



NetApp Element Plug-in for vCenter Server 4.3

ユーザ ガイド

2019年12月 | 215-14588_2019-12_ja-jp
ng-gpso-jp-documents@netapp.com

目次

本書の内容	8
vCenter Plug-inの概要	9
ネットワーク ポート要件	10
VMware vSphereの前提条件	14
開始前の準備	15
NetApp Element Plug-in for vCenter Serverのインストール	15
vCenter Plug-inのアップグレード	15
vCenter Serverのアップグレード	18
管理ノードのインストール	19
vCenterへのvCenter Plug-inの登録	23
社内（ダーク サイト）のHTTPサーバ用のvCenterプロパティの変更	26
管理ノードのアップグレード	29
管理ノードのバージョン11.5からバージョン11.7へのアップグ レード	29
管理ノードのバージョン11.3からバージョン11.7へのアップグ レード	31
管理ノードのバージョン11.0 / 11.1からバージョン11.7へのアップ グレード	33
管理ノード10.xからバージョン11.xへの移行	36
ストレージNICの設定（eth1）	38
永続ボリューム	39
vCSAのvCenter Plug-inの登録更新	39
Windows vCenterのvCenter Plug-inの登録更新	42
管理サービスの更新	45
NetApp Hybrid Cloud Controlを使用した管理サービスのアップグ レード	45
mNode APIを使用した管理サービスの更新	46
インストールしたプラグインへのアクセス	47
NetApp Element Plug-in for vCenter Serverの使用方法	49
NetApp Element Configuration拡張ポイント	49
NetApp Element Management拡張ポイント	50
vCenterリンク モード	52
複数クラスタを管理する場合のオブジェクト名のベストプラク ティス	53
クラスタ設定	54
クラスタの追加	54
クラスタの詳細の表示	55
クラスタの詳細	55
個々のクラスタの詳細	56
クラスタ プロファイルの編集	57

クラスタ プロファイルの削除	57
Virtual Volumesの有効化	58
保存データの暗号化の有効化	59
保存データの暗号化の無効化	59
SSHの有効化	59
SSHの無効化	60
SSHタイム リミットの変更	60
保護ドメインの監視設定	60
クラスタのシャットダウン	61
NetApp HCIの拡張	61
管理ノード (mNode) の設定	63
QoSSIOCの管理ノードの設定	63
QoSSIOCの管理ノード設定の編集	64
QoSSIOCの管理ノード設定のクリア	65
QoSSIOCサービスのパスワードの変更	65
QoSSIOCイベントの表示	67
QoSSIOCイベントの詳細	67
プラグインの製品情報	69
レポート作成	70
レポート概要	70
イベント ログの表示	72
イベント ログ	72
イベント タイプ	73
アラート	74
アラート エラー コード	75
iSCSIセッション	83
実行中のタスク	84
ボリュームのパフォーマンス	85
管理	87
データストア管理	87
データストアの作成	87
データストア リストの表示	90
データストアの拡張	91
データストアのクローニング	91
データストアの共有	94
VAAI UNMAPの実行	95
データストアの削除	96
QoSSIOC自動化	96
QoSSIOC自動化の有効化	98
QoSSIOC統合の無効化	98
ボリュームの管理	99
ボリュームの作成	99
ボリュームの詳細の表示	100
ボリュームの編集	104

ボリュームのクローニング	106
ボリュームのバックアップとリストアの処理	107
ボリュームの削除	113
ボリュームのパーシ	114
削除したボリュームのリストア	115
アクセス グループへのボリュームの追加	115
アクセス グループからのボリュームの削除	116
複数のボリュームへのQoSポリシーの適用	116
ボリュームのQoSポリシーの関連付けの変更	117
ユーザ アカウントの管理	117
アカウントの作成	118
アカウントの詳細	118
アカウントの編集	119
アカウントの削除	119
ボリューム アクセス グループ	120
アクセス グループの作成	120
ボリューム アクセス グループの詳細	121
アクセス グループの編集	121
アクセス グループの削除	122
イニシエータ	122
イニシエータの作成	122
イニシエータの詳細	123
イニシエータの編集	123
イニシエータの削除	124
ボリューム アクセス グループへのイニシエータの追加	124
QoSポリシー	125
QoSポリシーの作成	125
QoSポリシーの詳細	125
QoSポリシーの編集	126
QoSポリシーの削除	126
データ保護	128
ボリュームSnapshot	128
ボリュームSnapshotの作成	128
ボリュームSnapshotの詳細	129
Snapshotの編集	130
Snapshotからのボリュームのクローニング	131
Snapshotへのボリュームのロールバック	132
ボリュームSnapshotのバックアップ処理	132
Snapshotの削除	135
グループSnapshot	136
グループSnapshotの作成	136
グループSnapshotの詳細	137
グループSnapshotの編集	138
グループSnapshotからのボリュームのクローニング	138

グループSnapshotへのボリュームのロールバック	139
グループSnapshotの削除	140
Snapshotスケジュール	140
Snapshotスケジュールの作成	140
Snapshotスケジュールの詳細	141
Snapshotスケジュールの編集	142
Snapshotスケジュールのコピー	143
Snapshotスケジュールの削除	143
リアルタイムのリモートレプリケーションのためのクラスタとボ リュームのペアリング設定	144
クラスタのペアリング	145
ボリュームのペアリング	149
ボリュームレプリケーションの検証	157
レプリケーション後のボリューム関係の削除	157
ボリューム関係の管理	157
クラスタ管理	163
ドライブ	163
クラスタへの使用可能ドライブの追加	163
ドライブの詳細	164
ドライブの削除	165
ノード	165
NetApp HCIストレージ ノード	165
NetApp HCIコンピューティング ノード	165
SolidFireストレージ ノード	166
SolidFire Fibre Channelノード	166
クラスタへのノードの追加	166
ノードの詳細	167
クラスタからのノードの削除	168
クラスタ ノードの再起動	169
クラスタ ノードのシャットダウン	170
VLANの管理	170
VLANの作成	171
仮想ネットワークの詳細	172
仮想ネットワークの編集	172
仮想ネットワークの削除	173
仮想ボリューム	174
vSphere Virtual Volumes (VVOL) 機能の設定	174
NetApp Element VASA Providerの登録	174
VVOLデータストアの作成	175
仮想ボリュームの詳細の表示	176
仮想ボリュームの詳細	177
個々の仮想ボリュームの詳細	177
ストレージ コンテナ	181
ストレージ コンテナの作成	181

ストレージ コンテナの詳細の表示	182
ストレージ コンテナの削除	185
プロトコル エンドポイント	185
プロトコル エンドポイントの詳細の表示	186
vCenter Plug-inの登録解除	189
vCenter Plug-inの削除	191
トラブルシューティング	193
プラグインの登録は成功するがWeb Clientにアイコンが表示されない	193
登録画面からプラグインを登録中にエラーが発生する	194
登録画面からプラグインを更新中にエラーが発生する	194
登録画面でキーストア エラーが発生する	194
ネットアップの拡張機能をアップグレードできないというエラー メッセージが表示される	195
プラグインの削除は完了するがアイコンが残る	195
管理者パスワードの変更後にプラグインを登録解除または削除できない	196
プラグインの管理タスクが失敗するか、またはESXiホストからボリュームにアクセスできない	196
Firefox 59.0.2ブラウザでvCenter Plug-inを使用するとエラーが発生する	196
データストアの削除処理が失敗する	197
ペアリング キーを使用してクラスタ ペアを接続できない	197
QoSSIOCステータスに関するエラー メッセージ	197
QoSSIOCサービスが使用可能と表示されるが使用できない	198
データストアでQoSSIOCが有効になっているが使用できない	198
製品マニュアルとその他の情報の参照先	199
ネットアップ サポートへの問い合わせ	200
著作権に関する情報	201
商標に関する情報	202
マニュアルの更新について	203

本書の内容

このガイドでは、NetApp Element Plug-in for vCenter Serverを使用してストレージ クラスタを設定し、管理する方法について説明します。このガイドは、ストレージ ソリューションの導入、管理、トラブルシューティングの担当者、および仮想マシン（VM）のストレージを割り当てる必要があるVMware管理者の方を対象としています。また、その他のITプロフェッショナルやソフトウェア開発者の方にも役立ちます。

vCenter Plug-inの概要

NetApp Element Plug-in for vCenter Server (VCP) はWebベースのツールで、VMware vSphere Web Clientユーザ インターフェイス (UI) に統合されます。VMware vSphereの拡張機能として動作する使いやすく拡張性に優れた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 クラスタを管理および監視できます。

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つの論理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、各種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。

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、およびストレージ ノードの間の双方向通信を許可する必要があります。

ヒント: 管理ノード、ストレージ ノード、およびクラスタのMVIPの間でICMPを有効にします。

注: vSphereのネットワーク ポートの要件については、VMwareのドキュメントを参照してください。

この表では次の略語を使用します。

- MIP : 管理IPアドレス
- SIP : ストレージIP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

ソース	デスティネーション	ポート	説明
管理ノード	オンラインのソフトウェア リポジトリ : - 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
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 およびその他のタスク (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

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	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	(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
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ルックアップ
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

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 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
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QoSSIOC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てもかまいません。

VMware vSphereの前提条件

NetApp Element Plug-in for vCenter Serverを使用するには、vCenterとESXiを搭載し、ソフトウェアiSCSIアダプタとiSCSIネットワークが設定されたvSphere 6.0、6.5、または6.7が必要です。

このプラグインは、HTML5 vSphere Web Client/バージョン6.7 U2とは互換性がありません。Flash / FLEX用のvSphere Web Client/バージョン6.7 U2とは互換性があります。

データストアの作成には選択したESXiホストでサポートされる最も高いVMFSバージョンが使用されるので、VMFSの互換性に関する問題を防ぐために、実行するvSphereおよびESXiのバージョンをすべてのクラスタメンバーで統一する必要があります。

注意：vSphere HTML5 Web ClientとFlash Web Clientは別々のデータベースを使用しており、両データベースを統合することはできません。一方のクライアントに追加したクラスタは、もう一方のクライアントで認識されません。両方のクライアントを使用する場合は、両方にクラスタを追加してください。

開始前の準備

最新バージョンのNetApp Element Plug-in for vCenter Server (VCP) をvCenterに直接インストールし、vSphere Web Clientを使用してプラグインにアクセスできます。インストールが完了したら、Storage I/O Controlに基づくサービス品質 (QoSSIOC) サービスおよびvCenter Plug-inのその他のサービスを利用できます。

新規インストールを実行する、または既存のインストール環境を更新するには、次のいずれかのトピックを参照してください。

- 新規インストール : [NetApp Element Plug-in for vCenter Serverのインストール](#)
- 既存のインストール環境 : [vCenter Plug-inのアップグレード](#)

NetApp Element Plug-in for vCenter Serverのインストール

新規インストールの場合は、新しい管理ノードを導入してNetApp Element Plug-in for vCenter ServerをvCenter Serverに登録することで、このプラグインを手動でインストールできます。

タスク概要

vCenter High Availability (VCHA) はサポートされません。

手順

1. [vSphere Web Client](#)を使用して、[NetApp HCI](#)または[NetApp Element](#)ソフトウェアのインストール用OVAをダウンロードし、導入します。
2. [プラグインをvCenterに登録します。](#)
3. [プラグインを使用してストレージ クラスタを追加します。](#)
4. [プラグインを使用して管理ノードおよびQoSSIOCを設定します。](#)
5. [NetApp Hybrid Cloud Controlを使用した管理サービスのアップグレード](#)

関連概念

[インストールしたプラグインへのアクセス](#) (47ページ)

vCenter Plug-inのアップグレード

既存のインストール環境でNetApp Element Plug-in for vCenter Server (VCP) をアップグレードするには、最新のアップグレード パッケージを使用するか、またはFlashからHTML5バージョンのvSphere Web Clientに設定を移行する手順を実行します。

開始する前に

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。

手順

1. インストール環境およびアップグレード プランが以下のどの前提条件に該当するかに応じて、対応する手順に従ってプラグインをアップグレードします。

注意：プラグイン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ください。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。

前提条件	手順
- 現在のプラグインは 3.0.1または4.xで、vCenter Serverに登録されている。 - FlashベースのvSphere Web Clientを使用している。 - アップグレードしたプラグインをFlashバージョンのvSphere Web Clientで使用する。	- vSphere Web Clientからログアウトします。 - 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。 - 管理ノード11.0、11.1、11.3、または11.5からアップグレードする場合は、Elementソフトウェア11.7またはNetApp HCI 1.7の管理ノードISOをダウンロードして導入し、次のいずれかのアップグレード手順を実行します。 - 管理ノードのバージョン11.5からバージョン11.7へのアップグレード - 管理ノードのバージョン11.3からバージョン11.7へのアップグレード - 管理ノードのバージョン11.0/11.1からバージョン11.7へのアップグレード - 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、管理ノード11.3以降に更新する前に、管理ノード設定を管理ノード11.1の新しいVMに移行する必要があります。vCenter Plug-in 4.3には管理ノード11.3以降が必要です。 管理ノード10.xからバージョン11.xへの移行 - 登録ユーティリティ (https://[management node IP]:9443) を使用して、vCSAまたはWindowsからvCenterへのプラグインの登録を更新します。 注：必要に応じて、社内（ダークサイト）のHTTPサーバ用のプロパティを変更してください。 HTTPサーバのプロパティの変更 - 管理サービスを更新します。 NetApp Hybrid Cloud Controlを使用した管理サービスのアップグレード - vSphere Web Clientにログインし、アップグレードが正常に完了したことを確認します。 インストールしたプラグインへのアクセス

前提条件	手順
- 現在のプラグインは 3.0.1 または 4.x で、vCenter Server に登録されている。 - Flash ベースの vSphere Web Client を使用している。 - アップグレードしたプラグインをバージョン 6.5 または 6.7 の HTML5 vSphere Web Client で使用する。	- vSphere Web Client からログアウトします。 - 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。 - 管理ノード 11.0、11.1、11.3、または 11.5 からアップグレードする場合は、Element ソフトウェア 11.7 または NetApp HCI 1.7 の管理ノード ISO をダウンロードして導入し、次のいずれかのアップグレード手順を実行します。 管理ノードのバージョン 11.5 からバージョン 11.7 へのアップグレード 管理ノードのバージョン 11.3 からバージョン 11.7 へのアップグレード 管理ノードのバージョン 11.0 / 11.1 からバージョン 11.7 へのアップグレード - 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、管理ノード 11.3 以降に更新する前に、管理ノード設定を管理ノード 11.1 の新しい VM に移行する必要があります。vCenter Plug-in 4.3 には管理ノード 11.3 以降が必要です。 管理ノード 10.x からバージョン 11.x への移行 - 登録ユーティリティ (https://[management node IP]:9443) を使用して、vCSA または Windows から vCenter へのプラグインの登録を更新します。 注： 必要に応じて、社内（ダーク サイト）の HTTP サーバ用のプロパティを変更してください。 HTTP サーバのプロパティの変更 - 管理サービスを更新します。 NetApp Hybrid Cloud Control を使用した管理サービスのアップグレード - vSphere HTML5 Web Client にログインし、アップグレードが正常に完了したことを確認します。 インストールしたプラグインへのアクセス - プラグインを使用して次の手順を実行します。 ストレージ クラスタを追加します。 管理ノードと QoS SIOC を設定します。

前提条件	手順
- 現在のプラグインは4.1以降で、vCenter Serverに登録されている。 - FlashベースのvSphere Web Clientを使用している。 - プラグインはアップグレードせず、既存のバージョンを維持する。 - FlashベースのvSphere Web ClientからHTML5ベースのvSphere Web Clientに移行する。	vSphere Flash Web Clientで管理ノードの設定をクリアします。 - vSphere Flash Web Clientからログアウトします。 - vSphere HTML5 Web Clientにログインします。 - プラグインを使用して次の手順を実行します。 ストレージ クラスタを追加します。 管理ノードとQoSSIOCを設定します。

関連概念

[インストールしたプラグインへのアクセス](#) (47ページ)

関連タスク

[vCenter Plug-inの登録解除](#) (189ページ)

[vCenter Plug-inの削除](#) (191ページ)

[vCenterへのvCenter Plug-inの登録](#) (23ページ)

vCenter Serverのアップグレード

vCenter Serverをアップグレードする前にvCenter Plug-inの登録を解除して、アップグレードの完了後にもう一度プラグインを登録する必要があります。vCenter Serverをアップグレードするとプラグイン データが破棄されるため、クラスタの再設定や、場合によっては管理ノード (mNode) のQoSSIOCの再設定も必要になります。

手順

1. プラグインが関連付けられているvCenterからプラグインの登録を解除します。
2. vCenterを最新バージョンにアップグレードします。
3. アップグレードしたvCenterにプラグインを登録します。
4. プラグインを使用してクラスタを追加します。
5. オプション：管理ノードの設定を行います。

関連タスク

[vCenter Plug-inの登録解除](#) (189ページ)

[vCenterへのvCenter Plug-inの登録](#) (23ページ)

[クラスタの追加](#) (54ページ)

[QoSSIOCの管理ノードの設定](#) (63ページ)

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。

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：https://mysupport.netapp.com/products/p/element_software.html
 - NetApp HCI：<https://mysupport.netapp.com/products/p/hci.html>
 - a. 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。
 - b. **[Go]**をクリックします。
 - c. 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。

- 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) 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 ネットワークヘルレ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
- 12GB RAM
- 400GBの仮想ディスク、シンプロビジョニング
- インターネット アクセスとストレージMVIPへのアクセスが可能な仮想ネットワーク インターフェイス×1
- (SolidFireオールフラッシュ ストレージの場合はオプション) ストレージ クラスタへの管理ネットワーク アクセスが可能な仮想ネットワーク インターフェイス×1。ストレージ クラスタが管理ノード (eth0) とは別のサブネット上にある環境で永続ボリュームを使用する場合は、ストレージ サブネット (eth1) 上のVMに2つ目のネットワーク インターフェイス コントローラ (NIC) を追加するか、管理ネットワークからストレージ ネットワークヘルレ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。

- 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。

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には、キーボードのEnterキーを3回押して編集モードを開始します。テキストの入力が終了したら、もう一度Enterキーを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：eth1に2つ目のNICがある場合は、2つ目のNICの設定手順を参照してください。

ストレージNICの設定 (eth1)

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VMオプションの[Synchronize guest time with host]チェック ボックスがオンになっている必要があります。今後VMを変更する場合はこのオプションを無効にしないでください。

10. 管理ノードのセットアップ コマンドを設定します。

注： コマンドにパスワードを指定しないと、パスワードまたはその他の情報を入力するよう求められます。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]
```

- a. 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。

- b. (オプション)： パスワードまたは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。コマンドにこれらのパスワードを指定しないと、セキュアプロンプトでパスワードを入力するよう求められます。

--mnode_admin_password (-mp) [password]

管理ノードの管理者アカウントのパスワード。一般には、管理ノードへのログインに使用したユーザ アカウントのパスワードです。

--storage_password (-sp) [password]

--storage_usernameパラメータで指定したストレージ クラスタ管理者のパスワード。

--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。

- c. (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。

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。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. mNode APIを使用してアセットを追加します。****a. ブラウザを使用して、ストレージのMVIPにアクセスしてログインします。**

次の手順用に証明書が承認されます。

b. ブラウザを使用して、https://<ManagementNodeIP>/mnodeにアクセスします。**c. vCenterコントローラ アセットを、HCIの監視（NetApp HCI環境のみ）およびHybrid Cloud Control（HCC）用の管理ノードの既知のアセットに追加します。****d. [Authorize]をクリックし、MVIPのユーザ名とパスワードを入力します。ポップアップ ウィンドウを閉じます。****e. [GET /assets]を実行して、vCenter / コントローラ アセットを追加するために必要なベース アセットIDを取得します。****f. [POST /assets/{ASSET_ID}/controllers]を実行して、vCenterのクレデンシャルを使用してコントローラ アセットを追加します。****g. NetApp HCI用、またはHCCのクラウド サービス オプションにアクセスするために、管理ノードの既知のアセットにコンピューティング アセットを追加します。**

注意: この手順を実行しないと、HCCのクラウド サービス オプションを使用できません。

- h. **[Authorize]**をクリックし、MVIPのユーザ名とパスワードを入力します。ポップアップ ウィンドウを閉じます。
- i. **[GET /assets]**を実行して、コンピューティング アセットを追加するために必要なベース アセットIDを取得します。
- j. **[POST/assets/{asset_id}/compute-nodes]**を実行して、クレデンシャルを使用してコンピューティング アセットを追加します。タイプはESXi Hostです。

関連タスク

[vCenter Plug-inのアップグレード](#) (15ページ)

[NetApp Element Plug-in for vCenter Serverのインストール](#) (15ページ)

vCenterへのvCenter Plug-inの登録

vCenter Plug-in/パッケージをvSphere Web Clientに導入するには、vCenter Serverでパッケージを拡張機能として登録します。登録が完了すると、vSphere環境に接続されたすべてのvSphere Web Clientでこのプラグインを利用できるようになります。

開始する前に

- vSphere Web Clientからログアウトしておきます。
注: ログアウトしないと、このプロセスで行った更新がWeb Clientで認識されません。
- プラグインを登録するためのvCenter Administratorロールの権限が必要です。
- Elementソフトウェア11.3以降を実行する管理ノードOVAを導入しておきます。
- 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きます。
- SSHクライアントまたはWebブラウザ（Chrome 56以降またはFirefox 52以降）を使用します。
- ファイアウォールルールで、TCPポート443、8443、および9443でvCenterとストレージ クラスタMVIP間のオープン ネットワーク通信を許可します。ポート9443は登録に使用され、登録完了後は閉じてもかまいません。クラスタで仮想ボリュウム機能を有効にした場合は、VASA Providerアクセス用にTCPポート8444も開いていることを確認してください。

タスク概要

vCenter Plug-inは、そのプラグインを使用するすべてのvCenter Serverに登録する必要があります。

注: MOBデータの同期を保ち、プラグインをアップグレードできるようにするには、リンク モード環境内の各vCenter Serverにプラグインを登録する必要があります。

接続先のvCenter Serverにプラグインが登録されていない場合、vSphere Web Clientにはプラグインが表示されません。

手順

1. 登録用TCPポートを含む管理ノードのIPアドレスをブラウザに入力します ([https://\[management node IP\]:9443](https://[management node IP]:9443))。

プラグインの[Manage QoSSIOC Service Credentials]ページが表示されます。

2. オプション：vCenter Plug-inを登録する前に、QoSSIOCサービスのパスワードを変更します。
 - a. 次の情報を入力します。
 - **Old Password**：QoSSIOCサービスの現在のパスワード。パスワードをまだ割り当てていない場合は、デフォルトのパスワードを入力します。
solidfire
 - **New Password**：QoSSIOCサービスの新しいパスワード。
 - **Confirm Password**：新しいパスワードをもう一度入力します。
 - b. [Submit Changes]をクリックします。
注：変更を送信すると、QoSSIOCサービスが自動的に再起動されます。
3. [vCenter Plug-in Registration]をクリックします。

4. 次の情報を入力します。

- 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。
- vCenter Administratorのユーザ名。

注：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。

- vCenter Administratorのパスワード。
- (社内サーバ / ダーク サイトの場合) プラグインのZIPのカスタムURL。

注：ほとんどのインストールではデフォルトのパスが使用されます。HTTPサーバまたはHTTPSサーバ（ダーク サイト）を使用する場合や、ZIPファイルの名前またはネットワーク設定を変更した場合は、**[Custom URL]**をクリックして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プラグインのドキュメントを参照してください。

5. **[Register]**をクリックします。

6. オプション：**[Registration Status]**をクリックします。

7. オプション：次の情報を入力します。

- 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
- vCenter Administratorのユーザ名
- vCenter Administratorのパスワード

8. オプション：**[Check Status]**をクリックして、vCenter Serverに新しいバージョンのプラグインが登録されていることを確認します。

9. vSphere Web ClientにvCenter Administratorとしてログインします。

注：この操作でvSphere Web Clientでのインストールが完了します。vCenter Plug-inのアイコンがvSphereのメイン ページに表示されない場合は、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を参照してください。

関連タスク

[vCenter Plug-inのアップグレード](#) (15ページ)

[NetApp Element Plug-in for vCenter Serverのインストール](#) (15ページ)

[管理ノードのインストール](#) (19ページ)

[社内（ダーク サイト） のHTTPサーバ用のvCenterプロパティの変更](#) (26ページ)

関連資料

[プラグインの登録は成功するが Web Clientにアイコンが表示されない](#) (193ページ)

社内（ダーク サイト） のHTTPサーバ用のvCenterプロパティの変更

vCenter Plug-inの登録時に社内（ダーク サイト） のHTTPサーバのURLをカスタマイズする場合は、vSphere Web Clientのプロパティ ファイルを変更する必要があります。

開始する前に

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。

手順

1. vCenterがHTTPサーバからダウンロードを実行できるようにするために、ご使用の環境に対応する手順に従ってwebclient.propertiesファイルを変更します。

オプション	説明
vCSA	a. SSHでvCenter Serverに接続します。 <pre>Connected to service * List APIs: "help api list" * List Plugins: "help pi list" * Launch BASH: "shell" Command></pre> b. コマンドプロンプトで「shell」と入力してrootにアクセスします。 <pre>Command> shell Shell access is granted to root</pre> c. VMware vSphere Web Clientサービスを停止します。 <pre>service-control --stop vsphere-client service-control --stop vsphere-ui</pre> d. ディレクトリを変更します。 <pre>cd /etc/vmware/vsphere-client</pre> e. webclient.propertiesファイルを編集し、allowHttp=trueを追加します。 f. ディレクトリを変更します。 <pre>cd /etc/vmware/vsphere-ui</pre> g. webclient.propertiesファイルを編集し、allowHttp=trueを追加します。 h. VMware vSphere Web Clientサービスを起動します： <pre>service-control --start vsphere-client service-control --start vsphere-ui</pre>

オプション	説明
Windows	a. コマンド プロンプトからディレクトリを変更します。 <pre>cd c:\Program Files\VMware\vCenter Server\bin</pre> b. VMware vSphere Web Clientサービスを停止します。 <pre>service-control --stop vsphere-client service-control --stop vsphere-ui</pre> c. ディレクトリを変更します。 <pre>cd c:\ProgramData\VMware\vCenterServer\cfg\vsphere-client</pre> d. webclient.propertiesファイルを編集し、allowHttp=trueを追加します。 e. ディレクトリを変更します。 <pre>cd c:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui</pre> f. webclient.propertiesファイルを編集し、allowHttp=trueを追加します。 g. コマンド プロンプトからディレクトリを変更します。 <pre>cd c:\Program Files\VMware\vCenter Server\bin</pre> h. VMware vSphere Web Clientサービスを起動します。 <pre>service-control --start vsphere-client service-control --start vsphere-ui</pre>

注：登録手順が完了したら、変更したファイルからallowHttp=trueを削除してかまいません。

2. vCenterをリブートします。

関連タスク

[vCenter Plug-inのアップグレード](#) (15ページ)

[NetApp Element Plug-in for vCenter Serverのインストール](#) (15ページ)

管理ノードのアップグレード

管理ノードをバージョン10.xからバージョン11.0以降にアップグレードしたあと、バージョン11.7にアップグレードできます。vCenter Plug-in 4.3以降には管理ノード11.3以降が必要です。

手順

1. 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。
 - 管理ノード11.5からアップグレードする場合は、Elementソフトウェア11.7またはNetApp HCI 1.7の管理ノードISOをダウンロードして導入します。
[管理ノードのバージョン11.5からバージョン11.7へのアップグレード](#)
 - 管理ノード11.3からアップグレードする場合は、Elementソフトウェア11.7またはNetApp HCI 1.7の管理ノードISOをダウンロードして導入します。
[管理ノードのバージョン11.3からバージョン11.7へのアップグレード](#)
 - 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、Elementソフトウェア11.7またはNetApp HCI 1.7の管理ノードISOをダウンロードして導入します。
[管理ノードのバージョン11.0/11.1からバージョン11.7へのアップグレード](#)
 - 管理ノード10.xからアップグレードする場合は、管理ノード11.3以降に更新する前に、管理ノード設定を管理ノード11.1の新しいVMに移行する必要があります。
[管理ノード10.xからバージョン11.xへの移行](#)

管理ノードのバージョン11.5からバージョン11.7へのアップグレード

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11.5からバージョン11.7へのインプレース アップグレードを実行できます。

開始する前に

- 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。
注: 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11.5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11.7ではIPv6がサポートされません。
ヒント: 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。
- 次のいずれかのオプションを使用して、管理サービス バンドルを最新バージョン(2.1.368以降) に更新しておきます。
 - Hybrid Cloud Control (HCC) : <https://<ManagementNodeIP>>
注: HCCは管理サービス バンドル2.1.326で使用できます。NetApp HCIの場合は、NetApp Deployment Engineを使用して1回かぎりのアップグレードを実行した場合にのみ利用できます。 <https://<StorageNodeMIP>:442/nde>
 - 管理ノードAPI : <https://<ManagementNodeIP>/mnode>
注: 認証後、mNode API PUT /services/update/latestを使用してサービスを更新します。

- 必要な場合、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。

注：追加のネットワーク アダプタは、eth0をSVIPにルーティングできない場合に永続ボリュームで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。

- 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ておきます。
- [NetApp HCI](#)または[Elementソフトウェア](#)用の管理ノードのISOを、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にダウンロードしておきます。

注：ISOのファイル名はsolidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.isoなどです。

- 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ISOと比較することで、ダウンロードの整合性を確認しておきます。

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

手順

- 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
```

- ホーム ディレクトリに切り替え、/mntからISOファイルをアンマウントします。

```
sudo umount /mnt
```

- 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
```

- 11.5 (11.5.0.63) 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。

- 11.7の管理ノードで、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適用します。

注: 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>
```

関連タスク

[vCenter Plug-inのアップグレード](#) (15ページ)

[NetApp Hybrid Cloud Controlを使用した管理サービスのアップグレード](#) (45ページ)

[ストレージNICの設定 \(eth1\)](#) (38ページ)

管理ノードのバージョン11.3からバージョン11.7へのアップグレード

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11.3からバージョン11.7へのインプレース アップグレードを実行できます。

開始する前に

- 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。
注: 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11.3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11.7ではIPv6がサポートされません。
ヒント: 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。
- 次のいずれかのオプションを使用して、管理サービス バンドルを最新バージョン(2.1.368以降) に更新しておきます。
 - Hybrid Cloud Control (HCC) : <https://<ManagementNodeIP>>
注: HCCは管理サービス バンドル2.1.326で使用できます。NetApp HCIの場合は、NetApp Deployment Engineを使用して1回かぎりのアップグレードを実行した場合にのみ利用できます。 <https://<StorageNodeMIP>:442/nde>
 - 管理ノードAPI : <https://<ManagementNodeIP>/mnode>
注: 認証後、mNode API PUT /services/update/latestを使用してサービスを更新します。
- 必要な場合、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。
注: 追加のネットワーク アダプタは、eth0をSVIPにルーティングできない場合に永続ボリュームで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。
- 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ておきます。
- [NetApp HCI](#)または[Elementソフトウェア](#)用の管理ノードのISOを、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にダウンロードしておきます。
注: ISOのファイル名はsolidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.isoなどです。

- 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ISOと比較することで、ダウンロードの整合性を確認しておきます。

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

手順

1. 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
```

2. ホーム ディレクトリに切り替え、/mntからISOファイルをアンマウントします。

```
sudo umount /mnt
```

3. 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
```

4. 11.3 (11.3.0.14235) 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。

5. 11.7の管理ノードで、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適用します。

注：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>
```

関連タスク

[vCenter Plug-inのアップグレード](#) (15ページ)

[NetApp Hybrid Cloud Controlを使用した管理サービスのアップグレード](#) (45ページ)

[ストレージNICの設定 \(eth1\)](#) (38ページ)

管理ノードのバージョン11.0 / 11.1からバージョン11.7へのアップグレード

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11.7へのインプレース アップグレードを実行できます。

開始する前に

- 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。
注: 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11.7ではIPv6がサポートされません。
ヒント: 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。
注: 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。
- 必要な場合、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。
注: 追加のネットワーク アダプタは、eth0をSVIPにルーティングできない場合に永続ボリュームで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。
- 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ておきます。
- [NetApp HCI](#)または[Elementソフトウェア](#)用の管理ノードのISOを、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にダウンロードしておきます。
注: ISOのファイル名はsolidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.isoなどです。
- 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ISOと比較することで、ダウンロードの整合性を確認しておきます。

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

手順

- 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
```

2. ホーム ディレクトリに切り替え、/mntからISOファイルをアンマウントします。

```
sudo umount /mnt
```

3. 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
```

4. 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該当するスクリプトのみを実行してください。どのスクリプトでも、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。

- 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"
```

- 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"
```

- 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。

5. 11.7の管理ノードで、upgrade-mnodeスクリプトを実行して以前の設定を適用します。

注：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。

- 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>
```

- 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>
```

- 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>
```

- 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>
```

6. (NetApp Element Plug-in for vCenter Serverを使用するすべてのNetApp HCI環境およびSolidFireスタンドアロン ストレージ環境) 11.7の管理ノードでvCenter Plug-inを更新します。

- a. vSphere Web Clientからログアウトします。

注：Web Clientからログアウトしないと、このプロセスで行ったvCenter Plug-inに対する更新が認識されません。

- b. 登録ユーティリティ (<https://<ManagementNodeIP>:9443>) に移動します。

- c. **[vCenter Plug-in Registration]** タブをクリックします。

- d. **[Manage vCenter Plug-in]** で **[Update Plug-in]** を選択します。

- e. vCenterのアドレス、およびvCenter管理者のユーザ名とパスワードを更新します。

- f. **[Update]** をクリックします。

- g. vSphere Web Clientにログインし、**[Home] > [NetApp Element Configuration] > [About]** を選択して、プラグインの情報が更新されていることを確認します。

注：登録の更新後にvSphere Web Clientにログインすると、新しいプラグインの更新がインストールされ、新しいデータベースが作成されます。

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バージョン：4.3.0
- NetApp Element Plug-inビルド番号：233

7. mNode APIを使用してアセットを追加します。

- a. ブラウザを使用して、ストレージのMVIPにアクセスしてログインします。

次の手順用に証明書が承認されます。

- b. ブラウザを使用して、<https://<ManagementNodeIP>/mnode> にアクセスします。

- c. vCenterコントローラ アセットを、HCIの監視（NetApp HCI環境のみ）およびHybrid Cloud Control（HCC）用の管理ノードの既知のアセットに追加します。

- d. **[Authorize]** をクリックし、MVIPのユーザ名とパスワードを入力します。ポップアップ ウィンドウを閉じます。

- e. **[GET /assets]** を実行して、vCenter / コントローラ アセットを追加するために必要なベース アセットIDを取得します。

- f. **[POST /assets/{ASSET_ID}/controllers]** を実行して、vCenterのクレデンシャルを使用してコントローラ アセットを追加します。

- g. NetApp HCI用、またはHCCのクラウド サービス オプションにアクセスするために、管理ノードの既知のアセットにコンピューティング アセットを追加します。

注意: この手順を実行しないと、HCCのクラウド サービス オプションを使用できません。

- h. **[Authorize]**をクリックし、MVIPのユーザ名とパスワードを入力します。ポップアップ ウィンドウを閉じます。
- i. **[GET /assets]**を実行して、コンピューティング アセットを追加するために必要なベース アセットIDを取得します。
- j. **[POST/assets/{asset_id}/compute-nodes]**を実行して、クレデンシャルを使用してコンピューティング アセットを追加します。タイプはESXi Hostです。

関連タスク

[vCenter Plug-inのアップグレード](#) (15ページ)

[NetApp Hybrid Cloud Controlを使用した管理サービスのアップグレード](#) (45ページ)

[ストレージNICの設定 \(eth1\)](#) (38ページ)

管理ノード10.xからバージョン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。Elementソフトウェアを10.3以降から11.xにアップグレードするには、管理ノード11.0または11.1と最新のHealthToolsが必要です。

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、電源を投入します。
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。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。
3. 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。
4. 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
```

5. vSphereで、**[NetApp Element Configuration]** > **[mNode Settings]**を選択します。旧バージョンの場合、最初のメニューは**[NetApp SolidFire Configuration]**です。
6. **[Actions]** > **[Clear]**をクリックします。
7. 確認のために**[Yes]**をクリックします。**[mNode Status]**フィールドに**[Not Configured]**と表示されることを確認します。

注: **[mNode Settings]**タブに初めてアクセスした場合、**[mNode Status]**フィールドに**[UP]**ではなく**[Not Configured]**と表示され、**[Actions]** > **[Clear]**を選択できないことがあります。ブラウザの表示を更新すると、**[mNode Status]**フィールドの表示は**[UP]**に変わります。

8. vSphereからログアウトします。

9. Webブラウザで、管理ノードの登録ユーティリティ (<https://<mNode 11.1 IP address>:9443>) を開き、**[QoSSIOC Service Management]**を選択します。
10. QoSSIOCの新しいパスワードを設定します。
 注: デフォルトのパスワードはsolidfireです。新しいパスワードを設定するには、このパスワードが必要です。
11. **[vCenter Plug-in Registration]**タブをクリックします。
12. **[Update Plug-in]**を選択します。
13. 必要な値を入力します。作業が終了したら、**[UPDATE]**をクリックします。
14. vSphereにログインし、**[NetApp Element Configuration] > [mNode Settings]**を選択します。
15. **[Actions] > [Configure]**をクリックします。
16. 管理ノードのIPアドレス、ユーザID（ユーザ名はadmin）と登録ユーティリティの**[QoSSIOC Service Management]**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 Settings]**タブの**[mNode Status]**に**[UP]**と表示され、管理ノード11.1がvCenterに登録されたことを確認します。
17. 管理ノードの登録ユーティリティ (<https://<mNode 11.1 IP address>:9443>) で、**[QoSSIOC Service Management]**からSIOCサービスを再起動します。
18. 1分間待つてから、**[NetApp Element Configuration] > [mNode Settings]**タブを確認します。**[mNode Status]**に**[UP]**と表示されていることを確認してください。
 ステータスが**[DOWN]**の場合は、`/sf/packages/sioc/app.properties`に対する権限を確認します。ファイル所有者に読み取り、書き込み、および実行の権限が必要です。正しい権限は`-rwx-----`です。
19. SIOCプロセスが開始され、**[mNode Status]**に**[UP]**と表示されることを確認したら、管理ノードで`sf-hci-nma`サービスのログを確認します。エラーメッセージが記録されていないことを確認してください。
20. (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-nma
```

21. 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て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。
22. ONTAP SelectがvCenterに設定されている場合は、前の管理ノードの`.ots.properties` ファイルをバージョン11.1の`/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、`systemctl restart sf-hci-nma`コマンドを使用してNMAサービスを再起動します。
23. `journalctl -f | grep -i ots`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。
24. 次の手順でAIQ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. sfcollectorログで動作していることを確認します。
25. vSphereで、[NetApp Element Configuration] > [mNode Settings]タブの[mNode Status]に[UP]と表示されることを確認します。
 26. 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。
 27. 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。

ストレージNICの設定 (eth1)

ストレージに2つ目の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、eth1のネットワークをセットアップできます。

開始する前に

- eth0設定の詳細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。

手順

1. SSHまたはvCenterコンソールを開きます。
2. 以下のコマンドテンプレートを使用し、eth0およびeth1の各必須パラメータの値（\$で示した部分）を置き換えます。

注： コマンド テンプレート内のclusterオブジェクトはオプションであり、管理ノードのホスト名を変更する場合に使用できます。 - -insecureオプションと-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 $mnode-username:$mnode-password --insecure -X POST \
https://$mnode_management_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d '{
  "params": {
    "network": {
      "eth0": {
        "address": "$eth0_ip_mnode_management_IP",
        "dns-nameservers": "$dns_ip_or_hostname",
        "netmask": "$eth0_net_mask",
        "gateway": "$gateway_IP",
        "gatewayV6": ""
      }
    }
  }
}
```

```

        },
        "eth1": {
            "address": "$eth1_ip",
            "netmask": "$eth1_netmask",
            "status": "Up",
            "method": "static",
            "mtu": "9000"
        }
    },
    "cluster": {
        "name": "$desired_mNode_vm_hostname"
    }
},
"method": "SetConfig"
}

```

3. コマンドを実行します。

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： 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作成される新しいアカウントに割り当てられます。永続ボリュームの作成後に、ボリュームとその関連アカウントを変更または削除しないでください。

vCSAのvCenter Plug-inの登録更新

登録画面を使用して、vCenter Server Virtual Appliance (vCSA) のvCenter Plug-inを更新できます。登録画面にはクラスタの管理ノードのIPアドレスからアクセスできます。

開始する前に

- vSphere Web Clientからログアウトしておきます。
注： Web Clientからログアウトしないと、このプロセスで行ったvCenter Plug-inに対する更新が認識されません。
- vCenter ServerにvCenter Plug-in 3.0.1以降を登録済みである必要があります。
- プラグインを登録するためのvCenter Administratorロールの権限が必要です。
- Elementソフトウェア11.3以降を実行する管理ノードOVAを導入しておきます。
- 管理ノードを11.3以降にアップグレードしておきます。
- 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きます。

- SSHクライアントまたはWebブラウザ（Chrome 56以降またはFirefox 52以降）を使用します。
- ファイアウォールルールで、TCPポート443、8443、および9443でvCenterとストレージクラスタMVIIP間のオープン ネットワーク通信を許可します。ポート9443は登録に使用され、登録完了後は閉じてもかまいません。クラスタで仮想ボリューム機能を有効にした場合は、VASA Providerアクセス用にTCPポート8444も開いていることを確認してください。

タスク概要

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。

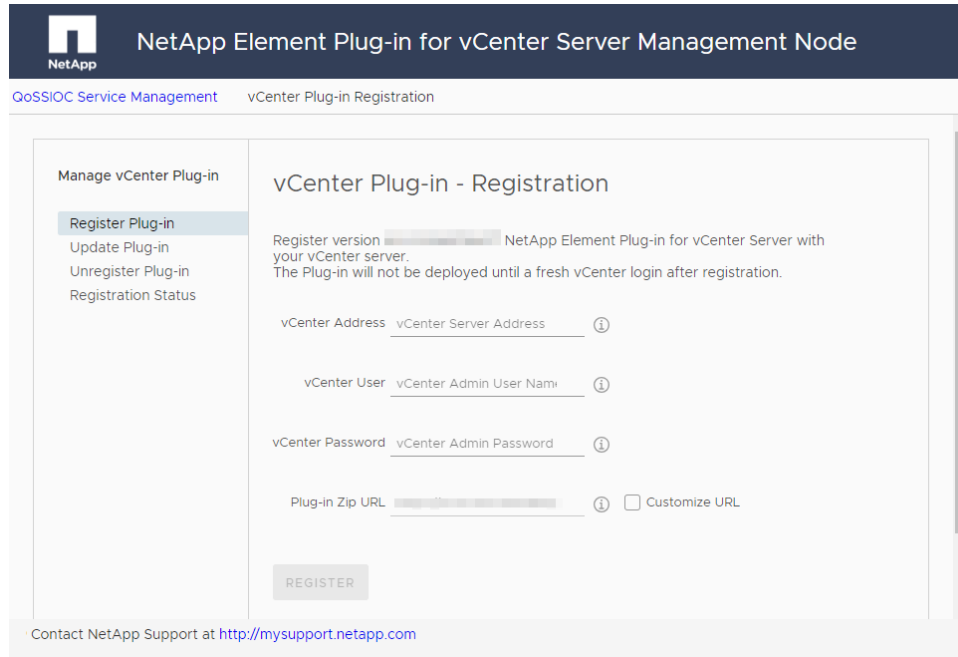
手順

1. 登録用TCPポートを含む管理ノードのIPアドレスをブラウザに入力します（[https://\[management node IP\]:9443](https://[management node IP]:9443)）。

プラグインの[Manage QoSSIOC Service Credentials]ページが表示されます。

The screenshot displays the 'NetApp Element Plug-in for vCenter Server Management Node' interface. The main heading is 'Manage QoSSIOC Service Credentials'. A yellow warning box states: 'The current QoSSIOC password is set to the default value of 'solidfire'. You should customize credentials to better ensure QoSSIOC service security.' Below this, there are three password input fields: 'Old Password' (with a hint 'Current password'), 'New Password' (with a hint 'New password' and an information icon), and 'Confirm Password' (with a hint 'Confirm New Password' and an information icon). A 'SUBMIT CHANGES' button is located at the bottom of the form. On the left, a sidebar shows 'QoSSIOC Management' with 'Manage Credentials' selected and 'Restart QoSSIOC Service' as an option. At the bottom, a link to 'Contact NetApp Support at <http://mysupport.netapp.com>' is provided.

