概念
Element Software

NetApp
November 18, 2025

目次

概念

Element ソフトウェアに関連する基本的な概念を学びます。

- "製品概要"
- 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
- "ボリューム"
- データ保護
- パフォーマンスとサービス品質

製品概要

SolidFireオールフラッシュ ストレージ システムは、単一のストレージ リソース プールに結合された個別のハードウェア コンポーネント (ドライブとノード) で構成されています。この統合クラスタは、外部クライアントが使用する単一のストレージ システムとして提供され、 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クラスター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 インフラストラクチャ全体のストレージ アクティビティを管理できます。

SolidFireの機能

Solidfire システムは、次の機能を提供します。

- 大規模なプライベートクラウドインフラストラクチャに高性能ストレージを提供します
- 変化するストレージニーズに対応できる柔軟なスケールを提供します
- API駆動型ストレージ管理Elementソフトウェアインターフェースを使用
- サービス品質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間での自動負荷分散が含まれます
- ノードが追加または削除されると、クラスターのバランスを自動的に再調整します。

SolidFireの導入

NetAppが提供し、 NetApp Elementソフトウェアと統合されたストレージ ノードを使用します。

"SolidFireオールフラッシュストレージアーキテクチャの概要"

詳細情報の参照

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

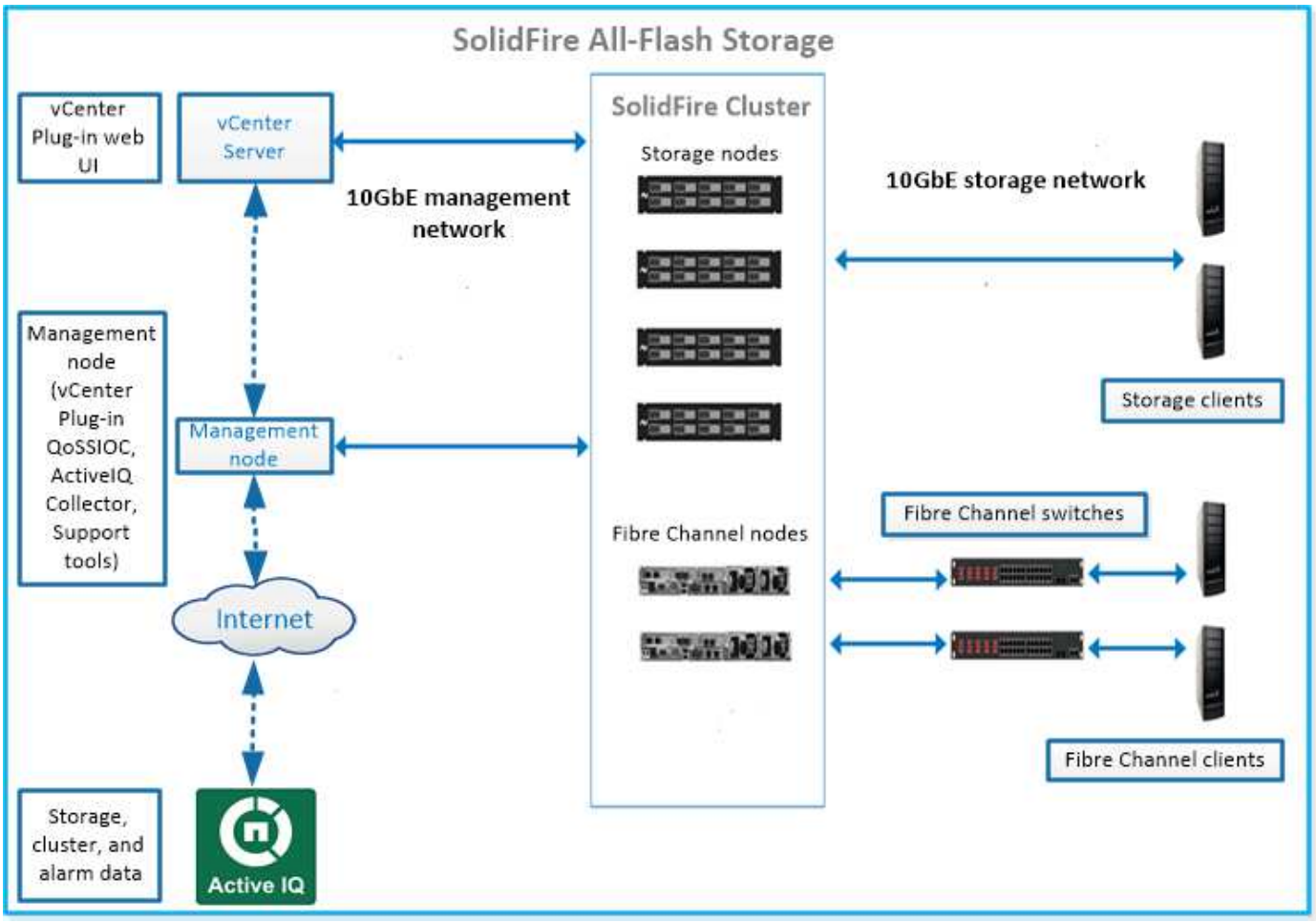
アーキテクチャとコンポーネント

SolidFireアーキテクチャについて学ぶ

SolidFireオールフラッシュ ストレージ システムは、個別のハードウェア コンポーネント (ドライブとノード) で構成され、各ノードで独立して実行されるNetApp Elementソフトウェアを使用してストレージ リソースのプールに結合されます。この単一のストレージ システムは、Element ソフトウェア 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 システムには、次のハードウェア コンポーネントが含まれています。

- クラスター: ノードの集合であるSolidFireストレージ システムのハブ。
- ノード: クラスター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。
  - ストレージノードは、ドライブの集合を含むサーバーです。
  - FCクライアントへの接続に使用するファイバーチャネル（FC）ノード
- ドライブ: クラスターのデータを保存するためにストレージ ノードで使用されます。ストレージ ノードには 2 種類のドライブが含まれます。
  - ボリューム メタデータ ドライブには、クラスター内のボリュームやその他のオブジェクトを定義する情報が保存されます。
  - ブロック ドライブはボリュームのデータ ブロックを保存します。



Element Web UI やその他の互換性のあるツールを使用して、システムを管理、監視、更新できます。

- "SolidFireソフトウェアインターフェース"
- "SolidFireActive IQ"
- "Elementソフトウェアの管理ノード"
- "管理サービス"

一般的な**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 は次のとおりです。

URL	説明
`https://[storage cluster MVIP address]`	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関するアラートを受信します。
`https://[management node IP address]`	NetApp Hybrid Cloud Control にアクセスして、ストレージのインストールをアップグレードし、管理サービスを更新します。

