース SSH トンネル
管理ノード	ストレージノードの MIP	22	サポート用 SSH アクセス
管理ノード	DNS サーバ	53 TCP/UDP	DNS ルックアップ
管理ノード	コンピューティングノードの BMC / IPMI	139	NetApp Hybrid Cloud Control の API 通信

ソース	宛先	ポート	説明
管理ノード	ストレージノードの MIP	442	ストレージノードおよび Element ソフトウェアへの UI および API アクセスアップグレード
管理ノード	ストレージノード MVIP	442	ストレージノードおよび Element ソフトウェアへの UI および API アクセスアップグレード
管理ノード	「 23.32.54.122`, 」216.240.21.15`	443	Element ソフトウェアのアップグレード
管理ノード	ベースボード管理コントローラ（ BMC ）	443	ハードウェア監視およびインベントリ接続（ Redfish および IPMI コマンド）
管理ノード	コンピューティングノードの BMC / IPMI	443	NetApp Hybrid Cloud Control の HTTPS 通信
管理ノード	「 onitoring.solidfire.com 」と入力します	443	Active IQ に報告するストレージクラスタ
管理ノード	ストレージクラスタの MVIP	443	ストレージノードおよび Element ソフトウェアへの UI および API アクセスアップグレード
管理ノード	VMware vCenter	443	NetApp Hybrid Cloud Control の HTTPS 通信
管理ノード	コンピューティングノードの BMC / IPMI	623 UDP	Remote Management Control Protocol （ RMCP ）ポート。NetApp Hybrid Cloud Control 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する場合は必須です。
管理ノード	ストレージノードのBMC / IPMI	623 UDP	RMCPポート。これはIPMI対応のシステムを管理するために必要です。
管理ノード	VMware vCenter	5988-5989	NetApp Hybrid Cloud Control の HTTPS 通信
管理ノード	監視ノード	9442	ノード単位の設定 API サービス
管理ノード	vCenter Server の各サービスを提供	ポート 1	vCenter Plug-in の登録。登録が完了したら、ポートを閉じることができます。
SNMP サーバ	ストレージクラスタの MVIP	161 UDP	SNMP ポーリング

ソース	宛先	ポート	説明
SNMP サーバ	ストレージノードの MIP	161 UDP	SNMP ポーリング
ストレージノードのBMC / IPMI	管理ノード	623 UDP	RMCPポート。これはIPMI対応のシステムを管理するために必要です。
ストレージノードの MIP	DNS サーバ	53 TCP/UDP	DNS ルックアップ
ストレージノードの MIP	管理ノード	80	Element ソフトウェアのアップグレード
ストレージノードの MIP	S3 / Swift エンドポイント	80	（オプション）バックアップとリカバリ用の S3 / Swift エンドポイントへの HTTP 通信
ストレージノードの MIP	NTP サーバ	123 UDP	NTP
ストレージノードの MIP	管理ノード	162 UDP	（任意） SNMP トラップ
ストレージノードの MIP	SNMP サーバ	162 UDP	（任意） SNMP トラップ
ストレージノードの MIP	LDAP サーバ	389 TCP/UDP	（任意） LDAP 検索
ストレージノードの MIP	管理ノード	443	Element ソフトウェアのアップグレード
ストレージノードの MIP	リモートストレージクラスタの MVIP	443	リモートレプリケーションのクラスタペアリング通信
ストレージノードの MIP	リモートストレージノードの MIP	443	リモートレプリケーションのクラスタペアリング通信
ストレージノードの MIP	S3 / Swift エンドポイント	443	（オプション）バックアップとリカバリ用の S3 / Swift エンドポイントへの HTTPS 通信
ストレージノードの MIP	LDAPS サーバ	636 TCP/UDP	LDAPS ルックアップ
ストレージノードの MIP	管理ノード	10514 TCP/UDP 、 514 TCP/UDP	syslog 転送
ストレージノードの MIP	syslog サーバ	10514 TCP/UDP 、 514 TCP/UDP	syslog 転送
ストレージノードの MIP	リモートストレージノードの MIP	2181	リモートレプリケーション用のクラスタ間通信
ストレージノードの SIP	S3 / Swift エンドポイント	80	（オプション）バックアップとリカバリ用の S3 / Swift エンドポイントへの HTTP 通信

ソース	宛先	ポート	説明
ストレージノードの SIP	コンピューティングノードの SIP	442	コンピューティングノード API 、設定と検証、ソフトウェアインベントリへのアクセス
ストレージノードの SIP	S3 / Swift エンドポイント	443	（オプション）バックアップとリカバリ用の S3 / Swift エンドポイントへの HTTPS 通信
ストレージノードの SIP	リモートストレージノードの SIP	2181	リモートレプリケーション用のクラスタ間通信
ストレージノードの SIP	ストレージノードの SIP	3260	ノード間 iSCSI
ストレージノードの SIP	リモートストレージノードの SIP	4000 ～ 4020	リモートレプリケーションのノード間のデータ転送
システム管理者の PC	ストレージノードの MIP	80	（ NetApp HCI のみ）NetApp Deployment Engine のランディングページ
システム管理者の PC	管理ノード	442	管理ノードへの HTTPS UI アクセス
システム管理者の PC	ストレージノードの MIP	442	NetApp Deployment Engine でのストレージノードへの HTTPS UI および API アクセス（ NetApp HCI のみ）の設定と導入の監視
システム管理者の PC	コンピューティングノードBMC/IPMI H410およびH600シリーズ	443	ノードリモート制御へのHTTPS UIおよびAPIアクセス
システム管理者の PC	管理ノード	443	管理ノードへの HTTPS UI および API アクセス
システム管理者の PC	ストレージクラスタの MVIP	443	ストレージクラスタへの HTTPS UI および API アクセス
システム管理者の PC	ストレージノードBMC/IPMI H410およびH600シリーズ	443	ノードリモート制御へのHTTPS UIおよびAPIアクセス
システム管理者の PC	ストレージノードの MIP	443	HTTPS によるストレージクラスタの作成、ストレージクラスタへの導入後の UI アクセス
システム管理者の PC	コンピューティングノードBMC/IPMI H410およびH600シリーズ	623 UDP	RMCPポート。これはIPMI対応のシステムを管理するために必要です。

ソース	宛先	ポート	説明
システム管理者の PC	ストレージノードBMC/IPMI H410およびH600シリーズ	623 UDP	RMCPポート。これはIPMI対応のシステムを管理するために必要です。
システム管理者の PC	監視ノード	8080 です	監視ノードのノード Web UI
vCenter Server の各サービスを提供	ストレージクラスタの MVIP	443	vCenter Plug-in の API アクセス
vCenter Server の各サービスを提供	リモートプラグイン	8333	Remote vCenter Plug-inサービス
vCenter Server の各サービスを提供	管理ノード	8443	（オプション） vCenter Plug-in の QoSSIOC サービス。
vCenter Server の各サービスを提供	ストレージクラスタの MVIP	8444	vCenter VASA プロバイダアクセス（ VVol のみ）
vCenter Server の各サービスを提供	管理ノード	ポート 1	vCenter Plug-in の登録。登録が完了したら、ポートを閉じることができます。

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

ネットワークとスイッチの要件

導入を成功させるためには、 NetApp HCI に使用するスイッチで特別な設定が必要になります。以降に記載するそれぞれの要件を環境に実装する手順については、使用するスイッチのドキュメントを参照してください。

NetApp HCI 環境には、次のトラフィックタイプごとに 1 つ、少なくとも 3 つのネットワークセグメントが必要です。

- 管理
- VMware vMotion
- ストレージ / データ

NetApp H シリーズのコンピューティングノードおよびストレージノードのモデルや計画しているケーブル構成に応じて、別々のスイッチを使用してこれらのネットワークを物理的に分離するか、または VLAN を使用して論理的に分離することができます。ただしほとんどの環境では、これらのネットワーク（およびその他の仮想マシンネットワーク）を VLAN を使用して論理的に分離する必要があります。

コンピューティングノードとストレージノードは、導入中およびその前後に通信可能である必要があります。ストレージノードとコンピューティングノードに別々の管理ネットワークを実装する場合は、それらの管理ネ

ットワーク間にネットワークルートが確立されていることを確認してください。これらのネットワークにはゲートウェイが割り当てられている必要があり、ゲートウェイ間にルートが必要です。ノードと管理ネットワーク間の通信を確保するために、新しい各ノードにゲートウェイが割り当てられていることを確認してください。

NetApp HCI スイッチの要件は次のとおりです。

- NetApp HCI ノードに接続するスイッチポートは、すべてスパニングツリーのエッジポートとして設定する必要があります。
  - Cisco スイッチでは、スイッチモデル、ソフトウェアバージョン、およびポートタイプに応じて、次のいずれかのコマンドを使用してこの操作を実行できます。
    - 「 panning - tree port type edge 」を選択します
    - 「パンニングツリーポートタイプエッジトランク」
    - ' パンツリー portfast
    - ' パンツリー portfast trunk
  - Mellanox スイッチでは ' panning tree port type edge コマンドを使用してこれを実行できます
- NetApp HCI ノードには、アウトオブバンド管理を除くすべてのネットワーク機能用に冗長なポートがあります。最大限の耐障害性を実現するには、これらのポートを 2 つのスイッチに分け、従来の階層型アーキテクチャまたはレイヤ 2 のスパイン / リーフ型アーキテクチャへの冗長なアップリンクを確保します。
- ストレージ、仮想マシン、 vMotion の各トラフィックを処理するスイッチは、ポートあたり 10GbE 以上の速度をサポートする必要があります（ポートあたり最大 25GbE がサポートされます）。
- 管理トラフィックを処理するスイッチは、ポートあたり 1GbE 以上の速度をサポートする必要があります。
- ストレージおよび vMotion のトラフィックを処理するスイッチポートには、ジャンボフレームを設定する必要があります。インストールを成功させるには、ホストが 9000 バイトのパケットをエンドツーエンドで送信できる必要があります。
- 各ホストの管理 NIC ポートに設定されているサイズの MTU を使用できるように、管理ネットワークスイッチポートを設定する必要があります。たとえば、ホスト管理ネットワークポートの MTU サイズが 1750 バイトの場合は、少なくとも 1 、 750 バイトの MTU を使用できるように管理ネットワークスイッチポートを設定する必要があります（管理ネットワークの MTU は 9 、 000 バイトである必要はありません）。MTU 設定はエンドツーエンドで一貫した値にする必要があります
- すべてのストレージノードとコンピューティングノード間のラウンドトリップネットワークレイテンシを 2 ミリ秒以下にする必要があります。

すべての NetApp HCI ノードは、専用の管理ポートを通じてアウトオブバンド管理機能を提供します。NetApp H300 、 H300E 、 H500S 、 H500E 、 H700S 、 H700E 、および H410C のノードでは、ポート A を介した IPMI アクセスも可能ですベストプラクティスとして、環境内のすべてのノードでアウトオブバンド管理を設定し、 NetApp HCI のリモート管理を容易にすることを推奨します。

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

ネットワークケーブルの要件

次のガイドラインを参考に、環境の規模に対応した正しい種類のネットワークケーブルを十分な数用意してください。RJ45 ポートには、 Cat 5e または Cat 6 のケーブルを使用する必要があります。

- ケーブル 2 本のコンピューティングノード構成：各コンピューティングノードを、 2 つの SFP+ / SFP28 インターフェイスで 10 / 25GbE ネットワークに接続する必要があります（もう 1 本の Cat 5e / 6 ケーブルはオプションで、アウトオブバンド管理用です）。
- ケーブル 6 本のコンピューティングノード構成：各コンピューティングノードを、 4 つの SFP+ / SFP28 インターフェイスで 10 / 25GbE ネットワークに接続し、 2 本の Cat 5e / 6 ケーブルで 1 / 10GbE ネットワークに接続する必要があります（もう 1 本の Cat 5e / 6 ケーブルはオプションで、アウトオブバンド管理用です）。
- 各ストレージノードを、 2 つの SFP+ / SFP28 インターフェイスで 10 / 25GbE ネットワークに接続し、 2 本の Cat 5e / 6 ケーブルで 1 / 10GbE ネットワークに接続する必要があります（もう 1 本の Cat 5e / 6 ケーブルはオプションで、アウトオブバンド管理用です）。
- NetApp HCI システムをネットワークに接続するためのネットワークケーブルが、スイッチに届く十分な長さであることを確認します。

たとえば、 4 つのストレージノードと 3 つのコンピューティングノード（ケーブル 6 本の構成を使用）がある環境では、次の本数のネットワークケーブルが必要になります。

- RJ45 コネクタ付属の Cat 5e / 6 ケーブル × 14 （さらに必要に応じて IPMI トラフィック用のケーブル × 7 ）
- SFP28 / SFP+ コネクタ付属の Twinax ケーブル × 20

これは、次の理由によるものです。

- 4 つのストレージノードに Cat 5e / 6 ケーブルと Twinax ケーブルがそれぞれ 8 本必要です。
- ケーブル 6 本の構成を使用する 3 つのコンピューティングノードに Cat 5e / 6 ケーブルが 6 本、 Twinax ケーブルが 12 本必要です。

> ケーブルを 6 本使用する構成では、 2 つのポートが VMware ESXi 用に予約されており、NetApp Deployment Engine によってセットアップおよび管理されます。Element の TUI または Element Web GUI を使用して、これらの ESXi 専用ポートにアクセスしたり管理したりすることはできません。

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

IP アドレスの要件

NetApp HCI には、導入の規模に応じた IP アドレスの要件があります。NetApp Deployment Engine を使用してシステムを導入する前に各ノードに割り当てた初期 IP ア

ドレスは、デフォルトでは一時的な IP アドレスであり、再利用することはできません。最終的な導入時に割り当て可能な、未使用かつ永続的な IP アドレスのセットをもう 1 つ確保しておく必要があります。

NetApp HCI の導入ごとに必要な IP アドレスの数

NetApp HCI ストレージネットワークと管理ネットワークでは、それぞれ連続した IP アドレス範囲を使用する必要があります。次の表を参照して、導入に必要な IP アドレスの数を確認してください。

システムコンポーネント	管理ネットワーク IP アドレスが必要です	必要なストレージネットワーク IP アドレス	必要な vMotion ネットワーク IP アドレス	コンポーネントごとに必要な合計 IP アドレス
コンピューティングノード	1.	2.	1.	4.
ストレージノード	1.	1.		2.
ストレージクラスタ	1.	1.		2.
VMware vCenter	1.			1.
管理ノード	1.	1.		2.
監視ノード	1.	1.		監視ノードあたり 2（2 ノードまたは 3 ノードごとに 2 つの監視ノードが導入されます ストレージクラスタ）

NetApp HCI で予約されている IP アドレス

NetApp HCI では、システムコンポーネント用に次の IP アドレス範囲が予約されます。ネットワークを計画するときは、次の IP アドレスは使用しないでください。

IP アドレス範囲	説明
10.0.0.0/24	Docker overlay ネットワーク
10.0.1.0/24 のようになります	Docker overlay ネットワーク
10.255.0.0/16	Docker Swarm Ingress ネットワーク
169.254.100.1/22	Docker bridge ネットワーク
169.254.104.0/22	Docker bridge ネットワーク

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

ネットワーク構成：

ネットワーク構成：

NetApp HCI では、複数の異なるネットワークケーブル配線と VLAN 構成を使用できます。導入を成功させるためには、ネットワーク構成を計画することが重要です。

必要なネットワークセグメント

NetApp HCI には、管理トラフィック、ストレージトラフィック、仮想化トラフィック（仮想マシンと VMware vMotion のトラフィックを含む）の少なくとも 3 つのネットワークセグメントが必要です。仮想マシンと vMotion のトラフィックを分けることもできます。これらのネットワークセグメントは、通常、 NetApp HCI ネットワークインフラ内で論理的に分離された VLAN として存在します。

これらのネットワークにコンピューティングノードとストレージノードを接続する方法は、ネットワークを設計する方法とノードをケーブル接続する方法によって異なります。このガイドで使用するネットワーク図は、次のネットワークに基づいています。

ネットワーク名	**VLAN ID**
管理	100
ストレージ	105
vMotion	107
仮想マシン	200 、 201

NetApp Deployment Engine で NetApp HCI ノードを自動的に検出して設定するには、ノード上の SFP+ / SFP28 インターフェイスに使用されているすべてのスイッチポートで、タグなし VLAN またはネイティブ VLAN として使用できるネットワークセグメントが必要です。これにより、すべてのノード間で検出と導入のためのレイヤ 2 通信が可能になります。ネイティブ VLAN がない場合、すべてのノードの SFP+ / SFP28 インターフェイスに VLAN および IPv4 アドレスを手動で設定し、検出されるようにする必要があります。このドキュメントのネットワーク構成例では、この目的で管理ネットワーク（ VLAN ID 100 ）を使用しています。

NetApp Deployment Engine を使用すると、初期導入時にコンピューティングノードとストレージノードのネットワークを簡単に設定できます。vCenter や管理ノードなどの一部の組み込みの管理コンポーネントを専用のネットワークセグメントに配置することができます。これらのネットワークセグメントには、 vCenter や管理ノードがストレージおよびコンピューティングの管理ネットワークと通信できるようにするためのルーティングが必要です。ほとんどの環境では、これらのコンポーネントは同じ管理ネットワーク（この例では VLAN ID 100 ）を使用します。

> 仮想マシンのネットワークは vCenter を使用して設定します。NetApp HCI 環境のデフォルトの仮想マシンネットワーク（ポートグループ「 VM_Network 」）では VLAN ID は設定されません。複数の仮想マシンネットワークをタグ付けして使用する予定の場合は（前述の例の VLAN ID 200 および 201 ）、ネットワーク計画に最初からそれらのネットワークを含めるようにしてください。

ネットワーク構成とケーブル配線のオプション

H410C コンピューティングノードには、シンプルな配線の 2 ケーブルネットワーク構成を使用できます。この構成では、 2 つの SFP+ / SFP28 インターフェイスに加え、 IPMI 通信用にオプションで RJ45 インターフ

ェイス（必須ではありませんが使用することを推奨）を使用します。これらのノードでは、 2 つの RJ45 インターフェイスと 4 つの SFP28 / SFP+ インターフェイスを備えた 6 ケーブル構成を使用することもできます。

H410S および H610S ストレージノードは、 4 つのネットワークポート（ポート A~D ）を使用するネットワークトポロジをサポートします。

コンピューティングノードは、ハードウェアプラットフォームに応じて、次の 3 種類のネットワークトポロジをサポートします。

設定オプション	**H410C** ノードのケーブル接続	**H610C** ノードのケーブル配線	**H615C** ノードのケーブル接続
オプション A	ポート D と E を使用する 2 本のケーブル	ポート C と D を使用する 2 本のケーブル	ポート A と B を使用する 2 本のケーブル
オプション B	6 本のケーブルでポート A ~ F を使用	使用できません	使用できません
オプション C	オプション B と同様ですが、管理、ストレージ、および vMotion ネットワーク用のスイッチにネイティブ VLAN （アクセスポート）が搭載されています		

正しい数のケーブルが接続されていないノードを導入することはできません。たとえば、ケーブル 6 本の構成では、ポート D と E しか接続されていないコンピューティングノードを導入することはできません。

NetApp HCI のネットワーク設定は、導入後にインフラのニーズに合わせて調整することができます。ただし、 NetApp HCI リソースを拡張する場合は、新しいノードのケーブル構成を既存のコンピューティングノードおよびストレージノードと同じにする必要があります。

ネットワークでジャンボフレームがサポートされていないために NetApp Deployment Engine で障害が発生した場合は、次のいずれかの対処方法を実行します。

- 静的 IP アドレスを使用して、 Bond10G ネットワークで 9000 バイトの最大伝送ユニット（ MTU ）を手動で設定してください。
- Bond10G ネットワークで 9000 バイトのインターフェイス MTU をアドバタイズするように動的ホスト構成プロトコルを設定します。

ネットワーク構成オプション

- "ネットワーク構成オプション A"
- "ネットワーク構成オプション B"
- "ネットワーク構成オプション C"

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

ネットワーク構成：

NetApp HCI では、複数の異なるネットワークケーブル配線と VLAN 構成を使用できま

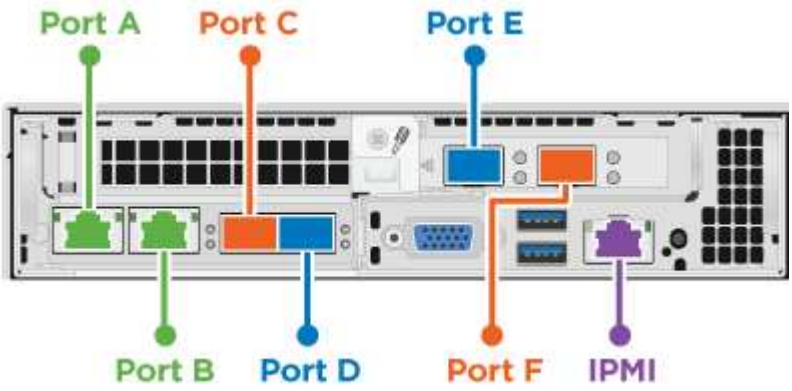
す。最初の構成では、オプション A でコンピューティングノードごとに 2 本のネットワークケーブルを使用します。

構成オプション **A** ：ケーブル **2** 本でのコンピューティングノードの構成

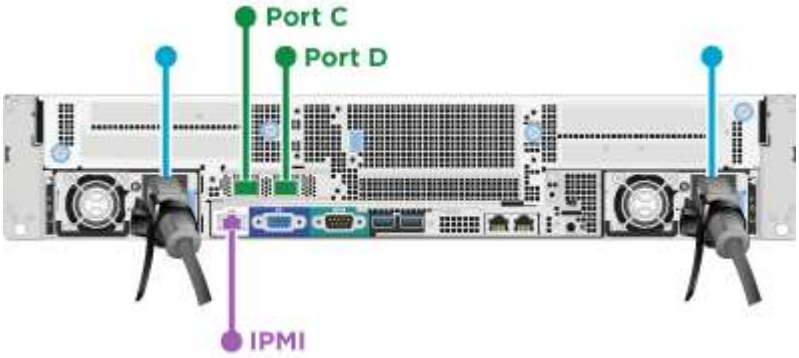
NetApp H410C 、 H610C 、および H615C コンピューティングノードは、 2 本のネットワークケーブルを使用してすべての NetApp HCI ネットワークに接続できます。この構成では、ストレージ、 vMotion 、および仮想マシンの各ネットワークで VLAN タギングを使用する必要があります。すべてのコンピューティングノードとストレージノードで同じ VLAN ID 方式を使用する必要があります。この構成では、 VMware vSphere Enterprise Plus のライセンスが必要な vSphere Distributed Switch を使用します。

NetApp HCI のドキュメントでは、 H シリーズノードの背面パネルにあるネットワークポートをアルファベットを使用して記載しています。

H410C ストレージノードのネットワークポートと場所は次のとおりです。



H610C コンピューティングノードのネットワークポートと場所は次のとおりです。



H615C コンピューティングノードのネットワークポートと場所は次のとおりです。

この構成では、各ノードで次のネットワークポートを使用します。

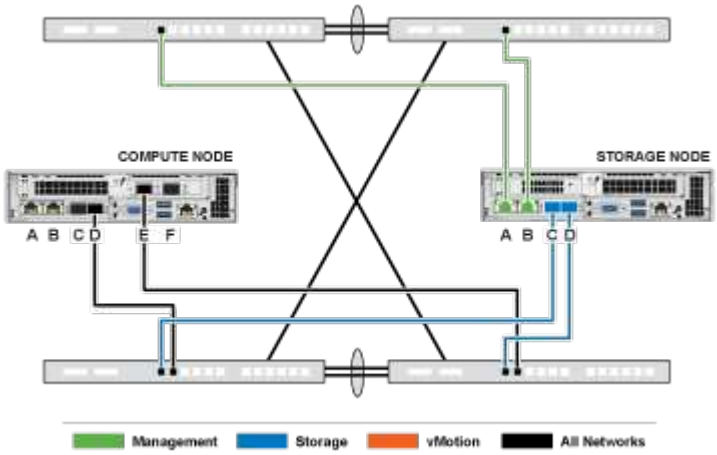
ノード	使用するネットワークポート
H410C	D および E
H610C	C および D
H615C	A と B

VLAN の設定

ベストプラクティスとして、ノードが使用しているすべてのスイッチポート上に必要なネットワークセグメントを構成することを推奨します。例：

ネットワーク名	**VLAN ID**	スイッチポートの設定
管理	100	ネイティブ
ストレージ	105	タグ付き
vMotion	107	タグ付き
仮想マシン	200 、 201	タグ付き

次の図は、ケーブル 2 本の H410C コンピューティングノードとケーブル 4 本の H410S ストレージノードの推奨されるケーブル構成を示しています。この例のスイッチポートはすべて同じ構成です。



スイッチコマンドの例

NetApp HCI ノードで使用するすべてのスイッチポートを構成する場合には次のコマンドを使用できます。このコマンドは Cisco の構成用ですが、少しの変更で Mellanox スイッチにも使用できます。この構成を実装するために必要なコマンドについては、スイッチのマニュアルを参照してください。インターフェイス名、説明、および VLAN を環境に応じた値に置き換えて使用してください。

インターフェイス { インターフェイス名、たとえば EthernetX/Y または GigabitEthernetX/Y/Z }`d 説明 { 必要な説明、たとえば NetApp-CI-nodex-porty }`m TU9216``witchport` トランクネイティブ `VLAN 100witchport` トランクネイティブ `VLAN 100`witchport トランク VLAN 105,107,200,200,200,ted' エッジのようなトランクタイプ

> 一部のスイッチでは、 VLAN の許可リストにネイティブ VLAN を含める必要があります。使用しているスイッチモデルとソフトウェアバージョンのドキュメントを参照してください。

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

ネットワーク構成：

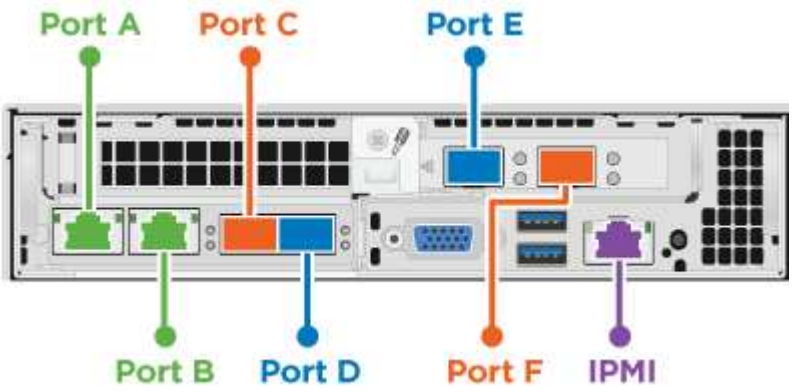
NetApp HCI では、複数の異なるネットワークケーブル配線と VLAN 構成を使用できます。最初の構成のオプション B では、コンピューティングノードごとに 6 本のネットワークケーブルを使用します。

構成オプション **B** ：ケーブル **6** 本でのコンピューティングノードの構成

セカンダリネットワーク構成オプションとして、 H410C コンピューティングノードでは 6 本のネットワークケーブルを使用してすべての NetApp HCI ネットワークに接続できます。この構成では、ストレージ、vMotion 、および仮想マシンの各ネットワークで VLAN タギングを使用する必要があります。この構成は、vSphere Standard Switch または vSphere Distributed Switch （ VMware vSphere Enterprise Plus のライセンスが必要）で使用できます。

NetApp HCI のドキュメントでは、 H シリーズノードの背面パネルにあるネットワークポートをアルファベットを使用して記載しています。

H410C コンピューティングノードのネットワークポートと場所は次のとおりです。

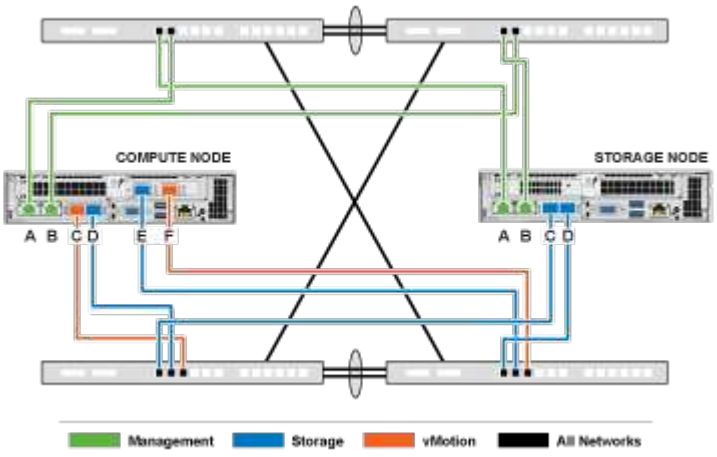


VLAN の設定

6 本のケーブルを使用してコンピューティングノードを導入し、 4 本のケーブルを使用してストレージノードを導入する場合は、ノードが使用しているすべてのスイッチポート上に必要なネットワークセグメントを構成することを推奨します。例：

ネットワーク名	**VLAN ID**	スイッチポートの設定
管理	100	ネイティブ
ストレージ	105	タグ付き
vMotion	107	タグ付き
仮想マシン	200 、 201	タグ付き

次の図は、ケーブル 6 本のコンピューティングノードとケーブル 4 本のストレージノードの推奨されるケーブル構成を示したものです。この例のスイッチポートはすべて同じ構成です。



スイッチコマンドの例

NetApp HCI ノードで使用するすべてのスイッチポートを構成する場合には次のコマンドを使用できます。このコマンドは Cisco の構成用ですが、少しの変更で Mellanox スイッチにも使用できます。この構成を実装するために必要なコマンドについては、スイッチのマニュアルを参照してください。インターフェイス名、説明、および VLAN を環境に応じた値に置き換えて使用してください。

インターフェイス { インターフェイス名、たとえば EthernetX/Y または GigabitEthernetX/Y/Z }`d 説明 { 必要な説明、たとえば NetApp-CI-nodex-porty }`m TU9216``witchport` トランクネイティブ `VLAN 100witchport` トランクネイティブ `VLAN 100`witchport トランク VLAN 105,107,200,200,200,ted' エッジのようなトランクタイプ

> 一部のスイッチでは、 VLAN の許可リストにネイティブ VLAN を含める必要があります。使用しているスイッチモデルとソフトウェアバージョンのドキュメントを参照してください。

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

ネットワーク構成：

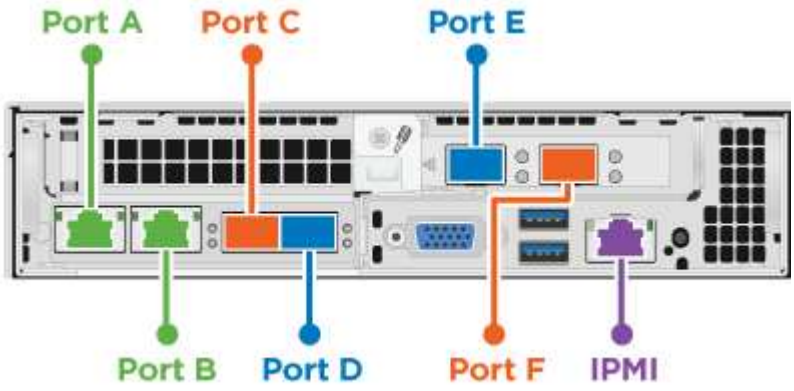
NetApp HCI では、複数の異なるネットワークケーブル配線と VLAN 構成を使用できます。3 つ目の構成では、オプション C でコンピューティングノードごとに 6 本のネットワークケーブルをネイティブ VLAN で使用します。

構成オプション **C** ：ケーブル **6** 本でのコンピューティングノードの構成 **-** ネイティブ **VLAN** を使用

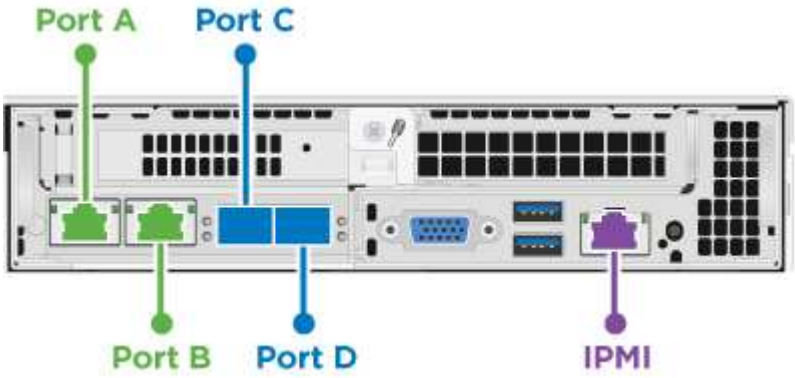
ストレージおよび仮想化トラフィックにタグ付けした VLAN を使用する代わりに、スイッチの設定を使用してネットワークセグメントを分離することで、 NetApp HCI を導入できます。この構成は、 vSphere Standard Switch または vSphere Distributed Switch （ VMware vSphere Enterprise Plus のライセンスが必要）で使用できます。

NetApp HCI のドキュメントでは、 H シリーズノードの背面パネルにあるネットワークポートをアルファベットを使用して記載しています。

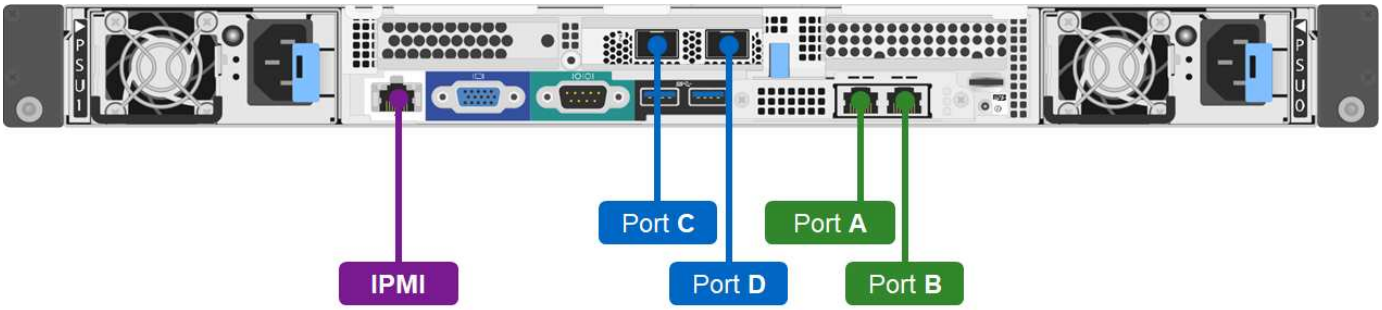
H410C ストレージノードのネットワークポートと場所は次のとおりです。



H410S ストレージノードのネットワークポートと場所は次のとおりです。



H610S ストレージノードのネットワークポートと場所は次のとおりです。



H410C 、 **H410S** 、および **H610S** ノードの **VLAN** 構成

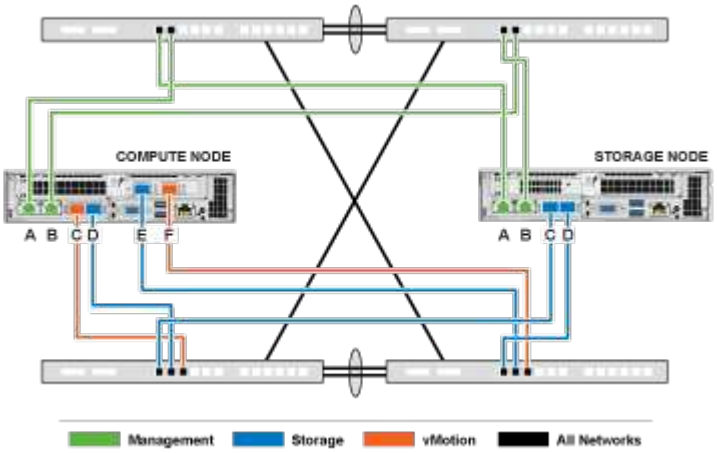
このトポロジオプションは、 H410C 、 H410S 、および H610S ノードで次の VLAN 構成を使用します。

使用するノードポート	ネットワーク名	**VLAN ID**	接続するスイッチポート設定
コンピューティングノードとストレージノードのポート A と B	管理	100	ネイティブ

使用するノードポート	ネットワーク名	**VLAN ID**	接続するスイッチポート設定
コンピューティングノードのポート D 、 E	ストレージ	105	ネイティブ
ストレージノードのポート C 、 D	ストレージ	105	ネイティブ
コンピューティングノードのポート C 、 F	vMotion	107	ネイティブ
コンピューティングノードのポート C 、 F	仮想マシン	200 、 201	タグ付き

この構成を導入する際は、スイッチポートを慎重に構成してください。このネットワークトポロジの構成に誤りがあると、診断が難しい導入エラーが発生する可能性があります。

次の図は、このトポロジオプションのネットワーク構成の概要を示しています。この例では、個々のスイッチポートを該当するネットワークセグメントでネイティブネットワークとして構成しています。



スイッチコマンドの例

NetApp HCI ノードで使用するスイッチポートを構成する場合には次のコマンドを使用できます。このコマンドは Cisco の構成用ですが、少しの変更で Mellanox スイッチにも使用できます。この構成を実装するために必要なコマンドについては、スイッチのマニュアルを参照してください。

管理ネットワーク用のスイッチポートを構成する場合には次のコマンドを使用できます。インターフェイス名、説明、および VLAN を構成に応じた値に置き換えて使用してください。

インターフェイス { インターフェイス名 (EthernetX/Y や GigabitEthernetX/Y/Z} 説明 {desion{desired の説明。NetApp-HCI -nodex-Porta|B}witchport access VLAN 100```panning tree port port type edge) など

ストレージネットワーク用のスイッチポートを構成する場合には次のコマンドを使用できます。インターフェイス名、説明、および VLAN を構成に応じた値に置き換えて使用してください。

「 interface { interface name 」 （ EthernetX/Y や GigabitEthernetX/Y/Z など）「説明 { desired description { desired description （ NetApp-CI-nodex-PortC|D}```

vMotion および仮想マシンネットワーク用のスイッチポートを構成する場合には次のコマンドを使用できま

す。インターフェイス名、説明、および VLAN を構成に応じた値に置き換えて使用してください。

「 interface { interface name 」（ EthernetX/Y や GigabitEthernetX/Y/Z など）「説明 { desired description {NetApp-CI-nodex-PortC|F}```m TU'9216 ‘」「 witchport mode trunk ‘ witchport trunk ’でネイティブ VLAN トランク’ 107 ’ witchport trunk allowed VLAN 200,201 ’ s panning tree type 」などの説明

> 一部のスイッチでは、 VLAN の許可リストにネイティブ VLAN を含める必要があります。使用しているスイッチモデルとソフトウェアバージョンのドキュメントを参照してください。

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

DNS とタイムキーパー機能の要件

導入前に、 NetApp HCI システムのドメインネームシステム（ DNS ）レコードを準備し、 NTP サーバの情報を収集する必要があります。NetApp HCI の導入を成功させるには、正しい DNS エントリと NTP サーバが設定された DNS サーバが必要です。

NetApp HCI を導入する前に、次の DNS およびタイムサーバの準備を行ってください。

- ホスト（個々のコンピューティングノードやストレージノードなど）の DNS エントリを必要に応じて作成し、そのエントリと IP アドレスの対応表を作成しておきます。導入時に、各ホストに適用されるプレフィックスをストレージクラスタに割り当てる必要があります。混乱を避けるため、 DNS の命名方法を念頭にプレフィックスを決めてください。
- 新しい VMware vSphere と一緒に NetApp HCI を導入するときに完全修飾ドメイン名を使用する場合は、導入前に vCenter Server のポインタ（ PTR ）レコードとアドレス（ A ）レコードを 1 つずつ、使用中のすべての DNS サーバに作成しておく必要があります。
- IP アドレスだけを使用する場合は vCenter の新しい DNS レコードを作成する必要はありません。NetApp HCI
- NetApp HCI には、タイムキーパー機能のための有効な NTP サーバが必要です。環境に NTP サーバがない場合は、一般に公開されているタイムサーバを使用してもかまいません。
- ストレージノードとコンピューティングノードのすべてのクロックが相互に同期されていること、および NetApp HCI へのログインに使用するデバイスのクロックが NetApp HCI ノードと同期されていることを確認してください。

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

環境要件

NetApp HCI の設置に使用するラックの電源が AC 電源コンセントから供給されること、および NetApp HCI の設置規模に応じた十分な冷却をデータセンターが提供できること

を確認します。

NetApp HCI の各コンポーネントの詳細な機能については、『 NetApp HCI 』を参照してください "データシート"。

> H410C コンピューティングノードは高電圧（ 200~240VAC ）でのみ動作します。既存の NetApp HCI 環境に H410C ノードを追加する場合は、電源要件が満たされていることを確認しておく必要があります。

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

保護ドメイン

NetApp Element ソフトウェアは、をサポートします "保護ドメイン" 機能：データの可用性を最大限に高めるために、ストレージノード上のデータレイアウトを最適化します。この機能を使用するには、 3 台以上の NetApp H シリーズシャーシにストレージ容量を均等に分割して、ストレージの信頼性を最適化する必要があります。この場合、ストレージクラスタで保護ドメインが自動的に有効になります。

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

2 ノードストレージクラスタの場合は、監視ノードのリソース要件が必要です

NetApp HCI では、最小インストールサイズとして、 2 つのストレージノードと 2 つのコンピューティングノードがサポートされます。2 ノードまたは 3 ノードのストレージクラスタを使用して NetApp HCI をインストールする場合は、 NetApp HCI 監視ノードとその仮想マシン（ VM ）リソースの要件について理解しておく必要があります。

ストレージクラスタは、 2 つまたは 3 つのノードを使用する場合、各ストレージクラスタと一緒に監視ノードのペアを導入します。監視ノードには、次の VM リソース要件があります。

リソース	要件
vCPU	4.
メモリ	12GB
ディスクサイズ	67 GB

NetApp HCI では、 2 ノードまたは 3 ノードのストレージクラスタでサポートされるストレージノードのモデ

ルには制限があります。詳細については、ご使用の NetApp HCI バージョンの『リリースノート』を参照してください。

- ベストプラクティス：監視ノードの VM でコンピューティングノードのローカルデータストアを使用するように設定する（ NDE のデフォルト設定）。 SolidFire ストレージボリュームなどの共有ストレージには設定しないでください。VM が自動的に移行されないようにするには、監視ノード VM の Distributed Resource Scheduler （ DRS ）自動化レベルを「 * Disabled 」に設定します。これにより、両方の監視ノードが同じコンピューティングノードで実行されないようにし、非ハイアベイラビリティ（ HA ）ペア構成を作成することができます。

NetApp HCI のインストールプロセスで監視ノードがインストールされると、 VM テンプレートが VMware vCenter に格納されます。これを使用して、誤って削除された場合、失われた場合、または破損した場合に監視ノードを再導入できます。また、監視ノードをホストしていた障害コンピューティングノードと交換する必要がある場合は、テンプレートを使用して監視ノードを再導入することもできます。手順については、 2 ノードおよび 3 ノードのストレージクラスタに対する監視ノードの再導入 * を参照してください "こちらをご覧ください"。

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

NetApp HCI の利用を開始しましょう

NetApp HCI のインストールと導入の概要

以下の手順を使用して、 NetApp HCI をインストールおよび導入します。このガイドには、詳細へのリンクが記載されています。

プロセスの概要を以下に示します。

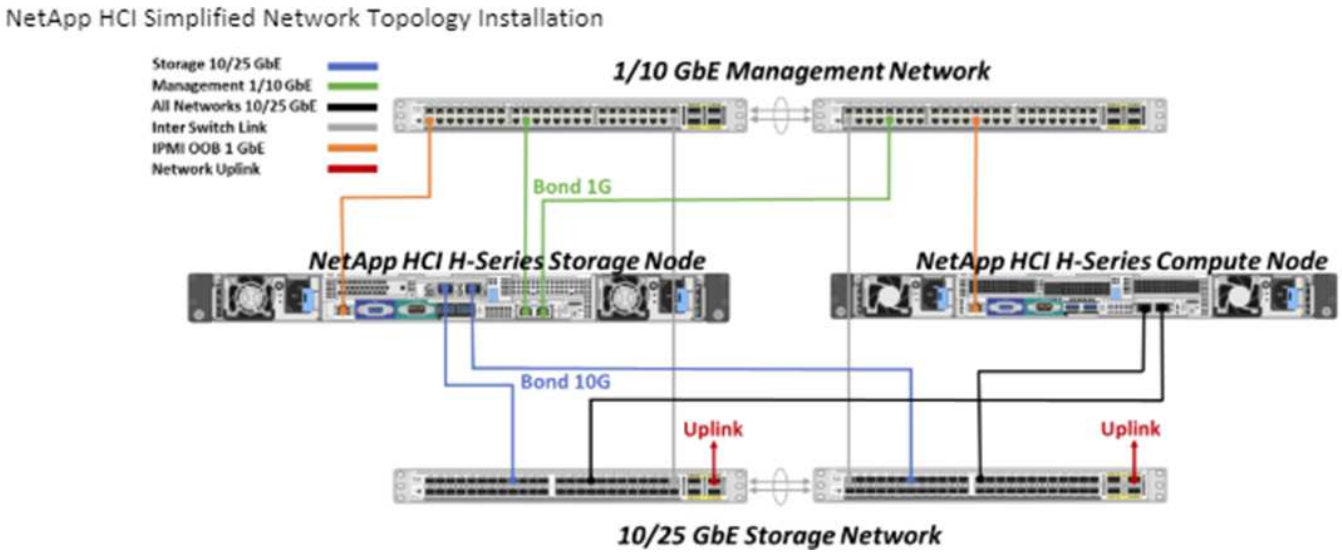
- [設置を準備]
- NetApp Active IQ Config Advisor でネットワークの準備状況を検証
- [ネットアップチームと連携]
- NetApp HCI ハードウェアを設置
- [ハードウェアの設置後にオプションの作業を実行します]
- NetApp Deployment Engine （ NDE ）を使用した NetApp HCI の導入
- vCenter Plug-in を使用して NetApp HCI を管理します
- Hybrid Cloud Control を使用して NetApp HCI を監視またはアップグレードします

設置を準備

インストールを開始する前に、ハードウェアを受け取る前に、 NetApp HCI インストレーションディスカバリーワークブックの事前チェックリストを完成させてください。

ネットワークと設置サイトを準備

NetApp HCI ネットワークトポロジを簡単にインストールするには、次の手順を実行します。



これは、単一のストレージノードと単一のコンピューティングノードのシンプルなネットワークトポロジです。NetApp HCI の最小クラスタは、 2 つのストレージノードと 2 つのコンピューティングノードです。

ネットワークトポロジは、ここに示すものとは異なる場合があります。これは一例です。

このセットアップでは、コンピューティングノードに 2 本のネットワークケーブルを使用してすべての NetApp HCI ネットワークに接続します。

次のリソースを参照してください。

- インストール前に NetApp HCI インストール検出ワークブック _ を使用してネットワークを設定してください。
- その他のサポートされる構成の詳細については、を参照してください "_TR-48820 ：『 NetApp HCI ネットワーククイックプランニングガイド』 _" および "NetApp HCI のインストールとセットアップの手順 _"。
- 4 つのストレージノードよりも小規模な NetApp HCI 構成の詳細については、を参照してください "TR-4823 ：『 NetApp HCI 2 Node Storage Cluster _ 』"。
- 各ストレージノードに使用されるスイッチポートでの Link Aggregation Control Protocol （ LACP ）の設定の詳細については、を参照してください "ストレージパフォーマンスを最適化するために LCAP を設定します"。

このセットアップにより、すべてのトラフィックが 2 つの物理冗長ポートに統合されるため、ケーブル配線が削減され、ネットワーク構成が合理化されます。この構成では、ストレージ、 vMotion 、および仮想マシンのネットワークセグメントで VLAN タギングを使用する必要があります。管理ネットワークセグメントでは、ネイティブ VLAN またはタグ付き VLAN を使用できますが、 NetApp Deployment Engine （ NDE ）がネットワークリソースを自動で割り当てることができるように、ネイティブ VLAN が推奨モードです（ Zero Conf ）。

このモードでは、 vSphere Distributed Switch （ vDS ）が必要です。これには VMware vSphere Enterprise Plus ライセンスが必要です。

作業を開始する前のネットワーク要件

ここでは前提条件の主な説明を示します。

前提条件の詳細については、を参照してください "NetApp HCI 導入の要件の概要"。

- Bond1G は、ストレージノード上の 1GbE ネットワークポートとコンピューティングノード上の管理インターフェイスを組み合わせた論理インターフェイスです。このネットワークは NDE API トラフィックに使用されます。すべてのノードが、同じ L2 ネットワーク内の管理インターフェイスを介して通信できる必要があります。
- Bond10G は 10 / 25GbE ポートを組み合わせた論理インターフェイスで、 NDE がビーコンとインベントリ用に使用します。すべてのノードが、 Bond10G インターフェイスを介してフラグメント化されていないジャンボフレームと通信できる必要があります。
- NDE では、 1 つのストレージノードの Bond1G インターフェイスに少なくとも 1 つの IP アドレスを手動で割り当てる必要があります。このノードから NDE が実行されます。
- すべてのノードには NDE 検出によって割り当てられる一時的な IP アドレスがあり、これは自動プライベート IP アドレス指定（APIPA）によって実行されます。

NDE プロセスでは、すべてのノードに永続的な IP アドレスが割り当てられ、一時的な IP が割り当てられた APIPA は解放されます。

- NDE では、管理用、 iSCSI 用、および vMotion 用に別々のネットワークが必要ですが、これらのネットワークはスイッチネットワーク上で事前に設定されて

NetApp Active IQ Config Advisor でネットワークの準備状況を検証

ネットワークが NetApp HCI に対応していることを確認するために、 NetApp Active IQ Config Advisor 5.8.1 以降をインストールします。このネットワーク検証ツールは他のツールと一緒に配置されています "ネットアップサポートツール"。このツールを使用して、接続性、 VLAN ID 、 IP アドレス要件、スイッチ接続などを検証します。

詳細については、を参照してください "Active IQ Config Advisor で環境を検証"。

ネットアップチームと連携

ネットアップチームは、 NetApp Active IQ Config Advisor レポートと *Discovery Workbook* を使用して、ネットワーク環境の準備ができているかどうかを検証します。

NetApp HCI ハードウェアを設置

NetApp HCI は、次のようなさまざまな構成にインストールできます。

- H410C コンピューティングノード：ケーブル 2 本の構成またはケーブル 6 本の構成
- H610C コンピューティングノード：ケーブルを 2 本使用する構成です
- H615C コンピューティングノード：ケーブル 2 本の構成
- H410S ストレージノード
- H610S ストレージノード

> 注意事項および詳細については、を参照してください "H シリーズハードウェアを設置"。

手順

1. レールとシャーシを設置
2. シャーシにノードを設置し、ストレージノード用のドライブを取り付けます。（ H410C と H410S を NetApp H シリーズシャーシに設置する場合のみ該当します）。
3. スイッチを設置します。
4. コンピューティングノードをケーブル接続します。
5. ストレージノードをケーブル接続
6. 電源コードを接続します。
7. NetApp HCI ノードの電源をオンにします。

ハードウェアの設置後にオプションの作業を実行します

NetApp HCI ハードウェアを設置したら、オプションでありながら推奨されるタスクを実行する必要があります。

すべてのシャーシでストレージ容量を管理

ストレージ容量がストレージノードを格納したすべてのシャーシに均等に分割されていることを確認します。

各ノードに **IPMI** を設定します

NetApp HCI ハードウェアをラックに設置してケーブル接続し、電源をオンにしたら、各ノードに Intelligent Platform Management Interface （ IPMI ）アクセスを設定できます。各 IPMI ポートに IP アドレスを割り当て、ノードへのリモート IPMI アクセスが可能になったらすぐにデフォルトの管理者 IPMI パスワードを変更します。

を参照してください "IPMI を設定します"。

NetApp Deployment Engine （ NDE ）を使用した NetApp HCI の導入

NDE UI は、 NetApp HCI のインストールに使用するソフトウェアウィザードインターフェイスです。

NDE UI を起動します

NetApp HCI では、ストレージノードの管理ネットワークの IPv4 アドレスを使用して NDE に最初にアクセスします。ベストプラクティスとして、 1 つ目のストレージノードから接続することを推奨します。

前提条件

- 初期ストレージノードの管理ネットワーク IP アドレスを手動で、または DHCP を使用して割り当てておきます。
- NetApp HCI 環境に物理的にアクセスできる必要があります。

手順

1. 初期ストレージノードの管理ネットワーク IP がわからない場合は、ターミナルユーザインターフェイス（ TUI ）を使用します。 TUI には、ストレージノードまたはのキーボードとモニタからアクセスします "USB スティックを使用します"。

   詳細については、を参照してください "NetApp Deployment Engine へのアクセス _"。

2. IP アドレスがわかっている場合は、 Web ブラウザで、 HTTPS ではなく HTTP 経由でプライマリノードの Bond1G アドレスに接続します。
   - 例 *: http://<IP_address>:442/nde/`

NDE UI で **NetApp HCI** を導入

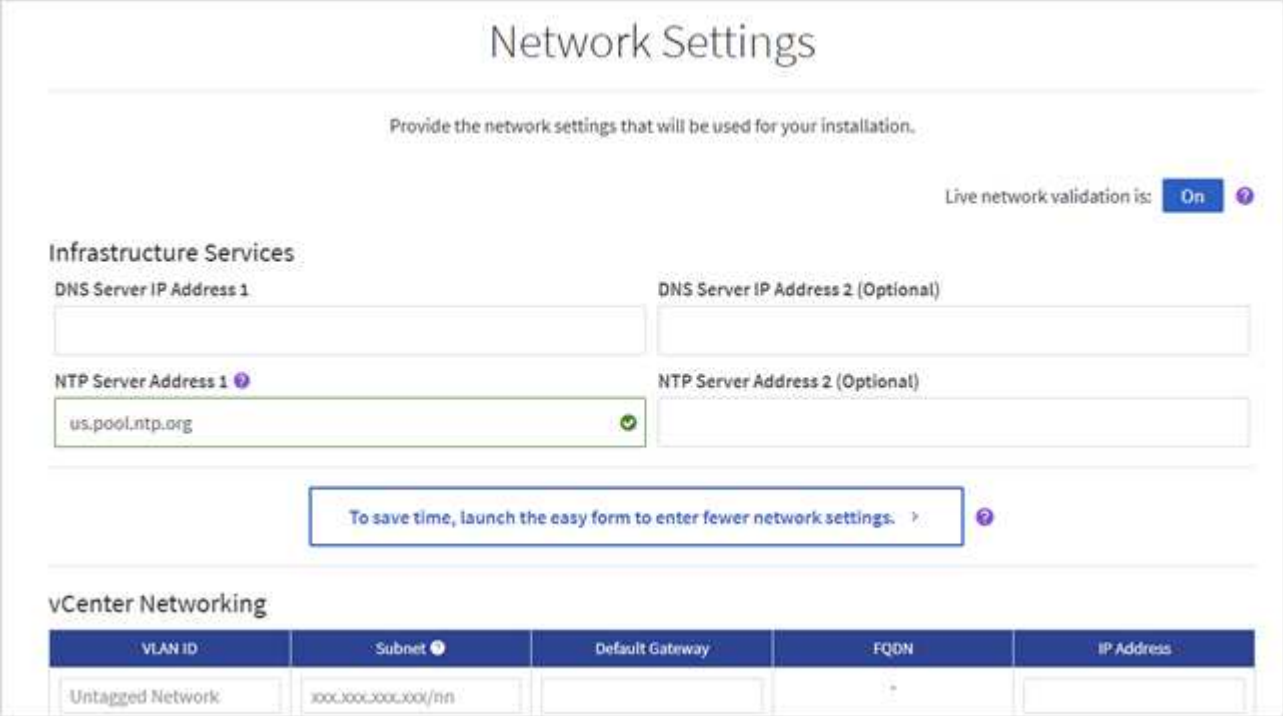
1. NDE で、前提条件に同意し、 Active IQ の使用を確認して、ライセンス契約に同意します。
2. 必要に応じて、 ONTAP Select によるデータファブリックファイルサービスを有効にし、 ONTAP Select ライセンスを受け入れます。
3. 新しい vCenter 環境を設定します。[完全修飾ドメイン名を使用して構成] をクリックし、 vCenter Server のドメイン名と DNS サーバの IP アドレスの両方を入力します。

   vCenter のインストールには、 FQDN の方法を使用することを強く推奨します。

4. すべてのノードのインベントリ評価が正常に完了したことを確認します。

NDE を実行しているストレージノードはすでにチェックされています。

5. すべてのノードを選択し、 * Continue * をクリックします。
6. ネットワークの設定を行います。使用する値については、「 NetApp HCI インストール検出ワークブック」を参照してください。
7. 青いボックスをクリックして、簡易フォームを起動します。



8. ネットワーク設定簡易フォームで次の手順を実行します。
   a. 名前のプレフィックスを入力します。（ NetApp HCI インストール検出ワークブックのシステムの詳細を参照してください _ ）。
   b. VLAN ID を割り当てるには、 [いいえ] をクリックしますか？（これらは、後のメインの [ネットワークの設定] ページで割り当てます）。
   c. ワークブックに従って、管理ネットワーク、 vMotion ネットワーク、および iSCSI ネットワークのサブネット CIDR 、デフォルトゲートウェイ、および開始 IP アドレスを入力します。（これらの値については、 _ NetApp HCI インストレーションディスカバリーワークブック _ の IP 割り当て方法セクションを参照してください）。
   d. [ネットワーク設定に適用] をクリックします。
9. に参加します "既存の vCenter" （オプション）。
10. NetApp HCI インストール検出ワークブックにノードのシリアル番号を記録します _ 。
11. vMotion ネットワークの VLAN ID と、 VLAN タギングが必要なすべてのネットワークを指定します。NetApp HCI インストール検出ワークブック _ を参照してください。
12. 構成を .csv ファイルとしてダウンロードします。
13. [展開の開始] をクリックします。
14. 表示された URL をコピーして保存します。

導入が完了するまでに約 45 分かかることがあります。

vSphere Web Client を使用してインストール環境を確認します

1. vSphere Web Client を起動し、 NDE の使用時に指定したクレデンシャルでログインします。

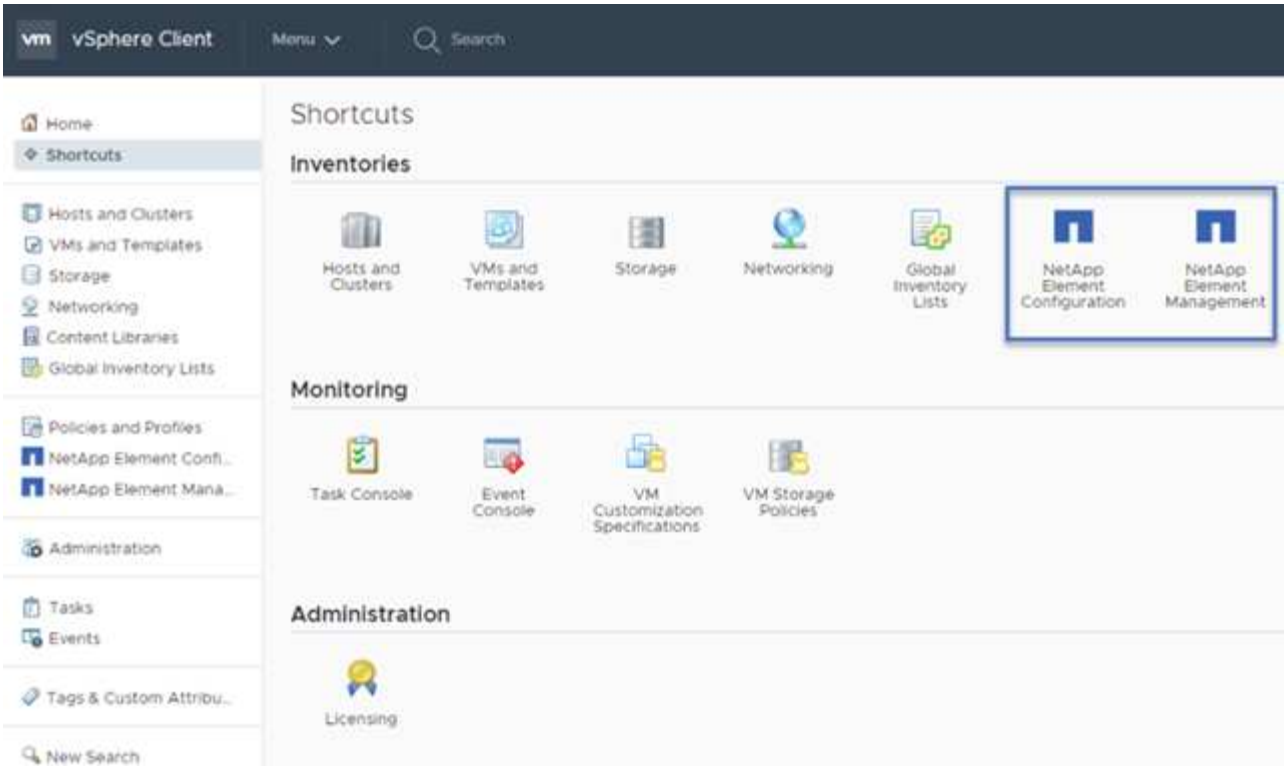
   ユーザ名に「 @vsphere.local 」を付加する必要があります。

2. アラームがないことを確認します。
3. vCenter 、 mNode 、および ONTAP Select （オプション）のアプライアンスが警告アイコンなしで実行されていることを確認します。
4. 2 つのデフォルトのデータストア（ NetApp-HCI-Datastore_01 と 02 ）が作成されていることを確認します。
5. 各データストアを選択し、すべてのコンピューティングノードがホストタブに表示されていることを確認します。
6. vMotion とデータストア -02 を検証してください。
   a. vCenter Server を NetApp-HCI-Datastore-02 （ Storage Only vMotion ）に移行します。
   b. vCenter Server を各コンピューティングノードに移行する（コンピューティング専用の vMotion ）。
7. NetApp Element Plug-in for vCenter Server に移動して、クラスタが表示されることを確認します。
8. ダッシュボードにアラートが表示されていないことを確認します。

vCenter Plug-in を使用して NetApp HCI を管理します

NetApp HCI をインストールしたら、 NetApp Element Plug-in for vCenter Server を使用して、クラスタ、ボリューム、データストア、ログ、アクセスグループ、イニシエータ、およびサービス品質（ QoS ）ポリシーを設定できます。

詳細については、を参照してください "_ NetApp Element Plug-in for vCenter Server のドキュメント _"。



Hybrid Cloud Control を使用して NetApp HCI を監視またはアップグレードします

必要に応じて、 NetApp HCI ハイブリッドクラウド制御を使用して、システムを監視、アップグレード、または拡張することができます。

NetApp Hybrid Cloud Control にログインするには、管理ノードの IP アドレスにアクセスします。

Hybrid Cloud Control を使用すると、次の操作を実行できます。

- "NetApp HCI のインストールを監視する"
- "NetApp HCI システムをアップグレードします"
- "NetApp HCI のストレージリソースまたはコンピューティングリソースを拡張します"
- 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。例：

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

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

     NetApp Hybrid Cloud Control のインターフェイスが表示されます。

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"

- "NetApp HCI のセットアップガイド"
- "TR-48820 ：『 NetApp HCI Networking Quick Planning Guide 』"
- "NetApp Element Plug-in for vCenter Server のドキュメント"
- "NetApp Configuration Advisor" 5.8.1 以降のネットワーク検証ツール
- "NetApp SolidFire Active IQ のドキュメント"

H シリーズハードウェアを設置

NetApp HCI の使用を開始する前に、ストレージノードとコンピューティングノードを正しくインストールする必要があります。

を参照してください "ポスター" 指示を視覚的に表示します。

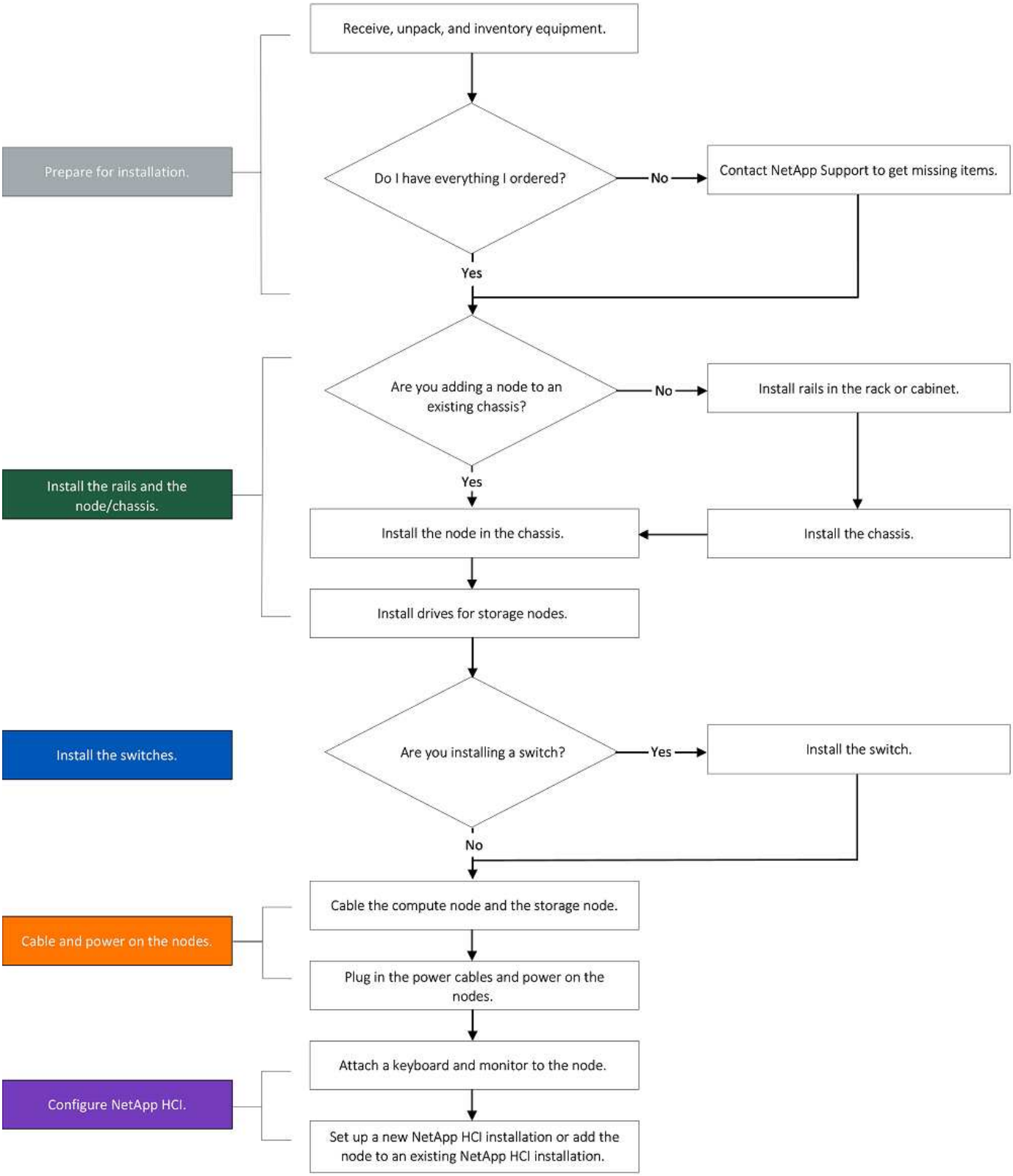
- [ワークフロー図]
- [設置を準備]
- [レールを取り付けます]
- ノード / シャーシを設置
- [スイッチを設置します]
- [ノードをケーブル接続]
- [ノードの電源をオンにします]
- NetApp HCI を設定します
- [設定後のタスクを実行]

ワークフロー図

このワークフロー図は、インストール手順の概要を示しています。手順は H シリーズモデルによって多少異なります。

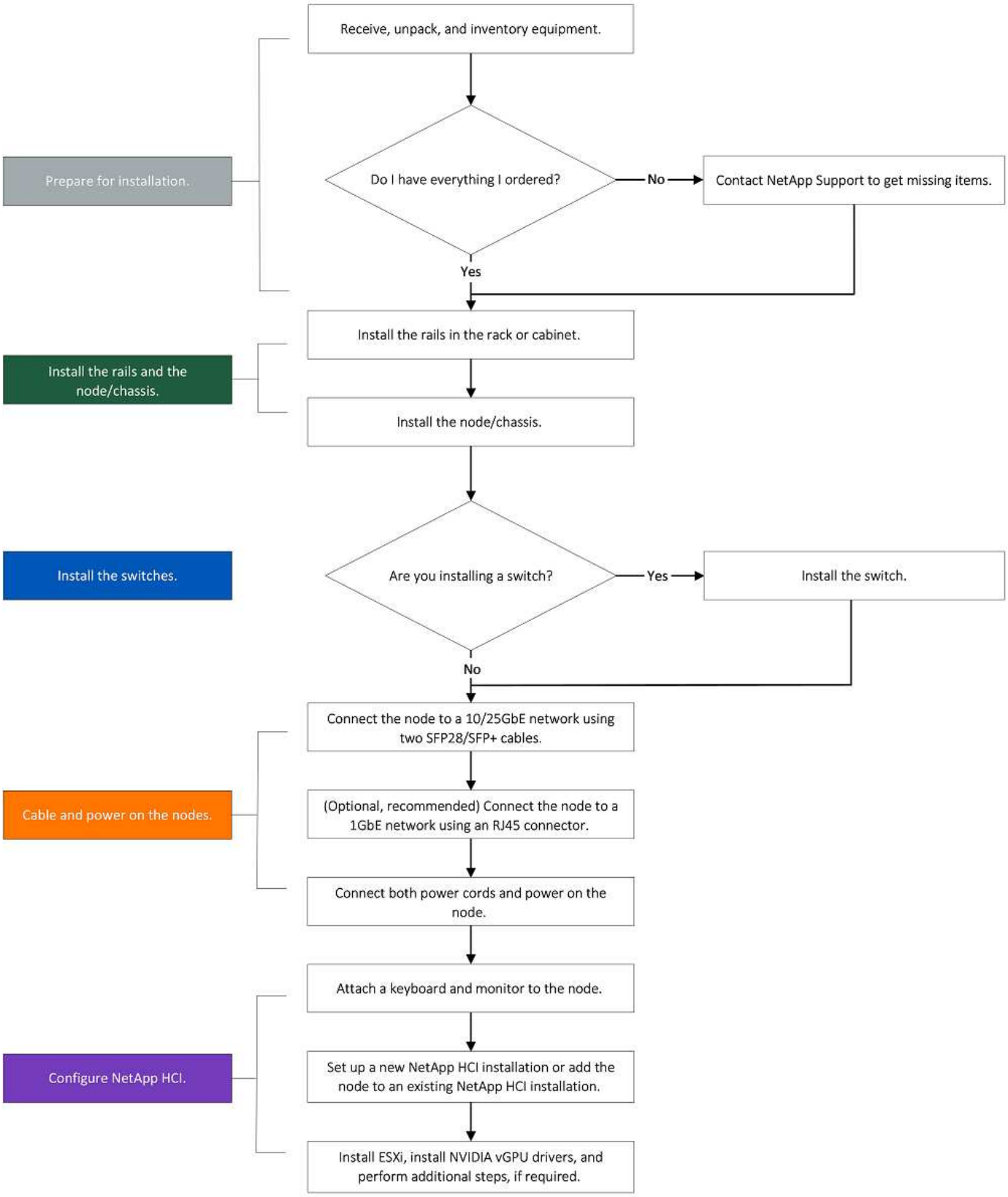
- H410C および H410S
- H610C および H615C
- [H610S]

H410C および H410S



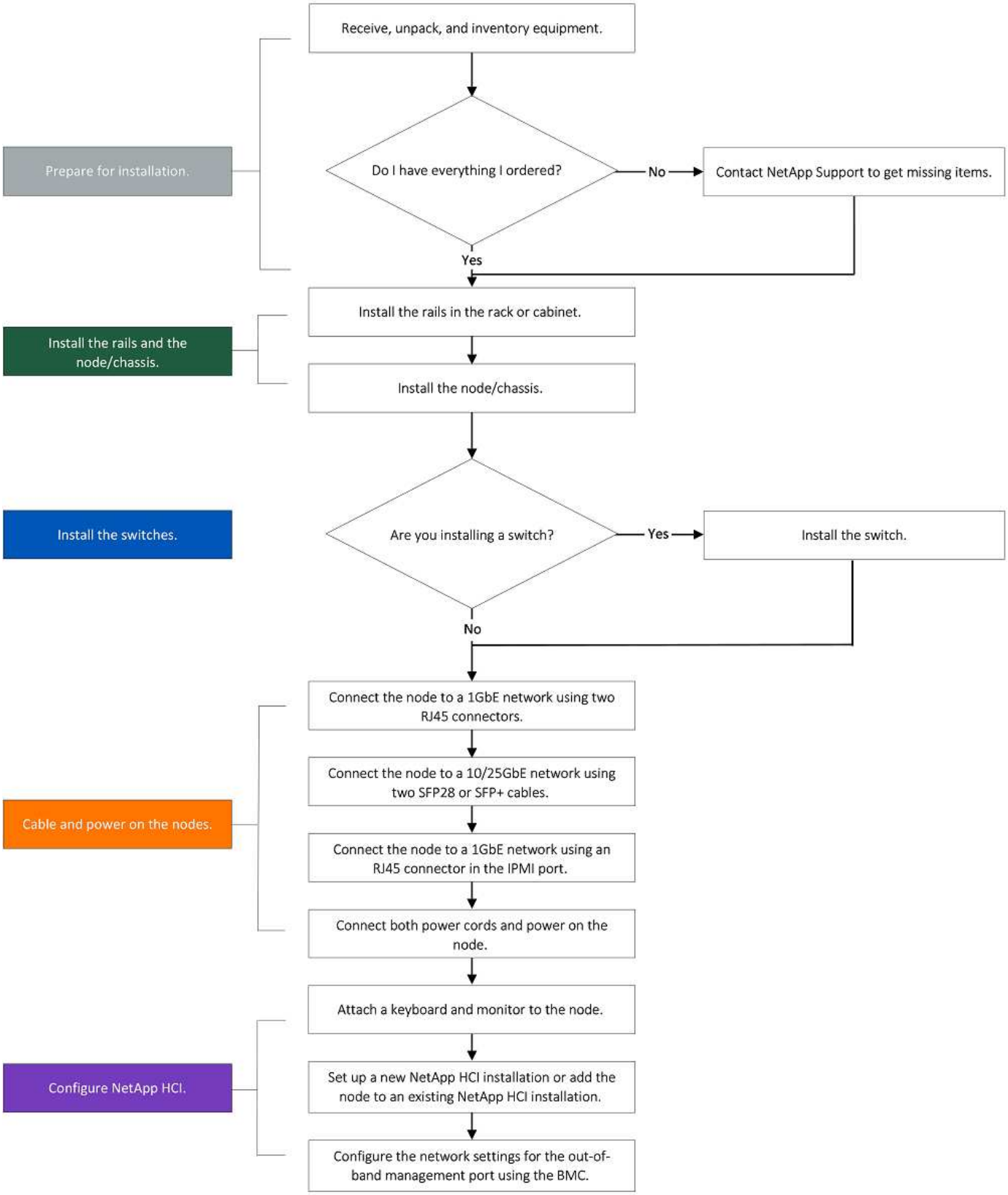
H610C および H615C

H610C および H615C では、 2U / 4 ノードシャーシと違ってノードとシャーシが別々のコンポーネントではないため、「ノード」と「シャーシ」は同じ意味で使用されます。



H610S

H610C および H615C では、 2U / 4 ノードシャーシと違ってノードとシャーシが別々のコンポーネントではないため、「ノード」と「シャーシ」は同じ意味で使用されます。


Prepare for installation.
Receive, unpack, and inventory equipment.
Do I have everything I ordered?
No
Contact NetApp Support to get missing items.
Yes
Install the rails and the node/chassis.
Install the rails in the rack or cabinet.
Install the node/chassis.
Install the switches.
Are you installing a switch?
Yes
Install the switch.
No
Cable and power on the nodes.
Connect the node to a 1GbE network using two RJ45 connectors.
Connect the node to a 10/25GbE network using two SFP28 or SFP+ cables.
Connect the node to a 1GbE network using an RJ45 connector in the IPMI port.
Connect both power cords and power on the node.
Configure NetApp HCI.
Attach a keyboard and monitor to the node.
Set up a new NetApp HCI installation or add the node to an existing NetApp HCI installation.
Configure the network settings for the out-of-band management port using the BMC.

