概念
Element Software

NetApp
January 15, 2024

目次

概念

Element ソフトウェアに関連する基本的な概念を確認できます。

- "製品の概要"
- SolidFire アーキテクチャの概要
- ノード
- クラスタ
- "セキュリティ"
- アカウントと権限
- "個のボリューム"
- データ保護
- パフォーマンスと QoS

詳細については、こちらをご覧ください

- "SolidFire オールフラッシュストレージの概要"
- "SolidFire および Element ソフトウェアのドキュメント"

製品の概要

SolidFire オールフラッシュストレージシステムは、独立したハードウェアコンポーネント（ドライブとノード）で構成され、これらのコンポーネントが 1 つのストレージリソースプールに統合されます。このユニファイドクラスタは、単一のストレージシステムとして外部クライアントに提供され、 NetApp Element ソフトウェアで管理されます。

Element インターフェイス、 API 、またはその他の管理ツールを使用して、 SolidFire クラスタのストレージ容量とパフォーマンスを監視し、マルチテナントインフラ全体のストレージアクティビティを管理できます。

SolidFire の機能

SolidFire システムには次の機能があります。

- 大規模なプライベートクラウドインフラに対応するハイパフォーマンスストレージを提供します
- 柔軟な拡張が可能で、変化するストレージニーズに対応できます
- API ベースのストレージ管理 Element ソフトウェアインターフェイスを使用します
- Quality of Service ポリシーを使用してパフォーマンスを保証します
- クラスタ内のすべてのノードにわたる自動ロードバランシングが含まれます
- ノードの追加や差分を実行すると、クラスタのリバランシングが自動的に実行されます

SolidFire の導入

ネットアップが提供し、NetApp Element ソフトウェアと統合されたストレージノードを使用できます。

"SolidFire オールフラッシュストレージアーキテクチャの概要"

詳細については、こちらをご覧ください

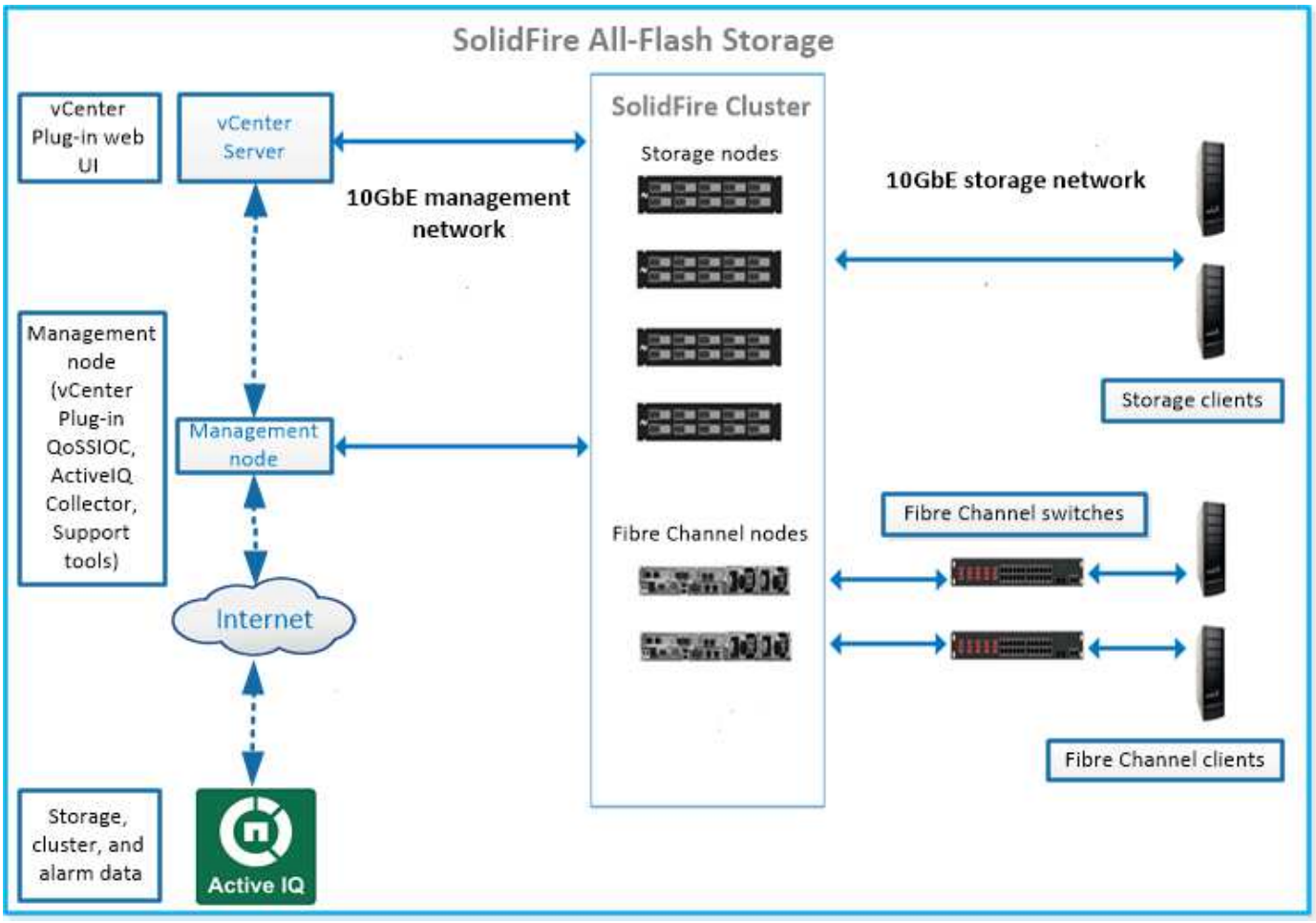
- "SolidFire オールフラッシュストレージの概要"
- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