URL	説明
`https://[IP address]:442`	ノードごとの UI から、ネットワークとクラスターの設定にアクセスし、システム テストとユーティリティを利用します。"詳細情報"
`https://[management node IP address]/mnode`	管理ノードから管理サービス REST API およびその他の機能を使用します。"詳細情報"
`https://[management node IP address]:9443`	vSphere Web Client に vCenter プラグイン パッケージを登録します。"詳細情報"

詳細情報の参照

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

SolidFireソフトウェアインターフェース

さまざまなNetApp Elementソフトウェア インターフェイスと統合ユーティリティを使用して、 SolidFireストレージ システムを管理できます。

オプション

- NetApp Elementソフトウェア ユーザー インターフェース
- NetApp Elementソフトウェア API
- vCenter Server 用NetApp Elementプラグイン
- NetApp Hybrid Cloud Control
- 管理ノードUI
- [追加の統合ユーティリティとツール]

NetApp Elementソフトウェア ユーザー インターフェース

Element ストレージを設定し、クラスターの容量とパフォーマンスを監視し、マルチテナント インフラストラクチャ全体でストレージ アクティビティを管理できます。 Element は、 SolidFireクラスターの中核となるストレージ 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ー内のすべてのノードで独立して実行され、クラスターのノードが外部クライアントに単一のストレージ システムとして提示されるリソースを組み合わせることを可能にします。 Element ソフトウェアは、システム全体のすべてのクラスター調整、スケール、および管理を担当します。ソフトウェア インターフェイスは Element API 上に構築されています。

"Elementソフトウェアでストレージを管理する"

NetApp Elementソフトウェア API

オブジェクト、メソッド、ルーチンのセットを使用して要素のストレージを管理できるようになります。 Element API は、HTTPS 経由の JSON-RPC プロトコルに基づいています。 API ログを有効にすると、Element UI で API 操作を監視できます。これにより、システムに発行されているメソッドを確認できます。リクエストとレスポンスの両方を有効にして、発行されたメソッドに対してシステムがどのように応答するかを確認できます。

"Element APIでストレージを管理する"

vCenter Server 用NetApp Elementプラグイン

VMware vSphere 内の Element UI の代替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 クラスターを構成および管理できます。

"vCenter Server 用NetApp Elementプラグイン"

NetApp Hybrid Cloud Control

NetApp Hybrid Cloud Control インターフェイスを使用して、Element ストレージおよび管理サービスをアップグレードし、ストレージ資産を管理できるようになります。

"NetApp Hybrid Cloud Control でストレージを管理および監視"

管理ノードUI

管理ノードには、REST ベースのサービスを管理するための UI と、ネットワークとクラスターの設定、オペレーティング システムのテストとユーティリティを管理するためのノードごとの UI の 2 つの UI が含まれています。 REST API UI からは、管理ノードからサービスベースのシステム機能を制御するサービス関連 API のメニューにアクセスできます。

追加の統合ユーティリティとツール

通常、ストレージはNetApp Element、 NetApp Element API、およびNetApp Element Plug-in for vCenter Server を使用して管理しますが、追加の統合ユーティリティおよびツールを使用してストレージにアクセスすることもできます。

Element CLI

"Element 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。

要素 PowerShell ツール

"要素 PowerShell ツール"Element API を使用してSolidFireストレージ システムを管理する Microsoft Windows PowerShell 関数のコレクションを使用できるようになります。

要素SDK

"要素SDK"以下のツールを使用してSolidFireクラスターを管理できます。

- Element Java SDK: プログラマーが Element API を Java プログラミング言語に統合できるようにします。
- Element .NET SDK: プログラマーが Element API を .NET プログラミング プラットフォームに統合できるようにします。
- Element Python SDK: プログラマーが Element API を Python プログラミング言語に統合できるようにします。

SolidFire Postman API テストスイート

プログラマーがコレクションを利用できるようにする"郵便配達員"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、複製されたSolidFireストレージ クラスター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。

SolidFirevRO

"SolidFirevRO"Element API を使用して、VMware vRealize Orchestrator でSolidFireストレージ システムを管理する便利な方法を提供します。

SolidFire VSSプロバイダー

"SolidFire VSSプロバイダー"VSS シャドウ コピーを Element スナップショットおよびクローンと統合します。

詳細情報の参照

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

SolidFireActive IQ

"SolidFireActive IQ"クラスター全体のデータの継続的に更新された履歴ビューを提供する Web ベースのツールです。特定のイベント、しきい値、またはメトリックに対してアラートを設定できます。 SolidFire Active IQすると、システムのパフォーマンスと容量を監視し、クラスターの健全性に関する情報を常に把握できます。

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

- ノードの数とノードのステータス: 正常、オフライン、または障害
- CPU、メモリ使用量、ノードスロットリングのグラフィカルな表現
- ノードに関する詳細情報（シリアル番号、シャーシ内のスロット位置、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）
- 仮想マシンのCPUおよびストレージ関連の情報

SolidFire Active IQの詳細については、 "SolidFire Active IQドキュメント" 。

詳細情報

- "SolidFireおよびElementソフトウェアのドキュメント"
- "vCenter Server 用NetApp Elementプラグイン"
- **NetApp**サポート サイト › **Active IQ**用ツール

Elementソフトウェアの管理ノード

その"管理ノード（mNode）"1 つ以上の Element ソフトウェア ベースのストレージ クラスターと並行して実行される仮想マシンです。このノードは、監視とテレメトリなどのシステム サービスのアップグレードと提供、クラスタのアセットと設定の管理、システムのテストとユーティリティの実行、NetAppサポートへのアクセス許可（トラブルシューティング）に使用します。

管理ノードはストレージ クラスターと対話して管理アクションを実行しますが、ストレージ クラスターのメンバーではありません。管理ノードは、API 呼び出しを通じてクラスターに関する情報を定期的に収集し、リモート監視 (有効な場合) のためにこの情報をActive IQに報告します。管理ノードは、クラスター 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、メジャー リリース以外で選択したソフトウェア サービスの更新を迅速に行うことができます。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*は"管理ノード"これにより、メジャー リリース以外で特定のソフトウェア サービスの更新を迅速に行うことができます。

管理サービスは、 SolidFireオールフラッシュ ストレージの集中管理機能と拡張管理機能を提供します。これらのサービスには以下が含まれます"NetApp Hybrid Cloud Control"、 Active IQシステムのテレメトリ、ログ記録、サービス更新、および vCenter の Element プラグインの QoSSIOC サービス。

詳細はこちら"管理サービスリリース"。

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ーにグループ化されたハードウェアまたは仮想リソースです。

NetApp Elementソフトウェアは、クラスターのさまざまなノード ロールを定義します。ノード ロールの種類は次のとおりです。

- [管理ノード]
- ストレージ ノード
- [ファイバーチャネルノード]