設置を準備

設置準備として、出荷されたハードウェアの中身を確認し、不足しているコンポーネントがあ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。

設置場所に次のものがあることを確認します。

- システム用のラックスペース。

ノードタイプ	ラックスペース
H410C ノードと H410S ノード	2 ラックユニット（ 2U ）
H610C ノード	2U
H615C および H610S ノード	1 ラックユニット（ 1U ）

- SFP28 / SFP+ 直接接続ケーブルまたはトランシーバ
- RJ45 コネクタ付属の CAT5e 以上のケーブル
- システムを設定するためのキーボード、ビデオ、マウス（ KVM ）スイッチ
- USB スティック（オプション）

出荷されるハードウェアは、注文内容によって異なります。新しく購入した 2U / 4 ノードの注文には、シャーシ、ベゼル、スライドレールキット、ストレージノード用ドライブ、ストレージノードとコンピューティングノード用ドライブ、電源ケーブル（シャーシあたり 2 本）が含まれます。H610S ストレージノードを購入した場合、シャーシにはあらかじめドライブが搭載されています。

ハードウェアの設置時に、梱包材と包装をすべてユニットから取り除いてください。これにより、ノードの過熱やシャットダウンが防止されます。

レールを取り付けます

出荷時のハードウェアの注文には、一連のスライドレールが含まれています。レールの取り付けを完了するには、ドライバが必要です。インストールの手順は、ノードのモデルごとに多少異なります。

装置が転倒しないように、ラックの下から順にハードウェアを設置してください。ラックに安定化デバイスが含まれている場合は、ハードウェアを取り付ける前に取り付けてください。

- H410C および H410S
- [H610C]
- H610S と H615C

H410C および H410S

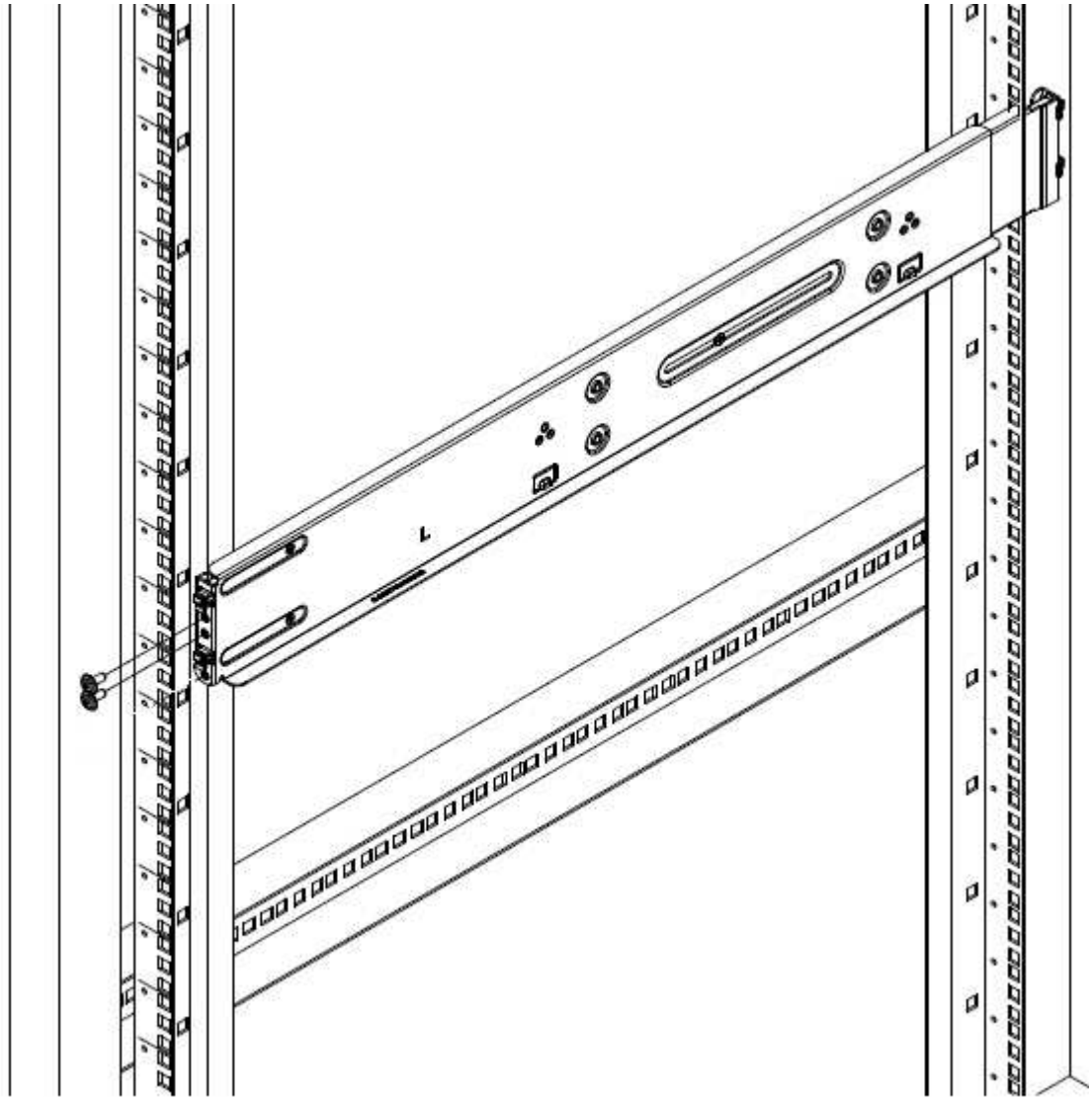
H410C ノードと H410S ノードは、 2 組のアダプタが搭載された 2U / 4 ノード H シリーズシャーシに設置されています。丸穴のラックにシャーシを設置する場合は、丸穴のラックに適したアダプタを使用してください。H410C ノードと H410S ノードのレールは、 29 インチ ~ 33.5 インチの奥行きのラックを収容します。レールが完全に収縮すると、長さは 28 インチになり、レールの前部と後部は 1 本のスクリュだけで固定されま

す。

> 完全に契約されたレールにシャーシを設置する場合は、レールの前面と背面のセクションが分かれていることがあります。

手順

1. レールの前面をラック前面ポストの穴に合わせます。
2. レール前面のフックをラック前面ポストの穴に押し込み、バネ付きのペグがラックの穴にカチッと収まるまで押し下げます。
3. レールをラックにネジで取り付けます。ラックの前面に取り付けられている左側のレールの図を次に示します。

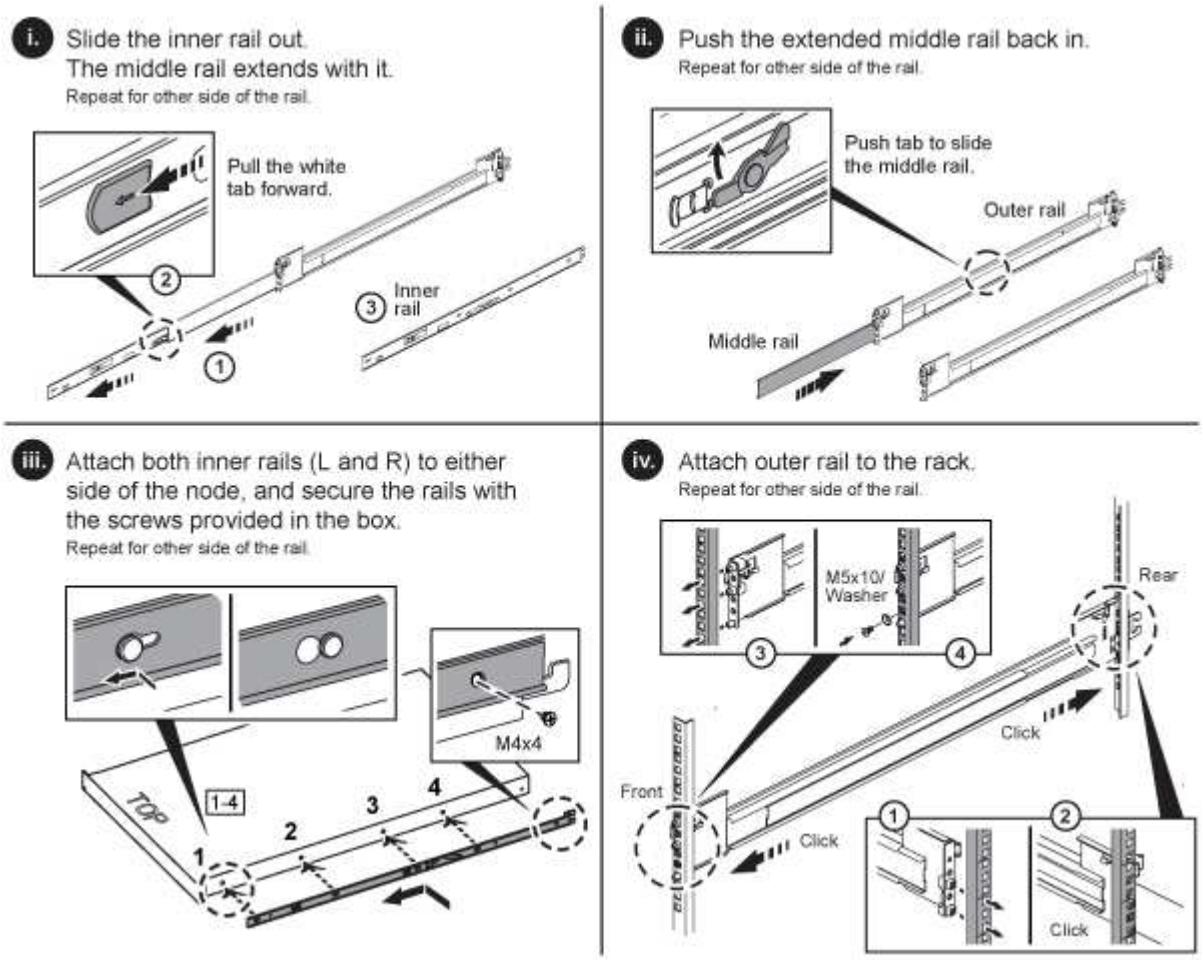


4. レールの後部をラックの背面ポストまで伸ばします。
5. レール背面のフックを背面ポストの適切な穴に合わせ、レールの前面と背面が同じ高さになるようにします。
6. レールの背面をラックに取り付け、レールをネジで固定します。

7. ラックの反対側で上記の手順をすべて実行します。

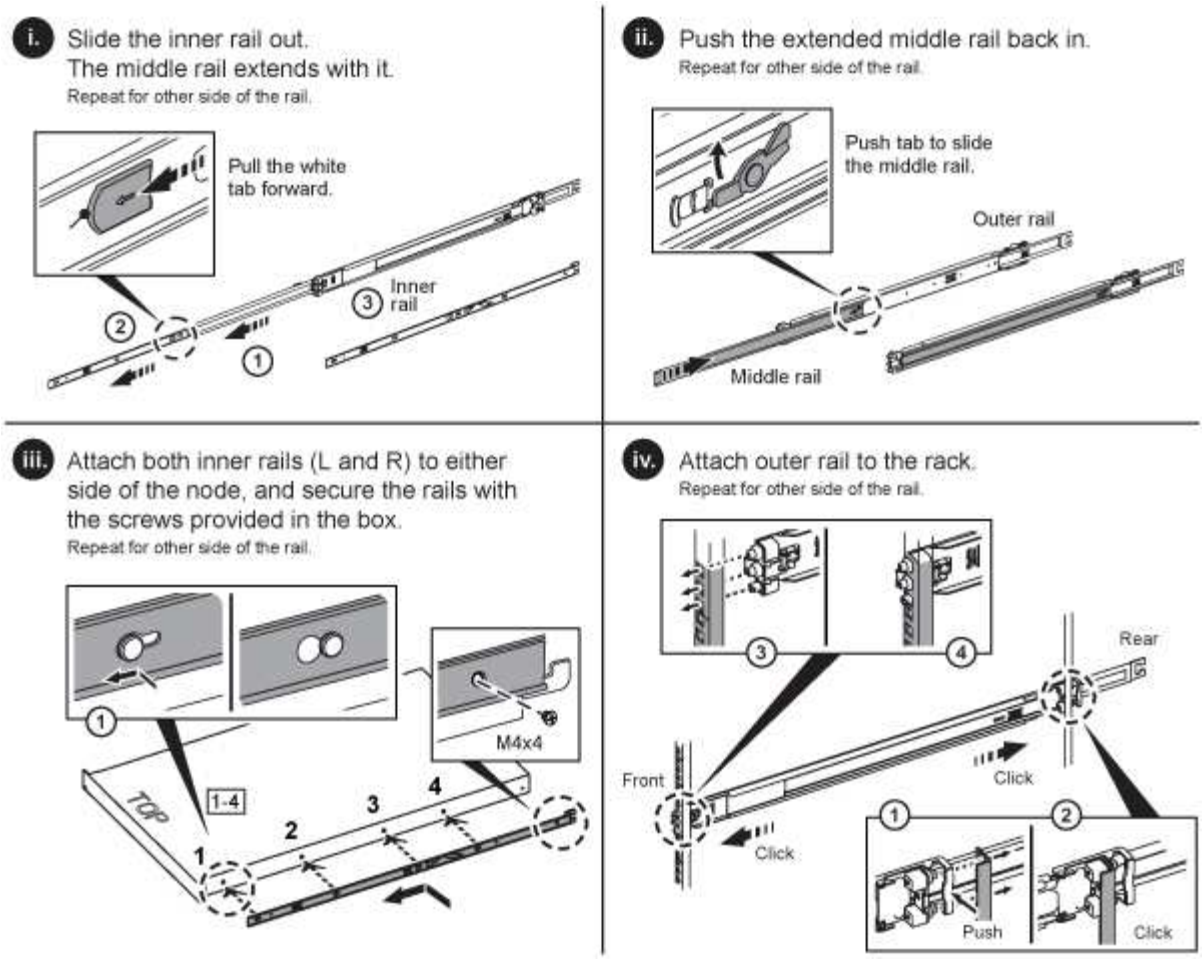
H610C

次の図は、 H61OC コンピューティングノード用のレールを設置する手順を示しています。



H610S と **H615C**

H610S ストレージノードまたは H615C コンピューティングノードのレールを設置する図を次に示します。



H610S と H615C には左右のレールがあります。H610S / H615C の取り付けネジを使用してシャーシをレールに固定できるよう、ネジ穴を下部に向けます。

ノード / シャーシを設置

H410C コンピューティングノードと H410S ストレージノードは、 2U / 4 ノードシャーシに設置します。H610C 、 H615C 、および H610S の場合、シャーシ / ノードをラックのレールに直接設置します。

NetApp HCI 1.8 以降では、 2 つまたは 3 つのストレージノードでストレージクラスタをセットアップできます。

梱包材と包装材をすべてユニットから取り除きます。これにより、ノードの過熱やシャットダウンが防止されます。

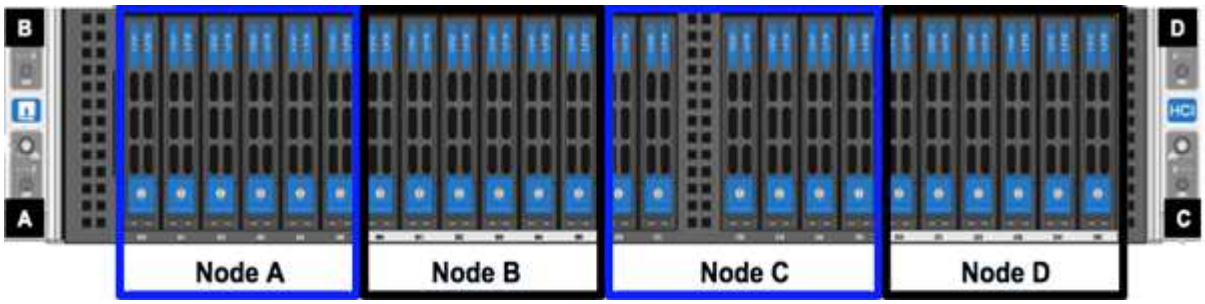
- H410C ノードと H410S ノード
- H610C ノード / シャーシ
- H610S および H615C ノード / シャーシ

H410C ノードと **H410S** ノード

手順

1. H410C ノードと H410S ノードをシャーシに設置します。4 つのノードを設置したシャーシの背面図の例を次に示します。

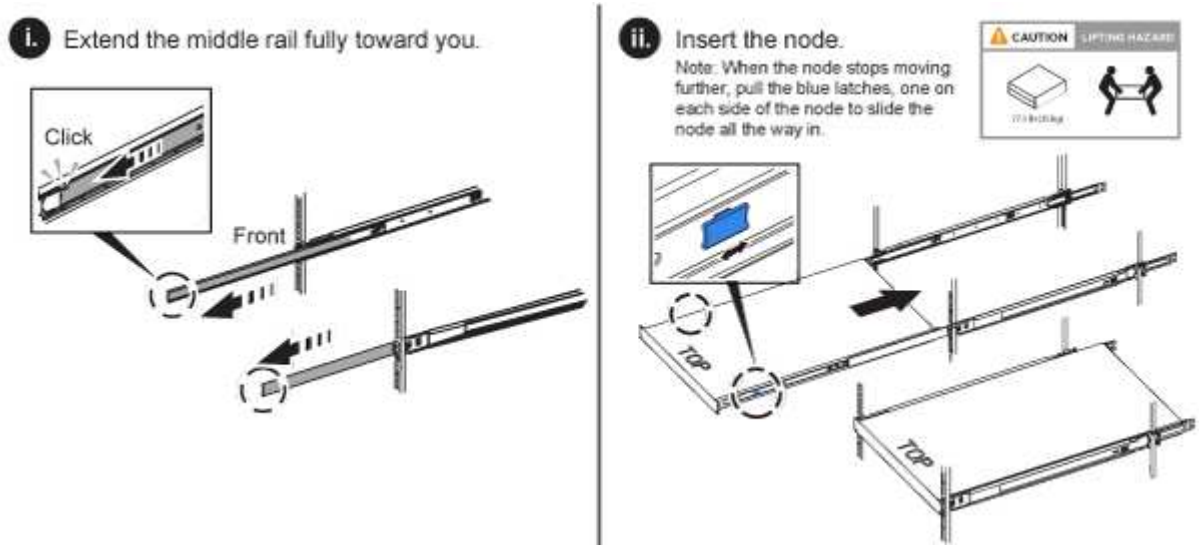
2. H410S ストレージノードのドライブを設置します。



H610C ノード / シャーシ

H610C では、 2U / 4 ノードシャーシとは異なり、ノードとシャーシが別々のコンポーネントではないため、「ノード」と「シャーシ」は同じ意味で使用されます。

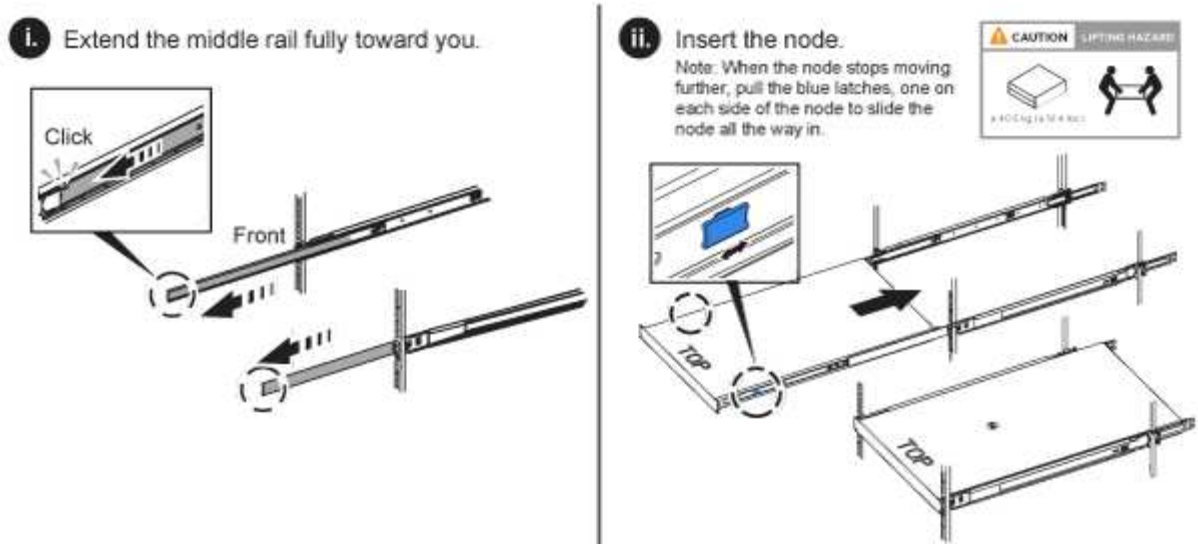
ノード / シャーシをラックに設置する場合の図を次に示します。



H610S および **H615C** ノード / シャーシ

H615C および H610S では、 2U / 4 ノードシャーシとは異なり、ノードとシャーシが別々のコンポーネントではないため、「ノード」と「シャーシ」は同じ意味で使用されます。

ノード / シャーシをラックに設置する場合の図を次に示します。



スイッチを設置します

NetApp HCI 環境で Mellanox SN2010 、 SN2100 、および SN2700 のスイッチを使用する場合は、次の手順に従ってスイッチを設置してケーブル接続します。

- "Mellanox ハードウェアユーザーマニュアル"
- "TR-4836 ：『 NetApp HCI with Mellanox SN2100 and SN2700 Switch Cabling Guide 』（ログインが必要）"

ノードをケーブル接続

既存の NetApp HCI 環境にノードを追加する場合は、追加するノードのケーブル配線とネットワーク構成が既存の環境と同じになるようにしてください。

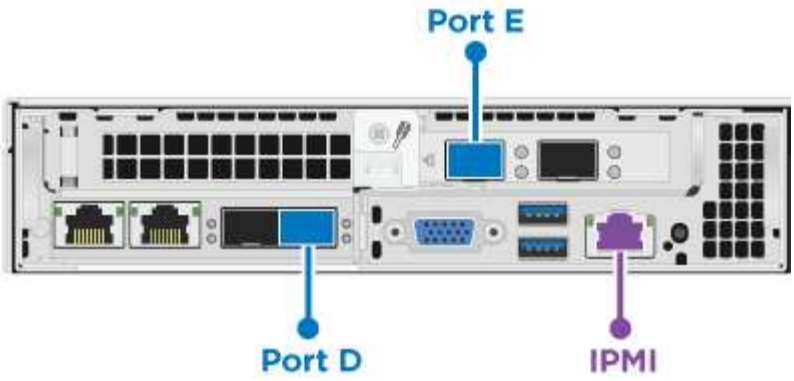
> シャーシ背面の通気口がケーブルやラベルで塞がれていないことを確認します。これにより、過熱によってコンポーネントで早期に障害が発生する可能性があります。

- H410C コンピューティングノードと H410S ストレージノード
- H610C コンピューティングノード
- H615C コンピューティングノード
- H610S ストレージノード

H410C コンピューティングノードと **H410S** ストレージノード

H410C ノードのケーブル接続には、 2 本のケーブルを使用する方法と 6 本のケーブルを使用する方法の 2 つがあります。

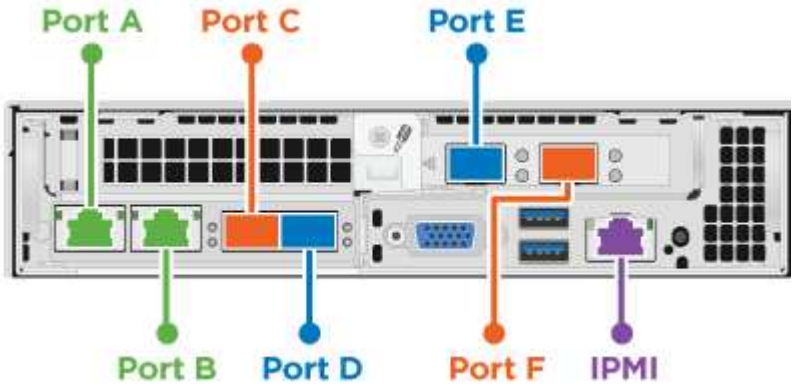
ケーブルを 2 本使用する構成は次のとおりです。



ポート D および E の場合は、 SFP28 / SFP+ ケーブルまたはトランシーバを 2 本接続して、管理、仮想マシン、ストレージの共有接続に使用します。

（オプションですが推奨） CAT5e ケーブルを IPMI ポートに接続します（アウトオブバンド管理接続用）。

ケーブルを 6 本使用する構成は次のとおりです。



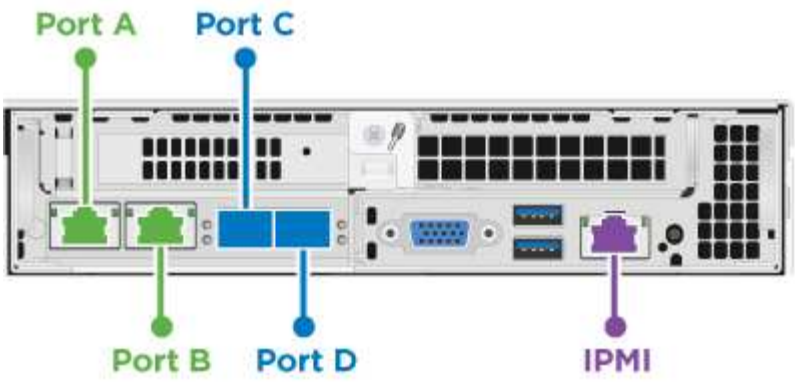
ポート A とポート B については、管理接続用に 2 本の CAT5e 以上のケーブルをポート A と B に接続します。

ポート C および F について、 SFP28 / SFP+ ケーブルまたはトランシーバを 2 本接続します。

ポート D および E の場合は、 SFP28 / SFP+ ケーブルまたはトランシーバを 2 本接続します。

（オプションですが推奨） CAT5e ケーブルを IPMI ポートに接続します（アウトオブバンド管理接続用）。

H410S ノードのケーブル配線は次のとおりです。



ポート A とポート B については、管理接続用に 2 本の CAT5e 以上のケーブルをポート A と B に接続します。

ポート C および D について、 SFP28 / SFP+ ケーブルまたはトランシーバを 2 本接続します。

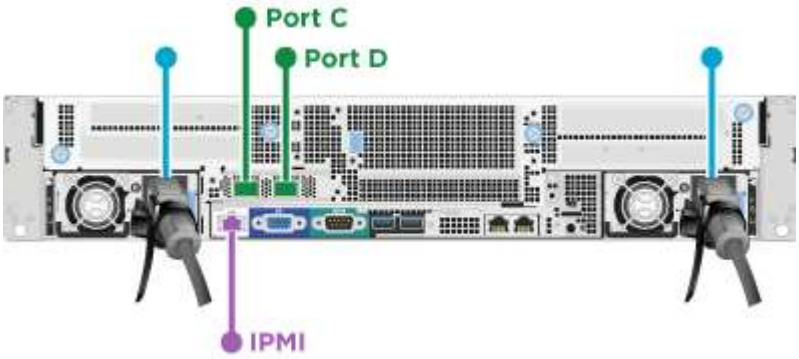
（オプションですが推奨） CAT5e ケーブルを IPMI ポートに接続します（アウトオブバンド管理接続用）。

ノードをケーブル接続したら、シャーシごとに 2 つある電源装置に電源コードを接続し、 240V の PDU または電源コンセントに差し込みます。

H610C コンピューティングノード

H610C ノードのケーブル配線は次のとおりです。

> H610C ノードはケーブルを 2 本使用する構成でのみ導入されます。すべての VLAN がポート C とポート D に存在することを確認します



ポート C および D の場合は、 SFP28 / SFP+ ケーブルを 2 本使用してノードを 10 / 25GbE ネットワークに接続します。

（オプション、推奨） IPMI ポートで RJ45 コネクタを使用してノードを 1GbE ネットワークに接続

両方の電源ケーブルをノードに接続し、 200~240V の電源コンセントに電源ケーブルを接続します。

H615C コンピューティングノード

H615C ノードのケーブル配線は次のとおりです。

> H615C ノードの導入は、ケーブルを 2 本使用する構成だけです。すべての VLAN がポート A とポート B に存在することを確認します

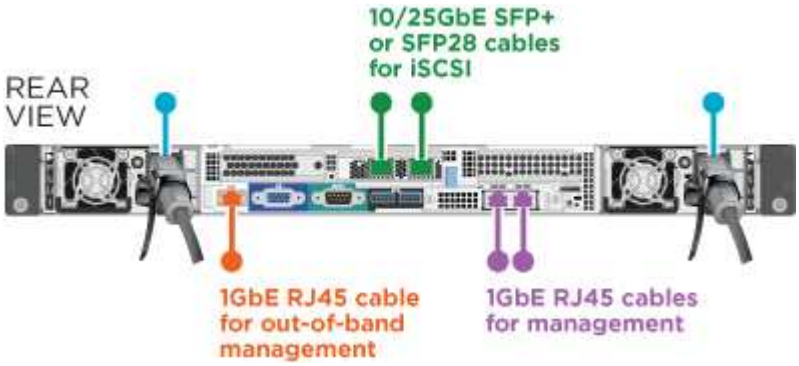
ポート A とポート B については、 SFP28 / SFP+ ケーブルを 2 本使用してノードを 10 / 25GbE ネットワークに接続します。

（オプション、推奨） IPMI ポートで RJ45 コネクタを使用してノードを 1GbE ネットワークに接続

両方の電源ケーブルをノードに接続し、電源ケーブルを 110~140V の電源コンセントに接続します。

H610S ストレージノード

H610S ノードのケーブル配線は次のとおりです。



IPMI ポートで 2 つの RJ45 コネクタを使用してノードを 1GbE ネットワークに接続します。

SFP28 または SFP+ ケーブルを 2 本使用してノードを 10 / 25GbE ネットワークに接続

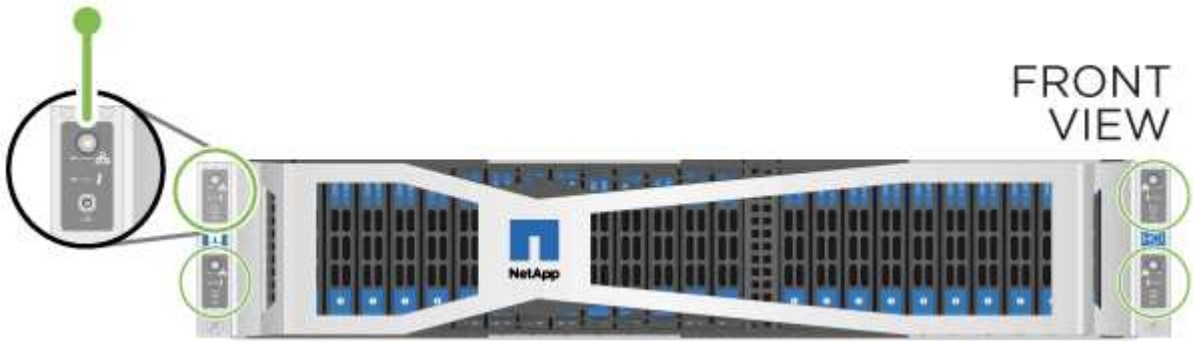
IPMI ポートで RJ45 コネクタを使用してノードを 1GbE ネットワークに接続

両方の電源ケーブルをノードに接続します。

ノードの電源をオンにします

ノードがブートするまでに約 6 分かかります。

次の図は、 NetApp HCI 2U シャーシの電源ボタンを示しています。



H610C ノードの電源ボタンを次の図に示します。

H615C および H610S ノードの電源ボタンを次の図に示します。

NetApp HCI を設定します

次のいずれかのオプションを選択します。

- 新しい NetApp HCI のインストール
- 既存の NetApp HCI インストールを展開します

新しい **NetApp HCI** のインストール

手順

1. 1 つの NetApp HCI ストレージノードの管理ネットワーク（ Bond1G ）で IPv4 アドレスを設定します。

> 管理ネットワークで DHCP を使用している場合は、 DHCP で取得されたストレージシステムの IPv4 アドレスに接続できます。

   a. キーボード、ビデオ、マウス（ KVM ）を 1 つのストレージノードの背面に接続します。
   b. ユーザインターフェイスで Bond1G の IP アドレス、サブネットマスク、ゲートウェイアドレスを設定します。Bond1G ネットワークの VLAN ID を設定することもできます。
2. サポート対象の Web ブラウザ（ Mozilla Firefox 、 Google Chrome 、 Microsoft Edge ）を使用し、手順 1 で設定した IPv4 アドレスに接続して NetApp Deployment Engine に移動します。
3. NetApp Deployment Engine のユーザインターフェイス（ UI ）を使用して NetApp HCI を設定します。

> 他のすべての NetApp HCI ノードは自動的に検出されます。

既存の **NetApp HCI** インストールを展開します

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。
2. NetApp HCI ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
3. ウィザードの手順に従って、ストレージノードとコンピューティングノードを NetApp HCI 環境に追加します。

> H410C コンピューティングノードを追加するには、既存の環境で NetApp HCI 1.4 以降を実行している必要があります。H615C コンピューティングノードを追加するには、既存の環境で NetApp HCI 1.7 以降を実行している必要があります。

> 同じネットワーク上に新しく設置した NetApp HCI ノードは自動的に検出されます。

設定後のタスクを実行

使用しているノードのタイプによっては、ハードウェアを設置して NetApp HCI を設定したあとで、追加の手順を実行する必要があります。

- H610C ノード
- H615C および H610S ノード

H610C ノード

設置した各 H610C ノード用の GPU ドライバを ESXi にインストールし、その機能を検証します。

H615C および **H610S** ノード

手順

1. Web ブラウザを使用して、デフォルトの BMC IP アドレス「 192.168.0.120 」に移動します
2. ユーザー名 root とパスワード calvin を使用してログインします
3. ノード管理画面で、 * Settings > Network Settings * と移動し、アウトオブバンド管理ポートのネットワークパラメータを設定します。

H615C ノードに GPU が搭載されている場合は、設置した H615C ノードごとに ESXi に GPU ドライバをインストールし、その機能を検証します。

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"
- "vCenter Server 向け NetApp Element プラグイン"
- "_TR-48820 ：『 NetApp HCI ネットワーククイックプランニングガイド』 _"
- "NetApp Configuration Advisor" 5.8.1 以降のネットワーク検証ツール

ストレージパフォーマンスを最適化するために **LACP** を設定します

NetApp HCI ストレージクラスタのパフォーマンスを最適化するには、各ストレージノードに使用するスイッチポートで Link Aggregation Control Protocol （ LACP ）を設定します。

作業を開始する前に

- NetApp HCI ストレージノードの 10 / 25GbE インターフェイスに接続されたスイッチポートを LACP ポートチャネルとして設定しておきます。
- ストレージトラフィックを処理するスイッチの LACP タイマーを「高速モード（ 1 秒）」に設定し、フェイルオーバー検出時間を最適化しておきます。導入時に、すべてのストレージノード上の Bond1G インターフェイスが自動的にアクティブ / パッシブモードに対応するように設定されます。
- ストレージネットワークを処理するスイッチで、 Cisco Virtual PortChannel （ vPC ）または同等のスイッチスタッキングテクノロジを設定しておきます。スイッチスタッキングテクノロジを使用することで LACP とポートチャネルを簡単に設定でき、ストレージノード上の 10 / 25GbE ポートとスイッチの間のトポロジでループが発生するのを防ぐことができます。

手順

1. スイッチベンダーの推奨事項に従って、 NetApp H シリーズストレージノードに使用するスイッチポートで LACP を有効にします。
2. NetApp HCI を導入する前に、ノード上のユーザインターフェイス（ターミナルユーザインターフェイスまたは TUI と呼ばれる）ですべてのストレージノードのボンディングモードを LACP に変更します。

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"

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

Active IQ Config Advisor で環境を検証

NetApp HCI ハードウェアを設置して NetApp HCI をインストールする前に、環境が NetApp HCI ネットワークの要件を満たしていることを確認する必要があります。Active IQ Config Advisor は、ネットワーク、スイッチ、および VMware vSphere の設定を検証することで、環境に対してチェックを実行します。このツールでは、問題の解決に役立つレポートが生成されます。また、インストールの準備やスケジュール設定のために、プロフェッショナルサービスエンジニアにレポートを転送できます。

Active IQ Config Advisor をインストールします

NetApp HCI ネットワークにアクセスできる PC に Active IQ Config Advisor をダウンロードしてインストールします。

手順

1. Web ブラウザで、ネットアップのサポートメニューから「 * Tools 」を選択し、 Active IQ Config Advisor を検索して、ツールをダウンロードします。

   "ネットアップサポートサイトのツール"。

   エンドユーザライセンス契約（ EULA ）に同意すると、ダウンロードページが表示されます。Microsoft Windows 、 Linux 、および Mac のバイナリは、「 * Client Tool * 」パネルから入手できます。

2. 実行ファイルを実行します。
3. 言語を選択し、 * OK * をクリックします。
4. 「 * 次へ * 」をクリックします。
5. EULA を読み、「 * I Agree * 」をクリックします。
6. 「 * Install * 」をクリックします。
7. [ファイル名を指定して実行（ Run Active IQ Config Advisor ）] が選択されていることを確認して、 [完了（ Finish ）]

   しばらくすると、新しいブラウザウィンドウまたはタブで Active IQ Config Advisor UI が開きます。

Active IQ Config Advisor を使用します

Active IQ Config Advisor はブラウザウィンドウで実行され、ネットワークと環境に関する情報を収集します。 NetApp HCI の導入に支障をきたす可能性のあるネットワークや設定の問題を解決するためのレポートを生成できます。

作業を開始する前に

管理ネットワーク、 VMware vCenter Server のネットワークにアクセスできるデバイス（既存の VMware 環境に参加する場合）、および NetApp HCI に使用するスイッチに Active IQ Config Advisor をインストールしておきます。

> Mellanox スイッチを使用しており、ネットアッププロフェッショナルサービスを導入の一環として設定する場合は、スイッチの情報を指定する必要はありません。

このタスクについて

Active IQ Config Advisor は、情報収集のために読み取り専用チェックのみを実行します。コレクションの一部として変更される設定はありません。

手順

1. Active IQ Config Advisor を開きます。

   Config Advisor が Web ブラウザに * 基本設定 * ウィンドウとともに表示されます。ここでは、グローバル収集設定を定義し、収集結果を暗号化できます。

2. コレクションプロジェクトを暗号化するには、「 * 暗号化設定 * 」セクションにパスフレーズを入力します。

   これにより、このコレクションプロジェクトを作成した後でロードできるのは、そのコレクションプロジェクトだけになります。

3. 「 * ユーザー検証 * 」セクションに自分の名前とメールアドレスを入力して、このコレクションレポートを自分のものとして特定します。
4. [保存（ Save ）] をクリックします。
5. [新しいデータ収集を作成する *] をクリックします。
6. [**Collection Type**](コレクションタイプ *) ドロップダウンメニューで [Solution Based *](ソリューションベース *)] を選択します。
7. [* プロファイル **]** ドロップダウンメニューで **[** NetApp HCI 事前展開 *] を選択します。
8. [**Type**] 列のデバイスのタイプごとに、 [*Actions] ドロップダウンメニューで NetApp HCI ネットワーク内のデバイスのタイプ番号を選択します。

   たとえば、 3 つの Cisco スイッチがある場合は、その行の [*Actions] カラムドロップダウンメニューから 3 を選択します。指定した Cisco スイッチごとに 1 つずつ、 3 行表示されます。

   > Mellanox スイッチを使用しており、ネットアッププロフェッショナルサービスを導入の一環として設定する場合は、スイッチの情報を指定する必要はありません。

9. 特定したスイッチについて、管理 IP アドレスおよび管理者のクレデンシャルを入力します。
10. 特定した VMware vCenter Server に対して、次のいずれかを実行します。
    - 新しい vCenter Server を導入する場合は、サーバで計画している IP アドレスまたは Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を指定してください。
    - 既存の vCenter Server に参加する場合は、 IP アドレスまたは FQDN と、そのサーバの管理者クレデンシャルを入力します。
11. オプション：スイッチに関する情報を追加した場合は、「 * Switch Validation * 」セクションにコンピューティングノードとストレージノードの数を入力します。
12. 使用するコンピューティングノードのケーブル接続構成は、「コンピューティングノードネットワーク」セクションで選択します。

13. [コンピューティングノードネットワーク *] セクションで、スイッチの管理ネットワーク、 vMotion ネットワーク、ストレージネットワークに使用する VLAN タグを、個々のスイッチポートと VLAN タグで入力します。
14. スイッチの管理ネットワークおよびストレージネットワークに使用する VLAN タグは、「ストレージノードネットワーク * 」セクションに個別のスイッチポートと VLAN タグで入力します。
15. 「 * Network Settings Check * 」セクションに、管理ネットワークの IP アドレスとゲートウェイ IP アドレス、および DNS 、 NTP 、 vCenter Server （ NetApp HCI を使用して新しい vCenter Server を導入する場合）用のサーバのリストを入力します。

    このセクションでは、 Active IQ Config Advisor を使用して管理ネットワークを確実に利用できるようにするとともに、 DNS や NTP などのサービスが適切に機能するようにします。

16. 入力したすべての IP アドレス情報とクレデンシャルが有効であることを確認するには、 * Validate * をクリックします。
17. [保存] または [収集] をクリックします。

    これにより収集プロセスが開始され、収集が実行される進行状況と収集コマンドのリアルタイムログを確認できます。[* 進捗状況 *] 列には、各収集タスクの進捗バーが色分けされて表示されます。

    進捗バーは、次の色を使用してステータスを表示します。

    - * 緑 * ：収集はコマンドの失敗なしで終了しました。展開リスクと推奨事項を確認するには、 * アクション * メニューの * 表示と分析 * アイコンをクリックします。
    - * 黄 * ：一部のコマンドエラーで収集が完了しました。展開リスクと推奨事項を確認するには、 * アクション * メニューの * 表示と分析 * アイコンをクリックします。
    - * 赤 * ：収集が失敗しました。エラーを解決してから、収集を再度実行する必要があります。
18. オプション：収集が完了したら、任意の収集行の双眼鏡アイコンをクリックすると、実行されたコマンドと収集されたデータが表示されます。
19. [* 表示と解析 * （ View & Analyze * ）] タブを選択します。

    このページには、環境の全般的な健全性レポートが表示されます。円グラフのセクションを選択して、特定のチェックに関する詳細や問題の説明のほか、導入の成功に支障をきたす可能性のある問題の解決に関する推奨事項を確認できます。このような問題は、お客様自身で解決することも、ネットアッププロフェッショナルサービスにご依頼いただくこともできます。

20. 「 * 書き出し * 」をクリックして、コレクションレポートを PDF または Microsoft Word 文書として書き出します。

    > PDF と Microsoft Word のドキュメント出力には、導入環境のスイッチ構成情報が含まれています。ネットアッププロフェッショナルサービスは、この情報を使用してネットワーク設定を検証します。

21. エクスポートしたレポートファイルをネットアッププロフェッショナルサービスの担当者に送信します。

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

各ノードに IPMI を設定します

NetApp HCI ハードウェアをラックに設置してケーブル接続し、電源をオンにしたら、各ノードに Intelligent Platform Management Interface （ IPMI ）アクセスを設定できます。各 IPMI ポートに IP アドレスを割り当て、ノードへのリモート IPMI アクセスが可能になったらすぐにデフォルトの IPMI 管理者パスワードを変更します。

前提条件

環境が NetApp HCI をサポートできる状態になっていることを確認し、潜在的な問題を解決したら、導入前にいくつかの最終的なタスクを完了する必要があります。

- Active IQ Config Advisor からのレポートが正常に作成されていることを確認します。
- ネットワーク、既存または導入予定の VMware インフラ、およびユーザクレデンシャルに関連する情報をすべて収集します。
- NetApp HCI をラックに設置し、ケーブルを配線して、電源をオンにします。

IPMI ポートの IP アドレスを手動で割り当てます

各 NetApp HCI ノードの IPMI ポートでは、動的ホスト構成プロトコル（ DHCP ）がデフォルトで有効になっています。IPMI ネットワークで DHCP を使用しない場合は、 IPMI ポートに静的 IPv4 アドレスを手動で割り当てることができます。

作業を開始する前に

各ノードの BIOS にアクセスするためのキーボード、ビデオ、マウス（ KVM ）スイッチまたはモニタとキーボードがあることを確認します。

このタスクについて

BIOS 内を移動するには、矢印キーを使用します。タブまたはオプションを選択するには、 Enter キーを押します。前の画面に戻るには、 Esc キーを押します。

手順

1. ノードの電源をオンにします。
2. 起動時に「 D 」キーを押して BIOS に入ります。
3. IPMI タブを選択します。
4. **BMC Network Configuration** を選択し 'Enter' キーを押します
5. 「はい」を選択し、「 Enter 」キーを押します。
6. 「 * Configuration Address Source * 」を選択し、「 Enter 」キーを押します。
7. 「 * Static * 」を選択し、「 Enter 」キーを押します。
8. ステーション IP アドレス * を選択し、 IPMI ポートの新しい IP アドレスを入力します。終了したら Enter キーを押します。

9. サブネットマスク * を選択し、 IPMI ポートの新しいサブネットマスクを入力します。終了したら Enter キーを押します。
10. ゲートウェイ IP アドレス * を選択し、 IPMI ポートの新しいゲートウェイ IP アドレスを入力します。終了したら Enter キーを押します。
11. イーサネットケーブルの一方の端を IPMI ポートに、もう一方の端をスイッチに接続します。

    このノードの IPMI ポートが使用可能になります。

12. IPMI ポートが設定されていない他の NetApp HCI ノードについて、この手順を繰り返します。

H410C ノードと H410S ノードのデフォルトの IPMI パスワードを変更します

IPMI ネットワークポートを設定したらすぐに、各コンピューティングノードとストレージノードで IPMI 管理者アカウントのデフォルトパスワードを変更する必要があります。

作業を開始する前に

各コンピューティングノードとストレージノードに IPMI の IP アドレスを設定しておきます。

手順

1. IPMI ネットワークにアクセス可能なコンピュータで Web ブラウザを開き、ノードの IPMI IP アドレスにアクセスします。
2. ログイン・プロンプトにユーザ名 ADMIN とパスワード ADMIN を入力します
3. ログインしたら、 * Configuration * タブをクリックします。
4. [* ユーザー *] をクリックします。
5. 「 Admin 」ユーザを選択し、「 * Modify User * 」をクリックします。
6. [パスワードの変更 *] チェックボックスをオンにします。
7. [パスワード *] フィールドと [パスワードの確認 *] フィールドに新しいパスワードを入力します。
8. [* 変更 *] をクリックし、 [OK] をクリックします。
9. デフォルトの IPMI パスワードを使用するすべての NetApp HCI H410C および H410S ノードについて、この手順を繰り返します。

H610C 、 H615C 、および H610S ノードのデフォルトの IPMI パスワードを変更します

IPMI ネットワークポートを設定したらすぐに、各コンピューティングノードとストレージノードで IPMI 管理者アカウントのデフォルトパスワードを変更する必要があります。

作業を開始する前に

各コンピューティングノードとストレージノードに IPMI の IP アドレスを設定しておきます。

手順

1. IPMI ネットワークにアクセス可能なコンピュータで Web ブラウザを開き、ノードの IPMI IP アドレスにアクセスします。
2. ログインプロンプトにユーザ名「 root 」とパスワード「 calvin 」を入力します。
3. ログインしたら、ページ左上のメニューナビゲーションアイコンをクリックしてサイドバードロワーを開

きます。

4. [* 設定 *] をクリックします。
5. [ユーザー管理] をクリックします。
6. リストから * Administrator * ユーザーを選択します。
7. [パスワードの変更 *] チェックボックスをオンにします。
8. [パスワード *] フィールドと [パスワードの確認 *] フィールドに、新しい強力なパスワードを入力します。
9. ページの下部にある「 * 保存」をクリックします。
10. デフォルトの IPMI パスワードを使用するすべての NetApp HCI H610C 、 H615C 、または H610S ノードについて、この手順を繰り返します。

詳細については、こちらをご覧ください

- "NetApp SolidFire Active IQ のドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

NetApp HCI を導入します

NetApp Deployment Engine にアクセスします

NetApp Deployment Engine のアクセスオプションの概要

NetApp HCI を導入するには、いずれかの NetApp H シリーズストレージノード上の NetApp Deployment Engine に、 Bond1G インターフェイスに割り当てられた IPv4 アドレスを使用してアクセスする必要があります。 Bond1G インターフェイスは、ストレージノードのポート A と B を組み合わせた論理インターフェイスです。このストレージノードを使用して導入プロセスを制御します。環境に応じて、 IPv4 アドレスを設定するか、またはいずれかのストレージノードから取得する必要があります。

> NetApp Deployment Engine へのアクセスに使用できるのは、ストレージノードの Bond1G インターフェイスのみです。Bond10G インターフェイスを使用して、ストレージノードのポート C とポート D を組み合わせた論理インターフェイスはサポートされていません。

NetApp Deployment Engine にアクセスするには、使用するネットワーク環境に最も近い次の方法のいずれかを使用します。

シナリオ（ **Scenario** ）	メソッド
DHCP を使用していない	"DHCP を使用していない環境では、 NetApp Deployment Engine にアクセスします"
環境で DHCP を使用している	"DHCP を使用している環境で NetApp Deployment Engine にアクセスします"
すべての IP アドレスを手動で割り当てる	"NetApp Deployment Engine にアクセスするには、IP アドレスを手動で割り当ててください"

詳細については、こちらをご覧ください

- "完全修飾ドメイン名 Web UI アクセスを設定します"

DHCP を使用していない環境では、 NetApp Deployment Engine にアクセスします

ネットワークで DHCP を使用していない場合は、 NetApp Deployment Engine へのアクセスに使用するストレージノード（制御用ストレージノード）の Bond1G インターフェイスに静的 IPv4 アドレスを設定する必要があります。制御用ストレージノードの NetApp Deployment Engine は、他のコンピューティングノードとストレージノードの Bond10G インターフェイスに自動で設定された IPv4 アドレスを使用し、これらのノードを検出して通信を確立します。ネットワークに特別な要件がないかぎり、この方法を使用してください。

必要なもの

- 自分またはネットワーク管理者が、『セットアップガイド』ドキュメントのタスクを完了している。

- NetApp HCI ノードに物理的にアクセスできるようにしておきます。
- すべての NetApp HCI ノードの電源をオンにしておきます。
- NetApp HCI ネットワークで DHCP が有効になっておらず、 NetApp HCI ノードが DHCP サーバから IP アドレスを取得していません。
- すべてのノードの Bond1G インターフェイスと Bond10G インターフェイスについて、 NetApp HCI 管理ネットワークをネイティブ VLAN として構成しておきます。

手順

1. いずれかの NetApp HCI ストレージノードの背面に KVM を接続します（このノードが制御用ストレージノードになります）。
2. ユーザインターフェイスで Bond1G の IP アドレス、サブネットマスク、ゲートウェイアドレスを設定します。必要に応じて、 Bond1G ネットワークの VLAN ID を設定することもできます。

   この IPv4 アドレスは、 NetApp Deployment Engine を使用した以降の導入時に再利用することはできません。

3. NetApp HCI 管理ネットワークにアクセスできるコンピュータで Web ブラウザを開きます。
4. 制御用ストレージノードに割り当てた IP アドレスにアクセスします。例：

   ```
   http://<Bond1G IP address>
   ```

   ここで HTTP を使用していることを確認してください。

   NetApp Deployment Engine のユーザインターフェイスが表示されます。

詳細については、こちらをご覧ください

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

DHCP を使用している環境で NetApp Deployment Engine にアクセスします

IPv4 の設定を DHCP から自動的に取得するようにサーバを構成している環境では、いずれかのストレージノードの Bond1G インターフェイスに割り当てられた IPv4 アドレスを使用して NetApp Deployment Engine にアクセスできます。このストレージノードの IPv4 アドレスは USB メモリを使用して取得できます。NetApp Deployment Engine は、 DHCP から割り当てられた IPv4 アドレスを使用している他のコンピューティングノードとストレージノードを自動的に検出します。ネットワークに特別な要件がないかぎり、この方法は使用しないでください。

必要なもの

- 自分またはネットワーク管理者が、『セットアップガイド』ドキュメントのタスクを完了している。
- NetApp HCI ノードに物理的にアクセスできるようにしておきます。

- すべての NetApp HCI ノードの電源をオンにしておきます。
- NetApp HCI の管理ネットワークとストレージネットワークで DHCP を有効にしておきます。
- DHCP アドレスプールは、 NetApp HCI ノードごとに 2 つの IPv4 アドレスを格納するのに十分な大きさです。

> NetApp HCI を適切に導入するためには、環境内のすべてのノードの IPv4 アドレスを DHCP から取得したアドレスか自動で設定したアドレスのどちらかにする必要があります（ IPv4 アドレスの割り当て方法を混在させることはできません）。

このタスクについて

DHCP をストレージネットワーク（ Bond10G インターフェイス）にのみ使用している場合は、リンクに記載されている手順を使用してください。 "DHCP を使用していない環境では、 NetApp Deployment Engine にアクセスします" NetApp Deployment Engine にアクセスします。

手順

1. ノードが IP アドレスを要求するまで数分待ちます。
2. ストレージノードを選択し、そのノードに USB メモリを挿入します。そのまま少なくとも 5 秒間待ちます。
3. USB スティックを取り外し、コンピュータに挿入します。
4. 'Re'DME.html' ファイルを開きますNetApp Deployment Engine のユーザインターフェイスが表示されます。

詳細については、こちらをご覧ください

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

NetApp Deployment Engine にアクセスするには、 IP アドレスを手動で割り当ててください

すべての NetApp HCI ノードの Bond1G インターフェイスと Bond10G インターフェイスに静的 IPv4 アドレスを手動で割り当て、 NetApp Deployment Engine にアクセスして NetApp HCI を導入することができます。ネットワークに特別な要件がないかぎり、この方法は使用しないでください。

必要なもの

- 自分またはネットワーク管理者が、『セットアップガイド』ドキュメントのタスクを完了している。
- NetApp HCI ノードに物理的にアクセスできるようにしておきます。
- すべての NetApp HCI ノードの電源をオンにしておきます。
- NetApp HCI ネットワークで DHCP が有効になっておらず、 NetApp HCI ノードが DHCP サーバから IP アドレスを取得していません。注： NetApp Deployment Engine を使用してシステムを導入する前に手動で割り当てる IP アドレスはすべて一時的な IP アドレスであり、再利用することはできません。IP アドレスを手動で割り当てる場合は、最終的な導入時に割り当て可能な、未使用かつ永続的な IP アドレスのセットをもう 1 つ確保しておく必要があります。

このタスクについて

この構成では、導入時にコンピューティングノードとストレージノードが静的 IPv4 アドレスを使用して他のノードを検出して通信を確立します。この構成は推奨されません。

手順

1. いずれかの NetApp HCI ストレージノードの背面に KVM を接続します（このノードが制御用ストレージノードになります）。
2. ユーザインターフェイスで Bond1G および Bond10G の IP アドレス、サブネットマスク、ゲートウェイアドレスを設定します。必要に応じて、各ネットワークの VLAN ID を設定することもできます。
3. 残りのストレージノードとコンピューティングノードについて手順 2 を繰り返します。
4. NetApp HCI 管理ネットワークにアクセスできるコンピュータで Web ブラウザを開きます。
5. 制御用ストレージノードに割り当てた Bond1G の IP アドレスにアクセスします。例：

   ```
   http://<Bond1G IP address>
   ```

   NetApp Deployment Engine のユーザインターフェイスが表示されます。

詳細については、こちらをご覧ください

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

導入を開始

NetApp HCI の導入を続行する前に、エンドユーザライセンス契約を読んで内容を理解しておく必要があります。

手順

1. NetApp HCI へようこそ * ページで、 * はじめに * をクリックします。
2. [前提条件 *] ページで、次の操作を行います。
   a. それぞれの前提条件が満たされていることを確認し、関連する各チェックボックスをクリックして確定します。
   b. [* Continue （続行）] をクリックします
3. [* エンドユーザーライセンス * （ End User Licenses * ）] ページで、次の手順を実行します。
   a. ネットアップのエンドユーザライセンス契約を読みます
   b. 条件に同意する場合は、契約テキストの下部にある [* 同意します] をクリックします。
   c. VMware のエンドユーザライセンス契約を読みます。
   d. 条件に同意する場合は、契約テキストの下部にある [* 同意します] をクリックします。
   e. [* Continue （続行）] をクリックします

詳細については、こちらをご覧ください

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

インストールプロファイルをインポートします

ネットアップを入手した場合は "ConfigBuilder" 出力されたインストール環境のプロファイルは、 NetApp HCI のインストールプロセスで NetApp Deployment Engine のフィールドに自動的に入力されるようにインポートできます。これはオプションの手順です。

このタスクについて

インストールプロファイルをインポートする場合も、 NetApp Deployment Engine のクレデンシャル * ページで NetApp HCI で使用するクレデンシャルを入力する必要があります。

> インストールプロファイルのフィールドを空白のままにするか、正しく入力しないと、 NetApp Deployment Engine のページで情報を手動で入力または修正しなければならない場合があります。情報を追加または修正する必要がある場合は、レコードおよびインストールプロファイルの情報を更新してください。

プロファイルをインポートします

1. [* インストールプロファイル *] ページで、 [* 参照] をクリックしてインストールプロファイルを検索し、アップロードします。
2. ファイルダイアログで、プロファイル JSON ファイルを選択して開きます。
3. プロファイルが正常にインポートされたら、 [* Continue （続行）] をクリックします。

   NetApp Deployment Engine の各ページで手順を実行して、インストールプロファイルからインポートされた設定を確認します。

プロファイルをインポートせずに続行します

1. インポート手順をスキップするには、 [* インストールプロファイル *] ページで [* 続行] をクリックします。

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"

VMware vSphere を設定します

VMware vSphere の設定

NetApp HCI は、 VMware vSphere の vCenter Server および ESXi コンポーネントを使用します。vCenter Server は、各コンピューティングノードにインストールされている VMware ESXi ハイパーバイザーを管理および監視するために使用されます。新しい vSphere 環境をインストールして設定することができます。この環境には NetApp Element Plug-in for vCenter Server もインストールされます。また、既存の vSphere 環

境に参加して拡張することもできます。

NetApp Deployment Engine を使用して vSphere を新規にインストールする場合は、次の点に注意してください。

- NetApp Deployment Engine は、「小規模」の導入規模オプションを使用して新しい vCenter Server Appliance をインストールします。
- vCenter Server ライセンスは一時的な評価ライセンスです。評価期間後も運用を継続するには、 VMware から新しいライセンスキーを取得して vCenter Server ライセンスインベントリに追加する必要があります。

> vSphere のインベントリ設定がフォルダを使用して vCenter データセンター内の NetApp HCI クラスタを格納している場合、 NetApp HCI コンピューティングリソースの拡張などの一部の処理が失敗します。NetApp HCI クラスタが vSphere Web Client インベントリツリーのデータセンターの直下にあり、フォルダに格納されていないことを確認してください。詳細については、ネットアップの技術情報アーティクルを参照してください。

新しい vCenter Server をインストールする場合は、ネットワーク構成時に vSphere 標準スイッチまたは vSphere Distributed Switch （ VDS ）をインストールできます。VDS を使用すると、 NetApp HCI の導入後に仮想マシンのネットワーク構成を簡単かつ一元的に管理できます。NetApp HCI のクラウドデータサービス機能には VDS が必要です。クラウドデータサービスでは vSphere Standard Switch はサポートされません。

詳細については、こちらをご覧ください

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

新しい **VMware vSphere** 環境を設定します

NetApp HCI のインストールプロセスでは、 vSphere で使用するいくつかのネットワーク情報を指定することで新しい vSphere 環境を導入できます。IP アドレスを使用して vSphere を設定する場合、インストール後にアドレスを変更することはできません。

必要なもの

導入する vSphere 環境のネットワーク情報を入手しておきます。

手順

1. ［ * 新しい vSphere 導入の構成 * ］ をクリックします。
2. 導入時にシステムによってインストールされる vSphere のバージョンを選択します。
3. 次のいずれかの方法で新しい vSphere 環境を設定します。

オプション	手順
ドメイン名を使用します（推奨）。	a. [完全修飾ドメイン名を使用して構成する *] をクリックします。 b. vCenter Server のドメイン名を「 * vCenter Server の完全修飾ドメイン名 * 」フィールドに入力します。 c. DNS サーバーの IP アドレスを、 *DNS サーバーの IP アドレス * フィールドに入力します。 d. [* Continue （続行）] をクリックします
IP アドレスを使用する。	a. IP アドレスを使用して設定 * をクリックします。 b. [* Continue （続行）] をクリックします

詳細については、こちらをご覧ください

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

既存の **VMware vSphere** 環境に参加します

vCenter Server のネットワーク情報とクレデンシャルを指定すると、既存の vSphere 環境を活用するように NetApp HCI を設定できます。

必要なもの

- 既存の vSphere 6.7 の環境に参加する場合は、 vCenter Server がバージョン 6.7 Update 1 を実行していることを確認します。
- 既存の vSphere 6.5 環境に参加する場合は、 vCenter Server がバージョン 6.5 Update 2 以降を実行していることを確認します。
- 既存の vSphere 環境のネットワークの詳細と管理者クレデンシャルを取得します。
- NetApp Element Plug-in for vCenter Server が既存の vCenter インスタンスに登録されている場合は、が必要です "登録解除します" 続行する前に。NetApp HCI の導入が完了すると、プラグインが再登録されます。

このタスクについて

vCenter リンクモードを使用して接続されている複数の vCenter Server システムに参加した場合、 NetApp HCI は 1 つの vCenter Server システムのみを認識します。

- Element Plug-in for vCenter Server 5.0以降では、を使用します "vCenter リンクモード "NetApp SolidFire ストレージクラスタを管理するvCenter Serverごとに、Element Plug-in を別々の管理ノードから登録します（推奨）。
- Element Plug-in for vCenter Server 4.10以前を使用して、他のvCenter Serverのクラスタリソースを管理する "vCenter リンクモード" はローカルストレージクラスタのみに制限されます。

手順

1. 「 * Join 」をクリックして、既存の vSphere 環境を拡張します。 *
2. ドメイン名または IP アドレスを「 * vCenter Server ドメイン名または IP アドレス * 」フィールドに入力します。ドメイン名を入力する場合は、表示される **DNS Server IP Address** フィールドにアクティブな DNS サーバの IP アドレスも入力する必要があります。
3. vSphere 管理者のクレデンシャルを「 * User Name 」フィールドと「 Password * 」フィールドに入力します。
4. [* Continue （続行）] をクリックします

> この手順で NetApp Element Plug-in for vCenter Server が登録されていると、エラーメッセージが表示されて要求されます "登録解除します" プラグイン。これは、 NetApp HCI の導入を続行する前に行ってください。導入完了後、プラグインが再登録されます。

詳細については、こちらをご覧ください

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

NetApp HCI クレデンシャルを設定する

導入時に、新しく導入する VMware vSphere 環境、 NetApp HCI のコンピューティングリソースとストレージリソース、および管理ノードで使用する一連のクレデンシャルを定義します。既存の vSphere 環境に NetApp HCI を導入する場合、既存の vCenter Server にこれらのクレデンシャルは適用されません。

このタスクについて

NetApp HCI Deployment Engine で設定するクレデンシャルについては、次の点に注意してください。

- * NetApp Hybrid Cloud Control （ HCC ）または Element UI * ：導入の成功時に NetApp HCC または Element ユーザインターフェイスにログインするには、この導入手順で指定したユーザ名とパスワードを使用します。
- **VMware vCenter**: vCenter にログインするには (展開の一部としてインストールされている場合) 、ユーザ名にサフィックス @vsphere. local またはビルトイン Administrator@vsphere.loca l のユーザアカウント、およびこの展開手順で指定されているパスワードを使用します。
- **VMware ESXi** ：コンピューティング・ノードで ESXi にログインするには ' ユーザー名 root と ' この導入手順で指定されているパスワードを使用します

VMware vCenter インスタンスと連携するために、 NetApp Hybrid Cloud Control では次のいずれかを使用します。

- 導入の一環としてインストールされた vCenter インスタンス上の組み込みの「 Administrator@vsphere.loca 」ユーザアカウント。
- 既存の VMware vCenter Server への NetApp HCI 環境の接続に使用した vCenter クレデンシャル。

手順

1. **[Credentials]** ページで、 **[*User Name]** フィールドにユーザ名を入力します。

2. [* パスワード *] フィールドにパスワードを入力します。パスワードは、「 * Password must contain * 」ボックスに表示されるパスワード基準に準拠している必要があります。
3. パスワードの再入力 * フィールドにパスワードを確認します。
4. [* Continue （続行）] をクリックします

詳細については、こちらをご覧ください

- "NetApp HCI でサポートされるファームウェアとESXiドライバのバージョン、NetApp HCI ストレージノードでサポートされるファームウェアのバージョンとファームウェアのバージョン"
- vCenter と ESXi のクレデンシャルをあとで更新する場合は、を参照してください "vCenter または ESXi のクレデンシャルを更新します"。

ネットワークトポロジを選択してください

NetApp HCI ノードのケーブル接続には、ニーズに応じて異なるネットワークケーブル構成を使用できます。コンピューティングノードについては、 6 つのすべてのネットワークポートを使用して各ポートペアに異なるタイプのトラフィックを割り当てることも、2 つのポートを使用してすべてのタイプのトラフィックをポートに割り当てることもできます。ストレージノードでは標準的なケーブル 4 本の構成を使用します。選択すると、インベントリでどのコンピューティングノードを選択できるかに影響します。

必要なもの

コンピューティングノードにケーブル 2 本のネットワークトポロジを使用する場合は、次の要件を考慮してください。

- 導入完了後に適用する VMware vSphere Enterprise Plus ライセンスが必要です。
- ネットワークとネットワークスイッチの構成が正しいことを確認しておきます。
- すべてのコンピューティングノードおよびストレージノードのストレージネットワークと vMotion ネットワークに VLAN タギングが必要です。

手順

1. Network Topology * ページで、 NetApp HCI 用のコンピューティングノードのインストール方法に適したコンピューティングノードトポロジを選択します。
   - *6 ケーブルオプション *: 6 ケーブルオプションでは、トラフィックの種類 (管理、仮想マシン、ストレージ) ごとに専用ポートを提供します。必要に応じて、 vSphere Distributed Switch （ VDS ）を有効にすることができます。VDS を有効にすると、分散スイッチが構成され、 NetApp HCI の導入完了後に仮想マシンのネットワーク構成を簡単かつ一元的に管理できるようになります。有効にした場合は、導入後に適用する vSphere Enterprise Plus ライセンスが必要です。
   - * 2 Cable Option * ：管理、仮想マシン、およびストレージのトラフィックを 2 つのボンディングポートに統合します。このケーブル接続オプションでは VDS は必須で、自動的に有効になります。導入後に適用する vSphere Enterprise Plus ライセンスが必要です。
2. 一部のケーブル配線オプションでは、ノードハードウェアのタイプ別に複数の背面パネル図が表示されます。背面パネル図を順に参照して、該当するノードモデルのネットワークケーブルとケーブル配線オプションを確認してください。
3. 完了したら、 [* Continue （続行）] をクリックします。

詳細については、こちらをご覧ください

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

在庫の選択

インベントリの選択とノードの互換性

導入するノードを選択する際、同じ環境で組み合わせ可能なノード構成にはいくつかの制限があります。

ストレージノードの互換性

NetApp HCI では、 SED （自己暗号化ドライブ）および FIPS 140-2 ドライブ暗号化機能を備えたストレージノードとドライブがサポートされます。NetApp HCI を導入または拡張する際 NetApp HCI には異なる暗号化レベルのノードを混在させることができますが、サポートされるのはより基本的な形式の暗号化のみです。たとえば、 FIPS 暗号化対応のストレージノードと SED 暗号化のみをサポートするノードが混在している場合、 SED 暗号化はサポートされますが、 FIPS ドライブ暗号化はサポートされません。

> FIPS ドライブ暗号化に対応したストレージノードをストレージクラスタに追加しても、 FIPS ドライブ暗号化機能は自動的には有効になりません。FIPS 対応ノードを含む環境を導入または拡張したら、 FIPS ドライブ暗号化を手動で有効にする必要があります。を参照してください "Element ソフトウェアのドキュメント" 手順については、を参照し

同じ導入環境で互換性を確保するためには、すべてのストレージノードが同じマイナーバージョンの Element ソフトウェアを実行している必要があります。たとえば、 Element 11.3.1 を実行しているストレージノードと Element 11.5 を実行しているストレージノードを混在させることはできません。

> ノードのハードウェア構成によっては、 H410S ストレージノードが、 H300S 、 H500S 、または H700S ストレージノードとしてインベントリリストに表示される場合があります。

NetApp HCI では、 2 ノードストレージクラスタでサポートされるストレージノードのモデルには制限があります。詳細については、を参照してください "2 ノードストレージクラスタ" または NetApp HCI バージョンの『リリースノート』を参照してください。

> 2 ノードのストレージクラスタ環境では、ストレージノードのタイプは 480GB と 960GB のドライブを搭載したノードに制限されます。

コンピューティングノードの互換性

コンピューティングノードをインベントリとして選択できるためには、ノードが次の要件を満たしている必要があります。

- VMware vMotion が適切に機能するように、すべてのコンピューティングノードの CPU 世代が一致している必要があります。インベントリからコンピューティングノードを 1 つ選択すると、そのノードとは CPU 世代が異なるノードは選択できなくなります。
- コンピューティングノードと GPU 対応のコンピューティングノードを同じコンピューティングクラスタ内に混在させることはできません。GPU 対応のコンピューティングノードを選択すると、 CPU のみのコ

ンピューティングノードは選択できなくなります。その逆も同様です。

- コンピューティングノードで実行されているソフトウェアのバージョンが、導入環境をホストしている NetApp Deployment Engine とメジャーおよびマイナーバージョンの両方で一致している必要があります。一致していない場合は、 RTFI プロセスを使用してコンピューティングノードを再イメージ化する必要があります。手順については、 RTFI に関するネットアップの技術情報アーティクルを参照してください。
- コンピューティングノードを「 * コンピューティングノード * 」リストで選択できるようにするには、ネットワークトポロジページで選択したケーブル構成がコンピューティングノードに含まれている必要があります。
- 同じモデルのコンピューティングノードのネットワークケーブル構成は、コンピューティングクラスタ内で同じである必要があります。

詳細については、こちらをご覧ください

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

インベントリを選択します

NetApp Deployment Engine は、「 * インベントリ」ページで利用可能なコンピューティングノードとストレージノードを自動的に検出し、すべての NetApp HCI リソースを選択して導入環境に追加できるようにします。導入の要件を満たしていないノードは選択できず、問題がエラーとして示されます。ノードの行のエラーにカーソルを合わせると、説明が表示されます。Inventory ページでノードインベントリを選択すると、NetApp Deployment Engine をホストしているストレージノードが自動的に選択され、選択を解除することはできません。

必要なもの

インベントリの検出が正しく機能するためには、ジャンボフレームを有効にする必要がありますインベントリにノードがまったく表示されない場合や、一部のノードしか表示されない場合は、 NetApp HCI ノードに使用されているスイッチポート（すべての SFP+ / SFP28 インターフェイス）にジャンボフレームが設定されていることを確認します。

手順

1. [* Inventory] ページで、使用可能なノードのリストを確認します。

   システムがインベントリを検出できない場合は、エラーが表示されます。エラーを修正してから続行してください。IP アドレスの割り当てに DHCP を使用するシステムの場合は、ストレージリソースとコンピューティングリソースがすぐにインベントリに表示されないことがあります。

2. オプション：リソースがすぐにインベントリに表示されない場合、またはエラーに対処してインベントリを更新する必要がある場合は、 [* インベントリの更新 *] をクリックします。インベントリを複数回更新しなければならない場合があります。
3. オプション：ノードタイプなどのノード属性でインベントリをフィルタリングするには、次の手順を実行します。
   a. [計算ノード *] または [ストレージノード *] リストのヘッダーで [* フィルタ *] をクリックします。
   b. ドロップダウンリストから条件を選択します。

c. ドロップダウンリストの下に、条件を満たす情報を入力します。

d. [フィルタを追加（ Add Filter ）] をクリックします

e. アクティブなフィルタの横にある **X** をクリックして個々のフィルタをクリアするか、フィルタのリストの上にある **X** をクリックしてすべてのフィルタをクリアします。

4. システムに付属しているすべてのコンピューティングノードを * コンピューティングノード * リストから選択します。

   導入を進めるには、少なくとも 2 つのコンピューティングノードを選択する必要があります。

5. システムに付属しているすべてのストレージノードを * ストレージノード * リストから選択します。

   導入を進めるには、少なくとも 2 つのストレージノードを選択する必要があります。

6. オプション：ストレージノードの選択ボックスにフラグが設定されている場合、そのストレージノードはストレージクラスタの総容量の 33% を超えています。次の手順を実行します。
   - フラグが設定されたストレージノードの選択ボックスをオフにします。
   - ストレージクラスタの容量がノード間でより均等に分散されるように、追加のストレージノードを選択します。
7. [* Continue （続行）] をクリックします

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

ネットワークの設定を行います

NetApp HCI には、ネットワーク設定を簡素化するためのセクションがいくつかあるネットワーク設定ページが用意されています。各セクションの手順に従って、各ネットワークのホストおよびノードの情報を入力するか、 IP アドレスを割り当てます。

必要なもの

- 次の情報を入手しておきます。
  - ホストとストレージクラスタの命名に使用するプレフィックス
  - 管理ネットワーク、 iSCSI ネットワーク、および vMotion ネットワークで使用するサブネットマスク、開始 IP アドレス、デフォルトゲートウェイ、および VLAN ID
  - 導入する VMware vCenter 環境のサブネットマスク、 IP アドレス、デフォルトゲートウェイ、および VLAN ID
  - NetApp HCI のネットワークタイムプロトコル（ NTP ）サーバアドレス
  - NetApp HCI の DNS サーバの IP アドレス情報
- vSphere Distributed Switch を導入する場合は、導入完了後に適用する vSphere Enterprise Plus ライセンスを準備しておきます。

- ターミナルユーザインターフェイス（ TUI ）設定時にノードポートに VLAN ID を割り当てた場合は、ネットワーク設定時に同じ VLAN ID でそれらのポートを設定する必要があります。接続されたスイッチポートで、タグ付きホストポートをアクセスポートまたはネイティブ VLAN として設定する必要はありません。
- ネットワークスイッチの構成が正しいことを確認しておきます。スイッチの設定（ VLAN や MTU サイズなど）に誤りがあると、導入エラーが発生する可能性があります。

このタスクについて

コンピューティングノードにケーブル 2 本のネットワークトポロジを使用する場合は、導入するすべてのコンピューティングノードおよびストレージノードの vMotion ネットワークとストレージネットワークに VLAN ID を使用する必要があります（管理ネットワークの VLAN ID は任意です）。これらの手順で入力した IP アドレスは NetApp HCI で検証されますが、 * ライブネットワーク検証は * ボタンで無効にできます。また、 NetApp HCI は、サブネットが重複しないようにする、複数のネットワークに VLAN ID が割り当てられていないこと、その他の基本的な検証など、この手順で入力したその他の情報についてもチェックを実行します。

> 導入前にホスト側で VLAN タギングが必要な環境で、 NetApp Deployment Engine でノードが検出されるようにコンピューティングノードとストレージノードに VLAN ID を設定した場合は、 NetApp Deployment Engine でネットワークを設定する際に正しい VLAN を使用するようにしてください。

2 ノードまたは 3 ノードのストレージクラスタを導入する場合は、監視ノードの IP アドレス情報を「 * ネットワーク設定 * 」ページで記入できます。

> IP アドレス割り当てページでは、 IP アドレスの自動割り当て * モードで入力した情報は、手動で IP アドレスを割り当てる * モードで入力した情報には影響しません。また、 IP アドレスの自動割り当て * モードで入力した情報にも影響しません。両方のモードで IP アドレスを入力すると、ページの下部にある [* Continue * （続行）] をクリックしたときに、 NetApp HCI はどのモードでも IP アドレス情報を使用します。

一般的な問題のトラブルシューティング

NetApp HCI は、これらのページに入力した情報をチェックします。一般的な問題とその回避策を次に示します。

問題	回避策
自動 IP アドレス割り当てモードでは、開始 IP アドレスを入力すると、「 IPs in the range are in use ：」というメッセージが表示されます。このメッセージには、使用中の IP アドレスがスクロール可能なドロップダウンリストが表示されます。	NetApp HCI には連続する IP アドレス範囲が割り当てられていますが、これらの IP アドレスのいくつかはすでに使用されています。使用中の IP アドレスを解放して再試行するか、手動 IP アドレス割り当てモードを使用して特定の IP アドレスを割り当てます。

問題	回避策
デフォルトゲートウェイを入力すると、「 The gateway is not valid」 というメッセージが表示されます。	デフォルトゲートウェイの IP アドレスが指定したサブネットと一致していないか、解決が必要なネットワークまたはサーバを含む問題があります。詳細については、次のネットアップナレッジベースの記事を参照してください。 • "NetApp Deployment Engine で無効なゲートウェイのトラブルシューティングを行います" • "ゲートウェイが NetApp Deployment Engine で無効です"
いくつかの * ネットワーク設定 * 設定ページを完了し、前のページのいずれかに間違った情報があることを認識している。	ページ上部の番号付きページシーケンスを使用して、以前に完了したページを選択し、そのページの情報を変更できます。完了したら、完了したページで [* Continue （続行）] をクリックして現在のページに戻ることができます。

DNS と NTP を設定

手順

1. [DNS / NTP] ページで、 NetApp HCI の DNS サーバおよび NTP サーバの情報を次のフィールドに入力します。

フィールド	説明
* DNS サーバー IP アドレス 1 *	NetApp HCI のプライマリ DNS サーバの IP アドレスです。vCenter の設定ページで DNS サーバを指定した場合は、このフィールドが設定され、読み取り専用になります。
* DNS サーバー IP アドレス 2 （オプション） *	NetApp HCI のセカンダリ DNS サーバのオプションの IP アドレスです。
* NTP サーバーアドレス 1 *	このインフラのプライマリ NTP サーバの IP アドレスまたは完全修飾ドメイン名です。
* NTP サーバアドレス 2 （オプション） *	このインフラのセカンダリ NTP サーバのオプションの IP アドレスまたは完全修飾ドメイン名です。

