



ネットアップの要素 **12.0**

『 **Management Node User Guide for
NetApp Element Software** 』を参照し
てください

2020年4月 | 215-14896_2020-04_ja-jp
ng-gpso-jp-documents@netapp.com

目次

本書の内容	4
Elementソフトウェアの管理ノード	5
SolidFireオールフラッシュストレージの管理サービス.....	5
永続ボリューム.....	5
ネットワークポート要件	6
管理ノードのインストール	10
ストレージ NIC の設定.....	15
管理ノードのアップグレード	16
管理ノードのリカバリ	17
管理ノードの使用	20
管理ノードへのアクセス.....	20
管理ノードのノードUIへのアクセス.....	20
管理ノードのREST API UIへのアクセス.....	21
REST APIを使用するための承認の取得.....	22
NetApp HCIのアラート監視.....	23
管理ノードのネットワーク設定.....	24
管理ノードのクラスタ設定.....	25
管理ノード設定のテスト.....	25
管理ノードからのシステムユーティリティの実行.....	26
ネットワークサポートによるリモート接続の有効化.....	27
SolidFireオールフラッシュストレージに対するActive IQコレクタ サービスの有効化.....	28
管理ノードへのアセットの追加.....	29
ストレージクラスタ管理者パスワードの変更.....	30
プロキシサーバの設定.....	31
管理サービスからのログの取得.....	32
製品マニュアルとその他の情報の参照先	34
ネットアップサポートへの問い合わせ	35
著作権に関する情報	36

商標に関する情報.....37

マニュアルの更新について.....38

本書の内容

このガイドでは、NetApp Elementソフトウェアベースのシステムの管理ノードについて説明します。このガイドを使用すると、管理ノードの機能をより詳しく理解し、手動によるインストールとアップグレードを実行できます。

Elementソフトウェアの管理ノード

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。このノードは、監視とテレメトリなどのシステム サービスのアップグレードと提供、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、ネットアップ サポートへのアクセス許可（トラブルシューティング）に使用します。

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。Active IQコレクタ、vCenter Plug-inのQoSSIOC、mNodeサービスなどのマイクロサービス（管理サービス）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 ソフトウェアのアップグレード用のHealthToolsやサポート ツール（リモートサポート トンネリング）などのサービスも管理ノードから利用できます。

SolidFireオールフラッシュ ストレージの管理サービス

管理サービスは、SolidFireオールフラッシュ ストレージに幅広い管理機能を一元的に提供します。管理サービスには、Active IQシステム テレメトリ、ログ、サービスの更新、およびElement Plug-in for vCenterのQoSSIOCサービスが含まれます。

関連情報

[Updating management services](#)

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すが、推奨される管理ノード設定です。

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、「NetApp-HCI-」で始まる名前の複数のボリュームが、割り当てられているクラスタに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同様、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。



注意：管理サービスに関連付けられた永続ボリュームは、インストール時またはアップグレード時に作成され、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、ボリュームまたは関連するアカウントを変更または削除しないでください。

ネットワークポート要件

システムをリモートから管理し、クライアントがデータセンターの外部からリソースに接続でき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TCP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、一部のポートは不要な場合もあります。

特に記載がないかぎり、ポートはすべてTCPで、ネットアップ 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双向通信を許可する必要があります。

ヒント: 管理ノード、Elementソフトウェアを実行するノード、およびクラスタのMVIP の間でICMPを有効にします。

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）
- SIP : ストレージIPアドレス（ノードごとのアドレス）
- 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	デスティネーション	ポート	説明
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	sfsupport.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	ストレージ ノードのMIP	442	ストレージノードおよびElementソフトウェアのアップグレードへの UI / APIアクセス
管理ノード	オンラインのソフトウェアリポジトリ： <ul style="list-style-type: none">• https://repo.netapp.com/bintray/api/package• https://netapp-downloads.bintray.com	443	管理ノード サービスのアップグレード
管理ノード	monitoring.solidfire.com	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ソフトウェアのアップグレードへの UI / APIアクセス

ソース	デスティネーション	ポート	説明
管理ノード	connect.pub.nks.cloud	443	NKSクラウド プロバイダとホスト型NKSサービスの間のセキュアな通信。たとえば、オンプレミスのNetApp HCIまたはVMwareにNKSが導入されている場合、トラフィックはこのNorthbound MTLSセキュアチャネルを使用します。
管理ノード	api.nks.netapp.io	443	オンプレミスの「リージョン」導入時の初期登録
管理ノード	repo.netapp.com	443	オンプレミス環境のインストール/更新に必要なコンポーネントへのアクセス
34.208.181.140 34.217.162.31 54.187.65.159 18.236.231.155	管理ノード	443	HTTPS (Kubernetesクラスタセキュリティ)
		6443	Kubernetes API (Kubernetesクラスタセキュリティ)
		12443	ダッシュボードへのプロキシ (Kubernetesクラスタセキュリティ)
		22	Kubernetesのアップグレードおよび他のタスク (Kubernetesクラスタセキュリティ)
管理ノード	amazonaws.com	443	ディスパッチトンネル
SNMPサーバ	ストレージ クラスタのMVIP	161 UDP	SNMPポーリング
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MIP	DNSサーバ	53 TCP / UDP	DNSレックアップ
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	(オプション) SNMPトラップ
ストレージ ノードのMIP	SNMPサーバ	162 UDP	(オプション) SNMPトラップ
ストレージ ノードのMIP	LDAPサーバ	389 TCP / UDP	(オプション) LDAP検索
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