SolidFire アーキテクチャの概要

SolidFire オールフラッシュストレージシステムは、独立したハードウェアコンポーネント（ドライブとノード）で構成されます。これらのコンポーネントはストレージリソースのプールに統合され、各ノードでそれぞれ独立して実行される NetApp Element ソフトウェアを備えています。この単一のストレージシステムは、 Element ソフトウェアの UI 、 API 、およびその他の管理ツールを使用して単一のエンティティとして管理されます。

SolidFire ストレージ・システムは、次のハードウェア・コンポーネントで構成されています。

- * クラスタ * ：ノードを集合化した SolidFire ストレージシステムのハブ。
- * Nodes * ：クラスタにグループ化されたハードウェアコンポーネント。ノードには次の 2 つのタイプがあります。
  - ストレージノード：複数のドライブを搭載したサーバです
  - Fibre Channel （ FC ）ノード。 FC クライアントに接続するために使用します
- * Drives * ：クラスタのデータを格納するストレージノードで使用します。ストレージノードには、次の 2 種類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：クラスタ内のボリュームやその他オブジェクトの定義情報を格納します。
  - ブロックドライブ：ボリュームのデータブロックを格納します。



Element Web UI やその他の互換性のあるツールを使用して、システムの管理、監視、更新を行うことができます。

- "SolidFire ソフトウェアインターフェイス"
- "SolidFire Active IQ の略"
- "Element ソフトウェアの管理ノード"
- "管理サービス"

共通 URL

SolidFire オールフラッシュストレージシステムで使用される一般的な URL を次に示します。

URL	説明
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。
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://[management ノード IP アドレス	NetApp Hybrid Cloud Control にアクセスして、ストレージのインストールサービスと更新管理サービスをアップグレードします。

URL	説明
「 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 」 /mnode 」を参照してください	管理サービス REST API および管理ノードのその他の機能を使用します。"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。"詳細はこちら。"

詳細については、こちらをご覧ください

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

SolidFire ソフトウェアインターフェイス

SolidFire ストレージシステムは、 NetApp Element の各種ソフトウェアインターフェイスや統合ユーティリティを使用して管理できます。

オプション（ **Options** ）

- NetApp Element ソフトウェアのユーザインターフェイス
- NetApp Element ソフトウェア API
- vCenter Server 向け NetApp Element プラグイン
- NetApp Hybrid Cloud Control の略
- 管理ノード UI
- [その他の統合ユーティリティおよびツール]