VLAN ID を割り当てます

[VLAN ID*] ページでは、 NetApp HCI ネットワークに VLAN ID を割り当てることができます。VLAN ID を使用しないように選択することもできます。コンピューティングノードにケーブル 2 本のネットワークトポロジを使用する場合は、導入するすべてのコンピューティングノードおよびストレージノードの vMotion ネットワークとストレージネットワークに VLAN ID を使用する必要があります（管理ネットワークの VLAN ID は任意です）。

> VLAN ID を割り当てる場合は、 NetApp HCI がネットワークトラフィックに適用する VLAN タグを設定します。ネイティブ VLAN を VLAN ID として入力する必要はありません。ネットワークにネイティブ VLAN を使用する場合は、該当するフィールドを空のままにしておきます。

手順

次のいずれかのオプションを選択します。

オプション	手順
VLAN ID を割り当てます	1. [* VLAN ID*] オプションには、 [* Yes*] を選択します。 2. [* VLAN ID*] 列に、 VLAN に割り当てるネットワークトラフィックのタイプごとに使用する VLAN タグを入力します。 コンピューティング vMotion トラフィックと iSCSI トラフィックはどちらも、共有されていない VLAN ID を使用する必要があります。 3. [* Continue （続行）] をクリックします
VLAN ID を割り当てないでください	1. [VLAN ID*] オプションに [**No**] を選択します。 2. [* Continue （続行）] をクリックします

管理ネットワークを設定

[* Management*] ページでは、開始 IP アドレスに基づいて NetApp HCI が管理ネットワークの IP アドレス範囲を自動的に設定するか、すべての IP アドレス情報を手動で入力するかを選択できます。

手順

次のいずれかのオプションを選択します。

オプション	手順
IP アドレスを自動的に割り当てます	1. [IP アドレスを自動的に割り当てる *] オプションを選択します。 2. [* Subnet*] 列に、各 VLAN の CIDR 形式でサブネット定義を入力します。 3. **Default Gateway** カラムに、各 VLAN のデフォルトゲートウェイを入力します。 4. [* Subnet*] 列に、 VLAN およびノードタイプごとに使用する開始 IP アドレスを入力します。 NetApp HCI では、ホストまたはホストグループごとに終了 IP アドレスが自動的に入力されます。 5. [* Continue （続行）] をクリックします

オプション	手順
IP アドレスを手動で割り当てます	1. [* IP アドレスを手動で割り当てる *] オプションを選択します。 2. [* Subnet*] 列に、各 VLAN の CIDR 形式でサブネット定義を入力します。 3. **Default Gateway** カラムに、各 VLAN のデフォルトゲートウェイを入力します。 4. 各ホストまたはノードの行に、そのホストまたはノードの IP アドレスを入力します。 5. 管理ネットワークの管理仮想 IP （ MVIP ）アドレスを入力します。 6. [* Continue （続行）] をクリックします

vMotion ネットワークを設定します

[*vMotion *] ページでは、開始 IP アドレスに基づいて NetApp HCI が自動的に vMotion ネットワークの IP アドレス範囲を入力するか、またはすべての IP アドレス情報を手動で入力するかを選択できます。

手順

次のいずれかのオプションを選択します。

オプション	手順
IP アドレスを自動的に割り当てます	1. [IP アドレスを自動的に割り当てる *] オプションを選択します。 2. [* Subnet*] 列に、各 VLAN の CIDR 形式でサブネット定義を入力します。 3. （任意） **Default Gateway** カラムに、各 VLAN のデフォルトゲートウェイを入力します。 4. [* Subnet*] 列に、 VLAN およびノードタイプごとに使用する開始 IP アドレスを入力します。 NetApp HCI では、ホストまたはホストグループごとに終了 IP アドレスが自動的に入力されます。 5. [* Continue （続行）] をクリックします

オプション	手順
IP アドレスを手動で割り当てます	1. [* IP アドレスを手動で割り当てる *] オプションを選択します。 2. [* Subnet*] 列に、各 VLAN の CIDR 形式でサブネット定義を入力します。 3. （任意） **Default Gateway** カラムに、各 VLAN のデフォルトゲートウェイを入力します。 4. 各ホストまたはノードの行に、そのホストまたはノードの IP アドレスを入力します。 5. [* Continue （続行）] をクリックします

iSCSI ネットワークを設定

[**iSCSI**] ページでは、 NetApp HCI が開始 IP アドレスに基づいて iSCSI ネットワークの IP アドレス範囲を自動的に入力するように選択することも、すべての IP アドレス情報を手動で入力することもできます。

手順

次のいずれかのオプションを選択します。

オプション	手順
IP アドレスを自動的に割り当てます	1. [IP アドレスを自動的に割り当てる *] オプションを選択します。 2. サブネット * 列に、 iSCSI ネットワーク用の CIDR 形式のサブネット定義を入力します。 3. （オプション） * Default Gateway * 列に、 iSCSI ネットワークのデフォルトゲートウェイを入力します。 4. [* Subnet*] 列に、各ノードタイプに使用する開始 IP アドレスを入力します。 NetApp HCI では、ホストまたはホストグループごとに終了 IP アドレスが自動的に入力されます。 5. [* Continue （続行）] をクリックします

オプション	手順
IP アドレスを手動で割り当てます	1. [* IP アドレスを手動で割り当てる *] オプションを選択します。 2. サブネット * 列に、 iSCSI ネットワーク用の CIDR 形式のサブネット定義を入力します。 3. （オプション） * Default Gateway * 列に、 iSCSI ネットワークのデフォルトゲートウェイを入力します。 4. 管理ノード * セクションに、管理ノードの IP アドレスを入力します。 5. ノードごとに、「 * コンピューティングノード * 」セクションに iSCSI A と iSCSI B の IP アドレスを入力します。 6. * Storage Virtual IP （ SVIP ） * の行に、 iSCSI ネットワークの SVIP IP アドレスを入力します。 7. 残りの行の各ホストまたはノードについて、そのホストまたはノードの IP アドレスを入力します。 8. [* Continue （続行）] をクリックします

クラスタ名とホスト名を割り当て

ネーミング * ページでは、 NetApp HCI によってクラスタ名およびクラスタ内のノード名が命名プレフィックスに基づいて自動的に入力されるようにするか、またはクラスタとノードのすべての名前を手動で入力するように選択できます。

手順

次のいずれかのオプションを選択します。

オプション	手順
クラスタ名とホスト名を自動的に割り当てます	1. クラスタ / ホスト名を自動的に割り当てる * オプションを選択します。 2. 「 * インストールプレフィックス * 」セクションで、クラスタ内のすべてのノードホスト名（管理ノードと監視ノードを含む）に使用する命名プレフィックスを入力します。 NetApp HCI では、ノードのタイプに基づいてホスト名が自動的に入力されます。また、一般的なノード名に対応するサフィックス（コンピューティングノードとストレージノードなど）も自動的に入力されます。 3. （任意） [**Naming Scheme**] カラムで、ホストの名前を変更します。 4. [* Continue （続行）] をクリックします
クラスタ名とホスト名を手動で割り当てます	1. クラスタ / ホスト名を手動で割り当てる * オプションを選択します。 2. [* ホスト / クラスタ名 *] 列に、各ホストのホスト名とストレージクラスタのクラスタ名を入力します。 3. [* Continue （続行）] をクリックします

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

構成を確認し、導入します

導入を開始する前に、指定した情報を確認できます。続行する前に、誤った情報や不完全な情報を修正することもできます。

> 導入時、管理ノードのインストールプロセスでは、 Element ストレージクラスタに「 NetApp-HCI - 」で始まる名前のボリュームが作成されます。また、「 tenant_ 」で始まる名前の SolidFire アカウントも作成されます。これらのボリュームやアカウントは削除しないでください。削除すると、管理機能が失われます。

手順

1. オプション：インストール情報を CSV 形式でダウンロードするには、「 * Download * 」アイコンを選択します。このファイルを保存し、あとで設定情報として参照できます。

> CSV ファイルをインストールプロファイルとして NetApp Deployment Engine （ NDE ）の「 * Installation Profile * 」ページにインポートできます。これは、将来のインストールで必要になった場合にのみ可能です。

2. 各セクションを展開し、情報を確認します。すべてのセクションを一度に展開するには、 * すべて展開 * を選択します。
3. オプション：表示されているセクションの情報を変更するには、次の手順を実行します。
   a. 対応するセクションで * Edit * を選択します。
   b. 必要な変更を行います。
   c. [* Review * （レビュー）] ページが表示されるまで、 [* Continue （続行）] を選択します。以前の設定は各ページに保存されます。
   d. 手順 2 と 3 を繰り返して、必要なその他の変更を行います。
4. ネットアップがホストしている SolidFire Active IQ サーバにクラスタの統計情報とサポート情報を送信しないようにする場合は、最後のチェックボックスをオフにします。

   これにより、 NetApp HCI のリアルタイムの健常性診断の監視機能が無効になります。この機能を無効にすると、ネットアップによる NetApp HCI のプロアクティブなサポートと監視が行われなくなるため、本番環境が影響を受ける前に問題を検出して解決できなくなります。

5. すべての情報が正しい場合は、「 * 導入の開始 * 」を選択します。

   ダイアログボックスが表示されます。最終セットアッププロセスでネットワーク接続に問題が発生したり、電源が切断されたりした場合、またはブラウザセッションが切断された場合は、ダイアログに表示された URL をコピーして、最後のセットアップの進捗ページを参照できます。

6. ダイアログ内の情報を確認し、 ［ * クリップボードにコピー * ］ を選択して URL をクリップボードにコピーします。
7. URL をコンピュータ上のテキストファイルに保存します。
8. 展開を続行する準備ができたら、 * OK * を選択します。

   導入が開始され、進捗状況ページが表示されます。導入が完了するまでは、ブラウザウィンドウを閉じたり進捗状況ページから移動したりしないでください。何らかの理由でブラウザセッションが切断された場合は、前の手順でコピーした URL を参照して（および表示されるセキュリティ警告を受け入れて）、最後のセットアップの進捗状況ページへのアクセスを再確立できます。

   > 導入に失敗した場合は、エラーメッセージのテキストを保存してネットアップサポートにお問い合わせください。

   導入が完了すると、コンピューティングノードが複数回リブートしてからサービスを開始できるようになることがあります。

完了後

「 vSphere の起動」を選択して、 NetApp HCI の使用を開始します。

- vSphere 6.7 を使用する NetApp HCI 環境では、このリンクをクリックすると、 HTML5 vSphere Web インターフェイスが起動します。vSphere 6.5 を使用する環境では、このリンクをクリックすると Adobe Flash vSphere Web インターフェイスが起動します。
- ストレージノードを 2 つ構成または 3 つ構成する場合、コンピューティングノード上のローカルデータストアを使用するように監視ノードが設定されます。その結果、 vSphere Client に「 Datastore usage on disk * 」という警告が 2 つ表示されます。続行するには、警告ごとに [緑にリセット] リンクを選択します。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"
- "SolidFire および Element ソフトウェアのドキュメント"

導入後のタスク

導入後のタスク

導入プロセスで選択した内容によっては、 NetApp HCI システムを本番環境で使用する前に、最終的なタスクをいくつか実行する必要があります。たとえば、ファームウェアやドライバの更新、必要な最終的な設定変更などです。

- "サポートされるネットワーク変更"
- "NetApp HCI コンピューティングノードで smartd サービスを無効にします"
- "設定済みのスイッチで「 lacp-individual 」コマンドを無効にします"
- "vCenter で NetApp HCC ロールを作成します"
- "VMware vSphere を最新の状態に維持"
- "GPU 対応のコンピューティングノード用の GPU ドライバをインストールします"
- "NetApp Hybrid Cloud Control にアクセスします"
- "NetApp HCI コンピューティングノードのブートメディアの摩耗度を低減します"

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"

サポートされるネットワーク変更

NetApp HCI を導入したあとは、デフォルトのネットワーク設定に限定的な変更を加えることができます。ただし、円滑な運用と適切なネットワーク検出のために必要な設定もあります。これらの設定を変更すると予期しない動作が発生し、コンピューティングリソースとストレージリソースを拡張できなくなる可能性があります。

システムの導入後、使用するネットワークの要件に応じて、 VMware vSphere のデフォルトのネットワーク構成を次の点で変更できます。

- vSwitch の名前を変更します
- ポートグループ名を変更します
- ポートグループを追加および削除します
- 追加のポートの vmnic インターフェイスのフェイルオーバー順序を変更します 追加したグループ

H300E 、 **H500E** 、 **H700E** 、 **H410C** の各コンピューティングノード

NetApp HCI は、 H300E 、 H500E 、 H700E 、 H410C の各ノードについて、次のネットワーク構成をサポートします。

VMware vSphere Distributed Switch （ VDS ）で 6 つのインターフェイスを使用する構成を次に示します。この構成は、 VMware vSphere Distributed Switch でのみサポートされ、 VMware vSphere Enterprise Plus ライセンスが必要です。

ネットワーク機能	**VMkernel**	**vmnic** （物理インターフェイス）
管理	vmk0	vmnic2 （ポート A ）、 vmnic3 （ポート B ）
iSCSI-A	vmk1	vmnic5 （ポート E ）
iSCSI-B	vmk2.	vmnic1 （ポート D ）
vMotion	vmk3.	vmnic4 （ポート C ）、 vmnic0 （ポート F ）

VMware vSphere Standard Switch （ VSS ）で 6 つのインターフェイスを使用する構成を次に示します。この構成では、 VMware vSphere Standard Switch （ VSS ）を使用します。

ネットワーク機能	**VMkernel**	**vmnic** （物理インターフェイス）
管理	vmk0	vmnic2 （ポート A ）、 vmnic3 （ポート B ）
iSCSI-A	vmk2.	vmnic1 （ポート E ）
iSCSI-B	vmk3.	vmnic5 （ポート D ）
vMotion	vmk1	vmnic4 （ポート C ）、 vmnic0 （ポート F ）

2 つのインターフェイスを使用する構成を次に示します。この構成は、 VMware vSphere Distributed Switch （ VDS ）でのみサポートされ、 VMware vSphere Enterprise Plus ライセンスが必要です。

ネットワーク機能	**VMkernel**	**vmnic** （物理インターフェイス）
管理	vmk0	vmnic1 （ポート D ）、 vmnic5 （ポート E ）
iSCSI-A	vmk1	vmnic1 （ポート E ）
iSCSI-B	vmk2.	vmnic5 （ポート D ）

ネットワーク機能	**VMkernel**	**vmnic** （物理インターフェイス）
vMotion	vmk3.	vmnic1 （ポート C ）、 vmnic5 （ポート F ）

H610C コンピューティングノード

NetApp HCI は、 H610C ノードについて次のネットワーク構成をサポートします。

この構成は、 VMware vSphere Distributed Switch （ VDS ）でのみサポートされ、 VMware vSphere Enterprise Plus ライセンスが必要です。

H610C ではポート A とポート B は使用されません。

ネットワーク機能	**VMkernel**	**vmnic** （物理インターフェイス）
管理	vmk0	vmnic2 （ポート C ）、 vmnic3 （ポート D ）
iSCSI-A	vmk1	vmnic3 （ポート D ）
iSCSI-B	vmk2.	vmnic2 （ポート C ）
vMotion	vmk3.	vmnic2 （ポート C ）、 vmnic3 （ポート D ）

H615C コンピューティングノード

NetApp HCI は H615C ノードのネットワーク構成を以下に示します。

この構成は、 VMware vSphere Distributed Switch （ VDS ）でのみサポートされ、 VMware vSphere Enterprise Plus ライセンスが必要です。

ネットワーク機能	**VMkernel**	**vmnic** （物理インターフェイス）
管理	vmk0	vmnic0 （ポート A ）、 vmnic1 （ポート B ）
iSCSI-A	vmk1	vmnic0 （ポート B ）
iSCSI-B	vmk2.	vmnic1 （ポート A ）
vMotion	vmk3.	vmnic0 （ポート A ）、 vmnic1 （ポート B ）

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

NetApp HCI コンピューティングノードで smartd サービスを無効にします

デフォルトでは 'martd' サービスは ' コンピューティング・ノード内のドライブを定期的にポーリングしますNetApp HCI を導入したあとに、すべてのコンピューティングノードでこのサービスを無効にする必要があります。

手順

1. SSH またはローカルコンソールセッションを使用して、コンピューティングノード上の VMware ESXi に root クレデンシャルを使用してログインします。
2. ランニングの「 martd 」サービスを停止します。

```
/etc/init.d/smartd stop
```

3. 起動時に 'martd' サービスが開始されないようにします

```
chkconfig smartd off
```

4. 環境内の残りのコンピューティングノードについて、上記の手順を繰り返します。

詳細については、こちらをご覧ください

- "VMware ESXi でスマートサービスをオフにします"
- "VMware の技術情報アーティクル 2133286"

設定済みのスイッチで「 lacp-individual 」コマンドを無効にします

デフォルトでは、 Mellanox スイッチ 'lacp-individual' コマンドと Cisco スイッチ 'LACP suspend-individual' コマンドは導入後も設定されたままになりますこのコマンドはインストール後には必要ありません。設定を維持すると、スイッチのトラブルシューティングまたはリブート時に原因ボリュームにアクセスできなくなる可能性があります。導入後は ' 各 Mellanox スイッチと Cisco スイッチの構成を確認し 'lacp-individual' または LACP suspend-individual コマンドを削除する必要があります

手順

1. SSH を使用して、スイッチへのセッションを開きます。
2. 実行コンフィギュレーションを表示します。

   'how running-config'

3. 「 lacp-individual 」コマンドまたは「 lacp suspend-individual 」コマンドのスイッチ設定出力を確認します。

「 xxx-xxx 」は、ユーザが指定したインターフェイス番号です。必要に応じて、 Multi-chassis Link Aggregation Group インターフェイス「 show MLAG interfaces 」を表示して、インターフェイス番号にアクセスできます

a. Mellanox スイッチの場合は、出力に次の行が含まれているかを確認します。

   'interface MLAG -port - channel xxx-xxx lacp-individual enable force

b. Cisco スイッチの場合は、出力に次の行が含まれているかどうかを確認します。

   インターフェイス MLAG ポートチャネル xxx-xxx lacp suspend-individual enable force

4. コマンドが存在する場合は、そのコマンドをコンフィギュレーションから削除します。
   a. Mellanox スイッチの場合：

      no interface MLAG-PORe-channel xxx-xxx lacp-individual enable force

   b. シスコ製スイッチの場合： no interface MLAG-PORe-channel xxx-xxx lacp suspend-individual enable force
5. 構成内のスイッチごとに上記の手順を繰り返します。

詳細については、こちらをご覧ください

- "トラブルシューティング中にストレージノードが停止する"

vCenter で NetApp HCC ロールを作成します

vCenterでNetApp HCCロールを作成して、インストール後にvCenterアセット（コントローラ）またはコンピューティングノード（ノード）を管理ノードに手動で追加したり、既存のコントローラやノードを変更したりする必要があります。

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

このタスクについて

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

新しい **NetApp HCC** ロールを作成します

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

vCenter で新しいユーザアカウントを設定します

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

手順

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

vCenter で新しい **NetApp HCC** ロールを作成します

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

手順

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

vCenter にユーザ権限を割り当てます

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

手順

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

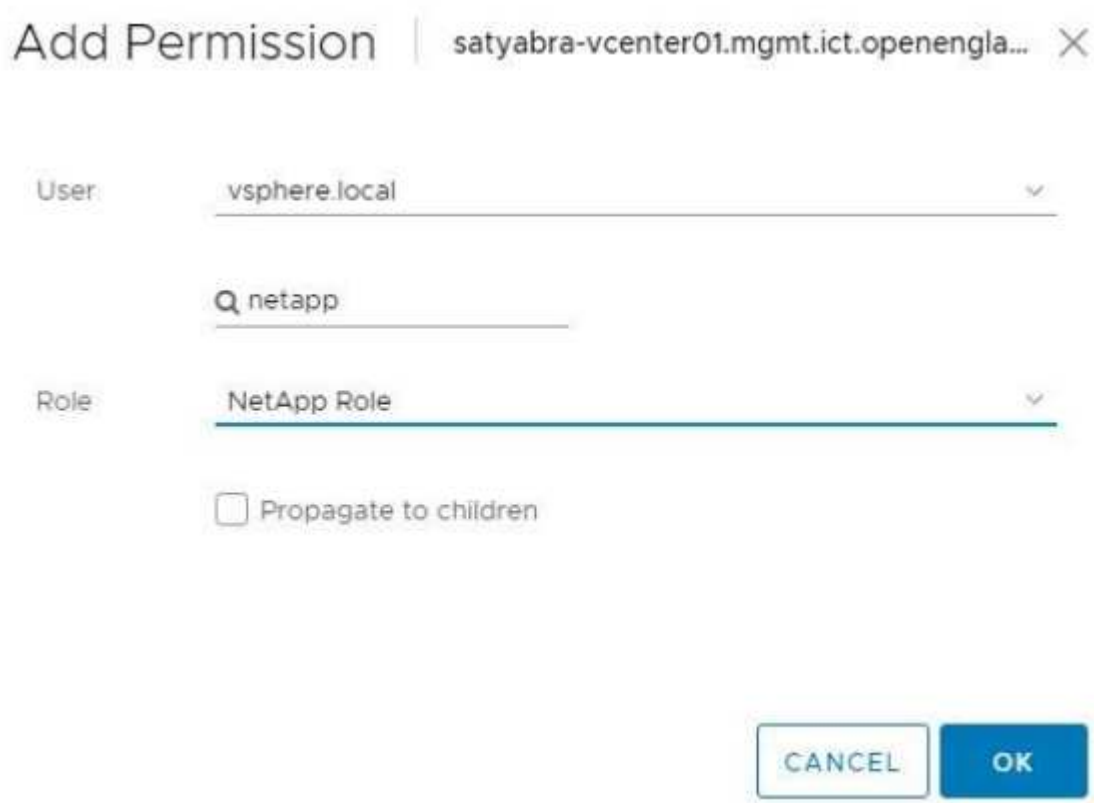
- NetApp Element Plug-in for vCenter Server 5.0以降では、を使用します "vCenter リンクモード"NetApp SolidFire ストレージクラスタを管理するvCenter Serverごとに、Element Plug-inを別々の管理ノードから登録します（推奨）。
- NetApp Element Plug-in for vCenter Server 4.10以前を使用して、他のvCenter Serverのクラスタリソースを管理する "vCenter リンクモード" はローカルストレージクラスタのみに制限されます。

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

   [権限の追加 *] ウィンドウに次の詳細を追加します。

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

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



データセンターにユーザ権限を割り当てます

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

手順

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

   [権限の追加 *] ウィンドウに次の詳細を追加します。

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

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

NetApp HCI データストアにユーザ権限を割り当てます

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

手順

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

   [権限の追加 *] ウィンドウに次の詳細を追加します。

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

ネットアップホストクラスタにユーザ権限を割り当てます

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

手順

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

[権限の追加 *] ウィンドウに次の詳細を追加します。

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

NetApp ESXi ホスト構成

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

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

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

手順

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

   [権限の追加 *] ウィンドウに次の詳細を追加します。

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

NetApp ESXi ホストが vCenter ホストクラスタに存在する

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

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

   [権限の追加 *] ウィンドウに次の詳細を追加します。

   a. 「 vSphered.local 」または LDAP ドメインを選択します。

b. 検索を使用して、で作成した新しいユーザを検索します vCenter で新しいユーザアカウントを設定します。

c. ［ NetApp Role ］ を選択します。

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

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

   [権限の追加 *] ウィンドウに次の詳細を追加します。

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

管理ノードにはすでにコントローラアセットが存在します

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

手順

1. 管理ノードの mNode サービス API UI にアクセスします。

   https://<ManagementNodeIP>/mnode`

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

管理ノードにアセットまたはコンピューティングノードを追加します

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

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"

VMware vSphere を最新の状態に維持

NetApp HCI を導入したら、 VMware vSphere Lifecycle Manager を使用して、 NetApp HCI で使用されている VMware vSphere バージョンの最新のセキュリティパッチを適用する必要があります。

を使用します "Interoperability Matrix Tool で確認してください" すべてのバージョンのソフトウェアに互換性があることを確認します。を参照してください "VMware vSphere Lifecycle Manager のドキュメント" を参照してください。

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

GPU 対応のコンピューティングノード用の GPU ドライバをインストールします

H610C などの NVIDIA グラフィックス処理ユニット（ GPU ）を搭載したコンピューティングノードでは、 NVIDIA ソフトウェアドライバを VMware ESXi にインストールして、強化された処理能力を活用できるようにする必要があります。GPU を搭載したコンピューティングノードを導入したら、 GPU 対応の各コンピューティングノードで以下の手順を実行して、 GPU ドライバを ESXi にインストールする必要があります。

手順

1. ブラウザを開き、次の URL から NVIDIA ライセンスポータルにアクセスします。

```
https://nvid.nvidia.com/dashboard/
```

2. ご使用の環境に応じて、次のいずれかのドライバパッケージをコンピュータにダウンロードします。

vSphere のバージョン	ドライバパッケージ
vSphere 6.5 の場合	「 nvidia -grid-vsphere-6.5-410.92-410.91 -412.16.zip 」という形式のファイルがあります
vSphere 6.7	「 nvidia -grid-vsphere-6.7-410.92-410.91 -412.16.zip」 と入力します

3. ドライバパッケージをコンピュータに展開します。

   圧縮されていないドライバファイル .VIB ファイルが展開されます。

4. コンピューターからコンピュート・ノード上で実行されている ESXi に、 `.VIB ’ドライバー・ファイルをコピーします。バージョンごとの次のコマンド例では、ドライバが管理ホストの「 $HOME/nvidia / ESX6.x/ 」ディレクトリにあることを前提としています。SCP ユーティリティはほとんどの Linux ディストリビューションに搭載されています。または、 Windows のすべてのバージョンに対応したユーティリティとしてダウンロードすることもできます。

ESXi のバージョン	説明
ESXi 6.5 の場合	'cp $HOME/nvidia / ESX6.5/nvidia **.vib root@<ESX_IP_addr>:/
ESXi 6.7	'cp $HOME/nvidia / ESX6.5/nvidia **.vib root@<ESX_IP_addr>:/

5. 次の手順に従って、 root として ESXi ホストにログインし、 NVIDIA vGPU Manager を ESXi にインストールします。
   a. 次のコマンドを実行して、 root ユーザとして ESXi ホストにログインします。

   ```
   ssh root@<ESXi_IP_ADDRESS>
   ```

   b. 次のコマンドを実行して、 NVIDIA GPU ドライバが現在インストールされていないことを確認します。

   ```
   nvidia-smi
   ```

   このコマンドは 'nvidia-smi: not found' というメッセージを返す必要があります

   c. 次のコマンドを実行して、ホストのメンテナンスモードを有効にし、 VIB ファイルから NVIDIA vGPU Manager をインストールします。

   ```
   esxcli system maintenanceMode set --enable true
   esxcli software vib install -v /NVIDIA**.vib
   ```

   「 Operation finished successfully 」というメッセージが表示されます。

   d. 次のコマンドを実行して、 8 つの GPU ドライバがすべてコマンド出力に表示されることを確認します。

   ```
   nvidia-smi
   ```

   e. 次のコマンドを実行して、 NVIDIA vGPU パッケージが正しくインストールされ、ロードされたことを確認します。

   ```
   vmkload_mod -l | grep nvidia
   ```

   コマンドは、「 nvidia 816 13808 」のような出力を返す必要があります

   f. 次のコマンドを実行してホストをリブートします。

```
reboot -f
```

g. 次のコマンドを実行してメンテナンスモードを終了します。

```
esxcli system maintenanceMode set --enable false
```

6. 新たに導入した NVIDIA GPU 搭載の残りのコンピューティングノードについて、手順 4~6 を繰り返します。
7. NVIDIA のドキュメントサイトに記載された手順に従って、次のタスクを実行します。
   a. NVIDIA ライセンスサーバをインストールします。
   b. NVIDIA vGPU ソフトウェア用に仮想マシンゲストを設定します。
   c. 仮想デスクトップインフラ（ VDI ）環境で vGPU 対応のデスクトップを使用している場合は、NVIDIA vGPU ソフトウェア用に VMware Horizon View を設定します。

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

NetApp Hybrid Cloud Control にアクセスします

NetApp Hybrid Cloud Control では NetApp HCI を管理できます。NetApp HCI の管理サービスやその他のコンポーネントをアップグレードして、インストール環境を拡張および監視できます。NetApp Hybrid Cloud Control にログインするには、管理ノードの IP アドレスにアクセスします。

必要なもの

- * クラスタ管理者権限 * ：ストレージクラスタに対する管理者権限があります。
- * 管理サービス * ：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 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。現在のサービスバンドルバージョンについては、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。例：

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

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

   NetApp Hybrid Cloud Control のインターフェイスが表示されます。

十分な権限を使用してログインしないと、 HCC のリソースページ全体で「ロードできません」というメッセージが表示され、リソースを使用できなくなります。

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

NetApp HCI コンピューティングノードのブートメディアの摩耗度を低減します

NetApp HCI コンピューティングノードでフラッシュメモリまたは NVDIMM ブートメディアを使用する場合、システムログをそのメディアに保存しておくと、そのメディアに頻繁に書き込まれます。これにより、最終的にフラッシュメモリが劣化する可能性があります。ホストロギングとコアダンプファイルを共有ストレージの場所に移動するには、次の技術情報アーティクルの手順に従います。これは、ブートメディアのパフォーマンスが低下しないようにし、ブートディスクのフルエラーを回避するのに役立ちます。

"のブートドライブの摩耗を低減する方法 NetApp HCI コンピューティングノード"

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 を管理します

NetApp HCI の管理の概要

NetApp HCI 、ユーザアカウント、ストレージクラスタ、ボリューム、ボリュームアクセスグループの完全修飾ドメイン名を設定し、クレデンシャルを管理できます。 イニシエータ、ボリュームの QoS ポリシー、および管理ノード。

使用できる項目は次のとおりです。

- "完全修飾ドメイン名 Web UI アクセスを設定します"
- "NetApp HCI でクレデンシャルを変更します"
- "vCenter および ESXi のクレデンシャルを更新します"
- "NetApp HCI ストレージアセットを管理します"
- "管理ノードを操作します"
- "NetApp HCI システムの電源をオフまたはオンにします"

詳細については、こちらをご覧ください

- "NetApp HCI のリソースページ"

完全修飾ドメイン名 Web UI アクセスを設定します

Element ソフトウェア 12.2 以降を搭載した NetApp HCI では、 Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を使用してストレージクラスタの Web インターフェイスにアクセスできます。FQDN を使用して、 Element Web UI 、ノード UI 、管理ノード UI などの Web ユーザインターフェイスにアクセスする場合は、クラスタで使用される FQDN を特定するストレージクラスタ設定を最初に追加する必要があります。

Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を使用してストレージクラスタの Web インターフェイスにアクセスできるようになりました。FQDN を使用して、 Element Web UI 、ノード UI 、管理ノード UI などの Web ユーザインターフェイスにアクセスする場合は、クラスタで使用される FQDN を特定するストレージクラスタ設定を最初に追加する必要があります。これにより、クラスタはログインセッションを適切にリダイレクトできるようになり、キー管理ツールやアイデンティティプロバイダなどの外部サービスとの統合が強化されて、多要素認証に対応できるようになります。

必要なもの

- この機能を使用するには、 Element 12.2 以降が必要です。
- NetApp Hybrid Cloud Control REST API を使用してこの機能を設定するには、管理サービス 2.15 以降が必要です。
- NetApp Hybrid Cloud Control の UI を使用してこの機能を設定するには、管理サービス 2.19 以降が必要です。
- REST API を使用するには、バージョン 11.5 以降を実行する管理ノードを導入しておく必要があります。

- 管理ノードおよび各ストレージクラスタの IP アドレスに正しく解決されるように、管理ノードと各ストレージクラスタの IP アドレスを完全修飾ドメイン名する必要があります。

NetApp Hybrid Cloud Control と REST API を使用して、 FQDN Web UI アクセスを設定または削除できます。正しく設定されていない FQDN をトラブルシューティングすることもできます。

- NetApp Hybrid Cloud Control を使用して、 FQDN Web UI アクセスを設定します
- REST API を使用して FQDN Web UI アクセスを設定します
- NetApp Hybrid Cloud Control を使用して、 FQDN Web UI アクセスを削除します
- REST API を使用して FQDN Web UI アクセスを削除します
- [トラブルシューティング]

NetApp Hybrid Cloud Control を使用して、 FQDN Web UI アクセスを設定します

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. ページの右上にあるメニューアイコンを選択します。
4. 「 * Configure * 」を選択します。
5. [完全修飾ドメイン名 *] ペインで、 [セットアップ *] を選択します。
6. 表示されたウィンドウで、管理ノードおよび各ストレージクラスタの FQDN を入力します。
7. [保存（ Save ）] を選択します。

   「 * Fully Qualified Domain Names * 」ペインには、各ストレージクラスタとその MVIP および FQDN が表示されます。

   FQDN が設定されている接続されたストレージクラスタのみが、「 * Fully Qualified Domain Names * 」ペインに表示されます。

REST API を使用して FQDN Web UI アクセスを設定します

手順

1. 環境で FQDN が解決されるように、 Element ストレージノードと管理ノードの DNS がネットワーク環境に対して正しく設定されていることを確認します。DNS を設定するには、ストレージノードのノード UI および管理ノードに移動し、 * Network Settings * > * Management Network * を選択します。
   a. ストレージ・ノードのノード単位の UI ： https://<storage_node_management_IP>:442`
   b. 管理ノード用のノード単位の UI ： https://<management_node_IP>:442`
2. Element API を使用してストレージクラスタの設定を変更します。

a. Element API にアクセスし、「 CreateClusterInterfacePreference 」 API メソッドを使用して次のクラスタインターフェイス設定を作成し、設定値としてクラスタ MVIP FQDN を挿入します。

   - 名前 :「 mvip 」
   - Value ： < クラスタ MVIP の完全修飾ドメイン名 >

     たとえば、 FQDN は「 toragecluster.my.org`: 」です

```
https://<Cluster_MVIP>/json-
rpc/12.2?method=CreateClusterInterfacePreference&name=mvip_fqdn&value=st
oragecluster.my.org
```

3. 管理ノードで REST API を使用して管理ノードの設定を変更します。

   a. 管理ノードの REST API UI にアクセスするには、管理ノードの IP アドレスに「 /mnode/2/」 を続けて入力します。例：

```
https://<management_node_IP>/mnode/2/
```

   b. 「 * Authorize * 」またはロックアイコンを選択し、 Element クラスタのユーザ名とパスワードを入力します。
   c. クライアント ID を「 m node-client 」として入力します。
   d. セッションを開始するには、 * Authorize * を選択します。
   e. ウィンドウを閉じます。
   f. 「 * GET / SETTINGS * 」を選択します。
   g. [* 試してみてください *] を選択します。
   h. [* Execute] を選択します。
   i. プロキシが 'Use_proxy' では 'true' または 'false' で示されているように使用されているかどうかに注意してください
   j. 「 * PUT / SETTINGS * 」を選択します。
   k. [* 試してみてください *] を選択します。
   l. 要求の本文領域で、管理ノードの FQDN を「 `m node_name 」パラメータの値として入力します。また 'use_proxy' パラメータにプロキシを使用するかどうかを指定します (前の手順の「 true 」または「 false 」)

```
{
  "mnode_fqdn": "mnode.my.org",
  "use_proxy": false
}
```

   m. [* Execute] を選択します。

NetApp Hybrid Cloud Control を使用して、 FQDN Web UI アクセスを削除します

この手順を使用して、管理ノードとストレージクラスタの FQDN Web アクセスを削除できます。

手順

1. [完全修飾ドメイン名 *] ペインで、 [編集 *] を選択します。
2. 表示されたウィンドウで、 **FQDN** テキストフィールドの内容を削除します。
3. [保存（ Save ）] を選択します。

   ウィンドウが閉じ、 [*Fully Qualified Domain Names] ペインに FQDN が表示されなくなります。

REST API を使用して FQDN Web UI アクセスを削除します

手順

1. Element API を使用してストレージクラスタの設定を変更します。

   a. Element API にアクセスし、「 D eleteClusterInterfacePreference 」 API メソッドを使用して次のクラスタインターフェイス設定を削除します。

      - 名前：「 mvip 」

        例：

```
https://<Cluster_MVIP>/json-
rpc/12.2?method=DeleteClusterInterfacePreference&name=mvip_fqdn
```

2. 管理ノードで REST API を使用して管理ノードの設定を変更します。

   a. 管理ノードの REST API UI にアクセスするには、管理ノードの IP アドレスに「 /mnode/2/」 を続けて入力します。例：

```
https://<management_node_IP>/mnode/2/
```

   b. 「 * Authorize * 」またはロックアイコンを選択し、 Element クラスタのユーザ名とパスワードを入力します。
   c. クライアント ID を「 m node-client 」として入力します。
   d. セッションを開始するには、 * Authorize * を選択します。
   e. ウィンドウを閉じます。
   f. 「 * PUT / SETTINGS * 」を選択します。
   g. [* 試してみてください *] を選択します。
   h. 要求の本文領域では、「 m node_fqdn 」パラメータに値を入力しないでください。また 'use_proxy' パラメータにプロキシを使用するかどうかを指定します ('true' または 'false')

```
{
  "mnode_fqdn": "",
  "use_proxy": false
}
```

i. [* Execute] を選択します。

トラブルシューティング

FQDN が正しく設定されていないと、管理ノード、ストレージクラスタ、またはその両方へのアクセスで問題が発生する可能性があります。問題のトラブルシューティングを行うには、次の情報を参照してください。

問題	原因	解決策：
• FQDN を使用して管理ノードまたはストレージクラスタにアクセスしようとするとブラウザエラーが表示されます。 • IP アドレスを使用して管理ノードまたはストレージクラスタにログインすることはできません。	管理ノードの FQDN とストレージクラスタ FQDN の両方が正しく設定されていません。	このページの REST API の手順を使用して、管理ノードとストレージクラスタの FQDN 設定を削除して設定し直します。
• ストレージクラスタ FQDN にアクセスしようとするとブラウザエラーが表示されます。 • IP アドレスを使用して管理ノードまたはストレージクラスタにログインすることはできません。	管理ノード FQDN が正しく設定されていますが、ストレージクラスタ FQDN が正しく設定されていません。	このページの REST API の手順を使用して、ストレージクラスタの FQDN 設定を削除して再度設定します。
• 管理ノード FQDN にアクセスしようとするとブラウザエラーが表示されます。 • IP アドレスを使用して管理ノードとストレージクラスタにログインできます。	管理ノード FQDN の設定に誤りがありますが、ストレージクラスタ FQDN が正しく設定されています。	NetApp Hybrid Cloud Control にログインして UI で管理ノードの FQDN 設定を修正するか、このページの REST API の手順を使用して設定を修正します。

詳細については、こちらをご覧ください

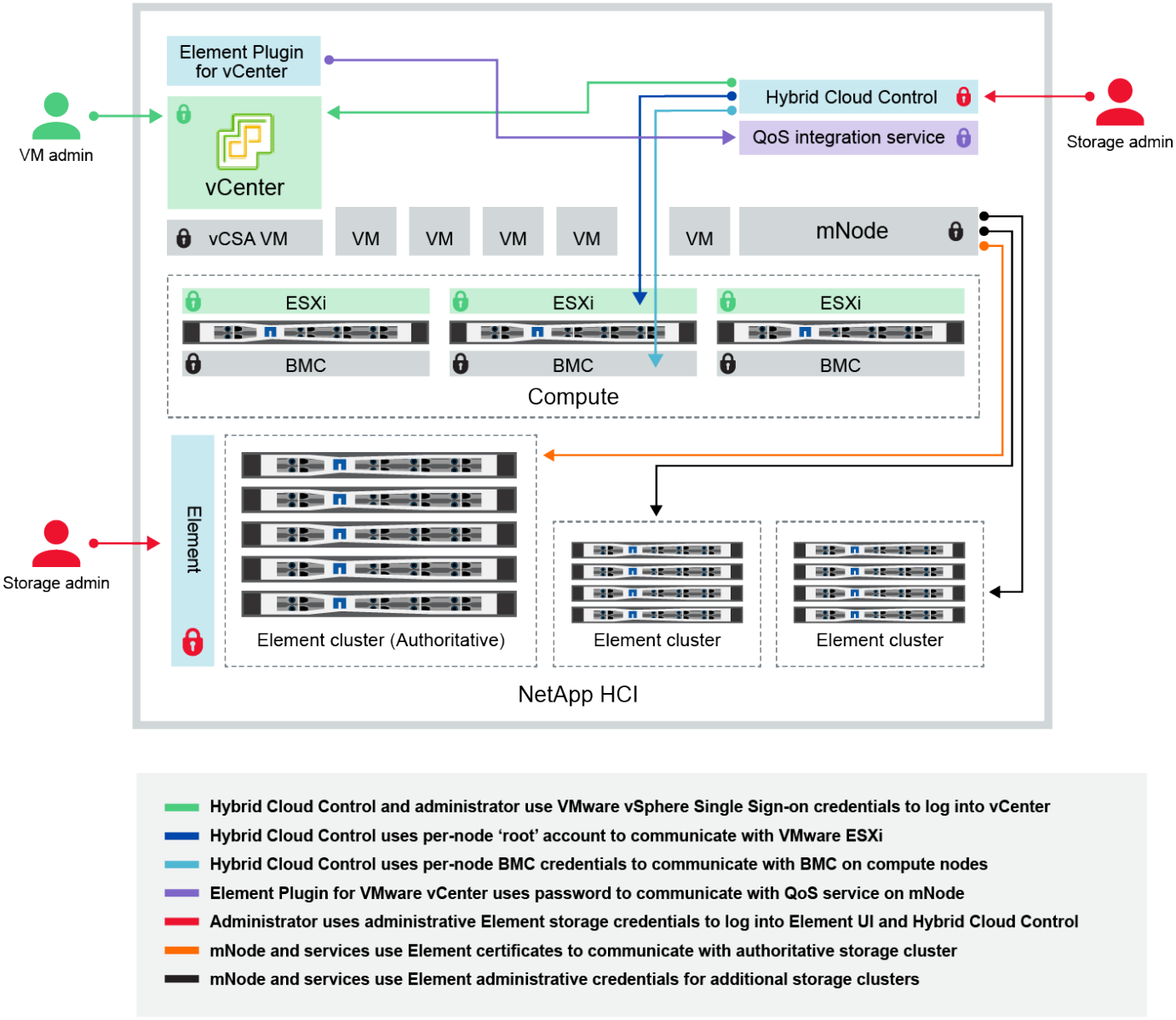
- "SolidFire および Element ドキュメントの CreateClusterInterfacePreference API 情報"
- "NetApp HCI のリソースページ"
- "SolidFire および Element ソフトウェアのドキュメント"

NetApp HCI と NetApp SolidFire でクレデンシャルを変更

NetApp HCI または NetApp SolidFire を導入している組織内のセキュリティポリシーに応じて、クレデンシャルやパスワードの変更はセキュリティの手法の一部として一般的に行われます。パスワードを変更する前に、導入環境内の他のソフトウェアコンポーネントへの影響を確認しておく必要があります。

NetApp HCI 環境または NetApp SolidFire 環境のいずれかのコンポーネントのクレデンシャルを変更する場合、次の表に示すガイダンスに従って他のコンポーネントに影響を与えます。

NetApp HCI コンポーネントの相互作用
：



資格情報の種類とアイコン	管理者による使用状況	これらの手順を参照してください
Element クレデンシャル	• 環境 * ： NetApp HCI および SolidFire 管理者は、次の資格情報を使用してログインします。 • Element ストレージクラスタの Element ユーザインターフェイス • 管理ノードでの Hybrid Cloud Control （ mNode ） Hybrid Cloud Control で複数のストレージクラスタを管理している場合は、ストレージクラスタの管理クレデンシャルのみを受け入れます。このクレデンシャルは、「 _authoritative cluster_that the mnode was initially set for 」と呼ばれます。ストレージクラスタがあとで Hybrid Cloud Control に追加された場合、 mnode は管理者クレデンシャルを安全に保存します。以降に追加したストレージクラスタのクレデンシャルが変更された場合は、 mnode API を使用して mNode でクレデンシャルを更新する必要があります。	• "ストレージクラスタの管理者パスワードを更新する"。 • を使用して、 mNode のストレージクラスタ管理者のクレデンシャルを更新します 。 "modifyclusteradmin API"。
vSphere Single Sign-On のクレデンシャル	• 環境 * ： NetApp HCI のみ 管理者は、このクレデンシャルを使用して VMware vSphere Client にログインします。vCenter が NetApp HCI のインストールに含まれている場合、 NetApp Deployment Engine でクレデンシャルが次のように設定されます。 • 指定したパスワード、およびを使用する username@vsphere.loca • 指定したパスワードを持つ administrator@vsphere.loca既存の vCenter を使用して NetApp HCI を導入する場合、vSphere のシングルサインオンクレデンシャルは IT VMware 管理者が管理します。	"vCenter および ESXi のクレデンシャルを更新します"。

資格情報の種類とアイコン	管理者による使用状況	これらの手順を参照してください
ベースボード管理コントローラ（BMC）のクレデンシャル	• 環境 * ： NetApp HCI のみ 管理者は、このクレデンシャルを使用して、 NetApp HCI 環境のネットアップコンピューティングノードの BMC にログインします。BMC は、基本的なハードウェア監視機能と仮想コンソール機能を備えています。 各ネットアップコンピューティングノードの BMC （ *ipmi* とも呼ばれる）クレデンシャルは、 NetApp HCI 環境の mNode に安全に保管されます。NetApp Hybrid Cloud Control は、サービスアカウント容量の BMC クレデンシャルを使用して、コンピューティングノードのファームウェアアップグレード中にコンピューティングノード内の BMC と通信します。 BMC のクレデンシャルが変更された場合、 mNode のすべての Hybrid Cloud Control 機能を維持するには、各コンピューティングノードのクレデンシャルも更新する必要があります。	• "NetApp HCI の各ノードに IPMI を設定します"。 • H410C 、 H610C 、および H615C ノードの場合、 "デフォルトの IPMI パスワードを変更します"。 • H410S および H610S ノードの場合、 "デフォルトの IPM パスワードを変更します"。 • "管理ノードで BMC クレデンシャルを変更します"。
ESXi クレデンシャル	• 環境 * ： NetApp HCI のみ 管理者は、 SSH またはローカル DCUI を使用して、ローカルの root アカウントで ESXi ホストにログインできます。NetApp HCI 環境では、ユーザ名は「 root 」で、パスワードは NetApp Deployment Engine でのコンピューティングノードの初回インストール時に指定されています。 ネットアップの各コンピューティングノードの ESXi ルートクレデンシャルが、 NetApp HCI 環境に mNode に安全に保存されている。NetApp Hybrid Cloud Control は、サービスアカウント容量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のファームウェアアップグレードや健全性チェックで ESXi ホストと直接通信します。 VMware 管理者が ESXi のルートクレデンシャルを変更した場合、各コンピューティングノードのクレデンシャルを mNode で更新し、ハイブリッドクラウド制御機能を維持する必要があります。	"vCenter および ESXi ホストのクレデンシャルを更新します"。

資格情報の種類とアイコン	管理者による使用状況	これらの手順を参照してください
QoS 統合パスワード	• 環境 * ： NetApp HCI および SolidFire ではオプション 管理者による対話型ログインには使用されません。 VMware vSphere と Element ソフトウェアの QoS 統合は、次の機能を通じて実現します。 • vCenter Server 向け Element プラグイン、および • mNode の QoS サービス。 認証の場合、 QoS サービスは、このコンテキストでのみ使用されるパスワードを使用します。QoS のパスワードは、 Element Plug-in for vCenter Server の初回インストール時に指定するか、NetApp HCI の導入時に自動生成されます。 他のコンポーネントには影響しません。	"NetApp Element Plug-in for vCenter で QoSSIOC クレデンシャルを更新します サーバ"。 NetApp Element Plug-in for vCenter ServerのSIOCパスワードは_QoSSIOCパスワードとも呼ばれます。 {url-peak} [Element Plug-in for vCenter Serverの技術情報アーティクル^]を確認します。
vCenter Service Appliance のクレデンシャル	• 環境 * ： NetApp HCI は、 NetApp Deployment Engine によってセットアップされている場合にのみ使用します 管理者は vCenter Server Appliance 仮想マシンにログインできます。NetApp HCI 環境では、ユーザ名は「 root 」で、パスワードは NetApp Deployment Engine でのコンピューティングノードの初回インストール時に指定されています。導入されている VMware vSphere のバージョンに応じて、 vSphere Single Sign-On ドメインの一部の管理者もアプライアンスにログインできます。 他のコンポーネントには影響しません。	変更は不要です。
NetApp 管理ノード管理者のクレデンシャル	• 環境 * ： NetApp HCI および SolidFire ではオプション 管理者はネットアップ管理ノード仮想マシンにログインして、高度な設定やトラブルシューティングを行うことができます。導入した管理ノードのバージョンに応じて、 SSH によるログインはデフォルトでは有効になりません。 NetApp HCI 環境では、 NetApp Deployment Engine でのコンピューティングノードの初回インストール時に、ユーザによってユーザ名とパスワードが指定されています。 他のコンポーネントには影響しません。	変更は不要です。

詳細については、こちらをご覧ください

- "Element ソフトウェアのデフォルトの SSL 証明書を変更"

- "ノードの IPMI パスワードを変更します"
- "多要素認証を有効にします"
- "外部キー管理の開始"
- "FIPS ドライブをサポートするクラスタを作成します"

vCenter および ESXi のクレデンシャルを更新します

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

このタスクについて

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

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

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

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

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

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

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

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

手順

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

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

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

3. [* Authorize * （認証）] または任意のロックアイコンをクリックして、次の手順を実行します。
   a. NetApp SolidFire クラスタの管理ユーザ名とパスワードを入力します。
   b. クライアント ID 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 * をクリックします。
   d. ウィンドウを閉じます。
4. REST API UI で、 * Get 操作対象のデバイス / アセット / コンピュートノード * をクリックします。

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

   UI からこの API に直接アクセスするには、次のリンクを使用します。

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

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

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

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

8. コンピューティングノードのアセットを設定します。
   a. PUT /assets/ ｛ asset_id ｝ /compute-nodes / ｛ compute_id ｝ * をクリックします。

      UI の API への直接リンクを次に示します。

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

a. [* 試してみてください *] をクリックします。

b. 「 parent 」情報を指定して「 asset_id 」を入力します。

c. "id" 情報を入力して、 "compute_id" を入力します。

d. ユーザインターフェイスの要求の本文を変更して、コンピューティングアセットレコードのパスワードとユーザ名のパラメータのみを更新します。

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

e. [* Execute] をクリックします。

f. 応答が HTTP 200 であることを確認します。 HTTP 200 は、参照先のコンピューティングアセットレコードに新しいクレデンシャルが格納されたことを示します

9. 新しいパスワードで更新する必要があるその他のコンピューティングノードアセットについて、前述の 2 つの手順を繰り返します。

10. に移動します https://<mNode_ip>/inventory/1/。

a. [* Authorize * （認証）] または任意のロックアイコンをクリックして、次の手順を実行します。

i. NetApp SolidFire クラスタの管理ユーザ名とパスワードを入力します。

ii. クライアント ID 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 * をクリックします。

iv. ウィンドウを閉じます。

b. REST API UI で、 * GET / Installations * をクリックします。

c. [* 試してみてください *] をクリックします。

d. [Refresh 概要（更新の設定）] ドロップダウンリストから [* True] を選択します。

e. [* Execute] をクリックします。

f. 応答が HTTP 200 であることを確認します。

11. vCenter のアカウントロックアウトメッセージが表示されなくなるまで約 15 分待ちます。

詳細については、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 ストレージを管理します

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

NetApp HCI では、 NetApp Hybrid Cloud Control を使用してこれらのストレージアセッ

トを管理できます。

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

詳細については、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"

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

Element ベースのストレージシステムでは、「管理者」または「読み取り専用」のユーザに付与する権限に応じて、権限のあるクラスタユーザを作成して NetApp Hybrid Cloud Control へのログインアクセスを有効にすることができます。クラスタユーザに加えてボリュームアカウントもあり、クライアントはこのアカウントを使用してストレージノード上のボリュームに接続できます。

次のタイプのアカウントを管理します。

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

LDAP を有効にします

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

手順

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

権限のあるクラスタアカウントを管理します

"権限のあるユーザアカウント" NetApp Hybrid Cloud Control の右上のメニューから User Management オプションを選択して管理します。このタイプのアカウントでは、ノードおよびクラスタの NetApp Hybrid Cloud Control インスタンスに関連付けられているストレージアセットに対して認証を行うことができます。このアカウントを使用すると、すべてのクラスタのボリューム、アカウント、アクセスグループなどを管理できます。

権限のあるクラスタアカウントを作成してください

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

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

手順

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

     LDAP を使用するには、最初に LDAP または LDAPS を有効にする必要があります。を参照してください LDAP を有効にします。

   - Auth Type として Cluster を選択した場合は、新しいアカウントの名前とパスワードを入力します。
6. 管理者権限または読み取り専用権限のいずれかを選択します。

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

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

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

権限のあるクラスタアカウントを編集してください

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

手順

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

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

4. テーブルの * アクション * 列で、アカウントのメニューを展開し、 * 編集 * を選択します。
5. 必要に応じて変更します。
6. [保存（ Save ）] を選択します。
7. NetApp Hybrid Cloud Control からログアウトします。
8. "クレデンシャルを更新します" NetApp Hybrid Cloud Control API を使用して、権限のあるクラスタアセットに対してアクセスします。

   NetApp Hybrid Cloud Control の UI でインベントリの更新に最大 2 分かかる場合があります。インベントリを手動で更新するには、 REST API UI インベントリサービス https://<ManagementNodeIP>/inventory/1/` にアクセスし、クラスタに対して「 get/installationses/{ id} 」を実行します。

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

権限のあるユーザアカウントを削除します

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

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

手順

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

ボリュームアカウントを管理する

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

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

ボリュームアカウントを作成します

このボリュームに固有のアカウントを作成します。

手順

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

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

7. 「 * アカウントの作成 * 」を選択します。

ボリュームアカウントを編集します

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

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

手順

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

ボリュームアカウントを削除します

不要になったアカウントを削除します。

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

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

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

手順

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

詳細については、こちらをご覧ください

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

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

ストレージクラスタを管理ノードアセットインベントリに追加すると、 NetApp Hybrid Cloud Control （ HCC ）を使用して管理できるようになります。システムセットアップ時に最初に追加されるストレージクラスタは、です デフォルト "信頼できるストレージクラスタです"を使用してクラスタを追加することもできます。

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

Element 12.2 以降では、を使用できます "メンテナンスモード" ストレージクラスタノードのメンテナンスモードを有効または無効にする機能オプション。

必要なもの

- * クラスタ管理者のアクセス許可 *: の管理者としてのアクセス許可があります "信頼できるストレージクラスタです"。信頼できるクラスタとは、システムのセットアップ時に管理ノードインベントリに最初に追加されるクラスタです。
- * Element ソフトウェア * ：ストレージクラスタで NetApp Element ソフトウェア 11.3 以降を実行している必要があります。
- * 管理ノード * ：バージョン 11.3 以降を実行する管理ノードを導入しておきます。

- * 管理サービス * ：管理サービスのバンドルをバージョン 2.17 以降に更新しました。

オプション（ **Options** ）

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

ストレージクラスタを追加

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

手順

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

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

   - ストレージクラスタのユーザ名とパスワード
6. 「 * 追加」を選択します。

   ストレージクラスタを追加したあとにクラスタのインベントリが更新されて新しい追加が表示されるまでに最大 2 分かかることがあります。変更を反映するには、ブラウザでページの更新が必要になる場合があります。

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

ストレージクラスタのステータスを確認

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

手順

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

2. ダッシュボードで右上のオプションメニューを選択し、 * 構成 * を選択します。
3. インベントリでのストレージクラスタのステータスを確認します。
4. Storage Clusters * ペインで、詳細を表示する * Storage Cluster Details * を選択します。

ストレージクラスタクレデンシャルを編集します

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

手順

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

ストレージクラスタを削除

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

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

手順

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

   > [はい] をクリックすると、クラスタがインストールから削除されます。

5. 「 * はい * 」を選択します。

メンテナンスモードを有効または無効にします

これ "メンテナンスモード" 機能オプションを使用すると、にアクセスできます -- 有効にします および - 無効にします ストレージクラスタノードの保守モード。

必要なもの

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

メンテナンスモードを有効にします

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

保守モードにできるノードは一度に 1 つだけです。

手順

1. Webブラウザで管理ノードのIPアドレスを開きます。例：

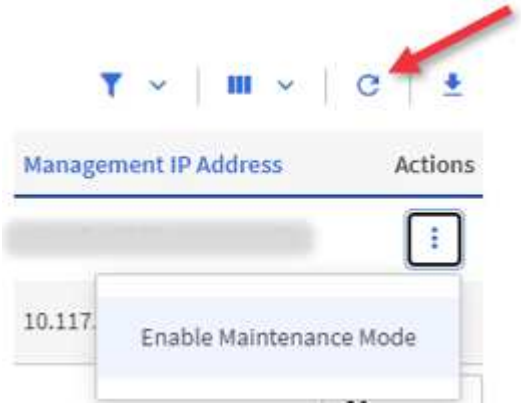
```
https://<ManagementNodeIP>
```

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

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

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

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



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

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

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

メンテナンスモードを無効にします

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

手順

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

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

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

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

トラブルシューティングを行う

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

詳細については、こちらをご覧ください

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

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

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

作成中に、ボリュームの QoS 設定を指定できます。

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

- [ボリュームを作成します]
- ボリュームに QoS ポリシーを適用します

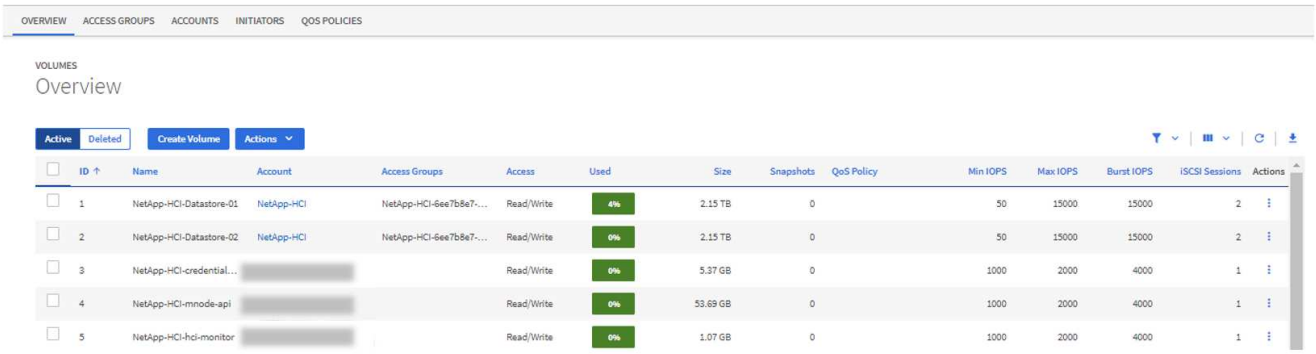
- [ボリュームを編集します]
- [ボリュームをクローニングする]
- [ボリュームアクセスグループにボリュームを追加します]
- [ボリュームを削除します]
- [削除したボリュームをリストアします]
- [削除したボリュームをパージします]

ボリュームを作成します

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

手順

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



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

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

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

   アカウントが存在しない場合は、「 * 新規アカウントの作成 * 」をクリックし、新しいアカウント名を入力して、「 * アカウントの作成 * 」をクリックします。アカウントが作成され、「 * Account * 」リストに新しいボリュームが関連付けられます。

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

9. ボリュームの QoS を設定するには、次のいずれかを実行します。
    - QoS 設定 * で、 IOPS の最小値、最大値、バースト値をカスタマイズするか、デフォルトの QoS 値を使用します。
    - 「サービス品質ポリシーの割り当て」の切り替えを有効にし、表示されたリストから既存の QoS ポリシーを選択して、既存の QoS ポリシーを選択します。
    - 新しい QoS ポリシーを作成して割り当てます。そのためには、「サービス品質ポリシーの割り当て」切り替えを有効にし、「 * 新しい QoS ポリシーの作成」をクリックします。表示されたウィンドウで、 QoS ポリシーの名前を入力し、 QoS 値を入力します。完了したら、 * Create Quality of Service Policy * （サービス品質ポリシーの作成）をクリックします。

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

10. [ボリュームの作成] をクリックします。

ボリュームに **QoS** ポリシーを適用します

NetApp Hybrid Cloud Control を使用して、既存のストレージボリュームに QoS ポリシーを適用できます。ボリュームに対してカスタムの QoS 値を設定する必要がある場合は、を使用します [ボリュームを編集します]。新しい QoS ポリシーを作成する手順については、を参照してください "ボリュームの QoS ポリシーの作成と管理"。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. 「 * Volumes * > * Overview * 」を選択します。
4. QoS ポリシーに関連付けるボリュームを 1 つ以上選択します。
5. ボリュームテーブルの上部にある * Actions * ドロップダウンリストをクリックし、 * Apply QoS Policy * を選択します。
6. 表示されたウィンドウで、リストから QoS ポリシーを選択し、 * QoS ポリシーの適用 * をクリックします。

    ボリュームで QoS ポリシーを使用している場合は、カスタム QoS を設定して、ボリュームとの QoS ポリシーの所属を削除できます。カスタムの QoS 値は、ボリュームの QoS 設定の QoS ポリシー値よりも優先されます。

ボリュームを編集します

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

このタスクについて

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

- 正常な動作状態。

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

手順

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

   a. ボリュームの合計サイズを変更します。

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

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

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

   b. 別のアカウントアクセスレベルを選択します。
      - 読み取り専用です
      - 読み取り / 書き込み
      - ロック済み
      - レプリケーションターゲット

   c. ボリュームへのアクセスを許可するアカウントを選択します。

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

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

   d. 次のいずれかを実行して QoS を変更します。

      i. 既存のポリシーを選択してください。

ii. Custom Settings で、 IOPS の最小値、最大値、バースト値を設定するか、またはデフォルト値を使用します。

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

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

6. [保存（ Save ）] を選択します。

ボリュームをクローニングする

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

作業を開始する前に

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

このタスクについて

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

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

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

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. [* Volumes （ボリューム） **>** Overview （概要） *] タブを選択します。
4. クローニングする各ボリュームを選択します。
5. ボリュームテーブルの上部にある * Actions * （アクション）ドロップダウンリストをクリックし、 * Clone * （クローン * ）を選択します。
6. 表示されたウィンドウで、次の手順を実行します。

a. ボリューム名のプレフィックスを入力します（これはオプションです）。

b. **Access** リストからアクセスタイプを選択します。

c. 新しいボリュームクローンに関連付けるアカウントを選択します（デフォルトでは、 * Copy from Volume * が選択され、元のボリュームと同じアカウントが使用されます）。

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

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

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

a. [* Clone Volumes] をクリックします。

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

ボリュームアクセスグループにボリュームを追加します

ボリュームアクセスグループには、単一のボリュームまたはボリュームのグループを追加できます。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. 「 * Volumes * > * Overview * 」を選択します。
4. ボリュームアクセスグループに関連付けるボリュームを 1 つ以上選択します。
5. ボリュームテーブルの上部にある * Actions * ドロップダウンリストをクリックし、 * Add to Access Group * を選択します。
6. 表示されたウィンドウで、 * ボリュームアクセスグループ * リストからボリュームアクセスグループを選択します。
7. [ボリュームの追加] をクリックします。

ボリュームを削除します

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

このタスクについて

削除されたボリュームはすぐにパージされるわけではなく、約 8 時間使用可能な状態のままになります。8 時間が経過すると消去され、利用できなくなります。この間にリストアしたボリュームはオンラインに戻り、

iSCSI 接続が再度確立されます。

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

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

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. 「 * Volumes * > * Overview * 」を選択します。
4. 削除するボリュームを 1 つ以上選択します。
5. ボリュームテーブルの上部にある * Actions * （アクション）ドロップダウンリストをクリックし、 * Delete * （削除）を選択します。
6. 表示されたウィンドウで、 * はい * をクリックして操作を確認します。

削除したボリュームをリストアします

削除したストレージボリュームは、削除後 8 時間以内にリストア可能です。

削除されたボリュームはすぐにパージされるわけではなく、約 8 時間使用可能な状態のままになります。8 時間が経過すると消去され、利用できなくなります。この間にリストアしたボリュームはオンラインに戻り、iSCSI 接続が再度確立されます。

手順

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

削除したボリュームをパージします

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

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid

Cloud Control にログインします。

2. ダッシュボードの左側のナビゲーションメニューで、ストレージクラスタの名前を展開します。
3. 「 * Volumes * > * Overview * 」を選択します。
4. 「削除済み」を選択します。
5. パージするボリュームを 1 つ以上選択します。
6. 次のいずれかを実行します。
   - 複数のボリュームを選択した場合は、テーブルの上部にある * Purge * クイック・フィルタをクリックします。
   - 1 つのボリュームを選択した場合は、 Volumes （ボリューム）テーブルの * Actions （アクション） * 列で、ボリュームのメニューを展開し、 * Purge * を選択します。
7. Volumes （ボリューム）テーブルの * Actions （アクション） * 列で、ボリュームのメニューを展開し、 * Purge * を選択します。
8. [はい] を選択してプロセスを確認します。

詳細については、こちらをご覧ください

- "ボリュームについて学習する"
- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

ボリュームアクセスグループを作成および管理します

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

必要なもの

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

ボリュームアクセスグループを追加

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

手順

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

3. [* Volumes （ボリューム）] を選択します
4. [* アクセスグループ *] タブを選択します。
5. [アクセスグループの作成 *] ボタンを選択します。
6. 表示されたダイアログで、新しいボリュームアクセスグループの名前を入力します。
7. （オプション）「 * Initiators * 」セクションで、新しいボリュームアクセスグループに関連付けるイニシエータを 1 つ以上選択します。

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

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

ボリュームアクセスグループを編集します

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

手順

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

ボリュームアクセスグループを削除する

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

手順

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

4. [* アクセスグループ *] タブを選択します。
5. アクセスグループテーブルの *Actions * 列で、削除するアクセスグループのオプションメニューを展開します。
6. オプションメニューで、 * 削除 * を選択します。
7. アクセスグループに関連付けられているイニシエータを削除しない場合は、「 * このアクセスグループ内のイニシエータを削除する * 」チェックボックスの選択を解除します。
8. [はい] を選択して、削除操作を確認します。

詳細については、こちらをご覧ください

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

イニシエータを作成および管理する

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

必要なもの

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

オプション（ **Options** ）

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

イニシエータを作成します

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

このタスクについて

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

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

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

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

手順

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

オプション	手順
1 つ以上のイニシエータを作成します	a. IQN または WWPN * フィールドにイニシエータの IQN または WWPN を入力します。 b. [* エイリアス] フィールドにイニシエータのフレンドリ名を入力します。 c. （オプション） Add Initiator * を選択して新しいイニシエータフィールドを開くか、代わりに bulk create オプションを使用します。 d. イニシエータの作成 * を選択します。
イニシエータを一括作成します	a. 「 * Bulk Add IQs/WWPN * 」を選択します。 b. IQN または WWPN のリストをテキストボックスに入力します。各 IQN または WWPN は、カンマまたはスペースで区切って指定するか、または独自の行に入力する必要があります。 c. [* IQN / WWPN の追加 *] を選択します。 d. （オプション）各イニシエータに一意のエイリアスを追加します。 e. インストール環境にすでに存在する可能性のあるイニシエータをリストから削除します。 f. イニシエータの作成 * を選択します。

ボリュームアクセスグループにイニシエータを追加します

ボリュームアクセスグループにイニシエータを追加できます。イニシエータをボリュームアクセスグループに

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

手順

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

イニシエータエイリアスを変更します

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

手順

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

イニシエータを削除する

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

手順

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

a. 削除するイニシエータを 1 つ以上選択します。

b. [* アクション > 削除（ * Actions > Delete * ）] を選択

c. 削除操作を確定し、 * はい * を選択します。

詳細については、こちらをご覧ください

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

ボリュームの **QoS** ポリシーの作成と管理

標準的なサービス品質設定を QoS ポリシーとして作成および保存して、複数のボリュームに適用することができます。QoS ポリシーを使用するには、 Element 10.0 以降のクラスタを選択する必要があります。 10.0 より前のクラスタでは QoS ポリシーを使用できません。

> の使用方法の詳細については、 NetApp HCI の概念に関するコンテンツを参照してください "QoS ポリシー" 個々のボリュームではなく "QoS"。

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

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

QoS ポリシーを作成する

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

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

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで、ストレージクラスタのメニューを展開します。
3. Storage > Volumes （ストレージ）を選択します。

4. [* QoS Policies] タブをクリックします。
5. [ポリシーの作成 *] をクリックします。
6. 「 * ポリシー名 * 」を入力します。

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

7. 最小 IOPS 、最大 IOPS 、バースト IOPS の値を入力します。
8. [Create QoS Policy] をクリックします。

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

ボリュームに **QoS** ポリシーを適用します

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

必要なもの

割り当てようとしている QoS ポリシーが削除されました 作成済み。

このタスクについて

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

手順

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

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

7. [保存（ Save ）] をクリックします。

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

ボリュームの **QoS** ポリシーの割り当てを変更します

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

必要なもの

変更するボリュームはです 割り当て済み QoS ポリシー。

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで、ストレージクラスタのメニューを展開します。
3. Storage > Volumes （ストレージ）を選択します。
4. 変更するボリュームの横にある * Actions * メニューをクリックします。
5. 表示されたメニューで、「 * 編集 * 」を選択します。
6. ダイアログボックスで、次のいずれかを実行します。
   - QoS ポリシーの割り当てを無効にし、個々のボリュームの QoS の最小 IOPS * 、最大 IOPS * 、バースト IOPS * の値を変更します。

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

   - 選択したボリュームに適用する別の QoS ポリシーをドロップダウンリストから選択してください。
7. [保存（ Save ）] をクリックします。

   更新されたボリュームが概要ページに表示されます。

QoS ポリシーを編集する

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

手順

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで、ストレージクラスタのメニューを展開します。
3. Storage > Volumes （ストレージ）を選択します。
4. [* QoS Policies] タブをクリックします。
5. 変更する QoS ポリシーの横にある * Actions * メニューをクリックします。
6. [編集（ Edit ）] をクリックします。
7. [Edit QoS Policy] ダイアログボックスで、次の 1 つ以上を変更します。
   - * Name * ： QoS ポリシーのユーザ定義名。

- * Min IOPS * ：ボリュームに対して保証されている最小 IOPS 。デフォルト値は 50 です。
- * Max IOPS * ：ボリュームで許可されている最大 IOPS 。デフォルト値は 15 、 000 です。
- * Burst IOPS * ：ボリュームに対して短期間で許可されている最大 IOPS 。デフォルト値は 15 、 000 です。

8. [保存（ Save ）] をクリックします。

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

> ポリシーの「 * Active Volumes * 」列のリンクをクリックすると、そのポリシーに割り当てられているボリュームをフィルタリングして表示できます。

QoS ポリシーを削除する

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

手順

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

詳細については、こちらをご覧ください

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

管理ノードを操作します

管理ノードの概要

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

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

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

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

管理ノードをインストールまたはリカバリします。

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

管理ノードにアクセスします。

- "管理ノード（ UI または REST API ）へのアクセス"

デフォルトのSSL証明書を変更します。

- "管理ノードのデフォルトSSL証明書を変更します"

管理ノード UI を使用してタスクを実行します。

- "管理ノード UI の概要"

管理ノード REST API を使用してタスクを実行します。

- "管理ノードの REST API UI の概要"

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

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

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

管理ノードをインストールまたはリカバリします

管理ノードをインストール

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

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

必要なもの

- クラスタで NetApp Element ソフトウェア 11.3 以降を実行している必要があります。
- インストール環境では IPv4 を使用します。管理ノード 11.3 では IPv6 がサポートされません。

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

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

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

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

このタスクについて

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

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

手順

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

ISO または **OVA** をダウンロードし、 **VM** を導入します

1. から、インストール環境に対応した OVA または ISO をダウンロードします "NetApp HCI" ネットアップサポートサイトのページ：
   a. Download Latest Release * を選択し、 EULA に同意します。
   b. ダウンロードする管理ノードのイメージを選択します。

2. OVA をダウンロードした場合は、次の手順を実行します。
   a. OVA を導入します。
   b. ストレージクラスタが管理ノード（ eth0 ）とは別のサブネット上にある環境で永続ボリュームを使用する場合は、ストレージサブネット（ eth1 など）上の VM に 2 つ目のネットワークインターフェイスコントローラ（ NIC ）を追加するか、管理ネットワークからストレージネットワークへルーティング可能なことを確認します。
3. ISO をダウンロードした場合は、次の手順を実行します。
   a. 以下の構成でハイパーバイザーから新しい 64 ビットの仮想マシンを作成します。
      - 仮想 CPU × 6
      - 24GB の RAM
      - ストレージアダプタのタイプが LSI Logic Parallel に設定されています

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

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

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

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

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

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

管理ノード管理者を作成し、ネットワークを設定

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

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

2. 管理ノードネットワーク（ eth0 ）を設定します。

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

時刻同期を設定します

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

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

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

   b. NTPD を停止：

   ```
   sudo service ntpd stop
   ```

   c. NTP 構成ファイル /etc/ntp.conf を編集します

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

      ii. 追加するデフォルトのタイムサーバごとに新しい行を追加します。デフォルトのタイムサーバは、同じ NTP サーバである必要があります で使用するストレージクラスタで使用します A "後の手順"。

      ```
      vi /etc/ntp.conf

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

      iii. 完了したら構成ファイルを保存します。

   d. 新しく追加したサーバと NTP 同期を強制します。

   ```
   sudo ntpd -gq
   ```

   e. NTPD を再起動します。

   ```
   sudo service ntpd start
   ```

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

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

i. 定期的な時刻同期を無効にします。

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

ii. サービスの現在のステータスを表示して確認します。

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

iii. vSphere で、 [VM オプション] の [ゲスト時刻をホストと同期する] チェックボックスがオフになっていることを確認します。

> 今後 VM を変更する場合は、このオプションを有効にしないでください。

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

管理ノードをセットアップ

1. 管理ノードのセットアップコマンドを設定して実行します。

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

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

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

> 内はコマンドの省略名で、正式な名前の代わりに使用できます。

- * --mnode_admin_user （ -mu ） [username] * ：管理ノードの管理者アカウントのユーザ名。一般には、管理ノードへのログインに使用したユーザアカウントのユーザ名です。
- * --storage_mvip （ -SM ） [MVIP アドレス] * ： Element ソフトウェアを実行しているストレージクラスタの管理仮想 IP アドレス（ MVIP ）。同じストレージクラスタを使用して管理ノードを設定します の間に使用しました "NTP サーバの設定"。

- *--storage_username(-su)[username] * ：「 --storage_mvip 」パラメータで指定したクラスタのストレージクラスタ管理者のユーザ名。
- * --metal_active （ -t ） [true]* ： Active IQ による分析のためのデータ収集を有効にする値を true のままにします。

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

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

c. （推奨）：永続ボリュームに関する以下のパラメータを追加します。永続ボリューム機能用に作成されたアカウントとボリュームを変更または削除しないでください。変更または削除すると、管理機能が失われます。

- * --use_persistent_volumes （ -pv ） [true/false 、デフォルト： false]* ：永続ボリュームを有効または無効にします。永続ボリューム機能を有効にするには、 true を入力します。
- **--persistent_volume_account (-pVA) [account_name]**:`--use_persistent_volumes が true に設定されている場合 ' このパラメータを使用して ' 永続ボリュームに使用するストレージ・アカウント名を入力します

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

- * - persistent_volumes _mvip （ -pvm ） [mvip] * ：永続ボリュームで使用する Element ソフトウェアを実行しているストレージクラスタの管理仮想 IP アドレス（ MVIP ）を入力します。このパラメータは、管理ノードで複数のストレージクラスタが管理されている場合にのみ必要です。複数のクラスタを管理していない場合は、デフォルトのクラスタ MVIP が使用されます。

d. プロキシサーバを設定します。

- * --use_proxy （ -up ） [true/false 、 default ： false]* ：プロキシの使用を有効または無効にします。このパラメータは、プロキシサーバを設定する場合に必要です。
- * --proxy_hostname_or_IP （ -pi ） [-host] * ：プロキシのホスト名または IP 。プロキシを使用する場合は必須です。これを指定すると '--proxy_port' の入力を求めるプロンプトが表示されます
- **--proxy_username （ -pu ） [username]**: プロキシユーザ名。このパラメータはオプションです。
- **--proxy_password (-pp)[password]**: プロキシパスワード。このパラメータはオプションです。
- * --proxy_port （ -pq ） [port 、 default ： 0]*: プロキシポート。これを指定すると ' プロキシ・ホスト名または IP (--proxy_hostname_or_ip`) の入力を求めるプロンプトが表示されます
- * --proxy_ssh_port （ -ps ） [port 、 default ： 443] * ： SSH プロキシポート。デフォルト値はポート 443 です。

e. （オプション）各パラメータに関する追加情報が必要な場合は、 help パラメータを使用します。

- **--help(-h)**: 各パラメータに関する情報を返します。パラメータは、初期導入時に必須またはオプションとして定義します。アップグレードと再導入ではパラメータの要件が異なる場合があります。

f. 「 etup-mnode 」コマンドを実行します。

1. インストール ID を確認します。
   a. ブラウザから、管理ノードの REST API UI にログインします。
   b. ストレージの MVIP にアクセスしてログインします。次の手順で証明書が承認されます。
   c. 管理ノードでインベントリサービス REST API UI を開きます。