2. [vCenter Plug-in Registration]をクリックします。



3. vCenter Plug-inがすでに登録されているかどうか、および現在のインストールのバージョン番号を確認するには、**[Registration Status]**をクリックし、必要なフィールドに入力して**[Check Status]**をクリックします。
4. **[Update Plug-in]**をクリックします。
5. 次の情報を確認し、必要に応じて更新します。
 - 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。
 - vCenter Administratorのユーザ名。

注： 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。
 - vCenter Administratorのパスワード。
 - (社内サーバ / ダーク サイトの場合) プラグインのZIPのカスタムURL。

注：ほとんどのインストールではデフォルトのパスが使用されます。HTTPサーバまたはHTTPSサーバ（ダーク サイト）を使用する場合や、ZIPファイルの名前またはネットワーク設定を変更した場合は、**[Custom URL]**をクリックして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プラグインのドキュメントを参照してください。
6. **[Update]**をクリックします。
7. オプション：vCenterに更新後のバージョンのプラグインが登録されたことを確認するには、**[Registration Status]**をクリックし、必要なフィールドに入力して**[Check Status]**をクリックします。
8. (vCenter Plug-in 3.0以前のみ) vCenter Plug-in 3.0以前から更新している場合は、vCSAのSSHセッションからrootアカウントとして次のコマンドを入力します。


```
# rm -rf /storage/vsphere-client/netapp-solidfire
# reboot
```

注：この操作により、vSphere Web Clientに新しいvCenter Plug-inがインストールされる前に、バージョン3.0.0のデータベースが削除されます。登録プロセスが完了したら、NetApp Element Configuration拡張ポイントを使用してもう一度クラスタを追加する必要があります。

9. vSphere Web ClientにvCenter Administratorとしてログインします。

注：この操作により、新しいプラグインの更新がインストールされ、新しいデータベースが作成されます。vCenter Plug-inのアイコンがvSphereのメインページに表示されない場合は、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を参照してください。

10. NetApp Element Configuration拡張ポイントの[About]タブでバージョンの変更を確認します。

注：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。

関連タスク

[vCenter Plug-inのアップグレード](#) (15ページ)

[管理ノードのインストール](#) (19ページ)

[社内（ダーク サイト）のHTTPサーバ用のvCenterプロパティの変更](#) (26ページ)

関連資料

[プラグインの登録は成功するがWeb Clientにアイコンが表示されない](#) (193ページ)

Windows vCenterのvCenter Plug-inの登録更新

登録画面から、Windows版vCenter ServerのvCenter Plug-inを更新できます。登録画面にはクラスタの管理ノードのIPアドレスからアクセスできます。

開始する前に

- vSphere Web Clientからログアウトしておきます。

注：Web Clientからログアウトしないと、このプロセスで行ったvCenter Plug-inに対する更新が認識されません。

- vCenter ServerにvCenter Plug-in 3.0.1以降を登録済みである必要があります。
- プラグインを登録するためのvCenter Administratorロールの権限が必要です。
- Elementソフトウェア11.3以降を実行する管理ノードOVAを導入しておきます。
- 管理ノードを11.3以降にアップグレードしておきます。
- 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きます。
- SSHクライアントまたはWebブラウザ（Chrome 56以降またはFirefox 52以降）を使用します。
- ファイアウォールルールで、TCPポート443、8443、および9443でvCenterとストレージクラスタMVI間でのオープン ネットワーク通信を許可します。ポート9443は登録に使用され、登録完了後は閉じてもかまいません。クラスタで仮想ボリューム機能を有効にした場合は、VASA Providerアクセス用にTCPポート8444も開いていることを確認してください。

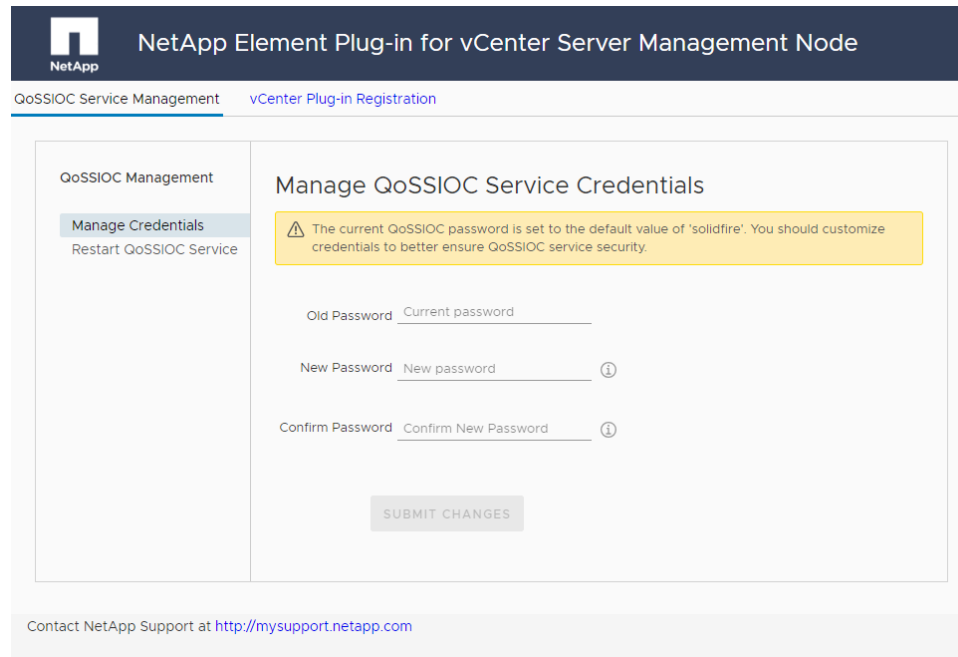
タスク概要

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。

手順

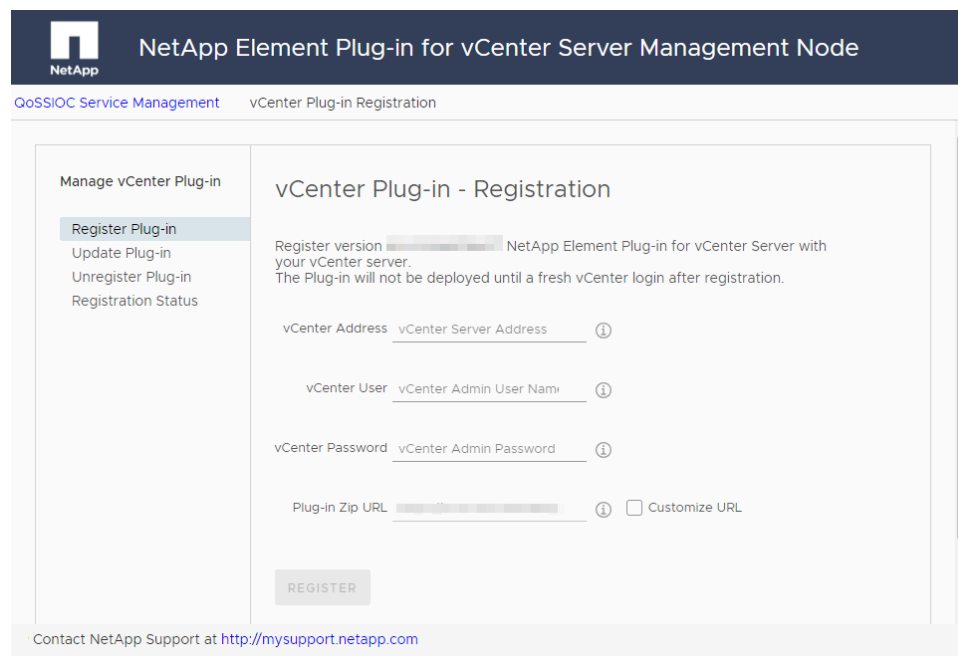
1. 登録用TCPポートを含む管理ノードのIPアドレスをブラウザに入力します（[https://\[management node IP\]:9443](https://[management node IP]:9443)）。

プラグインの[Manage QoSSIOC Service Credentials]ページが表示されます。



The screenshot shows the 'NetApp Element Plug-in for vCenter Server Management Node' interface. The left sidebar has 'QoSSIOC Management' selected, with 'Manage Credentials' highlighted. The main content area is titled 'Manage QoSSIOC Service Credentials'. A yellow warning box states: 'The current QoSSIOC password is set to the default value of 'solidfire'. You should customize credentials to better ensure QoSSIOC service security.' Below this are three password fields: 'Old Password' (with 'Current password' as a hint), 'New Password' (with a password strength icon), and 'Confirm Password' (with 'Confirm New Password' as a hint). A 'SUBMIT CHANGES' button is at the bottom. A footer link says 'Contact NetApp Support at <http://mysupport.netapp.com>'.

2. [vCenter Plug-in Registration]をクリックします。



The screenshot shows the 'NetApp Element Plug-in for vCenter Server Management Node' interface. The left sidebar has 'Manage vCenter Plug-in' selected, with 'Register Plug-in' highlighted. The main content area is titled 'vCenter Plug-in - Registration'. It includes a 'Register version' dropdown set to 'NetApp Element Plug-in for vCenter Server with your vCenter server.' and a note: 'The Plug-in will not be deployed until a fresh vCenter login after registration.' Below are four fields: 'vCenter Address' (with 'vCenter Server Address' as a hint), 'vCenter User' (with 'vCenter Admin User Name' as a hint), 'vCenter Password' (with 'vCenter Admin Password' as a hint), and 'Plug-in Zip URL' (with a file icon and a 'Customize URL' checkbox). A 'REGISTER' button is at the bottom. A footer link says 'Contact NetApp Support at <http://mysupport.netapp.com>'.

3. vCenter Plug-inがすでに登録されているかどうか、および現在のインストールのバージョン番号を確認するには、**[Registration Status]**をクリックし、必要なフィールドに入力して**[Check Status]**をクリックします。
4. **[Update Plug-in]**をクリックします。
5. 次の情報を確認し、必要に応じて更新します。
 - 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。
 - vCenter Administratorのユーザ名。
注: 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。
 - vCenter Administratorのパスワード。
 - (社内サーバ / ダーク サイトの場合) プラグインのZIPのカスタムURL。
注: ほとんどのインストールではデフォルトのパスが使用されます。HTTPサーバまたはHTTPSサーバ (ダーク サイト) を使用する場合や、ZIPファイルの名前またはネットワーク設定を変更した場合は、**[Custom URL]**をクリックして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プラグインのドキュメントを参照してください。
6. **[Update]**をクリックします。
7. vCenter Plug-in 3.0以前の場合、次の手順を実行します。
 - a. **serenity**フォルダとその内容をすべて削除します。Windows vCenter Server 6.xの場合、このフォルダのパスは次のとおりです。C:\ProgramData\VMware\vCenterServer\data\vSphere Web Client\SerenityDB\serenity
 - b. 削除した内容をごみ箱から完全に消去します。
 - c. vCenterをリブートします。
8. vSphere Web ClientにvCenter Administratorとしてログインします。
注: この操作でvSphere Web Clientでのインストールが完了します。vCenter Plug-inのアイコンがvSphereのメイン ページに表示されない場合は、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を参照してください。
9. **NetApp Element Configuration**拡張ポイントの**[About]**タブでバージョンの変更を確認します。
注: 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。

関連タスク

[vCenter Plug-inのアップグレード](#) (15ページ)

[管理ノードのインストール](#) (19ページ)

[社内 \(ダーク サイト\) のHTTPサーバ用のvCenterプロパティの変更](#) (26ページ)

関連資料

[プラグインの登録は成功するがWeb Clientにアイコンが表示されない](#) (193ページ)

管理サービスの更新

管理ノード11.3以降をインストールしたあと、管理サービスを最新バージョンに更新できます。管理ノード11.3以降では、プラグインのQoSSIOCサービスをElementソフトウェアリリースとは別に更新できます。

手順

1. 次のいずれかの管理サービス更新オプションを選択します。
 - Hybrid Cloud Control (HCC) から管理サービスを更新する：
[NetApp Hybrid Cloud Controlを使用した管理サービスのアップグレード](#)
 - 管理ノードAPIを使用して管理サービスを更新する：
[mNode APIを使用した管理サービスの更新](#)

NetApp Hybrid Cloud Controlを使用した管理サービスのアップグレード

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や修正を提供します。

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2.1.326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。

タスク概要

各バージョンのサービス バンドルで利用できるサービスについては、[管理サービスのリリース ノート](#)を参照してください。

手順

1. Webブラウザを開き、管理ノードのIPアドレスにアクセスします。

`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]をクリックします。
4. [Upgrades]ページで、[Management Services]タブを選択します。
[Management Services]タブには、管理サービス ソフトウェアの現在のバージョンと使用可能なバージョンが表示されます。

注：インターネットにアクセスできない環境では、現在のソフトウェア バージョンのみ表示されます。
5. 次のいずれかを実行します。

オプション	説明
インターネットにアクセスできる環境	管理サービスのアップグレードを利用できる場合は、 [Begin Upgrade] をクリックします。
インターネットにアクセスできない環境	- 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。 [Browse]をクリックして保存したパッケージを選択し、アップロードします。

アップグレードが開始され、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。

関連情報

[管理サービス リリース ノート](#)

mNode APIを使用した管理サービスの更新

管理サービスの更新は、NetApp Hybrid Cloud Controlのページから実行することを推奨します。または、管理ノードからREST API UIを使用して手動で更新することもできます。管理サービスの更新プログラムは、オンラインのソフトウェアリポジトリからサービスバンドルとして入手できます。

開始する前に

- インターネットへのアクセスが必要です。
- 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。
- 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。

タスク概要

ここでは、管理ノードAPIを使用して手動で管理サービスを更新する手順を説明します。管理サービスには、Element Plug-in for vCenterのSIOCサービス、Active IQコレクタ サービス、NetApp HCI監視サービス（NetApp HCI環境のみ）、およびその他のサービスが含まれます。管理ノードのサービスベースではないコンポーネントの更新は、更新イメージ（OVAまたはISO）として提供され、この手順を使用して更新することはできません。

手順

- 管理ノードでREST API UIを開きます。https://[management node IP]/mnode
- [Authorize]**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。
 - トークンのURL文字列をコピーし、別のブラウザ タブに貼り付けてトークン要求を開始します。
 - [Authorize]**をクリックしてセッションを開始します。
- （オプション）管理ノード サービスの使用可能なバージョンを確認します。GET /services/versions
- （オプション）最新バージョンに関する詳細情報を取得します。GET /services/versions/latest

5. (オプション) 特定のバージョンに関する詳細情報を取得します。GET /services/versions/{version}/info
6. 次のいずれかの管理サービス更新オプションを実行します。

オプション	説明
PUT /services/update/latest	このコマンドは、管理ノード サービスの最新バージョンに更新する場合に実行します。
PUT /services/update/{version}	このコマンドは、管理ノード サービスの特定のバージョンに更新する場合に実行します。

7. GET/services/update/statusを使用して更新のステータスを監視します。
更新が完了すると、次の例のような結果が返されます。

```
{
  "current_version": "2.1.346",
  "details": "Updated to version 2.1.346",
  "status": "success"
}
```

関連タスク

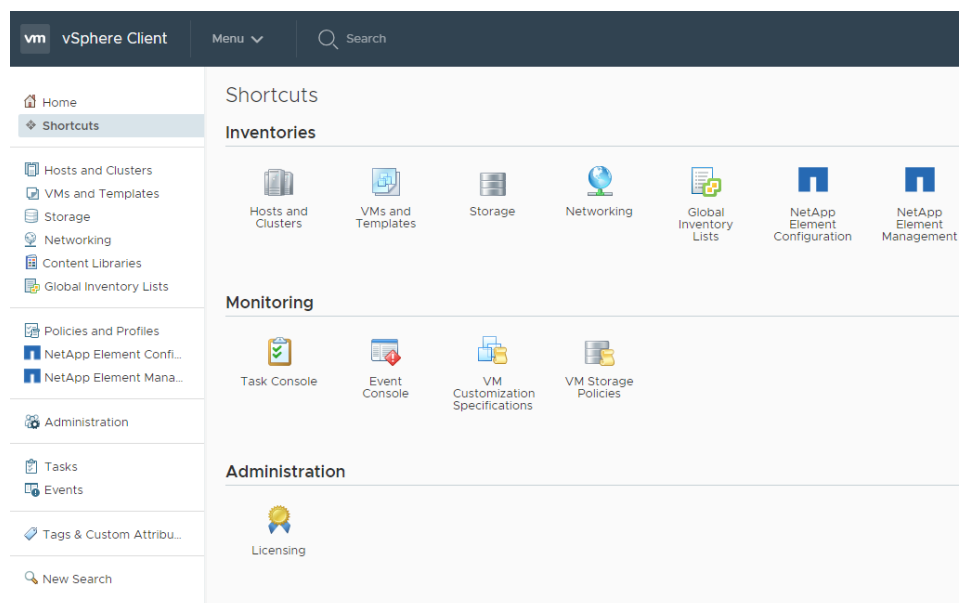
[NetApp Hybrid Cloud Controlを使用した管理サービスのアップグレード](#) (45ページ)

関連情報

[管理サービス リリース ノート](#)

インストールしたプラグインへのアクセス

インストールが完了すると、vSphere Web Clientの[Shortcuts]タブおよびサイド パネルに、NetApp Element Configuration拡張ポイントとNetApp Element Management拡張ポイントが表示されます。



注: vCenter Plug-inのアイコンが表示されない場合は、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を参照してください。

関連タスク

[vCenter Plug-inのアップグレード](#) (15ページ)

[NetApp Element Plug-in for vCenter Serverのインストール](#) (15ページ)

関連資料

[プラグインの登録は成功するが Web Clientにアイコンが表示されない](#) (193ページ)

NetApp Element Plug-in for vCenter Serverの使用 方法

NetApp Element Plug-in for vCenter Serverを使用すると、VMware vSphere Web Client内でNetApp Elementクラスタを設定、管理、監視することができます。Configuration拡張ポイントとManagement拡張ポイントを使用して、クラスタ全体に対する変更を行うことができます。

NetApp Element Configuration拡張ポイントでは、クラスタの追加と管理、リンクモードのvCenter Serverの割り当て、管理ノードのQoSSIOCの設定を行うことができます。NetApp Element Management拡張ポイントでは、Element UIと同等の監視および管理インターフェイスを通じて、ストレージシステムをクラスタ単位で一元管理できます。

関連資料

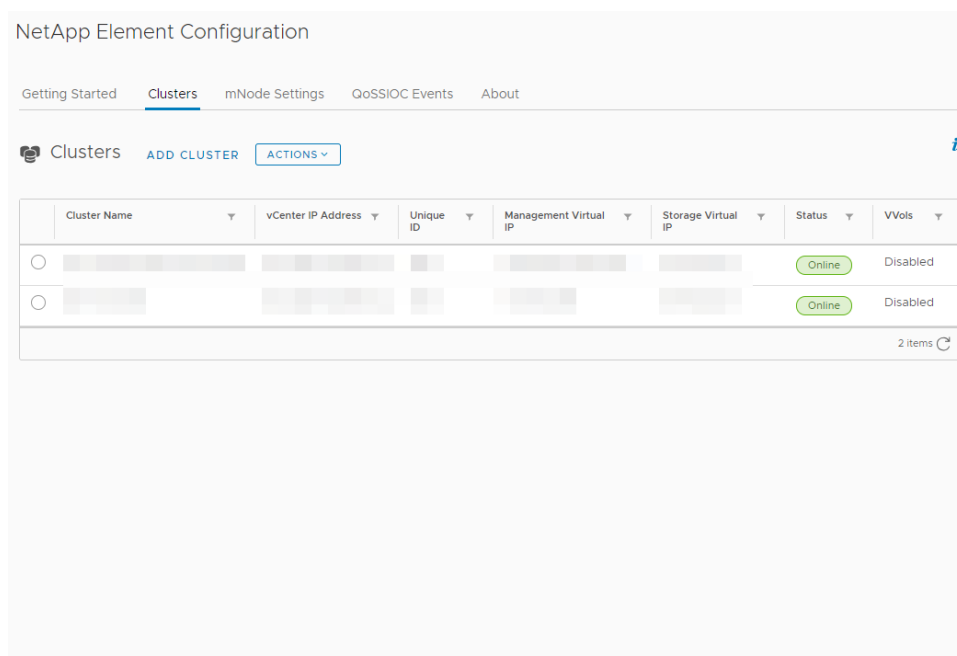
[NetApp Element Configuration拡張ポイント](#) (49ページ)

[NetApp Element Management拡張ポイント](#) (50ページ)

NetApp Element Configuration拡張ポイント

NetApp Element Configuration拡張ポイントでは、クラスタの追加と管理、リンクモードのvCenter Serverの割り当て、管理ノードのQoSSIOCの設定を行うことができます。

注: インストールされているvSphereのバージョンによっては、vSphere Web Clientの画面は以降のスクリーンショットと多少異なる場合があります。



NetApp Element Configuration拡張ポイントからは以下のタブを使用できます。

Getting Started

プラグインの拡張ポイントと実行できる操作の説明が表示されます。[Getting Started] ページはページ単位で非表示にでき、また NetApp Element Configuration 拡張ポイントの [About] タブで元に戻すことができます。

Clusters

プラグインで制御されている NetApp Element クラスタを管理します。クラスタ固有の機能を有効化、無効化、または設定することもできます。

mNode Settings

QoSSIOC サービスの管理ノードの設定を行います。

QoSSIOC Events

検出されたすべての QoSSIOC イベントに関する情報が表示されます。

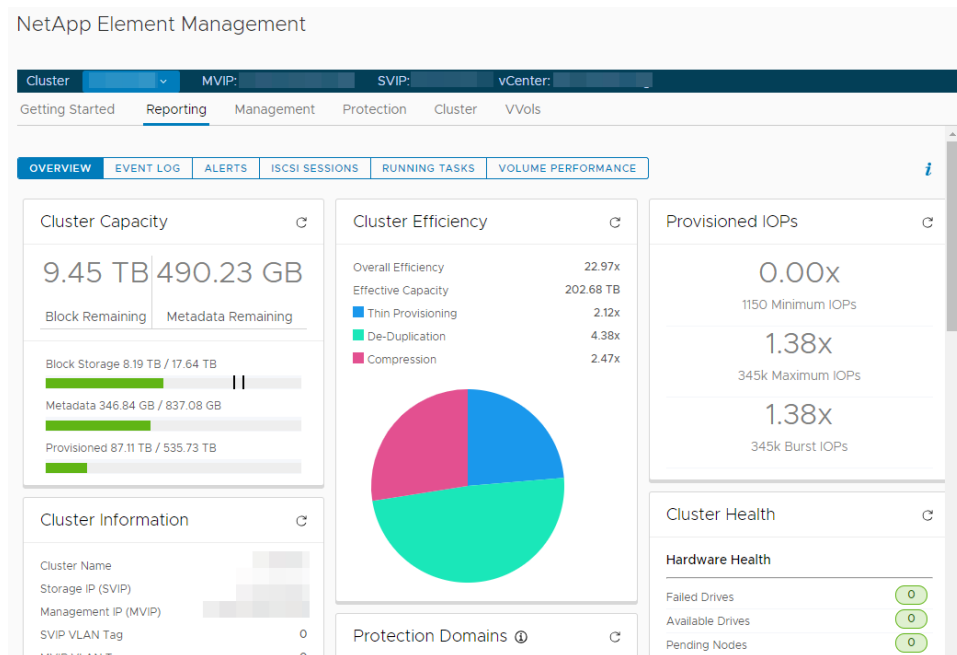
About

プラグインのバージョン情報が表示されます。サービスバンドルをダウンロードするオプションもあります。

NetApp Element Management 拡張ポイント

NetApp Element Management 拡張ポイントでは、Element UI と同等の監視および管理インターフェイスを通じて、ストレージシステムをクラスタ単位で一元管理できます。

注: インストールされている vSphere のバージョンによっては、vSphere Web Client の画面は以降のスクリーンショットと多少異なる場合があります。



クラスタナビゲーションバーでは、プラグインに追加されたクラスタ間をすばやく切り替えることができます。

Cluster

複数のクラスタが追加されている場合は、管理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。ドロップダウンリストから追加されたその他のクラスタを選択できます。

MVIP

選択したクラスタの管理仮想IPアドレス。

SVIP

選択したクラスタのストレージ仮想IPアドレス。

vCenter

選択したクラスタがアクセスできるvCenter Server。プラグインに追加されたクラスタには、vCenter Serverへのアクセスが割り当てられています。

NetApp Element Management拡張ポイントからは以下のタブを使用できます。

Getting Started

プラグインの拡張ポイントと実行できる操作の説明が表示されます。[Getting Started]ページはページ単位で非表示にでき、またNetApp Element Configuration拡張ポイントの[About]タブで元に戻すことができます。

Reporting

クラスタのコンポーネントに関する情報とクラスタのパフォーマンスの概要が表示されます。イベント、アラート、iSCSIセッション、実行中のタスク、およびボリュームのパフォーマンスに関する情報を検索することもできます。

Management

データストア、ボリューム、ユーザアカウント、アクセスグループ、およびインシエータを作成および管理します。バックアップ処理、クローニング、Snapshotを実行することもできます。NetApp Elementソフトウェア10以降を使用している場合は、QoSポリシーの作成と管理も可能です。

Protection

個々のSnapshotとグループSnapshotを管理します。Snapshotの作成スケジュールの設定、リアルタイムレプリケーションのためのクラスタのペアリング、ボリュームペアの管理も可能です。

Cluster

ドライブとノードを追加および管理します。VLANの作成と管理も可能です。

VVols

仮想ボリュームおよび仮想ボリュームに関連付けられたストレージコンテナ、プロトコルエンドポイント、およびバインドを管理します。

vCenterリンク モード

NetApp Element Plug-in for vCenter Serverでは、vCenterリンク モードを使用して他のvCenter Serverのクラスタ リソースを管理することができます。リンク モード グループに属するいずれかのvCenter Serverにログインし、リンクされた他のvCenter Serverが所有するリソースを同じ画面から管理できます。

プラグインを使用するリンク モード環境内の各vCenter Serverにプラグインを登録する必要があります。プラグインの登録ユーティリティを使用して、各vCenter Serverへの登録を完了してください。さらに、リンクされたそれぞれのvCenter ServerのvSphere Web Clientに一度ログインする必要があります。ログインすると、Web Clientにプラグインがインストールされます。

ベストプラクティス: [Add Cluster]設定プロセスでクラスタに関連付けたvCenter Serverからクラスタを管理します。

Elementソフトウェアベースのストレージを使用するホストは特定のvCenter Server専用であり、リンク モード グループのメンバー間では共有されません。そのため、クラスタのストレージ管理タスクはvCenter Server内で使用可能なホストに限定されます。

関連タスク

[クラスタの追加](#) (54ページ)

複数クラスタを管理する場合のオブジェクト名のベストプラクティス

クラスタ コンポーネントを簡単に識別できるように、NetApp Element Plug-in for vCenter Serverに関連するすべてのオブジェクトに一貫したわかりやすい命名規則を使用する必要があります。これは、特にvCenter Serverやクラスタを複数使用する環境において重要となります。

わかりやすい命名規則を使用しないと、複数のクラスタを管理する際に混乱が生じるおそれがあります。たとえば、インベントリにSF-cluster1とSF-cluster2がある場合は、アカウント、ボリューム、データストアにも同様のパターンで名前を付ける必要があります（SF1-account1、SF2-vol1など）。一貫した命名規則を使用すれば、**NetApp Element Management** 拡張ポイントのクラスタ ナビゲーション バーを調べなくても、作業中のクラスタを容易に識別できます。また、Elementソフトウェアベースのボリュームに関連付けられたデータストアなど、Elementソフトウェアベースのストレージ オブジェクトのバックアップ オブジェクトとして機能するvSphere内のオブジェクトを誤って変更する可能性も少なくなります。

クラスタ設定

NetApp Element Configuration拡張ポイントの[Clusters]タブでは、クラスタを追加することができます。追加したクラスタはNetApp Element Management拡張ポイントで管理できます。既存のクラスタ プロファイルを管理したり、Virtual Volumes (VVol) 機能をサポートされるクラスタで有効にしたり、クラスタをシャットダウンしてオフラインに切り替えたりすることもできます。

クラスタの追加

NetApp Element Configuration拡張ポイントを使用して、Elementソフトウェアを実行するクラスタを追加できます。クラスタへの接続が確立されると、そのクラスタをNetApp Element Management拡張ポイントを使用して管理できるようになります。

開始する前に

- IPアドレスまたはFQDNがわかっている使用可能な状態のクラスタが少なくとも1つ必要です。
- クラスタに対するフル権限を持つ現在のクラスタ管理者のユーザ クレデンシャルが必要です。
- ファイアウォール ルールで、TCPポート443および8443でvCenterとクラスタMVIP間のオープン ネットワーク通信を許可します。

注：NetApp Element Management拡張ポイントの機能を使用するには、クラスタが少なくとも1つ追加されている必要があります。

タスク概要

ここでは、クラスタ プロファイルを追加してクラスタをプラグインで管理できるようにする方法について説明します。プラグインを使用してクラスタ管理者のクレデンシャルを変更することはできません。クラスタ管理者アカウントのクレデンシャルを変更する手順については、『*NetApp Element*ソフトウェア ユーザ ガイド』を参照してください。

注意：vSphere HTML5 Web ClientとFlash Web Clientは別々のデータベースを使用しており、両データベースを統合することはできません。一方のクライアントに追加したクラスタは、もう一方のクライアントで認識されません。両方のクライアントを使用する場合は、両方にクラスタを追加してください。

手順

1. [NetApp Element Configuration] > [Clusters]を選択します。
2. [Add Cluster]をクリックします。
3. [Add Cluster]ダイアログ ボックスで、次の情報を入力します。
 - **IP address/FQDN：**クラスタのMVIPアドレスを入力します。
 - **User ID：**クラスタ管理者のユーザ名を入力します。
 - **Password：**クラスタ管理者のパスワードを入力します。

- **vCenter Server** : リンク モード グループを設定している場合、クラスタにアクセスするvCenter Serverを選択します。リンク モードを使用していない場合は、現在のvCenter Serverがデフォルトで選択されます。

注 : クラスタではvCenter Serverごとに専用のホストを使用します。選択したvCenter Serverから目的のホストにアクセスできることを確認してください。使用するホストをあとで変更する場合は、クラスタを削除し、別のvCenter Serverに再割り当てして再度追加します。

4. [OK]をクリックします。

処理が完了すると、クラスタが使用可能なクラスタのリストに表示され、NetApp Element Management拡張ポイントで使用できるようになります。

クラスタの詳細の表示

使用可能な各クラスタの詳細をまとめた概要情報を確認できます。

手順

1. [NetApp Element Configuration] > [Clusters]を選択します。
2. 確認するクラスタ プロファイルのチェック ボックスを選択します。
3. [Actions]をクリックします。
4. 表示されたメニューで[Details]を選択します。

クラスタの詳細

NetApp Element Configuration拡張ポイントの[Clusters]ページで、プラグインに追加されているすべてのクラスタに関する情報を確認できます。

Cluster Name

クラスタの名前。

vCenter IP Address

クラスタが割り当てられているvCenter ServerのIPアドレスまたはFQDN。

Unique ID

クラスタの一意的ID。

Management Virtual IP

管理仮想IPアドレス (MVIP)。

Storage Virtual IP

ストレージ仮想IPアドレス (SVIP)。

Status

クラスタのステータス。

VVols

クラスタのVVOL機能のステータス。

個々のクラスタの詳細

NetApp Element Configuration 拡張ポイントの[Clusters]ページでは、個々のクラスタを選択してその詳細を表示し、クラスタの詳細情報を確認できます。

Cluster Name

クラスタの名前。

Unique ID

クラスタの一意のID。

vCenter IP Address

クラスタが割り当てられているvCenter ServerのIPアドレスまたはFQDN。

Management Virtual IP

管理仮想IPアドレス（MVIP）。

MVIP Node ID

マスターMVIPアドレスを保持するノード。

Storage Virtual IP

ストレージ仮想IPアドレス（SVIP）。

SVIP Node ID

マスターSVIPアドレスを保持するノード。

Element Version

クラスタで実行されているNetApp Elementソフトウェアのバージョン。

VASA 2 Status

Elementクラスタ上のVASA Providerのステータス。

VASA Provider URL

Elementクラスタで有効になっているVASA ProviderのURL（該当する場合）。

Encryption At Rest Status

保存データの暗号化（Encryption At Rest）機能の状態。

有効な値は次のとおりです。

- Enabling：保存データの暗号化を有効にしています。
- Enabled：保存データの暗号化は有効です。
- Disabling：保存データの暗号化を無効にしています。
- Disabled：保存データの暗号化は無効です。

Ensemble Nodes

データベース アンサンブルに参加しているノードのIP。

Paired With

ローカル クラスタとペアリングされているその他のクラスタの名前。

SSH Status

Secure Shell（SSH）のステータス。有効な場合は残り時間が表示されます。

クラスタ プロファイルの編集

NetApp Element Configuration拡張ポイントを使用して、クラスタ プロファイルのクラスタ管理者のユーザ名とパスワードを変更できます。

タスク概要

ここでは、プラグインで使用するクラスタ管理者のユーザ名とパスワードを変更する方法について説明します。プラグインからクラスタ管理者のクレデンシャルを変更することはできません。クラスタ管理者アカウントのクレデンシャルを変更する手順については、『*NetApp Element*ソフトウェア ユーザ ガイド』を参照してください。

手順

1. [NetApp Element Configuration] > [Clusters]を選択します。
2. 編集するクラスタ プロファイルのチェック ボックスを選択します。
3. [Actions]をクリックします。
4. 表示されたメニューで[Edit]をクリックします。
5. [Edit Cluster]ダイアログ ボックスで、次の情報を必要に応じて編集します。
 - **User ID** : 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。

注 : クラスタ プロファイルのIPアドレスまたはFQDNは、クラスタの追加後は変更できません。また、割り当てられているリンク モードのvCenter Serverも追加済みのクラスタについては変更できません。クラスタのアドレスや関連付けられているvCenter Serverを変更する場合は、クラスタを削除して追加し直す必要があります。

6. [OK]をクリックします。

クラスタ プロファイルの削除

NetApp Element Configuration拡張ポイントを使用して、vCenter Plug-inでの管理対象から除外するクラスタのクラスタ プロファイルを削除できます。

タスク概要

リンク モード グループを設定している場合にクラスタを別のvCenter Serverに再割り当てするには、クラスタ プロファイルを削除してから、リンクされている別のvCenter ServerのIPで再度追加します。

手順

1. [NetApp Element Configuration] > [Clusters]を選択します。
2. 削除するクラスタ プロファイルのチェック ボックスを選択します。
3. [Actions]をクリックします。
4. 表示されたメニューで[Remove]をクリックします。
5. 操作を確定します。

Virtual Volumesの有効化

NetApp Element Configuration拡張ポイントを使用して、vSphere Virtual Volumes (VVol) 機能を手動で有効にする必要があります。ElementシステムのVVol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。VVol機能の有効化は1度だけ実行します。

開始する前に

- ElementクラスタがVVolに対応したESXi 6.0以降の環境に接続されている必要があります。
- Element 11.3以降を使用している場合は、クラスタをESXi 6.0 Update 3以降の環境に接続する必要があります。

手順

1. [NetApp Element Configuration] > [Clusters]を選択します。
2. 有効にするクラスタをリストから選択します。
3. [Actions]をクリックします。
4. 表示されたメニューで[Enable VVols]をクリックします。

注意：有効にしたVVol機能をあとから無効にすることはできません。vSphere Virtual Volumes機能を有効にすると、NetApp Elementソフトウェアの設定が永続的に変更されます。クラスタがVMware ESXi VVolに対応した環境に接続されている場合にのみ、VVol機能を有効にしてください。VVol機能を無効にしてデフォルト設定に戻すには、クラスタを工場出荷時のイメージに戻す必要があります。

5. [Yes]をクリックして、Virtual Volumes設定の変更を確定します。

注：VVol機能を有効にすると、ElementクラスタはVASA Providerを起動してVASAトラフィック用のポート8444を開き、vCenterおよびすべてのESXiホストから検出可能なプロトコルエンドポイントを作成します。

6. 選択したクラスタの[Actions]をクリックします。
7. 表示されたメニューで[Details]を選択します。
8. [VASA Provider URL]フィールドからVASA ProviderのURLをコピーします。このURLは、VASA ProviderをvCenterに登録する際に使用します。

注：vSphere Virtual Volumes機能に必要なその他の設定タスクについては、プラグインのドキュメントを参照してください。

関連タスク

[vSphere Virtual Volumes \(VVol\) 機能の設定](#) (174ページ)

保存データの暗号化の有効化

NetApp Element Configuration拡張ポイントを使用して、Encryption At Rest（EAR;保存データの暗号化）機能を手動で有効にすることができます。

手順

1. **[NetApp Element Configuration] > [Clusters]**を選択します。
2. 保存データの暗号化を有効にするクラスタを選択します。
3. **[Actions]**をクリックします。
4. 表示されたメニューで**[Enable EAR]**をクリックします。
5. 操作を確定します。

保存データの暗号化の無効化

NetApp Element Configuration拡張ポイントを使用して、保存データの暗号化（EAR）機能を手動で無効にすることができます。

手順

1. **[NetApp Element Configuration] > [Clusters]**を選択します。
2. 保存データの暗号化を無効にするクラスタのチェックボックスを選択します。
3. **[Actions]**をクリックします。
4. 表示されたメニューで**[Disable EAR]**をクリックします。
5. 操作を確定します。

SSHの有効化

NetApp Element Configuration拡張ポイントを使用して、Secure Shell（SSH）セッションを手動で有効にすることができます。SSHを有効にすると、ネットアップのテクニカル サポート エンジニアが指定された期間にストレージ ノードにアクセスしてトラブルシューティングを行うことができます。

手順

1. **[NetApp Element Configuration] > [Clusters]**を選択します。
2. SSHセッションを有効にするクラスタを選択します。
3. **[Actions]**をクリックします。
4. 表示されたメニューで**[Enable SSH]**をクリックします。
5. SSHセッションを有効にする期間（時間）を入力します。最大値は720です。処理を続行するには、値を設定する必要があります。
6. **[Yes]**をクリックします。