ソース	デスティネーション	ポート	説明
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	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	LDAPSサーバ	636 TCP / UDP	LDAPSバックアップ
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
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
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
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	ストレージノードへのHTTPS UIおよびAPIアクセス
			(NetApp HCIのみ) NetApp Deployment Engineでの設定および導入監視
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

ソース	デスティネーション	ポート	説明
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
vCenter Server	ストレージ クラスタの MVIP	443	vCenter Plug-inのAPIアクセス
vCenter Server	管理ノード	8443	(オプション) vCenter Plug-inの QoSIOCサービス。
vCenter Server	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	管理ノード	9443	vCenter Plug-inの登録。登録完了後はポートを閉じてもかまいません。

管理ノードのインストール

NetApp Elementソフトウェアを実行しているクラスタの管理ノードは、構成に応じたイメージを使用して手動でインストールできます。この手動プロセスは、管理ノードのインストールにNetApp Deployment Engineを使用していないSolidFireオールフラッシュストレージ管理者およびNetApp HCI管理者を対象としています。

開始する前に

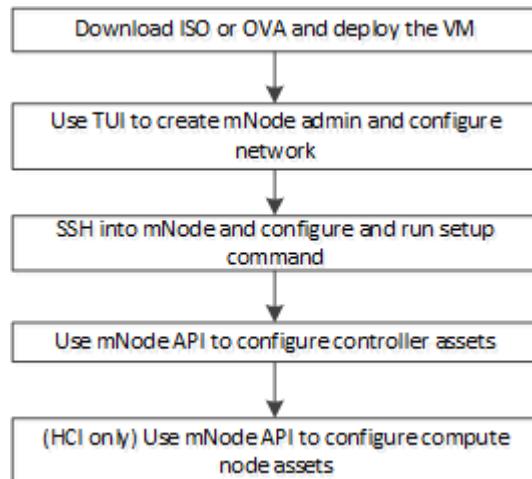
- クラスタでNetApp Elementソフトウェア11.3以降を実行している必要があります。
- インストール環境でIPv4を使用している必要があります。管理ノード11.3ではIPv6がサポートされません。
注: IPv6のサポートが必要な場合は、管理ノード11.1を使用してください。
- ネットアップサポートサイトからソフトウェアをダウンロードする権限が必要です。
- 使用するプラットフォームに適した管理ノードイメージの種類を特定しておきます。
次の表を参考にしてください。

プラットフォーム	インストールイメージの種類
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

タスク概要

この手順を実行する前に、永続ボリュームについて理解し、永続ボリュームを使用するかどうかを決定しておく必要があります。永続ボリュームを使用すると、管理ノードのデータを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。

次の図に、この手順の概要を示します。



手順

1. ネットアップ サポート サイトから、インストール環境に対応したOVAまたはISOをダウンロードします。
 - Elementソフトウェア :
 - NetApp HCI :
 1. ダウンロードするソフトウェアのバージョン番号を選択します。
 2. **Go**をクリックします。
 3. 表示されるプロンプトをそれぞれクリックして確認し、EULAに同意し、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。
 1. OVAを導入します。
 2. 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り、同一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、管理ネットワークがストレージネットワークにルーティングできることを確認します。
3. ISOをダウンロードした場合は、次の手順を実行します。
 1. 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
 - 12GB RAM
 - 400GBの仮想ディスク、シンプルビジョニング
 - インターネットアクセスとストレージMVIPへのアクセスが可能な仮想ネットワークインターフェイス×1
 - (SolidFireオールフラッシュストレージの場合はオプション) ストレージクラスタへの管理ネットワークアクセスが可能な仮想ネットワークインターフェイス×1。ストレージクラスタが管理ノード（eth0）とは別のサブネット上にある環境で永続ボリュームを使用する場合は、ストレージサブネット（eth1）上のVMに2つ目のネットワークインターフェイスコントローラ（NIC）を追加するか、管理ネットワークからストレージネットワークへルーティング可能なことを確認します。



注意: 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。

2. 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。
注: 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。
5. 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。

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

6. 管理ノードネットワーク（eth0）を設定します。
注: ストレージトラフィックを分離するために追加のNICが必要な場合は、別のNICの設定手順を参照してください。

ストレージ NICの設定 (15ページ)

7. 管理ノードにSSH接続します。
8. SSHを使用して次のコマンドを実行し、root権限を取得します。プロンプトが表示されたら、パスワードを入力します。

```
sudo su
```

9. 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 (NTP) ことを確認します。

注 : vSphere で **Synchronize guest time with host** は、 VM オプションのボックスをオンにする必要があります。今後VMを変更する場合はこのオプションを無効にしてください。

10. 管理ノードのセットアップ コマンドを設定します。

注 : セキュアプロンプトで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。

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

1. 次の各必須パラメータについて、[]内の値（かっこを含む）を置き換えます。

注 : ()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 address]

Elementソフトウェアを実行しているストレージ クラスタのMVIP（管理仮想IPアドレス）。

--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。

--telemetry_active (-t) [true]

trueのままにして、Active IQによる分析のためのデータ収集を有効にします。

2. (オプション) : アクティブな IQ エンドポイント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 データが処理される送信先エンドポイント。このパラメータを指定しない場合、デフォルトのエンドポイントが使用されます。

3. (オプション) : 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。



注意 : 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, default: false]

永続ボリュームを有効または無効にします。永続ボリューム機能を有効にするには、`true`を入力します。

--persistent_volumes_account (-pva) [account_name]

`--use_persistent_volumes`を`true`に設定した場合、永続ボリュームに使用するストレージアカウント名をこのパラメータに入力します。

注: 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]

永続ボリュームを使用する、Elementソフトウェアを実行しているストレージクラスタのMVIP（管理仮想IPアドレス）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須です。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。