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

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

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

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

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

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

択します。

> コントローラサブアセットを追加する場合は、vCenterで新しいNetApp HCCロールを作成する必要があります。この新しい NetApp HCC ロールにより、管理ノードのサービス表示がネットアップ専用のアセットに制限されます。を参照してください "vCenter で NetApp HCC ロールを作成します"。

d. [* 試してみてください *] を選択します。

e. クリップボードにコピーした親ベースアセットの ID を * asset_id * フィールドに入力します。

f. 必要なペイロード値を「 vcenter 」タイプと「 vcenter 」クレデンシャルタイプで入力します。

g. [* Execute] を選択します。

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

1. （ NetApp HCI のみ）管理ノードの既知のアセットにコンピューティングノードのアセットを追加します。

   a. コンピューティングノードアセットのクレデンシャルを使用してコンピューティングノードサブアセットを追加する場合は、「 * POST/assets/ ｛ asset_id ｝ /compute-nodes 」を選択します。

   b. [* 試してみてください *] を選択します。

   c. クリップボードにコピーした親ベースアセットの ID を * asset_id * フィールドに入力します。

   d. ペイロードで、 Model タブで定義されているとおりに必要なペイロード値を入力します。「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入力します。

   e. [* Execute] を選択します。

詳細はこちら

- "永続ボリューム"
- "管理ノードにコンピューティングアセットとコントローラアセットを追加します"
- "ストレージ NIC を設定します"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

ストレージネットワークインターフェイスコントローラ（ **NIC** ）の設定

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

作業を開始する前に

- eth0 の IP アドレスを確認しておきます。
- クラスタで NetApp Element ソフトウェア 11.3 以降を実行している必要があります。
- 管理ノード 11.3 以降を導入しておきます。

設定オプション

環境に適したオプションを選択します。

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

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

手順

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

> 新しいストレージ・ネットワーク・インターフェイスに必要なパラメータごとに値は「$」で表されます。次のテンプレート内の 'cluster' オブジェクトは必須であり ' 管理ノードのホスト名の変更に使用できます`-- 非セキュアなオプションや '-k オプションは ' 本番環境では使用しないでください

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

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

手順

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

> 新しいストレージ・ネットワーク・インターフェイスに必要なパラメータごとに値は「 $ 」で表されます。次のテンプレート内の 'cluster' オブジェクトは必須であり ' 管理ノードのホスト名の変更に使用できます`-- 非セキュアなオプションや '-k オプションは ' 本番環境では使用しないでください

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

詳細はこちら

- "管理ノードにコンピューティングアセットとコントローラアセットを追加します"
- "vCenter Server 向け NetApp Element プラグイン"

- "NetApp HCI のリソースページ"

管理ノードをリカバリ

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

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

必要なもの

- 以前の管理ノードで NetApp Element ソフトウェアバージョンを実行していた 11.3 以降 "永続ボリューム" 機能が関与している。
- 永続ボリュームを含むクラスタの MVIP と SVIP が必要です。
- クラスタで NetApp Element ソフトウェア 11.3 以降を実行している必要があります。
- インストール環境では IPv4 を使用します。管理ノード 11.3 では IPv6 がサポートされません。
- ネットアップサポートサイトからソフトウェアをダウンロードする権限が必要です。
- 使用するプラットフォームに適した管理ノードイメージのタイプを特定しておきます。

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

手順

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

ISO または **OVA** をダウンロードし、 **VM** を導入します

1. から、インストール環境に対応した OVA または ISO をダウンロードします "NetApp HCI" ネットアップサポートサイトのページ：
   a. [Download Latest Release] をクリックして、 EULA に同意します。
   b. ダウンロードする管理ノードのイメージを選択します。
2. OVA をダウンロードした場合は、次の手順を実行します。
   a. OVA を導入します。
   b. ストレージクラスタが管理ノード（ eth0 ）とは別のサブネット上にある環境で永続ボリュームを使用

する場合は、ストレージサブネット（ eth1 など）上の VM に 2 つ目のネットワークインターフェイスコントローラ（ NIC ）を追加するか、管理ネットワークからストレージネットワークへルーティング可能なことを確認します。

3. ISO をダウンロードした場合は、次の手順を実行します。
   a. 以下の構成でハイパーバイザーから新しい 64 ビットの仮想マシンを作成します。
      - 仮想 CPU × 6
      - 24GB の RAM
      - 400GB の仮想ディスク、シンプロビジョニング
      - インターネットアクセスとストレージ MVIP へのアクセスが可能な仮想ネットワークインターフェイス × 1
      - ストレージクラスタへの管理ネットワークアクセスが可能な仮想ネットワークインターフェイス×1。ストレージクラスタが管理ノード（ eth0 ）とは別のサブネット上にある環境で永続ボリュームを使用する場合は、ストレージサブネット（ eth1 ）上の VM に 2 つ目のネットワークインターフェイスコントローラ（ NIC ）を追加するか、管理ネットワークからストレージネットワークへルーティング可能なことを確認します。

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

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

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

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

ネットワークを設定します

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

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

2. 管理ノードネットワーク（ eth0 ）を設定します。

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

時刻同期を設定します

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

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

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

```
sudo service ntpd stop
```

3. NTP 構成ファイル /etc/ntp.conf を編集します
   a. 各サーバの前に # を追加して ' デフォルト・サーバ（サーバ 0.gentoo.pool.ntp.org ）をコメントアウトします
   b. 追加するデフォルトのタイムサーバごとに新しい行を追加します。デフォルトのタイムサーバは、同じ NTP サーバである必要があります で使用するストレージクラスタで使用します A "後の手順"。

```
vi /etc/ntp.conf

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

   c. 完了したら構成ファイルを保存します。
4. 新しく追加したサーバと NTP 同期を強制します。

```
sudo ntpd -gq
```

5. NTPD を再起動します。

```
sudo service ntpd start
```

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

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

   a. 定期的な時刻同期を無効にします。

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

   b. サービスの現在のステータスを表示して確認します。

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

c. vSphere で、 [VM オプション] の [ゲスト時刻をホストと同期する] チェックボックスがオフになっていることを確認します。

> 今後 VM を変更する場合は、このオプションを有効にしないでください。

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

管理ノードを設定

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

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

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

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

4. 生成されたファイルを '/sf/mnode -archive' ディレクトリに解凍します

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

5. アカウントとボリュームの構成ファイルを作成します。

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

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

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

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

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

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

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

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

b. 「 redeploy -mnode 」コマンドを実行します。再導入が完了すると、成功メッセージが表示されます。

c. システムの完全修飾ドメイン名（ FQDN ）を使用して Element または NetApp HCI の Web インターフェイス（管理ノードやネットアップハイブリッドクラウド制御など）にアクセスする場合は、 "管理ノードの認証を再設定します"。

> 提供する SSH 機能 "ネットアップサポートの Remote Support Tunnel （ RST ）セッションアクセス" 管理サービス 2.18 以降を実行する管理ノードでは、はデフォルトで無効になっています。以前に管理ノードで SSH 機能を有効にしていた場合は、が必要になることがあります "SSH を再度無効にします" リカバリされた管理ノード。

詳細はこちら

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

管理ノードにアクセスします

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

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

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

きます。

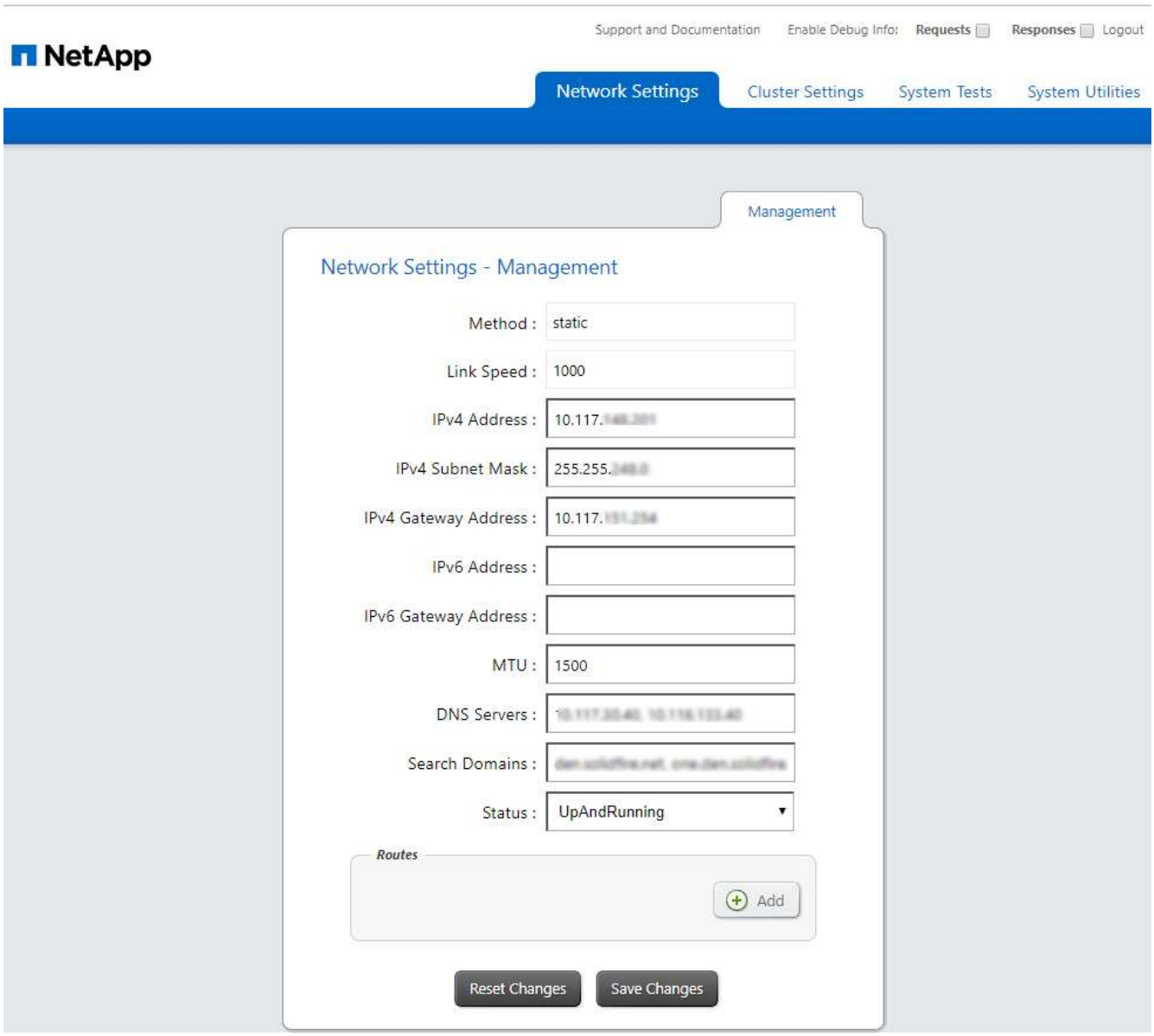
管理ノードのノード **UI** にアクセスします

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

手順

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

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



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

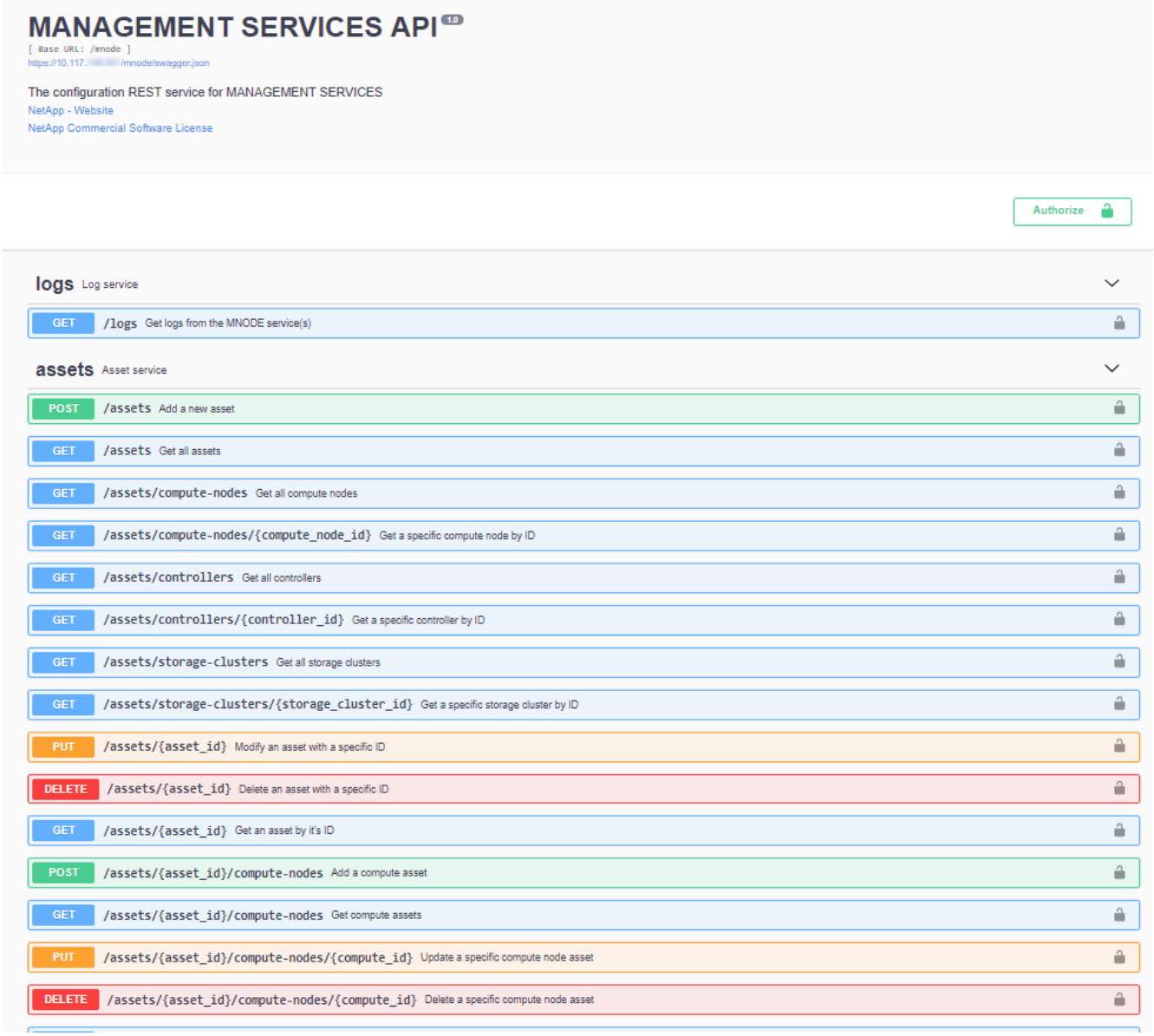
管理ノードの **REST API UI** にアクセスします

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

手順

1. 管理サービスの REST API UI にアクセスするには、管理ノードの IP アドレスに「 /mnode 」を続けて入力します。

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



2. Authorize * または任意のロックアイコンをクリックし、 API を使用する権限を付与するクラスタ管理者クレデンシャルを入力します。

詳細はこちら

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

管理ノードのデフォルト**SSL**証明書を変更します

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

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

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

- * GetNodeSSLCertificate *

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

- * SetNodeSSLCertificate *

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

- * RemoveNodeSSLCertificate *

  これ "RemoveNodeSSLCertificateメソッド" 現在インストールされているSSL証明書と秘密鍵を削除します。そのあと、クラスタで新しい自己署名証明書と秘密鍵が生成されます。

詳細については、こちらをご覧ください

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

管理ノード **UI** の操作

管理ノード **UI** の概要

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

管理ノード UI で実行できるタスクは次のとおりです。

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

詳細については、こちらをご覧ください

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

NetApp HCI でアラート監視を設定する

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

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

1. ノード単位の管理ノード UI を開きます (`https://[IP address:442')
2. [* Alert Monitor*] タブをクリックします。
3. アラート監視オプションを設定します。

アラート監視オプション

オプション（ **Options** ）	説明
Alert Monitor テストを実行します	モニタシステムテストを実行して次の項目を確認します。 • NetApp HCI と VMware vCenter の接続 • データストア情報を使用した NetApp HCI と VMware vCenter のペアリング QoSSIOC サービスによって提供されます • 現在の NetApp HCI アラームと vCenter アラームのリスト
アラートを収集します	NetApp HCI ストレージアラームの vCenter への転送を有効または無効にします。ドロップダウンリストからターゲットのストレージクラスタを選択できます。このオプションのデフォルト設定は「 enabled 」です。

オプション（ **Options** ）	説明
ベストプラクティスアラートを収集	NetApp HCI ストレージのベストプラクティスアラートの vCenter への転送を有効または無効にします。ベストプラクティスアラートは、最適化されていないシステム構成によってトリガーされた障害です。このオプションのデフォルト設定は「ディセーブル」です。無効にすると、 NetApp HCI ストレージのベストプラクティスアラートは vCenter に表示されません。
サポートデータを AIQ に送信	VMware vCenter から NetApp SolidFire Active IQ へのサポートデータと監視データのフローを制御します。 オプションは次のとおりです。 • Enabled ： vCenter アラーム、 NetApp HCI ストレージアラーム、およびサポートデータがすべて NetApp SolidFire Active IQ に送信されます。ネットアップによる NetApp HCI インストールのプロアクティブなサポートと監視が可能となるため、システムに影響が及ぶ前に問題を検出して解決できます。 • Disabled ： vCenter アラーム、 NetApp HCI ストレージアラーム、サポートデータはいずれも NetApp SolidFire Active IQ に送信されません。 NetApp Deployment Engine を使用して AIQ へのデータの送信 * オプションをオフにした場合は、が必要です "テレメータを有効にします" このページから、管理ノードの REST API を使用してサービスを設定し直してください。

オプション（ **Options** ）	説明
コンピューティングノードのデータを AIQ に送信	コンピューティングノードから NetApp SolidFire Active IQ へのサポートデータと監視データのフローを制御します。 オプションは次のとおりです。 • Enabled ：コンピューティングノードに関するサポートデータと監視データが NetApp SolidFire Active IQ に転送されるため、コンピューティングノードのハードウェアをプロアクティブにサポートできます。 • Disabled ：コンピューティングノードに関するサポートデータと監視データは NetApp SolidFire Active IQ に転送されません。 NetApp Deployment Engine を使用して AIQ へのデータの送信 * オプションをオフにした場合は、が必要です "テレメータを有効にします" このページから、管理ノードの REST API を使用してサービスを設定し直してください。

詳細はこちら

- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

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

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

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

管理ノードのネットワーク設定を更新します

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

1. ノード管理ノード UI を開きます。
2. [ネットワーク設定 *] タブをクリックします。
3. 次の情報を表示または入力します。

a. * method * ：インターフェイスを設定するには、次のいずれかの方法を選択します。
   - loopback ： IPv4 ループバックインターフェイスを定義する場合に使用します。
   - 「手動」：デフォルトで設定が行われないインターフェイスを定義する場合に使用します。
   - `d hop`: DHCP を介して IP アドレスを取得するために使用します。
   - 'tatic ：静的に割り当てられた IPv4 アドレスを持つイーサネットインターフェイスを定義する場合に使用します。
b. * リンク速度 * ：仮想 NIC によってネゴシエートされた速度。
c. **IPv4 Address** ： eth0 ネットワークの IPv4 アドレス。
d. **IPv4 Subnet Mask**: IPv4 ネットワークのアドレス分割。
e. *IPv4 ゲートウェイアドレス *: ローカルネットワークからパケットを送信するためのルータネットワークアドレス。
f. **IPv6 Address**: eth0 ネットワークの IPv6 アドレス。
g. *IPv6 ゲートウェイアドレス *: ローカルネットワークからパケットを送信するためのルータネットワークアドレス。

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

h. **MTU** ：ネットワークプロトコルが伝送できる最大パケットサイズ。1500 以上にする必要があります。2 つ目のストレージ NIC を追加する場合は、値を 9000 にする必要があります。
i. **DNS Servers** ：クラスタ通信に使用するネットワーク・インターフェイス。
j. * 検索ドメイン *: システムで使用可能な追加の MAC アドレスを検索します。
k. * ステータス * ：有効な値は次のとおりです。
   - 「 UpAndRunning 」
   - 「所有」
   - 「上」
l. * Routes * ：ルートが使用するように設定されている、関連付けられたインターフェイスを介した特定のホストまたはネットワークへのスタティックルート。

管理ノードのクラスタ設定を更新します

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

1. ノード管理ノード UI を開きます。
2. [クラスタ設定 *] タブをクリックします。
3. 次の情報を表示または入力します。
   - * ロール * ：管理ノードがクラスタ内に設定するロール。有効な値は「管理」です。
   - * バージョン * ：クラスタで実行されている Element ソフトウェアのバージョン。
   - * デフォルトインターフェイス * ： Element ソフトウェアを実行しているクラスタとの管理ノード通

信に使用されるデフォルトのネットワークインターフェイス。

管理ノードの設定をテストします

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

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

詳細はこちら

- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

管理ノードからシステムユーティリティを実行します

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

手順

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

> この処理を実行すると、ネットワーク接続が一時的に失われます。

- * アクション *: オプションには「再起動」と「停止」（電源オフ）が含まれます。
- * Wakeup Delay * ：ノードがオンラインに戻るまでの時間。

b. * クラスタサポートバンドルの作成 * ：クラスタ内のノードについてネットアップサポートの診断を受けるためのクラスタサポートバンドルを作成します。次のオプションを指定します。

- * Bundle Name * ：作成された各サポートバンドルの一意の名前。名前を指定しない場合、「 supportbundle 」とノード名がファイル名として使用されます。
- * Mvip * ：クラスタの MVIP 。バンドルは、クラスタ内のすべてのノードから収集されます。このパラメータは、 Nodes パラメータを指定しない場合のみ必要です。
- * Nodes * ：バンドルを収集するノードの IP アドレス。バンドルの収集元のノードを指定するには、 Nodes または Mvip のいずれかを使用します。両方を使用することはできません。このパラメータは、 Mvip を指定しない場合は必須です。
- * Username * ：クラスタ管理者ユーザ名。
- * Password * ：クラスタ管理者のパスワード。
- * Allow Incomplete * ： 1 つ以上のノードからバンドルを収集できない場合でもスクリプトが引き続き実行されます。
- * Extra Args * ：このパラメータは 's_make _support_bundle' スクリプトに渡されますこのパラメータは、ネットアップサポートから指示された場合にのみ使用します。

c. * Delete All Support Bundles * ：管理ノードに保存されているすべてのサポートバンドルを削除します。

d. * ノードのリセット * ：管理ノードを新しいインストールイメージにリセットします。これにより、ネットワーク設定を除くすべての設定がデフォルトの状態に変更されます。次のオプションを指定します。

- * Build * ：ノードをリセットするリモート Element ソフトウェアイメージの URL 。
- * オプション * ：リセット操作を実行するための仕様。詳細が必要な場合は、ネットアップサポートにお問い合わせください。

> この処理を実行すると、ネットワーク接続が一時的に失われます。

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

> この処理を実行すると、ネットワーク接続が一時的に失われます。

詳細はこちら

- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

管理ノード **REST API** の操作

管理ノードの **REST API UI** の概要

組み込みの REST API UI （ https://<managementNodeIP>/mnode` ）を使用すると、プロキシサーバの設定、サービスレベルの更新、アセット管理などの管理ノードサービス

に関連する API を実行したり、理解したりできます。

REST API で実行できるタスクは次のとおりです。

承認

- "REST API を使用するための許可を取得する"

アセットの設定

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

資産管理

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

詳細については、こちらをご覧ください

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

REST API を使用するための許可を取得する

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

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

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

作業を開始する前に

- クラスタで NetApp Element ソフトウェア 11.3 以降を実行している必要があります。

- バージョン 11.3 以降を実行する管理ノードを導入しておく必要があります。

API コマンド

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

REST API の **UI** の手順

1. サービスの REST API UI にアクセスするには、管理ノードの IP アドレスのあとにサービス名を入力します。例：「 /mnode/` ：

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

2. 「 * 許可」をクリックします。

   ⓘ または、任意のサービス API の横にあるロックアイコンをクリックすることもできます。

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

   ⓘ トークンの期限が切れた後にコマンドを実行しようとすると、「 401 Error: Unauthorized 」というメッセージが表示されます。このメッセージが表示された場合は、再度承認してください。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

Active IQ と **NetApp HCI** の監視を有効にします

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

Active IQ コレクタサービスは、履歴データのレポートおよびほぼリアルタイムのパフォーマンス監視用に、

設定データと Element ソフトウェアベースのクラスタパフォーマンス指標を NetApp Active IQ に転送します。NetApp HCI 監視サービスを使用すると、ストレージクラスタのエラーを vCenter に転送してアラート通知を送信できます。

作業を開始する前に

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

手順

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

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

   b. 「 * Authorize * 」（認証）をクリックして、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 * をクリックします。
      iv. ウィンドウを閉じます。
   c. REST API UI で、 * 一部のユーザに適用 / インストール * をクリックします。
   d. [* 試してみてください *] をクリックします。
   e. [* Execute] をクリックします。
   f. コード 200 の応答本文から ' インストールの ID をコピーします

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

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

2. テレメータの有効化：
   a. 管理ノードの mNode サービス API UI にアクセスします。管理ノードの IP アドレスに「 /mnode 」を続けて入力します。

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

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

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

      iv. 前の手順のベース ID を * asset_ID * に入力します。
      v. [* Execute] をクリックします。

         Active IQ サービスは、アセットが変更されるたびに自動的に再起動されます。アセットを変更すると、設定が適用されるまで短時間の遅延が発生します。

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

   NetApp HCI 監視サービスにはコントローラアセットが必要です。

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

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

「 ip 」は vCenter の IP アドレスです。

e. [* Execute] をクリックします。

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"

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

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

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

必要なもの

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

手順

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

   必要に応じて "コンピューティングノードの BMC クレデンシャルを変更します" NetApp Hybrid Cloud Control に表示されている「 Hardware ID not available 」または「 Unable to detect 」エラーを解決するため。

3. 管理ノードでインベントリサービス API をリフレッシュします。

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

また、 NetApp Hybrid Cloud Control の UI でインベントリが更新されるまで 2 分待つこともできます。

a. 「 * Authorize * 」（認証）をクリックして、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 * をクリックします。
   iv. ウィンドウを閉じます。
b. REST API UI で、 * 一部のユーザに適用 / インストール * をクリックします。
c. [* 試してみてください *] をクリックします。
d. [* Execute] をクリックします。
e. 応答から、インストールアセット ID （「 id 」）をコピーします。
f. REST API UI で、 * GET / Installations / ｛ id ｝ * をクリックします。
g. [* 試してみてください *] をクリックします。
h. 更新を「 True 」に設定します。
i. インストールアセット ID を **id** フィールドに貼り付けます。
j. [* Execute] をクリックします。

4. NetApp Hybrid Cloud Control のブラウザをリフレッシュして変更を確認します。

詳細については、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"

管理ノードにコンピューティングアセットとコントローラアセットを追加します

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

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

必要なもの

- クラスタで NetApp Element ソフトウェア 11.3 以降を実行している必要があります。
- バージョン 11.3 以降を実行する管理ノードを導入しておきます。
- これで完了です "vCenter で新しい NetApp HCC ロールを作成しました" 管理ノードのサービス表示をネットアップ専用のアセットに制限します。
- vCenter の管理 IP アドレスとクレデンシャルが必要です。
- コンピューティングノード（ ESXi ）の管理 IP アドレスとルートクレデンシャルが必要です。
- ハードウェア（ BMC ）の管理 IP アドレスと管理者のクレデンシャルが必要です。

このタスクについて

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

> コンピューティングノードを手動で追加する場合は、 BMC アセットも追加するようにしてください。追加しないとエラーが返されます。

手順

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

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

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

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

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

   g. REST API UI から、 * GET / Installations / ｛ id ｝ * を選択します。
   h. [* 試してみてください *] を選択します。

i. インストールアセット ID を **id** フィールドに貼り付けます。

j. [* Execute] を選択します。

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

2. （コンピューティングノードのみ） コンピューティングノードのハードウェアタグを確認します vSphere で実行されます。

3. コントローラアセット（ vCenter ）、コンピューティングノード（ ESXi ）、またはハードウェア（ BMC ）を既存のベースアセットに追加するには、次のいずれかを選択します。

オプション	説明
POST / assets / ｛ asset_id ｝ / コントローラ	a. 管理ノードで mNode サービス REST API UI を開きます。 `https://<ManagementNodeIP>/mnode` i. 「 * Authorize * 」（認証）を選択して、次の手順を実行 A. クラスタのユーザ名とパスワードを入力します。 B. クライアント ID を「 m node-client 」として入力します。 C. セッションを開始するには、 * Authorize * を選択します。 D. ウィンドウを閉じます。 b. 「 * POST /assets/ ｛ asset_id ｝ /controllers * 」を選択します。 c. [* 試してみてください *] を選択します。 d. 親ベースアセット ID を「 * asset_id * 」フィールドに入力します。 e. 必要な値をペイロードに追加します。 f. [* Execute] を選択します。

オプション	説明
POST / assets / ｛ asset_id ｝ / compute-nodes	a. 管理ノードで mNode サービス REST API UI を開きます。 `https://<ManagementNodeIP>/mnode` i. 「 * Authorize * 」（認証）を選択して、次の手順を実行 A. クラスタのユーザ名とパスワードを入力します。 B. クライアント ID を「 m node-client 」として入力します。 C. セッションを開始するには、 * Authorize * を選択します。 D. ウィンドウを閉じます。 b. 「 * POST /assets/ ｛ asset_id ｝ /compute-nodes 」を選択します。 c. [* 試してみてください *] を選択します。 d. 前の手順でコピーした親ベースアセットの ID を「 * asset_id * 」フィールドに入力します。 e. ペイロードで、次の手順を実行します。 i. ノードの管理 IP を [IP] フィールドに入力します ii. 「 hardwareTag 」には、前の手順で保存したハードウェアタグ値を入力します。 iii. 必要に応じて、他の値を入力します。 f. [* Execute] を選択します。

オプション	説明
POST / assets / ｛asset_id｝ / ハードウェアノード	a. 管理ノードで mNode サービス REST API UI を開きます。 `https://<ManagementNodeIP>/mnode` i. 「 * Authorize * 」（認証）を選択して、次の手順を実行 A. クラスタのユーザ名とパスワードを入力します。 B. クライアント ID を「 m node-client 」として入力します。 C. セッションを開始するには、 * Authorize * を選択します。 D. ウィンドウを閉じます。 b. 「 * POST /assets/ ｛asset_id｝ /hardware-nodes 」を選択します。 c. [* 試してみてください *] を選択します。 d. 親ベースアセット ID を「 * asset_id * 」フィールドに入力します。 e. 必要な値をペイロードに追加します。 f. [* Execute] を選択します。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

コンピューティングノードのハードウェアタグを確認する方法

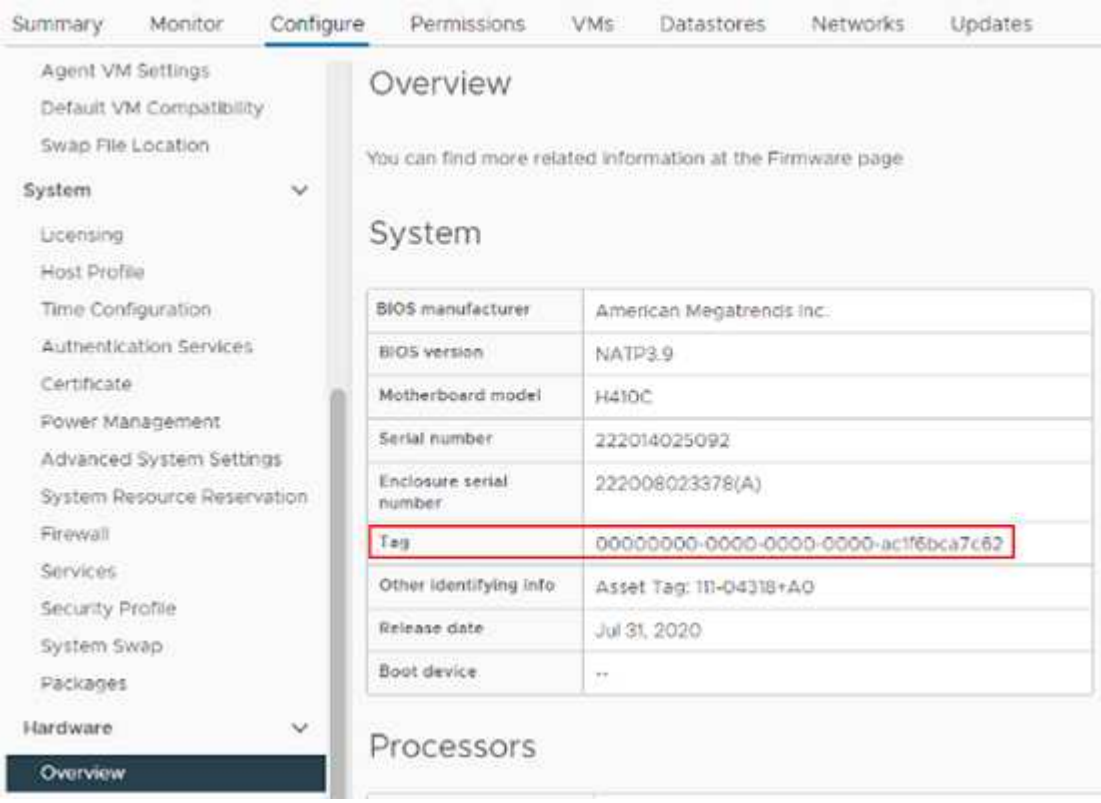
REST API UI を使用してコンピューティングノードアセットを管理ノードの構成に追加するには、ハードウェアタグが必要です。

VMware vSphere 8.0および**7.0**

VMware vSphere Web Client 8.0および7.0でコンピューティングノードのハードウェアタグを確認します。

手順

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



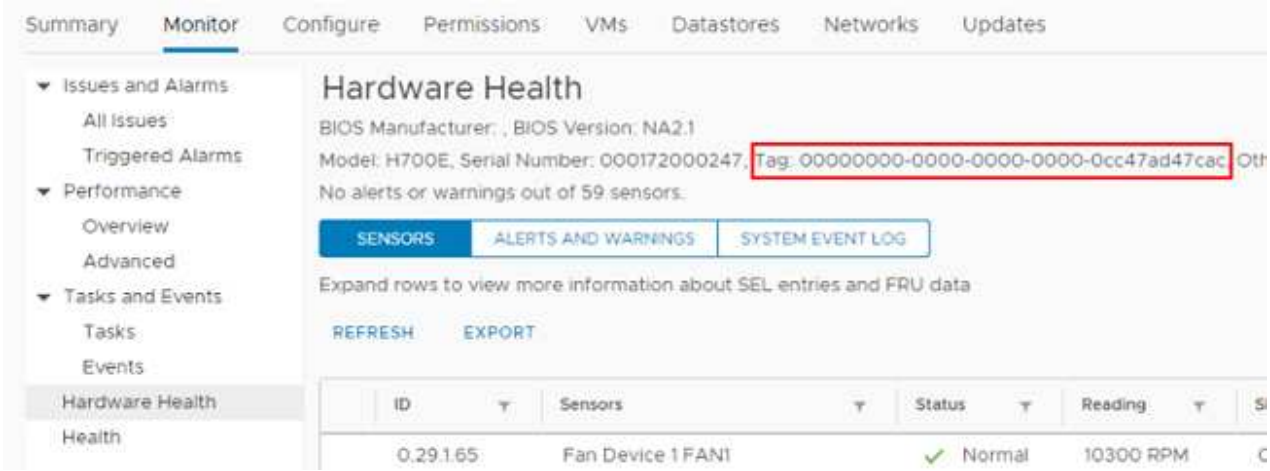
4. *Tag*の値をコピーして保存します。
5. コンピューティングアセットとコントローラアセットを管理ノードに追加します。

VMware vSphere 6.7および**6.5**

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

手順

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



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

ストレージクラスタアセットを作成および管理する

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

必要なもの

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

ストレージクラスタのアセット管理オプション

次のいずれかのオプションを選択します。

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

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

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

手順

1. 管理ノードの IP アドレスに続けて「 /inventory/1/` 」を入力して、インベントリサービスの REST API UI にアクセスします。

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

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

   API は、既知のすべてのインストールのリストを返します。

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

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

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

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

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

10. [* 試してみてください *] をクリックします。
11. 前の手順で保存したインストール ID を 'installationId' パラメータに入力します
12. [* Execute] をクリックします。

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

13. コード 200 の応答本文から、正しいストレージクラスタを探して、クラスタの「 torageId 」フィールドに値を保存します。これはストレージクラスタの ID です。

新しいストレージクラスタアセットを追加します

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

必要なもの

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

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

手順

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

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

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

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

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

6. [* Execute] をクリックします。

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

ストレージクラスタアセットに保存されているクレデンシャルを編集します

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

> の手順に従っていることを確認します ストレージのインストール ID とクラスタ ID を取得します クラスタアセット 続行する前に。

手順

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

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

2. [* Authorize * （認証）] または任意のロックアイコンをクリックして、次の手順を実行します。
   a. クラスタのユーザ名とパスワードを入力します。
   b. クライアント ID を「 m node-client 」として入力します。
   c. セッションを開始するには、 * Authorize * をクリックします。

d. ウィンドウを閉じます。

3. * PUT / clusters/ ｛ storageId ｝ * をクリックします。
4. [* 試してみてください *] をクリックします。
5. 以前にコピーしたストレージクラスタ ID を「 torageId 」パラメータに貼り付けます。
6. [**Request body**] フィールドで、次のパラメータの一方または両方を変更します。

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

パラメータ	を入力します	説明
「 password 」と入力します	文字列	ストレージクラスタとの通信に使用するパスワード。
「 userid` 」	文字列	ストレージクラスタとの通信に使用するユーザ ID （ユーザには管理者権限が必要）。

7. [* Execute] をクリックします。

ストレージクラスタアセットを削除します

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

> の手順に従っていることを確認します ストレージのインストール ID とクラスタ ID を取得します クラスタアセット 続行する前に。

手順

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

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

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

5. 「 torageId 」パラメータに、前の手順でコピーしたストレージクラスタ ID を入力します。
6. [* Execute] をクリックします。

   成功すると、 API は空の応答を返します。

詳細については、こちらをご覧ください

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

既存のコントローラアセットを表示または編集する

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

作業を開始する前に

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

管理サービス **REST API** にアクセスします

手順

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

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

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

既存のコントローラについて格納されている情報を表示する

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

手順

1. GET / compute / controllers * をクリックします。
2. [* 試してみてください *] をクリックします。

3. [* Execute] をクリックします。

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

4. 特定のコントローラの接続ステータスを取得する場合は ' そのコントローラの [id] フィールドからコントローラ ID をクリップボードにコピーし ' を参照してください [既存のコントローラのステータスを表示します]。

既存のコントローラのステータスを表示します

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

手順

1. GET / compute / controllers / ｛ controller_id ｝ / status * をクリックします。
2. [* 試してみてください *] をクリックします。
3. 以前にコピーしたコントローラ ID を 'controller_id パラメータに入力します
4. [* Execute] をクリックします。

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

コントローラの保存されているプロパティを編集します

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

手順

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

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

5. [* Execute] をクリックします。

   API から更新されたコントローラ情報が返されます。

詳細については、こちらをご覧ください

- "管理ノードにコンピューティングアセットとコントローラアセットを追加します"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

管理ノードからアセットを削除します

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

必要なもの

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

手順

1. 管理ノードの IP アドレスの後に「 /mnode/1/' 」を入力します。

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

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

プロキシサーバを設定します

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

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

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

作業を開始する前に

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

手順

1. 管理ノードの IP アドレスに「 /mnode 」を続けて入力し、管理ノードの REST API UI にアクセスします。

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

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

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

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

6. [* Execute] をクリックします。

環境によっては、管理ノードのリブートが必要になることがあります。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

管理ノードの **OS** とサービスのバージョンを確認

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

必要なもの

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

オプション（ **Options** ）

- API コマンド
- REST API の UI の手順

API コマンド

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

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

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

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

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

REST API の UI の手順

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

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

2. 次のいずれかを実行します。
   - 管理ノードで実行されている管理ノードの OS 、管理サービスバンドル、および管理ノードの API （ mnode-API ）サービスに関するバージョン情報を取得します。
     i. [**Get/About**] を選択します。
     ii. [* 試してみてください *] を選択します。
     iii. [* Execute] を選択します。

     管理サービスのバンドルバージョン（「 mnode_bundle_version 」）、管理ノードの OS バージョン（「 os_version 」）、および管理ノードの API バージョン（「 version 」）が応答の本文に示されます。
   - 管理ノードで実行されている個々のサービスに関するバージョン情報を取得します。
     i. [**get/services**] を選択します。
     ii. [* 試してみてください *] を選択します。
     iii. ステータスを「 * Running * 」と選択します。
     iv. [* Execute] を選択します。

     管理ノードで実行されているサービスは応答の本文に示されます。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

管理サービスからログを取得しています

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

必要なもの

- クラスタで NetApp Element ソフトウェア 11.3 以降を実行している必要があります。

- バージョン 11.3 以降を実行する管理ノードを導入しておきます。

手順

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

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

   - 管理サービス2.20.69以前の場合：

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

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

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

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

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

   - 「 service-name 」：サービス名を入力します。

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

   - 'setp` ：停止したサービスからログを取得するには 'true' に設定します
6. [* Execute] を選択します。
7. 応答の本文から「 * Download * 」を選択して、ログ出力を保存します。

詳細はこちら

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

- "NetApp HCI のリソースページ"

サポート接続を管理します

リモートのネットアップサポートセッションを開始します

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

ネットアップサポートとの SSH リバーストンネル接続用の TCP ポートを開くことができます。この接続を介して、ネットアップサポートはお客様の管理ノードにログインします。

作業を開始する前に

- 管理サービス 2.18 以降では、管理ノードでリモートアクセス機能がデフォルトで無効になっています。リモートアクセス機能を有効にするには、を参照してください "管理ノードで SSH 機能を管理します"。
- 管理ノードがプロキシサーバの背後にある場合は、次の TCP ポートを sshd.config ファイルで設定しておく必要があります。

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

手順

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

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

- リモートサポートトンネルを閉じるには、次のように入力します。

  rst — killall

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

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

詳細については、こちらをご覧ください

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

- "NetApp HCI のリソースページ"

管理ノードで **SSH** 機能を管理します

REST API を使用して、管理ノード（ mNode ）の SSH 機能の無効化、再有効化、ステータスの確認を行うことができます。提供する SSH 機能 "ネットアップサポートの Remote Support Tunnel （ RST ）セッションアクセス" 管理サービス 2.18 以降を実行する管理ノードでは、はデフォルトで無効になっています。

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

必要なもの

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

オプション（ **Options** ）

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

完了後、次のいずれかのタスクを実行できます "認証"：

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

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

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

> ストレージクラスタに対してSSHを使用してサポートアクセスを有効または無効にするには、を使用する必要があります "Element UIクラスタ設定ページ"。

手順

1. ダッシュボードで右上のオプションメニューを選択し、 * 構成 * を選択します。
2. Support Access for Management Node *画面で、スイッチを切り替えて管理ノードSSHを有効にします。

3. トラブルシューティングが完了したら、* Support Access for Management Node *画面で、スイッチを切り替えて管理ノードSSHを無効にします。

APIを使用して、管理ノードのSSH機能を無効または有効にします

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

API コマンド

管理サービス 2.18 以降の場合：

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

管理サービス 2.17 以前：

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

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

REST API の **UI** の手順

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

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

2. 「 * Authorize * 」（認証）を選択して、次の手順を実行
   a. クラスタのユーザ名とパスワードを入力します。
   b. クライアント ID を「 m node-client 」として入力します。
   c. セッションを開始するには、 * Authorize * を選択します。
   d. ウィンドウを閉じます。
3. REST API UI から、 * PUT / settingsusel/ssh * を選択します。
   a. [* 試してみてください *] をクリックします。
   b. SSH をディセーブルにするには **'enabled** パラメータを 'false' に設定し ' 前にディセーブルにした SSH 機能を再度イネーブルにするには 'true' を設定します

c. [* Execute] をクリックします。

APIを使用して、管理ノードのSSH機能のステータスを確認します

管理ノードで SSH 機能が有効になっているかどうかは、管理ノードのサービス API を使用して確認できます。管理サービス 2.18 以降を実行する管理ノードでは、 SSH はデフォルトで無効になっています。

API コマンド

管理サービス 2.18 以降の場合：

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

管理サービス 2.17 以前：

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

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

REST API の **UI** の手順

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

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

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

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"

NetApp HCI システムの電源をオフまたはオンにします

NetApp HCI システムの電源オン / オフを切り替えます

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

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

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

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

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

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

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

詳細については、こちらをご覧ください

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

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

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

手順

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

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

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

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

詳細については、こちらをご覧ください

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

NetApp HCI システムのストレージリソースの電源をオフにします

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

手順

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

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

レスです `nodes=[]` アレイには、手順4で記録したノードIDが含まれます。例：

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

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

6. クラスタ管理者のユーザ名とパスワードを入力します。
7. すべてのストレージクラスタノードが API 結果の「必要」セクションに含まれていることを確認して、API 呼び出しが正常に返されたことを検証します。

   すべての NetApp HCI ストレージノードの電源がオフになりました。

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

> クラスタを再起動するときは、特定の手順に従ってすべてのノードがオンラインになったことを確認する必要があります。
>
> 1. すべての重大度とを確認します `volumesOffline` クラスタの障害が解決されました。
> 2. クラスタが安定するまで10～15分待ちます。
> 3. データにアクセスするためのホストの起動を開始します。
>
> メンテナンス後にノードの電源をオンにして正常であることを確認する時間を長くしたい場合は、データの同期を遅らせて不要なビンの同期を回避する方法についてテクニカルサポートにお問い合わせください。

詳細については、こちらをご覧ください

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

NetApp HCI システムのストレージリソースの電源をオンにします

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

手順

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

詳細については、こちらをご覧ください

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

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

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

手順

1. ストレージノードの電源をオンにする場合と同じ手順で、コンピューティングノードの電源をオンにします。
2. すべてのコンピューティングノードが稼働状態になったら、 vCSA を実行していた ESXi ホストにログインします。
3. コンピューティングホストにログインし、すべての NetApp HCI データストアが表示されることを確認します。一般的な NetApp HCI システムでは、すべての ESXi ローカルデータストアと、少なくとも次の共有データストアが表示されます。

```
NetApp-HCI-Datastore-[01,02]
```

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

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

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

詳細については、こちらをご覧ください

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

NetApp Hybrid Cloud Control を使用して NetApp HCI システムを監視します

Hybrid Cloud Control でストレージリソースとコンピューティングリソースを監視します ダッシュボード

NetApp Hybrid Cloud Control のダッシュボードでは、すべてのストレージリソースとコンピューティングリソースを一目で確認できます。また、ストレージ容量、ストレージパフォーマンス、コンピューティング利用率も監視できます。

> 新しい NetApp Hybrid Cloud Control セッションを初めて起動したときに、管理ノードで複数のクラスタを管理しているときに NetApp Hybrid Cloud Control のダッシュボードビューのロードに時間がかかることがあります。ロードにかかる時間は、管理ノードでアクティブに管理されているクラスタの数によって異なります。その後の起動では、読み込み時間が短縮されます。

Hybrid Cloud Control Dashboard には、管理対象のコンピューティングノードと、 H シリーズハードウェアに管理対象ノードが少なくとも 1 つ含まれているクラスタだけが表示されます。

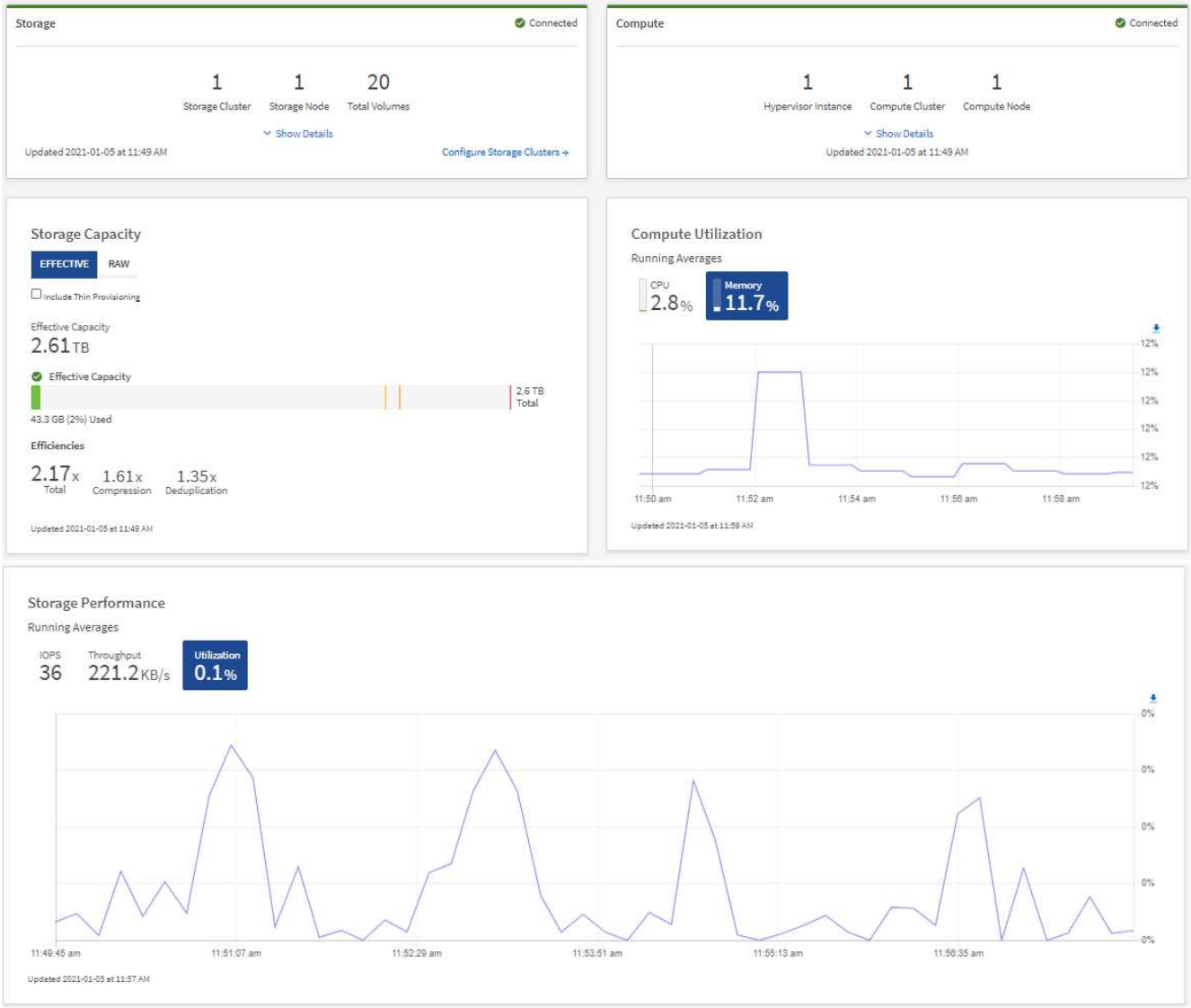
- NetApp HCC ダッシュボードにアクセスします
- [ストレージリソースを監視する]
- [コンピューティングリソースを監視]
- [ストレージ容量を監視]
- [ストレージパフォーマンスを監視]
- [コンピューティング利用率を監視]

NetApp HCC ダッシュボードにアクセスします

1. Webブラウザで管理ノードのIPアドレスを開きます。例：

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

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

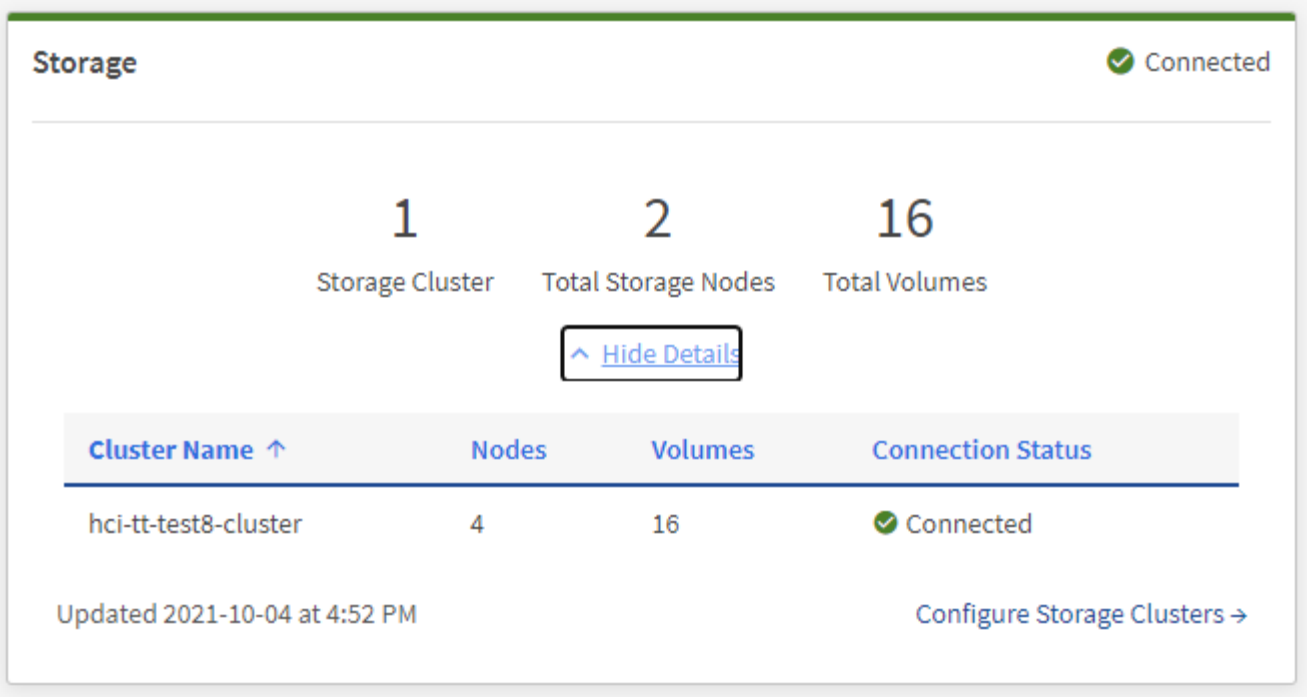


インストール環境によっては、これらのペインの一部またはすべてが表示されます。たとえば、ストレージのみのインストールの場合、 Hybrid Cloud Control Dashboard には、 Storage ペイン、 Storage Capacity ペイン、および Storage Performance ペインのみが表示されます。

ストレージリソースを監視する

「 * ストレージ * 」パネルを使用して、ストレージ環境全体を確認します。ストレージクラスタ、ストレージノード、およびボリュームの総数を監視できます。

詳細を表示するには、 Storage （ストレージ）ペインで * Show Details （詳細の表示） * を選択します。



合計ストレージノード数には、 2 ノードストレージクラスタからの監視ノードは含まれません。監視ノードは、そのクラスタの詳細セクションのノード番号に含まれます。

最新のストレージクラスタデータを表示するには、ストレージクラスタページを使用します。ダッシュボードよりもポーリングの頻度が高くなります。

コンピューティングリソースを監視

コンピューティング環境の種類を「 * Compute * 」パネルで確認してください。コンピューティングクラスタの数とコンピューティングノードの総数を監視できます。

詳細を表示するには、計算ペインで * 詳細を表示 * を選択します。

vCenter インスタンスは、少なくとも 1 つの NetApp HCI コンピューティングノードがそのインスタンスに関連付けられている場合にのみコンピューティングペインに表示されます。NetApp Hybrid Cloud Control にリンクされている vCenter インスタンスを一覧表示するには、を使用します "API"。

NetApp Hybrid Cloud Control でコンピューティングノードを管理するには、が必要です "コンピューティングノードを vCenter ホストクラスタに追加します"。

ストレージ容量を監視

環境のストレージ容量を監視することが重要です。Storage Capacity ペインを使用すると、圧縮、重複排除、シンプロビジョニングの各機能を有効または無効にして、ストレージ容量の効率化による効果を確認できます。

クラスタ内で使用可能な物理ストレージの合計スペースは、 **raw** タブに表示されます。また、プロビジョニングされたストレージに関する情報は、 *Effective * タブに表示されます。

クラスタの健常性を確認するには、 SolidFire Active IQ のダッシュボードも参照してください。を参照してください "NetApp SolidFire Active IQ で、パフォーマンス、容量、クラスタの健全性を監視します"。

手順

1. Raw タブを選択して、クラスタ内で使用済みおよび使用可能な物理ストレージの合計容量を表示します。

   縦の線を見て、使用済み容量が警告、エラー、または重大のしきい値を下回っていないかどうかを確認します。行にカーソルを合わせると詳細が表示されます。

   Warning のしきい値はデフォルトで Error のしきい値の 3% 下に設定できます。エラーしきい値とクリティカルしきい値は事前に設定されており、設計上の設定はできません。Error しきい値は、クラスタに容量が残っているノードが 1 つもないことを示します。しきい値の設定手順については、を参照してください "クラスタフルしきい値を設定しています"。

   関連するクラスタのしきい値 Element API の詳細については、を参照してください "「 getClusterFullThreshold 」" を Element ソフトウェア API ドキュメントで参照してください。ブロック容量とメタデータ容量の詳細については、を参照してください "クラスタフルレベルの概要" を参照してください。

2. 接続されているホストにプロビジョニングされている合計ストレージの情報を表示し、効率性の評価を表示するには、 * Effective * タブを選択します。

   a. 必要に応じて、 [シンプロビジョニングを含める] をオンにして、 [実効容量] 棒グラフでシンプロビジョニングの効率化率を確認します。

   b. * 実効容量の棒グラフ * ：縦の線を見て、使用済み容量が警告、エラー、または重大のしきい値を下回っていないかどうかを確認します。「 Raw 」タブと同様に、縦線にカーソルを合わせると詳細を確認できます。

   c. * 効率性 * ：上記の評価を参考に、圧縮機能、重複排除機能、シンプロビジョニング機能を有効にした場合のストレージ容量効率化の効果を判断してください。たとえば、圧縮率が「 1.3 倍」と表示される場合、圧縮を有効にした場合のストレージ効率は、圧縮を有効にしない場合と比べて 1.3 倍向上します。

> 総削減率は（ maxUsedSpace * efficiency factor ） /2 で、 efficiencyFactor = （ thinProvisioningFactor * deDuplicationFactor * compressionFactor ）です。このチェックボックスをオフにすると、合計効率には含まれません。

d. 実効ストレージ容量が Error または Critical のしきい値に近づく場合は、システムのデータをクリアすることを検討してください。または、システムの拡張を検討してください。

   を参照してください "拡張の概要"。

3. 詳細な分析と履歴のコンテキストについては、を参照してください "NetApp SolidFire Active IQ の詳細"。

ストレージパフォーマンスを監視

Storage Performance ペインを使用すると、クラスタから取得できる IOPS またはスループットを確認できます。このとき、リソースの有用なパフォーマンスを超過することはありません。ストレージパフォーマンスとは、レイテンシの問題が発生する前に利用率を最大限に高めるポイントです。

ストレージパフォーマンスペインでは、ワークロードが増加した場合にパフォーマンスが低下する可能性があるポイントにパフォーマンスが達していないかどうかを確認できます。

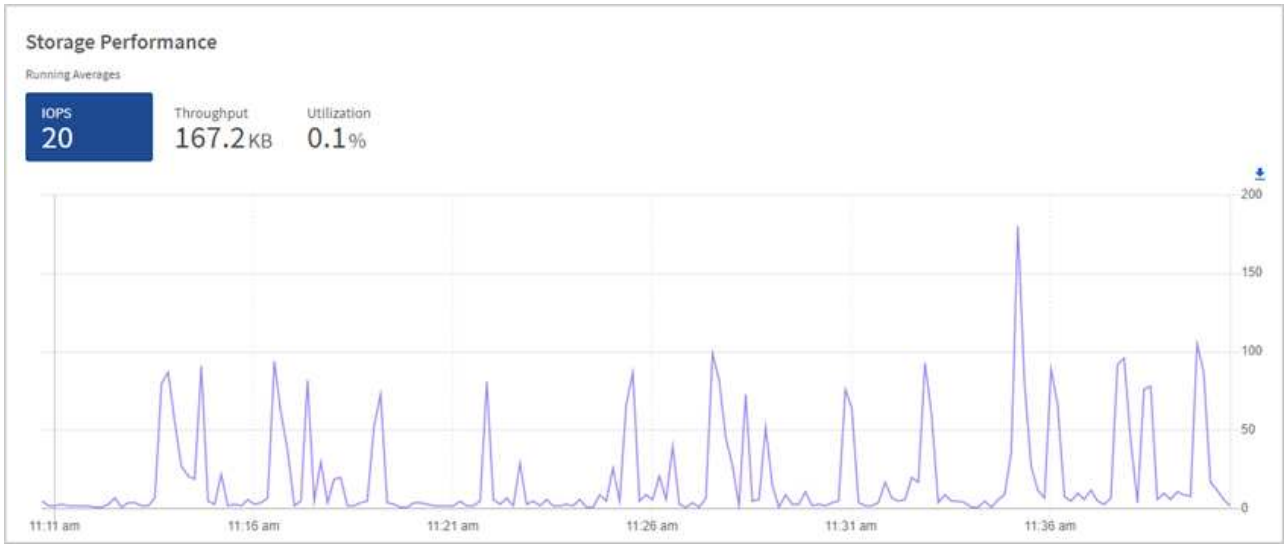
このペインの情報は 10 秒ごとに更新され、グラフ上のすべてのポイントの平均値が表示されます。

関連付けられている Element API メソッドの詳細については、を参照してください "GetClusterStats から参照できます" メソッド（ _Element ソフトウェア API ドキュメント内）。

手順

1. Storage Performance ペインを表示します。詳細については、グラフのポイントにカーソルを合わせます。

   a. * IOPS * タブ： 1 秒あたりの現在の処理数を表示します。データや急増しているデータを探す。たとえば、最大 IOPS が 160K で、そのうち 10 万 IOPS が空き IOPS または使用可能 IOPS であることが確認された場合は、このクラスタにワークロードを追加することを検討してください。一方、使用可能な容量が 140K しかない場合は、ワークロードのオフロードやシステムの拡張を検討してください。



   b. * Throughput * タブ：スループットのパターンまたはスパイクを監視します。また、スループットの

値が継続的に高くなっていないかどうかも監視します。リソースの使用率が最大値に近づいていることを示している可能性があります。

c. * Utilization * タブ： IOPS の利用率を、クラスタレベルで合計した使用可能な合計 IOPS を監視します。

2. さらに詳しい分析を行うには、 NetApp Element Plug-in for vCenter Server を使用してストレージのパフォーマンスを確認してください。

   "NetApp Element Plug-in for vCenter Server に表示されるパフォーマンス"。

コンピューティング利用率を監視

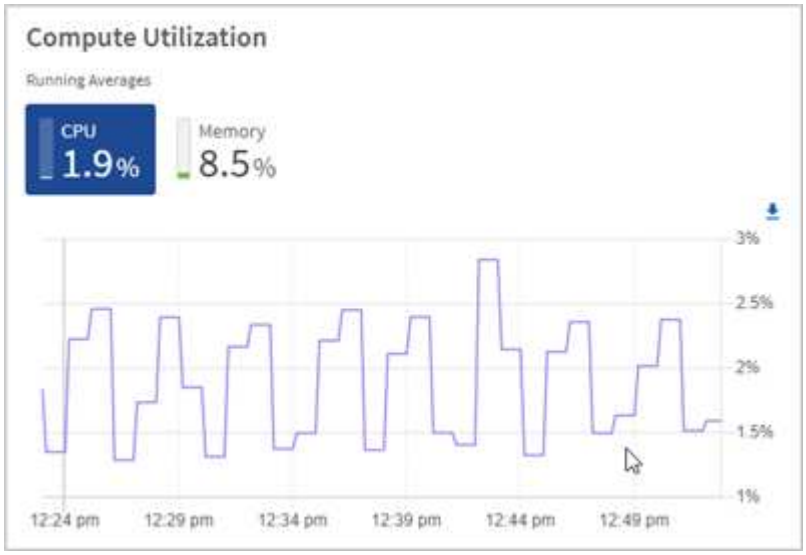
ストレージリソースの IOPS とスループットだけでなく、コンピューティングアセットの CPU とメモリの使用量も確認することができます。ノードで提供可能な合計 IOPS は、 CPU の数、 CPU の速度、 RAM の容量など、ノードの物理仕様に基づきます。

手順

1. [* Compute Utilization] ペインを表示します。CPU タブとメモリタブの両方を使用して、使用率のパターンまたはスパイクを探します。コンピューティングクラスタの最大利用率に近づいている可能性があるこ

とを示す、継続的な高使用率も確認します。

> このペインには、このインストールで管理されているコンピューティングクラスタのデータのみが表示されます。



a. * CPU * タブ：コンピューティングクラスタの CPU 利用率の現在の平均値を表示します。

b. * Memory * タブ：コンピューティングクラスタの現在の平均メモリ使用量を確認します。

2. コンピューティング情報の詳細な分析については、を参照してください "履歴データ用の NetApp SolidFire Active IQ"。

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 Active IQ のドキュメント"

ノードページでインベントリを表示します

システム内のストレージアセットとコンピューティングアセットの両方を表示し、それらの IP アドレス、名前、およびソフトウェアバージョンを確認することができます。

複数のノードシステム、および 2 ノードまたは 3 ノードクラスタに関連付けられた NetApp HCI 監視ノードのストレージ情報を表示できます。状況 "カスタムの保護ドメイン" が割り当てられている場合、特定のノードに割り当てられている保護ドメインを確認できます。

監視ノードはクラスタ内のクォーラムを管理します。監視ノードはストレージには使用されません。監視ノードは NetApp HCI のみに該当し、オールフラッシュストレージ環境には該当しません。

監視ノードの詳細については、を参照してください "ノードの定義"。

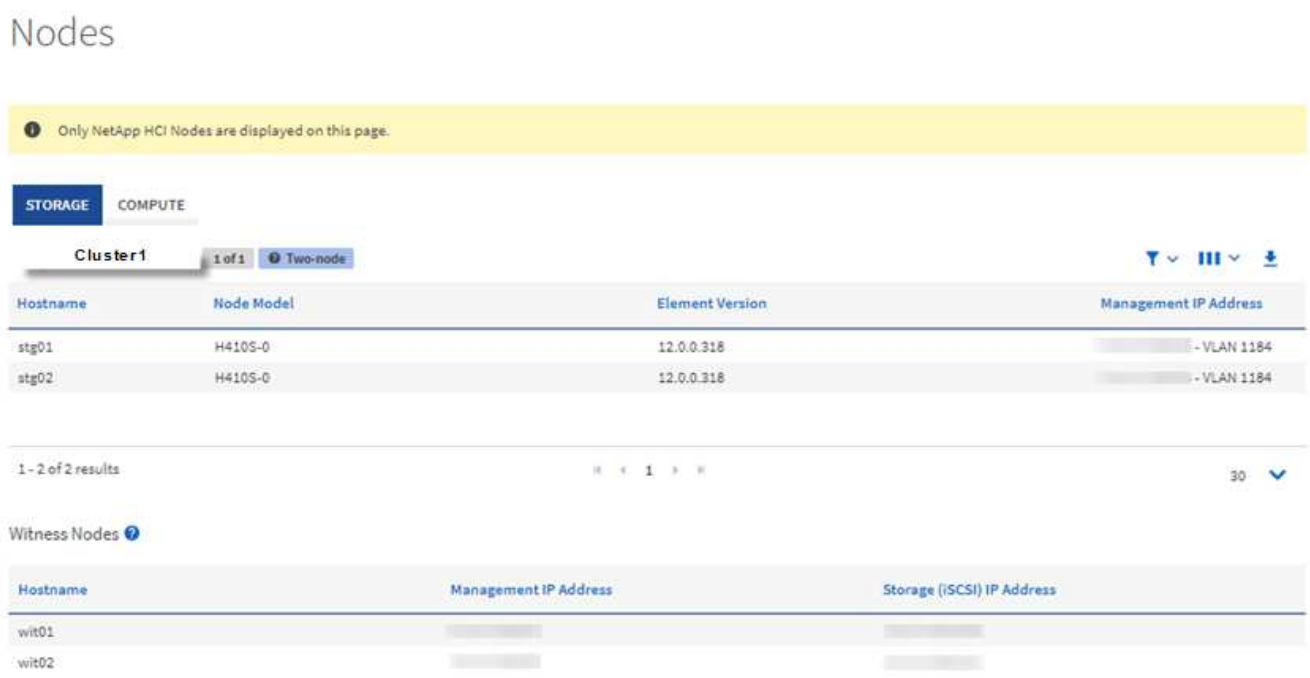
SolidFire エンタープライズ SDS ノードの場合、 [ストレージ] タブでインベントリを監視できます。

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。例：

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

2. NetApp HCI ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
3. 左側のナビゲーションで、 * ノード * をクリックします。



> 新しい NetApp Hybrid Cloud Control セッションを初めて起動したときは、管理ノードで多数のクラスタを管理しているときに NetApp Hybrid Cloud Control Nodes ページのロードに時間がかかることがあります。ロードにかかる時間は、管理ノードでアクティブに管理されているクラスタの数によって異なります。その後の起動では、読み込み時間が短縮されます。

4. Nodes ページの * Storage * タブで、次の情報を確認します。
   a. 2 ノードクラスタ： [Storage] タブには [2 ノード] ラベルが表示され、関連する監視ノードが表示されます。
   b. 3 ノードクラスタ：ストレージノードと関連する監視ノードが表示されます。3 ノードクラスタでは、ノード障害が発生した場合の高可用性を維持するために、監視ノードがスタンバイに導入されます。
   c. 4 ノード以上のクラスタ： 4 ノード以上のクラスタに関する情報が表示されます。監視ノードは適用されません。2 つまたは 3 つのストレージノードから開始してノードを追加しても、監視ノードは表示されたままです。指定しない場合、監視ノードのテーブルは表示されません。
   d. ファームウェアバンドルバージョンは 2.14 以降です。 Element 12.0 以降を実行しているクラスタがある場合は、これらのクラスタのファームウェアバンドルバージョンを確認できます。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は、「 * Firmware Bundle Version * 」列に「 * multiple * 」と表示されます。

e. カスタム保護ドメイン：カスタムの保護ドメインがクラスタで使用されている場合、クラスタ内の各ノードのカスタムの保護ドメインの割り当てを確認できます。カスタムの保護ドメインが有効になっていない場合は、この列は表示されません。

5. コンピューティングインベントリ情報を表示するには、 * Compute * をクリックします。
6. これらのページの情報は、いくつかの方法で操作できます。
   a. 結果の項目のリストをフィルタするには、 * フィルタ * アイコンをクリックしてフィルタを選択します。フィルタのテキストを入力することもできます。
   b. 列を表示または非表示にするには、 * 列の表示 / 非表示 * アイコンをクリックします。
   c. テーブルをダウンロードするには、 * ダウンロード * アイコンをクリックします。
   d. BMC 接続エラーが発生しているコンピューティングノード用に保存されている BMC クレデンシャルを追加または編集するには、「 * BMC Connection Status * 」列のエラーメッセージテキストで「 * Edit connection settings * 」をクリックします。コンピューティングノードの接続試行が失敗した場合にのみ、そのノードのこの列にエラーメッセージが表示されます。

ストレージリソースとコンピューティングリソースの数を表示するには、 NetApp Hybrid Cloud Control （ HCC ）ダッシュボードを参照します。を参照してください "HCC ダッシュボードを使用してストレージリソースとコンピューティングリソースを監視する"。

NetApp Hybrid Cloud Control でコンピューティングノードを管理するには、が必要です "コンピューティングノードを vCenter ホストクラスタに追加します"。

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

ベースボード管理コントローラの接続情報を編集します

ベースボード管理コントローラ（ BMC ）の管理者クレデンシャルは、各コンピューティングノードの NetApp Hybrid Cloud Control で変更できます。BMC ファームウェアをアップグレードする前に資格情報を変更したり、 NetApp Hybrid Cloud Control に表示される「 Hardware ID not available 」（ハードウェア ID が利用できません）または「 Unable to detect 」（検出できません）のエラーを解決したりする必要があります。

必要なもの

BMC クレデンシャルを変更するためのクラスタ管理者の権限。

ヘルスチェック時に BMC クレデンシャルを設定した場合、変更が * Nodes * ページに反映されるまでに最大 2 分かかることがあります。

オプション（ **Options** ）

BMC クレデンシャルを変更するには、次のいずれかのオプションを選択します。

- NetApp Hybrid Cloud Control を使用して BMC の情報を編集します

- BMC の情報を編集するには、 REST API を使用します

NetApp Hybrid Cloud Control を使用して BMC の情報を編集します

保存されている BMC クレデンシャルは、 NetApp Hybrid Cloud Control Dashboard を使用して編集できます。

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。例：

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

2. NetApp HCI ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
3. 左側のナビゲーション青いボックスで、 NetApp HCI のインストールを選択します。

   NetApp Hybrid Cloud Control Dashboard が表示されます。

4. 左側のナビゲーションで、 * ノード * をクリックします。
5. コンピューティングインベントリ情報を表示するには、 * Compute * をクリックします。

   コンピューティングノードのリストが表示されます。「 * BMC Connection Status * 」列には、各コンピューティングノードでの BMC 接続試行の結果が表示されます。コンピューティングノードの接続試行が失敗した場合は、そのノードのエラーメッセージがこの列に表示されます。

6. BMC 接続エラーが発生しているコンピューティングノード用に保存されている BMC クレデンシャルを追加または編集するには、エラーメッセージテキストで * 接続設定の編集 * をクリックします。
7. 表示されるダイアログで、このコンピューティングノードの BMC に対応する正しい管理者ユーザ名とパスワードを追加します。
8. [保存（ Save ）] をクリックします。
9. 保存されている BMC クレデンシャルが不足しているコンピューティングノードまたは正しくないコンピューティングノードに対して、手順 6~8 を繰り返します。

> BMC の情報を更新すると、インベントリが更新され、管理ノードのサービスで、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認識されるようになります。

BMC の情報を編集するには、 REST API を使用します

保存されている BMC クレデンシャルは、 NetApp Hybrid Cloud Control REST API を使用して編集できます。

手順

1. コンピューティングノードのハードウェアタグと BMC の情報を確認します。
   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）をクリックして、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 * をクリックします。
   iv. 承認ウィンドウを閉じます。
c. REST API UI で、 * GET / Installations * をクリックします。
d. [* 試してみてください *] をクリックします。
e. [* Execute] をクリックします。
f. 応答から ' インストール資産 ID (id`) をコピーします
g. REST API UI で、 * GET / Installations / ｛ id ｝ * をクリックします。
h. [* 試してみてください *] をクリックします。
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] をクリックします。
k. 応答から、後の手順で使用するために、ノードのアセット ID （「 id` 」）、 BMC の IP アドレス（「 bmcAddress 」）、ノードのシリアル番号（「 chassisSerialNumber 」）をコピーして保存します。

```
"nodes": [
  {
    "bmcDetails": {
      "bmcAddress": "10.117.1.111",
      "credentialsAvailable": false,
      "credentialsValidated": false
    },
    "chassisSerialNumber": "221111019323",
    "chassisSlot": "C",
    "hardwareId": null,
    "hardwareTag": "00000000-0000-0000-0000-ac1f6ab4ecf6",
    "id": "8cd91e3c-1b1e-1111-b00a-4c9c4900b000",
```

2. 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/
```

3. 「 * Authorize * 」（認証）をクリックして、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 * をクリックします。

d. ウィンドウを閉じます。

4. PUT /nodes / ｛hardware_id｝ * をクリックします。
5. [* 試してみてください *] をクリックします。
6. 先ほど保存したノードアセット ID を 'hardware_id' パラメータに入力します
7. ペイロードに次の情報を入力します。

パラメータ	説明
「 assetid="" 」と入力します	手順 1 (f) で保存したインストール資産 ID (id')
「 BMCIP 」	手順 1 （ k ）で保存した BMC の IP アドレス（「 bmcAddress 」）。
bmcPassword	BMC にログインするための更新されたパスワード。
「 bmcUsername 」と入力します	BMC にログインするために更新されたユーザ名。
'erialNumber'	ハードウェアのシャーシのシリアル番号。