ノードの状態クラスター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、監視やテレメトリなどのシステム サービスのアップグレードと提供、クラスタ 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NetAppサポート アクセスの有効化などに使用される仮想マシンです。"詳細情報"

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介して相互に通信するドライブのコレクションを含むサーバーです。ノード内のドライブには、データの保存とデータ管理のためのブロックとメタデータのスペースが含まれています。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 ノードには次の特性があります。

- 各ノードには一意の名前があります。管理者がノード名を指定しない場合は、デフォルトで SF-XXXX に設定されます。ここで、XXXX はシステムによって生成される 4 つのランダムな文字です。
- 各ノードには独自の高性能な不揮発性ランダム アクセス メモリ (NVRAM) 書き込みキャッシュがあり、システム全体のパフォーマンスを向上させ、書き込みの待ち時間を短縮します。
- 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、それぞれ冗長性とパフォーマンスのために 2 つの独立したリンクを備えています。各ノードには、各ネットワーク上の IP アドレスが必要です。
- 新しいストレージ ノードを使用してクラスターを作成したり、既存のクラスターにストレージ ノードを追加してストレージ容量とパフォーマンスを向上させることができます。
- サービスを中断することなく、いつでもクラスターにノードを追加したり削除したりできます。

ファイバーチャネルノード

SolidFireファイバー チャネル ノードはファイバー チャネル スイッチへの接続を提供し、ファイバー チャネル クライアントに接続できます。ファイバー チャネル ノードは、ファイバー チャネル 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します。これにより、新規または既存のSolidFireクラスターにファイバー チャネル接続を追加できます。

ファイバー チャネル ノードには次の特性があります。

- ファイバー チャネル スイッチはファブリックの状態を管理し、最適化された相互接続を提供します。
- 2 つのポート間のトラフィックはスイッチのみを通過し、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ており、他のポートの動作に影響を与えません。
- ファブリック内で複数のポートのペアが同時に通信できます。

ノードの動作状態

ノードは、構成のレベルに応じて、いくつかの状態のいずれかになります。

- 利用可能

  ノードには関連付けられたクラスター名がなく、まだクラスターの一部ではありません。

- 保留中

  ノードが設定され、指定されたクラスターに追加できます。

  ノードにアクセスするために認証は必要ありません。

- アクティブ保留中

  システムは、ノードに互換性のある Element ソフトウェアをインストール中です。完了すると、ノードはアクティブ状態に移行します。

- アクティブ

  ノードはクラスターに参加しています。

  ノードを変更するには認証が必要です。

これらの各状態では、一部のフィールドは読み取り専用になります。

詳細情報の参照

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

クラスタ

クラスターはSolidFireストレージ システムのハブであり、ノードの集合で構成されます。 SolidFire のストレージ効率を実現するには、クラスター内に少なくとも 4 つのノードが必要です。クラスターは単一の論理グループとしてネットワーク上に表示され、ブロック ストレージとしてアクセスできるようになります。

新しいクラスターを作成すると、ノードがクラスターの通信所有者として初期化され、クラスター内の各ノードのネットワーク通信が確立されます。このプロセスは、新しいクラスターごとに 1 回だけ実行されます。Element UI または API を使用してクラスターを作成できます。

追加のノードを追加することでクラスターをスケールアウトできます。新しいノードを追加しても、サービスは中断されず、クラスターは新しいノードのパフォーマンスと容量を自動的に使用します。

管理者とホストは仮想 IP アドレスを使用してクラスターにアクセスできます。クラスター内の任意のノードが仮想 IP アドレスをホストできます。管理仮想 IP (MVIP) は 1GbE 接続を介してクラスター管理を可能にし、ストレージ仮想 IP (SVIP) は 10GbE 接続を介してストレージへのホスト アクセスを可能にします。これらの仮想 IP アドレスにより、 SolidFireクラスターのサイズや構成に関係なく、一貫した接続が可能になります。仮想 IP アドレスをホストしているノードに障害が発生した場合、クラスター内の別のノードが仮想 IP アドレスのホスティングを開始します。

> Element バージョン 11.0 以降では、管理ネットワークのノードに IPv4、IPv6、またはその両方のアドレスを構成できます。これは、IPv6 をサポートしない管理ノード 11.3 以降を除き、ストレージ ノードと管理ノードの両方に適用されます。クラスターを作成する場合、MVIP には単一の IPv4 または IPv6 アドレスのみを使用でき、対応するアドレス タイプをすべてのノードで構成する必要があります。

クラスターの詳細

- [権威あるストレージクラスター]
- [三分割法]

- [取り残された容量]
- [ストレージ効率]
- [ストレージクラスタークォーラム]

権威あるストレージクラスター

権限のあるストレージ クラスターは、 NetApp Hybrid Cloud Control がユーザーを認証するために使用するストレージ クラスターです。

管理ノードにストレージ クラスターが 1 つしかない場合は、それが権限のあるクラスターになります。管理ノードに 2 つ以上のストレージ クラスタがある場合、それらのクラスタの 1 つ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ーのみがNetApp Hybrid Cloud Control にログインできるようになります。どのクラスターが権威あるクラスターであるかを調べるには、 `GET /mnode/about` API。応答では、`token_url`フィールドは、権限のあるストレージ クラスターの管理仮想 IP アドレス (MVIP) です。権限のあるクラスタにいないユーザーとしてNetApp Hybrid Cloud Control にログインしようとすると、ログイン試行は失敗します。

NetApp Hybrid Cloud Control の多くの機能は複数のストレージ クラスターで動作するように設計されていますが、認証と承認には制限があります。認証と承認に関する制限は、権限のあるクラスターのユーザーは、他のストレージ クラスターのユーザーでなくても、 NetApp Hybrid Cloud Control に関連付けられた他のクラスターでアクションを実行できることです。

複数のストレージ クラスターの管理に進む前に、権限のあるクラスターで定義されているユーザーが、他のすべてのストレージ クラスターでも同じ権限で定義されていることを確認する必要があります。ユーザーの管理は、"Elementソフトウェアのユーザーインターフェース" 。

見る"ストレージクラスター資産の作成と管理"管理ノード ストレージ クラスター アセットの操作の詳細については、こちらをご覧ください。

三分割法

NetApp SolidFireストレージ クラスター内でストレージ ノード タイプを混在させる場合、単一のストレージ ノードにストレージ クラスターの合計容量の 33% を超える容量を含めることはできません。

取り残された容量

新しく追加されたノードがクラスターの総容量の 50% 以上を占める場合、このノードの容量の一部は使用不可 (「取り残される」) になり、容量ルールに準拠します。ストレージ容量が追加されるまで、この状況は続きます。容量ルールにも従わない非常に大きなノードが追加された場合、以前に取り残されていたノードは取り残されなくなりますが、新しく追加されたノードは取り残されます。このような事態を回避するには、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、適切なクラスター障害がスローされます。