4. 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。プロキシサーバを設定する場合、このパラメータは必須です。

--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には必須です。このパラメータを指定すると、`--proxy_port`の入力を求められます。

--proxy_username (-pu) [username]

プロキシユーザ名。このパラメータは省略可能です。

--proxy_password (-pp) [password]

プロキシパスワード。このパラメータは省略可能です。

--proxy_port (-pq) [port, default: 0]

プロキシポート。このパラメータを指定すると、プロキシのホスト名またはIP（`--proxy_hostname_or_ip`）の入力を求められます。

--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。

11.（オプション）各パラメータに関する詳細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、初期導入時の構成に基づいて必須かオプションかが決まります。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。

12. `setup-mnode`コマンドを実行します。

13. ブラウザから、管理ノード REST API UI にログインします。

- Storage MVIP にアクセスしてログインします。
次の手順用に証明書が承認されます。

- 管理ノードで REST API UI を開きます。`https://[management node IP]/mnode`

14. Management Node REST API UI で **Authorize、または任意のロックアイコンをクリックし、次の手順を実行します。**

1. クラスタのユーザ名とパスワードを入力します。
 2. `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。
 3. **Authorize**クリックするとセッションが開始されます。
15. 次GET /assetsの手順で必要なベースアセット ID を検索するには、を実行します。
1. [GET /assets
 2. **Try it out**をクリックします。
 3. **Execute**をクリックします。
 4. ベースアセットの" `id`"の値をクリップボードにコピーします。

注: インストール環境には、インストール時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。

Server response

Code	Details
200	Response body <pre>[{ "compute": [], "config": { "collector": { "remoteHost": "monitoring" } }, "links": [{" "id": "84ba38b3-ed88-4916-ab3a-08b3b1b3da83", "name": "IP-4400", "ots": [], "storage": [{" "_links": { "compute": [{" "asset": "84ba38b3-ed88-4916-ab3a-08b3b1b3da83", "id": "84ba38b3-ed88-4916-ab3a-08b3b1b3da83", "name": "IP-4400", "storage": [] }] } }] }] }]</pre>

16. HCI 監視用の vCenter コントローラ資産（NetApp HCI インストールのみ）とハイブリッドクラウド制御（すべてのインストール用）を、管理ノードの既知の資産に追加します。
1. **POST /assets/{asset_id}/controllers**をクリックすると、コントローラのサブアセットが追加されます。
 2. **Try it out**をクリックします。
 3. **Model**タブで定義されている必要なペイロード値を vCenter と vCenter のクレデンシャルのタイプで入力します。
 4. クリップボードにコピーし `asset_id` た親ベースアセット ID を「」フィールドに入力します。
 5. **Execute**をクリックします。
17. （NetApp HCI の場合のみ）管理ノードの既知の資産にコンピューティングノード資産を追加します。
1. **POST/assets/{asset_id}/compute-nodes**をクリックすると、コンピュートノードアセットの資格情報を含むコンピュートノードサブアセットが追加されます。
 2. **Try it out**をクリックします。
 3. ペイロードに **Model**、タブで定義されている必要なペイロード値を入力します。
ESXi ホストを入力し、"Hardware_Tag" パラメータを削除します。
 4. クリップボードにコピーし `asset_id` た親ベースアセット ID を「」フィールドに入力します。
 5. **Execute**をクリックします。

関連概念

[永続ボリューム](#) (5ページ)

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すが、推奨される管理ノード設定です。

関連タスク

[管理ノードへのアセットの追加](#) (29ページ)

REST API UI を使用して、コンピューティング資産とコントローラ資産を管理ノード構成に追加できます。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。

ストレージ NIC の設定

ストレージに追加の NIC を使用している場合は、管理ノードに SSH で接続するか、vCenter コンソールを使用して curl コマンドを実行し、そのネットワークインターフェイスを設定できます。

開始する前に

- eth0 の IP アドレスがわかっている。
- 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。

手順

1. SSHまたはvCenterコンソールを開きます。
2. 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各パラメータについて、次のコマンドテンプレート（\$ で表示）の値を置き換えます。

注：次のテンプレートのクラスタオブジェクトは必須であり、管理ノードのホスト名の名前変更に使用できます。本番環境では、--insecure または -k オプションを使用しないでください。

```
curl -u $mnode_user_name : $mnode_password -- 安全でない -x post \
https://$mnode_ip:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d '{
  "params": {
    "network": {
      "$eth1": {
        "# default" : false ,
        "アドレス" : "$storage_ip" ,
        "auto" : true ,
        「ファミリー」:「 INET 」
        「方法」:「静的」,
        「MTU」:「 9000 」,
        「ネットマスク」:「 252.0 」,
        「ステータス」:「アップ」
      }
    },
    "cluster": {
      "名前" : "$mnode_host_name"
    }
  },
  "method": "SetConfig"
}'
```

3. コマンドを実行します。

管理ノードのアップグレード

管理ノードを管理ノードバージョン 12.0 にアップグレードするには、バージョン 11.0 以降に正常にアップグレードします。管理ノードバージョン 10.x を使用している場合は、10.x から 11.x にアップグレードすることはできません。アップグレードする前に、11.x への移行手順を実行する必要があります。

手順

次のいずれかの方法で管理ノードをアップグレードします。

- エンドツーエンドの NetApp HCI または SolidFire ストレージシステムのアップグレードの一部として管理ノードをアップグレードする場合は、製品に応じて次の手順を実行します。

[ネットアップのマニュアル：アップグレードの概要](#)