ペイロードの例：

```
{
  "assetId": "7bb41e3c-2e9c-2151-b00a-8a9b49c0b0fe",
  "bmcIp": "10.117.1.111",
  "bmcPassword": "mypassword1",
  "bmcUsername": "admin1",
  "serialNumber": "221111019323"
}
```

8. [* Execute] をクリックして、 BMC クレデンシャルを更新します。成功すると、次のような応答が返されます。

```
{
  "credentialid": "33333333-cccc-3333-cccc-333333333333",
  "host_name": "hci-host",
  "id": "8cd91e3c-1b1e-1111-b00a-4c9c4900b000",
  "ip": "1.1.1.1",
  "parent": "abcd01y3-ab30-1ccc-11ee-11f123zx7d1b",
  "type": "BMC"
}
```

詳細については、こちらをご覧ください

- "コンピューティングノードのアップグレードに関する既知の問題と対処方法"

- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

ストレージクラスタのボリュームを監視する

SolidFire システムは、ボリュームを使用してストレージをプロビジョニングします。ボリュームは、 iSCSI または Fibre Channel クライアントがネットワーク経由でアクセスするブロックデバイスです。ボリュームに関連付けられているアクセスグループ、アカウント、イニシエータ、使用済み容量、 Snapshot データ保護のステータス、 iSCSI セッションの数、およびサービス品質（ QoS ）ポリシーに関する詳細を監視できます。

また、アクティブボリュームと削除されたボリュームの詳細も確認できます。

このビューでは、最初に使用済み容量の列を監視することを推奨します。

この情報にアクセスできるのは、 NetApp Hybrid Cloud Control の管理者権限がある場合のみです。

手順

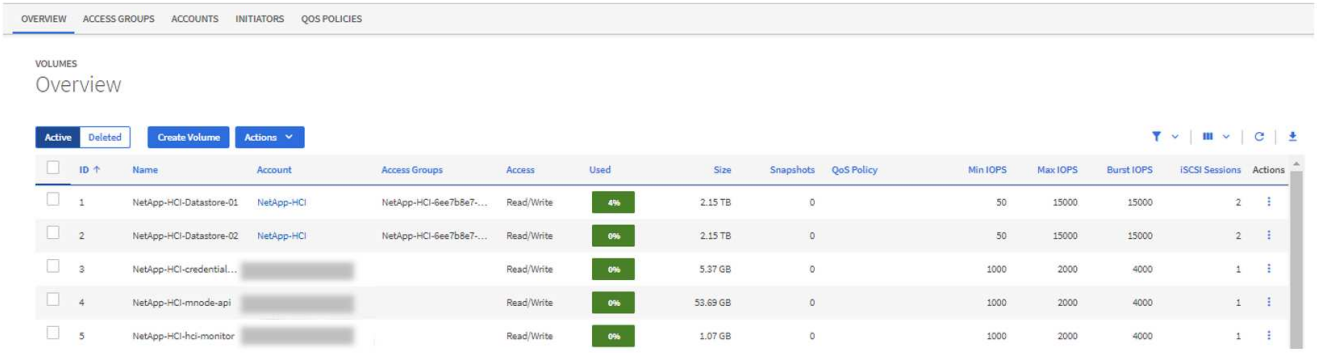
1. Webブラウザで管理ノードのIPアドレスを開きます。例：

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

2. NetApp HCI ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
3. 左側のナビゲーション青いボックスで、 NetApp HCI のインストールを選択します。

   Hybrid Cloud Control Dashboard が表示されます。

4. 左側のナビゲーションで、クラスタを選択し、 * Storage * > * Volumes * を選択します。



5. Volumes （ボリューム）ページで、次のオプションを使用します。

   a. [* フィルタ * （ * Filter * ）] アイコンをクリックして、結果をフィルタ処理します。

b. 列を非表示または表示するには、 * 非表示 / 表示 * アイコンをクリックします。

c. [更新 * （ Refresh ）] アイコンをクリックして、データを更新します。

d. 「 * ダウンロード * 」アイコンをクリックして CSV ファイルをダウンロードします。

6. 使用済み容量の列を監視します。警告、エラー、または重大のしきい値に達すると、使用済み容量のステータスが色で示されます。

   a. 警告 - 黄色

   b. エラー - オレンジ

   c. Critical - 赤

7. ボリュームビューで、タブをクリックしてボリュームのその他の詳細を確認します。

   a. * アクセスグループ * ：イニシエータから一連のボリュームにマッピングされたボリュームアクセスグループを表示して、アクセスを保護できます。

      については、を参照してください "ボリュームアクセスグループ"。

   b. * アカウント * ：クライアントがノード上のボリュームに接続できるようにするユーザアカウントを表示できます。ボリュームには、作成時に特定のユーザアカウントが割り当てられます。

      については、を参照してください "NetApp HCI ユーザアカウント"。

   c. * イニシエータ * ：ボリュームの iSCSI イニシエータ IQN または Fibre Channel WWPN を確認できます。アクセスグループに追加された各 IQN は、 CHAP 認証なしでグループ内の各ボリュームにアクセスできます。アクセスグループに追加された各 WWPN は、アクセスグループ内のボリュームへの Fibre Channel ネットワークアクセスを許可します。

   d. * QoS ポリシー * ：ボリュームに適用されている QoS ポリシーを確認できます。QoS ポリシーは、最小 IOPS 、最大 IOPS 、バースト時の IOPS の標準的な設定を複数のボリュームに適用します。

      については、を参照してください "パフォーマンスポリシーと QoS ポリシー"。

詳細については、こちらをご覧ください

- "SolidFire および Element のドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

SolidFire Active IQ を使用して、パフォーマンス、容量、クラスタの健全性を監視できます

SolidFire Active IQ を使用して、クラスタのイベント、パフォーマンス、容量を監視できます。SolidFire Active IQ には、 NetApp Hybrid Cloud Control Dashboard からアクセスできます。

- 始める前に *
- このサービスを利用するには、ネットアップサポートアカウントが必要です。

- 管理ノード REST API を使用するための許可が必要です。
- バージョン 12.0 以降を実行する管理ノードを導入しておきます。
- クラスタバージョンで NetApp Element ソフトウェア 12.0 以降が実行されています。
- インターネットにアクセスできる。Active IQ コレクタサービスをダークサイトから使用することはできません。
- このタスクについて * クラスタ全体の統計の履歴ビューを継続的に更新できます。クラスタで指定したイベント、しきい値、または指標について、通知を設定して迅速に対処できるようにすることができます。

ネットアップサポートは、通常のサポート契約の一環として、このデータを監視し、潜在的なシステムの問題をユーザに警告します。

- 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。例：

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

2. NetApp HCI ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
3. ダッシュボードの右上にあるメニューを選択します。
4. 「 * View Active IQ * 」を選択します。

   。 "SolidFire Active IQ ダッシュボード" 表示されます。

5. SolidFire Active IQ の詳細については、を参照してください "SolidFire Active IQ のドキュメント"。

   右上のメニューアイコンを選択して「* SolidFire Active IQ 」を選択すると、ダッシュボードからのドキュメントにアクセスすることもできます。

6. SolidFire Active IQ インターフェイスで、 NetApp HCI のコンピューティングノードとストレージノードから Active IQ にテレメトリが正しく報告されていることを確認します。
   a. 複数のNetApp HCI がインストールされている場合は、「*クラスタの選択」を選択し、リストからクラスタを選択します。
   b. 左側のナビゲーションペインで、 * ノード * を選択します。
7. リストに表示されないノードがある場合は、ネットアップサポートにお問い合わせください。

> ストレージリソースとコンピューティングリソースの数を表示するには、 Hybrid Cloud Control （ HCC ）ダッシュボードを参照します。を参照してください "HCC ダッシュボードを使用してストレージリソースとコンピューティングリソースを監視する"。

詳細については、こちらをご覧ください

- "NetApp SolidFire Active IQ のドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

トラブルシューティング用にログを収集する

NetApp HCI または SolidFire オールフラッシュストレージの設置で問題が発生した場合、ネットアップサポートに送信するログを収集して診断を支援できます。NetApp Hybrid Cloud Control または REST API を使用して、 NetApp HCI または Element システムのログを収集できます。

必要なもの

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

ログ収集オプション

次のいずれかのオプションを選択します。

- NetApp Hybrid Cloud Control を使用してログを収集します
- REST API を使用してログを収集する

NetApp Hybrid Cloud Control を使用してログを収集します

ログ収集領域には、 NetApp Hybrid Cloud Control のダッシュボードからアクセスできます。

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。例：

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

2. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
3. ダッシュボードの右上にあるメニューをクリックします。
4. [**Collect Logs**] を選択します。

   [**Collect Logs**] ページが表示されます。以前にログを収集したことがある場合は、既存のログパッケージをダウンロードするか、新しいログ収集を開始できます。

5. **Date Range** ドロップダウンメニューで日付範囲を選択し、ログに含める日付を指定します。

   カスタムの開始日を指定する場合は、日付範囲を開始する日付を選択できます。ログは、その日付から現時点まで収集されます。

6. ［ * ログ収集 * ］ セクションで、ログ・パッケージに含めるログ・ファイルのタイプを選択します。

   ストレージとコンピューティングのログの場合は、ストレージノードまたはコンピューティングノードのリストを展開し、ログを収集するノード（またはリスト内のすべてのノード）を個別に選択できます。

7. ログ収集を開始するには、 * ログ収集 * をクリックします。

ログ収集がバックグラウンドで実行され、ページに進捗状況が表示されます。

> 収集したログによっては、進捗状況バーが数分間一定のパーセンテージで表示されるか、または非常に遅い時点で進行している可能性があります。

8. [ログのダウンロード] をクリックして、ログパッケージをダウンロードします。

   ログパッケージは、圧縮された unix.tgz ファイル形式です。

REST API を使用してログを収集する

REST API を使用して NetApp HCI ログまたは Element ログを収集できます。

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>/logs/1/
      ```

   b. 「 * Authorize * 」（認証）をクリックして、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 * をクリックします。
2. NetApp HCI または Element からログを収集します。
   a. [**POST/BUNDLE**](POST / バンドル) をクリック
   b. [* 試してみてください *] をクリックします。
   c. 収集する必要があるログのタイプおよび期間に応じて、「 * Request body * 」フィールドで次のパラメータの値を変更します。

パラメータ	を入力します	説明
「変更されたシンセ」	日付文字列	この日時以降に変更されたログのみを含めます。たとえば、「 20-07-14T20 ： 19 ： 00.000Z 」という値は、 2020 年 7 月 14 日 20 ： 19 UTC の開始日を定義します。
「 computeLogs 」を参照してください	ブール値	コンピューティング・ノード・ログを含めるには ' このパラメータを TRUE に設定します

パラメータ	を入力します	説明
「 computeIds 」	UUID の配列	「 computeLogs 」が「 true 」に設定されている場合、このパラメータにコンピューティングノードの管理ノードアセット ID を入力して、ログ収集を特定のコンピューティングノードに制限します。GET を使用します https://<ManagementNodeIP>/logs/1/bundle/options` 使用可能なすべてのノード ID が表示されます。
「ムノドノグス」	ブール値	管理ノードのログを含めるには、このパラメータを「 true 」に設定します。
「 torageCrashDumps 」を参照してください	ブール値	ストレージ・ノード・クラッシュ・デバッグ・ログを含めるには、このパラメータを「 true 」に設定します。
'torageLogs'	ブール値	ストレージ・ノード・ログを含めるには、このパラメータを「 true 」に設定します。
「 torageNodeIds 」	UUID の配列	「 torageLogs 」が「 true 」に設定されている場合は、ログ収集を特定のストレージノードに制限するために、このパラメータにストレージクラスタのノード ID を入力します。GET を使用します https://<ManagementNodeIP>/logs/1/bundle/options` 使用可能なすべてのノード ID が表示されます。

d. [*Execute] をクリックして ' ログ収集を開始します次のような応答が返されます。

```
{
  "_links": {
    "self": "https://10.1.1.5/logs/1/bundle"
  },
  "taskId": "4157881b-z889-45ce-adb4-92b1843c53ee",
  "taskLink": "https://10.1.1.5/logs/1/bundle"
}
```

3. ログ収集タスクのステータスを確認します。

   a. [**Get/Bundle**] をクリックします。

   b. [* 試してみてください *] をクリックします。

c. 収集タスクのステータスを返すには、 [*Execute] をクリックします。

d. 応答の本文の一番下までスクロールします。

   コレクションの進行状況を示す「 percentComplete 」属性が表示されます。コレクションが完了すると、「 Download Link 」属性には、ログパッケージのファイル名を含む完全なダウンロードリンクが含まれます。

e. 「 downloadLink 」属性の末尾にファイル名をコピーします。

4. 収集したログパッケージをダウンロードします。

   a. [**get/bundle/{filename}**] をクリックします。

   b. [* 試してみてください *] をクリックします。

   c. 先ほどコピーしたファイル名を 'filename' パラメータテキストフィールドに貼り付けます

   d. [* Execute] をクリックします。

      実行後、応答の本文領域にダウンロードリンクが表示されます。

   e. [ファイルのダウンロード] をクリックし、結果のファイルをコンピューターに保存します。

      ログパッケージは、圧縮された unix.tgz ファイル形式です。

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 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。

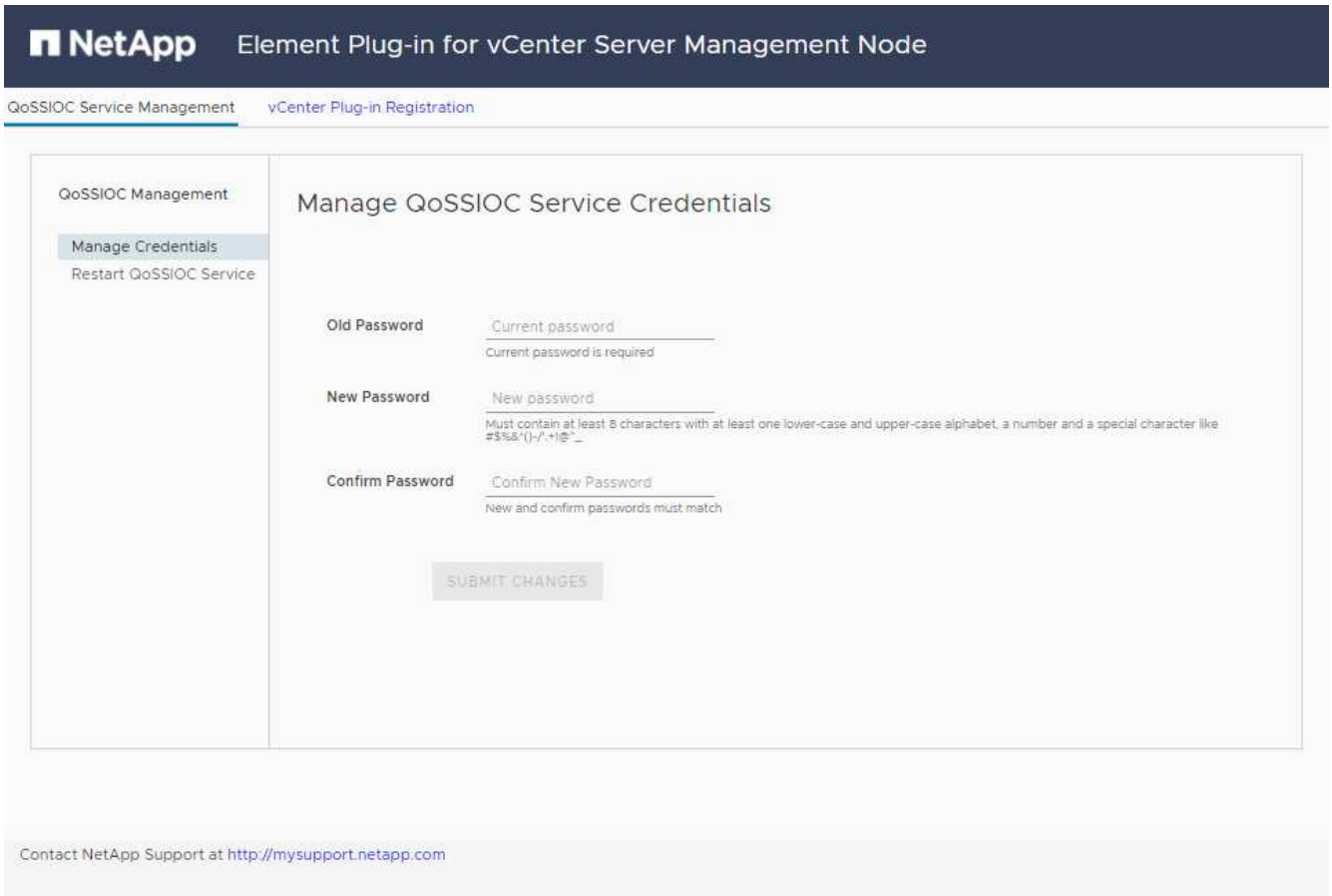
> このプラグインは、 HTML5 vSphere Web Client バージョン 6.7 U2 ビルド 13007421 および更新 2a より前にリリースされたその他の 6.7 U2 ビルド（ビルド 13643870 ）とは互換性がありません。サポートされる vSphere のバージョンの詳細については、のリリースノートを参照してください "プラグインのバージョン"。

必要なもの

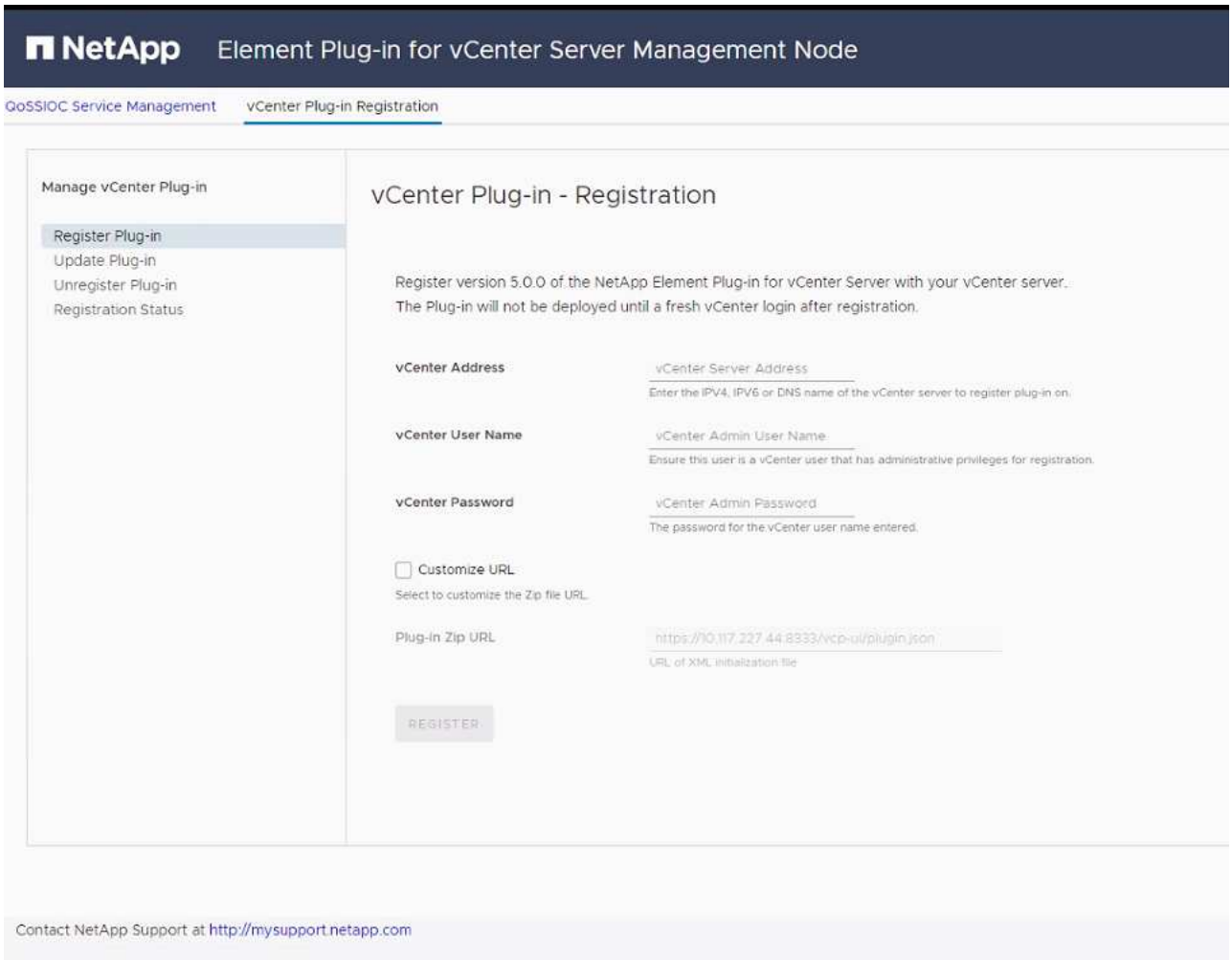
- * 管理者権限 * ：プラグインをインストールするための vCenter Administrator ロールの権限があります。
- * vSphere のアップグレード * ： NetApp Element Plug-in for vCenter Server をアップグレードする前に、必要な vCenter のアップグレードを実行しておきます。以下の手順は、 vCenter のアップグレードが完了していることを前提としています。
- * vCenter Server ：**vCenter Plug-in**バージョン**5.x**または**4.x**が**vCenter Server**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

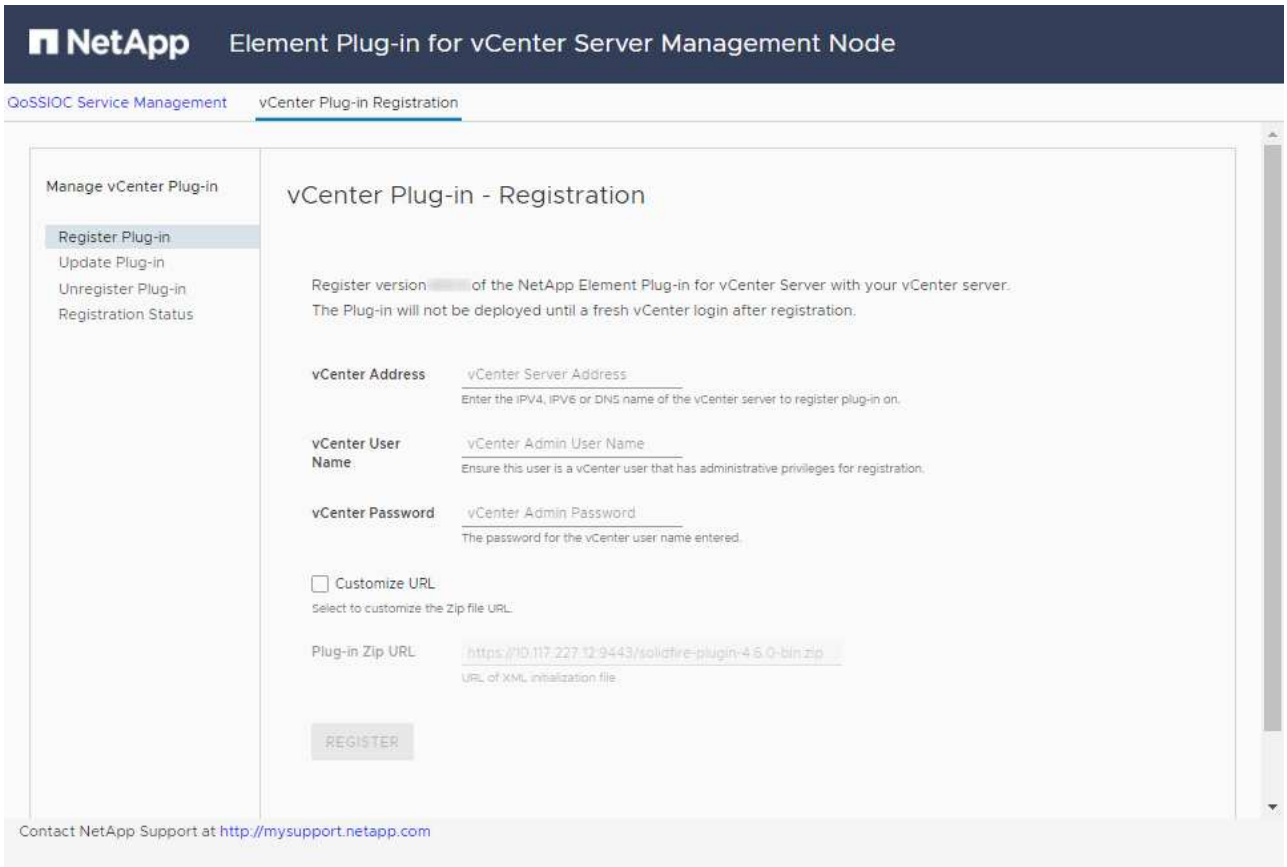
1. ブラウザに管理ノードの IP アドレスを入力します。登録用の TCP ポート「 https://[management node ip 」： 9443 でこのプラグインの登録ユーティリティ UI が開き、「 Manage QoSSIOC Service Credentials * 」ページが表示されます。



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。

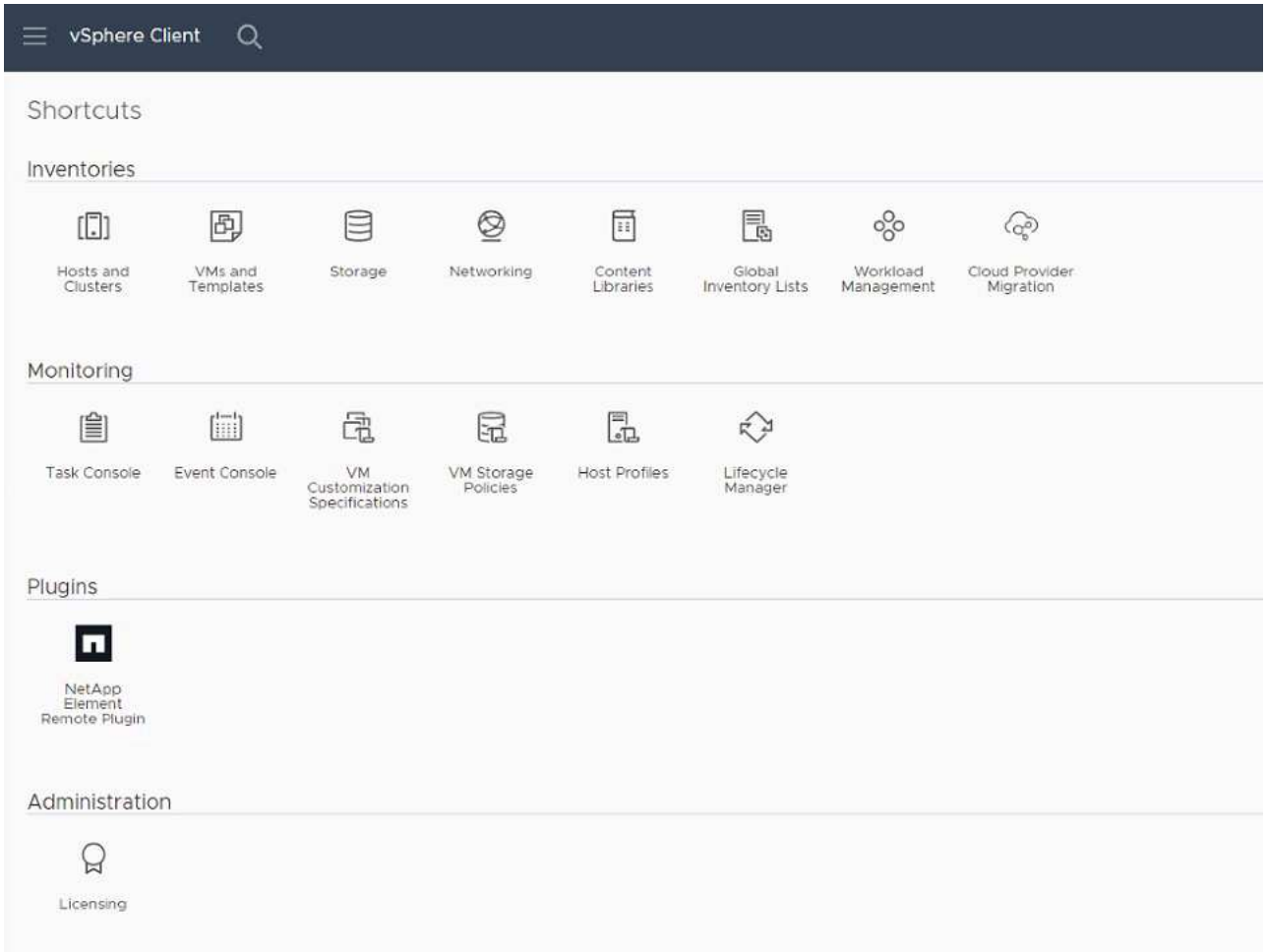
5. 「 * Update * 」を選択します。

   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。

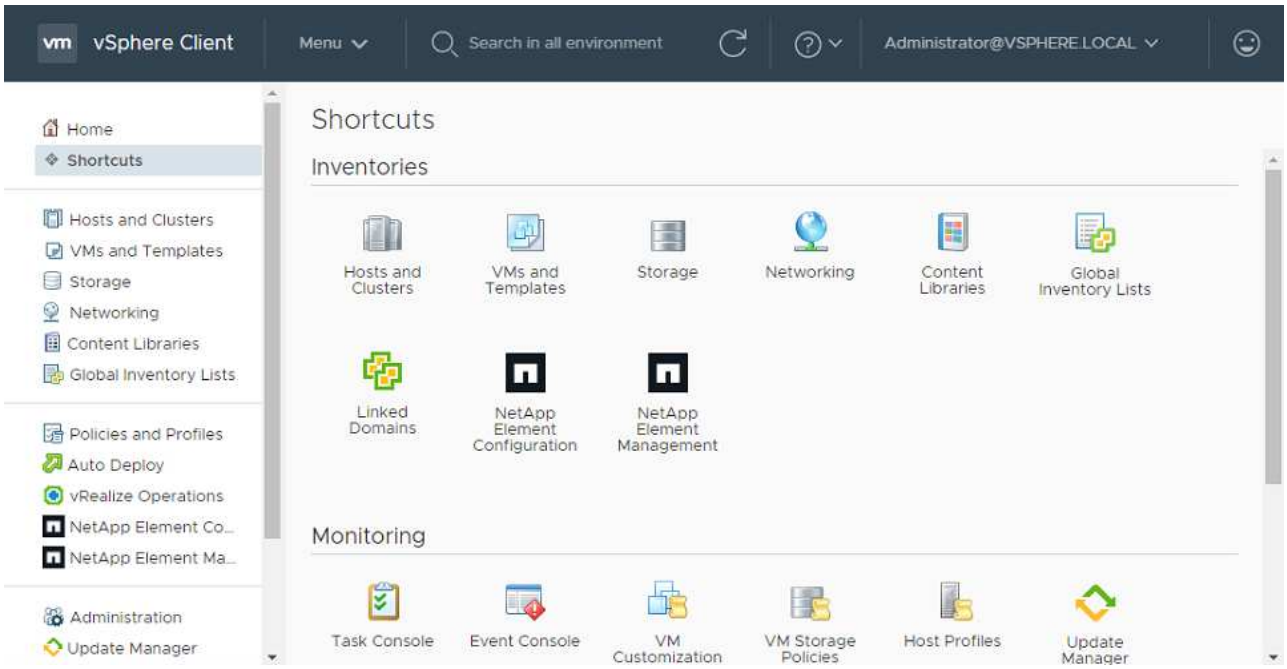
6. vSphere Web Client に vCenter Administrator としてログインします。vSphere Web Client にすでにログインしている場合は、ログアウトし、 2~3 分待ってから再度ログインする必要があります。

   > 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

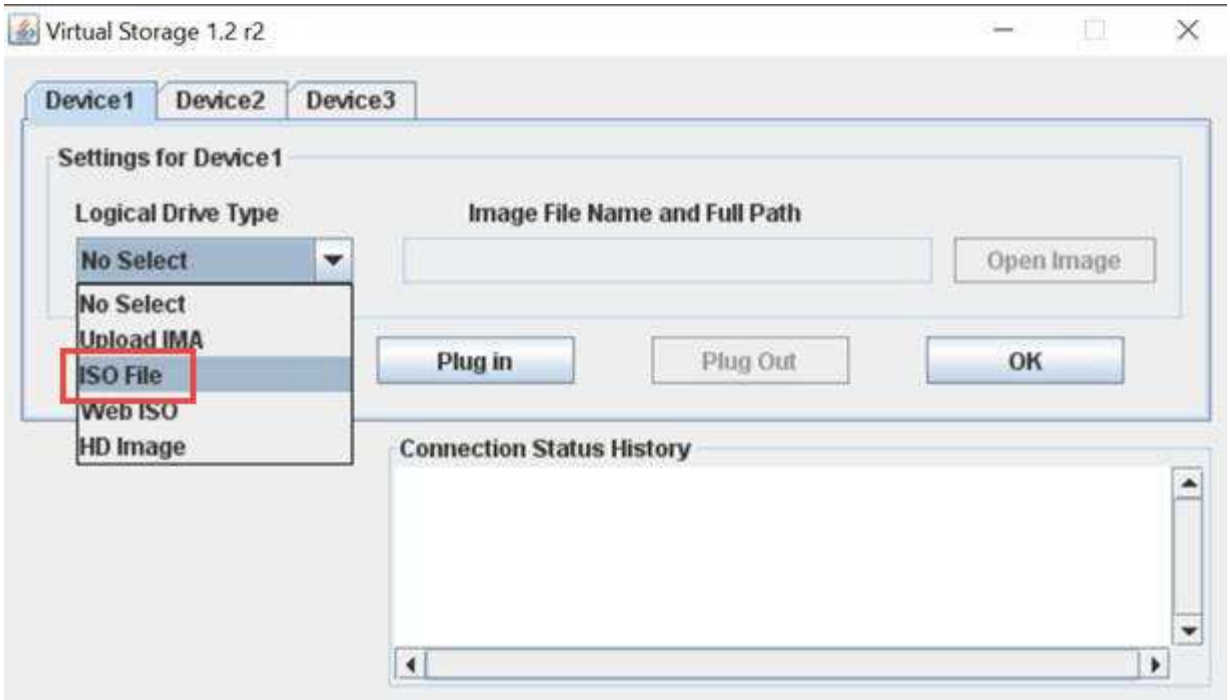
1. ノードがクラスタに参加している場合は、次のように保守モードにします。ない場合は、手順 2 に進みます。
   a. VMware vCenter Web Client にログインします。
   b. ホスト（コンピューティングノード）名を右クリックし、 * メンテナンスモード > メンテナンスモードへの切り替え * を選択します。
   c. 「 * OK 」を選択します。ホスト上の VM は、使用可能な別のホストに移行されます。移行する VM の数によっては、 VM の移行に時間がかかることがあります。

      > 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。

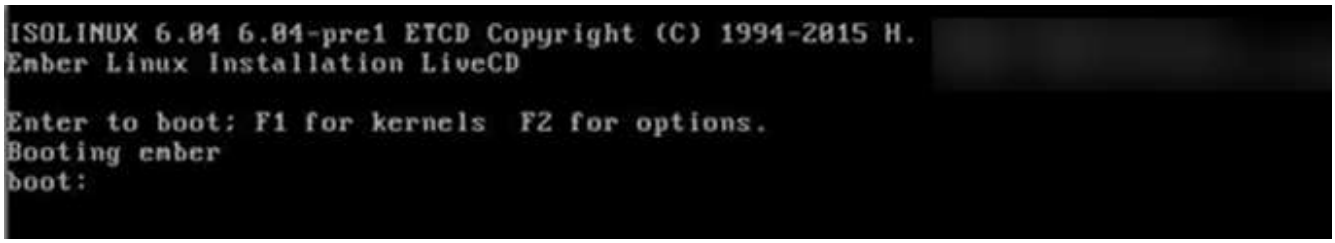
   > Java のインストールまたは更新が必要になる場合があります。

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。

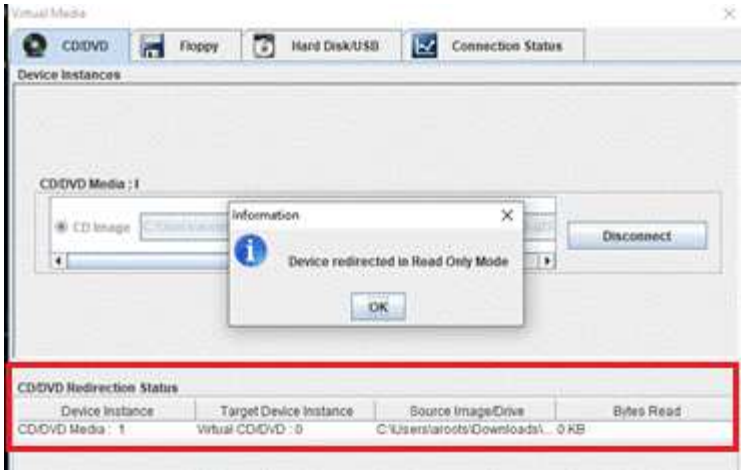
手順

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"

NetApp HCI システムを拡張します

拡張の概要

NetApp HCI システムは、 NetApp Hybrid Cloud Control を使用して拡張できます。ストレージリソースとコンピューティングリソースは、個別に拡張することも、同時に拡張することもできます。

> 新規およびスペアの H610S ストレージノードには、既存の Element ソフトウェアバージョンのストレージクラスタに基づいて追加のインストール要件がある場合があります。詳細については、ネットアップサポートにお問い合わせください。

NetApp HCI シャーシにノードを設置したら、 NetApp Hybrid Cloud Control を使用して、新しいリソースを使用するように NetApp HCI を設定します。NetApp HCI は既存のネットワーク設定を検出し、既存のネットワークと VLAN （存在する場合）内に設定オプションを提供します。

> インストール環境を拡張したあとに新しいアセットが構成に自動的に追加されなかった場合は、アセットを手動で追加しなければならないことがあります。を参照してください "管理ノードの概要"。

NetApp HCI は、 VMware Enhanced vMotion Compatibility （ EVC ）を使用して、 vSphere クラスタに CPU 世代が異なる複数のコンピューティングノードがある場合の vMotion を可能にします。拡張に EVC が必要な場合、 NetApp HCI は可能な場合は自動的に EVC を有効にします。

次の場合は、 vSphere クライアントで EVC の設定を手動で変更しなければならないことがあります。

- 既存のコンピューティングノードの CPU 世代が追加するコンピューティングノードよりも新しい。
- 制御用 vCenter インスタンスで必要な EVC レベルがサポートされていない。
- 追加するコンピューティングノードの CPU 世代が制御用 vCenter インスタンスの EVC 設定よりも古い。

> NetApp Deployment Engine で NetApp HCI のコンピューティングリソースまたはストレージリソースを拡張する場合は、既存の NetApp HCI コンピューティングノードを管理する vCenter インスタンスに接続してください。

詳細については、こちらをご覧ください

- "NetApp HCI コンピューティングリソースを展開します"
- "NetApp HCI ストレージリソースを展開します"
- "NetApp HCI のストレージリソースとコンピューティングリソースも同時に拡張します 時間"
- "NetApp HCI のリソースページ"
- "vCenter Server 向け NetApp Element プラグイン"

NetApp HCI ストレージリソースを展開します

NetApp HCI の導入が完了したら、ネットアップハイブリッドクラウド制御を使用して NetApp HCI のストレージリソースを拡張および設定できます。

作業を開始する前に

- 既存のノードと同じネットワークセグメントに未使用の空いている IPv4 アドレスがあることを確認してください（新しいノードは、同じタイプの既存のノードと同じネットワークにインストールする必要があります）。
- 次のいずれかのタイプの SolidFire ストレージクラスタアカウントがあることを確認しておきます。
  - 初期導入時に作成されたネイティブの管理者アカウント
  - Cluster Admin 、 Drives 、 Volumes 、 Nodes の各権限を持つカスタムユーザアカウント
- 新しいノードごとに次の操作を実行しておきます。
  - を使用して、新しいノードを NetApp HCI シャーシに設置します に従ってください "インストール手順"。
  - 新しいノードのケーブルを配線して電源をオンにします
- 設置済みのストレージノードの管理 IPv4 アドレスを確認しておきます。IP アドレスは、 NetApp Element Plug-in for vCenter Server の * NetApp Element Management* > * Cluster * > * Nodes * タブで確認できます。
- 新しいノードのネットワークトポロジとケーブル配線が既存のストレージクラスタまたはコンピューティングクラスタと同じであることを確認しておきます。

> ストレージリソースを拡張する際は、最大限の信頼性を実現するためにストレージ容量をすべてのシャーシに均等に分割してください。

手順

1. Webブラウザで管理ノードのIPアドレスを開きます。例：

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

2. NetApp HCI ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
3. インターフェイスの右上隅にある * Expand * をクリックします。

   ブラウザに NetApp Deployment Engine が表示されます。

4. ローカルのNetApp HCIストレージクラスタ管理者のクレデンシャルを指定してNetApp Deployment Engineにログインします。

   > Lightweight Directory Access Protocolのクレデンシャルを使用してログインすることはできません。

5. [ようこそ *] ページで、 [* いいえ *] をクリックし、 [続行] をクリックします。

6. [使用可能なインベントリ *] ページで、追加するストレージノードを選択し、 [続行 *] をクリックします。
7. [* ネットワークの設定 *] ページで、初期導入時に一部のネットワーク情報が検出されました。シリアル番号順に表示された新しいストレージノードのそれぞれについて、新しいネットワーク情報を割り当てる必要があります。新しいストレージノードごとに、次の手順を実行します。
   a. * ホスト名 *: NetApp HCI が名前のプレフィックスを検出した場合は、 [検出された名前のプレフィックス] フィールドから名前のプレフィックスをコピーし、 [ホスト名] フィールドに追加した新しい一意のホスト名のプレフィックスとして挿入します。
   b. * 管理アドレス * ：管理ネットワークサブネットにある新しいストレージノードの管理 IP アドレスを入力します。
   c. * ストレージ（ iSCSI ） IP アドレス * ： iSCSI ネットワークサブネット内にある新しいストレージノードの iSCSI IP アドレスを入力します。
   d. [* Continue （続行）] をクリックします

   入力した IP アドレスの検証には時間がかかることがあります。 NetApp HCIIP アドレス検証が完了すると、 Continue （続行）ボタンが使用可能になります。

8. [ネットワーク設定] セクションの [* レビュー] ページでは、新しいノードが太字で表示されます。セクションを変更するには、次の手順を実行します。
   a. そのセクションの * 編集 * をクリックします。
   b. 終了したら、以降のページで [* Continue （続行）] をクリックして [レビュー] ページに戻ります。
9. * オプション * ：ネットアップがホストする Active IQ サーバにクラスタの統計情報とサポート情報を送信しない場合は、最後のチェックボックスをオフにします。

   これにより、 NetApp HCI のリアルタイムの健常性診断の監視機能が無効になります。この機能を無効にすると、ネットアップによる NetApp HCI のプロアクティブなサポートと監視が行われなくなるため、本番環境が影響を受ける前に問題を検出して解決できなくなります。

10. [ノードの追加] をクリックします。

    リソースの追加と設定の進捗状況は、 NetApp HCI で監視できます。

11. * オプション * ：新しいストレージノードが Element Plug-in for vCenter Server に表示されることを確認します。

    2 ノードストレージクラスタを 4 ノード以上に拡張した場合でも、ストレージクラスタで以前に使用されていた監視ノードのペアは、 vSphere ではスタンバイ仮想マシンとして表示されます。新しく拡張したストレージクラスタでは使用されません。 VM リソースを再利用する場合は、を実行します "手動で削除します" 監視ノードの仮想マシン。

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 コンピューティングリソースを展開します

NetApp HCI の導入が完了したら、ネットアップハイブリッドクラウド制御を使用して NetApp HCI コンピューティングリソースを拡張および設定できます。

作業を開始する前に

- 分散仮想スイッチを使用している環境を拡張する場合は、 NetApp HCI の vSphere インスタンスで vSphere Enterprise Plus ライセンスが使用されていることを確認してください。
- NetApp HCI で使用しているすべての vCenter インスタンスと vSphere インスタンスでライセンス期間が終了していないことを確認しておきます。
- 既存のノードと同じネットワークセグメントに未使用の空いている IPv4 アドレスがあることを確認してください（新しいノードは、同じタイプの既存のノードと同じネットワークにインストールする必要があります）。
- vCenter 管理者アカウントのクレデンシャルを準備しておきます。
- 新しいノードごとに次の操作を実行しておきます。
  - を使用して、新しいノードを NetApp HCI シャーシに設置します に従ってください "インストール手順"。
  - 新しいノードのケーブルを配線して電源をオンにします
- 新しいノードのネットワークトポロジとケーブル配線が既存のストレージクラスタまたはコンピューティングクラスタと同じであることを確認しておきます。

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。例：

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

2. NetApp HCI ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
3. インターフェイスの右上隅にある * Expand * をクリックします。

   ブラウザに NetApp Deployment Engine が表示されます。

4. ローカルのNetApp HCIストレージクラスタ管理者のクレデンシャルを指定してNetApp Deployment Engineにログインします。

   Lightweight Directory Access Protocolのクレデンシャルを使用してログインすることはできません。

5. [ようこそ *] ページで、 [はい] をクリックし、 [続行] をクリックします。
6. [* エンドユーザライセンス *] ページで、 VMware エンドユーザライセンス契約を読み、 [* I accept （同意します）] をクリックして条項に同意し、 [* Continue （続行）] をクリックします。
7. vCenter * ページで、次の手順を実行します。
   a. NetApp HCI 環境に関連付けられている vCenter インスタンスの FQDN または IP アドレスと管理者の

クレデンシャルを入力します。

b. [* Continue （続行）] をクリックします

c. コンピューティングノードを追加する vSphere データセンターを選択するか、 * 新しいデータセンターの作成 * をクリックして、コンピューティングノードを新しいデータセンターに追加します。

> Create New Datacenter をクリックすると、 Cluster フィールドに自動的に値が入力されます。

d. 既存のデータセンターを選択した場合は、新しいコンピューティングノードを関連付ける vSphere クラスタを選択します。

> 拡張対象として選択したクラスタのネットワーク設定を NetApp HCI が認識できない場合は、管理、ストレージ、 vMotion ネットワーク用の VMkernel と vmnic マッピングが導入時のデフォルトに設定されていることを確認してください。を参照してください "サポートされるネットワーク変更" を参照してください。

e. [* Continue （続行）] をクリックします

8. ESXi クレデンシャル * ページで、追加するコンピューティングノードの ESXi root パスワードを入力します。

   NetApp HCI の初期導入時に作成したパスワードを使用する必要があります。

9. [* Continue （続行）] をクリックします

10. 新しい vSphere データセンタークラスタを作成した場合は、「 * ネットワークトポロジ * 」ページで、追加する新しいコンピューティングノードと一致するネットワークトポロジを選択します。

> ケーブル 2 本のオプションを選択するのは、コンピューティングノードがケーブル 2 本のトポロジを使用しており、既存の NetApp HCI 環境に VLAN ID が設定されている場合のみです。

11. Available Inventory * ページで、既存の NetApp HCI 環境に追加するノードを選択します。

> 一部のコンピューティングノードでは、 vCenter のバージョンでサポートされている最高レベルで EV を有効にしないと、インストール環境に追加できない場合があります。そのようなコンピューティングノードについては、 vSphere クライアントを使用して EVC を有効にする必要があります。有効にしたら、インベントリページをリフレッシュし、コンピューティングノードの追加をもう一度実行してください。

12. [* Continue （続行）] をクリックします

13. * オプション * ：新しい vSphere データセンタークラスタを作成した場合、 * ネットワーク設定 * ページで、既存の NetApp HCI 環境から * 既存のクラスタから設定をコピー * チェックボックスを選択してネットワーク情報をインポートします。

    これにより、各ネットワークにデフォルトゲートウェイとサブネットの情報が設定されます。

14. [* ネットワークの設定 *] ページで、初期導入時に一部のネットワーク情報が検出されました。シリアル番号順に表示された新しいコンピューティングノードのそれぞれについて、新しいネットワーク情報を割り当てる必要があります。新しいコンピューティングノードごとに、次の手順を実行します。

a. * ホスト名 *: NetApp HCI が名前のプレフィックスを検出した場合は、 [検出された名前のプレフィックス *] フィールドから名前のプレフィックスをコピーし、新しいホスト名のプレフィックスとして挿入します。

b. * 管理 IP アドレス * ：管理ネットワークサブネットにある新しいコンピューティングノードの管理 IP アドレスを入力します。

c. * vMotion IP Address * ： vMotion ネットワークサブネット内の新しいコンピューティングノードに vMotion IP アドレスを入力します。

d. * iSCSI A-IP アドレス * ： iSCSI ネットワークサブネットにあるコンピューティングノードの最初の iSCSI ポートの IP アドレスを入力します。

e. * iscsi B-IP Address * ： iSCSI ネットワークサブネットにあるコンピューティングノードの 2 番目の iSCSI ポートの IP アドレスを入力します

f. [* Continue （続行）] をクリックします

15. [ネットワーク設定] セクションの [* レビュー] ページでは、新しいノードが太字で表示されます。セクションを変更するには、次の手順を実行します。

    a. そのセクションの * 編集 * をクリックします。

    b. 終了したら、その後のページで [* Continue * （続行）] をクリックして、 [* Review * （レビュー）] ページに戻ります。

16. * オプション * ：ネットアップがホストする SolidFire Active IQ サーバにクラスタの統計情報とサポート情報を送信しない場合は、最後のチェックボックスをオフにします。

    これにより、 NetApp HCI のリアルタイムの健常性診断の監視機能が無効になります。この機能を無効にすると、ネットアップによる NetApp HCI のプロアクティブなサポートと監視が行われなくなるため、本番環境が影響を受ける前に問題を検出して解決できなくなります。

17. [ノードの追加] をクリックします。

    リソースの追加と設定の進捗状況は、 NetApp HCI で監視できます。

18. * オプション * ：新しいコンピューティングノードが VMware vSphere Web Client に表示されることを確認します。

詳細については、こちらをご覧ください

- "NetApp HCI のリソースページ"
- "NetApp HCI コンピューティングノードとストレージノードの設置とセットアップの手順"
- "VMware のナレッジベース：「 Enhanced vMotion Compatibility （ EVC ） processor support"

NetApp HCI のストレージリソースとコンピューティングリソースも同時に拡張します 時間

NetApp HCI の導入が完了したら、 NetApp Hybrid Cloud Control を使用して、 NetApp HCI のストレージリソースとコンピューティングリソースを同時に拡張および設定することができます。

作業を開始する前に

- 分散仮想スイッチを使用している環境を拡張する場合は、 NetApp HCI の vSphere インスタンスで vSphere Enterprise Plus ライセンスが使用されていることを確認してください。
- NetApp HCI で使用しているすべての vCenter インスタンスと vSphere インスタンスでライセンス期間が終了していないことを確認しておきます。
- vCenter 管理者アカウントのクレデンシャルを準備しておきます。
- 既存のノードと同じネットワークセグメントに未使用の空いている IPv4 アドレスがあることを確認してください（新しいノードは、同じタイプの既存のノードと同じネットワークにインストールする必要があります）。
- 次のいずれかのタイプの SolidFire ストレージクラスタアカウントがあることを確認しておきます。
  - 初期導入時に作成されたネイティブの管理者アカウント
  - Cluster Admin 、 Drives 、 Volumes 、 Nodes の各権限を持つカスタムユーザアカウント
- 新しいノードごとに次の操作を実行しておきます。
  - を使用して、新しいノードを NetApp HCI シャーシに設置します に従ってください "インストール手順"。
  - 新しいノードのケーブルを配線して電源をオンにします
- 設置済みのストレージノードの管理 IPv4 アドレスを確認しておきます。IP アドレスは、 NetApp Element Plug-in for vCenter Server の * NetApp Element Management* > * Cluster * > * Nodes * タブで確認できます。
- 新しいノードのネットワークトポロジとケーブル配線が既存のストレージクラスタまたはコンピューティングクラスタと同じであることを確認しておきます。

このタスクについて

- H410C コンピューティングノードは、 NetApp HCI の既存のコンピューティングノードやストレージノードと同じシャーシおよびクラスタに混在させることができます。
- コンピューティングノードと BPU 対応のコンピューティングノードを同じクラスタ内に混在させることはできません。GPU 対応のコンピューティングノードを選択すると、 CPU のみのコンピューティングノードは選択できなくなります。その逆も同様です。
- CPU 世代が既存のコンピューティングノードと異なるコンピューティングノードを追加する場合は、 Enhanced vMotion Compatibility （ EVC ）を有効にする必要があります。制御用 vCenter インスタンスで EVC が無効になっている場合は、有効にしてから次に進んでください。これにより、拡張完了後に vMotion を使用できます。

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。例：

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

2. NetApp HCI ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
3. インターフェイスの右上隅にある * Expand * をクリックします。

   ブラウザに NetApp Deployment Engine が表示されます。

4. ローカルのNetApp HCIストレージクラスタ管理者のクレデンシャルを指定してNetApp Deployment Engineにログインします。

> Lightweight Directory Access Protocolのクレデンシャルを使用してログインすることはできません。

5. [ようこそ *] ページで、 [はい] をクリックし、 [続行] をクリックします。
6. [* エンドユーザライセンス *] ページで、 VMware エンドユーザライセンス契約を読み、 [* I accept （同意します）] をクリックして条項に同意し、 [* Continue （続行）] をクリックします。
7. vCenter * ページで、次の手順を実行します。
   a. NetApp HCI 環境に関連付けられている vCenter インスタンスの FQDN または IP アドレスと管理者のクレデンシャルを入力します。
   b. [* Continue （続行）] をクリックします
   c. コンピューティングノードを追加する vSphere データセンターを選択するか、 * 新しいデータセンターの作成 * をクリックして、コンピューティングノードを新しいデータセンターに追加します。

   > Create New Datacenter をクリックすると、 Cluster フィールドに自動的に値が入力されます。

   d. 既存のデータセンターを選択した場合は、新しいコンピューティングノードを関連付ける vSphere クラスタを選択します。

   > 拡張対象として選択したクラスタのネットワーク設定を NetApp HCI が認識できない場合は、管理、ストレージ、 vMotion ネットワーク用の VMkernel と vmnic マッピングが導入時のデフォルトに設定されていることを確認してください。を参照してください "サポートされるネットワーク変更" を参照してください。

   e. [* Continue （続行）] をクリックします
8. ESXi クレデンシャル * ページで、追加するコンピューティングノードの ESXi root パスワードを入力します。

   NetApp HCI の初期導入時に作成したパスワードを使用する必要があります。

9. [* Continue （続行）] をクリックします
10. 新しい vSphere データセンタークラスタを作成した場合は、「 * ネットワークトポロジ * 」ページで、追加する新しいコンピューティングノードと一致するネットワークトポロジを選択します。

    > ケーブル 2 本のオプションを選択するのは、コンピューティングノードがケーブル 2 本のトポロジを使用しており、既存の NetApp HCI 環境に VLAN ID が設定されている場合のみです。

11. [使用可能なインベントリ *] ページで、追加するストレージノードとコンピューティングノードを選択し、 [続行] をクリックします。

> 一部のコンピューティングノードでは、 vCenter のバージョンでサポートされている最高レベルで EV を有効にしないと、インストール環境に追加できない場合があります。そのようなコンピューティングノードについては、 vSphere クライアントを使用して EVC を有効にする必要があります。有効にしたら、インベントリページをリフレッシュし、コンピューティングノードの追加をもう一度実行してください。

12. [* Continue （続行）] をクリックします
13. * オプション * ：新しい vSphere データセンタークラスタを作成した場合、 * ネットワーク設定 * ページで、既存の NetApp HCI 環境から * 既存のクラスタから設定をコピー * チェックボックスを選択してネットワーク情報をインポートします。

    これにより、各ネットワークにデフォルトゲートウェイとサブネットの情報が設定されます。

14. [* ネットワークの設定 *] ページで、初期導入時に一部のネットワーク情報が検出されました。シリアル番号順に表示された新しいストレージノードのそれぞれについて、新しいネットワーク情報を割り当てる必要があります。新しいストレージノードごとに、次の手順を実行します。
    a. * ホスト名 *: NetApp HCI が名前のプレフィックスを検出した場合は、 [検出された名前のプレフィックス] フィールドから名前のプレフィックスをコピーし、 [ホスト名] フィールドに追加した新しい一意のホスト名のプレフィックスとして挿入します。
    b. * 管理アドレス * ：管理ネットワークサブネットにある新しいストレージノードの管理 IP アドレスを入力します。
    c. * ストレージ（ iSCSI ） IP アドレス * ： iSCSI ネットワークサブネット内にある新しいストレージノードの iSCSI IP アドレスを入力します。
    d. [* Continue （続行）] をクリックします

    > 入力した IP アドレスの検証には時間がかかることがあります。 NetApp HCIIP アドレス検証が完了すると、 Continue （続行）ボタンが使用可能になります。

15. [ネットワーク設定] セクションの [* レビュー] ページでは、新しいノードが太字で表示されます。セクションを変更するには、次の手順を実行します。
    a. そのセクションの * 編集 * をクリックします。
    b. 終了したら、以降のページで [* Continue （続行）] をクリックして [レビュー] ページに戻ります。
16. * オプション * ：ネットアップがホストする Active IQ サーバにクラスタの統計情報とサポート情報を送信しない場合は、最後のチェックボックスをオフにします。

    これにより、 NetApp HCI のリアルタイムの健常性診断の監視機能が無効になります。この機能を無効にすると、ネットアップによる NetApp HCI のプロアクティブなサポートと監視が行われなくなるため、本番環境が影響を受ける前に問題を検出して解決できなくなります。

17. [ノードの追加] をクリックします。

    リソースの追加と設定の進捗状況は、 NetApp HCI で監視できます。

18. * オプション * ：新しいノードが VMware vSphere Web Client （コンピューティングノードの場合）または Element Plug-in for vCenter Server （ストレージノードの場合）に表示されることを確認します。

2 ノードストレージクラスタを 4 ノード以上に拡張した場合でも、ストレージクラスタで以前に使用されていた監視ノードのペアは、 vSphere ではスタンバイ仮想マシンとして表示されます。新しく拡張したストレージクラスタでは使用されません。 VM リソースを再利用する場合は、を実行します "手動で削除します" 監視ノードの仮想マシン。

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"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI コンピューティングノードとストレージノードの設置とセットアップの手順"
- "VMware のナレッジベース：「 Enhanced vMotion Compatibility （ EVC ） processor support"

クラスタの拡張後に監視ノードを削除します

2 ノードストレージクラスタを 4 つ以上のノードに拡張したら、監視ノードのペアを削除して、 NetApp HCI 環境のコンピューティングリソースを解放できます。以前ストレージクラスタで使用されていた監視ノードは、引き続き vSphere Web Client でスタンバイ仮想マシン（ VM ）として表示されます。

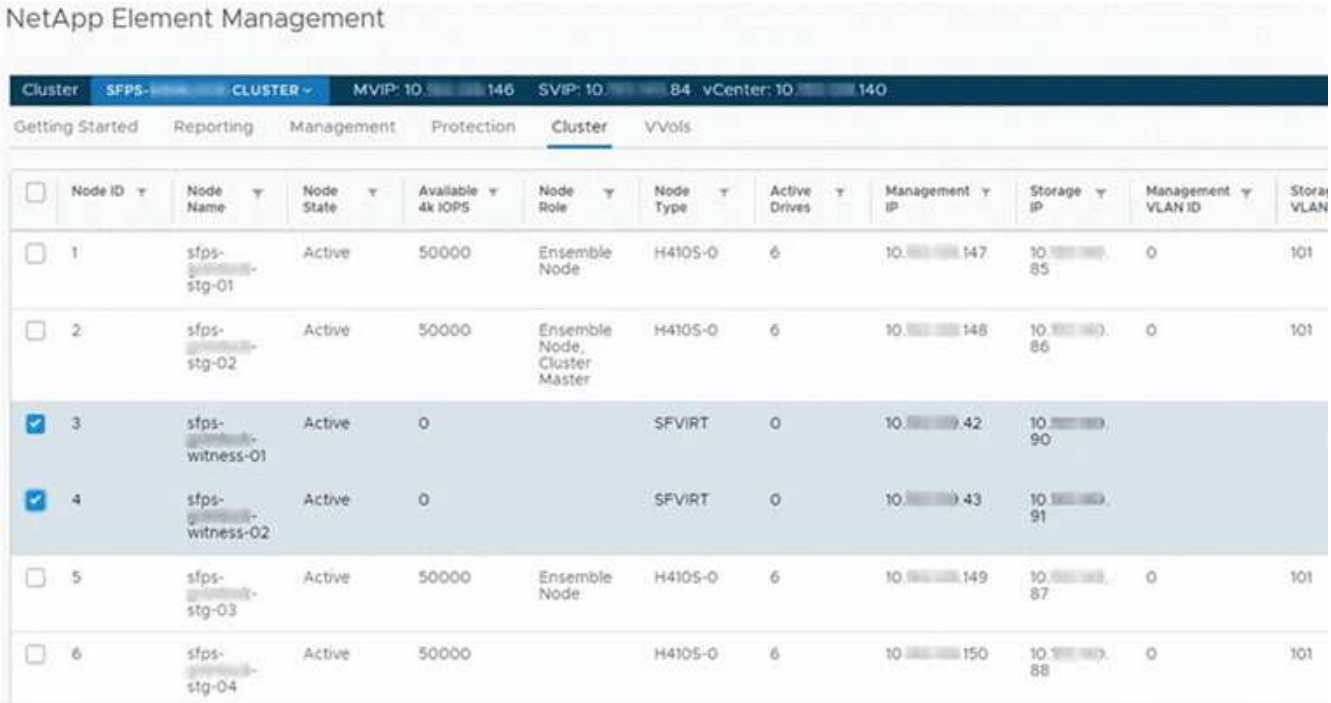
このタスクについて

監視ノードは、ストレージノードが 5 つ以上あるクラスタでは必要ありません。2 ノードクラスタを 4 つ以上のノードに拡張したあとに CPU とメモリを解放する場合は、この手順はオプションです。

クラスタの障害やエラーが報告されていないことを確認します。システムアラートに関する情報は、 vSphere の NetApp Element Management 拡張ポイントで、 * Reporting > Alerts * をクリックすると確認できます。

手順

1. vSphere から、 NetApp Element Management 拡張ポイントにアクセスするには、 * Shortcuts * タブまたはサイドパネルからアクセスします。
2. NetApp Element Management > Cluster > Nodes * の順に選択します。



3. 削除する監視ノードのチェックボックスを選択し、 * Actions > Remove * をクリックします。
4. プロンプトで操作を確認します。
5. [**Hosts and Clusters**] をクリックします。
6. 削除した監視ノード VM に移動します。
7. VM を右クリックして電源をオフにします。
8. 電源をオフにした VM を右クリックし、 * ディスクから削除 * をクリックします。
9. プロンプトで操作を確認します。

詳細については、こちらをご覧ください

- "NetApp HCI 2 ノードストレージクラスタ | TR-4823"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"
- "SolidFire と Element ソフトウェアドキュメントセンター"

NetApp HCI で Rancher を使用します

NetApp HCI の Rancher の概要

Rancher は、チームがコンテナを採用するための完全なソフトウェアスタックです。Rancher は、さまざまなインフラにわたって複数の Kubernetes クラスタを管理することによる運用上の課題とセキュリティ上の課題に対処しながら、 DevOps チームにコンテナ化されたワークロードを実行するための統合ツールを提供しています。

NetApp HCI に Rancher を導入すると、 Rancher コントロールプレーン（ *rancher server_* とも呼ばれます）が導入され、オンプレミスの Kubernetes クラスタを作成できます。Rancher コントロールプレーンを導入するには、 NetApp Hybrid Cloud Control を使用します。

導入後、 Rancher コントロールプレーンを使用して、開発チームと運用チームが使用する Kubernetes クラスタをプロビジョニング、管理、監視します。開発チームと運用チームは、 Rancher を使用して、 NetApp HCI 自体、パブリッククラウドプロバイダ、またはランチ元となるその他のインフラ上に存在するユーザクラスタに対してアクティビティを実行できます。

NetApp HCI の Rancher の利点

- インストールの容易さ： Rancher のインストールおよび設定方法を習得する必要はありません。NetApp HCI と Rancher が共同で開発したテンプレートベースの実装を展開できます。
- ライフサイクル管理：手動ランチサーバの実装では、ランチサーバアプリケーションまたは Rancher Kubernetes Engine （ RKE ）クラスタのアップデートは自動化されません。NetApp HCI の Rancher は、Rancher サーバおよび RKE を含む管理クラスタのアップデート機能を提供します。

NetApp HCI のランチマーでできること

NetApp HCI のランチマーを使用すると、次のことが可能になります。

- クラウドプロバイダとプライベートクラウドにまたがってサービスを導入できます。
- サービスレベル契約に違反せずに、クラウドの場所に関係なくハイブリッドクラウドアーキテクチャ全体でアプリとデータを移植できます。
- クラウドネイティブなアプリケーションを自分でスピンアップする。
- 複数のクラスタ（新規および既存）の一元管理。
- Kubernetes ベースのハイブリッドクラウドアプリケーションのオーケストレーションを実行

テクニカルサポートオプション

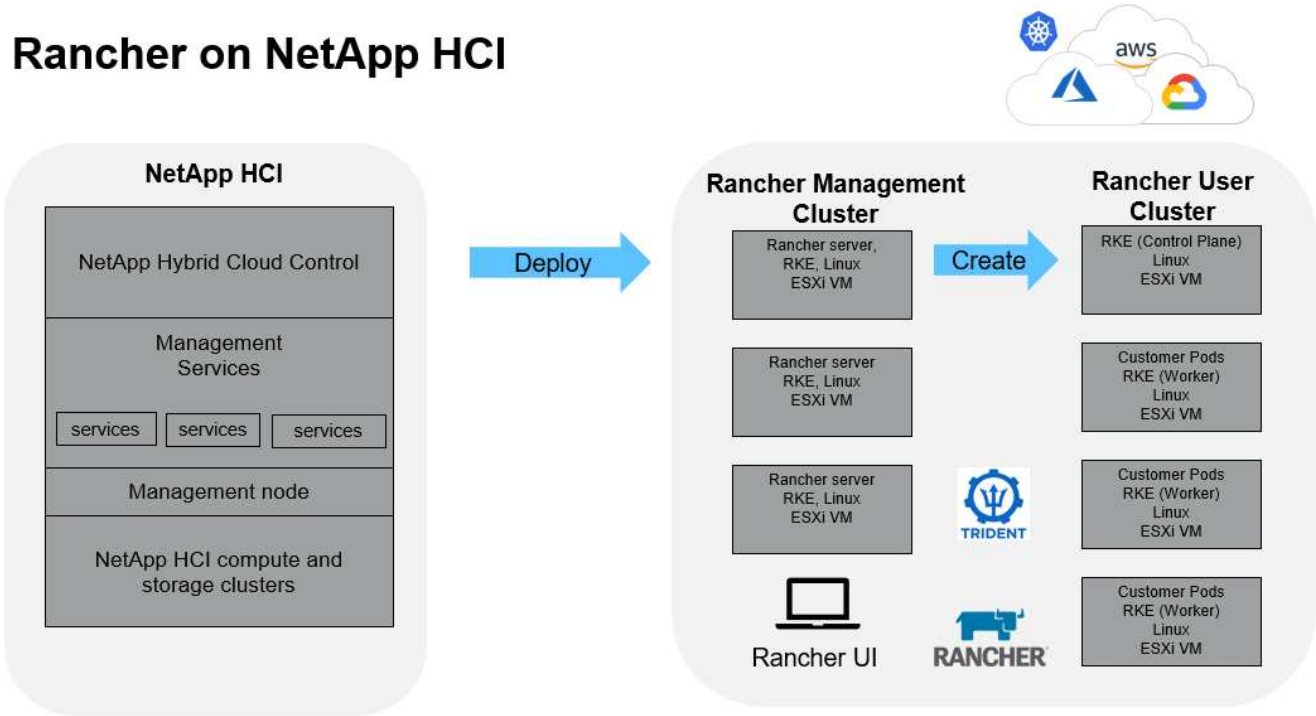
NetApp HCI と Kubernetes オープンソースソフトウェアで Rancher を使用すれば、無償での導入と使用が可能ライセンスキーは必要ありません。

ネットアップの Rancher サポートオプションを選択して、コアベースのエンタープライズサポートを入手できます。

Rancher サポートは、ネットアップサポートエッジ契約には含まれていません。オプションについては、ネットアップの営業担当者または代理店にお問い合わせください。ネットアップから Rancher サポートを購入された場合は、手順が記載された E メールをお送りします。

NetApp HCI のアーキテクチャとコンポーネントに関する Rancher

次に、 NetApp HCI の Rancher のさまざまなコンポーネントの概要を示します。



- * NetApp Hybrid Cloud Control * ：このインターフェイスを使用すると、 NetApp HCI のランチャに必要な NetApp HCI および NetApp Element ソフトウェアにランチャを導入できます。

  NetApp Hybrid Cloud Control を使用して、管理サービスのアップグレード、システムの拡張、ログの収集、インストール環境の監視も行うことができます。

- * 管理サービス * ：管理サービスは管理ノードで実行され、ネットアップハイブリッドクラウド制御を使用して NetApp HCI にランチャを導入できます。
- * 管理クラスタ * ： NetApp HCI の Rancher は、 Rancher 管理クラスタ上に 3 つの仮想マシンを導入しています。このクラスタでは、 NetApp Hybrid Cloud Control 、 vCenter Server 、または Rancher ユーザインターフェイスを使用して確認できます。管理クラスタの仮想マシンは、 Rancher サーバ、 Rancher Kubernetes Engine （ RKE ）、および Linux OS をホストします。

  最高のパフォーマンスとセキュリティを実現するために、ランチサーバ管理サーバ専用の Kubernetes クラスタを使用することを検討してください。管理クラスタではユーザワークロードを実行しないでください。

- * ユーザクラスタ * ：下流の Kubernetes ユーザクラスタでは、アプリケーションとサービスを実行します。Rancher から展開するクラスタ、または Rancher にインポートするクラスタは、ユーザクラスタです。

- * Trident * ： Trident カタログは、 NetApp HCI の Rancher で利用でき、ユーザクラスタで実行されます。このカタログが含まれているため、ユーザクラスタへの Trident の導入が簡単になります。

詳細については、こちらをご覧ください

- "アーキテクチャに関する Rancher ドキュメント"
- "NetApp HCI のリソースページ"

NetApp HCI の概念に関する Rancher

NetApp HCI の Rancher に関連する基本的な概念を学びます。

- * Rancher サーバー * または * コントロールプレーン * ： Rancher コントロールプレーン（ _ ランチエージェントサーバー _ と呼ばれることもあります）は、開発および運用チームが使用する Kubernetes クラスタをプロビジョニング、管理、監視します。
- * カタログ * ：カタログは GitHub リポジトリまたは Helm Chart リポジトリで、すぐに導入できるアプリケーションがいっぱいになっています。Rancher では、 Helm チャートのカタログを使用して、アプリケーションを繰り返し簡単に導入できます。Rancher には、組み込みのグローバルカタログとカスタムカタログの 2 種類のカタログが含まれています。Trident はカタログとして導入されています。を参照してください "カタログに関する Rancher のドキュメント"。
- * 管理クラスタ * ： NetApp HCI の Rancher は、 Rancher 管理クラスタに 3 台の仮想マシンを導入します。 Rancher 、 Hybrid Cloud Control 、および vCenter Plug-in を使用して確認できます。管理クラスタの仮想マシンは、 Rancher サーバ、 Rancher Kubernetes Engine （ RKE ）、および Linux OS をホストします。
- * ユーザクラスタ * ：これらのダウンストリーム Kubernetes クラスタは、アプリケーションとサービスを実行します。ランチサーバの Kubernetes 環境では、管理クラスタをユーザクラスタから分離する必要があります。Rancher ユーザーが rancher から展開するか、または rancher にインポートするクラスタは、ユーザークラスタと見なされます。
- * ランチャノードテンプレート * ： Hybrid Cloud Control では、ランチャノードテンプレートを使用して導入を簡易化しています。

  を参照してください "ノードテンプレートに関する Rancher のドキュメント"。

Trident ソフトウェアと永続的ストレージの概念

Trident は Kubernetes ネイティブのアプリケーションであり、 Kubernetes クラスタ内で直接実行されます。Trident を使用すると、 Kubernetes のユーザ（開発者、データサイエンティスト、 Kubernetes 管理者など）は、使い慣れた標準的な Kubernetes 形式で永続ストレージボリュームを作成、管理、操作できます。Trident を使用すると、 Kubernetes クラスタが作成した永続的ボリュームに対する要求をネットアップのソリューションで満たすことができます。

Rancher を使用すると、どのポッドからも独立して存在し、独自の有効期間を持つ永続ボリュームを使用できます。Trident を使用して Persistent Volume Claim （ PVC ；永続ボリューム要求）を管理することで、ポッドを作成する開発者は、アクセス対象のストレージの細かな実装作業から解放されます。

コンテナ化されたアプリケーションが永続的ボリューム要求（ PVC ）要求を発行すると、 Trident は要求されたパラメータを使用して、 NetApp HCI の NetApp Element ソフトウェアストレージレイヤにストレージを動的にプロビジョニングします。

Trident カタログは、 NetApp HCI 上の Rancher で利用でき、ユーザクラスタ内で実行されます。NetApp HCI 実装の Rancher の一部として、 Trident インストーラはデフォルトで rancher カタログから入手できます。このカタログが含まれているため、ユーザクラスタへの Trident の導入が簡単になります。

を参照してください "Trident を NetApp HCI に Rancher とともにインストール"。

詳細については、を参照してください "Trident のドキュメント"。

詳細については、こちらをご覧ください

- "アーキテクチャに関する Rancher ドキュメント"
- "Rancher 用の Kubernetes 用語"
- "NetApp HCI のリソースページ"

NetApp HCI の Rancher の要件

NetApp HCI に Rancher をインストールする前に、環境および NetApp HCI システムがこれらの要件を満たしていることを確認してください。

> 誤った情報（不正な Rancher サーバ FQDN など）を使用して NetApp HCI に Rancher を誤って展開した場合、展開を削除して再展開することなく修正する方法はありません。NetApp HCI インスタンスでランチャを削除してから、ネットアップハイブリッドクラウド制御 UI から NetApp HCI 上のランチャを再導入する必要があります。を参照してください "NetApp HCI でランチツールをインストールした場合は、取り外します" を参照してください。

ノード要件

- NetApp HCI システムに少なくとも 3 つのコンピューティングノードがあることを確認します。耐障害性を最大限に高めるには、この設定が必要です。NetApp HCI の Rancher は、ストレージ専用の構成ではサポートされていません。
- NetApp HCI 環境で Rancher に使用するデータストアに少なくとも 60GB の空きスペースがあることを確認してください。
- NetApp HCI クラスタで管理サービスバージョン 2.17 以降が実行されていることを確認します。

ノードの詳細

NetApp HCI の Rancher は、 3 ノード管理クラスタを導入しました。

すべてのノードに次の特徴があります。

vCPU	RAM （GB）	ディスク（GB）
2.	8.	20

ネットワーク要件

- NetApp HCI 管理クラスタにランチサーバを導入するネットワークに、管理ノード管理ネットワークへのルートがあることを確認します。

- NetApp HCI の Rancher は、コントロールプレーン（ Rancher サーバ）およびユーザクラスタの DHCP アドレスをサポートしていますが、実稼働環境には静的 IP アドレスを推奨します。本番環境に導入する場合は、必要な静的 IP アドレスを割り当てておきます。
  - Rancher サーバには、 3 つのスタティック IP アドレスが必要です。
  - 各ユーザクラスタには、クラスタ内のノードと同じ数の静的 IP アドレスが必要です。たとえば、 4 つのノードからなるユーザクラスタには、静的 IP アドレスが 4 つ必要です。
  - Rancher コントロールプレーンまたはユーザクラスタに DHCP アドレッシングを使用する場合は、DHCP リース期間が 24 時間以上であることを確認してください。
- HTTP プロキシを使用して NetApp HCI 上の rancher のインターネットアクセスを有効にする必要がある場合は、管理ノードに展開前の変更を加える必要があります。SSH を使用して管理ノードにログインし、を実行します 。 "手順" Docker のプロキシ設定を手動で更新するための Docker ドキュメント。
- 展開時にプロキシサーバをイネーブルにして設定すると、次の IP アドレス範囲とドメインが自動的に rancher server noProxy 設定に追加されます。

```
127.0.0.0/8, 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, .svc,
.cluster.local
```

- 管理ノードが DNS を使用してホスト名「 < 任意の IP アドレス >.nip.io 」を IP アドレスに解決できることを確認します。導入時に使用される DNS プロバイダです。管理ノードでこの URL を解決できない場合、導入は失敗します。
- 必要な静的 IP アドレスごとに DNS レコードが設定されていることを確認します。

VMware vSphere の要件

- 使用している VMware vSphere インスタンスがバージョン 6.5 、 6.7 、または 7.0 であることを確認します。
- vSphere Standard Switch （ VSS ）ネットワーク構成を使用することもできますが、その場合は、ランチ元 VM に使用される仮想スイッチと物理ホストが、通常の VM の場合と同じ方法ですべての同じポートグループにアクセスできるようにします。