NetApp Element ソフトウェアのユーザインターフェイス

Element ストレージをセットアップし、クラスタの容量とパフォーマンスを監視できるほか、マルチテナントインフラ全体のストレージアクティビティを管理できます。Element は、 SolidFire クラスタの中核をなすストレージオペレーティングシステムです。Element ソフトウェアはクラスタ内のすべてのノードで独立して動作します。 Element では、クラスタのノードが、単一のストレージシステムとして提供されるリソースを外部クライアントに結合することができます。Element ソフトウェアは、システム全体のすべてのクラスタの調整、拡張、管理を担います。ソフトウェアのインターフェイスは Element API を基盤としています。

"Element ソフトウェアでストレージを管理"

NetApp Element ソフトウェア API

一連のオブジェクト、メソッド、ルーチンを使用して Element ストレージを管理できます。Element API は、HTTPS 経由の JSON-RPC プロトコルに基づいています。Element UI で API 処理を監視するには、 API ログを有効にします。これにより、システムに対して実行されているメソッドを確認できます。要求と応答の両方を有効にすると、実行したメソッドに対するシステムの応答を確認できます。

"Element API を使用してストレージを管理します"

vCenter Server 向け NetApp Element プラグイン

VMware vSphere で Element UI の代わりのインターフェイスを使用して、 Element ソフトウェアを実行するストレージクラスタを設定および管理できます。

"vCenter Server 向け NetApp Element プラグイン"

NetApp Hybrid Cloud Control の略

NetApp Hybrid Cloud Control インターフェイスを使用して、 Element ストレージサービスと管理サービスをアップグレードし、ストレージアセットを管理できます。

"NetApp Hybrid Cloud Control の概要を使用してストレージを管理および監視します"

管理ノード UI

管理ノードには 2 つの UI が装備されています。 REST ベースのサービスを管理するための UI と、ネットワーク / クラスタ設定の管理とオペレーティングシステムのテスト / ユーティリティを実行するためのノード UI です。REST API UI からは、サービスベースのシステム機能を管理ノードから制御するサービス関連 API のメニューにアクセスできます。

その他の統合ユーティリティおよびツール

通常は NetApp Element 、 NetApp Element API 、および NetApp Element Plug-in for vCenter Server を使用してストレージを管理しますが、追加の統合ユーティリティやツールを使用してストレージにアクセスできます。

Element の CLI

"Element の CLI" Element API を使用せずにコマンドラインインターフェイスを使用して SolidFire ストレージシステムを制御できます。

Element PowerShell ツール

"Element PowerShell ツール" SolidFire ストレージシステムの管理に Element API を使用する一連の Microsoft Windows PowerShell 機能を使用できるようにします。

Element SDK

"Element SDK" 次のツールを使用して SolidFire クラスタを管理できます。

- Element Java SDK ： Element API と Java プログラミング言語を統合できます。
- Element .NET SDK ： Element API を .NET プログラミングプラットフォームに統合できます。
- Element Python SDK ： Element API と Python プログラミング言語を統合できます。

SolidFire Postman API テストスイート

プログラマがのコレクションを使用できるようにします "ポストマン" Element API 呼び出しをテストする関数。

SolidFire ストレージレプリケーションアダプタ

"SolidFire ストレージレプリケーションアダプタ" VMware Site Recovery Manager （ SRM ）と統合して、レプリケートされた SolidFire ストレージクラスタとの通信を可能にし、サポートされているワークフローを実行します。

SolidFire vRO

"SolidFire vRO" VMware vRealize Orchestrator を使用すると、 Element API を使用して SolidFire ストレージシステムを簡単に管理できます。

SolidFire VSS プロバイダ

"SolidFire VSS プロバイダ" VSS シャドウコピーを Element の Snapshot およびクローンと統合します。

詳細については、こちらをご覧ください

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

SolidFire Active IQ の略

"SolidFire Active IQ の略" は、クラスタ全体のデータの履歴ビューを提供する Web ベースのツールです。ビューは定期的に更新されます。特定のイベント、しきい値、または指標にアラートを設定できます。SolidFire Active IQ を使用すると、システムのパフォーマンスと容量を監視し、クラスタの健常性を常に把握できます。

システムに関する次の情報は、 SolidFire Active IQ で確認できます。

- ノードの数とステータス：健全、オフライン、またはエラー
- CPU、メモリ使用量、ノードスロットルをグラフィカルに表示します
- シリアル番号、シャーシ内のスロットの場所、モデル、ストレージ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など、ノードに関する詳細
- 仮想マシンの CPU およびストレージ関連情報