- 管理ノードをアップグレードして最新バージョンを取得する場合は、使用しているバージョンの手順に従います。

注：管理ノード 10.x から 11.x への移行手順についても説明します。

[ネットアップのマニュアル：管理ノードのアップグレード](#)

管理ノードのリカバリ

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。

開始する前に

- 以前の管理ノードでNetApp Elementソフトウェアバージョン11.3以降を実行し、永続ボリューム機能を使用していたことが条件です。
- 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IPv4を使用している必要があります。また、管理ノードでIPv6がサポートされていないことも条件です。
- 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種類を特定しておきます。

次の表を参考にしてください。

プラットフォーム	インストールイメージの種類
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

手順

- ネットアップサポートサイトから、インストール環境に対応したOVAまたはISOをダウンロードします。
 - Elementソフトウェア :
 - NetApp HCI :
 - ダウンロードするソフトウェアのバージョン番号を選択します。
 - Goをクリックします。
 - 表示されるプロンプトをそれぞれクリックして確認し、EULAに同意し、ダウンロードする管理ノードのイメージを選択します。
- OVAをダウンロードした場合は、次の手順を実行します。
 - OVAを導入します。
 - 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)を追加します。
- ISOをダウンロードした場合は、次の手順を実行します。
 - 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
 - 12GB RAM
 - 400GBの仮想ディスク、シンプルビジョニング
 - インターネットアクセスとストレージMVIPへのアクセスが可能な仮想ネットワークインターフェイス×1

- (SolidFireオールフラッシュストレージの場合はオプション) ストレージクラスタへの管理ネットワークアクセスが可能な仮想ネットワークインターフェイス×1。ストレージクラスタが管理ノード(eth0)とは別のサブネット上にある環境で永続ボリュームを使用する場合は、ストレージサブネット(eth1)上のVMに2つ目のネットワークインターフェイスコントローラ(NIC)を追加するか、管理ネットワークからストレージネットワークヘルーティング可能なことを確認します。



注意: 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。

2. 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。

注: 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。
5. 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。

ヒント: テキストを入力するEnterには、キーボードのを3回押して編集モードを開きます。テキストを入力したらEnter、をもう一度押して編集モードを終了します。フィールド間を移動するには矢印キーを使用します。

6. 管理ノードネットワーク(eth0)を設定します。

注: ストレージトラフィックを分離するために追加のNICが必要な場合は、別のNICの設定手順を参照してください。

ストレージ NICの設定 (15ページ)

7. 管理ノードにSSH接続するか、ハイパーバイザーが提供するコンソールを使用します。
8. SSHを使用して次のコマンドを実行し、root権限を取得します。プロンプトが表示されたら、パスワードを入力します。

```
sudo su
```

9. 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(NTP)ことを確認します。

注: vSphereでSynchronize guest time with hostは、VMオプションのボックスをオンにする必要があります。今後VMを変更する場合はこのオプションを無効にしてください。

10. クラスタでホストされている永続ボリュームに再接続し、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よう、管理ノードの再導入コマンドを設定します。

注: セキュアプロンプトでパスワードを入力するように求められます。

```
/sf /packages/mnode/REDEプロイ -mnode --mnode_admin_user [ ユーザ名 ]
```

注: 次の各パラメータについて、[] ブラケット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。

- 次の必須パラメータを追加するか、スクリプトで情報の入力を求めるプロンプトを表示できます。

--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_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。

--storage_mvip (-sm) [MVIP address]

Elementソフトウェアを実行しているストレージクラスタのMVIP（管理仮想IPアドレス）。リカバリ用の管理ノードデータが格納された永続ボリュームを含む。

--persistent_volumes_account (-pva) [account_name]

永続ボリュームを含むクラスタのストレージアカウント名。クラスタ内のボリュームを所有するストレージユーザアカウントの名前を正確に入力します。

- (オプション) 各パラメータに関する詳細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、初期導入時の構成に基づいて必須かオプションかが決まります。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。

11. redeploy-mnodeコマンドを実行します。

管理ノードの使用

管理ノード (mNode) は、システム サービスのアップグレード、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、Active IQへの接続（システム監視）、ネットアップ サポートへのアクセス許可（トラブルシューティング）に使用します。

Elementソフトウェアバージョン11.3以降を実行しているクラスタでは、管理ノードUI ([https://\[mNode IP\]:442](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。また、組み込みのREST API UI ([https://\[mNode IP\]/mnnode](https://[mNode IP]/mnnode)) 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、管理ノードが認識しているアセットの管理などの管理ノード サービスに関連するAPIを実行し、またその内容を把握することができます。

関連タスク

[管理ノードのノードUIへのアクセス](#) (20ページ)

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。

[管理ノードのREST API UIへのアクセス](#) (21ページ)

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。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。

[ネットワーク サポートによるリモート接続の有効化](#) (27ページ)

NetApp Elementソフトウェアベースのストレージ システムに関して技術的な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。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。

[REST APIを使用するための承認の取得](#) (22ページ)

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を指定する必要があります。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。