導入に関する考慮事項

必要に応じて、次の点を確認してください。

- 導入のタイプ
  - デモ環境
  - 本番環境への導入
- Rancher FQDN

> NetApp HCI の Rancher は、何らかのタイプのネットワークロードバランシングを設定しないかぎり、ノード障害に対する復元力がありません。簡単な解決策として、 rancher サーバ用に予約されている 3 つのスタティック IP アドレスのラウンドロビン DNS エントリを作成します。これらの DNS エントリは、 Rancher サーバホストにアクセスするために使用する rancher サーバ FQDN に解決する必要があります。これは、展開が完了すると rancher Web UI を提供します。

導入のタイプ

NetApp HCI に Rancher を展開するには、次の方法があります。

- * デモ展開 *: ターゲットの展開環境で DHCP が利用可能で、 NetApp HCI 機能で Rancher をデモする場合は、 DHCP 展開が最も効果的です。

  この配置モデルでは、管理クラスタ内の 3 つのノードのそれぞれから Rancher UI にアクセスできます。

  組織で DHCP を使用していない場合でも、本番環境の場合と同様に、導入前に割り当てられた 4 つの静的 IP アドレスを使用して DHCP を試してみることができます。

- * 本番環境の導入 * ：本番環境の導入で DHCP を使用できない場合は、導入前の作業が多少必要です。最初のステップでは、連続する 3 つの IP アドレスを取得します。の導入時に最初に入力します。

  本番環境では、 L4 ロードバランシングまたはラウンドロビン DNS 構成を使用することを推奨します。これには、 4 番目の IP アドレスと、 DNS 構成内の個別のエントリが必要です。

  - *L4 ロードバランシング *: nginx のようなアプリケーションをホストする仮想マシンまたはコンテナが、管理クラスタの 3 つのノードに要求を分散するように設定されている手法です。
  - * ラウンドロビン DNS * ： DNS システムで単一のホスト名が設定されている手法で、管理クラスタを形成する 3 つのホスト間で要求の回転を行います。

Rancher FQDN

インストールには、 Rancher URL を割り当てる必要があります。これには、インストールの完了後に Rancher UI が提供されるホストの完全修飾ドメイン名（ FQDN ）が含まれます。

いずれの場合も、 rancher UI には https プロトコル（ポート 443 ）経由でブラウザからアクセスできます。

本番環境では、管理クラスタノード全体に負荷が分散されるように FQDN が設定されている必要があります。FQDN とロードバランシングを使用しないと耐障害性に優れないため、デモ環境にのみ適しています。

必要なポート

「のポート」に含まれるポートのリストを確認してください Rancher Nodes on RKE 」の項を参照してください 公式のセクション "Rancher の文書" Rancher サーバーを実行しているノードとの間でファイアウォール設定を開いている。

必要な URL

次の URL は、 Rancher コントロールプレーンが存在するホストからアクセスできる必要があります。

URL	説明
https://charts.jetstack.io/	Kubernetes の統合
https://releases.rancher.com/server-charts/stable	Rancher ソフトウェアのダウンロード
https://entropy.ubuntu.com/	乱数生成用 Ubuntu エントロピーサービス
https://raw.githubusercontent.com/vmware/cloud-init-vmware-guestinfo/v1.3.1/install.sh	VMware ゲストの追加

URL	説明
https://download.docker.com/linux/ubuntu/gpg	Docker Ubuntu GPG 公開鍵
https://download.docker.com/linux/ubuntu	Docker ダウンロードリンク
https://hub.docker.com/	NetApp Hybrid Cloud Control 用 Docker Hub

NetApp HCI に Rancher を導入します

NetApp HCI 環境で Rancher を使用するには、最初に NetApp HCI に Rancher を導入します。

導入を開始する前に、データストアの空きスペースとその他を確認してください "NetApp HCI の Rancher の要件"。

Rancher サポートは、ネットアップサポートエッジ契約には含まれていません。オプションについては、ネットアップの営業担当者または代理店にお問い合わせください。ネットアップから Rancher サポートを購入された場合は、手順が記載された E メールをお送りします。

NetApp HCI に Rancher を導入するとどうなりますか。

の導入では、以下の手順を実行します。各手順についてさらに説明します。

- NetApp Hybrid Cloud Control を使用して導入を開始します。
- Rancher 展開は、 3 台の仮想マシンを含む管理クラスタを作成します。

  各仮想マシンには、コントロールプレーンとワーカーの両方の Kubernetes ロールがすべて割り当てられます。つまり、 rancher UI は各ノードで使用できます。

- Rancher コントロールプレーン（または *rancher Server* ）もインストールされます。簡単に導入できるように、 Rancher の NetApp HCI ノードテンプレートを使用します。Rancher コントロールプレーンは、NetApp HCI インフラの構築に使用した NetApp Deployment Engine の構成と自動的に連携します。
- 導入後、ネットアップから E メールが届きます。この E メールには、 NetApp HCI のランチマ展開に関するネットアップサポートに登録するオプションが記載されています。
- 導入後、開発チームと運用チームは任意の Rancher 環境と同様に、ユーザクラスタを導入できます。

NetApp HCI に Rancher を展開する手順

- NetApp Hybrid Cloud Control にアクセスします
- NetApp HCI に Rancher を導入します
- vCenter Server を使用して導入を確認します

NetApp Hybrid Cloud Control にアクセスします

導入を開始するには、 NetApp Hybrid Cloud Control にアクセスしてください。

1. Webブラウザで管理ノードのIPアドレスを開きます。例：

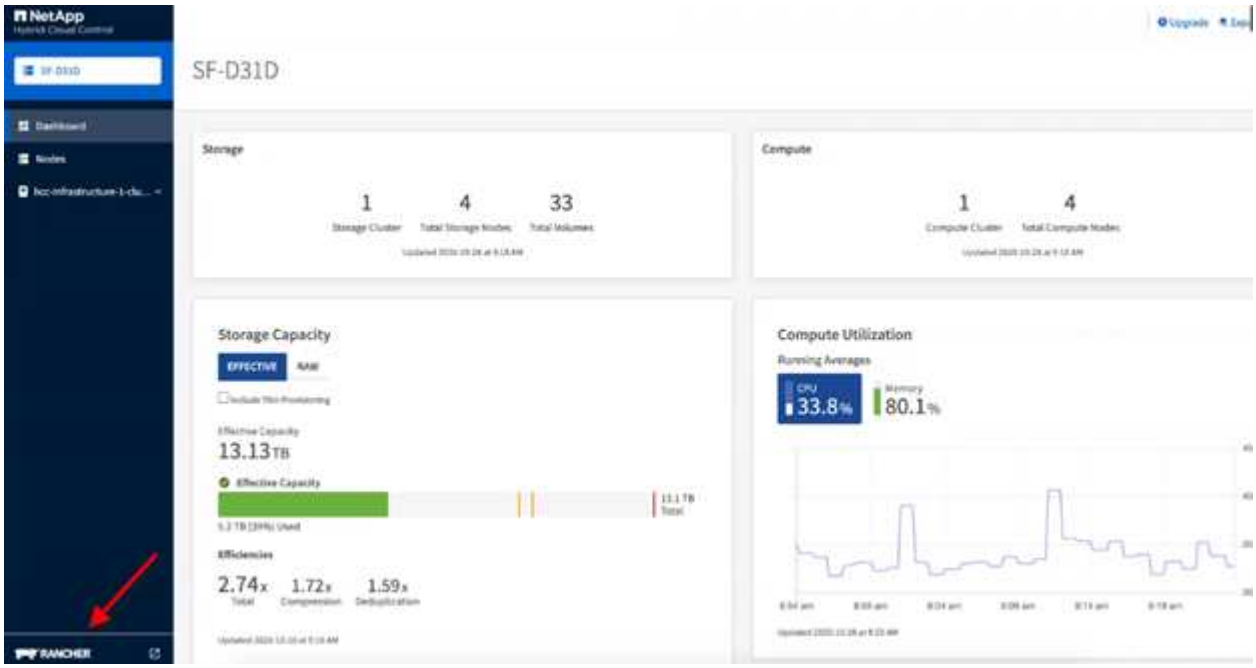
```
https://<ManagementNodeIP>
```

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

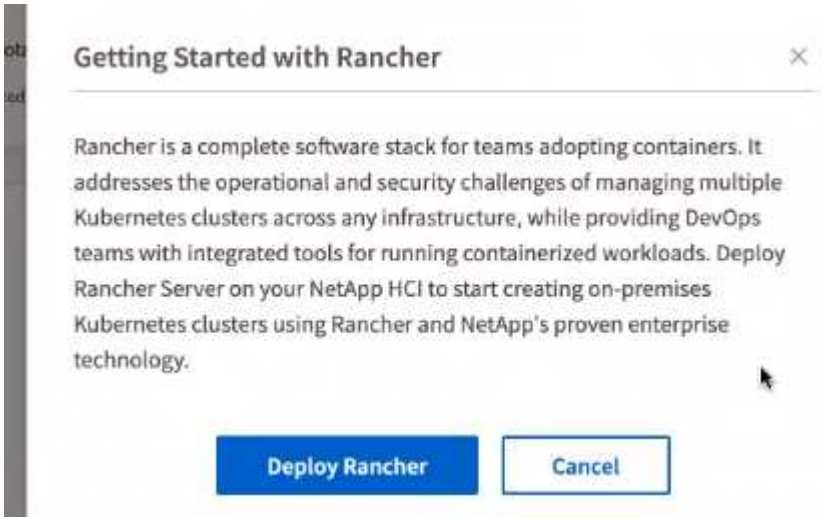
   NetApp Hybrid Cloud Control のインターフェイスが表示されます。

NetApp HCI に Rancher を導入します

1. Hybrid Cloud Control のナビゲーションバーの左下にある * ランチャ * アイコンをクリックします。

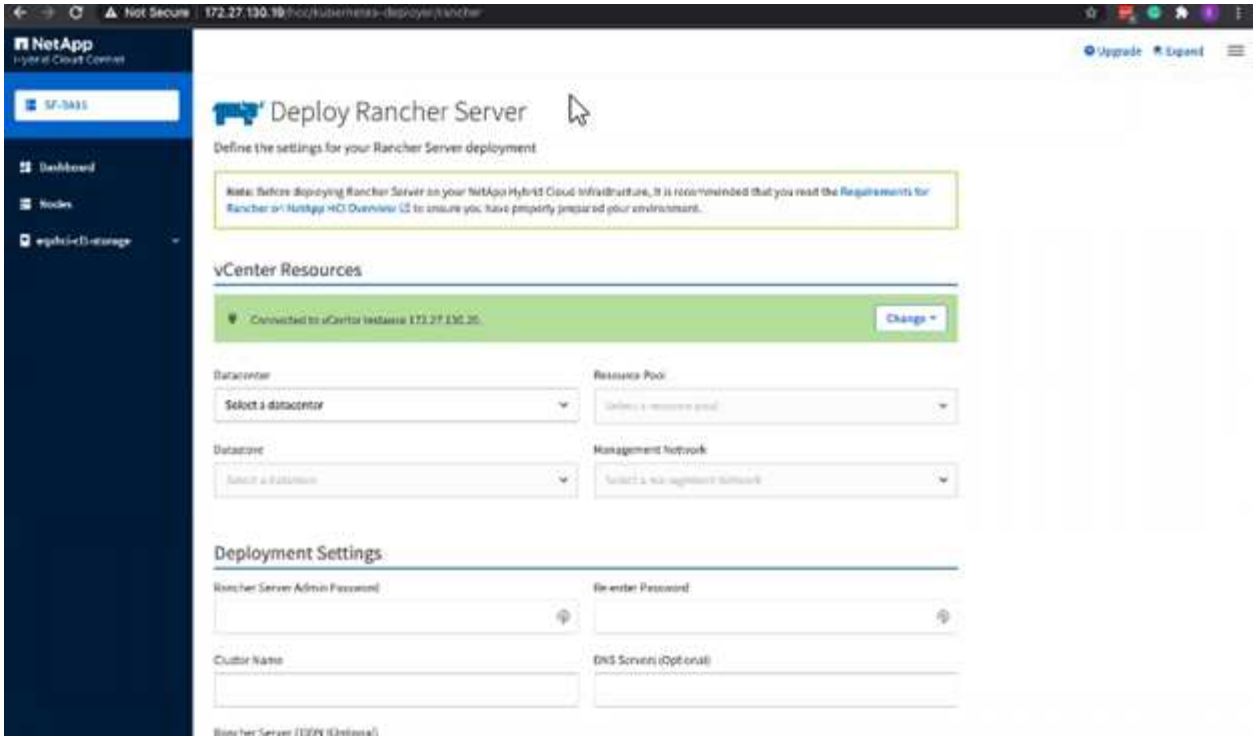


   ポップアップウィンドウに、 Rancher の使用を開始することを示すメッセージが表示されます。



2. [* ランチの展開 *] をクリックします。

   Rancher UI が表示されます。



vCenter のクレデンシャルは、 NetApp Deployment Engine のインストールに基づいて収集されます。

3. vCenter リソース情報を入力します。次に、一部のフィールドについて説明します。
   - * データセンター * ：データセンターを選択します。データセンターを選択すると、他のフィールドはすべて事前に入力されますが、変更することはできます。
   - * データストア * ： NetApp HCI ストレージノード上のデータストアを選択します。このデータストアは耐障害性が高く、すべての VMware ホストからアクセスできる必要があります。ホストの 1 つにしかアクセスできないローカルデータストアは選択しないでください。
   - * 管理ネットワーク * ：管理ステーションおよびユーザクラスタをホストする仮想マシンネットワークからアクセスできる必要があります。
4. 導入設定 * 情報を入力：
   - *DNS サーバ *: オプション。ロードバランシングを使用する場合は、内部 DNS サーバの情報を入力します。
   - **Rancher Server FQDN**: ノード障害時にランチサーバが使用可能な状態を維持するために、 DNS サーバが rancher サーバクラスタのノードに割り当てられた IP アドレスのいずれかに解決できる完全修飾ドメイン名 (FQDN) を指定します。"https" プレフィックスを含むこの FQDN は、ランチツールの実装にアクセスする際に使用するランチツール URL になります。

     ドメイン名を指定しない場合は、代わりにワイルドカード DNS が使用され、展開の完了後に提示された URL のいずれかを使用してランチサーバにアクセスできます。
5. 詳細設定 * 情報を入力：
   - * 静的 IP アドレスの割り当て * ：静的 IP アドレスを有効にする場合は、 3 つの IPv4 アドレスの開始 IP アドレスを順に指定し、各管理クラスタ仮想マシンに 1 つずつ指定します。NetApp HCI の Rancher は、 3 台の管理クラスタ仮想マシンを導入します。
   - * プロキシサーバーの設定 * ：

6. Rancher エンドユーザライセンス契約のチェックボックスを確認して選択します。
7. チェックボックスを確認して選択し、 Rancher ソフトウェアに関する情報を確認します。
8. [Deploy （配備）] をクリックします。

   導入の進捗状況はバーに表示されます。

   Rancher の導入には約 15 分かかる場合があります。

   展開が完了すると、 rancher は完了に関するメッセージを表示し、 rancher URL を提供します。

9. 展開の最後に表示される Rancher URL を記録します。この URL を使用して、 Rancher UI にアクセスします。

vCenter Server を使用して導入を確認します

vSphere Client には、 3 台の仮想マシンを含むランチ元管理クラスタが表示されます。

導入が完了したら、 Rancher サーバ仮想マシンクラスタの設定を変更したり、仮想マシンを削除したりしないでください。NetApp HCI の Rancher は、展開された RKE 管理クラスタの設定に依存して、正常に機能します。

次の手順

導入後、次の作業を実行できます。

- "導入後のタスクを実行"
- "Trident を NetApp HCI に Rancher とともにインストール"
- "ユーザクラスタとアプリケーションを導入"
- "NetApp HCI でランチ元を管理します"
- "NetApp HCI でランチをモニターします"

詳細については、こちらをご覧ください

- "Rancher 展開のトラブルシューティング"
- "アーキテクチャに関する Rancher ドキュメント"
- "Rancher 用の Kubernetes 用語"
- "NetApp HCI のリソースページ"

導入後のタスク

導入後のタスクの概要

NetApp HCI に Rancher を導入したら、展開後の作業を続行する必要があります。

- "Rancher サポートパリティを確認します"
- "VM の耐障害性を向上"
- "監視を設定"
- "Trident をインストール"
- "ユーザクラスタで Trident のサポートを有効にします"

詳細については、こちらをご覧ください

- "アーキテクチャに関する Rancher ドキュメント"
- "Rancher 用の Kubernetes 用語"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

Rancher サポートパリティを確認します

NetApp HCI に Rancher を導入したら、購入した Rancher サポートコアの数が、Rancher 管理 VM およびユーザクラスタに使用している CPU コアの数と一致していることを確認する必要があります。

NetApp HCI コンピューティングリソースの一部のみを対象に Rancher サポートを購入した場合は、 NetApp HCI の Rancher とその管理対象ユーザクラスタが Rancher サポートを購入したホストでのみ実行されるようにするために、 VMware vSphere でアクションを実行する必要があります。コンピューティングワークロードを特定のホストに限定することでこのような制限を実現する方法については、 VMware vSphere のドキュメントを参照してください。

詳細については、こちらをご覧ください

- "vSphere HA と DRS アフィニティルール"
- "VM 非アフィニティルールを作成します"
- "アーキテクチャに関する Rancher ドキュメント"
- "Rancher 用の Kubernetes 用語"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

VM の耐障害性を向上

NetApp HCI に Rancher を導入すると、 vSphere 環境に 3 つの新しいノードが仮想マシ

ンとして含まれ、 Rancher 環境をホストできるようになります。Rancher Web UI は、これらの各ノードから使用できます。完全な耐障害性を実現するには、電源再投入やフェイルオーバーなどのイベントが発生したあと、 3 台の仮想マシンと対応する仮想ディスクをそれぞれ別の物理ホストに配置する必要があります。

各 VM とそのリソースを別々の物理ホストに維持するために、 VMware vSphere Distributed Resource Scheduler （ DRS ）の非アフィニティルールを作成できます。これは、 NetApp HCI の導入で Rancher の一部として自動化されているわけではありません。

DRS 非アフィニティルールの設定方法については、次の VMware ドキュメントを参照してください。

"VM 非アフィニティルールを作成します"

"vSphere HA と DRS アフィニティルール"

詳細については、こちらをご覧ください

- "アーキテクチャに関する Rancher ドキュメント"
- "Rancher 用の Kubernetes 用語"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

監視を有効にします

NetApp HCI に Rancher を導入したあと、インストールまたはアップグレード時に Active IQ ストレージ監視機能（ SolidFire オールフラッシュストレージおよび NetApp HCI 用）と NetApp HCI コンピューティング監視機能（ NetApp HCI 専用）を有効にしていない場合、有効にすることができます。

モニタリングをイネーブルにする方法については、を参照してください "Active IQ と NetApp HCI の監視を有効にします"。

詳細については、こちらをご覧ください

- "アーキテクチャに関する Rancher ドキュメント"
- "Rancher 用の Kubernetes 用語"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

Trident をインストール

NetApp HCI に Rancher をインストールしたあとに Trident をインストールする方法をご確認ください。Trident は、 Docker と Kubernetes に統合されるストレージオーケストレーションツールであり、 Red Hat OpenShift 、 Rancher 、 IBM Cloud Private などのこれらのテクノロジを基盤に構築されたプラットフォームです。Trident の目的は、アプリケーションに対して、ストレージのプロビジョニング、接続、利用を透過的かつスム

ーズに行うことです。Trident は、ネットアップが管理する、完全にサポートされているオープンソースプロジェクトです。Trident を使用すると、使い慣れた標準の Kubernetes 形式で永続的ストレージボリュームを作成、管理、操作できます。

Trident の詳細については、を参照してください "Trident のドキュメント"。

必要なもの

- NetApp HCI に Rancher をインストールしておきます。
- ユーザクラスタを導入しておきます。
- Trident のユーザクラスタネットワークを設定しておきます。を参照してください "ユーザクラスタで Trident のサポートを有効にします" 手順については、を参照し
- Trident の作業ノードを準備するために必要な準備手順を完了しておきます。を参照してください "Trident のドキュメント"。

このタスクについて

Trident インストーラカタログは、 NetApp Hybrid Cloud Control を使用してランチャインストールの一部としてインストールされます。このタスクでは、インストーラカタログを使用して Trident をインストールおよび設定します。ランチシートインストールの一環として、ネットアップではノードテンプレートを提供しています。ネットアップが提供するノードテンプレートを使用せずに RHEL または CentOS でプロビジョニングする場合は、追加の要件がある可能性があります。ワーカーノードを RHEL または CentOS に変更する場合は、いくつかの前提条件を満たす必要があります。を参照してください "Trident のドキュメント"。

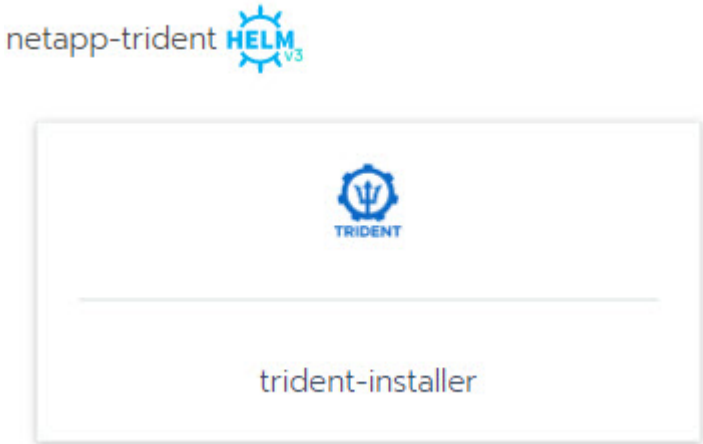
手順

1. Rancher UI から、ユーザークラスタのプロジェクトを選択します。

   プロジェクトと名前空間については、を参照してください "Rancher の文書"。

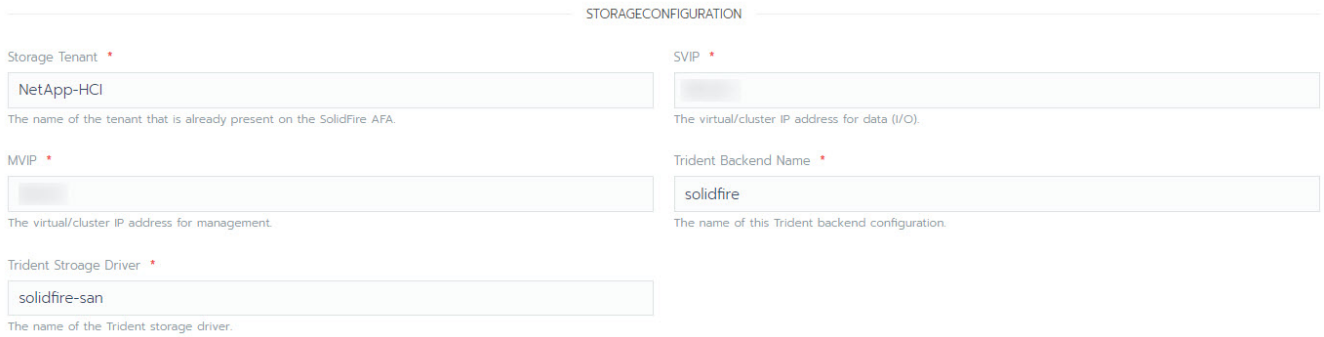
2. 「 * Apps * 」を選択し、「 * Launch * 」を選択します。

3. [**Catalog**] ページで、 Trident インストーラを選択します。



表示されたページで、「詳しい説明」の矢印を選択して Trident アプリの詳細を確認したり、へのリンクを確認したりできます "Trident のドキュメント"。

4. [* 構成オプション * （ Configurations Options ）] 矢印を選択し、クレデンシャルとストレージ構成情報を入力します。

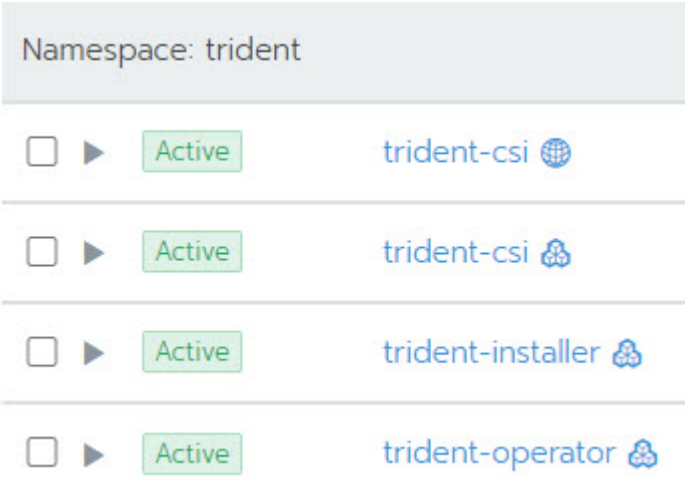


デフォルトのストレージテナントは NetApp HCI です。この値は変更できます。バックエンド名を変更することもできます。ただし、デフォルトのストレージドライバの値である * solidfire-san-* という値は変更しないでください。

5. [* 起動 *] を選択します。

   これにより、 Trident ワークロードが *trident * 名前空間にインストールされます。

6. リソース > ワークロード * を選択し、 * Trident * ネームスペースに次のコンポーネントが含まれていることを確認します。



7. （オプション）永続ボリュームに使用できるストレージクラスを表示するには、ユーザクラスタに対して * Storage * を選択します。

3 つのストレージクラスは、 * solidfire-cold* 、 * solidfire-plugin-2.* 、および * solidfire-plugin-2.銅 色 * です。これらのストレージ・クラスのいずれかをデフォルトにするには ' デフォルトの * カラムの下にあるアイコンを選択します

詳細については、こちらをご覧ください

- "ユーザクラスタで Trident のサポートを有効にします"
- "アーキテクチャに関する Rancher ドキュメント"
- "Rancher 用の Kubernetes 用語"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

ユーザクラスタで **Trident** のサポートを有効にします

NetApp HCI 環境の管理ネットワークとストレージネットワークの間にルートがなく、Trident のサポートが必要なユーザクラスタを導入する場合は、 Trident のインストール後にユーザクラスタネットワークをさらに設定する必要があります。各ユーザクラスタについて、管理ネットワークとストレージネットワークの間の通信を有効にする必要があります。これを行うには、ユーザクラスタ内の各ノードのネットワーク設定を変更します。

このタスクについて

ユーザクラスタ内の各ノードのネットワーク設定を変更するには、次の一般的な手順を実行します。次の手順では、 NetApp HCI に Rancher をインストールしたデフォルトノードテンプレートを使用してユーザクラスタを作成したものとします。

> これらの変更をカスタムノードテンプレートの一部として追加すると、以降のユーザクラスタで使用できるようになります。

手順

1. 既存のデフォルトテンプレートを使用してユーザクラスタを導入する。
2. ストレージネットワークをユーザクラスタに接続
   a. 接続されている vCenter インスタンスの VMware vSphere Web Client を開きます。
   b. ホストおよびクラスタインベントリツリーで、新しく導入したユーザクラスタ内のノードを選択します。
   c. ノードの設定を編集します。
   d. 設定ダイアログで、新しいネットワークアダプタを追加します。
   e. [新しいネットワーク *] ドロップダウン・リストで、ネットワークを参照し、 [* HCI _ 内部 _ ストレージ _ データ _ ネットワーク *] を選択します。
   f. [ネットワークアダプタ] セクションを展開し、新しいネットワークアダプタの MAC アドレスを記録します。
   g. [OK] をクリックします。
3. rancher で、ユーザクラスタ内の各ノードの SSH 秘密鍵ファイルをダウンロードします。
4. ダウンロードした秘密鍵ファイルを使用して、ユーザクラスタ内のノードに SSH を使用して接続します。

```
ssh -i <private key filename> <ip address>
```

5. スーパーユーザーとして '/etc/netplan/50-cloud-init.yaml ファイルを編集して保存し ' 次の例のように ens224' セクションが含まれるようにします「 <MAC アドレス >` 」を、前に記録した MAC アドレスに置き換えます。

```
network:
    ethernets:
        ens192:
            dhcp4: true
            match:
                macaddress: 00:50:56:91:1d:41
            set-name: ens192
        ens224:
            dhcp4: true
            match:
                macaddress: <MAC address>
            set-name: ens224
    version: 2
```

6. 次のコマンドを使用して、ネットワークを再設定します。

```
`netplan try`
```

7. ユーザクラスタの残りのノードについて、手順 4~6 を繰り返します。
8. ユーザクラスタ内の各ノードのネットワークを再設定したら、 Trident を利用するユーザクラスタにアプリケーションを導入できます。

ユーザクラスタとアプリケーションを導入

NetApp HCI に Rancher を導入した後、ユーザクラスタを設定し、それらのクラスタにアプリケーションを追加できます。

ユーザクラスタを導入

導入後、開発チームや運用チームは、任意のランチリーダーの導入と同様に、 Kubernetes ユーザクラスタを導入してアプリケーションを導入できます。

1. Rancher 展開の最後に提供された URL を使用して、 rancher UI にアクセスします。
2. ユーザクラスタを作成については、 Rancher のドキュメントを参照してください "ワークロードの導入"。
3. NetApp HCI の Rancher でユーザクラスタをプロビジョニングする。については、 Rancher のドキュメントを参照してください "Rancher で Kubernetes クラスタをセットアップする"。

ユーザクラスタにアプリケーションを導入する

任意のランチコンテナ環境と同様に、 Kubernetes クラスタにアプリケーションを追加します。

については、 Rancher のドキュメントを参照してください "クラスタ間でのアプリケーションの導入"。

詳細については、こちらをご覧ください

- "アーキテクチャに関する Rancher ドキュメント"
- "Rancher 用の Kubernetes 用語"
- "NetApp HCI のリソースページ"

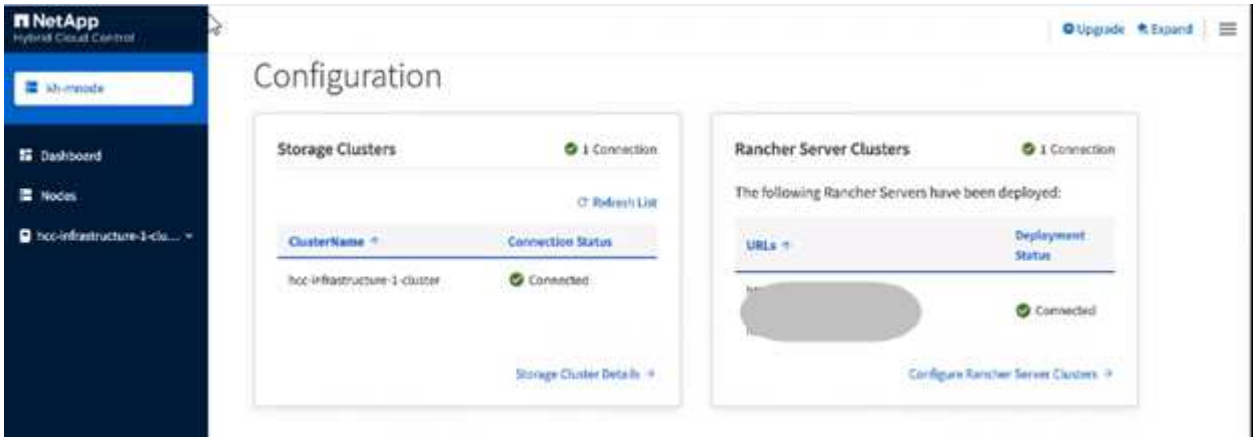
NetApp HCI でランチ元を管理します

NetApp HCI に Rancher を展開した後、 Rancher サーバクラスタの URL とステータスを表示できます。Rancher サーバを削除することもできます。

Rancher サーバクラスタの URL とステータスを特定します

Rancher サーバクラスタの URL を識別し、サーバのステータスを確認できます。

1. NetApp HCI または Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで右上のオプションアイコンを選択し、 * 構成 * を選択します。



Rancher Server Clusters ページには、展開された Rancher サーバクラスタ、関連する URL 、およびステータスのリストが表示されます。

詳細については、こちらをご覧ください

- "ランチを取り外す"
- "アーキテクチャに関する Rancher ドキュメント"
- "Rancher 用の Kubernetes 用語"
- "NetApp HCI のリソースページ"

NetApp HCI 実装の Rancher を監視する

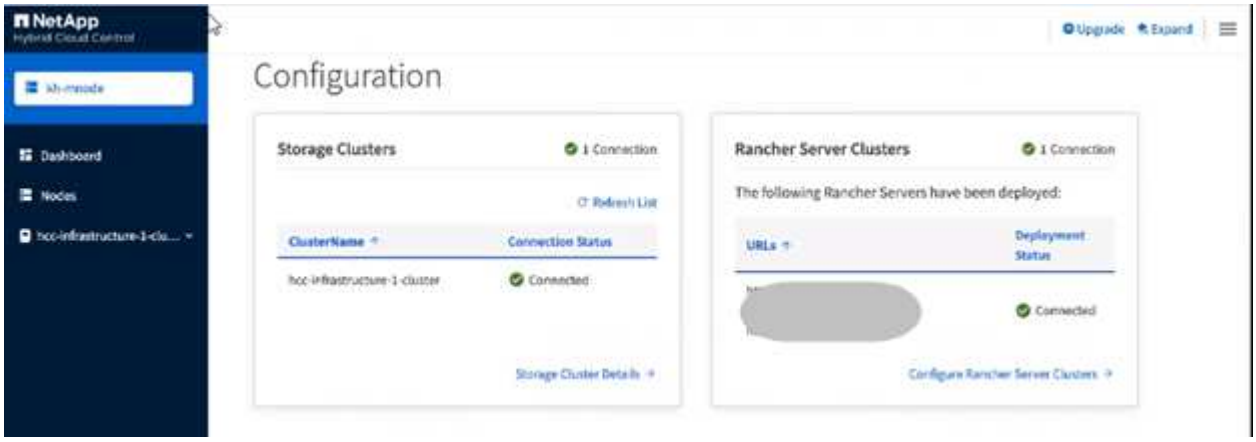
Rancher サーバ、管理クラスタ、およびその他の詳細を監視する方法は複数あります。

- NetApp Hybrid Cloud Control の略
- Rancher UI
- NetApp Active IQ の略
- vCenter Server の各サービスを提供

NetApp Hybrid Cloud Control を使用してランチャを監視します

NetApp Hybrid Cloud Control を使用して、 rancher URL と rancher サーバクラスタのステータスを確認できます。Rancher が実行されているノードを監視することもできます。

1. Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. ダッシュボードで右上のオプションアイコンをクリックし、 * 構成 * を選択します。



3. ノード情報を表示するには、 Hybrid Cloud Control Dashboard でストレージクラスタの名前を展開し、 * Nodes * をクリックします。

Rancher UI を使用して Rancher を監視します

Rancher UI を使用すると、 NetApp HCI 管理クラスタおよびユーザクラスタ上の rancher に関する情報を確認できます。

> Rancher UI では、管理クラスタを「ローカルクラスタ」と呼びます。

1. Rancher 展開の最後に提供された URL を使用して、 rancher UI にアクセスします。
2. を参照してください "Rancher v2.5 でのモニタリング"。

NetApp Active IQ を使用してランチを監視

NetApp Active IQ を使用すると、インストール情報、ノード、クラスタ、ステータス、ネームスペース情報などのランチツール計測データを表示できます。

1. Element ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
2. 右上のメニューから * NetApp Active IQ * を選択します。

vCenter Server を使用してランチ元を監視する

vCenter Server を使用すると、 Rancher 仮想マシンを監視できます。

詳細については、こちらをご覧ください

- "アーキテクチャに関する Rancher ドキュメント"
- "Rancher 用の Kubernetes 用語"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

NetApp HCI の Rancher をアップグレードします

rancher ソフトウェアをアップグレードするには、 NetApp Hybrid Cloud Control （ HCC ） UI または REST API を使用します。HCC は、 Rancher サーバ、 Rancher Kubernetes Engine （ RKE ）、および管理クラスタのノード OS （セキュリティアップデート用）など、 Rancher 導入環境のコンポーネントをアップグレードするための簡単なボタンプロセスを提供します。また、 API を使用してアップグレードを自動化することもできます。

アップグレードは、累積パッケージではなくコンポーネント単位で実行できます。このため、 Ubuntu OS などの一部のコンポーネントのアップグレードを、より迅速に行うことができます。アップグレードは、 Rancher サーバインスタンスと Rancher サーバが配置されている管理クラスタにのみ影響します。管理クラスタノードの Ubuntu OS へのアップグレードは、重要なセキュリティパッチのみを対象としており、オペレーティングシステムはアップグレードしません。ユーザクラスタは NetApp Hybrid Cloud Control からアップグレードできません。

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。
- * 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。

> Rancher 機能を使用するには、最新の管理サービスバンドル 2.17 以降にアップグレードする必要があります。

- * 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。
- 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を使用してランチャの導入環境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

次のいずれかのアップグレードプロセスを選択します。

- NetApp Hybrid Cloud Control の UI を使用してランチャをアップグレード 導入
- NetApp Hybrid Cloud Control API を使用してランチャをアップグレード 導入

NetApp Hybrid Cloud Control の UI を使用してランチャをアップグレード 導入

NetApp Hybrid Cloud Control の UI を使用して、ランチャ環境の以下のコンポーネントをアップグレードできます。

- Rancher サーバ
- Rancher Kubernetes Engine （ RKE ）
- ノード OS のセキュリティ更新

必要なもの

- インターネット接続が良好です。ダークサイトのアップグレード（外部接続のないサイトでのアップグレード）は利用できません。

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、 [* ランチー * （ * rancher * ）] を選択
5. アップグレードするソフトウェアの [* アクション *] メニューを選択します。
   - Rancher サーバ
   - Rancher Kubernetes Engine （ RKE ）
   - ノード OS のセキュリティ更新
6. Rancher サーバまたは RKE アップグレードの場合は * Upgrade * を、ノード OS のセキュリティアップデートの場合は * Apply Upgrade * を選択します。

> ノード OS の場合、セキュリティパッチの無人アップグレードは日単位で実行されますが、ノードは自動的にはリブートされません。アップグレードを適用すると、各ノードをリブートしてセキュリティ更新を有効にできます。

コンポーネントのアップグレードが正常に完了したことを示すバナーが表示されます。NetApp Hybrid Cloud Control の UI で更新後のバージョン番号が表示されるまでに最大 2 分かかる場合があります。

NetApp Hybrid Cloud Control API を使用してランチャをアップグレード 導入

API を使用して、 Rancher 展開内の次のコンポーネントをアップグレードできます。

- Rancher サーバ
- Rancher Kubernetes Engine （ RKE ）
- ノード OS （セキュリティ更新用）

任意の自動化ツールを使用して、管理ノードで使用可能な API または REST API UI を実行できます。

オプション（ **Options** ）

- Rancher サーバをアップグレードします
- RKE をアップグレードします
- ノード OS のセキュリティ更新を適用

> ノード OS の場合、セキュリティパッチの無人アップグレードは日単位で実行されますが、ノードは自動的にはリブートされません。アップグレードを適用すると、各ノードをリブートしてセキュリティ更新を有効にできます。

Rancher サーバをアップグレードします

API コマンド

1. アップグレードバージョンリストの要求を開始します。

```
curl -X POST "https://<managementNodeIP>/k8sdeployer/1/upgrade/rancher-versions" -H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

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

2. 前のコマンドのタスク ID を使用してタスクステータスを取得し、応答から最新のバージョン番号をコピーします。

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

3. Rancher サーバのアップグレード要求を開始します。

```
curl -X PUT "https://<mNodeIP>/k8sdeployer/1/upgrade/rancher/<version
number>" -H "accept: application/json" -H "Authorization: Bearer"
```

4. アップグレードコマンドの応答からタスク ID を使用してタスクステータスを取得します。

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

REST API の **UI** の手順

1. 管理ノードで管理ノード REST API UI を開きます。

```
https://<ManagementNodeIP>/k8sdeployer/api/
```

2. 「 * Authorize * 」（認証）を選択して、次の手順を実行
   a. クラスタのユーザ名とパスワードを入力します。
   b. クライアント ID を「 m node-client 」として入力します。
   c. セッションを開始するには、 * Authorize * を選択します。
   d. 承認ウィンドウを閉じます。
3. 最新のアップグレードパッケージを確認します。
   a. REST API UI から * POST/upgradeRunce/rancher-versions * を実行します。
   b. 応答から、タスク ID をコピーします。
   c. 前の手順で確認したタスク ID で * Get/taskTouled/{taskID}* を実行します。
4. /tasksuses/{taskID}* 応答から、アップグレードに使用する最新バージョン番号をコピーします。
5. Rancher Server アップグレードを実行します。
   a. REST API UI から、前の手順の最新バージョン番号を使用して * PUT / upgrade/Pedries/rancherRunce/ ｛ version ｝ * を実行します。
   b. 応答から、タスク ID をコピーします。
   c. 前の手順で確認したタスク ID で * Get/taskTouled/{taskID}* を実行します。

アップグレードが正常に完了したのは、「 PercentComplete 」が「 100 」を示し、「結果」がアップグレードされたバージョン番号を示している場合です。

RKE をアップグレードします

API コマンド

1. アップグレードバージョンリストの要求を開始します。

```
curl -X POST "https://<mNodeIP>/k8sdeployer/1/upgrade/rke-versions" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

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

2. 前のコマンドのタスク ID を使用してタスクステータスを取得し、応答から最新のバージョン番号をコピーします。

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

3. RKE アップ・リクエストを開始します

```
curl -X PUT "https://<mNodeIP>/k8sdeployer/1/upgrade/rke/<version
number>" -H "accept: application/json" -H "Authorization: Bearer"
```

4. アップグレードコマンドの応答からタスク ID を使用してタスクステータスを取得します。

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

REST API の UI の手順

1. 管理ノードで管理ノード REST API UI を開きます。

```
https://<ManagementNodeIP>/k8sdeployer/api/
```

2. 「 * Authorize * 」（認証）を選択して、次の手順を実行
   a. クラスタのユーザ名とパスワードを入力します。
   b. クライアント ID を「 m node-client 」として入力します。
   c. セッションを開始するには、 * Authorize * を選択します。
   d. 承認ウィンドウを閉じます。
3. 最新のアップグレードパッケージを確認します。
   a. REST API UI から、 * POST/upgradeRunce/RKE -versions * を実行します。
   b. 応答から、タスク ID をコピーします。
   c. 前の手順で確認したタスク ID で * Get/taskTouled/{taskID}* を実行します。
4. /tasksuses/{taskID}* 応答から、アップグレードに使用する最新バージョン番号をコピーします。

5. RKE アップグレードを実行します。
   a. REST API UI から、前の手順の最新バージョン番号を使用して * PUT / upgrade / RKE / ｛ version ｝ * を実行します。
   b. 応答からタスク ID をコピーします。
   c. 前の手順で確認したタスク ID で * Get/taskTouled/{taskID}* を実行します。

アップグレードが正常に完了したのは、「 PercentComplete 」が「 100 」を示し、「結果」がアップグレードされたバージョン番号を示している場合です。

ノード **OS** のセキュリティ更新を適用

API コマンド

1. アップグレードチェック要求を開始します。

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/upgrade/checkNodeUpdates"
-H "accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

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

2. 前のコマンドのタスク ID を使用してタスクステータスを取得し、応答から新しいバージョン番号を取得できることを確認します。

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

3. ノードの更新を適用します。

```
curl -X POST "https://<mNodeIP>/k8sdeployer/1/upgrade/applyNodeUpdates"
-H "accept: application/json" -H "Authorization: Bearer"
```

> ノード OS の場合、セキュリティパッチの無人アップグレードは日単位で実行されますが、ノードは自動的にはリブートされません。アップグレードを適用すると、各ノードを順番にリブートし、セキュリティ更新を有効にすることができます。

4. アップグレードの「 applyNodeUpdates 」応答からタスク ID を使用してタスクステータスを取得します。

```
curl -X GET "https://<mNodeIP>/k8sdeployer/1/task/<taskID>" -H "accept:
application/json" -H "Authorization: Bearer ${TOKEN}"
```

REST API の **UI** の手順

1. 管理ノードで管理ノード REST API UI を開きます。

```
https://<ManagementNodeIP>/k8sdeployer/api/
```

2. 「 * Authorize * 」（認証）を選択して、次の手順を実行
   a. クラスタのユーザ名とパスワードを入力します。
   b. クライアント ID を「 m node-client 」として入力します。
   c. セッションを開始するには、 * Authorize * を選択します。
   d. 承認ウィンドウを閉じます。
3. アップグレードパッケージがあるかどうかを確認します。
   a. REST API UI から * get/upgrade/checkNodeUpdates * を実行します。
   b. 応答から、タスク ID をコピーします。
   c. 前の手順で確認したタスク ID で * Get/taskTouled/{taskID}* を実行します。
   d. * /tasksanges/ ｛ taskID ｝ * 応答から、ノードに現在適用されているバージョン番号よりも新しいバージョン番号があることを確認してください。
4. ノード OS のアップグレードを適用します。

> ノード OS の場合、セキュリティパッチの無人アップグレードは日単位で実行されますが、ノードは自動的にはリブートされません。アップグレードを適用すると、各ノードを順番にリブートし、セキュリティ更新を有効にすることができます。

   a. REST API UI から * POST/upgrade投入 / applyNodeUpdates * を実行します。
   b. 応答から、タスク ID をコピーします。
   c. 前の手順で確認したタスク ID で * Get/taskTouled/{taskID}* を実行します。
   d. /tasksanges/{taskID}* 応答から、アップグレードが適用されたことを確認します。

アップグレードが正常に完了したのは、「 PercentComplete 」が「 100 」を示し、「結果」がアップグレードされたバージョン番号を示している場合です。

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"

NetApp HCI でランチツールをインストールした場合は、取り外します

誤った情報（不正な Rancher サーバ FQDN など）を使用して NetApp HCI に Rancher を誤って展開した場合は、インストールを削除してから再展開する必要があります。NetApp HCI インスタンス上の Rancher インストールを削除するには、次の手順を

実行します。

ユーザクラスタは削除されません。

> ユーザクラスタを保持しなければならない場合があります。これらを保持しておくと、後で別の Rancher 実装に移行できます。ユーザクラスタを削除する場合は、最初に rancher サーバを削除する前に、削除する必要があります。削除しないと、 rancher サーバの削除後にユーザクラスタを削除するのが難しくなります。

オプション（ **Options** ）

- ネットアップのハイブリッドクラウドコントロールを使用して NetApp HCI のランチャを削除 （推奨）
- REST API を使用して NetApp HCI のランチツールを削除します

ネットアップのハイブリッドクラウドコントロールを使用して **NetApp HCI** のランチャを削除

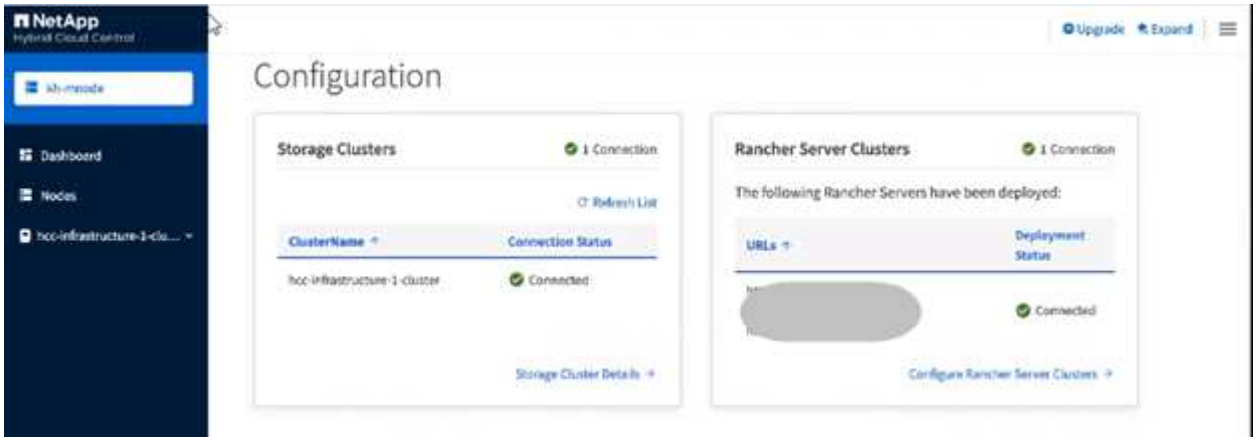
NetApp Hybrid Cloud Control Web UI を使用して、ランチサーバをホストするために導入時に設定した 3 つの仮想マシンを削除できます。

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. ダッシュボードの右上にあるメニューをクリックします。
4. 「 * Configure * 」を選択します。



5. [* Rancher Server Clusters] ペインで、 [* Rancher Server Clusters] をクリックします。
6. 削除する必要があるランチャのインストールの * アクション * メニューを選択します。

> 削除 * をクリックすると、 NetApp HCI 管理クラスタのランチ元がすぐに削除されます。

7. 「 * 削除」を選択します。

REST API を使用して NetApp HCI のランチツールを削除します

NetApp Hybrid Cloud Control REST API を使用して、ランチサーバをホストするために導入時に設定した 3 つの仮想マシンを削除できます。

手順

1. 管理ノードの IP アドレスのあとに「 /k8sdeployer/api/` 」を入力します。

```
https://[IP address]/k8sdeployer/api/
```

2. Authorize * または任意のロックアイコンをクリックし、 API を使用する権限を付与するクラスタ管理者クレデンシャルを入力します。
   a. クラスタのユーザ名とパスワードを入力します。
   b. 値が選択されていない場合は、タイプドロップダウンリストから * リクエスト本文 * を選択します。
   c. 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。
   d. クライアントシークレットの値は入力しないでください。
   e. セッションを開始するには、 * Authorize * をクリックします。
   f. ウィンドウを閉じます。
3. [**Available Authorizations (** 使用可能な承認 **)**] ダイアログボックスを閉じます。
4. [POST/destroy] をクリックします。
5. [* 試してみてください *] をクリックします。
6. [request body （要求の本文）] テキストボックスに、 [erverURL] 値として rancher サーバ FQDN を入力します。
7. [* Execute] をクリックします。

   数分後、ランチサーバの仮想マシンが vSphere Client のホストおよびクラスタリストに表示されなくなります。削除後は、 NetApp Hybrid Cloud Control を使用して NetApp HCI にランチシートを再導入できます。

詳細はこちら

- "Rancher 展開のトラブルシューティング"
- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

H シリーズハードウェアのメンテナンス

H シリーズハードウェアのメンテナンスの概要

システムが最適に機能するように、障害のあるノードの交換、ストレージノード内の障害のあるドライブの交換など、ハードウェアのメンテナンス作業を行う必要があります。

ハードウェアメンテナンスタスクへのリンクを次に示します。

- "2U H シリーズシャーシを交換"
- "H615C および H610S ノードの DC 電源装置を交換してください"
- "コンピューティングノードの DIMM を交換します"
- "ストレージノードのドライブを交換"
- "H410C ノードを交換してください"
- "H410S ノードを交換します"
- "H610C ノードと H615C ノードを交換してください"
- "H610S ノードを交換してください"
- "電源装置を交換してください"
- "SN2010 、 SN2100 、および SN2700 の各スイッチを交換してください"
- "2 ノードクラスタのストレージノードを交換"

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"
- "vCenter Server 向け NetApp Element プラグイン"
- "_TR-48820 ：『 NetApp HCI ネットワーククイックプランニングガイド』 _"
- "NetApp Configuration Advisor" 5.8.1 以降のネットワーク検証ツール

2U H シリーズシャーシを交換

シャーシにファンの障害または電源の問題がある場合は、できるだけ早く交換する必要があります。シャーシの交換手順は、 NetApp HCI 構成とクラスタの容量によって異なります。そのため、慎重な検討と計画が必要です。ネットアップサポートに連絡して指示を受け、交換用シャーシを注文する必要があります。

このタスクについて

シャーシを交換する前に、次の点を考慮してください。

- ラックに新しいシャーシ用のスペースは追加されていますか。

- 導入環境内のいずれかのシャーシに未使用のノードスロットがありますか？
- ラックにスペースが追加されている場合、障害が発生したシャーシから新しいシャーシに各ノードを一度に 1 つずつ移動できますか。この処理には時間がかかることがあります。
- 障害が発生したシャーシの一部であるノードを取り外しても、ストレージクラスタをオンラインのままにしておくことはできますか。
- 障害が発生したシャーシの一部であるコンピューティングノードを削除する際、仮想マシン（ VM ）と ESXi クラスタでワークロードを処理できますか？

交換オプション

次のいずれかのオプションを選択します。で追加の未使用スペースが使用可能になったら、シャーシを交換します ラック
追加の未使用スペースがない場合は、シャーシを交換します ラック内

で追加の未使用スペースが使用可能になったら、シャーシを交換します ラック

ラックにスペースが追加されている場合は、新しいシャーシを設置し、ノードを一度に 1 つずつ新しいシャーシに移動できます。取り付けられているシャーシのいずれかに未使用のノードスロットがある場合、障害が発生したシャーシから未使用のスロットに一度に 1 つずつノードを移動して、障害が発生したシャーシを取り外すことができます。手順を開始する前に、ケーブル長が十分であり、スイッチポートが使用可能であることを確認してください。

> コンピューティングノードを移動する手順は、ストレージノードを移動する手順とは異なります。ノードを移動する前に、ノードが正しくシャットダウンされていることを確認する必要があります。障害が発生したシャーシからすべてのノードを移動したら、シャーシをラックから取り外してネットアップに返却する必要があります。

新しいシャーシを設置します

新しいシャーシを設置して使用可能なラックスペースに設置し、ノードを移動できます。

必要なもの

- 静電放電（ ESD ）リストバンドを装着するか、静電気防止処置を行っておきます。
- 交換用シャーシを用意しておきます。
- ステップを実施するために、リフトを 1 人または 2 人以上の作業者がいること。
- No.1 プラスドライバを用意しておきます。

手順

1. 静電気防止処置を施します。
2. 交換用シャーシを開封します。障害が発生したシャーシをネットアップに返却するときは、パッケージを保管しておいてください。
3. 出荷時にシャーシに付属していたレールを挿入します。
4. 交換用シャーシをラックに挿入します。

> シャーシを設置する際は、常に十分な人員またはリフトを使用してください。

5. 前面取り付け用の蝶ネジでシャーシをラックに固定し、ネジをドライバで締めます。

コンピューティングノードを移動する

コンピューティングノードを新しいシャーシに移動したり、未使用のスロットがある既存のシャーシに移動したりする前に、仮想マシン（ VM ）を移行し、ノードを正しくシャットダウンして、ノードに挿入されているケーブルにラベルを付けたりする必要があります。

ノードを移動するときは、静電気防止処置を施します。

手順

1. ノード背面のステッカーに記載されているノードのシリアル番号をメモします。
2. VMware vSphere Web Client で、 **Hosts and Clusters** を選択し、ノード（ホスト）を選択してから * Monitor > Hardware Status > Sensor* を選択します。
3. 「 * Sensors * 」セクションで、ノード背面のステッカーに記載されているシリアル番号を探します。
4. 一致するシリアル番号が見つかったら、 VM を別の使用可能なホストに移行します。

   移行手順については、 VMware のドキュメントを参照してください。

5. ノードを右クリックし、 * 電源 > シャットダウン * を選択します。これで、ノードをシャーシから物理的に取り外す準備ができました。
6. ノードの背面にあるノードとすべてのケーブルにラベルを付けます。
7. 各ノードの右側にあるカムハンドルを下に引き、両方のカムハンドルを使用してノードをシャーシから引き出します。
8. カチッという音がするまでノードを押し込んで、ノードを新しいシャーシに再度取り付けます。ノードを削除する前に付けておいたラベルは、ヘルプガイドに記載されています。ノードは、正しくインストールすると自動的に電源がオンになります。

   ノードをインストールするときは、からサポートしていることを確認してください。ノードをシャーシにプッシュする際に力を入れすぎないようにしてください。

   新しいシャーシに設置する場合は、ノードをシャーシの元のスロットに設置します。

9. ノードの背面にある同じポートにケーブルを再接続します。ケーブルを外したときに使用していたラベルは、ガイドとして役立ちます。

   ケーブルをポートに無理に押し込まないでください。ケーブル、ポート、またはその両方が破損する可能性があります。

10. コンピューティングノード（ホスト）が VMware vSphere Web Client の ESXi クラスタに表示されることを確認します。
11. 障害が発生したシャーシ内のすべてのコンピューティングノードで次の手順を実行します。

ストレージノードを移動

ストレージノードを新しいシャーシに移動する前に、ドライブを取り外し、ノードを正しくシャットダウンして、すべてのコンポーネントにラベルを付けておく必要があります。

手順

1. 次の手順で、削除するノードを特定します。
   a. ノード背面のステッカーに記載されているノードのシリアル番号をメモします。
   b. VMware vSphere Web Client で、 * NetApp Element Management* を選択し、 MVIP IP アドレスをコピーします。
   c. Web ブラウザで MVIP IP アドレスを使用して、 NetApp Deployment Engine で設定したユーザ名とパスワードを使用して NetApp Element ソフトウェア UI にログインします。
   d. [*Cluster] > [Nodes] を選択します。
   e. 書き留めたシリアル番号と、記載されているシリアル番号（サービスタグ）を照合します。
   f. ノードのノード ID をメモします。
2. ノードを特定したら、次の API 呼び出しを使用して iSCSI セッションをノードから移動します。「 wget --no-check-certificate-q --user> -password=<user> -O-post-data' ｛ "method" ： "MovePrimaryiesAFrommNode " 、 "params" ： ｛ DEnodeID ｝ 」 https://<MVIP>/json-rpc/8.0`MVIP には MVIP IP アドレス、 NODEID にはノード ID 、 NetApp HCI のセットアップ時に NetApp Deployment Engine で設定したユーザ名にはユーザ名を、 NetApp HCI のセットアップ時に NetApp Deployment Engine で設定したパスワードには pass を指定します。
3. クラスタ > ドライブ * を選択して、ノードに関連付けられているドライブを削除します。

   取り外したドライブが使用可能として表示されるまで待ってから、ノードを削除します。

4. ノードを削除するには、 * Cluster > Nodes > Actions > Remove * を選択します。
5. 次の API 呼び出しを使用してノードをシャットダウンします。 <code>wget --no-check-certificate-q --user>--password=<pass> -O—post-data'{" method" ： "Shutdown" 、 "params" ： "option" 、 "nodes" ： [<NODEID> ｝] <a href="https://<MVIP>/json-rpc/8.0</code>" class="bare">https://<MVIP>/json-rpc/8.0</code>MVIP には MVIP IP アドレス、 NODEID にはノード ID 、 NetApp HCI のセットアップ時に NetApp Deployment Engine で設定したユーザ名にはユーザ名を、 NetApp HCI のセットアップ時に NetApp Deployment Engine で設定したパスワードには pass を指定します。ノードがシャットダウンされると、シャーシからノードを物理的に取り外すことができます。
6. 次の手順で、シャーシ内のノードからドライブを取り外します。
   a. ベゼルを取り外します。
   b. ドライブにラベルを付けます。
   c. カムハンドルを開き、各ドライブを両手で慎重に引き出します。
   d. ドライブを静電気防止処置を施した平らな場所に置きます。
7. 次の手順でノードをシャーシから取り外します。
   a. ノードとケーブルが接続されていることを示すラベルを付けます。
   b. 各ノードの右側にあるカムハンドルを下に引き、両方のカムハンドルを使用してノードを引き出します。
8. カチッという音がするまでノードを押し込んで、ノードをシャーシに再度取り付けます。ノードを削除す

る前に付けておいたラベルは、ヘルプガイドに記載されています。

> ノードをインストールするときは、からサポートしていることを確認してください。ノードをシャーシにプッシュする際に力を入れすぎないようにしてください。

> 新しいシャーシに設置する場合は、ノードをシャーシの元のスロットに設置します。

9. 各ドライブのカムハンドルをカチッと音がするまで押し下げて、ドライブをノードのそれぞれのスロットに取り付けます。
10. ノードの背面にある同じポートにケーブルを再接続します。ケーブルを外したときに付けたラベルは、ガイドとして役立ちます。

> ケーブルをポートに無理に押し込まないでください。ケーブル、ポート、またはその両方が破損する可能性があります。

11. ノードの電源がオンになったら、クラスタにノードを追加します。

> ノードが追加されて「 * Nodes > Active * 」の下に表示されるまでに最大 2 分かかることがあります。

12. ドライブを追加します。
13. シャーシ内のすべてのストレージノードで次の手順を実行します。

追加の未使用スペースがない場合は、シャーシを交換します ラック内

ラックに追加のスペースがない場合や、設置されているシャーシに未使用のノードスロットがない場合は、交換手順を実行する前に、オンラインのまま維持できるノードを確認する必要があります。

このタスクについて

シャーシの交換を行う前に、次の点を考慮する必要があります。

- 障害が発生したシャーシにストレージノードがない状態でも、ストレージクラスタをオンラインのままにしておくことはできますか。「いいえ」の場合は、 NetApp HCI 環境内のすべてのノード（コンピューティングとストレージの両方）をシャットダウンする必要があります。答えが「はい」の場合は、障害が発生したシャーシ内のストレージノードだけをシャットダウンできます。
- 障害が発生したシャーシにコンピューティングノードが搭載されていなくても、 VM と ESXi クラスタをオンラインのまま維持できますか？「いいえ」の場合は、障害が発生したシャーシのコンピューティングノードをシャットダウンできるように、適切な VM をシャットダウンまたは移行する必要があります。答えが「はい」の場合は、障害が発生したシャーシ内のコンピューティングノードだけをシャットダウンできます。

コンピューティングノードをシャットダウンします

コンピューティングノードを新しいシャーシに移動する前に、 VM を移行して正しくシャットダウンし、ノードに挿入したケーブルにラベルを付けます。

手順

1. ノード背面のステッカーに記載されているノードのシリアル番号をメモします。

2. VMware vSphere Web Client で、 **Hosts and Clusters** を選択し、ノード（ホスト）を選択してから * Monitor > Hardware Status > Sensor* を選択します。
3. 「 * Sensors * 」セクションで、ノード背面のステッカーに記載されているシリアル番号を探します。
4. 一致するシリアル番号が見つかったら、 VM を別の使用可能なホストに移行します。

   移行手順については、 VMware のドキュメントを参照してください。

5. ノードを右クリックし、 * 電源 > シャットダウン * を選択します。これで、ノードをシャーシから物理的に取り外す準備ができました。

ストレージノードをシャットダウンします

手順を参照してください こちらをご覧ください。

ノードを削除します

ノードをシャーシから慎重に取り外し、すべてのコンポーネントにラベルを付ける必要があります。ノードを物理的に取り外す手順は、ストレージノードとコンピューティングノードで同じです。ストレージノードの場合は、ノードを削除する前にドライブを取り外してください。

手順

1. ストレージノードの場合は、次の手順でシャーシ内のノードからドライブを取り外します。
   a. ベゼルを取り外します。
   b. ドライブにラベルを付けます。
   c. カムハンドルを開き、各ドライブを両手で慎重に引き出します。
   d. ドライブを静電気防止処置を施した平らな場所に置きます。
2. 次の手順でノードをシャーシから取り外します。
   a. ノードとケーブルが接続されていることを示すラベルを付けます。
   b. 各ノードの右側にあるカムハンドルを下に引き、両方のカムハンドルを使用してノードを引き出します。
3. 削除するすべてのノードで次の手順を実行します。これで、障害が発生したシャーシを取り外す準備ができました。

シャーシを交換してください

ラックのスペースが足りない場合は、障害が発生したシャーシを取り外し、新しいシャーシと交換する必要があります。

手順

1. 静電気防止処置を施します。
2. 交換用シャーシを開封し、平らな場所に保管します。障害ユニットをネットアップに返却するときは、梱包材を保管しておいてください。
3. 障害が発生したシャーシをラックから取り外し、平らな場所に置きます。

シャーシの移動中は、十分な人員またはリフトを使用してください。

4. レールを取り外します。
5. 交換用シャーシに付属している新しいレールを取り付けます。
6. 交換用シャーシをラックに挿入します。
7. 前面取り付け用の蝶ネジでシャーシをラックに固定し、ネジをドライバで締めます。
8. 次の手順に従って、新しいシャーシにノードを設置します。
   a. カチッという音がするまでノードを押し込んで、ノードをシャーシの元のスロットに再度取り付けます。ノードを削除する前に接続したラベル。

      ノードをインストールするときは、からサポートしていることを確認してください。ノードをシャーシにプッシュする際に力を入れすぎないようにしてください。

   b. ストレージノードの場合は、各ドライブのカムハンドルをカチッと音がするまで押し下げて、ドライブをノードのそれぞれのスロットに取り付けます。
   c. ノードの背面にある同じポートにケーブルを再接続します。ケーブルを外したときに付けたラベルは、ガイドとして役立ちます。

      ケーブルをポートに無理に押し込まないでください。ケーブル、ポート、またはその両方が破損する可能性があります。

9. ノードが次のようにオンラインになっていることを確認します。

オプション	手順
すべてのノード（ストレージとコンピューティングの両方）を再インストールした場合 NetApp HCI 環境に導入します	a. VMware vSphere Web Client で、コンピューティングノード（ホスト）が ESXi クラスタに表示されていることを確認します。 b. Element Plug-in for vCenter Server で、ストレージノードが Active と表示されていることを確認します。

オプション	手順
障害が発生したシャーシにノードだけを再設置した場合	a. VMware vSphere Web Client で、コンピューティングノード（ホスト）が ESXi クラスタに表示されていることを確認します。 b. vCenter Server 用 Element プラグインで、 * Cluster > Nodes > Pending * を選択します。 c. ノードを選択し、 * 追加 * を選択します。 ノードが追加されて「 * Nodes > Active * 」の下に表示されるまでに最大 2 分かかることがあります。 d. [* Drives] を選択します。 e. 使用可能なリストからドライブを追加します。 f. 再インストールしたすべてのストレージノードで、次の手順を実行します。

10. ボリュームとデータストアが起動してアクセス可能であることを確認してください。

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"
- "SolidFire と Element ソフトウェアドキュメントセンター"

H615C および H610S ノードの DC 電源装置を交換してください

H615C および H610S ノードは、 2 ~ 48 V ~ 60 V の DC 電源装置をサポートします。これらのユニットは、 H615C または H610S ノードを発注するとオプションのアドオンとして提供されます。これらの手順を使用して、シャーシ内の AC 電源装置を取り外して DC 電源装置ユニットに交換したり、障害のある DC 電源装置を新しい DC 電源装置ユニットに交換したりできます。

必要なもの

- 障害のある DC 電源装置を交換する場合は、交換用 DC 電源装置ユニットを調達しておきます。
- シャーシ内の AC 電源装置を DC 装置と交換する場合は、手順のダウンタイムを考慮する必要があります。
- 静電放電（ ESD ）リストバンドを装着するか、静電気防止処置を施しておきます。
- 電源装置の要件が満たされていることを確認します。
  - 電源電圧：–（ 48-60 ） V DC
  - 消費電流： 37A （最大）

- ブレーカーの要件： 40A ブレーカー

- 環境内のマテリアルが RoHS の仕様に従っていることを確認しておきます。
- ケーブルの要件が満たされていることを確認します。
  - UL 10 AWG 、最大 2 m （より線）黒ケーブル × 1 （ 48 ～ 60 V DC ）
  - UL 10 AWG 、最大 2 m （より線）赤ケーブル × 1 （ V DC リターン）
  - UL 10 AWG 、最大 2 m 緑 / 黄ケーブル、緑、黄のストライプ、より線（安全アース） 1 本

このタスクについて

この手順は、次のノードモデルに該当します。

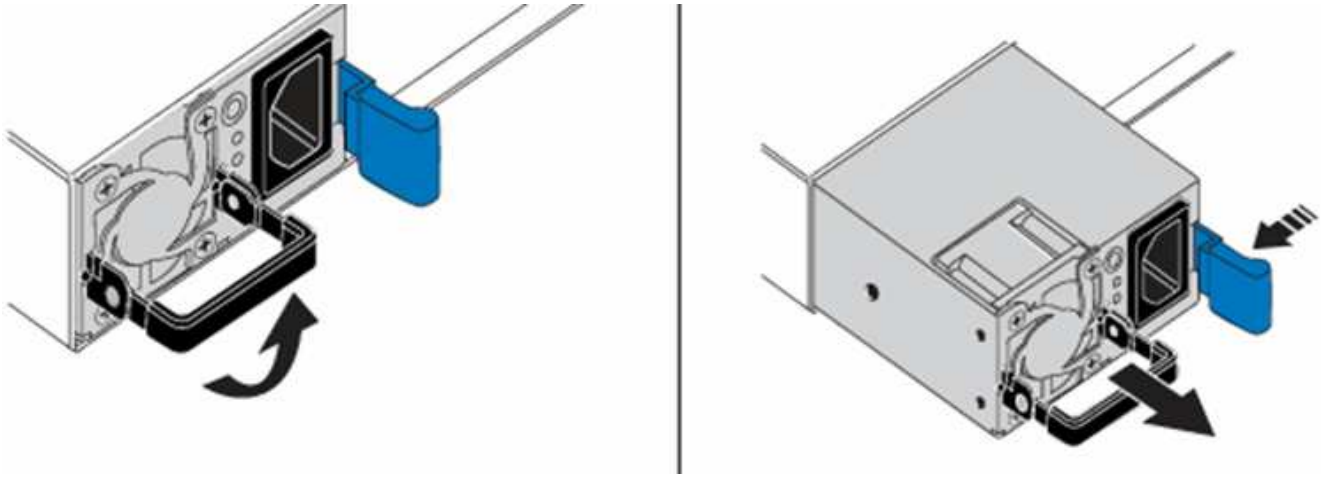
- 1 ラックユニット（ 1U ） H615C コンピューティングシャーシ
- 1U H610S ストレージシャーシ

H615C および H610S では、 2U / 4 ノードシャーシとは異なり、ノードとシャーシが別々のコンポーネントではないため、「ノード」と「シャーシ」は同じ意味で使用されます。

AC 電源装置と DC 電源装置を混在させることはできません。

手順

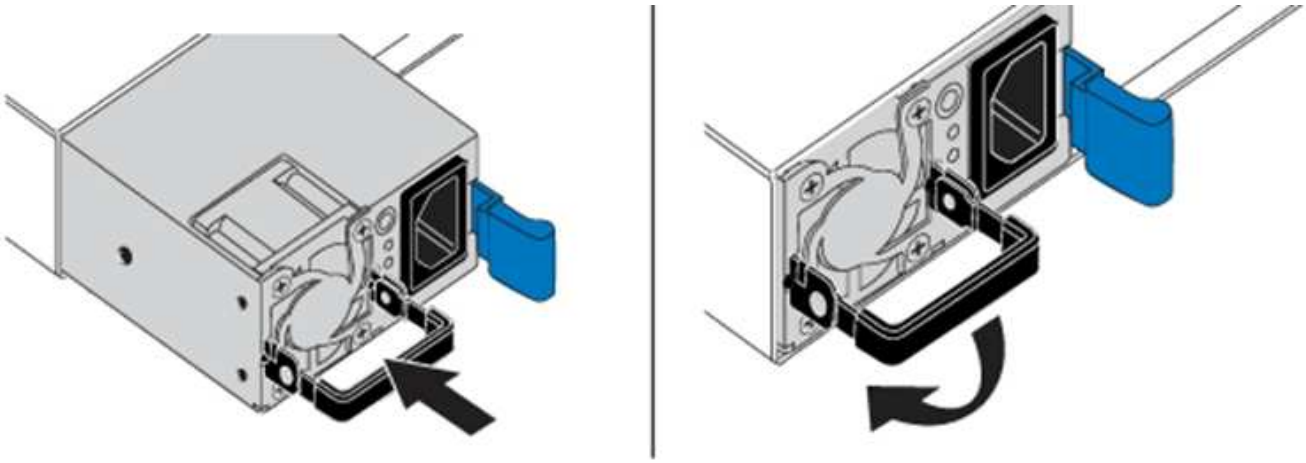
1. 電源装置をオフにして、電源コードを抜きます。障害のある DC 電源装置を交換する場合は、電源をオフにして、青色のコネクタに挿入されているすべてのケーブルを取り外します。
2. カムハンドルを持ち上げ、青色のラッチを押して電源装置ユニットを引き出します。



図は一例です。シャーシ内の電源装置の位置とリリースボタンの色は、シャーシのタイプによって異なります。

両手で電源装置の重量を支えてください。

3. 両手で電源装置の端をシャーシの開口部に合わせ、カムハンドルを使用して装置をシャーシにそっと押し込んで、カムハンドルを直立位置に戻します。



4. DC 電源装置をケーブル接続します。DC 電源装置と電源をケーブル接続する際には、電源がオフになっていることを確認してください。
   a. 青のコネクタに黒、赤、緑 / 黄色のケーブルを差し込みます。
   b. 青色のコネクタを DC 電源装置ユニットと電源に差し込みます。

5. DC 電源装置の電源をオンにします。

> DC 電源装置がオンラインになると、電源装置の LED が点灯します。緑色の LED ライトは、電源装置が正常に動作していることを示します。

6. 出荷時の箱に同梱されている手順に従って、障害が発生したユニットをネットアップに返送してください。

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"
- "SolidFire と Element ソフトウェアドキュメントセンター"

コンピューティングノードの DIMM を交換します

ノード全体を交換する代わりに、 NetApp HCI コンピューティングノード内の障害のある Dual Inline Memory Module （ DIMM ）を交換することができます。

必要なもの

- この手順を開始する前に、ネットアップサポートに連絡して交換用パーツを入手しておく必要があります。交換作業にはサポートが必要です。まだ行っていない場合は、にお問い合わせください "サポート"。
- ノードの電源をオフにするか再投入して NetApp セーフモードでノードをブートしてターミナルユーザインターフェイス（ TUI ）にアクセスする必要があるため、システムを停止することを検討しておきます。

このタスクについて

この手順は、次のコンピューティングノードモデルに該当します。

- H410C ノード。2U NetApp HCI シャーシに H410C ノードを挿入しておきます。
- H610C ノード：H610C ノードはシャーシに組み込まれています。
- H615C ノード：H615C ノードはシャーシに内蔵されています。

> H410C ノードと H615C ノードには、ベンダーの異なる DIMM が搭載されています。異なるベンダーの DIMM を 1 つのシャーシに混在させないようにします。

> H610C および H615C では、ノードとシャーシが別々のコンポーネントではないため、「シャーシ」と「ノード」は同じ意味で使用されます。

コンピューティングノードの DIMM の交換手順は次のとおりです。

- DIMM を交換する準備をします
- シャーシから DIMM を交換します

DIMM を交換する準備をします

DIMM に問題が発生すると、 VMware ESXi は「メモリ構成エラー」、「メモリ訂正不能 ECC 」、「重大への移行」、「メモリ重大な過熱」などのアラートを表示します。しばらくするとアラートが消えた場合でも、ハードウェアの問題が解決しないことがあります。障害が発生した DIMM の診断と対処を行う必要があります。障害のある DIMM に関する情報は vCenter Server から入手できます。vCenter Server で確認できる情報よりも多くの情報が必要な場合は、 TUI でハードウェアチェックを実行する必要があります。

手順

1. エラーを記録したスロットを次のように特定します。
   a. H615C の場合は、次の手順を実行します。
      i. BMC UI にログインします。
      ii. [ログとレポート *>*IPMI イベントログ *] を選択します。
      iii. イベントログで、メモリエラーを探し、エラーが記録されているスロットを特定します。

b. H410C の場合は、次の手順を実行します。

   i. BMC UI にログインします。

   ii. [* サーバーの正常性 * > * 正常性イベントログ *] を選択します。

   iii. イベントログで、メモリエラーを探し、エラーが記録されているスロットを特定します。

Severity	Time Stamp	Sensor	Description
!	[redacted]	BIOS OEM(Memory Error)	DIMM Receive Enable training is failed. (P2-DIMMF1) - Assertion

2. DIMM メーカーのパーツ番号を確認する手順を実行します。

> H410C ノードと H615C ノードにはメーカーが異なる DIMM が搭載されています。同じシャーシ内に異なるタイプの DIMM を混在させないでください。障害が発生した DIMM のメーカーを特定し、同じタイプの交換用 DIMM を注文する必要があります。

a. BMC にログインして、ノードでコンソールを起動します。

b. キーボードの * F2 * を押して、 * システムのカスタマイズ / ログの表示 * メニューを表示します。

c. プロンプトが表示されたら、パスワードを入力します。

> このパスワードは、 NetApp HCI のセットアップ時に NetApp Deployment Engine で設定したパスワードと同じである必要があります。

a. [システムのカスタマイズ] メニューから下矢印を押して [トラブルシューティングオプション] に移動し、 **Enter** キーを押します。

b. Troubleshooting Mode Options メニューから、上矢印または下矢印を使用して ESXi シェルおよび SSH を有効にします。これらは、デフォルトでは無効になっています。

c. Esc> キーを 2 回押して、トラブルシューティングオプションを終了します。

d. 次のいずれかのオプションを使用して 'biosDump' コマンドを実行します

オプション	手順
オプション A	i. ホストの IP アドレスと定義したルートクレデンシャルを使用して、 ESXi ホスト（コンピューティングノード）に接続します。 ii. 「 biosDump 」コマンドを実行します。次の出力例を参照してください。 `Memory Device:#30 Location: "P1-DIMMA1" Bank: "P0_Node0_Channel0_Dimm0" Manufacturer:"Samsung" Serial: "38EB8380" Asset Tag: "P1-DIMMA1_AssetTag (date:18/15)" Part Number: "M393A4K40CB2-CTD" Memory Array: #29 Form Factor: 0x09(DIMM) Type: 0x1a (DDR4) Type Detail: 0x0080 (Synchronous) Data Width: 64 bits (+8 ECC bits) Size: 32 GB`
オプション B	i. Alt + F1 * キーを押してシェルに入り、ノードにログインしてコマンドを実行します。