ストレージ効率

Netapp SolidFireストレージ クラスターは、重複排除、圧縮、シン プロビジョニングを利用して、ボリュームの保存に必要な物理ストレージの量を削減します。

- 圧縮

  圧縮では、データ ブロックを圧縮グループにまとめ、各ブロックを 1 つのブロックとして保存することで、ボリュームに必要な物理ストレージの量を削減します。

- 重複排除

  重複排除は、重複したデータ 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を削減します。

- 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 は、ストレージが事前に予約されていないボリュームまたは LUN です。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、空き領域がストレージシステムに解放されます。

ストレージクラスタークォーラム

Element ソフトウェアは、選択されたノードからストレージ クラスターを作成し、クラスター構成の複製されたデータベースを維持します。クラスターの回復力を確保するためにクォーラムを維持するには、少なくとも 3 つのノードがクラスター アンサンブルに参加する必要があります。

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、データは業界標準のセキュリティ プロトコルによって保護されます。

保存時の暗号化（ハードウェア）

ストレージ ノード内のすべてのドライブは、ドライブ レベルで AES 256 ビット暗号化を活用する暗号化が可能です。各ドライブには、ドライブが最初に初期化された際に作成される、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。このパスワードは、ドライブへのすべてのアクセスをパスワードで保護するために使用されます。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が、ドライブの電源が切断されるかドライブがロックされない限り、パスワードは必要ありません。

"保存時のハードウェア暗号化機能を有効にする"クラスターのパフォーマンスや効率には影響しません。暗号化が有効になっているドライブまたはノードが Element API または Element UI を使用してクラスター構成から削除されると、ドライブ上の保存時の暗号化は無効になります。ドライブを取り外した後、ドライブは`SecureEraseDrives`API メソッド。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、データはクラスター全体のパスワードとドライブの個別の暗号化キーによって保護されたままになります。

保存時の暗号化（ソフトウェア）

もう 1 つのタイプの保存時暗号化であるソフトウェア保存時暗号化を使用すると、ストレージ クラスター内の SSD に書き込まれるすべてのデータを暗号化できます。"有効にすると" 、書き込まれるすべてのデータを暗号化し、読み取られるすべてのデータをソフトウェアで自動的に復号化します。保存時のソフトウェア暗号化は、ハードウェアでの自己暗号化ドライブ (SED) 実装を反映し、SED がない場合でもデータのセキュリティを確保します。

SolidFireオールフラッシュ ストレージ クラスターの場合、保存時のソフトウェア暗号化はクラスターの作成中に有効にする必要があり、クラスターの作成後は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時暗号化は、どちらも単独で使用することも、組み合わせて使用することもできます。

外部キー管理

Element ソフトウェアを構成して、サードパーティの KMIP 準拠のキー管理サービス (KMS) を使用してストレージ クラスターの暗号化キーを管理できます。この機能を有効にすると、ストレージ クラスターのクラスター全体のドライブ アクセス パスワード暗号化キーは、指定した KMS によって管理されます。

Element は次のキー管理サービスを使用できます。

- ジェムアルト セーフネット キーセキュア
- セーフネット AT キーセキュア
- HyTrust キーコントロール
- Vormetric データセキュリティマネージャー
- IBM セキュリティ キー ライフサイクル マネージャー

外部キー管理の設定の詳細については、以下を参照してください。"外部キー管理を始める"ドキュメント。

多要素認証

多要素認証 (MFA) を使用すると、ログイン時にNetApp Element Web UI またはストレージ ノード UI で認証するために、ユーザーに複数の種類の証拠の提示を求めることができます。既存のユーザー管理システムおよび ID プロバイダー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 を構成できます。 Element を既存の SAML 2.0 ID プロバイダーと統合するように構成して、パスワードとテキスト メッセージ、パスワードと電子メール メッセージ、その他の方法など、複数の認証スキームを適用できます。

多要素認証は、Microsoft Active Directory Federation Services (ADFS) や Shibboleth などの一般的な SAML 2.0 互換 ID プロバイダー (IdP) と組み合わせることができます。

MFAを設定するには、 "多要素認証を有効にする" ドキュメント。

HTTPSおよび保存データの暗号化のためのFIPS 140-2

NetApp SolidFireストレージ クラスターは、暗号化モジュールの連邦情報処理規格 (FIPS) 140-2 要件に準拠した暗号化をサポートします。 SolidFireクラスターで、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。

クラスターで FIPS 140-2 動作モードを有効にすると、クラスターはNetApp暗号化セキュリティ モジュール (NCSM) をアクティブ化し、 NetApp Element UI および API への HTTPS 経由のすべての通信に FIPS 140-2 レベル 1 認定の暗号化を活用します。あなたは `EnableFeature`要素APIと `fips`FIPS 140-2 HTTPS 暗号化を有効にするパラメーター。 FIPS互換ハードウェアを搭載したストレージクラスタでは、保存データのFIPSドライブ暗号化を次のように有効にすることもできます。 `EnableFeature`要素APIと `FipsDrives`パラメータ。

FIPS 140-2暗号化用の新しいストレージクラスタの準備の詳細については、以下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" 。

既存の準備済みクラスタでFIPS 140-2を有効にする方法の詳細については、以下を参照してください。"EnableFeature要素API" 。

詳細情報

- "SolidFireおよびElementソフトウェアのドキュメント"
- "vCenter Server 用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、アクセスを提供するには、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 ストレージを使用すると、次の種類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ーの管理者ユーザーアカウント
- ストレージボリュームアクセス用のユーザーアカウント
- NetApp Hybrid Cloud Control の権限のあるクラスタ ユーザー アカウント

ストレージ クラスター管理者アカウント

NetApp Elementソフトウェアを実行しているストレージ クラスターには、次の 2 種類の管理者アカウントが存在できます。

- プライマリ クラスター管理者アカウント: この管理者アカウントは、クラスターの作成時に作成されます。このアカウントは、クラスターへの最高レベルのアクセス権を持つプライマリ管理アカウントです。このアカウントは、Linux システムの root ユーザーに類似しています。この管理者アカウントのパスワードを変更できます。
- クラスター管理者アカウント: クラスター管理者アカウントに、クラスター内で特定のタスクを実行するための限定された範囲の管理アクセス権を付与できます。各クラスター管理者アカウントに割り当てられた資格情報は、ストレージ システム内の API および Element UI 要求を認証するために使用されます。

> ノードごとの UI を介してクラスター内のアクティブなノードにアクセスするには、ローカル (LDAP 以外の) クラスター管理者アカウントが必要です。まだクラスターの一部ではないノードにアクセスするには、アカウント資格情報は必要ありません。

あなたはできる"クラスタ管理者アカウントを管理する"クラスタ管理者アカウントを作成、削除、編集し、クラスタ管理者パスワードを変更し、LDAP 設定を構成してユーザーのシステム アクセスを管理します。