管理ノードへのアクセス

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。

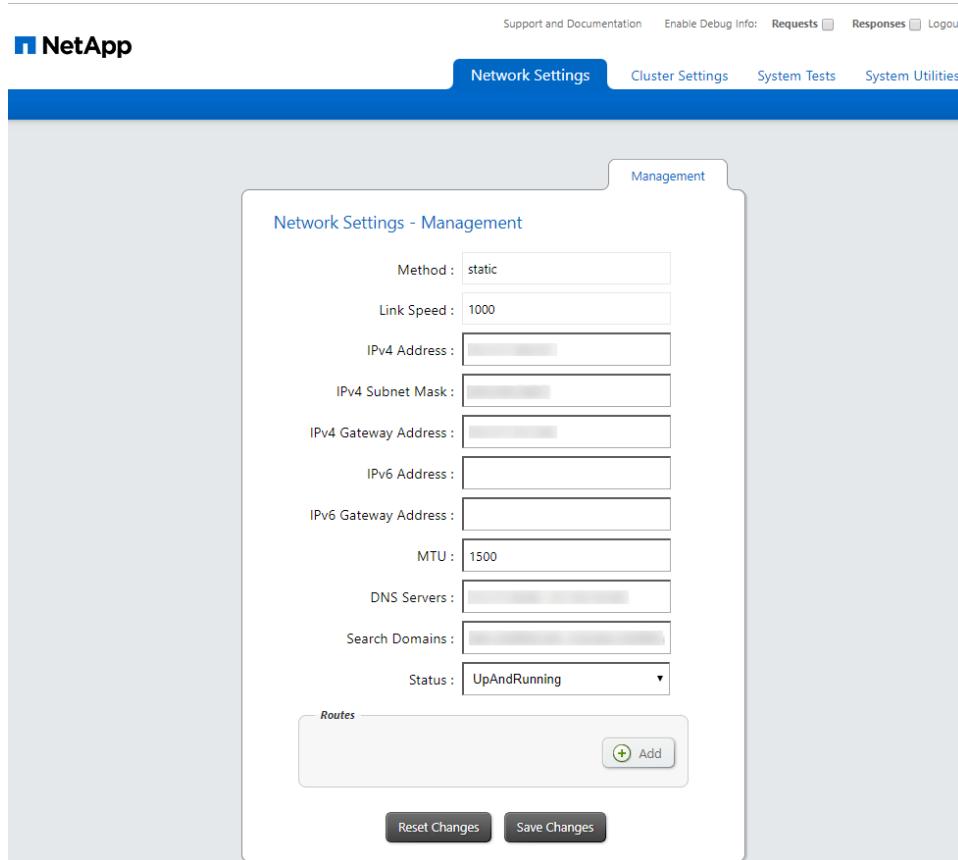
管理ノードのノードUIへのアクセス

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、管理ノードのIPアドレスに続けて「:442」と入力します。

[https://\[IP address\]:442](https://[IP address]:442)



- 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。

関連タスク

[管理ノードのREST API UIへのアクセス](#) (21ページ)

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。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。

管理ノードのREST API UIへのアクセス

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。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

- 管理サービスのREST API UIにアクセスするには、管理ノードのIPアドレスに続けて「/mnode」と入力します。

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

The screenshot shows the Management Services API Swagger UI. At the top, there's a header with the title 'MANAGEMENT SERVICES API' and a sub-header indicating it's the configuration REST service for MANAGEMENT SERVICES. It also shows the base URL as 'https://10.117.11.11/mnode/swagger.json'. Below the header, there are two main sections: 'logs Log service' and 'assets Asset service'. The 'logs' section contains one endpoint: 'GET /logs Get logs from the MNODE service(s)'. The 'assets' section contains several endpoints: 'POST /assets Add a new asset', 'GET /assets Get all assets', 'GET /assets/compute-nodes Get all compute nodes', 'GET /assets/compute-nodes/{compute_node_id} Get a specific compute node by ID', 'GET /assets/controllers Get all controllers', 'GET /assets/controllers/{controller_id} Get a specific controller by ID', 'GET /assets/storage-clusters Get all storage clusters', 'GET /assets/storage-clusters/{storage_cluster_id} Get a specific storage cluster by ID', 'PUT /assets/{asset_id} Modify an asset with a specific ID', 'DELETE /assets/{asset_id} Delete an asset with a specific ID', 'GET /assets/{asset_id} Get an asset by its ID', 'POST /assets/{asset_id}/compute-nodes Add a compute asset', 'GET /assets/{asset_id}/compute-nodes Get compute assets', 'PUT /assets/{asset_id}/compute-nodes/{compute_id} Update a specific compute node asset', and 'DELETE /assets/{asset_id}/compute-nodes/{compute_id} Delete a specific compute node asset'. Each endpoint has a lock icon next to it, indicating it's secured.

2. [Authorize]または任意のロックアイコンをクリックし、クラスタ管理者のクレデンシャルを入力してAPIを使用する権限を取得します。

関連タスク

[管理ノードのノードUIへのアクセス](#) (20ページ)

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。

[プロキシサーバの設定](#) (31ページ)

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。

[SolidFireオールフラッシュストレージに対するActive IQコレクタサービスの有効化](#)
(28ページ)

インストールまたはアップグレード時にSolidFireオールフラッシュストレージに対してストレージのテレメトリ(Active IQコレクタサービス)を有効にしていない場合、有効にすることができます。AIQ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データをNetApp SolidFire Active IQに転送します。

REST APIを使用するための承認の取得

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を指定する

必要があります。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。

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きます。

タスク概要

承認機能は、管理ノードのインストールおよび導入時に自動的にセットアップされます。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。

手順

- 管理ノードで REST API UI を開きます。 `https://[management node IP]/mnode`
- をクリックし**Authorize**て、次の手順を実行します。

注 : 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し、以下の手順に従って承認することもできます。

- クラスタのユーザ名とパスワードを入力します。
- Request bodytype** 値がまだ選択されていない場合は、ドロップダウンリストから選択します。
- 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。
- Authorize**をクリックするとセッションが開始されます。

注 : 承認の試行後に「Auth Error Type Error: Failed to fetch」というエラー メッセージが返された場合は、クラスタのMVIPのSSL証明書の受け入れが必要になる可能性があります。トークンURL内のIPをコピーし、別のブラウザ タブにIPを貼り付けて、再度承認してください。