3. 次の手順については、ネットアップサポートにお問い合わせください。ネットアップサポートでパーツの交換を処理するには、次の情報が必要です。
   - ノードのシリアル番号
   - クラスタ名
   - BMC UI からシステムイベントログの詳細を取得します
   - 「 biosDump 」コマンドの出力

シャーシから **DIMM** を交換します

シャーシ内の障害のある DIMM を物理的に取り外して交換する前に、すべての作業が完了していることを確認します "準備手順"。

> DIMM は、取り外したスロットと同じスロットで交換する必要があります。

手順

1. vCenter Server にログインしてノードにアクセスします。

2. エラーを報告しているノードを右クリックし、ノードをメンテナンスモードにするオプションを選択します。
3. 仮想マシン（ VM ）を使用可能な別のホストに移行します。

> 移行手順については、 VMware のドキュメントを参照してください。

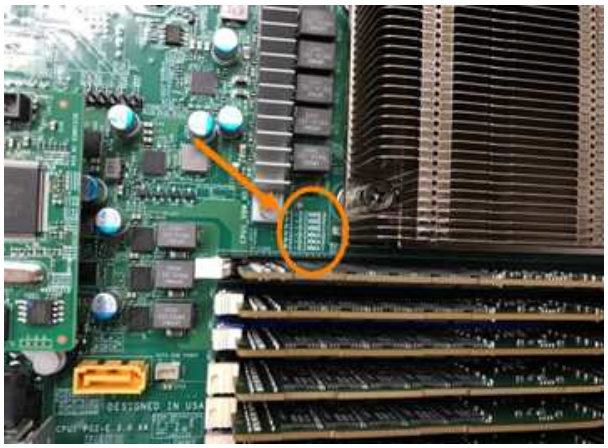
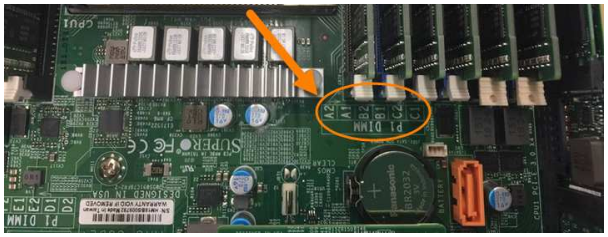
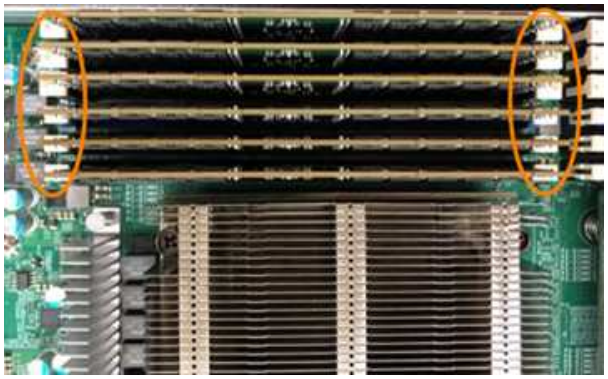
4. シャーシまたはノードの電源をオフにします。

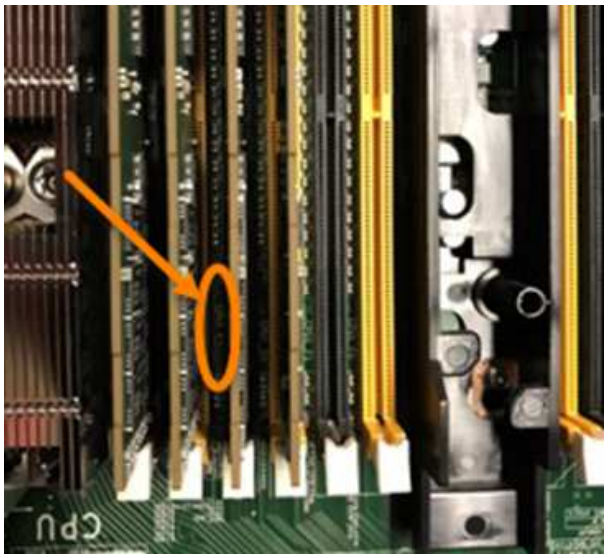
> H610C または H615C シャーシの場合は、シャーシの電源をオフにします。2U / 4 ノードシャーシに配置された H410C ノードでは、障害のある DIMM を搭載したノードの電源のみをオフにします。

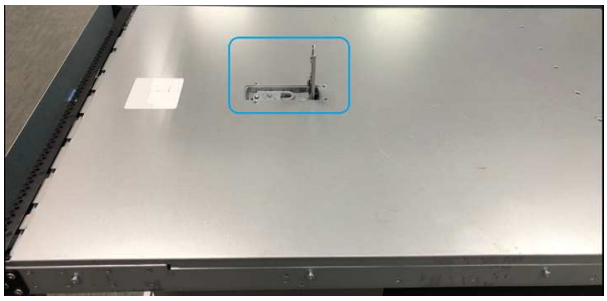
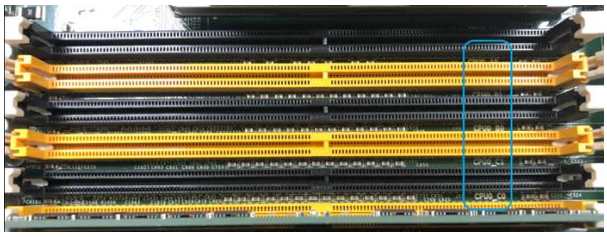
5. 電源ケーブルとネットワークケーブルを外し、ノードまたはシャーシをラックから慎重に引き出して、静電気防止処置を施した平らな場所に置きます。

> ケーブルにねじれタイを使用することを検討してください。

6. シャーシカバーを開いて DIMM を交換する前に、静電気防止処置を施します。
7. 使用しているノードモデルに関連する手順を実行します。

ノードモデル	手順
H410C	a. 前の手順でメモしたスロット番号とマザーボードの番号を照合して、障害が発生した DIMM を特定します。マザーボード上の DIMM スロット番号を示すサンプルイメージを次に示します。   b. 2 つの固定クリップを外側に押し、 DIMM を慎重に引き上げます。保持クリップを示すサンプル画像を次に示します。  c. 交換用 DIMM を正しく取り付けます。DIMM をスロットに正しく挿入すると、 2 つのクリップが所定の位置に固定されます。 DIMM の背面のみに触れてください。DIMM の他の部分を押すと、ハードウェアが破損する可能性があります。 d. ノードを NetApp HCI シャーシに取り付けます。ノードを所定の位置にスライドさせたら、カチッという音がして固定されたことを確認します。

ノードモデル	手順
H610C	a. 次の図に示すように、カバーを持ち上げます。  b. ノード背面の 4 本の青色のロックネジを緩めます。2 本のロックネジの位置を示すサンプルイメージを次に示します。他の 2 本はノードの反対側にあります。  c. 両方の PCI カードダミーを取り外します。 d. GPU とエアフローカバーを取り外します。 e. 前の手順でメモしたスロット番号とマザーボードの番号を照合して、障害が発生した DIMM を特定します。以下は、マザーボード上の DIMM スロット番号の位置を示すサンプル画像です。  2 つの固定クリップを外側に押し、 DIMM を慎重に引き上げます。

ノードモデル	手順
H615C	a. 次の図に示すように、カバーを持ち上げます。  b. GPU （ H615C ノードに GPU が搭載されている場合）と通気カバーを取り外します。  c. 前の手順でメモしたスロット番号とマザーボードの番号を照合して、障害が発生した DIMM を特定します。以下は、マザーボード上の DIMM スロット番号の位置を示すサンプル画像です。  d. 2 つの固定クリップを外側に押し、 DIMM を慎重に引き上げます。 e. 交換用 DIMM を正しく取り付けます。DIMM をスロットに正しく挿入すると、 2 つのクリップが所定の位置に固定されます。 DIMM の背面のみに触れてください。DIMM の他の部分を押すと、ハードウェアが破損する可能性があります。 f. エアーフローカバーを取り付けます。 g. カバーをノードに戻します。 H610C シャーシをラックに設置して、シャーシを所定の位置にスライドさせたときにカチッと音がすることを確認します。

8. 電源ケーブルとネットワークケーブルを差し込みます。[h]すべてのポートのライトが点灯していることを確認します。
9. ノードの設置時に電源が自動的にオンにならない場合は、ノード前面の電源ボタンを押します。
10. vSphere にノードが表示されたら、名前を右クリックして、ノードの保守モードを解除します。
11. ハードウェア情報を次のように確認します。
    a. ベースボード管理コントローラ（ BMC ） UI にログインします。
    b. [システム]>[ハードウェア情報 *] を選択し、リストされている DIMM を確認します。

次のステップ

ノードが通常動作に戻ったら、 vCenter で [Summary] タブをチェックして、メモリ容量が期待どおりであることを確認します。

DIMM が正しく取り付けられていないと、ノードは正常に動作しますが、メモリ容量は想定よりも少なくなります。

DIMM の交換手順が完了したら、 vCenter の Hardware Status タブで警告とエラーをクリアできます。これは、交換したハードウェアに関連するエラーの履歴を消去する場合に行います。"詳細はこちら。"。

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"
- "SolidFire と Element ソフトウェアドキュメントセンター"

ストレージノードのドライブを交換

ドライブに障害が発生した場合や、ドライブの摩耗度がしきい値を下回った場合は、交換する必要があります。Element ソフトウェア UI および VMware vSphere Web Client のアラームで、ドライブで障害が発生したときや障害が発生したときに通知されます。障害が発生したドライブをホットスワップできます。

このタスクについて

この手順は、 H410S および H610S ストレージノードのドライブを交換する場合の手順です。削除したドライブはオフラインになります。ドライブ上のデータはすべて削除され、クラスタ内の他のドライブに移行されます。システム内の他のアクティブドライブへのデータ移行には、クラスタの容量利用率とアクティブな I/O に応じて、数分から 1 時間かかります。

ドライブの取り扱いに際してのベストプラクティス

ドライブの取り扱いに際しては、次のベストプラクティスに従う必要があります。

- 取り付け準備ができるまで、ドライブを ESD バッグに入れたままにしておきます。
- ESD バッグを手で開けるか、バッグの上部をハサミで切り落とします。
- 作業中は常に ESD リストストラップを着用し、シャーシの塗装されていない表面部分にリストストラッ

プを接触させます。

- 取り外し、取り付け、持ち運びなど、ドライブを扱うときは常に両手で作業してください。
- ドライブをシャーシに無理に押し込まないでください。
- ドライブを発送するときは、必ず承認された梱包材を使用し
- ドライブ同士を積み重ねないでください。

ドライブの追加と取り外しを行う際のベストプラクティス

クラスタにドライブを追加し、クラスタからドライブを取り外す際は、次のベストプラクティスに従う必要があります。

- スライスドライブを追加する前に、ブロックドライブをすべて追加し、ブロックの同期が完了していることを確認します。
- Element ソフトウェア 10.x 以降の場合は、すべてのブロックドライブを一度に追加します。一度に 3 つ以上のノードでこの処理を行わないようにしてください。
- Element ソフトウェア 9.x 以前では、 3 本のドライブを一度に追加して完全に同期したあとに、次の 3 つのグループを追加してください。
- スライスドライブを取り外し、ブロックドライブを取り外す前にスライスの同期が完了したことを確認します。
- 一度に 1 つのノードからすべてのブロックドライブを削除します。ブロックの同期がすべて完了してから次のノードに進んでください。

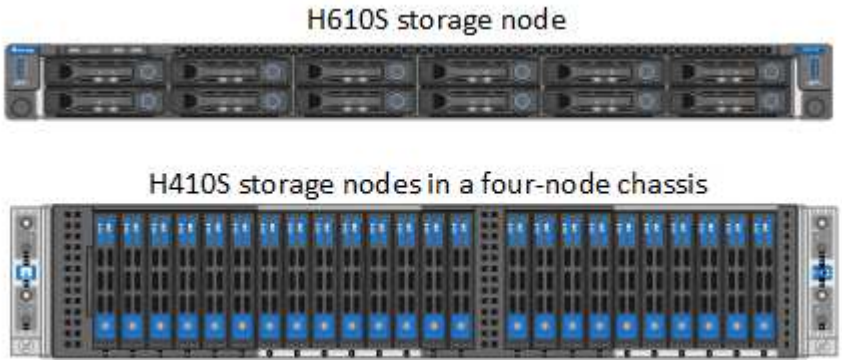
手順

1. vCenter Server 用 Element プラグインの NetApp Element ソフトウェア UI または NetApp Element 管理拡張ポイントを使用して、クラスタからドライブを削除します。

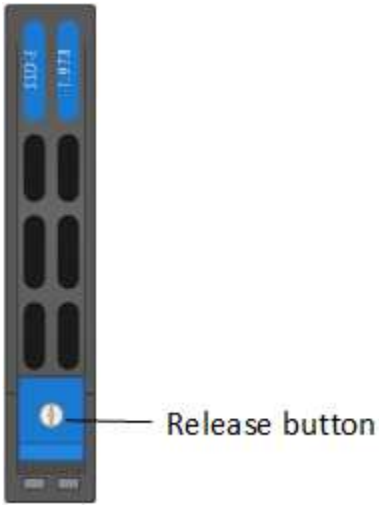
オプション	手順
Element UI を使用	a. Element UI で、 * Cluster > Drives * を選択します。 b. [Failed （失敗）] をクリックして、障害が発生したドライブのリストを表示します。 c. 障害が発生したドライブのスロット番号をメモします。この情報は、障害が発生したドライブをシャーシ内で特定する際に必要になります。 d. 削除するドライブの * アクション * をクリックします。 e. [削除（ Remove ）] をクリックします。 これで、ドライブをシャーシから物理的に取り外すことができます。

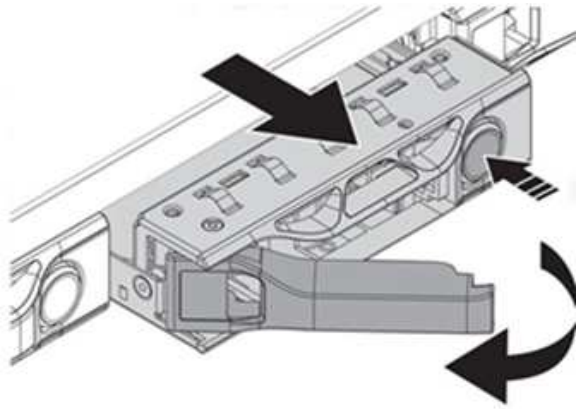
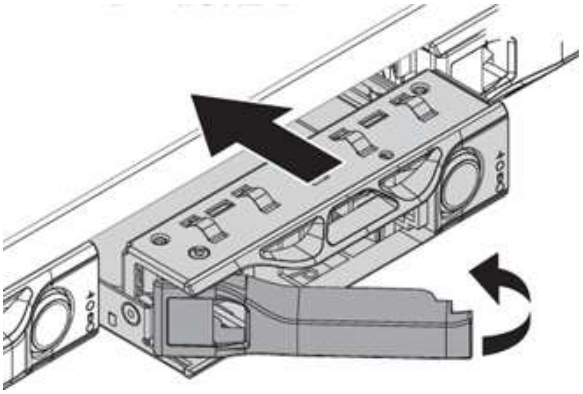
オプション	手順
vCenter Server UI 用 Element プラグインを使用する	a. vSphere Web Client の NetApp Element Management 拡張ポイントで、 * NetApp Element Management > Cluster * の順に選択します。 b. 複数のクラスタが追加されている場合は、このタスクに使用するクラスタがナビゲーションバーで選択されていることを確認してください。 c. ドロップダウンリストから「 * All * 」を選択して、ドライブの完全なリストを表示します。 d. 削除する各ドライブのチェックボックスを選択します。 e. ドライブの取り外し * を選択します。 f. 操作を確定します。 アクティブドライブを削除するための十分な容量がない場合は、ドライブの削除を確定した時点でエラーメッセージが表示されます。エラーを解決したら、ドライブをシャーシから物理的に取り外すことができます。

2. シャーシからドライブを交換します。
   a. 交換用ドライブを開封し、ラックの近くの静電気防止処置を施した平らな場所に置きます。障害ドライブをネットアップに返却するときのために、梱包材は保管しておいてください。H610S ストレージノードとドライブを搭載した H410S ストレージノードの前面図は次のとおりです。



   b. ノードモデルに応じて次の手順を実行します。

ノードモデル	手順
H410S	i. シリアル番号（サービスタグ）と Element UI でメモした番号を照合して、ノードを特定します。シリアル番号は、各ノードの背面にあるステッカーに記載されています。ノードを特定したら、スロット情報を使用して、障害ドライブが取り付けられているスロットを特定できます。ドライブは、 A ~ D のアルファベット順と 0 ~ 5 のアルファベット順に配置されています。 ii. ベゼルを取り外します。 iii. 障害が発生したドライブのリリースボタンを押します。  リリースボタンを押すと、ドライブのカムハンドルが途中まで開き、ドライブがミッドプレーンから外れます。 iv. カムハンドルを開き、両手でドライブを慎重に引き出します。 v. 静電気防止処置を施した平らな場所にドライブを置きます。 vi. 両手を使用して、交換用ドライブをスロットに最後まで挿入します。 vii. カムハンドルをカチッと音がするまで押し下げます。 viii. ベゼルを再度取り付けます。 ix. ドライブを交換したことをネットアップサポートに通知します。ネットアップサポートから障害ドライブの返却手順をお知らせします。

ノードモデル	手順
H610S	i. Element UI から取得した障害ドライブのスロット番号を、シャーシの番号と照合します。障害が発生したドライブの LED は黄色に点灯します。 ii. ベゼルを取り外します。 iii. リリースボタンを押し、次の図に示すように障害が発生したドライブを取り外します。  ドライブをシャーシから引き出す前に、トレイハンドルが完全に開いていることを確認します。 iv. ドライブを引き出し、静電気防止処置を施した平らな場所に置きます。 v. 交換用ドライブをドライブベイに挿入する前に、ドライブのリリースボタンを押します。ドライブトレイのハンドルが開きます。  vi. 力を入れすぎないように交換用ドライブを挿入します。ドライブが完全に挿入されると、カチッという音がします。 vii. ドライブトレイのハンドルを慎重に閉じます。 ベゼルを再度取り付けます。 ドライブを交換したことをネットアップサポートに通知します。ネットアップサポートが

3. vCenter Server 用 Element プラグインの Element UI または NetApp Element Management 拡張ポイントを使用して、ドライブをクラスタに再度追加します。

ら障害ドライブの返却手順をお知らせします。

> 既存のノードに新しいドライブをインストールすると、ドライブが自動的に * Available * として Element UI に登録されます。ドライブがクラスタに参加できるようにするには、ドライブをクラスタに追加する必要があります。

オプション	手順
Element UI を使用	a. Element UI で、 * Cluster > Drives * を選択します。 b. 使用可能なドライブのリストを表示するには、「 * Available * 」を選択します。 c. 追加するドライブの Actions （アクション）アイコンを選択し、 * Add * （追加）を選択します。
vCenter Server UI 用 Element プラグインを使用する	a. vSphere Web Client の NetApp Element Management 拡張ポイントで、 * NetApp Element Management > Cluster > Drives * の順に選択します。 b. Available （使用可能）ドロップダウンリストからドライブを選択し、 * Add * （追加）を選択します。 c. 操作を確定します。

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"
- "SolidFire と Element ソフトウェアドキュメントセンター"

H410C ノードを交換してください

CPU の障害、その他のマザーボードの問題、または電源が入らない場合は、コンピューティングノードを交換する必要があります。この手順は H410C ノードに該当します。NetApp HCI Bootstrap OS バージョン 1.6P1 以降の H410C コンピューティングノードを使用している場合は、メモリ DIMM に障害が発生した場合でもノードを交換する必要はありません。障害が発生した DIMM のみを交換する必要があります。ノード内の DIMM で障害が発生していない場合は、交換用ノードで使用できます。

交換用ノードには、 NetApp HCI 環境の他のコンピューティングノードと同じバージョンの NetApp HCI Bootstrap OS を搭載している必要があります。

NetAppでは、NetApp Deployment Engineを使用して交換用コンピューティングノードを追加することを推奨しています。ESXiのインストールにNetApp Deployment Engineを使用できない場合は、NetAppナレッジベースの記事を参照してください。 "NetApp HCIコンピューティングノードにESXiを手動でインストールする方法"。

必要なもの

- コンピューティングノードの交換が必要であることを確認します。
- 交換用コンピューティングノードを用意します。交換用ノードを注文する場合は、ネットアップサポートにお問い合わせください。コンピューティングノードには、 Bootstrap OS がインストールされた状態で出荷されます。ノードは、最新バージョンの Bootstrap OS を搭載した工場出荷状態です。次のシナリオでは、ノードで Return to Factory Image （ RTFI ）プロセスを実行する必要があります。
  - 現在の NetApp HCI インストールで、最新バージョンよりも前のバージョンの Bootstrap OS を実行しています。この場合、 RTFI プロセスによって、新しいノードが NetApp HCI のインストールを実行している OS バージョンにダウングレードされます。
  - 出荷された交換用ノードでは、最新バージョンよりも前のブートストラップ OS バージョンが実行されており、ノードを交換する NetApp HCI インストールではすでに最新バージョンが実行されています。この場合、 RTFI プロセスによって、新しいノードの OS バージョンが最新バージョンにアップグレードされます。を参照してください "USB キーを使用して RTFI を実行する方法（ログインが必要）" および "BMC を使用して RTFI を実行する方法（ログインが必要）"。
- 静電放電（ ESD ）リストバンドを装着するか、静電気防止処置を施しておきます。
- コンピューティングノードに接続される各ケーブルにラベルを付けておきます。

このタスクについて

VMware vSphere Web Client のアラームは、ノードで障害が発生したときに通知されます。VMware vSphere Web Client で障害が発生したノードのシリアル番号を、ノード背面のステッカーに記載されているシリアル番号と照合する必要があります。

H410C コンピューティングノードを交換する場合は、次の点を考慮してください。

- H410C コンピューティングノードは、 NetApp HCI の既存のコンピューティングノードやストレージノードと同じシャーシおよびクラスタに混在させることができます。
- H410C コンピューティングノードは高電圧（ 200~240VAC ）でのみ動作します。既存の NetApp HCI システムに H410C ノードを追加する場合は、電源要件が満たされていることを確認しておく必要があります。

手順の概要

ここでは、この手順の概要を示します。
[手順1：コンピューティングノードを交換する準備]
[手順2：シャーシ内のコンピューティングノードを交換する]
手順3：NetApp HCI 1.7以降でコンピューティングノードアセットを削除する
[手順4：クラスタにコンピューティングノードを追加する]
[手順5：2ノードおよび3ノードのストレージクラスタの監視ノードを再導入する]

次に、システムに固有の条件がある場合に実行する必要があるその他のタスクを示します。

- "コンピューティングリソースを解放するには、監視ノードを削除してください"

- 交換用ノードを受け取った場合は、パスワードを変更します BMC の標準以外のパスワード
- ノードの BMC ファームウェアをアップグレードします

手順1：コンピューティングノードを交換する準備

ノードでホストされている仮想マシン（ VM ）を使用可能なホストに移行して、障害ノードをクラスタから削除する必要があります。シリアル番号やネットワークの情報など、障害が発生したノードの詳細を確認する必要があります。

手順

1. VMware vSphere Web Client で、次の手順を実行して VM を別の使用可能なホストに移行します。

   移行手順については、 VMware のドキュメントを参照してください。

2. 次の手順を実行してインベントリからノードを削除します。手順は、現在のインストール環境の NetApp HCI のバージョンによって異なります。

NetApp HCI のバージョン番号	手順
NetApp HCI 1.3 以降	a. 障害が発生したノードを選択し、 * Monitor > Hardware Status > Sensors * を選択します。 b. 障害が発生したノードのシリアル番号をメモします。これにより、ノード背面のシリアル番号がメモしたシリアル番号とステッカーで示されたシリアル番号と一致するノードを識別できます。 c. 障害が発生したノードを右クリックし、 * Connection > Disconnect * を選択します。 d. 「 * はい * 」を選択して操作を確定します。 e. 障害が発生したノードを右クリックし、 * インベントリから削除 * を選択します。 f. 「 * はい * 」を選択して操作を確定します。

NetApp HCI のバージョン番号	手順
NetApp HCI 1.3 より前のバージョン	a. ノードを右クリックし、 * インベントリから削除 * を選択します。 b. 障害が発生したノードを選択し、 * Monitor > Hardware Status > Sensors * を選択します。 c. ノード 0 のシリアル番号をメモします。シリアル番号は障害が発生したノードのシリアル番号です。これにより、ノード背面のシリアル番号がメモしたシリアル番号とステッカーで示されたシリアル番号と一致するノードを識別できます。 d. 障害が発生したノードを選択し、 * Manage > Networking > VMkernel adapters * を選択して、リストされた 4 つの IP アドレスをコピーします。この情報は、 VMware ESXi でネットワークの初期設定手順を実行するときに再利用できます。

手順2：シャーシ内のコンピューティングノードを交換する

クラスタから障害ノードを削除したら、ノードをシャーシから取り外し、交換用ノードを設置できます。

ここで説明する手順を実行する前に、静電気防止処置を施してください。

手順

1. 静電気防止処置を施します。
2. 新しいノードを開封し、シャーシの近くの平らな場所に置きます。障害が発生したノードをネットアップに返却するときは、パッケージ化の資料を保管しておいてください。
3. 取り外すノードの背面に挿入されている各ケーブルにラベルを付けます。新しいノードを設置したら、ケーブルを元のポートに戻す必要があります。
4. ノードからすべてのケーブルを外します。
5. DIMM を再利用する場合は取り外します。
6. ノードの右側にあるカムハンドルを下に引き、両方のカムハンドルを使用してノードを引き出します。カムハンドルを下に引くと、そのハンドルの方向を示す矢印が表示されます。もう一方のカムハンドルは動かず、ノードを引き出せるようになっています。

   シャーシからノードを引き出すときは、両手でノードを支えてください。

7. ノードをレベルサーフェスに配置します。ノードをパッケージ化してネットアップに返却する必要があります。
8. 交換用ノードを設置
9. カチッという音がするまでノードを押し込みます。

ノードをシャーシに挿入する際に力を入れすぎないように注意してください。

ノードの電源がオンになっていることを確認します。自動的に電源がオンにならない場合は、ノード前面の電源ボタンを押します。

10. 前の手順で障害ノードから取り外した DIMM は、交換用ノードに挿入します。

障害が発生したノードの同じスロットの DIMM を交換する必要があります。

11. 元々ケーブルを外したポートにケーブルを再接続します。ケーブルを外したときに付けたラベルは、ガイドとして役立ちます。

シャーシ背面の通気口がケーブルやラベルで塞がれていると、過熱によってコンポーネントで早期に障害が発生する可能性があります。ケーブルをポートに無理に押し込まないでください。ケーブル、ポート、またはその両方が破損する可能性があります。

交換用ノードがシャーシ内の他のノードと同じ方法でケーブル接続されていることを確認します。

手順3：NetApp HCI 1.7以降でコンピューティングノードアセットを削除する

NetApp HCI 1.7 以降では、ノードを物理的に交換したあと、管理ノード API を使用してコンピューティングノードのアセットを削除します。REST API を使用するには、ストレージクラスタで NetApp Element ソフトウェア 11.5 以降が実行されていて、バージョン 11.5 以降が実行されている必要があります。

手順

1. 管理ノードの IP アドレスに続けて「 /mnode ： https://[IP address 」 /mnode 」と入力します
2. 「 * Authorize * 」またはロックアイコンを選択し、 API を使用する権限を付与するクラスタ管理者のクレデンシャルを入力します。
   a. クラスタのユーザ名とパスワードを入力します。
   b. 値が選択されていない場合は、タイプドロップダウンリストからリクエスト本文を選択します。
   c. mnode-client の値がまだ入力されていない場合は、クライアント ID を入力します。クライアントシークレットの値は入力しないでください。
   d. セッションを開始するには、 * Authorize * を選択します。

   承認しようとしたあとに「 Auth Error TypeError: Failed to fetch 」というエラーメッセージが表示された場合は、クラスタの MVIP の SSL 証明書を受け入れる必要があります。トークン URL の IP をコピーし、別のブラウザタブに IP を貼り付けて、再度承認します。トークンの期限が切れた後にコマンドを実行しようとすると、「 Error: Unauthorized 」エラーが表示されます。この応答が表示された場合は、再度承認してください。

3. 使用可能な承認ダイアログボックスを閉じます
4. [*Get/assets] を選択します。

5. [* 試してみてください *] を選択します。
6. [* Execute] を選択します。応答の本文を下にスクロールしてコンピューティングセクションに移動し、障害が発生したコンピューティングノードの親と ID の値をコピーします。
7. 削除 / アセット / ｛ asset_id ｝ / コンピュートノード / ｛ compute_id ｝ * を選択します。
8. [* 試してみてください *] を選択します。手順 7 で取得した親と ID の値を入力します。
9. [* Execute] を選択します。

手順4：クラスタにコンピューティングノードを追加する

コンピューティングノードをクラスタに再度追加する必要があります。手順は、実行している NetApp HCI のバージョンによって異なります。

NetApp HCI 1.6P1 以降

NetApp Hybrid Cloud Control は、 NetApp HCI 環境でバージョン 1.6P1 以降が実行されている場合にのみ使用できます。

必要なもの

- 分散仮想スイッチを使用している環境を拡張する場合は、 NetApp HCI で使用している vSphere インスタンスに vSphere Enterprise Plus ライセンスがあることを確認しておきます。
- NetApp HCI で使用しているすべての vCenter インスタンスと vSphere インスタンスでライセンス期間が終了していないことを確認しておきます。
- 既存のノードと同じネットワークセグメントに未使用の空いている IPv4 アドレスがあることを確認してください（新しいノードは、同じタイプの既存のノードと同じネットワークにインストールする必要があります）。
- vCenter 管理者アカウントのクレデンシャルを準備しておきます。
- 新しいノードのネットワークトポロジとケーブル配線が既存のストレージクラスタまたはコンピューティングクラスタと同じであることを確認しておきます。
- "イニシエータとボリュームアクセスグループを管理します" をクリックします。

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。例：

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

2. NetApp HCI ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
3. [インストールの展開] ペインで、 [* 展開 *] を選択します。
4. ローカルのNetApp HCIストレージクラスタ管理者のクレデンシャルを指定してNetApp Deployment Engineにログインします。

> Lightweight Directory Access Protocolのクレデンシャルを使用してログインすることはできません。

5. ようこそページで、 * はい * を選択します。
6. [End User License] ページで、次のアクションを実行します。
   a. VMware のエンドユーザライセンス契約を読みます。
   b. 契約条件に同意する場合は、契約テキストの最後にある「 * 同意します * 」を選択します。
7. 「 * Continue * 」を選択します。
8. vCenter のページで、次の手順を実行します。
   a. NetApp HCI 環境に関連付けられている vCenter インスタンスの FQDN または IP アドレスと管理者のクレデンシャルを入力します。
   b. 「 * Continue * 」を選択します。
   c. 新しいコンピューティングノードを追加する既存の vSphere データセンターを選択するか、「 * 新しいデータセンターの作成 * 」を選択して新しいコンピューティングノードを新しいデータセンターに追加します。

      Create New Datacenter を選択すると、 Cluster フィールドに自動的に値が入力されます。

   d. 既存のデータセンターを選択した場合は、新しいコンピューティングノードを関連付ける vSphere クラスタを選択します。

      選択したクラスタのネットワーク設定を NetApp HCI が認識できない場合は、管理、ストレージ、 vMotion ネットワーク用の VMkernel と vmnic のマッピングが導入時のデフォルトに設定されていることを確認してください。

   e. 「 * Continue * 」を選択します。
9. ESXi のクレデンシャルページで、追加するコンピューティングノードの ESXi root パスワードを入力します。NetApp HCI の初期導入時に作成したパスワードを使用する必要があります。
10. 「 * Continue * 」を選択します。
11. 新しい vSphere データセンタークラスタを作成した場合は、ネットワークトポロジページで、追加する新しいコンピューティングノードと一致するネットワークトポロジを選択します。

    ケーブル 2 本のオプションを選択できるのは、コンピューティングノードがケーブル 2 本のトポロジを使用しており、既存の NetApp HCI 環境に VLAN ID が設定されている場合のみです。

12. Available Inventory ページで、既存の NetApp HCI インストールに追加するノードを選択します。

    一部のコンピューティングノードは、使用している vCenter のバージョンでサポートされる最高レベルで EVC を有効にしないと、インストール環境に追加できません。そのようなコンピューティングノードについては、 vSphere クライアントを使用して EVC を有効にしてください。有効にしたら、 * Inventory * ページを更新して、もう一度コンピューティングノードを追加してください。

13. 「 * Continue * 」を選択します。
14. オプション：新しい vSphere データセンタークラスタを作成した場合は、ネットワーク設定ページで既存

の NetApp HCI 環境からネットワーク情報をインポートします。既存のクラスタから設定をコピー * チェックボックスを選択します。これにより、各ネットワークにデフォルトゲートウェイとサブネットの情報が設定されます。

15. [ネットワークの設定] ページで、初期展開から一部のネットワーク情報が検出されました。シリアル番号順に表示された新しいコンピューティングノードには、新しいネットワーク情報を割り当てる必要があります。新しいコンピューティングノードについて、次の手順を実行します。
    a. NetApp HCI が名前のプレフィックスを検出した場合は、 [検出された名前のプレフィックス] フィールドから名前のプレフィックスをコピーし、 [* ホスト名 *] フィールドに追加した新しい一意のホスト名のプレフィックスとして挿入します。
    b. [* Management IP Address] フィールドに、管理ネットワークサブネットにあるコンピューティングノードの管理 IP アドレスを入力します。
    c. vMotion IP Address フィールドに、 vMotion ネットワークサブネットにあるコンピューティングノードの vMotion IP アドレスを入力します。
    d. iSCSI A-IP Address フィールドに、 iSCSI ネットワークサブネットにあるコンピューティングノードの最初の iSCSI ポートの IP アドレスを入力します。
    e. iSCSI B-IP Address フィールドに、 iSCSI ネットワークサブネット内にあるコンピューティングノードの 2 番目の iSCSI ポートの IP アドレスを入力します。
16. 「 * Continue * 」を選択します。
17. [ネットワーク設定] セクションの [確認] ページでは、新しいノードが太字で表示されます。いずれかのセクションの情報を変更する必要がある場合は、次の手順を実行します。
    a. そのセクションの * 編集 * を選択します。
    b. 変更が完了したら、以降のページで [続行] をクリックして [確認] ページに戻ります。
18. オプション：ネットアップがホストしている SolidFire Active IQ サーバにクラスタの統計情報とサポート情報を送信しないようにする場合は、最後のチェックボックスをオフにします。これにより、 NetApp HCI のリアルタイムの健常性診断の監視機能が無効になります。この機能を無効にすると、ネットアップによる NetApp HCI のプロアクティブなサポートと監視が行われなくなるため、本番環境が影響を受ける前に問題を検出して解決できなくなります。
19. [* ノードの追加 *] を選択します。リソースの追加と設定の進捗状況は、 NetApp HCI で監視できます。
20. オプション：新しいコンピューティングノードが vCenter に表示されることを確認します。

NetApp HCI 1.4 P2 、 1.4 、および 1.3

NetApp HCI のインストールでバージョン 1.4P2 、 1.4 、または 1.3 を実行している場合は、ネットアップ導入エンジンを使用してクラスタにノードを追加できます。

必要なもの

- 分散仮想スイッチを使用している環境を拡張する場合は、 NetApp HCI で使用している vSphere インスタンスに vSphere Enterprise Plus ライセンスがあることを確認しておきます。
- NetApp HCI で使用しているすべての vCenter インスタンスと vSphere インスタンスでライセンス期間が終了していないことを確認しておきます。
- 既存のノードと同じネットワークセグメントに未使用の空いている IPv4 アドレスがあることを確認してください（新しいノードは、同じタイプの既存のノードと同じネットワークにインストールする必要があります）。
- vCenter 管理者アカウントのクレデンシャルを準備しておきます。

- 新しいノードのネットワークトポロジとケーブル配線が既存のストレージクラスタまたはコンピューティングクラスタと同じであることを確認しておきます。

手順

1. 既存のいずれかのストレージ・ノードの管理 IP アドレス（ http://<storage_node_management_IP_address>/` ）を参照します
2. ローカルのNetApp HCIストレージクラスタ管理者のクレデンシャルを指定してNetApp Deployment Engineにログインします。

   Lightweight Directory Access Protocolのクレデンシャルを使用してログインすることはできません。

3. 「 * インストールを展開する * 」を選択します。
4. ようこそページで、 * はい * を選択します。
5. [End User License] ページで、次のアクションを実行します。
   a. VMware のエンドユーザライセンス契約を読みます。
   b. 契約条件に同意する場合は、契約テキストの最後にある「 * 同意します * 」を選択します。
6. 「 * Continue * 」を選択します。
7. vCenter のページで、次の手順を実行します。
   a. NetApp HCI 環境に関連付けられている vCenter インスタンスの FQDN または IP アドレスと管理者のクレデンシャルを入力します。
   b. 「 * Continue * 」を選択します。
   c. 新しいコンピューティングノードを追加する既存の vSphere データセンターを選択します。
   d. 新しいコンピューティングノードを関連付ける vSphere クラスタを選択します。

      CPU 世代が既存のコンピューティングノードと異なるコンピューティングノードを追加する場合は、制御用 vCenter インスタンスで Enhanced vMotion Compatibility （ EVC ）を無効にしてから、次に進む必要があります。これにより、拡張完了後に vMotion を使用できます。

   e. 「 * Continue * 」を選択します。
8. ESXi のクレデンシャルページで、追加するコンピューティングノードの ESXi 管理者クレデンシャルを作成します。NetApp HCI の初期導入時に作成したマスタークレデンシャルを使用する必要があります。
9. 「 * Continue * 」を選択します。
10. Available Inventory ページで、既存の NetApp HCI インストールに追加するノードを選択します。

    一部のコンピューティングノードは、使用している vCenter のバージョンでサポートされる最高レベルで EVC を有効にしないと、インストール環境に追加できません。そのようなコンピューティングノードについては、 vSphere クライアントを使用して EVC を有効にしてください。有効にしたら、インベントリページをリフレッシュし、コンピューティングノードの追加をもう一度実行してください。

11. 「 * Continue * 」を選択します。

12. [Network Settings] ページで、次の手順を実行します。
    a. 初期導入時に検出された情報を確認します。
    b. シリアル番号順に表示された新しいコンピューティングノードのそれぞれについて、新しいネットワーク情報を割り当てる必要があります。新しいストレージノードごとに、次の手順を実行します。
        i. NetApp HCI が命名プレフィックスを検出した場合は、 [検出された命名プレフィックス] フィールドからコピーし、 [ホスト名] フィールドに追加した新しい一意のホスト名のプレフィックスとして挿入します。
        ii. Management IP Address フィールドに、管理ネットワークサブネットにあるコンピューティングノードの管理 IP アドレスを入力します。
        iii. vMotion IP Address フィールドに、 vMotion ネットワークサブネットにあるコンピューティングノードの vMotion IP アドレスを入力します。
        iv. iSCSI A-IP Address フィールドに、 iSCSI ネットワークサブネットにあるコンピューティングノードの最初の iSCSI ポートの IP アドレスを入力します。
        v. iSCSI B-IP Address フィールドに、 iSCSI ネットワークサブネット内にあるコンピューティングノードの 2 番目の iSCSI ポートの IP アドレスを入力します。
    c. 「 * Continue * 」を選択します。
13. [ネットワーク設定] セクションの [確認] ページでは、新しいノードが太字で表示されます。いずれかのセクションの情報を変更する場合は、次の手順を実行します。
    a. そのセクションの * 編集 * を選択します。
    b. 変更が完了したら、以降のページで「 * 続行」を選択して「レビュー」ページに戻ります。
14. オプション：ネットアップがホストしている Active IQ サーバにクラスタの統計情報とサポート情報を送信しないようにする場合は、最後のチェックボックスをオフにします。これにより、 NetApp HCI のリアルタイムの健常性診断の監視機能が無効になります。この機能を無効にすると、ネットアップによる NetApp HCI のプロアクティブなサポートと監視が行われなくなるため、本番環境が影響を受ける前に問題を検出して解決できなくなります。
15. [* ノードの追加 *] を選択します。リソースの追加と設定の進捗状況は、 NetApp HCI で監視できます。
16. オプション：新しいコンピューティングノードが vCenter に表示されることを確認します。

NetApp HCI 1.2 、 1.1 、および 1.0

ノードを物理的に交換したら、そのノードを VMware ESXi クラスタに再度追加して、使用可能なすべての機能を使用できるようにいくつかのネットワーク構成を実行する必要があります。

> これらの手順を実行するには、コンソールまたはキーボード、ビデオ、マウス（ KVM ）が必要です。

手順

1. 次のように、 VMware ESXi バージョン 6.0.0 をインストールして設定します。
    a. リモートコンソールまたは KVM 画面で、 * 電源制御 > 電源リセットの設定 * を選択します。再起動されます。
    b. 起動メニューウィンドウが開いたら、下矢印キーを押して「 * ESXi Install * 」を選択します。

このウィンドウは 5 秒間だけ開いたままになります。5 秒経っても選択しない場合は、ノードを再起動します。

c. Enter キーを押してインストールプロセスを開始します。

d. インストールウィザードの手順に従います。

ESXi をインストールするディスクを選択するよう求められたら、下矢印キーを押して、リストから 2 番目のディスクドライブを選択します。root パスワードの入力を求められたら、 NetApp HCI のセットアップ時に NetApp Deployment Engine で設定したパスワードと同じパスワードを入力する必要があります。

e. インストールが完了したら、 * Enter * を押してノードを再起動します。

デフォルトでは、ノードは NetApp HCI Bootstrap OS で再起動します。VMware ESXi を使用するには、ノードで 1 回限りの設定を実行する必要があります。

2. ノードで VMware ESXi を次のように設定します。

a. NetApp HCI Bootstrap OS Terminal User Interface （ TUI ；ターミナルユーザインターフェイス）ログインウィンドウで、次の情報を入力します。

i. ユーザ名： element

ii. パスワード : catchTheFire!

b. 下矢印キーを押して、 **OK** を選択します。

c. Enter * を押してログインします。

d. メインメニューで、下矢印キーを使用して [* Support Tunnel] > [Open Support Tunnel] を選択します。

e. 表示されたウィンドウで、ポート情報を入力します。

この情報については、ネットアップサポートにお問い合わせください。ネットアップサポートがノードにログインしてブート構成ファイルを設定し、設定作業を完了します。

f. ノードを再起動します。

3. 次のように管理ネットワークを設定します。

a. 次のクレデンシャルを入力して VMware ESXi にログインします。

i. ユーザ名： root

ii. Password ： VMware ESXi のインストール時に設定したパスワード。

このパスワードは、 NetApp HCI のセットアップ時に NetApp Deployment Engine で設定したパスワードと同じである必要があります。

b. Configure Management Network* （管理ネットワークの設定）を選択し、 * Enter * を押します。

c. [ネットワークアダプタ] を選択し、 **Enter** キーを押します。

d. [* vmnic2*] と [* vmnic3] を選択し、 Enter * を押します。

e. [**IPv4 Configuration**] を選択し、キーボードのスペースバーを押して、静的設定オプションを選択します。

f. IP アドレス、サブネットマスク、およびデフォルトゲートウェイの情報を入力し、 * Enter * キーを押します。ノードを削除する前にコピーした情報を再利用できます。ここで入力する IP アドレスは、以前にコピーした管理ネットワークの IP アドレスです。

g. **Esc** を押して、 Configure Management Network （管理ネットワークの設定）セクションを終了します。

h. 「 * はい * 」を選択して変更を適用します。

4. 次のように、ノードがクラスタ内の他のノードと同期されるようにネットワークを設定します。

vCenter 5.0以降向けElementプラグイン

Element Plug-in for vCenter 5.0以降では、データセンターにノード（ホスト）を追加します。

a. VMware vSphere Web Clientで、*[インベントリ]>[ホストおよびクラスタ]*を選択します。

b. データセンターを右クリックし、*[ホストの追加]*を選択します。

   ウィザードの指示に従ってホストを追加します。

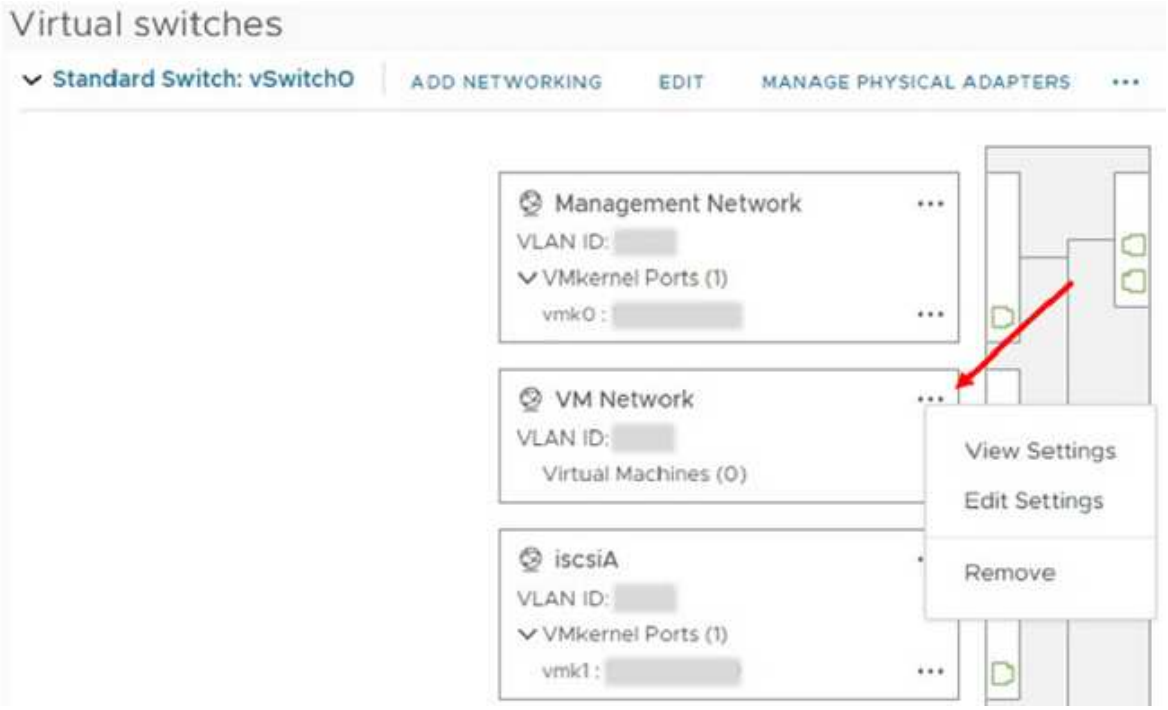
   > ユーザ名とパスワードの入力を求められたら、次のクレデンシャルを使用します。 User name ： root Password ： NetApp HCI のセットアップ時に NetApp Deployment Engine で設定したパスワード

   ノードがクラスタに追加されるまでに数分かかる場合があります。プロセスが完了すると、新しく追加したノードがクラスタの下に表示されます。

c. ノードを選択し、*[設定]>[ネットワーク]>[仮想スイッチ]*を選択して、次の手順を実行します。

   i. [vSwitch0]*を展開します。

   ii. 表示された図で、[VM Network]を選択します ･･･ アイコンの後に* Remove *が表示されます。



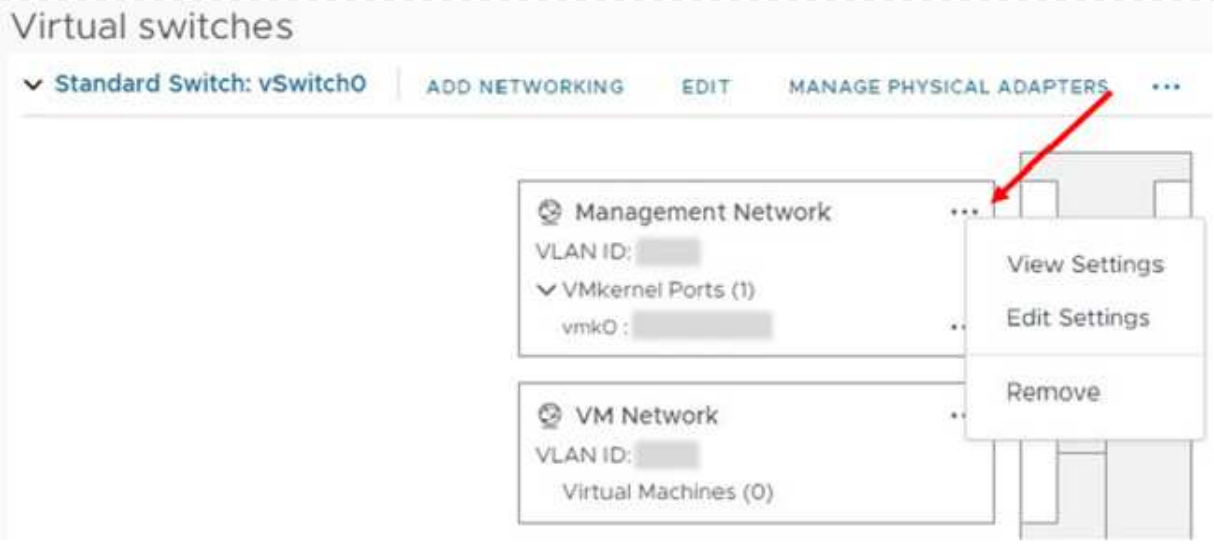
   iii. 操作を確定します。

   iv. vSwitch0ヘッダーで* edit *を選択します。

   v. vSwitch0 - 設定の編集ウィンドウで、 * チーミングとフェイルオーバー * を選択します。

   vi. [Standby adapters]にvmnic3が表示されていることを確認し、*[OK]*を選択します。

d. 表示された図で、[Management Network]を選択します ･･･ アイコンに続いて*[設定の編集]*が表示されます。

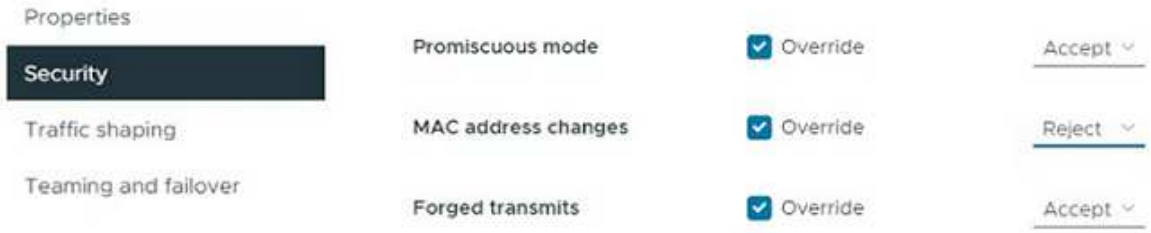


   i. 管理ネットワーク - 設定の編集ウィンドウで、 * チーム化とフェイルオーバー * を選択します。
   ii. [Standby adapters]にvmnic3が表示されていることを確認し、*[OK]*を選択します。

e. vSwitch0ヘッダーの*[Add Networking]*を選択し、表示されるウィンドウに次の詳細を入力します。
   i. 接続タイプには、標準スイッチ * の * 仮想マシンポートグループを選択し、 * 次へ * を選択します。
   ii. ターゲット・デバイスの場合は、*新しい標準スイッチ*を選択し、*次へ*を選択します。
   iii. [Create a Standard Switch]で、vmnic0とvmnic4を[Active adapters]に移動し、*[Next]*を選択します。
   iv. [Connection settings]で、[VM Network]がネットワークラベルであることを確認し、必要に応じてVLAN IDを入力します。
   v. 「 * 次へ * 」を選択します。
   vi. [Ready to Complete]画面を確認し、*[Finish]*を選択します。

f. vSwitch1を展開して* edit *を選択し、次のように設定を編集します。
   i. プロパティ（ Properties ）で MTU を 9000 に設定し、 * OK * を選択します。

g. 表示された図で、[VM Network]を選択します ⋯ アイコンの後に*[編集]*が表示されます。
   i. 「 * Security * 」を選択し、次のオプションを選択します。



   ii. チーム化とフェイルオーバー * を選択し、 * オーバーライド * チェックボックスを選択します。

iii. vmnic0をスタンバイアダプタに移動します。

iv. 「 * OK 」を選択します。

h. vSwitch1ヘッダーで*[Add networking]*を選択し、[Add Networking]ウィンドウで次の詳細を入力します。

i. 接続タイプには、 * VMkernel ネットワークアダプタ * を選択し、 * 次へ * を選択します。

ii. ターゲット・デバイスの場合は、既存の標準スイッチを使用するオプションを選択し、vSwitch1 を参照して * Next * を選択します。

iii. [Create a Standard Switch]で、vmnic1とvmnic5を[Active adapters]に移動し、*[Next]*を選択します。

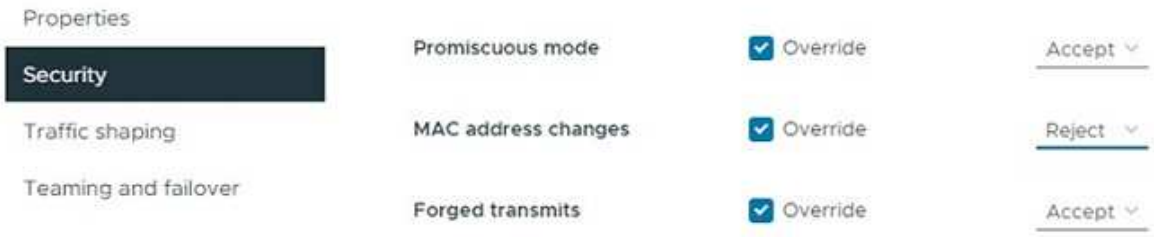
iv. ポートのプロパティで、ネットワークラベルを vMotion に変更し、 Enable services （サービスを有効にする）の下にある vMotion traffic （ vMotion トラフィック）のチェックボックスをオンにして、 * Next （次へ） * を選択します。

v. IPv4 設定で IPv4 情報を入力し、 * 次へ * を選択します。

vi. 続行する準備ができたら、「 * 完了 * 」を選択します。

i. 表示された図で、vMotionを選択します ··· アイコンの後に*[編集]*が表示されます。

i. 「 * Security * 」を選択し、次のオプションを選択します。



ii. チーム化とフェイルオーバー * を選択し、 * オーバーライド * チェックボックスを選択します。

iii. vmnic4をスタンバイアダプタに移動します。

iv. 「 * OK 」を選択します。

j. vSwitch1ヘッダーで*[Add networking]*を選択し、[Add Networking]ウィンドウで次の詳細を入力します。

i. 接続タイプには、 * VMkernel ネットワークアダプタ * を選択し、 * 次へ * を選択します。

ii. ターゲット・デバイスの場合は、*新しい標準スイッチ*を選択し、*次へ*を選択します。

iii. [Create a Standard Switch]で、vmnic1とvmnic5を[Active adapters]に移動し、*[Next]*を選択します。

iv. ポートのプロパティで、ネットワークラベルを iSCSI-B に変更し、 * Next * を選択します。

v. IPv4 設定で IPv4 情報を入力し、 * 次へ * を選択します。

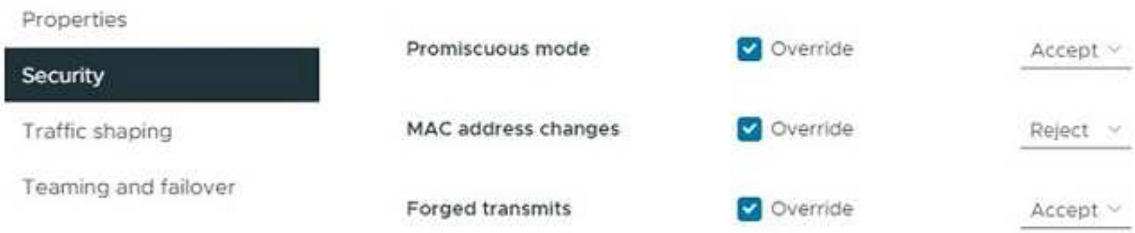
vi. 続行する準備ができたら、「 * 完了 * 」を選択します。

k. vSwitch2 を展開し、 edit *を選択します。

i. プロパティ（ Properties ）で MTU を 9000 に設定し、 * OK * を選択します。

l. 表示された図で、iSCSI-Bを選択します ⋯ アイコンの後に*[編集]*が表示されます。

   i. 「 * Security * 」を選択し、次のオプションを選択します。



   ii. チーム化とフェイルオーバー * を選択し、 * オーバーライド * チェックボックスを選択します。

   iii. vmnic1を未使用のアダプタに移動します。

   iv. 「 * OK 」を選択します。

m. vSwitch1ヘッダーで*[Add networking]*を選択し、[Add Networking]ウィンドウで次の詳細を入力します。

   i. 接続タイプには、 * VMkernel ネットワークアダプタ * を選択し、 * 次へ * を選択します。

   ii. ターゲットデバイスには、既存の標準スイッチを使用するオプションを選択し、 vSwitch2 に移動して * Next * を選択します。

   iii. ポートのプロパティで、ネットワークラベルを iSCSI-A に変更し、 * Next * を選択します。

   iv. IPv4 設定で IPv4 情報を入力し、 * 次へ * を選択します。

   v. 続行する準備ができたら、「 * 完了 * 」を選択します。

n. 表示された図で、[iSCSI-A]を選択します ⋯ アイコンの後に*[編集]*が表示されます。

   i. 「 * Security * 」を選択し、次のオプションを選択します。

   ii. チーム化とフェイルオーバー * を選択し、 * オーバーライド * チェックボックスを選択します。

   iii. 矢印アイコンを使用して、 vmnic5 を未使用のアダプタに移動します。

   iv. 「 * OK 」を選択します。

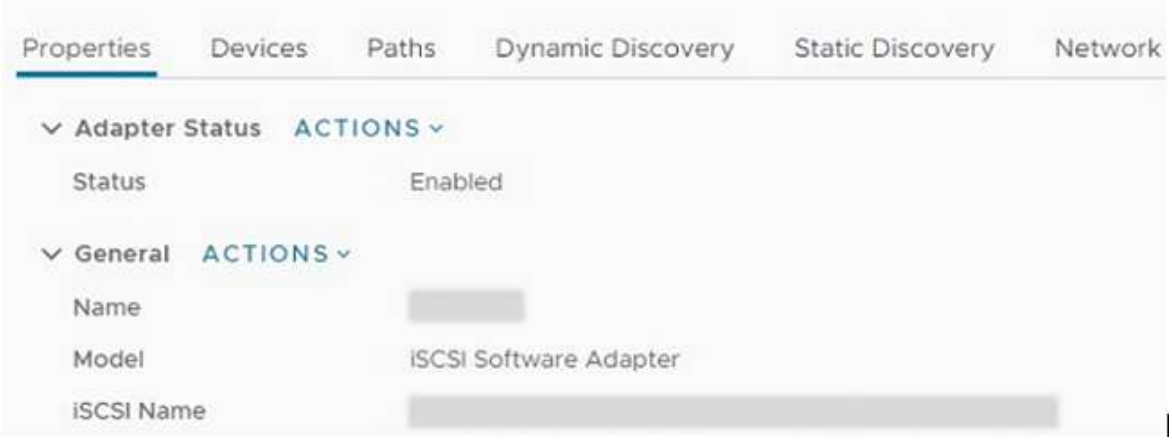
o. 新しく追加したノードを選択し、[設定]タブを開いた状態で*[ストレージ]>[ストレージアダプタ]*を選択し、次の手順を実行します。

   i. [ソフトウェアアダプタの追加]*リストを選択します。

   ii. を選択し、[OK]*を選択します。

   iii. [Storage Adapters]で、iSCSIアダプタを選択します

iv. [Properties]>[General]で、iSCSI名をコピーします。



イニシエータを作成するときに iSCSI 名が必要になります。

p. NetApp SolidFire vCenter Plug-in で、次の手順を実行します。

i. ターゲットインスタンスを選択します。

ii. [Management]*を選択します。

iii. ターゲットクラスタを選択

iv. [Management]>[Initiators]*を選択します。

v. イニシエータの作成 * を選択します。

vi. IQN / WWPN フィールドに、前の手順でコピーした IQN アドレスを入力します。

vii. 「 * OK 」を選択します。

viii. 新しいイニシエータを選択します。

ix. [操作]リスト>[一括操作]を選択し、[アクセスグループに追加]*を選択します。

x. ターゲットアクセスグループを選択し、*[追加]*を選択します。

q. VMware vSphere Web Client の [ストレージアダプタ] で、 iSCSI アダプタを選択し、次の手順を実行します。

i. [Dynamic Discovery]>[Add]*を選択します。

ii. iSCSI Server フィールドに SVIP IP アドレスを入力します。

SVIP IP アドレスを取得するには、「 * NetApp Element 管理 * 」を選択し、SVIP IP アドレスをコピーします。デフォルトのポート番号はそのままにしておきます。3260 にする必要があります。

iii. 「 * OK 」を選択します。

iv. を選択し、[追加]*を選択します。

v. [iSCSI-A]と[iSCSI-B]を選択し、*[OK]*を選択します

vi. [アダプタの再スキャン]*を選択します。

vii. を選択します。新しい**VMFS**ボリュームをスキャンし、 OK *を選択します。

viii. 再スキャンが完了したら、クラスタとデータストア内のボリュームが新しいコンピューティングノード（ホスト）で認識されるかどうかを確認します。

vCenter 4.10以前の**Element**プラグイン

Element Plug-in for vCenter 4.10以前の場合は、ノード（ホスト）をクラスタに追加します。

a. VMware vSphere Web Client で、 * Hosts and Clusters * を選択します。

b. ノードを追加するクラスタを右クリックし、 * ホストの追加 * を選択します。

   ウィザードの指示に従ってホストを追加します。

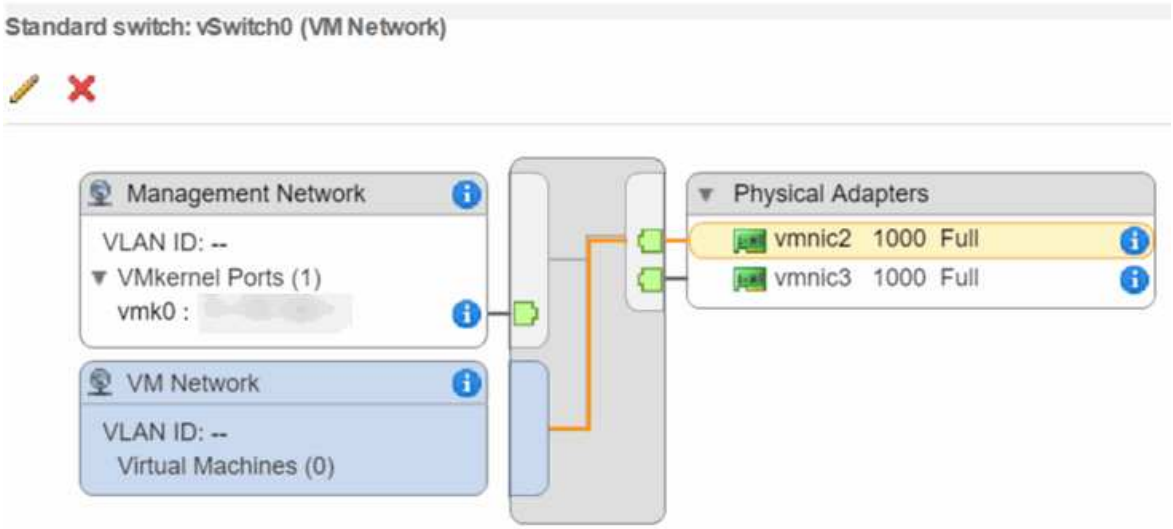
   > ユーザ名とパスワードの入力を求められたら、次のクレデンシャルを使用します。 User name ： root Password ： NetApp HCI のセットアップ時に NetApp Deployment Engine で設定したパスワード

   ノードがクラスタに追加されるまでに数分かかる場合があります。プロセスが完了すると、新しく追加したノードがクラスタの下に表示されます。

c. ノードを選択し、 * Manage > Networking > Virtual switches * を選択して、次の手順を実行します。

   i. vSwitch0 * を選択します。表示されるテーブルに vSwitch0 だけが表示されている。

   ii. 表示された図で、 * VM ネットワーク * を選択し、 * X * をクリックして VM ネットワークポートグループを削除します。



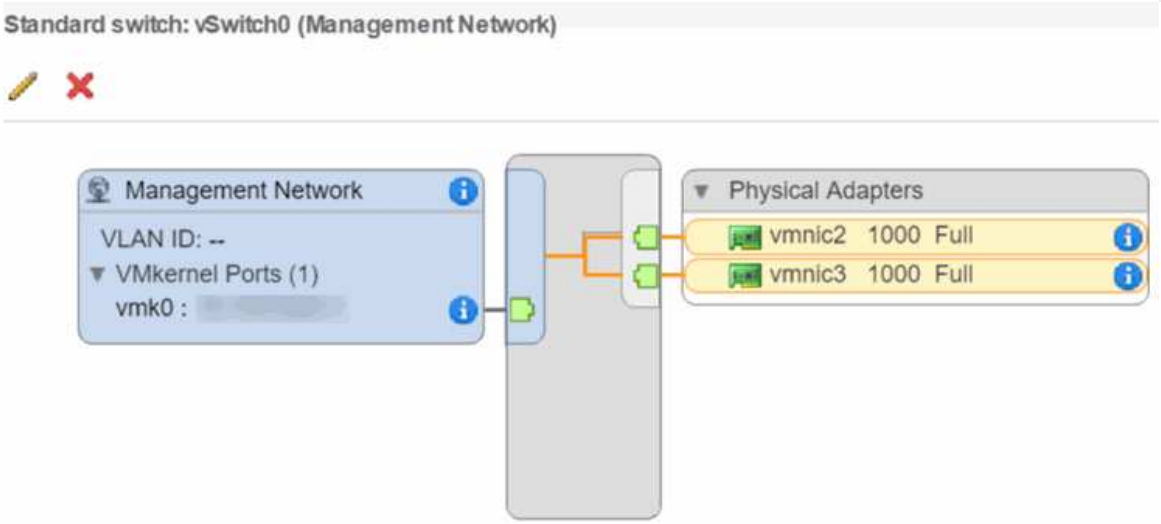
   iii. 操作を確定します。

   iv. vSwitch0 * を選択し、鉛筆アイコンを選択して設定を編集します。

   v. vSwitch0 - 設定の編集ウィンドウで、 * チーミングとフェイルオーバー * を選択します。

   vi. vmnic3 がスタンバイアダプタの下に表示されていることを確認し、 * OK * を選択します。

   vii. 表示された図で、 * 管理ネットワーク * を選択し、鉛筆アイコンを選択して設定を編集します。



viii. 管理ネットワーク - 設定の編集ウィンドウで、 * チーム化とフェイルオーバー * を選択します。

ix. 矢印アイコンを使用して vmnic3 をスタンバイアダプタに移動し、 * OK * を選択します。

d. Actions （アクション）ドロップダウンメニューから * Add Networking * （ネットワークの追加）を選択し、表示されるウィンドウに次の詳細を入力します。

i. 接続タイプには、標準スイッチ * の * 仮想マシンポートグループを選択し、 * 次へ * を選択します。

ii. ターゲット・デバイスの場合 ' 新しい標準スイッチを追加するオプションを選択して ' 次へを選択します *

iii. 「 * + * 」を選択します。

iv. Add Physical Adapters to Switch （スイッチへの物理アダプタの追加）ウィンドウで、 vmnic0 および vmnic4 を選択し、 * OK * を選択します。vmnic0 と vmnic4 がアクティブアダプタの下に表示されるようになりました。

v. 「 * 次へ * 」を選択します。

vi. 接続設定で、 VM ネットワークがネットワークラベルであることを確認し、 * 次へ * を選択します。

vii. 続行する準備ができたら、「 * 完了 * 」を選択します。仮想スイッチのリストに vSwitch1 が表示されます。

e. vSwitch1 * を選択し、鉛筆アイコンを選択して、次のように設定を編集します。

i. プロパティ（ Properties ）で MTU を 9000 に設定し、 * OK * を選択します。表示された図で、 * VM Network * を選択し、鉛筆アイコンをクリックして次のように設定を編集します。

f. 「 * Security * 」を選択し、次のオプションを選択します。

i. チーム化とフェイルオーバー * を選択し、 * オーバーライド * チェックボックスを選択します。

ii. 矢印アイコンを使用して、 vmnic0 をスタンバイアダプタに移動します。

iii. 「 * OK 」を選択します。

g. vSwitch1 を選択した状態で、 Actions （アクション）ドロップダウンメニューから * Add Networking （ネットワークの追加） * を選択し、表示されるウィンドウに次の詳細を入力します。

i. 接続タイプには、 * VMkernel ネットワークアダプタ * を選択し、 * 次へ * を選択します。

ii. ターゲット・デバイスの場合は、既存の標準スイッチを使用するオプションを選択し、 vSwitch1 を参照して * Next * を選択します。

iii. ポートのプロパティで、ネットワークラベルを vMotion に変更し、 Enable services （サービスを有効にする）の下にある vMotion traffic （ vMotion トラフィック）のチェックボックスをオンにして、 * Next （次へ） * を選択します。

iv. IPv4 設定で IPv4 情報を入力し、 * 次へ * を選択します。ここで入力する IP アドレスは、以前にコピーした vMotion IP アドレスです。

v. 続行する準備ができたら、「 * 完了 * 」を選択します。

h. 表示された図で vMotion を選択し、鉛筆アイコンを選択して次のように設定を編集します。

i. 「 * Security * 」を選択し、次のオプションを選択します。

ii. チーム化とフェイルオーバー * を選択し、 * オーバーライド * チェックボックスを選択します。

iii. 矢印アイコンを使用して、 vmnic4 をスタンバイアダプタに移動します。

iv. 「 * OK 」を選択します。

i. vSwitch1 を選択した状態で、 Actions （アクション）ドロップダウンメニューから * Add Networking （ネットワークの追加） * を選択し、表示されるウィンドウに次の詳細を入力します。

i. 接続タイプには、 * VMkernel ネットワークアダプタ * を選択し、 * 次へ * を選択します。

ii. ターゲット・デバイスの場合 ' 新しい標準スイッチを追加するオプションを選択して ' 次へを選択します *

iii. 「 * + * 」を選択します。

iv. Add Physical Adapters to Switch （スイッチへの物理アダプタの追加）ウィンドウで、vmnic1 および vmnic5 を選択し、 * OK * を選択します。vmnic1 と vmnic5 がアクティブアダプタの下に表示されるようになりました。

v. 「 * 次へ * 」を選択します。

vi. ポートのプロパティで、ネットワークラベルを iSCSI-B に変更し、 * Next * を選択します。

vii. IPv4 設定で IPv4 情報を入力し、 * 次へ * を選択します。ここで入力する IP アドレスは、前にコピーした iSCSI-B の IP アドレスです。

viii. 続行する準備ができたら、「 * 完了 * 」を選択します。仮想スイッチのリストに vSwitch2 が表示されます。

j. vSwitch2 * を選択し、鉛筆アイコンを選択して、次のように設定を編集します。

i. プロパティ（ Properties ）で MTU を 9000 に設定し、 * OK * を選択します。

k. 表示された図で「 * iSCSI-B * 」を選択し、鉛筆アイコンを選択して次のように設定を編集します。

i. 「 * Security * 」を選択し、次のオプションを選択します。

ii. チーム化とフェイルオーバー * を選択し、 * オーバーライド * チェックボックスを選択します。

iii. 矢印アイコンを使用して、 vmnic1 を未使用のアダプタに移動します。

iv. 「 * OK 」を選択します。

l. Actions （アクション）ドロップダウンメニューから、 * Add Networking * （ネットワークの追加）を選択し、表示されるウィンドウに次の詳細を入力します。

i. 接続タイプには、 * VMkernel ネットワークアダプタ * を選択し、 * 次へ * を選択します。

ii. ターゲットデバイスには、既存の標準スイッチを使用するオプションを選択し、 vSwitch2 に移動して * Next * を選択します。

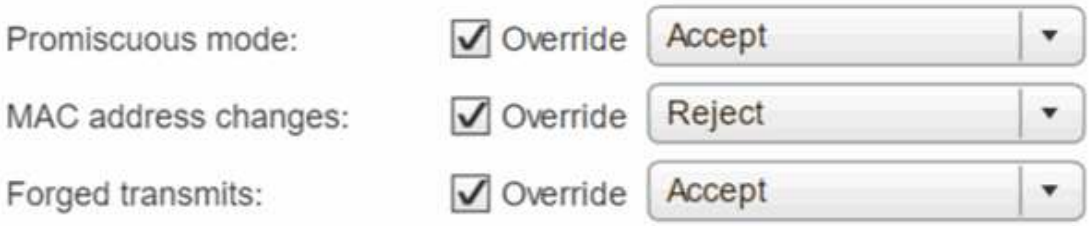
iii. ポートのプロパティで、ネットワークラベルを iSCSI-A に変更し、 * Next * を選択します。

iv. IPv4 設定で IPv4 情報を入力し、 * 次へ * を選択します。ここで入力する IP アドレスは、以前にコピーした iSCSI-A IP アドレスです。

v. 続行する準備ができたら、「 * 完了 * 」を選択します。

m. 表示された図で、 * iscsi-a * を選択し、鉛筆アイコンを選択して次のように設定を編集します。

i. 「 * Security * 」を選択し、次のオプションを選択します。



ii. チーム化とフェイルオーバー * を選択し、 * オーバーライド * チェックボックスを選択します。

iii. 矢印アイコンを使用して、 vmnic5 を未使用のアダプタに移動します。

iv. 「 * OK 」を選択します。

n. 新しく追加したノードを選択し、 [管理] タブを開いた状態で、 [ストレージ] > [ストレージアダプタ] を選択し、次の手順を実行します。

i. 「 * + 」を選択し、「 * Software iSCSI Adapter * 」を選択します。

ii. iSCSI アダプタを追加するには、ダイアログボックスで * OK * を選択します。

iii. ストレージアダプタで iSCSI アダプタを選択し、プロパティタブで iSCSI 名をコピーします。

イニシエータを作成するときに iSCSI 名が必要になります。

o. NetApp SolidFire vCenter Plug-in で、次の手順を実行します。

i. [* Management] > [Initiators] > [Create] を選択します。

ii. [* 単一イニシエータの作成 *] を選択します。

iii. IQN / WWPN フィールドに、前の手順でコピーした IQN アドレスを入力します。

iv. 「 * OK 」を選択します。

v. * Bulk Actions * を選択し、 * Add to Volume Access Group * を選択します。

vi. * NetApp HCI * を選択し、 * Add * を選択します。

p. VMware vSphere Web Client の [ストレージアダプタ] で、 iSCSI アダプタを選択し、次の手順を実行します。

i. [アダプターの詳細] で、 [* ターゲット] 、 [動的検出] 、 [追加] の順に選択します。

ii. iSCSI Server フィールドに SVIP IP アドレスを入力します。

> SVIP IP アドレスを取得するには、「 * NetApp Element 管理 * 」を選択し、SVIP IP アドレスをコピーします。デフォルトのポート番号はそのままにしておきます。3260 にする必要があります。

iii. 「 * OK 」を選択します。ストレージアダプタの再スキャンを推奨するメッセージが表示されます。

iv. 再スキャンアイコンを選択します。

v. [アダプタの詳細] で、 [ネットワークポートバインド **]** を選択し、 **[+*]** を選択します。

vi. iSCSI-B と iSCSI-A のチェックボックスをオンにし、 OK をクリックします。ストレージアダプタの再スキャンを推奨するメッセージが表示されます。

vii. 再スキャンアイコンを選択します。再スキャンが完了したら、クラスタ内のボリュームが新しいコンピューティングノード（ホスト）で認識されるかどうかを確認します。

手順**5**：**2**ノードおよび**3**ノードのストレージクラスタの監視ノードを再導入する

障害が発生したコンピューティングノードを物理的に交換したあと、障害が発生したコンピューティングノードが監視ノードをホストしていた場合は、 NetApp HCI 監視ノード VM を再導入する必要があります。ここで説明する手順は、 2 ノードまたは 3 ノードのストレージクラスタを使用する NetApp HCI 環境に含まれるコンピューティングノードにのみ該当します。