ユーザ アカウント

ユーザー アカウントは、 NetApp Elementソフトウェア ベース 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されます。ボリュームを作成するには、少なくとも 1 つのユーザー アカウントが必要です。

ボリュームを作成すると、アカウントに割り当てられます。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 コンテナーになります。

追加の考慮事項を次に示します。

- アカウントには、割り当てられたボリュームにアクセスするために必要な CHAP 認証が含まれています。

- 1 つのアカウントには最大 2000 個のボリュームを割り当てることができますが、1 つのボリュームは 1 つのアカウントにのみ属することができます。
- ユーザー アカウントは、 NetApp Element Management 拡張ポイントから管理できます。

権限のあるクラスターユーザーアカウント

権限のあるクラスタ ユーザー 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た任意のストレージ アセットに対して認証できます。このアカウントを使用すると、すべてのクラスターにわたってボリューム、アカウント、アクセス グループなどを管理できます。

権限のあるユーザー アカウントは、 NetApp Hybrid Cloud Control の右上メニューの [ユーザー管理] オプションから管理されます。

その"権威ストレージクラスター"NetApp Hybrid Cloud Control がユーザーを認証するために使用するストレージ クラスターです。

権限のあるストレージ クラスター上に作成されたすべてのユーザーは、 NetApp Hybrid Cloud Control にログインできます。他のストレージ クラスターで作成されたユーザーは、Hybrid Cloud Control にログインできません。

- 管理ノードにストレージ クラスターが 1 つしかない場合は、それが権限のあるクラスターになります。
- 管理ノードに 2 つ以上のストレージ クラスタがある場合、それらのクラスタの 1 つ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ーのみがNetApp Hybrid Cloud Control にログインできるようになります。

多くのNetApp Hybrid Cloud Control 機能は複数のストレージ クラスターで動作しますが、認証と承認には必要な制限があります。認証と承認に関する制限は、権限のあるクラスターのユーザーは、他のストレージ クラスターのユーザーでなくても、 NetApp Hybrid Cloud Control に関連付けられた他のクラスターでアクションを実行できることです。複数のストレージ クラスターの管理に進む前に、権限のあるクラスターで定義されているユーザーが、他のすべてのストレージ クラスターでも同じ権限で定義されていることを確認する必要があります。 NetApp Hybrid Cloud Control からユーザーを管理できます。

ボリュームアカウント

ボリューム固有のアカウントは、作成されたストレージ クラスターにのみ固有です。これらのアカウントを使用すると、ネットワーク全体の特定のボリュームに対する権限を設定できますが、それらのボリューム外部には影響がありません。

ボリューム アカウントは、 NetApp Hybrid Cloud Control Volumes テーブル内で管理されます。

ストレージ

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 またはファイバー チャネル クライアントによっ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。

エレメント ストレージを使用すると、ユーザー アカウントのボリュームを作成、表示、編集、削除、複製、

バックアップ、または復元できます。クラスター上の各ボリュームを管理したり、ボリューム アクセス グループ内のボリュームを追加または削除したりすることもできます。

永続ボリューム

永続ボリュームを使用すると、管理ノードの構成データを VM のローカルではなく、指定されたストレージ クラスターに保存できるため、管理ノードが失われたり削除されたりした場合でもデータを保持できます。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構成です。

永続ボリュームを有効にするオプションは、インストールおよびアップグレードスクリプトに含まれています。"新しい管理ノードを展開する" 。永続ボリュームは、VM の寿命を超えて存続するホスト管理ノード VM の管理ノード構成情報を含む、Element ソフトウェアベースのストレージ クラスター上のボリュームです。管理ノードが失われた場合、代替の管理ノード VM が失われた VM に再接続し、構成データを回復できます。

インストールまたはアップグレード中に永続ボリューム機能を有効にすると、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、他の Element ソフトウェア ベースのボリュームと同様に、設定とインストールに応じて、Element ソフトウェア Web UI、vCenter Server 用のNetApp Elementプラグイン、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構成データを維持するには、管理ノードへの iSCSI 接続を使用して永続ボリュームが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は、インストールまたはアップグレード中に作成され、新しいアカウントに割り当てられます。永続ボリュームを使用している場合は、ボリュームやそれに関連付けられた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（**vVols**）

vSphere Virtual Volumes は、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 に移行する VMware のストレージ パラダイムです。仮想ボリューム (vVols) を使用すると、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。

バインディング

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ディングを作成し、そのバインディングを ESXi ホストに返します。バインドされると、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 操作を実行できるようになります。

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、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て I/O 操作を実行します。ホスト上の仮想マシンが I/O 操作を実行すると、関連付けられたプロトコル エンドポイントは、ペアになっている仮想ボリュームに I/O を送信します。

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ーによって自動的に作成されます。クラスター内の各ノードに対して、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 ノードのクラスターには 4 つのプロトコル エンドポイントがあります。

iSCSI は、 NetApp Elementソフトウェアでサポートされている唯一のプロトコルです。ファイバー チャネル プロトコルはサポートされていません。プロトコル エンドポイントは、ユーザーによって削除または変更することはできず、アカウントに関連付けられておらず、ボリューム アクセス グループに追加することもできません。

保管容器

ストレージ コンテナは、 NetApp Elementアカウントにマップされ、レポートとリソースの割り当てに使用される論理構造です。これらは、生のストレージ容量をプールするか、ストレージ システムが仮想ボリュームに提供できるストレージ機能を集約します。 vSphere で作成された VVol データストアは、個別のストレージ コンテナーにマップされます。デフォルトでは、単一のストレージ コンテナーにNetApp Elementクラスターから使用可能なすべてのリソースが含まれます。マルチテナントに対してよりきめ細かなガバナンスが必要な場合は、複数のストレージ コンテナーを作成できます。

ストレージ コンテナーは従来のアカウントのように機能し、仮想ボリュームと従来のボリュームの両方を含めることができます。クラスターごとに最大 4 つのストレージ コンテナーがサポートされます。 VVols 機能を使用するには、少なくとも 1 つのストレージ コンテナーが必要です。 VVol の作成中に、vCenter でストレージ コンテナーを検出できます。

VASAプロバイダー

vSphere がNetApp Elementクラスタ上の vVol 機能を認識できるようにするには、vSphere 管理者がNetApp Element VASA プロバイダーを vCenter に登録する必要があります。 VASA プロバイダーは、vSphere と Element クラスタ間の帯域外制御パスです。 VM の作成、VM を vSphere で使用可能にする、ストレージ機能を vSphere にアドバタイズするなど、vSphere に代わって Element クラスタ上でリクエストを実行する役割を担います。