Available authorizations画面に**Authorized**が表示されます。

- Available authorizations ダイアログボックスを閉じます。

注 : トークンの期限が切れたあとでコマンドを実行しようとすると、「401 Error: UNAUTHORIZED」メッセージが返されます。この場合は、再度承認してください。

NetApp HCIのアラート監視

管理ノードのノードUIの[Alert Monitor]タブでは、NetApp HCIのアラート監視を設定することができます。

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、NetApp HCIのすべてのアラートをvSphere Web Clientインターフェイスで表示できるようにします。



注意 : これらのツールは、SolidFireオールフラッシュストレージなどのストレージ専用クラスタでは設定も使用もされません。ツールを実行すると次のような405エラーが表示されますが、これは設定に応じた想定どおりの動作です。
`webUIParseError : Invalid response from server. 405`

管理ノードのネットワーク設定

管理ノードのノードUIの[Network Settings]タブでは、管理ノードのネットワークインターフェイスに関するフィールドを変更できます。

Method

インターフェイスの設定に使用する方法。有効な方法は次のとおりです。

- 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。
- manual : デフォルトの設定がないインターフェイスを定義する場合に使用します。
- dhcp : DHCP経由でIPアドレスを取得する場合に使用します。
- static : IPv4アドレスが静的に割り当てられたイーサネット インターフェイスを定義する場合に使用します。

Link Speed

仮想NICによってネゴシエートされた速度。

IPv4 Address

eth0ネットワークのIPv4アドレス。

IPv4 Subnet Mask

IPv4ネットワークのアドレス分割。

IPv4 Gateway Address

ローカルネットワークの外部にパケットを送信するためのルータのネットワークアドレス。

IPv6 Address

eth0ネットワークのIPv6アドレス。



注意 : この機能は、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。

IPv6 Gateway Address

ローカルネットワークの外部にパケットを送信するためのルータのネットワークアドレス。



注意 : この機能は、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。

MTU

ネットワークプロトコルで送信可能な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。

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。

Search Domains

システムで利用可能な追加のMACアドレスの検索。

Status

有効な値は次のとおりです。

- UpAndRunning
- Down
- Up

Routes

特定のホストまたはネットワークへの静的ルート（ルートに設定されているインターフェイス経由）。

管理ノードのクラスタ設定

管理ノードのノードUIの[Cluster Settings]タブでは、ノードの状態がAvailable、Pending、PendingActive、およびActiveの場合に、クラスタインターフェイスに関するフィールドを変更できます。

Role

クラスタ内での管理ノードのロール。有効な値はManagementです。

Hostname

管理ノードの名前。

Version

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。

Default Interface

管理ノードとElementソフトウェアを実行しているクラスタとの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。

管理ノード設定のテスト

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あとに、テストを実行して変更を検証できます。

開始する前に

管理ノードの管理者クレデンシャルを使用して、管理ノードUI ([https://\[mNode IP address\]:442](https://[mNode IP address]:442)) にログインしておきます。

手順

1. 管理ノードのユーザインターフェイスで、[System Tests]をクリックします。
2. 次のいずれかを実行します。
 - 指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、[Test Network Config]をクリックします。
 - ICMPパケットを使用して1Gおよび10G両方のインターフェイスで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、[Test Ping]をクリックします。

以下のオプションを追加で定義することもできます。

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した最大MTUより小さくする必要があります。

Timeout mSec

個々のping応答を待機する時間（ミリ秒）を指定します。デフォルト値は500ミリ秒です。

Total Timeout Sec

pingがシステム応答を待機する時間（秒）。この期間を過ぎると、次のpingが実行されるか、またはプロセスが終了します。デフォルト値は5です。

Prohibit Fragmentation

ICMPパケットのDF（Do not Fragment）フラグを有効にします。

関連資料

[管理ノードのネットワーク設定](#) (24ページ)

管理ノードのノードUIの[Network Settings]タブでは、管理ノードのネットワークインターフェイスに関するフィールドを変更できます。

管理ノードからのシステムユーティリティの実行

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。

開始する前に

管理ノードの管理者クレデンシャルを使用して、管理ノードのノードUI (`https://[mNode IP address]:442`) にログインしておきます。

手順

1. 管理ノードのノードUIで、[System Utilities]をクリックします。
2. 実行するユーティリティのボタンをクリックします。
 - **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。



注意 : 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。

次のオプションを指定します。

Action

[Restart] または [Halt] (電源オフ) を選択できます。

Wakeup Delay

ノードがオンラインに戻るまでの時間。

- **Create Cluster Support Bundle** : 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

作成する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須です。

Nodes

バンドルを収集するノードのIPアドレス。[Nodes]または[Mvip]のいずれかを使用してバンドルの収集元のノードを指定します。両方を使用することはできません。このパラメータは、[Mvip]を指定しない場合のみ必須です。

Username

クラスタ管理者のユーザ名。

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るようにします。

Extra Args

このパラメータは、sf_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。

- **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。
- **Reset Node** : 管理ノードを新規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戻ります。



注意 : 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。

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。

Options

リセット処理を実行するための詳細。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。

- **Restart Networking** : 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。



注意 : 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。

ネットワークサポートによるリモート接続の有効化

NetApp Elementソフトウェアベースのストレージシステムに関して技術的な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。リモートアクセスを確立するために、ネットアップサポートはお客様の環境へのリバースSecure Shell (SSH) 接続を確立します。