SolidFire Active IQ の詳細については、を参照してください "SolidFire Active IQ のドキュメント"。

を参照してください。

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"
- "ネットアップサポートサイトと Active IQ 用ツール"

Element ソフトウェアの管理ノード

。 "管理ノード（ mNode ）" は、 Element ソフトウェアベースの 1 つ以上のストレージクラスタと同時に実行される仮想マシンです。このサービスは、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。

管理ノード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。

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" サービスバンドルとして頻繁に更新されます。

SolidFire オールフラッシュストレージの管理サービス

Element 11.3 リリース以降、 * 管理サービス * がでホストされます "管理ノード"を使用すると、メジャーリリース以外のソフトウェアサービスを迅速に更新できます。

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

の詳細を確認してください "管理サービスのリリース"。

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 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を定義します。ノードロールのタイプは次のとおりです。

- [管理ノード]
- [ストレージノード]
- Fibre Channel ノード

ノードの状態 クラスタの関連付けによって異なります。

管理ノード

管理ノードは、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る仮想マシンです。監視と計測のほか、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のためのネットアップサポートアクセスの有効化などを行います。"詳細はこちら。"

ストレージノード

SolidFire 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。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。

ストレージノードには次のような特徴があります。

- 各ノードには一意の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。
- 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。

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、新規または既存の任意の 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。

ノードの処理の状態

設定のレベルによって、ノードは次のいずれかの状態になります。

- * 利用可能 *

  ノードにはクラスタ名が関連付けられておらず、まだクラスタに含まれていません。

- * 保留中 *

  ノードが設定され、指定したクラスタに追加できるようになります。

  このノードにアクセスするための認証は必要ありません。

- * 保留中アクティブ *

  互換性のある Element ソフトウェアをノードにインストールしています。完了すると、ノードは Active 状態に移行します。

- * アクティブ *

  クラスタに参加しているノード。

  このノードを変更するには、認証が必要です。

上記の各状態では、一部のフィールドは読み取り専用です。

詳細については、こちらをご覧ください

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

クラスタ

クラスタは、 SolidFire ストレージシステムの中心であり、複数のノードで構成されます。SolidFire のストレージ効率化を実現するには、クラスタに少なくとも 4 つのノードが必要です。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、ブロックストレージとしてアクセスできます。

新しいクラスタを作成すると、 1 つのノードがそのクラスタの通信の所有者として初期化され、クラスタ内の各ノードに対してネットワーク通信が確立されます。このプロセスは、新しいクラスタごとに 1 回だけ実行します。Element UI または API を使用してクラスタを作成できます。

クラスタをスケールアウトするには、ノードを追加します。新しいノードを追加するときにサービスが中断されることはなく、追加したノードのパフォーマンスと容量がクラスタで自動的に使用されます。

管理者とホストは、仮想 IP アドレスを使用してクラスタにアクセスできます。クラスタ内のいずれのノードも仮想 IP アドレスをホストできます。管理仮想 IP （ MVIP ）は 1GbE 接続でのクラスタ管理を提供し、ストレージ仮想 IP （ SVIP ）はホストからストレージへの 10GbE 接続でのアクセスを提供します。これらの仮想 IP アドレスは、 SolidFire クラスタのサイズや構成に関係なく、一貫した接続を可能にします。仮想 IP アドレスをホストするノードで障害が発生した場合、クラスタ内の別のノードが仮想 IP アドレスを引き継ぎます。

> Element バージョン 11.0 以降では、ノードの管理ネットワークに IPv4 、 IPv6 、または両方のアドレスを設定できます。この環境は、ストレージノードと管理ノードの両方に対応します。ただし、 IPv6 をサポートしない管理ノード 11.3 以降がこれに該当します。クラスタの作成時には、 IPv4 または IPv6 のどちらかのアドレスを 1 つだけ MVIP に使用でき、これと同じアドレスタイプをすべてのノードで設定する必要があります。

クラスタに関する詳細情報

- [信頼できるストレージクラスタです]
- 3 分の 1 のルール
- [有効利用されない容量]
- [ストレージ効率]
- [ストレージクラスタのクォーラム]

