概念
NetApp HCI

NetApp
November 18, 2025

目次

概念 1
NetApp HCI 製品の概要 1
NetApp HCI のコンポーネント 1
NetApp HCI の URL 2
ユーザアカウント 2
ユーザアカウント管理 3
ストレージクラスタ管理者アカウント 3
権限のあるユーザアカウント 3
ボリュームアカウント 4
詳細については、こちらをご覧ください 4
データ保護 4
リモートレプリケーションの種類 5
データ保護用のボリューム Snapshot 6
ボリュームクローン 7
SolidFire ストレージのバックアップとリストアのプロセスの概要 7
保護ドメイン 7
Double Helix の高可用性 8
詳細については、こちらをご覧ください 8
クラスタ 8
信頼できるストレージクラスタです 8
有効利用されない容量 9
2 ノードストレージクラスタ 9
3 つ以上のノードを含むストレージクラスタ 10
詳細については、こちらをご覧ください 10
ノード 10
管理ノード 11
ストレージノード 11
コンピューティングノード 11
監視ノード 11
詳細については、こちらをご覧ください 12
ストレージ 12
メンテナンスモード 12
個のボリューム 13
ボリュームアクセスグループ 14
イニシエータ 15
カスタムの保護ドメイン 15
NetApp HCI ライセンス 16
NetApp HCI と VMware vSphere のライセンス 16
NetApp HCI と ONTAP Select のライセンス 16

詳細については、こちらをご覧ください 16
NetApp Hybrid Cloud Control の最大構成数 17
NetApp HCI セキュリティ 17
ストレージノードの保存データの暗号化 17
保存データのソフトウェア暗号化 18
外部キー管理 18
多要素認証 18
HTTPS 向けの FIPS 140-2 と保存データ暗号化 18
パフォーマンスと QoS 19
QoS パラメータ 19
QoS 値の制限 20
QoS パフォーマンス 20
QoS ポリシー 21

概念

NetApp HCI 製品の概要

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

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

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

NetApp HCI のコンポーネント

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

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

  の詳細を確認してください "管理サービスのリリース"。

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

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

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

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

NetApp HCI の URL

NetApp HCI で使用する一般的な URL を次に示します。

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

詳細については、こちらをご覧ください

- "vCenter Server 向け NetApp Element プラグイン"
- "NetApp HCI のリソースページ"

ユーザアカウント

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

ユーザアカウント管理

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

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

その他の考慮事項をいくつか示します。

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

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

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

ストレージクラスタ管理者アカウント

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

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

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

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

権限のあるユーザアカウント

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

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

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

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

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

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

ボリュームアカウント

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

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

詳細については、こちらをご覧ください

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

データ保護

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

NetApp HCI データ保護の概念は次のとおりです。

- [リモートレプリケーションの種類]
- データ保護用のボリューム Snapshot
- [ボリュームクローン]
- SolidFire ストレージのバックアップとリストアのプロセスの概要

- [保護ドメイン]
- Double Helix の高可用性

リモートレプリケーションの種類

データのリモートレプリケーションには、次の形式を使用できます。

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

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

クラスタ間の同期レプリケーションと非同期レプリケーション

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

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

同期レプリケーション

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

同期レプリケーションは、次のような状況に適しています。

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

非同期レプリケーション

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

非同期レプリケーションは、次のような状況に適しています。

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

Snapshot のみのレプリケーション

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

Snapshot レプリケーションの頻度を設定できます。

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

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

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

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

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

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

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

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

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

データ保護用のボリューム **Snapshot**

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

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

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

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

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

ボリュームクローン

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

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

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

SolidFire ストレージのバックアップとリストアのプロセスの概要

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

ボリュームは次の場所にバックアップできます。

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

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

保護ドメイン

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

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

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

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

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

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

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

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

Double Helix の高可用性

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

詳細については、こちらをご覧ください

"vCenter Server 向け NetApp Element プラグイン"