タスク概要

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。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	API呼び出し / HTTPS(オープン サポートトンネルを介したWeb UIへのリバース ポート転送)	管理ノードからストレージ ノードへ
22	SSHログインアクセス	管理ノードからストレージ ノードへ、またはストレージ ノードから管理ノードへ

手順

1. 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。
2. プロンプトで、`rst -r sfsupport.solidfire.com -u element -p < ポート番号 >`と入力します
SSH接続を使用して管理ノードにアクセスするために必要なポート番号は、ネットアップ サポートから入手します。
3. 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`

SolidFireオールフラッシュ ストレージに対するActive IQコレクタ サービスの有効化

インストールまたはアップグレード時にSolidFireオールフラッシュ ストレージに対してストレージのテレメトリ (Active IQコレクタ サービス) を有効にしていない場合、有効にすることができます。AIQ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データをNetApp SolidFire Active IQに転送します。

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きます。
- インターネットへのアクセスが必要です。Active IQコレクタ サービスをダークサイトから使用することはできません。

手順

1. 管理ノードで REST API UI を開きます。`https://[management node IP]/mnode`
2. **Authorize**をクリックするか、ロックアイコンをクリックして、次の手順を実行します。
 1. クラスタのユーザ名とパスワードを入力します。
 2. `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。
 3. **Authorize**クリックするとセッションが開始されます。
3. **GET /assets**をクリックします。
4. ベース アセットの"`id`"の値をクリップボードにコピーします。

注:ベース アセットとサブアセットは、管理ノードのインストールまたはアップグレード時にアップグレード スクリプトまたはセットアップ スクリプトを実行したときに作成されています。

Server response

Code	Details
200	Response body
[{ "compute": [], "config": { "collector": { "remoteHost": "monitoring" } }, {id": "84ba38b3-ed88-4916-ab3a-08b3b1b3da83", "links": [] }, "ots": [], "storage": [{ "_links": { "self": " /assets/84ba38b3-ed88-4916-ab3a-08b3b1b3da83/storage " } }]]]	

5. ベースアセットを設定します。

1. **PUT /assets/{asset_id}**をクリックします。
2. **Try it out**をクリックします。
3. JSONペイロードに次のコマンドを入力します。

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

4. の Base Asset ステップから IDasset_ID を入力します。
5. **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。

管理ノードへのアセットの追加

REST API UI を使用して、コンピューティング資産とコントローラ資産を管理ノード構成に追加できます。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。

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きます。

タスク概要

NetApp HCI システムを拡張した後に、HCC（ハイブリッドクラウドコントロールPOST /assets/{asset_id}/compute-nodes）にコンピュートノードが表示されない場合は、この手順で説明したを使用してコンピュートノードを追加できます。

手順

1. 管理ノードで REST API UI を開きます。 [https://\[management node IP\]/mnode](https://[management node IP]/mnode)
2. **Authorize**をクリックするか、ロックアイコンをクリックして、次の手順を実行します。
 1. クラスタのユーザ名とパスワードを入力します。
 2. 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。
 3. **Authorize**クリックするとセッションが開始されます。

3. 次のいずれかをクリックして、既存のベースアセットにコンピューティングノードまたはコントローラのサブアセットを追加します。

注 : インストール環境には、インストール時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。

オプション	説明
POST /assets/{asset_id}/controllers	コントローラサブアセットを作成する場合は、このコマンドを実行します。
POST /assets/{asset_id}/compute-nodes	コンピューティングノードサブアセットを作成する場合は、このコマンドを実行します。

4. Try it outをクリックします。
5. Modelタブで定義されている必要なペイロード値を入力します。
重要 : コンピュートノード資産の場合は、ペイロードの例で推奨されている "Hardware_Tag" パラメータを削除します。
6. 親ベースのアセット IDasset_id を「」フィールドに入力します。
7. Executeをクリックします。

ストレージクラスタ管理者パスワードの変更

ストレージクラスタ管理者パスワードは、REST API UIを使用して更新できます。

開始する前に

ストレージクラスタ管理者のパスワードは、NetApp Element ソフトウェアのUIを使用して変更しました。

手順

1. ブラウザから、管理ノード REST API UI にログインします。
 1. Storage MVIP にアクセスしてログインします。
次の手順用に証明書が承認されます。
 2. 管理ノードで REST API UI を開きます。 [https://\[management node IP\]/mnode](https://[management node IP]/mnode)
2. Management Node REST API UI でAuthorize、または任意のロックアイコンをクリックし、次の手順を実行します。
 1. クラスタのユーザ名とパスワードを入力します。
 2. 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。
 3. Authorizeをクリックするとセッションが開始されます。
3. 次GET /assetsの手順で必要なベースアセット ID を検索するには、を実行します。
 1. [GET /assets
 2. Try it outをクリックします。
 3. Executeをクリックします。
4. ベースアセットの「ID」の値をクリップボードにコピーします。
注 : ベースアセットとサブアセットは、管理ノードのインストールまたはアップグレード時にアップグレードスクリプトまたはセットアップスクリプトを実行したとき、またはNetApp Deployment Engineを使用してNetApp HCIを導入したときに作成されます。
5. ストレージ資産の取得：
 1. GET /assets/{ASSET_ID}/storage-clustersをクリックします。

2. **Try it out**をクリックします。
3. の Base Asset ステップから **IDasset_ID** を入力します。
4. **Execute**をクリックします。
6. ストレージ資産を更新します。
 1. **PUT /assets/{ASSET_ID}/storage-clusters/{STORAGE_ID}**をクリックします。
 2. **Try it out**をクリックします。
 3. **Model**タブで定義されている必要なペイロード値を更新します。
 - ホスト名と SSL 証明書の行を削除します。
 - パスワード行に新しいパスワードを入力します。

```
{  
    "username": "admin",  
    "password": "admin",  
    "IP": "10.10.1.124",  
    "config": {}  
}
```