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。からユーザを管理できます "Element ソフトウェアユーザインターフェイス"。

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。

3 分の 1 のルール

NetApp SolidFire ストレージクラスタ内でタイプの異なるストレージノードを混在させる場合、 1 つのストレージノードに格納できるストレージクラスタの総容量の 33% を超えることはできません。

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。

ストレージ効率

NetApp SolidFire ストレージクラスタでは、重複排除、圧縮、およびシンプロビジョニングを使用して、ボリュームの格納に必要な物理ストレージ容量を削減します。

- * 圧縮 *

  圧縮は、データブロックを圧縮グループに集約し、各データブロックを 1 つのブロックとして格納することで、ボリュームに必要な物理ストレージの量を削減する機能です。

- * 重複排除 *

  重複排除では、重複するデータブロックを破棄することでボリュームに必要な物理ストレージの量が削減されます。

- * シンプロビジョニング *

  シンプロビジョニングされたボリュームまたは LUN では、ストレージが事前に予約されません。代わりに、ストレージは必要に応じて動的に割り当てられます。ボリュームまたは LUN 内のデータが削除されると、空きスペースはストレージシステムに戻されます

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。

セキュリティ

SolidFire オールフラッシュストレージシステムを使用すると、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。

保存データの暗号化（ハードウェア）

ストレージノード内のドライブはいずれも、ドライブレベルの暗号化機能で AES 256 ビット暗号化を利用できます。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、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。ドライブの電源がオフになっているかドライブがロックされている場合以外は、パスワードは必要ありません。

"保存データのハードウェア暗号化機能の有効化" クラスタのパフォーマンスや効率には影響しません。Element API または Element UI を使用してクラスタの設定から暗号化が有効なドライブまたはノードを削除すると、保存データの暗号化がドライブで無効になります。ドライブを削除した後、「 ecureEraseDrives 」 API メソッドを使用してドライブを安全に消去できます。物理ドライブまたはノードが強制的に削除された場合でも、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（ソフトウェア）

保存データを暗号化するソフトウェア暗号化機能のもう 1 つのタイプを使用すると、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。 "有効になっている場合"ソフトウェアで自動的に読み取られたすべてのデータを暗号化し、復号化します。保存データのソフトウェア暗号化は、 SED （自己暗号化ドライブ）のハードウェアへの実装を反映して、 SED がない場合にデータセキュリティを提供します。

SolidFire オールフラッシュストレージクラスタの場合、クラスタ作成時に保存データのソフトウェア暗号化を有効にし、クラスタ作成後に無効にすることはできません。

ソフトウェアベースとハードウェアベースの保存データの暗号化機能は、どちらも単独で使用することも、相互に組み合わせて使用することもできます。

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 "外部キー管理の概要" ドキュメント

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" ドキュメント

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 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します"。

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"。

を参照してください。

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

アカウントと権限

システム上のストレージリソースを管理してアクセスできるようにするには、システムリソースのアカウントを設定する必要があります。

Element ストレージでは、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
- ストレージボリュームアクセス用のユーザアカウント
- NetApp Hybrid Cloud Control に対して権限のあるクラスタユーザアカウントが必要です

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。

可能です "クラスタ管理者アカウントを管理" 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 の設定を行います。

ユーザアカウント

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。

権限のあるクラスタユーザアカウントです

権限のあるクラスタ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。

ストレージ

個のボリューム

NetApp Element ストレージシステムは、ボリュームを使用してストレージをプロビジョニングします。ボリュームは、 iSCSI または Fibre Channel クライアントがネットワーク経由でアクセスするブロックデバイスです。

Element ストレージでは、 ユーザアカウントのボリュームをバックアップまたはリストアする。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。

永続ボリュームを有効にするオプションは、のインストールスクリプトおよびアップグレードスクリプトに含まれています "新しい管理ノードの導入"。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、で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

仮想ボリューム（ **VVOL** ）

vSphere Virtual Volumes は、 VMware が提供するストレージパラダイムであり、 vSphere のストレージ管理の多くをストレージシステムから VMware vCenter に移行します。Virtual Volumes （ VVOL ）では、個々の仮想マシンの要件に応じてストレージを割り当てることができます。