SSHの無効化

NetApp Element Configuration拡張ポイントを使用して、ストレージ クラスタ内のノードへの Secure Shell (SSH) アクセスを手動で無効にすることができます。

手順

1. **[NetApp Element Configuration] > [Clusters]**を選択します。
2. SSHアクセスを無効にするクラスタを選択します。
3. **[Actions]**をクリックします。
4. 表示されたメニューで**[Disable SSH]**をクリックします。
5. **[Yes]**をクリックします。

SSHタイム リミットの変更

NetApp Element Configuration拡張ポイントを使用して、アクティブなSecure Shell (SSH) セッションの期間を変更できます。

手順

1. **[NetApp Element Configuration] > [Clusters]**を選択します。
2. 変更するSSHセッションを実行しているクラスタを選択します。
3. **[Actions]**をクリックします。
4. 表示されたメニューで**[Change SSH]**をクリックします。
ダイアログ ボックスにSSHセッションの残り時間が表示されます。
5. SSHセッションの新しい期間 (時間) を入力します。処理を続行するには、値を設定する必要があります。
6. **[Yes]**をクリックします。

保護ドメインの監視設定

NetApp Element Configuration拡張ポイントを使用して、保護ドメインの監視を手動で有効にすることができます。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。

タスク概要

シャーシ ドメインは、シャーシレベルの障害に耐えるためのクラスタの耐障害性を確保します。ノード ドメインは、(場合によってはシャーシをまたいだ) 特定のノード グループの耐障害性を確保します。シャーシ ドメインの耐障害性を確保するためには、ノード ドメインよりも多くの容量リソースが必要です。保護ドメインのしきい値を超えると、データの可用性を中断せずに障害から回復するための十分な容量をクラスタで確保できなくなります。

注: 保護ドメインの監視機能を使用するには、Element 11.0以降のクラスタを選択する必要があります。Element 11.0より前のクラスタでは保護ドメイン機能を使用できません。

手順

1. [NetApp Element Configuration] > [Clusters]を選択します。
2. 保護ドメインの監視を有効にするクラスタを選択します。
3. [Actions]をクリックします。
4. 表示されたメニューで[Set Protection Domain Monitoring]をクリックします。
5. [Set Protection Domain Monitoring]ダイアログで、障害のしきい値を選択します。
 - **Node** : ノード レベルのハードウェア障害が発生するとクラスタが中断なくデータを提供できなくなるしきい値。ノードしきい値はシステムのデフォルト設定です。
 - **Chassis** : シャーシ レベルのハードウェア障害が発生するとクラスタが中断なくデータを提供できなくなるしきい値。
6. [OK]をクリックします。

クラスタのシャットダウン

NetApp Element Configuration拡張ポイントを使用して、ストレージ クラスタ内のすべてのアクティブ ノードを手動でシャットダウンできます。

開始する前に

I/Oを停止し、すべてのiSCSIセッションを切断しておきます。

注 : クラスタをシャットダウンするのではなく再起動する場合は、NetApp Element Management拡張ポイントの[Cluster]ページからすべてのノードを選択して再起動を実行できます。

手順

1. [NetApp Element Configuration] > [Clusters]を選択します。
2. シャットダウンするクラスタのチェック ボックスを選択します。
3. [Actions]をクリックします。
4. 表示されたメニューで[Shutdown]をクリックします。
5. 操作を確定します。

関連タスク

[クラスタ ノードのシャットダウン](#) (170ページ)

[クラスタ ノードの再起動](#) (169ページ)

関連情報

[Powering off and powering on a NetApp HCI system](#)

NetApp HCIの拡張

NetApp HCIを使用してノードを追加することにより、NetApp HCIインフラストラクチャを手動で拡張できます。システムを拡張するためのNetApp HCI UIへのリンクには、NetApp

Element拡張ポイントからアクセスできます。リンクにはNetApp Element Management拡張ポイントの[Getting Started]ページと[Cluster]ページからもアクセスできます。

手順

1. [NetApp Element Configuration] > [Clusters]を選択します。
2. 変更するクラスタを選択します。
3. [Actions]をクリックします。
4. 表示されたメニューで[Expand your NetApp HCI]をクリックします。

管理ノード（mNode）の設定

NetApp Element Configuration拡張ポイントの[mNode Settings]タブでは、QoSSIOCサービスに使用する設定を指定できます。有効な管理ノードを設定した時点でこれらの設定がデフォルトになります。設定を編集してクレデンシャルを更新したり、新しい管理ノード用に設定をクリアしたりできます。

リンク モードの場合は、NetApp Element Plug-in for vCenter Serverで登録するすべてのvCenter Serverに、1つのvCenter Serverで指定した管理ノード設定が使用されます。

設定ページの[mNode Status]フィールドには次のいずれかの値が表示されます。

- Up : QoSSIOCは有効です。
- Down : QoSSIOCは無効です。
- Not Configured : QoSSIOCは未設定です。
- Network Down : vCenterがネットワーク上のQoSSIOCサービスと通信できません。mNodeとSIOCサービスはまだ実行されている可能性があります。

関連タスク

[vSphere Virtual Volumes \(VVol\) 機能の設定](#) (174ページ)

QoSSIOCの管理ノードの設定

NetApp Element Configuration拡張ポイントを使用して、Element管理ノード（mNode）を設定できます。QoSSIOCサービスを有効にして使用するには、この設定が必要です。

手順

1. [NetApp Element Configuration] > [mNode Settings]を選択します。
2. [Actions]をクリックします。
3. 表示されたメニューで[Configure]を選択します。
4. [Configure mNode Settings]ダイアログ ボックスで、次の情報を入力します。
 - **mNode IP Address/FQDN** : QoSSIOCサービスが含まれているクラスタの管理ノードのIPアドレスです。
 - **mNode Port** : QoSSIOCサービスが含まれている管理ノードのポート アドレスです。デフォルト ポートは8443です。
 - **mNode User ID** : QoSSIOCサービスのユーザIDです。QoSSIOCサービスのデフォルトのユーザIDは`admin`です。NetApp HCIの場合、NetApp Deployment Engineを使用したインストールで入力されるユーザIDと同じです。
 - **mNode Password** : Element QoSSIOCサービスのパスワードです。QoSSIOCサービスのデフォルトのパスワードは`solidfire`です。カスタム パスワードを作成していない場合は、登録画面 (`https://[management node IP]:9443`) からパスワードを作成できます。
 - **vCenter User ID** : Administratorロールのすべての権限を持つvCenter管理者のユーザIDです。

- **vCenter Password** : Administratorロールのすべての権限を持つvCenter管理者のパスワードです。

5. **[OK]**をクリックします。

プラグインからサービスへの通信が確立されると、**[mNode Status]**フィールドに「UP」と表示されます。

注 : 有効な管理ノードを設定した時点でこれらの設定がデフォルトになります。別の有効な管理ノードを設定しないかぎり、最後に指定した有効なmNode設定に戻ります。新しい管理ノードのクレデンシャルを設定する場合は、先に既存の管理ノードの設定をクリアする必要があります。

関連情報

技術情報アーティクル : [vCenter Plugin \(VCP\) mnode settings credentials are no longer valid after management node redeployment or VCP re-registration on an HCI cluster](#)

QoSSIOCの管理ノード設定の編集

NetApp Element Configuration拡張ポイントを使用して、アクティブなElement管理ノード (mNode) のmNodeとvCenterのクレデンシャルを変更できます。

手順

1. **[NetApp Element Configuration] > [mNode Settings]**を選択します。
2. **[Actions]**をクリックします。
3. 表示されたメニューで**[Edit]**を選択します。
4. **[Edit mNode Settings]**ダイアログ ボックスで、次の情報を必要に応じて編集します。
 - **mNode User ID** : QoSSIOCサービスのユーザIDです。QoSSIOCサービスのデフォルトのユーザIDは`admin`です。NetApp HCIの場合、NetApp Deployment Engineを使用したインストールで入力されるユーザIDと同じです。
 - **mNode Password** : Element QoSSIOCサービスのパスワードです。QoSSIOCサービスのデフォルトのパスワードは`solidfire`です。カスタム パスワードを作成していない場合は、登録画面 ([https://\[management node IP\]:9443](https://[management node IP]:9443)) からパスワードを作成できます。
 - **vCenter User ID** : Administratorロールのすべての権限を持つvCenter管理者のユーザIDです。
 - **vCenter Password** : Administratorロールのすべての権限を持つvCenter管理者のパスワードです。

5. **[OK]**をクリックします。

プラグインからサービスへの通信が確立されると、**[mNode Status]**フィールドに「UP」と表示されます。

注 : 有効な管理ノードを設定した時点でこれらの設定がデフォルトになります。別の有効な管理ノードを設定しないかぎり、最後に指定した有効なmNode設定に戻ります。新しい管理ノードのクレデンシャルを設定する場合は、先に既存の管理ノードの設定をクリアする必要があります。

QoSSIOCの管理ノード設定のクリア

NetApp Element Configuration拡張ポイントを使用して、Element管理ノード (mNode) の各種設定をクリアできます。新しい管理ノードのクレデンシャルを設定するには、先に既存の管理ノードの設定をクリアする必要があります。mNode設定をクリアすると、vCenter、クラスタ、およびデータストアからアクティブなQoSSIOCが削除されます。

手順

1. [NetApp Element Configuration] > [mNode Settings]を選択します。
2. [Actions]をクリックします。
3. 表示されたメニューで[Clear]を選択します。
4. 操作を確定します。

プロセスが完了すると、[mNode Status]フィールドに「Not Configured」と表示されます。

関連タスク

[QoSSIOCサービスのパスワードの変更](#) (65ページ)

QoSSIOCサービスのパスワードの変更

管理ノードの登録画面を使用して、QoSSIOCサービスのパスワードを変更できます。

開始する前に

- NetApp Element Configuration拡張ポイントを使用して、Element管理ノード (mNode) の各種設定をクリアしておきます。
注: 新しい管理ノードのクレデンシャルを設定するには、先に既存の管理ノードの設定をクリアする必要があります。mNode設定をクリアすると、vCenter、クラスタ、およびデータストアからアクティブなQoSSIOCが削除されます。
- 管理ノードの電源をオンにしておきます。

タスク概要

ここでは、QoSSIOCパスワードのみを変更する方法について説明します。QoSSIOCのユーザー名を変更する場合は、NetApp Element Configuration拡張ポイントの[mNode Settings]ページから変更できます。

手順

1. 登録用TCPポートを含む管理ノードのIPアドレスをブラウザに入力します (https://[management node IP]:9443)。

プラグインの[Manage QoSSIOC Service Credentials]ページが表示されます。

2. 次の情報を入力します。

- **Old Password** : QoSSIOCサービスの現在のパスワード。パスワードをまだ割り当てていない場合は、デフォルトのパスワードを入力します。

solidfire

- **New Password** : QoSSIOCサービスの新しいパスワード。
- **Confirm Password** : 新しいパスワードをもう一度入力します。

3. [Submit Changes]をクリックします。

注 : 変更を送信すると、QoSSIOCサービスが自動的に再起動されます。

4. vSphere Web Clientで、[NetApp Element Configuration] > [mNode Settings]を選択します。

5. [Actions]をクリックします。

6. 表示されたメニューで[Configure]を選択します。

7. [Configure mNode Settings]ダイアログの[mNode Password]フィールドに新しいパスワードを入力します。

8. [OK]をクリックします。

プラグインからサービスへの通信が確立されると、[mNode Status]フィールドに「UP」と表示されます。

関連タスク

[QoSSIOCの管理ノード設定のクリア](#) (65ページ)

[QoSSIOCの管理ノード設定の編集](#) (64ページ)

QoSSIOCイベントの表示

QoSSIOCイベントは、NetApp Element Configuration拡張ポイントで確認できます。QoSSIOCイベントは、QoSが有効なデータストアがあるVMが再設定された場合、または電源イベントやゲストイベントが発生すると報告されます。

開始する前に

- クラスタが少なくとも1つ追加および実行されている必要があります。
- プラグインの[**mNode Settings**]ページを使用して、QoSSIOCサービスを設定し、実行する必要があります。
- 少なくとも1つのデータストアでQoSSIOC自動化が有効になっている必要があります。

タスク概要

QoSSIOCイベントは、ローカルに追加されたクラスタから表示されます。リンクモード環境では、クラスタがローカルに追加されているvSphere Web Clientにログインして、そのクラスタのQoSSIOCイベントを表示します。

手順

1. [NetApp Element Configuration] > [QoSSIOC Events]を選択します。
[QoSSIOC Events]ページにイベントの一覧が表示されます。

関連タスク

[QoSSIOCの管理ノードの設定](#) (63ページ)

[QoSSIOC自動化の有効化](#) (98ページ)

QoSSIOCイベントの詳細

NetApp Element Configuration拡張ポイントの[QoSSIOC Events]ページで、各クラスタのQoSSIOCイベントに関する情報を確認できます。

Date

QoSSIOCイベントの日時。

Datastore Name

ユーザが定義したデータストア名。

Cluster IP

イベントの発生元であるデータストアが含まれているクラスタのIPアドレス。

Volume ID

システムによって生成された関連するボリュームのID。

Min IOPs

ボリュームのQoS設定 - 現在の最小IOPS。

Max IOPs

ボリュームのQoS設定 - 現在の最大IOPS。

Burst IOPs

ボリュームのQoS設定 - 現在のバーストIOPS。

Burst Time

バーストが許可される期間。

プラグインの製品情報

NetApp Element vCenter Plug-inのバージョン、ビルド番号、およびIPアドレスに関する一般的な情報は、NetApp Element Configuration拡張ポイントから確認できます。**[About]**ページには、サービスバンドルをダウンロードするオプションのほか、両方の拡張ポイントから利用できる**[Getting Started]**ページを非表示にしたり再表示したりするオプションがあります。

レポート作成

[Reporting]タブには、クラスタのコンポーネントに関する情報とクラスタの利用状況の概要が表示されます。[Reporting]ページを開くと、クラスタのコンポーネントとリソースの概要が表示されます。

レポート概要

NetApp Element Management拡張ポイントの[Reporting]タブにある[Overview]ページでは、クラスタ全体の容量、効率、パフォーマンスなど、選択したクラスタの概要情報を確認できます。

Cluster Capacity

ブロックストレージ、メタデータ、およびプロビジョニング スペース用の残りの容量。しきい値情報を確認するには、進捗状況バーの上にポインタを移動してください。

Cluster Information

クラスタに固有の情報。クラスタの名前、クラスタで実行されているNetApp Elementソフトウェアのバージョン、MVIPアドレスとSVIPアドレス、クラスタのノード、4k IOPS、ボリューム、セッションの数などの情報が含まれます。

- **Cluster Name** : クラスタの名前。
- **Storage IP (SVIP)** : ストレージ仮想IPアドレス (SVIP)。
- **Management IP (MVIP)** : 管理仮想IPアドレス (MVIP)。
- **SVIP VLAN Tag** : マスターSVIPアドレスのVLAN識別子。
- **MVIP VLAN Tag** : マスターMVIPアドレスのVLAN識別子。
- **Node Count** : クラスタ内のアクティブ ノードの数。
- **Cluster 4K IOPS** : クラスタで1秒間に読み取り / 書き込みできる4096 (4K) ブロックの数。
- **Element OS Version** : クラスタで実行されているNetApp Elementソフトウェアのバージョン。
- **Volume Count** : クラスタのボリューム (仮想ボリュームは除く) の総数。
- **Virtual Volume Count** : クラスタの仮想ボリュームの総数。
- **iSCSI Sessions** : クラスタに接続されているiSCSIセッション。
- **Fibre Channel Sessions** : クラスタに接続されているFibre Channelセッション。

Cluster Efficiency

シンプロビジョニング、重複排除、および圧縮を考慮した、システム全体の容量に対する使用率。クラスタでの効率化は、シンプロビジョニング、重複排除、および圧縮を使用しない従来のストレージ デバイスにおける容量使用率と比較して計算されます。

Protection Domains

クラスタの保護ドメイン監視の概要。

- **Selected Monitoring Level** : ユーザが選択した保護ドメインの耐障害性レベル。有効な値は[Chassis]または[Node]です。緑は、クラスタが選択した監視レベルに対応していることを示します。赤は、クラスタが選択した監視レベルに対応しておらず、対処が必要なことを示します。
- **Remaining Block Capacity** : 選択した耐障害性レベルを維持したままで使用可能な残りのブロック容量を示します。
- **Metadata Capacity** : データの可用性を維持したままで障害から回復するための十分なメタデータ容量があるかどうかを示します。[Normal] (緑) は、選択した監視レベルを維持するための十分なメタデータ容量がクラスタにあることを示します。[Full] (赤) は、クラスタが選択した監視レベルに対応しておらず、対処が必要なことを示します。

Provisioned IOPS

クラスタ上のボリュームのIOPSについてのオーバープロビジョニングの状況の概要。[Provisioned IOPS]の値は、クラスタ上のすべてのボリュームのMin IOPS、Max IOPS、およびBurst IOPSのそれぞれを合計し、クラスタのMax IOPSで除算して求められます。

注 : たとえば、クラスタに4つのボリューム（それぞれMin IOPSが500、Max IOPSが15,000、Burst IOPSが15,000）がある場合、Min IOPSの合計は2,000、Max IOPSの合計は60,000、Burst IOPSの合計は60,000になります。クラスタのMax IOPSが50,000の場合、計算は次のようになります。

- Min IOPS : $2000/50000 = 0.04x$
- Max IOPS : $60000/50000 = 1.20x$
- Burst IOPS : $60000/50000 = 1.20x$

1.00xは、プロビジョニングされたIOPSがクラスタのIOPSと同じとなるベースラインです。

Cluster Health

クラスタのハードウェア、容量、およびセキュリティについての健全性。健全性は次のように色分けされます。

- 緑 : 正常
- 黄 : 重大
- 赤 : エラー

Cluster Input/Output

クラスタで実行中のI/O。値は、前回のI/O測定値と現在のI/O測定値から計算されます。グラフに表示される測定値を次に示します。

- **Total** : システムで発生している読み取りと書き込みのIOPSの合計。
- **Read** : 発生している読み取りIOPS。
- **Write** : 発生している書き込みIOPS。

Cluster Throughput

クラスタ上の読み取り、書き込み、および合計の帯域幅アクティビティ。

- **Total** : クラスタの読み取りアクティビティと書き込みアクティビティの合計 (MB/秒)。
- **Read** : クラスタの読み取りアクティビティ (MB/秒)。

- **Write** : クラスタの書き込みアクティビティ (MB/秒)。

Performance Utilization

消費されているクラスタIOPSの割合。たとえば、25万IOPSのクラスタが10万IOPSで実行されている場合、消費率は40%です。

イベント ログの表示

選択したクラスタで実行された処理のイベント ログと、発生する可能性があるクラスタ障害を確認できます。ほとんどのエラーはシステムで自動的に解決されます。システムで解決できないエラーについては、手動での対応が必要になる場合があります。

手順

1. **[NetApp Element Management] > [Reporting]**を選択します。

注 : 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を選択する必要があります。

2. **[Event Log]**をクリックします。

クラスタのすべてのイベントの一覧が表示されます。

3. 確認するイベントを選択します。

4. **[Details]**を選択します。

クラスタ イベントの詳細なメッセージが表示されます。

イベント ログ

NetApp Element Management拡張ポイントの**[Reporting]**タブにある**[Event Log]**ページで、システムで検出されたイベントに関する情報を確認できます。

Event ID

各イベントに関連付けられた一意のID。

Event Type

ログに記録されているイベントのタイプ (APIイベントやクローン イベントなど)。

Message

イベントに関連するメッセージ。

Service ID

イベントを報告したサービスのID (該当する場合)。障害がサービスに関連付けられていない場合、この値は0 (ゼロ) です。

Node

イベントを報告したノードのID (該当する場合)。

Drive ID

イベントを報告したドライブのID (該当する場合)。

Event Time

イベントが発生した日時。

イベントタイプ

システムからは複数のタイプのイベントが報告されます。各イベントは、システムが完了した処理を表しています。イベントには、日常的に発生するイベント、正常なイベント、または管理者による対応が必要なイベントがあります。[Event Log]ページの[Event Type]列は、システムのどの部分でイベントが発生したかを示しています。

注：読み取り専用のAPIコマンドはイベント ログに記録されません。

イベント ログに表示されるイベントのタイプは次のとおりです。

apiEvent

ユーザがAPIまたはWeb UIから開始した、設定を変更するイベント。

binAssignmentsEvent

データ ビンの割り当てに関連するイベント。ビンは簡単に言うとデータを保持するコンテナであり、クラスタ全体にマップされます。

binSyncEvent

ブロック サービス間でのデータの再割り当てに関連するシステム イベント。

bsCheckEvent

ブロック サービス チェックに関連するシステム イベント。

bsKillEvent

ブロック サービスの終了に関連するシステム イベント。

bulkOpEvent

ボリューム全体に対して実行された処理（バックアップ、リストア、Snapshot、クローンなど）に関連するイベント。

cloneEvent

ボリューム クローニングに関連するイベント。

clusterMasterEvent

クラスタの初期化時または設定変更（ノードの追加や削除など）時に発生するイベント。

dataEvent

データの読み取りと書き込みに関連するイベント。

dbEvent

クラスタ内のアンサンブル ノードによって管理されているグローバル データベースに関連するイベント。

driveEvent

ドライブの処理に関連するイベント。

encryptionAtRestEvent

クラスタでの暗号化プロセスに関連するイベント。

ensembleEvent

アンサンブル内のノード数の増減に関連するイベント。

ibreChannelEvent

ノードの設定と接続に関連するイベント。

gcEvent

ブロック ドライブ上のストレージを再利用するために60分ごとに実行されるプロセスに関連するイベント。このプロセスはガベージ コレクションとも呼ばれます。

ieEvent

内部システム エラー。

installEvent

ソフトウェアの自動インストール イベント。保留状態のノードにソフトウェアが自動的にインストールされています。

iSCSIEvent

システムでのiSCSIの問題に関連するイベント。

limitEvent

アカウントまたはクラスタ内で許可されているボリュームまたは仮想ボリュームの最大数に近づいていることを示すイベント。

networkEvent

仮想ネットワークのステータスに関連するイベント。

platformHardwareEvent

ハードウェア デバイスで検出された問題に関連するイベント。

remoteClusterEvent

リモート クラスタ ペアリングに関連するイベント。

schedulerEvent

スケジュールされたSnapshotに関連するイベント。

serviceEvent

システム サービスのステータスに関連するイベント。

sliceEvent

スライス サーバに関連するイベント（メタデータ ドライブまたはボリュームの削除など）。

snmpTrapEvent

SNMPトラップに関連するイベント。

statEvent

システムの統計に関連するイベント。

tsEvent

システム転送サービスに関連するイベント。

unexpectedException

予期しないシステム例外に関連するイベント。

vasaProviderEvent

vSphere APIs for Storage Awareness (VASA) Providerに関連するイベント。

アラート

アラートはクラスタの障害またはエラーであり、発生時に報告されます。アラートには、情報、警告、エラーがあり、クラスタの稼働状況を表すインジケータとして利用できます。ほとんどのエラーは自動的に解決しますが、一部のエラーでは手動での対応が必要です。

NetApp Element Management 拡張ポイントの[Reporting]タブにある[Alerts]ページで、個々のシステム アラートに関する情報を確認できます。

アラートが解決されると、そのアラートに関するすべての情報（解決された日付を含む）が[Resolved]ビューに移動します。

このページに表示される列は次のとおりです。

ID

クラスタ アラートの一意のID。

Severity

- **warning** : 近々対応が必要になる可能性があるが、深刻ではない問題です。システムのアップグレードは引き続き可能です。
- **error** : パフォーマンスが低下したり高可用性（HA）が失われたりする可能性のある障害です。通常、サービスへのそれ以外の影響はありません。
- **critical** : サービスに影響する深刻な障害です。システムは、API要求およびクライアントI/O要求を処理できません。この状態で運用を続けると、データが失われる可能性があります。
- **bestPractice** : 推奨されるシステム構成のベストプラクティスが使用されていません。

Type

- **node** : ノード全体に影響する障害。
- **drive** : 個々のドライブに影響する障害。
- **cluster** : クラスタ全体に影響する障害。
- **service** : クラスタ上のサービスに影響する障害。
- **volume** : クラスタ上のボリュームに影響する障害。

Node

このエラーに関連するノードのノードID。エラーのタイプがnodeとdriveの場合に表示され、それ以外の場合は「-」（ダッシュ）が表示されます。

Drive ID

このエラーに関連するドライブのドライブID。エラーのタイプがdriveの場合に表示され、それ以外の場合は「-」（ダッシュ）が表示されます。

Error Code

エラーの原因を示すコード。

Details

エラーの詳細な説明。

Time

この項目は[Active filter]ビューにのみ表示されます。エラーがログに記録された日時です。

Resolution Date

この項目は[Resolved filter]ビューにのみ表示されます。エラーが解決された日時です。

アラート エラー コード

[Alerts]ページには、システムから報告されたエラー コードと各アラートが表示されます。エラー コードは、アラートが発生したシステムのコンポーネントおよびアラートが生成された理由を判断する場合に役立ちます。

以下は、各種システム アラートのリストです。

availableVirtualNetworkIPAddressesLow

IPアドレス ブロック内の仮想ネットワーク アドレスの数が不足しています。この問題を解決するには、仮想ネットワーク アドレスのブロックにIPアドレスを追加してください。

blockClusterFull

単一ノードの損失をサポートするのに十分なブロック ストレージの空き容量がありません。この問題を解決するには、ストレージ クラスタにストレージ ノードをもう1つ追加してください。

blockServiceTooFull

ブロック サービスが大量の容量を使用しています。この問題を解決するには、プロビジョニング済み容量を追加してください。

blockServiceUnhealthy

ブロック サービスが正常ではないことが検出されました。影響を受けるデータは他の正常なドライブに自動的に移動されます。

clusterCannotSync

スペース不足です。オフラインのブロック ストレージ ドライブ上のデータをアクティブな状態のドライブに同期することはできません。この問題を解決するには、ストレージを追加してください。

clusterFull

ストレージ クラスタ内の空きストレージ スペースが不足しています。この問題を解決するには、ストレージを追加してください。

clusterIOPSAreOverProvisioned

クラスタのIOPSがオーバープロビジョニングされています。最小QoSのIOPSの合計が、クラスタの想定IOPSを上回っています。すべてのボリュームで同時に最小QoSを維持することができません。

disableDriveSecurityFailed

クラスタはドライブのセキュリティ（保存中のデータの暗号化）を有効にするようには設定されていませんが、少なくとも1つのドライブでドライブのセキュリティが有効になっているため、そのドライブでドライブのセキュリティを無効にできませんでした。この障害の重大度は「Warning」です。

この問題を解決するには、ドライブのセキュリティを無効にできなかった理由について障害の詳細を確認してください。次の理由が考えられます。

- 暗号化キーを取得できなかった場合は、キーまたは外部キー サーバへのアクセスに関する問題を調査してください。
- ドライブで無効化処理に失敗した場合は、間違ったキーが取得されていないかどうかを確認してください。

どちらでもない場合は、ドライブの交換が必要となる可能性があります。

正しい認証キーを指定してもセキュリティが無効にならないドライブに対して、リカバリを試みることができます。この処理を実行するには、ドライブの状態をAvailableに変更してシステムから取り外し、ドライブで完全消去を実行してからActiveに戻します。

disconnectedClusterPair

クラスタ ペアが切断されているか、正しく設定されていません。

disconnectedRemoteNode

リモート ノードが切断されているか、正しく設定されていません。

disconnectedSnapMirrorEndpoint

リモートSnapMirrorエンドポイントが切断されているか、正しく設定されていません。

driveAvailable

クラスタ内に利用可能なドライブがあります。通常は、すべてのクラスタにすべてのドライブが追加されていて、利用可能な状態のドライブはないはずですが、この問題が予期せずに発生する場合は、ネットアップ サポートにお問い合わせください。この問題を解決するには、利用可能なドライブをすべてストレージ クラスタに追加してください。

driveFailed

1 つ以上のドライブで障害が発生しています。認証キーにアクセスできないためにエラーが発生した場合は、キー サーバの接続に関する問題を解決します。その他の問題については、ネットアップ サポートにお問い合わせください。

driveWearFault

ドライブの残存寿命がしきい値を下回っていますが、まだ機能しています。この問題を解決するには、ドライブをすぐに交換してください。

duplicateClusterMasterCandidates

ストレージ クラスタ マスターの候補が複数検出されました。ネットアップ サポートにお問い合わせください。

enableDriveSecurityFailed

クラスタはドライブのセキュリティ（保存中のデータの暗号化）を要求するように設定されていますが、少なくとも1つのドライブでセキュリティを有効にできませんでした。この障害の重大度は「Warning」です。

この問題を解決するには、ドライブのセキュリティを有効にできなかった理由について障害の詳細を確認してください。次の理由が考えられます。

- 暗号化キーを取得できなかった場合は、キーまたは外部キー サーバへのアクセスに関する問題を調査してください。
- ドライブで有効化処理に失敗した場合は、間違ったキーが取得されていないかどうかを確認してください。

どちらでもない場合は、ドライブの交換が必要となる可能性があります。

正しい認証キーを指定してもセキュリティが有効にならないドライブに対して、リカバリを試みることができます。この処理を実行するには、ドライブの状態を Available に変更してシステムから取り外し、ドライブで完全消去を実行してから Active に戻します。

ensembleDegraded

1 つ以上のアンサンプル ノードへのネットワーク接続または電源が失われています。この問題を解決するには、ネットワーク接続または電源を復旧してください。

exception

想定外の障害が報告されました。この障害は障害キューから自動的に消去されません。ネットアップ サポートにお問い合わせください。

failedSpaceTooFull

ブロック サービスがデータ書き込み要求に応答していません。スライス サービスが失敗した書き込みを格納するための容量が足りなくなります。この問題を解決するには、書き込みを正常に処理し、失敗用の容量がスライス サービスからフラッシュされるように、ブロック サービス機能をリストアしてください。

fanSensor

ファン センサーで障害が発生しているか、ファン センサーが見つかりません。
ネットアップ サポートにお問い合わせください。

fibreChannelAccessDegraded

Fibre Channelノードが自身のストレージIPでストレージ クラスタ内の他のノード
に一定期間応答していません。この状態になると、ノードは応答していないと判
断され、クラスタ障害が生成されます。

fibreChannelAccessUnavailable

すべてのFibre Channelノードが応答していません。ノードIDが表示されます。

fibreChannelConfig

このクラスタ障害は、次のいずれかの状態を示します。

- PCIスロットに想定外のFibre Channelポートが接続されています。
- 想定外のFibre Channel HBAモデルが使用されています。
- Fibre Channel HBAのファームウェアに問題があります。
- Fibre Channelポートがオンラインではありません。
- Fibre Channelパススルーの設定中に永続的な問題が発生しました。

ネットアップ サポートにお問い合わせください。

fileSystemCapacityLow

いずれかのファイルシステムでスペースが不足しています。

この問題を解決するには、ファイルシステムに容量を追加してください。

FIPS drives mismatched

FIPS対応ストレージ ノードにFIPS非対応ドライブが挿入されているか、FIPS非対
応ストレージ ノードにFIPS対応ドライブが挿入されています。ノードごとにエ
ラーが生成され、影響を受けるすべてのドライブが表示されます。

この問題を解決するには、該当するドライブを取り外すか交換してください。

FIPS drives out of compliance

FIPSドライブ機能を有効にしたあとに保存データの暗号化を無効にしたことが検
出されました。このエラーは、FIPSドライブ機能が有効になっていて、FIPS非対
応のドライブまたはノードがストレージ クラスタに配置されている場合にも生成
されます。

この問題を解決するには、保存データの暗号化を有効にするか、FIPS非対応のハー
ドウェアをストレージ クラスタから取り外してください。

fipsSelfTestFailure

FIPSサブシステムのセルフ テスト中に障害が検出されました。

ネットアップ サポートにお問い合わせください。

hardwareConfigMismatch

このクラスタ障害は、次のいずれかの状態を示します。

- 構成がノードの定義と一致しません。
- このタイプのノードに対して正しくないドライブ サイズが使用されています。
- サポート対象外のドライブが検出されました。
- ドライブ ファームウェアが一致しません。

- ドライブの暗号化対応がノードと一致しません。

ネットアップ サポートにお問い合わせください。

inconsistentBondModes

VLANデバイスのボンディング モードが見つかりません。想定されるボンディング モードと使用中のボンディング モードが表示されます。

inconsistentInterfaceConfiguration

インターフェイスの設定が一貫していません。

この問題を解決するには、ストレージ クラスタ内のすべてのノード インターフェイスの設定を同じにしてください。

inconsistentMtus

このクラスタ障害は、次のいずれかの状態を示します。

- Bond1Gの不一致：Bond1Gインターフェイス間で異なるMTUが設定されています。
- Bond10Gの不一致：Bond10Gインターフェイス間で異なるMTUが設定されています。

該当するノードと設定されているMTU値が表示されます。

inconsistentRoutingRules

このインターフェイスのルーティング ルールが一貫していません。

inconsistentSubnetMasks

VLANデバイスのネットワーク マスクが、内部的に記録されたVLANのネットワーク マスクと一致しません。想定されるネットワーク マスクと使用中のネットワーク マスクが表示されます。

incorrectBondPortCount

ボンド ポートの数が正しくありません。

invalidConfiguredFibreChannelNodeCount

想定される2つのFibre Channelノード接続のいずれかがデグレード状態です。この問題は、Fibre Channelノードが1つしか接続されていない場合に発生します。

irqBalanceFailed

割り込み処理の負荷分散中に例外が発生しました。

ネットアップ サポートにお問い合わせください。

kmipCertificateFault

- ルート認証局（CA）証明書の有効期限が近づいています。
この問題を解決するには、有効期限まで30日以上ある新しい証明書をルート CAから取得し、ModifyKeyServerKmipを使用してルートCA証明書を更新します。
- クライアント証明書の有効期限が近づいています。
この問題を解決するには、GetClientCertificateSigningRequestを使用して新しいCSRを作成し、新しい有効期限まで30日以上あることを確認して署名し、ModifyKeyServerKmipを使用して期限が切れるKMIPクライアント証明書を新しい証明書に置き換えます。
- ルート認証局（CA）証明書の有効期限が切れています。
この問題を解決するには、有効期限まで30日以上ある新しい証明書をルート CAから取得し、ModifyKeyServerKmipを使用してルートCA証明書を更新します。

- クライアント証明書の有効期限が切れています。
この問題を解決するには、GetClientCertificateSigningRequestを使用して新しいCSRを作成し、新しい有効期限まで30日以上あることを確認して署名し、ModifyKeyServerKmpを使用し期限切れのKMIPクライアント証明書を新しい証明書に置き換えます。
- ルート認証局（CA）証明書のエラーです。
この問題を解決するには、正しい証明書が提供されていることを確認し、必要に応じてルートCAから証明書を再取得します。ModifyKeyServerKmpを使用して正しいルート認証局（CA）証明書をインストールします。
- クライアント証明書のエラーです。
この問題を解決するには、正しいKMIPクライアント証明書がインストールされていることを確認します。クライアント証明書のルートCAがEKSにインストールされている必要があります。ModifyKeyServerKmpを使用して正しいKMIPクライアント証明書をインストールします。

kmipServerFault

- 接続エラー
この問題を解決するには、外部キー サーバが稼働しており、ネットワーク経由でアクセスできることを確認します。TestKeyServerKmpとTestKeyProviderKmpを使用して、接続をテストします。
- 認証エラー
この問題を解決するには、正しいルートCAおよびKMIPクライアント証明書が使用されていることと、秘密鍵とKMIPクライアント証明書が一致することを確認します。
- サーバエラー
この問題を解決するには、エラーの詳細を確認します。エラーによっては、外部キー サーバでのトラブルシューティングが必要になる場合があります。

memoryUsageThreshold

メモリ使用量が正常値を上回っています。
ネットアップ サポートにお問い合わせください。

metadataClusterFull

単一ノードの損失をサポートするのに十分なメタデータの空き容量がありません。
この問題を解決するには、ストレージ クラスタにストレージ ノードをもう1つ追加してください。

mtuCheckFailure

ネットワーク デバイスに適切なMTUサイズが設定されていません。
この問題を解決するには、すべてのネットワーク インターフェイスとスイッチポートでジャンボ フレームが設定されている（MTUが最大9,000バイト）ことを確認してください。

networkConfig

このクラスタ障害は、次のいずれかの状態を示します。

- 想定されるインターフェイスが存在しません。
- インターフェイスが重複しています。
- 設定済みのインターフェイスが停止しています。

- ネットワークの再起動が必要です。

ネットアップ サポートにお問い合わせください。

networkErrorsExceedThreshold

このクラスタ障害は、次のいずれかの状態を示します。

- フレーム エラーの数が正常値を上回っています。
- CRCエラーの数が正常値を上回っています。

この問題を解決するには、エラーが報告されているインターフェイスに接続されたネットワーク ケーブルを交換してください。

ネットアップ サポートにお問い合わせください。

noAvailableVirtualNetworkIPAddresses

IPアドレスのブロックに利用可能な仮想ネットワーク アドレスがありません。クラスタにこれ以上ストレージ ノードを追加できません。

この問題を解決するには、仮想ネットワーク アドレスのブロックにIPアドレスを追加してください。

nodeOffline

Elementソフトウェアが指定されたノードと通信できません。

notUsingLACPBondMode

LACPボンディング モードが設定されていません。

この問題を解決するには、ストレージ ノードの導入時にLACPボンディングを使用してください。LACPを有効にして正しく設定していないと、クライアントでパフォーマンスの問題が発生する可能性があります。

ntpServerUnreachable

ストレージ クラスタが指定されたNTPサーバと通信できません。

NTPサーバ、ネットワーク、およびファイアウォールの設定を確認してください。

ntpTimeNotInSync

ストレージ クラスタと指定されたNTPサーバで時刻に大きな差があります。ストレージ クラスタはこの時間差を自動的に修正できません。この問題を解決するには、インストール時のデフォルトではなく、使用するネットワーク内のNTPサーバを使用してください。内部のNTPサーバを使用しても問題が解決しない場合は、ネットアップ サポートにお問い合わせください。

nvrAmDeviceStatus

NVRAMデバイスにエラーがあるか、障害が発生しようとしているか、または障害が発生しました。

ネットアップ サポートにお問い合わせください。

powerSupplyError

このクラスタ障害は、次のいずれかの状態を示します。

- 電源装置がありません。
- 電源装置で障害が発生しました。
- 電源装置の入力が見つからないか、範囲外です。

冗長な電源がすべてのノードに供給されていることを確認してください。ネットアップ サポートにお問い合わせください。

provisionedSpaceTooFull

クラスタのプロビジョニング済み容量がいっぱいです。

この問題を解決するには、プロビジョニング済みスペースを追加するか、またはボリュームを削除およびパージしてください。

remoteRepAsyncDelayExceeded

レプリケーションに設定されている非同期遅延を超えました。

remoteRepClusterFull

ターゲットストレージ クラスタがいっぱいのため、ボリュームがリモート レプリケーションを停止しました。

remoteRepSnapshotClusterFull

ターゲットストレージ クラスタがいっぱいのため、ボリュームがSnapshotのリモートレプリケーションを停止しました。

この問題を解決するには、ターゲットストレージ クラスタのスペースを解放してください。

remoteRepSnapshotsExceededLimit

ターゲットストレージ クラスタのボリュームがSnapshotの最大数を超えたため、ボリュームがSnapshotのリモートレプリケーションを停止しました。

scheduleActionError

スケジュールされたアクティビティが実行されましたが、失敗しました。

スケジュールされたアクティビティが再び実行されて成功するか、アクティビティが削除されるか、または停止後に再開されれば、障害はクリアされます。

sensorReadingFailed

ベースボード管理コントローラ（BMC）のセルフテストが失敗したか、センサーがBMCと通信できませんでした。

ネットアップ サポートにお問い合わせください。

serviceNotRunning

要求されたサービスが実行されていません。

ネットアップ サポートにお問い合わせください。

sliceServiceTooFull

スライス サービスに割り当てられたプロビジョニング済み容量が少なすぎます。

この問題を解決するには、プロビジョニング済み容量を追加してください。

sliceServiceUnhealthy

スライス サービスが正常な状態でないことをシステムが検出し、サービスを自動的に停止しています。

sshEnabled

ストレージ クラスタ内の1つ以上のノードでSSHサービスが有効になっています。

この問題を解決するには、該当するノードのSSHサービスを無効にするか、ネットアップ サポートにお問い合わせください。

sslCertificateExpiration

このノードに関連付けられているSSL証明書の有効期間が終了しています。

この問題を解決するには、SSL証明書を更新してください。必要であれば、ネットアップ サポートにお問い合わせください。

tempSensor

温度センサーが正常よりも高い温度を報告しています。この問題は、powerSupplyErrorまたはfanSensorとともに発生する可能性があります。

ストレージ クラスタの近くに通気を妨げる障害物がないかどうかを確認してください。必要であれば、ネットアップ サポートにお問い合わせください。

upgrade

アップグレードが24時間以上実行中です。

この問題を解決するには、アップグレードを再開するか、ネットアップ サポートにお問い合わせください。

unbalancedMixedNodes

1つのノードがストレージ クラスタの容量の1/3以上を使用しています。

ネットアップ サポートにお問い合わせください。

unresponsiveService

サービスが応答しなくなりました。

ネットアップ サポートにお問い合わせください。

virtualNetworkConfig

このクラスタ障害は、次のいずれかの状態を示します。

- インターフェイスがありません。
- インターフェイス上のネームスペースが正しくありません。
- ネットマスクが正しくありません。
- IPアドレスが正しくありません。
- インターフェイスが稼働していません。
- ノード上に不要なインターフェイスがあります。