クラスタ

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

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

信頼できるストレージクラスタです

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

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

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

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

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

有効利用されない容量

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

2 ノードストレージクラスタ

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

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

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

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

  の詳細を確認してください "監視ノード："

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

ストレージクラスタのクォーラム

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

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

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

2 ノードストレージクラスタでの自動修復と障害処理

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

3 つ以上のノードを含むストレージクラスタ

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

詳細については、こちらをご覧ください

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

ノード

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

グループ化されたハードウェアリソースまたは仮想リソースです。

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

管理ノード

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

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

ストレージノード

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

コンピューティングノード

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

監視ノード

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

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

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

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

詳細については、こちらをご覧ください

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

ストレージ

メンテナンスモード

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

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

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

- ノードでホストされているすべてのボリュームがフェイルオーバーされました
- ノードはのプライマリではなくなりました 任意のボリューム

- 一時スタンバイノードは、対象のすべてのボリュームに割り当てられます フェイルオーバーしました

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

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

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

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

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

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

詳細については、こちらをご覧ください

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

個のボリューム

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

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

永続ボリューム

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

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

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

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

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

詳細については、こちらをご覧ください

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

ボリュームアクセスグループ

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

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

ボリュームアクセスグループには次の制限があります。

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

詳細については、こちらをご覧ください

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

イニシエータ

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

詳細については、こちらをご覧ください

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

カスタムの保護ドメイン

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

カスタムの保護ドメインが割り当てられていない場合：

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

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

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

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

- GetProtectionDomainLayout - 各ノードのシャーシとカスタム保護ドメインを表示します。
- SetProtectionDomainLayout - 各ノードにカスタム保護ドメインを割り当てることができます。

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

詳細については、こちらをご覧ください

"Element API を使用してストレージを管理します"

NetApp HCI ライセンス

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

NetApp HCI と VMware vSphere のライセンス

VMware vSphere のライセンスは、構成によって異なります。

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

NetApp HCI と ONTAP Select のライセンス

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

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

詳細については、こちらをご覧ください

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

NetApp Hybrid Cloud Control の最大構成数

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

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

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

設定の最大数

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

NetApp HCI セキュリティ

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

ストレージノードの保存データの暗号化

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

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

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

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

保存データのソフトウェア暗号化

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

外部キー管理

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

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

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

多要素認証

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

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

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

HTTPS 向けの FIPS 140-2 と保存データ暗号化

NetApp SolidFire ストレージクラスタおよび NetApp HCI システムでは、暗号モジュールに関する Federal Information Processing Standard （ FIPS ；連邦情報処理標準） 140-2 の要件に準拠した暗号化がサポートされています。SolidFire または NetApp HCI クラスタで、 HTTPS 通信とドライブ暗号化の両方に対して FIPS 140-2 準拠を有効にすることができます。

クラスタで FIPS 140-2 動作モードを有効にすると、クラスタは NetApp Cryptographic Security Module （ NCSM ）をアクティブ化し、 NetApp Element UI および API との HTTPS を介したすべての通信に FIPS 140-2 レベル 1 認定の暗号化を利用します。FIPS 140-2 HTTPS 暗号化をイネーブルにするには 'EnableFeature`

Element API を 'fips' パラメータとともに使用しますFIPS 対応ハードウェアを搭載したストレージクラスタでは、「 EnableFeature` Element API 」パラメータを「 FipsDrives 」パラメータとともに使用して、保存データの FIPS ドライブ暗号化を有効にすることもできます。

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

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

パフォーマンスと QoS

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

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

QoS パラメータ

IOPS パラメータは、次のように定義します。

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

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

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

  Burst IOPS には 2 つの制限があります。

  - ボリュームは、蓄積したバーストクレジット数と同じ秒数だけ Max IOPS を超過できます。
  - ボリュームが Max IOPS の設定を超えた場合は、 Burst IOPS の設定によって制限されます。つまり、バースト時の IOPS がボリュームの Burst IOPS の設定を超えることはありません。
- * Effective Max Bandwidth * - 最大帯域幅は、（ QoS 曲線に基づく） IOPS に IO サイズを掛けて計算されます。