4. 親ベースのアセット **IDasset_id** を「」フィールドに入力します。
5. **Execute**をクリックします。

プロキシ サーバの設定

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。

開始する前に

- 設定するプロキシ サーバのホストおよびクレデンシャル情報が必要です。
- 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。
- 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。

タスク概要

このコマンドは管理ノードのプロキシ設定を更新し、現在の設定を返します。プロキシ設定は、Active IQ、NetApp Deployment Engineによって導入されたNetApp HCI監視サービス、および管理ノードにインストールされたその他のElementソフトウェアユーティリティ（ネットアップ サポート用のリバース サポート トンネルを含む）で使用されます。

手順

1. 管理ノードで REST API UI を開きます。 [https://\[management node IP\]/mnnode](https://[management node IP]/mnnode)
2. **Authorize**をクリックするか、ロックアイコンをクリックして、次の手順を実行します。
 1. クラスタのユーザ名とパスワードを入力します。
 2. **mnnode-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。
 3. **Authorize**クリックするとセッションが開始されます。
3. **PUT /settings**をクリックします。
4. **Try it out**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またはホスト名およびプロキシ ポートの接続先を入力します。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。

管理サービスからのログの取得

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。

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きます。

手順

- 管理ノードで REST API UI を開きます。 [https://\[management node IP\]/mnode](https://[management node IP]/mnode)
- Authorize**をクリックするか、ロックアイコンをクリックして、次の手順を実行します。
 - クラスタのユーザ名とパスワードを入力します。
 - 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。
 - Authorize**クリックするとセッションが開始されます。
- GET /logs**をクリックします。
- Try it out**をクリックします。
- 次のパラメータを指定します。
 - Lines : ログから取得する行数を入力します。このパラメータは整数で、デフォルト値は1000です。

ヒント : Linesを0に設定すると過去のログコンテンツがすべて取得されるので、注意してください。

- service-name : サービス名を入力します。

ヒント : 管理ノード上のサービスを表示するには、GET /servicesコマンドを使用します。

- type : 取得するログタイプを選択します。

1. service : 実行中の通常のパブリックサービスから取得します。これがデフォルトであり、最も一般的なオプションです。

2. syslog : ホストマシンのすべてのsyslogから取得します。

3. all : すべてのパブリックサービスとsyslogから取得します。

- since : サービスログの開始日時をISO-8601タイムスタンプで追加します。

ヒント: 長期間のログを収集する場合は、sinceパラメータに適切な値を指定してください。

- archived : ログ要求にアーカイブ ファイルを追加します。

6. **Execute**をクリックします。

製品マニュアルとその他の情報の参照先

NetApp HCIとSolidFireオールフラッシュストレージについてより詳しい使用および管理办法を知りたい場合は、それぞれの製品のドキュメントセンターとリソースページにある情報を参照してください。

ドキュメントセンターでは、ハードウェアの設置とメンテナンスに関する情報、利用可能なその他のコンテンツ、既知の問題と解決済みの問題へのリンク、および最新のリリースノートも参照できます。リソースページには、データシート、テクニカルレポート、ホワイトペーパー、およびビデオへのリンクが掲載されています。

- [*NetApp HCI*のマニュアル](#)
- [*NetApp HCI*ドキュメントセンター](#)
- [*NetApp HCI*のリソースページ](#)
- [*SolidFire* および *Element 12.0* ドキュメンテーションセンター](#)
- [*SolidFire* および *Element 11.8* ドキュメンテーションセンター](#)
- [*SolidFire / Element 11.7* ドキュメントセンター](#)
- [*SolidFire / Element 11.5* ドキュメントセンター](#)
- [*SolidFire / Element 11.3* ドキュメントセンター](#)
- [*SolidFire*のリソースページ](#)

ネットアップ サポートへの問い合わせ

ネットアップ製品に関するサポートのご依頼、ご意見やご要望については、ネットアップ
サポートまでお問い合わせください。

- Web : mysupport.netapp.com

著作権に関する情報

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S.A.

このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないかかる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を隨時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

ここに記載されている「データ」は商品目（FAR 2.101で定義）に該当し、その所有権はネットアップに帰属します。米国政府は、データが提供される際の米国政府との契約に関連し、かつ当該契約が適用される範囲においてのみ「データ」を使用するための、非独占的、譲渡不可、サブライセンス不可、世界共通の限定的な取り消し不可のライセンスを保有します。ここに記載されている場合を除き、書面によるネットアップの事前の許可なく、「データ」を使用、開示、複製、変更、実行、または表示することは禁止されています。米国国防総省のライセンス権限は、DFARS 252.227-7015 (b) 項に規定されている権限に制限されます。

商標に関する情報

NetApp、NetAppのロゴ、ネットアップの商標一覧のページに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。

<http://www.netapp.com/jp/legal/netapptmlist.aspx>

マニュアルの更新について

弊社では、マニュアルの品質を向上していくため、皆様からのフィードバックをお寄せいただく専用のEメールアドレスを用意しています。また、GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合にご案内させていただくTwitterアカウントもあります。

本マニュアルの改善についてご提案がある場合は、次のアドレスまでコメントをEメールでお送りください。

ng-gpso-jp-documents@netapp.com

その際、担当部署で適切に対応させていただくため、製品名、バージョン、オペレーティングシステム、弊社営業担当者または代理店の情報を必ず入れてください。

GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合のご案内を希望される場合は、Twitterアカウント@NetAppDocをフォローしてください。