ネットアップ サポートにお問い合わせください。

volumeDegraded

セカンダリ ボリュームのレプリケートと同期が終了していません。このメッセージは、同期が完了するとクリアされます。

volumesOffline

ストレージ クラスタ内の1つ以上のボリュームがオフラインです。

ネットアップ サポートにお問い合わせください。

関連情報

[ネットアップ サポート](#)

iSCSIセッション

NetApp Element Management拡張ポイントの[Reporting]タブにある[iSCSI Sessions]ページでは、選択したクラスタに接続されているiSCSIセッションに関する情報を確認できます。

Node

ボリュームのプライマリ メタデータ パーティションをホストしているノード。

Account

ボリュームを所有するアカウントの名前。値が空白の場合は、ダッシュ (-) が表示されます。

Volume

ノードでのボリュームの識別名。

Volume ID

ターゲットIQNに関連付けられたボリュームのID。

Initiator ID

システムによって生成されたイニシエータのID。

Initiator Alias

イニシエータが多数ある場合に特定のイニシエータを見つけやすくするための別名。

Initiator IP

セッションを開始するエンドポイントのIPアドレス。

Initiator IQN

セッションを開始するエンドポイントのIQN。

Target IP

ボリュームをホストしているノードのIPアドレス。

Target IQN

ボリュームのIQN。

Created On

セッションが確立された日時。

実行中のタスク

ListSyncJobsおよびListBulkVolumeJobs APIメソッドから報告される、実行中のタスクの進捗状況と完了ステータスを確認できます。**NetApp Element Management**拡張ポイントの[Reporting]タブにある[Running Tasks]ページでは、実行中のタスクを確認できます。

Task Type

同期ジョブまたは一括ボリューム ジョブのタイプ。

有効な値は次のとおりです。

- block
- clone
- read
- remote
- slice
- write

Node

クローンが書き込まれるノードのIDです。このIDは、タスク タイプがcloneの場合にのみ表示されます。

Description

システムで現在実行中の同期プロセスの詳細を示すオブジェクトのリスト、またはシステムで現在実行中の各一括ボリューム ジョブの情報。

Current Progress

ソース ボリュームのうち、クローンが処理したバイト数。この情報は、タスク タイプがcloneまたはsliceの場合にのみ表示されます。

Elapsed Time

ジョブが開始されてからの経過時間（秒）。

Remaining Time

処理が完了するまでの推定残り時間（秒）。

ボリュームのパフォーマンス

NetApp Element Management拡張ポイントの[Reporting]タブにある[Volume Performance] ページで、選択したクラスタ内のすべてのボリュームのパフォーマンス情報を確認できます。

[Refresh every] リストをクリックして別の値を選択すると、ページ上のパフォーマンス情報の更新頻度を変更できます。クラスタのボリューム数が1,000個未満の場合、デフォルトの更新間隔は10秒です。それ以外の場合は60秒です。[Never]を選択すると、ページの自動更新が無効になります。

ID

システムによって生成されたボリュームのID。

Name

ボリュームの作成時に指定した名前。

Account

ボリュームに割り当てられているアカウントの名前。

Access Groups

ボリューム アクセス グループまたはボリュームが所属するグループの名前。

Volume Utilization %

クライアントによるボリュームの使用率を示すパーセンテージ。

有効な値は次のとおりです。

- 0：クライアントはボリュームを使用していません。
- 100：クライアントは最大値まで使用しています。
- >100：クライアントはバースト値を使用しています。

Total IOPS

ボリュームに対して実行中のIOPS（読み取りおよび書き込み）の総数。

Read IOPS

ボリュームに対して実行中の読み取りIOPSの総数。

Write IOPS

ボリュームに対して実行中の書き込みIOPSの総数。

Total Throughput

ボリュームに対して実行中のスループット（読み取りおよび書き込み）の総量。

Read Throughput

ボリュームに対して実行中の読み取りスループットの総量。

Write Throughput

ボリュームに対して実行中の書き込みスループットの総量。

Total Latency (ms)

ボリュームに対する読み取りおよび書き込み処理が完了するまでの平均時間（マイクロ秒）。

Read Latency (ms)

過去500ミリ秒の、ボリュームに対する読み取り処理が完了するまでの平均時間（マイクロ秒）。

Write Latency (ms)

過去500ミリ秒の、ボリュームに対する書き込み処理が完了するまでの平均時間（マイクロ秒）。

Queue Depth

ボリュームに対する未処理の読み取りおよび書き込み処理の数。

Average IO Size

過去500ミリ秒の、ボリュームに対する最新のI/Oの平均サイズ（バイト）。

管理

[Management]タブでは、データストア、ボリューム、アカウント、アクセスグループ、イニシエータ、およびボリュームのQoSポリシーを作成および管理できます。

データストア管理

NetApp Element Plug-in for vCenter Serverでは、Elementボリューム上に作成されたデータストアを管理できます。データストアの作成、拡張、クローニング、共有、削除が可能です。また、VAAI UNMAP機能を使用して、シンプロビジョニングされたVMFSデータストアから解放されたブロックスペースをクラスタで再生することもできます。

データストア処理の進捗状況は、vSphereのタスク監視を使用して監視できます。

注: データストアを作成および管理するには、[Management] > [Accounts]でユーザ アカウントを少なくとも1つ作成しておく必要があります。データストアでQoSSIOCサービスを使用する場合は、まずNetApp Element Configuration拡張ポイントの[mNode Settings]ページで設定を行う必要があります。

関連タスク

[アカウントの作成](#) (118ページ)

[QoSSIOCの管理ノードの設定](#) (63ページ)

データストアの作成

NetApp Element Management拡張ポイントを使用して、データストアを作成できます。

開始する前に

- クラスタが少なくとも1つ追加および実行されている必要があります。

注: vCenterリンクモードを使用している場合は、クラスタが追加されているvCenter Serverが正しいことを確認してください。
- ユーザ アカウントを少なくとも1つ作成しておく必要があります。
- vCenter Serverにホストが少なくとも1つ接続されている必要があります。

タスク概要

データストアの作成には選択したESXiホストでサポートされる最も高いVMFSバージョンが使用されるので、VMFSの互換性に関する問題を防ぐために、実行するvSphereおよびESXiのバージョンをすべてのクラスタ メンバーで統一する必要があります。

注: データストアでQoSSIOCサービスを使用する場合は、まずNetApp Element Configuration拡張ポイントの[mNode Settings]ページで設定を行う必要があります。

手順

1. [NetApp Element Management] > [Management]を選択します。

注: 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。

2. **[Datastore]**ページで、**[Create Datastore]**をクリックします。

3. **[Create Datastore]**ダイアログ ボックスで、データストアの名前を入力します。

ヒント:各データストアにはデータセンター内で一意な名前を使用します。複数のクラスタやvCenter Serverを使用する環境では、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。

4. **[Next]**をクリックします。

5. データストアに必要なホストを1つ以上選択します。

注:新しいデータストアを作成するには、ホストが少なくとも1つ接続されている必要があります。ホストに複数のイニシエータがある場合は、いずれかのイニシエータを選択するか、またはホストを選択することですべてのイニシエータを選択します。vCenterリンク モードを使用している場合は、クラスタが割り当てられているvCenter Serverから使用可能なホストのみを選択できます。

6. **[Next]**をクリックします。

7. **[Configure Volume]**ペインで、既存のボリュームを選択して次の手順に進むか、新しいデータストア用に新しいボリュームを作成します。

a. データストアの基盤となるボリュームの名前を入力します。

b. アカウントのドロップダウン リストからユーザ アカウントを選択します。

注:新しいボリュームを作成するには、既存のユーザ アカウントが少なくとも1つ必要です。

c. 作成するボリュームの合計サイズを入力します。

注:デフォルトのボリューム サイズの単位はGBです。GBまたはGiB単位のサイズを使用してボリュームを作成できます。

- 1GB=1,000,000,000バイト

- 1GiB=1,073,741,824バイト

注:デフォルトでは、すべての新しいボリュームについて、512バイト エミュレーションがONに設定されます。

d. **[Quality of Service]**領域で、次のいずれかを実行します。

- **[Policy]**で、既存のQoSポリシーを選択します。

- **[Custom Settings]**で、IOPSの最小値、最大値、および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。

注意:データストアのQoSSSIOC設定を有効にすると、ボリューム レベルのQoS設定よりも優先されます。

注意: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。

8. **[Next]**をクリックします。

9. 次のいずれかを選択してホスト アクセスの認証タイプを設定します。

- **Use Volume Access Group**

- Use CHAP

注 : ボリュームを参照できるイニシエータを明示的に制限するには、ボリューム アクセス グループの認証タイプを使用します。シークレットベースのセキュアなアクセスで、イニシエータを制限しない場合はCHAPを使用します。

10. [Next]をクリックします。
11. [Use Volume Access Group]を選択した場合は、選択したホストのボリューム アクセス グループを設定します。
[Required by Selected Initiators]に表示されているボリューム アクセス グループは、前の手順で選択した1つ以上のホスト イニシエータにすでに関連付けられています。
 - a. 追加のボリューム アクセス グループを選択するか、またはボリューム アクセス グループを新規作成して、使用可能なイニシエータに関連付けます。
 - **Available :** クラスタ内のその他のボリューム アクセス グループを選択します。
 - **Create New Access Group :** 新しいアクセス グループの名前を入力し、[Add]をクリックします。
 - b. [Next]をクリックします。
 - c. **[Configure Hosts' Access]**ペインで、使用可能なホスト イニシエータ (IQNまたはWWPN) を、前のペインで選択したボリューム アクセス グループに関連付けます。ボリューム アクセス グループがすでに関連付けられているホスト イニシエータの場合、このフィールドは読み取り専用です。ボリューム アクセス グループに関連付けられていない場合は、イニシエータの横にあるドロップダウン リストから選択します。
 - d. [Next]をクリックします。
12. QoSSIOC自動化を有効にする場合は、[Enable QoS & SIOC]チェック ボックスをクリックしてオンにし、QoSSIOCの設定を行います。
注 : QoSSIOCサービスを使用できない場合は、まず**NetApp Element Configuration**拡張ポイントの[mNode Settings]ページで設定を行う必要があります。
 - a. [Enable QoS & SIOC]を選択します。
 - b. [Burst Factor]を設定します。
注 : バースト係数は、VMDKのIOPS制限 (SIOC) 設定に掛ける係数です。デフォルト値を変更する場合は、すべてのVMDKについて、IOPS制限にこの係数を掛けてもElementボリュームの最大バースト制限を超えない値を指定してください。
 - c. オプション : [Override Default QoS]を選択し、値を設定します。
注 : データストアに対して[Override Default QoS]設定を無効にした場合、[Shares]および[Limit IOPS]の値は各VMのデフォルトのSIOC設定に基づいて自動的に設定されます。
ヒント : SIOCシェア制限をカスタマイズするときは、SIOC IOPS制限も必ずカスタマイズしてください。
13. [Next]をクリックします。
14. 選択内容を確認し、[Finish]をクリックします。
15. vSphereのタスク監視を使用して、タスクの進捗状況を確認できます。データストアがリストに表示されない場合は、ビューを更新します。

関連概念

[複数クラスタを管理する場合のオブジェクト名のベストプラクティス](#) (53ページ)

関連タスク

[クラスタの追加](#) (54ページ)

[アカウントの作成](#) (118ページ)

[QoSIOCCの管理ノードの設定](#) (63ページ)

データストア リストの表示

使用可能なデータストアは、NetApp Element Management拡張ポイントの[Datastores]ページで確認できます。

手順

1. [NetApp Element Management] > [Management]を選択します。

注：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。

2. [Datastores]ページに、NetApp ElementおよびESXiの現在のデータストアがすべて表示されます。

注：複数のボリュームにまたがるデータストア（混在データストア）はリストに表示されません。[Datastore]ビューには、選択したNetApp ElementクラスタのESXiホストで利用できるデータストアのみが表示されます。

データストアの詳細

NetApp Element Management拡張ポイントの[Management]タブにある[Datastores]ページで、クラスタ上のすべてのデータストアに関する情報を確認できます。

Name

データストアに割り当てられている名前。

Host Name(s)

関連付けられている各ホスト デバイスのアドレス。

Status

有効な値は[Accessible]または[Inaccessible]です。データストアが現在vSphereに接続されているかどうかを示します。

Type

VMwareファイルシステムのデータストア タイプ。

Volume Name

関連付けられたボリュームに割り当てられている名前。

Volume NAA

関連付けられたボリュームのSCSIデバイスのグローバル一意識別子（NAA IEEE Registered Extended形式）。

Total Capacity (GB)

データストアのフォーマット後の総容量。

Free Capacity (GB)

データストアに使用できるスペース。

QoSSIOC Automation

QoSSIOC自動化が有効になっているかどうか。有効な値は次のとおりです。

- Enabled : QoSSIOCは有効です。
- Disabled : QoSSIOCは無効です。
- Max Exceeded : ボリュームの[Max QoS]が指定された制限値を超えています。

データストアの拡張

NetApp Element Management拡張ポイントを使用して、データストアを拡張してボリュームのサイズを大きくすることができます。データストアを拡張すると、そのデータストアに関連するVMFSボリュームも拡張されます。

手順

1. [NetApp Element Management] > [Management]を選択します。
注 : 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。
2. [Datastores]ページで、拡張するデータストアのチェックボックスを選択します。
3. [Actions]をクリックします。
4. 表示されたメニューで[Extend]をクリックします。
5. [New Datastore Size]フィールドに新しいデータストアのサイズを入力し、単位（GBまたはGiB）を選択します。
注 : データストアの拡張では、ボリューム全体のサイズが消費されます。新しいデータストアのサイズは、選択したクラスタで利用可能なプロビジョニングされていないスペースよりも大きくすることはできません。また、クラスタで許容される最大ボリューム サイズ以下でなければなりません。
6. [OK]をクリックします。
7. 更新されたデータストアがリストに表示されるまで、必要に応じてページを更新します。

データストアのクローニング

NetApp Element Plug-in for vCenter Serverでは、データストアのクローニングが可能で、新しいデータストアを目的のESXiサーバやクラスタにマウントする機能などが用意されています。作成したデータストアのクローンに名前を付け、QoSSIOC、ボリューム、ホスト、および認証タイプを設定できます。

開始する前に

- クラスタが少なくとも1つ追加および実行されている必要があります。
注 : vCenterリンク モードを使用している場合は、クラスタが追加されているvCenter Serverが正しいことを確認してください。
- ソース 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。
- vCenter Serverにホストが少なくとも1つ接続されている必要があります。
- ユーザ アカウントを少なくとも1つ作成しておく必要があります。

タスク概要

ソース データストアに仮想マシンが存在する場合は、クローン データストア上の仮想マシンが新しい名前でインベントリに格納されます。

手順

1. [NetApp Element Management] > [Management]を選択します。

注：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。

2. [Datastores]ページで、クローニングするデータストアのチェック ボックスを選択します。

3. [Actions]をクリックします。

4. 表示されたメニューで[Clone]をクリックします。

注：クローニングするデータストアにそのデータストアにないディスクが接続された仮想マシンが含まれている場合、クローンの作成後、その仮想マシンのコピーは仮想マシン インベントリに追加されません。

5. データストア名を入力します。

ヒント：各データストアにはデータセンター内で一意な名前を使用します。複数のクラスタやvCenter Serverを使用する環境では、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。

6. [Next]をクリックします。

7. データストアに必要なホストを1つ以上選択します。

注：新しいデータストアを作成するには、ホストが少なくとも1つ接続されている必要があります。ホストに複数のイニシエータがある場合は、いずれかのイニシエータを選択するか、またはホストを選択することですべてのイニシエータを選択します。vCenterリンク モードを使用している場合は、クラスタが割り当てられているvCenter Serverから使用可能なホストのみを選択できます。

8. [Next]をクリックします。

9. [Configure Volume]ペインで、次の手順を実行します。

注：クローン データストアのボリューム サイズは、ソース データストアを構成するボリュームのサイズと同じになります。デフォルトでは、すべての新しいボリュームについて、512バイト エミュレーションがONに設定されます。

- a. クローン データストアを構成する新しいNetApp Elementボリュームの名前を入力します。

- b. アカウントのドロップダウン リストからユーザ アカウントを選択します。

注：新しいボリュームを作成するには、既存のユーザ アカウントが少なくとも1つ必要です。

- c. [Quality of Service]領域で、次のいずれかを実行します。

- [Policy]で、既存のQoSポリシーを選択します。
- [Custom Settings]で、IOPSの最小値、最大値、および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。

注意：

- データストアのQoS SIOC設定を有効にすると、ボリューム レベルのQoS設定よりも優先されます。
- 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. [Next]をクリックします。

11. 次のいずれかのオプションを選択してホスト アクセスの認証タイプを設定します。

- **Use Volume Access Group**
- **Use CHAP**

注： ボリュームを参照できるイニシエータを明示的に制限するには、ボリューム アクセス グループの認証タイプを使用します。シークレットベースのセキュアなアクセスで、イニシエータを制限しない場合はCHAPを使用します。

12. [Next]をクリックします。

13. [Use Volume Access Group]を選択した場合は、選択したホストのボリューム アクセス グループを設定します。

[Required by Selected Initiators]に表示されているボリューム アクセス グループは、前の手順で選択した1つ以上のホスト イニシエータにすでに関連付けられています。

- 追加のボリューム アクセス グループを選択するか、またはボリューム アクセス グループを新規作成して、使用可能なイニシエータに関連付けます。
 - **Available：** クラスタ内のその他のボリューム アクセス グループを選択します。
 - **Create New Access Group：** 新しいアクセス グループの名前を入力し、[Add]をクリックします。

b. [Next]をクリックします。

- [Configure Hosts' Access]ペインで、使用可能なホスト イニシエータ (IQNまたはWWPN) を、前のペインで選択したボリューム アクセス グループに関連付けます。

ボリューム アクセス グループがすでに関連付けられているホスト イニシエータの場合、このフィールドは読み取り専用です。ボリューム アクセス グループに関連付けられていない場合は、イニシエータの横にあるドロップダウン リストから選択します。

d. [Next]をクリックします。

14. QoS SIOC自動化を有効にする場合は、[Enable QoS & SIOC]チェック ボックスをクリックしてオンにし、QoS SIOCの設定を行います。

注： QoS SIOCサービスを使用できない場合は、まずNetApp Element Configuration拡張ポイントの[mNode Settings]ページで設定を行う必要があります。

- [Enable QoS & SIOC]を選択します。
- [Burst Factor]を設定します。

注： バースト係数は、VMDKのIOPS制限 (SIOC) 設定に掛ける係数です。デフォルト値を変更する場合は、すべてのVMDKについて、IOPS制限にこの係数を掛けてもNetApp Elementボリュームの最大バースト制限を超えない値を指定してください。

c. オプション：[Override Default QoS]を選択し、値を設定します。

注：データストアに対して[Override Default QoS]設定を無効にした場合、[Shares]および[Limit IOPS]の値は各VMのデフォルトのSIOC設定に基づいて自動的に設定されます。

ヒント：SIOCシェア制限をカスタマイズするときは、SIOC IOPS制限も必ずカスタマイズしてください。

15. [Next]をクリックします。
16. 選択内容を確認し、[Finish]をクリックします。
17. データストアのクローンがリストに表示されない場合は、ビューを更新します。

関連概念

[複数クラスタを管理する場合のオブジェクト名のベストプラクティス](#) (53ページ)

関連タスク

[クラスタの追加](#) (54ページ)

[アカウントの作成](#) (118ページ)

データストアの共有

NetApp Element Management拡張ポイントを使用して、データストアを1つ以上のホストと共有できます。

開始する前に

- クラスタが少なくとも1つ追加および実行されている必要があります。

注： vCenterリンク モードを使用している場合は、クラスタが追加されているvCenter Serverが正しいことを確認してください。
- 選択したデータセンターに複数のホストが存在している必要があります。

注： データストアを共有できるのは、同じデータセンターにあるホストだけです。

手順

1. [NetApp Element Management] > [Management]を選択します。

注： 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。
2. [Datastores]ページで、共有するデータストアのチェック ボックスを選択します。
3. [Actions]をクリックします。
4. 表示されたメニューで[Share]をクリックします。
5. 次のいずれかを選択してホスト アクセスの認証タイプを設定します。
 - Use Volume Access Group
 - Use CHAP

注： ボリュームを参照できるイニシエータを明示的に制限するには、ボリューム アクセス グループの認証タイプを使用します。シークレットベースのセキュアなアクセスで、イニシエータを制限しない場合はCHAPを使用します。

6. **[Next]**をクリックします。

7. データストアに必要なホストを1つ以上選択します。

注：新しいデータストアを作成するには、ホストが少なくとも1つ接続されている必要があります。ホストに複数のイニシエータがある場合は、いずれかのイニシエータを選択するか、またはホストを選択することですべてのイニシエータを選択します。vCenterリンクモードを使用している場合は、クラスタが割り当てられているvCenter Serverから使用可能なホストのみを選択できます。

8. **[Next]**をクリックします。

9. **[Use Volume Access Group]**を選択した場合は、選択したホストのボリューム アクセス グループを設定します。**[Required by Selected Initiators]**に表示されているボリューム アクセス グループは、前の手順で選択した1つ以上のホスト イニシエータにすでに関連付けられています。

a. 追加のボリューム アクセス グループを選択するか、またはボリューム アクセス グループを新規作成して、使用可能なイニシエータに関連付けます。

- **Available：**クラスタ内のその他のボリューム アクセス グループを選択します。
- **Create New Access Group：**新しいアクセス グループの名前を入力し、**[Add]**をクリックします。

b. **[Next]**をクリックします。

c. **[Configure Hosts' Access]**ペインで、使用可能なホスト イニシエータ (IQNまたはWWPN) を、前のペインで選択したボリューム アクセス グループに関連付けます。

ボリューム アクセス グループがすでに関連付けられているホスト イニシエータの場合、このフィールドは読み取り専用です。ボリューム アクセス グループに関連付けられていない場合は、イニシエータの横にあるドロップダウン リストから選択します。

10. 選択内容を確認し、**[Finish]**をクリックします。

11. データストアの共有タスクが完了したら、リストを更新し、データストアのホストを確認します。

VAAI UNMAPの実行

VAAI UNMAP機能を使用すると、シンプロビジョニングされたVMFS5データストアから解放されたブロック スペースをクラスタで再生できます。

開始する前に

1. タスクに使用するデータストアがVMFS5以前のものであることを確認します。VMFS6では、ESXiで自動的に実行されるため、VAAI UNMAPは使用できません。
2. ESXiホストのシステム設定でVAAI UNMAPが有効になっていることを確認します。

```
esxcli system settings advanced list -o /VMFS3/EnableBlockDelete
```

値が1に設定されている必要があります。

3. ESXiホストのシステム設定でVAAI UNMAPが有効になっていない場合は、次のコマンドを使用して値を1に設定します。

```
esxcli system settings advanced set -i 1 -o /VMFS3/EnableBlockDelete
```

手順

1. [NetApp Element Management] > [Management]を選択します。
 注：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。
2. [Datastores]ページで、VAAI UNMAPを使用するデータストアのチェックボックスを選択します。
3. [Actions]をクリックします。
4. 表示されたメニューで[VAAI Unmap]をクリックします。
5. 名前またはIPアドレスでホストを選択します。
6. ホストのユーザ名とパスワードを入力します。
7. 選択内容を確認し、[OK]をクリックします。

関連情報

[VMware VAAI blog article](#)

データストアの削除

NetApp Element Management拡張ポイントを使用して、データストアを削除できます。この処理を実行すると、該当するデータストアのVMに関連付けられたすべてのファイルが完全に削除されます。プラグインでは、登録済みのVMを含むデータストアは削除されません。

手順

1. [NetApp Element Management] > [Management]を選択します。
 注：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。
2. [Datastores]ページで、削除するデータストアのチェックボックスを選択します。
3. [Actions]をクリックします。
4. 表示されたメニューで[Delete]をクリックします。
5. オプション：データストアに関連付けられたNetApp Elementボリュームを削除する場合は、[Delete associated volume]チェックボックスを選択します。
 注：ボリュームを削除せずに残し、あとで別のデータストアに関連付けることもできます。
6. [Yes]をクリックします。

QoSSIOC自動化

NetApp Element Plug-in for vCenter Serverでは、オプションで、データストア上のすべてのVMのStorage I/O Control (SIOC) 設定に基づいてQoSを自動で設定することができます。

QoSとSIOCの統合 (QoSSIOC) は、ユーザインターフェイスでデータストアに対して有効にすることができます。有効にすると、関連するすべてのVMのすべてのSIOC設定がスキャンされます。QoSSIOC自動化は、VMの電源、ゲスト、および再設定のアクティビティによってトリガーされます。QoSSIOCサービスは、SIOCのすべてのリザベーション (シェア) の

合計とIOPS制限の合計に基づいて、各データストアの基盤となるボリュームの最小QoSと最大QoSを決定します。また、バースト係数も設定できます。

データストアのQoS/SIOC設定時には次のダイアログ ボックスが表示されます。

A5T-BaG1 - QoS/SIOC Automation

Configure QoS/SIOC integration to optimize performance by virtual machines by leveraging NetApp Element QoS and vSphere SIOC

☐ Enable QoS & SIOC

Burst Factor * 4 ⓘ

☐ Override Default QoS

Shares * 1000 ⓘ

Limit IOPS * 2000 ⓘ

Refer to your VMware documentation on customizing VM disk shares.

OK

CANCEL

Enable QoS & SIOC

データストア上の各VMDKのSIOC値の自動監視を有効にし、その値に従って基盤となるボリュームのQoS値を設定します。

Burst Factor

各VMDKのSIOC IOPS制限値の合計に対する乗数です。この係数に基づいて、基盤となるボリュームに許容されるバーストIOPSが決まります。

Override Default QoS

オンにすると[Shares]と[Limit IOPS]を指定できるようになります。これらの値は、各VMのSIOC設定がデフォルトに設定されている場合に使用できます。

Shares

SIOC設定がデフォルトに設定されている場合に使用される各VMDKの最小IOPSです。

Limit IOPS

SIOC設定がデフォルトに設定されている場合に使用される各VMDKの最大IOPSです。

VMDKのSIOC設定がデフォルトの設定（シェア レベルが[Normal]、IOPS制限が[Unlimited]）の場合、[Shares]と[Limit IOPS]の値が基盤となるボリューム全体のQoSに加算されます。VMDKのSIOC設定がデフォルト レベルでない場合は、SIOCのシェアが基盤となるボリュームの最小QoSに、IOPS制限値が最大QoSに加算されます。

注: リザベーション値はvSphere APIでは設定できません。VMDKに対してリザベーション値が設定されている場合、シェアは無視され、代わりにリザベーション値が使用されます。

QoSSIOC自動化の有効化

NetApp Element Management拡張ポイントを使用して、QoSSIOCの自動化を有効にし、仮想マシンディスク（VMDK）のパフォーマンスレベルをカスタマイズすることができます。

開始する前に

NetApp Element Configuration拡張ポイントの[mNode Settings]ページでQoSSIOCサービスを設定しておきます。

注：QoSポリシーを使用する場合は、QoSSIOCを有効にしないでください。QoSSIOCはボリュームのQoS設定よりも優先されます。

手順

1. [NetApp Element Management] > [Management]を選択します。

注：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。

2. 選択したデータストアの[QoSSIOC Automation]列のステータス ボタンをクリックします。

ヒント：QoSの想定外の変更を防止するため、別のvCenterでは同じデータストアのQoSSIOC統合を有効にしないでください。

3. [Enable QoS & SIOC]を選択します。

4. [Burst Factor]を設定します。

注：バースト係数は、VMDKのIOPS制限（SIOC）設定に掛ける係数です。デフォルト値を変更する場合は、すべてのVMDKについて、IOPS制限にこの係数を掛けてもNetApp Elementソフトウェアベースのボリュームの最大バースト制限を超えない値を指定してください。

5. オプション：[Override Default QoS]を選択し、値を設定します。

注：データストアに対して[Override Default QoS]設定を無効にした場合、[Shares]および[Limit IOPS]の値は各VMのデフォルトのSIOC設定に基づいて自動的に設定されます。

ヒント：SIOCシェア制限をカスタマイズするときは、SIOC IOPS制限も必ずカスタマイズしてください。

6. [OK]をクリックします。

注：データストアに対してQoSSIOC自動化を有効にすると、ボタンが[Disabled]から[Enabled]に変わります。

関連タスク

[QoSSIOCの管理ノードの設定](#)（63ページ）

QoSSIOC統合の無効化

NetApp Element Management拡張ポイントを使用して、QoSSIOC統合を無効にできます。

手順

1. [NetApp Element Management] > [Management]を選択します。

注：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。

2. 選択したデータストアの[QoS SIOC Automation]列のボタンをクリックします。
3. [Enable QoS & SIOC]チェックボックスをオフにして統合を無効にします。

注：[Enable QoS & SIOC]チェックボックスをオフにすると、[Override Default QoS]オプションも自動的に無効になります。

4. [OK]をクリックします。

ボリュームの管理

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。

ボリュームの作成

新しいボリュームを作成し、そのボリュームを指定したアカウントに関連付けることができます（ボリュームはすべてアカウントに関連付ける必要があります）。この関連付けにより、アカウントは、iSCSIイニシエータ経由で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ます。作成中に、ボリュームのQoS設定を指定することもできます。

開始する前に

- クラスタが少なくとも1つ追加および実行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。

手順

1. [NetApp Element Management] > [Management]を選択します。

注：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。

2. [Volumes]サブタブをクリックします。
3. [Active]ビューで、[Create Volume]をクリックします。
4. ボリュームの名前を入力します。

ヒント：わかりやすい命名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。

5. 作成するボリュームの合計サイズを入力します。

注：デフォルトのボリュームサイズの単位はGBです。GBまたはGiB単位のサイズを使用してボリュームを作成できます。

- 1GB=1,000,000,000バイト

- 1GiB=1,073,741,824バイト

注：デフォルトでは、すべての新しいボリュームについて、512バイト エミュレーションがONに設定されます。VMwareではディスク リソースに512eが必要です。512eが有効になっていないとVMFSは作成できません。

6. **[Account]** ドロップダウン リストからユーザ アカウントを選択します。

7. **[Quality of Service]** 領域で、次のいずれかを実行します。

- **[Policy]** で、既存のQoSポリシーを選択します。
- **[Custom Settings]** で、IOPSの最小値、最大値、および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。

注意：

- データストアのQoS SIOC設定を有効にすると、ボリューム レベルのQoS設定よりも優先されます。
- 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。

8. **[OK]** をクリックします。

関連概念

[複数クラスタを管理する場合のオブジェクト名のベストプラクティス](#) (53ページ)

関連タスク

[クラスタの追加](#) (54ページ)

[アカウントの作成](#) (118ページ)

ボリュームの詳細の表示

NetApp Element Management拡張ポイントでは、クラスタ上のすべてのアクティブ ボリュームに関する全般的な情報を確認できます。また、各アクティブ ボリュームの詳細（効率性、パフォーマンス、QoSなど）および関連付けられているSnapshotを確認できます。

手順

1. **[NetApp Element Management]** > **[Management]** を選択します。

注： 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。

2. **[Volumes]** サブタブをクリックします。

アクティブ ボリュームに関する全般的な情報が表示されます。

3. 確認するボリュームのチェック ボックスを選択します。

4. **[Actions]** をクリックします。

5. 表示されたメニューで**[View details]**を選択します。

ボリュームの詳細

NetApp Element Management 拡張ポイントの[Management]タブにある[Volumes]ページで、ボリュームの詳細を確認できます。

注：VMwareではディスクリソースに512eが必要です。512eが有効になっていないとVMFSは作成できません。

Volume ID

システムによって生成されたボリュームのID。

Volume Name

ボリュームに割り当てられている名前。

Account

ボリュームに割り当てられているアカウントの名前。

Access Groups

ボリュームが属するボリューム アクセス グループの名前。

Access

ボリュームの作成時に割り当てられたアクセスのタイプ。

有効な値は次のとおりです。

- Read/Write：すべての読み取りと書き込みが許可されます。
- Read Only：すべての読み取りが許可されます。書き込みは許可されません。
- Locked：管理者アクセスのみが許可されます。
- ReplicationTarget：レプリケートされたボリューム ペアのターゲット ボリュームとして指定されています。

Volume Paired

ボリュームがペアリングされているかどうか。

Size (GB)

ボリュームの合計サイズ (GB)。

Snapshots

ボリュームに対して作成されたSnapshotの数。

QoS Policy

ユーザが定義したQoSポリシーの名前。

512e

ボリュームで512eが有効になっているかどうか。[Yes]または[No]のいずれかで

す。

個々のボリュームの詳細

NetApp Element Management 拡張ポイントの[Management]タブにある[Volumes]ページでは、個々のボリュームを選択してその詳細を表示し、アクティブ ボリュームの情報を確認できます。

[General Details]セクションには次の情報が表示されます。

Name

ボリュームに割り当てられている名前。

Volume ID

システムによって生成されたボリュームのID。

IQN

ボリュームのiSCSI Qualified Name。

Account ID

関連付けられているアカウントの一意のアカウントID。

Account

ボリュームに割り当てられているアカウントの名前。

Access Groups

ボリュームが属するボリューム アクセス グループの名前。

Size

ボリュームの合計サイズ (バイト)。

Volume Paired

ボリュームがペアリングされているかどうか。

SCSI EUI Device ID

ボリュームのSCSIデバイスのグローバル一意識別子 (EUI-64ベースの16バイト形式)。

SCSI NAA Device ID

プロトコル エンドポイントのSCSIデバイスのグローバル一意識別子 (NAA IEEE Registered Extended形式)。

[Efficiency]セクションには次の情報が表示されます。

Compression

ボリュームの圧縮による削減率。

Deduplication

ボリュームの重複排除による削減率。

Thin Provisioning

ボリュームのシンプロビジョニングによる削減率。

Last Updated

前回の削減率更新日時。

[Performance]セクションには次の情報が表示されます。

Account ID

関連付けられているアカウントの一意のアカウントID。

Actual IOPS

過去500ミリ秒の、ボリュームに対する実際のIOPS。

Async Delay

ボリュームが最後にリモート クラスタと同期されてからの時間。

Average IOP Size

過去500ミリ秒の、ボリュームに対する最新のI/Oの平均サイズ (バイト)。

Burst IOPS Size

ユーザが利用可能なIOPクレジットの合計数。ボリュームが最大IOPSに到達していない場合、クレジットは蓄積されます。

Client Queue Depth

ボリュームに対する未処理の読み取りおよび書き込み処理の数。

Last Updated

前回のパフォーマンス更新日時。

Latency USec

過去500ミリ秒の、ボリュームに対する処理が完了するまでの平均時間（マイクロ秒）。値「0」（ゼロ）はボリュームに対するI/Oがなかったことを意味します。

Non-zero Blocks

前回のガベージコレクション完了後、データが含まれる4KiBブロックの総数。

Performance Utilization

消費されているクラスタIOPSの割合。たとえば、25万IOPSのクラスタが10万IOPSで実行されている場合、消費率は40%です。

Read Bytes

ボリュームの作成以降にボリュームから読み込んだ累積バイト総数。

Read Latency USec

過去500ミリ秒の、ボリュームに対する読み取り処理が完了するまでの平均時間（マイクロ秒）。

Read Operations

ボリューム作成以降にボリュームに対して行った読み取り処理の合計数。

Thin Provisioning

ボリュームのシンプロビジョニングによる削減率。

Throttle

0～1の浮動小数点数。データの再レプリケーション、一時的なエラー、Snapshotの作成のために、クライアントの処理量をmaxIOPS未満に抑えている割合。

Total Latency USec

ボリュームに対する読み取りおよび書き込み処理が完了するまでの時間（マイクロ秒）。

Unaligned Reads

512eボリュームの場合、4kセクターの境界に沿っていない読み取り処理の数。アラインされていない読み取りが多数ある場合は、パーティションのアライメントが適切でない可能性があります。

Unaligned Writes

512eボリュームの場合、4kセクターの境界に沿っていない書き込み処理の数。アラインしていない書き込みが多数ある場合は、パーティションのアライメントが適切でない可能性があります。

Used Capacity

使用済み容量の割合。

Volume ID

システムによって生成されたボリュームのID。

Vol Access Groups

ボリュームに関連付けられているボリューム アクセス グループのID。

Volume Utilization

クライアントによるボリュームの使用率を示すパーセンテージ。

有効な値は次のとおりです。

- 0：クライアントはボリュームを使用していません。
- 100：クライアントは最大値まで使用しています。

- >100 : クライアントはバースト値を使用しています。

Write Bytes

ボリュームの作成以降にボリュームに書き込まれた累積バイト総数。

Write Latency USec

過去500ミリ秒の、ボリュームに対する書き込み処理が完了するまでの平均時間 (マイクロ秒)。

Write Operations

ボリュームの作成以降にボリュームに対して行った書き込み処理の累積総数。

Zero Blocks

前回のガベージ コレクション完了後、データが含まれない4KiBブロックの総数。

[Quality of Service]セクションには次の見出しがあります。

Policy

ボリュームに割り当てられているQoSポリシーの名前。

I/O Size

IOPSのサイズ (KB)。

Min IOPS

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。

Max IOPS

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。

Max Bandwidth

ブロックサイズの増加に対応するために使用が許可される最大帯域幅。

[Snapshots]セクションには次の情報が表示されます。

Snapshot ID

システムによって生成されたSnapshotのID。

Snapshot Name

ユーザが定義したSnapshotの名前。

Create Date

Snapshotが作成された日時。

Expiration Date

Snapshotが削除される日時。

Size

ユーザが定義したSnapshotのサイズ (GB)。

ボリュームの編集

QoS値、ボリュームのサイズ、バイト値の算出単位など、ボリュームの属性を変更できます。アクセス レベルおよびボリュームにアクセスできるアカウントを変更することもでき

ます。レプリケーションで使用するため、またはボリュームへのアクセスを制限するために、アカウント アクセスを変更することもできます。

タスク概要

管理ノードに永続ボリュームを使用している場合は、永続ボリュームの名前を変更しないでください。

手順

1. **[NetApp Element Management] > [Management]**を選択します。
注：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。
2. **[Volumes]**サブタブをクリックします。
3. **[Active]**ビューで、編集するボリュームのチェック ボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Edit]**をクリックします。
6. オプション：**[Volume Size]**フィールドに別のボリューム サイズ（GBまたはGiB）を入力します。
注：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。レプリケーション用にボリューム サイズを調整するときは、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先に拡張する必要があります。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。
7. オプション：別のユーザ アカウントを選択します。
8. オプション：別のアカウント アクセス レベルを選択します。次のいずれかを選択できます。
 - **Read/Write**
 - **Read Only**
 - **Locked**
 - **Replication Target**
9. **[Quality of Service]**領域で、次のいずれかを実行します。
 - **[Policy]**で、既存のQoSポリシーを選択します。
 - **[Custom Settings]**で、IOPSの最小値、最大値、および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。

ベストプラクティス：IOPSの値を変更する場合は、10または100の単位で増分します。また、有効な整数を入力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。

注意：

- データストアのQoSSSIOC設定はボリューム レベルのQoS設定よりも優先されます。
- 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. [OK]をクリックします。

ボリュームのクローニング

ボリュームのクローンを作成して、データのポイントインタイム コピーを作成できます。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。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。

開始する前に

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

タスク概要

クラスタでは、ボリューム1個につき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、あとから処理されます。

注: 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 メンバシップは継承されません。

手順

1. [NetApp Element Management] > [Management]を選択します。
注: 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。
2. [Volumes]サブタブをクリックします。
3. [Active]ビューで、クローニングするボリュームのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Clone]をクリックします。
6. [Clone Volume]ダイアログ ボックスで、新しいクローン ボリュームのボリューム名を入力します。
ヒント: わかりやすい命名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. クローン ボリュームのサイズ (GBまたはGiB) を選択します。
注: デフォルトのボリューム サイズの単位はGBです。GBまたはGiB単位のサイズを使用してボリュームを作成できます。

- 1GB=1,000,000,000バイト
- 1GiB=1,073,741,824バイト

注：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。

- 新しいクローン ボリュームに関連付けるアカウントを選択します。
- 新しいクローン ボリュームのアクセス タイプとして次のいずれかを選択します。
 - **Read/Write**
 - **Read Only**
 - **Locked**
- 必要に応じて512eの設定を調整します。

注：

 - デフォルトでは、すべての新しいボリュームについて、512バイト エミュレーションが有効になります。
 - VMwareではディスク リソースに512eが必要です。512eが有効になっていない場合は、VMFSを作成できず、ボリュームの詳細がグレー表示されます。

- [OK]をクリックします。

注：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。

関連概念

[複数クラスタを管理する場合のオブジェクト名のベストプラクティス](#) (53ページ)

関連タスク

[クラスタの追加](#) (54ページ)

[アカウントの作成](#) (118ページ)

[ボリュームの作成](#) (99ページ)