VASA プロバイダーは、Element ソフトウェアのクラスター マスターの一部として実行されます。クラスター マスターは、必要に応じてクラスター内の任意のノードにフェールオーバーする高可用性サービスです。クラスタ マスターがフェイルオーバーすると、VASA プロバイダーもそれとともに移動し、VASA プロバイダーの高可用性が確保されます。すべてのプロビジョニングおよびストレージ管理タスクでは、VASA プロバイダーが使用されます。VASA プロバイダーは、Element クラスターで必要な変更を処理します。

Element 12.5 以前の場合、1 つの vCenter インスタンスに複数のNetApp Element VASA プロバイダーを登録しないでください。 2 番目のNetApp Element VASA プロバイダーが追加されると、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 プロバイダーを vCenter にすでに登録している場合は、最大 10 個の vCenter に対する VASA サポートがアップグレード パッチとして利用できます。インストールするには、VASA39マニフェストの指示に従って、.tar.gzファイルを"NetAppソフトウェア ダウンロード"サイト。 NetApp Element VASA プロバイダーはNetApp証明書を使用します。このパッチにより、証明書は vCenter によって変更されずに使用され、VASA および VVols の使用のために複数の vCenter がサポートされるようになります。証明書を変更しないでください。カスタム SSL 証明書は VASA ではサポートされていません。

詳細情報の参照

- "SolidFireおよびElementソフトウェアのドキュメント"
- "vCenter Server 用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、ボリューム セットへのアクセスを制御できます。ボリューム セットとイニシエーター セットをボリューム 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ーにそのボリューム 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 グループにより、iSCSI イニシエーター IQN またはファイバー チャネル WWPN がボリュームのコレクションにアクセスできるようになります。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 グループに追加する各 WWPN により、アクセス グループ内のボリュームへのファイバー チャネル ネットワーク アクセスが可能になります。

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 個のイニシエーター。
- ボリュームあたり最大 64 個のアクセス グループ。
- アクセス グループは最大 2000 個のボリュームで構成できます。
- IQN または WWPN は、 1 つのボリューム アクセス グループにのみ属することができます。
- ファイバー チャネル クラスターの場合、1 つのボリュームは最大 4 つのアクセス グループに属することができます。

イニシエーター

イニシエーターは、外部クライアントがクラスター内のボリュームにアクセスできるようにし、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ます。ストレージ ボリュームへのアカウント ベースではなく、CHAP ベースのアクセスにイニシエーターを使用できます。単一のイニシエーターをボリューム 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を必要とせずに、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。イニシエーターは 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 スナップショット、ボリューム クローン、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。

要素ストレージのデータ保護には、次の概念が含まれます。

- [リモートレプリケーションの種類]
- [データ保護のためのボリュームスナップショット]
- ボリューム クローン
- Elementストレージのバックアップと復元プロセスの概要

- [保護ドメイン]
- カスタム保護ドメイン
- 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があります。

- [クラスター間の同期および非同期レプリケーション]
- [スナップショットのみのレプリケーション]
- SnapMirrorを使用したElementとONTAPクラスタ間のレプリケーション

詳細については、 "TR-4741: NetApp Elementソフトウェア リモート レプリケーション" 。

クラスター間の同期および非同期レプリケーション

NetApp Elementソフトウェアを実行しているクラスターでは、リアルタイム レプリケーションにより、ボリューム データのリモート コピーをすばやく作成できます。

ストレージ クラスターを最大 4 つの他のストレージ クラスターとペアリングできます。フェイルオーバーおよびフェイルバックのシナリオでは、クラスター ペアのいずれかのクラスターからボリューム データを同期的または非同期的に複製できます。

同期レプリケーション

同期レプリケーションは、ソース クラスターからターゲット クラスターにデータを継続的に複製し、遅延、パケット損失、ジッター、帯域幅の影響を受けます。

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。

- 短距離での複数システムの複製
- 発生源から地理的に近い災害復旧サイト
- 時間依存のアプリケーションとデータベースの保護
- プライマリサイトがダウンしたときにセカンダリサイトがプライマリサイトとして機能することを必要とするビジネス継続性アプリケーション

非同期レプリケーション

非同期レプリケーションは、ターゲット クラスターからの確認応答を待たずに、ソース クラスターからターゲット クラスターにデータを継続的に複製します。非同期レプリケーション中、書き込みはソース クラスターでコミットされた後にクライアント (アプリケーション) に確認応答されます。

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。

- 災害復旧サイトはソースから遠く離れており、アプリケーションはネットワークによって発生する遅延を許容しません。
- ソース クラスターとターゲット クラスターを接続するネットワークには帯域幅の制限があります。

スナップショットのみのレプリケーション

スナップショットのみのデータ保護では、特定の時点で変更されたデータをリモート クラスターに複製します。ソース クラスターで作成されたスナップショットのみが複製されます。ソースボリュームからのアクティブな書き込みは行われません。

スナップショットのレプリケーションの頻度を設定できます。

スナップショット 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**と**ONTAP**クラスタ間のレプリケーション

NetApp SnapMirrorテクノロジーを使用すると、災害復旧の目的で、 NetApp Elementソフトウェアを使用して作成されたスナップショットをONTAPに複製できます。 SnapMirror関係では、Element が一方のエンドポイントであり、 ONTAP がもう一方のエンドポイントです。

SnapMirrorは、災害復旧を容易にするNetAppスナップショット レプリケーション テクノロジであり、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ています。SnapMirrorテクノロジは本番データの複製（ミラー）をセカンダリ ストレージに作成し、プライマリ サイトで災害が発生した場合に、セカンダリ ストレージから引き続きデータを提供できるようにします。データのミラーリングはボリューム単位で行われます。

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 ストレージの宛先ボリューム間の関係は、データ保護関係と呼ばれます。クラスターはボリュームが存在するエンドポイントと呼ばれ、複製されたデータを含むボリュームはピアリングされる必要があります。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コントローラ上でネイティブに実行され、 NetApp HCIおよびSolidFireクラスタ上で実行される Element に統合されています。 SnapMirror を制御するロジックはONTAPソフトウェア内に存在するため、すべてのSnapMirror関係には、調整作業を実行するために少なくとも 1 つのONTAPシステムが関与する必要があります。ユーザーは主に Element UI を通じて Element とONTAPクラスタ間の関係を管理しますが、一部の管理タスクはNetApp ONTAP System Manager に存在します。ユーザーは、 ONTAPと Element で利用可能な CLI と API を通じてSnapMirror を管理することもできます。

見る "TR-4651: NetApp SolidFire SnapMirror のアーキテクチャと構成"（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無効になっており、新規インストールまたはアップグレードの一部として自動的に有効になることはありません。

SnapMirror を有効にすると、Element ソフトウェアの [データ保護] タブからSnapMirror関係を作成できます。

NetApp Elementソフトウェア 10.1 以降は、 ONTAPシステムでスナップショットをコピーおよび復元するためのSnapMirror機能をサポートしています。