バインド

NetApp Element クラスタは、最適なプロトコルエンドポイントを選択し、 ESXi ホストと仮想ボリュームをプロトコルエンドポイントに関連付けるバインドを作成し、 ESXi ホストにバインドを返します。バインドが完了すると、 ESXi ホストはバインドされた仮想ボリュームを使用して I/O 処理を実行できます。

プロトコルエンドポイント

VMware ESXi ホストは、プロトコルエンドポイントと呼ばれる論理 I/O プロキシを使用して、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ペアリング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。

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。このプールには、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様に機能し、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。クラスタあたり最大 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。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。

VASA Provider

vSphere で NetApp Element クラスタの VVol 機能を認識するには、 vSphere 管理者が NetApp Element VASA Provider を vCenter に登録する必要があります。VASA Provider は、 vSphere と Element クラスタ間のアウトオブバンド管理パスです。VM の作成、 vSphere での VM の利用可能化、 vSphere へのストレージ機能のアドバタイズなど、 vSphere に代わって Element クラスタで要求を実行します。

VASA Provider は、 Element ソフトウェアのクラスタマスターの一部として実行されます。クラスタマスターは可用性の高いサービスで、必要に応じてクラスタ内の任意のノードにフェイルオーバーします。クラスタマスターがフェイルオーバーすると、 VASA Provider も一緒に移動するため、 VASA Provider の高可用性が確保されます。プロビジョニングタスクとストレージ管理タスクはいずれも VASA Provider を使用します。 VASA Provider は、 Element クラスタで必要な変更を処理します。

> 1 つの vCenter インスタンスに複数の NetApp Element VASA Provider を登録しないでください。2 つ目の NetApp Element VASA Provider が追加されている場合、その結果、すべての VVOL データストアにアクセスできなくなります。

> VASA Provider を vCenter に登録済みの場合、アップグレードパッチとして最大 10 個の vCenter がサポートされます。をインストールするには、 VASA39 マニフェストの指示に従い、から .tar.gz ファイルをダウンロードします "ネットアップのソフトウェアダウンロード" サイトNetApp Element VASA プロバイダはネットアップの証明書を使用します。このパッチでは、 vCenter が証明書を変更せずに使用して、 VASA および VVOL に使用する複数の vCenter をサポートします。証明書は変更しないでください。カスタム SSL 証明書は VASA でサポートされません。

詳細については、こちらをご覧ください

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

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。

NetApp SolidFire ストレージのボリュームアクセスグループを使用すると、 iSCSI イニシエータの IQN または Fibre Channel の WWPN でボリュームの集合にアクセスできます。アクセスグループに追加した各 IQN は、 CHAP 認証を使用せずに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。

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。
- Fibre Channel クラスタの場合は、 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。

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。

データ保護

データ保護機能には、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などがあります。

Element ストレージ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]
- Element 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]
- カスタムの保護ドメイン
- 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

詳細については、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ディザスタリカバリを支える 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）

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。

NetApp Element ソフトウェア 10.1 以降では、 ONTAP システムの SnapMirror 機能による Snapshot のコピーとリストアがサポートされます。

Element 10.1 以降を実行するシステムには、 9.3 以降の ONTAP システム上の SnapMirror と直接通信できるコードが組み込まれています。Element API には、クラスタ、ボリューム、 Snapshot で SnapMirror 機能を有効にするメソッドが用意されています。さらに、 Element UI には、 Element ソフトウェアと ONTAP システムの間の SnapMirror 関係を管理する機能が搭載されています。

Element 10.3 以降および ONTAP 9.4 以降のシステムでは、機能は限定されますが、特定のユースケースで ONTAP ボリュームを Element ボリュームにレプリケートできます。

詳細については、 ONTAP のドキュメントを参照してください。

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、 Element クラスタから外部のオブジェクトストア、または別の Element 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。

Element 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

保護ドメインは、データの可用性を維持したまま、任意の部分またはすべてで障害が発生する可能性があるように、グループ化されたノードまたはノードのセットです。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。

NetApp Element Plug-in for vCenter Server の 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。Element API または Web UI を使用して、保護ドメインの監視を有効に