ボリュームのバックアップとリストアの処理

NetApp Elementソフトウェアベースのストレージの外部にあるオブジェクト ストア コンテナとの間でボリュームの内容をバックアップおよびリストアするようにシステムを設定できます。

リモートのNetApp Elementソフトウェアベースのシステムとの間でデータをバックアップおよびリストアすることもできます。1つのボリューム上で、一度に最大2つのバックアップまたはリストアの処理を実行できます。

ボリュームのバックアップ処理

NetApp Element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、Elementボリュームをバックアップできます。

関連タスク

[Amazon S3オブジェクトストアへのボリュームのバックアップ](#) (108ページ)

[OpenStack Swiftオブジェクトストアへのボリュームのバックアップ](#) (108ページ)

[Elementソフトウェアを実行しているクラスタへのボリュームのバックアップ](#) (109ページ)

Amazon S3オブジェクトストアへのボリュームのバックアップ

Amazon S3と互換性のある外部のオブジェクトストアにNetApp Elementボリュームをバックアップできます。

手順

1. **[NetApp Element Management] > [Management]**を選択します。
 注：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。
2. **[Volumes]**サブタブをクリックします。
3. **[Active]**ビューで、バックアップするボリュームのチェックボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Back Up to]**をクリックします。
6. ダイアログボックスの**[Back up volume to]**で、**[Amazon S3]**を選択します。
7. **[with the following data format]**でオプションを選択します。
 - **Native**：NetApp Elementソフトウェアベースのストレージシステムのみが読み取り可能な圧縮形式。
 - **Uncompressed**：他のシステムと互換性がある非圧縮形式。
8. **[Host name]**フィールドにオブジェクトストアへのアクセスに使用するホスト名を入力します。
9. **[Access key ID]**フィールドにアカウントのアクセスキーIDを入力します。
10. **[Secret access key]**フィールドにアカウントのシークレットアクセスキーを入力します。
11. **[Amazon S3 bucket]**フィールドにバックアップの格納先とするS3バケットを入力します。
12. オプション：**[Prefix]**フィールドにバックアップボリュームの名前のプレフィックスを入力します。
13. オプション：**[Nametag]**フィールドにプレフィックスに付加するネームタグを入力します。
14. **[OK]**をクリックします。

OpenStack Swiftオブジェクトストアへのボリュームのバックアップ

OpenStack Swiftと互換性のある外部のオブジェクトストアにNetApp Elementボリュームをバックアップできます。

手順

1. **[NetApp Element Management] > [Management]**を選択します。

注：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。

2. [Volumes]サブタブをクリックします。
3. [Active]ビューで、バックアップするボリュームのチェックボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Back Up to]をクリックします。
6. ダイアログボックスの[Back up volume to]で、[OpenStack Swift]を選択します。
7. [with the following data format]でオプションを選択します。
 - **Native**：NetApp Elementソフトウェアベースのストレージシステムのみが読み取り可能な圧縮形式。
 - **Uncompressed**：他のシステムと互換性がある非圧縮形式。
8. [URL]フィールドにオブジェクトストアへのアクセスに使用するURLを入力します。
9. [User name]フィールドにアカウントのユーザ名を入力します。
10. [Authentication key]フィールドにアカウントの認証キーを入力します。
11. [Container]フィールドにバックアップの格納先とするコンテナを入力します。
12. オプション：[Prefix]フィールドにバックアップボリュームの名前のプレフィックスを入力します。
13. オプション：[Nametag]フィールドにプレフィックスに付加するネームタグを入力します。
14. [OK]をクリックします。

Elementソフトウェアを実行しているクラスタへのボリュームのバックアップ

NetApp Elementソフトウェアを実行しているクラスタにあるボリュームをリモートのElementクラスタにバックアップできます。クラスタ間でバックアップまたはリストアを実行する際には、システムによってクラスタ間の認証に使用するキーが生成されます。ソースクラスタはこのボリュームの一括書き込みキーを使用してデスティネーションクラスタに対して認証し、デスティネーションボリュームへの書き込みがセキュリティで保護されます。バックアップまたはリストアを実行する際には、処理を開始する前に、デスティネーションボリュームからボリュームの一括書き込みキーを生成する必要があります。

手順

1. デスティネーションクラスタを含むvCenterから、[NetApp Element Management] > [Management]を選択します。

注：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。
2. [Volumes]サブタブをクリックします。
3. [Active]ビューで、デスティネーションボリュームのチェックボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Restore from]をクリックします。
6. ダイアログボックスの[Restore from]で、[NetApp Element]を選択します。

7. **[with the following data format]**でオプションを選択します。
 - **Native** : NetApp Elementソフトウェアベースのストレージ システムのみが読み取り可能な圧縮形式。
 - **Uncompressed** : 他のシステムと互換性がある非圧縮形式。
8. **[Generate Key]**をクリックして、デスティネーション ボリュームに対するボリュームの一括書き込みキーを生成します。
9. ボリュームの一括書き込みキーをクリップボードにコピーします。これは以降のソース クラスタの手順で使用します。
10. ソース クラスタを含むvCenterから、**[NetApp Element Management]** > **[Management]**を選択します。
11. **[Volumes]**サブタブをクリックします。
12. **[Active]**ビューで、デスティネーション ボリュームのチェック ボックスを選択します。
13. **[Actions]**をクリックします。
14. 表示されたメニューで**[Back Up to]**をクリックします。
15. ダイアログ ボックスの**[Back up volume to]**で、**[NetApp Element]**を選択します。
16. **[with the following data format]**で、デスティネーション クラスタと同じオプションを選択します。
17. **[Remote cluster MVIP]**フィールドにデスティネーション ボリュームのクラスタの管理仮想IPアドレスを入力します。
18. **[Remote cluster user name]**フィールドにデスティネーション クラスタのクラスタ管理者のユーザ名を入力します。
19. **[Remote cluster user password]**フィールドにデスティネーション クラスタのクラスタ管理者のパスワードを入力します。
20. デスティネーション クラスタで生成したキーを**[Bulk volume write key]**フィールドに貼り付けます。
21. **[OK]**をクリックします。

ボリュームのリストア処理

OpenStack SwiftやAmazon S3などのオブジェクトストアにあるバックアップ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。NetApp Elementベースのストレージ システムにバックアップされているNetApp Elementボリュームをリストアする場合、マニフェスト情報は不要です。SwiftおよびS3からのリストアに必要なマニフェスト情報は、**[Reporting]**タブの**[Event Log]**で確認できます。

関連タスク

[Amazon S3オブジェクトストア上のバックアップからのボリュームのリストア](#) (111ページ)

[OpenStack Swiftオブジェクトストア上のバックアップからのボリュームのリストア](#) (111ページ)

[Elementソフトウェアを実行しているクラスタ上のバックアップからのボリュームのリストア](#) (112ページ)

Amazon S3オブジェクトストア上のバックアップからのボリュームのリストア

プラグインを使用して、Amazon S3オブジェクトストア上のバックアップからボリュームをリストアできます。

手順

1. [NetApp Element Management] > [Reporting]を選択します。
 注：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。
2. [Event Log]サブタブをクリックします。
3. リストアする必要のあるバックアップを作成したバックアップ イベントを選択します。
4. イベントの[Details]ボタンをクリックします。
5. 表示されたメニューで[View Details]をクリックします。
6. マニフェスト情報をクリップボードにコピーします。
7. [Management] > [Volumes]の順にクリックします。
8. [Active]ビューで、リストアするボリュームのチェック ボックスを選択します。
9. [Actions]をクリックします。
10. 表示されたメニューで[Restore from]をクリックします。
11. [Restore Volume]ダイアログ ボックスの[Restore from]で、[Amazon S3]を選択します。
12. [with the following data format]でオプションを選択します。
 - **Native**：NetApp Elementソフトウェアベースのストレージ システムのみが読み取り可能な圧縮形式。
 - **Uncompressed**：他のシステムと互換性がある非圧縮形式。
13. [Host name]フィールドにオブジェクト ストアへのアクセスに使用するホスト名を入力します。
14. [Access key ID]フィールドにアカウントのアクセス キーIDを入力します。
15. [Secret access key]フィールドにアカウントのシークレット アクセス キーを入力します。
16. [Amazon S3 bucket]フィールドにバックアップの格納先とするS3バケットを入力します。
17. [Manifest]フィールドにマニフェスト情報を貼り付けます。
18. [OK]をクリックします。

OpenStack Swiftオブジェクトストア上のバックアップからのボリュームのリストア

プラグインを使用して、OpenStack Swiftオブジェクトストア上のバックアップからボリュームをリストアできます。

手順

1. [NetApp Element Management] > [Reporting]を選択します。
 注：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。

2. [Event Log]サブタブをクリックします。
3. リストアする必要のあるバックアップを作成したバックアップ イベントを選択します。
4. イベントの[Details]ボタンをクリックします。
5. 表示されたメニューで[View Details]をクリックします。
6. マニフェスト情報をクリップボードにコピーします。
7. [Management] > [Volumes]の順にクリックします。
8. [Active]ビューで、リストアするボリュームのチェック ボックスを選択します。
9. [Actions]をクリックします。
10. 表示されたメニューで[Restore from]をクリックします。
11. [Restore Volume]ダイアログ ボックスの[Restore from]で、[OpenStack Swift]を選択します。
12. [with the following data format]でオプションを選択します。
 - **Native** : NetApp Elementソフトウェアベースのストレージ システムのみが読み取り可能な圧縮形式。
 - **Uncompressed** : 他のシステムと互換性がある非圧縮形式。
13. [URL]フィールドにオブジェクト ストアへのアクセスに使用するURLを入力します。
14. [User name]フィールドにアカウントのユーザ名を入力します。
15. [Authentication key]フィールドにアカウントの認証キーを入力します。
16. [Container]フィールドにバックアップが格納されているコンテナの名前を入力します。
17. [Manifest]フィールドにマニフェスト情報を貼り付けます。
18. [OK]をクリックします。

Elementソフトウェアを実行しているクラスタ上のバックアップからのボリュームのリストア

NetApp Elementソフトウェアを実行しているクラスタ上のバックアップからボリュームをリストアできます。クラスタ間でバックアップまたはリストアを実行する際には、システムによってクラスタ間の認証に使用するキーが生成されます。ソース クラスタはこのボリュームの一括書き込みキーを使用してデスティネーション クラスタに対して認証し、デスティネーション ボリュームへの書き込みがセキュリティで保護されます。バックアップまたはリストアを実行する際には、処理を開始する前に、デスティネーション ボリュームからボリュームの一括書き込みキーを生成する必要があります。

手順

1. デスティネーション クラスタを含むvCenterから、[NetApp Element Management] > [Management]を選択します。

注 : 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。
2. [Volumes]サブタブをクリックします。
3. [Active]ビューで、リストアするボリュームのチェック ボックスを選択します。
4. [Actions]をクリックします。

5. 表示されたメニューで[Restore from]をクリックします。
6. [Restore Volume]ダイアログ ボックスの[Restore from]で、[NetApp Element]を選択します。
7. [with the following data format]でオプションを選択します。
 - **Native** : NetApp Elementソフトウェアベースのストレージ システムのみが読み取り可能な圧縮形式。
 - **Uncompressed** : 他のシステムと互換性がある非圧縮形式。
8. [Generate Key]をクリックして、デスティネーション ボリュームに対するボリュームの一括書き込みキーを生成します。
9. ボリュームの一括書き込みキーをクリップボードにコピーします。これは以降のソース クラスタの手順で使用します。
10. ソース クラスタを含むvCenterから、[NetApp Element Management] > [Management]を選択します。
11. [Volumes]サブタブをクリックします。
12. [Active]ビューで、リストアに使用するボリュームのチェック ボックスを選択します。
13. [Actions]をクリックします。
14. 表示されたメニューで[Backup to]をクリックします。
15. ダイアログ ボックスの[Back up volume to]で、[NetApp Element]を選択します。
16. [with the following data format]で、バックアップに一致するオプションを選択します。
17. [Remote cluster MVIP]フィールドにデスティネーション ボリュームのクラスタの管理仮想IPアドレスを入力します。
18. [Remote cluster user name]フィールドにデスティネーション クラスタのクラスタ管理者のユーザ名を入力します。
19. [Remote cluster user password]フィールドにデスティネーション クラスタのクラスタ管理者のパスワードを入力します。
20. デスティネーション クラスタで生成したキーを[Bulk volume write key]フィールドに貼り付けます。
21. [OK]をクリックします。

ボリュームの削除

NetApp Element Management拡張ポイントを使用して、NetApp Elementクラスタから1つ以上のボリュームを削除できます。

タスク概要

削除したボリュームはすぐにパージされるわけではありません。ボリュームを削除したあと約8時間はリストア可能です。パージされる前のボリュームはリストアできます。また、[Management] > [Volumes]の[Deleted]ビューから手動でボリュームをパージすることもできます。ボリュームをリストアすると、そのボリュームがオンラインに戻り、iSCSI接続を再確立できます。

注意: Snapshotの作成に使用したボリュームを削除すると、関連するSnapshotが、[Protection] > [Snapshots]ページの[Inactive]ビューに表示されます。削除したソース ボリュームをパージすると、[Inactive]ビューのSnapshotはシステムからも削除されます。

注：管理ノードによって作成された永続ボリュームは削除しないでください（該当する場合）。

手順

1. [NetApp Element Management] > [Management]を選択します。

注：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。

2. [Volumes]サブタブをクリックします。
3. 次の手順で1つ以上のボリュームを削除します。

- a. [Active]ビューで、削除する各ボリュームのチェックボックスを選択します。
- b. [Actions]をクリックします。
- c. 表示されたメニューで[Delete]をクリックします。

注：プラグインでは、データストアを含むボリュームは削除できません。

- d. 操作を確定します。

[Volumes]ページで、ボリュームが[Active]ビューから[Deleted]ビューに移動します。

関連タスク

[削除したボリュームのリストア](#)（115ページ）

ボリュームのパージ

削除したボリュームを手動でパージできます。

タスク概要

削除したボリュームは、8時間後に自動的にパージされます。ただし、スケジュールされているパージ時刻より前にボリュームをパージする場合は、次の手順に従って手動でパージできます。

注意：パージしたボリュームは、システムからただちに完全に削除されます。ボリューム内のデータはすべて失われます。

手順

1. [NetApp Element Management] > [Management]を選択します。

注：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。

2. [Volumes]サブタブをクリックします。
3. ビュー フィルタを選択し、ドロップダウン リストから[Deleted]を選択します。
4. パージするボリュームを1つ以上選択します。
5. [Purge]をクリックします。
6. 操作を確定します。

削除したボリュームのリストア

NetApp Elementシステムでは、削除したボリュームのうち、パージされていないボリュームをリストアできます。

タスク概要

削除したボリュームは約8時間後に自動的にパージされます。パージ済みのボリュームはリストアできません。

注：削除したあとにリストアしたボリュームは、ESXiで検出されません（データストアが存在する場合はデータストアも検出されません）。ESXi iSCSIアダプタから静的なターゲットを削除し、アダプタを再スキャンしてください。

手順

1. [NetApp Element Management] > [Management]を選択します。
注：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。
2. [Volumes]サブタブをクリックします。
3. ビュー フィルタを選択し、ドロップダウン リストから[Deleted]を選択します。
4. リストアするボリュームを1つ以上選択します。
5. [Restore]をクリックします。
6. ビュー フィルタを選択し、ドロップダウン リストから[Active]を選択します。
7. ボリュームとすべての接続がリストアされたことを確認します。

アクセス グループへのボリュームの追加

ボリューム アクセス グループにボリュームを追加することができます。各ボリュームは、複数のボリューム アクセス グループに属することが可能です。各ボリュームが属しているグループは、[Active]ボリューム ビューで確認できます。

開始する前に

- クラスタが少なくとも1つ追加および実行されている必要があります。
- 少なくとも1つのアクセス グループが必要です。
- 少なくとも1つのアクティブなボリュームが必要です。

手順

1. [NetApp Element Management] > [Management]を選択します。
注：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。
2. [Volumes]サブタブをクリックします。
3. アクセス グループに追加する各ボリュームのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで、[Add to Access Group]を選択します。

6. 表示されたダイアログ ボックスで詳細を確認し、ドロップダウン 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. [OK]をクリックします。

関連タスク

[ボリュームの作成](#) (99ページ)

[アクセス グループの作成](#) (120ページ)

アクセス グループからのボリュームの削除

アクセス グループからボリュームを削除できます。

タスク概要

アクセス グループからボリュームを削除すると、グループはそのボリュームにアクセスできなくなります。

注意: アクセス グループからボリュームを削除すると、ボリュームへのホスト アクセスが中断される可能性があります。

手順

1. [NetApp Element Management] > [Management]を選択します。
注: 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。
2. [Volumes]サブタブをクリックします。
3. アクセス グループから削除する各ボリュームのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Remove from Access Group]を選択します。
6. 表示されたダイアログ ボックスで詳細を確認し、選択した各ボリュームへのアクセスを中止するボリューム アクセス グループを選択します。
7. [OK]をクリックします。

複数のボリュームへのQoSポリシーの適用

既存のQoSポリシーを複数のボリュームに適用することができます。このプロセスは、ポリシーを1つ以上のボリュームに一括して適用する場合に使用します。

開始する前に

一括して適用するQoSポリシーを用意しておきます。

手順

1. [NetApp Element Management] > [Management]を選択します。
2. [Volumes]サブタブをクリックします。
3. QoSポリシーを適用する各ボリュームのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Apply QoS Policy]を選択します。

6. ダイアログ ボックスで、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。
7. [OK]をクリックします。

関連タスク

[QoSポリシーの作成](#) (125ページ)

ボリュームのQoSポリシーの関連付けの変更

NetApp Element Management拡張ポイントを使用して、QoSポリシーのボリュームへの関連付けを解除したり、別のQoSポリシーやカスタムのQoS設定を選択したりできます。

開始する前に

変更するボリュームにQoSポリシーが関連付けられていることが前提です。

手順

1. [NetApp Element Management] > [Management]を選択します。
 注：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。
2. [Volumes]サブタブをクリックします。
3. 変更するQoSポリシーが含まれているボリュームのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Edit]を選択します。
6. ダイアログ ボックスの[Quality of Service]で、ボリュームに適用する新しいQoSポリシーまたはカスタム設定を選択します。
7. [Custom Settings]を選択した場合は、[Min IOPS]、[Max IOPS]、および[Burst IOPS]の値を変更します。
 注：[Reset Default QoS]をクリックすると、デフォルトのIOPS値に戻すことができます。
8. [OK]をクリックします。

ユーザ アカウントの管理

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は、ストレージ コンテナがアカウントになります。アカウントには、そのアカウントに関連付け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。アカウントに関連付けることのできるボリュームの最大数は2,000ですが、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。

アカウントの作成

アカウントを作成し、ボリュームへのアクセスを許可することができます。作成したアカウント1つにつき、最大で2000個のボリュームを割り当てることができます。各アカウント名はシステム内で一意である必要があります。

開始する前に

クラスタが少なくとも1つ追加および実行されている必要があります。

手順

1. [NetApp Element Management] > [Management]を選択します。

注：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。

2. [Accounts]サブタブをクリックします。

3. [Create Account]をクリックします。

4. ユーザ名を入力します。

ヒント：わかりやすい命名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。

5. [CHAP Settings]セクションで次の手順を実行します。

- a. ノードセッションのCHAP認証用イニシエータシークレットを入力します。

- b. ノードセッションのCHAP認証用ターゲットシークレットを入力します。

注：イニシエータとターゲットには違うシークレットを指定する必要があります。これらのフィールドを空白にすると、システムによって認証クレデンシャルが生成されます。

6. [OK]をクリックします。

アカウントの詳細

NetApp Element Management拡張ポイントの[Management]タブにある[Accounts]ページで、すべてのアカウントのリストを確認できます。

Account ID

システムによって生成されたアカウントのID。

User name

アカウントの作成時に指定した名前。

Number of Volumes

アカウントに割り当てられているアクティブ ボリュームの数。

Status

アカウントのステータス。

アカウントの編集

アカウントを編集して、ステータスまたはCHAPシークレットを変更できます。CHAP設定を変更すると、ホストと関連付けられたボリュームの間の接続が切断されることがあります。

タスク概要

管理ノードに永続ボリュームを使用している場合は、永続ボリュームに関連付けられているアカウントの名前を変更しないでください。

手順

1. [NetApp Element Management] > [Management]を選択します。
注：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。
2. [Accounts]サブタブをクリックします。
3. 編集するアカウントのチェックボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Edit]をクリックします。
6. オプション：[Edit Account]で、アカウントのアクセスステータスを編集します。
注意：アクセスを[Locked]に変更すると、そのアカウントへのiSCSI接続はすべて停止され、そのアカウントにはアクセスできなくなります。アカウントに関連付けられているボリュームは維持されますが、iSCSIで検出できなくなります。
7. オプション：ノードセッションの認証に使用するイニシエータシークレットとターゲットシークレットのクレデンシャルを編集します。
注：クレデンシャルを変更しない場合、同じクレデンシャルが使用されます。クレデンシャルのフィールドを空白にすると、システムによって新しいパスワードが生成されます。
8. [OK]をクリックします。

アカウントの削除

ボリュームの関連付けを解除したアカウントは、NetApp Element Management拡張ポイントを使用して削除できます。

開始する前に

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するか、別のアカウントに割り当て直します。

タスク概要

管理ノードに永続ボリュームを使用している場合、永続ボリュームに関連付けられているアカウントは削除しないでください。

手順

1. [NetApp Element Management] > [Management]を選択します。

注：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。

2. [Accounts]サブタブをクリックします。
3. 削除するアカウントのチェックボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Delete]を選択します。
6. 操作を確定します。

関連タスク

[ボリュームの削除](#) (113ページ)

[ボリュームのパージ](#) (114ページ)

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。

アクセスグループを作成するには、iSCSIイニシエータのIQNまたはFibre ChannelのWWPNをボリュームのグループにマッピングします。アクセスグループに追加した各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した各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。

注：ボリューム アクセス グループには次の制限があります。

- 1つのアクセスグループに含めることができるIQNまたはWWPNは最大64個です。
- 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アクセスグループは1つだけです。
- 1つのボリュームが最大4つのアクセスグループに属することができます。

ボリューム アクセス グループは、NetApp Element Management拡張ポイントで管理できます。

アクセスグループの作成

1つ以上のイニシエータを含むボリューム アクセス グループを作成できます。クライアントのFibre Channel (WWPN) イニシエータまたはiSCSI (IQN) イニシエータをボリューム アクセスグループ内のボリュームにマッピングすることで、ネットワークとボリュームの間の安全なデータI/O通信が実現します。

手順

1. [NetApp Element Management] > [Management]を選択します。

注：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。

2. [Access Groups]サブタブをクリックします。
3. [Create Access Group]をクリックします。

4. ボリューム アクセス グループの名前を入力します。

ヒント: わかりやすい命名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。

5. **[Select an Initiator]** ドロップダウン リストから未割り当てのIQNまたはWWPNを選択し、**[Add Initiator]** をクリックします。

注: イニシエータは、ボリューム アクセス グループの作成後に追加または削除できます。

6. **[OK]** をクリックします。

ボリューム アクセス グループの詳細

NetApp Element Management拡張ポイントの**[Management]** タブにある**[Access Groups]** ページで、ボリューム アクセス グループの情報を確認できます。

ID

システムによって生成されたボリューム アクセス グループのID。

Name

ボリューム アクセス グループの作成時に指定した名前。

Active Volumes

ボリューム アクセス グループ内のアクティブ ボリュームの数。

Initiators

ボリューム アクセス グループに接続されているイニシエータの数。

アクセス グループの編集

NetApp Element Management拡張ポイントで、ボリューム アクセス グループの名前を編集したり、イニシエータの追加や削除を行ったりすることができます。

手順

1. **[NetApp Element Management]** > **[Management]** を選択します。

注: 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。

2. **[Access Groups]** サブタブをクリックします。
3. 編集するボリューム アクセス グループのチェック ボックスを選択します。
4. **[Actions]** をクリックします。
5. 表示されたメニューで**[Edit]** を選択します。
6. オプション: アクセス グループの名前を変更します。
7. オプション: イニシエータを追加または削除します。

注: イニシエータを削除するときは、ごみ箱アイコンをクリックして削除します。イニシエータを削除すると、そのイニシエータは該当するボリューム アクセス グループ内のボリュームにアクセスできなくなります。ボリュームへの通常のアカウントアクセスは引き続き可能です。

8. **[OK]** をクリックします。

アクセス グループの削除

NetApp Element Management拡張ポイントを使用して、ボリューム アクセス グループを削除できます。ボリューム アクセス グループを削除する前に、イニシエータIDを削除したり、グループとボリュームの関連付けを解除したりする必要はありません。アクセス グループを削除すると、ボリュームへのグループ アクセスが切断されます。

手順

1. **[NetApp Element Management] > [Management]**を選択します。
注：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。
2. **[Access Groups]**サブタブをクリックします。
3. 削除するボリューム アクセス グループのチェック ボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Delete]**を選択します。
6. 操作を確定します。

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。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することができます。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、グループ内のすべてのボリュームへのアクセスが可能になります。

イニシエータは、NetApp Element Management拡張ポイントの**[Management] > [Initiators]**ページで確認できます。

イニシエータの作成

iSCSI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。

手順

1. **[NetApp Element Management] > [Management]**を選択します。
注：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。
2. **[Initiators]**サブタブをクリックします。
3. **[Create Initiator]**をクリックします。
4. 単一のイニシエータを作成するには、次の手順を実行します。
 - a. **[Create a Single Initiator]**を選択します。
 - b. イニシエータのIQNまたはWWPNを**[IQN/WWPN]**フィールドに入力します。

- 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 (:)、ダッシュ (-) です。
形式の例を次に示します。

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

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

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

- c. イニシエータのフレンドリ名を[Alias]フィールドに入力します。
5. 複数のイニシエータを作成するには、次の手順を実行します。
 - a. **[Create Multiple Initiators]**を選択します。
 - b. 次のいずれかを実行します。
 - **[Scan Hosts]**をクリックして、vSphereホストをスキャンしてNetApp Elementクラスターで定義されていないイニシエータ値を検索します。
 - IQNまたはWWPNのリストをテキスト ボックスに入力し、**[Add Initiators]**をクリックします。
 - c. オプション : **[Alias]**で、エイリアスを追加する各エントリのフィールドをクリックします。
 - d. オプション : 必要に応じて、リストからイニシエータを削除します。
6. **[OK]**をクリックします。

イニシエータの詳細

NetApp Element Management拡張ポイントの[Management]タブにある[Initiators]ページでは、イニシエータに関する情報を確認できます。

ID

システムによって生成されたイニシエータのID。

Name

イニシエータの作成時に指定した名前。

Alias

イニシエータに指定したフレンドリ名 (該当する場合)。

Access Group

イニシエータが所属するボリューム アクセス グループ。

イニシエータの編集

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. **[NetApp Element Management] > [Management]**を選択します。

注：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。

2. **[Initiators]**サブタブをクリックします。
3. 編集するイニシエータのチェックボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Edit]**をクリックします。
6. イニシエータの新しいエイリアスを**[Alias]**フィールドに入力します。
7. **[OK]**をクリックします。

イニシエータの削除

不要になった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、関連す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。該当する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. **[NetApp Element Management] > [Management]**を選択します。
注：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。
2. **[Initiators]**サブタブをクリックします。
3. 削除するイニシエータのチェックボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Delete]**を選択します。
6. 操作を確定します。

ボリューム アクセス グループへのイニシエータの追加

アクセス グループにイニシエータを追加すると、そのイニシエータはボリューム アクセス グループ内のボリュームにCHAP認証なしでアクセスできるようになります。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、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ます。

手順

1. **[NetApp Element Management] > [Management]**を選択します。
注：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。
2. **[Initiators]**サブタブをクリックします。
3. アクセス グループに追加するイニシエータのチェックボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Add to Access Group]**をクリックします。
6. **[Add to Access Group]**ダイアログで、ドロップダウン リストからアクセス グループを選択します。

7. [OK]をクリックします。

QoSポリシー

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ポリシーは作成、編集、および削除できます。

QoSポリシーは、NetApp Element Management拡張ポイントの[Management] > [QoS Policies] ページで確認できます。

注：QoSポリシーを使用する場合は、QoSSIOCを有効にしないでください。QoSSIOCはボリュームのQoS設定よりも優先されます。

注：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。

QoSポリシーの作成

NetApp Element Management拡張ポイントからQoSポリシーを作成し、ボリュームの作成時に適用することができます。

手順

1. [NetApp Element Management] > [Management]を選択します。

注：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。

2. [QoS Policies]サブタブをクリックします。
3. [Create QoS Policy]をクリックします。
4. [Policy Name]を入力します。

ヒント：わかりやすい命名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。

5. [Min IOPS]、[Max IOPS]、および[Burst IOPS]の値を入力します。
6. [OK]をクリックします。

QoSポリシーの詳細

NetApp Element Management拡張ポイントの[Management]タブにある[QoS Policies]ページで、QoSポリシーに関する情報を確認できます。

ID

システムによって生成されたQoSポリシーのID。

Name

ユーザが定義したQoSポリシーの名前。

Min IOPS

ボリュームに対して保証されている最小IOPS。

Max IOPS

ボリュームに対して許可されている最大IOPS。

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。

Volumes

ポリシーを使用しているボリュームの数。数字をクリックすると、ポリシーが適用されたボリュームのリストが表示されます。

QoSポリシーの編集

NetApp Element Management拡張ポイントで、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ポリシーの変更は、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に反映されます。

手順

1. **[NetApp Element Management] > [Management]**を選択します。
注：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。
2. **[QoS Policies]**サブタブをクリックします。
3. 編集するQoSポリシーのチェックボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Edit]**を選択します。
6. **[Edit QoS Policy]**ダイアログボックスで、必要に応じて次のプロパティを変更します。
 - **Policy Name**
 - **Min IOPS**
 - **Max IOPS**
 - **Burst IOPS****注：****[Reset Default QoS]**をクリックすると、デフォルトのIOPS値に戻すことができます。
7. **[OK]**をクリックします。

QoSポリシーの削除

NetApp Element Management拡張ポイントから、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設定は維持されますが、ポリシーとの関連付けは解除されます。

手順

1. **[NetApp Element Management] > [Management]**を選択します。
注：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。
2. **[QoS Policies]**サブタブをクリックします。
3. 削除するQoSポリシーのチェックボックスを選択します。
4. **[Actions]**をクリックします。

5. 表示されたメニューで[Delete]を選択します。
6. 操作を確定します。

データ保護

[Protection]タブでは、データのコピーが必要な場所に確実に作成されて格納されるようにするためのタスクを実行できます。具体的には、ボリュームSnapshot、グループSnapshot、およびSnapshotスケジュールの作成と管理、リモート クラスタ間のレプリケーションのためのボリューム ペア関係とクラスタ ペア関係の作成です。

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 コピーです。ボリュームSnapshotの作成は少量のシステム リソースとスペースしか使用しないため、クローニングよりも短い時間で完了します。Snapshotを使用して、Snapshotが作成された時点の状態にボリュームをロールバックできます。ただし、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。

SnapshotをリモートのNetApp Element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。

ボリュームSnapshotは、[NetApp Element Management] > [Management] > [Volumes]ページで作成できます。作成したボリュームSnapshotは、[NetApp Element Management] > [Protection] > [Snapshots]ページで管理できます。

ボリュームSnapshotの作成

アクティブ ボリュームのSnapshotを作成すると、任意の時点におけるボリューム イメージを保持できます。Snapshotを今すぐ作成するか、スケジュールを作成してボリュームのSnapshotがあとで自動的に作成されるようにすることができます。1つのボリュームに最大32個のSnapshotを作成できます。

手順

1. [NetApp Element Management] > [Management]を選択します。
注：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。
2. [Volumes]サブタブをクリックします。
3. [Active]ビューで、Snapshotに使用するボリュームのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Create Snapshot]を選択します。
6. オプション：[Create Snapshot]ダイアログ ボックスで、Snapshotの名前を入力します。
ヒント：わかりやすい命名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。

注：Snapshotの名前を入力しなかった場合、デフォルトではSnapshotの作成日時が名前として使用されます。

7. オプション: 親ボリュームがペアリングされている場合にレプリケーションにSnapshotも含まれるようにするには、**[Include snapshot in replication when paired]**チェックボックスを選択します。
8. Snapshotの保持期間として次のいずれかを選択します。
 - **Keep forever** : Snapshotをシステム上に無期限に保持します。
 - **Set retention period** : Snapshotをシステム上に保持する期間（日数、時間、または分）を設定します。

注 : 保持期間には、（Snapshotの作成時間からではなく）現在の時刻からの期間を指定します。
9. 単一のSnapshotを今すぐ作成するには、**[Take snapshot now]**を選択します。
10. スケジュールを設定してあとでSnapshotを作成するには、次の手順を実行します。
 - a. **[Create snapshot schedule]**を選択します。
 - b. スケジュール名を入力します。
 - c. スケジュールタイプをリストから選択し、スケジュールの詳細を設定します。
 - d. オプション: スケジュールしたSnapshotの作成を定期的に繰り返すには、**[Recurrent Schedule]**チェックボックスを選択します。
11. **[OK]**をクリックします。

ボリュームSnapshotの詳細

NetApp Element Management拡張ポイントの**[Protection]**タブにある**[Snapshots]**ページで、クラスタ上のボリュームSnapshotに関する情報を確認できます。

次のビューでSnapshotをフィルタすることもできます。

- **Individual** : グループSnapshotのメンバーではないボリュームSnapshot。
- **Members** : グループSnapshotのメンバーであるボリュームSnapshot。
- **Inactive** : 削除されたがまだパーージされていないボリュームから作成されたボリュームSnapshot。

ID

システムによって生成されたSnapshotのID。

Snapshot UUID

Snapshotの一意のID。

Name

Snapshotのユーザが定義した名前またはシステムのデフォルト名。

Size

ユーザが定義したSnapshotのサイズ。

Volume ID

Snapshotの作成元のボリュームのID。

Volume Name

ユーザが定義したボリュームの名前。

Account

ボリュームに関連付けられているアカウント。

Volume Size

Snapshotの作成元のボリュームのサイズ。

Create Date

Snapshotが作成された日時。

Expiration Date

保持期間の定義に従ってSnapshotが削除される日時。

Group Snapshot ID

Snapshotが属するグループのID（他のボリュームSnapshotとグループ化されている場合）。

Remote Replication

NetApp Elementソフトウェアを実行しているリモート クラスタへのSnapshotのレプリケーションが有効かどうかを示します。

有効な値は次のとおりです。

- True : Snapshotのリモート レプリケーションが有効です。
- False : Snapshotのリモート レプリケーションが無効です。

Remote Status

NetApp Elementソフトウェアを実行しているリモート クラスタ上のSnapshotのステータスを示します。

有効な値は次のとおりです。

- Present : リモート クラスタにSnapshotが存在します。
- Not Present : リモート クラスタにSnapshotが存在しません。
- Syncing : ターゲット クラスタがSnapshotをレプリケート中です。
- Deleted : ターゲットがSnapshotをレプリケートしたあとで削除しました。

Snapshotの編集

Snapshotのレプリケーション設定または保持期間を変更できます。指定した保持期間は、新しい間隔の開始時点からの期間です。保持期間には、（Snapshotの作成時間からではなく）現在の時刻からの期間を指定します。間隔は、分、時間、および日数で指定できます。

手順

1. [NetApp Element Management] > [Protection]を選択します。

注 : 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。

2. [Snapshots]サブタブで、次の2つのうちのどちらかのビューを選択します。

- **Individual** : グループSnapshotのメンバーではないボリュームSnapshot。
- **Members** : グループSnapshotのメンバーであるボリュームSnapshot。

3. 編集するボリュームSnapshotのチェック ボックスを選択します。

4. [Actions]をクリックします。

5. 表示されたメニューで[Edit]を選択します。

6. オプション: 親ボリュームがペアリングされている場合にレプリケーションにSnapshotも含まれるようにするには、**[Include snapshot in replication when paired]**チェックボックスを選択します。
7. オプション: Snapshotの保持期間として次のいずれかを選択します。
 - **Keep forever**: Snapshotをシステム上に無期限に保持します。
 - **Set retention period**: Snapshotをシステム上に保持する期間（日数、時間、または分）を設定します。

注: 保持期間には、(Snapshotの作成時間からではなく) 現在の時刻からの期間を指定します。
8. **[OK]**をクリックします。

Snapshotからのボリュームのクローニング

ボリュームのSnapshotから新しいボリュームを作成できます。この処理では、Snapshotの作成時点でボリュームに含まれていたデータを使用して新しいボリュームをクローニングします。ボリュームの他のSnapshotに関する情報も新しく作成されたボリュームに保存されます。

手順

1. **[NetApp Element Management] > [Protection]**を選択します。

注: 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。
2. **[Snapshots]**サブタブで、次の2つのうちのどちらかのビューを選択します。
 - **Individual**: グループSnapshotのメンバーではないボリュームSnapshot。
 - **Members**: グループSnapshotのメンバーであるボリュームSnapshot。
3. ボリュームとしてクローニングするボリュームSnapshotのチェックボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで、**[Clone Volume from Snapshot]**をクリックします。
6. **[Clone Volume from Snapshot]**ダイアログボックスで、ボリューム名を入力します。
7. 新しいボリュームの合計サイズを入力し、単位（GBまたはGiB）を選択します。
8. ボリュームのアクセスタイプを選択します。
 - **Read Only**: 読み取り処理のみ可能です。
 - **Read / Write**: 読み取りと書き込みが可能です。
 - **Locked**: 読み取りも書き込みもできません。
 - **Replication Target**: レプリケートされたボリューム ペアのターゲットボリュームとして指定されます。
9. 新しいボリュームに関連付けるユーザ アカウントをリストから選択します。
10. **[OK]**をクリックします。
11. **[NetApp Element Management] > [Management]**を選択します。

12. **[Volumes]**サブタブをクリックします。
13. **[Active]**ビューで、新しいボリュームがリストに表示されていることを確認します。
注：新しいボリュームがリストに表示されるまで、必要に応じてページを更新します。

Snapshotへのボリュームのロールバック

ボリュームはSnapshotにいつでもロールバックできます。そのSnapshotの作成後にボリュームに対して行われた変更はすべて元に戻ります。

手順

1. **[NetApp Element Management] > [Protection]**を選択します。
注：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。
2. **[Snapshots]**サブタブで、次の2つのうちのどちらかのビューを選択します。
 - **Individual**：グループSnapshotのメンバーではないボリュームSnapshot。
 - **Members**：グループSnapshotのメンバーであるボリュームSnapshot。
3. ボリュームのロールバックに使用するボリュームSnapshotのチェックボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Rollback Volume to Snapshot]**を選択します。
6. オプション：Snapshotにロールバックする前にボリュームの現在の状態を保存するには、次の手順を実行します。
 - a. **[Rollback to Snapshot]**ダイアログボックスで、**[Save volume's current state as a snapshot]**を選択します。
 - b. 新しいSnapshotの名前を入力します。
7. **[OK]**をクリックします。

ボリュームSnapshotのバックアップ処理

統合型バックアップ機能を使用して、ボリュームSnapshotをバックアップできます。Snapshotは、NetApp Elementソフトウェアを実行しているクラスタから外部のオブジェクトストア、またはElementベースの別の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、読み取りおよび書き込み処理が許可されている必要があります。

関連タスク

[Amazon S3オブジェクトストアへのボリュームSnapshotのバックアップ](#)（133ページ）
[OpenStack SwiftオブジェクトストアへのボリュームSnapshotのバックアップ](#)（133ページ）
[Elementソフトウェアを実行しているクラスタへのボリュームSnapshotのバックアップ](#)（134ページ）

Amazon S3オブジェクトストアへのボリュームSnapshotのバックアップ

Amazon S3と互換性のある外部のオブジェクトストアにNetApp Element Snapshotをバックアップできます。

手順

1. **[NetApp Element Management] > [Protection]**を選択します。
注：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。
2. **[Snapshots]**サブタブで、バックアップするボリュームSnapshotのチェックボックスを選択します。
3. **[Actions]**をクリックします。
4. 表示されたメニューで**[Backup to]**をクリックします。
5. ダイアログの**[Back up volume to]**で、**[Amazon S3]**を選択します。
6. **[with the following data format]**でオプションを選択します。
 - **Native**：NetApp Elementソフトウェアベースのストレージシステムのみが読み取り可能な圧縮形式。
 - **Uncompressed**：他のシステムと互換性がある非圧縮形式。
7. **[Host name]**フィールドにオブジェクトストアへのアクセスに使用するホスト名を入力します。
8. **[Access key ID]**フィールドにアカウントのアクセスキーIDを入力します。
9. **[Secret access key]**フィールドにアカウントのシークレットアクセスキーを入力します。
10. **[Amazon S3 Bucket]**フィールドにバックアップの格納先とするS3バケットを入力します。
11. オプション：**[Prefix]**フィールドにバックアップ名のプレフィックスを入力します。
12. オプション：**[Nametag]**フィールドにプレフィックスに付加するネームタグを入力します。
13. **[OK]**をクリックします。

OpenStack SwiftオブジェクトストアへのボリュームSnapshotのバックアップ

OpenStack Swiftと互換性のあるセカンダリオブジェクトストアにNetApp Element Snapshotをバックアップできます。

手順

1. **[NetApp Element Management] > [Protection]**を選択します。
注：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。
2. **[Snapshots]**サブタブで、バックアップするボリュームSnapshotのチェックボックスを選択します。
3. **[Actions]**をクリックします。