必要なもの

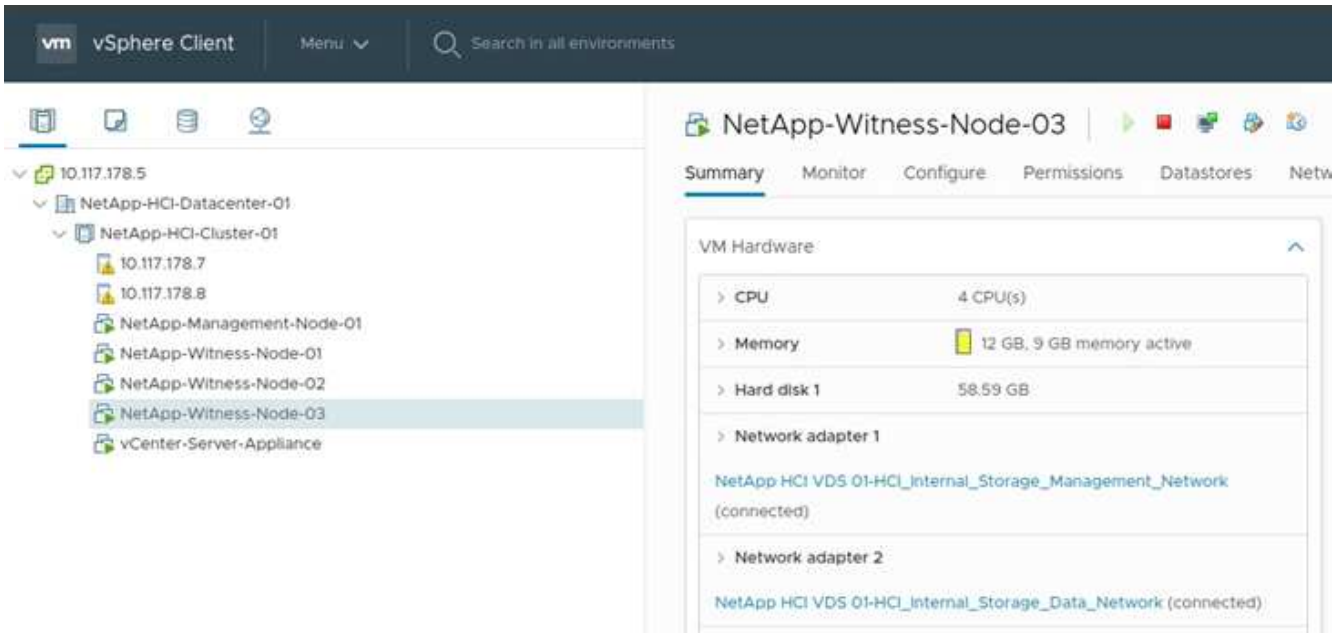
- 次の情報を収集します。
  - ストレージクラスタからクラスタ名
  - 管理ネットワークのサブネットマスク、ゲートウェイ IP アドレス、 DNS サーバ、およびドメインの情報
  - ストレージネットワークのサブネットマスク
- クラスタに監視ノードを追加できるように、ストレージクラスタにアクセスできることを確認してください。
- VMware vSphere Web Client またはストレージクラスタから既存の監視ノードを削除するかどうかを決定する際には、次の条件を考慮してください。
  - 新しい監視ノードに同じ VM 名を使用する場合は、古い監視ノードへの参照を vSphere からすべて削除してください。
  - 新しい監視ノードに同じホスト名を使用する場合は、最初に古い監視ノードをストレージクラスタから削除してください。

クラスタが停止している物理ストレージノードが 2 つだけ（監視ノードがない状態）になっている場合は、古い監視ノードを削除することはできません。このシナリオでは、古い監視ノードを削除する前に、最初に新しい監視ノードをクラスタに追加する必要があります。NetApp Element Management 拡張ポイントを使用して、クラスタから監視ノードを削除できます。

監視ノードを再導入する必要があるタイミング

次のシナリオで監視ノードを再導入する必要があります。

- NetApp HCI 環境の一部である、障害が発生したコンピューティングノードを交換しました。交換したコンピューティングノードには 2 ノードまたは 3 ノードのストレージクラスタがあり、障害が発生したコンピューティングノードが監視ノード VM をホストしていました。
- コンピューティングノードで Return to Factory Image （ RTFI ）手順を実行した。
- 監視ノード VM が破損しています。
- 監視ノード VM が誤って ESXi から削除された。この VM は、 NetApp Deployment Engine を使用した初期導入時に作成したテンプレートを使用して設定します。監視ノード VM の例を次に示します。



VM テンプレートを削除した場合は、ネットアップサポートに問い合わせて監視ノードの .ova イメージを取得して再導入する必要があります。テンプレートは、からダウンロードできます "こちら（ログインが必要です）"。ただし、サポートを利用して設定に関するガイダンスを受ける必要があります。

手順

1. VMware vSphere Web Client で、 * Hosts and Clusters * を選択します。
2. 監視ノード VM をホストするコンピューティングノードを右クリックし、 * 新規仮想マシン * を選択します。
3. [Deploy from template*] を選択し、 [Next] を選択します。
4. ウィザードの手順に従います。

a. 「 * Data Center * 」を選択し、 VM テンプレートを探して「 * Next * 」を選択します。

b. 次の形式で VM の名前を入力します。 NetApp-Witness-Node-##

> ## は数字で置き換えてください。

c. VM の場所はデフォルトのままにして、 * Next * を選択します。

d. デスティネーションのコンピューティングリソースのデフォルトの選択をそのままにして、 * Next * を選択します。

e. ローカルデータストアを選択し、 * Next * を選択します。ローカルデータストアの空きスペースはコンピューティングプラットフォームによって異なります。

f. 展開オプションのリストから * 作成後に仮想マシンをパワーオン * を選択し、 * 次へ * を選択します。

g. 選択内容を確認し、「 * 完了 * 」を選択します。

5. 監視ノードの管理ネットワーク、ストレージネットワーク、およびクラスタを次のように設定します。

a. VMware vSphere Web Client で、 * Hosts and Clusters * を選択します。

b. 監視ノードを右クリックし、電源がオンになっていない場合はオンにします。

c. 監視ノードのサマリビューで、 * Web コンソールの起動 * を選択します。

d. 監視ノードがブートして青い背景のメニューが表示されるまで待ちます。

e. コンソール内の任意の場所を選択して、メニューにアクセスします。

f. 次のように管理ネットワークを設定します。

i. 下矢印キーを押して [ネットワーク] に移動し、 *Enter キーを押して [OK] を押します。

ii. [ネットワークの設定 **]** に移動して、 ***Enter** キーを押して [OK] をクリックします。

iii. 「 * net0 * 」に移動し、「 * Enter * 」を押して OK を押します。

iv. IPv4 フィールドに移動するまで * Tab * を押し、必要に応じてフィールド内の既存の IP を削除して、監視ノードの管理 IP 情報を入力します。サブネットマスクとゲートウェイも確認してください。

> VLAN タギングは VM ホストレベルで適用されず、 vSwitch で処理されます。

v. Tab * を押して OK に移動し、 * Enter * を押して変更を保存します。管理ネットワークの設定が完了すると、画面がネットワークに戻ります。

g. ストレージネットワークを次のように設定します。

i. 下矢印キーを押して [ネットワーク] に移動し、 *Enter キーを押して [OK] を押します。

ii. [ネットワークの設定 **]** に移動して、 ***Enter** キーを押して [OK] をクリックします。

iii. 「 * Net1 * 」に移動し、「 * Enter * 」を押して OK を押します。

iv. IPv4 フィールドに移動するまで * Tab * を押し、必要に応じてフィールド内の既存の IP を削除して、監視ノードのストレージ IP 情報を入力します。

v. Tab * を押して OK に移動し、 * Enter * を押して変更を保存します。

vi. MTU を 9000 に設定します。

クラスタに監視ノードを追加する前に MTU が設定されていない場合は、 MTU 設定の不一致を示すクラスタの警告が表示されます。これにより、ガベージコレクションが実行されず、パフォーマンスの問題が発生するのを防ぐことができます。

vii. Tab * を押して OK に移動し、 * Enter * を押して変更を保存します。ストレージネットワークの構成が完了すると、画面が Network に戻ります。

h. クラスタの設定を次のように行います。

i. Tab* を押して Cancel （キャンセル）に移動し、 **Enter** を押します。

ii. 「 * Cluster settings * 」（クラスタ設定 * ）に移動し、「 * Enter 」（ * Enter ）を押して OK をクリックします。

iii. Tab * を押して [設定の変更] に移動し、 Enter キーを押して [設定の変更] を選択します。

iv. Tab キーを押して [Hostname] フィールドに移動し、ホスト名を入力します。

v. 下矢印キーを押して Cluster フィールドにアクセスし、ストレージクラスタからクラスタ名を入力します。

vi. 「 * tab * 」キーを押して「 OK 」ボタンに移動し、「 * Enter * 」キーを押します。

6. ストレージクラスタに監視ノードを次のように追加します。

a. vSphere Web Client で、 * Shortcuts * タブまたはサイドパネルから NetApp Element 管理拡張ポイントにアクセスします。

b. NetApp Element Management > Cluster * の順に選択します。

c. [ノード * （ Nodes * ）] サブタブを選択します。

d. ドロップダウンリストから「 * Pending * 」を選択して、ノードのリストを表示します。監視ノードは保留中のノードのリストに表示されます。

e. 追加するノードのチェックボックスを選択し、 * ノードの追加 * を選択します。操作が完了すると、ノードがクラスタのアクティブノードのリストに表示されます。

交換用ノードを受け取った場合は、パスワードを変更します **BMC** の標準以外のパスワード

一部の交換用ノードには、 Baseboard Management Controller （ BMC ；ベースボード管理コントローラ）UI 用の標準以外のパスワードが搭載されたものがあります。BMC の標準以外のパスワードを使用して交換用ノードを受け取った場合は、パスワードを default Admin に変更する必要があります。

手順

1. BMC の標準以外のパスワードを使用して交換用ノードを受け取ったかどうかを確認します。

a. 交換用ノードの背面にある IPMI ポートの下にステッカーを探します。IPMI ポートの下にラベルが貼付されている場合は、 BMC の標準以外のパスワードを記載したノードを受け取っていることを意味します。次のサンプルイメージを参照してください。

b. パスワードを書き留めます。

2. ステッカーに記載されている一意のパスワードを使用して BMC UI にログインします。
3. [* 出荷時のデフォルト *] を選択し、 [現在の設定を削除] を選択して、ユーザーのデフォルトを [管理 / 管理者 *] ラジオボタンに設定します。
4. [* Restore] を選択します。
5. ログアウトしてから再度ログインし、クレデンシャルが変更されたことを確認します。

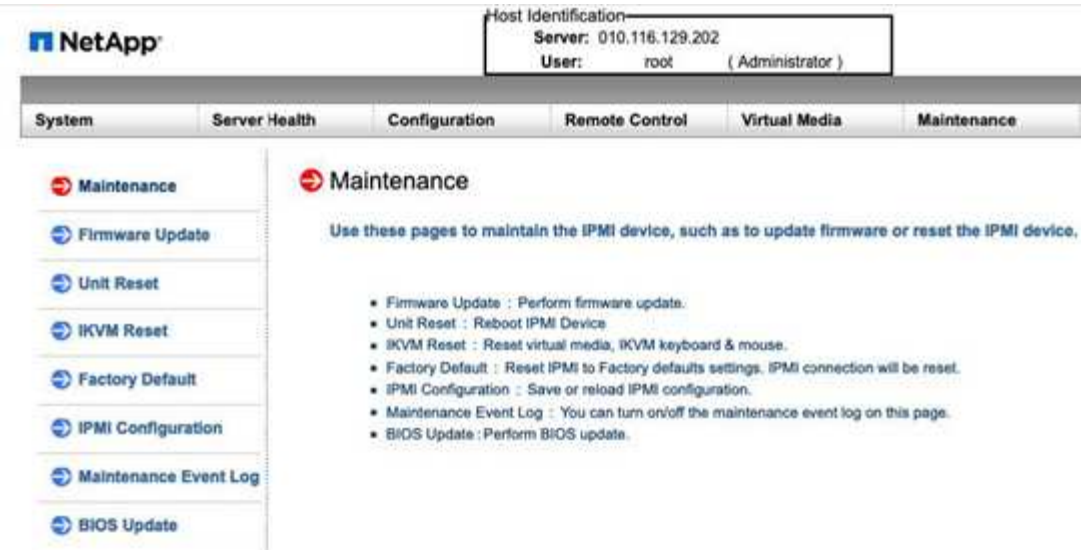
ノードの BMC ファームウェアをアップグレードします

コンピューティングノードを交換したあとで、ファームウェアのバージョンのアップグレードが必要になる場合があります。最新のファームウェアファイルはドロップダウンからダウンロードできます のメニュー "ネットアップサポートサイト（ログインが必要）"。

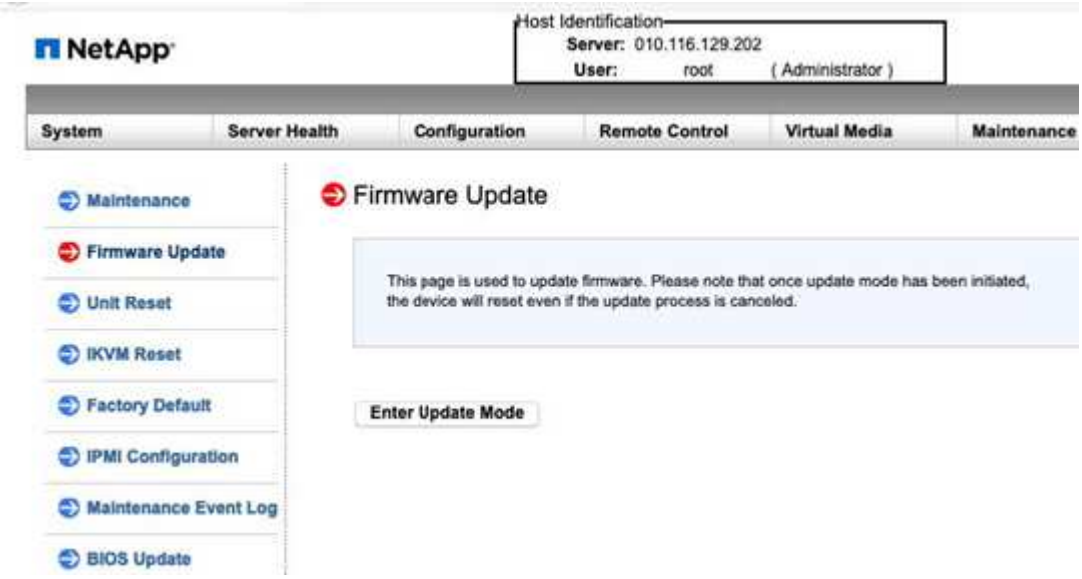
手順

1. ベースボード管理コントローラ（ BMC ） UI にログインします。
2. [* Maintenance] > [Firmware Update] を選択します。

3. BMC コンソールから、 * Maintenance * （メンテナンス）を選択します。



4. [Maintenance] タブで、 UI の左側のナビゲーションから [* Firmware Update*] を選択し、 [*Enter Update Mode] を選択します。



5. 確認ダイアログボックスで「 * はい * 」を選択します。
6. * Browse （参照） * を選択してアップロードするファームウェアイメージを選択し、 * Upload Firmware （ファームウェアのアップロード） * を選択します。ノードのすぐ近くにない場所からファームウェアをロードすると、ロード時間が長くなり、タイムアウトが発生する可能性があります。
7. 構成チェックを保持し、 * アップグレードを開始 * を選択します。アップグレードには約 5 分かかります。アップロード時間が 60 分を超える場合は、アップロードをキャンセルし、ノードの近くにあるローカルマシンにファイルを転送します。セッションがタイムアウトした場合、 BMC UI のファームウェア更新領域にログインしようとすると、いくつかのアラートが表示されることがあります。アップグレードをキャンセルすると、ログインページが表示されます。
8. 更新が完了したら、「 * OK 」を選択し、ノードがリブートするまで待ちます。アップグレード後にログインし、 * システム * を選択して、 * ファームウェア・リビジョン * バージョンがアップロードしたバージョンと一致することを確認します。

詳細については、こちらをご覧ください

- "NetApp HCI のリソースページ"
- "SolidFire と Element ソフトウェアドキュメントセンター"

H410S ノードを交換します

Dual Inline Memory Module （ DIMM ）の障害、 CPU の障害、 Radian カードの問題、その他のマザーボードの問題、または電源が入らない場合には、ストレージノードを交換する必要があります。ストレージノードに障害が発生すると、 VMware vSphere Web Client のアラームで警告されます。NetApp Element ソフトウェア UI を使用して、障害が発生したノードのシリアル番号（サービスタグ）を確認する必要があります。この情報は、シャーシ内で障害が発生したノードの場所を特定する際に必要になります。

必要なもの

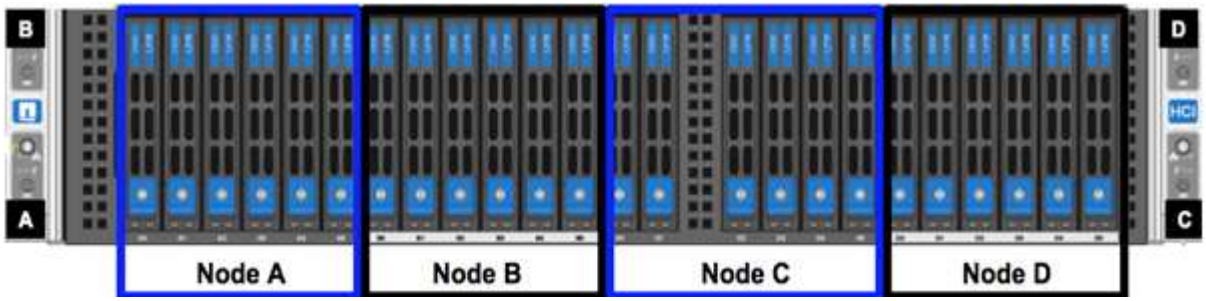
- ストレージノードの交換が必要であることを確認します。
- 交換用ストレージノードが必要です。
- 静電放電（ ESD ）リストバンドを装着するか、静電気防止処置を施しておきます。
- ストレージノードに接続された各ケーブルにラベルを付けておきます。

このタスクについて

交換手順は、 2 ラックユニット（ 2U ） / 4 ノード NetApp HCI シャーシ内の H410S ストレージノードで実行します。

H410S ノードが設置された 4 ノードシャーシの背面図を次に示します。

H410S ノードが設置された 4 ノードシャーシの前面図と各ノードに対応するベイを示します。



手順の概要

ここでは、この手順の概要を示します。[ストレージノードを交換する準備をします]
[シャーシ内のストレージノードを交換します]

[クラスタにストレージノードを追加します]

ストレージノードを交換する準備をします

交換用ノードを設置する前に、障害が発生したストレージノードをクラスタから正しく削除する必要があります。これは、サービスを中断することなく実行できます。障害ストレージノードのシリアル番号は、 Element UI から取得し、ノード背面のステッカーに記載されているシリアル番号と一致する必要があります。

> Dual Inline Memory Module （ DIMM ）障害など、ノードがオンラインで機能している状態で障害が発生した場合に、障害ノードを取り外す前にクラスタからドライブを取り外す必要があります。

手順

1. DIMM に障害が発生した場合は、交換するノードに関連付けられているドライブをクラスタから取り外します。ノードを削除する前に、 vCenter Server 用 Element プラグインの NetApp Element ソフトウェア UI または NetApp Element 管理拡張ポイントを使用できます。
2. NetApp Element ソフトウェア UI または Element Plug-in for vCenter Server の NetApp Element Management 拡張ポイントを使用して、ノードを削除します。

オプション	手順
Element UI を使用	a. Element UI で、 * Cluster > Nodes * を選択します。 b. 障害が発生したノードのシリアル番号（サービスタグ）をメモします。この情報は、ノード背面のステッカーに記載されているシリアル番号と一致する必要があります。 c. シリアル番号をメモしたら、次の手順でクラスタからノードを削除します。 d. 削除するノードに対して * Actions * を選択します。 e. 「 * 削除」を選択します。 これで、ノードをシャーシから物理的に取り外すことができます。

オプション	手順
vCenter Server UI 用 Element プラグインを使用する	a. vSphere Web Client の NetApp Element Management 拡張ポイントで、 * NetApp Element Management > Cluster * の順に選択します。 b. [ノード * （ Nodes * ）] サブタブを選択します。 c. アクティブビューで、削除する各ノードのチェックボックスを選択し、 * アクション > 削除 * を選択します。 d. 操作を確定します。クラスタから削除したノードがすべて Pending 状態のノードのリストに表示されます。

シャーシ内のストレージノードを交換します

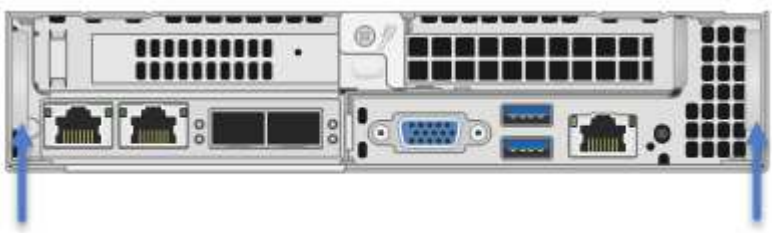
障害が発生したノードを取り外すシャーシの同じスロットに交換用ノードを設置する必要があります。UI からメモしたシリアル番号を使用して、ノードの背面にあるシリアル番号と照合します。

ここで説明する手順を実行する前に、静電気防止処置を施してください。

手順

1. 新しいストレージノードを開封し、シャーシの近くの平らな場所に置きます。障害が発生したノードをネットアップに返却するときは、パッケージ化の資料を保管しておいてください。
2. 取り外すストレージノードの背面に挿入されている各ケーブルにラベルを付けます。新しいストレージノードを設置したら、元のポートにケーブルを差し込む必要があります。
3. ストレージノードからすべてのケーブルを外します。
4. ノードの右側にあるカムハンドルを下に引き、両方のカムハンドルを使用してノードを引き出します。カムハンドルを下に引くと、そのハンドルの方向を示す矢印が表示されます。もう一方のカムハンドルは動かず、ノードを引き出せるようになっています。

   シャーシからノードを引き出すときは、両手でノードを支えてください。



5. ノードをレベルサーフェスに配置します。
6. 交換用ノードを設置
7. カチッという音がするまでノードを押し込みます。

ノードをシャーシに挿入する際に力を入れすぎないように注意してください。

8. 元々ケーブルを外したポートにケーブルを再接続します。ケーブルを外したときに付けたラベルは、ガイドとして役立ちます。

シャーシ背面の通気口がケーブルやラベルで塞がれていると、過熱によってコンポーネントで早期に障害が発生する可能性があります。ケーブルをポートに無理に押し込まないでください。ケーブル、ポート、またはその両方が破損する可能性があります。

交換用ノードがシャーシ内の他のノードと同じ方法でケーブル接続されていることを確認します。

9. ノード前面のボタンを押して電源をオンにします。

クラスタにストレージノードを追加します

ストレージノードをクラスタに再度追加する必要があります。手順は、実行している NetApp HCI のバージョンによって異なります。

必要なもの

- 既存のノードと同じネットワークセグメントに未使用の空いている IPv4 アドレスが必要です（新しいノードは、同じタイプの既存のノードと同じネットワークにインストールする必要があります）。
- 次のいずれかのタイプの SolidFire ストレージクラスタアカウントが必要です。
  - 初期導入時に作成されたネイティブの管理者アカウント
  - Cluster Admin 、 Drives 、 Volumes 、 Nodes の各権限を持つカスタムユーザアカウント
- 新しいノードをケーブル接続して電源をオンにしておきます。
- 設置済みのストレージノードの管理 IPv4 アドレスを確認しておきます。IP アドレスは、 NetApp Element Plug-in for vCenter Server の * NetApp Element Management > Cluster > Nodes * タブで確認できます。
- 新しいノードのネットワークトポロジとケーブル配線が既存のストレージクラスタと同じであることを確認しておきます。

最大限の信頼性を実現するために、ストレージ容量がすべてのシャーシに均等に分割されていることを確認します。

NetApp HCI 1.6P1 以降

NetApp Hybrid Cloud Control は、 NetApp HCI 環境でバージョン 1.6P1 以降が実行されている場合にのみ使用できます。

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。例：

```
https://<ManagementNodeIP>/manager/login
```

2. NetApp HCI ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
3. [インストールの展開] ペインで、 [* 展開 *] を選択します。
4. ローカルのNetApp HCIストレージクラスタ管理者のクレデンシャルを指定してNetApp Deployment Engineにログインします。

> Lightweight Directory Access Protocolのクレデンシャルを使用してログインすることはできません。

5. ようこそページで、 * いいえ * を選択します。
6. 「 * Continue * 」を選択します。
7. Available Inventory ページで、既存の NetApp HCI インストールに追加するストレージノードを選択します。
8. 「 * Continue * 」を選択します。
9. [ネットワークの設定] ページで、初期展開から一部のネットワーク情報が検出されました。シリアル番号順に表示された新しいストレージノードのそれぞれについて、新しいネットワーク情報を割り当てる必要があります。次の手順を実行します。
   a. NetApp HCI が命名プレフィックスを検出した場合は、 [検出された命名プレフィックス] フィールドからコピーし、 [ホスト名] フィールドに追加した新しい一意のホスト名のプレフィックスとして挿入します。
   b. Management IP Address フィールドに、管理ネットワークサブネットにある新しいストレージノードの管理 IP アドレスを入力します。
   c. Storage （ iSCSI ） IP Address フィールドに、 iSCSI ネットワークサブネットにある新しいストレージノードの iSCSI IP アドレスを入力します。
   d. 「 * Continue * 」を選択します。

   > 入力した IP アドレスの検証には時間がかかることがあります。 NetApp HCIIP アドレスの検証が完了すると、 Continue （続行）ボタンが使用可能になります。

10. [ネットワーク設定] セクションの [確認] ページでは、新しいノードが太字で表示されます。いずれかのセクションの情報を変更する必要がある場合は、次の手順を実行します。
    a. そのセクションの * 編集 * を選択します。
    b. 変更が完了したら、以降のページで「 * 続行」を選択して「レビュー」ページに戻ります。
11. オプション：ネットアップがホストしている Active IQ サーバにクラスタの統計情報とサポート情報を送信しないようにする場合は、最後のチェックボックスをオフにします。これにより、 NetApp HCI のリアルタイムの健常性診断の監視機能が無効になります。この機能を無効にすると、ネットアップによる NetApp HCI のプロアクティブなサポートと監視が行われなくなるため、本番環境が影響を受ける前に問題を検出して解決できなくなります。
12. [* ノードの追加 *] を選択します。リソースの追加と設定の進捗状況は、 NetApp HCI で監視できます。
13. オプション：新しいストレージノードが VMware vSphere Web Client に表示されることを確認します。

NetApp HCI 1.4 P2 、 1.4 、および 1.3

NetApp HCI のインストールでバージョン 1.4P2 、 1.4 、または 1.3 を実行している場合は、ネットアップ導

入エンジンを使用してクラスタにノードを追加できます。

手順

1. 既存のいずれかのストレージ・ノードの管理 IP アドレス（ http://<storage_node_management_IP_address>/` ）を参照します
2. ローカルのNetApp HCIストレージクラスタ管理者のクレデンシャルを指定してNetApp Deployment Engineにログインします。

   Lightweight Directory Access Protocolのクレデンシャルを使用してログインすることはできません。

3. 「 * インストールを展開する * 」を選択します。
4. ようこそページで、 * いいえ * を選択します。
5. [* Continue （続行）] をクリックします
6. Available Inventory ページで、 NetApp HCI インストールに追加するストレージノードを選択します。
7. 「 * Continue * 」を選択します。
8. [Network Settings] ページで、次の手順を実行します。
   a. 初期導入時に検出された情報を確認します。シリアル番号順に表示された新しいストレージノードのそれぞれについて、新しいネットワーク情報を割り当てる必要があります。新しいストレージノードごとに、次の手順を実行します。
      i. NetApp HCI が命名プレフィックスを検出した場合は、 [検出された命名プレフィックス] フィールドからコピーし、 [ホスト名] フィールドに追加した新しい一意のホスト名のプレフィックスとして挿入します。
      ii. Management IP Address フィールドに、管理ネットワークサブネットにある新しいストレージノードの管理 IP アドレスを入力します。
      iii. Storage （ iSCSI ） IP Address フィールドに、 iSCSI ネットワークサブネットにある新しいストレージノードの iSCSI IP アドレスを入力します。
   b. 「 * Continue * 」を選択します。
   c. [ネットワーク設定] セクションの [確認] ページでは、新しいノードが太字で表示されます。いずれかのセクションの情報を変更する場合は、次の手順を実行します。
      i. そのセクションの * 編集 * を選択します。
      ii. 変更が完了したら、以降のページで「 * 続行」を選択して「レビュー」ページに戻ります。
9. オプション：ネットアップがホストしている Active IQ サーバにクラスタの統計情報とサポート情報を送信しないようにする場合は、最後のチェックボックスをオフにします。これにより、 NetApp HCI のリアルタイムの健常性診断の監視機能が無効になります。この機能を無効にすると、ネットアップによる NetApp HCI のプロアクティブなサポートと監視が行われなくなるため、本番環境が影響を受ける前に問題を検出して解決できなくなります。
10. [* ノードの追加 *] を選択します。リソースの追加と設定の進捗状況は、 NetApp HCI で監視できます。
11. オプション：新しいストレージノードが VMware vSphere Web Client に表示されることを確認します。

NetApp HCI 1.2 、 1.1 、および 1.0

ノードをインストールすると、ノードの設定に必要なフィールドがターミナルユーザインターフェイス（ TUI

）に表示されます。ノードをクラスタに追加する前に、ノードに必要な設定情報を入力する必要があります。

> TUI を使用して、静的なネットワーク情報とクラスタ情報を設定する必要があります。アウトオブバンド管理を使用している場合は、新しいノードで設定する必要があります。

この手順を実行するには、コンソールまたはキーボード、ビデオ、マウス（ KVM ）が必要です。また、ノードの設定に必要なネットワーク情報とクラスタ情報が必要です。

手順

1. キーボードとモニタをノードに接続TUI が tty1 端末に表示され、 [ネットワーク設定] タブが表示されます。
2. 画面上の指示に従って、ノードの Bond1G および Bond10G ネットワークを設定します。Bond1G については、次の情報を入力する必要があります。
   - IP アドレス障害が発生したノードから管理 IP アドレスを再利用できます。
   - サブネットマスクわからない場合は、ネットワーク管理者からこの情報を提供できます。
   - ゲートウェイアドレス。わからない場合は、ネットワーク管理者からこの情報を提供できます。Bond10G について、次の情報を入力する必要があります。
   - IP アドレス障害が発生したノードからストレージ IP アドレスを再利用できます。
   - サブネットマスクわからない場合は、ネットワーク管理者からこの情報を提供できます。
3. 設定を保存するには「」と入力し、変更を確定するには「 y 」と入力します。
4. c` を入力して ' Cluster タブに移動します
5. 画面上の指示に従って、ノードのホスト名とクラスタを設定します。

   > デフォルトのホスト名を、削除したノードの名前に変更する場合は、ここで変更します。

   > 今後混乱しないように、交換したノードと同じ名前を新しいノードに使用することを推奨します。

6. 「」と入力して設定を保存します。クラスタメンバーシップが「 available 」から「 Pending 」に変わります。
7. NetApp Element Plug-in for vCenter Server で、 * NetApp Element Management > Cluster > Nodes * を選択します。
8. ドロップダウンリストから「 * Pending * 」を選択して、使用可能なノードのリストを表示します。
9. 追加するノードを選択し、 * 追加 * を選択します。

   > ノードがクラスタに追加され、 Nodes > Active の下に表示されるまでに最大 2 分かかることがあります。

   > ドライブを一度に追加するとシステムが停止する可能性があります。ドライブの追加と取り外しに関するベストプラクティスについては、を参照してください "こちらの技術情報アーティクル" （ログインが必要です）。

10. [* Drives] を選択します。

11. ドロップダウンリストから「 * Available * 」を選択して、使用可能なドライブを表示します。
12. 追加するドライブを選択し、 * Add * を選択します。

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"
- "SolidFire と Element ソフトウェアドキュメントセンター"

H610C ノードと H615C ノードを交換してください

シャーシを交換して、 CPU 、マザーボード、または電源が入らない場合にコンピューティングノードの障害を修復する必要があります。NetApp HCI Bootstrap OS バージョン 1.6 以降を実行する H610C コンピューティングノードで障害のある DIMM がある場合は、 DIMM を交換することができ、シャーシを交換する必要はありません。H615C ノードの場合、 DIMM に障害が発生したときはシャーシを交換する必要はありません。交換できるのは障害が発生した DIMM のみです。

> H610C および H615C では、ノードとシャーシが別々のコンポーネントではないため、「ノード」と「シャーシ」は同じ意味で使用されます。
>
> NetAppでは、NetApp Deployment Engineを使用して交換用コンピューティングノードを追加することを推奨しています。ESXiのインストールにNetApp Deployment Engineを使用できない場合は、NetAppナレッジベースの記事を参照してください。 "NetApp HCIコンピューティングノードにESXiを手動でインストールする方法"。

必要なもの

- ノードで障害が発生したことを確認した。
- 交換用シャーシを用意しておきます。交換品を注文する場合は、ネットアップサポートにお問い合わせください。
- 静電放電（ ESD ）リストバンドを装着するか、静電気防止処置を行っておきます。
- シャーシに接続された各ケーブルにラベルを付けておきます。

このタスクについて

VMware vSphere Web Client のアラームでは、ホストで障害が発生するとアラートが通知されます。VMware vSphere Web Client で障害が発生したホストのシリアル番号を、ノード背面のステッカーに記載されているシリアル番号と一致させる必要があります。

手順1：ノードを交換する準備

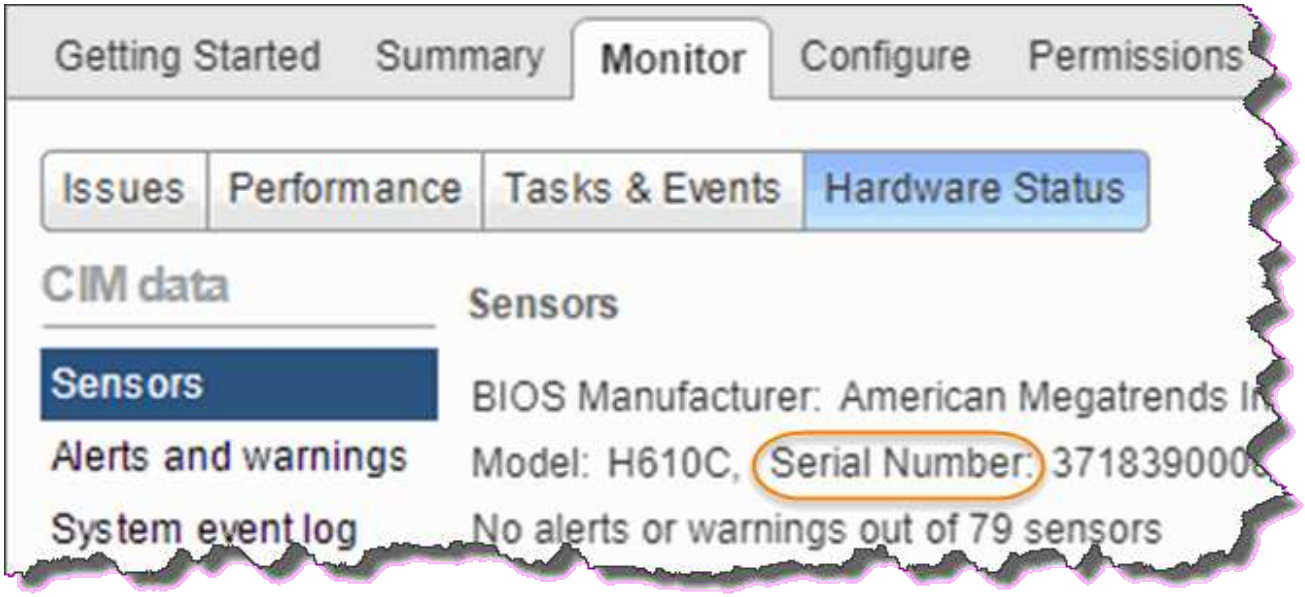
ノードを交換する前に、ノードでホストされている仮想マシン（ VM ）を使用可能なホストに移行し、クラスタからノードを削除しておく必要があります。シリアル番号やネットワーク情報など、ノードに関する詳細を記録しておく必要があります。VMの移行とノードの詳細の記録は、Dual Inline Memory Module（DIMM；デュアルインラインメモリモジュール）の障害など、ノードがオンラインで機能しているコンポーネント障害の場合にも適用されます。

手順

1. VMware vSphere Web Client で、次の手順を実行して VM を別の使用可能なホストに移行します。

   移行手順については、 VMware のドキュメントを参照してください。

2. 障害が発生したノードを選択し、 * Monitor > Hardware Status > Sensors * を選択します。
3. 障害が発生したノードのシリアル番号をメモします。次のスクリーンショットは一例です。



   シャーシを識別するには、ノード背面のラベルに記載されているシリアル番号と同じ番号を入力する必要があります。

4. 障害が発生したノードを右クリックし、 * Connection > Disconnect * を選択します。
5. 「 * はい * 」を選択して操作を確定します。
6. 障害が発生したノードを右クリックし、 * インベントリから削除 * を選択します。
7. 「 * はい * 」をクリックして操作を確定します。

手順2：ノードを交換する

クラスタから障害ノードを削除したら、障害が発生したシャーシを取り外し、交換用シャーシを設置できます。

ここで説明する手順を実行する前に、静電気防止処置を施してください。

手順

1. 新しいシャーシを開封し、平らな場所に置きます。障害が発生したシャーシをネットアップに返却するときは、梱包材を保管しておいてください。
2. 取り外すシャーシの背面に挿入されている各ケーブルにラベルを付けます。新しいシャーシを設置したら、ケーブルを元のポートに戻す必要があります。
3. シャーシの背面からすべてのケーブルを外します。
4. 取り付け耳の蝶ネジを外して、シャーシを取り外します。障害が発生したシャーシは、梱包してネットア

ップに返送する必要があります。

5. 交換用シャーシをレールにスライドさせます。

> シャーシをレールにスライドさせる際に力を入れすぎないように注意してください。

6. H615C のみ。障害が発生したシャーシから DIMM を取り外し、交換用シャーシにこれらの DIMM を挿入します。

> 障害が発生したノードの同じスロットから取り外した DIMM を交換する必要があります。

7. 障害が発生したシャーシの両側にある 2 台の電源装置を取り外し、交換用シャーシに挿入します。
8. 元々ケーブルを外したポートにケーブルを再接続します。ケーブルを外したときに追加したラベルは、ガイドとして役立ちます。

> シャーシ背面の通気口がケーブルやラベルで塞がれていると、過熱によってコンポーネントで早期に障害が発生する可能性があります。ケーブルをポートに無理に押し込まないでください。ケーブル、ポート、またはその両方が破損する可能性があります。

9. シャーシの電源をオンにします。

手順3：クラスタにノードを追加する

新しいコンピューティングノードを使用するように NetApp HCI を設定する必要があります。

必要なもの

- 分散仮想スイッチを使用している環境にノードを追加する場合は、 vSphere インスタンス NetApp HCI で使用している vSphere Enterprise Plus ライセンスがあることを確認しておきます。
- NetApp HCI で使用しているすべての vCenter インスタンスと vSphere インスタンスでライセンス期間が終了していないことを確認しておきます。
- 既存のノードと同じネットワークセグメントに未使用の空いている IPv4 アドレスが必要です（新しいノードは、同じタイプの既存のノードと同じネットワークにインストールする必要があります）。
- vCenter 管理者アカウントのクレデンシャルを準備しておきます。

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。例：

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

2. NetApp HCI ストレージクラスタ管理者のクレデンシャルを指定して NetApp Hybrid Cloud Control にログインします。
3. [インストールの展開] ペインで、 [* 展開 *] を選択します。

   ブラウザに NetApp Deployment Engine が表示されます。

4. ローカルのNetApp HCIストレージクラスタ管理者のクレデンシャルを指定してNetApp Deployment

Engineにログインします。

> Lightweight Directory Access Protocolのクレデンシャルを使用してログインすることはできません。

5. ようこそページで、 * はい * を選択します。
6. [End User License] ページで、次のアクションを実行します。
   a. VMware のエンドユーザライセンス契約を読みます。
   b. 契約条件に同意する場合は、契約テキストの最後にある「 * 同意します * 」を選択します。
7. Continue をクリックします。 .
8. vCenter のページで、次の手順を実行します。
   a. NetApp HCI 環境に関連付けられている vCenter インスタンスの FQDN または IP アドレスと管理者のクレデンシャルを入力します。
   b. 「 * Continue * 」を選択します。
   c. 新しいコンピューティングノードを追加する既存の vSphere データセンターを選択するか、 Create New Datacenter を選択して新しいコンピューティングノードを新しいデータセンターに追加します。

      > Create New Datacenter を選択すると、 Cluster フィールドに自動的に値が入力されます。

   d. 既存のデータセンターを選択した場合は、新しいコンピューティングノードを関連付ける vSphere クラスタを選択します。

      > 拡張対象として選択したクラスタのネットワーク設定を NetApp HCI が認識できない場合は、管理、ストレージ、 vMotion ネットワーク用の VMkernel と vmnic マッピングが導入時のデフォルトに設定されていることを確認します。

   e. 「 * Continue * 」を選択します。
9. ESXi のクレデンシャルページで、追加するコンピューティングノードの ESXi root パスワードを入力します。NetApp HCI の初期導入時に作成したパスワードを使用する必要があります。
10. 「 * Continue * 」を選択します。
11. 新しい vSphere データセンタークラスタを作成した場合は、ネットワークトポロジページで、追加する新しいコンピューティングノードと一致するネットワークトポロジを選択します。

    > ケーブル 2 本のオプションを選択できるのは、コンピューティングノードがケーブル 2 本のトポロジを使用しており、既存の NetApp HCI 環境に VLAN ID が設定されている場合のみです。

12. Available Inventory ページで、既存の NetApp HCI インストールに追加するノードを選択します。

一部のコンピューティングノードは、使用している vCenter のバージョンでサポートされる最高レベルで EVC を有効にしないと、インストール環境に追加できません。そのようなコンピューティングノードについては、 vSphere クライアントを使用して EVC を有効にしてください。有効にしたら、インベントリページをリフレッシュし、コンピューティングノードの追加をもう一度実行してください。

13. 「 * Continue * 」を選択します。
14. オプション：新しい vSphere データセンタークラスタを作成した場合は、ネットワーク設定ページで既存の NetApp HCI 環境からネットワーク情報をインポートします。既存のクラスタから設定をコピー * チェックボックスを選択します。これにより、各ネットワークにデフォルトゲートウェイとサブネットの情報が設定されます。
15. [ネットワークの設定] ページで、初期展開から一部のネットワーク情報が検出されました。シリアル番号順に表示された新しいコンピューティングノードのそれぞれについて、新しいネットワーク情報を割り当てる必要があります。新しいコンピューティングノードごとに、次の手順を実行します。
    a. NetApp HCI が命名プレフィックスを検出した場合は、 [検出された命名プレフィックス] フィールドからコピーし、 [ホスト名] フィールドに追加した新しい一意のホスト名のプレフィックスとして挿入します。
    b. Management IP Address フィールドに、管理ネットワークサブネットにあるコンピューティングノードの管理 IP アドレスを入力します。
    c. vMotion IP Address フィールドに、 vMotion ネットワークサブネットにあるコンピューティングノードの vMotion IP アドレスを入力します。
    d. iSCSI A-IP Address フィールドに、 iSCSI ネットワークサブネットにあるコンピューティングノードの最初の iSCSI ポートの IP アドレスを入力します。
    e. iSCSI B-IP Address フィールドに、 iSCSI ネットワークサブネット内にあるコンピューティングノードの 2 番目の iSCSI ポートの IP アドレスを入力します。
16. 「 * Continue * 」を選択します。
17. [ネットワーク設定] セクションの [確認] ページでは、新しいノードが太字で表示されます。いずれかのセクションの情報を変更する必要がある場合は、次の手順を実行します。
    a. そのセクションの * 編集 * を選択します。
    b. 変更が完了したら、以降のページで「 * 続行」を選択して「レビュー」ページに戻ります。
18. オプション：ネットアップがホストしている SolidFire Active IQ サーバにクラスタの統計情報とサポート情報を送信しないようにする場合は、最後のチェックボックスをオフにします。これにより、 NetApp HCI のリアルタイムの健常性診断の監視機能が無効になります。この機能を無効にすると、ネットアップによる NetApp HCI のプロアクティブなサポートと監視が行われなくなるため、本番環境が影響を受ける前に問題を検出して解決できなくなります。
19. [* ノードの追加 *] を選択します。リソースの追加と設定の進捗状況は、 NetApp HCI で監視できます。
20. オプション：新しいコンピューティングノードがすべて vCenter に表示されることを確認します。

手順4：GPUドライバをインストールする

H610C ノードなどの NVIDIA グラフィックス処理ユニット（ GPU ）を搭載したコンピューティングノードでは、 NVIDIA ソフトウェアドライバを VMware ESXi にインストールして、強化された処理能力を活用できるようにする必要があります。GPU ドライバをインストールするには、コンピューティングノードに GPU カードが必要です。

手順

1. ブラウザを開き、次の URL から NVIDIA ライセンスポータルにアクセスします。 https://nvid.nvidia.com/dashboard/`
2. お使いの環境に応じて、ドライバーパッケージのバージョンをコンピューターにダウンロードします。

   次の例は、vSphere 6.0、6.5、および6.7のドライバパッケージのバージョンを示しています。

vSphere のバージョン	ドライバパッケージ
vSphere 6.0	NVIDIA-GRID-vSphere-6.0-390.94-390.96-392.05.zip
vSphere 6.5 の場合	NVIDIA-GRID-vSphere-6.5-410.92-410.91-412.16.zip
vSphere 6.7	NVIDIA-GRID-vSphere-6.7-410.92-410.91-412.16.zip

3. ドライバパッケージをコンピュータに展開します。圧縮されていないドライバファイル .VIB ファイルが展開されます。
4. コンピュータからコンピューティングノード上で実行されている ESXi に .VIB ドライバファイルをコピーします。Secure Copy Protocol（SCP）ユーティリティは、ほとんどのLinuxディストリビューションで簡単に使用できます。また、すべてのバージョンのWindowsでダウンロード可能なユーティリティとして使用できます。

   次の例は、ESXi 6.0、6.5、および6.7に対するコマンドを示しています。このコマンドは、ドライバが管理ホストの$HOME/nvidia/ESX6.x/ディレクトリにあることを前提としています。

オプション	説明
ESXi 6.0	SCP $HOME/NVIDIA/ESX6.0/nvidia **.vibb root@<ESX_IP_addr> ： / 。
ESXi 6.5 の場合	SCP $HOME/nvidia / ESX6.5/nvidia **.vib root@<ESX_IP_addr> ： / 。
ESXi 6.7	SCP $HOME/nvidia / ESX6.5/nvidia **.vibb root@<ESX_IP_addr> ： / 。

5. 次の手順に従って、 root として ESXi ホストにログインし、 NVIDIA vGPU Manager を ESXi にインストールします。
   a. 次のコマンドを実行して、 root ユーザとして ESXi ホストにログインします。「 root @<ESXi_IP_address >` 」
   b. 次のコマンドを実行して、 NVIDIA GPU ドライバが現在インストールされていないことを確認します。「 nvidia-smi 」このコマンドは「 nvidia-smi ： not found 」というメッセージを返します。
   c. 次のコマンドを実行して、ホストのメンテナンスモードを有効にし、 VIB ファイルから NVIDIA vGPU Manager をインストールします。 esxcli system maintenanceMode set -enable true `esxcli`

`software vib install -v/nvidia **.vib` You should see the message 'Operation finishedly' 。

d. 次のコマンドを実行して、 8 つの GPU ドライバがすべてコマンド出力「 nvidia-smi 」に表示されていることを確認します

e. 次のコマンドを実行して、 NVIDIA vGPU パッケージが正しくインストールされ、ロードされたことを確認します。 vmkload_mod -l | grep nvidia 」コマンドは、「 nvidia 816 13808 」のような出力を返します

f. 次のコマンドを実行して、メンテナンスモードを終了し、ホストを再起動します。 esxcli system maintenanceMode set – enable false```re boot-f`

6. 新たに導入した NVIDIA GPU 搭載の残りのコンピューティングノードについて、手順 4~6 を繰り返します。

7. NVIDIA のドキュメントサイトに記載された手順に従って、次のタスクを実行します。

   a. NVIDIA ライセンスサーバをインストールします。

   b. NVIDIA vGPU ソフトウェア用に仮想マシンゲストを設定します。

   c. 仮想デスクトップインフラ（ VDI ）環境で vGPU 対応のデスクトップを使用している場合は、NVIDIA vGPU ソフトウェア用に VMware Horizon View を設定します。

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"
- "SolidFire と Element ソフトウェアドキュメントセンター"

H610S ノードを交換してください

ファン、 CPU 、または Dual Inline Memory Module （ DIMM ）に障害が発生した場合や、過熱やブートプロセスの問題を解決する場合には、シャーシの交換が必要になることがあります。シャーシ前面の黄色の LED の点滅は、シャーシの交換が必要な可能性があることを示しています。続行する前にネットアップサポートにお問い合わせください。

> を参照してください "こちらの技術情報アーティクル" H610S ノードの設置要件の詳細については、を参照してください。新規およびスペアの H610S ストレージノードには、既存の Element ソフトウェアバージョンのストレージクラスタに基づいて追加のインストール要件がある場合があります。詳細については、ネットアップサポートにお問い合わせください。

> H610S は、 1 ラックユニット（ 1U ）シャーシで、「ノード」と「シャーシ」は同じ意味で使用されます。

ドライブの追加と取り外しを行う際のベストプラクティス

クラスタにドライブを追加する際は、次のベストプラクティスに従う必要があります。

- スライスドライブを追加する前に、ブロックドライブをすべて追加し、ブロックの同期が完了していることを確認します。

- Element ソフトウェア 10.x 以降の場合は、すべてのブロックドライブを一度に追加します。一度に 3 つ以上のノードでこの処理を行わないようにしてください。
- Element ソフトウェア 9.x 以前では、 3 本のドライブを一度に追加して完全に同期したあとに、次の 3 つのグループを追加してください。
- スライスドライブを取り外し、ブロックドライブを取り外す前にスライスの同期が完了したことを確認します。
- 一度に 1 つのノードからすべてのブロックドライブを削除します。ブロックの同期がすべて完了してから次のノードに進んでください。

必要なもの

- ネットアップサポートに問い合わせます。交換用製品を注文する場合は、ネットアップサポートでケースをオープンする必要があります。
- 交換用ノードを入手します。
- 静電放電（ ESD ）リストバンドを装着するか、静電気防止処置を行っておきます。
- Return to Factory Image （ RTFI ）プロセスを実行する必要がある場合は、 USB キーを取得します。ネットアップサポートは、 RTFI プロセスを実行する必要があるかどうかの判断に役立ちます。
- キーボードとモニタを用意します。
- 障害ノードをクラスタから正しく削除しておきます。
- DIMM で障害が発生した場合は、クラスタからノードを取り外す前にドライブを取り外しておきます。

このタスクについて

VMware vSphere Web Client のアラームでは、ホストで障害が発生するとアラートが通知されます。VMware vSphere Web Client で障害が発生したホストのシリアル番号を、ノード背面のステッカーに記載されているシリアル番号と一致させる必要があります。

手順

1. 障害が発生したシャーシの前面でサービスタグを確認します。

2. 交換用シャーシを発注したときに、サービスタグのシリアル番号がネットアップサポートケース番号と一致していることを確認します。
3. キーボードとモニタを障害が発生したシャーシの背面に接続します。
4. ネットアップサポートで障害ノードのシリアル番号を確認します。
5. シャーシの電源を切ります。
6. 前面のドライブと背面のケーブルに位置を示すラベルを付け、交換後も同じ場所に戻すことができます。

   シャーシ内のドライブの配置については、次の図を参照してください。

7. ケーブルを取り外します。
8. 取り付け耳の蝶ネジを外して、シャーシを取り外します。障害が発生したシャーシは、梱包してネットアップに返送してください。
9. 交換用シャーシを設置
10. ドライブを障害が発生したシャーシから慎重に取り外し、交換用シャーシに挿入します。

    ドライブを取り外す前に、ドライブが取り付けられていたスロットにドライブを挿入する必要があります。

11. 障害が発生したシャーシから電源装置を取り外し、交換用シャーシに挿入します。
12. 電源装置ケーブルとネットワークケーブルを元のポートに差し込みます。
13. 交換用ノードの 10GbE ポートに、 Small Form-Factor Pluggable （ SFP ）トランシーバが差し込まれている場合があります。10GbE ポートにケーブルを接続する前に、これらを取り外す必要があります。

    スイッチがケーブルを認識しない場合は、スイッチベンダーのマニュアルを参照してください。

14. 前面の電源ボタンを押して、シャーシの電源をオンにします。ノードがブートするまでに約 5 分 30 秒かかります。
15. 設定手順を実行します。
    - H610S ノードが NetApp HCI 環境に含まれている場合は、 NetApp Hybrid Cloud Control を使用してストレージリソースを設定してください。を参照してください "NetApp HCI ストレージリソースを展開します"。
    - H610S ノードが SolidFire オールフラッシュストレージ環境に含まれている場合は、 NetApp Element のソフトウェアユーザインターフェイス（ UI ）を使用してノードを設定します。ネットアップサポートにお問い合わせください。

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"
- "SolidFire と Element ソフトウェアドキュメントセンター"

電源装置を交換してください

各シャーシには、電源を冗長化するために 2 つの電源装置が搭載されてい電源装置に障害が発生した場合は、シャーシの電源の冗長性を維持するために、できるだけ早く交換する必要があります。

必要なもの

- 電源装置に障害があることを確認しておきます。
- 交換用電源装置を用意します。
- 2 台目の電源装置が動作していることを確認します。
- 静電放電（ ESD ）リストバンドを装着するか、静電気防止処置を施しておきます。

このタスクについて

交換手順は次のノードモデルに該当します。

- 2 ラックユニット（ 2U ）、 4 ノード NetApp HCI シャーシ
- 2U H610C コンピューティングシャーシ
- 1 ラックユニット（ 1U ） H615C コンピューティングシャーシ
- 1U H610S ストレージシャーシ

> H610C 、 H615C 、および H610S では、 2U 、 4 ノードのシャーシとは異なり、ノードとシャーシが別々のコンポーネントではないため、「ノード」と「シャーシ」は同じ意味で使用されます。

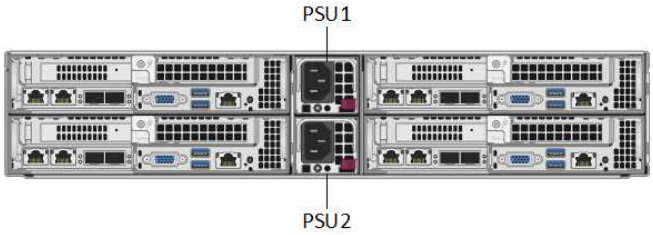
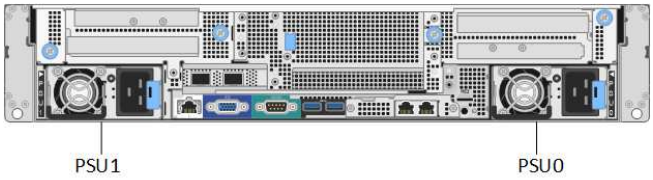
VMware vSphere Web Client のアラームには、障害が発生した電源装置に関する情報が PS1 または PS2 と記載されています。NetApp HCI 2U の 4 ノードシャーシでは、 PS1 はシャーシの一番上の列のユニット、 PS2 はシャーシの一番下の列のユニットです。冗長電源装置が機能していれば、シャーシの電源をオンにして稼働したまま、障害のある電源装置を交換できます。

手順

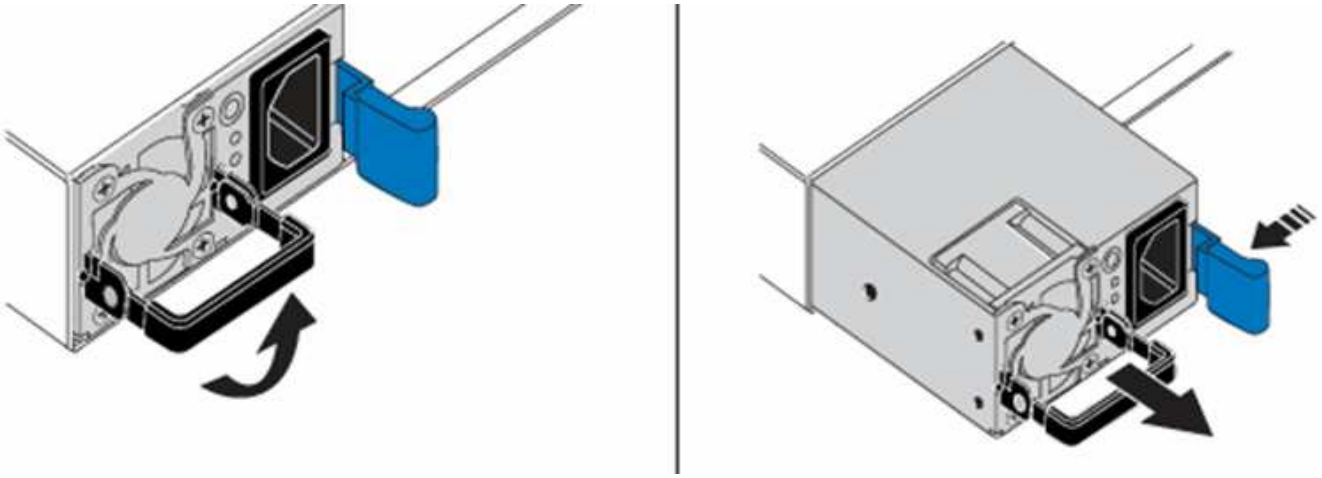
1. シャーシ内で障害のある電源装置の位置を確認します。障害のあるユニットの LED がオレンジに点灯します。

   > 電源装置の位置は、シャーシのタイプによって異なります。

   電源装置の位置については、次の図を参照してください。

モデル	電源装置の場所
2U / 4 ノード NetApp HCI ストレージシャーシ	 シャーシ内のノードの外観は、ノードのタイプ（ストレージまたはコンピューティング）によって異なる場合があります。
H610C シャーシ	
H615C シャーシ	
H610S シャーシ	

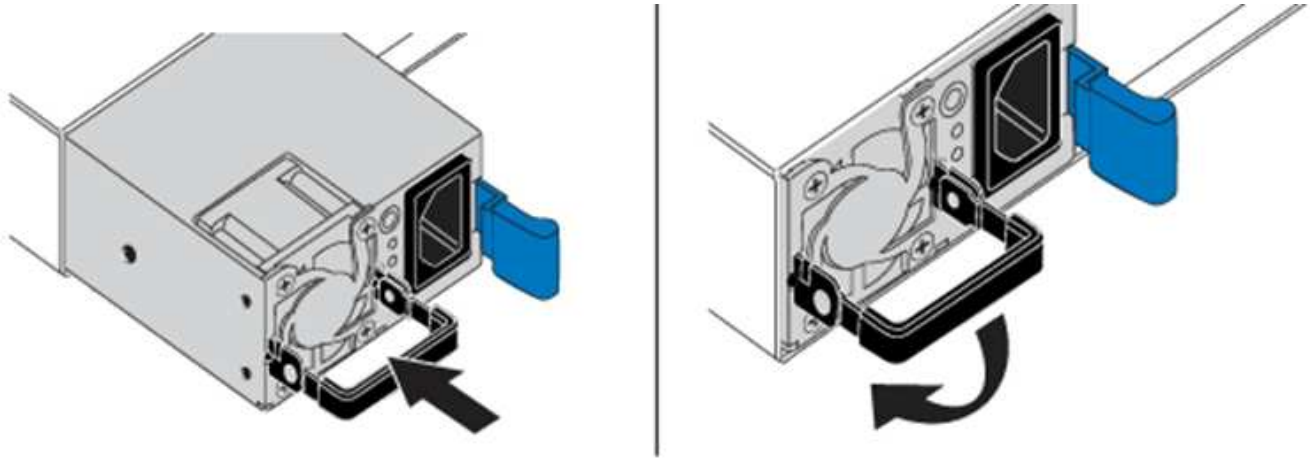
2. 電源装置から電源コードを抜きます。
3. カムハンドルを持ち上げ、青色のラッチを押して電源装置ユニットを引き出します。



図は一例です。シャーシ内の電源装置の位置とリリースボタンの色は、シャーシのタイプによって異なります。

両手で電源装置の重量を支えてください。

4. 両手で電源装置の端をシャーシの開口部に合わせ、カムハンドルを使用して装置をシャーシにそっと押し込んで、カムハンドルを直立位置に戻します。



5. 電源コードを接続します。
6. 出荷時の箱に同梱されている手順に従って、障害が発生したユニットをネットアップに返送してください。

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"
- "SolidFire と Element ソフトウェアドキュメントセンター"

SN2010 、 SN2100 、および SN2700 の各スイッチを交換してください

ネットアップが提供するベストプラクティスと手順に従って、障害のある SN2000 シリーズスイッチを無停止で交換できます。

必要なもの

- Putty がラップトップにインストールされていること、および出力をキャプチャしたことを確認します。このビデオでは、 Putty を設定して出力セッションをキャプチャする方法を紹介しています。

[] | *https://img.youtube.com/vi/2LZfWH8HffA/maxresdefault.jpg*

- 交換の前後に NetApp Config Advisor を実行していることを確認してください。これは、メンテナンスの開始前に他の問題を特定するのに役立ちます。Config Advisor をダウンロードしてインストールし、からクイックスタートガイドにアクセスします "こちら（ログインが必要です）"。
- 電源ケーブル、基本的な手工具、およびラベルを用意します。
- 2 時間から 4 時間のメンテナンス期間を計画していることを確認します。
- 以下のスイッチポートを確認してください。

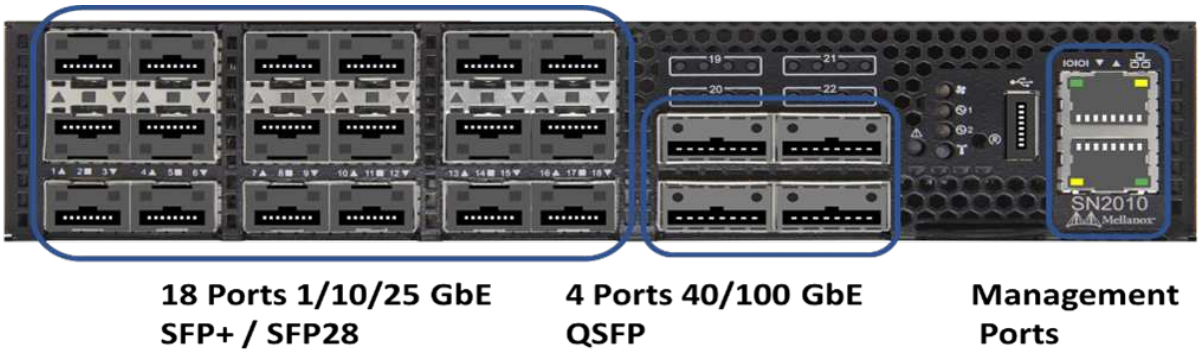


図 **1. SN2010** スイッチの前面プレートとポート

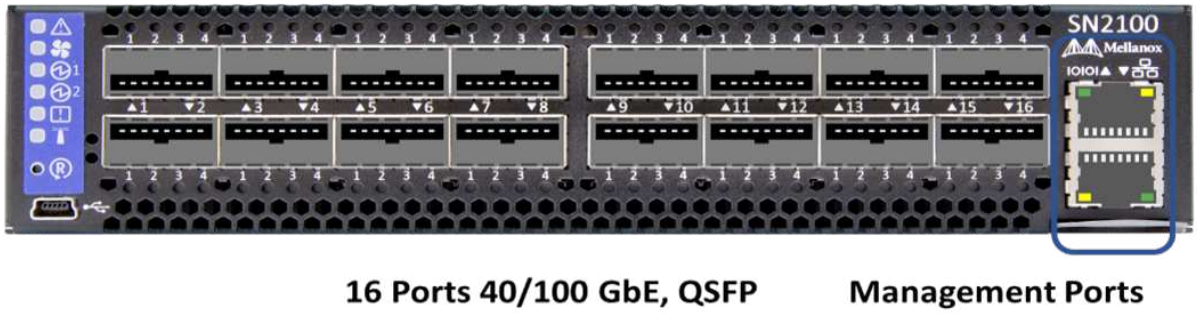


図 **2. SN2100** スイッチの前面プレートとポート

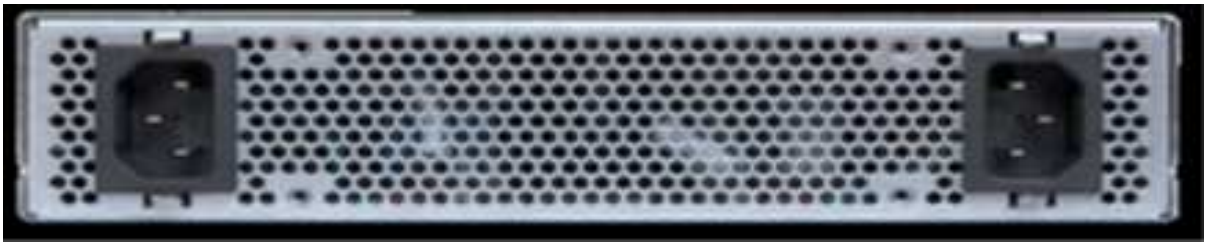


図 **3. SN2010** および **SN2100** スイッチの背面

図 **4. SN2700** スイッチの前面と背面

このタスクについて

この手順の手順は、次の順序で実行する必要があります。これにより、スイッチの交換前にダウンタイムを最小限に抑え、交換用スイッチを事前に設定することができます。

ガイダンスが必要な場合は、ネットアップサポートにお問い合わせください。

手順の概要を次に示します。[故障したスイッチを交換する準備をします]
[構成ファイルを作成します]
[障害のあるスイッチを取り外し、交換用スイッチを取り付けます]
[スイッチのオペレーティングシステムのバージョンを確認します]
[交換用スイッチを設定します]
[交換を完了します]

故障したスイッチを交換する準備をします

障害のあるスイッチを交換する前に、次の手順を実行します。

手順

1. 交換用スイッチのモデルが障害のあるスイッチと同じであることを確認します。
2. 障害のあるスイッチに接続されているすべてのケーブルにラベルを付けます。
3. スイッチ構成ファイルが保存されている外部ファイルサーバを特定します。
4. 次の情報を入手しておきます。
   a. 初期設定に使用されるインターフェイス： RJ-45 ポートまたはシリアルターミナルインターフェイス。
   b. スイッチアクセスに必要なクレデンシャル。障害が発生していないスイッチの管理ポートの IP アドレスと、障害が発生したスイッチです。
   c. 管理アクセス用のパスワード。

構成ファイルを作成します

スイッチは、作成した構成ファイルを使用して設定できます。次のいずれかのオプションを選択して、スイッチの構成ファイルを作成します。

オプション	手順

障害が発生したスイッチからバックアップ構成ファイルを作成します	1. 次の例に示すように、 SSH を使用してスイッチにリモート接続します。
	`ssh admin@<switch_IP_address`
	2. 次の例に示すように、コンフィギュレーションモードを開始します。
	`switch > enable`
	`switch # configure terminal`
	3. 使用可能な構成ファイルを次の例のように検索します。
	`switch (config) #`
	`switch (config) # show configuration files`
	4. アクティブなビン構成ファイルを外部サーバーに保存します。
	`switch (config) # configuration upload my-filename scp://myusername@my-server/path/to/my/<file>`

オプション	手順

ファイルを変更して、バックアップ構成ファイルを作成します 別のスイッチ	1. 次の例に示すように、 SSH を使用してスイッチにリモート接続します。
	`ssh admin@<switch_IP_address`
	2. 次の例に示すように、コンフィギュレーションモードを開始します。
	`switch > enable`
	`switch # configure terminal`
	3. 次の例に示すように、テキストベースの構成ファイルをスイッチから外部サーバにアップロードします。
	`switch (config) #`
	`switch (config) # configuration text file my-filename upload scp://root@my-server/root/tmp/my-filename`
	4. 障害が発生したスイッチに合わせて、テキストファイル内の次のフィールドを変更します。
	`## Network interface configuration`
	`##`
	`no interface mgmt0 dhcp`
	`interface mgmt0 ip address XX.XXX.XX.XXX /22`
	`##`
	`## Other IP configuration`
	`##`
	`hostname oldhostname`

障害のあるスイッチを取り外し、交換用スイッチを取り付けます

手順を実行して障害のあるスイッチを取り外し、交換用スイッチを取り付けます。

手順

1. 障害が発生したスイッチの電源ケーブルを確認します。
2. スイッチの再起動後に、電源ケーブルにラベルを付けて取り外します。
3. すべてのケーブルにラベルを付けてスイッチから取り外し、スイッチ交換時の破損を防ぐために固定します。
4. ラックからスイッチを取り外します。
5. 交換用スイッチをラックに取り付けます。
6. 電源ケーブルと管理ポートケーブルを接続します。

> AC 電源を投入すると、スイッチの電源が自動的にオンになります。電源ボタンがありません。システムステータス LED が緑色になるまで、最大 5 分かかることがあります。

7. RJ-45 管理ポートまたはシリアルターミナルインターフェイスを使用してスイッチに接続します。

スイッチのオペレーティングシステムのバージョンを確認します

スイッチの OS ソフトウェアバージョンを確認します。障害が発生したスイッチと正常なスイッチのバージョンが一致している必要があります。

手順

1. SSH を使用して、スイッチにリモート接続します。
2. コンフィギュレーションモードを開始します。
3. 「 show version 」コマンドを実行します。次の例を参照してください。

```
SFPS-HCI-SW02-A (config) #show version
Product name:      Onyx
Product release:   3.7.1134
Build ID:          #1-dev
Build date:        2019-01-24 13:38:57
Target arch:       x86_64
Target hw:         x86_64
Built by:          jenkins@e4f385ab3f49
Version summary:   X86_64 3.7.1134 2019-01-24 13:38:57 x86_64

Product model:     x86onie
Host ID:           506B4B3238F8
System serial num: MT1812X24570
System UUID:       27fe4e7a-3277-11e8-8000-506b4b891c00

Uptime:            307d 3h 6m 33.344s
CPU load averages: 2.40 / 2.27 / 2.21
Number of CPUs:    4
System memory:     3525 MB used / 3840 MB free / 7365 MB total
Swap:              0 MB used / 0 MB free / 0 MB total
```

4. バージョンが一致しない場合は、 OS をアップグレードする必要があります。を参照してください "Mellanox ソフトウェアアップグレードガイド" を参照してください。

交換用スイッチを設定します

次の手順を実行して、交換用スイッチを設定します。を参照してください "Mellanox の構成管理" を参照してください。

手順

1. 該当するオプションから選択します。

オプション	手順

bin 構成ファイルから	1. 次の例に示すように、 bin 構成ファイルを取得します。
	
	`switch (config) # configuration fetch scp://myusername@my-server/path/to/my/<file>`
	
	2. 次の例に示すように、前の手順で取得した bin 構成ファイルをロードします。
	
	`switch (config) # configuration switch-to my-filename`
	
	3. 再起動を確認するには 'yes' と入力します

テキストファイルから	1. スイッチを工場出荷時のデフォルトにリセットします。
	
	`switch (config) # reset factory keep-basic`
	
	2. テキストベースの構成ファイルを適用します。
	
	`switch (config) # configuration text file my-filename apply`
	
	3. 次の例に示すように、テキストベースの構成ファイルをスイッチから外部サーバにアップロードします。
	
	`switch (config) #`
	`switch (config) # configuration text file my-filename upload scp://root@my-server/root/tmp/my-filename`
	
	テキストファイルの適用時にはリブートは必要ありません。

交換を完了します

手順を実行して交換手順を完了します。

手順

1. ケーブルを挿入するときは、ラベルを参考にしてください。
2. NetApp Config Advisor を実行します。からクイックスタートガイドにアクセスします "こちら（ログインが必要です）"。
3. ストレージ環境を確認します。
4. 障害が発生したスイッチをネットアップに返却します。

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"
- "SolidFire と Element ソフトウェアドキュメントセンター"

2 ノードクラスタのストレージノードを交換

2 ノードクラスタの一部であるストレージノードを交換する前に、最初に 3 つ目のストレージノード（新しい IP アドレスのセットが必要）を追加し、同期を完了させてから、障害ノードを削除してください。交換用ノードがクラスタに追加されるまで、クラスタはデグレード状態のままです。

必要なもの

- 新しい管理 IP アドレスとストレージ IP アドレスを用意します。
- ノードがオフラインになった後 ' クラスタに ClusterCannotSync' アラートが表示されていることを確認しておきますこれにより、新しいノードがクラスタに再度追加されたときに、クラスタの完全な再同期が実行されます。このアラートは、ストレージノードがオフラインになってから約 6 分後に表示されます。
- ネットアップサポートに問い合わせます。交換用製品を注文する場合は、ネットアップサポートでケースをオープンする必要があります。
- 交換用ノードを入手します。
- 静電放電（ ESD ）リストバンドを装着するか、静電気防止処置を行っておきます。

このタスクについて

VMware vSphere Web Client のアラームでは、ホストで障害が発生するとアラートが通知されます。VMware vSphere Web Client で障害が発生したホストのシリアル番号を、ノード背面のステッカーに記載されているシリアル番号と一致させる必要があります。

手順

1. 障害が発生したノードをラックから物理的に取り外します。実行する手順は、使用するストレージノードのタイプによって異なります。を参照してください "H410S ノードを交換します" および "H610S ノードを交換してください"。

> ⓘ この時点では、クラスタからノードを削除しないでください。

2. 交換用ノードを同じスロットに設置します。
3. ノードをケーブル接続
4. ノードの電源をオンにします。
5. キーボードとモニタをノードに接続
6. 設定手順を実行します。
   a. IPMI / BMC IP アドレスを設定します。
   b. 新しい管理 IP アドレスとストレージ IP アドレス、およびクラスタ名を使用して新しいノードを設定します。
7. ノードをクラスタに追加したら、ドライブを追加します。
8. 同期が完了したら、障害が発生したドライブとノードをクラスタから削除します。
9. NetApp Hybrid Cloud Control を使用して、追加した新しいストレージノードを設定します。を参照してください "NetApp HCI ストレージリソースを展開します"。

詳細については、こちらをご覧ください

- "NetApp HCI ドキュメントセンター"
- "SolidFire と Element ソフトウェアドキュメントセンター"

以前のバージョンの NetApp HCI ドキュメント

最新バージョンを実行していない場合は、以前のリリースの NetApp HCI に関するドキュメントを参照できます。

- "NetApp HCI 1.8P1"
- "NetApp HCI 1.8 以前"

法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

- "コンピューティングのアップグレードに向けた Ansible のロールに関する注意事項があります"
- "Ember OS 12.3.1 の注意"
- "Ember OS 12.3 の注意"
- "管理ノード 12.3.1 の通知です"
- "管理ノード 12.3 についての注意"
- "NetApp HCI 1.9P1 に関する通知です"
- "NetApp HCI 1.9 の注意事項"
- "ストレージファームウェアバンドル 2.146 に関する注意事項"
- "Compute Firmware Bundle 2.146 の注意"
- "ストレージファームウェアバンドル 2.99.2 に関する注意事項"
- "Compute Firmware Bundle 2.76 に関する注意"
- "ストレージファームウェアバンドル 2.76 に関する注意"

- "Compute Firmware Bundle 2.27 に関する注意"
- "ストレージファームウェアバンドル 2.27 に関する注意"
- "コンピューティングファームウェアの ISO についての通知"
- "H610S BMC に関する注意事項が表示されます"
- "管理サービス2.24.40（NetApp Element Plug-in for VMware vCenter Server 5.2.12）に関するお知らせ"
- "管理サービス2.23.64（NetApp Element Plug-in for VMware vCenter Server 5.1.12）に関する注意事項"
- "管理サービス2.22.7（vCenter Server 5.337用NetApp Element プラグイン）に関する注意事項"
- "管理サービス2.2.1.61（vCenter Server 4.10.12のNetApp Element プラグイン）に関する注意事項"
- "管理サービス2.20.69（vCenter Server 4.9.14用NetApp Element プラグイン）に関する注意事項"
- "管理サービス2.19.48の通知（vCenter Server 4.8.34用NetApp Element プラグイン）"
- "管理サービス2.18.91（NetApp Element Plug-in for vCenter Server 4.7.10）に関する注意事項"
- "管理サービス2.17.56（vCenter Server 4.6.32用NetApp Element プラグイン）に関する注意事項"
- "管理サービス2.17.52の注意事項（vCenter Server 4.6.29用NetApp Element プラグイン）"
- "管理サービス2.16の注意事項（vCenter Server 4.6.29用NetApp Element プラグイン）"
- "管理サービス2.14（NetApp Element Plug-in for vCenter Server 4.5.42）に関する注意事項"
- "管理サービス2.13に関する注意事項（vCenter Server 4.5.42用NetApp Element プラグイン）"
- "管理サービス2.11（vCenter Server 4.4.72用NetApp Element プラグイン）に関する注意事項"
- "NetApp HCI 1.8 の注意事項"