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

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

QoS 値の制限

QoS の最小値と最大値を次に示します。

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

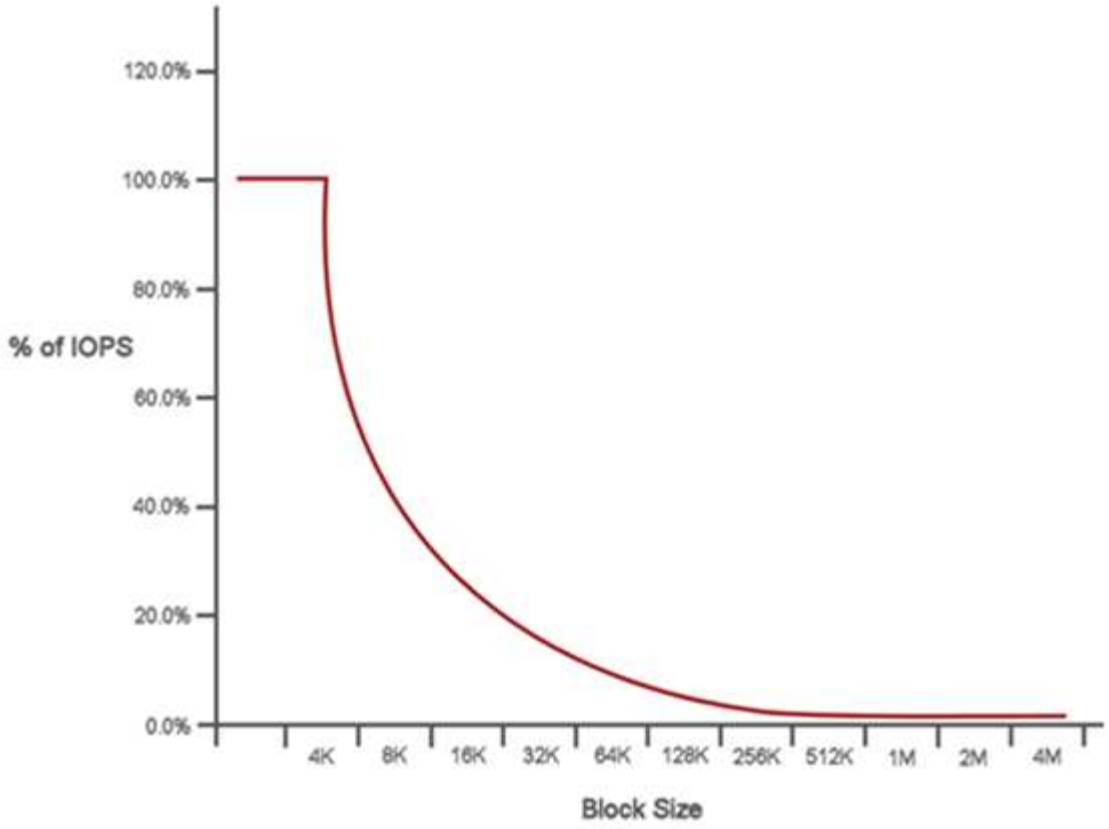
- これらは概算値です。** 最大 IOPS とバースト IOPS は最大 200 、 000 に設定できます。ただし、この設定は、ボリュームのパフォーマンスの制限を意図的に解放する場合にのみ使用できます。実際のボリュームの最大パフォーマンスは、クラスタの使用率とノードごとのパフォーマンスによって制限されます。

QoS パフォーマンス

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

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

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



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

QoS ポリシー

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

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

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

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

詳細については、こちらをご覧ください

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

- "NetApp HCI のリソースページ"

著作権に関する情報

商標に関する情報