4. 表示されたメニューで[Backup to]をクリックします。
5. ダイアログ ボックスの[Back up volume to]で、[OpenStack Swift]を選択します。
6. [with the following data format]でオプションを選択します。
 - **Native** : NetApp Elementソフトウェアベースのストレージ システムのみが読み取り可能な圧縮形式。
 - **Uncompressed** : 他のシステムと互換性がある非圧縮形式。
7. [URL]フィールドにオブジェクトストアへのアクセスに使用するURLを入力します。
8. [User name]フィールドにアカウントのユーザ名を入力します。
9. [Authentication key]フィールドにアカウントの認証キーを入力します。
10. [Container]フィールドにバックアップの格納先とするコンテナを入力します。
11. オプション : [Prefix]フィールドにバックアップ ボリュームの名前のプレフィックスを入力します。
12. オプション : [Nametag]フィールドにプレフィックスに付加するネーム タグを入力します。
13. [OK]をクリックします。

Elementソフトウェアを実行しているクラスタへのボリュームSnapshotのバックアップ

NetApp Elementソフトウェアを実行しているクラスタにあるボリュームSnapshotをリモートのElementクラスタにバックアップできます。

開始する前に

バックアップに使用するSnapshotと同じかそれ以上のサイズのデスティネーション クラスタにボリュームを作成する必要があります。

タスク概要

クラスタ間でバックアップまたはリストアを実行する際には、システムによってクラスタ間の認証に使用するキーが生成されます。ソース クラスタはこのボリュームの一括書き込みキーを使用してデスティネーション クラスタに対して認証し、デスティネーション ボリュームへの書き込みがセキュリティで保護されます。バックアップまたはリストアを実行する際には、処理を開始する前に、デスティネーション ボリュームからボリュームの一括書き込みキーを生成する必要があります。

手順

1. デスティネーション クラスタを含むvCenterから、[NetApp Element Management] > [Management]を選択します。

注 : 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。
2. [Volumes]サブタブで、デスティネーション ボリュームのチェック ボックスを選択します。
3. [Actions]をクリックします。
4. 表示されたメニューで[Restore from]をクリックします。
5. ダイアログ ボックスの[Restore from]で、[NetApp Element]を選択します。

6. **[with the following data format]**でオプションを選択します。
 - **Native** : NetApp Elementソフトウェアベースのストレージ システムのみが読み取り可能な圧縮形式。
 - **Uncompressed** : 他のシステムと互換性がある非圧縮形式。
7. **[Generate Key]**をクリックして、デスティネーション ボリュームに対するボリュームの一括書き込みキーを生成します。
8. ボリュームの一括書き込みキーをクリップボードにコピーします。これは以降のソース クラスタの手順で使用します。
9. ソース クラスタを含むvCenterから、**[NetApp Element Management]** > **[Protection]**を選択します。

注 : 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。
10. バックアップに使用するSnapshotのチェック ボックスを選択します。
11. **[Actions]**をクリックします。
12. 表示されたメニューで**[Backup to]**をクリックします。
13. ダイアログ ボックスの**[Back up volume to]**で、**[NetApp Element]**を選択します。
14. **[with the following data format]**で、デスティネーション クラスタと同じオプションを選択します。
15. **[Remote cluster MVIP]**フィールドにデスティネーション ボリュームのクラスタの管理仮想IPアドレスを入力します。
16. **[Remote cluster user name]**フィールドにリモート クラスタのユーザ名を入力します。
17. **[Remote cluster user password]**フィールドにリモート クラスタのパスワードを入力します。
18. デスティネーション クラスタで生成したキーを**[Bulk volume write key]**フィールドに貼り付けます。
19. **[OK]**をクリックします。

Snapshotの削除

NetApp Element Management拡張ポイントを使用して、NetApp Elementソフトウェアを実行しているクラスタからボリュームSnapshotを削除できます。削除したSnapshotは、システムからただちに削除されます。

タスク概要

レプリケート中のSnapshotをソース クラスタから削除できます。ターゲット クラスタと同期中のSnapshotを削除すると、同期レプリケーションが完了した時点でソース クラスタからSnapshotが削除されます。ターゲット クラスタからは削除されません。

ターゲットにレプリケート済みのSnapshotを、ターゲット クラスタから削除することもできます。削除したSnapshotは、ターゲットがソース クラスタでSnapshotが削除されたことを検知するまで、ターゲットの削除済みSnapshotのリストに保持されます。ソースSnapshotが削除されたことをターゲットが検知すると、ターゲットはそのSnapshotのレプリケーションを停止します。

手順

1. **[NetApp Element Management] > [Protection]**を選択します。

注：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。

2. **[Snapshots]**サブタブで、次の2つのうちのどちらかのビューを選択します。

- **Individual**：グループSnapshotに属していないボリュームSnapshotのリスト。
- **Inactive**：削除されたがまだパージされていないボリュームから作成されたボリュームSnapshotのリスト。

注：**[Snapshots]**サブタブでは、グループSnapshotの個々のメンバーを削除することはできません。この場合はグループSnapshotを削除する必要があります。グループSnapshotを削除する際のオプションで、グループSnapshotのメンバーを個別のSnapshotに変換する（グループSnapshotの関連付けを解除する）ことができます。

3. 削除するボリュームSnapshotのチェックボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Delete]**を選択します。
6. 操作を確定します。

グループSnapshot

関連する一連のボリュームのグループSnapshotを作成して、各ボリュームのメタデータのポイントインタイムコピーを保持できます。グループSnapshotをバックアップまたはロールバックとして使用して、ボリュームグループの状態を希望する時点にリストアすることができます。

グループSnapshotの作成

ボリュームグループのSnapshotを今すぐ作成するか、スケジュールを作成してボリュームグループのSnapshotがあとで自動的に作成されるようにすることができます。1つのグループSnapshotには一度に最大32個のボリュームのSnapshotを含めることができます。

手順

1. **[NetApp Element Management] > [Management]**を選択します。

注：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。

2. **[Volumes]**サブタブをクリックします。
3. **[Active]**ビューで、Snapshotに使用する各ボリュームのチェックボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Create Group Snapshot]**を選択します。
6. オプション：**[Create Group Snapshot]**ダイアログボックスで、グループSnapshotの名前を入力します。

ヒント：わかりやすい命名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。

注：グループSnapshotの名前を入力しなかった場合、デフォルトではSnapshotの作成日時が名前として使用されます。

7. オプション: 親ボリュームがペアリングされている場合にレプリケーションにSnapshotも含まれるようにするには、**[Include snapshot in replication when paired]**チェックボックスを選択します。
8. Snapshotの保持期間として次のいずれかを選択します。
 - **Keep forever** : Snapshotをシステム上に無期限に保持します。
 - **Set retention period** : Snapshotをシステム上に保持する期間（日数、時間、または分）を設定します。

注：保持期間には、（Snapshotの作成時間からではなく）現在の時刻からの期間を指定します。
9. 単一のSnapshotを今すぐ作成するには、**[Take group snapshot now]**を選択します。
10. スケジュールを設定してあとでSnapshotを作成するには、次の手順を実行します。
 - a. **[Create snapshot schedule]**を選択します。
 - b. スケジュール名を入力します。
 - c. スケジュールタイプをリストから選択し、スケジュールの詳細を設定します。
 - d. オプション: スケジュールしたSnapshotの作成を定期的に繰り返すには、**[Recurrent Schedule]**チェックボックスを選択します。
11. **[OK]**をクリックします。

グループSnapshotの詳細

NetApp Element Management拡張ポイントの**[Protection]**タブにある**[Snapshots]**ページで、グループSnapshotに関する情報を確認できます。

Snapshot Group ID

システムによって生成されたグループSnapshotのID。

Unique ID

グループSnapshotの一意のID。

Snapshot Group Name

グループSnapshotのユーザが定義した名前またはシステムのデフォルト名。

Create Date

グループSnapshotが作成された日時。

Status

Snapshotの現在のステータス。

有効な値は次のとおりです。

- **Preparing** : Snapshotは使用準備中で、まだ書き込みができません。
- **Done** : Snapshotの準備が完了し、使用可能な状態です。
- **Active** : Snapshotはアクティブです。

Number of Volumes

グループSnapshot内のボリュームの数。

グループSnapshotの編集

グループSnapshotのレプリケーション設定または保持期間を変更できます。指定した保持期間は、新しい間隔の開始時点からの期間です。保持期間には、（Snapshotの作成時間からではなく）現在の時刻からの期間を指定します。間隔は、分、時間、および日数で指定できます。

手順

1. **[NetApp Element Management] > [Protection]**を選択します。
注：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。
2. **[Group Snapshots]**サブタブをクリックします。
3. 編集するグループSnapshotのチェックボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Edit]**を選択します。
6. オプション：親ボリュームがペアリングされている場合にレプリケーションにSnapshotも含まれるようにするには、**[Include snapshot in replication when paired]**チェックボックスを選択します。
7. オプション：Snapshotの保持期間として次のいずれかを選択します。
 - Keep forever：Snapshotをシステム上に無期限に保持します。
 - Set retention period：Snapshotをシステム上に保持する期間（日数、時間、または分）を設定します。**注：**保持期間には、（Snapshotの作成時間からではなく）現在の時刻からの期間を指定します。
8. **[OK]**をクリックします。

グループSnapshotからのボリュームのクローニング

ボリュームのグループをポイントインタイムのグループSnapshotからクローニングできます。作成したボリュームは、システム内の他のボリュームと同様に使用できます。

手順

1. **[NetApp Element Management] > [Protection]**を選択します。
注：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。
2. **[Group Snapshots]**サブタブをクリックします。
3. ボリュームのクローンに使用するグループSnapshotのチェックボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Clone Volumes from Group Snapshot]**を選択します。
6. オプション：**[Clone Volumes From Group Snapshot]**ダイアログボックスで、新しいボリューム名のプレフィックスを入力します。

注：このプレフィックスは、新しいクローン ボリュームを既存のボリュームと区別するために、グループSnapshotから作成されるすべてのボリュームに適用されます。

7. オプション：クローンを割り当てる別のアカウントを選択します。アカウントを選択しない場合、新しいボリュームは現在のボリューム アカウントに割り当てられます。
8. オプション：クローン内のボリュームに適用する別のアクセス方法を選択します。アクセス方法を選択しない場合、現在のボリューム アクセス方法が使用されます。
 - **Read/Write**：すべての読み取りと書き込みが許可されます。
 - **Read Only**：すべての読み取りが許可されます。書き込みは許可されません。
 - **Locked**：管理者アクセスのみが許可されます。
 - **Replication Target**：レプリケートされたボリューム ペアのターゲット ボリュームとして指定されます。
9. [OK]をクリックします。

注：クローニング処理が完了するまでの時間は、ボリューム サイズおよびクラスタの現在の負荷によって異なります。

グループSnapshotへのボリュームのロールバック

一連のアクティブ ボリュームをグループSnapshotにロールバックできます。この処理では、グループSnapshot内の関連付けられているすべてのボリュームが、グループSnapshotが作成された時点の状態にリストアされます。ボリューム サイズも、元のSnapshotに記録されているサイズにリストアされます。ボリュームがパージされている場合は、そのボリュームのすべてのSnapshotもパージ時に削除されています。削除されたボリュームSnapshotはリストアされません。

手順

1. [NetApp Element Management] > [Protection]を選択します。

注：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。
2. [Group Snapshots]サブタブをクリックします。
3. ボリュームのクローンに使用するグループSnapshotのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Rollback Volumes to Group Snapshot]を選択します。
6. オプション：Snapshotにロールバックする前にボリュームの現在の状態を保存するには、次の手順を実行します。
 - a. [Rollback To Snapshot]ダイアログ ボックスで、[Save volumes' current state as a group snapshot]を選択します。
 - b. 新しいグループSnapshotの名前を入力します。
7. [OK]をクリックします。

グループSnapshotの削除

システムからグループSnapshotを削除できます。グループSnapshotを削除する場合は、グループに関連付けられているすべてのSnapshotについて、削除するか個別のSnapshotとして保持するかを選択できます。

タスク概要

グループSnapshotに含まれているボリュームまたはSnapshotを削除すると、そのグループSnapshotにロールバックできなくなります。ただし、各ボリュームを個別にロールバックすることは可能です。

手順

1. **[NetApp Element Management] > [Protection]**を選択します。
注：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。
2. **[Group Snapshots]**サブタブをクリックします。
3. 削除するグループSnapshotのチェックボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Delete]**をクリックします。
6. 確認のダイアログボックスで、次のいずれかを実行します。
 - ・ グループSnapshotとグループ内のSnapshotをすべて削除するには、**[Delete group snapshot and all group snapshot members]**を選択します。
 - ・ グループSnapshotを削除し、グループ内のSnapshotは保持するには、**[Retain group snapshot members as individual snapshots]**を選択します。
7. 操作を確定します。

Snapshotスケジュール

指定した間隔でSnapshotを自動的に作成するように、ボリュームのSnapshotのスケジュールを設定できます。1つのボリュームのSnapshotまたはグループのSnapshotを自動的に実行するスケジュールを設定できます。

ボリュームがレプリケートされている場合、Snapshotスケジュールの作成時に、作成されたSnapshotをリモートのNetApp Elementストレージシステムに格納するように設定できます。

注：スケジュールはUTC+0時間を使用して作成されます。タイムゾーンに基づいて、Snapshotが実行される実際の時刻の調整が必要になる場合があります。

Snapshotスケジュールの作成

ボリュームのSnapshotのスケジュールを設定し、指定した間隔でSnapshotを自動的に作成できます。

タスク概要

Snapshotスケジュールには、曜日または日にちに基づく間隔を設定できます。次のSnapshotを作成するまでの日数、時間、および分を指定することもできます。Snapshotのスケジュールを5分以外の間隔で設定した場合、Snapshotは5分単位に繰り上げた時間で実行されます。

たとえば、12:42:00 UTCに実行するようにSnapshotのスケジュールを設定した場合、12:45:00 UTCに実行されます。Snapshotのスケジュールを5分未満の間隔で実行するように設定することはできません。

手順

1. **[NetApp Element Management] > [Protection]**を選択します。
注：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。
2. **[Schedules]**サブタブをクリックします。
3. **[Create Schedule]**をクリックします。
4. **[Create Schedule]**ダイアログ ボックスで、**[Volume IDs CSV]**フィールドに、Snapshot処理に含めるボリュームIDまたは複数のボリュームIDをカンマで区切って入力します。
5. 新しいスケジュール名を入力します。
6. スケジュール タイプをリストから選択し、スケジュールの詳細を設定します。
7. オプション：Snapshotスケジュールを無期限に繰り返すには、**[Recurring Schedule]**を選択します。
8. オプション：**[New Snapshot Name]**フィールドに、新しいSnapshotの名前を入力します。
注：Snapshotの名前を入力しなかった場合、デフォルトではSnapshotの作成日時が名前として使用されます。
9. オプション：親ボリュームがペアリングされている場合にレプリケーションにSnapshotも含まれるようにするには、**[Include snapshot in replication when paired]**チェック ボックスを選択します。
10. Snapshotの保持期間として次のいずれかを選択します。
 - **Keep forever**：Snapshotをシステム上に無期限に保持します。
 - **Set retention period**：Snapshotをシステム上に保持する期間（日数、時間、または分）を設定します。
注：保持期間には、（Snapshotの作成時間からではなく）現在の時刻からの期間を指定します。
11. **[OK]**をクリックします。

Snapshotスケジュールの詳細

NetApp Element Management拡張ポイントの**[Protection]**タブにある**[Schedules]**ページでは、Snapshotスケジュールに関する情報を確認できます。

ID

システムによって生成されたスケジュールのID。

Type

スケジュールのタイプを示します。現時点でサポートされているタイプはSnapshotのみです。

Name

スケジュールの作成時に指定した名前。

Frequency

スケジュールを実行する頻度。頻度は時間と分、曜日、または日にちで設定できます。

Recurring

スケジュールが1回だけ実行されるか、定期的に実行されるかを示します。

Paused

スケジュールが手動で一時停止されているかどうかを示します。

Volume IDs

スケジュールの実行時に使用されるボリュームのIDを表示します。

Last Run

最後にスケジュールが実行された日時を表示します。

Last Run Status

スケジュールの前の実行結果を表示します。SuccessまたはFailureのいずれかです。

Snapshotスケジュールの編集

既存のSnapshotスケジュールを変更できます。変更後、次のスケジュール実行時に更新された設定が使用されます。元のスケジュールで作成されたSnapshotはストレージシステムに保持されます。

手順

1. **[NetApp Element Management] > [Protection]**を選択します。
 注：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。
2. **[Schedules]**サブタブをクリックします。
3. 編集するSnapshotスケジュールのチェックボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Edit]**を選択します。
6. **[Volume IDs CSV]**フィールドで、現在Snapshot処理の対象となっているボリュームID、または複数のボリュームIDをカンマで区切ったリストを変更します。
7. オプション：アクティブなスケジュールを一時停止したり、一時停止したスケジュールを再開したりするには、**[Manually Pause Schedule]**チェックボックスを選択します。
8. 必要に応じて、**[New Schedule Name]**フィールドに別のスケジュール名を入力します。
9. 必要に応じて、現在のスケジュールタイプを次のいずれかに変更します。
 - a. **Days of Week**：Snapshotを作成する曜日（複数選択可）と時刻を選択します。
 - b. **Days of Month**：Snapshotを作成する日にち（複数選択可）と時刻を選択します。
 - c. **Time Interval**：Snapshotを作成する間隔（日数、時間、分）を選択します。
10. オプション：Snapshotスケジュールを無期限に繰り返すには、**[Recurrent Schedule]**を選択します。
11. オプション：**[New Snapshot Name]**フィールドで、スケジュールの定義対象とするSnapshotの名前を入力または変更します。

注：このフィールドを空白のままにすると、Snapshotの作成日時が名前として使用されます。

12. オプション：親ボリュームがペアリングされている場合にレプリケーションにSnapshotも含まれるようにするには、**[Include snapshots in replication when paired]**チェック ボックスを選択します。

13. オプション：Snapshotの保持期間として次のいずれかを選択します。

- **Keep forever**：Snapshotをシステム上に無期限に保持します。
- **Set retention period**：Snapshotをシステム上に保持する期間（日数、時間、または分）を設定します。

注：保持期間には、（Snapshotの作成時間からではなく）現在の時刻からの期間を指定します。

14. **[OK]**をクリックします。

Snapshotスケジュールのコピー

Snapshotスケジュールのコピーを作成して、新しいボリュームに割り当てたり他の目的に使用したりできます。

手順

1. **[NetApp Element Management]** > **[Protection]**を選択します。

注：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。

2. **[Schedules]**サブタブをクリックします。
3. コピーするSnapshotスケジュールのチェック ボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Copy]**をクリックします。

[Copy Schedule]ダイアログ ボックスが、スケジュールの現在の設定が入力された状態で表示されます。

6. オプション：コピーしたスケジュールの名前を入力し、設定を変更します。
7. **[OK]**をクリックします。

Snapshotスケジュールの削除

Snapshotスケジュールを削除できます。スケジュールを削除すると、以降のスケジュールされたSnapshotは実行されません。過去にスケジュールで作成されたSnapshotはストレージ システム上に保持されます。

手順

1. **[NetApp Element Management]** > **[Protection]**を選択します。

注：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。

2. **[Schedules]**サブタブをクリックします。
3. 削除するSnapshotスケジュールのチェック ボックスを選択します。

4. [Actions]をクリックします。
5. 表示されたメニューで[Delete]をクリックします。
6. 操作を確定します。

リアルタイムのリモート レプリケーションのためのクラスタとボリュームのペアリング設定

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。リアルタイムのリモートレプリケーションを利用するには、2つのNetApp Elementクラスタをペアリングしてから、各クラスタのボリュームをペアリングする必要があります。

開始する前に

- プラグインにクラスタを少なくとも1つ追加しておきます。
- 管理およびストレージ両方のネットワークのすべてのノードIPアドレスが、ペアリングするクラスタ間で相互にルーティングされている必要があります。
- すべてのペア ノードでMTUが同じでなければならず、クラスタ間でエンドツーエンドでサポートされている必要があります。
- クラスタのNetApp Elementソフトウェアのバージョンの違いが1メジャー バージョン以内である必要があります。それよりも離れている場合、データレプリケーションを実行するには一方のクラスタをアップグレードする必要があります。

注：ネットアップは、データのレプリケーション時にWANアクセラレータ アプライアンスを使用することを認定していません。データをレプリケートする2つのクラスタ間にこのアプライアンスを配置すると、圧縮および重複排除の妨げとなる場合があります。WANアクセラレータ アプライアンスを本番環境に導入する前に、影響を十分に検証してください。

手順

1. **クラスタのペアリング** (145ページ)
リアルタイム レプリケーション機能を使用するには、最初に2つのクラスタをペアリングする必要があります。2つのクラスタをペアリングして接続したあと、一方のクラスタのアクティブなボリュームをもう一方のクラスタに継続的にレプリケートするように設定することで継続的なデータ保護 (CDP) を実現できます。両方のクラスタにクラスタ管理者としてアクセスできる場合は、ターゲット クラスタのMVIPを使用してソースとターゲットのクラスタをペアリングできます。クラスタ ペアの一方のクラスタにしかクラスタ管理者としてアクセスできない場合は、ターゲット クラスタでペアリング キーを使用してクラスタをペアリングします。
2. **ボリュームのペアリング** (149ページ)
クラスタ ペアのクラスタ間の接続を確立したら、一方のクラスタのボリュームをもう一方のクラスタのボリュームとペアリングできます。両方のクラスタのクレデンシャルがわかっている場合は、それらを使用してボリュームをペアリングできます。ソース クラスタのクレデンシャルしかわからない場合は、ペアリング キーを使用してボリュームをペアリングできます。両方のクラスタのクレデンシャルを把握している場合は、リモートクラスタにレプリケーション ターゲット ボリュームを作成してソース クラスタとペア

リングすることもできます。ボリューム ペアリング関係を確立したら、どちらのボリュームをレプリケーション ターゲットにするかを指定する必要があります。

3. **ボリューム レプリケーションの検証** (157ページ)
 ボリュームがレプリケートされたら、ソース ボリュームとターゲット ボリュームがアクティブになっていることを確認する必要があります。状態がActiveの場合は、ボリュームがペアリングされ、ソース ボリュームからターゲット ボリュームにデータが送信されて同期されています。
4. **レプリケーション後のボリューム関係の削除** (157ページ)
 レプリケーションが完了してボリューム ペアリング関係が不要になったら、ボリューム関係を削除できます。
5. **ボリューム関係の管理** (157ページ)
 レプリケーションの一時停止、ボリューム ペアリングの反転、レプリケーション モードの変更、ボリューム ペアの削除、クラスタ ペアの削除など、さまざまな方法でボリューム関係を管理できます。

クラスタのペアリング

リアルタイム レプリケーション機能を使用するには、最初に2つのクラスタをペアリングする必要があります。2つのクラスタをペアリングして接続したあと、一方のクラスタのアクティブなボリュームをもう一方のクラスタに継続的にレプリケートするように設定することで継続的なデータ保護 (CDP) を実現できます。両方のクラスタにクラスタ管理者としてアクセスできる場合は、ターゲット クラスタのMVIPを使用してソースとターゲットのクラスタをペアリングできます。クラスタ ペアの一方のクラスタにしかクラスタ管理者としてアクセスできない場合は、ターゲット クラスタでペアリング キーを使用してクラスタをペアリングします。

開始する前に

- ペアリングするクラスタの一方または両方に対するクラスタ管理者権限が必要です。
- クラスタ間のラウンドトリップ レイテンシが2,000ミリ秒未満である必要があります。
- クラスタのNetApp Elementソフトウェアのバージョンの違いが1メジャー バージョン以内である必要があります。
- ペア クラスタのすべてのノードIPを相互にルーティングする必要があります。

注：クラスタをペアリングするには、管理ネットワーク上のノードどうしが完全に接続されている必要があります。レプリケーションを実行するには、ストレージ クラスタ ネットワーク上の個々のノードが接続されている必要があります。

タスク概要

ボリュームのレプリケーション用に、1つのNetApp Elementクラスタを最大4つの他のクラスタとペアリングすることができます。同じクラスタ グループに含まれるクラスタどうしをペアリングすることもできます。

手順

1. **クレデンシャルを使用したクラスタのペアリング** (146ページ)
 一方のクラスタのMVIPを使用してもう一方のクラスタとの接続を確立することにより、リアルタイム レプリケーション用に2つのクラスタをペアリングできます。この方法を使用するには、両方のクラスタに対するクラスタ管理者アクセスが必要です。
2. **ペアリング キーを使用したクラスタのペアリング** (147ページ)
 ローカル クラスタにはクラスタ管理者としてアクセスできるが、リモート クラスタにはアクセスできない場合は、ペアリング キーを使用してクラスタをペアリングします。

ローカル クラスタで生成したペアリング キーをリモート サイトのクラスタ管理者に安全な方法で送信して接続を確立し、リアルタイム レプリケーション用にクラスタをペアリングします。

3. **クラスタ ペア接続の検証** (148ページ)
クラスタ ペアリングが完了したら、クラスタ ペアの接続を検証して、レプリケーションが成功したかどうかを確認することができます。

クレデンシャルを使用したクラスタのペアリング

一方のクラスタのMVIPを使用してもう一方のクラスタとの接続を確立することにより、リアルタイム レプリケーション用に2つのクラスタをペアリングできます。この方法を使用するには、両方のクラスタに対するクラスタ管理者アクセスが必要です。

タスク概要

クラスタをペアリングする前に、クラスタ管理者のユーザ名とパスワードを使用してクラスタ アクセスを認証します。MVIPがわからない場合やクラスタへのアクセスが許可されていない場合は、ペアリング キーを生成し、そのキーを使用して2つのクラスタをペアリングできます。詳細については、ペアリング キーを使用したクラスタのペアリングに関するブライグインのドキュメントを参照してください。

手順

1. ローカル クラスタを含むvCenterから、**[NetApp Element Management] > [Protection]**を選択します。

注：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。
2. **[Cluster Pairs]**サブタブをクリックします。
3. **[Create Cluster Pairing]**をクリックします。
4. **[Create Cluster Pairing]**ダイアログ ボックスで、以下のいずれかを選択します。
 - **Registered Cluster**：この方法は、ペアリングするリモート クラスタがNetApp Element Plug-in for vCenter Serverの同じインスタンスで制御されている場合に選択します。
 - **Credentialed Cluster**：この方法は、リモート クラスタにNetApp Element Plug-in for vCenter Serverの外部で設定された既知のクレデンシャルがある場合に選択します。
5. **[Registered Cluster]**を選択した場合は、使用可能なクラスタのリストからクラスタを選択して**[Pair]**をクリックします。
6. **[Credentialed Cluster]**を選択した場合は、次の手順を実行します。
 - a. リモート クラスタのMVIPアドレスを入力します。
 - b. クラスタ管理者のユーザ名を入力します。
 - c. クラスタ管理者のパスワードを入力します。
 - d. **[Start Pairing]**をクリックします。
7. タスクが完了して**[Cluster Pairs]**ページに戻ったら、クラスタ ペアが接続されていることを確認します。
8. オプション：リモート クラスタで、**[NetApp Element Management] > [Protection] > [Cluster Pairs]**を選択するかElement Web UIを使用して、クラスタ ペアが接続されていることを確認します。

関連タスク

ペアリング キーを使用したクラスタのペアリング (147ページ)

ローカル クラスタにはクラスタ管理者としてアクセスできるが、リモート クラスタにはアクセスできない場合は、ペアリング キーを使用してクラスタをペアリングします。ローカル クラスタで生成したペアリング キーをリモート サイトのクラスタ管理者に安全な方法で送信して接続を確立し、リアルタイム レプリケーション用にクラスタをペアリングします。

クラスタのペアリング (145ページ)

リアルタイム レプリケーション機能を使用するには、最初に2つのクラスタをペアリングする必要があります。2つのクラスタをペアリングして接続したあと、一方のクラスタのアクティブなボリュームをもう一方のクラスタに継続的にレプリケートするように設定することで継続的なデータ保護 (CDP) を実現できます。両方のクラスタにクラスタ管理者としてアクセスできる場合は、ターゲット クラスタのMVIPを使用してソースとターゲットのクラスタをペアリングできます。クラスタ ペアの一方のクラスタにしかクラスタ管理者としてアクセスできない場合は、ターゲット クラスタでペアリング キーを使用してクラスタをペアリングします。

ペアリング キーを使用したクラスタのペアリング

ローカル クラスタにはクラスタ管理者としてアクセスできるが、リモート クラスタにはアクセスできない場合は、ペアリング キーを使用してクラスタをペアリングします。ローカル クラスタで生成したペアリング キーをリモート サイトのクラスタ管理者に安全な方法で送信して接続を確立し、リアルタイム レプリケーション用にクラスタをペアリングします。

タスク概要

この手順では、ローカル サイトとリモート サイトでvCenterを使用し、2つのクラスタをペアリングする方法について説明します。vCenter Plug-inで制御されていないクラスタについては、Element Web UIを使用してクラスタのペアリングを開始または完了することができます。Element Web UIからクラスタのペアリングを開始または完了する詳しい手順については、NetApp Elementソフトウェアのユーザ ガイドを参照してください。

手順

1. ローカル クラスタを含むvCenterから、[NetApp Element Management] > [Protection]を選択します。

注：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。

2. [Cluster Pairs]サブタブをクリックします。
3. [Create Cluster Pairing]をクリックします。
4. [Create Cluster Pairing]ダイアログ ボックスで、[Inaccessible Cluster]を選択します。
5. [Generate Key]をクリックします。

注：この操作により、ペアリング用のテキスト キーが生成され、ローカル クラスタにクラスタ ペアが未設定の状態で作成されます。この手順を途中で中止した場合は、クラスタ ペアを手動で削除する必要があります。

6. クラスタ ペアリング キーをクリップボードにコピーします。
7. [Close]をクリックします。
8. このペアリング キーをリモート クラスタ サイトのクラスタ管理者に渡します。

注: クラスタ ペアリング キーには、リモート レプリケーション用にボリューム接続を許可するためのMVIPのバージョン、ユーザ名、パスワード、およびデータベース情報が含まれています。このキーの取り扱いには十分に注意し、ユーザ名やパスワードが誤って外部に漏れたり不正に使用されたりしないように適切に管理してください。

注意: ペアリング キーの文字はいっさい変更しないでください。変更するとキーは無効になります。

9. リモート クラスタを含むvCenterから、**[NetApp Element Management] > [Protection]**を選択します。

注: 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。

注: Element UIを使用してペアリングを実行することもできます。

10. **[Cluster Pairs]**サブタブをクリックします。

11. **[Complete Cluster Pairing]**をクリックします。

注: ロード中のスピナー アイコンが消えてから次の手順に進みます。ペアリング プロセス中に予期しないエラーが発生した場合は、ローカル クラスタとリモート クラスタで未設定のクラスタ ペアがあれば手動で削除し、ペアリングをもう一度実行してください。

12. ローカル クラスタのペアリング キーを**[Cluster Pairing Key]**フィールドに貼り付けます。

13. **[Pair Cluster]**をクリックします。

14. タスクが完了して**[Cluster Pair]**ページに戻ったら、クラスタ ペアが接続されていることを確認します。

15. リモート クラスタで、**[NetApp Element Management] > [Protection]**を選択するかElement UIを使用して、クラスタ ペアが接続されていることを確認します。

関連タスク

クレデンシャルを使用したクラスタのペアリング (146ページ)

一方のクラスタのMVIPを使用してもう一方のクラスタとの接続を確立することにより、リアルタイム レプリケーション用に2つのクラスタをペアリングできます。この方法を使用するには、両方のクラスタに対するクラスタ管理者アクセスが必要です。

クラスタのペアリング (145ページ)

リアルタイム レプリケーション機能を使用するには、最初に2つのクラスタをペアリングする必要があります。2つのクラスタをペアリングして接続したあと、一方のクラスタのアクティブなボリュームをもう一方のクラスタに継続的にレプリケートするように設定することで継続的なデータ保護 (CDP) を実現できます。両方のクラスタにクラスタ管理者としてアクセスできる場合は、ターゲット クラスタのMVIPを使用してソースとターゲットのクラスタをペアリングできます。クラスタ ペアの一方のクラスタにしかクラスタ管理者としてアクセスできない場合は、ターゲット クラスタでペアリング キーを使用してクラスタをペアリングします。

クラスタ ペア接続の検証

クラスタ ペアリングが完了したら、クラスタ ペアの接続を検証して、レプリケーションが成功したかどうかを確認することができます。

手順

1. ローカル クラスタで、**[Data Protection] > [Cluster Pairs]**の順に選択します。

2. [Cluster Pairs]ウィンドウで、クラスタ ペアが接続されていることを確認します。
3. ローカル クラスタに戻り、[Cluster Pairs]ウィンドウでクラスタ ペアが接続されていることを確認します。

ボリュームのペアリング

クラスタ ペアのクラスタ間の接続を確立したら、一方のクラスタのボリュームをもう一方のクラスタのボリュームとペアリングできます。両方のクラスタのクレデンシャルがわかっている場合は、それらを使用してボリュームをペアリングできます。ソース クラスタのクレデンシャルしかわからない場合は、ペアリング キーを使用してボリュームをペアリングできます。両方のクラスタのクレデンシャルを把握している場合は、リモート クラスタにレプリケーション ターゲット ボリュームを作成してソース クラスタとペアリングすることもできます。ボリューム ペアリング関係を確立したら、どちらのボリュームをレプリケーション ターゲットにするかを指定する必要があります。

開始する前に

- クラスタ ペアのクラスタ間の接続を確立しておきます。
- ペアリングするクラスタの一方または両方に対するクラスタ管理者権限が必要です。

手順

1. [クレデンシャルを使用したボリュームのペアリング](#) (149ページ)
ローカル ボリュームをリモート クラスタの別のボリュームとペアリングできます。この方法は、ボリュームをペアリングする両方のクラスタにクラスタ管理者としてアクセスできる場合に使用します。リモート クラスタのボリュームのボリュームIDを使用して接続を開始します。
2. [ターゲット ボリュームの作成およびローカル ボリュームとのペアリング](#) (152ページ)
2つ以上のローカル ボリュームをリモート クラスタに関連するターゲット ボリュームとペアリングできます。このプロセスでは、選択した各ローカル ソース ボリュームに対して、リモート クラスタにレプリケーション ターゲット ボリュームが作成されます。この方法は、ボリュームをペアリングする両方のクラスタにクラスタ管理者としてアクセスでき、リモート クラスタがプラグインで制御されている場合に使用します。リモート クラスタの各ボリュームのボリュームIDを使用して接続が開始されます。
3. [ペアリング キーを使用したボリュームのペアリング](#) (153ページ)
ペアリング キーを使用して、ローカル ボリュームをリモート クラスタの別のボリュームとペアリングできます。この方法は、クラスタ管理者としてアクセスできるのがソース クラスタだけの場合に使用します。ペアリング キーを生成し、そのキーをリモート クラスタで使用してボリュームをペアリングします。
4. [ペアリングされたボリュームに対するレプリケーションのソースとターゲットの割り当て](#) (155ページ)
ボリュームのペアリング中にレプリケーション ターゲットにするボリュームを割り当てていない場合、設定は完了していません。この手順を使用して、ソース ボリュームとそのレプリケーション ターゲット ボリュームを割り当てることができます。ボリューム ペアのどちらのボリュームをレプリケーションのソースまたはターゲットにしてもかまいません。この手順は、ソース ボリュームが使用できなくなったときに、データをソース ボリュームからリモート ターゲット ボリュームにリダイレクトする場合にも使用できます。

クレデンシャルを使用したボリュームのペアリング

ローカル ボリュームをリモート クラスタの別のボリュームとペアリングできます。この方法は、ボリュームをペアリングする両方のクラスタにクラスタ管理者としてアクセスできる

場合に使用します。リモート クラスタのボリュームのボリュームIDを使用して接続を開始します。

開始する前に

- リモート クラスタのクラスタ管理者のクレデンシャルが必要です。
- 該当するボリュームを含むクラスタがペアリングされていることを確認します。
- このプロセスで新しいボリュームを作成する場合を除き、リモート ボリュームのIDが必要です。
- ローカル ボリュームをソースにする場合は、ボリュームのアクセス モードが[Read/Write]に設定されていることを確認します。

手順

1. ローカル クラスタを含むvCenterから、[NetApp Element Management] > [Management]を選択します。

注：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。

2. [Volumes]サブタブをクリックします。
3. [Active]ビューで、ペアリングするボリュームのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Volume Pairing]をクリックします。
6. [Volume Pairing]ダイアログ ボックスで、以下のいずれかを選択します。
 - **Volume Creation**：この方法は、リモート クラスタにレプリケーション ターゲット ボリュームを作成する場合に選択します。この方法は、NetApp Element Plug-in for vCenter Serverで制御されているリモート クラスタでのみ使用できます。
 - **Volume Selection**：この方法は、ターゲット ボリュームを含むリモート クラスタがNetApp Element Plug-in for vCenter Serverで制御されている場合に選択します。
 - **Volume ID**：この方法は、ターゲット ボリュームを含むリモート クラスタにNetApp Element Plug-in for vCenter Serverの外部で設定された既知のクレデンシャルがある場合に選択します。
7. ドロップダウン リストから[Replication Mode]を選択します。
 - **Real-time (Synchronous)**：書き込みはソース クラスタとターゲット クラスタの両方でコミットされたあとにクライアントに通知されます。
 - **Real-time (Asynchronous)**：書き込みはソース クラスタでコミットされたあとにクライアントに通知されます。
 - **Snapshots Only**：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。
8. ペアリング モードのオプションとして[Volume Creation]を選択した場合は、次の手順を実行します。
 - a. ドロップダウン リストからペア クラスタを選択します。

注：この操作により、次の手順で選択する、クラスタで使用可能なアカウントが設定されます。

- b. レプリケーション ターゲット ボリュームを含むターゲット クラスタ上のアカウントを選択します。
- c. レプリケーション ターゲット ボリューム名を入力します。

注：このプロセスではボリューム サイズを調整できません。

- 9. ペアリング モードのオプションとして[**Volume Selection**]を選択した場合は、次の手順を実行します。

- a. ドロップダウン リストからペア クラスタを選択します。

注：次の手順で選択する、クラスタ上の使用可能なボリュームが表示されます。

- b. オプション：リモート ボリュームをボリューム ペアリングのターゲットとして設定する場合は、[**set remote volume to Replication Target**]オプションをクリックします。ローカル ボリュームが読み取り / 書き込みに設定されていれば、ローカル ボリュームがペアのソースになります。

注意：レプリケーション ターゲットとして既存のボリュームを割り当てると、そのボリュームのデータは上書きされます。レプリケーション ターゲットには新しいボリュームを使用することを推奨します。

注：レプリケーションのソースとターゲットは、[**Volumes**] > [**Actions**] > [**Edit**]からペアリングプロセスを実行してあとで割り当てすることもできます。ペアリングを完了するには、ソースとターゲットを割り当てする必要があります。

- c. 使用可能なボリュームのリストからボリュームを選択します。

- 10. ペアリング モードのオプションとして[**Volume ID**]を選択した場合は、次の手順を実行します。

- a. ドロップダウン リストからペア クラスタを選択します。
- b. クラスタがプラグインに登録されていない場合は、クラスタ管理者のユーザIDを入力します。
- c. クラスタがプラグインに登録されていない場合は、クラスタ管理者のパスワードを入力します。
- d. ボリュームIDを入力します。
- e. リモート ボリュームをボリューム ペアリングのターゲットとして設定する場合は、[**set remote volume to Replication Target**]オプションをクリックします。ローカル ボリュームが読み取り / 書き込みに設定されていれば、ローカル ボリュームがペアのソースになります。

注意：レプリケーション ターゲットとして既存のボリュームを割り当てると、そのボリュームのデータは上書きされます。レプリケーション ターゲットには新しいボリュームを使用することを推奨します。

注：レプリケーションのソースとターゲットは、[**Volumes**] > [**Actions**] > [**Edit**]からペアリングプロセスを実行してあとで割り当てすることもできます。ペアリングを完了するには、ソースとターゲットを割り当てする必要があります。

- 11. [**Pair**]をクリックします。

注：ペアリング操作を確定すると、2つのクラスタでボリュームを接続するプロセスが開始されます。ペアリングプロセス中は、[**Volume Pairs**]ページの[**Volume Status**]列で進捗メッセージを確認できます。

注意：レプリケーション ターゲットにするボリュームをまだ割り当てていない場合、ペアリングの設定は完了していません。ソースとターゲットが割り当てられるまで、ボリューム ペアにはPausedMisconfiguredと表示されます。ボリューム ペアリングを完了するには、ソースとターゲットを割り当てる必要があります。

12. いずれかのクラスタで、**[Protection]** > **[Volume Pairs]**を選択します。

13. ボリューム ペアリングのステータスを確認します。

関連タスク

[ペアリングされたボリュームに対するレプリケーションのソースとターゲットの割り当て](#) (155ページ)

ボリュームのペアリング中にレプリケーション ターゲットにするボリュームを割り当てていない場合、設定は完了していません。この手順を使用して、ソース ボリュームとそのレプリケーション ターゲット ボリュームを割り当てることができます。ボリューム ペアのどちらのボリュームをレプリケーションのソースまたはターゲットにしてもかまいません。この手順は、ソース ボリュームが使用できなくなったときに、データをソース ボリュームからリモート ターゲット ボリュームにリダイレクトする場合にも使用できます。