Element 10.1 以降を実行しているシステムには、9.3 以降を実行しているONTAPシステム上のSnapMirrorと直接通信できるコードが含まれています。 Element API は、クラスター、ボリューム、スナップショットでSnapMirror機能を有効にするメソッドを提供します。さらに、Element UI には、Element ソフトウェアとONTAPシステム間のSnapMirror関係を管理する機能も含まれています。

Element 10.3 およびONTAP 9.4 システム以降では、機能が制限された特定のユースケースで、 ONTAP で生成されたボリュームを Element ボリュームに複製できます。

詳細については、 "NetApp ElementソフトウェアとONTAP間のレプリケーション (ONTAP CLI)"。

データ保護のためのボリュームスナップショット

ボリューム スナップショットは、ボリュームの特定の時点のコピーであり、後でボリュームをその特定の時点に復元するために使用できます。

スナップショットはボリューム クローンと似ていますが、スナップショットは単にボリューム メタデータのレプリカであるため、マウントしたり書き込んだりすることはできません。ボリューム スナップショットの作成には少量のシステム リソースとスペースしか必要ないため、クローン作成よりもスナップショットの作成が高速になります。

スナップショットをリモート クラスターに複製し、ボリュームのバックアップ コピーとして使用できます。これにより、複製されたスナップショット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るようになります。また、複製されたスナップショットからボリュームのクローンを作成することもできます。

Element クラスターのスナップショットを外部オブジェクト ストアまたは別の Element クラスターにバックアップできます。スナップショットを外部オブジェクト ストアにバックアップする場合は、読み取り/書き込み操作を許可するオブジェクト ストアへの接続が必要です。

データ保護のために、個々のボリュームまたは複数のボリュームのスナップショットを作成できます。

ボリューム クローン

単一ボリュームまたは複数ボリュームのクローンとは、データの特定時点のコピーです。ボリュームのクローンを作成すると、システムはボリュームのスナップショットを作成し、スナップショットによって参照されるデータのコピーを作成します。

これは非同期プロセスであり、プロセスに必要な時間は、複製するボリュームのサイズと現在のクラスターの負荷によって異なります。

クラスターは、ボリュームごとに一度に最大 2 つの実行中のクローン要求と、一度に最大 8 つのアクティブなボリューム クローン操作をサポートします。これらの制限を超えるリクエストは、後で処理するためにキューに入れられます。

Elementストレージのバックアップと復元プロセスの概要

ボリュームを他のSolidFireストレージや、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 ストアにバックアップおよび復元できます。

ボリュームを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ー
- 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 からボリュームを復元する場合は、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たボリュームを復元する場合、マニフェスト情報は必要ありません。

保護ドメイン

保護ドメインとは、データの可用性を維持しながら、その一部または全部に障害が発生しても問題がないようにグループ化されたノードまたはノード セットです。保護ドメインにより、ストレージ クラスターはシャーシ (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るようになります。

vCenter Server 用のNetApp ElementプラグインのNetApp Element構成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。ノードまたはシャーシ ドメインに基づいて保護ドメイン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。

保護ドメイン レイアウトでは、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ています。

- ノード レベルでは、各ノードは独自の保護ドメインに属します。
- 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。
  - ノードがクラスターに追加されると、シャーシ レベルのレイアウトは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内にあるクラスターでは、これら 2 つのレベルは機能的に同一です。

新しいクラスターを作成するときに、共有シャーシ内にあるストレージ ノードを使用している場合は、保護ドメイン機能を使用してシャーシ レベルの障害保護を設計することを検討してください。

カスタム保護ドメイン

特定のシャーシとノードの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、各ノードを 1 つのカスタム保護ドメインにのみ関連付けることができます。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。

カスタム保護ドメインが割り当てられていない場合:

- クラスタの動作には影響ありません。
- カスタム レベルは、寛容性も回復力もありません。

クラスターのカスタム保護ドメインを構成する場合、Element Web UI ダッシュボードから確認できる 3 つの保護レベルがあります。

- 保護されていません: ストレージ クラスターは、カスタム保護ドメインの 1 つで発生した障害から保護されていません。これを修正するには、クラスターにストレージ容量を追加するか、クラスターのカスタム保護ドメインを再構成して、クラスターをデータ損失から保護します。
- フォールト トレラント: ストレージ クラスターには、カスタム保護ドメインの 1 つに障害が発生してもデータの損失を防ぐのに十分な空き容量があります。
- 障害耐性: ストレージ クラスターには、カスタム保護ドメインの 1 つに障害が発生した後でも自己修復できる十分な空き容量があります。修復プロセスが完了すると、追加のドメインに障害が発生した場合でも、クラスター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したドメインを個別のカスタム保護ドメインに割り当てます。これが不可能な場合は、重複を別々のノードに割り当てることになります。

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 プロバイダー、アンサンブルなど) はこれを独立して実行します。

Element UIを使用すると、"カスタム保護ドメインを構成する"または、次の API メソッドを使用することもできます。

- "保護ドメインレイアウトの取得"- 各ノードがどのシャーシとどのカスタム保護ドメインに属しているかを表示します。
- "保護ドメインレイアウトの設定"- 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 つの冗長データ 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 システムのすべてのレベルにわたって複数の同時障害を吸収し、迅速に修復できるようになります。

パフォーマンスとサービス品質

SolidFireストレージ クラスターには、ボリュームごとに QoS (Quality of Service) パラメータを提供する機能があります。 QoS を定義する 3 つの構成可能なパラメータ (最小 IOPS、最大 IOPS、バースト IOPS) を使用して、1 秒あたりの入出力数 (IOPS) で測定されるクラスターのパフォーマンスを保証できます。

SolidFire Active IQには、最適な構成と QoS 設定のセットアップ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。

サービス品質パラメータ

IOPS パラメータは次のように定義されます。

- 最小 **IOPS** - ストレージ クラスターがボリュームに提供する 1 秒あたりの持続的な入出力 (IOPS) の最小数。ボリュームに設定された最小 IOPS は、ボリュームの保証されたパフォーマンス レベルです。パフォーマンスはこのレベル以下に低下しません。
- 最大 **IOPS** - ストレージ クラスターがボリュームに提供する持続的な IOPS の最大数。クラスターの IOPS レベルが非常に高い場合、この IOPS パフォーマンス レベルを超えることはありません。
- バースト **IOPS** - 短いバースト シナリオで許可される IOPS の最大数。ボリュームが最大 IOPS を下回って実行されている場合、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り、最大レベルに達すると、ボリューム上で IOPS の短時間のバーストが許可されます。