することもできます。

Protection Domain レイアウトは、各ノードを特定の保護ドメインに割り当てます。

保護ドメインレベルと呼ばれる 2 つの異なる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、各ノードが独自の保護ドメインに存在します。
- シャーシレベルでは、シャーシを共有するノードのみが同じ保護ドメインに存在します。
  - 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。

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。

カスタム保護ドメイン

特定のシャーシおよびノードレイアウトに一致するカスタム保護ドメインレイアウトを定義し、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るようにすることができます。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。

クラスタにカスタムの保護ドメインを設定すると、 Element Web UI ダッシュボードに表示される 3 つのレベルで保護が可能です。

- Not protected ：ストレージクラスタ内のカスタムの保護ドメインのいずれかに障害が発生しても、ストレージクラスタは保護されません。これを修正するには、クラスタにストレージ容量を追加するか、クラスタをデータ損失から保護するようにクラスタのカスタムの保護ドメインを再設定します。
- フォールトトレランス：カスタムの保護ドメインの 1 つで障害が発生した場合にデータ損失を防ぐために、ストレージクラスタに十分な空き容量が確保されています。
- 障害への耐障害性：カスタムの保護ドメインの 1 つに障害が発生した場合に自己回復可能な十分な空き容量がストレージクラスタにある。修復プロセスの完了後、他のドメインで障害が発生してもクラスタはデータ損失から保護されます。

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個別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。

次の API メソッドを使用すると、カスタムの保護ドメインを設定できます。

- "GetProtectionDomainLayout の略" - 各ノードがどのシャーシに配置されているか、およびどのカスタム保護ドメインが表示されます。
- "SetProtectionDomainLayout の略" - 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。

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。

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

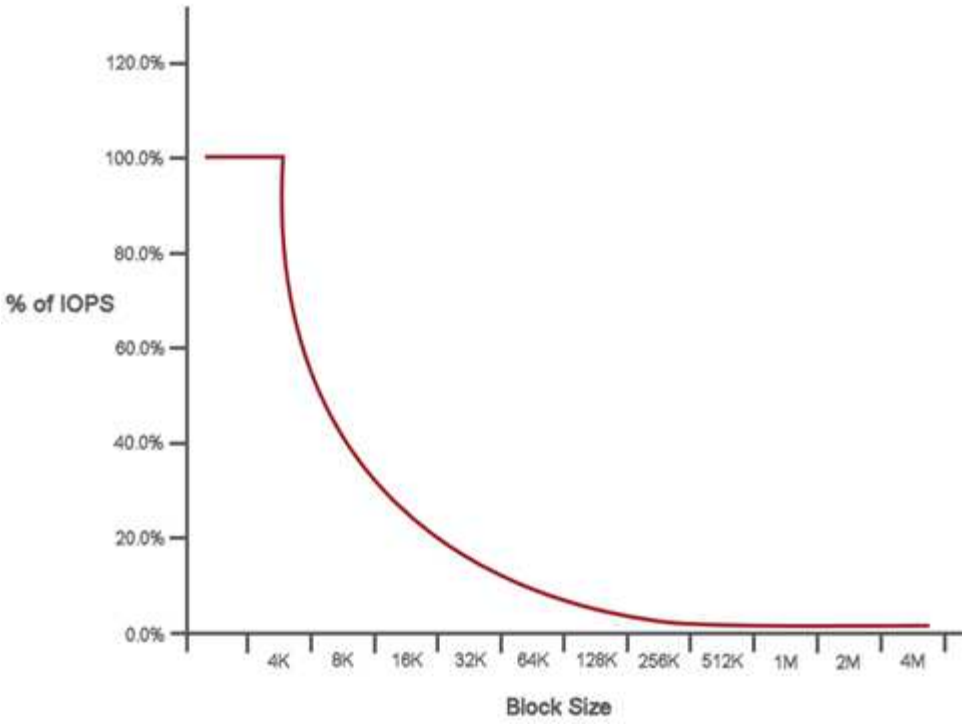
- これらは概算値です。** 最大 IOPS とバースト IOPS は最大 200 、 000 に設定できます。ただし、この設定は、ボリュームのパフォーマンスの制限を意図的に解放する場合にのみ使用できます。実際のボリュームの最大パフォーマンスは、クラスタの使用率とノードごとのパフォーマンスによって制限されます。

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

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

著作権に関する情報

商標に関する情報