関連資料

[ボリューム ペアリングに関するメッセージ](#) (161ページ)

[ボリューム ペアリングに関する警告](#) (161ページ)

ターゲット ボリュームの作成およびローカル ボリュームとのペアリング

2つ以上のローカル ボリュームをリモート クラスタの関連するターゲット ボリュームとペアリングできます。このプロセスでは、選択した各ローカル ソース ボリュームに対して、リモート クラスタにレプリケーション ターゲット ボリュームが作成されます。この方法は、ボリュームをペアリングする両方のクラスタにクラスタ管理者としてアクセスでき、リモート クラスタがプラグインで制御されている場合に使用します。リモート クラスタの各ボリュームのボリュームIDを使用して接続が開始されます。

開始する前に

- リモート クラスタのクラスタ管理者のクレデンシャルが必要です。
- 該当するボリュームを含むクラスタがプラグインを使用してペアリングされていることを確認します。
- リモート クラスタがプラグインで制御されていることを確認します。
- 各ローカル ボリュームのアクセス モードが[Read/Write]に設定されていることを確認します。

手順

1. ローカル クラスタを含むvCenterから、**[NetApp Element Management]** > **[Management]**を選択します。

注：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。

2. **[Volumes]**サブタブをクリックします。
3. **[Active]**ビューで、ペアリングする2つ以上のボリュームのチェック ボックスを選択します。

4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Volume Pairing]**をクリックします。
6. **[Multiple Volume Pairing with Target Volume Creation]**ダイアログ ボックスで、ドロップダウン リストから**[Replication Mode]**を選択します。
 - **Real-time (Synchronous)** : 書き込みはソース クラスタとターゲット クラスタの両方でコミットされたあとにクライアントに通知されます。
 - **Real-time (Asynchronous)** : 書き込みはソース クラスタでコミットされたあとにクライアントに通知されます。
 - **Snapshots Only** : 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。
7. ドロップダウン リストからペア クラスタを選択します。
8. レプリケーション ターゲット ボリュームを含むターゲット クラスタ上のアカウントを選択します。
9. オプション : ターゲット クラスタの新しいボリューム名に使用するプレフィックスまたはサフィックスを入力します。

注 : 指定したプレフィックスまたはサフィックスを含むサンプルのボリューム名が表示されます。
10. **[Create Pairs]**をクリックします。

注 : ペアリング操作を確定すると、2つのクラスタでボリュームを接続するプロセスが開始されます。ペアリング プロセス中は、**[Volume Pairs]**ページの**[Volume Status]**列で進捗メッセージを確認できます。プロセスが完了すると、リモート クラスタに新しいターゲット ボリュームが作成されて接続されます。
11. いずれかのクラスタで、**[Protection] > [Volume Pairs]**を選択します。
12. ボリューム ペアリングのステータスを確認します。

関連資料

- [ボリューム ペアリングに関するメッセージ \(161ページ\)](#)
- [ボリューム ペアリングに関する警告 \(161ページ\)](#)

ペアリング キーを使用したボリュームのペアリング

ペアリング キーを使用して、ローカル ボリュームをリモート クラスタの別のボリュームとペアリングできます。この方法は、クラスタ管理者としてアクセスできるのがソース クラスタだけの場合に使用します。ペアリング キーを生成し、そのキーをリモート クラスタで使用してボリュームをペアリングします。

開始する前に

該当するボリュームを含むクラスタがペアリングされていることを確認します。

ベストプラクティス : ソース ボリュームを**[Read/Write]**に設定し、ターゲット ボリュームを**[Replication Target]**に設定します。ターゲット ボリュームは、データが格納されておらず、かつサイズ、512e、QoSなどの特性がソース ボリュームとまったく同じである必要があります。レプリケーション ターゲットとして既存のボリュームを割り当てると、そのボリュームのデータは上書きされます。ターゲット ボリュームにはソース ボリュームと同じかそれ以上のサイズのボリュームを使用できますが、ソース ボリュームより小さいボリュームは使用できません。

タスク概要

この手順では、ローカル サイトとリモート サイトでvCenterを使用し、2つのボリュームをペアリングする方法について説明します。vCenter Plug-inで制御されていないボリュームについては、Element Web UIを使用してボリュームのペアリングを開始または完了することができます。Element Web UIからボリュームのペアリングを開始または完了する詳しい手順については、NetApp Elementソフトウェアのユーザ ガイドを参照してください。

注：ボリューム ペアリング キーには、暗号化されたボリューム情報が格納されており、機密情報が含まれている場合があります。このキーは必ず安全な方法で共有してください。

手順

1. ローカル クラスタを含むvCenterから、[NetApp Element Management] > [Management]を選択します。

注：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。

2. [Volumes]サブタブをクリックします。
3. [Active]ビューで、ペアリングするボリュームのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Volume Pairing]をクリックします。
6. [Volume Pairing]ダイアログ ボックスで、[Inaccessible Cluster]を選択します。
7. [Replication Mode]をリストから選択します。
 - **Real-time (Synchronous)：**書き込みはソース クラスタとターゲット クラスタの両方でコミットされたあとにクライアントに通知されます。
 - **Real-time (Asynchronous)：**書き込みはソース クラスタでコミットされたあとにクライアントに通知されます。
 - **Snapshots Only：**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。
8. [Generate Key]をクリックします。

注：この操作により、ペアリング用のテキスト キーが生成され、ローカル クラスタにボリューム ペアが未設定の状態で作成されます。この手順を途中で中止した場合は、ボリューム ペアを手動で削除する必要があります。

9. ペアリング キーをクリップボードにコピーします。
10. [Close]をクリックします。
11. このペアリング キーをリモート クラスタ サイトのクラスタ管理者に渡します。

注：ボリューム ペアリング キーの取り扱いには十分に注意し、誤って外部に漏れたり不正に使用されたりしないように適切に管理してください。

注意：ペアリング キーの文字はいつさい変更しないでください。変更するとキーは無効になります。

12. リモート クラスタを含むvCenterから、[NetApp Element Management] > [Management]を選択します。

注：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。

13. **[Volumes]**サブタブをクリックします。
14. **[Active]**ビューで、ペアリングするボリュームのチェックボックスを選択します。
15. **[Actions]**をクリックします。
16. 表示されたメニューで**[Volume Pairing]**をクリックします。
17. **[Volume Pairing]**ダイアログ ボックスで、**[Complete Cluster Pairing]**を選択します。
18. もう一方のクラスタのペアリング キーを**[Pairing Key]**ボックスに貼り付けます。
19. **[Complete Pairing]**をクリックします。

注：ペアリング操作を確定すると、2つのクラスタでボリュームを接続するプロセスが開始されます。ペアリング プロセス中は、**[Volume Pairs]**ページの**[Volume Status]**列で進捗メッセージを確認できます。ペアリング プロセス中に予期しないエラーが発生した場合は、ローカル クラスタとリモート クラスタで未設定のクラスタ ペアがあれば手動で削除し、ペアリングをもう一度実行してください。

注意：レプリケーション ターゲットにするボリュームをまだ割り当てていない場合、ペアリングの設定は完了していません。ソースとターゲットが割り当てられるまで、ボリューム ペアにはPausedMisconfiguredと表示されます。ボリューム ペアリングを完了するには、ソースとターゲットを割り当てする必要があります。

20. いずれかのクラスタで、**[Protection] > [Volume Pairs]**を選択します。
 21. ボリューム ペアリングのステータスを確認します。
- 注：**ペアリング キーを使用してペアリングされたボリュームは、リモート側のペアリング プロセスが完了してから表示されます。

関連タスク

[ペアリングされたボリュームに対するレプリケーションのソースとターゲットの割り当て \(155ページ\)](#)

ボリュームのペアリング中にレプリケーション ターゲットにするボリュームを割り当てていない場合、設定は完了していません。この手順を使用して、ソース ボリュームとそのレプリケーション ターゲット ボリュームを割り当てることができます。ボリューム ペアのどちらのボリュームをレプリケーションのソースまたはターゲットにしてもかまいません。この手順は、ソース ボリュームが使用できなくなったときに、データをソース ボリュームからリモート ターゲット ボリュームにリダイレクトする場合にも使用できます。

関連資料

[ボリューム ペアリングに関するメッセージ \(161ページ\)](#)

[ボリューム ペアリングに関する警告 \(161ページ\)](#)

ペアリングされたボリュームに対するレプリケーションのソースとターゲットの割り当て

ボリュームのペアリング中にレプリケーション ターゲットにするボリュームを割り当てていない場合、設定は完了していません。この手順を使用して、ソース ボリュームとそのレプリケーション ターゲット ボリュームを割り当てることができます。ボリューム ペアのどちらのボリュームをレプリケーションのソースまたはターゲットにしてもかまいません。

この手順は、ソース ボリュームが使用できなくなったときに、データをソース ボリュームからリモート ターゲット ボリュームにリダイレクトする場合にも使用できます。

開始する前に

ソース ボリュームとターゲット ボリュームを含むクラスタへのアクセス権が必要です。

タスク概要

この手順では、ローカル サイトとリモート サイトでvCenterを使用し、2つのクラスタ間にソース ボリュームとレプリケーション ボリュームを割り当てる方法について説明します。vCenter Plug-inで制御されていないボリュームについては、Element Web UIを使用してソース ボリュームまたはレプリケーション ボリュームを割り当てることができます。Element Web UIからクラスタ ペア的一端を削除する詳しい手順については、NetApp Elementソフトウェアのユーザ ガイドを参照してください。

レプリケーション ソース ボリュームには読み取り / 書き込みのアカウント アクセスが設定されます。レプリケーション ターゲット ボリュームには、レプリケーション ソースのみが読み取り / 書き込みアクセスできます。

ベストプラクティス : ターゲット ボリュームは、データが格納されておらず、かつサイズ、512e、QoSなどの特性がソース ボリュームとまったく同じである必要があります。ターゲット ボリュームにはソース ボリュームと同じかそれ以上のサイズのボリュームを使用できますが、ソース ボリュームより小さいボリュームは使用できません。

手順

1. **NetApp Element Management**拡張ポイントで、レプリケーション ソースとして使用するペアリングされたボリュームが含まれているクラスタを選択します。
2. **[NetApp Element Management] > [Management]**を選択します。
3. **[Volumes]**サブタブをクリックします。
4. **[Active]**ビューで、編集するボリュームのチェック ボックスを選択します。
5. **[Actions]**をクリックします。
6. 表示されたメニューで**[Edit]**を選択します。
7. **[Access]**ドロップダウン リストで**[Read/Write]**を選択します。

注意 : ソースとターゲットの割り当てを逆にしている場合、新しいレプリケーションターゲットが割り当てられるまでボリューム ペアにはPausedMisconfiguredと表示されます。アクセスを変更すると、ボリューム レプリケーションが一時停止し、データの転送が中止されます。これらの変更が両方のサイトで調整されていることを確認してください。

8. **[OK]**をクリックします。
9. **NetApp Element Management**拡張ポイントで、レプリケーション ターゲットとして使用するペアリングされたボリュームが含まれているクラスタを選択します。
10. **[NetApp Element Management] > [Management]**を選択します。
11. **[Volumes]**サブタブをクリックします。
12. **[Active]**ビューで、編集するボリュームのチェック ボックスを選択します。
13. **[Actions]**をクリックします。
14. 表示されたメニューで**[Edit]**を選択します。

15. [Access]ドロップダウン リストで[Replication Target]を選択します。

注意：レプリケーション ターゲットとして既存のボリュームを割り当てると、そのボリュームのデータは上書きされます。レプリケーション ターゲットには新しいボリュームを使用することを推奨します。

16. [OK]をクリックします。

関連資料

[ボリューム ペアリングに関するメッセージ](#) (161ページ)

[ボリューム ペアリングに関する警告](#) (161ページ)

ボリューム レプリケーションの検証

ボリュームがレプリケートされたら、ソース ボリュームとターゲット ボリュームがアクティブになっていることを確認する必要があります。状態がActiveの場合は、ボリュームがペアリングされ、ソース ボリュームからターゲット ボリュームにデータが送信されて同期されています。

手順

1. ペアリングのどちらかのクラスタで、[NetApp Element Management] > [Protection]を選択します。

注：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。

2. [Volume Pairs]サブタブをクリックします。
3. ボリュームのステータスがActiveであることを確認します。

レプリケーション後のボリューム関係の削除

レプリケーションが完了してボリューム ペアリング関係が不要になったら、ボリューム関係を削除できます。

手順

1. ボリューム ペアリング関係を削除する手順を実行します。 [ボリューム ペアの削除](#)

ボリューム関係の管理

レプリケーションの一時停止、ボリューム ペアリングの反転、レプリケーション モードの変更、ボリューム ペアの削除、クラスタ ペアの削除など、さまざまな方法でボリューム関係を管理できます。

関連タスク

[レプリケーションの一時停止](#) (158ページ)

[レプリケーション モードの変更](#) (158ページ)

[ボリューム ペアの削除](#) (159ページ)

関連資料

[ボリューム ペアの詳細](#) (160ページ)

レプリケーションの一時停止

ボリューム ペアのプロパティを編集して、レプリケーションを手動で一時停止することができます。

手順

1. [NetApp Element Management] > [Protection]を選択します。
注：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。
2. [Volume Pairs]サブタブをクリックします。
3. 編集するボリューム ペアのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Edit]を選択します。
6. [Edit Volume Pair]ペインで、レプリケーション プロセスを手動で一時停止または開始します。
注意：ボリューム レプリケーションを手動で一時停止または再開すると、データの転送が中止または再開されます。これらの変更が両方のサイトで調整されていることを確認してください。
7. [Save Changes]をクリックします。

レプリケーション モードの変更

ボリューム ペアのプロパティを編集して、ボリューム ペア関係のレプリケーション モードを変更することができます。

手順

1. [NetApp Element Management] > [Protection]を選択します。
注：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。
2. [Volume Pairs]サブタブをクリックします。
3. 編集するボリューム ペアのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Edit]を選択します。
6. [Edit Volume Pair]ペインで、新しいレプリケーション モードを選択します。
注意：レプリケーション モードの変更はすぐに反映されます。これらの変更が両方のサイトで調整されていることを確認してください。
 - **Real-time (Synchronous)：**書き込みはソース クラスタとターゲット クラスタの両方でコミットされたあとにクライアントに通知されます。
 - **Real-time (Asynchronous)：**書き込みはソース クラスタでコミットされたあとにクライアントに通知されます。
 - **Snapshots Only：**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。

7. [Save Changes]をクリックします。

ボリューム ペアの削除

2つのボリューム間のペア関係を解除するには、ボリューム ペアを削除します。

タスク概要

この手順では、ローカル サイトとリモート サイトでvCenterを使用し、2つのボリュームのペアリング関係を削除する方法について説明します。vCenter Plug-inで制御されていないボリュームについては、Element Web UIを使用してボリューム ペアを削除することができます。Element Web UIからボリューム ペアを削除する詳しい手順については、NetApp Element ソフトウェアのユーザ ガイドを参照してください。

手順

1. [NetApp Element Management] > [Protection]を選択します。
 注：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。
2. [Volume Pairs]サブタブをクリックします。
3. 削除するボリューム ペアのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Delete]を選択します。
6. [Delete Volume Pair]ダイアログ ボックスで、各ボリューム ペアの詳細を確認します。
 注：プラグインで管理されていないクラスタの場合、ローカル クラスタ側のボリューム ペア関係のみが削除されます。ペアリング関係を完全に削除するには、リモート クラスタ側のボリューム ペア関係を手動で削除する必要があります。
7. (プラグインで管理されているクラスタ向け、オプション) [Change Replication Target Access to]チェック ボックスを選択し、レプリケーション ターゲット ボリューム用の新しいアクセス モードを選択します。新しいアクセス モードは、ボリューム ペアリング関係の削除後に適用されます。
8. [Yes]をクリックします。

クラスタ ペアの削除

ローカル サイトとリモート サイトでvCenterを使用して、2つのクラスタ間のクラスタ ペアリング関係を削除できます。クラスタ ペアリング関係を完全に削除するには、ローカルとリモートの両方のクラスタからクラスタ ペアを削除する必要があります。

タスク概要

vCenter Plug-inを使用してクラスタ ペアを削除できます。vCenter Plug-inで制御されないクラスタについては、Element Web UIを使用してクラスタ ペアを削除することもできます。Element Web UIを使用してクラスタ ペアを削除する詳しい手順については、NetApp Element ソフトウェアのユーザ ガイドを参照してください。

手順

1. いずれかのクラスタで、[NetApp Element Management] > [Protection]を選択します。
2. [Cluster Pairs]サブタブをクリックします。

3. 削除するクラスタ ペアのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Delete]をクリックします。
6. 操作を確定します。

注：この操作では、ローカル クラスタ側のクラスタ ペアのみが削除されます。ペアリング関係を完全に削除するには、リモート クラスタ側のクラスタ ペアを手動で削除する必要があります。

7. クラスタ ペアリングのリモート クラスタで同じ手順を実行します。

ボリューム ペアの詳細

NetApp Element Management拡張ポイントの[Protection]タブにある[Volume Pairs]ページで、ペアリング済み、またはペアリング中のボリュームに関する情報を確認できます。

[Volume Status]列に、ペアリングおよび進捗に関するメッセージが表示されます。

Local Volume ID

システムによって生成されたボリュームのID。

Local Volume Name

ボリュームの作成時に指定した名前。ボリューム名は最大223文字で、使用できる文字はa～z、0～9、およびダッシュ (-) です。

Account

ボリュームに割り当てられているアカウントの名前。

Volume Replication status

ボリュームのレプリケーション ステータス。

Snapshot Replication status

Snapshotボリュームのレプリケーション ステータス。

Mode

クライアントの書き込みレプリケーション方法を示します。有効な値は次のとおりです。

- Asynchronous
- Snapshot-Only
- Synchronous

Local Volume Access

ボリューム ペアリングのローカル側のアクセス モード。

Direction

ボリューム データの方向を示します。

-  アイコンは、クラスタの外部のターゲットにデータを書き出していることを示します。
-  アイコンは、外部のソースからローカル ボリュームにデータが書き込まれていることを示します。

Remote Cluster

ボリュームが配置されているリモート クラスタの名前。

Remote Volume ID

リモート クラスタのボリュームのボリュームID。

Remote Volume Name

リモート ボリュームの作成時に指定した名前。

関連資料

[ボリューム ペアリングに関するメッセージ](#) (161ページ)

[ボリューム ペアリングに関する警告](#) (161ページ)

ボリューム ペアリングに関するメッセージ

NetApp Element Management拡張ポイントの[Protection]タブにある[Volume Pairs]ページで、最初のペアリング プロセス中に表示されるメッセージを確認できます。メッセージは[Volume Status]列に表示され、ペアリングのソースとターゲットの両方で表示することができます。

PausedDisconnected

ソース レプリケーションまたは同期RPCがタイムアウトし、リモート クラスタへの接続が失われました。クラスタへのネットワーク接続を確認してください。

ResumingConnected*

リモート レプリケーションの同期がアクティブになりました。同期処理が開始され、データを待っている状態です。

ResumingRRSync*

ペア クラスタにボリューム メタデータのSingle Helixコピーを作成しています。

ResumingLocalSync*

ペア クラスタにボリューム メタデータのDouble Helixコピーを作成しています。

ResumingDataTransfer*

データ転送が再開されました。

Active

ボリュームがペアリングされ、ソース ボリュームからターゲット ボリュームにデータが送信されて同期されています。

Idle

実行中のレプリケーション アクティビティはありません。

*この処理はターゲット ボリュームで開始され、ソース ボリュームには表示されない場合があります。

関連資料

[ボリューム ペアリングに関する警告](#) (161ページ)

ボリューム ペアリングに関する警告

NetApp Element Management拡張ポイントの[Protection]タブにある[Volume Pairs]ページで、ボリュームをペアリングしたあとに表示される警告メッセージを確認できます。メッセージは[Volume Status]列に表示され、ペアリングのソースとターゲットの両方で表示することができます。

特に記載がないかぎり、これらのメッセージはペアリングのソースとターゲットの両方に表示されます。

PausedClusterFull

ターゲット クラスタがいっぱいのため、ソース レプリケーションと一括データ転送を続行できません。このメッセージは、ペアのソースにのみ表示されます。

PausedExceededMaxSnapshotCount

ターゲット ボリュームに格納されたSnapshotの数が最大数に達しており、Snapshotをこれ以上レプリケートできません。

PausedManual

ローカル ボリュームが手動で一時停止されています。レプリケーションを再開するには、一時停止を解除する必要があります。

PausedManualRemote

リモート ボリュームが手動で一時停止されています。レプリケーションを再開するには、リモート ボリュームの一時停止を手動で解除する必要があります。

PausedMisconfigured

ソースとターゲットがアクティブになるのを待っています。手動でレプリケーションを再開する必要があります。

PausedQoS

ターゲット QoSの受信IOを維持できませんでした。レプリケーションは自動で再開されます。このメッセージは、ペアのソースにのみ表示されます。

PausedSlowLink

低速リンクが検出されたため、レプリケーションが停止しました。レプリケーションは自動で再開されます。このメッセージは、ペアのソースにのみ表示されます。

PausedVolumeSizeMismatch

ソース ボリュームよりも小さいターゲット ボリュームが使用されています。

PausedXCopy

ソース ボリュームに対してSCSI XCOPYコマンドを実行中です。このコマンドが完了するまでレプリケーションを再開できません。このメッセージは、ペアのソースにのみ表示されます。

StoppedMisconfigured

永続的な設定エラーが検出されました。リモート ボリュームがパージされたかペアが解除されました。対処方法はなく、新しいペアリングを確立する必要があります。

関連資料

[ボリューム ペアリングに関するメッセージ](#) (161ページ)

クラスタ管理

NetApp Element Management 拡張ポイントの[Cluster]タブから、クラスタ全体の設定を表示および変更したり、クラスタ固有のタスクを実行したりできます。

ドライブ

各ノードには1つ以上の物理ドライブが搭載され、クラスタのデータの一部分が格納されます。クラスタにドライブが追加されると、そのドライブの容量とパフォーマンスがクラスタで使用されるようになります。

ストレージ ノードには、次のタイプのドライブが含まれます。

ボリューム メタデータ ドライブ

クラスタ内の各ボリューム、クローン、またはSnapshotの定義情報を圧縮して格納します。システム内のメタデータ ドライブの合計容量により、ボリュームとしてプロビジョニング可能なストレージの最大容量が決まります。プロビジョニング可能なストレージの最大容量は、クラスタのブロック ドライブに実際に格納されるデータ量とは関係ありません。ボリューム メタデータ ドライブには、Double Helixデータ保護を使用してデータがクラスタ内に重複して格納されます。

注:一部のシステム イベント ログおよびエラー メッセージでは、ボリューム メタデータ ドライブではなくスライス ドライブと表記される場合があります。

ブロック ドライブ

サーバ アプリケーション ボリューム用に、重複排除済みのデータ ブロックを圧縮して格納します。ブロック ドライブはシステムのストレージ容量の大部分を占めます。データの書き込み要求に加えて、クラスタにすでに格納されているデータの読み取り要求の大部分がブロック ドライブで発生します。格納可能なデータの最大容量は、システム内のブロック ドライブの合計容量に、圧縮、シンプロビジョニング、および重複排除の効果を加味して決まります。

クラスタへの使用可能ドライブの追加

NetApp Element Management 拡張ポイントを使用して、クラスタにドライブを追加できます。クラスタにノードを追加したり、既存のノードに新しいドライブを設置すると、ドライブが自動的にAvailableとして登録されます。それぞれの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しておく必要があります。

タスク概要

次の場合、ドライブは[Available]リストに表示されません。

- ドライブがActive、Removing、Erasing、Failedのいずれかの状態である。
- ドライブが含まれているノードがPending状態である。

手順

1. [NetApp Element Management] > [Cluster]を選択します。

注: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。

2. [Drives]サブタブで、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のリストを表示します。

3. 次の手順でドライブを追加します。
 - a. 追加する各ドライブのチェックボックスを選択します。
 - b. **[Add Drives]**をクリックします。
4. 追加するドライブの詳細を確認し、操作を確定します。

ドライブの詳細

NetApp Element Management拡張ポイントの**[Cluster]**タブにある**[Drives]**ページの**[Active]**ビューで、クラスタ内のアクティブドライブのリストを確認できます。ドロップダウンフィルタで使用可能なオプションを選択すると、ビューを切り替えることができます。

クラスタを最初に初期化した時点では、アクティブドライブのリストは空です。新しいクラスタを作成したら、**[Available]**タブに表示されている、クラスタに割り当てられていないドライブを追加できます。アクティブドライブのリストに表示される項目は次のとおりです。

Drive ID

ドライブに割り当てられている連番。

Drive State

ドライブのステータス。

有効な値は次のとおりです。

- **Active** : クラスタで使用されているドライブです。
- **Available** : クラスタに追加できるドライブです。
- **Removing** : ドライブは現在削除中です。このドライブに以前保存されていたデータをクラスタ内の他のドライブに移行しています。
- **Erasing** : ドライブは完全消去中です。このドライブ上のデータは完全に消去されます。
- **Failed** : 障害が発生したドライブです。このドライブに以前保存されていたデータは、クラスタ内の他のドライブに移行されました。ドライブの自己診断によりそのドライブでエラーが発生したことがノードに通知された場合、あるいはドライブとの通信が5分半以上停止した場合、ドライブは障害状態になります。

Node ID

ノードがクラスタに追加された際に割り当てられたノード番号。

Node Name

ドライブが配置されているノードの名前。

Slot

ドライブが物理的に配置されているスロットの番号。

Capacity (GB)

ドライブのサイズ (GB)。

Serial

SSDのシリアル番号。

Wear Remaining

摩耗レベル インジケータ。

Type

ドライブ タイプはblockまたはmetadataです。

ドライブの削除

NetApp Element Management拡張ポイントを使用して、クラスタからドライブを削除できます。この操作は、クラスタの容量を減らしたり、サービス寿命の終わりに近づいているドライブの交換準備を行ったりするときに実行します。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、削除され、ドライブがクラスタから削除される前にすべて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、クラスタの容量の使用状況やアクティブなI/Oに応じて、数分から1時間かかります。

タスク概要

Failed状態のドライブを削除しても、ドライブの状態はAvailableまたはActiveには戻りません。そのドライブはクラスタで使用できなくなります。

手順

1. [NetApp Element Management] > [Cluster]を選択します。
2. 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。
3. ドロップダウン リストから[All]を選択して、すべてのドライブのリストを表示します。
4. 次の手順でドライブを削除します。
 - a. 削除する各ドライブのチェック ボックスを選択します。
 - b. [Remove Drives]をクリックします。
5. 操作を確定します。

注：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。

ノード

ノードは、クラスタにグループ化され、ブロックストレージまたはコンピューティング リソースとしてアクセスされるハードウェアです。

NetApp HCI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。ノード上のドライブには、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。

NetApp HCI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環境における仮想化に必要なリソース（CPU、メモリ、ネットワークなど）を提供するノードハードウェアです。各サーバがVMware ESXiを実行するため、NetApp HCIコンピューティング ノードの管理（ホストの追

加と削除)はプラグインの外部(vSphereの[Hosts and Clusters]メニュー)で行う必要があります。

SolidFireストレージ ノード

SolidFireオールフラッシュ アレイ ストレージ ノードは、CIP1 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ドライブの集まりです。ノード上のドライブには、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。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、または既存のクラスタにストレージ ノードを追加して、ストレージの容量およびパフォーマンスを拡張できます。

ストレージ ノードには次のような特徴があります。

- 各ノードには固有な名前が付けられます。管理者が名前を指定しない場合、ノードにはデフォルトで「SF-xxxx」という名前が付けられます。xxxxは、システムによってランダムに生成される任意の4文字です。
- 各ノードに高性能な専用のNon-Volatile Random Access Memory (NVRAM;不揮発性RAM)書き込みキャッシュが搭載されており、システム全体のパフォーマンスの向上と書き込みレイテンシの低減が実現します。
- 各ノードは2つの独立したリンクで2つのネットワークに接続され、冗長性とパフォーマンスが確保されます。それぞれのノードに各ネットワークのIPアドレスが必要です。
- クラスタに対するノードの追加や削除は、サービスを中断することなくいつでも実行できます。

SolidFire Fibre Channelノード

SolidFire Fibre ChannelノードはFibre Channelスイッチへの接続を提供し、Fibre ChannelスイッチはFibre Channelクライアントに接続できます。Fibre Channelノードは、Fibre ChannelプロトコルとiSCSIプロトコルの間のプロトコル コンバータとして機能するため、新規または既存のあらゆるSolidFireクラスタへのFibre Channel接続を追加できます。

Fibre Channelノードには次の特徴があります。

- Fibre Channelスイッチがファブリックの状態を管理し、相互接続が最適化されます。
- 2つのポート間のトラフィックはスイッチ経由でのみ送信され、他のポートには送信されません。
- ポートの障害は分離され、他のポートの動作には影響しません。
- 1つのファブリック内で複数のポート ペアが同時に通信することができます。

Fibre Channelノードはペアで追加され、アクティブ / アクティブ モードで動作します(すべてのFibre Channelノードがクラスタのトラフィックをアクティブに処理します)。SolidFireクラスタでのFibre Channel接続には、少なくとも2つのFibre Channelノードが必要です。

NetApp Elementソフトウェア9.0以降を実行しているクラスタでは、最大4つのFibre Channelノードがサポートされます。

クラスタへのノードの追加

クラスタを作成する場合やストレージの追加が必要な場合に、ストレージ ノードを追加できます。

開始する前に

- 追加するノードのセットアップ、電源投入、設定を完了しておきます。

- ソフトウェアの互換性を確保するために、ソフトウェアのメジャーバージョン番号とマイナーバージョン番号の両方がクラスタ内の各ノードで一致する必要があります。たとえば、Elementバージョン9.0とバージョン9.1は互換性がありません。

注: 追加するノードのNetApp Elementソフトウェアのメジャーバージョンまたはマイナーバージョンがクラスタで実行されているバージョンと異なる場合、クラスタマスターで実行されているNetApp Elementソフトウェアのバージョンに非同期で更新されます。更新されたノードは、自動的にクラスタに追加されます。この非同期プロセスの実行中、ノードの状態はpendingActiveになります。

タスク概要

ノードは、初回の電源投入時に初期設定を行う必要があります。ノードのセットアップと設定が完了すると、ノードの設定時に指定したクラスタにノードが登録され、NetApp Element Management拡張ポイントの[Cluster] > [Nodes]ページにある選択可能なノードのリストに表示されます。

既存のクラスタには、大きささまざまな容量のノードを追加できます。

手順は、NetApp Elementソフトウェアを実行しているFibre Channelノードまたはストレージノードを追加する場合と同じです。

手順

1. [NetApp Element Management] > [Cluster]を選択します。
注: 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。
2. [Nodes]サブタブをクリックします。
3. 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。
4. ノードを追加するには、次の手順を実行します。
 - a. 追加する各ノードのチェック ボックスを選択します。
 - b. [Add Node]をクリックします。
5. 追加するノードの詳細を確認し、操作を確定します。
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。

ノードの詳細

NetApp Element Management拡張ポイントの[Cluster]タブにある[Nodes]ページで、クラスタ内のノードの一覧を表示できます。アクティブ ノードの一覧を表示するには、[Active]ビューを選択する必要があります。ドロップダウン フィルタを使用して[Pending]、[PendingActive]、[All]のいずれかのオプションを選択すると、ビューを切り替えることができます。

Node ID

システムによって生成されたノードのID。

Node Name

システムによって生成されたか管理者が割り当てたノード名。

Node State

ノードのステータス。

有効な値は次のとおりです。

- **Active** : ノードはクラスタのアクティブなメンバーであり、別のクラスタに追加できません。
- **Pending** : ノードは特定の名前付きクラスタに対してPendingの状態、追加可能です。
- **PendingActive** : ノードは工場出荷時のソフトウェア イメージに戻されており、まだクラスタのアクティブなメンバーではありません。完了すると、**Active**状態に移行します。

Available 4k IOPS

ノードに設定されたIOPSが表示されます。

Node Role

クラスタ内でのノードのロールを示します。Cluster Master、Ensemble Member、Fibre Channel Nodeのいずれかです。

Node Type

ノードのモデル タイプが表示されます。

Active Drives

ノード内のアクティブ ドライブの数。

Management IP

ノードに割り当てられた管理IP（MIP）アドレス。1GbEまたは10GbEネットワークの管理タスクで使用されます。

Storage IP

ノードに割り当てられたストレージIP（SIP）アドレス。iSCSIネットワークの検出およびすべてのデータ ネットワーク トラフィックに使用されます。

Management VLAN ID

管理ローカル エリア ネットワークの仮想ID。

Storage VLAN

ストレージ ローカル エリア ネットワークの仮想ID。

Version

各ノードで実行されているNetApp Elementソフトウェアのバージョン。

クラスタからのノードの削除

ノードのストレージが不要になったときや、ノードのメンテナンスが必要なときは、サービスを中断することなくクラスタからノードを削除できます。

開始する前に

ノード内のすべてのドライブをクラスタから削除しておきます。*RemoveDrives*のプロセスが完了してすべてのデータがノードから移行されるまで、ノードを削除することはできません。

タスク概要

NetApp ElementクラスタでのFibre Channel接続には、少なくとも2つのFibre Channelノードが必要です。Fibre Channelノードが1つしか接続されていない場合、別のFibre Channelノードをクラスタに追加するまで[Event Log]にアラートが記録されます。ただしFibre Channelのすべてのネットワーク トラフィックは、Fibre Channelノードが1つしかない状態でも引き続き処理されます。

手順

1. [NetApp Element Management] > [Cluster]を選択します。
注：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。
2. [Nodes]サブタブをクリックします。
3. 1つ以上のノードを削除するには、次の手順を実行します。
 - a. [Active]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ます。
 - b. [Actions]をクリックします。
 - c. [Remove]を選択します。
4. 操作を確定します。
 クラスタから削除されたノードは、[Pending]のノード リストに表示されます。

関連タスク

[ドライブの削除](#) (165ページ)

クラスタ ノードの再起動

NetApp Element Management拡張ポイントを使用して、クラスタ内の1つ以上のアクティブノードを再起動できます。

開始する前に

同時に複数のノードを再起動する場合は、I/Oを停止し、すべてのiSCSIセッションを切断しておきます。

タスク概要

クラスタを再起動するには、すべてのクラスタ ノードを選択します。

注意：このメソッドは、ノードのすべてのネットワークサービスをリスタートします。このため、ネットワーク接続が一時的に失われます。

手順

1. [NetApp Element Management] > [Cluster]を選択します。
注：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。
2. [Nodes]サブタブをクリックします。
3. [Active]ビューで、再起動する各ノードのチェックボックスを選択します。
4. [Actions]をクリックします。
5. [Restart]を選択します。
6. 操作を確定します。

クラスタ ノードのシャットダウン

NetApp Element Management拡張ポイントを使用して、クラスタ内の1つ以上のアクティブノードをシャットダウンできます。クラスタをシャットダウンするには、すべてのクラスタノードを選択して同時にシャットダウンします。

開始する前に

同時に複数のノードをシャットダウンする場合は、I/Oを停止し、すべてのiSCSIセッションを切断しておきます。

手順

1. [NetApp Element Management] > [Cluster]を選択します。

注：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。

2. [Nodes]サブタブをクリックします。
3. [Active]ビューで、シャットダウンする各ノードのチェックボックスを選択します。
4. [Actions]をクリックします。
5. [Shutdown]を選択します。
6. 操作を確定します。

注：ノードが何らかの理由でシャットダウン状態になって5分半以上が経過すると、NetApp Elementソフトウェアはノードが再びクラスタに参加することはないと判断します。Double Helixデータ保護は、レプリケートされた個々のブロックを別のノードに書き込んでデータをレプリケートするタスクを開始します。ノードがシャットダウンしていた時間によっては、ノードがオンラインに戻ったあとにドライブを再度クラスタに追加する必要があります。

関連タスク

[クラスタ ノードの再起動](#) (169ページ)

関連情報

[Powering off and powering on a NetApp HCI system](#)

VLANの管理

NetApp Elementストレージの仮想ネットワークを使用すると、別々の論理ネットワークに属する複数のクライアント間のトラフィックを1つのNetApp Elementクラスタに接続できます。Elementでは、仮想ネットワークを実装する基盤テクノロジーとしてVLANを使用しています。

NetApp Element Plug-in for vCenterでは、選択したクラスタのVLANを管理できます。VLANの作成、表示、編集、削除が可能です。VLANの管理オプションは、NetApp Element Management拡張ポイントからのみ使用できます。

VLANの作成

クラスタ構成に新しい仮想ネットワークを追加すると、マルチテナント環境からNetApp Elementソフトウェアを実行しているクラスタに接続できるようになります。

開始する前に

- ESXiホストにiSCSIソフトウェア アダプタが1つ必要です。
- VLAN用にホストまたはスイッチが設定されている必要があります。
- クラスタ ノード上の仮想ネットワークに割り当てるIPアドレス範囲を特定しておきます。
- NetApp Elementのすべてのストレージ トラフィックのエンドポイントとして使用するストレージ ネットワークIP (SVIP) アドレスを特定しておきます。

注意：この構成では、次の条件を考慮する必要があります。

- VRFは、VLANの作成時にのみ有効にすることができます。非VRFに戻す場合は、VLANを削除して再作成する必要があります。
- VRFが有効でないVLANでは、SVIPと同じサブネットにイニシエータが含まれている必要があります。
- VRFが有効なVLANでは、SVIPと同じサブネットにイニシエータが含まれている必要はなく、ルーティングがサポートされます。

タスク概要

仮想ネットワークを追加すると、各ノードのインターフェイスが作成され、そのそれぞれに仮想ネットワークIPアドレスが必要となります。新しい仮想ネットワークを作成する際に指定するIPアドレスの数は、クラスタ内のノードの数以上であることが必要です。仮想ネットワーク アドレスはまとめてプロビジョニングされ、個々のノードに自動的に割り当てられます。仮想ネットワーク アドレスをクラスタ内のノードに手動で割り当てる必要はありません。

手順

1. [NetApp Element Management] > [Cluster]を選択します。
注：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。
2. [Network]サブタブをクリックします。
3. [Create VLAN]をクリックします。
4. [Create VLAN]ダイアログ ボックスで、VLANの名前を入力します。
5. VLANタグを整数で入力します。
6. ストレージ クラスタのストレージ仮想IP (SVIP) アドレスを入力します。
7. 必要に応じて、ネットマスクを調整します。

デフォルトは

255.255.255.0

です。

8. オプション：VLANの説明を入力します。
9. オプション：[Enable Virtual Routing and Forwarding]チェック ボックスを選択します。
 注：仮想ルーティング / 転送（VRF）を有効にすると、ルーティング テーブルの複数のインスタンスをルータ内に共存させ、同時に使用することができます。この機能はストレージ ネットワークでのみ使用できます。
 - a. 仮想ネットワークのゲートウェイのIPアドレスを入力します。
10. VLANに含めるホストを選択します。
 注：vCenterリンク モードを使用している場合は、クラスタが割り当てられているvCenter Serverから使用可能なホストのみを選択できます。
11. ストレージ ノードのIPアドレス ブロックを次の手順で設定します。
 注：少なくとも1つのIPアドレス ブロックを作成する必要があります。
 - a. [Create Block]をクリックします。
 - b. IP範囲の開始アドレスを入力します。
 - c. アドレス ブロックに含めるIPアドレスの数を入力します。
 注：IPアドレスの総数は、ストレージ クラスタのノードの数と一致しなければなりません。
 - d. エントリの外部をクリックして値を受け入れます。
12. [OK]をクリックしてVLANを作成します。

仮想ネットワークの詳細

NetApp Element Management拡張ポイントの[Cluster]タブにある[Network]ページで、VLANに関するネットワーク情報を確認できます。

ID

Elementシステムによって割り当てられたVLANネットワークの一意のID。

VLAN Name

VLANネットワークにユーザが割り当てた一意の名前。

VLAN Tag

仮想ネットワークの作成時に割り当てられたVLANタグ。

SVIP

仮想ネットワークに割り当てられたストレージ仮想IPアドレス。

IPs Used

仮想ネットワークで使用される仮想ネットワークIPアドレスの範囲。

仮想ネットワークの編集

VLAN名、ネットマスク、IPアドレス ブロックのサイズなどのVLAN属性を変更できます。

タスク概要

VLANのVLANタグおよびSVIPは変更できません。ゲートウェイ属性を変更できるのはVRF VLANのみです。iSCSI、リモートレプリケーション、またはその他のネットワーク セッションの実行中は、変更失敗することがあります。

手順

1. [NetApp Element Management] > [Cluster]を選択します。
 注：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。
2. [Network]サブタブをクリックします。
3. 編集するVLANのチェックボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Edit]をクリックします。
6. 表示されたメニューで、VLANの新しい属性を入力します。
7. 仮想ネットワークに連続しないIPアドレス ブロックを追加するには、[Create Block]をクリックします。
8. [OK]をクリックします。

仮想ネットワークの削除

VLANオブジェクトとそのIPブロックを完全に削除できます。VLANに割り当てられていたアドレスブロックは、割り当てが解除されて、別の仮想ネットワークに再割り当てできるようになります。