  Element ソフトウェアは、クラスターの IOPS 使用率が低い状態でクラスターが実行されているときにバースト IOPS を使用します。

  1 つのボリュームでバースト IOPS を蓄積し、クレジットを使用して、設定された「バースト期間」の間、最大 IOPS を超えてバースト IOPS レベルまでバーストすることができます。クラスターにバーストに対応できる容量がある場合、ボリュームは最大 60 秒間バーストできます。ボリュームは、最大 IOPS 制限を下回る 1 秒ごとに 1 秒のバースト クレジット (最大 60 秒) を蓄積します。

  バースト IOPS は次の 2 つの方法で制限されます。

- ボリュームは、蓄積されたバースト クレジットの数に等しい秒数、最大 IOPS を超えてバーストすることができます。
- ボリュームが最大 IOPS 設定を超えてバーストすると、バースト IOPS 設定によって制限されます。したがって、バースト IOPS はボリュームのバースト IOPS 設定を超えることはありません。

- 実効最大帯域幅 - 最大帯域幅は、IOPS 数 (QoS 曲線に基づく) と IO サイズを掛けて計算されます。

  例: QoS パラメータ設定を 100 最小 IOPS、1000 最大 IOPS、1500 バースト IOPS にすると、パフォーマンスの品質に次のような影響があります。

  - ワークロードは、クラスター上で IOPS のワークロード競合の状態が明らかになるまで、最大 1000 IOPS に到達して維持することができます。その後、すべてのボリュームの IOPS が指定された QoS 範囲内になり、パフォーマンスの競合が軽減されるまで、IOPS は段階的に削減されます。
  - すべてのボリュームのパフォーマンスは、最小 IOPS 100 に近づきます。レベルは最小 IOPS 設定を下回ることはありませんが、ワークロードの競合が軽減されると 100 IOPS より高いままになる可能性があります。
  - パフォーマンスは、持続的に 1000 IOPS を超えることはなく、100 IOPS を下回ることはありません。 1500 IOPS (バースト IOPS) のパフォーマンスは許可されますが、最大 IOPS 未満で実行してバースト クレジットを獲得したボリュームに対してのみ、短期間のみ許可されます。バーストレベルは決して持続されません。

QoS値の制限

QoS に可能な最小値と最大値は次のとおりです。

パラメータ	最小値	デフォルト	**4 4KB**	**5 8KB**	**6 16KB**	**262 KB**
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

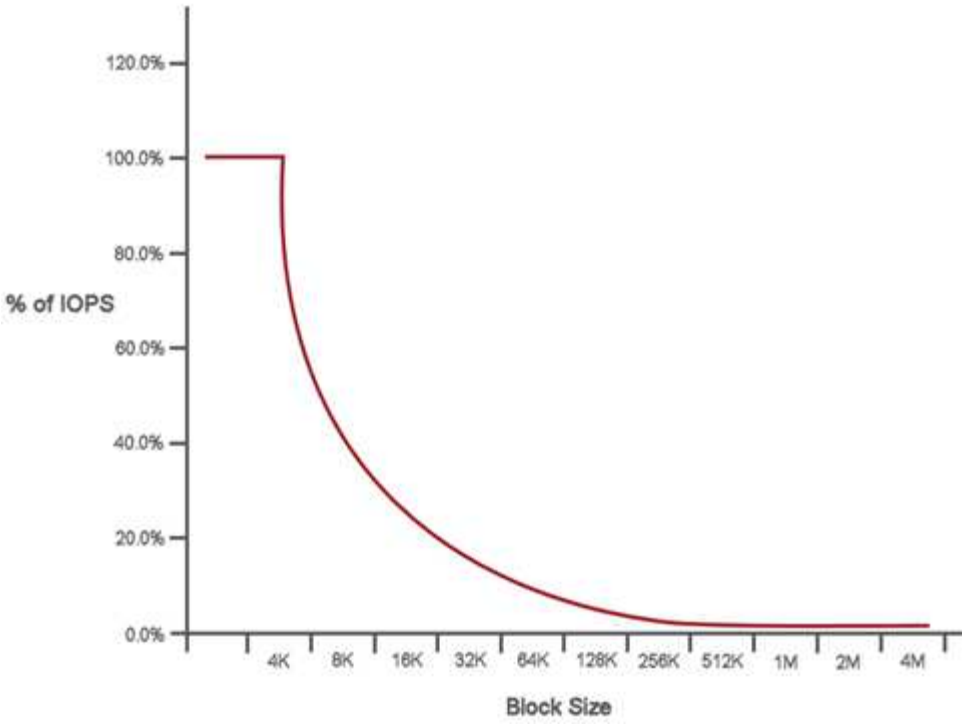
*これらの見積りは概算です。 **最大 IOPS とバースト IOPS は最大 200,000 まで設定できますが、この設定はボリュームのパフォーマンスを実質的に制限しない場合にのみ許可されます。ボリュームの実際の最大パフォーマンスは、クラスターの使用状況とノードごとのパフォーマンスによって制限されます。

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 のパーセンテージの関係を示します。

ブロック サイズと帯域幅は、アプリケーションが取得できる IOPS の数に直接影響します。 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、受信するブロック サイズを考慮します。ワークロードに基づいて、システムはブロック サイズを増やす可能性があります。ブロック サイズが大きくなるにつれて、システムはより大きなブロック サイズを処理するために必要なレベルまで帯域幅を増加させます。帯域幅が増加すると、システムが達成できる IOPS の数は減少します。

QoS パフォーマンス曲線は、ブロック サイズの増加と IOPS の割合の減少の関係を示します。



たとえば、ブロック サイズが 4k、帯域幅が 4000 KBps の場合、IOPS は 1000 になります。ブロック サイズが 8k に増加すると、帯域幅は 5000 KBps に増加し、IOPS は 625 に減少します。ブロック サイズを考慮することにより、システムは、バックアップやハイパーバイザ アクティビティなど、高いブロック サイズを使用する優先度の低いワークロードが、より小さなブロック 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過度に消費しないようにします。

QoSポリシー

QoS ポリシーを使用すると、多くのボリュームに適用できる標準化されたサービス品質設定を作成して保存できます。

QoS ポリシーは、再起動がほとんどなく、ストレージへの一定のアクセスが常に必要なデータベース、アプリケーション、インフラストラクチャ サーバーなどのサービス環境に最適です。個別ボリューム QoS は、仮想デスクトップや特殊なキオスク タイプの VM など、毎日または 1 日に数回再起動、電源オン、電源オフが行われる可能性のある軽量 VM に最適です。

QoS と QoS ポリシーを併用しないでください。 QoS ポリシーを使用している場合は、ボリューム上でカスタム QoS を使用しないでください。カスタム QoS は、ボリューム QoS 設定の QoS ポリシー値を上書きして調整します。

QoS ポリシーを使用するには、選択したクラスターが Element 10.0 以降である必要があります。それ以外の場合、QoS ポリシー機能は使用できません。

詳細情報の参照

- "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