手順

1. [NetApp Element Management] > [Cluster]を選択します。
 注：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。
2. [Network]サブタブをクリックします。
3. 削除するVLANのチェックボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Delete]をクリックします。
6. 操作を確定します。

仮想ボリューム

NetApp Element Management拡張ポイントから、仮想ボリュームおよび仮想ボリュームに関連付けられたストレージ コンテナ、プロトコル エンドポイント、バインド、およびホストの情報を確認して、タスクを実行できます。Virtual Volumes機能をクラスタで使用できるように事前に有効にしておく必要があります。

vSphere Virtual Volumes (VVol) 機能の設定

NetApp Element Plug-in for vCenter Serverで仮想ボリューム（VVol）機能を使用するには、初期設定手順を実行する必要があります。

開始する前に

NetApp ElementクラスタがVVolに対応したESXi 6.0以降の環境に接続されている必要があります。

手順

1. NetApp Element Configuration拡張ポイントを使用して、NetApp Elementクラスタの仮想ボリューム機能を有効にします。
2. VASA ProviderをvCenterに登録します。
3. NetApp Element Management拡張ポイントを使用して、ストレージ コンテナおよび関連付けるVVolデータストアを作成します。
4. ストレージ コンテナの作成時にデータストアを作成しなかった場合は、vCenterでVVolデータストアを作成してストレージ コンテナに関連付けます。

関連タスク

[Virtual Volumesの有効化](#)（58ページ）

[NetApp Element VASA Providerの登録](#)（174ページ）

[ストレージ コンテナの作成](#)（181ページ）

[VVolデータストアの作成](#)（175ページ）

NetApp Element VASA Providerの登録

vCenterでクラスタのVVol機能が認識されるように、NetApp Element VASA ProviderをvCenterに登録する必要があります。vCenterへのVASA Providerの登録は1度だけ実行します。

開始する前に

- クラスタでVVol機能を有効にしておきます。
- vCenter 6.xが必要です。
- ESXi 6.xが必要です。

注意： NetApp Element VASA Providerを複数のvCenterインスタンスに登録しないでください。vCenterでのSSLの処理に制約があるため、NetApp Element VASA Providerは1つのvCenterにしか登録できません。1つのvCenterに複数のNetApp Elementクラスタを作成できますが、2つのvCenterインスタンス間でクラスタを共有することはできません。

タスク概要

ここでは、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。

手順

1. vCenter Serverで、**[Hosts and Clusters]**を選択します。
2. NetApp Element VASA Providerを登録するvCenter Serverを選択します。
3. **[Configure] > [Storage Providers]**を選択します。
4. **[Storage Providers]**で、追加アイコンをクリックします。
[New Storage Provider]ダイアログ ボックスが表示されます。
5. 次の情報を入力します。
 - VASA Providerの名前。
 - VASA ProviderのURL。
 注：VASA ProviderのURLは、vCenter Plug-inでVVolを有効にすると提供されます。また、このURLは、**[NetApp Element Configuration] > [Clusters]**で有効にするクラスタの**[Actions]**をクリックし、**[Details]**をクリックすると確認できます。
 - NetApp Elementクラスタの管理用アカウントのユーザ名。
 - NetApp Elementクラスタの管理用アカウントのパスワード。
 - **[OK]**をクリックしてVASA Providerを追加します。
6. プロンプトが表示されたら、SSLのサムプリントを承認します。
 これでNetApp Element VASA Providerが登録され、ステータスがConnectedになります。
 注：プロバイダの初回登録後にプロバイダの最新のステータスを表示するには、ストレージ プロバイダを更新します。**[NetApp Element Configuration] > [Clusters]**で、プロバイダが有効になっていることを確認することもできます。有効にするクラスタの**[Actions]**をクリックし、**[Details]**をクリックします。

VVolデータストアの作成

NetApp Elementクラスタ上のストレージ コンテナを表す仮想ボリューム データストアをvCenterで作成する必要があります。VVolデータストアは、ストレージ コンテナ作成ウィザードまたは以下のプロセスを使用して作成できます。VVolを使用する仮想マシンのプロビジョニングを開始するためには、少なくとも1つのVVolデータストアを作成する必要があります。

開始する前に

- VVol機能が有効になっているNetApp Elementソフトウェアがクラスタで実行されている必要があります。
- 仮想環境にストレージ コンテナが存在している必要があります。
- VASA ProviderをvCenterに登録する必要があります。

注：場合によっては、vCenterでNetApp Elementストレージを再スキャンし、ストレージ コンテナを検出する必要があります。

手順

1. vCenterの**ナビゲータ** ビューで、ストレージ クラスタを右クリックし、**[Storage] > [Datastores] > [New Datastore]**を選択します。
2. **[New Datastore]**ダイアログ ボックスで、作成するデータストアのタイプとして**[VVol]**を選択します。
3. **[Datastore name]**フィールドにデータストアの名前を入力します。
4. **[Backing Storage Container]**リストからNetApp Elementストレージ コンテナを選択します。
 注：プロトコル エンドポイント（PE）のLUNを手動で作成する必要はありません。
 LUNはデータストアが作成されると自動的にESXiホストにマッピングされます。
5. データストアへのアクセスを必要とするホストを選択します。
6. **[Next]**をクリックします。
7. 設定を確認し、**[Finish]**をクリックしてVVolデータストアを作成します。

関連タスク

[Virtual Volumesの有効化](#)（58ページ）
[NetApp Element VASA Providerの登録](#)（174ページ）
[ストレージ コンテナの作成](#)（181ページ）

仮想ボリュームの詳細の表示

NetApp Element Management拡張ポイントでは、クラスタ上のすべてのアクティブな仮想ボリュームに関する全般的な情報を確認できます。また、各仮想ボリュームに固有な情報（効率性、パフォーマンス、QoSなど）および関連付けられているSnapshot、親仮想マシン、バインド、タスク ステータスも確認できます。

開始する前に

- VVolの有効化およびVASA Providerの登録を完了しておきます。
- 仮想ボリュームを少なくとも1つ作成しておきます。
- 仮想ボリュームの詳細が表示されるようにVMの電源をオンにしておきます。

手順

1. **[NetApp Element Management] > [VVols]**を選択します。
 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。
2. **[Virtual Volumes]**タブで、特定の仮想ボリュームを検索します。
3. 確認する仮想ボリュームのチェック ボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Details]**を選択します。

関連タスク

[vSphere Virtual Volumes \(VVol\) 機能の設定](#)（174ページ）

仮想ボリュームの詳細

NetApp Element Management拡張ポイントの[VVols]タブにある[Virtual Volumes]ページで、クラスタ上のすべてのアクティブな仮想ボリュームに関する情報を確認できます。

Virtual Machine ID

仮想マシンのUUID。

Name

仮想ボリュームに割り当てられている名前。

Type

仮想ボリュームのタイプ (Config、Data、Memory、Swap、またはOther)。

Container

仮想ボリュームを所有するストレージ コンテナのUUID。

Volume ID

基盤となるボリュームのID。

Virtual Volume ID

仮想ボリュームのUUID。

個々の仮想ボリュームの詳細

NetApp Element Management拡張ポイントの[VVols]タブにある[Virtual Volumes]ページでは、個々の仮想ボリュームを選択してその詳細を表示し、仮想ボリューム情報を確認できます。

[General Details]セクションには次の情報が表示されます。

Name

仮想ボリュームに割り当てられている名前。

Volume ID

基盤となるボリュームのID。

Virtual Volume ID

仮想ボリュームのUUID。

Virtual Volume Type

仮想ボリュームのタイプ (Config、Data、Memory、Swap、またはOther)。

Status

VVolタスクのステータス。

Storage Container

仮想ボリュームを所有するストレージ コンテナのUUID。

Size

ボリュームのサイズ (GBまたはGiB)。

Access

仮想ボリュームに割り当てられている読み取り / 書き込み権限。

[Efficiency]セクションには次の情報が表示されます。

Compression

ボリュームの圧縮による削減率。

Deduplication

ボリュームの重複排除による削減率。

Thin Provisioning

ボリュームのシンプロビジョニングによる削減率。

Last Updated

前回の削減率更新日時。

[Performance]セクションには、次の詳細が表示されます。

Account ID

関連付けられているアカウントの一意のアカウントID。

Actual IOPS

過去500ミリ秒の、ボリュームに対する実際のIOPS。

Async Delay

ボリュームが最後にリモート クラスタと同期されてからの時間。

Average IOP Size

過去500ミリ秒の、ボリュームに対する最新のI/Oの平均サイズ（バイト）。

Burst IOPS Size

ユーザが利用可能なIOPクレジットの合計数。ボリュームが最大IOPSに到達していない場合、クレジットは蓄積されます。

Client Queue Depth

ボリュームに対する未処理の読み取りおよび書き込み処理の数。

Last Updated

前回のパフォーマンス更新日時。

Latency USec

過去500ミリ秒の、ボリュームに対する処理が完了するまでの平均時間（マイクロ秒）。値「0」（ゼロ）はボリュームに対するI/Oがなかったことを意味します。

Non-Zero Blocks

前回のガベージ コレクション完了後、データが含まれる4KiBブロックの総数。

Performance Utilization

消費されているクラスタIOPSの割合。たとえば、25万IOPSのクラスタが10万IOPSで実行されている場合、消費率は40%です。

Read Bytes

ボリュームの作成以降にボリュームから読み込んだ累積バイト総数。

Read Latency USec

過去500ミリ秒の、ボリュームに対する読み取り処理が完了するまでの平均時間（マイクロ秒）。

Read Operations

ボリューム作成以降にボリュームに対して行った読み取り処理の合計数。

Thin Provisioning

ボリュームのシンプロビジョニングによる削減率。

Throttle

0～1の浮動小数点数。データの再レプリケーション、一時的なエラー、Snapshotの作成のために、クライアントの処理量をmaxIOPS未満に抑えている割合。

Total Latency USec

ボリュームに対する読み取りおよび書き込み処理が完了するまでの時間（マイクロ秒）。

Unaligned Reads

512eボリュームの場合、4kセクターの境界に沿っていない読み取り処理の数。アラインされていない読み取りが多数ある場合は、パーティションのアライメントが適切でない可能性があります。

Unaligned Writes

512eボリュームの場合、4kセクターの境界に沿っていない書き込み処理の数。アラインしていない書き込みが多数ある場合は、パーティションのアライメントが適切でない可能性があります。

Volume ID

システムによって生成されたボリュームのID。

Volume Size

ボリュームのサイズ (バイト)。

Volume Utilization

クライアントによるボリュームの使用率を示すパーセンテージ。

有効な値は次のとおりです。

- 0 : クライアントはボリュームを使用していません。
- 100 : クライアントは最大値まで使用しています。
- >100 : クライアントはバースト値を使用しています。

Write Bytes

ボリュームの作成以降にボリュームに書き込まれた累積バイト総数。

Write Latency USec

過去500ミリ秒の、ボリュームに対する書き込み処理が完了するまでの平均時間 (マイクロ秒)。

Write Operations

ボリュームの作成以降にボリュームに対して行った書き込み処理の累積総数。

Zero Blocks

前回のガベージ コレクション完了後、データが含まれない4KiBブロックの総数。

Used Capacity

使用済み容量の割合。

[Quality of Service]セクションには、次の詳細が表示されます。

I/O Size

IOPSのサイズ (KB)。

Min IOPS

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。

Max IOPS

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。

Max Bandwidth

ブロックサイズの増加に対応するために使用が許可される最大帯域幅。

[Virtual Machine]セクションには、次の詳細が表示されます。

Virtual Machine ID

仮想マシンのUUID。

VM Name

仮想マシンの名前。

Guest OS Type

仮想ボリュームに関連付けられたオペレーティング システム。

Virtual Volumes

仮想ボリュームのUUIDおよびVM名のリスト。

[Bindings]セクションには次の見出しがあります。

Host

仮想ボリュームをホストしていて、クラスタが認識しているESXiホストのUUID。

Protocol Endpoint ID

クラスタ内の各ノードに対応するプロトコル エンドポイントID。

PE Type

プロトコル エンドポイントのタイプ（NetApp Elementソフトウェアで使用可能なプロトコルはSCSIのみです）。

[Tasks]セクションには、次の詳細が表示されます。

Operation

タスクが実行している処理のタイプ。

値は次のとおりです。

- unknown：不明なタスク処理です。
- prepare：タスクは仮想ボリュームを準備中です。
- snapshot：タスクは仮想ボリュームのSnapshotの作成中です。
- rollback：タスクは仮想ボリュームをSnapshotにロールバック中です。
- clone：タスクは仮想ボリュームのクローンを作成中です。
- fastClone：タスクは仮想ボリュームの高速クローンを作成中です。
- copyDiffs：タスクは仮想ボリュームに異なるブロックをコピー中です。

Status

仮想ボリューム タスクの現在のステータス。

値は次のとおりです。

- Error：タスクは失敗し、エラーが返されました。
- Queued：タスクは実行待ちです。
- Running：タスクは現在実行中です。
- Success：タスクは正常に完了しました。

Task ID

タスクの一意のID。

ストレージ コンテナ

ストレージ コンテナは、NetApp Elementアカウントにマッピングされた論理構成要素であり、レポートの作成やリソースの割り当てに使用されます。このコンテナには、ストレージシステムが仮想ボリュームに提供できる物理ストレージ容量またはアグリゲートのストレージ機能がプールされます。vSphereで作成されたVVolデータストアは、個々のストレージ コンテナにマッピングされます。1つのストレージ コンテナには、NetApp Elementクラスタから使用可能なリソースがデフォルトですべて含まれています。マルチテナンシーをより詳細に管理する必要がある場合は、複数のストレージ コンテナを作成できます。

ストレージ コンテナは従来のアカウントと同じように機能し、仮想ボリュームとトラディショナル ボリュームの両方を格納できます。クラスタごとに最大4つのストレージ コンテナがサポートされます。VVol機能を使用するには、少なくとも1つのストレージ コンテナが必要です。NetApp Element Management拡張ポイントの[VVols] > [Storage Containers]ページで、ストレージ コンテナの作成、削除、および詳細の表示を行うことができます。vCenterではVVolの作成時にストレージ コンテナを検出できます。

ストレージ コンテナの作成

ストレージ コンテナはNetApp Element Management拡張ポイントの[VVols]タブで作成できます。VVolを使用する仮想マシンのプロビジョニングを開始するためには、少なくとも1つのストレージ コンテナを作成する必要があります。

開始する前に

- クラスタでVVol機能を有効にしておきます。
- 仮想ボリューム用のNetApp Element VASA ProviderをvCenterに登録しておきます。

手順

1. [NetApp Element Management] > [VVols]を選択します。
注：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。
2. [Storage Containers]サブタブをクリックします。
3. [Create Storage Container]をクリックします。
4. [Create a New Storage Container]ダイアログ ボックスにストレージ コンテナ情報を入力します。
 - a. ストレージ コンテナの名前を入力します。
ヒント：わかりやすい命名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。
 - b. CHAP用のイニシエータ シークレットとターゲット シークレットを設定します。
ベストプラクティス：シークレットを自動生成するには、[CHAP Settings]フィールドを空白のままにしてください。
 - c. オプション：データストアの名前を入力します。[Create a datastore]チェック ボックスはデフォルトで選択されます。

注：vSphereでストレージ コンテナを使用するにはVVolデータストアが必要です。ここでデータストアを作成しない場合は、あとでvSphereの新しいデータストアウィザードを使用してデータストアを作成する必要があります。

d. データストアのホストを1つ以上選択します。

注：vCenterリンク モードを使用している場合は、クラスタが割り当てられているvCenter Serverから使用可能なホストのみを選択できます。

e. **[OK]**をクリックします。

5. 新しいストレージ コンテナが**[Storage Containers]**サブタブのリストに表示されていることを確認します。

注：NetApp ElementアカウントIDは自動的に作成されてストレージ コンテナに割り当てられるため、アカウントを手動で作成する必要はありません。

6. オプション：**[Create a datastore]**を選択した場合は、関連するデータストアもvCenterの選択したホストに作成されていることを確認します。

関連概念

[複数クラスタを管理する場合のオブジェクト名のベストプラクティス](#) (53ページ)

関連タスク

[vSphere Virtual Volumes \(VVol\) 機能の設定](#) (174ページ)

ストレージ コンテナの詳細の表示

NetApp Element Management拡張ポイントでは、クラスタ上のすべてのアクティブなストレージ コンテナに関する情報を確認できます。効率とパフォーマンスの指標、関連付けられた仮想ボリュームなど、各ストレージ コンテナの詳細も確認できます。

開始する前に

- クラスタでVVol機能を有効にしておきます。
- 少なくとも1つのストレージ コンテナが選択可能である必要があります。

手順

1. **[NetApp Element Management]** > **[VVols]**を選択します。

注：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。

2. **[Storage Containers]**タブをクリックします。
3. 確認するストレージ コンテナのチェック ボックスを選択します。
4. **[Actions]**をクリックします。
5. 表示されたメニューで**[Details]**を選択します。

関連タスク

[vSphere Virtual Volumes \(VVol\) 機能の設定](#) (174ページ)

ストレージ コンテナの詳細

NetApp Element Management 拡張ポイントの[VVols]タブにある[Storage Containers]ページでは、クラスタ上のすべてのアクティブなストレージ コンテナに関する情報を確認できます。

Account ID

ストレージ コンテナに関連付けられたNetApp Element アカウントのID。

Name

ストレージ コンテナの名前。

Status

ストレージ コンテナのステータス。

有効な値は次のとおりです。

- Active : ストレージ コンテナが使用中です。
- Locked : ストレージ コンテナがロックされています。

Volume Count

ストレージ コンテナ アカウントに関連付けられたアクティブな仮想ボリュームの数。

個々のストレージ コンテナの詳細

NetApp Element Management 拡張ポイントの[VVols]タブにある[Storage Containers]ページでは、個々のストレージ コンテナを選択してその詳細を表示し、ストレージ コンテナ情報を確認できます。

[General Details]セクションには次の情報が表示されます。

Account ID

ストレージ コンテナに関連付けられたクラスタ アカウントのID。

Storage container ID

仮想ボリュームのストレージ コンテナのUUID。

Storage Container Name

関連付けられているストレージ コンテナの名前。

Datastore Name

関連付けられているデータストアの名前。

Status

ストレージ コンテナのステータス。

有効な値は次のとおりです。

- Active : ストレージ コンテナは使用中です。
- Locked : ストレージ コンテナはロックされています。

Protocol Endpoint Type

プロトコル エンドポイントのタイプ (NetApp Elementソフトウェアで使用可能なプロトコルはSCSIのみです)。

Initiator Secret

イニシエータの一意のCHAPシークレット。

Target Secret

ターゲットの一意のCHAPシークレット。

Number of Volumes

ストレージ コンテナ アカウントに関連付けられたボリ्यूムの数。

[Efficiency]セクションには次の情報が表示されます。

Compression

アカウント内のボリ्यूムの圧縮による削減率。

Deduplication

アカウント内のボリ्यूムの重複排除による削減率。

Thin Provisioning

アカウント内のボリ्यूムのシンプロビジョニングによる削減率。

Missing Volumes

効率性に関するデータを照会できなかったボリ्यूム。

Last Updated

前回の削減率更新日時。

[Performance Metrics]セクションには次の情報が表示されます。

Read Bytes

アカウント内のすべてのボリ्यूムから読み取られたバイト数の累積合計。

Read Operations

アカウント作成以降にアカウント内のすべてのボリ्यूムに対して行った読み取り処理の合計数。

Write Bytes

アカウント内のすべてのボリ्यूムに書き込まれたバイト数の累積合計。

Write Operations

アカウント作成以降にアカウント内のすべてのボリ्यूムに対して行った書き込み処理の合計数。

Unaligned Reads

アカウント内のすべての512eボリ्यूム（仮想ボリ्यूムはデフォルトで512e）について、4kセクターの境界に沿っていない読み取り処理の数。アラインされていない読み取りが多数ある場合は、パーティションのアライメントが適切でない可能性があります。

Unaligned Writes

アカウント内のすべての512eボリ्यूム（仮想ボリ्यूムはデフォルトで512e）について、4kセクターの境界に沿っていない書き込み処理の数。アラインしていない書き込みが多数ある場合は、パーティションのアライメントが適切でない可能性があります。

Non-Zero Blocks

前回のガベージ コレクション完了後、データが含まれる4KiBブロックの総数。

Zero Blocks

前回のガベージ コレクション完了後、データが含まれない4KiBブロックの総数。

Last Updated

前回のパフォーマンス更新日時。

[Virtual Volumes]セクションには次の情報が表示されます。

Volume ID

基盤となるボリュームのID。

Virtual Volume ID

仮想ボリュームのUUID。

Name

仮想ボリュームの名前。

Status

VVolタスクのステータス。

ストレージ コンテナの削除

NetApp Element Management拡張ポイントからストレージ コンテナを削除できます。

開始する前に

- 既存のストレージ コンテナが削除可能である必要があります。
- すべてのボリュームをストレージ コンテナから削除しておく必要があります。

手順

1. [NetApp Element Management] > [VVols]を選択します。
 注：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。
2. [Storage Containers]タブをクリックします。
3. 削除するストレージ コンテナのチェック ボックスを選択します。
4. [Actions]をクリックします。
5. 表示されたメニューで[Delete]を選択します。
6. 操作を確定します。
7. [Storage Containers]サブタブでストレージ コンテナのリストを更新して、ストレージ コンテナが削除されていることを確認します。

プロトコル エンドポイント

VMware ESXiホストは、論理I/Oプロキシ（プロトコル エンドポイント）を使用して仮想ボリュームと通信します。ESXiホストは、I/O処理を実行するために仮想ボリュームをプロトコル エンドポイントにバインドします。ホスト上の仮想マシンがI/O処理を実行すると、関連付けられているプロトコル エンドポイントがバインドされている仮想ボリュームにI/Oを転送します。

NetApp Elementクラスタ内のプロトコル エンドポイントは、SCSI管理論理ユニットとして機能します。各プロトコル エンドポイントはクラスタによって自動的に作成されます。クラスタ内のノードごとに、対応するプロトコル エンドポイントが作成されます。たとえば、4ノード クラスタの場合は4つのプロトコル エンドポイントが作成されます。

NetApp ElementソフトウェアでサポートされているプロトコルはiSCSIだけです。Fibre Channelプロトコルはサポートされません。

ユーザがプロトコル エンドポイントを削除または変更することはできません。プロトコル エンドポイントはアカウントには関連付けられず、またボリューム アクセス グループに追加することはできません。

NetApp Element Management 拡張ポイントの[VVols] > [Protocol Endpoints] ページでは、プロトコル エンドポイント情報を確認できます。

プロトコル エンドポイントの詳細の表示

NetApp Element Management 拡張ポイントでは、クラスタ上のすべてのプロトコル エンドポイントに関する情報を確認できます。

手順

1. [NetApp Element Management] > [VVols] を選択します。
注： 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。
2. [Protocol Endpoints] タブをクリックします。
 クラスタ上のすべてのプロトコル エンドポイントに関する情報が表示されます。
3. 確認するプロトコル エンドポイントのチェック ボックスを選択します。
4. [Actions] をクリックします。
5. 表示されたメニューで [Details] を選択します。

プロトコル エンドポイントの詳細

NetApp Element Management 拡張ポイントの[VVols] タブにある[Protocol Endpoint] ページでは、クラスタ上のすべてのプロトコル エンドポイントに関する情報を確認できます。

Primary Provider

プライマリ プロトコル エンドポイント プロバイダのID。

Secondary Provider

セカンダリ プロトコル エンドポイント プロバイダのID。

Protocol Endpoint ID

プロトコル エンドポイントのUUID。

Status

プロトコル エンドポイントのステータス。

有効な値は次のとおりです。

- Active : プロトコル エンドポイントは使用中です。
- Start : プロトコル エンドポイントは起動中です。
- Failover : プロトコル エンドポイントはフェイルオーバーしました。
- Reserved : プロトコル エンドポイントはリザーブされています。

Provider Type

プロトコル エンドポイント プロバイダのタイプ。

有効な値は次のとおりです。

- Primary

- Secondary

SCSI NAA Device ID

プロトコル エンドポイントのSCSIデバイスのグローバル一意識別子（NAA IEEE Registered Extended形式）。

個々のプロトコル エンドポイントの詳細

NetApp Element Management 拡張ポイントの[VVols]タブにある[Protocol Endpoint]ページでは、個々のプロトコル エンドポイントを選択してその詳細を表示し、プロトコル エンドポイント情報を確認できます。

注：仮想ボリュームの詳細は、VMの電源がオンになっているときにのみ表示されます。

Primary Provider ID

プライマリ プロトコル エンドポイント プロバイダのID。

Secondary Provider ID

セカンダリ プロトコル エンドポイント プロバイダのID。

Protocol Endpoint ID

プロトコル エンドポイントのUUID。

Status

プロトコル エンドポイントのステータス。

有効な値は次のとおりです。

- Active : プロトコル エンドポイントは使用中です。
- Start : プロトコル エンドポイントは起動中です。
- Failover : プロトコル エンドポイントはフェイルオーバーしました。
- Reserved : プロトコル エンドポイントはリザーブされています。

Provider Type

プロトコル エンドポイント プロバイダのタイプ。

有効な値は次のとおりです。

- Primary
- Secondary

SCSI NAA Device ID

プロトコル エンドポイントのSCSIデバイスのグローバル一意識別子（NAA IEEE Registered Extended形式）。

[Hosts]セクションには次の情報が表示されます。

Host Name

ESXiホストの名前。

Host Address

ESXiホストのIPアドレスまたはDNS名。

Initiator

仮想ボリュームのホストのイニシエータIQN。

Virtual Volume Host ID

仮想ボリュームをホストしていて、クラスタが認識しているESXiホストのUUID。

[Virtual Volumes]セクションには次の情報が表示されます。

Volume ID

基盤となるボリュームのID。

Virtual Volume ID

仮想ボリュームのUUID。

Name

仮想マシンの名前。

Status

VVolタスクのステータス。

vCenter Plug-inの登録解除

ご使用のインストール環境に対応する手順を使用して、NetApp Element Plug-in for vCenter Serverの登録を解除できます。プラグインの登録解除は無効にした場合と同じ効果がありますが、関連するファイルやフォルダは削除されません。

開始する前に

- プラグインの登録を解除するためのvCenter Administratorロールの権限。
- 管理ノードのIPアドレス。
- プラグインの登録を解除するvCenterのURLとクレデンシャル。

タスク概要

注: vCenter Serverでプラグインパッケージの登録を解除しても、ローカルにインストールされているプラグインパッケージ ファイルは削除されません。すべてのプラグイン ファイルを削除するには、プラグインの削除手順を参照してください。

手順

1. プラグインの登録を解除するには、インストールされているバージョンに応じた手順に従ってください。
 - バージョン3.0 以降：
 - vCenter Plug-in登録ユーティリティを使用してプラグインの登録を解除します。
 - a. 登録用TCPポートを含む管理ノードのIPアドレスをブラウザに入力します (https://[management node IP]:9443)。
 - b. **[Unregister Plug-in]**をクリックします。
 - c. 次の情報を入力します。
 - i. プラグインを登録したvCenterサービスのIPアドレスまたはFQDNサーバ名。
 - ii. vCenter Administratorのユーザ名。
 - iii. vCenter Administratorのパスワード。
 - d. **[Unregister]**をクリックします。
 - バージョン2.7～バージョン3.0（3.0を除く）：
 - ブラウザでvCenter Managed Object Browser（MOB）インターフェイスを使用して、登録を手動で解除します。
 - a. MOBのURL (https://[vcenter]/mob) を入力します。
 - b. **[Content] > [Extension Manager] > [UnregisterExtension]**の順にクリックします。
 - c. 「com.solidfire」と入力します。
 - d. **[Invoke Method]**をクリックします。

- PowerCLIを使用して登録を解除します。

```
Connect-VIServer -Server $vcenter -User  
administrator@vsphere.local  
-Password xxxxxx -Force -ErrorAction Stop -SaveCredentials  
$em = Get-View ExtensionManager  
$em.ExtensionList | ft -property Key  
$em.UnregisterExtension("com.solidfire")  
$em.UpdateViewData()  
$em.ExtensionList | ft -property Key  
Disconnect-VIServer * -Confirm:$false
```

- バージョン2.6.1以前：
 - a. ブラウザで、登録ユーティリティのURLを入力するか、プログラム ディレクトリから探します。
 - `https://<FDVA or management node IP>:8443`
 - `/opt/solidfire/vcp/bin/vcp-reg.sh`
 - b. [vCenter Plugin Register/Unregister]ウィンドウで、**[Unregister]**をクリックします。

関連タスク

[vCenter Plug-inの削除](#) (191ページ)

vCenter Plug-inの削除

vCenter Plug-in 2.5以降では、vCenter Serverからファイルを手動で削除する必要があります。

開始する前に

- 既存のプラグインの登録を解除し、vCSAまたはvCenter ServerへのSSH、RDP、またはその他の適切な接続を確立しておきます。

タスク概要

次のプロセスを実行して、プラグインに関連付けられたすべてのファイルを削除する必要があります。

手順

1. vCenter Serverを実行しているサーバに管理者としてログインし、コマンドプロンプトを開きます。
2. vCenter Serverのサービスを停止します。

- Windows :

- (Flashクライアントの場合) 次のコマンドを入力します。

```
C:\Program Files\VMware\vCenter Server\vmmon>.\vmmon-cli --stop  
vsphere-client
```

- (HTML5クライアントの場合) 次のコマンドを入力します。

```
C:\Program Files\VMware\vCenter Server\vmmon>.\vmmon-cli --stop  
vsphere-client  
C:\Program Files\VMware\vCenter Server\vmmon>.\vmmon-cli --stop  
vsphere-ui
```

- vCenter Server Appliance (vCSA) : 次のコマンドを使用します。

- (Flashクライアントの場合) 次のコマンドを入力します。

```
service-control --stop vsphere-client
```

- (HTML5クライアントの場合) 次のコマンドを入力します。

```
service-control --stop vsphere-client  
service-control --stop vsphere-ui
```

3. SolidFireのフォルダとファイルを次の場所から削除します。

- Windows: エクスプローラを使用して、C:\ProgramData\VMwareとC:\Program Files\VMwareで「SolidFire」を検索します。

注: ProgramDataフォルダは非表示になっています。このフォルダにアクセスするには、ファイルの完全パスを入力する必要があります。

- vCSA : 次のコマンドを使用します。

```
find / -name "*solidfire*" -exec rm -rf {} \;
```

4. vCenter Serverのサービスを開始します。

- Windows :

- (Flashクライアントの場合) 次のコマンドを入力します。

```
C:\Program Files\VMware\vCenter Server\vmmon>.\vmmon-cli --start  
vsphere-client
```

- (HTML5クライアントの場合) 次のコマンドを入力します。

```
C:\Program Files\VMware\vCenter Server\vmmon>.\vmmon-cli --start  
vsphere-client  
C:\Program Files\VMware\vCenter Server\vmmon>.\vmmon-cli --start  
vsphere-ui
```

- vCSA : 次のコマンドを使用します。

- (Flashクライアントの場合) 次のコマンドを入力します。

```
service control --start vsphere-client
```

- (HTML5クライアントの場合) 次のコマンドを入力します。

```
service control --start vsphere-client  
service-control --start vsphere-ui
```

関連タスク

[vCenter Plug-inの登録解除](#) (189ページ)

トラブルシューティング

NetApp Element Plug-in for vCenter Serverで発生する代表的な問題とその解決方法を理解しておく必要があります。

プラグインの登録は成功するがWeb Clientにアイコンが表示されない

説明

登録に成功したと表示されますが、プラグインのアイコンがvSphere Web Clientに表示されません。

対処方法

- vSphere Web Clientからログアウトし、再度ログインします。必要に応じて、ブラウザを閉じて開き直します。
- ブラウザ キャッシュをクリアします。
- vCenterで、Windows管理ツールの[サービス]メニューからvSphere Web Clientサービスを再起動するか、vCenterをリブートします。
- 必要なデフォルトの管理者権限がすべてvCenter Administratorロールに関連付けられていることを確認します。
- プラグインのZIPファイルがvCenterにダウンロードされていることを確認します。

1. vCenterでvsphere_client_virgo.logを開きます。vCenterバージョン6.5および6.7のログ ファイルは次の場所にあります。

- Flashクライアントの場合：/var/log/vmware/vsphere-client/logs/vsphere_client_virgo.log
- HTML5クライアントの場合：/var/log/vmware/vsphere-ui/logs/vsphere_client_virgo.log

2. ZIPのダウンロードに失敗したというエラー メッセージが表示された場合は、ZIPをもう一度ダウンロードします。

注：URLがアクセス不能または無効な場合は修正する必要があります。修正したURLでプラグインの登録を更新するか、プラグインの登録を解除して登録し直してください。allowHTTP設定を変えずにHTTP URLを指定した場合も、ZIPのダウンロードが失敗することがあります。

- ネットワーク ポートを確認します。vCenterから管理ノードに必要なポート経由で双方向にアクセスできることを確認します。
- vCenterのMOB拡張レコード (<https://<vcenterIP>/mob/?moid=ExtensionManager&doPath=extensionList%5b%22com%2esolidfire%22%5d%2eserver>) でプラグインのZIPのダウンロードURLを確認します。

1. このURLをブラウザに貼り付けます。
2. プラグインのZIPをダウンロードできるかどうかを確認します。

- 。 プラグインのZIPをダウンロードできる場合は、次の手順に進みます。
 - 。 プラグインのZIPをダウンロードできない場合は、vCenter Serverと管理ノード間のネットワークに問題がないか確認してください。
3. プラグインをダウンロードできない場合は、MOBレコード内のserverThumbprintを、ブラウザに表示されているZIP URLの証明書SHA-1と比較します。
 - a. MOBの登録レコードに含まれているURLまたはSHA-1が正しくない場合や古い場合は、プラグインの登録を解除して再登録します。
 - b. 問題が解決せず、ZIPに到達できない場合は、ZIP URLを調べて、使用されている管理ノード アドレスに問題がないか確認します。場合によっては、ZIPファイルをダウンロードできるように、プラグインの登録ユーティリティを使用してURLをカスタマイズする必要があります。

関連タスク

[社内（ダーク サイト）のHTTPサーバ用のvCenterプロパティの変更](#)（26ページ）

関連資料

[ネットワーク ポート要件](#)（10ページ）

登録画面からプラグインを登録中にエラーが発生する

説明

登録ユーティリティを使用してプラグインをvCenter Serverに登録する際にエラーが発生します。キーがcom.solidfireのプラグインがすでにインストールされています。

対処方法

登録ユーティリティで、[Register Plug-in]ではなく[Update Plug-in]を使用します。

登録画面からプラグインを更新中にエラーが発生する

説明

登録ユーティリティを使用してプラグインをvCenter Serverに対して更新する際にエラーが発生します。更新対象となるキーがcom.solidfireのプラグインがインストールされていません。

対処方法

登録ユーティリティで、[Update Plug-in]ではなく[Register Plug-in]を使用します。

登録画面でキーストア エラーが発生する

説明

登録ユーティリティを使用する際に、/opt/solidfire/registration/keystore および/var/cache/jetty/tmp/.etc/keystoreにキーストアが見つからないというエラーが発生します。

対処方法

1. 管理ノードをリブートするか、次のコマンドを実行します。

```
sudo /opt/solidfire/vcp-reg.bash -F
```

2. 登録ユーティリティのWeb UI表示を更新します。

ネットアップの拡張機能をアップグレードできないというエラー メッセージが表示される

メッセージ

```
org.springframework.transaction.CannotCreateTransactionException:
Could not open JPA EntityManager for transaction; nested exception
is javax.persistence.PersistenceException:
org.hibernate.exception.GenericJDBCException: Could not open
connection.
```

説明

Windows vCenter Serverをバージョン6.0から6.5にアップグレードしているときに、ネットアップの拡張機能をアップグレードできない、または新しいvCenter Serverでは動作しない可能性があるという警告が表示されます。アップグレードの完了後にvSphere Web Clientにログインし、vCenter Plug-inの拡張ポイントを選択すると、エラーが発生します。このエラーは、ランタイム データベースを格納するディレクトリがバージョン6.0から6.5に変更されたために発生します。vCenter Plug-inが実行時に必要なファイルを作成できません。

対処方法

1. プラグインの登録を解除します。
2. プラグインのファイルを削除します。
3. vCenterをリブートします。
4. プラグインを登録します。
5. vSphere Web Clientにログインします。

関連タスク

[vCenter Plug-inの登録解除](#) (189ページ)

[vCenter Plug-inの削除](#) (191ページ)

[vCenterへのvCenter Plug-inの登録](#) (23ページ)

プラグインの削除は完了するがアイコンが残る

説明

vCenter Plug-inパッケージ ファイルを削除したあとも、vSphere Web Clientにプラグインのアイコンが表示されます。

対処方法

vSphere Web Clientからログアウトし、再度ログインします。必要に応じて、ブラウザを閉じて開き直します。vSphere Web Clientからログアウトしても問題が解決しない場合は、必要に応じてvCenter Server Webサービスをリブートします。

管理者パスワードの変更後にプラグインを登録解除または削除できない

説明

プラグインの登録時に使用したvCenterの管理者パスワードを変更すると、vCenter Plug-inの登録解除や削除ができなくなります。

対処方法

バージョン2.6では、vCenter Plug-inの[Register/Unregister]ページに移動します。
[Update]ボタンをクリックして、vCenterのIPアドレス、ユーザID、およびパスワードを変更します。

バージョン2.7以降では、プラグインの[mNode Settings]でvCenter Administratorのパスワードを更新します。

プラグインの管理タスクが失敗するか、またはESXiホストからボリュームにアクセスできない

説明

データストアの作成、クローニング、共有のタスクが失敗する、あるいはESXiホストからボリュームにアクセスできません。

対処方法

- データストア処理用のESXiホストにソフトウェアiSCSI HBAがあって有効になっていることを確認します。
- ボリュームが削除されていないか、または間違ったボリューム アクセス グループに割り当てられていないかを確認します。
- ボリューム アクセス グループのホストIQNが正しいことを確認します。
- 関連付けられているアカウントのCHAP設定が正しいことを確認します。
- ボリューム ステータスがactiveであること、ボリューム アクセスが readWriteであること、および512eがtrueに設定されていることを確認します。

Firefox 59.0.2ブラウザでvCenter Plug-inを使用するとエラーが発生する

メッセージ

```
Name:HttpResponse Raw Message:Http failure response for
https://vc6/ui/solidfire-war-4.2.0-SNAPSHOT/rest/vsphere//servers:
500 Internal Server Error Return Message:Server error. Please try
again or contact NetApp support
```

説明

この問題は、Firefoxを使用するvSphere HTML5 Webクライアントで発生します。
vSphere Flashクライアントに影響はありません。

対処方法

ブラウザのURLにFQDNを使用します。

データストアの削除処理が失敗する

説明

データストアの削除処理が失敗します。

対処方法

データストアからすべてのVMが削除されていることを確認します。データストアを削除する前に、データストアからVMを削除する必要があります。

ペアリング キーを使用してクラスタ ペアを接続できない

説明

ペアリング キーを使用してクラスタをペアリング中に接続エラーが発生します。
[Create Cluster Pairing]ダイアログ ボックスには、ホストへのルートがないことを示すエラー メッセージが表示されます。

対処方法

ローカル クラスタに作成された未設定のクラスタ ペアを手動で削除し、もう一度クラスタ ペアリングを実行します。

QoSSIOCステータスに関するエラー メッセージ

説明

プラグインのQoSSIOCステータスに警告アイコンとエラー メッセージが表示されます。

対処方法

- Unable to reach IP address
IPアドレスが無効であるか、応答がありません。アドレスが正しいこと、および管理ノードがオンラインで使用可能な状態になっていることを確認します。
- Unable to communicate
IPアドレスに到達できていますが、アドレスの呼び出しに失敗しています。指定されたアドレスでQoSSIOCサービスが実行されていないか、ファイアウォールでトラフィックがブロックされている可能性があります。
- Unable to connect to the SIOC service
管理ノードの/var/log（古い管理ノードの場合は/var/log/solidfire/）にあるsioc.logを開き、SIOCサービスが起動していることを確認します。SIOCサービスの起動には50秒以上かかることがあります。サービスが起動しなかった場合は、もう一度実行します。SIOCサービスの現在のステータスを確認するには、管理ノードの/var/log/にあるsiocStatus.logを開きます。

関連タスク

[QoSSIOCの管理ノードの設定](#)（63ページ）

関連資料

[ネットワークポート要件](#)（10ページ）

QoSSIOCサービスが使用可能と表示されるが使用できない

説明

QoSSIOCサービスの設定には「UP」と表示されていますが、QoSSIOCを使用できません。

対処方法

NetApp Element Configuration拡張ポイントの[mNode Settings]タブで、QoSSIOCサービスの更新ボタンをクリックします。必要に応じて、IPアドレスまたはユーザ認証情報を更新します。

データストアでQoSSIOCが有効になっているが使用できない

説明

データストアでQoSSIOCが有効になっていますが、使用できません。

対処方法

データストアでVMware SIOCが有効になっていることを確認します。

1. 管理ノードの/var/logにあるsioc.logを開きます。
2. 次のテキストを検索します。

SIOC is not enabled

3. vSphere Web ClientまたはCLIを使用して、データストアでSIOCを有効にします。

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方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ドキュメントセンター](#)
- [NetApp HCIのリソース ページ](#)
- [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 © 2019 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いかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

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

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

ここに記載されている「データ」は商用品目（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。